実被害から考えるセキュリティ対策

～サイバー保険の必要性～

あいおいニッセイ同和損害保険株式会社

質問

2月1日～3月18日の期間は
なに「月間」でしょう？

ヒント：318（サイバー）

答え

政府の
「サイバーセキュリティ月間」

今年のテーマは
「サイバーはひとごとじゃない」

サイバーセキュリティ月間とは

2月1日から3月18日は「サイバーセキュリティ月間」です。

毎日のように、サイバー攻撃のニュースが報道されています。
フィッシングによるアカウント乗っ取り、サポート詐欺による金銭被害、
ランサムウェアによる企業の業務の停止など、
サイバー攻撃は私たちの暮らしを脅かすものとなっています。

政府では、毎年2月1日から3月18日を「サイバーセキュリティ月間」と定め、
内閣官房国家サイバー統括室（NCO）を中心に、産官学民が連携して、
サイバーセキュリティに関する取組を集中的に行っています。

2026年は「サイバーはひとごとじゃない」をテーマとし　一人一人が、
　　だと考えて、
対策していただけるようなコンテンツの発信、普及啓発を行っていきます。

今日の内容　４つのパートに分けて話をします！

サイバー攻撃は　身近！

…サイバー攻撃のハナシ

サイバー攻撃を受けると　お金がかかる！

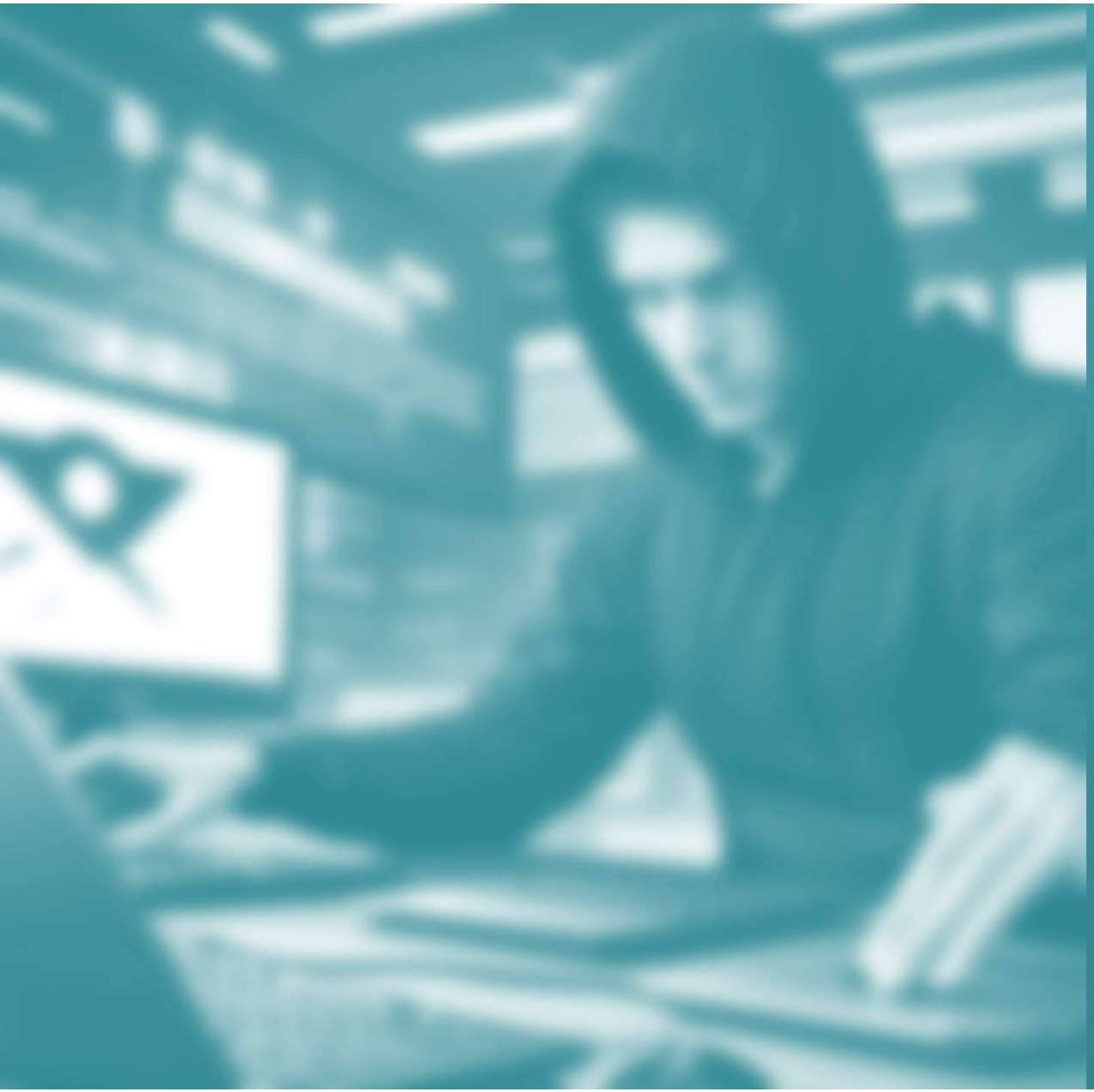
…被害額のハナシ

サイバー攻撃の対策は　事後対策も重要！

…対策のハナシ

サイバー保険の必要性　火事は119番、サイバー攻撃は？

…金銭的な補償だけではないサイバー保険



パート１

サイバー攻撃は

身近

はじめに

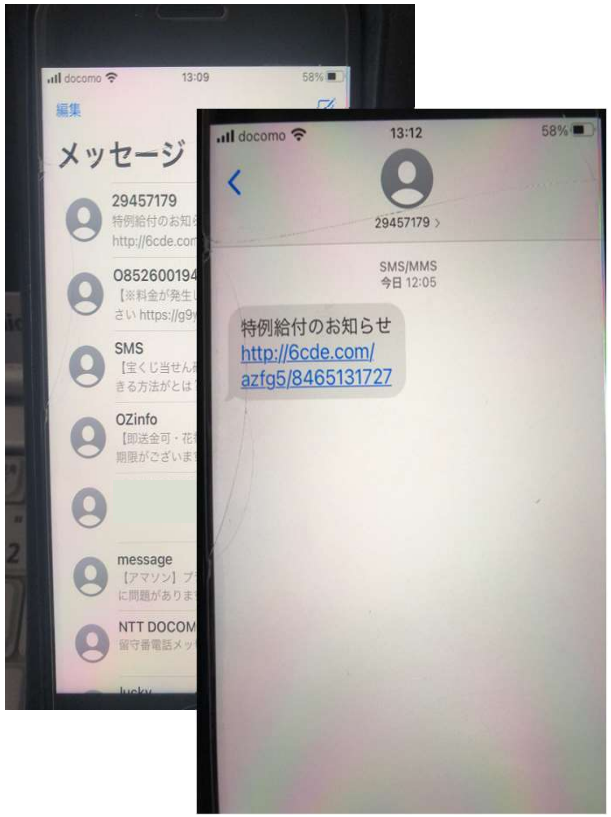
身近であることを意識・理解できていますか？

質問

サイバー攻撃を受けたことはありますか？

プライベート・仕事は問わず…

こんなのみたことありませんか？



フィッシング詐欺

メールやSMS等により、
クレジットカード情報、ネットバンキングに関する
各種情報、ID/パスワードなどを盗み出す行為

誰もがサイバー攻撃、サイバー犯罪の脅威にさらされている時代

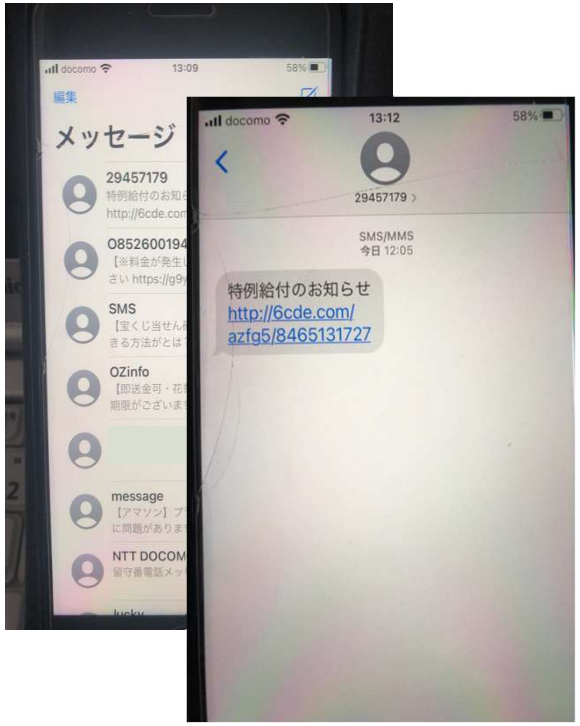
対策例

◇リンク、添付ファイルは開かない！

⇒攻撃手法が多様化しているので、QRを読まない、
[WIN＋r」「Ctrl＋L」「Ctrl＋V」を押さない！なども・・・。
なので、

公式アプリや**公式サイト**をみる！

⇒Google検索等で正規サイトを調べると、
正規サイトを語った偽サイトが上位に表示される
可能性があることにも留意。公式サイトはお気に入り登録を



◇万一リンク等を開いたとしても
クレカ番号、暗証番号等は**入力しない！**

