MS&AD InterRisk Report

No.26-040

2026.11.02

サイバーセキュリティニュース ＜2026 年度第 2 号＞

本誌では、サイバーセキュリティに関する国内外の最新動向を踏まえ、重要なトピックスを四半期ごとにわかりやすく紹介します。
※当社オフィシャルサイト「RM NAVI」に掲載したコラム記事を再構成し、取りまとめたものです。

サイバーリスクによる財務影響の可視化が求められる時代へ
― 従来の「定性評価」から「定量評価」へのアップデート ―

2026 年 8 月 31 日掲載

1. サイバーリスクが経営課題となる背景

昨今、DX の推進や生成 AI の普及により、社会全体の利便性は飛躍的に向上している。その一方で、デジタル基盤への依存度の高まりやサプライチェーンの複雑化に伴い、サイバーリスクは企業経営に重大な影響を及ぼす喫緊の課題となっている。特に近年は、ランサムウェアをはじめとするサイバー攻撃により、単なる情報漏えいにとどまらず、事業停止や多額の損失につながる事案が相次いでいる。

2. セキュリティ投資に求められる定量評価

このような状況下では、あらゆるサイバー攻撃に備えるため、継続的なセキュリティ対策への投資が不可欠である。ただし、投資可能な予算には限りがあるため、対策には優先順位を設け、計画的に投資を進める必要がある。したがって、経営層がセキュリティ投資を判断するうえで求められるのは、単に「リスクがある」という定性的な情報ではなく、「どの程度の財務影響が想定されるのか」という定量的な情報である。

しかし、多くの企業では「IT 資産の管理」や「セキュリティ対策の実施有無」といった定性的な評価が中心である。PwC が 2025 年度に 77 カ国・7 地域の経営層 4,042 名を対象に実施したサイバーリスク調査では、サイバーリスクの財務影響を相当程度把握している企業は、全体の 15%にとどまった。(※1)「サイバー攻撃を受けた場合、自社はいくらの損失を被るのか」といったサイバーリスクを金額換算し、定量的に把握できている企業は、依然として少ないのが実情である。

3. CRQ（サイバーリスク定量化）の台頭

そこで近年、欧米企業を中心に導入が進んでいるのが、CRQ（Cyber Risk Quantification：サイバーリスク定量化）である。CRQ は、サイバー攻撃による情報漏えいやシステム停止などの損失を金額として可視化し、セキュリティ投資やリスク許容度の設定、保険設計など、経営層の意思決定を後押しする手法として注目されている。また、Market Intelo 社の調査によると世界の CRQ 市場は、2025 年に 28 億ドルと評価され、2026 年から 2034 年にかけて年平均成長率 14.7%で成長し、将来的に 96 億ドルに達すると見込まれている（※2)。CRQ への関心の高まりは、今後さらに加速することが予想される。

4. サイバーリスクを金額でとらえる重要性

サイバーリスクを金額としてとらえ、経営の意思決定に反映させるアプローチは、国内外でその重要性を一層高めており、世界的に新たなスタンダードとなりつつある。
サイバーリスクを金額で可視化し、セキュリティ投資の優先順位を明確にすることは、限られた予算の中で合理的な意思決定を行ううえで有効である。各対策の損失回避効果を見極め、対策費用と想定損失のバランスを踏まえることで、投資先と投資額を判断できる。結果として、場当たり的な対応を避け、戦略的な投資判断につながる。

5. 火災や自然災害のリスク管理に学ぶ定量評価

この考え方自体は新しいものではない。企業はこれまでも火災リスクや水災、地震などの自然災害リスクに対して予想最大損失額を算出し、設備投資や事業継続計画の策定、保険設計の判断に活用してきた。つまり、「リスクを金額で把握し、経営判断に活用する」という考え方は、すでに他のリスク管理分野では一般的なのである。

6. CRQ が求められる時代へ

サイバーリスクもまた、火災や自然災害と同様に、財務影響を見据えて管理すべき経営リスクである。今後は、定性的な評価にとどまらず、定量的な把握を前提としたリスクマネジメントへ移行することが、より一層求められていくだろう。

