Strictly Confidential

サイバーリスク対策セミナー

サイバー攻撃の実態と
中小企業における対策のポイント

MS&ADインターリスク総研株式会社
MS&AD INSURANCE GROUP

はじめに

サイバー空間では、
悪意を持った攻撃者などが起こす
サイバーセキュリティ事故が多発しており、
企業を取り巻くサイバーリスクは確実に高まっている。

© MS&AD InterRisk Research & Consulting, Inc.

本日のアジェンダ

01 サイバーセキュリティインシデントの特徴

02 サイバー攻撃の実態

03 サイバー攻撃の目的とメカニズム

04 代表的なサイバー攻撃の手法

05 中小企業における対策のポイント

© MS&AD InterRisk Research & Consulting, Inc.

本日のアジェンダ

01 サイバーセキュリティインシデントの特徴

02 サイバー攻撃の実態

03 サイバー攻撃の目的とメカニズム

04 代表的なサイバー攻撃の手法

05 中小企業における対策のポイント

© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティとは？

- 電子データの漏えい・改ざん等や、期待されていた IT システムや制御システム等の機能が果たされないといった不具合が生じないようにすること。

- 簡単に言うと、インターネットやパソコン、スマートフォンなどを
  安全に利用するための対策や技術のことです。
  コンピュータウィルスや不正アクセスによるサイバー攻撃の危険から、個人や企業のデータやシステムを守る役割があります。

出典：「サイバーセキュリティ経営ガイドライン Ver 3.0」 2023年3月24日（経済産業省・独立行政法人情報処理推進機構）を参考に弊社が作成
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティインシデントとは？

- インシデント(Incident)とは「出来事」「事件」という意味

- コンピュータやネットワークにおいて、
  「情報が危険にさらされた」「セキュリティ上の問題が起きた」ことを
  サイバーセキュリティインシデントと呼びます。

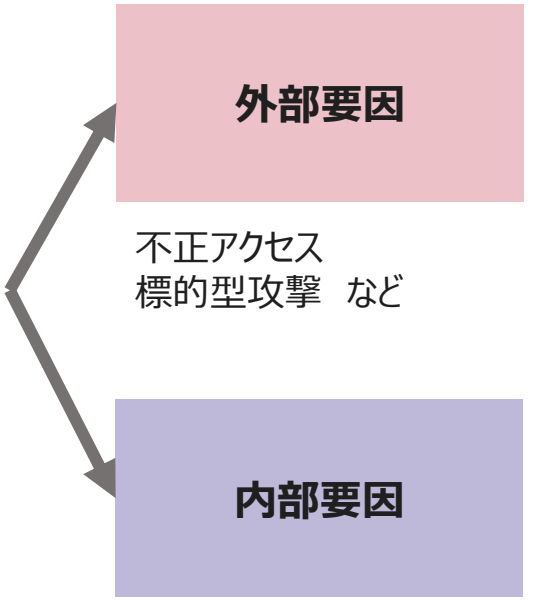
- 例えば、次のようなことが起きた場合です。
  ✓ マルウェア（コンピュータウィルス等）に感染させられる
  ✓ 不正アクセスされる
  ✓ 個人情報等の重要データが
  　漏れる、盗まれる、紛失する、消される、改ざんされる　など

© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティインシデントの特徴

サイバーセキュリティインシデントの発生要因は様々であり、発生時に何が起こるかあらかじめ予測がつかない。

- 情報システム・サービスの妨害
  （例）インターネットバンキングが動かない！
- 機器の物理的な損壊
  （例）過剰なCPU負荷によりサーバーが熱暴走！
- 情報漏えい
  （例）営業秘密がライバル組織に漏れている！
- 情報改ざん
  （例） HPを改ざんされ、ウィルスを埋め込まれていた！



何が起きているか、次何が起こるのか、ぱっとわからない。

© MS&AD InterRisk Research & Consulting, Inc.

本日のアジェンダ

01 サイバーセキュリティインシデントの特徴

02 サイバー攻撃の実態

03 サイバー攻撃の目的とメカニズム

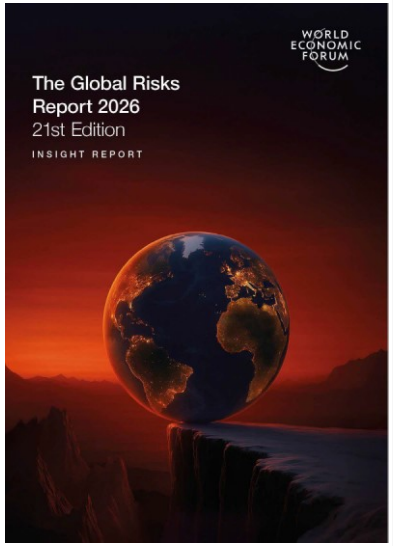
04 代表的なサイバー攻撃の手法

05 中小企業における対策のポイント

© MS&AD InterRisk Research & Consulting, Inc.

世界経済フォーラム「グローバルリスク報告書2026年版」

- 短期(2年間)に発生しうる深刻なグローバルリスクでは、2位に「**誤情報と偽情報**」、6位に「**サイバー不安**」がランクイン
- 長期(10年間)では、4位に「誤情報と偽情報」、8位に「サイバー不安」、また5位には「**AI技術の悪影響**」が挙げられている。



	Short term (2 years)	Long term (10 years)
1.	Geoeconomic confrontation	Extreme weather events
2.	Misinformation and disinformation	Biodiversity loss and ecosystem collapse
3.	Societal polarization	Critical change to Earth systems
4.	Extreme weather events	Misinformation and disinformation
5.	State-based armed conflict	Adverse outcomes of AI technologies
6.	Cyber insecurity	Natural resource shortages
7.	Inequality	Inequality
8.	Erosion of human rights and/or of civic freedoms	Cyber insecurity
9.	Pollution	Societal polarization
10.	Involuntary migration or displacement	Pollution

出典：世界経済フォーラム「グローバルリスク報告書2026年版」

© MS&AD InterRisk Research & Consulting, Inc.

IPA情報セキュリティ10大脅威　過去5年の推移

社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約200名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものをIPAが毎年公表している。

	2022	2023	2024	2025	2026
1位	ランサムウェアによる被害	ランサムウェアによる被害	ランサムウェアによる被害	ランサム攻撃による被害	ランサム攻撃による被害
2位	標的型攻撃による機密情報の窃取	サプライチェーンの弱点を悪用した攻撃	サプライチェーンの弱点を悪用した攻撃	サプライチェーンや委託先を狙った攻撃	サプライチェーンや委託先を狙った攻撃
3位	サプライチェーンの弱点を悪用した攻撃	標的型攻撃による機密情報の窃取	内部不正による情報漏えい	システムの脆弱性を突いた攻撃	AIの利用をめぐるサイバーリスク
4位	テレワーク等ニューノーマルな働き方を狙った攻撃	内部不正による情報漏えい	標的型攻撃による機密情報の窃取	内部不正による情報漏えい等	システムの脆弱性を悪用した攻撃
5位	内部不正による情報漏えい	テレワーク等のニューノーマルな働き方を狙った攻撃	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	機密情報等を狙った標的型攻撃	機密情報を狙った標的型攻撃
6位	脆弱性対策情報の公開に伴う悪用増加	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	不注意による情報漏えい等の被害	リモートワーク等の環境や仕組みを狙った攻撃	地政学的リスクに起因するサイバー攻撃（情報戦を含む）
7位	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	ビジネスメール詐欺による金銭被害	脆弱性対策情報の公開に伴う悪用増加	地政学的リスクに起因するサイバー攻撃	内部不正による情報漏えい等
8位	ビジネスメール詐欺による金銭被害	脆弱性対策情報の公開に伴う悪用増加	ビジネスメール詐欺による金銭被害	分散型サービス妨害攻撃（DDoS攻撃）	リモートワーク等の環境や仕組みを狙った攻撃
9位	予期せぬIT基盤の障害に伴う業務停止	不注意による情報漏えい等の被害	テレワーク等のニューノーマルな働き方を狙った攻撃	ビジネスメール詐欺	DDoS攻撃（分散型サービス妨害攻撃）
10位	不注意による情報漏えい等の被害	犯罪のビジネス化（アンダーグラウンドサービス）	犯罪のビジネス化（アンダーグラウンドサービス）	不注意による情報漏えい等	ビジネスメール詐欺

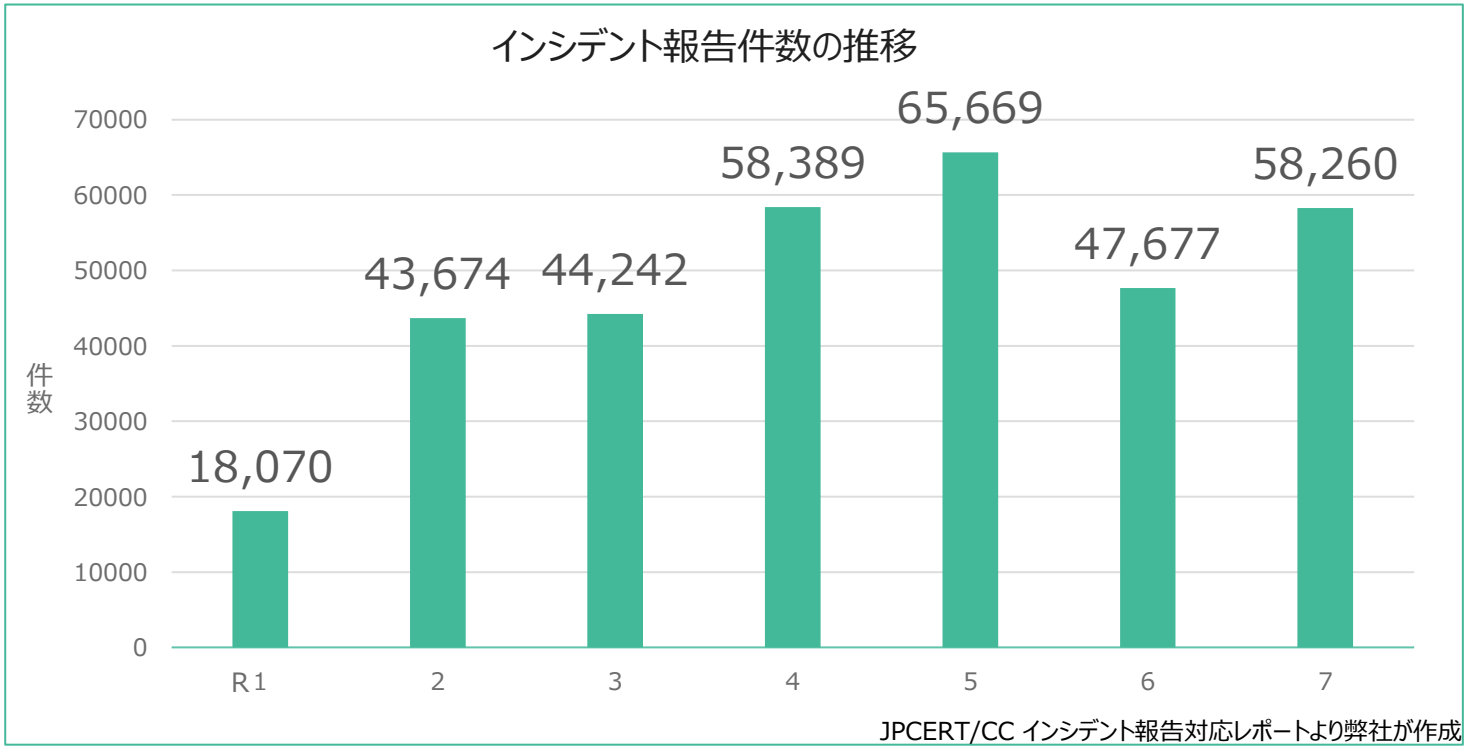
出典：「情報セキュリティ10大脅威 2026」2026年1月29日公開（独立行政法人情報処理推進機構）より弊社が作成
https://www.ipa.go.jp/security/10threats/10threats2026.html

情報セキュリティには様々な脅威が存在

© MS&AD InterRisk Research & Consulting, Inc.

サイバーインシデント報告件数の推移

インシデント(※1)等の報告を受け付けるJPCERT/CC (※2)に向けた報告件数



JPCERT/CC インシデント報告対応レポートより弊社が作成

※1 インシデント … インシデントとは英語で「出来事」「事件」の意味で、セキュリティインシデントは企業や組織が情報セキュリティに関する事故や攻撃などに遭うこと。具体的には、マルウェアの感染やコンピューターへの不正アクセス、従業員の不正による情報漏えい等を指す。

※2 JPCERT/CC … Japan Computer Emergency Response Team Coordination Center　JPCERTコーディネーションセンターはインターネットを介して発生する侵入やサービス妨害等のインシデントについて、日本国内に関するインシデント等の報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行っている。

2019年(令和元年)比では約3倍で推移

© MS&AD InterRisk Research & Consulting, Inc.

