DIR SOC Quarterly

2023 autumn vol.6

わが国の政策・法制度の動向

わが国の『サイバーセキュリティ2023』の公表

トピックス

DMARCの導入にかかわる動向

大和総研
Daiwa Institute of Research

目次

はじめに……2

第 1 部：わが国の政策・法制度の動向

1. 『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……3
2. 『金融機関等コンピュータシステムの安全対策基準・解説書』（第 11 版）の公表……5
3. 『政府機関等のサイバーセキュリティ対策のための統一基準群』（令和 5 年度版）を策定……7
4. 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……9
5. 『金融機関のシステム障害に関する分析レポート』の公表……11

第 2 部：インシデント事例の紹介

1. ランサムウェアによる名古屋港のシステム障害……13
2. 多数の米国大手エネルギー企業が QR コードを悪用したフィッシング攻撃の標的に……16

第 3 部：トピックス

1. DMARC の導入にかかわる動向……18
2. 新しい DNS キャッシュポイズニング攻撃 MaginotDNS と Black Hat について……22

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 2 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。

日本を取り巻くサイバー空間の情勢や政府の今後取り組む施策等についてまとめられた『サイバーセキュリティ 2023』が公表されました。また FISC(The Center for Financial Industry Information Systems：公益財団法人金融情報システムセンター)は、最近金融機関でも利活用が進んでいるクラウドサービスの導入・運用時の参考となる『金融機関等コンピュータシステムの安全対策基準・解説書』（第 11 版）を公表しました。いずれも第 1 部にてその概要を紹介しておりますが、本ガイドラインは金融機関が情報システムを構築する際の安全対策基準として事実上の標準となっているため、今後強化していく施策等を各社が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、日本ではまだあまり馴染みのない QR コードを使用したフィッシングメール詐欺に関して紹介しています。企業のセキュリティシステムでは、画像である QR コードはメール本文記載の URL よりも検疫される可能性が低いため、今後日本でもこのような攻撃が実行されるかもしれません。対策はフィッシングメール対策と同じくメールに記載された QR コードを安易に読み取らないことになりますが、対策の 1 つとなりうる送信メールのなりすましを防止する DMARC という技術の解説、併せて政府機関や業界団体の動向を第 3 部にて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 10 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 2023（2022 年度年次報告・2023 年度年次計画）』の公表

概要

政府は 2023 年 7 月 4 日、『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）』（以下、「サイバーセキュリティ 2023」と略記）を決定し、公表しました (*1)。「サイバーセキュリティ 2023」は、下表に示すサイバーセキュリティ基本法の政策目的とサイバーセキュリティ戦略（2021 年 9 月 28 日決定）の施策推進の方向性に従って整理されており、日本を取り巻くサイバー空間の情勢や政府のこれまでの取り組み実績、今後取り組む施策等についてまとめられています。

サイバーセキュリティ基本法が定める 3 つの政策目的
経済社会の活力の向上及び持続的発展
国民が安全で安心して暮らせる社会の実現
国際社会の平和及び安全の確保並びに我が国の安全保障に寄与すること
サイバーセキュリティ戦略の 3 つの施策推進の方向性
デジタル改革を踏まえたデジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進
公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保
安全保障の観点からの取組強化

出典：「サイバーセキュリティ 2023」の内容を基に大和総研作成

「サイバーセキュリティ 2023」の構成は前年度と同様に「第 1 部 サイバーセキュリティ 2023 のポイント（エグゼクティブ・サマリー）」、「第 2 部 サイバーセキュリティに関する情勢」及び「第 3 部 サイバーセキュリティ戦略に基づく昨年度の取組実績・評価及び今年度の取組」の 3 部構成となっています。

今年度特に強力に取り組む施策

政府は昨今の厳しく複雑な国際情勢等を背景に、昨年 12 月に「国家安全保障戦略」（2022 年 12 月 16 日決定）を策定しました。同戦略では、サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するため、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させることが必要である旨が示されています。

今年度においては、この国家安全保障戦略の趣旨を踏まえつつ、サイバーセキュリティ戦略の 3 つの方向性に基づいて施策を推進していくこととしており、特に強力に取り組む施策として、次ページの施策が選出されています。

なお、次ページの表の①④⑤ の施策については、昨年度も選出されていますが、引き続き施策を推進する必要があるため、今年度においても選出された施策となっています。

(*1) https://www.nisc.go.jp/pdf/policy/kihon-s/cs2023.pdf

①　中小企業のサイバーセキュリティ対策
サプライチェーンの中でも比較的弱い中小企業へのサイバー攻撃を経由して、発注元の大企業も被害を受けている実態への取組強化が必要であるため「サイバーセキュリティお助け隊サービス (*1)」の拡充や普及拡大を実施するなどの中小企業への支援を行い、サプライチェーン全体のサイバーセキュリティの底上げを図る。
②　サプライチェーン・リスクを踏まえたソフトウェアセキュリティの高度化に関する取組
脆弱性情報と SBOM（Software Bill of Materials）(*2)の機械的な紐付けに係る実証を行うなど、2022 年度までの取組を深化させ、ソフトウェアセキュリティの高度化に向けた取組を進める。また、代表的な通信システムを対象に SBOM を作成・評価するなど、通信分野での SBOM 導入に向けた取組を進める。
③　政府情報システムの防護のための一元的な取組
政府統一基準群の改定及びこれを踏まえた情報セキュリティの確保を図り、政府機関等における情報システムのレジリエンスの向上を図る。また、安全性や透明性の検証が可能なセンサーを政府端末に導入して、海外製品に頼らずに端末情報を収集し、日本独自のサイバーセキュリティ関連情報を生成する。
④　医療分野をはじめとする重要インフラ事業者等のサイバーセキュリティ強化
安全基準等策定指針の改定等を通じ、重要インフラ事業者等において、組織統治にサイバーセキュリティを組み入れるための取組が推進され、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応が一層促進されるよう努める。
⑤　インド太平洋地域における能力構築支援の推進（ASEAN 官民連携支援及び島しょ国支援の強化）
インド太平洋地域のセキュリティ対策支援は、この地域のみならず国際社会全体の平和維持と産業発展に欠かせない活動であるため、官民連携等の強化、サイバーセキュリティ演習をはじめとする各種演習やイベント、外国捜査機関等に対する支援などを通して、インド太平洋地域を含む途上国のサイバー分野に係る人材育成を含む能力構築支援の強化等に取り組む。
⑥　日米豪印上級サイバーグループ会合及びランサムウェア対策多国間会合の枠組みを通じた国際連携
日米豪印において、重要インフラ防護、ソフトウェアセキュリティに関する 4 か国の共通原則の策定・実施やインド太平洋地域における能力構築プログラム・啓発活動の協調等を図る。また、ランサムウェア対策において、同志国との間での我が国の官民連携に係る知見の共有や国際的な情報共有に向けた検討へ参加する。

出典：「サイバーセキュリティ 2023」の内容を基に大和総研作成

最後に

「サイバーセキュリティ 2023」の公表により、今後政府が取り組む施策の具体的な内容が明らかになりました。中小企業への支援やソフトウェアセキュリティの高度化、政府情報システムの防護といった施策から、サプライチェーンのセキュリティ強化が重要視されていることがうかがえます。特に②のソフトウェアのサプライチェーン強化として期待されている SBOM については、有識者の意見として「SBOM は国内だけでなく、同盟国・友好国とも協調した取り組みが必要であり、バリューチェーン・サプライチェーンに参加するための必須要件（国際資格）と考えるべきである。」という旨が記載されています。そのため、現状国内で SBOM 管理を実用化している企業は少ないと考えられますが、今後は各企業に対して SBOM の導入を求める動きが活発化することが予想されます。

