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

2021年度
第4四半期

目次　グローバルセキュリティ動向　四半期レポート2021年度　第4四半期

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。

多発するNFT盗難事件

2021年ごろから大きく注目され始めていた「NFT」。2022年に入ってから、NFTの盗難事件が多発しています。NFTはブロックチェーン技術を拠りどころに高い改ざん耐性を有し、デジタルデータの「唯一性」と「所有者」を証明できます。

一方で、NFTを取り扱う際には、次の3つの注意点を押さえておく必要があります。①デジタルデータそのものが偽物で偽造品を購入してしまうおそれがあります。②取り引きに必要な認証情報をフィッシングにより詐取されて不正取引によりNFTを盗まれるおそれがあります。③NFTなどのデジタルデータは法的な所有権を認められていないため、盗まれたNFTなどのデジタルデータの法的な差し押さえや返還要求ができないおそれがあります。

上記の注意点に対するセキュリティ対策として、まずは取り引き前にNFTクリエイターの信頼性を確認しましょう。また、署名する前にNFT取引内容の妥当性を確認しましょう。さらに、取引所へログインする際の認証方式を多要素化する等の認証方式を強化したうえで、取り引きに必要な認証情報を厳格に管理しましょう。攻撃者は、人間が取り引きに関わる部分を狙うため、NFTに関連する詐欺や盗難に対しては、上記の認証や承認の手続きを行う時のセキュリティ対策を徹底しましょう。

遂に来るか、パスワード不要な認証の世界

今日に至るまで、認証情報の漏えいや窃取による情報セキュリティインシデントは、数多く発生しています。この問題を解決すべく、FIDO Allianceは、長年、認証の世界からパスワードそのものを不要とするための仕組みを検討し、2019年には、W3Cとともに、パスワードレス認証の技術仕様としてWebAuthnを公開しています。しかし、その普及は十分に進んできませんでした。

2022年3月、FIDO AllianceとW3C WebAuthn WGは、WebAuthn 新バージョン（「Level 3」）の仕様検討の開始を公表しました。この発表では、従来のFIDOの普及における課題を克服する2つの新機能を発表しています。本機能を実現できれば、いよいよパスワードレス認証が認証の世界のデファクトスタンダードになるかもしれません。

本稿では、現在のFIDOの普及における課題と今回発表された新機能を解説します。そして、最後に来たるパスワード不要な認証の世界に乗り遅れないために、インターネット時代を生きるすべての企業が、今のうちに対応すべきことを提案します。

Emotetの感染再拡大

2021年11月に攻撃活動を再開したEmotetの感染被害が、日本国内で再拡大しています。Emotetの感染手法は、不正な「.xlsm」ファイルを格納したパスワード付きZIPファイルをメールにて送付する手法が主流です。攻撃者は、日本のみで普及していたPPAPと呼ばれる、ファイルをメールに添付して送る慣習に便乗したPPAP型攻撃メールを使用しています。PPAPはメールセキュリティ対策製品の検知をすり抜ける確率が高いため、Emotetだけではなく様々なランサムウェア、マルウェアの感染手法としても悪用できる非常に危険な手法です。Emotetの感染が再拡大している状況から、今こそPPAPの業務利用禁止に踏み切るべきではないでしょうか。

予測

日本国内において、PPAP型の攻撃メールによるEmotetの感染拡大により、PPAPの業務利用禁止の動きが加速すると予想します。PPAPの代替手段としてファイル共有サービスの利用が増加した場合、サービスを悪用してマルウェアに感染させる手口による被害が増加すると予測します。

今後、NFTの利用が拡大するにつれて、初めて取り引きする利用者が増え、NFT盗難被害がより広がるおそれがあります。NFTの法整備を進めている英国での動きは世界中に広がり、利用者を法的に保護するべきか否かについての議論が今後進んでいくと予測します。

2022年3月、トヨタ自動車における関連会社を狙ったサプライチェーン攻撃等、サイバー攻撃により部品供給/生産管理が止まり、企業活動が影響を受けるケースのサプライチェーン攻撃による被害が増えています。今後もしばらくは自動車業界だけではなく、同様な影響を受ける企業、業界を狙ったサプライチェーン攻撃が拡大していくと推測します。

2 注目トピック①
NFTに潜むセキュリティリスク

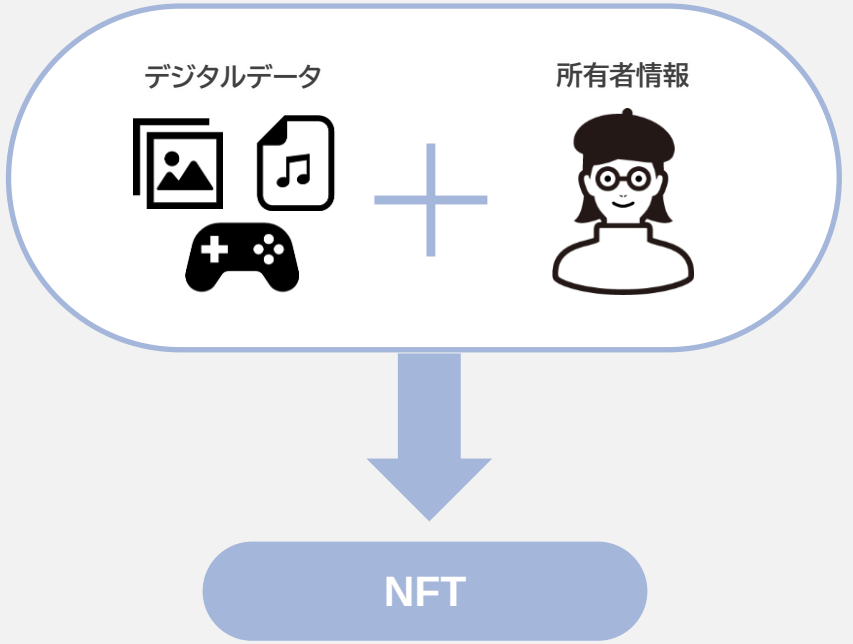
2.1. 多発するNFT盗難事件

2021年ごろから大きく注目され始めていた「NFT」は、2022年に入ってから、盗難事件が多発しています。2022年2月には、Ozone Networks, Inc.が運営する世界最大のNFT取引所 OpenSeaにおいて、過去最大規模のNFT盗難事件が発生しました。OpenSeaの利用者を標的とした攻撃により、利用者が保有していたNFTが不正に攻撃者に盗まれた事件です。OpenSeaから盗まれたNFTは、いずれも人気のある高額なコレクションでした。17ユーザから盗まれたNFTの総被害額は170万ドル以上です。

2.2. NFTとは

NFTは「Non Fungible Token：非代替性トークン」の略称で、文字通り「代替が不可能な固有のトークン」を意味します。2017年頃から登場して、2021年頃から話題を集めるようになった技術です。
NFTは、デジタルアートやゲームアイテム等のデジタルデータの「所有者」と「唯一性」を担保する仕組みとして利用されています。
デジタルデータの所有者と唯一性を担保する場合は、担保したいデジタルデータに対して、所有者の情報を付与してNFT化します。
NFT化とは、ブロックチェーン上でデジタルデータおよびその所有者を記録することです（図 2-1）。NFTはブロックチェーンにより発行・管理されるため、複製が容易なデジタルデータであってもNFTを参照することで対象のデジタルデータの所有者と唯一性を証明することが可能になります。

図 2-1：NFTとは



通常のシステムでは、重要なデータをサイバー攻撃から守る場合、インターネットからの脅威を排除したシステムを構築し、データの漏えいや改ざんを防ぐためのセキュリティ対策を実装してデータを集中的に管理します。この従来のデータの管理方法は、内部の有権限者による改ざんを防ぐことが困難です。一方でNFTは、データをオープンかつ分散管理するブロックチェーン上で発行・記録して、データの複製や改ざんを防ぎます。

ブロックチェーン技術は、もともと暗号資産ビットコインの取引記録を管理する台帳技術として発展してきました。ブロック内に「いつ」「どこから」「どこに」「どれだけの暗号資産を移動したか」といった取り引きの情報を記録して、チェーン形式で管理します。新しいブロックを生成するたびに、前のブロックのハッシュ値を新規ブロックへ格納して、取引情報が時系列につながる仕組みです（図 2-2）。NFTは、デジタルデータを誰が作成したのか、誰が誰に対して渡したのか等の取引情報をブロックチェーン上に記録していきます。

攻撃者は、デジタルデータの受取人を自分にするために、ブロック内のNFT取引情報を改ざんしようとします。しかし、もし攻撃者があるブロック内のNFT取引情報を改ざんできた場合でも、第三者はそのブロックの後続のブロックに含まれるハッシュ値を使って、NFT取引情報が改ざんされているかどうかを判断できます（図 2-3）。後続のすべてのブロックに含まれるハッシュ値への影響を調整することは非常に困難であるため、NFT取引情報の完全性を保つことができます。また、たとえ後続のすべてのブロックに含まれるハッシュ値への影響を調整できたとしても、改ざんしたブロックと他で分散管理しているブロックはハッシュ値が異なるため、改ざんを判断できます。このブロックチェーン技術を拠りどころとして、NFTは、NFT取引情報の改ざんを困難なものとし、デジタルデータの所有者と唯一性を担保します。よってNFTは、組織の内部と外部の攻撃者に関わらず、データの改ざんに対する高い耐性を持ちます。

ブロックチェーン技術の詳細を知りたい方は、NTTデータのWebサイトに掲載しているブロックチェーン記事 [1]をご参照ください。

図 2-2：ブロックチェーン技術とは

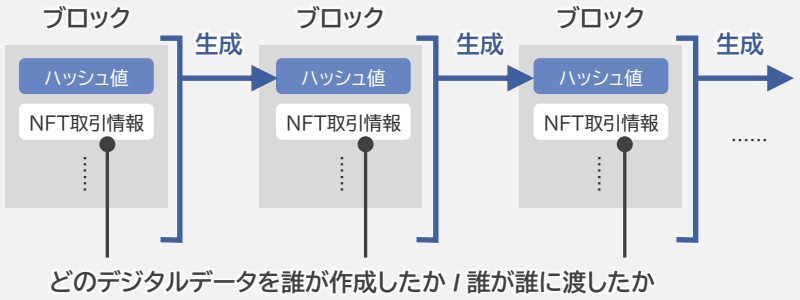
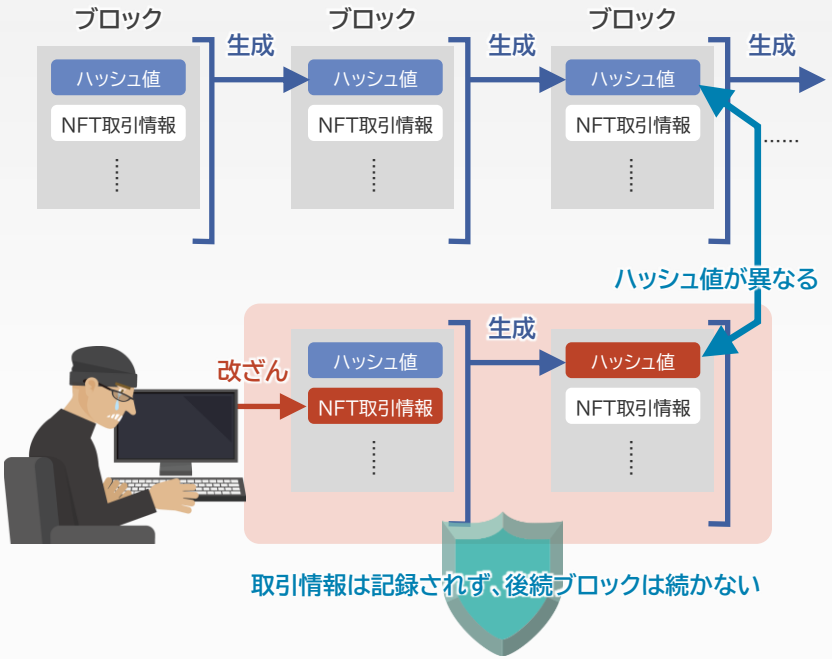


図 2-3：ブロックチェーンの改ざん耐性



2.3. おさえておきたい3つの注意点

（1） 対象のデジタルデータそのものが偽物

NFTを参照すれば、対象のデジタルデータの所有者が誰で、唯一のデジタルデータであることを確認できます。しかし、デジタルデータそのものが偽造したデータで、その偽造データをNFT化している場合は、NFTを参照するだけでは判別できません。対象のデジタルデータそのものが本物か、偽造したものなのかは、購入者が事前に調査して判断する必要があります（図 2-4の「偽物のデータ」）。

（2） 詐欺やハッキングにより盗まれる

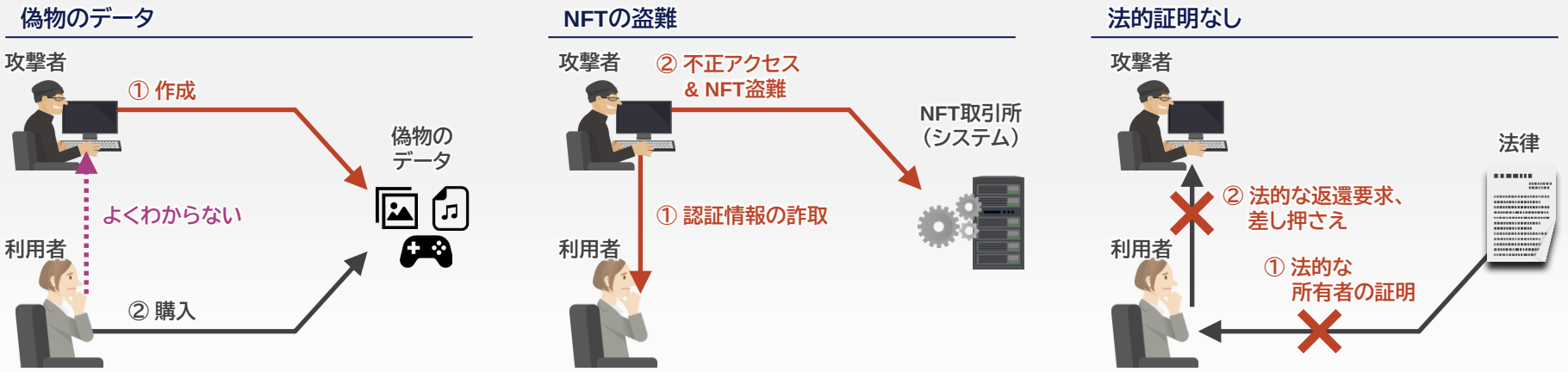
NFTは複製や改ざんに高い耐性をもつ資産です。しかし、デジタルデータとしてシステム上で管理されている以上、攻撃者がNFT所有者を騙して、秘密鍵やシードフレーズを盗めば、攻撃者はデジタルデータを不正に取り引きして自分の所有へ変更できてしまいます。また、システムのバグを悪用して不正に取り引きを行って、NFTを盗むことができる確率もゼロではありません（図 2-4の「NFTの盗難」）。

