NTT DATA
Trusted Global Innovator

グローバルセキュリティ動向

# 四半期レポート

# 2022年度 第1四半期

# 目次　グローバルセキュリティ動向　四半期レポート2022年度　第1四半期

# 1 エグゼクティブサマリー

本レポートは、NTTDATA-CERTが期間中に収集したサイバーセキュリティ関連情報に基づき、
その四半期におけるグローバル動向を独自の観点で調査・分析したものです。

## 農業分野に対するサイバー攻撃

アメリカでは、IT化が進む農業分野を狙ったサイバー攻撃が近年増加しています。これは攻撃者にとって、侵入やサイバー攻撃のターゲットになる農業分野のITシステムが増えたことや、サイバー攻撃によって食品サプライチェーン全体に甚大な被害を与えることができるようになり、身代金が支払われる確率が高まったことが理由と推測します。現在日本では農家や農業法人を狙ったサイバー攻撃はみあたりませんが、日本でも農業分野のIT化が進むにつれて農家や農業法人がサイバー攻撃の標的になるケースが増加していくと予測します。加えて日本の農業分野はIT化の初期段階であり、スマート機器を利用している農業従事者全体に情報セキュリティの教育が行き届いているとは言えません。そのため農業分野のIT化を進めると同時にサイバー攻撃に対する予防法やサイバー攻撃を受けた際の対応方法を農業従事者に教育することが大切です。またITの専門家ではない農業従事者が安全にIT化を進めるため、IoTシステムそのものの情報セキュリティの向上も考えていく必要があります。

## 不正オンライン決済を阻止する新たな認証の仕組みと対策基準

ECサイトを狙った攻撃によりクレジットカード情報が漏えいするインシデントが継続的に発生しています。こうした背景を踏まえて、業界としても新たな認証の仕組みEMV 3-Dセキュアへの移行を促しています。EMV 3-Dセキュアはクレジットカードの不正利用を防ぐ上で有効ですが、クレジットカード情報の漏えいの対策としては不十分です。クレジットカード情報を非保持にしたECサイトシステムにおいても、Webスキミング攻撃への対策を盛り込んだ新しいPCI DSSに準拠した対策の強化が必要です。本稿ではECサイトを構築、運用する組織がどのような対策を取るべきかを解説します。

## Internet Explorer11のサポート終了に伴うセキュリティリスクと対処法

2022年6月にMicrosoft社が提供するWebブラウザ Internet Explorer11 デスクトップアプリケーション（以下、「IE11」）のサポートが終了しました。サポート終了後はセキュリティ更新プログラムの提供がなくなり、IE11を使い続けることには、ゼロデイ攻撃のリスクが伴います。企業のシステム管理者やウェブサービス事業者は、社内にIE11でのみ閲覧・動作するシステムが残っているかどうか調査しましょう。残っていた場合には、システム担当者や開発者へ速やかにシステムの改修を呼びかけ、最新のWebブラウザへ対応したシステムへ移行してください。

# 2 注目トピック

## 2.1. 農業分野に対するサイバー攻撃

### 2.1.1. アメリカにおける農業・食品分野へのランサムウェア攻撃の増加

2022年4月、連邦捜査局（FBI）は、農業・食品分野に対するランサムウェア攻撃が増加しているとして、注意喚起を行いました [1]。この文書によると、2021年から2022年にかけてランサムウェアの技術と攻撃戦略はさらなる進化を続けており、攻撃者が食品サプライチェーンへ深刻な影響を与えるサイバー攻撃を行う確率が高くなっています。またFBIは、その前年の2021年9月にも農業・食品分野を狙ったランサムウェア攻撃の注意喚起を行っており、その深刻さが伺えます [2]。また、ブラジルやカナダ、オーストラリアでも同じく農業分野を狙ったランサムウェア攻撃が発生しています。

近年IoTや機械学習を用いた農作業の自動化が急速に進んでいます。例えば農場全体にセンサやカメラを搭載したIoT機器を設置しての気温や湿度、日照時間などの情報収集をしています。また、それらの情報を分析した結果にもとづいて水や肥料の自動投入もしています。他にもドローンによる農薬散布や無人トラクターの使用といった農作業の省力化や、ITを使って収穫量及び出荷量の自動管理をするようになってきました。このように農作業にIT技術が広く用いられるようになったことで、労働環境や収益性の改善が進みました。

その一方で農業分野がサイバー攻撃の標的になってきました。これまでは、ITへの依存度が高い重要インフラ分野や医療分野、製造業がランサムウェアの主な標的でした。農業分野は、ITに依存していない部分が多く、サイバー攻撃とはあまり縁がありませんでした。しかしながら、農業のIT化が進んだことで攻撃者がサイバー攻撃可能になっただけでなく、サイバー攻撃が成功した場合にIT技術に頼っていた様々な作業が停止するようになり、農作物の供給に深刻な影響が及ぶようになりました。

またFBIは農業分野におけるランサムウェア攻撃の特徴として、作付けや収穫といった特定の時期にサイバー攻撃が集中していると報告しています。農作物の生産は作付けや収穫、及び収穫から出荷までの時間的な制約が大きいにも関わらずそれらの時期は作業量が多く、時機を逸すると多大な損失を受けてしまいます。ランサムウェア攻撃によりIT技術に依存していた農作業や出荷作業が停止した場合、たとえそれらが復旧するまでの間、作業を手動で行うとしても作業効率は大幅に低下してしまいます。よってこれらの時期におけるランサムウェア攻撃による作業の停止は、食品サプライチェーン全体に多大な悪影響を及ぼします。そのため、ランサムウェア被害が発生した農家や農業法人は、一刻も早く作業を再開するために身代金の支払いに応じる可能性が高いと考えます。このように、農家や農業法人は身代金を支払うための十分な動機が存在するため、攻撃者が標的にするようです。

2021年以降だけを見ても、アメリカでは農業協同組合を含む様々な農業・食品分野の企業がランサムウェア攻撃の被害にあっています。例えば、2021年には穀物の収穫時期の9月15日から10月6日までの一か月足らずの間で、6つの穀物協働組合がランサムウェア攻撃を受けました。一部の管理機能の喪失に留まった組合もあれば、完全に生産活動が停止してしまった組合も存在しました。また、2022年に入ってからも農業・食品関連企業へのサイバー攻撃が複数回発生しており、FBIは今後もサイバー攻撃は続いていくだろうと警告しています。

攻撃者は様々な方法でランサムウェア攻撃を仕掛けますが、FBIの報告によると最も一般的な感染経路は電子メールを用いたフィッシングとリモートデスクトップやソフトウェアの脆弱性へのサイバー攻撃です。また共有ネットワークの悪用やマネージドサービスの侵害による関連組織への二次感染も発生しています [1, 2]。

### 2.1.2. 日本国内での農業分野のサイバー攻撃

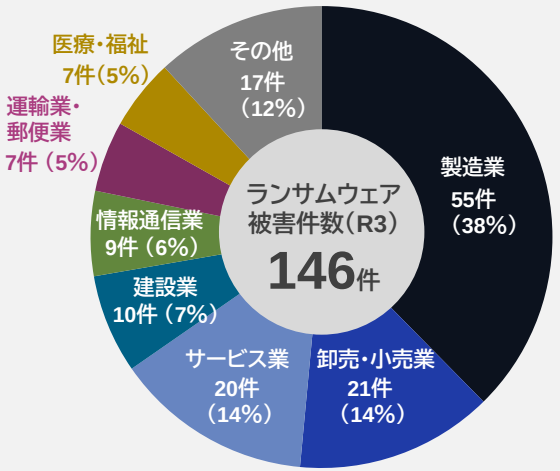
日本国内における農業分野へのサイバー攻撃としては、不正アクセスによる情報漏えいが報告されています。2022年6月に農業用品メーカーが運営するECサイトが攻撃者から不正アクセスを受け、5000件余りの個人情報と400件あまりのクレジットカード情報が漏えいしました。また2022年4月、ある農業関連の公益社団法人の職員が、関係者を装ったメールを開封してEMOTETに感染し、PCに保存していたメールアドレスや電子メールの内容が漏えいしました。EMOTETについては、弊社の2021年度第3四半期のグローバルセキュリティ動向四半期レポートにて解説しておりますので、詳細はそちらをご参照ください [3]。

アメリカのような農家や農業法人を標的としたランサムウェア攻撃などのサイバー攻撃の傾向は、今のところ日本国内には見あたりません。警察庁が公表した令和3年にランサムウェア攻撃を受けた企業や団体の業種別件数（図 2 1）を見ると、最も多い業種は製造業、次いで卸売、小売業であり、農業はありません。

今後のために、日本国内においても農業分野の情報セキュリティを考えることは非常に重要だと思います。2019年から農林水産省主導で「スマート農業加速化実証プロジェクト」を進めており、2025年までにほぼ全ての農業従事者がデータを活用した農業を実践することを目標にしています [5]。これにより、センサやカメラを用いたデータの収集や活用に始まり、水や肥料の自動供給、ドローンやロボットを用いた作業の自動化が今後さらに進んでいくと予測します。このように日本国内においても農業のIT化が進むことでサイバー攻撃の糸口がつかまれやすくなるとともに、サイバー攻撃に成功した際の被害が大きくなるため、農家や農業法人が標的になる確率が高くなると思います。加えて、農業分野はIT化の初期段階であり、農業従事者の情報セキュリティへの意識が醸成できていないと予想します。そのため、農家や農業法人は攻撃者からソフトターゲットと見られ、サイバー攻撃の対象になるおそれがあると考えられます。

では日本の農業分野に対して、今後どのようなサイバー攻撃が行われるでしょうか。先ほど述べたように、日本国内には農家や農業法人を標的としたランサムウェア攻撃の傾向は見あたりません。しかしこのまま日本国内の農業分野のIT化が進み、攻撃者が、日本国内の農家や農業法人は身代金の支払いに応じると判断した場合、農作業を停止に追い込むようなランサムウェア攻撃を仕掛けると予測します。ランサムウェア攻撃の他にも農業に使用するIoT機器へ不正アクセスしてデータを改ざんしたり、設定を変更して異常な動作をさせて被害を引き起こしたりする懸念もあります。例えば、IoT機器を異常動作させれば、農作物に不適切な分量の水や肥料を与えて、枯らすことができるかもしれません。農業特有の問題として、そのサイバー攻撃の影響が作物に表れるタイミングは、時間が経過してその作物が成長したあとであるため、サイバー攻撃に気づかなかったり発見が遅れたりするおそれがあります。またサプライチェーン攻撃は、さまざまな業界で広く問題になっています。同様に、農業分野でも食品サプライチェーン上の別の企業を踏み台にして農業従事者や他の企業に対して二次感染を狙うサイバー攻撃が増えるかもしれません。このサプライチェーン攻撃は、食品サプライチェーン上のどこかの企業のセキュリティ対策が手薄でサイバー攻撃が成功してしまうと、食品サプライチェーン全体が影響を受けてしまい、消費者に商品が届かなくなってしまいます。これらのようなサイバー攻撃の被害にあわないようにするため、農業のIT化を進めると同時にそのセキュリティについても考えていく必要があります。

図 2-1: ランサムウェア被害の被害企業･団体等の業種別報告件数 [4]



### 2.1.3. サイバー攻撃への対策

サイバー攻撃の被害にあわないようにするためには、まずは基本的なセキュリティ対策を徹底することが重要です。例えば送られてきた電子メールに添付されているファイルやハイパーリンクを不用意に開かないといったことや、IoT機器を含む全てのIT機器のOSやソフトウェア、及びファームウェアのアップデートやパッチの適用をして、脆弱性を残さないようにすることが大切です。

またマルウェアに感染してしまった場合に備え、被害軽減策を講じておくことも重要です。定期的にデータやサーバのバックアップをとり、ネットワークから切り離して保管したり、それらからシステムを復旧する際の計画を事前に策定したりしておくことなどが挙げられます。また重要な機能を特定しておき、システムがオフラインになってしまった場合の運用計画を立てておくことも有効です。

内閣サイバーセキュリティセンター（NISC）ではサイバーセキュリティ向上のためのポータルサイトを運営しています [6]。その中には様々な公共機関がランサムウェア攻撃に対する対策や注意喚起を行っているページをまとめた特設ページも掲載されていますのでそちらをご参照ください [7]。

### 2.1.4. まとめ

日本国内も農業のIT化によって、農作業の省力化や品質、収穫量の向上が進んでいます。それに伴ってサイバー攻撃を受ける確率や、サイバー攻撃を受けた際の影響も大きくなっていくと予想します。今後は、より強固に情報セキュリティ対策を行い、サイバー攻撃の被害にあわないように対策を講じることや、サイバー攻撃にあった際に被害拡大を抑える方法を事前に検討しておく必要があります。

しかしながら、農業従事者が自分自身だけで十分なセキュリティ対策を行うことは困難だと思います。農林水産省の令和2年の調査によると、農業経営体のうち95%以上が個人経営体です [8]。農業経営体の大部分を占める農家に、十分なセキュリティ対策の検討と導入、その運用を求めることは難しいと思います。このことから、今後、農業のさらなるIT化を進めるにあたっては、単なるIT機器の導入だけではなく、農業従事者にセキュリティに関する知識を身に着けてもらうための教育機会を提供することも必要になると思います。また、個々の農家や農業法人のセキュリティ対策や運用の負担を軽減できるように、農業用のIoT機器へセキュリティ機能を標準搭載したり、ログの自動監視や共同SOC、マネージドセキュリティサービスの契約を付帯したりするなど、IoT機器とセキュリティをセットにした展開も必要になっていくのではと思います。加えて農業従事者が農作物の生産に必要な資材を調達したり、生産した作物を消費者に届けたりするためにも、食品サプライチェーン全体として、セキュリティ対策を進めていくことが重要となってきます。

# 3 情報漏えい①
# 不正オンライン決済を阻止する新たな認証の仕組みと対策基準

## 3.1. クレジットカード情報漏えいインシデントの現状

本レポートでは、EC-CUBEの脆弱性を悪用したクレジットカード情報漏えいのインシデント事例を2021年度第1四半期、第3四半期と継続して取り上げてきました。そして2022年度第1四半期も、同脆弱性に起因するものかは不明ですが、表 3-1に示すとおりクレジットカード情報が漏えいするインシデントが継続して発生しています。

表 3-1で挙げたインシデントの多くは、攻撃者が脆弱性を悪用して不正アクセスしてペイメントアプリケーションを改ざんしたことが原因です。これらのインシデントは、システムでクレジットカード情報を保持していなかったにも関わらず、クレジットカード情報が漏えいしています。このことから、現在はクレジットカード情報を非保持にするだけではセキュリティ対策が不十分であり、ECサイトのシステムは、上記の不正アクセスと改ざんを対策しなければならないことわかります。

こうした背景から、クレジットカード情報の漏えいや不正利用を防ぐために、クレジットカード業界は新たな認証の仕組みの導入やセキュリティ対策ガイドラインの整備などを進めています。本章では業界の流れを踏まえ、オンライン決済システムのクレジットカード不正利用と情報漏えいに対して、ECサイトを構築、運用する組織がとるべきセキュリティ対策を整理します。まずクレジットカード情報の不正利用への対策としてEMV 3-Dセキュアの仕組みを説明しますが、これだけでは対策として十分ではありません。攻撃からシステムを守るためには多層的に対策を講じる必要があり、そもそもカード情報の漏えいを阻止するためには、システム自体のセキュリティ水準を高める必要があります。今回はクレジットカードの情報漏えいへの対策として、約8年ぶりの改定が行われたPCI DSS [9]について説明します。また本章で記載している各組織の説明を表 3-2、図 3-1、および図 3-2に示します。

**表3-1：クレジットカード情報漏えいのインシデント事例（2022年第1四半期）**

| # | 公表日 | ECサイト名 | ECサイト運営会社 |
|---|---|---|---|
| 1 | 2022/4/25 | いいもの、あるよ! | 宇都宮ケーブルテレビ株式会社 |
| 2 | 2022/5/18 | MACHATT ONLINE STORE | 株式会社 machatt |
| 3 | 2022/5/24 | 宗家源吉兆庵オンラインショップ | 株式会社 宗家 源吉兆庵 |
| 4 | 2022/5/24 | CHUOHネットショップ | 中央教育研究所 株式会社 |
| 5 | 2022/6/7 | スイーツパラダイス オンラインショップ | 井上商事株式会社 |
| 6 | 2022/6/7 | 誠和ホームページ、<br>誠和オンラインショップ、新時代農業塾 | 株式会社誠和 |
| 7 | 2022/6/7 | 東京シャツ公式オーダーサイト | 東京シャツ株式会社 |
| 8 | 2022/6/29 | サンシティオンライン通信販売サイト | 株式会社サンシティ |
| 9 | 2022/6/30 | 人形工房ひととえオンラインショップ | 株式会社松永 |

