DIR SOC Quarterly

2024 autumn

vol 9

政策・法制度の動向

- 「金融分野におけるサイバーセキュリティに関するガイドライン」（案）の公表

トピックス：ランサム攻撃を巡る動向

- 脅威インテリジェンス
- 国内におけるランサムウェアを巡る情勢と政策動向

大和総研
Daiwa Institute of Research

目次

はじめに

本冊子は、サイバーセキュリティに関する動向をタイムリーにお伝えすることを目的としています。今回は、2024 年度第 2 四半期の話題を取り上げます。

本冊子は三部構成となっています。国家が主導しているサイバー攻撃対策について理解を深めるためには、それを指揮する行政機関の動向をウォッチすることが重要です。第 1 部ではこの点にフォーカスしています。また第 2 部と第 3 部では昨今、国内でも頻発しているランサム攻撃に関する話題を取り上げました。なお、ニュースなどでもよく目にするランサムウェア攻撃は、コンピュータウイルスの一種で、感染するとファイルを暗号化したり、デバイスをロックしたりして、元に戻すために身代金を要求するものです。他に SaaS などから情報を摂取し、身代金を要求する攻撃もあります。したがって、本レポートではランサムウェア攻撃も包含する「ランサム攻撃」として表記しています。

第 2 部ではランサム攻撃による被害状況や身代金要求などに関する実態を概観し、続いて第 3 部ではランサム攻撃の具体的な対策などについて紹介する構成としています。

本冊子で取り扱っている話題について、簡単にご紹介します。

近年ますます深刻化するサイバーリスクに対処するため、金融庁が公表した監督指針などの改正内容と新たなガイドラインのポイントについて解説します。また、特殊詐欺の被害も拡大している状況にあることから策定された『国民を詐欺から守るための総合対策』も紹介しています。対策の一つとして記載されている送信ドメイン認証は、企業活動を行う上でも必要性が増してきている対策といえます。

併せて、第 1 部ではサイバー攻撃キャンペーンについて紹介しています。このキャンペーンはわが国の JPCERT/CC のみならず、米国 CISA も注意喚起を出している攻撃手法です。取りうる対策も紹介していますので、是非参考にしていただければと思います。

第 2 部では、ランサム攻撃による被害やその影響のみならず、平時の対策および有事の対応方法などについて、事前に対策を検討しておくことが推奨される項目を列挙しておりますので参考にしてください。

第 3 部では、ランサム攻撃の主な対策となりうる脅威インテリジェンス、ASM（アタックサーフェスマネジメント）、脆弱性情報管理の技術的なトピックと国内のランサムウェア被害の状況並びに政策状況などを紹介しております。

上記トピックスのいずれかが皆さまの日々の活動に関連する何らかの「気づき」や「きっかけ」となれば幸いです。

2024 年 9 月　株式会社大和総研執筆者一同

1.『主要行等向けの総合的な監督指針』等の一部改正（案）及び『金融分野におけるサイバーセキュリティに関するガイドライン』（案）の公表

要約

- 近年ますます深刻化するサイバーリスクに対処するため、金融庁が『主要行等向けの総合的な監督指針』等の一部改正（案）および『金融分野におけるサイバーセキュリティに関するガイドライン』（案）を公表（*1）した。
- 『金融分野におけるサイバーセキュリティに関するガイドライン』（案）ではサイバーセキュリティに関する「ガバナンス」、「特定」、「防御」などの６項目についてそれぞれ「基本的な対応事項」および「対応が望ましい事項」を明確化して記載している。

今回の公表内容について

金融庁は 2024 年６月 28 日に、主要行や金融商品取引業者など向けの監督指針（全 10 種類）と資金移動業者・暗号資産交換業者など向けの事務ガイドライン（全６種類）の改正案および「金融分野におけるサイバーセキュリティに関するガイドライン」（案）（以降、新ガイドライン）をとりまとめ、公表しました。

監督指針・事務ガイドラインの改正では、新ガイドラインを踏まえたセキュリティ対策が行われることを前提として、参照先としての新ガイドラインの追加、記載の一部削除・簡略化などの見直しが図られています。下表は『主要行等向けの総合的な監督指針』の新旧対照表（案）です。「現行」において詳しく書かれていた箇所の一部は削除され、「新ガイドラインを踏まえ」という簡潔な記載になっています。なお、その他の監督指針、事務ガイドラインの改正も同様の内容となっています。

改正案	現行
Ⅲ－３－７－１－２　主な着眼点 （５）　サイバーセキュリティ管理 ①　取締役会等は、サイバーセキュリティの重要性を認識し、「金融分野におけるサイバーセキュリティに関するガイドライン」を踏まえ、必要な態勢を整備しているか。 （現行②～⑥の削除）	Ⅲ－３－７－１－２　主な着眼点 （５）　サイバーセキュリティ管理 ①　サイバーセキュリティについて、取締役会等は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。 ②～⑥　サイバーセキュリティ管理態勢の整備、サイバー攻撃対策、サイバー攻撃の被害拡大防止対策、システムの脆弱性管理、セキュリティ水準の定期的な評価の実施に関する記述
②　現行⑦を踏襲	⑦　インターネット等の通信手段を利用した非対面の取引を行う場合のセキュリティ対策に関する記述
③　現行⑧を踏襲	⑧　インターネットバンキング等の不正利用防止のための適切な手続きに関する記述
（現行⑨、⑩の削除）	⑨、⑩　サイバー攻撃を想定したコンティンジェンシープラン策定、サイバーセキュリティ人材育成などに関する記述
Ⅲ－３－７－２　ATMシステムのセキュリティ対策 Ⅲ－３－７－２－２　主な着眼点 （２）　セキュリティの確保 （略）また、個別の対策を場当たり的に講じるのではなく、セキュリティ全体の向上を目指しているか。セキュリティの確保に当たっては、「金融分野におけるサイバーセキュリティに関するガイドライン」も参照すること。（略）	Ⅲ－３－７－２　ATMシステムのセキュリティ対策 Ⅲ－３－７－２－２　主な着眼点 （２）　セキュリティの確保 （略）また、個別の対策を場当たり的に講じるのではなく、セキュリティ全体の向上を目指しているか。（略）

出典：『主要行等向けの総合的な監督指針』等の一部改正（案）及び『金融分野におけるサイバーセキュリティに関するガイドライン』（案）（*1）を基に大和総研作成

（*1）『主要行等向けの総合的な監督指針』等の一部改正（案）及び『金融分野におけるサイバーセキュリティに関するガイドライン』（案）の公表について

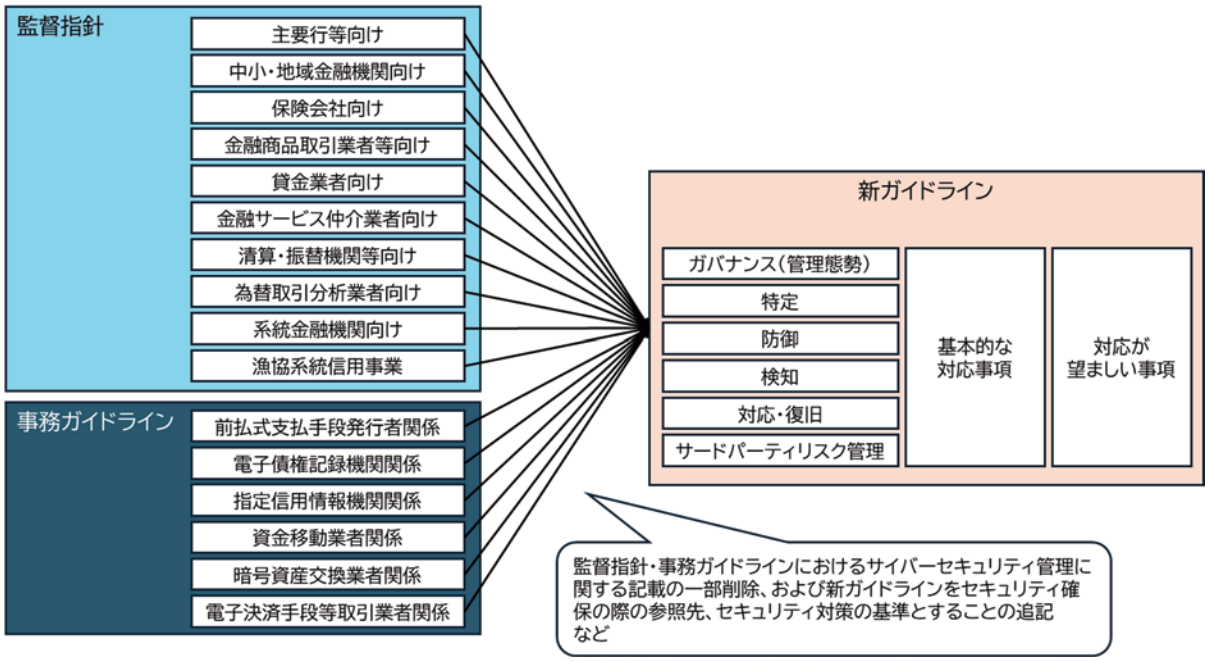
新ガイドラインの概要

昨今のサイバー攻撃の脅威は金融サービスの利用者および金融システムの安定に多大な悪影響を及ぼしかねず、金融庁はその任務である「金融機能の安定と預金者の保護」のために、金融セクター全体のサイバーセキュリティの強化が不可欠であると考えています。金融庁はこれまでも金融業界と協力し、監督指針や事務ガイドラインを通じて金融セクター全体のサイバーセキュリティの強化を促進してきましたが、このたび、これまでの検査・モニタリングの結果および金融セクター内外の状況の変化を踏まえ、監督指針などとは別に、さらに詳細なガイドラインとして新ガイドラインを策定しました。新ガイドラインは、下表のとおりの３節で構成されています。これまでは業種別の監督指針や事務ガイドラインにおいて業種ごとの特性に応じて策定されていた項目などを、新ガイドラインにおいて業種横断の共通項目として一本化しています。

節	概要
1．基本的考え方	金融機関などに求められるサイバーセキュリティに関する基本的な考え方や、自主的かつ積極的なサイバーセキュリティへの取り組み、経営陣の主体的な関与の重要性を記載。またサイバーセキュリティ強化のための業界団体や中央機関などの果たすべき役割についても言及。
2．サイバーセキュリティ管理態勢	サイバーセキュリティの観点から見たガバナンス、特定、防御、検知、対応・復旧、サードパーティリスク管理の 6 項目に関する着眼点について規定し、各項目について「基本的な対応事項」および「対応が望ましい事項」を明確化して記載。
3．金融庁と関係機関の連携強化	脆弱性情報の把握・共有、分析能力の強化のため、金融庁と各種機関との連携に対する基本的な考え方について記載。

