

OpenText™ Dynamic Application Security Testing (Fortify WebInspect)

ソフトウェアバージョン: 25.4.0

Windowsオペレーティングシステムおよび一部 macOS 用 ツール

ツールガイド

ドキュメントリリース日: 2025年 10月

ソフトウェアリリース日: 2025年 10月

法的通知

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

著作権表示

Copyright 2004-2025 Open Text.

Open Textとその関連会社およびライセンサ(以下「Open Text」)の製品およびサービスに関する保証は、製品およびサービスに付属する保証規定に明示されている内容に限定されます。本書のいかなる記述も、追加の保証を構成するものではありません。Open Textは、本書の技術的誤り、編集上の誤り、欠落に関して責任を負いません。ここに記載する情報は、予告なしに変更されることがあります。

商標表示

「OpenText」およびその他のOpen Textの商標およびサービスマークは、Open Textまたはその関連会社に帰属します。その他すべての商標またはサービスマークは、それぞれの所有者に帰属します。

ドキュメントの更新情報

このドキュメントのタイトルページには、次の識別情報が記載されています。

- ソフトウェアバージョン番号
- ドキュメントリリース日。ドキュメントが更新されるたびに更新されます
- ソフトウェアリリース日。ソフトウェアのこのバージョンのリリース日付を示します

このドキュメントのは、12月 15, 2025に作成されました。

オンラインヘルプのこのPDF版について

このドキュメントは、オンラインヘルプのPDF版です。このPDFファイルの提供によって、ヘルプ情報から複数のトピックを簡単に印刷したり、オンラインヘルプをPDF形式で閲覧したりできます。このコンテンツは、もともとWebブラウザで表示するオンラインヘルプとして作成されたため、一部のトピックが適切な形式で表示されない可能性があります。このPDF版では、一部の対話型トピックを表示できない場合があります。それらのトピックは、オンラインヘルプから正常に印刷できます。

目次

序文	20
カスタマサポート へのお問い合わせ	20
詳細情報	20
製品の機能紹介ビデオ	20
変更ログ	21
第1章:OpenText™ Dynamic Application Security Testing (DAST)ツールへようこそ	24
プロキシでのツールの使用	24
製品名の変更	24
関連ドキュメント	25
すべての製品	25
OpenText ScanCentral DAST	26
OpenText DAST	26
Fortify WebInspect Enterprise	28
第2章:監査入力エディタ	30
チェック入力	30
エンジン入力	31
第3章:Compliance Manager(OpenText DASTのみ)	34
仕組み	34
コンプライアンステンプレートの作成	35
使用上のメモ	40
一般的なテキスト検索グループ	40
脅威クラス	40
第4章:エンコーダ/デコーダ	42
文字列のエンコーディング	42
文字列のデコード	43
エンコードされた文字列の操作	43

エンコーディングタイプ	44
第5章:HTTPエディタ	46
要求ビューア(Request Viewer)	47
応答ビューア(Response Viewer)	47
HTTP Editorのメニュー	47
ヘルプ(Help)]メニュー	48
要求アクション(Request actions)	48
応答アクション	50
要求の編集と送信	51
要求または応答の検索	52
設定(Settings)	53
オプション(Options)]タブ	53
認証(Authentication)]タブ	56
プロキシ(Proxy)]タブ	56
正規表現	57
正規表現の拡張と演算子	58
正規表現タグ	59
正規表現演算子	59
例	60
第6章:Log Viewer(OpenText DASTのみ)	61
第7章:ポリシーマネージャ	62
ビュー	62
ポリシーの作成または編集	65
カスタムチェックの使用	66
カスタムチェックの作成	66
カスタムチェックの有効化	74
カスタムチェックの削除	74
カスタムチェックの編集	74
特定のエージェントの検索	75
カスタムエージェントの使用	76
手法	76
パラメータ操作	77

パラメータオーバーフロー	79
パラメータ追加	79
サイト検索 (Site search)	81
アプリケーションマッピング	82
Webサーバの評価	83
コンテンツ調査	84
総当たり認証攻撃	85
既知の攻撃	85
ポリシー	85
OAST関連チェックについて	86
ベストプラクティス	86
タイプ別	87
カスタム	89
危険	90
非推奨になったチェックおよびポリシー	90
Policy Managerのアイコン	92
監査エンジン	92
監査オプション	96
一般的なアプリケーションテスト	96
サードパーティのWebアプリケーション	96
Webのフレームワーク/言語	96
Webサーバ	96
カスタムエージェント	97
カスタムチェック	97
正規表現	97
正規表現の拡張	99
正規表現タグ	99
正規表現演算子	99
例	99
第8章:正規表現エディタ	101
正規表現のテスト	101
正規表現	102
正規表現の拡張と演算子	104
正規表現の拡張	104
正規表現演算子	105

例	105
第9章:Server Analyzer(OpenText DASTのみ)	106
サーバの分析	106
設定の変更	107
Analyzerの結果のエクスポート	107
認証設定	107
認証メソッド	107
認証資格情報	108
プロキシ設定	108
直接接続(プロキシ無効)(Direct Connection (proxy disabled))	108
プロキシ設定の自動検出 (Auto detect proxy settings)	108
システムのプロキシ設定を使用する(Use system proxy settings)	108
Firefoxプロキシ設定を使用する(Use Firefox proxy settings)	108
PACファイルを使用してプロキシを設定する(Configure proxy using a PAC file)	109
プロキシを明示的に設定する(Explicitly configure proxy)	109
HTTPS用の代替プロキシを指定する(Specify alternative proxy for HTTPS)	109
第10章:Server Profiler	110
ツールとしてのServer Profilerの起動	110
スキャンの開始時にServer Profilerを起動する	111
第11章:SmartUpdate	112
SmartUpdateの実行(インターネットに接続している場合)	112
OpenText DASTを更新せずにチェックをダウンロードする	113
オフラインのSmartUpdateの実行	114
第12章:SQL Injector(OpenText DASTのみ)	115
SQL Injectorのタブ	118
要求ペイン	118
データベースペイン	119
情報ペイン	119
SQL Injectorの設定	119
オプション(Options)] タブ	119
認証(Authentication)] タブ	121
プロキシ(Proxy)] タブ	121

第13章:Traffic Viewer	123
オプションを有効にする必要がある	123
プロキシサーバ	123
Traffic Monitorの有効化	124
すべてのスキャンに対するTraffic Monitorの有効化	124
個々のスキャンに対するTraffic Monitorの有効化	124
Traffic Viewerの起動	124
開いているスキャンから	125
スタンドアロンツールとして	125
インターフェイスの使用	125
既存のファイルを開く	125
サイトツリーの使用	126
サイトツリーのアイコン	126
リソースのトラフィックの表示	126
ホスト名のみを表示	127
選択したホストのフィルタ処理	127
すべてのホスト名の表示	127
グリッドビューのカスタマイズ	127
列のサイズ変更	128
列の位置変更	128
列の追加/削除	128
詳細ビューのカスタマイズ	129
レイアウトの変更	129
カラーテーマの変更	129
[HTTP] 詳細ビューの表示と非表示	129
UI要素のサイズ変更、折りたたみ、および展開	130
要素のサイズ変更	130
要素の折りたたみ	130
要素の展開	130
自動スクロールの使用	130
自動スクロールの有効化	131
自動スクロールの無効化	131
トラフィックの操作	131
トラフィックの探索	131
リソースのトラフィックの表示	131
ブレードクラムリンクの使用	131
セッションの操作	132
HTTP詳細の表示	132
テキストの折り返し	132

パーセントエンコード文字のデコード	133
要求の再送信	133
ブラウザでのセッションの表示	133
圧縮コンテンツの展開	133
パラメータの使用	134
パラメータについて	134
パラメータ詳細の表示	134
トラフィックグリッドへのパラメータ列の追加	135
トラフィックデータのドリルダウン	135
リソースのトラフィックの表示	135
セッションの関連トラフィックの表示	135
積み重なったグリッドの操作	136
積み重なったグリッドの表示と終了	136
検索とフィルタ処理	136
グリッドビューでの検索	137
非グリッドビューでの検索	137
検索のクリア	137
グリッドでのソート	138
グリッド内のフィルタ処理	138
グリッド内のフィルタ処理のルール	138
フィルタされたビューのクリア	139
検索式について	139
クエリの基本形式	139
演算子	141
正規表現の使用	143
検索できるトラフィック文字列プロパティ	143
チルダ(~)演算子の使用	143
RegExp構文の使用	143
RegExp構文について	144
正規表現	144
Traffic Viewerプロキシ	146
Traffic Viewerプロキシの使用	146
プロキシモードの開始	146
新しいプロキシファイルの作成	147
プロキシリスナの設定	147
プロキシの設定	147
クライアント証明書の設定	149
プロキシ除外の設定	150
検索および置換の設定	150
テキストの検索と置換	151

ルールでの正規表現の使用	152
ルールの適用	152
ルールの有効化	153
ルールの無効化	153
ルールの削除	153
ルールの編集	153
第14章:Web検出	154
仕組み	154
サイトの検出	155
検出されたサイトの保存	156
設定(Settings)	156
第15章:Webフォームエディタ	158
Webフォーム値の記録	158
Webフォームの値の手動による追加と変更	160
ファイルのインポート	162
ショートカットメニュー	162
Webフォームファイルを使用したスキャン	163
Webフォームリストと入力コントロールのマッチング	164
Webフォーム値のマッチングのルール	164
設定: 全般	166
設定: プロキシ	167
スマート資格情報	169
第16章:Web Fuzzer	170
ファジングとは	170
Web Fuzzerへのアクセス	170
Fuzzerメニューについて	170
ファイル(File)メニュー	170
編集(Edit)メニュー	171
セッション(Session)メニュー	171
フィルタ(Filters)メニュー	172
Web Fuzzerの使用	172
サーバの設定	173

Session Editorの使用	173
セッションの作成	173
セッションの編集	174
セッションの設定	174
メソッド(Method)] タブ	174
パス(Path)] タブ	175
クエリ(Query)] タブ	175
バージョン(Version)] タブ	176
ヘッダ(Headers)] タブ	176
クッキー(Cookies)] タブ	177
POSTデータ(Post Data)] タブ	177
Raw Editorの使用	178
Fuzzerジェネレータについて	179
フィルタの操作	180
フィルタ(Filters)] ダイアログへのアクセス	181
フィルタの作成	181
フィルタの編集	181
フィルタの使用	181
フィルタの削除	181
Fuzzer設定	182
一般設定	182
プロキシ設定	183
プロキシの設定	184
第17章:セッションベースのWeb Macro Recorder	185
マクロについて	185
IEテクノロジー	185
ログインマクロ	185
ワークフローマクロ	186
セッションベースのWeb Macro Recorderへのアクセス	186
ログインマクロ	187
ワークフローマクロ	187
セッションベースのWebマクロレコーダのインタフェースについて	188
ツールバー	189
場所ペイン	189
マクロの記録	192
ログインマクロの記録	192

ワークフローマクロの記録	193
ログアウト条件エディタ	193
ログアウト条件の追加	194
ログアウト条件の削除	194
ブラウザ設定	195
プロキシ設定 (Proxy Settings)] タブ	195
ネットワーク認証 (Network Authentication)] タブ	196
マクロのデバッグ	196
場所 (Locations)] ペインでの場所の詳細と状態の表示	197
ステップ(場所)の再生	197
再生中のステップ(場所)の無効化/有効化	198
ステップ(場所)の削除	198
第18章: イベントベースのWebマクロレコーダ	199
使用可能なバージョン	199
用語「センサ」について	199
マクロについて	199
TruClientテクノロジー	199
Webマクロレコーダの制限	200
マクロ内のCookieヘッダ	200
マクロ内のURL	200
イベントベースのWebマクロレコーダのインストール	200
WindowsでのスタンドアロンWebマクロレコーダのインストール	200
MacでのスタンドアロンWebマクロレコーダのインストール	201
イベントベースのWebマクロレコーダへのアクセス	201
OpenText DASTまたはFortify WebInspect Enterpriseのログインマクロ	201
OpenText DASTまたはFortify WebInspect Enterpriseのワークフローマクロ	202
OpenText ScanCentral DASTのログインマクロ	203
OpenText ScanCentral DASTのワークフローマクロ	203
macOS上のスタンドアロンWebマクロレコーダ	203
ログインマクロ	204
ログアウト条件	204
ワークフローマクロ	205
メインアプリケーションウィンドウの操作 (Macのみ)	205
マクロアイコンについて	206
最近のリストの使用	207

最近のリストオプションの使用	207
Webマクロレコーダウィジェットの使用 (Macのみ)	207
ウィジェットの編集	208
クイックルックの使用 (Macのみ)	208
ユーザインタフェースについて	210
TruClientサイドバーのマストヘッド	210
TruClientサイドバーのツールバー	211
コンテキストメニュー	213
TruClientBrowserメニュー (Macのみ)	215
関数ライブラリタブについて	215
関数ライブラリツールバー	216
ショートカットキーの使用	217
基本機能	217
最近の項目機能 (Macのみ)	218
ログインおよびワークフロー機能 (Macのみ)	218
検索機能	218
ステップ関連機能	219
オブジェクト選択機能	223
ステップボックスの使用	224
ステップの追加	224
ステップをお気に入りとしてマークする	224
お気に入りステップの表示	225
機能タブ	225
[フロー制御] タブ	226
[その他] タブ	227
[複合ステップ] タブ	228
レコードボタンの使用 (Macのみ)	228
ログインマクロの開始	228
ワークフローマクロの開始	228
ログインマクロを使用したワークフローの開始	229
マクロの記録	229
ログインマクロの記録	229
ワークフローマクロの記録	230
クライアント側フレームワークの自動検出	230
検出されたフレームワークの表示	231
マクロの編集	231
マクロの検索	232
ステップの検索	232

特定のステップ番号への移動	233
CLIの使用(Windowsのみ)	233
CLIの起動	233
CLIオプション	233
チャレンジレスポンス方式認証	234
複数のチャレンジ	234
チャレンジのグループ	234
チャレンジレスポンス方式ログイン用のマクロの記録	235
秘密の質問に対する質問と回答の追加	237
追加ステップの記録	238
2要素認証の使用	238
推奨	238
既知の制限事項	239
Gmailアカウントに関する考慮事項	239
ガイドライン	239
2要素認証グループステップの追加	240
2FAを待機するステップの設定	242
入力ステップとクリックステップの追加	242
TOTP認証の使用	244
TOTP認証者の設定	244
TOTPを使用したマクロの記録	246
TOTPのトラブルシューティング	248
QRコードエラーのトラブルシューティング	248
マクロ再生エラーのトラブルシューティング	248
OAuth2でのIMAP多要素認証の使用	249
作業を開始する前に	250
OAuth 2.0を使用したマクロの記録	250
OAuthの関数ライブラリの作成	250
OAuth関数ライブラリへの関数の追加	251
電子メール(IMAP XOAUTH2)の2要素認証ステップの設定	252
2FAを待機するステップの設定	252
ステップの再構成	253
トークンテキストボックスステップのタイプ [値] の設定	253
マクロ再生レベルの変更	253
イベントハンドラの使用	254
イベントハンドラの作成	254
関数ライブラリの使用	256
既知の制限事項	256

関数ライブラリの作成	256
関数の作成	257
引数の編集	258
引数の削除	258
終了イベントについて	258
ログアウト条件の使用	259
ログアウト条件の種類	260
以前のバージョンのWebマクロレコーダからのログアウト条件	260
ログアウト条件エディタへのアクセス	260
セッションベースのログアウト条件の追加	261
イベントベースのログアウト条件の追加	262
ログアウト条件の編集	264
ログアウト条件の削除	264
イベントベースのログアウトテンプレートについて	264
Missing Local Storage Key	264
Missing Session Storage Key	265
Object Exists	266
アクションの使用	267
マクロへのアクションの追加	267
アクションの順序の並び替え	268
アクションの削除	268
Webストレージキーの使用	269
Webストレージキーエディタへのアクセス	269
再生からのキーのロード	269
Webストレージキーの追加	269
Webストレージキーのフィルタリング	270
フィルタのクリア	271
Webストレージキーの編集	271
Webストレージキーの削除	271
パラメータの使用	271
大文字と小文字を区別するパラメータ名	272
ユーザ名とパスワードパラメータの使用	272
ステップでのパラメータの作成	272
パラメータダイアログで値のリストを作成する	273
ポリシー	275
URLパラメータの使用	275
ステップでのパラメータの作成	275
パラメータダイアログで値のリストを作成する	276
ポリシー	277

2要素認証用のパラメータの作成	278
電話番号パラメータの作成	278
電子メールおよび電子メールパスワードパラメータの作成	279
オブジェクトに関連するステップ引数	280
オーディオの役割	281
ブラウザの役割	281
アクティブ化	281
[アクティブ化]タブ	281
[閉じる]タブ	282
[追加]タブ	282
移動	282
戻る	283
進む	283
リサイズ	283
スクロール	283
ダイアログ - 確認	284
ダイアログプロンプト	284
ダイアログ - 認証	284
ダイアログ - パスワードの確認	284
検証	285
チェックボックスの役割	285
日付選択の役割	285
要素の役割	285
マウス操作	286
ドラッグ	286
ドラッグ先	287
プロパティの取得	287
スクロール	288
アップロード	288
検証	288
プロパティの待機	289
ファイルボックスの役割	290
Flashオブジェクトの役割	290
フォーカス可能な役割	290
リストボックスの役割	291
Multi_listboxの役割	291
選択	291
複数選択	292
ラジオグループの役割	292
スライダの役割	292

テキストボックスの役割	293
ビデオの役割	293
オブジェクトに関連しないステップ引数	293
JavaScriptを評価する	294
オブジェクト上でJSを評価する	294
Catchエラー	294
Forループ	295
汎用APIアクション	295
Ifブロック	295
待機	296
マクロの強化	296
ステップの変更	296
ループとループ修飾子の挿入	297
「For」ループの挿入	297
「Break」ステートメントの挿入	297
「Continue」ステートメントの挿入	298
Ifブロック、If-elseブロック、および終了ステップの挿入	298
Ifブロックの挿入	298
Else条件の追加	299
Exitステップの挿入	299
コメントの挿入	299
Catchエラーステップの挿入	300
オブジェクトが存在することの検証	300
汎用ステップの挿入	300
待機ステップの挿入	301
マクロのデバッグ	301
再生エラーの表示	302
マクロの実行手順	302
ブレークポイントの使用	302
ブレークポイントの挿入	302
ブレークポイントの削除	303
ステップレベルの変更	303
ステップの無効化/有効化	304
ステップをオプションにする	304
ステップの再生	304
ステップからマクロの終わりまで再生する	305
オブジェクト識別問題の解決	305
オブジェクトの強調表示	306
オブジェクト識別の改善	306
代替ステップの使用	306

代替ステップの表示と選択	307
オブジェクト識別方法の変更	308
使用可能な方法	308
オブジェクト識別方法の選択	309
マクロタイミングの変更	309
他のオブジェクトへのオブジェクトの関連付け	310
ヒント	310
オブジェクトの置き換え	311
設定の構成	311
TruClient一般設定へのアクセス	311
ブラウザ設定	312
対話型オプション	316
2要素認証	317
2要素認証コントロールセンター	318
モバイルアプリケーション	318
Fortify2FAモバイルアプリのインストールと設定	319
証明書の設定	325
Macにカスタムキーチェーンを追加	326
証明書の設定	326
イベントベースのWebマクロレコーダのアンインストール	326
MacでのWebマクロレコーダのクリーンアップまたはアンインストール	327
[トラブルシューティング]メニューの使用	327
第19章:Web Proxy	328
Web Proxyの使用	328
セッションの保存	330
セッションのクリア	331
メッセージの検索	331
すべてのメッセージの検索	331
オプションの変更	332
Web Proxyのタブ	332
表示(View)	332
分割(Split)	333
情報(Info)	333
ブラウザ	333
Web Proxy対話型モード	333
対話型モードの有効化	334

設定 (Settings)	335
設定: 全般	335
プロキシリスナーの設定	335
記録しない (Do not record)	335
対話型 (Interactive)	336
ログ記録 (Logging)	336
高度なHTTP解析 (Advanced HTTP Parsing)	336
設定: プロキシサーバ	336
プロキシサーバの追加	337
プロキシサーバのインポート	337
プロキシサーバの編集	338
プロキシサーバの削除	338
プロキシサーバのバイパス	338
アドレスの削除	339
設定: 検索と置換	339
テキストの検索と置換	339
ルールの削除	340
ルールの編集	340
ルールの無効化	340
設定: フラグ	340
設定: 回避	340
設定: ネットワーク認証	344
Webマクロの作成	344
Burp ProxyまたはHARファイルの使用	344
選択されたセッションからのWebマクロの作成	345
クライアント証明書 (Client certificates)	346
正規表現	346
正規表現の拡張	347
正規表現タグ	348
正規表現演算子	348
例	349
ブラウザの手動設定	349
第20章: Webサービステスト デザイン	350
手動によるサービスの追加	356
Global Values Editor	357
自動値の使用	358
操作のインポートとエクスポート	359

設計のテスト	359
設定 (Settings)	362
ネットワークプロキシ	362
ネットワーク認証	363
クライアント証明書の使用	363
WSセキュリティ	364
Webサービスの設定	365
[WS-Security] タブ	365
[WS Addressing] タブ	367
WCFサービス(CustomBinding)の設定	367
WCFサービス(フェデレーション)の設定	368
サーバ	368
Security	368
識別情報	368
STS (Security Token Service)の詳細	368
WCFサービス(WSHttpBinding)の設定	369
セキュリティの詳細設定	371
[エンコーディング(Encoding)] タブ	371
高度な標準(Advanced Standards)] タブ	371
[セキュリティ(Security)] タブ	372
[HTTP & プロキシ(HTTP & Proxy)] タブ	373
ドキュメントのフィードバックを送信する	374

序文

カスタマサポートへのお問い合わせ

[カスタマサポート](#) Webサイトにアクセスして、次の作業を実行できます。

- ライセンスとエンタイトルメントの管理
- 技術サポートリクエストの作成と管理
- ドキュメントやナレッジ記事の閲覧
- ソフトウェアのダウンロード
- コミュニティの探索

詳細情報

OpenText Application Security Testing製品の詳細については、「[OpenText Application Security](#)」を参照してください。

製品の機能紹介ビデオ

[YouTube™](#)の[Fortify Unpluggedチャンネル](#)で、OpenText Application Security Softwareの製品と機能を紹介するビデオをご覧ください。

変更ログ

次の表に、このドキュメントに加えられた変更を一覧表示します。このドキュメントの改訂版は、変更が製品の機能に影響を与える場合にのみ、ソフトウェアリリース間で発行されます。

ソフトウェアリリース/ ドキュメントバージョン	変更点
25.4.0	<p>更新:</p> <ul style="list-style-type: none">• ユーザーエージェントリストに含まれている、最新のFirefoxブラウザバージョンのブラウザ設定コンテンツ。「"ブラウザ設定" ページ312」を参照してください。
25.2.0	<p>追加:</p> <ul style="list-style-type: none">• MacバージョンのWebマクロレコーダのメインアプリケーションウィンドウ、ウィジェット、およびクイックルックに関連するコンテンツ。次のピックを参照してください。<ul style="list-style-type: none">• "メインアプリケーションウィンドウの操作 (Macのみ)" ページ205• "Webマクロレコーダウィジェットの使用 (Macのみ)" ページ207• "クイックルックの使用 (Macのみ)" ページ208• OAuth 2.0認証を使用する、TOTPに関連するコンテンツ。「"OAuth2でのIMAP多要素認証の使用" ページ249」を参照してください。 <p>Webマクロレコーダの次のコンテンツを更新しました。</p> <ul style="list-style-type: none">• Mac用の新しいオプションを使用したWebマクロレコーダへのアクセス。「"イベントベースのWebマクロレコーダへのアクセス" ページ201」を参照してください。• Macバージョンに固有のWebマクロレコーダUIの説明。「"ユーザーインタフェースについて" ページ210」を参照してください。• 最近のリスト機能付きのショートカットキー(Macのみ)。「"ショートカットキーの使用" ページ217」を参照してください。• Macバージョンで新しいマクロを起動する手順。「"レコードボタンの使用 (Macのみ)" ページ228」を参照してください。• 新しいトラブルシューティングオプションを使用してMac上のWebマ

ソフトウェアリリース/ ドキュメントバージョン	変更点
	<p>クロレコーダをアンインストールするためのオプション。「"MacでのWebマクロレコーダのクリーンアップまたはアンインストール" ページ327」を参照してください。</p> <p>削除:</p> <ul style="list-style-type: none"> Mac用のWebマクロレコーダのアンインストールツールに関連するコンテンツ。
24.4.0	<p>更新:</p> <ul style="list-style-type: none"> バージョン番号とリリース日。
24.2.0	<p>追加:</p> <ul style="list-style-type: none"> イベントベースのWebマクロレコーダのインストール手順。「"イベントベースのWebマクロレコーダのインストール" ページ200」を参照してください。 MacOS上のイベントベースのWebマクロレコーダへのアクセス手順。「"イベントベースのWebマクロレコーダへのアクセス" ページ201」を参照してください。 イベントベースのWebマクロレコーダのショートカットキーを説明したコンテンツ。「"ショートカットキーの使用" ページ217」を参照してください。 イベントベースのWebマクロレコーダのMacバージョンでレコードボタンと再生ボタンの使用に関するコンテンツ。「Using the Record and Play Buttons (Mac Only)」を参照してください。 イベントベースのWebマクロレコーダでWindowsおよびMacの証明書を設定するためのコンテンツ。「"証明書の設定" ページ325」を参照してください。 イベントベースのWebマクロレコーダのアンインストール手順。「Uninstalling the Event-based Web Macro Recorder」を参照してください。 <p>更新:</p> <ul style="list-style-type: none"> OWASP API Top 10 <年>ポリシーおよび非推奨のAggressiveLog4Shellポリシー関連のコンテンツ。「"ポリシー" ページ85」を参照してください。 正規表現の拡張とその説明、およびリストからの[TEXT]拡張子の

ソフトウェアリリース/ ドキュメントバージョン	変更点
	<p>削除。「"正規表現の拡張と演算子" ページ104」を参照してください。</p> <ul style="list-style-type: none">• MacバージョンのイベントベースのWebマクロレコーダに関するコンテンツ。次のトピックを参照してください。<ul style="list-style-type: none">• "イベントベースのWebマクロレコーダ" ページ199• "ユーザインタフェースについて" ページ210• クリックアンドドラッグオプションでのQRコードの選択に関するイベントベースのWebマクロレコーダのTOTPコンテンツ。「"TOTP認証の使用" ページ244」を参照してください。 <p>削除：</p> <ul style="list-style-type: none">• SWFScanツールのコンテンツ。• イベントベースのWebマクロレコーダのブラウザ設定からのSSL設定とFirefoxプロキシ設定

第1章:OpenText™ Dynamic Application Security Testing (DAST)ツールへようこそ

OpenText DAST (Fortify WebInspect)ツールは、OpenText DASTおよびOpenText™ Fortify WebInspect Enterpriseにパッケージされた診断および侵入テストツールおよび設定ユーティリティの堅牢なセットです。

Fortify WebInspect Enterpriseで提供されるツールは、OpenText DASTで提供されるツールのサブセットです。このガイドでは、OpenText DASTで提供され、Fortify WebInspect Enterpriseでは提供されないツールについて説明する章は、タイトルが「(OpenText DASTのみ)」で終わります。

プロキシでのツールの使用

プロキシを組み込んだツールを使用する場合、クライアント証明書が必要であっても、クライアント証明書を要求しないサーバが発生することがあります。この状況に対応するには、SPI.Net.Proxy.Configファイルを編集する必要があります。

製品名の変更

OpenTextでは、次の製品名を変更中です。

前の名前	新しい名前
Fortify Static Code Analyzer	OpenText™ Static Application Security Testing (OpenText SAST)
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	OpenText™ Dynamic Application Security Testing (OpenText DAST)
Fortify on Demand	OpenText™ Core Application Security
Debricked	OpenText™ Core Software Composition Analysis (OpenText Core SCA)
Fortifyアプリケーションとツール	OpenText™ Application Security Tools

これらの製品名は、製品のスプラッシュページ、マストヘッド、ログインページ、および製品が識別されるその他の場所で変更されました。名前の変更は、製品の機能を明確にし、Fortify Software製品とOpenText製品をより適切に適合させることを目的としています。ドキュメントのタイトルページなど、場合によっては、古い名前が一時的に括弧に含まれる場合があります。今後の製品リリースで、さらに多くの変更を予定しています。

関連ドキュメント

このピックでは、OpenText Application Security Software製品に関する情報を提供するドキュメントについて説明します。

注記: ほとんどのガイドは、PDF形式とHTML形式の両方で提供されています。製品ヘルプは、OpenText DAST製品内で利用できます。

すべての製品

以下のドキュメントには、すべての製品に関する一般情報が記載されています。特に明記されている場合を除き、これらのドキュメントは各製品の製品マニュアルのWebサイトで利用できます。

ドキュメント/ファイル名	説明
<i>OpenText Application Security Software</i> について appsec-docs-n-<version>.pdf	この文書では、OpenText Application Security Software製品のドキュメントにアクセスする方法について説明します。 注記: このドキュメントは、製品のダウンロードにのみ含まれています。
<i>OpenText Application Security Software</i> ソフトウェア<version>の新機能 appsec-wn-<version>.pdf	このドキュメントでは、OpenText Application Security Software製品の新機能について説明します。
<i>OpenText Application Security Software</i> リリースノート appsec-rn-<version>.pdf	このドキュメントでは、OpenText Application Security Softwareのこのリリースで行われた変更の概要と、他の製品ドキュメントには記載されていない重要な情報について説明します。

OpenText ScanCentral DAST

次のドキュメントでは、OpenText ScanCentral DASTの情報について説明します。特に明記されている場合を除き、これらのドキュメントは製品マニュアルのWebサイト (<https://www.microfocus.com/documentation/fortify-ScanCentral-DAST>)で利用できます。

ドキュメント/ファイル名	説明
<i>OpenText™ ScanCentral DAST の設定および使用ガイド</i> sc-dast-ugd-<version>.pdf	このドキュメントでは、OpenText ScanCentral DASTを設定および使用して、Webアプリケーションの動的スキャンを実行する方法について説明します。
<i>OpenText™ Fortify License and Infrastructure Managerインストールおよび使用ガイド</i> lim-ugd-<version>.pdf	このドキュメントでは、Fortify License and Infrastructure Manager (LIM)をインストール、設定、使用する方法について説明します。LIMは、ローカルWindowsサーバにインストールして、Dockerプラットフォーム上のコンテナイメージとして使用できます。
<i>OpenText™ Dynamic Application Security TestingおよびOAST on Dockerユーザガイド</i> dast-docker-ugd-<version>.pdf	このドキュメントでは、Dockerプラットフォーム上のコンテナイメージとして利用可能なOpenText DASTおよびFortify OASTをダウンロード、設定、使用する方法について説明します。OpenText DASTイメージの目的は、コマンドラインインタフェース(CLI)またはアプリケーションプログラミングインタフェース(API)を経由して設定されたヘッドレスセンサとして自動化プロセスで使用する事です。OpenText ScanCentral DASTのセンサとして実行し、Application Securityと組み合わせて使用することもできます。Fortify OASTは、帯域外のアプリケーションセキュリティテスト(OAST)サーバであり、OAST脆弱性の検出のために、DNSサービスを提供します。

OpenText DAST

次のドキュメントでは、OpenText DAST (Fortify WebInspect)の情報について説明します。これらのドキュメントは製品マニュアルのWebサイト (<https://www.microfocus.com/documentation/fortify-webinspect>)で利用できます。

ドキュメント/ファイル名	説明
<i>OpenText™ Dynamic Application</i>	このドキュメントでは、OpenText DASTの概要、イ

ドキュメント/ファイル名	説明
<i>Security Testing</i> インストールガイド dast-igd-<version>.pdf	インストール方法、製品ライセンスの有効化手順について説明します。
<i>OpenText™ Dynamic Application Security Testing</i> ユーザガイド dast-ugd-<version>.pdf	<p>このドキュメントでは、OpenText DASTを設定および使用して、WebアプリケーションやWebサービスをスキャンして分析する方法について説明します。</p> <p>注記: このドキュメントは、OpenText DASTヘルプのPDF版です。このPDFファイルは、ヘルプ情報から簡単に複数のトピックを印刷したり、ヘルプをPDF形式で閲覧したりできるようにするために用意されています。このコンテンツは、もともとWebブラウザで表示するヘルプとして作成されたため、一部のトピックが適切な形式で表示されない可能性があります。また、このPDF版では一部の対話型トピックやリンクされたコンテンツを表示できない場合があります。</p>
<i>OpenText™ Dynamic Application Security Testing</i> およびOAST on Dockerユーザガイド dast-docker-ugd-<version>.pdf	このドキュメントでは、Dockerプラットフォーム上のコンテナイメージとして利用可能なOpenText DASTおよびFortify OASTをダウンロード、設定、使用する方法について説明します。OpenText DASTイメージの目的は、コマンドラインインタフェース(CLI)またはアプリケーションプログラミングインタフェース(API)を経由して設定されたヘッドレスセンサとして自動化プロセスで使用することです。OpenText ScanCentral DASTのセンサとして実行し、Application Securityと組み合わせて使用することもできます。Fortify OASTは、帯域外のアプリケーションセキュリティテスト(OAST)サーバであり、OAST脆弱性の検出のために、DNSサービスを提供します。
<i>OpenText™ Fortify License and Infrastructure Manager</i> インストールおよび使用ガイド lim-ugd-<version>.pdf	このドキュメントでは、Fortify License and Infrastructure Manager (LIM)をインストール、設定、使用する方法について説明します。LIMは、ローカルWindowsサーバにインストールして、Dockerプラットフォーム上のコンテナイメージとして使用できます。
<i>OpenText™ Dynamic Application Security Testing</i> ツールガイド	このドキュメントでは、OpenText DASTおよびFortify WebInspect Enterpriseにパッケージ化された

ドキュメント/ファイル名	説明
dast-tgd-<version>.pdf	OpenText DASTの診断および侵入テストツールと設定ユーティリティの使用方法について説明します。
<i>OpenText™ Dynamic Application Security Testing Agent</i> インストールおよびルールパックガイド dast-agent-igd-<version>.pdf	このドキュメントでは、OpenText DAST Agentのインストール方法と、OpenText DAST Agentルールパックキットの検出機能について説明します。 OpenText DAST AgentルールパックキットはOpenText DAST Agentの上で実行され、実行時にコードを監視してソフトウェアのセキュリティ脆弱性を検出できるようにします。OpenText DAST Agentルールパックキットは、動的な結果を静的な結果に関連付けるのに役立つランタイムテクノロジーを提供します。

Fortify WebInspect Enterprise

次のドキュメントでは、Fortify WebInspect Enterpriseの情報について説明します。特に明記されている場合を除き、これらのドキュメントは製品マニュアルのWebサイト (<https://www.microfocus.com/documentation/fortify-webinspect-enterprise>)で利用できます。

ドキュメント/ファイル名	説明
<i>OpenText™ Fortify WebInspect Enterprise</i> インストールおよび実装ガイド WIE_Install_<version>.pdf	このドキュメントでは、Fortify WebInspect Enterpriseの概要、Fortify WebInspect Enterpriseのインストール手順、Application SecurityやOpenText DASTとの統合、およびインストールのトラブルシューティングについて説明します。また、Fortify WebInspect Enterpriseシステムのコンポーネントの設定方法についても説明します。これには、Fortify WebInspect Enterpriseのアプリケーション、データベース、センサ、およびユーザが含まれています。
<i>OpenText™ Fortify WebInspect Enterprise</i> ユーザガイド WIE_Guide_<version>.pdf	このドキュメントでは、Fortify WebInspect Enterpriseを使用してOpenText DASTセンサの分散ネットワークを管理し、WebアプリケーションとWebサービスをスキャンして分析する方法について説明します。 注記: このドキュメントは、Fortify WebInspect EnterpriseヘルプのPDF版です。このPDFファイル

ドキュメント/ファイル名	説明
	は、ヘルプ情報から簡単に複数のトピックを印刷したり、ヘルプをPDF形式で閲覧したりできるようにするために用意されています。このコンテンツは、もともとWebブラウザで表示するヘルプとして作成されたため、一部のトピックが適切な形式で表示されない可能性があります。また、このPDF版では一部の対話型トピックやリンクされたコンテンツを表示できない場合があります。
<i>OpenText™ Dynamic Application Security Testing</i> ツールガイド dast-tgd-<version>.pdf	このドキュメントでは、OpenText DASTおよびFortify WebInspect Enterpriseにパッケージ化されたOpenText DASTの診断および侵入テストツールと設定ユーティリティの使用方法について説明します。

第2章:監査入力エディタ

このツールを使用すると、監査エンジンおよび個別のチェックセットへの入力を作成または編集できます。

Audit Inputs Editorにアクセスするには、次の2つの方法があります。

- Policy Manager (Policy Managerの **ツール(Tools)**]メニューを使用)。この方法を使用し、入力ファイル(<filename>.inputs)を作成または変更します。こうすると、スキャン設定を変更するときにこのファイルを指定できます。
入力ファイルを変更するには、Audit Inputs Editorのツールバーの **開く(Open)**] アイコンをクリックするか、**ファイル(File)] > 開く(Open)]**の順に選択します。
- デフォルトまたは現在の設定からは、攻撃の除外設定の **Audit Inputs Editor]** ボタンをクリックします。この方法を使用すると、デフォルトの設定ファイルを直接変更できますが、個別の入力ファイルを作成することはできません。

デフォルト設定または現在の設定からAudit Inputs Editorにアクセスする場合は、作成または変更したチェック入力が設定ファイルの一部になります。

ただし、Policy ManagerからAudit Inputs Editorにアクセスする場合は、次のように、チェック入力変更を含む保存されたファイルを、OpenText DASTにインポートする必要があります。

1. OpenText DASTのメニューバーで、**編集(Edit)] > デフォルト設定(Default Settings)]**の順にクリックします。
2. **監査設定(Audit Settings)]** で **攻撃の除外(Attack Exclusions)]**を選択します。
3. **監査入力のインポート(Import Audit Inputs)]**をクリックします。
4. 作成したファイル(*.inputs)を選択し、**開く(Open)]**をクリックします。

現在の設定(Current Settings)] ウィンドウまたは **デフォルト設定(Default Settings)]** ウィンドウの **攻撃の除外(Attack Exclusions)]** パネルからアクセスすると、Audit Inputs Editorにメニューバーやツールバーが表示されません。

チェック入力

特定のチェックでは、ターゲットWebサイトの特定の設計に対応する入力が必要です。OpenText DASTはこれらのチェックをデフォルト値を使用して行うため、ユーザによる変更は不要です。

特定のチェック用に入力を作成または変更するには:

1. **チェック入力(Check Inputs)]** タブをクリックします。
2. リストからチェックを選択します。
選択したチェックの入力が右側に表示されます。
3. 要求された入力値を入力します。

4. 次のいずれかを実行します。

- デフォルト設定または現在の設定からAudit Inputs Editorを起動した場合は、**OK**]をクリックします。
- Policy ManagerからAudit Inputs Editorを起動した場合は、**ファイル(File)] > 保存(Save)]**または **ファイル(File)] > 名前を付けて保存(Save As)]**の順にクリックします。

参照情報

["エンジン入力" 下](#)

エンジン入力

監査エンジンへの入力を作成または変更するには:

1. **エンジン入力(Engine Inputs)]** タブをクリックします。
2. ドロップダウン矢印をクリックします。
 - a. すべての監査エンジンに変更を適用するには、**デフォルト(Default)]**を選択します。デフォルトパラメータが、デフォルトの「OpenText DAST監査設定-攻撃の除外」から抽出されます。
 - b. 特定の監査エンジンの入力を変更するには、リストからいずれか1つを選択します。
3. エンジン入力を選択します。
4. 次のいずれかを選択した場合:
 - 除外されたクエリパラメータ(Excluded Query Parameters)
 - 除外されたポストパラメータ(Excluded Post Parameters)
 - 除外クッキー(Excluded Cookies)
 - 除外ヘッダ(Excluded Headers)
 - ルートディレクトリ(Root Directories)

次の操作を実行します。

- 項目をリストに追加するには、**追加(Add)]**をクリックします。
- 項目を編集するには、項目を選択して **編集(Edit)]**をクリックします。
- 項目を削除するには、項目を選択して **削除(Remove)]**をクリックします。
- (デフォルトではなく)特定のエンジンを選択した場合は、次のいずれかのオプションを選択します。
 - **デフォルトとマージ(Merge with defaults)** -指定したパラメータがデフォルトリストに追加され、すべてのエンジンに適用されます。
 - **デフォルトを置き換える(Replace defaults)** -エンジンは、デフォルトリストで指定したパラメータの代わりに、指定したパラメータを使用します。

注記: ルートディレクトリを指定すると、エンジンは実際のルートではなく、指定したディレクトリ内のオブジェクトを攻撃します。たとえば、エンジンが通常、デフォルトのルートディレクトリ `rootdir (/rootdir/filename.txt)` の `filename.txt` を攻撃する場合、`/foobar/` のルートディレクトリを指定すると、エンジンは `/foobar/filename.txt` を攻撃します。

5. 次のいずれかを選択した場合:

- ヘッダ監査ルール(Header Audit Rules)
- クッキー監査ルール(Cookie Audit Rules)

次の操作を実行します。

- a. **デフォルトの値を使用(Use value from defaults)]** チェックボックスをオフにします。
- b. ドロップダウンリストからオプションを選択します。オプションは次のとおりです。

ヘッダ監査ルール(Header Audit Rules)

- **毎回すべてを攻撃(Attack All Every Time)** -リクエストごとにヘッダを攻撃します。
- **ディレクトリごとに1回攻撃(Attack Once Per Directory)** -各ディレクトリの各名前付きヘッダを最初に検出された場合にのみ攻撃します。
- **1回だけ攻撃(Attack Only Once)** -スキャン中に初めて検出されたホストごとにヘッダを1回だけ攻撃します。

クッキー監査ルール(Cookie Audit Rules)

- **すべて攻撃(Attack All)** -スキャン中にすべての要求で発生したクッキーを攻撃します。
- **親で設定された子セットのクッキーのみ攻撃(Attack Only Cookies In Children Set In Parent)** -継承されたクッキーを、それが見つかったすべての子セッションで攻撃します。

たとえば、親セッション要求がJSESSION IDで次のクッキーを設定するとします。

```
GET /auth/link.page; HTTP/1.1
Referer: http://zero.webappsecurity.com/auth/security-check.html
...
Cookie:
CustomCookie=WebInspect83644ZX632F0EE21C7249358BE159C67CEE9085YCE51;
JSESSIONID=2DC913EA;username=username;password=password
```

かつ、子セッションには、継承されたクッキーが含まれるとします。

```
GET /auth/link.page HTTP/1.1
Referer: http://zero.webappsecurity.com/auth/link.page;
...
Cookie:
CustomCookie=WebInspect83644ZX632F0EE21C7249358BE159C67CEE9085YCE5
```



```
1;  
JSESSIONID=2DC913EA;username=username;password=password
```

この場合、クッキーは子セッションで攻撃されます。

1つの子セッションに複数のクッキーがある場合でも、親セッションで設定されたクッキーだけが攻撃されます。

- **各クッキーを1回だけ攻撃 (Attack Each Cookie Once)** - スキャン中に最初に検出されたホストごとに一度だけ固有のクッキーを攻撃します。
6. デフォルトまたは現在の設定からAudit Inputs Editorを起動した場合は **OK**]をクリックします。また、Policy ManagerからAudit Inputs Editorを起動した場合は **ファイル(File)] > 保存(Save)]** または **ファイル(File)] > 名前を付けて保存(Save As)]** の順にクリックします。

参照情報

["チェック入力" ページ30](#)

第3章:Compliance Manager(OpenText DASTのみ)

OpenText DASTは、Webベースのアプリケーションのセキュリティ上の欠陥を検出するために設計された膨大な数の攻撃エージェントを使用します。Fortify WebInspectは何千ものHTTP要求によってシステムをプローブし、個々の応答を評価します。このセッションベースの評価では、それぞれの脆弱性が報告され、アプリケーション内のその脆弱性がある箇所が特定され、実行すべき修正処置が推奨されます。これは基本的には、システムの定量分析です。

OpenText DASTは、特定の政令による規制や企業が定めたガイドラインにアプリケーションがどの程度準拠しているかを評価して、定量分析を行うこともできます。たとえば、医療保険の携行性と責任に関する法律(HIPAA: Health Insurance Portability and Accountability Act)は、Webベースのアプリケーションを使用するヘルスケア提供機関に、「パスワードを作成、変更、および保護するための手順」の策定を義務付けています。OpenText DASTでは、アプリケーションを評価して、アプリケーションがこのHIPAA規則にどの程度準拠しているかを評価するコンプライアンスレポートを生成することができます。

仕組み

ユーザは要件を1つ以上の攻撃エージェントまたは脆弱性に関連付けるコンプライアンステンプレートを作成します。たとえば、「アプリケーションは「非表示の」フィールドを使用しません」などのステートメント(または質問)を含めることができます。この要件に対するコンプライアンスをテストする攻撃エージェントは、ID番号4727の「非表示フォーム値(Hidden Form Value)」([一般的なテキスト検索グループ](#) ページ40)に含まれるエージェントの1つです。

コンプライアンステンプレートは非常に柔軟です。要件を個別に有効または無効にすることができます。攻撃エージェントまたは[脅威クラス](#) ページ40を追加したり削除したりして、要件を変更することもできます。柔軟性を最大限に高めるために、独自のエージェントを作成して、ユーザが定義した要件に関連付けることもできます。

OpenText DASTには、会社の特定の要件に合わせて編集できるサンプルのコンプライアンステンプレートが含まれています。

ポリシーの作成の詳しい手順については、「["コンプライアンステンプレートの作成" 次のページ](#)」を参照してください。

Webサイトのコンプライアンスをテストするには:

1. 必要に応じて、コンプライアンステンプレートを作成または変更します。
2. Webサイトをスキャンします。
3. OpenText DASTの **開始(Start)** ページで、**レポートの生成(Generate a Report)** をクリックします。

レポートの生成(Generate a Report) ウィンドウが開きます。

4. スキャンデータが別のデータベースに格納されている場合は、**DBの変更(Change DB)**をクリックしてデータベースを選択します。
5. スキャンを選択します(名前、URL、またはIPアドレスで指定)。
6. **次へ(Next)**をクリックします。
7. **コンプライアンス(Compliance)**を選択します。
8. すべてのレポートを1つのタブにまとめるのではなく、個々のレポートを個別のタブに生成する場合は、**個別のタブでレポートを開く(Open Reports in Separate Tabs)**を選択します。
9. レポート形式として、**Adobe PDF**と**HTML**のいずれかを選択します。
ポータブルデータ形式(PDF)でのレポートの読み込みには、Adobe Reader 7以降が必要です。
10. コンプライアンステンプレートを指定します。リストからデフォルトのテンプレートを選択するか、参照ボタンをクリックして作成済みのテンプレートを参照するか、Compliance Managerを開いてカスタムテンプレートを作成することができます。
11. **完了(Finished)**をクリックします。
12. OpenText DASTがレポートを生成してタブに表示したら、ツールバーの **レポートの保存(Save Report)** アイコンをクリックしてそのレポートを保存できます。

参照情報

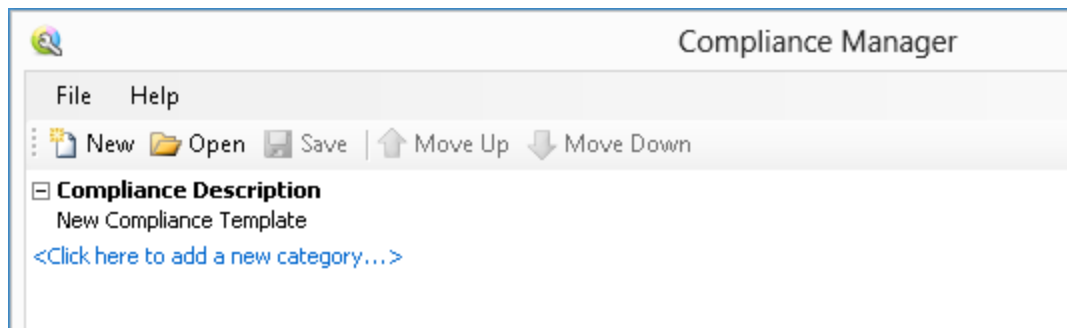
["コンプライアンステンプレートの作成" 下](#)

コンプライアンステンプレートの作成

コンプライアンステンプレートを作成するには:

1. OpenText DASTのメニューバーで、**ツール(Tools)] > [Compliance Manager]**の順にクリックします。

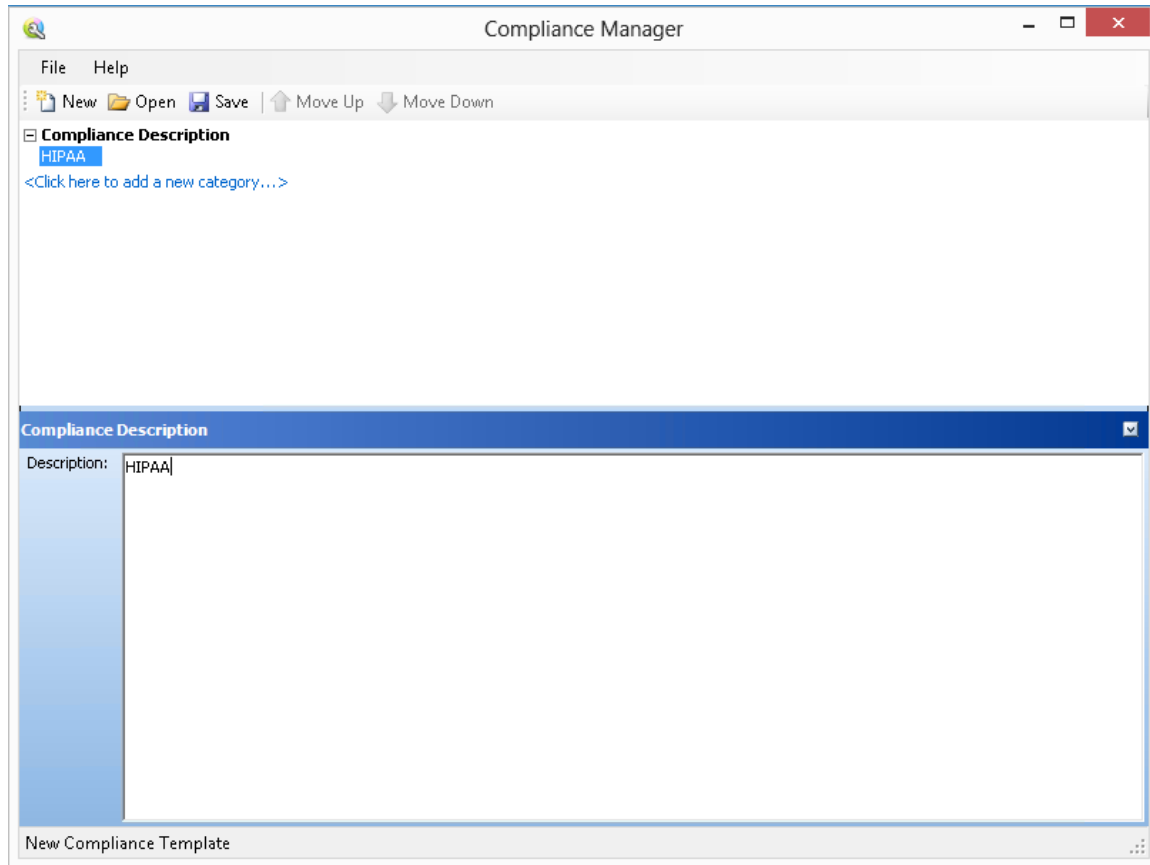
[Compliance Manager] ウィンドウが開き、新しいテンプレートの概略が表示されます。



2. 「新しいコンプライアンステンプレート(New Compliance Template)」というフレーズをクリックします。

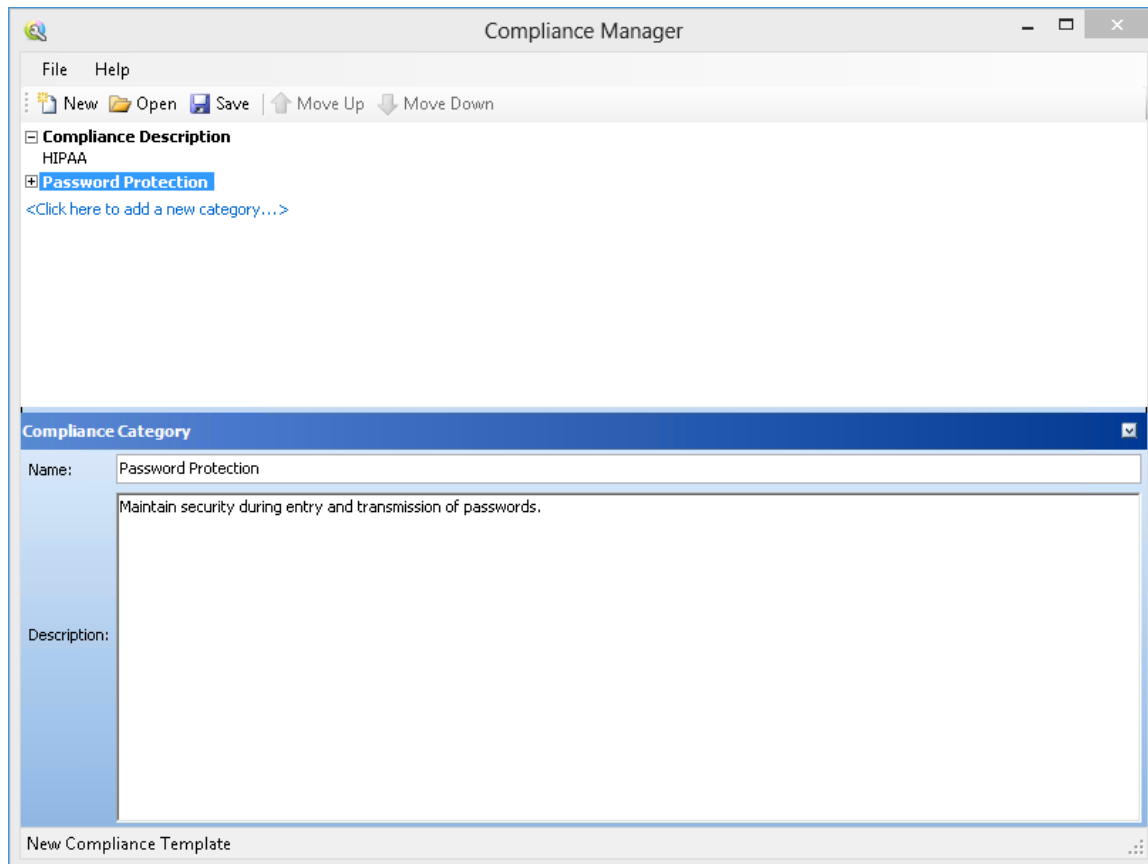
Compliance Managerのウィンドウの下半分に編集エリアが表示されます。

3. 編集エリアで、「新しいコンプライアンス テンプレート (New Compliance Template)」というフレーズを、作成するテンプレートの説明(この例では「HIPAA」)に置き換えます。



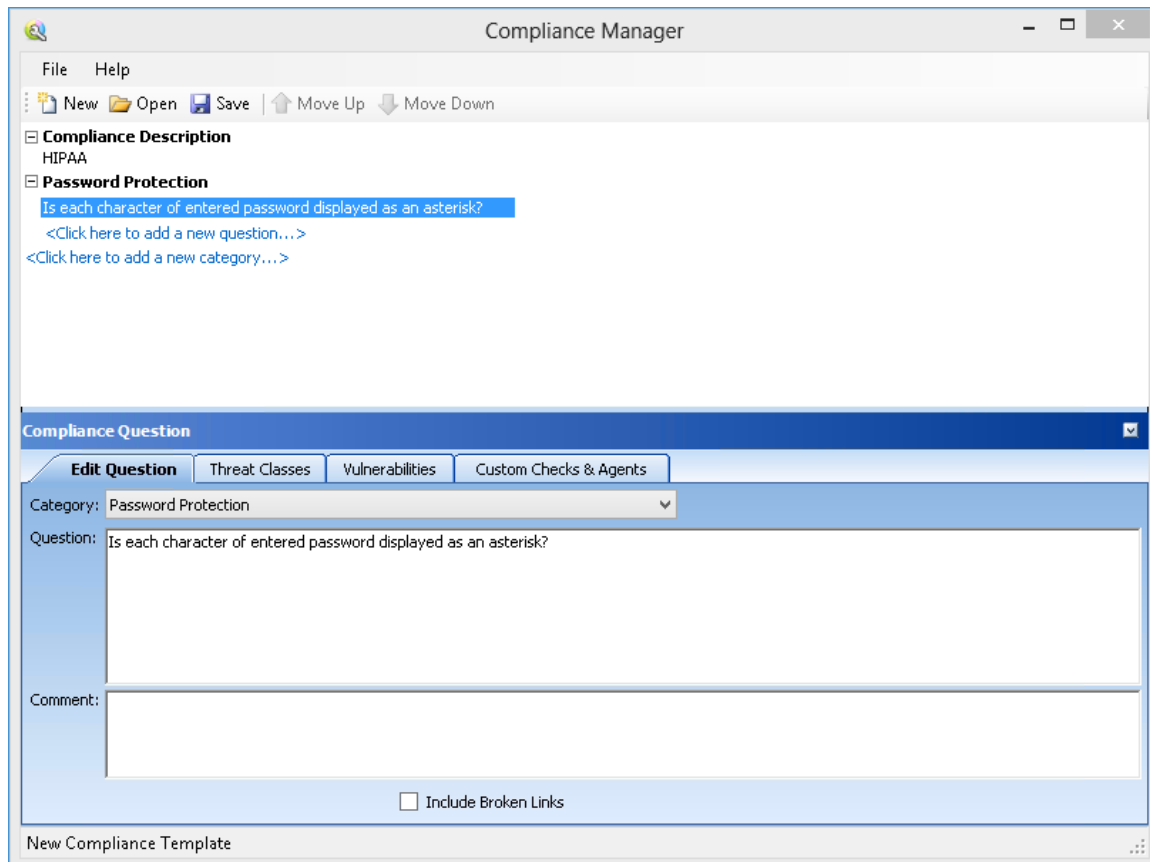
4. 「<新しいカテゴリを追加するにはここをクリック...>(<Click here to add a new category...>)」というフレーズをクリックします。

5. 編集エリアで、新しいカテゴリの名前と説明を入力します。この例では、名前は「パスワード保護>Password Protection)」で、説明は「パスワードの入力と送信のときにセキュリティを維持する(Maintain security during entry and transmission of passwords)」です。



6. プラス記号 (+) をクリックして、「パスワード保護>Password Protection)」というラベルの付いたノードを展開します。
7. 「<新しい質問を追加するにはここをクリック...>(<Click here to add a new question...>)」というフレーズをクリックします。
8. 「新しい質問(New Question)」というフレーズをクリックします。
編集エリアにタブが表示されるので、それらのタブを使用して「パスワード保護」カテゴリに関連する質問を作成することができます。

9. **質問(Question)]** エリアに、カテゴリに関連する質問を入力します。この例では、「入力されたパスワードの各文字はアスタリスクとして表示されているか?(Is each character of entered password displayed as an asterisk?)」という質問を入力しています。



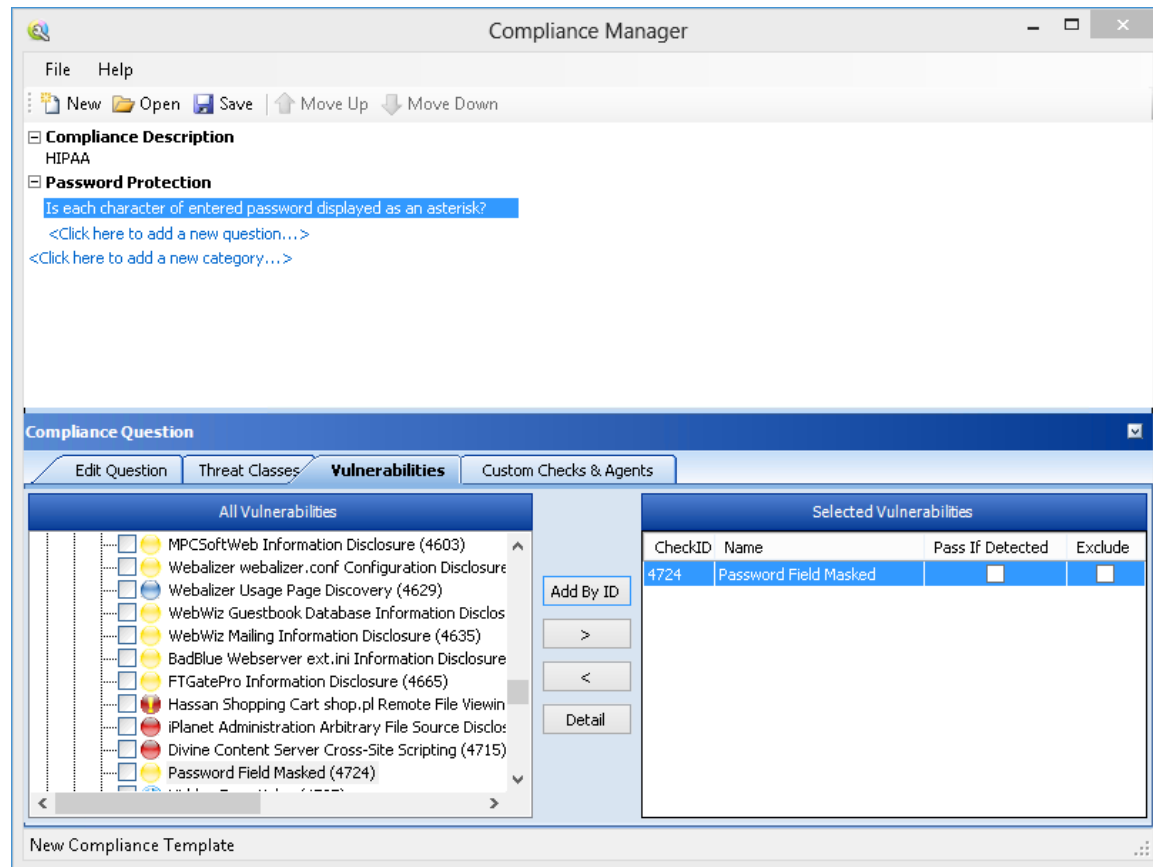
10. この質問を、**脅威クラス**、OpenTextが定義した脆弱性、または以前に作成したカスタムチェックやエージェントに関連付けることができます。この例では、**脆弱性(Vulnerabilities)]** タブをクリックしてから、**[IDで追加(Add By ID)]** をクリックします。

注記: 脆弱性または脅威クラスを選択してから  をクリックすることによって、その脆弱性または脅威クラスをこの質問の **選択した脆弱性(Selected Vulnerabilities)]** または **選択した脅威クラス(Selected Threat Classes)]** のセクションに含めることもできます。

11. **[IDによるチェックの追加(Add Check By ID)]** ウィンドウで、「4724」と入力して **[OK]** をクリックします。4724は「マスクされたパスワードフィールド>Password Field Masked)」というチェックのID番号です。

注記: 複数のIDを追加できます(1行に1つずつ追加します)。

指定したチェックが **選択した脆弱性(Selected Vulnerabilities)** エリアに表示されます。



12. **選択した脆弱性(Selected Vulnerabilities)** エリアには、次の2つのチェックボックスがあります。

- **検出された場合は合格(Pass If Detected)** - チェックが、アプリケーションセキュリティに寄与する属性を確認することを目的としたものである場合は、このオプションを選択します。たとえば、コンプライアンスプログラムの一部であるファイル(Privacy Policy.html など)の存在をチェックするカスタムチェックを開発する場合には、このオプションを使用できます。
- **除外(Exclude)** - チェックのグループを追加しているとき、そのうちの特定のチェックを除外する場合は、このオプションを選択します。

この例では、どちらのチェックボックスも選択しません。

13. コンプライアンスレポートに壊れたリンクのリストを表示するには、**壊れたリンクを含める(Include Broken Links)** チェックボックスをオンにします。

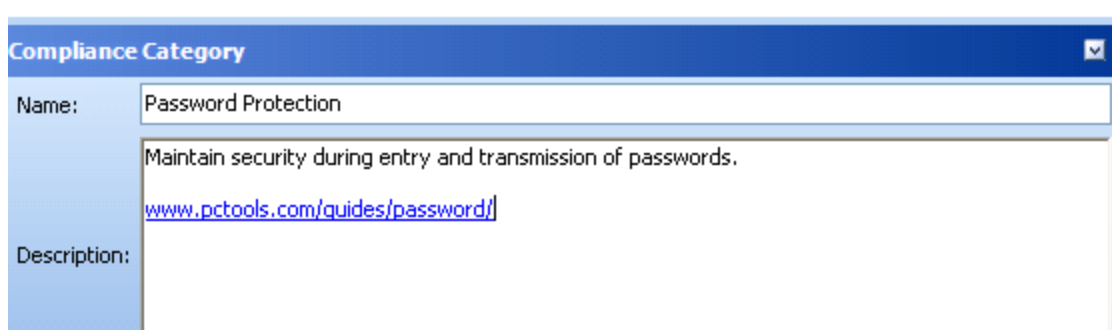
このチェックボックスをオンにしている場合、コンプライアンスレポートを実行すると、見つかった壊れたリンクがレポートの最後の一覧表示されます。壊れたリンクがテンプレート内の質問に関連付けられている場合、その質問は失敗としてマークされます。

14. 脅威クラス、脆弱性、またはカスタムチェックの追加を続行して、コンプライアンスの質問についてアプリケーションを十分に検査するためのすべてのチェックを追加します。

15. 追加の質問とカテゴリを上記の手順で作成して、コンプライアンステンプレートを完成させます。
16. **Save**をクリックします。

使用上のメモ

- カテゴリまたは項目を並べ替えるには、項目を選択して **上へ移動** または **下へ移動** をクリックします。
- カテゴリまたは項目を挿入する場合は、カテゴリまたは質問を右クリックして、ショートカットメニューから **挿入** を選択します。項目が、選択した項目の上に挿入されます。
- 次の画像のように、説明または質問にHTMLリンクを追加できます。



The screenshot shows a 'Compliance Category' dialog box. It has a 'Name' field with the text 'Password Protection' and a 'Description' field with the text 'Maintain security during entry and transmission of passwords.' and a blue hyperlink 'www.pctools.com/guides/password/'. There is a small 'X' icon in the top right corner of the dialog box.

一般的なテキスト検索グループ


主にディレクトリ列挙(Directory Enumeration)エンジンによって使用されるこのエージェントグループは、サイトにあるすべての既知および未知のパスをたどります。個々のチェックは、A (Accountingという名前のディレクトリの検索で始まる)からZ (Zipsという名前のディレクトリの検索で終わる)までのアルファベット順にグループ化されます。このグループには、Microsoft FrontPageやMicrosoft Internet Information Serverのログファイル(W3SVCnn)に関連付けられているディレクトリなどのよくある他のタイプのディレクトリのチェックも含まれています。

使用可能なすべてのエージェントの詳細については、Policy Managerを標準ビューで開始し、**一般的なテキスト検索 (General Text Searching)** ノードを展開して、任意のエージェントをクリックしてください。

脅威クラス

Web Application Security Consortiumは、Webサイトのセキュリティに対する脅威を明確化して整理するための、業界標準の用語を作成しています。それらは **脅威クラス(Threat Classes)** タブにリストされています。

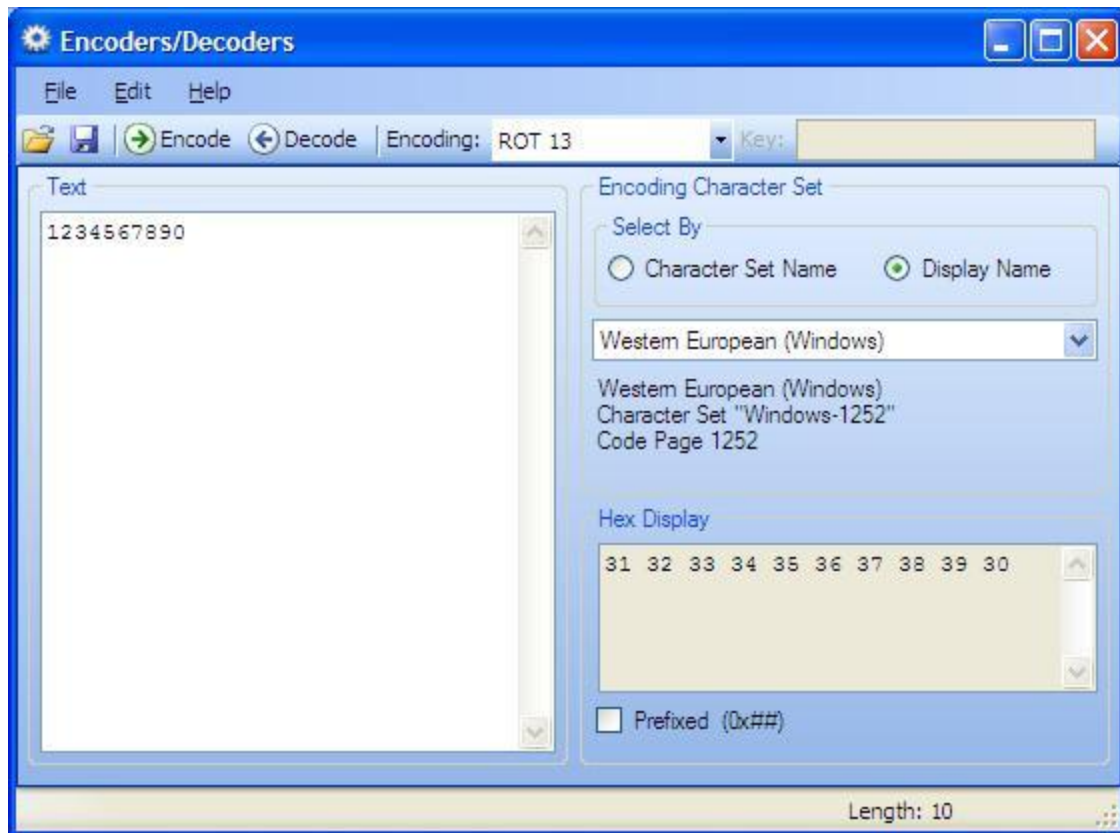
それらの脅威に対する脆弱性がスキャンにより判明したかどうかを判定するには:

1. 脅威クラス(またはそのコンポーネントのいずれか)を選択します。
2. をクリックして、それをこの質問の **選択された脅威クラス(Selected Threat Classes)**に含めます。

第4章:エンコーダ/デコーダ

このツールにより、Base 64、16進数、MD5などのスキームを使用して、値をエンコードおよびデコードできます。文字列をUnicode文字列にエンコードすることや、URLの構築で特殊文字を使用することもできます。

スキャン結果の分析中に、エンコードまたは暗号化された形式と思われる文字列が検出された場合は、文字列をコピーして、Encoders/Decodersツールに貼り付け、**デコード (Decode)]**をクリックするだけです。



文字列のエンコーディング

文字列をエンコードするには:

1. **テキスト (Text)]** エリアに文字列を入力する(または貼り付ける)か、メニューから **ファイル (File)] > 開く (Open)]** を選択してファイルの内容を読み込みます。
2. **文字セット名 (Character Set Name)]** または **表示名 (Display Name)]** のいずれかを使用してエンコーディング文字セットを選択します。

3. **エンコーディング(Encoding)** リストから暗号の種類を選択します。詳細については、「[エンコーディングタイプ](#)」次のページ」を参照してください。
4. 必要に応じて、**キー(Key)** フィールドにキーを入力します。有効なキーを入力すると、**エンコード(Encode)** ボタンと **デコード(Decode)** ボタンが有効になります。
5. **エンコード(Encode)** をクリックします。
テキスト(Text) エリアには、エンコードされた文字列が表示されます。**16進表示(Hex Display)** エリアには、エンコードされた文字列内の各文字の16進値が(選択した文字セットでフォーマットされて)表示されます。
プレフィックス付き(Prefixed) を選択すると、16進数の先頭に「0x」が追加されます。C および類似した構文の言語(C++、C#、Java、JavaScriptなど)では、16進数の先頭に「0x」を付けます(たとえば0x5A3)。先頭の0Iによってパーサは数値であることを認識します。「x」は16進値を表します。

文字列のデコード

文字列をデコードするには:

1. **テキスト(Text)** エリアに文字列を入力する(または貼り付ける)か、メニューから **ファイル(File)] > 開く(Open)]** を選択してファイルの内容を読み込みます。
2. **エンコーディング(Encoding)** リストから暗号の種類を選択します。
3. 必要に応じて、**キー(Key)** フィールドにキーを入力します。
4. **デコード(Decode)** をクリックします。

HTTP Editorで、OpenText DASTのエンコーディングおよびデコーディング機能を使用することもできます。セッションの編集集中に右クリックすると、エンコーディングとデコーディングのオプションにアクセスできます。

エンコードされた文字列の操作

エンコードされた形式の文字列には、印刷不可能な文字が含まれている場合があります。ハッシュベースのエンコーディングスキームまたはキーを必要とするエンコーディングスキームを使用する場合に、これが頻繁に発生します。印刷不可能な文字はWindowsクリップボードにコピーできないので、単純にEncoder/Decoderからコピーしたり、それに貼り付けたりすることはできません。ただし、この制限を回避するための2つの方法があります。

- エンコードされた文字列をファイルに保存しておき、それをデコードするときには、メニューから **ファイル(File)] > 開く(Open)]** を選択して、Encoderツールにロードします。その後、元の方法と(該当する場合)はキーを使用してデコードします。
- また、選択したエンコーディング方式とキーを使用して文字列をエンコードした後、結果の文字列をBase 64方式を使用してエンコードすることもできます。その後、その文字列をクリップボードにコピーし、クリップボードの内容を貼り付け、Base 64を使用してデコードしてから、元の方法と(該当する場合)はキーを使用して再びデコードします。

エンコーディングタイプ

Encoder/Decoderでは、次の表に記載されたエンコーディングタイプを選択できます。

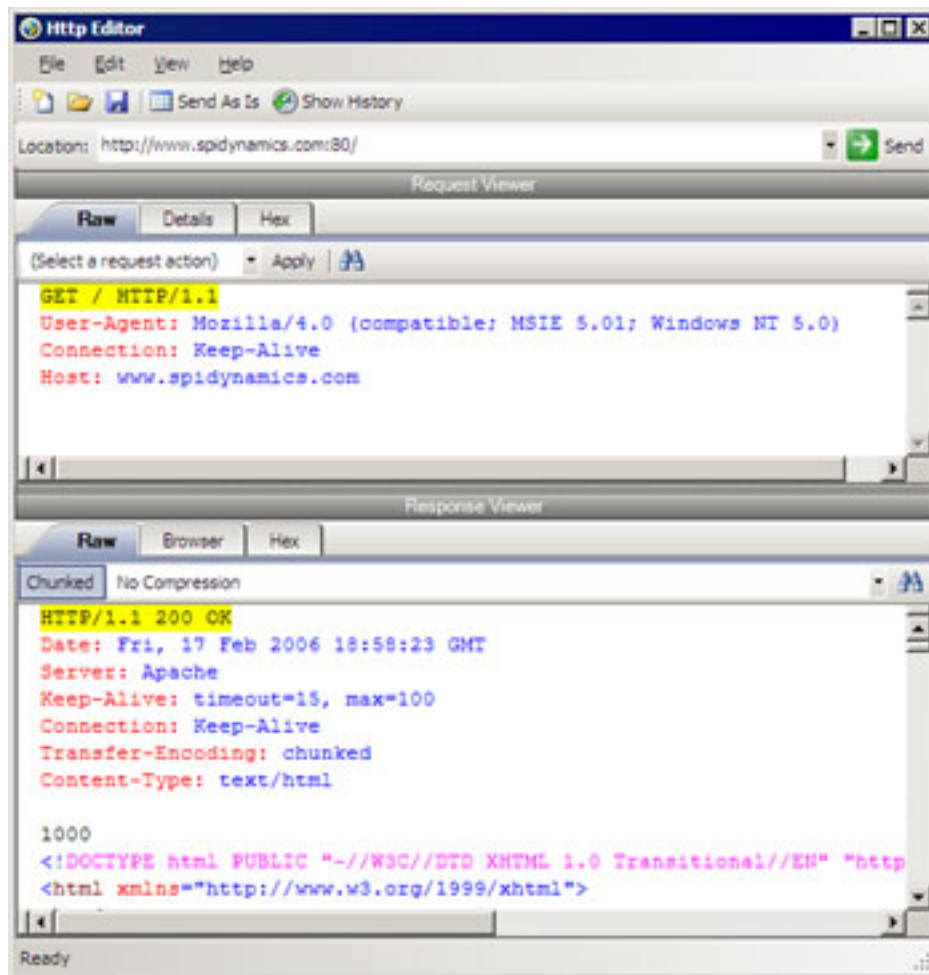
エンコーディングタイプ	定義
3DES	Triple DES。データを3回暗号化するDES暗号化アルゴリズムのモード(文字列が暗号化され、その暗号が暗号化され、その結果の暗号テキストに3回目の暗号化が行われます)。キーは128ビットまたは192ビット(16文字または24文字)でなければなりません。
Base64	8ビットオクテットの3つ組を、4文字のグループとしてエンコードおよびデコードします。各文字は、ソースである24ビットの中の6ビットを表します。ASCIIおよびEBCDICのすべてのバリエーションに含まれる文字だけを使用することにより、他のエンコーディング形式にある非互換性を回避しています。
Blowfish	DESアルゴリズムの代わりとして使用できる暗号化アルゴリズム。
DES	データ暗号化標準。7京2000兆を超える異なるプライベートの(かつ秘密の)暗号化キーを使用できる、広く使用されているデータ暗号化方式。送信元とユーザの両方が同じ秘密鍵を使用する必要があります。
Hex	16進数。
MD5	何であれ入力したデータに対して、128ビットの「指紋」または「メッセージダイジェスト」を生成します。
RC2	Ronald Rivestが設計した可変鍵サイズのブロック暗号。ブロックサイズは64ビットで、ソフトウェアではDESより約2倍から3倍高速です。
RC4	Ronald Rivestが設計したストリーム暗号。これは、バイト指向の操作を行う、可変鍵サイズのストリーム暗号です。RSA SecurPCなどの製品のファイル暗号化に使用されることに加え、SSLプロトコルを使用した安全なWebサイトとの間のトラフィックの暗号化のように、安全な通信にも使用されます。
ROT13	各文字をアルファベットで13文字後にある文字に置き換えて、テキストを暗号化するために使用される単純なCaesar暗号。
SHA1	セキュアハッシュアルゴリズム。NISTによって開発され、標準FIPS 180で定義されている、一方向ハッシュ関数。SHA-1は1994年に発行された改訂版で、ANSI標準X9.30(パート2)にも記載されています。

エンコーディングタイプ	定義
SHA256	256ビット暗号化を使用するセキュアハッシュアルゴリズム。
SHA384	384ビット暗号化を使用するセキュアハッシュアルゴリズム。
SHA512	512ビット暗号化を使用するセキュアハッシュアルゴリズム。
ToLower	大文字を小文字に変更します。
ToUpper	小文字を大文字に変更します。
TwoFish	以前のBlowfishに基づく暗号化アルゴリズム。
Unicode	プラットフォーム、プログラム、および言語に関係なく、各文字に対して固有の数値を指定します。
URL	非標準の文字と記号のURLエンコーディングに使用できる値を作成し、それをサポートするブラウザやプラグインで表示できるようにします。
XHTML	入力されたデータをテキストタグで、<text>データ</text>のようにカプセル化します。
XOR	XORは排他的OR操作を実行します。キーを指定する必要があります。キー文字列の長さが1文字だけの場合、その文字は、エンコード/デコード文字列内の各文字に対してOR処理されます。

第5章:HTTPエディタ

HTTP Editorは、要求を作成または編集してサーバに送信し、応答を生のHTMLで表示したり、ブラウザにレンダリングして表示したりするために使用します。HTTP Editorは手動のハッキングツールであるため、使用にはHTML、HTTP、および要求メソッドの実務知識が必要です。

プロキシパラメータおよび認証パラメータを設定するには、必要に応じて **編集(Edit)] > 設定(Settings)]** を選択します。



要求ビューア(Request Viewer)

要求ビューア(Request Viewer)]にはHTTP要求メッセージが表示されます。このメッセージは、次のタブを使用して4つの異なる形式で表示できます。

- **生(Raw)** -要求メッセージをテキスト形式で1行ずつ表示します。
- **詳細(Details)** -ヘッダ名とフィールド値をテーブル形式で表示します。
- **16進数(Hex)** -メッセージを16進数とASCIIの表記で表示します。
- **XML** -メッセージ本文のXMLコンテンツを表示します。(このタブは、要求にXML形式のデータが含まれている場合にのみ表示されます)。

応答ビューア(Response Viewer)

応答ビューア(Response Viewer)]にはHTTP応答メッセージが表示されます。このメッセージは、次のタブを使用して4つの異なる形式で表示できます。

- **生(Raw)** -応答メッセージをテキスト形式で1行ずつ表示します。
- **ブラウザ** -応答メッセージをブラウザにレンダリングして表示します。
- **16進数(Hex)** -応答メッセージを16進数とASCIIの表記で表示します。
- **XML** -メッセージ本文のXMLコンテンツを表示します。(このタブは、応答にXML形式のデータが含まれている場合にのみ表示されます)。

HTTP Editorのメニュー

ファイル(File)]メニュー

ファイル(File)]メニューには、次のオプションがあります。

- **新規要求(New Request)** -以前のセッションからのすべての情報を削除し、ロケーションURLをリセットします。
- **要求を開く(Open Request)** -以前のセッション中に保存されたHTTP要求を含んだファイルをロードできます。
- **要求の保存(Save Request)** - HTTP要求を保存できます。
- **名前を付けて要求を保存(Save Request As)** - HTTP要求を保存できます。
- **URL同期(URL Synchronization)** -これを選択すると、**アドレス**]コンボボックスに入力した文字が、HTTP要求行のRequest-URIに追加されます。
- **そのまま送信(Send As Is)** -このオプションを選択した場合、選択したその他の設定に関係なく、HTTP Editorは要求を変更しません。このオプションを使用すると、意図的に誤った形式にしたメッセージを送信することができます。このオプションを使用すると、認証およびプロキシの設定は無効になります。

注記: プロキシを経由するように要求を手動で編集することはできますが、多くの標準HTTPプロキシサーバは非標準のHTTP要求を処理できません。

- **終了(Exit)** - HTTP Editorを閉じます。

編集(Edit)]メニュー

編集(Edit)]メニューには、次のオプションがあります。

- **切り取り(Cut)** - 選択したテキストを削除し、クリップボードに保存します。
- **コピー(Copy)** - 選択したテキストをクリップボードに保存します。
- **貼り付け(Paste)** - クリップボードからテキストを挿入します。
- **検索(Find)** - 指定したテキストを検索するためのダイアログボックスを表示します。
- **設定(Settings)** - HTTP Editorの要求パラメータ、認証パラメータ、およびプロキシパラメータを設定できます。

表示(View)]メニュー

表示(View)]メニューには、次のオプションがあります。

- **履歴の表示(Show History)** - 送信したHTTP要求を一覧にしたペインを表示します。
- **折り返し(Word Wrap)** - すべてのテキストを規定の余白内に収めます。

[ヘルプ(Help)]メニュー

[ヘルプ(Help)]メニューには、次のコマンドがあります。

HTTP Editorヘルプ(HTTP Editor Help) - ヘルプファイルが開き **目次(Contents)]** タブがアクティブになります。

インデックス(Index) - ヘルプファイルが開き **[インデックス(Index)]** タブがアクティブになります。

検索(Search) - ヘルプファイルが開き **検索(Search)]** タブがアクティブになります。

HTTP Editorについて(About HTTP Editor) - HTTP Editorに関する情報を表示します。

要求アクション(Request actions)

要求ビューア(Request Viewer)] ペインの **要求アクション(Request Action)]** リストからは、次のオプションを使用できます。

PUTファイルのアップロード(PUT file upload)

PUTメソッドは、指定したRequest-URIの下に括弧内のエンティティを格納することを要求します。

サーバにファイルを書き込むには:

1. 要求ビューア(Request Viewer)] ペインのドロップダウンリストから **PUTファイルのアップロード(PUT File Upload)]** を選択します。
2. リストの右側に表示されるテキストボックスに、ファイルのフルパスを入力します。
- または -
フォルダを開く(Open Folder)] アイコンをクリックして、アップロードするファイルを選択します。
3. **Apply]** をクリックします。これにより、コンテンツ長の再計算も行われます。

Content-Lengthの変更(Change content-length)

通常モードでは、ユーザが要求のメッセージ本文を編集すると、HTTP Editorがコンテンツ長を再計算して、Content-Lengthヘッダ内の値を適切な値に置き換えます。しかし、**そのまま送信(Send As Is)]** オプションを使用する場合は、HTTP Editorはコンテンツ長を変更しません。要求を送信する前にこの再計算を強制的に実行するには、**Content-Lengthの変更(Change Content-Length)]** を選択して **適用(Apply)]** をクリックします。

パラメータ値のURLエンコーディング/デコーディング(URL encode/decode param values)

URLの仕様(RFC 1738、94年12月)は、URLに使用できる文字を、US-ASCII文字セットのサブセットに限定しています。一方、HTMLではISO-8859-1 (ISO-Latin)文字セットの全範囲をドキュメントで使用できます。またHTML4では使用できる文字の範囲が拡張されており、Unicode文字セット全体も範囲に含まれています。この制限の回避策としては、非標準の文字をエンコーディングして、それらをサポートするブラウザやプラグインで表示できるようにするという方法があります。

文字のURLエンコーディングは、「%」記号の後にその文字のISO-Latinコードポイントの2桁の16進表記が続く形式になります。例:

- アスタリスク記号「*」= ISO-Latinセットの10進数の42
- 10進数の42 = 16進数の2A
- アスタリスクのURLコード = %2A

URLエンコーディングを使用すると、ISO-Latin文字セットのみを使用して要求メッセージを検査することで特定のキーワードを検出する不正侵入者検出システム(IDS)をバイパスできます。たとえば、IDSは「login」(ISO-Latin)は検索できますが、この単語をURLエンコーディングしたものである「%4C%4F%47%49%4E」は検索しません。

メッセージ全体でパラメータをURLコードに置き換えるには、**{パラメータ値のURLエンコーディング(URL Encode Param Values)]** を選択し、**適用(Apply)]** をクリックします。

URLエンコーディングされたパラメータをISO-Latinに変換するには、**{パラメータ値のURLデコーディング(URL Decode Param Values)]** を選択し、**適用(Apply)]** をクリックします。

要求のUnicodeエンコーディング/デコーディング(Unicode encode/decode request)

Unicode Worldwide Character Standardでは、世界のすべての主要な記述言語の文字、数字、特殊文字、句読点、および技術記号を、統一されたエンコードスキームを使用して定義しています。クライアントサーバ型アプリケーションやWebサイトにUnicodeを組み込むと、従来の文字セットを使用する場合に比べて大幅にコストを削減できる可能性があります。

Unicodeを使用すると、1つのソフトウェア製品または1つのWebサイトを、再エンジニアリングなしで複数のプラットフォーム、言語、および国に向けて提供できます。また多くの異なるシステム間でデータを破損することなく転送できます。

要求メッセージ全体をUnicodeに変換するには、**要求のUnicodeエンコーディング(Unicode Encode Request)**]を選択し、**適用(Apply)**]をクリックします。

要求メッセージ全体をUnicodeからISO-Latinに変換するには、**要求のUnicodeデコーディング(Unicode Decode Request)**]を選択し、**適用(Apply)**]をクリックします。

マルチパートPostの作成(Create MultiPart post)

POSTメソッドは、要求内の括弧に入ったエンティティを、Request-LineのRequest-URIで指定されたリソースの新しい従属リソースとして受け入れるよう、発信元サーバに要求するために使用されます。POST要求メッセージを操作して、データのアップロードを試みることができます。

ファイルからデータを挿入するには:

1. **要求ビューア(Request Viewer)]** ペインの **アクション(Action)]** ドロップダウンリストから **マルチパートPostの作成(Create MultiPart Post)]** を選択します。
2. **アクション(Action)]** リストの右側にあるテキストボックスに、ファイルのフルパスを入力します。
- または -
フォルダを開く(Open Folder)] アイコンをクリックして、挿入するファイルを選択します。

3. **Apply]** をクリックします。

マルチパートPostの削除(Remove MultiPart post)

マルチパート要求の一部であるファイルを削除するには、**要求ビューア(Request Viewer)]** ペインの **アクション(Action)]** リストから **マルチパートPostの削除(Remove MultiPart Post)]** を選択します。

応答アクション

応答ビューア(Response Viewer)] ペインのタブのすぐ下のエリアには、次の3つのコントロールがあります。

- **チャンク(Chunked)]** ボタン
- **コンテンツコーディング(Content Coding)]** ドロップダウンリスト
- **🔍** ボタン。これを使用すると **応答で検索(Find In Response)]** ダイアログボックスが開き、そこでテキスト文字列を指定して応答内で検索できます。

チャンク(Chunked)

サーバは、応答の合計長を把握する前にその応答の送信を開始する場合、応答全体を小さなチャンクに分割して順番に送信します。このような応答には、「Transfer-Encoding: chunked」というヘッダが含まれています。チャンクメッセージ本文には、一連のチャンクが含ま

れ、その次に「0」(ゼロ)の行が続き、その後にオプションのフッタと空白行が続きます。各チャンクは、次の2つの部分で構成されます。

- 16進数のチャンクデータサイズを含んだ行。サイズの後にはセミicolonと追加のパラメータが続いている場合がありますが、それらは無視できます(現時点ではいずれも標準ではありません)。行の末尾はCRLFです。
- データそのもの。その後にCRLFが続きます。

コンテンツコーディング(Content codings)

HTTP応答に圧縮データが含まれている場合は、次のリストにあるオプションのいずれかを使用してデータを圧縮解除できます。

- GZIP - GNUプロジェクト用に作成された圧縮ユーティリティです。
- Deflate - RFC 1950 [31]で定義されている「zlib」形式を、RFC 1951 [29]で記述されている「deflate」圧縮メカニズムと組み合わせたものです。

参照情報

["要求の編集と送信" 下](#)

["要求または応答の検索" 次のページ](#)

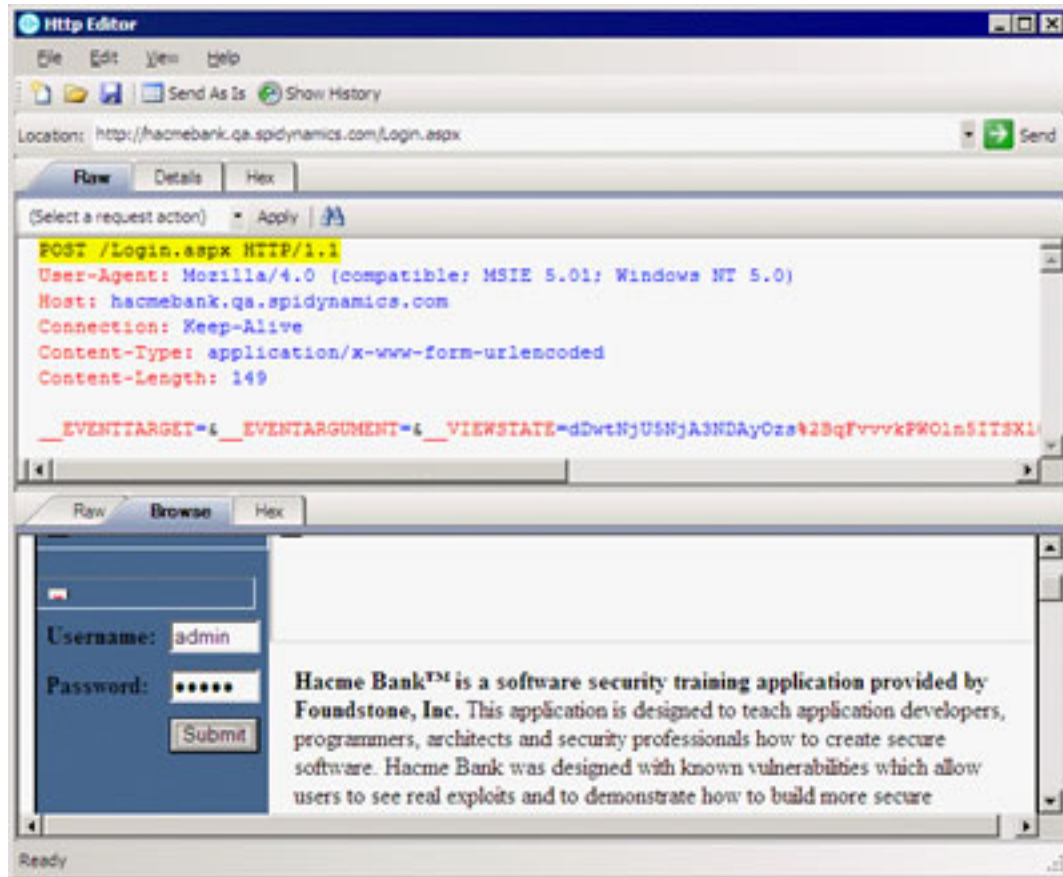
要求の編集と送信

要求を編集して送信するには:

1. **要求ビューア(Request Viewer)]** ペインで要求メッセージを変更します。
テキスト文字列をエンコードまたはデコードするには、テキストを選択して右クリックし、ポップアップメニューから **エンコーディング(Encoding)]** または **デコーディング(Decoding)]** を選択します。
要求の特定の項目を変更するには、**アクション(Action)]** リストから項目を選択し、**適用(Apply)]** をクリックします。詳細については、「["HTTPエディタ" ページ46](#)」を参照してください。
2. **送信(Send)]** をクリックして、HTTP要求メッセージを送信します。
HTTP応答メッセージを受信すると、**応答ビューア(Response Viewer)]** ペインにそのメッセージが表示されます。
3. 応答をブラウザにレンダリングして表示するには、**ブラウザ(Browser)]** タブをクリックします。
4. **ブラウザ(Browser)]** タブにレンダリングされたHTMLコントロールまたはJavaScriptコントロールを使用して、次に送信するHTTP要求を準備できます。この機能を使用するには、**対話型ナビゲーション(Interactive Navigation)]** オプション(**編集(Edit)]** > **設定(Settings)]** の順にクリック)を選択する必要があります。
 - a. **場所(Location)]** フィールドにURLを入力し、**送信(Send)]** をクリックします。
アプリケーションがログオンフォームを返します。
 - b. **応答(Response)]** ペインで、**ブラウザ(Browser)]** タブをクリックします。

- c. レンダリングされたページで、ユーザ名とパスワードを入力し、**送信 (Submit)]**をクリックします。

次の画像のようにHTTP Editorが要求(Login.aspx URLへのPOSTメソッドを使用する)をフォーマットし、それを **要求ビューア(Request Viewer)]** ペインに表示します。



- d. **送信 (Send)]**をクリックして、フォーマットされた応答(ユーザ名とパスワードを含む)をサーバに送信します。
5. 要求を保存するには、**ファイル(File)] > 要求の保存 (Save Requests)]**を選択します。

参照情報

"[要求または応答の検索](#)" 下

要求または応答の検索

要求または応答のテキストを検索するには:

1. 要求ビューア(Request Viewer)] ペインまたは 応答ビューア(Response Viewer)] ペインのいずれかで をクリックします。
2. 要求内の検索 (Find in Request)] ウィンドウまたは 応答内の検索 (Find in Response)] ウィンドウを使用して、文字列または正規表現を入力または選択します。

3. 検索文字列として正規表現を使用する場合は、**[Regex]** チェックボックスを選択します。
4. **[Find]** をクリックします。

設定(Settings)

HTTP Editorの設定を変更するには、**編集(Edit)] > 設定(Settings)]** をクリックし、次のいずれかのタブを選択して変更を加え、**[OK]** をクリックします。

