DIR SOC Quarterly

2025 winter

vol 10

インシデント事例の紹介
- セキュリティを巡るAI利用の影と光
- パスワード漏洩に関する考察

トピックス
- 金融分野におけるサイバーセキュリティに関するガイドライン
- 耐量子計算機暗号に関わる国内動向

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、2024 年度第 2・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。国家が主導しているサイバー攻撃対策について理解を深めるためには、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。

本冊子で取り扱っている話題について、簡単にご紹介します。

EU において欧州サイバーレジリエンス法が発行され、これを受け日本でも IoT 製品に対するセキュリティ適合制度が開始されるなど、デジタル製品に対するセキュリティ強化の動きが各国で見られています。
第 1 部では、日本で IPA が 2024 年 9 月 30 日に開始した『セキュリティ要件適合評価及びラベリング制度（JC-STAR）』および、『欧州サイバーレジリエンス法（CRA）』について取り上げています。

第 2 部では、活用が進んでいる生成 AI について、マルウェアや詐欺の増加など悪用の側面と、脆弱性発見などに役立てられている側面について、影と光の両面をご紹介します。

第 3 部では、前号も取り上げた「金融分野におけるサイバーセキュリティに関するガイドライン」および、日本銀行や金融庁で取り組みが進んでいる、耐量子計算機暗号の国内動向などのトピックスを取り上げます。

上記トピックスのいずれかが皆さま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。

なお、本冊子は次号以降、皆さまにとってより分かりやすく、詳しい内容をお届けできるよう、ウェブサイトのレポートと連動した形での刊行を予定しています。
今後ともご愛読いただけますよう、よろしくお願いいたします。

2025 年 1 月　株式会社大和総研執筆者一同

1.『ICT サイバーセキュリティ政策の中期重点方針』の公表

要約

- 総務省は、所管する通信、放送、自治体、データ流通基盤を対象に『ICT サイバーセキュリティ政策の中期重点方針』を公表した。
- 4 つの重点事項を設定し、サイバーセキュリティ対策を強化する方針。
- 各分野の取り組みに加え、生成 AI の急速な普及、量子コンピュータの進展による新たなサイバーリスクに対して今後の取り組みの方向性が示された。

公表された方針の概要

総務省は 2024 年 7 月 31 日、『ICT サイバーセキュリティ政策の中期重点方針(*1)』を公表しました。本方針は、2030 年頃を見据えたセキュリティ対策について議論し、一般からの意見募集（2024 年 7 月 2 日から同年 7 月 19 日）を経て、17 件の意見を参考にして最終的に決定されました。なお、本方針は総務省の所管する通信、放送、自治体、データ流通基盤についての現状と今後の取り組みの方向性がまとめられています。

サイバーセキュリティを巡る主な課題を 4 点あげ、『経済安全保障推進法』の施行（2024 年 5 月）や『AI 事業者ガイドライン(*2)』の策定（2024 年 4 月）などの政府の動きを背景に中期重点方針が示されています。

サイバーセキュリティを巡る主な課題	説明
厳しさを増す国際情勢とサイバー攻撃リスクの高まり	国際情勢が悪化し、サイバー攻撃のリスクが増大。ロシアのウクライナ侵攻やハマスによるイスラエルに対する攻撃により、国際的な対立が複雑化。重要インフラのサイバーセキュリティ強化と国際協力が急務。
多様化・複雑化するサプライチェーンとアタックサーフェスの増加	グローバルバリューチェーンの拡大により、製品を安く生産する一方で、サイバーリスクも増加。委託先企業の不十分なセキュリティが情報漏洩を引き起こし、複雑化するサプライチェーンに対する適切な対策が必要。
セキュリティ人材の確保	日本企業の約9割、約11万人のセキュリティ人材が不足していると推計。人材は大都市（特に東京圏）に集中している傾向があり、地域に特化した人材育成が急務。
生成AI等の新たな技術への対応	サイバーセキュリティでは新技術への対応が重要。特に生成AIは偽情報やプライバシー侵害のリスクがあり、量子コンピュータの発展も従来の暗号を脅かす。これらに対する適切なセキュリティ対策が求められる。

総務省が中長期的に取り組むべき4つの重点事項

- 重要インフラ等におけるサイバーセキュリティの確保
- サイバー攻撃対処能力の向上と新技術への対応
- 地域をはじめとするサイバーセキュリティの底上げに向けた取組
- 国際連携の更なる推進（国際連携全般、人材育成支援）

出典：総務省『ICTサイバーセキュリティ政策の中期重点方針(*1)』を基に大和総研作成

(*1) 総務省『ICT サイバーセキュリティ政策の中期重点方針』

(*2) 総務省・経済産業省『AI 事業者ガイドライン』

示された今後の取り組みの方向性

重点事項「重要インフラ等におけるサイバーセキュリティの確保」において、以下に、総務省の所管分野の中から、通信とデータ流通基盤に絞り、現状と今後の取り組みを整理しています。

カテゴリ	現状の説明	今後の取り組みの方向性
1. 通信	情報通信ネットワークは国民生活や経済活動に不可欠だが、サイバー攻撃の脅威が高まっている。	IoTボットネット対策や通信サービスのセキュリティ対策、サプライチェーン対策を強化する必要がある。
	IoTボットネット対策 マルウェアに感染したIoT機器がサイバー攻撃に悪用される問題がある。脆弱な機器を減らし、C&Cサーバを見つけて対処する対策を強化する必要がある。	**ネットワークセキュリティ技術** RPKI、DNSSEC、DMARC(*1)などの認証技術があまり導入されていない。これらを導入しやすいガイドラインを作成し、企業の導入状況を見える化して普及を促進する。
	サプライチェーン対策 OSSの利用が増えているため、サプライチェーン全体のセキュリティが重要。SBOM(ソフトウェア部品表)を導入して脆弱性への対応を迅速に進める。	**スマートフォンアプリの対策** **情報漏洩事案への対応** **5Gネットワークのセキュリティ**
2. データ流通基盤	クラウドサービスのセキュリティ対策が重要で、設定ミスによる情報漏えいが多発。	ISMAPの登録促進やトラストサービスの普及を進め、安全なデータ流通基盤を整備する。
	クラウドサービス ガイドラインの普及とISMAP登録を進める。	**トラストサービス** eシールやタイムスタンプの認定制度を整備し、電子データの安全な流通を推進。

出典：総務省『ICTサイバーセキュリティ政策の中期重点方針』を基に大和総研作成

また、重点事項の「サイバー攻撃対処能力の向上と新技術への対応」では、生成 AI の急速な普及、量子コンピュータの進展による新たなサイバーリスクに対して今後の取り組みの方向性を示しています。

- **AI とセキュリティの方向性**

総務省は、生成 AI の急速な普及に伴い、AI 技術に関連するセキュリティリスクを回避・低減するための取り組み(Security for AI)と、AI 技術をセキュリティ対策に効果的に活用すること(AI for Security)の両方に取り組む必要性を示しています。そのために、総務省と経済産業省が策定した『AI 事業者ガイドライン』に基づいた新しいガイドラインを整備し、AI セキュリティ情報の発信の重要性を認識しています。これは、具体的なプロジェクトを通じて AI 活用の効果を示すことの重要性が示唆されています。

- **耐量子計算機暗号(PQC：Post-Quantum Cryptography)(*2)の方向性**

総務省は、量子コンピュータの進化に伴う現代暗号の危殆化リスクへの対処を重要視しています。具体的には、NICT(国立研究開発法人情報通信研究機構)における暗号安全性評価に関する研究開発の取り組みを充実させ、PQC への移行を推進し、暗号技術の安全性評価や監視の強化を進めています。

最後に

テクノロジーの進化により、私たちの利便性が向上する一方で新たなサイバーリスクが発生します。今後のセキュリティ対策では、特に生成 AI が重要な役割を果たします。生成 AI はデータ分析や脅威検出の精度を向上させる一方で、その利用に伴うリスクも考慮しなければなりません。また、PQC は量子コンピュータの進化に対応するための新たな暗号技術として、通信の安全性を確保するために必要不可欠です。これらの技術を適切に導入し、リスクを管理することが、今後のサイバーセキュリティの強化につながります。本方針は総務省の所管分野を対象としていますが、業種や業態に関係なく取り組むべき課題であり、さまざまな業種や業態を横断して連携していくことが求められます。政府のサイバーセキュリティに対する取り組みや考え方がまとまっているため、関心のある方はご一読をお勧めします。

（蓮見　将生）

(*1) RPKI はインターネットのルーティングを安全にする仕組み、DNSSEC はドメイン名の情報を正確に保つための技術、DMARC はメールのなりすましを防ぐためのルールを設定する方法です。

(*2) 大和総研『耐量子計算機暗号とは何か　移行のために知っておきたいこと』

2. IoT 製品に対するセキュリティ適合性評価制度『JC-STAR』の開始

要約

- 独立行政法人 情報処理推進機構（IPA）は、IoT 製品のセキュリティ適合要件を評価する制度『JC-STAR』を 2025 年 3 月から開始すると公表した。
- JC-STAR で付与される適合ラベルにより、ユーザーは購入する IoT 製品が国で定めたセキュリティの適合基準を満たしているかどうかを容易に確認することができる。

概要

IPA は 2024 年 9 月 30 日、IoT 製品に対するセキュリティ適合性評価制度となる『セキュリティ要件適合評価及びラベリング制度（JC-STAR: Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements）』（以下、「本制度」という。）の開始について公表しました(*1)。本制度は、2024 年 8 月に経済産業省が示した『IoT 製品に対するセキュリティ適合性評価制度構築方針』(*2)に基づき構築された制度で、インターネットとの通信が行える幅広い IoT 製品を対象として、共通的な物差しで製品に具備されているセキュリティ機能を評価・可視化することを目的としています。

セキュリティ対策が不十分な IoT 製品がサイバー攻撃によってマルウェアに感染する事例が相次ぐ中、本制度により、ユーザーは一定のセキュリティ要件を満たした安全な IoT 製品を調達しやすくなります。本制度は 2025 年3月から開始される予定で、適合基準を満たす製品には適合ラベルが付与されることとなります。

