サイバーセキュリティセミナー2026

企業を守るサイバー防犯対策

～押さえておきたいサイバーセキュリティの勘所～

神　奈　川　県　警　察

サイバーセキュリティ対策本部

https://www. police .pref.kanagawa.jp/

サイバー空間の情勢概況

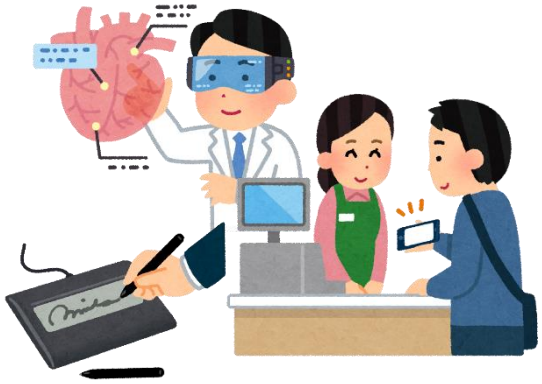
神奈川県警察

※　背景画像はBing Image Creatorを使用して作成

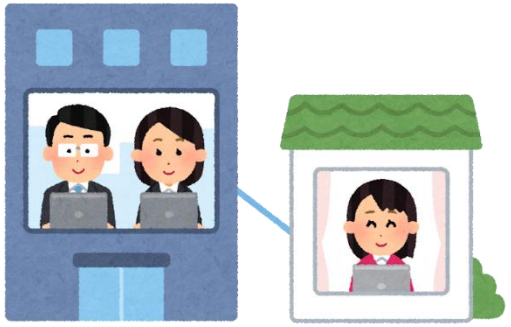
サイバー空間の「公共空間」化

- **コロナ禍において、社会のデジタル化が急激に進展し、あらゆる国民、企業等にとって、サイバー空間は「公共空間」として、より一層の重みを持つようになっている**

みんなが



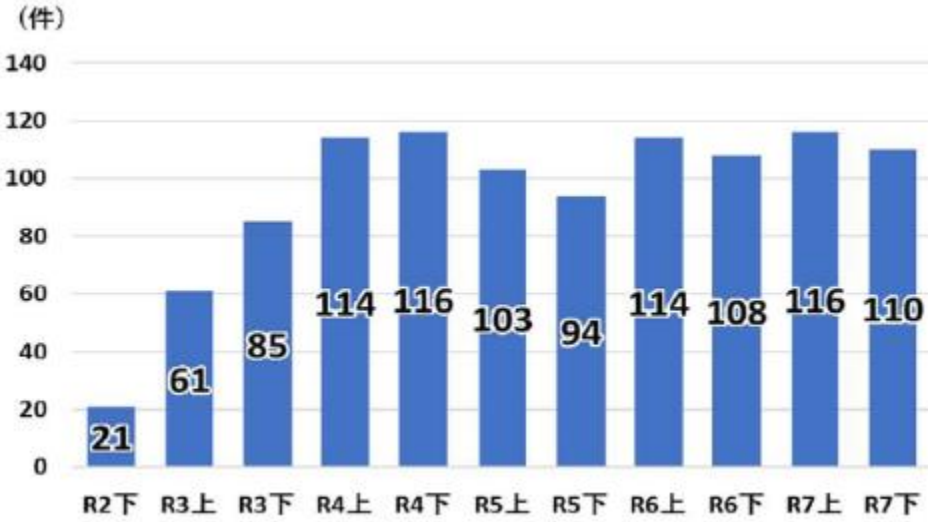
大切なことを



サイバー空間で

サイバー空間の脅威の情勢 極めて深刻

- **ランサムウェア攻撃の相次ぐ被害！！**
  - **被害報告件数が高水準で推移**
  - **被害の約3分の2は中小企業**
  - **国民生活に影響を及ぼす事案も複数発生**

