グローバルセキュリティ動向四半期レポート

2022 年度　第 3 四半期

目次

1. エグゼグティブサマリー

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。

注目トピック『ISMAP-LIU制度の使い道』

2022年11月1日にデジタル庁がISMAP-LIU（ISMAP for Low-Impact Use）の運用を開始しました。ISMAPと比較して、登録までにかかる外部監査によるキャッシュアウト等のコスト削減が見込まれる一方、内部監査の報告が必須となることから、社内に監査を実施できる人員や体制を準備することなどが必要になります。

政府機関はクラウドサービスを調達する際、ISMAP、ISMAP-LIUに登録されたサービスから調達することを原則とすると公表していることから、今後は、多くの企業においてもこの流れに追随することが予想されます。登録を検討する際には、メリットとデメリットを鑑み、コストパフォーマンスを検討し、制度を活用していくことが重要です。

注目トピック『パスワードレス認証の世界に向けた、パスキー対応の本格化』

2022年の5月に、Apple、Google、Microsoftが共同で、パスワードレス認証のサポートを拡大する為、マルチデバイス対応FIDO認証資格情報、通称「パスキー」を提供することを発表しました。

パスキーはプラットフォーム側、サービス提供側ともにサポートが拡大しており、今後ユーザはパスキーの特徴である複数デバイスでサービスを利用する際の利便性向上だけでなく、FIDO認証自体のフィッシング耐性やパスワードなしで認証できるといったメリットも享受することができるようになります。

企業などにおいても、今のうちに情報を収集し、パスキーによる認証を利用サービスの認証でどのような位置づけとするか、検討することを推奨します。

情報漏えい『ショーケース社情報漏えい事件からの学び』

2022年10月25日にショーケース社は、第三者が同社の複数のサービスへ不正アクセスしてソースコードを書き換えたため、サービスを利用していた複数の企業の情報が外部へ流出したおそれがあると発表しました。

近年、ECサイトは様々な外部サービスを活用し、ECサイトを実装している場合があり、ソフトウェアサプライチェーン攻撃によって、複数のサイトが情報漏えいの被害を受ける可能性があります。ECサイト側では、外部サービスを把握し、被害拡大防止やリスク回避、転嫁の観点で対策を検討しておくことが重要です。

脆弱性『Microsoft Exchange Serverにおけるリモートコード実行の脆弱性』

2022年11月に修正プログラムが配布された、ProxyNotShellと称されるMicrosoft Exchange Serverにおけるリモートコード実行の脆弱性について解説します。

ProxyNotShellは、複数の脆弱性を組み合わせた攻撃で、Exchange Serverでは過去、本脆弱性と同様に複数の脆弱性を連携させた攻撃によるProxyLogonやProxyShellなどの深刻な脆弱性が発生しています。

Exchange Serverの構成や設定の見直し、他のセキュリティシステムの導入によるリスク軽減だけでなく、各脆弱性について恒久対処となる修正パッチの適用を行うためにも、継続的に脆弱性情報を収集し対処する必要があります。

2. 注目トピック『ISMAP-LIU制度の使い道』

2022年11月1日にデジタル庁がISMAP-LIU（ISMAP for Low-Impact Use）の運用を開始しました [1]。ISMAP-LIUはISMAP（Information system Security Management and Assessment Program）の枠組みのうち、リスクの小さな業務・情報の処理に用いるSaaSサービスを対象とした制度です。

また政府機関はクラウドサービスを調達する際、ISMAP、ISMAP-LIUに登録されたサービスから調達することを原則とすると公表しました。ISMAP、ISMAP-LIUに登録されたサービスは政府機関が求める一定のセキュリティレベルを満たしていることが明確化されることから、 今後は公共分野のみならず、多くの企業においてもこの流れに追随することが予想されます。ISMAP、ISMAP-LIUへの登録はクラウド製品を用いてビジネスを行う上で重要な役割を果たすでしょう。

本稿ではSaaS製品を取り扱う企業担当者の観点から、ISMAP-LIUの内容・仕組み、ISMAPとの違いを説明します。本稿によってISMAP-LIU制度の理解を深め、ISMAPとISMAP-LIUのどちらを取得すべきかの判断材料として頂ければ幸いです。

2.1. ISMAP-LIUの概要

ISMAP-LIUは2022年11月1日から運用を開始した新しい制度です。上記でも記載した通り、ISMAP-LIUはISMAPの枠組みの内、リスクの小さな業務・情報の処理に用いるSaaSサービスを対象とした制度となります。

ISMAP-LIUはISMAPが一部サービスにとっては過剰なセキュリティ要求となってしまう懸念によって作成されました。ISMAPの対象となっている機密性２情報を扱う情報システムは IaaS、PaaS、SaaSと多岐に渡ります。その中でもSaaSはサービスの幅が広く、用途や機能が極めて限定的なサービスや、機密性２情報の中でも比較的重要度が低い情報のみを取り扱うサービス等リスクが低いサービスもあり、それらのサービスについてISMAPと一律の取扱いとした場合、過剰なセキュリティ要求となり、それにより当該サービスの活用が進まないことが懸念されていました。

そういった背景から機密性２情報を扱うSaaSのうち、セキュリティ上のリスクの小さな業務・情報の処理に用いるものに対する仕組みを創設しました。それがISMAP-LIUになります。 [2]

※ISMAP (Information system Security Management and Assessment Program）は政府情報システムのためのセキュリティ評価制度。

※ISMAPは政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的としている。

2.2. ISMAPとISMAP-LIUの制度内容

2.1で説明したようにISMAP-LIU創設の背景にはISMAPが密接に関わっていることが分かります。ここではISMAPとISMAP-LIUの制度内容を説明致します。

2.2.1. ISMAPの制度内容 [3]

（１） 制度導入の目的

クラウドサービスについて、統一的なセキュリティ基準を明確化し、実効性・

効率性のあるクラウドのセキュリティ評価制度とし、一定のセキュリティを担保できるようにすることを目的としています。

（2） 対象

クラウドサービス全般

（3） 登録までの流れ

内部監査→外部監査→登録申請→サービス登録
※内部監査は報告義務なし。

2.2.2. ISMAP-LIUの制度内容 [2]

（1） 制度導入の目的

SaaSにて現行のISMAPと一律の取扱いとした場合、過剰なセキュリティ要求となる場合があるため、SaaSに限定したセキュリティ評価制度を作成することで、一定のセキュリティを担保できるようにすることを目的としています。

（2） 対象

機密性2情報のうちセキュリティ上のリスクの小さな業務・情報を扱うSaaSが対象です。

ISMAP-LIUの対象となる業務（対象業務一覧）がデジタル庁により公表されています。公表された業務内容かつ、SaaSであるシステムはISMAP-LIUの対象となる可能性があります。各業務内容とそれぞれのシステム例は次の通りとなります。

表 2-1 ： ISMAP-LIUの対象となる業務内容とシステム例

No.	業務内容	システム例
1	公表を前提とした政策・制度の立案・調整過程等で民間と連携して作業する業務 （有識者を招いた審議会等の運営を行うために、Web会議による会議運用や、ファイル共有による情報の保存・管理・共有を行う用途）	Web会議サービス ファイル共有サービス
2	政府職員の業務上の役職・氏名情報を扱う業務（政府職員の役職・氏名情報を用いて職員の人事管理やタレントマネジメントを行う用途） ※業務の性質上、従事する職員の情報について厳格な秘匿が求められている場合を除く	人事管理サービス タレントマネジメントサービス
3	名刺情報等の一般に広く提供する範囲の情報、公開情報の配信に伴う配信先等管理情報を扱う業務 （企業、役職、氏名等の名刺情報を登録・管理を行う用途、政府機関等の顧客に対する映像・コンテンツ等の配信に伴う配信先の特定を目的とした情報の登録・管理を行う用途）	名刺管理サービス 映像・コンテンツ配信サービス
4	民間から提供される情報であり、当該情報提供者が低リスクだと判断している情報を処理する業務（民間企業・民間団体が利用しているWeb会議やファイル共有のためのSaaSを用いて、当該情報提供元企業が提供する情報の保存・管理を行う用途）	Web会議サービス ファイル共有サービス
5	オープンソース・公知の事実・一般公開情報を扱う業務だが例外的に要機密扱いとする必要がある場合	公開情報管理サービス

	（Webサイトの公開前情報など、公開が予定されている情報であり、当該情報の公開が意思決定されている情報を扱う用途 機械翻訳を用いて他国の政策情報や技術情報等を翻訳し調査を行う用途（政府の特定情報に対する調査傾向が要機密となる場合））	
6	災害時等に組織構成員の被災状況確認等を行う業務	安否確認サービス
7	組織構成員に対する組織ルールやビジネススキル等の教育を行う業務	社員教育サービス
8	「行政文書の管理に関するガイドライン」において保存期間１年未満に該当するもののうち、定型的・日常的な業務連絡等を扱う業務 （定型的・日常的な業務連絡、日程表等／出版物や公表物を編集した文書／○○省の所掌事務に関する事実関係の問い合わせへの応答／意思決定の途中段階で作成したもので、当該意思決定に与える影響が極めて小さい文書）	ヘルプデスク自動回答サービス 業務連絡サービス

（３） 登録までの流れ

利用省庁による影響度評価を実施→事前申請→LIU適応のSaaSであることの承認→内部監査→外部監査→本申請→サービス登録

2.3. ISMAPとISMAP-LIUの注目すべき相違点

2.3.1. 外部監査の報告項目の差

ISMAPは外部監査の項目として、ガバナンス基準を18項目、マネジメント基準を64項目、管理策基準を1074項目（選択制のため、実際の監査項目数との差異がある可能性あり）と定めています。 [3]

一方、ISMAP-LIUはガバナンス基準が18項目、マネジメント基準が64項目とガバナンス基準とマネジメント基準の項目数は変わらないものの、管理策基準が約148問（※）とISMAPの管理策基準と比較して1/5以下の項目数になっています。[2] [4]※必須となっていないその他の管理策基準は、言明の対象となるサービスにおける組織・環境・技術等に応じて必要とする事項を選択する。

ISMAP-LIUの外部監査では、ガバナンス・マネジメント基準はISMAPを踏襲し、監査項目全量を対象としつつ、管理策基準はサービス基盤・ 構成に直接的な影響を及ぼし得る管理策（一部の重要な管理策）を主な対象とし、外部監査の対象範囲を縮小させています。

これにより、外部監査のキャッシュアウトが削減され、SaaSサービス事業者の負担軽減が期待されます。

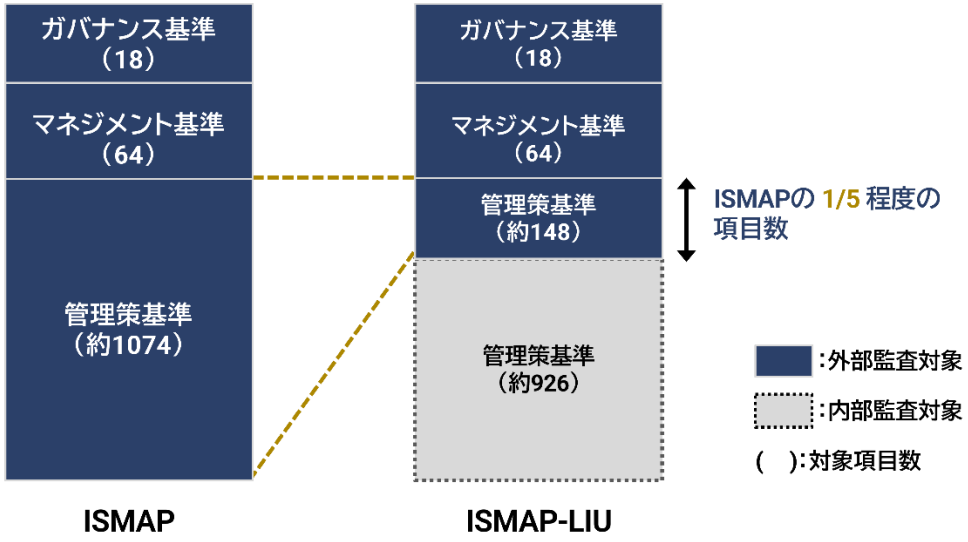


図 2-1 ： 外部監査対象項目数の比較

2.3.2. 内部監査の報告有無

2.3.1にてISMAP-LIUはISMAPと比較して外部監査の項目数が大幅に減少していることを記載しました。しかしながら、ISMAP-LIUにおいては外部監査の対象範囲として除外された項目に関しては、内部監査にて報告を行う必要があります。1.2.1(3)にて記載した通り、ISMAPも内部監査を実施する必要はありますが、全項目を外部監査を実施し、その報告を行うため、内部監査の報告義務はありませんでした。

