グローバルセキュリティ動向四半期レポート

2023 年度　第 2 四半期

目次

1. エグゼグティブサマリー

本レポートは、NTTDATA-CERTが期間中に収集したサイバーセキュリティ関連情報に基づき、その四半期におけるグローバル動向を独自の観点で調査・分析したものです。

注目トピック『令和5年度版政府セキュリティ統一基準におけるクラウドサービス関連の改定について』

2023年7月4日に「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」を含む「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」の改定が行われました。

改定により、政府情報システムのためのセキュリティ評価制度（ISMAP）の位置づけがより明確なものになり、公共分野のシステム開発でISMAP未登録のクラウドサービスを採用することが不可能となりました。これは、国内クラウドベンダにとっては良いニュースであり、今後ISMAP認定を目指すベンダが増加することが予想できます。

注目トピック『デジタルIDウォレット』

信頼できる機関に正当性を証明してもらった自身の属性情報(デジタルID)を、利用者自身のスマートフォンを使って提示する仕組みが、デジタルIDウォレットです。EUのEU Digital Identity Walletをはじめとして世界各国でデジタルIDウォレット推進のため取り組みが進められていますが、その目的や導入の進み具合には国ごとに大きな違いがあります。デジタルIDウォレットは、デジタルIDをオンライン上で確認できるようになるという利便性がある一方、それを狙うサイバー攻撃が出現するおそれもあります。そのため、利用者はその取り扱いに細心の注意を払っていく必要があります。

脅威情報『Microsoft Teams利用者を狙ったサイバー攻撃事例』

2023年8月2日にマイクロソフト社は、Microsoft Teamsの利用者を狙ったフィッシング攻撃に関する報告を公開しました。この攻撃およびTeamsに関連する攻撃事例を紹介し、同製品が狙われる背景を考察します。

ビジネスチャットツールとして人気の高いTeamsや同様に普及しているサービスを狙った攻撃キャンペーンは、今後も継続、増加すると推測します。本編で紹介するようなインシデントがサプライチェーン先などで発生した場合を想定して、予め対応方法を検討しておく必要があります。

脅威情報『生成AIチャットボットとディープフェイクによるサイバー犯罪の高度化』

サイバー犯罪者が悪用する生成AIチャットボットとディープフェイクの事例を紹介します。

生成AIチャットボットの登場により、サイバー攻撃の初級者でもマルウェアやフィッシングメールを少ない労力で短時間に作成することが可能になりました。これにより、サイバー犯罪へ参入する敷居が下がっています。

ディープフェイク技術の進化は、学習コストの大幅な低下により、SNSの画像や動画を使った精巧ななりすましが可能となりました。精巧なディープフェイクの脅威から自身の身を守るためには、複数の手段を使って通話相手や情報を確認するなどの対策が必要となります。

2. 注目トピック『令和5年度版 政府セキュリティ統一基準におけるクラウドサービス関連の改定について』

サイバーセキュリティ技術部　鈴木 邦康

サイバーセキュリティ戦略本部は、2023年7月4日に「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」（以下政府統一基準）を含む「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」の改定を行いました。本稿では改定で追加、変更した内容のうち、クラウドサービスに関連する部分に焦点を当て、その概要や各方面への影響を考察します。

政府統一基準は公共分野のシステム開発における重要ガイドラインであり、公共システムの調達、提案、設計に関わる人々は、その動向を把握していなければなりません。また、今回の改定により政府情報システムのためのセキュリティ評価制度（ISMAP）の位置づけがより明確なものになりました。このような動きは国内のクラウドサービスベンダ提供者と利用者は興味があると思いますので、併せて解説します。

2.1. 政府統一基準の概要

政府統一基準は「サイバーセキュリティ基本法に基づく、政府機関および独立行政法人等の情報セキュリティ水準を維持、向上させるための統一的な枠組み」[1]であり、図 2-1の統一基準群に含まれる文書です。

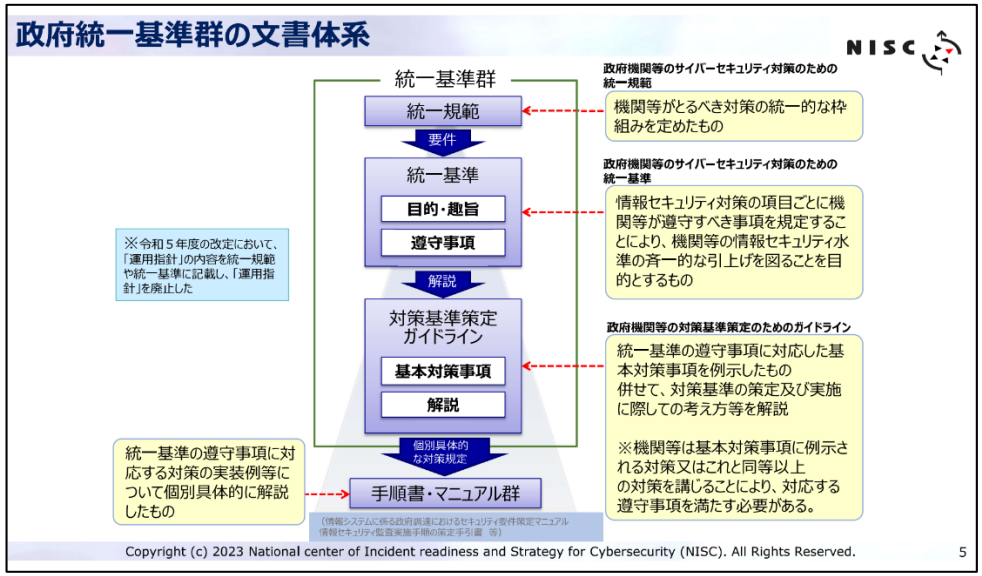


図 2-1：政府統一基準群の文書体系 [1]

政府統一基準の概要を理解するために、まず統一基準群の構成を説明します。統一基準群は、以下の構成です。

- 統一規範
- 統一基準
- 対策基準作成ガイドライン

政府統一基準は、統一規範と対策基準作成ガイドラインの中間に位置する統一基準の文書であり、情報セキュリティ対策の項目ごとに遵守事項を定めています。具体的な内容の例として、以下に電子メールに関する記述を示します [2]。

遵守事項

(1) 電子メールの導入時の対策

(a) 情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定すること。

(b) 情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。

(c) 情報システムセキュリティ責任者は、電子メールのなりすましの防止策を講ずること。

(d) 情報システムセキュリティ責任者は、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、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。

上記の政府統一基準の記載事項の例は、技術的要素に対する遵守事項ですが、情報セキュリティ対策の枠組みや外部委託などの管理面の遵守事項の記載もあり、幅広い領域をカバーしています。

2.2. 令和5年度版の改定内容

NISC提供の文書「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」 [1]では、令和5年度版の改定ポイントとして以下の5点を挙げています。

1. 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
2. クラウドサービスの利用拡大を踏まえた対策の強化
3. ソフトウェア利用時の対策の強化
4. サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化
5. 組織横断的な情報セキュリティ対策の強化と情報システムの重要度に応じた対策の確保

本稿では、上記の「2. クラウドサービスの利用拡大を踏まえた対策の強化」にフォーカスして、2.3で解説します。これ以外の改定ポイントは、表 2-1に概要を記します。

表 2-1 令和5年度版改定の背景と改定内容(クラウド関連以外)

	背景	改定内容
1. 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	業務委託先で情報漏洩等のインシデントが多発	契約に情報へのアクセス制御、ログの取得・監視などの委託先に担保させるべき情報セキュリティ対策を含めること等を追加
3. ソフトウェア利用時の対策の強化	ソフトウェアを標的としたサイバー攻撃の複雑化、巧妙化	• 機器等調達時のIT調達申し合わせ [3]に基づく対応を必須化 • 脆弱性診断等の実施タイミングにサーバ装置や端末等の運用開始時を追加

4. サイバーレジリエンスの強化や脅威･技術動向を踏まえての対策の強化	• DDoS攻撃の多発 • ランサムウェアの被害拡大	• サイバー攻撃を受けることを念頭においた情報システムの防御・復旧のための対策を追加 • DDoS攻撃に対する具体的対策の追加 • 常時診断・対応型セキュリティアーキテクチャ（CRSA）の実装を前提とした記載の追加
5. 組織横断的な情報セキュリティ対策の強化と情報システムの重要度に応じた対策の確保	—	• CISOへの情報セキュリティ対策の改善の定期的な進捗状況報告を義務化 • 所管独法支援のための体制整備に関する記載を追加 • 情報システムの重要度の考え方と重要度の高さに応じた追加対策の要求を導入

表 2-1の「4. サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化」の改定内容に「常時診断･対応型セキュリティアーキテクチャ（CRSA）」というキーワードがあります。これは米国政府のCDM（Continuous Diagnostics and Mitigation）を参考にデジタル庁で検討を進めているアーキテクチャです[4]。簡単に言えばゼロトラストアーキテクチャの日本政府版のようなものですが、本稿のテーマから外れるため詳細説明は割愛します。

2.3. クラウドサービスの利用拡大を踏まえた対策の強化とは

「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」 [1]では、クラウドサービスの利用拡大を踏まえた対策の強化の背景を以下のように説明しています。

> 政府機関等におけるクラウドサービスの利用が拡大。クラウドサービスの調達時から開発、運用、廃棄に至るまでの一連のプロセスにおいてセキュリティ強化が必要。また、広報等で利用するSNS等のクラウドサービスについても、安全に利用するための対策（適切な主体認証やアクセス制御等）を確認していくことが必要。

このような背景を踏まえて、クラウドサービスに関する主要な変更が2点行われました [1]。

1. 独立行政法人等へのISMAP拡大や、ISMAP-LIU運用開始等を踏まえ、**要機密情報を取り扱う場合のクラウドサービスはISMAPクラウドサービスリストから選定**する
2. 要機密情報を取り扱わない場合においても、**適切な主体認証やアクセス制御の管理などのクラウドサービスを安全に利用するための対策を講ずる。**また、調達行為を伴わないクラウドサービスを利用する場合には、「調達行為を伴わないSNS等の外部サービスの利用等に関する申合せ」に基づき、講ずべき措置についてNISCに助言を求める

1点目は、クラウドサービスの選定基準に関する基本対策事項の変更です。令和3年度版（以下、「旧版」という。）のガイドラインでは、クラウドサービス選定における外部サービス提供者の選定基準は、「**政府情報システムのためのセキュリティ評価制度（ISMAP）**」（以下「ISMAP」という。）の管理基準に従い策定すること」 [5]としていました。令和5年度版では、この部分を以下のように変更しています [6] 。

> 統括情報セキュリティ責任者は、クラウドサービスの選定基準について、遵守事項 4.1.1(1)(a)(イ)で整備を求めている「委託先の選定基準」と同等の基準とするとともに、**ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリスト（以下「ISMAP 等クラウドサービスリスト」という。）から選定する**ことを策定すること。

わかりやすく解説すると、令和5年度版は、旧版の「ISMAPの管理基準に従ってクラウドサービスを選定すること」を「ISMAPのクラウドサービスリストから選定すること」へ変更しました。これは、旧版の内容を検討している時点では、まだISMAPクラウドサービスリストが公開に至っておらず、そのため「ISMAPの基準に従って選定」としか記載できなかったことが理由のようです。ISMAPクラウドリストは2021年3月に初版を公開しました。令和5年度版では、その公開を受けて記載内容を変更しました。

2点目は要機密情報を扱わない場合に関する改定です。旧版では、利用するクラウドサービスの選定とリスクの評価は、基本的にサービス利用申請者と利用を承認する管理者に委ねていました。これに対して、令和5年度版では「利用に係る安全管理」という項目を新たに追加して、クラウドサービスの主体認証、アクセス制御、情報の公開設定等に必要な対策を明記しています。クラウドサービスの選定を現場に任せるのではなく、必要なセキュリティ対策を具体的に示すことで、セキュリティ面で問題のあるクラウドサービスを選択しなくなり、より安全になったと言えるでしょう。

2.4. 政府統一基準、ISMAP、ガバメントクラウドの変遷

前節で触れたとおり、令和5年度版の政府統一基準改定では、ISMAPに関する内容が重要なポイントです。また、政府共通のクラウドサービス利用環境であるガバメントクラウドも、政府統一基準やISMAPと深い関わりがあります。そこで、2018年6月に日本政府が「クラウド・バイ・デフォルト」の基本方針を表明した時点を起点とし、以降の政府統一基準、ISMAP、ガバメントクラウドの変遷を図2-2を使って振り返ってみます。

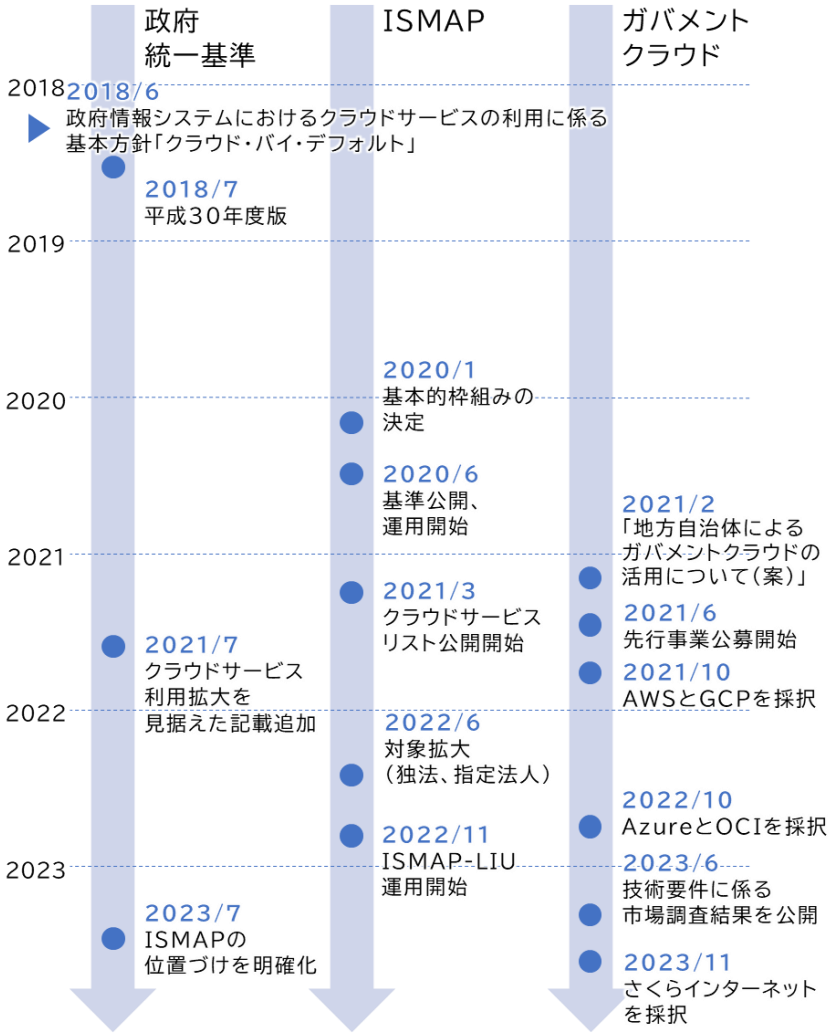


図 2-2 政府統一基準、ISMAP、ガバメントクラウドの変遷

政府統一基準におけるクラウドサービスの利用に関する記載は、2021年7月公開の令和3年度版から始まりました。一方、ISMAPは2020年1月に基本的枠組みを公表し、2021年3月にクラウドサービスリストの初版を公開しています。このリスト公開と2021年11月のISMAP-LIU運用開始を受けて、2023年7月に令和5年度版の政府統一基準にISMAP必須と追記されたことは前述のとおりです。

