グローバルセキュリティ動向四半期レポート

2023 年度　第 3 四半期

目次

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、グローバル動向を独自の観点で調査・分析したものです。

新様式マイナンバーカード

政府は、マイナンバーカードを刷新し、2026年中に新しい様式のカードを導入することを発表しました。券面偽造事件の発生などから、当初は券面の記載を無くしその内容をマイナンバーカードに搭載しているICチップに記録する、という検討を行っていましたが、目視や画像データによる本人確認の運用を考慮した結果、住所、氏名、生年月日、顔写真の情報を残すことになりました。

ICチップの読み取り環境の普及率が低いうちは、同様の状況が続くと考えられるため、目視確認を行う現場では対応に留意する必要があります。

多要素認証で大丈夫？　パスキーのすゝめ

パスワードレス認証『パスキー』は多要素認証の一種であり、従来の多要素認証の課題を解決して、さらにセキュリティとユーザビリティの両面を向上できるメリットがあります。

パスキーは、大手プラットフォームによるサポートが拡大するにつれ、ますます「新しい標準」となりつつあります。組織がこの変化に適応して行くことは、競争優位性を保つ上で不可欠です。そのため組織の情報システム担当者は、パスキーを積極的に評価し、その導入を検討することを推奨します。

セキュリティインシデント対応時の情報共有の重要性とその効果

近年、セキュリティインシデント対応時の情報共有の義務付けに向けた動きがさまざまな国で広まりつつありますが、日本国内では、セキュリティインシデント対応時の情報共有が必ずしも進んでいるとは言えません。

サイバー攻撃を受けた組織は、セキュリティインシデントの詳細情報の公開が自組織の風評に影響すると考え、情報公開に慎重になるケースが多くあります。『サイバー攻撃被害に係る情報の共有・公表ガイダンス』を活用して、的確な情報共有を行って自組織と社会全体の双方のメリットを最大化していくべきと考えます。

今もなお続くCitrix製品の深刻な脆弱性の悪用

Citrix製品のゼロデイ脆弱性「CVE-2023-3519」の概要、攻撃手法およびその対策、実際のインシデントレスポンス・脆弱性対応事例と得た学びを整理します。

ゼロデイ脆弱性は稀にしか発生しないイレギュラーケース、という認識がありますが、2023年度に公表された事例とその被害数は多く、かつ増加傾向にあることが分かりました。自組織をサイバー攻撃の被害から守っていくためには、ゼロデイ脆弱性を正しく理解し、必要な対応を欠かさないことが大切です。

ノーウェアランサム出現から考える、今後のランサムウェア攻撃手法

ノーウェアランサムというファイルの暗号化を行わないランサムウェアが登場しました。

データのバックアップ対策などを導入する組織の増加に伴い、従来のランサムウェア攻撃の被害は一定数に落ち着くと推測しますが、データの窃取を行うノーウェアランサム攻撃は増加すると推測します。また、復号が不要になるなどの理由で犯行組織によるテクニカルサポートが容易になることから、RaaS版ノーウェアランサムの供給が増え、それによる被害も増加すると推測します。

2. 注目トピック『新様式マイナンバーカード』

サイバーセキュリティ技術部　紀平 悠人

2.1. 新様式マイナンバーカードの変更点

2023年6月に政府は「デジタル社会の実現に向けた重点計画」を閣議決定しました [1]。その計画の一環として、2016年に交付が始まった現行のマイナンバーカードを刷新し、2026年中に新しい様式のカードを導入することを発表しました。現行のマイナンバーカードの有効期限は、発行日から10回目の誕生日までの約10年間であるため、交付開始直後からマイナンバーカードを持ち始めた人が更新を迎えるタイミングに合わせて、新様式のマイナンバーカードを導入することになります。この新様式のカードの機能向上に資する事項の検討を行うため、2023年9月に「次期個人番号カードタスクフォース」が発足しました [2]。このタスクフォースは、次期カードの変更点を決定し、2023年12月に中間とりまとめを公表しました [3]。

次期マイナンバーカードの変更点は多岐に渡りますが、利用者にとって特にうれしい変更点は、マイナンバーカードの電子証明書の有効期限を5年から10年に延長することです。現行のマイナンバーカードは、カード自体の有効期限が10年であるのに対して、電子証明書の有効期限は5年となっています。そのため利用者は発行から5年経った時点で電子証明書を更新するために市町村の窓口に出向く必要があり、利用者の負担となっていました。そこで電子証明書の有効期限をマイナンバーカードの有効期限と同じく約10年とすることで、これまで5年目に必要であった更新手続きがなくなり、利用者の負担が小さくなります。

これに伴い、暗号方式も見直します。現行のマイナンバーカードが利用しているRSA 2048bitは、電子政府推奨暗号リスト（CRYPTREC）において利用期限を2030年までに定めています [4]。電子証明書の有効期限が約10年となる次期マイナンバーカードでは、RSA 2048bitでは利用期限が過ぎてしまい、引き続き使うことができません。そのため、次期マイナンバーカードの公開鍵暗号方式には、2036年まで耐えうる強固な暗号方式として、ECDSA 256bit及びECDSA 384bitを採用する予定です。

また、他にもマイナンバーカードの券面デザインと記載事項を変更します。具体的なデザインはまだ公表されていませんが、偽造防止・ユニバーサルデザイン対応、視覚障碍者への配慮等を踏まえて、券面デザインの見直しを行う予定です。特に、文字の読みやすさに配慮するとともに、誰もが持ちたくなる魅力的なデザインを実現すると発表しています。また、現行のマイナンバーカードの券面には、住所、氏名、性別、生年月日の基本4情報と顔写真が記載されていますが、次期マイナンバーカードでは券面から性別が削除されることになりました。また、氏名のフリガナ追加や、希望者には、西暦の生年月日と氏名のローマ字が追記欄に記載される予定です。次期マイナンバーカードでは、ここに挙げたもの以外にも数多くの変更を実施する予定です。

2.2. 偽造事件の発生

次期個人番号タスクフォースが中間とりまとめを発表した時期に、マイナンバーカード関連で注目すべきもう一つのニュースがありました。それは、マイナンバーカードの偽造で初の逮捕者が出たというニュースです[5]。容疑者は、中国の指示役から送られてきた顔写真や住所などのデータを元にマイナンバーカードを

偽造し、ベトナムやインドネシアなどの国籍の男女に発送していました。偽造されたマイナンバーカードは、銀行口座の開設や携帯電話の契約の際に、対面の身元確認のための公的身分証明書として使用していたと推測します。そしてこれらの銀行口座や携帯電話は、特殊詐欺などの犯罪に使うためのものと推測します。

この偽造マイナンバーカードは、見た目を本物に近づけるため、ICチップを埋め込む工夫を施していましたが、本物のマイナンバーカードに施されているさまざまな偽造・変造対策は施しておらず、精巧な偽物とは到底言えません。ICチップに格納されている証明書を複製・偽造するのは極めて困難です。よって、ICチップも見た目だけで、何も情報は入っていません。そのため、券面のみの偽造である本件の偽マイナンバーカードでは、カード搭載のICチップを用いた認証を要するマイナポータルへのログインやe-Taxを用いた電子書類の提出などを実在する個人に成り代わって行うことはできません。このようなICチップを用いた認証は、利用者証明用電子証明書と署名用電子証明書というICチップに格納された2種類の電子証明書が用いられます。この電子証明書を用いた認証方式は現在最も広く利用されているID・パスワードによる認証とは全く異なる方式です。ICチップに格納されているこれらの証明書を複製・偽造するのは極めて困難であり、券面のみの偽造である本件の偽カードでは、これらの証明書を用いた認証を突破することはできません。

しかしマイナンバーカードは、対面での身元確認の際に運転免許証やパスポートと並んでそれ一点で顔写真付き本人確認書類として使用できるケースがほとんどです。また、マイナンバーカードの券面のコピーを書類へ貼り付けて郵送して、本人確認するという運用も存在しています。それらの場合、ICチップ内の情報を読み取らず、券面の目視のみでの本人確認に留まっています。ICチップ内の情報を用いて身元確認を行う運用であれば、簡単に偽造に気づけるのですが、券面の目視のみでの確認では、偽造判定は視覚に依存することとなり、見逃しが発生してしまうおそれがあります。もし、銀行の窓口担当者が偽造を見逃してしまった場合、不正な銀行口座が開設されてしまい、犯罪行為に利用されるおそれがあります。このような事態を防ぐためには、厳格な身元確認が重要です。そのため、今後は人間の目視だけに依存せず、ICチップ内の情報も併用した身元確認を推奨します。

2.3. 券面記載事項について

次期個人番号カードタスクフォース [3]では、盗難・紛失時の情報漏洩のおそれ等から、次期マイナンバーカードは、表面の基本4情報と顔写真、及び裏面のマイナンバーの記載を取りやめ、それらの情報はマイナンバーカードに搭載しているICチップに記録する、という検討を行っていました。しかし、現状、ICチップ内のデータを読み出す環境が全ての身元確認現場に整っていないことや、券面の目視による本人確認や券面をコピーする運用がすぐにはなくならないことを考慮した結果、券面に住所、氏名、生年月日、顔写真の情報を残すと決定しました。またマイナンバーカードの所有者が各機関にマイナンバーを提供する際に、手近にICチップ内のデータを読み出す環境がまだ整っていないため、マイナンバーカードに記載されたマイナンバーを参照すると考えて、現行と同じように裏面にマイナンバーの情報を残すと決定しました。一方で、対面で性別の目視確認が必要になる機会があまりないとの判断から、券面への性別の記載を取りやめ、ICチップでの記録にとどめることになりました。現場のマイナンバーカードの利用状況を加味して券面の記載情報を決定した結果、次期マイナンバーカードでも情報漏洩や偽造の危険性は今とほぼ変わらず残ったままとなっています。また、マイナンバーカードの券面を使った情報提供方法では、個人の属性情報のうち、名前だけや、生年月日（年齢）だけといった必要な情報だけを選択して相手に提示することが困難です。そのためマイナンバーカードを提示する側も提示される側も、不必要な情報を提示・入手してしまうというプライバシーの懸念があります。

2.4. 次々期以降のマイナンバーカードの展望

次期個人番号カードタスクフォースが公表した中間とりまとめによると、マイナンバーカードは今後も継続的に改良を重ねていく予定です。個人情報漏洩のおそれなどを考えると、マイナンバーカードの目指すべき姿は、全ての個人情報の券面の記載を取りやめて、身元確認はICチップ内のデータを利用して行うことです。しかし、次期マイナンバーカードでは、前述の理由から、券面からの性別の削除のみに留まりました。このことから、マイナンバーカードの理想形を実現するためには、身元確認を行う事業者と身元の提示を行う利用者の両者にとって、マイナンバーカードのICチップの読み取りのハードルを下げることが必要不可欠です。

事業者は、ICチップを用いた身元確認を行うためには、ICチップの読み取り装置やその内容の正当性を確認する仕組みを準備しなければなりません。また、現場に残っている券面をコピーする運用を見直してもらう必要もあります。これらは一朝一夕に行うことはできません。そこで、少しでも現状を改善していくため、国は今後スマホ等を通じてICチップから性別を含む基本4情報やマイナンバーを読み出すことができるアプリを開発、無償配布する方針です。これによりICチップを読み取り、検証するための専用の機器を導入せずとも、社用スマホなどをそのままICチップの読み取り装置として転用することが可能になるかもしれません。

また利用者向けには、ICチップを用いた身元認証の負担軽減の方法を議論しています。その一つとして、暗証番号の見直しが挙がっています。現在マイナンバーカードには、JPKI AP、住民基本台帳AP、券面事項確認AP、券面事項入力補助APの4つのAPが格納されており、それぞれ異なる暗証番号を設定することができます。JPKI APを除く3つのAPは、同一の暗証番号とすることも可能です。ただ一般的な利用者にとって、サービスがICチップの読み取りと暗証番号の入力を要求してきたときに、4つのAPのうち、利用しようとしているAPを特定して、正しい暗証番号を入力するのは困難です。また、サービスが複数のAPを利用する場合には、それぞれのAPに対応する暗証番号の入力をする必要があり、操作が煩わしいという問題もあります。これらの問題を受けて、次期マイナンバーカードでは、暗証番号を署名用の6~16桁の暗証番号とそれ以外の4桁の暗証番号の2つに統合し、かつ署名用の暗証番号の照合に成功した場合は、4桁暗証番号の照合を不要とする検討を引き続き行なっています。また、現在はAndroidスマホへのJPKI APの搭載が実現しています。今後、iPhoneへの対応やJPKI AP以外のAPもスマホ搭載を進めて、暗証番号の入力による認証ではなく、生体認証など更に利用者負荷の少ない認証方法の実現を検討していくとしています。

このように券面から個人情報の記載をなくすという理想形を実現するため、さまざまな取り組みを検討しています。しかしながら、身元確認現場でICチップの読み取り環境の普及率が100%になるのは、当分先になると予想します。どの程度普及すれば、券面から個人情報を削除してよいと判断するのか、普及のために今後どのような取り組みを行っていくのか、今後も議論をしていかなければなりません。また、たとえ普及率が十分高くなったとしても、災害時のような平時以外の状況での運用など、考慮すべき事項は多岐に渡ります。こういった課題への対策も考えていかなければなりません。現在、日本はさまざまな取り組みを通じて、デジタル社会の理想形に近づこうとしています。マイナンバーカードの券面からの個人情報の削除は、そのなかではほんの一つの側面でしかありませんが、その実現に向けて着実に進んで行くことを願っています。

