日本のサイバーセキュリティを「連携」「学び」「創造」

JNSA全国サイバーセキュリティセミナー2024

抵抗力と回復力が
新しいサイバーセキュリティ対策のカギ

特定非営利活動法人日本ネットワークセキュリティ協会
マーケティング部会　副部会長

持田啓司（株式会社ラック）

本日の講演内容は、持田の個人的見解であり、JNSAおよびラックグループの意見を代弁するものではありません。

自己紹介

- 所属・名前
  - 株式会社ラック
    サイバー・グリッド・ジャパン　CYBER GRID JAPAN
  - 持田 啓司（もちだ ひろし）
- 専門分野
  - 人材育成、組織開発
- 業務内容
  - 人事関連制度のコンサルタント（育成、評価等）
  - 業界団体の運営
  - 政府系会議の委員
- 社外活動
  - 業界団体活動
    - NPO 日本ネットワークセキュリティ協会
    - サイバーセキュリティイニシアティブジャパン (CSIJ) 事務局長
    - 一般社団法人ソフトウェア協会
    - 一般社団法人日本IT団体連盟
    - NPOスキル標準ユーザー協会 教育企画委員会 委員
    - 人材育成学会 会員
    - 一般社団法人日本ITストラテジスト協会 会員
  - 官公庁等委員
    - 総務省、経済産業省、(独)情報処理推進機構

agenda

- 始めに
- 数字で見る被害状況（警察庁広報資料より）
- サイバー攻撃を受けるとお金がかかる（JNSA調査より）
  - 各種損害のコスト
  - 実際の被害状況
- 事件から見る攻撃事例
- 企業における対策の考え方
  - NIST　CSF
  - METI　サイバーセキュリティ経営ガイドライン
  - NISC　サイバー攻撃被害に係る情報の共有・公表ガイダンス

始めに

なぜ中小企業としてもサイバーセキュリティを気にしなければならないのか？

近年のサイバーセキュリティリスク

- 情報セキュリティ白書2024（IPA）
  - 守るだけではない、被害を最小限にするためのセキュリティ対策

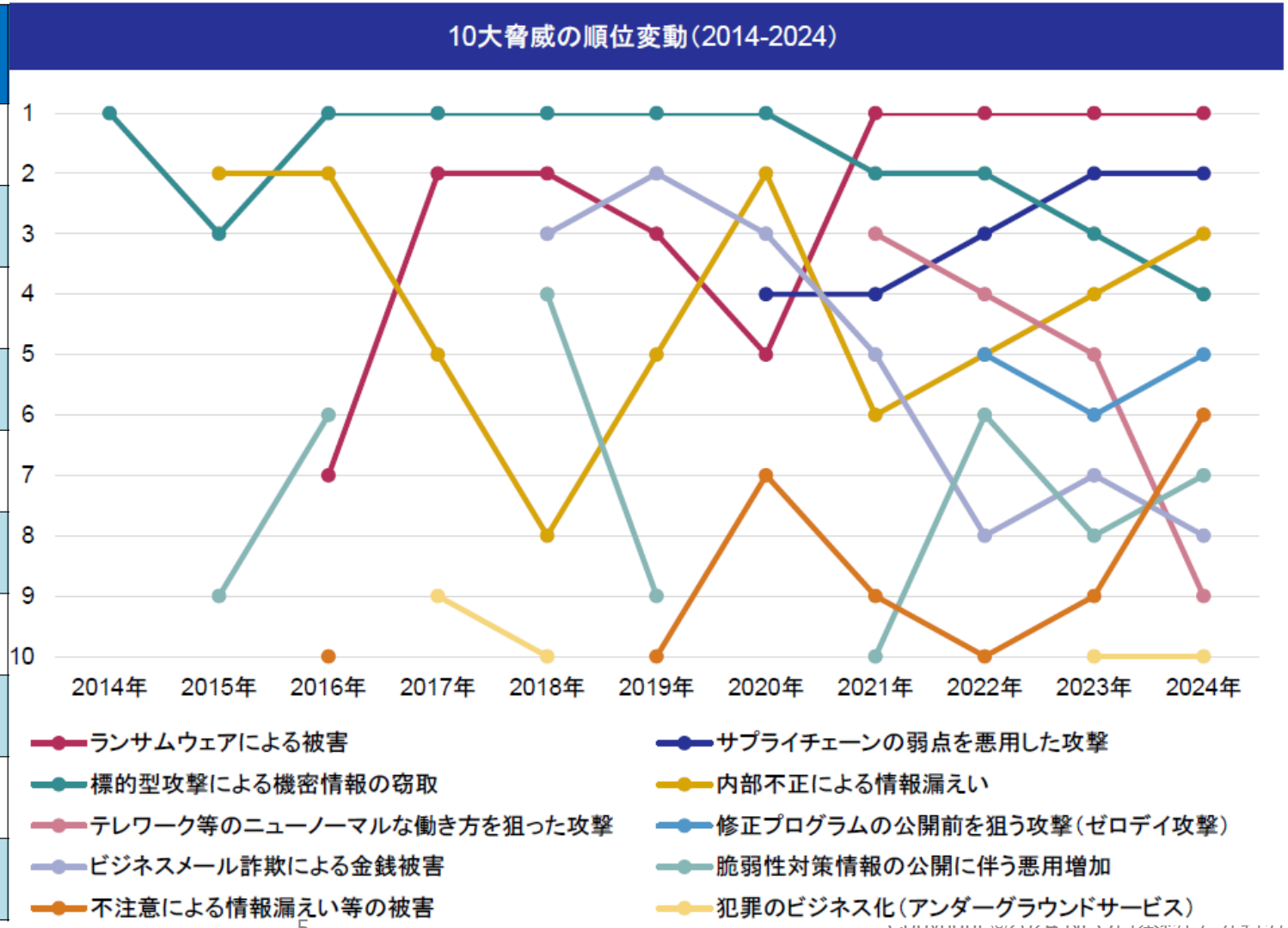
- 情報セキュリティ10大脅威（IPA）
  - 犯罪者はビジネスとして組織化して攻撃を行っている
    - 1　ランサムウェアによる被害
    - 2　サプライチェーンの弱点を悪用した攻撃
    - 3　内部不正による情報漏えい等の被害
    - 8　ビジネスメール詐欺による金銭被害
    - 10　犯罪のビジネス化（アンダーグラウンドサービス）

- ツールの活用とソーシャルエンジニアリングの複合攻撃
- 攻撃者優位の現状

- 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（警察庁）
  - フィッシング報告件数：119万6,390件（前年比で22万7,558件増加）、過去最多
  - ランサムウェアによる被害報告：197件、規模・業種を問わず被害が発生

情報セキュリティ10大脅威（IPA）

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6	不注意による情報漏えい等の被害
7	脆弱性対策情報の公開に伴う悪用増加
8	ビジネスメール詐欺による金銭被害
9	テレワーク等のニューノーマルな働き方を狙った攻撃
10	犯罪のビジネス化（アンダーグラウンドサービス）



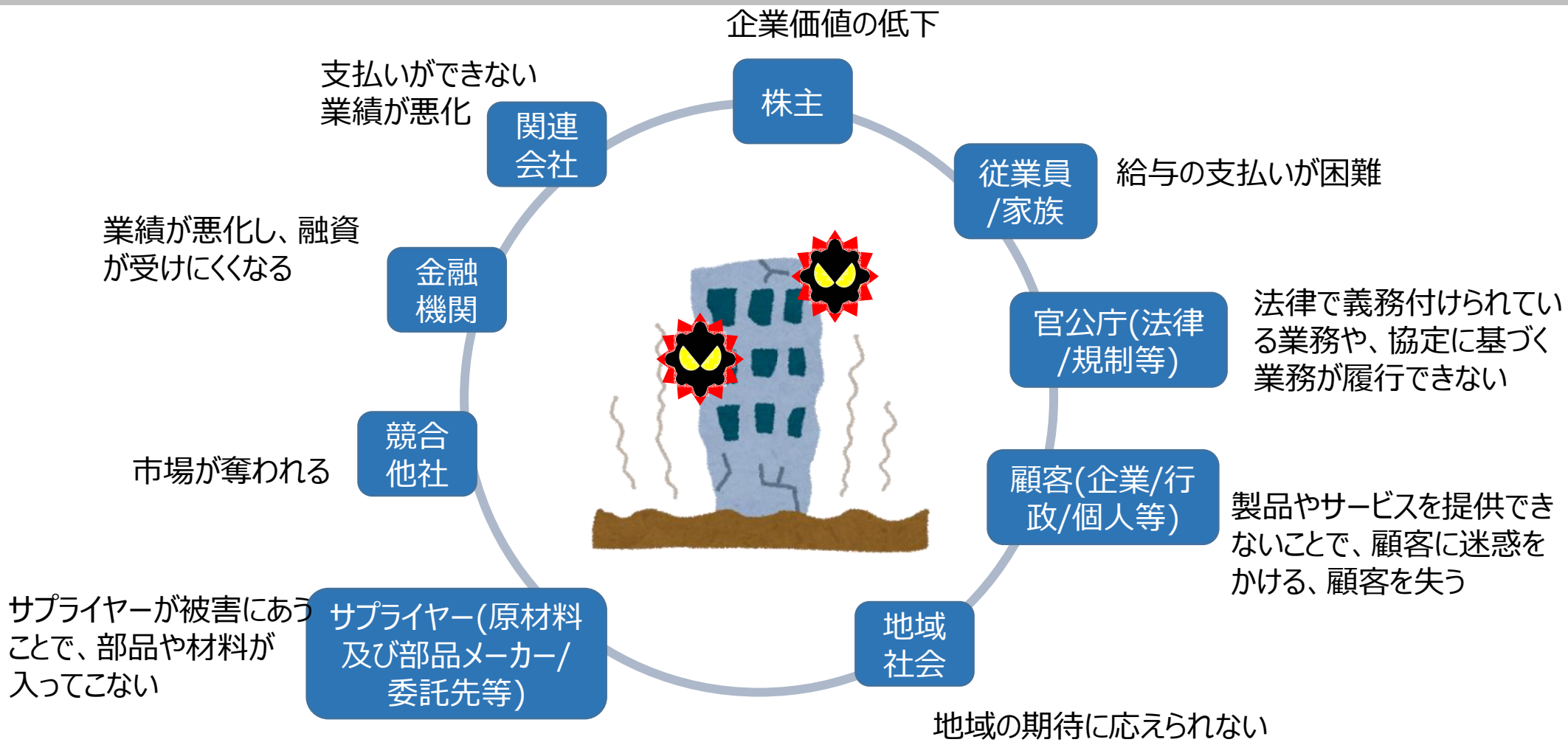
サイバーを取り巻く状況

- サイバー空間を巡る昨今の状況
  - サイバー攻撃の**洗練化・巧妙化**が一層進展
  - **生成AI等の新技術の普及**に伴う新たなリスクも増大

- サイバー攻撃のリスクとの**共存が避けられない**時代
  - 攻撃を受けた際の抵抗力から回復力までを想定した対策が求められる

- 経済社会の活力向上及び持続的発展
  - サプライチェーン・リスクへの対応強化とDX推進・支援の強化が重要
  - 多くの**中小企業が主要な取引企業**として参加する