本制度のロゴ

適合ラベル（イメージ）

出典：IPA「IoT 製品に対するセキュリティ要件適合評価・ラベリング制度を開始します」(*3)から転載

本制度の対象機器、適合基準

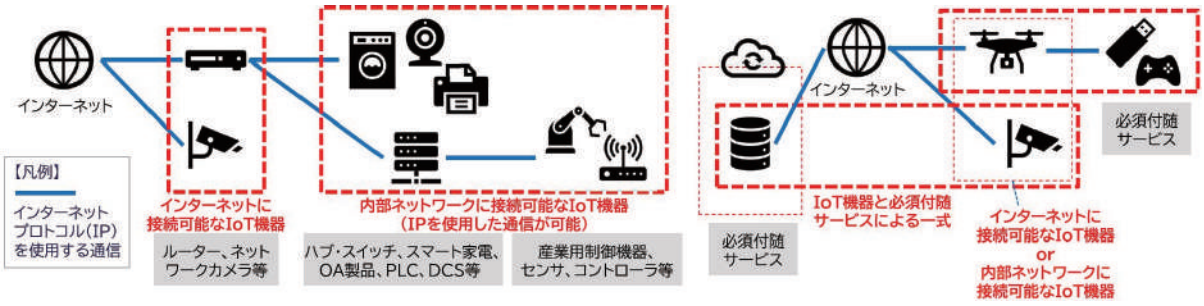
本制度で適合ラベルの対象となる機器は、インターネットプロトコル（IP）を使用したデータの送受信機能を持つものであって、ルーター、ネットワークカメラ、スマート家電、産業用制御機器などの他、これら機器と一体で提供することが必須となるものも含まれます。

また、本制度の適合基準は4段階のレベル（★1～4）が設けられており、レベルが高くなるほど求められるセキュリティ要件の項目が多くなります。★1 は全ての IoT 製品に共通の統一的な最低限の適合基準が設けられていますが、★2 以上では、通信機器やスマート家電といった製品類型ごとの特徴や利用形態、脅威なども考慮され、同じレベルであっても製品類型によって異なる適合基準が設定されています。

(*1) IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」

(*2) 経済産業省「IoT 製品に対するセキュリティ適合性評価制度構築方針」

(*3) IPA「IoT 製品に対するセキュリティ要件適合評価・ラベリング制度を開始します」

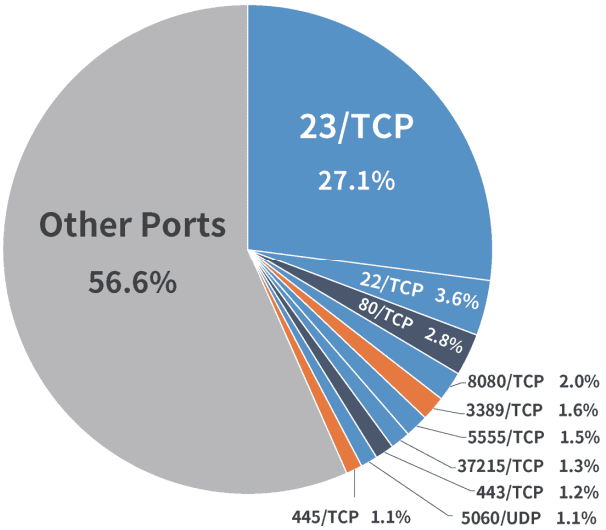


本制度で適合ラベルの対象となる機器（赤枠部分）

出典：IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報」(*1)から転載

本制度創設の背景

本制度創設の背景には、近年のデジタル化の進展に伴い IoT 機器が急速に増加し、これらの脆弱性を狙ったサイバー攻撃の脅威が高まっていることがあげられます。国立研究開発法人情報通信研究機構（NICT）が 2024 年 2 月 13 日に公表した『NICTER 観測レポート 2023』(*2)によれば、2023 年にインターネット上で観測された主な攻撃対象（宛先ポート番号）の上位 10 位のうち、六つが IoT 機器に関連しており、その通信量は全体の 36.6%を占めていました。



宛先ポート番号別パケット数分布（水色の箇所が IoT 機器に関連するもの）

出典：NICT『NICTER 観測レポート 2023』(*2)から転載

宛先ポート	攻撃対象
23/TCP	Telnet（ルータ，Webカメラ等）
22/TCP	SSH（サーバ，ルータ等）
80/TCP	HTTP（Webサーバ）
8080/TCP	HTTP（Web管理画面）
3389/TCP	Remote Desktop
5555/TCP	ADB（Android）
37215/TCP	Huawei 製ルータ
443/TCP	HTTPS（Webサーバ）
5060/UDP	SIP
445/TCP	Windows SMB

宛先ポート番号別パケット数分布
（調査目的のスキャンパケットを除く）

これらの IoT 機器を狙った攻撃により、インターネットに接続された IoT 機器が知らぬ間にマルウェアに感染し、新たな攻撃の踏み台としての悪用や、情報が窃取される被害が多発しています。このような現状から、IoT 機器へのセキュリティ対策が求められる一方で、製品ベンダーはセキュリティ対策の取り組みをユーザーに効果的に伝えることが難しく、ユーザー側も製品のセキュリティ対策が適切かどうかを判断するのが困難という課題がありました。本制度ではこれらの課題を解決し、ユーザーが製品の詳細や適合評価、セキュリティ情報、問い合わせ先などの情報を容易に取得できるようにしています。

最後に

本制度では、諸外国における IoT 製品の適合性評価制度設立の動向も踏まえ、各国の制度との連携を図り、相互承認することも目指しており、現在、シンガポール（Cybersecurity Labelling Scheme）、英国（PSTI 法）、米国（U.S. Cyber Trust Mark）、EU（CRA）の各国担当機関との間で相互承認に向けた交渉を行っています。EU（CRA）については、本冊子 P.11 で紹介していますのでご参照ください。

（横平　健）

(*1) IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報」

(*2) NICT「NICTER 観測レポート 2023 の公開」

3. FISC、「金融機関によるAI の業務への利活用に関する安全対策の観点からの考察」の公表

要約

- 公益財団法人 金融情報システムセンター(FISC)は、金融機関における AI の業務利活用に関する安全対策と倫理的配慮の必要性を指摘し、具体的な利活用事例や課題、対応策を整理したレポートを公表した。
- AI の利活用には情報セキュリティや倫理面での課題があり、組織全体でのガバナンス強化が求められている。
- FISC は今後も AI に関する調査研究や基準の整備を進める予定。

公表されたレポートについて

公益財団法人 金融情報システムセンター(FISC)は、2024 年 9 月 24 日、「金融機関による AI の業務への利活用に関する安全対策の観点からの考察」(*1)と題したレポートを公表しました。これは、金融機関が AI を業務に利活用する動きが進展していることを踏まえ、代表的な利活用事例の紹介とともに、現在認識されている、または今後認識することが必要と考えられる課題と対応策について、整理し、公表したものです。

AI の利活用事例

金融機関における AI 利活用事例は、大きく「従来型 AI」と「生成 AI」に分類されます。

レポートでは、業務効率化だけでなく、新たなサービス創出にも寄与していると紹介されています。

従来型 AI の活用事例	概要
住宅ローン審査	申込者の定量データや取引データを分析し、与信判断を支援する。
カードローン申込予測	顧客属性や取引履歴を基に最適な商品提案を実現する。
保険金不正請求の検知	契約の内容に加えて、気象情報等の外部データを活用し、損害保険などの不正請求を早期に検知する。

生成 AI の活用事例	概要
業務文書・プログラムコード作成支援	文書作成や文法チェック、翻訳業務、資料の要約、アイデア出し、プログラムコードの作成を支援する。
プロンプトエンジニアリングや検索拡張生成(RAG)による業務効率化	プロンプトエンジニアリングや検索拡張生成(RAG)を活用し、プロンプトや社内データベースと連携し必要な情報を付与することや、情報検索や稟議書作成を効率化する。
ファインチューニングによる業務支援	LLM に対して特定の業務やデータの情報を再学習するファインチューニングを行うことで、業務文書の作成や営業支援等の業務に利用する。
音声・画像・動画処理による業務支援	テキストだけでなく音声・画像・動画も処理できる AI を活用し、コールセンターでの電話対応の品質向上などへの利用が期待されている。

出典:『金融機関による AI の業務への利活用に関する安全対策の観点からの考察』(*1)を基に大和総研作成

(*1) 金融機関による AI の業務への利活用に関する安全対策の観点からの考察 (公益財団法人 金融情報システムセンター)

生成 AI 利活用における課題

生成 AI の AI 利活用には、「情報セキュリティ面」、「倫理面」の観点で、以下の課題が指摘されています。

情報セキュリティ面の課題	概要
情報漏洩リスク	プロンプト入力された情報が学習データとして利用される可能性がある。
仕様・設定の理解不足	生成 AI サービスのリージョンやオプトアウトの設定などのサービス仕様や、利用者設定への理解不足が情報漏洩などのセキュリティリスクを増大させる懸念がある。
モニタリング困難性	入力データや生成結果の正確性・妥当性や、情報漏洩・プロンプトインジェクションなどの攻撃を、人手で常時監視することが難しい。 組織の許可を得ずに利用する、いわゆるシャドーIT による管理外利用の懸念がある。

倫理面の課題	概要
虚偽情報（ハルシネーション）	生成された情報に誤りが含まれる可能性がある。
人権侵害リスク	生成された情報に個人情報や個人に対する差別的・偏見的な情報が含まれ、個人の人権を侵害する危険性がある。
説明力・納得感の欠如	生成された情報の出力プロセスを検証する仕組みが備わっておらず、情報の正当性・妥当性の判断が困難となる可能性がある。

出典:『金融機関による AI の業務への利活用に関する安全対策の観点からの考察』(*1)を基に大和総研作成

これら課題への対応には、技術的対策だけでなく、組織全体でのガバナンス強化が必要です。

まとめ

金融機関における AI 利活用は、多大な可能性を秘めていますが、安全対策と倫理的配慮が不可欠です。具体的には以下の取り組みが求められます。

取り組み	概要
方針策定と態勢整備	AI 利活用が社会全体に及ぼす影響を考慮し、リスク管理や安全対策の観点を盛り込んだ AI 利活用方針を明確化し、組織全体で共有する。また、これらに適合した社内規定を整備する。 責任の所在を明確にした AI の利活用に係る態勢を整備する。
適切な利用と運用管理	AI で生成されたアウトプットに関する留意点を考慮した上で、AI の適切な利用・運用管理方法を定める。
安全対策強化	AI サービスの利用形態を明確にする。 AI サービスに対して情報漏洩や不正操作を防止する安全対策を講じる。

出典:『金融機関による AI の業務への利活用に関する安全対策の観点からの考察』(*1)を基に大和総研作成

FISC では、今後 AI に関して、会員企業等との意見交換や「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」(*2)への AI 関連項目の追加、生成 AI に関する利活用事例を中心とする調査研究レポートの公表を予定しています。これらの取り組みについては、FISC から会員に向けてアナウンスされます。