ISMAP-LIUの内部監査では管理策基準の全ての統制目標（言明書において対象外とした統制目標を除く）について、直近3年間において少なくとも一度は内部監査の対象とされていることが条件となっています。 [2]

一部例外はあるものの、ISMAP-LIUは管理策基準の統制目標とされる3桁管理策（A.B.Cといった3階層目までの項目）を外部監査にて監査し、それを達成するための手段となる詳細管理策である4桁管理策（A.B.C.Dといった4階層目の項目）を内部監査の実施対象としています。 [2] [4]

例）

【外部監査対象】8.1.2 目録の中で維持される資産は、管理する。

【内部監査対象】8.1.2.1 資産の管理責任を時機を失せずに割り当てることを確実にするためのプロセスにおいて、資産が生成された時点、または資産が組織に移転された時点で、適格な者（資産のライフサイクルの管理責任を与えられた個人及び組織）に管理責任を割り当てる。

【内部監査対象】8.1.2.2 資産の管理責任者は、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。

特定の範囲を内部監査で実施するといった切り分けではないことから、機密性2情報のうちセキュリティ上のリスクの小さな業務・情報を扱うSaaSサービス（=ISMAP-LIU対象のシステム）に対しても1年に1度の確認を行う必要があるセキュリティレベルの項目を外部監査にて担保し、詳細のセキュリティ項目は内部監査にて3年に一度点検するとしています。ISMAP-LIUでは内部監査の点検期間を延ばすことで、監査全体におけるランニングコストの削減を図ることも可能と考えられます。しかしながら、監査の周期を伸ばすことは問題の発見が遅れるリスクにもつながるため、ビジネスリスクを鑑みた上で、適切な期間を設定することが重要となります。

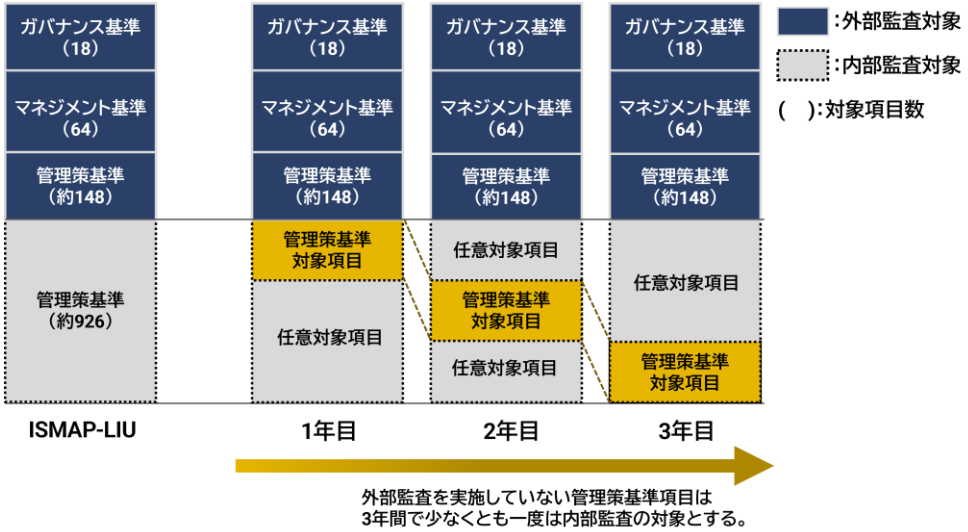


図 2-2 ： 1年ごとの内部監査対象項目

2.3.3. 取消・公表制度

ISMAP-LIUにおける取消公表の流れは、ISMAPにおける再監査、再申請のプロセスを基本的には踏襲しています。しかし、ISMAP-LIUでは特に重大な影響を及ぼしうるインシデントが発生した際には、ISMAP-LIU制度運営側で当該サービスの登録を即座に一時停止する制度設計となっています。 [2]

具体的な一時停止の基準は公表されていませんが、一時停止の制度が追加されたことにより、一時停止中の調達が不可能になります。

2.4. まとめ

冒頭でも記載した通り、ISMAP、ISMAP-LIUに登録することにより、公共機関からのシステム調達が可能になります。ISMAP、ISMAP-LIUに登録することはクラウドサービスの信頼性をアピールすることにつながるため、クラウドサービス事業者のビジネスに重要な役割を果たすことが想定されます。

ISMAPは外部監査の基準レベルが高く項目も多いため、登録までに外部監査のキャッシュアウト等のコストが多く発生していました。対象となるSaaSサービスは限定されますが、ISMAP-LIUの運用が開始されたことで、この外部監査によるキャッシュアウトの削減が見込まれます。また、外部監査の対象から外された項目が3年で1回の内部監査で代替されることから、監査に関わるランニングコストを抑えて、登録することが可能となりました。

ただし、LIUは内部監査の報告が必須となることから、より精度の高い内部監査が必要となるので、社内に監査を実施できる人員や体制を準備することや、登録の一時停止中は調達が不可能になることなど、ISMAP-LIUには注意が必要な点もあります。

メリット・デメリットを鑑み、コストパフォーマンスを検討し、制度を活用していくことが重要になります。

3. 注目トピック『パスワードレス認証の世界に向けた、パスキー対応の本格化』

2022年の5月に、Apple、Google、Microsoftが共同で、パスワードレス認証のサポートを拡大する為、マルチデバイス対応FIDO認証資格情報、通称パスキーを提供することを発表しました [5]。その際は、2023年中に各社のプラットフォームで利用できるようになる予定とのことでしたが、FY2022 Q3に早くも対応が始まりました。

このパスキー、何が期待されているのか、また現状より何が良くなるのか、今後の動向含めご紹介します。

3.1. 普及に課題が残っていたFIDO認証

現在、最もよく使われる認証方式であるパスワード認証は、パスワードの推測、漏洩したパスワードの悪用、フィッシングなど様々な攻撃により、近年も被害事例が絶えません。

そのような問題の多いパスワード認証から脱却し、パスワードレスな世界を目指している認証方法として、FIDO(Fast Identify Online)という国際標準規格があります [6]。

FIDOは、公開鍵暗号方式に基づきます。具体的には、サービスのドメインごとにユーザのデバイスで鍵ペアを作成、秘密鍵はデバイス内の安全な領域に、公開鍵はサービス提供者の認証サーバに送信し、登録します [7]。認証は、デバイスの所持とユーザの生体/知識による本人性確認の組み合わせで多要素認証を実現します。本人性確認結果が成功すれば、サーバから送られたチャレンジに秘密鍵で署名をしてサーバに送付、サーバ側でユーザの公開鍵により署名検証し、認証完了となります。

この仕組みは、パスワード認証にあった問題をクリアしています。デバイス内の秘密鍵の推測は出来ませんし、サービス側で公開鍵が漏洩してもチャレンジへの署名は出来ず、認証情報を不正に生成できません。また、サービスのドメイン名毎に鍵が管理される為、フィッシングサイトに認証情報が送られることもありません。

しかし、2022年12月の段階では、十分に多くのサービスで普及しているとは言い難い状況です。主な理由として、デバイスごとにFIDO鍵の登録が必要な事が挙げられます。たとえば、デバイスの紛失や機種変更の場面を考えてみると、ユーザはサービスごとに鍵の登録をやり直し、サービス提供者は紛失時のアカウントリカバリ用にFIDO認証以外の手段を備える必要があり、煩雑です。認証手段がなくなることに備え複数デバイスを事前に登録する方法もありますが、各サービスを各デバイスに登録する必要があり、ユーザの使い勝手を損なうことにつながります。

3.2. パスキーによる課題の解消

このようなFIDOの課題の解消に向け、2022年の3月にパスキーの導入が発表されました [8]。

パスキーの特徴は、鍵がプラットフォームベンダのアカウントに紐づいたクラウドにバックアップされることです。この仕組みにより、機種変更や紛失によっ

てデバイスを変更する場合や、複数のデバイスを使う場合に、プラットフォームベンダのアカウントにログインすることで鍵が新しいデバイスに同期されます。これにより、従来のFIDOの問題点であった、機種変更や紛失時のサービスへの再登録は必要なくなりました。また、アカウントリカバリ用に認証強度の低いパスワード認証などを残す必要性も減少します。

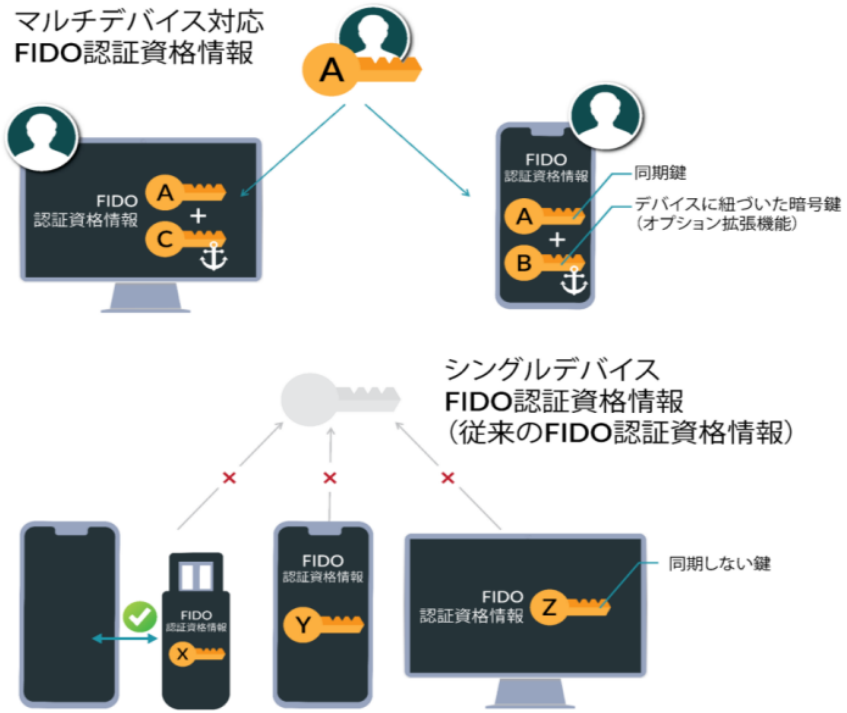


図 3-1 ： マルチデバイス対応FIDO資格情報と従来のFIDOの比較 [9]

