サイバーセキュリティレポート
2025.10

NTT セキュリティ・ジャパン株式会社
プロフェッショナルサービス部 OSINT モニタリングチーム

目次

【1 ページサマリー】

当レポートでは 2025 年 10 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『アサヒ GHD を襲ったサイバー攻撃：Qilin ランサムウェアの脅威』

- 9 月 29 日、アサヒグループホールディングスは、サイバー攻撃によるシステム障害の発生を公表した。数日後、この攻撃は、ロシア系ランサムウェアグループ「Qilin」によるものと判明した。
- Qilin は、窃取し暗号化したデータの復号と引き換えにアサヒ GHD に身代金を要求したと主張し、交渉に向けて同社に圧力をかけるため、機密データの一部画像を公開した。
- この攻撃により、国内の受注・出荷業務やコールセンター業務が全面停止し、工場での生産も一時中断。現在も完全復旧には至らず、一部業務は手作業で継続しており、サプライチェーンや小売業にも影響が波及している。

第 2 章『急増する「シャドーAI」が企業にもたらすリスク』

- 職場で承認されていない AI ツールを業務で利用する行為を「シャドーAI」と呼ぶ。マイクロソフト社の調査により、シャドーAI の利用経験がある人の割合が 71%にも及ぶことが明らかになっている。
- シャドーAI の利用により、意図しない機密情報の漏洩などが発生する恐れがある。企業での安全な AI 利用にあたり、公的機関により策定されたガイドラインを参照して、ガバナンスを構築することが推奨されている。
- AI の利用を過度に抑制するのではなく、実用性と安全性のバランスを見極めることが、これからの企業経営において重要な課題となる。

第 3 章『NIST のパスワードポリシーガイドライン更新』

- デジタルアイデンティティのガイドラインである NIST(米国国立標準技術研究所)の SP 800-63 の改訂により、認証とライフサイクル管理に関するドキュメント中のパスワードポリシーガイドラインも最新化された。
- 覚えやすい長文を使用したパスフレーズの利用をさらに促進するため、阻害要因となるパスワード定期変更や文字種に記号を混ぜるといった古いパスワードポリシーを、従来の「すべきではない」から禁止へと明確化する等の更新がされている。
- 同ガイドラインを参考に、自社のパスワードポリシーをセキュリティとユーザビリティを両立した現代的なものへと見直すことを推奨する。

1. アサヒ GHD を襲ったサイバー攻撃：Qilin ランサムウェアの脅威

1.1. 概要

10 月 3 日、アサヒグループホールディングス(以下、アサヒ GHD)は、同社に対して 9 月に実行されたサイバー攻撃がランサムウェアによるものであったことを公表した。攻撃により、従業員の業務負荷が増加している他、サプライチェーン全体で物流遅延が発生し、取引先への影響が広がっている。さらにブランド毀損による顧客からの信頼の低下や、株価下落の懸念も高まっている。アサヒ GHD の発表から数日後、ロシア系ランサムウェアグループ「Qilin」(チーリン)が犯行声明を出した。

図 1 サイバー攻撃によるシステム障害に関する発表(第 1 報、アサヒ GHD のサイトより)[1]

1.2. アサヒ GHD へのランサムウェア攻撃[2, 3]

アサヒ GHD が国内のシステム障害を公表したのは 9 月 29 日。攻撃を受けてから数日間は、国内での受注・出荷やコールセンターに係る業務が全面停止し、工場での生産も中断を余儀なくされた。5 日後の 10 月 3 日、同社は攻撃が「ランサムウェア」によるものであることを初めて認め、情報漏洩の可能性を示す痕跡を確認したとも述べた[4]。

この言葉を裏付けるように、10 月 7 日にはランサムウェアグループ Qilin が、アサヒ GHD から 9,300 件以上のファイルを盗み出し、暗号化したデータの復号と引き換えに、同社に身代金を要求したと自身のリークサイトで主張した。同時に、盗み出した証拠として、財務諸表、従業員の個人情報、機密契約書などを示す 29 枚の画像も公開した。身代金交渉に向けてアサヒ GHD に対して圧力をかける狙いがあったとみられる(図 3)。

---

[1] 出典: アサヒグループホールディングス『サイバー攻撃によるシステム障害発生について』
https://www.asahigroup-holdings.com/newsroom/detail/20250929-0102.html

[2] 出典: BleepingComputer『Qilin ransomware claims Asahi brewery attack, leaks data』
https://www.bleepingcomputer.com/news/security/qilin-ransomware-claims-asahi-brewery-attack-leaks-data/

[3] 出典: Resecurity『Qilin Ransomware and the Ghost Bulletproof Hosting Conglomerate』
https://www.resecurity.com/blog/article/qilin-ransomware-and-the-ghost-bulletproof-hosting-conglomerate

[4] 出典: アサヒグループホールディングス『サイバー攻撃によるシステム障害発生について(第 2 報)』
https://www.asahigroup-holdings.com/newsroom/detail/20251003-0104.html

この翌日以降、アサヒ GHD は、インターネットに流出した疑いのある情報を確認し、その中に個人情報が含まれている可能性があること等を公表した[5, 6]。その後、第 3 四半期の決算発表を延期する事態にも至り、会計処理や社内システムにも影響が及んでいることが明らかとなった[7]。

現在、システム全体の復旧には至っておらず、商品の供給は手作業による受注で対応しており、通常の決済・流通システムは依然として制限されている。専門家からは、システムの中枢が破壊されている可能性があるとの指摘もある。侵入経路などについては、現時点で信頼のおける情報は確認されていない。

