2026 年 4 月 22 日

レポート

# 情報セキュリティ 10 大脅威の変遷とこれからの対応

コンサルティング事業本部　デジタルイノベーションビジネスユニット
デジタルビジネスコンサルティング部
シニアマネージャー　谷口智史

2026 年 1 月、独立行政法人情報処理推進機構（IPA）は「情報セキュリティ 10 大脅威 2026」を発表した。「情報セキュリティ 10 大脅威」は、前年に発生した情報セキュリティの事故や攻撃の状況などを対象に、情報セキュリティ分野の研究者、企業の実務担当者などによる審議・投票を経て決定する。情報セキュリティをめぐる脅威の傾向を把握し、対策を検討できる貴重な資料であり、また、脅威を「組織」と「個人」に分けて示している点も特徴的である。

本レポートでは、「情報セキュリティ 10 大脅威」の変遷を踏まえた上で、情報セキュリティ対策を考える上で有用なヒントとなる「情報セキュリティ 10 大脅威 2026 [組織]」に着目し、組織が講じるべきアクションを考察する。


（お問い合わせ）コーポレート・コミュニケーション室　e-mail：info@murc.jp

## 1. 2026 年の 10 大脅威

2026 年の組織における 10 大脅威は図表 1 の通りである。2026 年の 10 大脅威は、2 件を除き、6 回目以上連続で選出された脅威で構成されている。

最近登場した 2 件は、初選出の「3 位　AI の利用をめぐるセキュリティリスク」と 2 回目選出の「6 位　地政学的リスクに起因するサイバー攻撃（情報戦を含む）」であった。この 2 つのリスクは、地政学的緊張が高まる世界情勢と、AI が急激に進化・普及する経済・社会環境下では、脅威が掛け合わされ大きくなるおそれがある。

**図表 1　情報セキュリティ 10 大脅威 2026 [組織]**

| 順位 | 「組織」向け脅威 | 初選出年 | 10 大脅威での取り扱い（2016 年以降） |
|---|---|---|---|
| 1 | ランサム攻撃による被害 | 2016 年 | 11 年連続 11 回目 |
| 2 | サプライチェーンや委託先を狙った攻撃 | 2019 年 | 8 年連続 8 回目 |
| 3 | AI の利用をめぐるサイバーリスク | 2026 年 | 初選出 |
| 4 | システムの脆弱性を悪用した攻撃 | 2016 年 | 6 年連続 9 回目 |
| 5 | 機密情報を狙った標的型攻撃 | 2016 年 | 11 年連続 11 回目 |
| 6 | 地政学的リスクに起因するサイバー攻撃（情報戦を含む） | 2025 年 | 2 年連続 2 回目 |
| 7 | 内部不正による情報漏えい等 | 2016 年 | 11 年連続 11 回目 |
| 8 | リモートワーク等の環境や仕組みを狙った攻撃 | 2021 年 | 6 年連続 6 回目 |
| 9 | DDoS 攻撃（分散型サービス妨害攻撃） | 2016 年 | 2 年連続 7 回目 |
| 10 | ビジネスメール詐欺 | 2018 年 | 9 年連続 9 回目 |

（出所）　独立行政法人情報処理推進機構(IPA)「情報セキュリティ 10 大脅威 2026 [組織]」(2026)を基に当社作成。赤字は当社が注目した項目である

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

## 2. 10 大脅威の傾向

過去 5 年間の 10 大脅威を、被害範囲や攻撃対象などの視点で分類した結果を図表 2 に示した。被害範囲に関しては、以前は自社のみを意識していれば事足りていた。しかし、2019 年に「サプライチェーンや委託先を狙った攻撃」が選出され、2025 年には「地政学的リスクに起因するサイバー攻撃」がランクインして一気に国家レベルへと範囲が拡大した。昨今の国際情勢を鑑みるに、地政学的リスクは改善する兆しは見えず、組織にとって潜在的かつ深刻な脅威が残ると思われる。

攻撃対象は、情報技術の進歩と普及に伴って多様化し、それに合わせた対策も進展している。その中でもいまだに十分な対策が難しいのが「ランサム攻撃による被害」である。2016 年に初登場して以降、1 位を譲っていない。この背景には、ランサム攻撃は攻撃者にとって高額の身代金が入り高収益であること、対策が進んでいない委託先から攻撃するサプライチェーン攻撃が増加していること、攻撃手法の高度化と分業化が進んでいることがある。当面、勢いは衰えないと思われる。

一方、「AI の利用をめぐるサイバーリスク」は 2026 年にはじめて登場した。今後、企業活動や情報システムにおける AI の重要性は、ますます高まっていくことが予想される。さらに、AI 自体が進化すると AI を活用した攻撃も進化すると考えられるため、長期にわたって上位にとどまり、脅威の「常連」となると思われる。