**表3-2：各組織の説明 [10]**

| # | 組織名 | 説明 |
|---|---|---|
| 1 | イシュアー | 利用者と契約し、キャッシュレス手段を発行・提供する会社のこと。利用者の獲得や利用者への請求が主な業務である。 |
| 2 | アクワイアラー | お店に対して、キャッシュレス手段の導入に向けた契約を行ったり管理したりする会社のこと。その他、イシュアー（クレジットカード利用者と契約する決済会社）への購入代金の請求、加盟店（お店）への代金支払いが主な業務である。 |
| 3 | 決済代行業者（PSP） | 決済代行サービスを提供する会社のこと。<br>※決済代行サービスとは、加盟店とクレジットカード会社や決済サービス会社の間に入り、複数のクレジットカード会社や決済サービス会社との契約や精算を代行するサービスのこと。 |
| 4 | 加盟店 | キャッシュレス手段で支払えるお店や企業のこと。決済会社と契約して、そのサービスに対応していることを加盟と呼んでいる。 |
| 6 | 国際ブランド | 世界各地に数多くの加盟店を持ち、国際的に通用するクレジットカードブランドのこと。 一般的には、VISA（ビザ）、MasterCard（マスターカード）、American Express（アメリカン・エキスプレス）、DinersClub（ダイナースクラブ）、JCB（ジェーシービー）、Discover Card（ディスカバーカード）と銀聯（ぎんれん）の 7つを指す。（2019年2月時点） |

図 3-1:クレジットカードでの支払いにおけるお金の流れ [10]

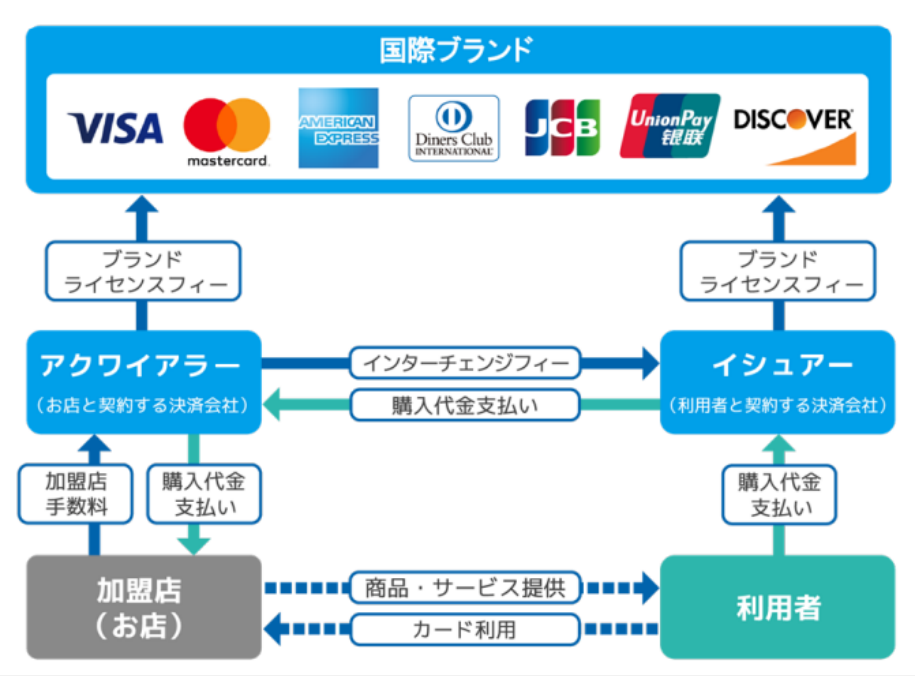
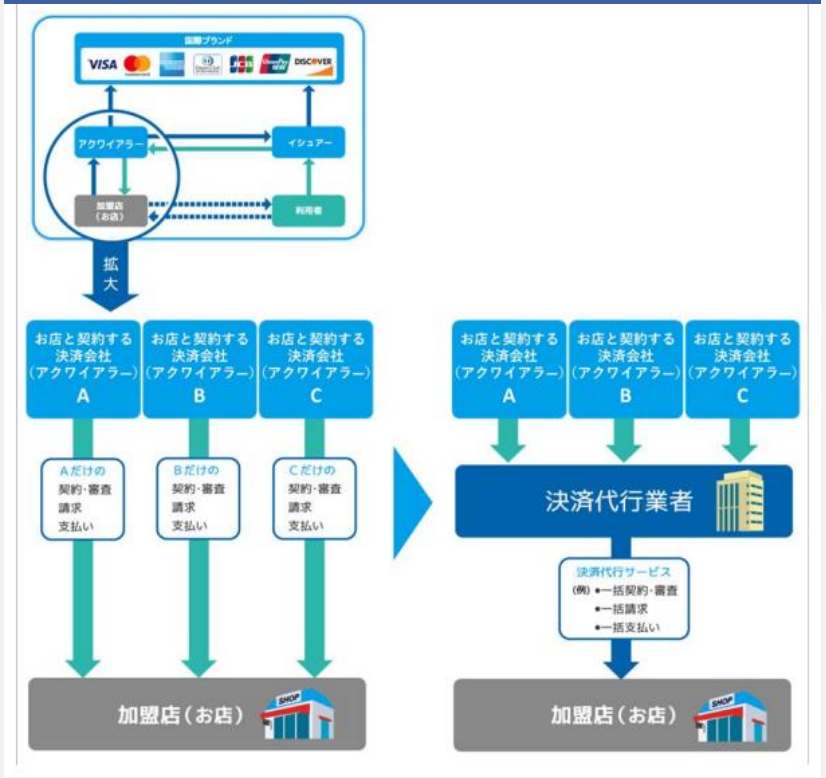



図 3-2:決済代行業者の役割 [10]



## 3.2. 旧3-Dセキュアの廃止・EMV 3-Dセキュアへの移行

オンライン決済時にクレジットカード情報に加えてパスワード入力を求めることで本人認証を行う3-Dセキュア1.0というサービスがあります。このサービスが2022年10月で終了し、以降はEMV 3-Dセキュアに準拠した本人認証を行うサービスへ移行することを推奨しています [11]。

### 3.2.1. EMV 3-Dセキュアとは

EMV 3-Dセキュアは、従来の3-Dセキュア1.0の欠点を改善し、「リスクベース認証を使ったパスワード入力負荷の低減」「スマートフォンアプリへの対応」「非決済分野への対応」「多要素認証の導入」など、ユーザビリティの向上と不正利用防止の仕組みを取り入れた技術です [12]。特に「多要素認証の導入」は追加認証を要求する際に、ワンタイムパスワードや生体認証を求めることで悪意のある第三者のなりすましのリスクを低減させることができるため、不正利用防止に役立ちます。

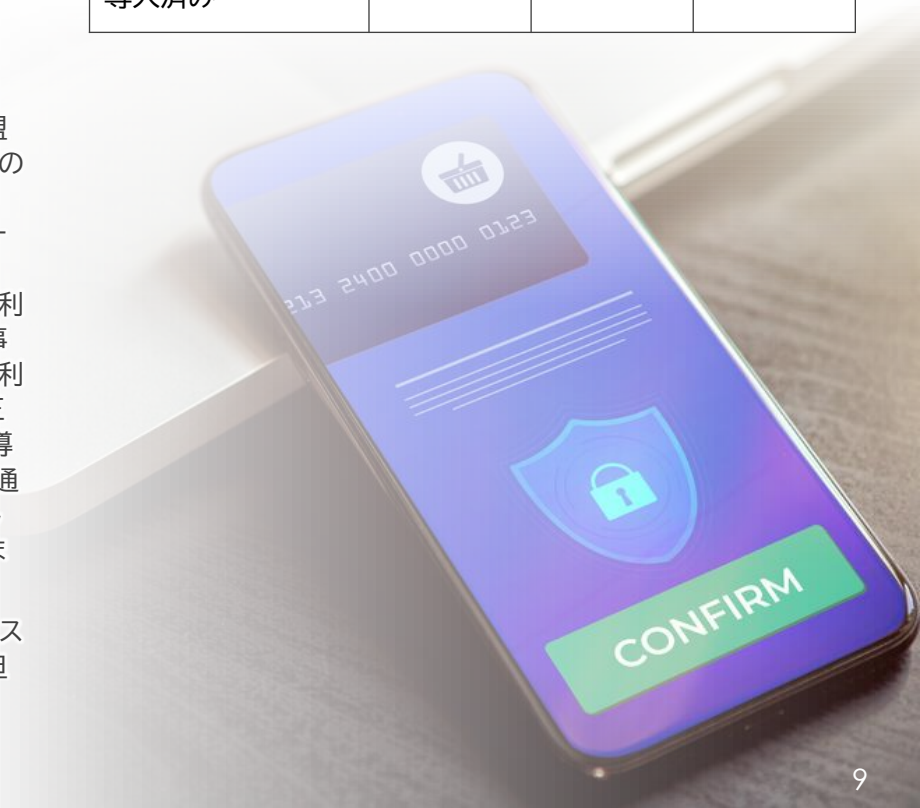
### 3.2.2. EMV 3-Dセキュア未導入時の代金負担のリスク

本移行に伴い、イシュアー（クレジットカード利用者と契約する決済会社）が加盟店または決済代行業者（以下、「PSP」という）へチャージバック請求を実施した際の補償金負担に関する規約が変更となります [11]。不正利用発生時のイシュアーのチャージバック請求とは、クレジットカードの不正利用等が発生してクレジットカード利用者がそれを理由に代金の支払に同意しない場合に、イシュアーがアクワイアラー（お店と契約する決済会社）を通じて、加盟店またはPSPへクレジットカードの利用代金や売上の取消しを請求することを指します。各組織間の契約内容や発生した事例ごとに異なりますが、チャージバック請求が成立すると、加盟店またはPSPが不正利用等の代金を負担しなければなりません。従来は3-Dセキュア1.0を導入すれば、不正利用が加盟店の責任ではないことを示すことができて、イシュアーが3Dセキュアを導入している加盟店やPSPで発生した代金の負担を補償しました。しかし表 3-3に示す通り、2022年10月以降は主要な国際ブランドのルールでは、EMV3-Dセキュアを導入していなければ、イシュアーは代金の負担を補償しないため、加盟店が代金を負担します。

つまりEMV3-Dセキュア未導入の場合、悪意のある第三者が不正利用に成功するリスクが高い上に、攻撃者がクレジットカードを不正利用した場合に加盟店が代金を負担しなければなりません。

**表3-3：不正利用発生時の加盟店/PSPの代金の負担の有無 [13]**

| 加盟店のセキュリティ対策 | 2021年10月まで | 2021年10月～2022年10月 | 2022年10月以降 |
|---|---|---|---|
| 3-Dセキュア未導入 | 負担あり | 負担あり | 負担あり |
| 旧3-Dセキュア導入済み | 負担なし | 一部負担あり | 負担あり |
| EMV 3-Dセキュア導入済み | 負担なし | 負担なし | 負担なし |



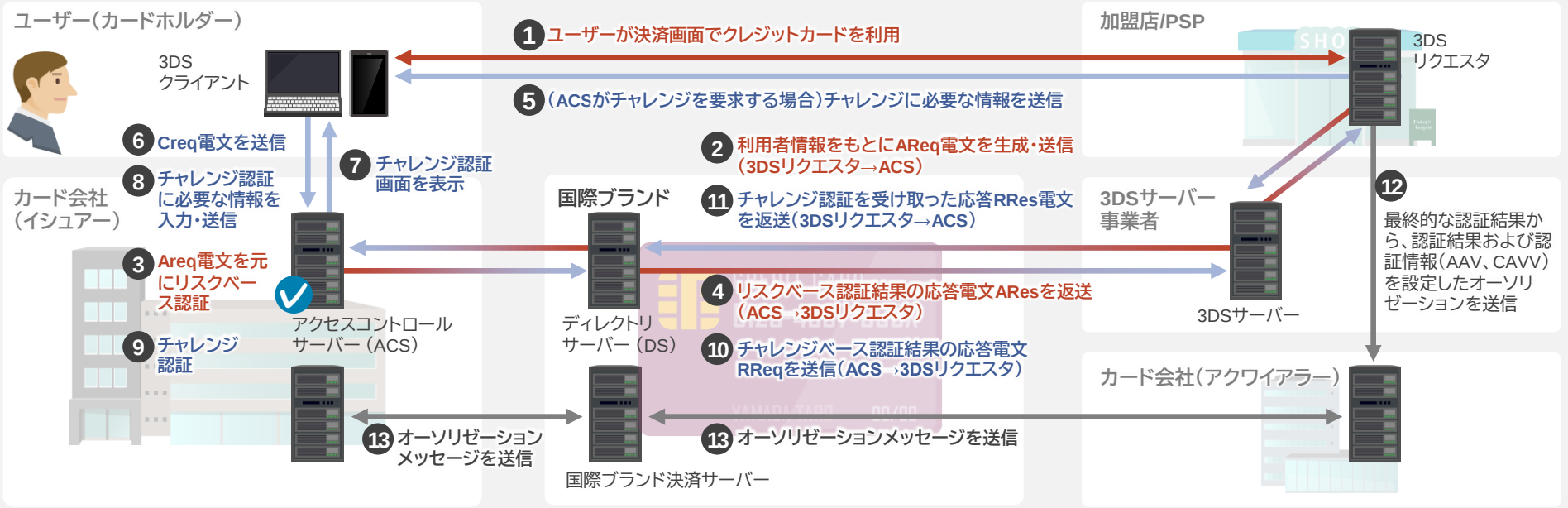
### 3.2.3. EMV 3-Dセキュアの仕組み

図 3-3にEMV 3-Dセキュアを使ったクレジットカードのオンライン決済処理のフローを示します。図 3-3に示す通り、基本的な決済処理は、赤矢印と赤字のリスクベース認証フロー（①-④）です。リスクベース認証時に不正利用の可能性確率が高いと判断してチャレンジ認証が必要になった場合は、青矢印と青字のチャレンジ認証フロー（⑤-⑪）を実行します。2つの認証が成功したあとは、黒字のフロー（⑫-⑬）を実行して、このクレジットカードで決済して問題ないと判断し、加盟店または加盟店の委託先PSPからカード会社へ信用承認（オーソリゼーションメッセージ）を送信します。

ではECサイトを構築、運用する組織、つまり加盟店または加盟店から委託されたECサイト構築、運用業者が、3-Dセキュア 1.0からEMV 3-Dセキュアへ移行導入時に実施すべきことは何でしょうか。

ここでECサイトを構築、運用する組織が、クレジットカードのオンライン決済処理のフローの中へ、新規にかかわりを持つ要素が3DSサーバ事業者および事業者が保有する3DSサーバです。EMV 3-Dセキュア使ってオンライン決済処理する場合は、ECサイトを運用する3DSリクエスタから3DSサーバへ、新たな通信の接続が必要となります。またその際にECサイトを構築、運用する組織が対応しなければならない他組織および他システムを図 3-4に示します。対応箇所はシステムが自社構築か、PSPへの委託かによって異なります。

図 3-3：EMV 3-Dセキュアを使った決済処理フロー [11]