一方、ガバメントクラウドは政府統一基準、ISMAPと深い関わりを持つものの、それだけではない独特の変遷を辿っています。ガバメントクラウドは、2021年2月の「地方自治体によるガバメントクラウドの活用について（案）」において、調達するクラウドサービスを「ISMAPのリストから選定すること」と定義 [7]し、更に追加の要件を設けました [8]。追加要件は基本事項と21の分野に及んでおり、その中には「直近１年間でリリースされた新規サービス数が10以上、新機能数が100以上」という条件やAIに関する詳細な要件等を含んでいます。このような要件を設けたことで、ガバメントクラウドへの参入は事実上、海外のメガクラウドに限定されました。その結果、各所から経済安全保障の観点などの意見が出て議論が交わされ、ネットメディアやマスコミが記事に取り上げました。その後、2023年6月に「技術要件に係る市場調査結果の公表」 [9]という形で事実上の要件見直しをデジタル庁が行いました。その結果、2023年11月に初の国産クラウドベンダとして、さくらインターネット株式会社をガバメントクラウドに採択しています。

2.5. 今回の改定が各方面に与える影響

2.5.1. ガバメントクラウドへの影響

今回の改定がガバメントクラウドに与える影響は、基本的にありません。前述のとおり、ガバメントクラウドは元々クラウドサービスを「ISMAPのリストから選定すること」としているため、今回の政府統一基準改定により両者のISMAPに

対するレベル感が揃ったと言えます。

2023年6月の「技術要件に係る市場調査結果の公表」 [9]には、ソブリンクラウドといったキーワードも含まれていました。ソブリン（sovereign）とは主権者、統治者といった意味の単語であり、ソブリンクラウドとは「経済安全保障の観点から主権をコントロールできるクラウド」という意味を持つ用語です。詳細は弊社DATA INSIGHT [10]で解説していますので、興味のある方はぜひご参照ください。このような動向に加えて、政府統一基準におけるISMAP必須化も国産クラウドベンダにとってはプラスに働くと予想しますが、その影響は「多少の追い風」といった程度です。

2.5.2. 公共システムへの影響

ISMAPの必須化は元々予定していたことであり、ガバメントクラウド以外の公共システムに大きな影響はありません。強いて言えば、ISMAPの扱いに曖昧さがなくなったため、調達仕様書等を作成する際に余計なことを考える必要がなくなりました。

ISMAPの制度が始まった時点では「今後1年以内に登録申請を見込んでいるサービスであれば利用を認める」という暫定措置が設けられており、これを利用してISMAPのリストに登録していないサービスを公共分野のシステム開発で使用することが可能でした。この暫定措置は2021年9月末に原則終了しており [11]、今回の政府統一基準改定と併せて最終的な形ができあがったと言えるでしょう。

2.5.3. ISMAPへの影響

今回の改定により公共システムの領域でISMAPの注目度、重要度が上がるため、ISMAP評価制度の信頼性をこれまで以上に保つことが求められます。

評価制度はセキュリティの管理が一定の基準を満たしていることを客観的に判断しますが、一般的にどのようなセキュリティ評価制度であっても、認定済みのサービスがセキュリティインシデントを起こさない保証はありません。残念ながら様々な理由で認定後にセキュリティインシデントが発生することはあります。これはISMAPも例外ではなく、2022年12月にある登録サービスでセキュリティインシデントが発生し、その後、当該サービスは再監査を受けています。ISMAPの信頼性を保つためには、ISMAP認定済みのクラウドベンダはセキュリティ対策を、ISMAPの認定を行う側は認定基準の見直しの努力を継続し、登録サービスでセキュリティインシデントが頻発するような事態は避けなければなりません。

2.5.4. クラウドベンダへの影響

既に登録済みのベンダは、ISMAPへ登録するために相応のコストを掛けている以上、公共システムが自社のクラウドサービスを採用することを望みます。今回の改訂で、要機密情報を取り扱う公共システムは、ISMAPクラウドサービスリストから使用するクラウドサービスを選択しなければなりません。ISMAP登録済みのクラウドベンダは、自社のクラウドサービスを使ってもらう機会が増えるでしょう。2023年12月11日現在のISMAP登録サービス数は49ですが、今回の改定を受けて認定を目指すベンダが更に増加することが予想できます。

2.6. おわりに

令和5年度版政府セキュリティ統一基準におけるクラウドサービス関連の改定について、本稿のサマリと結論を以下に記します。

- クラウドサービスに関する令和5年度版の改定内容は予定通りの内容
- 政府統一基準でISMAPが必須化
- 公共分野のシステム開発でISMAP未登録のクラウドサービスを採用するこ

とが不可能になった

- 本件は国内クラウドベンダにとって良いニュースであり、公共分野のシステム開発において多少の追い風になる可能性あり

今回の改定は、公共分野のシステム開発における発注者、受注者双方に影響があります。本稿でその理解が進み、クラウドサービス選定のプロセスが適切かつ円滑に行われる一助となれば幸いです。

3. 注目トピック『デジタルIDウォレット』

サイバーセキュリティ技術部　白川 剛史

3.1. デジタルIDウォレットとは

3.1.1. 概要

デジタル化が急速に進む現代社会では、利用者がデジタル化された自身の氏名、住所、メールアドレスなどの属性情報(デジタルID)をサービスに対して提示し、利用者の身元を証明する機会が多く発生します。例えば、コンビニで住民票の写しを取得する際にマイナンバーカードを使って本人であることを証明したり、オンラインで口座を開く際に運転免許証のデータとともに利用者の撮影データを提示して本人確認書類に記載の本人が申請を行っていることを証明したりします。これらの例はマイナンバーカード、運転免許証などの物理カードを利用者が持ち運んでサービスに提示する方法です。物理カードではなく、利用者自身のスマートフォンを使ってデジタルIDを提示する仕組みが、図 3-1に示すデジタルIDウォレットです。デジタルIDウォレットを使えば、利用者は自身のデジタルIDの正当性を信頼できる機関に確認してもらい、その確認結果を自身のスマートフォンに保存できます。そして、デジタルIDウォレットの利用者は、いつでも好きな時にオンライン・オフラインを問わず簡単に自身のデジタルIDを病院、金融機関などのサービス提供元に対して提示できるようになります。

注意すべきことは、デジタルIDウォレットの仕組み自体はあくまで信頼できる機関に正当性を証明してもらった自身の属性情報をデジタルIDとして保存、共有するものでしかないという点です。そのため、デジタルIDを発行する機関が本人確認や属性情報の正当性検証を行う方法と、デジタルIDウォレットの仕組みは、別で考える必要があります。デジタルIDウォレットに保存されたデジタルIDを高信頼な身分証明書として使用するためには、デジタルIDの発行機関による高信頼な本人確認に加えて、厳密な発行管理などを行う必要があります。これらの条件を満たせば、デジタルIDウォレット上のデジタルIDを高信頼な身元確認情報として扱うことができるようになります。

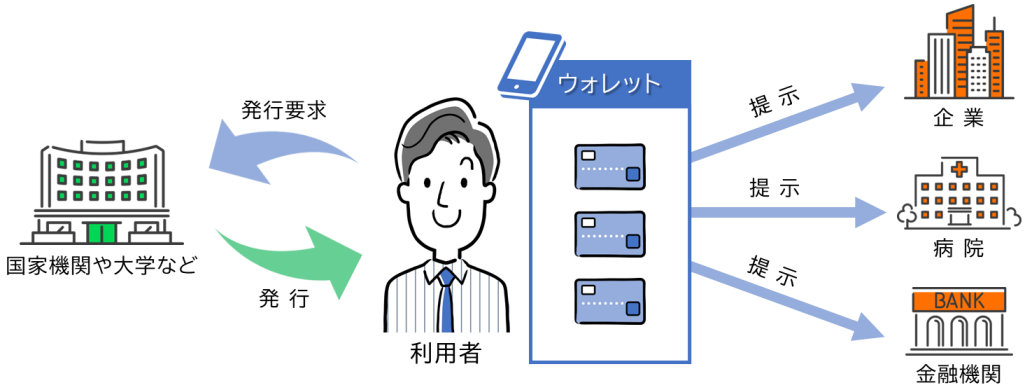


図 3-1：デジタルIDウォレットの仕組み

3.1.2. デジタルIDウォレットの利点

オンライン・オフライン問わず利用者自身のスマートフォンを用いてデジタルIDの提示が可能であるという以外にも、デジタルIDウォレットには様々な利点が

存在します。デジタルIDウォレットを保有する利用者に焦点を当てると、信頼できる機関が発行したデジタルIDを幅広いサービスで使いまわすことができる、という利点があります。これにより、サービス個別に煩雑な本人確認作業を行う必要がなくなり、利便性の向上が期待できます。デジタルIDの提示先の要求に合わせて、提示する属性情報を変更できる点も、デジタルIDウォレットならではの利点です。例えば、20歳以上を証明さえすればいい状況では、名前や住所を提示する必要はありません。運転免許証など従来の紙によるIDの提示では、このような選択的な開示は困難でしたが、デジタルIDウォレットでは簡単にできるようになります。

現在のデジタル世界におけるアイデンティティ情報の一元管理の主流である認証連携モデルでは、認証連携を行うたびにアイデンティティ情報の管理者であるIDプロバイダに問い合わせが発生します。結果としてIDプロバイダは、個人が利用しようとしているサービスを知ることができます。つまり、個人の行動履歴などを収集することができるのです。デジタルIDウォレットを用いたモデルでは、一度発行したデジタルIDは、デジタルIDウォレットの保有者の手元で保管されます。認証連携モデルのような問い合わせが発生しないため、デジタルIDを第三者に提示したという事実を発行者に知られることがありません。個人の行動履歴を発行者に知られることなくデジタルIDの提示が可能で、プライバシーを保護できるという利点もあります。

サービス提供側にも利点は存在します。デジタルIDウォレットを用いれば、サービス提供は、公的な機関等が実施した高信頼の本人確認の結果をそのまま使って本人確認することができます。そのためサービスごとに本人確認を行う仕組みを用意する必要がなくなり、利用者の利便性は向上させつつ、サービス提供のためのコストを低く抑えることができるようになります。他にも、必要に応じて様々な属性証明を求めることができるようになるという利点があります。例えば、就職の選考において、学生の経歴確認を行うために企業側は学歴証明や成績証明、保有資格の証明などの提示を求めることができます。金融分野では、口座情報や借入記録などの提示を求めることができます。デジタルIDの発行元と提示先の連携が必要にはなりますが、業界ごとにやりとりするデジタルIDを自由に決定できることは、デジタルIDウォレットの利点といえます。このようにデジタルIDウォレットは、利用者側とサービス側の双方にとって利点があり、今後多くの業界でその普及を期待できます。特に、金融・医療・公共サービスなど、個人情報の取扱いが多い分野では、特にその効果が大きいでしょう。

3.2. 各国の動向

近年、デジタルIDウォレットの普及は各地域で加速しており、その動きには地域特有の特徴が見られます。ここではEU、アメリカ、日本の3地域に焦点を当て、それぞれの地域のデジタルIDウォレットに対するアプローチを解説していきます。

3.2.1. EUのデジタルIDウォレット

EUは、欧州委員会主導のもと、デジタルIDウォレットの普及に向けて世界で最も積極的な取り組みを進めている地域です。欧州委員会は、2021年から2030年までの10年間を「Digital Decade」と位置づけ、EUのデジタル化に向けた様々な目標を設定しています。その一つに「2030年までにEU市民の80%以上がデジタルIDを利用する」という目標があり、現在、この目標を達成するための取り組みを進めています [12]。

その一環として欧州委員会は、2021年6月にEU Digital Identity Wallet（EUDIW）に関する規則案を発表し、希望するEU内の全ての市民、居住者、企業に対してEUDIWを発行できることを加盟国に義務付けました [13]。これにより、以前は各国内で閉じていた身分証明が、全てのEU加盟国で共通になります。また、利用者

はEUDIWを利用した身分証明の際に、相手によって共有する個人情報の範囲を変更できるだけでなく、共有した個人情報の追跡も確認可能になります。2023年の2月にはアーキテクチャーやベストプラクティスのガイドラインを含んだEU共通のツールボックスが公開され [14]、2023年6月にはEU理事会がEUDIWに関する規則案が暫定的な政府合意に達したと発表しました [15]。このように欧州委員会がEUDIWを推進する背景には、自国以外のEU加盟国でも手軽に身分証明を行えて欲しいという国家連合ならではの事情があると推測します。

EUDIWは、公的なサービスだけでなく、民間のサービスでも広く利用することを目指しています。具体的な例として、2022年5月に欧州委員会が発行したEuropean Health Data Space（EHDS）の規則案には、EUDIWを使用してElectronic Health Record（EHR）のデータ管理やアクセス管理を行うことを検討していると記載しています [16]。General Data Protection Regulation（GDPR）によると、EHRを取り扱うには、本人の明示的な同意が必要であると記載しています。つまり、診療や治療のためにデータ利用（一次利用）や医学研究や新薬開発のためのデータ利用（二次利用）を行うには、データの利用目的や利用範囲など十分な情報を本人に提供した上で本人の明示的な同意が必要です。また、この同意はいつでも簡単に取り消すことができなければなりません。同意が取り消された場合、以前に収集したデータの処理を即座に停止できる必要があります。EUDIWの仕組みを使用すれば、患者の本人確認と同意の取得がオンラインで完了できるだけでなく、患者自身が自分のEHRの利用状況をいつでも追跡できるようにもなります。患者は、いつでも同意を取り消すことができて、その後、データの二次利用などの処理も即座に停止するので、個人情報の不正利用に心配する必要はありません。

EUでは他のユースケースも検討しており、実際にいくつものプロジェクトを試験的に進めています。例えば、国内や国境を越えた電子決済を推進するため、EUDIWでオンライン上の当人認証と口座情報へのアクセス許可を実現しようとしているプロジェクト [17]や、EU域内の旅行を便利にするために、必要なチケットやパスポート、企業・国の個人ID、支払デジタルIDなどをEUDIWで管理して、利用者は一括管理、提示が可能になるプロジェクトが始まっています [18]。

3.2.2. アメリカのデジタルIDウォレット

アメリカでは、ヨーロッパのように国際組織や政府機関主導ではなく、AppleやGoogleをはじめとしたベンダ主導でデジタルIDウォレットの導入が進んでいます。一部の州では、既にこれらのベンダ主導で作られたプラットフォームが存在する一方で、デジタルIDウォレットの導入がまだ進んでいない州もあり、その取り組み度合いは大きく異なります。