3. 注目トピック『多要素認証で大丈夫？ パスキーのすゝめ』

サイバーセキュリティ技術部　程吉 英仁

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 四半期で取り上げたパスワードレス認証『パスキー』はセキュリティの向上と同時にユーザビリティも大幅に改善される多要素認証の一種であり、四半期レポートの予測どおり国内のサービスでも導入が進んでいます [5]。

このパスキーの状況や基本概念などに触れながら、導入のステップや注意事項をご紹介します。

3.1. パスキー導入のための環境は揃った

パスキーの導入と普及は、2022年後半からプラットフォーム（Apple、Google）での対応が始まりました。2023年に入ると、Microsoft Windowsでもパスキーのサポートも始まり、主要なプラットフォームでパスキーを利用できるようになりました。さらに、1PasswordやLastPass等のパスワード管理サービスもパスキーに対応し、クロスプラットフォームでパスキーを利用できるようになりました。ユーザが簡単かつ安全にログインできるように、Adobe、Amazon、Apple、CVSHealth、Dashlane、DocuSign、Google、メルカリ、NTTドコモ、任天堂などの多数のサービスが、パスキーを提供し始めています [6]。大手プラットフォームによるパスキーのサポートの拡大は、パスキーの採用と提供が、今後さらに容易になることを意味します。

これらのパスキーの進展は、企業の情報システム担当者にとって重要な意味を持ちます。企業は、パスキーのような最先端のセキュリティ技術を採用すれば、従業員の情報システムへのログインプロセスを簡素化し、かつ安全性を高めることができます。

3.2. パスキーの解説

3.2.1. パスキーの基本概念と動作原理

パスキーは、パスワードレス認証の新しい方式であり、これまでのパスワードレス認証方式よりも、セキュリティの確保とユーザビリティの向上を狙って設計されています。パスキーは公開鍵暗号技術を使用しており、公開鍵と秘密鍵の2つの鍵を用いて認証を行います。公開鍵は情報システムに登録され、機密保持すべき秘密鍵はユーザのデバイスのみに保持されます。

パスキーを使った認証プロセスでは、ユーザが情報システムへログインするときにアカウントのIDを入力すると、情報システムが認証リクエストをユーザの使用するPCやスマホなどのデバイスへ送信します。デバイスは秘密鍵を使用してこのリクエストに署名します。次に、この署名されたリクエストを情報システムに送り返し、サービスプロバイダーは公開鍵を使用して署名を検証します。署名の検証が成功すれば、ユーザがそのアカウントの正当な所有者であることが証明されるため、情報システムへのログインを許可します。

パスキーの重要な点は、秘密鍵がユーザのデバイスのみに存在して、決してユーザのデバイス外へ秘密鍵を送信しないことです。これにより、ユーザがフィッ

シング攻撃に引っかかってパスワードを漏らす恐れがなく、認証のセキュリティを大幅に強化しました。

3.2.2. 特徴1：強固なセキュリティ

パスキーによる認証は公開鍵暗号技術にもとづくこの認証方式であり、秘密鍵がユーザのデバイスのみに保持されデバイス外へ送信することがないため、秘密鍵の漏洩リスクが極めて低いです。認証プロセスでは、秘密鍵を使用してリクエストに署名し、その署名がサービスプロバイダーによって検証されます。このプロセスは、不正アクセスやデータ侵害のリスクを大幅に減少させるため、企業やユーザにとって強固なセキュリティを提供します。

3.2.3. 特徴2：ユーザビリティの向上

パスキーは、ユーザビリティの大幅な向上を実現します。従来のパスワードや複雑な多要素認証プロセスに代わり、パスキーではユーザはデバイスの生体認証やPINを使用して簡単に認証を完了できます。このシンプルで直感的なアプローチは、ログインプロセスを迅速化し、ユーザビリティを向上させることに貢献します。

多要素認証は、認証の防御力が向上する代わりに、認証時のユーザビリティが低下します。例えば、SMSで認証コードを受信する方式や物理トークンを使う方式は、ユーザへ認証プロセスの追加の手間をもたらします。このように多要素認証には、ユーザビリティとセキュリティのトレードオフが存在します。

多要素認証とは対照的に、パスキーは認証プロセスの追加の手間や物理トークンなどの追加のセキュリティ対応を必要としません。情報システムへアクセスするときにユーザのデバイスを用いて生体認証するだけで認証を完了できるため、ユーザビリティが大幅に向上します。このように、パスキーは多要素認証のユーザビリティを大幅に改善する新しい認証方式です。

3.2.4. 特徴3：フィッシング攻撃への耐性

パスキーによる認証は、特に認証情報の盗難やフィッシングといった認証情報を盗んで悪用する攻撃方法に対して強力な耐性を持っています。

パスキーが近年のセキュリティ環境に適している理由は、その根本的なセキュリティ構造にあります。

まず、パスワードの代わりにデバイスの生体認証を使用することで、攻撃者が利用できる攻撃ベクトルが大幅に削減されます。つぎに、この認証方式では、ユーザがサービスプロバイダーに自身の秘密鍵情報を提供することはなく、認証プロセスが完全にデバイス内で完結するため、攻撃者がフィッシングサイトを通じて認証情報を盗み出すことが困難になります。パスキーはユーザのデバイスに安全に秘密鍵を保持し、公開鍵を通じて認証を行うため、攻撃者がユーザの認証情報を盗み出すことが非常に困難になります。加えて、パスキーの認証プロセスは、正当なサービスプロバイダーからのリクエストのみを認証するため、偽の認証リクエストを効果的に排除します。

このようにパスキーは、近年のフィッシング攻撃などの認証情報を狙ったセキュリティ脅威に対抗するための強力なツールであり、企業がセキュリティとユーザビリティのバランスを効果的に実現するための鍵となります。

3.2.5. パスキーと多要素認証の比較

パスキーと多要素認証の間には、いくつかの重要な違いがあります。

多要素認証は、パスワードなどの知識情報、デバイスなどの所持情報、指紋などの生体情報から、複数の認証要素を組み合わせて認証することによって、セキュリティを強化します。パスワードのみの認証は攻撃者が突破する認証の壁は1

つだけですが、多要素認証は不正アクセスに対して複数の障壁を提供します。多要素認証は、認証の防御力が向上する代わりに、図 3-1の課題①に示すように、ユーザへ複数回の認証の手間をもたらすため、ユーザビリティが低下します。つまり、ユーザビリティとセキュリティのトレードオフが存在します。また、多要素認証には図 3-1の 課題② 及び 課題③に示す脆弱性も存在します。例えば、攻撃者は、この脆弱性を狙ってフィッシングやパスワードスプレー等によりID及びパスワード等の情報を窃取できる恐れがあります。攻撃者は窃取したIDとパスワードを使って、SIMを攻撃者のSIMに移転することにより、認証を突破することが可能です。

多要素認証とは対照的に、パスキーは認証プロセスの追加や物理トークンなどの追加デバイスを必要とせず、情報システムへアクセスするときにユーザのデバイスを用いて生体認証するだけで認証を完了できます。そのため、図 3-1の 解決策①に示すように1回の操作で認証することができ、ユーザビリティが大幅に向上します。さらに、パスキーは、図 3-1の 解決策② 及び 解決策③に示すように、パスワードなどの認証情報を使用せずに認証結果を送信して認証し、かつ十分な強度の公開鍵暗号技術を使用しているため、フィッシング攻撃やパスワードリスト攻撃に対して耐性があります。

このように、パスキーは多要素認証方式よりも安全で、ユーザビリティを大幅に改善する新しい認証方式です。

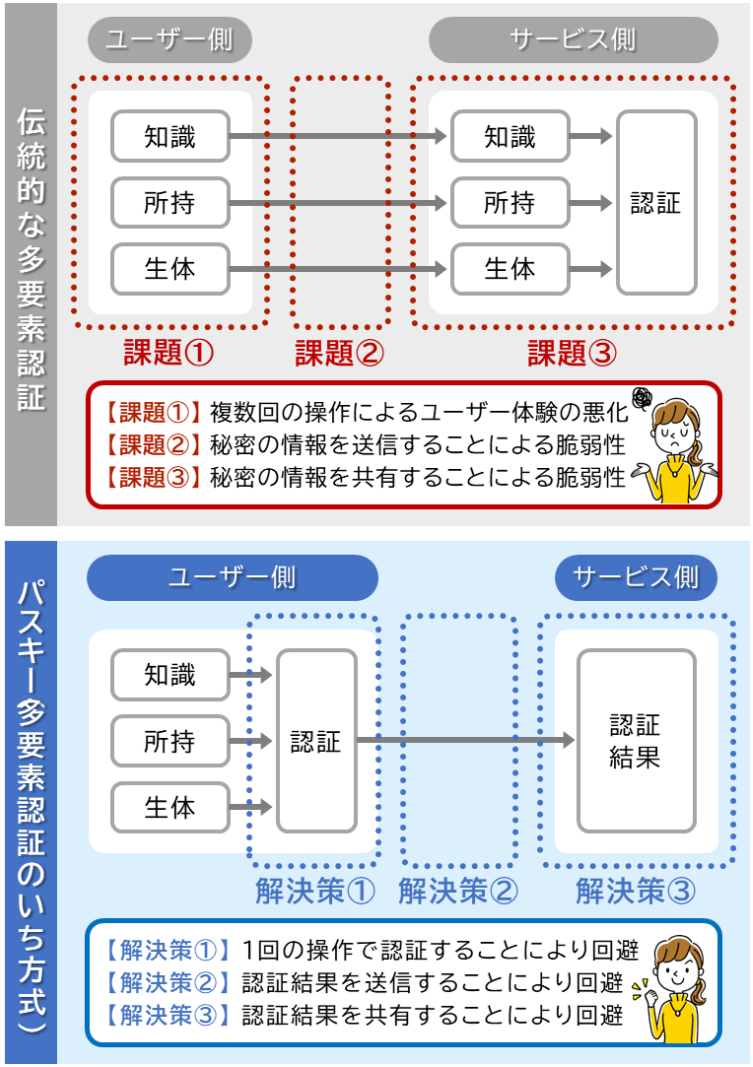


図 3-1：多要素認証とパスキーの比較

3.3. パスキーの導入と運用に向けて

3.3.1. 導入のステップ

オンラインサービス、モバイルアプリケーション、クラウドベースのサービスなどの新しいシステムは、FIDO認証に対応していることが多く、パスキーの導入は容易です。パスキーは、ユーザのデバイスを使用して認証する仕組みであるため、OA環境、リモートワーク環境など、個人の認証が必要な情報システムへの導入に向いています。

一方で、認証時に個人を識別しない情報システム、共用PCなど複数人で1つのアカウントを使用する情報システムには導入できません。また、認証リクエストをユーザのデバイスから情報システムへ送信するための工夫が必要となるため、インターネットに接続しない情報システムへの導入も向いていません。

そのため、情報システムへ導入する場合は、まず現在の認証システムとパスキーの互換性を評価して、パスキーをサポートするために必要なシステムのアップデートや変更を特定します。次に、適切なパスキー製品のベンダーと設計と導入に必要な技術を選択し、ニーズに合ったパスキーの実装プランを策定します。また導入ステップには、技術的な事項だけでなく、従業員への教育とトレーニングも必要となります。従業員がパスキーの概念と利用方法を理解して、安全にパスキーを使えるようにするためにガイダンスを提供することも必要です。最後に、パスキーの運用をサポートするためのポリシーと手順を確立し、適切なセキュリティ監視とレポーティングメカニズムを導入します。

3.3.2. 導入時と運用時の考慮事項

パスキーを導入し運用する際には、複数の考慮事項があります。

3.3.2.1. 互換性

ユーザが使用するPCやスマホなどのデバイスを社内で統一していない場合は、ユーザは自分好みのPCやスマホ、オペレーティングシステムを使用します。そのため、情報システム担当者はそれら全てのデバイスとオペレーティングシステムとの互換性を考慮し、さまざまなデバイスとオペレーティングシステムを幅広くサポートできる知識と体制を確保しなければなりません。

便益とコストとを比較検討し、必要によってはユーザが使用するPCやスマホなどのデバイスの種類を限定する対策等を行う必要があります。

3.3.2.2. サポート

パスキーによる認証はユーザのデバイスに認証に必要な情報を保存しているため、従来のパスワードベースの認証と比較して、ユーザのデバイスが故障したり、紛失したり、新しいデバイスに移行したりする場合、認証の復旧プロセスが複雑になる可能性があります。そのため、復旧プロセスを詳細に検討する必要があります。