⇒フィッシングが拡大しているなか、事業者が
メールやSMS経由でクレカ情報等の入力を要求することはあり得ない

サイバー攻撃の目的

◇サイバー攻撃の目的はお金

⇒「国家による諜報活動」「政治的・社会的主張を展開する集団の活動」等もあるが、
とりあえず認識すべきは「犯罪者・集団による金銭（営利）目的の活動」

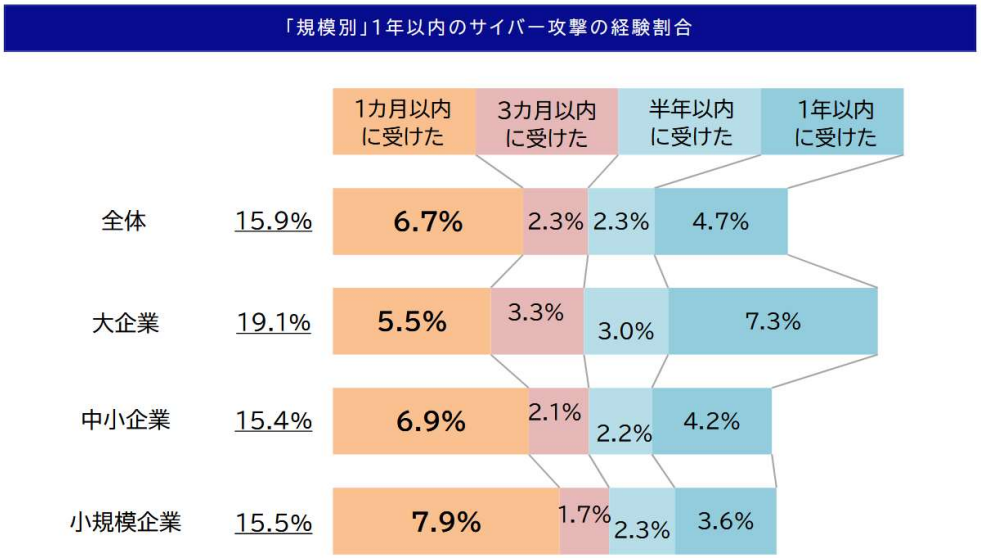
◇ネット上の詐欺師・泥棒によって、年間数千億（兆？）の被害

⇒証券口座乗っ取り、クレカ不正利用、SNS型投資詐欺、SNS型ロマンス詐欺、
ネットバンキング不正送金、ビジネスメール詐欺等、さまざまな手法が展開

当然法人も狙われる

◇個人だけを狙うわけもなく・・・。法人も当然狙われる

◇帝国データバンク調査(2025年6月公表)
　1年以内に攻撃を受けた企業は、15.9%　6社に1社！



よくあるサイバー攻撃（とその対策例）

3つほどご紹介

よくあるサイバー攻撃（とその対策例）

よくある事象　（サイバー保険のお支払いでよくあるもの）

- **サポート詐欺など、各種不正送金**
- **ウェブサイトの改ざん**
- **ランサムウェア**

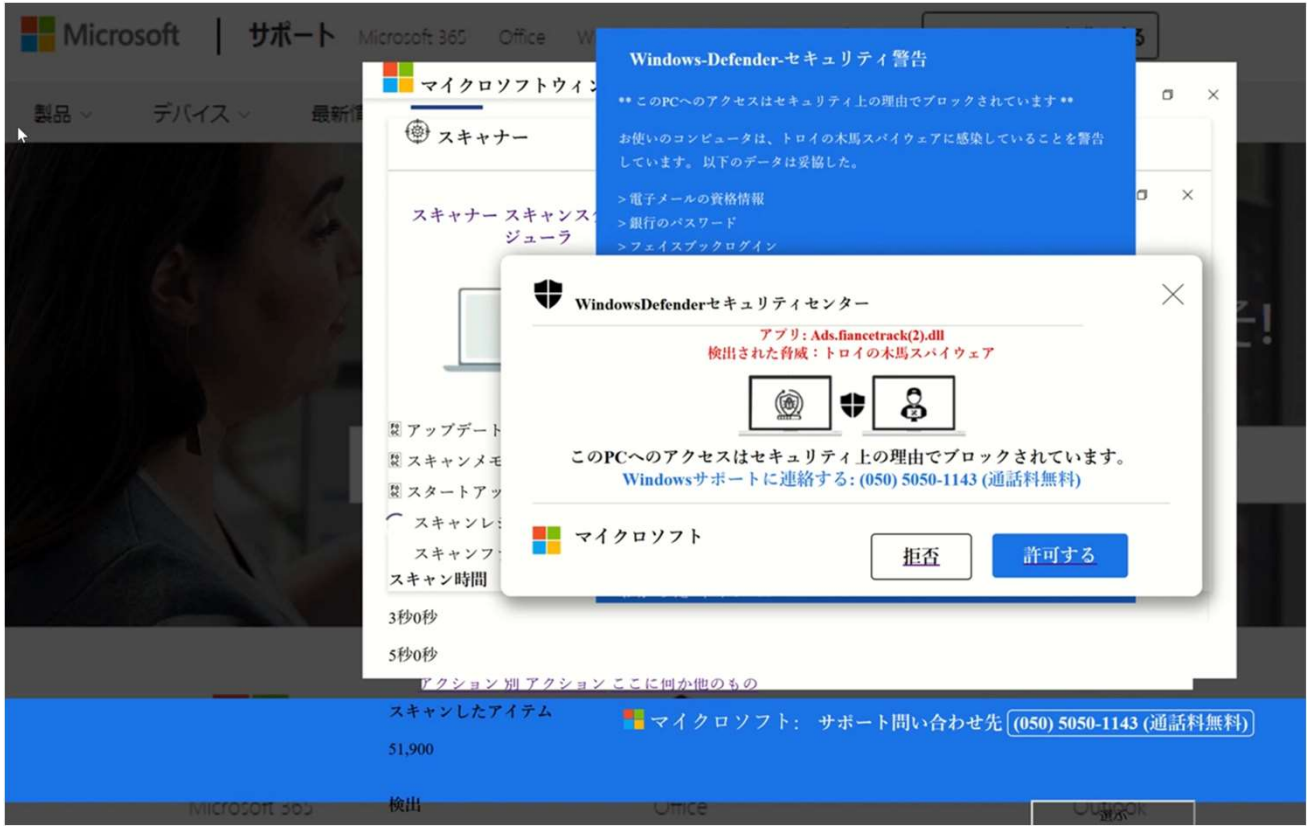
注意	ここ数年、よくあるサイバー攻撃・・・。 が、他にもあるし、今後、新たな攻撃が発現する可能性もある

サポート詐欺など、各種不正送金

～被害は個人だけではありません～

こんなのみたことありませんか？

◇ネットで探しものをしてたら、いきなり、こんな画面が・・・



サポート詐欺　～概要～

◇マイクロソフト等のサポートを装った単純な詐欺

◇**電話するとサポート料を要求**される。具体的には、
「コンビニ行って、電子マネー(Apple、Amazon、Google等)
を買ってこい！」と言われる(あなたマイクロソフトじゃないの？笑)

◇個人だけではなく、**法人の従業員**がひっかかる
事例も多い

◇最悪、遠隔操作ソフトを自らインストールするよう
誘導され、**PCが乗っ取られる**・・・
乗っ取られる＝PC内の情報漏えいの可能性・・・
各種事故対応も必要に

YouTubeに突撃動画がたくさん
投稿されています
(「サポート詐欺　TEL」で検索)
これをみるのもおすすめ！

サポート詐欺　～ネットバンキングを狙うパターンも～

◇電子マネーではなく、ネットバンキングの
　預金を狙うパターンも

◇巧みに、ネットバンキング利用端末に
　遠隔操作ソフトをインストールさせ
　パスワード等を聞き出して送金

◇被害事例

山梨の商工会	1,000万円	
滋賀の企業	4,250万円	
福島の企業	490万円	
福島の商工会	390万円	
埼玉の社団法人	1,000万円	
三重の福祉団体	100万円	など