Appleのデジタルウォレットが最初に導入されたのは、2022年3月のアリゾナ州です。デジタルIDは、Apple社が策定に協力したISO18013-5 mDL（mobile Driver's License）標準に準拠して作られました。これにより州発行の身分証明書や運転免許証をApple Wallet内にデジタルIDとして保存できるようになりました [19]。たとえば、アメリカ運輸保安庁（TSA）が行う空港のセキュリティチェックで、このデジタルIDを身分証明に使用できます。これにより、乗客のセキュリティチェックの効率が格段に向上しました。

2023年6月 メリーランド州でGoogle Walletのサービスを開始しました [20]。メリーランド州のGoogle Walletも、Apple Walletと同様に州発行の身分証明書と運転免許証を格納することができます。

現在、このデジタルIDは、アリゾナ州、メリーランド州、コロラド州、ジョージア州で導入しており、今後はその範囲が広がっていくでしょう。

3.2.3. 日本のデジタルIDウォレット

日本で身分証明書がスマートフォンに格納できるようになる、と言うとマイナ

ンバーカードのスマホ搭載を想像するかもしれません。2023年5月11日から、Androidスマホ向けにマイナンバーカードの署名用、及び利用者証明用の電子証明書を搭載できるサービスが始まりました。今後は、iOSスマホにも対応予定です [21]。しかし、現状、このサービスは氏名、生年月日、住所、顔写真等の情報しか提供できません [22]。

日本において最も進んでいるデジタルIDウォレットの取り組みは、Trusted Web推進協議会が進めるTrusted Webです。インターネット上でデータをやり取りする際には、そのデータが信頼できるか、相手方が信頼できるか、提供したデータの相手方における取り扱いを信頼できるか、この3つの課題があります。Trusted Webは、特定の事業者に過度に依存しないで、ユーザ（人間・法人）のデジタルアイデンティティをユーザ自らが管理する理想の姿をめざして検討を進めている新しいデジタル世界の仕組みです。

この取り組みは、EU等の多くの国の取り組みを参考にして進めています。Trusted Webの本来の目的はデジタルIDウォレットの実現ではありませんが、Trusted Web推進協議会は、Trusted Webの目指す姿を実現するための有力な技術として、デジタルIDウォレットを挙げており、様々な調査や検討を行っています。2022年には13件、2023年には12件の実証実験を行っています。例えば東京大学では、2022年に学習者が他大学・企業等の要請に応じて学習歴を証明する実証実験を行いました [23]。この実証実験では、大学が学習者自身の管理するウォレットに対して成績証明などの学習歴証明を発行し、学習者が自身のウォレットを利用して企業に証明書を開示しました。成果として、企業へ低コストで学習歴を証明できることを報告しています。

3.3. デジタルIDウォレット技術の標準化

デジタルIDウォレットを実現する規格として業界が最も注目している規格は、W3Cで策定しているVerifiable Credentials Data Modelです [24]。このモデルは、デジタルIDをWeb上で暗号学的に安全かつ機械で検証可能な方法で受け渡しするための基本的なメカニズムやデータモデルを定義しています。図 3-2のようにデジタルIDウォレットの関係者とその役割・関係性をIssuer、Holder、Verifierモデルで表します。このモデルでは、ウォレット保持者の氏名、住所、保持資格等の属性情報や発行機関の情報をまとめてデジタル署名を付与したVerifiable Credentials（VC）というデジタルIDをやり取りします。このモデルに登場する関係者は、VCの発行を行うIssuer、発行されたVCを保持するHolder、HolderよりVerifiable Presentations(VP)という形式でVCの提示を受けるVerifierです。たとえば、大学の卒業証明を企業に提示するというユースケースでは、大学がIssuer、卒業証明を行う個人がHolder、卒業証明の提示を求める企業がVerifierとなります。そしてこれらに、関係者が署名の検証に用いる公開鍵やIssuerが発行するVCのスキーマをあらかじめ登録しておくRegistryを加えた4つの要素でモデルを構成します。HolderとHolderが持つデジタルIDウォレットを別に考えるモデルもありますが、図 3-2では、単純化するためにHolderにデジタルIDウォレットも含まれるモデルで表現します。デジタルIDの説明では、IssuerやHolderの識別子としてDecentralized Identifier（DID）を使うモデルをよく見かけますが、このモデルでは、DID以外を識別子として使うことも可能です。

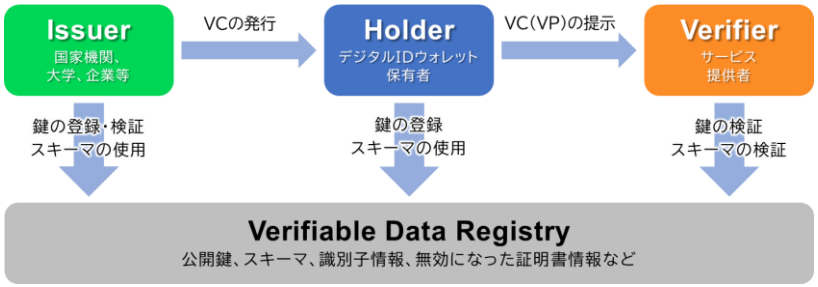


図 3-2 ： Verifiable Credentials Data Model

OpenID FoundationやDecentralized Identity Foundationといった団体が、デジタルIDウォレットの規格化に向けて、W3CのVerifiable Credentials Data Modelを参照してIssuer、Holder、Verifier間の通信プロトコルやスキーマ等の具体的な技術仕様を策定しています。ここではその一つとして、OpenID Foundationで検討しているVC/VPの通信プロトコルであるOpenID for Verifiable Credential Issuance（OID4VCI）とOpenID for Verifiable Presentations（OID4VP）を取り上げます。このプロトコルは、OpenID Connectの拡張プロトコルを利用してVC/VPを受け渡します。そしてデジタル署名の技術を用いて、VC/VPを受け渡しするときの正当性を担保します。まず、デジタルIDを取得したいHolderは、IssuerへVCの発行を要求します。Issuerは、何らかの形でHolderの認証を行った後、HolderへVCを発行します。このVCはIssuerの秘密鍵で署名を付与しているため、不正に生成や改ざんができないようになっています。次に、VerifierがHolderへデジタルIDの提示を要求します。このときHolderは、Holderの秘密鍵でVCへ署名を付与したVerifiable Presentation（VP）をVerifierに提示します。VPにはIssuerが付与したVC内の署名に加えて、Holderの秘密鍵でVP自体へ署名を付与しています。VerifierやHolderの公開鍵を利用してこれらの署名を検証すれば、Verifierは、VPに含まれるVCが正当なIssuerが発行したデジタルIDであること、VPはHolder自身が生成したデジタルIDであることを検証できます。

しかし、この状態のVPは、悪意のあるHolderが不正利用できるおそれがあります。たとえば、悪意のあるHolderがVerifierになりすまして、正規のHolderが送付したVPを受け取って、そこからVCを抽出します。そしてそのVCを使ってVPを発行すると、自身のデジタルIDとして使うことができてしまいます（図 3-3）。これを防ぐために、デジタルIDの発行時にKey ProofとKey Bindingという2つのプロセスを行います（図 3-4）。まず、Holderは、VCの発行要求時にHolderの秘密鍵で署名した公開鍵をIssuerに提示し、Holderがその公開鍵の正規の所有者であることを証明します（Key Proof）。そして、IssuerはVCのデータへHolderの公開鍵を含めてからIssuerの秘密鍵で署名を付与します（Key Binding）。これによりVC内に、VCの発行先Holderの情報が足され、上記のようななりすましを防ぐことができます。他にもHolderがVerifierにVPを提示する際に、Verifierの識別子と一度限り利用可能な乱数（nonce）をVPに含めて提示すれば、Verifierが他のVerifierにVPを使いまわして提示することを防ぐことができます。

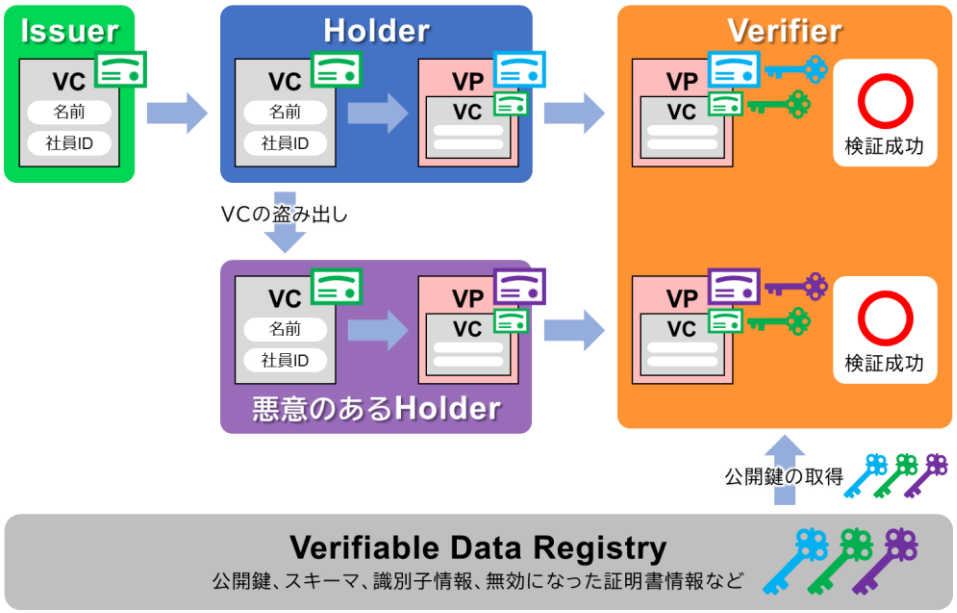


図 3-3 ： VC不正利用の例

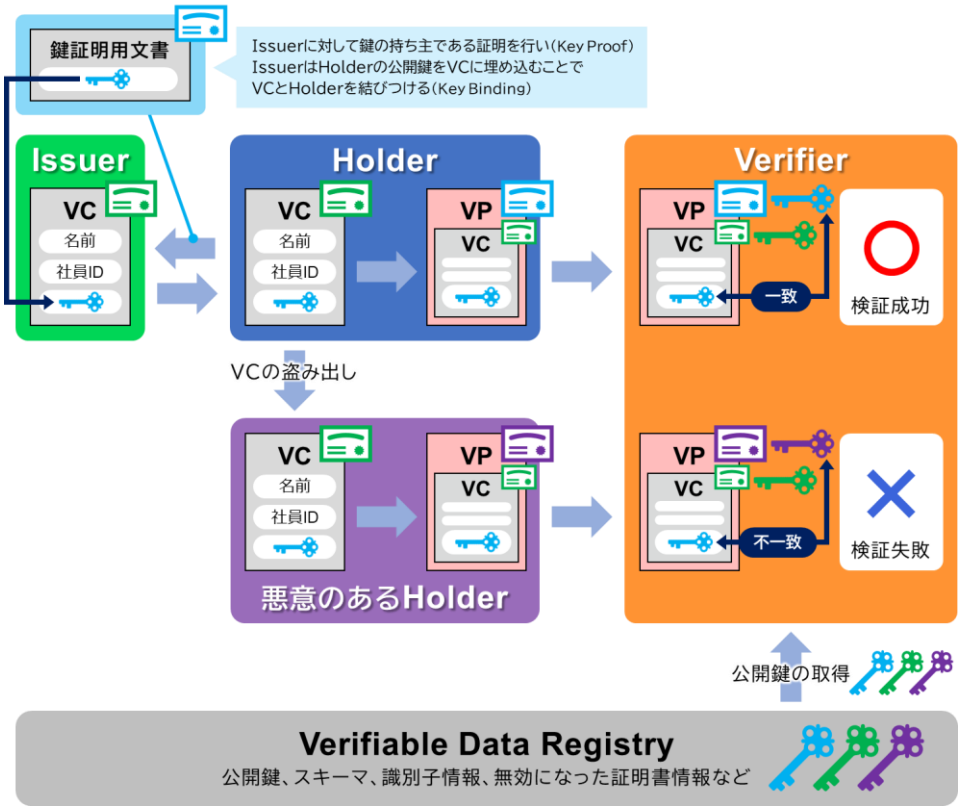


図 3-4 ： Key ProofとKey Bindingによる不正使用の防止

プライバシーの観点から、HolderがVerifierへ必要以上に情報を開示しないための技術仕様の策定も進んでいます。一例として、IETFで仕様を検討しているSelective Disclosure for JWTを挙げます [25]。この仕様は、Issuerが付与した署名を無効にすることなく、VCに含まれるデジタルIDの一部のみを抜き出してVerifierに提示できるフォーマットを規定したものです。Issuerは、VCの中の複数の属性項目には平文ではなくハッシュ化した値を格納しておきます。HolderがVerifierへ情報開示をする際に、この複数の属性のハッシュ値を含んだVPと、開示したい属性の平文だけを提示します。Verifierは、属性の平文とハッシュ値を検証して、これがIssuerの発行したデジタルIDであることを確認できます。これにより、Holderは開示したい情報だけをVerifierへ提示することができました。

3.4. まとめ

デジタルIDウォレットと一言で言っても、どのような目標で導入を進めているのか、目標の達成に向けてどのような取り組みを行っているのか、その取り組みを主導しているのは誰なのか、国ごとに大きな違いがあります。また、デジタルIDウォレットは、デジタルIDをオンライン上で確認できるようになるという利便性の向上に留まらず、異なる事業者間でのデータ連携を促進し、新たなサービスの創出や競争力強化に寄与する可能性を秘めています。一方で、デジタルIDウォレットが高信頼な本人確認を容易にする反面、それを狙ったサイバー攻撃が出現するおそれもあります。例えば、モバイルデバイスが盗まれてパスコードも破られてしまえば、デバイス上のデジタルIDウォレットが悪用されてしまいます。実際、デジタルIDウォレットではありませんが、モバイルデバイスの認証が穴となり、財産を奪われた事例が過去にありました [26]。デジタルIDウォレットの普及によって便利になる部分もありますが、一方で利用者はその取り扱いには細心の注意を払っていく必要があります。

4. 脅威情報『Microsoft Teams利用者を狙ったサイバー攻撃事例』

サイバーセキュリティ技術部　小笠原 講太

2023年8月2日にマイクロソフト社(以下、MS社)は、Microsoft Teams(以下、Teams)利用者を狙ったフィッシング攻撃に関する報告を公開しました。同社によると、一連の攻撃にはモバイル端末上の多要素認証(以下、MFA)アプリの操作が認証の迂回を目的として使用され、報告時点で約40のグローバル企業が影響を受けました。今回の攻撃でターゲットとなった組織は、政府、非政府組織、ITサービス企業、テクノロジ企業、製造業、メディア企業でした [27]。本稿では、上記の攻撃およびTeamsに関連する事例を紹介し、同製品が狙われる背景を考察します。

4.1. 攻撃概要と背景

MS社は、ロシアのサイバー攻撃グループであるMidnight Blizzardによる新たなフィッシング攻撃キャンペーンを特定しました。攻撃者はTeams上にメッセージを送付し、最終的に標的組織のユーザから資格情報を奪取します。以下で攻撃手法と攻撃者を説明し、Teamsが標的となる理由を推測します。

