DIR SOC Quarterly

2023 summer vol.5

わが国の政策・法制度の動向

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

トピックス

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―

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います。今回は、2023 年度第 1 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。また第 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。

近年、国際的にインフラ事業に対してサイバー攻撃が行われた事案が多数発生していることから、インフラサービスの安定的な提供の確保は各国政府にとって喫緊の課題となっています。本号では、第 1 部で経済安全保障推進法に関連し、『基幹インフラ役務の安定的な提供の確保に関する制度』に関して政府が 2023 年 4 月 28 日に閣議決定した基本方針の概要やインフラ事業者に求められる対応などについてご紹介します。本制度は 2024 年 2 月までに施行される予定であるため、インフラ事業者だけでなく、その委託先を含む関係事業者は施行に備えて準備を進める必要があります。

日本でも被害が報道された SIM スワップ詐欺は、多要素認証の信頼性が揺らぎかねない深刻な問題です。この対策の 1 つとなりうるパスキーはパスワードが不要な認証技術であり、今後さらに注目が集まるであろうと推測されます。この詐欺の手口に関しては第 2 部で、パスキーの概要、メリット・課題などに関しては第 3 部でご紹介します。

また昨今、組織内に侵入したマルウェア（ウイルスやランサムウェアなどの悪意のあるソフトウェア）の拡散を防ぐための技術としてマイクロセグメンテーションが注目されています。マイクロセグメンテーションの概要や製品の特長、導入時並びに運用時の注意点などについて第 3 部で紹介していますので、ご参照ください。

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。

2023 年 7 月　株式会社大和総研執筆者一同

1. 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

概要

政府は 2023 年 4 月 28 日、経済安全保障推進法 (*1) における 4 つの経済施策の 1 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』（本制度）に関して、『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』（基本指針）を閣議決定し、公表しました (*2) 。

本制度は、近年、国際的にインフラ事業に対してサイバー攻撃が行われた事案が多数発生していることから、インフラサービスの安定的な提供を確保するため、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。基本指針では、事前届出が義務付けられる事業者の指定基準や設備等の範囲、事前届出事項、審査にあたっての考慮要素、審査の際に考慮される事業者によるリスク管理措置の例などが明らかにされました。

経済安全保障推進法の4つの経済施策	1. 重要物資の安定的な供給の確保
	2. 基幹インフラ役務の安定的な提供の確保 ⇒**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**
	3. 先端的な重要技術の開発支援
	4. 特許出願の非公開

表：基本指針の位置付け

出典：経済安全保障推進法の内容を基に大和総研作成

事業者に求められる対応とは？

本制度では、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、一定の基準 (*3) に該当する事業者が「特定社会基盤事業者」として、主務大臣によって指定 (*4) されます。

本制度で事前届出が義務付けられる場合、特定社会基盤事業者は審査で承認されるために、サイバー攻撃などによりインフラサービスの提供が阻害されないよう、リスク管理措置の実施が求められます。基本指針では、様々なリスク管理措置を具体的な措置の例とともに示しており、主なものは次のようになっています。

(*1) 経済安全保障推進法については、大和総研『DIR SOC Quarterly 2022 the first issue』
(https://www.dir.co.jp/publicity/publication/socquarterly2210.html) でも取り上げていますのでご参照ください。

(*2) https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin2.pdf

(*3) 基本指針では、基準として事業を行う者の事業規模と代替可能性が挙げられています。

(*4) 指定は 2023 年 11 月 17 日までの政令指定日以降に行われます。

リスク管理措置	具体的な措置の例
特定重要設備 (*1) 及び構成設備の供給者における製造等の過程で、特定重要設備及び構成設備に不正な変更が加えられることを防止するために必要な管理がなされ、当該管理がなされていることを特定社会基盤事業者が確認できることを契約等により担保している。	・調達時に指定した情報セキュリティ要件（特定重要設備及び構成設備に最新のセキュリティパッチが適用されているか否か、不正プログラム対策ソフトウェアを最新化しているか否か等）の実装状況が確認できる。 ・特定重要設備及び構成設備の製造環境において、アクセス可能な従業員を物理的（入退室管理等）かつ論理的（データやシステム等へのアクセス制御）に適切に制限していることが確認できる。
特定重要設備及び構成設備について、不正な妨害が行われる兆候を把握可能な体制がとられており、不正な妨害が加えられた場合であっても、冗長性が確保されているなど、役務の提供に支障を及ぼさない構成となっている。	・ランサムウェア等に感染した場合のバックアップ体制（バックアップの取得・隔離管理、復旧手順の明確化等）について、具体的な管理手順等が整備されている。
委託された重要維持管理等 (*2) の実施に当たり、委託（再委託（再委託された重要維持管理等の全部又は一部が更に委託されるものを含む。以下同じ。）を含む。）を受けた者（その従業員等を含む。）によって、特定重要設備について特定社会基盤事業者が意図しない変更が加えられることを防止するために必要な管理等がなされ、その管理等に関する事項を特定社会基盤事業者が確認できることを契約等により担保している。	・委託の相手方において特定重要設備の操作ログや作業履歴等の保管に関する手順が明確に定められており、ログの確認による不正行為の有無を定期的に確認している。 ・委託の相手方が、作業担当者や管理責任者に対して、サイバーセキュリティに関する教育や研修を定期的（年間 1 回以上）に実施しており、サイバーセキュリティリテラシーの維持向上に努めている。
特定社会基盤事業者が、特定重要設備及び構成設備の供給や委託（再委託を含む。）した重要維持管理等の適切性について、外国の法的環境等により影響を受けるものではないことを確認している。	・特定重要設備及び構成設備の供給者や委託（再委託を含む。）の相手方が、外国の法的環境や外部の主体の指示によって、特定社会基盤事業者との契約を違反する行為が生じた可能性がある場合、これを特定社会基盤事業者に対して報告することが契約等により担保されている。

出典：基本指針におけるリスク管理措置の一部を抜粋して大和総研作成

基本指針からの示唆

本制度は 2024 年 2 月までに施行される予定で、特定社会基盤事業者として指定される事業者だけでなく、その委託先にも影響が及ぶため、委託先を含む関係事業者は施行に備えて準備を進める必要があります。

基本指針に例示されたリスク管理措置は、昨今問題となっている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上でも大いに参考になるため、対応を検討することが望ましいと考えられます。また、審査においてリスク管理措置の実施状況を確認するにあたっては、事業ごとの実態を十

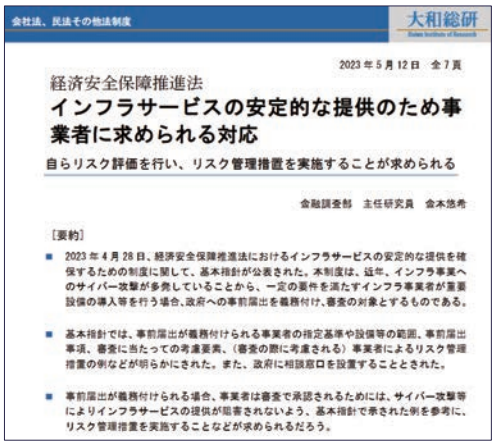
(*1) 国外からインフラサービスの安定的な供給を妨害する行為の手段として使用される恐れがある設備のことで、ハードウェアの他、プログラム（ソフトウェア）も含まれます。

(*2) 特定重要設備の一定の維持管理または操作を行うことをいいます。

分に踏まえ、特定社会基盤事業者等の主体的な取り組みについても適切に評価するとされています。そのため、関係事業者においては、本制度の趣旨を理解し、自らリスク評価を行い、その結果に応じて適切なリスク管理措置を行うことが重要です。

基本指針には、政府が事前相談窓口を設置し、必要な助言その他の援助を行うことが明記されており、内閣府の Web サイトにおいて本制度に関する各省庁の相談窓口の一覧を確認することができます (*1)。関係する事業者にあっては、これら相談窓口を活用し、準備を進めることが有効だと考えられます。

