network system
Vulnerability Diagnosis Probe

KATABAMI VDP

～ 効能編 ～

2022年12月（初版）

2023年3月（社外向け 1.0版）

株式会社SYNCHRO 中村 健

SYNCHRO®
CSCC
Cyber Security Countermeasures Center

サイバー攻撃
Cyber Attack

SYNCHRO®
CSCC
Cyber Security
Countermeasures
Center

サイバー攻撃とは？
Cyber Attack の実態

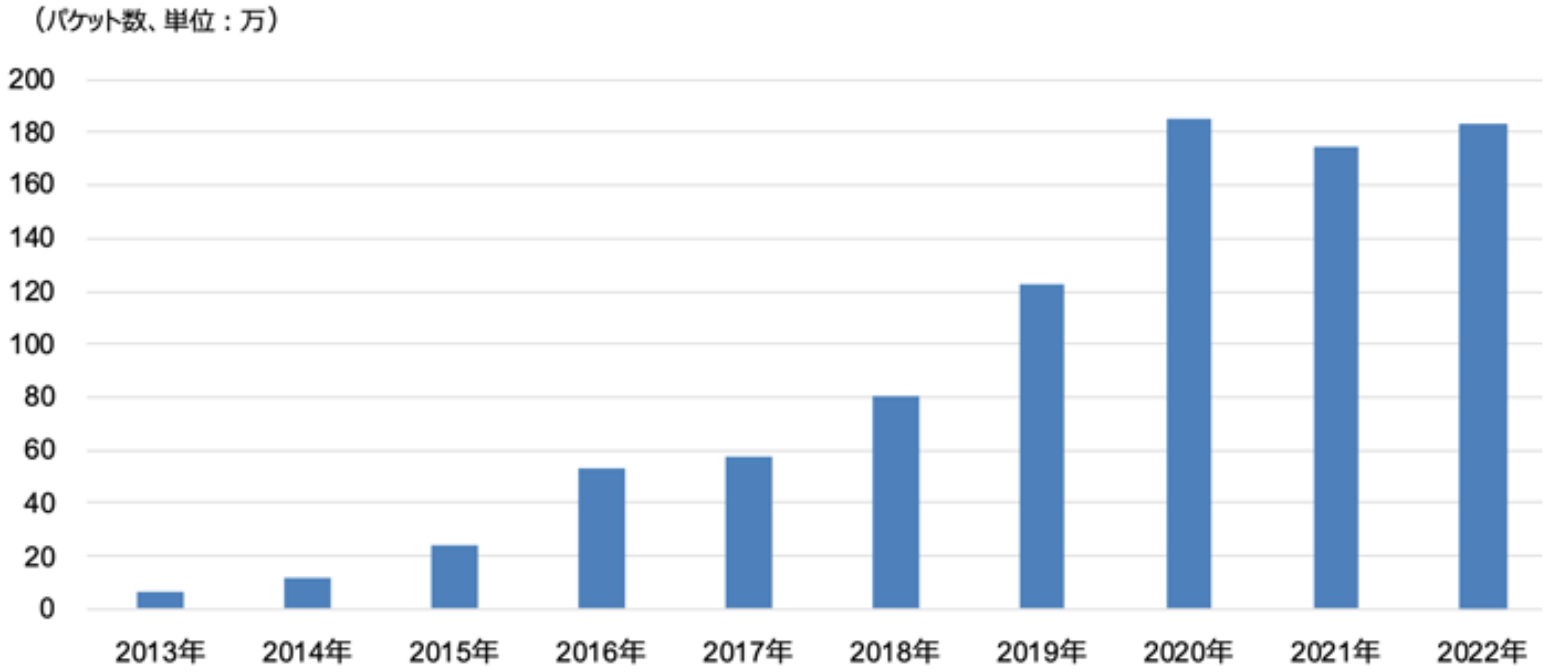
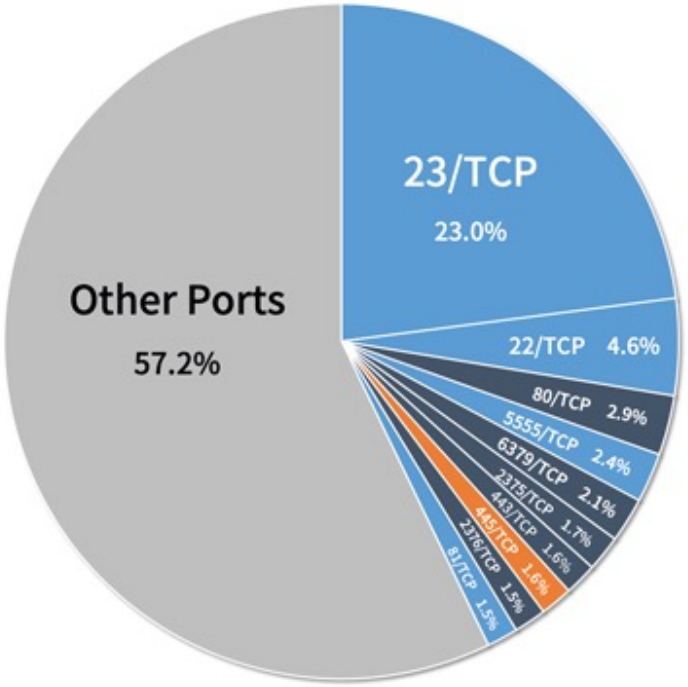


