中堅中小組織における
サイバー事故対応体制の現実と課題

一般社団法人日本シーサート協議会
運営委員，チームトレーニング委員会副委員長，NCAトレーナー
高野 梨紗
（東京海上ディーアール株式会社，PIRATES）

自己紹介

■ 一般社団法人日本シーサート協議会（NCA）からきました

- 運営委員、チームトレーニング委員会副委員長、NCAトレーナー

■ 経歴

- 現職は3社目。
- 1社目で情シスキャリアスタート
- IPOに伴うガバナンス強化
  - ワークフロー整備、ISMS・プライマシーマーク認証、情報セキュリティ委員会
- 上司が羽ばたき、**ひとり情シス**。後、**兼任情シス**
  - 総務、法務、＋メンバーマネジメントおよび評価
- 組織拡大と、バックオフィスの多能工化
  - 意思決定以外は**ベンダーと二人三脚**
- 転職して、化学系製造業のセキュリティガバナンス担当
  - グローバル展開する製造業のグループ全体の統制整備と強化施策。法務部門との密な連携
  - 日本、中国、シンガポール。GDPR対応は必要性の説明から
  - CSIRT立ち上げ、セキュリティチームのリード

組織紹介

CSIRT(シーサート):サイバー事故対応組織の略。Computer Security Incident Response Team
サイバー事故が起きた際に、**「誰が」「いつ」「どうやって」**動くのか、その体制と役割を担う専門チーム

■ 名称

- 正式名称　一般社団法人 日本シーサート協議会
- 略称　日本シーサート協議会、NCA(エヌシーエー)
- 英語名　NIPPON CSIRT ASSOCIATION
- Webサイト　https://www.nca.gr.jp/

CSIRT
日本シーサート協議会

■ 設立

- 2007年3月(2020年4月より一般社団法人として活動開始)

■ 使命

- 本協議会の全会員による緊密な連携体制等の実現を追及することにより、会員間に共通する課題の解決を目指す
- 社会全体のセキュリティ向上に必要な仕組みづくりの促進を図る

どうして今日、ここでおはなししているのか

CSIRT
日本シーサート協議会

備えがある組織と接している

サプライチェーンセキュリティの課題を抱えている声を見聞きする。
自社はサイバー事故対応への備えがあっても、委託先では備えがないケースがある。しかしながら、備えを強要することはできない。

▼ ▼ ▼

サプライチェーンセキュリティに対してできることを模索してみる。
活動をとにかく始めてみる。続けてみよう。

PIRATES
Professionals of Intelligence-based Risk Assessment and Total Emergency Services

備えがない企業と接している

サイバー事故対応への備えがない企業が助けを求めてくる現実を日々目の当たりにしている。サイバー事故が起きたあとのひとたちに提供するのは止血のための支援であって、備えの提案ではない。

▼ ▼ ▼

備えがない企業に平時からの備えの必要性についてサイバー事故が起きる前に働きかけができたならば、サイバー事故が減るのに！

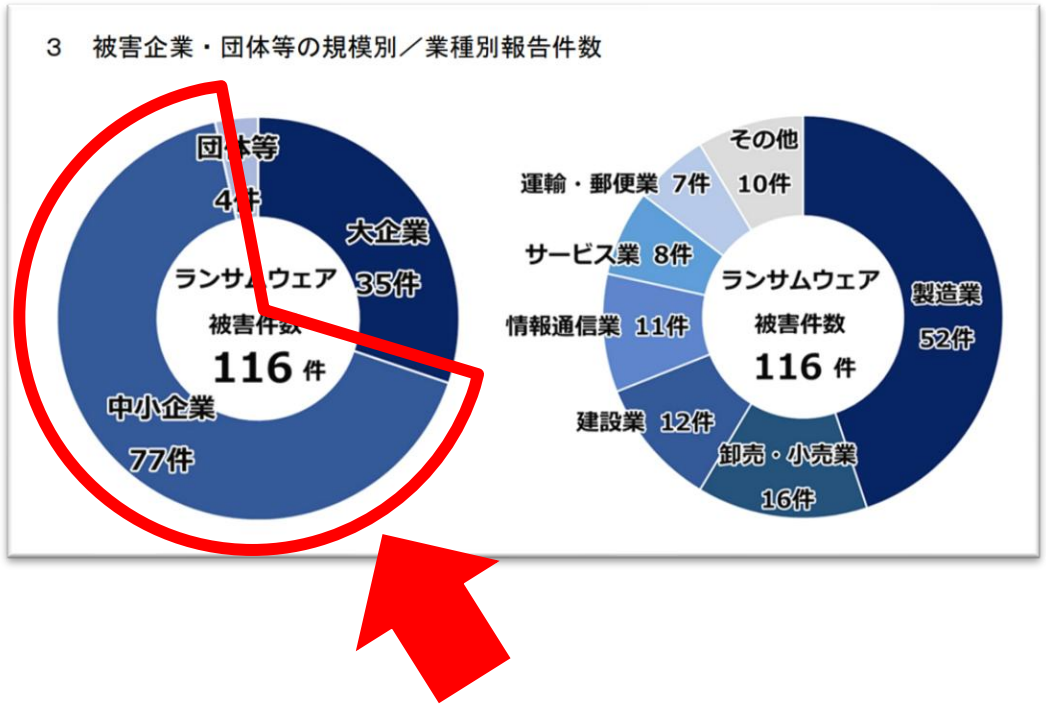
備えがないことで不安を感じている中堅中小企業が最低限備えておけることの提案をしたい！