出典：『主要行等向けの総合的な監督指針』等の一部改正（案）及び『金融分野におけるサイバーセキュリティに関するガイドライン』（案）（*1）を基に大和総研作成

図：監督指針及び事務ガイドラインと新ガイドラインの位置付け



出典：『主要行等向けの総合的な監督指針』等の一部改正（案）及び『金融分野におけるサイバーセキュリティに関するガイドライン』（案）（*1）を基に大和総研作成

新ガイドラインのポイント

新ガイドラインでは「基本的な対応事項」を“金融機関等が一般的に実施する必要のある基礎的な事項”、「対応が望ましい事項」を“実践することが望ましいと考えられる取組み”と定義しており、いずれも一律の対応を求めるものではなく、自組織を取り巻く事業環境、経営戦略およびリスクの許容度を踏まえた上でサイバーセキュリティリスクを特定、評価し、リスクに見合った低減措置を講ずることを求めています。以降、新ガイドラインにおける主なポイントを記載します。

（*1）『主要行等向けの総合的な監督指針』等の一部改正（案）及び『金融分野におけるサイバーセキュリティに関するガイドライン』（案）の公表について

- 規定内容の詳細化
  『主要行等向けの総合的な監督指針』を例として、監督指針から削除された項目の一部が新ガイドラインにおいてどのように定められているかを下表にまとめました。新ガイドラインでは各項目についてより具体的な対応内容が記載されていることがわかります。

新ガイドラインでの項目	新ガイドライン「基本的な対応事項」の例（要点）	監督指針での削除箇所の内容
ガバナンス（管理態勢） 人材育成	・定年や退職を踏まえた持続可能な人事政策の実施、資質・意欲のある職員の人材育成を阻害する人事異動の回避。 ・人材育成の観点から中長期的かつ計画的な人的配置の実施、外部からの採用・外部人材の活用だけでなく、内部人材の育成も考慮　など	サイバーセキュリティに係る人材について、育成、拡充するための計画を策定し、実施しているか。
特定 脆弱性管理	・脆弱性管理に係る手続の「脆弱性情報の入手先・入手プロセス、脆弱性の深刻度・影響の大きさおよび影響範囲の評価に関すること」などを含めた策定、必要に応じた見直し ・システムの重要度、リスク又は脆弱性の深刻度に基づいたパッチ適用などの対応期限の設定および対応実績の管理 ・深刻度の高い脆弱性は、グループ会社、海外拠点のシステムについても対応の範囲に含め、サードパーティが保有する重要なシステムについては対応の管理を行う　など	システムの脆弱性について、OS の最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。
対応・復旧 サイバー攻撃の被害拡大防止策	サイバー攻撃による被害拡大を防止するための対応（封じ込め）を行う際の考慮点は以下のとおり。 ・被害拡大防止のため通信遮断やシステム停止などの実施判断者の事前の明確化。また判断に必要な「停止する時間帯や期間、業務影響、業務の代替手段」などの情報整理 ・通信遮断やシステム停止などを行う場合、封じ込めと証拠保全のいずれを優先すべきか、インシデントの状況や自組織の方針に従い判断すること　など	サイバー攻撃を受けた場合に被害の拡大を防止するために、以下のような措置を講じているか。 ・攻撃元の IP アドレスの特定と遮断 ・DDoS 攻撃に対して自動的にアクセスを分散させる機能 ・システムの全部又は一部の一時的停止 等

出典：『主要行等向けの総合的な監督指針』等の一部改正（案）及び『金融分野におけるサイバーセキュリティに関するガイドライン』（案）（*1）を基に大和総研作成

- 管理態勢、規程などの定期的な見直し
  攻撃手法が多様化・巧妙化している現状、最新のサイバー攻撃の傾向などを踏まえ「サイバーセキュリティに係る管理態勢、規程及び業務プロセス、サイバー攻撃の脅威情報・脆弱性情報の収集元及び収集・分析方法、サイバーセキュリティリスク評価のプロセス」などについては、少なくとも１年に１回の見直しを求めています。
- サイバーセキュリティに関する取り組みの対外公表の推奨
  「対応が望ましい事項」として自組織のサイバーセキュリティに関する取り組みの意義を内外の関係者に表明するため、その内容を対外公表することを求めています。なお、この対外公表により、攻撃者の攻撃を助長する可能性があることも注意としてあげています。
- サードパーティリスク管理の詳細化
  サプライチェーン全体を考慮したサイバーセキュリティ戦略の策定、サードパーティが提供する商品・サービスの自組織での位置付けに応じたリスク評価の実施、サードパーティ管理のための台帳整備、サードパーティも含めたサイバーインシデント対応計画やコンティンジェンシープランの整備など、サプライチェーン全体のセキュリティ向上のためのより細やかな取り組みが求められています。

この他、新ガイドラインには様々な対応内容が詳細に記載されていますので、ご一読をお勧めします。

最後に

金融機関向けのサイバーセキュリティ対策についてはこれまで監督指針や事務ガイドラインはあったものの、具体的な対応内容などは提示されていませんでした。今回の公表により金融機関の業種横断的な指針が示され、自組織の状況に応じた必要な対応の検討が求められます。また、策定した方針や規程については昨今の攻撃手法やサードパーティのサービス利用などによるシステム構成の変化を踏まえ、継続的な見直しも計画に含めることが必要です。

（田川　晋作）

（*1）『主要行等向けの総合的な監督指針』等の一部改正（案）及び『金融分野におけるサイバーセキュリティに関するガイドライン』（案）の公表について

2.『国民を詐欺から守るための総合対策』の策定

要約

- 国内外で科学技術を悪用した特殊詐欺によって被害が拡大していることから、フィッシングなどを対象に『国民を詐欺から守るための総合対策』が策定された。
- 本総合対策では、送信者ドメイン認証技術やパスキーの導入推進、本人確認でのマイナンバーカードによる公的個人認証への原則一本化などがあげられている。

策定の背景

信頼とは様々な社会活動・経済活動を円滑に行うために不可欠なものであり、安全・安心な社会を支える基盤です。しかし、近年ではその信頼を逆手にとり、相手をだまして財産を奪い取る詐欺が増えています。そのような事案に対して政府は対策プランを策定し、官民一体となった対策を講じてきました。

しかしながら、官民をあげた対策に応じて特殊詐欺の手口も変化しています。その要因の一つとして急速に発展している科学技術の悪用があげられます。それにより、犯罪の手口が急激に巧妙化・多様化し、引き起こされる被害も拡大している状況が見受けられます。

このことは日本だけでなく国際的にも問題となっており、2023 年に水戸で行われた G7 茨城水戸内務・安全担当大臣会合においても共通の課題として認識が共有されました。また、2024 年にはロンドンで国際詐欺サミットが開催され、G7 以外の国を含むより広い枠組みで国境を越える組織的詐欺に協働して対処していくことが確認されました。

これらの背景を踏まえて、特殊詐欺、SNS 型投資・ロマンス詐欺、フィッシングを対象に、『国民を詐欺から守るための総合対策』(以降、本総合対策)(*1)が策定されました。

総合対策の概要

本総合対策は以下の章立てとなっています:

章題	内容
「被害に遭わせない」ための対策	①SNS 型投資・ロマンス詐欺、②フィッシング、③特殊詐欺等のそれぞれの被害実態に注目した対策について。
「犯行に加担させない」ための対策	主に「闇バイト」に関する対策について。
「犯罪者のツールを奪う」ための対策	携帯電話や預貯金口座、暗号資産、空き家等に関する対策について。
「犯罪者を逃さない」ための対策	犯罪グループの存在を見据えた取締り・実態解明や適正な科刑の実現、マネー・ローンダリング対策、財産的被害の回復について。

出典:『国民を詐欺から守るための総合対策』(*1)を基に大和総研作成

対策の具体的な内容

本総合対策の中では、利用者などに対する注意喚起や啓発、実効的な広告審査や偽広告の削除、無登録業者による偽広告の掲載が違法となり得る旨の明確化、取締り及び実態解明の促進や適正な科刑の実現といった、様々な場面、レイヤー、粒度での対策案があげられています。その中には情報技術に関わるものも含まれています。

(*1) 犯罪対策閣僚会議『国民を詐欺から守るための総合対策』(令和 6 年 6 月 18 日)

次に、フィッシングへの対策として、送信ドメイン認証技術（SPF、DKIM など）やパスキーがあげられました。送信者ドメイン認証技術とは、IP アドレスや電子署名を基に送信元の正当性を確認する技術です。また、パスキーとは、パスワードを使わずに認証する技術です。具体的な技術は以下の表のとおりです：

技術	概要
SPF	Sender Policy Framework の略。 送信元サーバーの IP アドレスから送信元の正当性を確認する仕組み。
DKIM	DomainKeys Identified Mail の略。 電子メールに付加された電子署名により送信元と本文の正当性を確認する仕組み。
DMARC	Domain-based Message Authentication, Reporting, and Conformance の略。 SPF または DKIM での認証に利用したドメイン名と表示上の送信元ドメインが一致するかを確認する。 一致しない場合には指定の操作が行われ、認証結果を送信側が受け取る仕組み。
BIMI	Brand Indicators for Message Identification の略。 DMARC での認証に成功したメールにロゴを表示させる技術。 オプションでロゴについての証明書を指定可能。
VMC	Verified Mark Certificate の略。 BIMI で表示されるロゴについての証明書。 ドメイン認証に加え、ロゴの商標登録、公証人や弁護士などによる申請者自身の確認などが求められる。
パスキー	パスワードの代わりに、アクセス先とアカウントに紐付いた公開鍵に対応する秘密鍵で生成した署名によって認証を行う技術。 ドメイン情報が一致しないと認証できないため、フィッシング耐性が高い。

出典：『国民を詐欺から守るための総合対策』を基に大和総研作成

なお、SPF/DKIM/DMARC については DIR SOC Quarterly vol.6 2023 autumn(*1)の『DMARC の導入にかかわる動向』で、パスキーについては vol.5 2023 summer(*2)の『パスワード不要の新しい認証方式「パスキー」』でそれぞれ取り上げています。たとえば、Gmail でロゴを表示させるためには VMC が必須となっています(*3)。また、au やメルカリ、任天堂といった企業では既にパスキーでの認証に対応しています。

他に、「犯罪者のツールを奪う」「犯罪者を逃さない」ための対策が記載され、契約などにあたっての本人確認があげられました。預貯金口座の開設や携帯電話の契約などの際には犯罪収益移転防止法(*4)や携帯電話不正利用防止法(*5)で本人確認することが定められています。この本人確認における本人確認書類の券面の偽変造が相次いでいるため、非対面での本人確認手法はマイナンバーカードの公的個人認証に原則一本化し、運転免許証などを送信する方法や顔写真のない本人確認書類などは廃止するとしています。また、対面であっても、IC チップ情報の読み取りを義務付けるとしています。

最後に

本総合対策は政府や地方自治体だけではなく、民間事業者の協力を得て推進するものとされています。そのため、これを基に各業界のガイドラインにセキュリティ対策として反映されることが予想されます。

本総合対策であげられた対策は特定の業界におけるものも含まれるため、必ずしも読者の皆さまの業界に当てはまるとは限りません。しかし、対策方法から逆説的に犯罪の手口がうかがえますので、私的な防犯対策としても一度読んでおくと良いでしょう。

