

2010/02/17

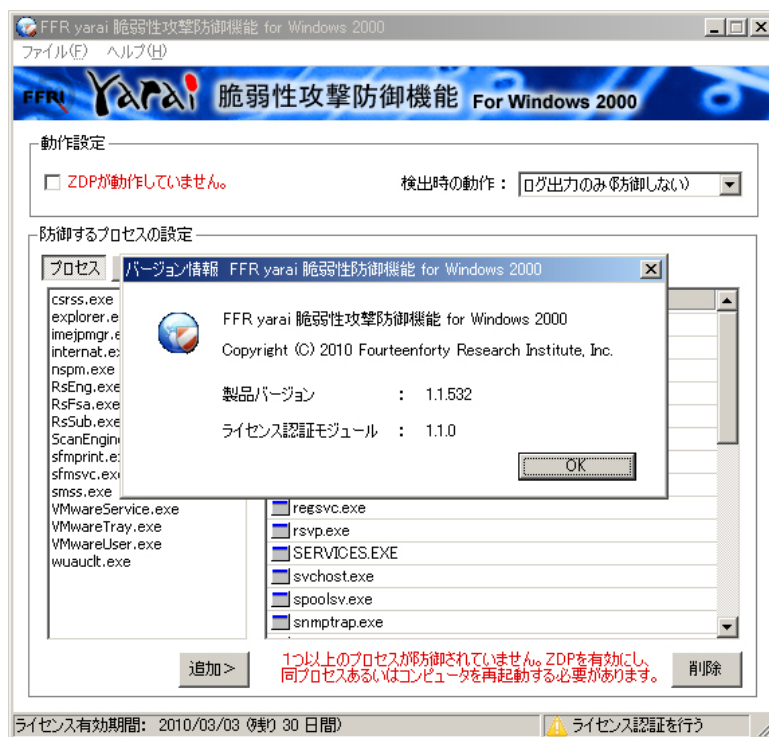
FFR yarai 脆弱性攻撃防御機能 for Windows 2000 操作説明

株式会社フォーティンフォーティ技術研究所

本資料は、FFR yarai 脆弱性攻撃防御機能の使用イメージを深めていただくために作成したものです。本製品は、簡単な操作で複雑な防御機能を有効にできるよう実装されています。

1. バージョン確認画面

本製品のインストール後に製品のバージョン情報は以下のように表示されています。新しい脆弱性を狙った攻撃手法に対応した場合に、新しいエンジンへ更新を行った場合には、製品バージョンが更新されます。



2. アクティベーション画面

本製品を使用する場合、アクティベーションを行っていただく必要があります。本製品のライセンスは永久使用ライセンスとなっており、ライセンスキーはオフラインアクティベーションが可能なライセンスファイルとして提供されますので、こちらの画面から設定をお願いします。