3.3.2.3. 規則等

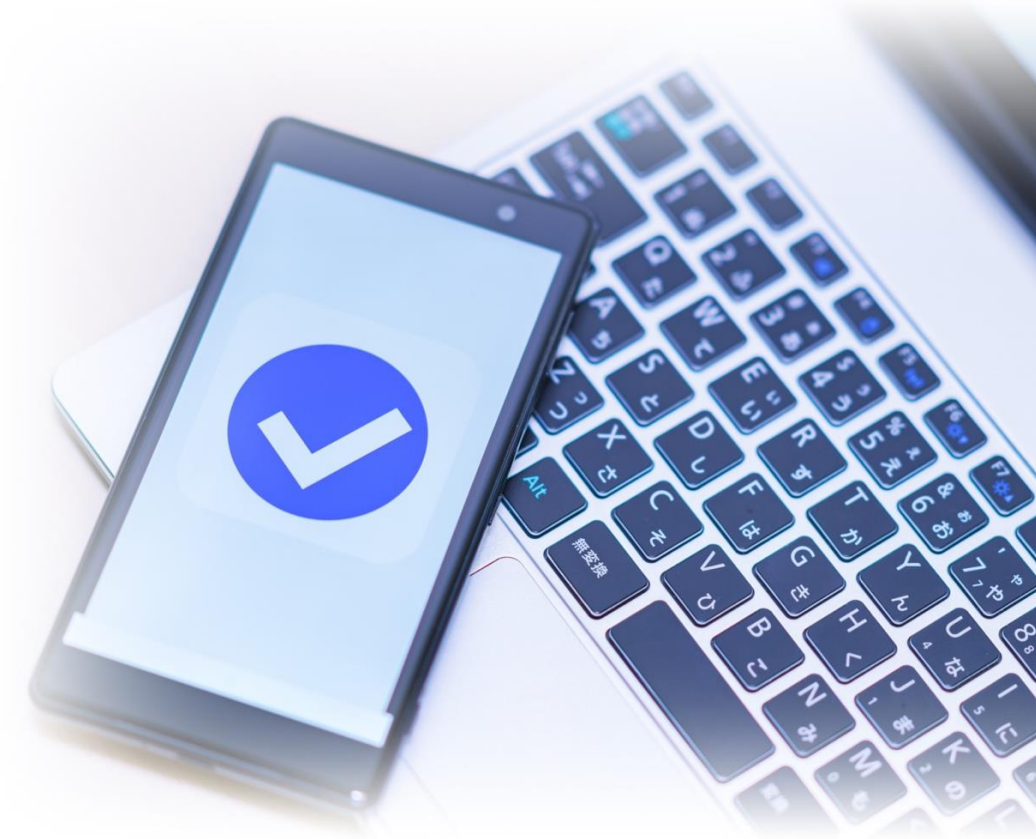
パスキーを使った情報システム（に限った話ではありませんが）はユーザのデバイスも含め、ユーザデータの安全性及びプライバシーに係る法令、セキュリティポリシー、プライバシー要件、及び業界のベストプラクティス等を守っていることが求められます。ユーザデータの安全性とプライバシーを最優先事項として扱い、法令等を守っていることを確認する必要があります。

3.4. まとめ

パスキーは、近年のセキュリティ環境において重要な役割を果たす新しい認証方式です。パスキーの利用は、多要素認証の課題を解決して、さらにセキュリティとユーザビリティの両面を向上できるメリットがあります。

加えて、近年、攻撃者が取引先企業やグループ会社へ侵入して、その組織のユーザになりすまして標的の企業を攻撃するインシデントが発生しており、注目が集まっています。このようなサプライチェーンセキュリティのリスクに、顧客や親会社は、サプライチェーン先の組織のユーザ認証のセキュリティ対策の強化を求めています。このような背景を踏まえると、企業が自社の情報システムへパスキーを導入することは、単に最新の認証方式を採用すること以上の意味があります。パスキーの導入は、顧客の信頼を獲得し、業界内で競争力を保つための戦略的な決断です。これまでにパスキーを導入した企業では、パスキーを採用することのメリットを実感しています。

またパスキーは大手プラットフォームによるサポートが拡大するにつれ、ますます「新しい標準」となりつつあります。企業がこの変化に適応して行くことは、競争優位性を保つ上で不可欠です。そのため情報システム担当者は、パスキーを積極的に評価し、その導入を検討することを推奨します。



4. 情報漏えい『セキュリティインシデント対応時の情報共有の重要性とその効果』

サイバーセキュリティ技術部　田杉 怜子・武田　晃

2023年8月4日に内閣サイバーセキュリティセンター(以下、NISCと記述)と気象庁、および気象研究所の3組織は、メール関連機器に対する不正通信により、個人情報を含むメールデータの一部が外部に漏えいしたおそれがあると公表しました。本稿では、上記の事後対応を紹介し、インシデント報告の要否の見解を述べます。

4.1. セキュリティインシデントに関する情報共有の各国における動き

近年、セキュリティインシデント対応時の情報共有の義務付けに向けた動きがさまざまな国で広まりつつあります。

米国では、米国証券取引委員会（SEC）が2023年12月からサイバーセキュリティ開示規則を米国市場の一部上場企業へ適用しました [7]。これはサイバーセキュリティ開示規則では、一部上場企業がセキュリティインシデントを発見して被害が重大であると判断してから4日以内に、財務状況や株価に影響を与える重要事項についての報告書式「Form 8-K」での報告を求めています。

一方、欧州では、現在、欧州サイバーレジリエンス法 [8]を検討しています。この法律は、デジタル要素を持つ製品に対して、さまざまなセキュリティ対策を課す法律です。製造元の企業や開発者へ、脆弱性の悪用の発見時やセキュリティインシデント発生時に、24時間以内の報告を求めています。

日本国内では、2022年4月より改正個人情報保護法によって、個人データの漏えい等が発生して個人の権利利益を害するおそれがある場合には、個人情報保護委員会への報告を義務付けました [9]。一方で、それ以外のセキュリティインシデント発生時の報告義務等は存在しないものの、総務省の「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項[緊急提言]」 [10]にて、セキュリティインシデントに関する速やかな情報共有を求めています。

セキュリティインシデント対応時の情報共有を薦める理由は、複数あります。1つ目の理由は、SECのサイバーセキュリティ開示規則が求めている、投資家に向けたインシデントに関する被害状況の透明性の確保です。2つ目の理由は、欧州サイバーレジリエンス法や総務省の提言が求めている、被害者の保護、および公共の利益です。しかし、日本国内では、セキュリティインシデント対応時の情報共有が必ずしも進んでいるとは言えません。ここでは、NISCと気象庁、および気象研究所のメールデータ漏えいインシデントの事後対応を考察します。

4.2. 3組織のメールデータ漏えいインシデント

（1） NISC のセキュリティインシデントの概要

2023年6月13日、NISCの電子メール関連のシステム・機器から不正通信の痕跡が見つかりました。NISCは状況を調査するため、速やかに影響を受けたシステム

の運用を停止しました。その後、電子メール関連機器の交換を実施し、他の機器にも異常がないことを確認したあとに、当該システムを再稼働しました。その後、外部のセキュリティ専門機関による調査の結果から、NISCが2022年10月上旬から2023年6月中旬までの間にNISC外から届いた個人情報を含むメールデータの一部が、外部に漏えいしたおそれがあることが判明しました [11]。

（2） 気象庁と気象研究所のセキュリティインシデントの概要

気象庁と気象研究所は、それぞれが使用していたメール関連機器へ、ゼロデイ脆弱性を狙った不正通信があったことを発表しました。気象庁と気象研究所は、脆弱性を狙った不正通信を受けた全ての機器をセキュリティ対策を強化した機器へ交換しました。その他にも、いくつかのセキュリティ対策を実施しました。また調査の結果から、2022年6月上旬から2023年5月下旬までに気象庁と気象研究所を含む、全国の気象官署へ届いたメールのうち、一部のデータが外部に流出したおそれが判明しました [12] 。

4.3. インシデント情報共有の要否の考察

4.3.1. 情報共有とセキュリティ保安

両事例とも、あるメール関連機器の脆弱性が原因のセキュリティインシデントであると発表しています [11] [12]。しかしNISCと気象庁および気象研究所は、サイバー攻撃を受けたメール関連機器の機種名や悪用された脆弱性など、セキュリティインシデントの詳細情報を公表していません。NISCは、詳細情報を非開示にした理由が、セキュリティ保安上のためと答えています [13]。

サイバー攻撃被害に係る情報の共有・公表ガイダンス [14]に、ゼロデイ脆弱性情報の取り扱いや、公表によって二次被害を引き起こす懸念がある場合の脆弱性情報の取り扱いの記載があります。同ガイダンスは、基本的に脆弱性情報等の脅威情報は速やかに共有することが望ましいと記載しています。ただし例外的に、広くソフトウェア製品一般にありうる設定不備に関する情報等は、模倣犯等を惹起するおそれがあり、広く共有することは望ましくないと記載しています。

今回の両事例は、いずれも「メーカーにおいてこれまで確認できていなかったシステムの脆弱性を狙った不正通信があった」としています [11] [12]。この文面からは両事例が「広くソフトウェア製品一般にありうる設定不備を狙ったサイバー攻撃」ではなく「ゼロデイ脆弱性による特定製品を狙ったサイバー攻撃」であると考えられます。そのため、３組織の取った情報非開示の方針は、サイバー攻撃被害に係る情報の共有・公表ガイダンス [14]に反するものであり不適切と言えます。

4.3.2. なぜ情報共有が必要なのか

そもそも、なぜセキュリティインシデントの情報共有が必要なのでしょうか。攻撃者はセキュリティ対策を回避するために、より複雑で高度なサイバー攻撃手法を編み出しています。自組織だけでは、このような攻撃者やサイバー攻撃を迅速に把握、理解することは難しく、すぐには対抗できません。複数の組織で攻撃者やサイバー攻撃、インシデントの情報を共有すれば、自組織だけでは見つけられなかった攻撃者やサイバー攻撃の情報を獲得できます。これらの情報は、同様のサイバー攻撃を受けたときに、その原因や被害範囲の特定、被害拡大防止、適切な再発防止策に役立ちます。

以下にインシデント情報を共有して、効果的にインシデント対応する方法、活動の例を紹介します。

1つ目の例は、すべてのセキュリティインシデント被害組織の利益の最大化をめざした方法です。サイバー攻撃手法が高度化する昨今、特に自組織内にセキュリティの専門部署を持たないような組織が単独でセキュリティインシデントを全容解明することがより困難になってきています。セキュリティインシデントの全

容が解明できなかった場合、被害範囲の見積もりや事後対応、再発防止策など、適切なインシデント対応をおこなえません。このようなとき、同様のインシデント被害にあった複数の組織がそれぞれの持つセキュリティインシデントの詳細情報を公開することにより、すべての被害組織が、その詳細情報を使ってセキュリティインシデントの全容解明により近づくことができます。その結果、すべての被害組織が、適切なインシデント対応をおこなえます。

2つ目は、業界内の組織が参加してセキュリティインシデントの情報共有や連携を行うISAC（Information Sharing and Analysis Center）活動の例です。ISACは、もともとは米国で大統領令にもとづいて設立された非営利団体です。ISACは組織が業界別に集まって、セキュリティ関連の情報を共有、分析して活用します。日本国内には、既に金融ISACや交通ISAC、電力ISACなどがあります。ISAC内の組織は、加盟組織で発生したインシデント情報を共有して、自組織で同様のインシデントが起きないように未然防止のセキュリティ対策を整えたり、インシデントが起きたときの対応に役立てたりできます。

4.3.3. なぜ情報共有しない組織があるのか

JPCERT/CCは、3組織がインシデントの情報を公表しない件について、下記のコメントを発表しています。

「（前略）悪用された脆弱性等について言及がなされていない点について指摘する声がありますが、JPCERT/CCとしては、どのような分野の被害組織であれ、被害公表だけでなく、情報共有や専門機関との連携含め、『サイバー攻撃被害に係る情報の共有・公表ガイダンス」で示されている対応がなされることで、被害組織のインシデント対応に適切な評価が得られるようになるだけでなく、他の被害組織を含め、あらゆる関係者にとって必要な情報の非対称性が解消され、国全体として攻撃活動への対処がなされるものと考えています。」 [15]

しかし、情報共有活動のメリットに反して、情報を公開しない組織も存在しているのが実情です。現状では、サイバー攻撃を受けた組織は、セキュリティインシデントの詳細情報の公開が自組織の風評に影響すると考え、情報公開に慎重になるケースが多くあります。また、セキュリティインシデントの被害に関する情報のうち、どの情報をどのタイミングでどのような範囲へ共有することが適切なのか、判断することが難しいと思います。そのことも、円滑かつ効果的な情報共有が進まない一因となっていると思います。

4.3.4. セキュリティインシデント情報共有の実例

4.3.3にて述べたセキュリティインシデント情報の公開タイミングと公開範囲は、JPCERT/CCのコメントで言及している「サイバー攻撃被害に係る情報の共有・公表ガイダンス」 [14] が詳述しています。たとえば、以下の2つの情報共有の方針を紹介します。

1. インシデント発覚後は可能な限り早期に技術面に関する情報、その中でも特にインディケータ情報（不正な通信のIPアドレス、マルウェアのハッシュ値等）を、非公開な場で関係機関にのみ共有する
2. インシデント発覚後一定の調査が進んだ後（典型的には調査終了後等）に、インシデントがあったという事実、被害内容、事後対応等について公開の場で発表する

上記１の「非公開な場で関係機関にのみ共有する」という方針は、前述のISACの活動方法と一致します。マスコミやSNSなどによる風評を心配せずに、自組織の情報を非公開な場で関係機関へ公開できます。

ISACに限らず、非公開な場でセキュリティインシデントの情報共有を行っている事例があります。たとえば、日本シーサート協議会 インシデント事例分析ワーキンググループも、多様な業界のセキュリティインシデント対応の実務者が集

