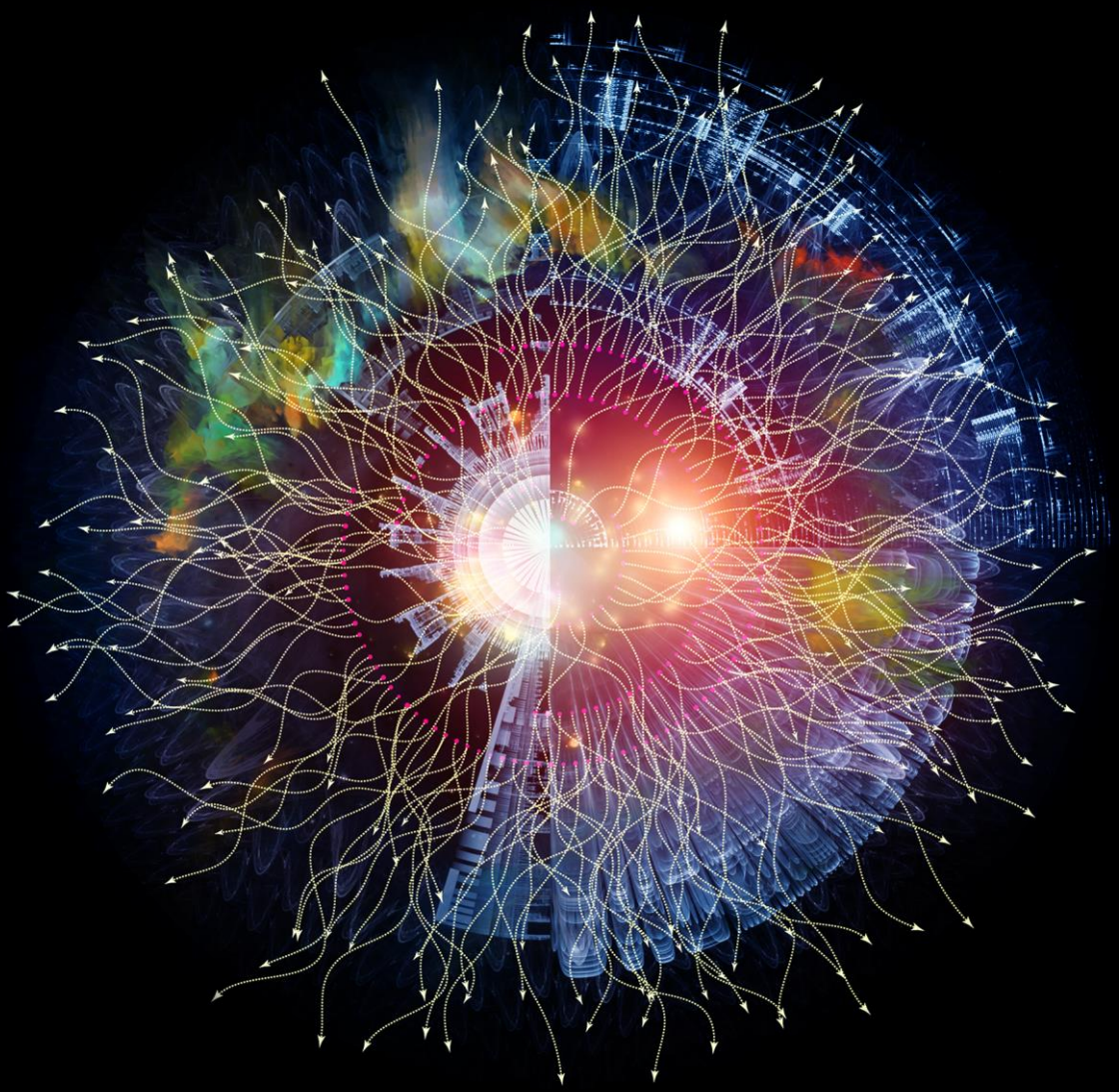
Deloitte.
デロイト トーマツ



Deloitte Cyber Trends & Intelligence Report

2022

Nov 2022
デロイト トーマツ サイバー合同会社
Cyber Intelligence Center (CIC)

はじめに

国家間の緊張が高まり地政学リスクが高まっていること、自動車部品メーカーがランサムウェア攻撃を受けたことで連係関係にある大手自動車メーカー(OEM)が製造ラインを停止させたこと、この2つの出来事によって2022年は初頭からサイバーリスクの増大を予感させられるスタートを迎えました。

国際紛争とサイバー攻撃という点では、ハクティビストに加え、国家の呼びかけにより一般人が"サイバー軍"の民兵として相手国や相手国の重要インフラへの攻撃に参加するという今までになかった構図が生まれ、今後の国家間紛争におけるサイバー戦の新しい形を示しました。

また、昨年より猛威を振るっているランサムウェアの勢いは衰えることなくその被害が広がっています。2022年10月には奈良県の県民の約半数が会員となっている食品配送業団体がランサムウェア攻撃を受け、食品の配送が長期に渡って止まる可能性が高い状況であることが報道によって伝えられています。攻撃先を特定の標的・産業に限定することなく、インターネット側から見て脆弱な機器や不適切な設定がなされている機器を手当たり次第に攻撃する二重恐喝ランサムウェアによって、私たちの日常生活に大きな影響が起こりうることが証明されたと言えるのではないでしょうか。

さらに、前述したOEMの事案後、取引先がランサムウェア被害に遭うことで自社の生産が影響を受けないかというサプライチェーンリスクに関する議論も活発化しており、従来の性善説に基づくアセスメントの限界が見えてきました。

こういった状況の中、本レポートでは二重恐喝ランサムウェアの脅威動向をお伝えすると共に、昨今サプライチェーンリスクの観点でも注目を集めているアタック・サーフェスマネジメント（ASM - Attack Surface Management）をご紹介します。

また、やや技術寄りの内容になりますが、Webアプリケーションの不正操作の検知やデロイト CICで数年前から導入しているSOAR(Security Orchestration, Automation, and Response)運用の舞台裏をご紹介するとともに、マルウェアEmotetを題材にEDRとネットワークログの統合監視によるインシデント全体像の可視化について解説します。

本レポートが各社における脅威情報のインプットとして、対策立案の参考としてご活用いただければ幸いです。

ランサムウェア脅威の動向

ランサムウェアはPCなどのデータを暗号化し、それを解除するためのカギと引き換えに金銭を要求するマルウェアです。元々は個人のPCを標的としていましたが、2015年頃から企業等の内部ネットワークに侵入し、システム全体を利用不能にして業務継続を盾に脅迫するものが出ています。

2019年後半以降はデータを暗号化する前に盗み出し、支払いに応じなければデータを暴露すると脅す「二重恐喝(Double Extortion)」手法が登場して被害を広げています。この手口では、ITシステムが利用できなくなることで業務継続が脅かされるだけでなく、データ暴露によりレピュテーションも毀損されます。

支払いに応じなかった企業等のデータは、攻撃者がダークWeb上に開設した「リークサイト」で公開され、リークサイトにアクセスすることができれば誰でもダウンロードできるようになります。ランサムウェア攻撃グループの多くがこうしたリークサイトを運営しており、セキュリティ監視を行っているデロイト CICでは通算で70個以上のリークサイトを確認しています。

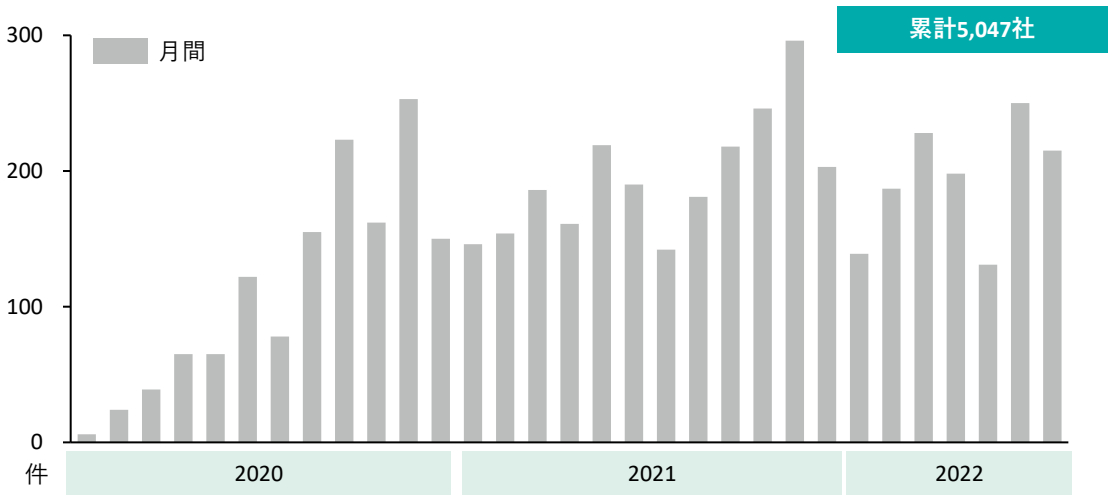
図表1　二重恐喝ランサムウェアの概要

二重恐喝ランサムウェアによるデータ暴露被害の状況

リークサイトでデータを暴露された企業等の件数推移は図表2の通りです。2020年3月頃からリークサイトを開設する攻撃グループが増えたことで被害件数も増加し、2022年7月末時点で累計5,047社以上のデータが世界全体で暴露されています。

リークサイトは開設・閉鎖が頻繁に行われていますが、2021年以降は常時20～30個程度が稼働し、月間で約200社のデータが暴露される事態となっています。

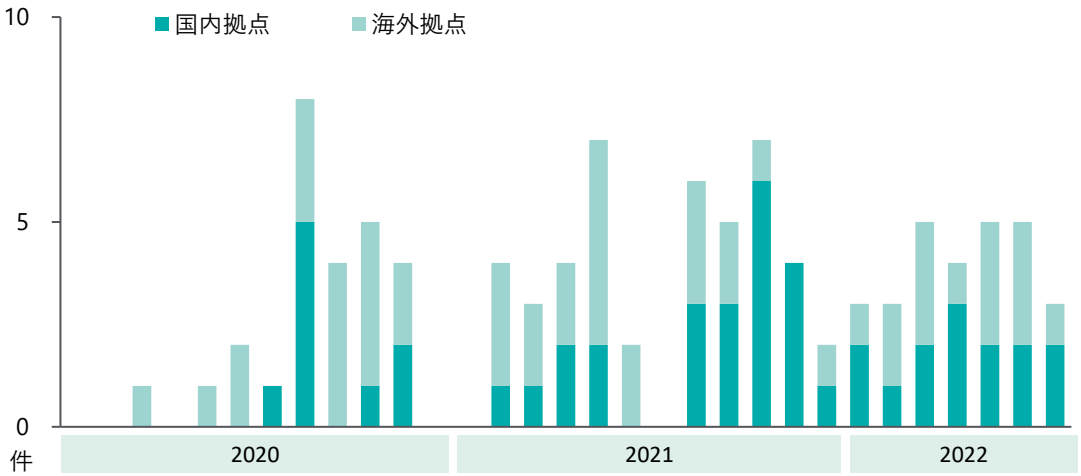
図表2　リークサイトでデータを暴露された企業等の件数の推移



出所：デロイトCICの調査により作成

二重恐喝ランサムウェアによるデータ暴露は、日本企業にとっても無縁ではありません。図表3に示すように、2021年中盤以降では国内拠点、海外拠点あわせて毎月5社程度のデータがリークサイトで暴露されています。

