サイバーセキュリティレポート

2022.7

NTT セキュリティ・ジャパン株式会社
コンサルティングサービス部　脅威インテリジェンス管理チーム

目次

【当レポートについて】

当レポートでは 2022 年 7 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『中国で約 10 億人分のデータ流出事件発生』

- 2022 年 7 月の初め、10 億人分の中国国民に関するデータベースを 10 ビットコイン（約 20 万米ドル）で売りに出すというハッカーフォーラムへの書き込みが発見された。
- 上海国家警察の職員が設定を誤って公開していたデータベースが漏洩元とみられており、公開されたサンプルの正確性から漏洩データは本物と考えられている。
- 中国政府は国民の個人データを大量に集めて統治に活用し、近年は「サイバーセキュリティ法」「データセキュリティ法」「個人情報保護法」といったサイバー法制度を整備している。一方で、中国政府からの個人データ漏洩は長年続いており、今回の個人データ漏洩からは実効的なセキュリティ対策を取れていない中国政府の状況が伺える。

第 2 章『NIST、ポスト量子暗号の候補 4 つを公表』

- 7 月 5 日、米国立標準技術研究所(NIST)は、将来的に量子コンピューターが登場しても暗号化されたデータの安全性を確保できる、量子コンピューターに耐えられる暗号の候補として 4 方式を発表した。
- 既存のコンピューターでは解読に天文学的な時間がかかり安全とされている暗号であっても、量子コンピューターを用いると解読が容易になる恐れがある。
- NIST は量子コンピューターが実現するまでは、まだ年単位で時間がかかるので、落ち着いて準備を始めるように呼び掛けている。

第 3 章『AiTM フィッシング攻撃』

- Microsoft のセキュリティ研究チームが、Microsoft 365 アカウントを乗っ取る AiTM (Adversary-in-The-Middle) フィッシング攻撃の大規模なキャンペーンを確認した。
- このキャンペーンで、攻撃者が多要素認証（MFA）を突破し、ターゲットになりすまし、ビジネスメール詐欺（BEC 攻撃)を行っていることが確認されている。
- AiTM 攻撃への対策として、FIDO 認証が注目されている。これは「公開鍵暗号方式」を使用しており、パスワードや多要素認証の弱点を克服しているため、AiTM 攻撃も認証を突破することができない。

1. 中国で約 10 億人分のデータ流出事件発生

1.1. 概要

2022 年 7 月の初め、10 億人分の中国国民に関するデータベースが、ハッカーフォーラムで売りに出されていたのが発見された。上海国家警察から漏洩したという触れ込みで、売主は 10 ビットコイン（約 20 万米ドル）の値を付けていた。被害人数の多さからニュースでは「史上最大級の個人情報漏洩」と紹介されている。[1]

中国政府は警察の治安維持等の統治に活用するために、自国民の膨大な個人データを集めている。今回の事件は、それらの情報の保護が十分でなく、漏洩しやすい状況にあることを露呈させた。

1.2. 流出したデータについて

【漏洩したデータの内容】[2] [3]

データベースを売りに出していたのは「ChinaDan」と名乗るハッカーであった。ChinaDan はハッカーフォーラムで、データベースには中国人居住者 10 億人の情報と、氏名、住所、出生地、公民身分番号（国民 ID）、携帯電話番号、犯罪・事件の詳細の記録など数十億件のデータが含まれていると主張した。

ChinaDan は販売するデータベースの一部の約 75 万件を、無料のサンプルデータとして公開していた。この中には例えば上海市のある男性について、2010 年にコンピューターを盗まれる被害に遭い、警察に通報した履歴が記載されている（図 1）。サンプルデータを各メディアが調査したところ、情報が事実と確認できた[4] [5]ことから、販売していたデータベース本体も本物と考えられている。

図 1 ハッカーが公開した犯罪関連のサンプルデータの一部（黒字が記録。個人情報はマスク済）

[1] 出典：Asia Markets 『Shanghai police database for sale in what could be China's biggest ever data breach』 https://www.asiamarkets.com/shanghai-police-database-for-sale-in-what-could-be-chinas-biggest-ever-data-breach/

[2] 出典：Bleeping Computer 『Hacker claims to have stolen data on 1 billion Chinese citizens』 https://www.bleepingcomputer.com/news/security/hacker-claims-to-have-stolen-data-on-1-billion-chinese-citizens/

[3] 出典：ロイター 『中国人 10 億人分の情報、警察から入手 ハッカー主張』 https://jp.reuters.com/article/china-data-hack-idJPKBN2OF1GV

[4] 出典：Twitter 『_KarenHao』 https://twitter.com/_KarenHao/status/1543951891197042688

[5] 出典：CNN.co.jp 『中国１０億人の個人情報流出、１年以上前から放置 警察の犯罪記録も』 https://www.cnn.co.jp/tech/35190030.html

【流出元について】[6] [7]

データベースは 2022 年に上海国家警察から漏洩したと説明されている。セキュリティ研究者の分析では、漏洩の大きな原因は、データベースを扱う上海国家警察の職員が犯した 2 つの錯誤と考えられている。

まず 1 つ目の誤りは、実際のデータを使用したことである。この職員は開発者とみられ、中国国内向けに公開した技術ブログで、ダミーデータを使わずに上海国家警察の本物のデータベースを使用し、その認証情報を表示させていた。

2 つ目の誤りは、データベースのアクセス権限が、設定ミスにより公開状態になっていたことである。使用していたデータベースは ElasticSearch で、ElasticSearch のアクセス権限設定ミスは中国に限らず世界中で度々発生しており、攻撃者に狙われている。データベースは少なくとも 2021 年 4 月から公開状態であったとみられ、URL さえ知っていればパスワードを入力しなくても、誰でもアクセスできる状態が続いていた。一部のハッカーやセキュリティ研究者は事件以前から存在に気づいていたとみられており、6 月半ばごろにはランサム攻撃に遭っていることを検知した研究者もいる（ChinaDan による攻撃かは不明）。データベースは ChinaDan による流出発覚後に閉鎖された。

【書き込みの削除】[8]