※ここでいう備えとは、CSIRT(Computer Security Incident Response Team)=サイバー事故対応組織がある組織を指す

サイバー攻撃って、身近にあるもの

ですよね？

被害件数の実数は大企業より中堅中小企業が多い



中小企業が全体の約3分の2

出典：https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

従業員数1,000名未満が6割

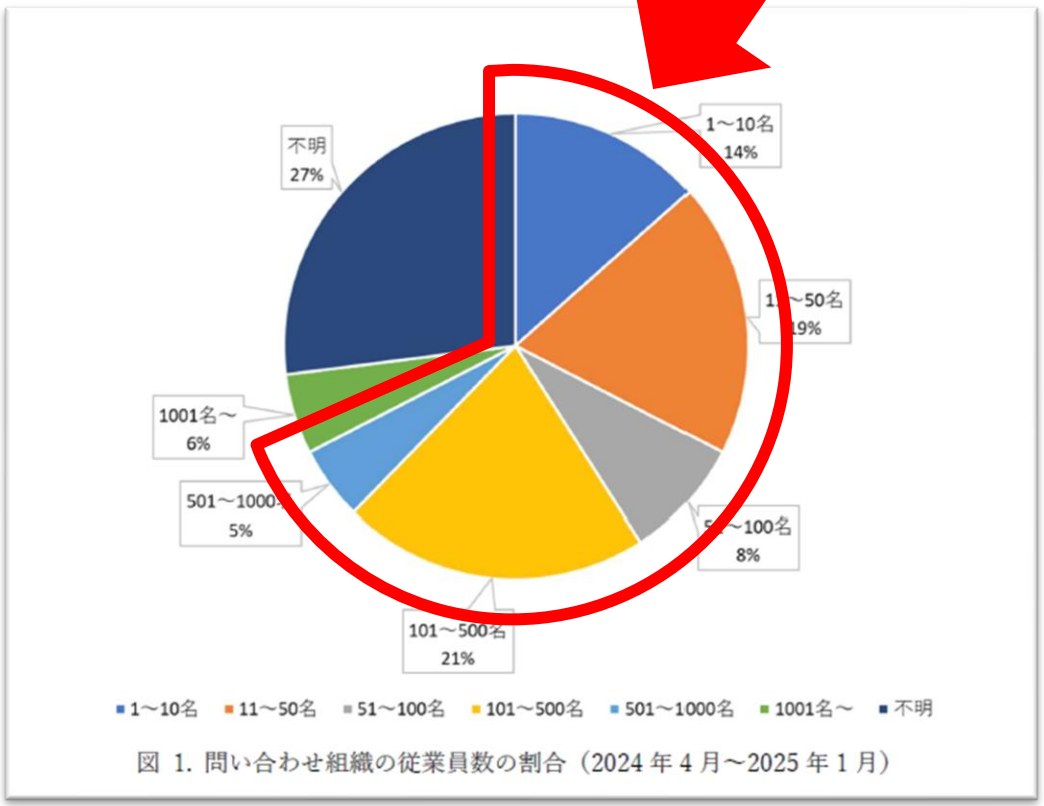


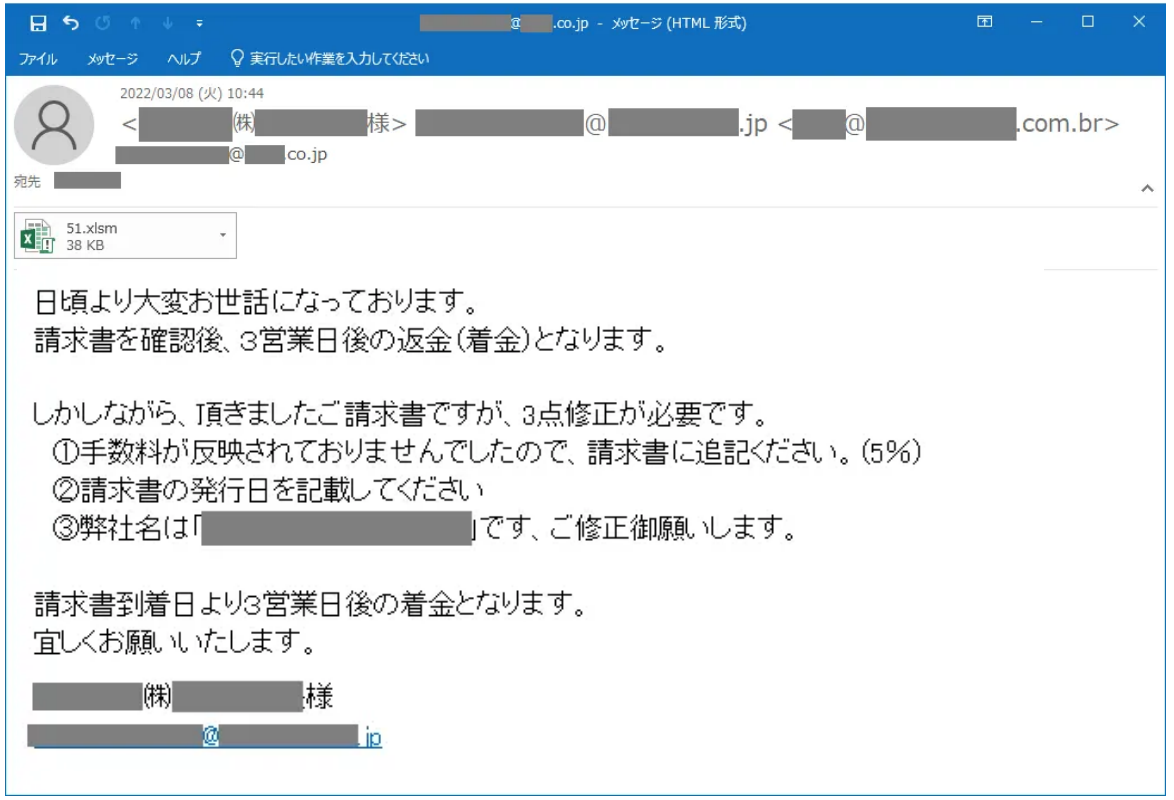
図 1. 問い合わせ組織の従業員数の割合（2024 年 4 月～2025 年 1 月）