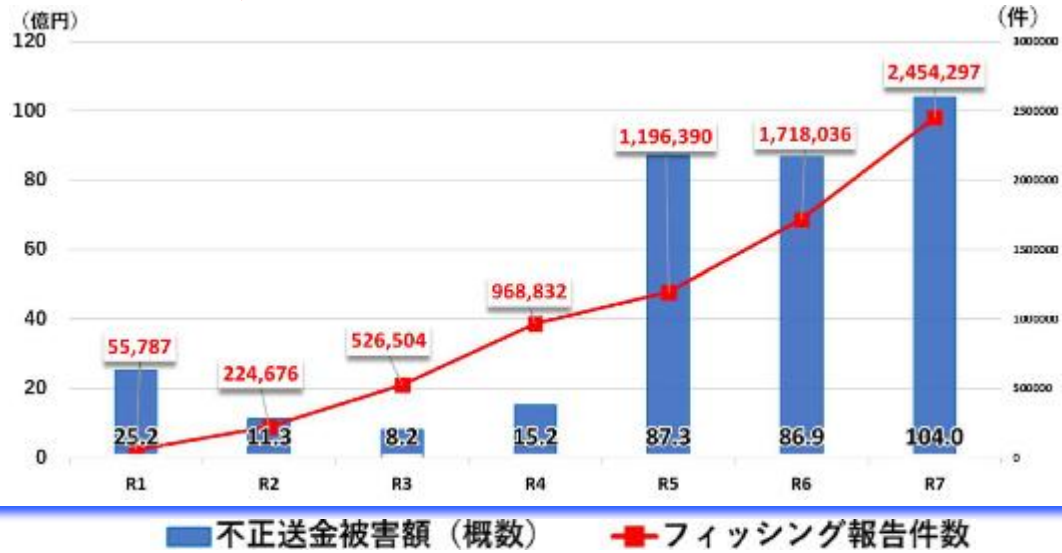


被害企業・団体等の規模別

警察庁「令和7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」よりデータ引用
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

サイバー空間の脅威の情勢 極めて深刻

- フィッシングによる不正送金、不正取引
  - 令和7年における**フィッシング報告件数**は**245万4,297件**、**インターネットバンキングに係る不正送金**事犯の**被害総額は約104億円**