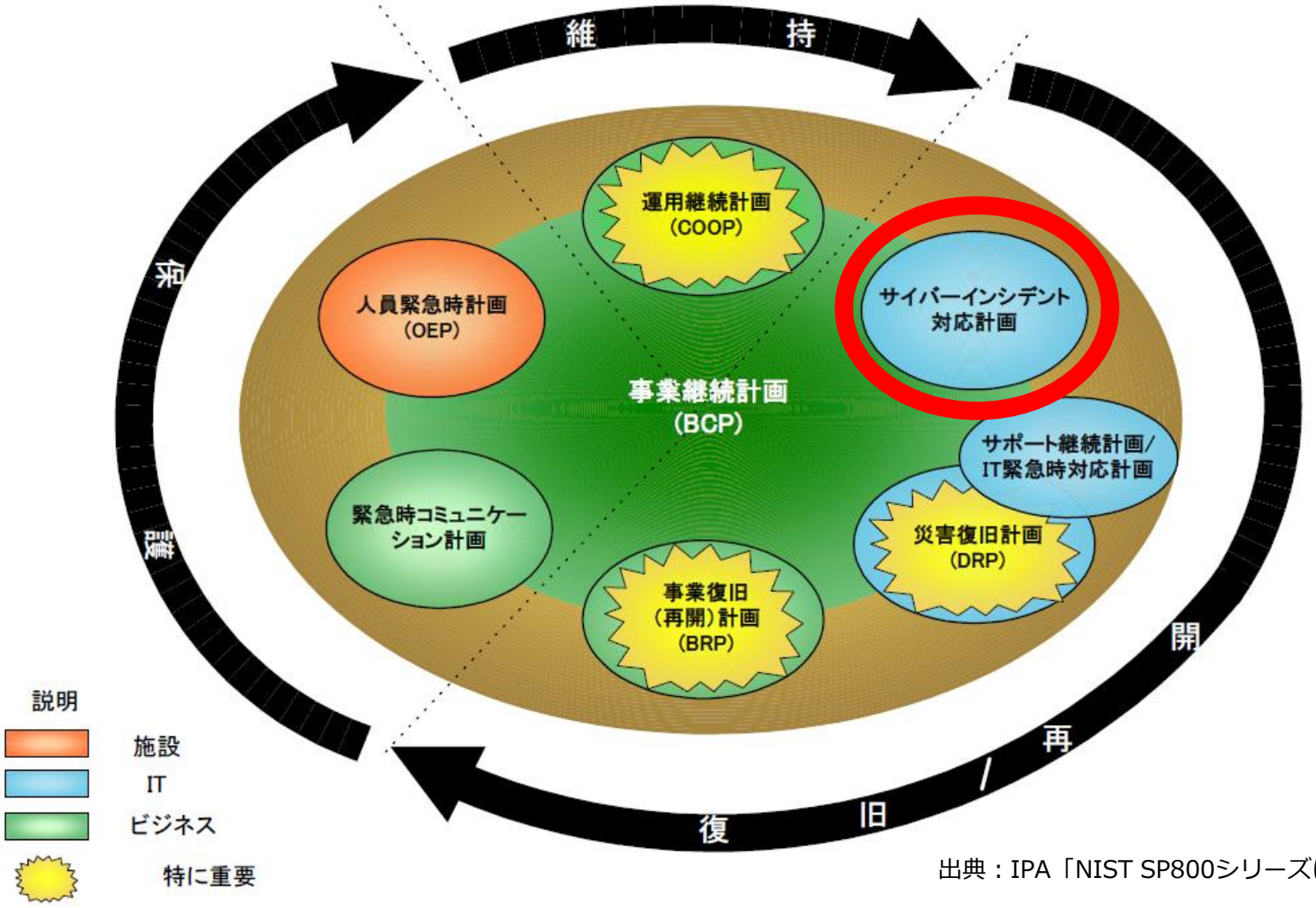
サイバーインシデントによるステークホルダーへの影響



想定される被害例

想定リスク		サイバー攻撃	他の災害例（地震）
リソース	人	影響低	•怪我 •出社不能
	社会インフラ	影響低	•停電、断水 •交通マヒ
	建物	影響低	•損壊 •入館不可
	資金	•壊れた資産の復旧・調達 •情報漏えい賠償 •改ざん復旧費用	•壊れた資産の復旧・調達
	取引先等	影響低	•同時被災 •調達停止
	IT機器	•破損 •使用不可	•破損 •使用不可
	データ	•データの破損 •改ざん・情報漏洩の可能性	•データの破損

セキュリティは事業リスクの一つとして捉えること



出典：IPA「NIST SP800シリーズに見る情報セキュリティと事業継続計画」

あらためて本日のテーマは！

「アタフタしないためのセキュリティ前始末のすすめ」
～組織に求められる困難をしなやかに乗り越え回復する力～

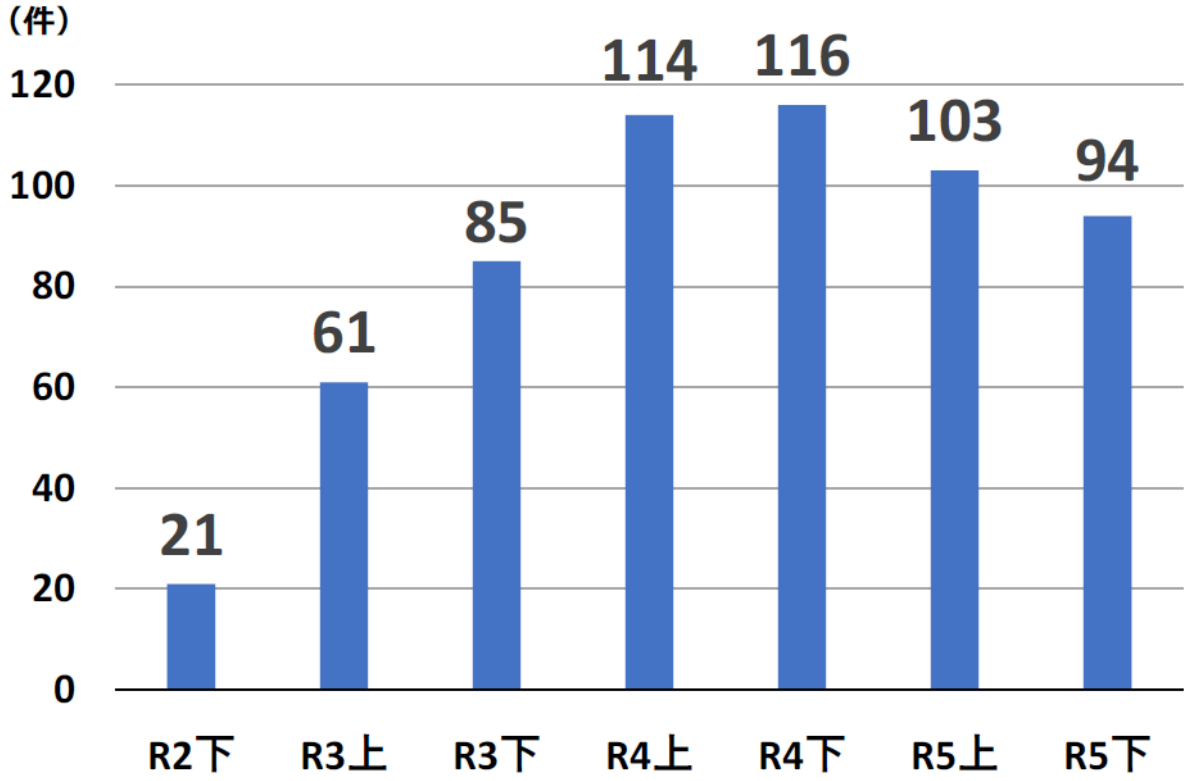
- 中小企業はお金や人材不足でセキュリティ対策できない
  - 何か事が起きたときに対応が難しく、余裕がないため窮地に追い込まれやすい
- だからこそ
  - 事が起こったときのために**常に準備**
  - 事が起こっていないか**継続的に実行**
- 結果として
  - 事が起こったときに**早期に回復**が行える

