HP Unified Functional Testing

ソフトウェア・バージョン： 12.01

UFT セキュリティ・リファレンス

ドキュメント・リリース日：2014 年 7 月
ソフトウェア・リリース日：2014 年 7 月

ご注意

保証

HP 製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載は、追加保証を提供するものではありません。ここに含まれる技術的、編集上の誤り、または欠如について、HP はいかなる責任も負いません。

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。

権利の制限

機密性のあるコンピューターソフトウェアです。これらを所有、使用、または複製するには、HP からの有効な使用許諾が必要です。商用コンピューターソフトウェア、コンピューターソフトウェアに関する文書類、および商用アイテムの技術データは、FAR12.211 および 12.212 の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

商標について

Adobe®は、Adobe Systems Incorporated (アドビシステムズ社) の登録商標です。

Intel®は、Intel Coporationの米国およびその他の国における登録商標です。

OracleとJavaは、Oracle Corporationおよびその関連会社の登録商標です。

Microsoft®およびWindows®は、米国におけるMicrosoft Corporationの登録商標です。

UNIX®は、The Open Groupの登録商標です。

ドキュメントの更新情報

このマニュアルの表紙には、以下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の番号は、ソフトウェアのバージョンを示します。
  - ピリオドの前の数字は、メジャー・リリース番号を特定します。
  - ピリオドの後の最初の数字は、マイナー・リリース番号を特定します。
  - ピリオドの後の 2 番目の数字は、マイナー・マイナー・リリース番号を特定します。
- ドキュメントリリース日は、ドキュメントが更新されるたびに変更されます。
- ソフトウェアリリース日は、このバージョンのソフトウェアのリリース期日を表します。

更新状況、またはご使用のドキュメントが最新版かどうかのご確認には、次のサイトをご利用ください。

http://support.openview.hp.com/selfsolve/manuals

このサイトを利用するには、HP Passport への登録とサインインが必要です。HP Passport ID の登録は、次の Web サイトから行なうことができます。

http://h20229.www2.hp.com/passport-registration.html（英語サイト）

または、HP Passport のログインページの [New users - please register] リンクをクリックします。

適切な製品サポートサービスをお申し込みいただいたお客様は、更新版または最新版をご入手いただけます。詳細は、HP の営業担当にお問い合わせください。

サポート

以下の HP ソフトウェアのサポート Web サイトを参照してください。

http://support.openview.hp.com/

このサイトでは、HP のお客様窓口のほか、HP ソフトウェアが提供する製品、サービス、およびサポートに関する詳細情報をご覧いただけます。

HP ソフトウェアオンラインではセルフソルブ機能を提供しています。お客様のビジネスを管理するのに必要な対話型の技術サポートツールに、素早く効率的にアクセスできます。HP ソフトウェアサポートのサイトでは、次のようなことができます。

- 関心のあるナレッジドキュメントの検索
- サポートケースの登録とエンハンスメント要求のトラッキング
- ソフトウェアパッチのダウンロード
- サポート契約の管理
- HP サポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部を除き、サポートのご利用には HP Passport ユーザとしてご登録の上、ログインしていただく必要があります。また、多くのサポートのご利用には、有効なサポート契約が必要です。サポートのアクセスレベルに関する詳細は、

http://support.openview.hp.com/access_level.jsp

HP Passport ID を登録するには、次の Web サイトにアクセスしてください。

http://h20229.www2.hp.com/passport-registration.html（英語サイト）

目次

はじめに

概要

UFT セキュリティ・リファレンスへようこそ

本書は，ユーザが最新の企業において，Unified Functional Testing（UFT）インスタンスをセキュアな方法でデプロイして管理する際に役に立つガイドです。本書の目的は，最新の企業のセキュリティ・ニーズを満たすために UFT が提供するさまざまな機能に関して，ユーザが十分に情報を得た上で意思決定を行えるようにすることです。

企業のセキュリティ要件は日々進化しています。本書は，このように厳しい要件を満たすために HP が行った最善の努力の結果です。本書で扱っていない追加のセキュリティ要件がある場合は，HP サポート・チームと協力してサポート・ケースを開いてドキュメント化してください。それらの本書の改訂時に随時追加される予定です。

セキュアな方法による UFT のインストールと使用

UFT とは，ビジネス・ネットワーク内の 1 つのコンピュータまたは複数のコンピュータにインストールされたデスクトップ・アプリケーションです。このため，UFT のセキュリティ関連の問題は，その他の Windows ベース・アプリケーションのセキュリティ関連問題とよく似ています。