1) PwC Japan 社「Digital Trust Insights 2025 : CxO と CISO の連携が、複雑化するデジタル法規制によって生じるギャップを埋める」〈https://www.pwc.com/jp/ja/knowledge/thoughtleadership/digital-trust-insights2025.html〉（最終アクセス 2026 年 8 月 18 日）
2) Market Intelo 社「Cyber Risk Quantification Market Research Report 2034」〈https://marketintelo.com/report/cyber-risk-quantification-market〉（最終アクセス 2026 年 8 月 18 日）

生成 AI の悪用でどう変わった？
高度化するサイバー詐欺と今すぐできる対策フロンティア AI が変えるサイバーセキュリティの前提

2026 年 9 月 24 日掲載

1. はじめに

近年、生成 AI 技術は目覚ましい進歩を遂げているが、AI（人工知能）そのものの歴史は長い。1950 年、イギリスの数学者アラン・チューリングは、「機械が人間と見分けがつかないほど自然に対話できるなら、その機械は人間的である」という考え方を示した。これは後に「チューリングテスト」として知られるようになり、AI の知的能力を考えるうえでの象徴的な概念の一つである。その後、1980 年代には専門知識をルールとして扱う AI が登場し、1990 年代以降はコンピューターの性能向上を背景に、機械学習やディープラーニングが急速に発展した。

2022 年には生成 AI「ChatGPT」が一般公開され、文章、画像、音声などを高い精度で生成できるようになった。2025 年 4 月には、ChatGPT のモデルの一つ「GPT-4.5」が前述のチューリングテストに合格したとする報告もみられた。チューリングの定義ではすでに「人間的」な能力を持つ生成 AI は、文書作成、翻訳、要約、調査補助など幅広い用途で利便性をもたらしている一方、その高い能力は、すでにサイバー詐欺に悪用されつつある。 本稿では、従来の代表的なサイバー詐欺の手口を整理したうえで、生成 AI によってそれらがどのように高度化したのかを示し、個人や組織が今すぐできる対策を紹介する。

2. これまでの手口

2.1. フィッシングメール

フィッシングとは、銀行、EC サイト、宅配便業者、通信事業者などを装ったメールや SMS によって受信者をだまし、偽のログイン画面や入力フォームへ誘導して、ID・パスワード、クレジットカード情報などを盗み取る手口である。

「アカウント確認が必要です」「不正ログインを検知しました」「支払い方法に問題があります」「本日が最終期限です」といった文言で不安や焦りをあおり、受信者に即時の行動を促す文面が典型的である。

従来のフィッシングメールには、日本語が不自然なものや、レイアウトや差出人表示に違和感があるものが見られた。そのため、「文面を注意深く確認しましょう」という対策に一定の有効性があった。

2.2. 標的型メール

標的型メールとは、不特定多数ではなく、特定の企業や組織、部署、担当者を狙って送られる悪意のあるメールである。添付ファイルを開かせたり、URL をクリックさせたりして、マルウェア感染や認証情報窃取につなげることを目的とする。

件名や本文は、実際の業務に関係しそうな内容に偽装されることが多く、「請求書」「会議資料」「採用応募書類」「年末調整」などが典型例である。

従来は、ビジネス文書としては不自然な言い回しや文面の粗さ、本人の文体との違い、業務実態と微妙にずれた内容がみられることがあった。

2.3. ビジネスメール詐欺（BEC）

ビジネスメール詐欺とは、攻撃者が取引先、委託先などになりすまし、送金口座の変更や請求書の差し替えなどを指示することで金銭をだまし取ろうとする手口である。特に経理、財務など、金銭の支払いに直接かかわる部門が狙われやすく、メールのみで業務が進んでしまう運用の隙を

突いて被害を引き起こす。

攻撃者は事前にメールサーバーに侵入し、実際の担当者間のやり取りを基にした巧妙なメールを作成するなど、非常に巧妙で多額の被害が報告されている。それでも、言葉遣いの違和感、普段と異なる文体、差出人メールアドレスのわずかな違いなどが、詐欺を見抜く手がかりになることがあった。

