DIR SOC Quarterly

2024 spring

vol 7

政策・法制度の動向

- NISC、セキュアバイデザイン原則に共同署名
- 欧州サイバーレジリエンス法案の合意

トピックス

- 多要素認証が破られる-AiTM攻撃とは
- CVSSの歴史と最新版(v4.0)での改善点

大和総研
Daiwa Institute of Research

目次

はじめに

本冊子は、サイバーセキュリティに関する動向をタイムリーにお伝えすることを目的として発刊を始め、今春で 3 年目を迎えます。今号より親しみやすいフォントへの変更と図表の活用による可読性の向上を新たな取り組みとして始めました。これまで以上に皆様へ有益な情報をお届けできるように執筆者一同切磋琢磨してまいります。今後とも温かい目で見守っていただけますと幸いです。

今回は、2023 年度第3四半期の話題を取り上げます。

本冊子は三部構成となっています。国家主導の下に行われているサイバー攻撃対策については、それを指揮する行政機関の動向をウォッチすることが重要です。第 1 部ではこの点にフォーカスしています。また実際のインシデント事例は、組織がさらされているサイバー攻撃の状況を端的に示すと同時に、組織の対策のあるべき姿を浮かび上がらせるものです。第 2 部はこの点に注目しています。第 3 部では注目度の高いサイバーセキュリティ関連の話題をトピックスとして詳しく説明します。

本冊子にて取り扱っている話題について、いくつかご紹介します。

サイバー攻撃から企業を守る観点で、経営者が認識する必要がある事項などをまとめたものとして『サイバーセキュリティ経営ガイドライン Ver3.0 実践のためのプラクティス集 第 4 版』が公表されました。また米国 CISA は最近急速に利活用が進んでいる AI に関して初めてロードマップを示し、セキュリティ向上のための AI 利用推進や重要インフラ分野への AI 導入支援などに関する取り組みについてまとめられています。

いずれも第 1 部にてその概要を紹介しておりますが、各社のサイバーセキュリティ態勢のチェックもしくは今後強化していく施策などを検討する上で大変有用な内容となっています。

第 2 部では、従来のランサムウェアに代わり確認されているノーウェアランサムによる被害と、国内の複数の企業や大学で確認された短縮 URL サービスを利用した QR コードの問題を取り上げております。いずれも今後の被害拡大が想定される手法ですので、留意しておくべき事象でしょう。

第 3 部では、多要素認証を行っていても破られる可能性のある AiTM 攻撃を取り上げています。認証に対する攻撃は年々巧妙となっているため、様々な攻撃手法が出てきていることをご認識いただければと思っています。また、今回初めて、テクニカルトピックスとして、計算エラーの発生によって秘密鍵が復元される可能性に関するレポートを紹介しています。基礎技術的な専門性の高い内容になりますが、セキュリティに関するトピックスの多様性を体感いただけますと幸いです。

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

2024 年 2 月　株式会社大和総研執筆者一同

1.『サイバーセキュリティ経営ガイドライン Ver 3.0 実践のためのプラクティス集 第4版』の公表

要約

- サイバーセキュリティ経営ガイドラインの実践に役立つ事例を掲載したプラクティス集が公表された。
- DX 推進を見据えたセキュリティ確保の仕組みづくりや、役割に応じた社員教育の手法など、あらゆるセキュリティ対策の課題解決に参考となる実践のためのステップや実践内容が掲載されている。

プラクティス集の内容

独立行政法人情報処理推進機構(IPA)は、2023 年 10 月 31 日、『サイバーセキュリティ経営ガイドライン Ver3.0　実践のためのプラクティス集　第4版』(以下、「本プラクティス集」と略記)を公表しました(*1)。本プラクティス集には、2023 年 3 月に経済産業省と IPA が発行した『サイバーセキュリティ経営ガイドライン Ver3.0(*2)』(以下、「経営ガイドライン Ver3.0」と略記)の「重要 10 項目」を実践する際に参考となる考え方やヒント、実施手順、実践事例が記載されています。

経営ガイドライン Ver3.0 では、サプライチェーンを介したサイバー攻撃の拡大を踏まえたサプライチェーン全体にわたる対策の推進や、制御系を含むデジタル基盤を守ることを意識した対策の普及等を狙った改訂が行われています。これに合わせて本プラクティス集では、サイバー攻撃への備えをさらに強化するため、国内で実際に行われている事例を基に「リテラシーにとどまらないプラスセキュリティ教育の実践」「DX 推進を支える仕組みづくり」「サプライチェーンでの連携体制の構築」などのプラクティスが追加されています。

本プラクティス集の利用場面・構成

本プラクティス集で紹介されている取り組みは、企業へのアンケートやインタビューを通じて収集した、実際に行われている施策に基づいて作成されており、経営者、CISO 等およびセキュリティ担当者が以下のタイミングや場面において利用することが想定されています。

利用するタイミング	具体的な利用場面	第 2 章に掲載されているプラクティスの例
新たにサイバーセキュリティ部門を設置・所管することになった場合や、CISO 等に着任した場合など	どこからサイバーセキュリティの取組に着手してよいかわからない際に、はじめの一歩として実践事例や参考情報を活用する	2-1 サイバーセキュリティリスクに対応するための、兼任のサイバーセキュリティ管理体制の構築
経営環境の変化(デジタルトランスフォーメーションへの取組着手など)により、サイバーセキュリティ対策の重要性が増し、対策を検討する場合など	経営ガイドラインに紐づく実践事例を参考に、サイバーセキュリティ対策の検討に役立てる	5-5 事業部門による DX 推進をセキュリティ確保の観点から支える仕組みづくり 9-2 サプライチェーンで連携する各社が『自社ですべきこと』を実施する体制の構築
インシデントが発生し、サイバーセキュリティ対策を強化しなければならない場合など	取組や工夫の例を参考にインシデントの再発防止に向けた対策の実施に役立てる	7-3 想定されるインシデントについてのセキュリティ分析計画の事前策定 7-4 CSIRT 業務の属人化回避も兼ねたインシデントや脅威に関する情報の共有・蓄積
セキュリティ担当者へ教育を実施する場合や、外部の事業者としてサイバーセキュリティ対策を支援する場合など	人材育成の担当者が教材として活用する、また企業のサイバーセキュリティ対策支援に役立てる	3-2 経営層やスタッフ部門等の役割に応じた、リテラシーにとどまらないセキュリティ教育実践 3-3 サイバーセキュリティ対策のための、必要なサイバーセキュリティ人材の定義・育成

表:本プラクティス集の利用が想定されるタイミング、利用場面およびプラクティスの例

出典:本プラクティス集を基に大和総研作成

(*1) https://www.ipa.go.jp/security/economics/hjuojm00000044dc-att/cms_practice_v4.pdf

(*2) https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf

また、本プラクティス集の構成は

- 第１章　経営とサイバーセキュリティ
- 第２章　サイバーセキュリティ経営ガイドライン実践のプラクティス
- 第３章　セキュリティ担当者の悩みと取組のプラクティス
- 付録　サイバーセキュリティに関する用語集、サイバーセキュリティ対策の参考情報

となっており、経営者は第１章が、CISO 等およびセキュリティ担当者は本プラクティス集全体が参考となるように構成されています。各ページ上部の見出し欄には対象読者やセキュリティ対策の取り組みのレベルなどが示されており、それぞれの読者が置かれている立場や状況に応じて、より最適な内容を参照しやすい形となっています。

図：重要 10 項目ごとにまとめたプラクティス（第２章）

出典：本プラクティス集から転載

本プラクティス集の活用

本プラクティス集は、様々なセキュリティ対策の課題に対して、実践のためのステップや実践内容が具体的に記されているため、実用性が高く、自社のセキュリティ対策の強化を図る上で非常に参考になると思われます。

近年、DX 化やサプライチェーンリスクの拡大などによって、対策が必要なセキュリティ上の課題は複雑化しているところ、一体何に取り組んだらよいか悩んでいる経営者やセキュリティ担当者は多いのではないでしょうか。そういった悩みの解決に向けた具体的な道筋を立てるためにも、本プラクティス集は大変参考になるでしょう。

2. 米国CISA、サイバーセキュリティにおけるAI に関する初のロードマップ発表

要約

- 米国 CISA が2023年 11 月 14 日、サイバーセキュリティにおける AI に関する初のロードマップを発表した。本ロードマップは、5 つの取り組みと計 24 個の目標で構成されている。
- 日本国内においても、2023 年 11 月 28 日に、G7 各国含む計 18 カ国が参加し作成した『セキュア AI システム開発ガイドライン』に共同署名するといった AI 利用に関する動きがある。

CISAがサイバーセキュリティのAIロードマップを発表

米国国土安全保障省（DHS：Department of Homeland Security）のサイバーセキュリティ・インフラストラクチャー安全保障庁（CISA：Cybersecurity and Infrastructure Security Agency）は、2023 年 11 月 14 日、AI に関する初のロードマップ『2023 2024 CISA ROADMAP FOR ARTIFICIAL INTELLIGENCE(*1)』を発表しました(*2)。本ロードマップは、安全・セキュアで信頼できる AI の開発・利用に関する大統領令 EO 14110(*3)に沿った内容で、セキュリティ向上のための AI 利用推進や重要インフラ分野への AI 導入支援などに関する CISA としての取り組みなどについてまとめられています。

5 つの取り組みと計 24 個の目標

今回公表されたロードマップは、以下の表のように、5 つの戦略的な取り組み（LINE OF EFFORT）と計 24 個の目標（OBJECTIVE）で構成されています。

戦略的な取り組み（LINE OF EFFORT）	目標（OBJECTIVE）
1　使命をサポートするために責任をもって AI を使用する	1.1　CISA による AI の使用に関するガバナンスと監視プロセスを確立する。 1.2　CISA のミッションをサポートするために、AI のユースケースを収集、レビュー、優先順位づけする。 1.3　次世代の AI 対応テクノロジーの導入戦略を策定する。 1.4　サイバー防御、インシデント管理、復旧手順を AI システムとプロセスに組み込む。 1.5　CISA における AI 利用に対するバイアスを制限するための総合的なアプローチを検討する。 1.6　CISA の役割を支援するために、責任をもって安全に AI システムを導入する。
2　AI システムを評価して保証する	2.1　重要インフラ分野における AI 導入のサイバーセキュリティリスクを評価する。 2.2　重要インフラ分野の関係者と協力して、AI 導入におけるセキュリティとレジリエンスの課題を特定する。 2.3　連邦企業全体で使用されている AI システムの範囲を把握する。 2.4　安全な AI システムの調達、開発、運用に関するベストプラクティスとガイダンスを開発する。 2.5　AI システムに対する強力な脆弱性管理手法の導入を推進する。 2.6　AI システムをセキュアバイデザインの取り組みに組み込む。

(*1) CISA『2023 2024 CISA ROADMAP FOR ARTIFICIAL INTELLIGENCE』
(https://www.cisa.gov/sites/default/files/2023-11/2023-2024 CISA-Roadmap-for-AI 508c.pdf)