（3） デジタルデータの法的な所有者を証明できない

自宅に飾っておいた1点ものの高価な絵画が泥棒に盗まれた場合、現実の世界であれば、法律に則って泥棒が盗んだ絵画の差し押さえや返還要求ができます。一方で、攻撃者がNFTを盗んだ場合、法律は情報を有体物/財物として認めていないため、法律では窃盗として裁くことができません。NFTなどのデジタルデータの窃盗を取り締まるための法整備はこれからです。

詐欺やハッキングによりNFT盗難事件が発生した場合、詐欺罪等により逮捕できる可能性はありますが、デジタルデータの所有権は法的に明確にできず、差し押さえや返還要求ができないおそれがあります（図 2-4の「法的証明なし」）。

図 2-4：3つの注意点



2.4. NFTが関連する主な事件

（1） 偽バンクシー詐欺事件 [2]

先述のおさえておきたい1つ目「偽物のデータ」の注意点に該当する事件です。2021年9月、あるコレクターがバンクシーの偽造NFTを約34万ドルで購入したという詐欺事件が発生しました。結果的に、購入したコレクターには、手数料を除いた金額が返金されました。NFTは、デジタルデータの唯一性と所有者を確認することはできますが、デジタルデータそのものが本物か偽物かを判断するためには、NFTを発行するクリエイターの信頼性を確認する必要があります。しかし、クリエイターの信頼性を確認するためには、その分野の情報を収集し知識を蓄えたうえで、クリエイターの活動を調査して信用できるか否かを判断しなければなりません。NFTが普及してNFT取引に参加する利用者が増えるにつれて、NFTにそこまで詳しくない利用者の絶対数も増加するため、このような詐欺事件は増えていくと予想します。

（2） OpenSeaにおけるNFT盗難事件 [3]

冒頭の「2.1.1 多発するNFT盗難事件」で紹介したこの事件は、上記のおさえておきたい2つ目「NFTの盗難」と3つ目「法的証明なし」の注意点に該当します。攻撃者はNFT取引所OpenSeaの特定の利用者へフィッシング詐欺攻撃を行い、利用者を言葉巧みに騙したり、購入をあせらせて真偽を確認する前に取り引きを行ってNFTを盗みました。OpenSea CTOのNadav Hollander氏によるTwitter上での状況説明 [4]によると、判明した取引内容には、被害を受けた利用者の有効な署名が入っていました。これは、利用者が攻撃者に騙されて、どこかで悪意のある取り引きに署名をしてしまったことを示します。OpenSeaは、2022年5月時点で、Twitter以外では詳細な経緯や攻撃手法を公表していません。取り引きが完了したNFTは、攻撃者から奪還できませんでした。

有名なコレクションのNFT発行の直後は、購入者からの注文が殺到します。購入者は、誰よりも早く取り引きしようと焦ります。その際、購入者は攻撃者の巧みな言葉に騙されやすく、焦ってうっかり取り引きをしてしまうのです。

（3）Nifty GatewayにおけるNFT盗難事件 [5]

上記のおさえておきたい2つ目「NFTの盗難」と3つ目「法的証明なし」の注意点に該当する事件です。Nifty Gateway社のNFT取引所の利用者のパスワードが漏えいし、2021年3月に攻撃者が、NFT取引所の多要素認証を有効化していなかったアカウントへ、漏えいしたパスワードを使って不正にログインし、アカウントを乗っ取りました。攻撃者は価値の高いNFTを盗み出し、被害総額は15万ドル以上となりました。取り引きが完了したNFTは、攻撃者から奪還できませんでした。

2.5. NFTを守るためのセキュリティ対策まとめ

NFTは、デジタルデータの複製や改ざんに対して高い耐性をもつ証明方式です。しかし、偽造デジタルデータを用いた詐欺や認証情報の詐取による不正取引に対しては、利用者が気を付けなければなりません。前述のおさえておきたい3つの注意点に対して、現在実施できるセキュリティ対策を紹介します。今後NFTを取り扱う場合は、以下の3つの対策を行うべきです。

（1）NFTクリエイターの信頼性の確認

取り引きをしようとしているNFTを発行するクリエイターが実際に存在するのか、活動しているのか、クリエイターが用意しているWebサイトやSNS等を確認したうえで取り引きを行いましょう。

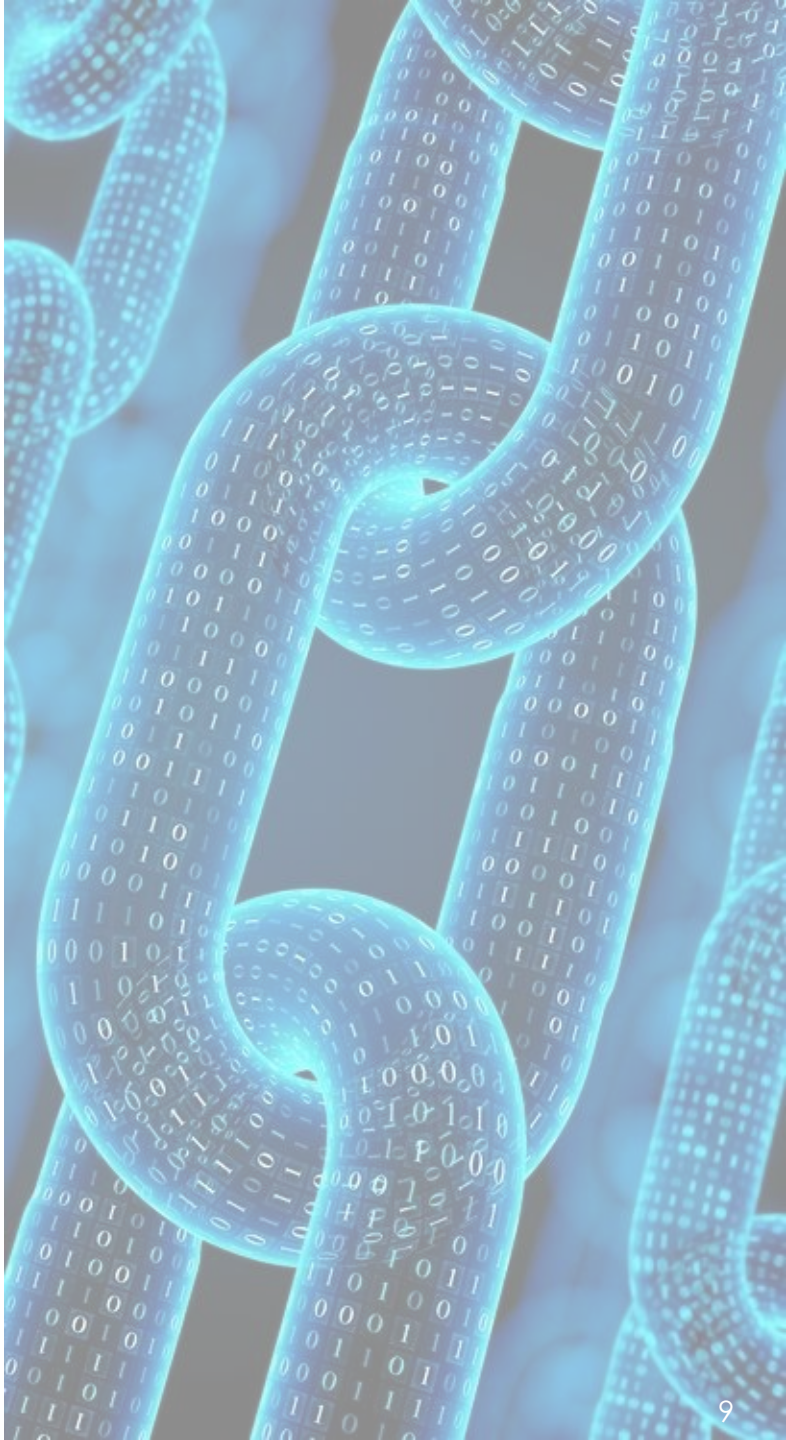
（2）標的型攻撃、フィッシング詐欺の対策

送られてきたメールの送信者は本当に正しいNFT取引所か、記載しているURLのリンク先は正しいNFT取引所か、偽のサイトや偽のアプリではないことを必ず確認してから取り引きを行いましょう。また取り引き時に秘密鍵やシードフレーズを用いて署名する際は、必ず誰とどのような取り引きをしているかを確認しましょう。

（3） 取り引きに必要な認証の強化および認証情報の強固な管理

NFT取引所へのログインには、強固なパスワードを設定するとともに、多要素認証を必ず有効化しておきましょう。万が一パスワードが漏えいした場合でも、攻撃者がログインできないようにします。

取り引きに必要な認証情報である秘密鍵やシードフレーズは手書きメモとして保管し、誰にも見られないようにしましょう。また詐欺的手法で聞き出そうとする攻撃者も考慮し、誰にも話さないように気を付けましょう。秘密鍵やシードフレーズを電子データとして機器上に保管する場合は、攻撃者がその機器へ不正侵入して認証情報を盗めないように、普段はハードウェアウォレット等に保管し、取り引きで必要な時に取り出して使うようにしましょう。



3 注目トピック②
遂に来るか、パスワード不要な認証の世界

3.1. FIDOの新バージョン（WebAuthn Level 3）の検討開始

今日の主要な認証方式は、依然としてパスワード認証です。しかし、FIDO AllianceとW3C WebAuthn WGが発表した新機能が実現できれば、認証の世界の常識が変わるかもしれません。2022年3月、FIDO AllianceとW3C WebAuthn WGは、パスワードレス認証の普及を加速させる新機能の実現方針を公開しました。特筆すべき点は、今回の発表を受けて、すぐに主要OSベンダーであるApple、Google、Microsoftが新機能の実現に向けた協力意思を発表していることです [6]。さらにこの3社は、それぞれ来年にかけて実装をすすめる予定も公開しています。これはすなわち、業界全体として、よりセキュアで便利な認証の世界を実現しようとする気運が高まっているということを意味しています。今後、近い将来、FIDOを用いたパスワードレスな認証がスタンダートな認証方式となる日がやってくるでしょう。

そこで、本稿では、FIDOの仕組みと特徴を簡単におさらいしたあとに、現在のFIDOの普及における課題、FIDO Allianceが発表した新機能を解説します。そして、最後に来たるパスワード不要な認証の世界に乗り遅れないために、インターネット時代を生きるすべての企業が、今のうちに対応すべきことを提案します。

3.2. FIDOの仕組みと特徴

従来から用いているパスワード認証には、語りつくせないほど多くの課題があります。パスワードの推測による攻撃、フィッシングサイトを使った認証情報の詐取、ネットワーク上のやりとりやサーバからの認証情報の漏えい、そして悪用などの数々の情報セキュリティインシデントは、パスワード認証を利用していることと関係しています。

人々をパスワードの管理の手間から解放し、自らがこれらの情報セキュリティインシデントの対応から解放されることは、多くのセキュリティエンジニアの悲願です。これを実現することを目的に、FIDO（Fast Identity Online）という認証方式が考案されました。

FIDOでは、サービス利用者が所持するデバイス内で、指紋、顔などの生体情報を利用した認証、もしくはPINなどのサービス利用者自身が記憶している情報を利用して認証を行い、サービス利用者自身の利用か否かを検証します。なお、この検証機能を担うデバイスを認証器と呼びます。そして、認証器は、その検証結果を暗号化してサーバへ送信します。

ここで重要な点は、FIDOはサービス利用者自身の利用か否かを照合するための指紋や顔やPIN等の情報をサーバへ送信しないことです。つまり、FIDOでは、ネットワーク上に認証情報が流れず、またサーバ側で情報漏えいが発生しても、サーバは認証情報を保持していないので、認証情報の窃取も漏えいも起こり得ないのです。そのため、FIDOはセキュアな認証方式といわれています。

FIDOの仕組みについて、詳細を知りたい方は、こちらのFIDO Alliance の解説「FIDOの仕組み｜FIDO Alliance 」 [7]をご参照ください。

3.3. FIDOの普及状況および課題

FIDOは、セキュアな認証方式であることは前述のとおりです。では、このセキュアな認証方式は、世の中に十分に普及しているのか、というと、そうとは言えません。Microsoftの報告では、Azure ADの利用企業のうち、78%の企業はFIDOやMFAを利用していません [8]。FIDOの普及を阻害する要因は、以下の2つです。

（1）要因①：アカウントリカバリ時のサービス利用者の負荷

認証器として利用しているデバイスを紛失した場合、新しいデバイスでFIDOを再度利用できるようにするためには、サービス利用者は、FIDOを使っているサービスごとに認証器の登録をやりなおす必要があります。つまり、サービス利用者が多くのサービスでFIDOを利用していればしているほど、アカウントリカバリ時のサービス利用者の認証器の登録作業の負荷が高くなってしまいます。

一方、サービス提供側は、サービス利用者から新しい認証器の登録を受け付ける前に、サービス利用者当人の利用か否かをFIDO以外の方法で検証しなければなりません。その際、一度手放したはずのパスワード認証に頼らざるを得ないケースがほとんどです。結果として、アカウントリカバリまでを考慮に入れると、完全なパスワードレスの認証方式を実現できません。

FIDO Allianceの推奨するベストプラクティスは、事前に複数のデバイスを認証器として登録しておくこと [9]ですが、複数デバイスを所持していないサービス利用者は対応できません。また、複数デバイスを所持している場合でも、登録作業をサービス利用者に強制すれば、サービス利用者の認証器の登録作業の負荷が高くなってしまいます。そのため、これらの方法は十分ではありませんでした。

（2）要因②：FIDO Allianceの安全性認定済のデバイスの普及遅れ

多くのユーザが利用したい認証方法は、指紋や顔など生体情報を利用したFIDOでしょう。デバイスがFIDOに対応するためには、まずFIDO Allianceが安全性を認定した認証器を利用しなければなりません。さらに、生体認証を用いたい場合は、認証器が搭載している赤外線、カメラ、指紋リーダ等も、同様に安全性を認定していなければなりません。スマートフォンを認証器として利用するには、iphoneであればiOS14以降のOS、androidであればandroid7以降のOSを搭載しているデバイスであれば、FIDO Allianceの認定を取得しています。また、これらのデバイスは、カメラや指紋リーダも認定基準を満たしたものを搭載しています。現状のスマホ普及率に鑑みると、多くのスマートフォンは、生体情報を利用したFIDOを使用できると考えられます。一方、PCの場合は、Windows OSを搭載したデバイスについては、生体情報を利用したFIDOを利用できないケースがあります。例えば、エントリーモデルのPC等、基本性能が低いデバイスは、デバイスに搭載されているセキュリティチップがFIDO Allianceの認定基準を満たしていないケースがあります。また、セキュリティチップの要件を満たしていても、赤外線、カメラ、指紋リーダを搭載していない、あるいはカメラを搭載していても認定基準を満たしていない場合、生体情報を利用したFIDOが使用できません。前者は、Windows11のシステム要件として一定バージョンのセキュリティチップの搭載が必須化されるため、時間の経過とともに解消される見込みですが、後者は、今後も課題として残り続けるでしょう。