なお、当社研究員による本制度および基本指針の詳しい解説レポートを公開していますので、内容については下記の当社 Web サイトをご参照ください。


会社法、民法その他制度

大和総研

2023 年 5 月 12 日　全 7 頁

経済安全保障推進法

インフラサービスの安定的な提供のため事業者に求められる対応

自らリスク評価を行い、リスク管理措置を実施することが求められる

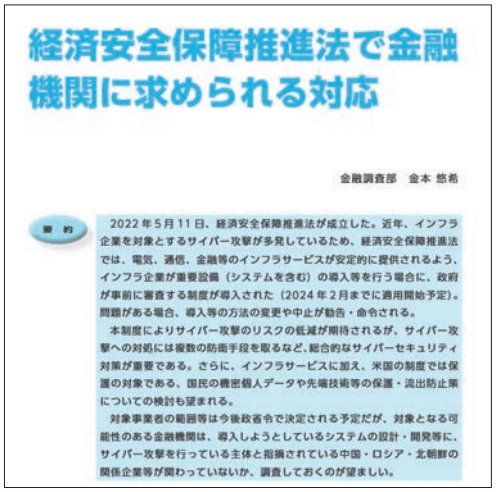
金融調査部　主任研究員　金本悠希

［要約］

- 2023 年 4 月 28 日、経済安全保障推進法におけるインフラサービスの安定的な提供を確保するための制度に関して、基本指針が公表された。本制度は、近年、インフラ事業へのサイバー攻撃が多発していることから、一定の要件を満たすインフラ事業者が重要設備の導入等を行う場合、政府への事前届出を義務付け、審査の対象とするものである。
- 基本指針では、事前届出が義務付けられる事業者の指定基準や設備等の範囲、事前届出事項、審査に当たっての考慮要素、（審査の際に考慮される）事業者によるリスク管理措置の例などが明らかにされた。また、政府に相談窓口を設置することとされた。
- 事前届出が義務付けられる場合、事業者は審査で承認されるためには、サイバー攻撃等によりインフラサービスの提供が阻害されないよう、基本指針で示された例を参考に、リスク管理措置を実施することなどが求められるだろう。

インフラサービスの安定的な提供のため事業者に求められる対応（2023 年 5 月 12 日掲載）

https://www.dir.co.jp/report/research/law-research/law-others/20230512_023790.html


経済安全保障推進法で金融機関に求められる対応

金融調査部　金本 悠希

要　約

2022 年 5 月 11 日、経済安全保障推進法が成立した。近年、インフラ企業を対象とするサイバー攻撃が多発しているため、経済安全保障推進法では、電気、通信、金融等のインフラサービスが安定的に提供されるよう、インフラ企業が重要設備（システムを含む）の導入等を行う場合に、政府が事前に審査する制度が導入された（2024 年 2 月までに適用開始予定）。問題がある場合、導入等の方法の変更や中止が勧告・命令される。

本制度によりサイバー攻撃のリスクの低減が期待されるが、サイバー攻撃への対処には複数の防衛手段を取るなど、総合的なサイバーセキュリティ対策が重要である。さらに、インフラサービスに加え、米国の制度では保護の対象である、国民の機密個人データや先端技術等の保護・流出防止策についての検討も望まれる。

対象事業者の範囲等は今後政省令で決定される予定だが、対象となる可能性のある金融機関は、導入しようとしているシステムの設計・開発等に、サイバー攻撃を行っている主体と指摘されている中国・ロシア・北朝鮮の関係企業等が関わっていないか、調査しておくのが望ましい。

経済安全保障推進法で金融機関に求められる対応

（2022 年 10 月 20 日掲載）

https://www.dir.co.jp/report/research/law-research/law-others/20221020_030115.html

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

2. 『ソフトウェア管理に向けた SBOM の導入に関する手引（案）』に対する意見募集

意見募集の概要

経済産業省は 2023 年 4 月 25 日、『ソフトウェア管理に向けた SBOM（Software Bill of Materials）(*1)の導入に関する手引（案）』に対する意見公募手続（パブリックコメント）を開始しました（5 月 25 日終了）(*2)。提出された意見は整理した上で検討の結果が公表される予定です。

経済産業省が設置する「産業サイバーセキュリティ研究会 WG1」内のサイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースでは、SBOM に関する実証や議論を行っています。その結果を踏まえ、SBOM の導入を検討する企業が参考にできる手引が作成されました。

手引の対象読者は、開発・設計部門や製品セキュリティ担当部門などのソフトウェアセキュリティに関わる部門と経営層です。特に SBOM という用語は聞いたことがあるが具体的な内容は把握できていない組織など SBOM 初級者向けの内容になっています。このため、手引には「SBOM とは」「SBOM 導入のメリット」など SBOM の基本的な情報も記載されています。手引の全体的な構成は、下表のとおりで、以降では 3 章から 6 章に記載されている内容を紹介します。SBOM の概要や動向については、『DIR SOC Quarterly 2022 vol.2(*3)』でも取り上げていますのでご参照ください。

章		概要
1	背景と目的	SBOM が注目を集める背景、本手引の目的、活用方法などが記載されています。
2	SBOM の概要	海外などの情報を基に、SBOM とは何か、SBOM の最小要素、フォーマット、導入のメリットなど SBOM に関する基本情報について記載されています。
3	SBOM 導入に関する基本指針・全体像	体制整備から運用管理まで導入に向けたプロセスとポイントが記載されています。詳しくは以降で紹介します。
4-6	実施事項・認識しておくべきポイント	
7	付録	実施事項チェックリスト、用語集、SBOM ツール(*4)一覧が記載されています。

出典：『ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引（案）』を基に大和総研作成

SBOM 導入に向けたプロセス

手引では、SBOM 導入に向けたプロセスを 3 つのフェーズに分け、実施事項と重点ポイントを整理しています。この重点ポイントに従って自社の状況を点検することで、全体的な導入プロセスや導入における課題などを把握することができます。

(*1)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た一覧表のことで「ソフトウェア部品表」とも呼ばれる。ソフトウェアの透明性が向上し、ソフトウェアの脆弱性を迅速に特定・対処できるものとして期待されています。

(*2)https://public-comment.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595223028&Mode=0

(*3)大和総研『 DIR SOC Quarterly 2022 vol.2』（ https://www.dir.co.jp/publicity/publication/socquarterly2211.html ）

(*4)SBOM の作成、共有、活用、管理ができるツールです。手引では具体的な製品が紹介されています。

■環境構築・体制整備フェーズ		
ステップ	実施事項	認識しておくべきポイント
SBOM 適用範囲の明確化	・開発言語、コンポーネントの形態等、ソフトウェアの情報を明確化する。 ・ソフトウェアの構成図を作成する。	・組織内外の知見を活用することで、効率的な情報収集を行うことができる。 ・構成図でリスク管理範囲を明確にできる。
SBOM ツールの選定	・ツール選定基準を整理する。 ・複数のツールを評価し選定する。	・複数ツールの使い分けは非効率な場合がある。 ・有償ツールは一般に高価である。
SBOM ツールの導入・設定	・ツールの導入要件を確認し環境を整備する。 ・取扱説明書などを確認し初期設定を行う。	・無償ツールは構築や設定に関する情報が不足している場合がある。
SBOM ツールに関する学習	・取扱説明書などを確認し使い方を学習する。 ・ツールのノウハウを組織内で共有する。	・ツールの販売代理店やベンダーのサポートを活用することで効率的に使い方を習得できる。
■作成・共有フェーズ		
コンポーネントの解析	・ツールを用いてソフトウェアのスキャンを行う。 ・誤検出や検出漏れが無いか確認する。	・ツールを用いることで、手動に比べ、効率的に解析を行うことができる。 ・解析方法、解析環境によって結果が異なる。
SBOM の作成	・SBOM の項目、フォーマット、出力ファイル形式等の要件を決定する。	・正確な情報を不足なく SBOM に記載する。 ・SBOM 利用者も分かる名称設定を行う。
SBOM の共有	・共有方法を検討し必要に応じて共有する。 ・改ざん防止のため電子署名等を検討する。	・ツールによってインポートできる SBOM 形式やフォーマットに制約がある場合がある。
■運用・管理フェーズ		
SBOM に基づく脆弱性管理、ライセンス管理等の実施	・OSS のライセンス違反がないかを確認する。 ・脆弱性の有無を確認する。	・ツールの脆弱性やライセンス情報が誤っている場合があり、結果を確認する必要がある。
SBOM 情報の管理	・SBOM は一定期間保管する。	・組織内の PSIRT(*1)に相当する部門が SBOM を管理することが効果的である。

出典：『ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引（案）』を基に大和総研作成

手引からの示唆

手引は、SBOM ツールを前提とした内容になっていますが、SBOM を手動で作成、管理することも可能です。SBOM の整備はソフトウェアサプライチェーン全体で取り組むことで、ソフトウェアの透明性が向上し、脆弱性の少ない製品が増えます。このため、SBOM ツールや手動での導入にかかわらず、自社に適した方法で SBOM を活用することが大切です。

第 1 部の「1. 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」で触れた基本指針では、事業者に求められる対応として、セキュリティパッチが適用されていることや脆弱性対応が実施されていることなどがリスク管理措置の具体例として挙げられています。当該基本指針では SBOM の導入に関する記述はありませんが、SBOM の活用によってリスク管理措置の一部に対応できると考えられます。

(*1)Product Security Incident Response Team の略で、自社製品を対象にインシデントが発生した際に対応する組織のことです。

