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

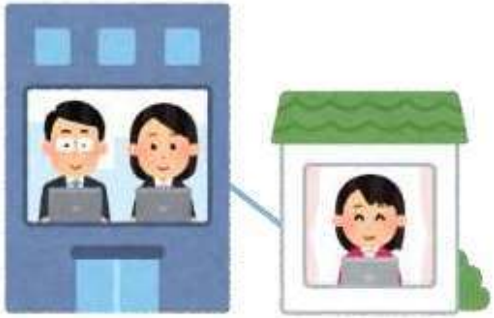
※　背景画像はBing Image Creatorを使用して作成

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

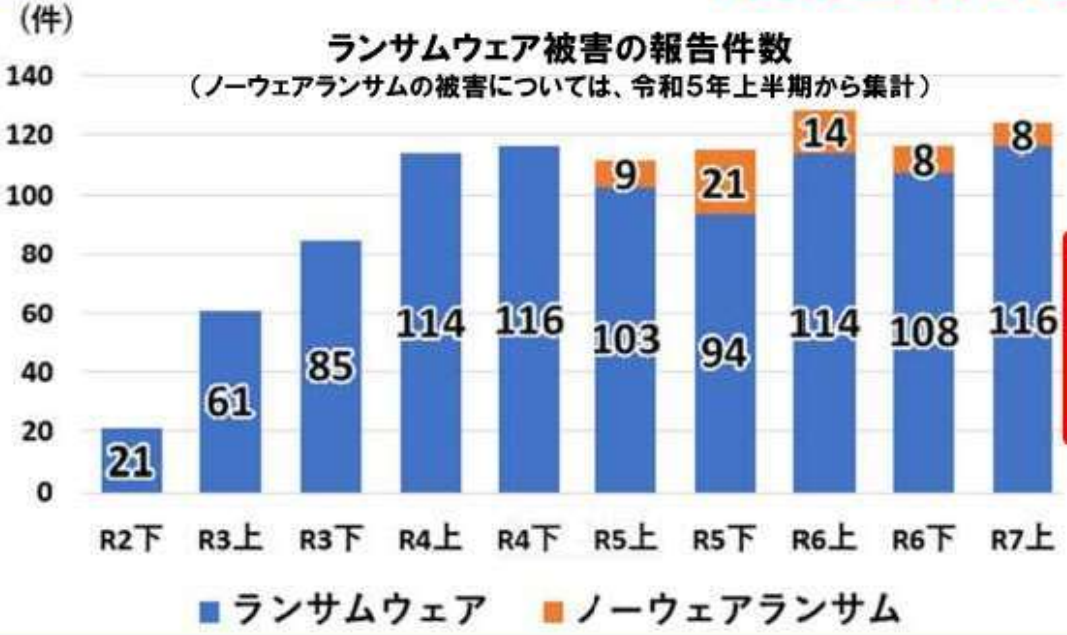
大切なことを

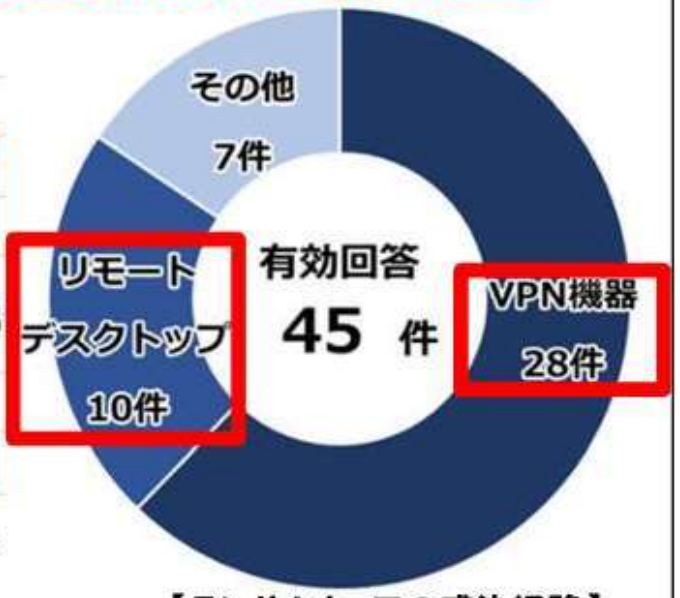


サイバー空間で

サイバー空間の脅威の情勢 極めて深刻

- **ランサムウェア被害が依然として高水準で推移**
- **VPN機器、リモートデスクトップを利用した感染を多数確認**
- **ランサムウェア感染により市民生活にも重大な影響が発生**