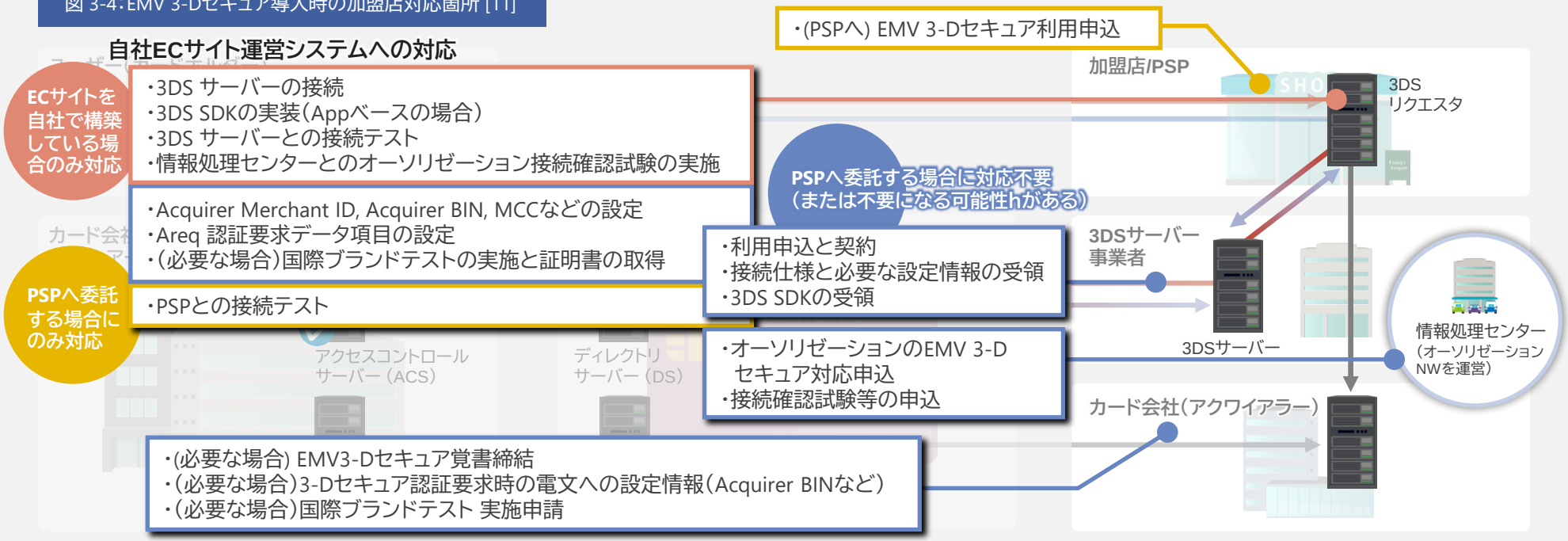


### 3.2.4. ECサイトを構築、運用する組織が対応すべきこと

#### （1） 自社構築の組織がEMV 3-Dセキュアを導入する場合

もし自社構築の場合、3DSサーバ事業者が提供する3DS SDKをシステムに実装するなど、一部システムに変更を加える必要があります。またEMV 3-Dセキュア利用に関連する各種申し込みや、変更を加えた機能の接続確認など、自社対応が必要な箇所が存在します。自社構築のメリットは、自社内でシステムや契約面を管理、把握できる点やPSP委託の費用を削減できる点にあります。反対にデメリットとしては、自社対応の箇所が多いため、管理が煩雑になる点、または自社で技術者を用意しなければならない点です。他業者へシステム構築を委託する方法もありますが、いずれにしても自社でリソースを用意する必要があります。

図 3-4：EMV 3-Dセキュア導入時の加盟店対応箇所 [11]



### （2） PSPと契約する組織がEMV 3-Dセキュアを導入する場合

一方でPSPへ一部業務を委託している場合は、PSPが3DSサーバに関する接続や契約面を一部代行するため、自社構築の場合よりシステムへ手を加える箇所が少なく済みます。また契約形態は大きく2つあります。

1つ目は、加盟店がアクワイアラーと直接加盟店契約を行い、決済業務のみPSPへ委託している場合です。この場合、加盟店はアクワイアラーとPSPの2者と契約やシステムの対応などが必要となりますが、その他の3DSサーバ事業者や情報処理センターへの手続きはPSPが代行します。

2つ目は、加盟店がPSPへ、アクワイアラーとの加盟店契約と決済業務の両方を委託している場合です。この場合、PSPが、加盟店とアクワイアラーとの契約手続きも担ってくれるため、加盟店はPSPとの契約およびシステム対応を行うだけで済む場合が多いです。

PSPへ業務委託している場合のメリットは、契約面やシステム面の対応を簡略化できる点です。反対にデメリットは、PSP委託の費用がかかる点や契約やシステムの一部が自社の管理外になってしまう点です。委託業務の細かい内容はPSPとの契約により異なりますが、委託先PSPが信頼できる企業か、契約面に不都合はないかなど十分に考慮することが重要になります。

ECサイトを構築、運用する各組織は、それぞれが運用するECサイトのシステム形態に応じて導入を検討する必要があります。既にPSPへ決済業務を委託している場合は、契約の管理面を自社のルールと照らし合わせた上で、委託先へ詳細を確認しEMV 3-Dセキュア導入の一部作業を委託するとよいでしょう。自社構築でECサイトを構築、運用している組織は、予算や自社のルールを鑑みて自社で対応すべきか、PSPへ委託すべきかを考えるとよいでしょう。

### 3.2.5. EMV 3-Dセキュアが阻止できない攻撃

ここまでは、ECサイトを構築、運用する組織がEMV 3-Dセキュア移行時に注意すべき変更点を説明しました。冒頭でも説明しましたが、EMV 3-Dセキュアでは対策として不十分です。例えば、攻撃者がシステムの脆弱性を悪用してECサイトへ不正侵入しWebスキミング攻撃を仕掛けた場合、ECサイトがEMV 3-Dセキュアを使っていても、ECサイトの利用ユーザが決済画面へクレジットカード情報を入力してしまうと、クレジットカード情報が攻撃者へ盗聴されてしまいます。EMV 3-Dセキュアは、ECサイトの利用者の情報や操作と決済画面へ入力したクレジットカード情報から不正利用を見抜いて防ぐ仕組みです。攻撃者のECサイトへの不正侵入や決済画面への盗聴機能の挿入の検知や防止はできません。

つまりEMV 3-Dセキュアは、クレジットカード情報が漏えいした後の不正利用は防ぐことが出来ますが、クレジットカード情報の漏えい自体を防止することができません。クレジットカード情報の漏えいを未然防止するには、従来通りシステム自体のセキュリティ対策を徹底するしかありません。

以上から、ECサイトを構築、運用する組織はEMV 3-Dセキュアの導入とは別にクレジットカード情報の漏洩を防止するために、ECサイトの脆弱性対策やECサイトのセキュリティ対策の強化が必要です。

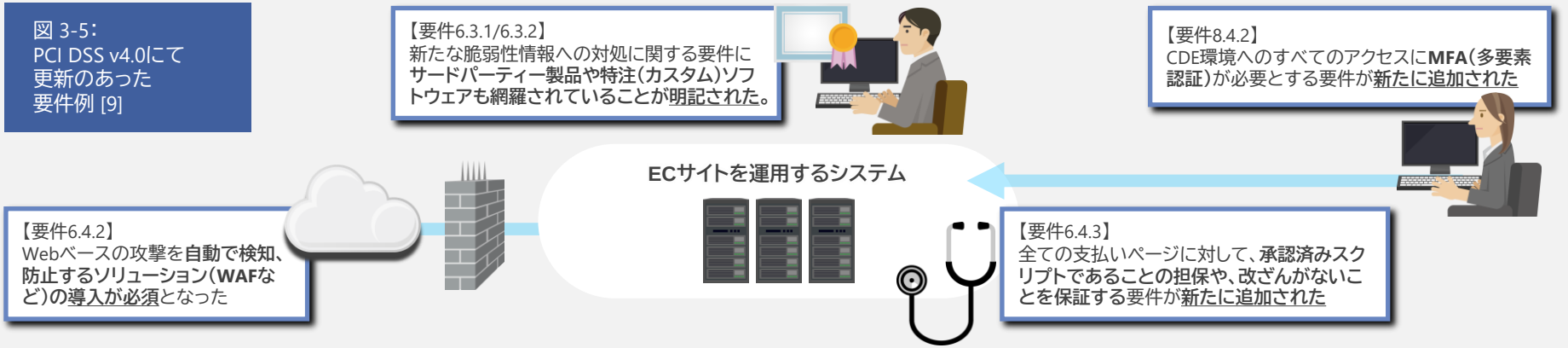
## 3.3. PCI DSSが約8年ぶりのメジャーアップデート

American Express、Discover、JCB、MasterCard、VISAの5社が共同で設立したPayment Card Industry Security Standards Council(PCI SSC)は、2022年3月に約8年ぶりにメジャーアップデートしたPCI DSS v4.0を公開しました [9]。アップデートの中には、クレジットカード情報漏えいに関連して、フィッシング攻撃やWebスキミング攻撃への対策を追加しています。

図 3-5に加盟店のECサイトシステムをベースにPCI DSS v4.0で変更のあった要件の例をピックアップしました。例えば、Webスキミング攻撃への対策として、要件6.4.3のようなスクリプト改ざんへの対処を要求する項目を追加しています。またこれまで明記していなかったサードパーティ製品やカスタムソフトウェアを利用したシステムの脆弱性管理の要件を要件6.3.1/6.3.2として明記するようになっています。EC-CUBEなどのECサイトのパッケージソフトウェアを利用した場合の脆弱性のリスクを対処するための要件です。

ECサイトを狙ったサイバー攻撃を防ぐためには、これをしておけばよいという対策はなく、さまざまなリスクや攻撃方法を防ぐために、システム上の攻撃可能な複数のポイントに対して、多層的にシステムを守る仕組みを導入することが重要です。カード会員データや機密認証データを保存、処理、送信するすべての事業体はPCI DSSを準拠することが必須ですが、カード会員データや機密認証データの非保持によりPCI DSSを準拠するシステムもPCI DSSの各要件に則ったECサイトの脆弱性対策やECサイトのセキュリティ対策の強化を実施することを推奨します。

図 3-5:
PCI DSS v4.0にて
更新のあった
要件例 [9]



## 3.4. まとめ

昨今のクレジットカード情報漏えい事例を踏まえて、業界全体としても制度の改定・対策の整備が進んでいます。クレジットカード情報漏えい後の不正利用やチャージバック負担の回避などのリスクに備えて、ECサイトを構築、運用する組織はEMV 3-Dセキュアを導入することを推奨します。

また導入時には各組織が運用するECサイトのシステム形態に応じて検討する必要があります。既にPSPへ決済業務を委託している場合は、契約の管理面を自社のルールと照らし合わせた上で、委託先へ詳細を確認しEMV 3-Dセキュア導入の一部作業を委託するとよいでしょう。自社構築でECサイトを構築、運用している組織は、予算や自社のルールを鑑みて自社で対応すべきか、PSPへ委託すべきかを考えるとよいでしょう。

またEMV 3-Dセキュアのみでは、カード情報漏えいを防ぐことはできないため、PCI DSSなどのガイドラインを参考にしつつカード会員データや機密認証データの非保持によりPCI DSSを準拠するシステムもPCI DSSの各要件に則ったECサイトの脆弱性対策やECサイトのセキュリティ対策の強化を実施することを推奨します。ECサイトの脆弱性対策やセキュリティ対策の強化によって、情報漏えいを阻止し、EMV 3-Dセキュアによって不正利用を阻止するといった複数の対策で多層的にシステムを守ることが重要です。

# 4 情報漏えい②
# OAuthトークン漏えい事件から学ぶこと

2022年4月15日にGitHub社が、ユーザのOAuthトークンを使ったGitHubのプライベートリポジトリへの不正アクセス事案が発生したと発表しました。同社によると、本事件ではGitHubだけでなく、npmも含む、数十のプライベートリポジトリが不正アクセスを受けており、npmのリポジトリからは10万人分のユーザ情報が流出しました [13]。本稿では、このOAuthトークン漏えい事件から、攻撃者の意図や不正アクセスへの対策を考察します。

## 4.1. OAuthトークン漏えい事件の経緯

2022年4月、何者かが、窃取したユーザのOAuthトークンを悪用して、GitHubのプライベートリポジトリに不正にアクセスしてデータを窃取するサイバー攻撃が発生しました [13]。攻撃者が窃取したOAuthトークンは、GitHubに保持していたものではなく、GitHubと連携しているサードパーティ製アプリケーションのHerokuやTravis-CIから盗まれたと言われています。またGitHub社は、このサイバー攻撃はOAuthトークンを悪用して標的を厳選している高度な標的型攻撃だったと分析しています。右の表 4-1に、GitHub社が発表したOAuthトークン漏えい事件の経緯を示します。

**表4-1：GitHubでのOAuthトークン漏えい事件のタイムライン**

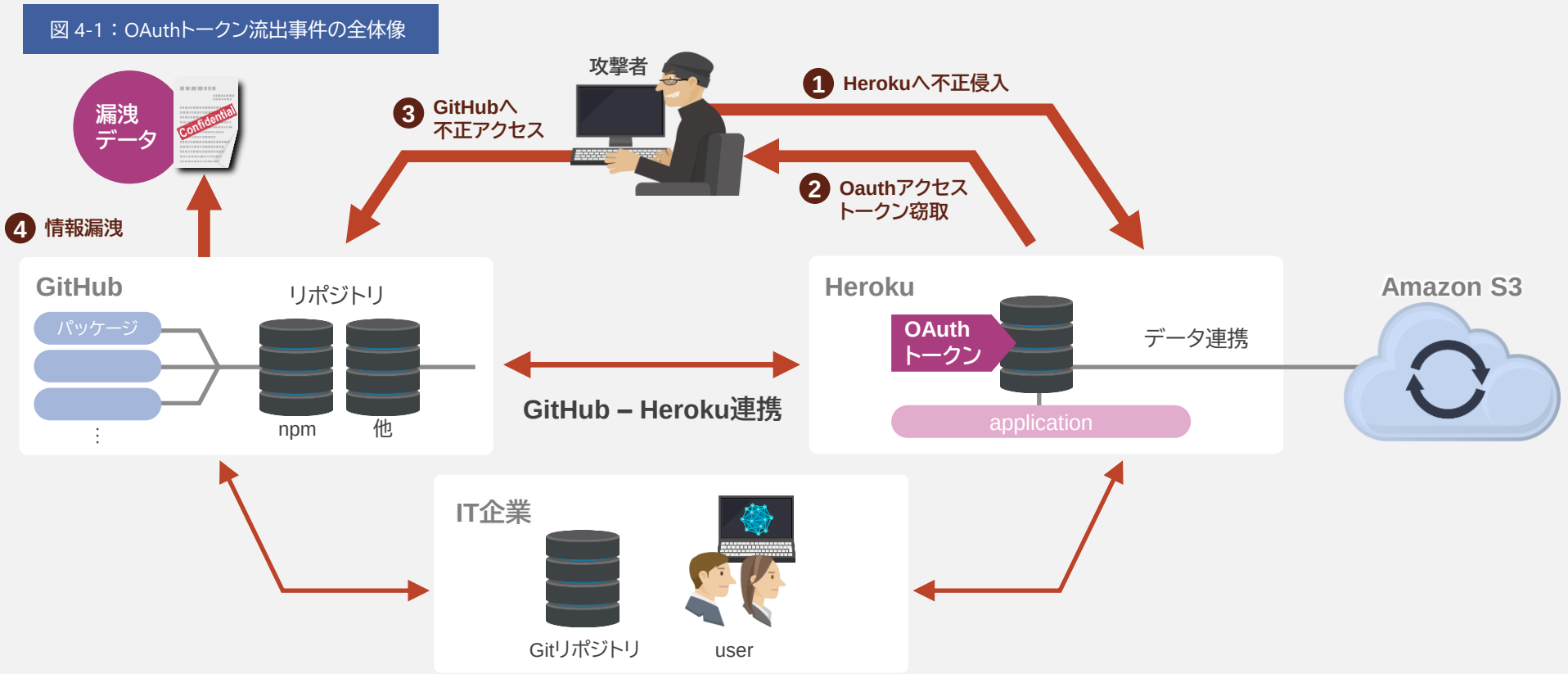
| 日付 | 経緯 |
|---|---|
| 2022/4/7 | 攻撃者がHerokuのデータベースへ不正アクセスし、OAuthトークン窃取 |
| 2022/4/9 | 攻撃者がHerokuから窃取したOAuthトークンを悪用してGitHub等のプライベートリポジトリからデータを不正にダウンロード |
| 2022/4/12 | GitHub社のセキュリティチームが調査を開始し、npmのリポジトリへの不正アクセスを発見 |
| 2022/4/13,14 | GitHub社が、調査結果をHeroku社、Travis-CI社へ通知 |
| 2022/4/13 | Heroku社が窃取されたOAuthトークンの無効化を開始 |
| 2022/4/15 | GitHub社とHeroku社が本事件をブログで公開 |
| 2022/4/17 | 全てのHeroku DashboardのOAuthトークンの無効化が完了 |
| 2022/4/18 | Travis-CI社がブログを公開 |
| 2022/4/18 | GitHub社が被害を受けたユーザに対して通知および対応喚起を実施 |
| 2022/4/27 | GitHub社が、本攻撃は複数の組織を対象とした標的型攻撃という分析結果を発表 |
| 2022/5/5 | Heroku社がパスワードリセットを実施 |
| 2022/5/26 | GitHub社が具体的な流出データを報告 |