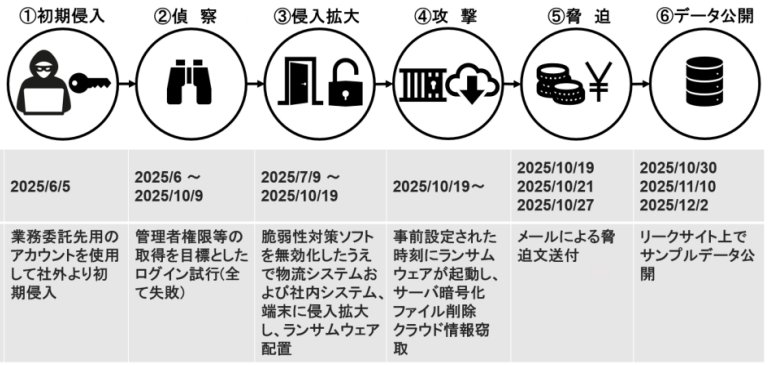
最近発生したサイバー・セキュリティインシデント事例

日付	業種	事例
2025年 4月	IT関連	法人向けメールセキュリティサービス設備がサイバー攻撃を受け、メールアカウント・パスワード、メール本文・ヘッダ情報、他社クラウド連携認証情報、あわせて**586契約・約31万件の情報漏洩**が発生した。調査の結果、2024年8月頃から不正アクセスが行われ、不正プログラムが動作していたことが判明した。この不正アクセスは、第三者製メールシステムのバッファオーバーフロー脆弱性が悪用されたもので、本事例が発覚するまでの間は**知られていない脆弱性が悪用された、いわゆるゼロデイ攻撃**によるものであった。
2025年 夏頃	証券 会社	**フィッシング等**により窃取したと思われるログインID・パスワードを用いて、証券会社のインターネット取引サービスへの不正アクセス・不正ログインが急増している。 被害口座内の株式等を勝手に売却し、その売却代金で**国内外の小型株を買い付けることにより株価操縦を試みる攻撃**手法が主流。金融庁によれば、5月までに10,000件を超える不正アクセス、売買合わせて5,000億円以上の不正取引が報告されている。

（報道記事等をもとに、ＭＳ＆ＡＤインターリスク総研にて作成）

© MS&AD InterRisk Research & Consulting, Inc.

最近発生したサイバー・セキュリティインシデント事例

日付	業種	事例
2025年 9月	食品	• サイバー攻撃によるシステム障害が発生し、**国内グループ各社の受注・出荷を含めた各種業務に影響**が生じ、社外からの電子メール受信も不可能となった • 攻撃者はネットワーク機器を経由してデータセンターのネットワークに侵入し、ランサムウエアが一斉に実行され、ネットワークに接続する範囲で起動中の複数のサーバーや一部のパソコン端末のデータが暗号化されたことが判明 • データセンターを通じて、従業員に貸与している一部のパソコン端末のデータが流出 • データセンターにあるサーバー内に保管されていた個人情報も流出の可能性あり • **流出したデータは約190万件**（流出のおそれ含む）
2025年 10月	小売	• ランサムウェアによる攻撃を受け、**すべての受注・出荷業務を停止**した • 調査の結果、一部データ（バックアップデータを含む）が暗号化されて使用不能になるとともに、当該データの一部が攻撃者により窃取、公開（流出）されたことが判明 • **流出したデータは約74万件**（流出のおそれ含む） 

（報道記事、プレスリリース等をもとに、ＭＳ＆ＡＤインターリスク総研にて作成）

© MS&AD InterRisk Research & Consulting, Inc.

最近発生したサイバー・セキュリティインシデント事例（福島県内）

日付	業種	事例
2017年 8月 発生 2020年 12月 公表	病院	県内公立病院の複数の部署において、**ランサムウェアの亜種のマルウェア**（暗号化や脅迫文を表示する機能を有さない）が原因と疑われる検査装置の不具合が発生した。そのうち、放射線撮影装置の不具合により放射線画像の再撮影を行うことになった事案が2例あった。 ・CT撮影中に**管理端末が再起動**し撮影画像の保存に失敗 ・胸部撮影の**フイルム画像読み取り装置が再起動**し読み取りに失敗 **当時、被害発生を公表せず、厚生労働省にも報告していなかった。** 2020年になって厚生労働省からウイルス関連の影響による医療情報消失事案の照会があり、当該の2件が該当することが判明。公表および当該の患者に対する事案の説明と謝罪が行われた。

（報道記事、プレスリリース等をもとに、ＭＳ＆ＡＤインターリスク総研にて作成）

© MS&AD InterRisk Research & Consulting, Inc.

最近発生したサイバー・セキュリティインシデント事例（福島県内）

日付	業種	事例
2024年 7月	印刷	県内公立学校及び幼稚園の卒業・卒園アルバム制作に関する委託先印刷会社（仙台市）が**ランサムウェア**の被害を受けた。調査の結果、テキスト（**個人名**・委員会クラブなど）のデータ、個別の写真（**顔写真**・スナップ）及び校名を含む紙面構成データの**漏えいのおそれ**があることが判明した。 2024年7月に異常を検知、9月よりデジタル鑑識調査（デジタルフォレンジック調査）開始、2025年4月に宮城県警サイバー犯罪対策課へ被害を届け出た。
2024年 11月	イベント企画	県内自治体がイベント運営業務を外部事業者に委託していたところ、 委託先事業者の再委託先（仙台市）が**ランサムウェア**の被害を受けた。 当該サーバーには、**イベント申込者の情報：1,513 件**（氏名、性別、学年、保護者氏名、住所、電話番号、メールアドレス）が保管されていた。 当該再委託先事業者はイベント当選者情報（516件）を送付する際、宛先**メールアドレスの入力ミスにより誤って第三者に送信**する事象も発生させた。
2025年 8月	商工会	県内商工会職員が**サポート詐欺**に遭い、有名IT企業の社員を騙る攻撃者の指示により業務用PC1台が遠隔操作され、預金口座から**3回にわたり計390万円を不正送金された。** 攻撃者は個人情報が保存されているファイルサーバーにも接続できる状態となっていたが、その後の調査で個人情報の漏えいは確認されなかった。

（報道記事、プレスリリース等をもとに、ＭＳ＆ＡＤインターリスク総研にて作成）

© MS&AD InterRisk Research & Consulting, Inc.

社会・企業全体において
サイバーセキュリティ対策の重要性が高まっている

企業を取り巻く環境・サイバー攻撃による脅威は
日々変化している

© MS&AD InterRisk Research & Consulting, Inc.

本日のアジェンダ

01 サイバーセキュリティインシデントの特徴

02 サイバー攻撃の実態

03 サイバー攻撃の目的とメカニズム

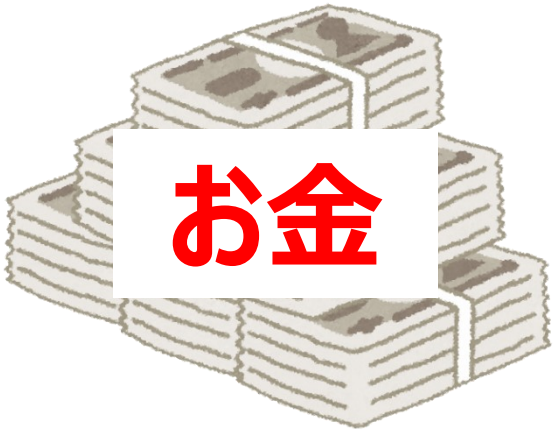
04 代表的なサイバー攻撃の手法

05 中小企業における対策のポイント

© MS&AD InterRisk Research & Consulting, Inc.

サイバー攻撃の目的と、標的となる企業

サイバー攻撃の目的は愉快犯、能力の誇示、政治目的など様々あるが、近年では「お金」が主な目的である。サイバー攻撃者は、大企業だけでなく、その周辺の取引先を踏み台とするなど、標的とする企業をすべての企業に拡大している。

サイバー攻撃(例)	サイバー犯罪の目的
(Webなど)不正な改ざん	愉快・欲求
フィッシング攻撃	
ランサムウェアによる攻撃	
DDoS攻撃	
機密情報の盗聴	
APT攻撃	政治・社会的主張

狙われる企業は？

- 大企業
- 高価格で転売可能な秘密を持つ企業
- 大企業と取引のある**<u>すべての企業</u>**

© MS&AD InterRisk Research & Consulting, Inc.

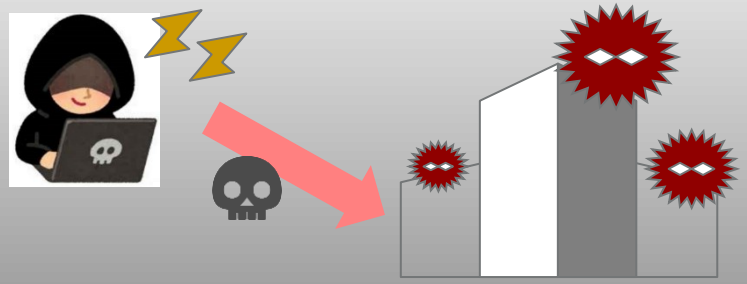
攻撃のメカニズム　サイバーキルチェーン

攻撃者は、公開情報等よりターゲット企業の脆弱性情報を収集して侵入を試みる。
社内ネットワークに侵入後、権限昇格等を繰り返し足場を固めた上で、攻撃を実施する。

偵察 → 配信 → エクスプロイト → インストール → コマンド＆コントロール → 感染活動 → 目的実行

© MS&AD InterRisk Research & Consulting, Inc.

サイバー攻撃を受けると発生しうる被害・損失



- 重要情報・個人情報が漏えいする
- データが改ざんされる、滅失する
- システムが停止、破壊される

- 原因究明、対策のためのコンサル費用
- データ、システム復旧のための費用
- 事業中断による金銭的被害
- 賠償請求による金銭的被害
- レピュテーション低下
- 将来的な事業展開／継続の障害

© MS&AD InterRisk Research & Consulting, Inc.

「お金」を目的にあらゆる企業が狙われている

サイバー攻撃の被害は多岐に渡る可能性がある

© MS&AD InterRisk Research & Consulting, Inc.

本日のアジェンダ

01 サイバーセキュリティインシデントの特徴

02 サイバー攻撃の実態

03 サイバー攻撃の目的とメカニズム

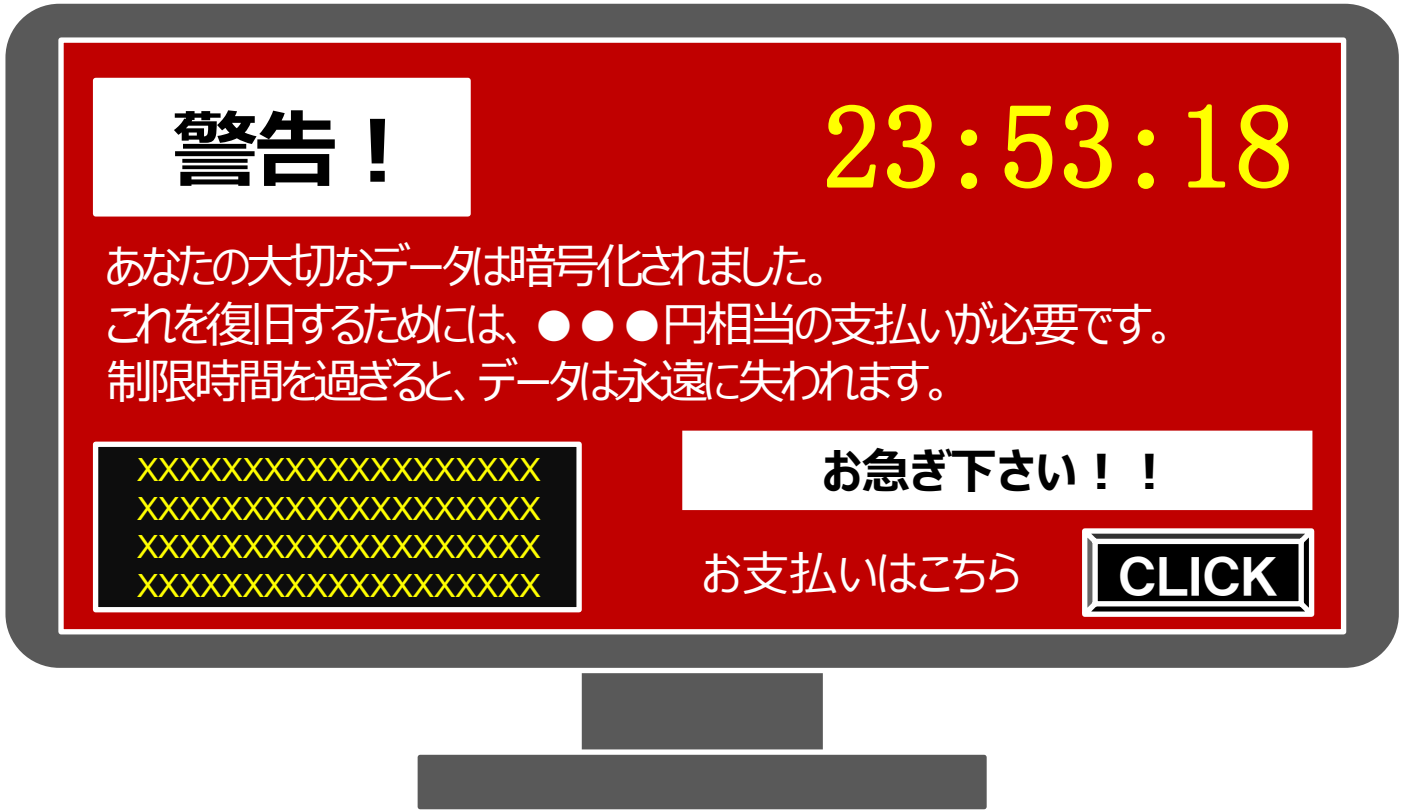
04 代表的なサイバー攻撃の手法

05 中小企業における対策のポイント

© MS&AD InterRisk Research & Consulting, Inc.

