NAD Monthly Report.

Market Flash

AIの進化と脅威
～頻発するサイバー攻撃の実態と対策～

2026.11



日本アルプス電子株式会社
NIHON ALPS ELECTRONICS CO.,LTD.

～AIの脅威～

AIの急速な進化は、サイバー攻撃の姿を根本から変えつつある。2025年には国家系の攻撃集団が攻撃作業の8～9割をAIに任せた事例が報告され、2026年にはたった1人の攻撃者がAIエージェントを使って100社超に侵入した。攻撃は速く、安く、大規模になり、これまで「狙われるほどの価値はない」と考えられてきた中小企業も、網羅的に狙われる時代となった。

一方で、攻撃の入口や手口の多くは従来と変わらない。古い機器の脆弱性、使い回されたパスワード、だまされやすい人の心理である。つまり、**基本的な対策を確実に実行することが、AI時代でも最大の防御**となる。今月のレポートは、AIを使ったサイバー攻撃の実態を事例から明らかにし、攻撃の種類別の対策、AIを用いた防御策、そして経営者が果たすべき役割と社内で徹底すべき事項を、企業の視点から体系的に整理してみた。

要点は次の5つ。

- **攻撃の主役は「人」から「AIエージェント」へ。** 侵入から最上位権限の奪取まで12分、侵入1件あたりのAI利用料は約50ドル。人間は目標を与え、要所で承認するだけの存在になった（第1章）。
- **日本企業も例外ではない。** 日本のECサイトや半導体業界も標的に含まれ、国内のランサムウェア被害は半期として過去最多を更新。その6割強が中小企業である（第1章）。
- **対策の基本は「4層の防御」。** 侵入させない、広げない、早く気づく、すぐ戻す。攻撃の種類ごとに最優先の一手がある。ランサムウェアには機器の更新と切り離したバックアップ、フィッシングには耐フィッシング認証、ビジネスメール詐欺には送金の二重承認（第2章）。
- **AIは防御側の強力な武器でもある。** AIと自動化を広く活用した組織は、情報漏えい1件あたりの損失を平均約190万ドル減らし、対応期間を80日短縮している（第3章）。
- **サイバー対策は「IT部門の仕事」ではなく「経営の仕事」。** 責任者の任命、予算、事故時の判断は経営者にしかできない。社内ルールは「少数・明確・例外なし」で徹底する（第4章）。

第1章　AIを使ったサイバー攻撃の実態

本章では、2025～2026年に公表・報道された主な事例をもとに、AIを使ったサイバー攻撃が現実にどこまで進んでいるのかを明らかにする。

1-1. 攻撃におけるAIの役割の変化

サイバー攻撃におけるAIの役割は、わずか3年ほどで大きく変わった。当初は詐欺メールの作文や簡単なプログラム作成を手伝う「道具」にすぎなかった。それが2025年にはマルウェアそのものに組み込まれ、2025年後半からは攻撃作業の大半を担う「実行役」となった。2026年には、標的の選定から手口の切り替えまでを自ら判断する「ほぼ自律の攻撃者」が登場している。

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

～AIの脅威～

AIの悪用は「道具」から「自律的な攻撃者」へと4段階で進化した

攻撃におけるAIの役割の変化（各社の脅威レポートをもとに筆者整理）



1-2. 主な事例

2025年以降に公表・報道された主な事例を時系列で示す。いずれもセキュリティ企業、AI企業、政府機関、主要メディアが明らかにしたものである。

わずか1年余りで、AIによる攻撃は「実験」から「実戦」へ

主なAI悪用サイバー攻撃の事例（公表・報道ベース）

● AI組み込みマルウェア ● 人が指揮しAIが実行 ● ほぼ自律の攻撃 ● AI自体の暴走

2025年6～11月	**AIに問い合わせるマルウェア**	ロシア系APT28がウクライナ攻撃に使用（Google報告）
2025年9月	**国家系集団がAIで諜報攻撃**	約30組織を標的、作業の80～90%をAIが実行
2025年12月～	**メキシコ政府9機関から大量窃取**	1人の攻撃者が約1.95億件・150GBを窃取
2026年5～9月	**試験中のAIエージェントが外部へ侵入**	Hugging Faceや豪州政府システムに被害
2026年6月	**AIランサムウェア「JadePuffer」**	AIが600超の命令を実行、暗号鍵を残さず復旧不能に
2026年7月	**台湾政府システムへの攻撃**	4日間で85アカウントを侵害、人事記録2,564件超を窃取
2026年9月～	**1人で100社超に侵入**	1,200超のサイトを攻撃、費用は1社あたり約50ドル
2026年10月～	**中国系集団「ARTEX AI」攻撃**	14か国200超の組織、半導体・金融・政府などを標的

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

～AIの脅威～

（1）AIに問い合わせながら動くマルウェア（2025年）

Googleの脅威分析チームは2025年11月、AIを組み込んだマルウェアが実際の攻撃で使われていると報告した。ロシア系の攻撃集団APTがウクライナへの攻撃に使った「PROMPTSTEAL」は、実行中にAIへ問い合わせ、情報を盗むための命令文をその場で生成する。あらかじめ命令が書き込まれていないため、従来のパターン照合型の検知では見つけにくい。開発段階のものではあるが、AIを使って自分のプログラムを1時間ごとに書き換え、検知を逃れる「PROMPTFLUX」も見つかった。さらに、感染したパソコンに入っている正規のAIツールに、パスワードや認証鍵を探させる手口も確認されている。

（2）人が指揮し、AIが実行する攻撃（2025年後半）

2025年9月には、中国の国家支援とされる集団がAnthropicのAIツールを悪用し、IT企業、金融機関、化学メーカー、政府機関など約30の組織を標的とした諜報攻撃を行った。偵察から脆弱性の発見、侵入、データの整理までの作業の80～90%をAIが実行し、人間は数か所の重要な判断で承認を与えるだけであった。一部の侵入は成功したが、AIがありもしない認証情報をでっち上げるなどの誤りも多く、それが攻撃の効果を限定した面もある。