## 4.2. 本事件の解説

### （1） 原因

本事件の全体像を図 4-1に示します。漏えいしたOAuthトークンは、GitHubのプライベートリポジトリへアクセスできる認可トークンでした。本事件の場合、GitHubが、OAuthアプリケーションのHerokuとTravis-CI向けに発行したOAuthトークンが、何らかの方法で流出してしまい、攻撃者の手に渡ってしまったため、攻撃者がGitHubのプライベートリポジトリへ不正ログインできました。Heroku社の発表によると、侵入契機は明らかになっていませんが、何かしらの方法で攻撃者がHeroku社内のマシンへ侵入し、OAuthトークンを管理しているデータベースへたどり着き、DB内から情報を取り出したようです [14]。

図 4-1：OAuthトークン流出事件の全体像



### （2） 影響

（1）で述べた今回の攻撃によって、どのような影響があったのでしょうか。下記に漏えいを確認した情報の一覧を記載します [15]。

- GitHub発行のOAuthトークン
- skimdb.npmjs.comのバックアップデータ
- npmリポジトリの2015年以降の登録ユーザ情報(ユーザ名、パスワードハッシュ、電子メールアドレス) 10万件分
- 2021年4月17日時点の全てのプライベートなnpmパッケージのマニフェストとパッケージメタデータ
- 2022年4月10日時点のnpmの全てのプライベートパッケージの名前と公開バージョン番号、アーカイブを含む一連のCSVデータ
- 2つの組織のプライベートパッケージ

上記のようにnpm関連の漏えい被害が見つかっています。npmのリポジトリから、登録ユーザ情報10万件や全てのプライベートなパッケージのアーカイブ情報が漏えいしています。これについてGitHub社は、ログとイベントの分析やバージョン・ハッシュを確認した結果、攻撃者はGitHub上の公開パッケージの改ざん、および既存のパッケージへ向けた新バージョンの公開などは行われていないだろうと述べていますが、プライベートリポジトリへの被害についてこれ以上詳細な言及はしていないのが現状です。

### （3） 企業側の対応

本事件において、GitHub社、Heroku社、Travis-CI社は、いくつかの対応を実施しています。

GitHub社はHeroku社、Travis-CI社を通して該当ユーザへ通知メールで、今回の事件の被害内容とGitHubが実施した対応、緊急連絡先を伝えています。また、本事件に由来する対策かどうかは分かりませんが、GitHub社は2023年度末までに2要素認証を必須化すると発表しており、セキュリティ強化の動きがみられています [16]。

Heroku社は、漏えいしたOAuthトークンを使って不正にログインできるすべてアカウントの認証情報のリフレッシュを行いました [14]。また、ユーザへ、定期的にHeroku社の公式ブログをチェックして、アップデートがあれば、適切に対応するよう連絡しました。

Travis-CI社は、漏えいしたOAuthトークンを悪用した顧客のリポジトリやデータへの不正アクセスが発生しなかったため、顧客に関する問題やリスクはないと述べています。そのため、特段の対応はしていないようです [17]。

## 4.3. 攻撃者の意図

GitHub社の情報では、攻撃者はOAuthトークンを使ってアクセスできる組織を一覧化した後、標的の組織を選んで、その組織のプライベートリポジトリへ不正アクセスしたようです [14]。また、攻撃者は、npmのリポジトリへの不正アクセスも成功しており、攻撃者はnpmのS3バケットにもアクセスできたという情報もあります。あくまで推測ですが、組織を一覧化して取捨選択している点から、攻撃者はGitHub上から大量の個人情報を窃取することが主たる目的ではないと思います。GitHubからアクセストークンや個人情報等の情報を盗むことも確かに目的の一つなのかもしれませんが、攻撃者にとって、アクセストークン等の情報を取得してGitHubに不正アクセスしただけでは大した利益は得られません。そのため攻撃者の主たる目的は、製品のコードを改ざんしてバックドアを仕込み、多くの組織を侵害して、標的の組織へサプライチェーン攻撃を仕掛けることだったのではないかと推測しています。実際GitHub社も、高度な標的型攻撃を行っていたのではないかという分析結果を報告しています [13]。

本事件では、GitHub社がGitHubで公開しているリポジトリを調査した限りでは、ソースコードの改ざんや不審なファイルは見つかりませんでした。しかしGitHubのプライベートリポジトリは所有者がアクセスを制限しているため、調査できません。攻撃者が侵入可能なプライベートリポジトリ内のソースコードを改ざんしているおそれは拭いきれません。

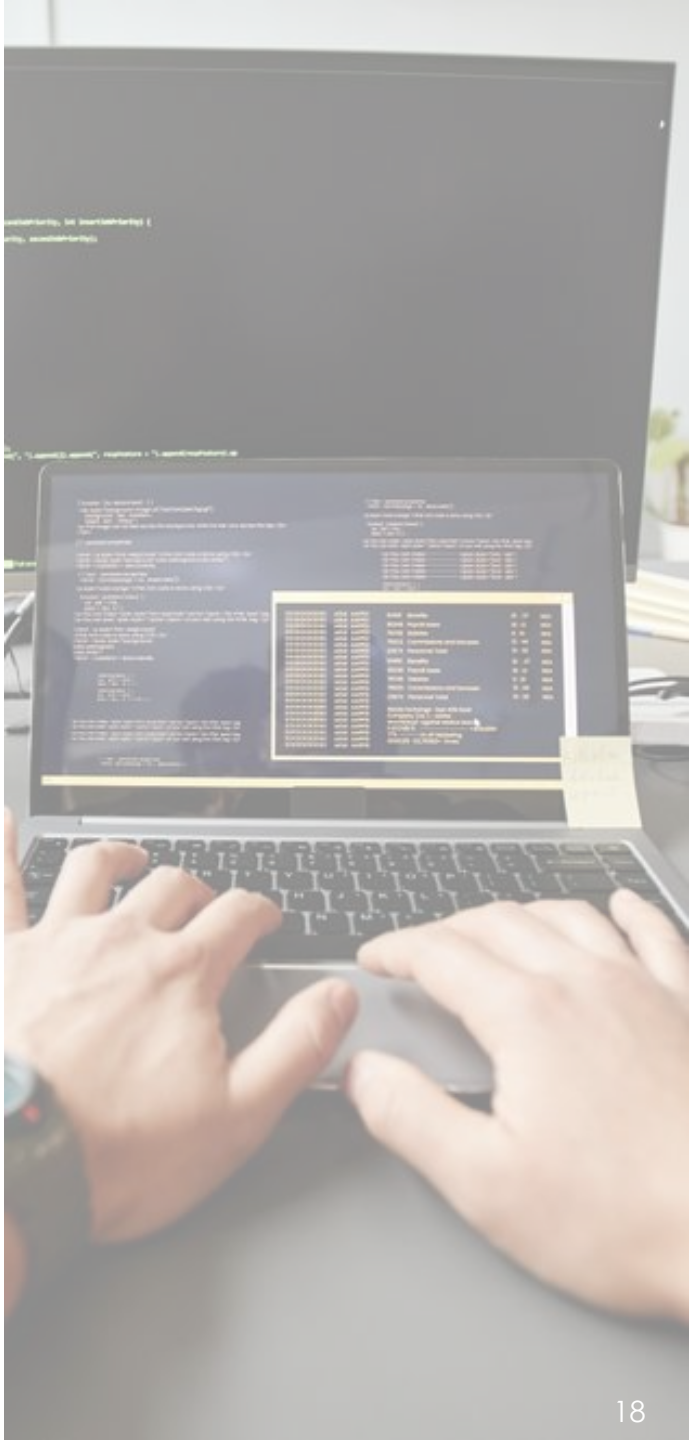
## 4.4. 開発環境を狙ったサプライチェーン攻撃

攻撃者がGitHubのような開発環境を足がかりにしてソフトウェア・サプライチェーン攻撃をおこなった場合に備えて、ソフトウェア開発企業はどのような対策を講じておくべきか、以下で解説します。

### （1） 開発環境で発生した類似インシデントとの比較

**4.3**で述べたように、GitHub社は、公開リポジトリからは改ざんなどの被害が見つかっていないと発表しています。GitHub社が調査した範囲だけであれば、GitHubへ不正アクセスされて、公開しているリポジトリの情報が窃取されただけで、それ以上の被害が発生していないことになります。この場合と類似の事件として、2021年度第1四半期のグローバルセキュリティ動向四半期レポート [18]で取り上げたメルカリ社の事件があります。メルカリ社の事件 [18]は、攻撃者がCodecovという開発者用のクラウドサービスを攻撃して、そこから同サービスの利用者の開発環境内へ芋づる式に侵入しようとしたソフトウェア・サプライチェーン攻撃です。メルカリ社の事件では、攻撃者はメルカリ社の本番環境へ侵入できず、ソースコードへバックドアやWebスキミングを仕込んだプログラムのデプロイは成功しませんでした。

しかし本事件では、GitHub社がチェックできないプライベートリポジトリには、攻撃者がバックドアを仕込んだプログラムが存在する危険性をはらんでいます。もしバックドアを仕込んだ製品をデプロイして、複数組織へ侵害が広がっているとしたら、類似の事件として2020年度第3四半期のグローバルセキュリティ動向四半期レポート [19]で取り上げたSolarWinds社の事件があります。SolarWinds社の事件 [19]では、攻撃者がSolarWinds社の開発環境へ侵入して、運用監視ソフトウェアのOrion Platformのソースコードへバックドアを仕込んで、デプロイしました。複数のユーザ企業は、そのバックドアを含んだOrion Platformのアップデートプログラムをダウンロードしてインストールしてしまい、攻撃者がバックドアからユーザ企業へ侵入して被害が発生しました。つまりOAuthトークン漏えいの本事件は、GitHub社がリポジトリでの改ざんが無いと発表しているのでメルカリ社の事件のタイプのように見えますが、GitHub社が調査できないプライベートリポジトリで改ざんが発生していて、それを気づかずにプログラムをデプロイしている場合は、SolarWinds社の事件のようにソフトウェア・サプライチェーン攻撃に発展しているおそれがあります。



### （2） 開発環境を狙ったソフトウェア・サプライチェーン攻撃の対策

そこで2つの過去の事件を参考に、開発環境や本番環境を狙ったソフトウェア・サプライチェーン攻撃へのセキュリティ対策を提案します。

ソフトウェア・サプライチェーン攻撃に対する対策は複数ありますが、まず重要な対策は本番環境への侵害を防ぐことです。過去の事件でも、本番環境への侵入を防止して被害を抑えることができています。そのため、攻撃者が本番環境へ侵入できないように、接続できる対象を制限したり、アクセス制御をしたりするべきです。本番環境だけを強固にしたとしても、DevOpsな環境では、開発環境へ侵入できてしまえば、ソースコードを改ざんして本番環境へバックドアやマルウェアを含んだプログラムをデプロイできてしまいます。そうすると、攻撃者は本番環境へも侵入できるようになります。そのため、開発環境に対しても、まずは適切な接続制限やアクセス制御が必要です。GitHub社が今後必須化すると発表している多要素認証を使ったなりすまし防止も、DevOps環境には有効な対策です。上記の対策をしていても、不正アクセスできてしまうこともあります。その場合、ソースコードが改ざんされていないか、プログラムにバックドアやマルウェアが忍び込んでいないか、プログラムをリリースする前に発見できれば大事には至りません。きちんと変更管理やレビューのプロセスを整えてチェックすれば、リリース前のソースコードの改ざんや不正なコードを見つけることができるでしょう。

ここに挙げた対策は、英国・国家サイバーセキュリティセンター(NCSC：National Cyber Security Centre)の「安全な開発と展開のためのガイダンス」内の「コードリポジトリ保護のための10のガイダンス」の５番、７番、８番です [20] [21] [22]。これら以外にも、有効な対策がわかりやすくまとまっています。他にも、導入する製品・サービスの管理体制やインシデント対応体制を整備するなど、幅広い運用やリスク管理の対策も必要です。こういった様々な対策は公的機関が文書を公開しています。アメリカ国立標準技術研究所（NIST：National Institute of Standards and Technology）はサプライチェーンのリスク管理に関する文書 「SP800-161」、欧州ネットワーク情報セキュリティ機関（ENISA：The European Union Agency for Cybersecurity）はサプライチェーン攻撃の分析結果と対策方法をまとめた「Threat Landscape for Supply Chain Attacks」を公開しているので、これらに記載している対策も実施することが大切です。

## 4.5. まとめ

OAuthトークン漏えい事件は、攻撃者がサードパーティ製のアプリケーションから多数の認証情報を取得して、その中からプライベートリポジトリの複数の組織を侵害しようとしたと推測すると、大規模なソフトウェア・サプライチェーン攻撃だったと思います。そして、GitHubと連携しているサードパーティ製アプリケーションから認証情報 OAuthトークンを盗む手口やクラウド上のDevOps環境を狙った手口、改ざんしたソフトウェアを配布してソフトウェア・サプライチェーン攻撃を仕掛ける手口、それらを組み合わせているため、複雑で高度なサイバー攻撃です。しかし、メルカリ社の事件やSolarWinds社の事件から、OAuthトークン漏えい事件を未然に防ぐセキュリティ対策方法を知ることができます。つまり複雑で高度なサイバー攻撃であっても、決して防ぐことができない攻撃ではありませんでした。

ソフトウェア開発企業は、他の高度なインシデントを参考にしたり、「安全な開発と展開のためのガイダンス」の「コードリポジトリ保護のための10のガイダンス」などの公的機関のセキュリティ対策ガイドを参考にしたりしてセキュリティ対策を強化して、OAuthトークン漏えい事件からソフトウェア・サプライチェーン攻撃へ発展するようなサイバー攻撃に対抗していかなければなりません。

# 5 脆弱性
# Internet Explorer11のサポート終了に伴う、セキュリティリスクと対処法

2022年6月16日（日本時間）をもって、Microsoft社が提供するWebブラウザ Internet Explorer11 デスクトップアプリケーション（以下、「IE11」という）のサポートが終了しました。サポート終了後はセキュリティ更新プログラムの提供がなくなり、セキュリティリスクが高まる恐れがあります。本章では、IE11のサポート終了に伴う、ユーザおよび企業が受ける影響とセキュリティリスク、リスクに対する対策を解説します。

## 5.1. 約27年の歴史に幕、IEサポート終了に伴う影響と対策とは

IE11とは、Microsoft社が開発・提供しているWebブラウザです。1995年にインターネットが普及するきっかけともなったWindows 95の拡張機能として、初代IEの提供を開始しました。以来、Windows標準のWebブラウザとしてインターネットを牽引し、2000年頃にはIEは市場の9割以上を占めるWebブラウザとなっています [23]。

ではなぜ2022年現在、IEはサポート終了に至ったのでしょうか。一つの理由として、Webブラウザ関連技術の標準化団体「W3C（World Wide Web Consortium）」の規格にIEが準拠しなかったことが挙げられます。Microsoft社は、IEの脆弱性が見つかるたびに、更新プログラムを提供して対応していきましたが、更新プログラムや独自機能が追加されるたびに動作が重くなるなど問題が生じてきました。一方、W3Cの標準規格に準拠したWebブラウザが続々とインターネットに登場し、IEのユーザビリティに不満を持ったユーザが、シンプルで動きが速く更新も頻繁に実施するGoogle Chromeなどに流れ、徐々にシェアを下げました。その結果、IEの市場シェアが低下して、2015年にMicrosoft社はIEの開発を終了し、IEの後継のWebブラウザとなるMicrosoft Edgeを発表しました。Edgeは、W3C標準規格に準拠しています。そして2022年6月15日をもってMicrosoft社はIE11のサポートを終了し、IE11との完全な互換性を持つ「Internet Explorer モード」（以下、「IEモード」という）を搭載したMicrosoft Edgeが正式にWindows標準のWebブラウザとなりました。