まって、定期的にセキュリティインシデント対応の成功や失敗の事例を共有しています。同WGが使っているチャタムハウスルールも、風評被害を防いで情報共有する手段の一つです。チャタムハウスルールとは、会議に参加した人は誰でも、会議の情報を自組織へ持ち帰って自由に使用できる。ただし、情報源の組織や人を特定できる情報は持ち帰らないというルールです。これら以外にも、草の根では、さまざま組織が集まって非公開な場でインシデントの情報の情報共有を行っていいます。

　また弊社では、弊社が公開しているAndroidアプリ「MyPallete」で脆弱性が発覚した際に、下記のように早期の脆弱性情報の届出や公開などの脆弱性ハンドリングを実施して、セキュリティインシデントの被害防止に寄与しています。まず上記の1のとおりに、早期にIPAの脆弱性届出窓口とMyPalleteを利用してアプリを開発している関係各社のみへ、直ちに脆弱性の情報と脆弱性を修正したソースコードの共有を行いました。関係各社のアプリの修正完了後、上記の2のように、JPCERT/CCと連携して当社から脆弱性に関する事実を公表して、脆弱性を修正したバージョンへのアップデートの呼びかけを行いました。

4.4. まとめ

　各組織は、主体的にかつ継続的にセキュリティインシデントの情報を共有できるようになれば、社会全体でセキュリティインシデントに適切に対応できるようになります。組織は、セキュリティインシデント発生時に『サイバー攻撃被害に係る情報の共有・公表ガイダンス』を活用して、的確な情報共有を行って自組織と社会全体の双方のメリットを最大化していくべきでしょう。

5. 脆弱性『今もなお続くCitrix製品の深刻な脆弱性の悪用』

サイバーセキュリティ技術部　田島 臣啓

サイバー攻撃の手法は数多くありますが、そのトレンドは時代と共に変遷しています。1980年代のインターネットの爆発的な普及時には、ファイアウォールが存在せず、攻撃者がインターネットから組織内のネットワークへ侵入することは容易でした。1990年代にはファイアウォールが誕生し、インターネットから組織内のネットワークへの侵入は困難になり、標的型攻撃といったユーザの操作ミスを狙ったサイバー攻撃が広がっていきました。そして、2010年頃になるとゼロデイ脆弱性を狙ったサイバー攻撃が増加し、今はそれが主流となっています。

最近世の中を騒がせ、今もなお続いているCitrix製品の脆弱性「CVE-2023-3519」は、ゼロデイ脆弱性を狙ったサイバー攻撃です。2023年10月には、本脆弱性を悪用して、リモートから任意のコードを実行してユーザ資格情報を取得するサイバー攻撃キャンペーンが世界各国で発生しました。NTTデータグループでも、本脆弱性を狙ったサイバー攻撃を受けましたが、適切なインシデントレスポンスにより被害は生じませんでした。しかし、NTTDATA-CERTでは本脆弱性対応に大いに苦労させられました。このレポートでは、Citrix製品の脆弱性「CVE-2023-3519」の概要、本脆弱性を狙ったサイバー攻撃手法およびその対策、そして実際のインシデントレスポンス・脆弱性対応事例と得た学びを整理します。

5.1. 脆弱性CVE-2023-3519とは

NetScaler ADC（旧Citrix ADC）および NetScaler Gateway（旧Citrix Gateway）は、ネットワーク構築時に使用するアプライアンス製品で、オンラインアプリケーションのパフォーマンス・強度・セキュリティを向上させます。同製品は世界中に広く普及しており、この脆弱性は多くの企業へ影響しました。ここでは、Citrix製品の脆弱性「CVE-2023-3519」の概要と攻撃手法、および対策を解説します。

5.1.1. 概要

Citrix製品の脆弱性「CVE-2023-3519」は、2023年7月18日に公開されました。この脆弱性は、表 5-1のバージョンのNetScaler ADCおよびNetScaler Gatewayにリモートから任意のコードを実行できる脆弱性で、そのCVSS深刻度スコアは9.8です。

表 5-1：CVE-2023-3519の影響があるCitrix製品一覧 [16]

No.	製品名	影響があるバージョン
1	NetScaler ADC および NetScaler Gateway 13.1	13.1-49.13 より前のバージョン
2	NetScaler ADC および NetScaler Gateway 13.0	13.0-91.13 より前のバージョン
3	NetScaler ADC および NetScaler Gateway 12.1	EOL
4	NetScaler ADC 13.1-FIPS	13.1-37.159 より前のバージョン
5	NetScaler ADC 12.1-FIPS	12.1-55.297 より前のバージョン
6	NetScaler ADC 12.1-NDcPP	12.1-55.297 より前のバージョン

本脆弱性を悪用すると、認証なしで第三者から遠隔で任意コードを実行されるおそれがあります。実際に一定数の企業で本脆弱性を悪用したサイバー攻撃が確認されており、被害が拡大するおそれがあるため、Citrix社は脆弱性情報とパッチを公表しました。

5.1.2. 攻撃手法

アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁(CISA)は、実際に攻撃者がこのゼロデイ脆弱性を悪用して、重要インフラ組織のNetScalerアプライアンスを攻撃して不正アクセスに成功した、と報告しています [17]。CISAが公表した攻撃フローは、以下の通りです [18]。

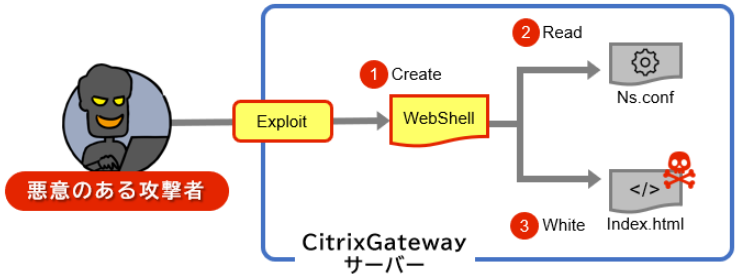


図 5-1:攻撃フロー①～③(事前準備フェーズ)

攻撃者は、CVE-2023-3519を悪用して攻撃対象のCitrix機器にPHP Webシェルをドロップします(①)。具体的には、Citrix機器のメモリ破損の脆弱性を悪用して、Citrix機器に単純なPHP Webシェルを書き込みます。攻撃者はPHP Webシェルの対話型アクセスを使用して、デバイス上のNs.confファイルの内容を取得します(②)。攻撃者は/flash/nsconfig/keys/updated/* および /nsconfig/ns.conf にある構成ファイルの中から暗号化されたパスワードを見つけます。このパスワードはNetScaler ADCに保存されている暗号鍵で復号可能なものです。これらのキーを使用して、Active Directory資格情報が構成ファイルから復号されます。

そして、攻撃者はユーザ認証時にフォームへ入力したユーザ名/パスワード含むデータを収集して、攻撃者に送信するJavaScriptを用意します。PHP Webシェルを使って、Citrix機器へJavaScriptを保存し、「index.html」へこのJavaScriptを参照するコードを追加します(③)。

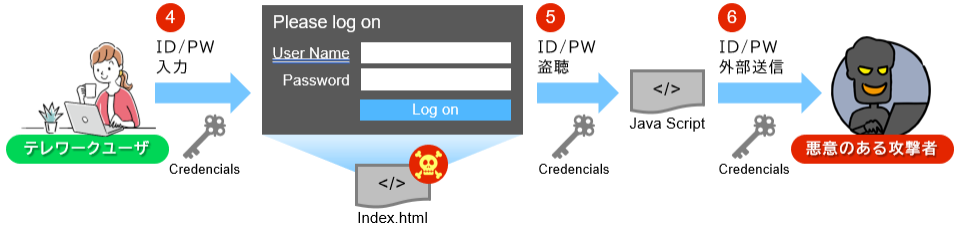


図 5-2:攻撃フロー④～⑥(情報窃取フェーズ)

ユーザがログイン時にユーザ名/パスワードを入力(④)するとJavaScriptが起動して、その情報を窃取(⑤)して攻撃者へ送信します(⑥)。

5.1.3. 対策

この脆弱性の対策は、脆弱性が修正済みのNetScaler ADCおよびNetScaler Gatewayの更新バージョンをできるだけ早くインストールすることです。また、CISAが推奨する恒久的な対策は、NetScalerを含む社内システムへ多要素認証を導入すること、そして堅牢なネットワークセグメンテーションを構成し、NetScalerアプライアンスやその他インターネットに接続する機器へ侵入した攻撃者の横広がりを阻止することです [17] 。

5.2. NTT DATAの対応と学び

NTT DATAにおけるCitrix脆弱性「CVE-2023-3519」の対応を紹介します。

5.2.1. 脆弱性対応の概要

（１） NTTDATA-CERT の脆弱性対応方針

NTTDATA-CERTでは、日頃から脆弱性情報を収集、その重大度を判定して、それに応じた対応を行っています。表 5-2に示すように、特に重大度の高い脆弱性の場合は、組織やプロジェクトへその保有システムと関係する脆弱性情報を提供して、対応を指示します。重大度に応じて、周知範囲や是正作業、報告期限などの対応内容が異なります。

表 5-2：NTTDATA-CERTの脆弱性の重大度別の対応方針

重大度	対応方針
0	対応無し（各プロジェクトで独自に判断して対応）
0+	• 社内セキュリティBlogへ注意喚起を掲載 • 全社ポータルで注意喚起を周知
1	• 上記の重大度0+の対応 • インベントリ情報DBで、脆弱性の影響がある組織およびシステムを特定 • 該当組織へ注意喚起の文書を送付して、脆弱性対策を依頼
2	• 上記の重大度0+の対応 • 社内の全組織へ脆弱性の影響有無の調査と回答を依頼 • 該当組織へ脆弱性の是正を指示 • チケット管理システムで、全組織の調査結果と対策状況を管理

CVE-2023-3519の脆弱性の重大度は１でした。そのため、表 5-2に則り、NTTDATA-CERTでは、以下の脆弱性の対応手順を実施しました。

(ア) 脆弱性の重大度１と判断
(イ) 脆弱性の影響があるシステムを特定
(ウ) 対象システムを保有する組織やプロジェクトへ、以下の対応を実施
　① 脆弱性情報を提供
　② 対象システムの脆弱性の影響有無の調査を依頼
　③ パッチ適用とその完了報告を指示
(エ) 対象システムの進捗状況を管理
　① 脆弱性の影響有無の調査報告の催促
　② パッチ適用完了の報告の催促
(オ) 脆弱性の問い合わせ対応

（２） CVE-2023-3519 の脆弱性対応の時系列

NTTDATA-CERTが実施したCVE-2023-3519の脆弱性対応を時系列で解説します。NTTDATA-CERTは、日本時間の2023年7月19日のこの脆弱性の公開後、すぐにCVE-2023-3519の情報を入手しました(①)。そして、脆弱性に関係するシステムを保有しているNTTデータ本社3社とグループ会社の組織やプロジェクトへ、上記の脆弱性対応を指示し(②)、3日後の2023年7月22日には、ほとんどのシステムでパッチ適用が終わり、脆弱性対応が完了していました(③)。

しかし、今回のCitrix脆弱性は特殊な事例で、脆弱性情報の公開後しばらくしてから本脆弱性がゼロデイ脆弱性であることが判明しました(④)。図 5-3に示すように、このCitrix製品の脆弱性はその公表の1ヵ月前から脆弱性を悪用したサイバー攻撃とその被害が発生していました(⓪)。NTTDATA-CERTがゼロデイ脆弱性であることを知ったのは、ほとんどの脆弱性対応が完了したあとでした。

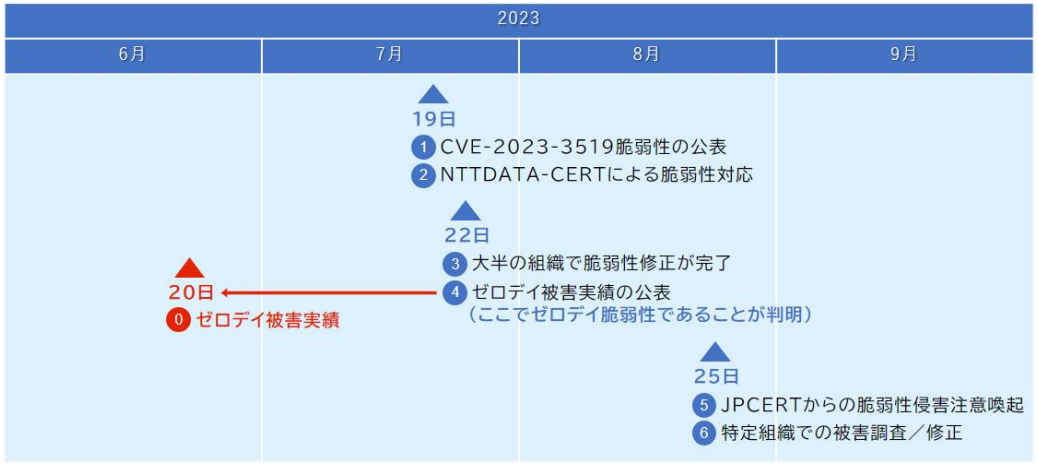


図 5-3：Citrix機器の脆弱性対応の時系列

ゼロデイ脆弱性とは、脆弱性の修正パッチ提供よりも前に脆弱性を悪用したサイバー攻撃が発生しているものを指します。脆弱性情報が公表され、それを知った時にはすでにサイバー攻撃が成功して、対象システムが侵害されているケースがあります。その場合、修正パッチを適用するだけでは、すでに対象システム内に侵入している攻撃者やマルウェアを排除できません。ゼロデイ脆弱性の脆弱性対応では、すでにサイバー攻撃を受けてシステムが侵害されている前提で、侵害調査とパッチ適用を実施することが基本の手順です。