ランサムウェア攻撃

ランサムウェア攻撃とは、VPN機器や電子メールなどを通じて侵入して、PCをロックして使用不能にしたり、PC内のファイルを暗号化することにより参照・使用不能にした後で、元に戻すことと引き換えに「身代金（Ransom）」を要求する不正プログラムを指す。



© MS&AD InterRisk Research & Consulting, Inc.

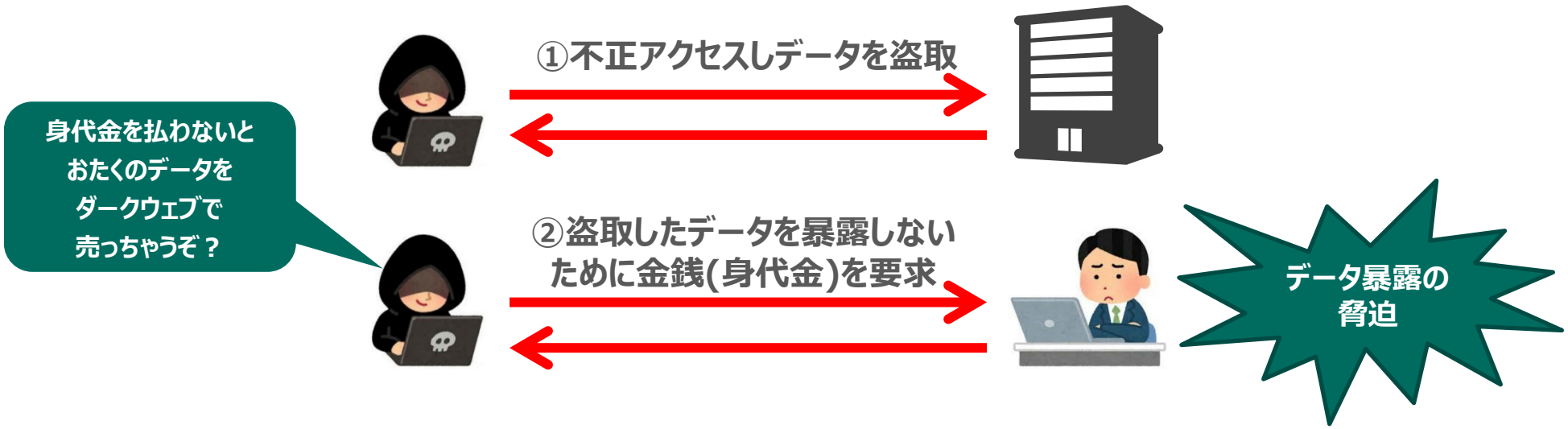
ランサムウェア攻撃 二重の脅迫

近年は、予め重要情報を盗取した上でその情報を暗号化をし、使用可能な状態に復号することと、盗取した情報を第三者に暴露しないことの両方で身代金を要求する「二重の脅迫」が行われる。身代金の支払いを拒否すると、盗取した重要情報をダークウェブ等で暴露される。

© MS&AD InterRisk Research & Consulting, Inc.

ノーウェア（非暗号化型）ランサム攻撃

さらに最近では、暗号化することなくデータの盗取のみを行い、盗取した重要情報を第三者に暴露しないことに対する身代金のみを要求する「ノーウェア（非暗号化型）ランサム」という攻撃手法も見られる。暗号化を行わないため、**攻撃にかかる時間が短く、検知が難しい**という特徴がある。

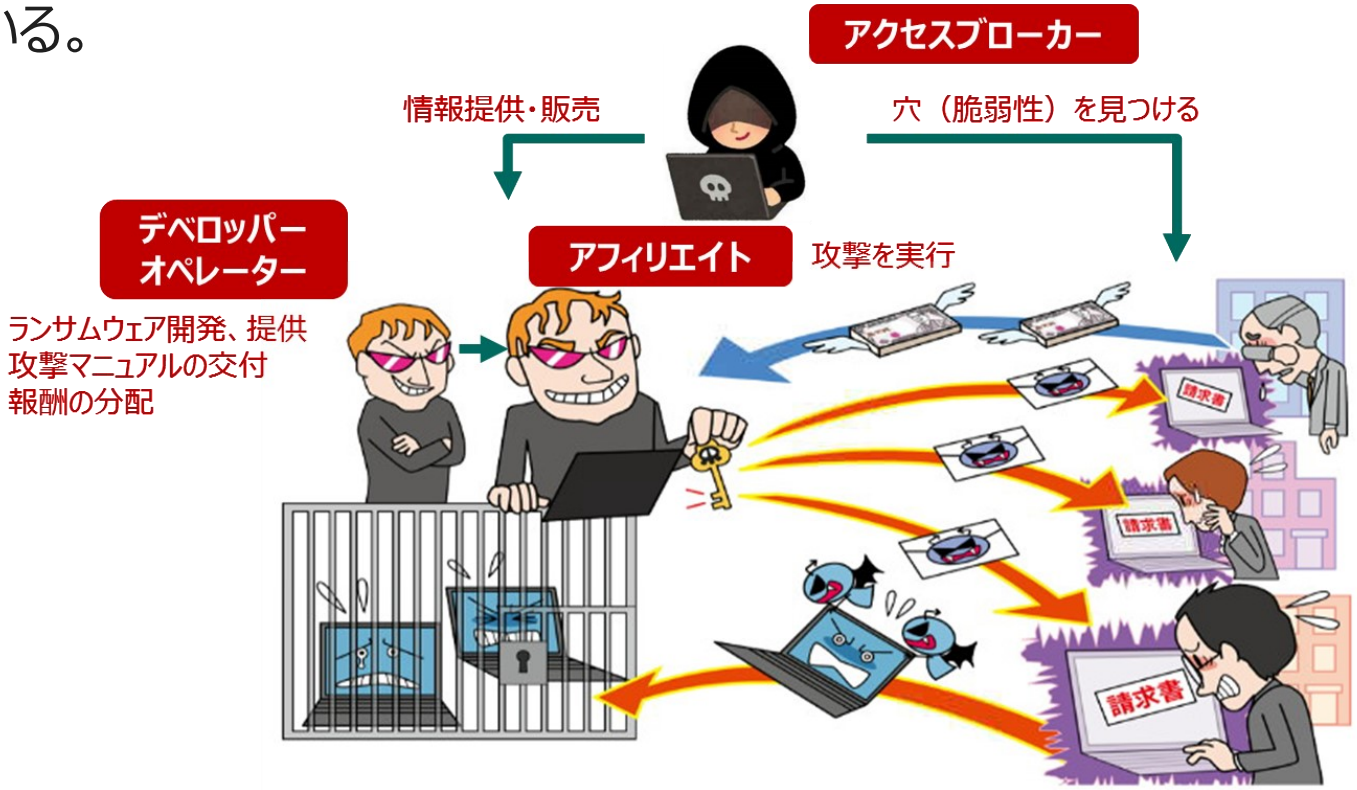


© MS&AD InterRisk Research & Consulting, Inc.

ランサムウェア攻撃 犯罪エコシステムの成長

ランサムウェア攻撃は高度化・分業化が進んでおり、「RaaS（Ransomware as a Service）」と呼ばれる、特殊詐欺集団と同じような組織形態が確立している。

そのため、ソフトウェア開発等の詳しいノウハウを持たずともランサムウェア攻撃が可能になっている。



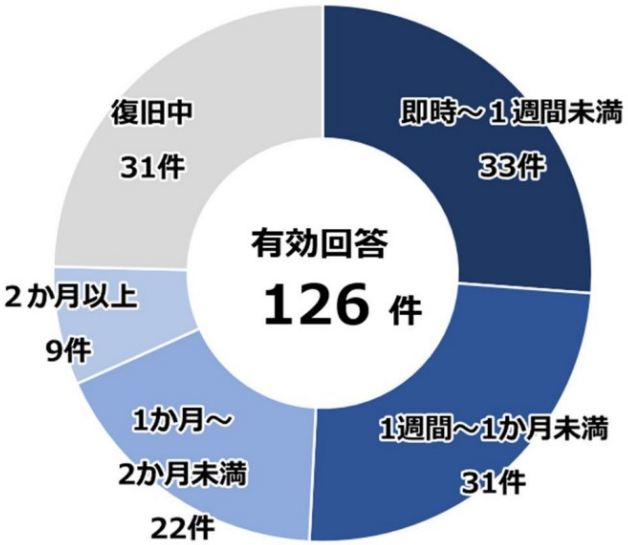
出典：「情報セキュリティ10大脅威」IPAをもとに弊社が加工

© MS&AD InterRisk Research & Consulting, Inc.

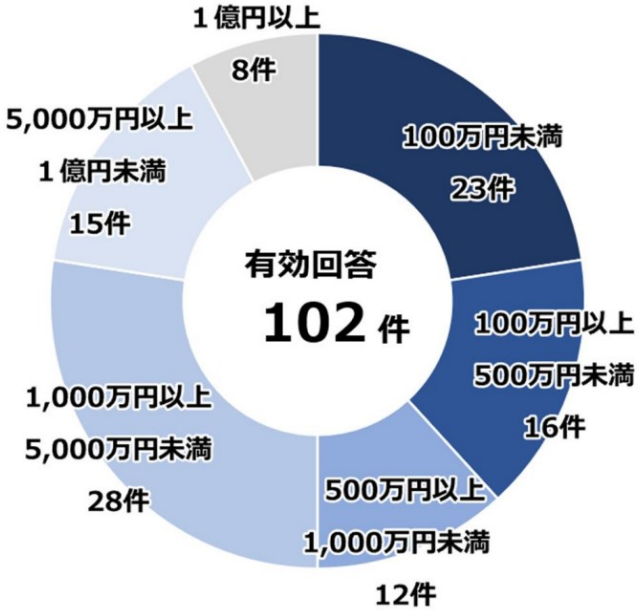
ランサムウェアによる被害（警察庁公表資料）

ランサムウェアに感染した企業のうち、約半数が復旧に「1週間以上」、約25%が「1か月以上」を要しており、被害額も約半数が「1,000万円以上」、約23%が「5,000万円以上」となっている。
また、組織の規模によらず多くの被害が報告されている。

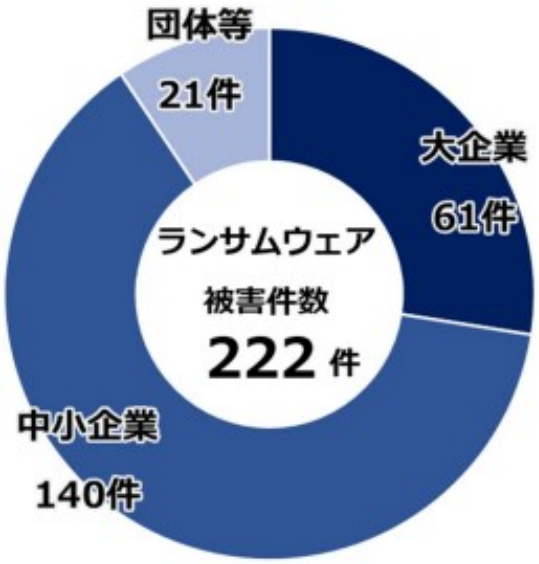
復旧に要した時間



被害額



規模別報告件数



**ランサムウェア被害をはじめとするサイバー攻撃は事業継続に
長期的な影響を与える可能性があり、経営マターで対策を検討することが重要**

警察庁公表資料(https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf)から当社が一部加工

© MS&AD InterRisk Research & Consulting, Inc.