(*1) 中小企業等に対するサイバー攻撃への対処として不可欠なサービスをワンパッケージで安価に提供するサービス。

(*2) 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」とも呼ばれます。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. 『金融機関等コンピュータシステムの安全対策基準・解説書』（第 11 版）の公表

第 11 版の公表

公益財団法人金融情報システムセンター（FISC：The Center for Financial Industry Information Systems、以下 FISC と略記）は、2023 年 5 月に『金融機関等コンピュータシステムの安全対策基準・解説書』（第 11 版）(*1)を公表しました。昨今、金融機関においてクラウドサービスの利用が拡大していることを受け、第 11 版ではクラウドサービスを導入・運用する際の留意事項が基準項目に取り込まれました。

FISC 安全対策基準・解説書とは

『金融機関等コンピュータシステムの安全対策基準・解説書』は、FISC が刊行している金融業界向けのセキュリティ対策基準です。初版は 1985 年に刊行され、その後も金融機関を取り巻く環境の変化に応じて改訂を重ねています。かつては金融庁が金融機関を検査する際の「金融検査マニュアル」で参照されており、検査官が必要に応じて、この安全対策基準・解説書に基づいて確認を行っていました。現在は「金融検査マニュアル」は廃止されていますが、金融機関ではこの安全対策基準・解説書を基にシステムを構築・点検することが定着しており、事実上の標準（デファクトスタンダード）となっていると言えます。

今回の改訂の経緯と改訂内容

FISC はこれまでもクラウドサービス利用にかかわる考え方や管理基準を「安全対策基準・解説書」に取り込んできました。たとえば 2013 年刊行の第 8 版追補や 2015 年刊行の第 8 版追補改訂ではクラウドサービス利用にかかわる安全対策基準を追加・拡充しました。また 2018 年刊行の第 9 版では、外部委託基準とクラウド基準の整理・統合やクラウドサービス固有のリスク管理基準の追加などを行いました (*2)。

2021 年には、金融機関においてクラウドサービスの利用が拡大する中、クラウドサービスを導入・運用する際に安全対策基準をどのように適用するかについての解説が求められていたことを背景として、「金融機関等におけるクラウド導入・運用に関する解説書策定に関する有識者検討会」を設置しました。そして、この検討会での検討結果を「金融機関等におけるクラウド導入・運用に関する解説書(試行版)」として刊行しました (*3)。

(*1) FISC 『『金融機関等コンピュータシステムの安全対策基準・解説書』（第 11 版）【PDF 版】』（ https://www.fisc.or.jp/publication/academic/005831.php ）

(*2) FISC 『安全対策基準（第 9 版）の改訂概要』（ https://www.fsa.go.jp/singi/kessai_kanmin/siryou/20171220/04.pdf ）

(*3) FISC 『金融機関等におけるクラウド導入・運用に関する解説書（試行版）PDF 版』（ https://www.fisc.or.jp/publication/book/004842.php ）

この解説書は、『金融機関等コンピュータシステムの安全対策基準・解説書』を補足する位置づけの文書であり、およそ 1 年後を目途に試行結果を確認のうえ、試行版の確定または安全対策基準への取込みを検討する予定としていました。

今回の第 11 版は、上述の約 1 年間の試行期間に得られた知見や、金融機関等から寄せられた質問・意見を踏まえ、試行版解説書に記載されていたクラウドサービス固有で対応すべき事項や特に留意すべき事項、参考情報などを「安全対策基準・解説書」に取り込んだものです。

一例をあげると、「蓄積データの漏洩防止策」については、セキュリティ基準を充足しているかを確認するために、クラウド事業者に対して、暗号鍵のアクセス権や暗号化設定の範囲や強度などを確認すべきであるなどと解説が追加されています。またそれに加えて参考情報として、クラウド事業者が提供する保存データの暗号化機能の種類が分類・列挙されています。

最後に

今回の改訂により、クラウドサービスを導入・運用する際に FISC の安全対策基準をどのように適用すれば良いかがより明確になりました。

ただし、FISC の安全対策基準は合計 313 項目もあります。特に初めてクラウドサービスを利用する場合、全ての項目についてクラウドサービス事業者側の対応状況を調査したり、自社でどのような対応が必要かを確認したりするのは非常に手間がかかります。そのような場合、クラウドサービス事業者やそのパートナー企業が公開しているリファレンスガイドも併せて参照すると良いでしょう。このようなリファレンスガイドには、クラウドサービス事業者が FISC 安全対策基準の各項目についてどのように対応しているのか、また利用企業側がどのような対応をする必要があるのかなどについて記載されています。

また安全対策基準が 313 項目もあると準拠すること自体が目的化して、安全対策基準の本来の目的を見失ってしまうかもしれません。しかし、セキュリティ対策基準やガイドラインなどは本来、網羅的で質の高いセキュリティ対策を実装する助けとなるものです(*1)。FISC の安全対策基準も非常に網羅的なものであり、その意味では活用する価値の高いものと言えます。前述のクラウドサービス事業者やそのパートナー企業が提供するリファレンスガイドなども参照しながら、積極的に活用していくと良いでしょう。

(*1) 大和総研『セキュリティフレームワーク - 抜け漏れのないセキュリティ対策への近道 -』
（ https://www.dir.co.jp/world/entry/solution/security-framework ）

3. 『政府機関等のサイバーセキュリティ対策のための統一基準群』（令和 5 年度版）を策定

サイバーセキュリティ対策のための統一基準群策定

政府は 2023 年 7 月に『政府機関等のサイバーセキュリティ対策のための統一基準群』（以下、統一基準群と略記）の令和 5 年度版を策定し、公開しました。内閣サイバーセキュリティセンターの Web ページ(*1)によると、「統一基準群は、国の行政機関及び独立行政法人等（以下「政府機関等」という。）の情報セキュリティ水準を向上させるための統一的な枠組みであり、政府機関等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定」しているもので、以下の 3 つの文書から構成されます。

① **政府機関等のサイバーセキュリティ対策のための統一規範**

政府機関等がとるべき対策の統一的な枠組みを定めたもの。

② **政府機関等のサイバーセキュリティ対策のための統一基準**

情報セキュリティ対策の項目ごとに政府機関等が遵守すべき事項を規定。

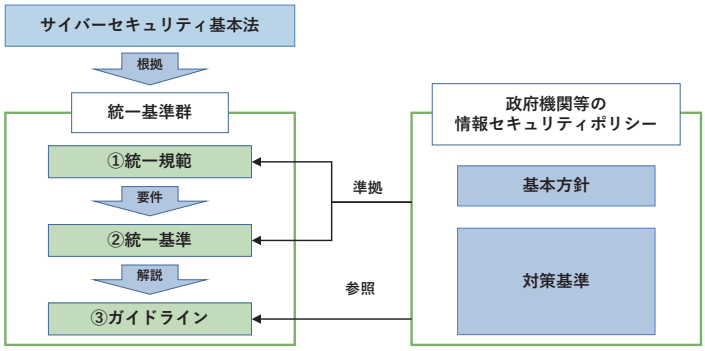
機関等の情報セキュリティ水準の斉一的な引上げを図ることが目的。

③ **政府機関等の対策基準策定のためのガイドライン**

統一基準の遵守事項に対応した基本対策事項を例示。

併せて対策基準の策定及び実施に際しての考え方等を解説。

政府機関等は、自組織の特性を踏まえつつ、統一規範や統一基準に準拠した情報セキュリティ対策の基本方針と対策基準を定める必要があります（下図）。



図：統一基準群と政府機関等の情報セキュリティポリシーの関係

出典：内閣サイバーセキュリティセンター『政府機関等のサイバーセキュリティ対策のための統一基準群の改定のポイント』(*2)を基に大和総研作成

(*1) https://www.nisc.go.jp/policy/group/general/kijun.html

(*2) https://www.nisc.go.jp/pdf/policy/general/rev_pointr5.pdf

今回の改定内容

統一基準群はサイバーセキュリティ基本法第 26 条第 1 項第 2 号に基づいて策定されているもので、およそ 2 年に 1 度改定されています。今回の改定では、たとえば下表のようなセキュリティ対策の強化などが盛り込まれました。

