

報道関係者各位
プレスリリース

2015 年 7 月 1 日
株式会社 FFRI



**FFRI が 2015 年 7 月 1 日より Amazon マーケットプレイスに出店
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」を販売**

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：鶴飼裕司、以下 FFRI）は、2015 年 7 月 1 日より Amazon マーケットプレイスに出店し、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」（パッケージ 1 年版）を販売いたします。

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。

Amazon マーケットプレイスを通じて、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 2015 年 4 月より『FFRI オンライン・ショップ』（http://www.ffri.jp/online_shop/index.htm）にて、パッケージ 1 年版は 6 月 22 日より全国のヤマダ電機にて販売・取扱いを行ってまいりましたが、このたび同パッケージ 1 年版を Amazon マーケットプレイスで販売開始いたします。Amazon マーケットプレイスでの販売を通して、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

【リリース日/価格】

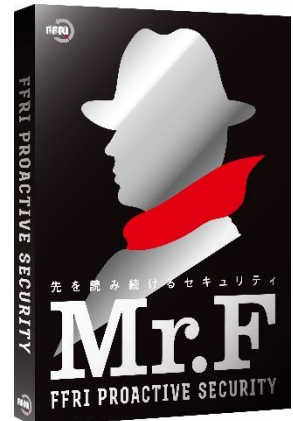
パッケージ1年版：2015年6月22日/8,500円（税抜）

【Amazon マーケットプレイス URL】

<http://www.amazon.co.jp/dp/B00ZICLBDK>

【Amazon マーケットプレイス運営開始日】

2015年7月1日 10:00～



※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。

日本年金機構を狙うマルウェア「Emdivi」 vs. 「FFRI プロアクティブ セキュリティ」

2015年6月1日、日本年金機構より基礎年金番号を含む個人情報、約125万件の流出が発表されました。報道によると、悪意の第三者により職員宛てに送信されたマルウェアが添付された電子メールを開封した結果、マルウェアに感染し、情報の窃取に至ったとされています。

近年、こうした情報窃取等の明確な目的の下、特定組織を狙った標的型攻撃が増加しています。標的型攻撃においては、ほとんどの場合新種のマルウェアが利用されますが、こうしたマルウェアは一般に流布していないため事前にパターンを用意することが困難であり、現在広く普及している「パターンマッチング方式」のアンチウイルス製品では、防御することが極めて困難です。今回の日本年金機構を狙った攻撃もこうした標的型攻撃の一種であり、職員端末に導入されていたアンチウイルス製品では防御できなかったことが報道されています。

FFRI は、日本年金機構を対象とした標的型攻撃で使用されたと見られるマルウェア「Emdivi」の検体をセキュリティ業界関係ルートで入手し、当社製品で検知・防御できるか否かの確認を実施いたしました。その結果、メール添付されたと見られる検体は、下記の製品でリアルタイムで検知・防御できることを確認いたしました。

・FFRI プロアクティブ セキュリティ Version 1.0.217 (2015年4月24日リリース)

未知のマルウェアに対応する「プログレッシブ・ヒューリスティック技術」

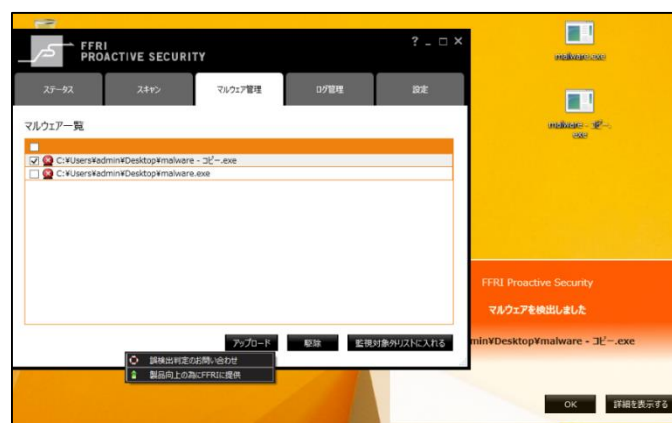
FFRI プロアクティブ セキュリティでは、FFRIが独自に開発したプログレッシブ・ヒューリスティック技術により、既知・未知に関係なく、マルウェアの脅威から防御します。

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。

【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】

アプリケーションを脆弱性攻撃から守る	
	ZDPエンジン
マルウェアを検出する	
	Static分析エンジン
	Sandboxエンジン
	HIPSエンジン
	機械学習エンジン
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」「バッカー分析」「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^{※4}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。

※4 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 2014【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・資料等をご入用の場合もお問い合わせください。

株式会社 FFRI
経営企画部 PR 担当
TEL：03-6277-1811
E-Mail：pr@ffri.jp URL：<http://www.ffri.jp>

「FFRI」、「FFR yarai」は、株式会社 FFRI の登録商標です。

Amazon マーケットプレイス、Amazon.co.jp および Amazon は Amazon.com, Inc. またはその関連会社の商標です。

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。