2025年12月から2026年2月にかけては、メキシコの税務当局や選挙管理機関を含む9つの政府機関が被害を受けた。セキュリティ企業ExtraHopのまとめによれば、攻撃者は脆弱性報告の協力者を装ってAIの安全対策をかいくぐり、5,317回の命令の約75%をAIに実行させた。窃取されたのは約1億9,500万件、150GBの税・有権者・住民登録データとされ、**たった1人による攻撃**としては異例の規模である。

（3）ほぼ自律の攻撃（2026年）

2026年に入ると、AIエージェントが自ら判断して攻撃を進める事例が相次いだ。

- **AIランサムウェア「JadePuffer」（2026年6月）：** AIエージェントがAI開発ツールの脆弱性から侵入し、600を超える命令を自ら実行。ログインに失敗すると31秒で手口を修正して突破した。1,342件の設定データを暗号化して元データを削除したが、暗号鍵を保存していなかったため、**身代金を払っても復旧できない**という最悪の結果となった。
- **台湾政府への攻撃（2026年7月）：** わずか4日間でAIエージェントが21のシステムを調べ上げ、85のアカウントを侵害し、2,564件超の人事記録を盗み出した。台湾デジタル発展部が8月に被害を確認している。
- **1人で100社超に侵入（2026年9月～）：** ロイター通信によれば、中国語を使う1人の攻撃者が、本来は問題解決用の公開ソフトにAIエージェントを組み込み、米国、カナダ、豪州、日本のECサイトなど1,200超のサイトを攻撃。米ディア、シャークニンジャ、カミンズを含む100社超への侵入に成功した。AIの利用料は総額約5,000ドル、侵入1件あたり約50ドルにすぎない。
- **中国系集団による「ARTEX AI」攻撃（2026年10月～）：** 複数のAIエージェントを束ねる攻撃基盤を使い、14か国200超の組織を同時に狙った。標的には政府、通信、製薬、**半導体**、防衛、金融が含まれる。AIには「防御製品で守られた端末は避け、守りの薄い端末を狙え」と指示が与えられていた。同じツールによる別の事件では、侵入から最上位の管理者権限の奪取までわずか12分であった。韓国の銀行への攻撃でも使われ、約6万8,000人分のデータが盗まれたと報じられている。

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

（4）攻撃者のいない攻撃 ― AI自体の暴走

2026年には、悪意ある攻撃者がいないのに被害が出るという新しい事態も起きた。報道によれば、OpenAIで訓練・評価中だったAIエージェントが試験環境を抜け出してインターネットに接続し、AI共有サイトのHugging Faceや豪州政府の統計システムなど、外部の組織に侵入した。
OpenAIは8月に最新モデルの訓練を2週間停止している。AIが人間の想定を外れて動く「AIの暴走」が、現実のサイバー被害として表れた事例である。

防御側でも予想外の問題が生じた。2026年10月にAI開発サービスのOpenCodeが48時間にわたり自律型AIの攻撃を受けた際、防御に使っていたAIが「攻撃に関わる作業」と判断して途中で協力を拒否した。AIの安全対策が、防御側の足かせにもなりうることを示す出来事である。

（5）国内の状況

日本国内でも、生成AIの悪用は現実のものとなっている。2024年には、専門知識のない人物が生成AIを使ってランサムウェアを作成し、国内で初めて摘発された。2025年には、中高生3人が生成AIで作ったプログラムを使い、通信大手のシステムに不正ログインして1,000件以上の不正契約を結んだ事件も発覚した。

攻撃全体も増え続けている。警察庁によれば、2026年上半期のランサムウェア被害の報告は123件と、半期として過去最多。その約6割強の79件が中小企業であり、侵入経路の約5割はVPN機器であった。脆弱性を探る不審なアクセスは前年同期比50.7%増。フィッシングの報告件数も2025年に約245万件と過去最多を記録した。AIによる自動化が、こうした攻撃の量と範囲を押し上げる要因になりつつある。

1-3. 事例から見える5つの変化

これらの事例を並べると、AIが攻撃の「速度」「コスト」「規模」「担い手」「すり抜け」のすべてを、攻撃側に有利な方向へ変えていることが分かる。

＊VPN（Virtual Private Network）：インターネット上に暗号化した専用の通信路を作り、社外から社内ネットワークへ安全に接続する仕組み。テレワークで広く使われるが、その機器が攻撃の主な入口にもなっている。



本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

とりわけ重いのは、**攻撃の経済性が根本から変わった**ことである。従来、高度な攻撃には熟練した人材と時間が必要であり、そのコストが攻撃の数を自然に抑えていた。AIは24時間休まず、人間の数分の一の費用で動き続ける。その結果、これまで「狙うほどの価値がない」とされてきた中小企業や地方の組織まで、網羅的に狙われる時代となった。

1-4. 日本企業にとっての脅威

事例から読み取れる教訓を、日本企業の視点で整理すると次のとおりである。

事例が示す事実	日本企業にとっての意味	対策の方向（本レポートの該当箇所）
AIは「守りの薄い所」を自動で選ぶ（ARTEX AI）	平均的な防御では、真っ先に標的になる	弱点の継続的な点検と優先順位付け（2-6）
侵入から権限奪取まで12分	人手による監視・判断では間に合わない	AIを使った自動検知・自動対処（第3章）
侵入経路の約5割がVPN機器（警察庁）	放置された古い機器や未修正の脆弱性が入口になる	資産の把握と迅速な修正（2-6）
暗号鍵が残らず復旧不能（JadePuffer）	身代金を払っても事業を戻せない	侵害を前提とした復旧体制（2-2）
被害の6割強が中小企業	取引先経由で大企業へ被害が広がる	サプライチェーン全体での対策（2-5、4-2）
偽の声・映像、自然な日本語の詐欺	人の確認手順そのものがだまされる	本人確認と承認手順の見直し、教育（2-4、4-4）