図表3　日本企業のデータ暴露被害件数の推移



出所：デロイトCICの調査により作成

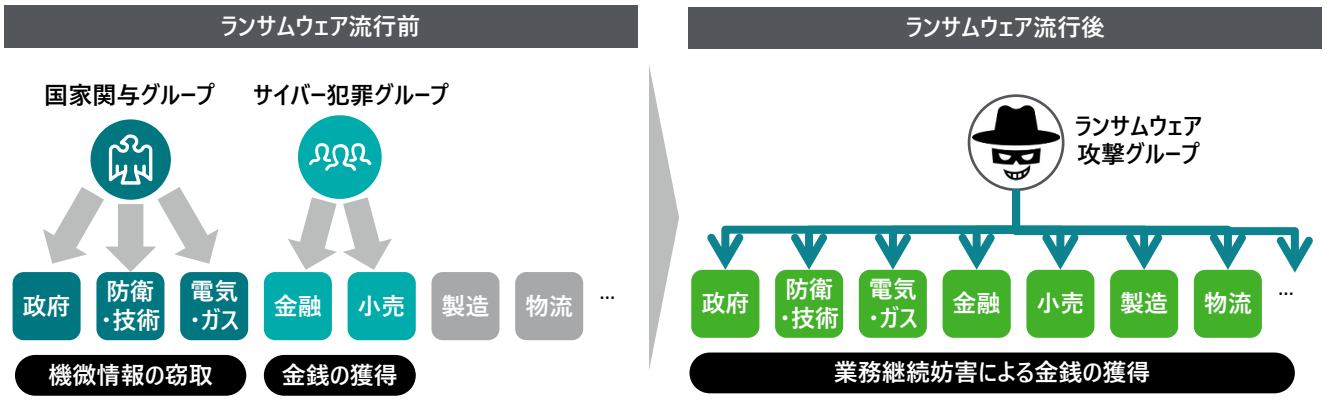
ランサムウェア被害と業種

ランサムウェア攻撃グループが用いる攻撃手法は決して新しいものではありません。それでも被害が拡大しているのは、ネットワーク内に侵入する攻撃への対策が不十分な組織が多いことを示しています。これは、ランサムウェアの登場により脅威環境が大きく変化したことが原因と考えられます。

従来、ネットワーク内に侵入する攻撃の多くは機微情報の窃取を目的とするものでした。国家関与グループであれば政府機関や防衛産業、先端技術、ライフラインなどを対象とし、サイバー犯罪グループであれば金融機関や小売店などが主な標的となっていました。このように、従来はネットワーク内に侵入する攻撃の影響を受ける業種は概ね決まっていたといえます。

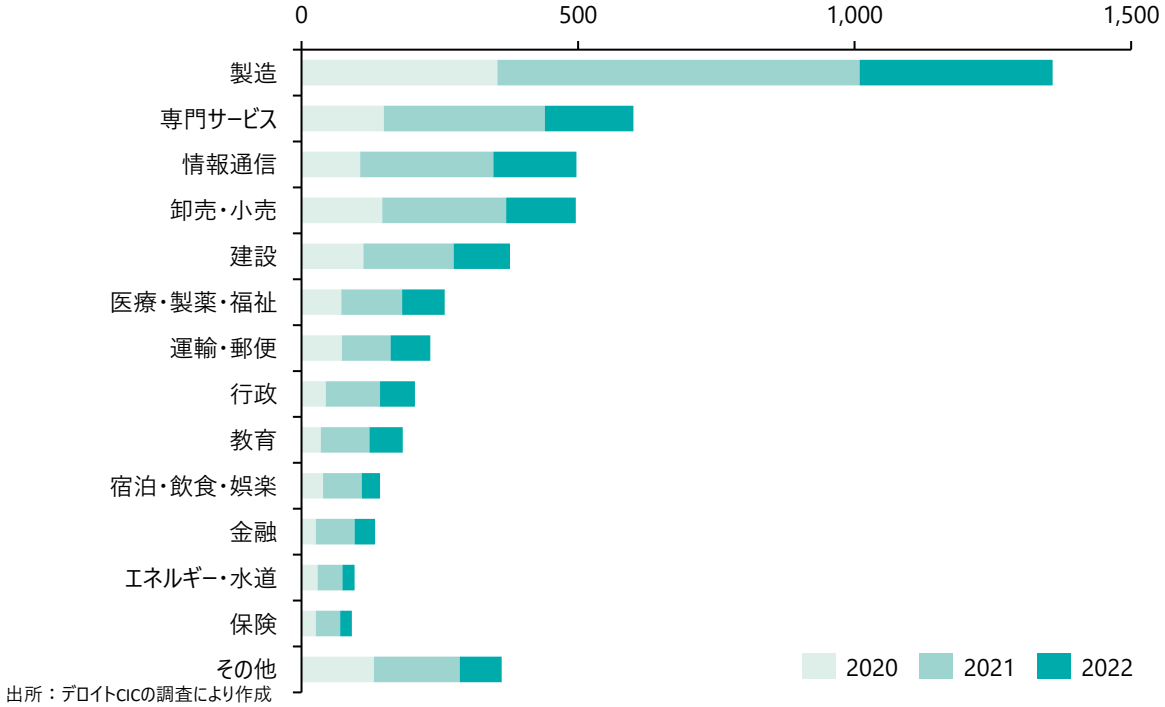
ところが、ランサムウェアの流行により状況が一変しました。ランサムウェア攻撃は業務継続を盾にとるため、攻撃者にとってあらゆる業種の組織が標的となります。このため、これまで標的となることが少なく対策が不十分な組織が狙い撃ちにされ、多くの被害を出しているものと考えられます。

図表4　業種別におけるランサムウェア流行前後の脅威比較



実際に、二重恐喝によるデータ暴露被害について業種ごとに世界全体の被害件数を見ると、製造業を始めとして幅広い業種で被害が出ていることが分かります(図表5)。

図表5　業種別データ暴露被害件数



出所：デロイトCICの調査により作成

尚、製造業の被害が最も多いのは、他業種に比べて企業数が多いことに加え、中小企業が多く、サイバーセキュリティ上の対策が不十分であることが影響していると考えられます。もし、重要な部品の生産を担っているサプライヤーがランサムウェア攻撃により業務中断を余儀なくされた場合、その影響は生産を担っている企業だけにとどまらず、その部品を調達している企業やその他関連する多くのステークホルダーにまで及びます。

業務継続に影響するランサムウェア攻撃が製造業に対して活発に行われている状況は憂慮すべきものであり、企業の生産活動においてサプライチェーンリスクが高まっているといえます。

ランサムウェア対策と Attack Surface Management

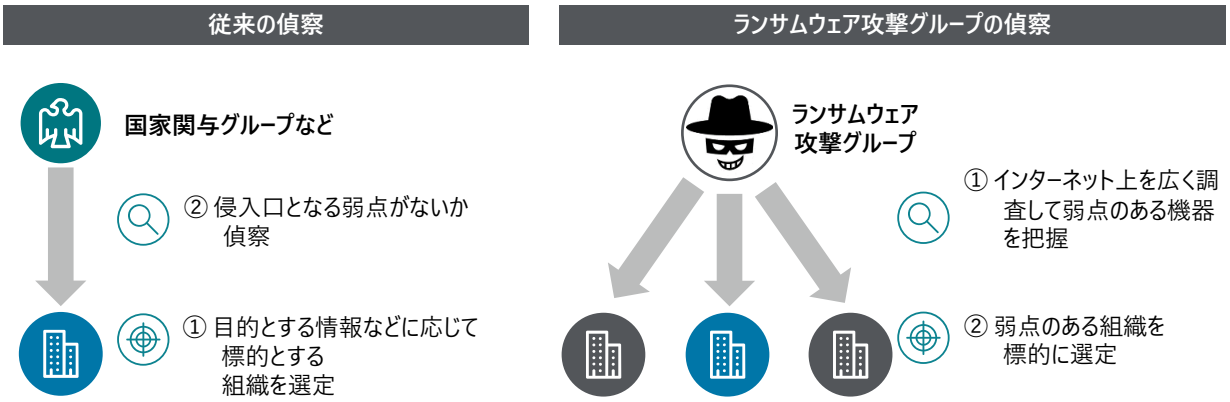
攻撃者の偵察活動

前述の通り、ランサムウェア攻撃は業務継続を盾にとるため、攻撃者にとってはあらゆる業種が標的となります。サイバー攻撃の前には標的の弱点を調査する偵察活動が行われることが一般的ですが、この偵察のやり方もランサムウェア攻撃者とそれ以外では異なります。

図表1に示すように、従来の攻撃ではその目的に応じてまず標的とする組織が選定され、その組織の内部ネットワークへの侵入口を探るために偵察が行われます。

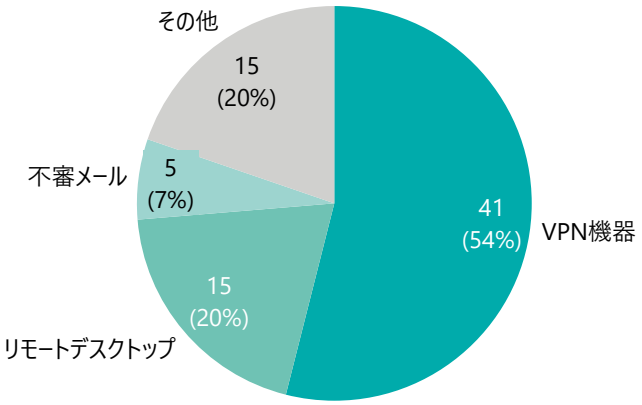
一方、ランサムウェア攻撃では、まずインターネット上を広く調査して外部から侵入できる弱点のある機器を把握します。そして、弱点のある機器をもつ組織を標的として選定します。

図表1　従来の偵察とランサムウェア攻撃グループの偵察



また、日本国内のランサムウェア被害における初期侵入経路を見ると、VPN機器、リモートデスクトップという外部からアクセス可能な機器が7割以上を占めています（図表2）。基本的なことながらも、インターネットに接続されている機器のセキュリティの重要性を示すものであるといえます。

図表2　日本国内のランサムウェア被害における初期侵入経路



出所：警視庁「令和３年におけるサイバー空間をめぐる脅威の情勢等について」,2022年4月7日を元にデロイトCIC作成

Attack Surface Management（ASM）とは

VPN機器やWebサーバーなど、外部からの攻撃に晒される箇所はAttack Surface（攻撃対象領域）と呼ばれます。ランサムウェア脅威の増大により、近年攻撃される可能性のある機器、すなわちAttack Surfaceを適切に管理することの重要性が高まっています。

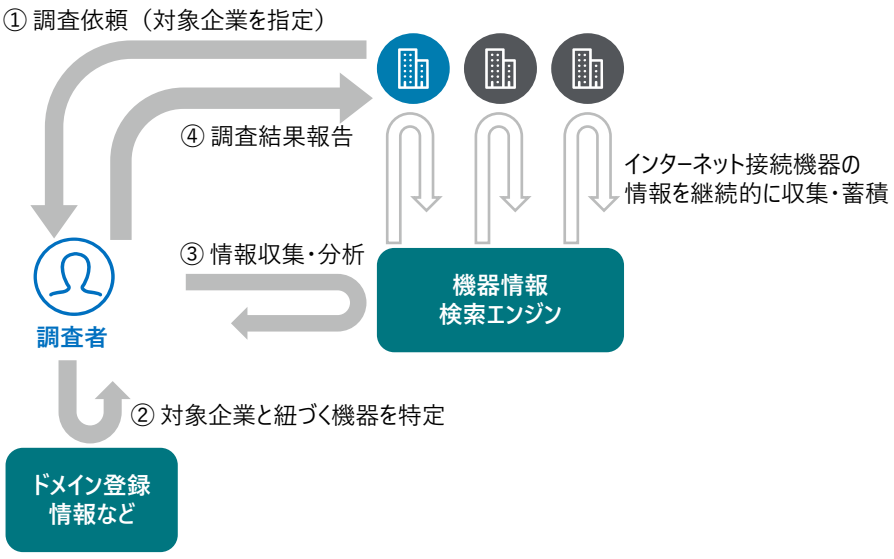
図表3　Attack Surfaceとは

インターネット接続機器を適切に管理することの重要性は広く認識されています。しかし、これを実行するのは容易ではありません。主に次のような理由で、インターネット接続機器が脆弱な状態に置かれているケースが散見されます。

- 各事業部門が独自に運用しているサーバーがIT部門の管理外で、脆弱性管理などが行われていない
- 海外拠点のIT環境を現地に任せており監督していない
- 保守作業などで一時的に行った設定変更が戻されていない

インターネット接続機器の管理状況の実態を把握するうえで、各機器の管理者による自己申告では限界があります。
そこで近年注目されているのが、Attack Surface Management（ASM）と呼ばれる取り組みです。
ASMでは、対象とする組織のインターネット接続機器を外部から調査してその状態を把握します。調査に使用するのは誰でも利用可能な公開情報源（機器検索サービス等）であり、IT資産台帳などの内部の情報は使用しません。調査に使用する情報源は攻撃者も偵察の際に使用するものであり、「攻撃者からどう見えているか」を把握できます。

