Deloitte.
デロイト トーマツ

Deloitte Cyber Trends & Intelligence Report

2021

Nov 2021

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

はじめに

COVID-19の流行が収まる気配が見えない中、2020年度の前半は米国の石油パイプライン運営企業の操業が一時停止し、日本国内の企業では決算報告が延期になるなど二重恐喝ランサムウェアによる大規模インシデントが発生してサイバーリスクの高まりを強く感じています。

本レポートの冒頭では二重恐喝ランサムウェアの地域別・業種別の被害状況の分析結果をお伝えし、二重恐喝ランサムウェア対策として非常に有効なEDR (Endpoint Detect and Response)製品を用いた分析方法について解説します。

また、二重恐喝ランサムウェアの侵入にも使われる脆弱性の早期情報収集の重要性について事例を取り上げて説明いたします。その他にインターネットに公開されているWebシステム向けの侵入防御レイヤーという考え方のご紹介や、Deloitteの海外監視センターをコラムで取り上げています。
冒頭にお伝えする二重恐喝ランサムウェアの傾向分析結果と実際に発生したインシデントの時系列を重ね合わせることによって、日本国内で発生した二重恐喝ランサムウェアインシデントの被害の予測がある程度できたのではないかと思います。

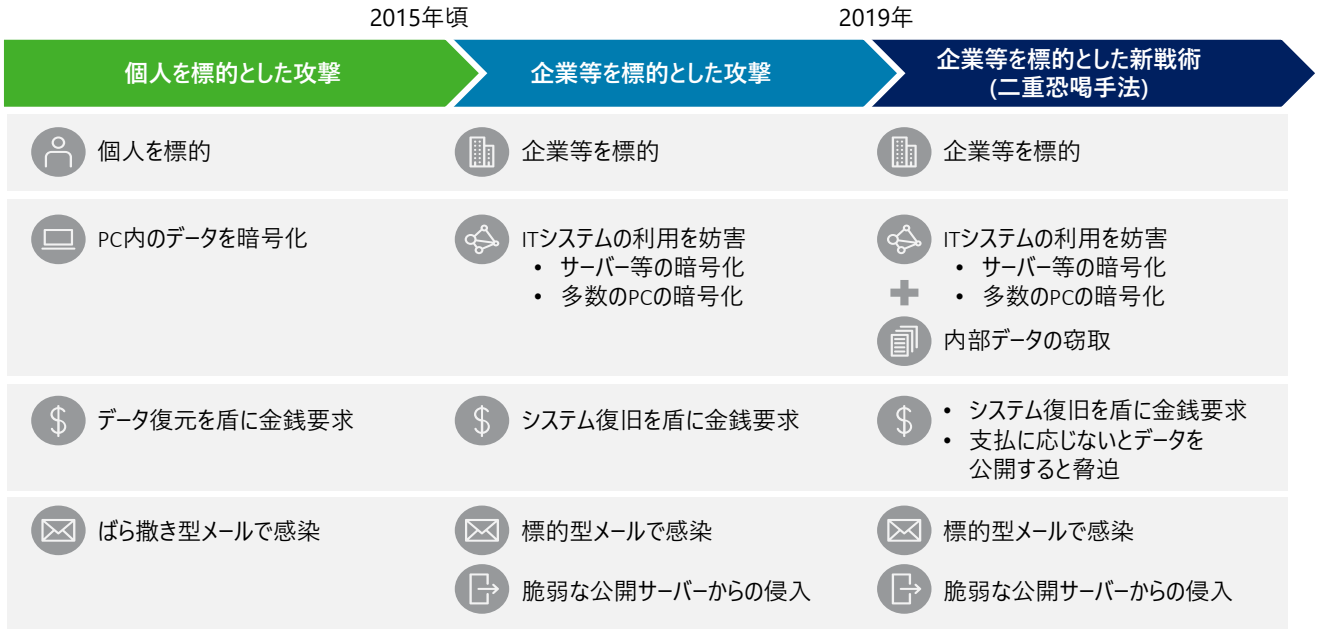
本レポートを各組織における脅威情報のインプットとしてご活用いただければ幸いです。

二重恐喝ランサムウェアの動向

ランサムウェアはPC等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を標的とする傾向がありましたが、2015年頃から企業・団体等を狙ってITシステムそのものを麻痺させ、業務継続を盾に脅迫するケースも出ています。

2019年後半以降は新たに「二重恐喝(Double Extortion)」と呼ばれる手法が流行し、被害が急速に拡大しています。また2021年5月には米国の石油パイプライン運営企業がランサムウェアDarksideによるサイバー攻撃を受けたことで操業が停止する事態が発生し、市民生活にも大きな影響が出ました。このように、ランサムウェアはもはや個々の企業ではなく、社会全体にとっての脅威になっているといえます。

図表1　ランサムウェア攻撃のトレンドの変化

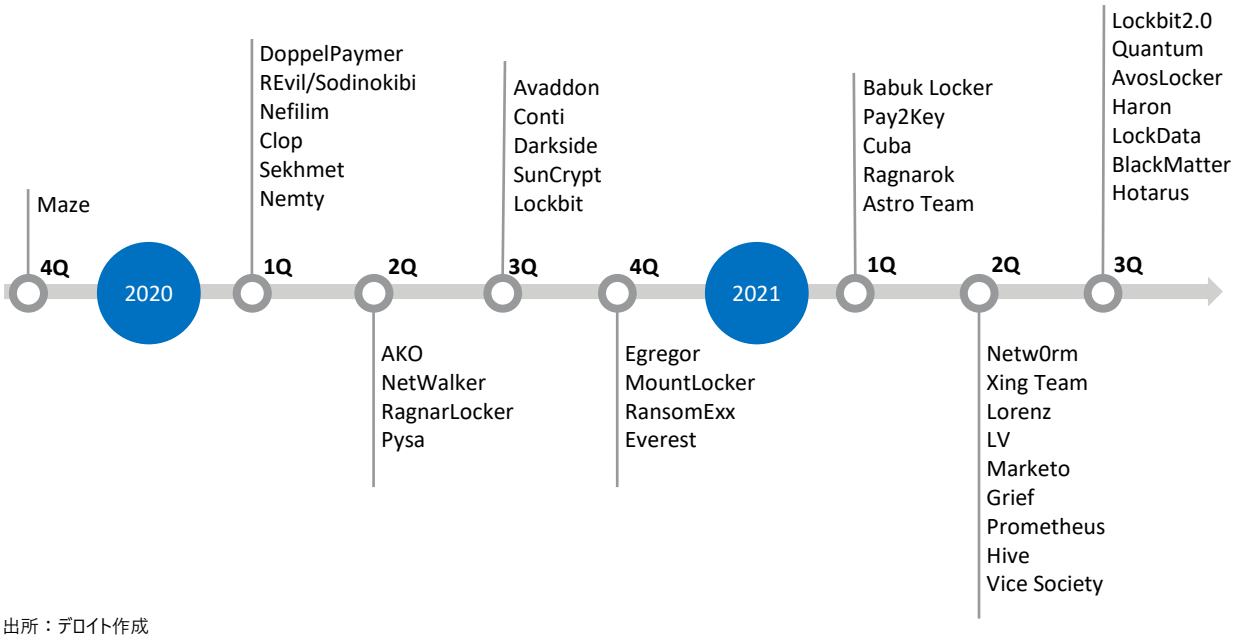


出所：デロイト作成

二重恐喝ランサムウェアとは

二重恐喝ランサムウェアの攻撃者は、データを暗号化するだけでなく事前に盗み出し、支払いに応じなければデータを公開すると脅すことが特徴です。従来の「データ復旧を盾にした恐喝」に加え、「データ公開を盾にした恐喝」を行うことから「二重恐喝」と呼ばれます。二重恐喝ランサムウェア攻撃を受け、支払いに応じなかった企業のデータは、攻撃者によってダークWeb上に開設された「リークサイト」で徐々に公開されていきます。リークサイトの開設は活発に行われており、セキュリティ監視を行っているDeloitteでは通算で約40個のリークサイトを確認しています(図表2)。

図表2　二重恐喝ランサムウェアリークサイトの開設時期

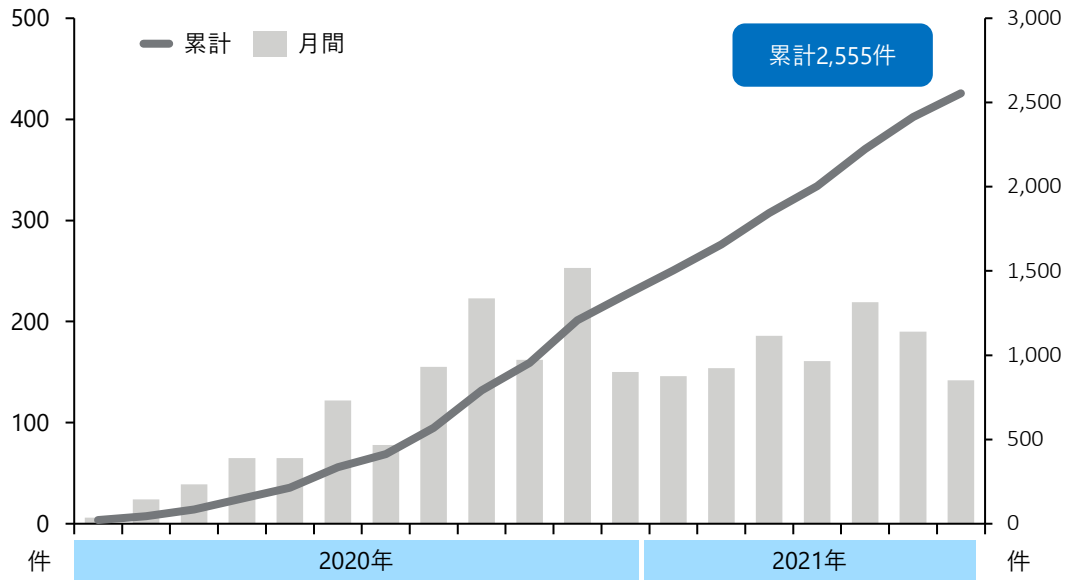


出所：デロイト作成

二重恐喝ランサムウェアによるデータ公開被害の状況

ランサムウェアのリークサイト上で公開された企業等の件数推移は、図表3の通りです。累計件数は2021年7月末時点で2,500件を超えており、月ごとでは2020年8月以降、大半が150件以上と、攻撃活動が1年にわたり活発であることを示しています。

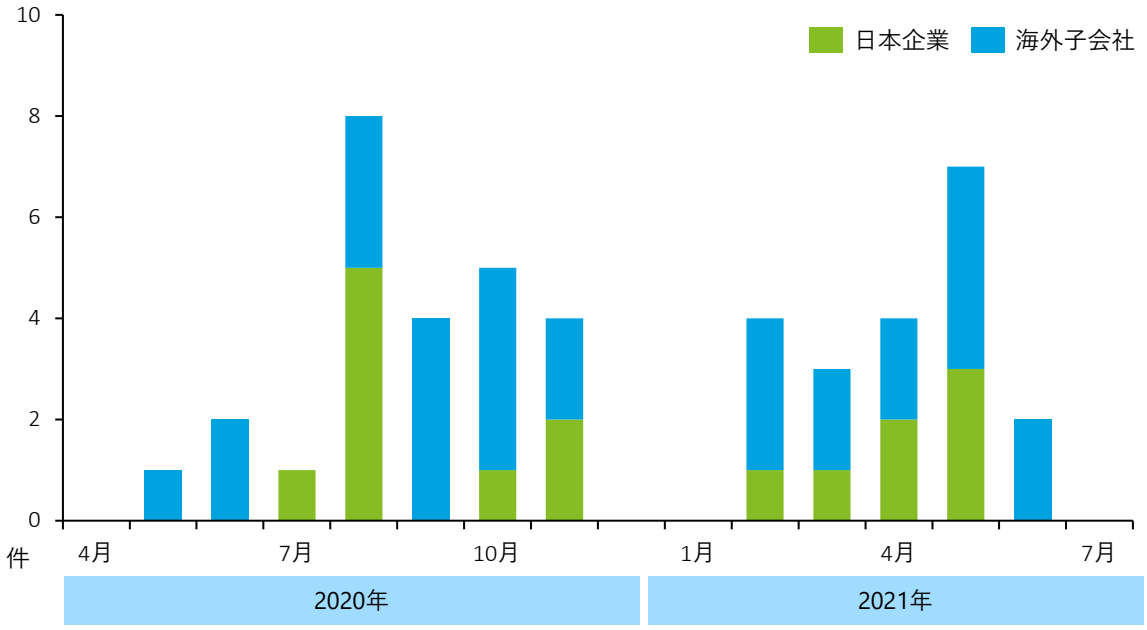
図表3　ランサムウェアのリークサイトで公開された企業等の件数推移



出所：デロイト作成

日本企業とその海外子会社のデータ公開被害状況を図表4に示します。件数としては少ないながらも、2020年5月以降は毎月のように被害が生じています。日本企業にとってもランサムウェア攻撃が決して対岸の火事ではないことを示すものといえます。