数字で見る被害状況

中小企業で起こっていること

警察庁　広報資料より

ランサムウェアによる被害概況（報告件数）

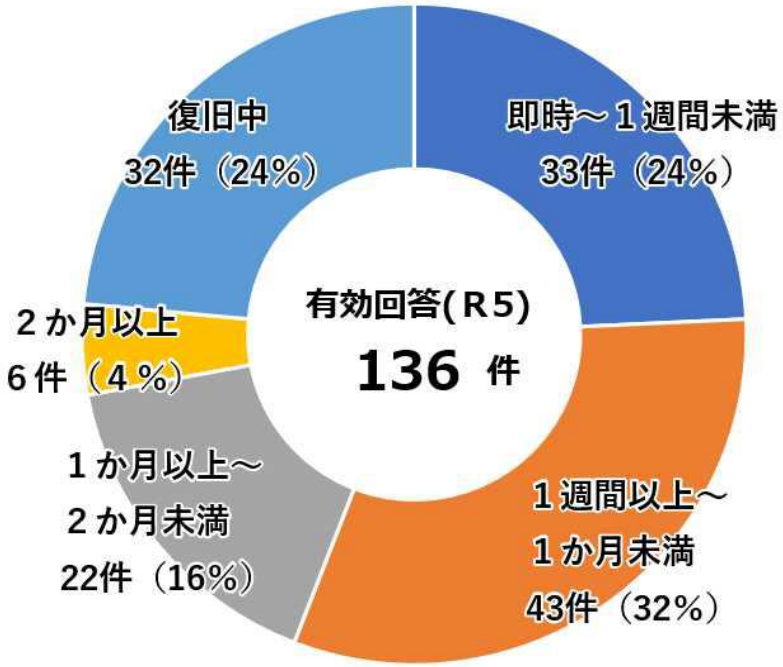


■ 企業・団体等におけるランサムウェア被害の報告件数の推移

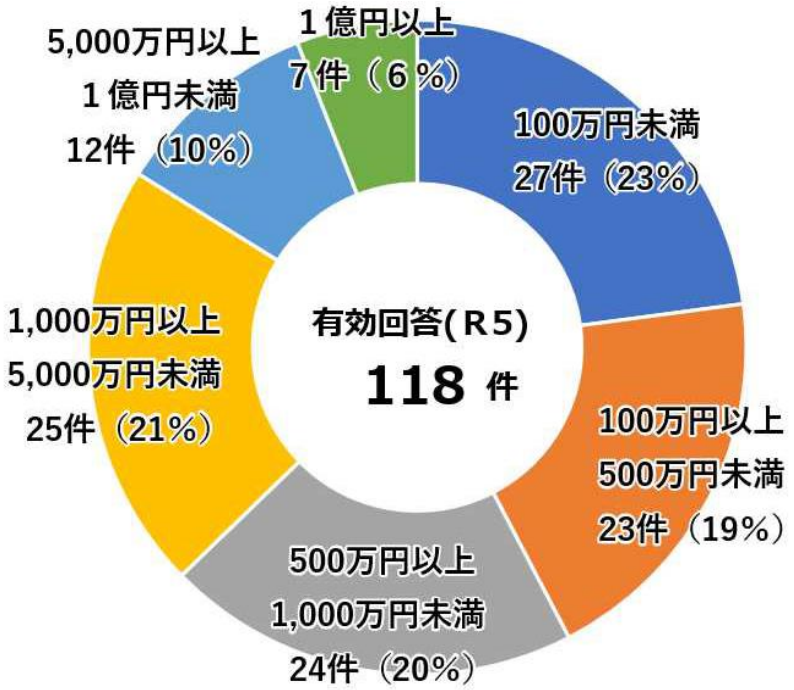
ランサムウェア被害は、令和４年上半期以降、高い水準で推移

出典：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
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

ランサムウェアによる被害概況（復旧期間、費用）



■ 復旧に要した期間



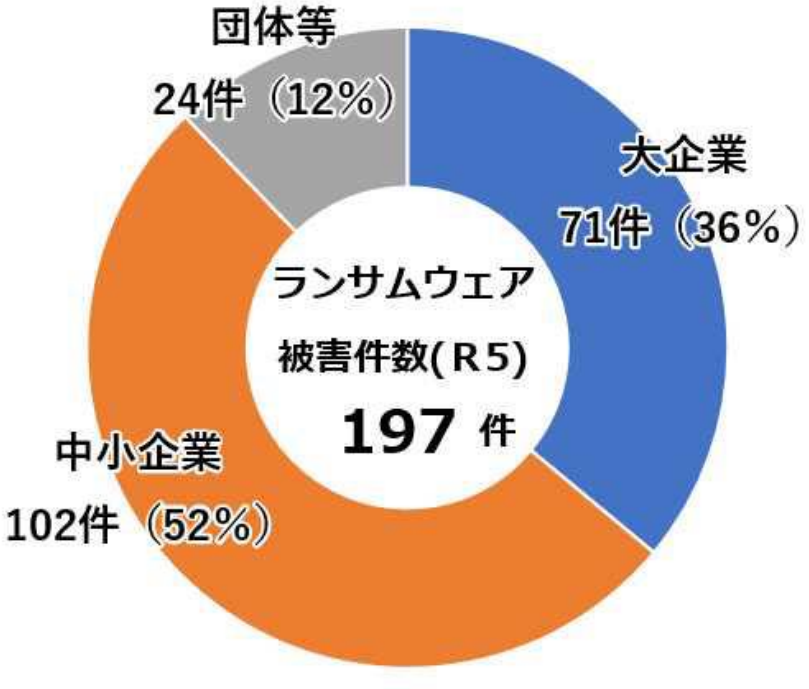
■ 調査・復旧費用の総額

復旧までに１か月以上を要したものが28件（136件中）

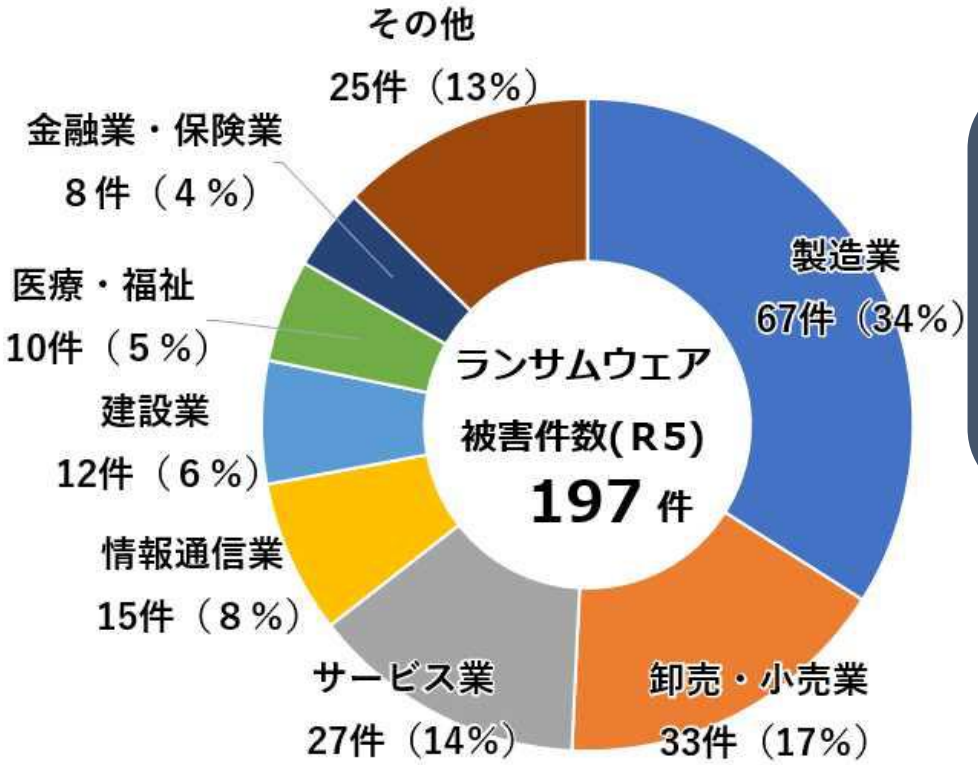
調査・復旧費用総額が1,000万円以上を要したものが44件（37%）

出典：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
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

ランサムウェアによる被害概況（規模、業種）



■ 被害企業・団体等の規模別報告件数

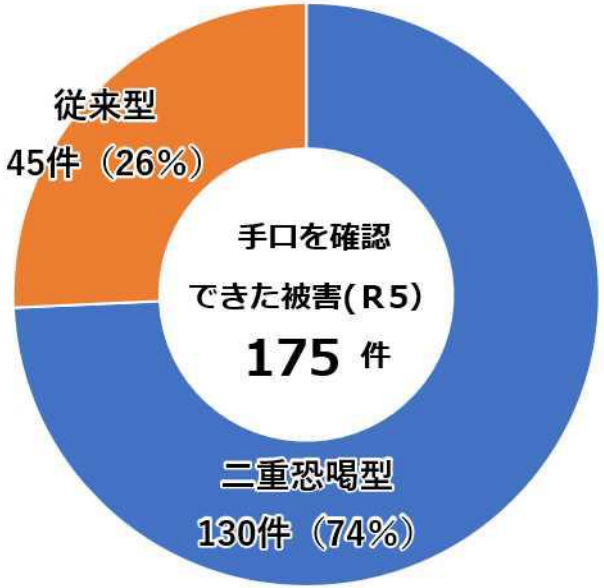


■ 被害企業・団体等の業種別報告件数

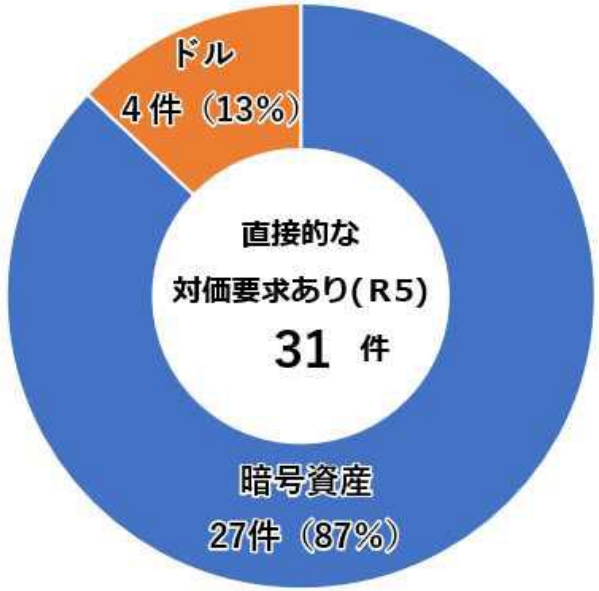
ランサムウェア被害は、規模や業種に関係なく被害が広がっている

出典：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
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