図表4　Attack Surface Managementの流れ



ASMとプラットフォーム診断の違い

インターネット接続機器の状態を把握する手段としては、従来からプラットフォーム診断があります。機器の状態を把握するという目的は同じであるものの、ASMとプラットフォーム診断では図表の通りアプローチが異なります。

図表5　ASMとプラットフォーム診断のアプローチの違い

	ASM	プラットフォーム診断*
対象とする機器	実施者側で洗い出し	依頼者側が指定
調査方法	■ 外部の情報源を使用 ■ 対象機器へのアクセスはほとんどなし	対象機器に対して疑似攻撃コードを送信

＊　疑似攻撃コードの送信やポートスキャンなど対象機器に直接調査目的の通信を行うものを想定しています。
プラットフォーム診断の実施方法は企業によってさまざまであり、このアプローチをとらないものがある点に留意が必要です。

プラットフォーム診断では、依頼者側が対象とする機器を指定するため、管理から漏れている機器はカバーできません。また、直接疑似攻撃コードなどの送信を行うため、実施にあたっては機器の管理者と調整しないと攻撃と誤認される恐れがあります。

一方、ASMは調査者側が機器の洗い出しを行うため、管理から漏れている機器もカバーできます。また、対象機器へのアクセスはほぼないため、運用中の機器に対して事前の調整なしで安全に実施できるのが特徴です。

ASMとサプライチェーンリスク

ASMは機器に直接アクセスせずに調査することから、自社管理外の機器に対しても事前の調整なしに安全に実施できます。

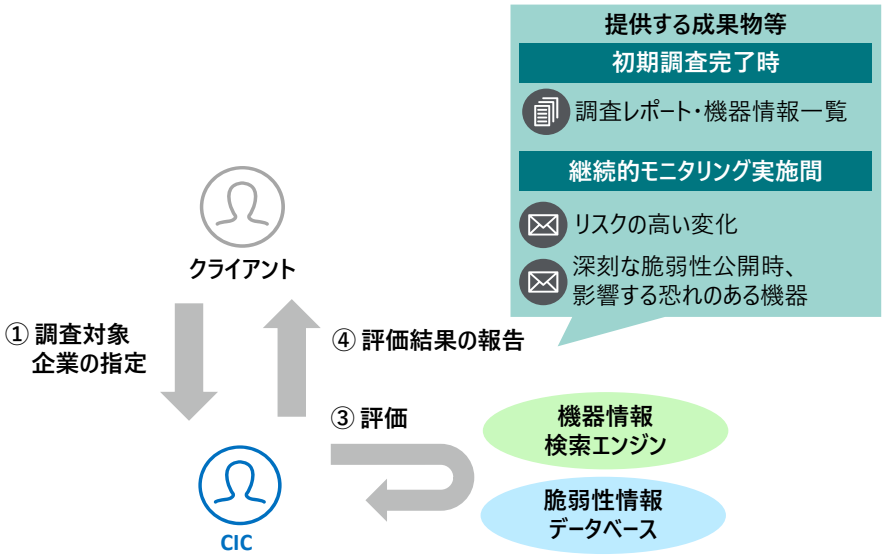
前述の通り、最近ではサプライヤーがランサムウェア攻撃の被害を受けることで、その取引先の生産活動に影響する可能性が増しています。重要なサプライヤーをASMでカバーすることで、自社グループだけでなくサプライチェーン全体のサイバーセキュリティを強化することができます。すでにこうしたアプローチを取り入れる日本企業も出てきています。

デロイトのAttack Surface Management「侵害リスク評価サービス」

デロイト CICでは、Attack Surface Managementをサポートする「侵害リスク評価サービス」を提供しています。2020年1月からワンショットの調査サービスとして提供しており、これまでに製造業、金融、電気・ガスといった業界のお客様20社以上に提供した実績があります。

また、2022年からは年間を通じた継続モニタリングもサービスラインナップに加えました。機器情報の収集・分析に加え、お客様の機器で稼働する重要なソフトウェアについて脆弱性情報のモニタリングも行うことで、新たな脆弱性が発見された場合の初動対応もサポートできるのが特徴です。

図表6　侵害リスク評価サービスの概要



セキュリティ機器では発見できないWebアプリケーション機能に対する不正操作の監視

Webの利用拡大と共に、多様なWebアプリケーションが開発されてきました。身近なものではECサイトやSNS、また会社のシステムで行う経費申請や勤怠システムなどの多くもWebアプリケーションで運用されています。Webアプリケーションを使ったサービスは私たちの生活や仕事に恩恵を与える一方で、多くの不正操作のターゲットとなっています。特に不正ログインをはじめとしたWebアプリケーション機能を悪用した不正操作は、通信上は正常なアクセスと変わらないため、IDS/IPS、WAF等のセキュリティ機器では対応できない脅威となっています。

本稿では、こうした脅威への対策として、Webアプリケーションのログを監視する方法をご紹介します[1]。

Webアプリケーション機能を悪用した不正操作とは何か

SQLインジェクション等の攻撃では、情報窃取等を行う悪性コードやコマンドを注入して、Webアプリケーションが同処理を行うように悪用します。しかしWebアプリケーション機能を悪用する不正操作は、悪性コードを用いません。その手法として、何らかの方法で入手した情報を使って正規ユーザーになりすましたり、アプリケーションの仕様の不備を突いたりすることで、不正操作が行われます。

その一例として、パスワードリスト攻撃等による不正ログインが挙げられます。ユーザーが複数のWebサービスで同じユーザーID、パスワードを使い回していた場合、パスワードリスト攻撃ではこの使い回しが悪用され攻撃が行われます。攻撃者は、外部から何らかの手段で窃取したユーザーID、パスワードのリスト[2]を使ってログインを試行し、ECサイト等にアクセスしてポイントの不正利用や会員情報の不正閲覧などを行います。

セキュリティ機器によるWebアプリケーション機能を悪用した不正操作検知の難しさ

図表1はユーザーID、パスワードとしてWebアプリケーション上でやり取りされる情報例です。

図表1　正常な通信、攻撃通信、不正ログインにおける通信内容

（1）	正常な通信 (ログイン成功)	userID=UserA&password=abcd
（2）	脆弱性を試行する攻撃通信 (悪性ファイルをダウンロード)	userID=UserA&password=wget (省略)
（3）	不正ログイン (窃取情報によるログイン)	userID=UserZ&password=zzzz

(1)は、正常なログインの際にやり取りされる情報、(2)は、サーバーに悪性ファイルのダウンロードの命令を試行する脆弱性の攻撃通信の例となります。「wget」は、指定したURLにあるファイルをダウンロードするサーバーコマンドですが、Webアプリケーションでサーバーのコマンドを送信することはほとんどあり得ません。IDS/IPS、WAFなどのセキュリティ機器は、このようなサーバーコマンドの文字列が含まれている不審な通信を検知します。これは他の脆弱性でも同様で、SQLやコード等の不審な文字列を探し出して不正アクセスとして検知することが可能です。

一方、(1)と(3)の不正ログインを比較するとわかる通り、いずれも通信上は不審な文字列がありません。したがってセキュリティ機器では正常な通信に見えるため、不正な動きとしての検知は難しくなります。

*1：webアプリケーションに焦点を当てて紹介しますが、同様にスマートフォン、タブレットからWebアクセス可能なモバイルアプリケーションの監視も可能です。
*2：ダークWeb(特殊なツールを利用しないとアクセスできない領域)では、これらのユーザーID、パスワードの情報が売られていたり、流通していたりする事例もあります。

Webアプリケーションログの監視による不正操作の検知、可視化

前頁では一例として紹介しましたが、Webアプリケーション機能を悪用した不正操作を可視化して検知するためには、Webアプリケーションログに記録される操作傾向を監視することが必要となります。

図表2はログに取り込まれたWebアプリケーションへのログイン時の情報です。それぞれの明細を見ると正常なログイン通信に見えますが、不正ログインを疑う場合、複数の明細を組み合わせて、送信元IPアドレス、ユーザーID、機能、ログイン試行の間隔などの操作傾向を監視します。

図表2　ログに取り込まれたログインのWebアプリケーションのログイベント例

#	時刻	送信元IPアドレス	ユーザーID	ログイン結果	パス: 機能(URL)
1	12:00:01	送信元IPアドレスA	userA	ログイン成功	/login
2	12:00:14	送信元IPアドレスB	userB	ログイン成功	/login

Webアプリケーションログ監視例

Webアプリケーションログ監視のアプローチ

Webアプリケーションのログ監視では、一般的に次の2つのアプローチがあります。

1つ目は、「閾値による監視」です。特定の操作に関して閾値を設定して、閾値を超えた場合は不正操作と検知する方法です。この方法では、ログイン等の特定の操作に対して「m分間にn回以上～の操作」をした場合に不正操作として検知します。

2つ目は「複数操作の相関からの監視」です。この方法では、「Aの操作をした後に、Bの操作を行う」という複数操作の流れから不正と判断するユースケースを定義して、検知ルールを設定します。

以降でそれぞれのアプローチによる監視例を説明します。

閾値による監視

閾値による監視に関しては、多要素認証の突破を例に説明します。

不正操作手順: 多要素認証の突破

近年では不正ログイン対策として、ログインの際に、ユーザーID、パスワード以外の要素の照合を行う多要素認証を実装しているWebアプリケーションが多くなっています。例えば、「スマホ通知によるログイン承認」では、ユーザーのスマホの多要素認証アプリにログイン承認依頼の通知を表示させ、ユーザーが承認ボタンを押下することで正規ユーザーとして認証されます。しかしこの方法は不正ログイン後、就寝時間帯に大量の承認依頼を行い、通知を煩わしく感じたユーザーが承認ボタンを不注意で押下するという突破例が確認されています。攻撃の流れは次の通りとなります。

■ プロンプト爆撃(ログイン承認を求める通知の大量送信)

1. 攻撃者が外部サイトで窃取したログインID、パスワードでログインを試行
2. 就寝時間帯にログイン承認依頼の通知を大量送信
3. ユーザーに承認ボタンを誤って押下させる

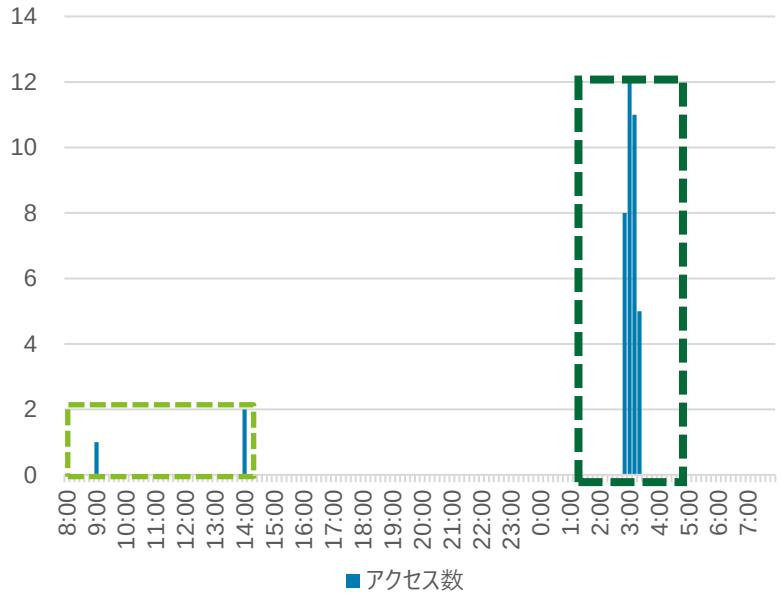
当該攻撃では、ビジネス用サービスでの会員アカウントの不正利用等が確認されています。

監視方法

監視するにあたって重要なことは、「何が正常で、何が異常か」を判別することです。当該攻撃の監視では、ログイン承認依頼通知のリクエスト通信を見ることで対応が可能となります。