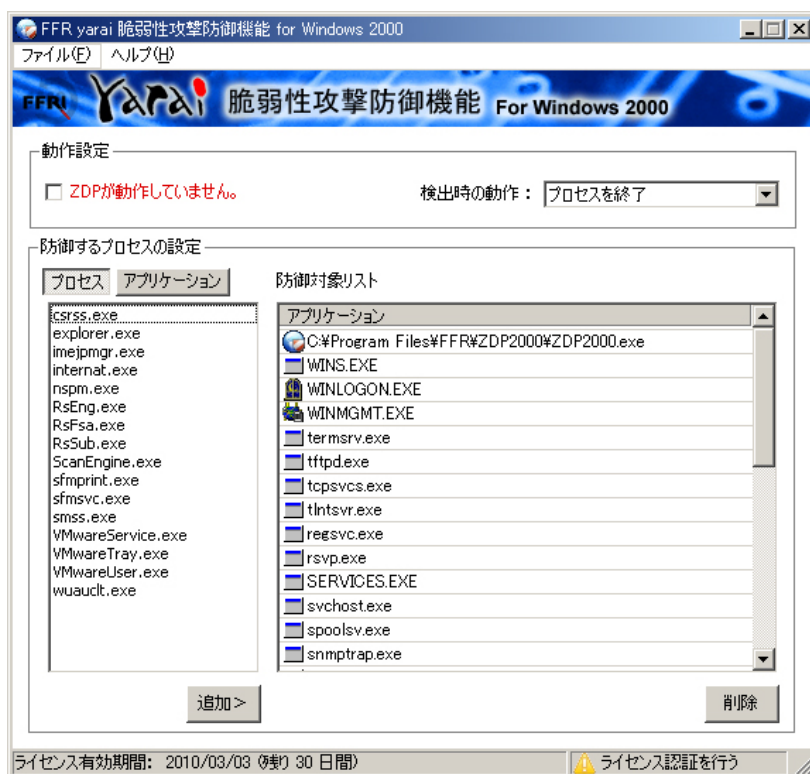


3. メイン画面 1

本製品の設定を行うメイン画面です。上段には動作全般の設定項目があります。

赤字で表示されているチェックボックスは、本製品による防御の有効/無効を設定するものです。このチェックボックスが外れている場合、赤字で表示されているように **ZDP**（ゼロデイ保護エンジン）が停止中ですので、すべてのシステムは保護管理下に無い状態を示しています。

[検出時の動作] 設定は、本製品が防御中のプロセスが、脆弱性を悪用した攻撃を検出した場合に、攻撃を受けたプロセスを停止するか、プロセスを動作させ続けるかを選択できます。システムへ本製品を導入した当初は、互換性確認のためにプロセスを動作させ続けるモードを選択してください。



4. メイン画面 2

脆弱性攻撃を停止するよう ZDP 機能を有効にした場合の画面です。

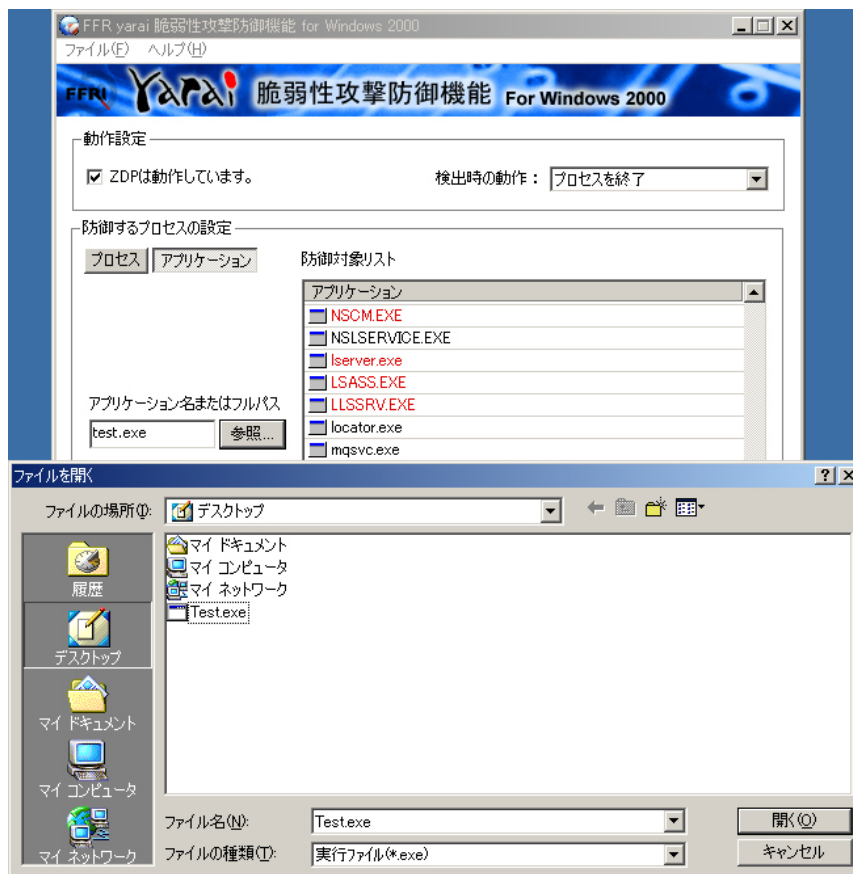
防御するプロセスの一覧には、プロセスが稼働中のため防御が有効にできていないプロセスが左側に、保護対象になっているプロセスが右側に表示されます。本製品がプロセスを保護する場合、各プロセスの実行プログラム内にインジェクト（挿入）し、動作環境を監視します。このインジェクトを行うため、サービスなどの再起動が必要となる場合があります。そのため、防御対象となっても防御が有効ではない場合には、プロセス名が赤字に表示されることになります。