図表4　海外子会社を含む日本企業のデータ公開被害状況



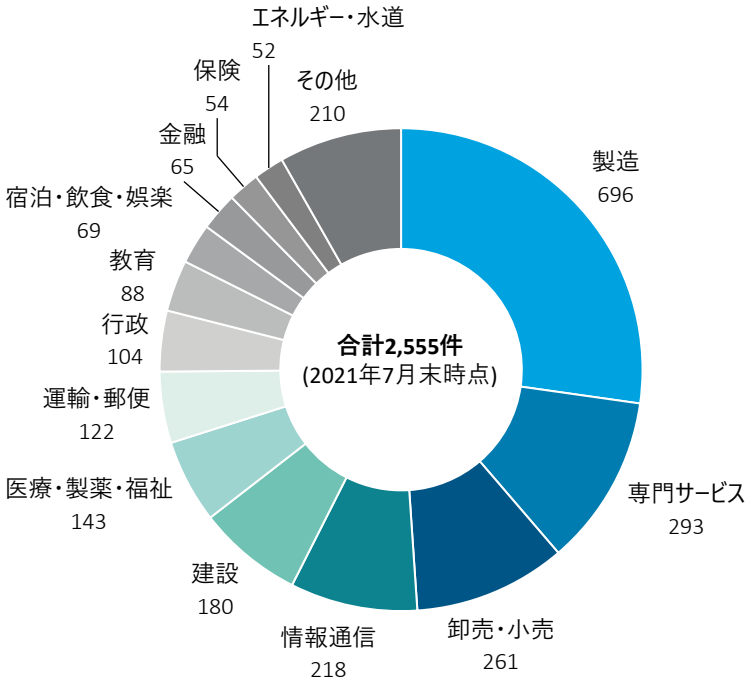
出所：デロイト作成

リークサイト掲載企業から見る被害の傾向

リークサイトに掲載された企業件数を図表5に示します。業種別の中では製造業が最も多いですが、これは製造業が特に狙われているというよりは、他業種に比べて企業数が多いことや中小規模の企業はセキュリティレベルが低い傾向にあるといったことに起因するものと考えます。

昨今のランサムウェア攻撃では、VPN機器等のリモート接続システムが主要な侵入手段となっています。攻撃者側は、インターネット上でリモート接続システムを探索し、脆弱なものに対して攻撃を行っていると考えられます。このため、外部に対して侵入する隙を見せないようセキュリティレベルを維持し続けることがこれまで以上に重要となります。

図表5　リークサイトに掲載された業種別企業件数

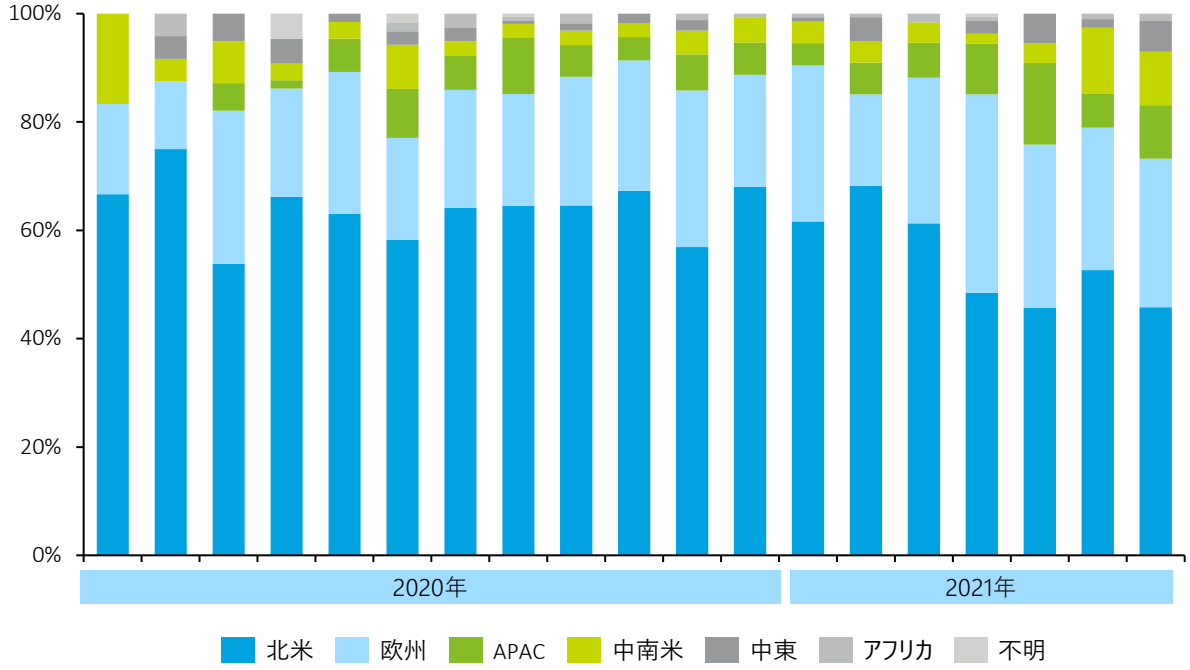


出所：デロイト作成

また、月ごとの地域別の被害件数の割合を図表6に示します。北米が被害の大半を占める傾向は続いていますが、2021年に入ってからは件数、割合共に減少しており、欧州やAPACでの被害も増加しています。北米での被害減少が政治的背景によるもので、ランサムウェアが米国企業への攻撃を避けるようになったのか、侵入が容易で身代金の支払いが期待できる組織が減少したためかは不明です。

ランサムウェア攻撃は業務継続の可否を人質にとるというシンプルな手法であり、国・業種を問わないことから、攻撃者にとってより魅力的な「マーケット」があれば標的はシフトしていくといえます。

図表6　リークサイトに掲載されたデータの地域別割合



出所：デロイト作成

政治動向　～ランサムウェアの脅威は止まるか～

2021年5月に発生した米国の石油パイプライン運営企業への攻撃等、サイバー攻撃が社会に与えるダメージは深刻化し、それに伴いランサムウェアは政治的問題に発展しています。2021年6月の主要7カ国首脳会議(G7サミット)では、すべての国家に対して自国内のランサムウェア犯罪ネットワークを破壊するよう求める公式声明が出されました。[*1]

こうした政治的な動向を受け、アンダーグラウンドの一部では牽制効果が見られます。ランサムウェア攻撃のパートナー探しに使われていた有名なロシア語フォーラムでは、ランサムウェアの話題が禁止され、リークサイトを閉鎖したランサムウェアもいくつか出ています。

ただしこれらはあくまで一部であり、こうした動きがランサムウェア全体に広がっているわけではありません。G7サミットでの声明公表後も新たなリークサイトの開設は相次いでおり、ランサムウェア攻撃が収束に向かう動きは今のところ見られません。

まとめ

ランサムウェア攻撃は標的を選びません。これは、人質にとるのが「業務継続」そのものであるためです。ITシステムがダウンして困るのであれば攻撃対象は誰でもいいということを意味しており、「先端技術を保有していない」、「大量の個人情報を扱っていない」、「政府から仕事を請け負っていない」といったことは、ランサムウェア攻撃者にとって標的から外す理由にはならないのです。

DXの推進、テレワークの拡大など、社会全体でITへの依存はますます高まっています。しかしそれは同時に、企業のサービス提供基盤や基幹システムといった攻撃者にとっての標的の魅力が増す、ということを意味しています。

「社内PCがすべて起動しなくなった」、「顧客向けサービスのサーバーが停止した」、「自社のデータがリークサイトに掲載された」－ランサムウェア攻撃により、こうした事態は突然起こり得ます。ランサムウェアの被害を予防するためには、外部公開機器の脆弱性対策、内部ネットワークの監視、エンドポイントや重要なデータの保護、バックアップといった基本的な対策を、隙なく続けることが重要です。

*1：G7 Cornwall UK2021, “CARBIS BAY G7 SUMMIT COMMUNIQUÉ”,「Our Shared Agenda for Global Action to Build Back Better」,2021年6月: https://www.g7uk.org/wp-content/uploads/2021/06/Carbis-Bay-G7-Summit-Communique-PDF-430KB-25-pages-5.pdf

クラウドからの情報流出

情報流出の原因は、サイバー攻撃だけではありません。自らの設定ミス等によって誤って情報が公開されてしまうケースも数多く見られます。特に近年ではクラウド上の情報流出が目立っています。

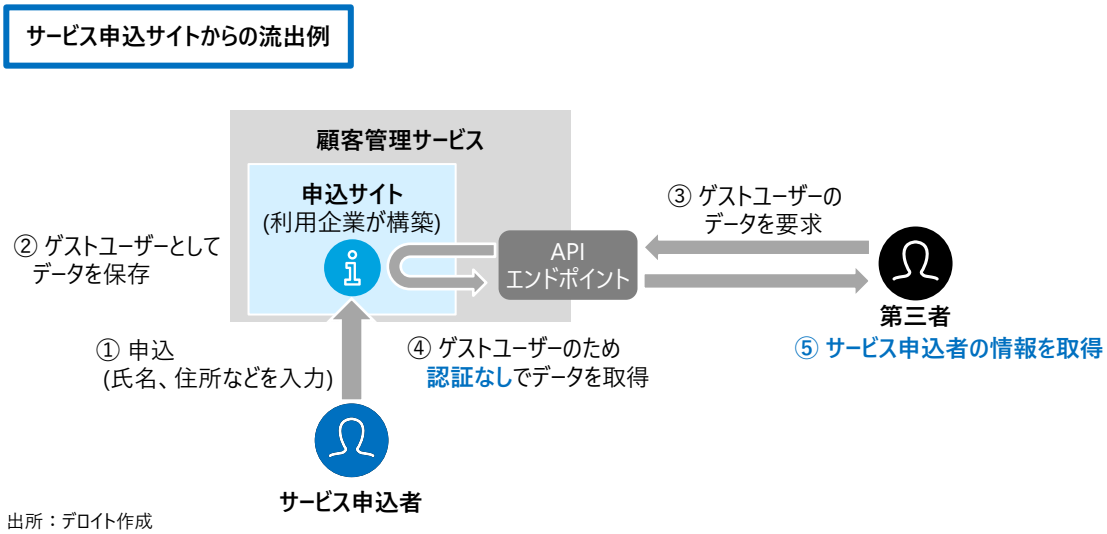
よく見られるパターンは以下のように、クラウドサービス利用者(ユーザー企業)側の設定ミスに起因するものがほとんどです。

- クラウドストレージで情報公開範囲をPublicに設定してしまい、誰でも閲覧できるようになっていた
- ソフトウェアのコード管理サービスで、誰でも閲覧可能な状態でコード開発を行い、認証情報やAPIキーなどが公開されてしまった

国内事例

2020年末以降、顧客管理サービスを利用して構築されたサイトが、外部から情報を閲覧できる状態だったという事案が国内で相次いでいます。この事案の構図は図表1の通りで、利用者側がデータをゲストユーザーとして保存したため、API経由で第三者が閲覧可能だったというものです。

図表1　顧客管理サービスから情報流出した際の構図



出所：デロイト作成

この事案は、クラウドでよく見られるサービス利用者側のデータの権限設定不備が原因のひとつといえますが、利用者側の設定不備がすべての原因とは言い切れません。クラウドサービス事業者側にも、機能のアップデートによってこの問題を顕在化させたという側面があります。

外部からのデータ閲覧はAPI経由で行われていますが、このAPI機能は2016年に追加されたものです。データの権限設定不備だけであれば外部からの閲覧は難しいですが、APIという第三者が容易に利用できる経路が実装されたことで問題が表面化したといえます。

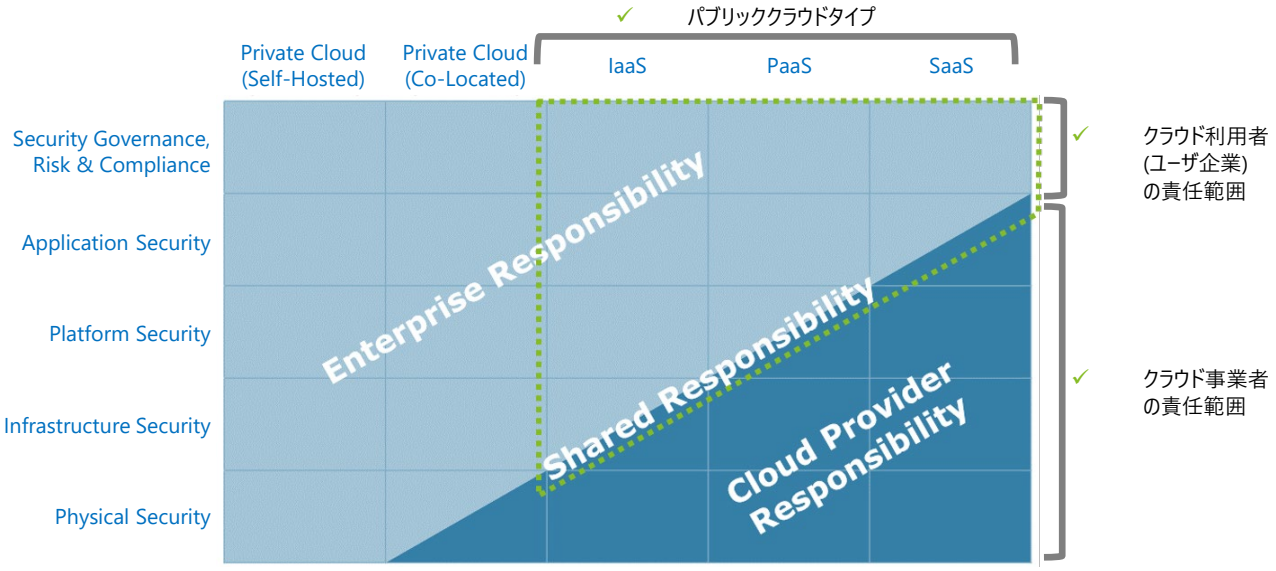
Software as a Service(SaaS)では、ユーザー企業側が開発を行わなくてもサービス側のアップデートを行うことで便利な機能を利用可能になるというメリットがありますが、一方で、アップデートによって今まで隠れていた問題が顕在化してしまうといった事象も起こり得るのです。