**表5-1：OS ごとの IE11 / IEモードサポート終了スケジュール [24]**

| OS version | アプリケーション | サポート期限 |
|---|---|---|
| Windows 7 | IE<br>IEモード | 2020年1月※<br>2022年1月 |
| Windows 8.1 | IE / IEモード | 2023年1月 |
| Windows 10 Enterprise Version 20H2 | IE<br>IEモード | 2022年6月<br>2023年5月 |
| Windows 10 Enterprise Version 21H1 | IE<br>IEモード | 2022年6月<br>2022年12月 |
| Windows 10 Enterprise Version 21H2 | IE<br>IEモード | 2022年6月<br>2024年6月 |
| Windows 11 Enterprise Version 21H2 | IEモード | 2024年10月 |
| Windows 11 Enterprise Version 22H2 | IEモード | 2025年10月 |
| Windows 10 Enterprise 2015 LTSB | IE / IEモード | 2025年10月 |
| Windows 10 Enterprise 2016 LTSB | IE / IEモード | 2026年10月 |
| Windows 10 Enterprise LTSC 2019 | IE / IEモード | 2029年1月 |
| Windows 10 Enterprise LTSC 2021 | IE / IEモード | 2027年1月 |
| Windows Server 2012 | IE / IEモード | 2023年1月 |
| Windows Server 2016 | IE / IEモード | 2027年1月 |
| Windows Server 2019 | IE / IEモード | 2029年1月 |
| Windows Server, version 20H2 | IE / IEモード | 2022年8月 |
| Windows Server 2022 | IE<br>IEモード | 2031年1月<br>2029年1月 |
| Windows Server 2022 | IE<br>IEモード | 2031年1月<br>2029年1月 |
| Windows 7 | IE<br>IEモード | 2020年1月※<br>2022年1月 |
| Windows 8.1 | IE / IEモード | 2023年1月 |

※ Windows 7は、2020年にOSのサポートを終了しています。ただし、組織が法人向け延長セキュリティプログラムのESUライセンスを購入している場合、2023年1月までOSのサポートを延長します。この場合、IE11 デスクトップアプリケーションもOSのサポート期限に合わせて、2023年1月までサポートを延長します。

### 5.1.1. 影響を受ける対象

今回のサポート終了の対象は、Version 20H2以降のWindows 10 クライアント SKU、およびVersion 20H2以降のWindows 10 IoTに搭載しているIE11です [24]。一方、Windows7、Windows 8.1、 Windows 10 LTSC/LTSB、Windows Serverに搭載しているIEは、まだサポート終了ではありません。それぞれのオペレーティングシステムのサポート終了日まで、IEのサポートを継続する予定です。

また、それぞれのOS上のMicrosoft Edgeへ搭載したIEモードは、そのOSのライフサイクルにあわせてサポートを終了します。Microsoft社は、OSのサポート終了が2029年以降の場合、すくなくとも2029年までIEモードのサポートを継続すると発表しています。2029年以降のIEモードのサポート終了日は未定であり、サポート終了日の1年前にはMicrosoft社より告知があります。

### 5.1.2. サポート終了後のIEのセキュリティリスク

2019年2月に投稿されたMicrosoft社の公式ブログでは、IEをデフォルトのWebブラウザとして使用することは危険だとして最新のWebブラウザを利用するよう勧告しています [25]。同社のサイバーセキュリティアーキテクトであるChris Jackson氏は、IEを使い続けることによって、企業は「技術的負債」を持つことになると述べています。2015年にIEの開発を停止したにも関わらず、企業はいまだにIEの利用を継続しています。世界のWebブラウザシェア調査サービスStatcounterによると、サポートが終了した2022年8月時点でも、日本では1.71%の人がIEを使用しています [23]。10年前のIEのシェア50%以上から徐々にその割合は下がっているものの、2022年8月時点のグローバルのIEの使用率0.79%と比較して、日本は未だIEのシェアが一定数残っていることがわかります。

図 5-1: 日本におけるデスクトップブラウザシェア率の推移 [23]

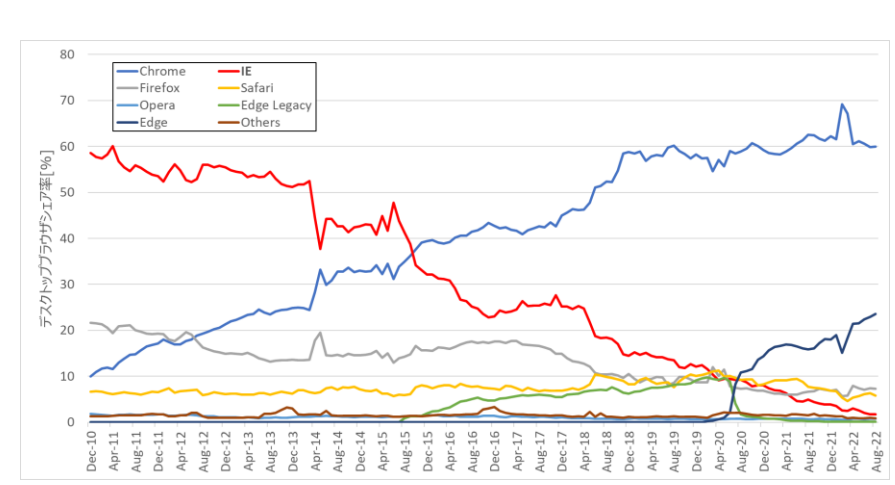
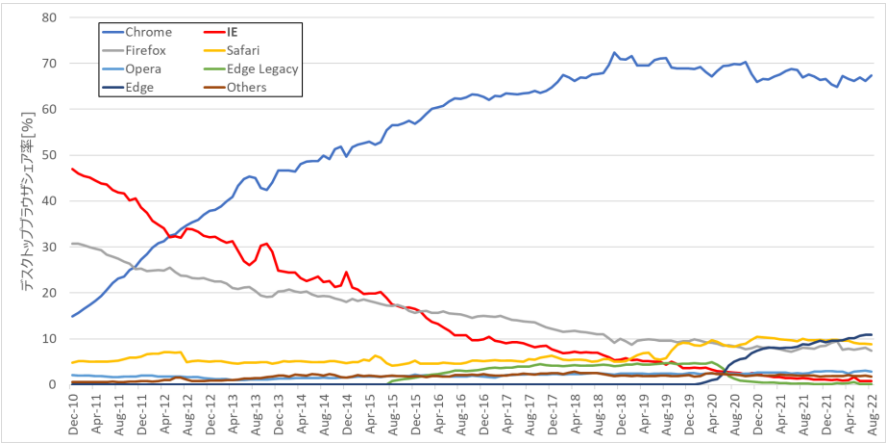



図 5-2: 世界におけるデスクトップブラウザシェア率の推移 [23]



日本のIEのシェアが一定数残る要因の一つとして、IEでアクセスすることを前提に開発した業務システムやWebアプリケーションの存在が挙げられます。インターネット初期から高いシェアを誇っていたIEは、多くの業務システムのユーザインタフェースに採用されました。IEを他の最新のWebブラウザへ変更すると、システムが正常に動作しない懸念や、動かなくなった機能の代わりに業務オペレーションを変更して現場に負担がかかるおそれもあります。移行コストの問題やリソース不足から、IEからMicrosoft Edgeや他のWebブラウザへの移行作業を後回しにしているかもしれません。そのような理由で、企業がいまだにIEを使い続けているおそれがあります。

しかしながら、サポート期限切れのIEを使い続けることは、セキュリティリスクが伴います。セキュリティリスクの代表格として挙げられるのが、ゼロデイ脆弱性やゼロデイ攻撃です。ゼロデイ脆弱性とは、ソフトウェアの開発元がパッチや更新プログラムを提供できていない脆弱性で、ゼロデイ脆弱性を悪用した攻撃がゼロデイ攻撃です。ゼロデイ脆弱性は、あらゆるWebブラウザやアプリケーションで生じる確率があります。既にサポートが終了しているIEは、脆弱性が発覚しても更新プログラムが提供されないため、ゼロデイ攻撃を受けるリスクが特に高まります。Webブラウザを悪用した攻撃の例としては、悪意あるウェブサイトにアクセスすると、スパイウェアやランサムウェアなどの不正なプログラムをWebブラウザ経由でダウンロードさせて感染させるドライブバイダウンロード攻撃や、攻撃ターゲットがよくアクセスするサイトを改ざんしてマルウェアに感染させる水飲み場攻撃などが挙げられます。

IEのゼロデイ脆弱性を悪用してマルウェアが企業のユーザのマシンへ侵入した場合、情報漏洩や不正アクセス、ランサムウェアによる被害が発生したり、他の攻撃の踏み台として悪用されたりするおそれがあります。すでにサポート切れとなっているIEは、攻撃の標的となりやすい上、脆弱性が発見されてもセキュリティパッチが出ないため攻撃が成功する確率が高くなります。セキュリティインシデントの発生によって、事後対応に多大な費用がかかることは想像に容易いですが、企業のブランドイメージへも大きな悪影響を及ぼすことも忘れてはなりません。Microsoft社によるサポートが既に終了しているIEを継続利用したために発生したインシデントとなると、社会的な信頼性の低下やビジネスへの損害は測り知れません。長期的な目線で見ると、サポート切れのIE11を使い続けるリスクは大きく、万が一インシデントが発生した場合、移行コストを上回る多大な被害コストを生じるおそれがあります。

### 5.1.3. 求められる対策

本節では、Microsoft社によるIEのサポート終了に伴って必要になるセキュリティ対策について述べます。企業の従業員/一般ユーザおよびシステム管理者/ウェブサービス事業者は、以下の対策を実施してください [26]。

#### （1） 企業の従業員 / 一般ユーザ

Microsoft社によると、2022年6月15日のWindows 10のIEのサポート終了後は、月例累積更新プログラムを適用していれば、Windows 10のIEを起動してWebページを表示しようとすると自動的にMicrosoft Edgeにリダイレクトする仕様になります。ただし、自社のWindowsドメインへ参加している場合は、グループポリシのIE無効化ポリシの有無にしたがうため、上記の自動リダイレクトをしない場合があります [24]。その場合は、IE11を使用せず、別のWebブラウザを利用するようにしましょう。IE11でWebコンテンツを閲覧したい場合は、Microsoft EdgeのIEモードを使えば、IE11と同様の処理でWebコンテンツを閲覧できます。IEモードを使用するためにはIE11のMSHTMLエンジンが必要なので、IE11をアンインストールまたは削除しないよう注意点してください。

#### （2） システム管理者 / ウェブサービス事業者

システム管理者やウェブサービス事業者は、IE11を使っている利用者へ、サポート終了後は標準WebブラウザをMicrosoft Edge/Google Chrome/Safari/Firefox等のサポートが継続している最新のWebブラウザに変えるように周知しましょう。またシステム管理者やウェブサービス事業者は、自社内にIE11でのみ閲覧・動作するシステムやWebサイト、業務アプリケーションの有無を確認し、あれば代替のWebブラウザで正常動作するようシステム担当者や開発者へ改修を依頼しましょう。またシステム管理者は、IE11からの移行準備が整い次第、自社のWindowsドメインのグループポリシへIE無効化ポリシを設定してから、社員へWindowsの月例累積更新プログラムの適用を指示して、IE11を無効化しましょう。注意点は、IEモードのサポート期限です。Microsoft社は、IEモードとして残ったIEのMSHTMLエンジンのサポートを継続します。しかしながら、Microsoft社は、IEモードを2029年までサポートすると案内していますが、それ以降は未定のため、IEモードを用いたIEコンテンツが閲覧できなくなるおそれもあります。早めにコンテンツの改修とWebブラウザの移行を進めましょう。

## 5.2. まとめ

サポートが終了し、今後プログラムを更新しないサービスやアプリケーションを使い続けることには、ゼロデイ攻撃のリスクが伴います。インターネット初期から長い間、ユーザや企業が幅広く利用してきたMicrosoft社のWebブラウザ IE11のサポート終了は、特に企業にとって早急に対応すべき課題です。IE11は、社内の業務アプリケーションのインタフェースとして広く使用されてきた背景から、最新のWebブラウザへの移行は容易ではないかもしれません。しかし、IE11に関係したインシデントが一度でも発生してしまうと、被害額、インシデント対応のコスト、社会的な信用を失うことによる機会損失などのビジネスへの悪影響は計り知れません。システム管理者やウェブサービス事業者は、自社内にIE11でのみ閲覧・動作するシステムが残っているかどうか、調査しましょう。残っていた場合には、システム担当者や開発者へ速やかにシステムの改修を呼びかけ、最新のWebブラウザへ対応したシステムへ移行してください。可能であれば、移行完了後はIE無効化ポリシを適用して、IE11を無効化しましょう。

# 6 マルウェア・ランサムウェア
# 中小企業で増加するランサムウェア被害

ランサムウェアは依然、大きな脅威となっています。ニュースで大企業や重要インフラのランサムウェア被害を取り上げて注目を集めていますが、実際は業種や企業規模を問わずに被害が発生しており、誰もが自分事として捉えなければならない脅威です。特に、大企業と比較してセキュリティ対策が不十分である中小企業は、ランサムウェア被害が増加しており、早急にランサムウェア対策を含めたセキュリティ対策全般を推進するべきです。本稿では、中小企業にランサムウェア被害が多い原因を考察した後に、ランサムウェア対策を行うにあたって中小企業が取ることのできるアクションを示します。

## 6.1. 中小企業におけるランサムウェアの概況

### 6.1.1. 増加する中小企業のランサムウェア被害

情報処理推進機構（IPA）が発表した「情報セキュリティ10大脅威（組織）」 [27]では、前年に引き続き「ランサムウェアによる被害」が1位になりました。また警察庁のレポート [28]によると、ランサムウェア被害件数は令和2年下半期から右肩上がりで増加しています（図 6-1）。このことからも、2022年もランサムウェアの被害は増加していくと予想します。

このような中、中小企業のランサムウェア被害が増加しています。警察庁のレポート [28]によると、令和3年度に警察庁が把握したランサムウェア被害は146件あり、そのうち79件(54%)が中小企業の被害でした（図 6-2）。ExtraHop社が行った組織のサイバーセキュリティに関する調査 [29]では、調査を受けた組織の20%が仮にサイバー攻撃を受けたとしても公表しないと回答しています。また、中小企業は大企業と比べてインシデント対応ルールが整備できていない傾向があると考えられ、大企業と比べて被害を報告していない事例が多く存在すると予想します。よって、実際の中小企業のランサムウェア被害の件数は、警察庁の報告よりも多いと予想します。

また同レポートでは、ランサムウェア被害を受けた企業のうち、復旧費用に1000万円以上の費用を要した企業が43%あり、復旧期間に2か月以上を要した企業が存在していたことも報告しています。

ランサムウェア被害は自社のシステムが停止して事業活動が停止するだけでなく、情報漏えいや取引先への被害の拡大など、2次被害が起きる恐れもあります。実際に、身代金の支払いに応じなければ窃盗した情報を公開する、と恐喝する二重恐喝が横行しており、漏えいした個人情報の公開は、その企業の信用失墜につながりかねません。近年では、二重恐喝から更に恐喝を行う四重恐喝という手口も出てきています。四重恐喝とは、二重恐喝に加えて、DoS攻撃によるサービス停止を示唆したり、被害者の顧客やビジネスパートナー、従業員に連絡を取ることで身代金の支払いを促したりする恐喝方法です。これらは、明らかに事業の存続や企業の信用に悪影響を及ぼします。つまり、一度ランサムウェアに感染してしまうと、身代金の支払いを行わなくとも大きな被害が出てしまう恐れがあります。特に、大企業よりも企業体力が低い中小企業は、ランサムウェア攻撃の被害や多大な復旧費用は事業の存続を脅かします。

図 6-1:
ランサムウェア被害件数の推移 [28]

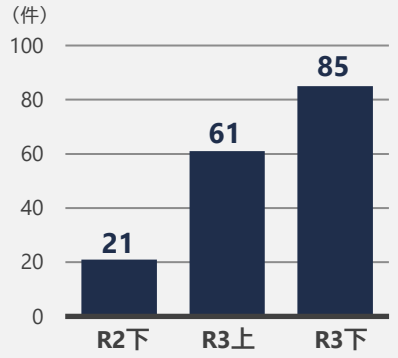
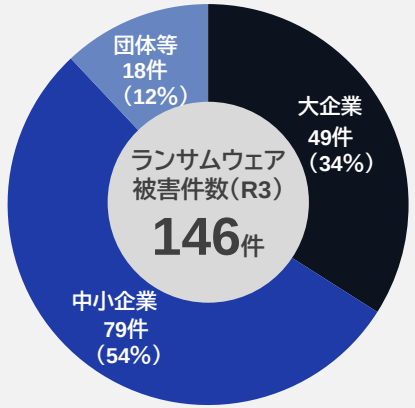



図 6-2:
ランサムウェア被害企業・団体等の規模別報告件数 [28]



### 6.1.2. 中小企業のランサムウェア事例（2022年第1四半期）

2022年度第1四半期も、中小企業のランサムウェア被害が複数報告されています（表 6-1）。どの被害事例も、業務に多大な影響を与えるまでには至っていませんでした。しかし、攻撃者はサーバ内への不正アクセスを行っているため、6.1.1項で述べた2次被害の発生や企業の信用低下といったリスクが残ります。こうしたリスクを発生させないためにも、中小企業は早急にセキュリティ対策を推進するべきです。

