MSYS
丸紅情報システムズ

News Release

2015 年 6 月 19 日

丸紅情報システムズ株式会社

ファイア・アイ社 標的型攻撃対策製品の取り扱いを開始
～ i-Filter 連携ソリューションを軸に販売 ～

丸紅情報システムズ株式会社（略称：エムシス/MSYS 本社：東京都渋谷区 社長：伊吹 洋二）は、サイバー攻撃対策の製品・サービスを提供する米ファイア・アイ社（FireEye, Inc. 取締役会長 兼 CEO：デビッド デワルト/David DeWalt 本社：カリフォルニア州ミルピタス 設立：2004 年）と販売代理店契約を締結し、セキュリティアプライアンス製品「FireEye（ファイア・アイ）」の取り扱いを開始します。また、「FireEye」と WEB フィルタリング製品「i-Filter（アイフィルター）」の両製品の正規販売代理店として初めて連携ソリューションを販売します。

FireEye は、サンドボックス技術（*1）を駆使してマルウェア（*2）や未知の攻撃からの脅威を守る標的型攻撃（APT *3）に特化したセキュリティ製品です。これまでに、ゼロデイ・エクスプロイト（*4）からの攻撃を他に先駆けて検知した多数の実績があります。WEB 経由の攻撃を検知する FireEye NX シリーズ、E メールを利用した攻撃を検知する FireEye EX シリーズ、FireEye NX/EX を一元管理する FireEye CM シリーズの 3 製品から構成されます。各製品の外観は 1U または 2U のラックマウントサイズです。

FireEye NX では、HTTP トラフィックをキャプチャし、内部に持つ仮想実行エンジンの解析を基にして未知の脆弱性を突く攻撃やマルウェアを検知する入口対策と、FireEye で見つけられた C&C サーバ（*5）の情報を基に、C&C サーバへの通信を検知・ブロックする出口対策が可能です。FireEye EX は、Email の添付ファイルを内部の仮想実行エンジンで解析し、未知の脆弱性を突く攻撃やマルウェアを検知、攻撃メールをブロックします。FireEye CM は FireEye EX と FireEye NX の情報を一元管理し、さらに全世界の FireEye ユーザで取得された C&C サーバの情報を適用します。なお、FireEye NX は単体での利用も可能です。

さらに、FireEye NX で未知の C&C サーバや不正が潜むと思われる WEB サイトを検知してからブロックするまで、ネットワーク環境などによっては一定の時間を要することから、MSYS はより即時的な防御を求める企業に向けて、2002 年より一次販売代理店として販売する i-Filter との連携ソリューションを提供します。i-Filter は、既知の C&C サーバや不正な WEB サイトをフィルタリングするソリューションです。FireEye との連携ソリューションでは、FireEye で検知した C&C サーバのアドレスを i- Filter 連携モジュールが自動取得しフィルタルールに追加することで、C&C サーバへの通信があった場合、即時に既知の脅威と同様にブロックすることが可能となります。また、FireEye NX 単独では利用者が通信をなぜブロックされたか知り得ない機能上の課題に対し、i-Filter ではアクセス先の URL が危険なサイトであることをブラウザへ警告を表示する機能により利用者はブロックされた理由を把握することができ、ユーザビリティの向上が図れます。

近年のサイバー攻撃は、特定の企業や政府機関を狙った標的型攻撃が主流になりつつありますが、標的型攻撃は従来のアンチウイルスやファイアウォールといった、既知の攻撃からの防御を目的とする定義ファイル検知型のセキュリティ対策では攻撃者に回避されてしまいます。これらの背景から、未知の脆弱性を突く、あらゆる脅威からサイバー攻撃の兆候をリアルタイムに検知し、即時に対応するためのソリューションが市場に強く求められています。

MSYS は、標的型攻撃への防衛強化に取り組む製造業・アミューズメント企業などに向けて FireEye および i-Filter によるソリューションを提供し、今後 1 年間で 3 億円の売り上げを目指します。

【FireEye 製品ホームページ】
http://www.marubeni-sys.com/sec/fireeye/

【FireEye x i-Filter 連携ソリューションホームページ】
http://www.marubeni-sys.com/sec/fireeye/apt.html

(*1) 仮想環境として「攻撃されてもよいホスト」を作成し、その中でマルウェアを動作させて、振る舞いをチェックするもの
(*2) 不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称
(*3) 未知の脆弱性を利用して、特定企業の PC に不正プログラムを感染させるもの Advanced Persistent Threat
(*4) 世間で発見されていないソフトウェア(OS・ブラウザなど)の脆弱性
(*5) Command and Control server マルウェアに感染してボットと化したコンピュータ群(ボットネット)に指令(command)を送り、制御(control)の中心となるサーバのこと

【FireEye について】
高度なセキュリティ・ソリューションで業界をリードする FireEye は、世界中のお客様がもつ最も重要な資産を攻撃者から守ります。テクノロジー、脅威情報、専門知識を統合的に提供し、またインシデント・レスポンス担当者の強力なサポートによりセキュリティ侵害の被害を回避できます。攻撃者は侵害のあらゆる局面で検知され、阻止されます。FireEye のソリューションを導入すれば、サイバー攻撃のリアルタイム検知が可能になるほか、最も重要な資産に及ぼすリスクの把握や、セキュリティ・インシデントへ迅速な対応、解決するための態勢を容易に整えられます。FireEye が世界規模で展開する防御コミュニティは、Fortune 500 企業の 200 社以上を含む、世界 67 か国 3,100 を超えるお客様組織で構成されています。
FireEye ホームページ: https://www.fireeye.jp/

【i-Filter について】
「i- Filter」は、導入シェア・データベース品質・顧客満足度において No.1 を誇るサーバーインストール型の Web フィルタリングソフトです。Web アクセスの制御と可視化はもちろん、Web アクセスの入口対策から出口対策までトータルな Web セキュリティ・ソリューションを提供し、情報漏洩対策を強力に支援します。また、業界最高水準の URL データベースと、特許を取得したフィルタリングテクノロジー「ZBRAIN」により、圧倒的なフィルタリング精度を誇ります。
i-Filter ホームページ: http://www.daj.jp/bs/i-filter/

【丸紅情報システムズについて】

丸紅情報システムズは、最先端 IT を駆使した付加価値の高いソリューションやサービスを、お客様視点で提供するソリューションプロバイダです。製造・流通・サービス・小売・金融業を中心とする様々な業界の知見と高度な提案力と、グローバルな視点からお客様の差別化に貢献する最先端技術やそれを活用した新しいソリューションの開発力が当社の強みです。ソリューションや製品、サービスを通じて、お客様の期待を超える新しい「価値」の創出でお客様のビジネスを支援します。

＜お問い合わせ先＞

丸紅情報システムズ株式会社
URL: http://www.marubeni-sys.com/
〒150-0002 東京都渋谷区渋谷 3-12-18 渋谷南東急ビル
広報部 広報課（プレス関係者窓口）
電話：03-5778-8885 ファックス：03-5778-8999

＜製品に関するお問い合わせ＞

丸紅情報システムズ株式会社
プラットフォームソリューション事業本部 ストレージ・インフラソリューション一部
電話：03-5778-8772