図表3は特定のユーザーAのログイン承認依頼の通知のリクエストが何時に何件送信されたかを10分単位で示したグラフです。

図表3　ユーザーAによる10分単位におけるログイン承認依頼に関する通知件数の推移



出所：デロイトCICの調査により作成

緑枠の正常な通知では日中に1～2件のみ送信されているのに対し、赤枠の時間を見ると、夜中に合計36件発行されています。通常、正規のユーザーがこのような操作を行うことは考えにくいので、攻撃者が通知を悪用した攻撃を実施した恐れがあります。したがって、例えば「同じユーザーが夜間に短時間に複数回以上通知を実施」という閾値のルールを設定し、不正な動きを可視化することが効果的です。

このような閾値を基にした監視は、他にもシステムへのログイン状況、管理者権限の利用状況、ECサイトでのポイントチャージの回数など、様々な操作に対して適用が可能です。

複数操作の相関からの監視

複数操作の相関からの監視では、ECサイトでの不正な商品注文を例に説明します。

不正操作手順: ECサイトでの不正な商品注文

攻撃者はECサイトに不正ログインした後、なりすましたユーザーIDで不正に商品注文するため、あらかじめ、登録住所やメールアドレスを変更しようとします。登録住所は攻撃者が商品を受け取るために、またメールアドレスは正規ユーザーに不正注文の通知メールを受信させないために行います。これらの事前準備の段階から実際の注文までの一連の動きを複数の不正な操作としてログから捉えます。

監視方法

前述の一連の操作が行われる時間の幅はまちまちですが、本例では攻撃者が一連の操作を短時間実行する傾向にあることを把握したと仮定します。この脅威想定に基づき「同じユーザーIDがメールアドレスおよび登録住所の変更後、1時間以内に商品を注文した場合は不正操作が疑われる」というユースケースを定義します。次に定義したユースケースをルール化するために、必要なログ項目を整理します。ルール検知では「ユーザーID」や「時刻」に加え、どの操作を行ったのかをURLの「パス」で識別します [1]。最後に、図表4のようにそれぞれの変更操作と商品注文のログからユースケースに該当するユーザーID、時刻を突合し、疑わしいイベントを抽出します。

このようにWebアプリケーションログから不正な動きを検知するためには、適切なユースケースの定義と複数ログの相関をチェックする仕組みが必要となります。

*1：パスはURL「https:// website.XXX.co.jp/login」の「/login」に該当します。当該項目は、Webアプリケーションの機能が格納されているサーバー上の場所を指します。不正注文の例ではパスを、メールアドレス変更「/change_email」、登録住所変更「/change_address」、商品注文「/confirm_order」と仮定しています。

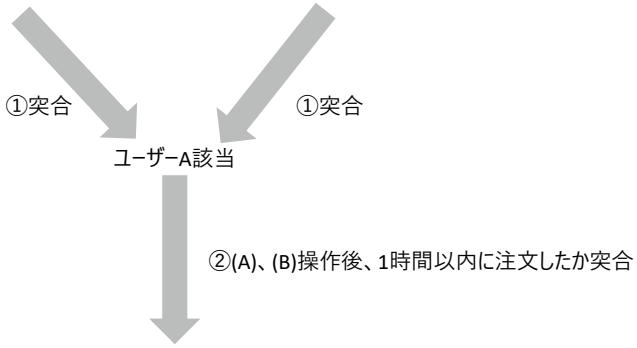
図表4　メールアドレス変更、登録先住所変更、商品注文のユーザーID、時刻リストによる検知例

(A)　メールアドレス変更したユーザーIDのリスト

#	時刻	ユーザーID	パス
1	**2022/08/20 19:26:50**	**UserA**	**/change_email**
2	2022/08/20 19:37:47	UserB	/change_email
3	2022/08/20 20:25:14	UserC	/change_email

(B)　登録住所変更したユーザーIDのリスト

#	時刻	ユーザーID	パス
1	2022/08/19 12:05:23	UserD	/change_address
2	**2022/08/20 19:33:11**	**UserA**	**/change_address**
3	2022/08/20 21:49:53	UserE	/change_address



(C)　商品注文したユーザーIDのリスト

#	時刻	ユーザーID	パス
1	2022/08/19 17:33:11	UserF	/confirm_order
2	2022/08/20 15:30:07	UserG	/confirm_order
3	**2022/08/20 19:48:32**	**UserA**	**/confirm_order**

SIEMによるWebアプリケーションログの監視

Webアプリケーションのログ監視では、操作傾向に基づき不審なイベントを見つけます。リアルタイム監視を行う場合は、イベント抽出(検知)を自動化して通知する機能も必要です。また不正操作を検知するための前提として、Webアプリケーションの仕様も把握する必要があります。さらに、Webアプリケーションごと、攻撃ごとに正常・異常の傾向は異なるため、それぞれの傾向を把握したうえで検知ルールに反映させる必要があります。

これらの課題に対処するために、自作のツールを開発する方法もありますが、実装にはスキルを持つ人員の確保や維持が必要になります。それを解決する手段の一つがSIEMの活用です。SIEMでは、Webアプリケーションのログも含めて様々な種類のログを取り込むことができます。また、イベントのフィルタリング、指定した項目からのルール設定を通じてイベント抽出および、自動化ができます。Webアプリケーションの仕様・傾向もSIEMを通じて把握できます。さらに、製品によっては機械学習による不審な行動を行うユーザーの検知も可能です。

監視例で挙げた不正操作は、例えば不正ログインに対するアカウントロックなど、Webアプリケーション側の機能実装で対処すべきものも多いです。しかし、コストや環境面でアプリの改修が難しい場合は、SIEMが強力な監視ツールとなります。

まとめ

本稿ではセキュリティ機器では検知が難しいWebアプリケーション機能を悪用した不正操作の監視を取り上げました。Webアプリケーションの仕様やログ形式を理解したうえで、通常とは異なる挙動をSIEMでルール化することによりWebアプリケーションに対する不審なアクセスをリアルタイムで検知することができます。また、統計情報から平常時の状態を把握しておくこともセキュリティ対策として重要です。

デロイト CICでも、24時間体制でWebアプリケーションのログを監視していて、日々、不正操作のアクセスに対応しています。本稿がWebアプリケーションログの監視の一助となれば幸いです。

SOAR運用の舞台裏 ~セキュリティ運用のコード化~

はじめに

SOAR（Security Orchestration, Automation, and Response ）という言葉をご存じでしょうか？SOARとは米調査会社Gartner社が提唱した概念[1]で、セキュリティ運用に関わるプロセスを統合して対応を自動化・効率化するソリューションです。現在では様々なSOAR製品が販売されていますが、その活用方法や利用時の注意点といった利用者目線での情報はまだまだ多くはない状況です。

そこで本稿では、実際にSOARを運用しているCICがどのような点に注力、苦悩し、メリットを享受できたのかを紹介します。

CICがSOARを導入した背景

CICでは様々なセキュリティ製品のアラートやサーバー/アプリケーションのログをSIEMに取り込んでルールを設計しています。監視対象の拡大やルールの増加に伴って次のような課題が顕在化していました。

- セキュリティアラートの増加に伴う対応工数増への対処
- 繰り返し発生するアラートの定型処理の効率化
- 部分的には作業を自動化していたものの、インシデント対応の初動から対処までを自動化する仕組みがない

当初は個別に自動化ツールを開発し、それらを組み合わせて対応を行っていました。しかし、現状のオペレーションに沿って統一的に自動化を実現する基盤があることが望ましいと考え、海外のデロイト CICにおけるSOAR活用例をも踏まえて日本のCICでもSOARの導入を検討しました。その際、SOARの機能を理解することはもちろんですが、導入後の効果測定を行うためにも以下のように自動化によって短縮が見込まれる作業やその工数の算出も行いました。

- 1アラートに割いている分析の平均工数の算出
- 自動化によって短縮が可能な作業の洗い出し
- 削減可能なコストとSOARに関わる費用のバランス

これらを考慮した結果、ある程度のコスト削減が見込めたことや、SOARを運用することによるノウハウの蓄積に加えて、アナリストとしての技術的な好奇心が後押ししたこともあり、導入を決定しました。

SOARの特徴とCICの使用状況

SOAR製品を調べると各社の製品紹介ページで次のような単語をよく目にすると思います。

- 自動化
- プレイブック
- オーケストレーション
- インシデント管理

これらはSOARの強みを表現するキーワードとなっていますが、具体的にどのような機能であるかをイメージしにくいと感じる方も多いのではないのでしょうか。ここからは、これらのキーワードを中心にCICでの運用状況を説明していきます。

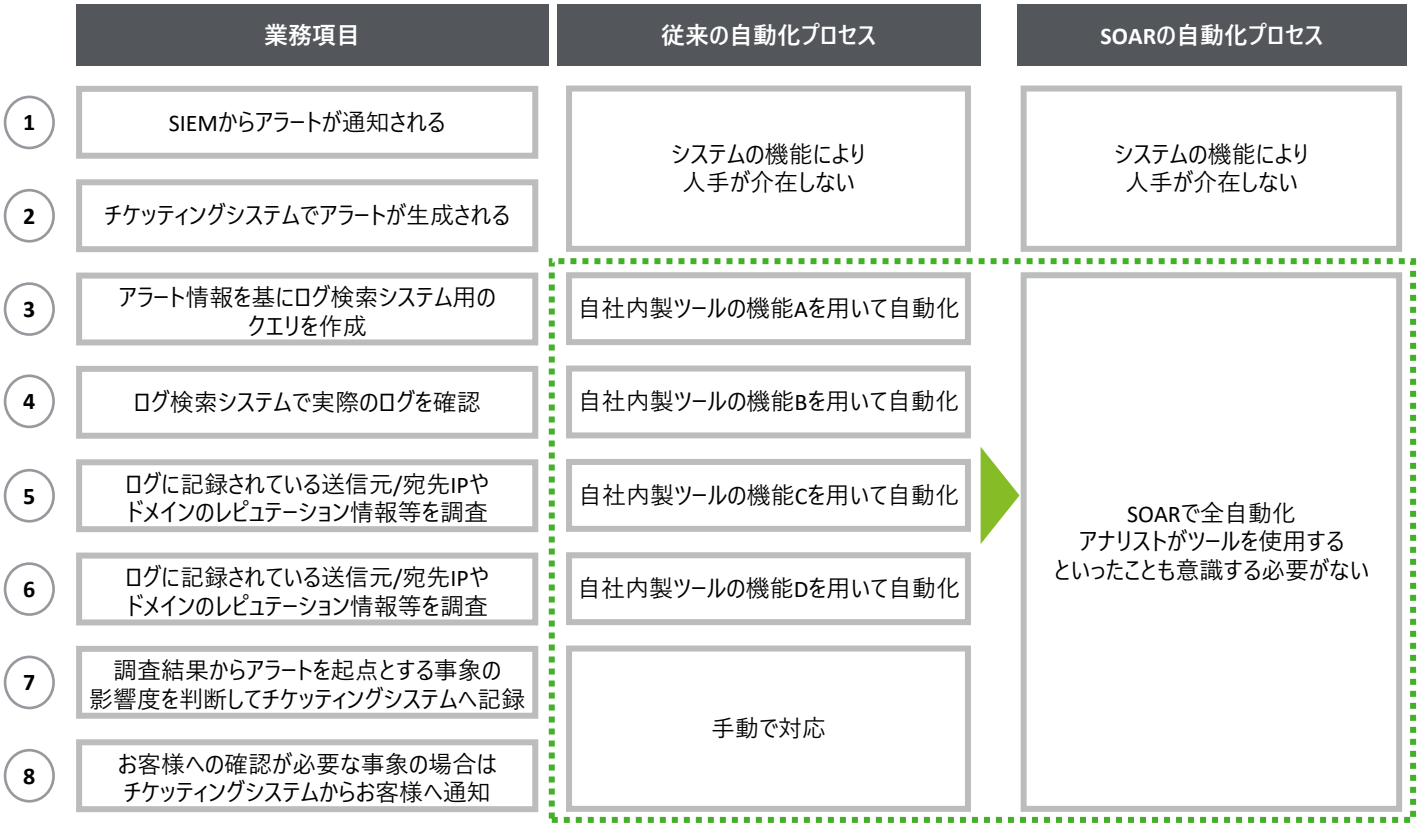
自動化

SOARにおける自動化を端的に表現すると「業務の各作業をコードへ置き換えたもの」と言うことができます。この点においては自作ツールで業務を効率化するのと変わりはありませんが、後述するプレイブックの概念と組み合わせてコードを利用することがSOARにおける特徴的な考え方だと思います。

