



トラフィック分析による現状評価サービス

ネットワークトラフィックから現状の脅威や被害状況を把握する

トラフィック分析による現状評価サービスの概要

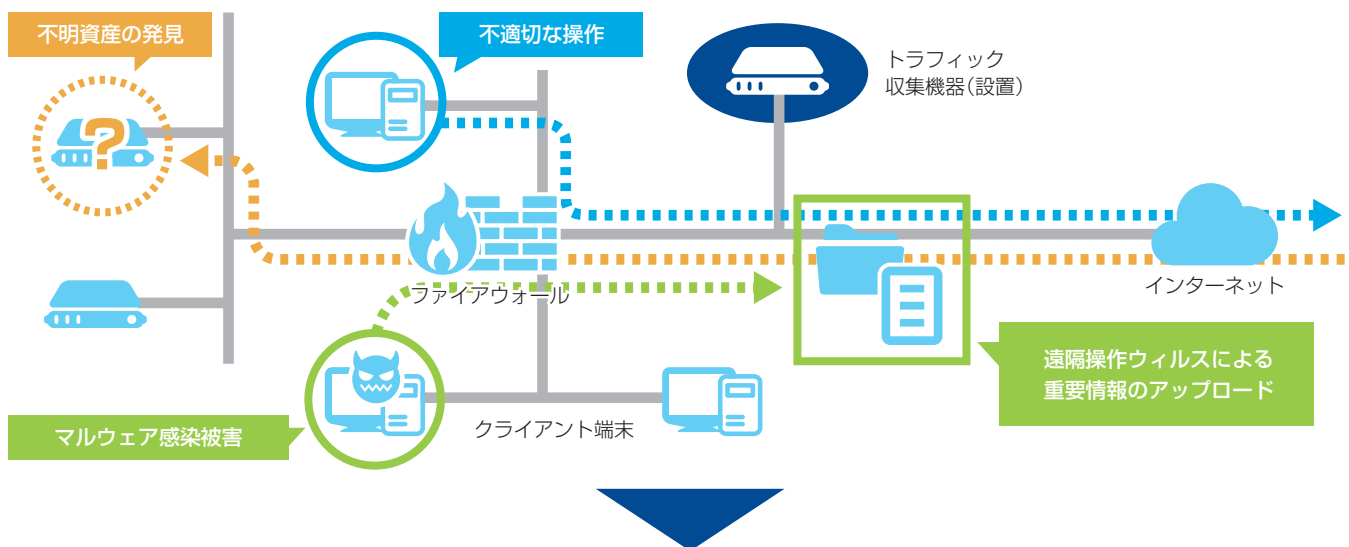
近年のサイバー攻撃の多くはマルウェア対策ソフト等の既存の対策のみでは検出が困難です。

また、従業員によるクラウドストレージの無断利用や私物スマートデバイスのネットワーク接続など、組織として意図しない通信も増加しております。このように発見が難しくなっている脅威や被害を可視化する1つの方法として、組織内から発生するネットワークトラフィックを分析する方法があります。本サービスでは、組織内のネットワークトラフィックを一定期間取得し、その内容を分析します。取得トラフィックを分析することにより、ネットワークに接続されている資産や脅威を洗い出します。

トラフィック分析による現状評価サービスの特徴

本サービスは、組織内のトラフィックを分析することにより、「マルウェア感染被害」、「不適切な操作」、「不明資産の発見」といった脅威の洗い出しを行ないます。

脅威の把握



トラフィックの分析結果例

マルウェア感染被害

遠隔操作ウィルスなどにより生じたトラフィックを発見することができます。

不適切な操作

従業員の利用する端末からのトラフィックを分析し、どのような操作が行われているかを知ることができます。

不明資産の発見

BYOD(私的デバイス利用)により持ち込まれた所有者不明、用途不明のシステムの検出ができます。
※貴社へのヒアリングなど作業が発生します。

トラフィック分析による現状評価サービスのアウトプットイメージ

トラフィック分析による現状評価サービスでは、次の分析方法を用いて事象を確認します。

| 分析手法 | 説明 |
|-------------------------|---|
| データベース照合 | 独自のデータベースに含まれるブラックリスト及び異常パターンとの照合を行います。本データベースの情報は商用およびオープンインテリジェンスから得られた情報やデロイトが独自に収集した情報から構成されています。 |
| ネットワークフロー分析 | 通信先の国情報や使用する通信ポートをキーに、ある特定の日から突発的に発生した通信や異常発生する通信、常習性や周期性、規則性を持つ通信を調査します。 |
| ストリームデータ分析 | パケットストリームデータ部の異常パターンの検出やデータ部の再構築を行い、ダウンロードファイルのマルウェア解析を行います。 |
| プロトコル分析 (非標準プロトコル含む) | 上記解析方法から得られた情報をもとに、通信プロトコルやアプリケーション通信の識別を行います。また、異常通信の検出も可能なため、マルウェア通信の検出も期待できます。 |
| アナリティクス分析 | 変化点検出技術により、マルウェア等が利用する特有の通信の検出を行います。 |

トラフィック分析による現状評価サービスの進め方

トラフィック分析による現状評価サービスは、次の4つのフェーズから構成されています。



対象組織のシステムやネットワーク構成を確認します。また、トラフィック取得の最適なポイントや期間について検討します。

パケットキャプチャ用の装置を設置し、トラフィックの取得を実施します。

取得トラフィックを弊社解析環境で分析します。分析は、上表記載の複数の分析手法を組み合わせ実施します。

分析結果を報告書に取り纏めます。また、報告会を開催し、検出された課題内容の説明や対策方法等の助言を行ないます。

国内ネットワーク

有限責任監査法人トーマツ

東京 〒100-0005 東京都千代田区丸の内3-3-1 新東京ビル Tel:03-6213-1112
大阪 〒541-0042 大阪府大阪市中央区今橋4-1-1 淀屋橋三井ビルディング Tel:06-4560-6021
名古屋 〒450-8530 愛知県名古屋市中村区名駅3-13-5 名古屋ダイヤビルディング3号館 Tel:052-565-5517
福岡 〒810-0001 福岡県福岡市中央区天神1-4-2 エルガーラ Tel:092-751-1517

デロイト トーマツ リスクサービス株式会社

本社 〒100-0005 東京都千代田区丸の内3-3-1 新東京ビル Tel:03-6213-1300

トーマツグループは日本におけるデロイト トウシュ トーマツ リミテッド(英国の法令に基づく保証有限責任会社)のメンバーファームおよびそれらの関係会社(有限責任監査法人トーマツ、デロイト トーマツ コンサルティング株式会社、デロイト トーマツ ファイナンシャルアドバイザー株式会社および税理士法人トーマツを含む)の総称です。トーマツグループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各社がそれぞれの適用法令に従い、監査、税務、コンサルティング、ファイナンシャルアドバイザー等を提供しております。また、国内約40都市に約7,600名の専門家(公認会計士、税理士、コンサルタントなど)を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はトーマツグループWebサイト(www.tohmatsu.com)をご覧ください。

Deloitte(デロイト)は、監査、税務、コンサルティングおよびファイナンシャル アドバイザーサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150カ国を超えるメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを提供しています。デロイトの約200,000名におよぶ人材は、“standard of excellence”となることを目指しています。

Deloitte(デロイト)とは、デロイト トウシュ トーマツ リミテッド(英国の法令に基づく保証有限責任会社)およびそのネットワーク組織を構成するメンバーファームのひとつあるいは複数指します。デロイト トウシュ トーマツ リミテッドおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。その法的な構成についての詳細は www.tohmatsu.com/deloitte/ をご覧ください。