一方、パスキーを導入することにより、それまでのFIDOでの前提であった、デバイスとFIDO鍵の紐づけはなくなってしまいます。そのため、パスキーを使う複数デバイスで、どのデバイスからパスキーが来たのかを判別するための、デバイスに紐づいた鍵ペアを作成するオプションが提供されます。このデバイスに紐づいた鍵ペアの秘密鍵は、デバイスに安全に格納されており、抽出が出来ず、パスキーと異なりプラットフォームベンダのアカウントに紐づいて同期されることはありません。

また、パスキーを使うケースを増やす仕組みとして、別端末のパスキーを利用してログインをするhybrid方式も利用可能です [10]。hybrid方式を使うことで、異なるプラットフォーム(AppleやGoogle、Microsoft等)でもパスキーを利用できます。別端末との接続を確立する際には、QRコードとBluetooth Low Energy(BLE)を用います。まず、元のデバイスでQRコードを表示した後、パスキーのあるデバイスで読み込みます。すると、BLE上に認証のやり取りを行うための経路が出来ます。この時、Bluetoothがペアリングされている必要はありません。なお、BLEを利用することで、両方の端末が近くにあり、所持が同じユーザであることを担保し、セキュリティを高めています。

3.3. 2022年10月から本格化したパスキーの導入

3.3.1. FY2022 Q3での主なプラットフォームの対応状況

FY2022 Q3でパスキー対応が進んだプラットフォームベンダはAppleとGoogleです。それぞれの対応状況は以下の通りです。

（1） Apple

プラットフォームとしての対応で先陣を切ったのは、Appleです。FY2022 Q3の直前である9月13日に配信が開始されたiOS16をはじめとして、10月24日にmacOS Ventura、10月25日にiPadOS16.1において、パスキーへの対応を開始しました [11] [12] [13]。同時に、ブラウザはSafari 16から対応が開始しています

Apple系のプラットフォームで作成されたパスキーは、iCloud Keychainに保存されます。これにより、同一のApple IDでログインしているiOS/iPadOS/macOSで横断的にパスキーを利用できます。

（2） Google

Googleも、10月12日にβ版を公開後、FY2022 Q3の後半にかけて、Android 9.0以上向けにパスキーの対応を開始しました [14]。また、Google ChromeもGoogle Chrome 108より、Android/Windows11/macOSでパスキーの対応が開始されました [15]。

Androidでは、パスキーはGoogleアカウントに紐づいたGoogle パスワードマネージャーに保存されます。そのため、Android OS登載端末で横断的にパスキーを利用できます。

3.3.2. クロスプラットフォームの対応状況

AppleとGoogleの事例で紹介した通り、同一プラットフォーム内では、デバイスをまたいだパスキー利用が進んでいます。Windowsはまだパスキーがサポートされていませんが、今後サポートがされることが期待されます。

クロスプラットフォームの対応状況は、現時点では本格な対応は始まっていません。iOS/iPadOS/macOSでのパスキー共有が唯一の事例となります。それ以外はhybrid方式を使うことになります。これは、たとえ同じブラウザを利用した場合でも変わらず、プラットフォームが異なる場合はパスキーが共有されないケースがあるため注意が必要です。一例としては、GoogleのChromeは各プラットフォームでリリースされていますが、パスキーの保存されるプラットフォームベンダのアカウントによって、パスキーの共有される範囲は異なります [16]。

3.4. 2023年のパスキーの想定動向

FY2022 Q3に拡大したパスキーのサポートですが、2023年以降どのように広がっていくでしょうか。

プラットフォーム側では、MicrosoftによるWindowsでのパスキーのサポートが予定されています。予定通りサポート開始されれば、AndroidやiOS/iPad/macOSと合わせて、主要なプラットフォームでパスキーが利用できることになります。

また、クロスプラットフォームでのパスキー利用については、1PasswordやLastPassといったパスワードマネージャーベンダがパスキー対応を表明しています [17] [18]。パスワードマネージャーに対応しているプラットフォーム間で、パスキーを利用できるようになりますので、実現が期待されるところです。一方、LastPassでのインシデントおよびハッキング被害といった事例があります [19]。管理用のアカウントやパスキーがバックアップされたクラウドが被害を受ければ、大きな影響が予想されます。そのため、パスキーのバックアップに用いるプラットフォームのアカウントやパスワードマネージャーの選択は慎重に行う必要があると言えるでしょう。

サービス提供側は、2023年から順次対応が始まると想定されます。すでにいくつかのサービスでは対応が開始、または予定されており、ヤフーのYahoo!JAPAN IDやNTT docomoのdアカウント等があります。このようなIDプロバイダや通信キ

ャリアから導入が始まり、各種サービスに波及していくと想定されます [20] [21]。

サービス提供側のパスキー対応を促進するために、GoogleがAndroidアプリ開発者向けに提供するCredential Managerの様に、プラットフォーマーから実装を容易にするためのライブラリ提供が想定されます [22]。しかしながら、実際にパスキーを導入するには、パスキーをサービスの認証の中でどのような位置づけにするかを決める必要があります。その判断には、プラットフォームのサポート状況も関わってきますので、やはりWindowsでのパスキーサポートがなされてから本格的に動き出すことになると思われます。

3.5. まとめ

パスキー導入は、2022年の後半になってプラットフォームでのサポートが始まったところであり、また、3.1.2で言及したデバイスとの紐づけがオプションとなってしまう問題も含め、まだ仕様が未確定な状態です。しかしながら、残る大きなプラットフォームであるWindowsも当初よりパスキーのサポートを表明しており、利用対象が拡大していくことは間違いありません。これらが解消することで、導入するための環境が揃っていくと思われます。その結果、ユーザは、パスキーの特徴である複数デバイスでサービスを利用する際の利便性向上はもちろん、FIDO認証自体のフィッシング耐性やパスワードなしで認証できるといったメリットも享受できます。

サービス提供側としても、サービス全体としてはすぐにパスワード認証をやめることは出来ないと想定されるものの、パスキー方式を選択したユーザに、フィッシング耐性のある認証方式を提供できるといったメリットがあります。そのため、企業担当者は、導入するための情報収集及び計画立案を行うことを推奨します。計画立案にあたっては、パスキーによる認証を、サービスの認証の中でどのような位置づけとするかをご検討ください。

4. 情報漏えい『ショーケース社情報漏えい事件からの学び』

2022年10月25日にショーケース社は、第三者が同社の複数のサービスへ不正アクセスしてソースコードを書き換えたため、サービスを利用していた複数の企業の情報が外部へ流出したおそれがあると発表しました [23]。その後、同社のサービスを利用していた企業12社は、相次いで情報漏えいの経緯と被害状況の公表を行いました。ショーケース社のサービスは、その特徴からECサイトでの利用が多いと推察します。そこで本稿では、ECサイトにショーケース社のエントリーフォーム最適化ツールを埋め込むなど、自社のECサイトへサービス提供者のサーバ上で処理するツールを組み込む場合に、ECサイト運営者が考慮すべきポイントを解説します。

4.1. ショーケース社情報漏えい事件の概要

ショーケース社によると、攻撃者が不正アクセスしてソースコードを書き換えたサービスは「フォームアシスト」「サイト・パーソナライザ」「スマートフォン・コンバータ」の3つのサービスです。企業が同社のサービスを利用する場合は、同社が提供するJavaScriptを自社のWebサイトのページへ埋め込みます。「フォームアシスト」「サイト・パーソナライザ」「スマートフォン・コンバータ」は、それぞれWebサイトのフォームの入力支援、個別マーケティングの支援やサイトの表示最適化を行います。(図 4-1)

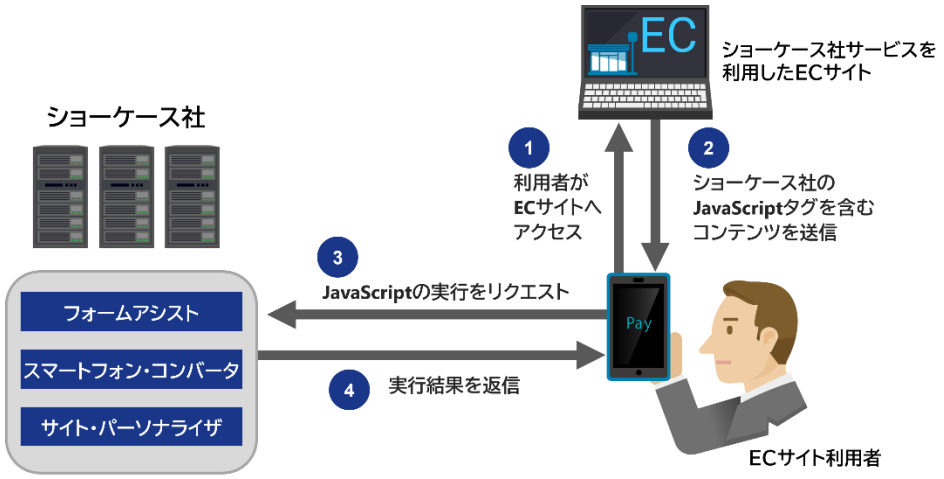


図 4-1 ： サービスの仕組み

こうした仕組みを踏まえ、攻撃者は図 4-2で示す流れで情報の窃取を行ったものとみられます。

① 攻撃者がショーケース社の「フォームアシスト」「サイト・パーソナライザ」「スマートフォン・コンバータ」を提供するサーバの脆弱性を悪用して不正アクセスする。同サーバ上の「フォームアシスト」「サイト・パーソナライザ」「スマートフォン・コンバータ」の JavaScript を改ざんする。
② 利用者がショーケース社のサービスを利用している EC サイトへアクセスする。

③ EC サイトは、ショーケース社の JavaScript タグを含むコンテンツを利用者のブラウザへ送信する。
④ ブラウザは、ショーケース社に JavaScript の実行をリクエストする。
⑤ ショーケース社のサーバは、JavaScript の実行結果をブラウザへ返す。
⑥ ブラウザはショーケース社のサーバの処理結果を表示する。利用者は、例えば商品購入のために郵便番号のフォームへ情報を入力すると、フォームアシスト機能が郵便番号を住所へ変換して住所入力用のフォームへ表示する。このとき、正規の JavaScript は郵便番号を住所にした結果を返すが、攻撃者が改ざんした JavaScript の場合は入力した個人情報を外部に送信する処理が追加されていた。
⑦ 入力した個人情報が、攻撃者のサーバへ送信される。

このように、利用者のブラウザがECサイトのコンテンツを表示した後に、ショーケース社のJavaScriptはショーケース社のサーバで実行してサービスを提供します。そのため、ECサイトのログにはJavaScriptの実行や攻撃者のサーバへの通信の情報が残らないため、ECサイトの運営者が、JavaScriptの改ざんに気付くことは困難だと考えます。このようにして漏えいした情報は、企業が公表した内容によるとクレジットカード番号、有効期限、セキュリティコードなどのクレジットカードに関する情報でした。