改定ポイント	改定の主な内容についての解説
情報セキュリティに関するサプライチェーン対策の強化	業務委託先などサプライチェーンの脆弱な部分を起点としたサイバー攻撃によるリスクが増大していることを踏まえ、政府機関等が業務委託先に実施を求めるべき情報セキュリティ対策が大幅に具体化されました。この情報セキュリティ対策は、米国 NIST(*1)が策定・公表している情報セキュリティ基準 SP 800-171 を参考にしており、インシデント対処能力の確立・維持、情報へのアクセス制御、ログの取得・監視など 8 類型が規定されています。業務委託先の企業は委託期間を通じてこれら 8 類型すべての対策を実施する必要があります。「業務委託先」には、再委託先、再々委託先など多段階の委託先を含みますので、多くの民間企業が影響を受けるものと推測されます。
クラウドサービスの利用拡大を踏まえた対策の強化	政府機関等が利用するクラウドサービスは原則として ISMAP または ISMAP-LIU(*2)のクラウドサービスリストから選定することが明記されました。したがって、今後は ISMAP や ISMAP-LIU のクラウドサービスリストに登録されていないクラウドサービスは政府機関等から原則として選定されなくなります。
サイバーレジリエンスの強化	サイバー攻撃を受けることを念頭に、情報システムの構築時に復旧手順を整備することや運用時には適切なバックアップの取得、復旧手順・バックアップ要件の定期的な見直しが必要であると明記されました。

出典：内閣官房 内閣サイバーセキュリティセンター 政府機関総合対策グループ『政府機関等のサイバーセキュリティ対策のための統一基準群の改定のポイント』(*3)を基に大和総研作成

最後に

今回の統一基準等の改定において、サプライチェーン対策の強化が盛り込まれましたが、近年、サプライチェーンリスクは民間企業にとっても重大な問題となっています。今後は、政府機関等が関係しない、民間企業のみから構成されるサプライチェーンでも、NIST SP 800-171 を参考にした情報セキュリティ対策が求められる場面が増える可能性があり、留意が必要です。

また、サイバーセキュリティを含む IT レジリエンスの強化は、昨今の金融業界でも大きな課題となっています。これについては本冊子の「5.『金融機関のシステム障害に関する分析レポート』の公表」で詳しく解説していますのでご参照ください。

(*1) 正式名称は、米国国立標準技術研究所（National Institute of Standards and Technology）です。

(*2) ISMAP は政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録する制度です。また、本制度のうち、リスクの小さな業務・情報の処理に用いる SaaS サービスを対象とするのが ISMAP-LIU です。

(*3) https://www.nisc.go.jp/pdf/policy/general/rev_pointr5.pdf

4. 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

概要

米国証券取引委員会（以下、SEC）は 2023 年 7 月 26 日、上場企業に対してサイバーセキュリティに関する重大インシデントの発生状況の開示と、サイバーセキュリティのリスク管理、戦略、ガバナンスに関する重要情報の年次開示を義務付ける規則を採択しました。加えて、海外民間発行体（FPI）にも同等の開示を義務付ける規則も採択しました。本改定は 2023 年 8 月 4 日に連邦官報(*1)へ掲載され、2023 年 9 月 5 日から有効になりました。

本改定の概要は次のとおりです：

項目	開示要件の概要
Regulation S–K (*2) Item 106(b) Risk management and strategy（リスク管理及び戦略）	登録者は、サイバーセキュリティの脅威から生じる重大なリスクの評価、特定、管理のためのプロセスがある場合にはそれを記述し、サイバーセキュリティの脅威から生じるリスクが事業戦略、経営成績、財務状況に重大な影響を与えたか、または与える可能性が合理的にあるかどうかを説明しなければならない。
Regulation S–K Item 106(c) Governance（ガバナンス）	登録者は以下を行う必要がある： -サイバーセキュリティの脅威によるリスクに対する取締役会の監督について説明する。 -サイバーセキュリティの脅威による重大なリスクの評価と管理における経営陣の役割を説明する。
Form 8–K (*3) Item 1.05 Material Cybersecurity Incidents（重要なサイバーセキュリティインシデント）	登録者は、重要であると判断されたサイバーセキュリティインシデントに遭遇した場合、その重要な点について開示しなければならない： -インシデントの性質、範囲、時期。 -影響または合理的に起こりうる影響。 Form 8-K Item 1.05 は、インシデントが重要であると判断されてから 4 営業日以内に提出されなければならない。但し、米国司法長官が、即時開示が国家安全保障または公共の安全に対する実質的なリスクをもたらすと判断した場合、登録者は提出を延期することが出来る。登録者は、Item 1.05(a)で求められている情報のうち、最初の Form 8-K 提出時に確定していなかったもの、または入手できなかったものを開示するため、以前の Form 8-K Item 1.05 を修正しなければならない。
Form 20–F (*4)	FPI は以下を行う必要がある： -サイバーセキュリティの脅威によるリスクに対する取締役会の監督について説明する。 -サイバーセキュリティの脅威による重大なリスクの評価と管理における経営陣の役割を説明する。
Form 6–K (*5)	FPI は、外国の司法管轄区、証券取引所、または証券保有者に対して開示または公表する重要なサイバーセキュリティインシデントに関する情報を Form 6-K に記載しなければならない。

出典：Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure を基に大和総研作成

(*1) Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896 (Aug. 4, 2023)

(*2) 登録者が登録届出書、定期報告書及びその他の提出書類において、事業の重要な定性的記述事項をどのように開示すべきかを概説する規則です。

(*3) アメリカ企業に対して SEC への提出を義務付けている報告書で、臨時報告書に相当します。

(*4) 外国企業に対して SEC への提出を義務付けている報告書で、年次報告書に相当します。

(*5) 外国企業に対して SEC への提出を義務付けている報告書で、臨時報告書に相当します。

背景

本改定以前にサイバーセキュリティに関するリスクやインシデントについて明示的に言及した開示要件はありませんでしたが、一部の登録者は自主的にインシデントを報告していました。その形式は企業によって異なり、 SEC のレビューによれば記載されたインシデントに関する情報の具体性も様々でした。加えて、開示の多くは Form 10-K(*1)の「リスク要因」のセクションで行われていましたが、関連性のない他の開示と共に記載されていました。そのため、投資家がサイバーセキュリティに関して提供された情報を見つけ、解釈し、分析することが困難となっていました。

また、近年ではサイバーセキュリティインシデントによるコストや悪影響は増大し、ランサムウェアやブラックマーケットの存在によってその発生頻度も高まっています。そのため、投資家や他の市場参加者はサイバーセキュリティに関するよりタイムリーかつ信頼性の高い情報を必要としています。従って、サイバーセキュリティに関して一定の水準や形式で開示が行われるように本改定が行われました。

本改定のポイント

本改定の内容は主に次の 3 点になります：

1. 重要であると判断したサイバーセキュリティに遭遇した場合、Form 8-K Item 1.05 に基づく報告書は原則としてその状況等を 4 営業日以内に開示しなければならない（Form 8-K General Instruction B. 1.）。
2. 年次報告書において、サイバーセキュリティの脅威から生じるリスクの評価等を行うプロセスやそのリスクの影響、サイバーセキュリティの脅威に対する取締役会の監督及び役割について説明しなければならない（Form 10-K General Instruction G (2)及び Part I. Item 1C）。
3. 海外民間発行体に対しても同様の開示を求める（ Form 6-K General Instruction B 及び Form 20-F Item 16K）。