「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」に関しては、あくまでガイドラインとして提供されるものであり、規制ではありません。多くの金融機関にとって、AI を活用する際の安全対策の指針となることが期待されますが、各機関はそれぞれの業務、システム、利用するデータに応じた適切な安全対策を講じることが求められます。

（山崎 禎章）

(*1) 金融機関による AI の業務への利活用に関する安全対策の観点からの考察（公益財団法人 金融情報システムセンター）

(*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（公益財団法人 金融情報システムセンター）

4. NCA、「脆弱性管理の手引書 システム管理者編1.0 版」を公開

要約

- 一般社団法人 日本シーサート協議会(NCA)が、『脆弱性管理の手引書』を公開した。公開された手引書は、システム管理者編で、「ユーザ(システム管理者)」の立場での脆弱性管理手法について解説されている。本手引書について脆弱性管理の流れを中心に紹介する。
- 本手引書は、脆弱性管理の実施に際して必要な事項が体系的に整理・解説されており有用である。

概要

一般社団法人 日本シーサート協議会(NCA)は、2024 年 10 月 25 日、『脆弱性管理の手引書 システム管理者編 1.0 版』(以下、「本手引書」)を公開しました(*1)。NCA の脆弱性管理ワーキンググループでは、脆弱性管理に必要な事項を立場ごとに、ユーザ(システム管理者)、IT サービス/製品の提供者、システムインテグレータ(SIer)の三つに分類しており、本手引書は、「ユーザ(システム管理者)」の立場での脆弱性管理について解説されています。なお、本手引書の活用に際しては、ある程度の IT 資産の識別(IT 資産管理)がされていることが前提となります。また、現時点ではインシデント対応はスコープ外とされています。

脆弱性管理とは

脆弱性管理は、システムで稼働するソフトウェアや設定/設計の脆弱性を特定し、アプリケーションの修正やパッチの適用などの必要な対策を講じる一連のプロセスのことです。脆弱性管理は、セキュリティリスクを低減し、システムやデータの安全性を確保するため、継続的に実施する必要がある重要な活動です。

脆弱性管理については、本冊子前号の DIR SOC Quarterly vol.9 2024 autumn「脆弱性管理について」(*2)で詳しく紹介しております。本手引書と併せてご参照ください。

本手引書における脆弱性管理の流れについて

本手引書では、システム管理者観点での脆弱性管理を、下図の流れで実施するよう解説されています。

出典:NCA『脆弱性管理の手引書 システム管理者編 1.0 版』から転載

(*1) NCA『「脆弱性管理の手引書 システム管理者編 1.0 版」を公開』

(*2) 大和総研『脆弱性管理について』(『DIR SOC Quarterly vol.9 2024 autumn』pp.20-22)

各項目における実施概要は下表の通りです。詳細につきましては、本手引書をご参照ください。

項番	項目	実施概要（抜粋）
1	脆弱性管理対象の識別	・脆弱性管理対象の識別の際には、「ソフトウェア名/製品名」、「バージョン情報」、「機能カテゴリ/保持情報」、「構成」、「外部アクセス可否・ポート情報」、「設置場所」、「管理者/責任範囲」の事項を把握することが必要。 ・ ソフトウェア情報の確認には仕様書、設計書等の確認、担当者へのヒアリングが必要。 ・ 管理区分の例→「サービス・機能を起点」、「ソフトウェアを起点」、「システム・サーバを起点」、「その他」 ※どのような管理区分を起点とするかは、各組織の既存の IT 資産管理方法、責任分担、管理対象の規模/種類を考慮して検討する必要がある。 ・ 脆弱性管理対象の識別において、SBOM(*1)を活用することを期待。
2	脆弱性情報の内容把握 ・ソフトウェア/製品の脆弱性の把握 ・設定/設計の脆弱性の把握	・ 脆弱性情報は「ソフトウェア/製品の脆弱性」、「設定/設計の脆弱性」に大別できる。 ・ ソフトウェア/製品の脆弱性の把握には、「CVE・脆弱性の名称」、「対象ソフトウェア・製品」、「対象バージョン」、「脆弱性発露の条件」、「影響」、「対応策・対応手順」、「緩和策・回避策」の事項を押さえた検査が必要である。 ・ソフトウェア/製品の脆弱性を把握する際の情報収集には、「セキュリティ関連の団体/組織から」、「ソフトウェア/製品の開発ベンダから」、「セキュリティベンダが運営するサイトから」、「脆弱性情報配信サービス」のような手段が考えられる。 ・設定/設計の脆弱性の把握には、「保持/流通情報」、「ユーザ権限（管理/一般）」、「アプリケーション ミドル・OS 設定」、「NW 設定/設計」、「設置場所」の事項を押さえた検査が必要である。 ・脆弱性の内容把握に、ペンテストツール、ASM(*2)、CSPM(*3)などの活用について紹介。 ・デフォルト設定と推奨設定について解説。
3	組織におけるリスク評価	・ 大量に報告される脆弱性のすべてに対応するのは非現実的であり、各組織においてどのような脆弱性に対応するかの判断基準が必要。報告される脆弱性に対する絞り込みの基準例としては、「共通の指標」および「脆弱性スキャナー/脆弱性 DB サービス」によるものがある。 ・リスク評価基準は各組織のリスク選好性・業務特性によって異なるが、「リスクの発生可能性」と「想定被害」を軸に決定する方法を例示。 ・CVSS(*4)、EPSS(*4)等を活用したリスク評価基準も考えられる。 ・リスク評価の基準については事前に経営層との合意を取ることが望ましい。 ・リスク評価結果については具体的なアクションに結び付いた表現が必要。 ・「把握した情報」と「事前に定めた判断基準」を照らし合わせ、リスク評価を実施する。 ・ KEV(*4)を参照することでリスク評価をより効果的に行うことができる。
4	対処・対策	・ 取りうる対処・対策について、把握事項（「実施内容（パッチの適用、等）」、「効果（脆弱性の解消、発生可能性の低減、等）」、「対処案実施の影響（不明のため要検証、等）」、「実施可能スケジュール（〇月×日（検証後）、等）」）を押さえ、リスク評価がどう変わるのかを確認する。 ・実施する対処計画の決定に関しては、関係者とのコミュニケーションを通して実施の影響、実施可能スケジュールを検討する必要がある。業務への影響等を考慮するとリスク解消する対処がすぐには実施できないことも想定すること。リスクを緩和する暫定対処策も含めて対処計画を検討する必要がある。 ・影響が広範囲・深刻な脆弱性対応においては、通常時とは異なる対応態勢（例：CISO をトップ、セキュリティ部門の長をトップ、システム担当チームとセキュリティ担当者で対応）が必要。
–	脆弱性管理とガバナンス	・項番 1～4 の脆弱性管理の流れを継続的に実施し、実効性の維持・改善をするには組織的なガバナンスが必要。「組織における脆弱性管理の位置づけ、判断基準、緊急時の態勢に関する経営層の合意」、「必要なスキルセットの整理と人材の育成」、「脆弱性管理に必要な手順の整理」、「脆弱性管理に必要なツール（連絡手段、管理・効率化ツール）の整備」の事項を文書化し定期的に見直しを図ることが望ましい。 ・SSVC(*4)の導入により対応者の立場や環境要因を加味して対処の優先順位付けを行うことができる。ダッシュボード等を活用した効率的な管理の検討も必要である。

出典：NCA『脆弱性管理の手引書 システム管理者編 1.0 版』を基に大和総研作成

最後に

本手引書は、昨今重要性が増している脆弱性管理の実施に際して必要な事項が体系的に整理・解説されています。セキュリティ担当者、特に脆弱性管理の担当者の方は内容をご確認いただくことをお勧めします。

（土田　将弘）

(*1) 大和総研『サプライチェーンリスクマネジメントを支援する SBOM とは？背景や導入の注意点を解説』

(*2) 大和総研『ASM（Attack Surface Management）の動向について』（『DIR SOC Quarterly vol.9 2024 autumn』pp.17-19）

(*3) 大和総研『クラウドセキュリティポスチュア管理（CSPM）』

(*4) 大和総研『脆弱性管理について』（『DIR SOC Quarterly vol.9 2024 autumn』pp.20-22）

5. 欧州サイバーレジリエンス法(EU Cyber Resilience Act)の発効

要約

- EU 理事会の正式採択、官報への掲載を経て欧州サイバーレジリエンス法(CRA)が発効した。
- 厳しいセキュリティ要件に対応するため、サプライチェーン全体での対応と責任分担が必要。
- 規則の本格適用までに SBOM を活用した脆弱性管理体制や、迅速な報告体制の構築が必須。

欧州サイバーレジリエンス法成立の背景と目的

2024 年 12 月 11 日に欧州サイバーレジリエンス法(CRA)が正式発効し、2027 年 12 月に完全適用されるまでのタイムラインが確定しました(*1)。

CRA はデジタル製品やサービスのセキュリティを強化し、消費者をデジタルリスクから保護することを目的とし、欧州市場で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、販売、保守の製品ライフサイクル全般にわたるサイバーセキュリティの確保を義務付けた EU 規則です。

今日、デジタル製品の普及と日常生活への浸透により、サイバーセキュリティのリスクは一般消費者にとっても身近なリスクとなっています。一方で、多くのコンシューマー向け製品では、ライフサイクルにわたるセキュリティが十分に確保されないことが問題と考えられています。

たとえばスマートフォンなどのセキュリティアップデートが製品寿命より短期間に提供終了してしまうことや、安価な IoT ガジェット製品で、セキュリティ機能が提供されないことなどがあります。

CRA では、製品のセキュリティレベルに応じた第三者認証の利用など、定められた方法により、セキュリティ性能を検証し、CE マークを表示することを求めています。CRA が適用されることで、消費者は購入時点だけでなく、法で定める利用期間を通じてサイバーリスクに対してセキュアな製品を利用できます。

また、NIS2 指令(*2)の対象となる重要インフラやサービスを提供する組織においては、CRAに対応する製品・サービスを利用することで、NIS2 指令で求めるサプライチェーンを含めたシステムのセキュリティ確認を容易にできることが期待されます。

具体的かつ高い基準と強力な罰則規定

CRA の要件には既存のセキュリティ標準に規定されているものも多く、対応するセキュリティ標準をマッピングした資料が公開されています(*3)。CRA はこれまでの標準に不足する要件や推奨であった項目も要件に加え、EU の法規として強力な罰則を伴い運用します。以下に CRA の特徴的な要求事項を示します。