サポート詐欺　～対策例～

◇相手にしない（ウイルスに感染していません）

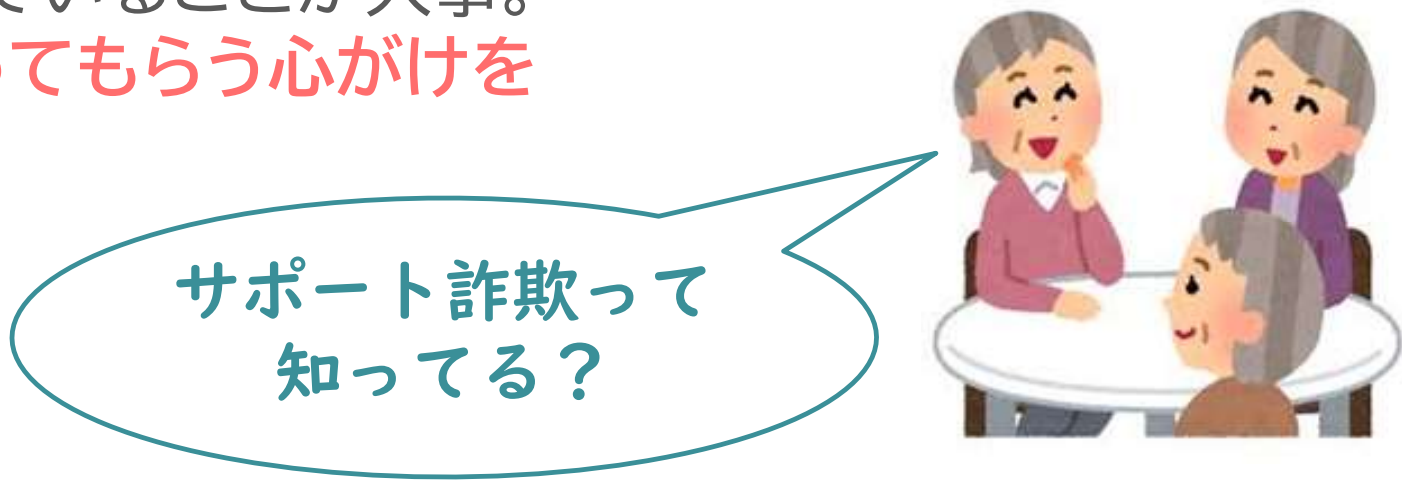
◇ブラウザを閉じる（ESCキーを長押しする、強制終了等）

◇電話しない（画面に電話番号が表示していても無視）

◇電話しちゃってもすぐに切る（いかにもアヤシイのでわかると思います…）

◇とにかく、知っていることが大事。

多くの人に知ってもらう心がけを



ビジネスメール詐欺①

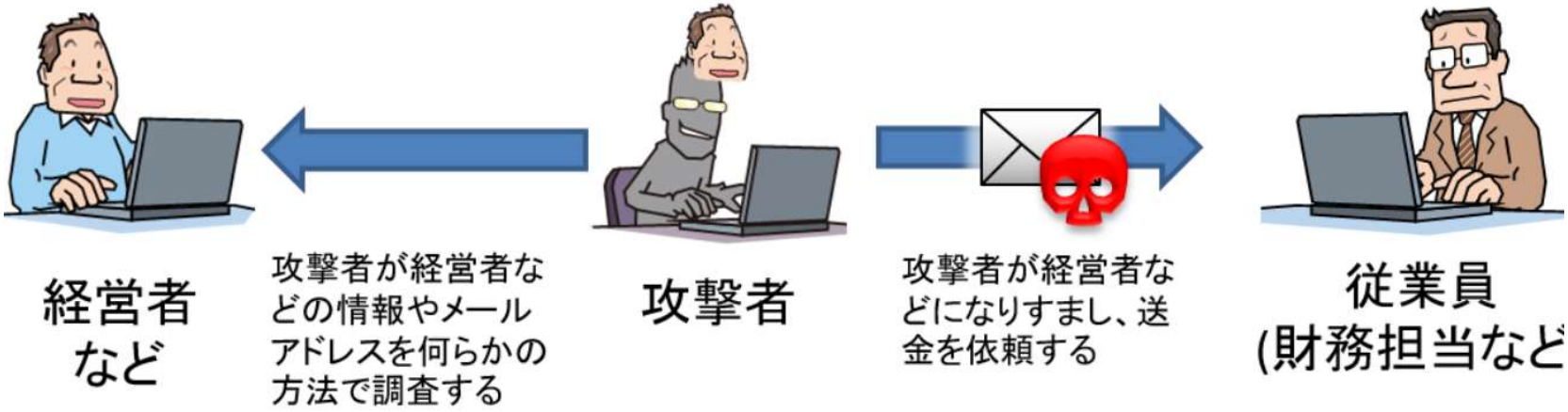
メールによる詐欺

◇Business Email Compromise･･･通称「BEC」

◇取引先や経営者を騙ったビジネス上のメールで送金を指示する詐欺

◇メールのやり取りを盗み見て、絶妙なタイミングで指示をしてくるケースも

◇上場企業において数千万、数億円の損失事例は多数発生



IPA「ビジネスメール詐欺（BEC）対策特設ページ」からの抜粋

ビジネスメール詐欺②

メールによる詐欺

◇2025年12月から、経営者を騙ったメールに始まり、**LINEグループに誘導**し、不正送金を図る事例が爆増

◇ウイルス配布型等、変化しながらの**現在進行形**

◇被害事例

長野の企業	2,950万円	
北海道の企業	4,980万円	
北海道の企業	8,000万円	
新潟の企業	4,000万円	
新潟の企業	1,900万円	
山形の団体	2,300万円	
三重の企業	1,000万円	
岐阜の企業	1億円	
長崎の企業	1,130万円	
船橋の企業	5,000万円	など

ウェブサイトの改ざん

～ホームページのセキュリティ…。考えていますか？～

ウェブサイトの改ざん　～概要～

◇ホームページ等、ウェブサイトが改ざんされる事例は昔も今も多く発生

◇各種データベースと繋がっていると、情報漏えいの可能性も

◇ECサイトでは利用者が入力するカード情報の窃取を狙った改ざんも
不正利用等で高額賠償金が発生するケースも

◇とにかく、ホームページのセキュリティ対策ができていない企業が多すぎる

ウェブサイトの改ざん　～対策例～

◇セキュリティがわかっているホームページの制作会社に相談

⇒「ホームページのセキュリティ対策ができていない企業が多い」のは、
セキュリティがわかっていない、わかっているけど十分説明できていない制作会社が多いかもしれない・・・

◇それなりにお金をかける

⇒ホームページは、セキュリティ対策コストをかけずに公開するものではない・・・

◇セキュリティベンダのサービス等も検討する

⇒セカンドオピニオンも含め、セキュリティ本業の人と対策を検討

◇自社ECサイトは相当の覚悟をもって
構築する必要アリ

⇒まずは、自社ではなく、楽天、Yahoo、Amazonでの検討
自社ECサイトのセキュリティ対策コストはかなりの額・・・

ランサムウェア

～最近の一番の脅威～

ランサムウェア　～概要～

◇Ransom（ランサム）＝**身代金**
◇データを**暗号化**。復号（回復）と引換に身代金を要求するウイルス
◇システム停止等で業務が阻害。**取引先・顧客にも迷惑をかける事態に**
◇次のような事例で誰もが知るところに

2021年10月　徳島のつるぎ町立**半田病院**
2022年　3月　**トヨタ**の工場停止（サプライヤーである小島プレス工業が感染）
2022年10月　**大阪急性期・総合医療センター**
2023年　7月　**名古屋港**（名古屋港運協会）
2024年　6月　**KADOKAWA**（ニコ動、ドワンゴ）
2025年　9月　**アサヒGHD**
2025年10月　**アスクル**
2026年　2月　**日本医科大学武蔵小杉病院**

ランサムウェア　～一番の脅威～

◇IPA(注)が毎年発表している
「情報セキュリティ10大脅威」において
直近(2026/1/27公表)の**第1位！（6年連続）**

(注)アイピーエー。独立行政法人情報処理推進機構。経済産業省、デジタル庁共管の独立行政法人。サイバー攻撃から企業・組織を守る取組み等を実施
「中小企業の情報セキュリティ対策ガイドライン」など多くのセキュリティ関連のコンテンツを公開

順位	内容
1位	ランサム攻撃による被害
2位	サプライチェーンや委託先を狙った攻撃
3位	AIの利用をめぐるサイバーリスク
4位	システムの脆弱性を悪用した攻撃
5位	機密情報を狙った標的型攻撃

IPA「情報セキュリティ10大脅威 2026」

◇政府組織、セキュリティの業界団体、多くのセキュリティベンダ等を含めて、**業界の一番の関心事＆脅威はランサムウェア！**

ランサムウェア　～大企業だけではない～

◇警察庁の広報資料からも被害拡大は明らか！！！

はじめに

令和７年上半期においては、政府機関、金融機関等の重要インフラ事業者等における DDoS 攻撃とみられる被害や情報窃取を目的としたサイバー攻撃、国家を背景とする暗号資産獲得を目的としたサイバー攻撃事案等が相次ぎ発生したほか、生成 AI を悪用した事案等の高度な技術を悪用した事案も発生している。このようなサイバー攻撃の前兆ともなるぜい弱性探索行為等の不審なアクセス件数は前年に引き続き高水準で推移しており、その大部分が海外を送信元とするアクセスが占めている。また、令和７年上半期におけるランサムウェアの被害報告件数は 116 件と、令和４年下半期と並び最多となっており、このようなランサムウェアの被害拡大の背景には、ランサムウェアの開発・運営を行う者が、攻撃の実行者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（RaaS）を中心とした攻撃者の裾野の広がりがあると指摘されている。

また、情報通信技術の発展が社会に便益をもたらす反面、インターネット空間を悪用した犯罪も脅威となっている。例えば、インターネットバンキングに係る不正送金、証券口座への不正アクセス・不正取引、SNS を通じて金銭をだまし取る詐欺、暗号資産を利用したマネー・ローンダリングが発生するなど、インターネット上の技術・サービスが犯罪インフラとして悪用されている実態が見られる。