本改定により、これまでと比べて、サイバーセキュリティインシデントを迅速に分析し対応するための優れたサイバーセキュリティ体制が、そして経営陣にはサイバーセキュリティに対するより深い理解や専門的な知識が求められるようになります。

国際社会はサイバーセキュリティへ力を入れており、日本も例外ではありません。そのため、いずれ日本でも本改定と同様の法令等が導入されるかもしれません。本改定への米国企業や米国市場に上場する日本企業の対応は参考になることでしょう。

(*1) アメリカ企業に対して SEC への提出を義務付けている報告書で、年次報告書に相当します。

5. 『金融機関のシステム障害に関する分析レポート』の公表

概要

金融庁は 2023 年 6 月 30 日、『金融機関のシステム障害に関する分析レポート』を公表しました(*1)。本レポートは 2019 年以降毎年公表されており、今回は 2022 年度（2022 年 4 月～2023 年 3 月）のシステム障害の傾向に加え、2018 年 7 月から 2023 年 3 月までのシステム障害のうち代表的な事例の事象、原因及び対策についてまとめられています。

2022 年度の主なシステム障害傾向

2022 年度のサイバーセキュリティに関係する主な障害傾向は以下のとおりです。

2022 年度の主な障害傾向（サイバーセキュリティ関係）	分析・考察
・外部委託先のシステムへの外部からの不正アクセスにより、大量の顧客情報漏えいが発生。 ・外部委託先を含む金融機関への DDoS 攻撃により、金融機関のホームページの閲覧ができなくなる等の事案が発生。 ・サポート期限切れの機器を使用したことに起因した脆弱性に対する外部からの不正アクセスによるランサムウェア被害や、なりすましメールに添付されたファイルを開封したことにより、エモテットに感染する事案が発生。	・重要な外部委託先も含めたサイバーセキュリティ対策等の整備状況の把握及びその実効性の検証といった IT レジリエンスの向上が必要である。 ・IT 資産の適切な管理や不審メール受信時の対応といった基本的な対策を実施するための態勢整備が引き続き課題となっている。 ・経営陣がサイバーセキュリティを含む IT レジリエンスの強化（重要な外部委託先を含む。）を主導すること、その下で、経営上の計画における施策を策定するとともに実施すること、必要なリソース（予算及び人材）を確保するとともに適切に配置すること、インシデント対応においては顧客目線での対応、インシデントの影響の最小化、重要業務の早期復旧等を実現させるための態勢整備を行うことが、依然として金融業界の課題となっている。

出典：『金融機関のシステム障害に関する分析レポート』（金融庁）を基に大和総研作成

近年、金融機関の IT システムの複雑化、IT システムの委託関係の複雑化・相互接続の進展に加え、「サイバー攻撃の高度化」などにより多くの顧客に影響を及ぼす事案が発生しており、サイバーセキュリティを含めた IT リスク管理態勢の強化、特に、障害発生時の業務の早期復旧や顧客影響の軽減（レジリエンス）の強化が一層求められています。

事案例・課題・今後の金融庁の対応

サイバーセキュリティに関係するシステム障害の端緒となる「サイバー攻撃・不正アクセス等の意図的な行為」の事案例と課題、および今後の金融庁の対応は以下のとおりです。公表された 3 つの特徴的な事例は、サイバーセキュリティ事例として従来指摘されていた一般的なものであると見受けられます。

(*1) 金融庁『「金融機関のシステム障害に関する分析レポート」の公表について』
（https://www.fsa.go.jp/news/r4/sonota/20230630-2/20230630-2.html ）

事案例		課題	今後の金融庁の対応
I	外部委託先への不正アクセスによる情報漏えい	委託元における外部委託先の情報セキュリティ管理態勢に関する実効性の検証、および、委託元における外部委託先のデータ管理態勢の実効性の検証。	サイバーリスクの趨勢を踏まえ、金融機関のサイバーセキュリティ管理態勢の実効性について検査を通じて検証（サイバーセキュリティ管理態勢に関するモニタリング）するとともに、地域金融機関、証券会社、保険会社等に対しては、サイバーセキュリティに関する自己評価の実施を求める。加えて、金融業界横断的なサイバーセキュリティ演習を実施し、金融業界のインシデント対応能力の底上げを図る。
II	マルウェア感染	IT 資産の適切な管理等といった基本的な対策を組織全体に浸透させる取組を行うこと、不正な通信を検知するためのシステム・体制の整備、不正な外部サーバーとの通信制御等のマルウェア対策、不審メール受信時等の対応態勢整備はもとより、重要な外部委託先を含め、定期的な訓練等による実効性の確保。	
III	DDoS 攻撃	アクセス制限や DDoS 対策ツールの導入といった基本的な対策はもとより、外部委託先を含め、障害発生時の部署間の連絡体制等をあらかじめ整備すること。	

出典：『金融機関のシステム障害に関する分析レポート』（金融庁）を基に大和総研作成

金融庁の対応として、サイバーセキュリティ管理態勢に関するモニタリング、自己評価の実施を求めることに加えて、演習を実施しインシデント対応能力の底上げを図ることが示されています。

サイバーセキュリティに起因した新規システム障害事例

今回金融庁では、「サイバー攻撃・不正アクセス等の意図的な要因から発生したシステム障害」として 19 事例を公表しています。この内以下の 8 事例が新規で本レポート初掲載となります。

新規掲載事例（「サイバー攻撃・不正アクセス等の意図的なもの」の内）		業態
1	外部委託先における認証設定の不備による情報漏えい	保険会社等
2	外部委託先への DDoS 攻撃	信用金庫・信用組合等
3	金融機関のエモテット感染の疑い	信用金庫・信用組合等
4	顧客口座に対する不正アクセス	金融商品取引業者等
5	多数の IP アドレスを使用した DDoS 攻撃	金融商品取引業者等
6	他社システムへの DDoS 攻撃の波及によるホームページ利用不可	地域銀行
7	二要素認証設定未済利用者への不正アクセスによる暗号資産不正出庫	暗号資産交換業者
8	ランサムウェア感染に伴う情報漏えい	信用金庫・信用組合等

出典：『金融機関のシステム障害に関する分析レポート』（金融庁）を基に大和総研作成

本レポートからの示唆

本レポートからは、従来と異なる対策を求めているわけではなく、「外部委託先管理」「マルウェア対策」「DDoS 対策」といった従来からの対策をベースにそれをブラッシュアップすることの重要性がうかがえます。金融機関においては特に、本レポートや各種基準・ガイドラインなどの内容を踏まえ、自組織の体制・対策を適宜見直し、IT レジリエンスの強化を推進することが望まれます。

1. ランサムウェアによる名古屋港のシステム障害

概要

2023 年 7 月 5 日、名古屋港運協会は名古屋港統一ターミナルシステム（NUTS、 Nagoya United Terminal System）において、4 日 6 時 30 分頃からランサムウェアによるシステム障害が発生していることを公表しました (*1) 。このシステム障害によって名古屋港にある全てのターミナルが影響を受け、コンテナの積み降ろし作業などができなくなり、多くの関連事業者にも影響が波及しました。このため、報道機関でも当時大きく取り上げられました (*2) 。

本事案の時系列は下表のとおりとなっています。システムの復旧作業が完了し、全てのターミナルの作業が再開したのは 6 日 18 時 15 分頃とされており、この間、約 2 日半にわたって物流サービスの提供に支障が出ていたこととなります。