- オプション
- 認証(Authentication)
- Proxy

各タブの設定については、次のセクションで説明します。

オプション(Options)] タブ

要求グループ(Request Group)] には次のオプションがあります。

- **そのまま送信(Send As Is)** -このオプションを選択した場合、選択したその他の設定に関係なく、HTTP Editorは要求を変更しません。このオプションを使用すると、意図的に誤った形式にしたメッセージを送信することができます。このオプションを使用すると、**認証(Authentication)]** および **プロキシ(Proxy)]** の設定は無効になります。

注記: プロキシを経由するように要求を手動で編集することはできますが、ほとんどの標準HTTPプロキシサーバは非標準のHTTP要求を処理できません。

- **要求の操作(Manipulate Request)** -このオプションを選択した場合、HTTP Editorは次のパラメータに対応するように要求を変更します。
- **状態の適用(Apply State)** -アプリケーションが、セッション内の状態を維持するためにクッキー、URL再書き込み、またはPOSTデータの技術を使用する場合、HTTP Editorはその方式を特定し、それに従って応答を変更しようとします。
- **プロキシの適用(Apply Proxy)** -このオプションを選択した場合、HTTP Editorはユーザが指定したプロキシ設定に従って要求を変更します。
- **フィルタの適用(Apply Filter)** -このオプションは、OpenText DASTの使用中にスキャンタブにフォーカスがあるとき(つまり、スキャンを開いた後かスキャンの実行中)にHTTP Editorを起動した場合のみ表示されます。このオプションが選択されている場合、HTTP Editorは、OpenText DASTの **現在のスキャン設定(Current Scan Settings)]** にある **フィルタ(Filters)]** 設定を適用して、HTTP要求および応答の検索および置換のルールを追加します。

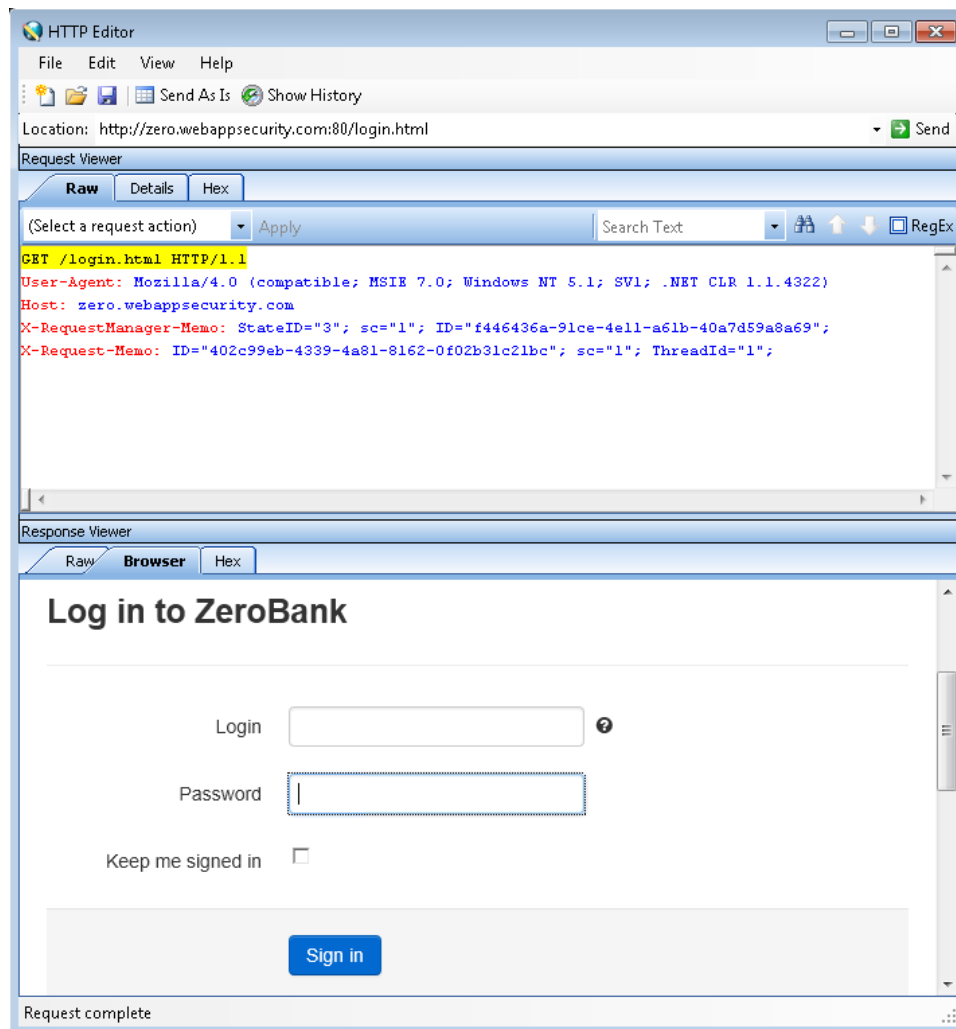
注記: HTTP Editorを呼び出す前に **現在のスキャン設定(Current Scan Settings)]** を変更しても、効果はありません。HTTP Editorは、スキャンの開始時に有効であった設定を使用します。

- **ヘッダの適用 (Apply Header)** -このオプションは、OpenText DASTの使用中にスキャンタブにフォーカスがあるとき(つまり、スキャンを開いた後かスキャンの実行中)にHTTP Editorを起動した場合のみ表示されます。このオプションが選択されている場合、HTTP Editorは、OpenText DASTの現在のスキャン設定(Current Scan Settings)]にある **クッキー/ヘッダ(Cookies/Headers)]** 設定をHTTP要求のために適用します。

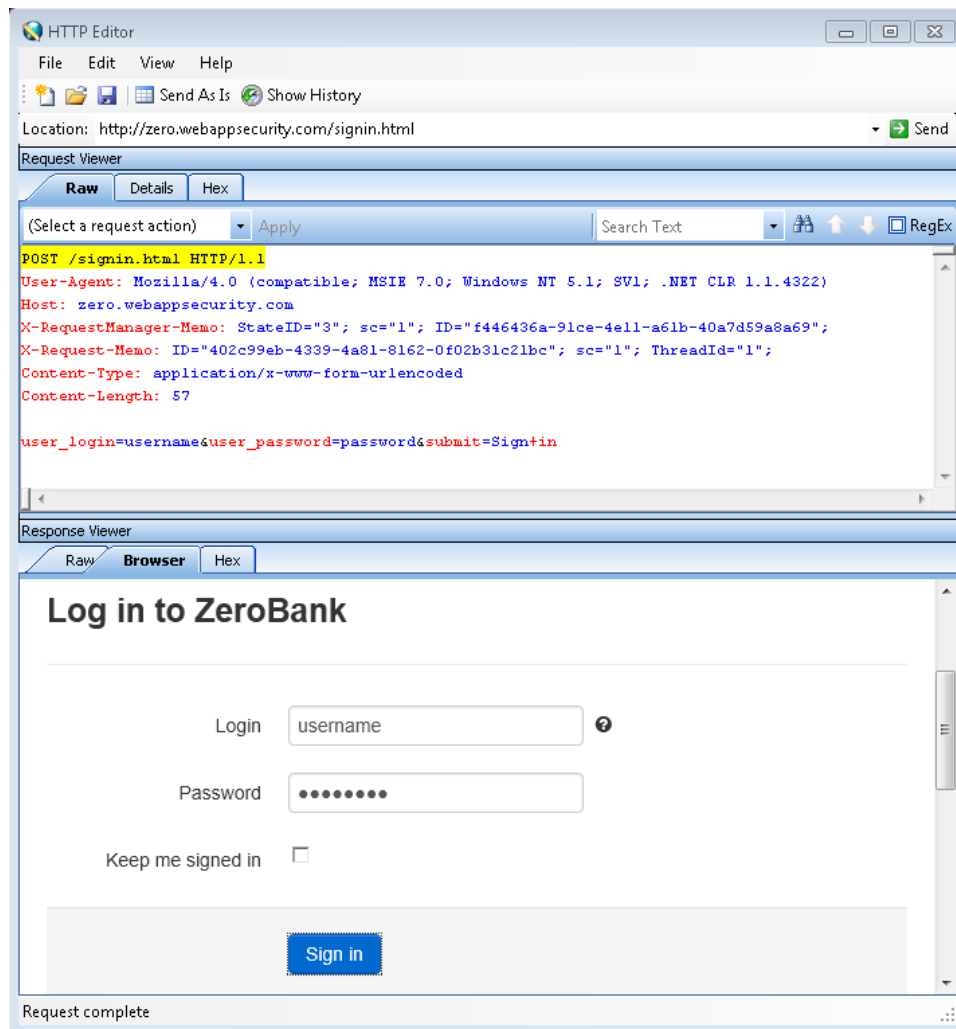
注記: HTTP Editorを呼び出す前に **現在のスキャン設定(Current Scan Settings)]** を変更しても、効果はありません。HTTP Editorは、スキャンの開始時に有効であった設定を使用します。

ナビゲーショングループ(Navigation group)] で、**なし(None)]**、**対話型(Interactive)]**、または **ブラウザモード(Browser Mode)]** を選択します。

応答ビューア(Response Viewer)] (下部ペイン)で **ブラウザ(Browser)]** タブを選択すると、サーバ応答をブラウザにレンダリングして表示できます。**対話型(Interactive)]** 機能が有効になっている場合は、ブラウザにレンダリングされたHTMLコントロールまたはJavaScriptコントロールを使用して、次に送信するHTTP要求を準備できます。



たとえば、`http://zero.webappsecurity.com:80/login.html`のログインページ(上の画像のもの)を使用する場合は、**[Login]**の名前(「username」と**Password**)(「password」)を入力してから**Sign in**をクリックできます。HTTP Editorは、要求(`signin.html`リソースへのPOSTメソッドを使用する)をフォーマットし、次の画像のように要求を**要求ビューア(Request Viewer)**に表示します。その後、ログインメッセージを編集するか(必要な場合)、そのまま**送信(Send)**をクリックしてサーバに送信します。



ブラウザモード(Browser Mode) オプションを選択すると、**対話(Interactive)** モードは有効になりますが、HTTP Editorは直ちに要求を送信します。先にユーザが編集できるように要求を**要求ビューア(Request Viewer)**に表示することはしません。

アクティブコンテンツを有効にする(Enable Active Content) チェックボックスをオンにすると、すべてのブラウザウィンドウでJavaScriptおよび他のダイナミックコンテンツを実行できるようになります。

ほとんどのWebページには、使用すべき文字セットをブラウザに指示する情報が含まれています。この指示は、HTMLドキュメントのHEADセクションのContent-Type応答ヘッダ(またはHTTP-EQUIV属性を持つMETAタグ)を使用して行われます。文字セットをアナウンスしていないページ用にHTTP Editorで使用するべき文字セットを指定できます。**高度なHTTP解析**

(Advanced HTTP Parsing)]グループで、**想定される「文字セット」エンコード(Assumed 'charset' Encoding)]**を選択します。

認証(Authentication)]タブ

認証が必要な場合は、**認証(Authentication)]**リストからタイプを選択します。認証メソッドを選択した後、ユーザ名とパスワードを入力します。認証メソッドは次のとおりです。

- 自動
- HTTP基本(HTTP Basic)
- NTLM

認証メソッドを選択した後、**ユーザ名(User name)]**と**パスワード(Password)]**に入力します。入力ミスを防ぐため、**パスワードの確認(Confirm Password)]**フィールドにパスワードを再入力する必要があります。

プロキシ(Proxy)]タブ

プロキシサーバを介してHTTP Editorにアクセスするには、次の設定を使用します。

- **直接接続(プロキシ無効)(Direct Connection (proxy disabled))** - プロキシサーバを使用しない場合は、このオプションを選択します。
- **プロキシ設定の自動検出(Auto detect proxy settings)** - WPAD (Web Proxy Autodiscovery Protocol)を使用してプロキシ自動設定ファイルを見つけ、それを使用してブラウザのWebプロキシ設定を行う場合は、このオプションを選択します。
- **システムのプロキシ設定を使用する(Use System proxy settings)** - ローカルマシンからプロキシサーバ情報をインポートするには、このオプションを選択します。
- **Firefoxプロキシ設定を使用する(Use Firefox proxy settings)** - Firefoxからプロキシサーバ情報をインポートするには、このオプションを選択します。

注記: ブラウザのプロキシ設定を使用しても、プロキシサーバ経由でインターネットにアクセスできる保証はありません。Firefoxブラウザの接続設定が「プロキシなし」に設定されている場合、プロキシは使用されません。

- **プロキシを明示的に設定する(Explicitly configure proxy)** - プロキシサーバ経由でインターネットにアクセスするには、このオプションを選択し、要求された情報を以下のように入力します。
 - a. **サーバ(Server)]**フィールドにプロキシサーバのURLまたはIPアドレスを入力し、続いて**(ポート(Port)]**フィールドにポート番号(8080など)を入力します。
 - b. プロキシサーバ経由のTCPトラフィックの処理のためのプロトコルを、SOCKS4、SOCKS5、または標準の中から選択します。

- c. 認証が必要な場合は、**認証(Authentication)]**リストからタイプを選択します。
 - **自動**

メモ: 自動検出を指定すると、スキャンの処理が遅くなります。把握している別の認証メソッドを指定すると、スキャンのパフォーマンスは大幅に向上します。
 - **基本**
 - **ダイジェスト**
 - **Kerberos**
 - **ネゴシエート(Negotiate)**
 - **NTLM**
- d. プロキシサーバで認証が必要な場合は、適格な **ユーザ名(User name)]**と **パスワード>Password)]**を入力します。
- e. 特定のIPアドレス(内部テストサイトなど)にアクセスするためにプロキシサーバを使用する必要がない場合は、**プロキシをバイパスするサイト(Bypass Proxy For)]**フィールドにアドレスまたはURLを入力します。エントリを区切る場合は、カンマを使用します。
- **HTTPS用の代替プロキシを指定する(Specify Alternative Proxy for HTTPS)**

HTTPS接続を受け入れるプロキシサーバの場合は、**HTTPS用の代替プロキシを指定する(Specify Alternative Proxy for HTTPS)]**チェックボックスを選択し、要求された情報を入力します。

正規表現

正規表現のパターンは、特殊な文字やシーケンスを使用して作成されます。次の表に、これらの文字の一部を示し、その簡単な使用例を示します。推奨する他の参照先として「[Regular Expression Library](#)」があります。

文字	説明
\	次の文字を特殊文字としてマークします。/n/は文字「n」に一致します。シーケンス\n/は、改行文字に一致します。
^	入力または行の先頭に一致します。 文字クラスとともに使用すると、否定文字を意味します。たとえば、contentディレクトリ内の/content/enおよび/content/caを除くすべてを除外するには、/content/[^(en ca)].*.*を使用します。\\S\\D\\Wも参照してください。
\$	入力または行の末尾に一致します。
*	先行する文字の0回以上の反復と一致します。/zo*/は「z」とも「zoo」とも一致します。
+	先行する文字の1回以上の反復と一致します。/zo+/は「zoo」に一致しますが、

文字	説明
	「z」には一致しません。
?	先行する文字の0回または1回の出現と一致します。/a?ve?/は「never」の「ve」に一致します。
.	改行文字を除く任意の1文字に一致します。
[xyz]	文字セット。括弧内の任意の1文字に一致します。/[abc]/は「plain」の「a」に一致します。
\b	スペースなどの単語境界に一致します。/ea*r\b/は、「never early」の「er」に一致します。
\B	単語以外の境界に一致します。/ea*r\B/は「never early」の中の「ear」と一致します。
\d	1つの数字に一致します。[0-9]と同じです。
\D	数字以外の1文字に一致します。[^0-9]と同じです。
\f	改ページ文字に一致します。
\n	改行文字に一致します。
\r	キャリッジリターン文字に一致します。
\s	スペース、タブ、改ページなどの空白に一致します。[\f\n\r\t\v]と同じです。
\S	空白文字以外の文字に一致します。[^ \f\n\r\t\v]と同じです。
\w	アンダースコアを含む任意の単語文字に一致します。[A-Za-z0-9_]と同じです。
\W	英数字以外の文字に一致します。[^A-Za-z0-9_]と同じです。

参照情報

["正規表現の拡張と演算子" 下](#)

正規表現の拡張と演算子

OpenTextのエンジニアにより、通常の正規表現構文の拡張、およびそれに伴う一連の演算子が開発および実装されました。

正規表現タグ

正規表現を構築する場合、この拡張を使用して、要求または応答のどの要素内で一致を検索するかを指定できます。次の表に、拡張の説明を示します。

拡張	要素
[ALL]	要求または応答のすべての要素
[BODY]	要求の本文 応答本文
[COOKIES]	要求のクッキー
[HEADERS]	要求ヘッダ(Request Headers) 応答ヘッダ(Response Headers)
[METHOD]	要求のメソッド(Request Method)
[POSTDATA]	Postデータ
[REQUESTLINE]	要求行(HTTP要求の開始行)
[SETCOOKIES]	Set-Cookie応答ヘッダ
[STATUSCODE]	ステータスコード(Status Code)
[STATUSDESCRIPTION]	ステータスの説明(クライアントに返されるHTTP出力のステータスを説明する文字列)
[STATUSLINE]	ステータス行(HTTP応答の開始行)
[URI]	要求ターゲット(URI)
[VERSION]	HTTPバージョン

正規表現演算子

OpenTextのエンジニアにより、複雑な正規表現パターンの構築に使用できる正規表現演算子が開発されました。演算子は次のとおりです。

- AND
- OR
- NOT

- []
- ()

例

以下の段落に、拡張と演算子の使用例を示します。

- (a)ステータス行にステータスコード「200」が含まれており、かつ(b)メッセージ本文のどこかに「logged out」という語句が含まれている応答を検出するには、次の正規表現を使用します。

[STATUSCODE]200 AND [BODY]logged\sout

- 要求されたリソースが一時的に別のURI (リダイレクト)に存在することを示しており、かつ応答のどこかにパス「/Login.asp」への参照が含まれる応答を検出するには、次の正規表現を使用します。

[STATUSCODE]302 AND [ALL]Login.asp

- (a)ステータスコードが「200」、かつ「logged out」または「session expired」という語句が本文のどこかに含まれている、または(b)ステータスコード「302」、かつ応答のどこかにパス「/Login.asp」への参照が含まれている応答のいずれかを検出するには、次の正規表現を使用します。

([STATUSCODE]200 AND [BODY]logged\sout OR [BODY]session\sexpired) OR ([STATUSCODE]302 AND [ALL]Login.asp)

注記:「開き括弧」または「閉じ括弧」の前と後にスペースを含める必要があります。スペースを含めないと、括弧は誤って正規表現の一部と見なされます。

- リダイレクト Locationヘッダのどこかに「login.aspx」が現れるリダイレクト応答を検出するには、次の正規表現を使用します。

[STATUSCODE]302 AND [HEADERS]Location:\slogin.aspx

- ステータス行のReason-Phrase部に特定の文字列(「Please Authenticate」など)が含まれる応答を検出するには、次の正規表現を使用します。

[STATUSDESCRIPTION]Please\sAuthenticate

参照情報

["正規表現" ページ57](#)

第6章:Log Viewer(OpenText DASTのみ)

OpenText DASTが管理するさまざまなログを検査するには、Log Viewerを使用します。この機能は主に、報告されたインシデントを調査するためにカスタマサポートグループによって使用されます。

ログファイルを表示するには:

1. **ツール(Tools)] > [Log Viewer]**をクリックします。
スキャンが含まれるタブにフォーカスがあるときにLog Viewerを開いた場合、プログラムはユーザがそのスキャンのログを表示しようとしているものと見なします。ステップ4に進みます。
2. **スキャンを開く(Open Scan)]**をクリックします。
3. **スキャンを開く(Open Scan)]** ウィンドウで、ログを表示するスキャンを選択し、**開く(Open)]**をクリックします。別のデータベースのスキャンを開く場合は、**データベースの変更(Change Database)]**をクリックします。
4. **ログタイプ(Log Type)]** リストからログを選択します。使用可能なタイプは、(OpenText DASTの **アプリケーション設定 (Application settings)]** で)そのスキャンに対して選択されたログレベルによって異なります。
5. ログ内のテキストを検索するには、ツールバーの **検索(Find)]** をクリックします。
- または -
編集(Edit)] > 検索(Find)] を選択します。
6. ログファイルを保存するには、ツールバーの **エクスポート(Export)]** をクリックします。
- または -
ファイル(File)] > ログのエクスポート(Export Logs)] を選択します。
7. 特定のスキャンに関連しないログを表示するには、ツールバーの **DASTログ(DAST Logs)]** をクリックします。

第7章:ポリシーマネージャ

ポリシーとは、OpenText DASTがWebアプリケーションの監査またはWeb探索を行うときに使用する監査エンジンおよび攻撃エージェントのコレクションです。各コンポーネントには、クロスサイトスクリプティングの受けやすさのテスト、サイトツリーの構築、既知のサーバ脆弱性のプローブなど、特定のタスクがあります。これらのコンポーネントは、次のグループに分けられます。

- 監査エンジン
- 監査オプション
- 一般的なアプリケーションテスト
- 一般的なテキスト検索
- サードパーティのWebアプリケーション
- Webのフレームワーク/言語
- Webサーバ
- Webサイトの検出
- カスタムエージェント
- カスタムチェック

監査エンジンを除くこれらすべてのコンポーネントは、まとめて攻撃グループと呼ばれます。各攻撃グループには、Webサイトの脆弱性をチェックする個別のモジュール(攻撃エージェントと呼ばれる)のサブグループが含まれています。

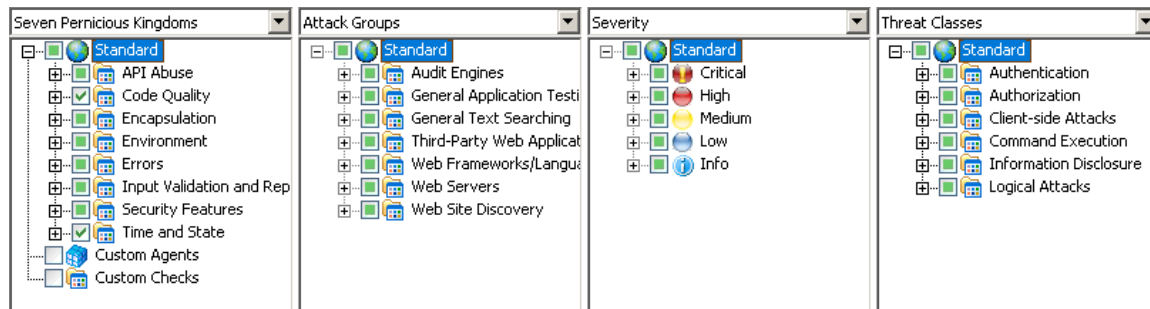
OpenText DASTには、ほとんどのユーザ要件に合うように設計された、事前パッケージ化されたポリシーがいくつか含まれています。すべてのポリシーには使用可能なすべての監査エンジンとエージェントが含まれていますが、これらのコンポーネントのうち有効にされるサブセットは、ポリシーごとに異なります。ポリシーは、監査エンジンおよび/または個々の攻撃エージェント(またはエージェントのグループ)を有効または無効にすることで編集できます。ポリシーを作成するには、既存のポリシーを編集して、新しい名前で作成します。

ビュー

Policy Managerには、標準ビューと検索ビューの2種類のビューがあります。これらは [ビュー (View)] メニューからツールバーのアイコンをクリックして切り替えることができます。

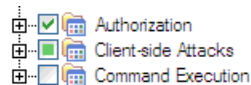
標準ビュー

このビューには、デフォルトでは7つの有害な界ごとに分類されたチェックのリストが表示されます。ドロップダウンリストを使用して、攻撃グループごと、重大度ごと、および脅威クラスごとにチェックを表示することもできます(分類は、Web Application Security Consortiumの分類に従ったものになります)。



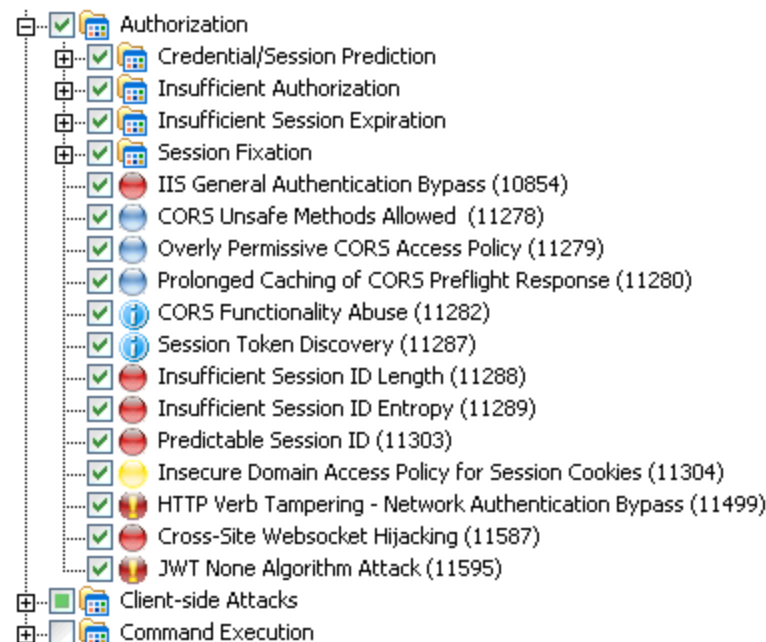
コンポーネントを有効または無効にするには、コンポーネントに関連付けられているチェックボックスをオンまたはオフにします。

展開されていないノードの横にあるチェックボックスは、ノード内のオブジェクトの「選択」ステータスを示します。



- チェックは、すべてのオブジェクトが選択されていることを示します。
- 緑色の四角は、一部のオブジェクトが選択されていることを示します。
- 空のボックスは、オブジェクトがまったく選択されていないことを示します。

ノードを展開するには、プラス記号  をクリックします。

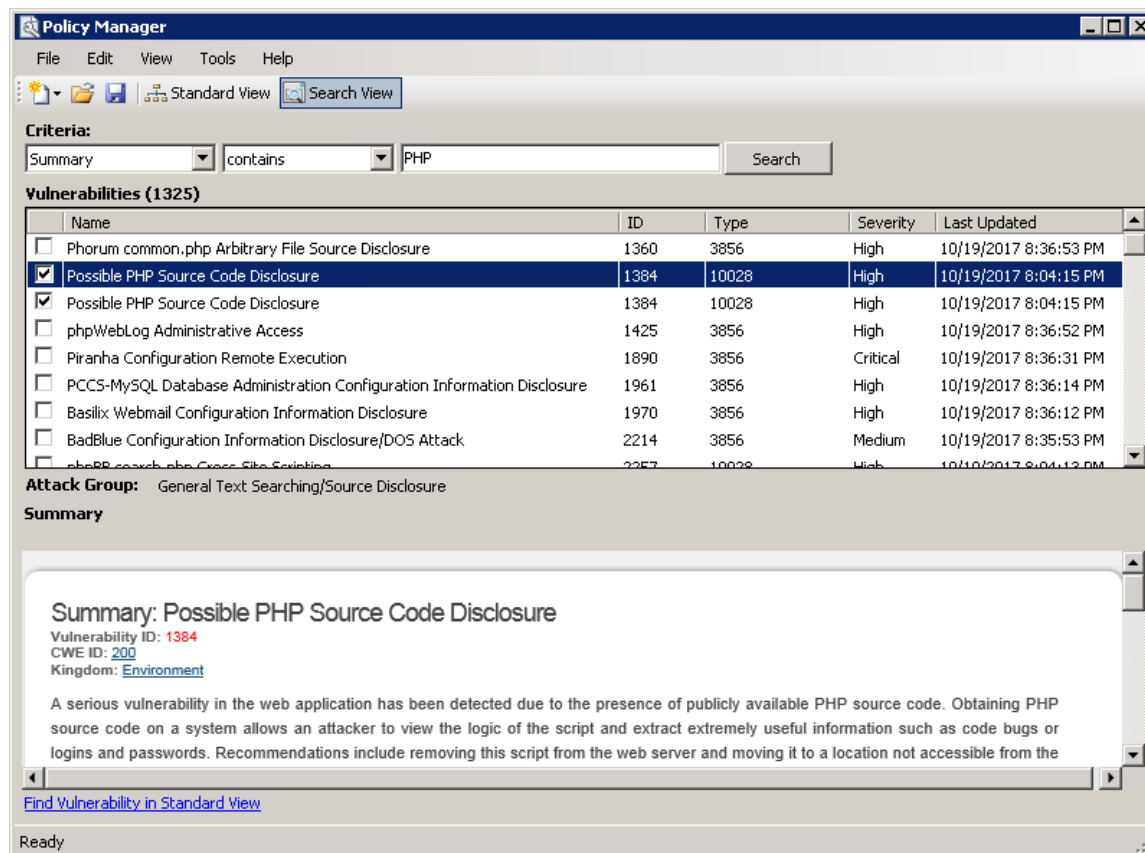


検索ビュー

このビューでは、基準リストから選択した属性に基づいて攻撃エージェントを検索できます。

- 脆弱性ID
- 脆弱性名
- エンジンタイプ
- 最終更新日時
- CWE ID
- 界
- 概要
- 意味
- 実行
- 修復
- 参照情報

この機能は、無効にするチェックを見つけるために最もよく使用されます。たとえば、PHPスクリプトを含まないアプリケーションをスキャンする場合、概要フィールドで「PHP」を検索できます。検索条件と一致する攻撃エージェントがPolicy Managerにリストされたら、そのエージェントに結び付いたチェックボックスをクリアしてエージェントを無効にできます。その後、変更したポリシーを保存する(そのポリシーの変更を永続的にする)か、変更したポリシーを単純に現在のスキャンに適用することができます。



参照情報

["ポリシー" ページ85](#)

["ポリシーの作成または編集" 下](#)

["特定のエージェントの検索" ページ75](#)

["カスタムチェックの使用" 次のページ](#)

ポリシーの作成または編集

OpenText DASTには、多くのユーザに対応できるように設計された、事前パッケージ化されたポリシーがいくつか含まれています。これらのポリシーは恒久的に変更することはできません。ただし、これらのいずれかをテンプレートとして開き、内容を変更してカスタムポリシーを作成し、カスタマイズしたこのポリシーを新しい名前で保存することはできます。カスタムポリシーは、名前を変更せずに編集および保存できます。

ポリシーを編集または作成するには:

1. ツールバーで、**[Policy Manager]** をクリックします。
- または -
[ツール(Tools)] > [Policy Manager] の順に選択します。
Policy Managerが開きます。デフォルトでは、標準ポリシーがロードされます。
2. 次のいずれかを実行します。
 - 以前に作成したポリシー(つまり、カスタムポリシー)を編集するには、**[ファイル(File)] > 開く(Open)]** の順に選択し、ポリシーを選択します。
 - 事前パッケージ化されたポリシーの1つを基にポリシーを作成するには、**[ファイル(File)] > 新規(New)]** の順に選択(または **新規ポリシー(New Policy)]** アイコンをクリック)し、新しいポリシーのモデルにするポリシーを選択します。
3. 攻撃グループに対応するチェックボックスをクリア(または選択)することによって、攻撃グループを無効(または有効)にします。グループ内のエージェントを個別に無効または有効にするには、まずグループを展開してから、該当するチェックボックスを編集します。
4. 攻撃グループの名前を変更するには:
 - a. 攻撃グループを右クリックします。
 - b. ショートカットメニューから、**名前変更(Rename)]** を選択します。
5. 攻撃グループを追加するには:
 - a. 既存の攻撃グループを右クリックします。
 - b. ショートカットメニューから、**新規攻撃グループ(New Attack Group)]** を選択します。
新規攻撃グループ(New Attack Group)] という項目が強調されて表示されます。
 - c. その新しいグループを右クリックし、**名前変更(Rename)]** を選択します。
 - d. グループに攻撃エージェントをドラッグアンドドロップして追加します。
6. カスタムチェックを作成することもできます。詳細については、「["カスタムチェックの使用" 次のページ](#)」を参照してください。

7. **自動更新(Auto Update)]** チェックボックスが選択されている場合、OpenText DASTはOpenTextデータベースからダウンロードされる更新された攻撃エージェントや新しい攻撃エージェントを有効にするか無効にするかを、その兄弟エージェントの分析結果に基づいて決定します。たとえば、MicrosoftのIIS (Internet Information Server)を対象とする攻撃エージェントを無効にして **自動更新(Auto Update)]**を選択すると、OpenText DASTはシステムにダウンロードするIIS関連の攻撃エージェントを有効にしません。逆に、ポリシーで有効になっているエージェントに関連する新しい攻撃エージェントや更新された攻撃エージェントは有効にされます。

注記: スマートアップデートによってダウンロードされた新しい脆弱性チェックは、ユーザの作成したカスタムポリシーに自動では追加されません。

8. **ファイル(File)] > 名前を付けて保存(Save As)]**の順に選択します。 **ファイル名(File name)]** フィールドにカスタムポリシーの名前を入力し、 **保存(Save)]** をクリックして新しいポリシーをOpenText DASTの*.policy形式で保存します。デフォルトポリシーの名前(攻撃(Assault)、ブランク(Blank)、標準(Standard)など)を使用してポリシーを保存することはできません。

参照情報

["カスタムエージェントの使用" ページ76](#)

["特定のエージェントの検索" ページ75](#)

["カスタムチェックの使用" 下](#)

カスタムチェックの使用

OpenText DASTは実在または潜在するセキュリティ上の脆弱性を検出するためにWebサイト全体を綿密に調べますが、アプリケーションに固有の脆弱性を検出するにはカスタムチェックが必要な場合があります。

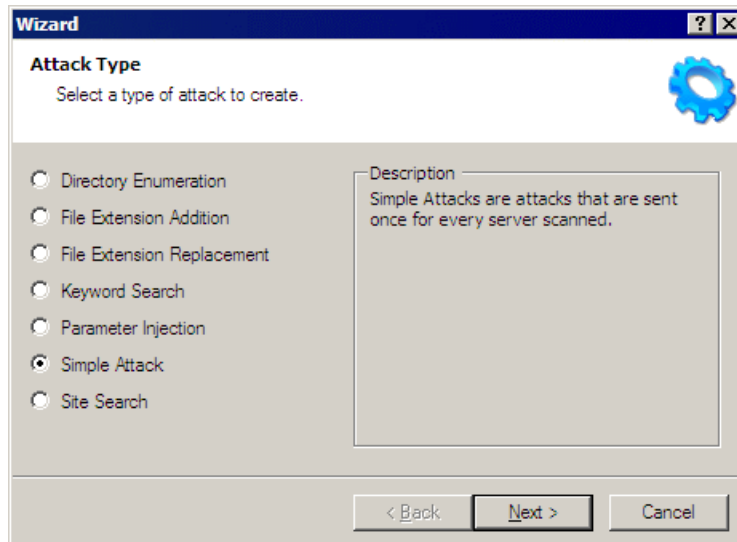
OpenText DASTが実行する攻撃と重複するカスタムチェックを作成した場合は、該当する標準のチェックを無効にしない限り、その新しいチェックは送信されません。たとえば、OpenText DASTは通常、「(copy)」というサフィックスの付いたバックアップディレクトリを検索するディレクトリ列挙チェックを実行します。作成したカスタムチェックがこれと同様にサフィックス「(copy)」の付いたバックアップディレクトリを検索するチェックである場合は、番号11485の「バックアップディレクトリ((copy))(Backup Directory ((copy)))」という名前のチェックを無効にしないと、OpenText DASTは(そのディレクトリをすでに検索しているので)このカスタムチェックを送信しません。

カスタムチェックの作成

Policy Managerでカスタムチェックを作成するには:

1. 次のいずれかを実行します。
 - 以前に作成したポリシーを編集するには、 **ファイル(File)] > 開く(Open)]**の順に選択し、ポリシーを選択します。

- 事前パッケージ化されたポリシーを基に新しいポリシーを作成する場合は、**ファイル (File)] > 新規(New)]**の順に選択(または **新規ポリシー(New Policy)]** アイコンをクリックし、新しいポリシーのモデルにするポリシーを選択します。
2. **標準ビュー(Standard view)]** が選択されていて、左側のペインに7つの有害な界がリストされていることを確認します。
 3. **カスタムチェック(Custom Checks)]** を右クリックし、ショートカットメニューから **新規カスタムチェック(New Custom Check)]** を選択します。
カスタムチェックウィザードが表示されます。



4. 以下の攻撃タイプから1つを選択します。各タイプの詳細説明と例も、共に以下に示します。

- **ディレクトリ列挙(Directory enumeration)**

このチェックでは、指定した名前のディレクトリが検索されます。

- 攻撃タイプ: ディレクトリ列挙(Directory Enumeration)
- 攻撃: /directory_name/ (directory_nameは検索するディレクトリの名前)
- シグニチャ: [STATUSCODE]3\d\d OR [STATUSCODE]2\d\d OR [STATUSCODE]40[13]

- **ファイル拡張子の追加(File extension addition)**

このタイプのチェックでは、指定したファイル拡張子を持つファイルが検索されます。

OpenText DASTはWeb探索中に何らかの名前と何らかの拡張子のファイル(たとえば、global.asa)を検出すると、それと同じ名前で、検出した拡張子とユーザが指定した拡張子が付いたファイルのHTTP要求を送信します。たとえば、ユーザが.backupというファイル拡張子を指定している場合、OpenText DASTはglobal.asaというファイルを検出すると、続いてglobal.asa.backupというファイルを検索します。

通常、サーバはglobal.asaファイルの要求を拒否しますが、プログラマがサーバ上にバックアップファイルを残していて、そのファイルに別の拡張子が付いていると(global.asa.backupなど)、そのファイル(これにはglobal.asaファイルの完全なソースが含まれている)をサーバが返してしまう可能性があります。

特定の追加された拡張子を持つファイルを検索するカスタムチェックを作成するには、カスタムチェックウィザードで以下を入力します。

- 攻撃タイプ: ファイル拡張子の追加 (File Extension Addition)
- 攻撃: .ext (extは検索するファイルのファイル拡張子) 先頭にドットまたはピリオド(.)が必要です。
- シグニチャ: [STATUSCODE]200 AND ([HEADERS]Content-Type:\stext/plain OR [HEADERS]Content-Type:\sapplication/octet-stream)

- **ファイル拡張子の置換 (File extension replacement)**

このタイプのチェックでは、指定したファイル拡張子を持つファイルが検索されます。

たとえば、OpenText DASTには、拡張子 .old が付いたファイルを検索する標準のチェックが含まれています。WebInspectはWeb探索中に検出する任意の名前および任意の拡張子のファイル(たとえば、startup.asp)について、それと名前が同じで拡張子 .old が付いているファイル(たとえば、startup.old)のHTTP要求を送信します。

特定の拡張子を持つファイルを検索するカスタムチェックを作成するには、カスタムチェックウィザードで以下を入力します。

- 攻撃タイプ: ファイル拡張子の置換 (File Extension Replacement)
- 攻撃: ext (「ext」は検索するファイルのファイル拡張子) 先頭にドットまたはピリオド(.)は付けません。
- シグニチャ: [STATUSCODE]200 AND ([HEADERS]Content-Type:\stext/plain OR [HEADERS]Content-Type:\sapplication/octet-stream)

- **キーワード検索 (Keyword search)**

このタイプのチェックでは、指定の単語または語句(正規表現で定義される)がHTTP応答内に存在するかどうかを判定します。

次の例は、HTTP応答で、社会保障番号形式の9桁の数字を検索します(\d = 任意の数字)。

- 攻撃タイプ: キーワード検索 (Keyword Search)
- 攻撃: N/A
- シグニチャ: [BODY]\d\d\d-\d\d\d-\d\d\d\d

- **パラメータインジェクション (Parameter injection)**

このタイプの攻撃では、引数値が攻撃文字列に置き換えられます。

例:

http://www.samplesite.com/webapp.asp?ValidParameter=ValidArgument

が次のように変更されます。

http://www.samplesite.com/webapp.asp?ValidParameter=AttackArgument

パラメータインジェクションには、次のようないくつかの種類があります。

- コマンド実行 (Command Execution)
コマンド実行のチェックでは、特殊文字からなる文字列が、オペレーティングシステムレベルのコマンドと組み合わせられます。これは(Webアプリケーションが入力をチェッ

くして阻止できない場合に) Webアプリケーションに指定の文字列を使用してコマンドを実行させようとする試みです。

次の例では、support_page.cgiというプログラムに疑似的な入力を提供することで、パラメータインジェクションを検査します。正規表現と一致するデータがHTTP応答に含まれている場合、アプリケーションはコマンド実行に対して脆弱ということになります。

- 攻撃タイプ: パラメータインジェクション(Parameter Injection)
- 攻撃: /support_page.cgi?file_name=|id|
- シグニチャ: [BODY]uid= AND [BODY]gid=

- SQLインジェクション

SQLインジェクションとは、アプリケーションにSQLコードを渡す操作です。これらの攻撃文字列はSQL構文の断片で構成されており、WebアプリケーションがSQLステートメントを作成する際に事前に特定の文字を除去しないでこの文字列を使用すると、そのSQL構文の断片がデータベースサーバで実行されます。

- 攻撃タイプ: パラメータインジェクション(Parameter Injection)
- 攻撃: ' (1つのアポストロフィ)
- シグニチャ: [STATUSCODE]5\d\d

- クロスサイトスクリプティング(Cross-Site Scripting)

この問題は、ダイナミックに生成されたWebページに、正しく検証されない入力が表示されている場合に発生します。この場合、攻撃者は生成されたそのページに悪意のあるJavaScriptを埋め込み、悪意のあるそのページを閲覧した任意のユーザのマシンでスクリプトを実行することができます。ユーザがテキストメッセージを投稿できるサイトは、このような攻撃に対して脆弱な可能性があります。

次の例では、Fusion Newsアプリケーションでのクロスサイトスクリプティングを検査します。

- 攻撃タイプ: パラメータインジェクション(Parameter Injection)
- 攻撃: /fullnews.php?id=<script>alert(document.cookie)</script>
- シグニチャ: [ALL]Powered\sby\sFusion\sNews And [ALL]<script>alert\ (document\.cookie\)</script>

- ディレクトリトラバーサル

ディレクトリトラバーサルでは、不正なURL文字列を送信して、Webサーバのコンテンツの非公開部分にアクセスします。攻撃者は、相対ハイパーリンクを使用して、サーバ上のさまざまなファイルにアクセスしようとします。たとえば、攻撃者は2つのピリオドとスラッシュの3文字(../)をターゲットURLに追加し、トラバースするディレクトリの数をさまざまに変化させることによって、www.server.com/../../../../passwordなどのシステムパスワードファイルを見つけてそれにアクセスする可能性があります。

次の例では、boot.iniファイルが検索されます。

- 攻撃タイプ: パラメータインジェクション(Parameter Injection)
- 攻撃: ../../../../../../../../../../boot.ini
- シグニチャ: [ALL]\[boot\loader\]
- 異常入力(Abnormal Input)

異常入力の攻撃文字列は、予期しない入力禁止されていないWebアプリケーションで未処理例外(プログラムに処理がコーディングされていないエラー)を引き起こす可能性がある文字で構成されます。多くの場合、未処理例外が発生すると、アプリケーションの内部メカニズムに関する機密情報を開示するエラーメッセージがサーバにより表示されます。ソースコードも開示される場合があります。

次の例では、バッファオーバーフローを引き起こすために、過度に長い文字列が送信されます。

- 攻撃タイプ: パラメータインジェクション(Parameter Injection)
- 攻撃: AAAAAAAAAAAAAA...AAAAAAAAA (文字「A」の1000回の繰り返し)
- シグニチャ: [STATUSCODE]5\d\d

- **単純攻撃(Simple attack)**

このタイプの攻撃は、サーバをスキャンするたびに1回送信されます。

次の例では、ターゲットのURLまたはIPアドレスに攻撃文字列を追加することにより、UNIXパスワードファイルの取得を試みます。

- 攻撃タイプ: 単純攻撃(Simple Attack)
- 攻撃: /etc/passwd
- シグニチャ: [ALL]root: AND [ALL]:0:0

- **サイト検索(Site search)**

このタイプの攻撃は、Webサーバによく残されることがあるファイルを検出する目的で行われます。たとえば、ID番号279のチェックでは、log.htmというファイルを検索します。

次の例では、ターゲットのURLまたはIPアドレスに攻撃文字列を追加することにより、xanadu.htmlというファイルを検索します。

- 攻撃タイプ: サイト検索(Site Search)
- 攻撃: xanadu.html
- シグニチャ: [STATUSCODE]2\d\d OR [STATUSCODE]40[1]

confidential.txtという名前のファイルを検索するカスタムチェックを作成するには、カスタムチェックウィザードで以下を入力します。

- 攻撃タイプ: サイト検索(Site Search)
- 攻撃: confidential.txt
- シグニチャ: [STATUSCODE]2\d\d AND ([HEADERS]Content-Type:\stext/plain OR [HEADERS]Content-Type:\sapplication/octet-stream)

5. **次へ(Next)]**をクリックします。

6. **攻撃(Attack)]**フィールドに、攻撃に使用するデータを入力します。

上記のディレクトリ列挙の例のチェックでは、ターゲットのURLまたはIPアドレスに攻撃文字列(/personnel/)を追加することで、「personnel」というディレクトリを検索します。

7. ユーザはシグニチャを指定する必要があります。シグニチャとは単なる正規表現(検索パターンを記述する特殊なテキスト文字列)です。OpenText DASTはHTTP応答を検索し、シグニチャで記述されたテキストを見つけると、そのセッションに脆弱性フラグを設定します。 **検索対象(Search for)]**フィールドとドロップダウンリストを使用して正規表現を作成することができます。ウィンドウの下部にあるテキストボックスに正規表現を直接入力することもできます。

検索対象(Search for)]フィールドを使用するには:

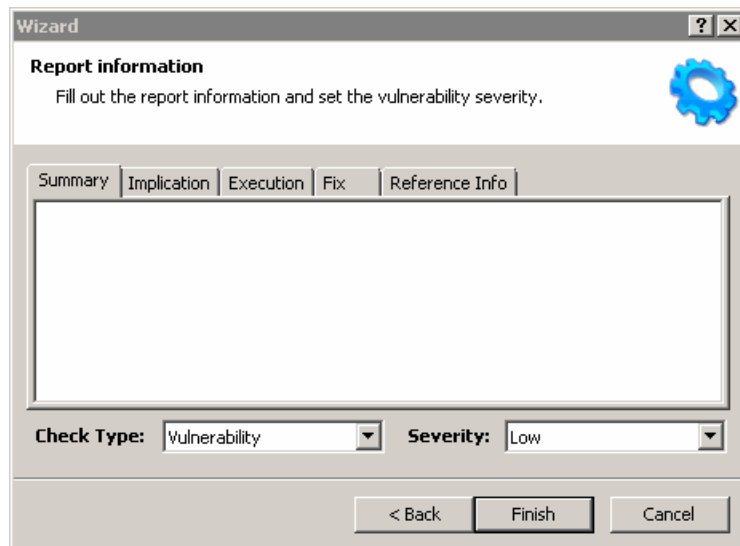
- a. 検索するテキストを入力します。

検索対象(Search for)]フィールドにはテキストのみを入力します。正規表現は入力しないでください。

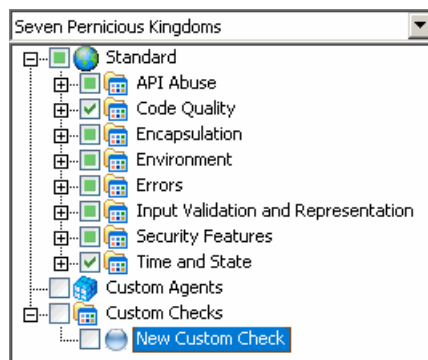
この例(「personnel」というディレクトリを検索する場合、ディレクトリが存在する場合はサーバがステータスコード200を返すので、 **検索対象(Search for)]**フィールドに「200」と入力します。ただし実際には、200番台または300番台のステータスコードや、ステータスコード401または403を受け入れる場合もあるでしょう。

- b. ドロップダウン矢印をクリックして、検索するHTTP応答のセクションを指定します。
c. (オプション)複雑な検索を作成する場合は、2番目のドロップダウンをクリックして、ブール演算子(AND、OR、またはNOT)を選択します。
d. **挿入(Insert)]**をクリックします。
e. (オプション)複雑な検索を行う場合は、必要に応じてステップaからdを繰り返します。下部のテキストボックスに表示される正規表現を編集または置換することもできます。

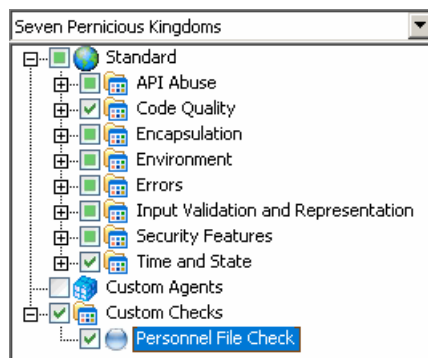
8. **次へ(Next)]**をクリックします。



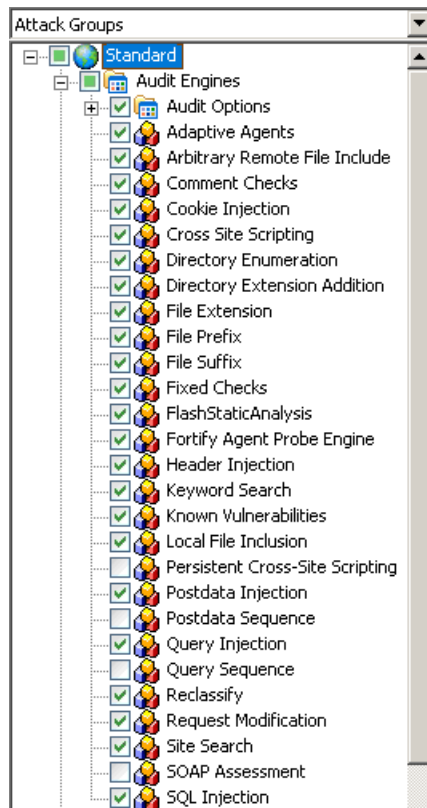
9. **レポートの情報 (Report Information)]** パネルで各タブをクリックし、説明として表示するテキストを入力します。
10. **確認のタイプ(Check Type)]** リストから項目を選択します。
11. **重大度(Severity)]** リストから重大度レベルを選択します。
12. **完了(Finish)]** をクリックします。
13. デフォルト名「New Custom Check」を、チェックの目的が分かる名前に変更します。



14. カスタムチェックが有効になっている(チェックマークが付いている)ことを確認します。



15. ドロップダウンリストから **攻撃グループ(Attack Groups)]**を選択し、をクリックして **監査エンジン(Audit Engines)]** フォルダを展開します。



16. 次の表を参照し、作成したチェックのタイプに対して適切な監査エンジンが有効になっている(チェックマークが付いている)ことを確認します。

攻撃のタイプ...	使用する監査エンジン...
ディレクトリ列挙(Directory Enumeration)	ディレクトリ列挙(Directory Enumeration)
ファイル拡張子の追加(File Extension Addition)	ファイル拡張子(File Extension)
ファイル拡張子の置換(File Extension Replacement)	ファイル拡張子(File Extension)
キーワード検索(Keyword Search)	キーワード検索(Keyword Search)
パラメータインジェクション(Parameter Injection)	Postデータインジェクション(Post Data Injection)
単純攻撃(Simple Attack)	固定チェック(Fixed Checks)
サイト検索(Site Search)	サイト検索(Site Search)

17. **ファイル(File)] > 保存(Save)]**の順に選択します。
18. 新しいポリシーの名前を入力して、**保存(Save)]**をクリックします。
OpenText DASTがすべてのカスタムチェックをすべてのポリシーに追加します。ただし、有効にはしません。他のポリシーでカスタムチェックを有効にするには、"[ポリシーの作成または編集](#)" [ページ65](#)を参照してください。

カスタムチェックの有効化

カスタムチェックを無効にするには:

1. カスタムチェックを選択します。
2. それに関連付けられたチェックボックスをオフにします。

カスタムチェックの削除

カスタムチェックを削除するには:

注意! {/b}ポリシーからカスタムチェックを削除すると、そのチェックがすべてのポリシーとシステム全体から削除されます。

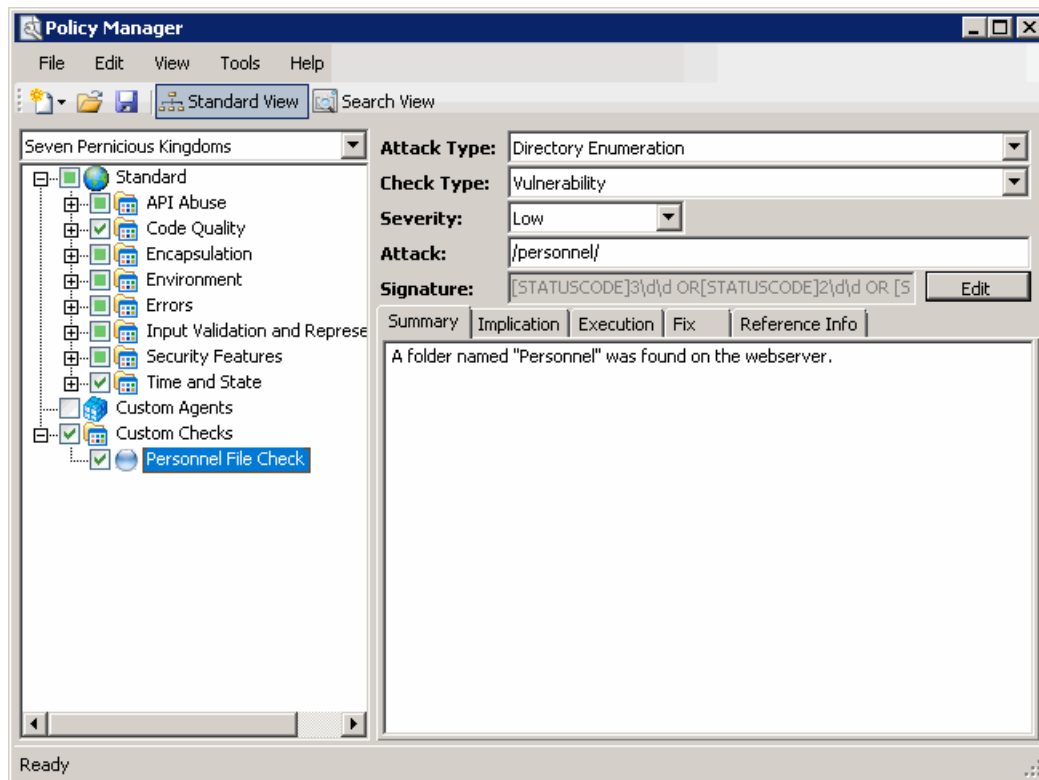
1. カスタムチェックを右クリックします。
2. ショートカットメニューから **削除(Delete)]**を選択します。

カスタムチェックの編集

カスタムチェックを編集するには:

1. ポリシーを開きます。
2. カスタムチェックを選択します。

3. Policy Managerの右 ペインで、カスタムチェックのプロパティを変更します。



4. 保存(Save)] アイコンをクリックします。

参照情報

["正規表現" ページ97](#)

["正規表現の拡張" ページ99](#)

特定のエージェントの検索

特定の脆弱性チェック(攻撃エージェント)を検索するには、Policy Managerの 検索(Search)]ビューを使用します。その後、個々のエージェントを含めるか除外するかを選択できます。

攻撃エージェントを検索するには:

1. ツールバーで、[Policy Manager] をクリックします。
- または -
[ツール(Tools)] > [Policy Manager] の順に選択します。
2. ポリシーを選択していない場合は、[ポリシーを開く(Open Policy)] ウィンドウからポリシーを選択し、[OK] をクリックします。
3. 表示(View)] > 検索(Search)] の順に選択します。

すべての攻撃エージェントの説明に、概要、意味、実行、推奨、修復などの「レポートフィールド」が含まれています。検索機能を使用すると、選択したレポートフィールドで指定したテキストを含む攻撃エージェントを検索できます。

4. **基準(Criteria)]**リストから、検索するレポートフィールドを選択します。
5. ドロップダウンリストから演算子を選択します(等しい(is)]、 より大きい(is greater than)]、 より小さい(is greater than)]、 含む(contains)])。
6. テキストボックスに、検索するテキストまたは数字を入力します。
7. **検索(Search)]**をクリックします。
8. Policy Managerの **チェック(Checks)]**エリアに、検索条件と一致するすべての攻撃エージェントがリストされます。アクティブなエージェントの名前の横には、チェックマークが付いています。チェックボックスをオン(またはオフ)にすることで、エージェントをアクティブ(または非アクティブ)にすることができます。
9. **保存(Save)]**をクリックして、変更したポリシーを保存します。

カスタムエージェントの使用

OpenText DASTの監査拡張機能は、組織内のソフトウェア開発者が開発し、カスタムエージェントとしてSecureBaseに公開します。これらは、ポリシーで有効にしてスキャンの実行に使用することができます。Policy Managerでカスタムエージェントを有効にするには:

1. 次のいずれかを実行します。
 - カスタムエージェントチェックのみを含む新しいポリシーを作成するには、 **ファイル(File)] > 新規(New)] > 空のポリシー(Blank Policy)]**の順に選択して、ステップ2に進みます。
 - カスタムエージェントチェックを、既存のポリシー内の他のチェックと一緒に有効にする場合は、ステップ2に進みます。
2. ドロップダウンリストから、 **1つの有害な界]**を選択します。
3. **カスタムエージェント(Custom Agents)]**グループを開きます。
4. リストからカスタムエージェントを選択します。
5. **ファイル(File)] > 保存(Save)]**の順に選択します。

スキャンを実行するときに、有効にしたカスタムエージェントチェックを含むポリシーを選択します。

注記: 開発者が拡張機能を再公開した場合は、Policy Managerを閉じてから再度開いて、改訂されたカスタムエージェントを取得する必要があります。

手法

Webアプリケーションには、Webサイトを作成するコードだけではなく、Webサイトを一般に公開して役立つものにするために必要なアーキテクチャコンポーネントも含まれます。Webアプリ

セッションのセキュリティを検討するときは、世界に公開されている部分だけではなく、Webサイトを成り立たせるために協働するすべてのコンポーネントを考慮しなければなりません。

OpenText DASTはWebアプリケーションを分析して潜在的なセキュリティ上の欠陥を特定し、許可されていないユーザがそれらを悪用できるようになる前に、セキュリティの問題を解決するために必要な最新の情報を提供します。Webのような変化し続けるダイナミックな環境では、常に最新のセキュリティツールを使用することが絶対的に必要です。この点を意識し、OpenTextの設計チームは、ソフトウェアが使用されるたびに、成功した既知のハッキング手法を記録した組み込みのナレッジベースが自動更新されるように設計しました。更新の後、ソフトウェアはテスト対象のアプリケーションに対してそれらのハッキング手法をエミュレートします。ナレッジベースは、OpenTextのセキュリティの専門家だけではなく、さまざまなサードパーティの大手のセキュリティ組織やアナリストから広く収集されています。

新しい攻撃手法が検出されると、OpenTextはSecureBase™脆弱性データベースをその日のうちにアップグレードします。以下は、Webアプリケーションのセキュリティ上の脆弱性を評価するときにOpenText DASTが使用する主な手法です。

パラメータ操作

パラメータ操作では、URLパラメータを改ざんして、ユーザが通常なら利用できない情報を取得します。パラメータ操作では、パラメータ名および/または引数を変更、追加、または削除します。基本的に、どんな入力でも変更可能です。パラメータ操作攻撃は、Webルートの上のファイルの開示、データベースからの情報の抽出、および任意のオペレーティングシステムレベルコマンドの実行など、いくつかの目的の達成のために使用できます。この手法は以下に対して適用されます。

- **クエリ文字列。** Webアプリケーションでは、クライアントとサーバの間でデータを受け渡しする簡単な方法としてクエリ文字列がよく使われます。クエリ文字列は、ハイパーリンクにデータ呼び出しを追加し、リンク先のページが表示されたときにその情報を取得するための方法です。攻撃者はクエリ文字列を操作して、容易にデータベースから情報を盗んだり、Webアプリケーションのアーキテクチャの詳細を入手したり、Webサーバ上でコマンドを実行したりする可能性があります。OpenText DASTは監査を行う際、高度なクエリ文字列操作を実装してサーバでのコマンドの実行の実現性を確認し、クエリ文字列操作に対するWebアプリケーションの脆弱性を判定します。
- **Postデータ。** クエリ文字列の操作は、ブラウザのアドレスバーにテキストを入力するように簡単にできるため、多くのWebアプリケーションでは、GETではなく、フォームとPOSTメソッドを組み合わせることで使用することによって、ページ間でのデータの受け渡しを行っています。通常、ブラウザではPOSTデータが表示されないため、一部のプログラマは、データの変更は困難または不可能だと思い込んでいますが、実際は逆です。OpenText DASTは、パラメータ操作のPOSTメソッドを利用した攻撃に対するアプリケーションの脆弱性を判定します。
- **ヘッダ。** HTTP要求と応答では、HTTPメッセージに関する情報の引き渡しにヘッダが使用されます。多くのWebアプリケーションはトラフィックの統計情報を収集するために「referrer」や「user-agent」などのヘッダをデータベースにログ記録しているにもかかわらず、HTTPヘッダを入力エリアであると見なしていない開発者もいます。OpenText DASTは監査の際にヘッダ情報を傍受してさまざまなパラメータ値を受け渡すを試みます。
- **クッキー。** 多くのWebアプリケーションはクッキーを使用して、ユーザIDやタイムスタンプなどの情報をクライアントのマシンに保存します。悪意のあるユーザは、これらの値を変更したり、

クッキーを「ポイズニング」したりすることで、他のユーザのアカウントや情報にアクセスする可能性があります。また、攻撃者がユーザのクッキーを盗み、IDとパスワードの入力などの認証をバイパスして、ユーザのアカウントに直接アクセスすることもあります。OpenText DASTはスキャン中に検出されたすべてのクッキーをリストし、監査時にそれらのパラメータの変更を試みます。

パラメータ操作は、次のセクションで説明するような、いくつかのサブカテゴリに分けられます。

パラメータインジェクション(Parameter injection)

パラメータインジェクション攻撃では、引数値が攻撃文字列に置き換えられます。

例:

「`http://www.site.com/webapp.asp?ValidParameter=ValidArgument`」を
「`http://www.site.com/webapp.asp?ValidParameter=AttackString`」に変更します

URLに関連するパラメータを操作しようとするこうした試みは、通常は次のような攻撃につながります。

コマンド実行(Command execution)

コマンド実行攻撃の文字列は、特殊文字とオペレーティングシステムレベルコマンドの組み合わせで構成されます。Webアプリケーションが事前に特殊文字を解析せずにこの文字列をオペレーティングシステムコマンドの呼び出しで使用すると、この文字列のオペレーティングシステムレベルコマンドが実行されます。

例: `;&id;`。

OpenText DASTはIDコマンドなどの害のないコマンドを送信して、攻撃者によってコマンドが挿入されて実行される可能性を確認します。

SQLインジェクション

SQLインジェクションとは、開発者が意図していないSQLコードをアプリケーションに渡す動作です。これらの攻撃文字列はSQL構文の断片から構成されており、WebアプリケーションがSQLステートメントを作成する際に事前に特定の文字を解析することなくこの文字列を使用すると、そのSQL構文の断片がデータベースサーバで実行されます。

例: `'+(SELECT TOP 1 name FROM sysobjects WHERE 1=1)+'`

SQL文字列を閉じてユーザに想定外のシステムとアプリケーションのアクセス権を与えるおそれがある、アポストロフィ(')などの悪意がある可能性がある入力に対する保護対策を開発者が講じていないと、問題が発生することがあります。

クロスサイトスクリプティング

この問題は、ダイナミックに生成されたWebページに、正しく検証されない入力が表示されている場合に発生します。この場合、攻撃者は生成されたそのページに悪意のあるJavaScriptを埋め込み、悪意のあるそのページを閲覧した任意のユーザのマシンでスクリプトを実行することができます。ユーザがテキストメッセージを投稿できるサイトは、このような攻撃に対して脆弱な可能性があります。この脆弱性は、以下でよく見られます。

- 入力された検索キーワードを繰り返す検索エンジン
- エラーを含む文字列を繰り返すエラーメッセージ
- 値が後でユーザに表示される入力フォーム
- ユーザが独自のメッセージを投稿できるWebメッセージボード。

攻撃者がクロスサイトスクリプティングに成功すると、機密情報が侵害されたり、クッキーが操作または窃取されたり、有効なユーザのものと間違えられる可能性がある要求が作成されたり、悪意のあるコードがユーザのシステムで実行されたりするおそれがあります。

異常入力 (Abnormal Input)

異常入力攻撃の文字列は、予期しない入力が解析されないWebアプリケーションにおいて未処理例外 (プログラムが処理できないエラー) を引き起こす可能性がある文字で構成されます。多くの場合、未処理例外が起きると、アプリケーションの内部メカニズムに関する機密情報を開示するエラーメッセージが表示されます。ソースコードも開示される場合があります。

例: %00

パラメータオーバーフロー

パラメータオーバーフロー攻撃では、パラメータまたはクッキーヘッダの引数またはパラメータ名の形式でWebアプリケーションに大量のデータが送信されます。Webアプリケーションが予期しない大量のデータを適切に処理できるようにプログラムされていない場合は、任意のオペレーティングシステムレベルコードが実行されたり、サービス拒否状態が引き起こされたりする可能性があります。

バッファのオーバーフロー

バッファのオーバーフロー攻撃は、任意のオペレーティングシステムコマンドを実行するために使用される可能性があります。OpenText DASTはバッファのオーバーフロー攻撃に対して脆弱かどうかを判定し、バッファのオーバーフローの脆弱性を修正するための詳細情報を提供します。

例:

`http://www.site.com/webapp.asp?ValidParameter=ValidArgument`

が次のように変更されます。

`http://www.site.com/webapp.asp?XXXXXXXXXXXXXXXXXXXX さらに数千個の文字]XXX=ValidArgument`

次のように変更される場合もあります。

`http://www.site.com/webapp.asp?ValidParameter=XXXXXXXXXXXXXXXXXXXX さらに数千個の文字]XXX`

パラメータ追加

パラメータ追加攻撃では、制限されている、または文書化されていないアプリケーション機能にアクセスしたり、内部のアプリケーション設定を操作したりするために、HTTP要求に新しいパ

ラメータ(admin=trueなど)が挿入されます。

アプリケーションデバッグまたはバックドアモードのパラメータ

アプリケーションデバッグ/バックドアモードのパラメータは、品質保証のためにプログラマによって追加された、文書化されていないアプリケーション機能であることが多いものです。デバッグモードやバックドアモードにアクセスされると、Webアプリケーションの内部メカニズムや管理制御にも関わる機密情報が漏えいする可能性があります。

例:

`http://www.site.com/webapp.asp?ValidParameter=ValidArgument&debug=true`

パス操作

パス操作攻撃では、Webルートの上のファイルへのアクセス、権限付与設定のバイパス、ディレクトリ一覧の表示、またはファイルソースの表示のために、HTTP要求のRequest-URIセクションが工作または変更されます。パス操作の手法には、次のようなものがあります。

パスの切り捨て

パスの切り捨て攻撃は、ファイル名がない既知のディレクトリを求める要求です。これにより、ディレクトリ一覧が表示される場合があります。OpenText DASTはパスの切り捨てを実行し、その際にディレクトリの一覧が表示されたり、異常なエラーが発生したりしないかを確認します。

例:

リンクに「`http://www.site.com/folder1/folder2/file.asp`」が含まれる場合、パスを切り捨てて「`http://www.site.com/folder1/folder2/`」や「`http://www.site.com/folder1/`」の検索を行うと、Webサーバがディレクトリの内容を開示したり、未処理例外が発生したりします。

文字エンコーディング

文字エンコーディング攻撃では、既知のリソースに対する要求の中の文字が、それと同等のエンコードされた文字に置き換えられます。Webアプリケーションが、エンコードされた文字を事前に解析せずに、権限付与や処理の目的で、そのエンコードされたURIを使用して文字列比較を実行すると、権限付与の設定が無効になったり、ソースコードが漏えいしたりする可能性があります。OpenText DASTはエンコードされたさまざまな文字列を送信して、Webアプリケーションが特殊文字を正しく解析するかどうかを確認します。OpenText DASTが文字エンコーディングテストを実行するとき、対象となるのは以下の要素です。

- **Unicode:** Unicode Worldwide Character Standardでは、世界のすべての主要な記述言語の文字、数字、特殊文字、句読点、および技術記号を、統一されたエンコーディングスキームを使用して定義しています。OpenText DASTは同等のUnicode文字列に変換された文字列を送信し、この操作を通して不正に認証資格情報を取得することを試みます。
- **16進コーディング:** これは、文字を同等の16進数文字に置き換えることです。OpenText DASTは16進エンコーディングされた文字列を送信し、この操作を通して不正に認証資格情報を取得することを試みます。

MS-DOS 8.3の短いファイル名

MS-DOS 8.3の短いファイル名攻撃では、ファイル名がMS-DOS 8.3形式(1から8文字。これに対し、最近のWindowsバージョンでのファイル名の文字制限は225文字)に変換されます。

Webアプリケーションが、権限付与や処理の目的で、事前にFAT32/NTFS形式への変換を行わずにそのMS-DOS 8.3形式のファイル名を使用して文字列比較を実行すると、権限付与の設定が無効になったり、ソースコードが漏えいしたりする可能性があります。

例:「longfilename.asp」は「longfi~1.asp」になります

ディレクトリトラバーサル

ディレクトリトラバーサル攻撃は、URIに含められた式です。Webアプリケーションが事前にトラバーサル文字を十分に解析せずにこの文字列を使用してファイルの場所を指定すると、その式によって、Webルートの上のファイルの内容をWebサーバが表示します。

例: ../../../../boot.ini

文字の削除

文字の削除攻撃では、サーバまたはアプリケーションが解析する可能性があるURIに特殊文字が追加されます。サーバまたはアプリケーションが、権限付与または要求処理のために、事前に特殊文字を取り除かずにそのURIを使用して文字列比較を行うと、権限付与の設定が無効になったり、ソースコードが漏えいしたりする可能性があります。

文字の追加

文字の追加攻撃では、ファイル名またはディレクトリ名の末尾に特殊文字が追加されます。

例:「file.asp」が「file.asp%00」にされます

サイト検索 (Site search)

これは、情報収集の段階と考えられ、不正侵入者が攻撃を開始する前にWebアプリケーションについてできるだけ多くのことを知ろうとしていることを示します。サイト検索は、Webユーザに閲覧させることは意図されていないドキュメント、アプリケーション、およびディレクトリなどのサーバ上のリソースを検索するために使用されます。このようなリソースが開示されると、機密データ、内部のサーバとアプリケーションの環境設定やその他の設定に関する情報、サイトへの管理アクセス情報、およびアプリケーションのソースコードの情報が漏えいする可能性があります。OpenText DASTはWebアプリケーションのユーザが、特に以下を利用できるかどうかを判定します。

- テストファイルとサンプルファイル: これらのファイルには、攻撃を実行するために利用できる情報が含まれていることがよくあります。たとえば、サーバ上に残されている認証済みのテストスクリプトから、サイトの機密の領域が攻撃者に知られる可能性があります。
- 管理インタフェース: これは、ネットワーク管理者がリモート保守を実施するためにネットワーク上によく配置するアプリケーションです。
- アプリケーションデータ: データベース内の情報や、他の方法でページからページに受け渡されるデータがこれに該当します。
- プログラムダンプ: プログラムは多くの場合、途中で終了するとサーバ上にダンプファイルを残します。攻撃者はしばしば、さまざまな方法でアプリケーションを中断させて、ダンプファイルから重要な情報を取得しようとします。
- アプリケーションログ: いくつかのソフトウェアアプリケーションは、製品のインストールの詳細情報が含まれたデフォルトアプリケーションログを残します。アプリケーションログには、Webアプ

リケーションのアーキテクチャに関する重要な情報(隠し領域の場所など)が示されている場合があります。

- **インストールドキュメント:**一部のソフトウェアパッケージは、構成情報を記載したデフォルトインストールドキュメントをサーバ上に残します。
- **バックアップファイル:**ネットワーク管理者と開発者は、バックアップのファイルやスクリプトをWebサーバに残すことがよくあります。サイトのセキュリティを侵害するために使用できる情報がこれらのファイルに含まれていることも珍しくありません。バックアップファイル検索では、ファイルの拡張子を置き換えて、サイトに保存されている古いバージョンやバックアップバージョンを検索します。たとえば、hi.aspを見つけた攻撃者は、hi.oldやhi.backを検索してそのスクリプトのソースコードを取得する可能性があります。
- **サイトの統計情報ページ:**これらのページでは、サイトの閲覧者に関する情報を知ることができます。しかしその情報は、攻撃者が攻撃の企てに利用する可能性がある、サイトの他の領域の場所などの情報も明らかにしている場合があります。

アプリケーションマッピング

OpenText DASTはサイト上にあるすべての既知および不明のリンクを検出して、それらをたどります。これにより、脆弱性チェックとアプリケーションテストのためのベースラインが作成されます。

Web探索

Webアプリケーションのセキュリティ上の脆弱性を検出する際に最も重要な要素の1つは、その内部構造のマッピングです。Web探索では、サイトのツリー構造全体がマッピングされます。基本的に、Web探索は、URL上のリンクがそれ以上たどれなくなるまで続けられます。

自動フォーム入力

Web探索中に見つかるすべてのフォームに対して(たとえば、ページで電話番号の入力を求められた場合などに)データを自動的に送信するように、OpenText DASTを設定することができます。

SSLのサポート

OpenText DASTはSSLを使用するすべてのサイトをWeb探索し、データが適切に暗号化され、保護されているかどうかを判定できます。

プロキシのサポート

プロキシサーバは、ネットワークセキュリティを確保し、適切なキャッシュ機能を提供し、管理制御を適正に実施するために使用できます。OpenText DASTはプロキシサーバを使用するサイトをWeb探索し、その環境設定に特に関連する脆弱性をチェックできます。

クライアント証明書サポート

証明書とは、個人の身元やWebサイトのセキュリティを立証するステートメントです。攻撃者は、Webアプリケーションに不正にアクセスするために、クライアント証明書の値を変更しようとします。

状態管理

状態とは、接続のプロパティです。HTTPはステートレスプロトコルです。HTTPでは、クライアントとサーバの通信を処理するときに、セッションの状態の概念が保持されません。OpenText DASTは、Webアプリケーションで使用されているクッキーは安全か(期限が設定されていて、適切に処理されているかなど)、またセッションIDは安全に管理されているかを判定します。

ディレクトリ列挙(Directory enumeration)

ディレクトリ列挙では、機密情報を含んでいる可能性のある隠しディレクトリも含め、アプリケーションサーバ上のすべてのディレクトリパスとその可能性のあるものがリストされます。OpenText DASTはディレクトリ列挙リストを作成する際、既知のフォルダ(admin、test、logs など)とWeb探索中に見つかる隠し領域のデータベースを使用します。

Webサーバの評価

OpenText DASTはWebサーバを評価するときに、サイト検索で収集された情報や他の応用的手法を活用して、専有のWebサーバの脆弱性をテストします。プロトコルと拡張機能の実装分析を使用して、サーバが提供するサービスの内容、そのサービスがそのサービスに関して確立されている標準に準拠しているかどうか、およびそのサービスの実装の詳細を判定します。コンテンツの提供とアプリケーションの起動はWebサーバの設定に基づいて行われるため、未保護の専有Webサーバが攻撃を受けた場合は、損害として、サービス拒否、サイトへの不適切なメッセージや画像の投稿、ファイルの削除、および損害を与えるコードやソフトウェアパッケージがサーバに残されることが考えられます。

HTTPコンプライアンス

HTTPコンプライアンステストでは、WebサーバまたはプロキシサーバがHTTP/1.0およびHTTP/1.1の規則に適切に準拠しているかどうかの評価されます。このテストでは、指定されているバッファ長を超えるデータを送信する(バッファオーバーフロー)などの攻撃が実行されます。正常な要求内には見られないヘッダを各種の手法と組み合わせてサーバをテストし、サーバがデータを適切にサニタイズするかどうかを確認して、Webサーバが要求を適切に処理するかどうかを判定します。これらの攻撃によって、WebサーバまたはWebデバイスがHTTPの仕様に準拠しているかどうかを判別でき、未知の脆弱性が発見される場合もあります。

WebDAVコンプライアンス

WebDAVを使用すると、ユーザはWebサーバ上のディレクトリにファイルを配置したり、ファイルを操作したりできます。OpenText DASTはWebサーバ上でWebDAV特権を超える行為が可能かどうか、またこの特権を操作することが可能かどうかを判定します。

SSL強度

SSL強度判定では、Webサーバが受け入れる暗号化レベルを判定します。これは、セキュアクライアントが期待されている基準より低い暗号化レベルで接続することがないようにするため、またデータを適切に暗号化してデータ傍受を防ぐために重要となります。

証明書分析

OpenText DASTはSSL証明書を分析して、不明なCA証明書の分析や期限切れなどの不適切なプロパティを検出します。

HTTPメソッドのサポート

OpenText DASTはWebサーバがサポートするHTTPメソッドを判定します。

たとえば、GET、PUT、INDEX、POST、CONNECTなどをWebサーバがサポートするかどうかを判定します。

コンテンツ調査

コンテンツ調査では、サイト検索中に検出されたコンテンツを検索して、非公開であるべきにもかかわらずWebアプリケーションのユーザが利用できるようになっている情報を検出します。OpenText DASTはコンテンツ調査を行うとき、次の項目(ただし、これがすべてではない)を検索して、各項目の潜在的な悪用レベルを判定します。

スパムゲートウェイ検出

スパムゲートウェイは、クライアントが非表示のフォーム入力またはパラメータを介して電子メール受信者の場所を指定できる電子メールWebアプリケーションです。

クライアント側価格設定

クライアント側価格設定とは、クライアントが非表示のフォーム入力またはパラメータを介して項目の価格設定を指定できてしまうというWebアプリケーションの欠陥です。

開発者の機密コメント

HTMLの中の開発者のコメントは、アプリケーションの内部メカニズムと設定に関する機密情報を示していることがよくあります。たとえば、テーブル内のフィールドの必須の順序についてのコメント、といった一見無害な情報が、サイトのセキュリティを破るのに必要となる重大な情報を攻撃者に与えてしまうことがあります。OpenText DASTはサイトのコード内で見つかったすべてのコメントを、情報ペインの [コメント (Comments)] エリアに一覧にします。

WebサーバとWebパッケージの識別

OpenText DASTはWebサーバ上のすべてのサービスとバナーを識別し、Webアプリケーションが使用するすべてのソフトウェアパッケージのベンダーとバージョン番号を確認します。次のさまざまな手段を用いて、それを行います。

- ヘッダの証拠-たとえば、Server: Microsoft-IIS/5.0
- リンクの証拠-たとえば、は、PHP Webアプリケーションサーバが実行されていることを示します。
- デフォルト/テンプレートページの証拠-たとえば、「これが表示されれば、このシステムへのApache Web Serverソフトウェアのインストールが成功していることになる」と言えるページなど。

絶対パスの検出

OpenText DASTは、アプリケーション内のどこかで完全修飾パス名が見つかったかどうかを検知します。一部の脆弱性は、攻撃者が完全修飾パス名を入手した場合にのみ、悪用される可能性があります。

例: /opt/Web/docroot/、c:\inetpub\wwwroot"

エラーメッセージの識別

エラーメッセージは、それが本来明らかにするはずの情報以外の情報を明らかにすることがあります。たとえば、/servletimages/logo2circle.gifを含むページは、デフォルトテンプレートのBEA WebLogicエラーのページです。このことを知っている攻撃者は、そのサーバ固有の脆弱性を利用するために自分の攻撃をカスタマイズすることができます。

パーミッションの評価

OpenText DASTはWebアプリケーションのさまざまな領域で使用可能になっている許可レベル(Webサーバへのファイルのアップロード、データの編集、ディレクトリ間の移動など)を判定し、それに特有のセキュリティ脆弱性を改善する最善の方法を決定します。

総当たり認証攻撃

総当たり攻撃は、辞書攻撃(よく使用されるログオンとパスワードを含んだファイル)に対する脆弱性を明らかにします。OpenText DASTは基本認証、NTLM認証、およびWebフォーム認証を検査して、総当たり攻撃に対する脆弱性を調べます。

既知の攻撃

既知の攻撃には、公開や投稿などによって周知されている、Webサーバ、アプリケーション、およびその他のサードパーティコンポーネントにある悪用可能なすべてのセキュリティホールやバグが含まれます。これらの脆弱性のほとんどには対応するパッチが存在しますが、ハッカーはパッチがしかるべき時期にインストールされていないシステムを利用しようとします。既知の攻撃の情報は、他のすべての手法に取り入れられています。

OpenText DASTはWorld Wide Webの誕生以降に出現した既知の攻撃の指紋を含む独自のデータベースを利用しています。WebInspectチームは、実行のたびに新しいリスクやエクスプロイトをチェックしてダウンロードし、製品を常に最新かつハッキング技術の最先端を行く状態に保っています。

ポリシー

各ポリシーはスマートアップデート機能により最新の状態に保たれ、最近発見された脅威のほとんどを正確に検出できるようになっています。OpenText DAST(またはセンサ)には、パッケージ化された以下のポリシーが含まれています。スキャンおよびWeb探索では、これらのポリシーを使用して、Webアプリケーションの脆弱性を判定できます。

注記: このリストは、製品に表示されるポリシーと一致しないことがあります。このドキュメントの執筆後にSmartUpdateによって追加または非推奨にされたポリシーが存在する場合があります。

OAST関連チェックについて

インターネットにアクセス可能なネットワークでは、OpenText DASTはOAST関連チェックの実行時にパブリックDNSサービスを使用します。ファイアウォールがfortify-oast.netへのアクセスをブロックしないことを確認してください。インターネットにアクセスできないネットワークでは、Fortify OAST on Dockerイメージを使用できます。詳細については、『*OpenText™ Dynamic Application Security Testing*および*OAST on Docker*ユーザガイド』を参照してください。

ベストプラクティス

ベストプラクティスグループには、Webアプリケーションに最も広く見られる厄介なセキュリティ上の脆弱性についてアプリケーションをテストするためのポリシーが含まれています。

- **API:** このポリシーには、APIセキュリティ評価に関連するさまざまな問題を対象としたチェックが含まれています。これには、各種のインジェクション攻撃、トランスポート層セキュリティ、およびプライバシー侵害が含まれますが、クライアントサイドの問題の検出のチェックや攻撃露呈部分の検出(ディレクトリ列挙やバックアップファイル検索のチェックなど)は含まれません。このポリシーによって検出される脆弱性はすべて、攻撃者から直接攻撃の的とされる可能性があります。このポリシーは、Web APIを使用するアプリケーションをスキャンするためのものではありません。
- **CWE Top 25 <バージョン>:** Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Errors (CWE Top 25)は、MITREが作成したリストです。このリストは、ソフトウェアの脆弱性につながるおそれのある、まん延の度合いと重大性が最も高いソフトウェアの弱点を示しています。
- **DISA STIG <バージョン>:** Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG)には、アプリケーションの開発過程全体に関するセキュリティガイダンスがあります。このポリシーには、DISA STIG <バージョン>の安全なコーディングの要件をアプリケーションが満たすために役立つ選定されたチェックが含まれます。ベストプラクティスグループ内には、DISA STIGポリシーの複数のバージョンが存在する場合があります。
- **General Data Protection Regulation (GDPR):** EU一般データ保護規則(GDPR、General Data Protection Regulation)は、データ保護指令95/46/ECに代わるものとして、組織が個人データを取り扱うための枠組みを提供しています。以下に挙げるGDPR条項は、アプリケーションセキュリティに関連しており、製品およびサービスの設計および開発中に個人データを保護することを企業に義務付けています。
 - 第25条「データ保護バイデザインおよびデータ保護バイデフォルト」。この条項により、企業は、各特定の処理の目的に必要な個人データのみを取り扱うことをデフォルトで保証するために、適切な技術的および組織的な手段を講じる必要があります。
 - 第32条「取り扱いの安全性」。この条項により、企業は、個人データの偶発的または不法な破壊、損失、改変、不正開示、または不正アクセスからシステムおよびアプリケーションを保護する必要があります。

このポリシーには、特にGDPRのアプリケーションセキュリティに関連して個人データを特定および保護する上で役立つチェックが精選されています。

- **NIST-SP80053R5:** NIST Special Publication 800-53 Revision 5 (NIST SP 800-53 Rev.5)には、米国連邦政府の機関および情報システムをセキュリティ上の脅威から保護することを目的とするセキュリティ制御およびプライバシー制御のリストが指定されています。このポリシーには、NIST SP 800-53 Rev.5のガイドラインと規格を満たすために監査に含める必要がある選定されたチェックが含まれています。
- **OWASP API Top 10 <年>:** OWASP API Top 10 <年>は、特定の年の、APIに影響する上位のセキュリティリスクのリストを提供します。このリストは、APIセキュリティの脆弱性に関する認識を高め、WEB APIのセキュリティを確保する必要がある開発者、設計者、アーキテクト、マネージャ、組織などの、APIの開発および保守に関与する人々を教育することを目的としています。OWASP API Top 10は、Web APIに影響を与える脆弱性に焦点を当てており、単独での使用を目的としていません。むしろ、他の標準やベストプラクティスと組み合わせることで、関連するすべてのリスクを包括的に捕捉することを目的としています。たとえば、インジェクションなどの入力検証に関連する問題を特定するには、これをOWASP Top 10と組み合わせる必要があります。
- **OWASP Application Security Verification Standard (ASVS):** Application Security Verification Standard (ASVS)は、設計者、開発者、テスト担当者、セキュリティ専門家、ツールベンダー、およびコンシューマが安全なアプリケーションを定義、作成、テスト、および検証するために使用できる、アプリケーションのセキュリティ要件またはセキュリティテストのリストです。
このポリシーは、組み込むSecureBaseチェックの各カテゴリに、OWASP ASVSが提示するCWEマッピングを使用しています。CWEは階層的な分類であるため、このポリシーには、「ParentOf」関係を使用してOWASP ASVSが提示するCWEから暗黙的に指定される追加のCWEにマップするチェックも含まれています。
- **OWASP Top 10 <年>:** このポリシーは、Webアプリケーションセキュリティの最低限の基準を提供します。OWASP Top 10は、Webアプリケーションの最も重大なセキュリティ上の欠陥についての幅広いコンセンサスを表します。OWASP Top 10の採用は、おそらく、組織内のソフトウェア開発文化を安全なコードを生み出す文化へと変化させるための最も効果的な最初のステップと言えます。OWASP Top 10のポリシーには、複数のリリースが存在する場合があります。詳細については、「[OWASP Top Ten Project](#)」を参照してください。
- **SANS Top 25<年>:** SANS Top 25 Most Dangerous Software Errorsでは、ソフトウェアの深刻な脆弱性を引き起こす最も広く見られる重大なエラーをCWE (Common Weakness Enumeration) ID別に分類して列挙しています。多くの場合、これらのソフトウェアエラーは見つけるのも悪用するのも簡単です。これらのエラーにつきものの危険としては、攻撃者がソフトウェアを完全に乗っ取ったり、データを盗んだり、ソフトウェアを完全に停止させたりできるということがあります。
- **標準:** 標準スキャンは、サーバの自動Web探索を含んでおり、SQLインジェクションやクロスサイトスクリプトなどの既知と未知の脆弱性のチェックのほか、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層での不適切なエラー処理や脆弱なSSL設定についてのチェックを実行します。

タイプ別

タイプ別グループには、特定のアプリケーション層、脆弱性の種類、または汎用機能に焦点を絞って設計されたポリシーが含まれます。たとえば、アプリケーションポリシーには、オペレーティ

ングシステムではなくアプリケーションをテストする目的で設計されたすべてのチェックが含まれます。

- **積極的なSQLインジェクション:** このポリシーは、SQLインジェクションの脆弱性に対するWebアプリケーションのセキュリティを総合的に評価します。SQLインジェクションとは、入力が検証されないという脆弱性を利用してWebアプリケーションから任意のSQLクエリやコマンドを渡し、バックエンドのデータベースで実行させるという攻撃手法です。このポリシーを使用すると、より正確で確実になりますが、スキャン時間は長くなります。
- **Apache Struts:** このポリシーは、Apache Strutsフレームワークに対する、サポートされている既知のアドバイザリを検出します。
- **ブランク:** このポリシーは、ユーザが独自のポリシーを作成するために使用できるテンプレートです。サーバの自動クロールを含み、脆弱性チェックを行いません。このポリシーを編集して、特定の脆弱性のみをスキャンするカスタムポリシーを作成できます。
- **クライアント側:** このポリシーは、攻撃者が攻撃を仕掛けるためにフィッシングを行うことが必要となるすべての問題を検出することを目的としています。それらの問題は通常はクライアント側に現れるので、フィッシングが必要となります。これには、反射型クロスサイトスクリプティングのチェックと、さまざまなHTML5のチェックが含まれます。このポリシーをサーバ側ポリシーと組み合わせることで、クライアントとサーバの両方をカバーすることができます。 This policy intends to detect all issues that require an attacker to perform phishing in order to deliver an attack. These issues are typically manifested on the client, thus enforcing the phishing requirement. This includes Reflected Cross-site Scripting and various HTML5 checks. This policy may be used in conjunction with the Server-side policy to provide coverage across both the client and the server.
- **重大および高:** 重大および高のポリシーは、運用サーバを危険にさらすことなく、差し迫った緊急の脆弱性を検出するためにWebアプリケーションを迅速にスキャンする場合に使用します。このポリシーは、SQLインジェクションやクロスサイトスクリプティングなど、重大度が「重大」および「高」の脆弱性をチェックします。これは、データベースにデータを書き込んだり、サービス拒否状態を生じさせたりする可能性があるチェックは含んでいないため、運用サーバに対して安全に実行できます。
- **クロスサイトスクリプティング:** このポリシーは、XSS(クロスサイトスクリプティング)の脆弱性について、Webアプリケーションのセキュリティスキャンを実行します。XSSとは、攻撃者が提供した実行可能コード(HTMLコードやクライアント側スクリプトなど)をWebサイトにエコーさせて、ユーザのブラウザにそのコードをロードする攻撃手法です。このような攻撃は、アクセス制御の回避やフィッシング詐欺に利用される可能性があります。
- **DISA STIG <バージョン>:** Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG)には、アプリケーションの開発過程全体に関するセキュリティガイダンスがあります。このポリシーには、DISA STIG <バージョン>の安全なコーディングの要件をアプリケーションが満たすために役立つ選定されたチェックが含まれます。タイプ別グループには、DISA STIGポリシーの複数のバージョンが存在する場合があります。
- **モバイル:** モバイルスキャンは、モバイルアプリケーションとそれをサポートするバックエンドサービスの間で観察された通信に基づいて、セキュリティ上の欠陥を検出します。
- **NoSQLおよびNode.js:** このポリシーは、サーバの自動Web探索を含んでおり、NoSQLベースのデータベース(MongoDBなど)や、JavaScriptベースのサーバ側インフラストラクチャ(Node.jsなど)を対象にした既知と未知の脆弱性のチェックを実行します。

- **OAST:** このポリシーには、スキャンロジックでOAST (Out-of-band Application Security Testing)技術を使用するすべてのチェックが含まれています。
- **パンプスキャン:** パンプスキャンポリシーは、積極的なエクスプロイトを発生させなくても検出可能なアプリケーションの脆弱性をスキャンします。したがって、運用サーバに対しても安全に実行できます。このポリシーによって検出される脆弱性には、パスの開示の問題、エラーメッセージの問題、および類似した性質を持つその他の問題が含まれます。
- **PCI DSS <バージョン>:** Payment Card Industry Data Security Standard (PCI DSS: ペイメントカード業界データセキュリティ基準)は、顧客データを保護するために設計された技術要件と運用要件のベースラインを提供します。このポリシーには、PCI DSSの安全なコーディングの要件を満たすために監査に含める必要があるチェックが含まれています。
- **PCI Software Security Framework <バージョン> (PCI SSF <バージョン>):** PCI SSFは、安全な支払いシステムと支払いトランザクション処理ソフトウェアを作成するための要件とガイダンスのベースラインを提供します。このポリシーには、PCI SSFの安全なコーディングの要件を満たすために監査に含める必要があるチェックが含まれています。
- **権限のエスカレーション:** 権限のエスカレーションのポリシーは、攻撃者がデータやアプリケーションへの昇格されたアクセス権を獲得することを許してしまうプログラミングエラーや設計上の欠陥を検出するために、Webアプリケーションをスキャンします。このポリシーは、同一の要求をさまざまな特権レベルで実行してその応答を比較するチェックを実行します。
- **サーバ側:** このポリシーには、サーバ側アプリケーションのさまざまな問題を対象とするチェックが含まれています。これには、さまざまなインジェクション攻撃、トランスポート層のセキュリティ、およびプライバシー侵害が含まれますが、ディレクトリ列挙やバックアップファイルの検索などのアタックサーフェスの検出は含まれません。このポリシーによって検出される脆弱性はすべて、攻撃者から直接攻撃の的とされる可能性があります。このポリシーをクライアント側ポリシーと組み合わせて使用することで、クライアントとサーバの両方をカバーすることができます。 This policy contains checks that target various issues on the server-side of an application. This includes various injection attacks, transport layer security, and privacy violation, but does not include attack surface discovery such as directory enumeration or backup file search. All vulnerabilities detected by this policy may be directly targeted by an attacker. This policy may be used in conjunction with the Client-side policy to provide coverage across both the client and the server.
- **SQLインジェクション:** SQLインジェクションポリシーは、SQLインジェクションの脆弱性について、Webアプリケーションのセキュリティスキャンを実行します。SQLインジェクションとは、入力が検証されないという脆弱性を利用してWebアプリケーションから任意のSQLクエリやコマンドを渡し、バックエンドのデータベースで実行させるという攻撃手法です。
- **トランスポート層セキュリティ:** このポリシーは、安全でないSSL/TLS設定や、トランスポート層の重大なセキュリティ脆弱性(Heartbleed攻撃、Poodle攻撃、SSL再ネゴシエーション攻撃など)について、Webアプリケーションのセキュリティ評価を実行します。
- **WebSocket:** このポリシーは、アプリケーション内のWebSocket実装に関連する脆弱性を検出します。

カスタム

カスタムグループには、ユーザが作成したすべてのポリシーと、ユーザが変更したカスタムポリシーが含まれます。

危険

危険グループには、運用サーバの障害を引き起こす可能性があるサービス拒否攻撃などの危険をはらんだチェックを含んでいるポリシーが含まれます。このポリシーは、運用以外のサーバおよびシステムのみに使用してください。

- **全チェック:** 全チェックスキャンには、サーバの自動Web探索が含まれており、データベースであるSecureBaseのアクティブなすべてのチェックを実行します。このスキャンには、FortifyのWebアプリケーションとWebサービスの脆弱性のスキャンのための製品で利用可能なコンプライアンスレポートにリストされるすべてのチェックが含まれます。これには、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層での既知と未知の脆弱性のチェックが含まれます。

注意! 全チェックスキャンには、データベースにデータを書き込んだり、フォームを送信したり、サービス拒否状態を発生させたりする可能性のあるチェックが含まれています。OpenTextでは、全チェックポリシーはテスト環境でのみ使用することを強くお勧めします。