5. 防御するアプリケーションの追加

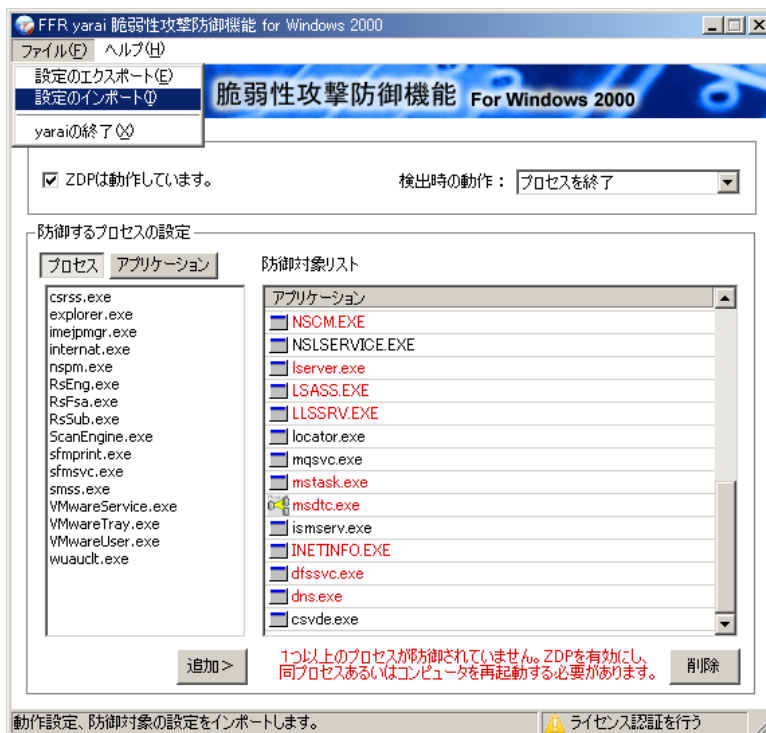
現在稼働中のプロセスに表示されていないようなアプリケーション、たとえば **Adobe Reader** のようにその都度実行されるようなアプリケーションも防御対象にすることが可能です。

下図のように、アプリケーションの存在するディレクトリとファイル名、もしくはファイル名のみ（この場合、同一のファイル名は全て防御対象になります）を指定することで、起動時に防御のためにインジェクトを行います。



6. 設定のエクスポートとインポート

上記の防御するプロセスの設定は、他のサーバーへ同一の展開をするためにエクスポートとインポート機能を持っています。設定内容を .yar ファイルとして暗号化ファイルに保存しますので、その内容を同構成の他のサーバーへインポートしてください。