ChinaDan の書き込みは 7 月 3 日頃に、ハッカーフォーラムの管理者によって削除された。それまでに、6 ビットコインでの買取りの打診が 1 件書き込まれていたが、実際にデータベースが売られたかは確認されていない。

1.3. 事件の影響

【中国政府の反応】

この漏洩事件について中国政府は公的には反応を示していない。中国外務省の趙立堅副報道局長は記者会見で事実関係を問われ、「把握していない。コメントは控える」と答えた[9]。一方で、習近平国家主席は、漏洩事件後、公的機関に「情報セキュリティを守る」よう促したと伝えられている[10]。

---

[6] 出典：Twitter 『@cz_binance』
https://twitter.com/cz_binance/status/1543700689611792386
https://twitter.com/cz_binance/status/1543905416748359680

[7] 出典：CNN.co.jp 『中国１０億人の個人情報流出、１年以上前から放置　警察の犯罪記録も』
https://www.cnn.co.jp/tech/35190030.html

[8] 出典：Asia Markets 『Shanghai police database for sale in what could be China's biggest ever data breach』
https://www.asiamarkets.com/shanghai-police-database-for-sale-in-what-could-be-chinas-biggest-ever-data-breach/

[9] 出典：日本経済新聞 『中国個人情報、10 億人分流出か』
https://www.nikkei.com/article/DGKKZO62354760V00C22A7FF8000

[10] 出典：BBC News 『Security warning after sale of stolen Chinese data』
https://www.bbc.com/news/technology-62097594

【中国国民の反応】

ChinaDan の書き込みの後、中国国内でも SNS「微博（ウェイボー）」や「微信（ウィーチャット）」で漏洩事件が発生したとの情報が広まった。だが、子細に個人情報を収集する中国政府の長年の統治から、政府の監視体制や情報漏洩について多くの中国国民は受け入れており、このような巨大な漏洩事件であっても反応は薄かった[11]。

それでも、流出情報には、生活に欠かせない公民身分番号と携帯電話番号まで含まれており中国国民を不安にさせかねないため、情報統制として微博では 7 月 3 日午後までに、データ漏洩を話題にする中国語のハッシュタグがブロックされた[12]。

1.4. 中国漏洩事情

【国民の個人データを活用する中国政府】

中国の政府組織は中国国民の個人データを大量に集め、データベースにして分析し、国民の監視等に活用している。今回の事件で情報の漏洩元になった上海警察もそのひとつである。

上海警察は 2021 年、データベースをビッグデータ解析し、ジュース専門店チェーンのフランチャイズ加盟店で経営悪化が発生していることを発見した。この分析結果をきっかけに捜査に乗り出したことが、フランチャイズ加盟店に詐欺を行っていた開店支援コンサルタント集団の逮捕に繋がった[13]。

一方で、中国政府の巨大なデータベースはひとたび漏洩すると被害者数が膨大になることを、今回の事件は露見させた。

【個人データを売る役人たち】[14] [15] [16]

中国では、企業の社員や政府職員といった内部犯が職務上アクセスできる個人データを売人へと売り渡すことで、個人情報漏洩が発生している。個人データは闇市場へ流れ、電話詐欺で多額の資金をだまし取られる等の被害が発生している。

売人は、政府の公式名簿を活用してターゲットとなる政府職員を簡単に見つけ出し、声をかける。データベースを売り渡すと数年分の収入に相当する稼ぎを手に入れられるため、薄給の政府職員は賄賂にすぐなびくと売人は語っている。警官も例外ではなく、一部の若い中国人警察官は、VPN 等で海外のテレグラムに接続して売人と連絡を取ることで、個人データを売っている。中には「警務通」と呼ばれる交通警察のシステムを利用することにより手に入れた個人の写真や住所を、15 元（約 290 円）で販売している警官もいるという。

---

[11] 出典：ZDNet Japan 『企業による従業員への監視強化に抵抗する中国の人々』
https://japan.zdnet.com/article/35190892/

[12] 出典：ロイター 『中国人 10 億人分の情報、警察から入手 ハッカー主張』
https://jp.reuters.com/article/china-data-hack-idJPKBN2OF1GV

[13] 出典：ZDNet Japan 『中国警察が犯罪発見にビッグデータを活用』
https://japan.zdnet.com/article/35174339/

[14] 出典：WSJ 『中国「監視国家」の副作用、流出情報を闇取引』
https://jp.wsj.com/articles/china-has-a-problem-with-data-leaks-one-reason-is-its-surveillance-state-11658451483

[15] 出典：文春オンライン 『「習近平の ID 番号でユーザー登録すると…」ダメ警官が指導者の個人情報を転売、中国"最強監視社会"のショボい裏側』
https://bunshun.jp/articles/-/47249

[16] 出典：自由時報電子報 『習近平與女兒個資怎曝光？知情者：中國警察賣掉的』
https://news.ltn.com.tw/news/world/breakingnews/3437280

【個人データの暴露】[17] [18] [19]

2018 年、ある警官が習近平国家主席の個人データを 6,000 元（約 11 万 9,000 円）で売人に販売した。情報は中国国外のサーバーに設けられた中国語アングラサイトに暴露され、目にした若者たちは悪乗りして習近平の公民身分番号でゲームのアカウントを取得した。また 2019 年には、習近平の情報を基にして特定された、習近平の娘の個人データがアングラサイトに暴露され、娘はいたずら電話を掛けられる等の被害を受けた。（図 2）

これらの事件に関連した 24 人の若者が有罪判決を受け、首謀者とされた若者は懲役 14 年の判決を受けていたことが、2021 年に明らかになった。

図 2 アングラサイトに暴露された習近平と娘の個人データ[20]

2020 年には、中国の反体制グループが 2016 年に窃取した中国共産党の党員約 200 万人分の機密情報（党での役職、生年月日、公民身分番号、民族等）が、オーストラリアの報道機関へ渡された。[21]

これらの暴露活動は、2014 年頃から中国の若者による反体制ハッカーグループにより行われている。グループは複数存在し、緩やかな繋がりであることから「中国のアノニマス」とも呼ばれる。彼らは政府当局の取り締まり等に遭いながらも、中国国外のインターネットに接続して、アングラサイトやテレグラムのグループ内で活動している。