非推奨になったチェックおよびポリシー

以下のチェックとポリシーは非推奨となっており、保守されていません。

- **積極的なLog4Shell (非推奨):** このポリシーは、脆弱なバージョンのApache Log4jライブラリにおけるJNDI参照インジェクションに対するWebアプリケーションのセキュリティを総合的に評価します。脆弱なバージョンのLog4jでは、JNDI機能が制限されません。このため、ログメッセージを制御できる攻撃者は、攻撃者の制御下にあるサーバを指したJNDI参照を挿入できるようになります。これは、脆弱なターゲット上でのリモートコード実行につながりかねません。このポリシーを使用すると、Log4Shellエージェントを含むその他のポリシーと比較して、より正確で確実になりますが、多数の要求が生成されるため、スキャン時間は長くなります。
- **アプリケーション(非推奨):** アプリケーションポリシーは、既知および未知のWebアプリケーション攻撃を送信することで、Webアプリケーションのセキュリティスキャンを実行し、アプリケーション層を評価する特定の攻撃のみを送信します。エンタープライズレベルのWebアプリケーションのスキャンを実行する場合は、アプリケーションのみのポリシーをプラットフォームのみのポリシーと組み合わせて使用することで、スキャンの速度とメモリ使用量を最適化してください。
- **攻撃(非推奨):** 攻撃スキャンには、サーバの自動Web探索が含まれており、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層で既知および未知の脆弱性のチェックを実行します。アサルトスキャンには、サービス拒否状態を作り出す可能性のあるチェックが含まれます。攻撃スキャンはテスト環境でのみ使用することを強くお勧めします。
- **非推奨のチェック:** テクノロジーのライフサイクルが終わりに向かい、技術動向から姿を消していくのに従い、実質的に不要になったチェックをポリシーから削除する必要があります。非推奨のチェックポリシーには、現在の技術的状況に基づいて役目を終えたと見なされたチェッ

クや、コアOpenText DASTフレームワークの最近の拡張機能を活用するスマートで効率的な監査アルゴリズムを使用して再実装されたチェックが含まれます。








- **開発者(非推奨):** 開発者スキャンには、サーバの自動Web探索が含まれており、Webアプリケーション層に限定した既知および未知の脆弱性のチェックを実行します。このポリシーは、サービス拒否状態を引き起こす可能性のあるチェックは実行しないので、運用システムで安全に実行できます。
- **OpenSSL Heartbleed(非推奨):** このポリシーは、重大なTLSハートビート読み取りオーバーランの脆弱性について、Webアプリケーションのセキュリティ評価を実行します。この脆弱性により、悪意のあるユーザが、サイトをホストしているサーバに不正な形式のハートビート要求を送信した場合に、サーバメモリ内の重要なサーバおよびWebアプリケーションのデータが漏えいする可能性があります。
- **OWASP Top 10 Application Security Risks - 2010 (非推奨):** このポリシーは、Webアプリケーションセキュリティの最低限の基準を提供します。OWASP Top 10は、Webアプリケーションの最も重大なセキュリティ上の欠陥についての幅広いコンセンサスを表します。OWASP Top 10の採用は、おそらく、組織内のソフトウェア開発文化を安全なコードを生み出す文化へと変化させるための最も効果的な最初のステップと言えます。このポリシーには、2010 Top 10リストに固有の要素が含まれています。詳細については、「[OWASP Top Ten Project](#)」を参照してください。
- **プラットフォーム(非推奨):** このポリシーは、特にWebサーバおよび既知のWebアプリケーションに対して攻撃を送信することで、Webアプリケーションプラットフォームのセキュリティスキャンを実行します。エンタープライズレベルのWebアプリケーションのスキャンを実行する場合は、プラットフォームのみのポリシーをアプリケーションのみのポリシーと組み合わせて使用することで、スキャンの速度とメモリ使用量を最適化してください。
- **QA(非推奨):** このポリシーは、QA担当者がWebアプリケーションセキュリティの観点からプロジェクトリリースの決定を下すのに役立ちます。これは、Webアプリケーションの既知および未知の脆弱性のチェックを実行します。ただし、危険性をはらんだチェックは実行しないため、運用システムで安全に実行できます。
- **クイック(非推奨):** このスキャンには、サーバの自動Web探索が含まれており、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層で、メジャーパッケージの既知の脆弱性と未知の脆弱性のチェックを実行します。クイックスキャンは、サービス拒否状態を生じさせる可能性のあるチェックは実行しないため、運用システムで安全に実行できます。
- **セーフ(非推奨):** セーフスキャンには、サーバの自動Web探索が含まれており、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層で、メジャーパッケージの既知の脆弱性のほとんどと、未知の脆弱性のいくつかについてのチェックを実行します。セーフスキャンは、機密性の高いシステムでも、サービス拒否状態を引き起こす可能性のあるチェックは実行しません。
- **標準(非推奨):** 標準(非推奨)ポリシーは、R1 2015リリースで改訂される前のもともとの標準ポリシーと同じものです。標準スキャンには、サーバの自動Web探索が含まれており、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層で既知および未知の脆弱性のチェックを実行します。標準スキャンは、サービス拒否状態を生じさせる可能性のあるチェックは実行しないため、運用システムで安全に実行できます。

参照情報

["ポリシーマネージャ" ページ62](#)

Policy Managerのアイコン

次の表では、Policy Managerのツリービューで使用されるアイコンについて説明しています。

アイコン	定義
	ポリシー。
	攻撃グループフォルダ: 脆弱性評価を含むフォルダ。
	監査手法: 監査手法を構成するチェックのセット。たとえば、サイト検索は監査手法の一部です。手法の詳細については、 "手法" ページ76 を参照してください。
	攻撃者がサーバ上でコマンドを実行したり、個人情報を取得および変更したりできる可能性のある重大な脆弱性。
	高レベルの脆弱性。一般に、ソースコード、Webルート外のファイル、および機密性の高いエラーメッセージの表示が可能になります。
	中レベルの脆弱性。機密性が高い可能性のあるHTML以外のエラーまたは問題を示します。
	低レベルの脆弱性。注目すべき問題、またはより高いレベルの問題になる可能性のある問題を示します。

監査エンジン

OpenText DASTは以下の監査エンジンを使用します。

- **アダプティブエージェント(Adaptive Agents):** 一部の脆弱性は、その検査に大量のロジックを必要とします。たとえば、バッファオーバーフローJRunチェックは、脆弱性データベースを使用して行くと、サーバがクラッシュすることがあります。その代わりに、適切な量のロジックを使用するアダプティブエージェントを作成して、この問題を回避することができます。このスマートなアプローチにより、OpenText DASTは、特定のアプリケーション環境に合った適切な評価リソースを継続的に適用します。
- **任意のリモートファイルの組み込み(Arbitrary Remote File Include):** このエンジンは、攻撃者が提供する任意のURLからデータをフェッチして組み込む結果を招きかねない脆弱性がないかをチェックします。
- **コメントチェック(Comment Checks):** コメント監査では、コメント内にファイル名またはURLがないかを、セッションごとに検査します。ファイル名またはURLを検出すると、そのファイルまたはURLが存在するかどうかを検査します。

- **クッキーインジェクション(Cookie Injection):** クッキーおよびヘッダは、フォームのテキストフィールドと同じくらいインジェクション攻撃に対して脆弱です。クッキーインジェクションは、未検証のデータがユーザのブラウザによってクッキーの一部として送信されるときに発生します。クッキーインジェクション(Cookie Injection)監査エンジンは、さまざまなクッキー値に対して、ある従来型のパラメータインジェクション攻撃を試みます。
- **クロスサイトスクリプティング(Cross-Site Scripting):** このエンジンは、クロスサイトスクリプティングパラメータインジェクション攻撃を実行します。アプリケーションからサーバに返されるクライアント提要データを開発者が適切にフィルタ処理または検証しないと、アプリケーションはこれらの攻撃に脆弱になります。
- **ディレクトリ列挙(Directory Enumeration):** ディレクトリ列挙では、機密情報を含んでいる可能性のある隠しディレクトリを含め、アプリケーションサーバ上のすべてのディレクトリパスとその可能性のあるものが検索されます。これは、OpenText DASTがターゲットサイトの完全かつ正確なマップを作成するのに役立ちます。
- **ディレクトリ拡張子の追加(Directory Extension Addition):** ディレクトリ拡張子チェックでは、ディレクトリに拡張子を追加し、末尾のスラッシュを削除して、サーバ上に残っているアーカイブディレクトリを検索するという操作が行われます。OpenText DASTは、攻撃者に利用されるおそれがある、サーバ上に残されたすべてのディレクトリの検索を試みます。
- **ファイル拡張子(File Extension):** ネットワーク管理者や開発者は、バックアップのファイルやスクリプトをWebサーバ上に残すことがよくあります。サイトのセキュリティを侵害するために使用できる情報がこれらのファイルに含まれていることも珍しくありません。拡張子チェックでは、ファイルの拡張子を置き換えて、サイトに保存されている古いバージョンやバックアップバージョンを検索するという操作が行われます。たとえば、hi.aspを見つけた攻撃者は、hi.oldやhi.backを検索してそのスクリプトのソースコードを取得する可能性があります。OpenText DASTは、攻撃者に利用されるおそれがある、サーバ上に残されたすべてのファイルの検索を試みます。
- **ファイルプレフィックス(File Prefix):** ネットワーク管理者や開発者は、バックアップのファイルやスクリプトをWebサーバ上に残すことがよくあります。サイトのセキュリティを侵害するために使用できる情報がこれらのファイルに含まれていることも珍しくありません。プレフィックスチェックでは、ファイル名に値を追加して、サイトに保存されている古いバージョンやバックアップバージョンを検索するということが行われます。
- **ファイルサフィックス(File Suffix):** ファイルサフィックスチェックでは、ファイル名に値を追加して、サイトに保存されている古いバージョンやバックアップバージョンを検索するということが行われます。詳細については、「ファイルプレフィックス(File Prefix)」を参照してください。
- **固定チェック(Fixed Checks):** この監査は、既知の脆弱性を持つファイルのチェックを実行します。固定チェック監査は、攻撃を送信する前にディレクトリ構造をプローブしない点を除けば、ABSチェック監査と同じです。
- **FlashStaticAnalysis:** Flashソースコード分析を実行して脆弱性を検出します。
- **Fortifyエージェントプローブエンジン(Agent Probe Engine):** このエンジンは、特定のパラメータまたはインジェクションポイントが、監査入力で指定された攻撃サジェスションに対して脆弱であるかどうかを示すヒントを得るためにプローブを送信します。
- **Hacker Level Insights:** このエンジンは、DASTが従来検出している昔ながらの弱点や脆弱性の域を超えたデータを提供します。
- **ヘッダインジェクション(Header Injection):** クッキーおよびヘッダは、フォームのテキストフィールドと同じくらいインジェクション攻撃に対して脆弱です。HTTPヘッダインジェクションは、悪

意のあるコンテンツを含むユーザ入力によってHTTPヘッダがダイナミックに生成されるときに発生します。ヘッダイнジェクション監査エンジンは、さまざまなタイプのHTTPヘッダに対して、いくつかの従来型のパラメータインジェクション攻撃を試みます。

- **キーワード検索(Keyword Search):** 情報公開攻撃では、匿名ユーザに公開すべきではないシステム固有の情報や機密データ(ユーザデータを含む)をWebサイトに開示させる方法が焦点となります。キーワード検索監査エンジンは、Webサーバからのすべての応答を調べ、Webサイトによって適切に保護されていない情報(エラーメッセージ、ディレクトリ一覧、クレジットカード番号など)がないかを確認します。
- **既知の脆弱性(Known Vulnerabilities):** このエンジンは、既知の脆弱性を持つファイルがないかチェックします。この監査では、そのようなファイルが含まれていることが分かっているディレクトリを検索し、検出されたディレクトリに基づいて要求を送信します。
- **ローカルファイルインクルード(Local File Inclusion):** ローカルファイル読み込みとローカルファイルインクルージョンの脆弱性は、攻撃者がアプリケーションに影響を与えて攻撃者が指定する(おそらく任意の)ファイルをアプリケーションに読み込ませることができる場合に存在します。このエンジンは、既知の特定ファイルの相対ファイル名と絶対ファイル名のさまざまな組み合わせを含んださまざまな値をWebアプリケーションに送信します。このエンジンは、これらのファイルの内容が表示された場合、その攻撃を成功と見なします。
- **持続型クロスサイトスクリプティング(Persistent Cross-Site Scripting):** 持続型クロスサイトスクリプティング(格納型クロスサイトスクリプティングとも呼ばれる)の脆弱性をチェックするには、このエンジンを有効にする必要があります。持続型クロスサイトスクリプティングが成功すると、攻撃者がターゲットアプリケーションのクライアント側コードに悪意のあるスクリプトを挿入する可能性があります。
- **Postデータインジェクション(Postdata Injection):** クエリ文字列の操作はブラウザのアドレスバーにテキストを入力するような簡単なことであるため、多くのWebアプリケーションでは、(GETではなく)フォームとPOSTメソッドを組み合わせる使用することによって、ページ間でのデータの受け渡しを行っています。通常、ブラウザではPOSTデータが表示されないため、一部のプログラマは、データを変更することは困難または不可能だと思い込んでいますが、実際は逆です。OpenText DASTは、パラメータ操作のPOSTメソッドを利用した攻撃に対するアプリケーションの脆弱性を判定します。
- **Postデータシーケンス(Postdata Sequence):** クエリ文字列の操作は、ブラウザのアドレスバーにテキストを入力するように簡単にできるため、多くのWebアプリケーションでは、(GETではなく)フォームとPOSTメソッドを組み合わせる使用することによって、ページ間でのデータの受け渡しを行っています。通常、ブラウザではPOSTデータが表示されないため、一部のプログラマは、データを変更することは困難または不可能だと思い込んでいますが、実際は逆です。OpenText DASTは、断片化されたデータをターゲットに送信することで、パラメータ操作のPOSTメソッドを利用した攻撃に対するアプリケーションの脆弱性を判定します。
- **クエリインジェクション(Query Injection):** Webアプリケーションでは、クライアントからサーバにデータを受け渡すための簡単な方法として、クエリ文字列がよく使用されます。クエリ文字列は、ハイパーリンクにデータ呼び出しを追加し、リンク先のページが表示されたときにその情報を取得するための方法です。攻撃者はクエリ文字列を操作して、容易にデータベースから情報を盗んだり、Webアプリケーションのアーキテクチャの詳細を入手したり、Webサーバ上でコマンドを実行したりする可能性があります。

OpenText DASTは監査を行う際、高度なクエリ文字列操作を実装してサーバでのコマンドの実行の実現性を確認し、クエリ文字列操作に対するWebアプリケーションの脆弱性を判定します。

- **クエリシーケンス(Query Sequence):** Webアプリケーションでは、クライアントからサーバにデータを受け渡すための簡単な方法として、クエリ文字列がよく使用されます。クエリ文字列は、ハイパーリンクにデータ呼び出しを追加し、リンク先のページが表示されたときにその情報を取得するための方法です。攻撃者はクエリ文字列を操作して、容易にデータベースから情報を盗んだり、Webアプリケーションのアーキテクチャの詳細を入手したり、Webサーバ上でコマンドを実行したりする可能性があります。

OpenText DASTは監査を行う際、高度なクエリ文字列操作を実装してサーバでのコマンドの実行の実現性を確認し、断片化されたデータをターゲットに送信することによってクエリ文字列操作に対するWebアプリケーションの脆弱性を判定します。

- **再分類(Reclassify):** このエンジンは、特定のアプリケーションに固有ではない一般的な攻撃に対する応答を分析し、特定の脆弱性インスタンスを既知のアプリケーション脆弱性に再分類します。
- **要求変更(Request Modification):** ある種の攻撃では、不正な形式の要求を使用して、Webサーバから失敗の応答が返ってくるようにします。要求変更エンジンは、あるパターンと一致する他の要求から派生要求を生成し、その応答を評価して、この種の攻撃が可能かどうかを判定します。
- **サイト検索(Site Search):** これは、攻撃者が攻撃を開始する前にWebアプリケーションに関する情報をできるだけたくさん収集しようとする情報収集段階と考えられます。サイト検索は、Webユーザに閲覧させることは意図されていないドキュメント、アプリケーション、およびディレクトリなどのサーバ上のリソースを検索するために使用されます。このようなリソースが開示されると、機密データ、内部のサーバとアプリケーションの環境設定やその他の設定に関する情報、サイトへの管理アクセス情報、およびアプリケーションのソースコードに関する情報が漏えいする結果になる可能性があります。
- **SOAPアセスメント(SOAP Assessment):** Webサービスとは、(ユーザではなく)他のアプリケーションと通信し、情報の要求に応答するプログラムです。ほとんどのWebサービスは、SOAP (Simple Object Access Protocol)を使用して、Webサービスと、情報要求を行うクライアントWebアプリケーションとの間でXMLデータを送信します。SOAPアセスメントでは、そのトランスポートメカニズムに内在するセキュリティ上の脆弱性がないかがチェックされます。
- **SQLインジェクション:** SQLインジェクションとは、ハッカーがインターネットブラウザを介してSQLステートメントを使用し、データの抽出、追加、または変更、サービス拒否の生成、認証のバイパス、またはリモートコマンドの実行を行う攻撃です。SQLインジェクションエンジンは、次の攻撃を検出します。
 - Webフォーム内の悪意のある文字列など、ユーザ入力を介したインジェクション
 - 攻撃文字列を含んだ変更されたクッキーフィールドなど、クッキーを介したインジェクション
 - 操作されて攻撃文字列を追加されたヘッダなど、サーバ変数を介したインジェクション
- **WAF検出:** このエンジンは、Webアプリケーションファイアウォールの存在を検出します。

監査オプション

OpenText DASTは以下の監査オプションを使用します。

- **CVSエントリパーサ(CVS Entries Parser)**: このエンジンは、Web探索プログラムエンジンに追加するリンクのスキャンで検出されたエントリファイルを解析します。
- **Robots.txtパーサ(Robots.txt Parser)**: このエンジンは、Web探索プログラムエンジンに追加するリンクのスキャンで検出されたrobots.txtファイルを解析します。
- **WebInspectスキャンングニチャ(WebInspect Scan Signature)**: このシグニチャは、「SCANNED-BY-HP-」というテキストをサーバに送信します。このテキストはWebサーバのログに表示され、スキャンが発生したことを示します。
- **Ws_ftp.logパーサ(Ws_ftp.log Parser)**: このエンジンは、Ws_ftp.logファイルを検索して解析し、サイトディレクトリツリーにリンクを追加します。

一般的なアプリケーションテスト

このグループのチェックはすべてのWebアプリケーションに広く一般に適用できます。このグループには、サーバのルートにある共通ディレクトリを検出するディレクトリ列挙が含まれます。また、SQLインジェクションやクロスサイトスクリプティングなどの入力インジェクションのチェックも含まれます。

サードパーティのWebアプリケーション

このグループのチェックは、サードパーティのWebアプリケーションに関連する既知の脆弱性を検出します。

Webのフレームワーク/言語

このグループのエージェントは、Webアプリケーションサーバに関連する既知の脆弱性を検出します。また、特定のスクリプト言語に存在する既知の欠陥がターゲットシステムで悪用される可能性も判断します。

Webサーバ

このグループのエージェントは、以下のWebサーバに関連する既知の脆弱性を検出します。

- Apache
- IIS
- Lotus Domino

- マイナー(ATPhttpd、4D、Abyss、Alibaba、およびBadBlueなどのサーバのコレクション)
- Netscape/iPlanet
- Secure IIS
- Website Pro
- WebSphereプロキシ
- Zeus

使用可能なすべてのエージェントについて詳細を確認するには、Webサーバのノードを展開し、任意のエージェントをクリックしてください。

カスタムエージェント

OpenText DASTは通常のスキャン中に数千のエージェントを起動してWebアプリケーションを評価しますが、開発者は使用する環境またはアプリケーションに固有な特定の条件をチェックすることもできます。そのような場合、開発者はWebInspectソフトウェア開発者キット (SDK) を使用してカスタムエージェントを作成することができます。作成したカスタムエージェントは、Policy Managerを使用して1つ以上のポリシーに統合できます。

参照情報

["カスタムエージェントの使用" ページ76](#)

カスタムチェック

カスタムチェックは、標準のチェックでは検出できない特定の脆弱性を検出するユーザ定義のプロブです。カスタムチェックは、シンプルなウィザードを使用して作成できます。

参照情報

["カスタムチェックの使用" ページ66](#)

正規表現

正規表現のパターンは、特殊な文字やシーケンスを使用して作成されます。次の表に、これらの文字の一部を示し、その簡単な使用例を示します。推奨する他の参照先として「[Regular Expression Library](#)」があります。

文字	説明
\	次の文字を特殊文字としてマークします。/n/は文字「n」に一致します。シーケンス\n/は、改行文字に一致します。
^	入力または行の先頭に一致します。

文字	説明
	文字クラスとともに使用すると、否定文字を意味します。たとえば、contentディレクトリ内の/content/enおよび/content/caを除くすべてを除外するには、/content/[^(en ca)].*/.*を使用します。\\S \\D \\Wも参照してください。
\$	入力または行の末尾に一致します。
*	先行する文字の0回以上の反復と一致します。/zo*/は「z」とも「zoo」とも一致します。
+	先行する文字の1回以上の反復と一致します。/zo+/は「zoo」に一致しますが、「z」には一致しません。
?	先行する文字の0回または1回の出現と一致します。/a?ve?/は「never」の「ve」に一致します。
.	改行文字を除く任意の1文字に一致します。
[xyz]	文字セット。括弧内の任意の1文字に一致します。/[abc]/は「plain」の「a」に一致します。
\\b	スペースなどの単語境界に一致します。/ea*r\\b/は、「never early」の「er」に一致します。
\\B	単語以外の境界に一致します。/ea*r\\B/は「never early」の中の「ear」と一致します。
\\d	1つの数字に一致します。[0-9]と同じです。
\\D	数字以外の1文字に一致します。[^0-9]と同じです。
\\f	改ページ文字に一致します。
\\n	改行文字に一致します。
\\r	キャリッジリターン文字に一致します。
\\s	スペース、タブ、改ページなどの空白に一致します。[\\f\\n\\r\\t\\v]と同じです。
\\S	空白文字以外の文字に一致します。[^\\f\\n\\r\\t\\v]と同じです。
\\w	アンダースコアを含む任意の単語文字に一致します。[A-Za-z0-9_]と同じです。
\\W	英数字以外の文字に一致します。[^A-Za-z0-9_]と同じです。

正規表現の拡張

通常の正規表現構文に対する拡張がOpenTextのエンジニアにより開発および実装されています。正規表現を作成する場合は、次のタグと演算子を使用できます。

正規表現タグ

- [ALL]
- [BODY]
- [STATUSLINE]
- [HEADERS]
- [STATUSCODE]
- [STATUSDESCRIPTION]
- [COOKIES]

正規表現演算子

- AND
- OR
- NOT
- []
- ()

例

- (a)ステータス行にステータスコード「200」が含まれており、かつ(b)メッセージ本文のどこかに「logged out」という語句が含まれている応答を検出するには、次の正規表現を使用します。

[STATUSCODE]200 AND [BODY]logged\sout

- 要求されたリソースが一時的に別のURI (リダイレクト)に存在することを示しており、かつ応答のどこかにパス「/Login.asp」への参照が含まれる応答を検出するには、次の正規表現を使用します。

[STATUSCODE]302 AND [ALL]Login.asp

- (a)ステータスコードが「200」、かつ「logged out」または「session expired」という語句が本文のどこかに含まれている、または(b)ステータスコード「302」、かつ応答のどこかにパス「/Login.asp」への参照が含まれている応答のいずれかを検出するには、次の正規表現を使用します。

([STATUSCODE]200 AND [BODY]logged\sout OR [BODY]session\sexpired) OR ([STATUSCODE]302 AND [ALL]Login.asp)

注記:「開き」括弧または「閉じ」括弧の前後にスペース(ASCII 32)を含める必要があります。そうしないと、括弧が誤って正規表現の一部と見なされます。

- リダイレクト Location ヘッダのどこかに「login.aspx」が現れるリダイレクト応答を検出するには、次の正規表現を使用します。
[STATUSCODE]302 AND [HEADERS]Location:\slogin.aspx
- ステータス行の Reason-Phrase 部に特定の文字列(「Please Authenticate」など)が含まれる応答を検出するには、次の正規表現を使用します。
[STATUSDESCRIPTION]Please\sAuthenticate

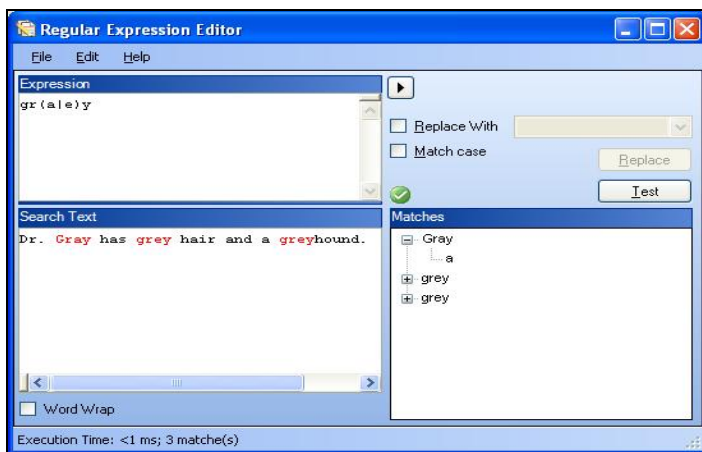
第8章:正規表現エディタ

正規表現とは、文字列のセットを表すパターンです。正規表現は、さまざまな演算子を使用して小さな式を組み合わせることによって、数式と同様に構成されます。正規表現に関する実用的な知識を持つ上級ユーザだけがこの機能を使用すべきです。


正規表現のテスト

Regular Expression Editorを使用して、次のように正規表現をテストおよび検証します。

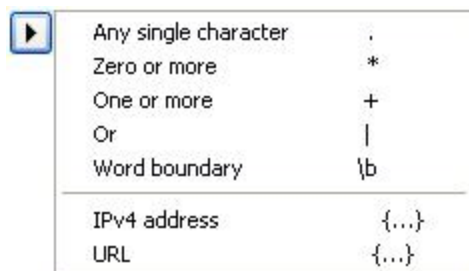
1. ツール(Tools)] > [Regular Expression Editor]をクリックします。
[Regular Expression Editor] ウィンドウが開きます。



2. 式(Expression)] エリアに、検索するテキストが見つかると思われる正規表現を入力または貼り付けます。

支援が必要な場合は、をクリックしてオブジェクトのリストを表示します。これには、URLとIPアドレスを定義するメタ文字と正規表現が含まれます。オブジェクトをクリックして挿入します。

注記: 正規表現の拡張を使用して、特定のエリアのHTTPメッセージに検索を制限することもできます。



入力した式の構文がRegular Expression Editorによって検査され、 (有効な場合)または (無効な場合)が表示されます。

3. 検索先のテキストを **検索テキスト(Search Text)** エリアに入力します(または貼り付けます)。
または、以前にHTTP Editorを使用して保存したHTTP要求または応答メッセージを次のようにしてロードできます。
 - a. **ファイル(File)] > 要求を開く(Open Request)]**をクリックします。
要求ファイルは、実際には、HTTP要求と応答の両方のデータを含むセッションです。
 - b. 標準のファイル選択ウィンドウを使用して、保存されたセッションを含むファイルを選択します。
 - c. **要求(Request)]**または **応答(Response)]**を選択します。
 - d. **OK]**をクリックします。
4. 式の大文字と小文字と一致する出現箇所のみを検索するには、**大文字/小文字を区別する(Match Case)]**チェックボックスをオンにします。
5. 正規表現によって識別された文字列を別の文字列で置き換えるには、以下の操作を実行します。
 - a. **置換文字列(Replace With)]**チェックボックスを選択します。
 - b. ドロップダウンコンボボックスを使用して文字列を入力または選択します。
6. **テスト(Test)]**をクリックして、正規表現に一致する文字列をターゲットテキストで検索します。一致は赤色で強調表示されます。
7. **置換(Replace)]**オプションを選択した場合は、**置換(Replace)]**をクリックして、検索された文字列すべてを置換文字列と置き換えます。

参照情報

["正規表現" 下](#)

["正規表現の拡張と演算子" ページ104](#)

正規表現

正規表現のパターンは、特殊な文字やシーケンスを使用して作成されます。次の表に、これらの文字の一部を示し、その簡単な使用例を示します。推奨する他の参照先として「[Regular Expression Library](#)」があります。

文字	説明
\	次の文字を特殊文字としてマークします。/n/は文字「n」に一致します。シーケンス\n/は、改行文字に一致します。
^	入力または行の先頭に一致します。 文字クラスとともに使用すると、否定文字を意味します。たとえば、contentディレ

文字	説明
	クトリ内の/content/enおよび/content/caを除くすべてを除外するには、/content/[^(en ca)].*/.*を使用します。\\S\\D\\Wも参照してください。
\$	入力または行の末尾に一致します。
*	先行する文字の0回以上の反復と一致します。/zo*/は「z」とも「zoo」とも一致します。
+	先行する文字の1回以上の反復と一致します。/zo+/は「zoo」に一致しますが、「z」には一致しません。
?	先行する文字の0回または1回の出現と一致します。/a?ve?/は「never」の「ve」に一致します。
.	改行文字を除く任意の1文字に一致します。
[xyz]	文字セット。括弧内の任意の1文字に一致します。/[abc]/は「plain」の「a」に一致します。
\\b	スペースなどの単語境界に一致します。/ea*r\\b/は、「never early」の「er」に一致します。
\\B	単語以外の境界に一致します。/ea*r\\B/は「never early」の中の「ear」と一致します。
\\d	1つの数字に一致します。[0-9]と同じです。
\\D	数字以外の1文字に一致します。[^0-9]と同じです。
\\f	改ページ文字に一致します。
\\n	改行文字に一致します。
\\r	キャリッジリターン文字に一致します。
\\s	スペース、タブ、改ページなどの空白に一致します。[\\f\\n\\r\\t\\v]と同じです。
\\S	空白文字以外の文字に一致します。[^\\f\\n\\r\\t\\v]と同じです。
\\w	アンダースコアを含む任意の単語文字に一致します。[A-Za-z0-9_]と同じです。
\\W	英数字以外の文字に一致します。[^A-Za-z0-9_]と同じです。

正規表現の拡張と演算子

OpenTextのエンジニアにより、通常の正規表現構文の拡張、およびそれに伴う一連の演算子が開発および実装されました。

正規表現の拡張

正規表現を構築する場合、この拡張を使用して、要求または応答のどの要素内で一致を検索するかを指定できます。次の表に、拡張の説明を示します。

拡張	要素
[ALL]	要求または応答のすべての要素
[BODY]	要求の本文 応答本文
[COOKIES]	要求のクッキー
[HEADERS]	要求ヘッダ(Request Headers) 応答ヘッダ(Response Headers)
[METHOD]	要求のメソッド(Request Method)
[POSTDATA]	Postデータ
[REQUESTLINE]	要求行(HTTP要求の開始行)
[SETCOOKIES]	Set-Cookie応答ヘッダ <div>注記: この拡張は、Regular Expression Editorツールでは機能しません。ただし、この拡張を使用する正規表現はエディタの外部で機能します。</div>
[STATUSCODE]	ステータスコード(Status Code)
[STATUSDESCRIPTION]	ステータスの説明(クライアントに返されるHTTP出力のステータスを説明する文字列)
[STATUSLINE]	ステータス行(HTTP応答の開始行)
[URI]	要求ターゲット(URI)
[VERSION]	HTTPバージョン

正規表現演算子

OpenTextのエンジニアにより、複雑な正規表現パターンの構築に使用できる正規表現演算子が開発されました。演算子は次のとおりです。

- AND
- OR
- NOT
- []
- ()

例

以下の段落に、拡張と演算子の使用例を示します。

- (a)ステータス行にステータスコード「200」が含まれており、かつ(b)メッセージ本文のどこかに「logged out」という語句が含まれている応答を検出するには、次の正規表現を使用します。

```
[STATUSCODE]200 AND [BODY]logged\sout
```

- 要求されたリソースが一時的に別のURI (リダイレクト)に存在することを示しており、かつ応答のどこかにパス「/Login.asp」への参照が含まれる応答を検出するには、次の正規表現を使用します。

```
[STATUSCODE]302 AND [ALL]Login.asp
```

- (a)ステータスコードが「200」、かつ「logged out」または「session expired」という語句が本文のどこかに含まれている、または(b)ステータスコード「302」、かつ応答のどこかにパス「/Login.asp」への参照が含まれている応答のいずれかを検出するには、次の正規表現を使用します。

```
( [STATUSCODE]200 AND [BODY]logged\sout OR [BODY]session\sexpired ) OR ( [STATUSCODE]302 AND [ALL]Login.asp )
```

注記:「開き」括弧または「閉じ」括弧の前後にスペース(ASCII 32)を含める必要があります。そうしないと、括弧が誤って正規表現の一部と見なされます。

- リダイレクト Locationヘッダのどこかに「login.aspx」が現れるリダイレクト応答を検出するには、次の正規表現を使用します。

```
[STATUSCODE]302 AND [HEADERS]Location:\slogin.aspx
```

- ステータス行のReason-Phrase部に特定の文字列(「Please Authenticate」など)が含まれる応答を検出するには、次の正規表現を使用します。

```
[STATUSDESCRIPTION]Please\sAuthenticate
```

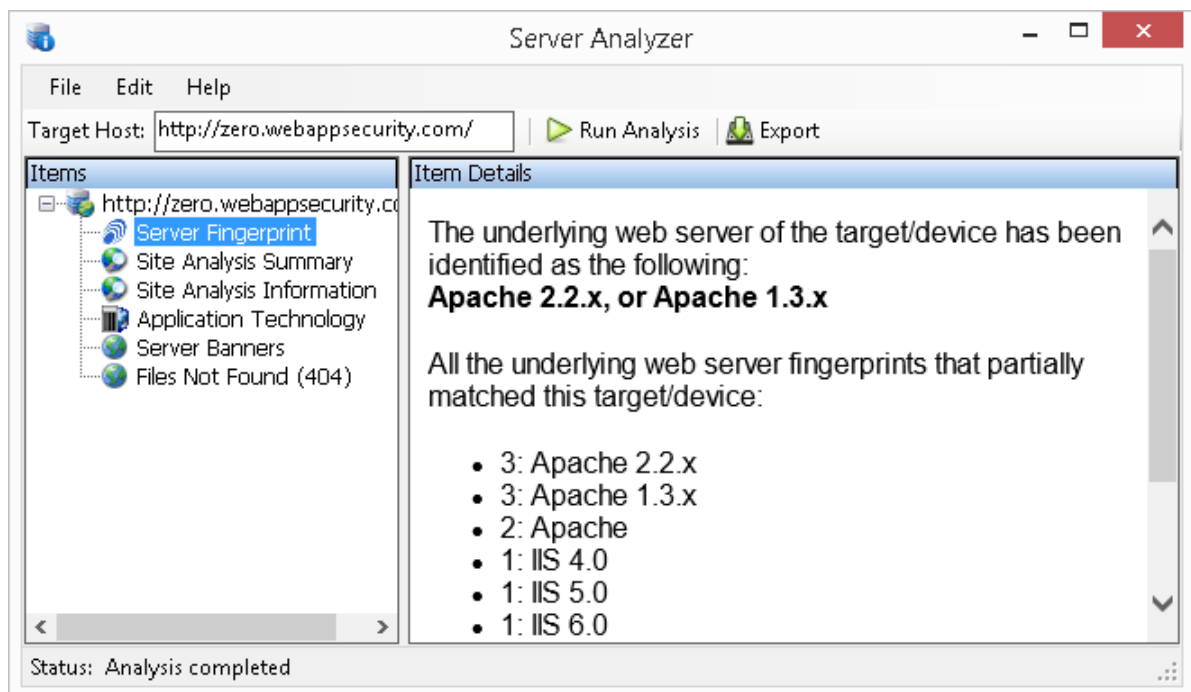
第9章:Server Analyzer(OpenText DASTのみ)

Server Analyzerは、サーバに問い合わせをしてサーバのオペレーティングシステム、バナー、クッキー、その他の情報を明らかにします。

サーバの分析

サーバを分析するには:

1. **ターゲットホスト(Target Host)** フィールドに、ターゲットサーバのURLまたはIPアドレスを入力します。
2. ホスト認証(ユーザ名とパスワード)が必要な場合、またはプロキシサーバを介してターゲットサーバにアクセスする場合は、**編集(Edit)> 設定(Settings)**をクリックして、要求された情報を入力します。詳細については、「["認証設定" 次のページ](#)」および「["プロキシ設定" ページ108](#)」を参照してください。
3. **分析の実行(Run Analysis)** アイコンをクリックします。
終了すると、Server Analyzerに「分析完了 (Analysis completed)」のステータスと、分析済みの項目のリストが表示されます。
4. **項目の詳細(Item Details)** ペインに情報を表示するには、**項目(Item)** ペインで項目を選択します。



設定の変更

Server Analyzerの設定を変更するには:

1. **編集(Edit)] > 設定(Settings)]**をクリックします。
2. 次のいずれか1つを選択します。
 - **ホスト認証(Host Authentication)]**。「["認証設定" 下](#)」を参照してください。
 - **プロキシ(Proxy)]**。「["プロキシ設定" 次のページ](#)」を参照してください。
3. **OK]**をクリックします。

Analyzerの結果のエクスポート

分析結果をHTMLファイルにエクスポートするには:

1. **ファイル(File)] > エクスポート(Export)]**をクリックします。
2. **ファイルのエクスポート (Export File)]** ウィンドウで、場所とファイル名を選択または入力します。
3. **Save]**をクリックします。

参照情報

["認証設定" 下](#)

["プロキシ設定" 次のページ](#)

認証設定

認証者設定を使用すると、認証メソッドと認証資格情報を設定できます。

認証メソッド

認証が必要な場合は、認証の種類を選択してください:

- 自動

注記: 自動検出を指定すると、スキャンの処理が遅くなります。把握している別の認証メソッドを指定すると、スキャンのパフォーマンスは大幅に向上します。

- ダイジェスト
- HTTP基本(HTTP Basic)
- Kerberos
- NTLM (NT LanMan)

認証資格情報

ユーザ名 (User name)] フィールドにユーザIDを入力し、**[パスワード (Password)]** フィールドにユーザのパスワードを入力します。入力ミスを防ぐために、**[パスワードの確認 (Confirm Password)]** フィールドにパスワードを繰り返し入力します。

Server Analyzerでパスワード入力コントロールが検出されるたびにこれらの資格情報を使用するには、**[パスワード入力フィールドがあるフォームにはこれらの資格情報を送信する (Submit these credentials to forms with password input fields)]** を選択します。

プロキシ設定

この機能にアクセスするには、**編集 (Edit)] > 設定 (Settings)]** をクリックします。次に、**プロキシ (Proxy)]** を選択します。

直接接続(プロキシ無効)(Direct Connection (proxy disabled))

プロキシサーバを使用しない場合は、このオプションを選択します。

プロキシ設定の自動検出 (Auto detect proxy settings)

このオプションを選択すると、Server AnalyzerはWPAD (Web Proxy Autodiscovery Protocol)を使用してプロキシ自動設定ファイルを見つけ、それを使用してブラウザのWebプロキシ設定を行います。

システムのプロキシ設定を使用する(Use system proxy settings)

ローカルマシンからプロキシサーバ情報をインポートするには、このオプションを選択します。

Firefoxプロキシ設定を使用する(Use Firefox proxy settings)

Firefoxからプロキシサーバ情報をインポートするには、このオプションを選択します。

注記: ブラウザのプロキシ設定を使用しても、プロキシサーバ経由でインターネットにアクセスできる保証はありません。Firefoxブラウザの接続設定が「プロキシなし」に設定されている場合、プロキシは使用されません。

PACファイルを使用してプロキシを設定する(Configure proxy using a PAC file)

このオプションを選択すると、[URL]フィールドで指定した場所にあるPAC (Proxy Automatic Configuration)ファイルからプロキシ設定がロードされます。

プロキシを明示的に設定する(Explicitly configure proxy)

プロキシサーバ経由でインターネットにアクセスするには、このオプションを選択し、要求された情報を以下のように入力します。

1. **サーバ(Server)**フィールドにプロキシサーバのURLまたはIPアドレスを入力し、続いて (**ポート(Port)**)フィールドにポート番号(8080など)を入力します。
2. プロキシサーバ経由でTCPトラフィックを処理するプロトコルの **タイプ(Type)**を、SOCKS4、SOCKS5、または標準から選択します。
3. 認証が必要な場合は、**認証(Authentication)**リストからタイプを選択します。

- 自動

注記: 自動検出を指定すると、スキャンの処理が遅くなります。把握している別の認証メソッドを指定すると、スキャンのパフォーマンスは大幅に向上します。

- 基本

- ダイジェスト

- Kerberos

- ネゴシエート(Negotiate)

- NTLM (NT LanMan)

4. プロキシサーバで認証が必要な場合は、適格なユーザ名とパスワードを入力します。
5. 特定のIPアドレス(内部テストサイトなど)にアクセスするためにプロキシサーバを使用する必要がない場合は、**プロキシをバイパスするサイト(Bypass Proxy For)**フィールドにアドレスまたはURLを入力します。エントリを区切る場合は、カンマを使用します。

HTTPS用の代替プロキシを指定する(Specify alternative proxy for HTTPS)

HTTPS接続を受け入れるプロキシサーバの場合は、**[HTTPS用の代替プロキシを指定する(Specify Alternative Proxy for HTTPS)]**チェックボックスを選択し、要求された情報を入力します。

第10章:Server Profiler

Server Profilerを使用してWebサイトの事前テストを行い、OpenText DASTの特定の設定を変更する必要があるかどうかを判断します。変更が必要だと思われる場合、Profilerは提案のリストを返します。これらの提案は、受け入れることも拒否することもできます。

たとえば、Server Profilerは、サイトに入るために権限付与が必要であるものの、有効なユーザ名とパスワードが指定されていないことを検出するかもしれません。そのままスキャンを続行して著しく質の低い結果を得るのではなく、Server Profilerのプロンプトに従って、続行する前に必要な情報を設定することができます。

同様に、設定では、OpenText DASTが「ファイルが見つからない」の検出を実行しないように指定されていることもあります。このプロセスは、存在しないリソースをクライアントから要求されてもステータス「404 Not Found」を返さないWebサイトで役に立ちます(代わりにステータス「200 OK」が返される場合がありますが、応答にはファイルが見つからないというメッセージが含まれます)。Profilerは、このような手法がターゲットサイトに実装されていると判断した場合、この特徴に対応できるようにOpenText DAST設定を変更することを推奨します。

Server Profilerは、ガイド付きスキャン中に選択することも、[アプリケーション(Application)]設定で有効にすることもできます。

ツールとしてのServer Profilerの起動

プロファイラをスキャンウィザードの外部でツールとして起動するには、次の手順に従います。

1. OpenText DASTの **ツール(Tools)** メニューをクリックし、 **サーバ(Server)プロファイラ(Profiler)** を選択します。
2. **[URL]** ボックスで、URLまたはIPアドレスを入力または選択します。
3. (オプション)必要に応じて、 **サンプルサイズ(Sample Size)** を変更します。大規模なWebサイトでは、要件を十分に分析するために、デフォルトのセッション数を超えるセッションが必要な場合があります。
4. **分析(Analyze)** をクリックします。
Profilerは、提案の一覧(または変更が不要であるというステートメント)を返します。
5. 提案を拒否するには、関連するチェックボックスのチェックを外します。
6. ユーザ入力が必要な提案については、要求された情報を入力してください。
7. (オプション)変更した設定をファイルに保存するには:
 - a. **設定の保存(Save Settings)** をクリックします。
 - b. 標準のファイル選択ウィンドウを使用して、設定をSettingsディレクトリのファイルに保存します。

スキヤンの開始時にServer Profilerを起動する

スキヤンの開始時にProfilerを起動するには、次の手順に従います。

1. 次のいずれかの方法でスキヤンを開始します。
 - OpenText DASTの **開始ページ(Start Page)]** で、 **基本スキヤンの開始(Start a Basic Scan)]** をクリックします。
 - **【ファイル(File)]> 新規(New)]> 基本スキヤン(Basic Scan)]** をクリックします。
 - (ツールバーの) **新規(New)]** アイコンでドロップダウン矢印をクリックして、 **基本スキヤン(Basic Scan)]** を選択します。
 - OpenText DASTの **開始ページ(Start Page)]** で、 **スケジュールされたスキヤンの管理(Manage Scheduled Scans)]** をクリックし、 **追加(Add)]** をクリックしてから **基本スキヤン(Basic Scan)]** を選択します。
2. スキヤンウィザードのステップ4(詳細スキヤン設定)で、 **プロファイル(Profile)]** をクリックします(**Profilerを自動的に実行する(Run Profiler Automatically)]** が選択されている場合を除く)。
Profilerは、提案の一覧(または変更が不要であるというステートメント)を返します。
3. 提案を拒否するには、関連するチェックボックスのチェックを外します。
4. ユーザ入力が必要な提案については、要求された情報を入力してください。
5. **次へ(Next)]** をクリックします。

第11章:SmartUpdate

インターネットに接続しているインストール環境では、SmartUpdate機能がOpenTextデータセンターと通信して、新規または更新されたアダプティブエージェント、脆弱性チェック、およびポリシー情報を確認します。SmartUpdateでは、OpenText DASTの最新バージョンを使用しているかどうかを確認され、新しいバージョンがダウンロード可能な場合には通知されます。

アプリケーションを起動するたびにSmartUpdateを実行するようにOpenText DASTを設定できます(**編集(Edit)**メニューから **アプリケーション設定(Application Settings)**を選択し、**スマートアップデート(Smart Update)**を選択します)。

OpenText DASTユーザインタフェースからSmartUpdateをオンデマンドで実行することもできます。このためには、OpenText DASTの **開始ページ(Start Page)**から **SmartUpdateを開始(Start SmartUpdate)**を選択するか、**ツール(Tools)**メニューから **SmartUpdate**を選択するか、または標準ツールバーの **SmartUpdate**ボタンをクリックします。

インターネットに接続していないインストール環境の場合は、["オフラインのSmartUpdateの実行" ページ114](#)を参照してください。

注意! {b}エンタープライズインストールの場合、OpenText DASTが使用する特定のファイルがSmartUpdateによって変更または置換されると、センササービスが停止し、センサで「オフライン」ステータスが表示されることがあります。OpenText DASTアプリケーションを起動し、サービスを再起動する必要があります。手順は次のとおりです:

1. **編集(Edit)**> **アプリケーション設定(Application Settings)**をクリックします。
2. **センサとして実行(Run as a Sensor)**を選択します。
3. **センサステータス(Sensor Status)**エリアの **開始(Start)**ボタンをクリックします。

SmartUpdateの実行(インターネットに接続している場合)

OpenText DASTがインターネットに接続している場合にSmartUpdateを実行するには:

1. 次のいずれかを実行します。
 - ツールバーで **SmartUpdate**をクリックします。
 - **ツール(Tools)**メニューから **SmartUpdate**を選択します。
 - OpenText DASTの **開始ページ(Start Page)**から **SmartUpdateの開始(Start SmartUpdate)**を選択します。

アップデートが利用可能な場合は、[SmartUpdater] ウィンドウが開き、[サマリ (Summary)] タブが表示されます。[サマリ (Summary)] タブには、次のアイテムをダウンロードするための折りたたみ可能な別個のペインが最大3つ表示されます。

- 新規チェックおよび更新されたチェック
 - OpenText DASTソフトウェア
 - SmartUpdateソフトウェア
2. 1つ以上のダウンロードオプションに対応するチェックボックスをオンにします。
 3. (オプション)更新されるチェックの詳細を表示するには
 - a. **チェックの詳細 (Check Detail)]** タブをクリックします。

左側のペインには、更新されるチェックのID、名前、およびバージョンを示すリストが表示されます。リストは [追加 (Added)]、[更新 (Updated)]、および [削除 (Delete)] でグループ化されます。
 - b. 更新される特定のチェックを含むポリシーを確認するには、リストでそのチェックを選択します。

影響を受けるポリシーのリストが **関連ポリシー (Related Policies)]** ペインに表示されます。
 4. (オプション)影響を受けるポリシーの詳細を表示するには:
 - a. **ポリシーの詳細 (Policy Detail)]** タブをクリックします。

左側のペインに、更新の影響を受けるポリシーが英字順で一覧表示されます。

注記: このリストには、更新されるチェックの影響を受けるポリシーだけが表示されます。[ポリシーの詳細 (Policy Detail)] タブには、アップデートに含まれている可能性があるその他のポリシー変更(ポリシーへの新しいチェックの関連付けまたはポリシー名の変更など)は表示されません。
 - b. 特定のポリシーで更新されるチェックを表示するには、リストからポリシーを選択します。

関連チェック (Related Checks)] ペインに、更新されるチェックのID、名前、およびバージョンを示すリストが表示されます。リストは [追加 (Added)]、[更新 (Updated)]、および [削除 (Delete)] でグループ化されます。
 5. アップデートをインストールするには、**ダウンロード (Download)]** をクリックします。

OpenText DASTを更新せずにチェックをダウンロードする

スキャン中に特定のチェックを実行するには、エンジンの更新が必要です。最新バージョンのOpenText DASTを使用していない場合、スキャン中にSecureBaseのチェックの一部を実行できない可能性があります。すべて最新のチェックを使用してアプリケーションをテストするには、最新バージョンのOpenText DASTを使用する必要があります。

オフラインのSmartUpdateの実行

オフラインのOpenText DASTに対してSmartUpdateを実行するには、次の手順に従います。


ステージ	説明
1.	サポートケースを作成します。カスタマサポート担当者から、オフラインFTPサーバのURLとログイン資格情報が提供されます(必要な場合)。詳細については、" 序文 " ページ20 の「Fortifyカスタマサポートへのお問い合わせ」を参照してください。
2.	インターネットにアクセスできるマシンで、オフラインFTPサーバにアクセスします。
3.	OpenText DASTのスタティックSmartUpdate ZIPファイルをダウンロードします。
4.	OpenText DASTがインストールされているマシンで、ZIPファイルからすべてのファイルを解凍します。
5.	OpenText DASTを閉じます。
6.	解凍した SecureBase.db ファイルおよび version.txt ファイルを、SecureBaseデータがあるディレクトリにコピーします。デフォルトの場所： C:\ProgramData\HP\HP WebInspect\SecureBase ヒント: Windowsでは、デフォルトではこれらのフォルダは表示されません。フォルダオプションを変更して隠しファイルを表示してください。

第12章:SQL Injector(OpenText DASTのみ)

SQLインジェクションとは、有害な可能性がある文字を最初に削除しないでクライアント提供のデータをSQLクエリに使用するWebアプリケーションを悪用する手法です。SQL Injectorは、MS-SQL、Oracle、Postgres、MySQL、およびDB2のデータベースタイプをサポートし、日本語を含む複数の言語のシステムもサポートします。

注意! このツールは、SQLサーバによって処理される可能性のあるHTTP要求を作成して送信することにより、SQLインジェクションの脆弱性をテストします。Webアプリケーションでユーザ提供のデータを使用してデータベースレコードを更新または作成できる場合、SQL Injectorによって疑似的なレコードが作成されることがあります。このような可能性を回避するために、運用データベースに対してはテストを行わないでください。代わりに、データベースのコピーを使用するか、運用データにアクセスできないテストアカウントを使用するか、データベースのデータを更新したり削除したりする可能性があるページを監査から除外してください。これらの代替方法をとることができない場合には、運用データベースのバックアップを事前に作成したうえで、サイトに顧客トラフィックがほとんどまたはまったくないときにテストを行ってください。

SQLインジェクションに対する脆弱性をテストするには:

1. プロキシサーバを使用している場合、またはターゲットサイトで認証が必要な場合は、**設定(Settings)** タブをクリックして適切な情報を入力します。詳細については、「[SQL Injectorの設定" ページ119](#)」を参照してください。
2. **ファイル(File)** > **新規(New)** を選択します。
- または -
新規要求(New Request) アイコン  をクリックします。
3. **ロケーション(Location)** フィールドに、SQLインジェクションに対して脆弱だと思われるURLを入力するか貼り付けます。次の例を参照してください。
 - GETメソッドの場合(クエリパラメータはURLに埋め込まれます):
`http://172.16.61.10/Myweb/MSSQL/Welcome.asp?login=aaa&password=bbb`
 - POSTメソッドの場合(クエリパラメータはメッセージ本文に含まれます):
`http://172.16.61.10:80/Myweb/MSSQL/Welcome.asp`

SQL InjectorのデフォルトはGETメソッドであるため、**生(Raw)** タブ(これは **ビュー(View)** > **要求の表示(Show Request)** を選択すると表示されます)でPOST要求を編集する必要もあります。編集した要求は次のようになります。

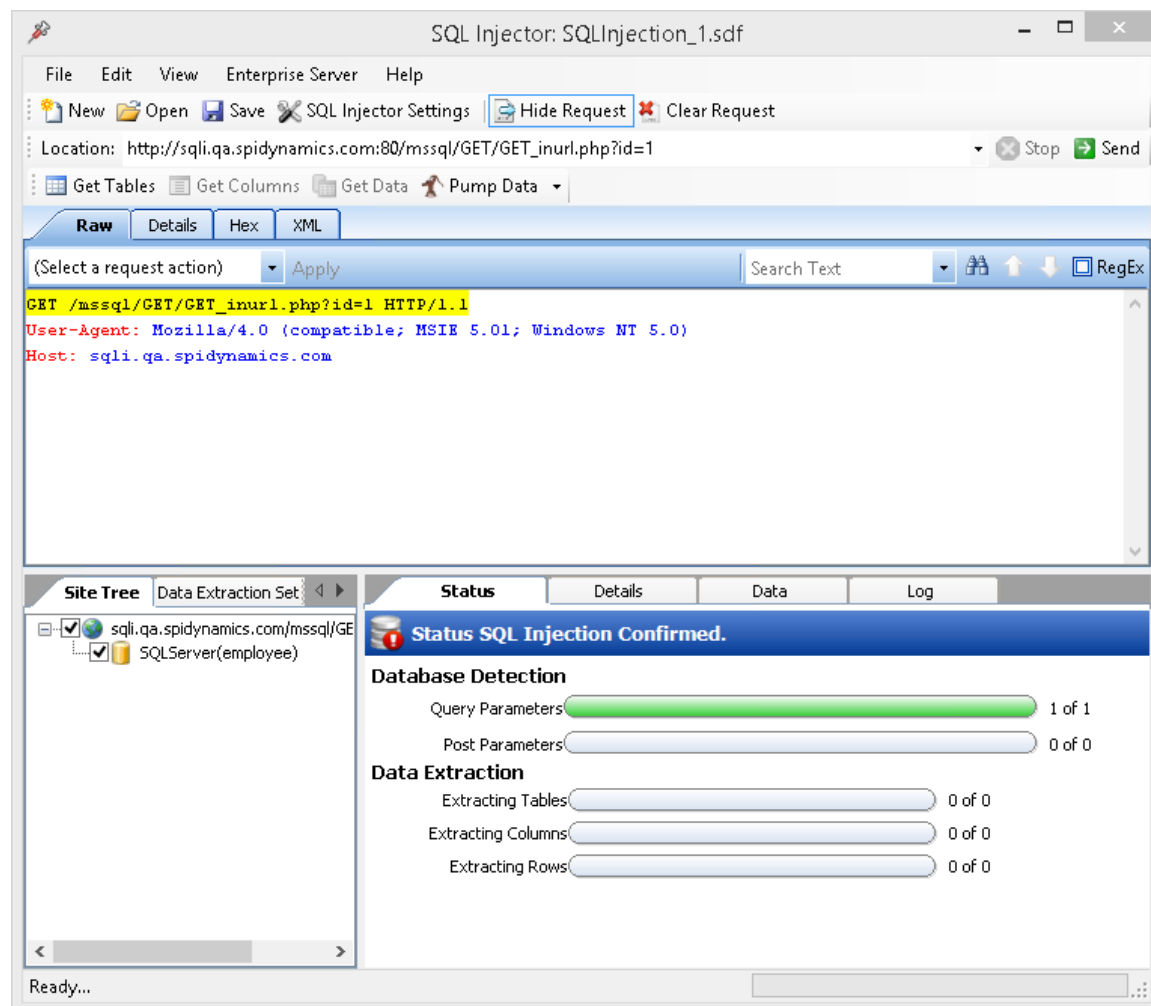
```
POST /Myweb/MSSQL/POST/2.asp HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: 172.16.61.10
Content-Length: 22
```

Content-Type: application/x-www-form-urlencoded
login=qqq&password=aaa


注記: OpenText DASTがSQLインジェクションの脆弱性を検出した場合は、OpenText DASTのナビゲーションペインで脆弱なセッションを右クリック(またはサマリペインの **脆弱性(Vulnerabilities)** タブで脆弱なURLを右クリック)して、ショートカットメニューから **ツール(Tools)] > SQL Injector]** を選択できます。

4. **送信(Send)]** をクリックします。

SQLインジェクションに成功すると、**ステータス(Status)]** タブに **SQLインジェクション確認済み(SQL Injection Confirmed)]** と表示され、左下ペインの **サイトツリー(Site Tree)]** タブにデータ階層ツリーの先頭が表示されます。



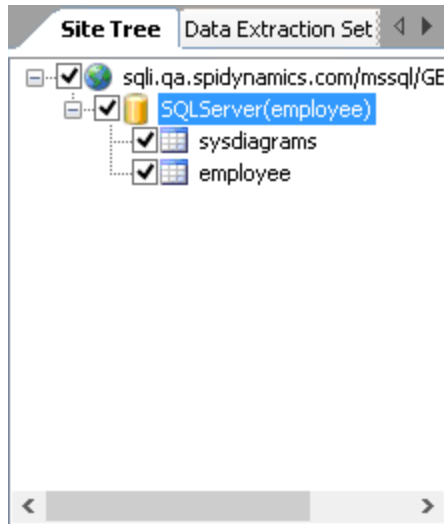
この画面のタブの詳細については、**"SQL Injectorのタブ" ページ118**を参照してください。

5. すべてのテーブルからすべてのデータを抽出するには、**データ抽出(Pump Data)]** アイコン  **Pump Data** をクリックします。

または、次の手順を使用して、テーブルと列を選択的に調査することもできます。

- a. **テーブルの取得(Get Tables)]**を選択します。

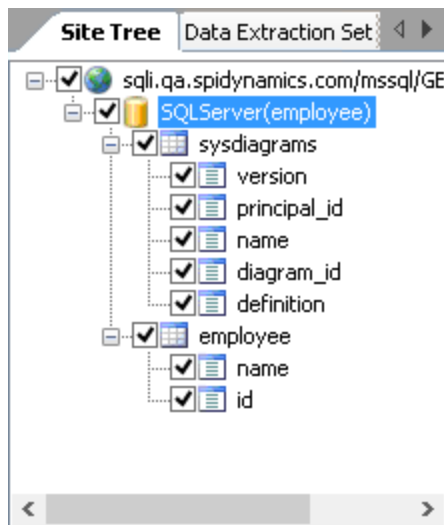
SQL Injectorが、ターゲット データベース内のすべてのテーブルの名前を返します。



- b. テーブルに関連付けられているチェックボックスをオンまたはオフにして、テーブルを選択します。

- c. **列の取得(Get Columns)]**をクリックします。

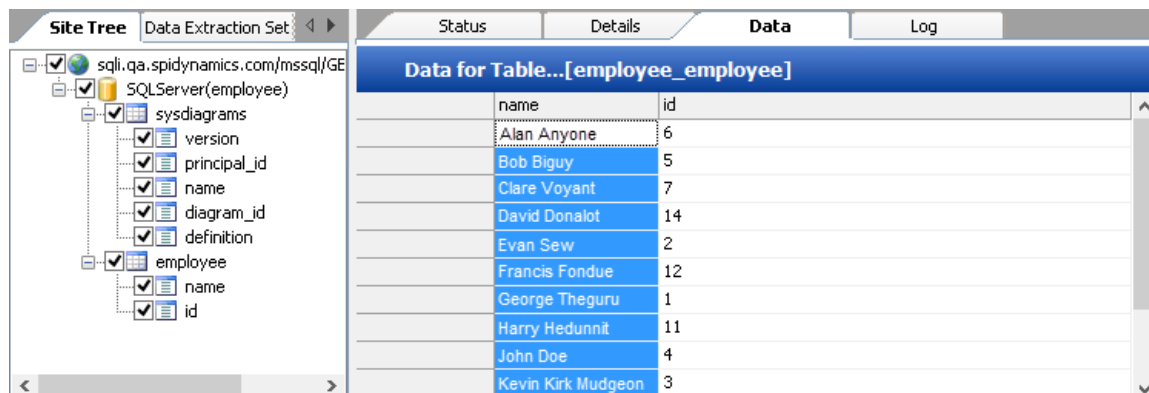
SQL Injectorが、選択したテーブル内のすべての列の名前を返します。



- d. 列に関連付けられているチェックボックスをオンまたはオフにして、列を選択します。

- e. **データの取得(Get Data)]**をクリックします。

6. 列を選択し、**データ(Data)]**タブをクリックして、列の値を表示します。



注記: SQL Injectorがデータを抽出できない場合は、脆弱なデータベースの名前を取得することによって、SQLインジェクションの脆弱性の存在を確認できる可能性があります。この機能を有効にするには、トピックの「推論/時間ベースの抽出」を参照してください。

参照情報

["SQL Injectorのタブ" 下](#)

["SQL Injectorの設定" 次のページ](#)

SQL Injectorのタブ

SQLインジェクションが成功すると、SQL Injectorは次のペインとタブを表示します。

要求ペイン

要求ペインには、次のタブがあります。

- **生(Raw)** - HTTP要求のテキストを表示します。
- **詳細(Details)** - 要求を、メソッド、要求URI、およびプロトコルのセグメントに分けて表示します。要求のヘッダフィールドとその関連値も一覧表示します。
- **Hex(16進数)** - HTTP要求を16進形式で表示します。

要求ペインの表示を切り替えるには、**要求の表示(Show Request)]/ 要求の非表示(Hide Request)]**をクリックします。

要求を削除してデフォルトのhttp://localhost:80/に置き換えるには、**要求のクリア(Clear Request)]**をクリックします。

データベースペイン

左下のペインには、次のタブがあります。

- **サイトツリー(Site Tree)** - URL、データベース、テーブル、および列を表示します。
- **データ抽出設定(Data Extraction Settings)** -データの抽出時に返されるテーブル、列、および行の最大数を表示します。これらの値は設定から抽出されますが、ここから **設定** ダイアログで変更できます。

情報ペイン

右下のペインには、次のタブがあります。

- **ステータス(Status)** -検出機能と抽出機能の進行状況バーを表示します。
- **詳細(Details)** -データベースの情報と挿入可能なパラメータの詳細を表示します。
- **データ(Data)** -選択したテーブルおよび列から抽出されたデータを表示します。
- **ログ(Log)** -関係する関数の概要と発生した時刻が表示されます。

SQL Injectorの設定

SQL Injectorの設定を変更するには、次のようにします。

1. **編集(Edit)] > 設定(Settings)]**をクリックします。
2. 次のいずれかのタブを選択し、以下のセクションで説明するように設定を指定します。
 - オプション(" [オプション\(Options\)\] タブ](#)" 下を参照)
 - 認証(" [認証\(Authentication\)\] タブ](#)" ページ121を参照)
 - プロキシ(" [プロキシ\(Proxy\)\] タブ](#)" ページ121を参照)
3. **OK]**をクリックします。

オプション(Options)] タブ

タイムアウト(秒) (Timeout in seconds)

SQL Injectorがセッションを終了する前に応答を待つ時間を秒数で指定します。

状態の適用(Apply state)

アプリケーションがセッション内の状態を維持するためにクッキー、URL再書き込み、またはPOSTデータの技術を使用している場合、SQL Injectorはその方式を特定し、それに従って応答を変更しようとします。

プロキシの適用(Apply proxy)

このオプションを選択すると、SQL Injectorはユーザが指定したプロキシ設定に従って要求を変更します。

ログ記録(Logging)

ログに記録するイベントを選択します。

- 要求
- 応答
- エラー
- デバッグメッセージ

ログファイルはxml形式で<drive>:\Users\<user name>\Documents\HP\Tools\SQLInjector\logsに保存されます。

各ファイル名の先頭は、YYYY_MM_DD<current-process-id>という形式になります。名前の残りの部分は、次のような形式になります。

- _sqli_debug.log: そのセッションのデバッグメッセージが含まれます。
- _errors.log: そのセッションで発生したエラーと例外が含まれます。
- _RequestsResponses.log: SQL Injectorによって送受信された要求と応答すべてが含まれます。

データ抽出(Data extraction)


SQLインジェクションに対して脆弱なURLでデータを抽出するときに返されるテーブル、列、および行の最大数を指定します。これらの値は、データベースペインの **データ抽出設定(Data Extraction Settings)** タブにも表示されます。これらの値は、このタブまたは **設定(Settings)** ダイアログを使用して変更できます。

また、データ抽出に使用する同時スレッドの最大数も指定します。

推論/時間ベースの抽出(Inferential/time-based extraction)

SQL Injectorは、SQLインジェクションの脆弱性が検出された場合に、2つの異なる方法でデータを抽出できます。すべての試みは、HTTP応答の内容を調べる推論技法を使用して実行されます。この方法が失敗した場合には、時間ベースの抽出と呼ばれる2つ目の技法をツールに強制的に使用させることができます。この手法では、テーブルデータを抽出する代わりに、データベース名の各文字に対して実行時間が長い4-5個のデータベースクエリを送信することで、データベースの名前を取得することを試みます。これはかなり時間がかかる処理になることがあるため、ユーザはSQLインジェクション脆弱性の存在を確認するために必要な文字数を指定できます。

マクロの使用(Use a macro)

マクロを使用する場合は、このチェックボックスをオンにし、参照ボタン  をクリックしてマクロを選択します。

データベースファイルパス(Database file path)

この読み取り専用テキストボックスには、SQL Injectorツールが攻撃データを保存し、攻撃されたデータベースの一部を複製するために作成したデータベースへのパスが表示されます。

認証(Authentication)] タブ

認証メソッド

サイトで認証が不要な場合は、**なし(None)]**を選択します。それ以外の場合は、**認証(Authentication)]** リストから認証メソッドを選択します。

- **自動**

注記: 自動検出を指定すると、スキャンの処理が遅くなります。把握している別の認証メソッドを指定すると、スキャンのパフォーマンスは大幅に向上します。

- HTTP基本(HTTP Basic)
- NTLM (NT LanMan)

認証資格情報

ユーザ名 (User name)] フィールドにユーザIDを入力し、**{パスワード(Password)]** フィールドにユーザのパスワードを入力します。入カミスを防ぐために、**{パスワードの確認(Confirm Password)]** フィールドにパスワードを繰り返し入力します。

プロキシ(Proxy)] タブ

プロキシサーバを介してSQL Injectorにアクセスするには、次の設定を使用します。

直接接続(プロキシ無効)(Direct Connection (proxy disabled))

プロキシサーバを使用しない場合は、このオプションを選択します。

プロキシ設定の自動検出(Auto detect proxy settings)

このオプションを選択すると、SQL InjectorはWPAD (Web Proxy Autodiscovery Protocol)を使用してプロキシ自動設定ファイルを見つけ、それを使用してブラウザのWebプロキシ設定を行います。

システムのプロキシ設定を使用する(Use system proxy settings)

ローカルマシンからプロキシサーバ情報をインポートするには、このオプションを選択します。

Firefoxプロキシ設定を使用する(Use Firefox proxy settings)

Firefoxからプロキシサーバ情報をインポートするには、このオプションを選択します。

注記: ブラウザのプロキシ設定を使用しても、プロキシサーバ経由でインターネットにアクセスできる保証はありません。Firefoxブラウザの接続設定が「プロキシなし」に設定されている場合、プロキシは使用されません。

PACファイルを使用してプロキシを設定する(Configure a proxy using a PAC file)

このオプションを選択すると、[URL]フィールドに指定したファイルの場所にあるPAC (Proxy Automatic Configuration)ファイルからプロキシ設定がロードされます。

プロキシを明示的に設定する(Explicitly configure proxy)

プロキシサーバ経由でインターネットにアクセスするには、このオプションを選択し、要求された情報を以下のように入力します。

1. **サーバ(Server)**フィールドにプロキシサーバのURLまたはIPアドレスを入力し、続いて (**ポート(Port)**)フィールドにポート番号(8080など)を入力します。
2. プロキシサーバ経由でTCPトラフィックを処理するプロトコルの **タイプ(Type)**]を、SOCKS4、SOCKS5、または標準から選択します。
3. 認証が必要な場合は、**認証(Authentication)**]リストからタイプを選択します。

- 自動

注記: 自動検出を指定すると、スキャンの処理が遅くなります。把握している別の認証メソッドを指定すると、スキャンのパフォーマンスは大幅に向上します。

- 基本

- ダイジェスト

- Kerberos

- ネゴシエート(Negotiate)

- NTLM (NT LanMan)

4. プロキシサーバで認証が必要な場合は、適格なユーザ名とパスワードを入力します。
5. 特定のIPアドレス(内部テストサイトなど)にアクセスするためにプロキシサーバを使用する必要がない場合は、**プロキシをバイパスするサイト(Bypass Proxy For)**フィールドにアドレスまたはURLを入力します。エントリを区切る場合は、カンマを使用します。

HTTPS用の代替プロキシを指定する(Specify alternative proxy for HTTPS)

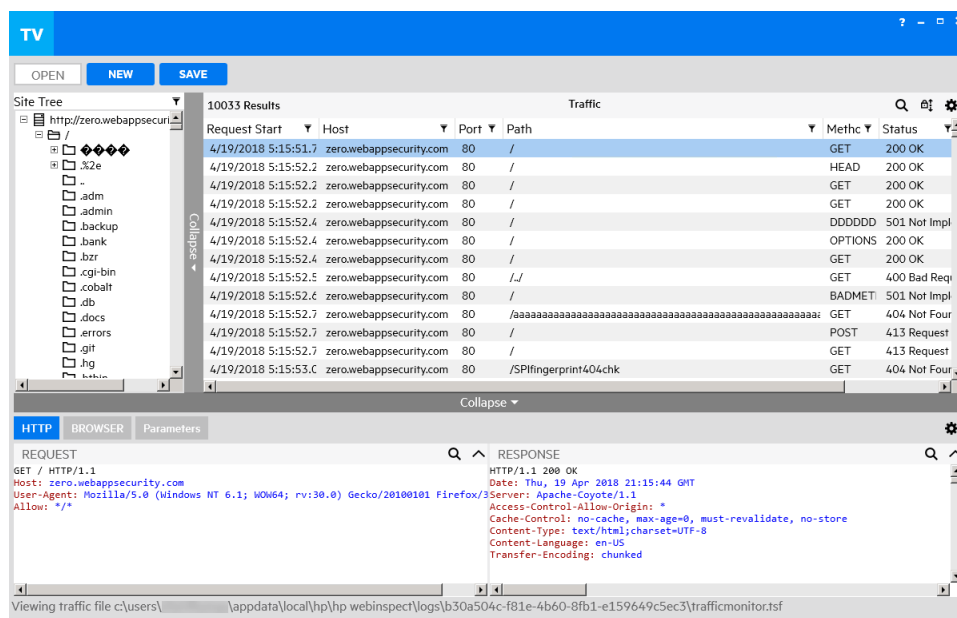
HTTPS接続を受け入れるプロキシサーバの場合は、**[HTTPS用の代替プロキシを指定する(Specify Alternative Proxy for HTTPS)]**チェックボックスを選択し、要求された情報を入力します。

第13章:Traffic Viewer

通常、OpenText DASTのナビゲーションペインにはWebサイトまたはWebサービスの階層構造だけが表示され、それに加えて脆弱性が検出されたセッションが表示されます。一方、Traffic Viewerでは、OpenText DASTが送信したすべてのHTTP要求と、サーバから受信した関連HTTP応答を表示して確認することができます。

Traffic Viewerのイメージ

以下のイメージは、スキャンのトラフィックファイルを表示しているTraffic Viewerを示しています。



オプションを有効にする必要がある

Traffic Viewerを使用するには、スキャンを実行する前に『Traffic Monitorログ(Traffic Monitor Logging)』オプションを有効にする必要があります。スキャンを実行する前に『Traffic Monitorログ(Traffic Monitor Logging)』を有効にしないと、そのスキャンに関してはTraffic Viewerは使用できません。詳細については、「["Traffic Monitorの有効化" 次のページ](#)」を参照してください。

プロキシサーバ

Traffic Viewerには、デスクトップ上で設定して実行できる自己完結型のプロキシサーバも含まれています。これを使用すると、ブラウザがHTTP要求を送信し、Webサーバから応答を受け取るときのブラウザのトラフィックを監視できます。Traffic Viewerプロキシはデバッグと侵入評

価を行うためのツールであり、ユーザはサイトをブラウズしながら、すべての要求とサーバ応答を見ることができます。

また、この機能を使用して、OpenText DASTで使用するワークフローマクロやログインマクロを作成することもできます。

Traffic Monitorの有効化

OpenText DASTで、すべてのスキャンまたは個別のスキャンに対してTraffic Monitorを有効化できます。

すべてのスキャンに対するTraffic Monitorの有効化

デフォルト設定でTraffic Monitorを有効にするには:

1. **編集(Edit)] > デフォルトのスキャン設定(Default Scan Settings)]**の順にクリックします。
2. **スキャン設定(Scan Settings)] ペインで、 全般(General)]**をクリックします。
3. **Traffic Monitorのログ記録を有効にする(Enable Traffic Monitor Logging)]**を選択します。

注記: Traffic Viewerはトラフィックファイルの暗号化をサポートしません。 **Traffic Monitorファイルを暗号化(Encrypt Traffic Monitor File)]** オプションは、レガシトラフィックファイルがある特別な状況でのみ使用するものです。

4. **OK]**をクリックします。

個々のスキャンに対するTraffic Monitorの有効化

スキャンウィザードを使用してスキャンを開始するときにTraffic Monitorを有効にするには、次のいずれかを実行します。

- スキャンウィザードの下部にある **設定(デフォルト)]**を選択し、"**すべてのスキャンに対するTraffic Monitorの有効化**" 上の手順2から4に従います。
- スキャンウィザードの **詳細なスキャン設定(Detailed Scan Configuration)]** ウィンドウで、**Traffic Monitorの有効化(Enable Traffic Monitor)]**を選択します。

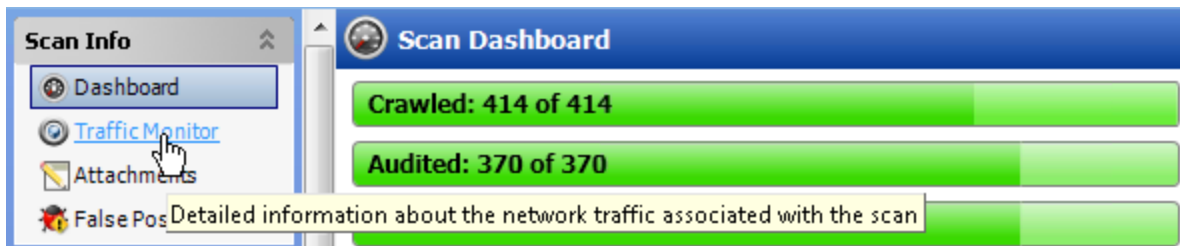
Traffic Viewerの起動

Traffic Viewerは、OpenText DASTとFortify WebInspect Enterpriseで開いているスキャンの中の **スキャン情報(Scan Info)]** パネルから起動できます。この方法でツールを起動すると、トラフィックファイルが表示されたTraffic Viewerが開きます。スキャンの外部でスタンドアロンツールとして、トラフィックやプロキシのデータを表示せずにツールを開くこともできます。

開いているスキャンから

OpenText DASTとFortify WebInspect Enterpriseで開いているスキャンからTraffic Viewerを起動するには:

- [スキャン情報 (Scan Info)] パネルで **Traffic Monitor** をクリックします。



注記: スキャンを行う前に **Traffic Monitorログ(Traffic Monitor Logging)** を有効にしないと、Traffic Viewerは使用できません。

スタンドアロンツールとして

スタンドアロンのTraffic Viewerを起動するには、次のいずれかの操作を実行します:

- OpenText DASTで **ツール(Tools)] > Traffic Viewer** の順にクリックします。
- Fortify WebInspect Enterprise管理コンソールで **ツール(Tools)] > Traffic Viewer** の順にクリックします。

トラフィックやプロキシのデータが表示されていないTraffic Viewerが起動します。

注記: Windowsの **[スタート]** メニューからTraffic Viewerを起動することもできます。

インターフェイスの使用

このセクションでは、既存のファイルを開く方法、サイトツリーの使用方法、グリッドビューと詳細ビューのカスタマイズ方法、ユーザインタフェース(UI)要素のサイズ変更方法、および自動スクロールの使用方法について説明します。

既存のファイルを開く

Traffic Viewerで次のタイプの既存のファイルを開き、セッションを調べることができます。

- トラフィックセッションファイル(.tsf)
- レガシプロキシセッションファイル(.psf)
- Burp Proxyファイル
- HTTPアーカイブ(.har)ファイル

注記: レガシプロキシセッションファイル(.psf)を開くと、Traffic Viewerがそのファイルをトラフィックファイル(.tsf)に変換します。

既存のファイルを開くには:




1. **開く(OPEN)]**をクリックします。
開く(Open)] ダイアログボックスが開きます。
2. ドロップダウンリストから、開くファイルのタイプを選択します。
3. ファイルに移動して開きます。
Traffic Viewerでセッションが表示されます。

サイトツリーの使用

サイトツリーには、デフォルトでは、スキャン中に生成されたすべてのトラフィックのツリービューが、フィルタされていない状態で表示されます。ツリーには、ホストとホスト内のすべてのサブディレクトリのリストが含まれます。このビューでは、最上部のホストを選択してサブディレクトリを展開し、各レベルで発生する要求と応答を確認できます。サイトツリーで項目を選択すると、その項目のトラフィックが表示されます。

サイトツリーのアイコン

次の表では、サイトツリーに表示されるアイコンを説明しています。

アイコン	名前(Name)	表しているもの
	サーバ/ホスト	サイトのツリー構造の最上レベル
	Folder	ディレクトリ
	ページ	ファイル

リソースのトラフィックの表示

サイトツリー内のリソースのトラフィックを表示できます。項目のトラフィックを表示するには:

- **サイトツリー**で項目を選択します。
その項目に関係するすべてのトラフィックが **トラフィック(Traffic)]** グリッドに表示されます。

詳細については、「["セッションの操作" ページ132](#)」を参照してください。

ホスト名 のみの表示

ホスト名 のみのリストを表示するには:

- デフォルト のツリービューで、フィルタアイコンを1回 クリックします。
サイトツリーにホスト名 だけが表示 されます。このビューでは、サブディレクトリにはアクセスできません。このビューから、1つ以上 のホストを選択し、残りを除外 できます。「["選択したホストのフィルタ処理" 下](#)」を参照してください。

ツリー全体の表示に戻るには:

- もう一度フィルタアイコンをクリックします。

選択したホストのフィルタ処理

調査対象を絞り込むために、サイトツリー内の特定のホストをフィルタ処理 できます。選択したホストとそのサブディレクトリのみをサイトツリーに表示するには:

1. サイトツリーにホスト名 だけが表示されている状態で、表示するホストを1つ以上 選択します。
2. フィルタアイコンをクリックします。
選択したホストだけがサイトツリーに表示 されます。
3. ホストを展開して、そのサブディレクトリを表示 します。

すべてのホスト名 の表示

すべてのホスト名 の表示に戻るには:

1. フィルタアイコンをクリックします。
サイトツリーに、以前に表示した選択済みのホストのホスト名 だけが表示 されます。
2. 選択済みの各ホストをクリックして、それぞれの選択を解除 します。
3. フィルタアイコンをクリックします。
フィルタ処理されていないツリービューがサイトツリーに表示 され、すべてのトラフィックが表示 されます。

参照情報

["UI要素のサイズ変更、折りたたみ、および展開" ページ130](#)

グリッドビューのカスタマイズ

グリッドビューに表示される列のサイズ変更、位置変更、追加、および削除 ができます。

列のサイズ変更

列のサイズを変更するには:

1. サイズを変更する列見出しの右側の境界にカーソルを移動します。
カーソルが両矢印になり、列見出しの背景色が薄い灰色に変わります。

Host ▼	Port ▼	Path ▼	Method ▼	Status
zero.webappsecurity.com	80	/docs/api/index.html?org/apache/catalina/websocket/V	GET	200
zero.webappsecurity.com	80	/account/	GET	500

2. 次のいずれかを実行します。
 - 必要な幅になるまで、列の境界を右または左にドラッグします。
 - 境界をダブルクリックすると、列のサイズは列内で最も幅広のデータの幅になります。
ウィンドウの下部に水平スクロールバーが追加されることがあります。

列の位置変更

グリッドで列の順序を変更するには:

1. 移動する列見出しにカーソルを移動します。
列見出しの背景色が薄い灰色に変わります。
2. 1回クリックします。
列見出しの背景色が白に変わります。
3. 目的の位置まで列を右または左にドラッグします。

Request Start ▲ ▼	Host ▼	Port ▼	Path ▼
11/28/2017 10:58:00.477	zero.webappsecurity.com	80	/docs/api/index.html?org/apache/catalina/websocket/V
11/28/2017 10:30:50.353	zero.webappsecurity.com	80	/account/

データの列が移動し、残りの列は右または左に1列分移動します。

列の追加/削除

デフォルトでは、すべてのデータ列がグリッドに表示されるわけではありません。グリッドビューの設定で、グリッドに表示するデータ列を選択できます。表示する列を追加または削除するには:

1. グリッドビューで⚙️をクリックします。
使用可能な列のリストが表示されます。

注記: 列名はスキャン時に生成されるメモヘッダを示します。

2. 次の操作を実行します。
 - 表示に追加する各列のチェックボックスをオンにします。
 - 表示から削除する各列のチェックボックスをオフにします。


3. 列のリスト外の任意の場所をクリックして、リストを閉じます。
表示列が更新されます。

詳細ビューのカスタマイズ

グリッド以外の詳細ビューのレイアウトとカラーテーマを選択したり、[HTTP] 詳細ビューの表示と非表示を切り替えたりすることができます。


レイアウトの変更

要求(Request)] 詳細ビューと 応答(Response)] 詳細ビューなど、ある項目に対して2つの詳細ビューが表示されている場合は、それらの詳細ビューの配置を並べ替えて、縦(上下)に重ねたり、水平方向(横並び)に配置したりすることができます。レイアウトを変更するには:

1. 詳細ビューで  をクリックします。
設定メニューが開きます。
2. 次のいずれかを実行します。
 - 詳細ビューを縦(上下)に並べるには、**縦レイアウト(Vertical Layout)]** をクリックします。
 - 詳細ビューを横に並べるには、**横レイアウト(Horizontal Layout)]** をクリックします。

カラーテーマの変更

デフォルトのカラーテーマは、白のバックグラウンドに黒および色付きのテキストです。ただし、黒のバックグラウンドに白と色付きのテキストを使用することもできます。カラーテーマを変更するには:

1. 詳細ビューで  をクリックします。
2. 次のいずれかを実行します。
 - 白いバックグラウンドに黒と色付きのテキストを使用するには、**淡色テーマ(Light Theme)]** をクリックします。
 - 黒いバックグラウンドに白と色付きのテキストを使用するには、**濃色テーマ(Dark Theme)]** をクリックします。

[HTTP] 詳細ビューの表示と非表示

要求(Request)] または 応答(Response)] 詳細ビューなど、[HTTP] 詳細ビューの1つを折りたたむ(または非表示にする)ことで、他の [HTTP] 詳細ビューの内容のみを表示することができます。

詳細ビューを非表示にするには:

- 詳細ビューの非表示アイコン(⌵)をクリックします。

非表示の詳細ビューを表示するには:

- 表示アイコン(▼)をクリックします。

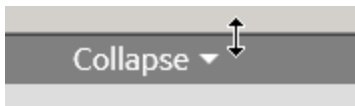
UI要素のサイズ変更、折りたたみ、および展開

サイトツリーやデータのグリッドビューなど、特定のユーザインタフェース(UI)要素については、サイズを変更したり、非表示(折りたたむ)にしたり表示(展開)したりすることが可能です。

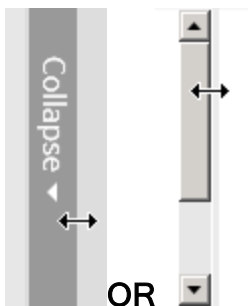
要素のサイズ変更

要素のサイズを変更するには、次のいずれかの操作を実行します:

- グリッドビューなど、水平のデータレイアウトになっているUI要素の場合は、**折りたたみ(Collapse)**] 水平バーをドラッグして、要素の幅を広げたり狭めたりします。



- サイトツリーなど、垂直のデータレイアウトになっているUI要素の場合は、**折りたたみ(Collapse)**] 垂直バーまたはスクロールバーをドラッグして、パネルの幅を広げたり狭めたりします。



要素の折りたたみ

要素を折りたたむには:

- **折りたたみ(Collapse)**]をクリックします。

要素の展開

要素を展開するには:


- **展開(Expand)**]をクリックします。

自動スクロールの使用

自動スクロールを有効にしている場合、新しいセッションが追加されるとトラフィックグリッドが上にスクロールし、常に最新のトラフィックセッションが表示されます。自動スクロール機能は、現在実行中のスキャンを操作しているときにのみ適用されます。


自動スクロールの有効化

自動スクロールを有効にするには:

- スクロールロックアイコン()をクリックします。

自動スクロールの無効化

【トラフィック(Traffic)】グリッドでセッションを調べるために、自動スクロールを一時停止できます。自動スクロールを無効にするには:

- スクロールロックアイコン()をクリックします。

注記: アクティブスキャン中はいつでも自動スクロールを再開できます。

トラフィックの操作

このセクションでは、トラフィックを探索する方法、セッションとパラメータを操作する方法、トラフィックデータの検索とフィルタの方法、正規表現を使用する方法を説明します。

トラフィックの探索

デフォルトでは、スキャン中に生成されたすべてのトラフィックが【トラフィック(Traffic)】グリッドに表示され、スキャン全体のトラフィックを探索できます。ただし、特定のリソースのトラフィックを表示および探索することもできます。【トラフィック(Traffic)】グリッド内のデータを検索、ソート、およびフィルタ処理できます。詳細については、「["検索とフィルタ処理" ページ136](#)」を参照してください。

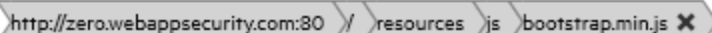
リソースのトラフィックの表示

サイトツリー内のリソースのトラフィックを表示できます。項目のトラフィックを表示するには:

- **サイトツリー**で項目を選択します。
その項目に関係するすべてのトラフィックが【トラフィック(Traffic)】グリッドに表示されます。

ブレッダラムリンクの使用

サイトツリーでリソースを選択すると、ここに示すサンプルのようにブレッダラムリンクがトラフィックグリッドの上部に表示されます。



これらのブレッダラムリンクは、ブレッダラムリンクにリストされている最後のリソースのトラフィックのみをフィルタ処理して表示していることを示しています。

一連のブレッダラムリンクの他の位置にリストされている特定のリソースのトラフィックをフィルタ処理するには:

- ブレッダラムリンク内のリソースをクリックします。

たとえば、前のイメージに表示されているresourcesフォルダのすべてのトラフィックを表示する場合は、[resources]をクリックします。

選択したリソースが最後のブレッダラムリンクになり、トラフィックセッションが更新されて、選択したリソースのトラフィックのみが表示されます。

フィルタを完全に削除するには:

- ブレッダラムリンクの末尾の [X] をクリックします。
ブレッダラムリンクが削除され、トラフィックセッションがフィルタ処理されなくなります。

参照情報

["セッションの操作" 下](#)

["トラフィックデータのドリルダウン" ページ135](#)

セッションの操作

スキャンのトラフィックファイルに表示されているデータを変更することはできません。ただし、Traffic Viewerでトラフィックデータを調査して、スキャン中に起きたことについての理解を深めることはできます。たとえば、HTTP Editorを使用して要求を再送信したり、ブラウザでセッションを表示したりすることができます。

HTTP詳細の表示

セッションの要求と応答は、[HTTP] 詳細ビューで見ることができます。このビューは、ほとんどのグリッドで選択されるセッションのデフォルトビューです。ただし、別の詳細ビューが表示されているときに、その代わりに要求と応答を表示する場合は、[HTTP] 詳細ビューに切り替えます。[HTTP] 詳細ビューでセッションを表示するには:

1. グリッドでセッションを選択します。
2. [HTTP] をクリックします。
[HTTP] 詳細ビューが開き、選択したセッションの要求と応答が表示されます。

テキストの折り返し

要求(Request)詳細ビューや 応答(Response)詳細ビューなどの詳細ビューでは、テキスト行が長いと、水平スクロールバーを使用しないではコンテンツを確認できないことがあります。折り返し(Word Wrap)設定を使用してテキストを折り返せば、水平スクロールバーは表示されません。折り返し(Word Wrap)設定は詳細ビューごとに設定できるものであり、すべての詳細ビューに対するグローバルな設定ではありません。折り返し(Word Wrap)設定は、ユーザ設定ファイルに詳細ビューごとに保存され、次回アプリケーションを開くときにその詳細ビューのデフォルト動作となります。

テキストを折り返すには:

- 詳細ビューを右クリックし、**折り返し(Word Wrap)]**を選択します。
長いテキスト行が折り返され、水平スクロールバーがなくなります。

パーセントエンコード文字のデコード

デフォルトで、要求と応答では予約文字にパーセントエンコーディングが使用されています。要求または応答のテキストに%3Bや%40などのパーセントエンコード文字がある場合は、これらの文字をデコードして、テキストを読みやすくすることができます。要求または応答の文字をデコードすると、選択したセッションのすべての親セッションと子セッションの要求または応答もデコードされます。これらの文字がデコードされた状態に保たれるのは、スキャンが開いている間だけです。スキャンを閉じて再度開くと、デフォルトの表示が適用され、予約文字は再びパーセントエンコードされます。

パーセントエンコード文字をデコードするには:

- **応答(RESPONSE)]**タブまたは **要求(REQUEST)]**タブ内で右クリックして **URLデコード(URL Decode)]**を選択します。
パーセントエンコード文字が、読みやすいテキストに変換されます。

要求の再送信

HTTP Editorを使用して要求を再送信できます。要求を再送信するには:

1. グリッドでセッションを選択して要求と応答を表示します。
2. [HTTP] 詳細ビューが開いていない場合は、[HTTP]をクリックします。
3. **要求(REQUEST)]** 詳細ビューを右クリックして **HTTP Editorで表示(View in HTTP Editor)]**を選択します。

要求に対してHTTP Editorが開きます。HTTP Editorの使用法について詳しくは、HTTP EditorのオンラインヘルプまたはOpenText™ Dynamic Application Security Testingツールガイドの「HTTP Editor」の章を参照してください。

ブラウザでのセッションの表示

[ブラウザ(Browser)] 詳細ビューでセッションを表示して、サイト内のどこでトラフィックが発生したかを確認できます。[ブラウザ(Browser)] でセッションを表示するには:

1. グリッドでセッションを選択します。
2. **ブラウザ(BROWSER)]**をクリックします。
ブラウザ(Browser)] 詳細ビューが開き、選択したセッションが表示されます。

圧縮コンテンツの展開

コンテンツを圧縮(または軽量化)すると、コードからスペース、改行マーカー、コメント、およびブロック区切り記号が削除され、ファイルサイズが小さくなります。しかしこの方法では、コンテンツが人間にとって読みにくいものになります。美化(Beautify)] 設定を使用すれば、圧縮されたテキストを展開できます。美化(Beautify)] 設定は詳細ビューごとに設定できるものであ

り、すべての詳細ビューに対するグローバルな設定ではありません。美化(Beautify)]設定は、ユーザ設定ファイルに詳細ビューごとに保存され、次回アプリケーションを開くときにその詳細ビューのデフォルト動作として使用されます。

圧縮されたコンテンツを展開するには:

- 詳細ビューで右クリックし、**美化(Beautify)]**を選択します。
圧縮されたコンテンツが展開され、読みやすくなります。

注記: 一部のテキストは美化できないので、このオプションが表示されない場合もあります。

参照情報

["パラメータの使用" 下](#)

パラメータの使用

トラフィックセッションで使用されるパラメータのタイプ、名前、および値を表示できます。【パラメータ詳細(Parameters Detail)]ビューには、トラフィックセッションで使用されるクッキーまたはクエリ文字列ごとに1つのレコードを含むグリッドが表示されます。同じパラメータが使用されているすべてのトラフィックレコードを表示することもできます。【パラメータ(Parameters)]詳細ビューには、トラフィック(Traffic)]グリッドと 関連トラフィック(Related Traffic)]グリッドからアクセスできます。

パラメータについて

パラメータには、次のいずれかを指定できます。

- クッキーデータ
- HTTP要求のURLの一部として送信される(または別のヘッダに含まれる)クエリ文字列
- Postメソッドを使用して送信されるデータ(set_<parametername>など)

パラメータ詳細の表示

セッションのパラメータの詳細を表示するには:

1. トラフィック(Traffic)]グリッドまたは 関連トラフィック(Related Traffic)]グリッドでセッションを選択します。
2. 【パラメータ(PARAMETERS)]をクリックします。

選択したセッションで使用されているパラメータが表示された【パラメータ(Parameters)]詳細ビューが開きます。

注記: 詳細ビューのレイアウト設定は【パラメータ(Parameters)]グリッドには影響しません。

トラフィックグリッドへのパラメータ列の追加

【トラフィック(Traffic)】グリッドに列を追加して、【パラメータ(Parameters)】詳細ビューに一覧にされているパラメータを表示できます。【トラフィック(Traffic)】グリッドにこれらのデータ列を追加しておく、ワークフローマクロを使用しているときに、セッションで状態パラメータを監視して、いつどのような理由でアプリケーションからログアウトされているかを判別する必要がある場合に便利です。

たとえば、JSESSIONIDパラメータの値を表示して各セッションでのこの値を調べ、どこでこの値が変化しているかを確認できます。JSESSIONIDパラメータの列を、それに付随する列set_JSESSIONIDと一緒に追加して、値が変化しているところを示すことができます。

パラメータの列を追加するには:

1. 【パラメータ(Parameters)】詳細グリッドで、パラメータの行を右クリックします。
2. **列の作成...(Build Columns...)**を選択します。

注記: 選択したパラメータの列を以前に追加したことがある場合、**列の作成(Build Columns)**オプションは使用できません。

パラメータ名の列が、パラメータ値を設定するメソッドの列(該当する場合)と共に、【トラフィック(Traffic)】グリッドに追加されます。これらの列は、現在のスキャンのデータベースに永続的に追加されます。これらの列名はグリッド設定メニューにも追加されます。グリッド設定メニューを使用して、ビューに列を追加したり削除したりできます。「["列の追加/削除" ページ128](#)」を参照してください。

トラフィックデータのドリルダウン

サイトツリー内のリソースのトラフィックを表示し、ドリルダウンしてセッションの関連トラフィックを【トラフィック(Traffic)】グリッドビューに表示できます。

リソースのトラフィックの表示

サイトツリー内のリソースのトラフィックを表示できます。項目のトラフィックを表示するには:

- **サイトツリー**で項目を選択します。
その項目に関係するすべてのトラフィックが【トラフィック(Traffic)】グリッドに表示されます。

セッションの関連トラフィックの表示

【トラフィック(Traffic)】グリッドでセッションの関連トラフィックを表示できます。

セッションの関連トラフィックを表示するには:

- **【トラフィック(Traffic)】**グリッドでセッションをダブルクリックします。
関連トラフィック(Related Traffic)グリッドが表示されます。親トラフィックセッションが使用可能な場合は、親のリストをクリックして、それらの【HTTP】詳細ビューおよび【ブラウザ(Browser)】詳細ビューを表示できます。

トラフィック(Traffic)] グリッドに戻るには:

- **トラフィック(Traffic)] 垂直タイトルバーをクリックします。**
トラフィック(Traffic)] グリッドが表示され、すべてのトラフィックが表示されます。
詳細については、「["積み重なったグリッドの操作" 下](#)」を参照してください。

積み重なったグリッドの操作

グリッドデータをドリルダウンすると、垂直タイトルバーが付いた新たなグリッドが開きます。グリッドデータの複数の層をドリルダウンすると、垂直タイトルバーが見える状態で新しいグリッドが前のグリッドに重なっていきます。次の例は、積み重なった3つのグリッドを示しています。



注記: すべてのアプリケーションに、上に示すグリッドがすべて含まれるわけではありません。

積み重なったグリッドの表示と終了

重なりの中の特定のグリッドを表示するには、そのグリッド上に重なっているすべてのグリッドを閉じます。また、積み重なったすべてのグリッドを一度に閉じることもできます。