**表6-1：2022年度第1四半期の中小企業の主なランサムウェア被害事例**

| # | 発生の日付 | 被害者 | 従業員数 | インシデントの概要 |
|---|---|---|---|---|
| 1 | 4月2日 | 株式会社<br>月桂冠 | 365名 | 同社は不正アクセスによるランサムウェア攻撃を受け、お客様の情報を含めた多数の個人情報が流出した恐れがあると発表した [30] |
| 2 | 4月8日 | 京成建設<br>株式会社 | 326名 | 同社が運用するサーバが不正アクセスを受け、一部のデータが暗号化されたと発表した [31] |
| 3 | 5月11日 | 理研農産化工<br>株式会社 | 210名 | 同社はサーバ内のデータが暗号化され、社内システムが停止したと発表した。5/12より業務は再開しているが、基幹システムの全面復旧には時間を要すると説明している [32] |
| 4 | 6月1日 | 株式会社<br>アイウエア | 63名 | 同社が運営する帰国生向けサービスJOBAの運用サーバへランサムウェアとみられる攻撃があり、内部のデータが暗号化される事態が発生した [33] |

### 6.1.3. 半田病院の事例

中小企業が適切なセキュリティ対策を行っていなかったために、ランサムウェア被害が発生してしまった事例を紹介します。2021年10月31日未明に、徳島県つるぎ町立半田病院の電子カルテシステムなどの主要情報システムが、ランサムウェアに感染してファイルを暗号化された結果、約2か月にわたってシステムが利用不可能になりました。業務の縮小により病院業務は維持できたものの、システムの代わりに手作業での対応を余儀なくされたため、患者及び地域の医療体制に多大な影響を与えました。2022年6月16日に、半田病院は有識者会議がインシデントの経緯などをまとめた調査報告書 [34]を公開しました。

報告書をもとに、インシデントの原因を紐解きます。主な原因は、セキュリティ対策を推進する人員がいないことでした。半田病院はIT担当者が一人しかおらず、適切なセキュリティ対策を講じる余裕がありませんでした。その結果、システムの設計や構築、運用保守を委託事業者に丸投げすることとなったこと、委託元と委託先の責任範囲が曖昧であったことから、脆弱性を放置して攻撃者がサイバー攻撃できる隙を生み出してしまいました。また人員不足の背景には、予算が不足しているという原因も存在しています。自治体病院の予算策定では、なによりも利益改善することを求めており、まだ発生していないセキュリティ事故に対して予算を確保することは困難であったと思います。

半田病院の事例からは、セキュリティ対策を行うリソースがない、そしてその背景として経営層がセキュリティ対策の重要性を理解していないという原因があったと考えます。

## 6.2. なぜ中小企業なのか

### 6.2.1. 中小企業の被害が多い背景

6.1節では、近年、中小企業でランサムウェア被害が増加していると述べました。そこで本章では、ランサムウェア攻撃が中小企業を狙う理由を考察します。

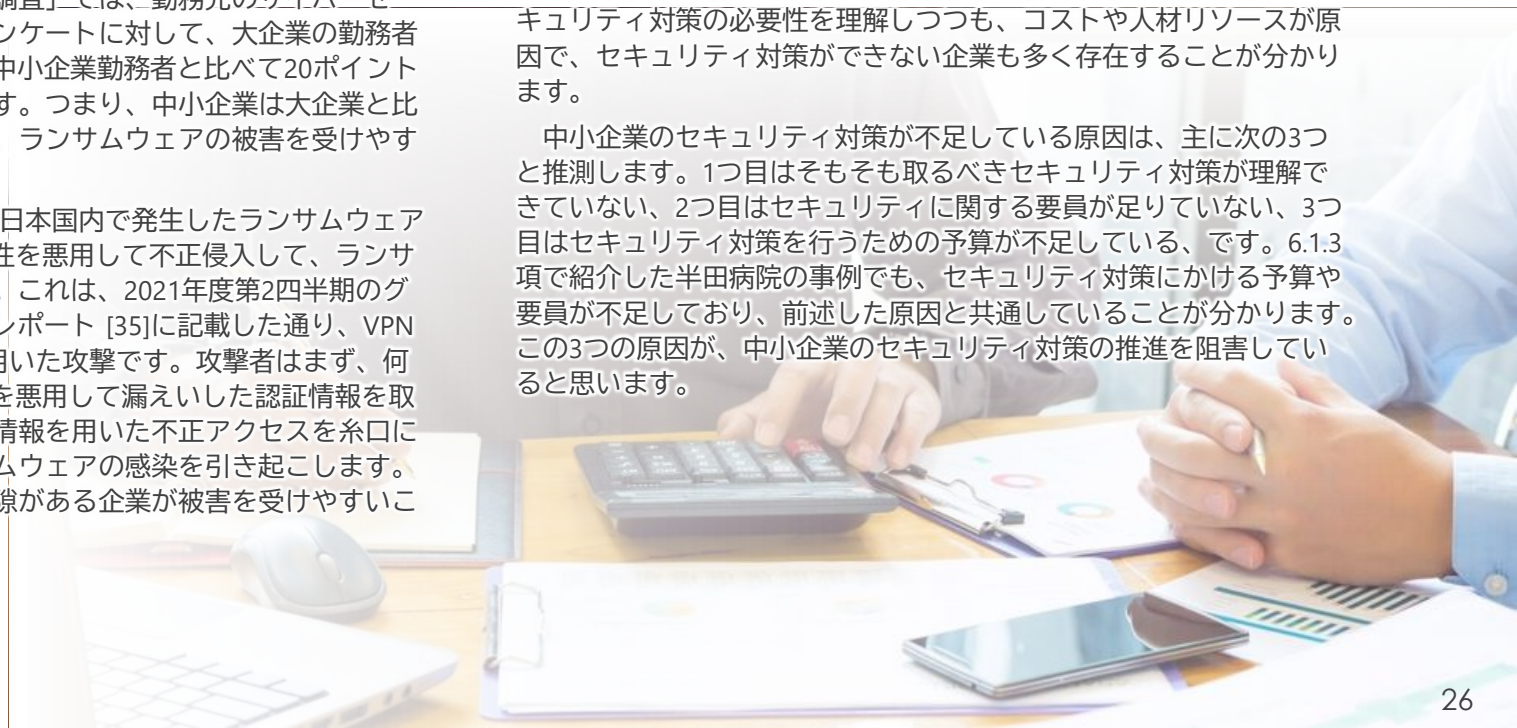
攻撃者の視点で、中小企業を狙う原因を考えてみます。攻撃者の主な目的は、金銭を得ることです。最終的に金銭を得ることができるのであれば、業種や企業規模を問わず、攻撃対象になりえます。つまり、攻撃者は特定の業種や企業規模を対象にしておらず、さまざまな組織をランサムウェア攻撃しています。結果的にセキュリティ対策に隙のある企業でランサムウェア攻撃が成功して被害が発生してしまいます。ここでいう隙とは、IT機器やソフトウェアの脆弱性の放置、セキュリティ教育を実施しておらず従業員のセキュリティリテラシーが不十分であることなどを指します。また、日経BPコンサルティングが行った「勤務先のサイバーセキュリティ調査」では、勤務先のサイバーセキュリティ対策の実現度を問うアンケートに対して、大企業の勤務者で「できている」と答えた割合は中小企業勤務者と比べて20ポイント近く高かったという結果があります。つまり、中小企業は大企業と比べて攻撃する隙のあることが多く、ランサムウェアの被害を受けやすいと考えられます。

例えば、令和3年度(2021年度)に日本国内で発生したランサムウェア被害の主な攻撃方法はVPNの脆弱性を悪用して不正侵入して、ランサムウェアを感染させる方法でした。これは、2021年度第2四半期のグローバルセキュリティ動向四半期レポート [35]に記載した通り、VPN装置FotiGateの脆弱性を間接的に用いた攻撃です。攻撃者はまず、何者かがVPN装置 FotiGateの脆弱性を悪用して漏えいした認証情報を取得します。そして、取得した認証情報を用いた不正アクセスを糸口にして、侵入したシステムでランサムウェアの感染を引き起こします。このように、脆弱性の放置などの隙がある企業が被害を受けやすいことが分かります。

### 6.2.2. 中小企業のセキュリティ対策が不足している原因

では、なぜ中小企業では大企業と比べてセキュリティ対策が不足している傾向にあるのでしょうか。2021年度中小企業における情報セキュリティ対策に関する実態調査 [36]では、33.1%もの中小企業が、過去3期において情報セキュリティ対策投資を行わなかったと回答しました。また、それらの企業に対して情報セキュリティ投資を行わなかった理由も調査しています。結果は、「必要性を感じていない（40.5%）」と回答した企業が最も多く、「費用対効果が見えない（24.9%）」、「コストがかかりすぎる（22.0%）」、「どこからどう始めたらよいかわからない（20.7%）」が続いています。「必要性を感じていない」と「費用対効果が見えない」という回答が多いところを見ると、やはりまだまだセキュリティ対策の重要性を理解していない企業が多いことがわかります。一方、「コストがかかりすぎる」や「どこからどう始めたらよいか分からない」という回答からは、セキュリティ対策の必要性を理解しつつも、コストや人材リソースが原因で、セキュリティ対策ができない企業も多く存在することが分かります。

中小企業のセキュリティ対策が不足している原因は、主に次の3つと推測します。1つ目はそもそも取るべきセキュリティ対策が理解できていない、2つ目はセキュリティに関する要員が足りていない、3つ目はセキュリティ対策を行うための予算が不足している、です。6.1.3項で紹介した半田病院の事例でも、セキュリティ対策にかける予算や要員が不足しており、前述した原因と共通していることが分かります。この3つの原因が、中小企業のセキュリティ対策の推進を阻害していると思います。



## 6.3. 中小企業のセキュリティ対策を推進するには

6.2節で中小企業のランサムウェア被害が増加している原因は、中小企業のセキュリティ対策が不十分であると考えました。ランサムウェア被害にあわないために、セキュリティの重要性を理解し、セキュリティ対策を推進するべきです。中小企業ではセキュリティ対策を阻害する原因として、「取るべきセキュリティ対策が分からない」「人材不足」「予算不足」という3つがあると推測しました。本節では、中小企業のセキュリティ対策の推進を阻害している3つの原因の解決案を示します。

### （1）取るべきセキュリティ対策が理解できていない場合

中小企業で実際にセキュリティ対策を実施する担当者は、自社のセキュリティを改善するために何をどう行えばよいか、分かっていません。サイバー攻撃から会社を守るためのセキュリティ対策は、無数にあります。担当者は、その中から効果や実現可能性を考慮して、自社に合ったセキュリティ対策を取捨選択しなければなりません。そのためにはセキュリティリスクアセスメントを行い、自社のリスクを洗い出したうえで、それらのリスクに対応するセキュリティ対策を策定、そして実施していくといった流れを行います。こういった流れを実際に推進していくためには、セキュリティに対する知識や経験が重要となってきます。中小企業では、セキュリティ担当者のセキュリティに対する知識や経験が不足していることが、セキュリティ対策の推進を阻害する一つの原因であると考えます。

経験不足の解決策の一つとして、IPAが公表している中小企業の情報セキュリティ対策ガイドライン [41]を活用すると良いでしょう。このガイドラインはセキュリティに対する知識や経験がない人でも企業それぞれの事情に適したセキュリティ対策を推進できるように、対策を実践する際の具体的な手順や手法をまとめています。このガイドラインでは、セキュリティ対策を推進するための4つのステップ示しています。ステップ1では、これまで情報セキュリティを全く行っていなかった中小企業へ、最低限必要な5つの対策を示しています。ステップ2では、自社のセキュリティの現状を把握して、セキュリティ対策が不足している部分への対策を指示しています。ガイドラインには、ステップ2を進めるための様式集を添付しているため、リスク分析の経験が少ない方でも取り組みやすくなっています。ステップ2まで行うと、これまでセキュリティ対策をおこなっていなかった中小企業は、大幅な改善ができます。ステップ3では、より本格的なセキュリティ対策として、まず自社に合った情報セキュリティ規程を策定します。そして、策定した規定を順守してもらうために従業員に周知と教育を行います。その後、規程内容が順守されているかの確認と評価を行い、必要に応じて改善を指示します。ステップ3は、より高度な情報セキュリティ対策の作業が発生しますが、こちらも様式集があるため、様式集を自社に合わせて追記、修正から始めていきましょう。ステップ4では、さらにセキュリティを強固にするための追加対策の実施方法を説明しています。ステップ3まで実施できた中小企業の担当者は、自社に必要な追加対策を実施できます。

セキュリティ対策の策定、改善を継続的に行っていくためには、中長期的な視点で担当者をセキュリティ人材として育てることも重要です。中小企業に最低限必要な人材は、企業の情報セキュリティを統括できる人材だと考えます。具体的には、セキュリティポリシーの策定や従業員のセキュリティ教育、経営層への啓発などを主導できることが必要です。なぜなら、これらの業務は各企業の特性と密接に関係しており、自社への理解が強く求められるためです。一方、ログの解析やセキュリティ製品の実装、運用など技術的にセキュリティ対策を行う業務は高度な専門性が求められます。自社で人材を確保できない場合、後の（２）で述べるようなMSSや外部委託を活用するといった選択肢があります。

では企業のセキュリティを統括できる人材に育成するためには、どうすればよいでしょうか。そのような人材になるためには、セキュリティの幅広い知識と社内のセキュリティを推進する経験が必要だと考えます。セキュリティの幅広い知識を身に着けるためには、資格や教育プログラムを活用するとよいでしょう。情報処理安全確保支援士というセキュリティ知識全般を学べる資格や、IPAの中核人材育成プログラムという1年間かけてセキュリティを統括する人材を育成するプログラムなどがあります。セキュリティ対策を推進する経験は、実際にセキュリティポリシーの策定や社内教育などを業務として行いながら身に着けるとよいでしょう。中小企業の情報セキュリティ対策ガイドラインに沿った活動もよい経験となります。セキュリティ人材の育成には、知識の習得だけでも最低1年、そこから経験を積むことを考えると数年単位の時間がかかると考えます。未来の企業の安全のために少しずつ進めていきましょう。

### （2）人材が不足している場合

人材不足は多くの中小企業が抱える悩みです。人材がいなければ、（1）でセキュリティを統括できる人材を育成することもできません。セキュリティを統括する人材以外にも、実際にセキュリティ対策を実行していくにあたって、多様な人材も必要です。理想は、社内にサイバーセキュリティ人材育成の体制を作り、サイバーセキュリティ人材のキャリアアップの制度も用意することです。東京都では、中小企業に向けてサイバーセキュリティ人材の育成や社内の育成体制整備の支援を行っています [37]。また経済産業省は、企業がサイバーセキュリティの組織体制を構築し、必要な人材を確保するためのポイントをまとめた「サイバーセキュリティ体制構築・人材確保の手引き」 [38]を公開しています。予算や要員を準備できる中小企業であればこれらを活用し、サイバーセキュリティ人材の確保を行えばよいでしょう。しかし、これらの施策を行う余裕のない企業が多いと考えます。その場合は、マネージドセキュリティサービス（MSS）といった外部への作業委託を利用して、社内の人材不足を補うことができます。6.1.3の半田病院の事例では、外部委託先への業務の丸投げがインシデントの原因の一つでした。外部委託を契約する際は、業務実績の豊富さや外部認証（ISMS、Pマーク等）の取得有無といった選定基準を設けて委託先を選定したうえで、委託する業務内容を明確にしましょう。外部委託中は、業務を丸投げしないで、委託先の対応状況をチェックしてミスや遅れを指摘するなどの委託先の監督を行いましょう。

