

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

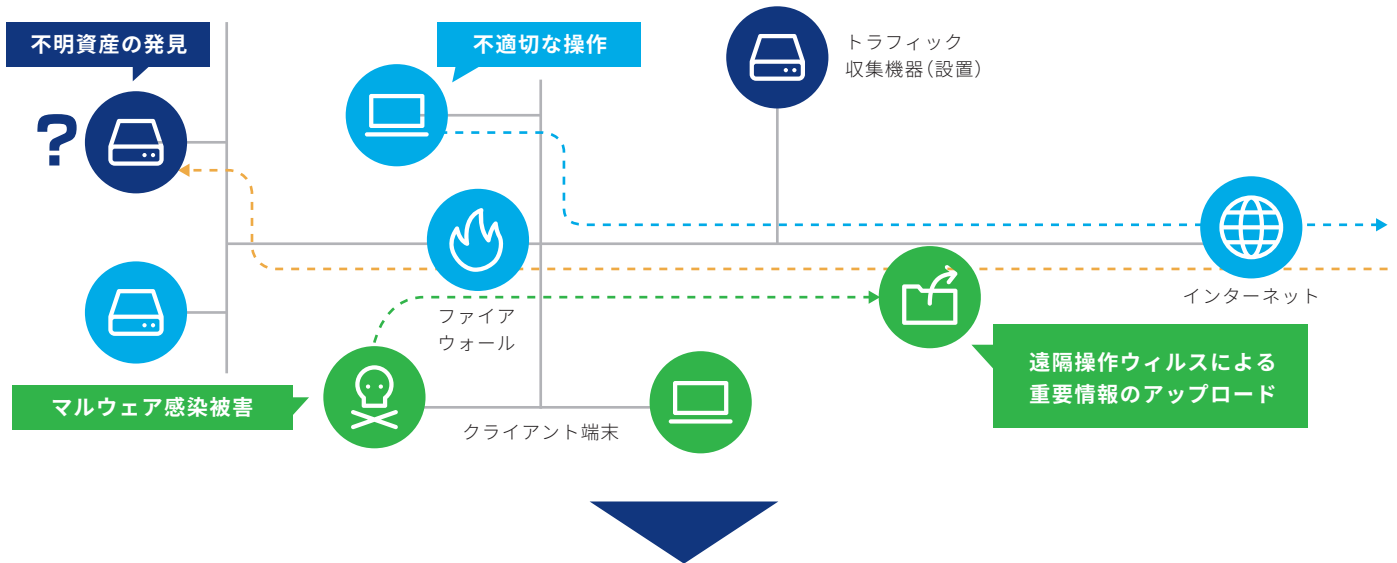
近年のサイバー攻撃の多くはマルウェア対策ソフト等の既存の対策のみでは検出が困難です。また、従業員によるクラウドストレージの無断利用や私物スマートデバイスのネットワーク接続など、組織として意図しない通信も増加しております。このように発見が難しくなっている脅威や被害を可視化する一つの方法として、組織内から発生するネットワークトラフィックを分析する方法があります。

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。取得した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

遠隔操作ウイ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。

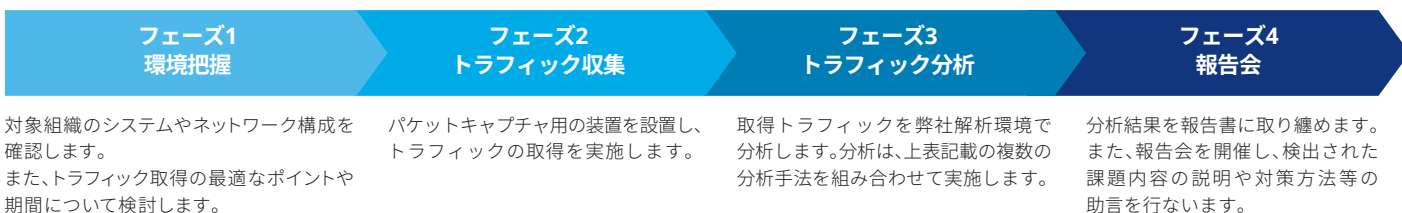
トラフィック分析による現状評価サービスのアウトプットイメージ

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 (非準拠プロトコル含む)	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。



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
名古屋 〒450-6337 愛知県名古屋市中村区名駅1-1-1 JPTタワー名古屋 Tel:052-565-5950

デロイト 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のグループ法人(有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザー合同会社、デロイト トーマツ 税理士法人およびDT(弁護士法人を含む)の総称です。デロイト 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、各法人がそれぞれの適用法令に従い、監査、税務、法務、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います。また、国内約40都市に約8,700名の専門家(公認会計士、税理士、弁護士、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。詳細はデロイト トーマツグループWebサイト (www.deloitte.com/jp) をご覧ください。

Deloitte(デロイト)は、監査、コンサルティング、ファイナンシャルアドバイザーサービス、リスクマネジメント、税務およびこれらに関連するサービスを、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を超える国・地域の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 Fortune Global 500® の8割の企業に提供しています。“Making an impact that matters”を自らの使命とするデロイトの約225,000名の専門家については、Facebook、LinkedIn、Twitterもご覧ください。

Deloitte(デロイト)とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド (“DTL”)ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数指します。DTL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。DTL(または“Deloitte Global”)はクライアントへのサービス提供を行いません。Deloitteのメンバーファームによるグローバルネットワークの詳細は www.deloitte.com/jp/about をご覧ください。

Member of
Deloitte Touche Tohmatsu Limited