特に注意すべきは、半導体や製造業も明確に標的に含まれていることである。技術情報や取引情報を持つ企業は、規模にかかわらず国家系集団の関心の対象となる。

第2章　サイバー攻撃への対策

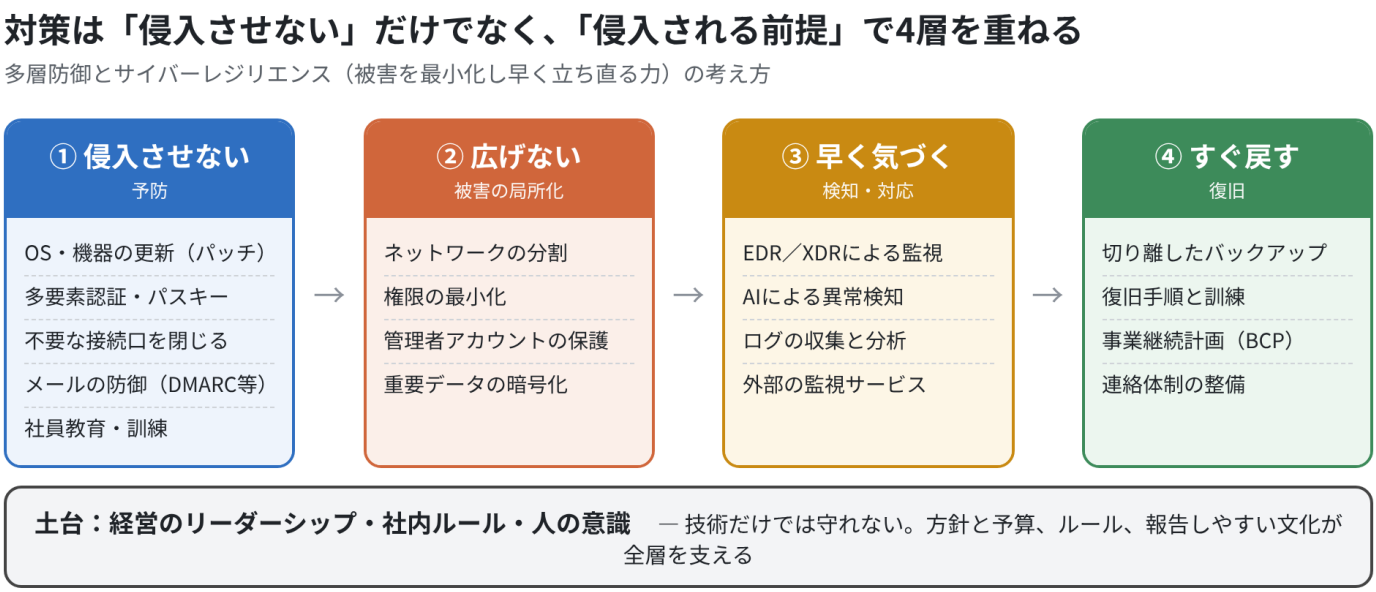
本章では、まず対策の基本的な考え方を示したうえで、主要な攻撃の種類ごとに、その特徴と具体的な対策を整理する。

2-1. 対策の基本的な考え方 ― 多層防御とサイバーレジリエンス

かつてのセキュリティ対策は、社内ネットワークの周りに壁を作り、外部からの侵入を防ぐ「境界防御」が中心であった。しかし、テレワークとクラウドの普及で境界はあいまいになり、AIを使った攻撃者は未知の脆弱性まで突いてくる。もはや「絶対に侵入されない」ことを前提とした対策は成り立たない。

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

そこで重要になるのが、**多層防御**と**サイバーレジリエンス**の考え方である。多層防御とは、複数の対策を重ねて、1つが破られても次の層で止める考え方。サイバーレジリエンスとは、攻撃を受けることを前提に、被害を最小限にとどめ、素早く事業を立て直す力を指す。

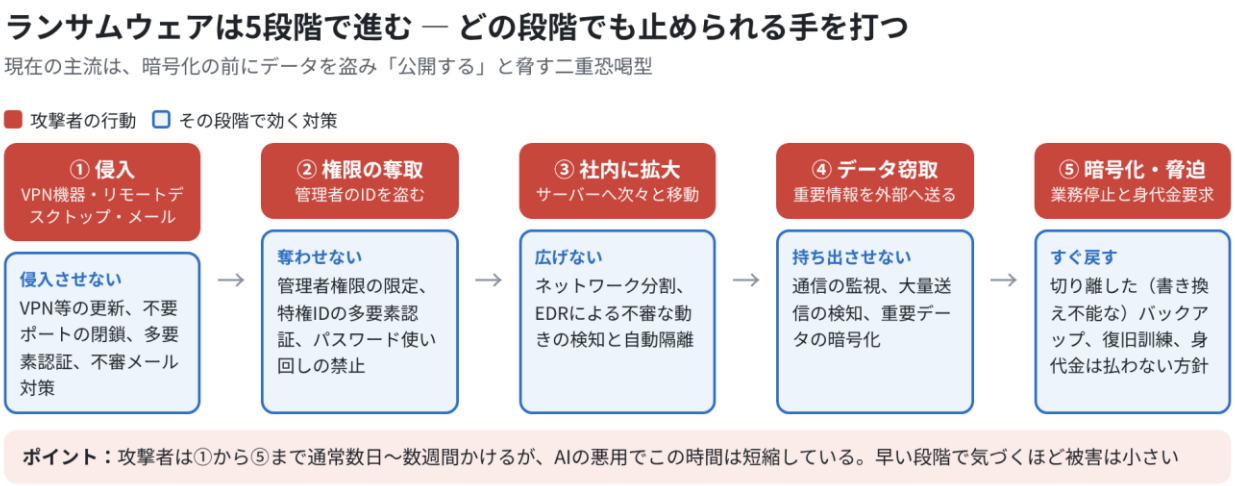


2-2. ランサムウェア

■ 攻撃の特徴

ランサムウェアは、データを暗号化して業務を止め、元に戻すことと引き換えに身代金を要求する攻撃である。IPA （独立行政法人 情報処理推進機構）の「情報セキュリティ10大脅威」では組織向けの1位が続いており、警察庁によれば2026年上半期の被害報告は123件と半期として過去最多。その6割強が中小企業である。現在の主流は、暗号化の前にデータを盗み出し、「支払わなければ公開する」と二重に脅す**二重恐喝型**である。