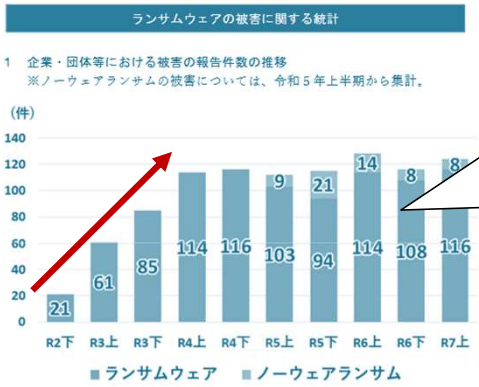
さらに、インターネット上には、規制薬物の広告等の違法情報や犯罪を誘発するような有害情報が存在するほか、近年 SNS 上に氾濫する犯罪実行者募集情報は深刻な治安上の脅威となっている。

このような状況に対し、警察では検挙に向けた取組を進めており、例えば、全国のクレジットカード情報不正利用関連犯罪を分析し、不正に取得・売買されたクレジットカード情報の支払いに用いられたと認められる暗号資産の流れを捜査した結果、令和６年９月から令和７年３月までの間に、サイバー特別捜査部及び関係都道府県警察において、男女 20 名の被疑者を検挙した。

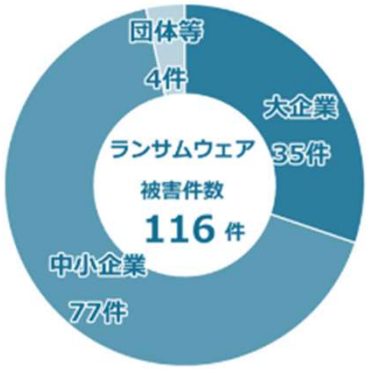
このほか、警察庁では、中国を背景とするサイバー攻撃グループ「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリーの共同署名に加わり、パブリック・アトリビューションとしてアドバイザリーを公表するとともに、ランサムウェア「Phobos/8Base」により暗号化されたデータを復号するツールを開発し広く周知するなど、被害の未然防止・拡大防止に向けた様々な取組を実施している。

本資料は、第１部で令和７年上半期中のサイバー空間の脅威情勢を、第２部で警察の取組を取りまとめたものである。

警察庁サイバー警察局
「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」

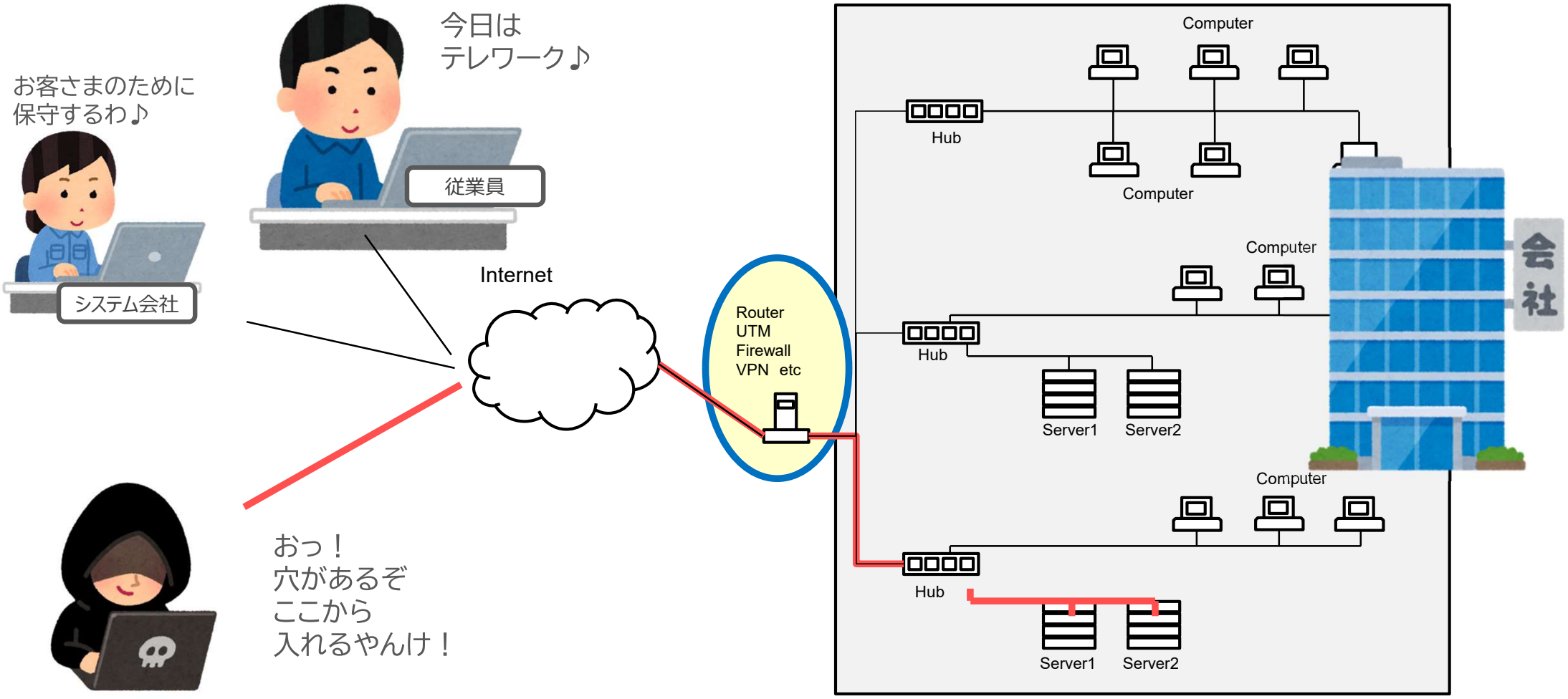


2020年下期に比し
2025年上期は約6倍
高水準で推移



大企業だけの被害
ではない。
中小企業や団体等の
被害が約7割

ランサムウェア　～侵入イメージ～



参考　インターネットに接続された機器

◇いろいろなものがインターネットに接続されている･･･。

スマホ、PC、ネットワーク関連機器（ルーター、VPN等）、テレビ、
HDDレコーダー、エアコン、ドラレコ、ウェブカメラ等




◇接続されているということは、逆に
他人につなげられる（見られる）可能性もある･･･。

ランサムウェア　～対策例～

◇インターネットに接続している機器・サービスの**管理徹底**
とりわけVPN、リモートデスクトップツールといった、
会社のネットワークに接続するための機器・サービス

管理を徹底すべきものの一例
①脆弱性対応
・・・OS・ソフトウェアの更新等（ITベンダへの確認）
②認証情報の適正な運用
・・・複雑なID/パスワード設定、二要素認証の導入（ITベンダへの確認）

