Soliton®

News Release

報道関係各位

2020 年 9 月 29 日

株式会社ソリトンシステムズ

エンドポイント・ログ収集ソフト「InfoTrace Mark II」を機能強化、新版、V3 をリリース
サイバー脅威ハンティングの自動化に対応

株式会社ソリトンシステムズ（代表取締役社長：鎌田信夫　以下ソリトン）は、自組織内のサイバー攻撃を見つけ出す「脅威ハンティング」の自動化に対応した、EDR(*1)のためのツール「InfoTrace Mark II」の新バージョン、V3 を開発し、来月、10 月 1 日からリリースします。

新型コロナウイルスの感染拡大を機に、在宅勤務が普及し、クラウドサービスの利用が多くなりました。エンドポイントの環境も変わり、そのセキュリティ対策とその管理が極めて Critical なものとなっています。一方、日々増え続けるサイバー脅威に対抗するため、業界内や企業グループ内で確認されたマルウェアのハッシュ値などの脅威情報を共有する取り組みが進んでいますが、受け取った脅威情報を基に自社内の感染状況を確認するプロセスが実に複雑です。

今回の InfoTrace Mark II の新版 V3 では、

（1）　国際標準規格である STIX/TAXII(*2)に対応。STIX で記述された脅威情報を TAXII にて受領し、端末の侵害有無をチェックする「脅威ハンティング」の自動化に対応しました。これにより、脅威情報を活用した感染チェックや、該当端末のネットワーク隔離、当該ファイルの実行禁止までを自動化することができます。

（2）　端末の管理面での機能強化も実現しています。セキュリティパッチや導入ソフトウェアなどのインベントリ情報の取得、端末への任意ファイル転送やコマンドの実行など、 EDR 運用に役立つ端末管理機能を標準搭載しました。さらに、国内でも感染を広げるマルウェア「Emotet」の感染確認に役立つ Office 文書ファイルのマクロ有効化の記録など、証跡ログを増やしています。新版 V3 は、運用負荷をも軽減しています。

この InfoTrace は、2004 年にソリトンにおいて開発がスタート。端末の OS 周りの、カーネルレベルの活動を収集、記録する 3 つのモジュールからなる大きいシステムです。今日一般化している OS メーカーによる Eventlog が出現する頃、ソリトンは独自に対応するものを開発。標準 Eventlog を超える種類のデータをも集める特徴を内在しています。InfoTrace はその後、サイバー攻撃、内部不正を意識したものに発展しています。InfoTrace は「Security Incident の原因究明の基礎データ」のみでなく、「事実の記録」そのものを提供します。

最近のサイバー攻撃の中には、エンドポイントによって把握できないものも現れ、EDR 以外の情報も必要であるという意見も提唱されています。この EDR:InfoTrace とネットワークのパケットも調べる Network Knowledge（AI 機能内蔵の Soliton NK）が連携されることが期待されます。一方の「事実の記録」そのものは、今後、公官庁や自治体で重要になると予想されます。

*1 EDR（Endpoint Detection and Response）とは、エンドポイント（端末）でサイバー攻撃を検知し、いち早く対応するソリューション。

*2 STIX（Structured Threat Information eXpression）は、観察されるサイバー攻撃の指標（IoC; Indicator of compromise）を記述する技術仕様。TAXII（Trusted Automated eXchange of Indicator Information）は STIX 等の脅威情報を交換する手順。

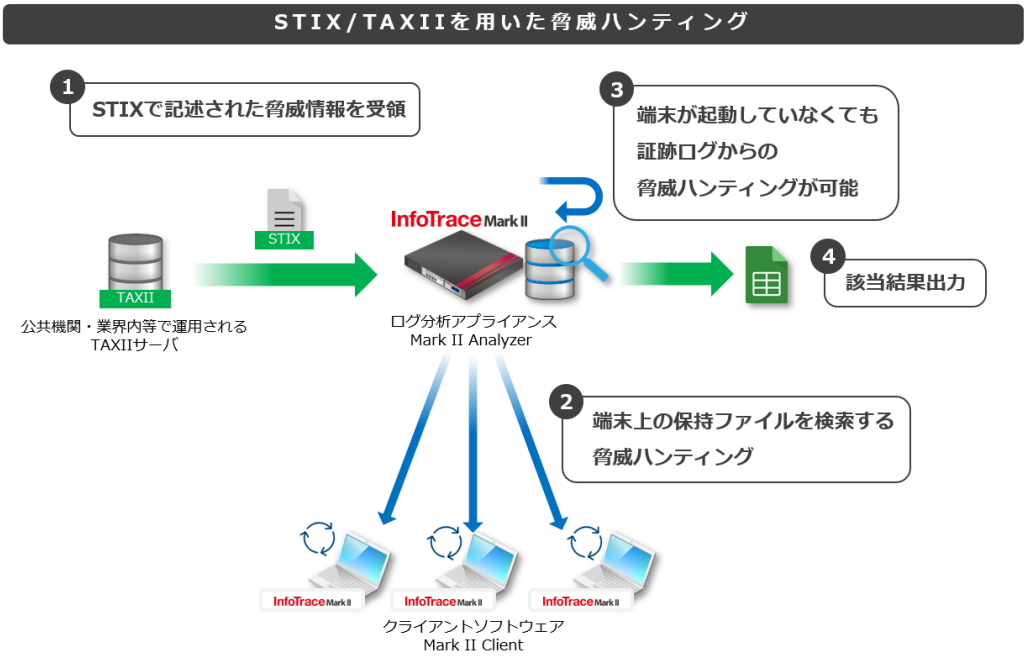

図 1： InfoTrace Mark II V3.0 での脅威ハンティング自動化 概要

■InfoTrace Mark II V3.0 の主な特長

- STIX/TAXII によるサイバー脅威ハンティング自動化
- インベントリ情報の取得や、ファイル転送・コマンド実行などの端末機能の標準搭載
- マルウェア感染を引き起こす Office 文書のマクロ有効化の記録
- メールログ、DNS クエリログなどのログ強化

InfoTrace Mark II V3.0

【提供開始】2020 年 10 月 1 日

【製品ページ】https://www.soliton.co.jp/lp/itmk2/

Soliton®

News Release

【株式会社ソリトンシステムズについて】
設立以来、ソリトンシステムズは IT・エレクトロニクス業界にあって、常に新しい技術トレンドを見据え、いくつもの「日本で初めて」を実現してきました。近年は、認証を中心とした IT セキュリティからサイバー対策製品まで、また、携帯電話回線4G、5G や Wi-Fi を利用したハイビジョン・レベルの映像伝送システム、リモートドライブなどに取り組んでおります。国産メーカーとして、オリジナルの「もの創り」、「独創」にこだわった製品とサービスを提供しております。
設立：1979 年、売上 155 億円（2019 年 12 月期・連結）、東証 1 部

HP： https://www.soliton.co.jp/
Facebook： https://www.facebook.com/soliton.s/
Twitter:： @soliton_jp

【 InfoTrace Mark II V3.0 に関する問合せ先 】
株式会社ソリトンシステムズ IT セキュリティ事業部
Tel: 03-5360-3811 netsales@soliton.co.jp

【 このリリースに関するマスコミからの問合せ先】
株式会社ソリトンシステムズ 広報
Tel: 03-5360-3814 press@soliton.co.jp