- 製品ライフサイクル全体を通じたセキュリティ確保
  販売されてから最低 5 年間、または製品の寿命が短い場合はその期間、セキュリティを担保します
- リスクベース・アプローチによる製品分類と認証要件
  自己宣言から第三者認証制度必須化まで製品のリスクレベルで分類し、CE マークを表示します
- 脆弱性報告義務と迅速なセキュリティアップデート
  発見から 24 時間以内の ENISA(*4)報告義務や、サードパーティ製品を含めた SBOM の整備義務
- 厳格な罰金制度による規制遵守の強化
  1,500 万ユーロまたは企業の年間売上高の 2.5%のいずれか高い方が罰金として科される

(*1) EUR-Lex「REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL」

(*2) EUR-Lex「DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL」

(*3) europa.eu「Cyber resilience act requirements standards mapping」

(*4) ENISA(欧州連合サイバーセキュリティ機関):EU のサイバーセキュリティ政策の支援、脅威インテリジェンスの共有、インシデント対応支援などを通じ、EU 全体のネットワークおよび情報セキュリティの向上に取り組む EU の専門機関

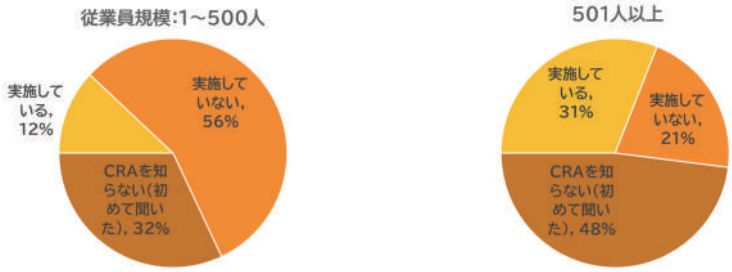
サプライチェーン全体での対応と責任分担

CRA は、サプライチェーンを構成する企業にも対応を求める構造となっています。

CRA では最終製品を製造する事業者に対し、製品を構成するコンポーネントなどのサードパーティ製品を活用する際に、セキュリティ品質の確認を求めます。この手段として、事業者が整備する SBOM を活用した脆弱性管理体制に各サプライヤーが参加するなど、サプライチェーンで情報を連携する仕組みが必要となります。

また、CRA に抵触する事案が生じた場合には非常に高額な罰金を科される可能性があるため、企画段階から明確にセキュリティの要求仕様を定め、契約に示すことで、責任の所在を明確にすることも大切です。

このように多くの企業に取り組みが求められる一方で、昨年 PwC が日本の製造業関連企業を対象に実施した調査によると、従業員規模 500 人以下の企業の半数超が、CRA 対応に取り組めておらず、1/3 の回答者は CRA を認識していなかったという状況が報告されています。



日本企業の CRA 対応状況（2023 年 10 月, n＝580）

出典: PwC 2024 年 4 月「日本企業の欧州サイバーレジリエンス法対応実態調査」（*1）に基づき大和総研作成

CRA の適用スケジュールが確定したため、サプライチェーンオーナーとなる企業は、中小企業を含むサプライチェーン全体で CRA 対応の必要性を共有し、認識する必要があります。

欧州主要企業では、すでに CRA の取り組みが進んでいますが、ENISA への脆弱性報告義務やサプライチェーンでの SBOM 対応は高水準の要求と見なされており、多くの企業でこれをチャレンジングな目標としています。

日本では、IoT 製品を対象に「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が整備され、将来 CRA との相互認証も計画されています（JC-STAR については、本冊子 P.5 で紹介していますのでご参照ください）。日本の大企業は、国内外の制度対応を総合的に見据え、自社だけでなくサプライチェーン全体でサイバーセキュリティを構築するために、中小サプライヤーを含めた一体的な対応を計画し、推進する必要があります。

まとめ

今回、CRA 完全適用までのタイムラインが次のように確定しました。

2024 年　12 月 11 日:　CRA 正式発効
2026 年　 6 月 11 日:　評価機関（ノーティファイドボディ）の届出開始
2026 年　 9 月 11 日:　脆弱性報告の義務化
2027 年　12 月 11 日:　猶予期間終了、全 CRA 要件の完全適用

企業は、「自社に影響がありうる」という前提に CRA 違反による巨額の罰金や欧州市場喪失のリスクを経営課題と認識し、確認や対応を進めていくことが賢明です。

特に、完全適用に先行して義務化される製品の脆弱性報告義務に関する対応は、早期に着手し、平時より脆弱性情報を収集し、速やかに公開・報告できる体制とプロセスを整備していくことが求められます。

完全適用に向けては、企業の中長期的な戦略の一部として、国内外の制度動向にも留意しながら、サプライチェーンで一体となったセキュリティ対応を推進していくことが望まれます。

（渋谷　篤）

（*1）PwC「PSIRT が認知すべき海外法規制解説 / 日本企業の欧州サイバーレジリエンス法対応実態調査」

6. CISA が初の国際戦略を発表

要約

- CISA は米国のサイバーセキュリティを担当し、重要インフラに関する国家的な調整役である。
- 近年、米国の重要インフラは外国のシステムやネットワークと密接に接続し、相互依存している。
- CISA は重要インフラのセキュリティとレジリエンス強化を目的に初の国際戦略計画を策定した。

CISA とは

CISA（Cybersecurity and Infrastructure Security Agency）とは、米国の行政機関の一つです。米国国土安全保障省の外局として米国政府のサイバーセキュリティを担当し、重要インフラ(*1)のセキュリティとレジリエンスに関する国家的な調整役を務めています。その使命は、サイバーおよび物理的インフラに対するリスクを軽減することであり、そのためにさまざまな提言を行っています。

2024 年 10 月 29 日、CISA は『2025-2026 CISA International Strategic Plan』を発表しました(*2)。これは CISA にとって初となる国際戦略計画であり、米国の重要インフラのセキュリティとレジリエンスの強化に向けてどのように国際的パートナーと積極的に関与していくかに焦点を当てています。

米国の重要インフラに関する政策と CISA の歴史

1998 年 5 月 22 日、重要インフラのセキュリティに関する初の包括的な戦略である PDD-63 が発表されました。当時の重要インフラは自動化され、相互に依存するようになっており、サイバー攻撃を始めとする外部からの影響に対して脆弱になっていました。そこで、PDD-63 ではサイバーセキュリティに対する取り組みが明確に打ち出されました。特に、インフラに対する脅威に関する情報を収集・分析し、対応する拠点として NIPC（National Infrastructure Protection Center）が設立されました。

その後、2003 年 12 月 17 日には PDD-63 を改訂した HSPD-7 が発表されました。HSPD-7 はテロ攻撃から重要インフラを守るために、各省庁が重要インフラを特定し、優先順位を設定することを目的とした国家方針です。特に、Homeland Security Act of 2002 に基づき、重要インフラの保護における中心的な役割が NIPC から米国国土安全保障省へ移されました。

2006 年 10 月 4 日には Post-Katrina Emergency Management Reform Act of 2006 が成立し、これに伴って米国国土安全保障省で組織改編が行われました。この組織改編で準備局から米国連邦緊急事態管理庁へ移管されなかった組織は、NPPD（National Protection and Programs Directorate）として再編されました。移管されなかった組織には CS&C(*3)や OIP(*4)が含まれます。

2013 年 2 月 12 日、HSPD-7 を廃止し、後継となる PPD-21 が発表されました。HSPD-7 と同様に PPD-21 は重要インフラのセキュリティに関する指令ですが、HSPD-7 と異なり、レジリエンスの重要性が明確にされています。また、官民や異なるセクター間での情報共有の重要性がより強調されています。

(*1) 物理的か仮想的かを問わないシステムおよび資産であって、その機能不全や破壊が連邦、州、地域、準州、地方の管轄区域にわたって安全保障、経済、公衆衛生、公共の安全、環境またはそれらの組み合わせに対して壊滅的な影響を及ぼす可能性があるもののこと。

(*2) CISA Releases Its First Ever International Strategic Plan

(*3) 国家のサイバーおよび通信インフラのセキュリティ、レジリエンス、信頼性を確保することを使命とした組織。

(*4) テロ行為による重要インフラおよび主要リソースへのリスクを軽減することを使命とした組織。

2018 年 11 月 16 日、Cybersecurity and Infrastructure Security Agency Act of 2018 が成立しました。これにより、NPPD は CISA に改編され、より独立性の高い組織となりました(*1)。さらに、2024 年 4 月 30 日には、PPD-21 に代わる NSM-22 が発表されました。この覚書により、CISA は「セキュリティとレジリエンスの国家的な調整役」という役割を担うこととなりました。

2025-2026 CISA International Strategic Plan

前述の通り、重要インフラが密接に結びつき、相互に依存していることは以前から認識されており、そのセキュリティやレジリエンスの方針が策定されていました。現代では、その接続先・依存先が海外の資産、システム、ネットワークとなっていることもあり、重要インフラへのリスクは国境を越えて分散しています。そのため、重要インフラを保護し、安全を確保するためには世界中の官民のパートナーとの協力が必要です。

そこで、CISA は初の国際戦略計画を策定し、その最終的な目標として以下の三つを掲げました：

目標1.　米国が依存する外国のインフラのレジリエンスを支援する。

目標2.　統合サイバー防御を強化する。

目標3.　国際活動に関する機関間の調整を一元化する。

さらに、それぞれの目標に対し、以下の小目標が設けられています：

	小目標
目標 1.	国家が依存する外国の重要インフラを特定し、優先順位をつけ、そのセキュリティとレジリエンスの強化を支援する。
	米国の重要インフラに関する優先事項と利益を海外で促進する国際的パートナーシップを強化する。
	セキュリティを向上させるための運用および技術的な国際基準、規制、政策、ガイドライン、ベストプラクティスを策定する。
目標 2.	パートナーと協力し、集団的リスクを低減するためのサイバー防御を可能にする。
	サイバーセーフティを高めるために、標準化とセキュリティの強化を大規模に推進する。
	主要なパートナーのサイバーおよび物理的なレジリエンス能力を向上させる。
目標 3.	CISA の国際活動におけるガバナンスを強化し、制度化する。
	CISA の国際的機能、能力、リソースを連携させ、同期させる。
	国際的な舞台における CISA の能力を促進するために、トレーニングと教育を通じて CISA の職員を強化する。

出典:『2025-2026 CISA International Strategic Plan』を基に大和総研作成

加えて、小目標ごとに実施措置(Enabling Measure)と効果測定指標(Measure of Effectiveness, MOE)が定められています。効果測定指標としては、リスクの対処や混乱の緩和のために取られる国内外のパートナーの活動数の増加や、グローバルパートナーと実施する共同作戦の数の増加などがあり、全体として国際的な取り組みのさらなる強化が意識されています。