3. 『重要インフラのサイバーセキュリティに係る安全基準等策定指針（案）』等に対する意見募集

意見募集対象の 2 つの文書

内閣サイバーセキュリティセンター（NISC）は 2023 年 4 月 24 日に、『重要インフラのサイバーセキュリティに係る安全基準等策定指針(案)』（以下、「安全基準等策定指針」と略記）および『重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書(案)』（以下、「リスクマネジメント等手引書」と略記）に対する意見公募手続（パブリックコメント）を開始しました（5 月 23 日終了）(*1)。いずれの文書も政府のサイバーセキュリティ戦略本部が 2022 年 6 月に策定した『重要インフラのサイバーセキュリティに係る行動計画』(*2)（以下、「行動計画」と略記）の内容を踏まえ、大幅に改変された内容となっています。

2 つの文書の位置付け

政府はサイバーセキュリティを確保するための基準や参考文書類を「安全基準等」と呼んでおり、法令に基づいて重要インフラ所管省庁が定める「基準」や「ガイドライン」、業界団体等が定める「業界標準」、重要インフラ事業者自身が定める「内規」などの種類があると定義しています。

今回の意見募集対象の一つである安全基準等策定指針は、これらの安全基準等を策定・改訂する際の指針であり、安全基準等に規定されることが期待されるサイバーセキュリティ対策や取り組みが記載されています。またもう一つの意見募集対象であるリスクマネジメント等手引書は、この安全基準等策定指針で示す取り組みについての参考情報という位置付けです。

2 つの文書の改定のポイント

2 つの文書は、前述のとおり行動計画の内容を踏まえて改定されています。主な改定のポイントは以下のとおりです。

安全基準等策定指針

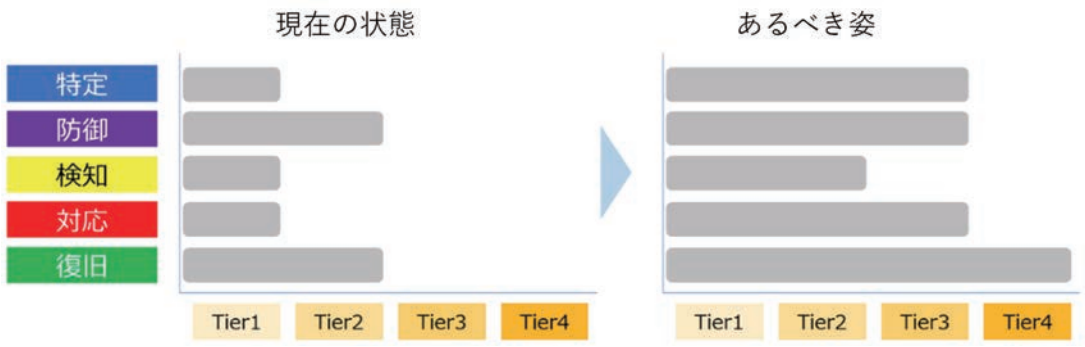
改定前の第 5 版では情報セキュリティ対策の PDCA に沿った章立てで記載されていましたが、これが抜本的に改められ、組織統治とリスクマネジメントを中心にした章立てに変更されました。行動計画では、組織統治の一部としてサイバーセキュリティを組み入れること、そして、サプライチェーンリスクも含めてリスクマネジメントを活用してリスク管理していくことの重要性が強調されており、それが明確に反映された形となっています。

(*1) https://www.nisc.go.jp/policy/group/infra/pubcom_shishin6.html

(*2) https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf

リスクマネジメント等手引書

改定前の文書名は『重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書』(*1)であり、リスクアセスメントにフォーカスした文書でした。しかし、今回の改定で記載の範囲がリスクマネジメント全体に拡大され、文書名も変更になりました。また行動計画に明記されているとおり海外の指針も適宜参考にされています。特に国際的に評価の高い米国国立標準技術研究所（NIST）のサイバーセキュリティフレームワーク(*2)の考え方や手法が随所に取り入れられています。たとえば、今回のリスクマネジメント等手引書には、組織の現状とあるべき姿を比較分析し、分析結果に基づいて対策を講じていくというリスク対応の手法（下図）が記載されていますが、これは NIST のサイバーセキュリティフレームワークを参考にしています。



図：組織の現状と目標とするあるべき姿を比較分析し、分析結果に 基づいて対策を講じる（図中の Tier1～Tier4 は対応の程度）

出典：NISC『重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書(案)』(*3)に掲載の図を基に大和総研が加筆

改定からの示唆

サイバーセキュリティは組織統治の一部であるという考え方や、リスクマネジメントの対象として適切にサイバーセキュリティリスクをコントロールしていく必要があるという考え方は、今回の 2 つの文書以外にも、政府から公開される様々な文書に見受けられます。たとえば、2023 年 3 月に経済産業省と独立行政法人情報処理推進機構（IPA）が共同で策定した『サイバーセキュリティ経営ガイドライン Ver3.0』(*4)も同様の考え方に基づいています。今後、重要インフラ事業者だけでなく、その他の組織についても組織統治とリスクマネジメントの対象としてサイバーセキュリティを扱うことが求められる傾向がますます強まっていくものと考えられます。

(*1) https://www.nisc.go.jp/files/tebikishorev.zip

(*2) https://www.nist.gov/cyberframework

(*3) https://www.nisc.go.jp/pdf/policy/infra/pubcom_tebikisho2.pdf

(*4) https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

4. 『金融機関の IT ガバナンスに関する対話のための論点・プラクティスの整理』の改訂（案）に対する意見募集

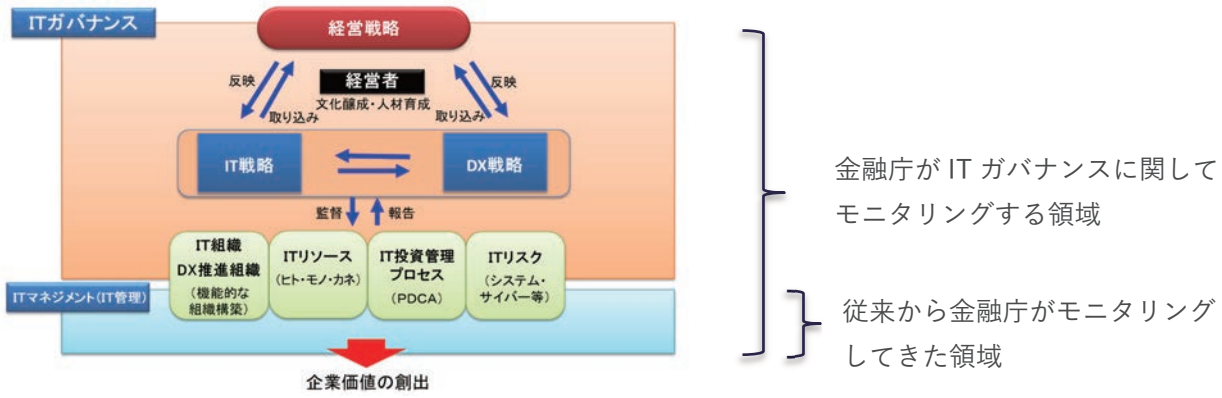
意見募集対象の文書

金融庁は 2023 年 4 月 24 日に、『金融機関の IT ガバナンスに関する対話のための論点・プラクティスの整理』の改訂（案）に対する意見公募手続（パブリックコメント）を開始しました（5 月 31 日終了）(*1)。この文書の初版は 2019 年 6 月に公表されましたが、今回の第 2 版（案）ではセキュリティに関する記載が増加しています。

この文書の位置付け

金融庁は 2018 年に『金融検査・監督の考え方と進め方（検査・監督基本方針）』(*2)を公表し、それまでの形式的な最低基準（ミニマムスタンダード）を重視する金融行政から、金融機関との対話を通じてベスト・プラクティスの追求を促す金融行政へと転換を図っています。この方針転換に基づき、金融庁は個別のテーマ・分野ごとに具体的な対話の材料としてディスカッションペーパーをいくつか公表しており、今回意見募集対象の『金融機関の IT ガバナンスに関する対話のための論点・プラクティスの整理』もその一つです。

この文書では IT ガバナンスを「経営者がリーダーシップを発揮し、IT と経営戦略を連携させ、企業価値の創出を実現するための仕組み」と定義(*3)しています。その上で、IT ガバナンスの論点を扱う理由として、現在の金融機関は自らの経営理念を実現するために IT システムを経営戦略と連携させていくことが強く求められており、従来の IT マネジメントのモニタリングだけでなく、IT ガバナンスをいかに有効に機能させるかについて対話の重要性が高まっていることをあげています(*3)。



