

ISP 事業者各位

2015 年 11 月 20 日  
株式会社 FFRI



---

**「FFRI プロアクティブ セキュリティ」を月額課金での販売を開始  
取扱い ISP 事業者様を募集いたします**

---

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 当社）は、個人・SOHO 向け「FFRI プロアクティブ セキュリティ（製品愛称：Mr.F）」の月額版の販売を開始いたします。

**月額版の販売により、幅広いお客様のニーズに対応**

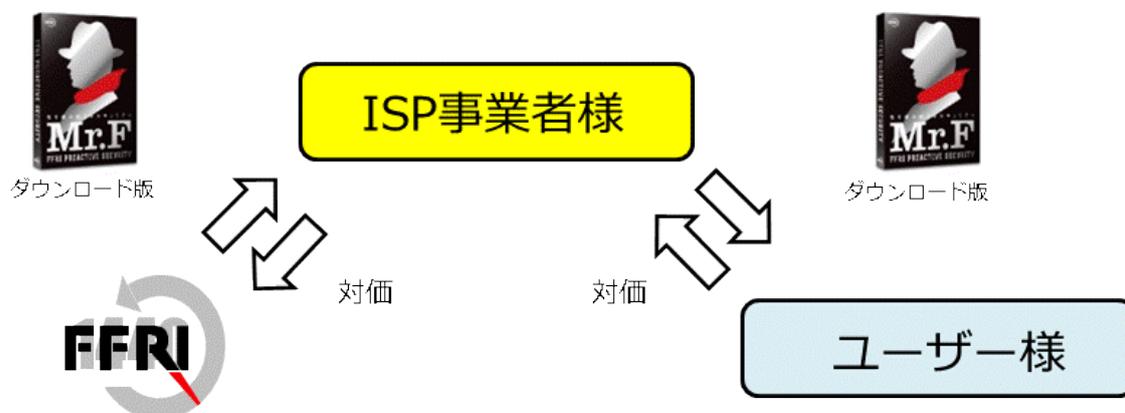
当社は月額版「FFRI プロアクティブ セキュリティ」の第 1 弾として、群馬インターネット株式会社（本社：群馬県高崎市、代表取締役：石田安利）から 2015 年 10 月 30 日（金）より販売を開始しておりましたが、お客様の幅広いニーズに対応するため、他の事業者様向けに月額版「FFRI プロアクティブ セキュリティ」の販売を開始いたします。

**取扱い ISP 事業者様を募集いたします**

この度、月額版「FFRI プロアクティブ セキュリティ」の販売開始に伴い、当社ではこれをお取扱いいただける全国の ISP 事業者様の募集をいたします。

ISP 事業者様におかれましては、月額版「FFRI プロアクティブ セキュリティ」の取扱いを通じて、各 ISP 事業者様の契約ユーザー様はインターネットサービスを利用するにあたって抱えるセキュリティ・リスクを大幅に低減することが可能です。

## 想定事業モデル



注) 上記は一例です。その他の商流やモデル、ユーザーのアフターサポートについてご相談承ります。  
詳細はお問い合わせください。

## 販売の概要

### 【製品】

FFRI プロアクティブ セキュリティ (製品愛称：Mr.F) (個人・SOHO 向け)

### 【メディア】

ダウンロード版

### 【価格】

ご相談

## 本件に関するお問い合わせ

月額版「FFRI プロアクティブ セキュリティ」のお取扱いを検討の ISP 事業者様は下記までご連絡をお願いいたします。

### 株式会社 FFRI

経営管理本部 事業戦略担当

TEL : 03-6277-1811

E-Mail : [business@ffri.jp](mailto:business@ffri.jp) URL : <http://www.ffri.jp>

## 【FFRI プロアクティブ セキュリティについて】

### 既存の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<sup>※1</sup>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つ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。