【ランサムウェアの感染経路】

神奈川県警察

警察庁「令和7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」よりデータ引用
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

サイバー空間の脅威の情勢 極めて深刻

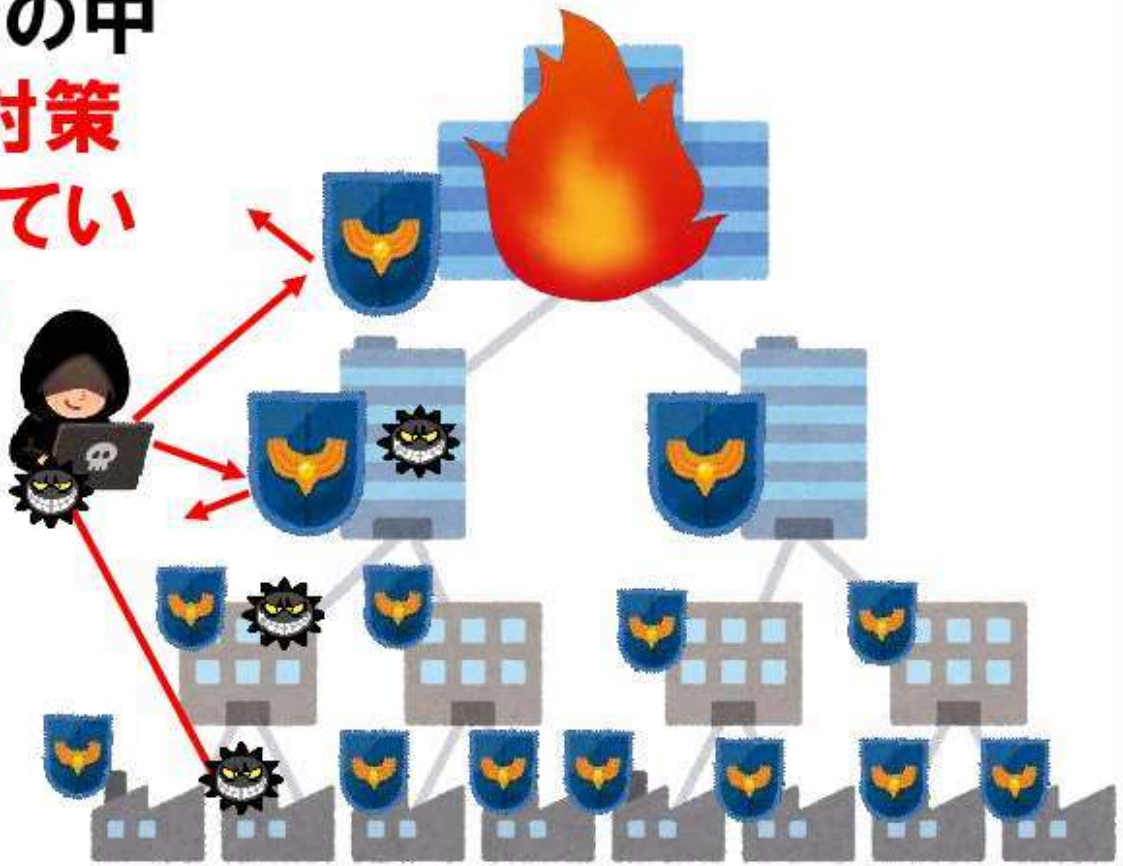
- **フィッシング報告件数は右肩上がりの増加、インターネットバンキングに係る不正送金事犯の9割はフィッシング**

神奈川県警察

警察庁「令和7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」よりデータ引用
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

