Soliton®

InfoTrace Mark II | CaseStudy 導入事例

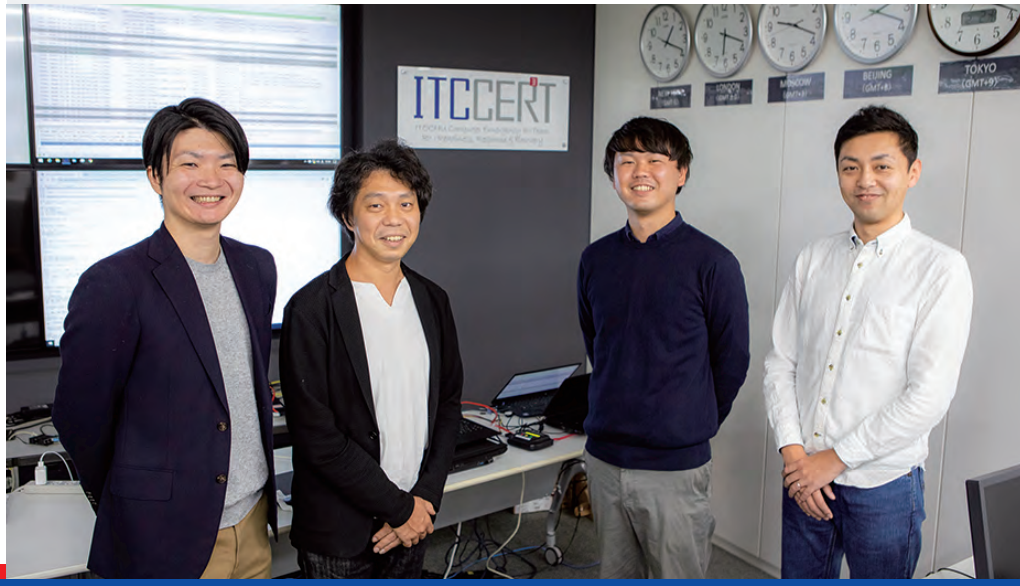
伊藤忠商事株式会社 様

User Profile

伊藤忠商事株式会社

本社：東京都港区北青山２丁目５番１号
URL：https://www.itochu.co.jp/

伊藤忠商事株式会社は、1858年初代伊藤忠兵衛が麻布の行商で創業したことにはじまり、一世紀半にわたり成長を続けてまいりました。現在は世界62ヶ国に約100の拠点を持つ大手総合商社として、繊維、機械、金属、エネルギー、化学品、食料、住生活、情報、金融の各分野において国内、輸出入及び三国間取引を行うほか、国内外における事業投資など、幅広いビジネスを展開しております。



セキュリティ対策製品によってビジネスを止めるな！
InfoTrace Mark IIを活用したプロアクティブなセキュリティ対策

課　題	導入効果
1 セキュリティを意識せず ビジネスに集中できる環境の整備	独自の検知ルールで、ビジネスを止めない プロアクティブなセキュリティ監視を実現
2 一般的な EDR 製品では、 セキュリティリスク全体をカバーできない	サイバー攻撃に限定されない、 セキュリティリスク全体への幅広い貢献
3 イベント発生時のシステム状況の正確な把握	イベント発生時の状況把握が可能となり、 対応スピードが向上

サイバーセキュリティへのプロアクティブな対応により、社員の安全なビジネス活動を支える「ITCCERT」とは

伊藤忠商事では、全社のセキュリティレベル向上を目的としたITCCERT（伊藤忠セキュリティ・インシデント・レスポンス・チーム）が活動している。発足は国内大手企業への標的型攻撃が発覚し始めた2012年。同社の営業カンパニーを横断的に、全社インフラの情報化推進を担当するIT企画部内に設置された。チームはIT企画部のメンバー 20名弱の体制で構成されているが、普段のサイバーセキュリティ運用に特化してセキュリティを専門とする分析官と運用オペレータを配し、本社約5,500台のPCと、約300台のサーバーを守る。インシデント発生時には、攻撃対象となったシステムを主管する各営業カンパニーのIT担当部署と連携しながらインシデント収束に向けた支援を行い、時にはグループ会社のインシデントにも対応する。また平時には、サイバー攻撃への対策を強化するべく最新の脅威情報の分析および製品情報の収集・検証や、イン