3. 生成 AI によってサイバー詐欺の手口はどのように高度化したか

3.1. 攻撃に用いられる文面が自然になった

生成 AI のもっともわかりやすい影響としては、攻撃に用いられるメールや SNS などにおける文章の不自然さが減り、読み手に違和感を抱かせない、自然な文面となったことが挙げられる。明らかな誤字脱字や不自然な言い回し（例：「お客さんの口座が…」）が減ったことで、文面のみからサイバー詐欺を見抜くことがより困難になっている。

3.2. ターゲットに合わせた文面が作られるようになった

生成 AI は、相手の立場や業務内容に応じて文面を作り分けることを得意とする。企業サイト、SNS、ニュースリリースなど、インターネット上の公開情報を集めることで、部署や担当業務に合わせたもっともらしいメールを作成できる。

その結果、「誰にでも当てはまる一斉送信メール」ではなく、心理的な警戒をすり抜けやすい「自分宛てに書かれたように見えるメール」が増えている。

3.3. 大量送信と個別最適化を両立できるようになった

従来、高度にターゲットに最適化された巧妙な詐欺メールの作成には相応の事前調査が必要であり、攻撃者にとってコストと手間が必要であった。生成 AI を使えば、件名、本文、署名、返信文まで含め、相手ごとに少しずつ内容を変えて最適化した巧妙な文面を、短時間で量産でき、攻撃の成功率が高まりやすい。

4. なぜ生成 AI によるサイバー詐欺は危険なのか

生成 AI によってサイバー詐欺の危険性が増している最大の理由は、これまで見抜く手がかりとされてきた、ある種の「粗さ」が失われていることにある。従来は、攻撃者が自然な日本語を作成することが困難であったことが、防御壁として機能していた。（表 1）

表 1：フィッシングメールの文面例（筆者作成）
（左：従来のフィッシングメール／右：生成 AI によるフィッシングメール）

件名: アカウント確認必要のお知らせ 本文: お客様、こんにちは。 私たちはあなたのアカウントに異常活動を見つけました。安全のため、情報確認を必要です。もし確認しない場合、サービスは 24 時間で停止されるかもしれません。 ご不便をかけて申し訳ありませんが早く対応をお願いします。 ありがとうございます。	件名: 【重要】アカウント情報ご確認のお願い 本文: 平素よりご利用いただきありがとうございます。 お客様のアカウントに通常と異なる利用が確認されたため、安全確保の観点からご本人様による確認をお願いしております。 お手数をおかけいたしますが、内容をご確認のうえ、必要なお手続きをお願いいたします。 なお、一定期間ご対応がない場合、一部機能のご利用を制限させていただくことがあります。 ご不明な点がございましたら、下記窓口までお問い合わせください。

生成 AI はターゲットに合わせて文面を作り分けることも得意であり、結果として「自分宛てに書かれたように見える」「自然で整った日本語」が生成され、受信者の心理的な警戒をすり抜けやすいと考えられる。

サイバー詐欺の本質は以前から変わっておらず、不安や焦り、業務を通じた信頼関係などを利用して確認行動を省略させようとする点にあると考えられる。生成 AI は、その心理的な誘導をより自然かつ効率的にしていると考えられる。

5. 今すぐできる対策なぜ生成 AI によるサイバー詐欺は危険なのか

生成 AI の普及によって、フィッシングメール、標的型メール、ビジネスメール詐欺などは、以前よりも自然で精巧になり、見抜きにくくなっている。特に、これまで判断材料となっていた不自然な日本語、文面の粗さに頼った見分け方は通用しにくくなっている。

しかし、サイバー詐欺対策の基本は変わっていない。具体的には、次のような対策が有効である。

- メールや SMS に記載された URL は安易に開かない
- ログインや支払い確認が必要と書かれていても、まずは疑い、記載されたリンク先に直接アクセスしない
- サイトへのログインは、公式アプリやブックマークした正規サイトから行う
- メールに記載された URL からのアクセスは避ける
- 送金や口座変更など重要な依頼は、メールだけで完結させない
- 特に業務上の重要なやり取りは、電話や対面など別経路で確認する