○×クイズ

ランサムウェアに感染する
最大の原因は**メール**？

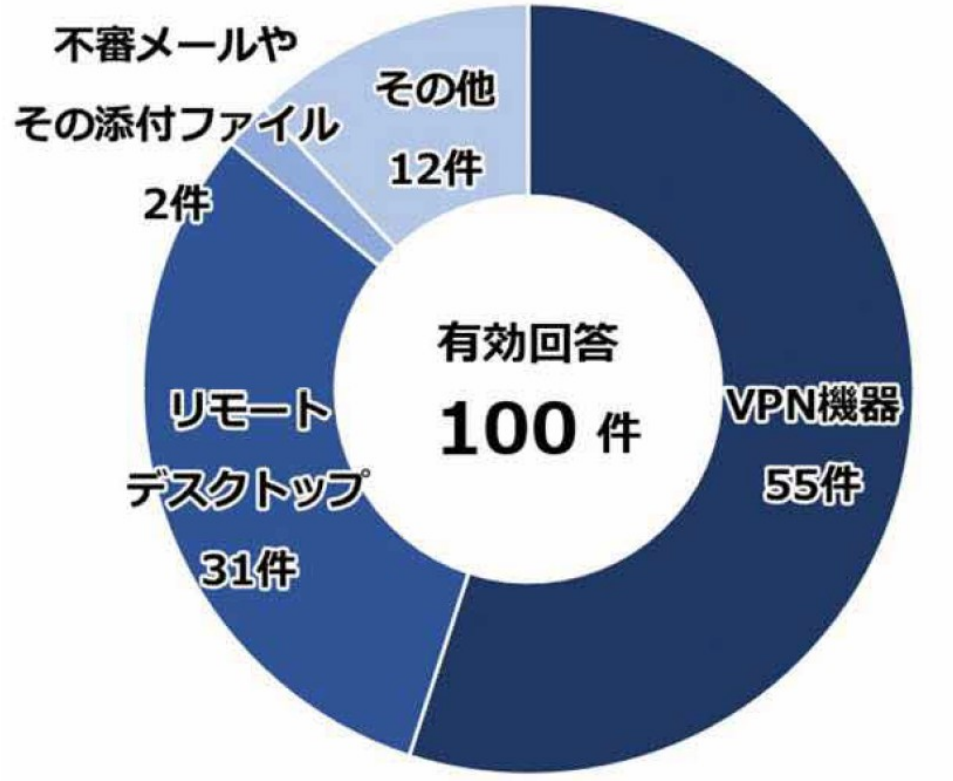
© MS&AD InterRisk Research & Consulting, Inc.

○×クイズ

© MS&AD InterRisk Research & Consulting, Inc.

ランサムウェアの感染原因

- ランサムウェアに感染する原因の多くはVPN機器等からの侵入です。
- ただし侵入に至るまでの準備活動として、メールを利用した攻撃による感染やアカウント情報の窃取はありえます。

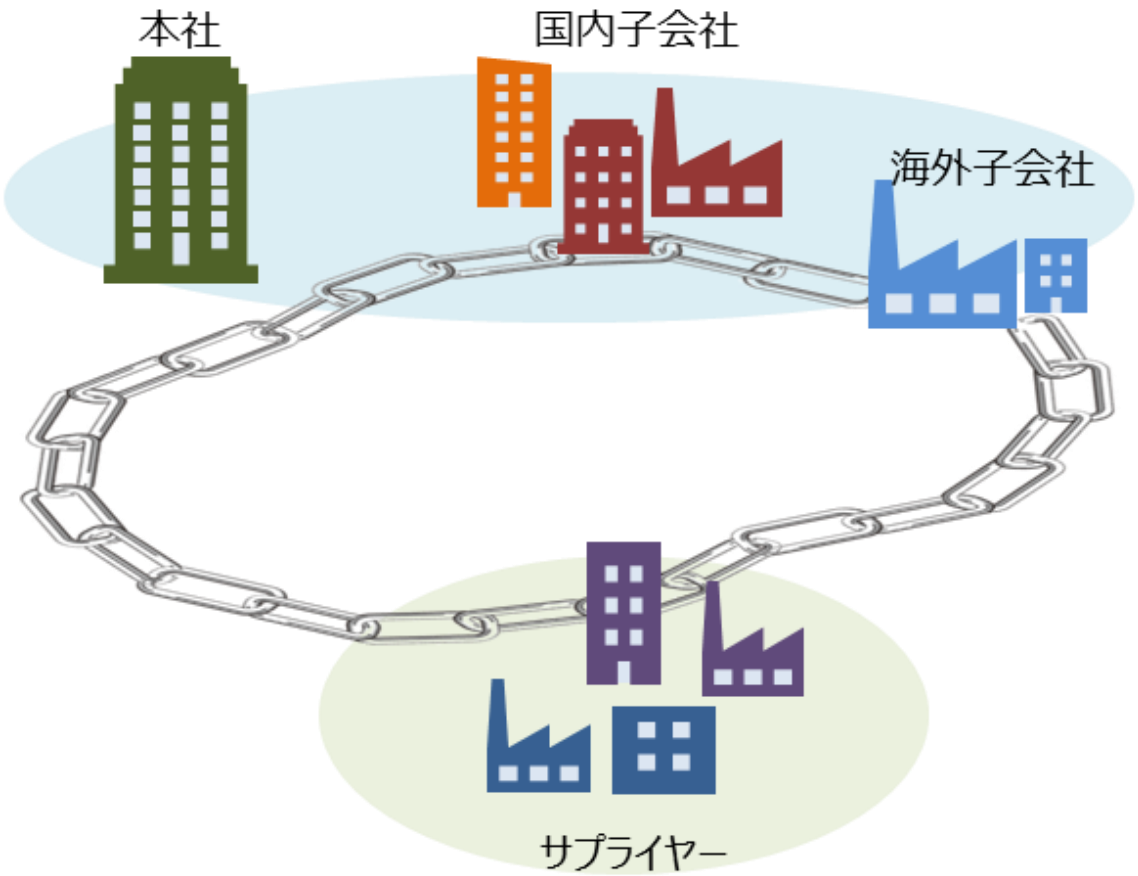


出典：「令和6年におけるサイバー空間をめぐる脅威の情勢等について」2025年3月13日公開（警察庁）

© MS&AD InterRisk Research & Consulting, Inc.

サプライチェーン攻撃とは

サプライチェーン攻撃とは、まずはサプライチェーン上でセキュリティ対策が進んでいない企業をターゲットに攻撃し、その結果またはそれを契機に大企業や本社に直接的・間接的に被害を与える攻撃を指す。



© MS&AD InterRisk Research & Consulting, Inc.

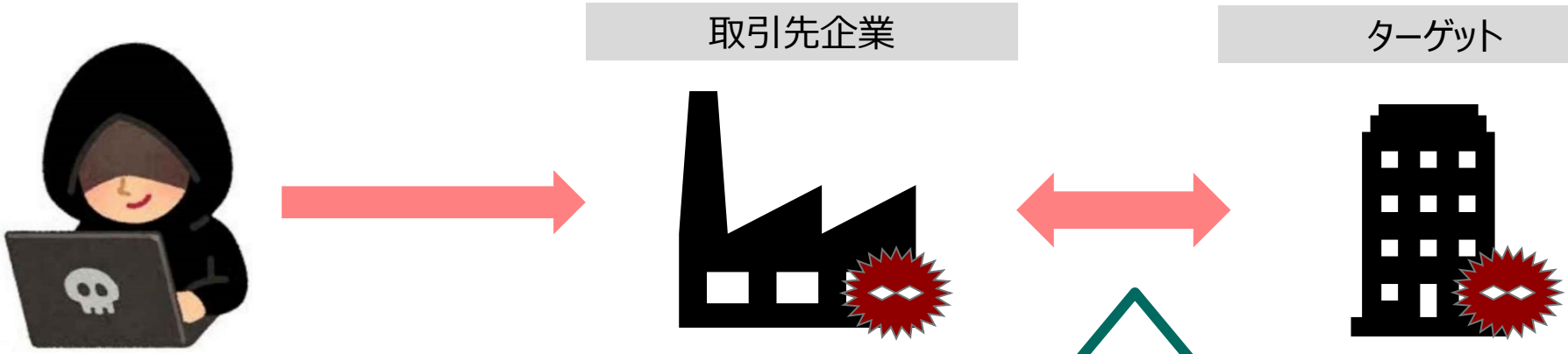
サプライチェーン攻撃とは　VPN機器を通じた侵入

修正パッチが適用されていない、VPN機器の脆弱性を悪用した攻撃が増加しており、サプライチェーン全体でセキュリティ対策の実施状況を確認する必要がある。

攻撃①
取引先企業が利用しているネットワーク情報を分析して、攻撃可能な脆弱性を特定

攻撃②
取引先企業が利用しているVPN機器の脆弱性を悪用して、取引先企業ネットワークに侵入

攻撃③
ターゲット企業に侵入し、ランサムウェア攻撃の実施
⇒システムが稼働停止



取引先企業とターゲット企業間には、ネットワーク上のつながりが存在
⇒サプライチェーンを起点にターゲットに侵入成功

© MS&AD InterRisk Research & Consulting, Inc.

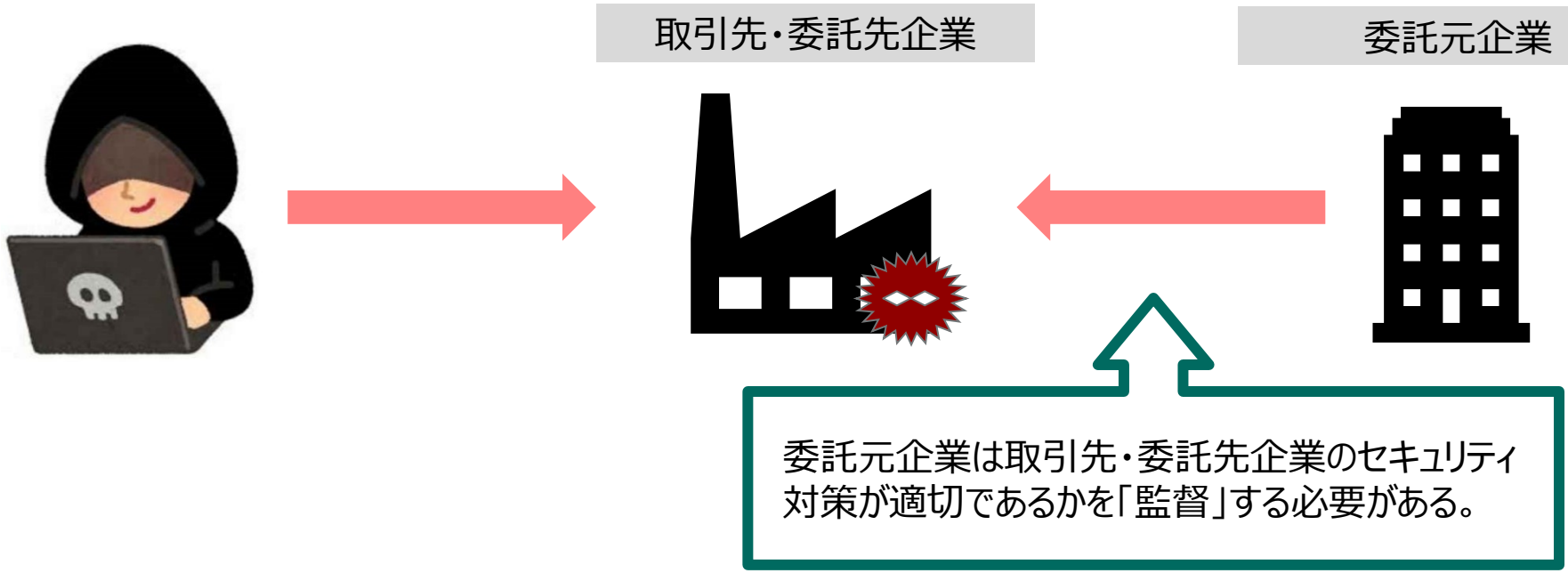
サプライチェーン攻撃とは　取引先・委託先経由の情報漏えい

取引先・委託先企業がサイバー攻撃を受けて、委託元企業の情報が漏えいした場合、委託元企業に顧客（エンドユーザー）への説明責任が発生する。

攻撃①
取引先・委託先企業が抱える
セキュリティ上の脆弱性を
狙い攻撃

攻撃②
取引先・委託先企業が
ランサムウェア等に感染して、
情報漏えい

影響
取引先・委託先経由で自社の
情報が漏えいした際、委託元
企業が顧客対応を行う



© MS&AD InterRisk Research & Consulting, Inc.

テクニカルサポート詐欺

正規のサポートを装った詐欺。本物に見せかけたセキュリティ警告が表示され、電話をかけると、オペレーターにパソコンを遠隔操作され有償サポート契約と代金支払いへ誘導される。

表示されている電話番号にかけると
偽のサポートセンターにつながる

IPA　偽セキュリティ警告（サポート詐欺）の月間相談件数が過去最高に　から当社が一部加工
https://www.ipa.go.jp/security/anshin/attention/2022/mgdayori20230228.html

© MS&AD InterRisk Research & Consulting, Inc.