*1：Reviews for Security Orchestration, Automation and Response Solutions Reviews 2022 | Gartner Peer Insights

CICでもSOARの導入までは内製のツールで作業を自動化していましたが、インシデント対応の始まりから終わりまでのすべてを自動化する仕組みは存在していませんでした。各作業項目とSOAR導入前後の自動化プロセスの比較を図表1に示します。

図表1　アラート分析における作業項目とSOAR導入前後のプロセス



実際のオペレーションでは、アラートの検知からお客様への通知まで複数のステップに分かれています。SOAR導入前もCICでは、手動作業をなるべく減らすために作業ごとに内製の自動化ツールを利用していました。しかし、アラートの増加に伴って、一つ一つのツールを実行する工数すら無視できない負荷となっていたことや、作業によっては手動対応が残らざるを得ない状況が課題となっていました。

しかしSOARはこのような一連の処理を自動化することが可能です。これによって、アナリストは繰り返しツールを実行するといった単純操作から解放されるとともに、より複雑なアラートの分析に工数を割くことが可能になりました。

SOARでは、自動化に必要な汎用的なシステム連携の機能等が公開されているケースもあります。しかし、製品から提供される汎用的な機能のみで既存業務の最適な自動化が実現できないことも考えられます。CICで導入した際も、ノーコードで業務にフィットした自動化を行うことは難しい状況でした。したがって、導入時には業務に合わせた機能の作り込みにそれなりに工数が必要であると考えたほうがよいと思います。

プレイブック

プレイブックという言葉はSOARの核となる考え方だと思います。プレイブックについてはSOAR製品によって説明の細部が異なっていますが、ここでは「業務フローをプログラムレベルのフローへ置き換えたもの」と定義します。そして「業務フローをプログラムレベルのフローへ置き換えること」は、業務を機械的に処理しても影響が出ない状態に標準化することを意味します。この過程で、作業の細分化、あいまいな処理の排除、例外処理の取り扱い方法の決定、などが必要となります。

SOAR導入の初期段階では、業務プロセスの見直しと修正を繰り返して業務を標準化させていく作業が圧倒的な割合を占めます。まさにこのプロセスが重要で、SOARを用いるから業務が標準化されるのではなく、標準化しなければSOARでプレイブックを実装することができないという関係を理解する必要があります。SOARを導入して動作させることが目的ではなく、業務を標準化する運用サイクルを確立することがSOAR有効活用のカギと言えるでしょう。

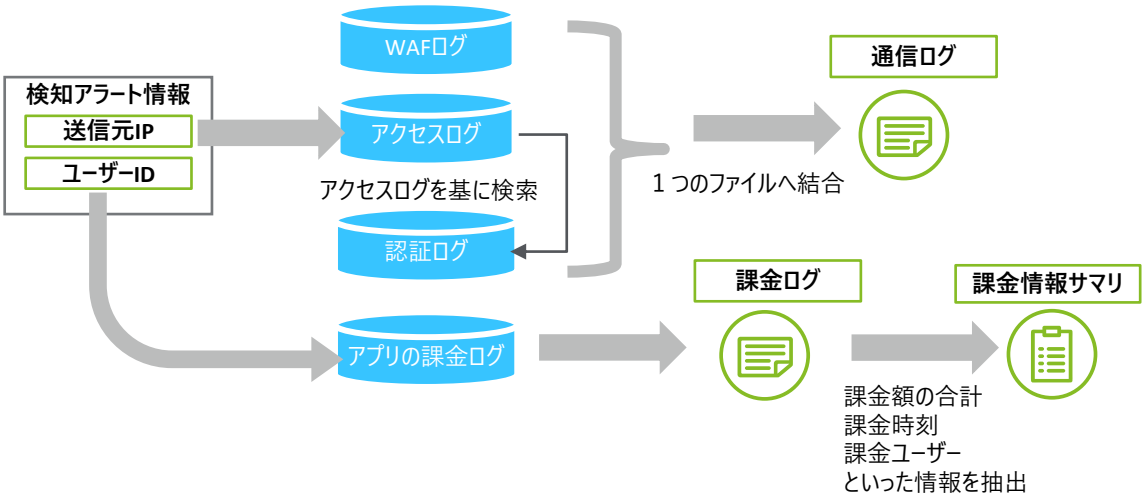
このようにプレイブックは重要な概念ですが、プレイブックを具体的にイメージしていただくためにいくつか事例を用いて説明します。

プレイブック実装例

ここではECサイトにおいて短時間で決済アプリへの高額課金を繰り返す振る舞いを、不正課金の疑いがあるとして検知するアラートの処理をプレイブック化した事例を紹介します。

対応の簡単な流れは、決済アプリへの不正課金が疑われる操作をトリガーとして、複数のログを検索した後に「課金ログ」と「アプリの通信ログ」の2種類のログを出力するものです。この情報を受け取った管理者は、正規ユーザーによる操作かどうかを調査します。

図表2　検知アラート情報から提供する情報を抽出するまでの流れ



図表2で示したように、アラート検知から目的のログを出力するまでに複数の操作が必要となります。これらを自動化することを目的に、さらに手順を分解してそれぞれをプレイブックとして定義していきます。詳細化のイメージは図表3の通りです。

図表3　細分化した対応手順とプレイブックの実装内容

分析手順	対応手順(アナリスト)	プレイブック実装内容(SOAR)	プログラム
ログの検索	アラートの内容から送信元IPを確認	アラートの内容から送信元IPを抽出	コードA
	ログ集約システム上で送信元IPからアクセスログを検索	検索システムで検索するための任意の条件が設定されたクエリ文を入力値として条件に合致したログデータを出力する機能	コードB
	アクセスログをログ集約システム上から出力		
	アクセスログから認証ログを検索	検索システムで検索するための任意の条件が設定されたクエリ文を入力値として条件に合致したログデータを出力する機能	コードB
	認証ログを出力		
	ログ集約システム上で送信元IPからWAFログを検索	検索システムで検索するための任意の条件が設定されたクエリ文を入力値として条件に合致したログデータを出力する機能	コードB
	WAFログを出力		
	アクセスログ/認証ログ/WAFログをエクセルに整形	取得したログデータを提出用のログフォーマットへ変換してファイルに保存する機能	コードC
	ログ集約システム上でアカウント名から課金ログを検索	検索システムで検索するための任意の条件が設定されたクエリ文を入力値として条件に合致したログデータを出力する機能	コードB
	課金ログを出力		
	アクセスログ/認証ログ/WAFログをエクセルに整形	取得したログデータを提出用のログフォーマットへ変換してファイルに保存する機能	コードC
ログの添付	状況説明の証跡として出力したログをWeb上のポータルサイトへアップロード	Web上のポータルサイトへログファイルをアップロードする機能	コードD
レポートの作成+アップロード	ログ上から課金を行ったユーザー/課金金額/課金時刻等の情報を抽出してレポートへ記載	ログデータから課金を行ったユーザー/課金金額/課金時刻等の情報を取得してレポートを生成する機能	コードE
	アラートにおける関連情報や抽出した情報を記載したレポートをポータルサイトへアップロード	Web上のポータルサイトへ生成したレポートをアップロードする機能	コードF
ポータルサイトから通知	ポータルサイトからお客様へレポートの内容を通知	ポータルサイトからお客様へレポートの内容を通知する機能	コードG

注）プレイブック化の説明のため、対応手順は簡略化しています

このようにアナリストの各作業をコード化して自動実行できるようにします。その際、他の手順でも行うような作業については汎用性を持たせてモジュール化しておくことで、別のプレイブックで利用することが可能になります(図表内コードB やコードCに該当する作業)。
それまではいくつもの検索を実行してログを取得したりフォーマット変換をしたりしていましたが、SOARで自動化することによって対応の省力化を実現できました。

作成が容易/困難なプレイブック

様々なプレイブックの作成を検討する中で、プレイブック化しやすい処理と、そうではない処理があります。対応手順が確立しているものや、例外があっても過去の実績からある程度対処が決まってくるものはプレイブック化が容易です。一方、例えばEDRの分析のように強い専門性が求められる処理は、状況に応じた判断の分岐も多く、実装の難易度が高くなります。

図表4　業務の特徴とプレイブック化の難易度

	プレイブック化が容易なアラート	プレイブック化が困難なアラート
アラートの特徴	■ 対応手順が明確化されている ■ ある程度の例外対応が文書化/明文化されている ■ 業務に必要なシステムに連携できるインターフェース(API等)が存在している	■ 対応に大量の条件分岐が必要なアラート ■ 実装しづらい例外処理が存在するアラート ■ 対応に深い専門的な知識が必要なアラート
アラート例	■ 特定のログのみを用いた一定の閾値を超えるイベントをトリガーとするアラート ➢ 主に認証失敗検知等のアラート ➢ 特定のアカウントが不正に利用されているかどうかをCICで収集するログで判断ができず、お客様への確認を必ず行う必要があるもの等	■ EDRの検知を起点とするアラート ➢ アラートの分析にエンドポイントの深い知識が求められる ➢ クラウド上にデータを集約している場合には不定期なデータの同期のタイミングで分析結果が変わってしまうケースが存在する

高難易度のアラートも突き詰めればある程度の自動化は見込めると考えていますが、開発工数がかかることを考慮してCICではプレイブック化しやすいアラートから優先的に対応しています。

また、セキュリティオペレーションの手順や体制が確立されていない場合にはSOARを導入しても省力化/自動化の効果を見込むことが難しいため、注意が必要です。

オーケストレーション

オーケストレーションとは、主に同一プラットフォームでアラート対応における始まりから終わりまでを完結できる、他システムとの連動機能のことを意味します。いずれのSOAR製品においても、コードを自作できる機能が存在しているため、連携したいシステムにAPI等のインターフェースが存在していれば実現可能です。

別システムとの連携が必要なシーンの例

- ログ集約システムからログ取得を行う
- 検知したアラートの特定情報をIoCフィードから検索する
- 処理結果をポータルサイト等へ反映させる（データの更新）

インシデント管理

多くのSOAR製品でアラート情報等を管理する機能が実装されていると思います。CICではチケットシステムでインシデントの管理を行っており、SOAR導入の際にインシデント管理の移行を検討しました。しかし、全てのインシデント対応のプレイブックをSOARで実装するには相当な工数が必要であり、一部の管理のみSOARで行うことはオペレーションが混乱すると考え、インシデント管理のSOARへの移行は見送りました。

現在の業務でインシデント管理の仕組みがない場合はSOARの導入と同時に利用することが効率的だと考えますが、既存の仕組みがある場合は、移行の工数や業務への影響を考えたうえで慎重に検討する必要があると考えます。

SOARを運用して享受できたメリット

最後にSOAR導入がセキュリティ監視・運用にもたらすメリットを5つ挙げます。

1. 対応工数の削減
   本来の目的でもありましたが自動化や定型作業の効率化によって、CICでは大幅な工数削減を実現することができました。約1,200件のアラートを処理する月では、そのうち約20%も自動化による効率化が図れています。今後もプレイブックの実装を進めるにつれて、この割合がさらに上がることが期待できます。
2. オペレーションの統一
   プレイブック化に伴って業務の標準化が一層進んだことにより、分析レポートの作成やログデータの取りまとめなど、お客様に成果物を提供するまでの対応にブレが生じなくなりました。
3. 自動化による作業ミスの減少
   手動での作業が削減できたことで、作業ミスやその心配を大幅に減らすことができました。
4. 業務に必要な知識量の削減
   作業自体を自動化しているプレイブックも作成しているため、経験の浅いアナリストへのレクチャーなど、手順を教える時間が削減でき、教える側も教わる側も負荷の軽減を図ることができました。
5. 品質の向上
   アナリストは詳細なログ分析等より高度なタスクに時間を多く割けるようになり、結果的にサービス品質の向上につながっています。

最後に

本稿は、SOARの運用について具体的な情報があまり公表されておらず、CICが実装の際に苦労した経験から、情報を発信しようと考えたのがきっかけとなりご紹介しました。私たちのSOAR活用の取り組みはまだ道半ばであり、現在も様々な課題に取り組んでいます。

本レポートをきっかけに、セキュリティオペレーションの負荷軽減が実現し、アナリストが本来の専門性を活かしてセキュリティインシデントの対応により注力できるようになることを願っています。