図：IT ガバナンスの概念

出典：金融庁『金融機関の IT ガバナンスに関する対話のための論点・プラクティスの整理　第 2 版（案）』の p6 に掲載の図表を基に大和総研が加筆

(*1) https://www.fsa.go.jp/news/r4/sonota/20230424/20230424.html

(*2) https://www.fsa.go.jp/news/30/wp/supervisory_approaches_revised.pdf

(*3) 金融庁『金融機関の IT ガバナンスに関する対話のための論点・プラクティスの整理　第 2 版（案）』p1
(https://www.fsa.go.jp/news/r4/sonota/20230424/01.pdf)

改訂のポイント

第 2 版（案）でも 2019 年公表の初版を概ね踏襲し、IT ガバナンスについて主に以下の 6 つの考え方・着眼点が整理されています(*1)。

① 経営陣によるリーダーシップ
② 経営戦略と連携した「IT 戦略」・「DX 戦略」
③ IT 戦略を実現する「IT 組織」・「DX 推進組織」
④ 最適化された「IT リソース(資源管理)」
⑤ 企業価値の創出に繋がる「IT 投資管理プロセス」
⑥ 適切に管理された「IT リスク」

ただ第 2 版（案）では、初版と比較すると DX（デジタルトランスフォーメーション）の考え方・着眼点が盛り込まれたことに加え、セキュリティに関連する記載が増加しています。特に上記⑥の「IT リスク」に関しては DX 推進のリスクの一つとしてサイバーリスクを含む情報セキュリティリスクがあげられ、また新商品・新サービスの企画・設計段階からセキュリティ要件を組み込む「セキュリティバイデザイン」を実践することの重要性などについても触れられています。

さらに第 2 版（案）では上記の①、②、③でも、初版と比較するとサイバーセキュリティ管理態勢の構築、情報セキュリティ方針の策定、情報セキュリティ人材の確保などについて追記されています。

改訂からの示唆

この文書『金融機関の IT ガバナンスに関する対話のための論点・プラクティスの整理』は金融庁と金融機関の対話の材料（ディスカッションペーパー）であり、チェックリストや何らかの基準として用いられるようなものではありません。あくまでも金融機関がベスト・プラクティスを追求する上でのヒントを提供するようなものです。しかし、セキュリティに関する記載の増加から、IT ガバナンスを推進する上でいかにセキュリティの重要性が増しているかをうかがい知ることができます。そして、このことは金融機関のみならず、その他のあらゆる業界にも当てはまることであると言えます。この文書は、金融業界以外の企業の経営層や IT ガバナンスに関わる部署の人間にとっても示唆に富み、参考になるものと言えるでしょう。

(*1) 金融庁『金融機関の IT ガバナンスに関する対話のための論点・プラクティスの整理　第 2 版（案）』p7
(https://www.fsa.go.jp/news/r4/sonota/20230424/01.pdf)

5. 日本銀行および金融庁『地域金融機関における CSSA の集計結果（2022 年度）』を公開

概要

日本銀行と金融庁は 4 月 18 日、地域金融機関向けの「サイバーセキュリティセルフアセスメント（Cyber Security Self-Assessment、CSSA）」の集計結果（自己評価期間：2022 年 7 月～8 月、対象：地域銀行、信用金庫及び信用組合の 498 機関）を公開しました(*1)。

ここで使われた CSSA の点検票は、日本銀行や金融庁が、金融情報システムセンター（FISC）と協力して作成したもので、地域金融機関自身が自己評価に基づき、自律的にサイバーセキュリティ対策の強化に取り組むことを促すためのものです。設問は、NIST（米国国立標準技術研究所）のサイバーセキュリティフレームワーク（CSF）をはじめとした主要なサイバーセキュリティ管理の枠組みや、アンケート調査の設問等を参考に作成され、最近のサイバー攻撃の脅威動向も考慮されています。

CSSA 点検票

CSSA の点検票は、全 42 問の設問からなる自己評価ツールで、自組織の位置付けや役割を他の金融機関と比べ、課題を特定するために整備されました。公開された CSSA の目的に記載されているように、大手金融機関では、国際的なフレームワークを活用した成熟度評価が行われている一方で、地域金融機関ではこのツールが広く使われていなかったため、自己評価ツールが整備されました。

点検項目において注目すべきは、「サイバーインシデント対応・業務復旧の態勢」「サードパーティ(*2)等の管理」の項目数が多いことです。

CSSA点検票の設問内容	設問数	設問の主な論点
サイバーセキュリティに関する経営層の関与	4	サイバーセキュリティに関する経営方針や経営計画、経営層への定期報告、随時報告など
サイバーセキュリティに関するリスクの把握と対応	4	サイバー攻撃の把握、情報収集、リスク評価、リスクへの対応方針の決定など
サイバーセキュリティに関する監査	3	監査対象、監査結果の報告先、指摘事項に対する改善の実施状況の確認
サイバーセキュリティに関する教育・訓練	1	サイバーセキュリティに関する注意喚起・教育・訓練の実施状況
新たなデジタル技術の評価	2	新たなデジタル技術の導入に際するリスク評価の体制など
資産管理	3	システム管理簿の整備状況、ハードウェア、ソフトウェアの管理状況など
アクセス管理	2	重要なシステムへのアクセス権、リモートアクセスの管理状況など
データ保護	2	データ保護（暗号化、伝送制限）、バックアップ対策など
監査証跡(ログ)の管理	1	重要なシステムの監査証跡(ログ)に関する規定
システムの脆弱性に関する管理・対応	4	脆弱性診断やペネトレーションテストの実施状況、パッチ適用方針など
サイバー攻撃に関する技術的な対策	3	端末、境界、Webサイト・インターネットバンキングシステムにおける技術的な対策
サイバーインシデントの検知	2	監視・分析等の実施状況、モニタリング内容
サイバーインシデント対応・業務復旧の態勢	6	サイバーインシデント発生時の対応要員、対応ルール・手順の整備など
サードパーティ等の管理	5	サードパーティ管理状況、クラウドサービスに対する安全対策など

表：サイバーセキュリティセルフアセスメント（CSSA）の点検票
出典：『地域金融機関におけるCSSAの集計結果（2022年度）(*1)』に掲載の図を基に大和総研作成

(*1) 金融庁 地域金融機関における CSSA の集計結果（2022 年度）（https://www.fsa.go.jp/news/r4/cyber/20230418.html ）

(*2) 自組織がサービスを提供するために、業務上の関係や契約等を有する他の組織（例：システム子会社、ベンダー等の外部委託先、クラウド等のサービス提供事業者等）

「侵入された場合に迅速なサービス復旧を行うこと」と「サードパーティのリスク管理」は、日本銀行や金融庁が注目している点検項目と考えられます。

集計結果からの示唆

CSSA の集計結果によれば、重要なサードパーティに関するサイバーセキュリティのリスクは、半数以上が統括部署による一元管理が行われており、80%以上が少なくとも各所管部署で管理されていることが明らかになりました（図 1）。また、企業の多くは、有事に備えたコンティンジェンシープランを整備していますが、その中で、外部委託先が訓練や演習に参加している企業はわずか 30%未満であることがわかりました（図 2）。

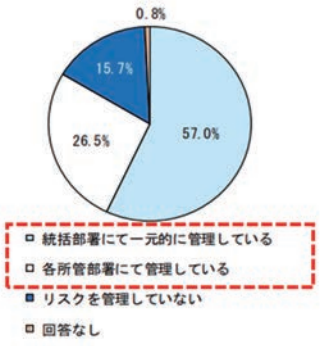


図 1：重要なサードパーティ、また、それらが提供するサービス等のサイバーセキュリティに関するリスク管理状況
出典：『地域金融機関におけるCSSAの集計結果（2022年度）(*1)』に掲載の図を基に大和総研作成

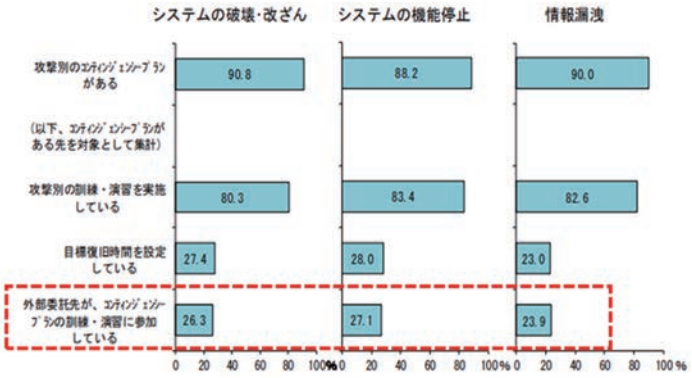


図 2：サイバー攻撃（被害）に対応するコンティンジェンシープランおよび取組内容
出典：『地域金融機関におけるCSSAの集計結果（2022年度）(*1)』に掲載の図を基に大和総研作成