---

[17] 出典：The Japan Times 『China prosecutes people who posted leaked info on Xi's daughter』
https://www.japantimes.co.jp/news/2021/04/24/asia-pacific/politics-diplomacy-asia-pacific/china-xi-daughter-courts/

[18] 出典：RFA 自由亞洲電台粵語部 『【惡俗維基案】習家訊息從公安購得 販賣訊息官僚已被內部處理』
https://www.rfa.org/cantonese/news/leak-02232021111044.html

[19] 出典：Yahoo!ニュース-個人 『「日系企業社員にも」中国共産党員リストの情報流出を仕掛けた中華ハッカー組織の正体（安田峰俊）』
https://news.yahoo.co.jp/byline/yasudaminetoshi/20210205-00221021

[20] 出典：自由時報電子報 『習近平與女兒個資怎曝光？知情者：中國警察賣掉的』
https://news.ltn.com.tw/news/world/breakingnews/3437280

[21] 出典：Infosecurity Magazine 『Data Leak Exposes Details of Two Million Chinese Communist Party Members』
https://www.infosecurity-magazine.com/news/data-leak-chinese-communist-party/

【中国政府の個人情報保護法制】

中国では 2010 年代後半、民間企業で漏洩事件が多発して多くの国民が被害に遭った。例えば、2018 年に「微博」など主要 SNS から、30 億件もの個人データが不正アクセスにより盗まれ、マーケティングに悪用されたことがあった。このとき流出した個人データは中国の闇サイトで、1 件 3,000 元(約 5 万 9,000 円)前後で売買された[22]。このような事件から、個人情報保護の意識が急速に高まった。

また中国政府も同時期に、国家の安全保障のためのインターネット上の統治を目的として、情報漏洩等のインシデント時の漏洩元の組織および個人の責任等を規定した「サイバーセキュリティ法」（2017 年施行）、データ処理者の責務を規定した「データセキュリティ法」（2021 年施行）、個人情報および個人情報主体の権利の保護について規定した「個人情報保護法」（2021 年施行）といった、罰則を定めた個人情報やサイバーセキュリティに関連する法律を施行している[23]。

一方で、統治における個人データ活用（捜査でのビッグデータ解析等）に注力し続ける中国政府自身は、セキュリティ関連法を順守できる体制にないとの指摘もある[24]。

1.5. まとめ

サイバーセキュリティーにおいて中華人民共和国は、情報機関や人民解放軍が標的型攻撃を行い、また数多くのサイバー犯罪者が野放しにされていることから、サイバー犯罪の最大の加害者の一角とみなされている。

しかし、今回の大量の情報漏洩から、中国自体も容易に被害者になることが明らかになった。中国政府は国民の統治のために自国民の膨大な個人データを集積していたが、逆にそれが国家安全保障上の脅威となる大量の個人データの国外への漏洩を招いた。

今回の事件は、中国政府が個人情報保護法制施行後も実効的なセキュリティ対策を取れておらず、今後も政府からの巨大な漏洩事件に悩まされ続けるであろうことを示唆している。

[22] 出典：産経ニュース 『「微博」など中国ＳＮＳから個人情報３０億件流出　現地ＩＴ企業トップが首謀か』
https://www.sankei.com/article/20180829-CPO3TXPZXNISHPQ62J7XJ5OIPM/

[23] 出典：ジェトロ 『中国におけるサイバーセキュリティー、データセキュリティーおよび個人情報保護の法規制にかかわる対策マニュアル（2021 年 11 月）』
https://www.jetro.go.jp/world/reports/2021/02/0c080037fe572f0d.html

[24] 出典：WSJ 『中国「監視国家」の副作用、流出情報を闇取引』
https://jp.wsj.com/articles/china-has-a-problem-with-data-leaks-one-reason-is-its-surveillance-state-11658451483

2. NIST、ポスト量子暗号の候補 4 つを公表

2.1. 概要

7 月 5 日、米国立標準技術研究所（NIST）は、将来的に量子コンピューターが登場しても暗号化されたデータの安全性を確保できる、ポスト量子暗号（Post-Quantum Cryptography）の候補として 4 方式を発表した[25]。また、量子コンピューターは複雑な計算処理を高速で行うことが可能であるため、将来これが利用できるようになると、現在広く利用されている技術で作成された暗号データは解読される恐れがあるため、備えを始めるように呼び掛けた。この発表を受け、米国土安全保障省サイバーセキュリティインフラセキュリティ庁（CISA）も、「ポスト量子暗号イニシアチブ」を設立し、各省庁のポスト量子暗号への準備を推進することを発表した[26]。

図 3 NIST のニュースリリース [25]

2.2. インターネットと暗号技術

【インターネットと暗号技術】

インターネットは、元々は米国内の大学や学術機関を接続する形で始まり、論文や研究データの交換といった公開情報の共有目的で利用されていたため[27]、暗号はほとんど利用されていなかった[28]。1989 年に商用 ISP が誕生し、一般に開放されると、利用者が増えると共に、通信速度の向上や暗号技術が発展していった。徐々に、電子署名、電子証明書等、実社会と変わらない信用をつなぐ基盤が整備されていき、現在ではビジネスや行政サービス等も内包する社会インフラへと大きく発展した。

【現在利用されている暗号技術の概要】

現在広く利用されている暗号方式として、まず、暗号化と復号に同じ鍵を利用する「**共通鍵暗号**」がある。これは比較的少ない処理で暗号化・復号できるが、事前に鍵となる情報を安全に交換しておく必要がある。例としては、無線 LAN の暗号化等で利用されている「AES (Advanced Encryption Standard)」がある。

---

[25] 出典：NIST 『NIST Announces First Four Quantum-Resistant Cryptographic Algorithms』
https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[26] 出典：CISA 『CISA ANNOUNCES POST-QUANTUM CRYPTOGRAPHY INITIATIVE』
https://www.cisa.gov/news/2022/07/06/cisa-announces-post-quantum-cryptography-initiative

[27] 出典：総務省 『インターネットの登場・普及とコミュニケーションの変化』
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd111120.html