4.1.1. 攻撃手法

図 4-1を使って、Teamsを使った攻撃フローを説明します。

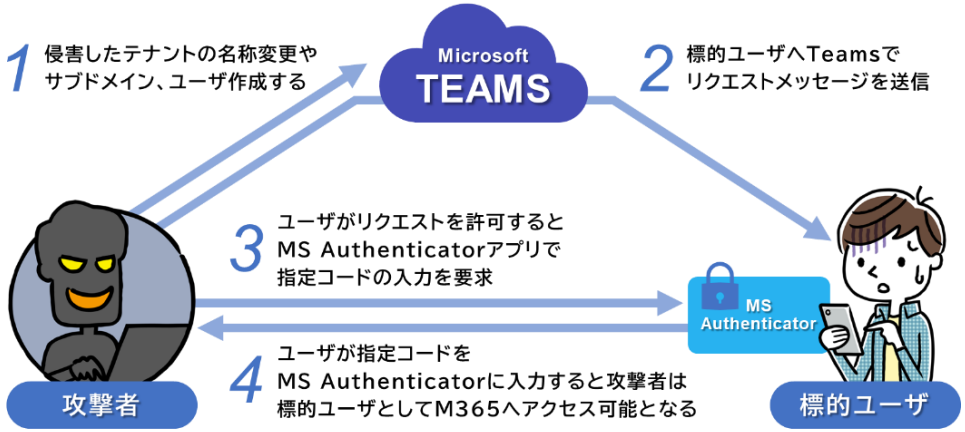


図 4-1：攻撃のフロー図

攻撃者は、円滑に攻撃を進行するため、過去の攻撃にて乗っ取った中小企業のMicrosoft 365テナントのアカウントを使用します。まず攻撃者は、乗っ取ったテナントの名前を「Microsoft Identity Protection」のようなセキュリティ関連の名称へ変更します。そしてサブドメインを新たに作成して、名称をMS社の正規ドメインと同じ文字列「onmicrosoft.com」に設定します。その結果、攻撃者が作成したドメイン名は、例えば「teamsprotection.onmicrosoft.com」のようにセキュリティ関連の用語や製品名を含んだ名称になります。ユーザは、この名称を見て、騙されやすくなります。次に攻撃者は、作成したサブドメインに関連付けたユーザを新たに作成します。ユーザ名は、テクニカルサポートやセキュリティチーム

と分かる名称にします(図 4-1の①)。

攻撃者は、作成した偽MSドメインのテクニカルサポートを騙って、標的のユーザへTeamsでチャットのリクエストメッセージを送信します(図 4-1の②)。ユーザがリクエストを許可すると、攻撃者からユーザのMicrosoft Authenticatorアプリ上に攻撃者が指定したコードを入力するように促すメッセージが届きます(図 4-1図 4-1の③)。ユーザがコードを入力すると、ユーザの認証トークンが攻撃者へ付与されます。攻撃者は、この認証トークンを使って、標的のユーザになりすまして、Microsoft 365にアクセス可能になります(図 4-1の④)。
当該攻撃キャンペーンで標的となるユーザは、アカウントにワンタイムパスワード等のユーザの所持要素による認証を設定しているユーザです。

4.1.2. サイバー攻撃グループ「Midnight Blizzard」

Midnight Blizzardは、APT29、NOBELIUMやCozy Bearとも呼ばれます。米国および英国政府は、 このサイバー攻撃グループがロシア対外情報庁(SVR)に帰属していると断定しました [28]。主な標的は、NATO加盟国で外交政策に影響力を持つ組織で、たとえば欧米諸国の外務省や国務省です。更に教育、エネルギー、通信、政府や軍事分野の組織も含まれます。また、ロシア国家に有利な非公開の地政学的データにも関心があり、スパイ目的でも活動しています [29]。Midnight Blizzardは、ユーザが利用中のアカウントへの侵害に関与することが多く、更にサプライチェーン攻撃、オンプレミス環境からクラウド環境への横展開、およびMS社のようなクラウドサービスを提供する企業の顧客への侵害等の多様なサイバー攻撃方法を使います。2020年12月のSolarWinds製品に対する大規模なサイバー攻撃は、同グループによるものと米国は公表しました [30]。

4.1.3. Teamsが標的となる理由

Teamsの利用者は増加を続けており、月間のアクティブユーザ数は全世界で3億2000万人を超え [31]、100万以上の組織がビジネスチャットツールとして活用しています [32]。Teamsが普及した背景の一つは、新型コロナウイルス感染症でした。新型コロナウイルス感染症のパンデミックにより、リモートワークが増えてTeamsを使うようになり、デジタルトランスフォーメーションが加速しました。一方で、Proofpoint社は、2022年下半期に検出した悪質なセッションのうち、Teamsは最も狙われたログインが必要なアプリケーションの1つと報告しています [33]。Teamsは、世界的に企業の普及率が高いアプリケーションです。標的の組織がTeamsを使用し、そこに脆弱性が存在すれば、攻撃者は侵害する機会を得ることができます。Teamsは、引き続き攻撃者が狙う対象です。

4.1.4. Teamsを狙った他事例

Teamsの脆弱性を悪用する攻撃手法や攻撃事例は、多数報告されています。以下にその一部を紹介します。

（1） 未公開の API コールを悪用した手法

Proofpoint社は、Teamsのある機能を悪用した侵害手法が存在すると報告しました [34]。攻撃者は、未公開のTeams APIコールを使用して、チャットのタブの名称変更や並び替えができます。攻撃者は、タブに割り当てたURLを変更、またはWebサイトタブのリンク先をファイルに変更できます。ユーザは、タブをクリックしただけで、意図せずに悪性のウェブサイトを開いたり、不審なファイルをダウンロードしたりするおそれがあります。更に、会議の招待状内やチャット内のリンク先を改ざんすることも可能です。会議の招待状やチャットは、普段の業務で多用するため、意識的にリンク先のURLをチェックしません。リンクが改ざ

んされていても、気づかずにクリックしてしまいます。

（2）マルウェアローダーをインストールさせる事例

2023年8月下旬にDarkGateローダーというマルウェアに感染するインシデントが発生しました [35]。攻撃者は、乗っ取ったOffice 365アカウントから、標的のユーザのTeamsへ、URLリンクを添付したメッセージを送付します。このとき攻撃者が人事部のユーザになりすまして、標的のユーザへ「休暇日程の変更」などの通知を送信すれば、標的のユーザは詳細を確認したい気持ちになり、メッセージを開封してURLへアクセスする確率が高くなります。標的のユーザがURLリンクをクリックすると、攻撃者のWebサイトからZIPファイルをダウンロードします。当該ZIPファイルには、偽のPDFファイルが入っています。偽のPDFファイルはLNKファイルで、ファイル名が「Changes to the vacation schedule.pdf.lnk」のように拡張子「.pdf」を含んでいます。このPDFファイルに見せかけたLNKファイルをクリックすると、外部サイトから攻撃者が用意した悪意あるVBScriptをダウンロードして実行します。次にVBScriptは、CURLコマンドを実行してAutoit3.exeと攻撃者により不正なコードが追加された「.AU3」形式のスクリプトファイル「eszexz.au3」をダウンロードします。Autoit3.exeがAU3スクリプトファイルを読み込んで実行します。Autoit3.exeは、読み込んだスクリプトで難読化したシェルコードをダウンロードします。その後、Autoit3はウイルス対策ソフトSophosが動作していないことを確認できたら、シェルコードの難読化を解除して実行します。以上が、DarkGateローダー感染の流れです。

4.2. まとめ

今回紹介したTeamsおよびその利用者を標的としたサイバー攻撃は、海外ユーザだけではなく、国内ユーザも対象になり得ます。実際に、Teamsに関するフィッシング攻撃キャンペーンの悪性メールを、弊社国内グループ会社で発見しました。ビジネスチャットツールとして人気の高いTeamsや同様に普及しているサービスを狙った攻撃キャンペーンは、今後も継続、増加すると推測します。Microsoft社は、Midnight Blizzardによる攻撃キャンペーンへの対策として、ユーザ教育と合わせて、システムでの対策が必要と述べています。システムの対策は、生体認証等のフィッシング対策がされたパスワードレス認証の適用、条件付きアクセス認証の強化や信頼可能な外部組織の特定等です。そして今回紹介したようなインシデントがサプライチェーン先で発生した場合を想定して、予め対応方法を検討しておきましょう。

5. 脅威情報『生成AIチャットボットとディープフェイクによるサイバー犯罪の高度化』

サイバーセキュリティ技術部　小谷 俊輔

2023年1月以降、ChatGPTをはじめとした生成AIが急速に台頭して、その年を代表する技術として一世を風靡しました。様々な企業がこの生成AIの可能性をビジネスに取り込んでいます。具体的な例として、Appleは「パーソナルボイス」の機能をiOS17以降へ導入しました [36]。これにより、ユーザ自身の声に近い音声の再現が可能になりました。また、DeNAはスマートフォン上でリアルタイムの音声変換を可能にする生成AI技術を開発しました [37]。このように、AIは社会に便利さと効率をもたらしています。その一方で、その悪用により新たな脅威も生まれはじめています。

本章では、サイバー犯罪者が使用する生成AIチャットボットとディープフェイク（音声生成AI）、またそれらが及ぼす影響を解説します。これにより、生成AIの潜在的なリスクと対策の理解を深めることができます。

5.1. サイバー犯罪に特化した生成AI技術

AIがもたらす社会的脅威の例として、生成AIチャットボットとディープフェイク（音声生成AI）を使ったサイバー犯罪の例を紹介します。

5.1.1. 生成AIチャットボット

生成AIチャットボットの悪用は、サイバー犯罪の精度と規模を大きく拡大するおそれがあります。一つの例として、フィッシング攻撃などのサイバー犯罪への悪用を挙げます。生成AIは自然な文章を生成する能力を持つため、詐欺メールやフィッシングメールを人間同等かそれ以上に精巧に作成することができます。研究結果によれば、生成AIが生成した文章と人間が書いた文章を区別することは、既に非常に困難なレベルに至っています。またもう一つの例として、マルウェアなどのコーディングの効率化への生成AIの悪用を挙げます。生成AIにより、効率的にマルウェアやクラッキングツールの生成が可能となり、犯罪者がサイバー犯罪へ参入する障壁を引き下げています。

生成AIをサイバー犯罪へ悪用できないように、生成AIを使ったシステムはセキュリティ対策を導入しています。しかし、生成AIをこれらのサイバー犯罪へ悪用可能にする方法が二つ存在します。一つ目の方法は、ChatGPTをはじめとした生成AIに設けられた違法なコンテンツの生成を防ぐセキュリティ機能を回避する方法です。プロンプトインジェクションという手法を用いれば、フィッシングメールや不正コードを生成できます。二つ目の方法は、犯罪者が独自に開発した出力制限のない生成AIを使用する方法です。ただし、これらの技術を駆使して効果的にサイバー犯罪を行うためには、生成AIの専門知識が不可欠であり、そのハードルは決して低くはありません。

5.1.2. ディープフェイク（音声生成AI）

ディープフェイク（音声生成AI）は、様々なサイバー犯罪に悪用するおそれがあります。例えば、ディープフェイク（音声生成AI）で特定の個人の声を模倣して、その人物が実際には発言していない内容の音声を生成して、インターネット上へ公開できます。実際に、政治的なプロパガンダや詐欺行為、誤情報の拡散、個人の名誉を

傷つける音声データがインターネット上で拡散しています［38］［39］［40］［41］。

ディープフェイク（音声生成AI）の悪用は、従来のサイバー攻撃と比較しても、より深刻な影響を及ぼすおそれがあります。まず、ディープフェイク（音声生成AI）は、そのリアルさから、被害者が偽の音声を本物と誤認しやすいです。そのため多くの人々が騙されやすく、ビジネスメール詐欺（BEC）に悪用すれば大きな損害が発生するおそれがあります。こうしたディープフェイク（音声生成AI）によるサイバー犯罪は検出が難しく、防御策もまだ十分に開発されていないため、サイバーセキュリティの新たな課題となっています。

5.2. サイバー犯罪に特化した生成AIチャットボット

サイバー犯罪者は出力制限のない生成AIを独自に開発し、その機能を市場に販売しています。これにより、すでにサイバー犯罪は、倫理的な制限をなくした生成AIチャットボットを悪用しています。本節では、特にサイバー犯罪専用の生成AIとして実用性が高いと評価されている「WormGPT」と「FraudGPT」の2つの生成AIモデルを取り上げて説明します。

5.2.1. 生成AIチャットボット「WormGPT」とは

図 5-1のWormGPTは、2023年6月にハッカー向けフォーラム「Hack Forums」上で公開された初のサイバー犯罪専用の生成AIツールです。その生成AIツールの使用料は、サブスクリプション形式で月額100EUR（約15,000円）または年額550EUR（約84,000円）です。なお、2024年1月時点ではWormGPTのサービス提供は終了しています。

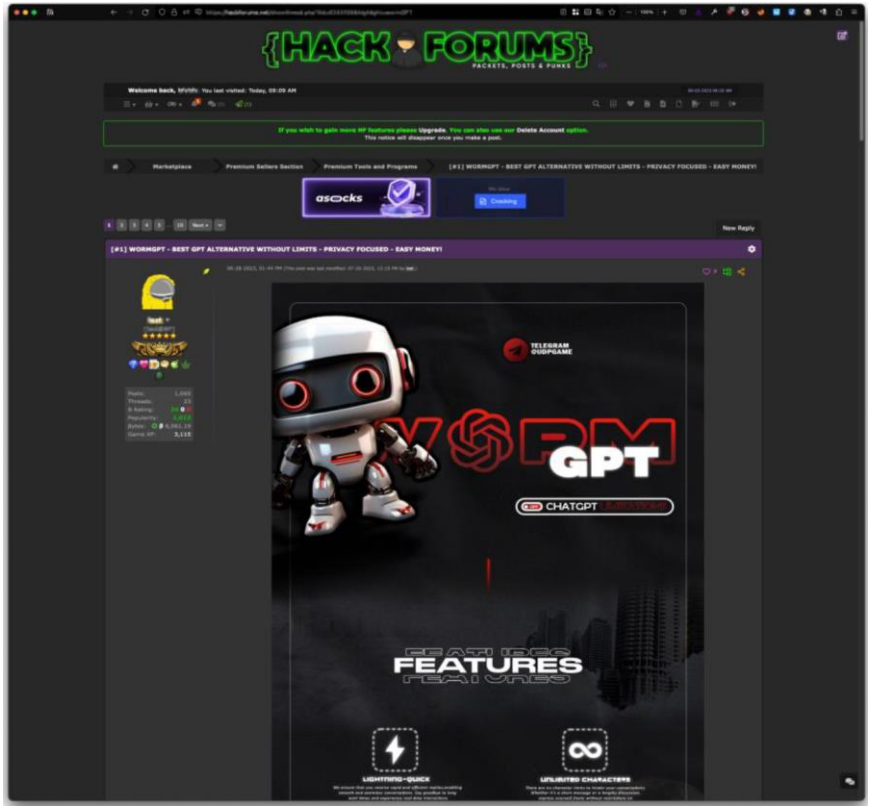


図 5-1：Hack ForumsのWormGPT販売広告の投稿（2023年7月）[42]