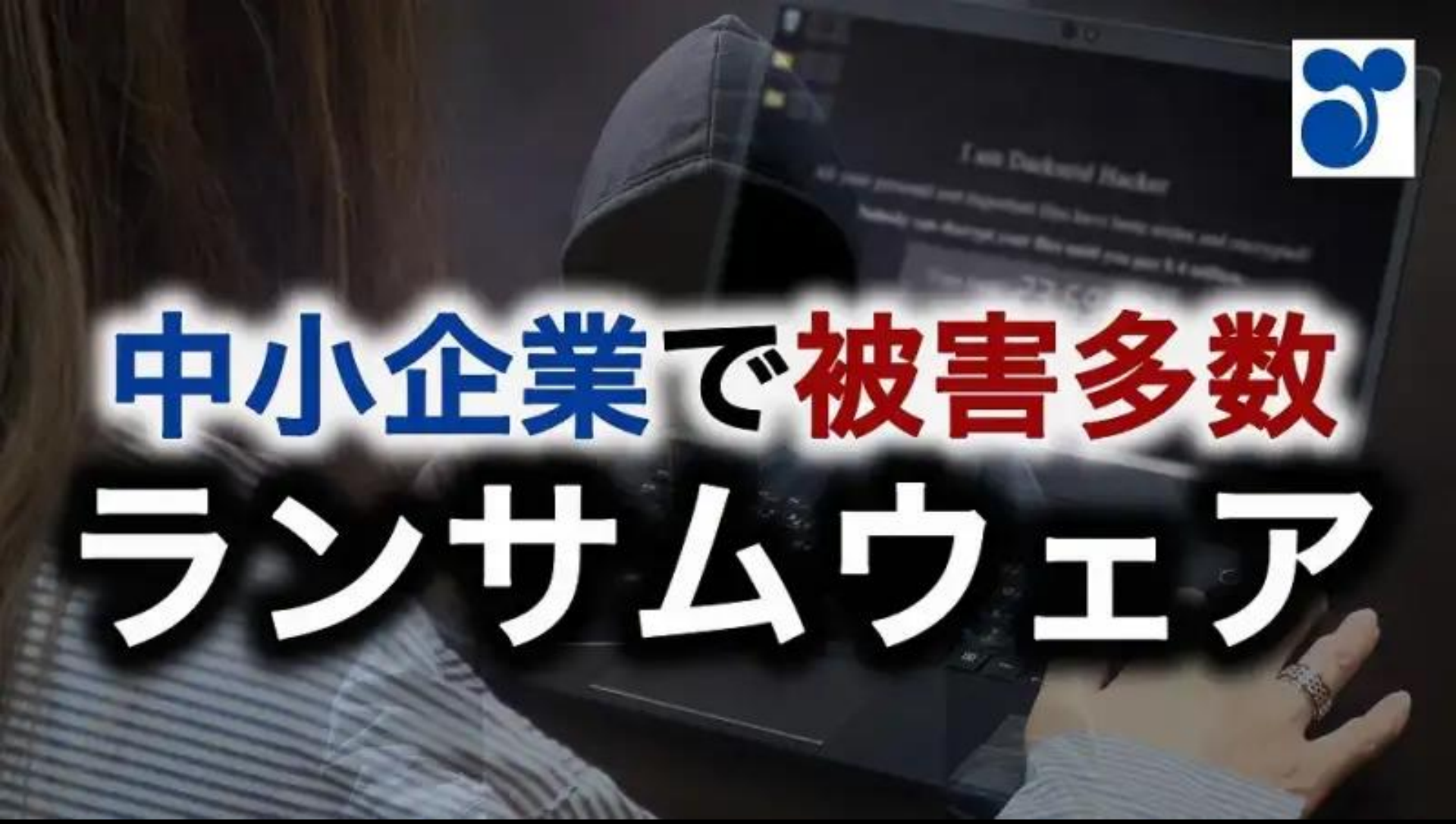


警察庁「令和7年におけるサイバー空間をめぐる脅威の情勢等について」よりデータ引用
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

サイバー犯罪、サイバー攻撃の情勢

神奈川県警察

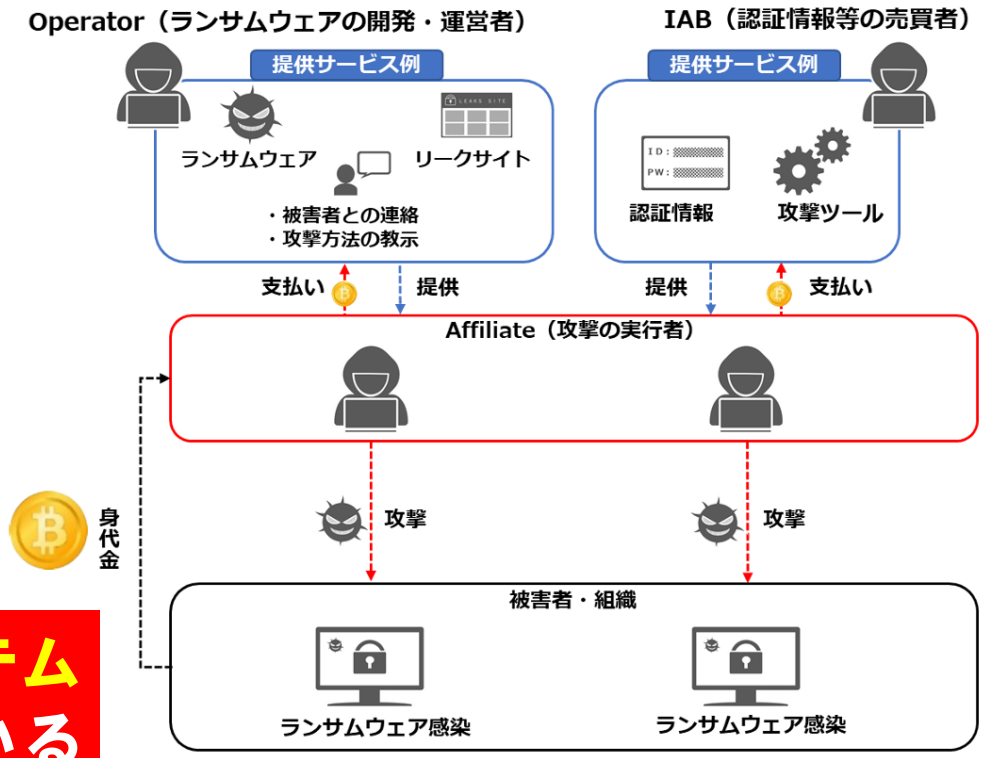
※　背景画像はBing Image Creatorを使用して作成



引用元：政府インターネットテレビ
出　典：中小企業で被害多数　ランサムウェア
https://www.gov-online.go.jp/useful/202506/video-298784.html