重なりの中の特定のグリッドを表示するには:

- 表示するグリッドのタイトルバーをクリックします。
表示するグリッドの上に積み重ねられたすべてのグリッドが閉じます。

積み重なったすべてのグリッドを閉じるには:

- 左端のグリッドのタイトルバーをクリックします。
積み重なったすべてのグリッドが閉じます。

参照情報

["グリッドビューのカスタマイズ" ページ127](#)


検索とフィルタ処理

グリッドビューとほとんどの非グリッドビューに表示されるデータに対して検索を行うことができます。グリッドに表示される各列でソートとフィルタ処理を行うこともできます。アクティブスキャンを表示している場合は、実行中のスキャンのライブデータを検索したり、フィルタ処理したり、そ

のライブデータでソートしたりすることができます。検索クエリの形式の詳細については、「[検索式について](#)」 [ページ139](#)を参照してください。

グリッドビューでの検索

グリッドに表示される1列のデータまたは複数列のデータを検索できます。グリッドに表示されているデータに対して検索を行うには:

1. 検索アイコン()をクリックします。
2. **検索(Search)]**フィールドに、列名(スペースなし)、演算子、および検索する値を入力します。


例:

```
Status='404 Not Found'  
ResponseStart>'9/4/2015 9:08:52.242 AM'  
Status~'3[0-9][0-9].*'
```

3. (オプション)複数の列に対して検索を行うには、**スペースバー**を押して、次の列名(スペースなし)、演算子、および検索する値を入力します。複数の列に対する検索はAND検索として扱われます。各列に対して指定された検索条件を含むレコードのみが表示されます。検索する各列について、この手順を繰り返します。

例:

```
Method=GET Status~'3[0-9][0-9].*'
```

4. **<Enter>**キーを押すか、をクリックします。


正規表現を使用してグリッド内でパターンを検索することもできます。詳細については、「[検索式について](#)」 [ページ139](#)を参照してください。

非グリッドビューでの検索

要求(Request)]タブや **応答(Response)]**タブなどの非グリッドビューでデータを検索できません。タブで検索するには:

1. グリッド内のデータ行を選択します。
選択したデータの詳細が、**要求(Request)]**タブや **応答(Response)]**タブなどの関連付けられたタブに表示されます。
2. 検索する値をタブ検索フィールドに入力します。
3. (オプション)検索条件で正規表現を使用するには、**RegEx]**チェックボックスを選択します。詳細については、「[検索式について](#)」 [ページ139](#)を参照してください。
4. **<Enter>**キーを押します。

検索のクリア

検索条件をクリアするには、検索アイコンの  をクリックします。

グリッドでのソート

グリッド内の任意の列でソートするには:

- 列見出しをクリックします。

グリッド内のフィルタ処理

グリッド内の1つ以上の列でフィルタ処理するには:

1. 列見出しの▼をクリックします。
列見出しの下にフィルタパネルが表示されます。
2. [フィルタ(filter)]フィールドにフィルタ式を入力します。

フィルタ式は、オプションの演算子(>、<、>=、<=、!=、~、=)か、「in」、「notin」、または「regex」のいずれかの関数と、その後続く文字列で構成されます。範囲演算子(..)は、2つの文字列の間にあるので例外です。詳細については、「["検索式について" 次のページ](#)」を参照してください。

例:

```
443
'400 Bad Request'
30*
'9/3/2015 10:53:08.000 AM'..'9/3/2015 10:53:12.089 AM'
in(200,300) notin(400,500)
```

注記: 等しい(=)演算子は、日時情報を含む列に正確にフィルタを適用しない場合があります。

詳細については、「["グリッド内のフィルタ処理のルール" 下](#)」を参照してください。

3. <Enter>キーを押します。
入力された式に基づいてグリッド内のデータがフィルタ処理されます。フィルタ処理された列見出しのアイコンが▼に変わります。
4. 追加の列でフィルタ処理するには、それらの列ごとにステップ1から3を繰り返します。

グリッド内のフィルタ処理のルール

グリッド内のフィルタ処理には、次のルールが適用されます。

- フィールド名を指定する必要はありません。特定の列でフィルタを編集するので、フィールド名は暗黙的に特定されます。
- [フィルタ(filter)]フィールドでは検索演算子を使用できます。詳細については、「["演算子" ページ141](#)」を参照してください。
- [フィルタ(filter)]フィールドに演算子やワイルドカードが指定されない場合、フィルタはfield:*string*の形式の「contains」句に変換されます。検索が引用符で囲まれている場合、フィルタはfield:'*string*'に変換されます。

たとえば、[ステータス(Status)]列のフィルタ文字列404 Not FoundはStatus: '*404*' Status: '*Not*' Status: '*Found*'に変換され、ステータスが「404」、「Not」、または「Found」を含むすべてのセッションが表示されます。フィルタ結果には、「302 Found」、「404 Not Found」、および「405 Method Not Allowed」などのステータスが含まれると考えられます。

「ステータス(Status)」列のフィルタ文字列 '404 Not Found' はStatus: '*404 Not Found*'に変換され、「404 Not Found」を含んだステータスを持つすべてのセッションが表示されます。

- フィルタフィールドには、複数の検索フィルタをスペースで区切って指定できます。
- 日付と時刻のフィールドのフィルタは、単一引用符(')または二重引用符(")で囲む必要があります。

フィルタされたビューのクリア

グリッド内の1つ以上の列でフィルタされたビューをクリアするには:

1. フィルタ処理された列見出しの▼をクリックします。
検索パネルが列見出しの下に表示されます。
2. **クリア(Clear)**をクリックします。
列内のデータはフィルタ処理されなくなります。
3. 追加の列のフィルタをクリアするには、フィルタ処理された列ごとにステップ1と2を繰り返します。

検索式について

このトピックでは、グリッドおよびタブでの検索に使用される式の構成要素について説明します。

クエリの基本形式

検索クエリの基本形式は次のとおりです。

`<PropertyName><Operator><SearchValue>`

グリッド全体で検索する場合、PropertyNameは検索に含める列名です。要求(Request)]タブや応答(Response)]タブなどのタブで検索する場合、PropertyNameはフィールド/プロパティ名(「Request」や「Response」など)です。

グリッドの1つの列内を検索する場合は、PropertyNameを省略します。このタイプの検索の形式は次のとおりです。

`<Operator><SearchValue>`

検索で正規表現(RegExp)構文を使用するには、次の形式を使用します。

`<PropertyName> RegExp('[RegexSearchValue]','[RegexFlags]')`

正規表現の使用の詳細については、["正規表現の使用" ページ143](#)を参照してください。

単純なクエリ

特殊文字を含まない文字列データや整数の単純なクエリを実行できます。単純なクエリとは次のようなものです。

```
Method=GET
```

```
Scan.CheckId=6
```

 [詳細については、「YouTube™」を参照してください。](#)

スペース文字または特殊文字を含むデータの検索

検索するコンテンツにスペース文字や特殊文字がある場合は、コンテンツを単一引用符 (') または二重引用符 (") で囲みます。

```
Status='404 Not Found'
```

```
Path='/signin.html'
```

 [詳細については、「YouTube™」を参照してください。](#)

引用符をワイルドカードと組み合わせることができます。

```
ResponseStart:*'7/8/2015 4:22: '*
```

複数の式を使用した検索

1つの検索に同時に複数の式を含めることができます。それぞれの式はスペースで区切ります。

```
Path='/banklogin.asp' Method=GET
```

 [詳細については、「YouTube™」を参照してください。](#)

同じフィールドが複数表示されている場合は、「OR」式になります。

```
Path='/banklogin.asp' Path='/login1.asp'
```

この検索では、Pathが「/banklogin.asp」または「/login1.asp」であるすべてのレコードが返されます。

式に追加される他のフィールドは、「AND」式として扱われます。

```
Path='/banklogin.asp' Path='/login1.asp' Method=POST
```

この検索では、Pathが「/banklogin.asp」または「/login1.asp」であり、かつMethodが「POST」であるすべてのレコードが返されます。

AND/OR検索のもう1つの例を次に示します。

```
Method=POST Scan.Engine:Sql* Scan.Engine:Cross*
```

この検索では、Methodが「POST」であり、かつScan.Engineの値の先頭が「Sql」または「Cross」であるすべてのレコードが返されます。

 [詳細については、「YouTube™」を参照してください。](#)

Nullデータの検索

Null (空)エントリを含むデータを検索するには、=演算子を使用し、その後2つの一重引用符(")を入力します。

```
ParameterValue=' '
```

特定の列にnull (空)エントリが含まれているデータをフィルタ処理するには、**列フィルタ (column filter)** フィールドで=演算子を使用し、その後2つの一重引用符(")を入力します。

 [詳細については、「YouTube™」を参照してください。](#)

検索クエリでの列名の使用

スペースを含む列名またはフィールド名で検索する場合、検索クエリではそのスペースは削除します。たとえば、グリッドの **Response End** 列を検索するには、次の形式を使用します。

```
ResponseEnd='7/8/2015 4:22:52 PM'
```

正規表現の使用

パターンを検索するには、正規表現演算子(~)を使用して正規表現を検索に含めることができます。

```
Response~'[0-9].*='
```

 [詳細については、「YouTube™」を参照してください。](#)

正規表現構文を作成することもできます。

```
Response RegExp('[0-9].*=', 'i')
```

正規表現の使用の詳細については、"[正規表現の使用](#)" [ページ143](#)を参照してください。

演算子

次の表では、検索およびフィルタに使用できる演算子と関数について説明しています。例の列で使用されているPropertyNameは、グリッドで検索を行う場合は列名、タブで検索を行う場合はフィールド/プロパティ名になります。列に直接フィルタを適用する場合は、**列フィルタ (column filter)** フィールドにフィールド/プロパティ名を含めないでください。


演算子	説明	例
=	検索文字列に完全一致するもののみを検索	PropertyName=asdf
>	検索数値または日付より大きいデータを検索	PropertyName>123
>=	検索数値または日付より大きいか等しいデータを検索	PropertyName>=123

演算子	説明	例
<	検索数値または日付より小さいデータを検索	PropertyName<123
<=	検索数値または日付より小さいか等しいデータを検索	PropertyName<=123
!=	検索文字列と等しくないデータを検索	PropertyName!=asdf
:	ワイルドカードを使用して検索文字列と完全一致するもののみを検索(検索では大文字と小文字を区別する) 検索文字列にスペースまたはダッシュ(-)が含まれている場合は、単一引用符または二重引用符で囲む必要があります。	PropertyName:asdf (完全一致検索) PropertyName:*asdf (検索文字列で終わるデータを検索) PropertyName:*asdf* (検索文字列を含むデータを検索) PropertyName:asdf* (検索文字列で始まるデータを検索)
..	指定した値の範囲内のデータを検索	PropertyName:'7/15/2015 5:00 PM'..'7/15/2015 5:15 PM'
~	正規表現を使用した検索文字列の検索 正規表現の使用の詳細については、" 正規表現の使用 " 次のページを参照してください。	PropertyName~'sea[a-z]ches'
in	括弧で囲まれた検索値に一致するものを検索(複数の値を検索するには、カンマ区切りのリストを括弧で囲む)  詳細については、「 YouTube™ 」を参照してください。	PropertyName in(123,456)または PropertyName in(abc,def) Port in(80,443) (ポートが80または443のすべてのセッションを検索) Method in(GET) (「GET」メソッドを使用するすべてのセッションを検索)
notin	括弧で囲まれた検索値以外のすべてを検索(複数の値を除外するには、カンマ区切りのリストを括弧で囲む)  詳細については、「 YouTube™ 」を参照してください。	PropertyName notin(123,456)または PropertyName notin(abc,def) Port notin(80,443) (ポートが80または443のすべてのセッションを除外) Method notin(GET) (「GET」メソッドを使用するすべてのセッションを除外)

正規表現の使用

チルダ(~)演算子を正規表現で使用すると、チルダの左側にあるものが、右側の正規表現を使用して検索されます。さらに複雑な正規表現(RegExp)構文を作成することもできます。

検索できるトラフィック文字列プロパティ

正規表現を使用して、任意のトラフィック文字列プロパティ(数値、文字列、または日付)を検索できます。これには、[トラフィック(Traffic)]グリッドビューの設定アイコン()をクリックすると一覧表示されるフィールドすべてが含まれます。

チルダ(~)演算子の使用

チルダ(~)演算子を使用する場合、形式は次のようになります。

`<PropertyName>~'RegexPattern'`

一重引用符または二重引用符を使用できます。

例

次のクエリは、要求ヘッダ内のRefererにindex.jspファイルが指定されているセッションのリストを返します。

```
Request~'Referer:\\s.+\\/index\\.\\.jsp'
```

次のクエリは、応答ヘッダ内のLocationにindex.phpファイルまたはindex.htmlファイルが指定されているセッションのリストを返します。

```
Response~'Location:\\s.+\\/index\\.\\. (php|html)'
```

次のクエリは、「Cross」または「Sql」で始まる名前の監査エンジンによって攻撃された、index.htmlファイルまたはindex.phpファイルを使用するセッションのリストを返します。

```
Path~'\\/index\\. (html|php)' Scan.Engine~'^ (Cross|Sql)'
```

RegExp構文の使用

RegExp構文はJavaScriptに似ており、次の形式を使用します。

`<PropertyName> RegExp('RegexPattern')` -大文字と小文字を区別して検索を実行します

`<PropertyName> RegExp('RegexPattern','i')` -大文字と小文字を区別しないで検索を実行します

例

次のクエリは、要求ヘッダ内のRefererにindex.jspファイルが指定されているセッションのリストを返します。

```
Request RegExp('Referer:\\s.+\\/index\\.\\.jsp','i')
```

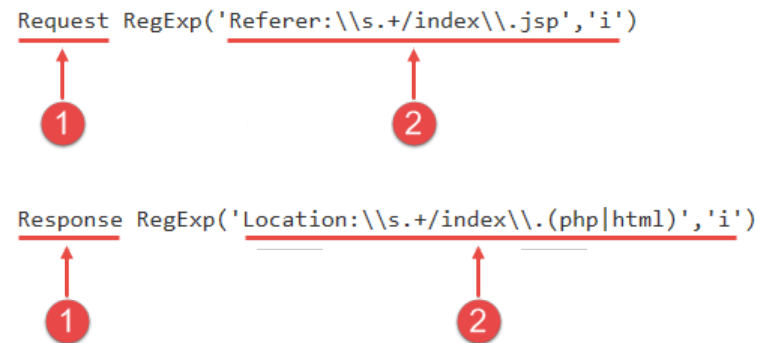

次のクエリは、応答ヘッダ内のLocationにindex.phpファイルまたはindex.htmlファイルが指定されているセッションのリストを返します。

```
Response RegExp('Location:\\s.+ /index\\.(php|html)', 'i')
```

詳細については、「YouTube™」を参照してください。

RegExp構文について

次の図で、RegExp構文の各部の意味を説明します。



項目	説明
1	生のHTTP要求データを検索するのか、生のHTTP応答データを検索するのかを指定します(ヘッダデータと本文データの両方を含みます)
2	次の表に示す正規表現文字を使用して、検索する正規表現パターンを定義します

正規表現

正規表現のパターンは、特殊な文字やシーケンスを使用して作成されます。次の表に、これらの文字の一部を示し、その簡単な使用例を示します。推奨する他の参照先として「Regular Expression Libraryオンライン」(<http://regexlib.com/Default.aspx>)があります。

文字	説明
\\	次の文字を特殊文字としてマークします。/n/は文字「n」に一致します。シーケンス\\n/は、改行文字に一致します。
^	入力または行の先頭に一致します。 文字クラスとともに使用すると、否定文字を意味します。たとえば、contentディレクトリ内の/content/enおよび/content/caを除くすべてを除外するには、/content/[^(en ca)].*.*を使用します。\\S \\D \\Wも参照してください。

文字	説明
\$	入力または行の末尾に一致します。
*	先行する文字の0回以上の反復と一致します。/zo*/は「z」とも「zoo」とも一致します。
+	先行する文字の1回以上の反復と一致します。/zo+/は「zoo」に一致しますが、「z」には一致しません。
?	先行する文字の0回または1回の出現と一致します。/a?ve?/は「never」の「ve」に一致します。
.	改行文字を除く任意の1文字に一致します。
	2つ以上のリテラルテキスト検索語句の間のORを示します。たとえば、次のクエリは、パスに/index.htmlか/index.phpが含まれているセッションのリストを返します。 Path~/index\.(html php)'
i	大文字と小文字を区別しません。この文字は、RegExpの2番目の引数で使 用します。例： PropertyName RegExp('stuff[abc]','i') これを、他のフラグと組み合わせることができます。例： PropertyName RegExp('stuff[abc]','mi')
m	複数行モードで検索します。この文字は、RegExpの2番目の引数で使 用します。例： PropertyName RegExp('stuff[abc]','m') これを、他のフラグと組み合わせることができます。例： PropertyName RegExp('stuff[abc]','mi')
[xyz]	文字セット。括弧内の任意の1文字に一致します。/[abc]/は「plain」の「a」に 一致します。
\b	スペースなどの単語境界に一致します。/ea*\b/は、「never early」の「er」に一致 します。
\B	単語以外の境界に一致します。/ea*\B/は「never early」の中の「ear」と一致し ます。
\d	1つの数字に一致します。[0-9]と同じです。

文字	説明
\D	数字以外の1文字に一致します。[^0-9]と同じです。
\f	改ページ文字に一致します。
\n	改行文字に一致します。
\r	キャリッジリターン文字に一致します。
\s	スペース、タブ、改ページなどの空白に一致します。[\f\n\r\t\v]と同じです。
\S	空白文字以外の文字に一致します。[^ \f\n\r\t\v]と同じです。
\w	アンダースコアを含む任意の単語文字に一致します。[A-Za-z0-9_]と同じです。
\W	英数字以外の文字に一致します。[^A-Za-z0-9_]と同じです。

Traffic Viewerプロキシ

このセクションでは、プロキシモードを開始する方法、新しいプロキシファイルを作成する方法、Traffic Viewerのプロキシ設定を行う方法を説明します。

Traffic Viewerプロキシの使用

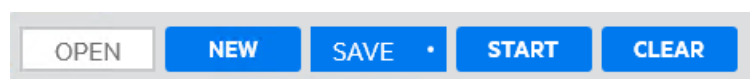
プロキシモードのTraffic Viewerを使用して新しいプロキシファイルを作成できます。このファイルはトラフィックファイルかマクロとして保存できます。たとえば、Webサイトのログインプロセスを記録し、キャプチャされたデータをログインマクロとして保存できます。

プロキシモードの開始

プロキシモードを開始するには、次のいずれかの操作を実行します。

- 開いているスキャンからトラフィックデータを表示しているときに **新規(NEW)**をクリックします。
- ツール(Tools)**メニュー(またはFortify WebInspect Enterpriseのツールキット)からTraffic Viewerを起動した後、以前に記録されたプロキシファイルを表示する場合は **開く(OPEN)**をクリックし、新しいプロキシファイルを作成する場合は **新規(NEW)**をクリックします。

ウィンドウの上部にプロキシツールのボタンが表示されます。



新しいプロキシファイルの作成

新しいプロキシファイルを作成するには:

1. **NEW]**をクリックします。
ウィンドウの上部にプロキシツールのボタンが表示されます。
2. プロキシファイルの記録を開始するために、**開始(START)]**をクリックします。
3. **参照(BROWSE)]**をクリックします。
ツールがTruClientをFirefoxブラウザで起動します。
4. ブラウザで、プロキシファイルで見たいサイトの部分まで移動します。
Traffic Viewerのグリッドに、プロキシ経由のトラフィックが入ります。
5. 終了したら **停止(STOP)]**をクリックします。
6. 次のいずれかを実行します。
 - プロキシファイルをトラフィックファイル(.tsf)として保存するには、**保存(SAVE)]**をクリックします。
 - プロキシファイルをマクロ(.webmacro)として保存するには、**保存(SAVE)]**ドロップダウンメニューをクリックし、**マクロとして(as Macro)]**を選択します。

プロキシリスナの設定

プロキシリスナは、ブラウザからの着信接続をリスンするローカルHTTPプロキシサーバです。プロキシリスナの設定は設定ページで行います。をクリックして設定にアクセスします。

プロキシリスナを設定するには:


- **全般(GENERAL)]**エリアでプロキシリスナの **ローカルIPアドレス(Local IP Address)]**と **ポート(Port)]**番号を入力します。

注記: デフォルトでは、プロキシはlocalhost (IPアドレス127.0.0.1)とポート8080を使用しますが、これは必要に応じて変更できます。

自分のホスト上のWeb Proxyを別のホストで使用するようには、ローカルIPアドレスの値を変更する必要があります。デフォルトのアドレスである127.0.0.1は、外部ホストでは使用できません。この値をワークステーションの現在のIPアドレスに変更すれば、リモートステーションでそのワークステーションをプロキシとして使用できます。

プロキシとWebブラウザの両方で同じIPアドレスとポートを使用する必要があります。プロキシモードで **ブラウズ(Browse)]** ボタンを使用すると、これらの設定がブラウザに自動的に適用されます。Traffic Viewerの外部でブラウザを起動する場合、この設定は適用されません。

プロキシの設定

プロキシ設定はアプリケーション設定で行います。をクリックして設定にアクセスします。

プロキシを設定するには:


1. **プロキシ(PROXY)]** セクションでオプションを選択します。次の表で、オプションについて説明します。

オプション	説明
直接接続(プロキシ無効)(Direct Connection (proxy disabled))	プロキシサーバを使用しない場合は、このオプションを選択します。
プロキシ設定の自動検出(Auto detect proxy settings)	WPAD (Web Proxy Autodiscovery)プロトコルを使用してプロキシ自動設定ファイルを探し、ブラウザのWebプロキシ設定を行います。
システムのプロキシ設定を使用する(Use System proxy settings)	ローカルマシンからプロキシサーバ情報をインポートします。
Firefoxプロキシ設定を使用する(Use Firefox proxy settings)	Firefoxからプロキシサーバ情報をインポートします。 注記: ブラウザのプロキシ設定を使用しても、プロキシサーバ経由でインターネットにアクセスできる保証はありません。Firefoxブラウザの接続設定が プロキシを使用しない] に設定されている場合、プロキシサーバは使用されません。
PACファイルを使用してプロキシを設定する(Configure proxy using a PAC file)	PACファイルURL(PAC File URL)] フィールドで指定した場所にあるPAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードします。
プロキシ設定を明示的に行う(Explicitly configure proxy settings)	プロキシを設定するには、以下の情報を提供します: a. プロキシサーバを経由するTCPトラフィックを処理するためのプロトコルのタイプ(Socks4、Socks5、または標準)を、 タイプ(Type)] リストから選択します。 b. 認証が必要な場合は、 認証タイプ(Authentication Type)] リストから次のいずれかのタイプを選択します。 <ul style="list-style-type: none">○ 自動○ 基本○ ダイジェスト

オプション	説明
	<ul style="list-style-type: none"> ◦ Kerberos ◦ ネゴシエート(Negotiate) ◦ NTLM (NT LAN Manager) <p>c. サーバ(Server)]フィールドにプロキシサーバのURLまたはIPアドレスを入力し、続いて(ポート(Port)]フィールドに)ポート番号(8080など)を入力します。</p> <p>d. プロキシサーバが認証を要求する場合は、 ユーザ名(User Name)]フィールドと パスワード(Password)]フィールドに資格情報を入力します。</p> <p>e. 特定のIPアドレス(内部テストサイトなど)にアクセスするためにプロキシサーバを使用する必要がない場合は、 プロキシをバイパスするサイト(Bypass Proxy For)]フィールドにアドレスまたはURLを入力します。エントリを区切る場合は、カンマを使用します。</p>

2. **保存(SAVE)]**をクリックします。

クライアント証明書の設定

クライアント証明書の設定はTraffic Viewerのプロキシ設定で行います。をクリックして設定にアクセスします。

クライアント証明書を有効にし、使用する証明書を指定するには:


1. **クライアント証明書(CLIENT CERTIFICATES)]**エリアで **クライアント証明書を有効にする(Enable Client Certificates)]**を選択します。
2. 使用する証明書の **証明書ストア(Certificate Store)]**を選択します。オプションは次のとおりです。
 - **ローカルマシン(Local Machine)]**-コンピュータのローカルにあり、コンピュータ上のすべてのユーザに対してグローバルな証明書ストア。
 - **現在のユーザ(Current User)]**-コンピュータ上の現在のユーザアカウントのローカルにある証明書ストア。

注記: 共通アクセスカード(CAC)リーダで使用される証明書はユーザ証明書であり、現在のユーザ(Current User)]に保管されます。

3. 次のいずれかを実行します。
 - 「個人」(「マイ」)証明書ストアから証明書を選択するには、ドロップダウンリストから **マイ(My)]**を選択します。

- 信頼されたルート証明書を選択するには、ドロップダウンリストで **【ルート(Root)】** を選択します。
4. Webサイトは共通アクセスカード(CAC)リーダを使用しますか?
- 「はい」の場合は、次の手順を実行します。
 - i. **証明書(Certificate)】** リストから、「(SmartCard)」というプレフィクスが付いた証明書を選択します。
選択した証明書に関する情報とPINフィールドが **証明書情報(Certificate Information)】** エリアに表示されます。
 - ii. PINが必要な場合は、**【PIN】** フィールドにCACのPINを入力します。
 - iii. **テスト(Test)】** をクリックします。
正しいPINを入力した場合は、成功メッセージが表示されます。
 - 「いいえ」の場合は、**証明書(Certificate)】** リストから証明書を選択します。
選択した証明書に関する情報が **証明書(Certificate)】** リストの下に表示されます。
5. **保存(SAVE)】** をクリックします。

プロキシ除外の設定

イメージファイルやPDFなどの特定のタイプのファイルをプロキシデータに含めたくない場合があります。それらは記録の対象から除外することができます。これらのファイルを除外すれば、メッセージの本文から不要なものを取り除かれて、HTTP要求/応答の行とヘッダに集中することができます。これらのファイルはTraffic Viewerのプロキシ設定で除外します。 をクリックして設定にアクセスします。

ファイルタイプを除外するには:


1. **記録しない(DO NOT RECORD)】** エリアで正規表現を使用してプロキシファイルへのキャプチャから除外するファイル拡張子を入力します。
例:
.jpg\$,.png\$,*.bmp\$
詳細については、「["正規表現の使用" ページ143](#)」を参照してください。
2. **保存(SAVE)】** をクリックします。

検索および置換の設定

検索および置換では、プロキシを経由して到着するHTTPメッセージ内のテキストや値の検索と置換のためのルールを作成できます。この機能は、攻撃のシミュレーションを自動的に行うための非常に柔軟なツールを提供します。推奨される用途は次のとおりです。

- ユーザ名やパスワードなどの機密データのマスク
- 各要求へのクッキーの追加

- Accept要求ヘッダフィールドを変更して、応答で許可されるメディアタイプを追加または削除する
- 要求URI内の変数をクロスサイトスクリプティング攻撃に置換する

検索および置換の設定はTraffic Viewerのプロキシ設定で行います。をクリックして設定にアクセスします。

テキストの検索と置換

要求または応答のテキストを検索して置き換えるには:

1. **ADD**をクリックします。
デフォルトのエントリが表に追加されます。
2. そのエントリの **検索場所(Search On)** 列をダブルクリックします。
3. ドロップダウン矢印をクリックして、検索するメッセージエリアを選択します。オプションは次のとおりです。
 - RequestFull -要求メッセージ全体で検索と置換を行います。
 - RequestHeader -要求ヘッダの中だけで検索と置換を行います。
 - RequestBody -要求本文の中だけで検索と置換を行います。
 - ResponseFull -応答メッセージ全体で検索と置換を行います。
 - ResponseHeader -応答ヘッダの中だけで検索と置換を行います。
 - ResponseBody -応答本文の中だけで検索と置換を行います。次の図は応答メッセージの各部分を示しています。

RESPONSE

1

HTTP/1.1 302 Object moved
Date: Wed, 08 Jul 2015 20:22:39 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Location: banklogin.asp
Content-Length: 134
Content-Type: text/html
Cache-control: private

2

<head><title>Object moved</title></head>

<body><h1>Object Moved</h1>This object may be found here

項目	説明
1	応答ヘッダ
2	応答本文

4. **検索対象(For)]** 列には、検索するデータ(またはデータを表す正規表現)を入力します。
5. **置換データ(Replace With)]** 列に、見つかったデータを置き換えるデータを入力します。

注記: 検索対象(For)] 列や 置換データ(Replace With)] 列で正規表現を使用するには、**Regex]** チェックボックスを選択します。「["ルールでの正規表現の使用" 下](#)」を参照してください。

6. 検索ルールを追加で作成するには、ステップ1-5を繰り返します。
7. **保存(SAVE)]** をクリックします。

ルールでの正規表現の使用

注意! このセクションは、正規表現構文の作成経験を持つ上級ユーザのみを対象としています。

上級ユーザは、**検索対象(For)]** 列と **置換(Replace With)]** 列の両方で正規表現を使用して検索と置換のルールを設定できます。たとえば、正規表現を使用してResponseBodyで(<return>)([^<]+)(</return>)を検索して見つかったデータを\$1<![CDATA[\$2]]>\$3に置き換えるルールを有効にすると、この検索ルールにより、以下に示す変更が加えられることになります。

This Response Value...	Is Replaced With this Value...
<pre> HTTP/1.1 200 OK Date: Fri, 31 Jul 2015 14:22:40 GMT Server: Apache/2.0.63 (Win32) DAV/2 mod_auth_sspi/1.0.4 PHP/5.2.5 mod_ssl/2.0.63 OpenSSL/0.9.7m X-Frame-Options: SAMEORIGIN X-Powered-By: PHP/5.2.5 X-Token: CX45865478 Content-Length: 207 Keep-Alive: timeout=15, max=98 Connection: Keep-Alive Content-Type: application/xml <?xml version="1.0" encoding="UTF-8"?> <Data xmlns="http://scanme/serv001"> <Body> <testResponse> <result>return</result> <return>222</return> </testResponse> </Body> </Data> </pre>	<pre> HTTP/1.1 200 OK Date: Fri, 31 Jul 2015 14:22:40 GMT Server: Apache/2.0.63 (Win32) DAV/2 mod_auth_sspi/1.0.4 PHP/5.2.5 mod_ssl/2.0.63 OpenSSL/0.9.7m X-Frame-Options: SAMEORIGIN X-Powered-By: PHP/5.2.5 X-Token: CX45865478 Content-Length: 207 Keep-Alive: timeout=15, max=98 Connection: Keep-Alive Content-Type: application/xml <?xml version="1.0" encoding="UTF-8"?> <Data xmlns="http://scanme/serv001"> <Body> <testResponse> <result>return</result> <return><![CDATA[222]]></return> </testResponse> </Body> </Data> </pre>

詳細については、「["正規表現の使用" ページ143](#)」を参照してください。

ルールの適用

要求/応答ルールは表示されている順序で順次適用されます。たとえば、あるルールがHTTPSをSSLに変更し、その後に続くルールがSSLをSECUREに変更する場合は、結果的にHTTPSがSECUREに変更されます。

ルールの有効化

ルールを有効にするには:

1. 有効にするルールの **有効(Enabled)]** チェックボックスをオンにします。
2. **保存(SAVE)]** をクリックします。

ルールの無効化

ルールを削除せずに無効にするには:

1. 無効にするルールの **有効(Enabled)]** チェックボックスをオフにします。
2. **保存(SAVE)]** をクリックします。

ルールの削除

ルールを削除するには:

1. 削除するルールを選択します。
2. **削除(REMOVE)]** をクリックします。
3. **保存(SAVE)]** をクリックします。

ルールの編集

ルールを編集するには:

1. **検索場所(Search On)]** 列、**検索対象(For)]** 列、または **置換データ(Replace With)]** 列のエントリをクリックします。
2. データを変更します。
3. **保存(SAVE)]** をクリックします。

第14章:Web検出

Web Discoveryを使用すると、エンタープライズ環境内で開いているすべてのホストを検索できます。

仕組み

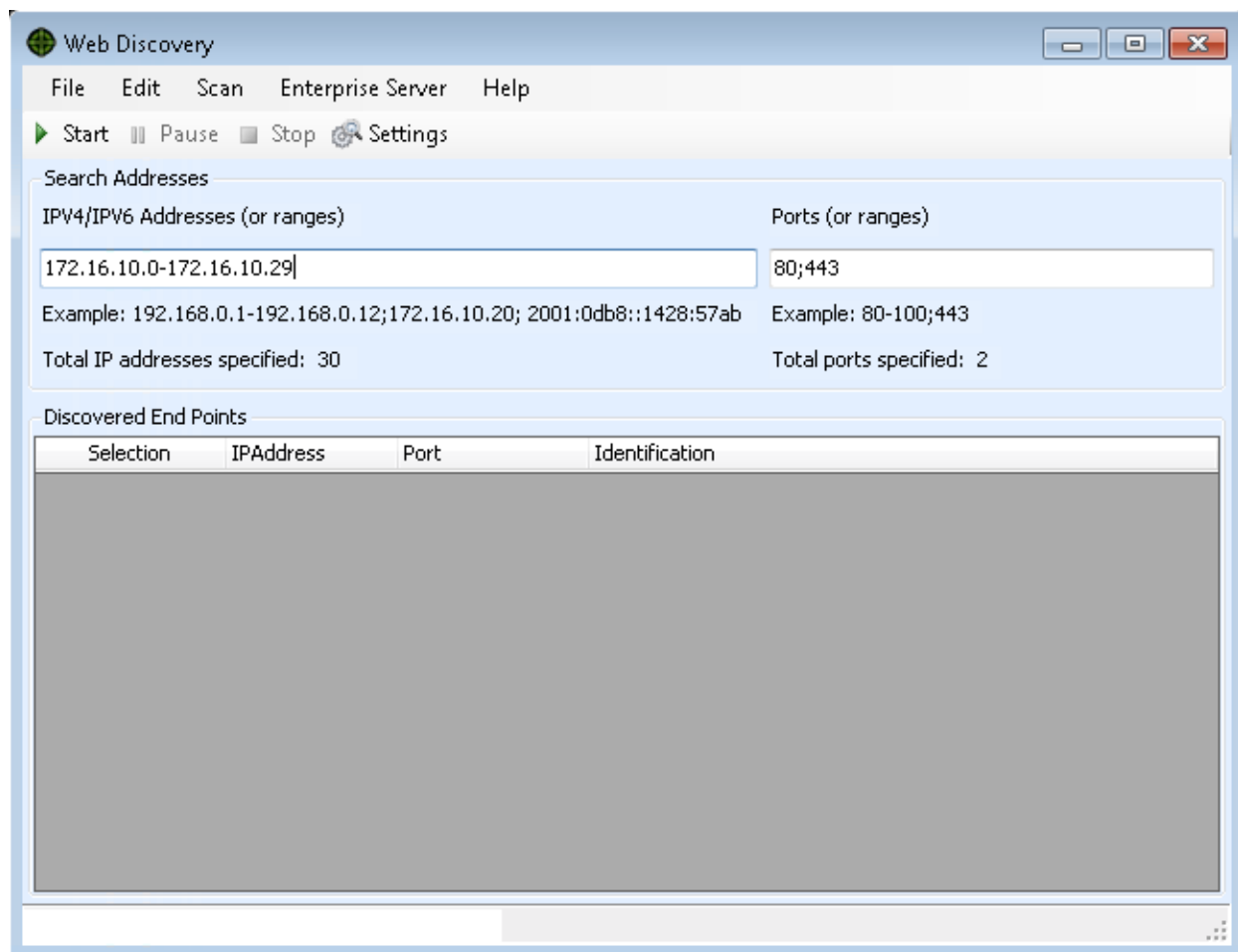
Web Discoveryは(指定されたIPアドレスとポートの範囲内の)すべてのオープンポートにパケットを送信し、サーバ応答を調べて特定の情報を検索し、結果を表示します。Web Discoveryには、Web ServerとSSL Web Serverという事前定義された2つのパケットが含まれています。これらの両方に、次のHTTP要求が含まれています。

GET / HTTP/1.0

Web Discoveryは、HTTP応答を調べて文字列「HTTP」を検索し、その文字列が見つかったら、そのIPアドレス、ポート番号、および「WebServer」というテキストを表示し、さらにその後に、サーバの名前とバージョン番号を明示するように設計された正規表現検索の結果を表示します。

検出されたサーバのリストをテキストファイルに保存できます。

Web Discoveryツールのイメージ



サイトの検出

Web Discoveryを実行してサイトを検出するには:

1. **[IPv4/IPv6アドレス(または範囲)(IPv4/IPv6 Addresses (or ranges))]** ボックスに、1つ以上のIPアドレス(またはIPアドレスの範囲)を入力します。
 - 複数のアドレスを区切るには、セミコロンを使用します。
例: 172.16.10.3;172.16.10.44;188.23.102.5
 - 範囲の開始IPアドレスと終了IPアドレスを区切るには、ダッシュまたはハイフンを使用します。
例: 10.2.1.70-10.2.1.90

注記: IPv6アドレスは括弧で囲む必要があります。例:

- http://[::1]の場合:
OpenText DASTは「localhost」をスキャンします。

- `http://[fe80::20c:29ff:fe32:bae1]/subfolder/`の場合:
OpenText DASTは、指定されたアドレスのホストのスキャンを「subfolder」ディレクトリから開始します。
- `http://[fe80::20c:29ff:fe32:bae1]:8080/subfolder/`の場合:
OpenText DASTは、ポート8080で実行されているサーバのスキャンを「subfolder」から開始します。

2. **ポート(または範囲)(Ports (or ranges))** ボックスに、スキャンするポートを入力します。
 - 複数のポートを区切るには、セミコロンを使用します。
例: 80;8080;443
 - 範囲の開始ポートと終了ポートを区切るには、ダッシュまたはハイフンを使用します。
例: 80-8080。
3. Web Discoveryの設定を変更するには、**設定(Settings)**をクリックします。詳細については、「[Web Discoveryの設定](#)」を参照してください。
4. **開始(Start)**をクリックして検出プロセスを開始します。
結果が 検出されたエンドポイント(Discovered EndPoints) エリアに表示されます。
5. **[Pアドレス(IP Address)]** 列のエントリをクリックして、そのサイトをブラウザで表示します。
6. **識別(Identification)** 列のエントリをクリックして、セッションプロパティ(Session Properties) ウィンドウを開き、生の要求と応答を確認します。

検出されたサイトの保存

検出されたサーバのリストを保存するには:

1. **ファイル(File)> エクスポート(Export)**をクリックします。
データを.csvファイルにエクスポートすると、それらのIPアドレスがデフォルトのOpenText™ Application Security Centerアプリケーションになります。これらのアプリケーションと関連データは、Excelで編集できます。その後、Fortify WebInspect Enterpriseで、アプリケーションをApplication Securityにインポートできます。詳細については、Fortify WebInspect Enterpriseのオンラインヘルプを参照してください。
2. 標準のファイル選択ウィンドウを使用して、ファイルに名前を付けて保存します。

設定(Settings)

Web Discoveryツールの設定を変更するには:

1. **編集(Edit)> 設定(Settings)**をクリックします。
2. **プロトコルの選択(Select Protocols)** グループで、プロトコル名の横のチェックボックスをオンまたはオフにして、送信するパケットを選択します。

3. **ログ記録(Logging)]**グループで、ログ記録する要素を選択します。
 - **オープンポートをログ記録(Log Open Ports):** ホスト上で検出された使用可能なすべてのオープンポートをログに記録します。Webサーバ情報のみをログファイルに保存します。
 - **サービスをログ記録(Log Services):** 検出中に識別されたすべてのサービスをログに記録します。
 - **Webサーバをログ記録(Log Web Servers):** 識別されたWebサーバをログに記録します。
4. **ログの記録先(Log To)]**ボックスにファイルの場所を入力するか、省略記号ボタンをクリックして標準のファイル選択ウィンドウを使用して、ログエントリを記録するファイルを指定します。
5. **コネクティビティ(Connectivity)]**グループで、次のタイムアウト(ミリ秒)を設定します。
 - **接続タイムアウト(Connection Time Out):** IPアドレスから情報が返されない場合に、Web Discoveryがポートスキャンを停止するまでに待機する時間。
 - **送信タイムアウト(Send Time Out):** メッセージ送信をリモートIPエンドポイント¹に対して行うときに、送信内容は小さなパケットに分割されます。指定された時間内にIPエンドポイントが送信パケットを受信確認しない場合、ソケットは閉じられ、そのエンドポイントの検出ではサービスが報告されません。
 - **受信タイムアウト(Receive Time Out):** リモートIPエンドポイントにメッセージを送信するときに、送信内容は小さなパケットに分割されます。指定された時間内にWeb Discoveryツールが送信パケットを受信しない場合、ソケットは閉じられ、そのエンドポイントの検出ではサービスが報告されません。
6. **ソケット(Sockets)]**ボックスを使用して、オープンソケットの数を調整します。オープンソケットの数が多すぎると、スキャンが高速になります。ただし、サーバのしきい値を超える数を設定すると、誤検出が発生する可能性があります。
7. **OK]**をクリックして更新した情報を保存し、**[Web Discovery]**ウィンドウに戻ります。

¹(トランスポート層接続の一端のエントリの名前であり、サービスがネットワークに接続するポイント。サービス指向アーキテクチャでは、1つのネットワーク対話に2つのエンドポイントが関係し、一方がサービスを提供する側、他方がサービスを使用する側となる。Webサービスでは、エンドポイントはURIで指定される)

第15章:Webフォームエディタ

ほとんどのWebアプリケーションには、入力コントロール(テキストボックス、ボタン、ドロップダウンリストなど)が含まれたフォームがあります。ユーザは通常、入力コントロールを変更(テキストを入力したり、チェックボックスを選択したりするなど)してフォームを「完成」させてから、そのフォームを処理のためにエージェントに送信します。通常、この処理が行われると、ユーザはアプリケーションの別のページまたはセクションに移動します。たとえば、ログオンフォームに入力すると、ユーザはアプリケーションの開始ページに進みます。

スキャナがアプリケーション内でたどることのできるすべてのリンクをナビゲートするためには、各フォームに適切なデータを送信する機能が必要になります。

Web Form Editorでは、すべての入力コントロールの名前と、Webサイトのスキャン中に送信する必要があるそれらの入力コントロールの関連値を含んだファイルを作成または変更できます。これらのエントリはURLごとに分類されるので、別のページにある別のコントロールに同じ名前が付いている場合でも、Web Form Editorはそれらを区別できます。一方、特定のフォームエントリを「グローバル」として指定することもできます。「グローバル」として指定されたエントリ値は、どのURLにあるかに関係なく、同じ名前属性を持つすべての入力コントロールに対して送信されます。

作成したファイルのエントリとは名前属性が一致しない入力コントロールをスキャン中に検出した場合、スキャナはデフォルト値(12345)を送信します。

フォーム値のリストを作成する方法には、次の2つがあります。

- 手動でリストを作成する。
- アプリケーション内をナビゲートしながら値を記録する。

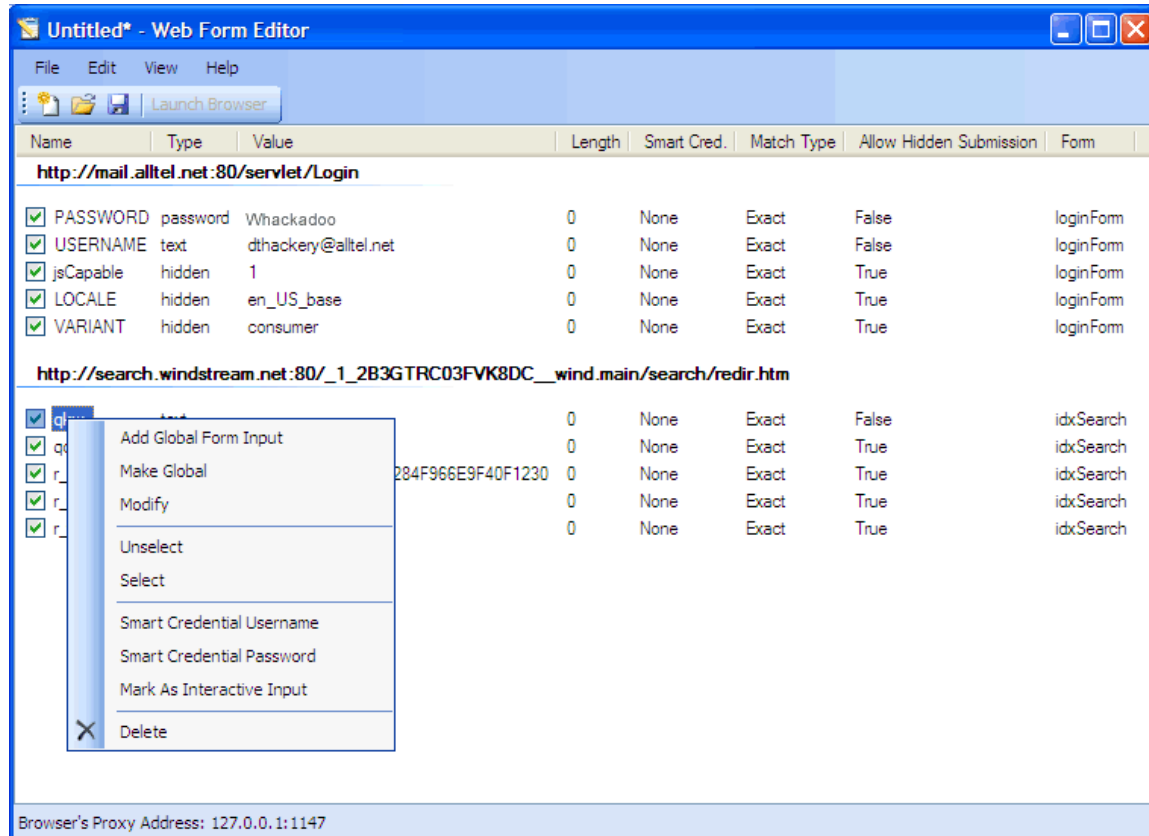
Webフォーム値の記録

Web Form Editorは、ブラウザとターゲットWebサイト間のHTTPトラフィックを処理するプロキシとして機能します。デフォルトでは、ローカルIPアドレス127.0.0.1と使用可能なポートを使用します。ただし、**編集(Edit)**メニューから**設定(Settings)**を選択して、別のIPアドレスとポートを指定することができます。

Webサイト上の入力コントロールの名前と値をキャプチャするには、次の手順に従います。

1. フォーム値のリストを作成するには、**ファイル(File)**メニューから**新規(New)**を選択します(またはツールバーの**新規(New)**アイコンをクリックします)。
2. 既存のリストにフォーム値を追加するには、**ファイル(File)**メニューから**開く(Open)**を選択し(またはツールバーの**開く(Open)**アイコンをクリックし)、標準のファイル選択ダイアログボックスを使用してファイルを選択します。
3. ブラウザのアドレスバーを使用してURLを入力または選択し、フォームが置かれているページに移動します。

4. フォームを完成させ、送信します(通常は、**[ログイン]**、**[送信]**、**[進む]**などのボタンをクリックすることで送信されます)。
5. その他のページに移動してフォームを送信します。これを、たどる必要があるすべてのリンクを一巡するまで続けます。



たとえば、上記のリストの最後の2つのエントリは、次のHTMLフラグメントから得たものです ...

```
<form name="loginForm" action="/servlet/Login" method="POST">
<input type="password" size="16" name="PASSWORD">
<input type="text" size="16" name="USERNAME" value="">
<input type="SUBMIT" value="Submit"></form>
```

...ユーザは自分の名前とパスワードを入力しました。

6. 必要に応じて、エントリを右クリックして項目を変更し、ショートカット(ポップアップ)メニューを使用して項目を変更できます。
 - エントリを編集するには、**変更(Modify)**を選択します。
 - エントリを追加するには、**グローバルフォーム入力の追加(Add Global Form Input)**を選択します。グローバルエントリは、特定のURLに関連付けられていないエントリです。
 - エントリを除外するには、**選択解除(Unselect)**を選択します。これにより、そのエントリは処理対象から除外されます。ただし、ファイルからは削除されません。

- エントリを削除するには、**削除(Delete)]**を選択します。
- エントリをスマート資格情報として指定するには、**スマート資格情報ユーザ名(Smart Credential Username)]**または**スマート資格情報パスワード(Smart Credential Password)]**を選択します。詳細については、「["スマート資格情報" ページ169](#)」を参照してください。
- スキャナでのスキャンを強制的に一時停止し、ユーザにこのエントリの値の入力を求めるウィンドウを表示するには、**対話型入力としてマーク(Mark As Interactive Input)]**を選択します。

スキャナのオプション **Webフォーム値の入力を要求する(Prompt For Web Form Values)]**が選択されている場合、スキャナはHTTPフォームまたはJavaScriptフォームを検出すると、スキャンを一時停止して、ユーザがフォーム内の入力コントロールの値を入力するためのウィンドウを表示します。しかし、スキャナのオプション **タグ付き入力のみを要求する(Only Prompt Tagged Inputs)]**が同時に選択されている場合は、特定の入力コントロールに **対話型入力としてマーク(Mark As Interactive Input)]**が指定されていない限り、スキャナはユーザ入力のための一時停止を行いません(ただし、パスワードの場合は除きます。パスワードの場合、スキャナは常に一時停止して入力を求めます)。

7. **ファイル(File)]**メニューから、**保存(Save)]**または**名前を付けて保存(Save As)]**を選択します。

Webフォームの値の手動による追加と変更

Webフォームの値を追加または変更するには:

1. 次のいずれかを実行します。
 - Webフォームの値を追加するには、Web Form Editorの作業エリア内の任意の場所を右クリックし、ショートカット(ポップアップ)メニューから **グローバルフォーム入力の追加(Add Global Form Input)]**を選択します。
 - Webフォームの値を変更するには、エントリを右クリックし、ショートカット(ポップアップ)メニューから **変更(Modify)]**を選択します。
- ユーザ定義入力の追加(Add User-Defined Input)]** ウィンドウまたは **入力の変更(Modify Input)]** ウィンドウが表示されます。
2. **名前(Name)]** ボックスで、入力要素の名前属性を入力(または変更)します。
 3. **長さ(Length)]** ボックスに、次のいずれかを入力します。
 - サイズ属性で指定する値。
 - ゼロ(サイズ属性を指定しない入力要素の場合)。

たとえば、次のHTMLフラグメントのデータを送信する場合は...

```
<INPUT TYPE="password" NAME="accessID" MAXLENGTH="6">
```



... 名前(Name)]にaccessIDを指定してこの名前のエントリを作成し、長さ(Length)]にサイズ「6」を指定する必要があります。

4. **値(Value)]**ボックスに、入力要素に関連付けるデータ(パスワードなど)を入力します。
5. **一致(Match)]**リストを使用して、このエントリが特定の入力コントロールへの送信に適しているかをスキャナが判定する条件基準を指定します。オプションは次のとおりです。
 - **厳密(Exact)** -入力コントロールの名前属性が、このエントリに割り当てられた名前と完全に一致している必要があります。
 - **次で始まる(Starts with)** -入力コントロールの名前属性が、このエントリに割り当てられた名前で始まっている必要があります。
 - **含む(Contains)** -入力コントロールの名前属性に、このエントリに割り当てられた名前が含まれている必要があります。
6. プログラマは、クライアントとサーバの間で交換される情報(通常はHTTPのステートレスという性質のために失われてしまう)を保存するために、type="hidden"を指定した入力コントロールを使用することがあります。Web Form Editorは非表示のコントロールの属性を収集して表示しますが、スキャナは **非表示送信を許可(Allow Hidden Submission)]** が選択されていないと、非表示のコントロールの値を送信しません。
7. **追加(Add)]**または **変更(Modify)]**をクリックします。
8. 必要に応じて、エントリを右クリックし、ショートカット(ポップアップ)メニューを使用して追加の属性を割り当てることができます。
 - エントリを除外するには、**選択解除(Unselect)]**を選択します。これにより、チェックマークがオフになり、そのエントリは処理対象から除外されます。ただし、ファイルからは削除されません。
 - エントリをアクティブにするには、**選択(Select)]**を選択します。これにより、チェックマークが付き、そのエントリが処理対象として設定されます。
 - エントリを削除するには、**削除>Delete)]**を選択します。
 - エントリをスマート資格情報として指定するには、**スマート資格情報ユーザ名(Smart Credential Username)]**または **スマート資格情報パスワード(Smart Credential Password)]**を選択します。詳細については、「["スマート資格情報" ページ169](#)」を参照してください。
 - **対話型入力としてマーク(Mark As Interactive Input)]**を選択すると、スキャナがスキャンを一時停止し、このエントリの値の入力を求めるウィンドウが表示されます(スキャンオプションに **スキャン中にWebフォーム値の入力を要求する(Prompt For Web Form Values During Scan)]** および **タグ付き入力のみを要求する(Only Prompt Tagged Inputs)]** の設定が含まれる場合)。

注記: 対話型入力としてマーク(Mark As Interactive Input)]を使用してパスワードにタグを付ける必要はありません。

ファイルのインポート

以前のバージョンの Fortify WebInspect 用に設計および作成されたファイルをインポートして、現在の Web Form Editor で使用できるファイルに変換できます。

1. **ファイル(File)]**メニューから **インポート(Import)]**を選択します。
[Webフォーム値の変換(Convert Web Form Values)] ウィンドウが表示されます。
2. **インポートするファイルの選択(Select File To Import)]**の横にある参照ボタン  をクリックします。
3. 標準のファイル選択ウィンドウを使用して、Web Form Editorの以前のバージョンで作成されたXMLファイルを探します。
4. **ターゲットファイルの選択(Select Target File)]**の横にある参照ボタン  をクリックします。
5. 標準のファイル選択ウィンドウを使用して、変換後のファイルのファイル名と場所を指定します。
6. **OK]**をクリックします。

ショートカットメニュー

Web Form Editorの作業エリアを右クリックすると表示されるポップアップメニューからは、以下のコマンドを使用できます。




コマンド	説明
グローバルフォーム入力の追加(Add Global Form Input)	[ユーザ定義入力の追加(Add User-Defined Input)] ウィンドウを表示します。ユーザはこのウィンドウで入力コントロールの名前、長さ、および値を指定できます。詳細については、「 "Webフォームの値の手動による追加と変更" ページ160 」を参照してください。
グローバルにする(Make Global)	選択したエントリと特定のURLの関連付けを解除します。これを行うと、スキャナはこのエントリの名前属性を持つ入力コントロールを検出したときに、そのコントロールの場所に関係なく値を送信ようになります。
変更(Modify)	エントリの名前、長さ、値、および一致タイプの属性を変更できます。
選択解除(Unselect)	エントリに関連付けられたチェックボックスをオフにします。そのエントリは保存されません。またエントリが出現したこのページを再び表示しても、エントリがリストに再び追加されることはありません。

コマンド	説明
選択 (Select)	エントリに関連付けられたチェックボックスをオンにして、保存されるリストにそのエントリが含まれるようにします。
スマート 資格 情報 ユーザ名 (Smart Credential Username)	ユーザがエントリをスマート 資格 情報 ユーザ名として指定している場合、Web Form Editor はユーザが入力したその値を保存しません。スキャナは、このエントリに関連付けられた入力要素を含んだページをスキャンすると、 認証 (Authentication) のオプションで指定されたユーザ名 (ユーザ名が指定されていない場合は、文字列「FormFillText」) を代入します。
スマート 資格 情報 パスワード (Smart Credential Password)	ユーザがエントリをスマート 資格 情報 パスワードとして指定している場合、Web Form Editor はユーザが入力したその値を保存しません。スキャナは、このエントリに関連付けられた入力要素を含んだページをスキャンすると、 認証 (Authentication) のオプションで指定されたパスワード (パスワードが指定されていない場合は、文字列「FormFillText」) を代入します。
対話型入力としてマーク (Mark As Interactive Input)	OpenText DAST の場合のみ: OpenText DAST のオプション スキャン中に Web フォーム 値の入力を要求する (Prompt For Web Form Values During Scan) および タグ付き入力のみを要求する (Only Prompt Tagged Inputs) の両方が設定されている場合にユーザ入力が必要なエントリとしてこのエントリをタグ付けします。OpenText DAST はこのエントリに関連付けられた入力要素を含んだページをスキャンすると、ユーザがこの入力値を入力するまでスキャンを一時停止します。これは、固有の値を必要とするフォームでは特に便利です。その例としては、注文処理システム (番号が重複していると、「その注文はすでに処理されています」などの応答を返す) や、CAPTCHA (応答がコンピュータによって生成されないことを確認するための一種のチャレンジ/レスポンス方式のテスト) などがあります。
削除 (Delete)	選択されたエントリをリストから削除します。そのエントリは保存されません。ただし、このエントリが出現したページを再表示すると、そのエントリが再びリストに追加されます。

Web フォーム ファイルを使用したスキャン

デフォルトのスキャン設定で Web フォーム ファイルを指定した場合、スキャナは Web サイト の評価を開始するときに毎回自動的にそのファイルを選択します。ただし、その選択内容は、特定のスキャンに対して別のファイルを選択することで、上書きすることができます。

作成した Web フォーム 値 のリストを使用してサイトをスキャンするには、次の手順に従います。

1. OpenText DAST の **編集 (Edit)** メニューをクリックして、**デフォルトのスキャン設定 (Default Scan Settings)** を選択します。デフォルト 設定 (Default Settings) ウィンドウが開きます。
2. **スキャン設定 (Scan Settings)** セクションで **方法 (Method)** を選択します。
3. **スキャン動作 (Scan Behavior)** グループで **Web 探索時の Web フォームの自動入力 (Auto-fill Web Forms During Crawl)** を選択します。
4. 以前に記録したファイルを選択するには:
 - a. 参照 ボタン  をクリックします。
 - b. 標準のファイル選択ウィンドウを使用して、使用する Web フォーム 値 を含んだファイルを選択し、**開く (Open)** をクリックします。
 - c. (オプション) エントリを右クリックしてコンテキストメニューからオプションを選択することにより、内容を編集できます。
5. Web フォームの値を記録するには:
 - a. **新しい Web フォーム 値 の作成 (Create New Web Form Values)**  をクリックします。
 - b. **ファイル (File)** メニューをクリックし、**新規 (New)** を選択します。
 - c. **ブラウザの起動 (Launch Browser)** をクリックします。
 - d. 詳細については、「["Web フォーム 値 の記録" ページ 158](#)」を参照してください。
6. 選択したファイルの Web フォーム 値 を編集するには:
 - a. **現在の Web フォーム 値 の編集 (Edit Current Web Form Values)**  をクリックします。
 - b. 詳細については、「["Web フォーム 値 の記録" ページ 158](#)」を参照してください。

Web フォーム リスト と入 力 コント ロール のマッチング

Web アプリケーションを Web 探索して Web フォームの値を送信するとき、OpenText スキャナは Web フォーム 値 のファイルのエントリを分析して、値を送信すべきかどうか判定します。適合していると判定するためのロジックを、推奨度の高いものから順に次の表に示します。

Web フォーム 値 のマッチングのルール

値	適合条件	説明
ページ固有 フォーム 値	完全一致 名前 (Name) が完全一致、長さ (Length) が完全一致	Web 探索した Web ページで検出した特定の Web ページ、Web フォーム 名、および値の長さが、スキャン用に選択された webformvalues.xml 内の 1 つのレコードと完全に一致している。

値	適合条件	説明
	部分一致 名前 (Name)]のみ一致し、長さ(Length)]はワイルドカードを許可	Web探索したWebページで検出した特定のWebページおよびWebフォーム名が、スキャン用に選択されたwebformvalues.xml内の1つのレコードと一致している。そのフォーム値に関連付けられているフィールド長は、どのようなフィールド入力長への送信にも対応する(ワイルドカードフィールド長一致)。
グローバルフォームの値	完全一致 名前 (Name)]が完全一致、長さ(Length)]が完全一致	Web探索したWebページで検出したWebフォーム名および値の長さが、スキャン用に選択されたwebformvalues.xml内のグローバルWebフォーム値セクションにある1つのレコードと一致している。
	部分一致1 名前 (Name)]は完全一致、長さ(Length)]はワイルドカードを許可	Web探索したWebページで検出したWebフォーム名が、スキャン用に選択されたwebformvalues.xml内のグローバル値セクションにあるフォーム名と完全に一致している。そのフォーム値に関連付けられているフィールド長は、どのようなフィールド入力長への送信にも対応する(ワイルドカードフィールド長一致)。
	部分一致2 フィールド名 の先頭が 名前 (Name)]の値であり、長さ(Length)]は完全一致	ファイル内のWebフォーム値が、見つかったフィールド名と部分的に一致している。そのWebフォーム値に含まれているすべての文字がWebページフィールド名の先頭部分と一致し、Web探索したWebページで検出したフィールド長が、スキャン用に選択されたwebformvalues.xml内のグローバルWebフォーム値セクションにあるレコードと一致している。
	部分一致3 フィールド名 の先頭部分が 名前 (Name)]の値であり、長さ(Length)]はワイルドカードを許可	ファイル内のWebフォーム値が、見つかったフィールド名と部分的に一致している。そのWebフォーム値に含まれているすべての文字が、Webページフィールド名の先頭部分と一致している。そのレコードのフィールド長は、任意のフィールド長への送信に対応する(ワイルドカードフィールド長一致)。

値	適合条件	説明
	部分一致4 名前 (Name)] の値がフィールド名に含まれ、長さ (Length)] は完全一致	ファイル内の Web フォーム値が、見つかったフィールド名と部分的に一致している。その Web フォーム値に含まれているすべての文字が、Web ページフィールド名の一部と一致し、Web 探索した Web ページで検出したフィールド長が、スキャン用に選択された webformvalues.xml 内のグローバル Web フォーム値 セクションにあるレコードと一致している。
	部分一致5 名前 (Name)] の値がフィールド名に含まれ、長さ (Length)] はワイルドカードを許可	ファイル内の Web フォーム値が、見つかったフィールド名と部分的に一致している。この Web フォーム値に含まれているすべての文字が、Web ページフィールド名の一部と一致している。そのレコードのフィールド長は、任意のフィールド長への送信に対応する (ワイルドカードフィールド長一致)。
一致なし	フィールド名は完全にも部分的にも Web フォーム値と一致しない	Web フォーム値との一致がない。指定されたデフォルト値 ([デフォルト (Default)]) が送信される。
デフォルト値なし	Web フォーム値のファイルにデフォルト値が指定されていない	Web フォーム値の一致はなく、Web フォーム値のファイルにデフォルト値がない。「見つかりません (not found)」が送信される。

設定: 全般

ブラウザがターゲット Web サイトとやり取りする方法を、以下の設定を使用して指定することができます。これらの設定にアクセスするには、**編集 (Edit)] > 設定 (Settings)] > 全般 (General)]** を選択します。

設定	説明
プロキシリスナ (Proxy Listener)	Web Form Editor は、ブラウザとターゲット Web サイト間の HTTP トラフィックを処理するプロキシとして機能します。デフォルトでは、ローカル IP アドレス 127.0.0.1 と使用可能なポートを使用します。ただし、ユーザは別のローカル IP アドレスとポートを指定することができます。

設定	説明
	すでに使用されているポートを指定する可能性を回避するには、 ポートの自動割り当て(Automatically Assign Port) を選択します。
高度な HTTP 解析 (Advanced HTTP Parsing)	ほとんどの Web ページには、使用する文字セットをブラウザに知らせる情報が含まれています。この指示は、HTML ドキュメントの HEAD セクションの Content-Type 応答ヘッダ(または HTTP-EQUIV 属性を持つ META タグ)を使用して行われます。文字セットをアナウンスしていないページ用に Web Form Editor で使用すべき文字セットを、 想定される「文字セット」エンコード(Assumed 'charset' Encoding) リストで指定できます。

設定: プロキシ

プロキシサーバを介して Web Form Editor にアクセスするには、以下の設定を使用します。これらの設定にアクセスするには、**編集(Edit)] > 設定(Settings)] > プロキシ(Proxy)]**を選択します。

設定	説明
直接接続(プロキシ無効)(Direct Connection (proxy disabled))	プロキシサーバを使用しない場合は、このオプションを選択します。
プロキシ設定の自動検出 (Auto detect proxy settings)	WPAD (Web Proxy Autodiscovery Protocol) プロトコルを使用してプロキシ自動設定ファイルを見つけ、ブラウザの Web プロキシ設定を行うには、このオプションを選択します。
Firefox プロキシ設定を使用する (Use Firefox proxy settings)	Firefox からプロキシサーバ情報をインポートするには、このオプションを選択します。
システムのプロキシ設定を使用する (Use System proxy settings)	ローカルマシンからプロキシサーバ情報をインポートするには、このオプションを選択します。
PAC ファイルを使用してプロキシを設定	PAC (Proxy Automatic Configuration) ファイルからプロキシ設定をロードするには、このオプションを選択します。次に、 [URL] ボックス

設定	説明
する(Configure a proxy using a PAC file)	でファイルの場所を指定します。
プロキシを明示的に設定する(Explicitly configure proxy)	<p>プロキシサーバ経由でインターネットにアクセスするには、このオプションを選択し、要求された情報を以下のように入力します。</p> <ol style="list-style-type: none"> 1. サーバ(Server)] ボックスにプロキシサーバの URL または IP アドレスを入力し、続いて(ポート(Port)] ボックスに) ポート番号 (8080 など) を入力します。 2. プロキシサーバ経由の TCP トラフィックの処理のためのプロトコルを、SOCKS4、SOCKS5、または標準の中から選択します。 3. 認証が必要な場合は、認証(Authentication)] リストからタイプを選択します。 <ul style="list-style-type: none"> • 自動 <div> <p>注記: 自動検出を指定すると、スキャンの処理が遅くなります。把握している別の認証メソッドを指定すると、スキャンのパフォーマンスは大幅に向上します。</p> </div> • 基本(Basic) • ダイジェスト(Digest) • Kerberos • ネゴシエート(Negotiate) • NT LAN Manager (NTLM) 4. プロキシサーバで認証が必要な場合は、適格なユーザ名とパスワードを入力します。 5. 特定の IP アドレス(内部テストサイトなど)にアクセスするためにプロキシサーバを使用する必要がない場合は、プロキシをバイパスするサイト(Bypass Proxy For)] ボックスにアドレスまたは URL を入力します。エントリはカンマで区切ります。
HTTPS 用の代替プロキシを指定する(Specify Alternative Proxy for HTTPS)	HTTPS 接続を受け入れるプロキシサーバの場合は、 [HTTPS 用の代替プロキシを指定する(Specify Alternative Proxy for HTTPS)] を選択し、要求された情報を入力します。

スマート 資格 情報

Web フォーム 値 を記録しているときは、ユーザ名とパスワードの入力を求めるログオンフォームが表示されることがよくあります。自分のユーザ名とパスワードを安全に使用できますが、そのためには、ファイルを保存する前に、ユーザ名とパスワードのエントリを「スマート 資格 情報」として指定する必要があります。実際のパスワードとユーザ名は保存されません。

スキャナは、このエントリに関連付けられた入力コントロールを含んだページをスキャンすると、製品の 認証 (Authentication) オプションで指定されているパスワードを代入します。このオプションでは、セキュリティを必要としない既知のユーザ名とパスワードが指定されます。ユーザ名またはパスワードが指定されていない場合、スキャナは文字列「FormFillText」を送信します。

第16章:Web Fuzzer

Web Fuzzerツールを使用すると、次に挙げるような一般的なクラスのWebアプリケーションセキュリティ脆弱性に対して、いくつかの自動テストを実行できます。

- SQLインジェクション
- 文字列のフォーマット
- クロスサイトスクリプティング
- パストラバーサル
- 奇妙な文字
- バッファのオーバーフロー
- プロトコルの実装に関する問題

ファジングとは

「ファジング」は、自動ソフトウェアテスト技術で、アプリケーションのさまざまなエリアにランダムまたはシーケンシャルなデータを生成して送信し、セキュリティの脆弱性を明らかにしようとしています。たとえば、バッファのオーバーフローを探す場合、テスト担当者はさまざまなサイズのデータを生成し、それをアプリケーションエントリポイントの1つに送信して、アプリケーションの処理方法を監視できます。

Web Fuzzerへのアクセス

Web Fuzzerツールにアクセスするには、次のいずれかを実行します。

- OpenText DASTツールバーで、**ツール(Tools)] > [Web Fuzzer]**をクリックします。
- セキュリティツールキットを使用して、**開始(Start)] > [OpenText] > [Web Fuzzer]**をクリックします。

Fuzzerメニューについて

このトピックでは、Web Fuzzerメニューバーのさまざまなオプションについて説明します。

[ファイル(File)] メニュー

次の表は、[ファイル(File)] メニューオプションの説明です。

オプション	説明
インポート (Import)	以前に保存したセッションを セッション(Sessions)] エリアにインポートします。
エクスポート	セッション(Sessions)] エリアのセッションをファイルにエクスポートします。
セッションのクリア (Clear Sessions)	セッションビューリストをクリアします。
終了 (Exit)	アプリケーションを閉じます。

編集(Edit)]メニュー

次の表は、編集(Edit)]メニューオプションの説明です。

オプション	説明
サーバ	ターゲットサーバを指定し、認証設定を選択できます。
設定(Settings)	一般設定、プロキシ設定、ソケット設定、およびプロトコル設定を指定できます。

セッション(Session)]メニュー

次の表は、セッション(Session)]メニューオプションの説明です。

オプション	説明
インポート (Import)	以前に保存したセッションが含まれているXMLファイルをインポートします。
エクスポート	セッションをXMLファイルにエクスポートします。
作成	Session Editor を開き、要求を作成するための構造化されたアプローチを提供します。
生の作成 (Raw Create)	Raw Editor を開き、標準要求を編集できます。
編集	セッションの選択後に使用できます。 Session Editor を開きます。
生の編集 (Raw Edit)	セッションの選択後に使用できます。 Raw Editor を開きます。

フィルタ(Filters)]メニュー

次の表は、フィルタ(Filters)]メニューオプションの説明です。

オプション	説明
編集	フィルタ(Filters)]ダイアログを開き、指定した応答のみを選択する正規表現を作成できます。
有効にする	セッションにフィルタを適用します。

Web Fuzzerの使用

次の表は、Web Fuzzerの使い方を説明しています。

ステージ	
1.	サーバ情報を設定します。詳細については、「 "サーバの設定" 次のページ 」を参照してください。
2.	設定を行います。詳細については、「 "Fuzzer設定" ページ182 」を参照してください。
3.	次のいずれかを実行します。 <ul style="list-style-type: none">セッションを作成します。以前に保存したセッションをインポートし、(必要な場合は)編集します。 詳細については、 "Session Editorの使用" 次のページ または "Raw Editorの使用" ページ178 を参照してください。
4.	開始(Start)] をクリックします。 セッション(Sessions)]エリアに、ツールによって生成された各セッション(要求と応答)が一覧表示されます。
5.	結果を確認するため、セッション(Sessions)]リストのエントリをクリックします。 選択したセッションのHTTP要求が 要求(Request)] エリアに表示されます。サーバ応答は、 ブラウザビュー(Browser View)] タブと 生の応答(Raw Response)] タブの両方に表示されます。
6.	構築した要求を編集するには、セッション(Sessions)]リストでセッションを

ステージ	
	選択し、 セッション(Session) メニューをクリックして、 編集(Edit) または 生の編集(Raw Edit) のどちらかを選択します。 詳細については、" Session Editorの使用 " 下または" Raw Editorの使用 " ページ178 を参照してください。

サーバの設定

サーバの設定 (Server Configuration) ダイアログを使用して、ターゲット Web サイトを識別し、通信設定を行います。

サーバ設定を行うには:

1. **編集(Edit)**をクリックし、**サーバ(Server)**を選択します。
サーバ設定 (Server Configuration) ダイアログが開きます。
2. **ホスト名/IP (Host Name/IP)** ボックスに、Web サイトの完全修飾ドメイン名 (FQDN) または IP アドレスを入力します。
3. **ポート (Port)** ボックスに、サーバのポート番号を入力します。
4. サーバが Secure Sockets Layer プロトコルを使用している場合は、**\$SSL** チェックボックスをオンにします。
5. 認証が必要な場合は、**タイプ(Type)** リストからメソッドを選択し、該当するボックスにユーザ名とパスワードを入力します。
6. **OK** をクリックします。

Session Editorの使用

Session Editor を使用して、HTTP 要求を作成したり、HTTP 要求の特定のセクションを変更したりします。テキストボックスにテキストの入力または貼り付けを行って、HTTP 要素と置き換えることができます。またはジェネレータを挿入して、生成されたデータを含んだ複数の要求を作成できます。

セッションの作成

セッションを作成するには:

- **セッション(Session)** > **作成(Create)**を選択します。
Session Editor が開きます。"[セッションの設定](#)" [次のページ](#)の手順に従います。

セッションの編集

セッションを編集するには:

1. **セッション(Sessions)]**リストで、セッションを選択します。
2. **セッション(Session)] > 編集(Edit)]**を選択します。
Session Editorが開きます。**"セッションの設定" 下**の手順に従います。

セッションの設定

Session Editorでセッションを設定するには:

1. タブをクリックします。
2. 各タブの詳細については、次のセクションを参照してください。
 - "**メソッド(Method)]**タブ" 下
 - "**パス(Path)]**タブ" 次のページ
 - "**クエリ(Query)]**タブ" 次のページ
 - "**バージョン(Version)]**タブ" ページ176
 - "**ヘッダ(Headers)]**タブ" ページ176
 - "**クッキー(Cookies)]**タブ" ページ177
 - "**POSTデータ(Post Data)]**タブ" ページ177
3. 次のいずれかを実行します。
 - テキストボックスに表示されるデータを編集します。
 - **ジェネレータを使用する(Use Generator)]** チェックボックスを選択し、**ジェネレータ]** をクリックして、ジェネレータを挿入します。詳細については、「"**Fuzzerジェネレータについて**" ページ179」を参照してください。
4. 他のエリアを変更するには、別のタブをクリックします。
5. 変更するエリアを設定した後で、**OK]** をクリックします。
6. **[Web Fuzzer]** ウィンドウに戻ったら、**開始(Start)]** をクリックします。

メソッド(Method)] タブ

デフォルトでGETメソッドが指定されています。任意のテキストに置き換えるか、メソッドジェネレータを挿入できます。

【パス(Path)]タブ

パスに関連する次の3つの要素をファジングできます。

- ファイルの名前
- ファイル拡張子
- ディレクトリレベルを指定する文字(通常はスラッシュ/)

これらの要素を任意のテキストに置き換えるか、ジェネレータを挿入できます。

【クエリ(Query)]タブ

一部のHTTP要求にはクエリ文字列が含まれます。各パラメータは、parameter=valueという形式で、アンパサンド(&)で区切ります。リソースは、区切り記号文字(通常は疑問符ですが、アプリケーションによっては他の文字を使用できます)によってクエリから分離されます。例:

`http://www.website.com/category.cfm?model_ID=0&category_ID=12`

クエリ文字列を作成するには:

1. **追加(Add)]**をクリックします。
name=valueがリストに表示されます。これは作成するクエリ文字列を表します。
2. **名前(Name)]**タブをクリックします。
「name」という名前のパラメータを編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)]** チェックボックスを選択して、 **ジェネレータ(Generator)]** をクリックします)。
3. **値(Value)]**タブをクリックします。
数式中の「value」を編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)]** チェックボックスを選択して、 **ジェネレータ(Generator)]** をクリックします)。
4. **セパレータ(Separator)]**タブをクリックします。
値から名前を分離する文字(通常は等号記号)を編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)]** チェックボックスを選択して、 **ジェネレータ(Generator)]** をクリックします)。
5. **フォーマット(Format)]**タブをクリックします。
数式要素が表示される順序を編集したり、要素の間に文字を挿入したりすることができます。
6. **名前と値のセパレータ(Name Value Separator)]** エリアで、パラメータを分離する文字(通常はアンパサンド)を編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)]** チェックボックスを選択して **ジェネレータ(Generator)]** をクリックします)。
7. 別のパラメータを追加するには、 **追加(Add)]** をクリックして、ステップ2-6を繰り返します。

【バージョン(Version)】タブ

バージョンは、要求の解釈に使用するHTTPバージョンをサーバに示します。有効なバージョンは、0.9、1.0、および1.1です。バージョン情報は「HTTP/version」の形式に従います。これは、スラッシュ(/)で区切られた名前と値のペアです。【プロトコル(Protocol)】、【セパレータ(Separator)】、および【バージョン(Version)】の3つのセクションすべてをファジングできます。順序を変更したり、無関係な文字を挿入したりして、形式をファジングできます。

【ヘッダ(Headers)】タブ

ヘッダには、サーバまたはアプリケーションが要求を処理するのに役立つ、クライアントによって発行された基本情報が含まれています。一般的なヘッダは、HostとUser-Agentです。各ヘッダは、「name: value」構文を使用して定義されます。この名前と値の構造を、ファジングの4つの機会に分割することもできます。

ヘッダを作成するには:

1. **追加(Add)**をクリックします。
name:valueがリストに表示されます。これは作成するヘッダを表します。
2. **名前(Name)**タブをクリックします。
「name」という名前のパラメータを編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)** チェックボックスを選択して、 **ジェネレータ(Generator)** をクリックします)。
3. **値(Value)**タブをクリックします。
「value」テキストを編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)** チェックボックスを選択して、 **ジェネレータ(Generator)** をクリックします)。
4. **セパレータ(Separator)**タブをクリックします。
値から名前を分離する文字(通常はコロン)を編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)** チェックボックスを選択して、 **ジェネレータ(Generator)** をクリックします)。
5. **フォーマット(Format)**タブをクリックします。
ヘッダ要素が表示される順序を編集したり、要素の間に文字を挿入したりすることができます。
6. **名前と値のセパレータ(Name Value Separator)**エリアで、ヘッダを分離する文字を編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)** チェックボックスを選択して **ジェネレータ(Generator)** をクリックします)。
7. 別のヘッダを追加するには、 **追加(Add)** をクリックして、ステップ2-6を繰り返します。

クッキー(Cookies)] タブ

クッキーは、ユーザと状態を管理するためにアプリケーションによって使用されるパラメータを含む特別なヘッダです。クッキー定義の形式は次のとおりです。

```
Cookie: name=value;name=value
```

各パラメータは、個別にファジングできる名前と値のペアです。

クッキーを作成するには:

1. **クッキー(Cookie)] リスト**で、**追加(Add)]**をクリックします。
クッキー(Cookie)] リストにCookie:が表示されます。これは作成するクッキーを表します。
2. **クッキーの詳細(Cookie Detail)] リスト**で、**追加(Add)]**をクリックします。
name=valueが **クッキーの詳細(Cookie Detail)]** リストに表示されます。
3. **クッキーの詳細(Cookie Detail)]** リストの右側にある **クッキー名(Cookie Name)]** タブをクリックします。
名前を編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)]** チェックボックスを選択して、 **ジェネレータ(Generator)]** をクリックします)。
4. **値(Value)]** タブをクリックします。
「value」テキストを編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)]** チェックボックスを選択して、 **ジェネレータ(Generator)]** をクリックします)。
5. **セパレータ(Separator)]** タブをクリックします。
値から名前を分離する文字(通常は等号記号)を編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)]** チェックボックスを選択して、 **ジェネレータ(Generator)]** をクリックします)。
6. **フォーマット(Format)]** タブをクリックします。
ヘッダ要素が表示される順序を編集したり、要素の間に文字を挿入したりすることができます。
7. **名前と値のセパレータ(Name Value Separator)]** エリアで、ヘッダを分離する文字を編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)]** チェックボックスを選択して **ジェネレータ(Generator)]** をクリックします)。
8. 別のクッキーを追加するには、ステップ1-7を繰り返します。

POSTデータ(Post Data)] タブ

クエリはRequest-URIに追加できるのに対し、POSTデータは要求の最後に追加されます。形式はURIクエリに似ており、ほとんどの場合、POSTメソッドで使用されます。POSTデータを使用する場合、要求には、POSTデータのサイズを示すContent-Lengthヘッダが含まれている必要があります。POSTデータだけでなく、Content-Length値もファジングして、サーバまたはアプリケーションがどのように相違を処理するかテストできます。

HTTP要求メッセージをファジングする場合、アプリケーション環境の2つの主な層(サーバプロトコルの実装とWebアプリケーション)に影響します。

POSTデータを作成するには:

1. **追加(Add)]**をクリックします。
name=valueがリストに表示されます。これは作成するPOSTデータを表します。
2. **名前(Name)]**タブをクリックします。
「name」という名前のパラメータを編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)]** チェックボックスを選択して、 **ジェネレータ(Generator)]** をクリックします)。
3. **値(Value)]**タブをクリックします。
「value」テキストを編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)]** チェックボックスを選択して、 **ジェネレータ(Generator)]** をクリックします)。
4. **セパレータ(Separator)]**タブをクリックします。
値から名前を分離する文字(通常はコロン)を編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)]** チェックボックスを選択して、 **ジェネレータ(Generator)]** をクリックします)。
5. **フォーマット(Format)]**タブをクリックします。
ヘッダ要素が表示される順序を編集したり、要素の間に文字を挿入したりすることができます。
6. **名前と値のセパレータ(Name Value Separator)]** エリアで、ヘッダを分離する文字を編集するか、代わりにジェネレータを使用できます(**ジェネレータを使用する(Use Generator)]** チェックボックスを選択して **ジェネレータ(Generator)]** をクリックします)。
7. 別のPOSTデータ要素を追加するには、 **追加(Add)]** をクリックして、ステップ2-6を繰り返します。

Raw Editorの使用

Raw Editorを使用して、HTTP要求メッセージを作成します。

要求のいずれかの部分を変更するには、ツールのテキスト編集機能を使用するか、ジェネレータを挿入します。

ジェネレータを挿入するには:

1. 次のいずれかを実行します。
 - 要求内の任意の場所にカーソルを移動します。
 - 要求の任意の部分を強調表示します。
2. 右クリックして、ショートカットメニューから **ジェネレータ(Generator)]** を選択します。
ジェネレータ(Generators)] ダイアログが開きます。

3. **ジェネレータ(Generators)]** ダイアログで、ジェネレータを選択し、**設定(Configure)]** をクリックします。
オプション(Options)] ダイアログが開きます。
 4. **オプション(Options)]** ダイアログで、設定情報を入力し、**OK]** をクリックします。
 5. **ジェネレータ(Generators)]** ダイアログで、**OK]** をクリックします。
 6. 作成したジェネレータは、カーソル位置に(またはステップ1で強調表示した任意の部分に置き換えて)挿入されます。
- 要求の編集またはジェネレータの挿入(またはその両方)を行った後で、**OK]** をクリックし、[Web Fuzzer] ウィンドウに戻ります。次に、**開始(Start)]** をクリックします。

Fuzzerジェネレータについて

ジェネレータを使用すると、ファジングに使用するセッションの作成に役立ちます。次の表は、Web Fuzzerで使用するジェネレータについて説明しています。

ジェネレータ	説明
ASCII	要求ごとに、指定した範囲内のASCII文字を1つ挿入します。 開始文字と終了文字、および一連の文字をループする回数を指定します。
文字	指定した文字を生成し、各要求にその文字を複数個挿入します。 最小文字数と最大文字数、および増分を指定します。
小数	指定した範囲内の小数を各要求に挿入します。 最小(Minimum)] と 最大(Maximum)] の数、 増分(Increment)] 、および一連の数をループする回数を指定します。
GUID	各要求にランダムなGlobally Unique Identifier (128ビットの数値)を挿入します。 要求の数を指定します。
HTTPメソッド	メソッド(GET、POST、PUTなど)を要求に挿入します。 プロトコルのバージョン(0.9、1.0、1.1、またはすべて)を指定します。
Number	指定した範囲内の数値を各要求に挿入します。 最小(Minimum)] と 最大(Maximum)] の数、 増分(Increment)] 、および一連の数をループする回数を指定します。
SQLインジェク	指定したテキストファイルから文字列を挿入します。要求の数は、ファイ

ジェネレータ	説明
シジョン	<p>ル内の段落数によって決まります。段落内のcharacters すべてが挿入されます。</p> <p>デフォルトのファイル(sqlinjections.txt)には、次の2つのエントリが含まれます。</p> <pre>' or 1=1 ' or like '%</pre>
Text	指定したテキストを1つの要求に挿入します。
WordListリーダー	指定したテキストファイルから文字列を挿入します。要求の数は、ファイル内の段落数によって決まります。段落内のすべての文字が挿入されます。
XSSインジェクション	<p>指定したテキストファイルから文字列を挿入します。要求の数は、ファイル内の段落数によって決まります。段落内のすべての文字が挿入されます。</p> <p>デフォルトのファイル(xssinjections.txt)には、次のエントリが含まれます。</p> <pre><script>alert('test')</script></pre>

フィルタの操作

フィルタは、名前、説明、およびルールで構成されます。「ルール」は、サーバ応答の特定のセクションで検索するテキストを定義する正規表現です。たとえば、応答本文に「error」という単語が含まれていて、かつ応答のステータスコードとして500-599も指定されている応答だけを表示するには、次のルールを使用します。

```
[STATUSCODE]5\d\d AND [BODY]\serror\s
```

次の表記法を使用して、応答のセクションを指定します。

[HEADERS]

[STATUSLINE]

[STATUSCODE]

[STATUSDESCRIPTION]

[ALL]

[SETCOOKIES]

[BODY]

フィルタ(Filters)] ダイアログへのアクセス

フィルタ(Filters)] ダイアログにアクセスするには:

- **フィルタ(Filters)] > 編集(Edit)]**を選択します。
フィルタ(Filters)] ダイアログが開きます。

フィルタの作成

フィルタを作成するには:

1. **フィルタ(Filters)]** ダイアログで、**追加(Add)]**をクリックします。
ツールによって「Default Rule」という名前のルールが作成されます。
2. **名前(Name)]**、**説明(Description)]**、および **ルール(Rule)]**を変更します。
3. **適用(Apply)]**をクリックして、フィルタを保存します。

フィルタの編集

フィルタを編集するには:

1. **フィルタ(Filters)]** ダイアログで、**フィルタ(Filters)]** リストからフィルタを選択します。
2. **名前(Name)]**、**説明(Description)]**、または **ルール(Rule)]**を変更します。
3. **適用(Apply)]**をクリックして、変更を保存します。

フィルタの使用

セッションでフィルタを使用するには:

1. **フィルタ(Filters)]** ダイアログで、**フィルタ(Filters)]** リストからフィルタを選択します。
2. **有効化(Enable)]** チェックボックスを選択します。

重要! 特定のルールを有効にすることのほかに、一般的なルールの使用も有効にする必要があります。そのためには、**フィルタ(Filter)] > 有効化(Enable)]**を選択します。

フィルタの削除

フィルタを削除するには:

1. **フィルタ(Filters)]** ダイアログで、**フィルタ(Filters)]** リストからフィルタを選択します。
2. **削除(Delete)]**をクリックします。

Fuzzer設定

設定 (Settings)] ダイアログでWeb Fuzzer設定を行うことができます。

Web Fuzzer設定を行うには:

1. **編集(Edit)]**をクリックし、**設定(Settings)]**を選択します。
設定 (Settings)] ダイアログが開きます。
2. 次のいずれかを実行します。
 - アプリケーション設定を行うには、左側のペインで **全般(General)]**を選択します。使用可能な設定の詳細については、"**一般設定**" 下を参照してください。
 - プロキシ設定を行うには、左側のペインで **プロキシ(Proxy)]**を選択します。使用可能な設定の詳細については、"**プロキシ設定**" 次のページを参照してください。
3. 終了したら、**OK]**をクリックします。

一般設定

次の表は、一般設定について説明しています。

設定	説明
フィルタの有効化 (Enable Filters)	フィルタのサポートを有効にします。このオプションを有効にすると、 フィルタ(Filters)] ダイアログでフィルタを追加、編集、および削除できます。詳細については、「" フィルタの操作 " ページ180」を参照してください。 注記: メニューバーの フィルタ(Filters)] > 有効化(Enable)] を選択して、フィルタを有効にすることもできます。
自動スクロールビュー (Auto Scroll View)	セッション(Sessions)] リストビューの自動スクロールを有効にします。このオプションを有効にすると、ビューは自動的に最新のセッションまでスクロールします。
ツールヒントを表示 (Show ToolTips)	ユーザインタフェース(UI)の特定の要素にマウスポインタを合わせると、ツールヒントが表示されます。
最大ソケット数(Max Sockets)	使用するソケットの最大数を指定します。
タイムアウト/秒 (Timeout/Seconds)	ソケット送信タイムアウトを秒単位で指定します。

設定	説明
Content-Lengthの強制(Enforce Content-Length)	Web Fuzzerは、必要に応じて要求のContent-Lengthの値を自動的に調整します。このオプションを有効にすると、Content-Lengthヘッダをファジングできません。
Hostヘッダの適用(Enforce Host Header)	Web Fuzzerは、すべての要求にHostヘッダを含めます。この機能を有効にすると、Hostヘッダをファジングできません。

プロキシ設定

次の表は、プロキシ設定について説明しています。

設定	説明
直接接続(プロキシ無効)(Direct Connection (proxy disabled))	プロキシサーバを使用しない場合は、このオプションを選択します。
プロキシ設定の自動検出(Auto detect proxy settings)	WPAD (Web Proxy Autodiscovery)プロトコルを使用してプロキシ自動設定ファイルを探し、ブラウザのWebプロキシ設定を行います。
システムのプロキシ設定を使用する(Use System Proxy Settings)	ローカルマシンからプロキシサーバ情報をインポートします。
Firefoxプロキシ設定を使用する(Use Firefox proxy settings)	Firefoxからプロキシサーバ情報をインポートします。
PACファイルを使用してプロキシを設定する(Configure a proxy using a	[URL] ボックスで指定した場所にあるPAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードします。

設定	説明
PAC file)	
プロキシを明示的に設定する (Explicitly configure proxy)	要求された情報を入力することによって、プロキシを設定します。「 "プロキシの設定" 下 」を参照してください。
HTTPS用の代替プロキシを指定する(Specify Alternative Proxy for HTTPS)	HTTPS接続を受け入れるプロキシサーバの場合は、このオプションを選択し、要求された情報を入力してプロキシを設定します。「 "プロキシの設定" 下 」を参照してください。

プロキシの設定

プロキシを設定するには:

1. **サーバ(Server)**] ボックスにプロキシサーバのURLまたはIPアドレスを入力し、続いて **(ポート(Port))** ボックスに)ポート番号(8080など)を入力します。
2. **タイプ(Type)**] リストから、プロキシサーバ経由のTCPトラフィックを処理するプロトコル(SOCKS4、SOCKS5、または標準)を選択します。
3. 認証が必要な場合は、**認証(Authentication)**] リストからタイプを選択します。

- 自動

注記: 自動検出を指定すると、スキャンの処理が遅くなります。把握している別の認証メソッドを指定すると、スキャンのパフォーマンスは大幅に向上します。

- 基本
- ダイジェスト
- Kerberos
- ネゴシエート(Negotiate)
- NT LAN Manager (NTLM)

4. プロキシサーバで認証が必要な場合は、適格なユーザ名とパスワードを入力します。

第17章:セッションベースのWeb Macro Recorder

OpenText DASTおよびFortify WebInspect EnterpriseにはセッションベースのWeb Macro Recorderツールが含まれています。1つはログインマクロ用、もう1つはワークフローマクロ用です。このドキュメントで、これらの2つのツールは、特定のログイン関連およびワークフロー関連のコンテンツを除き、一般に「セッションベースのWeb Macro Recorder」と呼ばれます。

セッションベースのWeb Macro Recorderは、いくつかの方法で起動できます。詳細については、「["セッションベースのWeb Macro Recorderへのアクセス" 次のページ](#)」を参照してください。

マクロについて

ログインマクロとは、Webサイトにアクセスしてログインするときに発生するイベントの記録です。その後、この記録を使用してスキャンを開始するように、OpenText DASTスキャナに指示できます。ワークフローマクロは、ログインステップ(必要に応じて)とサイト上の特定のURLの記録です。

注記:「スキャナ」という用語はしばしば「OpenText DASTおよびFortify WebInspect Enterprise」の代わりに使用されます(情報が両方の製品に当てはまる場合)。

IEテクノロジー

デフォルトでは、セッションベースのWeb Macro Recorderは、Internet Explorerブラウザテクノロジー(IEテクノロジーとも呼ばれます)を使用してマクロを記録および再生します。

ログインマクロ

ログインマクロは、WebサイトまたはWebアプリケーションにアクセスしてログインするために必要なアクティビティの記録です。通常は、ユーザ名とパスワードを入力し、[ログイン]や[ログオン]などのボタンをクリックします。スキャンを設定する場合、通常は、以前に記録したログインマクロを指定するか、またはスキャンで使用する時点で新しいログインマクロを記録します。

アプリケーションからログアウトした場合にスキャナが途中で終了することを防ぐため、ログインマクロには、ログアウトが発生したことを明確に示すログアウト条件を少なくとも1つ指定する必要があります。スキャン中に、スキャナはさまざまな理由でログアウトする場合があります。次に例を示します。

- ターゲットサイトによって引き起こされる通常のログアウト
- タイムアウトなどのターゲットサイトのエラー状態

- 無効なパラメータなどのマクロ自体のエラー

ログインマクロの一部としてログアウト条件を指定すると、スキャン中に予期しないログアウトが発生した場合に、ユーザが何度も手動でログインし直す必要がなくなります。スキャナは、サイトをスキャンする際に、ターゲットサイトの各応答を分析して状態を判断します。スキャナは、ログアウトしたと判断した場合はいつでも、ログインマクロを実行してログインし直し、ログアウトが発生した地点からサイトのWeb探索または監査を再開します。

ログインマクロを記録する最後のステップとして、セッションベースのLogin Macro Recorderは高度な分析を使用して「自動的に」ログアウト条件を検出し、それをログインマクロに指定しようと試みます。ほとんどの場合、手動でログアウト条件を特定する必要はありません。ただし、ログアウト条件を追加または編集できます。

ワークフローマクロ

ワークフローマクロは、ログインステップ(必要に応じて)と、サイト上で手動で移動する特定のURLの記録です。OpenText DASTまたはFortify WebInspect Enterpriseは、ワークフローマクロに記録されたURLのみを監査し、監査中に検出されたハイパーリンクを取得しません。この種のマクロは、アプリケーションの特定のサブセクションに焦点を当てるために最もよく使用されます。マクロ記録プロセスの観点では、ログインマクロとの基本的な違いは次のとおりです。

- ワークフローマクロには、記録中にユーザが移動した特定のURLのみが含まれます。ワークフローマクロは、再生時にそれらのURLにのみアクセスします。
- ワークフローマクロではログアウト条件が必須ではないので、セッションベースのWorkflow Macro Recorderのユーザインタフェースでは、ワークフローマクロを記録する際にログアウト条件機能が除外されます。

注記: Webサイトで認証が必要な場合は、ログインステップをワークフローマクロに記録しないでください。代わりに、別のログインマクロを記録してWebサイトにログインしてください。

セッションベースのWeb Macro Recorderへのアクセス

以下の段落では、セッションベースのWeb Macro Recorderを起動するさまざまな方法について説明します。

ログインマクロ

OpenText DASTまたはFortify WebInspect Enterpriseでは、セッションベースの新しいログインマクロを記録することも、記録が済んだセッションベースの既存のログインマクロを選択(およびオプションで編集)することもできます。次のように行います。

- Internet Explorerをレンダリングエンジンとしてガイド付きスキャンを設定する場合は、ターゲットサイトにログインマクロが必要であることを指定し、**作成(Create)**をクリックして新しいログインマクロを記録するか、既存のログインマクロを選択(およびオプションで編集)します。
- Internet Explorerをレンダリングエンジンとして、OpenText DASTの基本スキャンまたはFortify WebInspect EnterpriseのWebサイトスキャンを設定する場合、ステップ2で **サイト認証(Site Authentication)**を選択して新しいログインマクロを記録するか、既存のログインマクロを選択(およびオプションで編集)します。
- OpenText DASTツールバーで、**ツール(Tools)] > ログインマクロレコーダ(Login Macro Recorder)] > セッションベース(Session-based)]**をクリックして、ログインマクロレコーダをスタンドアロンモードで実行し、新しいログインマクロを記録するか、既存のログインマクロを開きます(およびオプションで編集します)。
- Fortify WebInspect Enterpriseの管理コンソールのツールバーで、**ツール(Tools)] > ログインマクロレコーダ(Login Macro Recorder)] > セッションベース(Session-based)]**をクリックして、ログインマクロレコーダをスタンドアロンモードで開き、新しいログインマクロを記録するか、既存のログインマクロを開きます(およびオプションで編集します)。
- セキュリティツールキットを使用して、**開始(Start)] > Fortify] > ログインマクロレコーダ(セッション)(Login Macro Recorder (Session))]**をクリックして、ログインマクロレコーダをスタンドアロンモードで実行し、新しいログインマクロを記録するか、既存のログインマクロを開きます(およびオプションで編集します)。
- Windowsエクスポーラで、セッションベースのLogin Macro Recorderを使用して記録された既存のログインマクロに移動し、ダブルクリックして開きます。セッションベースのLogin Macro Recorderがスタンドアロンモードで開きます。