(*2) CISA『DHS Cybersecurity and Infrastructure Security Agency Releases Roadmap for Artificial Intelligence』

(https://www.cisa.gov/news-events/news/dhs-cybersecurity-and-infrastructure-security-agency-releases-roadmap-artificial-intelligence)

(*3) Executive Office of the President『Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence』
(https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence)

3　AI の悪意ある使用から重要インフラを保護する	3.1　AI ツールを開発している業界の利害関係者と定期的に連携して、重要インフラ分野のセキュリティ上の懸念を評価して対処し、利害関係者の教育方法を評価する。 3.2　CISA パートナーシップとワーキンググループを利用して、AI による脅威に関する情報を共有する。 3.3　重要インフラに対する AI リスクを評価する。
4　省庁間、国際パートナー、市民と協力する	4.1　AI 政策問題に対する DHS 全体のアプローチの開発を支援する。 4.2　AI に関する省庁間の政策会議や省庁間のワーキンググループに参加する。 4.3　覚書やその他の製品などの AI 政策文書について、戦略的かつ国家レベルの視点を考慮した CISA の政策立案を行う。 4.4　CISA の戦略、優先順位、政策枠組みが省庁間の政策や戦略と一致していることを確認する。 4.5　グローバルな AI セキュリティに関して国際パートナーと連携する。
5　AI の専門知識を職員に拡大する	5.1　CISA の職員に既に存在する AI の専門知識を結びつけて強化する。 5.2　AI の専門知識を持つインターン、フェロー、スタッフを採用する。 5.3　CISA の職員に AI について教育する。 5.4　内部トレーニングには技術的な専門知識が反映されるだけでなく、CISA の業務のあらゆる側面にわたって AI 実装に関する法的、倫理的、政策的な考慮事項も組み込まれるようにする。

表：CISA の戦略的な取り組みと目標
出典：CISA『2023 2024 CISA ROADMAP FOR ARTIFICIAL INTELLIGENCE』を基に大和総研作成

AI に関する日本国内動向について

AI の利用について、日本国内では、内閣府科学技術・イノベーション推進事務局と内閣官房内閣サイバーセキュリティセンター（NISC）が、2023 年 11 月 28 日に、日本の他、英国国家サイバーセキュリティセンター（NCSC）や米国 CISA など G7 各国含む計 18 カ国が参加し作成した『セキュア AI システム開発ガイドライン』の共同署名を行ったことを発表しました（*1）。

本ガイドラインは、「セキュアバイデザインの観点から、ソフトウェアのうち AI に焦点を当てて、AI を使用するシステムのプロバイダーによるセキュアな AI システムの構築を支援するための指針」との位置づけとなっています。内閣府科学技術・イノベーション推進事務局および NISC は、「今後は、技術の進歩が早い分野であることも踏まえ、本件文書の具体化に当たり、産業界とも継続的に対話を重ねつつ、引き続き、AI 及びサイバーセキュリティ分野での国際連携の強化に努めてまいります」と述べており、CISA が今回発表したロードマップの内容なども踏まえ、日本国内においても、安全・セキュアで信頼できる AI の開発・利用が推進されるものと見受けられます。

本ロードマップ発表からの示唆

米国でサイバーセキュリティの中枢を担う CISA が AI について今回のような具体的なロードマップを発表することは興味深く、AI の急速な発展・普及により、サイバーセキュリティに対する脅威が増大していることが背景にあるものと見受けられます。NISC など日本におけるサイバーセキュリティの中枢を担う組織も、セキュアな AI システム開発などで国際連携を推進しており、サイバーセキュリティと AI がこれからより密接に関わってくることが確実視されます。

AI とサイバーセキュリティは、共進化の関係にあると考えられます。AI の発展にともない、より高度なセキュリティ対策が求められる一方で、AI 自体もサイバーセキュリティの脅威となる可能性があります。このような状況下で、AI とサイバーセキュリティの研究と開発を進めるには、ロードマップでも述べられているように技術的な側面だけでなく、法的・倫理的な側面も含めて総合的なアプローチが求められるものと考えられます。日本国内だけでなく国際的な動向を注視することが必要であるといえるでしょう。

（*1）内閣府科学技術・イノベーション推進事務局、内閣官房内閣サイバーセキュリティセンター『セキュア AI システム開発ガイドラインについて』（ https://www.nisc.go.jp/pdf/press/press Guidelines for Secure AI System Development.pdf ）

3. NISC がセキュアバイデザイン原則に関する国際共同ガイダンスに署名

要約

- NISC がセキュアバイデザイン・セキュアバイデフォルト原則に関する国際共同ガイダンスに署名した。
- このガイダンスでは、製品やサービスの提供側がサイバーセキュリティに関してより大きな責任を担うべきと提言されている。
- 今後、わが国の法令やガイドラインに取り込まれていく可能性もあり、提供側の事業者は留意すべき。

NISC が共同署名したガイダンス

2023 年 10 月 17 日、内閣官房内閣サイバーセキュリティセンター（NISC）は、セキュアバイデザイン・セキュアバイデフォルト原則に関する国際共同ガイダンス（以下、「本ガイダンス」と略記）に署名しました(*1)。本ガイダンスはもともと 2023 年 4 月に米国をはじめとして、オーストラリア、英国、カナダなど各国のセキュリティ関連の 10 組織が共同で策定・公表したもの(*2)ですが、今回改訂版を公表するにあたり、新たに 8 組織が加わり、合計 18 組織で共同署名しました。NISC も今回新たに共同署名に加わった 8 組織のうちの一つです。

なお、本ガイダンスによれば(*3)、「**セキュアバイデザイン**」とはリスクアセスメントによりサイバー脅威を把握して製品の計画段階からセキュリティを考慮し、悪意ある攻撃者による不正アクセスを十分に防げるような仕方で製品が作られていることを意味します。また「**セキュアバイデフォルト**」とは製品購入後に特に設定を変更することなく、また追加費用を支払うこともなく、広く悪用される攻撃手法に対して強靭な状態にあることを意味します。なお、本ガイダンスではサービスについても製品とほぼ同列に論じられていることから、ここでの製品はクラウドサービスなどのサービスも含むものと考えられます。

図：セキュアバイデザイン・セキュアバイデフォルト原則に関する国際共同ガイダンスに署名した 18 組織
出典：本ガイダンスから転載(*4)

(*1) https://www.nisc.go.jp/pdf/press/press Shifting the Balance of Cybersecurity Risk.pdf

(*2) https://www.cisa.gov/sites/default/files/2023-06/principles approaches for security-by-design-default 508c.pdf

(*3) CISA 他『Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software』pp.8-9（ https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign 1025 508c.pdf ）

(*4) 同上書 p.2

本ガイダンスで示されている 3 原則

本ガイダンスは、現状ではサイバーセキュリティを確保するためのコストを製品やサービスの提供者側ではなく、利用者側がより多く負担していることを問題視しています。たとえば、利用者側は製品バグを修正するためのセキュリティパッチを継続的に適用したり、セキュリティ確保のための設定に多大な注意を払ったりしなければなりません。

そこで、本ガイダンスでは、セキュアバイデザインとセキュアバイデフォルトの考え方がこの負担バランスを変更するとし、製品やサービスの提供者に対し、セキュリティをデザインプロセスに組み込むために以下の 3 原則に則るよう呼びかけています。そして、この 3 原則に則り、また則っていることを外部に示すための具体的な実践方法について詳細に紹介しています。

1. 顧客のセキュリティに責任をもつ
2. 徹底的な透明性と説明責任を引き受ける
3. これらの目的を達成するための組織構造とリーダーシップを構築する

セキュアバイデザイン・セキュアバイデフォルトの実践

また本ガイダンスでは、具体的なセキュアバイデザイン・セキュアバイデフォルト手法も例示しています。たとえば下表のような例が示されています。

セキュアバイデザイン手法（抜粋）	セキュアバイデフォルト手法（抜粋）
• メモリ安全なプログラミング言語を使用する • メモリを保護するようなハードウェアを採用する • 安全なソフトウェアコンポーネント（ライブラリ、ミドルウェア、フレームワークなど）を利用する • Web 攻撃に対する対策を実装してある Web テンプレートフレームワークを使用する • 静的・動的なアプリケーションセキュリティテストを実施する • ソースコードレビューを実施する • SBOM(*1)を生成する • 一つのセキュリティ対策の侵害がシステム全体の侵害とならないように多層防御を実装する	• デフォルトパスワードをなくす • 特権ユーザーは多要素認証を必須とする • シングルサインオンを実装する • 追加料金や設定変更なしで監査ログを提供する • 役割ごとに推奨する権限ロールを提供する • 後方互換性よりもセキュリティを優先する • 「セキュリティ強化ガイド」の内容をデフォルト設定に組み込み、ガイド自体は縮小する • 設定があること自体、ユーザーの認知負荷となるため、セキュリティ設定は製品自体に組み込んでなくすべきであり、設定が必要な場合はデフォルト設定をセキュアなものとする

出典：セキュアバイデザイン・セキュアバイデフォルト原則に関する国際共同ガイダンス(*2)を基に大和総研作成

示唆

実はわが国でも 2015 年 9 月に閣議決定された『サイバーセキュリティ戦略(*3)』に「**セキュリティ・バイ・デザイン**」という類似の概念が記載されており、その後も継続的にわが国の『サイバーセキュリティ戦略』や『年次計画・年次報告』で触れられてきました。また、2022 年 6 月にはデジタル庁が『政府情報システムにおけるセキュリティ・バイ・デザインガイドライン(*4)』という文書も策定しています。

今後は国内でこのような動きが加速し、わが国のその他のガイドラインや産業界のガイドラインにセキュアバイデザインの考え方が取り込まれ、さらには法制化されたり、事実上の標準（デファクトスタンダード）となったりする可能性もあり、ソフトウェア製品やサービスを提供する組織は注意が必要です。

(*1) software bill of materials の略で、ソフトウェアを構成するコンポーネントや依存関係などの情報が含まれているソフトウェア部品表のこと（ https://www.dir.co.jp/world/entry/solution/scrm ）

(*2) CISA 他『Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software』pp.28-31（ https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf ）

(*3) https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku.pdf

(*4) https://www.digital.go.jp/assets/contents/node/basic page/field ref resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/2a169f83/20220630 resources standard guidelines guidelines 01.pdf

4. 欧州サイバーレジリエンス法案(EU Cyber Resilience Act)の合意

要約

- 2023 年 11 月 30 日に欧州議会と EU 理事会が欧州サイバーレジリエンス法案に合意。
- デジタル製品の提供者は製品のライフサイクル全般にわたってセキュリティに責任を負う。
- 迅速な報告は世界的な潮流になっており、わが国でも動向に注視が必要。