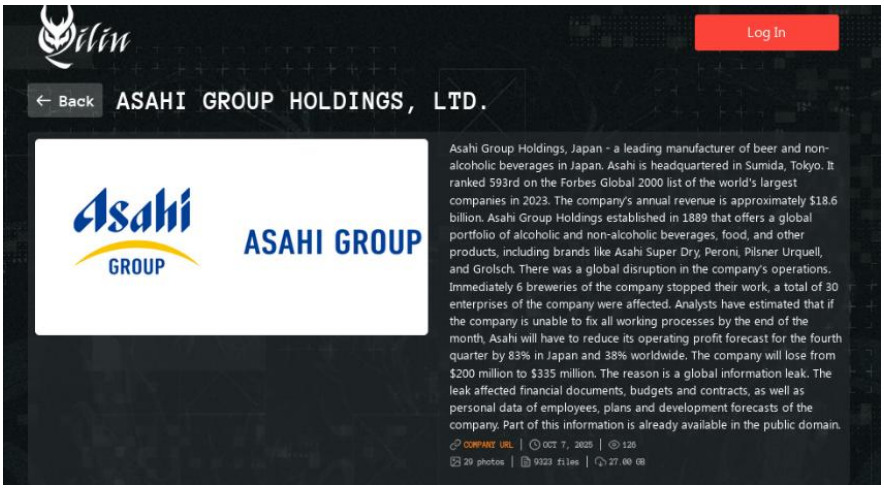

図 2 Qilin がリークサイト上に公開した犯行声明[8]

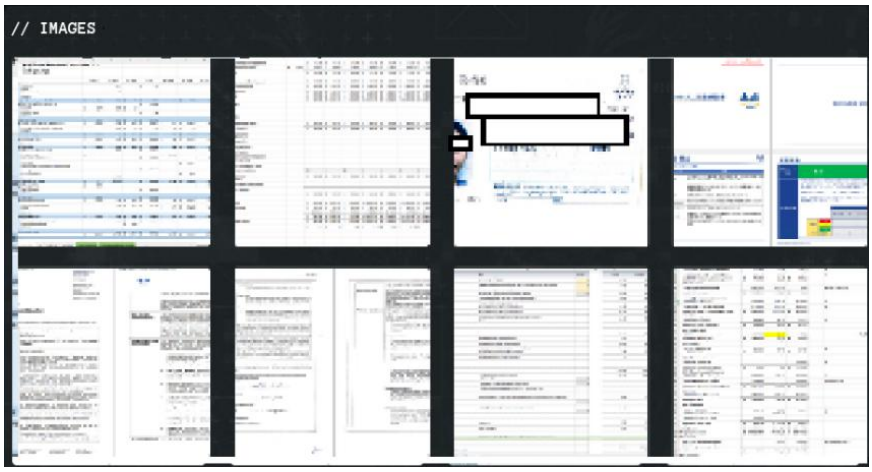

図 3 Qilin がリークサイト上に公開したデータの一部

---

[5] 出典: アサヒグループホールディングス『サイバー攻撃によるシステム障害発生について(第 3 報)』
https://www.asahigroup-holdings.com/newsroom/detail/20251008-0101.html

[6] 出典: アサヒグループホールディングス『サイバー攻撃によるシステム障害発生について(第 4 報)』
https://www.asahigroup-holdings.com/newsroom/detail/20251014-0103.html

[7] 出典: アサヒグループホールディングス『サイバー攻撃によるシステム障害発生に伴う 2025 年 12 月期第 3 四半期決算短信の開示が四半期末後 45 日を超えることに関するお知らせ』
https://www.asahigroup-holdings.com/newsroom/detail/20251014-0101.html

[8] 出典: Resecurity『Qilin Ransomware and the Ghost Bulletproof Hosting Conglomerate』
https://www.resecurity.com/blog/article/qilin-ransomware-and-the-ghost-bulletproof-hosting-conglomerate

1.3. ランサムウェアグループ「Qilin」

【Qilin とは何者か】

Qilin は、2022 年に登場したロシア系とみられるランサムウェアグループであり、現在では世界中から注目を浴びている。当初は「Agenda」という名称を用いていたが、同年 9 月に「Qilin」へ変更して以来、活動規模を拡大させ、技術力を強化している。

【Ransomware-as-a-Service (RaaS)とは】[9, 10]

Qilin は RaaS（Ransomware-as-a-Service [サービスとしてのランサムウェア]）と呼ばれる犯罪ビジネスモデルを採用しており、この運用のために、オペレーター(Operator)と呼ばれる開発・運営者、およびアフィリエイト(Affiliate)と呼ばれる攻撃実行者から成る分業体制を敷いている。他にもイニシャルアクセスブローカー(Initial Access Broker)という役割が存在し、これは、標的となる企業に侵入するために必要な認証情報をアフィリエイトに提供する。アフィリエイトは、この情報およびオペレーターから提供されるランサムウェアのツールを使用し、攻撃を実行する。後に被害企業から身代金が支払われた場合は、これを成功報酬としてオペレーターと山分けする。こうした RaaS の座組みにより、オペレーター側は自身で攻撃するよりも、アフィリエイトを巻き込むことでさまざまな企業や団体に攻撃を仕掛けることができ、身代金を得るチャンスが増える。加えて、アフィリエイトに有料でツールを提供することで収益を得ることも可能だ。