[28] 出典：JPINIC 『暗号～意識せずに使っている必要不可欠な技術～』
https://www.nic.ad.jp/ja/newsletter/No79/0320.html

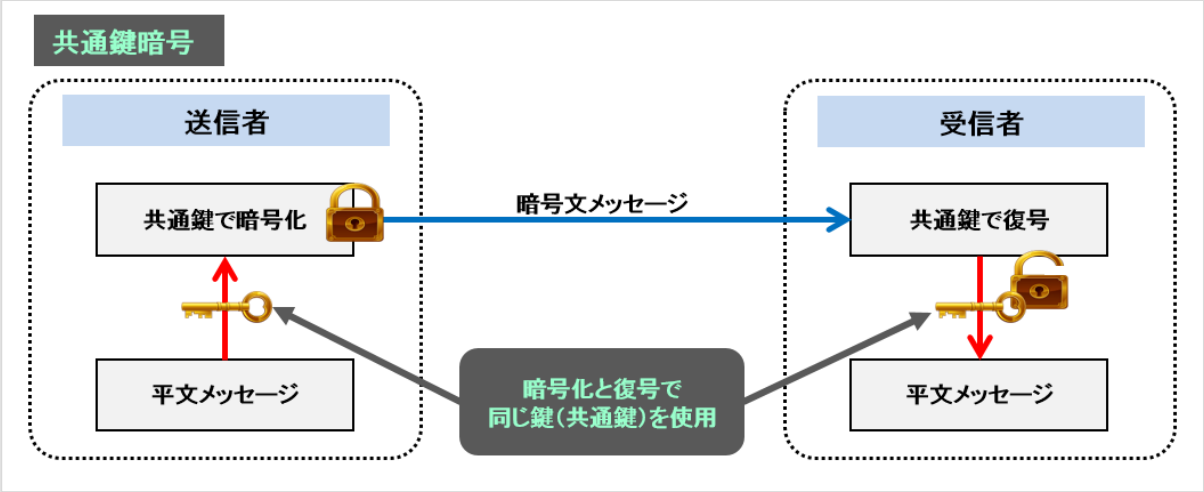

図 4 共通鍵暗号の模式図[29]

次に、「**公開鍵暗号**」がある。これは、暗号化用と復号用とで異なる 2 つのペアとなる鍵を用いる。処理に時間がかかるが、暗号化用の鍵は公開することが前提になっており、第三者に取得されてもその鍵で復号することはできず、事前の鍵交換は必要ない。例としては、SSL/TLS 等で用いられる「RSA 暗号」があげられる。

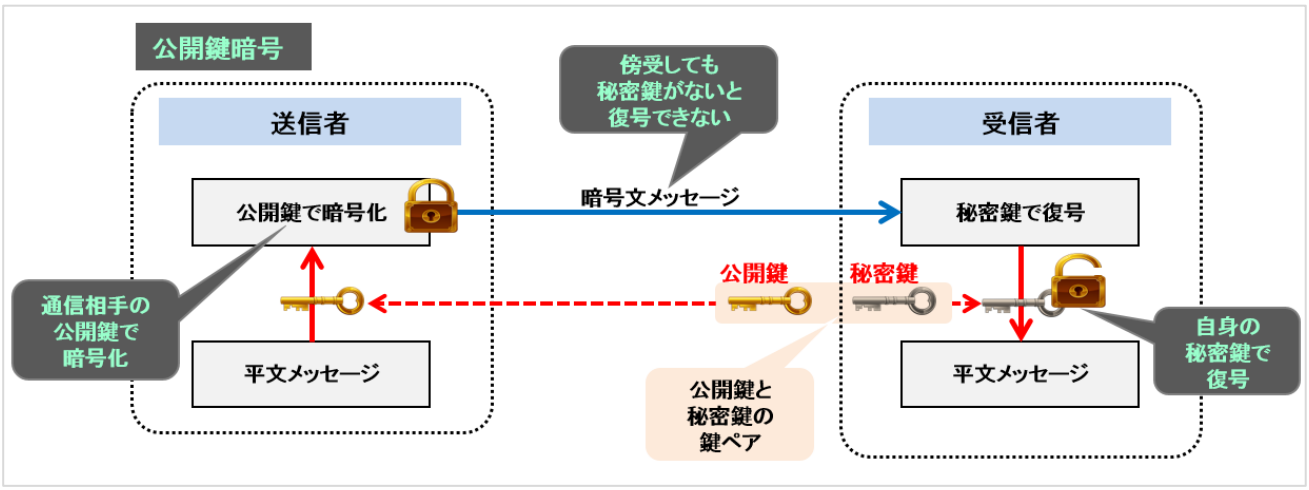

図 5 公開暗号の模式図[30]

さらに、同じデータからは同じ文字列が得られ、異なるデータから同じ文字列が出力されることはない「**一方向性ハッシュ関数**」という技術が、電子署名において通信相手のなりすましの防止やデータの改ざん防止に活用されている。この例としては、SSL/TLS のサーバー証明書などで利用されている「SHA-2」がある。

[29] 出典：JPRS 『共通鍵暗号』
https://jprs.jp/glossary/index.php?ID=0227
[30] 出典：JPRS 『秘密鍵暗号』
https://jprs.jp/glossary/index.php?ID=0226