ランサムウェアによる被害概況（特徴）



■ ランサムウェア被害の手口別報告件数



■ 要求された対価支払い方法別報告件数

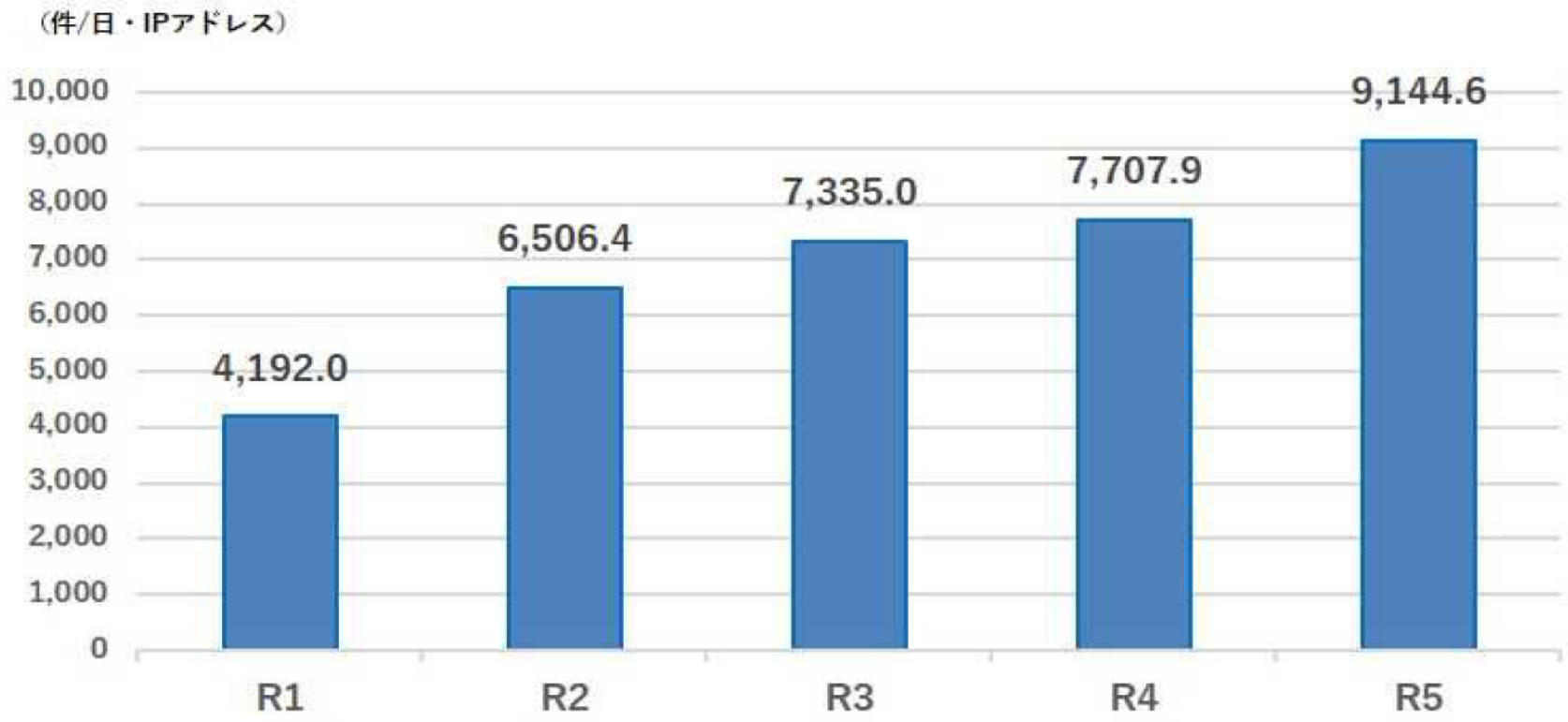
手口は二重恐喝（ダブルエクストーション）が多くを占める

対価支払いは暗号資産が多くを占める

二重恐喝（ダブルエクストーション）
要求1：データを復号してほしければ対価を払え。
要求2：データを公開してほしくなければ対価を払え。

出典：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
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

サイバー空間における脆弱性探索行為等の観測状況



■ **警察庁のセンサーにおいて検知したアクセス件数の推移**

１IPアドレス当たりのアクセス件数は継続的に増加（攻撃しやすいところを無作為に調査）

出典：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
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

サイバー攻撃を受けるとお金がかかる

～インシデント損害額調査レポートから考える サイバー攻撃の被害額～

JNSA 調査研究部会 インシデント被害調査WG

各種損害のコスト

～アウトソーシング先のヒアリング等からみえてくるコスト～

各種損害をアウトソーシング先のコスト等を踏まえてみると、中小企業においても数千万単位、場合によっては億単位の損害が発生する

インシデント対応の流れとアウトソーシングの必要性

専門の会社に
調査を委託

コールセンター会社に
対応を委託

発覚

初動対応
および調査

対外的対応
（外向きの対応）

復旧および再発防止
（内向きの対応）

収束

調査は継続して実施

出入りのITベンダに
システム復旧を
委託

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

インシデント発生時において生じる損害

各種事故対応についてアウトソーシング先への支払が発生

1．費用損害（事故対応損害）	被害発生から収束に向けた**各種事故対応**に関してアウトソーシング先への支払を含め、自組織で直接費用を負担することにより被る損害（下記２～６に該当しないもの）

さらに、次のような損害の発生も起こりうる

2．賠償損害	情報漏えいなどにより、第三者から損害賠償請求がなされた場合の**損害賠償金**や弁護士報酬等を負担することにより被る損害
3．利益損害	ネットワークの停止などにより、事業が中断した場合の**利益喪失**や、事業中断時における人件費などの固定費支出による損害
4．金銭損害	ランサムウェア、ビジネスメール詐欺等による**直接的な金銭（自組織の資金）の支払い**による損害
5．行政損害	個人情報保護法における**罰金**、GDPRにおいて課される**課徴金**などの損害
6．無形損害	風評被害、ブランドイメージの低下、株価下落など、無形資産等の価値の下落による損害、**金銭の換算が困難な**損害

損害の例①　費用損害（事故対応損害）

被害発生から収束に向けた各種事故対応に関して、アウトソーシング先への支払も含め、自組織で直接、費用を負担することにより被る損害

対応項目	対応	アウトソース先	コスト
事故原因・被害範囲調査	•その後の対応を進めるためにも原因や被害範囲等各種調査が必要 •サイバー攻撃等の場合、フォレンジック調査（注）が必要	インシデントレスポンス事業者	300~400万円
法律相談	•リーガル面（個人情報保護法等）を踏まえた対応が必要 •法律事務所へ依頼するのが通例	法律事務所	数十万円～
広告・宣伝活動	•お詫び文を作成し、ホームページへの掲載、DM送付等が必要 •新聞出稿の検討も必要	DM印刷・発送業者、新聞社	•DM印刷・発送　1通あたり封書130円～ •新聞（10cm2段） 全国紙240万円前後、地方紙50万円前後
コールセンター	•問い合わせ対応のため、電話受付体制の整備が必要 •コールセンター事業者への委託が一般的	コールセンター事業者	１オペレーター換算で１か月140万円～ ⇒３か月対応、初月はオペレーター３席、２か月目以降は１席とすると700～1,000万円
システム復旧	•システムの消失、改ざん等があった場合、データ復旧等が必要 •データ復旧は主としてバックアップされたデータの復旧	システムを構築したITベンダー等	対応規模によって大きく異なることから、ケースバイケース
再発防止	•今後の再発を防ぐため、その防止策の策定・実施が必要	セキュリティベンダー等	対応規模によって大きく異なることから、ケースバイケース

損害の例②　利益損害

事業が中断した場合の利益喪失や、事業中断時の人件費等の固定費支出による損害。
多くのシステムが生産・営業活動に直結している現状において、システムの停止は事業中断につながり、売上高の減少をもたらす。
当然、損失は売上規模、ITへの依存度等により**ケースバイケース**

利益損害のイメージ

項目	平時	事業中断時	差額
売上高	10億円	6億円	▲4億円
固定費 人件費、賃料等	2億円	2億円	—
変動費 材料費、電気代等	7億円	4.2億円	2.8億円
営業利益（損失）	**1億円**	**▲0.2億円**	**▲1.2億円**