欧州議会と EU 理事会の合意

2023 年 11 月 30 日に欧州議会と EU 理事会が欧州サイバーレジリエンス法案に合意しました(*1)。この法案は、デジタル製品の利用者を保護することを目的とし、製品を提供する事業者(製造者、輸入者、販売者)に対し、企画・設計、開発、販売、保守など製品のライフサイクル全般にわたってサイバーセキュリティに責任をもつことを課すものです。

欧州議会と EU 理事会が合意に達した実際の法案内容は公開されていませんが、2022 年 9 月に欧州委員会が提案した草案の本質的な部分は変更されていないようです(*2)。今後、欧州議会と EU 理事会での正式な承認手続きを経て発効し、デジタル製品を提供する事業者は、発効後 36 カ月以内(早ければ 2027 年初頭)、一部要件は 21 カ月以内(早ければ 2025 年後半)にこの法案が規定するセキュリティ要件を満たす必要があります(下図参照)。そして、要件を満たせない場合は、最大で 1,500 万ユーロ(約 24 億円)もしくは全世界での前年売上高合計の 2.5%のいずれか高い方の額を罰金として科される可能性(*3)があります。

なお、この法案の対象となる「デジタル製品」とは、直接的・間接的に他のデバイスやネットワークに接続するすべての製品であり、ホームカメラや冷蔵庫、テレビ、玩具など他のデバイスやネットワークに接続する製品であればこの法案の対象になります。逆に対象外とされるのは、既に EU の他の法令でサイバーセキュリティ要件が規定されている医療機器や航空関連製品、自動車など一部の製品です(*2)。

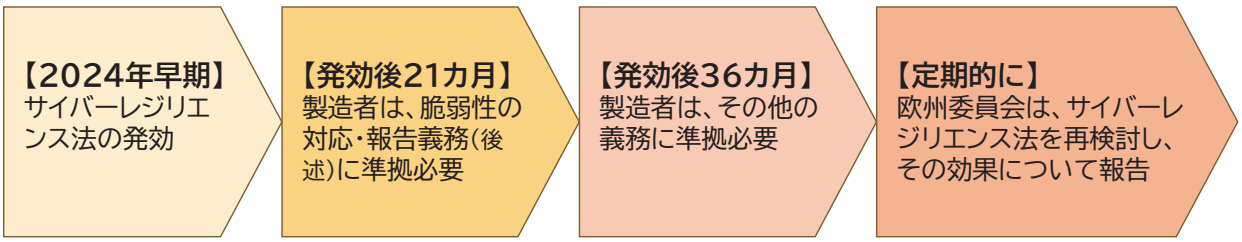


図: 欧州サイバーレジリエンス法の今後のタイムライン

出典: 欧州委員会『Cyber Resilience Act – Factsheet』(*4)および欧州委員会『Commission welcomes political agreement on Cyber Resilience Act』(*5)を基に大和総研作成

(*1) https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6168

(*2) EU 理事会『Cyber resilience act: Council and Parliament strike a deal on security requirements for digital products』(https://www.consilium.europa.eu/en/press/press-releases/2023/11/30/cyber-resilience-act-council-and-parliament-strike-a-deal-on-security-requirements-for-digital-products/)

(*3) Cyber Resilience Act の草案 53 条 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454)

(*4) https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet

(*5) https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6168

厳しいセキュリティ要件

この法案は、製品の提供者に対して非常に厳しいセキュリティ要件に準拠することを求めている点が大きな特徴です。特に製品の製造者は、製品の企画・設計段階からサイバーセキュリティを考慮する必要があり、リスクアセスメントの実施や 5 年間のセキュリティパッチの提供、技術文書および SBOM(*1)の作成も求められます。

また、脆弱性対応に関しては、活発に悪用されている脆弱性を発見したり、製品のセキュリティに重大な影響を与えるインシデントを認識したりした場合は、24 時間以内にセキュリティ担当の当局に報告する必要があります。下表は 2022 年 9 月に公表された草案に示されているセキュリティ要件の抜粋です。なお、草案ではこれらの義務は草案本文と附属書に分割して記載されていますが、以下では両者から抽出した主だった義務をまとめて記載しています。

製造者の義務（抜粋）
• デジタル製品はそのリスクに応じたレベルのサイバーセキュリティを確保する形で設計、開発、製造されていること。 • 製造者は製品のリスクアセスメントを実施し、その結果を製品の企画、設計、開発、製造、販売、保守の各フェーズで考慮に入れること。 • 上記のリスクアセスメントに基づいて、セキュアバイデフォルトの設定で出荷されること。 • 製造者は製品の脆弱性とコンポーネントについて特定し、文書化すること（ここには一般的な機械読み取り可能な形式の SBOM の作成も含む）。 • 製造者は、製品寿命か発売開始後 5 年間のいずれか短い方の期間の間、製品の脆弱性に対処すること。 • 製造者は、発売開始前に技術文書を作成して、適合性評価手続きを実施し、適合性が示された場合は製品に CE マークを貼付すること。
製造者の報告義務（抜粋）
• 製造者は、活発に悪用されている脆弱性を発見した場合は 24 時間以内に欧州ネットワーク情報セキュリティ機関に報告すること。 • 製造者は、製品のセキュリティに重大な影響を与えるインシデントを認識した場合は 24 時間以内に欧州ネットワーク情報セキュリティ機関に報告すること。 • 製造者は、製品の利用者に対してインシデントについて遅滞なく通知すること。また、必要ならばそのインシデントの影響を緩和する方法についてもユーザーに通知すること。

出典：Cyber Resilience Act の草案(*2)を基に大和総研作成

インシデントの迅速な報告

この法案は急増するサイバー攻撃被害からデジタル製品の利用者を保護するため、製品の提供者により重い責任を課し、製品のライフサイクル全般にわたってサイバーセキュリティを確保させようとしており、本冊子の「3. NISC がセキュアバイデザイン原則に関する国際共同ガイダンスに署名」で紹介した「セキュアバイデザイン・セキュアバイデフォルトの原則」に通じるものがあります。

また、この法案が求める脆弱性やインシデントの迅速な報告も世界的な潮流といえます。本冊子前号の DIR SOC Quarterly vol.6 2023 autumn(*3)でも米国証券取引委員会におけるサイバーセキュリティ開示義務規則の採択によってサイバーセキュリティインシデントの迅速な開示が求められるようになったことを紹介しました。

今後はこのような世界的な潮流の高まりの影響を受け、わが国でも何らかの形で法令化される可能性があります。セキュアバイデザイン・セキュアバイデフォルトの原則を自社の製品開発プロセスに組み込んだり、セキュリティインシデントを迅速に報告できるような社内体制を整えたりすることは、欧州や米国でビジネスを展開する企業にとってはもちろんのこと、国内のみでビジネスを展開する企業にとっても今後ますます重要性を増していくと考えて間違いありません。

(*1) software bill of materials の略で、ソフトウェアを構成するコンポーネントや依存関係などの情報が含まれているソフトウェア部品表のこと（ https://www.dir.co.jp/world/entry/solution/scrm ）

(*2) Cyber Resilience Act の草案 10 条、11 条、附属書Ⅰ（ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454 ）

(*3) https://www.dir.co.jp/publicity/publication/socquarterly2310.html

5. 基幹インフラ役務の安定的な提供の確保に関する制度（経済安全保障推進法）の施行

要約

- 政府は経済安全保障推進法に基づき、基幹インフラ役務の安定的な提供の確保に関する制度を施行した。
- 金融庁はパブリックコメントを受けて、本制度に関する Q&A を公表した。
- 以下では、パブリックコメントに対する回答のポイントを解説する。

施行された制度の概要

政府は 2023 年 11 月 17 日、経済安全保障推進法(*1)における 4 つの経済施策の一つである『基幹インフラ役務の安定的な提供の確保に関する制度』(以下、「本制度」と略記)を施行しました(*2)。本制度は法律上、2024 年 2 月 17 日までの政令指定日から施行される予定でしたが、期日より 3 カ月も早い施行となりました。

これまで本冊子で度々紹介してきましたが、本制度はインフラサービスの安定的な提供の確保を目的としています。具体的には、インフラ事業者が設備を導入または設備の維持管理等を委託する場合に、政府への事前届出を義務付け、審査の対象とするものです。同日に特定社会基盤事業者(*3)が初めて告示され、これらの特定社会基盤事業者については、6 カ月間の経過措置期間を経て 2024 年 5 月 17 日から制度の規制(届出義務)が適用されることとなります。

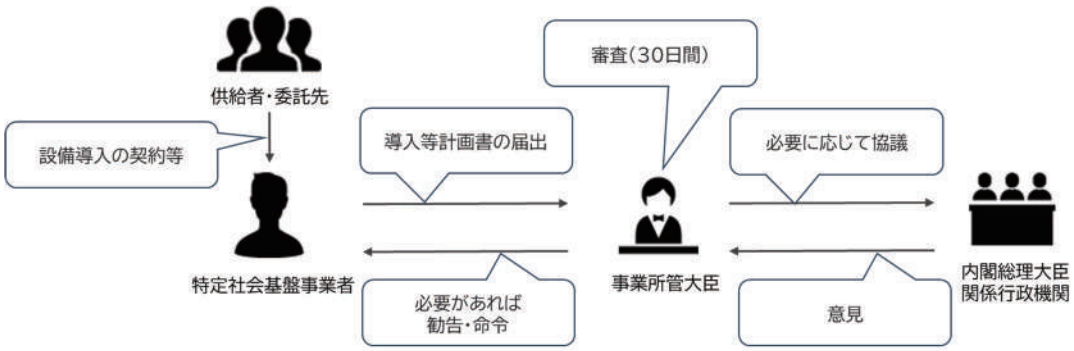


図:制度のスキーム
出典:内閣府『特定社会基盤役務の安定的な提供の確保に関する制度について』を参考に大和総研作成

金融分野における経済安全保障対策

金融庁では、構成設備や重要維持管理などの内容、特定重要設備の導入や他の事業者への委託に関する手続きを定めるために内閣府令を改正する「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律に基づく特定社会基盤事業者の指定等に関する内閣府令の一部を改正する内閣府令(案)(*4)」を、2023年9月 15 日から同年 10 月 14 日にかけて公表し広く意見を募りました。本件に関して、18 の個人および団体から 95 件のコメントが集まり、このパブリックコメントに対する金融庁の考え方が公表されています(*5)。

(*1) https://www.cao.go.jp/keizai_anzen_hosho/index.html

(*2) 内閣府『基幹インフラ役務の安定的な提供の確保に関する制度』
(https://www.cao.go.jp/keizai_anzen_hosho/infra.html)

(*3) 電気、ガス、水道、通信、金融サービスなどを行うインフラ事業者のうち、国が一定の基準のもと、規制対象とする事業者で、各事業所管省庁において公表(https://www.cao.go.jp/keizai_anzen_hosho/infra.html)

(*4) https://www.fsa.go.jp/news/r5/sonota/20230915/20230915.html

(*5) 金融庁『コメントの概要及びコメントに対する金融庁の考え方』
(https://www.fsa.go.jp/news/r5/sonota/20231116/01.pdf)