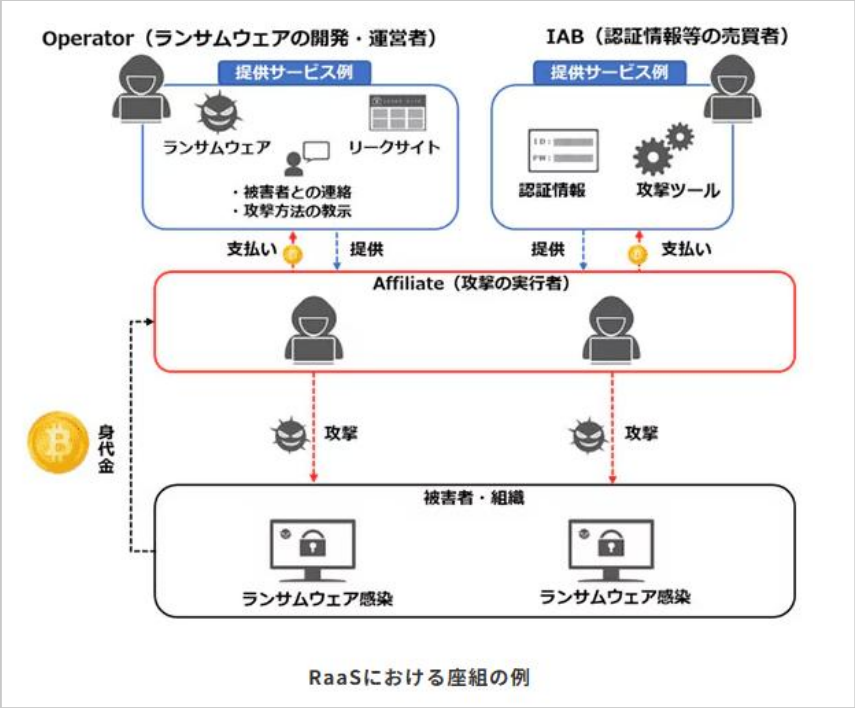

図 4 RaaS を利用したランサムウェア攻撃のイメージ[11]

[9] 出典: NTT ドコモビジネス『サイバー攻撃は「RaaS」でさらに激化する。防ぎ方は？』
https://www.ntt.com/bizon/raas.html?msockid=374f734cb69c625a0d946550b79963fb

[10] 出典: Trend Micro『RaaS (Ransomware as a Service)とは』
https://www.trendmicro.com/ja_jp/what-is/raas.html

[11] 出典: 警察庁『令和 6 年上半期におけるサイバー空間をめぐる脅威の情勢等について』(7 ページより引用)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

【Qilin の攻撃手法】[12]

Qilin のランサムウェアは、Rust や Go といった近年注目されているプログラミング言語を用いて開発されており、Windows、Linux、VMware ESXi といった異なる種類のシステム環境でも同じように動作し、攻撃を仕掛けることができる。彼らの攻撃は複数の段階を経て標的のネットワークに深く侵入し、最終的にはデータの暗号化と恐喝を行うという、極めて組織的かつ巧妙な手法で構成されている。

- **初期侵入**

  VPN 機器の脆弱性、フィッシングメール、改ざんされたウェブサイトや広告、リモートデスクトップを悪用する他、多要素認証(MFA)の回避、Web ブラウザ Chrome で保存された認証情報の窃取などを足がかりに侵入する。いくつかの事例では、ダークウェブ上に漏えいした管理者資格情報を悪用し、多要素認証(MFA)未設定の VPN に対して短時間で集中的に何度も認証突破を試みていた。そして成功後にリモートデスクトッププロトコル(RDP)で組織のネットワークへ侵入していた。

- **権限昇格・内部偵察**

  侵入後は、ネットワーク全体を管理できる「ドメイン管理者」の権限を奪取する。この権限を使用し、ドメインユーザー情報の収集、ユーザーの権限レベルの確認、実行中のプロセスの一覧化、クライアントアプリケーションから保存された認証情報の抽出などを行う。さらに、ネットワークスキャンによってホストや共有リソースの検出を行い、収集した情報を基にネットワーク侵入後の移動経路を検討したり、暗号化対象データの優先順位を決めたりする。

- **二重脅迫**

  データを窃取すると、Qilin はこれを外部の SMTP サーバーなどへ転送する。最近は、クラウドサーバーへのファイル転送を可能にする、「Cyberduck」というオープンソースの FTP クライアントソフトの悪用がみられる。

  転送後は、暗号化技術でデータを使用不可能な状態にする。Qilin のランサムウェアは、暗号化技術が非常に強力で復旧が困難とされている。ランサムウェアの被害を拡大させるために、一般ユーザーディレクトリだけでなく、仮想化インフラや(複数のサーバーを 1 つのサーバーであるかのように動作させる)クラスタ環境も暗号化する。

  その後、盗んだ情報を人質にし、「**データを返して欲しければ金を払え。払わなければそのデータを公開する**」と、被害企業を脅迫する。

- **証拠隠滅**

  自分たちの活動の痕跡となるログを消去し、バックアップを破壊するなどして、調査や復旧を妨害する。

[12] 出典: CISCO TALOS『Uncovering Qilin attack methods exposed through multiple cases』
https://blog.talosintelligence.com/uncovering-qilin-attack-methods-exposed-through-multiple-cases/

1.4. Qilin ランサムウェアによる攻撃被害

【世界的な被害】

Qilin の攻撃回数は年々増えており、2025 年 10 月時点で既に前年の倍以上の被害が出ている。2025 年に観測されている数あるランサムウェアグループの中で、Qilin が最も活発に活動している。