ランサムウェア攻撃の実態

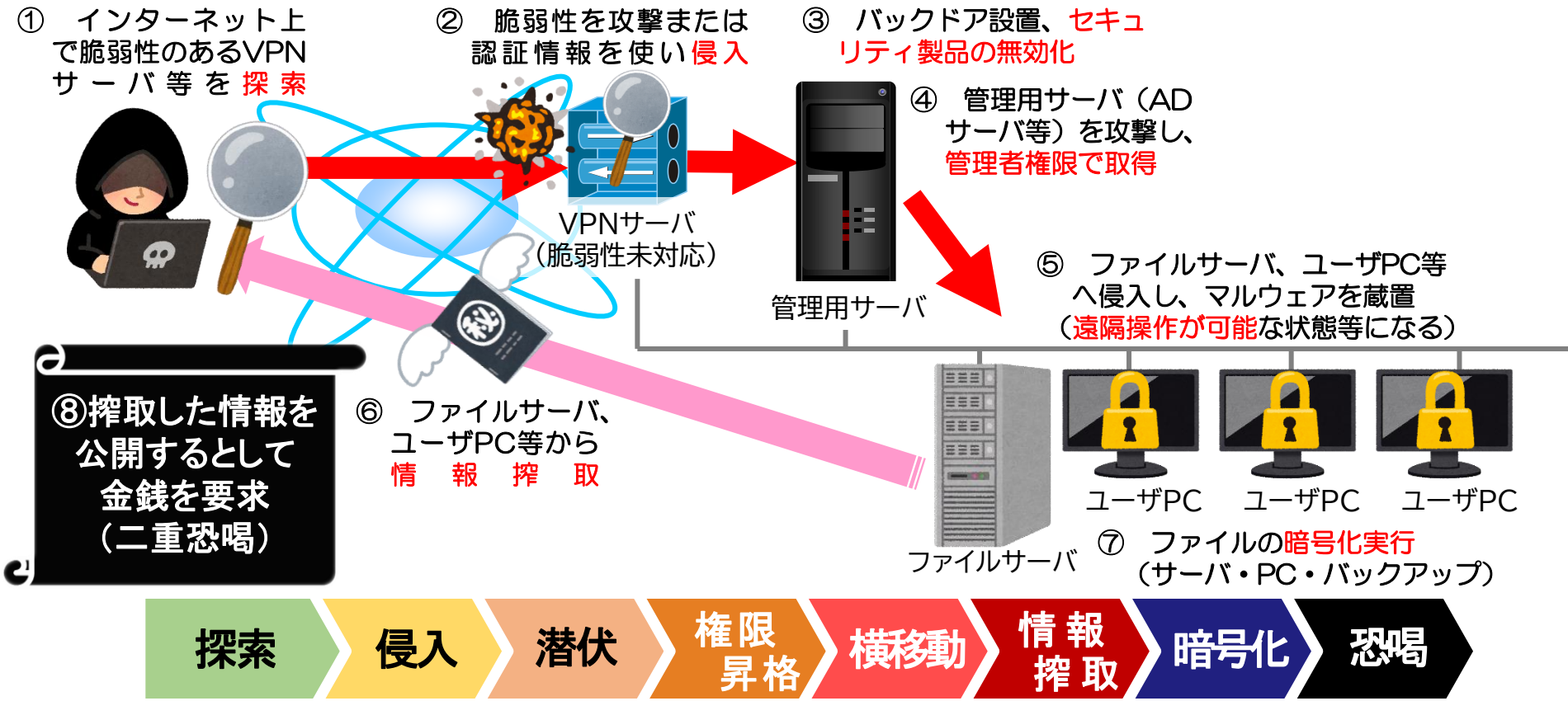
- RaaS（Ransomware as a Service）
  - 攻撃の実行者（Affiliate）にランサムウェア等を提供し、その見返りとして身代金の一部を受け取る態様
  - 標的企業のネットワークに侵入するための認証情報等を売買する者（IAB：Initial Access Broker）も存在



ビジネスライクなエコシステム（生態系）が構築されている

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」より図引用
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

ランサムウェア攻撃の実態



探索 → 侵入 → 潜伏 → 権限昇格 → 横移動 → 情報搾取 → 暗号化 → 恐喝

本質的な問題は「暗号化されること」ではなく、「侵入されていること」

侵入に早く気づけば、影響を少なくできる可能性がある!!