クラウドのセキュリティリスクへの対応

このようなクラウドの利用に関連するセキュリティリスクへの対応を検討する際には、クラウドにおける「責任共有モデル」を理解することが重要です。

クラウドでは、クラウドサービス事業者とクラウドサービス利用者の間にセキュリティに関する責任分界点が存在し、双方で責任を果たすことによって初めてクラウド環境におけるセキュリティが担保されることになります。このように、セキュリティに関する責任を両者で共有して対処するという考え方を「責任共有モデル」と呼んでいます(図表2)。

図表2　責任共有モデル



出所：デロイト作成

ここで、クラウドサービス利用者であるユーザー企業にとって重要なことは、自身の責任範囲を正確に把握し、その責任範囲内のセキュリティリスクを確実にコントロールするということです。

クラウドサービスのマーケティングメッセージとして、クラウドは安価で堅牢かつセキュアである、というイメージが伝えられることが多くなっています。これは、ある意味で正しいのですが、この文脈でセキュアな状態であるのはあくまでもクラウドサービス自体、すなわち、責任共有モデルにおけるクラウドサービス事業者の責任範囲においてセキュア、という意味であるため、クラウドサービス側に利用者側の範囲も含めた全てのセキュリティ対応を任せられるということではありません。クラウドサービス利用者であるユーザー企業側の責任範囲については、自社もしくは自身で確実に対応することが求められます。

こうした前提の上で、クラウドサービス利用者である企業が取り組むべきセキュリティリスク管理の取り組みとして3つのことを提言します。

1. クラウド利活用を前提としたセキュリティ管理規程の整備や運用プロセスの見直し

現行のセキュリティ管理規程や運用プロセスが、クラウド利用を前提としたものになっていないという課題感を持つ企業は多いと思われます。ここ数年でのクラウドサービスの進化は非常に目覚ましく、3～4年前に更新した規程が既に実態に合わず陳腐化しているといったことも珍しくはありません。

この状況で既存の管理規程をクラウドに当てはめようとした場合、厳密に解釈するとクラウドに対しては条件が厳しすぎるためにクラウド利用が認められなかったり、逆に解釈を緩めすぎるとルールが形骸化して適切な統制ができなかったりするといった問題をひき起こします。

現状のクラウドの利用実態に応じた適切なコントロールを可能にするためにも、クラウド利活用を前提とした管理規程や運用プロセスのアップデートが求められます。

2. 現場部門とリスク管理部門のクラウドセキュリティに関する連携強化

クラウドサービスは新規導入が容易であり、新たな高機能サービスが次々と登場することから、現場部門主導で利用が進んでいくことが多いと思われます。セキュリティ統制を掛ける役割であるリスク管理部門にとっては、新しいサービスに常にキャッチアップしていくことに苦労しているという声をよく耳にします。

一方で、現場部門の立場としては、クラウド導入プロジェクト内にセキュリティに関する専門家が配置されていないケースが多く、利用するクラウドサービスの仕様を読み、適切なセキュリティ対応を行うということが十分にできていない可能性があります。

クラウドサービスは仕様がそれぞれ異なるため、サービス毎に個別検討しなければならない部分が多くなる傾向にあります。これに対処するためには、やはり現場部門とリスク管理部門が双方の知見を持ち寄り、協力しあうことが効果的だと考えられます。

リスク管理部門は、現場に対するクラウドセキュリティに関するガイドラインやFAQの提供、また、コンサルテーションを行うための仕組みを用意することが望まれます。また、クラウド利用が進んでいる企業の中には、社内横断的な組織としてCloud Center of Excellence (CCoE)と呼ばれる、クラウド利活用に関する専門家による相談窓口を設置しているケースがありますが、この組織内にクラウドセキュリティに関する専門家を配置することも効果的です。

3. クラウド環境を前提とした全社サイバーセキュリティ評価の実施

多くの企業が定期的にサイバーセキュリティ管理態勢の評価を実施していると思いますが、これまでのセキュリティ評価は、どちらかと言うと主に自社管理が可能なオンプレミス環境を中心に行っているケースが多いと思われます。クラウド利用は、外部委託の一形態としての評価程度に留まっていることも多く、この評価からは前述したようなインシデントを予見することは難しいと考えられます。

近年、クラウドに焦点を当てた評価フレームワークも登場してきており、例えばクラウドセキュリティに関する団体であるCloud Security Alliance(CSA)がリリースしているCloud Control Matrix(CCM)等を利用することが可能です。従来のセキュリティ評価に対して、これらのフレームワークを追加的または補完的に実施することによって、クラウド環境を含む包括的なセキュリティ管理態勢の構築が期待できるのです。

まとめ

クラウド利用に伴うリスクは、設定不備に伴う情報流出だけではありません。オンプレミス環境とは異なることにより、以下のようなリスクも高くなります。

- 不正ログイン
  - フィッシング等により窃取した情報を悪用してクラウドサービスにログイン
  - クラウドサービスは一般にインターネットからアクセスできるため、不正ログインのハードルが低くなる
  - 不正ログイン等の監視について、サービスごとに仕組みを検討する必要がある
- クラウド上のデータの消失
  - クラウドサービス事業者の過失等によるデータの消失
  - バックアップの取得をすべてサービス側に委託し、自社で保持していない場合、データが完全に失われる恐れ

クラウド環境を含む包括的なサイバーセキュリティ態勢評価を行うこと、オンプレミス環境とは異なることを前提としたセキュリティ管理規定の整備や運用ルールの見直しを行うことが、クラウドサービスを安全に利用する上で重要です。

EDR製品とネットワークのログを活用したインシデント分析の整理

近年標的型攻撃対策等でEndpoint Detection and Response (EDR)を導入する企業が増加しています。EDRはエンドポイントで検知・分析、ウイルススキャンの実行や端末の隔離といった対処をリモートから可能にしているため、インシデント発生時の対応方法に大きな変化をもたらしています。

また、エンドポイントでの検知は端末の振る舞いを監視するため、従来のシグネチャベースの検知手法とは一線を画していると言えます。CICでは様々なアラートを分析していますが、EDRはエンドポイントの振る舞いも含めて詳細に分析することができる一方、ネットワークのログ等と突き合わせないと全体像が分からないといったケースも散見されます。

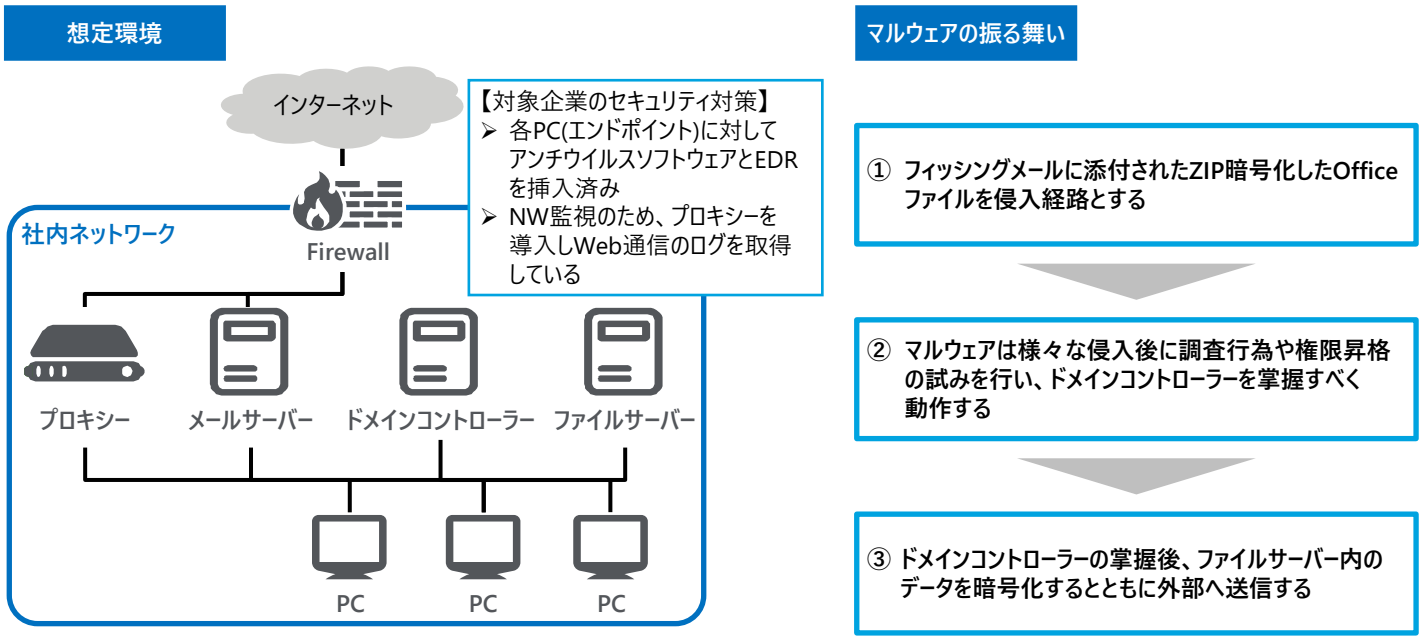
そこで、本項ではCICで分析した複数の事象を組み合わせた疑似インシデントを想定し、EDRとネットワークのログを活用してインシデント時の分析観点を整理します。

疑似インシデントの想定環境

疑似インシデントの想定環境として、EDR導入済みの企業ネットワークで二重恐喝ランサムウェアが動作したと想定します。

想定環境とマルウェアの振る舞いは図表1の通りです。

図表1　疑似インシデントの想定環境とマルウェアの振る舞い

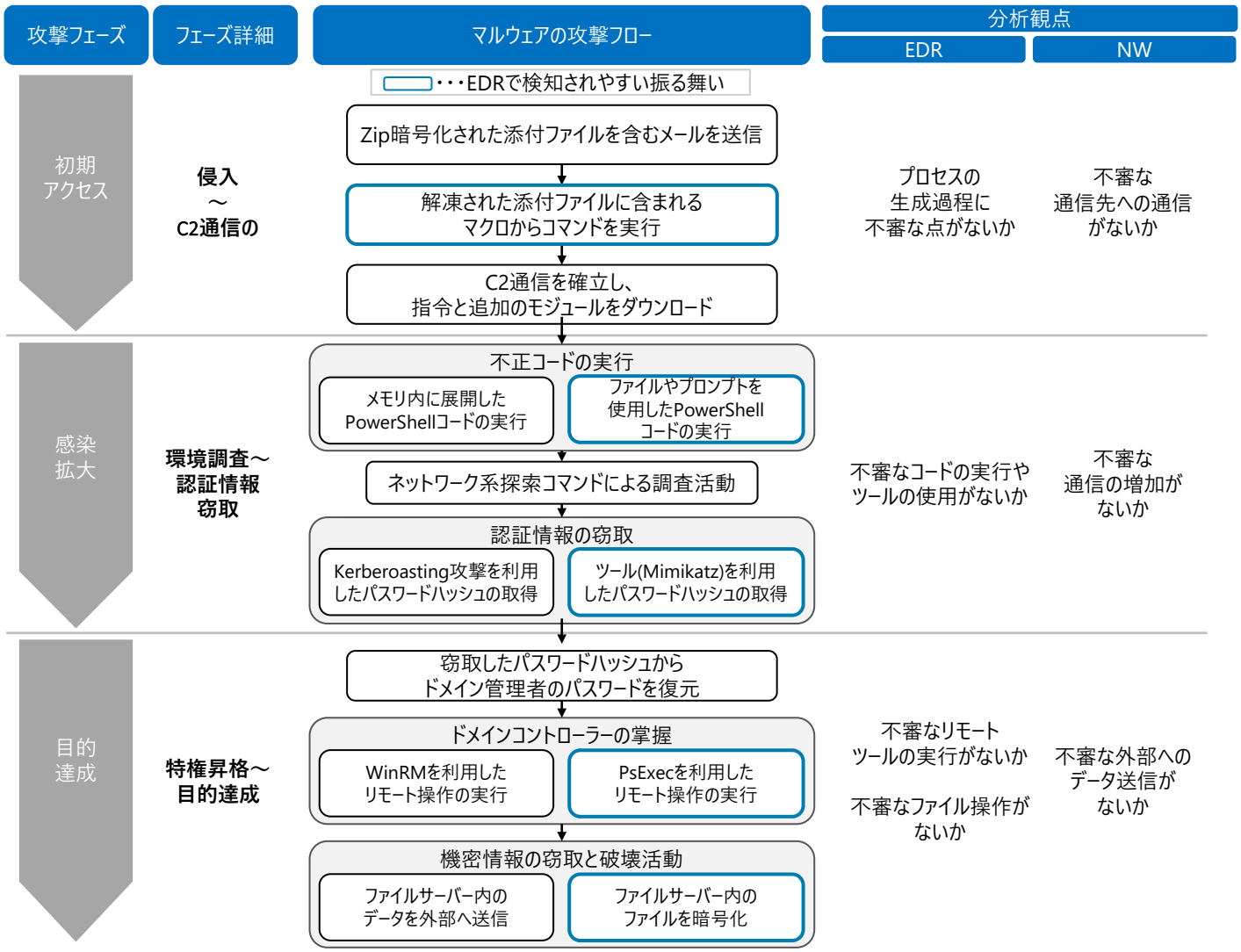


出所：デロイト作成

マルウェアの攻撃フローと分析観点

マルウェアが行う攻撃フローと、各攻撃フェーズにおけるEDR、ネットワークのログそれぞれの分析観点は図表2のように整理することができます。本件では全体の動作を把握するために、検知後も隔離等の対処は実行せず、目的達成までマルウェアを動作させることでEDRによって検知されやすいマルウェアの振る舞いを観測しました。その結果、図表2に示すように検知されやすいマルウェアの振る舞いが複数見つかったことがわかります。