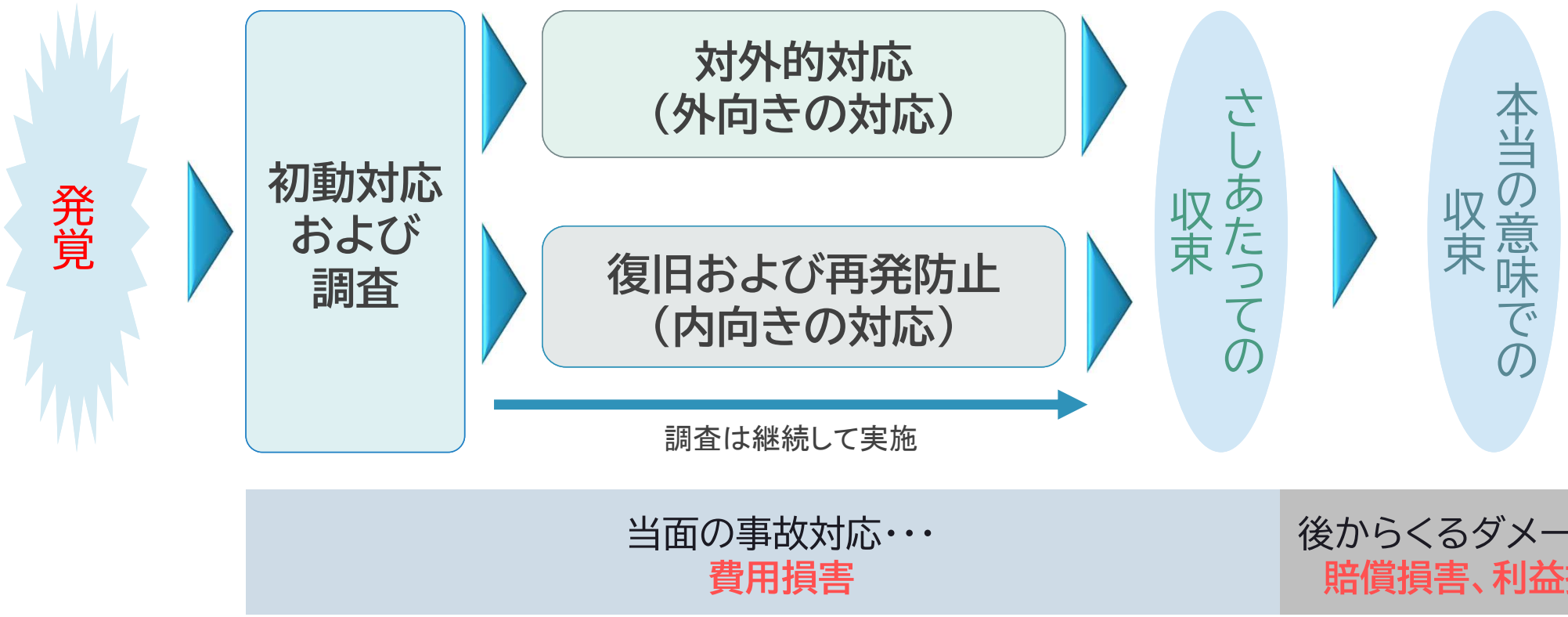
◇バックアップ対策
⇒「バックアップも狙われる」ことを前提とした**オフライン**での
バックアップ。そのバックアップから、**着実・迅速な復旧**が
行えるよう**定期的な訓練**