パブリックコメントで目立ったものでは、クラウドサービス技術の発展のスピードを鑑みた届出手続きの改善措置、構成設備の定義の明確化、構成設備に対する、官庁による事前審査の簡略化の要望などが挙げられます。

特に、事前審査の簡略化については、構成設備供給者に外資系の企業（準拠法が国外）も多く含まれることが想定されるなかで、供給者等の役員の旅券の写しなどのセンシティブ情報の収集に関する懸念、また汎用製品（OS、仮想化ソフト、セキュリティ対策ソフト、サーバー、ネットワーク機器等）の製造者は共通する供給者となり複数回の申請となることから煩雑な手続きが想定されるため、強く要望されています。

素案からの変更点

パブリックコメントを受けて変更が加えられた箇所は以下の5つがありましたが、方針内容には追加や変更はありませんでした。また、金融庁は 11 月 17 日の本制度の施行を受けて、パブリックコメントでの意見を踏まえた本制度の Q&A(*1)を公表し、特定重要設備や構成設備の粒度や具体的な例示についての情報を業種ごとに開示しています。

修正箇所	素案(*3)	修正後	修正理由
府令(*2)第24条第4号(3)	議決権の百分の五十	議決権の百分の五十以上の議決権の数を直接に保有する者に該当する者がある場合	記載不備
様式第8(2)のリード文	同法第3条に基づき	同条第3項に基づき	誤植
様式第 10 の題名	特定重要設備(緊急導入等届出書)の導入を行った後の構成設備の変更の報告書	特定重要設備の導入を行った後の構成設備の変更の報告書	緊急導入等届出書だけではなく導入計画書によって行われた場合にも使用されるため
様式第 4(1) 5.の④－1	定期的な確認	定期的又は随時に確認	設備の製造工程は特定重要設備や構成設備により様々であり、「定期的な確認」が必要な頻度も異なりうると考えられるため
様式第 4(1) 5.の④－2			

出典：『内閣府令(*2)』、『素案(*3)』、『コメントの概要及びコメントに対する金融庁の考え方(*4)』を基に大和総研作成

パブリックコメントの回答からの示唆

金融庁の回答から示唆されるのは、2023 年 4 月 28 日に閣議決定し、公表された基本指針(*5)に記載されているように、特定社会基盤事業者が『自ら』リスクを評価し、そのリスクの内容と程度に応じて対策を講じることが重要であるということです。このアプローチは、リスクアセスメント（特定、分析、評価）とリスクコントロール（低減、受容、移転、回避）というセキュリティの基本原則に適合します。これは、サプライチェーン攻撃やランサムウェアによる被害を防止するために企業が取り組むべき重要な要素であり、本制度の趣旨を踏まえてシステムの持続的な提供に不可欠といえるでしょう。

なお、本制度は、金融庁以外の省庁も関係しており、内閣府が、省庁横断的に関連情報を提供するサイトを設けています(*6)。

(*1) 金融庁『金融分野における経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説』（ https://www.fsa.go.jp/news/r5/economicsecurity/infra kaisetsu financesector.pdf ）

(*2) 経済安全保障推進法に基づく特定社会基盤事業者の指定等に関する内閣府令（e-Gov 法令検索）（ https://elaws.e-gov.go.jp/document?lawid=505M60000002061 ）

(*3) 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律に基づく特定社会基盤事業者の指定等に関する内閣府令の一部を改正する内閣府令（案）（ https://www.fsa.go.jp/news/r5/sonota/20230915/01.pdf ）

(*4) 金融庁『コメントの概要及びコメントに対する金融庁の考え方』（ https://www.fsa.go.jp/news/r5/sonota/20231116/01.pdf ）

(*5) 閣議決定『特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針』（ https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin2.pdf ）

(*6) 各省庁の相談窓口（ https://www.cao.go.jp/keizai anzen hosho/infra.html ）

1. サイバー攻撃の新たな手口「ノーウェアランサム」

要約

- 「ノーウェアランサム」とはデータを暗号化せずに脅迫を行うサイバー攻撃の手口のこと。
- 警察庁において、初めてノーウェアランサムによる国内の被害報告が確認された。
- ノーウェアランサムの感染対策として、ランサムウェアと同様の対策が必要である。

ノーウェアランサムとは

警察庁は 2023 年 9 月 21 日、『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』(以下、「本資料」と略記)を公表しました(*1)。本資料はサイバー空間の脅威の情勢を示す指標、事例を示すとともに、サイバー空間における安全・安心の確保に向けた警察の主な施策等を取りまとめたものとなっていますが、なかでも特に注目したい用語として「ノーウェアランサム」について言及されています。

「ノーウェアランサム」とは、ランサムウェアによってデータを暗号化することなくデータを窃取し、それを公開しない対価として企業・団体等に身代金を要求するサイバー攻撃の手口のことをいいます。現在、警察庁において確認されているランサムウェアの被害で最も多い手口は「二重恐喝(ダブルエクストーション)」となっていますが、この手口では攻撃者は暗号化したデータの復号を対価として身代金を要求するだけでなく、身代金が支払われない場合には窃取したデータを公開すると脅迫します。一方、ノーウェアランサムではデータを暗号化する手順が省かれており、窃取したデータによる脅迫のみが行われます。

警察庁では 2023 年上半期においてノーウェアランサムによる被害を国内で新たに 6 件確認しており、今後、従来のランサムウェアに代わり、ノーウェアランサムによる被害が拡大することが懸念されます。

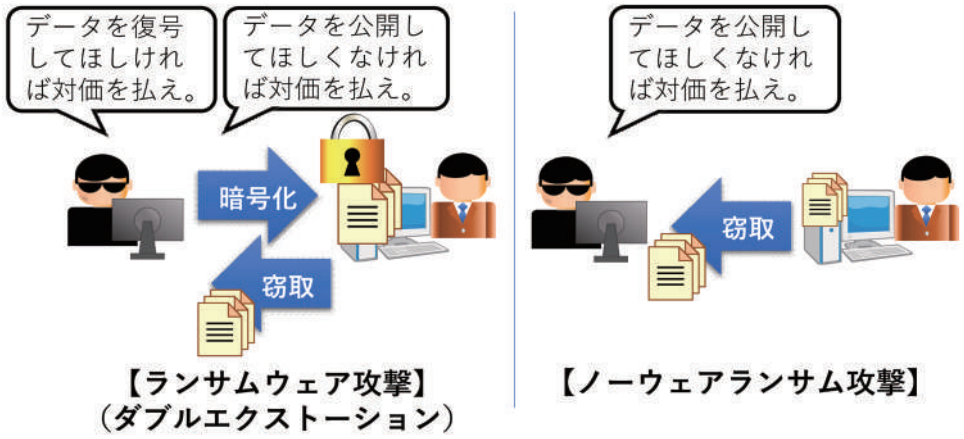


図:攻撃の流れ(左:ランサムウェア攻撃、右:ノーウェアランサム攻撃)
出典:本資料から転載

(*1) https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

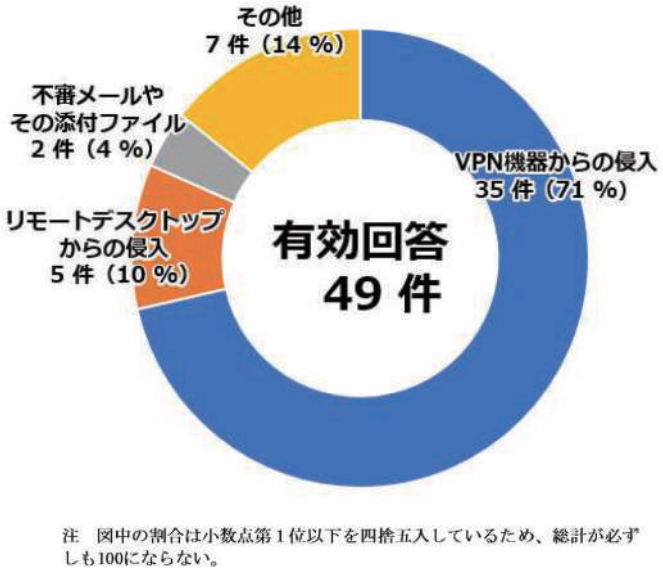
ノーウェアランサムが出現した背景

ノーウェアランサムが出現した背景の一つとして考えられることは、企業側のランサムウェアに対する対策の向上が挙げられます。独立行政法人情報処理推進機構（IPA）が毎年公表している「情報セキュリティ 10 大脅威(*1)」によれば、2021 年以降、組織における脅威として「ランサムウェアによる被害」が4年連続で 1 位にランクされるなど、近年、ランサムウェアの脅威は世界的に広く認識されるようになりました。これにともない、企業側の対策の強化が図られ、感染に備えてバックアップ体制が見直されるなど、以前のように暗号化したデータの復号を理由として、身代金が支払われることが少なくなりました。

攻撃者はデータを暗号化するために、ランサムウェアに対して管理者権限を奪取するなどの高度な機能を備えておく必要がありましたが、前述のとおりデータの復号を理由に身代金が支払われる可能性が低くなっていることから、暗号化の手間を省き、窃取したデータを公開しないことのみを理由に身代金を要求する手口に変更したと考えられます。

どのような対策が必要か？

ノーウェアランサムと従来のランサムウェアとの違いはデータを暗号化するか否かが異なるだけで、基本的には従来のランサムウェアと同じ経路で感染するものと考えられます。本資料によると、2023 年上半期にランサムウェアの被害報告を受けた企業・団体等における感染経路の割合は下図のとおりとなっており、特に VPN 機器やリモートデスクトップからの侵入が多いことがわかります。そのため、対策としてはこれら外部から接続可能な装置への脆弱性対策が重要です。



注　図中の割合は小数点第 1 位以下を四捨五入しているため、総計が必ずしも100にならない。

図：ランサムウェアの感染経路

出典：本資料から転載

示唆

サイバー攻撃の手口は時代に合わせて変化し続けていますが、攻撃の起点となる感染経路には以前から大きな変化は見られません。そのため、組織で保有する IT 資産を適切に管理し、継続的に組織内の IT 環境が脆弱なまま放置されないようにするなど、基本的なセキュリティ対策を徹底することが、ノーウェアランサムを含め、今後新たなサイバー攻撃の被害を防止する上で大切であるといえるでしょう。

(*1) https://www.ipa.go.jp/security/10threats/index.html

2. 短縮URL サービスおよびQR コード利用時のインシデント事例

要約

- 国内の複数の企業や大学で、QR コードを通じて意図していない広告サイトに誘導される問題が発生しており、注意が必要である。
- これは短縮 URL サービスを利用した QR コードの問題。
- 短縮 URL サービスの利用は簡単で便利ですが、安全性に問題があるため推奨されない。

インシデントの概要

某自動車関連企業が送信した会員向けダイレクトメールに含まれる QR コードから、予期しない広告サイトに誘導される事例が発生しました。一部の顧客は、カード番号などの決済情報の入力を求められたと報告されています。この問題について、当該企業は 11 月 13 日に、QR コードの読み取りを行わないように呼びかけています (*1)。また、国内の複数の企業や大学でも類似の事例が報告されており、QR コードの取り扱いに注意が必要です。