日時		内容
7 月 4 日	06:30 頃	システムの作動が停止したことを確認
	07:30 頃	システム専用のプリンターからランサムウェアの脅迫文書が印刷される
	09:00 頃	愛知県警察に通報
	14:00 頃	システムの各種サーバーが暗号化されていることが判明
7 月 5 日	12:00 頃	名古屋港運協会よりプレス発表
	21:00 頃	バックアップデータからもウイルスが検知されたため、駆除を開始
7 月 6 日	07:15 頃	バックアップデータの復元が完了したが、システムのネットワーク障害が発生
	14:15 頃	ネットワーク障害が解消し、準備が整ったターミナルより順次作業を再開
	18:15 頃	全てのターミナルの作業が再開

表：システム障害の時系列

出典：名古屋港運協会の公表資料 (*3) の内容を参考に大和総研作成

(*1) https://meikoukyo.com/wp-content/uploads/2023/07/165c5b14bf0021d077a4852f0cb232b8.pdf

(*2) 日本経済新聞　名古屋港にサイバー攻撃か システム障害、搬出入中止
(https://www.nikkei.com/article/DGXZQOFD053RH0V00C23A7000000/)

NHK　名古屋港 システム障害「ランサムウエア」感染確認 復旧急ぐ
(https://www3.nhk.or.jp/news/html/20230705/k10014119091000.html)

(*3) https://meikoukyo.com/wp-content/uploads/2023/07/0bb9d9907568e832da8f400e529efc99.pdf

感染したランサムウェアとは？

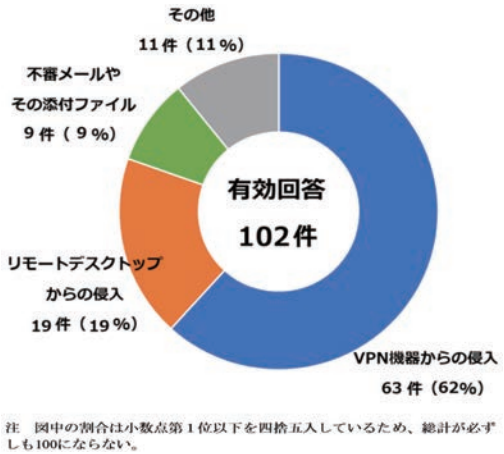
名古屋港運協会によると、システム専用のプリンターから脅迫文書が多数印刷されており、この脅迫文書にはランサムウェアである「LockBit」の感染を疑わせる英語のメッセージが確認されたとのことです。

LockBit は 2019 年 9 月頃に存在が確認されたランサムウェアの一種で、RaaS（Ransomware as a Service）(*1) と呼ばれるビジネスモデルを形成し、改良を繰り返しながら世界各地でさまざまな標的を狙う攻撃に悪用されています。過去、国内においても医療機関や大手企業などが被害に遭っており、業務に多大な支障をきたす事案が発生しています。

ランサムウェアの感染源は？

ランサムウェアに感染した原因の詳細は明らかになっていませんが、システムで利用する VPN 機器に脆弱性が存在していたことが確認されており、そこから不正なアクセスを受けたと考えられています。

警察庁の調査によると、2022 年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「VPN 機器からの侵入」が 62%を占めていました。前年の調査においても、半数以上の割合を占めており、脆弱性や強度の弱い認証情報等が放置された VPN 機器がランサムウェアの主要な感染経路として利用され続けている傾向がうかがえます。



図：ランサムウェアの感染経路

出典：警察庁「令和 4 年におけるサイバー空間をめぐる脅威の情勢等について」(*2)

(*1) サイバー犯罪グループが攻撃の実行者に対して、ランサムウェアをパッケージ化した製品として提供し、ランサムウェアの被害者から支払われた身代金を同グループと攻撃の実行者で分配するビジネスモデルのこと。

(*2) https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

政策における港湾施設の位置付けは？

政府はサイバーセキュリティ基本法において、国民生活や社会経済活動の基盤となるインフラのうち、機能が停止・低下すれば多大な影響を及ぼす恐れがある事業者を「重要インフラ事業者」として指定し、事業者が適切なサイバーセキュリティの確保に努めるように対策を講じています。一方、昨年成立した経済安全保障推進法においては、インフラサービスの安定的な提供を確保するため、基幹インフラを担う事業者のうち、一定の基準を満たす事業者を「特定社会基盤事業者」として指定し、重要な設備の導入などを行う際に政府の審査を必要とするよう定めています。

しかし今回、システム障害が発生した名古屋港を含む全国の港湾施設は、物流サービスの提供において重要な役割を担っているにもかかわらず、この「重要インフラ事業者」と「特定社会基盤事業者」のいずれにも指定されていませんでした。

今回の事案を受けて、政府は有識者らによる委員会を発足し、事案の原因究明と再発防止策を検討するとともに、両法で対象とする事業者に港湾施設を追加し、セキュリティ対策を強化することも念頭に議論を進めることとしています。

まとめ

サイバー攻撃が国民生活や社会経済活動に大きな影響をもたらす可能性があることは広く知られているところですが、本事案の発生によって、その脅威が現実のものであることを改めて認識することとなりました。今回、システム障害の発生から復旧に至るまでの期間が約 2 日半だったこともあり、物流サービスに致命的な影響を与えるほどの事態にはならなかったとの見解もありますが、政府においても委員会を発足してサイバーセキュリティ基本法や経済安全保障推進法における制度の対象とすることを検討するなど、本事案を非常に重く受け止めていることがわかります。

「LockBit」による被害は、組織の規模や業界を問わず、さまざまな組織で確認されています。このことから、名古屋港のシステムが標的となった理由も、日本の物流サービスの混乱を狙ったものではなく、攻撃者が幅広く標的を探していたところ、たまたま脆弱性のある VPN 機器が外部から接続可能な状態となっていたために狙われたものと考えられます。

そのため、どのような企業においても同様の被害に遭う可能性は十分にあることを認識し、本事案を教訓として、今一度自社の状況を確認するなど、適切なセキュリティ対策を講じていくことが大切です。

2. 多数の米国大手エネルギー企業が QR コードを悪用したフィッシング攻撃の標的に

概要

2023 年 8 月 16 日（現地時間）、米国セキュリティ企業の Cofense は、米国に拠点を置く大手エネルギー企業を標的とした、QR コードを用いた大規模なフィッシングキャンペーンが観測されたことを発表しました(*1)。

Cofense の発表によりますと、2023 年 5 月以降攻撃を観測しており、このキャンペーンにおける 1,000 通以上の悪意のある QR コードを含むメールの内、約 29%が米国の大手エネルギー企業を標的としたものでした。その他製造業、保険業、IT、金融サービスも標的になっています。2023 年 5 月より悪意ある QR コードフィッシング量が 25 倍以上に増加しています。当該フィッシングメールは、Microsoft 365 アカウントのセキュリティ更新通知を騙っており、QR コードの変換先 URL は、大部分が Bing のリダイレクト機能を使ってフィッシングサイトに誘導する構成でした。Bing の他にも krxd[.]com（Salesforce アプリ関連）や cf-ipfs[.]com（Cloudflare の Web3 サービス関連）などのドメインも利用されていました。Cofense においては、QR コードを利用したこのような大規模なキャンペーンを歴史上見たことがなく、悪意ある攻撃者が実行可能な攻撃ベクトルとして QR コードの実効性をテストしている可能性があると指摘しています。

QR コードを用いたフィッシング攻撃(Quishing)

QR コードを用いたフィッシング攻撃は、別名「Quishing」と呼ばれます。攻撃者は下図のような QR コードを埋め込んだメールを標的に配信し、QR コードがスキャンされることを狙っています。

図：QR コード画像サンプル

出典：Cofense 発表資料(*1)

(*1)　Cofense.『Major Energy Company Targeted in Large QR Code Phishing Campaign』
（https://cofense.com/blog/major-energy-company-targeted-in-large-qr-code-campaign/ ）