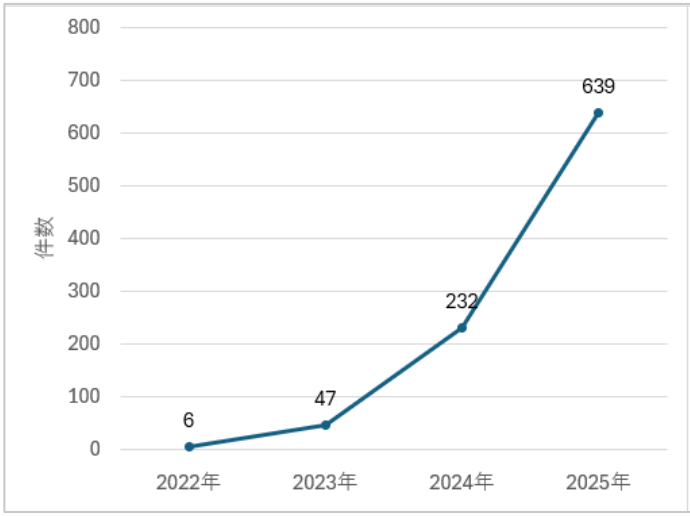

図 5 Qilin により被害に遭った組織の数 (2022 年～2025 年 10 月)

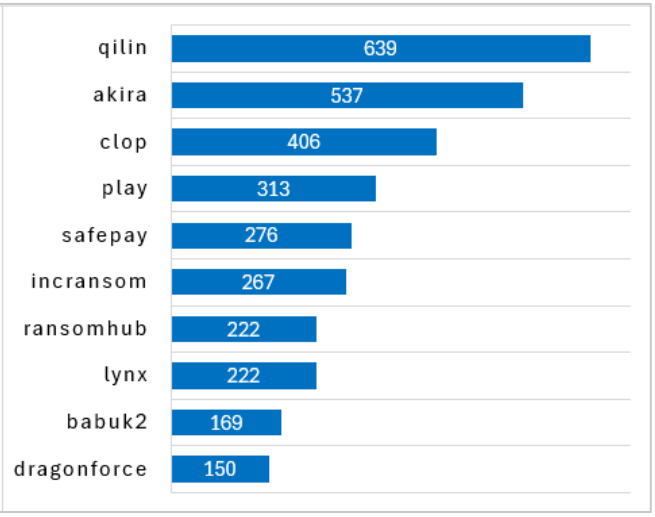

図 6 各ランサムウェアグループにより被害に遭った組織の数 [上位 10 グループ](2025 年観測)

Qilin による国ごとの被害組織の数は、1 位の米国が群を抜いて多く、日本は 8 位。米国以外の国々については、特に共通した傾向はみられない。なお、これらの被害組織の中に、CS 諸国(旧ソ連構成諸国)は含まれていない。

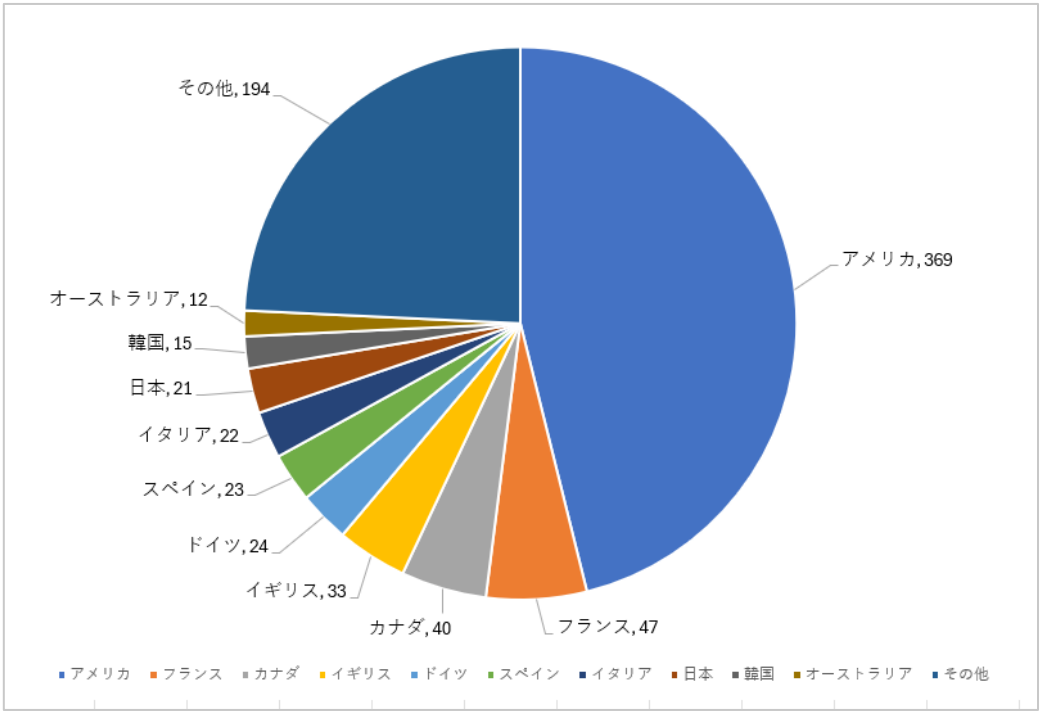

図 7 国ごとの被害組織の数(2022 年～2025 年 10 月)

Qilin によるこれまでの攻撃のうち、件数としては製造業、テクノロジー、医療・ヘルスケア等に関する組織を対象としたものが多いが、業種別に見ると特に偏りはみられない。