シデント対応力強化のためのグループ会社向け訓練なども行っている。

伊藤忠商事株式会社 IT企画部ITCCERT上級サイバーセキュリティ分析官の佐藤元彦氏は、その役割と特長を次のように説明する。

「ITCCERTはインシデントが起きてからの対応ではなく、起こさないためにどうするか、というプロアクティブな活動に重きを置いています。また、セキュリティ至上主義で社員にあれをするな、これをするなではなく、あくまでもビジネスを最優先に、社員にセキュリティを意識させず安全に業務していただく環境を作ることが、我々の役割と捉えています。」

伊藤忠商事株式会社
IT企画部 ITCCERT

上級サイバーセキュリティ分析官
佐藤 元彦 氏

「ブラックボックスな」EDR製品とは異なる、エンドポイントログ収集ツールInfoTrace Mark IIを選んだ理由

ITCCERTではさまざまなサイバーセキュリティ対策の中でも数年前からエンドポイントセキュリティに着目。数ある製品の中でInfoTrace Mark IIを検討した理由について、佐藤氏は次のように話す。

「エンドポイントセキュリティに期待するのは、攻撃者が掌握したPCから、近くのPCに横展開する挙動を早期に発見し食い止める、ということです。当社では旧来型のアンチウィルス製品ではこの対策が十分にできない、と言われ始めた4年ほど前から、数多くのEDR*製品の効果検証を行ってきました。その中で当時のEDR製品では、検知ルールがブラックボックス（非公開）のため過検知した場合に検知理由がわかりづらいことや、我々が分析して特定した攻撃者の振る舞いを検知する独自ルールが策定できないといった課題がありました。我々はビジネスが最優先ですので、EDR製品を導入し、ブラックボックスな検知ルールでビジネスが止められるということは絶対に避けなければなりません。ほとんどのEDR製品はシステムログを収集、その中の異常性によりアクションするという仕組みですので、システムログ*がきちんと収集できて、その上で我々自身が自社の活動に最適なルールを作るログ分析の仕組みを構築すれば、既存のEDR製品を導入するのと同等、もしくはそれ以上の効果が得られるのでは、と考えたのです。その観点で市場を探した結果、たどり着いたのがInfoTrace Mark IIでした。」

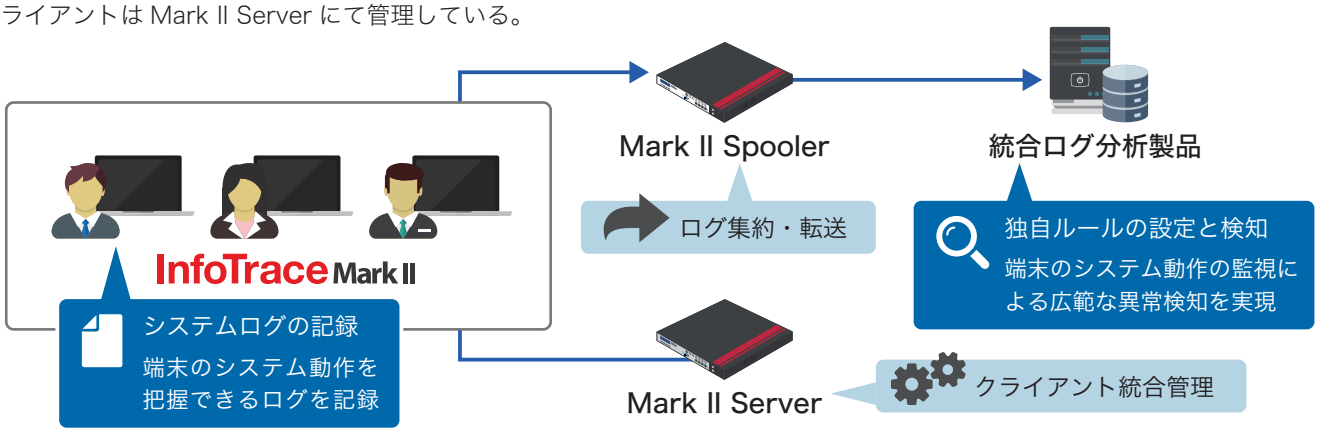
ソリトンの開発するログ収集・追跡ソフトウェアInfoTraceシリーズは、2004年の発売当初から端末の挙動を広く深く把握することに注力して開発されてきた。InfoTraceシリーズ最新世代のInfoTrace Mark IIでは、内部統制とサイバー攻撃の両方に対応するログを意識し、ユーザー操作だけではなく、バックグラウンドで行われるマルウェアやサイバー攻撃の挙動の記録が強化されている。OS標準のイベントログでは残らない情報も独自の方式で記録し、「インシデントの原因究明の基礎データ」のみでなく、「事実の記録」そのものを提供する点が特長だ。

