報道関係者各位
プレスリリース

2016 年 2 月 10 日
株式会社ＦＦＲＩ

NTT 東日本にて販売取次開始予定
従来のパターンマッチング型アンチウイルスソフトで防御不能な“未知の脅威”に対抗する
個人・SOHO 向けセキュリティソフト「FFRI プロアクティブ セキュリティ」

サイバーセキュリティ領域において国内で独自の研究開発活動を展開している株式会社ＦＦＲＩ（本社：東京都渋谷区、代表取締役社長：鵜飼裕司、以下 FFRI）が販売する個人・SOHO 向けセキュリティソフト「FFRI プロアクティブ セキュリティ（製品愛称：Mr.F）」（ダウンロード 1 年版）を、東日本電信電話株式会社（本社：東京都新宿区、代表取締役社長：山村雅之、以下：NTT 東日本）が販売取次を開始する予定となりましたことを 2016 年 2 月 10 日にご報告いたします。

アンチウイルスソフトでは検知できないマルウェアが急増中

近年の急激に増え続けるマルウェア※1 による攻撃に対しては、従来のパターンマッチング型のアンチウイルスソフトだけでは対抗することが難しくなってきています。最近では、悪意の第三者により日々膨大な数のマルウェアが作りだされており、アンチウイルスソフトは、パターンファイルの作成及び配信が追い付いていない状況です。さらに、高度なサイバー攻撃に使用されるマルウェアは、アンチウイルスソフトでは検知されない（パターンファイルに登録されていない）未知のマルウェアが使用されているという現実もあります。

「FFRI プロアクティブ セキュリティ」は、パターンマッチング技術※2 ではなく、独自のプログレッシブ・ヒューリスティック技術※3 により、未知のサイバー脅威に対抗する個人・SOHO 向けセキュリティソフトです。

NTT 東日本の販売網を通じて、幅広いお客様のニーズに対応

「FFRI プロアクティブ セキュリティ」ダウンロード 1 年版は『FFRI オンライン・ショップ』（http://www.ffri.jp/online_shop/index.htm）（2015 年 4 月～）、Vector PC Shop（2015 年 9 月～）、楽天ダウンロード（2015 年 10 月～）で販売を行ってきましたが、このたび NTT 東日本にて販売取次を開始予定となりました。NTT 東日本にて本商品を販売・取次いただくことで、より多くのお客様が安心・安全にインターネットをご利用いただけるよう取り組んでまいります。

【製品名称】

FFRI プロアクティブ セキュリティ （製品愛称：Mr.F）



【リリース日/価格】

ダウンロード１年版：2015 年 4 月 1 日/8,500 円（税抜）

※1 コンピュータ・ウイルス、スパイウェアなど、悪意のある目的を持ったソフトウェアやプログラムのこと。

※2 検査対象のプログラムと、パターンファイル（マルウェアのデータベース）をマッチングしてマルウェアを検知・防御する仕組み。パターンファイルを保持していなければ検知することができないため、新種や改造されたマルウェアは検知・防御することができません。

※3 パターンファイルに全く依存せず、マルウェアの構造や振る舞いを見て、マルウェアに特徴的な「悪意」を分析することにより検知・防御する技術。パターンマッチング技術では防御が難しい新種や改造されたマルウェアであっても、マルウェアに共通する「悪意」を検知して防御することが可能。

年金マルウェアや vvv ウイルスも防御！ 未知マルウェア対応の「プログレッシブ・ヒューリスティック技術」

FFRI プロアクティブ セキュリティは、FFRIが独自に開発したプログレッシブ・ヒューリスティック技術により、既知・未知に関係なく、マルウェアの脅威から防御します。

単一的なアプローチによるヒューリスティック分析では、検知精度が不十分なために、本来検知すべきマルウェアを検知できなかったり、正常なプログラムを誤検知してしまう懸念がありました。FFRI プロアクティブ セキュリティは、攻撃者の思考を先回りした先進的な検知ロジックを複数搭載するプログレッシブ・ヒューリスティック技術で検査対象のプログラムを多角的なアプローチで分析し、マルウェアをリアルタイムで高精度に検知・防御します。

2015 年 6 月の日本年金機構を対象とした標的型攻撃で使用されたとみられるマルウェア「Emdivi」、2015 年 12 月のランサムウェア※4「TeslaCrypt（vvv ウイルス）」も検知・防御できることを確認いたしました。