パート２

サイバー攻撃を
受けると
お金がかかる

インシデント発生時の流れ

各場面において、費用損害、賠償損害、利益損害が発生・・・



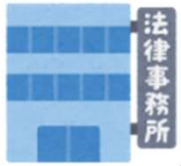
費用損害

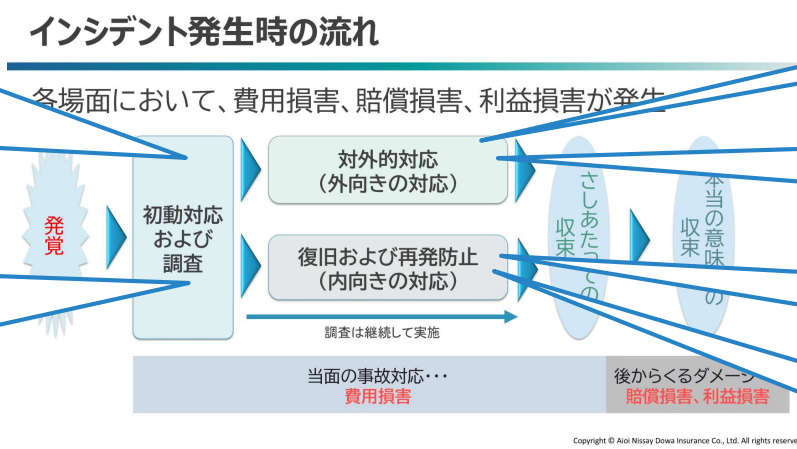
専門の会社に調査
（フォレンジック調査）を委託

900万円

法律事務所に
対応等を相談

300万円





被害者に詫び状を送付

1,300万円

コールセンター会社に
クレーム対応を委託

6,000万円

出入りのITベンダに
システム復旧を依頼

5,000万円

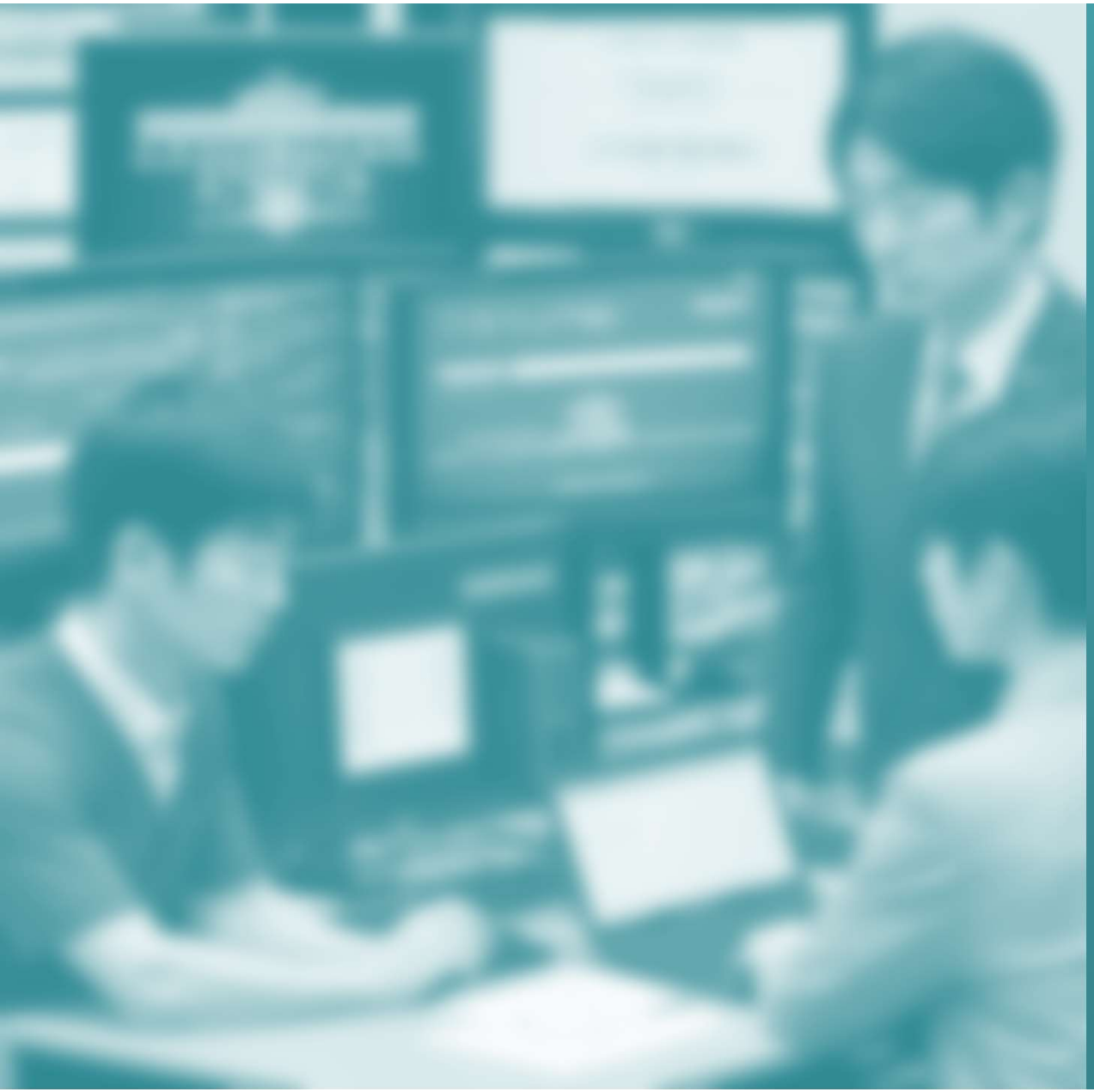
セキュリティベンダに
再発防止策を依頼

2,000万円

自社だけでの対応は困難…。専門会社へのアウトソーシングも必要
そのコスト負担は過大なものに（費用損害）