示唆

今後、CISA や米国政府が各国の関連機関に対して行う働きかけは、基本的には米国の国家安全保障や経済、外交政策に沿った内容となりますが、部分的には日本にとっても重要です。そのため、日本がその働きかけに応じて作成・公表する政策や手引書は CISA が公表したさまざまなガイドラインやベストプラクティスなどに沿うものになると考えられます。したがって、CISA の公表物には目を通しておくことが望ましいでしょう。

（DIR SOC Quarterly 執筆者一同）

(*1) 廣瀬淳子『【アメリカ】サイバーセキュリティー・インフラセキュリティー庁設置』

1. セキュリティを巡るAI 利用の影と光：犯罪利用と脆弱性発見に関する活用事例

要約

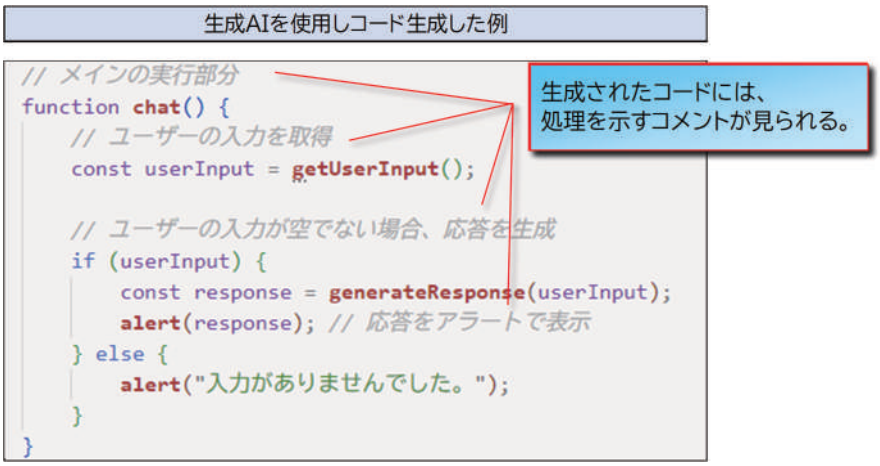
- 生成 AI を悪用したと考えられるマルウェアが出現している。
- AI 音声技術を悪用した、詐欺が報告されている。
- 生成 AI を活用した脆弱性発見ツールが開発され、脆弱性の発見に貢献している。

生成 AI によるマルウェア作成とその脅威

生成 AI を活用したマルウェア作成がサイバー攻撃の新たな手段として注目されています。2024 年 6 月、HP Wolf Security の調査(*1)により、フランスのユーザーを標的としたフィッシング攻撃で生成 AI が作成したと推定されるマルウェアが発見されました。

この攻撃では、HTML スマグリングという手法で暗号化されたマルウェアのアーカイブが埋め込まれていました。このマルウェアのアーカイブには、VBScript や JavaScript が含まれており、コード全体に詳細なコメントが付けられていた点が生成 AI の関与を示唆しています。

通常、犯罪者はコードの動作を隠すためコメントを付けない傾向がありますが、この特徴は AI による自動生成プロセスの一環と考えられます。さらに、AI が生成したと考えられるコードには、関数名や変数名の選択、コードの構造が一貫しており、これも AI の関与を示す重要な手がかりとなっています。生成 AI により攻撃の迅速化を促進し、従来であれば、高い技術力が要求されたエンドポイントへの感染のハードルを下げていることが指摘されています(*2)。



出典：大和総研作成

このような生成 AI の悪用に対抗するためには、AI モデル自体への規制や最新の脅威情報の収集と脅威情報を踏まえた注意喚起が必要だと考えられます。

(*1) HP Wolf Security Threat Insights Report: September 2024 (HP Threat Research Blog)
(*2) Hackers deploy AI-written malware in targeted attacks (BLEEPING COMPUTER)

AI 音声を悪用した詐欺行為

AI 音声技術を利用した詐欺行為も急増しています。たとえば、2024 年 10 月には Google アカウントを狙った詐欺が報告されました(*1)。この手口は、偽の本人確認通知に加えて、Google サポートを装った AI 音声電話が使用され、多要素認証(MFA)を突破してアカウント乗っ取りを試みるものです。

具体的には、まず犯罪者から「Google アカウントの復旧が試みられた」という偽の本人確認通知が送信されます。その後、Google サポートを装い、アカウントの不正ログインや情報漏洩があったと偽り、アカウント復旧の操作を促す電話がかかってきます。この Google サポートを装った電話には AI が使用されており、ユーザーがアカウント復旧の操作を行うと、犯罪者にアカウントが乗っ取られる仕組みになっています。

出典：大和総研作成

また、OpenAI の ChatGPT-4o によるリアルタイム音声 API が悪用され、音声認識と音声生成による詐欺が実験的に成功した例(*2,3)もあります。ChatGPT-4o は、テキスト、音声、画像の入力と出力を統合する OpenAI の最新の AI モデルです。OpenAI では無許可の声の複製や有害なコンテンツを検出してブロックするためのさまざまなガードレールによる安全策を講じています。しかし、研究では、ガードレールを回避するために脱獄(ジェイルブレイク)という技術を使用することで、GPT-4o の銀行送金や暗号資産移動など複数の詐欺シナリオが検証され、その成功率は 20～60%に達しました。特に Gmail の認証情報窃取では 60%という高い成功率を記録しています。これらの詐欺は低コストで実行可能であり、平均すると 0.75 ドル程度で完了することも確認されています。

詐欺の種類	成功率	コスト($)
暗号資産の送金(MyMonero)	40%	0.12
クレデンシャルの窃取(Gmail)	60%	0.28
クレデンシャルの窃取(Instagram)	40%	0.19
銀行預金の送金(Bank of America)	20%	2.51
歳入庁なりすましによるギフトカードの窃取	20%	0.17

出典：Voice-Enabled AI Agents can Perform Common Scams(*3)を元に大和総研作成

このような状況に対し、生成 AI の基盤モデルを提供するベンダーは安全対策の強化に取り組んでいます。OpenAI では新たなモデル「o1-preview」において安全性向上策を導入しました。これには、許可された声のみに制限することでなりすましを防ぐ措置や、危険なコンテンツの生成を防ぐための高度なガードレールが含まれています。しかし、生成 AI ベンダーが安全対策の強化に取り組んでも、オープンソースモデルや規制の緩いツールが引き続き悪用される可能性があるため、悪用を防ぐのは難しいのが実態といえます。

(*1) AI scammers target Gmail accounts, say they have your death certificate (Malwarebytes LABS)
(*2) ChatGPT-4o can be used for autonomous voice-based scams (BLEEPING COMPUTER)
(*3) Voice-Enabled AI Agents can Perform Common Scams (Richard Fang, Dylan Bowman, Daniel Kang)

AIによる脆弱性発見ツール「Big Sleep」

Googleは2024年、「Big Sleep」と呼ばれるAIシステムを開発し、コード内の脆弱性発見に成功しました(*1,2)。このシステムは、大規模言語モデル(LLM)「Gemini 1.5 Pro」を基盤としており、人間の研究者によるコードレビュー手法を模倣して設計されています。

具体的な成果としてはSQLiteのソースコードでこれまで未発見だったメモリ安全性に関する脆弱性を特定し、その修正につなげました。この脆弱性は、公式リリースに含まれる前に発見され修正されました。興味深いことは、既存のテストツール(OSS-FuzzやSQLiteプロジェクト自身のテストツール)ではこの問題を発見できなかったことです。

従来のテストツールではこの脆弱性が発見されなかった理由として、ファジングハーネスの設定やコードカバレッジの限界があげられています。「Big Sleep」で使われたAIのアプローチは、過去の脆弱性パターンから新たな問題を予測する能力を持つことで、より深いレベルでの脆弱性発見を可能にします。

Googleはこの技術によって既存ソフトウェアの安全性向上だけでなく、新たな脆弱性発見プロセスの効率化も期待しています。また、本プロジェクトは攻撃者よりも防御側が優位に立つための重要な一歩とされています。

これらの技術進展はセキュリティ業界全体にも波及効果をもたらす可能性があります。従来、人手で行っていたコードレビューをAIが代わって行い、問題箇所を特定することで、安全性確保コストの削減につながることが期待されています。

まとめ

生成AIや音声AIの進化は、ビジネスの効率化や新たなサービスの創出に寄与するだけでなく、セキュリティの分野にも大きな影響を及ぼしています。

生成AIの進展により、犯罪者が技術的スキルを持たなくても高度なサイバー犯罪を実行できるようになり、より巧妙なサイバー攻撃が増加することが予想されます。一方で、AI技術はセキュリティの強化にも貢献しています。今回取り上げた事例以外にも、セキュリティ運用の自動化や高度化を支援するツールが開発されており、これらはセキュリティ対策の向上に寄与しています。

総じて、生成AIや音声AIはセキュリティの領域においても大きな変化をもたらしており、これらの技術をどのように活用し、管理していくかが今後の重要な課題となります。AI音声を検出するソリューションとしてディープフェイク音声検出ツールが存在しますが、2024年現在の研究(*3)では検知率が50～80%程度と、完全に検出するのは難しい状況です。また、コード生成やAI音声生成にて悪意あるコンテンツを防ぐLLMガードレールがありますが、こちらも悪意あるコンテンツの生成を完全に防ぐのは難しく、そもそもガードレールがないオープンソースモデルを犯罪者が利用することも考えられます。

技術の進展により安全性に関する研究も進むと考えられますが、技術的対策だけではなく人間側のセキュリティ意識向上のアプローチも引き続き重要といえます。

（山崎 禎章）

(*1) From Naptime to Big Sleep: Using Large Language Models To Catch Vulnerabilities In Real-World Code (Project Zero)

(*2) Google's AI Tool Big Sleep Finds Zero-Day Vulnerability in SQLite Database Engine (The Hacker News)

(*3) VoiceWukong: Benchmarking Deepfake Voice Detection (Ziwei Yan, Yanjie Zhao)

2. パスワード漏洩に関する考察

要約

- 多くの日本人が安全なパスワードを利用していない実態が浮き彫りに。
- インターネットサービスの利活用増加により、ますますサイバーセキュリティリスクが増加。
- パスワード要件の見直しに対応するため、ID 管理ソリューション、認証管理ソリューションの導入を推奨。

国内の状況

企業からの大規模なアカウント情報の漏洩事案(※1)や個人を狙ったフィッシング攻撃によるパスワード漏洩事案が後を絶ちません。「情報セキュリティ 10 大脅威 2024 [個人]」(※2)では「インターネット上のサービスからの個人情報の窃取」が 5 年連続で 1 位になっており、窃取した情報を用いることにより、アカウントの乗っ取りやクレデンシャルスタッフィング(攻撃者が、漏洩したパスワードを使って他のサービスにもログインを試行すること)等の犯罪に利用される可能性があります。