（DIR SOC Quarterly 執筆者一同）

(*1) DIR SOC Quarterly vol.6 2023 autumn［第 3 部 1.］

(*2) DIR SOC Quarterly vol.5 2023 summer［第 3 部 2.］

(*3) Google Help『BIMI を使用してメールにブランドロゴを追加する』

(*4) 犯罪による収益の移転防止に関する法律（平成 19 年法律第 22 号）

(*5) 携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律（平成 17 年法律第 31 号）

3.『Operation Blotless攻撃キャンペーンに関する注意喚起』

要約

- Living Off The Land(LOTL)戦術と呼ばれる攻撃に対する警戒が高まっている。
- LOTL 戦術とは、正規ツールを駆使して攻撃を行う手法であり、検知が難しいという特徴がある。初期侵入経路として SSL-VPN 製品の脆弱性を悪用した攻撃が多い。
- 将来の攻撃に備えるためには、脆弱性対策が重要であり、インフラとアプリケーションの両面で考慮する必要がある。これには、ASM ツールや SBOM(SCA)ツールの活用により、脆弱性のリスクを低減することが期待される。
- 脆弱性を可視化し、基本的なパッチの適用を行うことが攻撃を防ぐための重要な対策である。

概要

2024 年 6 月 25 日、JPCERT/CC は『Operation Blotless 攻撃キャンペーンに関する注意喚起』を発表し、環境寄生型(LOTL:Living Off The Land)戦術を利用するサイバー攻撃キャンペーン「Operation Blotless」に対して注意を喚起しました(*1) 。

LOTL 戦術は、以前から持続的な標的型攻撃(APT:Advanced Persistent Threat)を行う攻撃者が使用する高度な手法として、米国のサイバーセキュリティに関する主要な連邦機関の一つである CISA (Cybersecurity and Infrastructure Security Agency)からも注意喚起が行われ、国際的にも広く認知されている攻撃手法です。2023 年以降、日本の組織を標的にした攻撃活動が確認されており、JPCERT/CC だけでなく、NISC(内閣サイバーセキュリティセンター)も注意を呼びかけています(*2)。

出典:JPCERT/CC『Operation Blotless 攻撃キャンペーンに関する注意喚起』(*1)

出典:NISC『Living Off The Land 戦術等を含む最近のサイバー攻撃に関する注意喚起』(*2)

LOTL 戦術は検知されにくい

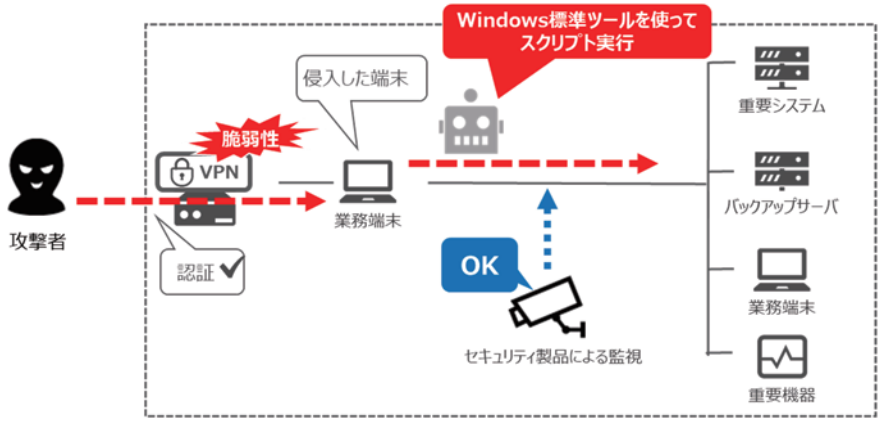
LOTL 戦術の特徴は、マルウェアを使用せずに、正規ツールを駆使してサイバー攻撃を行うことです。商用ツールやオープンソースのツールなど、組織内にあっても不審ではないツールや、OS などの侵入した環境に必ずある機能を操作することで、セキュリティ製品やログの監視・調査を回避します。

特に、近年のランサムウェア攻撃では、Microsoft の PowerShell が頻繁に悪用されているといわれて

(*1) JPCERT/CC『Operation Blotless 攻撃キャンペーンに関する注意喚起』

(*2) NISC『Living Off The Land 戦術等を含む最近のサイバー攻撃に関する注意喚起』

います。PowerShell は、通常の Windows に搭載されているスクリプト言語と実行環境です。攻撃者は、セキュリティ製品による検知を回避するため、マルウェアを送り込むことなく、不正なスクリプトを入力して PowerShell を利用し、別のマルウェアをダウンロードするなどの不正な行動を促します。



出典：大和総研作成

環境寄生型（LOTL：Living Off The Land）戦術

Volt Typhoon の攻撃活動との関連

JPCERT/CC は、この注意喚起において、特定の国の組織的なサイバー攻撃グループ「Volt Typhoon」による同様の攻撃を例にあげ、具体的な対策の提案をしています。Volt Typhoon は、2021 年頃から活動が確認され、2023 年 5 月に Microsoft がその活動を指摘したことで注目を浴びました。ただし、現時点では Operation Blotless が Volt Typhoon による攻撃活動だけであるかどうかは確定していません。Volt Typhoon は、先述の LOTL 戦術を徹底しているため、攻撃の痕跡がほとんど残らず、また、1 回の侵害期間が短く、侵害範囲も限定的であるため、被害現場にはほとんど証拠が残らないといわれています。これらの点が共通していると考えられています。

将来の攻撃に備えるには

Volt Typhoon は、初期侵入経路として SSL-VPN 製品の脆弱性を悪用した攻撃を頻繁に行っています。脆弱性対策は非常に重要であり、インフラ面では、インターネットからアクセス可能な IT 資産を特定し、それらのリスク（脆弱性など）を継続的に検出・評価する ASM（Attack Surface Management）ツールの使用が考えられます。JPCERT/CC も本注意喚起の文面において ASM の利用を推奨しています。なお、本冊子 P.17 では ASM の動向について詳しく紹介しています。

また、アプリケーション面では OSS の脆弱性に慎重な対応が求められます。OSS はコスト効率が高く、柔軟性に優れるため、多くの企業や組織が利用しています。しかし、コードの品質やセキュリティの脆弱性が見落とされる可能性があるため、攻撃者が脆弱性を見つけ出しやすいという点に留意が必要です。これには、SBOM（SCA）ツール(*1)を活用することで、ソフトウェア構成要素を把握し、脆弱性のリスクを継続的に低減することが期待されます。

これらのツールを活用して脆弱性を可視化し、基本的なパッチの適用を行うことが、攻撃を防ぐための重要な対策となります。セキュリティ意識を高め、適切な対策を講じることで、企業や組織の情報資産を守ることができます。安全な環境を維持するために、脆弱性対策の重要性を常に意識することが必要です。

（蓮見　将生）

(*1) 大和総研『サプライチェーンリスクマネジメントを支援する SBOM とは？背景や導入の注意点を解説』
SBOM（ソフトウェア部品表）を作成、共有、活用、管理することができるツールのこと。SBOM 管理ツール、OSS 管理ツール、ソフトウェア構成解析（SCA）ツールなどとも呼ばれる。

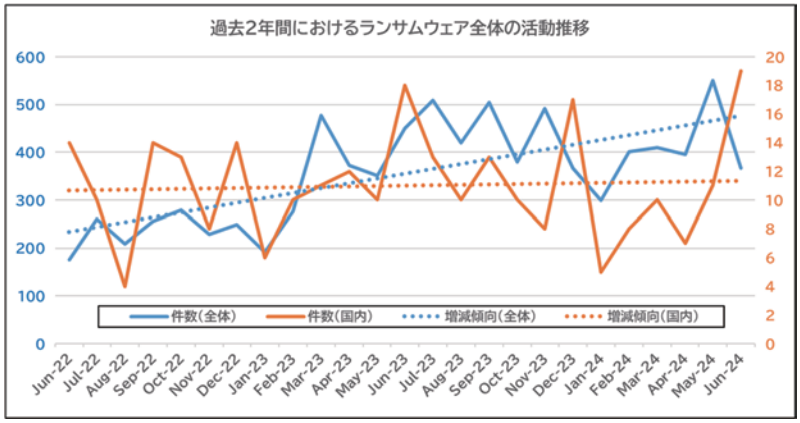
1. 拡大するランサム攻撃による被害：平時の対策と有事の対応方法

要約

- ランサム攻撃の被害が話題になっている。ランサム攻撃の被害に遭った場合、経済的な損失や評判の毀損など企業に多大な被害をもたらす。
- 攻撃者から要求される身代金については、法規制や復旧する保証がないことなどから、原則支払うべきではない。
- アップデートやバックアップなどの平時の対策に加えて、万が一発生した際にどのように対応するのか有事の対応方法について検討しておくことが重要。

ランサム攻撃による被害状況

ランサムウェアを代表とするサイバー攻撃を行い、身代金を要求するランサム攻撃による被害が大きな話題になっています。直近 2 年間のランサム攻撃の被害の件数としてダークウェブ上のリークサイトに掲載された企業数を調査したところ、右肩上がりで増加しているとするレポートもあります(*1)。また、情報処理推進機構(IPA)が公表している情報セキュリティの 10 大脅威(*2)においても、ランサム攻撃は 2021 年から 2024 年の 4 年間にわたり、組織に対する最大の脅威として位置付けられています。



出典：暴露型ランサムウェア攻撃統計 CIG マンスリーレポート 2024 年 7 月号（三井物産セキュアディレクション株式会社）(*1)を元に大和総研作成

ランサム攻撃を行う攻撃者の恐喝手法は、ランサムウェアによるデータの暗号化に加えて、窃取したデータをダークウェブ上のリークサイト上で公開すると脅す二重恐喝や、被害を受けた企業だけでなく、窃取した情報に含まれる個人や企業をさらに恐喝する三重恐喝など、多様化しています。

			
種別	(従来型)ランサムウェア	二重恐喝型ランサムウェア	三重恐喝型ランサムウェア
特徴	データの暗号化を行い、復号する代わりに身代金を支払うように要求する。	(従来型に加え、)身代金を支払わなければダウンロードしたデータを公開すると恐喝する。	(二重恐喝型に加え、)ダウンロードしたデータに含まれる個人・企業に対し、攻撃被害企業が身代金を支払わなければあなたのデータが公開されると間接的に恐喝する。

出典：大和総研作成 アイコンとして(*3)を使用

(*1) 暴露型ランサムウェア攻撃統計 CIG マンスリーレポート 2024 年 7 月号（三井物産セキュアディレクション株式会社）

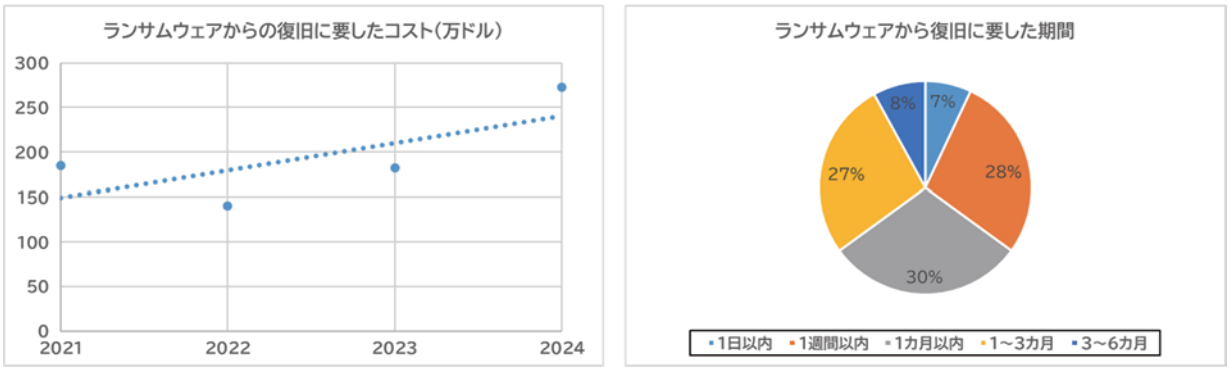
(*2) 情報セキュリティ 10 大脅威 2024（情報処理推進機構）

(*3) Dark web icons created by Freepik – Flaticon、https://www.flaticon.com/free-icons/speak