問題があった QR コードは、短縮 URL(URL Redirection Service)と組み合わせて利用されていたことがわかっています。QR コードは情報をコンパクトにエンコードするための二次元バーコードです。一方、短縮 URL は、長い URL を短くするためのサービスであり、「転送電話」のように短縮 URL サービスの運営者が転送サービスを提供しています。短縮 URL サービスは、長い URL を短く簡潔にし、文字数を節約し、視覚的にも見やすくします。また、ソーシャルメディアやメッセージングアプリで URL を共有する際に便利です。広告キャンペーンやマーケティング活動によく利用され、キャンペーンのトラッキングやクリック数の分析(*2)にも役立ちます。

当該事象では、短縮 URL から元の URL にリダイレクト(*3)するまでの数秒間、スマートフォンの画面下部に広告が表示されていたようです。この広告枠では、利用者を誤認させる表示が行われ、誤ってタップすると悪意のあるサイトに誘導される場合があることが確認されています。某自動車関連企業が利用していた短縮 URL サービス運営者に悪意があったのではなく、当該短縮 URL サービス運営者は悪意ある広告を意図せず利用させられていました。

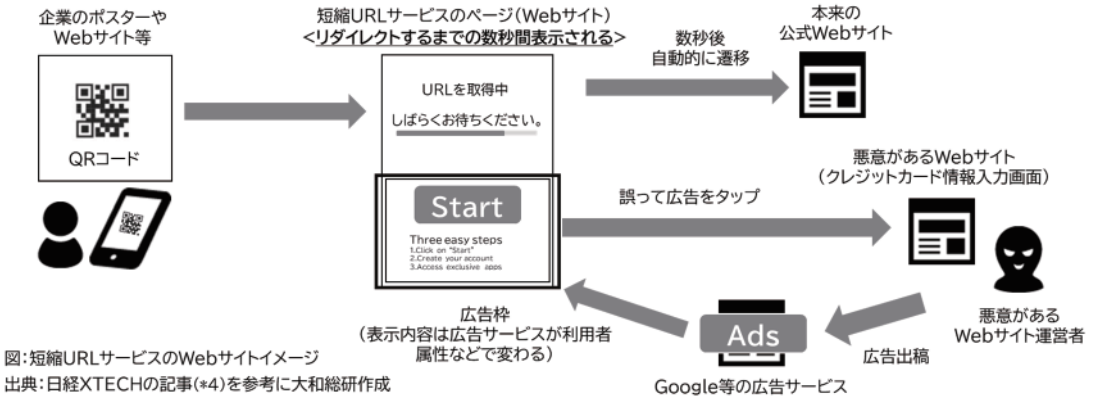


図:短縮URLサービスのWebサイトイメージ
出典:日経XTECHの記事(*4)を参考に大和総研作成

(*1) https://www.autobacs.com/notice/notice20231113.pdf

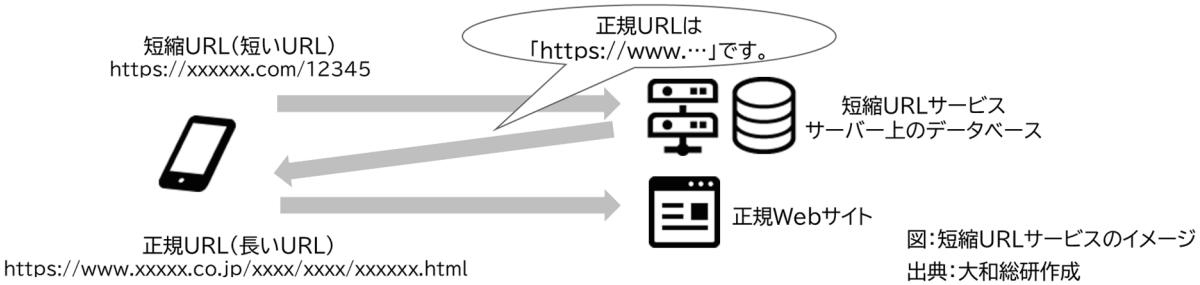
(*2) リダイレクト処理を担う短縮 URL サービス側のページ(Web サイト)に計測タグを組み込むことで実現されます。具体的には、クリック数やリファラ情報(ユーザーがどのサイトやアプリからリンクをクリックして現在のページにアクセスしたか)、ユーザーエージェント情報(デバイスやブラウザの種類)などが計測タグにより取得されます。

(*3) リダイレクトは、Web サイトやアプリケーションでよく使われる機能です。たとえば、特定の Web ページにアクセスしようとしたとき、そのページが移動したり存在しなかったりする場合、リダイレクトは別のページに自動的に転送します。

(*4) 日経 XTECH「公式 QR コードからなぜか不正サイトに移動、原因は短縮 URL 利用時の悪意広告」
(https://xtech.nikkei.com/atcl/nxt/column/18/01157/122600101/)

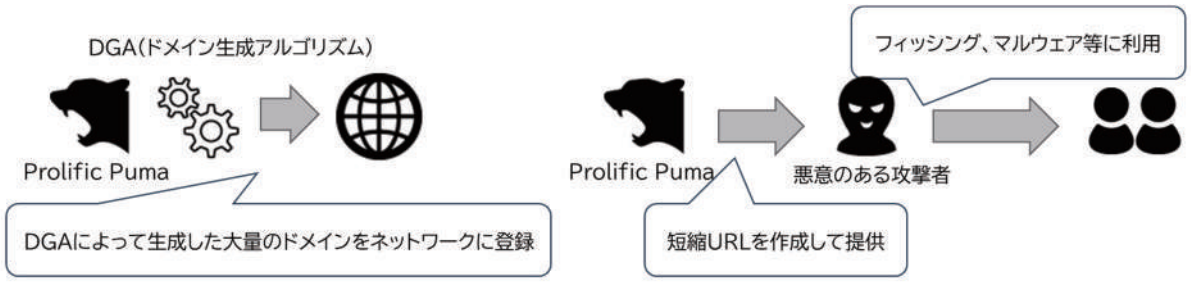
悪意のある短縮 URL サービス

短縮 URL の仕組みは、短縮 URL サービスのサーバーに、元の URL（正規 URL）と短縮 URL を紐づけて保存しておき、短縮 URL にアクセスすると正規 URL にリダイレクトされるというものです。つまり、短縮 URL サービスの運営者に悪意がある場合、短縮 URL が広まった後に紐づけたリダイレクト先を変更すれば悪意あるサイトに誘導できるということです。



図：短縮URLサービスのイメージ
出典：大和総研作成

前述の事例で使用されたサービスとは異なりますが、悪意のある短縮 URL サービスの提供元として Prolific Puma の存在が確認されています(*1)。Prolific Puma は、犯罪者向けに短縮 URL サービスを提供している犯罪グループです。運用にはドメイン生成アルゴリズム（DGA）(*2)が使用されており、3 万 5,000～7 万 5,000 のドメイン名が登録されているといわれています。Prolific Puma はこれらのドメインを使用して他の悪意のある攻撃者向けの短縮 URL を生成し攻撃者に提供し、攻撃者は、フィッシング、詐欺、マルウェアを配布する際の検出を回避するために使用します。



図：サイバー犯罪サプライチェーンにおけるProlific Pumaの役割
出典：大和総研作成

本件からの示唆

当該企業は、事前に動作確認済みと説明しており、本来の Web サイトが表示されたと述べています。しかし、QR コードからアクセスすると短縮 URL サービスのページが経由され、そのページに利用者が誤認するような広告が表示されることに気づいていませんでした。QR コードの利用に関しての注意点は本冊子前号(*3)でも触れていますが、利用者は当該企業が提供した URL や QR コードであれば信頼して、警戒することなく利用する傾向にあるため、利用者側だけで対策を取ることは困難です。

短縮 URL サービスは、サービスが停止すると本来の URL に正常にリダイレクトできなくなり、リンク先が無効となってしまう恐れもあるため、利用は推奨されません。システム開発に長けている組織であれば短縮 URL サービスと同様の効果を持つ仕組みを自組織で作成できるかもしれませんが、システムに疎い組織ではそのような方法は難しいでしょう。もし、自組織において短縮 URL サービスを利用している場合や意図せず利用していた場合は、対象となる利用者において不正広告による影響を受けている恐れはないか、短縮 URL サービス運営元の利用規約や注意事項をよく読んで、信頼できるか、問題が起きた際に対応してもらえるか、短縮 URL サービス利用によるリスク(*4)が受け入れ可能かどうか、再度点検することが推奨されます。

(*1) PROLIFIC PUMA: SHADOWY LINK SHORTENING SERVICE ENABLES CYBERCRIME
(https://blogs.infoblox.com/cyber-threat-intelligence/prolific-puma-shadowy-link-shortening-service-enables-cybercrime/)

(*2) 文字列をランダムに組み合わせて、多数の新しいドメイン名を生成するプログラム。

(*3) DIR SOC Quarterly vol.6 2023 autumn［第2部 2.］
(https://www.dir.co.jp/publicity/publication/socquarterly2310.html)

(*4) 指定先 URL が全く別の URL に置き換えられる可能性、サービスが停止されたときにリンク URL が無効になるなど。

1. CVSS の歴史と最新版（v4.0）での改善点

要約

- 国際的な脆弱性評価の指標である CVSS の最新版（v4.0）がリリースされた。CVSS の歴史、これまでの課題と、最新版における変更点について解説する。

CVSS v4.0 の発表

米国の非営利団体である FIRST（Forum of Incident Response and Security Teams）(*1)は、2023 年 11 月 1 日、CVSS（Common Vulnerability Scoring System）の最新版である v4.0 を正式発表しました(*2)。本記事では、CVSS、および、今回発表された CVSS v4.0 について解説します。

CVSS とは

CVSS（共通脆弱性評価システム）は、脆弱性の深刻度を数値化し、それに基づいて対策や優先づけを行うために使用される、国際的な指標です。CVSS は、脆弱性の影響度、攻撃の容易さ、攻撃の範囲などの要素を考慮して、ベンダーに依存しない中立的な基準でスコアを算出します。スコアは 0～10.0 の範囲で数値化され、高いスコアほど脆弱性の深刻度が高いことを示し、これにより客観的に評価することが可能となります。CVSS はセキュリティ専門家や組織にとって重要な指標であり、セキュリティの脆弱性を効果的に管理するために活用されています。

CVSS の歴史

CVSS の歴史は古く、2005 年 2 月に CVSS v1 がリリースされました。その後、2007 年 6 月に CVSS v2、2015 年 6 月に CVSS v3.0 がリリースされ、2019 年 6 月に v3.1 がリリースされました。現在では CVSS v1 は使われておりません。