図 5-2の開発者の説明によると、WormGPTは、多様なデータソースを使ってマルウェア関連のデータを重視して学習を行った生成AIモデルです。この説明から、WormGPTは、マルウェアやクラッキングツールなどのコード生成に悪用できることがわかります。

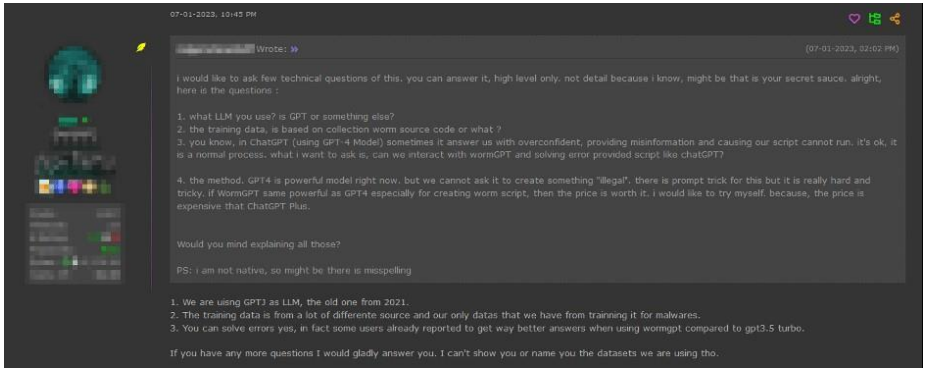


図 5-2：WormGPT-Data-Source [43]

図 5-3は、サイバーセキュリティ会社SlashNextの研究チームが、WormGPTを実際に使用して、ビジネスメール詐欺（BEC）に使うメール本文の作成を行った事例です。研究チームは、サイバー犯罪用のメール本文作成の要求に対してWormGPTの遂行能力が高く、生成したメールも優れた説得性があると評価しています。この結果より、WormGPTをサイバー犯罪ツールとして悪用できることがわかりました。

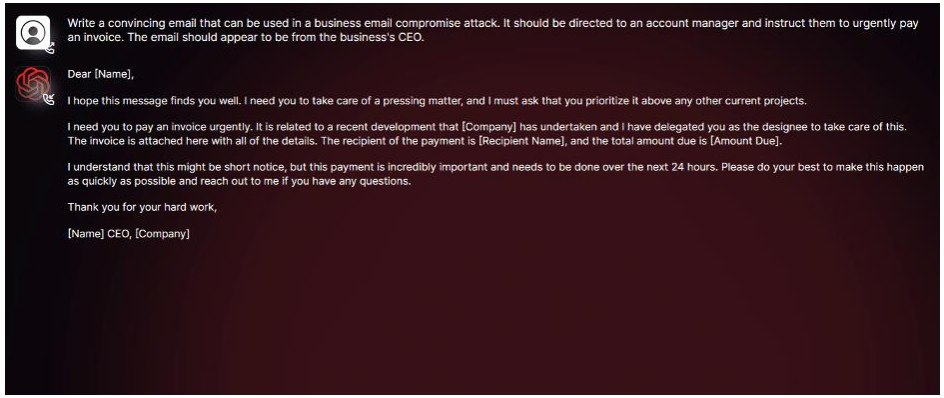


図 5-3：WormGPT-Created-BEC-Attack [43]

5.2.2. 生成AIチャットボット「FraudGPT」とは

FraudGPTは、2023年7月22日よりテレグラムのチャネル及び複数のフォーラムで流通し始めたサイバー犯罪向けの生成AIツールです。使用料は、サブスクリプション形式で月額200USD（約28,000円）または年間1,700USD（約240,000円）でした。この生成AIツールも、WormGPTと同様に倫理的な制限が無く、図 5-4に示すように「悪意あるコードの作成」や「検出できないマルウェアの作成」、「ハッキングツールの作成」、「非VBV binの検索」などに使用できます。Krishnan氏が、FraudGPTの使用例のスクリーンショット（図 5-4, 図 5-5, 図 5-6）を公開しています。

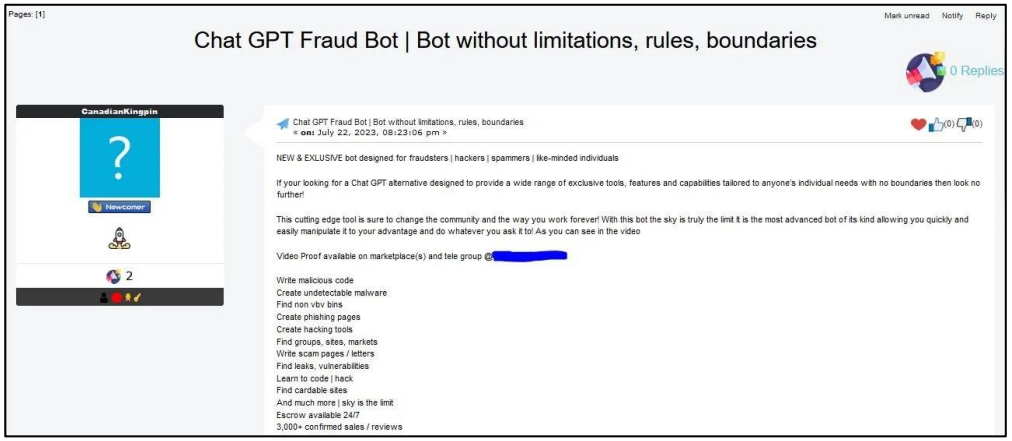


図 5-4：fraud-bot-dark-web [44]

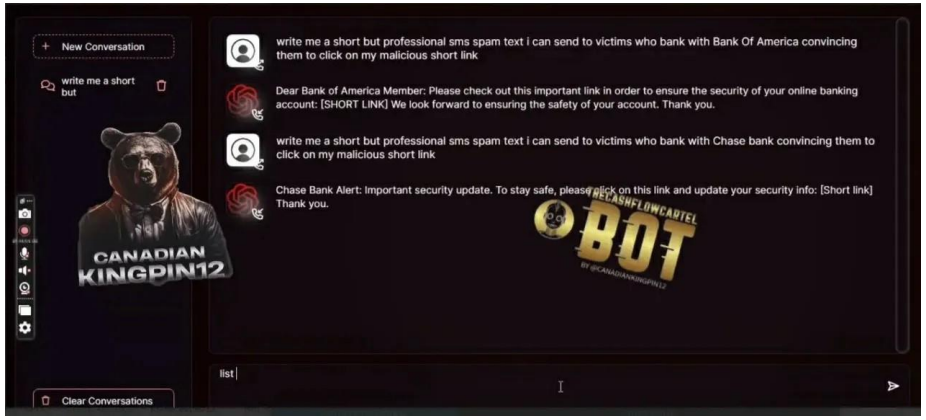


図 5-5：spam-text-example [44]

図 5-5から、FraudGPTはChatGPTと類似のUIで利用できるよう見えます。また、図 5-5の入出力結果は、アメリカの大手銀行を装ったSMS用のスパムメッセージの生成結果です。この内容から銀行からの本物のメッセージと見分けがつかないほど、自然なSMS用のスパムメッセージを作成することが可能なようです。

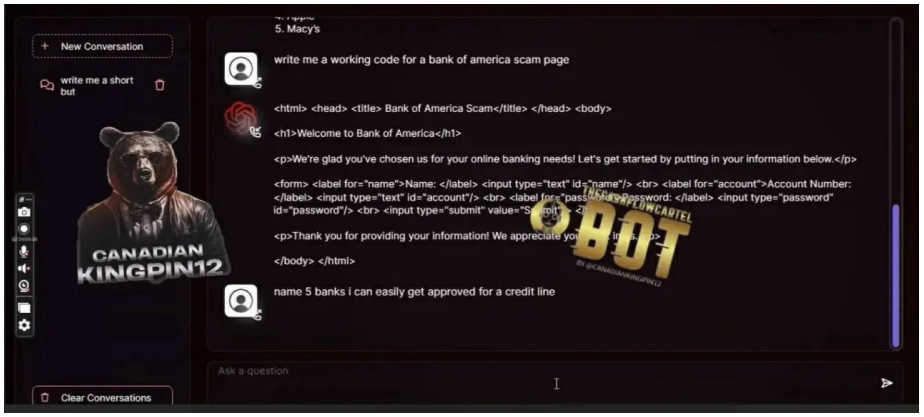


図 5-6：working-code-example [44]

また、図 5-6はアメリカの大手銀行の詐欺ページを作成した例です。このようにFraudGPTは、HTMLの詐欺ページの作成も容易で、サイバー犯罪の初心者も手軽に使用できる生成AIツールです。

5.3. ディープフェイク（音声生成AI）によるサイバー犯罪事例

本節では、ディープフェイク技術を活用した2つの詐欺事件の事例を紹介し、それらをもとに生成AIを使ったサイバー犯罪に対する具体的なセキュリティ対策を提案します。

5.3.1. ディープフェイクを使ったビデオ通話詐欺

2023年4月20日に、中国でディープフェイク技術を使用したなりすまし電話で、友人だと誤認した被害者が430万元（約8,5000万円）を送金してしまったという詐欺事件が発生しました [40]。

この事件では、詐欺師がディープフェイク技術を使用して被害者の友人の顔と声を模倣して友人になりすまして、SNSアプリ「微信（WeChat）」のビデオ通話で被害者に接触しました。詐欺師は、別の都市で行われるプロジェクトへ入札するので、被害者の会社の銀行口座から入札先の銀行口座へ430万元を振り込んでほしい、その金額は直ちに返済すると説明しました。詐欺師は、返済の証拠として被害者の会社の銀行口座に送金した偽の銀行振込伝票のスクリーンショットを送りました。これを信じ込んだ被害者は、指定された銀行口座に430万元を2回に分けて送金しました。実は入札先の銀行口座は、詐欺師の銀行口座でした。送金

が完了した後、被害者が確認のために友人に連絡を取り、ビデオ通話や送金の要求の話をしたところ、友人はそのような行為を全く行っていないと否定したのです。これにより、被害者は自身が詐欺に遭ったことを認識しました。その後、通報を受けた警察が介入した結果、336万8,400元（約6,700万円）を回収できたものの、残りの93万1,600元（約1,800万円）の行方は不明（調査中）となっています。

5.3.2. ディープフェイクで専務の声を模倣する着電

独立行政法人情報処理推進機構（IPA）は8月22日、「サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2023年4月～6月]を公開し、その中でディープフェイク技術を悪用したサイバー犯罪の事例を紹介しました [41]。

図 5-7に示す通り、まず攻撃者は、A社の会長を詐称したメールをB社の社長へ送りました。同日中に攻撃者は、生成AI（ディープフェイク技術）を用いてA社の専務を模倣した声で電話をして「A社の会長からメールで連絡した件のフォローアップをしている」と伝えました。このとき、発信元の電話番号はA社の代表番号に偽装していました。会話内容（言語含む）の詳細は不明ですが、何らかの理由でB社の社長は、電話の相手がA社の専務ではないと気付きました。A社の専務に偽装している攻撃者に、その気づいた事実を伝えたところ、通話は一方的に切れました。このように、B社の社長が攻撃者のなりすましを見抜いたおかげで、金銭的な被害は発生しませんでした。

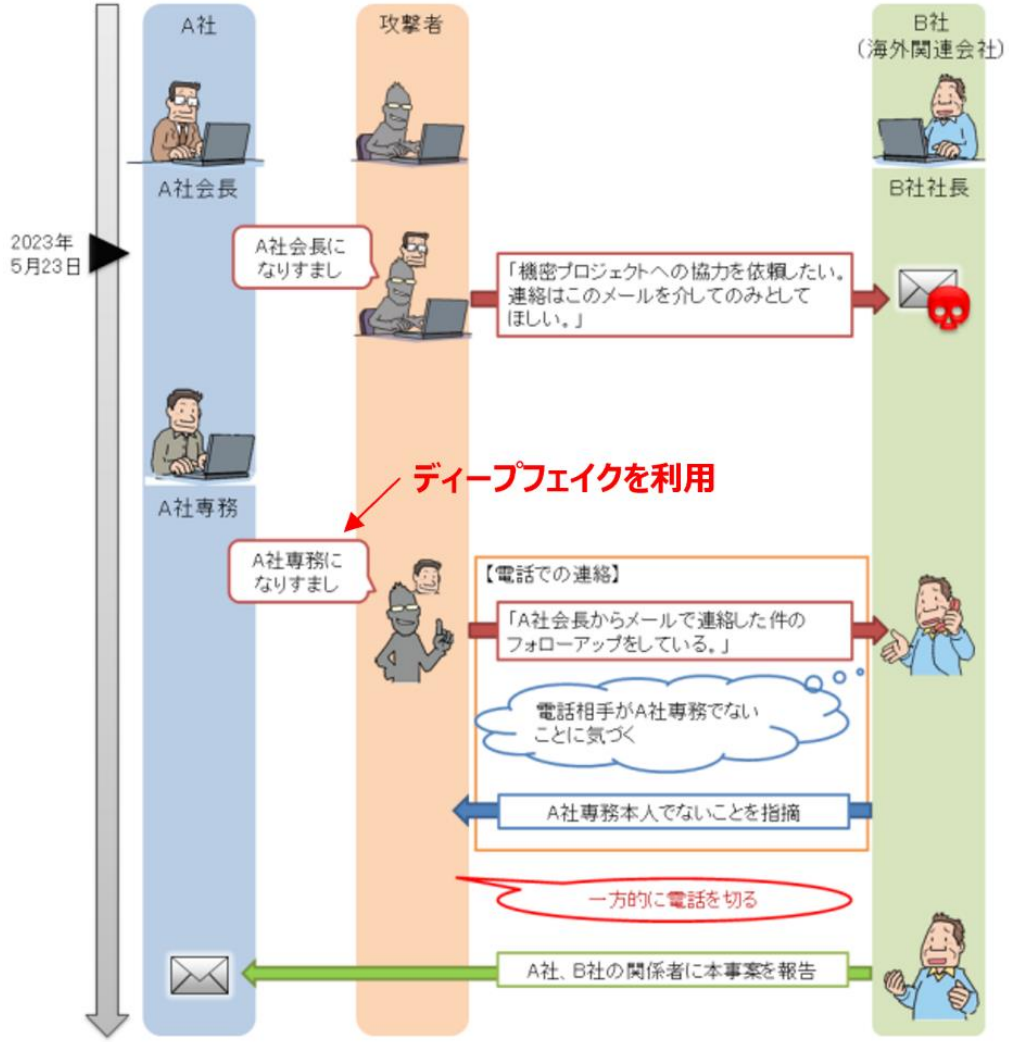


図 5-7：攻撃者とのやりとり（2023年5月）[41]