基本的なランサムウェア対策

事前対策

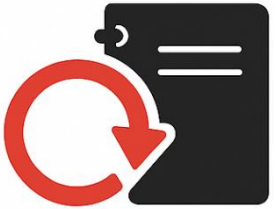
- メールに気を付ける（開く前に確かメル）等の職員教育
- パソコン、サーバ、ネットワーク機器（VPN機器等）の脆弱性対策、設定の見直し
- 利用者認証の強化（多要素認証の導入等）

早期発見

- 各種サーバでのログの保存と確認
- EDR（Endpoint Detection and Response）の導入と適切な運用
- ネットワークの監視

拡大防止

- 管理者権限の適切な運用
- 共有フォルダのアクセス権見直し
- 業務の機密性、重要度によるネットワーク分離とアクセス制御



事業継続

- バックアップ（オフライン）の実施
- 復旧手順の整備と訓練の実施
- サイバーセキュリティを含めた事業継続計画（BCP）の策定
- インシデント対応体制の整備

フィッシング(Phishing)に注意!!

- 実在する企業等を装ったSMSやメールを送りつけ、受信者をフィッシングサイト(偽物のサイト)へ誘導してIDやパスワード等を入力させ、不正に個人情報等を搾取する手口

フィッシング（Phishing）

フィッシング（Fishing）

神奈川県警察

※　騙すための手口が洗練されていることから「sophisticated(洗練された)」の「ph」を「fishing」の「fi」と置き換えられた(諸説あり)

フィッシングメールの例

From：XYZ銀行 件名 ：【重要】取引停止のお知らせ	From：XYZカード 件名 ：【緊急】不正アクセスを検知しました	050xxxxxxx
本人かどうか確認が取れない取引がありましたので停止しました。 確認してください。 http:// xyz-bank.com	第三者からの不正なアクセスを検知しました。 確認してください。 http:// xyz-card.com	お荷物のお届けがありましたが、不在の為持ち帰りました。 http://example.jp
取引の停止 偽	不正アクセス 偽	不在持ち帰り 偽

銀行等を装ったメールやSMSから偽のウェブサイトに誘導し、**金融情報や個人情報を不正に入手**する手口、それが**フィッシング**です！

- 銀行口座を操作されて勝手に送金される
- ＥＣサイトで勝手に買物をされる
- アカウントを乗っ取られる

神奈川県警察

警察庁「サイバー警察局便りR6 Vol.3「そのメール、フィッシングかも！」より引用
https://www.npa.go.jp/bureau/cyber/pdf/R6_Vol.3cpal.pdf

フィッシング対策の勘どころ

- **普段から使っているサイトやサービス提供会社、有名な企業等からのメールでも・・・**
  - ✓ メールやSMSに記載されたURLを安易にタップ（クリック）しない
  - ✓ 送信元のメールアドレス等が普段と同じかどうか確認する
  - ✓ メールの内容、書式、文章等に普段と違う、違和感がないか確認する
- **日頃から習慣づけていただきたいこと**
  - ✓ サイトやサービスには、ブラウザのブックマーク等からアクセス、アプリがあればアプリを使う
  - ✓ アプリがある場合には、パスワード設定やカード情報の入力はアプリから行う

神奈川県警察

ログインさせようとするメール/SMSは全部偽物

※　人物画像はBing Image Creatorを使用して作成

サイバーセキュリティ対策の勘所

神奈川県警察

※　背景画像はBing Image Creatorを使用して作成

企業、組織が認識すべきこと

サイバー犯罪、サイバー攻撃が日々進化する中

常に新たな脅威に対する備えが必要であるため

サイバーセキュリティには

１００％はありえない

リスクを低減し、攻撃を受ける前提で被害を最小限にする対策（ダメージコントロール）と事業継続計画（BCP）が必要

被害のきっかけは「偽～」

- サイバー犯罪、サイバー攻撃の手口では、「偽～」が使われています
  - 取引先を装った偽メールを使う標的型メール攻撃
  - 偽ショッピングサイトで詐欺の被害
  - 偽メール、偽SMSを使うフィッシング
  - 偽ウイルス警告がでるサポート詐欺