図表 2　情報セキュリティ 10 大脅威 [組織]の変遷

| 視点 | 対象の変遷 | 10 大脅威（順位は 2026 年版と初選出年） |
|---|---|---|
| 1．被害範囲 | 国家<br>↑<br>委託先・供給連鎖<br>↑<br>自社 | **地政学的リスクに起因するサイバー攻撃（6 位。初選出 2025 年）**<br>↑<br>**サプライチェーンや委託先を狙った攻撃（2 位。初選出 2019 年）**<br>↑<br>記載なし |
| 2．攻撃対象 | AI<br>↑<br>リモートワーク<br>↑<br>↑<br>基幹系システム<br>↑<br>ビジネスメール<br>↑<br>OS・アプリケーション<br>内部不正者<br>ウェブシステム | **AI の利用をめぐるサイバーリスク（3 位。初選出 2026 年）**<br>↑<br>リモートワーク等の環境や仕組みを狙った攻撃（8 位。初選出 2021 年）<br>修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）（2026 年版は選外。初選出 2022 年）<br>↑<br>予期せぬ IT 基盤の障害に伴う業務停止（2026 年版は選外。初選出 2022 年）<br><br>ビジネスメール詐欺（10 位。初選出 2018 年）<br>↑<br>**ランサム攻撃による被害（1 位。初選出 2016 年）**<br>システムの脆弱性を悪用した攻撃（4 位。初選出 2016 年）<br>機密情報を狙った標的型攻撃（5 位。初選出 2016 年）<br>内部不正による情報漏えい等（7 位。初選出 2016 年）<br>DDoS 攻撃（分散型サービス妨害攻撃）（9 位。初選出 2016 年） |

（出所）IPA 独立行政法人情報処理推進機構ウェブサイト「情報セキュリティ 10 大脅威」を基に当社作成

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

（注）過去 5 年間（2022～2026 年分）を用いて作成

## 3. 今後の脅威の変化予測

10 大脅威の傾向を踏まえて、今後の脅威の変化を予測する。特に注目したい脅威は「3 位 AI の利用をめぐるサイバーリスク」と「6 位 地政学的リスクに起因するサイバー攻撃」である。例を挙げると、イランへの米国の攻撃に際しては、イランが米国の IT 企業への攻撃を発表した。日本は、米国企業のデジタルインフラへの依存度が高い。そのため、地政学リスクが高まる局面では、「地政学×AI」の掛け合わせで、日本国内のリスクもさらに高まる可能性がある。

### (1) 地政学的リスクに起因するサイバー攻撃の影響

今やサイバー空間は「新たな戦場」とも表現できる。国家やその支援を受けた攻撃者は、潤沢な資金と軍事レベルに匹敵するような高度で組織的な技術力で、企業や政府、社会インフラに攻撃を仕掛けている。さらに近年、国際情勢の不安定化に伴い、地政学的リスクを背景にしたサイバー攻撃の脅威は急激に存在感を増している（図表 3）。これらは有事の際に攻撃が始まるのみではなく、有事発生時を見越して、あらかじめ仕掛けられる場合がある。そのため、気づいた場合には手遅れとなる事態も想定される。

世界各国では、中国製の機器が重要インフラ（通信、エネルギー、交通、行政など）に広範囲で採用されているが、米中対立が厳しさを増す中、日米欧を中心として、セキュリティ上の深刻なリスクとして警戒されている。台湾有事の際には日本もサイバー攻撃を受けるおそれがあり、潜在的な脅威は小さくない。

また、ウクライナ戦争では、侵攻直前に見られた破壊型マルウェアの攻撃、電力網へのサイバー攻撃が発生した。中東ではイスラム教シーア派組織ヒズボラの携帯通信機が一斉に爆破される事件が発生した。なお、2025 年からのイランにおける軍事衝突ではイラン革命防衛隊が米テック企業 7 社を標的にすると宣言しており、標的企業のサービスを利用している場合、組織に影響が出るおそれがある。地政学的リスクによるサイバー攻撃は近年顕著になってきており、日本企業においても備えは不可欠である。

こうした中、各国ではサイバー攻撃の侵入経路となり得るセキュリティが脆弱な製品やサービスを排除するため、規制や認証制度を設ける動きがある。また、地政学的に対立している国のネットワーク機器や IoT 機器等を排除する動きも見られる。日本でも経済産業省と IPA が「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」を整備している。

**図表 3　地政学的リスクに起因するサイバー攻撃の例**

| | |
|---|---|
| 1. 社会混乱や業務停止を狙う攻撃 | a）政府機関などの公共サービスの停止<br>b）物流、金融、医療、エネルギーなど重要インフラの停止 |
| 2. 情報資産を狙う攻撃 | a）先端技術情報の窃取による産業競争力の低下<br>b）安全保障情報の窃取による防衛力の低下 |
| 3. デマ流布やなりすまし攻撃 | a）社会不安や国民分断<br>b）特定組織や個人の信用失墜 |