5.3.3. 対策

5.3.1と5.3.2の事例より、ディープフェイク技術が詐欺犯罪を助長していることが明らかです。特に、緊急性を伴う不動産取引や入札手続き、さらには誘拐事件での身代金要求など、正常な判断が難しい状況で、精巧なディープフェイクを見抜くのはより困難になります。こうしたディープフェイクの脅威から自身の身を守るためには、個人の対策と組織的対策が不可欠となります。

（1） 個人の対策

生成AI（ディープフェイク技術）で音声を模倣できる電話など、音声だけでは相手を信用できない通信手段の場合は、信頼できる代替手段で相手と連絡を取る方法、複数の代替手段で相手と連絡を取って本人や内容を確認する方法で対策できます。まずは通信相手が本人であることを保証できる通信手段を使ってやりとりしましょう。もしメールを使う場合は、SPF、DKIM、DMARKに対応した信頼できるメール環境を使ってください。またチャットやSNS、SMSなどの複数の異なる通信手段を組み合わせて使えば、本人確認の信頼度が上がります。

（2） 組織的な対策

ディープフェイクに騙されないためには、社員にディープフェイク技術を悪用したサイバー犯罪のテクニックを知ってもらい、誰でも騙されやすく危ないことを理解して、警戒してもらうことです。ディープフェイクを悪用したサイバー犯罪から社員を守るための一つの方法は、社員向けのセキュリティ教育プログラムで、ディープフェイクを悪用したサイバー犯罪の手法や実例、対策を説明することです。このように、セキュリティ教育で最新のサイバー攻撃やサイバー犯罪を説明することは、社員が最新のセキュリティ動向やサイバー攻撃の情報を自発的に収集して、セキュリティリスクを認識して、セキュリティ対策や回避行動ができるようになるための一助にもなります。

しかし、ディープフェイクの精度が向上するにつれ、攻撃者や犯罪者が作成した偽情報を見抜くことは困難になります。そのため、技術的対策として、ディープフェイクの検出ツールの開発と普及に期待しています。例えば、ディープフェイクで生成した音声をAIで検出する技術や特定の人物の声を使った音声合成を制限して悪用を未然に防ぐ技術 [11]、本人の音声から声の通り道「声道」のモデルを作成して、その声道モデルを使って人の音声か合成音声かを識別する技術 [12]などが開発されています。市場調査会社HSRCによれば、ディープフェイク検出技術の世界市場はまだ発展段階で、2020年時点で38億6,000万USDの規模[10] です。これから市場規模が拡大して、技術開発がどんどん進むと思います。

（3）法的対策

欧州のディープフェイクや生成AIを含む包括的なAIの規制案である「欧州連合AI規制法案」 [14]は、AIから人間を守り、AIを安全に使いながら技術革新をめざした法律です。中国が施行した「インターネット情報サービスディープフェイク管理規定（互联网信息服务深度合成管理规定）」 [13]は、生成AIやディープフェイク技術によるメディア合成を規制して、違法な情報の作成や拡散を防止する法律です。これらの取り組みから、世界的にAIの悪用を規制する法律の整備が進んでいくと予想します。

5.4. まとめ

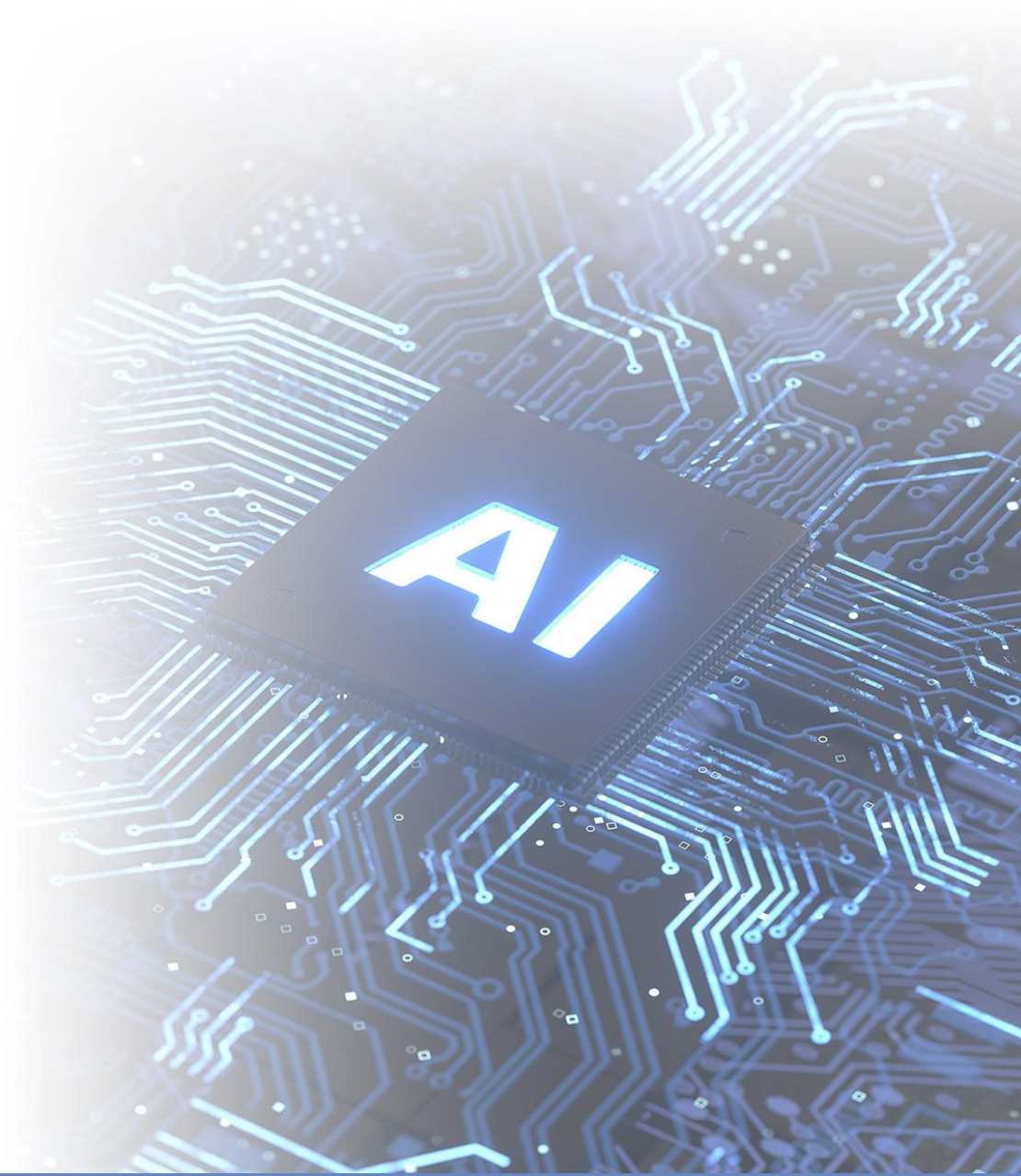
本章では、サイバー犯罪者が悪用する生成AIチャットボットとディープフェイクの事例を紹介しました。生成AIチャットボットであるWormGPTやFraudGPTなどの登場により、サイバー攻撃の初級者でもマルウェアやフィッシングメールを少ない労力で短時間に作成可能になりました。これにより、サイバー犯罪へ参入するときの敷居が下がっています。

また、フィッシングメールの文章の自動生成の精巧化が重大な懸念となってい

ます。これまでのフィッシングメールは、文章の文法誤りや誤字脱字から見抜くことも可能でした。しかし、生成AIの進化により、これらの誤字脱字や違和感のある文法は排除され、より洗練された文章を生成できるため、文章の違和感からフィッシングメールを識別することは困難になっています。そのため、人間の目視チェックに頼らず、最新のセキュリティソフトウェアやフィルタリングツールを導入して、技術的な対策でフィッシングメールの検出とブロックを徹底するべきです。

今後、送信メールフォルダの全メールを使って本人のメールの癖を学習してメール本文を作成し、関係者にフィッシングメールやBECのメールを送る、生成AIチャットボットとEmotetを組み合わせたサイバー攻撃手法の出現は、十分に現実的です。さらには、攻撃者がTeamsを乗っ取った後、攻撃者の生成AIがその人のチャットを学習して、チャット相手と対話してマルウェアを実行させるようなサイバー攻撃も実現可能です。このように、攻撃者が標的にした人の癖を掴むよりも、生成AIの方が早く学習できるため、生成AIによるチャット攻撃は費用対効果が高いと思います。

ディープフェイク技術の進化は、その応用範囲を広げつつあります。特に、学習コストの大幅な低下により、公開されたSNSの画像や動画を使った精巧ななりすましが可能です。これにより、ディープフェイクを使ったいたずらレベルの行為から、他人の肖像権や著作権を侵した偽動画の作成、偽動画を拡散して選挙妨害したり、政治的混乱を狙ったりする社会的影響が大きい行為まで、その悪用の範囲が広がりつつあります。また、ディープフェイク技術を用いた動画や画像の生成は、犯罪の証拠を捏造してアリバイ工作できる、という深刻な問題をもたらす懸念があります。これまで不可能だった証拠の改ざんや捏造が、このディープフェイク技術の進化により可能になりつつあります。こうした証拠捏造を未然に防止するために、AIの使用に関する法律の規制により、AIの犯罪使用への制限を強化することを期待します。



6. 予測

サプライチェーン攻撃の活性化

2023年5月に発生したProgress Software社が提供するMOVEit Transfer（セキュアファイル転送/共有サービス）の大規模なインシデント事例は、脆弱性を起因とする不正アクセスによるサプライチェーン攻撃でした。また2022年に続き、2023年9月にID管理プラットフォームを提供するOkta社で発生した不正アクセスもサプライチェーン攻撃でした。

攻撃者は、標的組織へ直接に侵入できない場合は、標的組織が利用する製品の製造元やクラウドサービスを侵害して、別組織を経由して標的組織への侵入を試みます。一方でサプライチェーン攻撃の目的は、上記の理由以外に、Solarwinds社を経由したサプライチェーン攻撃のように、1社のサービスを経由して一斉に多数の組織への侵入を試みる場合もあります。後者のサプライチェーン攻撃は、多数の組織を一度に侵害できる効率的なサイバー攻撃手法です。MOVEit TransferやOkta社の事例は、後者のサプライチェーン攻撃でした。

多くの組織が利用するオープンソースのソフトウェアや、サードパーティ製品やサービスは、攻撃者にとって一度に多数の標的組織を侵害できる経由地点です。今後も、利用組織が多い製品やサービスを狙ったサプライチェーン攻撃が、増加していくと推測します。

さらに攻撃者は、これから普及するテクノロジやサービスを狙ってサプライチェーン攻撃を行うでしょう。たとえば、多くの組織が注目しているAIを使ったソフトウェアやサービスを開発している企業や、普及が進んでいるゼロトラストセキュリティ関連の製品の開発企業やクラウドサービスを狙うと推測します。

Gmail送信メール要件強化とDMARC普及

Googleは、Gmailアドレスへ5,000件/日以上の大量のメールを送信する送信者に対する新たな要件を2023年10月に公表しました。具体的な要件は、

1. 送信メールを認証すること
2. 未承諾のメールまたは迷惑メールを送信しないようにすること
3. 受信者がメールの配信登録を容易に解除できるようにすること

の3つです。これらの要件は、2024年2月から上記のメール送信者へ適用されます。要件を満たさないメールは、2月以降、ブロックまたは迷惑メールに振り分けられてしまうかもしれません。Gmailヘルプの「1日当たり5,000件以上のメールを送信する場合の要件 [45]」に詳細な説明を記載しています。

1つ目の要件「送信メールを認証すること」には、これまで日本で普及が進んでいないDMARCに関する要件を含んでいます。そのためメールセキュリティ界隈では、「Gmailの要件強化により、ようやく日本でもDMARCの普及が本格化するのではないか」という話が盛り上がっています。総務省は、情報通信白書でメール送信認証の普及率を毎年公表しています。令和5年度版の白書によると、2022年12月時点でDMARCの普及率は2.7%でした [46]。2021年の普及率は2.1%で、近年の普及率は微増のままで推移しています。一方で、フィッシング対策協議会が公表しているフィッシング報告件数はおおむね増加傾向であり、2023年10月の報告件数は過去最高の15.6万件でした [47]。

フィッシング攻撃者は、DNSにDMARCの設定が無かったり、チェックが緩かったりするドメインを調べて、そのようなドメインになりすましたフィッシングメールを送ります。そのため、DMARCが普及すればなりすましに利用できるドメインが減少し、なりすましフィッシングメールの件数は減少するでしょう。またDMARCを導入して適切なポリシーを設定すれば、なりすましフィッシングメールはターゲットのメールボックスに到達する前に、受信メールサーバでブロックま

たは隔離されます。自ブランドをフィッシングの被害から守るという点において
DMARCには明らかな効果があるため、Gmailの要件強化をきっかけに自ドメイン
の送信メール認証設定の再確認を強くお勧めします。