出典：東京海上ディーアールIHCCレポート

Emotet（2022年頃頻発）

- 社外からのメールに添付されているファイルを開封した
  - ファイル開封後、パソコン利用に違和感無し
- 取引先から、不審なメールが来ていると問合せあり
  - 引用メールは確かに身に覚えがある内容だが、取引先にメールは送信していない
- 問合せが多数あり、その中には重要取引先からの報告を求めるものも

メールアカウントやメール本文情報を窃取し、なりすましメール送信による拡散型マルウェア



出典：感染被害の大幅拡大/日本語で書かれた新たな攻撃メール（2022年3月9日）（情報処理推進機構）

サポート詐欺（2023年頃から現在）

- **Webサイトを閲覧していたら急にセキュリティ警告画面が出てパソコン操作を阻害された**
  - 不安をあおる文字と、信頼できそうな電話連絡先
  - 周囲に相談できる相手がいない
- **表示された電話番号にかけると、サポートデスクの対応が始まる**
  - リモートデスクトップ機能を使った詐欺者によるパソコン遠隔操作
- **対応費用の請求があり、ネットバンキングで即時高額支払い**
  - 電話口で断り辛い状況に誘導

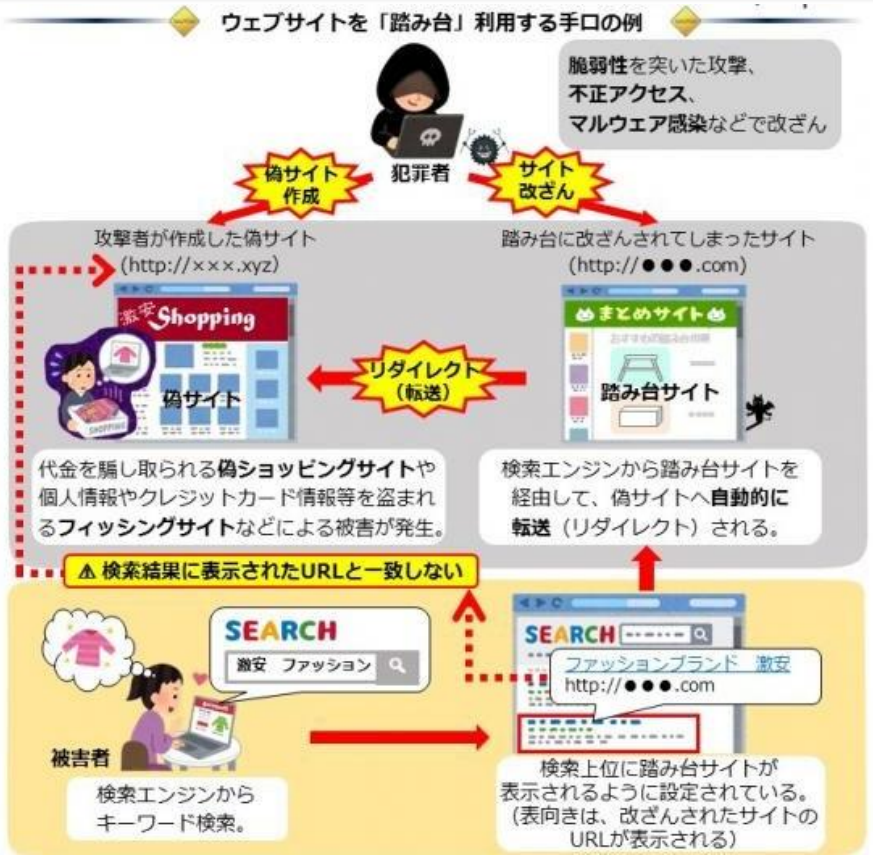
パソコンを使った金銭詐欺。
個人から多額送金可能な企業に狙い先がシフト

出典：サポート詐欺対策のページより（警察庁）

Webサイト改ざん（2016年頃から現在）

- **自組織ホームページがいつもと違うと問合せ**
  - 自組織で作成していない不審コンテンツに書き換わっていたので、バックアップデータから戻し
  - 管理サービス会社から、不審なアクセスを検知しパスワード初期化したという数か月前のメール連絡を発見
- **改ざんの頻発と都度バックアップ戻し**
- **ホームページ管理権限の乗っ取り**
  - Webサイト管理画面にアクセス不能に
  - 警察から情報提供の連絡が入った

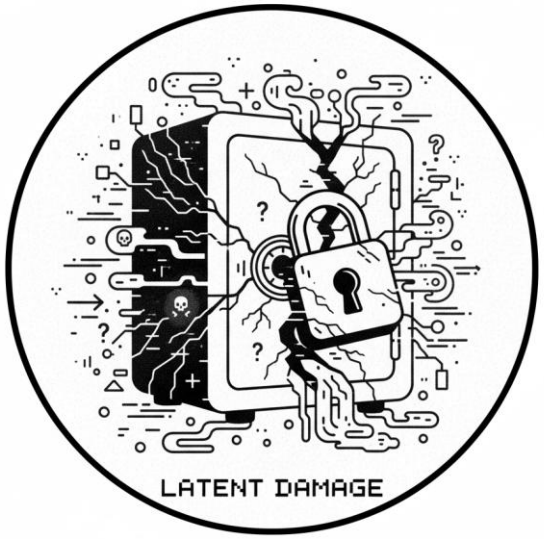
CMS脆弱性を悪用した「踏み台」サーバー化による攻撃加担



出典：サイバー犯罪の「踏み台」にされないために（埼玉県警察）

改めて、サイバー攻撃 is なに

実行者特定困難



攻撃被害潜在化

どこからでも攻撃可能

サイバー攻撃には、①攻撃の実行者の特定が難しい、②攻撃の被害が潜在化する傾向がある、③国境を容易に越えて実行可能であるといった特徴があり、我が国においても、サイバー空間の脅威に対する対処能力の強化が求められています。