◇事業中断による売上が4割減

◇事業が中断していても
固定費は定額必要

◇通常1億円稼げるのに、
営業損益▲0.2億円

◇結果として、
▲0.2億円－1億円＝▲1.2億円
の損失が発生

実際の被害状況

被害組織に対するアンケート等からみえてくるもの～

実被害をみても、中小企業においても数千万単位、場合によっては億単位の損害が発生する

ランサムウェア感染組織の被害金額

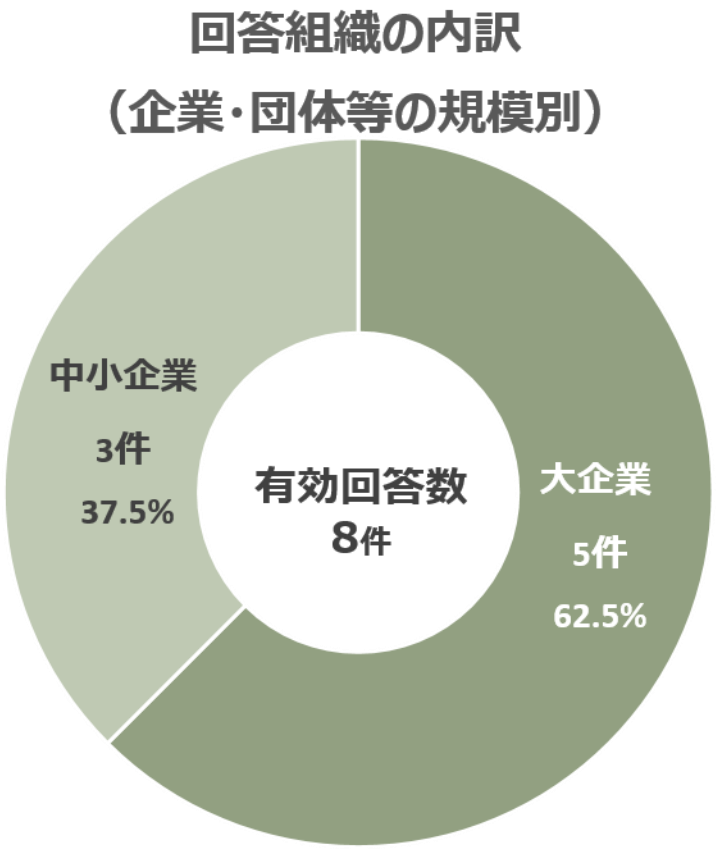
◇平均被害金額：**2,386万円**

◇対応に要した組織の内部工数平均：**27.7人月**

◇ランサムウェア被害のすべての回答組織が
身代金は支払っていないと回答

◇暗号化されたデータを復旧できた組織は**50%**

◇ほとんどの被害組織について、
被害金額は1,000万円超
被害に遭った場合の影響が大きいことを確認

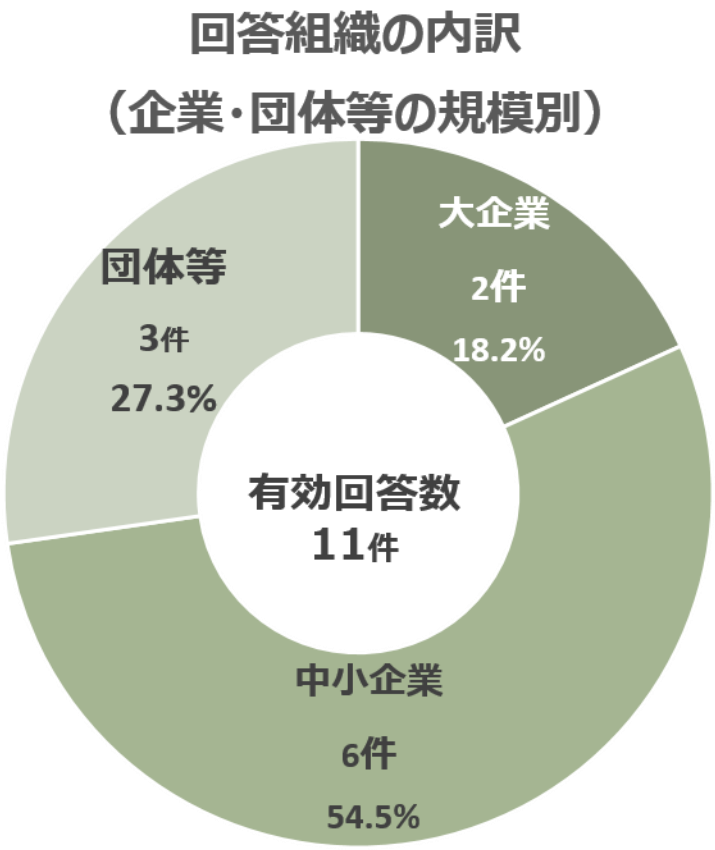


エモテット感染組織の被害金額

◇平均被害金額：**1,030万円**

◇対応に要した組織の内部工数平均：**2.9人月**

◇被害金額のばらつきが大きい



ウェブサイトからの情報漏えい被害組織の被害金額

◇平均被害金額

クレジットカード情報および個人情報の漏えい：

3,843万円

個人情報のみの漏えい：

2,955万円

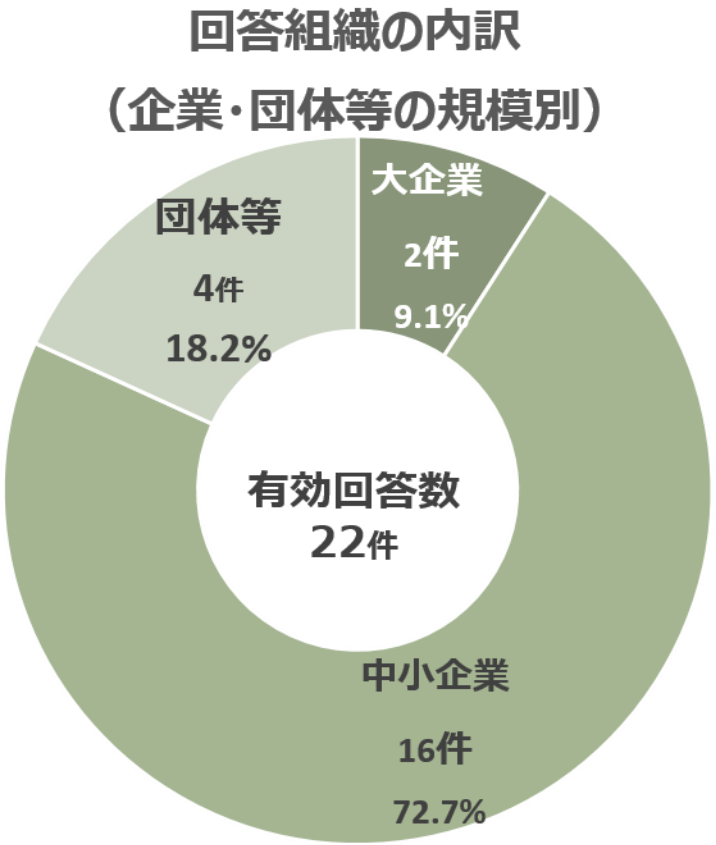
◇対応に要した組織の内部工数平均

クレジットカード情報および個人情報の漏えい：

13.3人月

個人情報のみの漏えい：

13.5人月

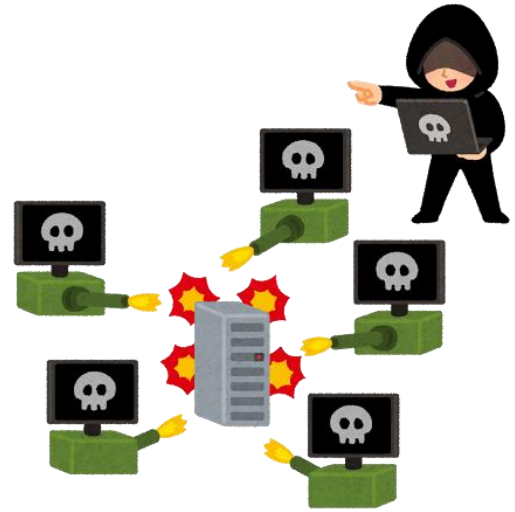


あらためてアンケート調査を見ると

被害種別	平均被害金額
ランサムウェア感染被害	2,386万円
エモテット感染被害	1,030万円
ウェブサイトからの情報漏えい（クレジットカードおよび個人情報）	3,843万円

アンケート調査の回答が少ないこと、
人件費、逸失利益は含まれていないことを勘案するに、
実際の損失はもっと高額と考えられる

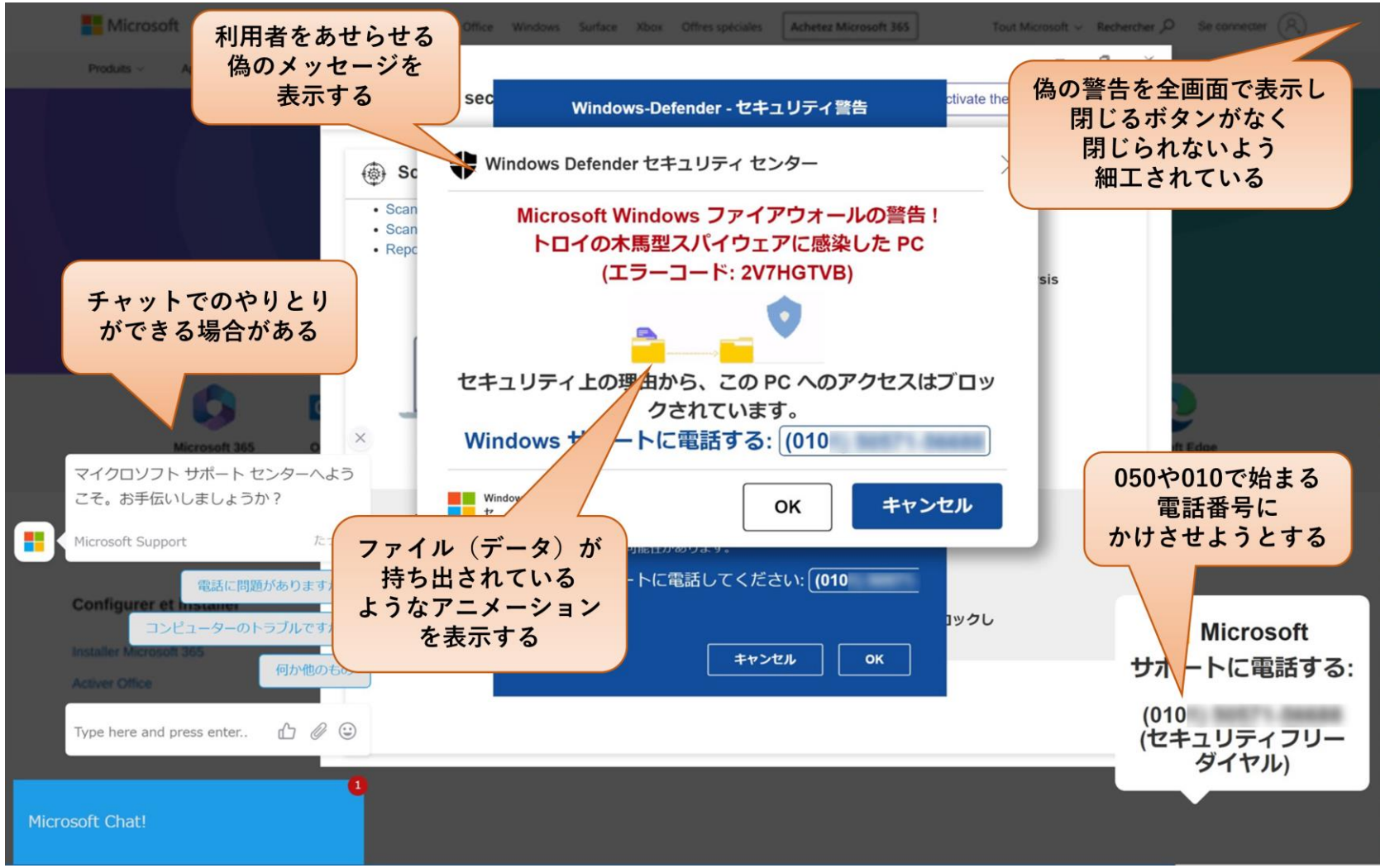
リアルな実態をみても
サイバー攻撃を受けると**「お金がかかる」**
ケースによって、数千万～億の損失がでてもおかしくない



事件から見る攻撃事例

サプライチェーンで起こっていること

サポート詐欺の偽セキュリティ警告



IPA　偽セキュリティ警告
（サポート詐欺）対策特集ページ
「画面の閉じ方体験サイト」

ランサムウェア「WannaCry」感染実演デモ

IPA　ランサムウェア「WannaCry」感染実演デモサイト

サプライチェーン攻撃で鉄壁の守りも突破

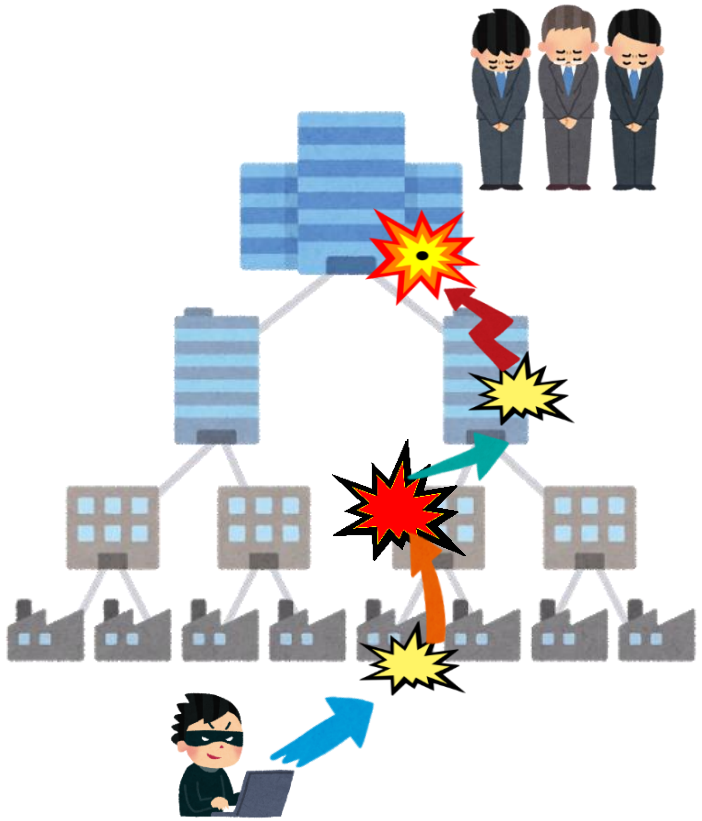
- ビジネス活動の流れ(サプライチェーン)の途中を攻撃し、最終的にターゲットを攻撃する。