など

被害のきっかけは「偽～」

「本物」、「偽物」を見極める
「勘所」を押さえておきましょう！

偽サイト、偽メールに騙されないための勘どころ

- ✓メールアドレス、URLはおかしくないか？
  - 送信元メールアドレス、URLは普段どおりか？

    本物：～company.co.jp　⇔　偽物：～cornpany.co.jp
  - 見慣れないドメインを使ってないか？

    「～.co.jp.～.xyz/～」などの紛らわしいものもある

    スマホは画面が狭く、見づらいので特に注意！
- ✓違和感を感じるところがないか？
  - 機会翻訳の様な片言の日本語がないか？
  - 言い回しや書式など普段と違うところがないか？

キッカケはメール！！

- **サイバー犯罪、サイバー攻撃**の**切っ掛け**となるのは**メール！！**
- 英文で添付ファイルが付いている**怪しいメール**ではなく、**よくある怪しくないメールが危ない！**
- 少しでも**違和感**があれば**確認する、**周り（同僚、上司等）に**相談、報告**する、**検索をしてみる**

メールに気を付けるという**当たり前のことを徹底**することで被害を防げることが多いことを知っておきましょう！！

そのメール
開く前に、まず
確かめる。

コンピュータ・ウイルスは
メールから感染することが多い
ことを知っていますか？

日頃からの情報収集

- 日々、巧妙化、複雑化するサイバー犯罪、サイバー攻撃に対応していくためには、日頃からの情報収集が不可欠
- 手口を知っているか知らないかが、被害に遭うか遭わないかの分かれ目
- 警察をはじめとしたサイバーセキュリティ関係機関のホームページやSNSなどで確認
- インターネットのニュースサイト等でも情報収集

SECURITY ACTION
セキュリティ対策自己宣言

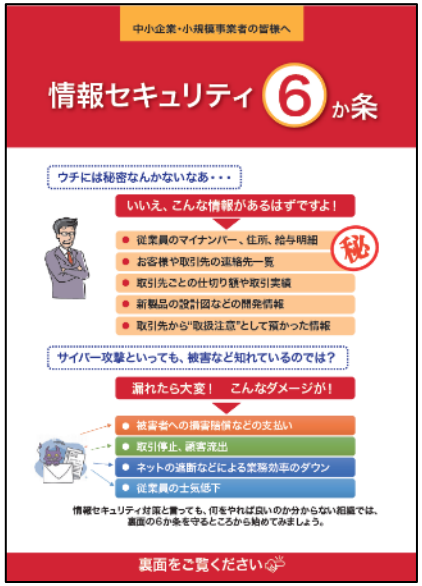
- 「SECURITY　ACTION」は、**中小企業自らが情報セキュリティ対策に取組むことを自己宣言**する制度
- 「**中小企業の情報セキュリティ対策ガイドライン**」の実践をベースとした**2段階の取組目標**

独立行政法人 情報処理推進機構(IPA)「SECURITY ACTIONセキュリティ対策自己宣言」より
https://www.ipa.go.jp/security/security-action/

SECURITY ACTION
セキュリティ対策自己宣言

★一つ星

「**情報セキュリティ6か条**」に**取組ことを宣言**



★★二つ星

「**5分でできる！情報セキュリティ自社診断**」を**実施**し、「**情報セキュリティ基本方針**」を**定め、公開したことを宣言**

神奈川県警察

独立行政法人 情報処理推進機構(IPA)「SECURITY ACTIONセキュリティ対策自己宣言」より
https://www.ipa.go.jp/security/security-action/

SECURITY ACTION
セキュリティ対策自己宣言

- 「SECURITY ACTION」のメリット
  - 情報セキュリティ対策への取組の見える化
    ロゴマークをウェブサイトに掲出したり、名刺やパンフレットに印刷することで**自らの取組姿勢をアピール**
  - 顧客や取引先との信頼関係の構築
    既存顧客との**信頼関係強化**や新規顧客の**信頼獲得のきっかけ**
  - 公的補助金・民間の支援を受けやすく
    SECURITY ACTIONを要件とする補助金の申請、普及
    賛同企業から提供される**様々な支援策**が利用可能

独立行政法人 情報処理推進機構(IPA)「SECURITY ACTIONセキュリティ対策自己宣言」より
https://www.ipa.go.jp/security/security-action/