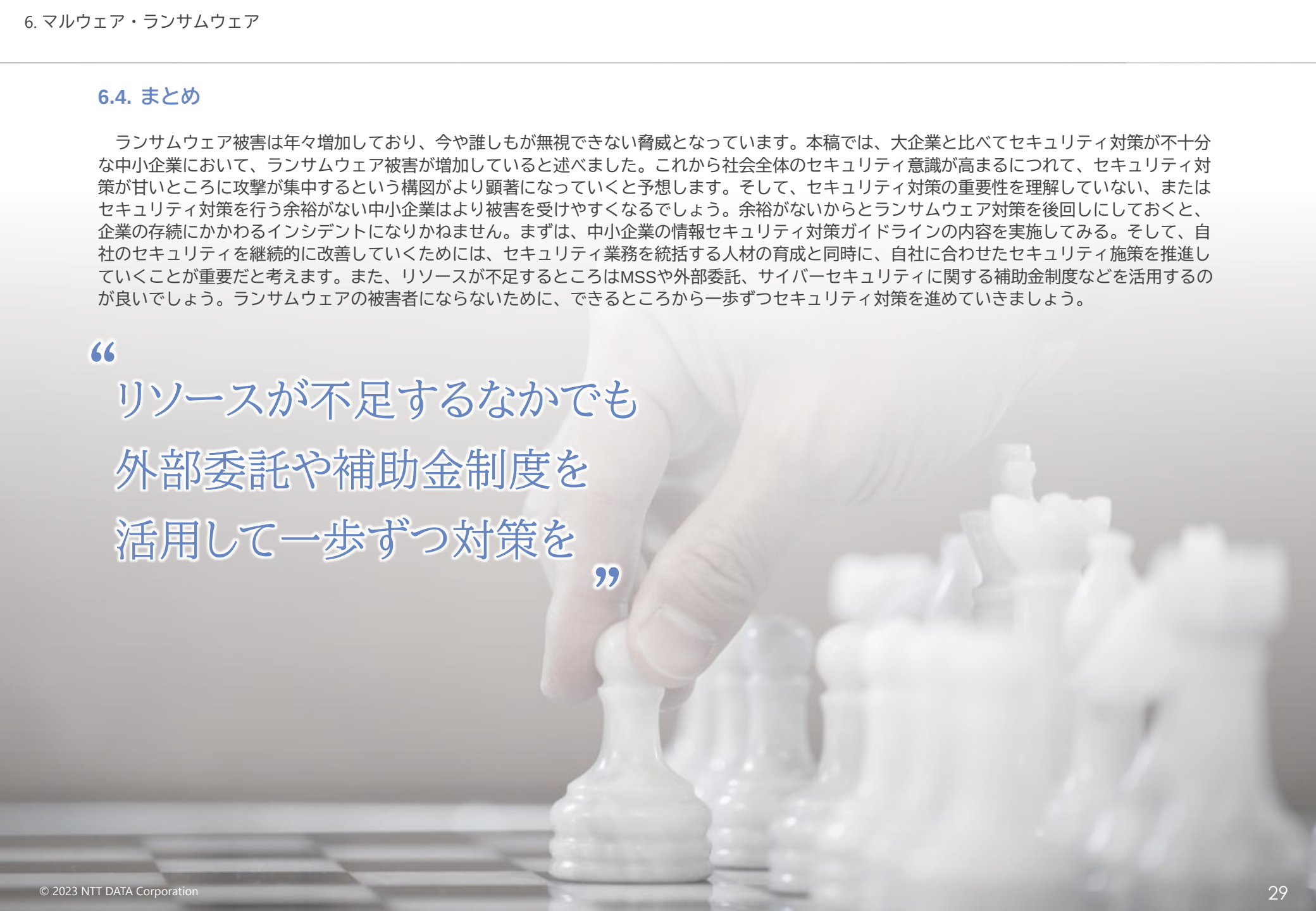
### （3）予算が不足している場合

人員不足は、予算不足も関係します。実際、6.2.2項で紹介した2021年度中小企業における情報セキュリティ対策に関する実態調査 [36]では、情報セキュリティ投資を行わなかった理由として「費用対効果が見えない」、「コストがかかりすぎる」といった意見が多くありました。解決策の一つとして、中小企業であれば機関や自治体から補助金を受けるという手段があります。東京都中小企業振興公社では、令和4年度に中小企業に向けて、サイバーセキュリティ対策促進助成金 [39]を支給しています。この助成金は、サイバーセキュリティ対策を実施するために必要となる機器等の導入、およびクラウド利用に係る経費を補助するものです。また経済産業省は、中小企業に対して、IT導入補助金セキュリティ対策推進枠 [40]というサイバーセキュリティ対策実施を支援する施策を行っています。これは、IPAが行っているサイバーセキュリティお助け隊サービスというセキュリティ対策サービスの利用料を補助するものです。中小企業であれば、これらの補助金を活用することが可能です。

そして補助金を獲得した後、セキュリティ対策の推進や継続的なセキュリティ対策予算の獲得のためには、経営層の理解を得るということが重要です。IT担当者は経営者に向けてサイバーセキュリティに関する地道な啓発活動を続けていく必要があります。

## 6.4. まとめ

ランサムウェア被害は年々増加しており、今や誰しもが無視できない脅威となっています。本稿では、大企業と比べてセキュリティ対策が不十分な中小企業において、ランサムウェア被害が増加していると述べました。これから社会全体のセキュリティ意識が高まるにつれて、セキュリティ対策が甘いところに攻撃が集中するという構図がより顕著になっていくと予想します。そして、セキュリティ対策の重要性を理解していない、またはセキュリティ対策を行う余裕がない中小企業はより被害を受けやすくなるでしょう。余裕がないからとランサムウェア対策を後回しにしておくと、企業の存続にかかわるインシデントになりかねません。まずは、中小企業の情報セキュリティ対策ガイドラインの内容を実施してみる。そして、自社のセキュリティを継続的に改善していくためには、セキュリティ業務を統括する人材の育成と同時に、自社に合わせたセキュリティ施策を推進していくことが重要だと考えます。また、リソースが不足するところはMSSや外部委託、サイバーセキュリティに関する補助金制度などを活用するのが良いでしょう。ランサムウェアの被害者にならないために、できるところから一歩ずつセキュリティ対策を進めていきましょう。



# 7 予測

## マイナンバーカードの事実上の義務化

政府は、2024年秋にも現在の健康保険証を原則廃止し、マイナンバーカードと一体となった「マイナ保険証」に切り替える方針を示しました。これが実現した場合、日本では国民皆保険制度を採用しているため、マイナンバーカードの取得を事実上義務化することを意味します。マイナンバーカードの普及率は、2022年9月時点の49.0%から大幅に上昇すると予測できます。

マイナンバーカードの利用には、顔写真や暗証番号による本人確認が必要であること、カードに秘匿性の高い情報が入っていないこと、ICチップが耐タンパ性を有すことなどから盗難・紛失に対する安全性は高いと言われています。しかしながらマイナンバーカードと暗証番号が同時に流出した場合、攻撃者がマイナポータルへ不正ログインして特定個人情報を不正に取得したり、民間のオンライン認証サービスを通じて本人になりすまし、銀行口座の開設やクレジットカードの作成をしたりするおそれがあります。今後は、マイナンバーカードの普及率が上昇することを見越して、マイナンバーカードを活用する民間サービスが増加すると予測できます。そのため、マイナンバーカードを足がかりにして、金銭奪取を狙うサイバー攻撃が増加すると予測します。マイナンバーカードそのもののセキュリティ強度が高くても、カードの保持者がカードを適切に管理しなければ、攻撃者がマイナンバーカードと暗証番号を窃取して、悪用する危険性が潜んでいるといえます。

事実上義務化されるマイナンバーカードを前に、日本国民全体のセキュリティリテラシーの向上が必要です。加えて生体認証を取り入れるなど、マイナンバーカードのリスク自体を小さくするセキュアな仕組みを整備することが急務です。

## FIFAワールドカップカタール2022を狙ったサイバー攻撃

2022年11月20日から約一か月にわたり、カタールワールドカップが開催されます。このような大規模イベントは世界的に注目を集めることもあり、サイバー攻撃の標的となります。2021年に東京で開催した同じく世界的なスポーツイベントである夏季オリンピック・パラリンピックは、大会運営を妨害するようなインシデントは発生しなかったものの、4.5億件ものサイバー攻撃を受けました。オリンピック・パラリンピック競技大会組織委員会といった主催組織だけなく、委託先のシステム会社などのサプライチェーンや観戦希望者といったステークホルダを狙ったサイバー攻撃も発生しました。カタールワールドカップも、主催組織以外もサイバー攻撃の対象となりえます。

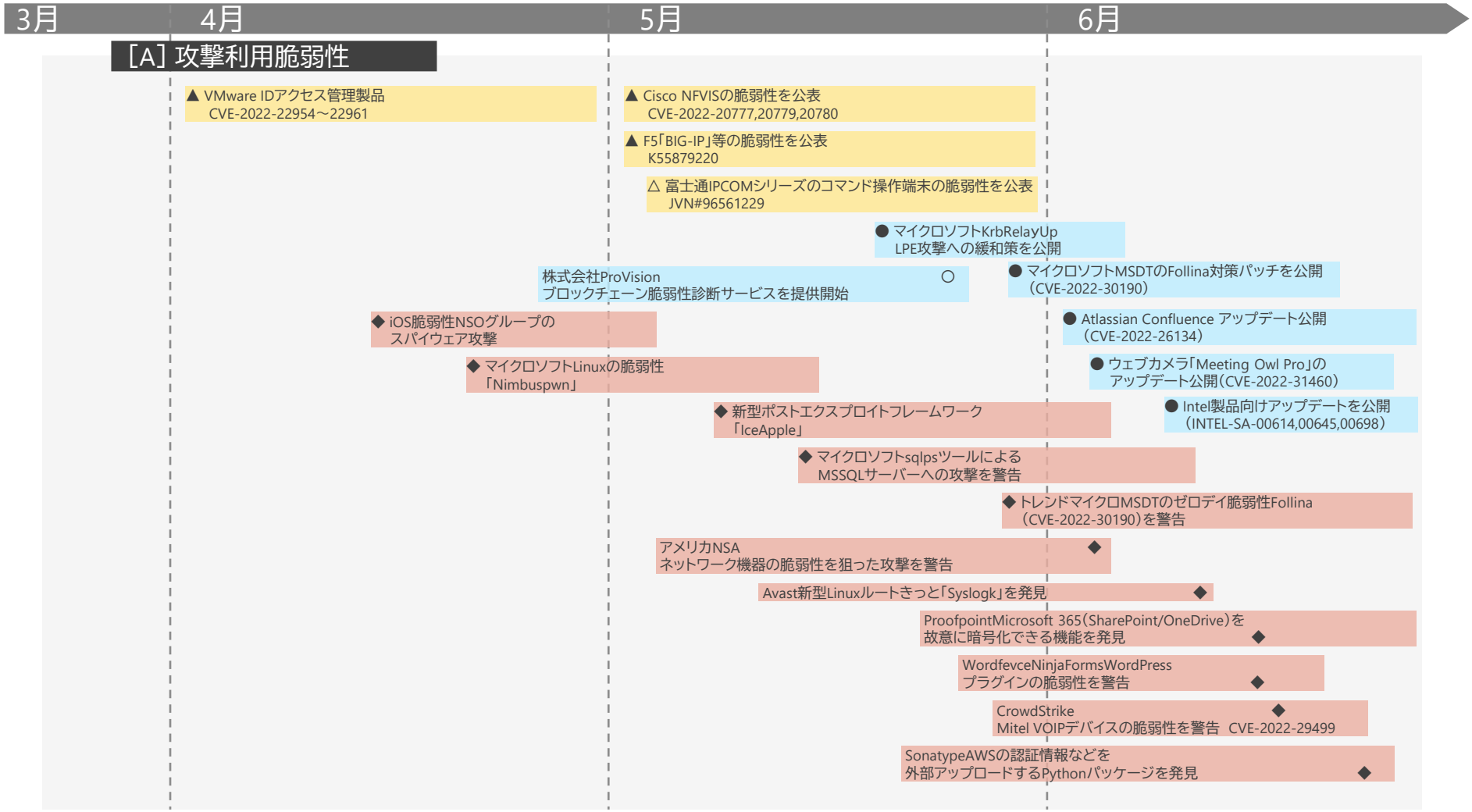
たとえば、攻撃者が偽のワールドカップ関連サイトを用意してサッカー観戦者へフィッシング攻撃を仕掛けるかもしれません。昨今では、インターネット中継でスポーツを観戦したり、競技の情報を収集したりする人々が増えています。準備期間も含めた大会期間中は、攻撃者がスポーツファンを偽の中継サイトやチケット予約サイトへ誘導して、個人情報を窃取するおそれがあります。フィッシング攻撃は「情報セキュリティ10大脅威 2022」の個人分野の第一位となっており、ワールドカップでも今の流行に沿ったサイバー攻撃が発生すると推測します。