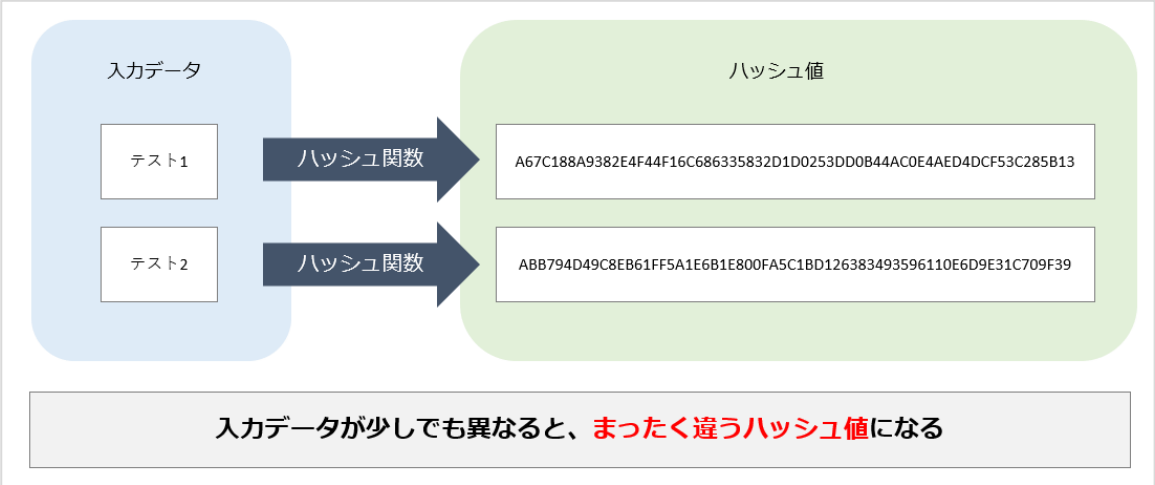

図 6 一方向性ハッシュ関数の模式図[31]

【量子コンピューターによる暗号技術の危殆化】

現在利用されている暗号技術は、数学的な計算処理を取り入れている。これによって暗号化されたデータだけを入手しても、鍵がなければ解読に天文学的な時間がかかる。例えば、前述の公開鍵暗号「RSA 暗号」の解読には素因数分解が使われるが、大きな桁の素数同士を掛け合わせた数を素因数分解することは、処理に非常に時間がかかる。そのため、解読は実質的に不可能であることを安全性の根拠としている[32]。

また、一般的に、鍵となるデータが長ければ長いほど、復号に時間を要し、より安全となる[33]。例えば、RSA 暗号方式で暗号化されたデータを現在最速のスーパーコンピューターを用いて解読する場合、鍵の桁数が 1024 ビットだと 1 年未満で解読できるが、2048 ビットになると 1 億年以上かかるといわれている[34]。

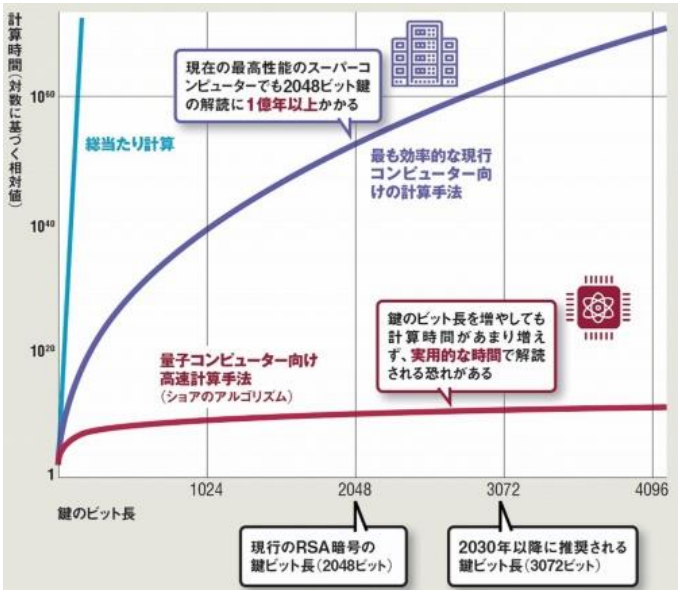

図 7 鍵の長さに対しての現在のコンピューターと量子コンピューターの計算時間の比較 [34]

このように現在利用されているコンピューターを前提とした場合、鍵の桁数を増やすことで、復号のための計算量と時間が飛躍的に増す。しかし、専門家によると、Google や IBM が開発を行っている**量子コンピューター**の場合、計算速

[31] 出典：IT を分かりやすく解説 『ハッシュ関数の仕組みを図解で分かりやすく解説』
https://medium-company.com/%E3%83%8F%E3%83%83%E3%82%B7%E3%83%A5%E9%96%A2%E6%95%B0/

[32] 出典：サイバートラスト研究開発ブログ 『現在の暗号強度と量子コンピュータの量子ビット数』
https://www.cybertrust.co.jp/blog/rd/pqc/cryptographic-strength.html

[33] 出典：IPA 『暗号技術 Q&A』
https://www.ipa.go.jp/security/enc/qa.html

[34] 出典：日経 XTECH 『量子コンピューターが暗号技術を「破壊」する？その真偽を検証してみた』
https://xtech.nikkei.com/atcl/nxt/column/18/01191/012900001/

度の向上に加え、量子コンピューターが得意とする桁数の大きな素因数分解に効率的な計算方法（ショアのアルゴリズム）を用いることで、鍵の桁数をどれほど増やしていっても解読にあまり時間がかからなくなる。例えば、1024 ビットから 2048 ビットに増えたとしても、計算時間は 8 倍程度の増加で済んでしまう[34]。

2.3. ポスト量子暗号への取り組み

量子コンピューターの登場によって、既存のコンピューターにとって解読が困難であることを安全性の根拠とした暗号化方式による暗号データが解読される可能性、ひいては、現在インターネットが担っている社会インフラが深刻なダメージを受ける可能性が予測されるようになった。NIST は 2016 年にポスト量子暗号への取り組みを発表、暗号方式を公募し、これまで評価と選定を行ってきた。

量子コンピューターを以てしても、解読が困難と考えられる複数の暗号方式が議論され[35]、その成果として、今年 7 月 5 日、NIST はポスト量子暗号の候補として 4 つのアルゴリズムを発表した。

まず、 Web サイトにアクセスするときに使用される一般的な暗号化のための「**CRYSTALS-Kyber**」アルゴリズムがある。この方式は、比較的小さな暗号鍵で済み、処理速度が速いことが利点であると NIST は説明している。