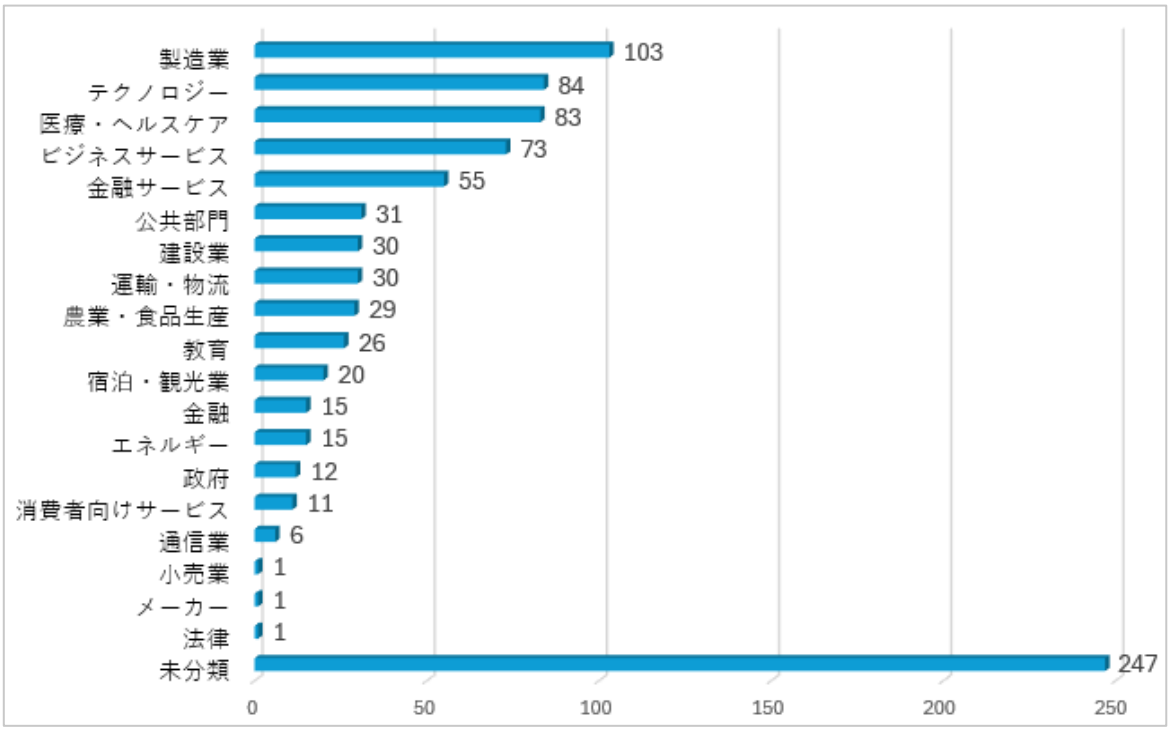

図 8 業種別被害組織件数(2022 年～2025 年 10 月)

【日本国内での被害】

2025 年から、Qilin は日本の組織(主に製造業や医療機関)に対しても相次いで攻撃を実行しており(表 表)、諸外国と同様に国内でも継続的な脅威となっている。

被害公表月	主な被害組織	漏えい内容(Qilin 主張)
2025 年 10 月	アサヒグループホールディングス株式会社	財務諸表、予算、契約書、従業員の個人情報、同社の計画や開発予測
2025 年 8 月	株式会社クリエイティブボックス(日産のデザイン子会社)	3D デザインデータ、レポート、写真、動画、日産自動車に関する各種文書
2025 年 8 月	株式会社丸菱ホールディングス	履歴書、外国人労働者の在留カード情報、交通費書類、検査表
2025 年 8 月	新興プラスチックス株式会社	カード利用情報、支払情報、検収書
2025 年 2 月	医療法人 DIC 宇都宮セントラルクリニック	X 線画像、診療記録、心電図・ホルター心電図、医療検査データ、保険証画像、医療機器のマニュアル、会議議事録等

表 1 日本企業の Qilin ランサムウェア被害事例

1.5. まとめ

Qilin による攻撃を受けたアサヒ GHD では、事業の継続にあたり重大な支障が生じた。過去には、2023 年に名古屋港が攻撃を受け、2024 年には KADOKAWA も同様の被害を受けており、サイバーリスクが災害・環境・地政学リスクと同様に事業運営に直接的な影響を与えることが、今回の事件でも改めて示された。アサヒ GHD をはじめ多くの企業が DX を推進する中、IT への依存度は高まっており、サイバー攻撃のリスクも増大している。そのため、デジタル化の推進と並行してセキュリティ対策を強化することが不可欠である。

2. 急増する「シャドーAI」が企業にもたらすリスク

2.1. 概要

2025 年 10 月、マイクロソフト社が英国の従業員 2,000 人以上を対象に実施した調査結果を公開し、職場で承認されていない個人用 AI ツール利用の実態について警告した[13]。AI ツールの急速な普及に、企業での規程や管理方法の整備が追いついておらず、利便性と安全性のバランスをどう取るべきかが問われている。

2.2. 「シャドーAI」とは?

企業の情報システム部門が把握・管理していない状況下で、部門や従業員が独自に導入・利用している IT 機器やサービスを「シャドーIT」と呼ぶ。業務の効率化や利便性を求める現場のニーズから生まれることが多く、必ずしも利用者に悪意があるわけではないが、セキュリティやコンプライアンスの観点からは重大なリスクを伴う。こうした背景の下、近年急速に注目されているのが「シャドー**AI**」である。

シャドーAI とは、職場で承認されていない AI ツールを業務で利用する行為を指す。例えば、業務におけるメール文面の作成、議事録の要約、翻訳、コードの生成などを、従業員が個人で契約した生成 AI を使って行うケースが挙げられる。マイクロソフト社の調査では、シャドーAI の利用経験がある人の割合が 71%にも及ぶことが明らかになっている [13]。

こうしたシャドーAI を利用する割合が大きくなっている背景の一つとして、私生活で AI に慣れ親しみ、その利便性を実感していることが考えられる。2025 年 1 月の調査時と比較すると、今回の 10 月の調査結果では、AI の利用に自信を持っている人の割合は 34%から 57%に増加し、AI をどこから始めればよいか分からない人の割合は 44%から 36%に低下していることからも [13]、AI の利用が当たり前のものとなりつつあることが伺える。