そして、少しでも疑わしいと感じたときは、あわてず、一人で判断せず、最も安全と認められる方法を考えて行動することが重要である。見かけの「本物らしさ」に惑わされず、確認を前提に行動する習慣を、個人と組織の双方で定着させることで、サイバー詐欺の被害を未然に防ぐことができる。

データ保有の妥当性が問われる時代に
― 相次ぐ情報漏えい事案から見る不要データのリスク ―

2026 年 10 月 27 日掲載

1. はじめに

2026 年秋、サイバー攻撃被害や情報漏えいに関する公表が相次ぎ、個人情報保護委員会、独立行政法人情報処理推進機構（IPA）、JPCERT／CC、金融庁、警察庁、国家サイバー統括室などが短期間に注意喚起を発表した。こうした動きを受け、「公的機関から新たなサイバーセキュリティ対策が求められているのではないか」と受け止める向きもあるかもしれない。

しかし、各機関の注意喚起の内容を見ると、基本的な考え方が大きく変わったわけではないことが分かる。

多要素認証、脆弱性管理、最小権限、ログ確認、委託先管理、経営関与といった論点が注意喚起の中に含まれていたが、これらの内容は従来求められてきた内容と大きな違いはない。たとえば、経済産業省および IPA の「サイバーセキュリティ経営ガイドライン Ver3.0」では、サイバーセキュリティを経営課題として位置付け、サプライチェーンを含めた委託先管理や、経営者のリーダーシップの必要性が以前から示されている（※1）。金融庁のガイドラインでも、復旧訓練、外部委託管理、認証管理、経営陣の関与などは以前から論点となっていた（※2）。

今回、特に強調されたのは、侵入を防ぐことに加え、「不要なデータを保有しないこと」まで含めてサイバーリスクを管理せよというメッセージである。

2. 公的機関の注意喚起の内容

今回の一連の注意喚起には、複数の公的機関がそれぞれの所管・観点から同じ問題を扱っているという特徴がある。個人情報保護委員会は個人情報保護の観点から、IPA は企業のセキュリティ対策と経営責任の観点から、JPCERT／CC は攻撃手法と初動対応の観点から、金融庁は金融サービスの信頼性維持と犯罪防止の観点から、警察庁は犯罪利用と二次被害防止の観点から注意喚起を行っている（※3,※4,※5,※6）。

各公表内容においては、パッチ適用や認証強化といった従来型の基本対策が引き続き重視される一方で、次の三点が特に強く打ち出されている。

第一に、攻撃対象の範囲の広さである。

外部公開 Web システムだけではなく、クラウド、VPN（通信を暗号化し、公衆回線において安全性の高い通信環境を実現するための技術）、API（アプリケーション間のデータ共有を可能にする技術）、業務用アプリケーション、従業員向けシステムなども含め、保有する資産を網羅的に把握することが求められている（※4,※5）。

第二に、漏えい後の二次被害まで含めて評価する姿勢が強調されている。

個人情報保護委員会は、件数だけではなく、機微性、財産的被害の恐れ、詐欺に利用される恐れといった観点を示した（※3）。金融庁は、本人確認書類画像の漏えいを踏まえ、各種取引申し込み時の本人確認強化を求めている（※6）。

第三に、データ保有そのものもリスク管理の対象となっていることである。

個人情報保護委員会は、利用する必要がなくなった個人データの消去が徹底されないことで、漏えい事案がより深刻になった例に接しているとして、保有の必要性の再確認を求めた（※3）。IPA も、保有情報を必要最小限にするよう促し（※4）、JPCERT／CC も、保存期間を過ぎたデータ

や利用目的を終えたデータを残さないよう推奨している（※5）。

以上を踏まえると、「どう守るか」だけでなく、「なぜそのデータを持つ必要があるのか」「なぜそこにデータを保管しているのか」「なぜ今そのデータが残っているのか」まで含めて説明責任を果たせるかが問われている。