図表2　マルウェアの攻撃フローにおけるEDRで検知されやすい振る舞いと分析観点



出所：デロイト作成

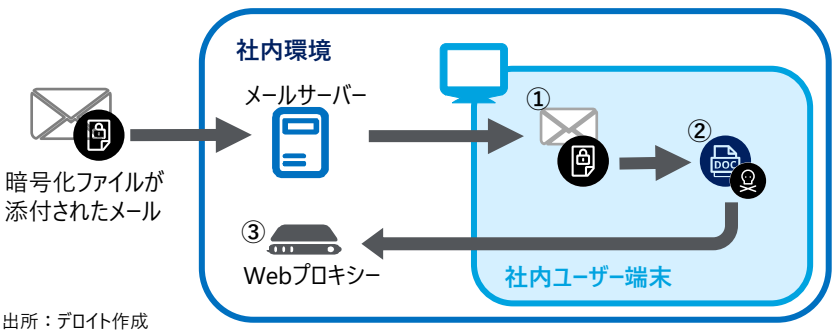
各攻撃フェーズにおける検知と分析観点の詳細

各攻撃フェーズの詳細は以下の通りです。

各攻撃フェーズにおける検知と分析観点の詳細

疑似インシデントでの初期アクセスフェーズにおけるマルウェアの振る舞いを図表3に示します。

図表3　初期アクセスフェーズの概要



出所：デロイト作成

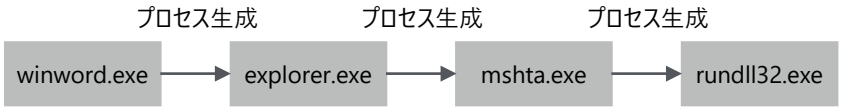
EDRによる分析観点

本フェーズでは「プロセスの生成過程に不審な点がないか」に注目してEDRログを分析していきます。図表3における ①、②の部分で通常のユーザー操作とは異なる形でプロセスが生成されていないかを確認します。

オフィスソフトであるwinword.exe からDLL(プログラムのパーツ)関数を呼び出して処理を実行させるrundll32.exeのプロセスが生成されている場合、呼び出された関数によっては不審と判断することが可能です(図表4)。

このマクロから関数を呼び出す振る舞いは、マルウェアの特徴的な部分として、EDRにより数多くのケースが検知されています。

図表4　winword.exeからrundll32.exeのプロセス生成



出所：デロイト作成

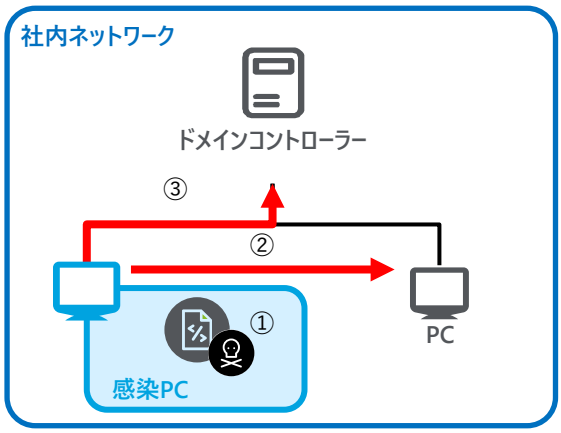
ネットワークのログによる分析観点

本フェーズでは「不審な通信先への通信がないか」に注目してネットワークのログを分析していきます。具体的には図表３③のように通信がWebプロキシーを介して行われる場合、そのログで不審な通信がないかということ点です。実際のアクセスのログとマルウェアの通信先の情報等と突き合わせることで、EDRの振る舞い検査でも検知できなかったマルウェアを発見することが可能です。

感染拡大フェーズの分析手法

次に「感染拡大フェーズ」におけるマルウェアの振る舞いを図表5に示します。

図表5　感染拡大フェーズの概要



出所：デロイト作成

EDRを用いた分析

本フェーズでは「不審なコードの実行やツールの使用がないか」に注目し、図表内及び以下に示す①～③のすべての部分で普段のユーザーと異なる動作を行っていないかを確認します。

① PowerShellを使用しない端末で、PowerShell等の起動があるか
② Net等の調査コマンドが使用されているか
③ パスワード解析ツールMimikatzの使用があった場合等、不審な振る舞いがあるか

ただし、これらはコマンドやツールの業務利用による誤検知も考えられるため、端末の日頃の利用傾向と比べて不審な動作かどうか判断する必要があります。

これらは最近のマルウェアによく見られる動作であり、EDRでも検知されますが、こういった動作を隠ぺいするマルウェアも存在します。既存のプロセスが展開したメモリ領域にコードをインジェクションする手法や、パスワードハッシュの取得に脆弱性を悪用するKerberoasting攻撃を使用した場合、EDR製品によっては検知できないといったケースもあります。

ネットワークのログを用いた分析

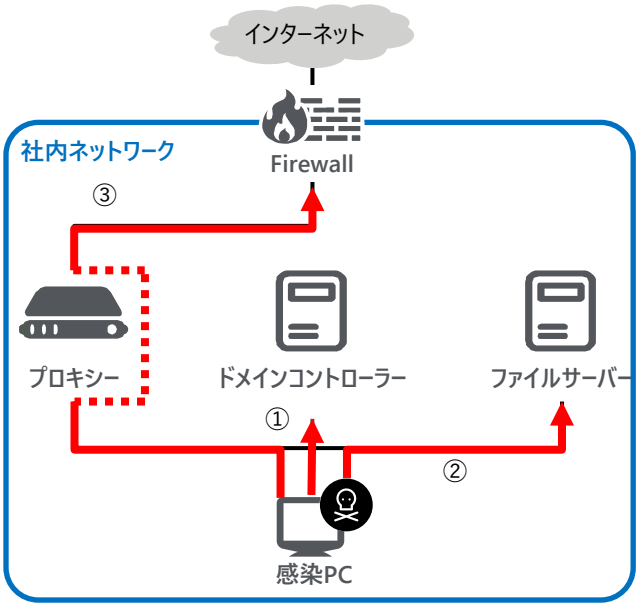
ネットワークのログを分析する際には「不審な通信の増加がないか」に注目します。具体的には図表5②、③の部分で他端末やサーバーに対してスキャン行為を行うため、存在しない宛先への通信や普段使用しないプロトコルの通信が増加していないかという点です。

保守作業や障害による通信増加などがネットワークログに影響を与えている可能性もあるので、メンテナンスや障害情報を把握して誤検知判断に役立てます。

目的達成フェーズの分析手法

本疑似インシデントでの最終フェーズである「目的達成フェーズ」におけるマルウェアの振る舞いを図表6に示します。

図表6　目的達成フェーズの概要



出所：デロイト作成

EDRを用いた分析

本フェーズでは「不審なリモートツールの実行がないか」と「不審なファイル操作がないか」に注目し、許可されていない端末によるリモート操作や、大量のファイルの書き換えといった異常な動作がないかを確認します。

リモートツールのマルウェアで頻繁にPsExecが利用されるためか、PsExecはEDRでよく検知されますが、同様のリモートツールでもWinRMを使用した場合では検知されなかったというケースも見られました。EDRで特定のツールの使用を検知した際に適切に判断できるよう、自社環境でどういったリモート操作が許可されているか、把握しておく必要があります。

また、ランサムウェアによるファイルの暗号化を、EDRでは短時間での大量のファイル作成、削除として検知していたこともわかりました。

ネットワークのログを用いた分析

ネットワークのログを分析する際には「外部への不審なデータ送信がないか」に注目します。データの外部送信では攻撃者が用意したサーバーのほか、正規のクラウドサービスが利用されるケースがあります。NATされたネットワーク環境等ではEDRのネットワーク関連ログの分析が難しい場合がありますが、ネットワークのログと組み合わせることでEDRで分析をした内容の精度を上げることができます。その際は、通信先の情報だけでなく、送信されたデータ量や回数などの傾向も含めて不審かどうか判断する必要があります。

まとめ

疑似インシデントで整理したようにEDRは有用なツールですが、単体では見えない部分もあるということがわかりました。攻撃の全体像を把握するために、EDRのログとネットワークのログとを組み合わせて分析することで、マルウェアを検知できる確率を高めることが可能となります。それに加えて、実際にマルウェアを検知し、攻撃フェーズに合わせた適切な対処を行うためには、EDR製品で何をどこまでできるのかといった仕様の把握と、マルウェアの攻撃手法を理解し、各種ログを分析する技能が必要になります。そのため、EDR製品を導入した際は、そのまま利用するのではなく、インシデント事例の分析や製品のトレーニングを重ねて運用の高度化を図っていくことが肝要です。もちろんこういった対応を実現していくためには、分析技術を持ったエンジニアを維持し、時間をかけて運用を高度化していく必要があるため、監視のアウトソースを検討することも選択肢の一つと言えるでしょう。

脆弱性公開から短期間で攻撃された事象から考える、攻撃に対する日頃からの備え

パッチ適用の重要性は広く認知されているものの、速やかに適用できない現実があることも事実です。特に、パッチ適用時に公開しているサービスを停止させなければいけない場合には、速やかなパッチ適用について組織内で合意を得ることが難しいかもしれません。システム管理者にとって、パッチ適用までどのぐらいの猶予期間があるかは悩ましいところです。本項では、CICで観測した事例を元に、脆弱性公開から攻撃が開始されるまで、実際にどの程度の期間があったのかを紹介します。また、脆弱性公開後に発生する攻撃に備えて、日頃から行うべきことを考察します。

2021年3月に公開されたF5 Networks社製品の脆弱性

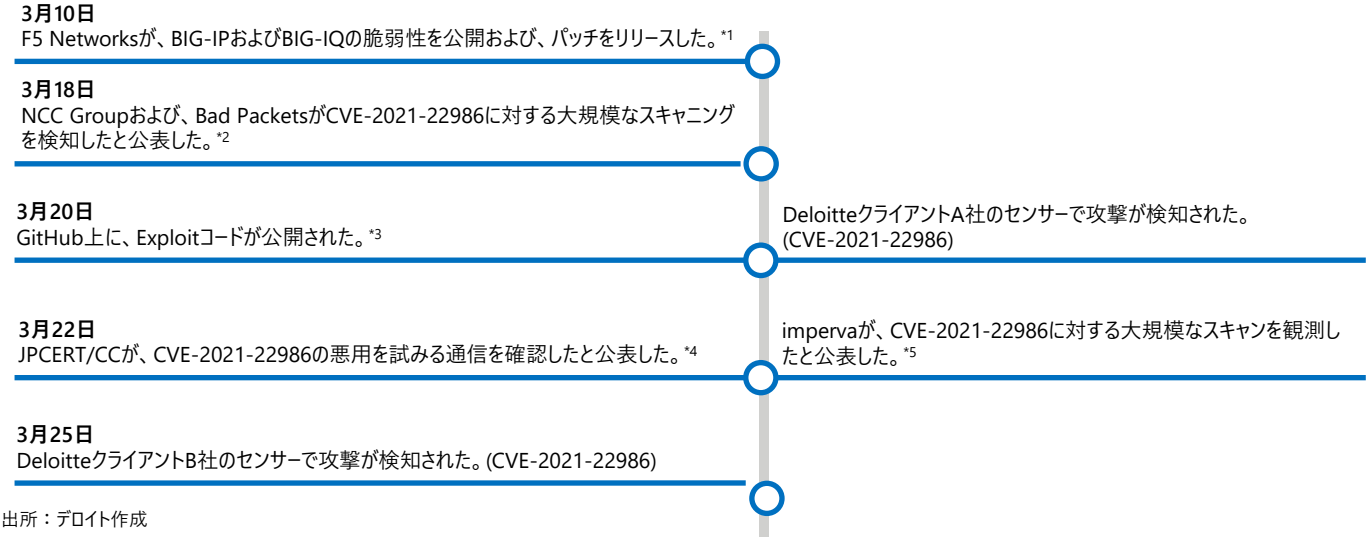
2021年3月に公開されたF5 Networks社製品の脆弱性を事例として取り上げます。同社は、BIG-IPおよびBIG-IQの合計21件の脆弱性を公開しましたが[*1]、公開された脆弱性には、以下のような特徴があります。

- 脆弱性の公表とともにベンダーからパッチが公開された
  脆弱性公開とともにパッチが公開され、迅速な対応により被害を防ぐことが可能となりました。
- インターネット公開機器の脆弱性である
  BIG-IPおよびBIG-IQは、インターネット上に公開されることが多いと考えられます。そのため、SHODANやCensys、ZoomEyeといったIoT検索エンジンの検索結果や外部からのスキャニングにより、脆弱性の可能性がある機器の特定は容易になります。
  また、攻撃活動が観測されているCVE-2021-22986は、BIG-IP製品の特定の共通機能に存在する脆弱性です。そのため、当該機能を有効化している場合、インターネット境界で用いられるVPNやロードバランサーなどが影響を受ける可能性があります。しかし、通信の安全性が重視されるインフラ事業者やネットバンキングにおいてはサービスの中断が難しく、パッチ適用のための社内調整に時間がかかると考えられます。

脆弱性に対する攻撃のタイムライン

脆弱性に対する攻撃のタイムラインを、図表1に示します。

図表1　2021年3月に公開された脆弱性に対する攻撃のタイムライン



出所：デロイト作成

*1：AskF5, "K02566623: Overview of F5 vulnerabilities (March 2021)", 2021/09/09アクセス: https://support.f5.com/csp/article/K02566623
*2：(Research and Intelligence Fusion Team,) RIFT: Detection capabilities for recent F5 BIG-IP/BIG-IQ iControl REST API vulnerabilities CVE-2021-22986, nccgroup, 2021年3月18日: https://research.nccgroup.com/2021/03/18/rift-detection-capabilities-for-recent-f5-big-ip-big-iq-icontrol-rest-api-vulnerabilities-cve-2021-22986/
*3：GitHub, "h4x0r-dz/RCE-Exploit-in-BIG-IP", 2021/09/09アクセス: https://github.com/h4x0r-dz/RCE-Exploit-in-BIG-IP
*4：JPCERTCC, "複数のBIG-IP製品の脆弱性(CVE-2021-22986)に関する注意喚起", 2021/09/09アクセス: https://www.jpcert.or.jp/at/2021/at210014.html
*5：(Shiran Bareli, Sarit Yerushalmi,) Attacks Spike Following The Disclosure Of CVE-2021-22986: F5 Networks BIG-IP iControl Remote Command Execution Vulnerability, imperva, 2021年3月22日: https://www.imperva.com/blog/attacks-spike-following-the-disclosure-of-cve-2021-22986-f5-networks-big-ip-icontrol-remote-command-execution-vulnerability/