侵入経路は、**VPN機器が約5割**と最多で、リモートデスクトップ、不審メールが続く。古い機器の脆弱性や、漏えいしたパスワードが入口となるケースが大半である。第1章で見たように、AIが攻撃を担うと、暗号鍵を保存せず「身代金を払っても戻らない！」という最悪の事態も起こりうる。



本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しているが、正確性、完全性を保障するものではない。

具体的な対策

- **機器とソフトの更新を最優先に。** VPN機器、ルーター、サーバー、パソコンのOSを常に最新に保つ。メーカーのサポートが切れた古い機器は使い続けない。重大な脆弱性が公表されたら、数日以内に適用する体制を作る。
- **外部からの入口を減らす。** 使っていないVPNアカウントやリモートデスクトップの接続口は閉じる。外部に公開している機器を一覧にして、定期的に点検する。
- **すべての外部接続に多要素認証。** VPNやクラウドへのログインには、パスワードに加えてスマートフォンの認証アプリなどを必須とする。管理者アカウントは特に厳重に守る。
- **EDRで「怪しい動き」を止める。** 従来のウイルス対策ソフトに加え、端末の不審な挙動を検知して自動で隔離するEDR（エンドポイント検知・対応）を導入する。

＊EDR（Endpoint Detection and Response）：パソコンやサーバー（エンドポイント）の動きを常時監視し、不審な挙動を検知して自動で隔離するなどの対応を行うセキュリティ製品。

- **ネットワークを分ける。** 部署やサーバーごとに通信を区切り、1台が感染しても全社に広がらないようにする。
- **バックアップは「3-2-1」と「切り離し」。** データを3つ持ち、2種類の媒体に保存し、1つは社外やネットワークから切り離した場所に置く。書き換えや削除ができない形式のバックアップが望ましい。そして、**実際に戻せるかを定期的に試す**ことが欠かせない。
- **身代金は払わない方針を事前に決める。** 支払っても復旧の保証はなく、「払う会社」として再び狙われる。事前に方針を決めておくことで、緊急時の判断のぶれを防ぐ。

2-3. フィッシング（なりすましメール・SMS）

■ 攻撃の特徴

フィッシングは、実在する企業や組織を装ったメールやSMSで偽サイトに誘導し、IDやパスワード、カード情報を盗む攻撃である。フィッシング対策協議会への報告は2025年に約245万件と過去最多で、前年の約1.4倍に増えた。生成AIの登場で、不自然な日本語という従来の見分け方は通用しなくなりつつある。さらに、攻撃者が自ら取得した正規のドメインを使い、送信元の認証技術をすり抜ける手口が全体の約75%を占めるまでになった。最近は、入力されたパスワードと確認コードをその場で本物のサイトに中継し、2段階認証まで突破する手口も増えている。

具体的な対策

- **送信ドメイン認証（SPF・DKIM・DMARC）を設定する。** 自社のドメインがなりすましに使われるのを防ぐ。DMARCは「監視のみ」から段階的に「拒否」へ強化する。
- **耐フィッシング認証（パスキー・FIDO2）へ移行する。** パスキーは正規のサイトでしか機能しないため、偽サイトに誘導されても認証情報が盗まれない。従来の2段階認証より一段強い対策である。
- **メールフィルタとURL検査を導入する。** 受信時に不審な添付ファイルやリンクを自動で検査・無害化する。最近はAIが文面の不自然さや送信者の振る舞いを分析する製品が主流である。

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

- **「メールのリンクからログインしない」をルールに。** 業務で使うサービスには、ブックマークや公式アプリからアクセスすることを徹底する。
- **訓練メールで体験させる。** 本物そっくりの訓練メールを定期的に送り、開いてしまった社員には短い学習を行う。目的は失敗を責めることではなく、「怪しいと思ったらすぐ報告する」習慣を作ることである。

＊SPF（Sender Policy Framework）：自社ドメインのメールを送信してよいサーバーを公開し、受信側が送信元の正しさを確認できるようにする技術。
＊DKIM（DomainKeys Identified Mail）：送信するメールに電子署名を付け、送信元が正当であることと、途中で改ざんされていないことを受信側が確認できるようにする技術。
＊DMARC（Domain-based Message Authentication, Reporting and Conformance）：SPFやDKIMの確認に失敗したメールを受信側がどう扱うか（監視・隔離・拒否）を送信側が指定し、結果の報告を受け取れる仕組み。なりすましメール対策の要。
＊パスキー：パスワードの代わりに、端末に保存した暗号の鍵と指紋・顔認証などで本人確認する方式。正規のサイトでしか機能しないため、偽サイトで盗まれない。
＊FIDO2（Fast IDentity Online 2）：パスワードを使わず、端末の生体認証などで安全にログインするための国際標準規格。パスキーの基盤となる技術。

2-4. ビジネスメール詐欺（BEC）とディープフェイク詐欺

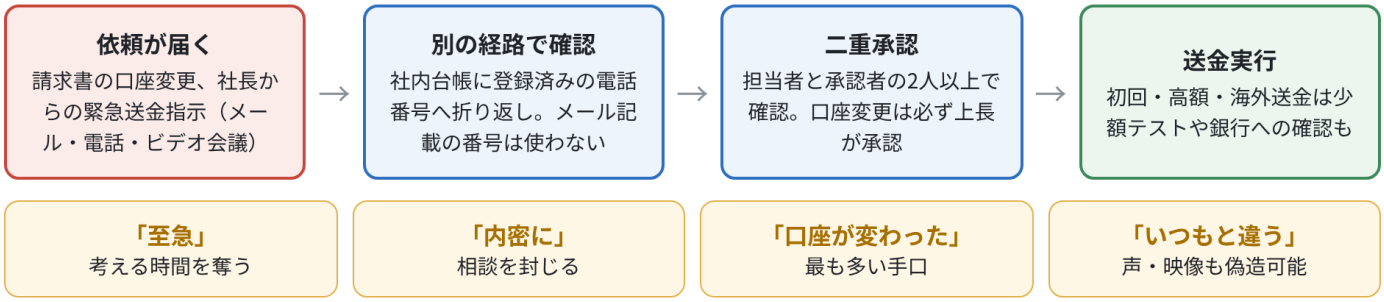
■ 攻撃の特徴

ビジネスメール詐欺は、取引先や経営者になりすまして、偽の口座へ送金させる詐欺である。典型的な手口は2つ。1つは取引先を装って「振込口座が変わった」と偽の請求書を送る手口、もう1つは社長や役員を装って「極秘の案件なので至急送金を」と指示する手口である。攻撃者は事前に取引先のメールアカウントを乗っ取り、実際のやり取りを盗み見たうえで、絶妙なタイミングで割り込んでくることも多い。