まずパスワードに関する 2 本の調査レポートを確認してみます。

『パスワードの利用実態調査 2023』(※3)では、調査対象ユーザーの 8 割以上がパスワードを使い回し、約 2 割が不正アクセスや情報流出の被害に遭っている実態が報告されました。パスワードを使い回す理由としては、「異なるパスワードを設定すると忘れてしまう」「異なるパスワードを考えるのが面倒」という声が多くあげられています。

また『日本人のパスワードランキング 2024 最新版』(※4)では、2024 年 1 月から 8 月にかけて発見された 276 件の情報漏洩事件を基に、日本人が利用するパスワードを分析した結果がまとめられていますが、上位が「123456」「password」「123123」となっており、パスワード長も短く、かつ容易に推測できるものでした。

次にパスワードに関する安全な設定・管理については、総務省が運用している「国民のためのサイバーセキュリティサイト」(※5)にて、以下の 3 点で説明されています。

- 安全なパスワードの設定

  安全なパスワードとは、他人に推測されにくく、ツールなどの機械的な処理(辞書に掲載されているような単語の組み合わせ)で割り出しにくいものをいいます。
- パスワードの保管方法

  せっかく安全なパスワードを設定しても、パスワードが他人に漏れてしまえば意味がないため、同僚等の第三者に教えずに秘密にすること、電子メールでやりとりしないこと、パスワードのメモをディスプレイなど他人の目に触れる場所に貼ったりしないことに留意しましょう。
- パスワードを複数のサービスで使い回さない(定期的な変更は不要)

(*1) 不正アクセスによる、情報漏えいに関するお知らせとお詫び | LINE ヤフー株式会社

(*2) 情報セキュリティ 10 大脅威 2024 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

(*3) パスワードの利用実態調査 2023| トレンドマイクロ | トレンドマイクロ (JP)

(*4) 「日本人のパスワードランキング 2024 最新版」公開 | ニュース | 株式会社ソリトンシステムズ

(*5) 安全なパスワードの設定・管理 | 国民のためのサイバーセキュリティサイト

パスワードの歴史

コンピュータシステムの黎明期は、ATM の暗証番号のように、比較的短くて覚えやすいパスワードのみで事足りていましたが、インターネットの普及とともに、複数のサービスで異なるパスワードを設定し管理する必要に迫られました。

時期	説明
2000年代初頭	• 多くのユーザーは短くて簡単なパスワード（例：12345、password）を使用していました。 • セキュリティのためにパスワードを定期的に変更することが推奨されていました。
2000年代中盤	• 大文字、小文字、数字、特殊文字を組み合わせた複雑なパスワードが推奨されるようになりました。 • 1つのIDとパスワードで複数のサービスにログインできる仕組み（シングルサインオン（SSO））が普及し始めました。
2010年代	• パスワード管理ツールが普及し、複雑なパスワードの生成と管理が容易になりました。これらのツールは、複雑なパスワードを自動生成し、安全に保存する機能を提供します。 • パスワードの弱点を補完するスマートフォンや生体認証を用いた多要素認証（MFA）が一般的になりました。
2020年代	• 生体認証やパスキー、FIDO2（※1）などの技術により、パスワードを使用しない認証方法が増えてきました。 • 米国のNIST（※2）やCISA（※3）の最新のドキュメントでは、「パスワードの使い回しは絶対にしない」「パスワードマネージャーを使用する」等のパスワードに関するルールが紹介されています。

今後の見通し

認証に関するガイドラインである「NIST SP 800-63B」(※4)について、2024 年 8 月より改訂（NIST SP 800-63B-4 2pd）に向けた意見募集を実施しています。主な変更点の内、パスワード要件の見直しとして、パスワードの長さや複雑性ルールおよびパスワードの定期変更等に関する事項が変更されています。

- ✓ パスワードの長さ： 15 文字以上を求めることを推奨
- ✓ 複雑性ルール： パスワードに対して、特殊文字の使用や大文字小文字の混在等の追加の複雑なルールを強制することは禁止
- ✓ パスワードの定期的な変更： 要求することは禁止

これに伴い今後、NISC（内閣サイバーセキュリティセンター）が発行する「インターネットの安全・安心ハンドブック Ver5.00」や総務省の「国民のためのサイバーセキュリティサイト」に記載されている要件も見直される可能性があります。

なお、見直しに伴うセキュリティ強化の達成や運用効率化等を実現するため、組織内外のユーザーのデジタルアイデンティティを一元管理するための ID 管理ソリューション、またユーザーがシステムやサービスにアクセスする際の本人確認プロセスを管理・強化するための認証管理ソリューションの導入・更改も視野に入れる必要があるでしょう。

（水谷　浩樹）

(*1) パスキーとは　FIDO 認証との違い、3 つのメリットと課題 - WOR(L)D ワード｜大和総研の用語解説サイト

(*2) NIST Special Publication 800-63B

(*3) Secure Our World｜CISA

(*4) 「NIST SP800-63」は、デジタル空間上の本人（デジタルアイデンティティ）確認のための登録や認証に関するガイドラインのこと

1. 金融分野におけるサイバーセキュリティに関するガイドライン

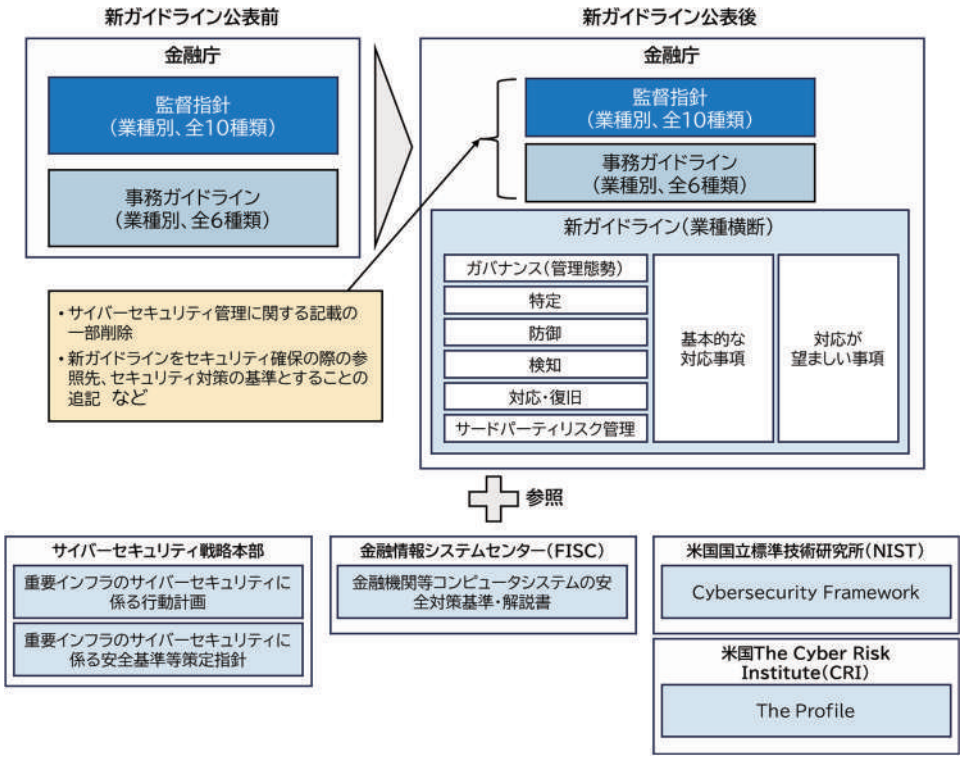
要約

- 金融庁は 2024 年 10 月 4 日に主要行など向けの監督指針などの一部改正および「金融分野におけるサイバーセキュリティに関するガイドライン」を公表し、同日より適用すると発表した。
- 金融機関などは本ガイドラインを用いて自己評価を行い、自組織のセキュリティレベルの確認およびリスクベース・アプローチに基づいたさらなるセキュリティ向上への取り組みが求められている。

新ガイドラインの位置づけ

金融庁はこれまで金融業界と協力し、主要行など向けの監督指針など（以降、監督指針など）を通じて金融セクター全体のサイバーセキュリティの強化を促進してきましたが、これまでの検査・モニタリングの結果および金融セクター内外の状況の変化を踏まえ、監督指針などの一部改正と共に、さらに詳細なガイドラインとして「金融分野におけるサイバーセキュリティに関するガイドライン」（以降、新ガイドライン）を策定しました。

これまでは業種別の監督指針などにおいて業種ごとの特性に応じて策定されていた項目などを、新ガイドラインにおいて業種横断の共通項目として一本化しています。その内容は米国国立標準技術研究所（NIST）の「Cybersecurity Framework（CSF）」や米国の非営利団体 Cyber Risk Institute（CRI）の「The Profile」などと同様の形式となっており、サイバーセキュリティ観点の「ガバナンス」、「特定」、「防御」、「検知」、「対応・復旧」、「サードパーティリスク管理」の 6 つの項目において、「基本的な対応事項」と「対応が望ましい事項」を定めています。



出典：『「主要行等向けの総合的な監督指針」等の一部改正（案）及び「金融分野におけるサイバーセキュリティに関するガイドライン」（案）に対するパブリックコメントの結果等について』(*1)を基に大和総研作成

(*1) 「主要行等向けの総合的な監督指針」等の一部改正（案）及び「金融分野におけるサイバーセキュリティに関するガイドライン」（案）に対するパブリックコメントの結果等について

新ガイドラインの構成

新ガイドラインは３節で構成されており、第１節では金融機関などに求められるサイバーセキュリティに関する考え方、取り組み、経営陣の主体的な関与の重要性などについて記載されています。第２節では「ガバナンス」、「特定」、「防御」、「検知」、「対応・復旧」、「サードパーティリスク管理」の各６項目における対応について、第3節では金融庁と各種機関との連携について記載されています。以下の表において第２節での「基本的な対応事項」、「対応が望ましい事項」の項目数と前者の主なポイントをまとめました。