出典：https://www.npa.go.jp/archive/keibi/syouten/syouten283/pdf/02_10-15P.pdf

サイバー攻撃における時代背景

	主な出来事	サイバー攻撃史
1940年代 - 1980年代	● コンピューター誕生、インターネット黎明期 ● 研究と教育のためのインターネット、電子メール誕生 ● 民間：パソコン通信、固定電話、フロッピーディスク	● 1971 Creeper：はじめてのワーム ● 1988 Morris Worm：大規模な実害をもたらしたワーム
1990年代	● インターネット普及期 ● 私的・商業的なインターネット利用の解禁 ● 携帯電話の普及、Windows 3.1誕生、Web誕生、i-mode誕生	● 1991 Michelangelo: アンチウイルスソフトの引き立て役 ● 1999 Melissa：メールで拡散されたマクロウイルス
2000年代	● インターネットのビジネス利用 ● 電子メールの普及、SNS誕生(mixi, Facebook, Twitter)、iPhone誕生	● 2001 CodeRedワームによるインターネット麻痺 ● 2003 フィッシング詐欺のはじまりと急速な台頭
2010年代	● 生活基盤となったインターネット ● スマートフォンの普及、仮想通貨取引所の誕生、IoTの流行	● 2010 Stuxnet によるイラン核関連施設攻撃 ● 2015 日本年金機構への標的型攻撃 ● 2017 ランサムウェア WannaCry の猛威 ● 2018 コインチェック事件 ● 2019 Emotet：巧妙ななりすましメールによる感染流行
2020年代	● コロナ禍 ● 生成AI	● 2020 ソフトウェアサプライチェーン攻撃 Orion ● 2023 二重脅迫ランサムウェアグループの猛威

サイバー攻撃者は何を目的に攻撃を行うのか

- 攻撃の「ビジネス化」と組織化
- 目的の分類は変わっていないが、金銭目的を占める割合が増加してきている

目的	攻撃者の種別	主な手口	代表的な事例
金銭の窃取	組織的犯罪集団等	・ランサムウェア ・ビジネスメール詐欺(BEC※1)	・徳島県の病院へのランサムウェア攻撃 (2021年) ・名古屋港へのランサムウェア攻撃 (2023年) ・宿泊予約管理システムへの攻撃 (2023年)
情報の窃取	産業スパイ等	・認証情報を窃取した不正アクセス ・サプライチェーンを狙った攻撃	・米Yahoo!で30億アカウント流出 (2017年) ・Facebookで5億人の個人情報流出 (2021年) ・プロジェクト情報共有ツールへの攻撃で官庁の重要情報流出 (2021年)
思想の主張	ハクティビスト等 社会的な主張で敵対する団体にサイバー攻撃し、SNS等で犯行声明を出す団体、個人	・DDoS※2攻撃によるサービス妨害 ・Webページの改竄	・Anonymous等のハクティビストによる攻撃 ・ソニーピクチャーズへの攻撃 (2014年)
国益の追及	国家等	・標的型メール攻撃 ・重要インフラへのサービス妨害	・Stuxnet (2010年) ・ウクライナでの大規模停電 (2015年) ・ロシア、ウクライナのサイバー戦 (2022年)

※1 BEC:Business Email Compromise　従業員を騙して不正送金させる行為
※2 DDoS:Distributed Denial of Service　外部からWebサーバーなどに対して通信パケットを大量に送付しサービス提供を妨げる行為

自社が直接受けたわけじゃないのにサイバー攻撃の被害者に

- 2023年6月、社会保険労務士向けクラウドサービスが自社サーバーでランサムウェアによる不正アクセスを受けてサービス停止と、登録者の情報漏えいを公表した
- 多くの組織で、自組織がサイバー攻撃を受けていないのに従業員の情報が流出の可能性
  - 2023年7月、サービス提供元は漏えいの可能性を認めつつ事実は確認されていないと公表
- 未だ事案は終息していない
  - 2024年3月個人情報保護委員会が個人情報の保護に関する法律第147条の規定による指導を発表
  - 2025年7月利用者90人が原告となり損害賠償を大阪地裁に民事訴訟提起

出典:エムケイシステムホームページリリース（2022/12/8）

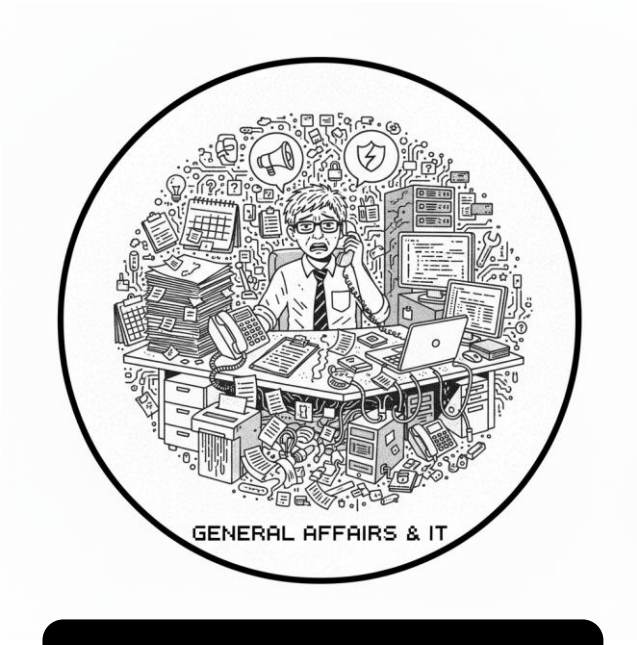
出典:社労夢ユーザー90人がエムケイシステムに集団訴訟　3億円超請求、ランサム被害で（日経クロステック　2025/8/22）
https://xtech.nikkei.com/atcl/nxt/news/24/02770/