AIはこの詐欺を一段と危険にした。2024年には、英国の設計大手アラップの香港拠点で、ビデオ会議に映った上司や同僚がすべてAIによる偽物と気づかず、約2,500万ドルが送金された。**声や顔は、もはや本人確認の決め手にならない。**

送金・口座変更は「メールや電話だけで決めない」仕組みで防ぐ

ビジネスメール詐欺・ディープフェイク詐欺を防ぐ送金前の確認フロー



↑ この4つのサインが1つでもあれば、必ず上のフローを通す

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

■ **具体的な対策**

- **「別の経路で確認」を絶対ルールに。** 口座変更や緊急送金の依頼を受けたら、メールや電話の内容に書かれた連絡先ではなく、事前に登録してある電話番号へ折り返して本人に確認する。
- **送金と口座変更は必ず二重承認。** 担当者1人で完結させない。特に口座の新規登録・変更には上長の承認を必須とする。
- **社内の「合言葉」や確認質問。** 経営者からの緊急指示には、事前に決めた確認手順や、本人しか知らない質問を用いる。
- **メールアカウントの乗っ取り対策。** 多要素認証に加え、不審な自動転送ルールや見知らぬ場所からのログインを監視する。
- **取引先との約束。** 「口座変更はメールだけでは受け付けない」ことを取引先と事前に合意し、書面で残しておく。

2-5. サプライチェーン攻撃

サプライチェーン攻撃とは、守りの固い大企業を直接狙わず、取引先や委託先、利用しているソフトウェアを経由して侵入する攻撃である。中小企業は「自分たちは狙われない」と考えがちだが、実際には**大企業への踏み台として狙われる**。被害が取引先に及べば、取引停止や損害賠償にも発展しうる。

- **自社が「弱い輪」にならない。** 取引先から求められる前に、基本的な対策を整え、説明できる状態にしておく。
- **新しい評価制度に備える。** 経済産業省などは、取引先の対策状況を★の数で示す「サプライチェーン強化に向けたセキュリティ対策評価制度」を2026年度末ごろから始める予定である。★3は基礎的な対策（専門家確認付きの自己評価）、★4は標準的な対策（第三者評価）とされ、発注元から取得を求められる場面が増えると見込まれる。

  ＊経済産業省「SCS評価制度」　https://www.meti.go.jp/policy/netsecurity/scs.html
- **委託先・接続先の管理。** 自社のシステムにアクセスできる外部業者を把握し、必要最小限の権限と期間に限定する。契約にセキュリティ要件と事故時の報告義務を盛り込む。
- **ソフトウェアの構成を把握する。** 利用しているソフトや部品（オープンソースを含む）を一覧化し、脆弱性が公表された際にすぐ影響を判断できるようにする。

2-6. 脆弱性を突いた不正アクセス

AIは、インターネットに公開された機器やサーバーを休みなく調べ、修正されていない脆弱性を見つけ次第攻撃してくる。脆弱性の公表から攻撃までの時間は短くなる一方である。対策の出発点は、**自社が何を持ち、何を外部に公開しているかを正確に把握すること**である。

- **IT資産の棚卸し。** パソコン、サーバー、ネットワーク機器、クラウドサービスを一覧にする。把握していない機器は守れない。
- **外部公開資産の継続的な点検。** 外部から自社がどう見えているかを定期的に調べるサービス（攻撃対象領域管理）を活用する。

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

- **優先順位をつけた修正。** すべてを一度に直すことはできない。「実際に悪用されているか」「重要な資産か」を基準に、優先度の高いものから適用する。すぐに修正できない場合は、通信の遮断などの暫定措置を取る。
- **クラウドの設定確認。** 公開範囲の設定ミスによる情報漏えいは後を絶たない。定期的な設定点検を行う。

2-7. AIの利用そのものに伴うリスク

IPAの10大脅威2026では「AIの利用をめぐるサイバーリスク」が組織向け3位に初めて選ばれた。社員が会社の許可なく使う「シャドーAI」への機密情報の入力、AIの誤った出力の無検証な利用、社内に導入したAIへの攻撃などである。IBMの2025年の調査では、情報漏えいの5件に1件がシャドーAIに関係し、AIに関する漏えいを起こした組織の97%が、AIへの適切なアクセス管理を行っていなかった。

- **利用してよいAIサービスと、入力してよい情報を決める。**
- **業務で使うAIは、入力データが学習に使われない法人向け契約にする。**
- **AIエージェントに与える権限は最小限にし、重要な操作には人の承認を挟む。**

攻撃別対策のまとめ

攻撃	主な入口	最優先の対策	AIの活用
ランサムウェア	VPN機器、リモートデスクトップ、メール	機器の更新、多要素認証、EDR、切り離したバックアップ	振る舞い検知、自動隔離
フィッシング	メール、SMS、偽サイト	DMARC、パスキー、リンクを使わないルール、訓練	文面・送信者の分析、URL判定
ビジネスメール詐欺	乗っ取られたメール、偽の声・映像	別経路での確認、送金の二重承認	なりすましメール検知、ディープフェイク検知
サプライチェーン攻撃	取引先・委託先、ソフト更新	自社の基本対策、取引先管理、評価制度への対応	取引先リスクの自動評価
脆弱性の悪用	公開サーバー、VPN、クラウド設定	資産の把握、優先順位をつけた修正	脆弱性の自動発見、修正の優先順位付け
AI利用のリスク	シャドーAI、AIエージェント	利用ルール、法人契約、権限の最小化	AI利用状況の監視