パターン①

– 大企業や政府組織などを攻撃するため、防御の手薄なビジネスパートナー等を“侵入口”として攻撃。そこからターゲットの組織へ潜入する。

パターン②

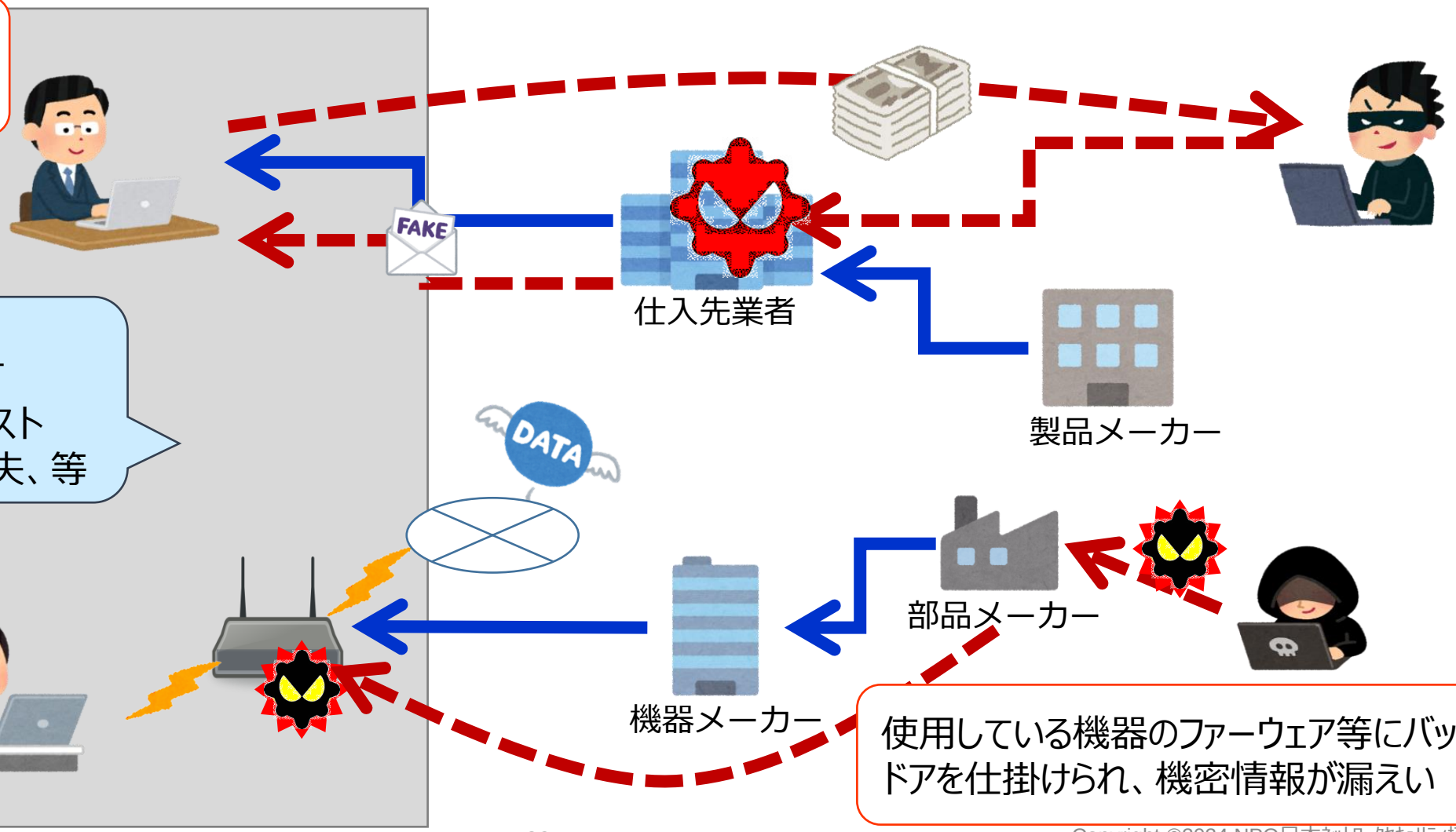
– 多くの組織が利用している製品・ソフトウェア等の開発元などに侵入し、密かにマルウェア等を混入し、それを利用している組織を攻撃する。



サプライチェーン攻撃のリスクイメージ

仕入先業者のメールが
盗聴され、ビジネスメール
詐欺による被害が発生

パターン①



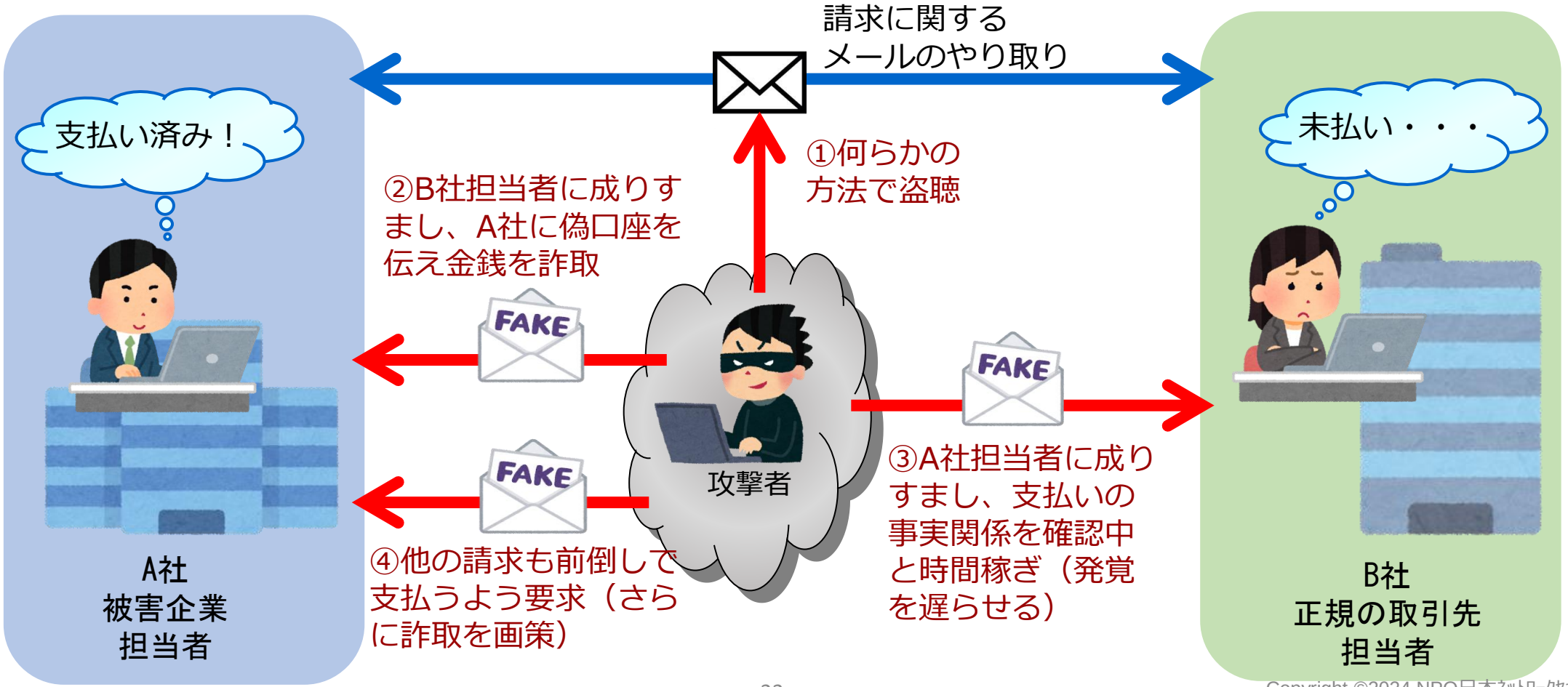
ビジネス上の影響
- 信用失墜・ブランド力低下
- リコール・修理等の追加コスト
- サービス停止中の機会損失、等

パターン②

使用している機器のファーウェア等にバックドアを仕掛けられ、機密情報が漏えい

ビジネスメール詐欺の被害拡大

ビジネスメール詐欺（BEC：Business E-mail Compromise）事例



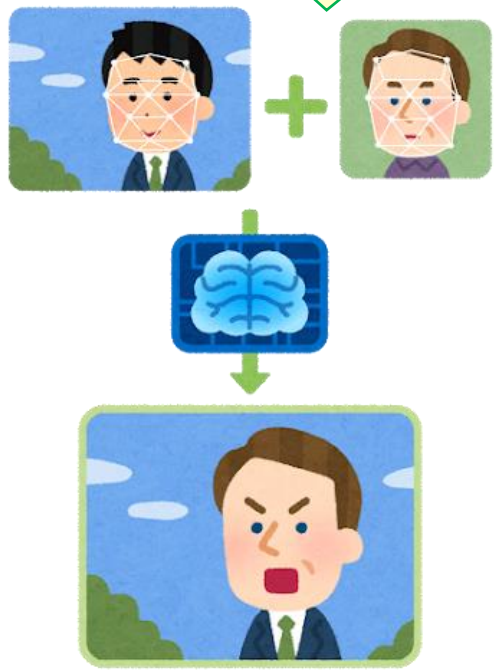
ビジネスメール詐欺の手口

- 取引担当者等になりすまし
  - 税務調査が入っており、従来の口座が使用できない
  - 従来の口座が不正取引に使用され、凍結されてしまった
  - 技術的な問題が発生しており、従来の口座が使用できない