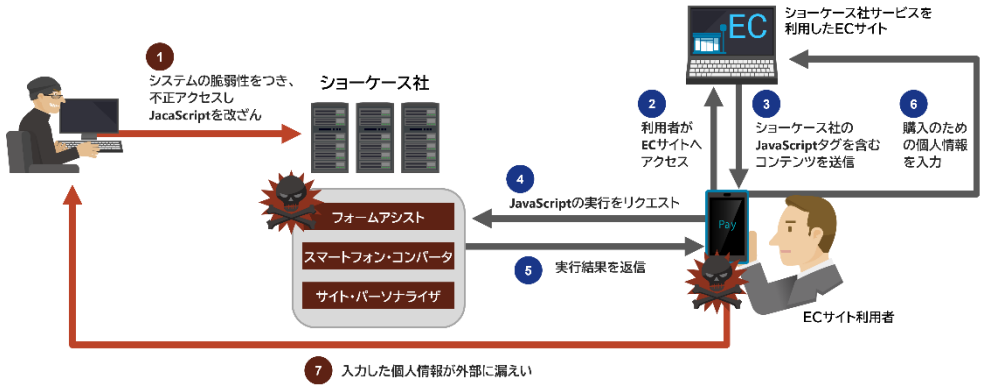


図 4-2：攻撃の流れ

4.2. 本事件の考察

4.2.1. サイバー攻撃の原因の考察

本事件は、ECサイトが使用する外部サービスのソースコードを改ざんし、複数のECサイトから効率的にクレジットカード情報を窃取するサイバー攻撃でした。これは、ECサイトのソフトウェアサプライチェーンに潜在するリスクを巧妙に突いた攻撃と言えます。

ソフトウェアサプライチェーン攻撃とは、ソフトウェアの開発元や配布元などソフトウェアのサプライチェーンを通じて、マルエウェアや攻撃コードを挿入したソフトウェアを配布して攻撃の足がかりにする手法です。今回のショーケース

社の攻撃でも、攻撃者はソフトウェアの開発元であるショーケース社のサーバへ不正アクセスし、サーバ上のJavaScriptを改ざんしています。ECサイトの運営者は、HTMLへショーケース社のサーバ上のJavaScriptタグを追加するのみのため、ショーケース社のJavaScriptの変更の監視は皆無と考えます。たとえ、ECサイトの運営者がJavaScriptを監視したとしても、サービス提供者の正規の変更なのか、攻撃者の改ざんなのか判断することは難しいと考えます。

一方、サービス提供者であるショーケース社の観点でみると、攻撃者が情報を窃取するようソースコードを書き換えたサービスは、クレジットカードなどの決済処理に使う想定ではなかったと推測します。そのため、JavaScriptを実行するサーバのセキュリティ対策や監視体制などは、決済サービス等の厳しいセキュリティ対策基準を満たしおらず、サイバー攻撃が成功したのではと推測します。

4.2.2. クレジットカード決済再開に関する考察

ショーケース社から被害の公表後、すぐに自社の被害を公表してECサイトのクレジットカード決済を再開したECサイトがある一方、ECサイトの被害公表がショーケース社の公表から大きく遅れたり、被害公表後からさらに数カ月経過してからクレジットカード決済を再開したサイトがあったりしました。このようにECサイトの対応期間に差が出てしまった原因は何でしょうか。今回被害のあったECサイトは、表示の最適化やフォームの入力支援等を行うために、WebページのHTMLへショーケース社のJavaScriptタグを追加しています。ECサイト自体の作りを大きく見直さなくても、一時的に当該JavaScriptタグをはずせば、当該ツールからの情報漏えいを停止できたと推測します。当該JavaScriptタグの削除程度の改修であったにもかかわらず、ECサイトの再開が遅れたのは、きちんと利用者が納得できる原因と対策を説明しなければ、顧客離れにつながるおそれがあるため、利用者が納得する情報漏えいの原因や被害を受けた際のサポート、再発防止策など説明の準備に時間がかかったのではないか、と思います。今回のような情報漏えい事件の対応は、ECサイトのコンテンツを更新するだけの対応とは異なります。情報漏えい事件に対応できる要員がいなかったため、慌てて情報セキュリティの専門会社へ相談を行い、対応体制を整えてから対応したために、公表やECサイトの再開に時間がかかったと推測します。

4.2.3. サービス提供者の賠償に関する考察

ショーケース社のサービスを利用するECサイトが、サービス提供者であるショーケース社へ、情報漏えい対応やシステム改修の費用、機会損失などの損害賠償を請求する場合があります。本事件では、ショーケース社がECサイトの運営者へ、どの程度の賠償を行ったのか、明らかになっていませんが、一般的にSaaSサービスにおいて、障害やセキュリティインシデントで発生した損害に対して支払われる賠償額はそれほど高くありません。一般社団法人情報サービス産業協会（JISA）が定める「ASPサービスモデル利用規約」 [24]によると、「現実に発生した通常の損害」かつ「過去12カ月の平均月額料金の1カ月分」を上限とし、「特別の事情から生じた損害、遺失利益」は免責とする旨の記載があります。サービス提供者が多額の賠償を防ぐための対応の一つとして、規約や約款などにこうした記載を含んでいるかもしれません。その場合は、セキュリティインシデントが特別の事情に該当するとした場合、損害賠償額は高くならない可能性があるためです。このような場合、ECサイトは損害を補う手段がありません。

4.3. EC サイト運営者が考慮すべきポイント

ショーケース社の情報漏えい事件は、サービス提供者が管理しているソースコードの改ざんが原因のため、ECサイトの運営者が事件を未然に防ぐ手立てはあり

ません。同等のサービスを内製するという対策も考えられますが、内製に対応できる人材確保と製造コストを負担できるのは、大規模なごく一部のECサイトのみです。では、それ以外のECサイトではどういった点を考慮すればよいでしょうか。

4.3.1. ソフトウェアサプライチェーンの把握

このような事件が起こりうることを踏まえ、まず考慮すべきはソフトウェアサプライチェーンの把握を行うことです。

自社で運営するECサイトで使用している外部サービスの有無を調査して、使用している場合はどのWebページにどういった機能をどういった形式で組み込んでいるか明確にしておきましょう。万が一外部サービスで問題発生した場合に、どのような影響が発生するのか予め整理しましょう。外部サービスで発生するおそれがある問題のケースを列挙して、それぞれのケースを詳細に整理することが理想的です。検討を詳細に行うほど、万が一インシデントが発生した場合も原因調査や暫定処置、復旧判断などの一連の対応が迅速に行えます。それが難しいは、外部サービスの使用状況、使用した外部サービスが停止した際にECサイト自体が停止するのか、そのままでも販売が継続できるかなど、ECサイトへの影響の概要を押さえておくだけでも、有事の際の対応時間の短縮に寄与できるのではと考えます。

なお、クレジットカード番号を保持するECサイトには、PCI DSS Version 4.0 [25]の6.3.2で特注ソフトウェア、およびカスタムソフトウェアのインベントリ維持の遵守が求められています。

4.3.2. インシデント対応や対策検討の相談先の選定

ECサイトの運営者が、インシデント対応も暫定対処、本格対処も行うことができればよいですが、できない場合がほとんどです。その場合は、予めインシデント発生時に相談や対処を依頼する情報セキュリティの専門会社を決めておきましょう。その際参考となる情報としては、経済産業省が策定した情報セキュリティサービス基準に適合すると認められたサービスをまとめたIPAの「情報セキュリティサービス基準適合サービスリスト」[26]やJNSAの「サイバーインシデント緊急対応企業一覧」[27]が挙げられます。こうした情報を元に、相談先を検討するのも一案です。

4.3.3. サイバー保険の活用

ソフトウェアサプライチェーンの把握を行った結果、外部サービスに問題があった場合は、ECサイトの運営者が外部サービス上で発生する情報セキュリティインシデントを未然に防止できないおそれがあります。加えて、4.2.3で考察したように、サービス提供元と損害賠償について係争を行ったとしても約款に基づき少額の賠償に留まるおそれがあります。その後の対応として別サービスの導入が考えられますが、こちらもコストや時間がかかることが推測されます。こうした場合、発生した被害や損害のリスクの転嫁方法としてサイバー保険へ加入することが挙げられます。サイバー保険では、一般的に被害者への損害賠償や争訟費用だけでなく、インシデントの原因調査や問合せコールセンタの設置、喪失利益なども補償の範囲に含まれているため、万が一事件が発生した場合の備えとなります。日本損害保険協会によると、サイバー保険は8社から提供[28]されており、付帯サービスとして簡易リスク診断やインシデント発生時の緊急支援など、インシデント防止や対応のサポートを行ってくれる保険プランもあります。複数の保険を比較した上で、システムやビジネスの規模や補償内容に合った適切な保険プランへ加入すれば、損害を減らすことが可能です。

4.4. まとめ

本稿では、ショーケース社が提供するサービスの改ざんに伴う、クレジットカード情報の漏えい事件の概要を解説し、サイバー攻撃の原因やクレジットカード決済再開、サービス提供者の賠償という観点で考察を行いました。万が一このような事件が起こった場合の備えとして、ECサイト運営者が考慮すべきポイントとして、ソフトウェアサプライチェーンの把握、相談や対処を依頼する情報セキュリティの専門会社選定、サイバー保険という3点を解説しました。こうしたポイントを予め考慮し、問題が起きても迅速に対応し、被害を最小限に留められるよう備えをしておきましょう。

5. 脆　弱　性『 Microsoft Exchange Serverにおけるリモートコード実行の脆弱性』

5.1. Microsoft Exchange Serverにおけるリモートコード実行の脆弱性

本稿では2022年11月に修正プログラムが配布 [29]されたProxyNotShellと称されるMicrosoft Exchange Server（以下Exchange Serverとする）におけるリモートコード実行の脆弱性について解説します。ProxyNotShellは、CVE-2022-41040とCVE-2022-41082を組み合わせた攻撃によりリモートコードが実行可能となる脆弱性の総称です。

5.1.1. タイムライン

本脆弱性についてマイクロソフトによる修正パッチの公開までの出来事を表 5-1に時系列順で示します。

2022年9月28日、ベトナムのセキュリティ企業であるGTSCは監視していたExchange Serverが新しい脆弱性を用いて攻撃されたことをブログで公表しました[30]。マイクロソフトは同年9月30日に脆弱性と緩和策について公表しましたが、修正パッチの提供までには1カ月以上を要しています。

表 5-1 ： ProxyNotShell発見から修正パッチ公開までの時系列

日付	できごと
2022年8月	GTSCが監視するシステムへの攻撃者による攻撃
2022年9月28日	本脆弱性についてGTSCがブログで公表 [30]
2022年9月30日	Microsoftによる脆弱性の公表、および緩和策のガイダンスの提供 [31]
2022年10月上旬	各セキュリティベンダによるIDS/IPS,WAF用のシグネチャのリリース
2022年10月11日	10月の月例セキュリティ更新プログラム公開 （本脆弱性の修正パッチは含まれず）
2022年11月8日	11月の月例セキュリティ更新プログラム公開 [29] （本脆弱性の修正パッチを含む）

5.1.2. 脆弱性の内容

（１） 攻撃対象

本脆弱性の影響を受けるバージョンは、Exchange Server 2013/2016/2019（Exchange Onlineは対象外）です。

（２） 脆弱性の概要

攻撃者は表 5-2に示す2つの脆弱性を連携させた攻撃によってExchange Server上でリモートコードが実行可能となります。

表 5-2 ： 脆弱性の概要

CVE番号	内容	CVSSスコア
CVE-2022-41040	SSRF(Server Side Request Forgery)によりExchange ServerのPowerShellバックエンドに到達できる脆弱性	8.8
CVE-2022-41082	Exchange Serverでリモートコードが実行される脆弱性	8.8

（3） 攻撃の流れ

本脆弱性を悪用した攻撃の流れについてはZero Day InitiativeにおいてPiotr Bazydło氏がPoCを用いて詳細な解析を行っています [32]。図 5-1に示すように、攻撃は2つの脆弱性を順に使って行われます。