3. 「不要データの管理」というサイバーリスク対策

2026 年秋に公表された情報漏えい事案には、漏えい時の本人への影響が大きい情報が含まれていた。例えば、顔写真付き公的身分証明書画像や健康診断結果などが漏えいした事案、運転免許証画像等の本人確認書類が対象に含まれていた事案がある。

これらの事案が示しているのは、同じ個人情報漏えいでも、含まれるデータによってリスクの性質が大きく異なるということである。氏名とメールアドレスの漏えいと、本人確認書類画像や健康情報の漏えいとでは、想定される二次被害が異なる。後者は、なりすまし、本人確認突破、精緻な詐欺、長期的なプライバシー侵害につながる恐れがある。

ここで企業が認識すべきなのは、漏えいリスクの大きさは、漏えい件数だけでは判断できないということである。

少数の漏えいであっても、本人確認に利用可能な画像情報、健康情報、番号情報などが組み合わされていれば、本人への影響は長期かつ深刻になりうる。したがって、経営として問うべきは、「データ保有の必要性を説明できるか」である。

どれほど防御を強化しても、侵入可能性をゼロにすることはできない。そういった前提に立つと、事業上の合理的な理由なく高リスクデータを保有し続けること自体が、経営として追加のリスクを抱え込むことになる。

4. 企業が見直すべき三項目

以上を踏まえ、保有するデータの取り扱いについて、企業は少なくとも三点を見直す必要がある。

第一に、高リスクデータの所在把握である。本人確認書類画像、マイナンバー、健康情報、金融関連情報などの、漏えい時の影響が大きいデータが、どのシステムに、何件、どの目的で保管されているかを把握しなければ、影響評価も削除判断もできない。

第二に、保有理由の明確化である。法令上の保存義務、契約履行上の必要性、単なる慣行を切り分けて整理し、説明できないものは削除候補として扱う必要がある。

第三に、削除を確実に行う仕組みの整備である。保存期間、削除責任者、委託先を含めた削除確認まで含めて設計しなければ、「削除方針」は実務において形骸化してしまう可能性がある。

この三点は、システム部門だけで完結するものではなく、法務、個人情報保護、業務部門、調達部門、リスクマネジメント部門が関与し、最終的には経営が優先順位を決めて取り組むべき経営課題である。サイバー攻撃被害や情報漏えいが相次ぐ中、攻撃を前提とした対策設計が求められており、不要データを残さないことはその対策の中に含める必要がある。

1) 経済産業省・IPA「サイバーセキュリティ経営ガイドライン Ver3.0」〈https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf〉（最終アクセス 2026 年 10 月 16 日）

2) 金融庁「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」〈https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf〉（最終アクセス 2026 年 10 月 16 日）
3) 個人情報保護委員会「大規模な漏えい等事案を踏まえた対応について（注意喚起）」〈https://www.ppc.go.jp/files/pdf/261007_houdou.pdf〉（最終アクセス 2026 年 10 月 16 日）
4) IPA「不正アクセスによる漏えい等の事案を踏まえ、速やかに実施すべき対策等について」〈https://www.ipa.go.jp/security/security-alert/2026/alert20261009.html〉（最終アクセス 2026 年 10 月 16 日）
5) JPCERT/CC「直近で相次いでいる国内組織における不正アクセスに関する注意喚起」〈https://www.jpcert.or.jp/at/2026/at260030.html〉（最終アクセス 2026 年 10 月 16 日）
6) 金融庁「現下の情勢を踏まえたサイバーセキュリティ対策の強化と各種取引申込等における対応について」〈https://www.fsa.go.jp/news/r8/sonota/20261009/20261009.html〉（最終アクセス 2026 年 10 月 16 日）

編集者コメント

本誌コラムにも記載されているように、国内組織の情報漏えい事案が相次いでいる。被害組織の中には原因を公表していないところも多いが、関係機関の分析では、Android アプリの解析を通じたバックエンド API への攻撃（A2B 攻撃）（※1）や、ソフトウェアの既知の脆弱性を悪用した攻撃（※2）などが原因と考えられている。