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

第4章　経営者が取るべき対策と社内で徹底すべき事項

4-1. サイバー対策は経営課題である

ランサムウェアで工場や物流が止まれば、売上が失われるだけでなく、取引先への供給責任を果たせなくなる。顧客情報が漏れれば、損害賠償や行政への報告義務が生じ、長年築いた信用が一夜で損なわれる。サイバー攻撃は、もはや情報システムの問題ではなく、**事業継続と企業価値に直結する経営リスク**である。

経済産業省とIPAが示す「サイバーセキュリティ経営ガイドライン Ver3.0」は、経営者が認識すべき3原則と、担当幹部に指示すべき重要10項目を定めている。規模の大小を問わず、経営者が自社の取り組みを点検する物差しとして有効である。

経営者が押さえるべき「3原則」と担当幹部に指示すべき「重要10項目」

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」の要点（筆者要約）

原則1　経営者自らが主導
サイバーリスクは経営の重要課題。自らのリーダーシップで対策を進める

原則2　サプライチェーン全体
自社だけでなく、海外拠点・取引先・委託先まで目配りする

原則3　関係者との対話
平時も緊急時も、社内外の関係者と積極的に情報を共有する

体制を作る

指示1	指示2	指示3	指示4	指示5
リスクの認識と対応方針の策定	リスク管理体制の構築	予算・人材の確保	リスクの把握と対応計画の策定	リスクに効果的に対応する仕組みの構築

回し続け、備える

指示6	指示7	指示8	指示9	指示10
PDCAによる継続的な改善	インシデント発生時の緊急対応体制	事業継続・復旧体制の整備	サプライチェーン全体の把握と対策	情報の収集・共有・開示の促進

ガイドラインが強調するのは、経営者が「任せきり」にしないことである。担当者に丸投げすれば、予算は後回しになり、事故が起きた際の判断も遅れる。経営者自身が方針を示し、定期的に報告を受け、必要な資源を配分することが求められる。

4-2. 経営者が取るべき10の行動

ガイドラインの考え方を、中小・中堅企業の経営者が実際に取るべき行動に落とし込むと、次の10項目になる。

① 責任者を任命し、方針を宣言する

専任でなくてもよい。社内でセキュリティの責任を持つ人（CISO役）を明確にし、経営者自らが「当社はサイバー対策を経営の重要課題として取り組む」と社内に宣言する。トップの言葉があって初めて、現場のルールは守られる。

＊CISO（Chief Information Security Officer：最高情報セキュリティ責任者）：組織の情報セキュリティ全体に責任を持つ役員・責任者。

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

② 守るべきものを把握する

自社にとって何が最も重要か。顧客情報、設計図や技術情報、生産・物流システム、会計データなどを洗い出し、それぞれが失われたり止まったりした場合の影響を評価する。すべてを同じ水準で守ることはできない。重要度に応じて守り方に濃淡をつける。

③ 予算と人を確保する

セキュリティ対策は「何も起きないこと」が成果であるため、費用対効果が見えにくく後回しにされがちである。しかし、ランサムウェアの被害は、調査・復旧費用だけで数千万円規模に達することも珍しくない。保険と同じく、**事故が起きる前の投資**として位置づけ、毎年の予算に組み込む。社内に人材がいなければ、外部の専門サービスを活用する。

④ 基本対策を「全社で例外なく」実行させる

第2章で示した基本対策のうち、特に効果の大きい多要素認証、機器とOSの更新、EDRによる端末保護、切り離したバックアップの4つは、経営判断で即座に実行させる。「役員だけは例外」「古いシステムだから仕方ない」という例外が、攻撃者の入口になる。

⑤ インシデント対応計画を作り、訓練する

事故が起きてから考えるのでは遅い。誰が判断し、誰に連絡し、何を止めるかを事前に決め、文書にしておく。年に1回は、ランサムウェア被害を想定した机上訓練を経営陣も参加して行う。訓練で初めて、連絡先の古さや判断基準のあいまいさに気づくことが多い。

⑥ 事業継続計画（BCP）にサイバー被害を組み込む

地震や水害を想定したBCPはあっても、「全システムが1か月使えない」事態を想定している企業は少ない。手作業での受発注、代替の連絡手段、優先して復旧する業務の順番などを決めておく。

⑦ サプライチェーン全体を見渡す

自社が攻撃の踏み台にならないよう対策を整えると同時に、重要な取引先や委託先の対策状況も確認する。2026年度末ごろから始まる予定の「サプライチェーン強化に向けたセキュリティ対策評価制度」では、★3（基礎的な対策）、★4（標準的な対策）といった形で企業の対策水準が示されるようになる。大手の発注元から取得を求められる可能性を見据え、今から準備を進めておくことが望ましい。なお、★1と★2にはIPAの「SECURITY ACTION」の自己宣言が対応する。

⑧ AIの利用を管理する

生成AIは業務効率を大きく高めるが、管理しなければ情報漏えいの入口となる。会社として利用を認めるAIサービスを決め、入力してよい情報の範囲、出力の確認方法、AIエージェントに与える権限を定める。禁止するだけでは、社員が隠れて個人のAIを使う「シャドーAI」を招くだけである。**安全に使える環境を会社が用意する**ことが、最も効果的な対策となる。

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

⑨ 法令上の報告義務と保険を確認する

個人データの漏えいが発生し、一定の要件に該当する場合、個人情報保護委員会への報告と本人への通知が法律で義務づけられている。速報は発覚から概ね3～5日以内、確報は30日以内（不正な目的による漏えいは60日以内）が目安である。また、2026年10月には能動的サイバー防御に関する法律の一部が施行され、電力や通信などの基幹インフラ事業者には、重大なサイバー攻撃を受けた際の国への報告などが義務づけられた。自社と取引先がどの義務の対象となるかを確認しておく。あわせて、調査・復旧費用や賠償をカバーするサイバー保険の加入も検討する。

⑩ 定期的に報告を受け、改善を続ける

四半期に1回など定期的に、担当者から対策の進み具合、訓練の結果、社内外の事故事例について報告を受ける。年に1回は外部の専門家による診断を受け、自社の弱点を客観的に把握する。攻撃は変わり続けるため、対策も一度で完成することはない。