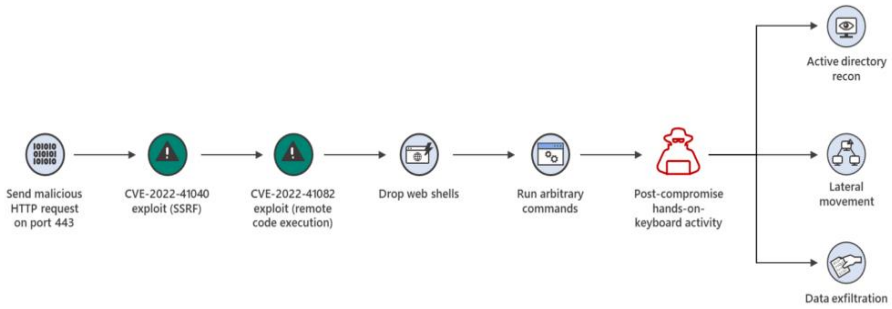


図 5-1 ： ProxyNotShellによる攻撃のダイアグラム [33]

ステップ1（CVE-2022-41040）：

Exchange ServerにはOutlook等のクライアントが構成情報を自動で設定するための自動検出サービス(autodiscover)が備わっています。自動検出サービスはIIS(Internet Information Service)上で実行されるサービスで、悪用のためのリクエストを自動検出サービスへ送信するSSRF攻撃によりExchange ServerのPowerShellバックエンドへの到達が可能となる脆弱性を用いて攻撃が行われます。

この脆弱性を用いた攻撃を行うには認証済みのアクセスが必要となりますが、特権ユーザである必要はなく一般のユーザアカウントを使用することができます。認証情報（ID/パスワード）はフィッシング攻撃やアンダーグラウンドの市場で入手されることも考えられます。

ステップ2（CVE-2022-41082）：

ステップ1で到達可能となったPowerShellでリモートプロトコルを用い攻撃用のオブジェクトをシリアライズしたものをペイロードに乗せることで攻撃が行われます。通常はPowerShellのデシリアライズ処理によって攻撃用のオブジェクトは検証されインスタンス化されることはありませんが、一部のシリアライズ処理に問題があり攻撃者は任意のオブジェクトをインスタンス化することができます。Piotr Bazydło氏による検証ではXamlReaderオブジェクトを利用することでリモートからのコード実行に成功しています [32]。また、XamlReaderオブジェクトの他にも悪用できるオブジェクトがあることも示唆されています。

これら2つのステップを経て攻撃に成功した攻撃者は、Webシェルを配置するなどして、ラテラルムーブメントやデータの窃盗を行うことが可能となります。GTSCによる報告ではオープンソースのWebサイト管理ツールであるAntSword、およびそれに含まれるWebシェルが配置されていたことが確認されたと公表されています [30]。

5.2. 対策

前節で見てきた攻撃の流れをふまえて、5.1.1節のタイムラインに沿って本脆弱性への対策について時系列で考察します。

5.2.1. 脆弱性が公表されるまで

この段階では攻撃自体を検知・防止することは困難ですが、設計やセキュリティシステムによる未然防止や検知が行えた可能性はあります。

■ 攻撃されにくい構成や設定

Exchange Serverについて本脆弱性が成立しない構成や設定をとっていれば攻撃を未然に防止できました。たとえば、

- VPNを使用するなどExchange Serverを外部に直接公開しない構成としていた場合(CVE-2022-41040への対策)
- PowerShellの実行権限を持つユーザを管理者などに限定していた場合(CVE-2022-41082への対策)

など、攻撃に晒される対象をあらかじめ減らしておくことによって攻撃のリスクを軽減することができました。

■ 侵入後のアクション検知

攻撃者は脆弱性による侵入に成功した後、Webシェルの配置やシステムファイルの書換えなど次の攻撃のためのアクションを行います。これらのアクションを構成管理ツールやアンチマルウェアソフトによって検知できれば被害をおさえられました。

5.2.2. 脆弱性の公表から修正パッチのリリースまで

マイクロソフトは脆弱性の公表とともに修正パッチのリリースまでの期間のために緩和策についてガイダンスを提供しました。

また、セキュリティベンダはマイクロソフトの公表から数日でIDS(Intrusion Detection System)/IPS(Intrusion Prevention System), WAF(Web Application Firewall)等、自社のセキュリティ製品のための対応をリリースしています(表 5-3)。これらを適用することで、マイクロソフトによる修正パッチのリリースまでの期間、攻撃を検知もしくは防止することができました。

IDS/IPS, WAF用のシグネチャは自動適用できるものもありますが、マイクロソフトが提供する緩和策についても2021年9月以降のCU(Cumulative Update) に含まれるEEMS(Exchange Emergency Mitigation Service) を利用していれば自動的に緩和策が適用されます。そのため、EEMSは脆弱性情報の収集が頻繁に行えない場合には有効です。

表 5-3 ： セキュリティベンダによる対応例

ベンダ	情報公開日	対応製品／サービス
Fortinet	2022年9月30日 [34]	FortiWeb FortiGate 等
トレンドマイクロ	2022年9月30日 [35]	Cloud One Deep Discovery Inspector
Imperva	2022年9月30日 [36]	Cloud WAF WAF Gateway
Akamai	2022年10月3日 [37]	Kona Defender App&API Protector
F5	2022年10月3日 [38]	ASM Advaced WAF

5.2.3. 修正パッチのリリース後

2022年11月8日に本脆弱性への修正パッチが含まれた月例セキュリティ更新プログラム（KB5019758）が公開されました [29]。修正パッチの適用により本脆弱性への恒久対処が完了となります。

5.2.4. 侵入済みの可能性

5.2.1～5.2.3節のいずれの対策も実施する前に、本脆弱性を悪用した攻撃により既に攻撃者の侵入を許している可能性を考慮する必要があります。

それぞれの対策を講じる前に攻撃者が侵入していないか充分に調査を行い、もし攻撃が認められた場合には、その影響を排除してから対策を行いましょう。

5.3. 過去の脆弱性との比較

ProxyNotShellは、DEVCORE社のTsai氏により2021年に発見された脆弱性であるProxyShellに倣って命名されました。Tsai氏は、本レポートでも取り上げたProxyLogonとProxyShell以外にもExchange Serverの複数の脆弱性を組み合わせるとサイバー攻撃が成立する脆弱性ProxyOracle, ProxyRelayも発見しています [39] [40] [41] [42]。

これらのProxyNotShell以前の脆弱性は、Tsai氏が脆弱性を発表した後に実際のサイバー攻撃が発生していました。しかしProxyNotShellでは開発元のMicrosoftやセキュリティの公的機関が脆弱性を発表する前に、攻撃者は本脆弱性を悪用してサイバー攻撃を行っていました。つまり攻撃者は、複数の脆弱性を組み合わせた複雑な脆弱性を見つける技術を獲得して、複雑な脆弱性を探しはじめたと考えられ、脆弱性を狙ったサイバー攻撃は新しいステージに入ったといえます。

また、Tsai氏はExchange Serverのシステム構成に関係する別の脆弱性が存在するおそれも示唆しており、今後、攻撃者が複数の脆弱性を組み合わせた複雑な脆弱性を発見してサイバー攻撃する事例が、もっと多く発生すると予想します。

5.4. まとめ

本脆弱性はExchange ServerやPowerShellの仕様を熟知したものによる攻撃であり、脆弱性の具体的な内容が公表されるまでは攻撃そのものを検知もしくは防止することは困難と思われます。

5.2章で考察したように、Exchange Serverの構成や設定の見直し、他のセキュリティシステムの導入はリスク軽減にはなりますが、恒久対処にはなりません。Exchange Serverにおいては今後新たな脆弱性が発見される懸念もあり、各脆弱性について恒久対処となる修正パッチの適用を行うためにも継続的に脆弱性情報を収集し対処する必要があります。

6. 予測

アフターコロナの情報セキュリティ

2023年5月から、新型コロナウイルス感染症(COVID-19)の感染法上の分類が引き下げられます [43]。2022年度第2四半期の本レポートでも取り上げたように、COVID-19の流行下で各企業はテレワークの導入拡大や機密情報の取扱いに関して、特例や例外ルールを設けました [44]。しかし、特例や例外ルールは事業継続性の確保を優先しているため、セキュリティリスクの評価やセキュリティ対策が充分に行なえていないままの企業も多くあります。実際にテレワーク中の情報漏えい [45]も発生しており、企業は特例や例外ルールの見直しや廃止、または追加対策の導入へ速やかに着手するべきです。しかし、テレワークのメリットが大きくて出社勤務へ戻せない、セキュリティ対策を行うコストやノウハウがない等の理由からセキュリティリスクを抱えたまま、テレワークを継続する企業も残ると推測します。

アフターコロナへの移行期においては、各種規制や自粛の緩和により従業員がテレワークの実施場所を自宅からカフェやワーケーション先など情報セキュリティの担保が難しい場所へ拡大するため、端末や記憶媒体の紛失・盗難等の情報セキュリティインシデントが増加すると推測します。

テレグラムによる犯罪の増加

テレグラムは、暗号化はもちろん、一定時間で投稿を削除したり、スクリーンショットを制限したりするなど、セキュリティ機能が豊富で利用者が安心して使用できる秘匿チャットアプリです。ネット検閲が行われている国などでは、その対抗のためのツールとしても活用しています。一方でテレグラムは、身元と通信内容の秘匿性が高く、犯罪の証拠を隠滅しやすいため、犯罪者にとっても都合のよいアプリです。そのため、闇バイトや薬物売買などの犯罪でも悪用されています。「ルフィ」などと名乗る指示役らによる広域強盗事件でも使用され、広く報道されました。

こうした状況から、今後、犯罪にテレグラムを悪用する人やいじめなど悪意を持って使用する人が増加すると予測します。また、テレグラムを使って犯罪の情報を調べようとする人が増加することも懸念されます。

一方でテレグラムにも欠点があります。初期設定ではエンドツーエンドの通信を暗号化しない、3人以上のチャットでは完全な暗号化ができない点が挙げられます。加えて、自分の電話番号を相手に公開する設定が可能で、自身の身元判明につながるおそれもあります。テレグラムで闇バイトなどの情報に軽はずみにアクセスして、犯罪者にやりとりの記録や自分の情報が渡ってしまい、犯罪者に情報を悪用されたり、犯罪に巻き込まれたり…といったことが起こるかもしれません。

テレグラム自体は世界で広く使い使われているアプリで、利用すること自体は問題ありません。もちろんテレグラムを悪用して犯罪することはダメですが、テレグラムで犯罪に関する情報へ軽はずみにアクセスしないようにしましょう。