FIDOを採用してユーザをパスワードの管理の手間から解放することを目指しているシステム管理者は、これからFIDOを導入する環境のデバイスが、生体認証を利用できないのであれば、FIDOの採用を見送るかもしれません。

3.4. FIDOの新機能

上述した2つの要因により、FIDOがなかなか普及していません。こうした背景から、FIDO AllianceとW3C WebAuthn WGは、パスワードレス認証の普及を加速させる新機能の実現方針を公開しました。その中で、特に以下の2つは、重要な新機能であることを強調しています。

（1）新機能①：マルチデバイス対応 FIDO 認証資格情報 [10]

FIDO認証資格情報とは、認証器で行われた検証の結果を暗号化するための秘密鍵等の情報です。現在のFIDOの仕組み上、FIDO認証資格情報は、認証器内で安全に保管して、外から読み出せないようになっています。このように、1つのFIDO認証資格情報は、1つの認証器にしか存在しえないので、現在のFIDOは、シングルデバイス対応であると言えるでしょう。

課題①で述べているように、サービス提供側は、アカウントリカバリ時にFIDO以外の方法でサービス利用者を認証する仕組みを用意しなければならない、という問題があります。そして、サービス利用者は、アカウントリカバリ時にサービスごとに認証を行い、新しい認証器を登録しなければならない、という問題があります。これらの問題は、現在のFIDOがシングルデバイス対応であるがゆえに起こっている問題です。

新機能①は、複数デバイス間でFIDO認証資格情報を共有可能とする、つまりマルチデバイス対応にする、という機能です。そのために、FIDO Allianceは、各OSベンダーがFIDO認証資格情報を安全に同期できる機能を提供することを求めています。マルチデバイス対応が実現すれば、スマートフォンの機種変更時に多くの設定情報をクラウド経由で移行するのと同様の仕組みで、新しい端末へFIDO認証資格情報を同期することが可能になります。結果、サービス提供側はアカウントリカバリの仕組みとしてFIDO以外の方法を用意する必要はなく、サービス利用者はアカウントリカバリ時に新しい認証器を登録し直す必要もなくなります。ゆえに、課題①の解決が見込まれます。

なお、今回の発表には、OSを跨いだ同期機能が含まない点に留意してください。例えば、iphoneからandroidへ買い替えた場合、機能①では課題に対応できません。ただし、このケースは、後述する新機能②を利用すれば対応可能な見込みです。

（2）新機能②：スマートフォンをローミング認証器として利用 [10]

新機能②は、Bluetoothを利用してスマートフォンを外部認証器として利用可能にする機能です。例えば、PCからログインする際、PCとスマートフォンをBluetooth接続し、FIDOはスマートフォンで行い、その検証結果をPCに伝搬する機能です。

課題②で述べているように、FIDOの導入を促進するためには、認証を行うデバイスがFIDO認証器として機能できて、かつ生体認証を利用したFIDOを行える状況である必要があります。スマートフォンは普及率が高く、またPCに比べて定期的にデバイスを買い替えてハードウェアを最新化するため、多くのスマートフォンは精度の高い生体認証機能を持っておりFIDO認証器として利用可能です。

新機能②では、仮にPCがFIDOに対応していない、もしくは生体認証を利用したFIDOを行えないデバイスであったとしても、FIDO自体は、サービス利用者が持っているスマートフォンで生体認証を行い、Bluetoothでその検証結果をPCに伝搬することが可能になります。いままでFIDOの導入を見送ってきたシステム管理者にとっても、サービス利用者のスマートフォンを利用することが可能であれば、FIDOを導入する環境のデバイスに縛られずに、FIDOの導入検討を行えるでしょう。ゆえに、課題②の解決が見込まれます。

新機能①では、OSを跨いだFIDO認証資格情報の同期機能が提供されるとは限らないため、OSの異なるデバイスへ買い替えた場合にFIDO認証資格情報が共有できないことを説明しました。新機能②では、iphoneからとAndroidへ買い替えたとしても、アカウントリカバリ時に買い替えた新しいデバイスでログイン処理をすすめ、FIDOについては、Bluetooth接続し買い替え前のデバイスで行うことで、ログイン処理を完了させることが可能です。新しいデバイスを認証器として利用したい場合は、ログイン処理を完了させた後、サービス側で新しいデバイスを認証器として登録すれば、OS間を跨いだ乗り換えも比較的スムーズに行えると想像します。

3.5. FIDO対応のために今後すべきこと

今回の新提案は、Apple、Google、Microsoftなど、OSベンダーの協力のもと、2023年に検討がすすんでいきます。パスワード不要な認証の世界がデファクトスタンダードとなる日もそう遠くはないと考えます。スムーズにパスワード不要な世界へ移行できるために、以下の2つを検討しておくとよいでしょう。

（1）アカウント統合

FIDO認証資格情報はアカウントと紐づいています。ゆえに、1人のユーザが複数のアカウントを所持している状態では、FIDO認証への移行を阻害してしまいます。アカウントの統合は、一朝一夕では行えないので、乗り遅れないために早めに対応しておくことが重要でしょう。

（2）IDaaSの利用

FIDOに対応するには、サービス提供者は、認証器の検証結果を受けつけ、結果を確認するFIDOサーバを用意しなければなりません。しかしサービス提供者自らがFIDOサーバを用意しなくても、IDaaSの利用で容易に代替可能です。FIDOの新しい規格が出た際も、FIDOサーバの変更はIDaaSが対応すると考えられるので、これを機に、IDaaSの利用を検討するのもよいでしょう。

4 情報漏えい
メタップスペイメント社の個人情報漏えい事件から学ぶこと

2022年2月28日に決済代行業者の株式会社メタップスペイメントが、不正アクセスによる情報流出に関する報告を公開しました。同社によると個人情報を含む情報が最大で460,395件漏えいしたとのことです [11]。本稿では、この個人情報漏えい事例から、不正アクセスへの対策やインシデントが発生した際の適切な対応方法を考察します。

4.1. 情報漏えい事故の概要

メタップスペイメント社は、同社のデータセンターサーバー内に配置したクレジットカード決済処理サービスのWebアプリケーションの脆弱性を悪用されて、不正アクセスを受けました。攻撃者は、2021年8月31日から2022年1月25日にわたって表4-1①～③の複数種類の攻撃を行い、決済情報等を格納しているデータベースにまで侵入しました。そして、個人情報を含む最大460,395件の情報を外部へ持ち出しました [11]。

右の表4-1に、メタップスペイメント社が発表した情報漏えい事故の経緯を示します [11]。

表4-1：メタップスペイメント社の対応のタイムライン

日付	経緯と対策詳細
2021/8/31	メタップスペイメント社へ攻撃開始
日付不明	脆弱性を悪用して、不正ログイン成功…①
2021/12/14	メタップスペイメントは、クレジットカード会社より自社提供のクレジットカード決済処理サービス「イベントペイ」の不正利用の懸念の連絡を受領
2021/12/15	クレジットカード会社から情報提供を受けたものの、同社の調査で原因を特定できず、第三者機関によるフォレンジック調査を決定
2021/12/16	イベントペイのクレジットカード決済処理を停止
2021/12/17	• 第三者機関によるフォレンジック調査の開始 • クレジットカード会社から追加の不正利用の懸念の追加情報を受領 • クレジットカード決済サービス「会費ペイ」を含む3サイトのクレジットカード決済処理を新たに停止
2021/12/29	• 上記の決済処理を停止したイベントペイと会費ペイを含む、加盟店の4サイトで不正アクセスによる情報漏えいの懸念が判明 • 当該4サイトの管理者へ連絡 • 当該インシデントに関係する加盟店へフォレンジック調査を開始した旨を通知
2022/1/5	クレジットカード決済処理サービスのWebアプリケーションへのSQLインジェクション攻撃を確認…②
2022/1/8	• 攻撃者の排除を完了 • 同Webアプリケーションに対するSQLインジェクション攻撃の防止の対策を完了
2022/1/21	情報流出を裏付ける証拠を発見
2022/1/24	不審なプログラムのファイル（バックドアプログラム）を発見…③
2022/1/25	• クレジット決済処理サービス「トークン方式」のWebアプリケーションを全停止 • バックドアプログラムの全削除を完了 • 「不正アクセスに関するご報告とお詫び」を公表
2022/2/8	第三者機関からフォレンジック調査の最終報告書を受領
2022/2/18	警察に被害申告
2022/2/28	「不正アクセスおよび情報流出に関するご報告とお詫び」を公表

4.2. 攻撃方法と被害

メタップスペイメント社の報告書の内容をもとに、インシデントの内容を記載します（図 4-1参照）。

1. 社内用決済管理画面へのXSS攻撃

攻撃者は、同社の決済システムの社内用決済管理画面にあった脆弱性を悪用してクロスサイト・スクリプティング攻撃（①）を行い、決済システムのデータベース内に格納していた社内用決済管理画面へアクセスするための管理者アカウントの情報（UserID、パスワード）を取得（②）したと推測します。攻撃者は、管理者になりすまして不正ログインして（③）社内用決済管理画面を不正操作したり、同画面の構造を調査したと推測します。

2. A社アプリの画面へのSQLインジェクション攻撃

攻撃者は、同社がA社へ提供しているアプリケーションの会員向け申込フォームへSQLインジェクション攻撃（④）を行い、A社向けアプリケーションのデータベースから、同アプリケーションの管理画面へアクセスできる管理者アカウントの情報を取得（⑤）しました。さらに攻撃者は、 SQLインジェクション攻撃（⑥）で決済システムのデータベースへアクセスして、暗号化済みのクレジットカード番号やマスク済みのクレジットカード番号を取得（⑦）しました。

3. バックドアプログラムの設置及び攻撃

攻撃者は、取得した管理者アカウントの情報を使って、A社向けアプリケーションの管理画面へアクセス（⑧）して、管理機能の一つであるファイルアップロード機能を悪用して、決済サーバ上にバックドアプログラムを設置（⑨）しました。そして、バックドアプログラム経由で、決済システムのデータベースに格納していた全ての情報を不正取得（⑩）したと推測します。このデータベースから不正取得した情報には、暗号化されたカード情報を含みます。

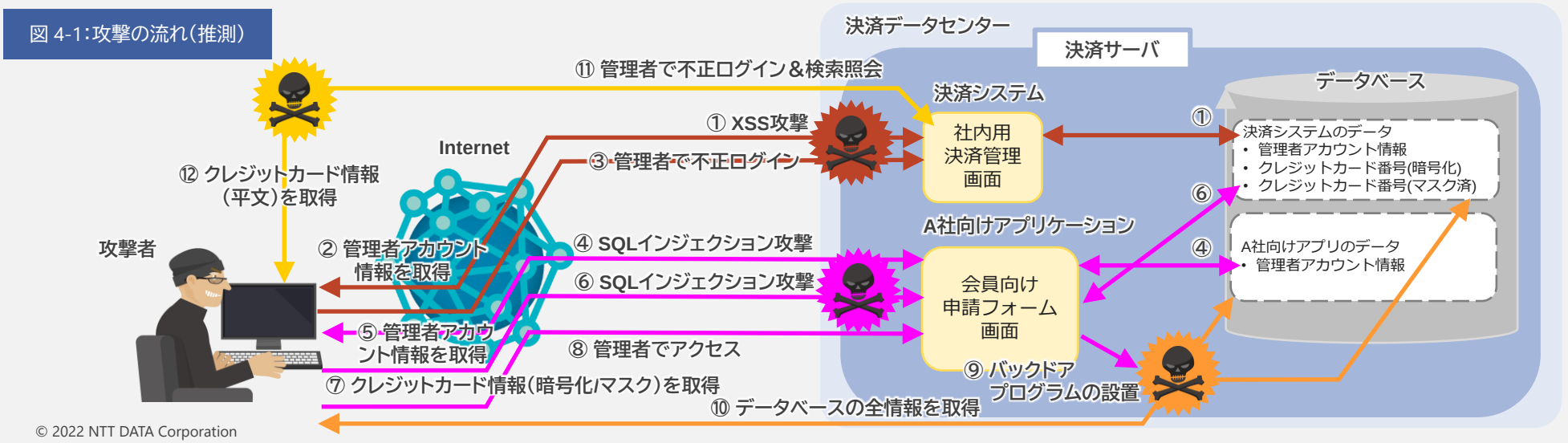
4. 社内用決済管理画面でのカード番号照会

攻撃者は、社内用決済管理画面へ不正ログインして、取得した暗号化済みやマスク済みのクレジットカード番号を検索照会（⑪）して、平文のクレジットカード番号を取得した（⑫）と推測します。

攻撃手法

① XSS攻撃で管理者アカウント情報を入手
③ 管理者アカウントで決済管理画面へ不正ログイン
④ SQLインジェクション攻撃で管理者アカウント情報を入手
⑥ SQLインジェクション攻撃でクレジットカード情報を入手
⑧ 管理者アカウントでA社管理画面へ不正ログイン
⑨ バックドアプログラムを設置
⑪ 管理者アカウントで決済管理画面へ不正ログイン
⑫ 平文のクレジットカード情報を取得

図 4-1:攻撃の流れ(推測)



4.2.1. 問題点

表 4-1のメタップスペイメント社の対応のタイムラインを分析すると、以下の2つの問題点が見つかりました。

（1）攻撃開始から侵害発覚までに時間がかかっている

メタップスペイメント社のWebアプリケーションは、2021年8月31日から攻撃を受けていました。メタップスペイメント社は、2021年10月25日にSQLインジェクション攻撃に気づいていましたが、2021年12月14日にクレジットカード会社からクレジットカードの不正利用の連絡を受けるまで、クレジットカード情報の漏えいのおそれに気づいていませんでした。なぜメタップスペイメント社は、クレジットカード会社から連絡を受けるまで、サイバー攻撃でクレジットカード情報が漏えいしたおそれがあることに気づかなかったのでしょうか。