サードパーティの管理は、自組織がサービスを提供するために必要なシステム子会社やベンダーなどの外部委託先が含まれるため、サプライチェーン管理の一部であると言えます。企業は製品やサービスを提供する際に、多くのサードパーティと関係を持っており、サプライチェーン全体でのリスク管理が重要な課題となっています。

これまでの『DIR SOC Quarterly(*2)』でも度々取り上げてきたように、経済産業省の『サイバーセキュリティ経営ガイドライン Ver3.0（2023 年 3 月）(*3)』、経団連の『経団連サイバーセキュリティ経営宣言 2.0（2022 年 10 月）(*4)』ではサプライチェーン管理について触れ、経営者に対してサプライチェーン全体を俯瞰したサイバーセキュリティを強化すべきと指示しています。これに基づき、サードパーティ管理は今後一層強化されることになるでしょう。コンティンジェンシープランの策定や訓練・演習においても、サードパーティを含めた視点で考える必要があると言えます。

(*1) https://www.fsa.go.jp/news/r4/cyber/20230418.html

(*2) 大和総研 DIR SOC Quarterly（ https://www.dir.co.jp/publicity/publication/dirsocquarterly.html ）

(*3) サイバーセキュリティ経営ガイドライン Ver3.0（ https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf ）

(*4) 経団連サイバーセキュリティ経営宣言 2.0（ https://www.keidanren.or.jp/policy/2022/087.html ）

1.SIM スワップ詐欺による不正送金事案の摘発

概要

2023 年 5 月 11 日、「SIM スワップ詐欺」と呼ばれる手口を使い、他人のネットバンキングの口座から 197 万円を別の口座へ不正送金したとして、警視庁サイバー犯罪対策課は詐欺や組織犯罪処罰法違反などの疑いで被疑者を逮捕したと複数の報道機関が報じました (*1) 。

今回逮捕された被疑者は「闇バイト」に応募した犯罪の実行役であり、背後に指示役などの犯罪グループが存在するとみられています。SIM スワップ詐欺による被害は全国で相次いでおり、警視庁は同様の手口などで昨年の 7 月から 10 月にかけて、約 9,000 万円を不正送金した疑いがあるとみて調べています。

SIM スワップ詐欺の手口

「SIM スワップ詐欺」とは、携帯電話の契約者になりすまして SIM カードの再発行手続を行い、被害者の電話番号を乗っ取ることで、被害者の銀行口座から犯罪者の口座に対して不正送金を行う犯罪手口のことをいいます。ネットバンキングにおいて利用者を認証する際、多要素認証 (*2) に使用される利用者の電話番号を犯罪者側に移し、認証を突破することを目的として行われます。

具体的な SIM スワップ詐欺の流れは次のとおりです。

① 個人情報の収集

犯罪者はフィッシングサイトなどを利用し、被害者の個人情報（氏名、生年月日、ネットバンキングの ID・パスワードなど）を入手します。

(*1) 産経新聞　スマホ乗っ取る「SIM スワップ」詐欺か　他人装い出金容疑で女逮捕　警視庁
(https://www.sankei.com/article/20230511-75NGJHDMMBJGZL2QFQMFUC3QLE/)

日本経済新聞　「SIM スワップ」知らぬ間にネット送金　本人認証を突破
(https://www.nikkei.com/article/DGXZQOUE09C920Z00C23A5000000/)

(*2) 認証の 3 要素である知識情報（本人しか知らないこと）、所持情報（本人しか持っていない物）、生体情報（本人の身体的特徴）のうち、異なる 2 つ以上の要素を組み合わせて行う認証のことです。

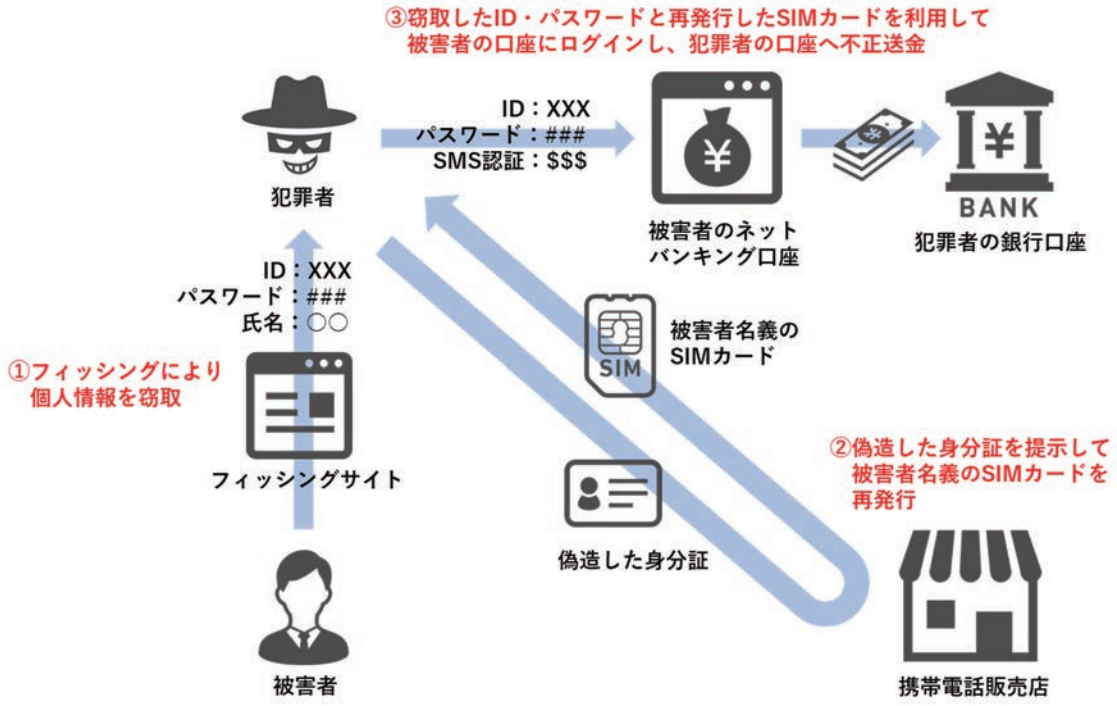
② SIM カードの再発行による電話番号の乗っ取り

犯罪者は入手した個人情報を利用して、被害者名義の運転免許証などの身分証を偽造します。その上で被害者になりすまし、携帯電話販売店で SIM カードの再発行を依頼します。この際、店側から本人確認が求められますが、偽造した身分証の提示によって再発行手続を完了させます。再発行された SIM カードを犯罪者側の携帯電話に挿入することで、被害者に対する電話や SMS は全て犯罪者側の携帯電話に届くようにし、被害者の電話番号を乗っ取ります。

③ 不正送金の実行

入手したネットバンキングの ID とパスワードを用いて被害者の口座にログインを試みます。この際、多要素認証として被害者に送られる SMS や自動音声によるワンタイムパスワードは犯罪者側の携帯電話に届くことになるため、犯罪者は利用者認証を突破し、不正送金を行います。

なお、多額のお金が一度に送金される場合、銀行から本人確認の電話を行うことがありますが、この電話も犯罪者側の携帯電話につながることになるため、不正送金を止めることはできません。



図：SIM スワップ詐欺のイメージ

出典：大和総研作成

報道内容の考察

SIM スワップ詐欺は海外では数年前から問題となっていましたが、国内でも昨年から多くの被害が確認されるようになりました。利用者の電話番号を多要素認証に使用するサービスは数多く存在しますが、SIM スワップ詐欺の被害が多く確認されている現状からすると、安全性が高い認証として過度に信頼を置くことは危険であると言わざるを得ません。そのため、上記で述べた犯行の手口を理解し、被害を防ぐために正しく対策をとる必要があります。

SIM スワップ詐欺の被害を防ぐには、まずは基本的なフィッシング対策と同様、偽のメールや Web サイトに注意し、ID、パスワードなどの認証に必要な情報を窃取されないようにすることが最も重要です。また、SNS が発展した現代においては SNS の情報を基に個人情報を取得される恐れもあるため、このようなサービスを利用する際には掲載する情報に十分注意を払うとともに、プライバシーの設定で公開範囲を限定するといった対策を行うことも、身分証の偽造防止を図る上で重要だと言えます。

さらに、近年では FIDO 認証と呼ばれる公開鍵暗号に基づくパスワードレスな認証方式を多要素認証として採用したサービスの普及が進んでいます。FIDO 認証が利用できるサービスの場合、電話番号を必要とせずに認証の強化が可能となるため、たとえ ID、パスワードなどの情報が窃取されたとしても SIM スワップ詐欺による被害を確実に防ぐことができます。FIDO 認証については第 3 部の「2. パスワード不要の新しい認証方式「パスキー」」で触れていますのでご参照ください。