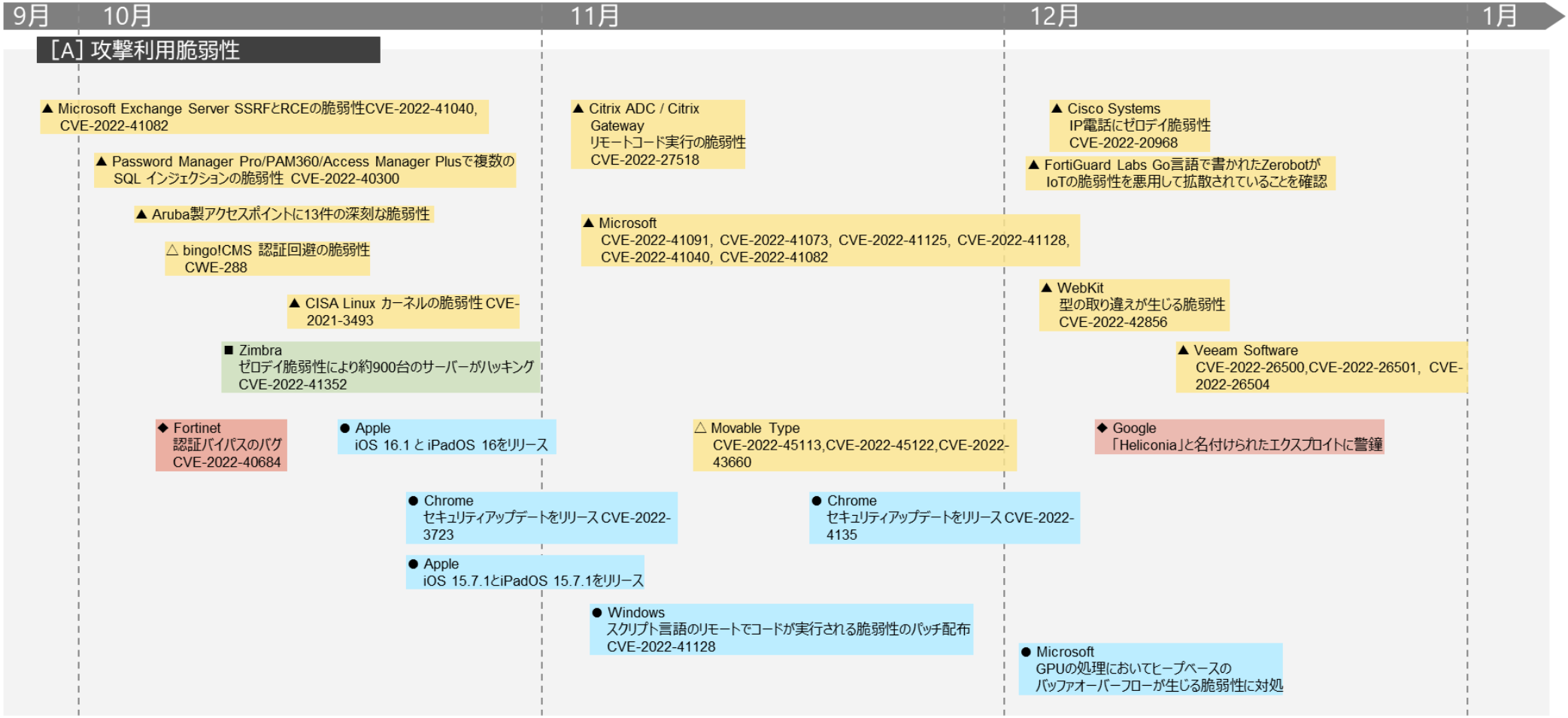
7. タイムライン

※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

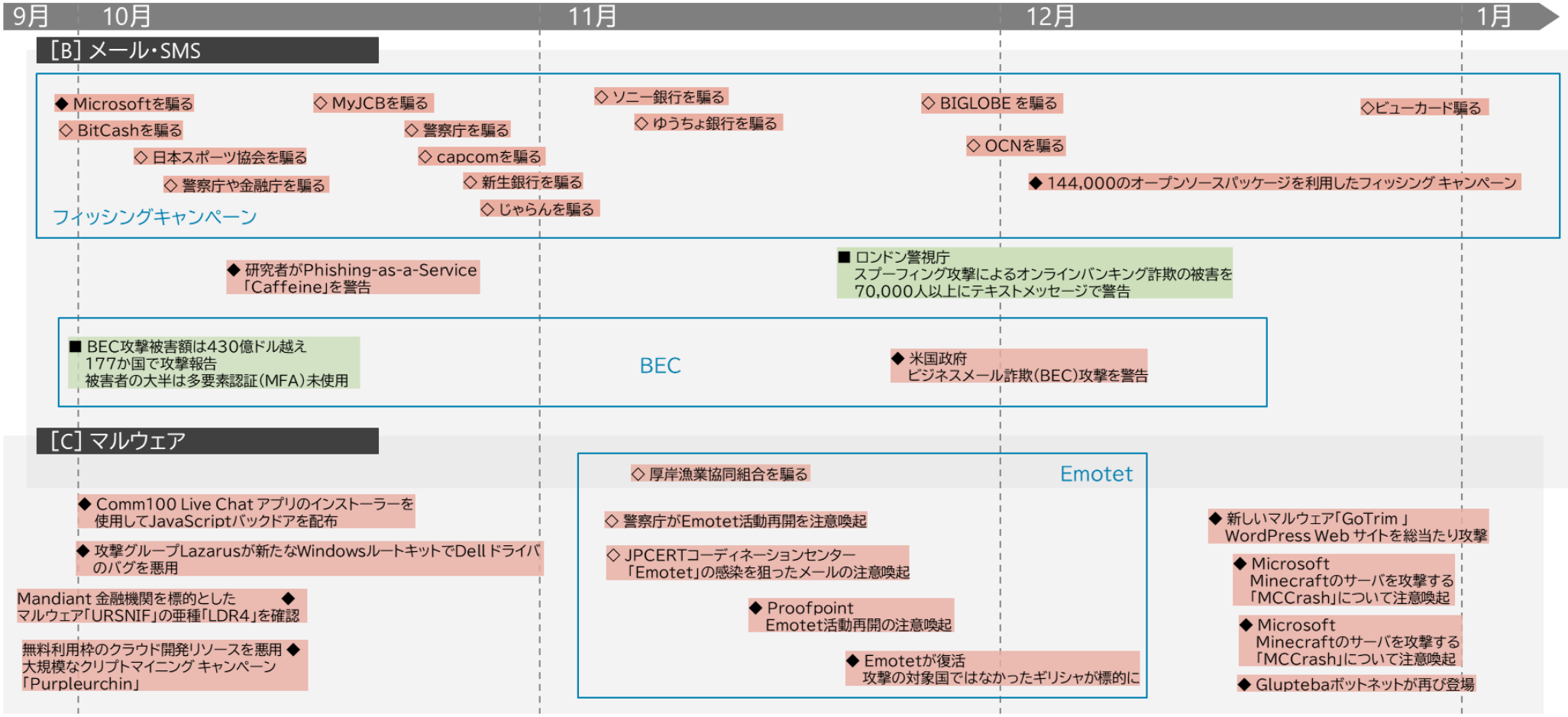


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

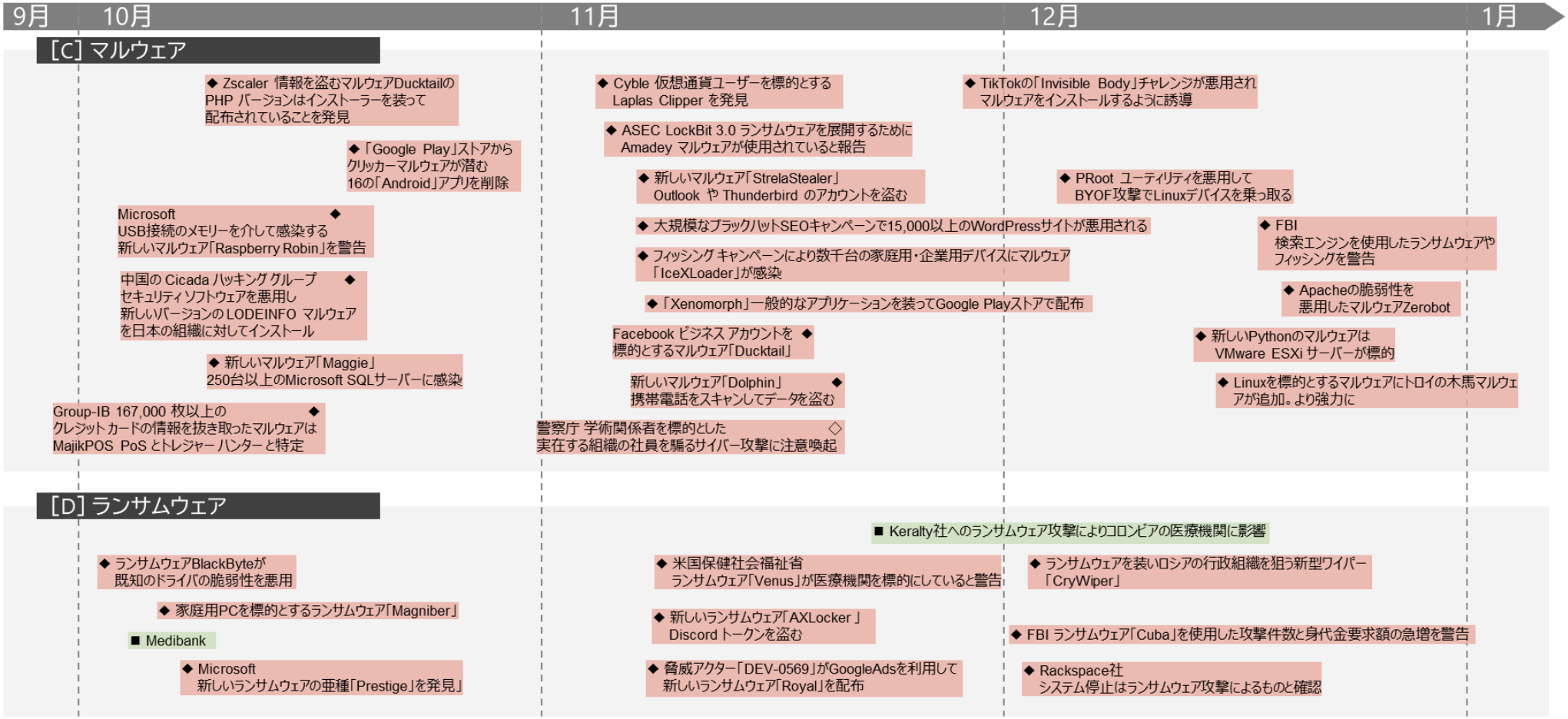


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

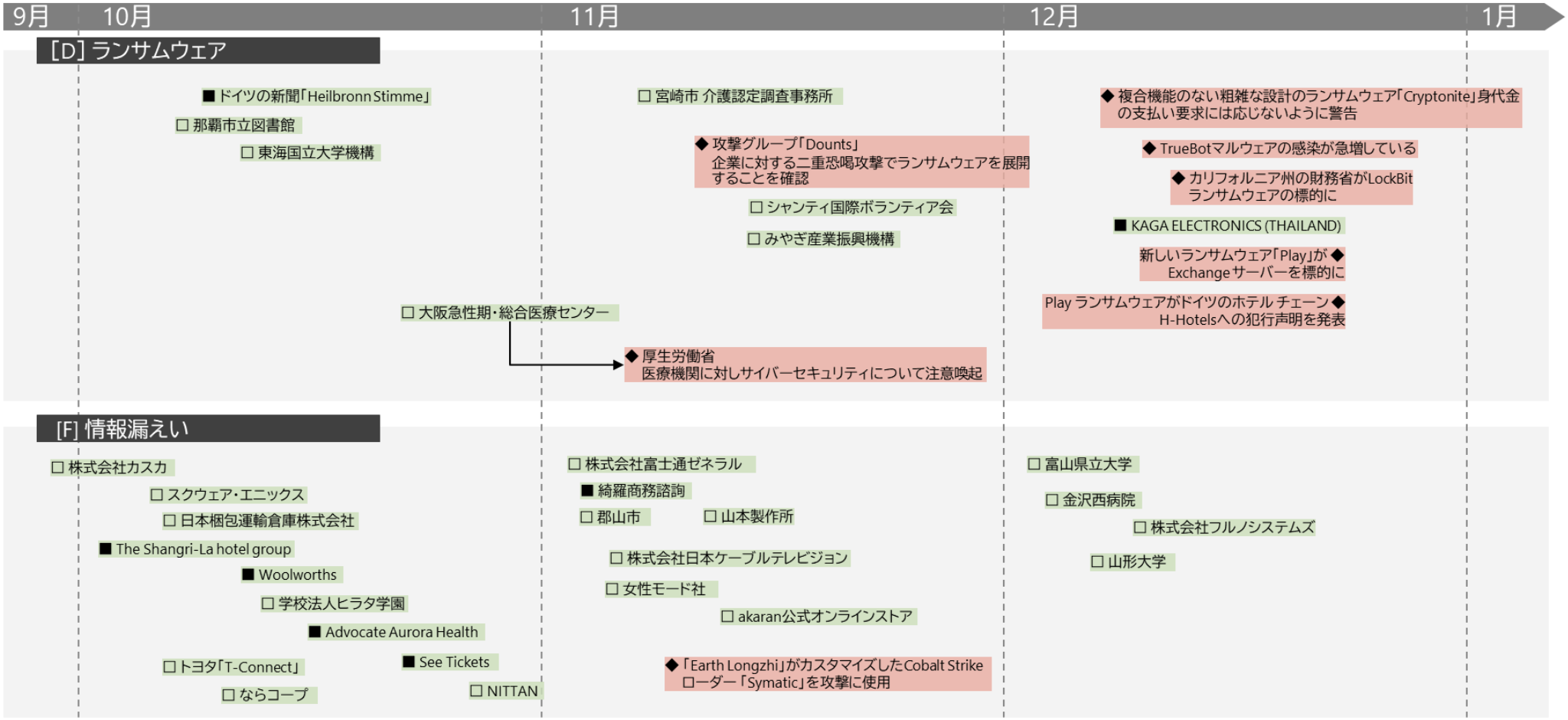


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

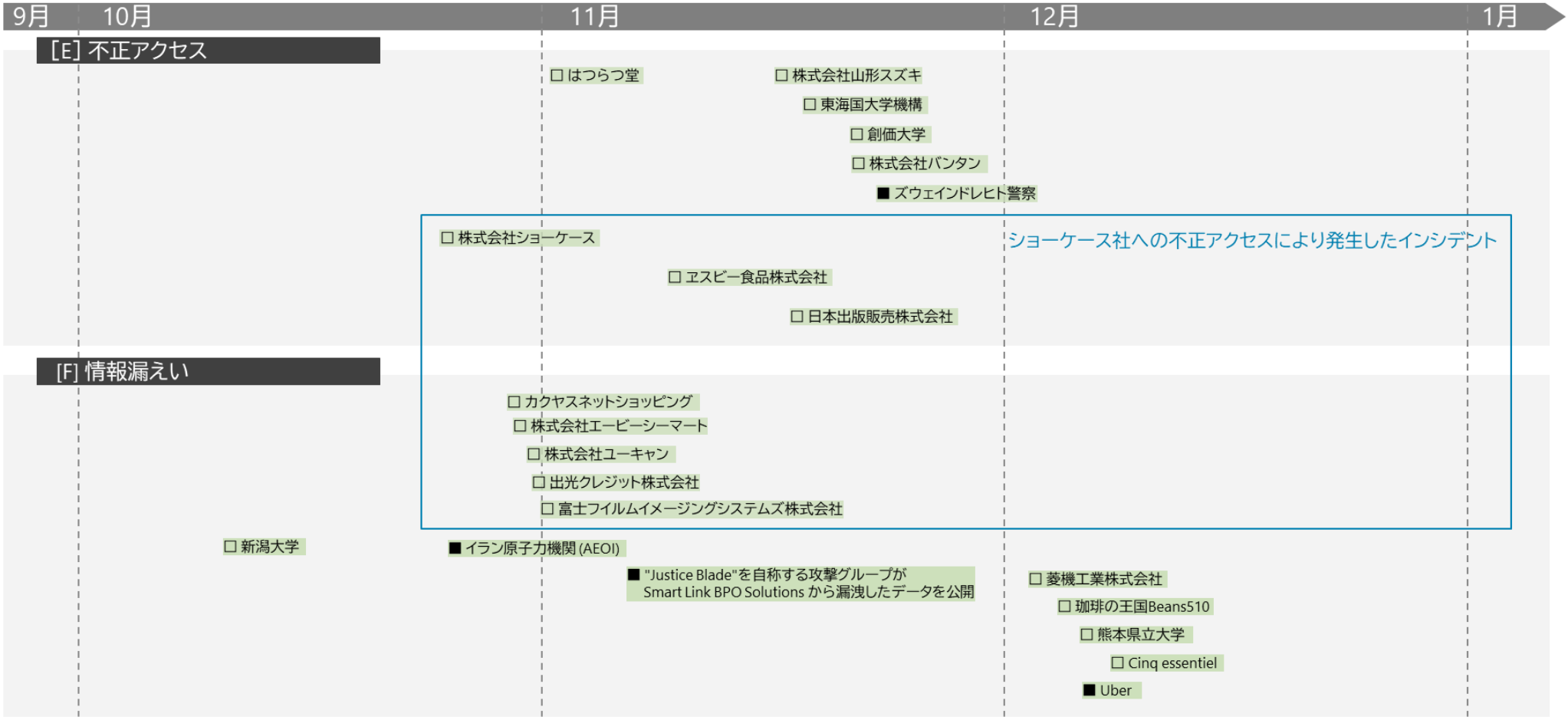


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

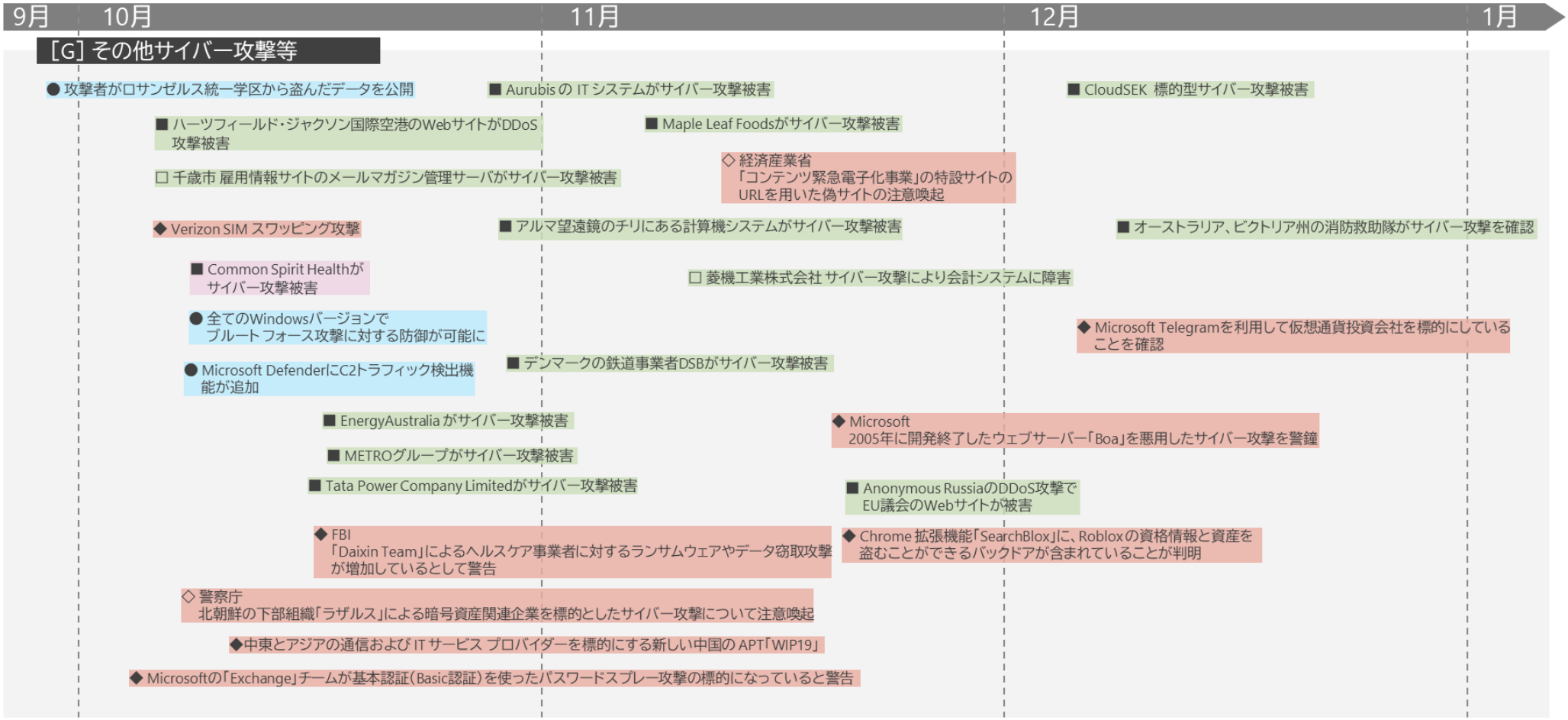


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策



参考文献

[1] デジタル庁, “「ISMAP-LIU」の運用を開始しました,” 1 11 2022. [オンライン]. Available: https://www.digital.go.jp/news/76af2f66-c63c-43ef-aa2d-90ab018d5a6c/.

[2] NISC、デジタル庁、総務省、経済産業省, “ISMAP-LIUについて,” 1 11 2023. [オンライン]. Available: https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005&sys_kb_id=96af45d0db21d110d2b773f4f3961995&spa=1.

[3] 内閣官房・総務省・経済産業省, “政府情報システムのためのセキュリティ評価制度（ISMAP）について,” 3 6 2022. [オンライン]. Available: https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005&sys_kb_id=96af45d0db21d110d2b773f4f3961995&spa=1.

[4] ISMAP 運営委員会, “ISMAP 管理基準,” 3 6 2021. [オンライン]. Available: https://www.ismap.go.jp/csm/ja?id=kb_article_view&spa=1&sys_kb_id=e2309a581b9d301013a78665cc4bcba9&sysparm_article=KB0010028.