生成 AI の利用により、英国経済全体で年間約 120 億時間、金額にして 2,070 億ポンド(=日本円で約 42 兆円)に相当する労働時間を節約できているとのデータもあり [13]、AI の利用が生産性の向上に寄与することに疑いの余地はない。

一方で、利便性を優先する余り、現場の判断で不用意にシャドーAI を持ち込むことのリスクを認識し、軽減していく必要がある。

2.3. シャドーAI がもたらすリスク

シャドーAI の最大のリスクは、個人用 AI ツールに入力されたデータが AI の学習に使用されることである。入力されたデータがどのように扱われるかは各 AI サービスの利用規約により異なる。従業員が持ち込んだシャドーAI によっては、入力した業務データや顧客情報が、別のユーザーへの回答に使われ、誰も把握できないまま機密情報が外部に漏洩する恐れがある。

図 9 のように、シャドーAI の利用により実際に機密情報が漏洩した例も報告されているものの、業務データや顧客情報が漏洩してしまうことを懸念している従業員の割合は、わずか 32%である [13]。

[13] 出典: Microsoft『Rise in 'Shadow AI' tools raising security concerns for UK organisations』
https://ukstories.microsoft.com/features/rise-in-shadow-ai-tools-raising-security-concerns-for-uk/

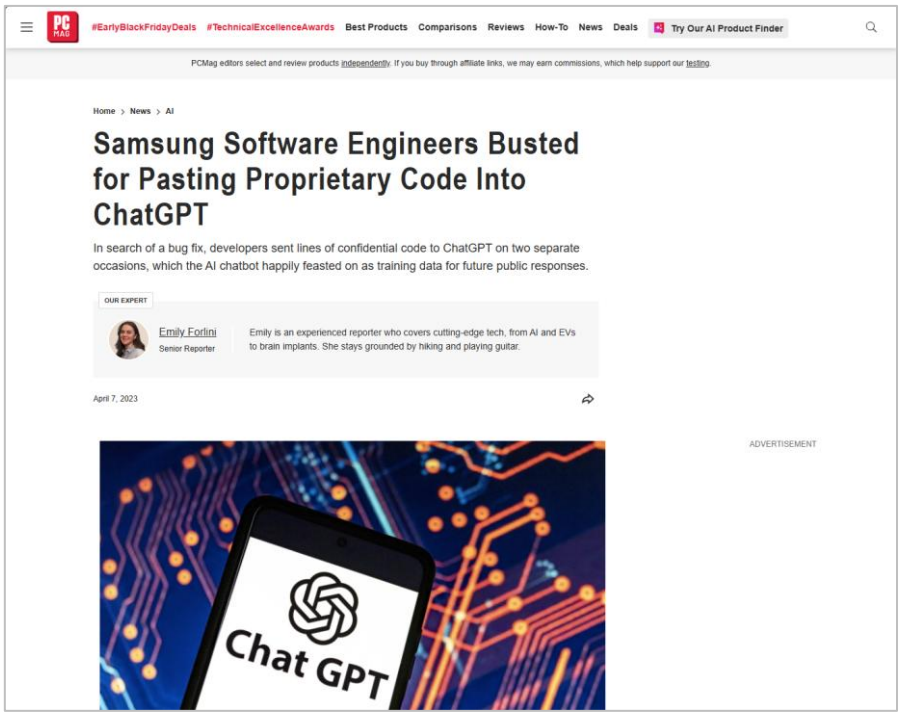

図 9 サムスン社従業員が機密情報を ChatGPT に流出させたとの報道[14]

また、シャドーAI に限った問題ではないが、AI が生成する内容には誤情報や偏りが含まれることにも注意が必要である。さらに、著作権や倫理的な問題も無視できず、AI が生成した文章や画像が第三者の権利を侵害している可能性もある。

このような情報が精査されないまま業務で活用されると、意思決定への悪影響、コンプライアンス違反などの問題により、経営上のリスクとなり得る。

2.4. 企業が取るべき対応

企業での安全な AI 利用にあたっては、公的機関が策定した以下のようなガイドラインが参考となる。

米国立標準技術研究所(NIST):「AI リスクマネジメントフレームワーク (AI RMF)」[15]

総務省および経済産業省:「AI 事業者ガイドライン」[16、17]

独立行政法人情報処理推進機構(IPA):「テキスト生成 AI の導入・運用ガイドライン」[18]

これらのガイドラインでは「シャドーAI」という言葉を直接使用していないものの、企業内での AI ツール利用について適切なガ

[14] 出典: PCMag『Samsung Software Engineers Busted for Pasting Proprietary Code Into ChatGPT』
https://www.pcmag.com/news/samsung-software-engineers-busted-for-pasting-proprietary-code-into-chatgpt

[15] 出典: NIST『AI Risk Management Framework』
https://www.nist.gov/itl/ai-risk-management-framework

[16] 出典: 総務省『「AI ネットワーク社会推進会議｜AI 事業者ガイドライン」掲載ページ』
https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02ryutsu20_04000019.html

[17] 出典: 経済産業省『AI 事業者ガイドライン』
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20240419_report.html

[18] 出典: IPA 独立行政法人 情報処理推進機構『テキスト生成 AI の導入・運用ガイドライン』
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/generative-ai-guideline.html

バナンス構築を求めており、結果としてシャドーAI によって生じるリスクへの対策を促す内容となっている。

具体的には、AI ツールの導入目的の明確化、リスク評価、社内ガイドラインの整備・継続的な見直し、従業員教育などの実施を推奨している。そして、各企業でこれらの推奨策が実施されることによって、AI の利点を活かしながらリスクを最小限に抑えることを目指している。AI ツールの安全な利用が積極的に推進されれば、シャドーAI の利用の抑制効果も期待できる。