QR コードは、メール本文や添付の PDF ファイル内に画像として埋め込まれています。 Cofense の発表資料でも述べられているように、フィッシングリンクをメール本文に記載した場合は、企業のセキュリティシステムで検疫される可能性が高いですが、画像である QR コードの内部に隠されたフィッシングリンクは、セキュリティシステムを突破して標的の受信トレイに到達する可能性が高くなります。また、QR コードを個人所有のデバイスでスキャンした場合は、企業のセキュリティシステムの保護の外に置かれることになり危険性が増大します。一方で、Quishing は攻撃を成功させるために標的が QR コードをスキャンする必要があるため、サイバー犯罪者の間では人気がない攻撃手法とされています。今回の大規模キャンペーンでは、Bing のような有名な URL を用いていることを含め、攻撃者が Quishing の実効性を高めるため試行錯誤している可能性が高いと考えられます。

QR コード利用時の注意点

QR コードを利用する際は、メールに記載された URL をクリックする際と同様、以下の点に注意し詐欺被害などを防止することが望まれます。

- 知らない送信元からのメールに記載された QR コードはスキャンしない
- サイト（URL）を開く前にリンク先が正規のドメインであることを確認する
- QR コードをスキャンする端末の OS、アプリを最新の状態に保つ

本キャンペーンからの示唆

今回発表された米国における大規模なフィッシングキャンペーンは、QR コードを利用する特殊性があります。スマートフォンなど QR コードをスキャン可能なデバイスが広く普及していることや、QR コードは URL リンクと比較して標的にフィッシングメールを受信させる可能性が高いことから、今後日本でも QR コードが埋め込まれた不審メールが増加する可能性を認識しておく必要があります。

本件に限らず攻撃者は日々新たなサイバー攻撃手法を模索・実行しており、サイバー攻撃は高度化・巧妙化の一途を辿っています。企業においてセキュリティシステムを導入し多層防御を講じている場合でも、セキュリティに 100%確実ということはなく、利用者側に防御をすり抜けて攻撃が到達することを想定しておくことが求められます。個々人が常日頃から「QR コード利用時の注意点」に記載したような基本的な対策を怠らず、セキュリティ被害発生の未然防止を図る意識を持つことが大切であると言えるでしょう。

1. DMARC の導入にかかわる動向

電子メールを起点とした詐欺被害の拡大

昨今、送信者を詐称した電子メールを送り付けて金融機関や EC サイトの偽サイトに誘導し、ID・パスワードやクレジットカード番号などを詐取するフィッシング詐欺の被害が拡大しています。また、企業の経営層や取引先になりすまして偽の電子メールを送り付け、従業員をだまして犯罪者の銀行口座に送金させるというビジネスメール詐欺も増加しています。このような状況を背景として、電子メール送信者のなりすましを防ぐ認証技術である DMARC が注目を集めています。本記事では、DMARC とはどのような技術なのかを簡単に解説した上で、政府機関や業界団体の DMARC 導入にかかわる動向を紹介します。

送信者のなりすましを防ぐ認証技術

現在、電子メール送信者のなりすましを防ぐ送信ドメイン(*1)認証技術として主に以下の 3 つがあります。

① **SPF（Sender Policy Framework）**

送信元サーバーの IP アドレスから送信元の正当性を確認する仕組みです。

② **DKIM（DomainKeys Identified Mail）**

電子メールに付加された電子署名により送信元と本文の正当性を確認する仕組みです。

③ **DMARC（Domain-based Message Authentication, Reporting, and Conformance）**

以下の 3 つの仕組みを備えています。

1. SPF もしくは DKIM で認証に利用したドメイン名とメールソフトで表示される送信元のドメイン名(*2)が一致していることを確認する。
2. 上記 1. の認証に失敗した電子メールを受信側がどのように扱うべきか（受信拒否する、特別な処理はしないなど）を送信側がポリシーとして指定する。
3. 認証結果を送信側がレポートとして受け取る。

現在注目を集める DMARC は、SPF と DKIM の認証結果を利用してさらに認証を強化する仕組みと言えます。SPF および DKIM の認証がいずれも失敗すると、DMARC の認証も失敗します。また、SPF と DKIM では認証に失敗した電子メールをどう扱うか受信側に任されているという問題や、メールソフトで表示される送信元のドメイン名を検証できないといった問題の解決が図られています。

(*1) 送信元電子メールアドレスの@より右の部分のことを送信ドメインと呼びます。

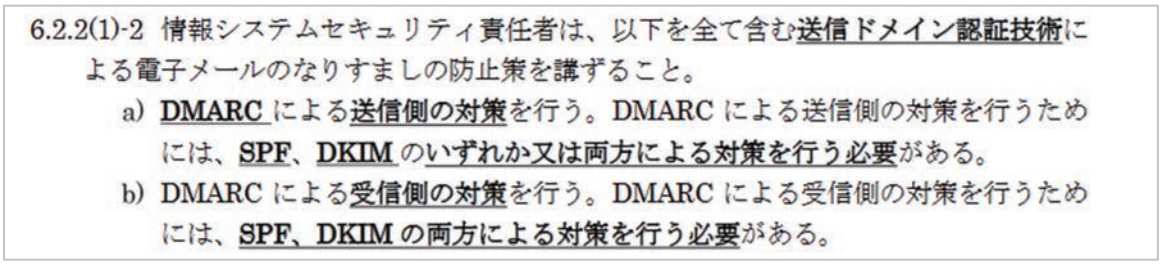
(*2) 詳しい説明は省略しますが、電子メールでは複数の「送信元メールアドレス」が存在します。SPF と DKIM では、実際に電子メールを読む人間が目にすることの多い「メールソフトで表示される送信元」の正当性を確認することができません。

政府関係機関の DMARC をめぐる動向

政府関係機関は、自身の DMARC 導入推進に加え、各業界の所管省庁がそれぞれの業界について DMARC 導入を推奨しています。以下では主だった政府関係機関についてその動向を紹介します。

内閣サイバーセキュリティセンターの動向

本冊子の「3.『政府機関等のサイバーセキュリティ対策のための統一基準群』（令和 5 年度版）を策定」でも紹介したとおり、政府は 2023 年 7 月に「統一基準群」を策定・公表しましたが、このうち『政府機関等の対策基準策定のためのガイドライン』は内閣サイバーセキュリティセンターが作成しているものです。このガイドラインの中で「電子メール」の「基本対策事項」として以下の内容が記載されています。



6.2.2(1)-2 情報システムセキュリティ責任者は、以下を全て含む送信ドメイン認証技術による電子メールのなりすましの防止策を講ずること。

a) DMARC による送信側の対策を行う。DMARC による送信側の対策を行うためには、SPF、DKIM のいずれか又は両方による対策を行う必要がある。

b) DMARC による受信側の対策を行う。DMARC による受信側の対策を行うためには、SPF、DKIM の両方による対策を行う必要がある。

出典：内閣官房 内閣サイバーセキュリティセンター『政府機関等の対策基準策定のためのガイドライン（令和 5 年度版）』p320 (*1)

改定前のガイドラインでは「なりすまし防止策」の一例として DMARC が言及されていたのですが、今回の令和 5 年度版ガイドラインでは「なりすまし防止策」として送信側、受信側ともに DMARC を導入することが必須となっています。このガイドラインは、政府機関等が情報セキュリティ対策基準を定める際に参照するものであるため、今後、政府機関等による DMARC 導入が大幅に進展する可能性があります。

総務省の動向

総務省は 2023 年 8 月に『ICT サイバーセキュリティ総合対策 2023』を公表しました。この中で、DMARC は国際的にも実装が進みつつあるにもかかわらず、わが国では導入が進んでいない技術の 1 つであるとして、国内 ISP 等における導入状況や導入に係る技術的課題の調査・分析を継続するとともに、「普及促進に向けたガイドライン案を作成し、技術導入の普及啓発に取り組む」(*2)と記載されています。今後、総務省から DMARC にかかわる何らかの「ガイドライン」が策定・公表されるかもしれません。