[5] FIDO Alliance, “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://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins-jp/?lang=ja.

[6] FIDO Alliance, “FIDO Alliance - Open Authentication Standards More Secure than Passwords,” [オンライン]. Available: https://fidoalliance.org/.

[7] FIDO ALLIANCE, “FIDOの仕組み,” [オンライン]. Available: https://fidoalliance.org/fido%e3%81%ae%e4%bb%95%e7%b5%84%e3%81%bf/?lang=ja.

[8] FIDO ALLIANCE, “パスワードレス認証の普及を加速させる取り組み,” 17 3 2022. [オンライン]. Available: https://fidoalliance.org/charting-an-accelerated-path-forward-for-passwordless-authentication-adoption-jp/?lang=ja.

[9] FIDO Alliance, “さまざまなユースケースへの FIDO の対応に向けて,” 24 4 2022. [オンライン]. Available: https://media.fidoalliance.org/wp-content/uploads/2022/04/%EF%BC%88%E5%9B%BD%E9%9A%9B%E7%89%88%E3%81%AE%E6%97%A5%E6%9C%AC%E8%AA%9E%E8%A8%B3%EF%BC%89How-FIDO-Addresses-a-Full-Range-of-Use-Cases-rF2.pdf.

[10] 板倉景子, “What are Passkeys?,” 9 12 2022. [オンライン]. Available: https://media.fidoalliance.org/wp-content/uploads/2022/12/Keiko-Itakura_What-are-Passkeys-final-as-of-Dec-12.pdf.

[11] Apple Inc., “iOS 16 のアップデートについて,” [オンライン]. Available: https://support.apple.com/ja-jp/HT213407.