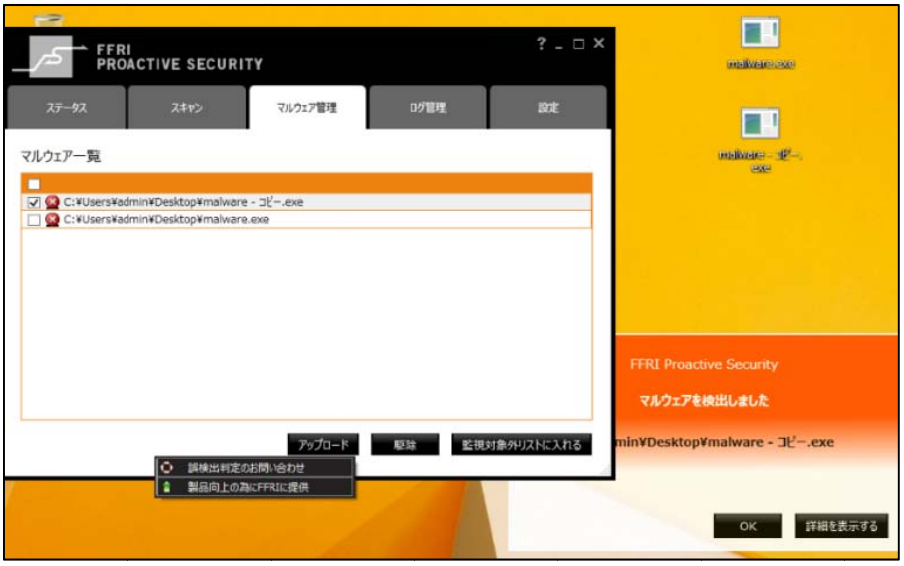
※4 身代金要求ウイルスとも言われ、ユーザーのデータを人質にとり、データ回復のために身代金を要求するウイルス。

【FFRI プロアクティブ セキュリティのプログレッシブ・ヒューリスティック技術】



■ZDPエンジン	メールやWebページ閲覧時の攻撃など、既知・未知の脆弱性を狙ったウイルス攻撃を防御。 独自の「API-NX」技術(特許第4572259号)で、任意コード実行型脆弱性の攻撃を防御。
■Static分析エンジン	プログラムを動作させることなく分析。「PE構造分析」「リンカー分析」「パッカー分析」「想定オペレーション分析」など 多数の分析手法「N-Static分析」で検知。
■Sandboxエンジン	仮想CPU、仮想メモリ、仮想Windowsサブシステムなどで構成される仮想環境上でプログラムを実行。 独自の「U-Sandbox検知ロジック」で命令の組み合わせに基づいて検知。
■HIPSエンジン	実行中プログラムの動作を監視。他プログラムへの侵入、異常なネットワークアクセス、 キーロガーやバックドア的な動作などの挙動を、独自の「DHIPSロジック」で検知。
■機械学習エンジン	FFRIが収集したマルウェアに関するビッグデータを元に実行中のプログラムを監視。 ビッグデータ上の振る舞い特性を抽出し、機械学習で分析した特徴により端末上の悪意ある挙動を検知。

【画面イメージ】



株式会社 FFRI について

当社は 2007 年、日本において世界トップレベルのセキュリティリサーチチームを作り、コンピュータ社会の健全な運営に寄与するために設立されました。現在では日々進化しているサイバー攻撃技術を独自の視点で分析し、日本国内で対策技術の研究開発に取り組んでいます。研究内容は国際的なセキュリティカンファレンスで継続的に発表し、海外でも高い評価を受けておりますが、これらの研究から得られた知見やノウハウを製品やサービスとしてお客様にご提供しています。主力製品となる、「FFR yarai」はミック経済研究所調べ※5 によるエンドポイント型標的型攻撃対策分野における出荷金額において No.1 を獲得しております。

※5　出典：ミック経済研究所「情報セキュリティソリューション市場の現状と将来展望 2015【外部攻撃防御型ソリューション編】」

本件に関するお問い合わせ先
写真・資料等がご入用の場合もお問い合わせください。

■報道機関からのお問い合わせ先
株式会社 FFRI
経営管理本部　PR 担当
TEL：03-6277-1811
E-Mail：pr@ffri.jp　URL：http://www.ffri.jp

「FFRI」、「FFR yarai」、「FFRI プロアクティブ セキュリティ」は、株式会社 FFRI の登録商標です。

その他すべての社名、製品・サービス名は、各社の商標または登録商標です。

出典資料の引用等、調査会社の著作物を利用する場合は、出典元にお問い合わせください。