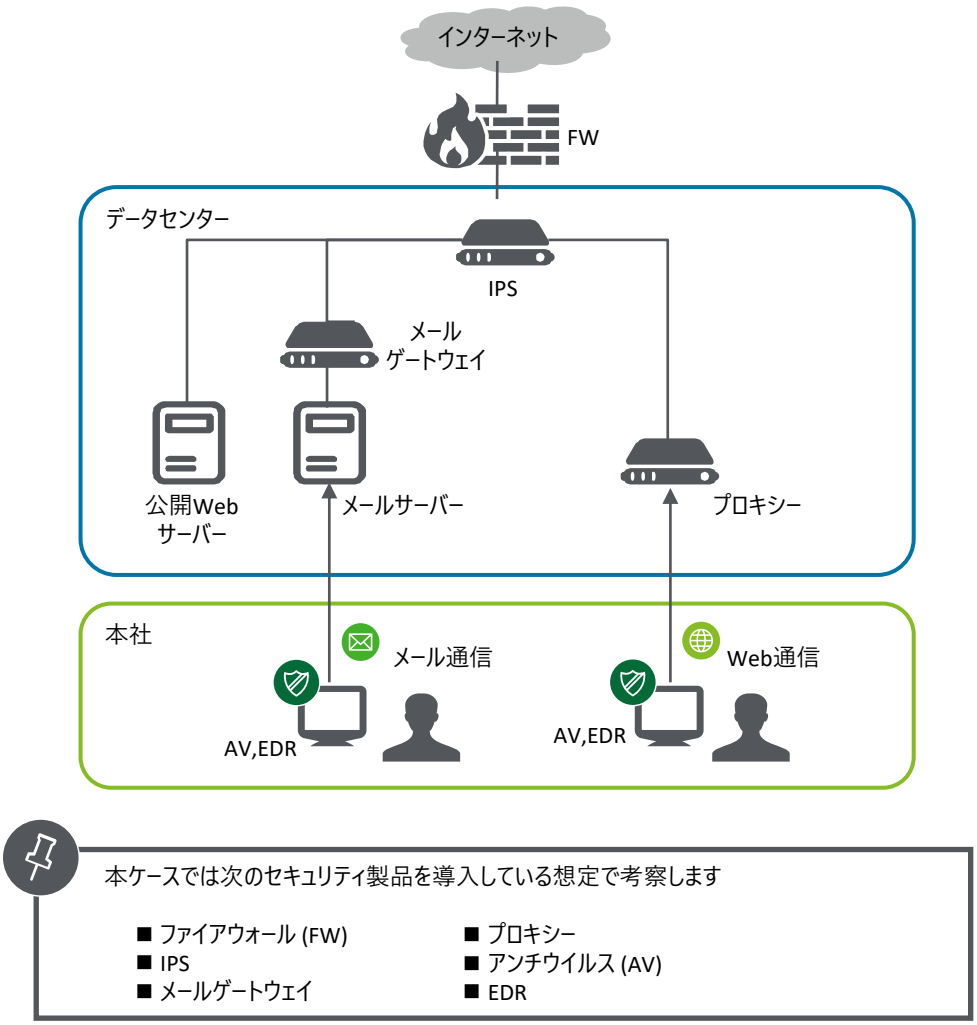
EDRとネットワークログを活用したインシデントの可視化

はじめに

インシデント発生時にやるべきことを組織内で具体的に検討したことはあるでしょうか。インシデント発生時には、被害最小化のための封じ込めや、被害範囲の調査等様々な対応が必要となります。本稿ではこうした対応の「調査」に焦点を当て、EDRのログ等からインシデントの全体像を把握する方法を紹介します。

尚、説明にあたって一般的なセキュリティ対策を行っている企業をモデルとして、バンキングマルウェアとされるEmotetを例に振る舞いやログの分析について考えていきます。

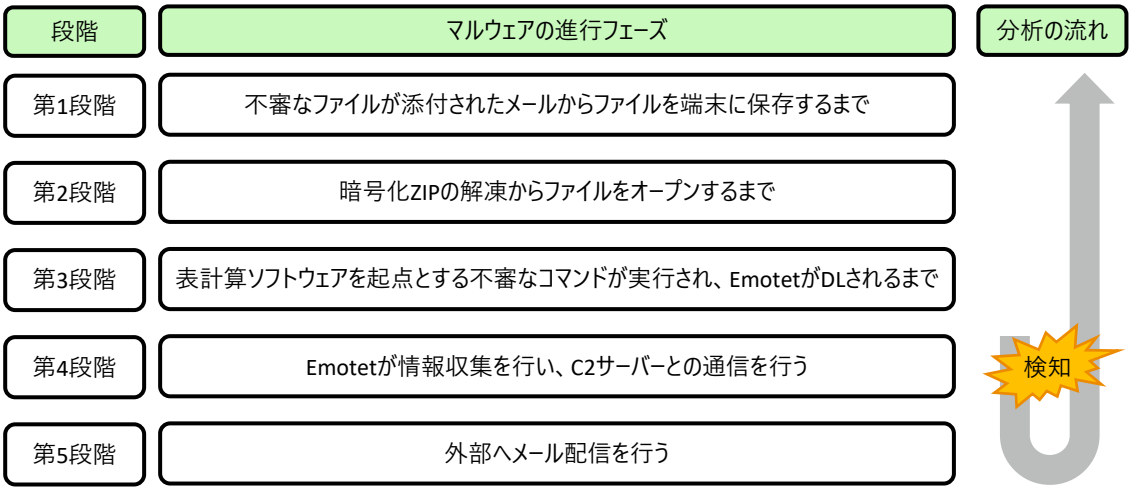
図表1　企業のモデル



Emotetにおけるインシデント事例

本稿ではEmotetの調査において対策として導入している各機器の特性を踏まえて、どの場面でどのように分析を行うのかを見ていきましょう。Emotetの調査は、次の5つのフェーズに分けることができます。

図表2　マルウェアの進行と調査フェーズ



本ケースではマルウェアの進行フェーズの第4段階で、セキュリティ製品によりEmotetが「検知」されたと想定します。ここで注意すべき点としては、セキュリティ製品がマルウェアの進行フェーズの一番最初の段階で検知するとは限らないということです。むしろ、ある程度マルウェアが進行している最中にアラートを検知し、調査を開始することが多いといえます。

このような状況下で分析を開始する場合、C2サーバーへの通信や外部へのメール配信の有無など進行中の事象の確認や、マルウェアの進行フェーズを遡ることが必要になります。本ケースにおける調査では、第4段階や第5段階の状況を先に確認する流れを取りますが、これは封じ込めを行うためです。現在進行中のマルウェアによる被害をまず食い止め、被害を拡大させないようにすることが最優先事項となります。

その後、第3段階→第2段階→第1段階と段階を遡るように分析を行っていきます。調査の段階では未知のマルウェアである可能性を考慮して、判明している情報から順にマルウェアの痕跡をたどっていくため、マルウェアの進行フェーズを後から遡るように分析していくのです。

本ケースでは複数のセキュリティ製品が導入されていることを想定して進めていますが、分析上の観点から各製品のログの有用性について〇△×で評価したいと思います。

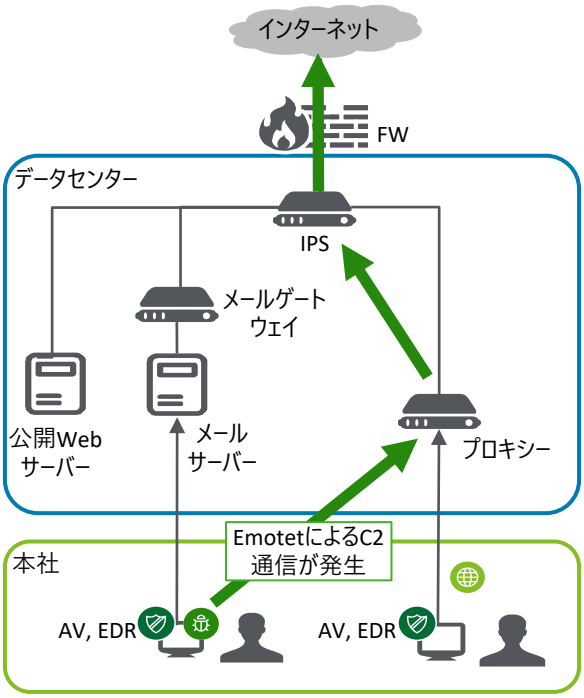
図表3　分析におけるログの有用性評価

評価	意味
〇	調査に活用できる情報が得られる
△	他の機器のログと相関すれば調査に活用できる情報が得られる
×	調査に活用できる情報は得られない

1. 【第4段階】Emotetが情報収集を行い、C2サーバーとの通信を行う

まず、セキュリティ製品で検知することが多い第4段階から考えていきます。本段階では、Emotetは端末内に保存されている機微情報の窃取を試みて、窃取した情報をC2サーバーへ送信します。この手法はEDRでルール化されているため、多くのEDR製品で検知することが可能です。

図表4　第4段階フェーズの概要



機器	分析有用性	概要
ファイア ウォール	○	外部へ通信が発生したことを確認 8070/tcpなどを宛先ポートとする異常な 通信を遮断
プロキシー	○	C2サーバーの一覧を確認
IPS/IDS	○	環境内で感染拡大を狙うような攻撃 行為が発生していないかを確認
メール ゲートウェイ	×	メールではないので対象外
アンチウイルス	×	アンチウイルスが対応しておらず検知すら されない可能性が高い
EDR	○	Emotetマルウェアの振る舞いベースで検知 Emotetマルウェアの振る舞いを確認

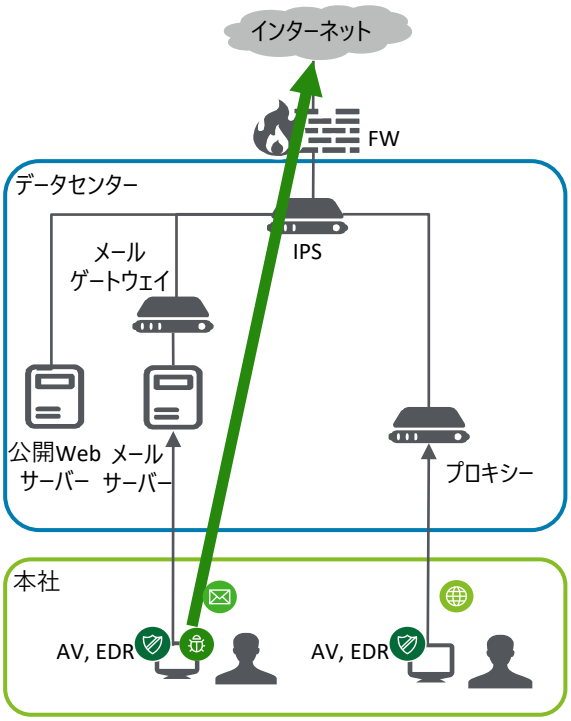
Emotetが外部へ情報を送信する際には、HTTP、HTTPS通信でデータを送信します。したがって、ファイアウォールやプロキシーのログ分析を行うことで、どこにデータを送信したのか、どの程度の量の通信が発生したのかを確認できます。また、どのようなファイルにアクセスを行ったのかなど、窃取された可能性のあるデータについてもEDRのログから確認可能です。

IPS/IDSのログをベースとする分析も有用です。Emotetに感染するまでの通信は暗号化されているケースが多く、IDS/IPSで検知ができる見込みは低いですが、感染後の横展開の挙動を検知できる可能性があります。その痕跡を用いて他端末への侵害状況を把握することが可能になります。

2. 【第5段階】外部へメール配信を行う

マルウェアの進行フェーズの次の段階である第5段階では、Emotetに感染した端末はボットとして外部へのメール送信を試みます。

図表5　第5段階フェーズの概要



機器	分析有用性	概要
ファイア ウォール	○	外部メールサーバーへの25/tcp通信を確認
プロキシー	×	HTTP通信ではないので対象外
IPS/IDS	×	メール通信を検査するものの、攻撃行為そのものではないため検知はしない
メール ゲートウェイ	×	端末から直接メールが配信されるため対象外
アンチウイルス	×	本フェーズまで進行している場合、アンチウイルスが対応しておらず検知すらされない
EDR	○	Emotetマルウェアのプロセスから通信が発生したことを確認