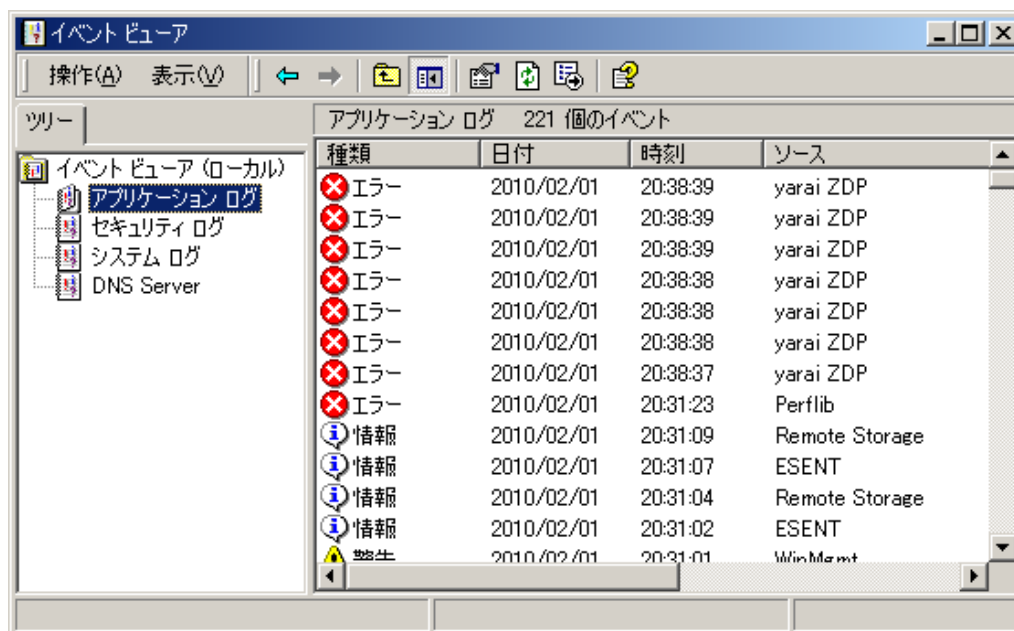


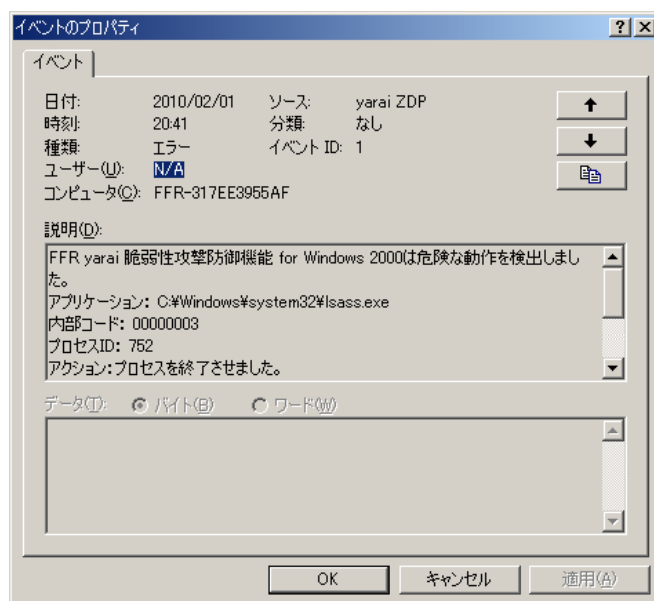
7. 攻撃検出の記録

本製品が防御をしている製品に脆弱性があり、その脆弱性を悪用した攻撃が行われた場合には、本製品が Windows のイベントログにエラーイベントを記録します。イベントの詳細には、アクションを示す内容が記載されており、プロセスを終了させたか、プロセスを続行させたかが明記されます。

サーバーのイベントログの収集と集中管理を行っているお客様は、このイベントログを参照することでサーバーの動作を確認することが可能です。

プロセスを続行させている場合、攻撃を受けたプロセス内でウイルスが継続して動作している可能性がありますし、突然サービスが停止をした場合にも、このイベントログが記録されている場合には何らかの攻撃を受けた可能性があることを把握できます。





以上、本製品の画面イメージと操作概要を説明いたしました。

非常に簡単な操作で、これまで攻撃の有無が把握できずに困難を極めたインシデント対応も、本製品を使用することで攻撃を可視化し、インシデント対応をスムーズに進めることが可能と考えております。