とある西洋料理店にて

「帽子と外套と靴をおとり下さい。」
「壺のなかのクリームを顔や手足にすっかり塗ってください。」
「あなたの頭に瓶の中の香水をよく振りかけてください。」
「どうかからだ中に、壺の中の塩をたくさんよくもみ込んでください。」

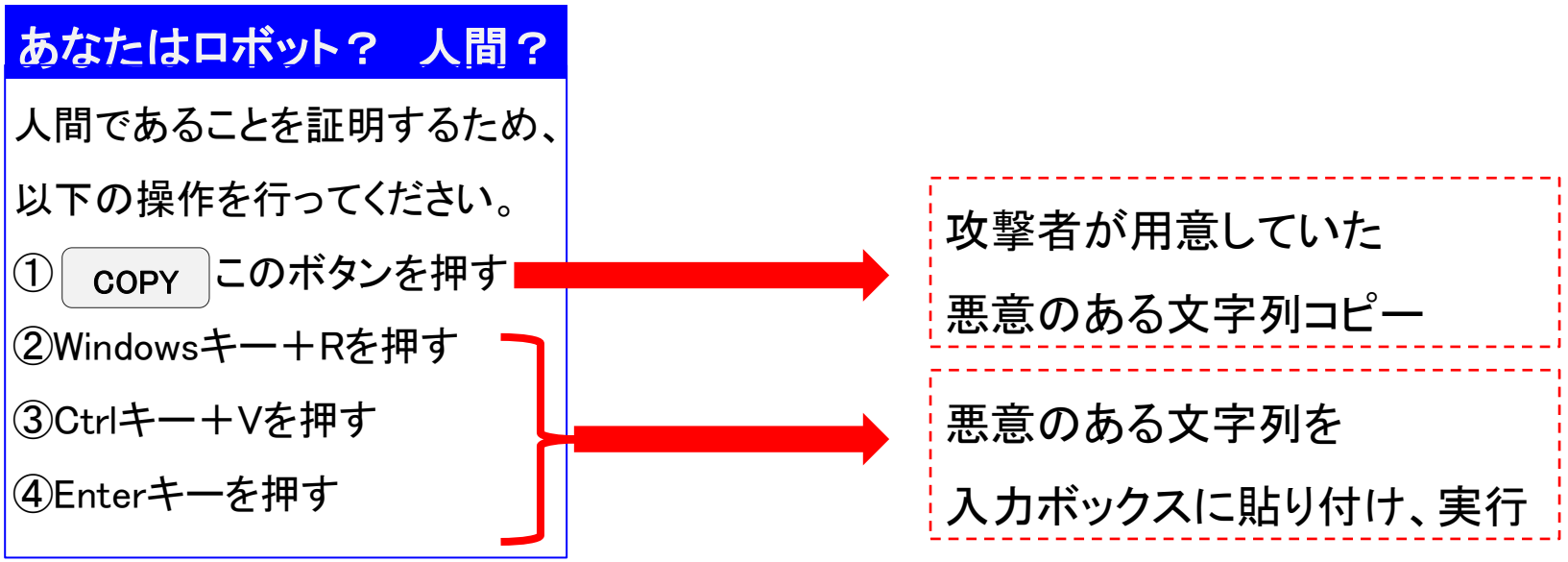
「これから火を起してフライにしてあげましょうか。」

意味を理解せずに言われたとおりにすると危ない！

© MS&AD InterRisk Research & Consulting, Inc.

ClickFix

- ユーザー自身に情報漏えいやパソコンを故障させる操作を実行させる攻撃手法。
- 以下の例のように、画面の指示通り操作をすると、
  自分の手でマルウェア（コンピュータウィルス等）をインストールしてしまう。



ショートカットキーやコマンド入力の要求に注意
意味を理解せずに表示したとおりに操作すると危ない！

© MS&AD InterRisk Research & Consulting, Inc.

代表者を騙るメール詐欺

理事長
（を騙るサイバー犯罪者）

件名　：　至急・極秘の送金依頼
差出人　：　理事長
本文　：　●●社と極秘のプロジェクトを進めている。M&Aに関わる話だ。
至急で資金が必要なので、対応してほしい。

件名：Re: 至急・極秘の送金依頼

理事長
お疲れ様です。経理のAです。
送金の件、内容によりますが可能な範囲で対応いたします。
詳細をご指示いただけますでしょうか。

経理担当者

件名：Re: 至急・極秘の送金依頼

先方は海外のM&A案件の相手先で、まだ**社内にも公表できない**段階だ。
この件は、**君と私だけの極秘**としたい。
まずは**テストとして、下記口座に 150,000 USD を送金**してほしい。

銀行名：XXXX BANK
支店名：LONDON BRANCH
口座番号：XXXXXXX
口座名義：ABC HOLDINGS LTD
本日中の送金が必須条件だ。他の役員にもこの件は話さないでほしい。

その「理事長」って、ホンモノですか？

© MS&AD InterRisk Research & Consulting, Inc.

ランサムウェア攻撃は巧妙化・汎用化が進む
サプライチェーンの仕組みを悪用される
事業規模問わず誰もが狙われる
手口は日々進化し続けている

© MS&AD InterRisk Research & Consulting, Inc.

本日のアジェンダ

01 サイバーセキュリティインシデントの特徴

02 サイバー攻撃の実態

03 サイバー攻撃の目的とメカニズム

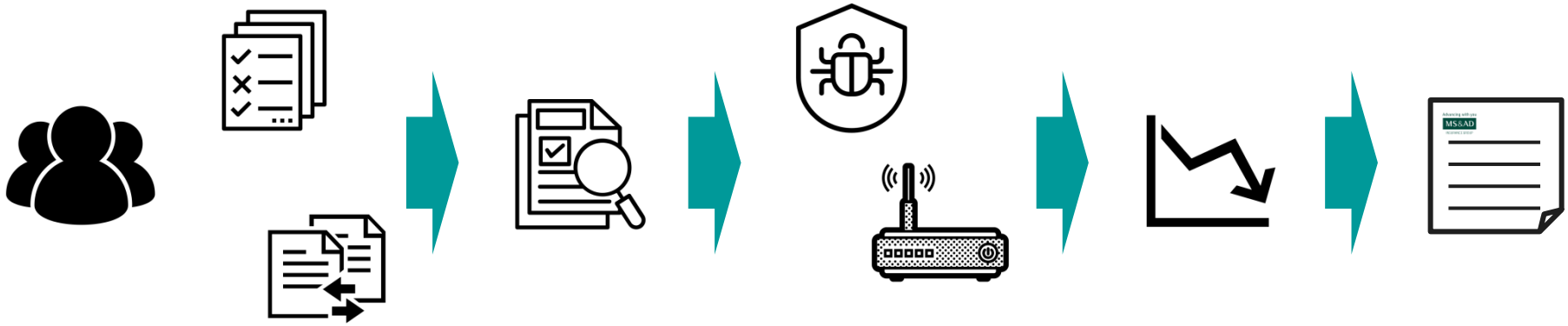
04 代表的なサイバー攻撃の手法

05 中小企業における対策のポイント

© MS&AD InterRisk Research & Consulting, Inc.

サイバーリスク対応体制整備の全体像

サイバー攻撃により被害を受けるリスクをコントロールできるよう
各フェーズ毎に対策案を検討する



組織体制整備	リスクの特定	防御・検知	対応・復旧	保険
・サイバーリスクは経営問題 ・経営の理解 ・対応組織を組成 **（組織体制整備）**	・ルールを定める ・情報資産を把握 ・脆弱性の洗い出し ・対策の優先順位づけ ・リスクアセスメント **（リスクの特定）**	・境界防御 ・アクセス管理 ・マルウェア対策 ・ログ管理 ・イベント発生チェック **（防御・検知）**	・事前準備・訓練 ・初動対応 ・報告・公表 ・復旧事業者とのホットライン **（対応・復旧）**	・リスクはゼロにならないので保険をかける **（保険）**

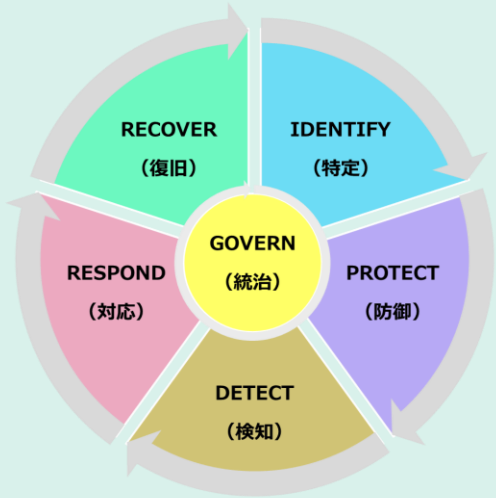
© MS&AD InterRisk Research & Consulting, Inc.