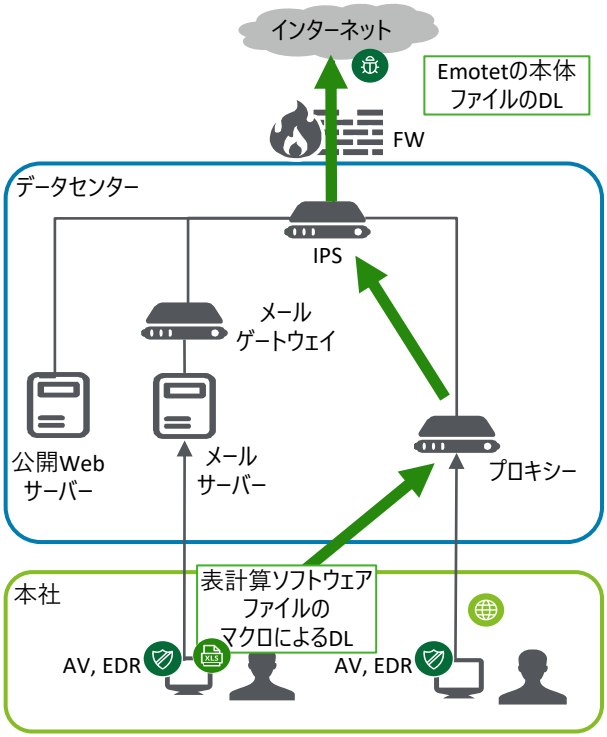
外部にメールが送信されるという大きな被害を食い止めるべく、どのような宛先に通信が発生しているのかなどを中心に分析を行います。同時に、環境内の境界に設定しているファイアウォールではtcp/25の通信やSMTPのサブミッションポートであるtcp/587が多く記録されていることを確認できます。EDRでは宛先ドメイン情報も記録されていることから、ファイアウォールのログとEDRのログを突合して最終的な通信先を特定します。

実際にCICでは、小規模拠点やリモートワークなど通信制御が緩い環境でEmotetに感染した端末が外部へメールを送信した事例を観測したことがあります。このような環境では社内のメールサーバーやメールゲートウェイを経由せず、宛先のメールサーバーへ直接送信されることがあります。その場合、そもそもメールゲートウェイを経由しないため、端末から送信されるメールを識別して不審なメールが送付されないようにすることは難しいと言えます。

3. 【第3段階】表計算ソフトウェアを起点とする不審なコマンドが実行され、Emotetがダウンロードされるまで

引き続きマルウェアの進行フェーズを遡って調査を継続します。第3段階では表計算ソフトウェアのマクロ機能を悪用し、Emotetの本体である実行ファイルをダウンロードします。

図表6　第3段階フェーズの概要



機器	分析有用性	概要
ファイア ウォール	○	外部へ通信が発生したことを確認
プロキシー	○	Emotet本体のダウンロード元URLの確認
IPS/IDS	×	対応するシグネチャがないことやHTTPS通信であれば検査ができない
メール ゲートウェイ	×	メールではないので対象外
アンチウイルス	△	Emotetの本体ファイルを検知する場合もあるが多くのケースでは検知しない
EDR	○	不審なコマンドが実行されたということで検知される。コマンドの引数などの詳細な振る舞いを記録

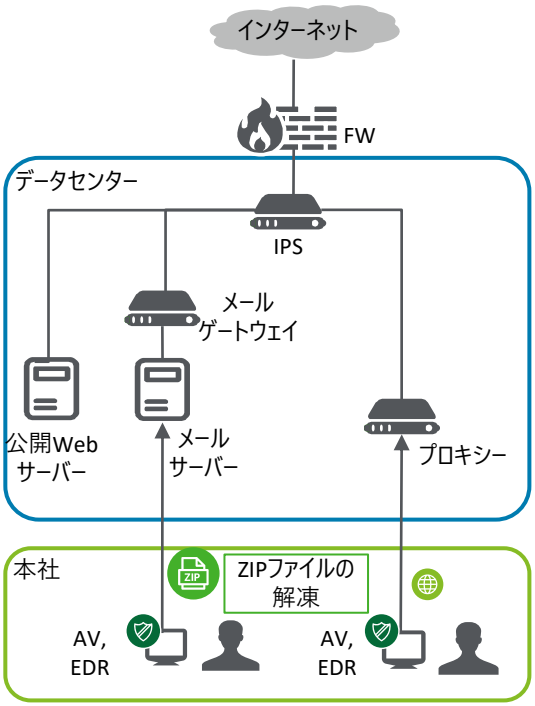
この段階の調査はEmotetが侵入してきた経緯を確認することを目的としています。まさに、インシデントの全体像を把握するために一つ一つ証拠を集めていくイメージです。

表計算ソフトウェアファイルが開かれることにより攻撃者によって組み込まれているマクロが実行されます。このマクロは外部からEmotet本体である不審なDLLファイルをダウンロードするように細工されています。HTTP通信を利用してEmotet本体をダウンロードするためプロキシーログに通信ログが記録されます。このログを確認することで、通信量や宛先URLから本体のファイルサイズやEmotetの配布先を特定することができます。これらの情報はEDRで確認できることもありますが、状況によってログに残らない場合もあり、事象の見逃しを防ぐために複数の種類のログを確認する必要があります。

4：【第2段階】暗号化ZIPの解凍からファイルをオープンするまで

さらに遡り、ユーザー自身が暗号化ZIPを解凍し、表計算ソフトウェアファイルを開く挙動を調査します。

図表7　第2段階フェーズの概要



機器	分析有用性	概要
ファイアウォール	×	端末でのみ確認可能
プロキシー	×	端末でのみ確認可能
IPS/IDS	×	端末でのみ確認可能
メール ゲートウェイ	×	端末でのみ確認可能
アンチウイルス	△	表計算ソフトウェアのマクロを対象として検知する場合もあるが多くのケースでは検知しない
EDR	○	検知はしないものの、アーカイブソフトにより展開され、表計算ソフトウェアが開かれた部分を確認可能

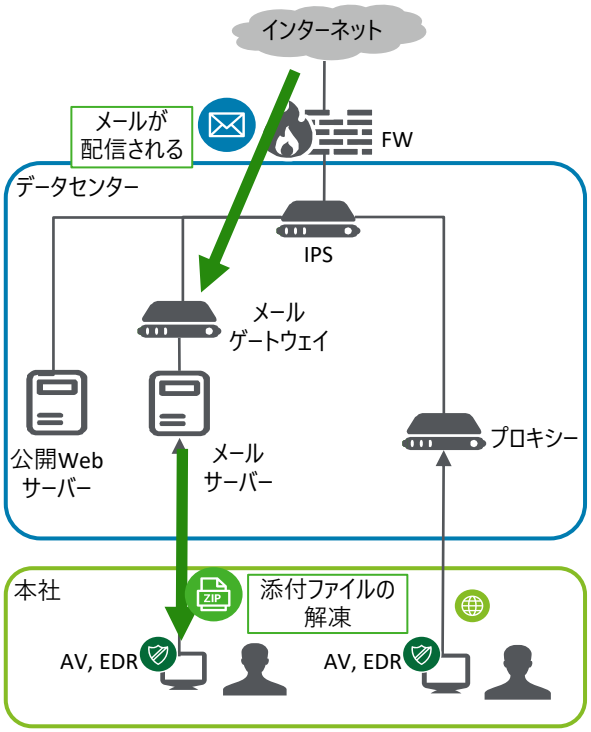
このフェーズでは基本的には通信が発生しないためネットワークログでの分析はできません。また、多くのケースでアンチウイルスによる検疫が行われないため、EDRを中心に分析を行うこととなります。EDRのログから、ユーザー自身がZIPファイルを解凍し、表計算ソフトウェアを開く振る舞いを確認することができます。

尚、ログに記録された時間も分析上のヒントになります。ユーザーの操作により発生したログであれば、記録される時間にばらつきが生じることがあります。これはユーザーがマウスやキーボードでPCを操作していることなどが原因と考えられます。このようにログに記録された時間と操作との関係を注意深く分析することで、人による操作なのか、マルウェアによる機械的な動作なのかを推測することも可能です。

5：【第1段階】不審ファイルを含むメールのばらまきからユーザーが添付ファイルを保存するまで

最後に、マルウェアの感染フェーズの第1段階まで遡り、分析の観点からわかることを考えます。Emotetが不審なファイルを含むメールをユーザーに対して送信し、ユーザーがそのファイルを端末内に保存するのがこの第1段階です。

図表8　第1段階フェーズの概要



機器	分析有用性	概要
ファイアウォール	○	外部のメールサーバーから環境内のメールサーバーまで通信が発生していることを確認
プロキシー	×	HTTP通信ではないため対象外
IPS/IDS	△	メール通信を検査するものの、攻撃行為そのものではないため検知はしない
メールゲートウェイ	○	メールの到着時刻、件名、送信元などメールに関する一通りの情報を確認
アンチウイルス	×	暗号化ZIPのまま検査を行うが、もちろんマルウェアではないため検知されない
EDR	○	マルウェアが動作していないため検知はされない。ただし、メールを開いた、暗号化ZIPを保存したなどのログは記録

外部から不審なファイルが添付されたメールが送信され、表計算ソフトウェアファイルがそのまま添付されていればメールゲートウェイでメールの破棄が行われます。ただし、パスワードで暗号化されたZIPファイルについては検査を行うことができず、ユーザーまでメールが届いてしまいます。そのようなメールはメールサーバーからも確認可能だとは思いますが、メールゲートウェイではメールの内容以上に脅威情報などの付加情報を確認できる場合もあるので、メールの内容を詳細に確認します。

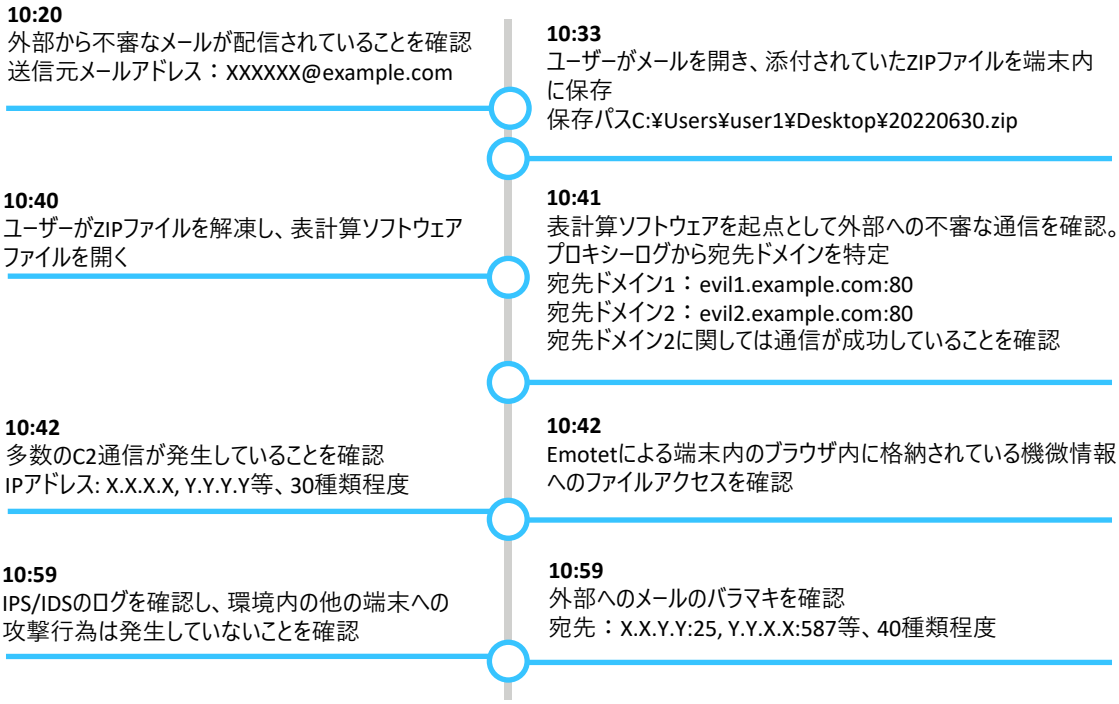
また、EDRのログからユーザーがいつメーラーを立ち上げたのか、いつ添付ファイルを保存したのかとうの詳細な情報を丁寧に確認していきます。このような情報は、後述するインシデントタイムラインの作成時に大きく役立ちます。