塵も積もれば

・・・山となる。

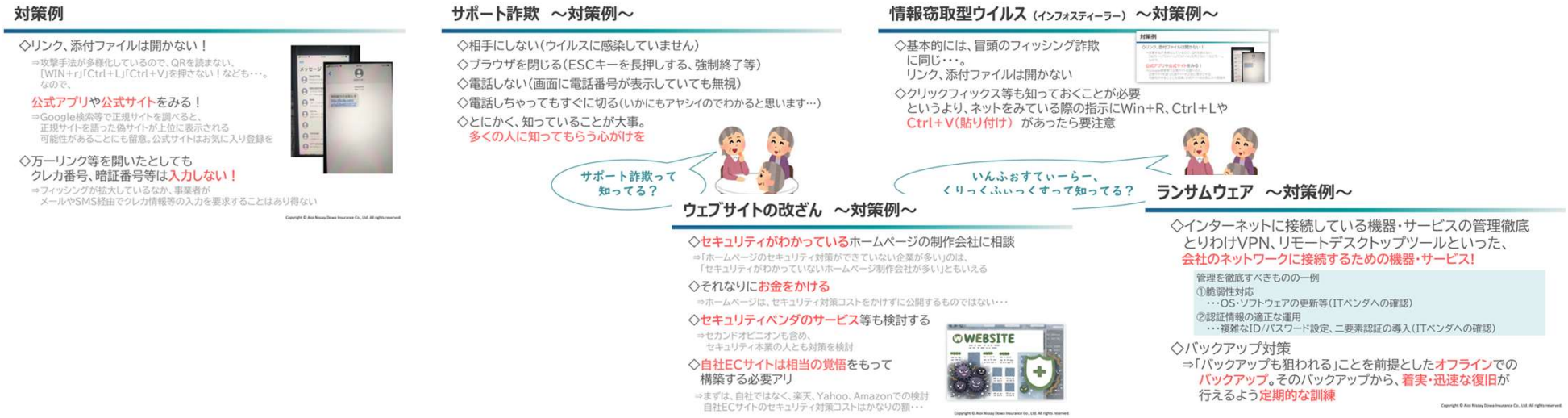


パート3
サイバー攻撃
の対策は
事後対策も重要

対策のポイント

◇実際に、**よくあるサイバー攻撃を踏まえた対策を！**
（今、実施の対策は、よくあるサイバー攻撃の対策ですか？）

◇セキュリティ機器・サービスの導入（技術的対策）ほか、
組織・ルール作り、従業員教育も



システム会社/ITベンダへの相談も！

◇対策には次のような種類があります

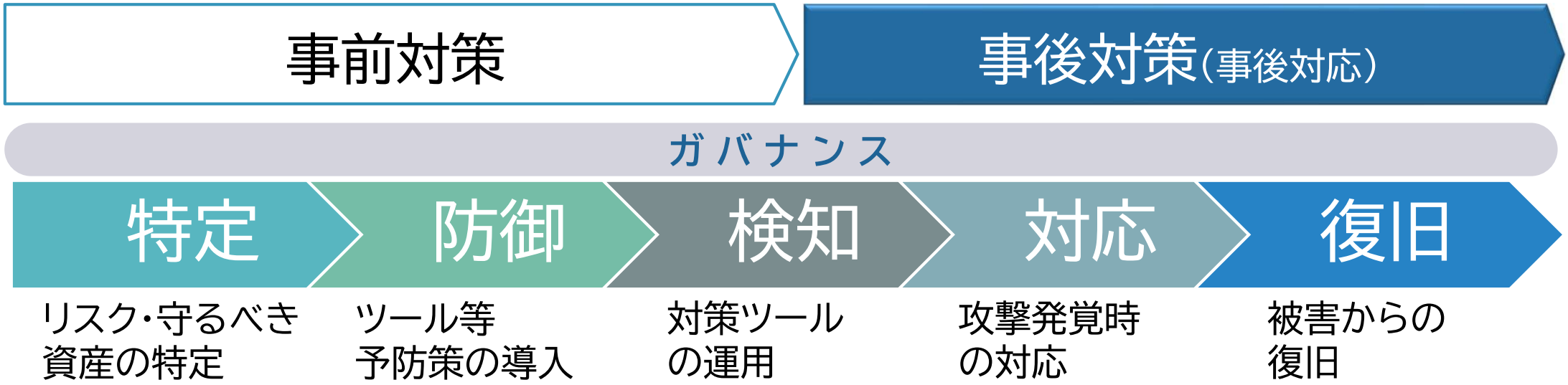
技術的対策	UTM(中小企業で多く導入されている総合型のセキュリティ機器・サービス)や、 バックアップ対策(特にオフラインでの保存)など
人的対策	従業員教育　など
組織的対策	ルール作り(セキュリティポリシー、事故発生時の体制整備)など
物理的対策	入退出の管理、盗難・紛失・持出し対策　など