サプライチェーン攻撃

- **サプライチェーンの中で、セキュリティ対策を適切に実施していない組織を攻撃し、それを足がかりにターゲット企業に侵入する**



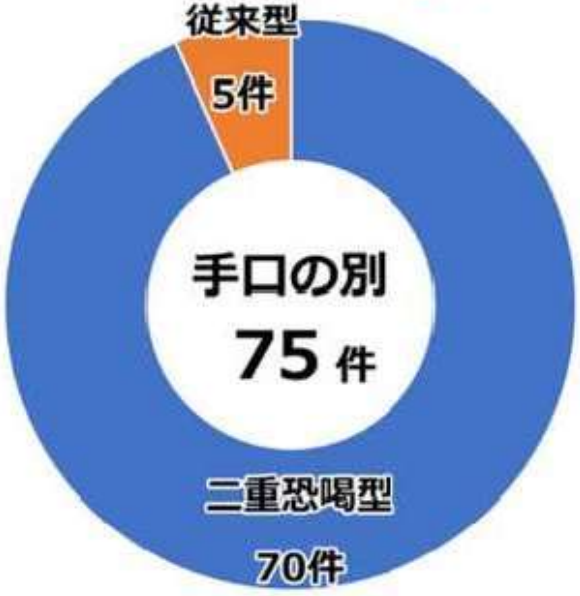
サイバー犯罪、サイバー攻撃の情勢

神奈川県警察

※　背景画像はBing Image Creatorを使用して作成

ランサムウェアの情勢

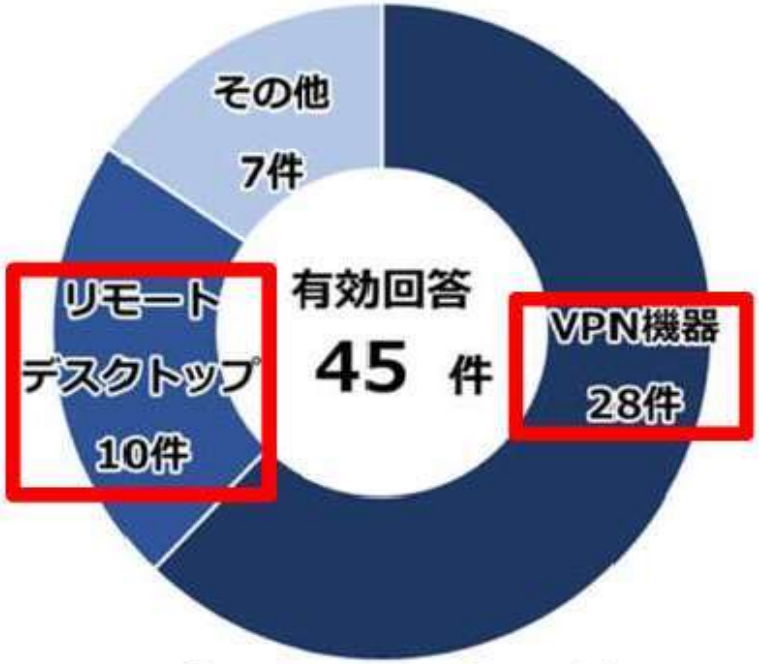
- ランサムウェアとは、**端末等に保存されているデータを暗号化**して使用できない状態にした上で、その**データを復号する対価として金銭を要求**する不正プログラム
- 暗号化のみならず、データを窃取した上で「**支払わなければデータを公開する**」などとして金銭を要求する**二重恐喝（ダブルエクストーション）**が多くみられる



警察庁「令和7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」よりデータ引用
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