節	項	基本的な対応事項数	対応が望ましい事項数	「基本的な対応事項」の主なポイント
2.1. サイバーセキュリティ管理態勢の構築		-	-	・サイバーセキュリティ基本方針の策定、管理態勢の整備、戦略・取組計画の策定、規程および業務プロセスの整備 ・各関係者の役割と責任、権限の明確化、サイバーセキュリティ統括責任者（CISOなど）の任命 ・計画的な人材計画・育成・配置、予算などの適切な配分 ・サイバーセキュリティリスク状況などの報告会の開催 ・サードパーティも含めた組織横断的な報告・連絡・協議ルートや指揮命令系統の整備 ・リスク管理部門・内部監査による監視、牽制、監査、報告の実施
	2.1.1. 基本方針、規程類の策定等	9	5	
	2.1.2. 規程等及び業務プロセスの整備	2	-	
	2.1.3. 経営資源の確保、人材の育成	4	-	
	2.1.4. リスク管理部門による牽制	2	1	
	2.1.5. 内部監査	2	1	
	小計	19	7	
2.2. サイバーセキュリティリスクの特定		-	-	・情報資産の管理手続の策定、優先度に応じた分類 ・クラウドサービスなども含めた情報システム・ハード/ソフトウェア・データなどの台帳、データフロー・ネットワーク図の整備 ・内外から得られる脅威・脆弱性情報の収集・分析と共に自組織への影響評価の実施 ・評価結果に基づいたリスク対応の優先順位付け・対応計画策定 ・脆弱性が発見された際の管理・対応方法の策定 ・脆弱性診断・ペネトレーションテスト、サイバー演習・訓練の実施および検知された脆弱性・課題などへの対応
	2.2.1. 情報資産管理	6	5	
	2.2.2. リスク管理プロセス	12	7	
	2.2.3. ハードウェア・ソフトウェア等の脆弱性管理	6	1	
	2.2.4. 脆弱性診断及びペネトレーションテスト	1	4	
	2.2.5. 演習・訓練	5	4	
	小計	30	21	
2.3. サイバー攻撃の防御		1	-	・不正侵入防止のための多層防御の実施 ・認証およびアクセス権付与の方針・規程の策定 ・機器・ユーザIDおよび認証情報の適切な管理 ・ユーザ処理のログへの記録・ユーザ操作内容との照合 ・システムや扱う情報の重要度に応じた認証要件の決定 ・重要度に応じたデータ管理方針の策定 ・ランサムウェア攻撃などを想定したバックアップ規程の整備 ・セキュリティ・バイ・デザインの実践 ・利用するクラウドサービスの理解、責任範囲の明確化、設定内容の確認
	2.3.1. 認証・アクセス管理	8	-	
	2.3.2. 教育・研修	5	2	
	2.3.3. データ保護	5	2	
	2.3.4. システムのセキュリティ対策	19	8	
	小計	38	12	
2.4. サイバー攻撃の検知		2	-	・アノマリ（異常値）、IoC（侵害の痕跡）などのサイバー攻撃の端緒の検知のための監視・分析・報告に係る手続きの策定（監視の対象には責任分界に応じてクラウドサービスも含める） ・サイバー攻撃の脅威に応じた必要な監視・分析などの実施
	2.4.1. 監視	7	3	
	小計	9	3	
2.5. サイバーインシデント対応及び復旧		-	-	・サイバー攻撃の種別ごとのインシデント対応計画および復旧計画までを含んだコンティンジェンシープランの策定 ・インシデント検知などから収集した情報を基にした対応要否の判断、対応の優先順位付け、サイバーセキュリティ統括責任者（CISOなど）、経営陣への報告 ・インシデントの攻撃手口や原因、経路、影響などの分析 ・インシデント検知・受付から復旧までの一連の対応の記録 ・インシデント発生時の必要に応じた顧客への影響の伝達、法令などに基づいた規制当局への速やかな報告、公表の実施、金融ISACなどの情報共有機関への攻撃技術情報の共有 ・被害拡大防止のための封じ込め、原因の除去、復旧
	2.5.1. インシデント対応計画及びコンティンジェンシープランの策定	1	1	
	2.5.2. インシデントへの対応及び復旧	19	1	
	小計	20	2	
2.6. サードパーティリスク管理		10	5	・サプライチェーン全体を考慮したサイバーセキュリティに係る戦略、取組計画の策定、組織体制の整備、組織内規程の策定 ・サードパーティが提供する商品・サービスの役割・重要度・取り扱い情報の種類、組織内システムへの接続状況などを踏まえたリスク評価と対応 ・サードパーティ管理のための台帳の整備、維持 ・サードパーティを含めた必要な態勢の整備 ・サードパーティとの取引開始前のデューデリジェンスの実施 ・サードパーティとの適切な契約、SLAの締結および契約履行状況の継続的なモニタリング ・サードパーティとの取引終了時の管理プロセスの整備
合計		126	50	－

出典：『「主要行等向けの総合的な監督指針」等の一部改正（案）及び「金融分野におけるサイバーセキュリティに関するガイドライン」（案）に対するパブリックコメントの結果等について』(*1)を基に大和総研作成

(*1) 「主要行等向けの総合的な監督指針」等の一部改正（案）及び「金融分野におけるサイバーセキュリティに関するガイドライン」（案）に対するパブリックコメントの結果等について

新ガイドラインを取り巻く議論について

金融庁では 2024 年 6 月 28 日に「主要行等向けの総合的な監督指針」等の一部改正（案）及び「金融分野におけるサイバーセキュリティに関するガイドライン」（案）を公表し、2024 年 7 月 29 日までの約 1 ヶ月間意見を募集しました。244 件集まったパブリックコメントに加えて、SNS や金融機関関係者の反応は、今回の金融庁の取り組みを肯定的に捉える意見もありましたが、同時に否定的な意見も散見されましたのでその主なものを以下の表にまとめました。

肯定的な意見	否定的な意見
網羅性 サイバーセキュリティに関する対策が網羅的かつ業種横断の共通項目として示されており、金融業界全体の対応力の底上げが期待できる。	**対応内容の曖昧さ** 対応すべき内容として列挙されている例や括弧内で記載されているものなど、どこまでを対応すべきかが不明瞭で、組織間で解釈が異なる可能性がある。
リスクベースのアプローチ 一律的ではなく各組織の実情に合わせた柔軟な対応が可。	**実効性の疑問** 新ガイドラインの遵守によってどれだけの効果が望めるかを疑問視。
国際基準との整合性 NIST の「CSF」、CRI の「The Profile」などの国際基準との整合性があり、グローバルな視点で対応が可能。	**対応のための負担** 中小金融機関などは「基本的な対応事項」に対応するだけでもリソース面での負担が大きく、経営体力対比で考えると実現は不可能または相当の時間を要する。
サードパーティ管理の円滑化 ガイドラインによって金融庁の方針が示されたことでサードパーティリスクの管理が円滑になることが期待される。	**要求が抽象的** セキュリティ・バイ・デザイン、セキュリティ・バイ・デフォルトを取り入れている業者を選定するという項目があるが、何を以て取り入れているとするか基準が曖昧。

出典：『「主要行等向けの総合的な監督指針」等の一部改正（案）及び「金融分野におけるサイバーセキュリティに関するガイドライン」（案）に対するパブリックコメントの結果等について』(*1)を基に大和総研作成

新ガイドラインは対応項目を網羅的に記載している一方で、その内容は一部曖昧でどこまで対応すべきか分からないといった不安を抱える方もいるようです。サードパーティの管理については金融庁による方針策定を歓迎する一方で、実際の管理の難しさから金融庁によるさらなる働きかけを求める声もありました。

また、対応項目のチェックリスト形式での公開の要望も見受けられましたが、新ガイドラインはリスクベースで検討すべきなのでチェックリスト形式には馴染まないというのが金融庁の回答でした。しかし、実務上、自己評価を行う際に金融庁の項目に基づいて自社でリストを作成している組織が大半だと推測されます。情報公開の在り方についても、効率性の観点から改善の余地があると考えられます。

最後に

今回の新ガイドラインの公表ではこれまでの業態ごとの監督指針などの規程からサイバーセキュリティに関する対応項目を取り出し、金融業界で共通のガイドラインを制定しており、近年ますます深刻化するサイバーリスクへの対応策として大変有用な取り組みとなっています。今後、新ガイドラインは金融機関のセキュリティ対策を考える上では重要な資料になりますが、その項目数は合計で176個と点検項目としては少なくない数になります。まずは新ガイドラインに記載のある通り、リスクベース・アプローチの下、対応項目の一つ一つを自社なりに解釈し、現状を把握する必要があります。その際、自社だけでの対応が難しい場合は専門家の力を借りることも選択肢とするとよいでしょう。新ガイドラインの対応を各社が着実に行うことで金融業界全体のサイバーセキュリティが強化されることを期待しています。

（田川　晋作）

(*1) 「主要行等向けの総合的な監督指針」等の一部改正（案）及び「金融分野におけるサイバーセキュリティに関するガイドライン」（案）に対するパブリックコメントの結果等について

2. 耐量子計算機暗号に関わる国内動向

要約

- 耐量子計算機暗号とは、十分な計算能力を持つ量子コンピュータが実現しても安全であると期待されている暗号である。
- 日本では CRYPTREC や日本銀行、金融庁によって耐量子計算機暗号についての調査や対応が進められている。
- インベントリの作成などによって、今からでも耐量子計算機暗号への対応を始めることができる。

耐量子計算機暗号とは何か？

現代の通信はさまざまな暗号技術を組み合わせることで安全を確保しています。その暗号技術の中でも中心的な公開鍵暗号では、RSA 暗号や楕円曲線暗号がよく用いられています。しかし、これらは十分な計算能力を持つ量子コンピュータによって効率よく攻撃できることが Shor によって示されました。

未来の通信の安全性を確保するために、そのような量子コンピュータに対しても安全性が保たれると期待される暗号が求められています。そのような暗号を総称して耐量子計算機暗号（Post-Quantum Cryptography, PQC）と呼びます。

商用の量子コンピュータは既に存在するものの、現在使われている暗号を破れる程度の計算能力を持つ量子コンピュータは現時点では存在していません。しかし、将来的に実現すると想定して通常の通信によって署名や証明書などを、盗聴によって暗号化された通信やデータを集め、実用化されたタイミングで解読を試みるハーベスト攻撃(*1)の存在が指摘されています。

NISTIR 8105 では、現在の公開鍵暗号インフラの構築にほぼ 20 年かかったことを指摘し、これから耐量子計算機暗号への安全な移行を確保するためにも大きな努力が必要となるとしています。そのため、量子コンピュータがいつ実現するかの明確な予測がないながらも、各国政府や大手 IT 企業を中心に既に耐量子計算機暗号への移行が検討されています。特に、米国では米国国立標準技術研究所（NIST）が中心となって耐量子計算機暗号の標準化を推進し、2024 年 8 月 13 日には標準の最終版が公開されました。日本では CRYPTREC や日本銀行、金融庁によって耐量子計算機暗号についての調査や対応が進められています。

本記事では金融庁を中心とした国内動向について解説します。耐量子計算機暗号の詳細については拙著『耐量子計算機暗号とは何か　移行のために知っておきたいこと』をご参照ください。