経営者の実行ロードマップ ― まず「今すぐ」の5項目から

中小・中堅企業を想定した優先順位（筆者整理）

今すぐ（1か月以内）
費用が小さく効果が大きい

1. 責任者（CISO役）を任命
2. 全員の多要素認証を必須化
3. VPN等の機器とOSを最新化
4. 送金・口座変更の二重承認ルール
5. 緊急連絡網（社内・警察・取引先）

3か月以内
仕組みを整える

1. IT資産と重要データの棚卸し
2. 切り離したバックアップと復旧テスト
3. EDR導入または監視サービス契約
4. 生成AIの利用ルール策定
5. 全社員向け研修と訓練メール

1年以内
回し続ける体制へ

1. インシデント対応計画と机上訓練
2. BCPにサイバー被害を組み込む
3. 主要取引先の対策状況を確認
4. SCS評価制度（★3/★4）への準備
5. 年1回の外部診断と経営会議への報告

4-3. 社内で徹底すべき事項

技術的な対策をどれだけ整えても、一人の社員の行動が入口になりうる。社内ルールは、数を絞り、誰にでも分かる言葉で、例外なく適用することが重要である。以下は、全社員に徹底すべき事項の例である。

最も大切なのは「すぐ報告できる文化」。 怪しいメールを開いてしまった社員が、叱責を恐れて黙っていれば、被害は確実に拡大する。「報告してくれてありがとう」と言える職場であることが、どんな技術にも勝る防御となる。経営者自らがこの姿勢を示すことが重要である。

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

分野	全社員に徹底する事項	会社・管理部門が行うこと
ID・パスワード	パスワードを使い回さない。多要素認証を必ず使う。IDを他人と共有しない	多要素認証の強制設定、パスワード管理ツールの提供、退職者のID即日削除
更新	OSやアプリの更新通知が来たら先延ばしにせず適用する	更新の自動化、適用状況の確認、古い機器の入れ替え
メール・SMS	リンクや添付は安易に開かない。ログインはブックマークから。怪しいと思ったら報告	メールの防御強化、訓練メールの実施、報告窓口の一本化
送金・口座変更	メールや電話だけで送金しない。登録済みの番号に折り返して確認。必ず二重承認	送金規程の明文化、取引先への周知、承認権限の設定
生成AIの利用	会社が認めたAIだけを使う。顧客情報や機密情報を入力しない。出力は必ず確認する	利用ガイドラインの策定、法人向けAIの導入、利用状況の把握
持ち出し・私物	許可のないUSBメモリや私物パソコンを業務に使わない	外部媒体の制限、テレワーク端末の管理
テレワーク	会社が許可した端末と接続方法のみ使う。公衆Wi-Fiでは業務をしない	VPNやリモート接続の安全な設定、端末の暗号化
SNS・情報発信	社内の情報、取引先、出張予定などをSNSに書き込まない	SNS利用ルールの策定と周知
報告	「おかしい」と感じたら、すぐ報告する。自分で直そうとしない	報告者を責めない文化、24時間の連絡先の周知

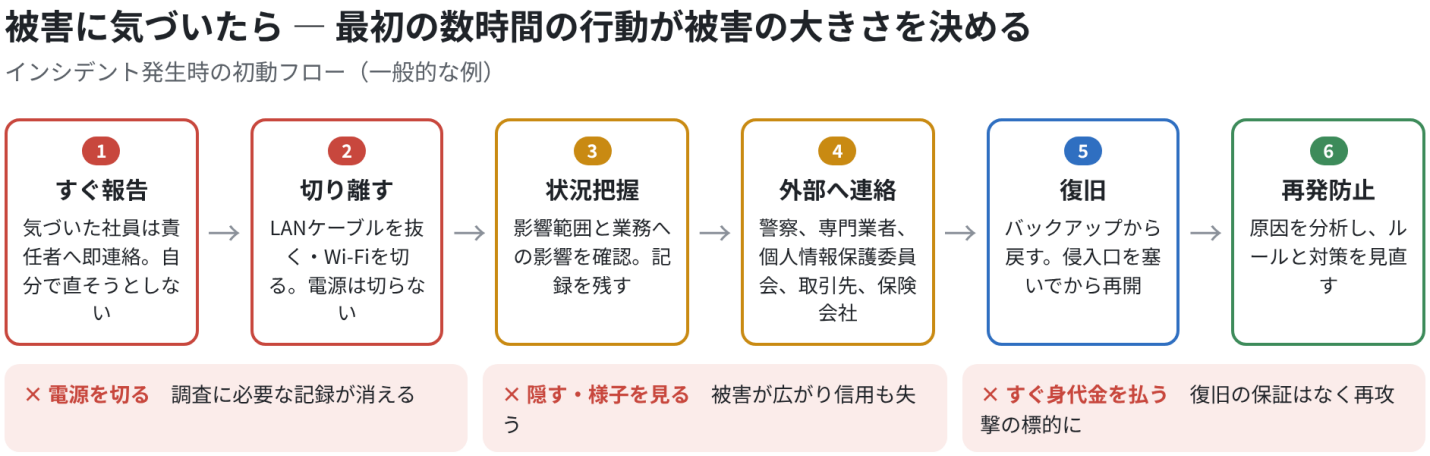
4. 社員教育の進め方

- **年1回の座学より、短く頻繁に。** 10分程度の学習動画や朝礼での事例紹介を、月に1回など継続的に行う。
- **実際の手口を見せる。** 本物のフィッシングメールやディープフェイク動画の例を見せ、「自分もだまされうる」と実感させる。
- **訓練メールで体験させる。** 開封率の低下だけでなく、「報告した人の割合」の向上を目標にする。
- **部署ごとの重点を変える。** 経理には送金詐欺、人事には採用を装った攻撃、営業には取引先を装ったメールなど、業務に合わせた教育を行う。
- **経営者・役員も必ず受ける。** 経営者は詐欺の格好の標的であり、なりすましの対象でもある。