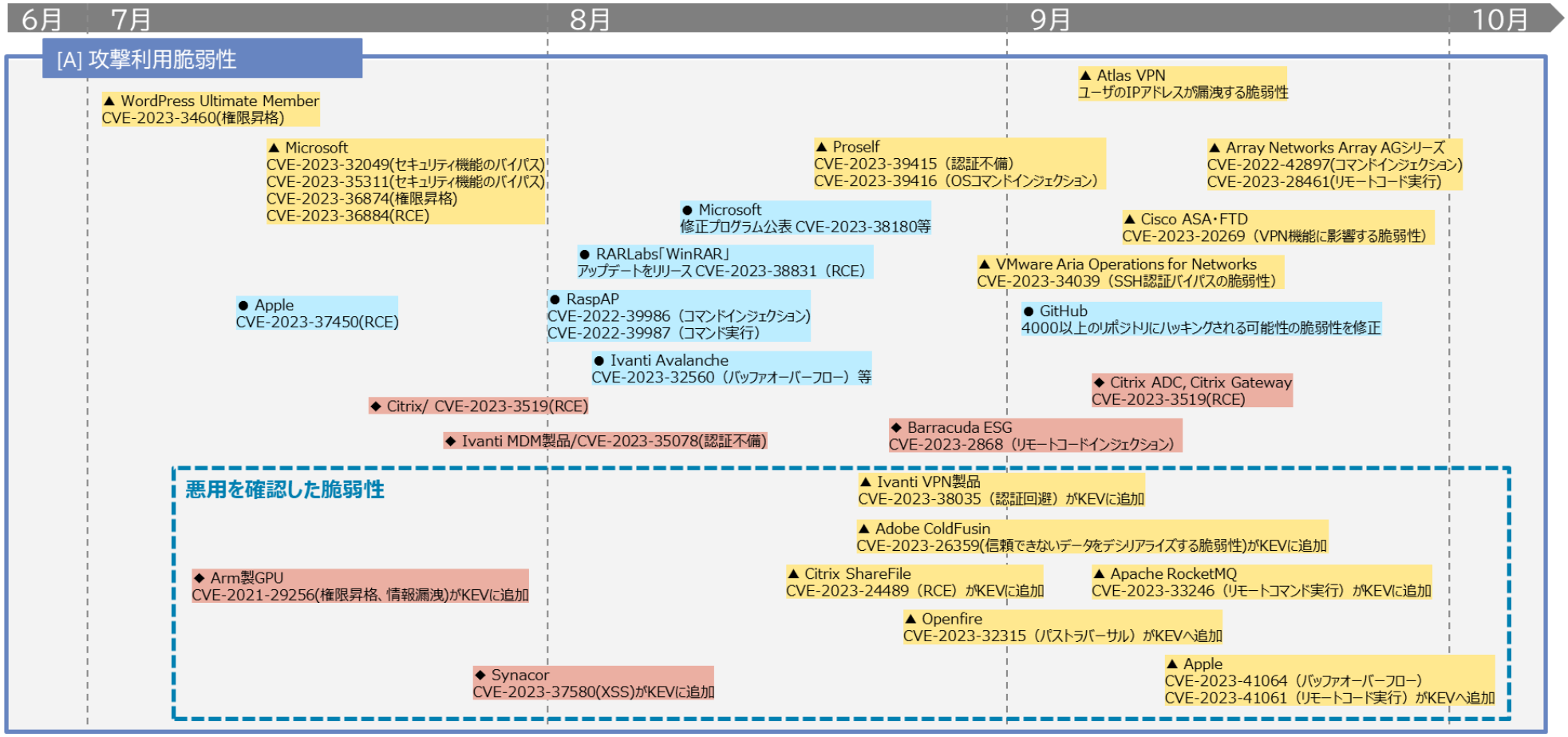
7. タイムライン

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

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

△□◇○:国内
▲■◆●:世界共通・国外

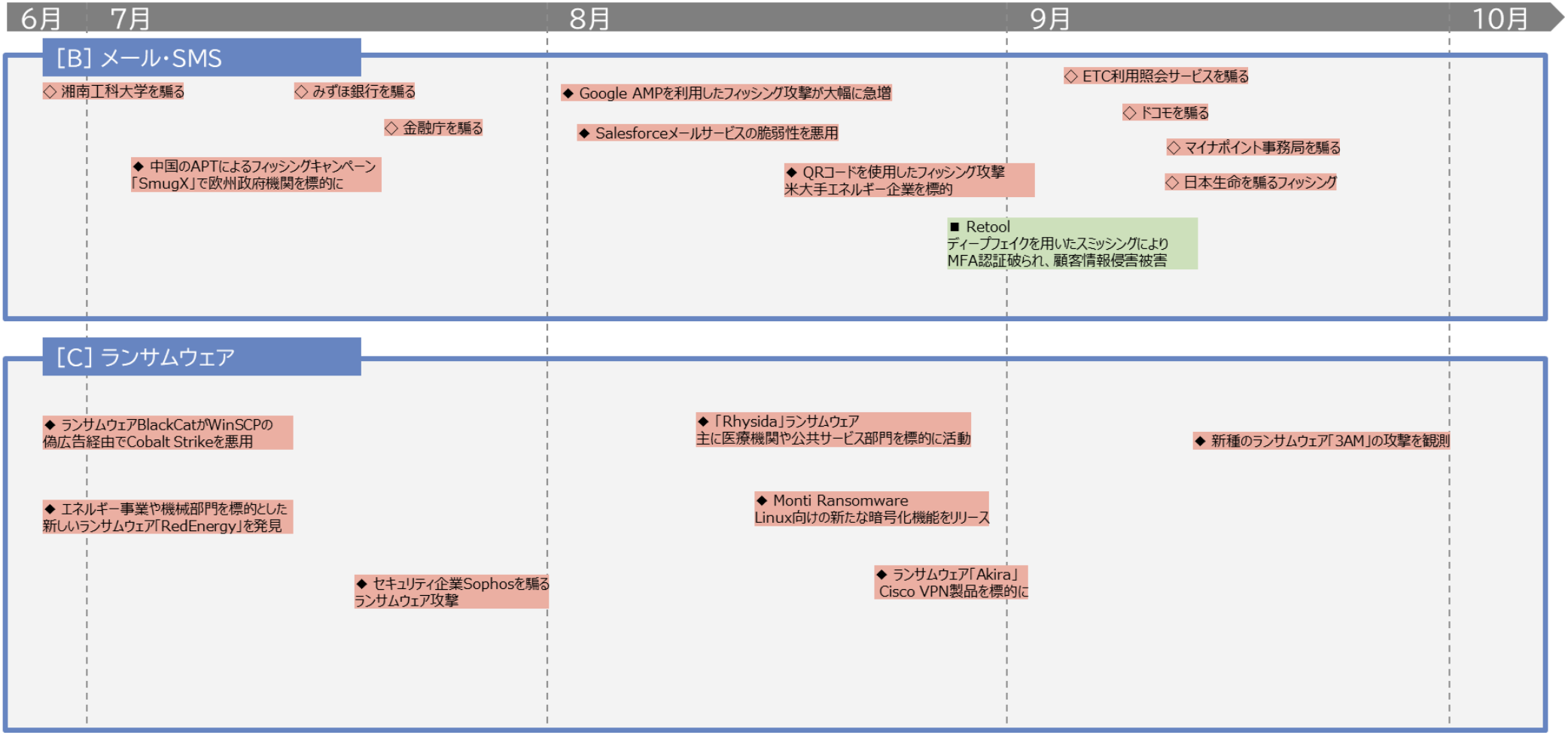
△▲:脆弱性
□■:事件・事故
◇◆:脅威
○●:対策



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

△□◇○:国内
▲■◆●:世界共通・国外

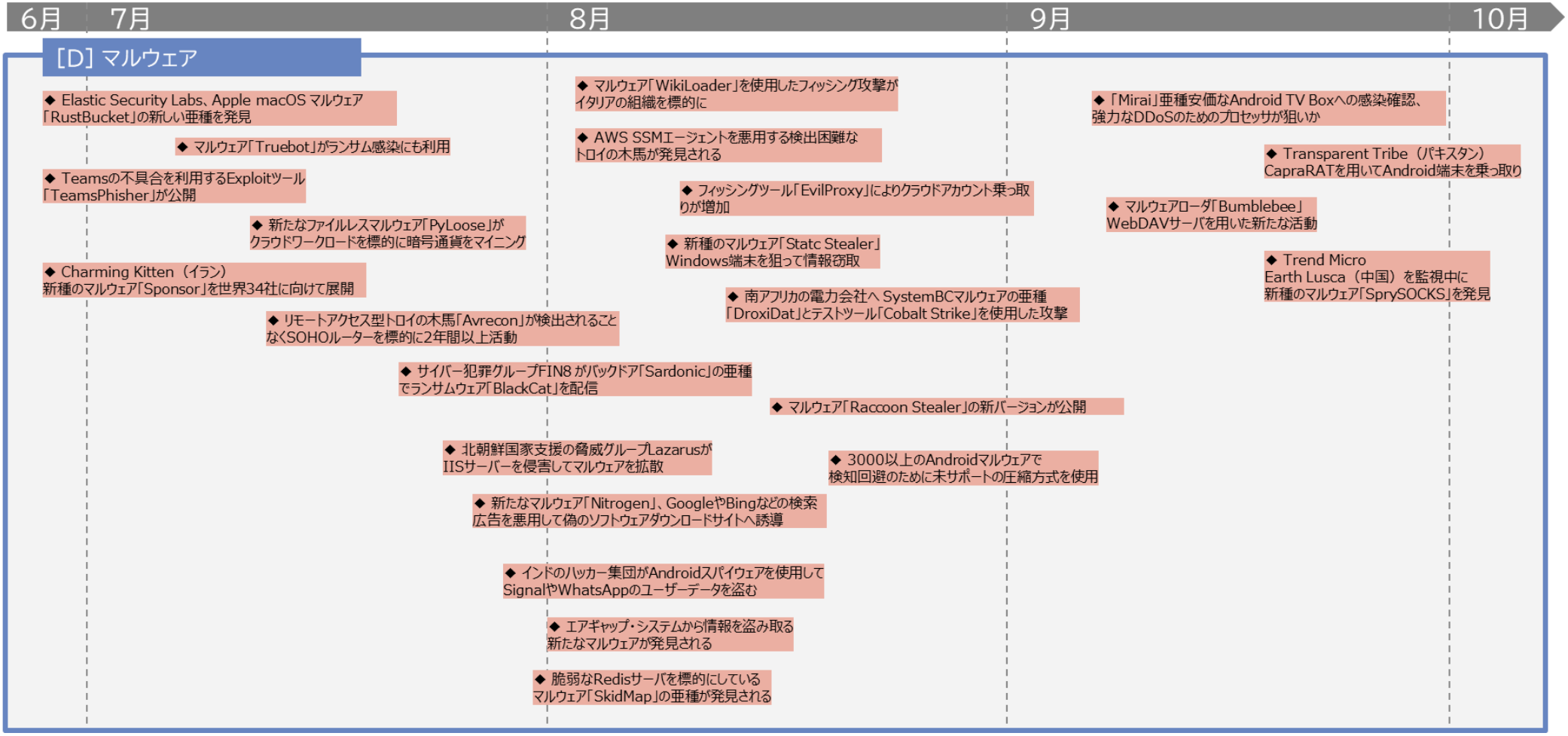
△▲:脆弱性
□■:事件・事故
◇◆:脅威
○●:対策



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

△□◇○:国内
▲■◆●:世界共通・国外

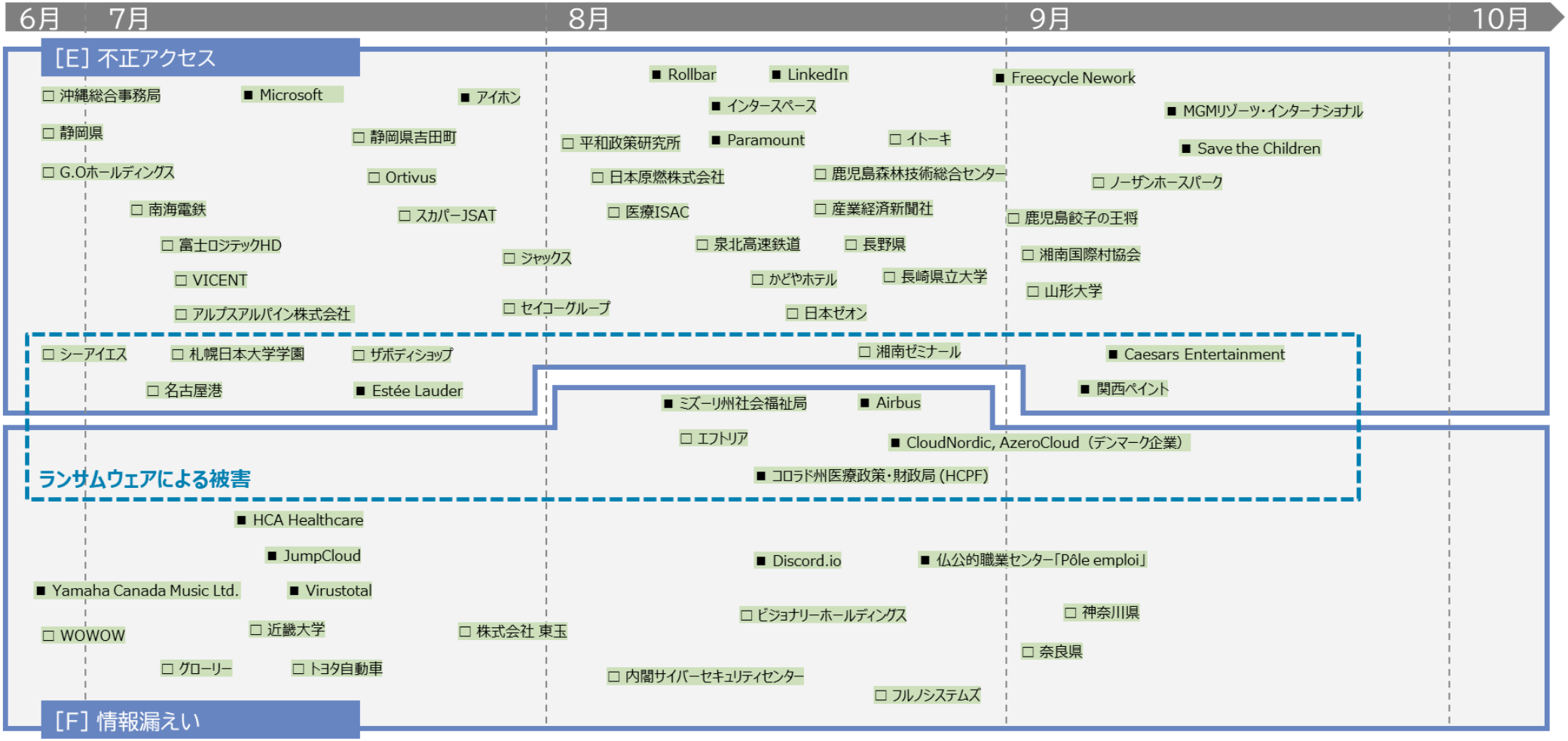
△▲:脆弱性
□■:事件・事故
◇◆:脅威
○●:対策



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

△□◇○:国内
▲■◆●:世界共通・国外

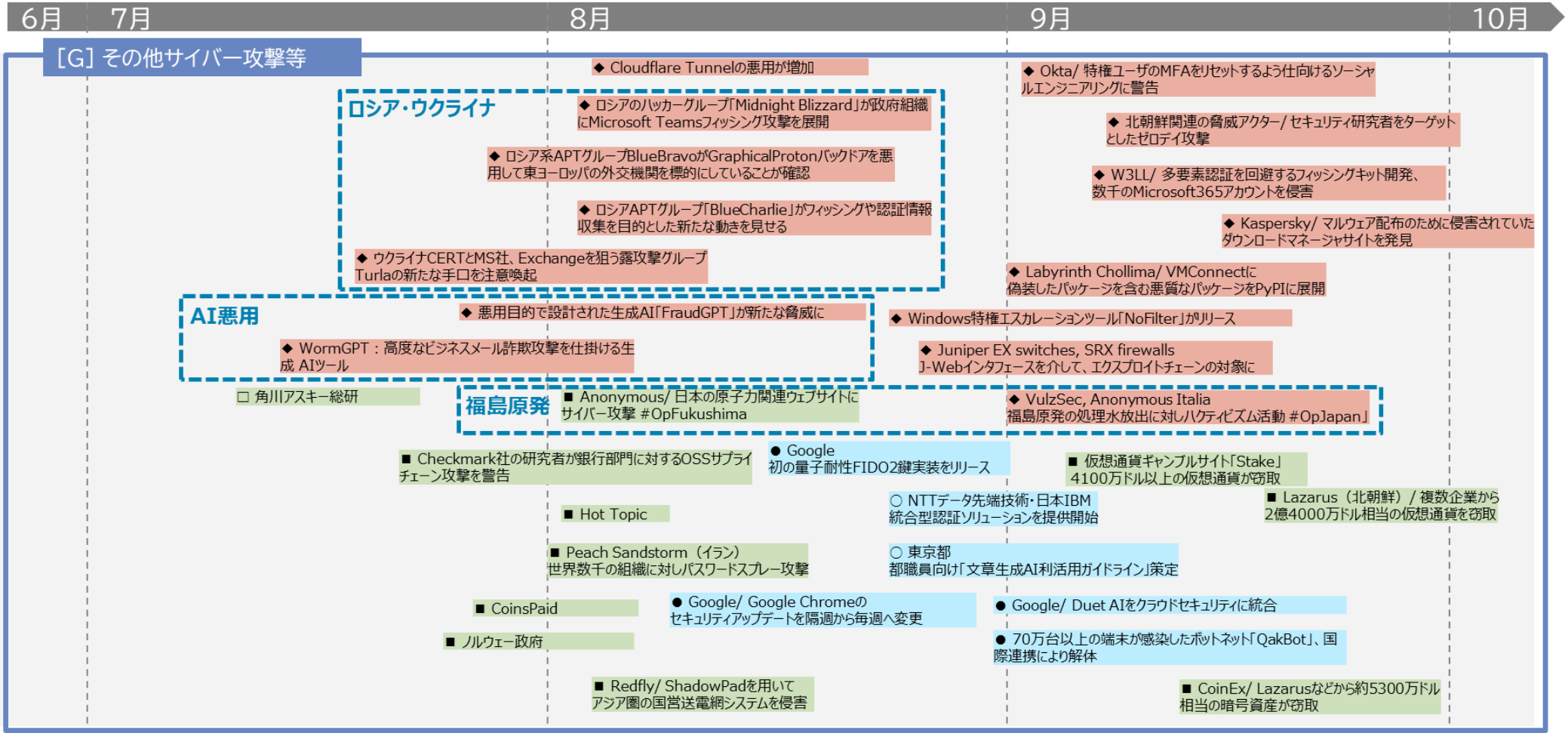
△▲:脆弱性
□■:事件・事故
◇◆:脅威
○●:対策



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

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故
◇◆:脅威
○●:対策



参考文献

[1] 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,” 5 2023. [オンライン]. Available: https://www.nisc.go.jp/pdf/policy/general/rev_pointr5.pdf.