2. ディープフェイクの脅威と対策

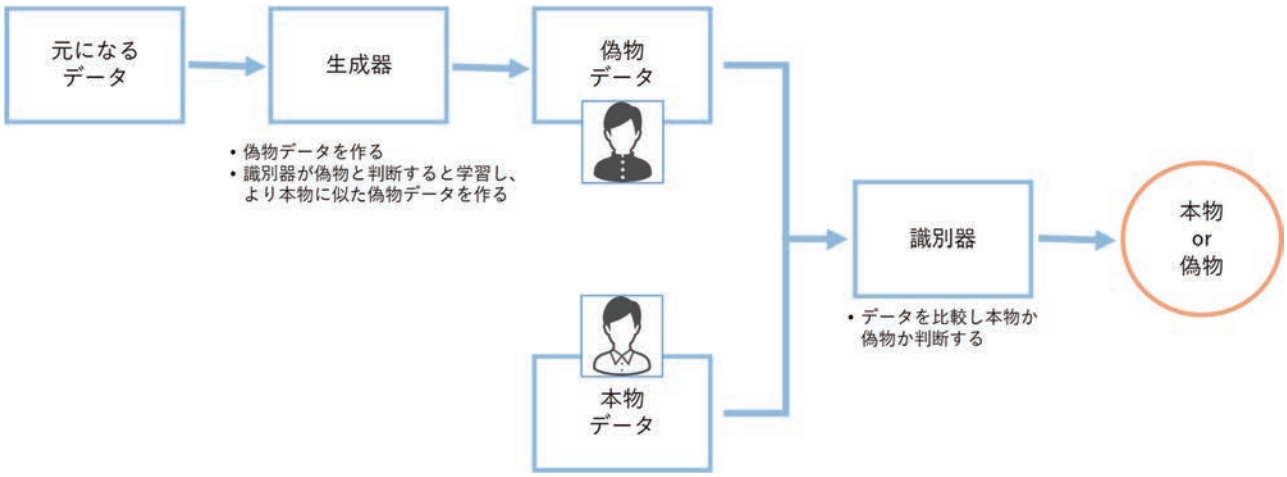
はじめに

近年、AI（人工知能）技術の進歩により、ディープフェイクの脅威が増しています。トレンドマイクロが 2022 年 12 月に公開した「2023 年セキュリティ脅威予測(*1)」では、ディープフェイクが主要なトピックの一つとして挙げられており、今後、ディープフェイクを用いた巧妙化した犯罪が増えてくることが予測されています。

ディープフェイクとは

ディープフェイクとは、「ディープラーニング」と「フェイク」を組み合わせた造語で、AI を用いて、画像や動画、音声などの一部を交換や結合をし、元とは異なる画像等を作成する技術です。つまり、動画や音声を合成する技術のことです。ディープフェイクによって、実際には行っていない行動をしたり、言っていないことを発言したりしているかのような動画（いわゆるフェイク動画）を作成することができます。

ディープフェイクで使用される代表的な技術として GAN（Generative Adversarial Network：敵対的生成ネットワーク）と呼ばれる生成モデルがあります。GAN は生成器（Generator）と識別器（Discriminator）から構成されています。生成器は画像を作り出し、識別器は画像が本物か偽物か判定します。この 2 つのモデルが競い合うことで、本物に近い画像を作り出します。



図：GAN のイメージ

出典：大和総研作成

(*1) https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20221226-01.html

ディープフェイクの脅威

ディープフェイクを用いてフェイク動画を作成するには一定のスキルが必要でしたが、近年、パソコンやスマートフォンで簡単にフェイク動画を作成できるサービスが登場しています。このため、誰でもフェイク動画を作成できるようになり、ディープフェイクを悪用した犯罪が増加しています。たとえば、以下のような事例があります。

- なりすましによる情報操作

  政治家になりすまし虚偽情報を発信し、情報操作が行われます。最近では、ウクライナのゼレンスキー大統領が市民に投降を呼びかける動画(*1)やアメリカのトランプ前大統領が逮捕される写真(*2)が SNS 上で公開され話題となりました。

- なりすましによる金銭要求

  知人になりすまし電話やビデオ通話で金銭を要求します。ディープフェイクボイス攻撃とも呼ばれ、実際に事件も発生しています(*3)。ディープフェイクボイス攻撃はビジネスメール詐欺と組み合わせることで手口が巧妙化する恐れがあります。攻撃者は経営者や取引先になりすましてメールを送信後、さらにディープフェイクを使って本人の声をまねて電話をかけ金銭を要求する可能性があります。

- 他人になりすまし顔認証を突破

  他人の身分証明書と他人の顔になりすました動画を使って本人確認を突破します。2021 年 6 月に株式会社日立製作所が発表した論文(*4)では、顔認証システムを用いて本人確認を実施した結果、同一人物であると判定されました。これにより、不正な口座開設などが可能だと判明しました。

(*1)https://news.sky.com/story/ukraine-war-deepfake-video-of-zelenskyy-telling-ukrainians-to-lay-down-arms-debunked-12567789

(*2)https://nypost.com/2023/03/22/chilling-deepfakes-claiming-to-show-trumps-arrest-spread-across-twitter/

(*3)36Kr Japan　AI がビデオ通話で「友達」になりすまし。会社社長が 8500 万円の振り込め詐欺被害：中国

(https://36kr.jp/234282/)

ZDNET Japan　CEO になりすましたディープフェイクの音声で約 2600 万円の詐欺被害か

(https://japan.zdnet.com/article/35142255/)

(*4)https://www.jstage.jst.go.jp/article/pjsai/JSAI2021/0/JSAI2021_1F2GS10a02/_pdf

ディープフェイク対策

フェイク動画や画像の完成度は高まっており、人間の目で判断することが難しくなっています。このような不確かな情報に騙されないために以下のような対策があります。

- 複数手段で確認

  情報源の確認やファクトチェックを実施するメディアの活用などを行い、情報が本物か見分けます。また取引先等と電話をする場合も詐欺の可能性を疑い、振込先の変更など重要な連絡に対しては複数の手段で確認することが必要です。

- ディープフェイク検出ツール

  ツールを用いてディープフェイクで作成されたフェイク動画や画像を検出します。AI によって人間の目ではわかりづらい色の違いや血流などの特徴を評価することで、フェイク動画や画像を検出することができます。

- 来歴を記録する規格「C2PA」

  C2PA は、Coalition for Content Provenance and Authenticity（略称 C2PA、コンテンツの来歴と真正性のための連合）が定めた技術規格です。画像に作成者や編集履歴などの情報を画像のメタデータとして保存することで改ざんを防ぐことができます。メタデータも公開鍵暗号基盤を使用した暗号化により保護されています。C2PA はディープフェイク検出ツールのように偽物を検出するためではなく、本物であることを保証するために利用します。

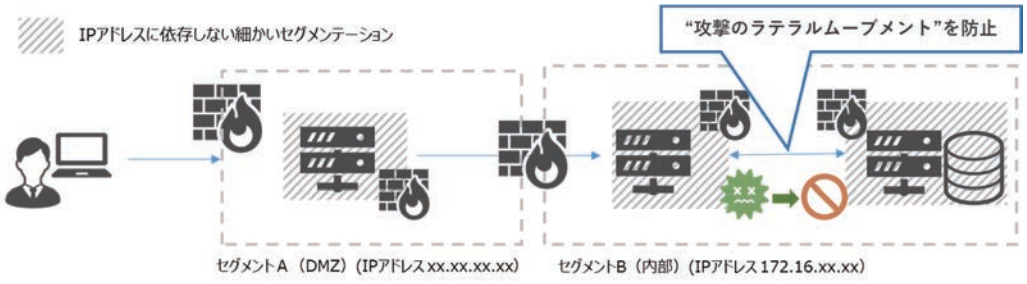
最後に

AI の技術は急速に発展しており今後もディープフェイクを悪用した犯罪が増加することが予想できます。特に組織が注意すべきは、上記で紹介したビジネスメール詐欺の巧妙化です。ChatGPT の登場により、経営者などになりすましたメールを誰でも作成できるようになりました。さらにディープフェイクを用いたなりすまし電話との組み合わせによりビジネスメール詐欺の被害が拡大する恐れがあります。企業は従業員の情報リテラシーを高めるとともに、金銭の要求があった場合は、複数の方法で確認できる体制を整備しておくことが大切です。

1. 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-

マイクロセグメンテーションとは

マイクロセグメンテーションは、ネットワーク内の通信を細かく制御してセキュリティを高める手法です。特に、組織内に侵入したマルウェア（ウイルスやランサムウェアなどの悪意のあるソフトウェア）の拡散を防ぐために、ラテラルムーブメント(*1)を制限することが重要な対策として挙げられます。