（2）侵害発覚後も攻撃が続いていた

メタップスペイメント社は2021年12月15日に侵害を認識して、2021年12月17日から第三者機関によるフォレンジック調査を開始していますが、2022年1月25日まで被害拡大を止めることができませんでした。なぜ、侵害発覚から41日間も被害拡大を止めることができなかったのでしょうか。

4.3. 侵害発覚に時間がかかった原因と対策

（1） 侵害発覚までに時間がかかった原因

2021年8月31日から攻撃が始まったが、2021年12月14日に外部から連絡を受けるまでの約4か月間、なぜメタップスペイメント社はサイバー攻撃に気が付かなかったのでしょうか。メタップスペイメント社は、サイバー攻撃や不正ログインを検知できませんでした。なぜ検知できなかったのでしょうか？検知システムが無かったためなのか？それとも、検知システムがあったが不十分だったのか？運用ができていなかったのか？どの点が原因であったのでしょうか。

サイバー攻撃の早期検知に必要なことは、適切な検知システムの導入と運用面での対応です。決済代行業者であるメタップスペイメント社はPCIDSSに準拠するためにも、検知システムを導入していると推測します。しかし、サイバー攻撃が成功していることから、検知能力が不十分だったのではないかと推測します。また、運用にも問題があったかもしれません。検知システムからのアラートやインシデントレポートに基づいてインシデントの発生を判断するのは人間のため、アラートを誤検知と判断したかもしれません。その結果、攻撃成功に気が付かず、大量の個人情報が漏えいしてしまったと推測します。

（2）短時間でサイバー攻撃を検知する方法

ではどのようにすれば、メタップスペイメント社のインシデントは、サイバー攻撃を短時間で検知できたのでしょうか。

当該インシデントで、検知できたと思われるサイバー攻撃や不審なアクションは、以下の4つです。脆弱性を悪用した攻撃は発見しにくいため、除外しています。これらを検知できる検知システムを使っていれば、早期検知できたかもしれません。

1. SQLインジェクション攻撃
2. バックドアプログラムの持ち込みと設置
3. バックドア通信

今回のメタップスペイメント社が受けたサイバー攻撃や不審なアクションのうち、バックドアプログラムの持ち込みと設置、バックドア通信の検知にはEDR（ファイルの振る舞い検知）が有効です。SQLインジェクション攻撃の検知は、UEBA（振る舞い検知）製品が有効です。これらのソリューションを導入していれば、メタップスペイメント社はサイバー攻撃を検知できていたかもしれません。

運用面では、情報セキュリティ専門会社の「SOC （Security Operation Center）」サービスを導入して、24時間365日体制でセキュリティ専門家にネットワークやサーバを監視してもらう対応を推奨します。情報セキュリティの知識や経験が少ない自社社員のみでは、アラートを誤判断して、攻撃成功や被害発生を見過ごしてしまうおそれがあります。最新のサイバー攻撃の知識やアラートの判断経験が豊富なセキュリティ専門家であれば、アラートからインシデント発生を正しく判断できます。

EDRやUEBAのセキュリティソリューションを導入して、SOCサービスを用いてアラートを判断して通知する仕組みを構築していれば、短時間で情報漏えいのリスクに気づいて、初動対応を開始できたかもしれません。

4.4. 侵害発覚後も攻撃が続いていた原因と対策

（1） 侵害発覚後も攻撃が続いた理由

メタップスペイメント社の報告によると、第三者機関によるフォレンジック調査を2021年12月17日に開始していたのにも関わらず、2022年1月25日まで、攻撃者の不正侵入と被害拡大を止めることができませんでした。表 4-1のメタップスペイメント社の対応のタイムラインには、1月8日に攻撃者の侵入を排除して、不正ログイン対策やSQLインジェクション攻撃の対策が完了したと書いてあります。しかし、1月25日にバックドアプログラムの全削除を完了と書いてあることから、1月25日まで攻撃者の侵入を完全に排除できていなかったと思われます。

なぜ、第三者機関によるフォレンジックが始まっていたにも関わらず、不正侵入を止めることができなかったのでしょうか。

① メタップスペイメント社とフォレンジック調査会社との間で、きちんとコミュニケーションできていたのか。

フォレンジック調査会社が、攻撃者がメタップスペイメント社のクレジットカード決済処理サービス「イベントペイ」のユーザの認証情報を取得して、不正な決済に成功していることを知っていれば、すぐクレジットカード決済処理の停止や漏えいしている利用者のアカウントの無効化を進言したでしょう。メタップスペイメント社は、不正なクレジットカード決済処理をもっと早い時期に止めることができたはずです。インシデント対応の担当者が、フォレンジック調査会社からメタップスペイメント社への報告から、正しくリスクを判断できずに、適切に上位へ報告できていなかったのではないかと推測します。

クレジットカードの不正利用被害が拡大し続けると、クレジットカード会社は、クレジットカード利用者の不正利用分を補償しなければなりません。クレジットカード会社は、メタップスペイメント社との取り引きを拒否するでしょう。または保証費用を求めるかもしれません。担当者は、損害の補償だけでなく、クレジットカードの取り引きが停止して事業が継続できなくなるリスクまで認識できなかったのではないでしょうか。そのため、適切な報告ができず、クレジットカード決済処理を停止して、被害拡大の防止が遅くなったのではないかと推測します。

② 経営判断は適切になされていたのか。

メタップスペイメント社は、システムを止めた場合の逸失利益よりも被害の補償額のほうが金額が少ないと判断して、システムを止めなかったのでしょうか。それとも、情報セキュリティインシデントの対応に慣れておらず、システム停止の経営判断に至らなかったのでしょうか。メタップスペイメント社が公表している大規模な情報セキュリティインシデントはこれが初めての事案だったため、大規模のサイバー攻撃でここまで被害が拡大していることが把握できておらず、暫定対処の実施候補の中にシステム停止が挙がらなかったかもしれません。またはお客様のECサイトへの影響を懸念して、迅速にシステム停止の経営判断ができなかったかもしれません。

本来ならば、個人情報の漏えいがあった場合、概ね3～5日以内に個人情報保護委員会へ報告するべきだと言われています。表4-1のタイムラインからは、メタップスペイメント社が個人情報保護委員会へ報告を行ったか否かがわかりません。サイバー攻撃の原因がわからない場合であっても、認証情報が大量に漏えいしていることが推測できれば、メタップスペイメント社は、システムを全面停止すべきだったと思います。メタップスペイメント社は、経営判断が適切におこなえずに、サイバー攻撃発覚後もシステムを全面的に止められず、被害が拡大していったと推測します。

（2）サイバー攻撃を止めて被害の拡大を防ぐために

前述の①、②の原因で被害が拡大したと推測しました。では、どのように対応すれば、もっと被害を少なくできたのでしょうか。各原因の裏返しになりますが、それぞれ以下の対応を取れば、被害の拡大を防ぐことができたでしょう。

①のコミュニケーションの問題は、インシデントが起きる前に、インシデントが発生した場合の具体的な被害の大きさを担当者へ認識させれば、解決すると思います。誤った判断でどれだけの損失が発生するのか、担当者から経営層への報告が遅れれば、遅れた時間でどれだけの損失が発生するのか、損失額を計算すると、迅速に経営層へ報告してシステム停止などの重大な判断を促すことが重要であることが理解できます。

②システム停止の経営判断の問題は、いざという時に組織として対応できるように、サイバー攻撃を想定したインシデント対応のフローやマニュアルを用意すること、実際にインシデントが発生した場合を想定したシナリオを使って、フローやマニュアルにしたがって行動できるように定期的に訓練することで解決できます。この時、担当者だけでなく経営層も訓練に参加して、インシデントの情報から迅速にシステム停止の経営判断を経験することが大切です。

4.5. まとめ

今回、メタップスペイメント社の事例を紹介して、必要な対策を紹介しました。メタップスペイメント社のインシデントでは、攻撃開始から侵害発覚までに時間がかかり、侵害発覚後も攻撃が続いていたため、情報が大量に漏えいしたり、サービス停止の対応が遅くなって被害が拡大したりしたと推測しています。上記の問題は、攻撃の検知の遅れとインシデント対応の担当者のリスク判断のミスとシステム停止の経営判断の遅れが原因だったと思います。EDRやUEBAなどのセキュリティソリューションの導入とサイバー攻撃を想定したインシデント対応のフローやマニュアルの用意、定期的にそれらに沿った訓練を行って、いざという時に迅速に対応できるように備えることが重要です。読者の皆様の組織においても、上記の対策の状況を確認して、サイバー攻撃を受けたときに迅速に対応できるように備えてください。

謝辞

本章の修正に際し、株式会社メタップス様から情報提供の他、多大なるご支援をいただきました。読者へ正確な記事を伝えることができたことに、厚く御礼申し上げます。

“マニュアルの用意はもちろん
経営層も含めた訓練が重要”

5 マルウェア・ランサムウェア
Emotetの感染再拡大、2020年感染ピーク時の5倍に

2021年度第3四半期のレポートにも掲載の通り、Emotetが2021年11月14日頃から攻撃活動を再開しています [12]。2021年度第4四半期も攻撃活動は継続しており、特に2022年2月以降に感染被害が急増しています。情報処理推進機能（以下、IPAという）によると、IPAの情報セキュリティ安心相談窓口へのEmotetに関する相談件数は、2022年2月1日～2月8日は45件、3月1日～3月8日は323件と非常に多い状況です [13]。また、一般社団法人JPCERTコーディネーションセンター（以下、JPCERT/CCという）の調査によると、Emotetに感染してメール送信に悪用されたおそれのある.jpドメインのメールアドレス数は、2020年の感染ピーク時の約5倍以上に急増しています [14]。国内組織でEmotet感染や被害が広がっていると考えられ、非常に危険な状況です。本稿では、2021年度第4四半期におけるEmotetの感染被害状況を整理し、被害が急増している背景の考察、および対策を説明します。

5.1. 止まらないEmotetの感染被害急増

5.1.1. Emotet 感染被害事例

2021年度第4四半期にEmotetの感染被害を発表した日本企業を表5-1へ示します。2021年度第4四半期に明示的に「Emotet感染」と記載している感染被害の事例が70件あり、Emotetの感染被害が急増していることが分かります。

このように感染が拡大したため、IPAおよびJPCERT/CCは、Emotetの感染再拡大を注意喚起しています [13] [14]。また経済産業省、内閣官房サイバーセキュリティセンター（以下NISC）を含む官公庁は、ロシアのウクライナ侵攻に関連した大規模なサイバー攻撃の注意喚起文の中で、同時期に発生したEmotetの増加も取り上げています [85] [86] [87]。

表5-1：Emotetによる感染被害事例（2021年度第4四半期）

No	公表日	組織名称	No	公表日	組織名称
1	2022/1/28	積水ハウス株式会社 [15]	36	2022/2/24	株式会社紀伊國屋書店 [16]
2	2022/1/28	秋葉山公園県民水泳場 [17]	37	2022/2/25	住友三井オートサービス株式会社 [18]
3	2022/2/3	ライオン株式会社 [19]	38	2022/2/25	株式会社京栄センター [20]
4	2022/2/3	株式会社イントラスト [21]	39	2022/2/25	マルイチ株式会社 [22]
5	2022/2/4	リコーリース株式会社 [23]	40	2022/2/26	株式会社ランディックス [24]
6	2022/2/4	株式会社コングレ [25]	41	2022/3/1	東北海道いすゞ自動車株式会社 [26]
7	2022/2/4	日新電機株式会社 [27]	42	2022/3/1	佐田建設株式会社 [28]
8	2022/2/4	コイト電工株式会社 [29]	43	2022/3/2	日本気象協会 [30]
9	2022/2/4	双葉電子工業株式会社 [31]	44	2022/3/2	株式会社農心ジャパン [32]
10	2022/2/4	株式会社風流舎 [33]	45	2022/3/2	NPO法人 アスクネット [34] *1
11	2022/2/4	弁護士法人 三宅法律事務所 [35]	46	2022/3/2	栗田工業株式会社 [36]
12	2022/2/4	テスコム電機株式会社 [37]	47	2022/3/2	株式会社ハクショウ [38]
13	2022/2/4	株式会社ジャストコーポレーション [39]	48	2022/3/2	平田機工株式会社 [40]
14	2022/2/5	株式会社アーキテックプランニング [41]	49	2022/3/2	シグマ光株式会社 [42]
15	2022/2/7	株式会社ワコール [43]	50	2022/3/2	行政書士法人IMS [44]
16	2022/2/7	エスケー工業株式会社 [45]	51	2022/3/2	株式会社ハイロジック [46]
17	2022/2/8	株式会社デザインアーク [47]	52	2022/3/3	フクシマガリレイ株式会社 [48]
18	2022/2/8	アニコムホールディングス株式会社 [49]	53	2022/3/3	株式会社マイナビ [50] *2
19	2022/2/8	株式会社MTG [51]	54	2022/3/3	株式会社共立メンテナンス [52]
20	2022/2/8	イン・プラス株式会社 [53]	55	2022/3/3	南那須地区広域行政事務組合立 [54]
21	2022/2/8	株式会社ワカ製作所 [55]	56	2022/3/4	株式会社マクロミル [56]
22	2022/2/8	株式会社三重電子計算センター [57]	57	2022/3/7	医療法人健晶会 [58]
23	2022/2/8	株式会社3rdcompass [59]	58	2022/3/7	株式会社FCN [60]
24	2022/2/9	株式会社北海道新聞社 [61]	59	2022/3/7	ミナモト通信株式会社 [62]
25	2022/2/9	社会医療法人大雄会 [63]	60	2022/3/8	西日本電信電話株式会社 [64]
26	2022/2/9	クラシエホールディングス株式会社 [65]	61	2022/3/8	一般社団法人日本産業カウンセラー協会 [66]
27	2022/2/9	国際医療福祉大学 [67]	62	2022/3/9	理化学研究所 [68]
28	2022/2/9	株式会社丸山製作所 [69]	63	2022/3/10	学校法人札幌大学 [70]
29	2022/2/9	株式会社エノモト [71]	64	2022/3/10	一般社団法人日本倉庫協会 [72]
30	2022/2/9	株式会社シムネット [73]	65	2022/3/11	株式会社エイチ・アイ・エス [74]
31	2022/2/9	西部電機株式会社 [75]	66	2022/3/15	福島イノベーション・コースト構想推進機構 [76]
32	2022/2/10	奄美市役所 [77]	67	2022/3/15	株式会社グッドマン [78]
33	2022/2/17	東芝ライフスタイル株式会社 [79]	68	2022/3/17	フューチャー・アンティークス株式会社 [80]
34	2022/2/19	福井県永平寺中学校 [81]	69	2022/3/18	株式会社ワイエス・ホームグループ [82]
35	2022/2/24	日本医師会 [83] *3	70	2022/3/23	五興商事株式会社 [84]