【参考】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（案）

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※2を提示しつつ、その状況を可視化する仕組み※3を構築。
- 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 本制度では、サプライチェーンを構成する企業等のIT基盤が対象。
※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（案）

成熟度の定義	★３	★４	★５［検討中※4］
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**到達点として目指すべき対策**: • 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
評価スキーム	**専門家確認付き自己評価**	**第三者評価**	**第三者評価**

※4 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。

制度の普及施策（例）

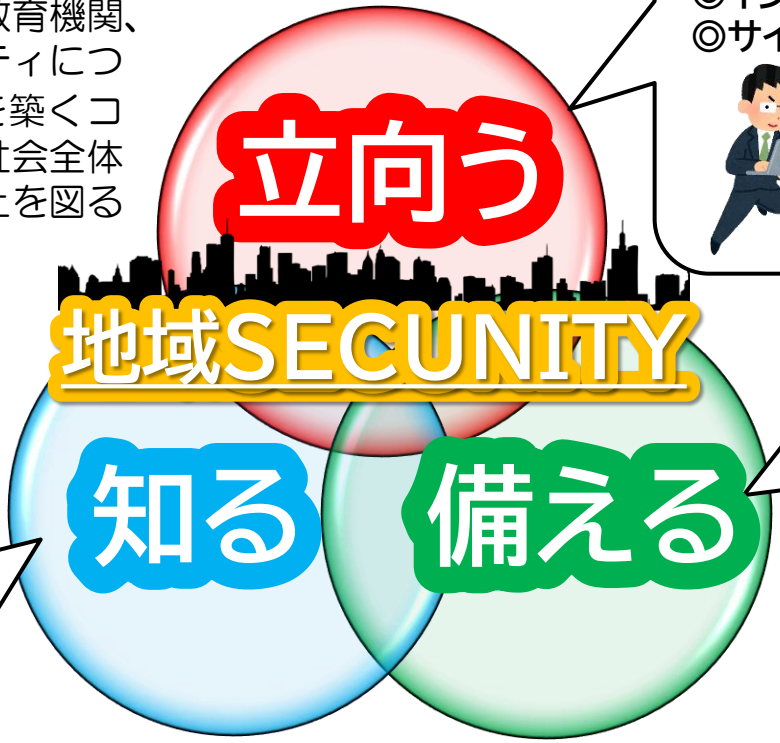
想定される課題	中小企業等における★取得の負担		中小企業等におけるセキュリティ専門家の確保	サプライヤー企業への★取得要請時の関係法令の適用
普及施策	サイバーセキュリティお助け隊サービス（新類型）の創設	中小企業ガイドライン整備	専門家の活用促進	取引先への要請等に係る考え方の整理
	★3・★4に対応した、サイバーセキュリティお助け隊サービスの新たな類型創設により、安価な"★"取得を実現	中小企業の情報セキュリティ対策ガイドライン及び付録サンプル規程の整備により、"★"の取得を容易化	「中小企業向けサイバーセキュリティ専門家リスト」の整備により、中小企業と専門家とのマッチングを促進	取引先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の策定により、費用に係る価格交渉を推進

経済産業省「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）の概要」より引用
https://www.meti.go.jp/press/2025/12/20251226001/20251226001-b.pdf

地域セキュリティコミュニティ(SECUNITY)の構築

地域SECUNITYの設計図

地域の民間企業、行政機関、教育機関、関係団体等がサイバーセキュリティについて語り合い、「**共助**」の関係を築くコミュニティの形成を通じ、地域社会全体のサイバーセキュリティ水準向上を図る



◎インシデントへの対応、復旧作業
◎サイバーお助け隊の活用　等

◎警察や関係機関の協働によるセミナー、シンポジウム等
◎同業種、異業種間の情報共有、意見交換(セキュリティサロン)
◎ハンズオンセミナー、CTF
等

◎セキュリティポリシー策定
◎検知、防御システム(EDR等)の導入等の対策実施
◎サイバー保険へ加入
◎各種訓練の実施　等

サイバーセキュリティは

知識よりも意識が大切です

「サイバーセキュリティは技術的に難しいからわからない」と思われがちですが、
当たりまえと思える対策等を確実に行うことで多くの被害は防げます。まずは
意識を高め、そのうえで技術的な知識も身に付けると万全です。

※　背景画像はBing Image Creatorを使用して作成