CVSS v2 と CVSS v3 では、評価する要素や基準が異なるため、同じ脆弱性を評価した場合でもスコアが異なります。CVSS v3.1 は CVSS v3.0 から新しい指標は加えられておりませんが、既存の基準や計算式などが改善されており、現時点では CVSS v3.1 が幅広く使われています。

なお、CVSS v3.0 が使われるケースや、CVSS v2 が併記されているケースも見受けられます。以降では、CVSS v3.1 と、今回正式発表された CVSS v4.0 の変更点を中心に解説します。

CVSS v3.1 について

CVSS v3.1 は、基本評価基準（Base Metrics）、現状評価基準（Temporal Metrics）、環境評価基準（Environmental Metrics）の 3 つの基準で評価しスコアを算出します。

基本評価基準は、当該脆弱性について以下 8 つの要素の各評価結果に重みづけを行い、それらを統合して基本スコア（Base Score）を算出します。基本スコアは、当該脆弱性の基本特性を示すもので、時間経過やシステムの稼働状況により変化しません。

(*1) 1990 年に米国 CERT/CC などが中心となり世界中の CSIRT における相互の情報交換やインシデント対応に関する協力関係の構築を目的として設立された国際的なフォーラムです。

(*2) FIRST『Common Vulnerability Scoring System version 4.0: Specification Document』
(https://www.first.org/cvss/v4.0/specification-document)

項番	要素	意味	基準値
1	攻撃元区分 （AV：Attack Vector）	どこから攻撃可能であるか （インターネット経由などで攻撃可能か）	N：ネットワーク A：隣接 L：ローカル P：物理
2	攻撃条件の複雑さ （AC：Attack Complexity）	攻撃する際に必要な条件の複雑さ （攻撃を成立させるために設定情報などが必要か）	L：低 H：高
3	必要な特権レベル （PR：Privileges Required）	攻撃する際に必要な特権レベル （攻撃時に管理者権限などが必要か）	N：不要 L：低 H：高
4	ユーザー関与レベル （UI：User Interaction）	攻撃する際に必要なユーザー関与レベル （ユーザーによるリンクのクリック、ファイル閲覧、設定変更などが必要か）	N：不要 R：要
5	スコープ （S：Scope）	攻撃による影響範囲 （攻撃の影響範囲がコンポーネントの帰属する範囲にとどまるか）	U：変更なし C：変更あり
6	機密性への影響 （C：Confidentiality Impact）	攻撃による機密性への影響 （情報が漏えいする可能性）	H：高 L：低 N：影響なし
7	完全性への影響 （I：Integrity Impact）	攻撃による完全性への影響 （情報が改ざんされる可能性）	H：高 L：低 N：影響なし
8	可用性への影響 （A：Availability Impact）	攻撃による可用性への影響 （業務が遅延・停止する可能性）	H：高 L：低 N：影響なし

表：基本評価基準項目
出典：IPA『共通脆弱性評価システム CVSS v3 概説』(*1)を基に大和総研作成

現状評価基準は、以下の 3 つの要素で構成され、基本評価基準と併用して現状スコア（Temporal Score）を算出します。

現状スコアは、脆弱性への対応状況に応じ、時間経過とともに変化します。

項番	要素	意味	基準値
1	攻撃される可能性 （E：Exploit Code Maturity）	攻撃コードや攻撃手法が実際に利用可能であるか	X：未評価 H：容易に攻撃可能 F：攻撃可能 P：実証可能 U：未実証
2	利用可能な対策のレベル （RL：Remediation Level）	脆弱性の対策がどの程度利用可能であるか	X：未評価 U：なし W：非公式 T：暫定 O：正式
3	脆弱性情報の信頼性 （RC：Report Confidence）	脆弱性に関する情報の信頼性	X：未評価 C：確認済 R：未確証 U：未確認

表：現状評価基準項目
出典：IPA『共通脆弱性評価システム CVSS v3 概説』を基に大和総研作成

環境評価基準は、以下の 2 つの要素で構成され、基本評価基準および現状評価基準と併用して環境スコア（Environmental Score）を算出します。

環境スコアは、ユーザーがシステムやソフトウェアを利用する環境の状況が加味されるため、脆弱性に対して想定される脅威に応じ、ユーザーごとに変化します。

(*1) IPA『共通脆弱性評価システム CVSS v3 概説』(https://www.ipa.go.jp/security/vuln/scap/cvssv3.html)

項番	要素	意味	基準値
1	対象システムのセキュリティ要求度（Security Requirements）	利用環境にて要求されるセキュリティ特性を、機密性(C)、完全性(I)、可用性(A) について重視する項目 ※各項目の末尾に R(Requirements)をつけ、CR、IR、AR と表現	X:未評価 H:高 M:中 L:低
2	環境条件を加味した基本評価の再評価(Modified Base Metrics)	基本評価基準の項目を緩和策や対策後の利用環境に対して再評価 ※各項目の頭に M(Modified)をつけ、MAV、MAC、MPR、MUI、MS、MC、MI、MA と表現	基本評価基準参照

表:環境評価基準項目
出典:IPA『共通脆弱性評価システム CVSS v3 概説』を基に大和総研作成

CVSS v3.1 の課題

CVSS v3.1 に対する課題については、FIRST が 2023 年 6 月に以下のように公開しました。

項番	CVSS v3.1 の課題
1	基本スコアがリスク分析への主要な入力として利用されている
2	リアルタイムの脅威と補足的な影響の詳細が十分に表現されていない
3	IT システムにしか適用できない
4	健康、人的安全、産業用制御システムについてはあまり適さない
5	ベンダーが公開するスコアは、「High」または「Critical」（スコア 7.0 以上）が多い
6	脆弱性を表現する粒度が不十分
7	現状評価基準が CVSS スコアに効果的に影響を与えていない
8	CVSS スコアの計算が複雑すぎて直観的に理解できない

表:CVSS v3.1 の課題
出典:FIRST 公開資料(*1)を基に大和総研作成

CVSS v4.0 の変更点

前述の CVSS v3.1 の課題に対処するため、CVSS v4.0 では以下のような変更が加えられました。

項番	CVSS v4.0 の変更点
1	基本評価基準の粒度の細分化 ● 「攻撃の実行条件(AT:Attack Requirements)」の追加 AT は当該脆弱性に対して攻撃を成立させるための実行条件について評価します。本要素は従来の「攻撃条件の複雑さ(AC:Attack Complexity)」と併せることで脆弱性の特性をより精密に表現することができます。 ● 「ユーザー関与レベル(UI:User Interaction)」の改善 UI の基準値が「N(不要)、R(要)」から「N(不要)、P(パッシブ)、A(アクティブ)」に変更されました。粒度が細かくなることで脆弱性の特性をより精密に表現することができます。
2	下流のスコアリングの曖昧さの削除(「スコープ」の廃止) ● 「スコープ(S:Scope)」の廃止 FIRST は「スコープ」について、「おそらく最も嫌われ、最も理解されていない CVSS メトリック」と表現(*2)しており、CVSS v4.0 では「スコープ」が廃止され、「脆弱なシステムの機密性(VC)・完全性(VI)・可用性(VA)」、「後続システムの機密性(SC)・完全性(SI)・可用性(SA)」が新たに導入されました。脆弱性の後続システムへの影響についてより厳密に評価できるようになります。

(*1) FIRST『Announcing CVSS v4.0 (Challenges and Critique of CVSS 3.1 (p.8))』
(https://www.first.org/cvss/v4-0/cvss-v40-presentation.pdf)

(*2) FIRST『Announcing CVSS v4.0 (Retired Base Metric: Scope (p.14))』
(https://www.first.org/cvss/v4-0/cvss-v40-presentation.pdf)

3	脅威メトリックの簡素化とスコアリングの影響の改善 ● (1)「現状評価基準」を「脅威評価基準」に名称変更 (2)「利用可能な対策のレベル(RL:Remediation Level)」と「脆弱性情報の信頼性(RC:Report Confidence)」を廃止 (3)「攻撃される可能性(E:Exploit Code Maturity)」を、「攻撃の成熟度(E:Exploit Maturity)」に名称変更 「脅威評価基準」は、CVSS v3.1 の「現状評価基準」と比較して、攻撃の成熟度にフォーカスし、簡素化されているため幅広く活用されるものと期待されます。
4	脆弱性対応のための補足評価基準の追加 ● 「補足評価基準(Supplemental Metrics)」の新設 「補足評価基準」が新設され、「安全性(S:Safety)、自動化可能性(AU:Automatable)、供給者による緊急度(U:Provider Urgency)、回復可能性(R:Recovery)、価値密度(V:Value Density)、対応の困難度(RE:Vulnerability Response Effort)」の 6 つの基準値が追加されました。補助評価基準に係る情報はベンダー側から任意で提供されます。なお、本基準値は CVSS 算出に使用されず、最終的な CVSS スコアに影響は与えません。
5	OT/ICS/IoT への適用可能化 ● 「環境評価基準」と「補足評価基準」で「安全性(S:Safety)」の基準値を追加 CVSS v3.1 では、IT システムを対象とするため、脆弱性が悪用された場合の人体への影響などを評価できませんでした。「安全性」は、IEC61508 に定義されているカテゴリに基づき脆弱性の影響を評価することができ、OT/ICS/IoT 環境が正式に評価対象に加えられたことになります。

表:CVSS v4.0 の変更点
出典:FIRST 公開資料(*1)を基に大和総研作成

また、上記の他に、CVSS v3.1 の「基本スコア」、「現状スコア」、「環境スコア」について、CVSS v4.0 では、基本評価基準(B)、脅威評価基準(T)、環境評価基準(E)、の組み合わせをスコア名に入れ、「CVSS-B、CVSS-BT、CVSS-BE、CVSS-BTE」と表記することになりました。CVSS のスコアがどの評価基準を使って算出されたのかが一目でわかることとなりわかりやすくなりました。

加えて、CVSS スコア計算が直観に反するといった課題に対応するため、AV などの基準値から重要度に応じた同値類(EQ:Equivalence class)をまとめ、EQ のスコアから CVSS スコアを決定するようになりました。詳細については、FIRST 公開資料(*2)をご参照ください。

最後に

CVSS v4.0 で多くの改善と新機能が提供されました。今後 CVSS v4.0 で脆弱性情報を提供するベンダーなども増えてくると考えられ、セキュリティ関係者の方は CVSS v4.0 を読み解けるようご確認をお勧めします。

(*1) FIRST『Announcing CVSS v4.0 (Overview of What's New in CVSS v4.0 (p.10))』
(https://www.first.org/cvss/v4-0/cvss-v40-presentation.pdf)

(*2) FIRST『Common Vulnerability Scoring System version 4.0: Specification Document "8.CVSS v4.0 Scoring"』(https://www.first.org/cvss/v4.0/specification-document#CVSS-v4-0-Scoring)

2. 多要素認証が破られる ―AiTM 攻撃とは

要約

- AiTM (Advisory-in-the-Middle) 攻撃によってセッションクッキーを窃取する事例が発生している。
- 攻撃者がセッションクッキーを窃取できると多要素認証が有効だったとしても認証を通過できる。
- 対策として FIDO2 準拠の認証や証明書ベースの認証の利用が推奨される。