ランサムウェアの情勢

- **VPN機器、リモートデスクトップを利用した感染を多数確認**
- **被害企業・団体等の規模別では中小企業が6割以上**



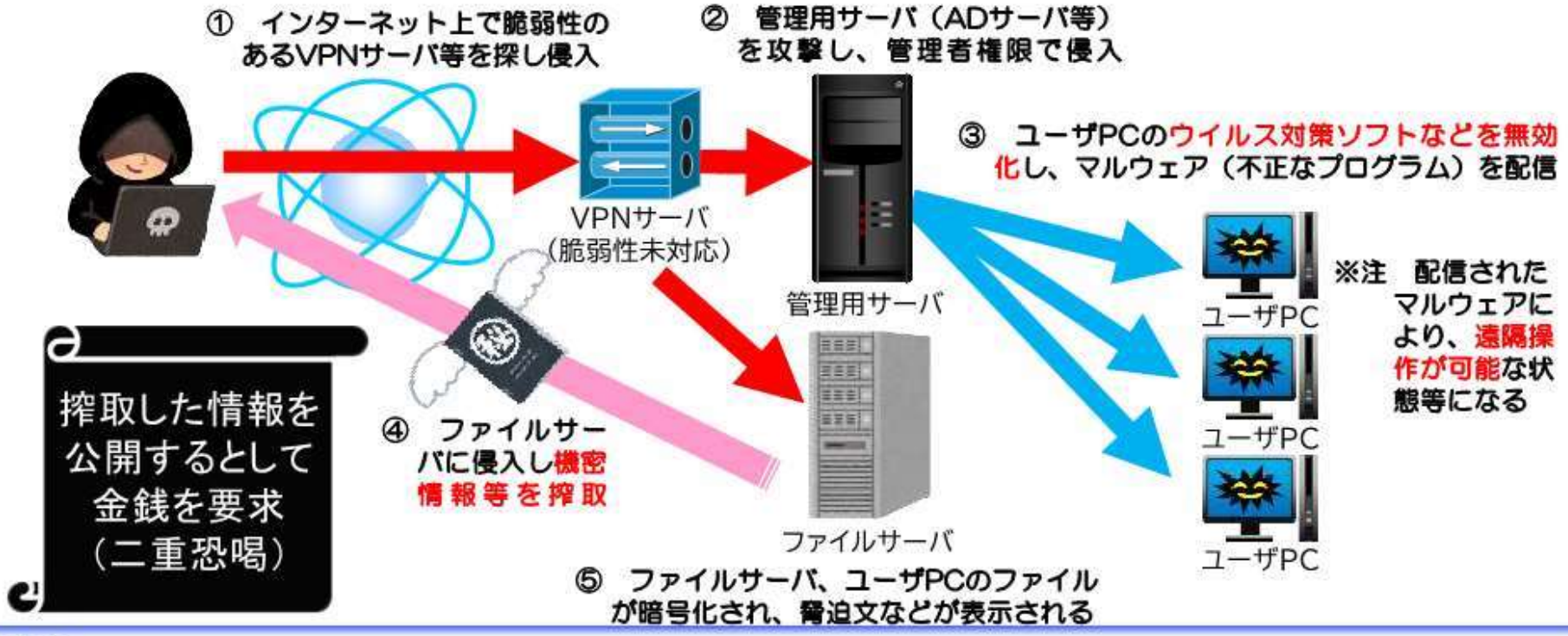
【ランサムウェアの感染経路】

【被害企業・団体等の規模別件数】

警察庁「令和7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」よりデータ引用
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

人手によるランサムウェア攻撃
(human-operated ransomware attack)