*1 社名及び実在する社員を名乗った不審メールの発信が確認されている。感染は未確認。
*2 社名及び実在する社員を名乗った不審メールの発信が確認されている。感染は未確認。
*3 2020年9月に感染した際に流出したデータが再利用されており、新たな感染被害はない。

5.1.2. Emotet感染手法の最新動向

続いて、2021年度第3四半期におけるEmotet感染手法の動向を説明します。Emotetが正規メールの返信を装った攻撃メールや、業務上のやり取りを模倣した巧妙な文面の攻撃メールを使用している点は、以前から変化していません。ただし、攻撃メールの巧妙さは増しており、添付ファイル名に実在する組織名を使ったり、メール本文に実在する組織名や署名などを掲載したりする新しいケースが見つかっています [14]。

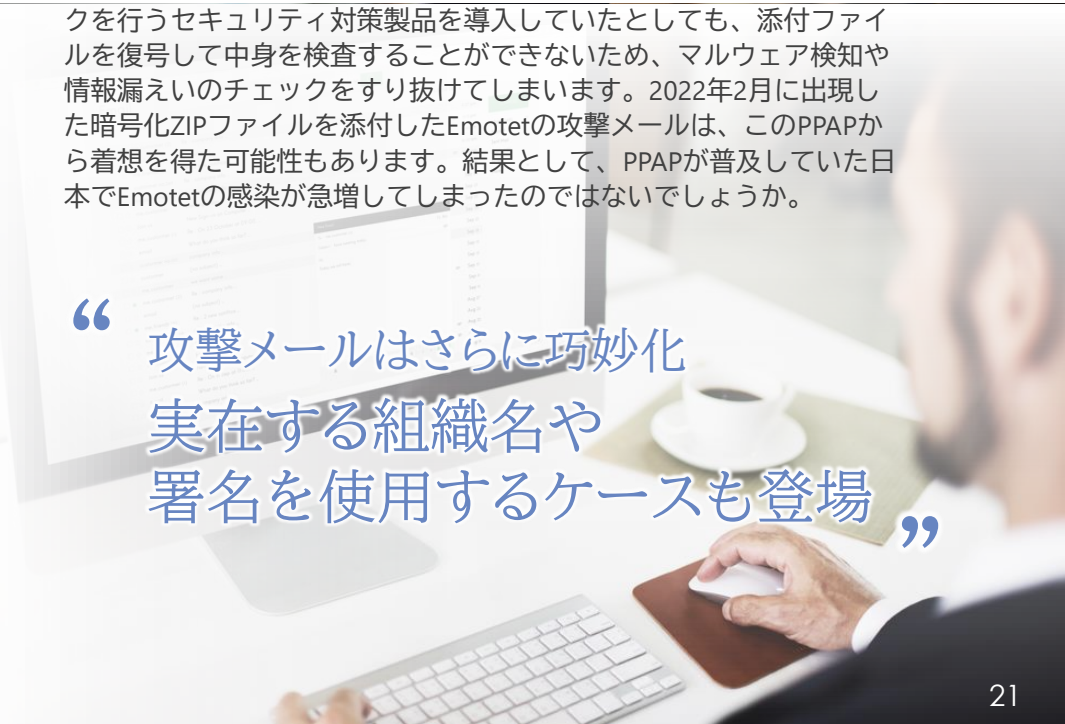
2021年度第3四半期は、Microsoft Wordのマクロ有効文書ファイル（拡張子「.docm」、「.doc」）やMicrosoft Excelのマクロ有効文書ファイル（拡張子「.xlsm」、「.xls」）を攻撃メールに直接添付しているケース、ZIPファイルを添付しているケース、およびメール内にURLリンクを記載しているケースなど、様々なケースがありました。しかし2021年度第4四半期からは、上記のような様々なケースのうち、「.xlsm」ファイルを添付しているパターンと「.xlsm」を格納したパスワード付きZIPファイルを添付しているパターンが主流になっています。

さらに、攻撃メールへ添付するMicrosoft WordやExcelで使用されているマクロが「VBAマクロ」から「Excel4.0」マクロへ変化しました [88]。Excel4.0（XLM）マクロとは、現在の主流であるVBAマクロよりも古いマクロの記述方式です。しかし、新しいバージョンのExcelでも実行可能です。VBAマクロはセキュリティ対策が強化されているため、攻撃者は古いExcel4.0マクロを使用して攻撃するようになりました [89]。2021年度第4四半期のEmotetの感染手法では、Emotet攻撃メールを受信したユーザが、添付されていたExcelファイルのExcel4.0マクロを実行してしまうと、そのマクロプログラムが攻撃者の支配下にあるサーバへ接続して、Emotetマルウェアをダウンロードします。ダウンロードしたダイナミックリンクライブラリファイル（拡張子「dll」「ocx」）をWindowsユーティリティファイル（ファイル名「regsvr32.exe」）から実行し、Emotetの感染に至ります。VBAマクロの場合は、Powershellを使用して実行可能なファイルのダウンロードと実行をおこなってEmotetを感染させていましたが、Excel4.0マクロの場合はPowershellを使用しないで同様の処理をおこなってEmotetを感染させるという特徴があります。

5.1.3. 感染状況の分析

Emotetは世界的に流行しており、CheckPoint社が公表した2022年2月および3月におけるグローバルのマルウェア脅威ランキングでEmotetが1位を獲得しています [90] [91]。その一方で、Cybereason社のグローバルSOCチームは、日本国内でEmotetの感染被害が急増していることに言及し、日本の組織が狙われていると述べています [92]。

グローバルのEmotetの感染被害と比べて、なぜ日本国内の感染被害は急増しているのでしょうか。JPCERT/CCによると、2022年2月に暗号化ZIPファイルを添付して本文に解凍パスワードを記載した攻撃メールが出現してから、被害が急増したと言われています [93]。このように暗号化ZIPファイルをメールへ添付して、その解凍パスワードを同じメールもしくは別メールで送付する方法は、PPAP（Password付きZIPファイルを送ります Passwordを送ります 暗号化Protocol）と呼ばれており、日本だけで普及していたファイルを添付したメールを送付する時の情報漏えい防止対策です。この方式は、送付した添付ファイルが暗号化されているため、メールの添付ファイルにセキュリティチェックを行うセキュリティ対策製品を導入していたとしても、添付ファイルを復号して中身を検査することができないため、マルウェア検知や情報漏えいのチェックをすり抜けてしまいます。2022年2月に出現した暗号化ZIPファイルを添付したEmotetの攻撃メールは、このPPAPから着想を得た可能性もあります。結果として、PPAPが普及していた日本でEmotetの感染が急増してしまったのではないでしょうか。



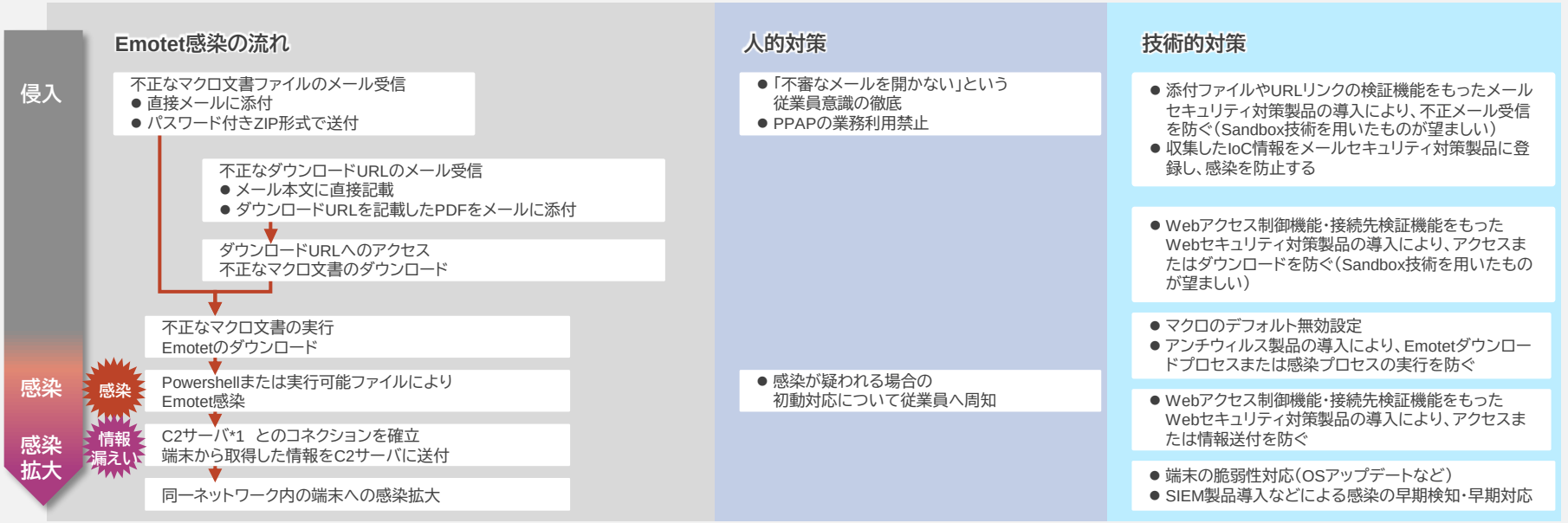
5.2. 対策

前述の感染手法の動向や感染状況の分析を踏まえて、本章ではEmotet感染への対策を説明します。

まず大前提として、Emotetは攻撃メールを契機に感染を拡大します。そのため、不審な添付ファイルやURLを開かないといった基本的な対策が重要です。ただし、前章でも述べた通り、Emotetの攻撃メールは年々巧妙さを増しており、通常の業務メールと見分けることは難しくなっています。そのため、「不審なメールを開かない」といった個人のセキュリティ意識を高めることはもちろん大切ですが、個人のセキュリティ意識だけでEmotet感染を防ぐことはできません。

Emotet感染は、「攻撃メールを開く」「Emotetをダウンロードする」など、感染に至るまでに様々なステップがあります。その一つ一つのステップに対して、それぞれに対策を行って多層防御すれば、Emotet感染のリスクを大きく軽減できます。たとえば2021年度第3四半期のレポートで提案した、Emotetに関するIoC（Indicators of Compromise）情報を入手して、メールセキュリティ対策製品などのセキュリティ機器へ反映する対策は、新しいケースのEmotetの感染を防ぐことができます。Emotet感染のステップに対する人的対策および技術的対策の例を図 5-1に示します。図 5-1の「技術的対策」は、Emotetだけではなく、多くのマルウェア・ランサムウェアに共通した対策です。以下では、図 5-1の「PPAPの業務利用禁止」という人的対策を取り上げて、詳細を説明します。

図 5-1：Emotet感染の流れに対応した人的/技術的対策



*1 Command and Control serverの略称

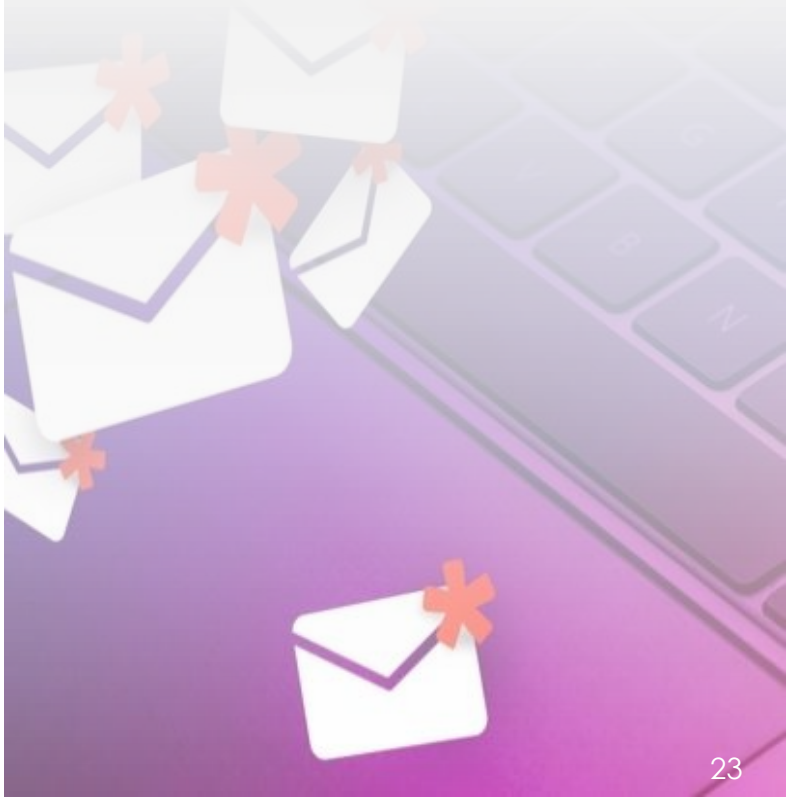
5.2.1. PPAPの業務利用禁止

5.1.3で述べた通り、2021年度第4四半期におけるEmotetの感染被害はPPAPと同じ方式の攻撃メールの出現により急増したと言われています。そもそもPPAPとは、「暗号化ZIPファイルをメールに添付して、その解凍パスワードを電話など別の手段で知らせる」という、個人情報を取り扱う際のセキュリティ対策手法が元になっています。しかし、運用方法の煩雑さから徐々に簡易化され、最終的に現在PPAPと呼ばれている「暗号化ZIPファイルをメールへ添付して、その解凍パスワードを同じメールもしくは別メールで送付する方法」になったと考えています。この手法は、暗号化ファイルと解凍パスワードを同じ経路で送付するため、メールが盗聴されている場合は、情報漏えいにつながるリスクがあります。また前述の通り、添付ファイルは暗号化ZIP形式であるため、多くのメールセキュリティ対策製品では添付ファイルのセキュリティチェックを行うことができません。そのため、攻撃者はマルウェアを暗号化ZIP形式でメールへ添付して送付しています。暗号化ZIPファイルを利用してマルウェアを送付する手法は、Emotetだけではなく IcedIDでも使用しています [94]。

これらの状況から、日本国内でPPAPを廃止する動きがあります。2020年11月に内閣府および内閣官房がPPAPの廃止を公表したことを皮切りに、2021年10月に日立製作所、2021年11月にインターネットイニシアティブ（IIJ）、2022年2月にソフトバンク株式会社が、PPAPの利用廃止を宣言しています [95][96]。一般財団法人日本情報経済社会推進協会と株式会社アイ・ティ・アールが共同で実施した調査結果によりますと、PPAPは送受信とも利用禁止する企業が増える傾向にあり、約3割の企業が受信を禁止する予定としています [97]。

昨今、マルウェアやランサムウェアがPPAPを悪用している状況を踏まえて、各企業のCISOがPPAPの業務利用禁止に踏み切ったとも考えられます。今回取り上げたEmotetの感染防止という観点でも、今こそPPAPの業務利用禁止に踏み切るべきではないでしょうか。