- 経営者層等になりすまし。
  - 極秘の買収案件で、資金が至急必要になった
  - 緊急かつ内密に送金してほしい（他者に相談させない）

- 弁護士等になりすまし

最近の傾向：
AIで成りすまし



被害防止対策

- 添付ファイルやリンク先を不用意に開かない
- ウイルス対策ソフト・OSを最新の状態に更新
- 不正アクセス対策を徹底する
- 電話などメール以外の方法で確認
- メール（アドレス）をよく確認
- 組織内外での情報共有

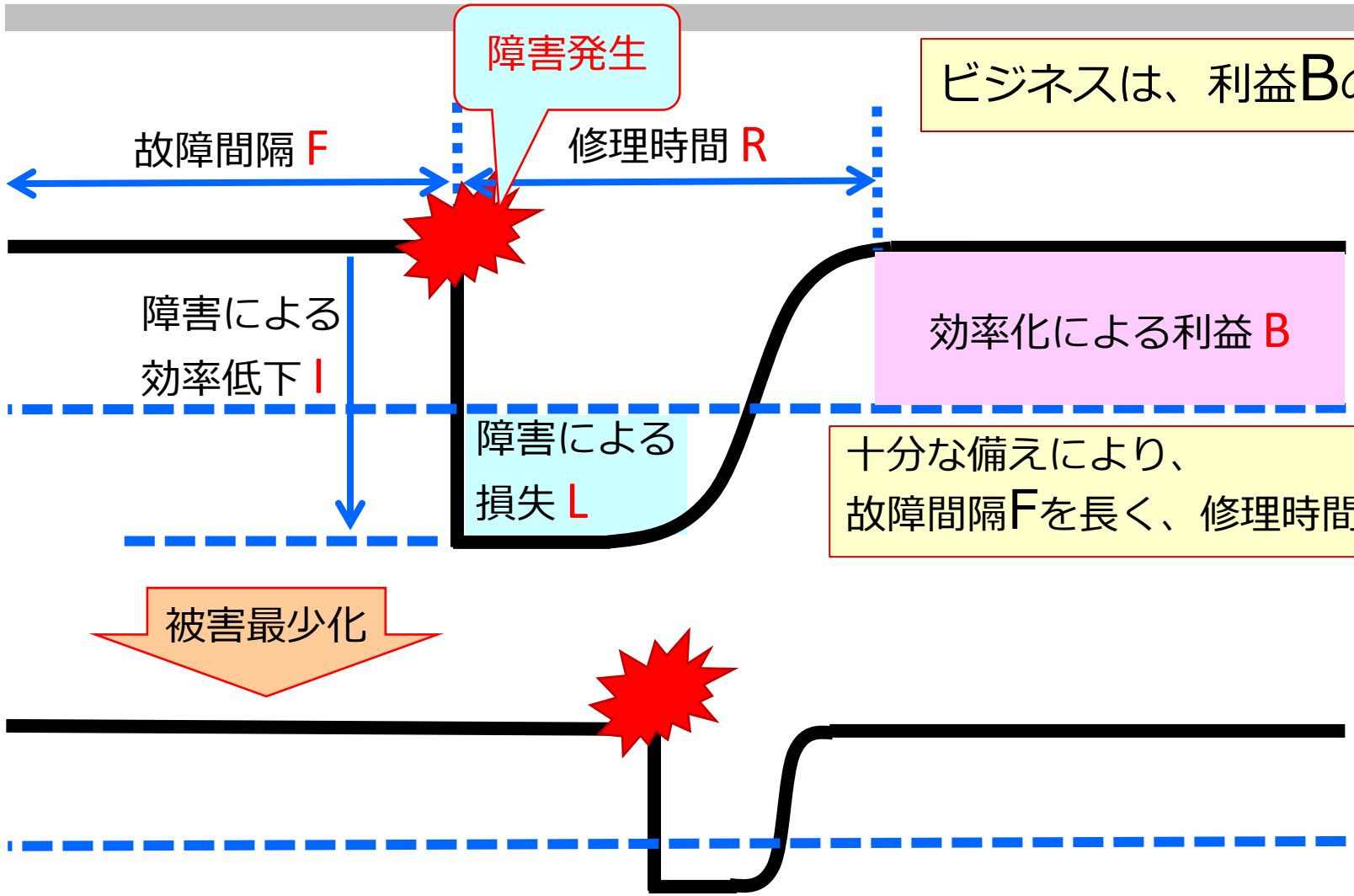
- ツールの活用と
  ソーシャルエンジニアリングの
  複合攻撃
- 攻撃者優位の現状

いかに早く気づけるかが重要！

企業における対策の考え方

対抗するための考え方の整理と回復力を高めるための前始末（周到な準備）

そもそもビジネスは障害時にいかに回復するか



ビジネスは、利益Bの最大化、損失Lの最少化

故に

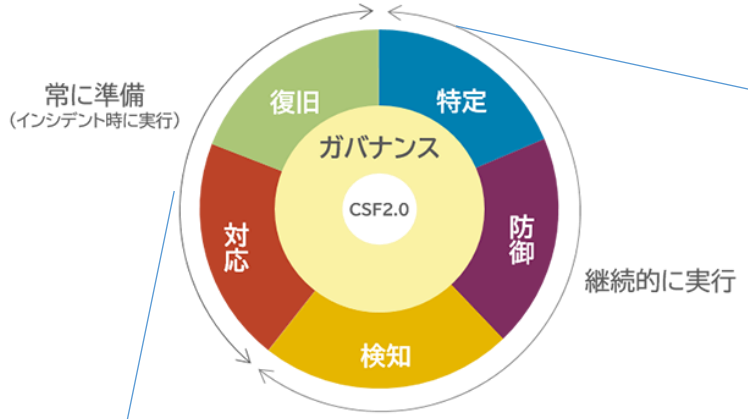
十分な備えにより、
故障間隔Fを長く、修理時間 R を短く、効率低下Iを小さく

しかし

セキュリティ事案では、
R は長く、Iは大きくなりがち

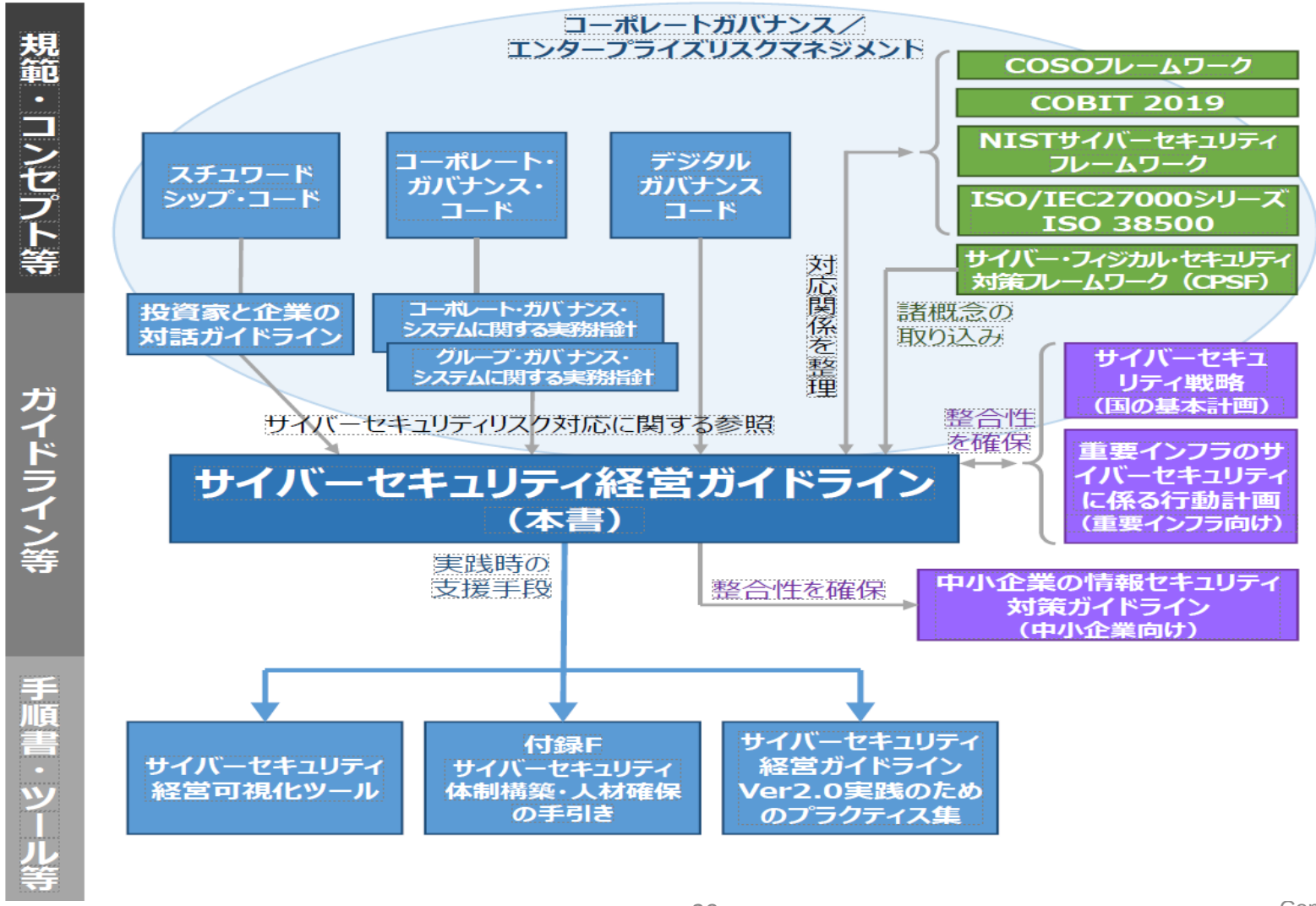
NIST サイバーセキュリティフレームワーク（CSF）

- 広い領域・適応範囲をカバー（2024年2月に改訂）
  - 脅威の侵入を防ぐ「事前対策」だけでなく、侵入などの有事が発生した後を想定した「事後対策」も含む、広範な管理策をカバー
  - 規模や業種、対策の成熟度に関係なく、中小企業を含むあらゆる企業や組織での利用が進むように再設計