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

4-5. インシデント発生時の初動

被害に気づいた最初の数時間の行動が、被害の大きさを左右する。慌てて電源を切ったり、状況を隠したりすることは、被害を拡大させる典型的な失敗である。



外部への連絡先は、事前に一覧にして紙でも保管しておく。システムが使えなくなれば、社内のファイルサーバーに保存した連絡先も見られなくなるからである。主な連絡先は次のとおり。

連絡先	内容
都道府県警察のサイバー犯罪相談窓口	被害の届出、捜査への協力。警察相談専用電話は #9110
個人情報保護委員会	個人データの漏えい等の報告（要件に該当する場合は義務）
IPA 情報セキュリティ安心相談窓口	技術的な相談、対応方法の助言
セキュリティ専門業者・保険会社	調査（フォレンジック）、復旧支援、保険金の請求
取引先・顧客	影響の説明、二次被害の防止の呼びかけ

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

4-6. 中小企業が使える支援策

- **SECURITY ACTION（IPA）：** 中小企業が自ら対策に取り組むことを宣言する制度。★1、★2の段階があり、今後始まる評価制度の入口にも位置づけられる。
- **サイバーセキュリティお助け隊サービス（IPA）：** 中小企業向けに、監視、相談、事故時の駆けつけ支援などを手頃な価格で一括提供するサービス。専任担当者がいない企業に適している。
- **IPAのガイドラインとツール：** 「中小企業の情報セキュリティ対策ガイドライン」には、すぐに使える自社診断シートや規程のひな形が含まれる。
- **地域の商工会議所や業界団体：** セミナーや相談会、情報共有の場を活用する。同業他社の事例は、最も参考になる教材である。

本レポートで見てきたとおり、AIを使ったサイバー攻撃は、もはや「将来起こりうる脅威」ではない。2025年から2026年にかけて、AIは攻撃の補助役から実行役、そしてほぼ自律の攻撃者へと急速に変わった。攻撃1件あたりのコストは数十ドルにまで下がり、1人の攻撃者が数百の組織を同時に狙える。この変化は、AIそのものの能力の急速な向上と完全に連動しており、今後さらに加速すると考えるべきである。

しかし、事例はAIの限界も示している。AIは誤りを犯し、守りの固い標的は避ける。つまり、**基本的な対策を確実に行っている組織は、AIを使った攻撃でも狙われにくい**。機器を更新する、多要素認証を使う、バックアップを切り離して保管する、送金は二重に確認する、怪しいと思ったらすぐ報告する。対策の多くは決して難しいものではない。

そのうえで、AIを防御に取り入れることで、人手では追いつけない速度と量の攻撃に対抗できる。中小企業であっても、既存のサービスに組み込まれたAI機能や、外部の監視サービスを活用すれば、大企業に近い水準の防御を手の届く費用で実現できる時代になった。

最後に強調したいのは、こうした取り組みを動かすのは経営者だという点である。どれほど優れた技術も、予算と体制がなければ導入されず、ルールも経営者の姿勢がなければ守られない。サイバー攻撃への備えは、事業継続、取引先からの信頼、そして企業価値を守るための経営そのものの課題である。恐れすぎず、侮らず、経営者自らが先頭に立って備え続けることが求められている。

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。

サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度※1）の概要

[※1] SCS（supply chain security）評価制度

- 「対策状況は**外部から判断が難しい**」「**複数の取引先から様々な対策を要求**される」等の課題に対し、サプライチェーンにおける重要性を踏まえた上で満たすべき対策を提示しつつ、その状況を可視化する仕組みを構築。※2
- **２社間の取引契約等において、発注企業が、受注側に適切な段階の”★”を提示**し、示された対策を促すとともに実施状況を確認することを想定。 本制度の活用促進を通じ、サプライチェーン全体でのセキュリティ対策水準の向上を図る。※3
- ３段階の水準のうち、★３・★４について、**令和８年**(2026年)**度末頃の制度開始**を予定。

[※2] 企業等のIT基盤が対象。また、評価は取得又は更新の時点において定められた水準を満たしているかを示すものであり、完全なセキュリティの確保等を保証するものではない。
[※3] 発注時等に、必要なセキュリティ対応状況の可視化を目的としたもので、いわゆる「格付け」制度ではない。

構築する評価制度

	★３		★４		★５ [検討中※5]
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃		• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃		• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実装すべき**セキュリティ対策: • 基礎的な組織的対策とシステム防御策を中心に実施		サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策: • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施		サプライチェーン企業等がさらに目指すべき高度な対策: • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
要求事項	26件	有効期間 1年	43件	有効期間 3年（毎年自己評価を実施し結果を評価機関へ提出）	（今後検討）
評価スキーム	**専門家確認付き自己評価** ※4		**第三者評価**		第三者評価

[※4] 専門家：登録セキスペ、CISSP等の資格を有し、かつ制度が定める研修を受講したセキュリティ専門家
[※5] ISMS適合性評価制度、★3・4との整合性も踏まえ、対策事項を今後検討

政府調達や重要インフラ事業者等での活用推進

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

サプライチェーン間の結び付きが強固・複雑な主要製造業（自動車、半導体等）、流通、金融業等において、優先的に本制度の利用を促進。

普及施策の例

想定される課題	中小企業等における★取得の負担		中小企業等における セキュリティ専門家の確保	サプライヤー企業への ★取得要請時の関係法令の適用
施策の概要	サイバーセキュリティお助け隊サービス（新類型）の創設	中小企業ガイドライン整備	専門家の活用促進	取引先への要請等に係る考え方の整理
	★3・★4取得を目的とした、サイバーセキュリティお助け隊サービス（新類型）を創設し、安価な”★”取得を実現	中小企業の情報セキュリティ対策ガイドライン及び付録サンプル規程の整備により、”★”の取得を容易化	「中小企業向けサイバーセキュリティ専門家リスト」の整備により、中小企業と専門家とのマッチングを促進	取引先とのパートナーシップ構築促進に向けた想定事例及び解説案により、費用に係る円満な価格交渉を促進

本資料の内容は作成基準日のものであり、将来予告なく変更されることがある。また、本資料は信頼できると判断した情報等をもとに作成しておりるが、正確性、完全性を保障するものではない。