> “情報漏えい対策効果も薄く、Emotet感染の温床となり得るPPAPは利用を避けるべき”



6 予測

PPAP禁止の加速、マルウェア・ランサムウェア配布手段の変化

Emotetの攻撃者が、日本で普及しているPPAPを利用する慣習に目をつけて、PPAP型の攻撃メールを使ったため、Emotet感染が日本国内で拡大しました。日本のEmotetの感染拡大状況から、PPAPの業務利用禁止の動きが加速すると予想します。これによってメールを使ってファイルを送付するケースは減り、ファイル共有サービスを介してファイルを送受信する方法が主流になるのではないでしょうか。

このような状況で気になるのは、今後のマルウェア・ランサムウェアの侵入手口の変化です。今後はEmotetの攻撃者が、PPAPの業務利用禁止を考慮して、ファイル共有サービスを模した攻撃手法を多用するおそれがあります。実際に2021年12月には、Google Driveの偽装ページを使ったEmotetの感染手法が見つかっています [98]。よって、攻撃者が、マルウェアを含んだパスワードZIPファイルを正規のファイル共有サービスへ保存して、標的のユーザにダウンロードさせてマルウェアに感染させる手口を使うことが予想できます。このように、PPAPの代わりにファイル共有サービスの利用が増加すると、ビジネスを装ってファイル共有サービスを悪用してマルウェアに感染させる手口による被害が増加すると予測します。

NFTに関連する法整備の展望

2022年に入ってから、NFT盗難事件が多発しています。デジタルデータには法的な所有権は認められていないため、盗んだ者に対する法的な差し押さえや返還要求を通すことは難しい状況です。

一方で、多発するNFT盗難事件による被害拡大を受けて、2022年4月下旬に英国高等法院は、NFTを財産とみなし盗まれた側は裁判所の差し止め命令により、盗まれたNFTを凍結できるという判決を下しました [99]。本判決については賛否両論ありますが、英国においてはNFTに関連する法整備が進んでいる状況です。

今後NFTの利用が拡大するにつれてNFTを初めて取り引きする利用者が増え、NFT盗難被害がより広がるおそれがあります。英国での動きは世界中に広がり、利用者を法的に保護するべきか否かについての議論が今後進んでいくと予測します。

サプライチェーン攻撃の拡大

サイバー攻撃が発端で、部品供給/生産管理が停止し、企業活動が影響を受けるケースのサプライチェーン攻撃による被害が様々な企業で増えております。2022年3月、トヨタ自動車では関連会社を狙ったサプライチェーン攻撃により、日本のすべての工場で生産停止に陥りました。同月、デンソーのグループ会社や自動車部品メーカーの三桜工業米国子会社おいてもランサムウェアの被害に遭っています。このようにITシステムが製造業の企業活動に占める役割が大きくなっているため、サイバー攻撃が企業リスクになってきています。