次にデジタル署名用の暗号方式として、「**CRYSTALS-Dilithium**」と「**FALCON**」、「**SPHINCS+**」の 3 つのアルゴリズムを候補としている。これらのうち、「CRYSTALS-Dilithium」は数学的な原理は前述の「CRYSTALS-Kyber」と共通しており、また効率も良いことから主要なアルゴリズムとして推奨されている。「FALCON」はより小さな署名を必要とする状況での利用を想定している。また、「SPHINCS+」は、他の 3 つのアルゴリズムが全て「格子暗号」と呼ばれる技術を用いているのに対し、別の数学的アプローチ(ハッシュ関数)に基づいていることから、バックアップとして候補になった[36]。なお NIST によると、今回採用された「格子暗号」や「ハッシュ関数」を用いない、別の暗号方式も引き続き検討中である。

格子暗号	鍵交換・暗号化：CRYSTALS-KYBER、NTRU、SABER、(Frodo-KEM、NTRU Prime) デジタル署名：CRYSTALS-DILITHIUM、FALCON
符号暗号	鍵交換・暗号化：Classic McEliece、(BIKE、HQC)
多変数多項式暗号	デジタル署名：Rainbow、(GeMSS)
ハッシュ関数署名	デジタル署名：(SPHINCS+)
同種写像暗号	鍵交換・暗号化：(SIKE)
その他	デジタル署名：(Picnic)

図 8 ポスト量子暗号の主な候補[37]

[35] 出典：サイバートラスト研究開発ブログ 『NIST による PQC 標準化プロジェクト』
https://www.cybertrust.co.jp/blog/rd/pqc/nist-pqc.html

[36] 出典：TECH+ 『4 つの「ポスト量子暗号アルゴリズム」発表、NIST』
https://news.mynavi.jp/techplus/article/20220707-2392078/

[37] 出典：CRYPTREC 『暗号技術検討会 ２０２０年度 報告書」
https://www.cryptrec.go.jp/report/cryptrec-rp-1000-2020.pdf

【欧州でのポスト量子暗号への取り組み】

ポスト量子暗号への取り組みは米国だけでなく、欧州各国でも行われている。例えば、3 月 2 日、NATO のサイバーセキュリティーセンター(NCSC)は、量子コンピューターの攻撃にも耐えられるネットワークの構築に成功したと発表した[38]。詳しい技術内容は公開されていないが、従来の暗号技術と新しい耐量子アルゴリズムを組み合わせた、ハイブリッドな暗号技術を採用しているという。NCSC の首席科学者である Konrad Wrona 氏は、「『harvest now and decrypt later』(今収集し、解読は後で行う)という脅威が迫っており、現在および将来の脅威から通信の安全を保護するために、こうした取り組みがますます重要になっている」と述べている。

図 9 NCSC のニュースリリース

2.4. ポスト量子暗号に向けて何をするべきか

NIST が 4 つの暗号方式を候補として発表したのと同日に CISA が発表した「将来の量子ベースの脅威から保護するための新しい暗号化標準の準備」という文書では、ポスト量子暗号への準備として、公開鍵暗号を利用するアプリケーションのリスト化、検証環境でのポスト量子暗号標準のテスト実施、従業員の教育といった比較的、手を付けやすいと思われる事項が上がっている。また、NIST は 2021 年 12 月に公開した動画の中で、現在の暗号を解読できるような量子コンピューターが実現するまでは、数十年とは言わないまでも何年も時間がかかるので、まずは落ち着いて準備を始めるように呼び掛けている[39]。

[38] 出典：NCIA 『NATO Cyber Security Centre experiments with secure network capable of withstanding attack by quantum computers』
https://www.ncia.nato.int/about-us/newsroom/nato-cyber-security-centre-experiments-with-secure-network-capable-of-withstanding-attack-by-quantum-computers.html

[39] 出典：NIST 『Post-Quantum Cryptography: the Good, the Bad, and the Powerful』
https://www.nist.gov/video/post-quantum-cryptography-good-bad-and-powerful

3. AiTM フィッシング攻撃

3.1. 概要

2022 年 7 月 12 日、Microsoft のセキュリティ研究チームが、HTTP プロキシ技術を使って Microsoft 365 アカウントを乗っ取る AiTM（Adversary-in-The-Middle）フィッシング攻撃の大規模なキャンペーンを確認したと発表した[40]。この攻撃は多要素認証（MFA:Multi-Factor Authentication）を回避することが可能で、2021 年 9 月以来、1 万以上の組織が標的となっている。

3.2. AiTM フィッシング攻撃とは

【AiTM フィッシング攻撃】

攻撃者は、フィッシングメール等でユーザーをフィッシングサイトへアクセスさせる。このフィッシングサイトは、不正なプロキシサーバーとして機能し、ユーザーとターゲット Web サイトの間に入り、通信を中継する（図 10）。当該サーバーは、オリジナルのページそのものをユーザーに表示することができるため、攻撃者はオリジナルに似せた偽のコンテンツを作成したり、維持したりする必要がない。ユーザーは正規サイトにアクセスしているつもりであるにもかかわらず、フィッシングサイト上で操作し、これがフィッシングサイトだと気づかずに多要素認証コードをユーザー自身が入力してしまい、フィッシングサイトにパスワードや MFA の PIN（暗証番号）、ログイン状態の維持に使用されるセッション Cookie などを盗まれてしまう。そして、攻撃者は盗んだセッション Cookie をブラウザに挿入することで、不正ログインする。