各フェーズで対応すべき対策を事前に確認し、各組織に見合った必要な対策を実施

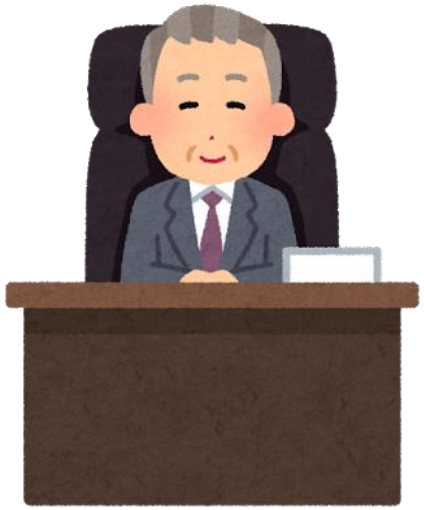
METI　サイバーセキュリティ経営ガイドラインの位置付け



最新版への改訂内容

- Ver2.0からVer3.0への改訂（2023年3月）の背景
  - **デジタル環境を活用**した働き方の多様化（テレワーク等）
  - サイバーセキュリティ対策対象の拡大（従来のIT系から**制御系を含むデジタル基盤に拡大**）
  - ランサムウェアによる被害の拡大（従来の情報漏洩から**事業停止に拡大**）
  - **サプライチェーン全体**でのサイバーセキュリティ対策の必要性の高まり
  - **コーポレートガバナンスおよびリスクマネジメントの改善**に向けた取り組みへの社会的関心の高まり

経営者が認識すべき３原則



① 経営者は、サイバーセキュリティリスクが**自社のリスクマネジメントにおける重要課題**であることを認識し、**自らの**リーダーシップのもとで対策を進めることが必要

② サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、**サプライチェーン全体にわたるサイバーセキュリティ対策**への目配りが必要

③ 平時及び緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との**積極的なコミュニケーション**が必要

インシデント発生時の報告内容
組織内で整理しておくべき事項（付録C）

有事の際に対応すべきことを事前に確認し、即時対応できるよう事前に準備

表1	基本項目	全てのインシデントで共通して調査すべき項目
表2	情報漏えいに係る項目	情報漏えいが発生した際に調査すべき項目
表3	ウイルス感染に係る項目	ウイルス感染が発生した際に調査すべき項目
表4	不正アクセスに係る項目	不正アクセスを受けた際に調査すべき項目
表5	(D)DoSに係る項目	(D)DoS攻撃を受けた際に調査すべき項目

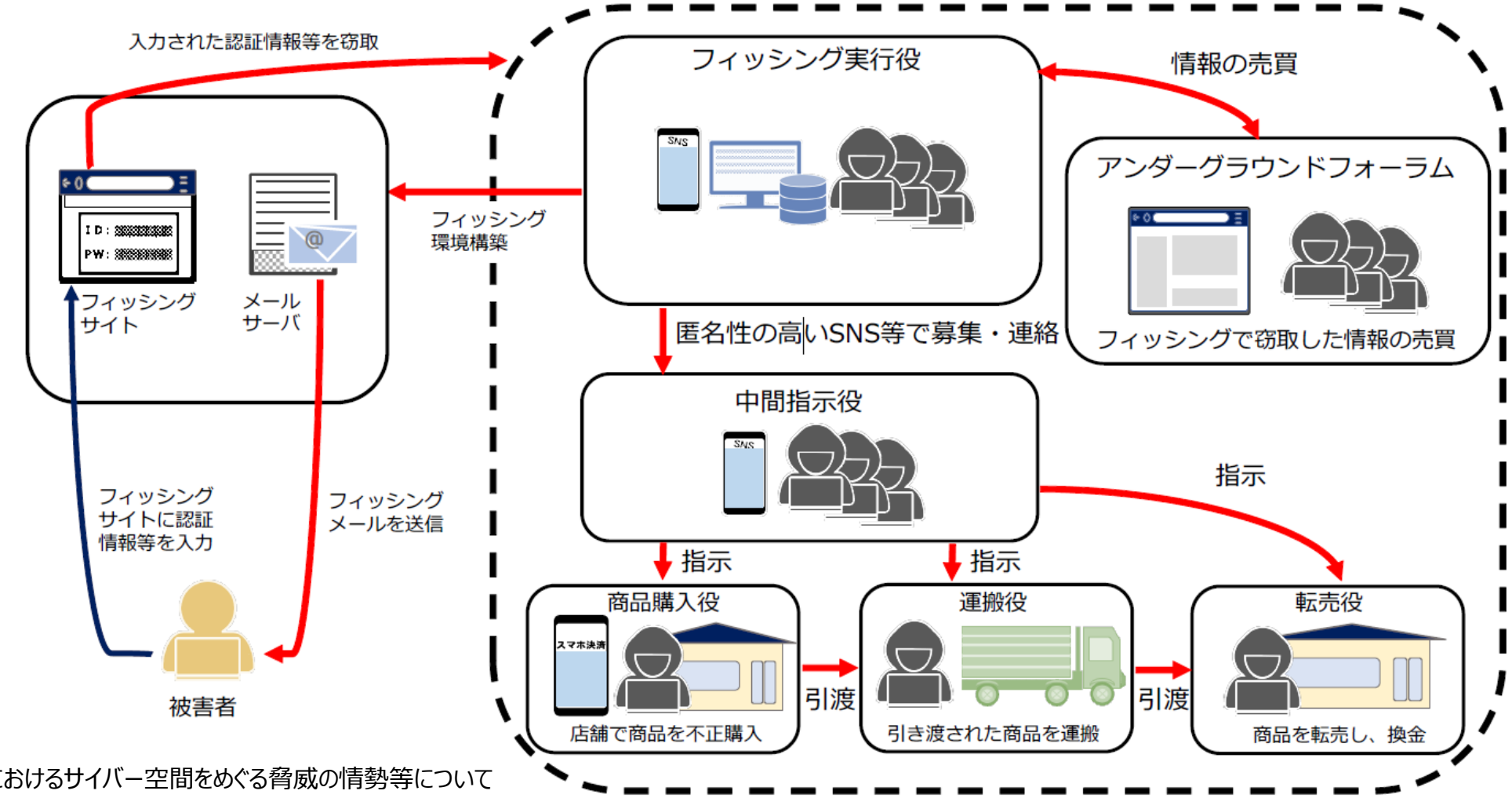
NISC　サイバー攻撃被害に係る情報の共有・公表

- サイバー攻撃被害に係る情報の共有・公表ガイダンス
- 令和５年３月８日公開
  - https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf
  - 被害組織で見つかった情報を「何のために」「どのような情報を」「どのタイミングで」「どのような主体に対して」共有／公表するのか、ポイントを整理したもの
  - 各種情報共有活動や、広範な組織での活用を想定し、情報共有の活性化に向けた参考として示すもの

攻撃者は組織化して
ビジネスとして攻撃してくる

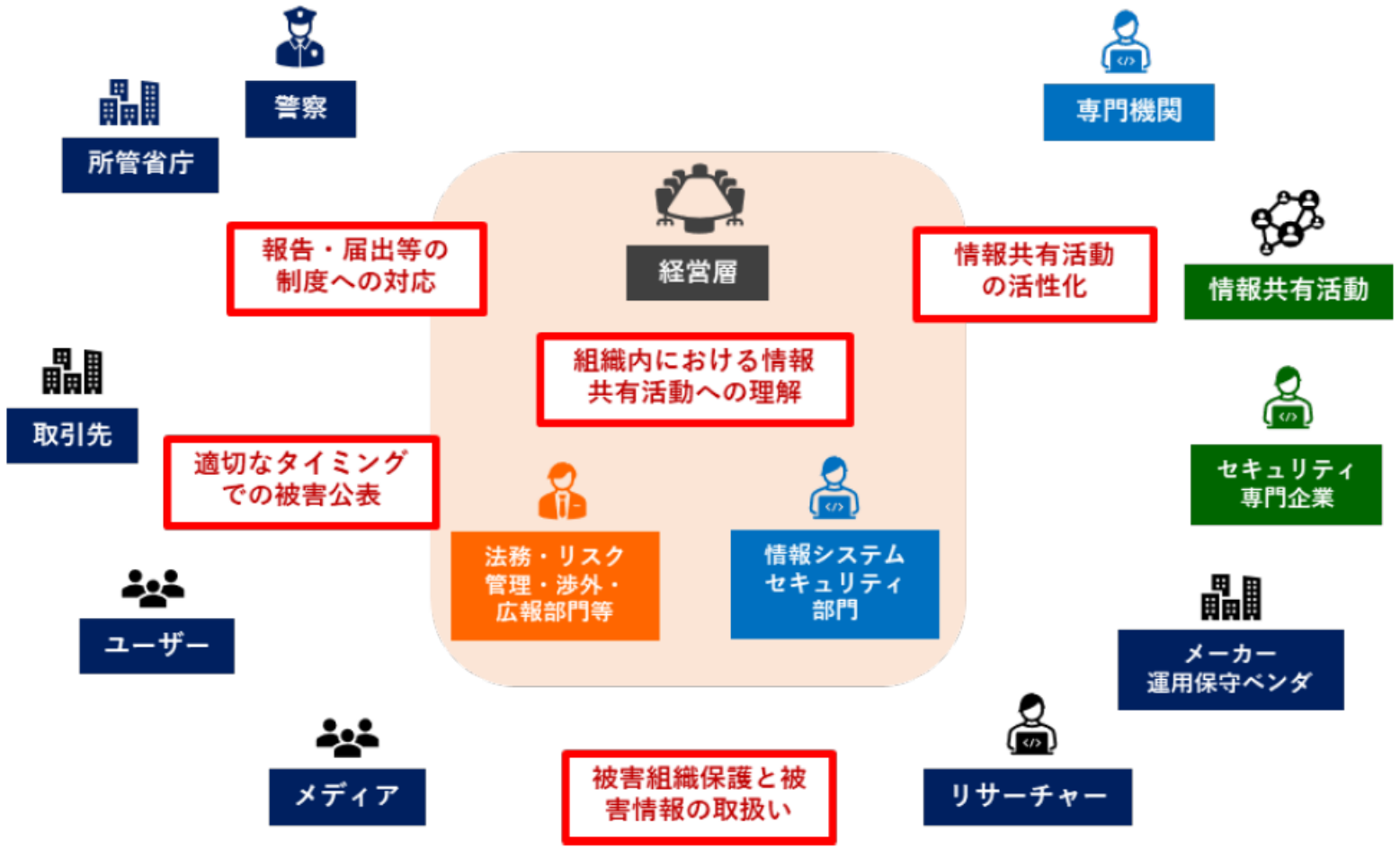
守る側も組織化し
有事に適切な対応の必要

攻撃者グループのエコシステム



出典：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
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

ステークホルダーとの関係



関係するであろうステークホルダーの洗い出しを事前に行い、有事に適切なタイミングでアプローチできるように事前に準備

出典：サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会　発行　サイバー攻撃被害に係る情報の共有・公表ガイダンス
https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf

JNSA

https://www.jnsa.org/