最近日本で発生したランサム攻撃による大きなインシデントとして、KADOKAWA とイセトーの事例があげられます。KADOKAWA は主に出版や動画サイトなどの B2C 事業を展開している企業で、ランサム攻撃による被害についてニュース記事や SNS で大きく報道されました。プレスリリース(*1)によれば、流出したデータには従業員情報だけでなく、KADOKAWA が運営する学校事業に関わる生徒の個人情報や、グループ会社の株式会社ドワンゴの取引先クリエイターの情報など、機微な情報も含まれていたとされています。一方、イセトーは B2B 事業を展開しており、情報処理業務を委託されている複数の自治体や銀行などの顧客の個人情報に関わるデータが流出したとされています(*2)。ランサム攻撃の被害発生当初は報道で多く取り上げられてはいませんでしたが、業務上の不備で個人情報が委託後も実際は削除されていなかったなど、被害状況が明らかになるにつれて、大きなニュースとして扱われるようになりました。

海外の大きなインシデント事例としては、米国の大手通信キャリアの AT&T の事例があげられます。AT&T は 2024 年の 4 月にランサム攻撃の被害を受け、同社のほぼ全ての顧客である約 1 億 1,000 万人ものアメリカ人の通信記録が窃取されました(*3)。攻撃者は当初、AT&T に対して流出したデータの削除のために 100 万ドル(約 1.5 億円)を要求しましたが、交渉の末、約 37 万ドル(約 5,600 万円)の支払いを行い、データの削除とデータを削除したことを示す動画を受け取ったとされています。なお、このインシデントの原因についてはセキュリティが不十分な SaaS サービスからのデータ流出とされています。企業の内部ネットワークには侵入されておらず、データの暗号化などランサムウェアは使用されていません。警察庁では今回のケースのようなランサムウェアを使用せずに、「窃取した情報を公開する」と恐喝するランサム攻撃をノーウェアランサム攻撃と呼んでおり、ランサム攻撃の多様化が進んでいる事例といえます。

これらの事例からも明らかなとおり、ランサム攻撃は経済的損害(ビジネス機会の喪失、復旧費用、身代金要求)、評判の毀損、時と場合によっては訴訟リスクをともなうこともあります。2024 年にランサム攻撃の被害を受けた企業の復旧には多くの場合、1 週間から 3 カ月の期間がかかり、平均の復旧費用は 273 万ドル(約 4.1 億円)にも及んでいるといったレポート(*4)もあります。身代金要求の観点については、次のセクションで詳しく取り上げます。



出典：ランサムウェアの現状 2024 年版 (Sophos)(*4)を元に大和総研作成

(*1) ランサムウェア攻撃による情報漏洩に関するお知らせ (株式会社 KADOKAWA)

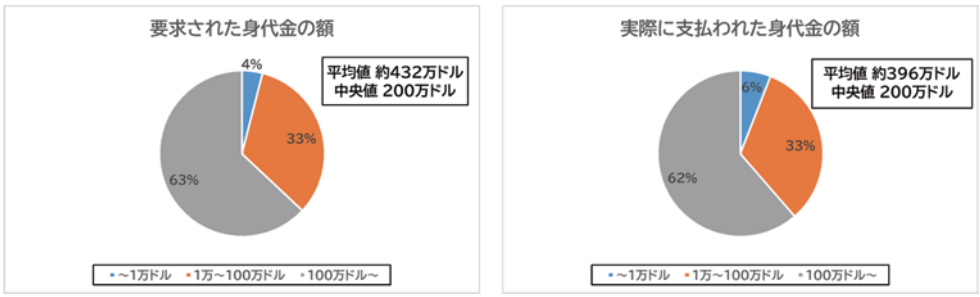
(*2) 「イセトー」にサイバー攻撃 委託元の約 150 万件の情報漏えいか (NHK)

(*3) AT&T Paid a Hacker $370,000 to Delete Stolen Phone Records (WIRED)

(*4) ランサムウェアの現状 2024 年版 (Sophos)

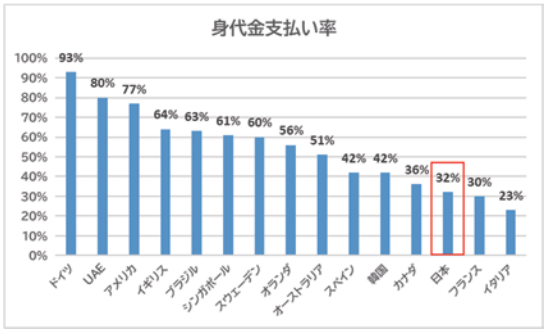
身代金要求の実態と対応

攻撃者からの身代金要求の実態は、世界的に見てかなり深刻です。前述のレポートでは、攻撃者から要求される金額の約 63%が 100 万ドル(約 1.5 億円)を超えており、その平均値は約 432 万ドル(約 6.5 億円)でした。実際に支払われた身代金の金額としては、中央値が 200 万ドル(約 3 億円)、平均値が約 396 万ドル(約 5.9 億円)となっています。企業が自社資産を用いて身代金を支払ったケースが最も多いものの、ランサム攻撃を含んだサイバー攻撃の被害を補償するサイバー保険も多く利用されていることが示されています。



出典：ランサムウェアの現状 2024 年版 (Sophos)を元に大和総研作成

一方で身代金支払い率の世界平均が 54%であるのに対し、日本の身代金支払率は 32%と低い水準となっているという調査(*1)もあります。これは、被害に備えたバックアップが取られていることや反社会的勢力に資金供与しない慣習もありますが、言語の壁で交渉が難しいことや、日本のサイバー保険の補償範囲に身代金支払いが含まれておらず資産調達ができないこと、また、身代金を支払ったとしても支払ったことを公表しない企業が多いことも理由として考えられます。



出典：ランサムウェア感染率/身代金支払率 15 カ国調査 2024(proofpoint)(*1)を元に大和総研作成

身代金の支払いに際しては、日本の外為法規制や米国の OFAC(Office of Foreign Assets Control)規制について把握しておく必要があります。外為法規制は、2001 年にアメリカで発生した同時多発テロを受けて、国際的にテロリストなどの犯罪者に資金供与を行わないようにするために強化されました。日本政府は、経済制裁を行っている対象者に対して政府の許可なく送金することを違法としています。現時点では、北朝鮮系のサイバー犯罪グループとして知られている“Lazarus Group”が経済制裁の対象として指定されています(*2)。米国の OFAC 規制は、特定の国や個人、団体に対する資金提供や取引を禁止する経済制裁を実施しており、経済制裁の対象には“Conti”や“TrickBot”と呼ばれるサイバー犯罪グループも含まれています(*3)。OFAC の規制は、米国内に居住する個人や企業だけでなく、米国の金融システムを利用する全ての取引にも適用され、これには、外国の金融機関が米ドルを使用する取引も含まれます。

攻撃者は通常、取引において身元を明かさないため、身代金を支払うことは外為法や OFAC の規制に抵触する可能性があります。また、身代金を支払ってもデータが復旧する保証がないことや、身代金を支払った企業だと知れ渡ることで別の攻撃者からも狙われる可能性もあるため、通常は身代金を支払うべきではありません。しかし、現実問題として、被害の状況によっては身代金の支払いが問題解決の手段の一つとなる場合があります。万が一、身代金を支払う必要があるかもしれないとなった場合でも、警察や弁護士などの専門家に相談を行うべきです。

(*1) ランサムウェア感染率/身代金支払率 15 カ国調査 2024 (proofpoint)

(*2) 経済制裁措置及び対象者リスト (財務省)

(*3) United States and United Kingdom Sanction Additional Members of the Russia-Based Trickbot Cybercrime Gang (Office of Terrorism and Financial Intelligence)

ランサム攻撃に対する平時の対策と有事の対応

これまで紹介したとおり、ランサム攻撃は多大な損害をもたらすため、平時からの予防策と有事の迅速な対応が求められます。本冊子でも取り上げている金融庁のガイドラインのように、各業界向けのガイドラインを確認することや、サイバーセキュリティに関する様々なフレームワークを取り入れるなど、網羅的な対策を継続的に行っていく必要があります。

ここでは、ランサム攻撃に対する平時における対策と有事の際の対応の観点としてそれぞれ記載しますので、ご参考にしていただければ幸いです。

平時の対策のポイント

対策箇所	対策観点
脆弱性対応	警察庁のレポート(*1)にあるとおり、ランサム攻撃の過半数が VPN 機器などの脆弱性が感染経路となっている。特にインターネットに接続している機器やサーバーの脆弱性については修正パッチ公開後、速やかに対応を行う必要がある。
有効なセキュリティ対策ソフトの導入	EDR や XDR などのランサムウェアの横展開を阻止するセキュリティ対策ソフトの導入が有効である。
有効なバックアップの実施	米国国土安全保障省配下の米国コンピュータ緊急事態対応チームが提唱するデータ保護の「3-2-1 ルール」など、定期的にバックアップを行いネットワークから切り離された形で保管するようにする。
適切なアクセス権限の設定と検知	最小権限の原則にのっとり、ユーザーに対して過剰な権限を設定しない。また、SaaS やクラウドのセキュリティ対策として、SSPM や CSPM を導入し、MFA の未設定や外部公開設定などのセキュリティ上のミスを検知する。
従業員への教育	ランサム攻撃の起点となるソーシャルエンジニアリングやフィッシングを防ぐために事例を交えた形で定期的にセキュリティ教育を行う。
ASM や脅威インテリジェンスの導入	インターネット上から不正にアクセスできる資産がないか確認するサービスを導入する。また、攻撃者がどういった手法でどのような企業をターゲットにしているか分析するサービスを導入する。 ※詳細は第3部で解説する。
インシデント対応計画の策定	有事に備え、従業員の対応や連絡フロー、感染後の復旧手順や身代金要求への対応方針などをまとめたインシデント対応計画の策定を行う。計画立案後はインシデント対応訓練などで有効性の検証を行うべきである。

有事の対応のポイント

対応箇所	対応観点
初動対応	横展開を防止するため、ランサムウェアが確認された端末・サーバーを隔離する。 ただし、フォレンジックのため、ランサムウェアを確認した端末のネットワーク抜線のみを行うか、電源自体を切るかについて事前に対応計画の中で検討しておくべきである。
被害状況の確認	ランサムウェアが確認された端末以外に被害がないか、ログなどから調査する。
関係者への報告	社内の関係者と社外の関係者(警察・IPA・JPCERT/CC・個人情報保護委員会・被害に遭った可能性がある企業など)に報告する。
復旧作業	隔離された端末・サーバー以外に被害がないことを確認した後に、バックアップから復旧を実施する。
フォレンジック	ランサムウェア攻撃についてどのように行われたのかログなどから調査を行う。
再発防止策の実施	フォレンジックの結果を元に、脆弱な箇所に対して対応を実施する。
情報の開示	自社ホームページやマスコミに対し、インシデントの内容について開示する。