- **標的型サイバー攻撃と同様、攻撃者が様々な攻撃手法を駆使して、企業・組織のネットワークへの侵入**



神奈川県警察

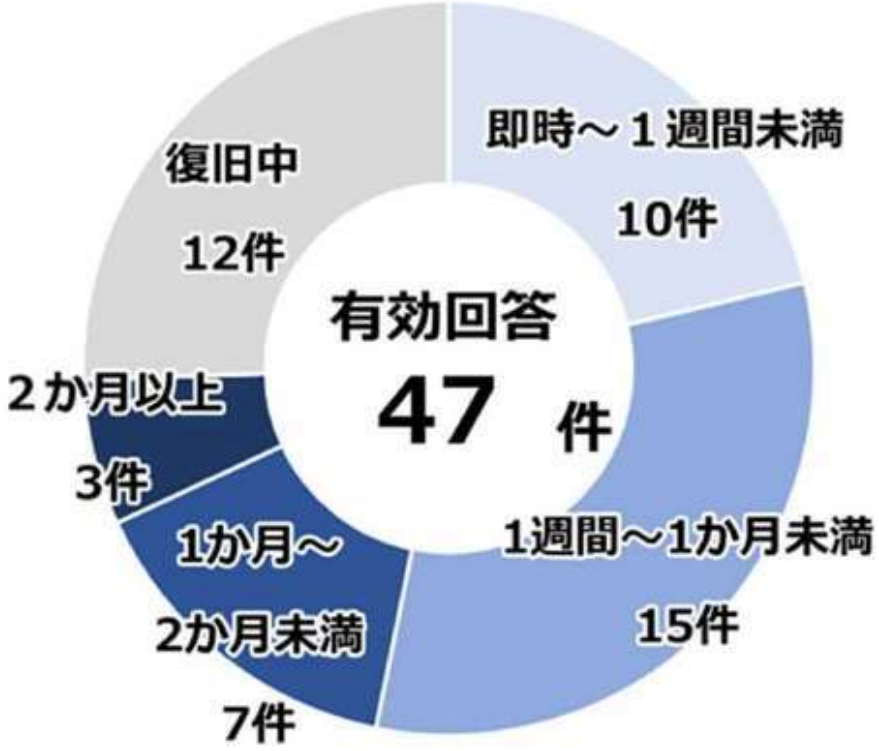
ノーウェアランサムによる被害

- **国内において、データを暗号化することなく、データを窃取して、対価を要求する(「ノーウェアランサム」)による被害を確認**

警察庁「令和5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/R5/R05_cyber_jousei.pdf

【参考】
ランサムウェアの被害に係る統計

■ 復旧等に要した期間／調査費用の総額



警察庁「令和7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」よりデータ引用
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

ランサムウェア対策

- 単純なウイルス対策ではなく、標的型メール等のサイバー攻撃と同様な対策が必要
  - メールに気を付ける（開く前に確かメル）
  - 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）
  - パソコンやサーバへのEDR（Endpoint Detection and Response）の導入、ネットワークの監視

- 完全には防げないので、システムの定期的なバックアップは必須です

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

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

被害のきっかけは「偽～」

- **サイバー犯罪、サイバー攻撃で使われる手口では、「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により機密情報を搾取される
  - 検索してたどり着いた偽ショッピングサイトで買い物をしてしまい詐欺の被害に遭う
  - 宅配業者、通信事業者を装った偽SMSから不正アプリをインストールしてしまう
  - フリマアプリ運営会社等を装った偽メールに誘導されてID・パスワードを取られる
  - いろいろなサイトを見ていたら、突然、ウイルス感染したという偽警告がでる　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！

神奈川県警察

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？
  - 機械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！！

神奈川県警察

神奈川県警察「メールに注意して、リスクの低減を図る」
https://www.police.pref.kanagawa.jp/mesd7040.htm

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**

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

★一つ星

「情報セキュリティ5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

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/

【参考】
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」構成・内容イメージ

IPA

- サイバー攻撃により、取引上共有している機微情報の漏洩や部品・サービスの供給途絶など、自社のみならずサプライチェーン全体に影響を及ぼす事態が発生しうる。このようなインシデントの予防・抑制を目的に、サプライチェーン構成企業全体のセキュリティ対策レベルの向上と、実施状況の効率的な確認ができる手法として「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」を提案。
- 中小企業を含めた多様なサプライチェーン企業が参照できるよう、三段階のセキュリティレベルを想定。

	三つ星（★３）	四つ星（★４）	五つ星（★５）
段階の考え方（企業がどういう状態にあるか）	**現場レベルや部分的なレベルでのセキュリティ対策が実践されている**	自社に合わせたセキュリティ対策の**組織的・継続的な実施・改善（PDCA）がなされている**	サイバー空間上の**リスクを適宜適切に把握し、合理的な対策を実施、継続的改善がなされている**
対象として想定する事業者	サプライチェーンを形成するすべての企業等	・産業界を代表・牽引する立場の企業等（それを目指す企業等を含む）の**サプライチェーンにおいて重要な機能・役割等を担うサプライヤー企業**	・産業界を代表・牽引する立場の企業等（それを目指す企業等を含む）の**サプライチェーンにおいて特に重要な機能・役割等を担うサプライヤー企業**等
対策セットの考え方（対策の規模感）	上記に該当する企業等が、最低限実装すべきセキュリティ対策の水準（１５項目程度）	上記に該当する企業等が、標準的に目指すべきセキュリティ対策の水準（～５０項目程度）	上記に該当する企業等が、現時点で到達点として目指すべきセキュリティ対策の水準（１００項目～）
	※既存のガイドラインや認証制度などを活用可能なスキームを検討※		
実施状況の評価・確認方法	・自己適合宣言（社内外の登録セキスペ等専門家による確認）	・自己適合宣言　（★３と同様） ・第三者評価 と二段階に分けることも考えられる（★４、★４plus）	・第三者評価

独立行政法人 情報処理推進機構（IPA）「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の構築について」より引用
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/pdf/001_05_00.pdf

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