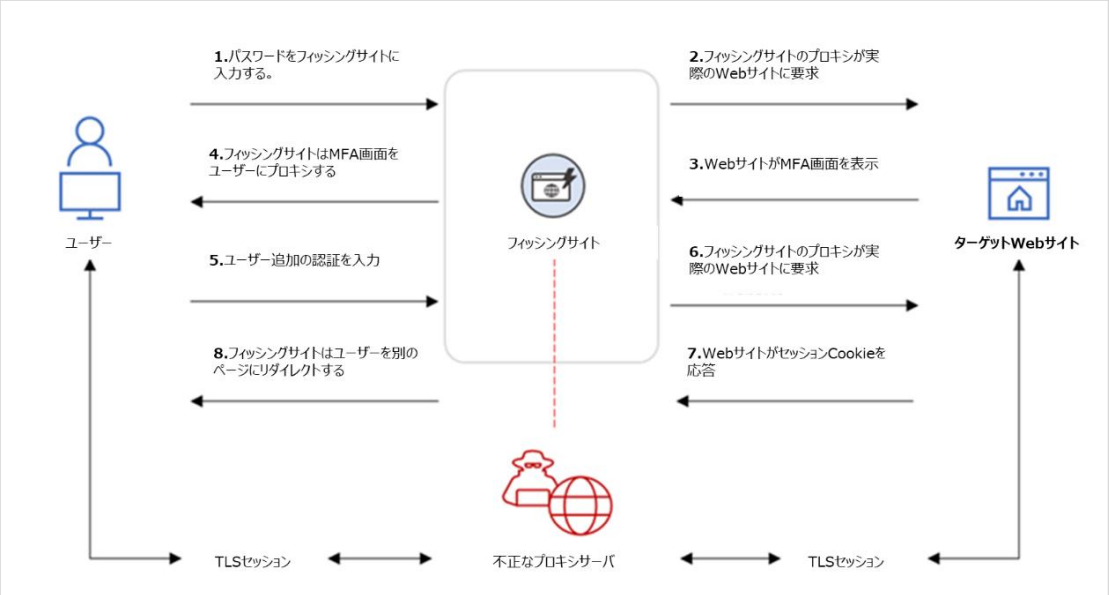

図 10 AiTM フィッシング攻撃の流れ（Microsoft の図を和訳）

[40] 出典：Microsoft 『From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud』
https://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

3.3. AiTM フィッシングキャンペーン

2021 年 9 月以降、Microsoft 365 Defender が 10,000 以上の組織を標的とした AiTM フィッシングキャンペーンを複数検出した。一例として、Microsoft 365 の認証ページをターゲットにした攻撃が挙げられている。

【フィッシング攻撃の例】

攻撃者は、Microsoft 365 ユーザーに対し、音声メッセージのダウンロードを促すメッセージが記載された電子メールを送信する（図 11）。ユーザーが、添付された HTML ファイルを開くと、偽のダウンロード画面が表示された後に、フィッシングサイトへログインするように誘導される。資格情報を入力して認証されると、正規の office.com ページにリダイレクトされる。攻撃者はプロキシサーバー上でセッション Cookie を傍受する。

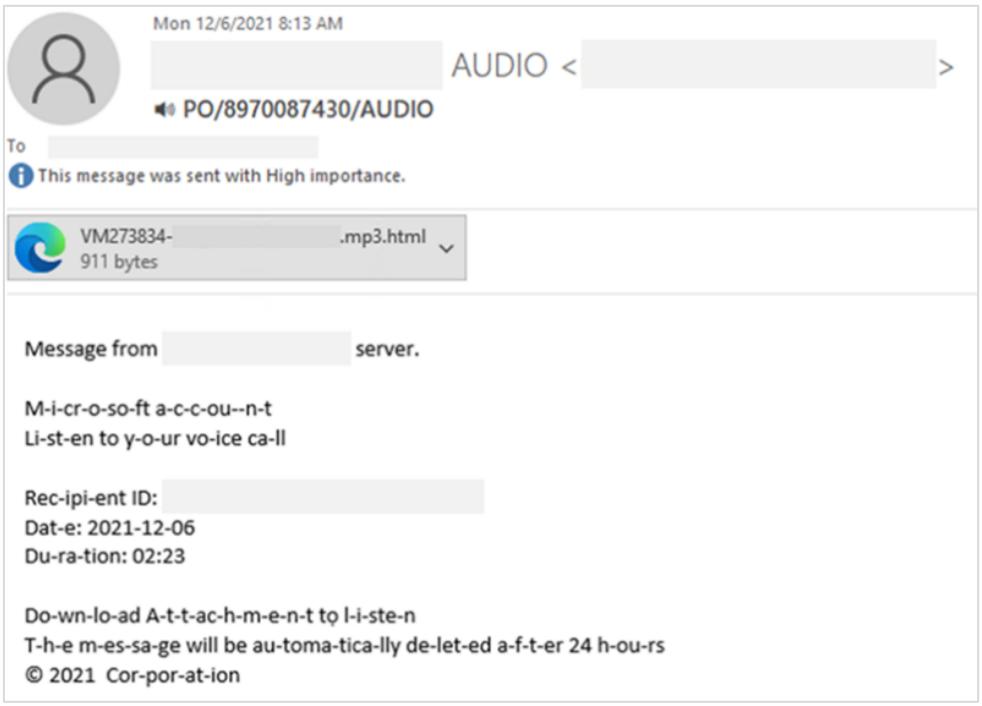

図 11 HTML ファイルが添付されたフィッシングメールのサンプル

【ビジネスメール詐欺（BEC）】

攻撃者は、上述の手法でユーザーから盗んだセッション Cookie を使用して Outlook online (outlook.office.com) に不正アクセスすると、金融関連の電子メールや添付ファイルを探す。（ユーザーが所属する）ターゲット組織と取引先との間で、請求・支払い処理が進行中であることを示す電子メールを見つけた場合は、ターゲット組織になりすましてメールを送信し、取引先から金銭をだましとる。また、これらのやり取りのメールを、ターゲット組織に気づかれないようにするため、全て削除する。

3.4. FIDO 認証[41] [42]

多要素認証を突破する AiTM 攻撃への対策として FIDO 認証が注目されている。**FIDO (Fast IDentity Online)** とは、「高速なオンライン ID 認証」という意味を持ち、生体認証などを利用し、ユーザーがパスワードを覚える必要のない「パスワードレス認証」である。

【FIDO 認証の仕組み】

FIDO 認証には「公開鍵暗号方式」が用いられており、ユーザーはパスワードの代わりに、本人であることを証明する署名をサービス側のサーバーに送る。署名を行う際には、デバイスの **FIDO 認証器**と呼ばれるところに厳正に保管されている、ユーザーの「秘密鍵」が使われ、サービス側とは共有されない。秘密鍵の暗号化による署名（後述）を行うことで、本人証明、非改ざん証明が行われ、ユーザーのなりすましを防ぐことができる。