# 8 タイムライン
# 事象発生の時系列表

※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

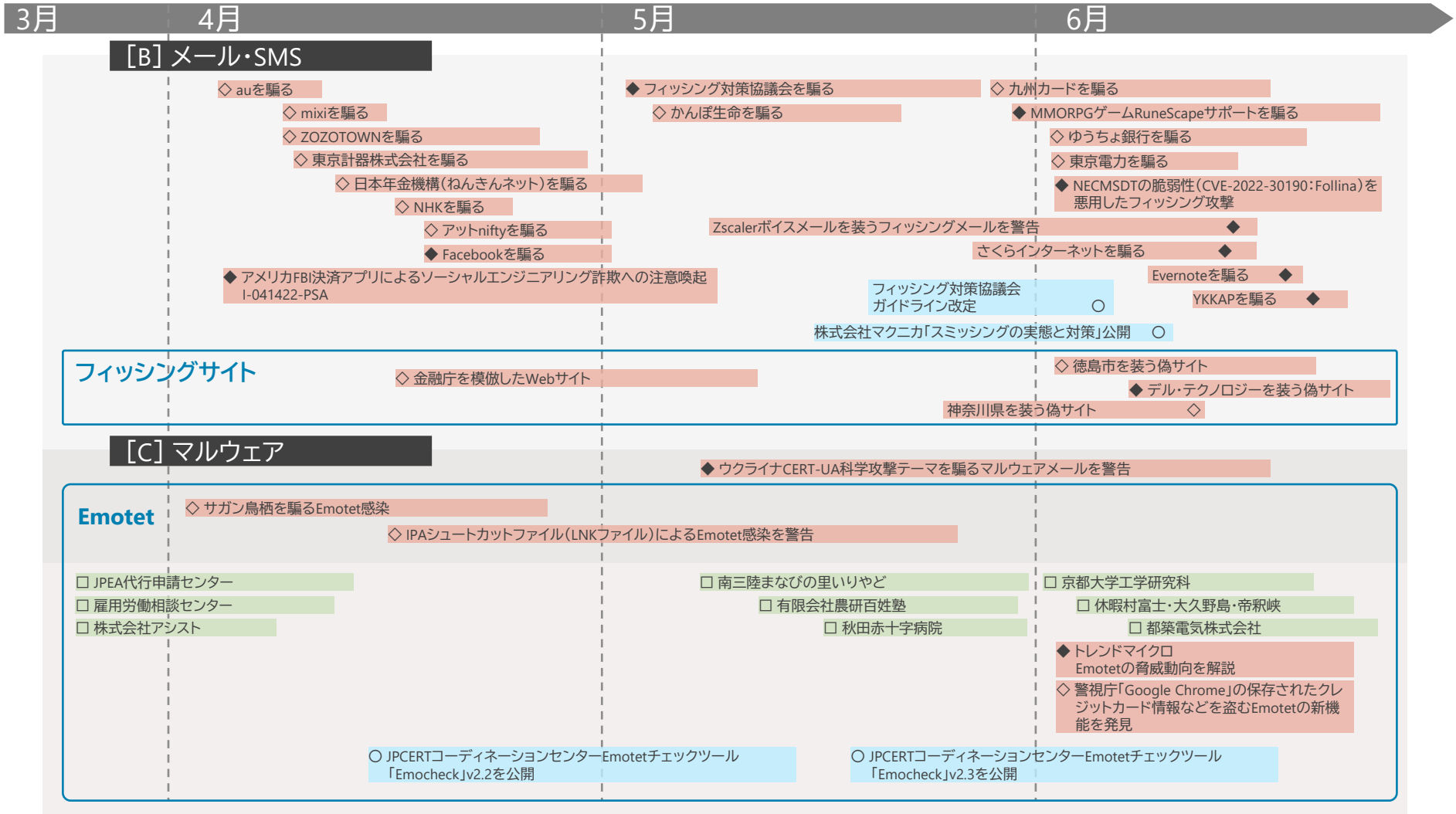
△▲:脆弱性
□■:事件・事故
◇◆:脅威
○●:対策



※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故
◇◆:脅威
○●:対策

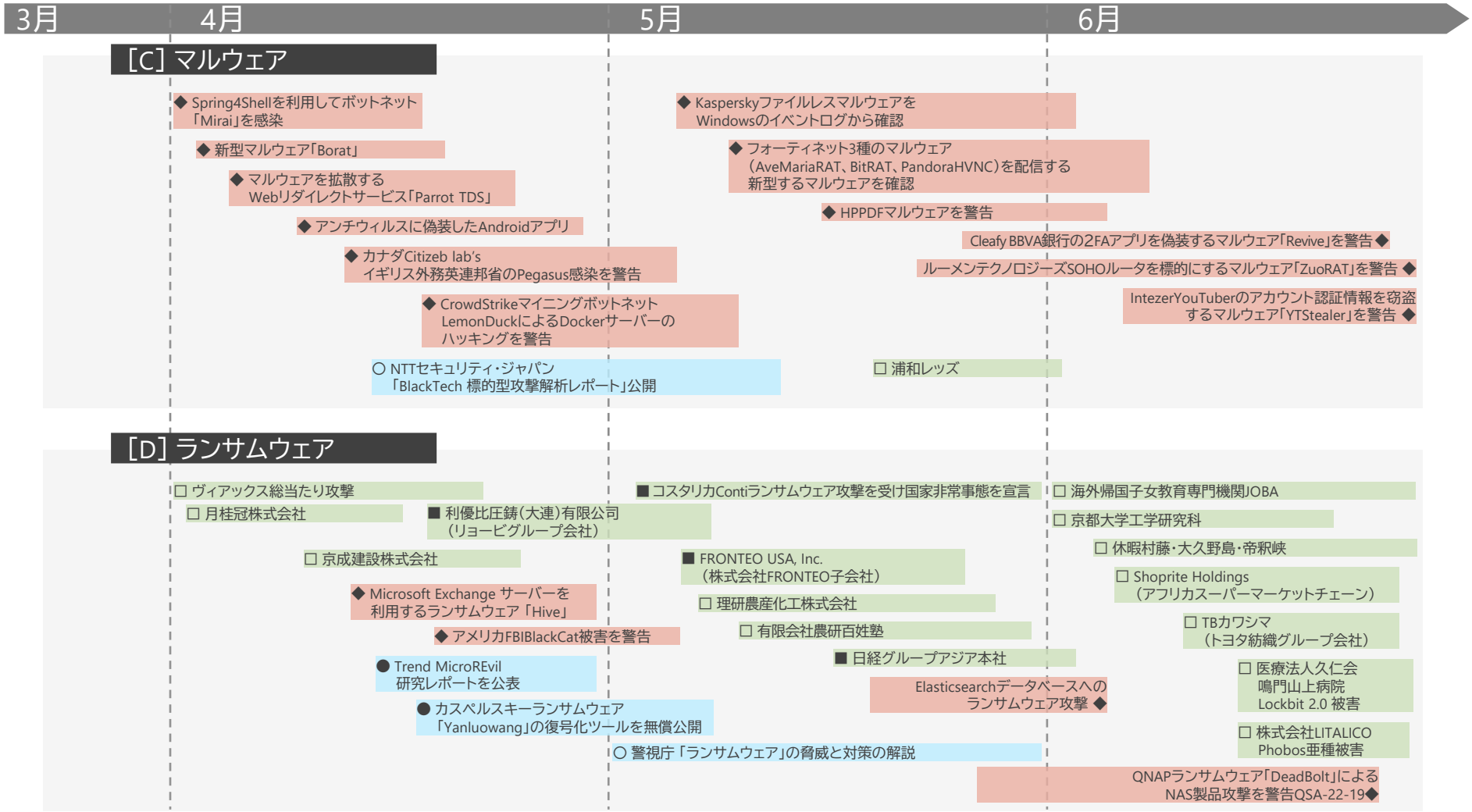


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

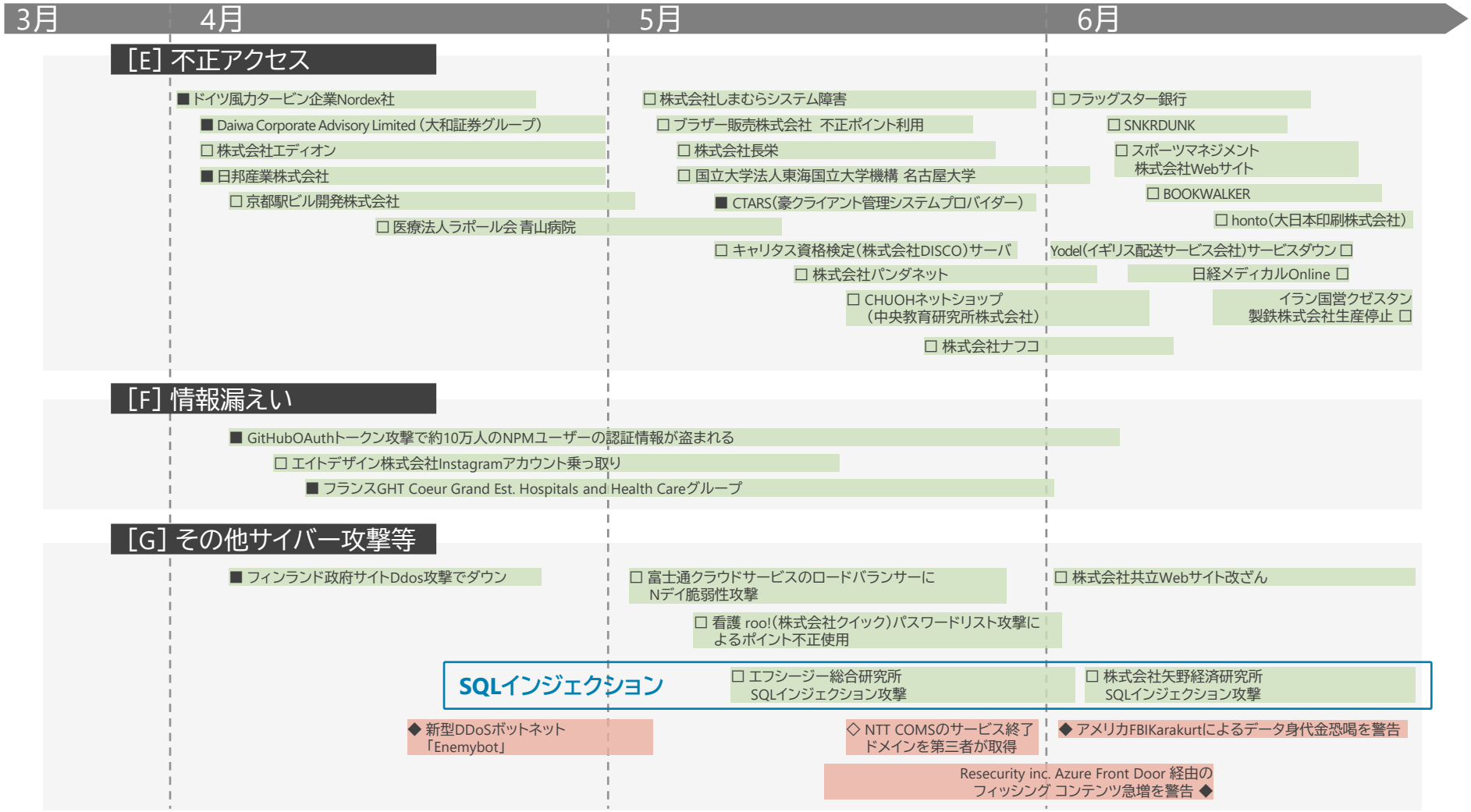
◇◆:脅威
○●:対策



※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故
◇◆:脅威
○●:対策



# 参考文献


[1] Federal Bureau of Investigation, “Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons,” 20 4 2022. [オンライン]. Available: https://www.ic3.gov/Media/News/2022/220420-2.pdf.

[2] Federal Bureau of Investigation, “Cyber Criminal Actors Targeting the Food and Agriculture Sector with Ransomware Attacks,” 1 9 2021. [オンライン]. Available: https://www.ic3.gov/Media/News/2021/210907.pdf.

[3] 株式会社NTTデータ, “「グローバルセキュリティ動向四半期レポート（2021年度第3四半期）」,” 15 3 2022. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2021_3q_securityreport.pdf.

[4] 警察庁, “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,” 7 4 2022. [オンライン]. Available: https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf.

[5] 農林水産技術会議, “「スマート農業実証プロジェクト」について：農林水産技術会議,” [オンライン]. Available: https://www.affrc.maff.go.jp/docs/smart_agri_pro/smart_agri_pro.htm.

[6] 内閣サイバーセキュリティセンター, “NISC | サイバーセキュリティ普及啓発・人材育成ポータルサイト構築,” [オンライン]. Available: https://security-portal.nisc.go.jp/.

[7] 内閣サイバーセキュリティセンター, “ランサムウェア特設ページ - NISC,” [オンライン]. Available: https://security-portal.nisc.go.jp/stopransomware/.

[8] 農林水産省, “2020年農林業センサス結果の概要（確定値）（令和2年2月1日現在）：農林水産省,” 11 6 2021. [オンライン]. Available: https://www.maff.go.jp/j/tokei/kekka_gaiyou/noucen/2020/index.html.

[9] PCI Security Standards Council, LLC., “Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards,” 3 2022. [オンライン]. Available: https://www.pcisecuritystandards.org/document_library/. [アクセス日: 26 10 2022].

[10] 経済産業省 商務情報政策局 商務・サービスグループ　キャッシュレス推進室, “キャッシュレス関連用語集,” 6 2019. [オンライン]. Available: https://www.meti.go.jp/policy/mono_info_service/cashless/image_pdf_movie/cashless_glossary_R1_06.pdf. [アクセス日: 27 10 2022].

[11] クレジット取引セキュリティ対策協議会, “EMV 3-Dセキュア導入ガイド 1.0版,” 8 3 2022. [オンライン]. Available: https://www.j-credit.or.jp/download/news20220309b4.pdf. [アクセス日: 25 10 2022].

[12] EMVCo, “3-D Secure - EMVCo,” 8 2022. [オンライン]. Available: https://www.emvco.com/emv-technologies/3d-secure/. [アクセス日: 1 11 2022].

[13] 経済産業省 商務・サービスグループ　商取引監督課, “クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性（クレジット・セキュリティ対策ビジョン2025）,” 2 6 2022. [オンライン]. Available: https://www.meti.go.jp/policy/economy/consumer/credit/2022060221001.pdf. [アクセス日: 18 11 2022].

[14] GitHub Inc, “Security alert: Attack campaign involving stolen OAuth user tokens issued to two third-party integrators,” 2022. [オンライン]. Available: https://github.blog/2022-04-15-security-alert-stolen-oauth-user-tokens/. [アクセス日: 25 10 2022].

[15] Salesforce , “Heroku Security Notification,” 2022. [オンライン]. Available: https://status.heroku.com/incidents/2413. [アクセス日: 25 10 2022].

[16] BLEEPINGCOMPUTER, “GitHub: Attackers stole login details of 100K npm user accounts,” 27 5 2022. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/github-attackers-stole-login-details-of-100k-npm-user-accounts/.

[17] GitHub Inc, “Software security starts with the developer: Securing developer accounts with 2FA,” 4 5 2022. [オンライン]. Available: https://github.blog/2022-05-04-software-security-starts-with-the-developer-securing-developer-accounts-with-2fa/.

[18] Travis CI, “SECURITY BULLETIN; Customer repositories have NOT been accessed,” 18 4 2022. [オンライン]. Available: https://blog.travis-ci.com/2022-04-17-securitybulletin.

# 参考文献


[19] 株式会社NTTデータ, “「グローバルセキュリティ動向四半期レポート（2021年度第1四半期）」,” 2 11 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2021_1q_securityreport.pdf.

[20] 株式会社NTTデータ, “「グローバルセキュリティ動向四半期レポート（2020年度第3四半期）」,” 16 3 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2020_3q_securityreport.pdf.

[21] National Cyber Security Centre, “Secure development and deployment guidance,” [オンライン]. Available: https://www.ncsc.gov.uk/collection/developers-collection/principles/protect-your-code-repository.

[22] 株式会社セキュアベース, “ソースコードおよびリポジトリ保護のためのセキュリティガイダンス,” 22 12 2021. [オンライン]. Available: https://secbase.jp/report/20211222_protect-your-code-repository.

[23] PNC株式会社, “英国NCSC、ソースコード保護のためのセキュリティガイダンス解説【前半】,” 22 12 2021. [オンライン]. Available: https://www.pnc.jp/blog/ncsc-source-code-security/.

[24] Statcounter, “Statcounter Global Stats,” [オンライン]. Available: https://gs.statcounter.com/browser-market-share/desktop-mobile-tablet/japan/.

[25] Japan Windows Blog, “Internet Explorer 11 デスクトップ アプリケーションのサポート終了 – 発表に関連する FAQ のアップデート,” 21 2 2022. [オンライン]. Available: https://blogs.windows.com/japan/2022/02/21/internet-explorer-11-desktop-app-retirement-faq/.

[26] C. Jackson, “The perils of using Internet Explorer as your default browser,” 6 2 2019. [オンライン]. Available: https://techcommunity.microsoft.com/t5/windows-it-pro-blog/the-perils-of-using-internet-explorer-as-your-default-browser/ba-p/331732.

[27] 独立行政法人情報処理推進機構, “Microsoft 社 Internet Explorer のサポート終了について,” 16 6 2022. [オンライン]. Available: https://www.ipa.go.jp/security/announce/ie_eos.html.

[28] IPA, “情報セキュリティ10大脅威 2022,” 27 1 2022. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/10threats2022.html.

[29] 警察庁, “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,” 7 4 2022. [オンライン]. Available: https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf.

[30] ExtraHop, “サイバーセキュリティの信頼度指数,” 23 5 2022. [オンライン]. Available: https://assets.extrahop.com/whitepapers/ExtraHop2022CyberConfidenceIndex_AsiaPacific_J.pdf.

[31] 株式会社月桂冠, “当社サーバへの不正アクセスに関するお知らせ,” 26 5 2022. [オンライン]. Available: https://www.gekkeikan.co.jp/company/news/detail/326/.

[32] 京成建設株式会社, “当社サーバに対する不正アクセスに関するご報告,” 18 4 2022. [オンライン]. Available: http://keisei-const.jp/info/%e4%b8%8d%e6%ad%a3%e3%82%a2%e3%82%af%e3%82%bb%e3%82%b9%e3%81%94%e5%a0%b1%e5%91%8a/.

[33] 理研農産化工株式会社, “不正アクセスによるシステム被害について,” 20 5 2022. [オンライン]. Available: https://rikenf.sagafan.jp/e982686.html.

[34] 株式会社アイウエア, “システム障害に関するお知らせとお詫び,” 13 6 2022. [オンライン]. Available: https://www.joba.jp/public_relations/.

[35] 徳島県つるぎ町立半田病院, “徳島県つるぎ町立半田病院コンピュータウイルス感染事案有識者会議調査報告書,” 27 6 2022. [オンライン]. Available: https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf.

[36] NTTデータ株式会社, “グローバルセキュリティ動向四半期レポート　2021年第2四半期,” [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2021_2q_securityreport.pdf.

# 参考文献


[37] IPA, “2021年度 中小企業における情報セキュリティ対策に関する実態調査,” 31 3 2022. [オンライン]. Available: https://www.ipa.go.jp/security/fy2021/reports/sme/index.html.

[38] 東京都, “セキュリティ対策に取り組む中小企業の人材育成・社内体制整備を支援します！,” 25 5 2022. [オンライン]. Available: https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2022/05/25/08.html.

[39] 経済産業省, “サイバーセキュリティ体制構築・人材確保の手引き,” 15 6 2022. [オンライン]. Available: https://www.meti.go.jp/policy/netsecurity/tebiki_taisei_jinzai.html.

[40] 東京都中小企業振興公社, “令和4年度 サイバーセキュリティ対策促進助成金,” 2022. [オンライン]. Available: https://www.tokyo-kosha.or.jp/support/josei/setsubijosei/cyber.html.

[41] 経済産業省, “IT導入補助金セキュリティ対策推進枠,” 2022. [オンライン]. Available: https://www.it-hojo.jp/security/.

[42] IPA, “中小企業の情報セキュリティ対策ガイドライン,” 19 3 2019. [オンライン]. Available: https://www.ipa.go.jp/security/keihatsu/sme/guideline/.

# グローバルセキュリティ動向四半期レポート
## 2022年度 第1四半期

2023年1月31日発行

株式会社NTTデータ
サイバーセキュリティ技術部
大谷 尚通 / 小林 義徳 / 大石 眞央 / 山下 大輔
松尾 俊彦 / 紀平 悠人 / 作田 尚美 / 齊藤 千紗 / 村田 直樹 / 高橋 達也 / 黒宮 雅史 / 工藤 完太郎
nttdata-cert@kits.nttdata.co.jp