脆弱性公開の約1週間後から攻撃が開始されていますが、CICで監視しているクライアントのセキュリティ機器も同様のタイミングで攻撃を検知しました。また、別のクライアントにおいては、当初、月例の定期メンテナンスのタイミングでパッチの提供を予定していましたが、脆弱性の緊急度を鑑み、定期メンテナンスを待たずにパッチ適用を実施するといった対応を取りました。

CICで観測した攻撃ログの一例を、図表2に示します。CICでは、セキュリティ製品のIPS機能のログから脆弱性を突く攻撃を検知しました。

図表2　セキュリティ製品のIPS機能で検知された攻撃

Time	deviceVendor	deviceEventCategory	sourceAddress	requestUrl
2021-03-20 21:41:54.000	[redacted]	F5 BIG-IP Remote Code Execution Vulnerability(90881)	23.251.45.232	"bash"
2021-03-20 21:05:48.000		F5 BIG-IP Remote Code Execution Vulnerability(90881)	23.251.45.232	"bash"
2021-03-20 20:40:45.000		F5 BIG-IP Remote Code Execution Vulnerability(90881)	23.251.45.232	"bash"
2021-03-20 20:21:11.000		F5 BIG-IP Remote Code Execution Vulnerability(90881)	23.251.45.232	"bash"
2021-03-20 17:31:39.000		F5 BIG-IP Remote Code Execution Vulnerability(90881)	23.251.45.232	"bash"
2021-03-20 17:21:29.000		F5 BIG-IP Remote Code Execution Vulnerability(90881)	23.251.45.232	"bash"
2021-03-20 16:27:24.000		F5 BIG-IP Remote Code Execution Vulnerability(90881)	23.251.45.232	"bash"
2021-03-20 16:25:38.000		F5 BIG-IP Remote Code Execution Vulnerability(90881)	23.251.45.232	"bash"
2021-03-20 15:46:04.000		F5 BIG-IP Remote Code Execution Vulnerability(90881)	23.251.45.232	"bash"
2021-03-20 15:06:00.000		F5 BIG-IP Remote Code Execution Vulnerability(90881)	23.251.45.232	"bash"
2021-03-20 15:02:14.000		F5 BIG-IP Remote Code Execution Vulnerability(90881)	23.251.45.232	"bash"

出所：デロイト作成

このようにパッチ適用のための猶予期間は、非常に短かいことがわかります。では、日頃からどのような備えが必要でしょうか。

脆弱性公開後の攻撃へ備えて日頃から行うべきこと

本事案で観測されたような脆弱性公開後に発生する攻撃に備えて、日頃から行うべき対応をご紹介します。

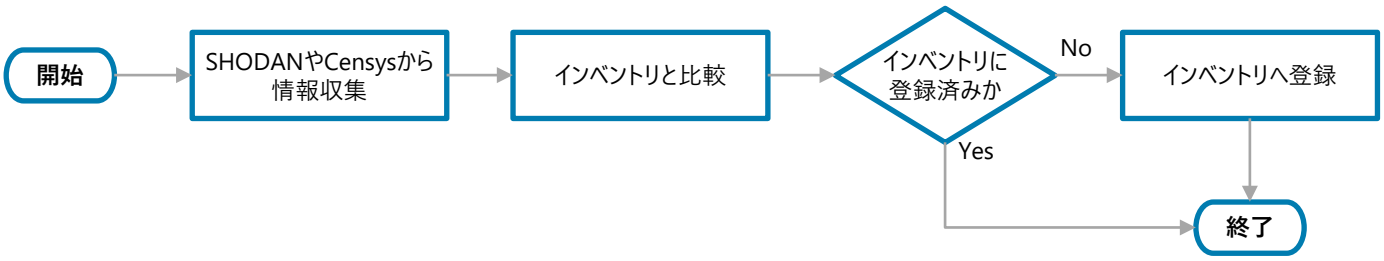
自社が利用している製品の脆弱性情報の収集

脆弱性が公開されると、開発元のベンダーからアドバイザリーが発行されます。また、攻撃手法のPoC (Proof of Concept)を公開するセキュリティ研究者もおり、こうした情報を日常的に収集、分析することで、対応するべき脆弱性に優先順位をつけることができます。

インターネット上に公開されている情報資産(サーバー、ネットワーク機器)の把握

インターネット上に公開されている情報資産の定期的な棚卸を実施し、自社の情報資産を把握する必要があります。また、SHODANやCensysといったIoT検索エンジンを活用することで、自社に紐づくインターネット公開機器の特定、利用ソフトウェアやバージョンを確認することができるため、IoT検索エンジンの情報を情報資産の棚卸に取り入れることも有効です(図表3)。

図表3　SHODANやCensysを使った情報資産の棚卸例



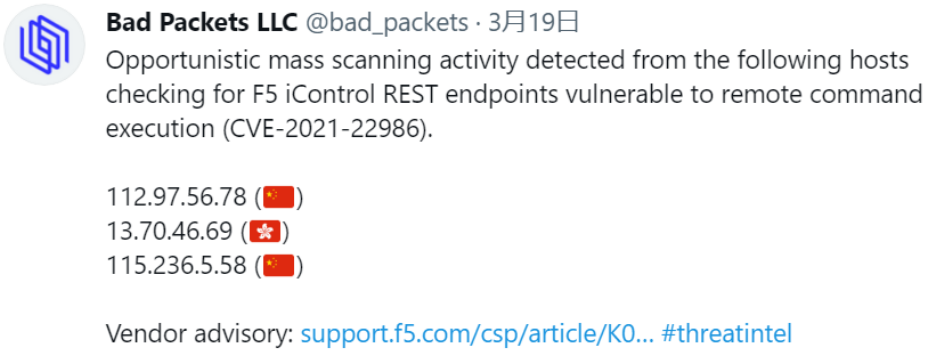
出所：デロイト作成

脆弱性に対する攻撃動向の収集

特定の脆弱性を攻撃するスキャニングが発生した場合に、大規模なハニーポットを運用しているベンダーやCDN、クラウドWAFベンダーが注意喚起を行うことがあります。また、Bad Packe社のように、Twitter等を通して、攻撃元のIPアドレスをリアルタイムに共有するベンダーもいます(図表4)

Security Information and Event Management (SIEM)を使って、攻撃元のIPアドレスと自社のインターネット境界のファイアーウォールのログを相関分析することで、自社への攻撃の状況を確認することができます。

図表4　Bad Packet社が公開したCVE-2021-22986に対するスキャン活動



出所：Bad Packet社Twitter

まとめ

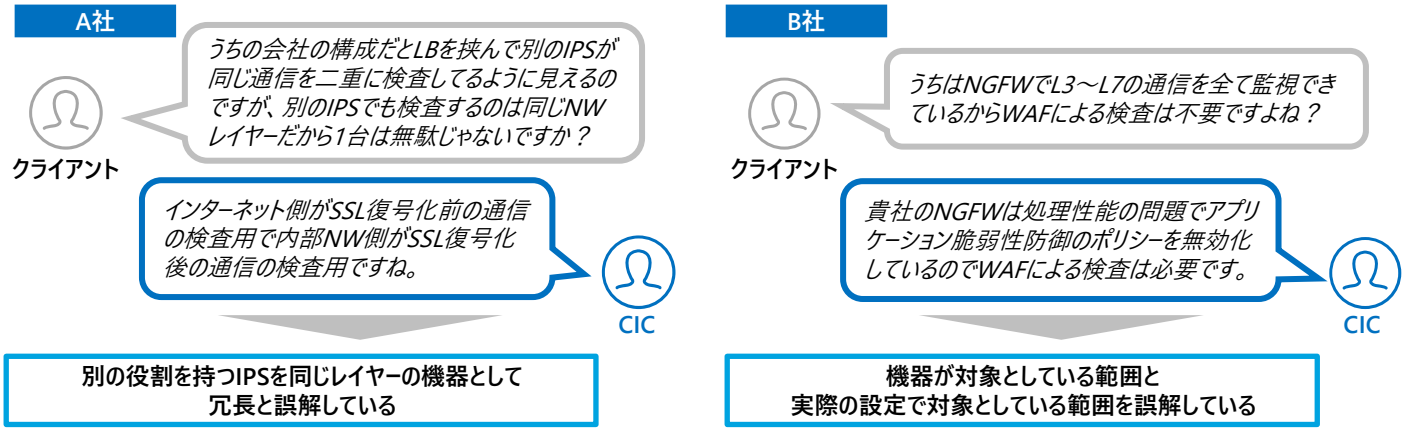
本項では、CICが対応した脆弱性公開から攻撃開始が短かった事例を紹介しました。脆弱性公開から約1週間という非常に短い期間で攻撃が開始されており、パッチ適用までの猶予期間は非常に短かったと考えられます。また、事例を元に、日頃からどのような準備を行うべきかについてご紹介しました。一般的な脆弱性管理に加えて、本項で紹介した方法を取り入れることで、攻撃開始前に自社への攻撃の可能性を把握することができ、攻撃開始後は、自社が実際に攻撃を受けているのかどうか理解することが出来ます。それにより、短い猶予期間の中で、脆弱性公開直後の攻撃に対して迅速に対応できるようになると考えられます。

インターネット公開WEBシステムの侵入防御レイヤーの再検討

従来のOSI参照モデルによる監視対象検討の限界

日頃、SOC業務の中でクライアントの情報セキュリティ担当者と会話をしていると、各セキュリティ機器の監視対象範囲に対する誤解から、思わぬ質問を受けることがあります。これは担当者が定期的に交代したり、セキュリティに詳しくなかったりと、自社の監視環境を十分に理解していないことが理由の一つとしてあげられますが、OSI参照モデルにおけるレイヤーごとのセキュリティ機器配置だけでなく、セキュリティ機器の持つ機能を考慮する必要があると考えます。そこで本項では、想定脅威を考慮した「新たな侵入防御レイヤー」の考え方をご紹介します。

図表1　顧客情報セキュリティ担当者との会話



出所：デロイト作成

いずれの会話でもIT担当の共通言語としてOSI参照モデルを使用していますが、図表2に示すいくつかの例の通りOSI参照モデルの階層と監視装置の対象範囲にはギャップがあり、誤解を生む要因となっています。

このミスマッチの例を次に示します。

図表2　OSI参照モデルと監視装置の対象範囲

階層	階層名	TCP/IP	監視装置の対象範囲
第7層	アプリケーション層	HTTPS/SMTP/FTPなど	【問題点①】対象の階層の境界があいまい / IDPS / NGFW・UTM / WAF / 【問題点③】機器の対象範囲は広いが、内部の機能が分かれており、ポリシー設定の整理が必要
第6層	プレゼンテーション層		
第5層	セッション層		
第4層	トランスポート層	TCP/UDP	DDoS対策装置 / 従来FW
第3層	ネットワーク層	IPなど	
第2層	データリンク層	Ethernet	【問題点②】機能は異なるのに対象の階層は同一 / 【問題点④】SSL復号化が必要な範囲を示すのに不向き
第1層	物理層		

出所：デロイト作成

上述した情報セキュリティ担当者の誤解の要因は、従来のOSI参照モデルに当てはめて、すべての階層を監視すればよい、という考え方にあります。
しかし、実際にはOSI参照モデルの階層と監視装置の対象範囲は異なるため、次のような問題が生じてしまいます。
問題点1. IDS/IPSの対象範囲を理解できない
問題点2. 機能の異なる監視装置が同一階層に存在するため対策が重複しているようにみえる
問題点3. 対象範囲が広く、機能も多いNGFW(次世代FW)/UTMについては各機能の役割を整理する必要がある
問題点4. SSL復号化のようにそもそも対象範囲をマッピングできない