◇うち、技術的対策は、システム会社/ITベンダに相談しましょう

餅は餅屋です！

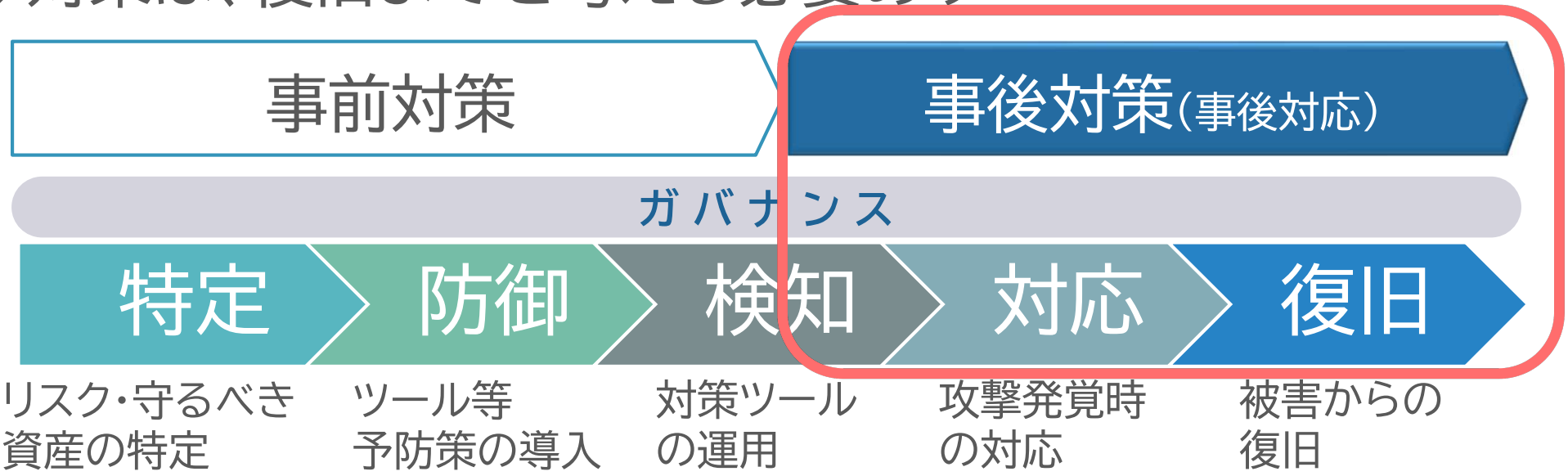
事後対策について

対策を時系列的にとらえると
「事前」と「事後」の2つ



事後対策も重要

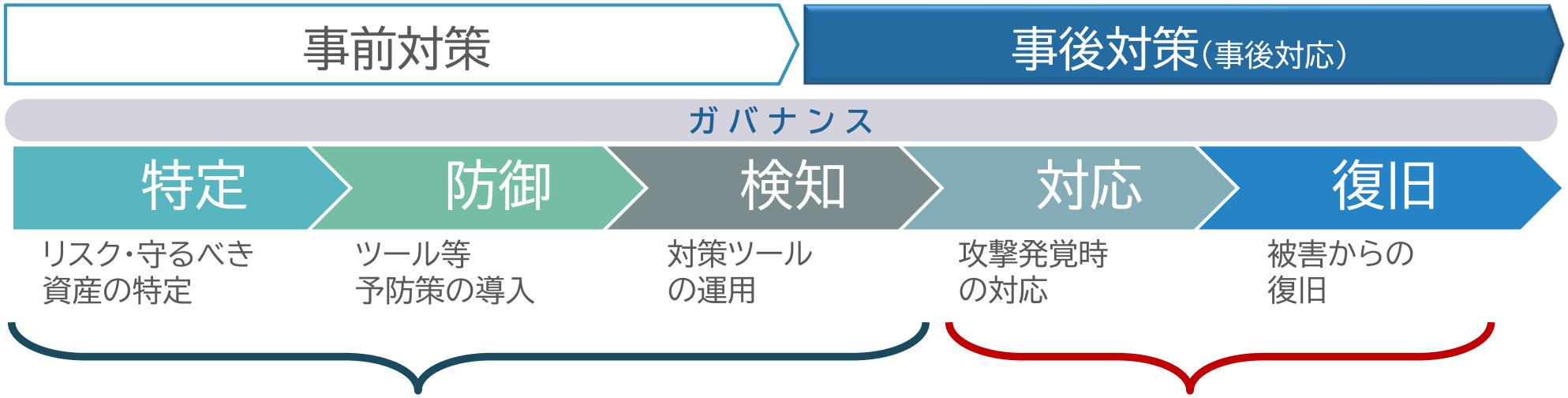
◇対策は、復旧までを考える必要あり



事前対策ほか、復旧までを考えた
事後対策の**両方が必要！**

パート４
サイバー保険

保険の必要性



事前対策

ウイルス対策ソフトは当然のこと、
UTM、バックアップ等による技術的対策
従業員教育による人的対策
ルール作り等の組織的対策　など

＋

事後対策

被害の極小化、早期復旧のための経済的な備え
⇒サイバー保険

など

サイバー保険

対象とする事故

①サイバー攻撃
②他人の情報の漏えいまたはそのおそれ
③IT事故(※)

※コンピュータシステムの所有、使用もしくは管理、または電子情報の提供に伴う、
他人の業務の阻害、電子情報の消失など

不測かつ突発的な事由によるネットワーク停止

対象とする損害

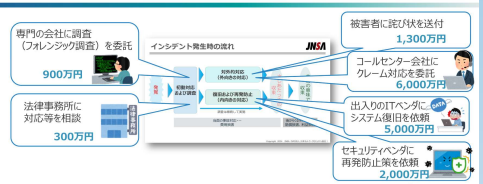
①②③による
費用損害(当面の事故対応にかかる自社コスト)

②③による
賠償損害(損害賠償金、弁護士報酬等)

利益損害(営業利益、固定費等)

具体例

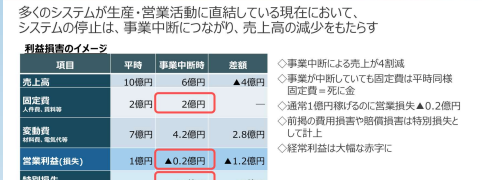
費用損害



自社だけでの対応は困難…。専門の会社へのアウトソーシングも必要
そのコスト負担は過大なものに（費用損害）

賠償損害

利益損害



前掲、**費用損害、賠償損害、利益損害を補償**

一例：事後対策（事後対応）のサービス

◇火事が起きたら「119番」・・・
　サイバー攻撃が起きたら？

◇保険会社が事故対応を支援
　⇒24時間365日の電話相談、
　　事故原因の調査を行う専門業者
　　の紹介・コーディネイトなど

◇サイバー保険の機能は、
　保険金支払だけではなく、
　この事故対応の支援が大きい

おわり

ご清聴ありがとうございました

サイバーはひとごとじゃない！
自分事、自分たち事！全員参加！

サイバー攻撃の対策の一つとして
サイバー保険をご検討いただければ幸いです