今後もしばらくは自動車業界だけでなく、ほかにも同様な影響を受ける企業、業界を狙ったサプライチェーン攻撃が拡大していくと推測します。

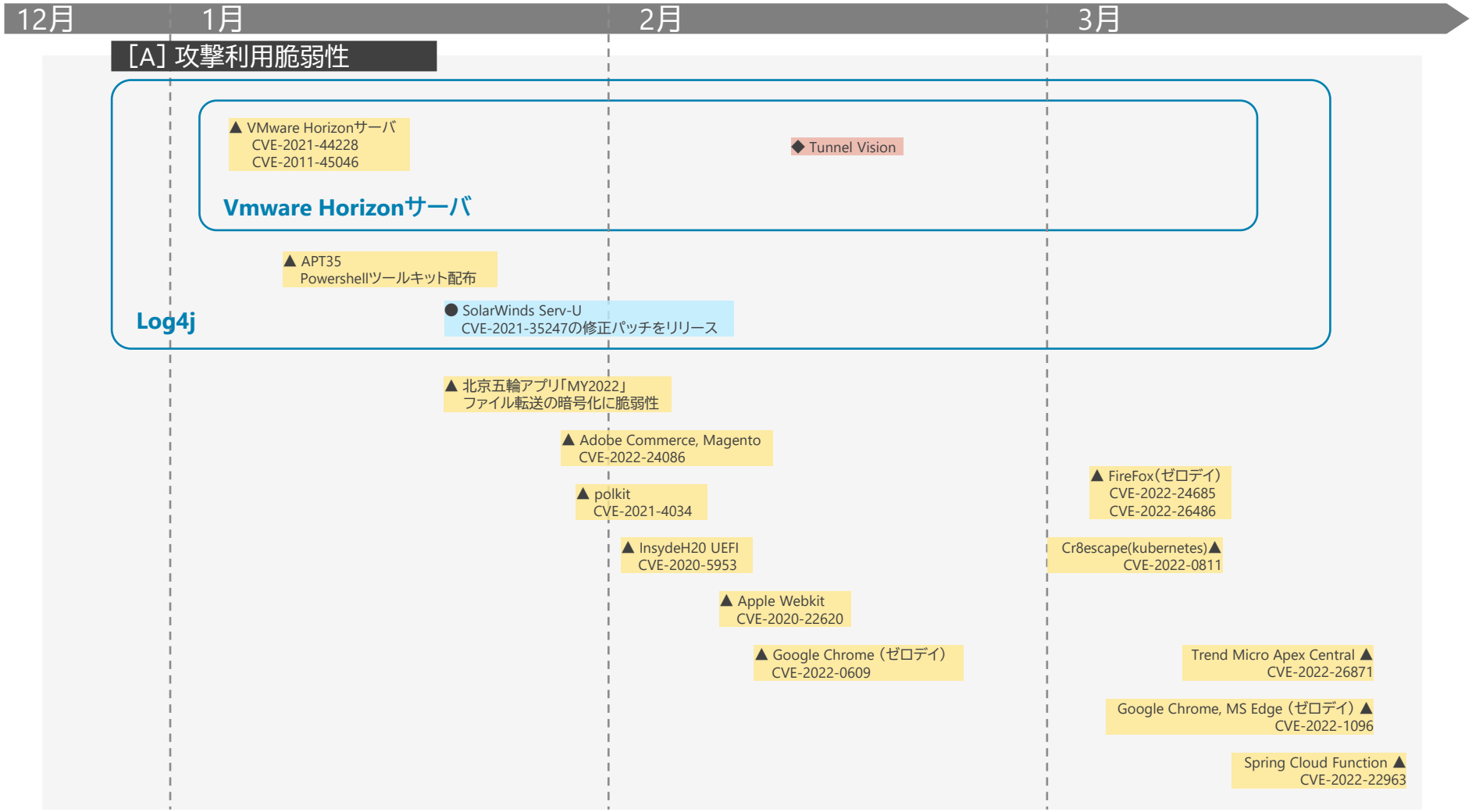
7 タイムライン
事象発生の時系列表

※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

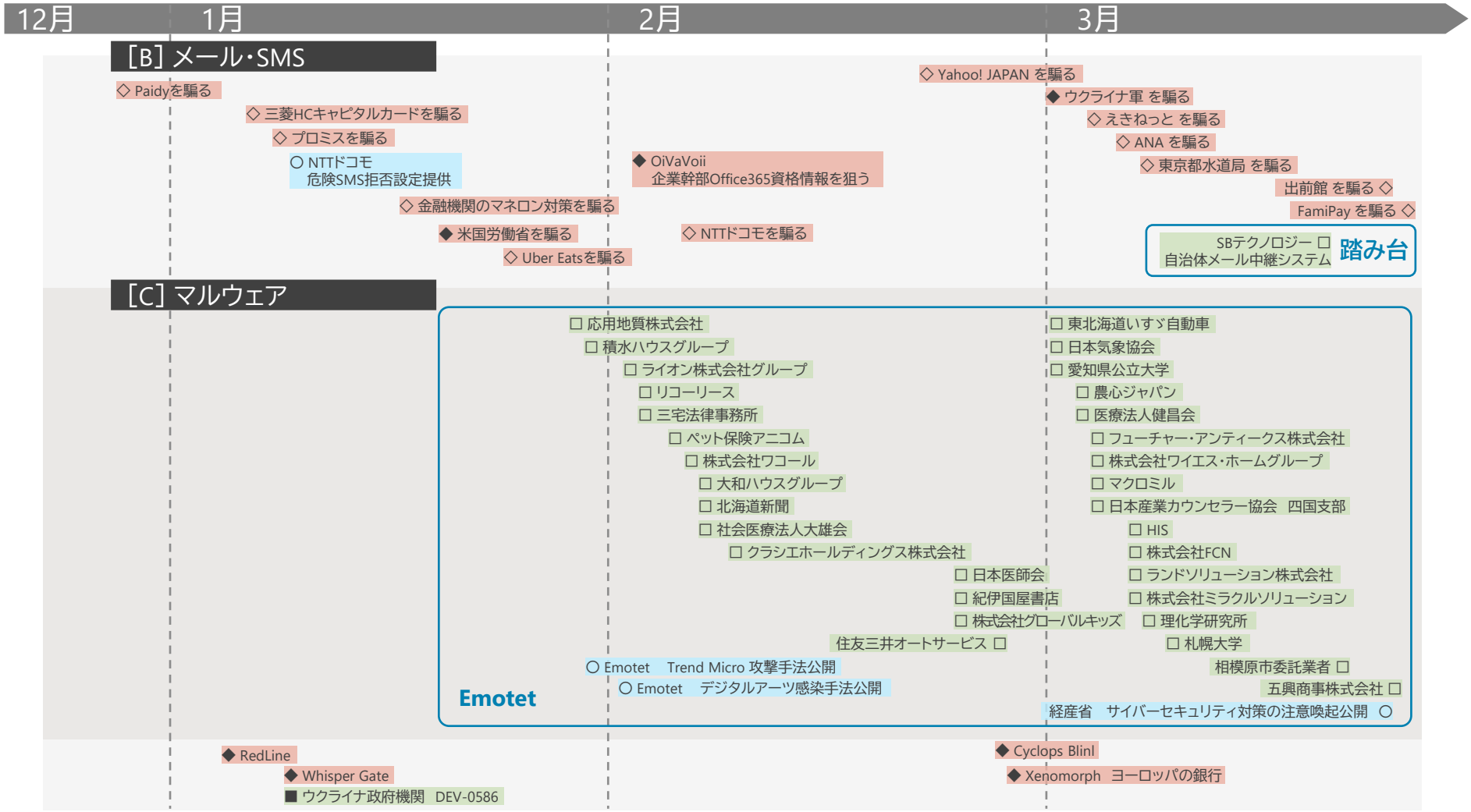


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

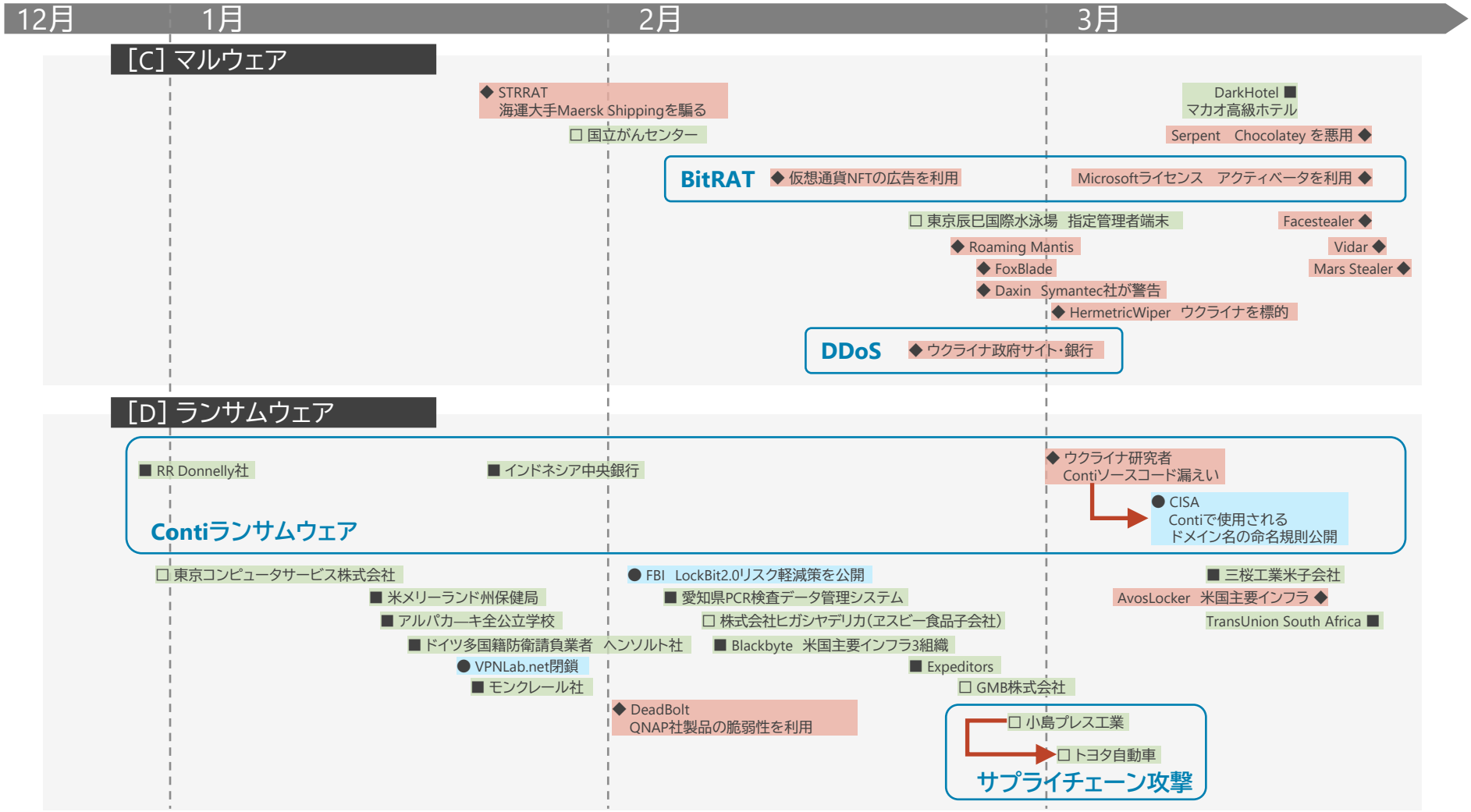
◇◆:脅威
○●:対策



※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

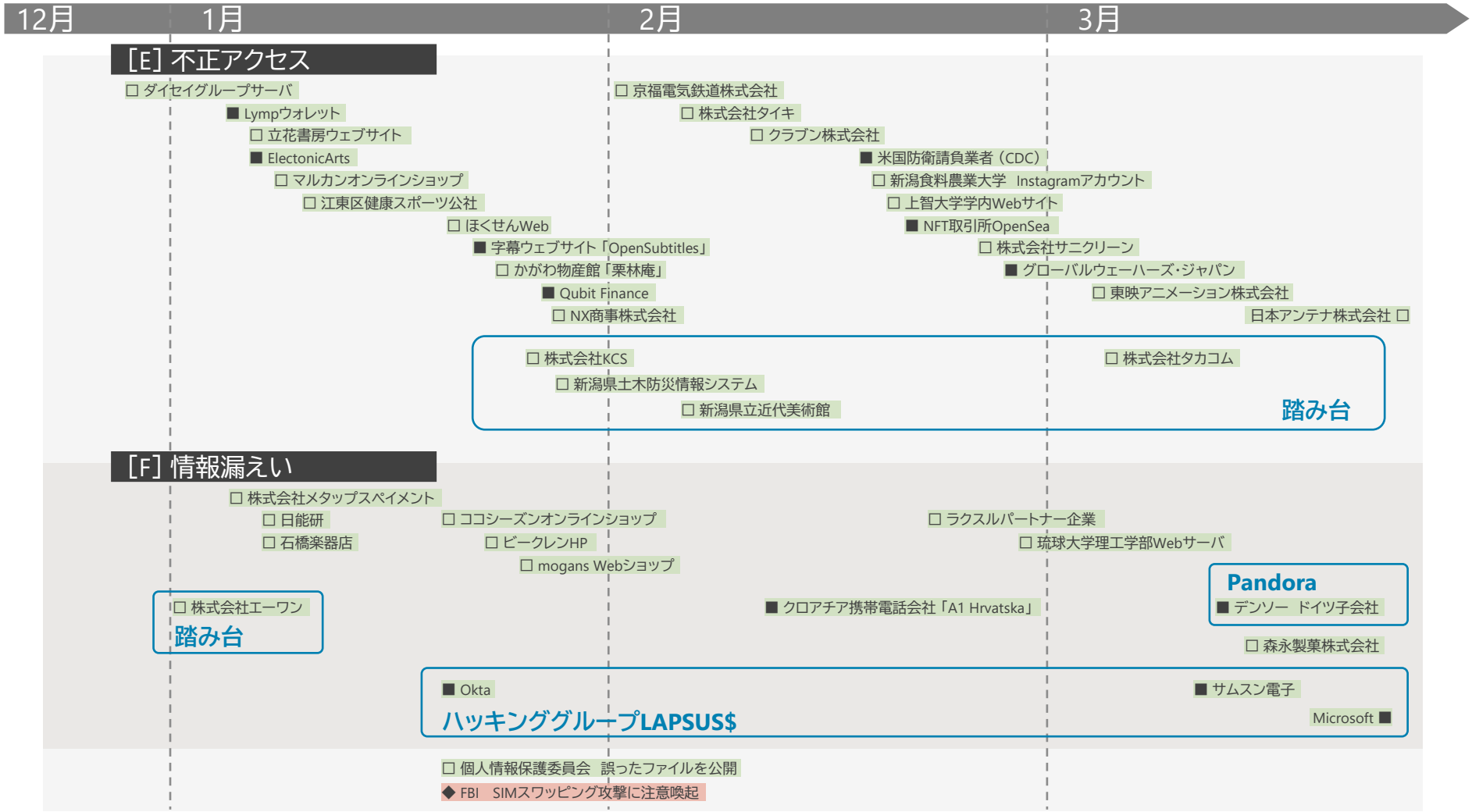


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

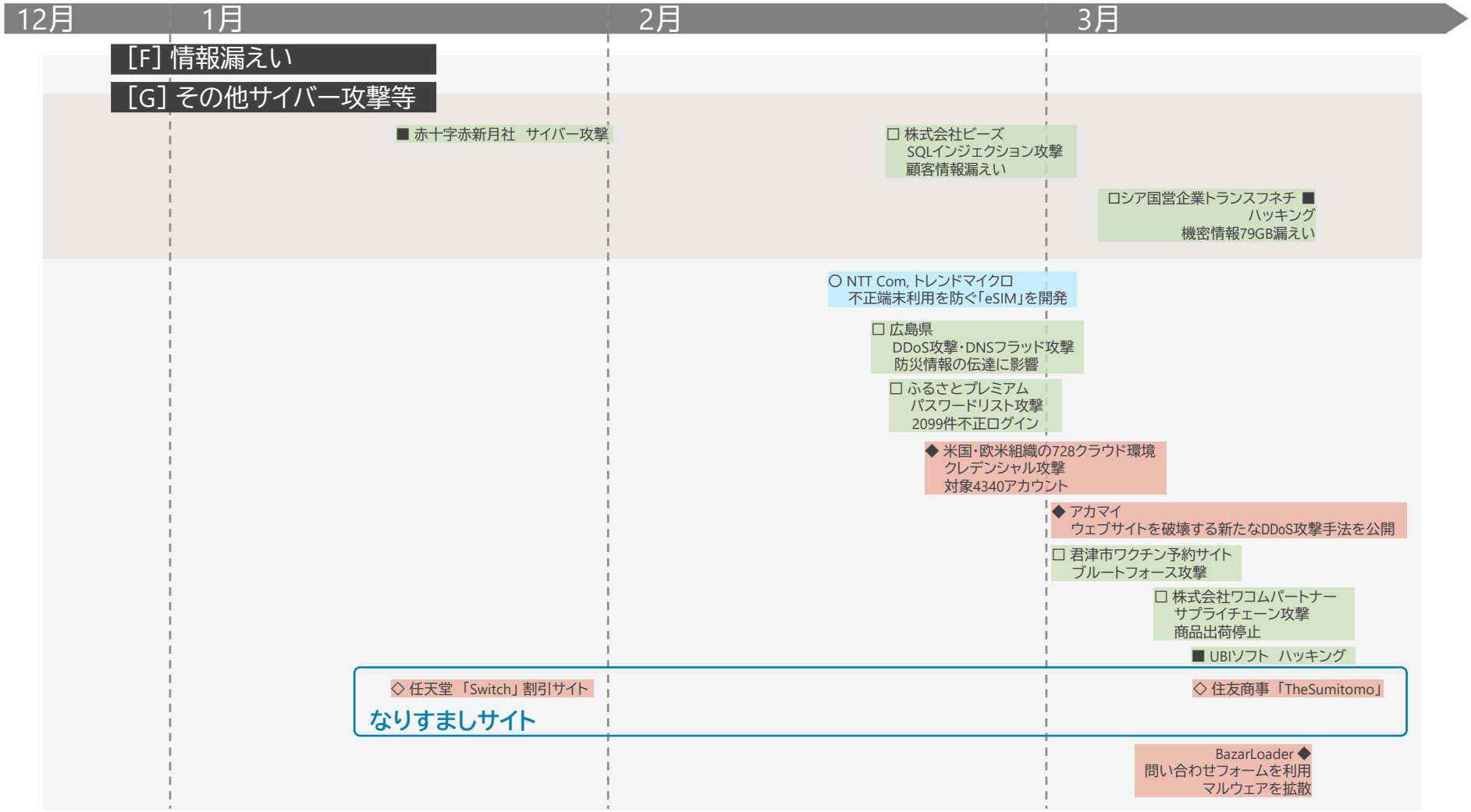


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策



参考文献

[1] “ブロックチェーン | NTTデータ,” [オンライン]. Available: https://www.nttdata.com/jp/ja/services/blockchain/002/.

[2] “BBC NEWS,” [オンライン]. Available: https://www.bbc.com/news/technology-58399338.

[3] “CoindDesk,” [オンライン]. Available: https://www.theverge.com/2022/2/20/22943228/opensea-phishing-hack-smart-contract-bug-stolen-nft.

[4] “Nadav Hollander氏による説明,” [オンライン]. Available: https://twitter.com/NadavAHollander/status/1495509511179755530.

[5] “CoindDesk,” [オンライン]. Available: https://www.coindesk.com/tech/2021/03/15/analysis-ongoing-nifty-gateway-addresses-nft-security-concerns/.

[6] 株式会社 PR TIMES, “Apple、Google、MicrosoftがFIDO標準のサポート拡大にコミット、パスワードレス認証の普及を促進, ” 5 5 2022. [オンライン]. Available: https://prtimes.jp/main/html/rd/p/000000021.000037279.html.

[7] FIDO Alliance, “How FIDO Works, ” [オンライン]. Available: https://fidoalliance.org/how-fido-works/.

[8] Microsoft Corporation, “Cyber Signals, ” [オンライン]. Available: https://news.microsoft.com/wp-content/uploads/prod/sites/626/2022/02/Cyber-Signals-E-1.pdf.

[9] FIDO ALLIANCE, “Multiple Authenticators for Reducing Account-Recovery Needs for FIDO-Enabled Consumer Accounts, ” [オンライン]. Available: https://fidoalliance.org/white-paper-multiple-authenticators-for-reducing-account-recovery-needs-for-fido-enabled-consumer-accounts/.

[10] FIDO ALLIANCE, “How FIDO Addresses a Full Range of Use Cases, ” [オンライン]. Available: https://media.fidoalliance.org/wp-content/uploads/2022/03/How-FIDO-Addresses-a-Full-Range-of-Use-Cases.pdf.

[11] “不正アクセスによる情報流出に関するご報告とお詫び,” メタップスペイメント社, 28 2 2022. [オンライン]. Available: https://www.metaps-payment.com/company/20220228.html.

[12] 株式会社NTTデータ, “サイバーセキュリティに関するグローバル動向四半期レポート（2021年10月~12月）,” 15 3 2022. [オンライン]. Available: https://www.nttdata.com/jp/ja/news/information/2022/031500/.

[13] 独立行政法人情報処理推進機構 セキュリティセンター, “「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて,” 26 4 2022. [オンライン]. Available: https://www.ipa.go.jp/security/announce/20191202.html.

[14] 一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）, “マルウェアEmotetの感染再拡大に関する注意喚起,” 26 4 2022. [オンライン]. Available: https://www.jpcert.or.jp/at/2022/at220006.html.

[15] 積水ハウス株式会社, “弊社グループ従業員を装った不審メールに関するお詫びとお知らせ,” 28 1 2020. [オンライン]. Available: https://www.sekisuihouse.co.jp/company/topics/topics_2022/20220128_m/.

[16] 株式会社紀伊國屋書店, “弊社従業員を装った不審メールに関するお詫び,” 24 2 2022. [オンライン]. Available: https://corp.kinokuniya.co.jp/press-20220224/.

[17] 秋葉山公園県民水泳場, “不審メールに関するお詫びとお知らせ,” 28 1 2022. [オンライン]. Available: https://www.akibasan-pool.jp/.

[18] 住友三井オートサービス株式会社, “当社を装った不審（なりすまし）メールに関するお詫びとお知らせ,” 25 2 2022. [オンライン]. Available: https://www.smauto.co.jp/topics/details/post-10.html.

[19] ライオン株式会社, “弊社を装った不審メールに関するお詫びとお知らせ,” 3 2 2022. [オンライン]. Available: https://www.lion.co.jp/ja/pdf/20220203.pdf.

[20] 株式会社京栄センター, “弊社を装った不審メールに関するお詫びとお知らせ,” 25 2 2022. [オンライン]. Available: https://kyoeicenter.com/information/.

[21] 株式会社イントラスト, “弊社を装った不審メールに関するお詫びとお知らせ,” 3 2 2022. [オンライン]. Available: https://www.entrust-inc.jp/press/2022/1076/.

[22] マルイチ株式会社, “当社従業員を装った不審メールに関するお詫び,” 25 2 2022. [オンライン]. Available: http://www.maruichi-yg.com/news/328/.

[23] リコーリース株式会社, “弊社を装った不審メールに関するお詫びとお知らせ,” 4 2 2022. [オンライン]. Available: https://www.r-lease.co.jp/news/20220204.html.

参考文献

[24] 株式会社ランディックス, “弊社を装った不審メールと個人情報等の流出の可能性に関するお詫びとお知らせ,” 26 2 2022. [オンライン]. Available: https://landix.jp/news/201.

[25] 株式会社コングレ, “当社従業員を装った不審メールに関するお詫びとお知らせ,” 4 2 2022. [オンライン]. Available: https://www.congre.com/news/20220204-12974/.

[26] 東北海道いすゞ自動車株式会社, “弊社社員を装った不審なメールのお詫びとお知らせ,” 1 3 2022. [オンライン]. Available: https://www.east-hokkaido.co.jp/post-1206/.

[27] 日新電機株式会社, “弊社を装った不審メールに関するお詫びとお知らせ,” 4 2 2022. [オンライン]. Available: https://nissin.jp/wp_nissin/wp-content/uploads/2022/02/45ec4c3cd3c86e434385f34e76fb0329.pdf.

[28] 佐田建設株式会社, “弊社を装った不審メールに関するお詫び,” 1 3 2022. [オンライン]. Available: https://www.sata.co.jp/uploads/2022/03/spoofed_mail.pdf.

[29] コイト電工株式会社, “弊社社員からと思われるウイルス付きメールへのご注意のお願い,” 4 2 2022. [オンライン]. Available: http://www.koito-ind.co.jp/news/pdf/20220204.pdf.

[30] 日本気象協会, “日本気象協会職員を装った不審なメールにご注意ください,” 2 3 2022. [オンライン]. Available: https://www.jwa.or.jp/news/2022/03/16006/.

[31] 双葉電子工業株式会社, “当社タイ子会社におけるパソコンのウイルス感染について,” 4 2 2022. [オンライン]. Available: https://www.futaba.co.jp/info/202202_incident.

[32] 株式会社農心ジャパン, “弊社を装った不審メールに関するお詫びとお知らせ,” 2 3 2022. [オンライン]. Available: https://www.nongshim.co.jp/20220302.html.

[33] 株式会社風流舎, “当社を装った不審なメールに関するお詫びと注意喚起について,” 3 2 2022. [オンライン]. Available: https://fuuryusya.com/news/20220204-emotet/.

[34] NPO法人 アスクネット, “弊団体職員を装った不審メールに関するお詫びとお知らせ,” 2 3 2022. [オンライン]. Available: https://asknet.org/topics-archive/.

[35] 弁護士法人 三宅法律事務所, “当事務所の弁護士・職員を装った不審メールに関するお詫びとお知らせ,” 4 2 2022. [オンライン]. Available: https://www.miyake.gr.jp/topics/archives/202202.

[36] 栗田工業株式会社, “弊社グループ従業員を装った不審メールに関するお詫びとお知らせ,” 2 3 2022. [オンライン]. Available: https://www.kurita.co.jp/site/groupnews_220302.html.