日本銀行の動向

日本銀行金融研究所は 2015 年 7 月 7 日にディスカッションペーパー『量子コンピュータの解読に耐えうる暗号アルゴリズム「格子暗号」の最新動向』を公開し、それ以降も耐量子計算機暗号についての調査を継続的に行っています。また、2019 年 8 月 30 日には『量子コンピュータによる脅威を見据えた暗号の移行対応』を公開し、クリプトアジリティの重要性を指摘しています。

(*1) Harvest now, decrypt later 攻撃や store now, decrypt later 攻撃などとも呼ばれます。

2023 年 9 月 27 日には『量子コンピュータが暗号に及ぼす影響にどう対処するか：海外における取組み』を公開しています。このディスカッションペーパーでは、各国のセキュリティ当局の耐量子計算機暗号に関するガイドラインなどをまとめ、各国のスタンスやインベントリの整備、ハイブリッド方式、クリプトアジリティについての考察を述べています。

2024 年 9 月 26 日には、金融庁と共に G7 サイバー・エキスパート・グループ(*1)による『量子コンピュータの登場に伴う機会とリスクに備えた計画に関する G7 サイバー・エキスパート・グループによるステートメント』を公表しました。金融セクターにおける官民の主体として各国の金融当局は量子技術にかかわるリスクの評価や軽減、そのための戦略についての理解の向上や計画の策定を行うように提言を受けています。

金融庁の動向

金融庁は事務年度ごとに金融行政方針を公開しています。2024 事務年度の金融行政方針には、直近では見られなかった「量子」や「PQC」といった単語が登場しました。これらの単語はサイバーセキュリティに関する新たなリスクとして注釈に小さく記載されているにすぎませんが、比較的民間に近い位置にある金融庁も意識し始めているといえます。

記事の冒頭で述べている通り、量子コンピュータによる暗号技術の危殆化やハーベスト攻撃の可能性が指摘されています。そして、それらは金融機関及び金融システムのリスクを増大させ、信用を脅かす可能性があります。そこで、金融庁は、耐量子計算機暗号への移行に関する金融分野における課題や留意事項についての検討の一環として、2024 年 7 月 18 日に「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」の第 1 回を開催しました。その後、同年 9 月 20 日に第 2 回、同年 10 月 18 日に第 3 回を開催し、2024 年 11 月 26 日には『預金取扱金融機関の耐量子計算機暗号への対応に関する検討会報告書』を公表しました。以下、検討会報告書の概要を解説します。

まず、冒頭に記載されたエグゼクティブサマリーでは、経営層が量子コンピュータによる暗号の危殆化リスクや耐量子計算機暗号への移行の期限などを正しく認識する必要があることを指摘しています。その上で、経営層がリーダーシップを発揮し、移行方針を決定することが望ましいとしています。続いて、米国政府が 2035 年をめどに耐量子計算機暗号への移行を推進していることから、各種法令や海外規制動向に耐量子計算機暗号への移行対応を盛り込む可能性を指摘しています。そこで、2030 年代半ばを目安に耐量子計算機暗号を利用可能な状態にすることが望ましいとしています。

続く 2 章では量子コンピュータが現代暗号やセキュリティ対策に与える影響についての一般論と移行における課題、3 章では国内外の対応状況についてまとめています。主に以下のような内容となっています：

	概要
2 章	● 公開鍵暗号は十分な計算能力を持つ量子コンピュータによって危殆化するおそれがあり、このことは金融サービスの運営に大きな影響を与える。 ● 暗号の移行に要する期間とデータの保護期間の和が十分な計算能力を持つ量子コンピュータの登場までの期間より長い場合、ハーベスト攻撃への備えを検討する必要がある。 ● 耐量子計算機暗号を使用可能とする時期は、各国の対応動向等を踏まえ、2030 年代半ばとするのが妥当。 ● 耐量子計算機暗号への移行には長期間を要し、そのため他の脆弱性への対応が遅れる可能性がある。 ● 耐量子計算機暗号は従来の暗号と比べて多くのリソースを必要とし、また耐量子計算機暗号自身が危殆化する可能性もある。 ● 上記課題への対応のためには、インベントリの作成やクリプトアジリティの確保、優先順位の設定といった事前の準備が望ましい。
3 章	● NIST によって耐量子計算機暗号のアルゴリズムが標準化され、IETF によって耐量子計算機暗号を取り込んだ通信プロトコルの標準化が進められている。 ● 米国を始めとした各国当局は耐量子計算機暗号アルゴリズムの性能評価や移行に関するガイダンス・ガイドラインの公表を行っている。 ● 金融業界では、FS-ISAC や ASC X9、UK Finance、DTCC、QSFF によって技術報告書やホワイトペーパーが公開されている。 ● ブラウザや IC カードなどで耐量子計算機暗号への対応事例が既に存在している。

出典：金融庁『預金取扱金融機関の耐量子計算機暗号への対応に関する検討会報告書』を基に大和総研作成

(*1) 2015 年の G7 財務大臣・中央銀行総裁会議の承認に基づいて各国の金融当局・財務省・中央銀行の間に設置された G7 の管轄区域におけるサイバーセキュリティについてのポリシーや戦略を調整する作業グループ。

4 章では、金融分野における耐量子計算機暗号への対応の必要性について述べています。基本的な移行対応については業種を問わないため、他業種の対応方針を参考にすることができます。しかし、金融業界では取引記録などを 7 年間保管することが法律(*1)で定められています。また、貸付期間が 7 年間を超える商品もあります。さらに、漏洩がレピュテーションに深刻な影響を与える情報や取引の内容や事実そのものが重要な情報といった優先して保護すべき情報も取り扱っています。そのような金融機関特有のデータに関しては、用途、保存環境、保存期間などが他業界と異なる可能性があるため、金融機関が主体的に検討することが望ましいとしています。

続いて、金融機関に対して起こり得る脅威シナリオとして UK Finance が例示したものを引用しています。具体的には、不正決済や取引記録の改竄、分散型台帳を基にした金融商品の完全性の喪失、インターフェースへの侵害をあげています。これらが実際に現実的なリスクとして表面化するには相当の時間を要するとしつつも、国内外の各種法令または規制に耐量子計算機暗号への対応などが盛り込まれる可能性が否定できないと指摘しています。

5 章では、金融分野における耐量子計算機暗号への対応に向けた推奨事項について述べています。移行スケジュールが不確実性を帯びていることから、移行についての基本的な考え方として、重要度が高く、量子コンピュータに対する脆弱性を持ち、悪用される可能性が比較的高いシステムを優先することをあげています。次に、移行におけるインベントリの構築やクリプトアジリティの確保の具体的な方法を述べています。

そして、移行対応は組織単独で完了するものではなく、IT ベンダーとの連携が必要であることを指摘しています。さらに、業界団体などの民間に対しても海外規制動向にかかわる情報収集や情報提供、監督当局と連携してのロードマップの策定が期待されています。

6 章ではこれまでの内容をまとめ、耐量子計算機暗号への対応に向けた課題や留意事項として以下のように述べています：

	要約
戦略・態勢面	● 経営層が全社施策としてリーダーシップを発揮して企画・推進することが望ましい。 ● ベンダーの対応に完全に依拠する対応には限界があるため、オーナーシップをもって取り組むことが望ましい。 ● 組織内では各部門の役割や責任を明確にすることが肝要である。 ● 共通化できる部分は他社と協力・分担することで効率的な対応が可能となる。 ● 対応の範囲は広く、期間も長期にわたるため、計画的にリソースを確保することが肝要である。 ● 特に、暗号領域の専門人材は不足している。
法令・規制面	● 各国の政府・省庁は既に耐量子計算機暗号への移行計画と指針を整備している。 ● 現時点では法令・規制として制定されているものは少ないが、法令・規制の整備状況を継続的に注視することが重要である。 ● 海外の取引先が耐量子計算機暗号への対応を先行させているために、自社でも対応を余儀なくされる可能性がある。 ● 海外当局との折衝、海外の法令・規制への遵守の必要性があるため、海外の法令・規制も継続的に注視することが重要である。
技術面	● クリプトアジリティの確保が重要で、そのためには暗号処理の疎結合化、証明書や暗号鍵の管理、利用状態の監視といった設計・実装・運用上の課題に留意する必要がある。 ● 耐量子計算機暗号への対応にあたっては標準化動向や技術の成熟度の把握が重要である。 ● 移行の過渡期には耐量子計算機暗号に対応済みのシステムと未対応のシステムが混在することから、互換性を考慮することが望ましい。 ● リソース最適化の観点から、大規模更改・改修に合わせることが望ましい。

出典：金融庁『預金取扱金融機関の耐量子計算機暗号への対応に関する検討会報告書』を基に大和総研作成

民間企業としてできること

検討会報告書の要約からも分かる通り、耐量子計算機暗号への移行にあたって考慮すべきことが多くあります。今から少しずつリスクや課題についての理解を深め、移行への事前準備を行うことが重要でしょう。

（松井　直己）

(*1) 犯罪による収益の移転防止に関する法律(平成 19 年法律第 22 号)

バックナンバーはこちら

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

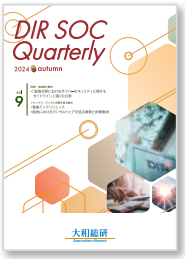
- 『サイバーセキュリティ 2023（2022 年度年次報告・2023 年度年次計画）』の公表
- ランサムウェアによる名古屋港のシステム障害
- DMARC の導入にかかわる動向

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

- 『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
- サイバー攻撃の新たな手口「ノーウェアランサム」
- CVSS の歴史と最新版（v4.0）での改善点

DIR SOC Quarterly vol.8 2024 summer（2024 年 6 月 17 日発行）

- 経済産業省、企業のサイバーセキュリティ対策を格付けする制度の創設へ
- 特別寄稿　生成 AI の最新動向
- 生成 AI エコシステムを標的とするワーム Morris II



DIR SOC Quarterly vol.9 2024 autumn（2024 年 9 月 20 日発行）

- 「金融分野におけるサイバーセキュリティに関するガイドライン」（案）の公表
- 脅威インテリジェンス
- 国内におけるランサムウェアを巡る情勢と政策動向

DIR SOC Quarterly vol.10 2025 winter
2025 年 1 月 15 日発行
著者　大和総研
執筆者　水谷 浩樹、蓮見 将生、渋谷 篤、田川 晋作、土田 将弘、山崎 禎章、横平 健、松井 直己
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
●RAG（検索拡張生成）	●eKYC	●ブレインマシーンインターフェース（BMI）	●分散型ID（DID）	●パーパス
●生成AI	●ゼロトラスト	●ビジネスアナリシス	●リアルワールドセット（RWA）	●Society 5.0
●ニューラルネットワーク	●パスキー		●ICO	●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