佐藤氏は、他のEDR製品との違いをこう説明する。

「世の中のEDR製品やログ取得製品の多くは、システム負荷が高くならないようにするため、すべてのイベントをログに記録しているわけではありません。また、コマンドの引数をとれるなど、丁寧にシステムログの取得をしてくれる製品は決して多くありません。世の中にログ取得製品は多々あり、主眼とする目的が異なるので一概に良し悪し

InfoTrace Mark II システム概要

端末にインストールされたInfoTrace Mark II クライアントからのログを Mark II Spooler で集約したうえで統合ログ分析製品に取り込み、ITCCERT 独自のルールによって様々な脅威を監視。
クライアントは Mark II Server にて管理している。



伊藤忠商事株式会社 様

はありませんが、我々の求めるサイバー攻撃対策用のログ取得という高度な要求を満たすのはInfoTrace Mark IIだけでした。また、サポートが受けられないツールだと我々の業務負荷が高くなります。Sysmonなどでも同様の仕組みは作り上げられるかもしれませんが、InfoTrace Mark IIならメーカーの正式なサポートが受けられるという点での安心感もありました。加えて、国産である点も、日本のビジネス環境に即したリクエストへの反映が早いというメリットが期待されました。」

同社ではEDR製品導入の意義についても製品検証を含めた検討が行われた。他のEDR製品ではあくまでサイバー攻撃対策だけに用途が限定されるため、システム障害などを含めたセキュリティリスク全体におけるEDR製品のカバー範囲は実はさほど大きいわけではない。旧来のウイルス対策製品に加え、EDR製品のライセンスコストやブラックボックスな検知ルールで運用していく対応コストを考慮すると、果たして効果が高いと言えるだろうかと疑問があったという。一方、InfoTrace Mark IIのログはサイバー攻撃に限定したものではないためITCCERTが担うセキュリティリスク全体への幅広い貢献が期待できた。もちろん、EDR製品には、異常な動作を止めるという決定的な機能差異はあるが、誤検知による停止リスクもある。

「我々がやりたいのはOSのシステム的な動作の監視による広範な異常検知網の確立です。サイバーセキュリティ視点で、InfoTrace Mark IIに期待した点もそこにありました。」（佐藤氏）

*EDR：Endpoint Detection and Response/従来型の脅威対策では100% 防御できないことを前提に、エンドポイントでの攻撃検知と早期対応を支援するソリューション。

* 本事例では、ユーザー操作ではない、OS やアプリケーション関連のイベントの記録を「システムログ」と表現しています。

取得したログと独自ルールを組み合わせ、セキュリティ対策を実施。脅威検知だけでなく、端末状況の可視化により対応スピードが向上

InfoTrace Mark IIは伊藤忠テクノソリューションズ株式会社（CTC）がシステムの導入を支援、端末にインストールされたクライアントからのログを統合ログ分析製品に取り込み、ITCCERT独自のルールによって「その時点で想定される様々な脅威の検知」を目指したセキュリティ監視を実施している。佐藤氏はInfoTrace Mark IIの魅力を「シンプルに、余計なことをせずにシステムログが取れるという点につきます。また、取得の設定が柔軟に行える点も魅力です。」と語る。

「当社は大半がビジネスユーザーであり、例えば社員が通常業務においてOSのシステムコマンドを使うことは、ほぼありません。こうしたコマンドが実行されると怪しい振る舞いだとすぐに判断することができ独自ルールを作りやすい点は恵まれた環境と言えるかもしれません。」

ITCCERTで同じく分析業務に携わる伊藤忠テクノソリューションズ株式会社 商社システム開発第1部 ネットワーク・セキュリティ推進課の岩永有平氏は、InfoTrace Mark IIの導入効果を次のように語る。

伊藤忠テクノソリューションズ株式会社
商社システム開発第1部
ネットワーク・セキュリティ推進課
岩永 有平 氏

「これまでは何かを検知した際、初動としてユーザーにヒアリングするか、実機を調査しなければなりませんでしたが、InfoTrace Mark IIでシステムログが正確に取得できるようになったおかげで、ユーザーにヒアリングしなくても端末の状況把握を正確かつスピーディに行えるようになりました。結果として対応処理の時間も削減されたと感じています。」

ソリトンとの共同プロジェクトを実施 機能拡充への貢献

ITCCERTとソリトンは2020年8月からの2か月間、共同プロジェクトを実施した。同社がInfoTrace Mark IIを”使い倒す”中で見えてきた課題点をソリトンと共有、両社のナレッジを交換して、さらなる監視強化や機能拡充を検討することが目的だ。