UFT は，ユーザ・アクションやネットワーク通信の記録に使用される可能性がある製品です。このため，UFT の実行は，機密性の高い情報が含まれないか，あるいはそのような情報へのアクセス手段がない専用のテスト・マシン上で行うことを強く推奨します。また，UFT を使用する前に，ラボ・ネットワーク・トポロジとアクセス権限を十分に確認する必要があります。

UFT のインストールおよび実行時には，特定の権限が必要になります。これらの権限のリストについては，『Unified Functional Testing インストール・ガイド』を参照してください。

UFT のインストールでは，次のセキュリティ設定が提供されています。

- コンピュータのユーザ・アカウント制御（UAC）を有効にした状態で，UFT をインストールおよび実行できます。
- インストール中に，リモート・コンピュータが UFT にアクセスして ALM からテストを実行したり，あるいはオートメーションを使用してテストを実行できるように，DCOM を設定するかどうかを指定できます。これらの設定はインストール後に行うこともできます。
- テスト中のアプリケーションに関する重要な機密情報を安全に格納できます。

次の各項では，UFT の使用時に発生する可能性があるセキュリティ上の問題について説明します。

インストールとデプロイメントのセキュリティ

UFT は UAC を有効にした状態でインストールできます。これには，前提条件となるすべてのソフトウェアに加えて，すべての UFT アドイン，UFT Add-in for ALM，インストール設定が含まれています。

インストールの実行時には，次の点に注意してください。

1. インストールの一部として UFT Add-in for ALM をインストールする場合，コンピュータの UAC が有効になっているときは，アドインの追加インストールは UFT のインストール後に実行する必要があります。

2. UFT と ALM 統合用の DCOM 設定を行うオプションは，標準設定で有効になっています。このオプションをクリアする場合は，インストール・ウィザードで行います。

セキュリティで保護されたインストールとデプロイメントの詳細については，『Unified Functional Testing インストール・ガイド』の「エンタープライズ・デプロイメント」の項を参照してください。DCOM 設定に関する追加情報については，次の項でも説明します。

UFT を操作する際の DCOM 設定

DCOM 設定を行うと，外部コンピュータまたは ALM から UFT コンピュータを操作してテストを実行することができます。この設定は，インストール中に実行するか，インストール後に手動で実行します。これらの設定の詳細については，『Unified Functional Testing インストール・ガイド』を参照してください。

DCOM 設定では，次の 2 つのオプションが用意されています。

1. **ALM 統合を有効にする DCOM 設定：**これは，ALM プロジェクトが使用中のコンピュータにアクセスしてそのコンピュータ上でテストを実行できるようにする DCOM 設定です。

   注：UFT コンピュータに対するアクセス・レベルを特定するために，ALM プロジェクトで追加設定を行う必要があります。**「ALM への UFT 接続」**に関する次の項を参照してください。

2. **オートメーション・テスト実行を有効にする DCOM 設定：**これは，任意のコンピュータが UFT オートメーション・オブジェクト・モデルを使用して，テストを実行できるようにする DCOM 設定です。この設定を有効にすると，リモート・コンピュータから UFT コンピュータへのフル・アクセスが可能になるため，セキュリティ・リスクが発生する可能性があります。

注：ALM からテストを実行するか，オートメーションを使用してテストを実行するにはこれらの設定を行う必要があるため，その必要性を判断するには注意が必要です。

DCOM 設定を行う場合，UFT を実行しているコンピュータのセキュリティを確保するために，次の設定が推奨されます。

- DCOM 設定内で，範囲の広いグループ（Anonymous Logon，Everyone，Interactive，Network グループなど）に対する DCOM アクセス許可を削除します。
- 特定のグループまたはユーザにのみ，アクセス許可を付与します。

ALM への UFT 接続

注：本項は，関連する DCOM 設定を行って，UFT と ALM 間の通信を有効にしたユーザが対象です。上記の DCOM のアクセス許可に関する項を参照してください。

ALM への接続時に，UFT は ALM 内で割り当てられている特定のユーザ・アクセス許可に関係なく，「スーパー・ユーザ」アクセス許可レベルを使用します。これにより，ALM プロジェクトでの作業のためにどのような権限が割り当てられていても，ALM のすべての機能を使用できるようになります。