セキュリティ対策の重要性　各国のガイドライン

セキュリティ対策は「経営課題」が世界の共通認識

NIST（米）
サイバーセキュリティ
フレームワーク(CSF) 2.0

- 世界各国の組織が採用しているフレームワーク
- V2.0で新たに「統治」が要素として加わった



NCSC（英）
Cyber Governance
Code of Practice

- サイバーセキュリティリスクの管理を進める上で、取締役会や役員が責任を持つべき行動がコンパクトにまとめられている

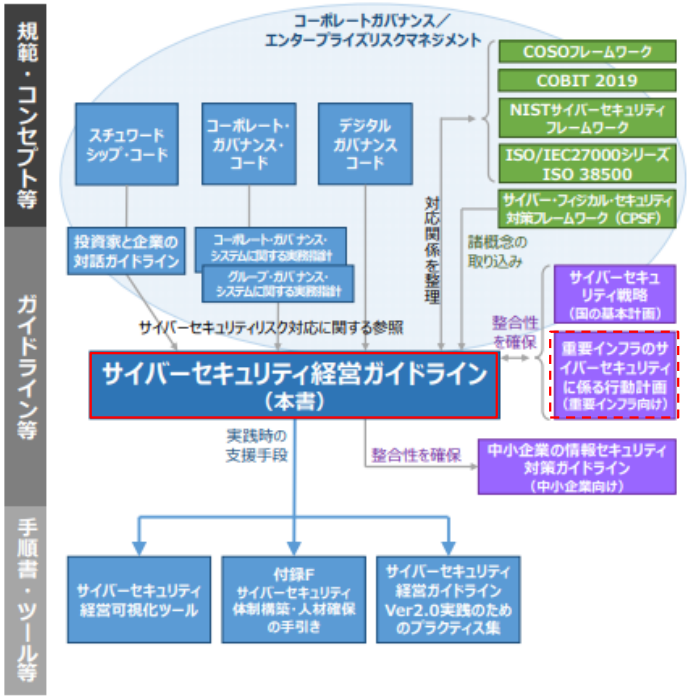
経済産業省
サイバーセキュリティ
経営ガイドライン

- サイバーセキュリティ対策を必要不可欠な「投資」と位置付け、経営層向けの「3原則」と「重要10項目」からなる

© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営ガイドライン

経済産業省は「サイバーセキュリティ経営ガイドライン」を策定。
大企業だけでなく、中小企業にとっても参考にできるガイドラインです。



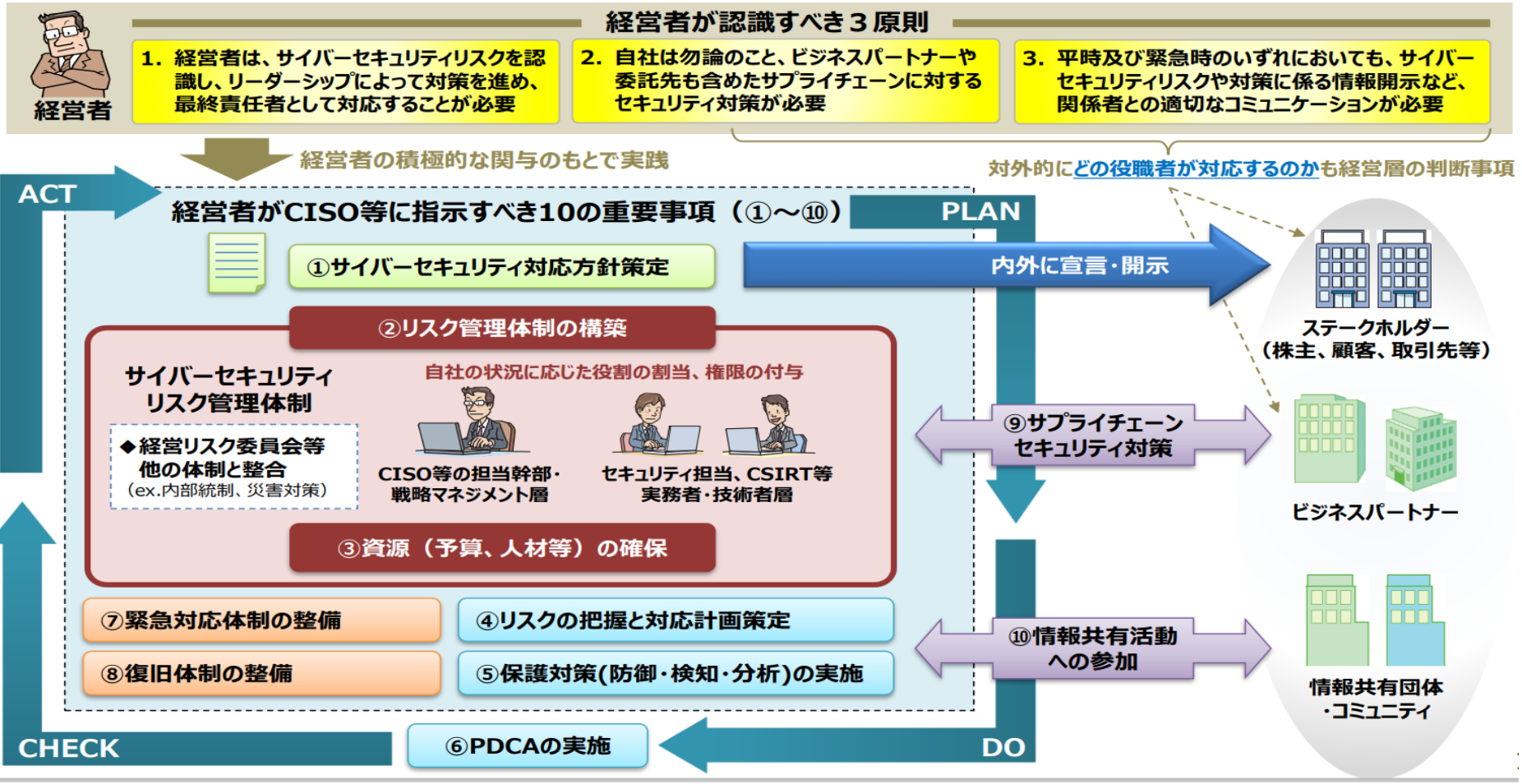
図：サイバーセキュリティ経営ガイドラインの体系
出典：経済産業省　サイバーセキュリティ経営ガイドライン Ver3.0　を基に作成
https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf

- ✓ 上場企業等と直接の取引がない中小企業であってもサプライチェーンを通じた間接的なつながりを持つ全ての企業において、リスクマネジメントが求められている。
- ✓ 具体的な手順やプラクティス（実践例）も充実。

© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営ガイドラインの全体像

本ガイドラインは**経営者を名宛人に、セキュリティ対策の重要性を説明**しており、
サイバーセキュリティ対策は、事業活動を行う上で必要不可欠な要素となっている。



出典：経済産業省・独立行政法人情報処理推進機構　サイバーセキュリティ経営ガイドライン　付録F概要版より引用
https://www.meti.go.jp/policy/netsecurity/tebikigaiyou2.pdf

© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営の重要10項目

■サイバーセキュリティリスクの管理体制構築
指示１：サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示２：サイバーセキュリティリスク管理体制の構築
指示３：サイバーセキュリティ対策のための資源（予算、人材等）確保

■サイバーセキュリティリスクの特定と対策の実装
指示４：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示５：サイバーセキュリティリスクに効果的に対応する仕組みの構築
指示６：PDCA サイクルによるサイバーセキュリティ対策の継続的改善

■インシデント発生に備えた体制構築
指示７：インシデント発生時の緊急対応体制の整備
指示８：インシデントによる被害に備えた事業継続・復旧体制の整備

■サプライチェーンセキュリティ対策の推進
指示９：ビジネスパートナーや委託先等を含めたサプライチェーン全体の
状況把握及び対策

■ステークホルダーを含めた関係者とのコミュニケーションの推進
指示10：サイバーセキュリティに関する情報の収集、共有及び開示の促進

© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営の重要10項目

■ **サイバーセキュリティリスクの管理体制構築**

指示１：サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示２：サイバーセキュリティリスク管理体制の構築
指示３：サイバーセキュリティ対策のための資源（予算、人材等）確保

■ サイバーセキュリティリスクの特定と対策の実装

指示４：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示５：サイバーセキュリティリスクに効果的に対応する仕組みの構築
指示６：PDCA サイクルによるサイバーセキュリティ対策の継続的改善

■ インシデント発生に備えた体制構築

指示７：インシデント発生時の緊急対応体制の整備
指示８：インシデントによる被害に備えた事業継続･復旧体制の整備

■ サプライチェーンセキュリティ対策の推進

指示９：ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策

■ ステークホルダーを含めた関係者とのコミュニケーションの推進

指示10：サイバーセキュリティに関する情報の収集、共有及び開示の促進

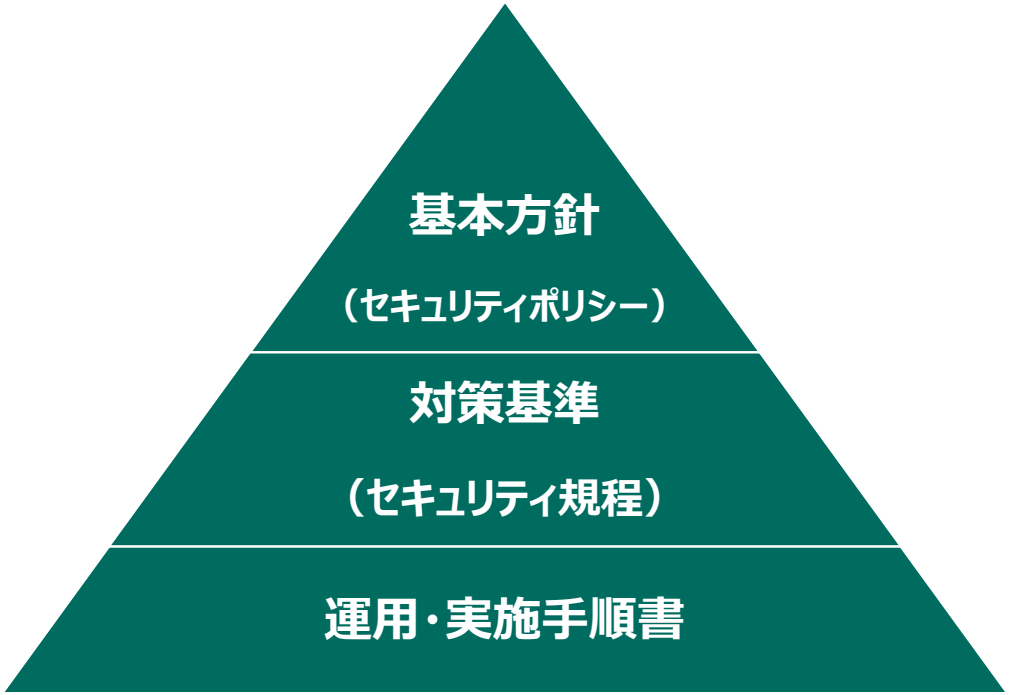
© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営の重要10項目（指示1）

指示１：サイバーセキュリティリスクの認識、組織全体での対応方針の策定

- ✓ サイバーセキュリティリスクを経営者が責任を負うべき経営リスクとして認識し、組織全体としての**対応方針（セキュリティポリシー）**を策定させる。
- ✓ 策定した対応方針を対外的な宣言として公表させる。

■基本方針(セキュリティポリシー)と規程類の関係



情報セキュリティに対する基本的な考え方・セキュリティ対策に取り組む理由を記載する。ミッションステートメントのようなイメージ

基本方針（セキュリティポリシー）を実践するために社内ルールを定める

対策基準（セキュリティ規程）を遵守するため必要に応じて手順書を用意する

© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営の重要10項目（指示2）

指示２：サイバーセキュリティリスク管理体制の構築

- ✓ サイバーセキュリティリスクの管理に関する**各関係者の役割と責任を明確にした上で、リスク管理体制を構築**させる。
- ✓ サイバーセキュリティリスクの管理体制の構築にあたっては、組織内のガバナンスや内部統制、その他のリスク管理のための体制との整合を取らせる。

■社内関係者の役割と責任の分担例

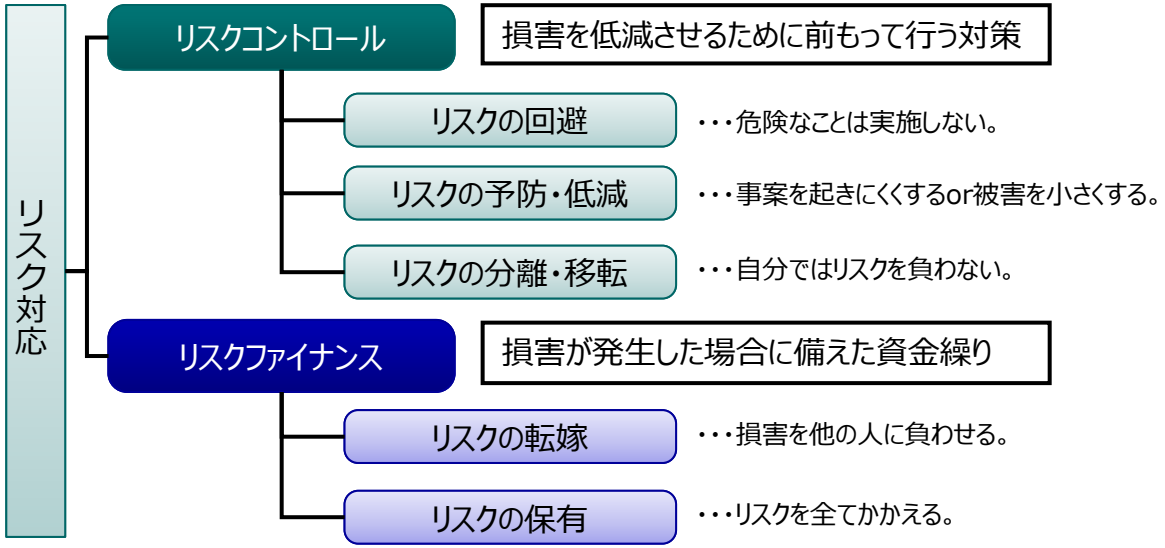
役職名	担当者	役割と責任
情報セキュリティ責任者	代表取締役社長	情報セキュリティ対策などの決定権限を有するとともに、全責任を負います。
情報セキュリティ部門責任者	○○事業部長	各部門における情報セキュリティの運用管理責任者です。各部門における情報セキュリティ対策の実施などの責任と権限を有します。
システム管理者	○○ ○○	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行います。
教育責任者	○○ ○○	情報セキュリティ対策を推進するために従業員への教育を企画・実施します。
点検責任者	○○ ○○	情報セキュリティ対策が適切に実施されているか点検します。

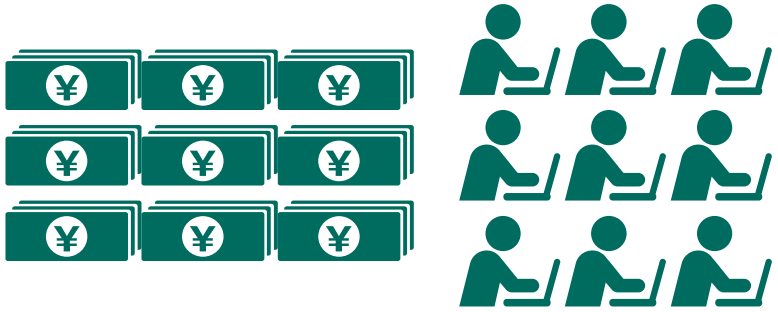
© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営の重要10項目（指示3）

指示３：サイバーセキュリティ対策のための資源（予算、人材等）確保

- ✓ サイバーセキュリティに関する**残存リスクを許容範囲以下に抑制**するための方策を検討させ、必要となる**資源（予算、人材等）を確保**した上で、具体的な対策に取り組ませる。
- ✓ 全ての役職員に自らの業務遂行にあたってセキュリティを意識させ、それぞれのサイバーセキュリティ対策に関する**スキル向上のための人材育成施策を実施**させる。





© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営の重要10項目

■サイバーセキュリティリスクの管理体制構築
指示１：サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示２：サイバーセキュリティリスク管理体制の構築
指示３：サイバーセキュリティ対策のための資源（予算、人材等）確保

■サイバーセキュリティリスクの特定と対策の実装
指示４：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示５：サイバーセキュリティリスクに効果的に対応する仕組みの構築
指示６：PDCA サイクルによるサイバーセキュリティ対策の継続的改善