伊藤忠商事株式会社 IT企画部 ITCCERT サイバーセキュリティ分析官の丹羽祐介氏は本プロジェクトの具体的な活動について、次のように話す。

伊藤忠商事株式会社
IT企画部 ITCCERT
サイバーセキュリティ分析官
丹羽 祐介氏

「マルウェアの横展開挙動の可視化および検出、ADサーバー侵害の可視化、ランサムウェアの挙動検出、内部不正による情報漏えい対策などのテーマを設定し、当社が実利用する中で気づいた点や、レッドチーム演習*で収集したログ情報などを基にInfoTrace Mark IIで捉えるべき攻撃挙動を整理した上で、課題解決に必要となる設定変更や追加機能について両社で検討しました。プロジェクトとしては2か月ほどで一区切りとしましたが、現在も定期的に情報交換を行っています。」

このプロジェクトで得られたアイデアは、2020年9月に発表された新バージョンにも生かされている。InfoTrace Mark IIの

伊藤忠商事株式会社 様

新バージョンでは、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、端末管理機能が標準搭載されたほか、国内でも感染を広げる新種のマルウェアの感染確認に役立つ情報が記録できるようになるなど、ログ取得範囲も拡充された。この点について佐藤氏は、「これまで、ユーザーからの『怪しい添付ファイルを誤って開いてしまった』という報告では、開封者自身も慌てていて、自分がどのような操作をしたか明確に記憶していないことが多く、細かい確認が必要でした。その点について伝えたところ、すぐに機能追加いただき、例えばマクロ実行の有無など詳細な挙動がログから分かるようになり、対応が効率的になりました。ソリトンには我々の意向を的確にくみ取っていただいた。また、ソリトンの開発陣の皆様は早期の実装に繋げていただいた。この動きには感謝しかない。」と高く評価する。

* レッドチーム演習：攻撃者視点で疑似的なサイバー攻撃を実施し、企業や組織が適切に対応できるかを評価・改善する対策強化手法。

今後、重要性が高まるエンドポイントセキュリティ。ビジネスに集中できる環境の提供に貢献するInfoTrace Mark IIと今後

佐藤氏は「今後、TLS1.3*やDoH（DNS over HTTPS）*などが普及し、通信経路の暗号化が更に進むことで、これまで以上にネットワークでのモニタリングが難しくなることが予想され、エンドポイントセキュリティの意義は増していくと思います。」と語る。そしてITCCERTに求められる役割とソリトンへの期待について、次のように結んだ。「ITCCERTにおけるサイバーセキュリティへの取り組みは、社員にセキュリティを意識させずビジネスに集中できる環境、そして万一事案が発生した場合にも、その原因にすぐにリーチし、被害の増大を抑えるための取り組みでもあります。その取り組みに貢献しているInfoTrace Mark IIには、今後もシンプルに今の品質を担保していっていただきたい。ソリトンにはこれからも継続的な情報交換や、日本のビジネス環境に安全をもたらす製品開発への取り組みに期待しています。」

*TLS 1.3: Transport Layer Security（TLS）は、暗号化プロトコル TLS の新しいバージョン。パフォーマンスとプライバシー、セキュリティが強化された一方、従来のようにネットワーク型製品を中間に設置しても暗号化通信を復号したり、コントロールしたりすることが出来なくなる。

*DoH（DNS over HTTPS）: HTTPS を用いて DNS 通信を行うプロトコル。従来の DNS への問い合わせは平文でおこなわれていたため盗聴や改ざんに弱い課題があったが、暗号化プロトコルである HTTPS のセキュリティ性質を生かすことでこれらの課題を解決し、安全な DNS 通信が実現できる。

CTC Challenging Tomorrow's Changes

伊藤忠商事株式会社における、InfoTrace Mark II およびInfoTrace Mark II のログを統合ログ分析製品に取り込み、ITCCERT 独自のルールによってセキュリティ監視を行う仕組みは、伊藤忠テクノソリューションズ株式会社（CTC）の支援により導入されました。

Soliton®
株式会社ソリトンシステムズ　https://www.soliton.co.jp/
〒160-0022　東京都新宿区新宿 2-4-3
TEL 03-5360-3811　netsales@soliton.co.jp
大阪営業所 06-7167-8881　福岡営業所 092-263-0400
名古屋営業所 052-217-9091　東北営業所 022-716-0766
札幌営業所 011-242-6111

このカタログは 2021 年 2 月現在のものです。仕様、デザインは予告なく変更することがあります。　CS-MK2-itochu-2102A