中堅中小組織の現実

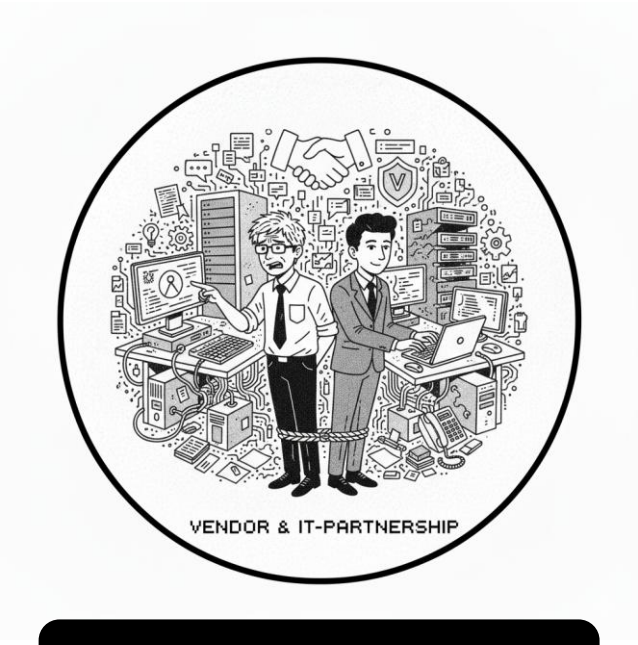
明日は我が身のサイバー事故ってなんだろう？

想定する情シスの典型像

ひとり情シス



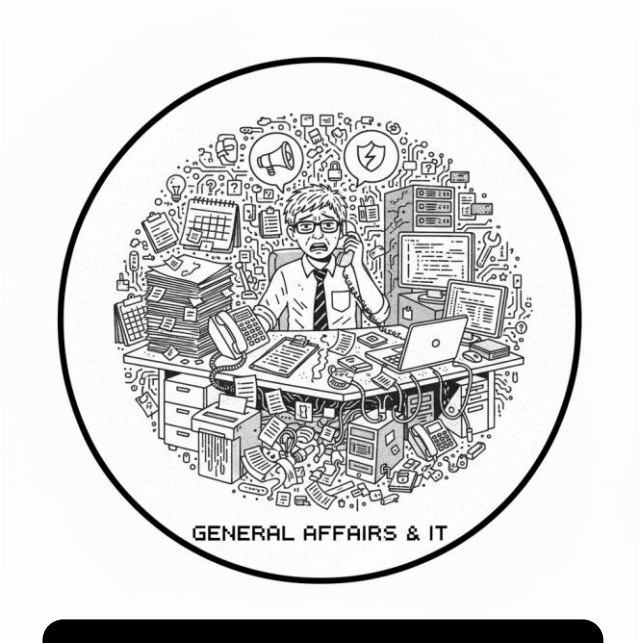
兼任情シス



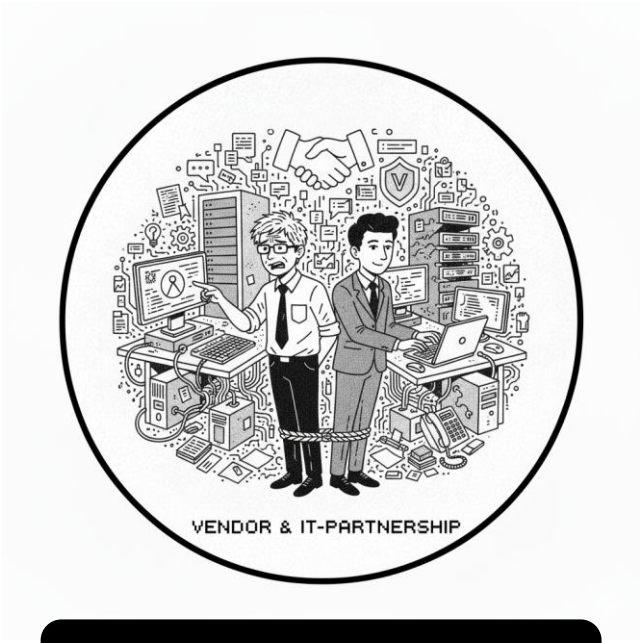
ベンダーと二人三脚

~~ただでさえやること多いのに、~~ほんとにサイバー事故まで担当するの？

ひとり情シス



兼任情シス



ベンダーと二人三脚

- 社内にセキュリティ専任者がいない。自分がなろうにも片手間感はどうしても否めず。
- 意思決定者がセキュリティに理解なし。「うまくやっといてよ」「結論は？」

“ベンダーと二人三脚“は一見するとなんとかなりそうだけど

ひとり情シス

兼任情シス

ベンダーと二人三脚

- 「何か起きたらベンダーに頼む」を前提として契約、関係構築。
- 実際には、ベンダーとの契約範囲や初動判断で支障が出る。「え、これも対象範囲外?!」

現場の実態１　マルウェア感染によるスパム送信と情報流出

組織	通信インフラ工事
売り上げ規模	10億円
従業員数規模	50名以下
概要	組織内で大量の送信エラーメールが届き調査を開始。社内アドレスが不正利用され、端末感染とマルウェアによるバックドアが判明した。 過去1年分のメール約2万件と顧客情報500件が流出の可能性。 重要インフラ顧客も含まれ、監督官庁への報告まで必要となった。 社長が初動から方針決定・謝罪・報告を一手に担ったが、過労で入院。 残された総務担当1名が状況理解不足のまま報告業務を背負い、責任感だけで対応した。
被害の実態	• 顧客情報500件、メール約2万件が流出可能性 • 社長に負荷集中し、過労で入院 • 総務担当が責任および専門知識なく重要報告を実施
教訓	初動判断や報告対応を1人に依存すると、不在時に組織は機能不全となる。権限分散と代替体制の準備が必要である。

現場の実態 2　ランサムウェアによる業務停止と調査不能

組織	製造加工・販売
売り上げ規模	40億円
従業員数規模	100名以下
概要	唯一のシステム管理者がファイルサーバーとADサーバーの暗号化を発見。 ベンダー契約は保守対象外、アンチウィルス会社からの対応拒否。 残っていたFireWallログを確認するも、デフォルト設定の少ない情報で有効な痕跡は得られず、さらにADサーバーに同居させていたアンチウィルス管理サーバーも暗号化され調査不能に。 専門家の助言でFireWall更新と被害サーバー再構築により復旧したが、根本的な対策は進まず、再攻撃の不安を抱えたまま業務再開を余儀なくされた。
被害の実態	• ファイルサーバー、ADサーバー暗号化で業務停止 • ベンダー支援不可 • 調査ログ喪失で侵入経路不明のまま復旧
教訓	契約外ベンダーや暗号化で調査不能に陥り、原因特定も再発防止もできない。 調査・復旧を想定した契約と体制を平時から整える必要がある。