ワークフローマクロ

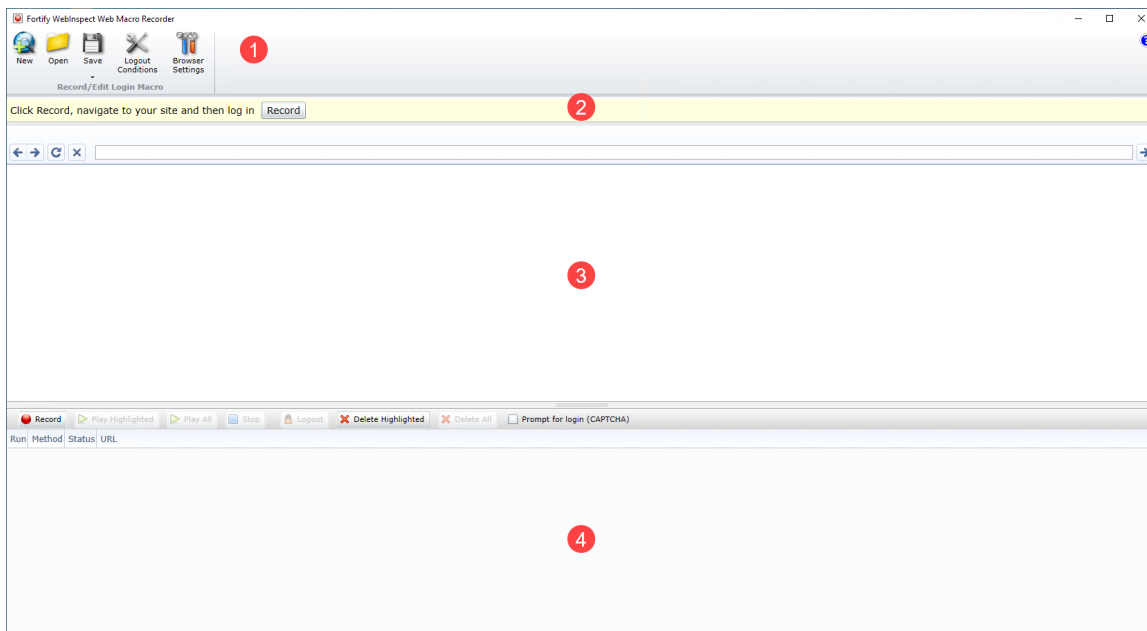
OpenText DASTまたはFortify WebInspect Enterpriseでは、新しいワークフローマクロを記録することも、記録が済んだ既存のワークフローマクロを選択(およびオプションで編集)することもできます。次のように行います。

- Internet Explorerをレンダリングエンジンとしてガイド付きスキャンを設定する場合は、**スキャンタイプ(Scan Type)]**を **ワークフロー(Workflows)]**に指定し、その後、**ワークフロー(Workflows)] > 1.ワークフローステップの管理**、新しいワークフローマクロの記録、または既存のワークフローマクロのインポートおよびオプションで編集を行います。
- Internet Explorerをレンダリングエンジンとして使用してOpenText DASTの基本スキャンを設定する場合、ステップ1で **ワークフロー駆動型スキャン(Workflow-Driven Scan)]**を選択し、**記録(Record)]**または **管理(Manage)]**をクリックして新しいワークフローマクロを記録するか、既存のワークフローマクロを選択(およびオプションで編集)します。

- OpenText DASTツールバーで、**ツール(Tools)] > [ワークフローマクロレコーダ(Workflow Macro Recorder)] > [セッションベース(Session-based)]**をクリックして、ワークフローマクロレコーダをスタンドアロンモードで実行し、新しいワークフローマクロを記録するか、既存のワークフローマクロを開きます(およびオプションで編集します)。
- Fortify WebInspect Enterpriseの管理コンソールのツールバーで、**ツール(Tools)] > [ワークフローマクロレコーダ(Workflow Macro Recorder)] > [セッションベース(Session-based)]**をクリックして、ワークフローマクロレコーダをスタンドアロンモードで開き、新しいワークフローマクロを記録するか、既存のワークフローマクロを開きます(およびオプションで編集します)。
- セキュリティツールキットを使用して、**開始(Start)] > [Fortify] > [ワークフローマクロレコーダ(セッション)(Workflow Macro Recorder (Session))]**をクリックして、ワークフローマクロレコーダをスタンドアロンモードで実行し、新しいワークフローマクロを記録するか、既存のワークフローマクロを開きます(およびオプションで編集します)。

セッションベースのWebマクロレコーダのインターフェースについて

このトピックでは、セッションベースのWebマクロレコーダのユーザインターフェースについて説明します。



次の表では、セッションベースのWeb Macro Recorderのユーザインターフェースのコンポーネントについて説明します。

項目	説明
1	ツールバー。詳細については、「 "ツールバー" 次のページ 」を参照してください。

項目	説明
2	ステップを追ったガイダンスを提供する黄色の指示バー。
3	ターゲット サイト ペイン。
4	場所 ペイン。詳細については、「 "場所 ペイン" 下 」を参照してください。 <div>ヒント: 場所 ペインの高さは、ターゲット サイト ペインを基準に調整できます。</div>

ツールバー

ツールバーには、次の表で説明するオプションが含まれています。

オプション	説明
新規(New)	新しいマクロを作成します。
開く	過去に記録されたマクロを開いて(またはインポートして)、再生または編集します。次のファイルタイプを開くことができます。 <ul style="list-style-type: none">• Webマクロ(*.webmacro)• Burp Proxy (*.*)• HTTPアーカイブ(HAR)ファイル(*.har)
保存/ 名前を付けて 保存	現在開いているマクロを保存します。
ログアウト 条件	(ログインマクロのみ)ログアウト 条件 エディタを開きます。詳細については、「 "ログアウト 条件 エディタ" ページ193 」を参照してください。
ブラウザ設定	ブラウザ設定 (Browser Settings) ダイアログを開きます。詳細については、「 "ブラウザ設定" ページ195 」を参照してください。

場所 ペイン

場所 ペインにはボタンバーがあり、そこに次の表で説明するボタンとチェックボックスが表示されます。

ボタン/チェック ボックス	説明
強調表示を再	クリックして強調表示した、単一の要求(行)を再生します。 実行

ボタン/チェックボックス	説明
生 (Play Highlighted)	(Run)] 列の関連付けられたチェックボックスが選択されている場合、強調表示された要求を再生します。 実行 (Run)] 列の他のチェックボックスは関係しません。
すべて再生 (Play All)	<p>実行 (Run)] 列で選択されている(オンになっている)要求のみを再生します。</p> <p>注記: 保存すると、すべてのステップがマクロに保存されますが、マクロを再生するたびに 実行 (Run)] 列で選択したステップだけが実行されます。</p>
停止	すべて再生 (Play All)] ボタンをクリックした後で、再生中に使用できません。現在の要求が完了すると再生を中止します。
ログアウト (Logout)	(ワークフローマクロでは表示されません。)サイトからログアウトします。ログアウトした場合に、再生される後続の要求に対してサイトがどのように反応するかを判断できます。
強調表示を削除 (Delete Highlighted)	クリックして強調表示した、単一の要求(行)を削除します。
すべて削除 (Delete All)	実行 (Run)] 列で選択されているかどうかに関係なく、すべての要求を削除します。
ログインのプロンプト (CAPTCHA)	(ワークフローマクロでは表示されません。)CAPTCHAは、ログイン応答を入力したのが人間であって、コンピュータで生成したものではないことを保証するために設計された、チャレンジアドレスポンステストです。ターゲットサイトでCAPTCHAを使用している場合は、このチェックボックスをオンにします。マクロは引き続きログアウト状態を検出しますが、OpenText DASTまたはFortify WebInspect Enterpriseのユーザは、スキャンの開始時およびログアウトが発生するたびに、手動でログインする必要があります。このオプションを選択すると、一覧表示されている要求の選択が無効にされ、HTTPトラフィックを表示する右側のペインが閉じます。

ボタンバーの下 の場所 ペインには場所が一覧表示され、次の表で説明する列が表示されます。

列	説明
実行(Run)	すべて再生(Play All)] をクリックすると、選択されている(オンになっている)ステップが実行されます。保存すると、すべてのステップがマクロに保存されますが、マクロを再生するたびに、選択したステップだけが実行されます。
除外 (Excluded)	[URL] 、 ディレクトリ(Directory)] 、または [ページ(Page)] を選択して、そのタイプの除外ルールを追加します。除外ルールは、このスキャン設定を使用するスキャンによって行われるすべての要求に適用されます。要求の除外が存在する場合、この列にはその原因も読み取り専用で表示されます。 カスタム(Custom)] 、 非許可ホスト(Disallowed Host)] 、または [ルート外(Outside Root)] (スキャンの設定の開始時に フォルダに限定(Restrict to folder)] が選択された場合)です。
メソッド	要求のメソッド(GETまたはPOSTなど)。
ステータス	要求に対する応答のステータス(302または200など)。
実際(Actual)	応答で返された実際のステータス。ステータスが予期した値と異なる場合、再生中に表示されます。
URL	要求のURL。

右下のペインには、次の表で説明するタブが含まれています。

タブ	説明
詳細(Details)	左側のペインで選択されている(強調表示されている)要求に関して、要求データが右上のペインに表示され、関連する応答データが右下のペインに表示されます。
状態(State)	状態を表している、または状態を表す可能性があるすべての項目のコレクション。これらは、マクロがアクセスしたあらゆる場所で見られたものです。これらを選んで自由に組み合わせたものを、ある状態を表すものとして位置づけたり、さまざまなタイプの項目を手動で追加したりすることができます。Webアプリケーションでは、特定のパラメータに「ステートフル」というマークを付けなければならない場合があります。
パラメータ (Parameters)	(ワークフローマクロでは表示されません。)ログインマクロでフォーム入力フィールドをユーザ名またはパスワード入力として指定できるようにします。こうして、IEテクノロジーを使用するマクロでユーザ名とパスワードのパラメータを使用して、スキャン時に指定できるようにします。

マクロの記録


セッションベースのWeb Macro Recorderは、IEテクノロジーを使用してマクロを記録します。このトピックでは、セッションベースのWeb Macro Recorderを使用してログインマクロとワークフローマクロを対話的に記録するタスクについて説明します。

注記: 以下の手順では、マクロの記録に関する一般的な手順について説明します。最良の結果を得るには、黄色の指示バーの案内に従ってマクロを記録してください。

セッションベースのWebマクロレコーダにアクセスする方法については、「["セッションベースのWeb Macro Recorderへのアクセス" ページ186](#)」を参照してください。

ログインマクロの記録

セッションベースのLogin Macro Recorderで、次の操作を行います。

1. **記録(Record)]**をクリックします。
2. アドレスフィールドにターゲット URLを入力して、 をクリックします。
3. アプリケーションにログインします。

注記: IEテクノロジーでは、ログインするためにユーザが可変セットの質問に回答する必要があるWebサイトはサポートされていません。

アプリケーションにアクセスしてログインすると、要求データのテーブルが場所ペインに追加されます。

4. ログインしたら、**停止(Stop)]**をクリックします。

重要! ログアウトしないでください。

マクロが保存されます。

5. **再生(Play)]**をクリックします。
マクロが最初から再生され、アプリケーションにアクセスしてログインします。
6. マクロが正しく再生されたかどうかを指定します。つまり、ログインマクロがターゲットサイトに正常にログインしたかどうかです。

- アプリケーションに正常にアクセスしてログインした場合は、**[はい(Yes)]**をクリックします。


マクロレコーダは自動的にログアウト条件を検出しようとします。ログアウト条件が検出されると、マクロは完了します。ログアウト条件が検出されない場合は、手動で識別する必要があります。詳細については、「["ログアウト条件エディタ" 次のページ](#)」を参照してください。

- アプリケーションに正常にアクセスしてログインしなかった場合は、**[いいえ(No)]**をクリックします。 **作成(Create)]**をクリックして新しいマクロを起動するか、「["マクロのデバッグ" ページ196](#)」を参照してください。

保存後にマクロを変更した場合は、Login Macro Recorderを閉じるときに、続行する前に変更を保存するように求めるメッセージが表示されます。

ワークフローマクロの記録

セッションベースのWorkflow Macro Recorderで、次の操作を行います。

1. アドレスフィールドにワークフローの開始 URL を入力して、 をクリックします。
2. **記録(Record)** をクリックします。
3. マクロに記録しようとしているページに移動します。
アプリケーション内を移動すると、要求データのテーブルが場所ペインに追加されます。
4. ワークフローのすべてのステップを記録した後で、**停止(Stop)** をクリックします。
マクロが保存されます。
5. **再生(Play)** をクリックします。
マクロが最初から再生され、ワークフローに記録されているアプリケーションの各部分にアクセスします。
6. マクロが正しく再生されたかどうかを指定します。
 - ワークフローに記録されているアプリケーションの各部分に正常にアクセスした場合は、**はい(Yes)** をクリックします。マクロが完了します。
 - ワークフローに記録されているアプリケーションの各部分に正常にアクセスしなかった場合は、**いいえ(No)** をクリックします。**作成(Create)** をクリックして新しいマクロを起動するか、「["マクロのデバッグ" ページ196](#)」を参照してください。

保存後にマクロを変更した場合は、Workflow Macro Recorderを閉じるときに、続行する前に変更を保存するように求めるメッセージが表示されます。

ログアウト条件エディタ


ログアウト条件エディタを使用して、ログインマクロのログアウト条件を作成または編集できます。必要な数の異なるログアウト条件を指定することが可能であり、これらの条件のいずれかが満たされた場合、OpenText DASTまたはFortify WebInspect Enterpriseはログインマクロを呼び出して再ログインし、中断した場所からスキャンを再開します。すべてのログアウト条件の最終セットは、ターゲットサイトのスキャン中にログアウトされるケースすべてについてカバーする必要があります。

セッションベースのLogin Macro Recorderが自動的にログアウト条件を検出することに成功すると、ログアウト条件は次のいずれかの種類に分類されます。

- **自動リダイレクト**。ターゲットサイトが302リダイレクトで応答することがセッションベースのLogin Macro Recorderによって検出された場合に、この種類のログアウト条件が作成されます。正規表現(regex)の形式になります。
- **自動**。ターゲットサイトが302リダイレクト以外(例: 200)で応答することがセッションベースのLogin Macro Recorderによって検出された場合に、この種類のログアウト条件が作成されます。

ログアウト条件の追加

新しいログアウト条件を追加するには:

1. ツールバーの **ログアウト条件(Logout Conditions)** ボタンをクリックします。
2. **ログアウト条件(Logout Conditions)** ペインで、 をクリックします。
新しいログアウト条件が追加されます。
3. **プロパティ(Properties)** ペインで、このログアウト条件のログアウトを識別する正規表現(regex)を作成します。


正規表現とは、文字列のセットを表すパターンです。正規表現は、さまざまな演算子を使用して小さな式を組み合わせることによって、数式のように構築されます。正規表現に関する知識を持つユーザだけが、この機能を使用するようにしてください。

Regexは、a)保護されたページにアクセスするためのログインユーザの要求への応答と、b)同じ保護されたページにアクセスするために、ログインしていないユーザからの同じ要求に対する応答の違いを反映する必要があります。Regexを構築する一般的な手順は次のとおりです。

- a. Webプロキシツールを起動して、Webトラフィックを記録します。『*OpenText™ Dynamic Application Security Testing*ツールガイド』のWeb Proxyのヘルプまたは「Web Proxy」の章を参照してください。
 - b. 正當にターゲットサイトにログインし、保護されたページのURLをコピーします。
 - c. ログアウトして、コピーしたURLを使用して、ログインせずに保護されたページにアクセスします。
 - d. 応答を比較し、ログインせずに保護されたページにアクセスした時の応答の固有な点を特定します。
 - e. 正規表現エディタツールを開きます。『*OpenText™ Dynamic Application Security Testing*ツールガイド』の正規表現エディタのヘルプまたは「正規表現エディタ」の章を参照してください。
 - f. ログインせずに保護されたページにアクセスした時の応答の固有な点を反映したRegexを構築します。
 - g. ログアウト条件エディタの **Regex** フィールドに正規表現をコピーします。
4. **OK** をクリックしてログアウト条件を保存し、ログアウト条件エディタを閉じます。

ログアウト条件の削除

ログアウト条件を削除するには:

1. **ログアウト条件(Logout Conditions)** ペインで、削除するログアウト条件を選択します。
2.  をクリックします。

ブラウザ設定

OpenText DASTまたはFortify WebInspect Enterprise管理コンソールで、セッションベースのWebマクロレコーダをスタンドアロンモードで使用する場合は、ツールバーの **ブラウザ設定 (Browser Settings)]** ボタンをクリックして、 **プロキシ設定 (Proxy Settings)]** タブと **ネットワーク認証 (Network Authentication)]** タブを表示します。

注記: ブラウザ設定はマクロには保存されません。

プロキシ設定 (Proxy Settings)] タブ

次の表で説明されているオプションのいずれかを選択します。

オプション	説明
直接接続(プロキシ無効) (Direct Connection (proxy disabled))	プロキシサーバを使用しない場合は、このオプションを選択します。
プロキシ設定の自動検出 (Auto detect proxy settings)	WPAD (Web Proxy Autodiscovery)プロトコルを使用してプロキシ自動設定ファイルを見つけ、ブラウザのWebプロキシ設定を行うには、このオプションを選択します。
システムのプロキシ設定を使用する(Use System proxy settings)	ローカルマシンからプロキシサーバ情報をインポートするには、このオプションを選択します。
Firefoxプロキシ設定を使用する(Use Firefox proxy settings)	Firefoxからプロキシサーバ情報をインポートするには、このオプションを選択します。
PACファイルを使用してプロキシ設定を行う(Configure proxy settings using a PAC file)	[URL] ボックスで指定した場所にあるPAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードするには、このオプションを選択します。
プロキシ設定を明示的に行う (Explicitly configure proxy settings)	次のように、要求された情報を入力してプロキシを設定するには、このオプションを選択します。 <ul style="list-style-type: none">• サーバ(Server): プロキシサーバのURLまたはIPアドレスを入力します。• ポート(Port): ポート番号を入力します(たとえば、8080など)。

オプション	説明
	<ul style="list-style-type: none">• タイプ(Type): プロキシサーバ経由のTCPトラフィックを処理するプロトコル(標準、SOCKS4、またはSOCKS5)を選択します。• 認証(Authentication): 認証方法を選択します。認証方法の詳細については、製品のヘルプまたはユーザガイドを参照してください。• ユーザ名 (User Name): ユーザ名を指定します。• パスワード(Password): パスワードを指定します。• プロキシをバイパスするサイト(Bypass proxy for): 特定のIPアドレス(内部テストサイトなど)にアクセスするためにプロキシサーバを使用する必要がない場合は、このオプションを選択して、ボックスにアドレスまたはURLを入力します。エントリを区切る場合は、カンマを使用します。

ネットワーク認証 (Network Authentication)] タブ

ネットワーク認証が必要な場合:

1. **ネットワーク認証 (Network Authentication)]** をクリックします。
2. **方法(Method)]** リストからいずれかの方法を選択します。方法は次のとおりです。
 - ADFS CBT
 - 自動
 - 基本
 - ダイジェスト
 - Kerberos
 - ネゴシエート(Negotiate)
 - NT LAN Manager (NTLM)
3. ネットワーク認証のユーザ名とパスワードを指定します。
4. **クライアント証明書(Client Certificate)]** チェックボックスをオンまたはオフにします。オンにした場合は、証明書ストアフィールドに入力して、証明書を選択します。

マクロのデバッグ

このトピックでは、主に **場所(locations)]** ペインでマクロを対話的にデバッグする基本的なステップについて説明します。

場所 (Locations)] ペインでの場所の詳細と状態の表示

記録された場所の詳細と状態を表示するには:

1. 場所(locations)] ペインのテーブルで、マクロでエラーが発生した場所を選択します。

Run	Method	Expected	Actual	URL
<input checked="" type="checkbox"/>	GET	200	302	http://zero.webappsecurity.com:80/bank/account-activity.html?acc
<input checked="" type="checkbox"/>	GET	200	200	http://zero.webappsecurity.com:80/resources/js/jquery-ui.min.js
<input checked="" type="checkbox"/>	GET	200	403	http://zero.webappsecurity.com:80/bank/account-activity-show-tr
<input checked="" type="checkbox"/>	POST	200	403	http://zero.webappsecurity.com:80/bank/account-activity-show-tr
<input checked="" type="checkbox"/>	POST	200	403	http://zero.webappsecurity.com:80/bank/account-activity-show-tr
<input checked="" type="checkbox"/>	GET	302	302	http://zero.webappsecurity.com:80/bank/redirect.html?url=transfe
<input checked="" type="checkbox"/>	GET	200	302	http://zero.webappsecurity.com:80/bank/transfer-funds.html
<input checked="" type="checkbox"/>	POST	200	302	http://zero.webappsecurity.com:80/bank/transfer-funds-verify.htm
<input checked="" type="checkbox"/>	GET	302	302	http://zero.webappsecurity.com:80/bank/redirect.html?url=pay-bil
<input checked="" type="checkbox"/>	GET	200	302	http://zero.webappsecurity.com:80/bank/pay-bills.html
<input checked="" type="checkbox"/>	GET	200	403	http://zero.webappsecurity.com:80/bank/pay-bills-saved-payee.ht

2. デフォルトでは、詳細(Details)] タブには要求データと応答データが表示されます。スキーム(Scheme)]、ホスト(Host)]、およびポート(Port)] が正しいことを確認します。
3. 状態(State)] タブをクリックして、マクロ再生中に状態が失われたかどうかを判別します。
4. 必要に応じて、状態を維持する新しい方法を追加できます。手順は次のとおりです:
 - a. タイプ(Type)] ドロップダウンリストからタイプを選択します。タイプのオプションは次のとおりです。
 - Regex
 - クエリ(Query)
 - ポスト(Post)
 - クッキー(Cookie)
 - カスタム(Custom)
 - b. 名前(Name)] フィールドに新しい方法の名前を入力します。
 - c. 追加(Add)] をクリックします。

ステップ(場所)の再生

1つのステップまたは場所を再生するには:

1. 場所(locations)] ペインのテーブルで、マクロでエラーが発生した場所を選択します。
2. 強調表示を再生(Play Highlighted)] をクリックします。

再生中のステップ(場所)の無効化/有効化

無効にされたステップまたは場所はマクロ内に残り、後で再び有効にできますが、再生されません。

再生中にマクロステップまたは場所を無効にするには:

- **場所(locations)]** ペインのテーブルで、その場所の **実行(Run)]** 列のチェックボックスをクリアします。

再生中にマクロステップを再び有効にするには:

- **場所(locations)]** ペインのテーブルで、その場所の **実行(Run)]** 列のチェックボックスをオンにします。

ステップ(場所)の削除

マクロから場所を永久に削除するには:

1. **場所(locations)]** ペインのテーブルで、マクロでエラーが発生した場所を選択します。
2. **強調表示を削除>Delete Highlighted)]** をクリックします。

第18章: イベントベースのWebマクロレコーダ

OpenText™ Dynamic Application Security Testing(DAST)、OpenText™ Fortify WebInspect Enterprise、およびOpenText™ ScanCentral DASTにはイベントベースのWebマクロレコーダツールが2つ含まれています。1つはログインマクロ用、もう1つはワークフローマクロ用です。この章では、これらの2つのツールは、特定のログイン関連およびワークフロー関連のコンテンツを除き、一般的に「Webマクロレコーダ」と呼ばれます。

使用可能なバージョン

イベントベースのWebマクロレコーダは、Microsoft Windows®およびMac®の両方のオペレーティングシステムで使用できます。この章では、WindowsバージョンのWebマクロレコーダが示されています。ただし、特に説明しない限り、Macバージョン機能も同じです。

用語「センサ」について

OpenText DASTユーザインタフェースを介した直接のユーザ操作なしにリモートでスケジュールまたは要求されたスキャンを実行する目的でFortify WebInspect EnterpriseまたはOpenText ScanCentral DASTに接続された場合、OpenText DASTセンサはOpenText DASTアプリケーションです。このドキュメントの内容がOpenText DAST、Fortify WebInspect Enterprise、およびOpenText ScanCentral DASTに適用される場合には、用語「センサ」が使用されます。

マクロについて

ログインマクロとは、Webサイトにアクセスしてログインするときに発生するイベントの記録です。その後、この記録を使用してセンサーにスキャンを開始するように指示できます。ワークフローマクロは、サイト上の特定のURLの記録です。詳細については、「["ログインマクロ" ページ204](#)」および「["ワークフローマクロ" ページ205](#)」を参照してください。

TruClientテクノロジー

イベントベースのWebマクロレコーダツールは、TruClientテクノロジーを使って設計されました。イベントベースの機能とTruClientブラウザテクノロジーを使用してマクロを記録および再生します。

Webマクロレコーダの制限

Webマクロレコーダは、FlashまたはSilverlightアプリケーションの記録をサポートしていません。

Webマクロレコーダで使用するTruClientテクノロジーは、元々、OpenTextLoadRunnerOpenTextおよびパフォーマンスセンターで使用するために開発されたAjax TruClientテクノロジーを応用したものです。これらの製品にフル機能バージョンのすべての機能が組み込み、またはサポートされているということではありません。

マクロ内のCookieヘッダ

マクロを再生すると、センサーは、記録されたマクロに組み込まれている可能性のあるCookieヘッダを送信しません。

マクロ内のURL

URLがマクロ内にある場合、スキャン設定の除外ルールに関係なく、マクロの再生時に要求が常に応答されます。

イベントベースのWebマクロレコーダのインストール

イベントベースのWebマクロレコーダは、WindowsにOpenText DASTをインストールする際に、OpenText DASTツールキットの一部としてインストールされます。スタンドアロンバージョンは、WindowsとMacの両方のオペレーティングシステムにインストールできます。

WindowsでのスタンドアロンWebマクロレコーダのインストール

Windowsバージョンをインストールするには:

1. **MacroRecorder.msi**ファイルをダブルクリックします。
[Fortifyマクロレコーダの設定 (Fortify Macro Recorder Setup)] が開きます。

注記: ScanCentral DAST APIコンテナからファイルをダウンロードした場合、ファイル名はMacroRecorderWindowsX64Setup.exeです。

2. チェックボックスをオンにして、ライセンス契約の条項に同意します。
3. **[インストール]** をクリックします。
4. **完了 (Finish)** をクリックします。

MacでのスタンドアロンWebマクロレコーダのインストール

重要! ダウンロードしたWebマクロレコーダのDMGファイルが、macOS® Gatekeeperにより隔離される場合は、このファイルを信頼されたソース(ScanCentral DAST APIコンテナなど)からダウンロードします。

Macバージョンをインストールするには:

1. **MacroRecorder<バージョン>.dmg** ディスクイメージファイルをダブルクリックします。
プログラムがシステムにマウントされます。

注記: ScanCentral DAST APIコンテナからファイルをダウンロードした場合、ファイル名はMacroRecorderMacOSArm64Setup.dmgです。

2. 左画面の **ロケーション(Locations)** で **マクロレコーダ(MacroRecorder)** をクリックし、インストールを開きます。
3. **マクロレコーダ(MacroRecorder)** アイコンを **アプリケーション** アイコンにドラッグします。

イベントベースのWebマクロレコーダへのアクセス

以下の段落では、OpenText DAST、Fortify WebInspect EnterpriseおよびOpenText ScanCentral DASTでイベントベースのWebマクロレコーダを起動するさまざまな方法について説明します。

OpenText DASTまたはFortify WebInspect Enterpriseのログインマクロ

新しいログインマクロを記録するか、OpenText DASTまたはFortify WebInspect EnterpriseのTruClientブラウザ技術を使用して記録された既存のログインマクロを次の方法で選択およびオプションで編集できます。

- Firefoxをレンダリングエンジンとしてガイド付きスキャンを設定する場合は、ターゲットサイトにログインマクロが必要と指定し、**[作成]** をクリックして新しいログインマクロを記録するか、既存のログインマクロを選択およびオプションで編集します。
- Firefoxをレンダリングエンジンとして、OpenText DASTの基本スキャンまたはFortify WebInspect EnterpriseのWebサイトスキャンを設定する場合、ステップ2で **サイト認証(Site Authentication)** を選択して新しいログインマクロを記録するか、既存のログインマクロを選択(およびオプションで編集)します。
- OpenText DASTツールバーで、**ツール(Tools)] > ログインマクロレコーダ(Login Macro Recorder)] > マクロエンジン(Macro Engine)] > イベントベース(優先)(Event-based (preferred))** の順にクリックして、ログインマクロレコーダをスタンドアロンモードで実行し、新しいログインマクロを記録するか、既存のログインマクロを開きます(必要に応じて編集します)。

- Fortify WebInspect Enterpriseの管理コンソールツールバーで、**ツール(Tools)] > ログインマクロレコーダ(Login Macro Recorder)] > マクロエンジン(Macro Engine)] > イベントベース(優先)(Event-based (preferred))**の順にクリックして、ログインマクロレコーダをスタンドアロンモードで開き、新しいログインマクロを記録するか、既存のログインマクロを開きます(必要に応じて編集します)。
- セキュリティツールキットを使用して、**起動(Start)] > Fortify] > ログインマクロレコーダ(イベント)(Login Macro Recorder (Event))**の順にクリックして、ログインマクロレコーダをスタンドアロンモードで実行し、新しいログインマクロを記録するか、既存のログインマクロを開きます(必要に応じて編集します)。
- 既存のマクロをダブルクリックして、TruClientサイドバーおよびブラウザでマクロを開きます。

OpenText DASTまたはFortify WebInspect Enterpriseのワークフローマクロ

新しいワークフローマクロを記録するか、OpenText DASTまたはFortify WebInspect EnterpriseのTruClientブラウザ技術を使用して記録された既存のワークフローマクロを次の方法で選択およびオプションで編集できます。

- Firefoxをレンダリングエンジンとしてガイド付きスキャンを設定する場合は、**[ワークフロー > 1]でスキャンタイプがワークフロー以降であることを指定します。ワークフローステップの管理、新しいワークフローマクロの記録、または既存のワークフローマクロのインポートおよびオプションで編集を行います。**
- FirefoxをレンダリングエンジンとしてOpenText DASTで基本スキャンを設定する場合、ステップ1で **[ワークフロー駆動型スキャン(Workflow-Driven Scan)]**を選択し、**記録(Record)]**または**管理(Manage)]**をクリックして新しいワークフローマクロを記録するか、既存のワークフローマクロを選択(およびオプションで編集)します。
- OpenText DASTツールバーで、**ツール(Tools)] > ワークフローマクロレコーダ(Workflow Macro Recorder)] > マクロエンジン(Macro Engine)] > イベントベース(優先)(Event-based (preferred))**の順にクリックして、ワークフローマクロレコーダをスタンドアロンモードで実行し、新しいワークフローマクロを記録するか、既存のワークフローマクロを開きます(必要に応じて編集します)。
- Fortify WebInspect Enterpriseの管理コンソールツールバーで、**ツール(Tools)] > ワークフローマクロレコーダ(Workflow Macro Recorder)] > マクロエンジン(Macro Engine)] > イベントベース(優先)(Event-based (preferred))**の順にクリックして、ワークフローマクロレコーダをスタンドアロンモードで開き、新しいワークフローマクロを記録するか、既存のワークフローマクロを開きます(必要に応じて編集します)。
- セキュリティツールキットを使用して、**起動(Start)] > [Fortify] > [ワークフローマクロレコーダ(イベント)(Workflow Macro Recorder (Event))**をクリックして、ワークフローマクロレコーダをスタンドアロンモードで実行し、新しいワークフローマクロを記録するか、既存のワークフローマクロを開きます(必要に応じて編集します)。
- 既存のマクロをダブルクリックして、TruClientサイドバーおよびブラウザでマクロを開きます。

OpenText ScanCentral DASTのログインマクロ

WebマクロレコーダツールをScanCentral DAST APIコンテナからローカルコンピュータにダウンロードした後、次の方法でログインマクロレコーダを開くことができます。

- **ScanCentral DAST設定の構成**ウィザードで標準スキャンを設定する場合は、**認証**ページで **マクロレコーダを開く25.4** をクリックします。

重要! Webマクロレコーダがローカルコンピュータにダウンロードおよびインストールされていない場合は、Webマクロレコーダを開くことができません。

- ログインマクロレコーダをスタンドアロンモードで実行するには、**[起動] > [Fortify ScanCentral DAST] > [ログインマクロレコーダ]** をクリックし、新しいログインマクロを記録するか、既存のログインマクロを開くおよびオプションで編集します。
- 既存のマクロをダブルクリックして、TruClientサイドバーおよびブラウザでマクロを開きます。

Webマクロレコーダのダウンロードの詳細については、「*OpenText™ ScanCentral DASTの設定および使用ガイド*」を参照してください。

OpenText ScanCentral DASTのワークフローマクロ

WebマクロレコーダツールをScanCentral DAST APIコンテナからローカルコンピュータにダウンロードした後、次の方法でワークフローマクロレコーダを開くことができます。

- **ScanCentral DAST設定の構成**ウィザードでワークフロー駆動型スキャンを設定する場合は、**ターゲット**ページで **ワークフローマクロレコーダを開く25.4** をクリックします。

重要! Webマクロレコーダがローカルコンピュータにダウンロードおよびインストールされていない場合は、Webマクロレコーダを開くことができません。

- ワークフローマクロレコーダをスタンドアロンモードで実行するには、**[起動] > [Fortify ScanCentral DAST] > [ワークフローマクロレコーダ]** をクリックし、新しいワークフローマクロを記録するか、既存のワークフローマクロを開くおよびオプションで編集します。
- 既存のマクロをダブルクリックして、TruClientサイドバーおよびブラウザでマクロを開きます。

Webマクロレコーダのダウンロードの詳細については、「*OpenText™ ScanCentral DASTの設定および使用ガイド*」を参照してください。

macOS上のスタンドアロンWebマクロレコーダ

スタンドアロンWebマクロレコーダをmacOSにインストールしたら、次の方法でアプリケーションを起動できます。

- **アプリケーション** で、 **MacroRecorder.app** アイコンをクリックします。
- **Launchpad** を使用して、検索フィールドに「MacroRecorder」と入力し、Webマクロレコーダアイコン  をクリックします。

- メニューバーのWebマクロレコーダアイコンをクリックし、[Webマクロレコーダを開く(Open Web Macro Recorder)]を選択します。
- 既存のマクロをダブルクリックして、TruClientサイドバーおよびブラウザでマクロを開きます。

ログインマクロ

ログインマクロは、WebサイトまたはWebアプリケーションにアクセスしてログインするために必要なアクティビティの記録です。通常は、ユーザ名とパスワードを入力し、[ログイン]や[ログオン]などのボタンをクリックします。スキャンを設定する場合、通常は、以前に記録したログインマクロを指定するか、またはスキャンで使用する時点で新しいログインマクロを記録します。

ログアウト条件

センサーがアプリケーションからログアウトした場合にスキャンが途中で終了するのを防ぐために、ログインマクロでは、ログアウトが発生したことを明確に示す少なくとも1つのログアウト条件も指定する必要があります。スキャン中に、センサーは次のさまざまな理由でログアウトされる可能性があります。

- ターゲットサイトが動作する通常のログアウト
- タイムアウトなどのターゲットサイトのエラー状態
- 無効なパラメータなどのマクロ自体のエラー

ログインマクロの一部としてログアウト条件を指定すると、スキャン中に予期しないログアウトが発生した場合に、ユーザが何度も手動でログインし直す必要がなくなります。サイトをスキャンする際、センサーは各ターゲットサイトの応答を分析して状態を判断します。センサーがログアウトしていると判断した場合は、ログインマクロを実行して再度ログインし、ログアウトが発生した時点でサイトのクロールまたは監査を再開します。

複数のログアウト条件を指定できます。これらの条件が満たされた場合、センサーはログインマクロを再生して再ログインし、中断した所からスキャンを再開します。

参照情報

["ログアウト条件の使用" ページ259](#)

ワークフローマクロ

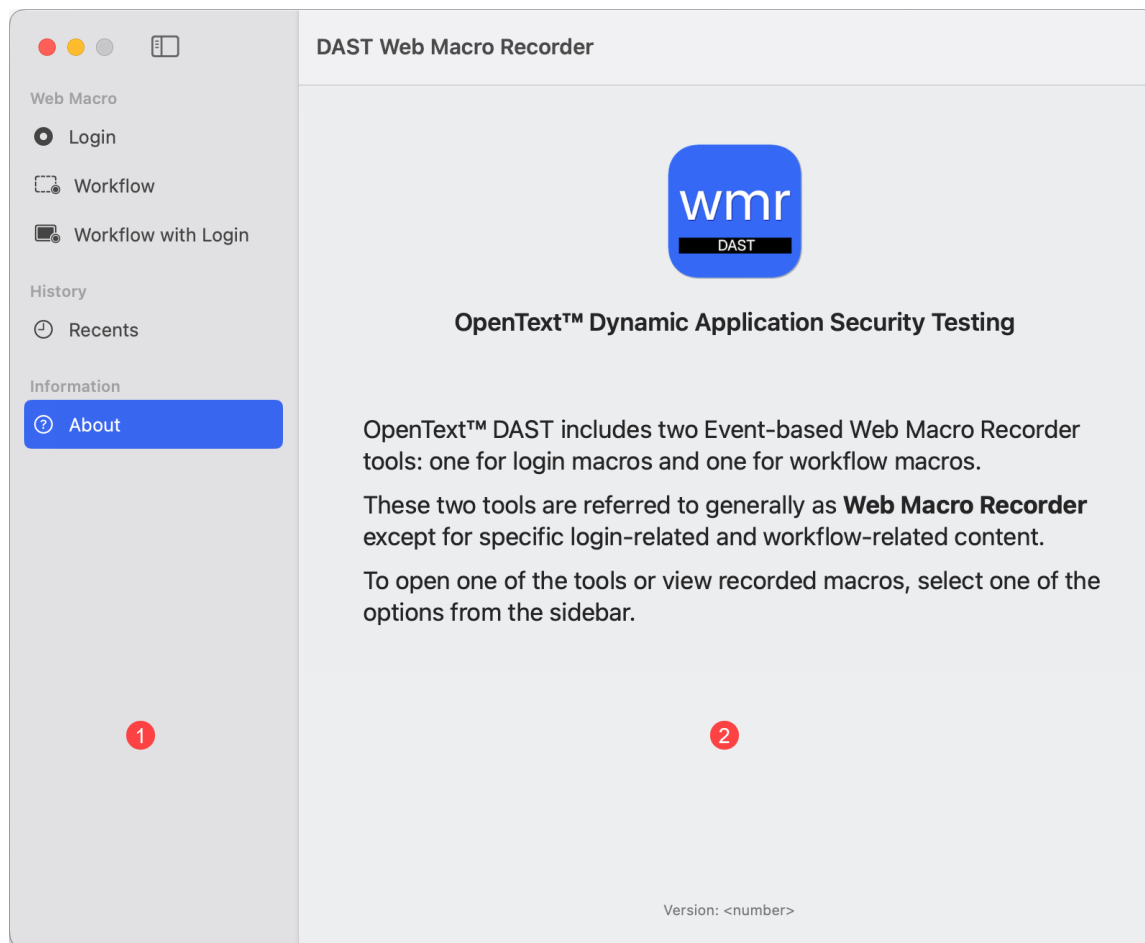
ワークフローマクロは、サイト上で手動で移動する特定のURLの記録です。、OpenText DASTでの基本スキャンまたはOpenText ScanCentral DASTやでのスキャンを設定する場合は、以前に記録したワークフローマクロを指定するか、スキャンを使用する時点で新しいワークフローマクロを記録します。センサーは、ワークフローマクロに記録されたURLのみを監査し、監査中に検出されたハイパーリンクは追いません。この種のマクロは、最も頻繁にアプリケーションの特定のサブセクションに焦点を当てる場合に使用されます。マクロ記録プロセスの観点では、ログインマクロとの基本的な違いは次のとおりです。

- ワークフローマクロには、記録中にユーザが移動した特定のURLのみが含まれます。ワークフローマクロは、再生時にそれらのURLにのみアクセスします。
- ワークフローマクロではログアウト条件は不要です。

注記: Webサイトで認証が必要な場合は、ログインステップをワークフローマクロに記録しないでください。代わりに、別のログインマクロを記録してWebサイトにログインしてください。詳細については、「["ログインマクロ" 前のページ](#)」を参照してください。

メインアプリケーションウィンドウの操作 (Macのみ)

macOSでWebマクロレコーダを起動すると、メインアプリケーションウィンドウが開きます。






次の表で、メインアプリケーションウィンドウの各部について説明します。

項目	説明
1	<p>ナビゲーションサイドバーには、ログイン、ワークフロー、およびログインマクロを使用したワークフローの記録用オプションと、最近編集したマクロにアクセスするためのオプションがあります。</p> <p>ナビゲーションサイドバーの [ログイン] ボタン、[ワークフロー] ボタン、および ログインを使用したワークフロー(Workflow with Login)] ボタンの使用の詳細については、"レコードボタンの使用 (Macのみ)" ページ228を参照してください。</p>
2	<p>詳細ビューには、ナビゲーションサイドバーで選択したオプションのさまざまな詳細や手順が表示されます。</p>

マクロアイコンについて

次の表で、さまざまな種類のマクロを示すために使用されるアイコンについて説明します。

アイコン	Type
	ログインマクロ
	ワークフローマクロ
	ログインマクロを使用したワークフロー

最近のリストの使用

最近のリストを使用すると、最近使用したマクロに素早くアクセスして表示または編集できます。


最近使用したマクロを表示または編集するには:

1. ナビゲーションサイドバーで、**最近 (Recents)** をクリックします。
最近編集した5つのマクロのリストが詳細ビューに表示されます。

ヒント: マクロの上にカーソルを合わせると、ツールチップにファイルへのディレクトリパスが表示されます。

2. 最近のリストのマクロをダブルクリックします。
マクロはTruClientサイドバーとブラウザで開きます。

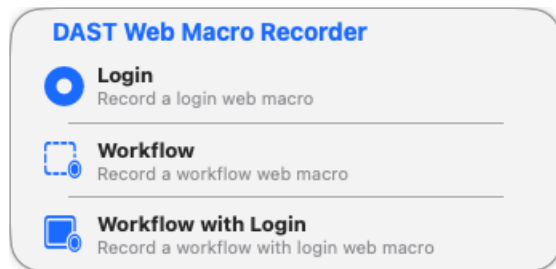
最近のリストオプションの使用

最近のリストでマクロのオプション()アイコンをクリックすると、次のオプションを使用できます。

- **開く** - TruClientサイドバーおよびブラウザでマクロを開きます。
- **ファイルの場所を開く (Open file location)** - マクロが保存されているディレクトリを開きます。
- **クイックルック** - Webマクロレコーダを開かなくてもマクロに関する情報を表示します。
- **削除** - 最近のリストからマクロを削除します。

Webマクロレコーダウィジェットの使用 (Macのみ)

Webマクロレコーダウィジェットを使用すると、Webマクロの記録をすばやく起動できます。デフォルトで、ウィジェットには [ログイン]、[ワークフロー]、[ログインマクロを使用したワークフロー] という記録オプションが表示されます。



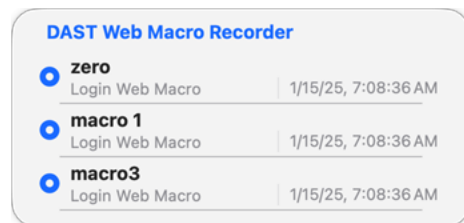
デスクトップにウィジェット追加する方法については、Apple®のドキュメントを参照してください。

ウィジェットの編集

Webマクロレコーダウィジェットをデスクトップに追加した後、マクロの最近のリストを表示する設定を行います。

1. Macで、Webマクロレコーダウィジェットをcontrolキーを押しながらクリックし、**[Edit "DAST Web Macro Recorder"...]**を選択します。
2. **[Show Recent Macros]**を有効の位置にスライドします。
3. **[Done]**をクリックします。

Webマクロレコーダウィジェットに、最近編集された3つのマクロが表示されます。リストからマクロを選択すると、Webマクロレコーダでそのマクロが開きます。



クイックルックの使用 (Macのみ)

macOSのクイックルック機能を使用すると、Webマクロレコーダを実際に関なくともWebマクロファイルに関する情報を表示できます。Webマクロは暗号化可能なので、個人識別情報 (PII)を公開しない情報だけが表示されます。

すべてのマクロについて、次の情報が表示されます。

- Macro Type - [ログイン]、[ワークフロー]、または [ログインマクロを使用したワークフロー] のいずれかを示します。
- Friendly Name - ユーザが指定したマクロ名を識別します。
- Engine Version -- TruClientエンジンのバージョンを示します。
- Browser Version - 使用されているTruClientブラウザのバージョン(130.0など)を示します。
- Macro Modification Date - マクロが最後に変更された日付を示します。

注記: この日付は、システムファイルの変更日とは異なる場合があります。例えば、別のマシンからコピーされたマクロでは、ファイルが最後に変更された日付ではなく、ファイルがコピーされた日付が表示される場合があります。

ログインマクロの場合、次の追加情報が表示されます。

- Start Url - マクロの開始URLを指定します。
- Username - 資格情報をアプリケーションへのログインに使用するユーザ名を指定します。
- Has MFA - マクロに多要素認証が含まれるかどうかを示します。
- Has Event-Based LC - マクロにイベントベースのログアウト条件が含まれるかどうかを示します。
- Has Verification Step - マクロにログイン検証ステップが含まれるかどうかを示します。

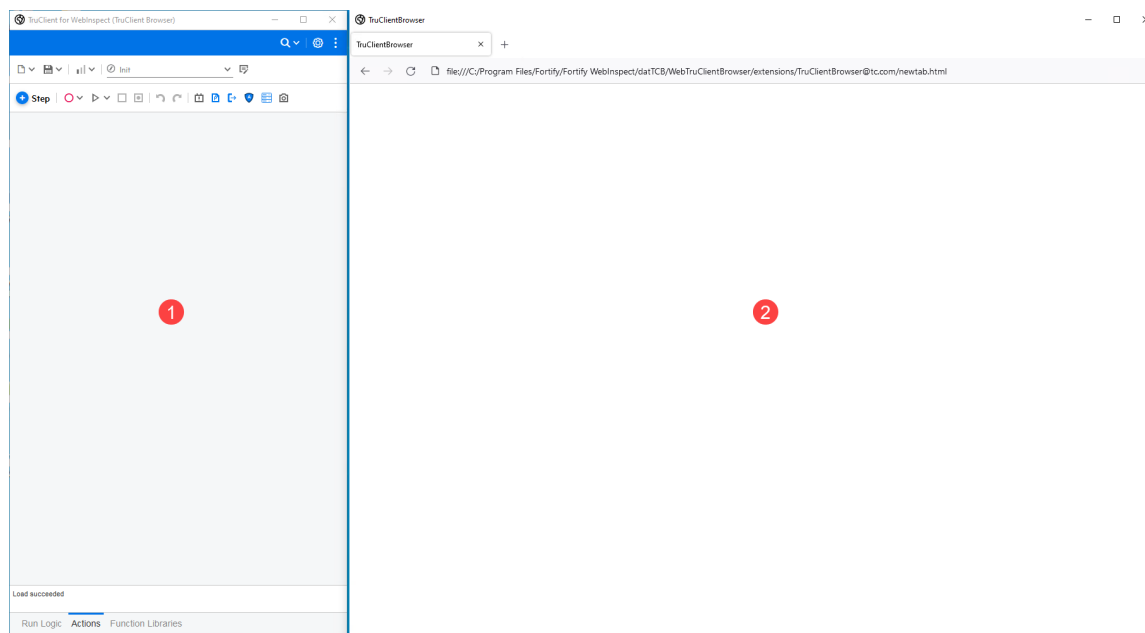
ヒント: マクロに関する情報を表示するには、ファイルへのアクセス権が必要です。必要に応じて、アクセス権を調整できます。アクセス権の調整方法については、Appleのドキュメントを参照してください。

クイックルックを使用するには:

- Webマクロファイルを選択した場合は、スペースバーを押します。
クイックルックには、マクロの詳細が表示されます。
クイックルックビューから、**マクロレコーダで開く(Open with MacroRecorder)**をクリックすると、Webマクロレコーダでマクロが開きます。

ユーザインタフェースについて

WindowsでWebマクロレコーダが開くと、次のイメージに示されているように、2つのウィンドウが横並びで表示されます。




次の表に、2つのウィンドウの説明を示します。



ウィンドウ	説明
1	TruClientサイドバーウィンドウ。このウィンドウでは、記録と編集の機能をコントロールできます。
2	TruClientブラウザウィンドウ。このウィンドウを使用して、Webサイトにアクセスします。

macOSのWebマクロレコーダは、マクロの記録または再生時にTruClientサイドバーおよびブラウザを開きます。

TruClientサイドバーのマストヘッド




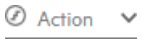
次の表は、TruClientサイドバーのマストヘッドにあるアイコンについて説明しています。











アイコン	名前(Name)	説明
	検索	検索パネルが開きます。ドロップダウンメニューには、マクロを検索したり、特定のステップ番号に移動するためのオブ





アイコン	名前(Name)	説明
		ションがあります。詳細については、「 "マクロの検索" ページ232 」を参照してください。
	一般設定	[一般設定]ダイアログボックスが開きます。詳細については、「 "設定の構成" ページ311 」を参照してください。
	詳細...	次のオプションを表示します。 ヘルプ - イベントベースのWebマクロレコーダのヘルプを開きます。 バージョン情報 - イベントベースのWebマクロレコーダのバージョン情報を表示するダイアログボックスを開きます。

TruClientサイドバーのツールバー

次の表は、TruClientサイドバーの上部にあるツールバーについて説明しています。

アイコン	名前(Name)	説明
	開く/新規	既存のマクロまたはスクリプトファイルを開くか、新しいマクロまたはスクリプトファイルを作成します。
	保存/名前を付けて保存	新しいマクロまたはスクリプトファイル、または既存のファイルのコピーを保存します。
	ステップレベル	スクリプトで表示および再生されるスクリプトレベルを変更します。 <ul style="list-style-type: none"> ■- レベル1のステップのみを表示および再生します。アプリケーションと対話するには、レベル1のステップが必要です。 ■- レベル1およびレベル2のステップを表示および再生します。レベル2のステップは、おそらくマクロにとって重要ではない方法でアプリケーションに影響します。 ■- レベル1、2、および3のステップを表示および再生します。レベル3のステップは、アプリケーションに対して明らかな影響はありません。 <p>詳細については、「"マクロ再生レベルの変更" ページ253」を参照してください。</p>
	アクションリスト	マクロに記録されている操作 (一連の手順) を表示しま

アイコン	名前(Name)	説明
		<p>す。</p> <p>注記: オプションは、[初期化]、[アクション]、および[終了]です。ただし、[初期化]オプションと[終了]オプションは適用されません。Webマクロレコーダは、[ロジックアクションの実行]ブロックにのみアクションを記録します。</p>
	アクションの管理	[アクション]ダイアログボックスが開きます。詳細については、「 "アクションの使用" ページ267 」を参照してください。
	ステップの追加	TruClientステップボックスを開き、マクロにステップを追加できるようにします。詳細については、「 "ステップボックスの使用" ページ224 」を参照してください。
	記録	マクロの記録を開始します。また、矢印を使用して、選択したステップの前、間、または後に記録するかどうかを指定できます。
	再生	マクロを再生 (または再生を再開) します。さらに、矢印を使用して、選択したステップのみを再生するか、スクリプトをステップごとに実行するか指定できます。スクリプトをステップごとに実行すると、各ステップの後に再生が一時停止します。
	一時停止	マクロの再生を一時停止します。
	停止	マクロの記録または再生を停止します。
	ブレークポイントの切り替え	選択したステップのブレークポイントを切り替えます。詳細については、「 "ブレークポイントの使用" ページ302 」を参照してください。
	元に戻す/やり直し	最後のアクションを元に戻したり、元の変更を復元したりします。
	イベントハンドラエディタ	[イベントハンドラエディタ]ダイアログボックスが開きます。詳細については、「 "イベントハンドラの使用" ページ254 」を参照してください。
	パラメータの編集	パラメータ値を設定します。詳細については、「 "パラメータの使用" ページ271 」を参照してください。

アイコン	名前(Name)	説明
	ログアウト条件の編集	ログアウト条件エディタが開きます。詳細については、「 "ログアウト条件の使用" ページ259 」を参照してください。
	認証者の編集 (Edit authenticators)	認証者 (Authenticator) ダイアログが開きます。詳細については、「 "TOTP認証の使用" ページ244 」を参照してください。
	Webストレージキーの編集	<p>Webストレージキーの管理 (Manage Web Storage Keys) ダイアログボックスが開きます。詳細については、「"Webストレージキーの使用" ページ269」を参照してください。</p> <p>このアイコンは、Webストレージのサポート (Support Web Storage) 設定が有効になっている場合にのみ表示されます。詳細については、「"対話型オプション" ページ316」を参照してください。</p>
	スナップショットビュー (Snapshot view)	サポートされていません。

コンテキストメニュー

TruClientサイドバーでステップを選択し、右クリックしてコンテキストメニューを表示します。次の表は、コンテキストメニューオプションについて説明しています。

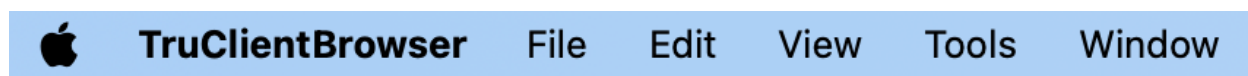
メニューオプション	説明
[このステップを再生]	選択したステップのみを再生します。
[このステップから再生]	<p>選択したステップから再生します。ターゲットステップが次の場合は、[このステップから再生]を使用できません。</p> <ul style="list-style-type: none"> 実行ロジックの一部ではないアクションに含まれています ForループまたはIfブロック内にあります Catchエラーステップです 現在のWebページでは利用できないWebオブジェクトで動作します
[このステップまで]	最初から再生し、選択したステップの前に停止します。

メニューオプション	説明
で再生]	
記録]> [ステップ前を記録 (Before step)]	選択したステップの前に、記録されたステップの次のセットを挿入します。
記録]> [ステップに記録 (Into step)]	記録されたステップの次のセットを、選択したステップに挿入します。
記録]> [ステップ後を記録 (After step)]	選択したステップの後に、記録されたステップの次のセットを挿入します。
ブレークポイントの切り替え	選択したステップにブレークポイントを挿入または削除します。
ステップをグループ化	複数のステップを1つのステップとしてグループ化します。
グループ化	<p>複数のステップを次のようにグループ化します。</p> <ul style="list-style-type: none"> • アクション - 新規または既存のアクションとして定義するステップのグループ。 • If句 - スクリプトのフローを制御するロジック構造。 • Forループ句 - ループに含まれるステップを指定された回数繰り返すロジック構造。 • 新規関数 - 関数として定義する、ログインなどのステップのグループ。 • 2要素認証 - 2要素認証コントロールセンターへの要求と、2要素認証応答を待機するステップを含むステップのグループ。
ステップのグループ解除	グループ化されたステップを複数のステップに戻します。
切り取り	選択したステップをマクロから切り取ります。
コピー	マクロ内で選択したステップをコピーします。
貼り付け	コピーしたステップをマクロに貼り付けます。
ステップのエクスポート	マクロ内で選択したステップをコピーして、別のマクロに貼り付けます。

メニューオプション	説明
ステップのインポート	エクスポートされたステップを2つ目のスクリプトに貼り付けます。
削除 (Delete)	マクロからステップを削除します。
有効にする、または無効にする	再生中にステップを無効にするか有効にするかを切り替えます。
ステップの編集	ステップを拡張して、ステップ、引数、およびトランザクションのプロパティを表示します。
すべてのステップを折りたたむ	すべてのステップとグループを最小化します。
すべてのステップを展開	すべてのステップとグループを表示します。
自動終了イベントをリセット	選択したステップを[自動: 未設定]にリセットできます。
オブジェクト識別方法を変更	オブジェクト識別方法を次に変更できます。 <ul style="list-style-type: none">• 自動• XPath• JavaScript• 記述子

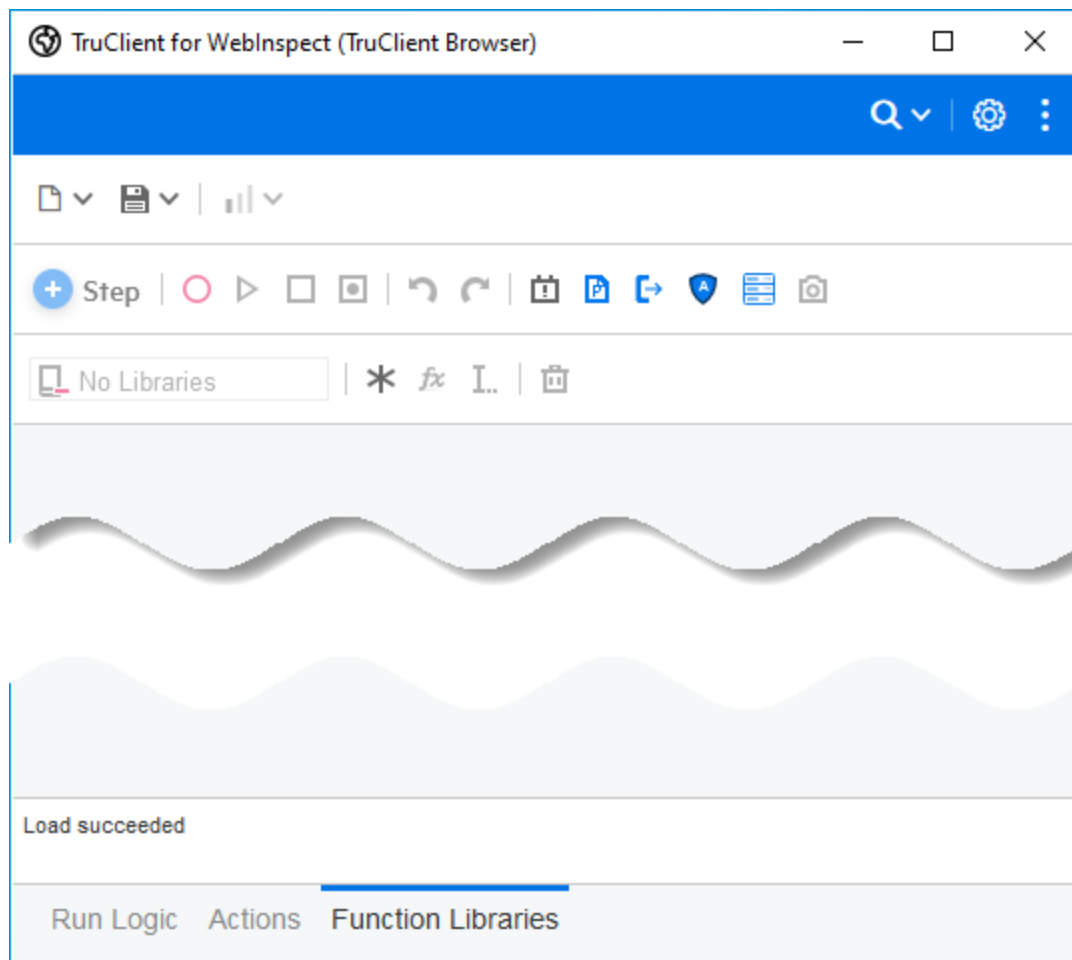
TruClientBrowserメニュー(Macのみ)

MacバージョンにはTruClientBrowserメニューが含まれています。これは、TruClient Browser ウィンドウを管理するための機能を持つMac固有のメニューです。



関数ライブラリタブについて


関数ライブラリ(Function Libraries)タブには、TruClient関数ライブラリを作成および管理するためのアイコンを含むツールバーがあります。



関数ライブラリツールバー

次の表では、関数ライブラリ(Function Libraries)]タブを選択した場合にTruClientサイドバーの上部で利用できるツールバーについて説明します。

アイコン	名前(Name)	説明
*	新規ライブラリ (New Library)]	新規ライブラリ(New Library)] ダイアログボックスが開き、新しいライブラリを作成できます。
fx	新規関数 (New Function)]	新しい関数を作成します。詳細については、「 関数ライブラリの使用 」ページ256」を参照してください。
I..	ライブラリ名の変更 (Rename Library)]	既存のライブラリの名前を変更します。 重要! {/b}ライブラリの名前を変更する場合は、そのライブラリへのすべての参照を変更します。

アイコン	名前(Name)	説明
	ライブラリの削除(Delete Library)]	スクリプトからローカル関数ライブラリを削除します。

ショートカットキーの使用

ショートカットキーを使用すると、Webマクロレコーダのほとんどの機能にアクセスできます。一部のショートカットキーは、WindowsキーボードとMacキーボードの両方で同じですが、多くは異なります。ショートカットキーを使用してさまざまな機能にアクセスする方法について、以下の表で説明します。

基本機能

次の表では、既存のマクロを開く、新しいマクロを作成する、特定の製品機能にアクセスするなどの基本的な機能のショートカットキーについて説明します。

機能	Windows	Mac
開く	<Alt>+<O>	<⌘>+<O>
新規(New)	<Alt>+<N>	<⌘>+<N>
保存	<Ctrl>+<Alt>+<S>	<⌘>+<⌘>+<S>
名前を付けて保存	<Ctrl>+<Alt>+<A>	<⌘>+<⌘>+<A>
記録	<Ctrl>+<Alt>+<R>	<⌘>+<⌘>+<R>
再生/一時停止	<Ctrl>+<Alt>+<5>	<⌘>+<⌘>+<5>
選択したステップの再生	<F7>	<F7>
ステップバイステップで再生	<F8>	<F8>
停止	<Ctrl>+<Alt>+<X>	<⌘>+<⌘>+<X>
ブレイクポイントの切り替え	<F9>	<F9>
次に移動	<Ctrl>+<G>	<⌘>+<G>
元に戻す	<Ctrl>+<Z>	<⌘>+<Z>
やり直し	<Ctrl>+<Y>	<⌘>+<Y>

機能	Windows	Mac
スナップショットビューア	<Ctrl>+<Alt>+<V>	<⌘>+<⌘>+<V>
ステップボックスを開く/閉じる	<Ctrl>+<Alt>+<K>	<⌘>+<⌘>+<K>

最近の項目機能 (Macのみ)

最近の項目で選択されたマクロで利用できるショートカットキーについて、以下の表で説明します。

機能	Mac
開く	<⌘>+<O> 入力
ファイルの場所を開く	<Shift>+<⌘>+<O>
クイックルック	<⌘>+<P> スペースバー

ログインおよびワークフロー機能 (Macのみ)

アプリケーションのログインセクションまたはワークフローセクションで利用できるショートカットキーについて、以下の表で説明します。

機能	Mac
TruClientサイドバーとブラウザを起動して、ログインマクロを記録 (ログインセクションから)	<⌘>+<S>
TruClientサイドバーとブラウザを起動して、ワークフローマクロを記録 (ワークフローセクションから)	

検索機能

次の表に、検索用のショートカットキーを示します。

機能	Windows	Mac	メモ
現在のビューで検索	<Ctrl>+<F>	<⌘>+<F>	検索ビューが閉じている場合に開く
	</> (スラッシュ)	</> (スラッシュ)	
	<'> (一重引用符)	<'> (一重引用符)	
次を検索	<F3>	<F3>	
前方検索	<Shift>+<F3>	<Shift>+<F3>	
	<Ctrl>+<Shift>+<G>	<⌘>+<Shift>+<G>	
検索から除外	<Esc>	<Esc>	検索ビューが開いている場合に閉じる
スクリプト全体を検索	<Ctrl>+<Shift>+<F>	<⌘>+<Shift>+<F>	

ステップ関連機能

ステップの再生、ステップの移動、ステップのグループ化など、記録されたマクロ内のステップに関連する機能のショートカットキーについて、次の表で説明します。

機能	Windows	Mac	メモ
ステップバイステップで再生	<F8>	<F8>	
このステップを再生	<F7>	<F7>	
	 (小文字のL)	 (小文字のL)	[ステップ]コンテキストメニューが開いている場合に
このステップから再生	<F>	<F>	[ステップ]コンテキストメニューが開いている場合に
このステップまで再生	<U>	<U>	
記録	<R>	<R>	

機能	Windows	Mac	メモ
(Record)] サブメニューを開く			
ステップ前を記録	包含	包含	記録(Record)] サブメニューが開いている場合に
ステップ後を記録	<A>	<A>	
ステップに記録	<I>	<I>	記録(Record)] サブメニューが開いていて、ステップがグループステップの場合に
ブレークポイントの切り替え	<F9>	<F9>	
	包含	包含	[ステップ] コンテキストメニューが開いている場合に
ステップをグループ化	<G>	<G>	[ステップ] コンテキストメニューが開いている場合に
[グループ化] サブメニューを開く	<u>	<u>	
アクションにグループ化	<A>	<A>	[グループ化] サブメニューが開いている場合、
If句にグループ化	<I>	<I>	
ループにグループ化	<F>	<F>	
新規関数にグループ化	<N>	<N>	
2要素認証にグループ化	<T>	<T>	

機能	Windows	Mac	メモ
切り取り	<Ctrl>+<X>	<⌘>+<X>	
	<t>	<t>	【ステップ】コンテキストメニューが開いている場合に
コピー	<Ctrl>+<C>	<⌘>+<C>	
	<C>	<C>	【ステップ】コンテキストメニューが開いている場合に
貼り付け	<Ctrl>+<V>	<⌘>+<V>	
貼り付け] サブメニューを開く	<P>	<P>	【ステップ】コンテキストメニューが開いている場合に
前に貼り付け	<Alt>+<P>	<⌘>+<P>	
	包含	包含	貼り付け(Paste)] サブメニューが開いている場合に
ここに貼り付け	<Alt>+<I>	<⌘>+<I>	
	<I>	<I>	貼り付け(Paste)] サブメニューが開いている場合に
別の場所に貼り付け	<Alt>+<E>	<⌘>+<E>	
後に貼り付け	<Alt>+<A>	<⌘>+<A>	
	<A>	<A>	貼り付け(Paste)] サブメニューが開いている場合に
ステップのエクスポート	<Ctrl>+<Alt>+<Q>	<⌘>+<⌘>+<Q>	
	x	x	【ステップ】コンテキストメニューが開いている場合に

機能	Windows	Mac	メモ
ステップのインポート	<Ctrl>+<Alt>+<I>	<⌘>+<⌘>+<I>	どのステップの後にインポートするかを選択する必要があります
	m	m	【ステップ】コンテキストメニューが開いている場合に
削除 (Delete)	<Delete>(⌫)	<Backspace>(⌫)	
	<D>	<D>	【ステップ】コンテキストメニューが開いている場合に
有効にする、または無効にする	<Ctrl>+</>	⌘ + /	
有効にする	<Shift>+</>	<Shift>+</>	
無効にする	<Alt>+</>	⌘ + /	
ステップの編集	<Ctrl>+<Alt>+<O>	<⌘>+<⌘>+<O>	ステップを拡張して、ステップ引数のプロパティを表示
	<E>	<E>	【ステップ】コンテキストメニューが開いている場合に
すべてのステップを折りたたむ	<Alt>+<0>	<⌘>+<0>	
すべてのステップを展開	<Alt>+<Shift>+<0>	<⌘>+<Shift>+<0>	
自動終了イベントをリセット	<Alt>+	<⌘>+	
オブジェクト識別方法を変更	<I>	<I>	【ステップ】コンテキストメニューが開いている場合に
【ステップ】コン	コンテキストメニュー	<⌘>+<Enter>	

機能	Windows	Mac	メモ
テキストメニューを開く	キー		
ステップオブジェクトの識別方法を「記述子」に設定	<Ctrl>+<Alt>+<3>	<⌘>+<⌘>+<3>	
すべてのステップを選択	<Ctrl>+<A>	<⌘>+<A>	
グループステップを展開	<右矢印>(▶)	<右矢印>(▶)	グループステップを選択する必要があります
グループステップを折りたたむ	<左矢印>(◀)	<左矢印>(◀)	
最後のステップに移動	<Page Down>	<Page Down>	
最初のステップに移動	<Page Up>	<Page Up>	
ステップ間を移動	<上矢印>または<下矢印>(▲ ▼)	<上矢印>または<下矢印>(▲ ▼)	
現在のステップより上のすべてのステップを選択	<Shift>+<Home>	<Shift>+<⌘>+<上矢印>(▲)	
現在のステップより下のすべてのステップを選択	<Shift>+<End>	<Shift>+<⌘>+<下矢印>(▼)	

オブジェクト選択機能

TruClientブラウザウィンドウのオブジェクト選択に関連する機能のショートカットキーについて、次の表で説明します。


機能	Windows	Mac	メモ
オブジェクト 選択を一時 停止	<Ctrl>+<Alt>+<F6>	<⌘ >+<⌘>+<F6>	オブジェクト選択 (Object Selection)] ダイアログが開いている必要があります。オブジェクト選択モードのままでアプリケーション要素にアクセスできます。
アプリケーションでオブジェクトを強調表示	<Ctrl>+<Alt>+<H>	<⌘ >+<⌘>+<H>	ステップを選択する必要があります

ステップボックスの使用

ステップボックス (以前のツールボックス) には、マクロに追加できるすべての手順が含まれています。

ステップの追加

マクロにステップを追加するには、次の手順を実行します。

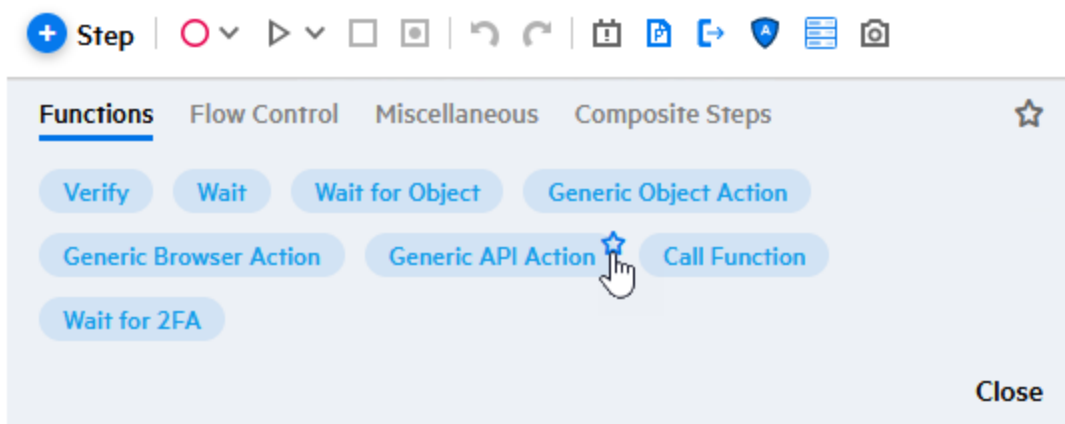
1. [TruClient] サイドバーで、[ステップの追加] アイコン( Step) をクリックします。
[ステップ] ボックスが開きます。
2. 追加するステップタイプのタブを選択します。タブの詳細については、次を参照してください。
 - "機能タブ" 次のページ
 - " [フロー制御] タブ" ページ226
 - " [その他] タブ" ページ227
 - " [複合ステップ] タブ" ページ228
3. タブでステップを選択し、マクロ内の目的の場所にドラッグします。

ステップをお気に入りとしてマークする

ステップをお気に入りとしてマークすると、お気に入りレビューですばやくアクセスできます。

ステップをお気に入りとしてマークするには、次を実行します。

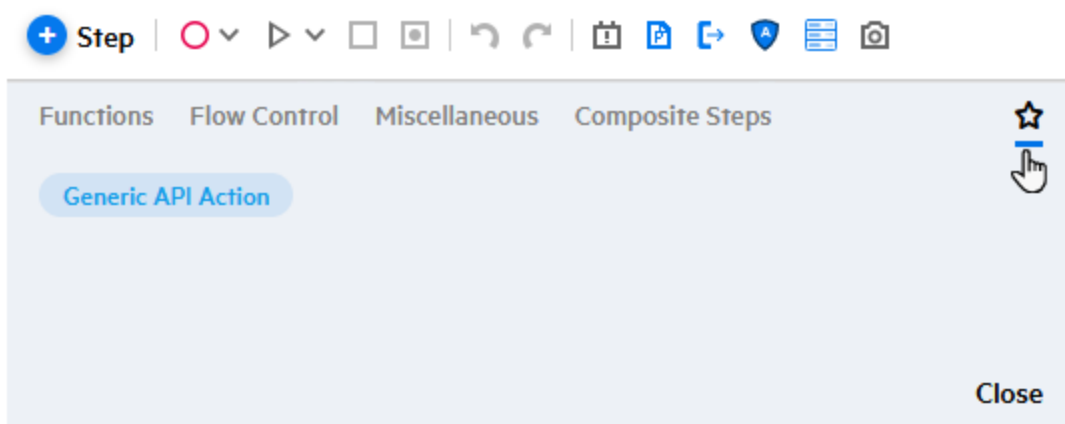
- お気に入りとしてマークしたいステップの星アイコンをクリックします。



お気に入りステップの表示

お気に入りステップを表示するには、次を実行します。

- ステップボックスの星アイコンをクリックします。



機能タブ

次の表に、関数のステップを示します。

ステップ	説明
検証	アプリケーションにオブジェクトが存在することを検証します。
待機	次のステップに進む前に、指定した秒数待機します。
オブジェクトの待	次のステップに進む前に、オブジェクトがロードされるのを待ちます。

ステップ	説明
機	
汎用オブジェクトアクション、汎用ブラウザアクション、または汎用APIアクション	<p>挿入して手動で設定できる空のステップ。API引数の詳細については、TruClientヘルプセンター(https://admhelp.microfocus.com/tc/en/2022-2022-r1/Content/TruClient/TC_Functions.htm)のAPIヘルプを参照してください。</p> <p>注記: Webマクロレコーダは、TruClient Help Centerで説明されているAPI引数のサブセットをサポートしています。</p>
呼び出し関数	サポートされていません。
2FAを待機	<p>2要素認証コントロールセンターから2要素認証応答が転送されるのを待ちます。2要素認証コントロールセンターは、アプリケーションサーバから受信したSMSおよび電子メール応答を処理します。詳細については、「"2要素認証の使用" ページ238」を参照してください。</p> <p>注記: このステップは、2要素認証グループステップに含まれています。</p>

フロー制御] タブ

次の表に、フロー制御のステップを示します。

ステップ	説明
Forループ	ループに含まれるステップを指定された回数繰り返すロジック構造。詳細については、「 "ループとループ修飾子の挿入" ページ297 」を参照してください。
Ifブロック	<p>条件が満たされた場合にブロックに含まれるステップを実行するロジック構造。</p> <ul style="list-style-type: none"> • Elseの追加 - [Elseの追加]リンクをクリックして、IfブロックにElseセクションを追加します。条件が満たされていない場合は、Elseセクションに含まれているステップが実行されます。 • Elseの削除 - IfブロックからElseセクションを削除します。 <p>注記: Elseセクションは、すべてのIfタイプ(If Block、If Exists、If Verify、およびIf Browser)に適用されます。Elseセクションにステップが含まれている場合に[elseの削除]をクリックすると、ステップが削除されます。それらをコピーしてマクロの本体に貼り付けて保存</p>

ステップ	説明
	<p>します。</p> <p>詳細については、「"Ifブロック、If-elseブロック、および終了ステップの挿入" ページ298」を参照してください。</p>
If Verify	「If Block」と「Verify」の組み合わせ。選択したオブジェクトのプロパティの条件が満たされた場合に、ブロックに含まれるステップを実行するロジック構造です。
If Exists	選択したオブジェクトがアプリケーションに存在する場合にブロックに含まれるステップを実行するロジック構造です。
Break	現在の繰り返しまたは残りの繰り返しを完了せずにループをすぐに終了します。
続行	現在のループの繰り返しをすぐに終了します。マクロは次の繰り返しに続きます。
Catchエラー	直前のステップでエラーを検出し、catchエラーステップのコンテンツを実行します。詳細については、「 "Catchエラーステップの挿入" ページ300 」を参照してください。
終了 (Exit)	指定した設定に応じて、繰り返しまたはマクロ全体を終了します。
2要素認証	<p>2要素認証コントロールセンターに要求を送信して、認証フローを開始します。このグループステップには、2要素認証コンポーネントの設定方法に関する基本的な手順が含まれています。詳細については、「"2要素認証の使用" ページ238」を参照してください。</p> <p>注記: これは、2FAを待機ステップを含むグループステップです。</p>

その他] タブ

次の表では、その他のステップについて説明します。

オプション	説明
JavaScriptを評価する	ステップに含まれるJavaScriptコードを実行します。
オブジェクト上でJSを評価する	指定したオブジェクトがアプリケーションにロードされた後に、ステップに含まれるJavaScriptコードを実行します。

オプション	説明
コメント	マクロにコメントを書き込むことができる空のステップ。

複合ステップ] タブ

セキュリティの質問に答える] ステップでは、セキュリティの質問をするインターフェイスオブジェクト(通常はラベル)と、ユーザが答えを入力するインターフェイスオブジェクト(通常はテキストボックス)を選択できます。選択後に、質問のテキストと回答を指定します。

レコードボタンの使用 (Macのみ)

MacバージョンのWebマクロレコーダでは、次の3種類のマクロを記録できます。

- ログイン - 従来のログインWebマクロ。「["ログインマクロ" ページ204](#)」を参照してください。
- ワークフロー - 従来のワークフローWebマクロ。「["ワークフローマクロ" ページ205](#)」を参照してください。
- ログインを使用したワークフロー - ログインアカウント情報を含むワークフローWebマクロ。このオプションを使用すると、TruClientサイドバーにロードされている既存のログインマクロを選択できます。その後、ログインステップを再生し、最初のワークフローステップに移動して記録を開始します。

ログインマクロの開始

ログインマクロの記録を開始するには:

1. メインアプリケーションウィンドウまたはWebマクロレコーダウィジェットで、**[ログイン]**をクリックします。
2. **開始(Start)]**をクリックします。
3. ["ログインマクロの記録" 次のページ](#)の手順に従います。

ワークフローマクロの開始

ワークフローマクロの記録を開始するには:

1. メインアプリケーションウィンドウまたはWebマクロレコーダウィジェットで、**[ワークフロー]**をクリックします。
2. **開始(Start)]**をクリックします。
3. ["ワークフローマクロの記録" ページ230](#)の手順に従います。

ログインマクロを使用したワークフローの開始

ログインマクロを使用したワークフローの記録を開始するには:

1. メインアプリケーションウィンドウまたはWebマクロレコーダウィジェットで、**ログインを使用したワークフロー(Workflow with Login)**をクリックします。
2. 認証に使用するログインマクロを選択またはドラッグアンドドロップします。
3. **開始(Start)**をクリックします。
ログインマクロがTruClientサイドバーにロードされ、自動的に再生されます。ログインに成功すると、ログインマクロが閉じます。これでログインし、ワークフローマクロを記録できます。
4. ["ワークフローマクロの記録" 次のページ](#)の手順に従います。




マクロの記録

マクロを記録する場合は、TruClientサイドバーを使用して記録機能を制御し、TruClientブラウザを使用してWebサイトにアクセスします。

ログインマクロの記録

この手順では、基本的なログインマクロを記録する方法について説明します。チャレンジ/レスポンス方式ログインマクロの詳細については、「["チャレンジ/レスポンス方式認証" ページ234](#)」および「["チャレンジ/レスポンス方式ログイン用のマクロの記録" ページ235](#)」を参照してください。

ログインマクロを記録するには、次のコマンドを実行します。

1. TruClientブラウザで、Webサイトの開始URLに移動します。
2. TruClientサイドバーで、**[記録]アイコン**()をクリックします。
3. TruClientブラウザで、ログインフォームに移動し、アプリケーションにログインします。
4. ログインした後、TruClientサイドバーの**[停止]アイコン**()をクリックしますが、ログアウトはしないでください。
5. TruClientサイドバーで**[再生]アイコン**()をクリックして、マクロが正しくログインされていることを確認します。
6. マクロは正しくログインされましたか?
 - 該当する場合は、TruClientサイドバーにログインが成功したことを示すオブジェクトを選択するように求めるメッセージが表示されます。次のステップに進みます。

注記: **[インタラクティブオプション]**タブで**[最後のステップを検証ステップに強制する]**設定が無効になっている場合、オブジェクトの選択を求めるプロンプトは表示されません。ステップ8に進みます。詳細については、「["設定の構成" ページ311](#)」を参照してください。


- 該当しない場合は、[ファイル] > [新規]をクリックします。プロンプトが表示された場合は、マクロを保存しないでください。ステップ1に戻ります。

7. TruClientブラウザで、ログインに成功した後にのみ表示されるオブジェクトを指定します。

重要! [インタラクティブオプション]タブで[最後のステップを検証ステップに強制する]設定が有効になっている場合、最後のステップは「オブジェクトの待機」ステップである必要があります。

選択したオブジェクトの待機アクションが、記録されたステップに追加されます。






Webマクロレコーダは、ログアウト状態を自動的に検出しようと試みます。ログアウト条件を後で追加または編集する方法については、「["ログアウト条件の使用" ページ259](#)」を参照してください。

8. [保存]アイコン()をクリックしてマクロを保存します。

ログインマクロにオプションを追加するには、「["マクロの強化" ページ296](#)」を参照してください。

ワークフローマクロの記録

ワークフローマクロを記録するには、次のコマンドを実行します。

1. TruClientブラウザで、ワークフローの開始URLに移動します。
2. TruClientサイドバーで、[記録]アイコン()をクリックします。
3. TruClientブラウザで、マクロに記録するページに移動します。
4. ナビゲーションを記録した後、TruClientサイドバーの[停止]アイコン()をクリックします。
5. 次のいずれかを実行します。
 - ナビゲーションが正しく記録されていることを検証するには、TruClientサイドバーの[再生]アイコン()をクリックします。
 - [ステップ]ボックスから記録されたナビゲーションにステップを追加するには、[ステップの追加]アイコン( Step)をクリックします。詳細については、「["ステップボックスの使用" ページ224](#)」を参照してください。
6. 終了したら、[保存]アイコン()をクリックしてマクロを保存します。

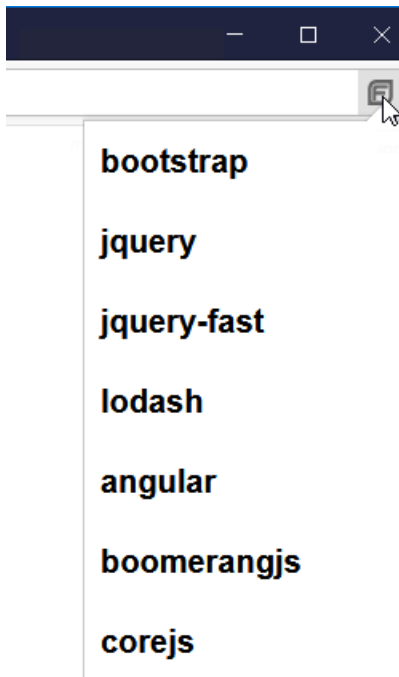
クライアント側フレームワークの自動検出

アプリケーションにアクセスする際、Webマクロレコーダは、ターゲットアプリケーションで使用されているクライアント側フレームワークの検出を試みます。Webマクロレコーダがこのようなフレームワークを検出すると、TruClientブラウザウィンドウのURLアドレスボックスの右側にFortifyロゴが付いたアイコンが表示されます。

検出されたフレームワークの表示

検出されたクライアント側フレームワークを表示するには、次の操作を行います。

1. URLアドレスの右側にあるFortifyロゴをクリックします。
検出されたフレームワークのリストが表示されます。



ヒント: シングルページアプリケーション(SPA)を示すフレームワークがリストに表示されている場合は、スキャン設定でSPAサポートオプションを有効にできます。詳細については、「*OpenText™ Dynamic Application Security Testing ユーザガイド*」または「*OpenText™ ScanCentral DAST の設定および使用ガイド*」を参照してください。



2. (オプション)リスト内のフレームワークにカーソルを合わせると、そのバージョンが表示されます。

注記: Webマクロレコーダは、すべてのバージョンのフレームワークを判別できません。このような場合は、「バージョン不明」と表示されます。

マクロの編集

マクロを編集する際は、TruClientサイドバーを使用して記録されたステップを追加または編集し、TruClientブラウザを使用してWebサイトにアクセスします。詳細については、「["ユーザーインターフェイスについて" ページ210](#)」を参照してください。

マクロを編集するには、次の手順を実行します。


1. TruClientサイドバーで、[ファイル]アイコン()のドロップダウン矢印をクリックし、[開く]を選択します。
2. マクロのステップを追加または編集します。詳細については、「["マクロの強化" ページ296](#)」および「["マクロのデバッグ" ページ301](#)」を参照してください。
3. [保存]アイコン()をクリックしてマクロを保存します。

マクロの検索

マクロを検索するか、マクロ内の特定のステップ番号に移動できます。

ステップの検索

マクロを検索するには、次のコマンドを実行します。

1. TruClientサイドバーで、検索アイコン()をクリックします。
検索パネルが開きます。
2. オプションで、ドロップダウンリストで検索する項目を指定します。検索スコープのオプションは次のとおりです。

- **現在のビュー** - 表示されているステップのみを検索
- **スクリプト全体** - 拡張されていないステップを含むすべてのステップを検索

エンティティタイプのオプションは次のとおりです。

- **すべて** - ステップおよびトランザクションを検索
- **ステップ** - ステップのみを検索


注記: トランザクションはWebマクロレコーダでは使用されないため、トランザクションエンティティタイプは適用されません。

3. 検索ボックスに検索文字列を入力します。
[現在のビュー]検索では、検索文字列は入力中に表示されているステップやトランザクションで強調表示されます。
[スクリプト全体]検索では、検索文字列が見つかったステップやトランザクションのリストが入力中に表示されます。
4. <Enter>キーを押して検索結果に移動します。

ヒント: 結果カウントの横にある[次の結果に進む]および[前の結果に戻る]アイコンを使用して、検索結果を移動することもできます。

特定のステップ番号への移動

マクロ内の特定のステップ番号に移動するには、次の手順に進みます。

1. [TruClient]サイドバーで、検索アイコンのドロップダウン矢印()をクリックし、[移動]を選択します。
[移動]ダイアログボックスが表示されます。
2. [ステップ番号]ボックスに数値を入力します。
3. [移動]をクリックします。
マクロ内でステップが強調表示されます。

CLIの使用 (Windowsのみ)

イベントベースのWebマクロレコーダを使用して、いくつかの一般的なタスクをコマンドラインインタフェース(CLI)により実行できます。

CLIの起動

CLIを起動するには、次のコマンドを実行します。

- Windowsのコマンドプロンプト(cmd.exe)アプリケーションを右クリックし、[管理者として実行]を選択します。
管理者: コマンドプロンプトウィンドウが表示されます。

重要! {b}コマンドプロンプトで、このcdコマンドを使用して、現在の作業ディレクトリをWebマクロレコーダアプリケーションがインストールされているディレクトリに変更します。

Webマクロレコーダは、OpenText DASTと同じディレクトリにインストールされています。デフォルトでは、インストールディレクトリは次の場所にあります。

```
C:\Program Files\Fortify\Fortify WebInspect
```

CLIオプション

次の表は、CLIのWebマクロレコーダツールで使えるオプションについて説明しています。

目的...	コマンドプロンプトに次のコマンドを入力します...
ログインマクロを記録する	macrorecorder.exe
編集用の既存のログインマクロをロードする	macrorecorder.exe --fileToLoad 'PathToFile'

目的...	コマンドプロンプトに次のコマンドを入力します...
ワークフローマクロを記録する	<code>macrorecorder.exe --workflow</code>
編集用の既存のワークフローマクロをロードする	<code>macrorecorder.exe --fileToLoad 'PathToFile' - -workflow</code>
ワークフローマクロを記録できるよう、既存のログインマクロをロードして自動的に再生する	<code>macrorecorder.exe --pre-workflow-login 'PathToLoginFile' --workflow</code>
既存のログインマクロをロードして自動的に再生し、その後に編集用の既存のワークフローマクロをロードして自動的に再生する	<code>macrorecorder.exe --fileToLoad 'PathToFile' - -pre-workflow-login 'PathToLoginFile' -- workflow</code>
CLIのヘルプを表示する	<code>macrorecorder.exe --help</code>

チャレンジレスポンス方式認証

チャレンジレスポンス方式認証は、サーバが質問(チャレンジ)を提示し、クライアントが有効な回答(レスポンス)を提供する必要があるプロトコルのファミリーです。最も単純な例では、チャレンジでパスワードが要求され、有効な回答が正しいパスワードになります。

複数のチャレンジ

Webサイトの中には、ユーザに対して複数のチャレンジを提示するものがあります。通常、ユーザが初めてWebサイトに登録するときに、そのユーザが回答を提供する質問のリストが表示されます。質問は、その後の認証に使用されます。例:

- お気に入りの色は?
- 最初のペットの名前は?
- あなたはどの町や都市で生まれましたか?
- 初めて購入した自動車のメーカーは?

ユーザが後でログインしようとする、Webサイトにこれらのチャレンジが2つ以上表示されます。

チャレンジのグループ

一部のサイトでは、次の例に示されている方法で、チャレンジのグループを作成し、新しいログイン試行ごとにグループからの質問を提示します。

この例のWebサイトに登録すると、ユーザーに9つの質問に対する回答を求めるメッセージが表示されます。9つの質問は、それぞれ次のように3つの質問のグループに分けられます。

グループ1

Q: あなたの使命は? A: 幸せ

Q: 名前は? A: スミス

Q: お気に入りの色は? A: 青

グループ2

Q: お気に入りのペットの名前は? A: ラスティー

Q: お母さんの旧姓は? A: ジョーンズ

Q: どの州で生まれましたか? A: デラウェア

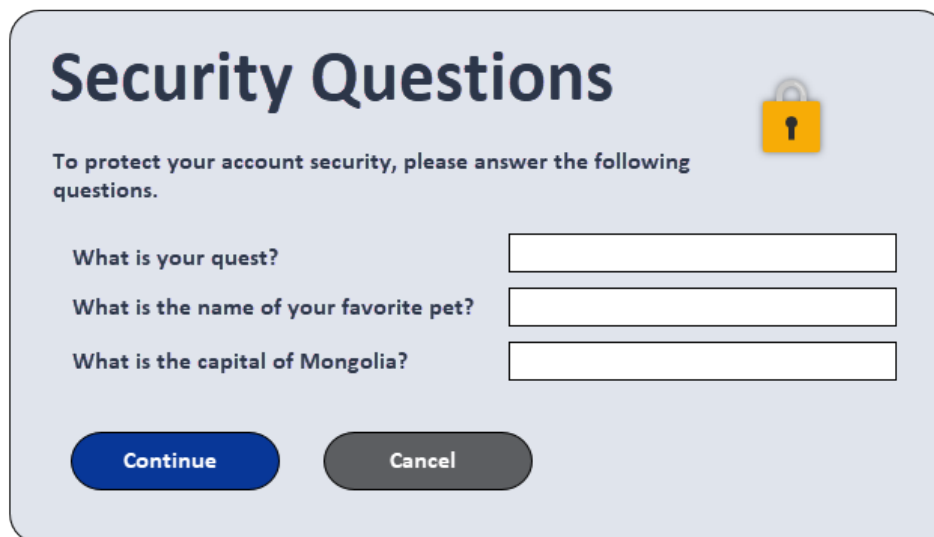
グループ3

Q: モンゴルの首都は? A: ウランバートル

Q: 海鳥の一種の名前は? A: アルバトロス

Q: あなたの父方の祖母の名前は? A: エスター

ログインページは次のようになります(各グループの最初の質問を使用)。



The image shows a login form titled "Security Questions" with a lock icon. The text reads: "To protect your account security, please answer the following questions." There are three questions, each with a text input field:

- What is your quest?
- What is the name of your favorite pet?
- What is the capital of Mongolia?

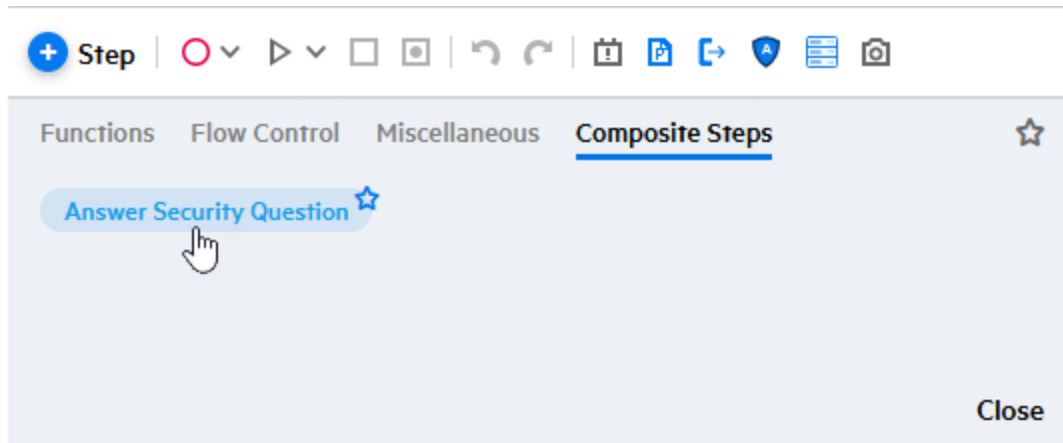
At the bottom, there are two buttons: "Continue" (blue) and "Cancel" (grey).