（山崎　禎章）

(*1) 令和5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（警察庁）

1. 脅威インテリジェンス

要約

- 脅威インテリジェンスはセキュリティ対策の効率を高め、事前対応型の脅威検出にも有効。
- 脅威インテリジェンスを機能させるためには組織にセキュリティ運用の成熟が求められる。
- 有償の CTI サービスは、導入前に組織の運用に沿って求める情報が取得できることを確認する。

今日、脅威インテリジェンスというキーワードは広く認知されるようになりましたが、セキュリティの専門家を除けば、具体的にどのようなものであるかわからない、といった方も少なくないのではないでしょうか。

本記事では、脅威インテリジェンスが、組織のセキュリティに対してどのような効果をもたらすのか、また組織の中でどのように活用されるべきかを紹介します。

脅威インテリジェンスが注目される背景

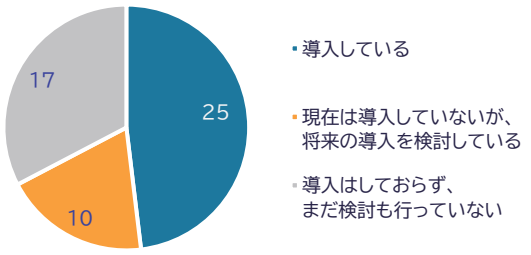
本冊子第 2 部でもご紹介したとおり、日本国内においてもランサム被害が拡大しています。

身代金被害額の高騰や多重恐喝などの悪質化は、攻撃者がより深く組織を侵害することに成功していることを表しています。標的型のサイバー攻撃では、攻撃者は時間をかけひそかに侵害を進め、その潜伏期間は平均して 277 日におよびます(*1)。ランサム被害を未然に防いだり軽減したりするためには、これまで見逃されがちであった潜伏・進行中の侵害を検出し、対処することが期待されます。

脅威インテリジェンスは、攻撃者の動向やその戦術を深く理解することで、進行する侵害の検出を可能にする様々な情報を提供します。ISMS の最新版 ISO27001 においても、セキュリティ管理策の一つとして脅威インテリジェンスの活用が明記され、その有効性が認められています(*2)。

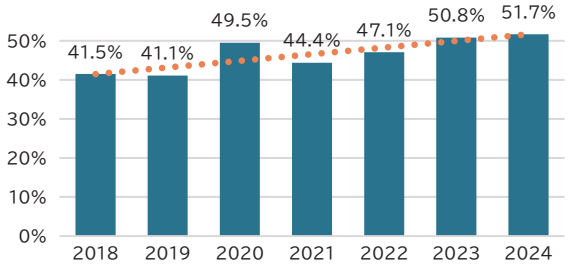
実際に、日本の重要インフラ事業者においても、約 7 割の企業で脅威インテリジェンスを導入済み、または導入を検討しているという調査結果が示され、国内企業においても関心の高さがうかがえます(*3)。

また、米国においては脅威インテリジェンスの専任部隊を構成する企業が年々増加しており、企業として積極的に脅威インテリジェンスを活用する流れが進んでいるようです(*4)。



国内企業における脅威インテリジェンスの導入状況

出典:IPA『脅威インテリジェンス導入・運用ガイドライン』を元に大和総研作成(*3)



脅威インテリジェンスに専任者を構成する企業

出典:SANS『2024 CTI Survey: Managing the Evolving Threat Landscape』を元に大和総研作成(*4)

(*1) IBM データ侵害のコストに関する調査 2023 年

(*2) ISO/IEC27001:2022 および ISO/IEC27002:2022 情報セキュリティ管理策の実践のための規範

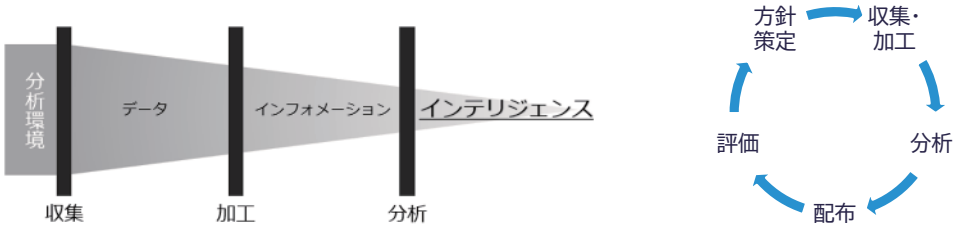
(*3) IPA 中核人材育成プログラム「脅威インテリジェンス導入・運用ガイドライン」

(*4) SANS 2024 CTI Survey: Managing the Evolving Threat Landscape

脅威インテリジェンスとは

サイバー脅威インテリジェンス（CTI: Cyber Threat Intelligence）とも呼ばれ、軍事や国防に端を発する概念で、組織や企業に対するサイバーセキュリティ上の脅威情報を収集・分析し、その結果をセキュリティ対策の意思決定に活用していく取り組みや、この分析を行う組織を指す言葉として用いられます。

また、脅威に対する意思決定をサポートする分析結果のことを「インテリジェンス」と呼ぶため、この情報自体を指して用いることも少なくありません。



インテリジェンスの生成過程とライフサイクル

出典:『脅威インテリジェンス導入・運用ガイドライン』を元に大和総研作成

脅威インテリジェンスの活用は、図に示すように次の 5 段階のライフサイクルで表され、継続して組織におけるセキュリティ対策の意思決定をサポートします。

方針策定	組織課題に応じたインテリジェンスの目的と要件を明確にし、求めるインテリジェンスに必要なデータの収集方針を定めます
収集・加工	方針に従い「データ」を収集し、集めたデータを分析しやすいよう、背景情報を付与した「インフォメーション」へ加工します
分析	要件に従って「インフォメーション」を分析し、組織の意思決定に必要なコンテキストを付加した「インテリジェンス」を作成します
配布	作成した「インテリジェンス」を経営層やセキュリティ部門、SOC 担当者などそれぞれの利用者の目線で必要とする粒度となるように編纂し、適切なタイミングで利用者へ届けます
評価	定期的に脅威インテリジェンスプロセス全体を評価し、ライフサイクルの改善を検討します

出典:『脅威インテリジェンス導入・運用ガイドライン』を元に大和総研作成

ライフサイクル全ての段階を自組織内のリソースで完結することは、多くの組織において容易なことではありません。特にフルタイムのリソースが求められる収集・加工段階や専門知識が必要となる分析段階については、オープンソースの CTI ツールやコミュニティを活用するほか、セキュリティ専門ベンダーの提供する脅威インテリジェンスサービスの導入も有用です。

また、脅威インテリジェンスは活用形態により大きく三つのカテゴリーに分類され、それぞれ提供先や成果物（インテリジェンス）の形式が異なります。

それぞれのインテリジェンスを組織の意思決定に活用するためには、提供先となる組織やその役席者、経営層メンバーが、セキュリティ的に成熟していることが求められます。

戦術的インテリジェンス	即時活用	インシデントの予防・進行中のサイバー攻撃の検知や対応に活用するため、セキュリティ運用部門へ IoC(*1)などを提供する
運用インテリジェンス	短期 ～中期的	組織が将来の攻撃を予測して防止策を検討するため、セキュリティ責任者、SIRT 部門などへ自組織への攻撃シナリオなどを提供する
戦略的インテリジェンス	中長期的	セキュリティ投資判断や意思決定を支援するため、CEO やその他の経営幹部、セキュリティ責任者などへレポートを提供する

出典:『脅威インテリジェンス導入・運用ガイドライン』を元に大和総研作成

(*1) IoC: Indicator of Compromise（侵害の指標。サイバー攻撃に用いられる IP アドレスやドメイン名、ファイルハッシュ値など）

脅威インテリジェンスの活用例

脅威ベースアプローチを併用したセキュリティ施策の最適化
従来のコンプライアンスベースのセキュリティ対応策は、抜けなく対策できる反面、保有資産が増大する状況に対しては、人的・金銭的リソースとのトレードオフが生じています。これに対し、運用インテリジェンスを用い脅威ベースのアプローチを併用することで、優先対応すべき資産や施策を絞り込むことが可能となります。これにより、限られたリソースに対して最大限の効果を得られる対策が実施できるでしょう。

アクティブ・サイバー・ディフェンス(*1)への活用
新たな脅威情報が連携された際、運用インテリジェンスとして、追加で対応すべき資産や施策を提案できたり、戦術的インテリジェンスとして遮断すべき IP アドレスやドメインなどの IoC 情報を提供したりすることで、新たな脅威による攻撃を未然に緩和することも期待されます。

脅威ハンティング(*2)と脅威インテリジェンスの相乗効果
脅威ハンティングは、既存のセキュリティソリューションを回避して組織のネットワークに潜伏するような、高度なサイバー攻撃や、潜在的な脅威を能動的に見つけ出し、隔離していくセキュリティプロセスです。最新の脅威ハンティングは、サイバーセキュリティツールと脅威インテリジェンスを連携させ、システム全体から収集した情報を自動化したプロセスで分析し、セキュリティエンジニアの洞察を支援します。また、戦術的インテリジェンスの提供する IoC 情報や、運用インテリジェンスが提供する攻撃シナリオは、調査対象を効果的に絞り込み、脅威を迅速に特定するために脅威ハンターにとっても欠かせない情報となります。

脅威インテリジェンスサービス導入時の検討事項

セキュリティベンダーの提供する「脅威インテリジェンス（CTI）サービス」は、OSINT(*3)結果をセキュリティベンダーの目線で分析し、IoC や汎用的な脅威傾向の分析レポートを提供するものから、個別のインテリジェンス要件に従って組織にカスタマイズされた分析を行うものまで、様々なサービス形態が存在します。

それぞれのサービスは独自の情報ソースを構成していますが、その内容は秘密のレシピとなっています。

有償サービスは高価なものが少なくありません。導入を検討する際には、複数のサービスで試用を行い、次のような視点で導入にふさわしいものか見定めるようにするとよいでしょう。

- 戦略インテリジェンスのレポートは経営層が理解し、判断に有効な情報として提供されているか
- JPCERT/CC などから注意喚起される日本向けの攻撃者や IoC が抽出できているか
- レポートされた脅威は、他社の分析結果などとも突合評価し、十分に信頼できるものか
- 提供される UI の機能や親切さ、サポートチームのコミュニケーションは組織での運用とマッチするか

まとめ

サイバーセキュリティには完成形がありません。攻撃者やそれらの用いる攻撃手法が目まぐるしく変容する状況は、防御する組織に対しても進化を要求し続けます。組織は、経営層まで含めた全体で最新の脅威を意識し、備える必要があります。脅威インテリジェンスを導入し、活用のライフサイクルを構築することは、組織のセキュリティを継続的に強化し、標的型攻撃の被害を回避または軽減することが期待できます。