現場の実態 3　開発委託先の設定ミスによる情報流出

組織	情報サービス提供
売り上げ規模	非公開
従業員数規模	30名以下
概要	新サービスサイトへの移行開発中、本番データ登録後の開発環境にて、開発委託先の設定ミスにより会員DBが一般公開された。 すぐに設定を是正したが、時すでに遅し、攻撃者から「会員データをコピーした。返してほしくば金銭を払え」と脅迫メッセージが残されていた。 対象は会員情報10万件だが、過去の消し忘れデータを含め最大100万件に拡大。 監督官庁から厳しく指導を受けたが、社内では「開発委託先任せか、第三者調査か」で真っ二つに意見が割れた。最終的に開発委託先主導で調査を進めたが、初期判断と主体性の欠如により混乱が長引いた。
被害の実態	• 会員情報最大100万件の漏えい可能性 • 初動で判断迷走、監督官庁から厳重指導
教訓	委託先任せでは初動が遅れ、信頼失墜や行政対応の混乱を招くことがある。開発委託時から自組織責任を明確にし、初動体制を自前で用意しておく必要がある。

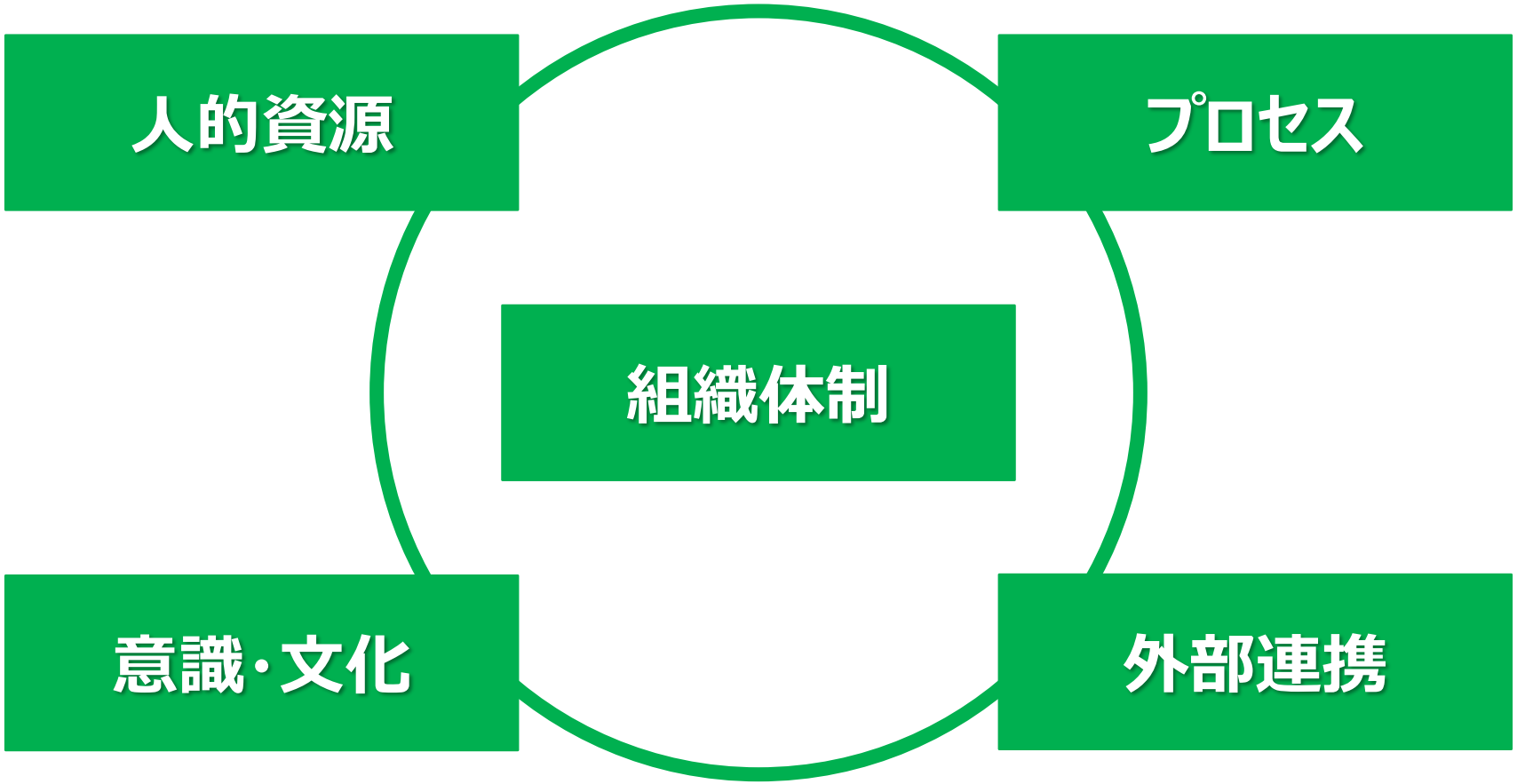
現実から見えてくる課題

- 「誰が」「いつ」「どうやって」動くかが決まっておらず現場が混乱
- 「人がいない」「権限が集中する」ことが混乱や限界を生む
- 技術的な調査手段や記録がなく、調査の限界を早い段階で迎える
- 「契約で支援が受けられない」「責任分担が不明確」により対応が遅れる