チャレンジ/レスポンス方式ログイン用のマクロの記録

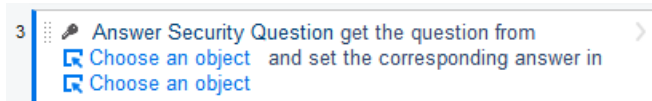
チャレンジ/レスポンス方式タイプのログイン用にマクロを記録する場合、1つのログイン時にそれらの組み合わせのサブセットのみが提示される場合でも、考えられるすべての質問と回答の組み合わせを知っている必要があります。マクロを記録する時は、特別なステップとしてこれらの組み合わせを手動で入力します。

通常、ユーザ名とパスワードの資格情報を使用してログインした後で、ターゲットサイトがセキュリティクエスチョンを聞く時点で、次の手順に従って、一連の質問に必要なステップを手動で作成します。

1. マクロの記録中に、TruClientサイドバーの[停止]アイコン(□)をクリックします。
2. TruClientサイドバーで、[ステップの追加]アイコン(+ Step)をクリックします。
3. [複合ステップ]をクリックし、[セキュリティの質問に答える]ステップをクリックして記録されたステップにドラッグします。

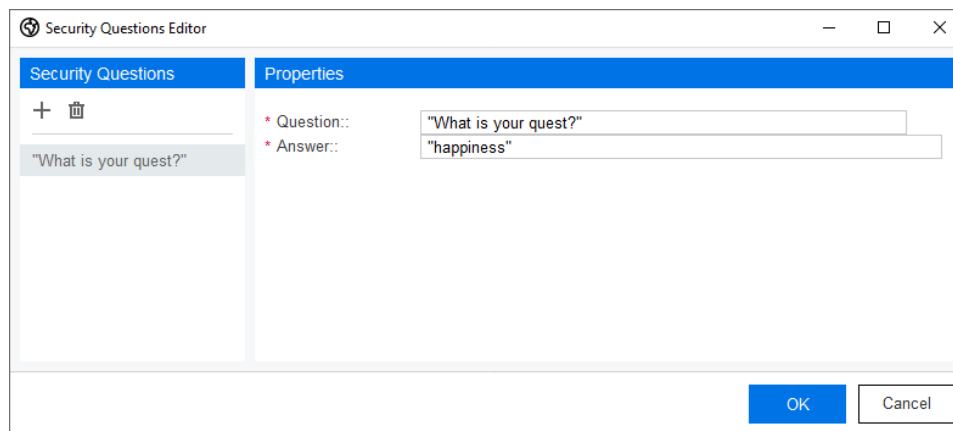


新しいステップが作成されます。



4. 新しいステップの最初の[クリックしてオブジェクトを選択する]リンクをクリックして、次にTruClientブラウザウィンドウで、質問を表すオブジェクト(通常はラベル)をクリックします。
5. 新しいステップの2つ目の[クリックしてオブジェクトを選択する]リンクをクリックして、次にTruClientブラウザウィンドウで、答えを表すオブジェクト(通常はテキストボックス)をクリックします。
6. TruClientサイドバーで、[セキュリティの質問に答える]ステップの[ステップエディタ]アイコン(➤)をクリックします。
ステップエディタが開きます。
7. [セキュリティの質問]セクションをクリック(展開)します。
8. +をクリックして、セキュリティの質問エディタを開きます。
9. セキュリティの質問エディタで、[新しい質問の追加]アイコン(+)をクリックします。
新しい質問がデフォルト名「質問1」で表示されます。プロパティには、[質問]というラベルのテキストボックス(デフォルト値の「質問1」も表示)と、[回答]というラベルが付いたテキストボックスとデフォルト値の「回答1」が含まれます。
10. [質問]テキストボックスに、デフォルトのテキストの上に、大文字と句読点を含め、ログインページに表示されるとおりの実際の質問を入力します。左側のペインの質問が同時に更新されます。

重要! {b}テキストは必ず引用符で囲んでください。



11. [回答]ボックスに、正しい回答を引用符で囲んで入力します。
12. ステップ9~11を繰り返して、Webページ上の同じ場所に表示されることのある2番目の質問の情報を追加します。この例では、「お気に入りのペットの名前は?」という質問を使用します。
13. ステップ9~11を繰り返して、Webページ上の同じ場所に表示されることのある3番目の質問の情報を追加します。この例では、「モンゴルの首都は?」という質問を使用します。
14. [OK]をクリックします。

質問と回答は、マクロステップの[セキュリティの質問]セクションの表に追加されます。

Security Questions		+ ✎ 🗑	
Question	Answer		
"What is your quest?"	"happiness"		
"What is the name of your favorite pet?"	"Rusty"		
"What is the capital of Mongolia?"	"Ulaanbaatar"		

ヒント: 後で質問または回答を編集する必要がある場合は、セキュリティの質問エディタを再度開きます。

これで、Webページ上のこの特定の場所のマクロステップが完了します。質問と回答を作成して秘密の質問をさらに追加するには、「["秘密の質問に対する質問と回答の追加" 下](#)」を継続します。

秘密の質問に対する質問と回答の追加

質問と回答を追加して秘密の質問を追加するには、次の手順を実行します。

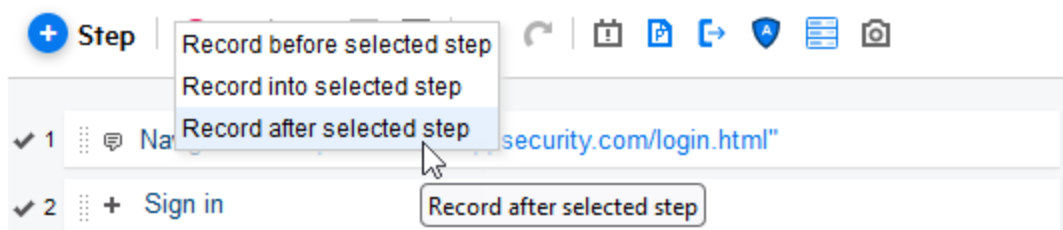
1. 次のいずれかの操作を行って、2番目の質問が表示されるまでWebページを更新します。
 - TruClientブラウザウィンドウ内をクリックし、<F5>キーを押します。
 - TruClientブラウザウィンドウ内で右クリックし、[再読み込み]アイコンを選択します。
2. 「["チャレンジレスポンス方式ログイン用のマクロの記録" ページ235](#)」のステップ2~14を繰り返して、Webページの2番目の場所にある3つの質問と回答の2番目のセットに別のマクロステップを追加します。

3. 次のいずれかの操作を行って、3番目の質問が表示されるまでWebページを更新します。
 - TruClientブラウザウィンドウ内をクリックし、<F5>キーを押します。
 - TruClientブラウザウィンドウ内で右クリックし、[再読み込み]アイコンを選択します。
4. 「["チャレンジ/レスポンス方式ログイン用のマクロの記録" ページ235](#)」のステップ2~14を繰り返して、Webページの3番目の場所にある3つの質問と回答の3番目のセットに別のマクロステップを追加します。

追加ステップの記録

考えられるすべての質問と回答の組み合わせに対するステップを作成した後に追加のステップを記録する必要がある場合は、次の手順を実行します。

1. TruClientサイドバーで、最後に作成したステップを選択します。
2. [記録]アイコン(○▼)のドロップダウン矢印をクリックし、[選択したステップの後に記録]を選択します。



3. 通常どおり記録を続行します。
4. [停止]アイコン(□)をクリックします。
5. マクロを再生して保存します。

2要素認証の使用

ログインマクロを記録したら、**2要素認証**グループステップをマクロに追加して、OpenText DASTまたはOpenText ScanCentral DASTのスキャンで2要素認証を使用できます。

注記: 2要素認証は、Fortify WebInspect Enterpriseではサポートされていません。

重要! 2要素認証をスキャンで使用する前にローカルでテストする場合は、まず2要素認証コントロールセンターとFortify2FAモバイルアプリケーションを設定する必要があります。詳細については、「["設定の構成" ページ311](#)」を参照してください。

推奨

個人情報保護の観点から、OpenTextでは個人の電話や電子メールアドレスの使用はお勧めしません。テスト用電話またはテスト用電子メールアドレスのみを使用することをOpenText

では強く推奨します。

既知の制限事項

次の既知の制限事項は、2要素認証機能に適用されます。

- IMAPおよびPOP3サーバがサポートされています。ただし、固有のID一覧 (UIDL) をサポートするPOP3サーバのみがサポートされます。
- 現在、サポートされているのはAndroid携帯電話のみです。
- 携帯電話では、OpenText DASTがインストールされているのと同じサブネット上にWi-Fi接続が必要です。

Gmailアカウントに関する考慮事項

Gmailアカウントに関連する次の点にご注意ください。

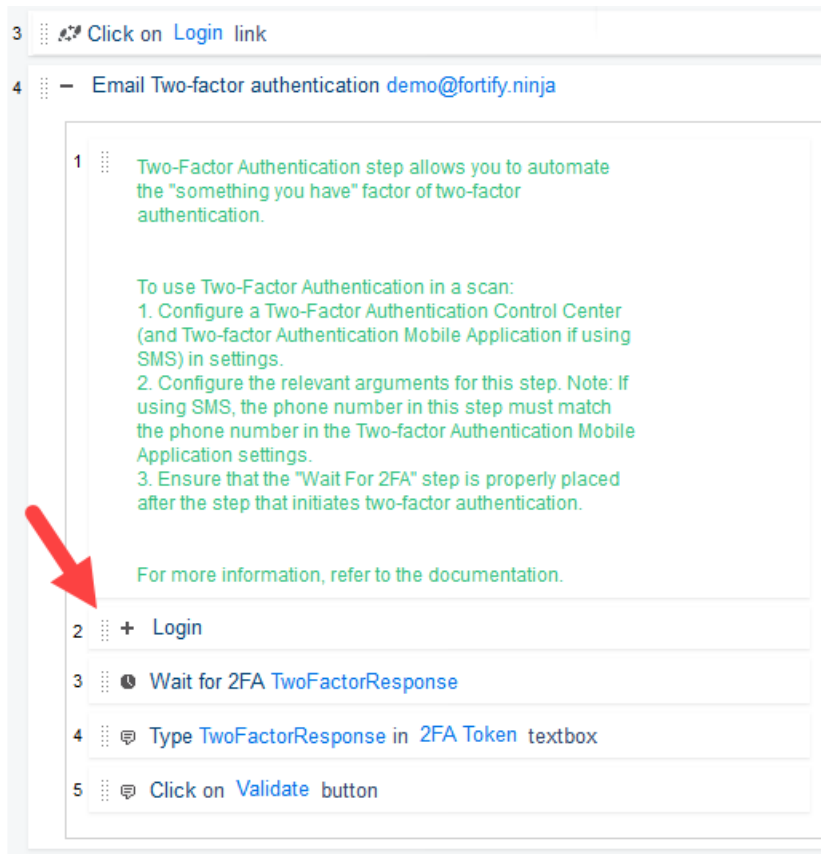
- Gmailアカウントの設定には、通常モードと最新モードが含まれます。Gmailアカウントを使用して新しい受信メールで問題が発生した場合、最新モードを使用することでこの問題が解決する可能性があります。最新モードを有効にするには、POP3アカウント設定でアカウント名を次の形式で設定します。
`recent:<email_address@gmail.com>`
- セキュリティの観点から、Googleは「Googleでログイン」を使用してGmailをユーザのGoogleアカウントに関連付けます。ユーザが作成したパスワードは受け付けません。Gmailアカウントを使用する場合、Googleアプリのパスワードを作成して使用する必要があります。詳細については、アプリパスワードの作成と使用に関するGoogleアカウントのマニュアルを参照してください。

ガイドライン

2要素認証を設定する場合は、次のガイドラインに従います。

- **2要素認証グループステップ**を別の**2要素認証グループステップ**内に設定することはできません。
- **2要素認証グループステップ**内に**2つの2FAを待機ステップ**を含むことはできません。
- ログインプロセスを完了するには、**2FAを待機ステップ**の後に、**入力ステップ**と**クリックステップ**を構成する必要があります。

- 2要素認証用にログインマクロを設定する場合、次の図に示すように、ログインステップを2要素認証グループステップ内に入れる必要があります。




2要素認証グループステップの追加

2要素認証グループステップは、2要素認証コントロールセンターに要求を送信して、認証フローを開始します。

重要! 2要素認証グループステップには、設定する必要がある2FAを待機ステップが含まれています。そのようにしない場合、2要素認証グループステップが失敗します。

2要素認証グループステップを追加するには、次の手順を実行します。

1. [TruClient]サイドバーで、[ステップの追加]アイコン( Step)をクリックします。
[ステップ]ボックスが開きます。
2. [フロー制御]をクリックします。
3. 2要素認証グループステップをクリックして、記録されたステップにドラッグし、ユーザ名とパスワードを入力した後にドロップします。
デフォルトでは、SMSの2要素認証ステップが追加されます。
4. 次の表に従って続行します。

設定項目	操作手順
SMS応答	<p>引数を展開し、次の設定を行います。</p> <ul style="list-style-type: none">• [電話番号]ボックスに、SMS応答を受信する電話番号を入力します。 <p>ヒント: JavaScriptを入力できますが、JavaScriptの実行結果は電話番号である必要があります。パラメータ名を使用することもできます。詳細については、「"2要素認証用のパラメータの作成" ページ278」を参照してください。</p> <ul style="list-style-type: none">• [正規表現]ボックスで、SMS応答からトークンのみを抽出する正規表現を構築します。 <p>ヒント: サンプルの正規表現については、ドロップダウン矢印をクリックしてください。</p>
電子メール応答	<p>a. ステップを展開します。</p> <p>b. [アクション]リストで、[MAP電子メール2要素認証 (IMAP Email Two-factor authentication)] または [POP3電子メール2要素認証 (POP3 Email Two-factor authentication)] を選択します。</p> <p>c. [引数]を展開し、次の設定を行います。</p> <ul style="list-style-type: none">◦ [電子メール]ボックスで電子メール応答を受信する電子メールアドレスを入力します。 <p>ヒント: JavaScriptを入力できますが、JavaScriptの実行結果は電子メールアドレスである必要があります。パラメータ名を使用することもできます。詳細については、「"2要素認証用のパラメータの作成" ページ278」を参照してください。</p> <ul style="list-style-type: none">◦ [サーバ]ボックスに、電子メールサーバのIPアドレスまたはURLを入力します。◦ [サーバポート]ボックスに、電子メールメッセージに使用するポートを入力します。◦ [TLS]ボックスで、電子メールサーバがTLSプロトコルを使用するかどうかを選択します。 <p>注記: デフォルト設定はtrueです。</p>

設定項目	操作手順
	<ul style="list-style-type: none">◦ [パスワード]ボックスに、電子メールアカウントのパスワードを入力します。◦ [正規表現]ボックスで、電子メール応答からトークンのみを抽出する正規表現を構築します。 <div>ヒント: サンプルの正規表現については、ドロップダウン矢印をクリックしてください。</div>

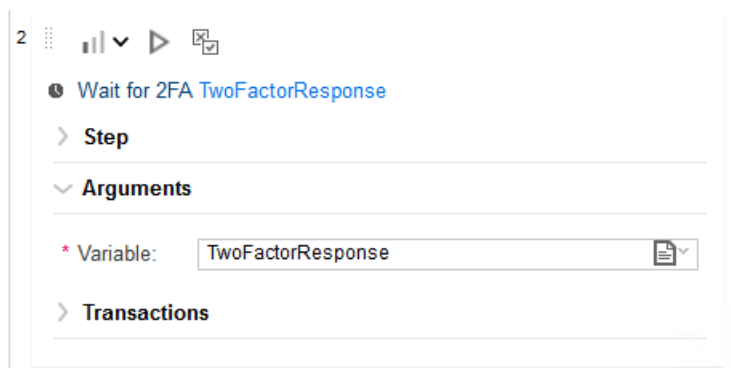
2FAを待機するステップの設定

2要素認証グループステップには、設定する必要がある**2FAを待機**ステップが含まれています。2FAを待機ステップは、2要素認証コントロールセンターから2要素認証応答が転送されるのを待ちます。

重要! 2FAを待機ステップは、2要素認証グループステップ内でのみ実行できます。スタンドアロンステップとして実行することはできません。

2FAを待機ステップを設定するには、次の手順を実行します。

1. デフォルトでは、**ステップタイムアウト**でマクロの再生時間が180秒延長されます。アプリケーションサーバからの応答が遅い場合など、再生時間をさらに延長するには、**ステップタイムアウト**設定の値を大きくします。
2. 引数を展開し、[変数]ボックスに変数名を入力します。
次のイメージでは、例としてTwoFactorResponseを使用しています。



Webマクロレコーダは、コントロールセンターからの応答をこの変数に保存します。

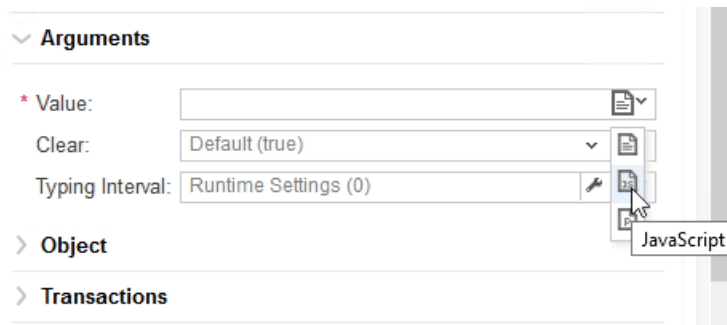
入力ステップとクリックステップの追加

2要素認証グループステップ内に、2つの汎用**オブジェクトアクション**ステップを追加する必要があります。1つは、コントロールセンターからの応答を2要素認証応答テキストボックスに入力

する入力ステップとして設定する必要があります。サイトにアクセスするためには、もう1つを[サインイン]や[次へ]などのボタンをクリックするクリックステップとして設定する必要があります。

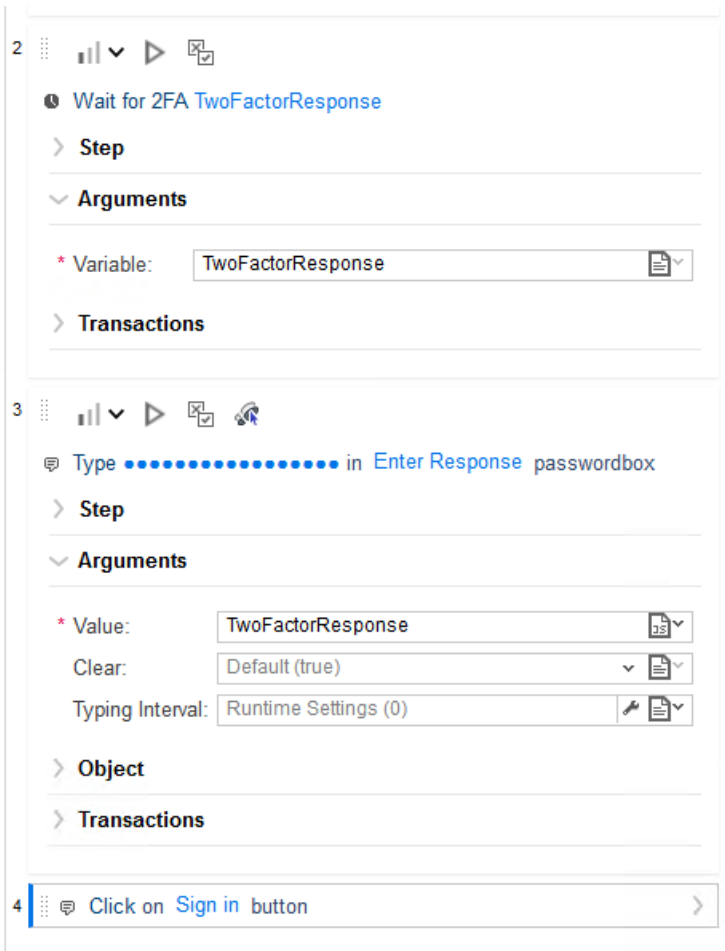
入力ステップとクリックステップを追加および設定するには、次の手順を実行します。

1. [TruClient]サイドバーで、[ステップの追加]アイコン(+ Step)をクリックします。
[ステップ]ボックスが開きます。
2. [機能]タブで、[汎用オブジェクトアクション]ステップをクリックして記録されたステップにドラッグし、2FAを待機ステップの直後に2要素認証グループステップ内にドロップします。
3. 次のようにステップを設定します。
 - a. [オブジェクトの選択]をクリックし、指示に従って2要素認証応答テキストボックスを選択します。
 - b. ステップを展開し、[アクション]リストから[入力]を選択します。
 - c. 引数を展開します。
 - d. [値]ボックスで[JS]を選択します。



- e. [値]ボックスに、2FAを待機ステップで作成した変数名を入力します。前のプロシージャでは、例としてTwoFactorResponseを使用しています。
4. [TruClient]サイドバーで、[ステップの追加]アイコン(+ Step)をクリックします。
[ステップ]ボックスが開きます。
 5. [機能]タブで、[汎用オブジェクトアクション]ステップをクリックして記録されたステップにドラッグし、入力ステップの直後に2要素認証グループステップ内にドロップします。
 6. 次のようにステップを設定します。
 - a. [オブジェクトの選択]をクリックし、指示に従って[サインイン]や[次へ]などのボタンを選択して、サイトにアクセスします。
 - b. ステップを展開し、[アクション]リストから[クリック]を選択します。

完了した入力ステップとクリックステップは、次のイメージと同様である必要があります。2FAを待機ステップの直後の配置に注意してください。



TOTP認証の使用

2要素認証のもう1つの方法は、時間ベースのワンタイムパスワード(TOTP)認証です。この方法では、SMSまたは電子メールでトークンを受信するのではなく、共有シークレットとシステム時刻を使用して、ユーザが入力するトークンを生成します。TOTP秘密鍵を持っている場合はそれを入力することもできますが、このプロセスはイベントベースのWebマクロレコーダで自動化できます。そのために、TOTP認証者を設定および管理し、次いで 時間ベースのワンタイムパスワードを入力する(Type Time-based One-time Password)] という新しいステップでその認証者を使用します。

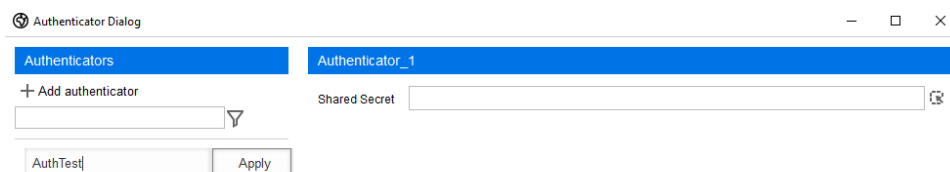
TOTP認証者の設定

認証者を登録する最初の段階では、通常、QRコードをスキャンします。イベントベースのWebマクロレコーダは、QRコードから情報を読み込み、TOTP認証者をシード処理するための秘密鍵を抽出できます。別の方法として、秘密鍵にアクセスできる場合はそれを自分で直


接 認証者 (Authenticator)] ダイアログに入力して、TOTP認証者をシード処理することもできます。

TOTP認証者を設定するには:

1. TruClientブラウザで、使用するWebアプリケーションに移動してログインします。
2. アプリケーションで2要素認証を有効にします。
これにより、ユーザインタフェースでQRコードまたは秘密鍵が生成されます。
3. [TruClient] サイドバーで、**認証者の編集 (Edit authenticators)]** アイコン(🔑)をクリックします。
認証者 (Authenticator)] ダイアログが開きます。
4. **認証者の追加 (+ Add authenticator)]** をクリックします。
新しい認証者がデフォルト名のAuthenticator_1で追加されます。新しい認証者がマクロに追加されるたびに、デフォルト名の末尾の番号が1つずつ増えます。
5. 必要に応じて、認証者の名前を次のようにして変更します。
 - a. 新しい認証者について、**認証者名の編集 (Edit authenticator name)]** アイコン(✎) をクリックします。
 - b. 認証者の名前を入力し、**適用 (Apply)]** をクリックします。
この例では、認証者名は「AuthTest」です。



6. 次の表に従って続行します。

状況	処理
共有シークレットが提供されているか、共有シークレットを知っている	共有シークレット (Shared Secret)] ボックスにシークレットを入力します。
QRコードが提供されている	<p>a. 共有シークレット (Shared Secret)] ボックスの右側にある オブジェクトの選択 (select object)] アイコン()をクリックします。</p> <p> [TruClient] サイドバーウィンドウに オブジェクトの選択 (Select Object)] ダイアログボックスが開きます。</p> <p>b. 次のいずれかを実行します。</p> <ul style="list-style-type: none">◦ TruClientブラウザでQRコードをクリックします。◦ ページのエリアをクリックし、カーソルをドラッグして、QRコードを含むページの領域を選択します。 <p>c. 選択 (Select)] をクリックします。</p> <p>共有シークレットが抽出され、マスキングされた状態で 共有シークレット (Shared Secret)] ボックスに入力されます。</p>




7. **[OK]** をクリックします。

ヒント: 同じマクロで使用するために、認証者名と共有シークレットの複数のペアを作成および管理できます。ただし、認証者名はそれぞれ固有である必要があります。

TOTPを使用したマクロの記録

TOTPをマクロで使用するには、ログインプロセスを通常どおり記録する必要がありますが、一時停止して **汎用オブジェクトアクション (Generic Object Action)]** ステップを追加し、これに **時間ベースのワンタイムパスワードを入力する (Type Time-based One-time Password)]** アクションを含める必要があります。

TOTPを使用したマクロを記録するには:

1. TruClientサイドバーで、**[記録 (Record)]** アイコン()をクリックします。
2. TruClientブラウザで、ログインフォームに移動し、アプリケーションにログインします。
3. 認証コードを入力する地点まで進んだら、[TruClient] サイドバーの **停止 (Stop)]** アイコン()をクリックします。
4. [TruClient] サイドバーで、**[ステップの追加]** アイコン( Step) をクリックします。
[ステップ] ボックスが開きます。

5. **機能(Functions)]** タブで **汎用オブジェクトアクション(Generic Object Action)]** ステップをクリックして、記録されたステップ群までこれをドラッグし、最後に記録したステップの後ろにドロップします。次のようにステップを設定します。
 - a. そのステップで、**オブジェクトの選択(Choose an object)]** をクリックします。
 - b. TruClientブラウザで、TOTPテキストボックス(またはフィールド)を選択します。
 - c. **汎用オブジェクトアクション(Generic Object Action)]** ステップで、**ステップ(Step)]** を展開し、**アクション(Action)]** リストから **時間ベースのワンタイムパスワードを入力する(Type Time-based One-time Password)]** を選択します。

6

Type Time-based One-time Password [Authenticator Name]

▼ Step

Action: Type Time-based One-time Password

Object Timeout: Runtime Settings (20)

Step Timeout: Runtime Settings (180)

Minimum Time: 0

End Event: Automatic: Not Yet Set

> Arguments

> Object

- d. **引数(Arguments)]** を展開し、使用する認証者名を **認証者(Authenticator)]** ボックスに入力します。

6

Type Time-based One-time Password AuthTest

> Step

▼ Arguments

* Authenticator: AuthTest

Clear: Default (true)

Typing Interval: Runtime Settings (0)

> Object

この例では、認証者名は「AuthTest」です。

ヒント: 使用可能な認証者を表示するには、**認証者の編集(Edit authenticators)]** アイコン(🔗)をクリックして **認証者(Authenticator)]** ダイアログを開きます。

6. **汎用オブジェクトアクション(Generic Object Action)]** ステップを選択した状態で **選択したステップの後に記録(Record after selected step)]** をクリックして、ログインプロセスの記録を続行します。

7. 『ruClient』サイドバーで、ログイン検証用のオブジェクトを選択するように求めるプロンプトが表示されない場合は、ログインステップの後に検証ステップを追加し、正常にログインした後にのみ表示されるオブジェクトを指定します。
8. **再生(Play)** アイコン(▶)をクリックして、マクロが正しくログインされていることを確認します。

TOTPのトラブルシューティング

TOTP認証を使用する際に問題が発生した場合は、考えられる原因と解決方法の判断にこのトピックが役立つ可能性があります。

QRコードエラーのトラブルシューティング

次の表に、QRコードエラーに関して考えられる原因と解決方法を示します。

エラー	考えられる原因	考えられる解決方法
「共有シークレットをQRコードから抽出できなかった」	QRコードに適切なTOTP登録URLが含まれていない可能性があります。	TOTP登録URLが正確で、正しい構文を使用していることを確認します。 たとえば、TOTP登録URLの先頭は次のようになっていることが普通です。 <code>otpauth://totp/IDENTIFICATION?secret=YOUR_SECRET</code>
「QRコードの解析に失敗しました」	Webページに表示されたQRコード要素をWebマクロレコーダで解析できませんでした。	QRコードを画像要素に変換すると、Webマクロレコーダで解析できる場合があります。

マクロ再生エラーのトラブルシューティング

次の表に、マクロ再生の失敗に関して考えられる原因と解決方法を示します。

エラーまたは症状	考えられる原因	考えられる解決方法
「名前が<name>の認証者が見つかりませんでした」	認証者(Authenticator)]ダイアログで認証者が正しく設定されていない可能性があります。	認証者(Authenticator)]ダイアログで認証者を再設定します。詳細については、「 TOTP認証者の設定 ページ244」を参照してください。

エラーまたは症状	考えられる原因	考えられる解決方法
「 <i>named <name></i> という名前の認証者のTOTPを生成できませんでした」	共有シークレットが正しくない可能性があります。	共有シークレットの再入力を手動で(可能な場合)、またはQRコードを使用して行います。詳細については、「 "TOTP認証者の設定" ページ244 」を参照してください。
	システム時刻が正しく設定されていません。	Webマクロレコーダが実行されているホストのシステム設定でシステム時刻を同期します。時刻とタイムゾーンが正しく設定されていることを確認します。
トークンが間違っており、ログインに失敗します。	システム時刻が正しく設定されていません。	Webマクロレコーダが実行されているホストのシステム設定でシステム時刻を同期します。時刻とタイムゾーンが正しく設定されていることを確認します。
	トークンのタイムフレームは30秒です。	時間ベースのワンタイムパスワードを入力する(Type Time-based One-time Password)] ステップを、再試行を含むForループステップでラップします。詳細については、「 "Forループ" ページ295 」および「 "ループとループ修飾子の挿入" ページ297 」を参照してください。

OAuth2でのIMAP多要素認証の使用

IMAPプロトコルでOAuth 2.0認証を使用する場合、イベントベースのWebマクロレコーダでは、トークンのプロンプトを含むログインマクロを記録し、それを変更してOAuth認証を追加できます。OAuth認証でサポートされている電子メールクライアントは、現在のところ、Microsoft® Outlook®のみです。

作業を開始する前に

マクロを記録して変更する前に、次のガイドラインに従います。

- OAuth認証をサポートする電子メールクライアント(オープンソースのMozilla Thunderbird電子メールアプリケーションなど)を設定する必要があります。設定には、メールサービスプロバイダでアプリケーションを設定するときに生成されるアプリケーションクライアントIDが必要です。
- 次の正しい許可を電子メールアプリケーションに提供します。
IMAP.AccessAsUser.All POP.AccessAsUser.All offline_access
- URIをhttp://localhostにリダイレクトする電子メールクライアントを設定します。詳細については、OAuthを使用したIMAP、POP、またはSMTP接続の認証に関するMicrosoftのマニュアルを参照してください。
- ログインマクロを記録する際には、電子メールからトークンをコピーし、トークンのテキストボックスに貼り付けて認証する必要があります。便宜上、登録されている電子メールアカウントにログインして、ターゲットWebアプリケーションからトークンを受け取ってください。

OAuth 2.0を使用したマクロの記録

OAuth 2.0を使用してマクロを記録するには、以下を実行します。

1. TruClientサイドバーで、**記録(Record)]**アイコン(○▼)をクリックします。
2. TruClientブラウザで、ログインフォームに移動し、アプリケーションにログインします。
3. トークンの入力を求めるプロンプトが表示されたら、登録されている電子メールアカウントに送信された電子メールからトークンを手動でコピーし、フォームに貼り付けて、**送信(submit)]**(または **Enter(入力)]**または **login(ログイン)]**をクリックします。アクションがマクロに記録されます。ステップは後で編集します。
4. TruClientサイドバーの **停止]**アイコン(□)をクリックします。

注記: ログインマクロの再生時には、ハードコードされたトークンの有効期限が切れているか無効になっているため、再生は失敗します。

5. ["OAuthの関数ライブラリの作成"](#) 下の手順に進みます。


OAuthの関数ライブラリの作成

関数ライブラリを作成するには:

1. **関数ライブラリ]** タブで、**新規ライブラリ(New Library)]**をクリックします*。
新規ライブラリ(New library)] ダイアログボックスが開きます。
2. **ライブラリ名 (Library Name)]** ボックスに、mfa_oauthなどのわかりやすい名前を入力します。
3. **OK]** をクリックします。
4. ["OAuth関数ライブラリへの関数の追加"](#) 次のページの手順に進みます。

OAuth関数ライブラリへの関数の追加

ライブラリに関数を追加するには、以下の手順を実行します。

1. **新規関数(New Function)]**ドロップダウン矢印  をクリックし、 **[OAuth 2.0]** を選択します。
新規OAuth 2.0関数(New OAuth 2.0 function)] ダイアログボックスが開きます。
2. **関数名(Function Name)]** ボックスに、outlook_loginなどのわかりやすい名前を入力します。
3. OAuth 2.0関数を初めて作成する場合は、クライアントアプリケーションを設定する必要があります。クライアントアプリケーションは、メールプロバイダに対してアプリケーションを識別する公開識別子です。これは、電子メールを開いて読む特定の権限が付与されたメールプロバイダにより事前登録され、認識される必要があります。クライアントアプリケーションを設定するには、次の操作を行います。
 - a. **クライアント設定を開く(Open Client Configuration)]** をクリックします。
2要素認証のOAuth 2.0設定(OAuth 2.0 for Two-Factor Authentication Configuration)] ダイアログが開きます。
 - b. **+ アプリケーションクライアントの追加(Add application client)]** をクリックします。
クライアントがデフォルト名のAppClient_<number>で追加されます。
 - c. 名前ボックスのAppClient_<number>をわかりやすい名前(Thunderbirdなど)に置き換えて、 **適用(Apply)]** をクリックします。
 - d. **サービスプロバイダ]** ドロップダウンリストで、 **[Office 365 (IMAP)]** を選択します。
 - e. **アプリケーションクライアントID(Application Client ID)]** に、クライアントIDのGUIDを貼り付けます。
 - f. **[OK]** をクリックします。
2要素認証のOAuth 2.0設定(OAuth 2.0 for Two-Factor Authentication Configuration)] ダイアログが閉じます。
4. **新規OAuth 2.0関数(New OAuth 2.0 function)]** ダイアログボックスの **クライアントアプリケーション]** ドロップダウンリストで、Thunderbirdなどのアプリケーションを選択します。
5. **電子メール]** ボックスで、トークンを受信する電子メールアドレスを入力します。これは、テスト中のサイトに登録されているアカウントです。

重要! 2要素認証の作成ステップ(Create Two-Factor Autnentication step)] チェックボックスが選択されていることを確認します。これにより、スキャン時に実行されているすべてのブラウザを同期する2要素認証ステップを、スクリプトで簡単に設定できるようになります。

6. **[OK]** をクリックします。
ログイン(login)] ページが開き、指定した電子メールアカウントのパスワードの入力を求められます。
7. パスワードを入力し、 **サインイン(sign in)]** をクリックします。

ナビゲーションがOAuth 2.0関数に記録されています。[アクション]タブに、以下のステップがマクロに追加されていることが表示されます。

- 電子メール(IMAP XOAuth2)の2要素認証
- IMAP XOAuth2を<client_application>に接続
- 2FAを待機する(これはトークンを待機するステップです。)

8. ["電子メール\(IMAP XOAuth2\)の2要素認証ステップの設定"](#) 下の手順に進みます。

電子メール(IMAP XOAuth2)の2要素認証ステップの設定

2要素認証ステップを設定するには、次の操作を行います。

1. ステップエディタで、**[引数]**を開きます。
2. **電子メール**]ボックスで、トークンを受信する電子メールアドレスを入力します。
3. **サーバ**]ボックスに、「outlook.office365.com」と入力します。
4. **サーバポート (Server Port)**]ボックスに、「993」を入力します。
5. **正規表現(Regular Expression)**]ドロップダウンリストで、電子メール内の数値ベーストークンを検索するデフォルトの正規表現を選択します。

ヒント: 数値以外のトークンを使用する場合は、カスタムの正規表現を作成し、**正規表現(Regular Expression)**]ボックスに貼り付けます。

6. ["2FAを待機するステップの設定"](#) 下の手順に進みます。

2FAを待機するステップの設定

2FAを待機するステップは、トークンを待機するステップです。

「2FAを待機」ステップを設定するには、次の手順を実行します。

1. ステップエディタで、**[引数]**を開きます。
2. **変数(Variable)**]ボックスに、電子メールから取得したトークンのプレースホルダになる変数名を入力します。たとえば、OTP1になります。
3. ["ステップの再構成"](#) [次のページ](#)の手順に進みます。

ステップの再構成

記録された元のログインステップとトークンテキストボックスステップを、OAuth 2.0関数のナビゲーションステップに適した順序に再構成する必要があります。


ステップを再構成するには、次の操作を行います。

1. スクリプトからログインステップを選択し、右クリックして **切り取り(Cut)**]を選択します。
2. **電子メール(IMAP XOAUTH2)の2要素認証** ステップで、IMAP XOAUTH2を<*client_application*>に**接続**ステップを選択し、右クリックして **貼り付け(Paste)]> 後ろに貼り付け(Paste After)]**を選択します。
3. トークンテキストボックスステップ(トークンテキストボックスをクリックやトークンテキストボックスに「Value」を入力など)を選択し、右クリックして **切り取り(Cut)]**を選択します。
4. **2FAを待機する**ステップを選択し、右クリックして **貼り付け(Paste)]> 後ろに貼り付け(Paste After)]**を選択します。
5. **"トークンテキストボックスステップのタイプ 値] の設定" 下**の手順に進みます。

トークンテキストボックスステップのタイプ 値] の設定

トークンテキストボックスステップのタイプ 値] からハードコードされた値を削除し、2FAを待機するステップの変数から値を受け入れるステップを設定する必要があります。

トークンテキストボックスステップで、タイプ 値]を設定するには、次の手順を実行します。

1. ステップエディタで、**変数]**を開きます。
2. **値(Value)]**ボックスで、次の操作を実行します。
 - a. ハードコードされた値を削除します。
 - b. ドロップダウンリストから **JS]**  (JavaScript)を選択します。
 - c. **2FAを待機する**ステップから変数名を入力します。たとえば、OTPになります。
3. マクロを保存します。
4. マクロを再生して、ログインが成功することを確認します。

マクロ再生レベルの変更

マクロを記録すると、TruClientは各ステップに1から3のレベルを割り当てます。例えば、マクロにはレベル1のステップが不可欠です。影響のないアプリケーションの領域で発生するクリックステップは、レベル2に割り当てられます。マウスオーバーステップは通常、マクロには不要と見なされ、レベル3に割り当てられます。

マクロステップは、TruClientブラウザの上部にあるツールバーのステップレベルスライダでレベル1、2、または3に指定された粒度で表示および再生されます。最も高い粒度はレベル3です。スライダをレベル3に設定すると、レベル1、2、および3ですべてのステップが表示および再生されます。再生に成功するにはより高い粒度を使用する必要がある場合がありますが、それに

よりマクロの実行に時間がかかる可能性があります。デフォルトでは、スクリプトレベルは 1 に設定されています。

マクロの再生レベルを変更するには、次の操作を行います。

- TruClient ブラウザで、ステップレベルのドロップダウン矢印 (▼) をクリックし、次のいずれかを選択します。
 - 1 - レベル 1 のステップのみを表示および再生します。アプリケーションと対話するには、レベル 1 のステップが必要です。
 - 2 - レベル 1 およびレベル 2 のステップを表示および再生します。レベル 2 のステップは、おそらくマクロにとって重要ではない方法でアプリケーションに影響します。
 - 3 - レベル 1、2、および 3 のステップを表示および再生します。レベル 3 のステップは、アプリケーションに対して明らかな影響はありません。

下位レベルを選択した場合、一部のステップは非表示になります。上位レベルを選択すると、追加のステップが表示されます。

イベントハンドラの使用

実行の度に発生するわけではないステップや、ランダムに発生するステップを記録または追加する場合、または要素がページ上のランダムな場所に表示される場合、その挙動が発生しないとマクロが失敗する可能性があります。

たとえば、ログオン時に次の通知が表示される場合があります。

「サーバーはビジー状態です。10 秒待ってから再試行してください。」("Server is busy. Please wait for 10 seconds and try again.")

または、Web サイトが訪問者に登録を行ってクーポンを受け取るように促すメッセージを表示することがあります。このような挙動を処理するステップがない場合、発生した場合にマクロが失敗する可能性があります。イベントハンドラは、条件が発生した場合にのみ条件を処理する関数を呼び出します。

イベントハンドラの作成

イベントを作成するには、次の手順を実行します。

1. TruClient サイドバーウィンドウで、[イベントハンドラエディタ] アイコン (🔧) をクリックします。
イベントハンドラエディタが開きます。
2. **新しいイベントハンドラの追加 (Add a new event handler)** アイコン (+) をクリックして、新しいイベントハンドラを追加します。
ハンドラを定義するのに十分な情報が追加されるまで、ハンドラ名の横にエラーアイコンが表示されます。
3. **全般 (General)** プロパティを次のように設定します。
 - a. **名前 (Name)** にイベントハンドラの名前を入力し、**適用 (Apply)** をクリックします。

- b. 現在の繰り返し中にイベントハンドラを1回だけ実行する(繰り返しが終了すると0にリセットされる)には、**一度だけ実行(Execute only once)**]を選択します。
- c. このイベントの実行中に他のイベントハンドラを実行するには、**他のイベントによる中断を許可する(Allow other handlers to interrupt)**]を選択します。
- d. Webマクロレコーダがマクロ再生を通じてイベントをリッスンし、イベントが発生するたびにイベントハンドラを呼び出すことを許可するには、**スクリプト全体を通じてイベントのトリガを許可する(Event can be triggered during the script)**]を選択します。
- e. Webマクロレコーダに対してマクロ再生の一部分のみのイベントのリッスンを許可する場合は、**スクリプト全体を通じてイベントのトリガを許可する(Event can be triggered during the entire script)**]のチェックを外します。

ヒント: このボックスのチェックを外すと、**開始(Start)**]および**終了(End)**]ドロップダウンリストが表示されます。これらのリストから開始ステップと終了ステップを選択して、イベントをトリガできるステップの範囲を指定します。

- f. **タイプ(Type)**]ドロップダウンリストから、次のいずれかを選択します。
 - **オブジェクト(Object)**] - オブジェクト関連のイベントが発生する場合。たとえば、ページ上に特定のオブジェクトが表示される場合や、特定のオブジェクトプロパティが特定の値を取得した場合などです。
 - **ダイアログ(Dialog)**] - ダイアログボックスがポップアップ表示される場合。たとえば、アラートやプロンプトが表示される場合です。
- 4. **オブジェクト(Object)**]のタイプで**オブジェクトの選択(Choose an object)**]をクリックし、TruClientブラウザウィンドウでオブジェクトを選択します。必要に応じて次のオプションを変更します。これらのオプションは自動的に入力されていることがあります。
 - **役割(Roles)**]ボックスで、オブジェクトに対して実行できる操作を指定します。詳細については、「**"オブジェクトに関連するステップ引数" ページ280**」を参照してください。
 - **Name(名前)**]ボックスに、オブジェクトの名前を入力します。
 - **[Dメソッド(ID Method)]**ドロップダウンリストから、次のいずれかを選択します。
 - 自動
 - XPath
 - JavaScript
 - 記述子TruClientディスクリプタの詳細については、
<https://admhelp.microfocus.com/tc/en/2022-2022-r1/Content/TruClient/descriptors.htm>を参照してください。
 - **関連オブジェクト(Related Objects)**]ボックスで、オブジェクトをアプリケーション内の別のオブジェクトに関連付け、再生中のオブジェクトの識別を容易にします。詳細については、「**"他のオブジェクトへのオブジェクトの関連付け" ページ310**」を参照してください。
- 5. オブジェクトイベントには、**タイプ(Type)**]ドロップダウンリストで次のいずれかを選択します。

- **オブジェクトが存在 (Object Exists)]** - 再生中にオブジェクトが存在する場合、イベントハンドラがトリガされます。
- **オブジェクトにプロパティが存在 (Property exists on Object)]** - オブジェクトのプロパティが定義された条件を満たすと、イベントハンドラがトリガされます。

注記: ダイアログイベントの場合、タイプは **ダイアログが開いた(Dialog Opened)]** です。指定したダイアログボックスが開いたときに、イベントハンドラがトリガされます。

6. 必要に応じて、ハンドラ関数を次のように設定します。

重要! ハンドラ関数はライブラリ内にある必要があります。

- a. **ライブラリ(Library)]** ドロップダウンリストから、関数を含むライブラリを選択します。
 - b. **関数(Function)]** ドロップダウンリストから関数を選択します。
 - c. 選択した関数に関数パラメータがある場合は、**引数(Arguments)]** フィールドに引数値を入力します。
7. **OK]** をクリックして変更内容を保存し、エディタを閉じます。

関数ライブラリの使用

関数ライブラリを使用すると、繰り返されるステップの実行を組み合わせることで1回の呼び出しにすることができます。また、一連のイベントを組み合わせることで論理的なフローまたはライブラリにすることで、関数を使用してさまざまなタスクを処理することもできます。

たとえば検索を含むSPAでは、検索フローを組み合わせることで、ステップは一定のまま入力だけが変化する検索ライブラリにすることができます。ステップを複製する必要はありません。

TruClient関数と関数ライブラリの詳細については、
https://admhelp.microfocus.com/tc/en/2022-2022-r1/Content/TruClient/_tc_c_step_functions.htmを参照してください。

既知の制限事項

現在はローカルライブラリだけがサポートされているため、ライブラリは自身が作成されたマクロでのみ使用できます。グローバルライブラリはサポートされていないので、マクロ間でライブラリを共有することはできません。

関数ライブラリの作成

関数ライブラリを作成するには:

1. TruClientサイドバーウィンドウの下部にある **関数ライブラリ(Function Libraries)]** タブを選択します。
2. **関数]** ツールバーの **新規ライブラリ(New Library)]** アイコン(*)をクリックします。

新規ライブラリ(New library)] ダイアログボックスが開きます。

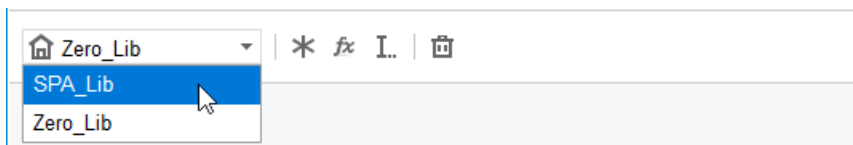
3. **ライブラリ名 (Library Name)]** ボックスでライブラリの名前を入力して、**OK]** をクリックします。


新しいライブラリが **関数 (Function)]** ツールバーにあるライブラリリストに追加されます。「[関数の作成"下](#)」の説明に従って、関数をライブラリに追加します。

関数の作成


関数を作成するには:

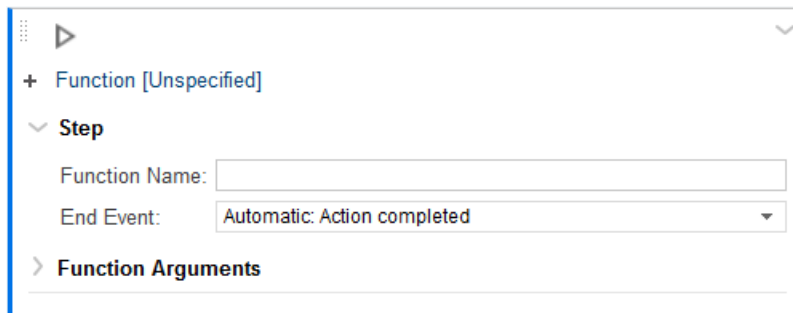
1. **関数 (Function)]** ツールバーで、ライブラリリストからライブラリを選択します。




2. **新規関数 (New Function)]** アイコン()をクリックして、新しい関数を作成します。
新しい、未指定の関数がライブラリに追加されます。



3. **ステップエディタを開く/閉じる (Open/Close the Step Editor)]** () アイコンをクリックして関数を展開し、ステップと関数の引数を表示します。



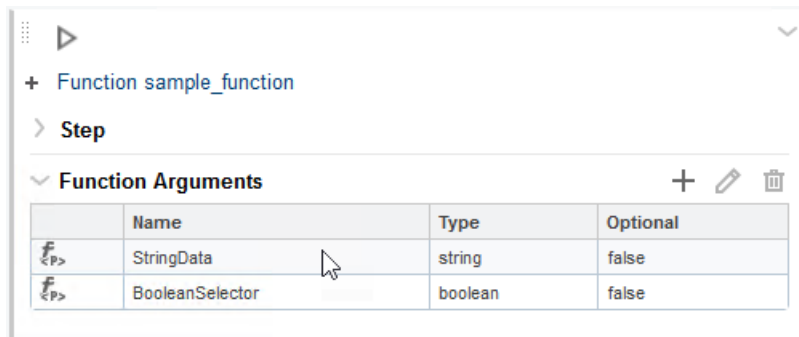
4. **関数名 (Function Name)]** ボックスで、関数の名前を入力します。
5. **終了イベント (End Event)]** リストから、終了イベントを選択します。詳細については、「[終了イベントについて"次のページ](#)」を参照してください。
6. **関数の引数 (Function Arguments)]** を展開します。
7. **新しい引数の作成 (Create a new argument)]** アイコン() をクリックします。
引数エディタが開きます。
8. 引数を次のように定義します。
 - a. **名前 (Name)]** ボックスに引数のわかりやすい名前を入力し、関数を使用するときどのような値を指定すべきかがわかるようにします。
 - b. **タイプ (Type)]** リストから、引数のタイプを選択します。選択肢は、**文字列 (string)]**、**整数 (integer)]**、**ブール値 (boolean)]** です。


- c. **任意(Optional)]**リストから、引数が任意であるかどうかを指定します。選択肢は **[はい(true)]** または **[いいえ(false)]** です。
- d. **[OK]** をクリックします。
引数がステップに追加されます。

引数の編集

関数の引数を編集するには:


1. **関数の引数(Function Arguments)]** テーブルで、編集する引数を選択します。



2. **引数の編集(Edit argument)]** アイコン() をクリックします。
引数エディタが開きます。
3. **"関数の作成" 前のページ**」のステップ8の説明に従って、引数を更新します。

引数の削除

引数を削除するには:

1. **関数の引数(Function Arguments)]** テーブルで、削除する引数を選択します。
2. **選択した引数を削除する>Delete the selected argument)]** アイコン() をクリックします。

終了イベントについて

Webマクロレコーダは、サポートされている各ブラウザでの最初のスクリプト再生時に終了イベントが発生するタイミングを定義します。Webマクロレコーダが自動的に識別する終了イベントを使用するか、ステップに別の終了イベントを割り当てることができます。

次の表では、Webマクロレコーダで使用可能な終了イベントについて説明します。

終了イベント	説明
Action completed	ステップはアクションが完了すると終了します。アクションの一例とし

終了イベント	説明
(アクションが完了)	て、ボタンクリックがあります。
Automatic: Action completed (自動: アクションが完了)	ステップは、アクションが完了したとTruClientが識別したときに終了します。
Dialog opened (ダイアログが開いた)	ステップはダイアログボックスが開いた時に終了します。
Document Loaded (ドキュメントがロードされた)	ステップは、ドキュメントのロード処理が完了したときに終了します。すべてのスクリプトとスタイルシートのロードが完了して実行され、すべてのイメージがダウンロードされて表示されています。
DOM Content Loaded (DOMコンテンツがロードされた)	ステップは、ページのDOM (Document Object Model)の準備ができたときに終了します。ページのコンテンツ、スタイル、および構造を操作するためのAPIは、アプリケーションのクライアント側コードから要求を受け取る準備が整っています。
Step network completed (ステップのネットワークが完了)	ステップは、XMLHttpRequestによって開始された要求を含む、すべてのHTTP要求が完了したときに終了します。
Step synchronous network completed (ステップの同期ネットワークが完了)	ステップはすべてのHTTP要求が完了したときに終了します(ステップに関係のないオープンな接続に関連付けられている要求は除く)。通常、これらの要求はXMLHttpRequestを使用してトリガされます。

ログアウト条件の使用

Webマクロレコーダは、ターゲットWebサイトのログアウト条件を自動的に検出できる場合があります。ただし、必要な数の異なるログアウト条件を指定できます。これらの条件が満たされた場合、センサーはログインマクロを呼び出して再ログインし、中断した所からスキャンを再開します。ログアウト条件エディタを使用して、ログアウト条件を追加、編集、および削除できます。

重要! すべてのログアウト条件の最終セットは、ターゲットサイトのスキャン中にログアウトされるケースすべてについてカバーする必要があります。


ログアウト条件の種類

ログアウト条件は複雑なものになり得ます。ログアウトをトリガできるページ内の要素を指定する必要があります。ログアウト条件エディタでは、次のタイプのログアウト条件を作成および管理できます。

- セッションベース - URLと正規表現を使用して、未認証のユーザを示すリダイレクトを特定します。トラフィックを確認して、ログアウトをトリガする要求への応答に適合する正規表現を記述するか、URLを入力する必要があります。
- イベントベース - 実行中にJavaScriptを使用してログアウトを検出し、Fortify WebInspect センサーに通知します。テンプレートのリストからサンプルのJavaScriptコードを選択し、アプリケーションに適したログアウト条件になるようにコードを編集できます。テンプレートの詳細については、「["イベントベースのログアウトテンプレートについて" ページ264](#)」を参照してください。


以前のバージョンのWebマクロレコーダからのログアウト条件

自動ログアウト検出を使用し、Macro Engine 5.<version>でWebマクロレコーダに記録されたマクロを使用してスキャンを実行した場合、好ましくない結果を引き起こす可能性があります。OpenTextでは、次の方法で、以前に検出されたログアウト条件を削除することをお勧めします。

1. イベントベースのWebマクロレコーダで既存のマクロを開きます。
2. **[ログアウト条件の編集]**アイコン()をクリックします。
ログアウト条件エディタが開き、すでに検出または作成済みのすべてのログアウト条件が表示されます。
3. 既存の自動ログアウト条件を削除します。
4. マクロを再生します。
新しいログアウト条件が自動的に検出されます。

ログアウト条件エディタへのアクセス

ログアウト条件エディタを開くには、次の手順を実行します。

- ログインが成功したら、**[ログアウト条件の編集]**アイコン()をクリックします。
ログアウト条件エディタが開き、すでに検出または作成済みのすべてのログアウト条件が表示されます。

セッションベースのログアウト条件の追加

セッションベースのログアウト条件を追加するには:

1. 左ペインで、**新しいセッションログアウト条件の追加(Add new session logout condition)]** アイコン(+)をクリックします。
セッションベースのログアウト条件が追加されます。
2. **名前(Name)]** ボックスに、新しい条件の名前を入力します。
左側の列の名前は、変更と同時に更新されます。
3. 使用するログアウト条件のタイプを選択し、そのタイプに必要な情報を入力します。次の表に、オプションの説明を示します。

オプション	説明
Regex	<p>このオプションを使用して、正規表現(regex)を構築します。正規表現とは、文字列のセットを表すパターンです。正規表現は、さまざまな演算子を使用して小さな式を組み合わせることによって、数式のように構築されます。正規表現に関する知識を持つユーザだけが、この機能を使用するようにしてください。</p> <p>Regexは、a)保護されたページにアクセスするためのログインユーザの要求への応答と、b)同じ保護されたページにアクセスするために、ログインしていないユーザからの同じ要求に対する応答の違いを反映する必要があります。Regexを構築する一般的な手順は次のとおりです。</p> <ol style="list-style-type: none">a. Webプロキシツールを起動して、Webトラフィックを記録します。 詳細については、Webプロキシのヘルプまたは『<i>OpenText™ Dynamic Application Security Testing</i>ツールガイド』を参照してください。b. ターゲットサイトにログインし、保護されたページのURLをコピーします。c. ログアウトして、コピーしたURLを使用して、ログインせずに保護されたページにアクセスします。d. 応答を比較し、ログインせずに保護されたページにアクセスした時の応答の固有な点を特定します。e. 正規表現エディタを開きます。詳細については、正規表現エディタのヘルプまたは『<i>OpenText™ Dynamic Application Security Testing</i>ツールガイド』を参照してください。f. ログインせずに保護されたページにアクセスした時の応答の固有な点を反映したRegexを構築します。

オプション	説明
	g. ログアウト 条件 エディタの[Regex]フィールドにregexをコピーします。
URL	このオプションを選択すると、現在表示されているWebページがデフォルト値として自動的に使用されます。ターゲット サイトがユーザをログアウトするときにはリダイレクトする静的URLを指定できます。ターゲットサイトの一般ログインページは指定しません。

4. [閉じる]をクリックしてログアウト 条件を保存し、ログアウト 条件 エディタを閉じます。

イベントベースのログアウト 条件 の追加

イベントベースのログアウト 条件を追加するには:

1. 左 ペインで、[ログアウト 条件 の追加 (Add logout condition)] ドロップダウンアイコン(▼)をクリックし、[イベントベース(Event-based)]を選択します。

イベントベースのログアウト 条件が追加され、JavaScriptコード エディタが表示されます。

The screenshot shows the 'Logout Condition Editor' window. The title bar says 'Logout Condition Editor'. The window is divided into two main sections. The left section, titled 'Logout Condition Editor', contains a list of conditions with 'EventBased_1' selected. The right section, titled 'Event-based Logout Condition', contains fields for 'Name' (set to 'EventBased_1') and 'Timeout' (set to '15'). Below these fields is a large text area for JavaScript code, with a placeholder comment: '// Start typing your JavaScript logout condition here'. At the bottom of the window, there are two buttons: 'Templates' and 'Close'. A red warning message is displayed at the bottom of the code editor area.

Logout Condition Editor

Event-based Logout Condition

Name: EventBased_1

Timeout: 15

// Start typing your JavaScript logout condition here

Important! An event-based logout condition uses JavaScript and runs in the browser only during execution.

Calling WebInspect JavaScript API 'WI.notifyLoggedOut' is required to end script execution. Refer to the Web Macro Recorder documentation for more information.

The code editor supports autocomplete functionality. To view autocomplete suggestions, press 'Ctrl + Space'.

Templates Close

2. [Name(名前)]ボックスで、新しい条件の名前を入力します。
左側の列の名前は、変更と同時に更新されます。
3. [タイムアウト (Timeout)]ボックスに、ログアウト条件がタイムアウトする時間を秒単位で入力します。有効な値は10 - 60秒です。デフォルト値は15秒です。

4. 次の表に従って続行します。

目的...	その場合 ...
定義済みテンプレートを使用する	<p>a. テンプレート (Templates)] をクリックします。 テンプレートリスト (Templates List)] ダイアログボックスが開きます。テンプレートの詳細については、「"イベントベースのログアウトテンプレートについて" 次のページ」を参照してください。</p> <p>b. 左側のペインで、テンプレートを選択します。</p> <p>c. ロード (Load)] をクリックします。 現在のイベントベースのログアウト条件が、選択したテンプレートのコードで上書きされることを警告するプロンプトが表示されます。</p> <p>d. 確定 (Confirm)] をクリックします。</p> <p>e. コードがコードエディタに追加されます。</p> <p>f. アプリケーションのイベントベースのログアウト条件での必要に応じてJavaScriptを編集します。</p>
独自のJavaScriptを作成する	<p>コードエディタでJavaScriptコードを入力します。</p> <p>ヒント: コーディング中にオートコンプリートの候補を表示するには、次のいずれかの操作を行います。</p> <ul style="list-style-type: none">• Windowsの場合は、<CTRL>+<Space>を押します。• macOSの場合は、<Ctrl>+<Cmd>+を押します。

重要! 定義済みのテンプレートを使用する場合も独自のコードを記述する場合も、OpenText DASTセンサにログアウト状態を通知してタイムアウトを回避するために、JavaScriptは次のコードで終わる必要があります。

```
WI.notifyLoggedOut(isLoggedOut);
```

5. **[閉じる]** をクリックしてログアウト条件を保存し、ログアウト条件エディタを閉じます。


ログアウト条件の編集

ログアウト条件エディタで既存のログアウト条件を編集するには、次の手順を実行します。

1. 左ペインで編集するログアウト条件を選択します。
[プロパティ]ペインにプロパティが一覧表示されます。
2. 必要に応じてプロパティを編集します。
3. [閉じる]をクリックしてログアウト条件を保存し、ログアウト条件エディタを閉じます。

ログアウト条件の削除

ログアウト条件エディタで既存のログアウト条件を削除するには、次の手順を実行します。

1. 左ペインで削除するログアウト条件を選択します。
2. **削除**アイコン()をクリックします。
[削除の確認]プロンプトが表示されます。
3. **Yes**をクリックします。
4. [閉じる]をクリックしてログアウト条件を保存し、ログアウト条件エディタを閉じます。

イベントベースのログアウトテンプレートについて

このトピックでは、アプリケーションの仕様に合わせて編集できるイベントベースのログアウトテンプレートについて説明します。

Missing Local Storage Key

このテンプレートは、ローカルストレージキーが見つからないときに発生するログアウト条件を処理します。このイベントベースのログアウト条件では、Webストレージの検出を有効にする必要があります。詳細については、「["対話型オプション" ページ316](#)」を参照してください。

次の表では、Missing Local Storage Keyテンプレートで使用されているJavaScriptコードについて説明します。

JavaScriptコード	説明
<pre>var token = window.localStorage.getItem("<key>");</pre>	ブラウザに保存されている指定されたキーの値を返し、それをtokenという名前の変数に格納します。
<pre>var isLoggedIn = document.location.origin == "http</pre>	document.location

JavaScriptコード	説明
<pre>(s)://<path>:<port>" && !token;</pre>	.originプロパティが指定したURLに一致するものの、トークンが見つからない場合にログアウト条件を確認します。
<pre>WI.notifyLoggedOut(isLoggedOut);</pre>	センサがログアウトしたことをOpenText DASTに通知します。

Missing Session Storage Key

このテンプレートは、セッションストレージキーが見つからないときに発生するログアウト条件を処理します。このイベントベースのログアウト条件では、Webストレージの検出を有効にする必要があります。詳細については、「["対話型オプション" ページ316](#)」を参照してください。

次の表では、Missing Session Storage Keyテンプレートで使用されているJavaScriptコードについて説明します。

JavaScriptコード	説明
<pre>var token = window.sessionStorage.getItem("<key>");</pre>	セッションに対して保存されている指定したキーの値を返し、それをtokenという名前の変数に格納します。
<pre>var isLoggedOut = document.location.origin == "http (s)://<path>:<port>" && !token;</pre>	document.location.originプロパティが指定したURLに一致するものの、トークンが見つからない場合にログアウト条件を確認します。
<pre>WI.notifyLoggedOut(isLoggedOut);</pre>	センサがログアウトしたことをOpenText DASTに通知します。

Object Exists

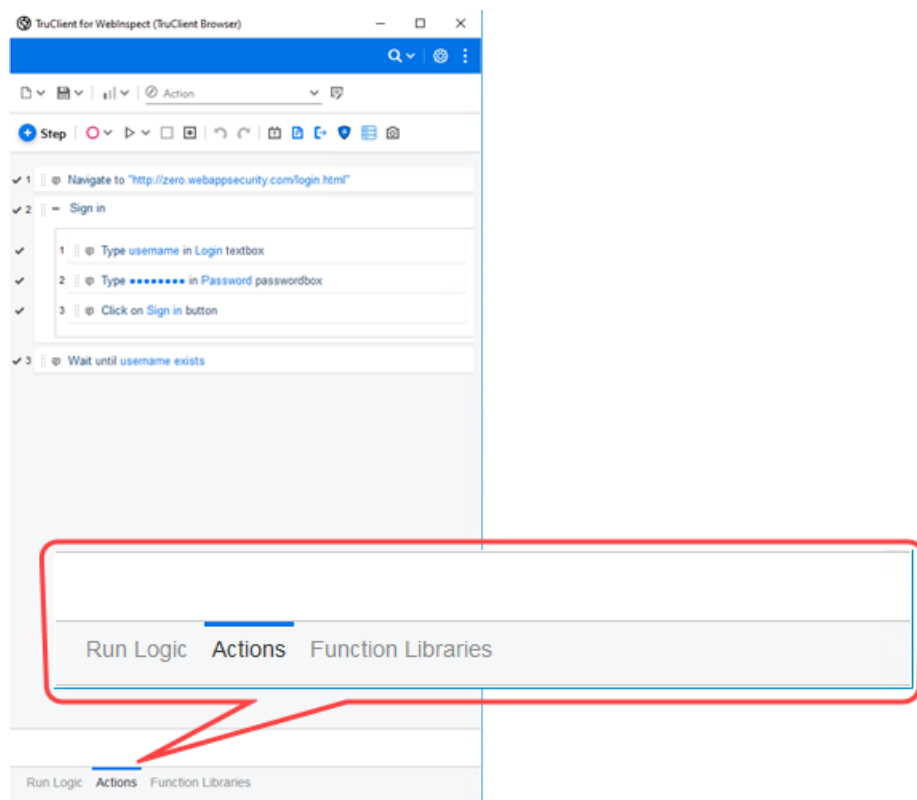
このテンプレートは、ログアウトを示すオブジェクトが存在するときに発生するログアウト条件を処理します。

次の表では、Object Existsテンプレートで使用されているJavaScriptコードについて説明します。

JavaScriptコード	説明
<pre>const element = document.getElementById("<element_id>");</pre>	指定したIDを持つ要素の定数参照を定義します。
<pre>WI.notifyLoggedOut(document.location.origin == "http (s)://<path>:<port>" && (element !== undefined && element !== null));</pre>	document.location.originプロパティが指定したURLに一致し、識別された要素が存在する場合に、センサがログアウトしたことをOpenText DASTに通知します。

アクションの使用

TruClientサイドバーウィンドウの下部からアクセスできる[アクション]タブでアクションの作成および実行ができます。

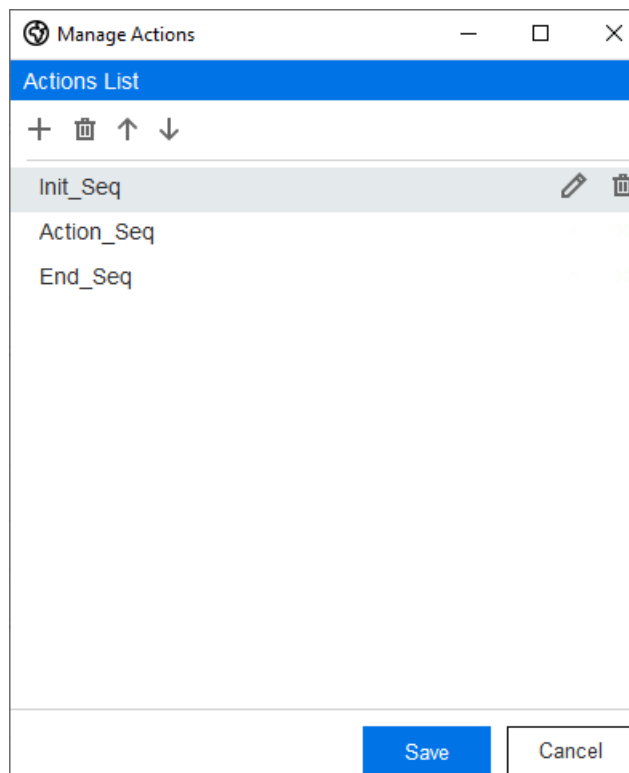


このタブでは、マクロの記録、編集、および再生を行います。

マクロへのアクションの追加

マクロにアクションを追加するには、次の操作を行います。

1. TruClientサイドバーウィンドウの右上隅にある[アクションの管理]アイコン(🔍)をクリックします。
[アクションの管理]ダイアログボックスが表示されます。



2. **[アクションの追加]**アイコン(+)をクリックします。アクションにわかりやすい名前を付けください。

アクションの順序の並び替え

アクションの順序を並べ替えるには、次の操作を行います。

1. TruClientサイドバーウィンドウの右上隅にある**[アクションの管理]**アイコン(🔧)をクリックします。
[アクションの管理]ダイアログボックスが表示されます。
2. アクションを選択します。
3. アクションをリスト内で上下に移動するには、**[上へ]**または**[下へ]**アイコン(↑ ↓)をクリックします。

アクションの削除

アクションを削除するには、次の操作を行います。

1. TruClientサイドバーウィンドウの右上隅にある**[アクションの管理]**アイコン(🔧)をクリックします。
[アクションの管理]ダイアログボックスが表示されます。
2. 削除するアクションを選択します。
3. **削除**アイコン(🗑️)をクリックします。

Webストレージキーの使用

状態管理にWebストレージを使用するアプリケーションでは、ログインプロセス中に関連するキーをローカルストレージに設定する場合があります。アプリケーションが状態を判別して維持できるようにするために、Webマクロレコーダでこれらのキーを同期する必要があります。そうしない場合、マクロ再生中にアプリケーションはWebストレージの状態を検出できず、認証されていないスキャンやリダイレクトが発生する可能性があります。

Webストレージキーエディタを使用すると、Webストレージキーを追加、編集、削除したり、再生からキーをロードしたりすることができます。

Webストレージキーエディタへのアクセス

Webストレージキーエディタを開くには:

- **Webストレージのサポート (Support Web Storage)]** 設定を有効にした後、**Webストレージキーの編集 (Edit Web Storage keys)]** アイコン()をクリックします。

Webストレージキーエディタが開きます。

注記: このアイコンは、**Webストレージのサポート (Support Web Storage)]** 設定が有効になっている場合にのみ表示されます。詳細については、「["対話型オプション" ページ316](#)」を参照してください。

再生からのキーのロード


Webストレージキーエディタを開く前にマクロを再生していた場合は、最近の再生で検出されたキーをロードできます。再生からキーをロードするには:

- **再生からロード (Load from playback)]** をクリックします。
Webストレージキーのリストにキーが表示されます。

Webストレージキーの追加

WebストレージキーエディタにWebストレージキーを追加するには:

1. **追加] アイコン(+)** をクリックします。
デフォルト値を持つWebストレージキーが追加されます。
2. **キー名 (Key Name)]** 列のデフォルト名をダブルクリックします。
フィールドを編集できるようになります。

#	Key Name	Key Name Type	Storage Type
 1	Key_1	Text	Local

3. フィールドに文字列または正規表現を入力します。

4. キー名のタイプを変更するには、**キー名のタイプ(Key Name Type)**列をダブルクリックし、ドロップダウンリストからタイプを選択します。オプションは次のとおりです。

- **テキスト(Text)** - プレーンテキストで構成されるキー名。
- **正規表現(Regex)** - 正規表現で構成されるキー名。

注記: 正規表現には構文検証が実行されます。

5. ストレージのタイプを変更するには、**ストレージのタイプ(Storage Type)**列をダブルクリックし、ドロップダウンリストからタイプを選択します。オプションは次のとおりです。

- **ローカル** - 有効期限がなく、ユーザがWebページに再アクセスするときに使用できるlocalStorage内のデータの場合。
- **セッション** - ブラウザが閉じたときにクリアされる、sessionStorage内のデータの場合。

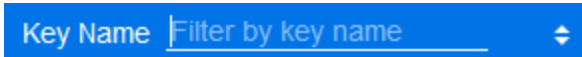
6. **Save**をクリックします。

Webストレージキーのフィルタリング

データの任意の列に基づいてWebストレージキーをフィルタできます。

リスト内のキーを **キー名(Key Name)**でフィルタするには:

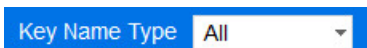
1. **キー名(Key Name)**列の見出しをダブルクリックします。
見出しに入力ボックスが表示されます。



2. ボックスに検索条件を入力します。
リストは入力に合わせてフィルタされます。

キーを **正規表現(Regex)**または **テキスト(Text)**でフィルタするには:

1. **キー名のタイプ(Key Name Type)**列の見出しをダブルクリックします。
見出しにドロップダウンリストボックスが表示されます。



2. フィルタ条件を選択します。
リストがフィルタされます。

ローカル(Local)または **セッション(Session)**でフィルタするには:

1. **ストレージのタイプ(Storage Type)**列の見出しをダブルクリックします。
見出しにドロップダウンリストボックスが表示されます。
2. フィルタ条件を選択します。
リストがフィルタされます。

フィルタのクリア

キー名 (Key Name)] によるフィルタをクリアするには:

- 見出しのフィルタボックスで **X** をクリックします。

キー名のタイプ (Key Name Type)] または **ストレージのタイプ (Storage Type)]** のフィルタをクリアするには:

- 見出しのドロップダウンリストボックスで、**すべて (All)]** を選択します。

Webストレージキーの編集

既存のWebストレージキーを編集するには:

注記: マクロ再生からキーがロードされた場合、これらのキーは編集できます。ただし、**キー名 (Key Name)]** を正規表現に変更し、**キー名のタイプ (Key Name Type)]** を **正規表現 (RegEx)]** に変更しない限り、編集は状態管理の役に立ちません。

- 変更する列の行をダブルクリックします。
- 次のいずれかを実行します。
 - キー名 (Key Name)]** の場合、必要に応じてテキストを編集します。
 - キー名のタイプ (Key Name Type)]** または **ストレージのタイプ (Storage Type)]** の場合、ドロップダウンリストから目的の値を選択します。

Webストレージキーの削除

既存のWebストレージキーを削除するには:

- 削除するキーを選択して、**削除] アイコン (🗑️)** をクリックします。
キーがリストから削除されます。

パラメータの使用

マクロを記録する場合は、パラメータを使用して次の操作を行います。

- ユーザ名とパスワードのパラメータを作成して、テスターがスキャンの開始時に独自の認証資格情報を使用したり、マルチユーザログインスキャンに複数の資格情報を使用したりできるようにします。詳細については、「["ユーザ名とパスワードパラメータの使用" 次のページ](#)」を参照してください。
- URLのパラメータを作成して、マクロの実行時にテスターが代替URLを指定できるようにします。この方法は、アプリケーションが複数の環境に存在し、継続的インテグレーションおよび継続的デリバリー (CI/CD) パイプラインの一部としてスキャンを実行する場合に便利です。

す。詳細については、「["URLパラメータの使用" ページ275](#)」を参照してください。

- 電話番号、電子メール、および電子メールパスワードのパラメータを作成して、テスターが2要素認証を必要とするマルチユーザログインスキャンを実行できるようにします。詳細については、「["2要素認証用のパラメータの作成" ページ278](#)」を参照してください。

大文字と小文字を区別するパラメータ名

パラメータ名では大文字と小文字が区別され、小文字のみを含む必要があります。


ユーザ名とパスワードパラメータの使用

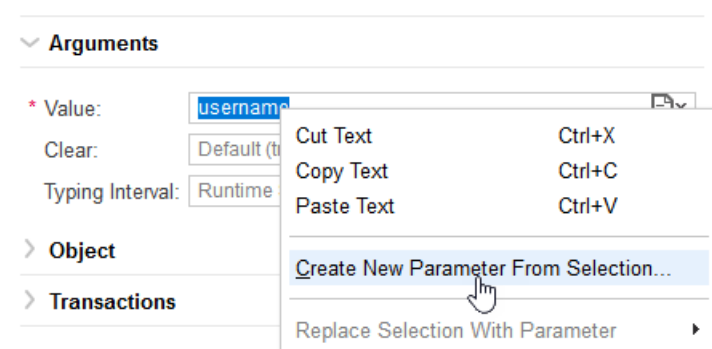
ログインマクロを作成してテストした後、記録された値をパラメータ名に置き換えるユーザ名とパスワードのパラメータを作成できます。その後、再生中にユーザ名とパスワードのパラメータを置き換える値のリストを作成できます。

ステップでのパラメータの作成

ユーザ名とパスワードのパラメータは、コンテキストメニューを使用してステップで直接作成できます。

ステップでパラメータを作成するには、次の手順に従います。

1. ユーザ名を含むステップで、**ステップエディタアイコン**()をクリックします。
ステップエディタが開きます。
2. **[引数]**をクリック(展開)します。
3. **[値]**ボックスで値を選択し、右クリックします。



4. **[Create New Parameter From Selection...(選択から新しいパラメータを作成)]**を選択します。
[パラメータ名の入力]ダイアログボックスが開きます。
5. **[パラメータ名]**ボックスにusernameと入力し、**[OK]**をクリックします。

✕

Enter Parameter Name

Parameter Name

username

Original Value


username

If the parameter name you use does not already exist, it will be added as a type 'File' and the Original Value will be set to 'username'.

OK

Cancel


重要! {/b}パラメータ名では大文字と小文字が区別され、小文字のみを含む必要があります。

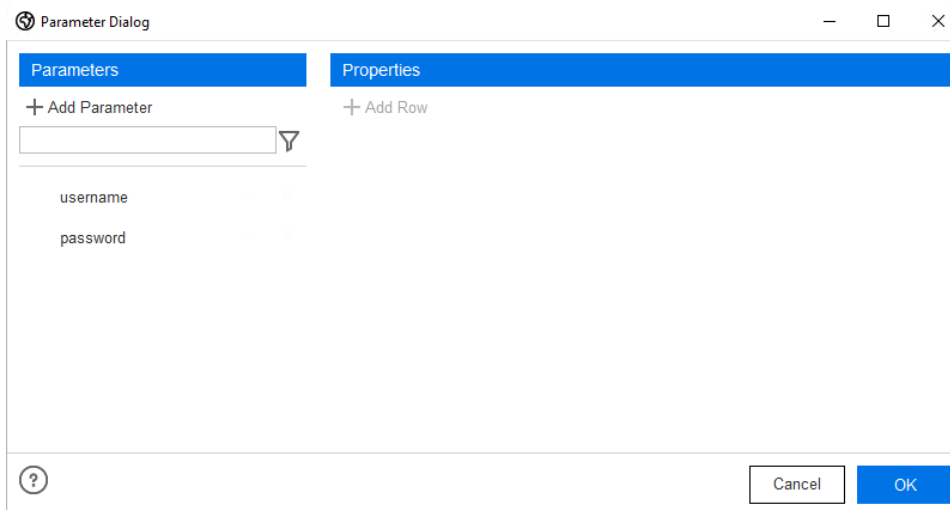
6. パスワードを含むステップで、**ステップエディタアイコン**()をクリックします。
ステップエディタが開きます。
7. **[引数]**をクリック(展開)します。
8. **[値]**ボックスで値を選択し、右クリックします。
9. **[Create New Parameter From Selection...(選択から新しいパラメータを作成)]**を選択します。
[パラメータ名の入力]ダイアログボックスが開きます。
10. **[パラメータ名]**ボックスにpasswordと入力し、**[OK]**をクリックします。
ユーザ名とパスワードのパラメータは、再生時に使用されるステップで直接作成されています。
ここで、パラメータダイアログを使用して、ユーザ名とパスワードパラメータの値のリストを作成する必要があります。

パラメータダイアログで値のリストを作成する

パラメータダイアログを使用して、ユーザ名とパスワードのパラメータを置き換える値のリストを作成します。

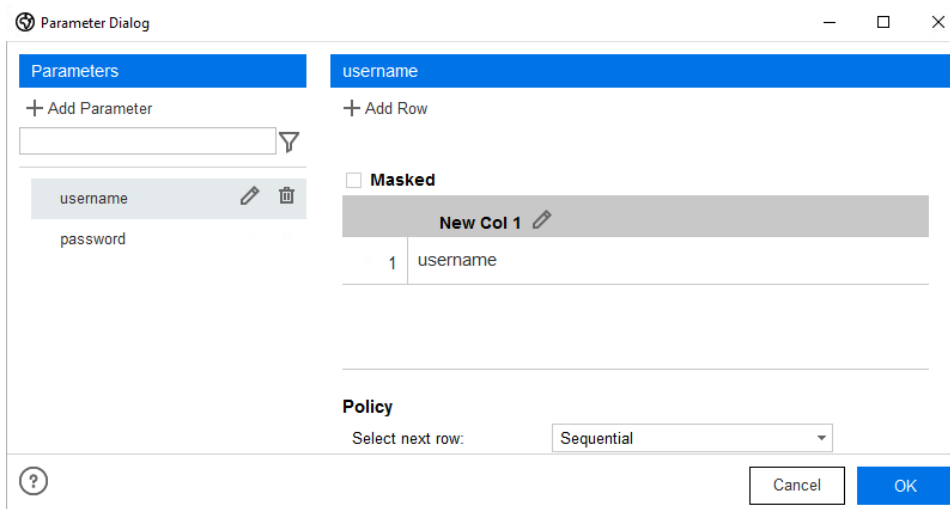
値のリストを作成するには、次の手順を実行します。

1. TruClientサイドバーで、**[パラメータの編集]**アイコン()をクリックします。
パラメータダイアログが開き、パラメータが一覧表示されます。



2. ユーザ名 パラメータをクリックします。

ユーザ名の値のリストが表示されます。マクロに記録された元の値は、マクロ再生時に使用する最初の値として一覧表示されます。



ヒント: 列名を編集するには、列ヘッダの編集アイコンをクリックして、新しい列名を入力します。例: User Names。

3. (オプション) 入力した値をマスクするには、[マスク]を選択します。

注記: Webマクロレコーダでマスクされた値は、OpenText DASTおよびFortify WebInspect Enterpriseでガイド付きスキャンを設定するときにもマスクされます。

4. (オプション) 別の値を追加するには(たとえば、マルチユーザログインスキャンのユーザ名のリストを作成する場合など)。
 - a. [行の追加]をクリックします。
 - b. カーソルを新しい行に移動します。

- c. マクロ再生時に使用する次の値を入力します。
- d. 追加する値ごとに、ステップaからcまでを繰り返します。
5. **パスワードパラメータ**をクリックします。
パスワードの値のリストが表示されます。マクロに記録された元の値は、マクロ再生時に使用する最初の値として一覧表示されます。
6. (オプション)入力した値をマスクするには、**[マスク]**を選択します。

注記: Webマクロレコーダでマスクされた値は、OpenText DASTおよびFortify WebInspect Enterpriseでガイド付きスキャンを設定するときにもマスクされます。
7. (オプション)別の値を追加するには(たとえば、マルチユーザログインスキャンのパスワードのリストを作成する場合など)。
 - a. **[行の追加]**をクリックします。
 - b. カーソルを新しい行に移動します。
 - c. マクロ再生時に使用する次の値を入力します。
 - d. 追加する値ごとに、ステップaからcまでを繰り返します。
8. **[OK]**をクリックしてパラメータをマクロに保存し、パラメータダイアログを閉じます。
9. マクロを再生して、ログインが正しいか検証します。
10. マクロを保存します。

ポリシー

パラメータダイアログに表示されるポリシー設定は、OpenText DASTIには適用できません。


URLパラメータの使用

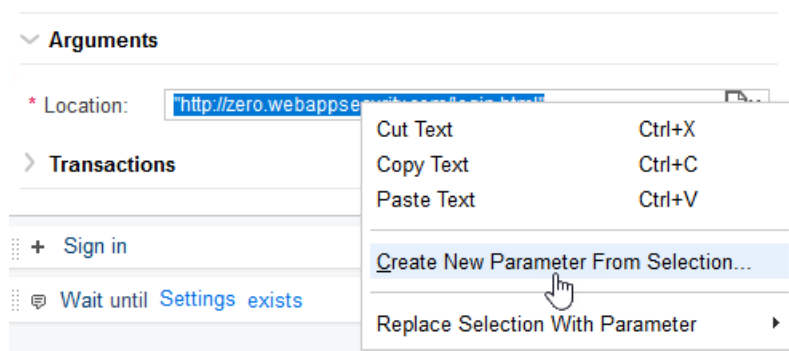
ログインマクロを作成してテストした後、記録された値をパラメータ名に置き換えるURLパラメータを作成できます。

ステップでのパラメータの作成

URLパラメータは、コンテキストメニューを使用してステップ内に直接作成できます。

ステップでパラメータを作成するには、次の手順を実行します。

1. URLを含むステップ(「...に移動する」)で、**ステップエディタアイコン**()をクリックします。
ステップエディタが開きます。
2. **[引数]**をクリック(展開)します。
3. **[場所]**ボックスで値を選択し、右クリックします。



4. **[Create New Parameter From Selection...(選択から新しいパラメータを作成)]**を選択します。
[パラメータ名の入力]ダイアログボックスが開きます。

Enter Parameter Name

Parameter Name

Original Value

If the parameter name you use does not already exist, it will be added as a type 'File' and the Original Value will be set to 'http://zero.webappsecurity.com/login.html'.