また、ゼロデイ脆弱性とゼロデイ脆弱性以外では、上記のNTTDATA-CERTから対象システムを保有する組織やプロジェクトへの対応指示(②)の内容が異なり、ゼロデイ脆弱性の場合は、早急な侵害調査も指示して、侵害が見つかった場合は、すぐにインシデント対応を開始しなければなりません。

CVE-2023-3519では、脆弱性情報の公開タイミングではゼロデイ脆弱性の情報がなかったため、対象システムの侵害調査の指示が遅れました。その結果、侵害の発見と必要なインシデント対応の開始が遅れてしまいました。

5.2.2. CVE-2023-3519のインシデント対応

とあるシステムは、上記のNTTDATA-CERTからの対応指示(図 5-3 ②)でパッチ適用は迅速に行われたものの、その後に攻撃者に侵害されていることが見つかりました。以下に、本インシデント対応を時系列に沿って説明します。

<8月25日>

Ⓐ NetScaler Gatewayサーバが侵害されているおそれがあることを発見。
Ⓑ 該当組織からNTTDATA-CERTへインシデント報告。
Ⓒ Citrix社へ侵害の調査方法を問い合わせて、侵害有無の調査に着手。
  ⓐ 侵害調査ツールにより、侵害の痕跡を示すファイルを検知。
  ⓑ 社内のセキュリティ技術者がNetScaler Gatewayサーバを調査し、攻撃者が設置したPHP Webシェルのファイル「xxxxx.php」を発見(図 5-1参照)
  ⓒ Citrix社へ検知したファイルの解析を依頼し、攻撃の侵害を示すファイルである旨の回答を受領
Ⓓシステム責任者や管理者との調整を通じ、NetScaler Gatewayサーバのネットワーク遮断を実施。
Ⓔ NetScaler Gatewayサーバから攻撃者が横広がりしたおそれのあるDMZ

上のサーバのログを取得し、侵害調査を実施。加えて、以下の被害シナリオに沿って、なりすまし/データ窃取/漏洩形跡の調査を実施。

(a) Citrix Gatewayサーバを踏み台に隣接サーバや内部のAセグメントやBセグメントへの侵入拡大をはかるケース

(b) リモートアクセスにより正規VPNユーザとして内部セグメント侵入拡大をはかるケース

<8月26日>

Ⓕ NetScaler Gatewayサーバのリストアおよびバージョンアップを実施

Ⓖ システムを復旧、業務再開

上記のⒺの調査で、NetScaler Gatewayサーバと同じセグメントであるDMZ内の隣接サーバは、ログイン認証やアクセス制限などのセキュリティ対策を強化していたため、攻撃者の侵害が無いことを確認しました。

また、攻撃者はNetScaler Gatewayサーバを踏み台にして内部セグメントへ侵入を試みたものの、図 5-4に示すように、当該システムはDMZセグメントから内部セグメントの間にファイアウォールを設置してアクセス制限をしていたことにより、内部セグメントへ通信ができず、内部セグメント上のサーバやPCを攻撃することができなかったことを確認しました。

このインシデントでは、Citrix製品の脆弱性を悪用してNetScaler Gatewayサーバが侵害されましたが、DMZのセグメンテーションと隣接サーバのセキュリティ対策強化により、攻撃者はNetScaler Gatewayサーバから別のサーバやセグメントへ侵害を拡大できず、幸いにも被害はNetScaler Gatewayサーバ1台の侵害のみで済みました。

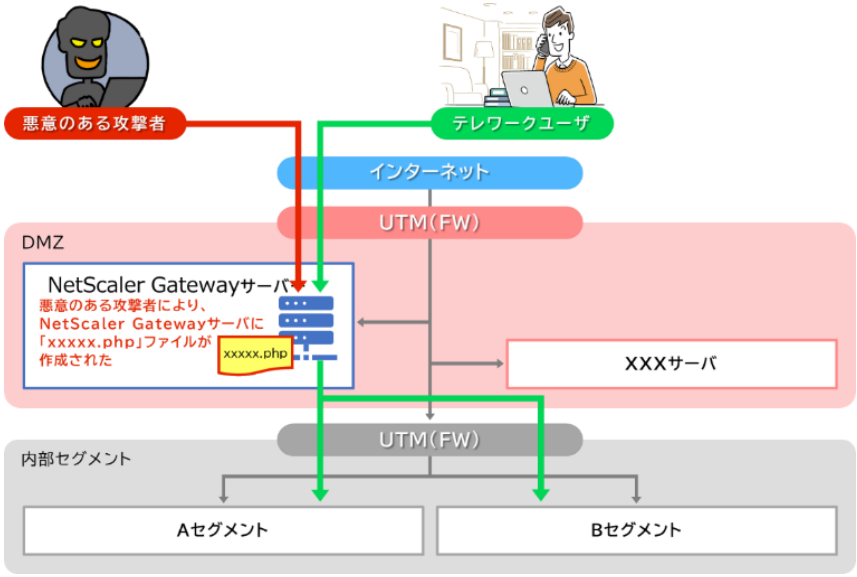


図 5-4：インシデントが発生したとあるシステムの構成

5.2.3. 脆弱性対応における大切なこと

ここでは、同インシデント事例と脆弱性対応から得た知見を整理します。

図 5-3に示すように、この脆弱性は最初の脆弱性情報の公表から3日が経過してからゼロデイ脆弱性であることが公表されました。脆弱性対応がすでに完了している場合、多くの組織は脆弱性対応を最初からやり直すことを敬遠するでしょう。しかし、事後であってもゼロデイ脆弱性であることが分かった時点で、可能な限り迅速に侵害調査を実施しなければなりません。

そして、脆弱性対応全般に言えることとして、脆弱性対応はプロジェクトの人員不足、それから生じる繁忙により延期されるケースが多々あります。CSIRTなどの情報セキュリティ運営組織とシステムを保有する組織やプロジェクトは、日

頃から脆弱性対応の発生に備えた体制の構築、および脆弱性対応フローの準備が重要です。どんな状況でも脆弱性対応へ臨機応変に対応するためには、十分な体制の構築は欠かせません。

また、システムの構築後に、アップデートをしていない製品が多く存在していることも大きな問題の一つです。パッチ適用やバージョンアップを行っていない製品で緊急の脆弱性対応が発生し、パッチを適用しようとするとさまざまな問題が発生します。たとえば、パッチ適用の手順が無くシステム管理者がパッチの入手方法や作業方法がわからない。脆弱性を修正するパッチを適用する前に、過去の全てのパッチやバージョンアップを実施しなければならない場合もあります。どんな製品でも、脆弱性対応が発生します。そのため、平常時の定期的なアップデートが重要です。その頻度は、最低でも年に一回から四半期に一回の実施が望ましいです。

5.3. まとめ

さまざまなサイバー攻撃の手法がありますが、その中でも大きな被害が発生するものがゼロデイ脆弱性を狙ったサイバー攻撃です。National Cyber Security Centre (NCSC)によると、近年のセキュリティ対策の進歩によってフィッシング攻撃を用いたシステム侵害が難しくなっていること、そしてゼロデイ脆弱性を見つけることの難易度がそれほど高くないことを背景に、攻撃者がネットワーク製品のゼロデイ脆弱性を攻撃してシステムを侵害する攻撃手法へ戦術を変更し始めているようです [19]。最近は、攻撃者がインターネットに接続している全てのネットワーク機器のゼロデイ脆弱性を常時探索して、攻撃の機会を狙っています。

本章では、Citrix製品のゼロデイ脆弱性「CVE-2023-3519」の脆弱性対応とそのインシデント対応を紹介しました。このレポートの読者の皆様の中にも、ゼロデイ脆弱性は稀にしか発生しないイレギュラーケース、という認識を持っている方が多いのではないでしょうか。私もその一人でした。しかし、改めて2023年度を振り返ると、公表されたゼロデイ脆弱性の数とその被害がとても多く、かつ増加傾向にあることが分かりました。自組織をサイバー攻撃の被害から守っていくためには、ゼロデイ脆弱性はイレギュラーケースではないと考えを改めなければなりません。自社を守っていくためには、ゼロデイ脆弱性を正しく理解し、必要な対応を欠かさないことが大切です。

6. マルウェア・ランサムウェア『ノーウェアランサム出現から考える、今後のランサムウェア攻撃手法』

サイバーセキュリティ技術部　嶌谷 直紀

ランサムウェアによる攻撃は、依然として世界的な脅威となっていますが、「ランサムウェア攻撃＝暗号化」という考え方は見直した方が良いかもしれません。なぜならノーウェアランサムというファイルの暗号化を行わないランサムウェアが登場したためです。本節では、ノーウェアランサムとは何なのか、なぜ出現したのかを考察し、ノーウェアランサムを使った攻撃のセキュリティ対策や今後のランサムウェア攻撃手法を解説します。

6.1. ノーウェアランサムとは

ノーウェアランサムという言葉自体は、2023年9月に警察庁が公表した「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」にて言及されており [20]、海外では「Encryption-less Ransomware」と呼ばれています。

ノーウェアランサムとランサムウェアの違いは、ファイルの暗号化を行うか否かの差です。ランサムウェアは、感染したコンピュータ内のファイルを暗号化します。ランサムウェア攻撃を仕掛けた攻撃者は、暗号化したファイルの復号の対価として身代金を要求します。加えて、ランサムウェアは、感染したコンピュータ内からファイルを窃取します。その窃取したファイルを公開しないことを条件として提示して、身代金を要求する場合もあります。それに対して、ノーウェアランサムを使った攻撃では、暗号化を行わず、窃取したファイルを公開しないことを条件として提示して、身代金を要求します。つまり、ランサムウェアから暗号化というアクションを除いて、ファイル公開をネタに脅迫して身代金の要求を行う攻撃手法です。まったく新しい攻撃が出現したのではなく、ランサムウェア攻撃の変化形です。

6.2. ランサムウェア攻撃の歴史

既存のランサムウェアとノーウェアランサムの違いはすぐ理解できますが、ノーウェアランサムが出現した理由を理解するには、ランサムウェアを用いた犯罪の歴史を理解しなければなりません。本項ではランサムウェアの変化の歴史を簡単に振り返ります。

6.2.1. 黎明期

いまから30年以上前に、ファイルを暗号化して身代金を要求するマルウェアは存在していました。有名なのが「AIDS Trojan」です。PC Cyborg Trojanとも呼ばれます。1989年に出現して、感染したコンピュータのファイル名を暗号化して、その復号を条件として身代金を要求しました。ファイルのデータ自体の暗号化を行わない点や、フロッピーディスク経由で感染する点など、現在のランサムウェアとはずいぶん異なる点がありますが、重要なファイルを暗号化して、身代金を要求するコンセプトは、現在のランサムウェア攻撃の原点です。

ではなぜ、現在ほど流行しなかったのでしょうか。さまざまな要因があると思いますが、攻撃者が身元を隠して身代金を入手する方法を簡単に用意できなかった点が大きいと考えます。銀行送金の場合は、警察が送り主と送り先を特定することが可能であり、サイバー犯罪者にとっては身元が特定されやすい状況でした。

6.2.2. 成長期

2010年代に入り、Bitcoinなどの仮想通貨が登場したことで状況が変わりました。仮想通貨では、取引に使うアドレスは当人の氏名などの個人情報に紐づいていません。そのため、特定のアドレスの取引履歴を追跡することは可能ですが、仮想通貨のシステムはアドレスの所有者の個人情報を持っていないため、そのアドレスの所有者を特定できません。仮想通貨の登場により、犯罪者は身元を特定されずに身代金を入手する方法を手に入れました。

仮想通貨で身代金の振り込みを求めるランサムウェアとしては、2013年に登場した「CryptoLocker」が有名です。CryptoLockerが猛威を振るったこの時期から、さまざまなランサムウェアが登場しています。

また、ランサムウェアによる攻撃をWebサービスとして提供するRaaS（Ransomware as a Service）も出現しました。ランサムウェアを用いた攻撃を行うために必要なランサムウェアやインフラ、ツールを有料で提供するサービスです。攻撃者は、ランサムウェアや攻撃用のインフラを開発したり維持運用したりする技術力や資金がなくても、ターゲットへランサムウェア攻撃を行うことが可能です。また、ランサムウェア開発者は、ランサムウェア攻撃を行わなくても、RaaSの利用料として他の攻撃者から金銭を取得することが可能になりました。このようにランサムウェア攻撃のエコシステムが構築されて、ランサムウェア攻撃が活発化しました。

6.2.3. 攻撃方法の多様化

ランサムウェアが猛威を振るう中、攻撃を受けるおそれのある企業もセキュリティ対策を進めていきます。代表的なセキュリティ対策は、データのバックアップです。仮にランサムウェアにコンピュータ内のデータが暗号化された場合でも、事前にデータのバックアップを取得しておけば、データの復旧が可能です。

サイバー犯罪者も、攻撃手法を変えています。「MAZE」というランサムウェアからは、ファイルの暗号化に加えて、窃取した情報を公開して、2重で脅迫して身代金を要求するようになりました。仮にデータのバックアップを取得していたとしても、データの公開をネタに身代金を要求できます。