結果として、事業継続と社会的責任の問題（経営リスク）が顕在化

課題を構造化してみると

現場で繰り返される“動けなさ”の5つの要因



課題の内訳

組織体制	「誰が」「いつ」「どうやって」動くかが決まっておらず現場が混乱

- ✓ すべて1人のキーパーソン(社長や管理者)に依存し、代替体制なし
- ✓ 速やかな決定が必要なシーンで意見が割れる

- ■ 初動時に「誰が」「いつ」「どうやって」動くかが曖昧なままでは、最終的に社長や担当者1人に負担が集中し、限界を迎える。
- ■ 本来は防災体制のように指揮系統を明確にし、代替体制を整えることで混乱を防ぐことが推奨される。
- ■ しかし、中小中堅組織では専任者を置くリソース余裕が無く、体制そのものを作れない現実がある。

体制が無いこと自体がリスクを増幅する。しかし…

課題の内訳

人的資源	「人がいない」「権限が集中する」ことが混乱や限界を生む

- ✓ 代替人員や支援者不在
- ✓ 専門知識に乏しく、判断を外部に依存

- ■ 担当者が1人しかいない、権限も知識も集中している----そんな状況は、もしその人が倒れたら組織活動が止まるリスクを抱える。現場では経営層や総務担当に過重な負荷がかかり、体調を崩してしまう事例もある。
- ■ 本来は複数人での役割分散が必要である。
- ■ しかし、中小中堅組織ではそもそも人材が不足しているため持続的な対応が難しい。

要員がいれば属人化と調査不能を回避できる。しかし…

課題の内訳

プロセス	技術的な調査手段や記録がなく、調査の限界を早い段階で迎える

- ✓ 流出可能性範囲が絞り込めず、また被害範囲確認にも膨大な負荷
- ✓ ログ喪失、未取得、暗号化等で原因追跡が不可能に

- ■ ログや調査手段が残っておらず、感染源や侵入経路を突き止められない----これは多くの中小中堅組織で繰り返されている。原因がわからなければ再発防止を全方位で検討実施しなければならず、大きな負荷となる。また、「とりあえず復旧」で業務を再開してしまうこともある。
- ■ 調査可能な仕組みを平時から整えることを推奨する。
- ■ しかし、中小中堅組織ではコストや専門知識が障壁となり後回しにされがちである。

検知後数時間で封じ込めできれば被害拡大防止できる。しかし…

課題の内訳

外部連携	「契約で支援が受けられない」「責任分担が不明確」により対応が遅れる

- ✓ ベンダーが動かない、動けない
- ✓ 現場担当が窓口担当も兼任し対応が遅れる

- ■ いざという時のためにベンダーや委託先に相談しても「契約外なので対応できません」と断られる例は少なくない。保守範囲や責任分担が不明確なままでは、初動対応が遅れてしまう。
- ■ 本来は契約内容や窓口を整理し、外部の力を即座に活用できる体制を築く必要がある。
- ■ しかし、中小中堅組織では日常業務に追われ整備できなかったり、保守費用の増額を受け入れられなかったりするのが現状。