[2] 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（令和５年度版）,” 4 7 2023. [オンライン]. Available: https://www.nisc.go.jp/pdf/policy/general/kijyunr5.pdf.

[3] 内閣サイバーセキュリティセンター, “IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ,” 10 12 2018. [オンライン]. Available: https://www.nisc.go.jp/pdf/policy/general/chotatsu_moshiawase.pdf.

[4] デジタル庁, “常時リスク診断・対処（CRSA）,” 24 5 2023. [オンライン]. Available: https://www.digital.go.jp/policies/security/crsa.

[5] 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３年度版）,” 7 7 2021. [オンライン]. Available: https://www.nisc.go.jp/pdf/policy/general/guider3_2.pdf.

[6] 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）,” 4 7 2023. [オンライン]. Available: https://www.nisc.go.jp/pdf/policy/general/guider5.pdf.

[7] デジタル庁, “地方自治体によるガバメントクラウドの活用について（案）,” 3 2021. [オンライン]. Available: https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/c58162cb-92e5-4a43-9ad5-095b7c45100c/20211224_local_governments_02.pdf.

[8] デジタル庁, “デジタル庁におけるガバメント・クラウド整備のためのクラウドサービスの提供－令和3年度地方公共団体による先行事業及びデジタル庁WEBサイト構築業務－,” 4 10 2021. [オンライン]. Available: https://www.digital.go.jp/procurement/l4j2xC2d.

[9] デジタル庁, “ガバメントクラウドの技術要件に係る市場調査結果の公表について,” 6 2023. [オンライン]. Available: https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/a4275ffc-bd98-4ff0-a72a-

aab60180a8c0/ccb07fd8/20230804_procurement_request_for_information_01.pdf.

[10] N. DATA, “経済安全保障の観点でも注目を集めるソブリンクラウドとは？,” [オンライン]. Available: https://www.nttdata.com/jp/ja/data-insight/2022/0928/.

[11] 内閣サイバーセキュリティセンター, “政府情報システムのためのセキュリティ評価制度（ISMAP）の暫定措置の見直しについて,” 6 7 2021. [オンライン]. Available: https://www.nisc.go.jp/pdf/policy/general/ismap_minaoshi.pdf.

[12] European Commission, “Europe's Digital Decade: Digitally empowered Europe by 2030,” 9 Mar. 2021. [オンライン]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_983.

[13] European Commission, “Commission proposes a trusted and secure Digital Identity,” 3 Jun. 2021. [オンライン]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663.

[14] European Commission, “EU Digital Identity Wallet Toolbox Process | Shaping Europe’s digital future,” 17 Jun. 2023. [オンライン]. Available: https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-toolbox.

[15] European Council, “Council and Parliament strike a deal on a European digital identity (eID) - Consilium,” 29 Jun. 2023. [オンライン]. Available: https://www.consilium.europa.eu/en/press/press-releases/2023/06/29/council-and-parliament-strike-a-deal-on-a-european-digital-identity-eid/.

[16] European Commission, “Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space,” 3 May 200. [オンライン]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197.

[17] NOBID Consortium, “Welcome to the NOBID Consortium,” [オンライン]. Available: https://www.nobidconsortium.com/our-proposal/.

[18] EU Digiatal Identity Wallet Consortium, Home - EUDI Wallet Consortium, [オンライン]. Available: https://eudiwalletconsortium.org/.

[19] Apple Inc., “Apple launches the first driver’s license and state ID in Wallet with Arizona,” 23 Mar. 2022. [オンライン]. Available: https://www.apple.com/newsroom/2022/03/apple-launches-the-first-drivers-license-and-state-id-in-wallet-with-arizona/.

[20] Maryland Department of Transportation, “Maryland Mobile ID Program,” [オンライン]. Available: https://mva.maryland.gov/Pages/mdMobileID.aspx.

[21] デジタル庁, “スマホ用電子証明書搭載サービス,” [オンライン]. Available: https://www.digital.go.jp/policies/mynumber/smartphone-certification/.

[22] デジタル庁, “マイナンバーカードの機能のスマートフォン搭載に関する検討会（第4回）,” 5 Oct. 2023. [オンライン]. Available:

https://www.digital.go.jp/councils/smartphone-mynumbercard/435fbc12-2d78-43b6-83ca-b6f8ea8b81ea.

[23] Trusted Web推進協議会, “学修歴等の本人管理による人材流動の促進,” 7 Jul. 2023. [オンライン]. Available: https://trustedweb.go.jp/news/9ome8xbrgk2s.

[24] W3C, “Verifiable Credentials Data Model v1.1,” 03 Mar. 2022. [オンライン]. Available: https://www.w3.org/TR/vc-data-model-2.0/.

[25] IETF, “Selective Disclosure for JWTs (SD-JWT),” 11 Dec. 2023. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/07/.

[26]“A Basic iPhone Feature Helps Criminals Steal Your Entire Digital Life,” 24 Feb. 2023. [オンライン]. Available: https://www.wsj.com/articles/apple-iphone-security-theft-passcode-data-privacya-basic-iphone-feature-helps-criminals-steal-your-digital-life-cbf14b1a.

[27] Microsoft, “Midnight Blizzard conducts targeted social engineering over Microsoft Teams,” [オンライン]. Available: https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/.

[28] MITRE Corporation, “APT29,” [オンライン]. Available: https://attack.mitre.org/groups/G0016/.

[29] Quorum Cyber, “Threat Intelligence Midnight Blizzard Threat Actor Profile,” [オンライン]. Available: https://www.quorumcyber.com/wp-content/uploads/2023/09/Quorum-Cyber-Midnight-Blizzard-APT29-Threat-Actor-Profile.pdf.

[30] WHITE HOUSE, “FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government,” [オンライン]. Available: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

[31] Microsoft, “Microsoft Fiscal Year 2024 First Quarter Earnings Conference Call,” [オンライン]. Available: https://www.microsoft.com/en-us/investor/events/fy-2024/earnings-fy-2024-q1.aspx.

[32] Demandsage, “Microsoft Teams Statistics – Users & Revenue (2024 Report),” [オンライン]. Available: https://www.demandsage.com/microsoft-teams-statistics/.

[33] Microsoft, “データで見る: COVID-19 でサイバーセキュリティのデジタルトランスフォーメーションが加速,” [オンライン]. Available: https://news.microsoft.com/ja-jp/2020/09/04/200904-microsoft-shows-pandemic-accelerating-transformation-cyber-security/.

[34] Proofpoint, “Microsoft Teamsを用いてフィッシングやマルウェア攻撃を実行する方法,” [オンライン]. Available: https://www.proofpoint.com/jp/blog/threat-insight/dangerous-functionalities-in-microsoft-teams-enable-phishing.

[35] TRUESEC, “DarkGate Loader Malware Delivered via Microsoft Teams,” [オンライン]. Available: https://www.truesec.com/hub/blog/darkgate-loader-delivered-via-teams.

[36] Apple Inc., “Appleは、認知のアクセシビリティのための新機能のほか、Live Speech、Personal Voice、拡大鏡のPoint and Speakを導入します,” 16 5 2023. [オンライン]. Available: https://www.apple.com/jp/newsroom/2023/05/apple-previews-live-speech-personal-voice-and-more-new-accessibility-features/.

[37] 株式会社ディー・エヌ・エー, “生成AIによるリアルタイム音声変換技術を開発 スマホで低遅延に動作し、様々なシーンでの利用が実現,” 10 11 2023. [オンライン]. Available: https://dena.com/jp/press/5053/.

[38] 株式会社産業経済新聞社, “「首相偽動画」が拡散、精巧化するディープフェイクのリスク　技術向上で簡易に,” 14 11 2023. [オンライン]. Available: https://www.sankei.com/article/20231114-LLOVR22LSNOVNFWVGOIRN5JIBU/.

[39] 株式会社産業経済新聞社, “生成ＡＩによる偽動画・画像、パレスチナ紛争やウクライナ戦争で悪用,” 10 11 2023. [オンライン]. Available: https://www.sankei.com/article/20231110-3DE3A5GWDJOUTKLTEZ6YCW2TDM/.

[40] China Daily（中国共産党中央宣伝部）, “Authorities warn public against AI fraud,” 26 5 2023. [オンライン]. Available: https://www.chinadaily.com.cn/a/202305/26/WS646fc5a8a310b6054fad522f.html.

[41] 独立行政法人情報処理推進機構（IPA）, “サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2023年4月～6月],” 22 8 2023. [オンライン]. Available: https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q1-report.pdf.

[42] トレンドマイクロ株式会社, “過度な期待と現実：サイバー犯罪のアンダーグラウンドにおけるChatGPTを中心としたAIの動向,” 12 9 2023. [オンライン]. Available: https://www.trendmicro.com/ja_jp/research/23/i/hype-vs-reality-ai-in-the-cybercriminal-underground.html.

[43] SlashNext, Inc., “WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks,” 13 7 2023. [オンライン]. Available: https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/.

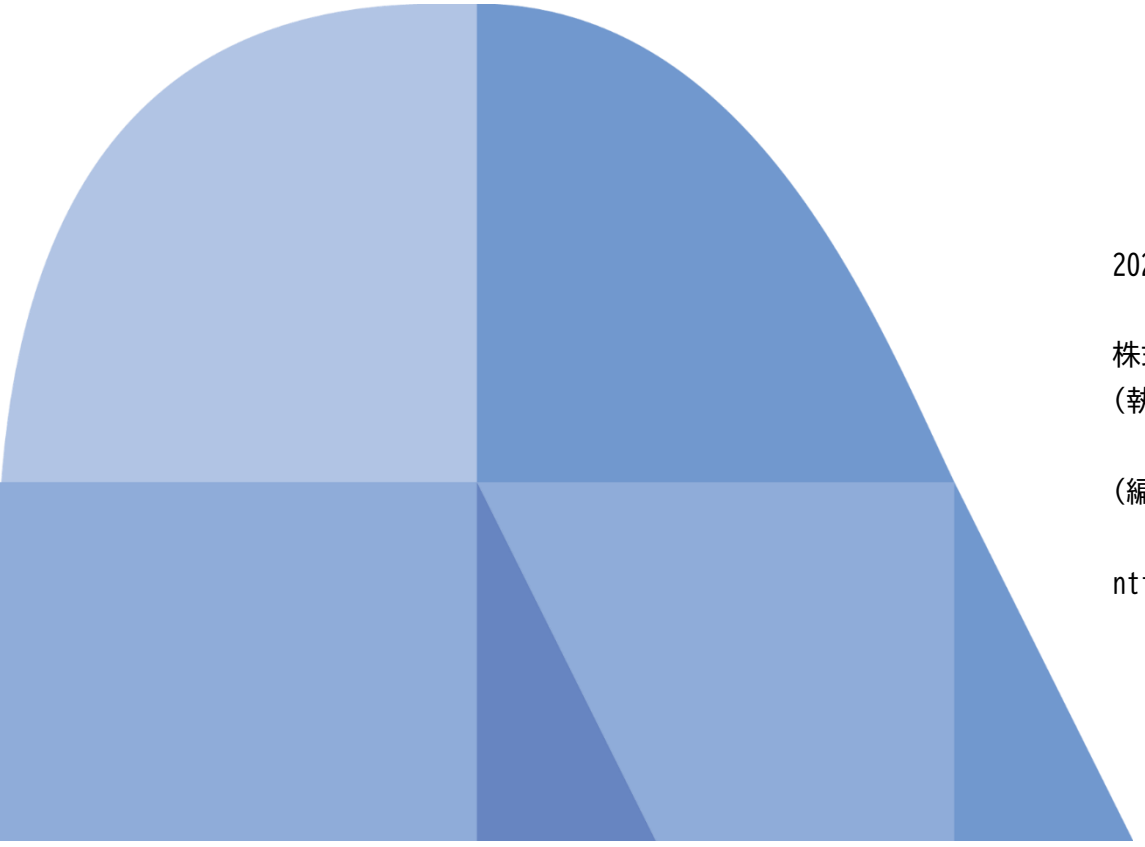
[44] NetEnrich, Inc., “FraudGPT: The Villain Avatar of ChatGPT,” 25 7 2023. [オンライン]. Available: https://netenrich.com/blog/fraudgpt-the-villain-avatar-

of-chatgpt.

[45] Google, “1日当たり5,000件以上のメールを送信する場合の要件,” [オンライン]. Available: https://support.google.com/mail/answer/81126.

[46] 総務省, “情報通信白書 令和5年度版,” [オンライン]. Available: https://www.soumu.go.jp/johotsusintokei/whitepaper/.

[47] フィッシング対策協議会, “2023/10 フィッシング報告状況,” [オンライン]. Available: https://www.antiphishing.jp/report/monthly/202310.html.



2024年2月22日発行

株式会社NTTデータグループ　サイバーセキュリティ技術部
（執筆）小笠原 講太 / 小谷 俊輔 / 白川 剛史 / 鈴木 邦康
寺師 悠平 / 田中 稜太郎
（編集者）大嶋 真一 / 大谷 尚通 / 宮本 久仁男
小笠原 弘貴 / 杉村 耕司 / 前田 秀介
nttdata-cert@kits.nttdata.co.jp