Advisory-in-the-Middle 攻撃

AiTM 攻撃とは、攻撃者はある正規のサイトに成り済まして攻撃対象と通信し、当該サイトとは攻撃対象に成り済まして通信することでセッションクッキー(後述)を窃取する攻撃です。セッションクッキーが攻撃者に窃取されたあるいは偽造された場合、その攻撃者は認証することなくそのクライアントに成り済ますことができます(*1)。この認証には多くのサイトで用いられる多要素認証も含まれます。

Microsoft が観測した AiTM 攻撃(*2)は次のような流れで行われました:

1. 攻撃対象に対して HTML ファイルを添付したメールを送信する。
2. HTML ファイルを開くと正規のサイトを模したフィッシングサイトへ転送される。
3. 攻撃対象がフィッシングサイトへ資格情報を入力し、それを攻撃者が正規のサイトへ入力する。
4. 認証が成功した場合、正規のページへ転送する。それを攻撃者は傍受し、攻撃者も認証を受ける。
5. 攻撃者は更なる攻撃(本件ではビジネスメール詐欺)を行う。

以下、具体的に紹介します。

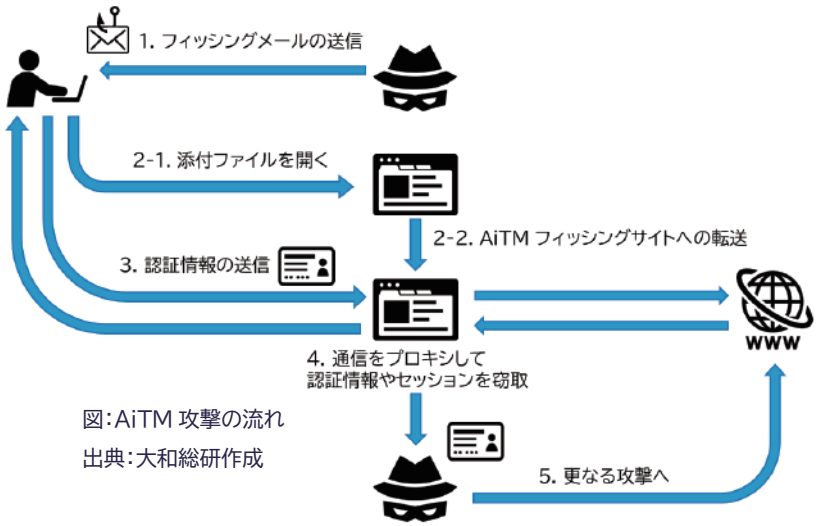


図:AiTM 攻撃の流れ
出典:大和総研作成

まず、添付された HTML ファイルは開かれると攻撃対象をリダイレクトサイトへ転送します。このリダイレクトサイトは攻撃対象が添付された HTML ファイルから来ているかどうかを確認します。具体的には、URL にフラグメント値(*3)があるかどうかを確認します。今回の場合、このフラグメント値はメールアドレスを Base64 方式で変換した文字列になります。

もしフラグメント値が存在すれば、フィッシングサイトのランディングページ、即ち、偽のサインインページの URL に結合します。これにより、偽のサインインページは自動的に攻撃対象のメールアドレスを入力することができます。この自動入力は正規のサインインページと思わせることに役立ち、加えて、その結合はアンチフィッシングソリューションが直接フィッシングサイトへアクセスすることを防ぐ試みでもあります。

(*1) このような攻撃手法は一般に Pass-the-Cookie 攻撃と呼ばれます。

(*2) https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

(*3) “example.com#test”のような URL の末尾についている#以降の値のこと。

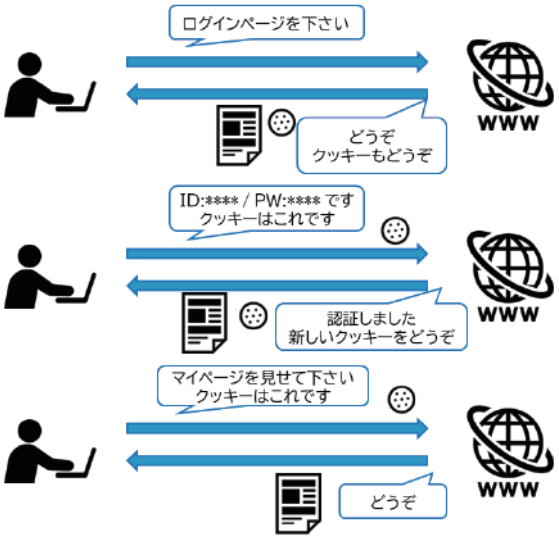
このフィッシングサイトはある中間者攻撃フレームワークを使用し、通常は login.microsoftonline.com となる組織の Azure Active Directory（Azure AD、現 Microsoft Entra）のサインインページをプロキシ(*1)します。攻撃対象が資格情報を入力して認証されると正規の office.com に転送されます。しかし、攻撃者はその資格情報やセッションクッキーを傍受しているので、攻撃者も認証を受けることができます。そして、攻撃者は組織内から様々な攻撃を行うことができるようになります。

セッションクッキーとは？

まず、通信技術におけるセッションとは開始から終了までを指す単語です。Web ページへのアクセスを例にすれば、Web サーバーにリクエストを送ってからレスポンスが返ってくるまでの一往復の対話をセッションとしてみることができます。この見方では、同一のクライアントと同一の Web サーバーとの間で複数回の対話があったとき、それぞれ別のセッションと見做されることになります。特に、Web サーバーから見るとクライアントが同一かどうかはわかりません。これを解決する方法としてはそれらの一連の対話が同一のセッションであると見做されるようにすればよく、それを実現する技術がセッションクッキーとなります。

クッキー（Cookie）とは、Web サーバーがクライアントに対して送付する文字列です。クライアントは所定の期限まで保管し、Web サーバーへリクエストを送る際に対応するクッキーを当該サーバーへ提示します。Web サーバー側は提示されたクッキーに応じて様々な処理が可能となります。その用途に応じてセッションクッキーやファーストパーティクッキー、トラッキングクッキー（サードパーティクッキー）といった名前で呼ばれます。そのうち、セッションクッキーはセッションを識別する用途で使われるクッキーです(*2)。

会員制の Web サイトの例でどのように機能するかを見てみましょう。まず、Web サーバーはページをクライアントへレスポンスする際に、最初にサイトに訪れた場合はセッションクッキーも送付します(*3)。ここでは最初にログインページへ訪れたとしましょう。クライアントはログインを試行する際に、認証情報と共にセッションクッキーを提示します。Web サーバー側はこのクライアントが先ほどログインページをレスポンスしたクライアントと同一であることがわかり、セッションクッキーを再発行(*4)してセッションクッキーをユーザーID 等と結び付けておきます。クライアントはページにアクセスする度にセッションクッキーを提示することで Web サーバー側はどのユーザーがアクセスしているかがわかるようになります。ログイン後の対話はセッションクッキーによって結び付けられているので、まとめて一つのセッションと見做すことができます。



図：セッションクッキーの使い方
出典：大和総研作成

フィッシングに耐性のある認証方式

AiTM 攻撃によって多要素認証を回避できます。だからといって多要素認証を放棄して別の認証方式に変える必要はありません。むしろ、多要素認証が重要であるからこそ、多要素認証を回避しようとする AiTM 攻撃が出現したといえます。従って、多要素認証の実装をフィッシングに対してより耐性のあるものにする方がよいでしょう。そのような実装として、Microsoft は以下の 2 つを挙げました(*5)：

- 証明書ベースの認証
- FIDO2 に準拠した認証

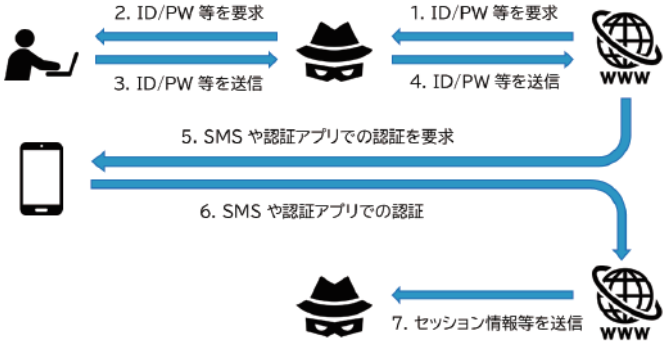
以下では、この 2 つの認証方式が何故有効なのかについて述べます。

(*1) クライアントの代わりにサーバーへアクセスすること。
(*2) セッションの内容は Web サーバー側で管理され、それに対応したセッション ID をクッキーとして使用します。
(*3) ログイン前のセッションを管理する必要がないサイトではセッションクッキーを発行しないこともあります。
(*4) ログイン前とログイン後で同一のセッション ID を使用するのはセキュリティ上の問題があるので再発行します。
(*5) 認証方式ではありませんが、条件付きアクセスポリシーによって多要素認証を補完できるとも述べています。

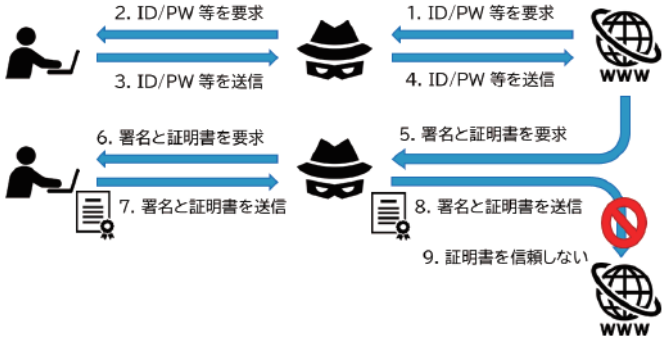
まず、証明書ベースの認証とは、認証の度にクライアントがサーバーに対して署名と証明書を提示する方式です。サーバーは提示された署名と証明書を検証し、成功した場合に認証します。証明書の規格として一般的とされる X.509(*1)に基づいている場合、証明書には主に署名アルゴリズムや発行者の名前、主体者(*2)の名前、公開鍵の情報等が記載されます。

次に、FIDO2 に準拠した認証とは、サーバーに対して事前に公開鍵を登録しておき、認証の度にクライアントが当該サーバーに対応する秘密鍵で署名を生成して提示する方式です。サーバーはログインを試行するユーザーに紐づいた公開鍵を使用して提示された署名を検証し、成功した場合に認証します。詳細は DIR SOC Quarterly vol.5 2023 summer(*3)の『パスワード不要の新しい認証方式「パスキー」』でも取り扱っています。

まず重要な点として、多要素認証がフィッシングサイトを経由するかどうかが挙げられます。たとえば、SMS や認証アプリを使用する場合、正規のサイトは「攻撃者を経由せず直接」攻撃対象へ認証を要求します。そのため、攻撃対象が認証に成功してしまうと、正規のサイトは攻撃対象に成り済ました攻撃者を攻撃対象と判断してしまいます。即ち、正規のサイトは攻撃者にセッションクッキーを渡してしまいます。