このように、ランサムウェア開発者は、さまざまな手段を使って、ランサムウェアの機能や攻撃方法を変化させてきました。

6.3. ノーウェアランサムの出現理由の考察

ランサムウェア変化の歴史を踏まえ、なぜノーウェアランサムが出現するに至ったのか、その理由を考察します。主にランサムウェア開発者の観点で考察を行います。

6.3.1. データ暗号化への攻撃対策

2023年現在、世界的にランサムウェア攻撃の身代金の支払率は減少傾向です[21]。

理由の1つ目は、ランサムウェア攻撃を受けてデータの暗号化が行われても、データをバックアップしていれば、データを復旧できるためです。そのため、データのバックアップを行っている企業が多くなっています[20]。

理由の2つ目は、Webサイト「No More Ransom」[22]のように、公的機関やセキュリティベンダーが、Web上でランサムウェアが暗号化したファイルを復号できるツールを公開しているためです。FBI等の公的機関がランサムウェアのインフラを捜査して復号キーを取得して、公開する事例も多くあります[23]。この復

号ツールや復号キーを使えば、攻撃者へ身代金を支払って復号キーを受け取らなくても、データの復号が行えます。

このようにランサムウェア攻撃の被害に遭ってデータの暗号化が行われても、データを復旧できるため、被害組織が身代金を支払わないケースが増えていると推測しています。ノーウェアランサムの場合、データの復旧有無に関係なく、脅迫して身代金を要求できます。攻撃者は、データの窃取だけを行うノーウェアランサムで金銭を要求する方が、金銭獲得の手段として効率が良いと判断したと思います。

6.3.2. 開発と維持運用が楽で、利益化までが早い

ノーウェアランサムは暗号化を行わないため、ランサムウェアに実装している暗号化機能をノーウェアランサムでは実装する必要がありません。暗号化機能はランサムウェアの主要機能です。ランサムウェア本体の暗号化機能を開発しないということは、暗号化機能と関係するインフラの開発工数も減って、開発要員などの開発コストを削減できます。加えて、その分、ランサムウェアの開発開始から攻撃を開始して身代金やRaaSの利用料の受け取りまでの開発期間も短縮できます。開発期間を短縮できれば、ターゲット企業が新しい脆弱性のセキュリティ対策を行う前に、その脆弱性を悪用したランサムウェア攻撃を仕掛けることが可能です。また、暗号化と復号に用いる鍵の管理を考える必要も無くなるため、インフラの運用を楽にすることができます。

6.3.3. 復号のテクニカルサポート疲れ

被害組織が身代金を払ったあとに復旧に成功しないと、そのランサムウェア攻撃/攻撃グループの評判が落ちて、他の被害者が、そのランサムウェア攻撃/攻撃グループに身代金を払わなくなります。そのため、攻撃グループは、被害組織の復号のトラブルをサポートする場合もありました。

またRaaSも、攻撃者へ購入後のテクニカルサポートを提供している場合があります。技術的スキルが低い攻撃者でも、RaaSを契約してテクニカルサポートを利用すれば、ランサムウェア攻撃を行うことが可能になります。技術的スキルが低い攻撃者にとって、テクニカルサポートは大きなメリットです。

攻撃者やRaaS提供者は、暗号化や復号が正常に行えない問題に対処しなければならず、サポートの負担が想定より高いケースが出てきてしまいました [24]。このようなテクニカルサポートが、攻撃者やRaaS提供者の大きな負担になったと推測します。ノーウェアランサムであれば、暗号化や復号ができないという状況にならないため、暗号化と復号に関係するテクニカルサポートを無くすことができます。

6.4. 今後のランサムウェア攻撃の推測

上記を踏まえ、今後のランサムウェア攻撃手法の変化を考察します。

1つ目は、ノーウェアランサムがより流行すると思います。データのバックアップを行っている企業が多いことから [20]、今後は、データの暗号化を行う従来のランサムウェア攻撃の被害は一定数に落ち着くと推測します。しかしランサムウェア攻撃の脅威は今後も続き、データの暗号化を行うランサムウェア攻撃の代わりにノーウェアランサムが増加すると推測します。

2つ目は、ノーウェアランサムのRaaSが増えると推測します。ノーウェアランサムのRaaSの場合、暗号化機能を搭載する必要が無く、鍵管理も不要で、テクニカルサポートも従来のRaaSより楽になると思います。そのため、高度な技術を持つ組織でなくともRaaSを開発して提供できるため、RaaSの供給が増えて、RaaSを使った攻撃も増えると推測します。

6.5. 今後のランサムウェア対策方針

ノーウェアランサムを使った攻撃は、暗号化部分を除けば、データの暗号化を行うランサムウェア攻撃と同様の攻撃手法です。したがって、組織は、従来のランサムウェアのセキュリティ対策で未然防止や復旧ができます。ノーウェアランサム攻撃を未然防止できずに、ノーウェアランサムの感染や内部への侵入を許してしまった場合、社内から機密データを持ち出させない対策が、ノーウェアランサムに対抗する有効な対策です。たとえば、攻撃者のサーバやRaaSへのファイルやデータの送信を許可しない仕組みや機密データの暗号化が対策案です。

ただし、ランサムウェア攻撃を受けたときに身代金を支払って対応する方針の組織は、今後対応を変えていく必要があります。2023年のSophos社の調査によると、サイバー保険に加入していない組織がデータを復元したケースと比べて、ランサムウェア被害の特約を含むサイバー保険に加入している組織が身代金を支払ってデータを復元するケースは、4倍も多いのです [25]。このことから、サイバー保険を使用して身代金を支払っている企業が多いことがわかります。米国財務省の外国資産管理局（OFAC）の規制や [26]、米国政府も身代金の支払の規制を検討していることもあり [27]、今後身代金を支払うことが困難になっていきます。サイバー保険を使用して身代金を支払うこと自体が出来なくなる確率が高いと思っています。

日本では、サイバー保険が身代金支払いを補償対象にしていないため [28]、諸外国とは状況が異なります。日本の組織は、保険金の補償で身代金を支払う方法をあてにしていないため、身代金支払の規制が強まると、身代金を支払って復旧するのではなく、今以上にマルウェア、ランサムウェア対策への投資を増やしていくと推測します。

7. 予測

選挙とディープフェイク

2024年は、世界情勢に大きな影響を与える国や地域での選挙が立て続けにある「選挙イヤー」です。1月の台湾総統選に始まり、3月にロシア大統領選、6月にEUヨーロッパ議会選、そして最後に11月にアメリカ大統領選があります。また、日本でも、2024年に解散総選挙が行われる可能性を否定できません。そして、これらの選挙期間に、生成AIで生成した偽の音声・画像・動画などのディープフェイクコンテンツを拡散して、選挙妨害が発生するおそれがあります。実際、2023年9月のスロバキアの総選挙では、ある立候補者が投票の買収を暴露した偽の音声データがSNSに投稿されました。投稿から数時間以内にこの音声は削除されたものの、既に拡散されてしまった後であり、この投稿は投票結果に影響を与えたと言われています。ここ最近は、生成AIを使用して、誰でもより簡単により精密に他人になりすましたディープフェイクコンテンツを作成できるようになってきています。立候補者になりすましたネガティブな内容のディープフェイクコンテンツが選挙期間にSNSなどで大量に拡散されると、投票結果に大きな影響を与えるでしょう。また、大量のディープフェイクコンテンツが出回れば、有権者はそのディープフェイクコンテンツと本物のコンテンツを見分けることができません。有権者は、立候補者のすべてのコンテンツに疑念を持ってしまいます。
2021年度第2四半期レポートの予測記事で書いたように、ディープフェイクを見破るAI技術の開発も進んでいます。将来的にディープフェイクを見破るツールがディープフェイク技術へ追いついて来るでしょう。しかし、そのようなツールができたとしても、すべての有権者がそのツールを使えるとは限りません。選挙妨害のディープフェイクコンテンツを対策できなければ、インターネット選挙公報活動は、今後を衰退してしまうかもしれません。

ビットコイン価格の上昇とクリプトジャッキングの増加

クリプトジャッキングとは、他人のコンピュータを不正に使用して暗号通貨をマイニングする行為です。マイニングには高性能なコンピュータリソースが必要なため、犯罪者は他人のコンピュータにマイニングマルウェアを感染させて、コンピュータリソースを不正利用してマイニングします。マイニングマルウェアに感染したコンピュータでは、処理速度の低下や消費電力量の増加などが発生します。

2024年3月11日にビットコインの価格が72,500ドルを突破し、市場最高値を更新しました。暗号通貨の価格が上昇すると、マイニングの収益性も上がるため、犯罪者によるクリプトジャッキングも増加します。2023年には、ビットコイン価格の上昇と呼応するように、世界中でクリプトジャッキングが増加しました。2024年もビットコイン価格が上昇していることから、引き続きクリプトジャッキングとその被害が増加すると予測します。