また、AI ツールの選定にあたっては、入力データの学習無効化、利用履歴や出力結果の記録・確認など、企業利用を想定した、情報漏洩防止につながる機能が備わっているかを確認することも重要である。

2.5. まとめ

AI は今後さらに進化し、業務のあらゆる場面に浸透していくことが予想され、企業での利用を全面的に禁止すれば、シャドーAI が拡大する恐れすらある。IT 部門や情報セキュリティ部門は、AI の利用を過度に抑制するのではなく、業務現場との対話を通じて、実用性と安全性の両立を図っていくことが望ましい。そのバランスを見極めることが、これからの企業経営において重要な課題となる。

3. NIST のパスワードポリシーガイドライン更新

3.1. 概要

NIST(米国国立標準技術研究所)はデジタルアイデンティティのガイドラインの最新版である SP 800-63 の第 4 版(SP 800-63-4)を公開している[19]。オンラインサービスにおける本人確認や認証のための技術面・運用面の基準を示しており、第 3 版が公開された 2017 年以降のデジタル環境の変化に対応した内容となっている[20]。

同ガイドラインは米政府機関を対象としたものであるが、国際的なベンチマークとなっており、企業でのパスワード管理ポリシーなどの見直しにも影響を及ぼす可能性がある。

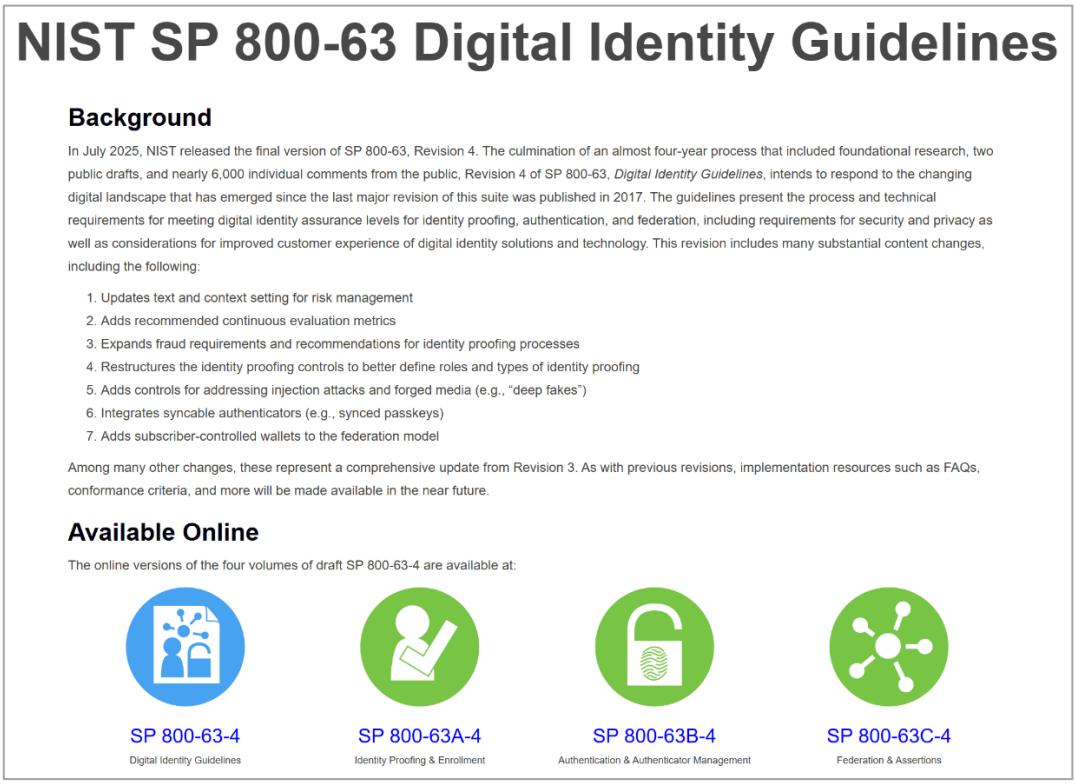

図 10 NIST による、SP 800-63 のページ

3.2. 「SP 800-63」とは

SP 800-63 は NIST が策定したデジタルアイデンティティに関するガイドラインである。オンラインサービスにおける本人確認や認証のための技術面・運用面の基準を示している。

初版は「電子認証に関するガイドライン」として 2004 年に公開され、以降、時代の変化を取り入れながら改訂を続けている[21]。2011 年に公開された SP 800-63-1 では、推奨レベルながら多要素認証についての要求事項が追加された。また、SP

[19] 出典: NIST『NIST SP 800-63 Digital Identity Guidelines』
https://pages.nist.gov/800-63-4/

[20] 出典: NIST『Let's get Digital! Updated Digital Identity Guidelines are Here!』
https://www.nist.gov/blogs/cybersecurity-insights/lets-get-digital-updated-digital-identity-guidelines-are-here

[21] 出典: NIST『Special Publication 800-63』
https://www.nist.gov/itl/applied-cybersecurity/special-publication-800-63

800-63-2 まで提言されていたパスワードの定期変更、パスワードの文字種を複数組み合わせるなどの施策は、多くの組織のパスワード管理ポリシーに組み込まれることとなった。

しかし、2017年に改訂されたSP 800-63-3で大きな見直しが行われ、パスワードの定期変更の強制が非推奨となったり、パスワードの複雑性よりも長さを重視したりする内容となった。合わせて、文書の構成も見直され、基本文書である SP 800-63 でガイドライン全体の概要を説明し、本人確認と登録プロセスに関する SP 800-63A、認証プロセスに関する SP 800-63B、システム間の ID 連携に関する SP 800-63C の 3 つの分冊で各論の詳細を説明する形式となった。