■インシデント発生に備えた体制構築
指示７：インシデント発生時の緊急対応体制の整備
指示８：インシデントによる被害に備えた事業継続･復旧体制の整備

■サプライチェーンセキュリティ対策の推進
指示９：ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策

■ステークホルダーを含めた関係者とのコミュニケーションの推進
指示10：サイバーセキュリティに関する情報の収集、共有及び開示の促進

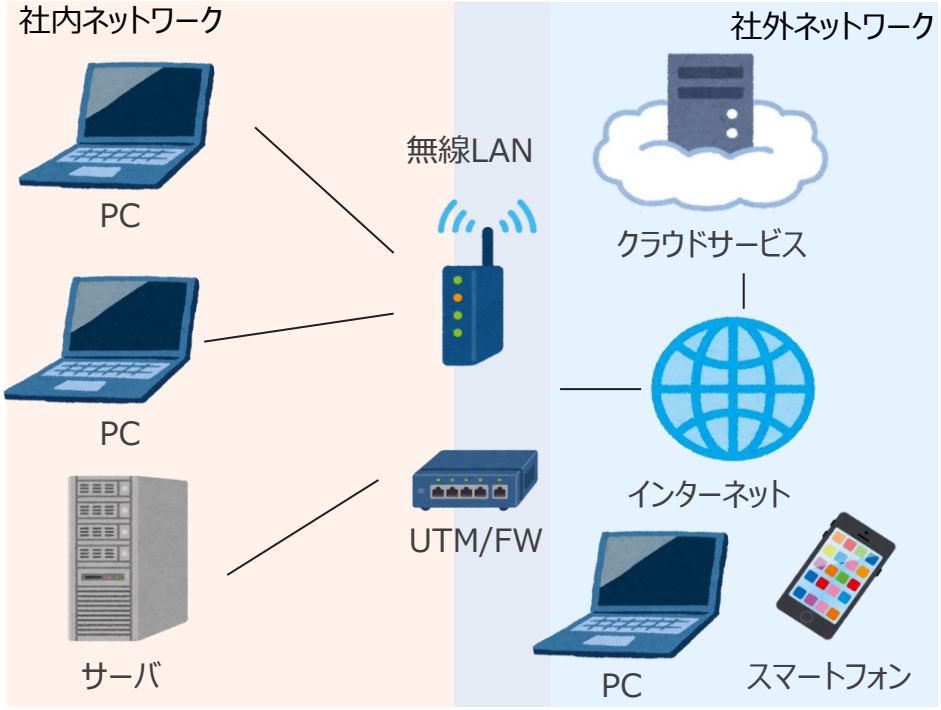
© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営の重要10項目（指示4）

指示４：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

- ✓ 事業に用いるデジタル環境、**サービス及び情報を特定**させ、それらに対するサイバー攻撃（過失や内部不正を含む）の脅威や影響度から、自組織や自ら提供する製品・サービスにおける**サイバーセキュリティリスクを識別**させる。
- ✓ サイバー保険の活用や守るべき情報やデジタル基盤の保護に関する専門ベンダへの委託を含めた**リスク対応計画を策定させ、対応後の残留リスクを識別**させる。

■社内外で利用している情報資産を特定する



業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値				保存期限	登録日
						個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性	重要度		
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC									
人事	社員名簿					有			3	1	1	3		2023/4/1
人事	健康診断の結					有			3	3	3	3		2023/4/1
経理	給与システム データ						有		3	3	2	3	5年	2023/4/1
経理	当社宛請求							有	3	3	2	3	7年	2023/4/1
経理	発行済請求書								2	2	2	2		2023/4/1
共通	電子メールデ								2	2	2	2		2023/4/1
						有			3	3	3	3		2023/4/1

© MS&AD InterRisk Research & Consulting, Inc.

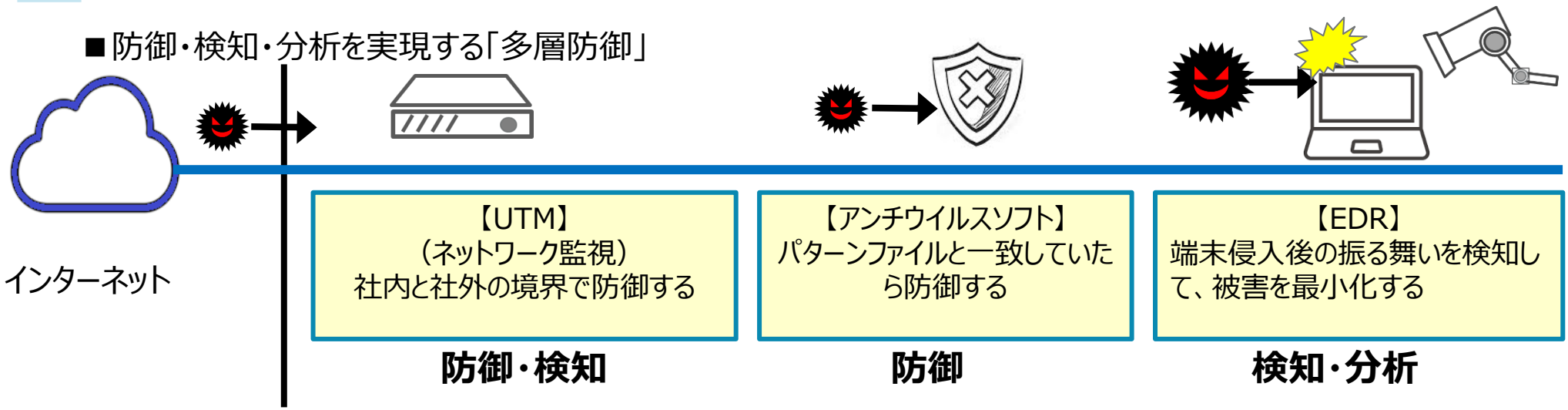
サイバーセキュリティ経営の重要10項目（指示5）

指示５：サイバーセキュリティリスクに効果的に対応する仕組みの構築

- ✓ サイバーセキュリティリスクに対応するための保護対策として、**防御・検知・分析の各機能を実現する仕組みを構築**させる。
- ✓ 構築した仕組みについて、事業環境やリスクの変化に対応するための見直しを実施させる。

	運用レベル	アクション
レベル３	**常時監視**	日々の運用を監視し、設定を見直す。インシデント発生時はレスキュー対応を実施。
レベル２	**ルールによる脅威の検知**	自社ルールを設定し、インシデント発生時や他部署の要請で検知結果を解析する
レベル１	**導入しただけ**	導入時の設定から見直していないため、過検知や誤検知、検知漏れが発生する
レベル０	**導入していない**	セキュリティ対策に穴がある

■防御・検知・分析を実現する「多層防御」

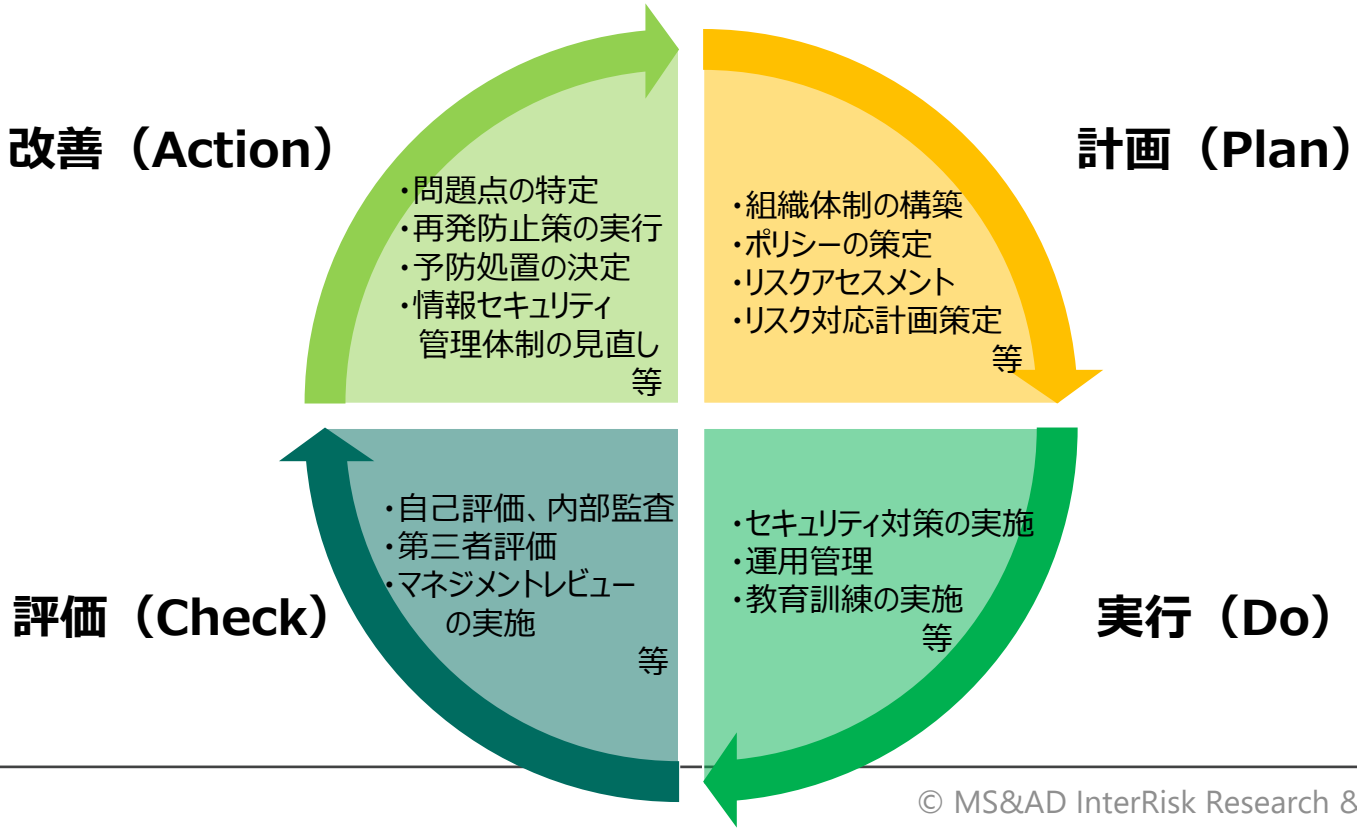


© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営の重要10項目（指示6）

指示６：PDCA サイクルによるサイバーセキュリティ対策の継続的改善

- ✓ リスクの変化に対応し、組織や事業におけるリスク対応を継続的に改善させるため、サイバーセキュリティリスクの特徴を踏まえた**PDCAサイクルを運用**させる。
- ✓ 経営者は対策の状況を定期的に報告させること等を通じて問題の早期発見に努め、問題の兆候を認識した場合は改善させる。
- ✓ 株主やステークホルダーからの信頼を高めるため、**改善状況を適切に開示**させる。



© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営の重要10項目

■サイバーセキュリティリスクの管理体制構築
指示１：サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示２：サイバーセキュリティリスク管理体制の構築
指示３：サイバーセキュリティ対策のための資源（予算、人材等）確保

■サイバーセキュリティリスクの特定と対策の実装
指示４：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示５：サイバーセキュリティリスクに効果的に対応する仕組みの構築
指示６：PDCA サイクルによるサイバーセキュリティ対策の継続的改善

■インシデント発生に備えた体制構築
指示７：インシデント発生時の緊急対応体制の整備
指示８：インシデントによる被害に備えた事業継続・復旧体制の整備

■サプライチェーンセキュリティ対策の推進
指示９：ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策

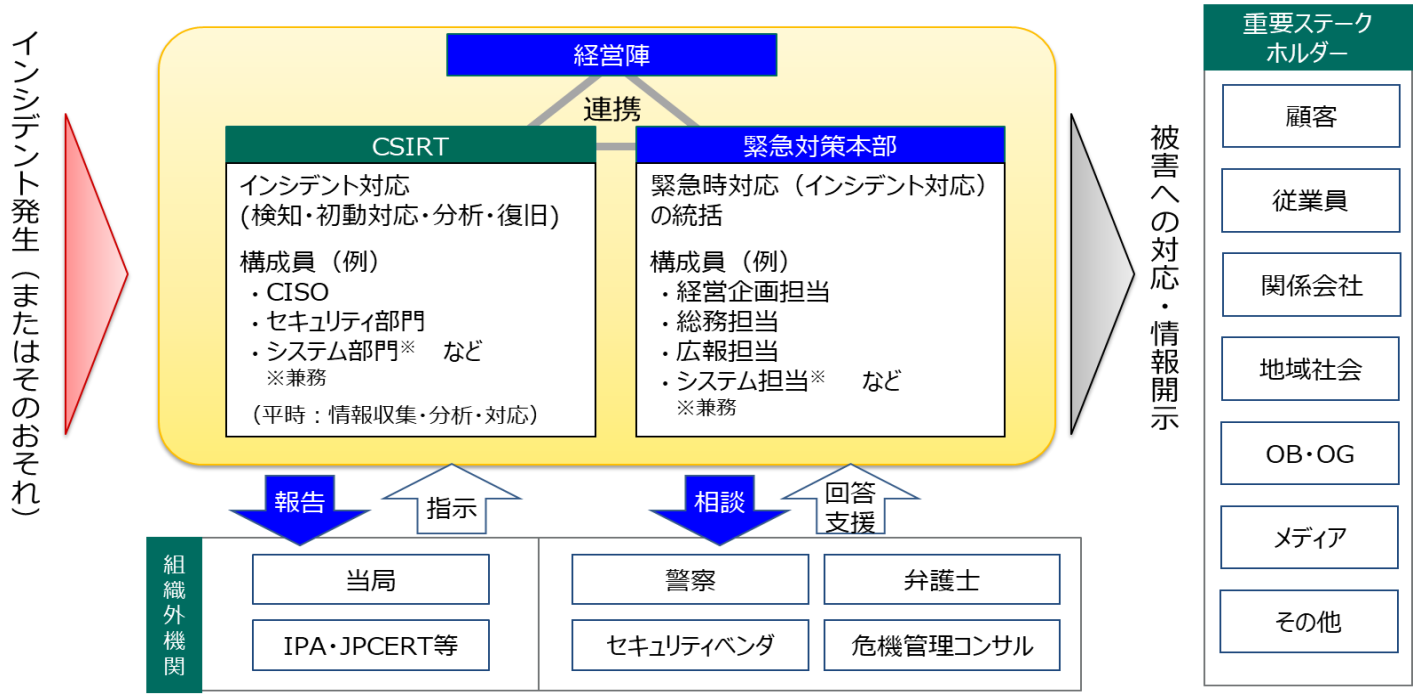
■ステークホルダーを含めた関係者とのコミュニケーションの推進
指示10：サイバーセキュリティに関する情報の収集、共有及び開示の促進

© MS&AD InterRisk Research Institute & Consulting, Inc.