Emotet感染インシデント発生後の対応

インシデントタイムラインの作成

ここまで行ってきた分析結果を時系列でつなげてインシデントのタイムラインを図表9に整理します。これにより作業を行うことで「いつ、どこで、何が発生したのか」が明らかになります。様々なログを基に作成したタイムラインでインシデントを俯瞰し、対応漏れがないのか、本当にこの環境は安全になったのかなど検討を重ねることが重要です。また、このインデントタイムラインは事後対応やインシデントの振り返り時の資料としても役立ちます。

図表9　インシデントのタイムライン



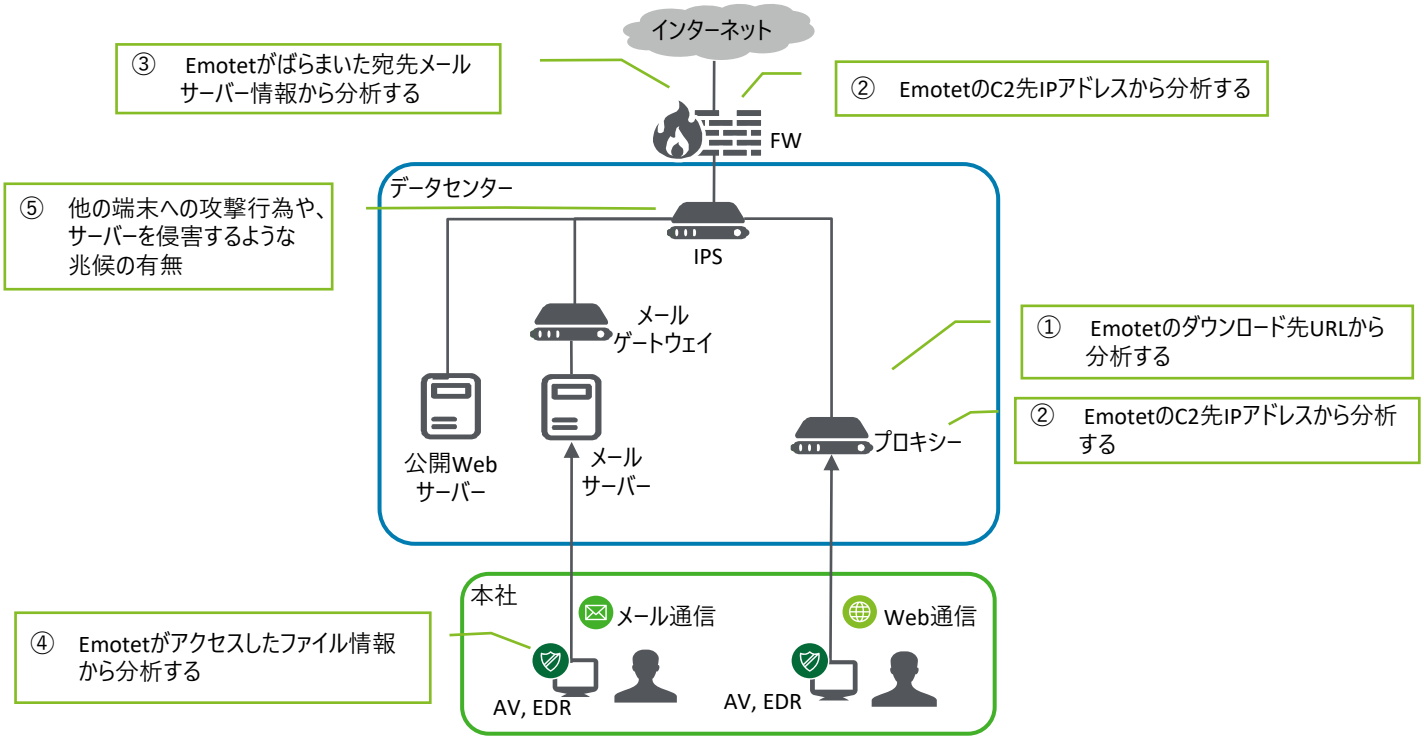
インシデントタイムラインを用いた対応

インシデントタイムラインを用いて、インシデントが発生した後の対応について検討します。マルウェア感染があった端末以外に、被害を受けた端末の有無を確認するべく、環境内で検索が可能な情報を考えます。次の5つの項目は前述のケースで取得が完了している情報です。

① Emotetのダウンロード先URL情報
② EmotetのC2通信先情報
③ Emotetがばらまいた宛先メールサーバー情報
④ Emotetがアクセスしたファイル情報
⑤ 他の端末への攻撃行為や、サーバーを侵害するような兆候

これらの情報をもとに環境内すべてを調査することで、同一マルウェアによる影響の有無を確認します。

図表10　インシデント発生後に取得した情報



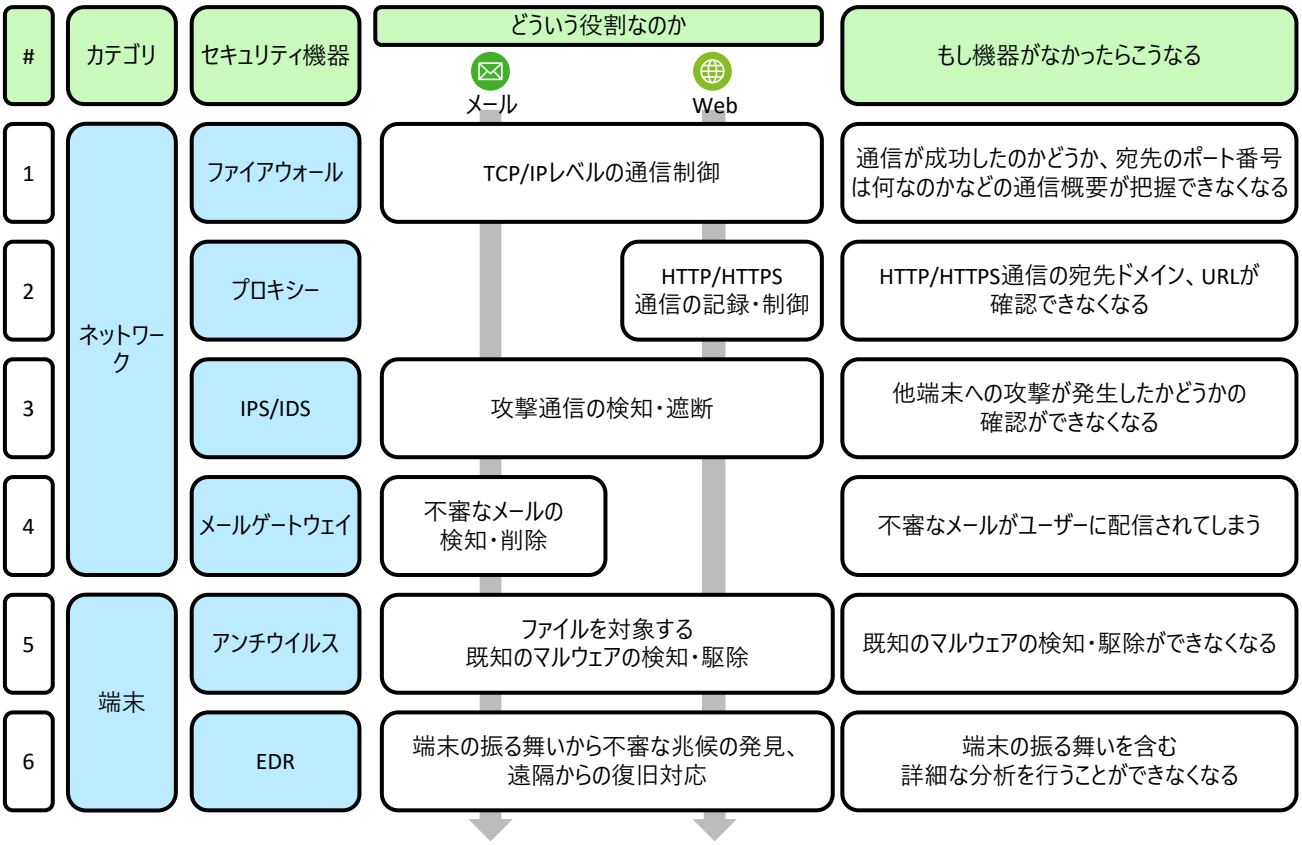
図表10に示した通り、Emotetが端末内部で行った振る舞いなどをベースとして、環境内のすべてのログを検索します。この作業では、セキュリティ製品のそれぞれに対して何かしらの分析を行う必要があります。また、セキュリティ製品に悪意ある振る舞いのすべてが記録されるわけではないため、プロキシーやファイアウォールなど通信を記録する製品やEDRなどの端末の振る舞いを検索できる製品から、環境内のすべての端末を対象として検索することも重要です。その検索結果をもとにインシデントの影響範囲の特定を行うことも可能です。

ただし、検索を行うためにはそのログを保管しておき、検索ができるような仕組みを構築している必要があります。この検索ができる仕組みもインシデントの全体像を把握ために重要なポイントとなるため押さえておきましょう。

Emotet感染インシデント発生後の対応

最後に、ここまでの内容を踏まえてセキュリティ機器・製品の役割を図表11に整理します。

図表11　セキュリティ機器の役割



このように俯瞰してみると、セキュリティ機器・製品によって、その役割や目的が異なっていることが分かります。最近では「EDRを入れたのでセキュリティ対策は万全」といったセキュリティ担当者の話を耳にすることがありますが、EDRはすべての役割を網羅しているわけではありません。インシデントの全体像の把握や、環境内の対処が本当に終わったのかなど、各機器・製品の役割を踏まえた網羅的な調査によって分析漏れを発生させないことが重要です。

最後に

ここまでEmotetを例としてインシデントが発生した際にどのような観点で調査分析を進めていくかをご紹介しました。脅威の変化に合わせて新しいセキュリティ製品が登場し、可視化が進むことで得られる情報量も増えています。大事なことは、セキュリティ製品それぞれの特性を理解し、分析によってログに記録された「点」の情報を「線」としてつなげることでインシデントの全体像を正確に把握することです。本稿でご紹介したアプローチがインシデントレスポンスの一助となれば幸いです。

おわりに

米調査会社Gartner社が発表した2022年のセキュリティとリスク管理の7大トレンドの一つが「攻撃対象範囲の拡大」でした。クラウド利用の進展やサプライチェーンの高度化によって、対処の難しい領域までサイバー攻撃の対象が拡大しているとされ、より広範囲にわたるリスク管理が推奨されています。本レポートでもその対応としてAttack Surface Management（ASM）をご紹介しました。

一方、「監視・検知・対応」に目を向けると、監視対象が拡大することによってセキュリティ担当者の負荷は高まっていると言えます。EDRのようにエンドポイント（端末）を直接監視して分析することが当たり前となり、それに伴って関連ログを調査する必要性も高まっています。この流れは近年提唱されているXDR（Extended Detection and Response）のソリューションによってさらに進むことが想定されます。また、アラートの誤検知抑止や、しきい値監視における過剰検知のチューニングなど、運用に関わる対応も依然として必要となります。

本レポートでご紹介したSOARは、セキュリティ担当者の負荷を軽減して本当に必要なアラートの分析に注力するための一つの解決策となると考えます。その際重要となるポイントは、単に自動化を目指すだけでなく、SOAR導入の前段階で検知・分析に関わる作業をプログラムできる状態に整理する点にあると考えます。

今後も本レポートでは、ASMやSOARのような新しいソリューションについても取り上げていきます。CICにおける実績や効果的な運用方法に関する情報がみなさまのセキュリティ対策の参考になれば幸いです。

本レポート執筆者

佐藤 功陛	パートナー
鳥谷部 彰則	マネージングディレクター
吉村 修	マネジャー
日平 祐介	**シニア**コンサルタント
大内 和樹	コンサルタント
水越 尚平	コンサルタント

Deloitte.
デロイト トーマツ

デロイト トーマツ サイバー合同会社
Cyber Intelligence Center (CIC)
Mail　ra_info@tohmatsu.co.jp
URL　www.deloitte.com/jp/dtcy
【国内ネットワーク】　東京・名古屋・福岡