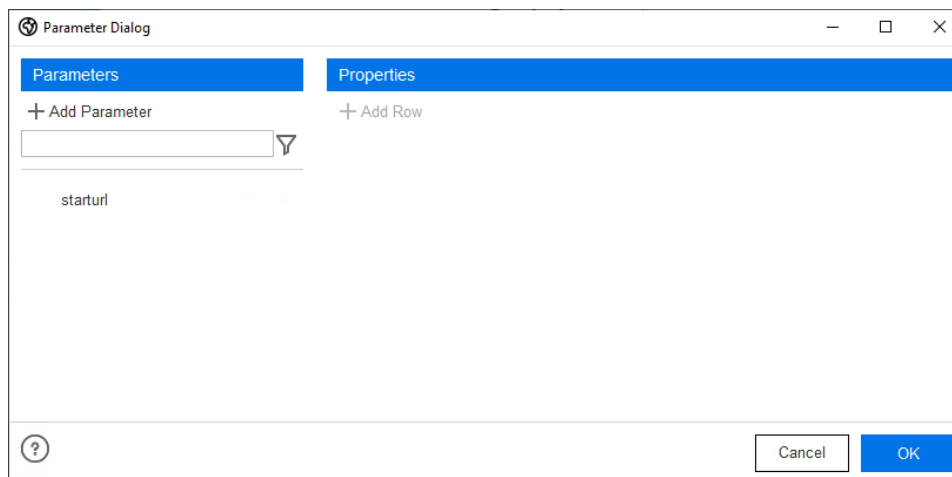
重要! パラメータ名では大文字と小文字が区別され、小文字のみを含む必要があります。

5. **[パラメータ名]**ボックスにstarturlなどの名前を入力し、**[OK]**をクリックします。
starturlパラメータは、再生中に使用されるステップに直接作成されています。ここで、パラメータダイアログを使用して、starturlパラメータの値のリストを作成する必要があります。

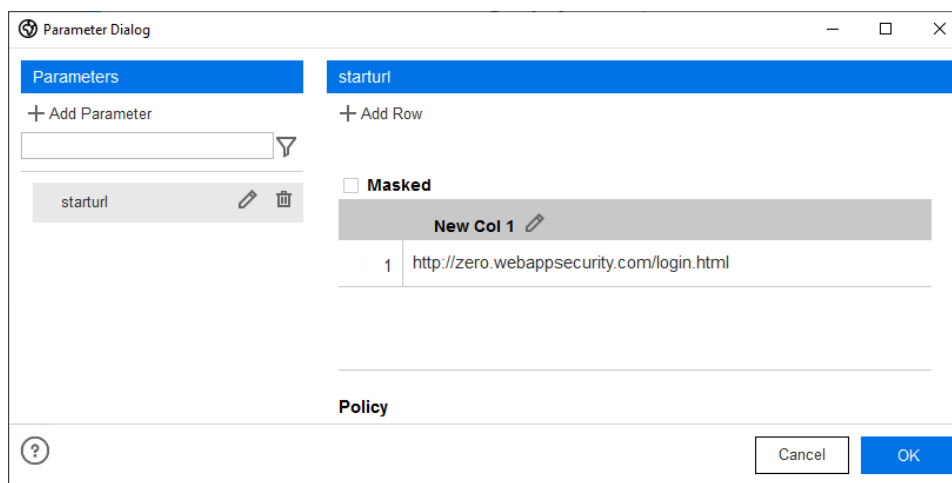
パラメータダイアログで値のリストを作成する

パラメータダイアログを使用して、starturlパラメータを置き換える値のリストを作成します。
値のリストを作成するには、次の手順を実行します。

1. TruClientサイドバーで、**[パラメータの編集]**アイコン(🔗)をクリックします。
パラメータダイアログが開き、パラメータが一覧表示されます。



2. URLパラメータをクリックします。この例ではstarturlとなっています。
URL値のリストが表示されます。マクロに記録された元の値は、マクロ再生時に使用する最初の値として一覧表示されます。



ヒント: 列名を編集するには、列ヘッダの編集アイコンをクリックして、新しい列名を入力します。例:URLs List。

3. (オプション)別の値を追加するには、次の手順を実行します。
 - a. [行の追加]をクリックします。
 - b. カーソルを新しい行に移動します。
 - c. マクロ再生時に使用する次の値を入力します。
 - d. 追加する値ごとに、ステップaからcまでを繰り返します。
4. [OK]をクリックしてパラメータをマクロに保存し、パラメータダイアログを閉じます。
5. マクロを再生して、ログインが正しいか検証します。
6. マクロを保存します。

ポリシー

パラメータダイアログに表示されるポリシー設定は、OpenText DASTIには適用できません。

2要素認証用のパラメータの作成


ログインマクロを作成してテストした後、電話番号、電子メール、および電子メールのパスワードパラメータを作成できます。その後、再生中にこれらのパラメータを置き換える値のリストを作成できます。2要素認証のパラメータを使用すると、マルチユーザログインスキャンを実行できます。

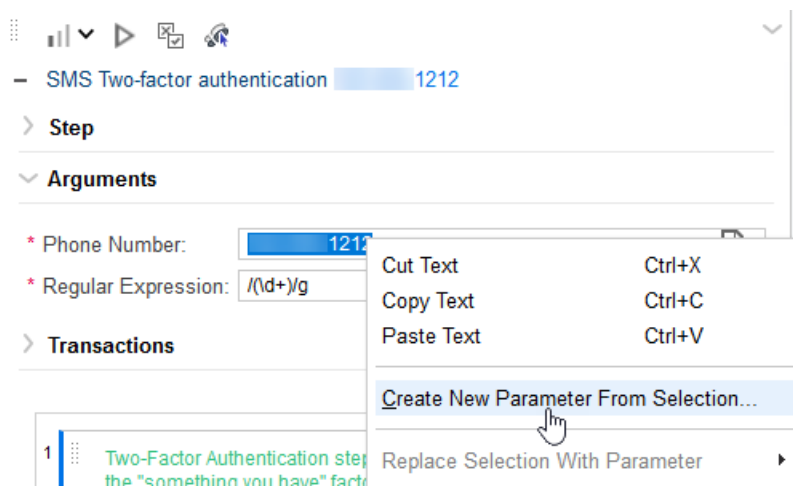
ヒント: イベントベースのWebマクロレコーダでパラメータを作成した後、マルチユーザログインスキャンを設定し、追加の電話番号、電子メールアドレス、および電子メールパスワードをOpenText DASTの [スキャン設定: 認証(Scan Settings: Authentication)] ダイアログボックスに入力できます。

電話番号パラメータの作成

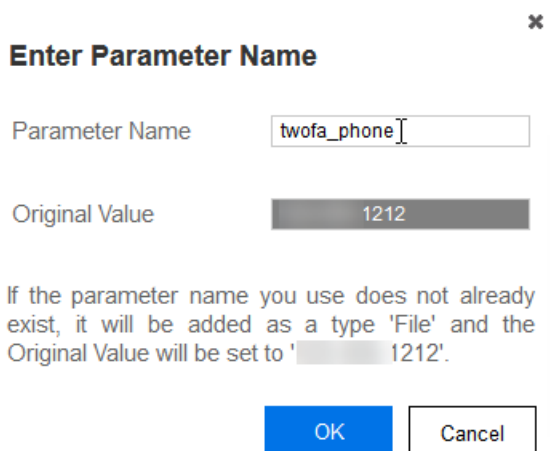
2要素認証グループステップでは、コンテキストメニューを使用して電話番号パラメータを直接作成できます。

電話番号パラメータを作成するには、次のコマンドを実行します。

1. 2要素認証グループステップで、**ステップエディタアイコン**()をクリックします。
ステップエディタが開きます。
2. **[引数]**をクリック(展開)します。
3. **[電話番号]**ボックスで番号を選択し、右クリックします。



4. **[Create New Parameter From Selection...(選択から新しいパラメータを作成)]**を選択します。
[パラメータ名の入力]ダイアログボックスが開きます。
5. **[パラメータ名]**ボックスにtwofa_phoneと入力し、**[OK]**をクリックします。




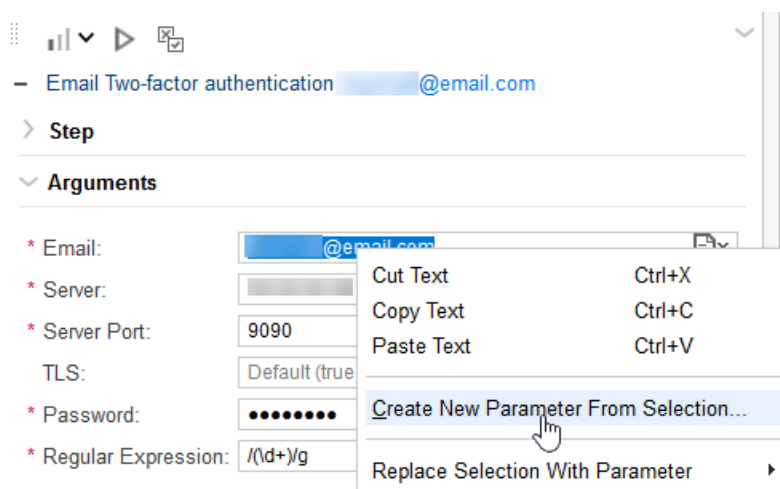
重要! {/b}パラメータ名では大文字と小文字が区別され、小文字のみを含む必要があります。

電子メールおよび電子メールパスワードパラメータの作成

2要素認証グループステップでは、コンテキストメニューを使用して電子メールおよび電子メールのパスワードパラメータを直接作成できます。

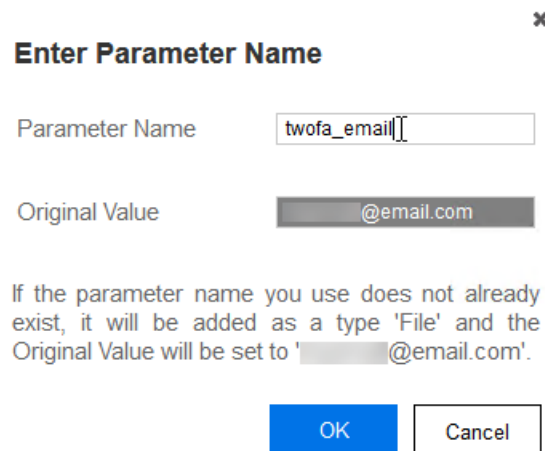
電子メールおよび電子メールのパスワードパラメータを作成するには、次のコマンドを実行します。

1. **2要素認証**グループステップで、**ステップエディタアイコン**()をクリックします。
ステップエディタが開きます。
2. **[引数]**をクリック(展開)します。
3. **[電子メール]**ボックスで電子メールアドレスを選択し、右クリックします。



4. **[Create New Parameter From Selection...(選択から新しいパラメータを作成)]**を選択します。
[パラメータ名の入力]ダイアログボックスが開きます。

5. **[パラメータ名]**ボックスにtwofa_emailと入力し、**[OK]**をクリックします。



重要! パラメータ名では大文字と小文字が区別され、小文字のみを含む必要があります。

6. **[パスワード]**ボックスでパスワードを選択し、右クリックします。
7. **[Create New Parameter From Selection...(選択から新しいパラメータを作成)]**を選択します。
- [パラメータ名の入力]**ダイアログボックスが開きます。
8. **[パラメータ名]**ボックスにtwofa_emailpasswordと入力し、**[OK]**をクリックします。

オブジェクトに関連するステップ引数

TruClientでは、役割別に分類されたオブジェクトに関連する次のステップ引数を使用できます。

- "オーディオの役割" 次のページ
- "ブラウザの役割" 次のページ
- "チェックボックスの役割" ページ285
- "日付選択の役割" ページ285
- "要素の役割" ページ285
- "ファイルボックスの役割" ページ290
- "Flashオブジェクトの役割" ページ290
- "フォーカス可能な役割" ページ290
- "リストボックスの役割" ページ291
- "Multi_listboxの役割" ページ291
- "ラジオグループの役割" ページ292
- "スライダの役割" ページ292

- ["テキストボックスの役割" ページ293](#)
- ["ビデオの役割" ページ293](#)

オーディオの役割

次の表は、オーディオ役割オブジェクトのシークアクションのステップ引数について説明しています。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

引数	説明
時間	オーディオ再生の現在の位置(秒)を設定または返します。

ブラウザの役割

次の表は、ブラウザの役割オブジェクトに関連するステップ引数について説明しています。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

アクティブ化

次の表は、アクティブ化アクションのステップ引数について説明しています。

引数	説明
序数	整数として定義されます。
タイトル	文字列として定義されます。 注記: タイトルは記録中に自動的に更新され、代替ステップとして設定できます。

[アクティブ化]タブ

次の表は、[アクティブ化]タブアクションのステップ引数について説明しています。

引数	説明
序数	アクティブ化するタブ(整数)を指定します。
タイトル	文字列として定義されます。

引数	説明
	注記: タイトルは記録中に自動的に更新され、代替ステップとして設定できます。

[閉じる]タブ

次の表は、[閉じる]タブアクションのステップ引数について説明しています。

引数	説明
序数	閉じるタブ(整数)を指定します。
タイトル	指定したブラウザウィンドウをフォアグラウンドに移動します。文字列として定義されます。 注記: タイトルは記録中に自動的に更新され、代替ステップとして設定できます。

[追加]タブ

次の表は、[追加]タブアクションのステップ引数について説明しています。

引数	説明
場所	新しく開いたタブで移動先のURLを指定します。
ウィンドウ	アプリケーションのグローバルウィンドウオブジェクトを指します 注記: window.locationオブジェクトは、Internet Explorerでは使用できません。代わりにdocument.URLオブジェクトを使用してください。

移動

次の表は、移動アクションのステップ引数について説明しています。

引数	説明
場所。	移動先のURLを指定します。

戻る

次の表は、[戻る]アクションのステップ引数について説明しています。

引数	説明
カウント	戻るページ数を指定します。

進む

次の表は、[進む]アクションのステップ引数について説明しています。

引数	説明
カウント	進むページ数を指定します。

リサイズ

次の表は、[リサイズ]アクションのステップ引数について説明しています。

引数	説明
幅	新しい幅を指定します。この値を空白のままにすると、幅のサイズは変更されないという意味になります。
高さ	新しい高さを指定します。この値を空白のままにすると、高さのサイズは変更されないという意味になります。

スクロール

次の表は、スクロールアクションのステップ引数について説明しています。

引数	説明
X座標	新しいx座標を示します。空白のままにすると、x軸に沿ってスクロールしないことを意味します。
Y座標	新しいy座標を示します。この値を空白のままにすると、y軸に沿ってスクロールしないことを意味します。

ダイアログ - 確認

次の表は、[ダイアログ - 確認]アクションのステップ引数について説明しています。

引数	説明
ボタン	[OK]または[キャンセル]を示します。

ダイアログプロンプト

次の表は、ダイアログプロンプトアクションのステップ引数について説明しています。

引数	説明
値	入力する文字列を示します。
ボタン	[OK]または[キャンセル]を示します。

ダイアログ - 認証

次の表は、[ダイアログ - 認証]アクションのステップ引数について説明しています。

引数	説明
ユーザ名	入力するユーザ名を指定します。
Password	入力するパスワードを指定します。
ドメイン	入力するドメインを指定します。
ボタン	[OK]または[キャンセル]を示します。

ダイアログ - パスワードの確認

次の表は、[ダイアログ - パスワードの確認]アクションのステップ引数について説明しています。

引数	説明
Password	入力するパスワードを指定します。
ボタン	[OK]または[キャンセル]を示します。

検証

次の表は、[検証]アクションのステップ引数について説明しています。

引数	説明
値	検証するプロパティの値を示します。
プロパティ	検証するプロパティを指定します。ブラウザオブジェクトの次のプロパティを検証できます。 <ul style="list-style-type: none">• タイトル - ブラウザウィンドウのタイトルを指定します。• 場所 - ブラウザウィンドウの場所を指定します。
条件	値とプロパティの引数間の関係を指定します。

チェックボックスの役割

次の表は、チェックボックス役割オブジェクトの**設定**アクションのステップ引数について説明しています。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

引数	説明
オン	チェックボックスをオン(true)またはオフ(false)に設定します。

日付選択の役割

次の表は、日付選択役割オブジェクトの**[日付の設定]**アクションのステップ引数について説明しています。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

引数	説明
曜日	曜日を表します。値は1～31の整数です。

要素の役割

次の表は、要素の役割オブジェクトに関連するステップ引数について説明しています。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

マウス操作

次の表は、マウスダウン、マウスアップ、マウスオーバー、クリック、およびダブルクリックの各アクションのステップ引数について説明しています。

注記: マウスオーバーにはX/Y座標引数は含まれません。

引数	説明
ボタン	クリックするマウスボタンを識別します。
X座標	オブジェクトの左上隅を基準にしたアクションのオフセット位置を識別します。指定しない場合、デフォルトはオブジェクトの中央になります。
Y座標	オブジェクトの左上隅を基準にしたアクションのオフセット位置を識別します。指定しない場合、デフォルトはオブジェクトの中央になります。
[Ctrl]キー	アクション中にこのキーを押すかどうかを示します。
[Alt]キー	アクション中にこのキーを押すかどうかを示します。
[Shift]キー	アクション中にこのキーを押すかどうかを示します。

ドラッグ

次の表は、[ドラッグ]アクションのステップ引数について説明しています。

引数	説明
ボタン	クリックするマウスボタンを識別します。
Xオフセット	x軸上でオブジェクトをドラッグするピクセルの量を示します。正の数は、右側へのドラッグを示します。
Yオフセット	y軸上でオブジェクトをドラッグするピクセルの量を示します。正の数は、ドラッグダウンを示します。
パス	ユーザのドラッグパスを表す座標のリストを指定します。この引数は変更しないでください。
[Ctrl]キー	アクション中にこのキーを押すかどうかを示します。

引数	説明
[Alt]キー	アクション中にこのキーを押すかどうかを示します。
[Shift]キー	アクション中にこのキーを押すかどうかを示します。

注記: Xオフセット、Yオフセット、およびパスの引数は相互排他的です。

ドラッグ先

次の表は、[ドラッグ先]アクションのステップ引数について説明しています。

引数	説明
ターゲットオブジェクト	ステップオブジェクトをこのターゲットオブジェクトにドラッグすることを示します。
HTML 5	ブラウザにドラッグアンドドロップサポートを提供し、コード化を容易にします。この引数が「true」の場合は、「ターゲットオブジェクト」引数と「HTML5」引数だけが表示されます。「false」の場合は、他の引数も表示されます。
ボタン	クリックするマウスボタンを識別します。
Xオフセット	x軸のターゲットオブジェクトの左上からのオフセットを指定します。この数は正である必要があります。
Yオフセット	y軸のターゲットオブジェクトの左上からのオフセットを指定します。この数は正である必要があります。
[Ctrl]キー	アクション中にこのキーを押すかどうかを示します。
[Alt]キー	アクション中にこのキーを押すかどうかを示します。
[Shift]キー	アクション中にこのキーを押すかどうかを示します。

プロパティの取得

次の表は、[プロパティの取得]アクションのステップ引数について説明しています。

引数	説明
プロパティ	指定した変数に保存される値を持つプロパティを示します。使用可能なプロパティのリストは、オブジェクトのすべての役割によって異なります。すべてのオブジェクトで利用できるデフォルトのプロパティを次

引数	説明
	に示します。 <ul style="list-style-type: none">• 表示されるテキスト - DOM textContentプロパティに対応する、項目の表示テキストを示します。• すべてのテキスト - DOM textContentプロパティに対応する項目のテキスト全体を示します。• 内部HTML - DOM innerHTMLプロパティに対応するオブジェクトの内部htmlマークアップを示します。
変数	指定したプロパティ値を格納する変数の名前を示します。

スクロール

次の表は、スクロールアクションのステップ引数について説明しています。

引数	説明
水平	水平方向にスクロールする距離(ピクセル単位)を指定します。
垂直	垂直方向にスクロールする距離(ピクセル単位)を指定します。

注記: どちらの引数も整数で、最小値とデフォルト値は0である必要があります。スクロールは、要素自体ではなく、含まれているドキュメントで実行されます。

アップロード

次の表は、アップロードアクションのステップ引数について説明しています。

引数	説明
パス	選択したパスを指定します。

検証

次の表は、[検証]アクションのステップ引数について説明しています。

引数	説明
値	検証する文字列または番号を示します。
プロパティ	値が検証されるオブジェクトプロパティを示します。検証に使用できるプロパティのリストは、オブジェクトのすべての役割によって異なります。

引数	説明
	<p>す。すべてのオブジェクトの検証に使用できるデフォルトのプロパティを次に示します。</p> <ul style="list-style-type: none">• 表示されるテキスト - アプリケーションに表示される項目を識別します。• すべてのテキスト - アプリケーション内にあるが、必ずしも表示されない項目を識別します。このカテゴリの項目は、DOMプロパティ <code>textContent</code> に含まれています。• 内部HTML - DOMプロパティ <code>innerHTML</code> に含まれる項目を識別します。
条件	値とプロパティの引数の関係を示します。

プロパティの待機

次の表は、[プロパティの待機]アクションのステップ引数について説明しています。

引数	説明
値	ステップがパスする前にステップが待機する、指定されたプロパティの値を示します。
プロパティ	<p>スクリプトが待機する値を持つオブジェクトプロパティを示します。待機できるプロパティのリストは、オブジェクトのすべての役割によって異なります。すべてのオブジェクトで使用するデフォルトのプロパティを次に示します。</p> <ul style="list-style-type: none">• 表示されるテキスト - アプリケーションに表示される項目を識別します。• すべてのテキスト - アプリケーション内にあるが、必ずしも表示されない項目を識別します。このカテゴリの項目は、DOMプロパティ <code>textContent</code> に含まれています。• 内部HTML - DOMプロパティ <code>innerHTML</code> に含まれる項目を識別します。
条件	値とプロパティの引数の関係を示します。

ファイルボックスの役割

次の表は、ファイルボックス役割オブジェクトの**設定アクション**のステップ引数について説明しています。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

引数	説明
パス	選択したパスを指定します。

Flashオブジェクトの役割

次の表は、Flashオブジェクト役割の**入力アクション**のステップ引数について説明しています。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

引数	説明
値	入力するテキストを指定します。

フォーカス可能な役割

次の表は、フォーカス可能な役割オブジェクトの**[キーを押す]**アクションのステップ引数について説明しています。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

引数	説明
キー名	<Enter>、<Space>、<Backspace>、<Tab>、<Escape>、<Delete>、<Up>、<Down>、<Left>、または<Right>を指定します。
[Ctrl]キー	アクション中にこのキーを押すかどうかを示します。
[Alt]キー	アクション中にこのキーを押すかどうかを示します。
[Shift]キー	アクション中にこのキーを押すかどうかを示します。

リストボックスの役割

次の表は、リストボックス役割オブジェクトの**選択**アクションのステップ引数について説明しています。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

引数	説明
Text	選択した文字列または正規表現を示します。この値はオプションです。
序数	リスト内で選択した項目の順序を指定します。テキスト引数も指定されている場合、この引数はリストボックス内の指定されたテキスト値のインスタンスを参照します。0の序数はランダムな値を生成します。テキストと序数の両方が空の場合、デフォルトの序数(1)が自動的に入力されます。
内部オブジェクト	コンテナオブジェクトを識別して序数を指定するのではなく、オプション要素自体に対するTruClientのオブジェクト識別メカニズムに基づいてオプションを選択できます。

Multi_listboxの役割

次の表は、multi_listboxの役割オブジェクトに関連するステップ引数について説明しています。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

選択

次の表は、選択アクションのステップ引数について説明しています。

引数	説明
Text	選択した文字列または正規表現を示します。
序数	リスト内で選択した項目の順序を指定します。テキスト引数も指定されている場合、この引数はリストボックス内の指定されたテキスト値のインスタンスを参照します。0の序数はランダムな値を生成します。

複数選択

次の表は、複数選択アクションのステップ引数について説明しています。

引数	説明
Text	オプションのテキスト。
序数別	項目の区切り記号の序数を指定します。
区切り記号	選択した値を分離するために使用する文字を指定します。

ラジオグループの役割

次の表は、ラジオグループ役割オブジェクトの[選択]アクションのステップ引数について説明しています。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

引数	説明
Text	選択した文字列または正規表現を示します。
序数	リスト内で選択した項目の順序を指定します。テキスト引数も指定されている場合、この引数はリストボックス内の指定されたテキスト値のインスタンスを参照します。0の序数はランダムな値を生成します。

スライダの役割

次の表は、スライダ役割オブジェクトの設定アクションのステップ引数について説明しています。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

引数	説明
値	スライダを設定する値を指定します。

テキストボックスの役割

次の表は、テキストボックス役割オブジェクトの[入力]アクションのステップ引数について説明しています。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

引数	説明
値	入力されたテキストを示します。
クリア	入力前にテキストボックスをクリアします。デフォルトの設定はtrueです。
タイピング間隔	キーストローク間の平均時間をミリ秒単位で示します。

ビデオの役割

次の表は、ビデオの役割オブジェクトのシークアクションのステップ引数について説明しています。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

引数	説明
時間	ビデオ再生の現在の位置(秒)を設定または返します。

オブジェクトに関連しないステップ引数

次の表は、オブジェクトに関連しないステップ引数について説明しています。これらのステップ引数のアクションは、オブジェクトに対しては動作しません。したがって、役割は割り当てられていません。

ヒント: 必須引数は、ユーザインタフェースの引数名の左側に赤い星で示されます。すべての引数はJavaScriptコードおよびTruClient機能を値として受諾することができます。

JavaScriptを評価する

[JavaScriptを評価する]アクションは、ステップに含まれるJavaScriptコードを実行します。次の表は、[JavaScriptを評価する]アクションのステップ引数について説明しています。

引数	説明
コード	実行するJavaScriptコードを指定します。

オブジェクト上でJSを評価する

[オブジェクト上でJSを評価する]アクションは、指定したオブジェクトがアプリケーションにロードされた後に、ステップに含まれるJavaScriptコードを実行します。また、「object」キーワードを使用してオブジェクトとのやり取りができます。たとえば、`object.click();`を実行してオブジェクトのクリックを開始できます。

次の表は、[オブジェクト上でJSを評価する]アクションのステップ引数について説明しています。

引数	説明
コード	実行するJavaScriptコードを指定します。

Catchエラー

[Catchエラー]アクションは直前のステップでエラーを検出し、Catchエラーステップのコンテンツを実行します。次の表は、[Cを評価する]アクションのステップ引数について説明しています。

引数	説明
エラータイプ。	<p>キャッチしたいエラータイプを指定します。</p> <ul style="list-style-type: none">• 任意• オブジェクトID - アクションが実行されたオブジェクトが見つからないことを示します。• ステップ引数 - 前のステップの1つ以上の引数が無効であることを示します。たとえば、データタイプが間違っている場合です。• ステップアクション - ユーザアクションが失敗したことを示します。たとえば、ナビゲーションステップでページが見つからなかった場合です。UI要素に対するアクションの場合、オブジェクトが見つかったにもかかわらず、アクションが失敗した場合に、このエラーがトリガされます。

Forループ

Forループは、ループに含まれるステップを指定された回数繰り返すロジック構造です。次の表は、Forループアクションのステップ引数について説明しています。

引数	説明
初期化	最初の繰り返しの条件をテストする前に満たされている必要がある初期化操作の条件を指定します。
条件	次の繰り返しに進むための条件を指定します。オプションは次のとおりです。 <ul style="list-style-type: none">• true - 指定した条件が満たされていることを示します。• false - 指定された条件が満たされていないことを示します。• 正規表現 - 正規表現を条件として定義します。
増分	条件のカウンタを増分します。

汎用APIアクション

汎用APIアクションは、挿入して手動で設定できる空のステップです。引数は、選択したAPIによって異なります。API引数の詳細については、TruClientヘルプセンター (https://admhelp.microfocus.com/tc/en/2022-2022-r1/Content/TruClient/TC_Functions.htm)のAPIヘルプを参照してください。

注記: Webマクロレコーダは、TruClient Help Centerで説明されているAPI引数のサブセットをサポートしています。

次の表は、汎用APIアクションのステップ引数について説明しています。

引数	説明
変数	戻り値が保存されるJavaScript変数の名前を指定します。

Ifブロック

Ifブロックアクションは、条件が満たされた場合にブロックに含まれるステップを実行するロジック構造です。次の表は、[Ifブロック]アクションのステップ引数について説明しています。

引数	説明
条件	次の繰り返しに進むための条件を指定します。オプションは次のとおりです。

引数	説明
	おりです。 <ul style="list-style-type: none">• true - 指定した条件が満たされていることを示します(デフォルト設定)。• false - 指定された条件が満たされていないことを示します。• 正規表現 - 正規表現を条件として定義します。

待機

待機アクションは、次のステップに進む前に、指定された秒数(またはミリ秒)待機します。次の表は、[PDFコンテンツの検証]アクションのステップ引数について説明しています。

引数	説明
間隔	ステップが渡される前にステップが待機する時間値を指定します。デフォルト値は3です。
単位	間隔の値を指定します。使用可能な単位プロパティは、秒(デフォルト設定)とミリ秒です。
思考時間	待機時間を思考時間の計算に含めるかどうかを指定します。デフォルト設定はtrueです。

マクロの強化

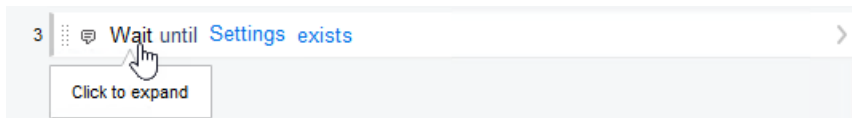
記録されたマクロに、次の拡張機能を追加することができます。

- ["ステップの変更" 下](#)
- ["ループとループ修飾子の挿入" 次のページ](#)
- ["Ifブロック、If-elseブロック、および終了ステップの挿入" ページ298](#)
- ["コメントの挿入" ページ299](#)
- ["Catchエラーステップの挿入" ページ300](#)
- ["オブジェクトが存在することの検証" ページ300](#)
- ["汎用ステップの挿入" ページ300](#)

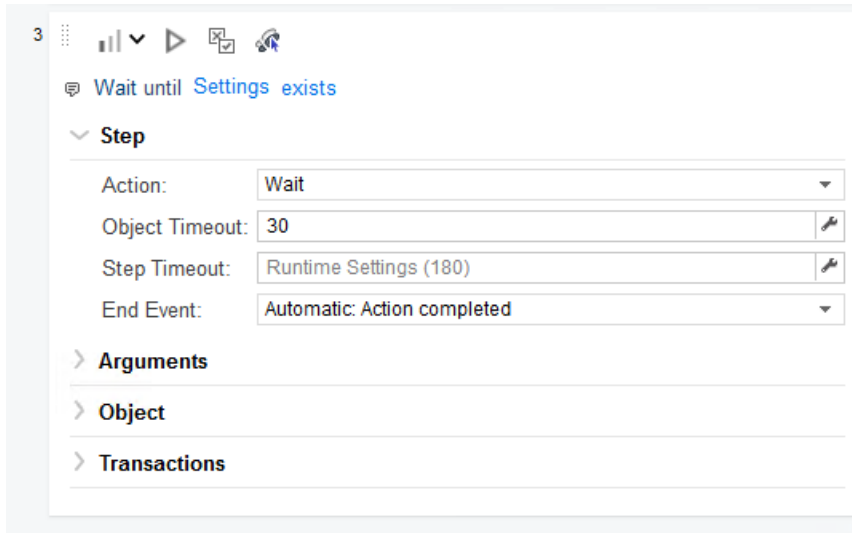
ステップの変更

ステップの引数とオブジェクトを変更するには、次の手順を実行します。

- 目的のステップを選択し、オプションを展開します。



これによりステップが展開され、オブジェクトとプロパティを変更できます。




ループとループ修飾子の挿入

ループは、一定の基準が満たされるまで、または指定された反復回数が繰り返されるまで、マクロの選択された部分を繰り返します。ループおよびブレイク/続行ループ修飾子は、[ステップ]ボックスの[フロー制御]セクションから挿入できます。

「For」ループの挿入

「For」ループは、終了条件が満たされるまで、またはコードがbreakステートメントに達するまでループで囲まれたステップを実行します。ループ引数はJavaScript構文を使用します。


Forループを挿入するには、次の操作を行います。

1. [TruClient]サイドバーで、[ステップの追加]アイコン( Step)をクリックします。
[ステップ]ボックスが開きます。
2. [フロー制御]をクリックします。
3. Forループステップをクリックして、記録されたステップ内の目的の場所にドラッグします。

「Break」ステートメントの挿入

Breakステートメントは、現在のループをすぐに終了する必要があることを示しています。たとえば、Forループで5回の繰り返しの2番目にBreakステートメントが発生した場合、ループは残りの繰り返しを完了せずにただちに終了します。


Breakステートメントを挿入するには、次の操作を行います。

1. [TruClient]サイドバーで、[ステップの追加]アイコン( Step)をクリックします。
[ステップ]ボックスが開きます。
2. [フロー制御]をクリックします。
3. **Break**ステップをクリックして、記録されたステップ内の目的の場所にドラッグします。

「Continue」ステートメントの挿入

Continueステートメントは、現在のループの繰り返しをすぐに終了する必要があることを示しています。その後、ループ条件がチェックされ、ループ全体を終了する必要があるかどうかも確認されます。たとえば、Forループで5回の繰り返しの2番目にContinueステートメントが発生した場合、2番目の反復はただちに終了され、3番目の反復が開始されます。

Continueステートメントを挿入するには、次の操作を行います。

1. [TruClient]サイドバーで、[ステップの追加]アイコン( Step)をクリックします。
[ステップ]ボックスが開きます。
2. [フロー制御]をクリックします。
3. **Continue**ステップをクリックして、記録されたステップ内の目的の場所にドラッグします。


Ifブロック、If-elseブロック、および終了ステップの挿入

マクロの一部を条件付きに設定するには、IfブロックまたはIf-elseブロックを挿入します。終了ステップを実行すると、マクロは繰り返しまたはマクロ全体を終了します。これらは、Ifステートメントと一緒に使用してマクロを終了したり、指定した条件が発生した場合の繰り返しに使用できます。

これらの各アクションおよび引数の詳細については、「["オブジェクトに関連しないステップ引数" ページ293](#)」を参照してください。

Ifブロックの挿入

Ifブロックを挿入するには、次の手順を実行します。

1. [TruClient]サイドバーで、[ステップの追加]アイコン( Step)をクリックします。
[ステップ]ボックスが開きます。
2. [フロー制御]をクリックします。
3. **Ifブロック**ステップをクリックして、記録されたステップ内の目的の場所にドラッグします。

Else条件の追加

Else条件を追加するには、次の手順を実行します。


1. 展開したステップで[Elseの追加]リンクをクリックします。



2. [Else]フィールドに、else条件を入力します。

Exitステップの挿入


Exitステップを挿入するには、次の手順を実行します。

1. [TruClient]サイドバーで、[ステップの追加]アイコン( Step)をクリックします。
[ステップ]ボックスが開きます。
2. [フロー制御]をクリックします。
3. Exitステップをクリックして、記録されたステップ内の目的の場所にドラッグします。

コメントの挿入

マクロにコメントを追加することで、マクロ内の特定のステップが何を達成するのか、他の人が理解できるようになります。

マクロにコメントを挿入するには、次の操作を行います。


1. [TruClient]サイドバーで、[ステップの追加]アイコン( Step)をクリックします。
[ステップ]ボックスが開きます。
2. [その他]をクリックします。
3. コメントステップをクリックして、記録されたステップ内の目的の場所にドラッグします。
4. 指定されたスペースにコメントを入力します。

Catchエラーステップの挿入

「Catchエラー」ステップは、前のステップにエラーが含まれている場合に内容を実行するグループステップです。さらに、エラーは「キャッチ」され、返されません。Catchエラーステップを定義して、すべてのエラーをキャッチ、または特定の種類のエラーをキャッチすることができます。連続する2つのcatchエラーステップがある場合は、両方とも同じステップに適用されます。

ヒント: ステップをグループ化するには、[Ctrl]キーを押しながらクリックして複数のステップを選択し、いずれかのステップを右クリックして、[グループステップ]をクリックします。


Catchエラーステップを挿入するには、次の操作を行います。

1. [TruClient]サイドバーで、[ステップの追加]アイコン( Step)をクリックします。
[ステップ]ボックスが開きます。
2. [フロー制御]をクリックします。
3. Catchエラーステップをクリックして、記録されたステップ内の目的の場所にドラッグします。
4. Catchエラーステップを展開し、引数を設定します。詳細については、「["オブジェクトに関連しないステップ引数" ページ293](#)」を参照してください。

オブジェクトが存在することの検証

検証ステップを挿入して、アプリケーションに文字列またはオブジェクトが存在することを検証できます。


検証ステップを挿入するには、次の手順を実行します。

1. [TruClient]サイドバーで、[ステップの追加]アイコン( Step)をクリックします。
[ステップ]ボックスが開きます。
2. [関数]をクリックします。
3. 検証ステップをクリックして、記録されたステップ内の目的の場所にドラッグします。
4. 検証ステップで、[クリックしてオブジェクトを選択]リンクをクリックします。
5. TruClientブラウザで、検証するオブジェクトを選択します。

汎用ステップの挿入

空白または汎用ステップを挿入して、手動で設定できます。

汎用ステップを挿入するには、次の手順を実行します。

1. [TruClient]サイドバーで、[ステップの追加]アイコン( Step)をクリックします。
[ステップ]ボックスが開きます。
2. [関数]をクリックします。

3. **[汎用オブジェクトアクション]**ステップまたは**[汎用ブラウザアクション]**ステップをクリックして、マクロステップ間での目的の場所にドラッグします。


ヒント: 汎用オブジェクトアクションは、オブジェクトに対して指定されていないアクションを実行します。汎用ブラウザアクションは、戻る、リロード、タブを切り替えるなどの不特定のアクションをブラウザで実行します。

4. ステップを展開し、ステップのプロパティを設定します。詳細については、「["オブジェクトに関連しないステップ引数" ページ293](#)」を参照してください。

待機ステップの挿入

待機ステップを実行すると、マクロは指定した時間一時停止してから次のステップに進みます。オブジェクトの待機ステップでは、マクロは指定したオブジェクトがアプリケーションに表示されるのを待った後に、次のステップに進みます。前のステップの終了イベントに達すると、待機ステップが開始されます。つまり、待機ステップに達した後も前のステップは実行し続ける可能性があります。

待機ステップを挿入するには、次の手順を実行します。

1. [TruClient]サイドバーで、**[ステップの追加]**アイコン( Step)をクリックします。
[ステップ]ボックスが開きます。
2. **[関数]**をクリックします。
3. **待機ステップ**または**オブジェクトの待機ステップ**をクリックして、記録されたステップ内の目的の場所にドラッグします。
4. オブジェクトの待機ステップを挿入した場合は、**[クリックしてオブジェクトを選択]**リンクを選択して、アプリケーション内のターゲットオブジェクトを選択します。

マクロのデバッグ

これらのタスクを試して、マクロを対話的にデバッグすることができます。

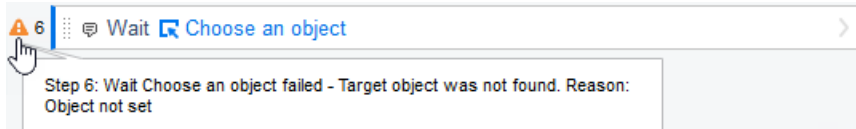
- ["再生エラーの表示" 次のページ](#)
- ["マクロの実行手順" 次のページ](#)
- ["ブレークポイントの使用" 次のページ](#)
- ["ステップレベルの変更" ページ303](#)
- ["待機ステップの挿入" 上](#)
- ["ステップの無効化/有効化" ページ304](#)
- ["ステップをオプションにする" ページ304](#)
- ["ステップの再生" ページ304](#)
- ["ステップからマクロの終わりまで再生する" ページ305](#)

再生エラーの表示

再生中に失敗したステップがある場合は、エラーアイコン(▲)によってマークされます。

エラーの詳細を表示するには、次の方法を実行します。

- エラーアイコンの上にマウスポインタを移動します。
エラーの説明が表示されます。



マクロの実行手順

ステップバイステップ再生では、各ステップの後に再生が一時停止するため、シーケンスをよりゆっくり、コントロールしながら見ることができます。

マクロのステップバイステップを実行するには、次の手順を実行します。

- TruClientサイドバーで、[再生]アイコン(▶)のドロップダウン矢印をクリックし、[ステップバイステップで再生]を選択します。
最初の(または次の)ステップが再生され、再生が停止します。

各ステップの後にこの手順を繰り返して、ステップバイステップで再生を続行します。

ブレークポイントの使用

ブレークポイントは、再生中にマクロの実行を停止するように指示します。マクロのデバッグに役立つブレークポイントを挿入(またはトグルオン)できます。ステップにブレークポイントを挿入した後、マクロはブレークポイントまで再生して一時停止します。この時点で、TruClientブラウザの下部にインスペクタパネルが開きます。その後、ブレークポイントからマクロの再生を続行できます。

注記: Webマクロレコーダは、再生中にマクロが失敗した場合にブレークポイントを自動的に追加します。

ブレークポイントの挿入

ブレークポイントを挿入するには、次の操作を行います。

1. TruClientブラウザで、ブレークポイントを挿入するステップを選択します。
2. ブレークポイントのトグルアイコン(🔍)をクリックします。
ブレークポイントがステップに追加されます。

ブレイクポイントの削除

ブレイクポイントを削除するには、次の操作を行います。

1. TruClientブラウザで、ブレイクポイントが挿入されたステップを選択します。
2. ブレイクポイントのトグルアイコン(☐)をクリックします。

ブレイクポイントがステップから削除されます。

ステップレベルの変更

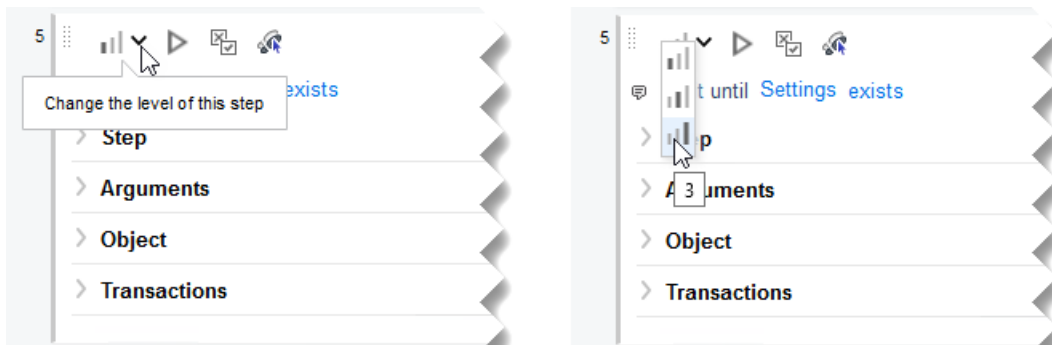
マクロを記録すると、TruClientは各ステップに1から3のレベルを割り当てます。例えば、マクロにはレベル1のステップが不可欠です。影響のないアプリケーションの領域で発生するクリックステップは、レベル2に割り当てられます。マウスオーバーステップは通常、マクロには不要と見なされ、レベル3に割り当てられます。

マクロステップは、TruClientブラウザの上部にあるツールバーのステップレベルスライダでレベル1、2、または3に指定された粒度で表示および再生されます。最も高い粒度はレベル3です。スライダをレベル3に設定すると、レベル1、2、および3ですべてのステップが表示および再生されます。再生に成功するにはより高い粒度を使用する必要がある場合がありますが、それによりマクロの実行に時間がかかる可能性があります。デフォルトでは、スクリプトレベルは1に設定されています。

場合によっては、マクロ全体ではなく、特定のステップのレベルを手動で変更したい場合があります。たとえば、特定のマウスオーバーステップを表示および再生したい場合などです。

ステップのレベルを変更するには、次の手順を実行します。

1. TruClientサイドバーで、ステップを変更するステップエディタアイコン(✎)をクリックします。ステップエディタが開きます。
2. [ステップレベル]ドロップダウン矢印をクリックし、目的のレベルを選択します。



重要! {b}ステップがグループステップの一部である場合、グループステップと個々のステップの両方を変更する必要があります。

ヒント: ステップをグループ化するには、[Ctrl]キーを押しながらクリックして複数のステップを選択し、いずれかのステップを右クリックして、[グループステップ]をクリックします。



参照情報

["マクロ再生レベルの変更" ページ 253](#)

ステップの無効化/有効化

記録したステップを無効にすると、マクロ内に残り、将来的に再有効化できますが、再生はされません。

再生中にマクロステップを無効または有効にするには、次の手順を実行します。



1. TruClient サイドバーで、ステップを変更する **ステップエディタ** アイコン() をクリックします。
ステップエディタが開きます。
2. ステップのツールバーの **[再生中に無効化/有効化]** アイコン() をクリックします。

ヒント: または、1 つ以上のステップを無効または再び有効にするには、Ctrl キーを押しながらクリックしてステップを選択し、ステップの 1 つを右クリックして、コンテキストメニューの **[ステップを無効にする]** または **[ステップを有効にする]** をクリックします。

ステップをオプションにする

いくつかの手順をオプションにできます。オプションのステップは、そのオブジェクトが見つからない場合、再生中にスキップされます。

ステップをオプションにするには、次の手順を実行します。



1. TruClient サイドバーで、ステップを変更する **ステップエディタ** アイコン() をクリックします。
ステップエディタが開きます。
2. ステップツールバーの **[ステップをオプションとして設定]** アイコン() をクリックします。

ヒント: ステップを再びオプションにしない場合は、アイコンを再度クリックします。

ステップの再生

特定のステップを再生して、ステップに記録されたアクティビティを検査できます。

1 つのステップを実行するには、次の操作を行います。

1. TruClient サイドバーで、ステップを変更する **ステップエディタ** アイコン() をクリックします。
ステップエディタが開きます。
2. ステップツールバーの **[このステップのみ再生]** アイコン() をクリックします。

ステップからマクロの終わりまで再生する

特定のステップで再生を開始し、マクロの最後まで再生を続けるには、次の操作を実行します。

1. 再生を開始するステップを選択します。
2. ステップを右クリックし、コンテキストメニューの[このステップから再生]を選択します。

オブジェクト識別問題の解決

動的なWebサイトでは、記録されたオブジェクトは、多くの場合、コンテンツを移動または変更することができます。オブジェクトの識別は、Web 2.0アプリケーションの記録と再生に関する最大の課題の1つです。これらのサイトの動的な性質により、マクロがオブジェクトの検索に失敗する可能性があります。

Webマクロレコーダには、オブジェクトを含むステップ内の**強調表示**、**オブジェクト識別の改善**、**置換**、および**関連オブジェクト**オプションなど、この課題を解決するための高度なメカニズムが含まれています。これらのオプションを使用するには、アプリケーションでオブジェクトを選択する必要があります。マウスオーバーやマウスクリックなど、オブジェクトを表示するためにアプリケーションでさまざまなアクションが必要な場合は、<Ctrl>+<Alt>+<F4>オプションを使用して、オブジェクトが表示されるまでオブジェクト選択モードを一時停止し、再度<Ctrl>+<Alt>+<F4>を押してオブジェクトを選択できます。

ウィンドウに記録されたアプリケーションのオブジェクトを識別する場合は、[ウィンドウ]タブを使用して正しいウィンドウが選択されていることを確認します。


変更のいずれかを実行した後、まずは失敗した問題のステップ1つを再生し、次にマクロ全体を再生します。これにより、発生した問題が変更によって解決されたかどうかを検証できます。

次のトピックでは、オブジェクト識別の問題を解決する方法について説明します。

- ["オブジェクトの強調表示" 次のページ](#)
- ["オブジェクト識別の改善" 次のページ](#)
- ["代替ステップの使用" 次のページ](#)
- ["オブジェクト識別方法の変更" ページ308](#)
- ["マクロタイミングの変更" ページ309](#)
- ["他のオブジェクトへのオブジェクトの関連付け" ページ310](#)
- ["オブジェクトの置き換え" ページ311](#)

オブジェクトの強調表示

ステップで以前に選択したオブジェクトの識別に役立つ情報を表示するには、次の手順を実行します。


1. TruClientサイドバーで、ステップを変更する**ステップエディタ**アイコン()をクリックします。
ステップエディタが開きます。
2. **[オブジェクト]**をクリック(展開)します。
3. **[強調表示]**をクリックして、アプリケーション内のオブジェクトを識別します。
オブジェクトが見つかったと、一時的に点滅ボックスで強調表示されます。
オブジェクトが見つからない場合は、エラーメッセージが表示されます。詳細については、「["オブジェクト識別の改善" 下](#)」を参照してください。

ヒント: このエラーは、時間の調整やタイミングの問題、またはオブジェクトを見つけ出す正しいページが現在表示されていないことを示している可能性があります。

オブジェクト識別の改善

オブジェクトの強調表示に失敗した場合は、オブジェクト識別の改善機能を使用してターゲットオブジェクトを再選択できます。


オブジェクトを再選択するには、次の手順を実行します。

1. 失敗したステップのステップエディタで、**[IDメソッド]**フィールドの横にある**[オブジェクト識別の改善]**アイコン()をクリックします。
Webマクロレコーダは、オブジェクトのプロパティを再学習し、記録中に学習したプロパティと比較します。検出された相違点に基づいて、必要な調整を行うことができます。アプリケーションの動的性によっては、オブジェクト識別の改善機能を複数回使用する必要があります。
2. ステップを再生して、問題が解決されたかどうかを確認します。

代替ステップの使用


代替ステップでは、ステップ内で可能な場合に、同じアクションを実行する複数の方法を表示できます。最適または最も一貫性のあるマクロパフォーマンスのため、またはデバッグ目的でステップを変更できます。

たとえば、ある値によってテキストが変化するリストのオプションをクリックすることができます。テキストに基づいてクリックすると、ステップが失敗する場合があります。リスト内のオプションの順番に基づいてリスト内の項目を選択する代替ステップを使用すると、テキストに関係なくクリックが成功します。

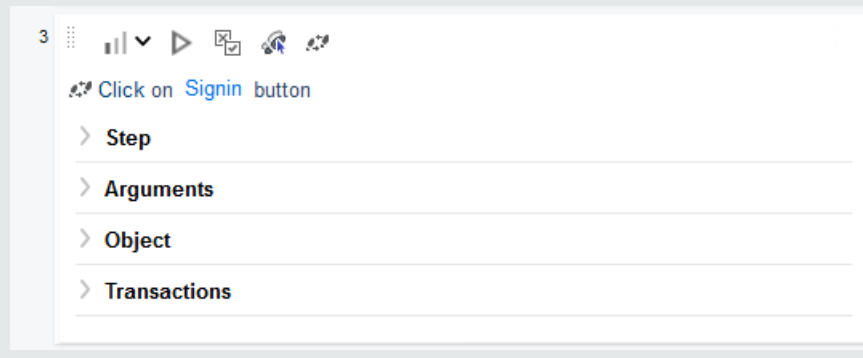
代替オプションを持つステップには、左側に代替ステップアイコン()が表示されます。

代替ステップの表示と選択

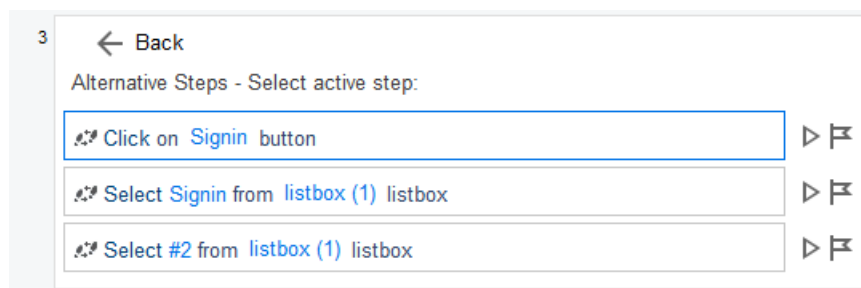
代替ステップを表示して選択するには、次の手順に従います。


1. 代替ステップアイコン()をクリックすると、そのステップの代替オプションが表示されます。

ヒント: ステップエディタが開いている場合は、ステップのツールバーに同じアイコンが表示され、同じ機能を実行します。




代替ステップが表示されます。



2. 次のいずれかを実行します。
 - アプリケーションで代替ステップを表示するには、代替の右側にある[AUTでオブジェクトを強調表示]アイコン()をクリックします。

ヒント: AUTとは、テスト中のアプリケーションを意味します。

これは、「**オブジェクトの強調表示** 前のページ」で説明したのと同じハイライト機能を実行し、マクロステップ内で一度に1つずつ強調表示できるという便利な機能を備えています。


- アプリケーション内で代替ステップを再生するには、代替の右側にある[再生]アイコン()をクリックします。
3. 代替をクリックしてアクティブにします。
 4. ステップエディタに戻る場合は、[戻る]をクリックします。
選択した代替のステップが表示されます。
 5. マクロを再生してテストします。

オブジェクト識別方法の変更

Webマクロレコーダがオブジェクトを識別する方法を変更するには、ステップエディタの[オブジェクト]セクションでオブジェクト識別方法(ID方法)を変更します。

使用可能な方法

次の表は、使用可能なオブジェクト識別方法について説明しています。

メソッド	説明
自動	<p>自動メソッドは、デフォルトであり、推奨されるオブジェクト識別方法です。このメソッドを使用すると、Webマクロレコーダは内部の高度なアルゴリズムを使用してオブジェクトを検索できます。</p> <p>ヒント: 再生中にこの方法でオブジェクトが正常に見つからない場合は、[オブジェクト識別の改善]アイコン()をクリックしてマクロを再び再生します。</p>
XPath	<p>オブジェクト識別や関連オブジェクトの改善機能を使用した後でも、自動識別に失敗した場合は、XPath識別方法を使用してみてください。この方法は、DOMツリー内のオブジェクトを定義するXPath式に基づいてオブジェクトを識別します。たとえば、検索する用語に関係なく最初の検索結果を選択する必要がある場合は、XPath識別を使用すると便利です。</p> <p>ヒント: XPath ID方法の場合、アイコン関数は式の再生成に変わります。このアイコンをクリックすると、インターフェイスでオブジェクトを選択し、関連するXPathを作成できます。</p>
JavaScript	<p>このメソッドは、オブジェクトを返すJavaScriptコードを使用します。たとえば、<code>document.getElementById("SearchButton")</code>は「SearchButton」というDOM ID属性を持つ要素を返します。</p> <p>このメソッドを使用すると、返されたドキュメントを参照するJavaScriptコードを記述できます。CSSセレクタおよび他の標準機能を使用できます。</p> <p>たとえば、サーバから返されたページに、同じ「title」属性(検索結果)を持つ複数のリンクが含まれており、スクリプトに利用可能なリンクの1つをランダムにクリックしてほしいとします。</p> <p>この場合のオブジェクト識別は、JavaScript識別方法を使用して、次のようになります。</p>

メソッド	説明
	<pre>var my_results = document.querySelectorAll('a [title="SearchResult"]'); random(my_results);</pre>
記述子	エディタ内のプロパティによってオブジェクトを識別できます。詳細については、「 https://admhelp.microfocus.com/tc/en/2022-2022-r1/Content/TruClient/descriptors.htm のTruClient記述子」を参照してください。

オブジェクト識別方法の選択

別のオブジェクト識別方法を選択するには、次の方法を実行します。

1. TruClientサイドバーで、ステップを変更する**ステップエディタ**アイコン(🔍)をクリックします。ステップエディタが開きます。
2. **[オブジェクト]**をクリック(展開)します。
3. **[ID方法]**ドロップダウンリストから別の方法を選択します。
4. 次の手順に従います。
 - **[自動]**を選択した場合、手順は完了です。
 - **XPath**を選択した場合、**[ID方法]**リストの下**のXPathテキストボックス**にコードスニペットが表示されます。必要に応じて、**[XPath]**テキストボックスの横にある**ドロップダウン矢印**をクリックし、オブジェクトの推奨XPathコードを選択します。

ヒント: XPathテキストボックスの右側にある**[編集]**アイコン(✎)をクリックすると、XPathエディタが開き、推奨されるXPathコードを編集できます。

- **JavaScript**を選択した場合、**[ID方法]**リストの下**のJavaScriptテキストボックス**にコードスニペットが表示されます。必要に応じて、**[JavaScript]**テキストボックスの右側にある**[編集]**アイコン(✎)をクリックし、JavaScriptエディタを開き、推奨されるJavaScriptコードを編集します。
- **[記述子]**を選択した場合、**[ID方法]**リストの下に**空の記述子テキストボックス**が表示されます。オブジェクトの記述子条件を作成するには、**[編集]**アイコン(✎)をクリックします。詳細については、「<https://admhelp.microfocus.com/tc/en/2022-2022-r1/Content/TruClient/descriptors.htm>のTruClient記述子」を参照してください。

マクロタイミングの変更

タイミングおよび同期の問題でオブジェクトが見つからない場合があります。例えば、マクロがアプリケーション内にあるオブジェクトを探しているのに、マクロの再生が速すぎて、すでに別のページに進んでいる場合などです。タイミングまたは同期の問題でオブジェクトが見つからない

と思われる場合は、待機ステップを挿入できます。詳細については、「["待機ステップの挿入" ページ301](#)」を参照してください。

他のオブジェクトへのオブジェクトの関連付け

他のオプションでオブジェクト識別の問題が解決しない場合は、**[関連オブジェクト]**オプションを使用してしてみてください。

オブジェクトを独自に識別するのが難しくなった場合は、別のより安定性の高いオブジェクトに基づいてオブジェクトにラベル付けできます。たとえば、動的ではないオブジェクトを選択し、ターゲットオブジェクトに「関連付ける」ことができます。関係は視覚的に定義され、他のオブジェクトからの距離(ピクセル単位)に従ってオブジェクトを関連付けます。関係は、オブジェクトごとにIDメソッドごとに定義されます。特定のオブジェクトのIDメソッドに対して複数の関係が定義されている場合、ステップを通過するには、両方の関係で同じオブジェクトを見つける必要があります。

この機能を使用するには、次のコマンドを実行します。

1. 失敗したステップのステップエディタで、**[オブジェクト]**をクリック(展開)します。

注記: **[関連オブジェクト]**オプションは、イベントハンドラエディタの **オブジェクト (Object)** エリアにも表示されます。

2. **[関連オブジェクト]**をクリック(展開)します。

関係テーブルが表示されます。

▼ Related Objects (0)

+ ✎ 🗑️ 🚩 🔍

Anchor Name	Roles
Select Add to add a new relation	

3. **新しい関係を追加** アイコン(+) をクリックします。
[関連オブジェクトの追加]ウィンドウが表示されます。

4. 画面の指示に従って関係を作成します。

アンカーオブジェクトが**[関連オブジェクト]**テーブルに追加されます。

▼ Related Objects (1)

+ ✎ 🗑️ 🚩 🔍

Anchor Name	Roles
Forgot your password ?	link, focusable, element

ヒント

[関連オブジェクト]オプションを使用する場合は、次のヒントに従ってください。

- リソースの負荷が高い場合がありますので、この機能は他の識別方法が失敗した場合にのみ使用してください。


- パフォーマンスを向上させるには、最小検索領域を使用してください。
- 関連オブジェクトは、ウィンドウサイズに依存します。サイズを変更すると、オブジェクトの位置や関係が変わる場合があります。これを考慮に入れてください。
- 各識別方法(自動、XPath、JavaScript、および記述子)には、関連するオブジェクトの独自のセットがあります。これらの関連オブジェクトは、識別方法間では共有されません。
- 複数の関係が存在する場合、識別を成功させるためには、すべての関係を検出する必要があります。

オブジェクトの置き換え

記録中に間違ったオブジェクトを選択した場合、またはオブジェクトが永続的に変更されている場合は、ステップを置き換えることなく、別のオブジェクトに置き換えることができます。これにより、元のステップに加えた変更(関係など)を削除し、ステップを効果的にリセットできます。

[置換]オプションを使用すると、現在ステップで参照されているオブジェクトが正しくないことがマクロレコーダに指示されます。マクロレコーダは、オブジェクトに関する現在の知識をすべて削除し、選択したオブジェクトを学習します。したがって、記録中に間違ったオブジェクトを使用した場合にのみ、[置換]オプションを使用する必要があります。

オブジェクトを置き換えるには、次の手順を実行します。


1. TruClientサイドバーで、ステップを変更する**ステップエディタアイコン**()をクリックします。
ステップエディタが開きます。
2. **[オブジェクト]**をクリック(展開)します。
3. **[置換]**をクリックします。
4. 新しいオブジェクトを選択します。
5. マクロを再生します。

設定の構成

ブラウザ設定と対話型設定は、TruClient一般設定で行います。

TruClient一般設定へのアクセス

一般設定にアクセスするには、次の方法を実行します。

1. TruClientサイドバーで、**[一般設定]アイコン**()をクリックします。
TruClient一般設定ウィンドウが表示されます。
2. 次のトピックの説明に従って設定を行います。
 - ["ブラウザ設定" 次のページ](#)
 - ["対話型オプション" ページ316](#)

- ["2要素認証" ページ317](#)
- ["証明書の設定" ページ325](#)

3. [完了]をクリックして設定を保存し、TruClient一般設定ウィンドウを閉じます。

ブラウザ設定

次の表は、[ブラウザ設定]タブのオプションについて説明しています。

設定	説明
ユーザエージェント - HTTPヘッダ	<p>ブラウザのユーザエージェント文字列を指定します。OpenText DASTとイベントベースのWebマクロレコーダの両方で同期するユーザエージェント設定を行えます。</p> <div><p>注記: スキャンウィザード内からイベントベースのWebマクロレコーダを開く場合、ユーザエージェントはOpenText DASTのアプリケーション設定から事前入力されます。OpenText DASTの [ツール(Tools)] メニューまたはWindowsの [スタート] メニューからイベントベースのWebマクロレコーダをスタンドアロンツールとして開く場合、ユーザエージェントフィールドが空になる場合があります。この場合、デフォルトのブラウザ値が使用されます。</p></div> <p>次のリストはサンプル値を示していますが、完全ではありません。</p> <p>デフォルト (Default)</p> <p>Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0</p> <p>Internet Explorer 6</p> <p>Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)</p> <p>Internet Explorer 7</p> <p>Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)</p> <p>Internet Explorer 8</p> <p>Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB5; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; InfoPath.2; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)</p>

設定	説明
	<p>Googlebot 2.1</p> <p>Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)</p> <p>Bingbot</p> <p>Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)</p> <p>Yahoo! Slurp Slurp</p> <p>Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)</p> <p>iPhone、iOS 14.3</p> <p>Mozilla/5.0 (iPhone; CPU iPhone OS 14_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.2 Mobile/15E148 Safari/604.1</p> <p>重要! {b}カスタムユーザエージェント文字列も使用できます。ただし、OpenTextでは、カスタムユーザエージェント文字列は上級ユーザのみ使用することを推奨します。</p>
<p>ユーザエージェント - ナビゲータインタフェース</p>	<p>これらの設定は、レガシーWebアプリケーションがブラウザの検出を容易にするために使用する情報を提供します。ブラウザ固有の動作が必要な場合は、これらの設定をカスタマイズできます。</p> <ul style="list-style-type: none"> • appName - すべてのブラウザが、このプロパティの値として「Netscape」を返します。 • appVersion - ブラウザは「4.0」またはブラウザに関するバージョン情報を表す文字列を返します。 • platform - ブラウザは空の文字列またはブラウザが実行されているプラットフォームを表す文字列を返します。 <p>例:</p> <p>MacIntel、Win32、Win64、iPhone</p>
<p>キープアライブタイムアウト値のカスタマイズ</p>	<p>チェックボックスを選択してこの設定を有効にする場合は、次の項目を構成します。</p> <ul style="list-style-type: none"> • キープアライブタイムアウト(ミリ秒) - アイドル状態の接続を開いた状態に保つタイムアウト(ミリ秒)を指定します。この設定

設定	説明
	は、直接接続とプロキシ接続の両方に適用されます。
一時インターネットファイル	<p>ブラウザは、Webページ、イメージ、メディアのコピーを保存し、後で素早く閲覧できるようにします。保存されたページの新しいバージョンのチェックを設定して、ブラウザがリソース(キャッシュ)のローカルコピーをWebサーバと比較する場合を決定します。オプションは次のとおりです。</p> <ul style="list-style-type: none"> • Webページにアクセスする度 - ブラウザは要求ごとにリソースをチェックし、最後に表示した後にページが変更されたかどうかを確認します。ページが変更されている場合は、ブラウザに新しいページが表示され、一時インターネットファイルフォルダに保存されます。 • ブラウザを起動する度 - ブラウザは、ブラウザの起動時にリソースをチェックします。同じブラウザセッションで以前にアクセスしたWebサイトを表示すると、ブラウザはページをダウンロードする代わりに、キャッシュされた一時インターネットファイルを使用します。 • 自動 - ブラウザは、以前のセッションまたは以前の日付に表示したページに戻った場合にのみ、新しいコンテンツをチェックします。時間の経過とともに、ページ上のイメージの変更頻度が低いとブラウザが判断した場合、新しいイメージをチェックする頻度がより低くなります。 • 実行しない - ブラウザはWebサーバで新しいコンテンツをチェックしません。
Proxy	<p>プロキシ設定を指定します。オプションは次のとおりです。</p> <ul style="list-style-type: none"> • 直接接続(プロキシ無効) - プロキシ接続なしで要求を行います。 • プロキシ設定の自動検出 - WPAD (Web Proxy Autodiscovery Protocol)を使用してプロキシ自動設定ファイルを見つけて使用し、ブラウザのWebプロキシ設定を構成します。 • システムプロキシ設定を使用する - ローカルコンピュータからプロキシサーバ情報をインポートします。 <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p>注記: システムプロキシ設定は、Macバージョンではサポートされていません。</p> </div> <ul style="list-style-type: none"> • PACファイルを使用してプロキシ設定をする - [URL]フィールド

設定	説明
	<p>ドで指定した場所のPAC (Proxy Automatic Configuration) ファイルからプロキシ設定をロードします。</p> <ul style="list-style-type: none"> • プロキシ設定を明示的に設定する - プロキシサーバを介してインターネットにアクセスします。次のサーバ情報を提供します。 <ul style="list-style-type: none"> • サーバ - プロキシサーバのURLまたはIPアドレスを入力します。 • ポート - ポート番号を入力します(たとえば、8080)。 • タイプ - プロキシサーバ経由のTCPトラフィックを処理するプロトコルタイプを選択します。オプションは、Standard、SOCKS4、またはSOCKS5です。 • 認証 - 認証が必要な場合は、認証リストからタイプを選択します。オプションは、なし、基本、NTLM、ダイジェスト、自動、Kerberos、またはネゴシエートです。 <div data-bbox="646 926 1403 1020" style="background-color: #f0f0f0; padding: 5px;"> <p>注記: Kerberosは、Windowsバージョンでのみサポートされています。</p> </div> • ユーザ名 - プロキシサーバで認証が必要な場合は、適切なユーザ名を入力します。 • パスワード - プロキシサーバで認証が必要な場合は、適切なパスワードを入力します。 • プロキシをバイパスする - プロキシサーバを使用して特定のIPアドレス(内部テストサイトなど)にアクセスする必要がない場合は、[プロキシをバイパスする]フィールドにアドレスまたはURLを入力します。エントリを区切る場合は、カンマを使用します。
ネットワーク認証	<p>サーバまたはフォームで認証が必要な場合に使用する認証の詳細を指定します。設定は次のとおりです。</p> <ul style="list-style-type: none"> • 認証(Authentication) - 認証(Authentication) リストからタイプを選択します。オプションは、なし(None)、基本(Basic)、NTLM、ダイジェスト(Digest)、自動(Automatic)、Kerberos、ネゴシエート(Negotiate)、ADFS CBTです。 <div data-bbox="646 1780 1403 1875" style="background-color: #f0f0f0; padding: 5px;"> <p>注記: Kerberosは、Windowsバージョンでのみサポートされています。</p> </div>

設定	説明
	<ul style="list-style-type: none">• ユーザ名 (Username) - 適格なユーザ名を入力します。• パスワード (Password) - 適格なパスワードを入力します。

対話型オプション

次の表は、[対話型オプション]タブの設定について説明しています。

設定	説明
Webmacroファイル暗号化を有効にする	<p>保存時にマクロファイル全体を暗号化します。それ以外の場合、ファイルはプレーンテキストで保存され、ユーザ名とパスワードが表示されます。このオプションはデフォルトで選択(オン)されています。</p> <p>注記: このオプションが選択されていない場合でも、暗号化されたマクロを開くことができます。また、Firefox 30でWebマクロレコーダを使用して記録された暗号化マクロを開くこともできます。</p>
最後のステップを検証ステップに強制する	<p>ログインマクロの最後のステップを検証ステップに強制的に設定します。記録されたマクロが正常に再生されると、ログイン検証に使用するオブジェクトを選択するように求めるメッセージが表示されます。オブジェクトを選択しない場合、オブジェクトの選択またはマクロの破棄を求めるプロンプトが表示され、この設定が強制されます。</p> <p>このオプションはデフォルトで選択(オン)されています。アプリケーションがログイン検証にオブジェクトを使用しない場合は、この設定を無効にします。</p>
Webストレージのサポート	<p>Webストレージの検出を有効にします。このオプションを有効にすると、Webストレージのカスタムキーを作成および管理できます。さらに、事前定義されたイベントベースのログアウト条件テンプレートが、ログアウト条件エディタで使用できるようになります。</p> <p>詳細については、「"Webストレージキーの使用" ページ269」および「"ログアウト条件の使用" ページ259」を参照してください。</p>
エラー時のアクション	<p>再生中にエラーが発生した場合にTruClientが実行するアクションを指定します。オプションは次のとおりです。</p>

設定	説明
	<ul style="list-style-type: none"> • スクリプトの中止 - エラー時にスクリプトを中止します。 • 次の繰り返しの進む - エラー時の繰り返しを停止し、次の繰り返しの進むに進みます。 • 次のステップに進む - エラー時に、次のステップに進みます。
スナップショットの生成	サポートされていません。
ステップの生成	<p>ステップ生成の設定を行います。デフォルトの識別方法の設定オプションは次のとおりです。</p> <ul style="list-style-type: none"> • サーバをパラメータで置き換える - サーバ名をナビゲーションステップのパラメータで置き換えます。 • 該当する場合に代替ステップを作成する - (該当する場合) 代替ステップを作成するかどうかを指定します。 • 記録中にレベル2またはレベル3のステップを作成する - レベル2またはレベル3でステップを作成するかどうかを指定します。
デバッグ	<p>デバッグ設定は、デバッグ以外の再生には適用されません。オプションは次のとおりです。</p> <ul style="list-style-type: none"> • オブジェクト識別アシスタントを有効にする - オブジェクト識別アシスタントを有効にします。 • 待機ステップを無視する - 待機ステップを無視してスクリプトのデバッグを迅速化します。 • インスペクタパネルを非表示にする - スクリプトがブレークポイントに達した場合は、インスペクタパネルを非表示にします。 • インスペクタペインに自動的に入力する - ユーザ定義データをインスペクタパネルに自動的にロードします。このオプションは、coded-actionデバッグには適用されません。

2要素認証

重要! 2要素認証コントロールセンターとモバイルアプリケーションの設定は、イベントベースのWebマクロレコーダのスタンドアロンインスタンスにのみ適用されます。スキャンで使用する前にローカルでテストすることを目的にしています。

「ユーザが持っているもの」の2要素認証には、アプリケーションサーバがWebアプリケーションへのログイン時にSMSまたは電子メール応答をユーザに送信する必要があります。スキャンで2要素認証を使用するには、Node.jsサーバをアプリケーションサーバから受信したSMSおよび電子メール応答を処理するコントロールセンターとして設定する必要があります。

注記: 固有のID一覧 (UIDL) をサポートするPOP3サーバのみがサポートされます。

2要素認証コントロールセンター

2要素認証コントロールセンターを設定するには、次の操作を行います。

1. [ローカルIPアドレス] ドロップダウンリストで、IPアドレスを選択します。

注記: これらのIPアドレスは、イベントベースのWebマクロレコーダがインストールされているコンピュータで使用できます。

2. 次のいずれかを実行します。

- 特定のポートを使用するには、[ポート] リストからポートを選択します。
- Webマクロレコーダでポートを選択するには、[ポートを自動的に割り当てる] チェックボックスを選択します。

重要! {/b} モバイルアプリケーションがサーバにアクセスするには、コントロールセンターのポートをファイアウォールで公開する必要があります。

3. [初期化] をクリックします。
コントロールセンターが起動します。

モバイルアプリケーション

アプリケーションサーバがSMS応答を送信する場合は、**Fortify2FA** モバイルアプリケーションをインストールし、2要素認証設定をダウンロードする必要があります。設定後、モバイルアプリケーションはSMS応答を受信し、コントロールセンターに転送します。

注記: 現在、モバイルアプリケーションはAndroid OSでのみ使用できます。

モバイルアプリケーションを設定するには、次の手順を実行します。

1. [電話番号] ボックスに、SMS応答を受信する電話番号を入力します。
2. [QRコードの生成] をクリックします。
コントロールセンターは、2要素認証設定とモバイルアプリケーションをダウンロードするリンクを含むクイックレスポンス (QR) コードを生成します。
3. モバイルアプリケーションをインストールして設定します。詳細については、「["Fortify2FAモバイルアプリのインストールと設定" 次のページ](#)」を参照してください。

ヒント: スキャンで複数のスレッドを使用する場合は、複数の電話を使用することをお勧めします。マルチユーザスキャンに同じ電話番号を使用すると、スキャン時間に影響する場合があります。

4. (オプション) 別の電話用にモバイルアプリケーションを設定するには、手順1~3を繰り返します。

Fortify2FAモバイルアプリのインストールと設定

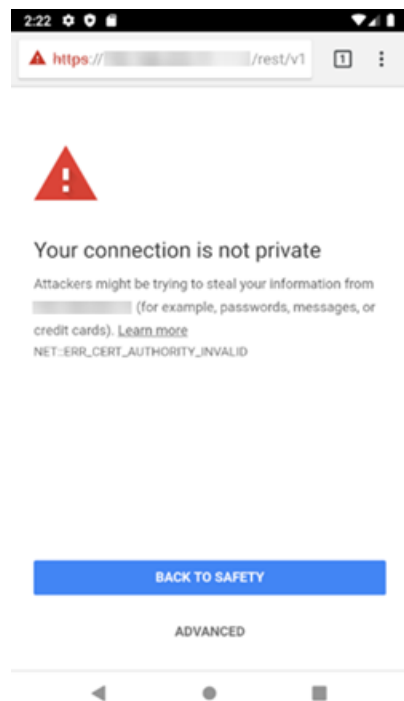
SMS応答を受信する電話にモバイルアプリケーションをインストールして設定するには、次の手順を実行します。

1. 携帯電話のカメラまたはQRコードスキャナを使用して、2要素認証モバイルアプリケーション設定のQRコードをスキャンします。

リンクが表示されます。

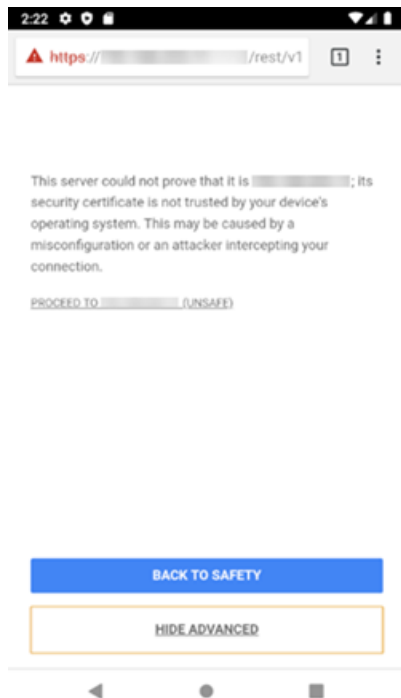
2. リンク(または[開く]ボタン)をクリックして、アプリをダウンロードするためのサイトにアクセスします。

自己署名証明書に関する警告が表示されます。

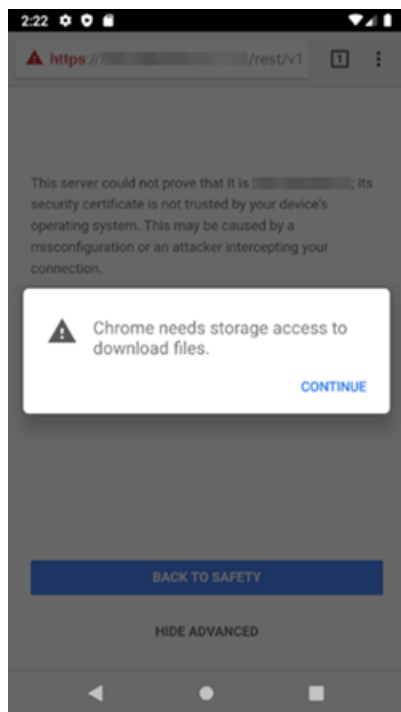


3. [詳細]をクリックします。

次に進むためのリンクと共に追加情報が表示されます。

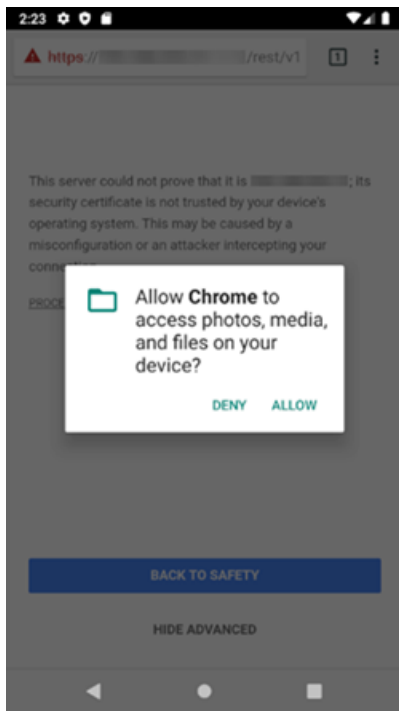


4. [**<ip_address>**に**続行する (安全でない)**]をクリックします。
ダウンロードファイルへのストレージアクセスを要求するプロンプトが表示されます。

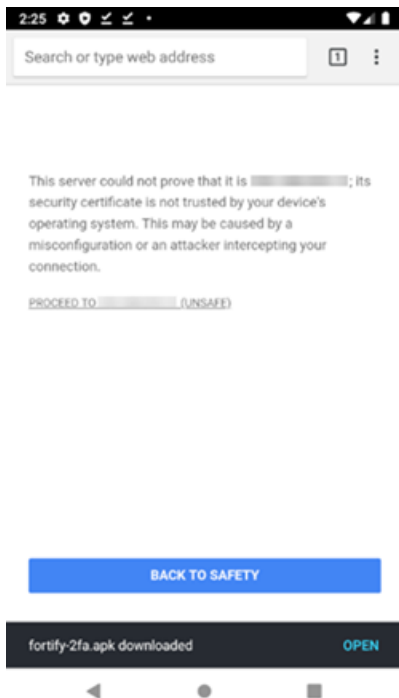


5. [**次へ**]をクリックします。

プロンプトがデバイス上の写真、メディア、およびファイルへのアクセスを要求します。

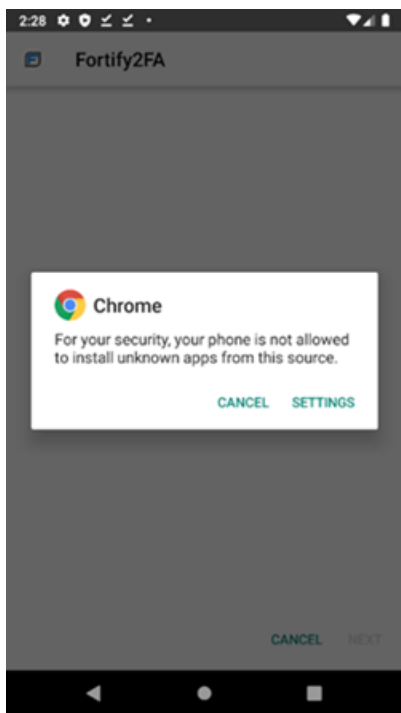


6. [許可]をクリックします。
fortify-2fa.apkファイルがダウンロードされます。

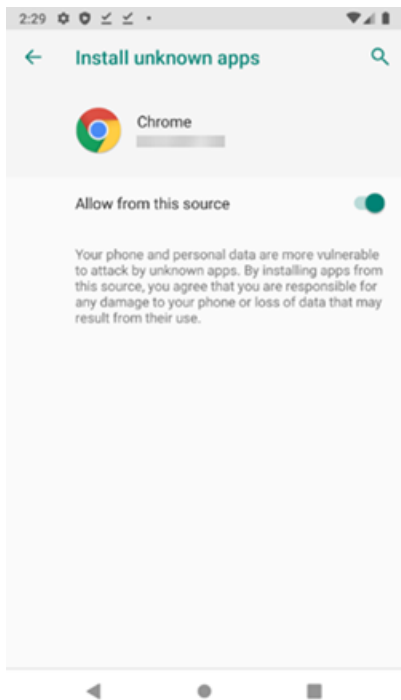


7. [開く]をクリックします。

不明なアプリのインストールについてプロンプトが表示されます。

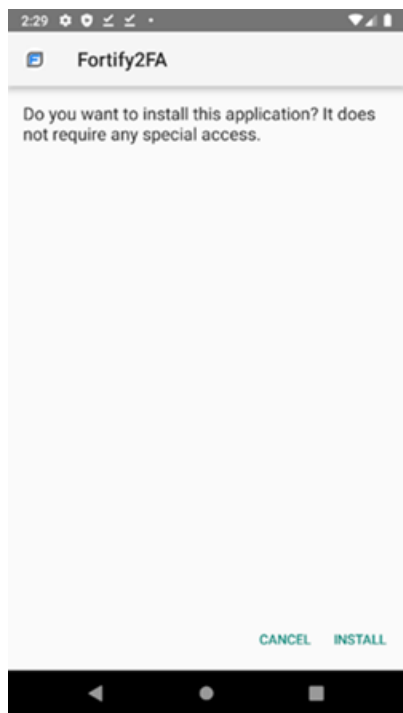


8. [設定]をクリックします。
[不明なアプリのインストール]設定が表示されます。

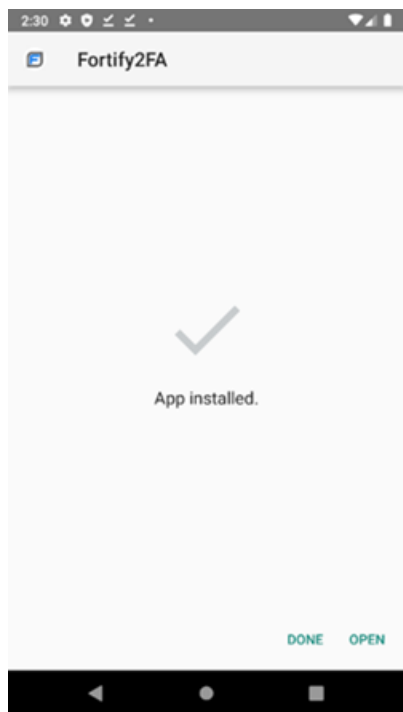


9. [このソースから許可]を有効にする。

アプリケーションをインストールするかどうかを確認するプロンプトが表示されます。

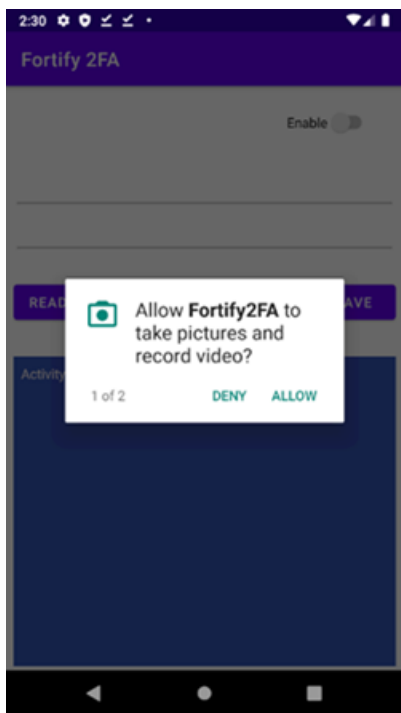


10. [インストール]をクリックします。
アプリがインストールされていることを示すメッセージが表示されます。

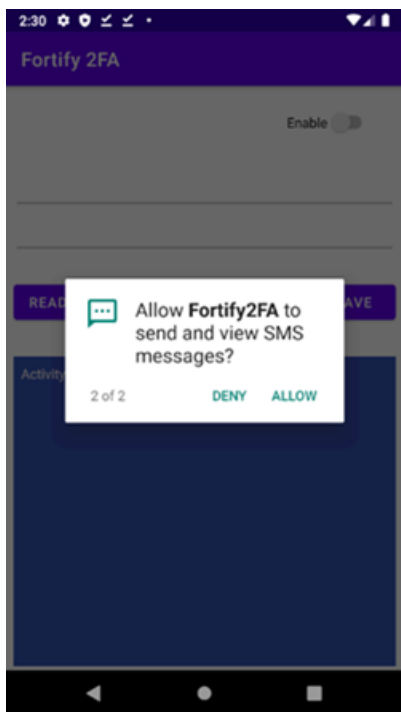


11. [開く]をクリックします。

写真やビデオ撮影の許可を要求するプロンプトが表示されます。

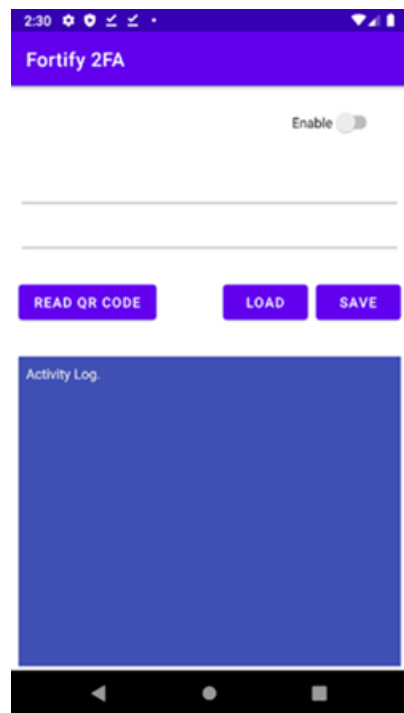


12. [許可]をクリックします。
SMSメッセージの送信と閲覧の許可を要求するプロンプトが表示されます。



13. [許可]をクリックします。

アプリを設定する準備が整いました。



14. [QRコードの読み込み]をクリックして、2要素認証モバイルアプリケーション設定のQRコードをスキャンします。
2要素認証設定は、Fortify2FAモバイルアプリケーションで設定されます。

証明書の設定

ブラウザ設定 (Browser Settings)] タブと **インタラクティブオプション (Interactive Options)]** タブ (Macバージョンの場合は **カスタムキーチェーン (Custom Keychains)]** タブ) には **証明書 (Certificates)]** ボタンがあります。このボタンを使用すると、ローカルストアからWebマクロレコーダ設定に証明書をインポートしてスキャンの際に使用できます。たとえば、信頼されていない証明書を使用するQA環境がターゲットアプリケーションである場合、信頼されていない証明書をローカルストアに追加して、Webマクロレコーダ設定にインポートできます。

Webマクロレコーダの設定で証明書を設定すると、証明書はマクロの一部としてパッケージ化され、スキャン中にサーバがクライアント証明書を要求したときに提供されます。

重要! {b}記録中に、クライアント証明書を必要とするサーバに移動すると、[ruClient] サイドバーウィンドウにダイアログが表示され、次のプロンプトが表示されます。

「サイト <ホスト> がクライアント証明書を要求しています。今すぐ設定しますか? (The site <host> is requesting a client certificate. Would you like to configure one now?)」

OpenTextでは、**[はい (Yes)]** をクリックして証明書を設定することを推奨します。プロンプトは1回だけ表示され、**[いいえ (No)]** をクリックすると、次のマクロ操作時に証明書を手動で設定する必要があります。証明書が設定されていない場合、スキャン中のマクロ再生が失敗することがあります。

Macにカスタムキーチェーンを追加

macOSでは、カスタムキーチェーンを証明書ストア名として追加できます。

カスタムキーチェーンを追加するには、次の操作を行います。

1. **カスタムキーチェーン(Custom Keychains)]** タブで **+** をクリックします。
2. 空のフィールドにキーチェーン名を入力します。
3. **完了(Done)]** をクリックします。
このストア名から、「**証明書の設定" 下**」の説明に従って証明書を設定できます。

証明書の設定

証明書を設定するには、次の操作を行います。

1. **TruClient一般設定(TruClient General Settings)]** で、 **証明書(Certificates)]** をクリックします。
証明書設定(Certificates Configuration)] ダイアログが開きます。
2. **証明書ストア]** エリアで、次のいずれかを選択します。
 - **ローカルマシン(Local Machine)]** - この証明書ストアはコンピュータにローカルに適用され、このコンピュータのすべてのユーザに対してグローバルに適用されます。
 - **現在のユーザ(Current User)]** - この証明書ストアはこのコンピュータのユーザアカウントにローカルに適用されます。
3. **証明書(Certificate)]** 領域で、マクロに追加する証明書を選択します。
4. **OK]** をクリックします。

イベントベースのWebマクロレコーダのアンインストール

WindowsでOpenText DASTをアンインストールすると、OpenText DASTツールキットの一部としてインストールされたイベントベースのWebマクロレコーダが自動的にアンインストールされます。Windowsオペレーティングシステム上のスタンドアロンバージョンをアンインストールすることもできます。

Windowsバージョンをアンインストールするには:

1. **コントロールパネル]** で、 **プログラム> プログラムと機能]** の順に移動します。
2. プログラムのリストで、 **OpenText DASTマクロレコーダ<バージョン>(OpenText DAST Macro Recorder <version>)]** を選択します。
3. **アンインストール]** をクリックします。
アンインストールを確認するメッセージが表示されます。
4. **はい]** をクリックして確認します。

MacでのWebマクロレコーダのクリーンアップまたはアンインストール

破損したファイルや確認メッセージのために、Webマクロレコーダが正常に動作しなくなる場合があります。macOSのメニューバーにある [トラブルシュート] メニューオプションを使用すると、Webマクロレコーダのインストールをクリーンアップして更新できます。Webマクロレコーダをアンインストールすることもできます。

[トラブルシュート] メニューの使用

[トラブルシュート] メニューを使用するには:

1. macOSのメニューバーで、**[Troubleshoot]** をクリックします。
2. 次のいずれかのメニューオプションを選択します。
 - **Clean Application State** - Webマクロレコーダの起動ツールとそのウィジェットのアプリケーション状態をクリーンアップします。
 - **Erase All Settings** - 設定の問題を修正するために、すべての設定を消去します。
 - **Erase TruClientBrowser Executable** - TruClientBrowser実行可能ファイルを消去してから再インストールし、インストールの問題を修正します。
 - **Uninstall** - Webマクロレコーダとそのすべてのデータをシステムから削除します。
3. Webマクロレコーダをアンインストールする場合は、次の手順に従って、アプリケーションとそのファイルおよびコンテナを完全に削除します。
 - a. DAST Webマクロレコーダのアンインストールメイン画面で、**[Configure All Files Access]** をクリックします。
[Full Disk Access] ダイアログが開きます。
 - b. **[+]** をクリックしてパスワードを入力します。
 - c. **[Applications]** リストから**MacroRecorder.app**を選択して、**[Open]** をクリックします。
メッセージプロンプトが表示されます。
 - d. **[Quit & Reopen]** をクリックします。
Webマクロレコーダが閉じて再度開きます。
 - e. macOSのメニューバーで、**[Troubleshoot]** > **[Uninstall]** の順にクリックします。
 - f. **[Continue]** をクリックします。
 - g. パスワードを入力し、**[OK]** をクリックします。
DAST Webマクロレコーダのアンインストールメイン画面に進行状況が表示されます。
 - h. 完了したら、**[Done]** をクリックします。

第19章:Web Proxy




Web Proxyはスタンドアロンの自己完結型プロキシサーバであり、デスクトップ上で設定および実行できます。これを使用すると、サーバとの間でHTTP要求の送信と応答の受信を行うスキャナ、ブラウザ、または他のツールからのトラフィックを監視できます。このツールは、デバッグと侵入評価を行うツールです。サイトのブラウズ中に、すべての要求とサーバ応答を表示できます。

OpenText DASTで使用可能なワークフローマクロまたはログインマクロを作成できます。

ヒント: Burp ProxyファイルのセットまたはHTTPアーカイブ(HAR)ファイルからワークフローマクロを作成できます。詳細については、「["Webマクロの作成" ページ344](#)」を参照してください。

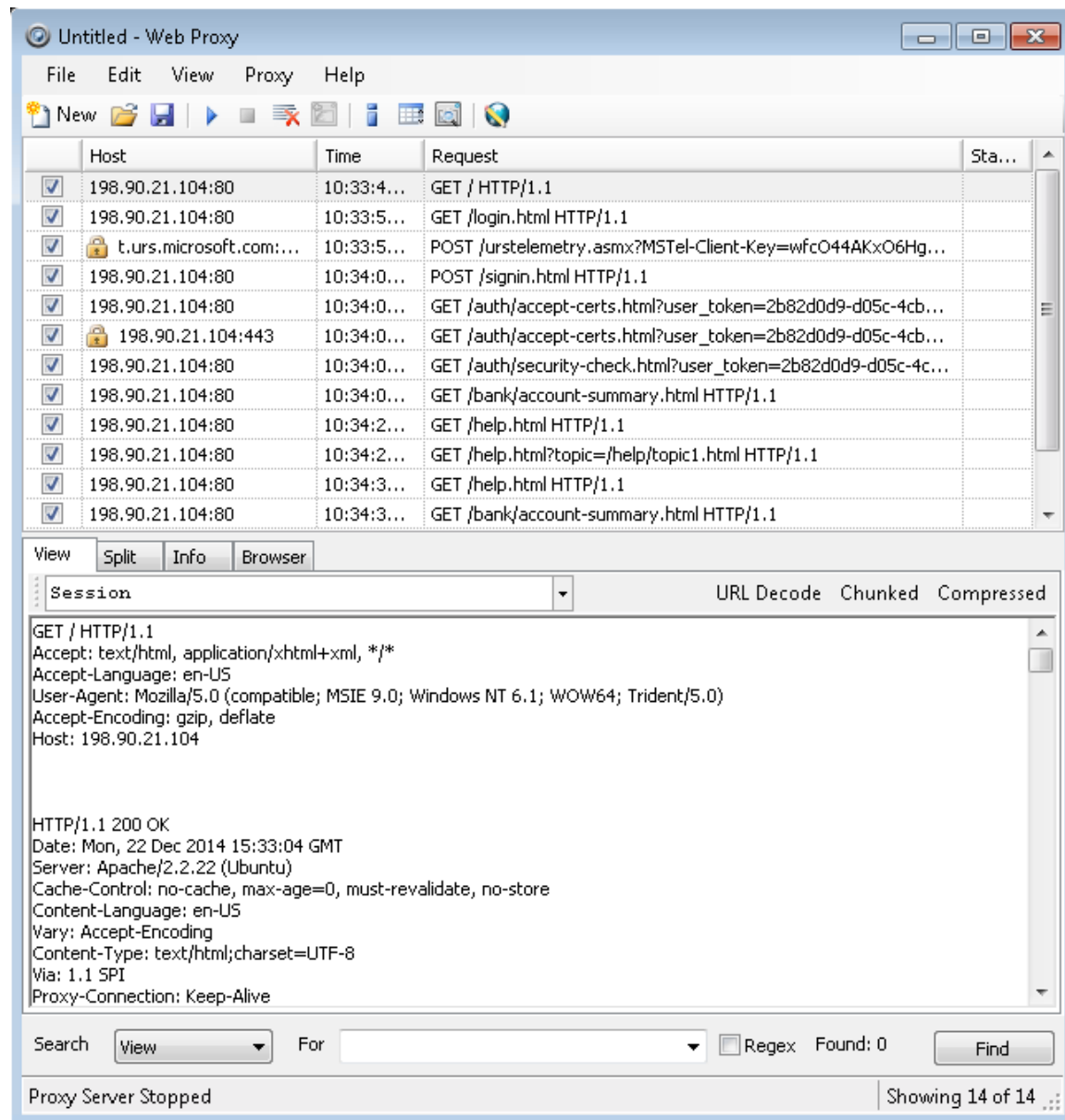
Web Proxyの使用

ブラウザでWeb Proxyを使用するには:

1. **ツール(Tools)] > [Web Proxy]**をクリックします。
Web Proxyウィンドウが開きます。
2. **開始(Start)]** をクリックします(または **プロキシ(Proxy)]** メニューから **開始(Start)]** を選択します)。
Web Proxyステータスバーに、「<サーバ:ポート 番号>でリスン中 (Listening on <server:port number>)」と表示されます。
3. **ブラウザの起動(Launch Browser)]** をクリックします。
これにより、Webブラウザが起動し、Web Proxy経由で通信を行うように設定されます。または、別のブラウザを使用する場合の設定手順については、「["ブラウザの手動設定" ページ349](#)」を参照してください。
4. 要求/応答をキャプチャするサイトを手動で操作します。
5. Web ProxyがWebサーバから証明書の要求を受け取った場合、証明書の特定を求めるダイアログボックスが表示されます。次に、プログラムは選択内容を「サーバ単位」でキャッシュします。したがって、その後、特定のサーバに対して別の証明書を使用する場合は、Web Proxyを停止してから再起動し、キャッシュをクリアする必要があります。
6. 必要なすべてのページを閲覧した後、Web Proxyに戻り、をクリックします(または、**プロキシ(Proxy)]** メニューから **停止(Stop)]** を選択します)。

Web Proxyのイメージ

次のイメージは停止した後のWeb Proxyを示しています。



7. メッセージの表示形式を変更するには、タブ(表示(View))、分割(Split)、情報(Info)、または ブラウザ(Browser))のいずれかを選択します。

表示(View)]タブまたは **分割(Split)]**タブを使用する場合は、**URLデコード(URL Decode)]**ボタンを選択して、要求と応答のURLデコードを有効または無効にできます。ほとんどのOpenText DAST攻撃トラフィックはURLでエンコードされているため、この機能を使用すると、HTTPメッセージの分析が容易になります。説明のために、同じGET要求の次のURLエンコードバージョンとデコードバージョンを比較します。

- GET
/notes.asp?noteid=1%20union%20%20select%20%2c1%2c2%20from%20information_schema.tables%20order%20by%204%20desc%20limit%201 HTTP/1.1
- GET /notes.asp?noteid=1 union select 0,1,2 from information_schema.tables order by 4 desc limit 1 HTTP/1.1

応答がチャンクエンコードまたは圧縮されている場合は、**チャンク(Chunked)]**ボタンと**圧縮(Compressed)]**ボタンが有効になります。この機能により、Web Proxyが受信した元の応答のほか、チャンク解除された応答または解凍された応答を表示できます。

8. 要求を(編集ありまたは編集なしで)再送信するには、表示されているセッションのリストから要求を選択し、HTTP Editorアイコンをクリックします(または、要求を右クリックし、コンテキストメニューから **HTTP Editor]**を選択します)。
9. リストからセッションをクリアするには、1つ以上のセッションを選択して<Delete>キーを押します(または、**編集(Edit)]> 選択をクリアする(Clear Selected)]**をクリックします)。すべてのセッションをクリアするには、**編集(Edit)]> すべてクリア(Clear All)]**をクリックします。

注記: Web Proxyのリストからセッションをクリアすると、そのセッションはキャプチャされたデータからも削除されます。たとえば、リストに100のセッションが含まれていて、そのうち98をクリアした後でセッションをファイルに保存した場合、残りの2つのセッションだけが含まれます。セッションをクリアする場合は、チェックボックスを無視してください。

ファイル(File)]メニューを使用して、選択した要求をトラフィックセッションファイル(.tsf)に保存し、後で分析用にロードします(**ファイル(File)]> 開く(Open)]**コマンドを使用)。また、一連の要求をWebマクロとして保存し、OpenText DASTスキャンを実行するときにも使用することもできます。すべての **ファイル(File)]**メニューコマンドは、「チェックマーク付き」要求に適用されます。

セッションの保存

後で分析するために1つ以上のセッションを保存するには:

1. 左側の列にチェックマークを付けて、保存するセッションを選択します。
2. **ファイル(File)]**メニューをクリックして、**保存(Save)]**または **名前を付けて保存(Save As)]**を選択します。
3. **ファイル名(File name)]**ボックスに名前を入力し、**保存(Save)]**をクリックします。

セッションのクリア


Web Proxyのリストからセッションをクリアすると、そのセッションはキャプチャされたデータからも削除されます。たとえば、リストに100のセッションが含まれていて、そのうち98をクリアした後にセッションをファイルに保存した場合、残りの2つのセッションだけが含まれます。

1つ以上のセッションをクリアするには:

1. セッションを選択します。複数のセッションの場合は、<Ctrl>キーまたは<Shift>キーを使用します。

注記: メモ: セッションをクリアする場合は、チェックボックスを無視してください。

2. 次のいずれかを実行します。
 - <Delete>キーを押します。
 - **編集(Edit)] > 選択をクリア(Clear Selected)]**をクリックします。

すべてのセッションをクリアするには、をクリックします(または、**編集(Edit)] > すべてクリア(Clear All)]**をクリックします)。

メッセージの検索

Web Proxyウィンドウの下部にあるコントロールを使用して、**表示(View)]**タブ、**分割(Split)]**タブ、または**情報(Info)]**タブに表示されるメッセージ内の情報を検索できます。

メッセージを検索するには:


1. **検索(Search)]**リストから、検索するタブを選択します。
2. **検索データ(For)]**ボックスに、検索するテキスト(またはテキストを表す正規表現)を入力します。
3. ステップ2で正規表現を入力した場合は、**正規表現(Regex)]**チェックボックスをオンにします。
4. **Find]**をクリックします。

注記: 上記の手順を使用して手動で検索しないで済むように、各セッションで情報を検索するルールを作成することもできます。「["設定: 検索と置換" ページ339](#)」および「["設定: フラグ" ページ340](#)」を参照してください。

すべてのメッセージの検索

すべてのセッションで特定の情報を検索できます。


すべてのメッセージを検索するには:

1. ツールバーの **検索ビューの切り替え(Toggle Search View)]** ボタンをクリックします(または **表示(View)]**メニューから **検索(Search)]**を選択します)。
2. **検索エリア(Search Area)]**リストを使用して、すべてのセッションの内容全体を検索するか、特定のセグメントに限定して検索するか指定します。
3. **検索データ(Search For)]**ボックスに、検索するテキストを表す正規表現を入力します。
4. **検索(Search)]**をクリックします。

注記: 上記の手順を使用して手動で検索しないで済むように、各セッションで情報を検索するルールを作成することもできます。「["設定: 検索と置換" ページ339](#)」および「["設定: フラグ" ページ340](#)」を参照してください。

オプションの変更

Web Proxyオプションを変更するには:

1. Web Proxyがリスンしている場合は、次のいずれかを実行します。
 - **プロキシ(Proxy)]**メニューをクリックし、**停止(Stop)]**を選択します。
 - ツールバーのをクリックします。
2. **編集(Edit)]> 設定(Settings)]**をクリックし、**プロキシサーバ(Proxy Servers)]**タブを選択します。

詳細については、「["設定: プロキシサーバ" ページ336](#)」を参照してください。

Web Proxyのタブ

各HTTPセッション(1つの要求と、それに関連する応答)が、Web Proxyの上部ペインに一覧表示されます。セッションを選択すると、Web Proxyの下部ペインにそのセッションに関する情報が表示されます。表示される情報は、選択するタブによって異なります。

ステータスバーのすぐ上にあるコントロールを使用して、これらのタブで特定のコンテンツを検索できます。

表示(View)

表示(View)]タブを使用して、検査するHTTPメッセージを選択します。タブ直下のドロップダウンリストから使用できるオプションは次のとおりです。

- セッション(Session): 完全なセッション(要求と応答の両方)を表示します
- ブラウザからWeb Proxyへの要求(Request from browser to Web Proxy): ブラウザがWeb Proxyに対して行った要求のみを表示します

- Web Proxyからサーバへの要求 (Request to server from Web Proxy): サーバへのWeb Proxy要求のみを表示します
- サーバからWeb Proxyへの応答 (Response from server to Web Proxy): Web Proxyに対するサーバ応答のみを表示します
- Web Proxyからブラウザへの応答 (Response to browser from Web Proxy): ブラウザに対するWeb Proxy応答のみを表示します

分割(Split)

分割(Split)] タブをクリックして、1つのセッションに2つの情報エリアを作成します。たとえば、ブラウザによって作成されたHTTP要求メッセージ(1つのエリア)と、サーバによって生成されたHTTP応答(2番目のエリア)を表示できます。

情報(Info)

情報(Info)] タブを使用して、要求に関する詳細情報を表示します。情報には、見つかったフォームの数、ヘッダ情報、およびページのプロパティが含まれます。

ブラウザ

ブラウザ(Browser)] タブをクリックして、ブラウザでフォーマットされた形式で応答を表示します。

Web Proxy対話型モード

メッセージがWeb Proxyに届いた時点で各ブラウザ要求と各サーバ応答を表示するには、対話型モードを使用します。**送信(Send)**] をクリックするまで、メッセージは宛先に向けて先に進みません。これにより、メッセージを配信前に変更できます。

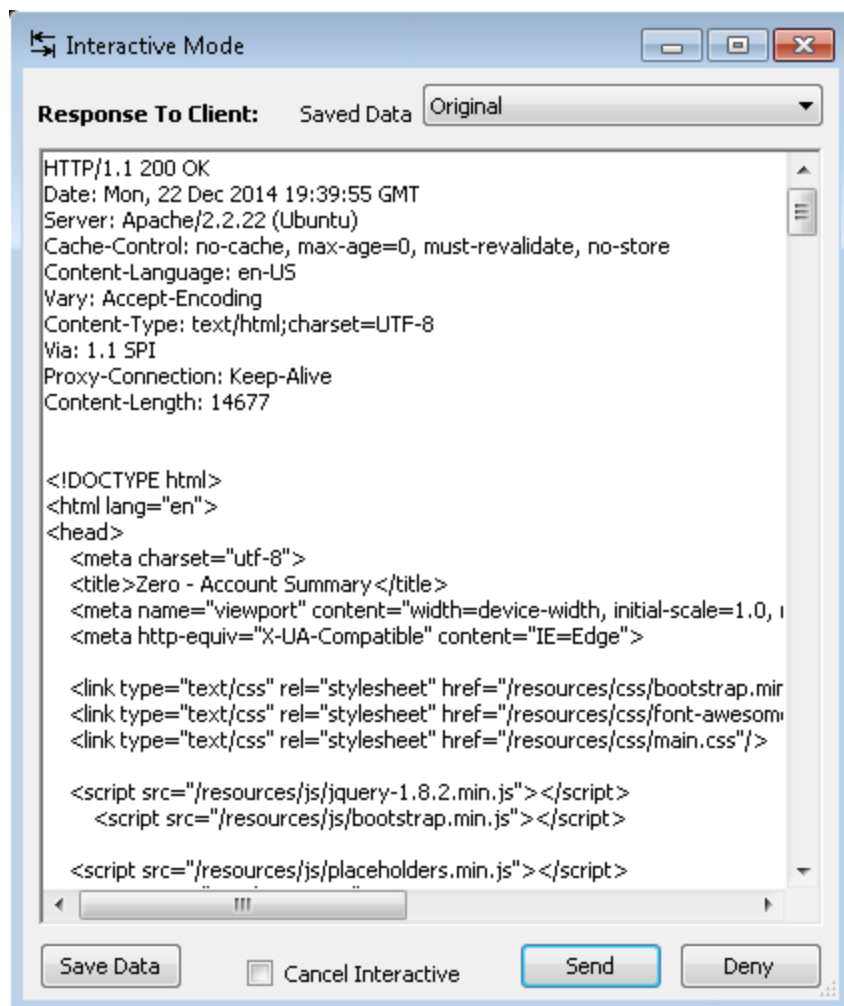
拒否(Deny)] をクリックして、メッセージがサーバに送信されないようにすることもできます。

Web Proxy設定 (Web Proxy Settings)] ウィンドウの **全般(General)**] タブを使用して、Web Proxyを強制的に次のように一時停止できます。

- 各要求の後
- 各応答の後
- 要求または応答に特定のテキストを見つけた後(検索ルールを使用)


Web Proxy対話型モードのイメージ


次のイメージは、対話型モードのWeb Proxyを示しています。



対話型モードの有効化

対話型モードを有効にするには:

1. **プロキシ(Proxy)]**メニューをクリックし、**停止(Stop)]**を選択します。
2. 次のいずれかを実行します。
 - **プロキシ(Proxy)]**メニューをクリックし、**対話型(Interactive)]**を選択します。
 - ツールバーの  をクリックします。
3. **プロキシ(Proxy)]**メニューをクリックし、**開始(Start)]**を選択します。

注記: Web Proxyが対話型モードの場合、**プロキシ(Proxy)]**メニューの **対話型(Interactive)]** コマンドの横にチェックマークが付き、対話型アイコンのバックライトが点灯した状態になります 。アイコンをクリックするか、コマンドを選択すると、対話型モードのオンとオフが切り替わります。

設定(Settings)

このプロパティシートを使用して、Web Proxyのインタフェースの設定、プロキシサーバの追加、および要求または応答内の特定の情報を検索するための正規表現の作成を行います。

注記: Web Proxyの実行中は設定を変更できません。[プロキシ(Proxy)]メニューから**停止(Stop)**を選択し、設定を変更して、Web Proxyを再起動します。