2025 年 7 月、最新版である SP 800-63-4 が正式公開された[22]。

同ガイドラインは米政府機関を対象としたものであるが、世界各国で参照されており、9 月 30 日にデジタル庁から刊行された「行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン」にも反映されている[23]。

3.3. パスワードポリシーガイドラインの変更点

SP 800-63-4 のうち認証とライフサイクル管理に関するドキュメントの SP 800-63**B**-4 は、多要素認証のさらなる強化等が前の版を踏まえ刷新された。その中でパスワードポリシーガイドラインも最新化されたため、注目されている。

【前版の SP 800-63B-3 が示した路線】

2017 年 6 月に発表された前の版である **SP 800-63B-3** では、認証について新しい考え方が多く反映された。まず、守るべき情報の重要性、深刻度によって、認証の強度を分けるべきという考えが示され、重要な情報についてはパスワード認証に加え多要素認証を加えることを推奨した。

さらに、それまでの反省に基づきパスワードポリシーに要求される事項が大きく変更された。これは、従来のパスワード定期変更や文字種に記号を混ぜるといった複雑な要求事項は、規則性のあるパスワードを作成する、覚えにくいことからメモに書き留める、といったセキュリティを低下させる行動を促していたという、米国連邦政府職員への調査結果[24]等の分析に基づいたものであった。

変更点として特に、覚えやすい**「パスフレーズ」**の使用が推奨されるようになったことが挙げられる。パスフレーズ(例：sunwalkraindrive)は、脳内で浮かぶイメージを活用して単語を列挙する手法(図 11)により、ユーザーが思い出しやすい長いフレーズを認証に使用してもらうことを主眼としている。これに伴い、パスフレーズを覚えにくくする等の要因となるパスワード定期変更や文字種に記号を混ぜるといった従来の要求事項は、「すべきではない」ということが示された。併せて、認証側（システム管理者など）でブロックリストと照合して、脆弱なパスワードを設定できないようにする等、弱いパスワードを使わせない仕組みを導入することが推奨された[25]。

---

[22] 出典: NIST『NIST SP 800-63 Digital Identity Guidelines』
https://pages.nist.gov/800-63-4/

[23] 出典: デジタル庁『行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン』
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/12cb1a6c/20250930_resources_standard_guideline_identityverification_01.pdf

[24] 出典: NIST『NISTIR 7991 United States Federal Employees' Password Management Behaviors – a Department of Commerce Case Study』
https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7991.pdf

[25] 出典: GMO トラスト・ログイン ブログ『世界の電子認証基準が変わる：NIST SP800-63-3 を読み解く』
https://blog.trustlogin.com/articles/2017/20171130

図 11 パスフレーズ導入について啓発する図(NIST) [26]

【より踏み込んだ SP 800-63B-4】

改訂により SP800-63B-4 は、SP 800-63B-3 から要求基準がより踏みこまれたものになった。

まず、パスワードの最小長が見直され、多要素認証と組み合わせる場合は改訂前と同じ 8 文字以上、パスワードのみで認証する場合は 15 文字以上と定義された。多要素認証の利用を基本とし、パスワード単体での認証は例外的なケースとして扱い、その場合は文字数を増やすことでパスフレーズの利用によるセキュリティ強度の確保を促している。さらに、パスワードの定期変更や複数文字種の強制といった要求を「すべきではない」の非推奨の表現から「してはならない」の禁止の表現へと明確化し、長く覚えやすいパスフレーズを使用する際の障壁を廃止するよう要求を強めている。[27,28]

項目	SP 800-63B-3	SP 800-63B-4
パスワードの最小長	8 文字以上	多要素認証と組み合わせる場合: **8 文字以上** パスワードのみで認証する場合: **15 文字以上**
パスワードの定期変更	パスワードを周期的に変更することを要求すべきではない。	パスワードを周期的に変更することを**要求してはならない**。
パスワード構成ルール	複数の文字種を強制したり、同じ文字の繰り返しを禁止したりするルールを課すべきではない。	複数の文字種を強制するルールを**課してはならない**。

表 2 SP 800-63B-4 のパスワードポリシーに関する主な変更点(前版 SP 800-63B-3 との比較)

3.4. まとめ

長年の慣習等により複雑なパスワードポリシーによる運用が浸透している。その一方で多要素認証が普及し、パスワード認

[26] 出典: NIST『Easy Ways to Build a Better P@$5w0rd』
https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd

[27] 出典: NIST『SP 800-63B A. Strength of Passwords』
https://pages.nist.gov/800-63-4/sp800-63b/passwords/

[28] 出典: Security Boulevard『NIST SP 800-63B Rev. 4 Password Updates』
https://securityboulevard.com/2025/09/nist-sp-800-63b-rev-4-password-updates/

証のみに頼ったセキュリティは過去のものになりつつある。

SP 800-63B-4 のパスワードポリシーガイドラインは、パスフレーズの推奨といった、セキュリティとユーザビリティの両立を図った現在のパスワード認証のあるべきかたちを示しているといえる。2017 年発表の SP 800-63B-3 以降、パスワード定期変更や文字種に記号を混ぜるといった従来の要求事項は求めるべきではないとされていたのがいよいよ禁止となり、多要素認証を用いないパスワードのみでの認証は例外的な扱いとなり、より長いパスワード長が要求されるようになった。今回の改訂を機に、守るべき情報の重要性や深刻度、多要素認証の実装と照らし合わせながら、自社のパスワードポリシーを見直すことを推奨する。

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
プロフェッショナルサービス部 OSINT モニタリングチーム
メールアドレス: nsj-co-osint-monitoring@security.ntt