8. タイムライン

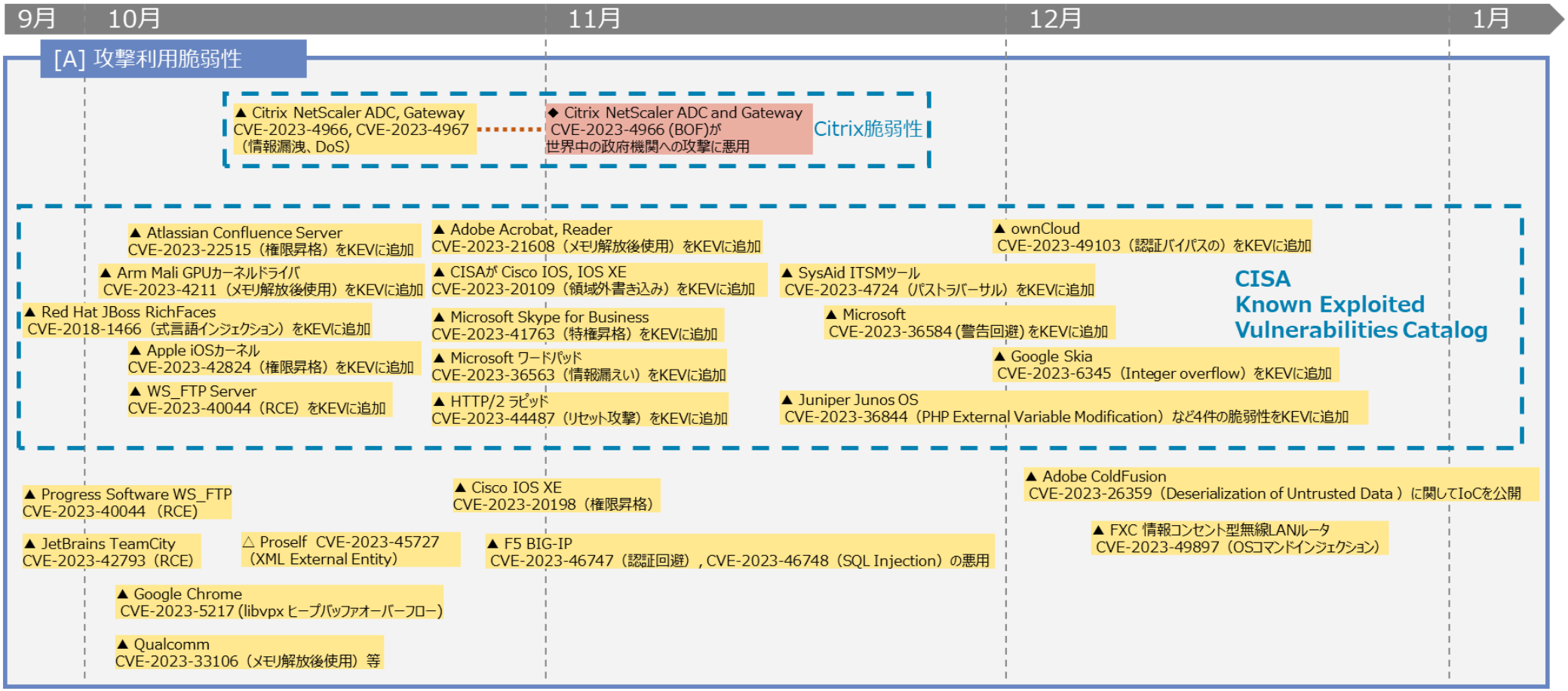
サイバーセキュリティ技術部　NTTDATA-CERT 寺師 悠平・田中 稜太郎

※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

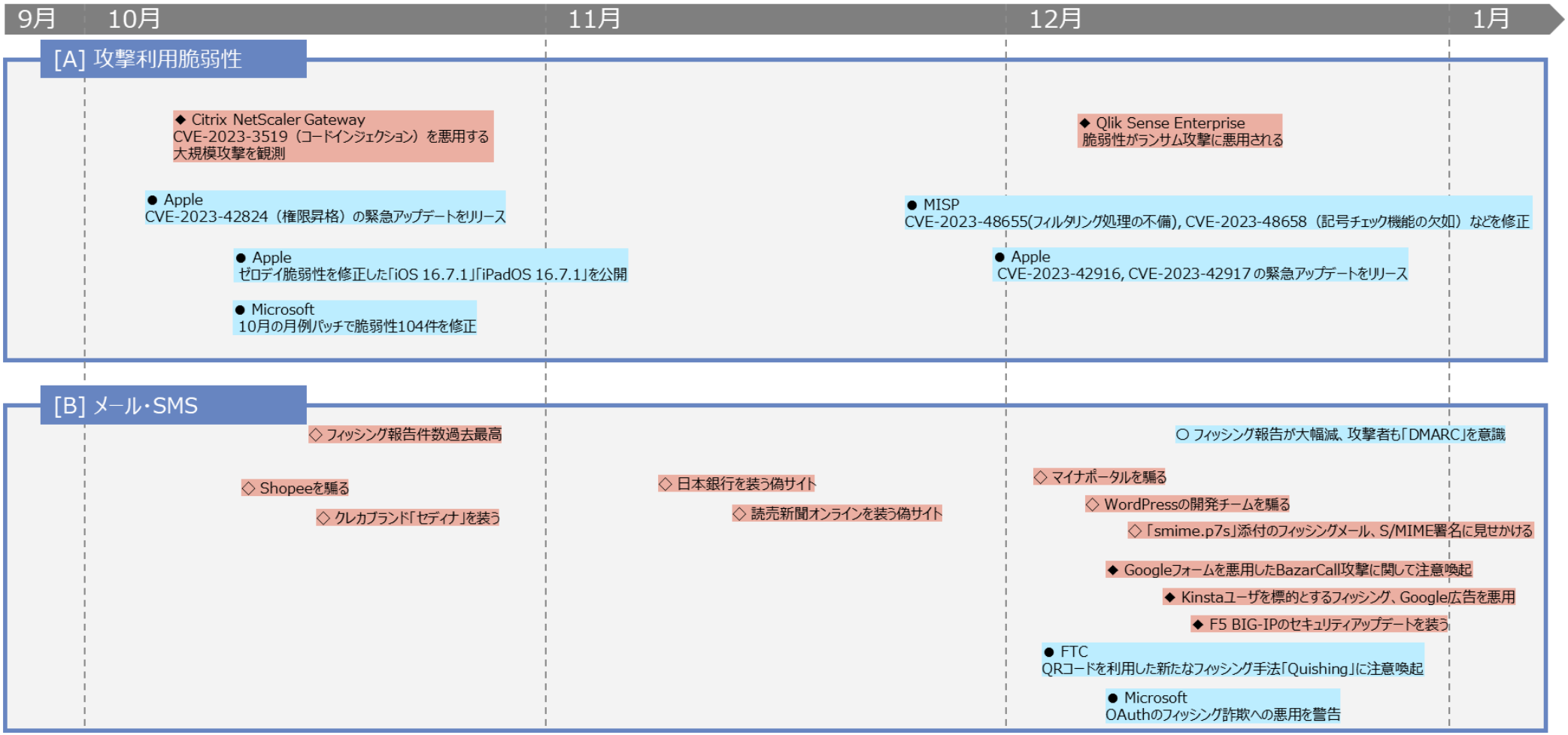


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

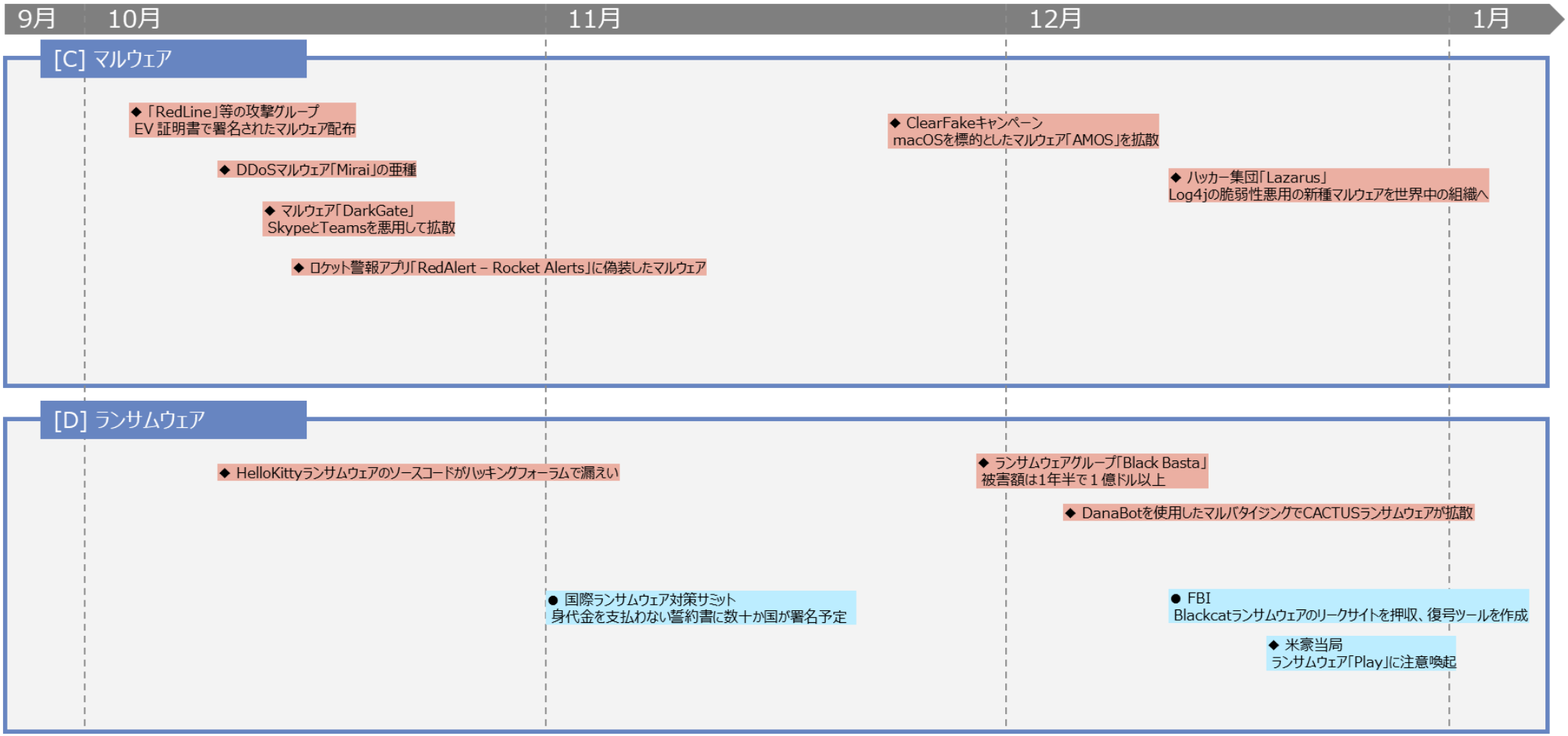


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

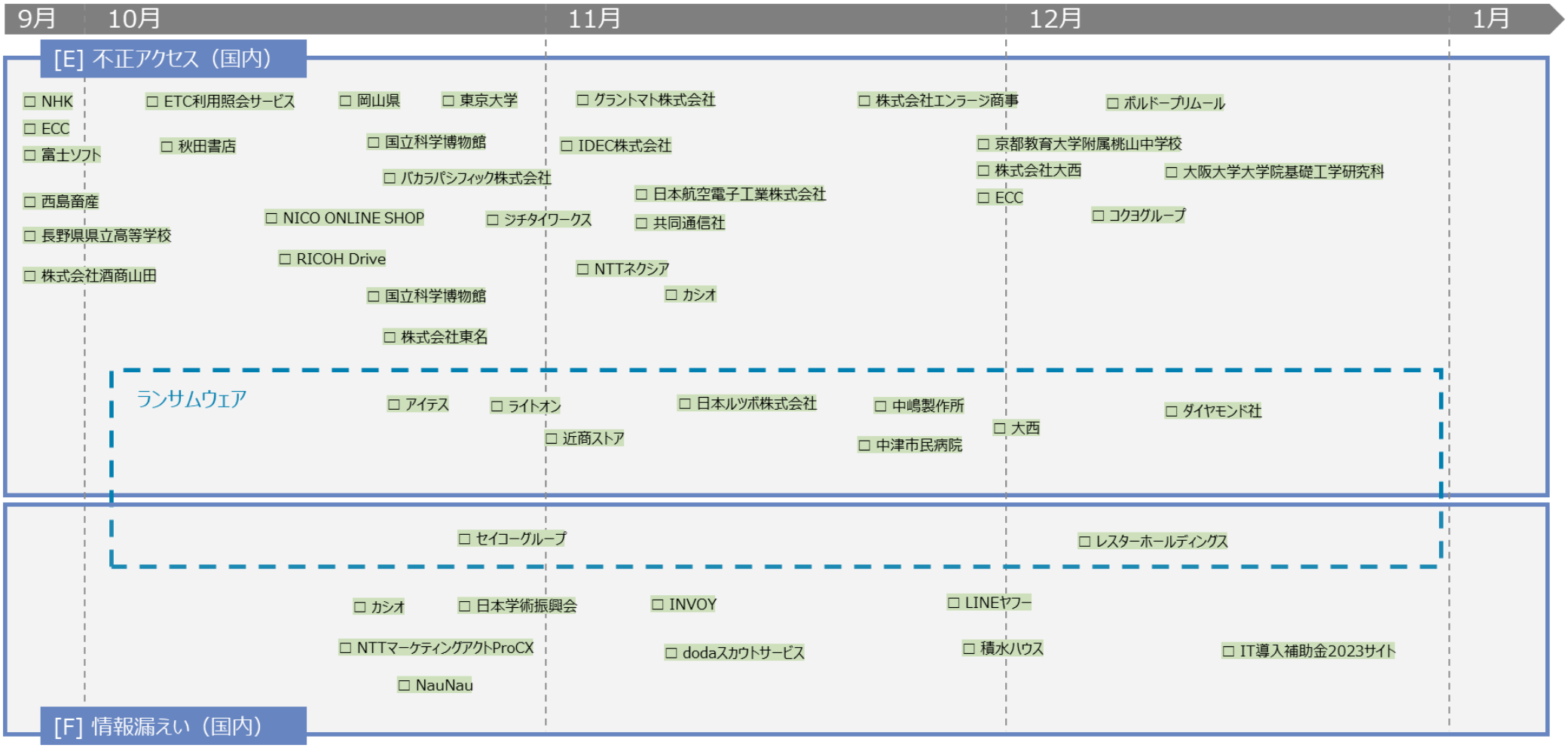


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

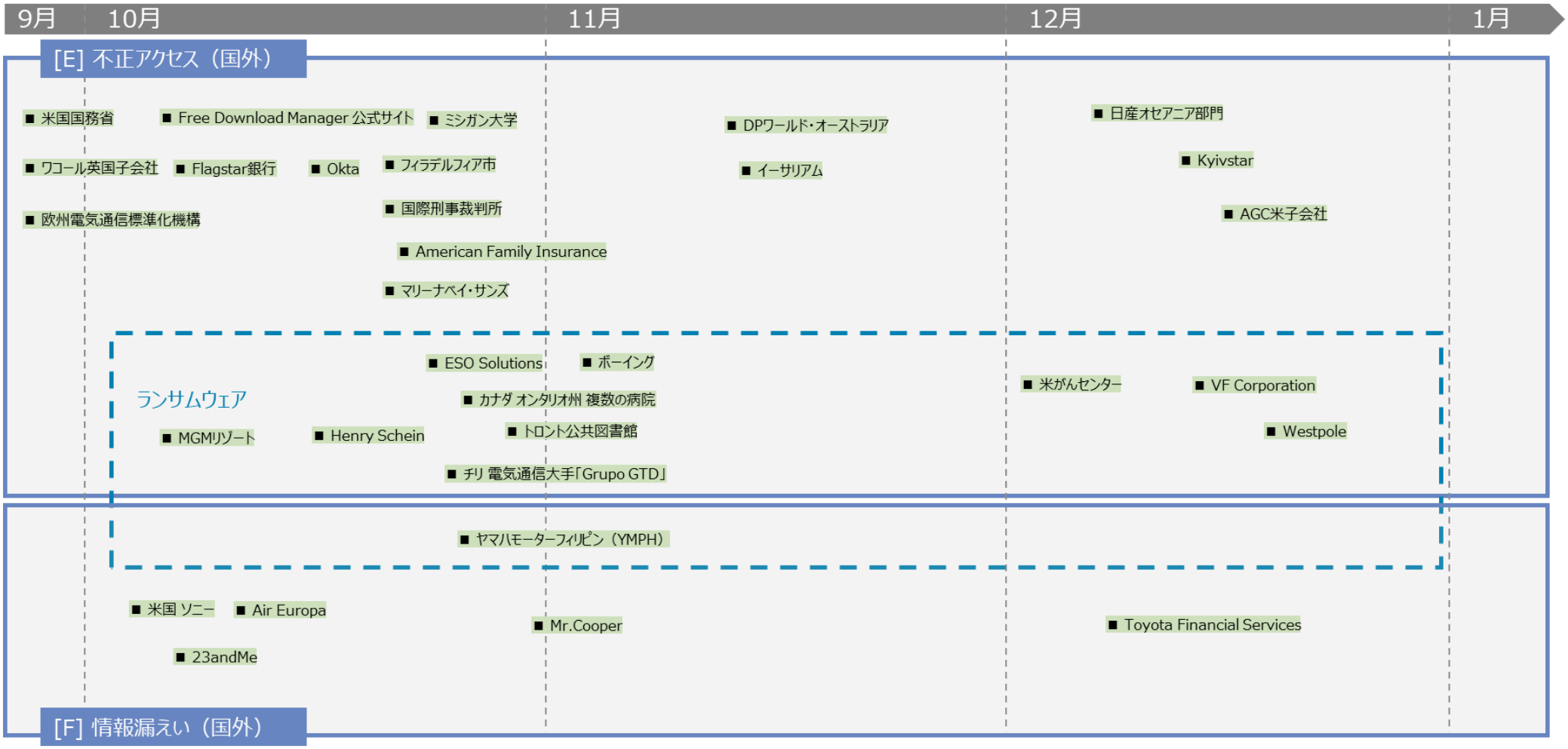


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

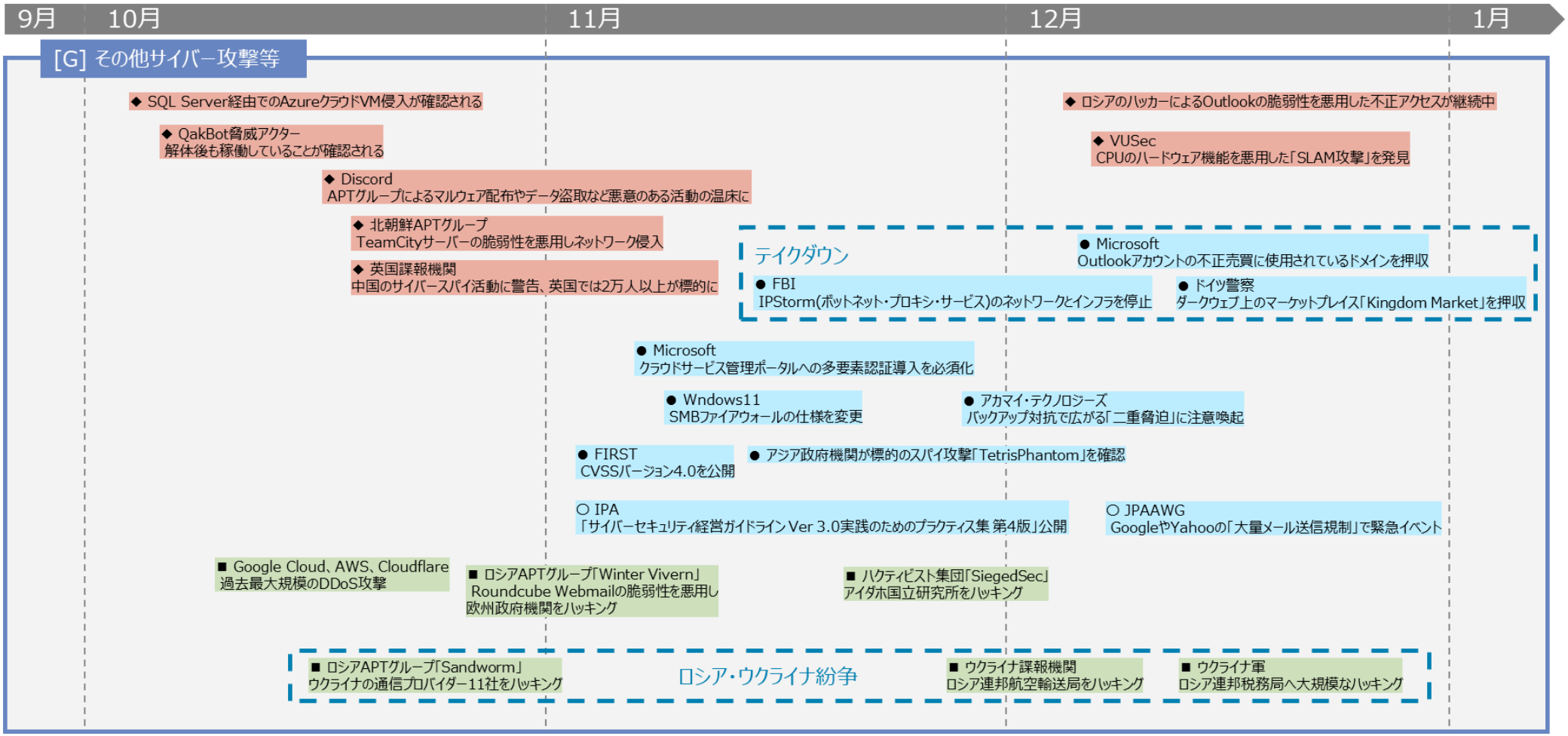


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○: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, “デジタル社会の実現に向けた重点計画,” 9 Jun. 2023. [オンライン]. Available: https://www.digital.go.jp/policies/priority-policy-program.

[2] デジタル庁, “次期個人番号カードタスクフォース（第1回）,” 7 Sep. 2023. [オンライン]. Available: https://www.digital.go.jp/councils/mynumber-card-renewal/8f5526a5-1a75-40e9-859b-281defa27d6c.

[3] デジタル庁, “次期個人番号カードタスクフォース（第3回）,” 26 Dec. 2023. [オンライン]. Available: https://www.digital.go.jp/councils/mynumber-card-renewal/088eeae8-1d38-4267-8ac4-d576eabf2d8d.

[4] CRYPTREC, Mar. 2022. [オンライン]. Available: https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf.

[5] NTT DATA, “グローバルセキュリティ動向四半期レポート,” 19 5 2023. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2022_3q_securityreport.pdf?rev=32ca0531eeb241a59ab983dced8f1a6e.

[6] FIDOアライアンス, “2023年にパスキーによるパスワードレスサインインが70億以上のオンラインアカウントで利用可能になり、FIDO認証の採用が急増,” 7 12 2023. [オンライン]. Available: https://fidoalliance.org/fido-authentication-adoption-soars-as-passwordless-sign-ins-with-passkeys-become-available-on-more-than-7-billion-online-accounts-in-2023/?lang=ja.

[7] COMMISSION, U.S. SECURITIES AND EXCHANGE, “Cybersecurity Disclosure,” [オンライン]. Available: https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214.

[8] European Commission, “EU Cyber Resilience Act,” [オンライン]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

[9] 個人情報保護委員会, “漏えい等報告・本人への通知の義務化について,” [オンライン]. Available: https://www.ppc.go.jp/news/kaiseihou_feature/roueitouhoukoku_gimuka/.

[10] 総務省, “我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項[緊急提言,” [オンライン]. Available: https://www.soumu.go.jp/main_content/000666221.pdf.

[11] 内閣サイバーセキュリティセンター, “内閣サイバーセキュリティセンターの電子メール関連システムからのメールデータの漏えいの可能性について,” [オンライン]. Available: https://www.nisc.go.jp/news/20230804.html.

[12] 国土交通省気象庁, “気象庁及び気象研究所のメール関連機器に対する不正通信の発生について,” [オンライン]. Available: https://www.jma.go.jp/jma/press/2308/04a/press_security_20230804.html.

[13] 日経XTECH, “JPCERT／CCがNISCに苦言？　メール漏洩の情報公開巡り,” [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/news/18/15730/.

[14] 内閣サイバーセキュリティセンター, “サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会,” [オンライン]. Available: https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html.