標的型攻撃は、企業の秘密や有能な人材の情報など、組織・企業にとって 3 年後、5 年後の利益や成功の種となるものを盗もうとします。組織・企業にとって脅威インテリジェンスは未来を守る管理策と考えることもできるのではないでしょうか。

（渋谷　篤）

(*1) JPCERT/CC「積極的サイバー防御」（アクティブ・サイバー・ディフェンス）とは何か
(*2) IBM 脅威ハンティングが重要な理由
(*3) OSINT: Open-Source Intelligence（一般に入手可能な公開情報を収集・分析するインテリジェンス手法）
（参考文献）「脅威インテリジェンスの教科書」／石川朝久［著］／技術評論社
（参考文献）IPA 中核人材育成プログラム「脅威インテリジェンス導入・運用ガイドライン」

2. ASM(Attack Surface Management)の動向について

要約

- 侵入前提の対策である EDR だけではなく、組織内部への侵入阻止を目的とした ASM が注目されている。
- 国内での導入はまだ進んでいないが、総務省のガイドラインなどの公表により今後の導入拡大が見込まれる。

背景と目的

デジタルトランスフォーメーションの進展により、クラウド利用の拡大やテレワークの増加などが一般的になった結果、サイバー攻撃の起点が増加しています。

本冊子の第 2 部でも紹介したように、ランサム攻撃により大きな被害が発生しています。これらのランサムウェアの原因として、警察庁の発表(*1)では、「国内で発生したランサムウェア被害の感染経路は、2022 年と 2023 年上半期のいずれも、80%以上が管理不十分な外部公開資産(VPN 機器やリモートデスクトップ)」とされています。

悪意ある攻撃者の入り口となりうる外部に公開された資産を漏れなく管理し、タイムリーなパッチ適用などの適切な管理・運用を行うことは容易ではありません。

このような環境変化に対応するため、外部から把握できる情報を用いて、IT 資産の適切な管理を可能にするソリューションとして、ASM(Attack Surface Management)が注目されています。

経済産業省のガイダンス紹介

2023 年 5 月、『ASM(Attack Surface Management)導入ガイダンス～外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～』(*2)が公表されました。本ガイダンスでは ASM の特徴を以下のように紹介しています。

- 情報システムを管理している部門が把握していない IT 資産を発見できること。
- 情報システムを管理している部門の想定と異なり、公開状態となっている IT 資産を発見できること。

ASM は、「組織の外部(インターネット)からアクセス可能な IT 資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセス」(ガイダンスの定義)となりますが、具体的な手法としては次のようなものがあります。

(*1) 出典:警察庁ウェブサイト　令和4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
出典:警察庁ウェブサイト　令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について

(*2)https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

① 自動的なアセット特定:
ツールを活用することで、自社や関連企業のアタックサーフェスを自動的かつ継続的に特定。未把握の機器や意図しない設定ミスを攻撃者視点から発見でき、リスク低減に寄与

② 脆弱性スキャン:
アセットに対して定期的な脆弱性スキャンを実施、脆弱性情報を収集し、適切な対応策を検討

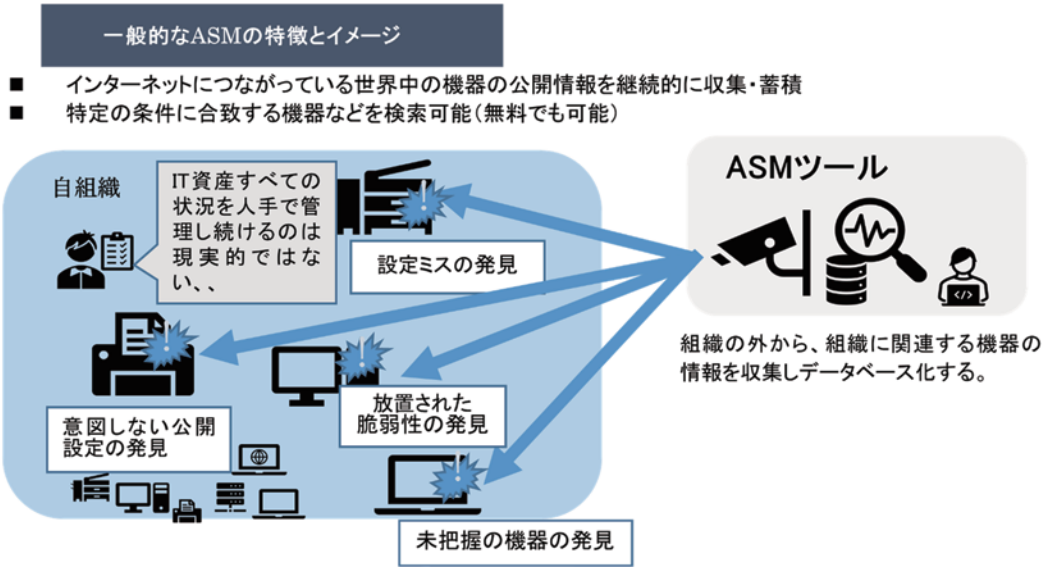
③ 設定の評価:
アセットの設定を評価し、セキュリティベストプラクティスに準拠しているかどうかを確認

④ 攻撃シナリオのモデリング:
アセットを攻撃者視点で分析し、潜在的な攻撃シナリオをモデリング

⑤ リスク評価と優先順位付け:
検出されたリスクを評価し、優先順位を付けて対応

ASM は自社のセキュリティ向上のために有効なソリューションではありますが、導入するツールの選択時には事前検証などの実施により、自社に適したツールの見極めも重要です。主に発生する課題は以下のとおりです。

- 自社と関係のない IT 資産(ノイズ)に関する通知の精査
- 収集された情報の発見理由や根拠の説明不足
- 対応すべき箇所を優先順位付けるための判断指標の追加



出典: ASM(Attack Surface Management)導入ガイダンス(経済産業省)

ASM を取り巻く国内の状況

国内の普及度に関する具体的な統計データは限られているが、トレンドマイクロ社が調査した「法人組織のアタックサーフェスに関するセキュリティ意識調査」(*1)によると、「アタックサーフェス（攻撃対象領域）が多様化することに懸念がある法人組織は 7 割以上」で「安全性に盲点があると答えた日本組織は約半数」というものでした。

一般的なセキュリティ対策への意識は高まっているようですが、ASM の普及が進んでいる、特に欧米諸国の企業や組織と比較すると、国内においては一部の大企業や金融機関、政府機関などでの利活用が始まったばかりで、中小企業や一般的な組織においてはまだまだ導入が進んでいないようです。それには他のセキュリティ対策と同様、以下のような原因が想定されます。

- 日本の一般的な企業や組織において、ASM の重要性やメリットに対する認識がまだ不十分
- 十分なスキルと経験を持った専門家の不足
- 組織全体でセキュリティ意識を高め、ASM を継続的に実施する文化の醸成がまだ不十分

最後に

ASM 製品の多くは、グラフを利用したアセットの状況の可視化ができ、リスクに対するアラートの通知などを 24 時間 365 日体制で監視する SOC（Security Operation Center）のスピーディーなインシデント対応の助けになります。

EDR（Endpoint Detection and Response）のような侵入されたことを前提とした事後的な対応だけではなく、そもそも侵入されないことを目的とする予防的な対応に位置する ASM の重要性は、今後ますます高まっていくものと考えられます。

（水谷　浩樹）

(*1)https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220629-01.html

3. 脆弱性管理について

要約

- 脆弱性管理とは、システムで稼働するソフトウェアの脆弱性を特定し、修正など必要な対策を講じるプロセスのことで、昨今のランサム攻撃の台頭などにより重要性が増している。
- 脆弱性管理に用いられる指標・フレームワークである「CVSS」「KEV」「EPSS」「SSVC」の概要とそれぞれの有用性・課題について、および脆弱性管理の今後について解説する。

脆弱性管理とは

脆弱性管理は、システムで稼働するソフトウェアの脆弱性を特定し、アプリケーションの修正やパッチの適用などの必要な対策を講じる一連のプロセスのことです。脆弱性管理は、セキュリティリスクを低減し、システムやデータの安全性を確保するため、継続的に実施する必要がある重要な活動です。

脆弱性管理は、一般的に以下の表のようなプロセスで実施されます。

項番	プロセス	プロセス概要
1	情報収集・発見	最新の脆弱性情報を幅広く収集する。収集においては、ベンダーサイト、セキュリティ情報サイトからの情報に加え、JPCERT/CC、IPA、米国 CISA（Cybersecurity and Infrastructure Security Agency：サイバーセキュリティ・インフラセキュリティ庁）などからの注意喚起情報にもアンテナを張る必要がある。
2	分類・評価	収集した脆弱性情報について、自組織に関係するものであるか、分類・評価する。
3	方針決定	分類・評価された脆弱性について、トリアージ(*1)を行い、脆弱性対応の方針・スケジュールを決定する。脆弱性対応のリソースは限られることから、全ての脆弱性に対して一律に対応することは現実的ではない。リスク受容を含めた実効性のある対応を効率的に行うためにトリアージが重要となる。
4	適用	決定した方針に従い、「修復（アップデート）、軽減（緩和策実施）、リスク受容」の対応を実施する。

出典：大和総研作成

脆弱性管理においては、上記のプロセスに加え、システムの定期的な監視と評価が必要です。加えて、システムやソフトウェアの変更、新たな脆弱性の出現に備えて、定期的な脆弱性スキャンやペネトレーションテストを行うことも推奨されます。昨今では、効率的なセキュリティ対策・脆弱性管理を推進するために、インターネットからアクセス可能な IT 資産を調査・管理する ASM と呼ばれるキーワードが注目されています。ASM については、本冊子の第 3 部-2.「ASM（Attack Surface Management）の動向について」で詳しく紹介していますので、ご参照ください。

なお、脆弱性管理に先立ち、システムで稼働しているソフトウェアを特定・可視化し把握する必要があります。把握していないソフトウェアの脆弱性に対処することは、当然ながら困難となります。もし、ソフトウェアの把握が困難である場合は、セキュリティベンダーによる脆弱性診断の受診やツールの使用などが推奨されます。脆弱性管理は、セキュリティを継続的に向上させるために欠かせないプロセスです。脆弱性管理の運用には専門的な知識と経験が必要ですが、適切に実施することでセキュリティリスクを最小限に抑え、システムやデータの安全性を確保することが可能となります。

(*1) トリアージ（triage）：一般的には、災害発生時などにおいて傷病者の緊急度や重症度に応じて治療優先順位を決めることです。サイバーセキュリティ対策においては、当該脆弱性に対して重要性や緊急度を見極め対応の優先順位を決定する意味合いで使用されます。

脆弱性管理の重要性が増した背景

従来ソフトウェアの脆弱性対応は、たとえば後述の CVSS スコアが「7.0 以上の脆弱性について全て対応する」といった運用が主流でした。しかし、近年 CVSS の対象となる脆弱性が急増し、報告された脆弱性全てに対応するのは人的リソースの不足などにより困難になりました。加えて、記憶に新しい 2021 年の Apache Log4j の脆弱性を悪用する攻撃や、ランサム攻撃の台頭などで、脆弱性対応の緊急性も増しており、迅速かつ効率的な対処が必要になりました。このような状況では、「CVSS スコア 7.0 以上の脆弱性は全て対応する」といった単純な視点だけでなく、たとえば PoC コード(*1)の存在や、悪用の状況、システムの設置状況などの新たな視点を考慮した上で、総合的に脆弱性管理を行う必要があります。