(*1) https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

(*2) 総務省『ICT サイバーセキュリティ総合対策 2023』p14（ https://www.soumu.go.jp/main_content/000895981.pdf ）

また、総務省が地方行政に関して公開しているドキュメントとして『地方公共団体における情報セキュリティポリシーに関するガイドライン』（2001 年 3 月策定、その後改定を重ね、直近版は 2023 年 3 月改定）があります。このガイドラインは、地方公共団体が情報セキュリティポリシーを各組織の実態に応じて自主的に定める際に参考とすべきものとされていますが、「電子メールのセキュリティ管理」については以下のような記載があり、ここでも DMARC 導入が求められています。

（１４） 電子メールのセキュリティ管理

メールサーバに対するセキュリティ対策等、電子メールのセキュリティ管理について定める。外部からの電子メール受信及び外部への電子メール送信においてなりすましを防ぐため、メールサーバのセキュリティ対策として電子署名を用いた DKIM（DomainKeys Identified Mail）や SPF（Sender Policy Framework）等の対策を実施するとともに、DMARC（Domain-based Message Authentication, Reporting & Conformance）も実施しなければならない。また、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、SMTP によるサーバ間通信を TLS による保護や、S/MIME 等の電子メールにおける暗号化及び電子署名の技術の利用等、電子メールのサーバ間通信の暗号化の対策を講ずることも考えられる。

出典：総務省『地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 5 年 3 月発表）』iii -88 (*1)

経済産業省の動向

経済産業省はクレジット業界の所管省庁であり、昨今、クレジット業界を標的にしたフィッシングメールが増加していることもあって対策を強化しています。2022 年 6 月 20 日には、『クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性（クレジット・セキュリティ対策ビジョン 2025）』(*2)を公表し、今後の方向性の一つとして DMARC 等のフィッシング対策を挙げています。また、2023 年 2 月 1 日には、警察庁とともに、クレジットカード会社等に対し、送信ドメイン認証技術（DMARC）の導入をはじめとするフィッシング対策の強化を要請(*3)しました。

警察庁の動向

警察庁サイバー警察局の「フィッシング対策」の Web ページ(*4)で事業者向けに DMARC の導入を推奨しています。また金融庁や総務省と連携して、銀行関連団体や通信事業者に向けて DMARC 導入の働きかけを行っています(*5)。

(*1) https://www.soumu.go.jp/main_content/000873096.pdf

(*2) https://www.meti.go.jp/policy/economy/consumer/credit/2022062019001.pdf

(*3) https://www.meti.go.jp/press/2022/02/20230201001/20230201001.html

(*4) https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html

(*5) 警察庁サイバー警察局『フィッシング対策への取組』p3
（ https://www.meti.go.jp/shingikai/mono_info_service/credit_card_payment/pdf/004_03_00.pdf ）

業界団体の DMARC 導入をめぐる動向

以下では DMARC 導入を推進する代表的な業界団体について紹介します。

迷惑メール対策推進協議会

電気通信事業者、広告事業者、配信 ASP 事業者、セキュリティベンダー、消費者団体、学識経験者、関係省庁などが最新の情報共有や対応方策の検討などを目的に設立した協議会です。『迷惑メール白書』や『送信ドメイン認証技術導入マニュアル』といった資料を Web ページ(*1)で公開しています。『送信ドメイン認証技術導入マニュアル』には SPF、DKIM、DMARC の仕組みや設定方法などが詳細に記載されており、総務省、経産省、警察庁などの Web サイトからもリンクされています。

フィッシング対策協議会

フィッシングに関する情報収集・提供、注意喚起等の活動を中心とした対策の促進を目的に 2005 年 4 月に設立された協議会です。毎年『フィッシング対策ガイドライン』(*2)を改定しており（最新版は 2023 年 6 月）、この中ではなりすましメール対策として DMARC の導入・設定が必要であると記載されています。またこの他にも DMARC 導入を推奨する文書や報告書などを Web サイト(*3)で公開しています。

最後に

DMARC が技術仕様として公開されたのは 2015 年のことですが、認証結果レポートの分析やそれに基づく設定の調整が必要になるなど一定の運用負荷がかかることから、これまで日本国内ではあまり導入が進んでいませんでした。しかし、昨今、送信者を詐称した電子メールを起点としたフィッシング詐欺が拡大しており、これを受けて政府関係機関も DMARC 導入を推進している状況です。前述の「統一基準群」で DMARC 導入が必須化されたことを受け、今後は政府機関等で導入が進むものと推測されます。また、総務省、経済産業省、金融庁などが所管する業界でもこれらの省庁の要請に応じる形で導入が進んでいくことが予想されます。

ただそれ以外の業界でも、自社ドメインのなりすましメールが増大し、利用者の被害が拡大すれば、自社のブランドイメージが損なわれる恐れもあります。DMARC を未導入の企業は、政府や業界団体が公表しているガイドラインなども参照しながら、自社への導入を検討してみると良いでしょう。

(*1) https://www.dekyo.or.jp/soudan/aspc/report.html

(*2) https://www.antiphishing.jp/report/guideline/

(*3) https://www.antiphishing.jp/

2. 新しい DNS キャッシュポイズニング攻撃 MaginotDNS と Black Hat について

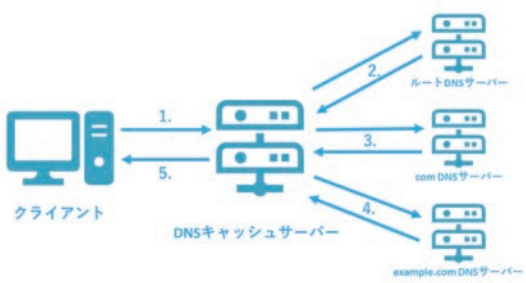
概要

カリフォルニア大学アーバイン校と清華大学の研究者(*1)たちは Black Hat USA 2023（詳細は後述）で MaginotDNS (*2)と名付けた新しい DNS キャッシュポイズニング攻撃を発表しました。この MaginotDNS がこれまでの DNS キャッシュポイズニング攻撃と異なる点として、次の 3 点が挙げられます：①条件付き DNS サーバーを攻撃対象としている、②ベイリウィックルールを破っている、③フォワーダの脆弱性を利用して再帰リゾルバを攻撃している。本記事では、研究者らの論文(*3)を基に MaginotDNS の概要を紹介します。

DNS キャッシュポイズニング攻撃

私たちが Web ページへアクセスする際、通常は URL と呼ばれるスキーム、ドメイン、パスで構成された文字列をアドレスバーに入力して、あるいはリンクをクリックしてそのページを返してくれるサーバーへアクセスします。接続先のサーバーはドメインから特定できますが、通信ではそのサーバーの IP アドレスを指定する必要があります。従って、ドメインから IP アドレスへの変換が必要です。このドメインと IP アドレスを対応付け、変換してくれるシステムが DNS（Domain Name System）です。以下はドメイン www.example.com に対応する IP アドレスを得る（名前解決する）流れです：

1. DNS サーバーに問い合わせを行うサーバー（DNS キャッシュサーバー）に問い合わせを依頼する。
2. このサーバーからルート DNS サーバーへ問い合わせる。これに対し、ルート DNS サーバーは com DNS サーバーへ問い合わせるよう返答する。
3. 次に、com DNS サーバーへ問い合わせる。これに対し、com DNS サーバーは example.com DNS サーバーへ問い合わせるよう返答する。



図：DNS による名前解決のイメージ
出典：大和総研作成

4. 次に、example.com DNS サーバーへ問い合わせる。 www.example.com に対応する IP アドレスがあればその IP アドレスを返答する。無ければその旨を返答する。
5. 最終的な返答を受け取る。