契約内容や窓口整理で外部支援をすぐ呼べる。しかし…

課題の内訳

意識・文化	結果として、事業継続と社会的責任の問題（経営リスク）が顕在化

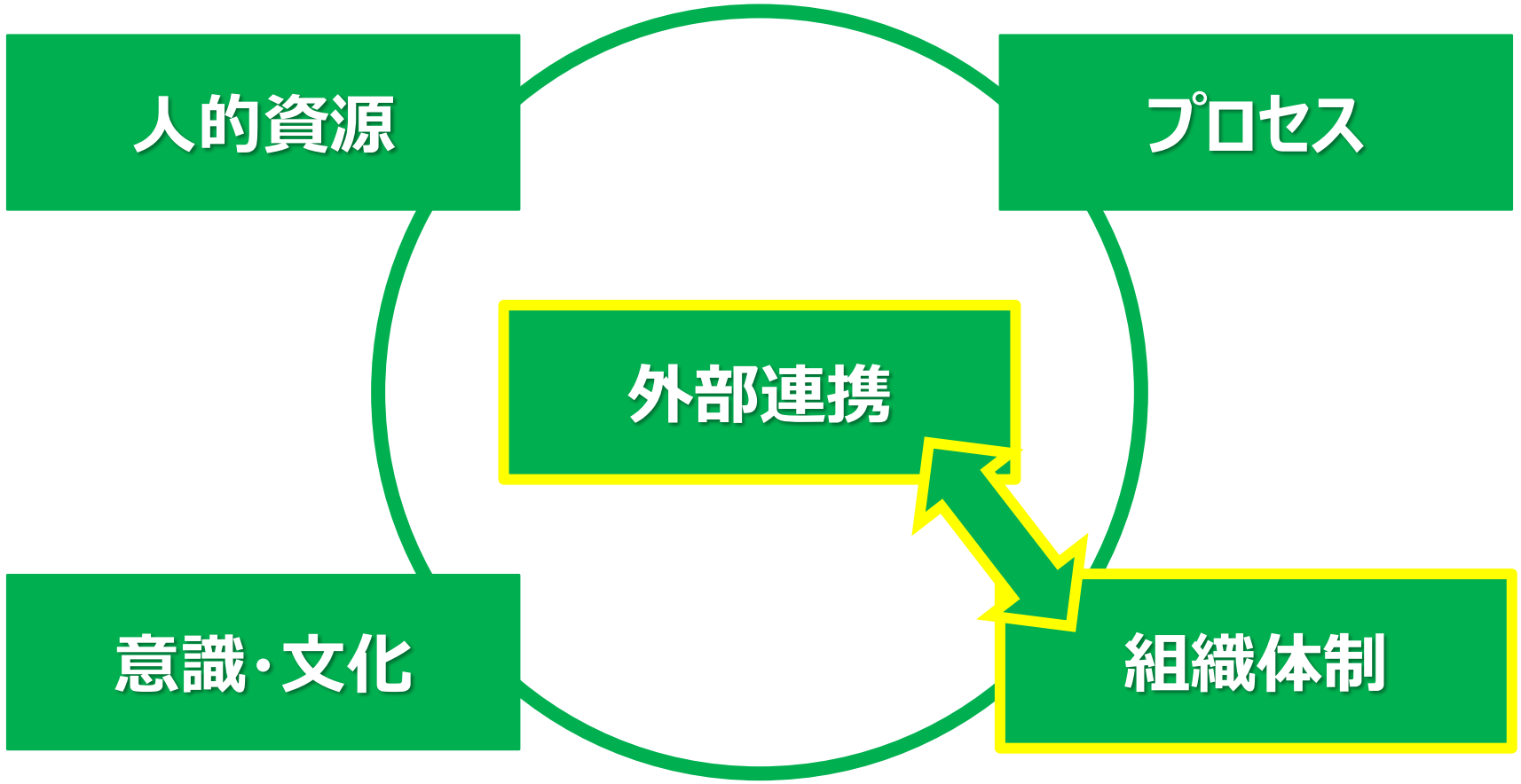
- ✓ 経営層の無関心
- ✓ 属人的対応の放置

- ■ サイバー事故は「システムの問題」ではなく、顧客対応や行政報告を通じて事業継続や社会的信頼に直結する経営リスクである。
- ■ しかし、中小中堅組織では担当者以外には「ITは自分事ではない」という風土が根強く、対策が後手に回りがち。

意識と文化は他の4要素を支える空気のような基盤

限られた資源でなにができるか

小規模ゆえの構造的ぜい弱性からの脱却案



限られた資源でも「止血処置としての初動体制」はつくれる

- **サイバー事故対応＝企業経営におけるダメージコントロール**
  - ダメージコントロールのために最も大切なのは「止血処置」
    - 被害範囲の拡大をさせないために、インターネット切断するなど

- **限られているのは組織内部の資源**
  - 必要な機能を特定して、それぞれにあったアウトソース先をみつける
    - インシデント対応のプロ
    - セキュリティ技術のプロ
    - 対外対応のプロ
    - 法律のプロ

- **とはいえ、最低限組織内に必要なひとも定める**
  - “責任者”と”意思決定者”は不可欠

▼ インシデント対応のプロの例

円滑なサイバー事故対応プロセスはつくれる

- **プロセスとエスカレーションフローを用意し、対応に迷う時間を減らす**
  - 連絡体制表をベースとした役割、権限および連絡先の明確化
  - 外部のプロの連絡先も連絡体制表には含まれる
  - 報告様式が決められている
  - 会議体が決められている
    - 報告、共有、意思決定がなされる場が明確になっている
    - 外部のプロが参加する場が明確になっている

意識・文化の醸成していくためのきっかけはつくれる

- **セキュリティならではの【意識・文化】の醸成を検討していく**
  - バックオフィスは口が軽いと信用を失う
  - 一方、セキュリティは一定のルールのもとで生々しい情報のやりとりがなされている
- **組織内部で仲間をつくる。味方をつくる**
  - ひとりでがんばらなくていい、助け合えるひとが必ずいる
- **組織の外にも仲間をつくる。味方をつくる**
  - 世の中のやりかたを知り、じぶんたちに合ったものさしをつくる

まとめ

備えがまだない中堅中小企業が最低限備えておけること

- **限られた資源でも「止血処置としての初動体制」はつくれる**
  - サイバー事故対応＝企業経営におけるダメージコントロールと理解する
  - サイバー事故対応に必要な機能のプロを見つける
  - “責任者”と“意思決定者”は組織内に確保する
- **円滑なサイバー事故対応プロセスはつくれる**
  - プロセスとエスカレーションフローを定める
  - 報告、共有、意思決定がなされる場を明確にする
- **意識・文化の醸成していくためのきっかけはつくれる**
  - セキュリティならではの【意識・文化】の醸成を検討開始してみる
  - 組織内部に仲間をつくる、味方をつくる
  - 組織外部に仲間をつくる、味方をつくる

ありがとうございました

APPENDIXES

NCA Annual Conference 2025 powered by 日本シーサート協議会

「共創と継承：新時代をつくる!」
～CSIRTの「想い」をつなぎ、未来をまもる～

「CSIRTってなんなの？」でも
ご参加いただける無料イベントです。
もしよろしければ、12月に赤坂で
お会いしましょう！

日程	2025年12月18日(木) 10:00-20:00 2025年12月19日(金) 09:30-18:00
目的	日本の情報セキュリティ向上に資するイベント ●国内の組織内CSIRTの情報共有と連携の強化 ●個々の組織内 CSIRT のインシデント対応能力の強化と技術力向上 ●加盟組織の経営層に対する啓発や CSIRT 活動への理解の醸成
場所	赤坂インターシティコンファレンス
構成内容	基調講演、特別講演、発表者募集採用講演、Lightning Talk、パネルディスカッション、ワークショップ、セミナー、企業展示など
対象	NCA加盟組織、及び、それ以外の組織でセキュリティやインシデントマネジメントに興味のある方（現場担当者から経営層まで）
参加費用	**無料**（NCA加盟、未加盟に関わらず参加無料）
主催	一般社団法人日本シーサート協議会
後援・協力(調整中)	一般社団法人 金融ISAC (F-ISAC Japan)一般社団法人 ICT-ISAC (ICT-ISAC-J)独立行政法人情報処理推進機構（IPA）特定非営利活動法人デジタル・フォレンジック研究会 (IDF)一般社団法人 Japan Automotive ISAC (J-Auto-ISAC)一般社団法人日本インターネットプロバイダー協会 (JAIPA)一般財団法人 日本サイバー犯罪対策センター (JC3)一般社団法人日本スマートフォンセキュリティ協会 (JSSEC)一般社団法人日本クレジット協会 (JCA)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 (JNSA)一般社団法人日本ネットワークインフォメーションセンター (JPNIC)一般社団法人ソフトウェア協会 (SAJ)一般社団法人交通ISAC (T-ISAC)ISACA 東京支部