図：マイクロセグメンテーションのイメージ
出典：大和総研作成

マイクロセグメンテーションが注目される背景

マイクロセグメンテーションは、2010 年代初頭に仮想化技術を活用することで開発され、データセンター内のセグメンテーション(*2)に利用されていました。当時は、データセンター内のサーバー間のセグメンテーションにフォーカスして、複数のサーバーにファイアウォールを入れる代わりに、ネットワーク仮想化の技術を使ってセグメントを細かく分けるというものでした。

現在は、クラウドシフトの加速やテレワークの普及により、従来の「境界型(*3)」から「ゼロトラスト(*4)」へ転換が進んでいます。これは、内部ネットワークに侵入される脅威が増えたため、従来の「境界型」だけではセキュリティが不十分になってきたためです。このような背景から、マイクロセグメンテーションは、日本でも一部の企業で採用され、セキュリティ強化のために注目されている技術となっています。

(*1) マルウェアが侵入した 1 つのコンピューターから他のコンピューターに手動または自動的に広がることを指します。

(*2) 共通の特徴を持つグループを作り、そのグループ間にファイアウォールを設置して、必要な通信だけを許可することで、セキュリティを強化する方法です。一般的には、IP アドレスやポート番号を制御することで、ネットワークの通信を管理します。

(*3) 信頼できる「内側」と信頼できない「外側」にネットワークを分け、境界線にファイアウォールや IDS/IPS などのセキュリティ機器を設置して、外部からの攻撃を遮断し、内部ネットワークを保護するセキュリティ対策の手法です。

(*4) 信頼性の有無に関係なく、全ての通信に対して常に認証を行い、不正なアクセスを防ぐセキュリティ対策の手法です。

海外では、2021 年 5 月には、米国大統領令によるサイバーセキュリティ強化策(*1)において、セグメンテーションが重視される動きがありました。ここでは、ランサムウェア攻撃が世界中の組織に混乱をもたらし、脅威が深刻かつ増加している中で、米国政府が推奨するベスト・プラクティスの 1 つとして説明されています。具体的には、セグメンテーションを行うことで、攻撃者がネットワーク全体を侵害することを防ぎ、攻撃の拡大を制限することができると説明されています。また、NIST のゼロトラスト文書（NIST SP800-207 Zero Trust Architecture(*2)）でも、マイクロセグメンテーションが言及されています。

マイクロセグメンテーション製品の特長

マイクロセグメンテーションに特化した製品には、次のようにネットワークの可視化やポリシーの定義・管理が管理画面を用いて容易に行え、使いやすさに優れたものがあります。

特長	説明
 ネットワークの可視化	可視化されたネットワークに基づくセキュリティ対策は、トラフィックや不正アクセスを迅速に発見し、細かいレベルでの対策を可能にします。可視化情報に基づいて、ネットワークのトポロジーや通信パターンを把握し、最適化することもできます。
 アクセス制御	プロセス単位やラベル単位など、従来のファイアウォールでは実現できない細かい単位でセグメンテーションができます。また、セグメントごとにルールやポリシーを設定することで、攻撃や不正アクセスを防止することができます。 各セグメントは独立しており、攻撃が発生しても他のセグメントに影響を与えず、被害範囲を最小限に抑えることができます。
 ハイブリッド、マルチクラウド管理	複数のクラウド環境やオンプレミス環境を統合的に管理することができます。 異なる環境でも共通のセキュリティポリシーを適用できるため、システム全体のセキュリティを強化することができます。

表：マイクロセグメンテーション製品の特長
出典：大和総研作成

マイクロセグメンテーション製品導入の注意点

マイクロセグメンテーション製品の管理画面は直感的な GUI により、可視性、可読性、操作性に優れています。一方で、適切な設計と運用には、以下の点に注意する必要があります。

(*1) サイバーセキュリティ強化のための大統領令（https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf ）

(*2)PwC コンサルティング合同会社　NIST SP800-207 「ゼロトラスト・アーキテクチャ」の日本語訳
（https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/assets/pdf/zero-trust-architecture-jp.pdf ）

設計面の注意点

マイクロセグメンテーション製品には「ラベル」と「ポリシー」という機能があり、これらの作成が重要です。ラベルは何を守るかを明確にし、ポリシーは通信可能なセグメントを定義するものです。適切に設計されると、ネットワークの見やすさと制御力が上がります。細かく分割しすぎると管理が難しくなり、大雑把にするとセキュリティが緩くなるため、重要なデータやシステムを把握し、細かさを決めることが大切です。ポリシーはラベル単位、ドメイン(*1)やサブネット(*2)単位、プロセス(*3)単位で制御することができ、これらを理解してラベルとポリシーを設計することが重要です。

運用面の注意点

マイクロセグメンテーション製品を効果的に使用するためには、長期的な視点での運用計画の策定、柔軟なセグメント設定、継続的な運用・監視が必要です。

- 長期的な視点での運用計画の策定

  今後も増加し続けるデバイス数やセキュリティ上の問題に対応するため、将来的な拡張性を考慮した計画を立てることが必要です。

- 柔軟なセグメント設定

  新しいデバイスが追加された場合やアプリケーションが変更された場合に、セグメント設定を変更する必要があるため、システムの設計においてセグメントの設定変更に柔軟に対応できるようにする必要があります。

- 継続的な運用・監視

  セキュリティレベルを保つためには、継続的な運用・監視が必要です。これにより、セキュリティ上の問題を早期に発見・修正し、最新の情報を把握して対策を講じることができます。また、以前はセキュリティ上問題がなかったが、今後問題が発生する可能性がある場合は、設計を見直す必要があります。

まとめ

マイクロセグメンテーション製品は、導入するだけでなく、自社のシステム構成・情報資源等に合わせた設計と運用が必要であり、「何を守るか（ラベル）」や「どのレベルでどのようなルールでセグメント化するか（ポリシー）」などの計画が非常に重要です。適切な設計と運用により、マイクロセグメンテーションは企業のセキュリティ戦略の重要な一部となり、従業員、顧客、企業資産を保護することができるでしょう。

(*1) ネットワーク内で特定の役割や機能を持つコンピューターやサーバーのグループ。

(*2) ネットワーク内で、IP アドレスの範囲を指定して分割した小さなネットワーク。

(*3) コンピューターで実行されるアプリケーションやサービス。

2. パスワード不要の新しい認証方式「パスキー」

概要

2023 年現在でも、オンラインバンキングやオンラインショッピングなど多くの Web サービスでユーザ認証の手段としてパスワードが用いられています。パスワード認証は最も基本的で普及している認証方式ですが、パスワードがフィッシング攻撃などによって攻撃者に盗まれると被害に直結しやすく、インターネット環境で使用するにはセキュリティ上の問題があります。昨今、パスワードを必要としない認証方式として「パスキー」と呼ばれる技術が急速に注目を集めています。最近では、日本時間 2023 年 4 月 5 日に NTT ドコモ d アカウントが(*1)、2023 年 5 月 4 日（世界パスワードの日）に Google アカウントが(*2)、パスキーに対応したことが話題になりました。

パスキーとは

パスキー(Passkeys)は、生体認証技術などの標準化を目指す米国の非営利団体である FIDO（ファイド）アライアンスと Web 標準化団体の W3C が共同で規格化した、パスワードが不要な認証技術です(*3)。「文字列（ワード）」の代わりに「暗号鍵（キー）」を使うパスキーによる認証（ここでは「（広義の）パスキー」と表現します）は、直感的で理解しやすく、一般社会にも急速に浸透する可能性があります。「（広義の）パスキー」は技術的には「FIDO2」と「（狭義の）パスキー」の組み合わせで実装されています。

① FIDO2

FIDO2 は、FIDO アライアンスが公開した認証規格である FIDO(Fast IDentity Online)の最新バージョンです(2018 年制定)。従来のパスワード認証では、あらかじめ登録した ID とパスワードのペアが正しく入力されているかをサーバー側でチェックしてログインを許可しますが、FIDO2 では、認証器と呼ばれるハードウェアキーや生体認証装置などを用いて認証するのが大きな特徴です。初回のログイン時には、アカウントとサイトに紐付いた一意の公開鍵を生成してサーバー側に登録し、対となる秘密鍵をスマートフォンなどユーザのデバイス側に保管します。次回ログイン時には、サーバーから送信されるデータに、デバイスから生体認証などで取り出した秘密鍵を使って署名をして応答し、サーバー側がペアの公開鍵で署名を検証してログインを許可します。FIDO2 には、WebAuthn(Web Authentication)と CTAP(Client To Authenticator Protocol)という技術仕様が含まれます。WebAuthn は、FIDO2 を Web アプリケーション上で使用可能にするための API 仕様で、CTAP は、プラットフォーム(OS)や Web ブラウザと認証器間の通信を定めた規格です。