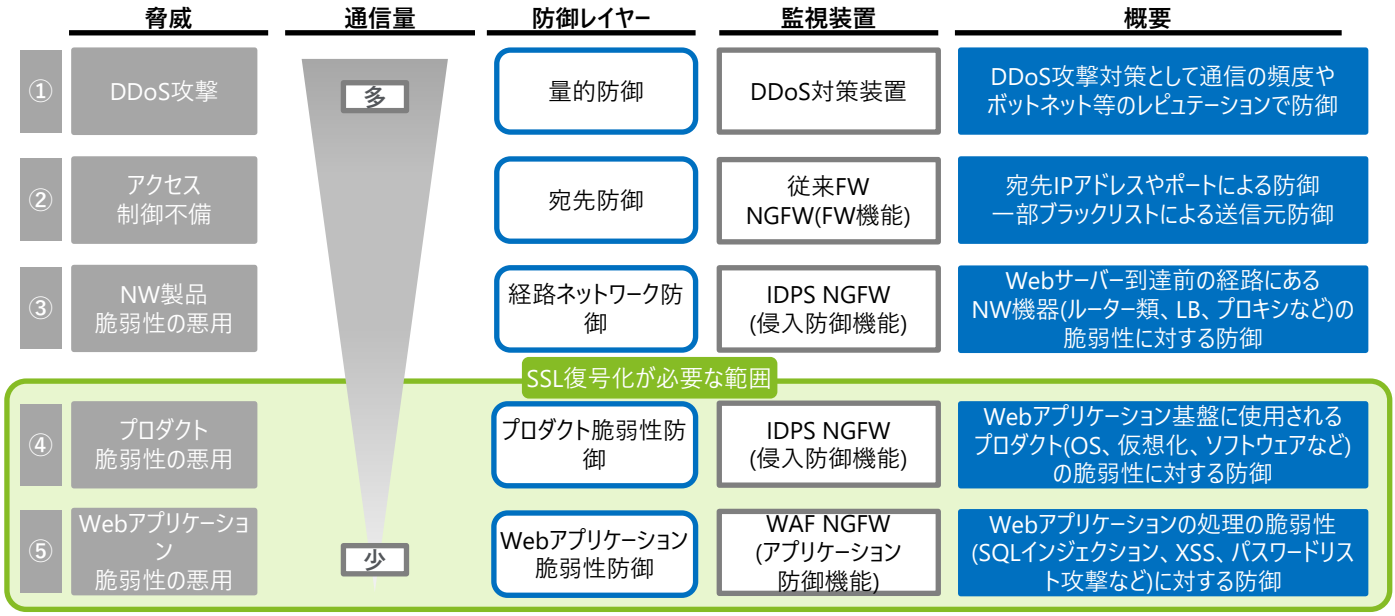
こうした理解のまま監視装置の構成を検討すると、本来必要な監視を不要と判断してしまう可能性があります。
特に問題点4のSSLの復号化が必要な範囲については、Webサーバーの常時SSL化の流れによって監視装置導入の後にSSL化を実施したことで、適切な監視ができていないケースが多く見受けられます。
そこで本項では、監視装置の対象範囲をより正確に理解するために、外部からの攻撃に対応する「新たな侵入防御レイヤー」の考え方をご紹介します。

新たに検討したインターネット公開Webシステムの侵入防御レイヤー

SOC業務による監視対象は外部からの不正侵入に限りませんが、本項ではインターネット上に公開されたWebシステムの環境を検討対象とし、新たな侵入防御レイヤーを次の5階層に整理しました。尚、これは前段のOSI参照モデルとは異なる考え方です。
① 量的防御層(DDoS攻撃等大量のトラフィックによる妨害の防御)
② 宛先防御層(宛先IPアドレスやポート、ブラックリストによる送信先の防御)
③ 経路ネットワーク防御層(サーバーを保護するNW機器の脆弱性に対する防御)
④ プロダクト脆弱性防御層(OS、仮想化、ミドルウェアの脆弱性に対する防御)
⑤ Webアプリケーション脆弱性防御層(SQLインジェクション、XSS攻撃などに対する防御)

新たな侵入防御レイヤーの5階層は、通信量が多く、防御対象のWebサーバーから遠いインターネット側で防御することが望ましい①～⑤の順で並べていますが、必ずしもこの順序で機器を設置する必要があるというわけではありません。
図表3で示した通り、常時SSLが標準化した環境において、④プロダクト脆弱性防御層と⑤Webアプリケーション脆弱性防御層は暗号化通信を復号化して監視を行う必要があります。

図表3　インターネット公開Webシステムの侵入防御レイヤー



出所：デロイト作成

新たな侵入防御レイヤーの5階層は、通信量が多く、防御対象のWebサーバーから遠いインターネット側で防御することが望ましい①～⑤の順で並べていますが、必ずしもこの順序で機器を設置する必要があるというわけではありません。
図表3で示した通り、常時SSLが標準化した環境において、④プロダクト脆弱性防御層と⑤Webアプリケーション脆弱性防御層は暗号化通信を復号化して監視を行う必要があります。

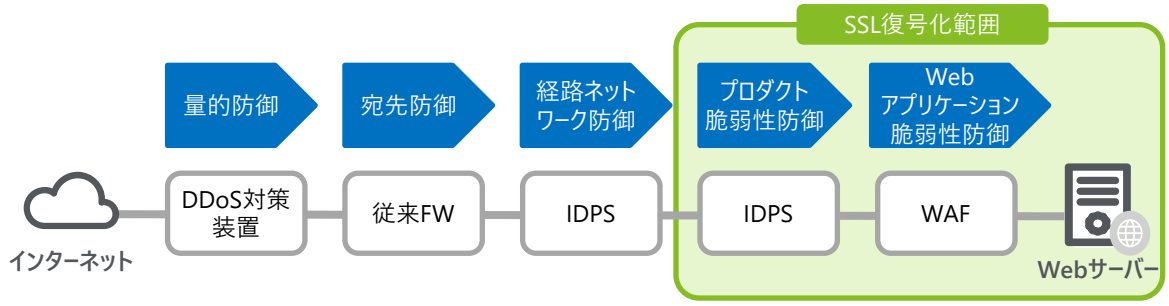
新たな侵入防御レイヤーの実環境への適用

新たにご紹介した侵入防御レイヤーの考え方をもとに、実際によくある環境を想定して3つの防御構成のパターンをあげます。

構成パターン1：各階層設置構成

すべてのレイヤーに一つずつ監視装置を設置した構成を図表4に示します。機器の台数分コストが高くなるため、実際にこの構成を採用するケースは稀ですが、高い信頼性が求められ、かつクラウドの利用が制限される場合に有効な構成です。

図表4　各階層設置構成

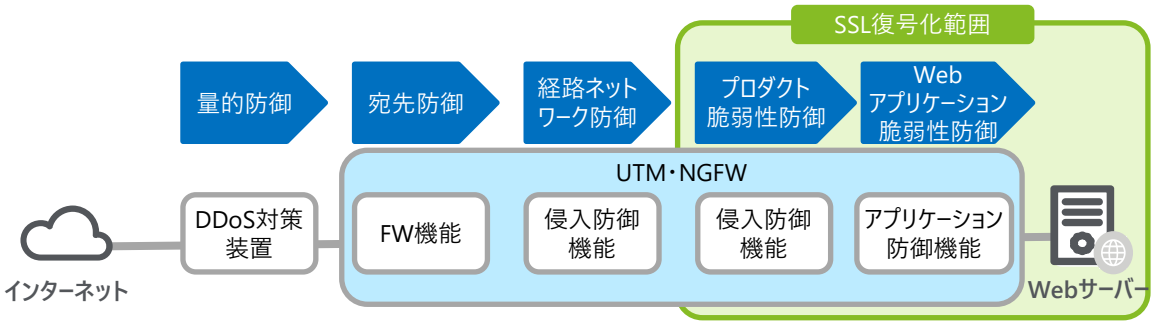


出所：デロイト作成

構成パターン2: NGFW・UTMの活用構成

NGFW・UTMによって幅広い範囲をカバーする構成を図表5に示します。機器の台数が少ないため、コストに優れる反面、処理性能の制約からトラフィック量によっては一部機能を専用機に代替する必要があります。また、機器の特性として、特にWebアプリケーション脆弱性防御層において専用機より精度が劣るケースがあり、その場合はWebサーバーの監査ログの監視などリスク低減策を検討する必要があります。

図表5　NGFW・UTMの活用構成



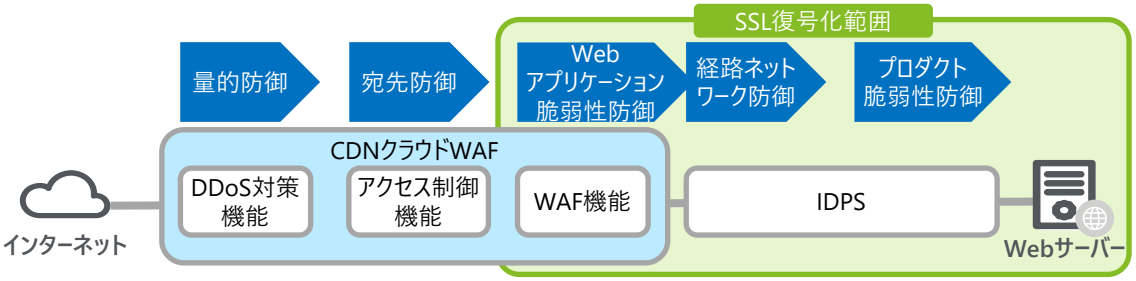
出所：デロイト作成

構成パターン3： CDNクラウドWAF構成

CDNクラウドWAFで第1、2、5層を防御し、内部では侵入防御のみを実施する構成を図表6に示します。クラウド環境でSSL復号化まで実施することで社内環境での負荷を低減することが可能です。CDNでWeb通信を一度終端させるため、第5層を3、4層よりも先に検査することが可能となっています。

クラウド上に証明書など多くのリソースを配置することが可能で、CDNを利用できる環境においては有効な構成です。

図表6　CDNクラウドWAF構成



出所：デロイト作成

まとめ

既述の通り、従来のOSI参照モデルを使用した考え方では監視装置の対象範囲とギャップがあるため、本来必要な監視ができない可能性があります。一方、今回のWebシステムの侵入防御に必要な機能ごとの階層に対し、通信量を抑制できる順で並べる考え方では各機器の対象範囲を正しく把握したうえで、より効率的な監視構成を実現することができます。

導入当初から環境が変化した監視対象の点検や、新規に追加される環境への監視対象の検討の際に、この新しい侵入防御レイヤーの考え方が検討の一助になれば幸いです。

セキュリティ製品以外のシステムのログによる効果的な監視：LINUXサーバーによるRCEの監視

セキュリティ監視を行う上で、Linuxにおけるシステムのログをどの程度確認されているでしょうか。セキュリティ監視では、一般的にIDS/IPS、WAF、アンチウイルス製品などのセキュリティログの監視をイメージされるかと思いますが、Linuxのログにも有用な情報があります。

本項では、Audit Daemonと呼ばれるLinuxのプログラムを例に、Apache Struts2の脆弱性CVE-2020-17530、S2-061によるRemote Code Execution(RCE：システム外部のネットワークから遠隔でサーバーのコマンドを実行)のイベントをいかにして監視し、影響の可否を確認するのかについてご紹介します。またAudit Daemonのログを監視することで、セキュリティ製品のシグネチャが未対応で攻撃を検知できない場合でも、Audit Daemonで同じ攻撃の確認や影響の把握が可能であるということも示します。

LinuxのAudit Daemon、Apache Struts2の脆弱性(S2-061)の概要

Audit Daemonとは、Linuxの監査ログを記録するプログラムで、サーバー上のカーネルにおけるシステムコールのイベントを確認する上で有用な手段です 。

また、Apache Struts 2とはWebアプリケーションを開発するためのフレームワークです。同脆弱性を悪用したCVE-2020-17530、S2-061はWebシェル(Webアプリケーション経由でサーバーのコマンドを実行)で任意のコード実行ができる脆弱性となっています 。

本件の検証環境を図表1に示します。RCEのイベントを被害者側のAudit Daemonのログから確認します。

図表1　攻撃者側と被害者側の検証環境

被害者側環境：
Apache Struts : 2.5.25
Maven
Eclipse
Tomcat
Audit Daemon

出所：デロイト作成

Audit Daemonのルール設定

LinuxのAudit Daemonを使用する場合は、Audit Daemonをインストールし、次のルールをauditctlというコマンドを入力してルールを設定します 。

本検証では、Webサーバーで実行されたコマンドのログを取得する次のルールを設定しました。

図表2　ログ取得のルール設定

```
$auditctl -a exit,always -F arch=b64 -F uid=1000 -S execve -k auditcmd
$auditctl -a exit,always -F arch=b32 -F uid=1000 -S execve -k auditcmd
```

出所：デロイト作成

尚、ルールの各項目と詳細は図表3の通りです。

図表3　Audit Daemonにおけるルール詳細

項目	詳細
-a	ルールを追加
exit	全てのシステムコール、ファイルシステムのリクエストをフィルターする設定
always	ログを出力
-F	ルールを作成するオプション
uid=1000	uidはシステムコールを行うユーザーを指定します。この場合、[1000」はWebサーバー及び開発環境を動かしているユーザー。uidは「id」コマンドで確認可能
arch	システムコールにおけるCPUのアーキテクチャを指していてb32は32ビット、b64は64ビット
-S execve	ルールに該当するシステムコールを設定するオプションで、「execve」は指定されたプログラムの実行を指す
-k auditcmd	Audit　Daemonに表示される識別用のkeyの値を設定するオプションで、「auditcmd」をkeyと設定。本項目は後述するログ検索の際に確認可能