[12] Apple Inc., “macOS Ventura のアップデートの新機能,” [オンライン]. Available: https://support.apple.com/ja-jp/HT213268.

[13] Apple Inc., “iPadOS 16 のアップデートについて,” [オンライン]. Available: https://support.apple.com/ja-jp/HT213408.

[14] D. Zavala, C. Brand, A. Naddaf , K. Buchanan, “Android と Chrome にパスキーを導入,” 4 11 2022. [オンライン]. Available: https://developers-jp.googleblog.com/2022/11/bringing-passkeys-to-android-and-chrome.html.

[15] A. Sarraf, “Chrome がパスキーに対応しました,” 15 12 2022. [オンライン]. Available: https://developers-jp.googleblog.com/2022/12/chrome.html.

[16] Google LLC, “Android と Chrome でパスキーをサポート,” 9 2 2023. [オンライン]. Available: https://developers.google.com/identity/passkeys/supported-environments?hl=ja.

[17] AgileBits, Inc., “The passwordless experience you deserve,” [オンライン]. Available: https://www.future.1password.com/passkeys/.

[18] C. Hoff, “Passwordless Is Possible: LastPass Gets You There Sooner,” 6 6 2022. [オンライン]. Available: https://blog.lastpass.com/2022/06/passwordless-is-possible-lastpass-gets-you-there-sooner/.

[19] W. Palant, “What's in a PR statement: LastPass breach explained,” 27 12 2022. [オンライン].

[20] ヤフー株式会社, “セキュリティリスクから守るパスワードレスとは？ 生体認証によるログインのメリットと設定方法,” 6 2 2023. [オンライン]. Available: https://about.yahoo.co.jp/info/blog/20230206/passwordless.html.

[21] 株式会社NTTドコモ, “dアカウントのログインにおける新たな認証手段（Web認証・パスキー）の提供を開始,” 17 10 2022. [オンライン]. Available: https://www.docomo.ne.jp/info/news_release/2022/10/17_00.html.

[22] D. Zavala, “Bringing together sign-in solutions and passkeys with Android's new Credential Manager,” 6 2 2023. [オンライン]. Available: https://android-developers.googleblog.com/2023/02/bringing-together-sign-in-solutions-and-passkeys-android-new-credential-manager.html.

[23] 株式会社ショーケース, “不正アクセスに関するお知らせとお詫び,” 25 10 2022. [オンライン]. Available: https://www.showcase-tv.com/pressrelease/202210-fa-info/.

[24] 一. 情報サービス産業協会, “ASPサービスモデル利用規約,” 3 2005. [オンライン]. Available: https://www.jisa.or.jp/Portals/0/resource/legal/download/asp_policy_model.pdf.

[25] PCISSC, “PCI DSS Version 4.0 日本語版,” 3 2022. [オンライン]. Available: https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0-JA.pdf.

[26] 独立行政法人情報処理推進機構, “情報セキュリティサービス基準適合サービスリストの公開,” 5 6 2018. [オンライン]. Available: https://www.ipa.go.jp/security/it-service/service_list.html.

[27] 特定非営利活動法人日本ネットワークセキュリティ協会, “サイバーインシデント緊急対応企業一覧,” 2 2023. [オンライン]. Available: https://www.jnsa.org/emergency_response/.

[28] 一. 日本損害保険協会, “サイバー保険取り扱い会社,” 12 2022. [オンライン]. Available: https://www.sonpo.or.jp/cyber-hoken/ins/.

[29] Microsoft Corporation, “Microsoft Exchange Server 2019、2016、および 2013 のセキュリティ更新プログラムについて: 2022 年 11 月 8 日 (KB5019758),” 8 11 2022. [オンライン]. Available: https://support.microsoft.com/ja-jp/topic/microsoft-exchange-server-2019-2016-%E3%81%8A%E3%82%88%E3%81%B3-2013-%E3%81%AE%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E6%9B%B4%E6%96%B0%E3%83%97%E3%83%AD%E3%82%B0%E3%83%A9%E3%83%A0%E3%81%AB%E3%81%A4.

[30] GTSC VIETNAM TECHNOLOGY SERVICES AND COMMERCIAL JOINT STOCK COMPANY, “WARNING: NEW ATTACK CAMPAIGN UTILIZED A NEW 0-DAY RCE VULNERABILITY ON MICROSOFT EXCHANGE SERVER,” 28 9 2022. [オンライン]. Available: https://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html.

[31] Microsoft Corporation, “Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server,” 30 9 2022. [オンライン]. Available: https://msrc.microsoft.com/blog/2022/09/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/.

[32] P. Bazydło, “CONTROL YOUR TYPES OR GET PWNED: REMOTE CODE EXECUTION IN EXCHANGE POWERSHELL BACKEND,” 16 11 2022. [オンライン]. Available: https://www.thezdi.com/blog/2022/11/14/control-your-types-or-get-pwned-remote-code-execution-in-exchange-powershell-backend.

[33] Microsoft Corporation, “Analyzing attacks using the Exchange vulnerabilities CVE-2022-41040 and CVE-2022-41082,” 30 9 2022. [オンライン]. Available: https://www.microsoft.com/en-us/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-

2022-41082/.

[34] Fortinet, Inc., “Microsoft Exchange 0-Day Vulnerability Updates,” 30 9 2022. [オンライン]. Available: https://www.fortinet.com/blog/threat-research/microsoft-exchange-zero-day-vulnerability-updates.

[35] トレンドマイクロ株式会社, “Microsoft Exchange Serverでゼロデイ攻撃が発生,” 30 9 2022. [オンライン]. Available: https://www.trendmicro.com/ja_jp/research/22/i/ms-exchange-zero-day.html.

[36] Imperva, Inc., “Microsoft Exchange Server Vulnerabilities CVE-2022-41040 and CVE-2022-41082,” 30 9 2022. [オンライン]. Available: https://www.imperva.com/blog/microsoft-exchange-server-vulnerabilities-cve-2022-41040-and-cve-2022-41082/.

[37] Akamai Technologies, Inc., “Microsoft Exchange Server のゼロデイ脆弱性（CVE-2022-41040 および CVE-2022-41082）への Akamai の対応,” 3 10 2022. [オンライン]. Available: https://www.akamai.com/ja/blog/security-research/akamais-response-zero-day-vulnerabilities-microsoft-exchange-server.

[38] F5, Incorporated, “K54470807: Mitigating CVE-2022-41082, CVE-2022-41040 with BIG-IP ASM / Adv WAF Attack Signatures,” 3 10 2022. [オンライン]. Available: https://support.f5.com/csp/article/K54470807.

[39] O. Tsai, “A New Attack Surface on MS Exchange Part 1 - ProxyLogon!,” 6 8 2021. [オンライン]. Available: https://devco.re/blog/2021/08/06/a-new-attack-surface-on-MS-exchange-part-1-ProxyLogon/.

[40] O. Tsai, “A New Attack Surface on MS Exchange Part 2 - ProxyOracle!,” 6 8 2021. [オンライン]. Available: https://devco.re/blog/2021/08/06/a-new-attack-surface-on-MS-exchange-part-2-ProxyOracle/.

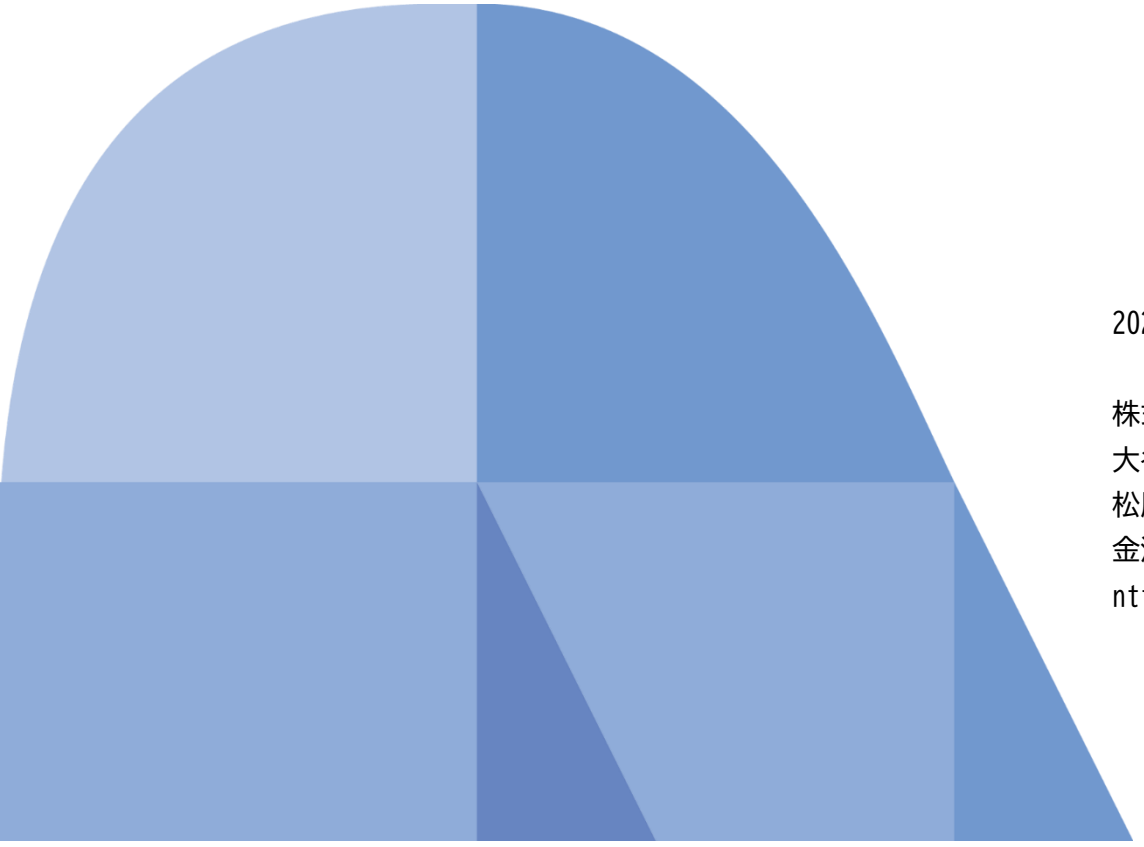
[41] O. Tsai, “A New Attack Surface on MS Exchange Part 3 - ProxyShell!,” 22 8 2021. [オンライン]. Available: https://devco.re/blog/2021/08/22/a-new-attack-surface-on-MS-exchange-part-3-ProxyShell/.

[42] O. Tsai, “A New Attack Surface on MS Exchange Part 4 - ProxyRelay!,” 19 10 2022. [オンライン]. Available: https://devco.re/blog/2022/10/19/a-new-attack-surface-on-MS-exchange-part-4-ProxyRelay/.

[43] 厚生労働省, “新型コロナウイルス感染症の感染症法上の位置づけの変更等に関する対応方針について,” 27 1 2023. [オンライン]. Available: https://www.mhlw.go.jp/content/001046577.pdf.

[44] NTTデータ, “グローバルセキュリティ動向四半期レポート 2022年度 第2四半期,” 30 3 2023. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2022_2q_securityreport.pdf?rev=3b94b7685d5840c7b2741e269cccc7d3.

[45] Security NEXT, “テレワーク環境でマルウェア感染、社内に拡大 - 三菱重工,” 11 8 2020. [オンライン]. Available: https://www.security-next.com/117404.



2023年5月19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
松尾 俊彦 / 宮井 理帆 / 塩田 明弘 / 出沢 信雄 / 田原 茂之
金澤 瑠維 / 大山 千尋 / 小笠原 弘貴
nttdata-cert@kits.nttdata.co.jp