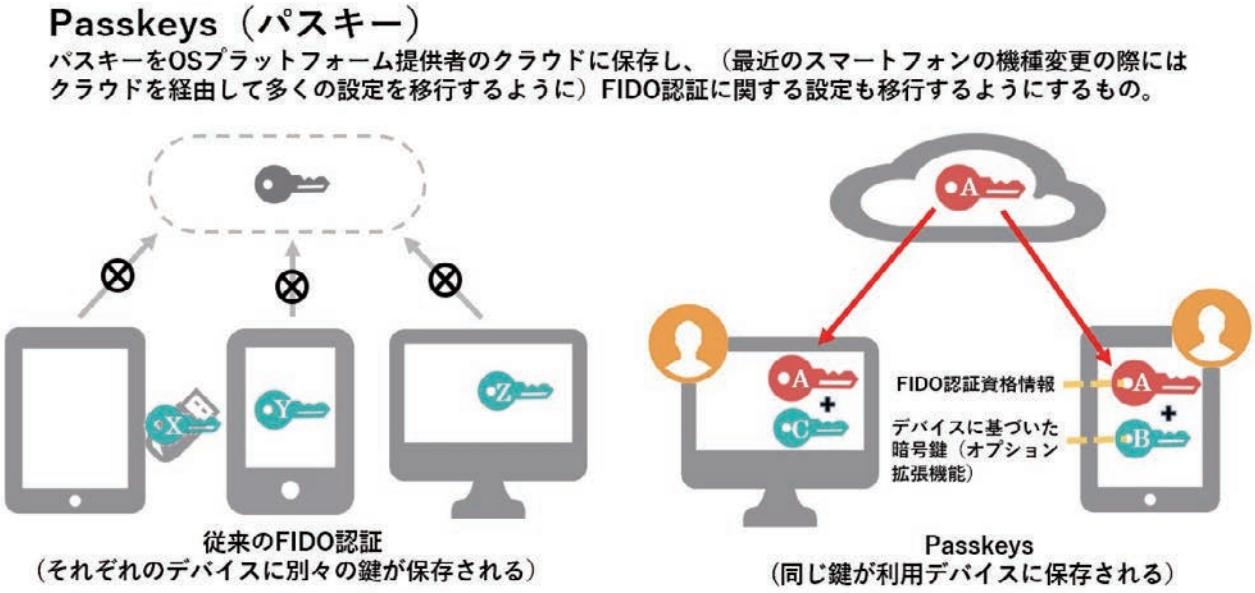
(*1) 株式会社 NTT ドコモ 『d アカウント「パスキー認証」の提供開始について』
（https://id.smt.docomo.ne.jp/src/utility/notice_20230313.html ）

(*2) Google Inc. 『The beginning of the end of the password』
（https://blog.google/technology/safety-security/the-beginning-of-the-end-of-the-password/ ）

(*3) FIDO Alliance 『Passkeys (Passkey Authentication)』
（https://fidoalliance.org/passkeys/ ）

② （狭義の）パスキー

従来の FIDO 認証では、以下の図左のように秘密鍵をユーザのデバイスから外に出さないことで安全性を高めていました。しかし、この方式では、デバイスの紛失やスマートフォンの機種変更など、認証器が使えなくなると認証不可能となり、新しいデバイスの再登録が必要となり、パスワード認証と比較して利便性が低下しました。この問題を解決するため、図右のように秘密鍵とそのメタデータに相当する「FIDO 認証資格情報（FIDO クレデンシャル）」をクラウド経由で同期し、複数のデバイスで利用できるようにする仕組みが考案されました。この仕組みまたは、FIDO クレデンシャルそのものを「（狭義の）パスキー」と呼びます。すなわち「（広義の）パスキー」とは、FIDO 認証の拡張技術と考えることができます。



図：従来の FIDO 認証と Passkeys（パスキー）の比較

出典： FIDO アライアンス資料(*1)を基に大和総研作成

パスキーの利点

パスキーは、以下のような利点があります。

① フィッシング攻撃に対する耐性が高い

パスキーにはサイトのドメイン情報がメタデータとして保存されています。WebAuthn は、ドメインを確認した上で認証情報を渡す仕様であり、ドメイン情報が一致しないと認証できません。このためドメインを本物に似せたフィッシングサイトに情報が渡されることはなく、フィッシングは実質不可能となります。ユーザ側もアクセス先の URL に注意する必要はありません。

(*1) FIDO Alliance 『What are Passkeys? -パスキー解説』
（https://media.fidoalliance.org/wp-content/uploads/2022/12/Keiko-Itakura_What-are-Passkeys-final-as-of-Dec-12.pdf ）

② ローカル認証である

パスキーによる認証ではユーザ側のデバイス上で生体認証などのローカル認証が必須です。パスワードによる認証ではユーザが入力したパスワードをサーバーに送りチェックしますが、パスキーによる認証ではローカル認証で取り出した秘密鍵でサーバーから送信されたデータに署名し、サーバーに送ります。サーバーでは公開鍵を使って署名を検証します。秘密情報となる生体情報などはネットワークに送られないため、ユーザのプライバシーも守られ安全です。

③ 不正アクセスが困難

パスキーなど FIDO 認証を行っているサイトに対し、不正アクセスで認証を突破するには、「秘密鍵」と「秘密鍵を取り出すための認証情報（生体情報など）」が必要となります。万一攻撃者がユーザのデバイスを不正入手したとしても、秘密鍵を利用するためには認証器を通した生体認証などが必要であり、本人以外のアクセスは困難な仕組みとなっています。

パスキーの課題

有望な技術であるパスキーですが、以下のような課題があります。

① パスキーの同期について

パスキーをクラウド上に保存し同期することにより、スマートフォンの機種変更のように新しいデバイスを容易に認証でき、利便性は向上しました。しかしながら、利便性とセキュリティ強化はトレードオフです。FIDO アライアンスは、「パスキー同期はエンドツーエンドで暗号化され、同期プロバイダーは強力なアカウントセキュリティ保護を備えています」と FAQ の中で答えています(*1)が、金銭を扱うオンラインバンキングなどでは、多少利便性が低下しても従来の FIDO 認証のようにデバイスを固定する仕組みを用いることも検討すべきと考えられます。

② 現状では、パスキー対応のサイト・サービスが少ない

d アカウントや Google アカウントなどが対応したことで、パスキーの利用は確実に拡大していくと思われます。しかし登場して間もない技術であるため、現状では対応するサイトやサービスがまだ少ない状況です。今後は各社の対応次第ですが、当面はパスワード認証についても認証アプリと組み合わせた二要素認証などでセキュリティを強化しながら継続されると考えられます。

最後に

サイバー攻撃手法は日々巧妙化しており、パスワードによる認証は限界に達していると思われます。パスワードを使用せずにユーザ側の利便性や導入の容易さも考慮した上で、セキュリティの高さも両立される新技術である「パスキー」には、パスワードレスの世界を大きく広げる可能性があり、期待が高まります。今後の動向に注目していきたいと思います。

(*1) FIDO Alliance『FAQ’s“ISN’T IT UNSAFE FOR PASSKEYS TO LEAVE THE DEVICE AND BE SYNCED TO OTHER DEVICES?”』（ https://fidoalliance.org/passkeys/#faq ）

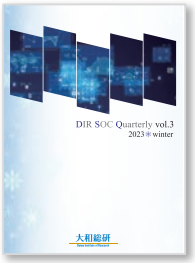
バックナンバーはこちら

DIR SOC Quarterly 2022 the first issue （2022 年 9 月 29 日発行）

- 『サイバーセキュリティ 2022（2021 年度年次報告・2022 年度年次計画）』の決定
- 経済安全保障推進法の成立
- ランサムウェアによる事業停止

DIR SOC Quarterly 2022 vol.2 （2022 年 11 月 21 日発行）

- 『クラウドサービスの利用・提供における適切な設定のためのガイドライン（案）』に対する意見募集
- 多発するクラウド設定ミスによる情報漏洩
- SBOM



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

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

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「WORLD」（ワード）を開設しました。

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4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
●MLOps	●eKYC	●マルチクラウド	●暗号資産（仮想通貨）
●マルチモーダルAI	●ゼロトラスト	●データマネジメントプラットフォーム	●セキュリティ・トークン・オファリング（STO）
●ニューラルネットワーク		●ノーコード開発/ローコード開発	

つながる　IT技術とビジネスをつなぐ深掘り解説

ビジネスでの活用が見込まれる技術を深掘り。技術発展の背景、関連技術の紹介や導入における注意点など、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