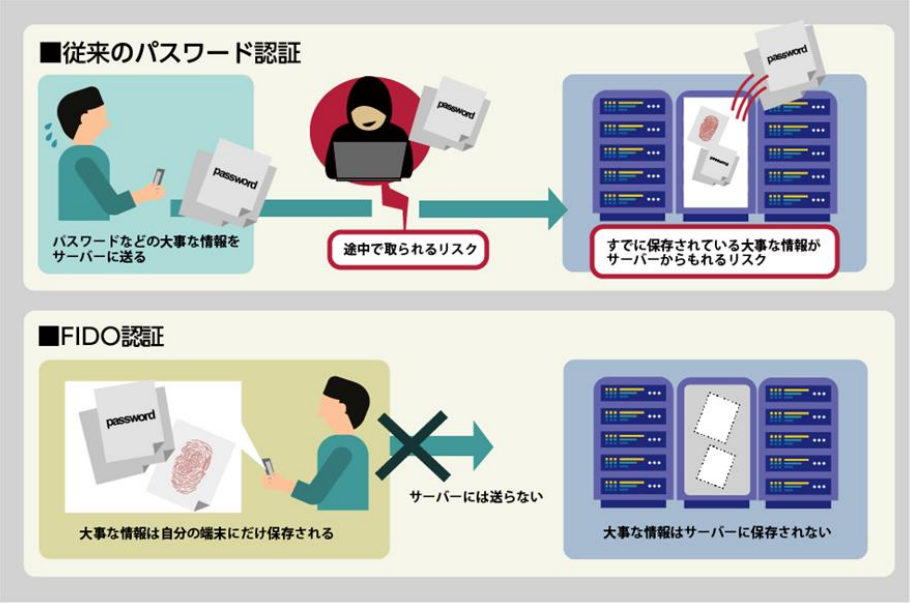

図 12　FIDO 認証の特徴

[41] 出典：NTT コム　オンライン　『パスワードが不要？FIDO 認証の仕組みやメリット・デメリット』
https://www.nttcoms.com/service/ciam/column/20220214/

[42] 出典：YAHOO! JAPAN　『「安全・安心・便利」FIDO（ファイド）を使ったパスワードレスログインとは』
https://about.yahoo.co.jp/info/blog/20190220/fido.html

【FIDO 認証の流れ】

ユーザーは、自身のデバイスにおいて公開鍵と秘密鍵のペアを作成する。その内、公開鍵をサービス側に事前に登録する。

ユーザーがログインする際、サービス側からユーザー専用の受け付け番号である「チャレンジ」が送られる。

ユーザーは自身のデバイスの秘密鍵にアクセスするために生体認証を実施し、サービス側から送られてきたチャレンジに秘密鍵で署名する。

それを受け、サービス側は公開鍵を使用して署名を検証し、問題がなければユーザーをログインさせる。

このように、FIDO 認証であれば、パスワード／多要素認証のように、通信の途中で認証情報を盗まれて使用されるリスクが無いため、AiTM 攻撃を防ぐこともできる。

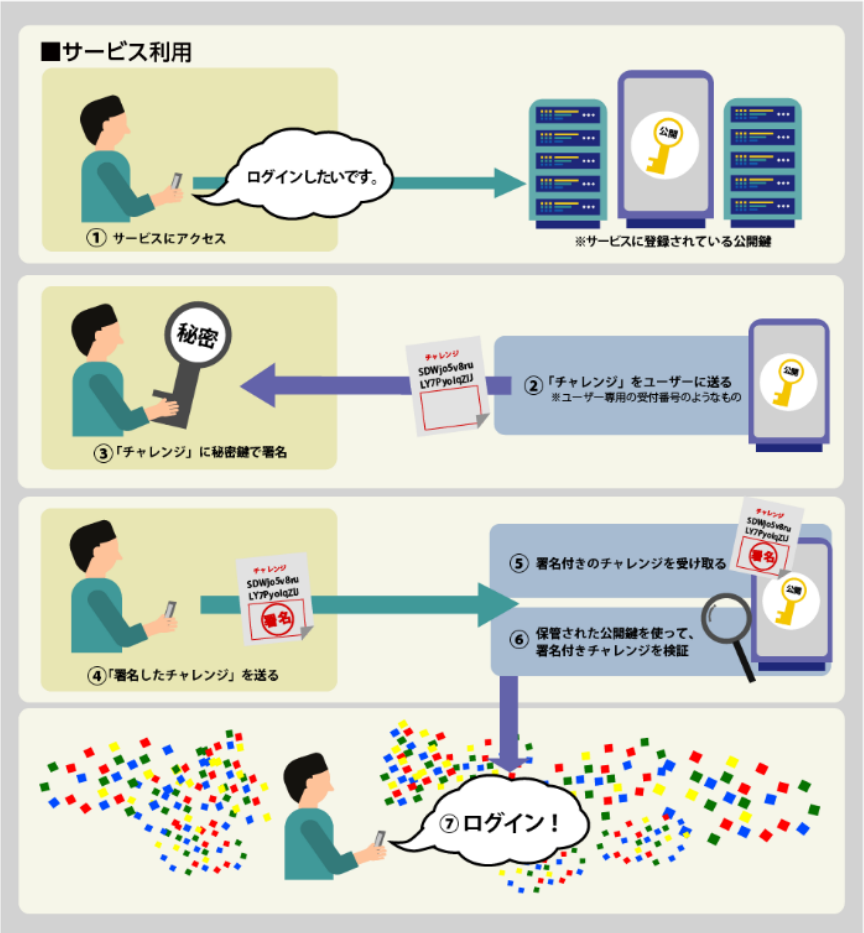

図 13　FIDO 認証の流れ

3.5. まとめ

パスワード認証の弱点を補うとされてきた MFA が AiTM フィッシング攻撃により突破され、多くの組織が攻撃のターゲットとされている。この状況に対し、FIDO 認証は、公開鍵暗号方式を使うことでサービス側が通信相手の検証を行い、AiTM フィッシング攻撃を排除している。フィッシング攻撃の手法は日々進化しているが、防御側の手法も同様であり、常に最新の情報を確認することは重要である。

以上

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

お問い合わせ先：NTT セキュリティ・ジャパン株式会社

コンサルティングサービス部　脅威インテリジェンス管理チーム
メールアドレス： WA_Advisorysupport@ntt.com