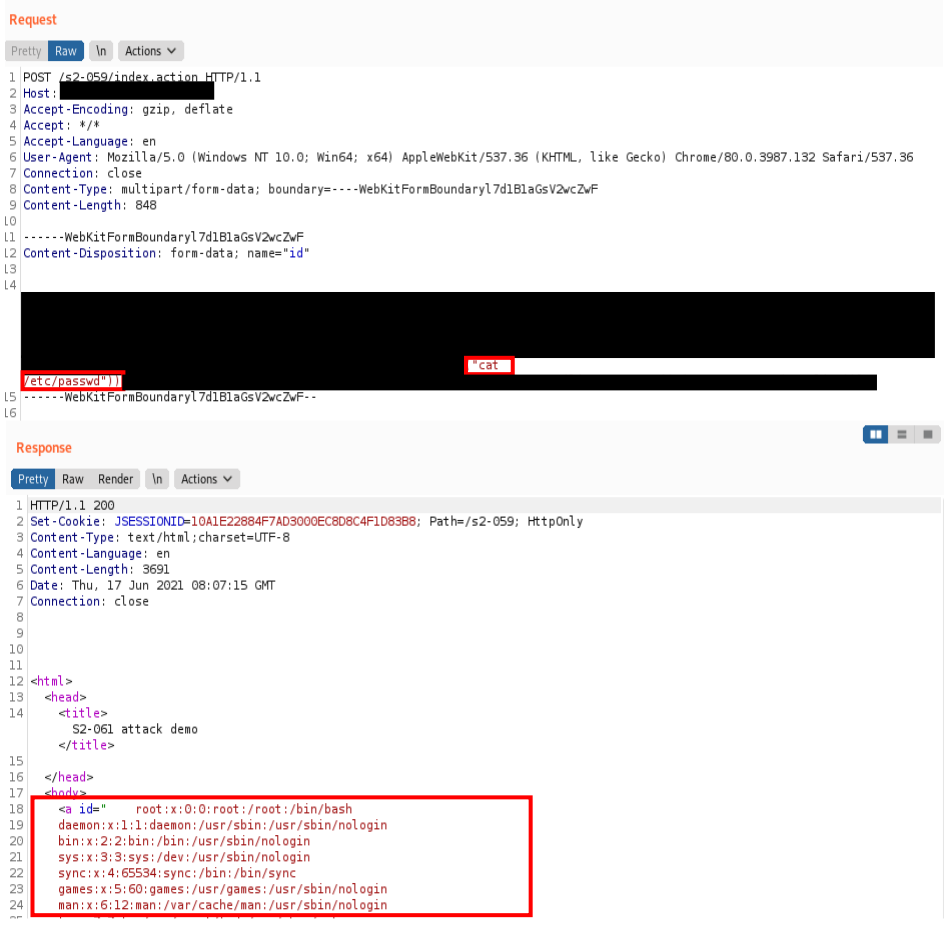
出所：デロイト作成

RCEの実行とAudit Daemonの確認

Audit Daemon側で監視を行う準備が整ったら、次に、実際にRCEの攻撃を実行してAudit Daemonでイベントのログを確認していきます。

Apache Struts 2の脆弱性(CVE-2020-17530、S2-061)を突いて攻撃を実行した結果を図表4に示します。図表内上部には、HTTPリクエストでサーバーのコマンドとして、「cat /etc/passwd(上赤枠)」の実行が示されています。図表内下部には、同コマンドの実行結果がHTTPレスポンスで表示されていることから、RCEが実行されていることが確認できます。

図表4　Apache Struts 2の脆弱性(CVE-2020-17530、S2-061)を使用したリクエストとサーバー側の実行結果



出所：デロイト作成

図表5　catコマンドの実行確認結果

```
test@ubuntu:~$ sudo ausearch -x cat -ts recent

----

time->Thu Jun 17 17:07:14 2021

type=PROCTITLE msg=audit(1623917234.961:4917): proctitle="70:73"

type=PATH msg=audit(1623917234.961:4917): item=1 name="/lib64/ld-linux-x86-
64.so.2" inode=264342 dev=08:05 mode=0100755 ouid=0 ogid=0 rdev=00:00
nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

type=PATH msg=audit(1623917234.961:4917): item=0 name="/usr/bin/cat"
inode=262314 dev=08:05 mode=0100755 ouid=0 ogid=0 rdev=00:00
nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

③type=CWD msg=audit(1623917234.961:4917): ④
cwd="/home/test/Developer/eclipse"

type=EXECVE msg=audit(1623917234.961:4917): argc=2 ②a0="cat" ③
a1="/etc/passwd"

type=SYSCALL msg=audit(1623917234.961:4917): arch=c000003e syscall=59
success=yes exit=0 a0=7fff44df2c10 a1=556b1e843320 a2=7fff44df2f68
a3=7fe501566ac0 items=2 ppid=7359 pid=7402 auid=1000 uid=1000 gid=1000
euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts2 ses=3 ①
comm="cat" exe="/usr/bin/cat" subj=unconfined ⑤key="auditcmd"
```

出所：デロイト作成

尚、図表5のログでRCE分析の際に必要な項目に番号(①～⑥)を記載しています。各項目についての詳細 は図表6の通りです。

図表6　2Audit Daemonにおけるログ項目詳細

#	項目	詳細
①	comm="cat"	• プロセスを開始するために使用されたコマンドを記録 • RCEで使用された「cat」コマンドが利用されたことを確認
②	a0="cat"	• 引数を表示 • 「cat」コマンドが実行されたことを確認
③	a1="/etc/passwd"	• 引数を表示 • ②のcatコマンドで「/etc/passwd」ファイルが参照されたことを確認
④	cwd="/home/test/Developer/eclipse"	• システムコールが開始したディレクトリーのパス • "/home/test/Developer/eclipse"のWebサーバー及び開発環境のプロセスで呼び出されていることを確認
⑤	key=auditcmd	• 先ほどのAudit Daemonのルールで設定したkeyの値「auditcmd」を表示

出所：デロイト作成

図表6の項目より「cat /etc/passwd(①、②、③)」のコマンドが、④「cwd="/home/test/Developer/eclipse"」のWebサーバー及び開発環境のプロセスで呼び出されていることがログ上で把握できます。具体的には、Webサーバーのプロセスが「cat /etc/passwd」のコマンド、RCEを実行したことが確認できます。

監視におけるAudit Daemonの有用性

前項までで、RCE実行のイベントを確認することができましたが、Audit Daemonで監視を行うことの有用性はどの点にあるのでしょうか。
本ケースを例に、次の3点の有用性が考えられます。

1. **セキュリティ製品で検知できなかった攻撃の事後的確認**
   Apache Struts2、DrupalなどのRCEの攻撃が、IDS/IPS、WAFなどのセキュリティ製品のシグネチャが未対応、もしくは設定不備などで検知ができなかった場合でも、Audit Daemonのログで事後的に確認することができるようになります。
2. **比較的早い攻撃段階でのインシデントの確認**
   今回のApache Struts 2のRCEは、攻撃の戦術や手法をまとめた枠組みのMITRE ATT&CK における、初期アクセスの「Exploit Public-Facing Application」の攻撃段階に該当しています(図表7)。ここで攻撃を確認することで比較的早い段階でのインシデント対応が可能になります。

図表7　Apache Struts 2の脆弱性(S2-061)のMITRE ATT&CK

出所：デロイト作成

3. **攻撃の可否および、影響の把握**
   IDS/IPS、WAFでは攻撃通信の検知は行えますが、システム(Linux)側の処理が確認できないため、攻撃が成功したのか、攻撃成功後に攻撃者はどこにアクセスし、何の情報を窃取したのかという影響の確認を行うことが困難です。一方、LinuxのAudit Daemonは、正常とは言えない異常なシステム側の処理を見ることができるため、より正確に攻撃の可否、影響を把握した上で、インシデント対応が行えるようになります。

まとめ

本項ではLinuxのAudit DaemonによるRCEのイベント監視や同プログラムを使用することでより効果的な監視が行える、という有用性についてご紹介しました。
一方でAudit Daemonの監視のログは、次のようなSIEMによるリアルタイム検知に向かない、手間がかるといった課題があります。

- Audit Daemonのログは、SIEMに取り込めるが正常動作も記録するため、サーバーの負荷(ログ増加)への対応および、正常動作と攻撃の区別が必要
- 本項で説明した手動でのルール設定が必要

こうした課題はあるものの、LinuxのAudit Daemonのシステムに関するログは、次のような効果的な監視が行えるという課題を上回るメリットもあります。

- セキュリティ製品のシグネチャ未対応で検知できなくてもRCEのような攻撃を確認することができる
- システムに関する処理の確認により正確な攻撃の影響の把握ができる

したがってAudit Daemonの監視はリアルタイム検知ではなく、次のような事後調査で使用することでより効果的なインシデント対応を行うことが可能になります。

- 定点的にRCEのような特定イベントを調査する(環境下で検知できていない脅威の確認)
- 攻撃検知時に同ログを調査して攻撃成功の可否や影響を把握する

システムのログにはセキュリティの観点で有用な情報が埋もれています。したがってAudit Daemonによるログの定期的チェックや事後調査は、課題を上回る有用性があるため、是非その利用のご検討をしてみてはいかがでしょうか。

インシデント対応準備

二重恐喝ランサムウェアによる被害は海外のみならず日本でも増加の一途を辿っています。米国の石油パイプライン運営企業が操業停止する事態や、日本の大手ゼネコンやゲーム会社等がダークウェブ上で機密情報をリークされるといった事案もでてきています。また、最近では大量のデータを送りつけて企業のサイトやサービスを停止させる「第3の脅迫」や、被害企業の取引先や顧客にまで連絡して揺さぶりをかける「第4の脅迫」も出てきており、その脅威はさらに高まっています。

Deloitteでは、二重恐喝ランサムウェアの被害にあった複数の企業に対して、侵入経路・攻撃手口・被害範囲の調査、封じ込め・除去・回復に係る助言、および顧客・ステークホルダー対応などを含む危機管理に係る助言等を行っています。海外拠点がサイバー攻撃を受け一定期間業務停止になった事案や、数百台のサーバーやクライアントが暗号化され事業継続が困難になった事案など数多くの対応実績があります。本項では、これらの経験から、二重恐喝ランサムウェアの被害に備え、どのような準備が必要であるのか、被害企業が事前に準備できていなかったことが多いポイントを６つに絞ってご紹介します。

事前準備１：インターネット出口へのホワイトリスト適用

攻撃者は、最初に悪用した入口が塞がれた場合でも再侵入できるように、バックドアを仕掛けることがあります。バックドアを塞がずにインシデント対応を進めてしまうと、インシデント対応中に２次攻撃を受け、さらなる情報流出やデータ暗号化によるシステム停止の被害が発生し、顧客や取引先のレピュテーションを著しく悪化させるという事態に繋がりかねません。また、復旧作業の手戻りや、やり直しといった問題も発生しかねません。

２次攻撃を抑止する対策の一つとして、バックドア対策が挙げられます。しかしバックドアはどこに仕掛けられているのか容易に発見できないということや、バックドアは感染した端末からインターネットへ通信を行うことが多いため、活動を止めるためには社内からインターネットへの通信を全面的に塞ぐ必要性がでてくるという点が課題になります。

昨今のビジネスでは、クラウドサービスの利用やインターネットを通じた取引先とのデータ交換は一般的になっており、社内からインターネットへの出口を全面的に塞いでしまうと、業務に多大な影響が及んでしまうことが想定されます。そのため、有事に備え、インターネットへの通信を遮断した場合の業務影響の確認や、最低限必要なインターネット通信先(ホワイトリスト)を準備し、即時適用できるようにしておくことが望まれます。また、バックドア対策の一つとして、Web分離という技術的対策がありますが、強力な対策である一方で利便性が損なわれることがあるため、業務効率への影響を考慮して検討を進める必要があります。

尚、不正侵入は、海外IPアドレスから行われることがほとんどであるため、海外IPアドレスへのアクセスを全面的に遮断するという方法も考えられますが、クラウドサービスを利用している場合や海外に取引先などがある場合は、一様に遮断できないことがあり留意が必要となります。

事前準備２：調査に必要となるログの収集・保管

２次攻撃を抑止するためのもう一つの対策として、悪用された侵入経路・攻撃手口を特定し是正するという方法があります。侵入経路・攻撃手口を特定するためには、大きく分類すると、ネットワーク、コンピュータ、セキュリティ製品のログが必要になるため、これらのログを収集し一定期間保管しておくことが望まれます。

ネットワークログは、被害にあったコンピュータが、いつ、どのコンピュータと、どの位の量の通信を行ったかを調査する際に必要になります。特に、攻撃者が利用したインターネット側のコンピュータの特定や、社外への情報流出量を特定する際に必要になり、主にF/W、Proxyサーバー、DNSサーバー、VPN装置、電子メールサーバーなどのログが必要になります。

コンピュータログは、OSの種類により取得できるものが異なりますが、二重恐喝ランサムウェアの攻撃対象となりやすいMicrosoft Windowsには、イベントログが重要な手掛かりとなります。イベントログにより、攻撃者がいつ不正ログインをしたのか、どのような不正プログラムが起動されたのかなどの手がかりが得られます。また、被害範囲の特定を目的に、攻撃者がどのコンピュータからどのコンピュータに渡り歩いたかを調査する際にもイベントログは必要になります。イベントログはデフォルト設定では上記のような調査に必要なログが充分に取得されないため、JPCERT/CCからの情報[*1]やMicrosoft社からの情報[*2]を参考に設定変更しておくと良いでしょう。

セキュリティ製品ログについては、EDR製品やアンチウイルスソフト製品、コンピュータの操作記録を取得する製品のログなどが調査に役立ちます。セキュリティ製品は多種多様であるため、各製品の特性を理解し、侵入経路・攻撃手口・被害範囲の調査にどのように活用できるか事前検討しておくことが望まれます。

*1：一般社団法人 JPCERT コーディネーションセンター,「ログを活用した Active Directory に対する攻撃の検知と対策」,2017年7月28日: https://www.jpcert.or.jp/research/AD_report_20170314.pdf

*2：Microsoft HP, "監査ポリシーの推奨事項", 2021/09/09アクセス: https://docs.microsoft.com/ja-jp/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

少しは話が変わりますが、調査対象期間のログが、保管期限が過ぎていて残存していないケースがしばしば見受けられます。JPCERT/CCでは、高度サイバー攻撃の調査においては1年以上ログを保管することを推奨しています。*3また、攻撃者によりログが意図的に削除されているケースも少なからずあるので調査に必要なログは、ログ収集サーバー等に転送し、さらにオフラインバックアップを取得しておくなど、安全に保管しておくことが望まれます。

さらに、被害にあったコンピュータを初期化する前には、データ保全の必要性について検討する必要があります。業務復旧を急ぐあまりに被害にあったコンピュータをデータ保全せずに初期化しているケースが散見されます。初期化してしまうとコンピュータ上にあるログも消失してしまい、侵入経路・攻撃手口・被害範囲の調査が困難になり、その結果、2次攻撃の抑止が難しい、もしくは被害者やステークホルダーなどへの報告が適切にできなくなる可能性があります。