一方で、証明書ベースの認証の場合、正規のサイトは対話をしている攻撃者に対して署名と証明書を要求します。攻撃者が自身の署名と証明書を提出した場合、サーバーは攻撃者の証明書を信頼しないので認証に失敗します。一方で、攻撃者が攻撃対象の署名と証明書を使用した場合、証明書の主体者は攻撃対象であって攻撃者ではないので、サーバーは証明書を信頼しません。従って、いずれの場合も認証に失敗します。



また、FIDO2 に準拠した認証の場合も同様に正規のサイトは攻撃者に対して署名を要求します。攻撃者が攻撃対象の署名を偽造することは困難なため、攻撃対象に署名を要求します。しかし、攻撃対象から見るとフィッシングサイトと正規のサイトのドメインが一致しないため、攻撃者に署名を渡すことはありません。従って、認証に失敗します。

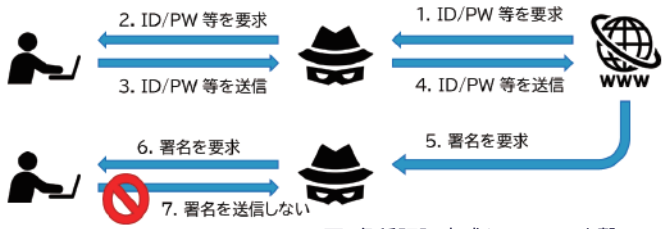


図:各種認証方式と AiTM 攻撃
出典:大和総研作成

示唆

証明書ベースの認証は昔から使われているため信頼できる技術であり、証明書を発行することで容易にアクセス権限を付与できる拡張性もあります。一方で、一度きりではあるものの構築のコストは低くなく、証明書の発行・更新・失効といった継続的な管理や運用のコストが必要になります。従って小規模な組織には向かないでしょう。これに対し、FIDO2 準拠の認証はモダンな技術であり発展性に期待できますが、過去の記事でも扱っているように、こちらも利便性とセキュリティの間にトレードオフの関係があります。用途や規模を勘案して証明書ベースの認証や FIDO2 準拠の認証、あるいは他のフィッシングに耐性がある認証方式の利用を検討するとよいでしょう。

(*1) RFC 5280 でその仕様が定められています。

(*2) 鍵の所有者のこと。

(*3) DIR SOC Quarterly vol.5 2023 summer [第 3 部 2.]
(https://www.dir.co.jp/publicity/publication/socquarterly2307.html)

3. テクニカルトピックスSSH の秘密鍵が解析される可能性

要約

- RSA 署名を生成する際に計算の誤りが発生すると秘密鍵が復元し得る。
- 誤った署名を含む通信を観測することで SSH の秘密鍵を復元できる可能性が指摘されていた。
- 実証実験によって実際にいくつかの SSH の秘密鍵が復元された。

RSA 署名と先行研究

RSA 署名とは RSA 暗号を用いたデジタル署名です。RSA 暗号による暗号化は次のような手順で行われます:

1. 十分大きな素数 p, q を生成し、N をそれらの積とする。
2. λ を $(p-1)(q-1)$ とし、e を λ と素な正の整数とする。このとき、e と N が公開鍵となる。
3. $ed \equiv 1 \bmod \lambda$ となる d を計算する。この d が秘密鍵となる。
4. 平文である正の整数 m について、暗号文 c は $c \equiv m^e \bmod N$ なるものとして計算される(*1)。

Euler の定理より $m \equiv c^d \bmod N$ となることから、$c^d \bmod N$ を計算することで暗号文を復号することができます。特に、N を素因数分解できると秘密鍵を復元できます。即ち、任意の暗号文を復号できます。

ここで、e と d の役割を入れ替えることで平文からデジタル署名を生成することができます。しかし、より高速に計算するために、実際は次のようにして署名を生成します(*2):

1. d_p を $d_p \equiv d \bmod (p-1)$ なるものとする。同様に、d_q を $d_q \equiv d \bmod (q-1)$ なるものとする。
2. s_p を $s_p \equiv m^{d_p} \bmod p$ なるものとする。同様に、s_q を $s_q \equiv m^{d_q} \bmod q$ なるものとする。
3. デジタル署名 s は $s \equiv s_p \bmod p$ かつ $s \equiv s_q \bmod q$ となるものとして計算される(*3)。

RSA 暗号と同様に、N を素因数分解できると署名の偽造が可能となります。

RSA 暗号・RSA 署名は歴史が長いこともあり、様々な攻撃が考えられています。署名生成時の計算に誤りがある場合に着目した研究として有名な Lenstra (1996)(*4)では、署名されたメッセージと誤った署名を知っている場合に N の素因数分解が可能となることが示されました。

更に、Boneh, DeMillo, and Lipton (2001)(*5)では、s_p と s_q のいずれか一方の計算に誤りがある場合に正しい署名を知っていると素因数分解が可能となることが示されました。つまり、署名を行うハードウェアに対して計算の誤りを誘発する攻撃をすることで秘密鍵を復元することが可能です。実際に、Weissman et al. (2020)(*6)ではロウハンマー(*7)を利用してこの攻撃が実証されました。

(*1) 実際は選択暗号文攻撃への耐性を付けるために平文にパディングを施します。

(*2) RFC 8017, Section 5.2.に記載されています。

(*3) そのような s の存在と一意性は中国剰余定理にから示されます。また、この高速化のテクニックを CRT-RSA といいます。

(*4) https://infoscience.epfl.ch/record/164524

(*5) https://link.springer.com/article/10.1007/s001450010016

(*6) https://tches.iacr.org/index.php/TCHES/article/view/8587

(*7) DRAM 内でメモリセルから電荷が漏れだすことで指定していないアドレスの内容が変化してしまう現象のこと。

TLS と SSH に対する攻撃

リモートサーバーで自然発生するフォールトから無効な署名が生成されることがあり、Weimer (2015)(*1)ではネットワークホストをスキャンして無効な署名に対して Lenstra (1996)の攻撃を適用することで TLS の秘密鍵を復元できました。なお、この攻撃は TLS のバージョンが 1.2 およびそれ以下ではサーバーの RSA 署名が検証に必要なハンドシェイク値と共に平文で送信されるという事実を利用しています。現在の TLS 1.3 では Diffie-Hellman の鍵交換後に発生するハンドシェイクメッセージが暗号化されているため、受動的な攻撃者はサーバー証明書やハンドシェイク署名を入手できません。従って、TLS 1.3 に対しては自らサーバーに接続して署名を収集する必要があります。

重要な点として、Lenstra (1996)の攻撃を実行するためには署名されたメッセージを知っている必要があります。これを克服するため、Coron et al. (2009)(*2)ではメッセージが部分的に未知である場合について研究されています。当該論文では ISO/IEC 9796-2 で指定されたメッセージのエンコーディングを考慮し、部分的に未知であるメッセージを二変数の一次式で表現しました。法 p で正しく計算されている場合、法 p では誤った署名の e 乗がエンコードされたメッセージと一致します。従って、法 p での二変数方程式を解くことで元の正しいメッセージを入手でき、Lenstra (1996)の攻撃手法へ帰着できます。この p は未知ですが、Herrman and May (2008)(*3)における Coppersmith ベースのテクニックによって当該二変数方程式を解くことができます。

特に、Coron et al. (2009)では PKCS#1 v1.5 パディングされたメッセージの場合は一変数となることが指摘され、パディングで使用するハッシュ関数の出力長が N の 4 分の 1 以下ならば無効な署名から秘密鍵を回復することが理論的に可能であると結論付けられました。当該論文中では実験が行われていなかったものの、Ryan, He, Sullivan, and Heninger (2023)(*4)において、SSH 通信の開始時に行う RSA 署名の生成時に計算の誤りが発生すると SSH の秘密鍵が復元し得ることが実証されました。

加えて、ハッシュ関数の出力長が論理的な境界である N の 4 分の 1 に近づくにつれて攻撃の実行時間が増大し、ハッシュ関数の出力長が N の 4 分の 1 より十分大きい場合はもはや現実的な時間では不可能であることが観察されました。更に、以下のいくつかの事象が観察されました：

- 収集したデータをホストごとに分類した結果、一部のホストは正常な署名を殆ど生成しなかった。
- RSA 署名から ECDSA に移行しつつある。
- RSA 署名で用いられる鍵長に関して、以前はあまり見られなかったが、2022 年以降 3072 ビットが使用されつつある。

当該論文中では、1 点目についてはそれらのホストには永続的なハードウェアの障害の可能性があることが指摘されています。また、2 点目については安全性というよりは単に楕円曲線暗号の人気が増しているからだろうと、3 点目については OpenSSH 8.0 からデフォルトの RSA 鍵のサイズが 2048 ビットから 3072 ビットに変更されたことが要因の一つだろうと推測されています。

対策

受動的な攻撃を検知することは困難です。しかし、この攻撃への対策は容易で、署名を送信する前に一度検証し、検証可能なら送信するように設定すれば問題ありません。一般的な SSH 実装である OpenSSH は OpenSSL を用いて署名を生成しており、OpenSSL はこの攻撃を含む様々な RSA フォールト攻撃への対策を既に実装しています。また、ハードウェアの障害によって恒常的に誤った署名を出力する可能性があるため、署名に用いているソフトウェアのバージョンだけではなく、デバイスの状態に気を使うことも重要でしょう。

(*1) https://www.redhat.com/en/blog/factoring-rsa-keys-tls-perfect-forward-secrecy

(*2) https://link.springer.com/chapter/10.1007/978-3-642-04138-9_31

(*3) https://link.springer.com/chapter/10.1007/978-3-540-89255-7_25

(*4) https://dl.acm.org/doi/10.1145/3576915.3616629

バックナンバーはこちら

DIR SOC Quarterly vol.3 2023 winter（2023 年 1 月 30 日発行）

- ビルシステムおよび工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインの公開
- 大阪急性期・総合医療センターにおけるセキュリティインシデント
- xSIRT

DIR SOC Quarterly vol.4 2023 spring（2023 年 4 月 7 日発行）

- 金融庁と業界団体との意見交換会の実施
- 警察庁による LockBit 暗号化済みデータの復元成功
- ChatGPT がサイバーセキュリティにもたらす影響

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

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

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

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

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

著者　大和総研
発行所　株式会社大和総研　フロンティア研究開発センター
印刷・製本　セキ株式会社

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

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

大和総研の用語解説サイト

WORLD

キーワードから、みえる、つながる、未来の日常（Life）

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

CONTENTS

キーワードから　旬のIT用語が一目でわかるトレンドワードクラウド

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

みえる　AI・データサイエンスなど5分野の用語を解説

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

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

つながる　IT技術とビジネスをつなぐ深掘り解説記事と、エンジニアブログ

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

大和総研の用語解説サイト
WORLD

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

大和総研
Daiwa Institute of Research