（出所） 当社作成

### (2) AI の利用をめぐるサイバーリスクの影響

AI の普及は、情報セキュリティ上における「AI 利用そのものへの攻撃」、そして「AI の攻撃手段としての活用」における新たなリスクを顕在化させている。

「AI 利用そのものへの攻撃」とは、AI システムの乗っ取りや妨害、データの窃盗などのリスクであり、AI の利用が進むにつれ急激に影響力を増すと予想される。特に、目的を持って状況を理解し、自分で判断して行動する「AI エージェント」は乗っ取りによって不正な動作をさせられるリスクをはらんでいる。2025 年に発生した特定国関係者と思われるハッカーによる米国製 AI 乗っ取りによるサイバー攻撃タスクの自動実行事件は、その懸念の先駆けとなった。

「AI の攻撃手段としての活用」とは、AI を用いたサイバー攻撃の高度化や効率化であり、攻撃の高度化と大規模化のリスクが同時に引き上がる懸念がある。自然で違和感のない日本語のメールや音声、文書を大量に自動生成したフィッシングなどは、従来の基準で「不自然な日本語を見分ける」といった注意喚起による対策が困難になる。また、少人数でも大規模かつ継続的な攻撃が可能なため、攻撃量の急増が予想される。すでに詐欺メールの“品質向上”で活用されており、対策が急務である（図表 4）。

**図表 4 AI の利用をめぐるサイバーリスクの例**

| | |
|---|---|
| 1. AI 利用そのものへの攻撃 | a）AI に機密情報や個人情報を入力して意図せず漏えいするリスク<br>b）AI の出力結果を過信して誤った意思決定や業務処理を行うリスク<br>c）プロンプト操作で本来想定されていない情報を引き出されるリスク<br>d）学習データを汚染して判断をゆがめさせる攻撃を受けるリスク<br>e）AI エージェントの乗っ取りにより不正な動作をさせられるリスク |
| 2. AI の攻撃手段としての活用 | a）AI を用いた違和感のない攻撃コンテンツの生成<br>b）AI を用いた情報収集に基づく最適な攻撃手法や文面の立案<br>c）AI を用いた攻撃プロセスの自動化・高速化 |

（出所） 当社作成

## 4. 対策の考え方

サイバー攻撃が「産業化」し、攻撃手法は年々高度化していた中、今後は「地政学×AI リスク」の影響により、攻撃の質と量がいっそう深刻化すると予想される。2026 年の 10 大脅威の趨勢を踏まえ、組織が新たにとるべき情報セキュリティ対策の要点は以下の 3 つである。

### （1） 最悪の被害を想定した復旧準備

ランサム攻撃に代表されるシステムやデータを破壊し大きな被害を与える「破壊型攻撃」では、オンライン上のバックアップや常時接続されたストレージまで被害に遭う事例が報告されている。そのため、バックアップは論理的・物理的に分離された環境で保管し、攻撃者が物理的にアクセスできない構成とすることが重要である。

また、バックアップからリカバリーができない場合でも安全な状態で再構築できるよう、設定情報、認証情報、業務アプリケーションの構成情報なども含めて検討する必要がある。データの保存にとどまらず、安全な訓練環境を

準備した上で定期的に復旧訓練を実施し、復旧に要する時間や手順を把握しておくのが望ましい。

### （2） 高度化する攻撃に耐えられる情報セキュリティ製品とサービスの採用

サイバー攻撃の巧妙化・自動化により、従来型の境界防御やセキュリティ製品の導入のみでは侵入経路を防御するのが難しくなっている。高度な攻撃を前提とした検知・対応能力を備える情報セキュリティ製品およびサービスを採用していく必要がある。

そのために、既知のマルウェアや攻撃パターンに即した防御に加え、通常とわずかに異なる通信などの兆候を見逃さない製品の導入や監視体制を構築していく。具体的には、ログやアラートの統合分析によって未知の攻撃を検知できる製品、侵入後の不審な挙動を早期に把握できるエンドポイントおよびネットワーク監視の仕組みの整備が挙げられる。

さらに、攻撃開始後に被害を拡大させずに情報資産を守るため、24 時間体制による監視や専門的知見に基づく分析を提供する、セキュリティ・オペレーション・センターなどのサービス活用も有効である。

### （3） 防御失敗を前提にした事業継続計画

軍事レベルに匹敵するような高度な攻撃を受けた場合、完璧な防御は極めて困難である。そのため、被害を受けた場合はいかに早期復旧を図るか、という視点も求められる。

また、自社が直接狙われていなくても、サプライチェーン上の関係者が被害を受ける場合や、自社が利用している重要インフラが攻撃されるリスクは高まっている。そのため、関係先の被害を想定した事業継続計画（BCP）の策定が必要となる。

以上についていずれも未対応の企業は、(1)から順番に取り組むことが推奨される。

「地政学×AI リスク」の台頭により、組織の情報セキュリティ対策に求められる水準はますます高まっている。さらに、高度化するサイバーリスクへの対応の遅れは、企業の存続に直結する深刻な影響につながりかねない。本稿で取り上げた内容を参考にして、サイバー攻撃を身近なものとして捉え、平時のうちから準備を進めることが望ましい。