サイバーセキュリティ経営の重要10項目（指示7）

指示７：インシデント発生時の緊急対応体制の整備

- ✓ 影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を適時に実施するため、**サプライチェーン全体のインシデントに対応可能な体制（CSIRT等）を整備**させる。
- ✓ 被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。
- ✓ インシデント発生時の対応について、適宜**実践的な演習を実施**させる。



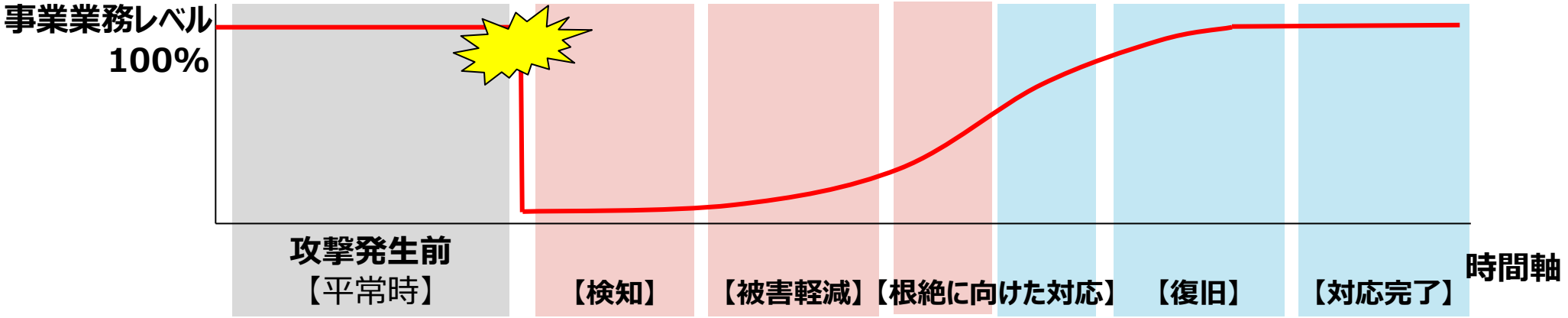
※上記は一般的な組織・企業で構成される対応体制の例です。

© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営の重要10項目（指示8）

指示８：インシデントによる被害に備えた事業継続・復旧体制の整備

- ✓ インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、**復旧に向けた手順書策定や、復旧対応体制の整備**をさせる。
- ✓ **BCPとの連携**等、組織全体として有効かつ整合のとれた復旧目標計画を定めさせる。
- ✓ 業務停止等からの復旧対応について、対象をIT系・社内・インシデントに限定せず、サプライチェーンも含めた**実践的な演習を実施**させる。



インシデント初動対応

サイバーインシデント対応マニュアルの発動
※原因や影響範囲を特定し、被害を最小化するための初動対応マニュアル。危機レベル判断や緊急対策本部の立ち上げ要否判断を含む。

ＢＣＰにおける事業継続対応

事業継続計画（BCP）の発動
※あれもこれも出来ないなかで、「組織全体にとって最適」となる戦略を選択し、その戦略に資源を集中投入することで事業の継続を図ること。

© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営の重要10項目

■サイバーセキュリティリスクの管理体制構築
指示１：サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示２：サイバーセキュリティリスク管理体制の構築
指示３：サイバーセキュリティ対策のための資源（予算、人材等）確保

■サイバーセキュリティリスクの特定と対策の実装
指示４：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示５：サイバーセキュリティリスクに効果的に対応する仕組みの構築
指示６：PDCA サイクルによるサイバーセキュリティ対策の継続的改善

■インシデント発生に備えた体制構築
指示７：インシデント発生時の緊急対応体制の整備
指示８：インシデントによる被害に備えた事業継続･復旧体制の整備

■サプライチェーンセキュリティ対策の推進
指示９：ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策

■ステークホルダーを含めた関係者とのコミュニケーションの推進
指示10：サイバーセキュリティに関する情報の収集、共有及び開示の促進

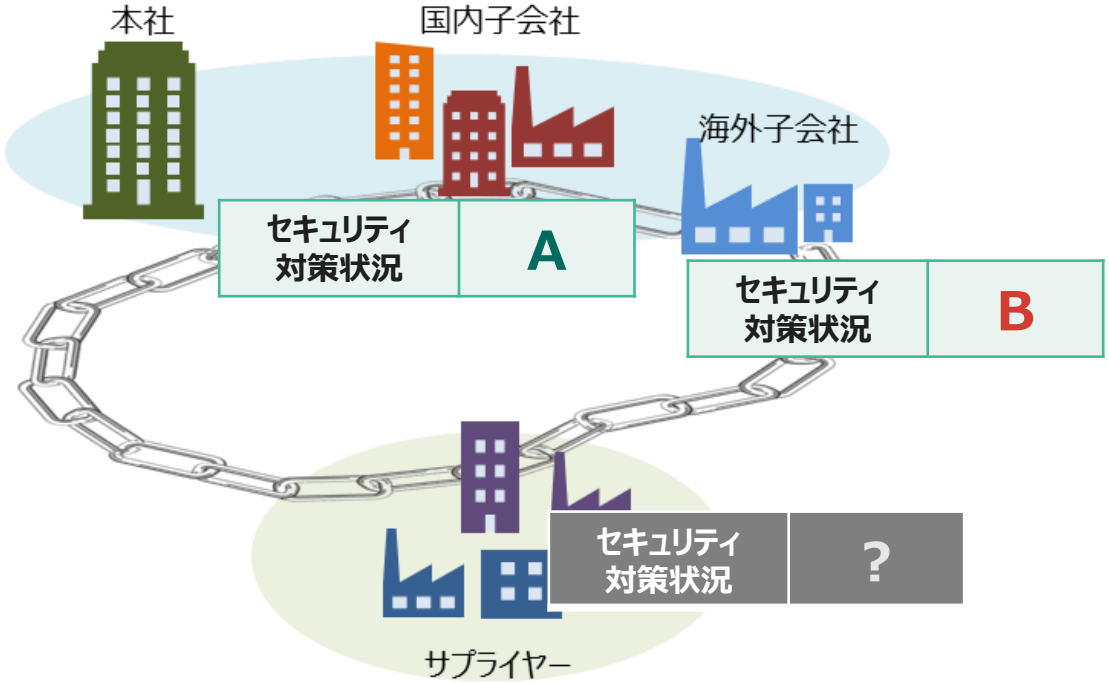
© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営の重要10項目（指示9）

指示９：ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策

- ✓ **サプライチェーン全体**にわたって適切なサイバーセキュリティ対策が講じられるよう、国内外の拠点、ビジネスパートナーやシステム管理の運用委託先等を含めた**対策状況の把握**を行わせる。
- ✓ ビジネスパートナー等との契約において、サイバーセキュリティリスクへの対応に関して**担うべき役割と責任範囲を明確化**するとともに、対策の導入支援や共同実施等、**サプライチェーン全体での方策の実効性を高めるための適切な方策**を検討させる。

■網羅的にサプライチェーン上の企業のセキュリティ対策状況を把握する



本社が求める
セキュリティ水準への引き上げ

© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営の重要10項目

■サイバーセキュリティリスクの管理体制構築
指示１：サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示２：サイバーセキュリティリスク管理体制の構築
指示３：サイバーセキュリティ対策のための資源（予算、人材等）確保

■サイバーセキュリティリスクの特定と対策の実装
指示４：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示５：サイバーセキュリティリスクに効果的に対応する仕組みの構築
指示６：PDCA サイクルによるサイバーセキュリティ対策の継続的改善

■インシデント発生に備えた体制構築
指示７：インシデント発生時の緊急対応体制の整備
指示８：インシデントによる被害に備えた事業継続･復旧体制の整備

■サプライチェーンセキュリティ対策の推進
指示９：ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策

■ステークホルダーを含めた関係者とのコミュニケーションの推進
指示10：サイバーセキュリティに関する情報の収集、共有及び開示の促進

© MS&AD InterRisk Research & Consulting, Inc.

サイバーセキュリティ経営の重要10項目（指示10）

指示10：サイバーセキュリティに関する情報の収集、共有及び開示の促進

- ✓ 有益な情報を得るには自ら適切な情報提供を行う必要があるとの自覚のもと、サイバー攻撃や対策に関する**情報共有を行う関係の構築及び被害の報告・公表への備え**をさせる。
- ✓ 入手した情報を有効活用するための環境整備をさせる。

■インシデント発生時に必要な情報共有先の例

情報共有先	担当者	報告概要
取引先	情報セキュリティ責任者	インシデントが発生した際、××日以内に情報共有を行う
IT／セキュリティベンダー	システム管理者	インシデント発生後の対応および復旧について相談・支援を依頼する
情報処理推進機構（IPA）	情報セキュリティ責任者	インシデントが発生した際、届出を行う
警察	情報セキュリティ責任者	インシデントが発生した際、届出を行う
個人情報保護委員会	情報セキュリティ責任者	個人情報漏えい・そのおそれがある場合は個人情報保護委員会に報告する
弁護士	総務担当	必要に応じて、インシデント発生後の対応について相談する
損害保険会社（サイバー保険加入時）	総務担当	必要に応じて、インシデント発生後の対応について相談する

© MS&AD InterRisk Research & Consulting, Inc.

まとめ

■社会と企業がサイバー攻撃者に狙われている

- システム前提の現代社会において、サイバーセキュリティ対策は社会課題の一つに
- 金銭獲得を目的にあらゆる企業が狙われる

■サイバー攻撃は事業継続性に大きなインパクトを与える

- システム停止により、事業を一時中断せざるを得ない場合も
- 事業停止により、自社だけではなく取引先に影響が波及する可能性も

■サイバーセキュリティ対策への取組は経営課題と認識する

- 経営課題の一つとして、関係者との積極的なコミュニケーションを
- 自社のビジネス目的に合わせて、セキュリティ対策を検討していく
- サイバーセキュリティ経営ガイドラインは具体的な手順や実践例も充実

© MS&AD InterRisk Research & Consulting, Inc.

ありがとうございました

ＭＳ＆ＡＤインターリスク総研のサイバーリスク／情報セキュリティコンサルティング
https://rm-navi.com/search/theme/6

RM NAVI
リスクマネジメント ナビ

お客さま向けのリスクソリューション提供にかかわる、新しいプラットフォーム
『リスクマネジメント ナビ(通称: RM NAVI)』を2024年4月にリリースしました。
https://rm-navi.com

MS&ADインターリスク総研株式会社
リスクマネジメント第三部　危機管理・サイバーリスクグループ
〒101-0063
東京都千代田区神田淡路町2-105　ワテラスアネックス
https://www.irric.co.jp/

※MS&ADインターリスク総研株式会社は、本資料に含まれるすべてのコンテンツについて、MS&ADインターリスク総研株式会社の書面による事前の許諾なしに、
貴社内での使用も含めて、複写、複製、再発行、アップロード、掲載、転送、配布または二次的著作物作成のために使用することをお断りいたします。
※当資料は、現時点で開示されている情報、公開されている情報を基に作成されています。今後の変化する状況情勢等について保証するものではございません。