Web Proxyの **設定(Settings)** プロパティシートには、次のタブがあります。

- 全般(**"設定: 全般"** 下を参照)
- プロキシサーバ(Proxy Servers)(**"設定: プロキシサーバ"** 次のページを参照)
- 検索と置換(Search and Replace)(**"設定: 検索と置換"** ページ339を参照)
- フラグ(Flag)(**"設定: フラグ"** ページ340を参照)
- 回避(Evasions)(**"設定: 回避"** ページ340を参照)
- ネットワーク認証(**"設定: ネットワーク認証"** ページ344を参照)

設定: 全般

全般(General) タブには、次のオプションが含まれます。

プロキシリスナーの設定

IPアドレスとポート番号を入力します。デフォルトでは、Web Proxyはアドレス127.0.0.1とポート8080を使用しますが、必要に応じて変更できます。

注記: Web ProxyとWebブラウザの両方で、同じIPアドレスとポートを使用する必要があります。

自分のホスト上のWeb Proxyを別のホストで使用するようには、ローカルIPアドレスの値を変更する必要があります。デフォルトのアドレスである127.0.0.1は、外部ホストでは使用できません。この値をワークステーションの現在のIPアドレスに変更すれば、リモートワークステーションでそのワークステーションをプロキシとして使用できます。

記録しない(Do not record)

このオプションを使用して、特定のタイプのファイルがWeb Proxyによって処理されるのを防ぐ正規表現フィルタを作成します。最も一般的なタイプは、すでにデフォルトとして除外されています。ただし、その他のタイプ(MPEG、PDFなど)も除外できます。この目的は、メッセージ本文から不要なデータを削除し、HTTP要求/応答の行とヘッダに焦点を当てることです。

対話型 (Interactive)

対話型モードを使用している場合、Web Proxyが次の動作を行う場合に一時停止を強制できます。

- クライアントから要求を受信する
- サーバから応答を受信する
- 作成した検索ルールを満たすテキストを検索する(**フラグ(Flag)** タブを使用)

これらのオプションのいずれかを選択した場合、 **許可(Allow)** ボタンをクリックしないとWeb Proxyは続行しません。

ログ記録(Logging)

ログファイルに記録する項目のタイプを選択し、ログファイルを保存するディレクトリを指定します。

要求または応答の記録を選択した場合は、Base 64エンコーディングを使用してデータを変換してログ記録することも選択できます。これは、応答に調査対象のバイナリデータ(イメージやFlashファイルなど)が含まれている場合に便利です。

- 生の要求とは、クライアントからWeb Proxyに送信されるHTTPメッセージを指します。
- 変更後要求とは、Web Proxyからサーバに送信されるHTTPメッセージを指します。
- 生の応答とは、サーバからWeb Proxyに送信されるHTTPメッセージを指します。
- 変更後応答とは、Web Proxyからクライアントに送信されるHTTPメッセージを指します。

高度なHTTP解析(Advanced HTTP Parsing)

ほとんどのWebページには、使用する文字セットをブラウザに知らせる情報が含まれています。この指示は、HTMLドキュメントのHEADセクションのContent-Type応答ヘッダ(またはHTTP-EQUIV属性を持つMETAタグ)を使用して行われます。文字セットをアナウンスしていないページ用にWeb Proxyで使用するべき文字セットを指定できます。

設定: プロキシサーバ

このエリアを使用して、Web Proxyによってルーティングされるすべての要求が通過する1つ以上のプロキシサーバを追加します。攻撃を複数のサーバに分散すると検出と対策が難しくなるため、ハッカーが侵入検知システムを回避しようとして使う可能性のある方法を模倣しています。

複数のプロキシサーバを使用する場合、Web Proxyは要求を「ラウンドロビン」で処理します(つまり、Web Proxyは最初の要求を最初のサーバに送信し、2番目の要求は2番目のサーバに送信するといった具合にプロキシサーバのリストを順次処理します)。

プロキシサーバを使用せずにアクセスするIPアドレスを指定することもできます。

プロキシサーバの追加

Web Proxy要求のルーティングの経由地となるプロキシサーバを追加するには:

1. **プロキシアドレス(Proxy Address)]** ボックスに、Web Proxy要求をルーティングする際に経由するサーバのIPアドレスを入力します。
2. **プロキシポート(Proxy Port)]** ボックスでポート番号を指定します。
3. **プロキシの種類(Proxy Type)]** リストからプロキシの種類(標準、SOCKS4、またはSOCKS5)を選択します。
4. 認証の種類として、**なし(None)]**、**自動(Auto)]**、**[Kerberos]**、**[NTLM]**、または**基本(Basic)]**を選択します。
使用する種類が不明な場合は、**自動(Auto)]**を選択します。Web ProxyはNTLM認証と基本認証の両方を試行します。
5. このサーバで認証が必要な場合は、**ユーザ名(Username)]** ボックスと **[パスワード(Password)]** ボックスに認証資格情報を入力します。
6. **追加(Add)]** をクリックすると、そのサーバが追加され、**使用可能なプロキシサーバ(Available Proxy Servers)]** リストにIPアドレスが表示されます。

プロキシサーバのインポート

プロキシサーバのリストをインポートするには:

1. **[インポート(Import)]** をクリックします。
2. 標準のファイル選択ダイアログボックスを使用して、プロキシサーバのリストを含む Delimited Textファイルを選択します。
3. **開く(Open)]** をクリックします。

プロキシ情報を含むファイルは、次の形式にする必要があります。

- 各行に1つのレコードを含め、その後にキャリッジリターンおよび改行文字を続けます。
- レコード内の各フィールドはセミコロンで区切ります。
- フィールドは、address;port;proxytype;username;password;authenticationtypeの順になります。
- ユーザ名とパスワードはオプションです。ただし、権限付与を使用しない場合は、プレースホルダとして2つのセミコロンを含める必要があります。

例:

```
128.121.4.5;8080;Standard;magician;abracadabra;NTLM
127.153.0.3;80;socks4;;None
128.121.6.9;443;socks5;myname;mypassword;None
```

プロキシサーバの編集

プロキシサーバのリストを編集するには:

1. **使用可能なプロキシサーバ(Available Proxy Servers)]** リストからサーバを選択します。
2. **プロキシアドレス(Proxy Address)]**、**プロキシポート(Proxy Port)]**、**プロキシタイプ(Proxy Type)]**、**ユーザ名 (Username)]**、または **パスワード(Password)]** のコントロールに表示される情報を変更します。
3. **更新(Update)]** をクリックします。

プロキシサーバの削除

リストからプロキシサーバを削除するには:

1. **使用可能なプロキシサーバ(Available Proxy Servers)]** リストからサーバを選択します。
2. **削除(Remove)]** をクリックします。
3. **はい(Yes)]** をクリックして、削除を確定します。

プロキシサーバのバイパス

特定のURL(内部テストサイトなど)へのアクセスにプロキシサーバを使用する必要がない場合は、**プロキシのバイパスリスト(Bypass Proxy List)]** エリアで1つ以上のホストを指定できます。特定のサイトにアクセスする際にプロキシサーバをバイパスするには:

1. **追加(Add)]** をクリックします。
プロキシのバイパス(Bypass Proxy)] ダイアログボックスが表示されます。
2. バイパスするHTTP URLのホスト部分を入力します。
プロトコル(http://など)は含めないでください。
たとえば、このURLのプロキシサーバをバイパスする場合
`http://zero.webappsecurity.com/Page.html`
この文字列を入力します。
`zero.webappsecurity.com`
またはこの文字列を入力します。
`zero.*`

注記: IPアドレスを入力することもできます。Web Proxyはホスト名をIPアドレスに解決しないことに注意してください。つまり、IPアドレスを指定し、かつHTTP要求に実際にその数値のIPアドレスが含まれている場合、Web Proxyはそのホストのプロキシサーバをバイパスします。しかし、HTTP要求に含まれているのが通常は指定したIPアドレスに解決されるホスト名である場合、(ホスト名も指定しない限り) Web Proxyは引き続きプロキシサーバに要求を送信します。

3. **OK]** をクリックします。

アドレスの削除

プロキシのバイパスリスト(Bypass Proxy List)] からアドレスを削除するには、アドレスを選択して **削除(Remove)]** をクリックします。

設定: 検索と置換

このタブを使用して、HTTPメッセージ内のテキストまたは値を検索および置換するルールを作成します。この機能は、攻撃のシミュレーションを自動的に行うための非常に柔軟なツールを提供します。推奨される用途は次のとおりです。

- ユーザ名 やパスワードなどの機密データのマスク
- 各要求へのクッキーの追加
- Accept要求ヘッダフィールドを変更して、応答で許容されるメディアタイプを追加または削除する
- 要求URI内の変数をクロスサイトスクリプティング攻撃に置換する

テキストの検索と置換

要求または応答のテキストを検索して置き換えるには:

1. **追加(Add)]** をクリックします。
Web Proxyによってテーブルにデフォルトのエントリが作成されます。
2. エントリの **検索フィールド(Search Field)]** 列をクリックします。
3. ドロップダウン矢印をクリックして、検索するメッセージエリアを選択します。
4. **検索データ(Search For)]** 列に、検索するデータ(またはデータを表す正規表現)を入力します。
5. **置換データ(Replace With)]** 列に、見つかったデータを置き換えるデータを入力します。
6. 検索ルールを追加で作成するには、ステップ1-5を繰り返します。

要求/応答ルールは表示されている順序で順次適用されます。たとえば、あるルールがHTTPSをSSLに変更し、その後に続くルールがSSLをSECUREに変更する場合は、結果的にHTTPSがSECUREに変更されます。

注記: 検索と置換のルールは、Web Proxyからサーバに送信される要求メッセージおよびWeb Proxyからブラウザに送信される応答メッセージに対して実行されます。 **情報(Info)]** タブを選択するか、 **表示(View)]** タブまたは **分割(Split)]** タブを選択し、タブの直下にあるドロップダウンリストから次のいずれかを選択して、変更されたメッセージを確認できます。

- 要求: WebProxy ->サーバ(Request: WebProxy -> Server)
- 応答: ブラウザ<- WebProxy (Response: Browser <- WebProxy)
- セッション(Session)

ルールの削除

ルールを削除するには:

1. 削除するルールを選択します。
2. **削除(Remove)]**をクリックします。

ルールの編集

ルールを編集するには:

1. **検索フィールド(Search Field)]** 列、 **検索データ(Search for)]** 列、または **置換データ(Replace with)]** 列のエントリをクリックします。
2. データを変更します。

ルールの無効化

ルールを削除せずに無効にするには:

1. **オン(On)]** チェックボックスをクリアします。
2. **OK]**をクリックします。

設定: フラグ

要求および応答メッセージのエリアを検索して、指定したデータを検索および強調表示できます。

1. **追加(Add)]**をクリックします。
Web Proxyによってテーブルにデフォルトのエントリが作成されます。
2. エントリの **検索フィールド(Search Field)]** 列をクリックします。
3. ドロップダウン矢印をクリックして、検索するメッセージエリアを選択します。
4. **検索(Search)]** 列に、検索するデータ(またはデータを表す正規表現)を入力します。
5. エントリの **フラグ(Flag)]** 列をクリックします。
6. ドロップダウン矢印をクリックして、データを強調表示する色(見つかった場合)を選択します。
7. 検索ルールを追加で作成するには、ステップ1-6を繰り返します。

設定: 回避

回避とは、侵入検知システム、モニタ、スニファ、ファイアウォール、ログパーサ、またはHTTP要求をフィルタ処理してシステムを攻撃から保護しようとするデバイスを回避するためにWeb Proxyが使用する技術です。通常、これらのフィルタは要求の一部を検査し、悪意のある脅

威またはシステムセキュリティの潜在的な脆弱性を示す「署名」を検索します。これらの署名が検出されると、要求は拒否されます。

検出を回避するために、Web ProxyはHTTP要求を変更してフィルタが検索する署名を覆い隠しますが、その一方でメッセージがサーバによって処理されるのに十分な整合性を保持します。もちろん、Web Proxyが使用する技術は必ずしも成功するとは限りません。開発者は、製品の有効性を損なう方法を認識するに従って、対抗手順を組み込みます。

注意! この機能は、侵入テストツールとして使用することを目的にしています。OpenText DASTで脆弱性評価スキャンを実行する場合は、このツールを使用したり有効にしたりしないでください。

回避を有効にするには、次の手順に従います。

1. **回避を有効にする(Enable Evasions)]**を選択します。
2. 以下のセクションの「」で説明するように、1つ以上の回避方法を選択します。

メソッドの一致

Web Proxyは、GETメソッドをHEADに置き換えます。これは、GETで始まる署名を検索するフィルタを無効にしようとする試みです。

たとえば、ブラウザは次のメッセージをWeb Proxyに送信します。

```
GET http://www.microsoft.com/secretfile.txt HTTP/1.1
```

Web Proxyは、次のメッセージをサーバに送信します。

```
HEAD http://www.microsoft.com/secretfile.txt HTTP/1.1
```

URLエンコーディング

Web ProxyはURL内の文字を、ISO-8859-1文字セット内の文字値に対応する、「%」とそれに続く2つの16進文字に変換します。

たとえば、ブラウザは次のメッセージをWeb Proxyに送信します。

```
GET http://zero.webappsecurity.com/cgi-bin/filename.cgi HTTP/1.1
```

Web Proxyは、次のメッセージをサーバに送信します。

```
GET %2f%63%67%69%2d%62%69%6e%2f%66%69%6c%65%6e%61%6d%65%2e%63%67%69 HTTP/1.1
```

```
Host: zero.webappsecurity.com
```

デバイスが署名として「cgi-bin」を探す場合、「%63%67%69%2d%62%69%6e」という文字列と一致しないので、要求は拒否されません。

二重のスラッシュ

Web Proxyは、各スラッシュ(/)を二重のスラッシュ(//)に変換します。

たとえば、ブラウザは次のメッセージをWeb Proxyに送信します。

```
GET http://www.microsoft.com/en/us/secrets.aspx HTTP/1.1
```

Web Proxyは、次のメッセージをサーバに送信します。

```
GET //en//us//secrets.aspx HTTP/1.1
Host: www.microsoft.com
```

デバイスが署名として「/secrets.aspx」を探す場合、「//secrets.aspx」という文字列と一致しないので、要求は拒否されません。

逆トラバーサル

この方法では、元の要求と同等の相対ディレクトリへの参照を挿入することで、特定のソースに対する要求を偽装しようとします。

たとえば、ブラウザは次のメッセージをWeb Proxyに送信します。

```
GET http://www.TargetSite.com/cgi-bin/some.cgi HTTP/1.1
```

Web Proxyは、次のメッセージをサーバに送信します。

```
GET /d/../../cgi-bin/d/../../some.cgi HTTP/1.1 [which equates to GET/cgi-bin/some.cgi]
Host: www.TargetSite.com
```

自己参照ディレクトリ

Web Proxyは、親ディレクトリ(..)とカレントディレクトリ(.)の表記を使用して要求を難読化します。

たとえば、ブラウザは次のメッセージをWeb Proxyに送信します。

```
GET http://www.TargetSite.com/cgi-bin/phf HTTP/1.1
```

Web Proxyは、次のメッセージをサーバに送信します。

```
GET ../cgi-bin/./phf HTTP/1.1 [which equates to GET /cgi-bin/phf]
Host: www.TargetSite.com
```

パラメータの非表示

要求には、ダイナミックページコンテンツの作成に使用されるパラメータを含めることができます。これらのパラメータは、通常、検索要求または選択が行われたときに使用され、次の形式を取ります。

```
/anypage.php?attack=paramhiding&evasion=blackhat&success...
```

この方法は、疑問符(?)に続く要求の部分を調べないデバイスに対して有効です。ただし、パラメータインジェクタを使用して、さらに関連するデータをマスクできます。

たとえば、ブラウザは次のメッセージをWeb Proxyに送信します。

```
GET /index.htm%3fparam=../cgi-bin/test.cgi
```

Web Proxyは、次のメッセージをサーバに送信します。

```
GET /index.htm?param=../cgi-bin/test.cgi
```

HTTP形式の誤り

HTTP要求の構造は明確に定義されています。

```
Method<space>URI<space>HTTP/Version<CR><LF>
```

ただし、Webサーバによっては、次のように、スペースの代わりにタブ文字を含む要求を受け入れる場合があります。

```
Method<tab>URI<tab>HTTP/Version<CR><LF>
```

検索する署名の一部としてスペースを(3つのコンポーネントの間に)組み込んでいるフィルタは、要求の拒否に失敗します。

長いURL

この方法は、要求文字列全体を調べず、プログラム可能な長さのサブセット(最初の50文字など)にのみ集中するデバイスを対象としています。Web Proxyは要求の先頭に多数のランダムな文字を挿入し、要求の機能する部分を、フィルタによって通常検査されるエリアの外に押し出します。

たとえば、ブラウザは次のメッセージをWeb Proxyに送信します。

```
GET http://zero.webappsecurity.com/ HTTP/1.1
```

Web Proxyは、次のメッセージをサーバに送信します。

```
GET /YPVIFAHD[hundreds of characters]NIWCJBXZPXMP/.. HTTP/1.1  
Host: zero.webappsecurity.com
```

DOS/Winディレクトリ構文

特定の署名(/cgi-bin/some.cgiなど)を検出しようとするWindowsベースのフィルタは、スラッシュを円記号に置き換えた場合(/cgi-bin\some.cgiなど)、だまされる可能性があります。WindowsベースのWebサーバでは、ディレクトリ構造を解釈するときにスラッシュを円記号に変換します。したがって、この表記法は有効です。ただし、HTTPルールでは、URIの最初の文字がスラッシュである必要があります。

NULLメソッドの処理

この方法では、メソッドの直後にURLエンコードのNULL文字が挿入されます(GET%00など)。これは要求に対して文字列操作を適用しようとするフィルタ用に設計されており、それらの文字列ライブラリはNULL文字を使用して文字列の終わりを示します。この戦略が成功すると、NULL文字の検出により、デバイスはメッセージの残りの部分を検査できなくなります。

大文字と小文字の区別

この方法は、大文字と小文字が区別される文字列を検索するフィルタを回避するように設計されています。

たとえば、ブラウザは次のメッセージをWeb Proxyに送信します。

```
GET http://zero.webappsecurity.com/cgi-bin/some.cgi HTTP/1.1
```

Web Proxyは、次のメッセージをサーバに送信します。

```
GET /CGI-BIN/SOME.CGI HTTP/1.1  
Host: zero.webappsecurity.com
```

設定: ネットワーク認証

プロキシサーバでネットワーク認証が必要な場合は、Web Proxy設定の **ネットワーク認証 (Network Authentication)** タブで設定できます。

ネットワーク認証を設定するには:

1. **ネットワーク認証を有効にする(Enable Network Authentication)**を選択します。
2. **認証タイプ(Authentication Type)** リストから認証タイプを選択します。使用可能なタイプは次のとおりです。
 - ADFS CBT
 - 自動
 - 基本
 - ダイジェスト
 - Kerberos
 - ネゴシエート(Negotiate)
 - NT LAN Manager (NTLM)
3. **ユーザ名 (Username)** ボックスにユーザIDを入力し、**パスワード(Password)** ボックスにユーザのパスワードを入力します。

Webマクロの作成

WebマクロレコードまたはWeb Proxyを使用して、ワークフローマクロまたはログインマクロを作成できます。

ワークフローマクロは、アプリケーションの特定のサブセクションに焦点を当てるために最もよく使用されます。これは、OpenTextスキャナがそのエリアへの移動に使用するURLを指定します。ログイン情報を含めることもできますが、スキャナがアプリケーションからログアウトすることを防ぐロジックは含まれません。Web Proxyでキャプチャされたセッションを使用することも、Burp ProxyファイルのセットまたはHTTPアーカイブ(HAR)ファイルを使用することもできます。

ログインマクロは、Webフォーム認証に使用され、スキャナがアプリケーションにログインできるようにします。スキャナが誤ってアプリケーションからログアウトするのを防ぐロジックを組み込むこともできます。

Burp ProxyまたはHARファイルの使用

Burp ProxyファイルのセットまたはHTTPアーカイブ(HAR)ファイルからワークフローマクロを作成するには:

1. **ファイル(File)] > 開く(Open)]**をクリックします。
標準のWindowsの **開く]** ダイアログボックスが開きます。
2. ドロップダウンリストで、 **Burp proxy (*.*)]** または **[Harファイル(*.har)(Har File (*.har))]** を選択します。
3. Burp Proxyまたは.Harファイルに移動して開きます。
Web Proxyでセッションが表示されます。
4. **"選択されたセッションからのWebマクロの作成"** 下の手順に従います。

選択されたセッションからのWebマクロの作成

Web Proxyで表示またはキャプチャされたセッションを使用してWebマクロを作成するには:

1. 左側の列にチェックマークを付けて、マクロに含めるセッションを選択します。
2. **ファイル(File)]** メニューをクリックして、 **Webマクロの作成(Create Web Macro)]** を選択します。
[Webマクロの作成(Create Web Macro)] ダイアログボックスが開きます。
3. (オプション) [Webマクロの作成(Create Web Macro)] ダイアログボックスで、 **ログアウトのチェックを有効にする(Enable Check for Logout)]** を選択し、ユーザがログアウトするとき、またはログインしていないユーザが保護されたURLへのアクセスを要求するときに、サーバのHTTP応答で発生する固有のテキストまたはフレーズを識別する正規表現を入力します。

例: 通常のスキャン中に、スキャナはホームページでサイトのWeb探索を開始します。別のリソースへのリンクが検出された場合(通常は<A HREF> HTMLタグを使用)、そのURLに移動して評価を続行します。ログアウトページへのリンクをたどる場合(または一定の分数が経過した後サーバがクライアントを自動的に「ログアウト」した場合)、クライアントがログインしていないと利用できない追加のリソースにスキャナはアクセスできなくなります。この予期せぬログアウトが発生した場合、スキャナはユーザの操作なしに再度ログインする必要があります。このプロセスは、ログイン状態ではなくなったときにスキャナがそれを認識できるかどうかにかかっています。

一部のアプリケーションでは、ユーザが(ボタンまたは他のコントロールをクリックして)ログアウトした場合、サーバは「Have a nice day」などの固有のメッセージを表示します。このフレーズをサーバのログアウト署名として指定すると、スキャナは応答メッセージが出るたびにこのフレーズを検索します。このフレーズが検出されると、スキャナはユーザ名とパスワードを含むHTTP要求を送信して再度ログインを試みます。

ログアウトしたことをスキャナが検出できる別の状況としては、パスワードで保護されたURLにスキャナがアクセスを試みるのに対して、サーバが特定の応答メッセージを送信する場合があります。たとえば、サーバがステータスコード「302 Object moved」で応答する場合があります。この応答から探すべき内容をスキャナが具体的に認識している場合、このプログラムはログアウトしたことを認識し、ログイン状態を再確立できます。

上の例を使用して、ユーザがアプリケーションからログアウトする際に「Have a nice day」などのメッセージがサーバから返される場合は、正規表現として「Have\s\snice\sday」と入

力します(正規表現ではスペースを指定するために「\s」が使用されます)。より可能性が高い例は、サーバが302ステータスコードを返し、新しいURLを参照する場合です。この場合、「[STATUSCODE]302 AND [ALL]http://login.myco.com/config/mail?」が一般的な正規表現のフレーズになる可能性があります。正規表現の作成に関するヒントについては、「["正規表現の拡張" 次のページ](#)」を参照してください。

4. **マクロに名前を付けて保存 (Save Macro As)** ボックスにパスとファイル名を入力するか、**参照 (Browse)** をクリックして標準のファイル選択ダイアログボックスを開き、ファイル名を指定します。
5. **OK** をクリックします。

クライアント証明書 (Client certificates)

Web ProxyがWebサーバから証明書の要求を受け取った場合、証明書の特定を求めるダイアログボックスが表示されます。次に、プログラムは選択内容を「サーバ単位」でキャッシュします。したがって、その後、特定のサーバに対して別の証明書を使用する場合は、Web Proxyを停止してから再起動し、キャッシュをクリアする必要があります。

正規表現

正規表現のパターンは、特殊な文字やシーケンスを使用して作成されます。次の表に、これらの文字の一部を示し、その簡単な使用例を示します。推奨する他の参照先として「[Regular Expression Library](#)」があります。

使用可能な特殊なタグと演算子については、「["正規表現の拡張" 次のページ](#)」も参照してください。

文字	説明
\	次の文字を特殊文字としてマークします。/n/は文字「n」に一致します。シーケンス\n/は、改行文字に一致します。
^	入力または行の先頭に一致します。 文字クラスとともに使用すると、否定文字を意味します。たとえば、contentディレクトリ内の/content/enおよび/content/caを除くすべてを除外するには、/content/[^(en ca)].*/*.*/を使用します。\\S \\D \\Wも参照してください。
\$	入力または行の末尾に一致します。
*	先行する文字の0回以上の反復と一致します。/zo*/は「z」とも「zoo」とも一致します。
+	先行する文字の1回以上の反復と一致します。/zo+/は「zoo」に一致し

文字	説明
	ますが、「z」には一致しません。
?	先行する文字の0回または1回の出現と一致します。/a?ve?/は「never」の「ve」に一致します。
.	改行文字を除く任意の1文字に一致します。
[xyz]	文字セット。括弧内の任意の1文字に一致します。/[abc]/は「plain」の「a」に一致します。
\b	スペースなどの単語境界に一致します。/ea*\b/は、「never early」の「er」に一致します。
\B	非単語境界に一致します。/ea*\B/は「never early」の中の「ear」と一致します。
\d	1つの数字に一致します。[0-9]と同じです。
\D	数字以外の1文字に一致します。[^0-9]と同じです。
\f	改ページ文字に一致します。
\n	改行文字に一致します。
\r	キャリッジリターン文字に一致します。
\s	スペース、タブ、改ページなどの空白に一致します。[\f\n\r\t\v]と同じです。
\S	空白文字以外の文字に一致します。[^ \f\n\r\t\v]と同じです。
\w	アンダースコアを含む任意の単語文字に一致します。[A-Za-z0-9_]と同じです。
\W	任意の非単語文字に一致します。[^A-Za-z0-9_]と同じです。

正規表現の拡張

OpenTextのエンジニアにより、通常の正規表現構文の拡張、およびそれに伴う一連の演算子が開発および実装されました。

正規表現タグ

正規表現を構築する場合、この拡張を使用して、要求または応答のどの要素内で一致を検索するかを指定できます。次の表に、拡張の説明を示します。

拡張	要素
[ALL]	要求または応答のすべての要素
[BODY]	要求の本文 応答本文
[COOKIES]	要求のクッキー
[HEADERS]	要求ヘッダ(Request Headers) 応答ヘッダ(Response Headers)
[METHOD]	要求のメソッド(Request Method)
[POSTDATA]	Postデータ
[REQUESTLINE]	要求行(HTTP要求の開始行)
[SETCOOKIES]	Set-Cookie応答ヘッダ
[STATUSCODE]	ステータスコード(Status Code)
[STATUSDESCRIPTION]	ステータスの説明(クライアントに返されるHTTP出力のステータスを説明する文字列)
[STATUSLINE]	ステータス行(HTTP応答の開始行)
[URI]	要求ターゲット(URI)
[VERSION]	HTTPバージョン

正規表現演算子

OpenTextのエンジニアにより、複雑な正規表現パターンの構築に使用できる正規表現演算子が開発されました。演算子は次のとおりです。

- AND
- OR
- NOT

- []
- ()

例

以下の段落に、拡張と演算子の使用例を示します。

- (a)ステータス行にステータスコード「200」が含まれており、かつ(b)メッセージ本文のどこかに「logged out」という語句が含まれている応答を検出するには、次の正規表現を使用します。

```
[STATUSCODE]200 AND [BODY]logged\sout
```

- 要求されたリソースが一時的に別のURI (リダイレクト)に存在することを示しており、かつ応答のどこかにパス「/Login.asp」への参照が含まれる応答を検出するには、次の正規表現を使用します。

```
[STATUSCODE]302 AND [ALL]Login.asp
```

- (a)ステータスコードが「200」、かつ「logged out」または「session expired」という語句が本文のどこかに含まれている、または(b)ステータスコード「302」、かつ応答のどこかにパス「/Login.asp」への参照が含まれている応答のいずれかを検出するには、次の正規表現を使用します。

```
( [STATUSCODE]200 AND [BODY]logged\sout OR [BODY]session\sexpired ) OR ( [STATUSCODE]302 AND [ALL]Login.asp )
```

注記:「開き括弧」または「閉じ括弧」の前と後にスペースを含める必要があります。スペースを含めないと、括弧は誤って正規表現の一部と見なされます。


- リダイレクト Locationヘッダのどこかに「login.aspx」が現れるリダイレクト応答を検出するには、次の正規表現を使用します。

```
[STATUSCODE]302 AND [HEADERS]Location:\slogin.aspx
```

- ステータス行のReason-Phrase部に特定の文字列(「Please Authenticate」など)が含まれる応答を検出するには、次の正規表現を使用します。

```
[STATUSDESCRIPTION]Please\sAuthenticate
```

ブラウザの手動設定

Web Proxyツールバーの **ブラウザの起動(Launch Browser)**  をクリックしてもWebブラウザが起動しない場合は、Web Proxyユーザインタフェースの外部でブラウザを起動できます。ただし、ブラウザのプロキシ設定を行う必要があります。具体的な手順については、ブラウザのマニュアルを参照してください。

第20章:Webサービステスト デザイナ

Webサービスは、(ユーザではなく)他のアプリケーションと通信し、情報の要求に回答するプログラムです。ほとんどのWebサービスは、SOAP (Simple Object Access Protocol)を使用して、Webサービスと、情報要求を開始したクライアントWebアプリケーションとの間でXMLデータを送信します。Webページの表示方法のみを説明するHTMLとは異なり、XMLは構造化されたデータを説明し、含むためのフレームワークを提供します。クライアントWebアプリケーションは、返されたデータを即座に理解し、その情報をエンドユーザに表示できます。

WebサービスにアクセスするクライアントWebアプリケーションは、WSDL (Web Services Definition Language)ドキュメントを受け取り、サービスとの通信方法を理解できます。WSDLドキュメントには、Webサービスに含まれるプログラミングされたプロシージャ、それらのプロシージャに必要なパラメータ、およびクライアントWebアプリケーションが受け取る戻り情報のタイプが記述されています。



Web Service Test Designerを使用して、Webサービススキャンの実行時に送信する必要がある値を含むWebサービステスト設計ファイル(<ファイル名>.wsd)を作成します。

次の手順では、OpenText DASTの **ツール(Tools)]** メニューからWeb Service Test Designerを起動しますが、OpenText DASTの **開始ページ(Start Page)]** から **Webサービススキャンの開始(Start a Web Service Scan)]** を選択し、プロンプトが表示されたらデザイナの起動を選択して、OpenText DASTスキャンウィザードからデザイナを開くこともできます。

注記: Web Service Test DesignerをOpenText DASTスキャンウィザードから起動する場合、WSDLがまだ設定されていない場合、デザイナは自動的にWSDLをインポートし、各パラメータに「自動値」を割り当て、すべての操作を呼び出します。これは、OpenText DASTの **ツール(Tools)]** メニューまたはセキュリティツールキットからツールを起動した場合には発生しません。

1. **ツール(Tools)] > Web Service Test Designer]** を選択します。
2. 起動ダイアログボックスで、次のいずれかを選択します。
 - **新しいWebサービステスト(New Web Service Test)]** -新しいWebサービステストを設計します。
 - **Webサービステストを開く(Open Web Service Test)]** -以前に作成した設計を編集します。

次の手順では、設計を作成する場合を想定しています。

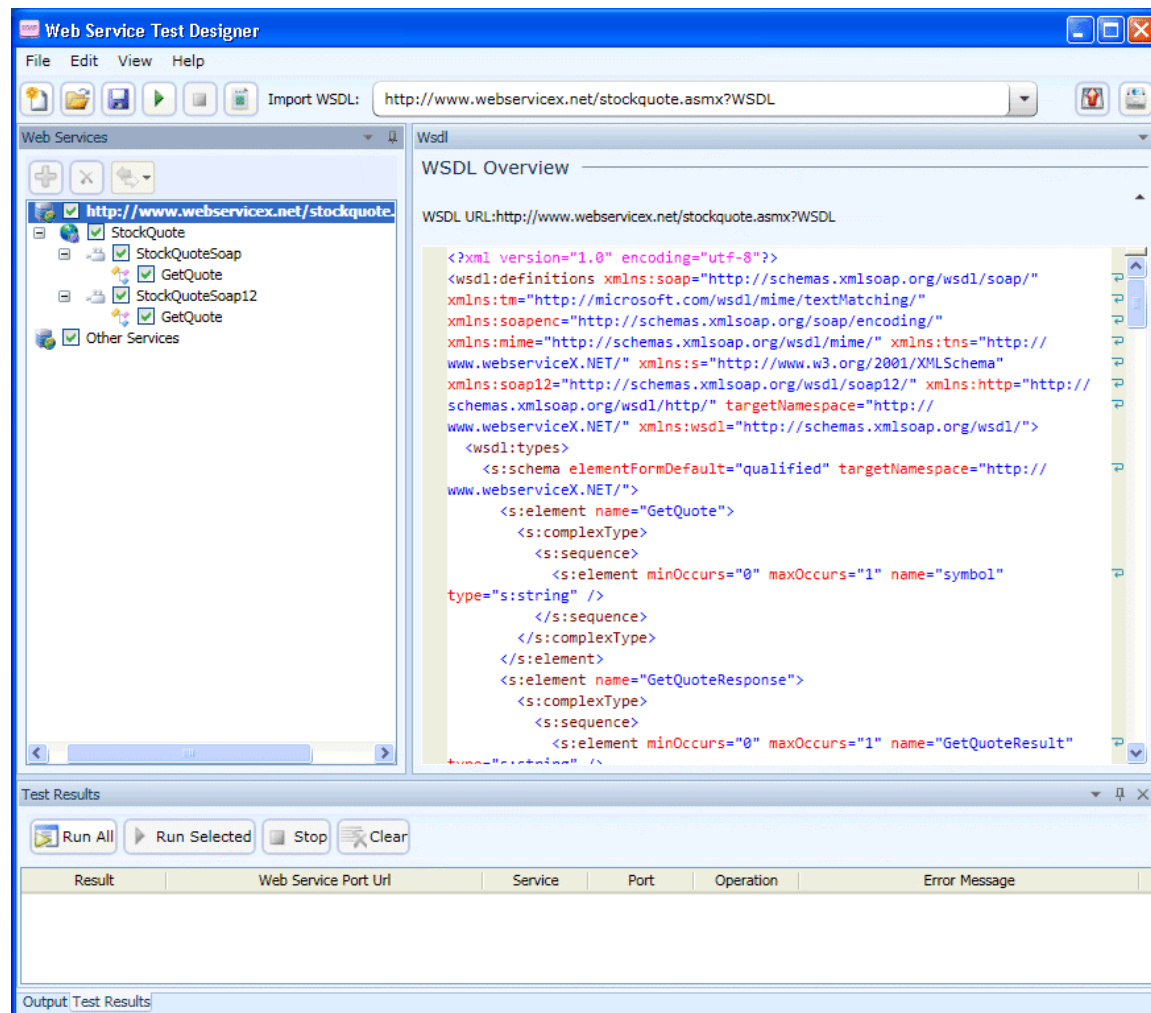
3. 次のいずれかを実行します。
 - **WSDLのインポート(Import WSDL)]** ボックスで、WSDLサイトのURL(たとえば、<http://www.webservices.net/stockquote.asmx?WSDL>など)を入力または選択し、**WSDLのインポート(Import WSDL)**  をクリックします。
 - **WSDLの参照(Browse for WSDL)]**  をクリックし、以前にローカルに保存したWSDLファイルを選択します。

注記: 認証が必要な場合、またはプロキシサーバ経由でSOAP要求を行う必要がある場合の詳細については、「[設定 \(Settings\)](#)」 [ページ362](#)を参照してください。

また、デフォルトでは [\[その他のサービス\(Other Services\)\]](#) が表示されることにも注意してください。この機能は、サービスがWSDLに関連付けされていない場合、サービスを手動で追加するために使用されます。詳細については、「[手動によるサービスの追加](#)」 [ページ356](#)」を参照してください。この項目の横のチェックマークを外します。

インポートされたWSDLのイメージ

次のイメージは、Web Service Test DesignerでのインポートされたWSDLを示しています。



4. 左側のペインでサービストランスポートを選択すると、右側のペインにポート情報が表示されます。ポートは、バインドのアドレスを指定することで、個々のエンドポイントを定義します。WSDLの記述にSOAPバージョン1.1とバージョン1.2の両方が含まれる場合、および両方の記述の操作が同じ場合、これらのバージョンは同一と見なされ、バージョン1.1のサービスだけが設定されます。両方のバージョンを攻撃する場合は、バージョン1.2の各操作のチェックボックスをオンにしてください。

注記: SOAPバージョン1.2の [ポートの概要 (Port Overview)] パネルには、HTTPヘッダにSOAPアクションを含める追加オプションが含まれています。

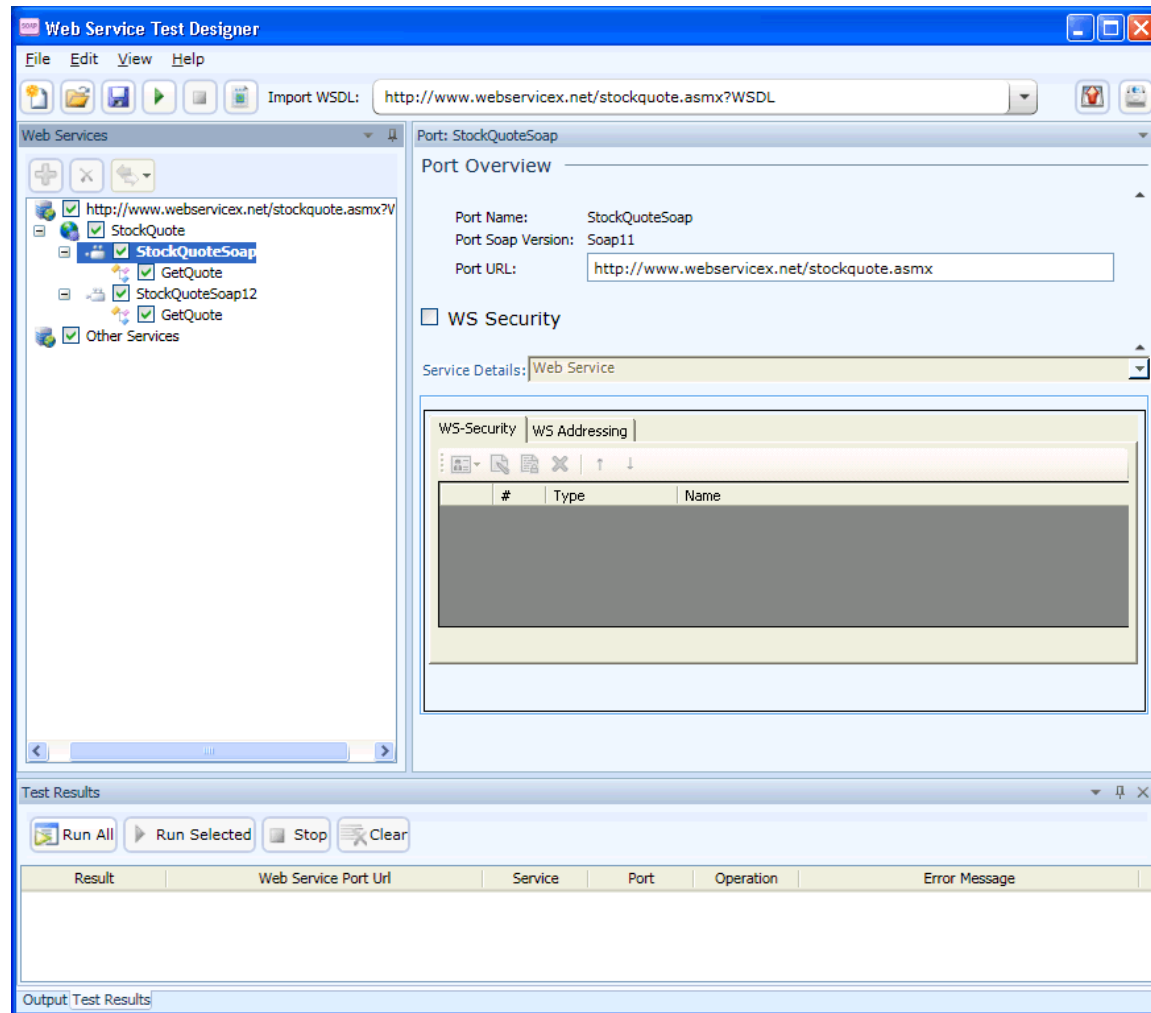
Port URL:	<input type="text" value="http://www.websvcex.net/stockquote.asmx"/>
<input type="checkbox"/> Include SOAP Action in HTTP Header	

SOAP仕様ではSOAPバージョン1.2のSOAPアクションがオプションと示されていますが、アーキテクチャによってはこれが必須の場合も、受け入れられない場合もあります。特定の環境に応じて、SOAP 1.2バインディングのSOAPアクションを含めるか除外するかを選択できます。SOAP 1.2ポートの場合のみチェックボックスが表示されます。デフォルトの設定はtrueです。

注意! RPCエンコードのサービスでは手動の設定が必要です。 [スキーマフィールド (Schema Fields)] タブは、デフォルトのSOAPスキーマを使用して入力されます。開発者またはプロキシキャプチャから目的のSOAPメッセージを取得し、そのメッセージを [XML] タブに貼り付ける(または、保存したメッセージをファイルからインポートする)ことができます。その後、 [送信 (Send)] をクリックして操作をテストできます。

サービストランスポート/ポート情報のイメージ

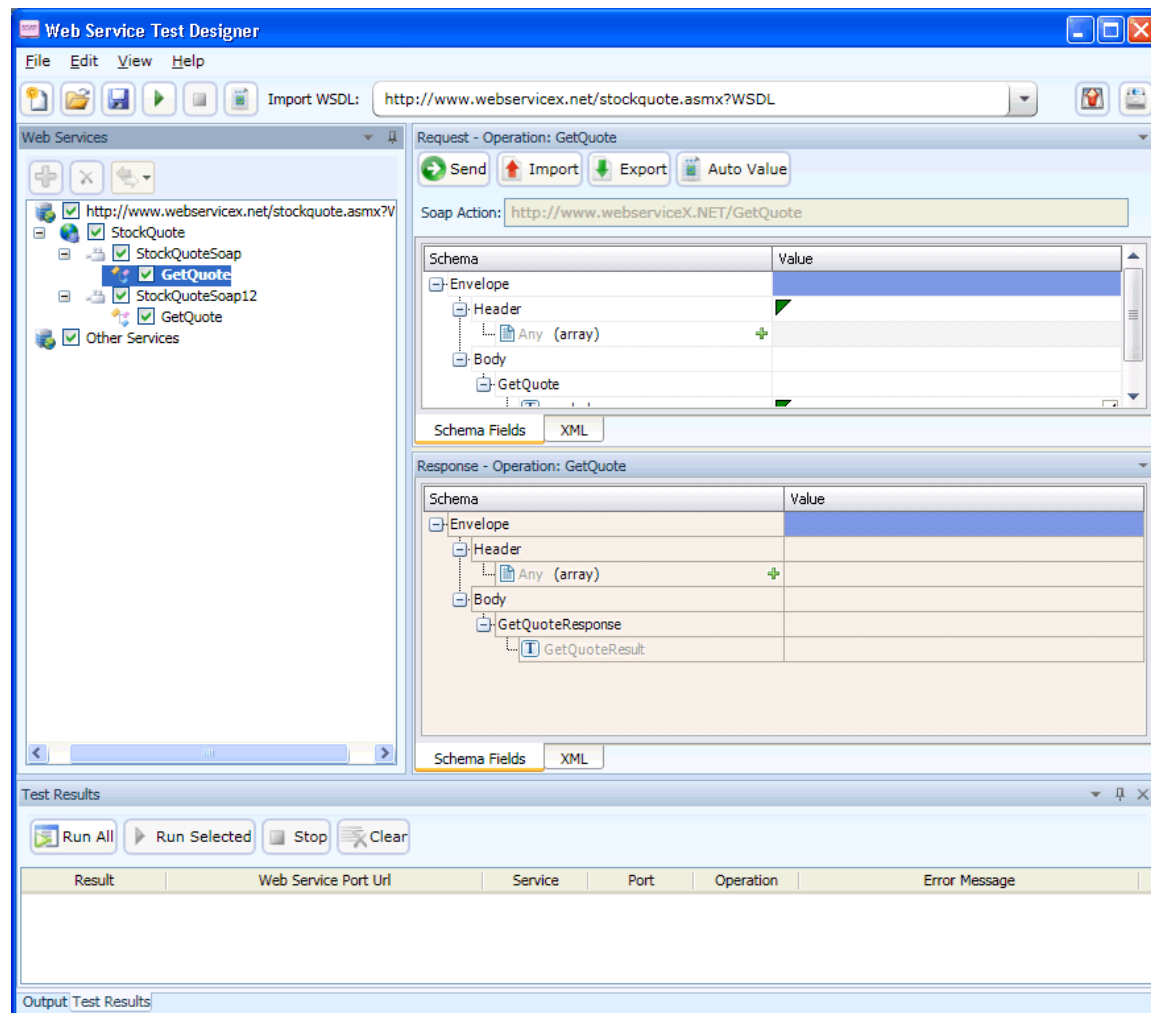
次のイメージは、選択したトランスポートのポート情報を示しています。



5. セキュリティが必要な場合:
 - a. **[WS Security]**を選択します。
 - b. **サービスの詳細(Service Details)**リストからオプションを選択します。
 - c. 必要な情報を入力します。セキュリティ設定の詳細については、["WSセキュリティ" ページ364](#)を参照してください。
6. 操作をクリックすると、要求のスキーマ(右側のペインの上半分)と応答(下半分)が表示されます。

要求/応答スキーマのイメージ

次のイメージは、選択した要求のスキーマを示しています。




7. 操作の値を入力します。この例では、ユーザはOTEX (Open Text Corporationの銘柄記号)を入力しました。

注記: 自動値(Auto Value)]をクリックすると、デザイナーによって操作に値が割り当てられます。この値は次のいずれかです。

- GlobalValuesDefault.xprファイルから取得される(このファイルにパラメータの名前に一致するエントリが含まれている場合)。詳細については、["Global Values Editor" ページ357](#)を参照してください。
- データタイプに基づいて、デザイナーによって作成される。この例では、デザイナーによってパラメータ「symbol」に値「symbol1」が入力されます。

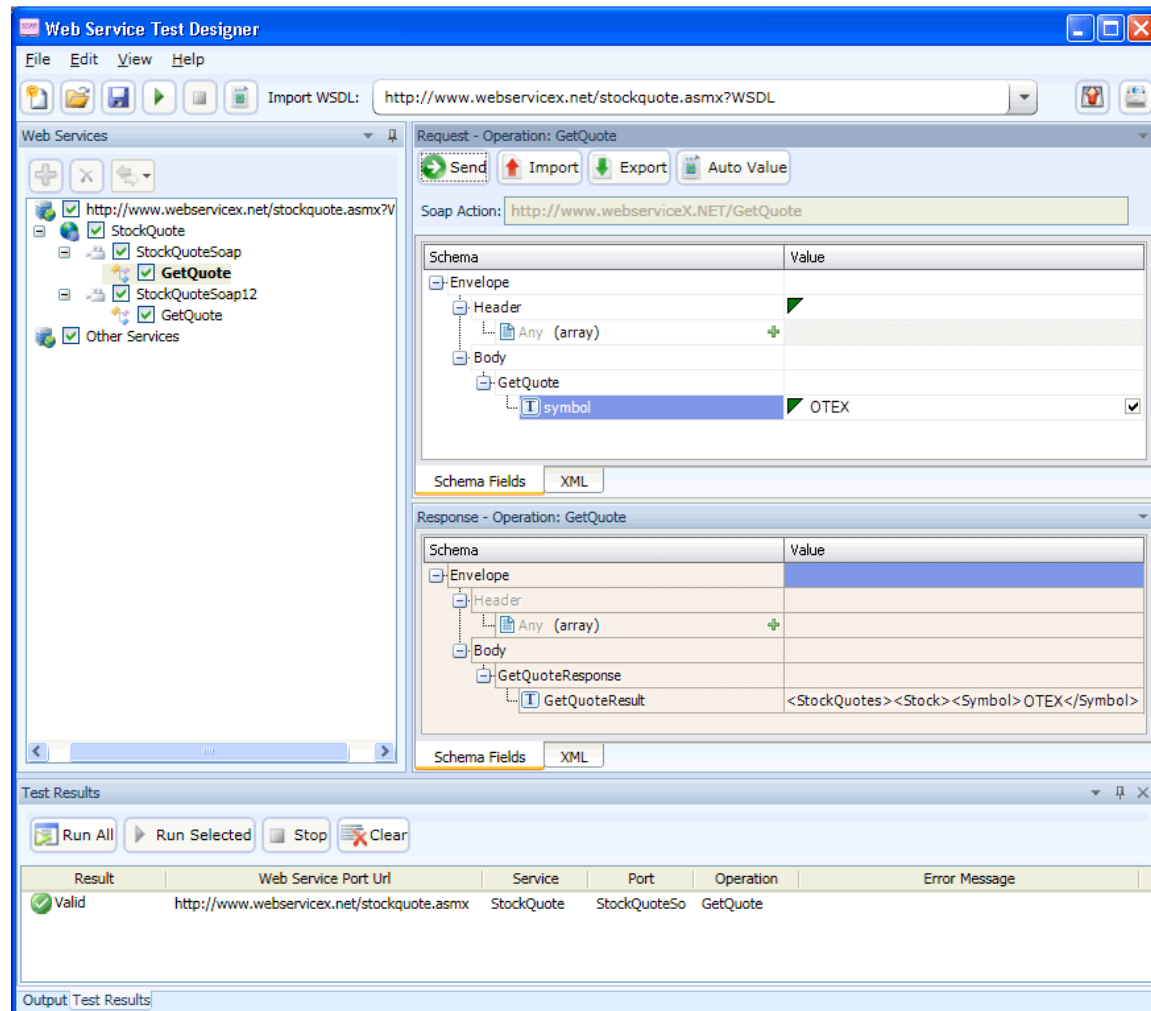
詳細については、「["自動値の使用" ページ358](#)」を参照してください。

8. 送信(Send)]  をクリックします。

結果は、下部の応答ペインに表示されます。適切なタブをクリックして、スキーマビューとXMLビューを切り替えることができます。

要求の送信のイメージ

次のイメージは、送信された要求のテスト結果を示しています。



9. 各操作に値を割り当ててテストした場合(この例では1つの操作しか示されていませんが)は、次のようにします:
 - a. **ファイル(File)] > 保存(Save)]**をクリックします。
 - b. 標準のファイル選択ダイアログボックスを使用して、Webサービス設計ファイル(.wsd)の名前と場所を選択します。

注記: WSDLに複数の操作が含まれている場合、操作にチェックマークが付けられているかどうかに関係なく、各操作のデータが保存されます。チェックマークは、単に操作が監査に使用されることを示すに過ぎません。

手動によるサービスの追加

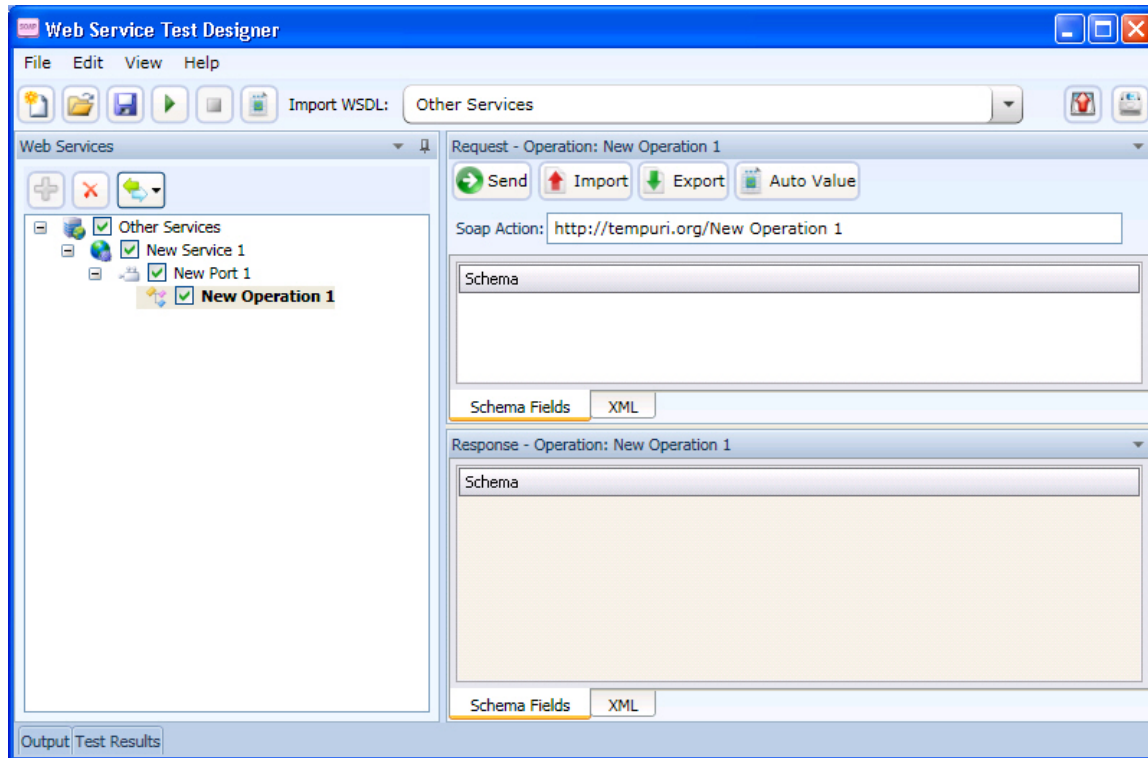
WSDLが関連付けられていないWebサービスが存在する場合があります。

たとえば、OpenText DAST Recommendationsモジュールはスキャンを監視して、徹底的なスキャンの干渉または妨げとなる、漏れ、異常、またはアノマリを検出します。Webサイトのスキャン中にSOAP要求を検出すると、そのサイトのWebサービススキャンを実行するよう推奨して、その目的でWebサービステスト設計ファイル(*filename.wsd*)を作成します。WSDLファイルが使用できる場合と使用できない場合があります。

次の例に示すように、サービスを手動で作成できます。

1. デフォルトの **その他のサービス(Other Services)** サービスを右クリックし、 **サービスの追加(Add Service)** を選択します。
新しいサービス1(New Service 1)が左側のペインのWebサービスツリーに表示されます。
2. 認証が必要な場合は、 **WSセキュリティ(WS Security)** を選択し、必要な資格情報を入力します。
3. 新しいサービス1(New Service 1)を右クリックし、 **ポートの追加(Add Port)** を選択します。次に、 **SOAP 1.1** または **SOAP 1.2** のいずれかを選択します。
Webサービスツリーに 新しいポート1(New Port 1)が表示されます。
4. **ポートURL(Port URL)** ボックスに、サービスの正しいURLを入力します。

5. 新しいポート1(New Port 1)]を右クリックし、**操作の追加(Add Operation)]**を選択します。



注記: サービス名、ポート名、または操作名を変更するには、名前をダブルクリックします。

6. SOAPエンベロープを含むファイルをインポートするか(おそらくWeb Proxyツールを使用して取得)、開発者から取得したSOAPエンベロープを **XML** タブにコピーして貼り付けることができます。
プロキシキャプチャからインポートする場合、SOAPアクションはHTTPヘッダにあります (Soapaction=<action_name>)。
7. 必要に応じて、**スキーマフィールド(Schema Fields)]** タブまたは **XML** タブを使用して値を変更します。
8. サービスをテストするには、**送信(Send)]** または **すべて実行(Run All)]** のいずれかをクリックします。

Global Values Editor

頻繁に発生する操作の名前/値パラメータのライブラリを作成できます。WSDLファイルをインポートした後、**自動値の設定(Set Auto Values)]** をクリックすると、Web Service Test Designer は、WSDL操作に含まれるパラメータの名前をグローバル値ファイルで検索します。一致する名前が見つかり、関連付けられた値がファイルからパラメータ値フィールドに挿入されます。



グローバル値を追加するには:

1. **編集(Edit)] > [Global Values Editor]** をクリックします。
Global Values Editorが開き、GlobalValuesDefault.xprという名前のデフォルトのxmlパラメータレジストリ(xpr)ファイルの内容が表示されます。
2. **追加(Add)]** をクリックします。
これにより、デフォルト名 [Name]とデフォルト値 [Value]のエントリが作成されます。
3. エントリの任意の場所をクリックし、デフォルトを実際の名前と値で置き換えます。
4. ステップ2-3を繰り返して、追加のエントリを作成します。
5. 次のいずれかを実行します。
 - **[OK]** をクリックして、ファイルを保存して閉じます。
 - **名前を付けて保存(Save As)]** をクリックして、別のファイル名または場所を使用し、ファイルを作成して閉じます。

自動値の使用

パラメータごとに特定の値を手動で入力することの代替方法として、自動値機能を使用します。Web Service Test Designerは各パラメータを分析し、サービス要件を満たす可能性がある値を挿入します。これにより、大規模なWebサービスを扱う際に大幅に時間を節約できます。

WSDLファイルを選択した後:

1. オートフィルを使用する各操作の横のチェックボックスをオンにします。
2. **自動値の設定(Set Auto Values)]**  をクリックします。
「デフォルト値を定義済みのグローバル値に置き換えますか?(Would you like the default values to be replaced with the defined global values?)」というメッセージが表示されます。
[はい(Yes)] をクリックすると、手動で入力した値は消去されます。また、任意の操作のパラメータ名がグローバル値ファイル内のパラメータ名と一致する場合は、その操作で通常生成される値がファイル内の関連付けられた値で置き換えられます。
[いいえ(No)] をクリックすると、機能は終了します。
3. **[Yes]** をクリックします。
4. **すべてのテストを実行(Run All Tests)]**  をクリックします。
Web Service Test Designerは、各操作に挿入された値とともにサービス要求を送信します。
5. **テスト結果(Test Results)]** タブ(ウィンドウの下部)をクリックします。
6. エラーを返す操作があった場合は、その操作をダブルクリックして **要求(Request)]** ペインで開き、値を手動で入力します。

参照情報

["Global Values Editor" 前のページ](#)

操作のインポートとエクスポート

操作とそれらの割り当てられた値のライブラリを構築して、他のWebサービスの設計を素早く変更したり、これらのコンポーネントを他の開発者またはテスト担当者と交換したりすることができます。各モジュールは、前の例で使った次の要求のようなXMLファイルとして保存されます。

```
<Envelope >
  <Header />
  <Body>
    <GetQuote >
      <symbol>MFGP</symbol>
    </GetQuote>
  </Body>
</Envelope>
```

操作を保存またはインポートするには:

1. 左側のペインで操作を選択します。
2. **要求のインポート(Import Request)]**  をクリックして操作をロードします。
3. **要求のエクスポート(Export Request)]**  をクリックして操作を保存します。

設計のテスト

任意の、またはすべての操作の設定をいつでもテストできます。

WSDLをインポートした後、**すべてのテストを実行(Run All Tests)]**をクリックします。

Run All Tests

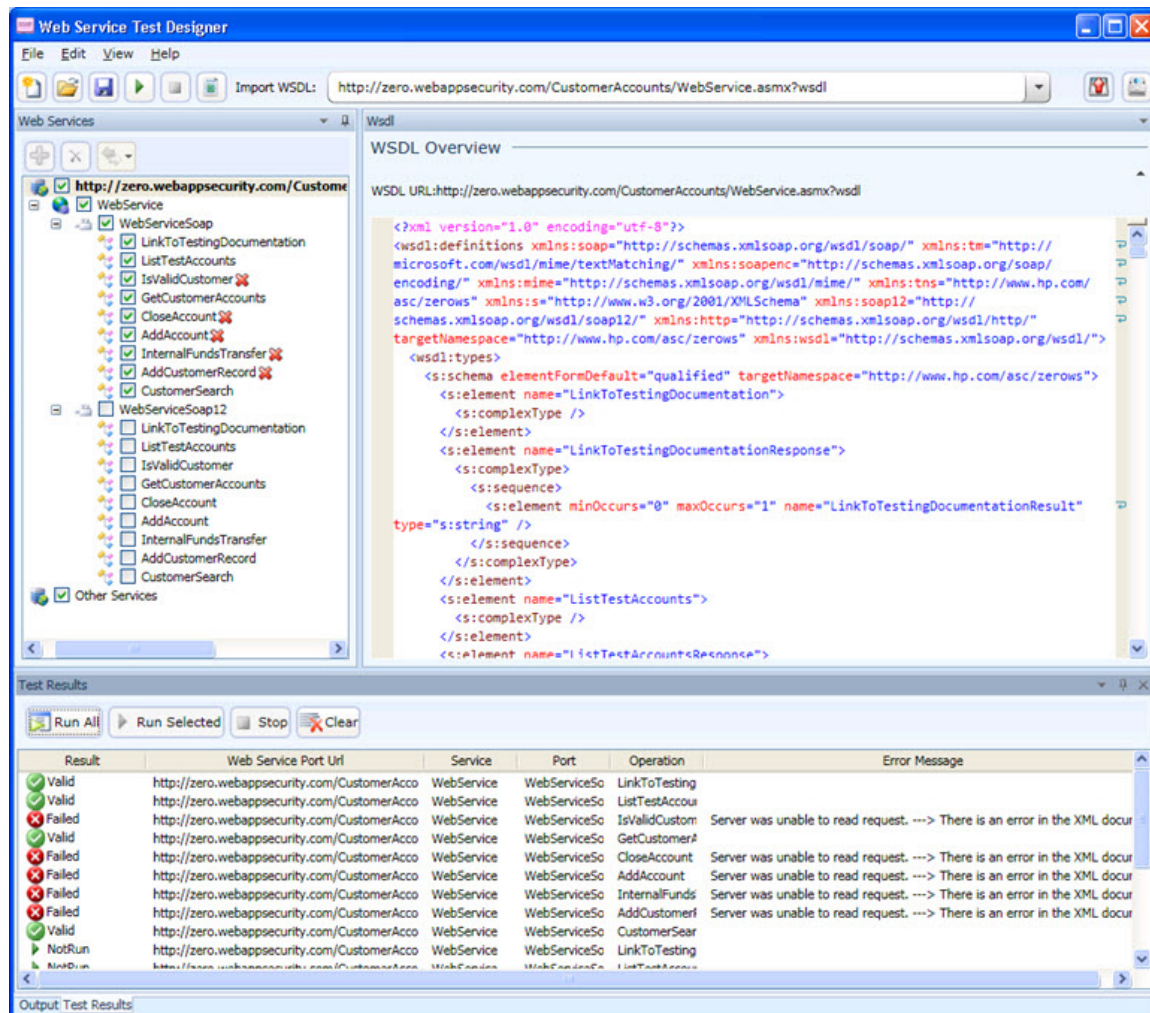


デザイナは、選択したすべての操作の送信を試み、結果を表示します。

特別な **テスト結果(Test Results)]** ペインを開くには、ステータスバーの **テスト結果(Test Results)]** をクリックします。

テスト結果のイメージ

次のイメージは、Web Service Test Designerでのテスト結果を示しています。



テスト結果[Test Results] ペインには、次の情報が表示されます。

- **結果(Result)]**-テスト結果。可能性がある値は次のとおりです。
 - 有効(Valid)] : サーバエラーまたはSOAP障害なしで操作が成功しました。
 - 未実行(Not Run)] : 操作が選択されなかったか(チェックボックスがオンではない)、操作が送信される前に 停止(Stop)] ボタンが押されたため、操作は送信されませんでした。
 - 保留中(Pending)] : 実行(Run)] ボタンが押されましたが、操作がまだ送信されていません。
 - 失敗(Failed)] : 要求が成功しなかった、サーバがエラーメッセージを返した、またはSOAP障害が受信されたのいずれかです。
- **WebサービスポートURL(Web Service Port URL)]**-項目に関連付けられているURL
- **サービス(Service)]**-項目に関連付けられているサービス
- **ポート(Port)]**-項目に関連付けられているポート

- **操作(Operation)]**-項目が表示操作
- **エラーメッセージ(Error Message)]**-エラーの説明

テスト結果(Test Results)] ツールバーには、次のボタンがあります。

- **すべて実行(Run All)]**-デザイナは、チェックされた各操作に対してサービス要求を送信します。
- **選択実行(Run Selected)]**-デザイナは、テスト結果(Test Results)] ペインで選択した操作に対してサービス要求を送信します。
- **停止(Stop)]**-サービス要求の送信をキャンセルします。
- **クリア(Clear)]**-テスト結果(Test Results)] ペインからすべての項目を削除します。

テスト結果(Test Results)] ペインで項目をダブルクリックすると、デザイナによってスキーマフィールド(Schema Fields)] ペインで関連する操作が強調表示され、そこで各パラメータの値を入力できます。

操作が強調表示された選択済みエラーのイメージ

次のイメージは、スキーマフィールド(Schema Fields)] ペインに表示された選択済みエラーとその操作を示しています。

The screenshot displays the Web Service Test Designer application. The top pane shows the 'Web Services' tree with 'IsValidCustomer' selected. The middle pane shows the 'Request - Operation: IsValidCustomer' with a 'Soap Action' and a 'Schema' section. The 'Schema' section shows a tree structure with 'Envelope', 'Header', 'Any (array)', and 'Body'. The 'Body' section contains 'IsValidCustomer' with fields 'name' and 'pin'. The bottom pane shows the 'Test Results' table with a 'Failed' result for the 'IsValidCustomer' operation. The error message is 'Server was unable to read request. ---> There is an error in the XML document. ---> Input string was not valid at line 1, column 1.' The 'Output Test Results' pane is empty.

Result	WSDL	Service	Port	Operation	Error Message
Valid	http://	WebService	WebServiceSoap	LinkToTesting	
Valid	http://	WebService	WebServiceSoap	ListTestAccounts	
Failed	http://	WebService	WebServiceSoap	IsValidCustomer	Server was unable to read request. ---> There is an error in the XML document. ---> Input string was not valid at line 1, column 1.
Valid	http://	WebService	WebServiceSoap	GetCustomerAccounts	
Failed	http://	WebService	WebServiceSoap	CloseAccount	Server was unable to read request. ---> There is an error in the XML document. ---> Input string was not valid at line 1, column 1.
Failed	http://	WebService	WebServiceSoap	AddAccount	Server was unable to read request. ---> There is an error in the XML document. ---> Input string was not valid at line 1, column 1.
Failed	http://	WebService	WebServiceSoap	InternalFundsTransfer	Server was unable to read request. ---> There is an error in the XML document. ---> Input string was not valid at line 1, column 1.
Failed	http://	WebService	WebServiceSoap	AddCustomerRecord	Server was unable to read request. ---> There is an error in the XML document. ---> Input string was not valid at line 1, column 1.
Valid	http://	WebService	WebServiceSoap	CustomerSearch	
NotRun	http://	WebService	WebServiceSoap12	LinkToTesting	
NotRun	http://	WebService	WebServiceSoap12	ListTestAccounts	
NotRun	http://	WebService	WebServiceSoap12	IsValidCustomer	

設定(Settings)

Web Services Designerには、次の2つのカテゴリの設定があります。

- ["ネットワークプロキシ" 下](#)
- ["ネットワーク認証" 次のページ](#)

ネットワークプロキシ

ネットワークプロキシを設定するには:

1. **プロキシプロファイル(Proxy Profile)]** リストからプロファイルを選択します。
 - **直接(Direct)]**: プロキシサーバを使用しません。
 - **自動検出(Auto Detect)]**: WPAD (Web Proxy Autodiscovery)プロトコルを使用してプロキシ自動設定ファイルを探し、これを使用してブラウザのWebプロキシ設定を行います。
 - **システムプロキシを使用(Use System Proxy)]**: ローカルマシンからプロキシサーバ情報をインポートします。
 - **PACファイルを使用(Use PAC File)]**: PAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードします。次に、**[URL]** ボックスでファイルの場所を指定します。
 - **明示的なプロキシ設定を使用(Use Explicit Proxy Settings)]**: プロキシの明示的な設定 (Explicitly Configure Proxy)] セクションで指定した情報を使用し、プロキシサーバを介してインターネットにアクセスします。
 - **Mozilla Firefoxを使用(Use Mozilla Firefox)]**: Firefoxからプロキシサーバ情報をインポートします。

注記: ブラウザのプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Firefoxブラウザの接続設定が「プロキシを使用しない」に設定されている場合、プロキシは使用されません。

2. **PACファイルを使用(Use PAC File)]** を選択した場合は、**[URL]** ボックスにPACファイルの場所を入力します。
3. **明示的なプロキシ設定を使用(Use Explicit Proxy Settings)]** を選択した場合は、次の情報を入力します。
 - a. **サーバ(Server)]** ボックスにプロキシサーバのURLまたはIPアドレスを入力し、続いて **(ポート(Port)]** ボックスにポート番号(8080など)を入力します。
 - b. **タイプ(Type)]** リストから、プロキシサーバ経由のTCPトラフィックを処理するプロトコル(SOCKS4、SOCKS5、または標準)を選択します。
 - c. 認証が必要な場合は、**認証(Authentication)]** リストからタイプを選択します。

- 自動

注記: 自動検出を指定すると、スキャンの処理が遅くなります。把握している別の認証メソッドを指定すると、スキャンのパフォーマンスは大幅に向上します。

- 基本
- ダイジェスト
- Kerberos
- ネゴシエート(Negotiate)
- NTLM (NT LAN Manager)

4. プロキシサーバで認証が必要な場合は、適格なユーザ名とパスワードを入力します。
5. 特定のIPアドレス(内部テストサイトなど)にアクセスするためにプロキシサーバを使用する必要がない場合は、**プロキシをバイパスするサイト(Bypass Proxy For)** ボックスにアドレスまたはURLを入力します。エントリを区切る場合は、カンマを使用します。
6. **[Save]** をクリックします。

ネットワーク認証

サーバ認証が必要ない場合は、**方法(Method)]** リストから **なし(None)]** を選択します。

それ以外の場合は、認証方法を選択し、ネットワーク資格情報を入力します。認証メソッドは次のとおりです。

- ADFS CBT
- 自動
- 基本
- ダイジェスト
- Kerberos
- ネゴシエート(Negotiate)
- NTLM (NT LAN Manager)

クライアント証明書の使用

クライアント証明書認証を使用すると、ユーザはユーザ名とパスワードを入力するのではなく、クライアント証明書を提示することができます。ローカルマシンから証明書を選択することも、現在のユーザに割り当てられた証明書を選択することもできます。コンピュータに接続された共通アクセスカード(CAC)リーダーなどのモバイルデバイスからの証明書を選択することもできます。クライアント証明書を使用するには:

1. **プロキシでクライアント証明書を有効にする(Enable client certificate on proxy)]** チェックボックスをオンにします。
2. **クライアント証明書(Client Certificate)]** をクリックします。

SOAPクライアント証明書(Soap Client Certificate)] ウィンドウが開きます。

3. 次のいずれかを実行します。

- コンピュータにとってローカルで、コンピュータ上のすべてのユーザにとってグローバルな証明書を使用するには、**ローカルマシン(Local Machine)]**を選択します。
- コンピュータ上のユーザアカウントにとってローカルな証明書を使用するには、**現在のユーザ(Current User)]**を選択します。

注記: 共通アクセスカード(CAC)リーダで使用する証明書はユーザ証明書であり、現在のユーザ(Current User)]に保管されます。

4. 次のいずれかを実行します。

- 「個人」(「マイ」)証明書ストアから証明書を選択するには、ドロップダウンリストから **マイ(My)]**を選択します。
- 信頼されたルート証明書を選択するには、ドロップダウンリストで **ルート(Root)]**を選択します。

5. WebサイトではCACリーダを使用しますか。

- 「はい」の場合は、次の手順を実行します。
 - i. **証明書(Certificate)]** リストから、「(SmartCard)」というプレフィクスが付いた証明書を選択します。
選択した証明書に関する情報とPINフィールドが **証明書情報(Certificate Information)]** エリアに表示されます。
 - ii. PINが必要な場合は、**PIN] フィールド**にCACのPINを入力します。

注記: PINが必要な場合に、この時点でPINを入力しないと、スキャン中にPINの入力を求められるたびに、Windowsの **セキュリティ]** ウィンドウにPINを入力する必要があります。

iii. **テスト(Test)]** をクリックします。

正しいPINを入力した場合は、成功メッセージが表示されます。

- 「いいえ」の場合は、**証明書(Certificate)]** リストから証明書を選択します。
選択した証明書に関する情報が **証明書情報(Certificate Information)]** エリアに表示されます。

6. **OK]** をクリックします。

WSセキュリティ

次に示すさまざまなサービスを使用して、Webサービスポート内のすべての操作に関するセキュリティ設定を行えます。


- Webサービス(「["Webサービスの設定" 下](#)」を参照)
- Windows Communication Foundation (WCF) サービス(「["WCFサービス\(CustomBinding\)の設定" ページ367](#)」を参照)
- WCFサービス(フェデレーション) (「["WCFサービス\(フェデレーション\)の設定" ページ368](#)」を参照)
- WWCfサービス(WSHttpBinding) (「["WCFサービス\(WSHttpBinding\)の設定" ページ369](#)」を参照)

サービス詳細(Service Details)] リストから適切なサービスを選択し、要求された情報を入力します。



Webサービスの設定

トークンと呼ばれるセキュリティ資格情報がSOAP要求に入っている場合、Webサーバはその資格情報が真正であることを確認してから、Webサービスにアプリケーションの実行を許可できます。Webサービスのセキュリティをさらに高めるために、SOAPメッセージにはデジタル署名または暗号化を使用するのが一般的です。SOAPメッセージにデジタル署名することにより、転送中にメッセージが変更されていないことを確認できます。SOAPメッセージを暗号化すると、目的の受信者以外がメッセージの内容を読むのが困難になり、Webサービスのセキュリティを確保する上で役立ちます。



[WS-Security] タブ

1. セキュリティトークンを追加するには、 をクリックし、トークンタイプを選択して、要求された情報を入力します。
 - **ユーザ名 (UserName)]**。このトークンは、ユーザ名とパスワードを指定します。nonceを含めることの選択、認証のためにサーバにパスワードを送信する方法(テキスト(Text))、なし(None))、または【ハッシュ(Hash))】の指定、およびタイムスタンプを含めるかどうかの指定を行うことができます。
 - **X509証明書(X509 Certificate)]**。このトークンはX.509証明書に基づいています。VeriSign, Inc.などの認証局から証明書を購入するか、独自の証明書サービスを設定して証明書を発行することができます。ほとんどのWindowsサーバは、証明書を作成できる公開鍵インフラストラクチャ(PKI)に対応しています。その後、認証局に署名してもらるか、署名されていない証明書を使用できます。証明書を選択し、参照タイプ(BinaryCertificateTokenまたはReference)を指定します。
 - **Kerberos /Kerberos2]**。(Windows 2003またはXP SP1以降の場合)。Kerberosプロトコルは、オープンでセキュリティ保護されていないネットワーク上のユーザとサービスを相互に認証するために使用されます。共有秘密鍵を使用して、ユーザ資格情報を暗号化および署名します。Kerberosキー配布センター(KDC)と呼ばれるサードパーティが資格情報を認証します。認証後、ユーザはネットワーク上の1つ以上のサービスにアクセスするためにサービスチケットを要求できます。チケットには、ユーザの暗号化された認証済み識別情報が含まれます。チケットは、現在のユーザの資格情報を使用して取得されます。KerberosトークンとKerberos2トークンの主な違いは、Kerberos2がセキュリティサポートプロバイダーインターフェース(SSPI)を使用する点です。したがって、

クライアントの識別情報を偽装するために昇格された特権は必要ありません。さらに、Kerberos2セキュリティトークンは、Webファームで実行されているWebサービスに送信されるSOAPメッセージを保護するために使用できます。ホストとドメインを指定します。

- **SAMLトークン(SAML Token)]**。SAML (Security Assertion Markup Language) は、インターネットを通じてビジネスパートナー間で、アサーションと呼ばれるセキュリティ関連情報を交換するためのXML標準です。アサーションには、属性ステートメント、認証、決定ステートメント、および権限付与決定ステートメントを含めることができます。
[ファイルからロード(Load from file)]をクリックして、SAML証明書参照します。[証明書(Certificate)]をクリックして、証明書をインポートします。最後に、証明書参照タイプ(X509データまたはRSA)を選択します。
2. メッセージ署名を追加するには、をクリックして、要求された情報を入力します。
- **署名トークン(Signing token)]**。署名に使用するトークン(通常はX.509タイプ)。追加されたすべてのトークンのリストから選択します。
 - **正規化アルゴリズム(Canonicalization algorithm)]**。正規化に使用するアルゴリズムのURL。ドロップダウンリストには、一般的なアルゴリズムが表示されます。使用する値が不明な場合は、デフォルトのままにします。
 - **変換アルゴリズム(Transform algorithm)]**。メッセージ署名に適用する変換アルゴリズムのURL。ドロップダウンリストには、一般的なアルゴリズムが表示されます。使用する値が不明な場合は、デフォルトのままにします。
 - **包含ネームスペースリスト(Inclusive namespaces list)]**。包含されるものとして扱われる、カンマで区切られたプレフィックスのリスト(オプション)。
 - **署名する情報(What to sign)]**。署名するSOAP要素(SOAP本文、タイムスタンプ、およびWS-Addressing)。
 - **XPath (オプション)(XPath (optional))]**。署名するメッセージ内の部分を指定するXPath。空白のままにすると、**署名オプション(Signature options)]** フィールドで選択した要素が署名されます。例: `//*[local-name(.)='Body']`
 - **トークン(オプション)(Token (optional))]**。署名するターゲットトークン。追加されたすべてのトークンのドロップダウンリストから選択します。ほとんどのサービスでは、このフィールドは空のままにする必要があります。
3. メッセージ暗号化を追加するには、をクリックして、要求された情報を入力します。
- **トークンの暗号化(Encrypting token)]**。暗号化に使用するトークン(通常はX.509タイプ)。以前に作成したすべてのトークンのリストから選択できます。
 - **暗号化タイプ(Encrypting type)]**。宛先要素全体を暗号化するか、そのコンテンツのみを暗号化するかを示します。
 - **鍵アルゴリズム(Key algorithm)]**。セッション鍵の暗号化に使用するアルゴリズム: RSA15またはRSAOAEP。
 - **セッションアルゴリズム(Session algorithm)]**。SOAPメッセージの暗号化に使用するアルゴリズム。共通値のリストから選択できます。

- **XPath (オプション)(XPath (optional))**。暗号化するメッセージの部分を示す XPath。空白のままにすると、SOAP本文だけが暗号化されます。
- **トークン(オプション)(Token (optional))**。暗号化されたトークンの名前。追加されたすべてのトークンのリストがドロップダウンボックスに表示されます。ほとんどのサービスでは、このフィールドは空のままにする必要があります。

4. 上下の矢印   を使用して、セキュリティ要素を優先度の順に配置します。

WS Addressing] タブ

WS-Addressing] タブを使用して、サービスでWS-Addressingを使用するかどうか、および使用する場合はバージョン番号を指定します。

WCFサービス(CustomBinding)の設定

WCFサービス(CustomBinding)により、最高レベルのカスタマイズが可能です。WCF customBinding標準に基づいているため、これを使用するとほとんどのWCFサービスと共に、WS - `<spec_name>`仕様を使用するJavaベースのサービスなど、他のプラットフォーム上のサービスをテストできます。

トランスポート(Transport)]。[HTTP]、[HTTPS]、または [AutoSecuredHTTP] を選択します。名前付きパイプとTCPトランスポートはサポートされていません。

エンコーディング(Encoding)]。[テキスト(Text)]、[MTOM]、または [WCFバイナリ(WCF Binary)] を選択します。

セキュリティ(Security)]。適切なリストから認証モードとブートストラップポリシーを選択します。

ネットセキュリティ(Net Security)]。ストリームセキュリティの種類: [なし(None)]、[Windows ストリームセキュリティ(Windows stream security)]、または [SSLストリームセキュリティ(SSL stream security)]。

信頼性の高いメッセージング(Reliable Messaging)]。信頼性の高いメッセージングを使用するには **有効(Enabled)**] を選択し、次に **順序あり(Ordered)**] または **順序なし(Not Ordered)**] のいずれかの形式を選択します。

識別情報(Identities)]。バインディングと証明書の識別情報を提供します:

- **ユーザ名(Username)**] と **パスワード(Password)**]
- **サーバ証明書/クライアント証明書(Server Certificate/Client certificate)**]。サーバまたはクライアントの識別情報を提供する証明書。 **参照(Browse)**] ボタンを使用して、証明書の選択(Select Certificate)] ダイアログボックスを開きます。
- **予期されるDNS(Expected DNS)**]、**SPN**]、および **UPN**]。DNS、SPN、またはUPN による、サーバの予期される識別情報。localhost、IPアドレス、またはサーバ名を指定できます。

クライアント Windows 識別 情報 (Client Windows Identity)]。クライアント Windows の識別 情報を入力します。

- **現在のユーザ (Current User)]**。マシンにログオンしたユーザの識別 情報。
- **カスタムユーザ (Custom User)]**。ユーザ名、パスワード、およびドメインを指定します。

詳細設定 (Advanced)] をクリックして、**詳細設定 (Advanced Settings)]** ダイアログボックスを開きます。詳細については、「["セキュリティの詳細設定" ページ371](#)」を参照してください。

WCF サービス (フェデレーション) の設定

WCF サービス (フェデレーション) を使用する場合、クライアントは Security Token Service (STS) に対して認証を行い、トークンを取得します。クライアントはトークンを使用してアプリケーションサーバに対する認証を行います。

サーバ

- **トランスポート (Transport)]**。トランスポートタイプ: HTTP または HTTPS。
- **エンコーディング (Encoding)]**。サーバのエンコーディングポリシー: テキスト または MTOM。

Security

- **認証モード (Authentication mode)]**。認証の可能なモードのドロップダウンリスト ([AnonymousForCertificate]、 [MutualCertificate] など)。
- **ブートストラップポリシー (Bootstrap Policy)]**。Secure Conversation 認証の可能なブートストラップポリシーのドロップダウンリスト ([SspiNegotiated]、 [UserNameOverTransport] など)。

識別 情報

バインディングと証明書 の識別 情報:

- **サーバ証明書 (Server certificate)]**。サーバの識別 情報を提供する証明書。 **参照 (Browse)]** ボタンを使用して、**証明書の選択 (Select Certificate)]** ダイアログボックスを開きます。
- **予期される DNS (Expected DNS)]**。DNS による、サーバの予期される識別 情報。 localhost、IP アドレス、またはサーバ名を指定できます。

STS (Security Token Service) の詳細

- **エンドポイント アドレス (Endpoint address)]**。STS のエンドポイント アドレス。 localhost、IP アドレス、またはサーバ名を指定できます。
- **バインディング (Binding)]**。STS に接続するバインディングを参照するシナリオ。

詳細設定 (Advanced)] をクリックして、**詳細設定 (Advanced Settings)]** ダイアログボックスを開きます。詳細については、「["セキュリティの詳細設定" ページ371](#)」を参照してください。

WCFサービス(WSHttpBinding)の設定

WCFサービス(WSHttpBinding)を使用すると、認証の種類を なし(None)]、[Windows]、[証明書(Certificate)]、または ユーザ名(メッセージ保護)(Username (message protection))]の中から選択できます。クライアント認証の種類の一覧からオプションを選択します。次に説明するように、選択に応じて必要な追加情報が決まります。

Type	パラメータ(Parameters)
なし	<ul style="list-style-type: none">• サーバ資格情報をネゴシエートする(Negotiate server credentials)]。Webサービスの証明書をサーバとネゴシエートします。サーバのDNS情報を指定することもできます。• サービス証明書を指定する(Specify service certificate)]。サービスの証明書の場所。このオプションを選択した場合、サーバ資格情報をネゴシエートする(Negotiate service credentials)]オプションは関係ありません。• 予想されるサーバDNS(Expected server DNS)]。ドメインネームシステムによる、サーバの予想される識別情報。localhost、IPアドレス、またはサーバ名を指定できます。また、証明書の発行に使用される一般名とすることもできます。• セキュアなセッションを有効にする(Enable secure session)]。証明書タイプ認証を使用したセキュアなセッションを許可します。
Windows	<ul style="list-style-type: none">• 予想されるサーバ識別情報(Expected server identity)]。サービスプリンシパル名 (SPN)またはユーザプリンシパル名 (UPN)。SPNを指定すると、SPNと、SPNに関連付けられた特定のWindowsアカウントとによってサービスが識別されます。UPNを指定すると、サービスは特定のWindowsユーザアカウントで実行されることとなります。ユーザアカウントは、現在ログオンしているユーザになるか、特定のユーザアカウントで実行されているサービスになるかのいずれかです。• クライアントWindows識別情報(Client Windows identity)]。クライアントWindowsの識別情報。<ul style="list-style-type: none">• 現在のユーザ(Current User)]。マシンにログオンしているユーザの資格情報を使用します。• カスタムユーザ(Custom User)]。ユーザ資格情報(ユーザ名、パスワード、およびドメイン)を入力し、必要に応じて偽装レベルを選択します(サーバがクライアントのコンテキストで実行できる操作がこれで決まります)。表示レベルは次のとおりです。<ul style="list-style-type: none">◦ なし(None)]-レベルが選択されません。◦ 匿名(Anonymous)]-サーバは、クライアントを偽装したり、識

Type	パラメータ(Parameters)
	<p>別したりすることはできません。</p> <ul style="list-style-type: none"> 識別 (Identification)] -サーバはクライアントの識別情報と特権を取得できますが、クライアントを偽装することはできません。 偽装 (Impersonation)] -サーバは、ローカルシステム上でクライアントのセキュリティコンテキストを偽装できます。 委任 (Delegation)] -サーバはリモートシステム上でクライアントのセキュリティコンテキストを偽装できます。 <ul style="list-style-type: none"> セキュアなセッションを有効にする(Enable secure session)]。Windowsタイプ認証を使用したセキュアなセッションを許可します。
証明書	<ul style="list-style-type: none"> クライアント証明書(Client certificate)]。クライアント証明書の場所。 参照(Browse)] ボタンを使用して、 証明書の選択(Select Certificate)] ダイアログボックスを開きます。 サーバ資格情報をネゴシエートする(Negotiate server credentials)]。Webサービスの証明書をサーバとネゴシエートします。サーバのDNS情報を指定することもできます。 サービス証明書を指定する(Specify service certificate)]。サービスの証明書の場所。このオプションを選択した場合、 サーバ資格情報をネゴシエートする(Negotiate server credentials)] オプションは無効です。 予想されるサーバDNS(Expected server DNS)]。DNSによる、サーバの予想される識別情報。localhost、IPアドレス、またはサーバ名を指定できます。また、証明書の発行に使用される一般名とすることもできます。 セキュアなセッションを有効にする(Enable secure session)]。証明書タイプ認証を使用したセキュアなセッションを許可します。
ユーザ名 (メッセージ保護)(User Name (Message Protection))	<ul style="list-style-type: none"> ユーザ名、パスワード(Username, Password)]。クライアントの認証資格情報。 サーバ資格情報をネゴシエートする(Negotiate server credentials)]。Webサービスの証明書をサーバとネゴシエートします。サーバのDNS情報を指定することもできます。 サービス証明書を指定する(Specify service certificate)]。サービスの証明書の場所。このオプションを選択した場合、 サーバ資格情報をネゴシエートする(Negotiate server credentials)] オプションは無効です。 予想されるサーバDNS(Expected server DNS)]。DNSによる、サーバの予想される識別情報。localhost、IPアドレス、またはサーバ

Type	パラメータ(Parameters)
	<p>名を指定できます。また、証明書の発行に使用される一般名とすることもできます。</p> <ul style="list-style-type: none"> • セキュアなセッションを有効にする(Enable secure session)]。ユーザ名タイプ認証を使用したセキュアなセッションを許可します。

セキュリティの詳細設定

このダイアログボックスでは、次のタブでテストのセキュリティ設定をカスタマイズできます。

[エンコーディング(Encoding)] タブ

[エンコーディング(Encoding)] タブには、次のオプションがあります。

- **[エンコーディング(Encoding)]**。メッセージに使用するエンコーディングタイプ(**テキスト(Text)**]、**[MTOM]**、または **[WCFバイナリ(WCF Binary)]**)。
- **[WS-Addressingバージョン(WS-Addressing version)]**。選択したエンコーディングのWS-Addressingのバージョン(**なし(None)**]、**[WSA 1.0]**、または **[WSA 04/08]**)。

高度な標準(Advanced Standards)] タブ

高度な標準(Advanced Standards)] タブには、次のオプションがあります。

- **[信頼性の高いメッセージング(Reliable messaging)]**。WS-ReliableMessaging仕様を実装するサービスの信頼性の高いメッセージングを有効にします。メッセージに使用するエンコーディングタイプ(**テキスト(Text)**]、**[MTOM]**、または **[WCFバイナリ(WCF Binary)]**)。
- **[信頼性の高いメッセージングの順序付け(Reliable messaging ordered)]**。信頼できるセッションに順序を付けるかどうかを示します。
- **[信頼性の高いメッセージングのバージョン(Reliable messaging version)]**。メッセージに適用されるバージョン: WSReliableMessagingFebruary2005またはWSReliableMessaging11。
- **[アドレス経由で指定する(Specify via address)]**。メッセージを中間サービスに送信し、そこから実際のサーバに送信されます。これは、デバッグプロキシにメッセージを送信する場合にも適用される場合があります。これは、WCF clientVia動作に対応しています。これは、メッセージが実際に送信される物理アドレスを、メッセージの送信先の論理アドレスと区別する場合に便利です。
- **[アドレス経由(Via address)]**。メッセージの送信先の論理アドレス。最終サーバの物理名または任意の名前を指定できます。SOAPメッセージに次のように表示されます。

```
<wsa:Action>http://myLogicalAddress<wsa:Action>
```

論理アドレスは、ユーザインタフェースから取得されます。デフォルトでは、WSDLで指定されたアドレスです。このフィールドを使用して、このアドレスを上書きできます。

セキュリティ(Security)] タブ

セキュリティ(Security)] タブには、次のオプションがあります。

- **セキュアなセッションを有効にする(Enable secure session)]**。WS-SecureConversation 標準を使用してセキュリティコンテキストを確立します。
- **サービス資格情報をネゴシエートする(Negotiate service credentials)]**。サービスのセキュリティをネゴシエートするために、WCF専用ネゴシエーションを許可します。
- **デフォルトのアルゴリズムスイート(Default algorithm suite)]**。対称/非対称暗号化に使用するアルゴリズム。アルゴリズムのリストは、WCFのSecurityAlgorithmSuite設定から入力されます。
- **保護レベル(Protection level)]**。SOAP本文を暗号化/署名するかどうかを指定します。指定可能な値は、なし(None)]、署名(Sign)]、および 暗号化と署名(Encrypt And Sign)](デフォルト)です。
- **メッセージ保護の順序(Message protection order)]**。署名と暗号化の順序。暗号化前に署名(Sign Before Encrypt)]、暗号化前に署名し、署名を暗号化(Sign Before Encrypt and Encrypt Signature)]、署名前に暗号化(Encrypt Before Sign)]から選択します。
- **メッセージセキュリティバージョン(Message security version)]**。WS-Securityセキュリティバージョン。また、メッセージの派生キーが必須かどうかを指定することもできます。
- **セキュリティヘッダレイアウト(Security header layout)]**。メッセージヘッダのレイアウト: Strict]、[ax]、[ax Timestamp First]、または [ax Timestamp Last]。
- **キーエントロピーモード(Key entropy mode)]**。セキュリティキーのエントロピーモード。可能な値は、クライアントエントロピー(Client Entropy)]、セキュリティエントロピー(Security Entropy)]、および 結合エントロピー(Combined Entropy)]です。
- **セキュリティコンテキストのキャンセルが必要(Require security context cancellation)]**。セキュリティコンテキストのキャンセルが必要かどうかを示します。このオプションを無効にすると、WS-SecureConversationセッションでステートフルなセキュリティトークンが有効になっている場合、そのトークンが使用されます。
- **タイムスタンプを含める(Include timestamp)]**。ヘッダにタイムスタンプを含めます。
- **返信時にシリアル化署名トークンを許可する(Allow serialized signing token on reply)]**。返信でシリアル化署名トークンを送信できます。
- **署名の確認が必要(Require signature confirmation)]**。応答で署名確認を送信するようにサーバに指示します。

注記: 次の4つのオプションは、X.509証明書を使用する場合にのみ適用されます。

- **X509包含モード(X509 Inclusion Mode)]**。X.509証明書をいつ含めるかを指定します: 常に受信者に(Always to Recipient)]、なし(Never)]、一度(Once)]、常にイニシエータに(Always To Initiator)]。
- **X509参照スタイル(X509 Reference Style)]**。証明書の参照方法を指定します: 内部(Internal)]または 外部(External)]。
- **X509には派生キーが必要(X509 require derived keys)]**。X.509証明書が派生キーを必要とするかどうかを示します。

- **X509キー識別子句の種類(X509 key identifier clause type)]**。X.509キーの識別に使用される句の種類: **任意(Any)]**、**拇印(Thumbprint)]**、**発行者シリアル(Issuer Serial)]**、**サブジェクトキー識別子(Subject Key Identifier)]**、**生データキー識別子(Raw Data Key Identifier)]**。

[HTTP & プロキシ(HTTP & Proxy)] タブ

[HTTP & プロキシ(HTTP & Proxy)] タブには、次のオプションがあります。

- **転送モード(Transfer mode)]**。要求/応答の転送方法です。指定可能な値は、**バッファ(Buffered)]**、**ストリーム(Streamed)]**、**ストリーム要求(Streamed Request)]**、および**ストリーム応答(Streamed Response)]**です。
- **最大応答サイズ(KB) (Max response size (KB))]**。連結前の応答の最大サイズ。
- **クッキーを許可する(Allow cookies)]**。クッキーを有効にするか無効にするかを示します。
- **キープアライブが有効(Keep-Alive enabled)]**。キープアライブ接続を有効にするか無効にするかを示します。
- **認証スキーム(Authentication scheme)]**。HTTP認証方法: **なし(None)]**、**ダイジェスト(Digest)]**、**ネゴシエート(Negotiate)]**、**[NTLM]**、**統合 Windows 認証(Integrated Windows Authentication)]**、**基本(Basic)]**、または **匿名(Anonymous)]**。
- **レルム(Realm)]**。URL形式の認証スキームのレルム。
- **クライアント証明書が必要(Require client certificate)]**。SSLトランスポートに証明書を必要とするかどうかを示します。
- **デフォルトのWebプロキシを使用する(Use default web proxy)]**。マシンのデフォルトのプロキシ設定を使用するかどうかを示します。
- **ローカルでプロキシをバイパスする(Bypass proxy on local)]**。サービスがローカルマシン上にあるときにプロキシを無視するかどうかを示します。
- **プロキシアドレス(Proxy address)]**。プロキシサーバのURL。
- **プロキシ認証スキーム(Proxy authentication scheme)]**。プロキシのHTTP認証方法: **ダイジェスト(Digest)]**、**ネゴシエート(Negotiate)]**、**[NTLM]**、**基本(Basic)]**、または **匿名(Anonymous)]**。

ドキュメントのフィードバックを送信する

このドキュメントに関するご意見は、電子メールでドキュメントチームまでお寄せください。

注記: 弊社製品に関する技術的な問題が発生した場合は、ドキュメントチームに電子メールを送信しないでください。代わりに、<https://www.microfocus.com/support>に問い合わせせてサポートを受けてください。

このコンピュータに電子メールクライアントが設定されている場合は、前のドキュメントチームに連絡するためのリンクをクリックすると、表題の行に以下の情報が付いた状態で電子メールウィンドウが開きます。

ツールガイド (Dynamic Application Security Testing 25.4.0) に関するフィードバック

電子メールにフィードバックを追加して、[送信]をクリックします。

電子メールクライアントが使用できない場合は、前の情報をWebメールクライアントの新しいメッセージにコピーして、fortifydocteam@opentext.comにフィードバックを送信してください。

皆様のご意見をお待ちしております。