ALM 11.XX または ALM 12.XX 以降を使用している場合，標準設定のアクセス・レベルは異なります。

ALM サーバでは，このスーパー・ユーザ・アクセスを制御するサイト・パラメータを設定できます。

- **ALM 11.XX バージョンの場合：**ALM プロジェクトはパラメータ FORCE_PERMISSION（標準設定は［No］）を使用します。このパラメータを有効にすると，UFT 経由で ALM にログインする際にユーザ・アクセス許可がチェックされます。
- **ALM 12.XX バージョンの場合：**ALM プロジェクトはパラメータ ALLOW_LEGACY_INTEGRATION_MODE を使用します。標準設定ではこのパラメータは無効になっているため，UFT 経由での ALM 内のアクティビティは，ALM プロジェクトで割り当てられているユーザ・アクセス許可によって制限されます。

これらのパラメータの詳細については，『ALM 管理者ガイド』を参照してください。

UFT 操作時のテスト情報のセキュリティ保護

テスト対象アプリケーションにアクセスするために，テストにユーザ名やパスワードなどの機密性の高い情報を含めなければならない場合があります。

UFT では，このようなデータのセキュリティを次の方法で保護できます。

1. GUI テストでは，通常の **Set** メソッドではなく，**SetSecure** テスト・オブジェクト・メソッドを使用してパスワードを入力します。

   注：このメソッドは完全にパスワードのセキュリティを保護するものではなく，テストの実行中に画面またはアプリケーションでパスワードを非表示にするために使用されます。

   SetSecure メソッドの詳細については，『UFT Object Model Reference for GUI Testing』を参照してください。

2. パスワード・エンコーダ・ツールを使用してパスワードを暗号化し，テスト・ドキュメントでごちゃまぜの状態にして表示します。これにより，実行セッション中に画面上のパスワードは非表示になります。

   注：パスワード・エンコーダ・ツールを使用しても，本当に暗号化されるわけではありません。実際のパスワード/情報は，引き続きテストで保存されています。

   パスワード・エンコーダ・ツールの詳細については，『Unified Functional Testing ユーザーズ・ガイド』の「キーワード・ビュー」を参照してください。

3. イベント・ハンドラを使用して，API テスト内のパスワードを暗号化します。

   イベント・ハンドラで暗号化を有効にする方法の詳細については，『UFT ユーザーズ・ガイド』のイベント・ハンドラ・コードの記述に関する項を参照してください。

   任意の HTTP または Web サービス呼び出しアクティビティの一部として，Web サービス呼び出しステップのセキュリティ・プロパティを設定できます。

   Web サービスのセキュリティ・プロパティを設定する方法の詳細については，『Unified Functional Testing ユーザーズ・ガイド』の「API テスト」の「Web サービスのセキュリティ」を参照してください。

UFT を使用した Mac 上の Safari での作業

UFT がリモート Mac コンピュータに接続する場合，Safari アプリケーションにアクセスして，Safari で実行されている Web アプリケーション上でステップを実行できます。このため，この接続のセキュリティを保護し，Mac への不適切なアクセスや，Mac がアクセスできる Web ページへの不適切なアクセスを防止することが重要となります。

UFT が Mac と通信する場合，UFT はクライアントとして動作し，UFT 接続エージェントがサーバとして動作します。

この通信のセキュリティは，次のようにさまざまなレベルで保護できます。

- クライアント認証を設定するには，UFT が Mac との通信に使用するパスフレーズを定義します。
- UFT と UFT 接続エージェントとの通信のセキュリティを保護するには，SSL 接続の使用を必須とし，SSL 通信に必要な証明書とキー・ファイルを提供します。

詳細については，『UFT アドイン・ガイド』の「**Web**」のリモート Mac コンピュータとの通信のセキュリティ保護に関するトピックを参照してください。

ご意見をお寄せください

このドキュメントについてご意見がありましたら，電子メールでドキュメントチーム宛てにご意見をお寄せください。このシステムに電子メールクライアントが設定されている場合，上記のリンクをクリックすると，電子メールウィンドウが開き，件名行に次の情報が表示されます。

Feedback on UFT Security Reference

お客様のご意見・ご感想を電子メールに入力して，［送信］をクリックしてください。

電子メール・クライアントが利用できない場合は，上記の情報を Web メール・クライアントの新規メッセージにコピーし，ご意見・ご感想を入力して SW-Doc@hp.com までお送りください。