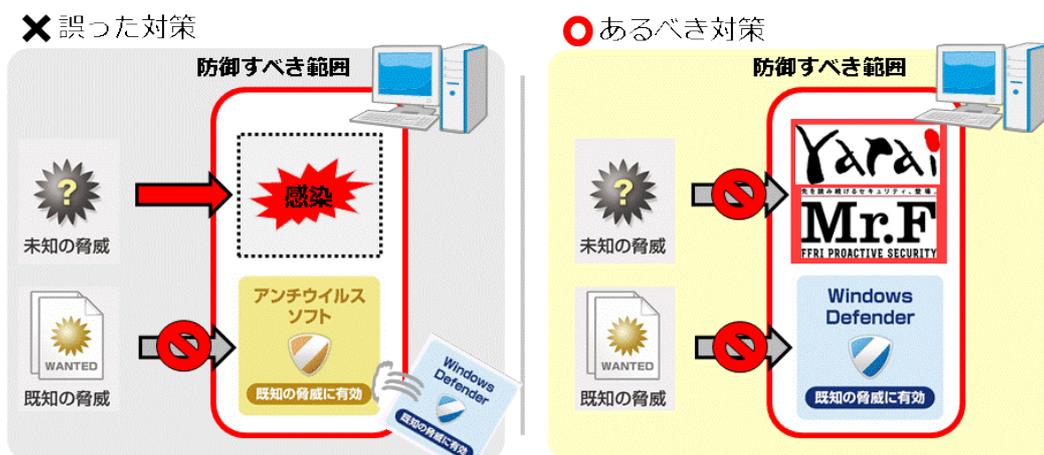
FFRI プロアクティブ セキュリティは、パターンマッチング技術<sup>※2</sup>ではなく、独自のプログレッシブ・ヒューリスティック技術<sup>※3</sup>により、未知のサイバー脅威に対抗するセキュリティソフトです。

### 既存のアンチウイルスソフトでは期待するセキュリティ体制を築くことはできない

現状多くのユーザーが既存のアンチウイルスソフトを購入して PC にインストールし、それだけで十分なセキュリティが確保されるものと誤解をしているケースが多くあります。

しかし実際は既存のアンチウイルスソフトは既知の脅威に効果を発揮するものであり、未知の脅威に対しては十分な効果を期待できません。またさらに、Windows8 以降の OS には既存のアンチウイルスソフトと同等の機能を持つ Windows Defender が無償で付属されています。

未知の脅威を防御するには FFRI プロアクティブ セキュリティを導入し、Windows Defender と併用することで効果的なセキュリティ体制を構築することができます。



□ Windows Defender（無料）を市販のウイルス対策ソフト（有料）に置き換えても防御範囲は同じなため、未知の脅威は防げない

□ FFR yarai又はFFRI プロアクティブ セキュリティを導入することで未知の脅威を防御可能

## **年金マルウェアもブロック！ 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 セキュリティは、当社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 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

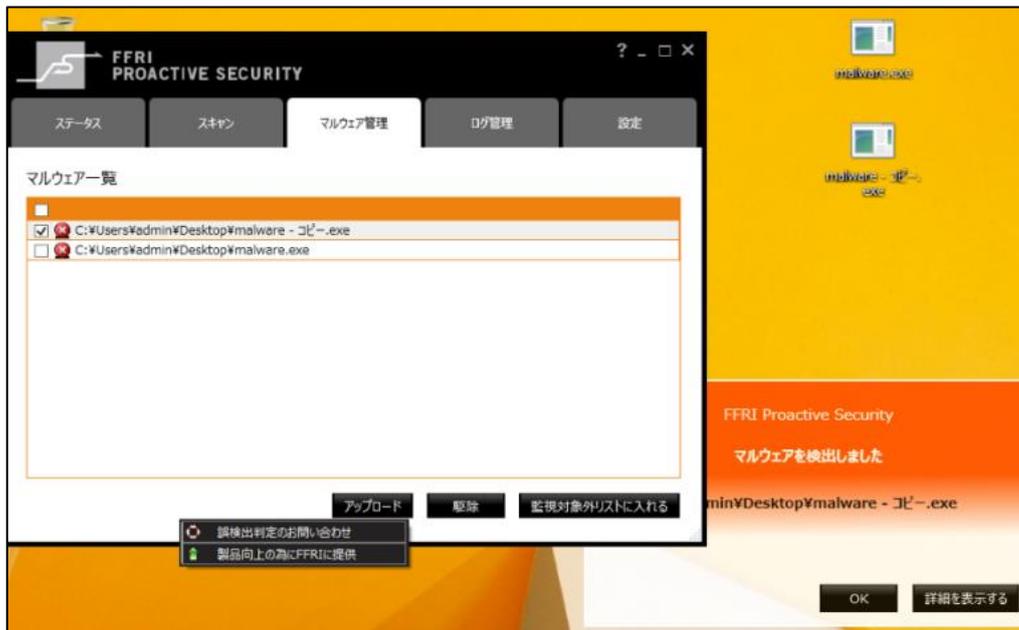
Sandboxエンジン

HIPSエンジン

機械学習エンジン

<b>ZDPエンジン</b>	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。
<b>Static分析エンジン</b>	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」「ハッカー分析」「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。
<b>Sandboxエンジン</b>	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。
<b>HIPSエンジン</b>	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。
<b>機械学習エンジン</b>	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<sup>※4</sup>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。

- ※ 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。
- 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 2015【外部攻撃防御型ソリューション編】」

「FFRI」、「FFR yarai」、「FFRI プロアクティブ セキュリティ」、「Mr.F」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。