脆弱性管理に用いられる代表的な指標・フレームワークについて（CVSS、KEV、EPSS、SSVC）

脆弱性管理の指標としては、「CVSS」の活用が一般的ですが、「CVSS」と併せてここ数年注目されている指標である「KEV」「EPSS」と、昨今注目の脆弱性管理フレームワークである「SSVC」を紹介します。

CVSS （Common Vulnerability Scoring System：共通脆弱性評価システム）

脆弱性管理において広く活用されている指標で、脆弱性の深刻度を数値化し、それに基づいて対策や優先付けを行うために使用される、国際的な指標です。CVSS は、脆弱性の影響度、攻撃の容易さ、攻撃の範囲などの要素を考慮して、ベンダーに依存しない中立的な基準でスコアを算出します。スコアは 0～10.0 の範囲で数値化され、高いスコアほど脆弱性の深刻度が高いことを示し、客観的に評価することが可能です。CVSS はセキュリティ専門家や組織にとって重要な指標であり、セキュリティの脆弱性を効果的に管理するために活用されています。なお、CVSS については、『DIR SOC Quarterly vol.7 2024 spring(*2)』で詳しく取り上げています。

KEV （Known Exploited Vulnerabilities Catalog）

米国 CISA が公開している、実際に攻撃に悪用された脆弱性のリスト(*3)です。KEV に登録されるには、「(1)CVE ID が割り当てられていること」、「(2)悪用されている証拠があること」、「(3)ベンダーが提供するパッチやアップデートなど、脆弱性に対する明確な修復アクションがあること」の三つの条件を満たす必要があります。KEV に登録された脆弱性については、リスクが非常に高く速やかに対策を講じる必要があります。

EPSS （Exploit Prediction Scoring System）

FIRST(Forum of Incident Response and Security Teams)が開発した、脆弱性対応の優先度を判断するための指標(*4)です。EPSS は、EPSS Probability(EPSS スコア)と、EPSS Percentile(EPSS パーセンタイル)の二つで構成されます。EPSS スコアは、今後 30 日以内に脆弱性が悪用される可能性を独自の機械学習モデルに基づき 0～1(0～100%)のスコアで算出します。EPSS パーセンタイルは、当該脆弱性の EPSS スコア全体におけるランクを表します。たとえば EPSS パーセンタイルが 0.90 の脆弱性は、当該脆弱性より EPSS スコアが低い脆弱性が 90%存在することを表します。EPSS スコアは、「脆弱性の天気予報」に近いイメージです。CVSS が脆弱性そのものの深刻度を評価するのに対して、EPSS は脆弱性が悪用される可能性を算出する点が異なります。

(*1) Proof of Concept(概念実証)コード：脆弱性の存在や悪用可能性を証明するための実証コードのことです。

(*2) CVSS の歴史と最新版(v4.0)での改善点（『DIR SOC Quarterly vol.7 2024 spring』 pp.17-20）

(*3) CISA『Known Exploited Vulnerabilities Catalog』

(*4) FIRST『Exploit Prediction Scoring System』

SSVC　(Stakeholder-Specific Vulnerability Categorization)

米国カーネギーメロン大学ソフトウェア工学研究所と米国 CISA と共同で作成された脆弱性管理フレームワーク(*1)です。脆弱性の有する技術的な深刻度だけでなく、どのように対策するかを決定することが可能となります。SSVC では、文字通りステークホルダー(サプライヤー、デプロイヤー、コーディネーター)ごとに決定木を用いて、「Exploitation(脆弱性の悪用状況)」、「Exposure(システムの露出度)」、「Utility(悪用の有用性)」、「Human Impact(攻撃によるインパクト)」を基に、脆弱性へのアクションを、「Immediate(即時対応)」、「Out-of-Cycle(通常よりも早く、緩和策・改善策を適用)」、「Scheduled(定例のメンテナンス時に対応)」、「Defer(現在は対応不要)」として決定します。SSVC は CVSS などの指標だけでは不足する点を補完するフレームワークであり、昨今は「脱 CVSS」に向けての一手法として注目されています。

各指標・フレームワークの有用性・課題

前述の各指標・フレームワークには、以下の表に示されるような有用性・課題があります。各指標の有用性と課題を理解した上で、複数の指標を併用して脆弱性管理を行うことが望ましいものと考えられます。

用語	有用性	課題
CVSS	・脆弱性の深刻度を定量的に評価できる。 ・ベンダーに依存しない中立的な評価基準である。	・脆弱性の理論上の深刻度を表現したものであり、悪用の状況などリアルタイムの脅威についての考慮が不十分である。
KEV	・実際に悪用された脆弱性のリストである。 ・米国の政府機関である CISA が公開したリストであり、米国政府機関では期日までに対応が求められるなど精度が高い。	・日本独自の製品などは掲載される期待が薄い。 ・掲載された脆弱性は、CVE ID が付与された脆弱性の 0.5%程度と少ない。
EPSS	・今後 30 日以内に脆弱性が悪用される蓋然性(確率)をスコア化しており、攻撃発生の予測が可能となる。 ・当該脆弱性における脅威情報の取得が困難な場合でも脅威を簡易的に評価できる。	・予測には機械学習などが用いられているが、モデルの詳細が開示されておらずスコアの説明が困難。また、現時点では精度が必ずしも高くない。 ・既存の攻撃手法を基に算出しており、未知の攻撃や新たな攻撃手法に対する予測は困難である。 ・EPSS を管理する FIRST が米国中心のフォーラムである性質上、日本独自の製品などは脅威情報の不足によりスコアが低く出る傾向がある。
SSVC	・脆弱性に対してどのように対応すべきかの対応方針を決定できる。 ・ステークホルダーごとに対応方針を決定できる。	・決定木のパラメーターや評価基準が組織やシステム環境により異なるため、各関係者と十分な意思共有を図る必要があるなど運用開始までのハードルが高い。

出典:大和総研作成

脆弱性管理の今後について

システムの脆弱性については、昨今のゼロトラストセキュリティモデルやマイクロセグメンテーションなどの推進により、機器個別のアクセス制御が強化され、当該システムへの攻撃自体が抑制される方向に進んでいます。これに加え、AI の活用などにより、脆弱性の検出と対応についても自動化が進むものと想定されます。現時点でも SOAR(*2)と呼ばれるソリューションの中で一部の対応について自動化が実現されています。

脆弱性情報が増えるとシステム部門の対応負荷が上がるため、自動化などにより負荷を下げる必要があります。そのためにも適切な指標を活用し、自組織のシステムの状態(インターネット接続の有無、動作権限、攻撃緩和策の有無など)を踏まえた適切な脅威評価とトリアージを行い、必要な対策を速やかに実施することが今後ますます重要になるものと考えられます。

(土田　将弘)

(*1) CISA『Stakeholder-Specific Vulnerability Categorization (SSVC)』

(*2) Security Orchestration, Automation and Response:「脅威と脆弱性の管理」、「セキュリティインシデント対応」、「セキュリティ運用の自動化」の三つの主要なソフトウェア機能を実現する製品・サービスのことです。

4. 国内におけるランサムウェアを巡る情勢と政策動向

要約

- 国内におけるランサムウェアの被害件数は高止まりの状況であり、攻撃の手口も進化している。
- 重要インフラ事業者がランサムウェアの被害に遭うことで、国民生活や社会経済活動に多大な影響が及ぶ事案も発生しているため、政府も重要インフラ事業者に対するサイバーセキュリティ対策の強化に取り組んでいる。

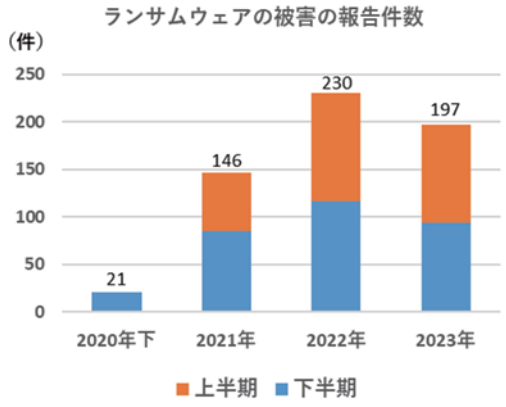
はじめに

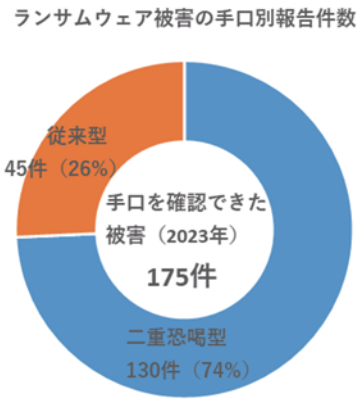
ランサムウェアは長年にわたりセキュリティ上の深刻な脅威として認識されており、情報処理推進機構（IPA）の「情報セキュリティ 10 大脅威」でも、組織向けの脅威において 4 年連続で 1 位にランクインしています。第 2 部のインシデント事例でも取り上げたように、今年に入ってからも国内で多数の組織が被害に遭っていることが確認されており、その脅威は収まる気配がみられません。近年、特に重要インフラ事業者などの社会インフラを支える組織がランサムウェアの被害に遭うことでシステムが機能不全に陥り、国民生活に多大な影響を及ぼす事例が相次いでいることから、各組織が自主的な対策を行うだけでなく、政府も国内におけるサイバーセキュリティの対策強化を図るべく、様々な取り組みを行っています。

そこで本記事では、国内で発生したランサムウェアによる被害の現状や過去の重大な被害事例について取り上げるとともに、政府のランサムウェアに関連する施策を紹介します。

ランサムウェア被害の現状

警察庁が公表した『令和5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』(*1)によると、2023 年における国内のランサムウェア被害の報告件数は 197 件となっており、過去最高を記録した 2022 年の 230 件からはやや減少したものの、依然として高止まりの状況が続いています。また、攻撃の手口として、従来は暗号化したデータを復号する代わりに身代金を要求していたところ、現在はデータを窃取した上で被害組織に対して「身代金を支払わなければ、データを公開する」と脅迫する二重恐喝（ダブルエクストーション）が主流となっています。ランサムウェアの被害が後を絶たない原因として、このような攻撃の手口の進化によって、被害組織は身代金の支払いを拒否することがますます困難になり、攻撃者にとって都合の良いビジネスとして成り立っていることがあげられます。





出典：『令和5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』(*1)を基に大和総研作成

(*1) 警察庁『令和5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』

このようにランサムウェアによるサイバー攻撃が猛威を振るう中、過去には下表のような重要インフラ事業者などの社会インフラを支える組織が標的となり、システムが停止する事案も発生しています。これらの事案では国民生活や社会経済活動に多大な影響が及んだことから、当時は報道機関でも頻繁に取り上げられ、広く世間の注目を集めました。