(*1) カリフォルニア大学アーバイン校：张起帆、李洲助教。清華大学：李想、陆超逸博士、刘保君助教、李琦助教、段海新教授。

(*2) https://maginotdns.net/

(*3) https://lixiang521.com/publication/security23/usenix23-li-maginot.pdf

ルートサーバーへのアクセスの集中を避けるため、問い合わせを行うサーバーは一定期間問い合わせの結果を記憶しておく（キャッシュする）ことがあります。そのため、この問い合わせを行うサーバーは DNS キャッシュサーバーとも呼ばれます。また、ドメインと IP アドレスの対応を管理しており、名前解決の際には自身が持っている情報または存在しない旨を返答する DNS サーバーを権威 DNS サーバーといいます(*1)。

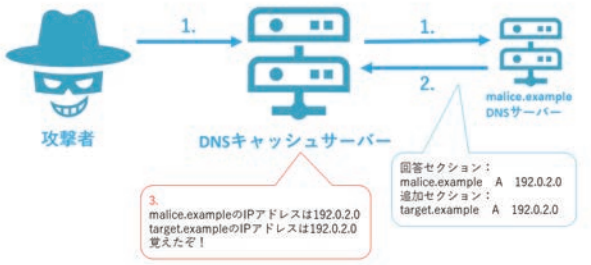
もし、2.から 4.の過程で正規のものとは異なる IP アドレスを返答された場合、www.example.com へのアクセスは異なる（場合によっては悪意のある）サイトに繋がります。そして、DNS キャッシュサーバーは一定期間問い合わせのたびに偽の IP アドレスを返答します。これを狙った攻撃を DNS キャッシュポイズニング攻撃といいます。

ベイリウィックルール

DNS キャッシュポイズニング攻撃の一つに Kashpureff 型攻撃があります。たとえば、malice.example を管理している攻撃者が target.example を乗っ取るとすると、次のような流れで行われます：

1. 攻撃対象の DNS キャッシュサーバーに malice.example の名前解決を依頼する。
2. malice.example の権威 DNS サーバーが IP アドレスを返答する際に、追加セクションに target.example と虚偽の IP アドレスの対応も記載する。
3. DNS キャッシュサーバーに malice.example と target.example に対応する IP アドレスがキャッシュされる。

この中で問題なのは 3.です。malice.example の権威 DNS サーバーが管轄外の target.example の IP アドレスを答えるのはおかしいので、本来ならキャッシュせずに無視するべきです。このように、Kashpureff 型攻撃を防ぐために、管轄外の応答を無視するルールをベイリウィック（bailiwick：管轄区域）ルール(*2)といいます。



図：Kashpureff 型攻撃のイメージ
出典：大和総研作成

(*1) 別の権威 DNS サーバーを紹介することもあります。

(*2) ベイリウィックルールは RFC 2181 に記載されています。bailiwick については RFC 8499 を参照のこと。

先行研究ではベイリウィックチェックを行わないデバイスを対象とするか、管轄内の不正な応答を受け入れるよういかに誤認させるかに焦点を当てていました。このことから、ベイリウィックルール自体を破ることは困難であることが示唆されます。

MaginotDNS

条件付き DNS サーバー（以下、CDNS）とは再帰リゾルバ(*1)と DNS フォワーダ(*2)の両方の機能を持った DNS サーバーで、これも DNS キャッシュサーバーの一つです。そして、MaginotDNS はこの CDNS を狙った攻撃です。

研究対象となった CDNS のキャッシュは再帰リゾルバモードと DNS フォワーダモードで共有されています。つまり、再帰リゾルバで作成したキャッシュを DNS フォワーダは上書きできるため、 DNS フォワーダを介して再帰リゾルバを攻撃することができます。

詳細は割愛しますが、MaginotDNS は二段階で行われます。第一段階は CDNS の特定です(*3)。第二段階は Kashpureff 型攻撃と同様の手順で行われます(*4)。

ベイリウィックルールに則るならこの攻撃は防がれるはずですが、何故上手く行くのでしょうか。これは、再帰リゾルバモードと DNS フォワーダモードでは異なるベイリウィックチェックが実装されており、DNS フォワーダモードで採用されているアルゴリズム(*5)には脆弱性が存在することが原因です。

その脆弱性の要点を述べると、DNS フォワーダとして処理する場合、クエリのゾーンを先祖ゾーンまたはルートゾーンで初期化してしまいます。そのため、応答の権威セクション及び追加セクションの任意のドメイン名のレコードが管轄内と見做され、破棄されずにキャッシュされてしまいます。こうして、DNS フォワーダを介して再帰リゾルバを攻撃することができるのです。

(*1) 問い合わせを受けたときに名前解決できるまで問い合わせ続ける DNS サーバーのこと。

(*2) 問い合わせを受けたときに名前解決可能な DNS サーバーへ転送する DNS サーバーのこと。

(*3) MaginotDNS に対して脆弱な CDNS を見つける方法は論文の 6 章に記載されています。

(*4) 攻撃の流れは論文の 3.2 節に、具体的な方法は 5 章に記載されています。

(*5) アルゴリズムの概要は論文の 4 章、詳細は Appendix C に掲載されています。

特に、研究者らは MaginotDNS によって.com や.net のようなトップレベルドメインやそのサブドメインまで乗っ取れる可能性を指摘しています。

最後に

今回発表された脆弱性は研究対象となった DNS ソフトウェアのベンダー全てに報告され、一部は既に修正が発表されています。該当するソフトウェアを利用している場合はアップデートを確認しておきましょう。また、研究者らは DNSSEC(*1)や 0x20 エンコーディング(*2)によって MaginotDNS に対抗することができると述べています。必要に応じてこれらの利用を検討すると良いでしょう。

本件に限らず、脆弱性や攻撃手法の報告は高度なことが往々にしてあり、セキュリティ担当者がその内容を常に正しく把握することは困難です。しかし、セキュリティ担当者はその重大さを判断し、必要に応じて対応しなければなりません。従って、脆弱性や攻撃手法への対策としてベンダーから提供されるパッチはその内容や重要性を見極めて速やかに適用することが望ましいでしょう。

Black Hat について

この攻撃手法が発表された Black Hat というイベントは、Jeff Moss 氏が創立した世界有数のサイバーセキュリティカンファレンスで、大きく Briefings, Trainings, Arsenal という 3 つのセクションに分かれています。Briefings はいくつかのトラックに分かれており、それぞれで専門家が情報セキュリティに関する研究成果を紹介しているほか、政府関係者等による基調講演が行われます。Trainings では侵入テストやネットワークインフラに対するハッキング等のハンズオンが提供されます。Arsenal ではオープンソースや製品等の展示が行われ、質疑応答やデモンストレーションもあります。

Black Hat USA 2023 では、米国政府関係者の登壇が目立ち、サイバーセキュリティ政策の決定においてハッカーコミュニティに協力を求めている状況が見て取れました。また Black Hat 創始者の Jeff Moss 氏もハッカーコミュニティが信頼を勝ち取ってルール形成に関わる機会であるとの発言をしており、両者が歩み寄っている様子がうかがえました。

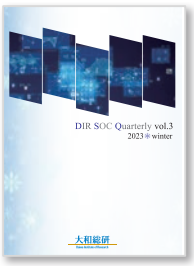
(*1) DNSSEC とは、権威 DNS サーバーが返答する際に電子署名を付加して出自と完全性を担保する技術です。

(*2) 0x20 エンコーディングとは、問い合わせ時にドメインの各文字をランダムに大文字または小文字へ変換することです。問い合わせと返答で QNAME の大文字・小文字のパターンが同一であれば偽装されていないと判断できます。

バックナンバーはこちら

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
- 多要素認証疲労攻撃 ユーザーが「承認」するまで繰り返される
- 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）

- 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

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