なお、直近（2026 年 10 月 22 日時点）でも、Web サイトで使用されている PHP に危険な脆弱性が報告され（※3）、多くの組織ではこの脆弱性対応のために Web サイトを一時停止するなどの緊急対応が行われている。また、高市首相も X に注意喚起を投稿しており（※4）、危険性や影響の大きさがうかがえる。

さらに、国内組織で情報漏えい事案が多発している要因の一つとして、AI ペネトレーションテストツールである「ARTEX」が使用されているとの報告もあり（※5）、サイバー攻撃の高速化・大規模化が進んでいる。

防御側としては、引き続き脆弱性が報告された場合は迅速にセキュリティパッチを適用するなど基本的な対策を取りつつ、侵入された場合でも迅速に検知でき、被害を最小限に抑える体制が必要である。

1) NICT「【注意喚起】相次ぐ情報漏えい、その原因の一つは「アプリ解析からのサーバ攻撃」〈https://www.nict.go.jp/press/2026/10/13-1.html〉（最終アクセス 2026 年 10 月 22 日）
2) JPCERT/CC「直近で相次いでいる国内組織における不正アクセスに関する注意喚起」<https://www.jpcert.or.jp/at/2026/at260030.html〉（最終アクセス 2026 年 10 月 22 日）
3) IPA「PHP の脆弱性対策について（CVE-2026-109618、CVE-2026-109619：PHP2shell）」〈https://www.ipa.go.jp/security/security-alert/2026/alert20261022.html〉（最終アクセス 2026 年 10 月 22 日）
4) 高市早苗 公式アカウント〈https://x.com/takaichi_sanae/status/2112890642590564386〉（最終アクセス 2026 年 10 月 22 日）
5) ビジネス＋IT「GMO 系、日本企業狙う不正アクセスの攻撃元に AI ツール「ARTEX」確認　標的は約 20 社」〈https://www.sbbit.jp/article/cont1/187590〉（最終アクセス 2026 年 10 月 22 日）

ＭＳ＆ＡＤインターリスク総研株式会社は、ＭＳ＆ＡＤインシュアランスグループのリスク関連サービス事業会社として、リスクマネジメントに関するコンサルティングおよび広範な分野での調査研究を行っています。本誌を編集している以下のグループでは、サステナビリティ関連のコンサルティング・セミナー等のサービスを提供しています。
ＭＳ＆ＡＤインターリスク総研サービスに関するお問い合わせ・お申し込み等は、下記のお問い合わせ先、または、お近くの三井住友海上、あいおいニッセイ同和損保の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研㈱
リスクマネジメント第三部　サイバーリスクグループ
cyberrisk_irric@ms-ad-hd.com
https://www.irric.co.jp/

主な担当領域は以下のとおりです。
＜サイバーリスク管理＞
- ◆ 現状評価・課題分析
- ◆ 体制構築
- ◆ リスクアセスメント
- ◆ 有価証券報告書における開示の充実化
- ◆ サイバーBCP策定支援
- ◆ サイバーインシデント時の情報開示・広報
- ◆ サイバーインシデント演習
- ◆ サイバーインシデント初動対応マニュアル策定支援
- ◆ 担当領域に係る研修　等

本誌は、マスメディア報道など公開されている情報に基づいて作成しております。
また、本誌は、読者の方々に対して企業のリスクマネジメント活動等に役立てていただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。

不許複製／Copyright ＭＳ＆ＡＤインターリスク総研 2026

MS&AD インターリスク総研は、2024 年 4 月、これまでのホームページを刷新し、リスクに強い組織づくりをサポートするプラットフォーム「RM NAVI（リスクマネジメント ナビ）」をリリースしました。「RM NAVI」は、MS&AD インターリスク総研の知見をフル活用して、情報提供から実践までをトータルサポート。コンサルタントの豊富な経験と、最先端のデジタルサービスで、リスクに強い組織づくりを支えます。
あなたに寄り添い、最適な答えへと導く、リスクマネジメントの羅針盤です。