事前準備３：オフラインバックアップ

企業におけるデジタル化は急速に進んでおり、情報システムが保有するデータは増大し続けています。そのため、バックアップ時間を短縮させるために、ハードディスク上でオンラインバックアップを行うことが多くなってきました。一方で、ランサムウェアは侵入したコンピュータ上からアクセス可能なデータ領域を暗号化するため、オンラインバックアップデータも暗号化されるリスクがあります。

Crowd Strike社が発表したレポートによると、ランサムウェア被害に遭った日本企業の32%が身代金を支払ったという結果が出ています。*4身代金を支払った理由は明記されていませんが、バックアップからの復旧が困難であったため、身代金を支払わざるを得なくなった企業が多いことが推察されます。そもそもバックアップが取得されていなかったケースもあるかと思いますが、オンラインバックアップが暗号化されてしまったケースも一定程度含まれると考えられます。Deloitteが対応した案件でも、オンラインバックアップが暗号化されてしまったというケースはでてきています。

重要システムが暗号化されバックアップデータから復旧できない状態になってしまうと、事業継続が非常に困難になります。受発注システムや会計システムなどの基幹系システムが、過去データを含め復旧不能になってしまった際の業務影響を想像してみてください。万が一に備え、ランサムウェアによるバックアップデータの暗号化について、対策を講じることが望まれます。ランサムウェア対策したデータバックアップソリューションは各ベンダーから出てきているため、それらを活用するというのもリスク低減の一つとなるでしょう。

*3：一般社団法人 JPCERT コーディネーションセンター,「高度サイバー攻撃への対処におけるログの活用と分析方法」,2016年10月19日: https://www.jpcert.or.jp/research/APT-loganalysis_Report_20161019.pdf

*4：CrowdStrike、2020年度版グローバルセキュリティ意識調査結果を発表, CROWDSTRIKE , 2020: https://www.crowdstrike.jp/press-releases/crowdstrike-releases-global-security-attitude-survey-2020/

事前準備4：情報管理

コンピュータが侵害を受け、ネットワークログ等で一定量以上のデータが外部送信された痕跡が見つかった場合、当該コンピュータ内の何かしらのデータが外部流出した蓋然性が高いと言えます。情報流出の蓋然性が高いコンピュータ内に、個人情報や取引先などに係る重要情報が保管されていた場合、2次被害を抑止するために、どのようなデータが保管されていたかを特定する必要性がでてきます。その際に、当該コンピュータ内のどこにどのようなデータが保管されていたか管理されていないと、コンピュータ内のデータを洗いざらい調査する必要性がでてきてしまい、調査に多大な時間とコストを要することになります。そのため、個人情報や取引先などに係る重要情報等は管理台帳を作成し、自社で保有している情報を把握しておくことが望まれます。

個人情報が漏えいした場合の報告及び本人通知は、現行法では努力義務となっていますが、2022年4月に施行される改正法により義務化されることが決まっています。[*5]対象となる監督官庁によっては、流出のおそれがある段階で報告義務を課している場合もあります。また、取引先等に係る重要情報については、契約書により情報流出に係る報告義務が課せられている場合もあります。情報流出の蓋然性が高くなった場合に、少なくとも報告義務がある情報については、具体的にどのような情報が流出したのか特定できるよう保管場所を限定し、必要最小限のアクセス権限を付与、アクセスログを取得しておくようにすることが望まれます。また、流出情報の種類により、どこに報告する必要があるのか事前に整理しておくことが望まれます。

事前準備５：内部ネットワークのアクセス制限

ランサムウェアの多くは自己拡散する機能を兼ね備えています。1台目のコンピュータに感染した後、ネットワーク接続可能なコンピュータを探し出し、被害範囲を広げていきます。社内ネットワークにアクセス制限がない場合、ランサムウェアの被害は一気に広がります。そうした事態にならないよう、内部ネットワークのアクセス制限を必要最小限にしておくことが望まれます。特に、重要システムネットワークとオフィスネットワーク間、本社ネットワークと支店・子会社ネットワーク間については、アクセス制限の強化を検討されることが望まれます。また、攻撃者がよく利用するSMB通信、RDP通信などを業務利用する場合についても慎重な検討が必要です。攻撃者に悪用されるリスクを想定し、特定の端末からしか利用できなくする、モニタリングを強化するなど追加対策を検討することが望まれます。

事前準備６：重大インシデント発生時の対応手順

二重恐喝ランサムウェアの被害にあった場合、サイバー攻撃対応、情報漏洩対応、事業継続対応を同時並行で進める必要があります。一方で、これらの対応を進める責任部署は分かれていることが多く、そのためどの部署が対応を主導するのか曖昧になりやすく、抜け漏れや重複により対応が遅れるケースが少なくありません。有事において速やかに対応できるよう組織体制・役割分担を事前に整理しておくことが重要となります。その際、自社でカバーすることが難しい、技術的な調査(フォレンジック調査)やステークホルダー対応(危機管理)などについては、どの外部専門家に依頼するのかを含め、整理しておくことが必要です。また、重大インシデントについては、取締役会決議により危機管理委員会等を立ち上げ、トップマネジメントが指揮をとるという体制作りが、実質的なコントロール強化と対外的な説明責任強化をする上で重要になるため、事前検討しておくことが望まれます。

さらに重要なポイントは、重要業務の洗い出しと、それを支えるITシステム・インフラを特定しておくことです。これは簡単なようですが、業務で利用しているAシステムを復旧させるためには、裏で動作しているBシステムを復旧させる必要がある場合や、大企業の場合、一人の担当者が全てのITシステムを把握しておらず、それぞれの担当者にヒアリングするといった必要が出てくるため、想定よりも時間を要することがあります。そのため、事前に特定しておくことが望まれます。

*5：個人情報保護委員会HP, "令和２年 改正個人情報保護法について", 2021/09/09アクセス: https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/

【コラム】
海外CIC紹介と日本との連携事例

本コラムでは海外のCICをご紹介すると共に、海外CICと日本CICの連携について触れたいと思います。
Deloitteでは、サイバーリスクにおける重要度の高い世界20カ国地域以上にサイバーインテリジェンスセンターを構え、グローバルで最新の脅威に対応しています(図表1)。
特に他地域に先駆けてオープンしたスペインやカナダのCICでは早期からSOAR *1やスレットハンティング*2を業務に取り入れるなど新たなセキュリティソリューションの導入、分析手法の採用に力を入れています。

図表1　デロイトサイバーインテリジェンスセンターのグローバル分布

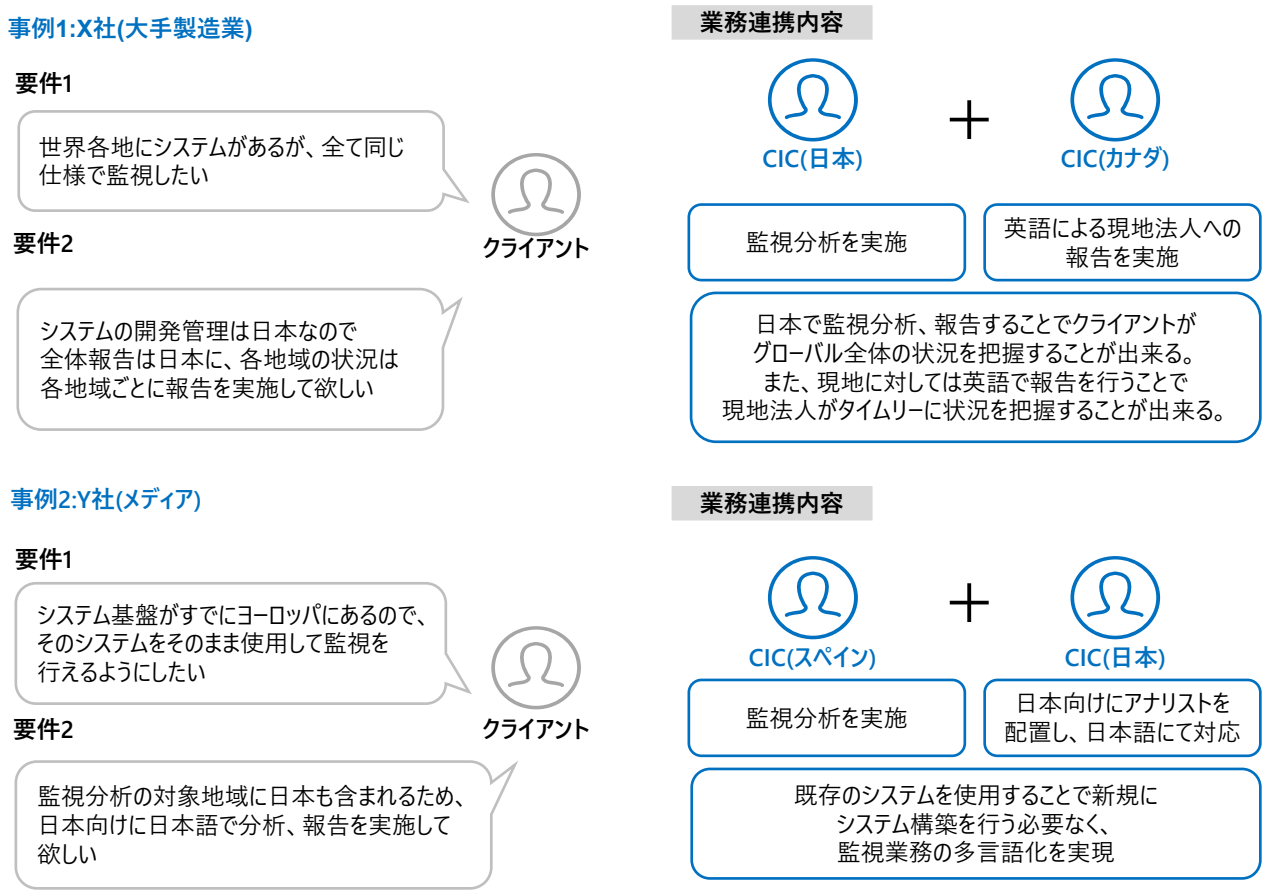
出所：デロイト作成

海外CICと日本CICとの連携

SOC業務を海外と連携する際は、監視時間帯ごとに監視地域をスライドさせる、いわゆる「フォロー・ザ・サン (Follow the Sun)」体制を取ることが一般的に多くなっています。監視対象拠点が世界中に存在するグローバル企業では、フォロー・ザ・サンのSOCサービスを利用することで、運用レベルにバラつきのないセキュリティ監視を実現することが出来ます。一方で、フォロー・ザ・サン体制には地域ごとのカスタマイズがしにくく、対応言語の統一を図る必要があることなど、結果として全体での柔軟な対応が難しくなるといった課題が残ります。
CICではフォロー・ザ・サンの体制はとらず、基本的に地域ごとに監視サービスを提供しています。各地域の脅威情報や運用体制に関する情報は共有し、CIC全体の高度化は推進しつつも、各地域ごとに独立したオペレーションを実施しています。
一方、グローバルに事業を展開しているクライアントからセキュリティ監視の相談を受けるケースは増えています。そのような場合は、海外CICと連携して複数拠点からの監視や、クライアントの業務時間や担当者の配置に合わせた運用体制を構築しています。
ここでは、日本CICと海外CICで実際に行っている連携事例をご紹介いたします。

*1：SOAR(Security Orchestration Automation and Response)。異なるセキュリティ製品を統合しつつ、監視運用を自動化するセキュリティのソリューションを指します。
*2：スレットハンティング(Threat Hunting)。セキュリティ製品で検知されない脅威をネットワークやサーバー等のログから探索する調査を指します。

図表2　日本CICと海外CICの連携事例



出所：デロイト作成

CICには海外監視を前提とした既存のサービスメニューが存在しているわけではなく、こうした要件が発生した際はクライアントの要件に合わせて運用形態をデザインし、監視を行っています。Deloitteではクライアントの要望に柔軟に対応するために、海外CICと調整を重ね、最適な監視体制の構築を目指しています。

本項では海外CICとの連携について紹介いたしました。次回以降は海外の業務内容についてより詳細に紹介する予定です。

おわりに

本レポートで取り上げたテーマのうち、「EDR製品とネットワークのログを活用したインシデント分析の整理」、「インシデント対応準備」は、実際にインシデントが発生した際にどのように調査して対応するかに関連します。CIC監視においても、EDRで検知したログの分析は増えています。一方、EDRを利用しているにも関わらず被害の拡散に気づけず、問題が大きくなってから対処している事例も散見されます。EDRの導入によって「迅速な初動対応」を期待したものの、その効果が発揮できない理由はどのような点にあるのでしょうか。

まず、EDRを導入してそのまま利用しているケースが挙げられます。製品によっては防御機能やリモートからの端末の制御など、有効化すべき機能を選択できます。デフォルトで稼働させるのではなく、利用する中でベンダーとも相談して実現したい機能を確認することが重要です。もう一つは導入後の運用が十分に練られていないケースが挙げられます。アラートが多過ぎて確認し切れない、個々の分析に時間がかかる、重要なアラートの検知後すぐに対処する体制ができていない、など運用上の課題は多岐にわたります。したがってEDRの検討段階で自組織でカバーする範囲を見極め、その効果を最大化する体制を整えることが必要となります。もちろんEDRも万能ではありません。本レポートでも紹介したように他のセキュリティ機器や関連ログと合わせて可視化レベルを高めることも引き続き必要でしょう。

今後もセキュリティ対策や情報収集の参考にしていただくべくCICの監視およびインテリジェンスサービスで得られた知見や分析結果を海外動向と合わせて発信していきます。

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