発生年月	対象	事案概要
2021 年 10 月	徳島県つるぎ町立半田病院	院内のシステムがランサムウェアに感染したことで、電子カルテが暗号化され閲覧不可になったほか、電子カルテのデータを参照する会計システムなども連鎖的に使用不能になり、新規患者の受け入れを停止するなど、業務が大幅に制限された。 復旧には約 2 か月を要した。
2022 年 10 月	大阪急性期・総合医療センター	調理を委託していた給食事業者のシステムを経由して、医療センターのシステムがランサムウェアに感染し、電子カルテなどが暗号化された。これにより、同センターでは新規患者の受け入れの停止や、緊急性が低い入院患者の自宅退院、周辺病院への転院を進めるなどの対応が必要となった。 復旧には約 2 か月を要した。
2023 年 7 月	名古屋港	総取り扱い貨物量日本一である名古屋港のコンテナターミナルを管理する中央システム「名古屋港統一ターミナルシステム（NUTS：Nagoya United Terminal System）」がランサムウェア感染により停止し、トレーラーを使用するターミナルでのコンテナの搬出入作業が全て中止された。 復旧には約 2 日半を要した。

出典：大和総研作成

ランサムウェアに関連する国内の政策

上記の事案のように重要インフラ事業者などの社会インフラを支える組織が被るランサムウェアの被害は、その影響の大きさから、同様の被害を防止するため、政府のサイバーセキュリティに対する施策にも大いに反映されています。以下では、前述の事案を受けて政府がどのような施策を行っているかを紹介します。

医療機関に対する施策

政府は 2024 年 7 月 10 日、『サイバーセキュリティ 2024（2023 年度年次報告・2024 年度年次計画）』（以降、「サイバーセキュリティ 2024」）を決定し、公表しました(*1)。「サイバーセキュリティ 2024」では、政府がサイバーセキュリティに関して特に強力に取り組む施策がまとめられており、現在における課題やそれらを解決するための取り組みについて概要が示されています。その中でも近年、医療機関においてランサムウェアの感染などによるシステムの機能停止や長期にわたる診療停止の事例が相次いでいることから、政府は特に医療機関を中心とした、以下の施策を進めています。

背景及び課題	取り組みの概要
医療機関のセキュリティ対策は、これまで各医療機関が自主的に取組を進めていたが、サイバー攻撃により長期に診療が停止する事案が発生したことから自主的な取組だけでは不十分と考えられる。医療機関におけるサイバーセキュリティ対策を強力に推進することが必要である。	・サイバーセキュリティインシデントが発生した医療機関に対する初動対応支援や、医療機関がサイバーセキュリティ対策を講じるに当たっての相談・助言、医療機関に特化したサイバーセキュリティ演習プログラム作成・実施を行う。また、「医療機関向けセキュリティ教育支援ポータルサイト」において、職員を対象とした研修にも活用できるコンテンツ等の作成・掲載を行う。 ・「医療情報システムの安全管理に関するガイドライン」第 6.0 版について、医療機関における研修の実施や普及啓発に取り組む。また、「医療機関におけるサイバーセキュリティ対策チェックリスト」において、医療機関における日々のセキュリティ対策を推進するとともに、チェックリストを用いた立入検査を行う。 ・厚生労働省委託事業において、病院の外部ネットワークとの接続の安全性の検証・検査や、オフライン・バックアップ体制の整備の支援を実施する。
医療機関等の重要インフラ事業者がサイバー攻撃により機能停止する事態が相次ぎ、当該分野のセキュリティ人材不足も原因の一つとなっている。行政が支援し、当該分野の実態を踏まえた早急な人材育成が必要である。	・NICT が保有する人材育成やサイバーセキュリティ研究の実績・知見を活用し、厚生労働省等と連携して、各分野に特化したものを含む新たな演習プログラムを開発し、民間企業・団体等に提供できる体制を構築・強化する。講師人材の育成も併せて行う。

出典：「サイバーセキュリティ 2024」(*1)を基に大和総研作成

(*1) NISC『サイバーセキュリティ 2024（2023 年度年次報告・2024 年度年次計画）』

これらの施策が示すとおり、政府による取り組みはインシデント発生時の初動対応支援やセキュリティ対策の相談・助言、人材育成など多岐にわたっています。特に昨年は医療法施行規則の改正により、医療機関の管理者はサイバーセキュリティ対策において必要な措置を講じることが義務化されたことに加え、その対策状況について行政による医療機関への立入検査が行われるようになったことで、より一層、政府によるセキュリティ対策への関与が高まっています。

港湾に対する施策

2023 年 7 月に発生した名古屋港コンテナターミナルへのランサムウェアによるサイバー攻撃は、2 日以上にわたり物流に大きな影響を与えましたが、この攻撃が発生した時点では「港湾」はサイバーセキュリティ基本法の「重要インフラ事業者」と経済安全保障推進法の「基幹インフラ事業者」の、いずれにも含まれていませんでした。

しかし、この事案によって港湾が果たす役割の重要性が再認識され、政府は有識者によるセキュリティ対策の検討委員会を設置し、港湾の位置付けを見直すこととなりました。その結果、2024 年 3 月 8 日にサイバーセキュリティ基本法において「港湾」が「重要インフラ事業者」の対象に追加され、官民一体となった迅速な情報共有体制の整備など、政府との連携が強化されました。

また、2024 年 5 月 10 日には経済安全保障推進法の改正案が参議院本会議で可決・成立し、「基幹インフラ事業者」の対象にコンテナターミナルで貨物の受け渡しを行う「港湾運送」が新たに追加されました。この改正により、今後、重要な設備を導入する際には、サイバー攻撃を防止するための適切な措置が講じられているかなどについて、政府による事前審査が必要となり、審査の結果、不備があると判断された場合は、設備の変更などを求める勧告や命令が出されることとなりました。

	サイバーセキュリティ基本法	経済安全保障推進法
法律の概要	国民生活や社会経済活動の基盤となるインフラのうち、機能が停止・低下すれば多大な影響を及ぼす恐れがある事業者を「重要インフラ事業者」として指定し、事業者が適切なサイバーセキュリティの確保に努めるように対策を講じている。	インフラサービスの安定的な提供を確保するため、基幹インフラを担う事業者のうち、一定の基準を満たす事業者を「特定社会基盤事業者（通称：基幹インフラ事業者）」として指定し、重要な設備の導入などを行う際に政府の審査を必要とするよう定めている。
対象の業種	情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油、**港湾**	電気、ガス、石油、水道、鉄道、貨物自動車運送、外航貨物、**港湾運送**、航空、空港、電気通信、放送、郵便、金融、クレジットカード

※赤字が事案発生後、新たに追加された業種

出典：大和総研作成

最後に

本記事で紹介した政府の施策は数ある中のごく一部であり、他にも、ランサムウェアをはじめとしたサイバー攻撃への対策を強化するため、重要インフラ事業者における被害発生を想定した演習や海外機関との連携などを通じて、国内全体のサイバーセキュリティの底上げを図っています。

前述した「サイバーセキュリティ 2024」には、サイバー空間の現下の情勢や、政府が昨年度取り組んできた施策、今年度特に力を入れて取り組む施策が網羅的にまとめられており、国内におけるサイバーセキュリティの動向を把握する上で大変参考になります。一度ご確認いただくことをお勧めします。

（横平　健）

バックナンバーはこちら

DIR SOC Quarterly vol.5 2023 summer（2023 年 7 月 14 日発行）

- 経済安全保障推進法の施行によって求められるインフラ事業者の対応
- SIM スワップ詐欺による不正送金事案の摘発
- マイクロセグメンテーション -ゼロトラストに基づく新しいセキュリティ戦略-

DIR SOC Quarterly vol.6 2023 autumn（2023 年 10 月 27 日発行）

- 『サイバーセキュリティ 2023（2022 年度年次報告・2023 年度年次計画）』の公表
- ランサムウェアによる名古屋港のシステム障害
- DMARC の導入にかかわる動向

DIR SOC Quarterly vol.7 2024 spring（2024 年 2 月 22 日発行）

- 『サイバーセキュリティ経営ガイドライン Ver 3.0 実践のためのプラクティス集 第 4 版』の公表
- サイバー攻撃の新たな手口「ノーウェアランサム」
- CVSS の歴史と最新版（v4.0）での改善点

DIR SOC Quarterly vol.8 2024 summer（2024 年 6 月 17 日発行）

- 経済産業省、企業のサイバーセキュリティ対策を格付けする制度の創設へ
- 特別寄稿　生成 AI の最新動向
- 生成 AI エコシステムを標的とするワーム Morris II

DIR SOC Quarterly vol.9 2024 autumn
2024 年 9 月 20 日発行
著者　大和総研
執筆者　水谷 浩樹、蓮見 将生、渋谷 篤、田川 晋作、土田 将弘、山崎 禎章、横平 健、松井 直己
発行所　株式会社大和総研　フロンティア研究開発センター
印刷・製本　セキ株式会社

お問い合わせ先　https://www.dir.co.jp/contact/solution/input.php

「WORLD」（ワード）は、大和総研が運営する、AI・データサイエンスなど先端技術に特化した用語解説サイトです。

大和総研の用語解説サイト

WORLD

キーワードから、みえる、つながる、未来の日常（Life）

「WORLD」（ワード）は、大和総研が運営する、AI・データサイエンスなど先端技術に特化した用語解説サイトです。
大和総研にはシステム、リサーチ、コンサルティング分野のスペシャリストが連携して、多くのお客様の幅広いニーズに応えてきた実績があります。用語解説サイト「WORLD」では、大和総研がこれまでに培ってきた豊富な経験をもとに、未来を築く新ソリューション創出の礎となる情報を、わかりやすく、深くご紹介していきます。
大和総研は先端テクノロジーやAI・データサイエンス技術を駆使し、デジタル社会を牽引するビジネスパートナーであり続けます。

CONTENTS

キーワードから　旬のIT用語が一目でわかるトレンドワードクラウド

国内約50のIT関連ニュースサイトで掲載された記事の中から、トレンドのワードをピックアップして視覚化。今押さえるべきIT用語が一目でわかるトレンドワードクラウドです。

みえる　AI・データサイエンスなど5分野の用語を解説

よく耳にする頻出用語から最新の用語まで、先端技術の研究・開発を通じてテクノロジーの可能性を追求しつづける大和総研の知見を活かした用語解説ページです。

解説用語例	AI・データサイエンス	セキュリティ	IT全般	ブロックチェーン	サステナビリティ
	●MLOps ●生成AI ●ニューラルネットワーク	●eKYC ●ゼロトラスト	●ニューロファイナンス ●ブレインテック ●ビジネスアナリシス	●非代替性トークン（NFT） ●セキュリティ・トークン・オファリング（STO）	●ゼロエミッション ●Society 5.0 ●人的資本

つながる　IT技術とビジネスをつなぐ深掘り解説記事と、エンジニアブログ

今後のビジネス活用が見込まれる技術の背景や、関連技術を紹介する深掘り解説記事と、技術検証事例を掲載するエンジニアブログ。WORLDは、未来を築く新ソリューション創出の礎となる情報をわかりやすく解説していきます。

大和総研の用語解説サイト
WORLD

https://www.dir.co.jp/world/

大和総研
Daiwa Institute of Research