[37] テスコム電機株式会社, “弊社を装った不審メールに関するお詫びとお知らせ,” 4 2 2022. [オンライン]. Available: https://www.tescom-japan.co.jp/news/14824.

[38] 株式会社ハクショウ, “当社従業員及び営業所名を装った不審メールに関するお詫びとお知らせ,” 2 3 2022. [オンライン]. Available: https://www.hakusho.co.jp/archives/886.

[39] 株式会社ジャストコーポレーション, “【重要】当社を装った不審なメールに関するお詫びとご報告,” 25 2 2022. [オンライン]. Available: https://www.just-shop.jp/corp/news.asp.

[40] 平田機工株式会社, “弊社社員を装った不審メールに関するお知らせとお詫び,” 2 3 2022. [オンライン]. Available: https://www.hirata.co.jp/files/optionallink/ns_20220302_01.pdf?682951822.

[41] 株式会社アーキテックプランニング, “弊社を装った不審メールに関するお詫びとお知らせ（2月5日）,” 5 2 2022. [オンライン]. Available: https://www.architec-net.jp/info/article.html?id=9567.

[42] シグマ光株式会社, “弊社従業員を装った不審メールに関するお詫びとお知らせ,” 2 3 2022. [オンライン]. Available: https://jp.optosigma.com/html/jp/important/download/20220302_announce_jp.pdf.

[43] 株式会社ワコール, “弊社グループ社員を装った不審メールについて,” 7 2 2022. [オンライン]. Available: https://www.wacoal.jp/info/wacoal/2022/02/post_452.html.

[44] 行政書士法人IMS, “迷惑メールに関するお詫びとお知らせ,” 2 3 2022. [オンライン]. Available: https://imsvisa.support/info/info-4345/.

参考文献

[45] エスケー工業株式会社, “【重要・ウイルス感染に関するお詫びとお知らせ】,” 8 2 2022. [オンライン]. Available: https://www.skkogyo.jp/cont9/main.html.

[46] 株式会社ハイロジック, “ＰＣのウイルス感染に伴う不審メールについてのお詫び,” 2 3 2022. [オンライン]. Available: https://www.hilogik.jp/profile/20220302.pdf.

[47] 株式会社デザインアーク, “弊社従業員を装った不審メールに関するお詫びとお知らせ,” 8 2 2022. [オンライン]. Available: https://www.designarc.co.jp/news/3a5b250fbd435dca35c9e33db9012255d22d5bf1.pdf.

[48] フクシマガリレイ株式会社, “弊社を装った不審メールに関するお詫びとお知らせ,” 3 3 2022. [オンライン]. Available: https://www.galilei.co.jp/info/2404/.

[49] アニコム ホールディングス株式会社, “弊社グループを装った不審メールに関するお詫びとお知らせ,” 8 2 2022. [オンライン]. Available: https://www.anicom.co.jp/news-release/2021/20220208/.

[50] 株式会社マイナビ, “マルウェア「Emotet（エモテット）」によるマイナビ社員を装った不審なメールに関するお知らせ,” 3 3 2022. [オンライン]. Available: https://www.mynavi.jp/topics/post_33410.html.

[51] 株式会社MTG, “弊社を装った不審メールに関するお詫びとお知らせ,” 8 2 2022. [オンライン]. Available: https://www.mtg.gr.jp/news/detail/2022/02/article_2028.html.

[52] 株式会社共立メンテナンス, “弊社グループを装った不審メールに関するお詫びとお知らせ,” 3 3 2022. [オンライン]. Available: https://www.kyoritsugroup.co.jp/news/news-4867/.

[53] イン・プラス株式会社, “弊社を装った不審メールに関するお詫びとお知らせ,” 8 2 2022. [オンライン]. Available: https://www.in-plus.co.jp/wp-content/uploads/2209-1-1.pdf.

[54] 南那須地区広域行政事務組合立, “那須南病院におけるコンピューターウイルス感染と関係者への不審メール発生に関するお詫びとお知らせ,” 3 3 2022. [オンライン]. Available: http://www.minaminasukouiki.jp/wp-content/uploads/2022/03/20220303kokuchi.pdf.

[55] 株式会社ワカ製作所, “弊社を装った不審メールに関するお詫びとお知らせ,” 10 2 2022. [オンライン]. Available: https://www.waka.co.jp/images_up/news/news20220210.pdf.

[56] 株式会社マクロミル, “マクロミルを装った不審メールに関するお詫びとお知らせ,” 4 3 2022. [オンライン]. Available: https://www.macromill.com/press/info/20220304.html.

[57] 株式会社三重電子計算センター, “Emotet感染を狙うなりすましメールに関する注意喚起,” 8 2 2022. [オンライン]. Available: https://www.mieden.co.jp/news/.

[58] 医療法人健晶会, “ウイルス感染に伴う不審メール発生に関するお詫び,” 7 3 2022. [オンライン]. Available: https://www.i-kenshokai.or.jp/news/news_info_20220307.html.

[59] 株式会社3rdcompass, “弊社を装った不審メールに関するお詫びとお知らせ,” 8 2 2022. [オンライン]. Available: https://hiroshima.edono1.com/wp-content/uploads/2022/02/220208_3-3.pdf.

[60] 株式会社FCN, “弊社社員を装う不審メールに関するお詫びと注意喚起,” 7 3 2022. [オンライン]. Available: https://fcn-co.jp/img/220307.pdf.

[61] 株式会社北海道新聞社, “【重要】北海道新聞社を装ったなりすましメールにご注意ください,” 9 2 2022. [オンライン]. Available: https://www.hokkaido-np.co.jp/article/643830.

[62] ミナモト通信株式会社, “弊社社員からと思われるウィルス付きメールへのご注意のお願い,” 7 3 2022. [オンライン]. Available: http://www.minatsu.co.jp/topics/20220307.pdf.

[63] 社会医療法人大雄会, “当会パソコンへのウイルス感染に伴う不審メール発生に関するお詫びとお知らせ,” 9 2 2022. [オンライン]. Available: https://www.daiyukai.or.jp/news/14145/.

[64] 西日本電信電話株式会社, “マルウェア感染による情報流出に関するお詫び、ならびに本件に伴い流出したデータを用いた不審メールに関する注意喚起について,” 7 3 2022. [オンライン]. Available: https://www.ntt-west.co.jp/newscms/attention/11977/20220307_info.pdf.

参考文献

[65] クラシエホールディングス株式会社, “【重要】弊社グループを装った不審メールに関するお詫び,” 9 2 2022. [オンライン]. Available: https://www.kracie.co.jp/soudanshitsu/info/10174101_3856.html.

[66] 一般社団法人 日本産業カウンセラー協会, “不審メールに関するお詫びとお知らせ,” 8 3 2022. [オンライン]. Available: https://www.counselor.or.jp/tabid/101/Default.aspx?itemid=404&dispmid=436.

[67] 国際医療福祉大学, “本学グループ教職員を騙った不審メールに関するお詫びとお知らせ,” 9 2 2022. [オンライン]. Available: https://www.iuhw.ac.jp/news-info/2022/pdf/20220209press.pdf.

[68] 理化学研究所, “（注意喚起）理化学研究所の部署名や職員名を騙る不審メールについて,” 9 3 2022. [オンライン]. Available: https://www.riken.jp/pr/news/2022/20220309_1/index.html.

[69] 株式会社丸山製作所, “弊社を装った不審メールに関するお詫びとお知らせ,” 9 2 2022. [オンライン]. Available: http://www.maruyama.co.jp/news/pdf/20220209-2.pdf.

[70] 学校法人札幌大学, “本学の教職員名を騙る不審メールにご注意ください,” 10 3 2022. [オンライン]. Available: https://www.sapporo-u.ac.jp/news/su-news/2022/03102510.html.

[71] 株式会社エノモト, “弊社を装った不審メールに関するお詫びとお知らせ,” 9 2 2022. [オンライン]. Available: https://enon.co.jp/category/news/.

[72] 一般社団法人日本倉庫協会, “弊協会を装った不審メールに関するお詫びとお知らせ,” 10 3 2022. [オンライン]. Available: https://www.nissokyo.or.jp/news/detail/351/.

[73] 株式会社シムネット, “【重要】アニコムグループを装った不審メールに関するお詫びとお知らせ,” 9 2 2022. [オンライン]. Available: https://www.simnet.co.jp/attentionInfo_03.php.

[74] 株式会社エイチ・アイ・エス, “弊社を装った不審メールに関するご注意のお知らせ,” 11 3 2022. [オンライン]. Available: https://www.his.co.jp/news/11769.html.

[75] 西部電機株式会社, “弊社を装った不審メールに関するお詫びとお知らせ,” 9 2 2022. [オンライン]. Available: https://www.seibudenki.co.jp/temporary/file/news/other/20220209164950.pdf.

[76] 福島イノベーション・コースト構想推進機構, “【重要】マルウェア「Emotet」感染が原因と思われる弊所メールアドレスを悪用したメール送信のお詫びとお知らせ,” 15 3 2022. [オンライン]. Available: https://www.fipo.or.jp/news/18728.

[77] 奄美市役所, “奄美市役所の課名や職員名を装う不審なメールについて,” 10 2 2022. [オンライン]. Available: https://www.city.amami.lg.jp/dx/emotet_202202.html.

[78] 株式会社グッドマン, “当社パソコンのウイルス感染確認とインターネット接続停止について,” 15 3 2022. [オンライン]. Available: https://www.goodmankk.com/data/pressrelease_20220315.pdf.

[79] 東芝ライフスタイル株式会社, “弊社グループを装った不審メールに関するお詫びとお知らせ,” 17 2 2022. [オンライン]. Available: https://www.toshiba-lifestyle.com/jp/topics/2022/02/17/1667/.

[80] フューチャー・アンティークス株式会社, “弊社社員になりすました不審メールに関するお詫びと注意喚起,” 17 3 2022. [オンライン]. Available: https://futureantiques.co.jp/news/emailspoofing/.

[81] 福井県永平寺中学校, “永平寺中学校のパソコンがウイルス感染　世界的被害の「Emotet」、福井県内の教員名で偽造メール,” 19 2 2022. [オンライン]. Available: https://www.fukuishimbun.co.jp/articles/-/1496540.

[82] 株式会社ワイエス・ホームグループ, “当社従業員を騙った不審メールに関するお詫びとお知らせ,” 18 3 2022. [オンライン]. Available: https://www.yshome.jp/input/1111222.pdf.

[83] 日本医師会, “【注意喚起】コンピュータウイルス付きメール(Emotet)に関する注意喚起,” 24 2 2022. [オンライン]. Available: https://www.med.or.jp/people/info/doctor_info/010514.html.

[84] 五興商事株式会社, “弊社社員を装った不審メールに関する注意喚起,” 23 3 2022. [オンライン]. Available: https://www.gokoh.co.jp/pdf/release_20220323.pdf.

参考文献

[85] 経済産業省, “昨今の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）,” 23 2 2022. [オンライン]. Available: https://www.meti.go.jp/press/2021/02/20220221003/20220221003-1.pdf.

[86] 経済産業省、金融庁、総務省、厚生労働省、国土交通省、警察庁、内閣官房内閣サイバーセキュリティセンター, “サイバーセキュリティ対策の強化について（注意喚起）,” 1 3 2022. [オンライン]. Available: https://www.nisc.go.jp/pdf/press/20220301NISC_press.pdf.

[87] 経済産業省、総務省、警察庁、内閣官房内閣サイバーセキュリティセンター, “現下の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）,” 24 3 2022. [オンライン]. Available: https://www.nisc.go.jp/pdf/press/20220324NISC_press.pdf.

[88] デジタルアーツ株式会社, “マクロつきOfficeファイルに注意！EmotetとxlsmファイルとExcel4.0マクロ,” 24 3 2022. [オンライン]. Available: https://www.daj.jp/security_reports/220324_1/.

[89] ZDNet Japan, “マイクロソフト、「Excel 4.0」マクロをデフォルトで無効化,” 25 1 2022. [オンライン]. Available: https://japan.zdnet.com/article/35182549/.

[90] Check Point Software Technologies Ltd., “February 2022’s Most Wanted Malware: Emotet Remains Number One While Trickbot Slips Even Further Down the Index,” 9 3 2022. [オンライン]. Available: https://blog.checkpoint.com/2022/03/09/february-2022s-most-wanted-malware-emotet-remains-number-one-while-trickbot-slips-even-further-down-the-index/.

[91] Check Point Software Technologies Ltd., “March 2022’s Most Wanted Malware: Easter Phishing Scams Help Emotet Assert its Dominance,” 12 4 2022. [オンライン]. Available: https://blog.checkpoint.com/2022/04/12/march-2022s-most-wanted-malware-easter-phishing-scams-help-emotet-assert-its-dominance/.

[92] Cybereason Inc., “THREAT ALERT: Emotet Targeting Japanese Organizations,” 7 3 2022. [オンライン]. Available: https://www.cybereason.com/blog/research/threat-alert-emotet-targeting-japanese-organizations.

[93] 一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）, “日本中で感染が広がるマルウェアEmotet,” 7 3 2022. [オンライン]. Available: https://www.youtube.com/watch?v=wvu9sWiB2_U.

[94] マクニカネットワークス株式会社, “IceID/IcedIDマルウェアへの対応について,” 11 12 2020. [オンライン]. Available: https://mnb.macnica.co.jp/2020/11/iceid.html.

[95] 日本経済新聞, “自動暗号化ZIPファイル廃止　内閣府と内閣官房,” 24 11 2020. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO66572390U0A121C2PP8000/.

[96] ソフトバンク株式会社, “当社におけるパスワード付き圧縮ファイルの利用廃止に関するお知らせ,” 15 2 2022. [オンライン]. Available: https://www.softbank.jp/corp/news/info/2022/20220215_01/.

[97] 一般財団法人日本情報経済社会推進協会、株式会社アイ・ティ・アール, “コロナ禍の長期化に伴い、企業の72.7%がテレワークを実施　電子契約の利用企業は69.7%に拡大,” 17 3 2022. [オンライン]. Available: https://www.jipdec.or.jp/news/news/20220317.html.

[98] Bleeping Computer, 1 12 2021. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/emotet-now-spreads-via-fake-adobe-windows-app-installer-packages/.

[99] “ARTNews,” [オンライン]. Available: https://www.artnews.com/art-news/news/are-nfts-property-stolen-opensea-uk-case-1234627040/.

グローバルセキュリティ動向四半期レポート

2021年度 第4四半期

2022年10月20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 / 大石 眞央 /
松尾 俊彦 / 蓮岡 聡美 / 若林 優太 / 古市 祐貴 / 佐川 友里香
nttdata-cert@kits.nttdata.co.jp