[15] JPCERT/CC, “電子メール関連システムからのメールデータ漏えい被害が公表されている件について,” [オンライン]. Available: https://www.jpcert.or.jp/press/2023/PR20230807_notice1.html.

[16] 独立行政法人 情報処理推進機構, “Citrix ADC および Citrix Gateway の脆弱性対策について(CVE-2023-3519 等),” [オンライン]. Available: https://www.ipa.go.jp/security/security-alert/2023/alert20230719.html.

[17] CISA, “Threat Actors Exploiting Citrix CVE-2023-3519,” [オンライン]. Available: https://www.cisa.gov/sites/default/files/2023-07/aa23-201a_csa_threat_actors_exploiting_citrix-cve-2023-3519_to_implant_webshells.pdf.

[18] securityintelligence.com, “X-Force uncovers global NetScaler Gateway credential harvesting campaign,” [オンライン]. Available: https://securityintelligence.com/x-force/x-force-uncovers-global-netscaler-gateway-credential-harvesting-campaign/.

[19] National Cyber SecurityCentre, “Products on your perimeter considered harmful,” [オンライン]. Available: https://www.ncsc.gov.uk/blog-post/products-on-your-perimeter.

[20] 警察庁, “令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について,” 21 9 2023. [オンライン]. Available: https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf.

[21] Coveware, “New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying,” 26 1 2024. [オンライン]. Available: https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying.

[22] NO MORE RANSOM, “The No More Ransom Project,” [オンライン]. Available: https://www.nomoreransom.org/ja/index.html.

[23] The Register, “FBI develops decryptor for BlackCat ransomware, seizes gang's website,” 19 12 2023. [オンライン]. Available: https://www.theregister.com/2023/12/19/blackcat_domain_seizure/.

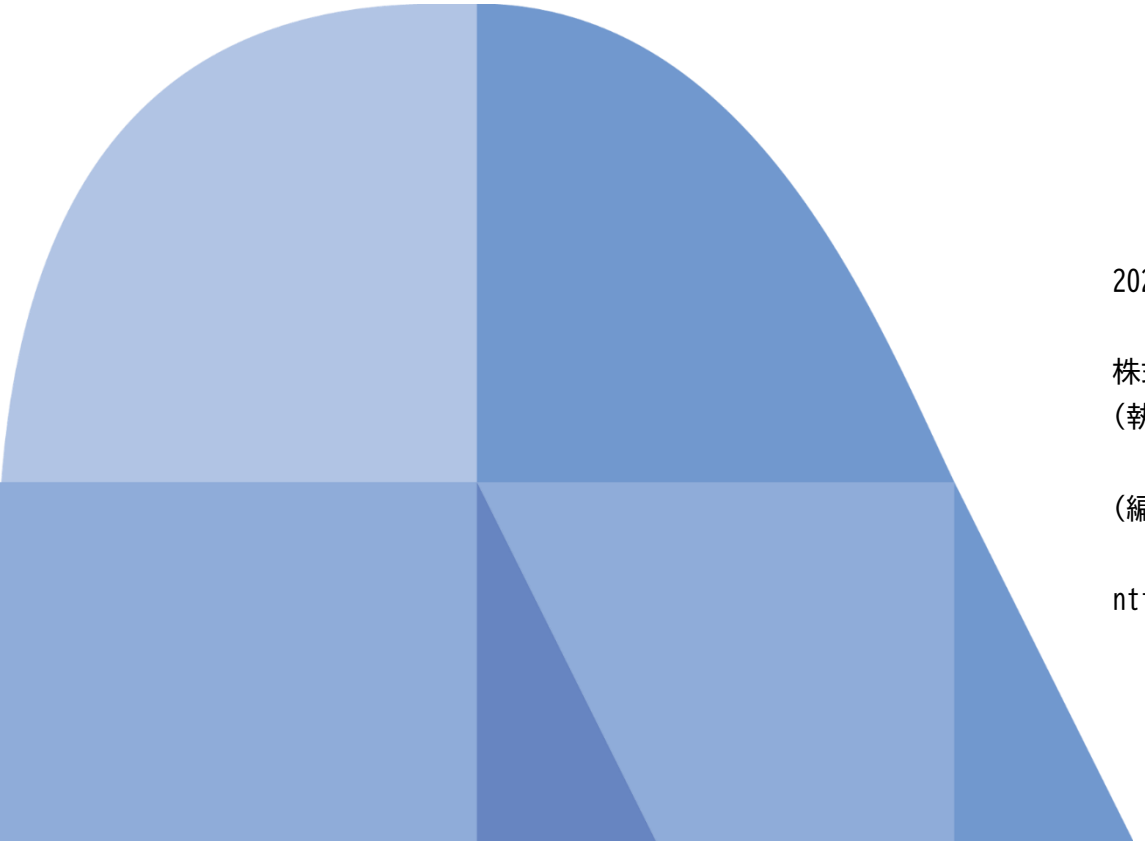
[24] The Register, “When are we gonna stop calling it ransomware? It's just data kidnapping now,” 9 10 2022. [オンライン]. Available: https://www.theregister.com/2022/10/09/extortion_ransomware_threats_category/.

[25] Sophos, “サイバー保険の導入：サイバーディフェンスの最前線で果たす重要な役割,” 3 5 2023. [オンライン]. Available: https://news.sophos.com/ja-jp/2023/05/03/cyber-insurance-adoption-the-critical-role-of-frontline-cyber-defenses-jp/.

[26] 米国OFAC, “Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,” 1 10 2020. [オンライン]. Available: https://ofac.treasury.gov/media/48301/download?inline.

[27] Cybersecurity Dive, “White House considers ban on ransom payments, with caveats,” 8 5 2023. [オンライン]. Available: https://www.cybersecuritydive.com/news/white-house-considers-ransom-payment-ban/649673/.

[28] 一般社団法人 日本損害保険協会, “サイバー保険とは | サイバー保険 | 日本損害保険協会,” [オンライン]. Available: https://www.sonpo.or.jp/cyber-hoken/about/.



2024年6月19日発行

株式会社NTTデータグループ　サイバーセキュリティ技術部
（執筆）紀平 悠人 / 程吉 英仁 / 田杉 怜子 / 武田 晃 / 田島 臣啓 / 嶌谷 直紀
寺師 悠平 / 田中 稜太郎
（編集者）大嶋 真一 / 大谷 尚通 / 杉村 耕司 / 小笠原 弘貴
前田 秀介 / 棚橋 和也 / 宮崎 大輔 / 澤田 貴順
nttdata-cert@kits.nttdata.co.jp