図1. 1 IPアドレス当たりの年間総観測パケット数（過去10年間）

NICTER 観測レポート 2022 (2023.2.14)

SYNCHRO®
CSCC
Cyber Security Countermeasures Center

サイバー攻撃とは？
Cyber Attack の実態



ポート番号	攻撃対象
23/TCP	Telnet（ルータ，Webカメラ等）
22/TCP	SSH（サーバ，ルータ等）
80/TCP	HTTP（Web管理画面）
5555/TCP	ADB (Android Debug Bridge)
6379/TCP	Redis
2375/TCP	Docker REST API
443/TCP	HTTPS (Webサーバ)
445/TCP	Windows SMB
2376/TCP	Docker REST API
81/TCP	HTTP（ホームルータ等）

宛先ポート番号別パケット数分布
（調査目的のスキャンパケットを除く）

図2. 宛先ポート番号別パケット数分布（調査目的のスキャンパケットを除く）

注: 2位の22/TCPには、一般的なサーバ（認証サーバなど）へのスキャンパケットも含まれます。また、その他のポート番号（Other Ports）の中にはIoT機器を狙ったパケットが多数含まれます。

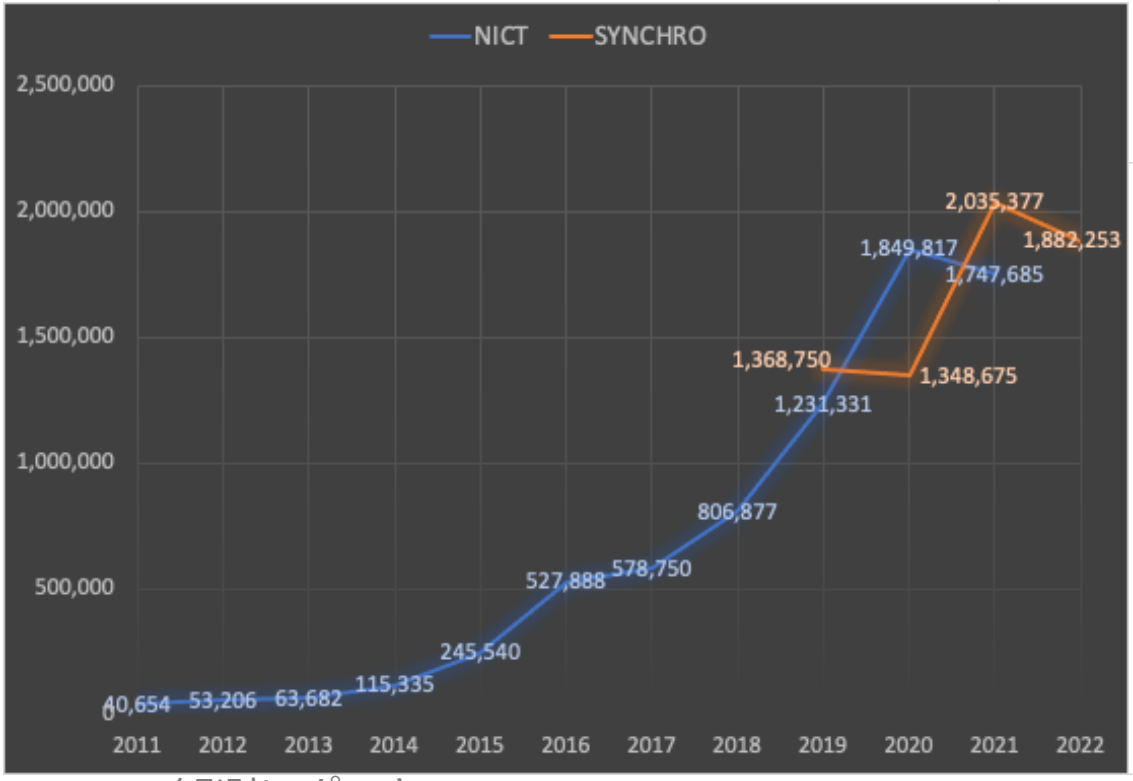
NICTER 観測レポート 2022

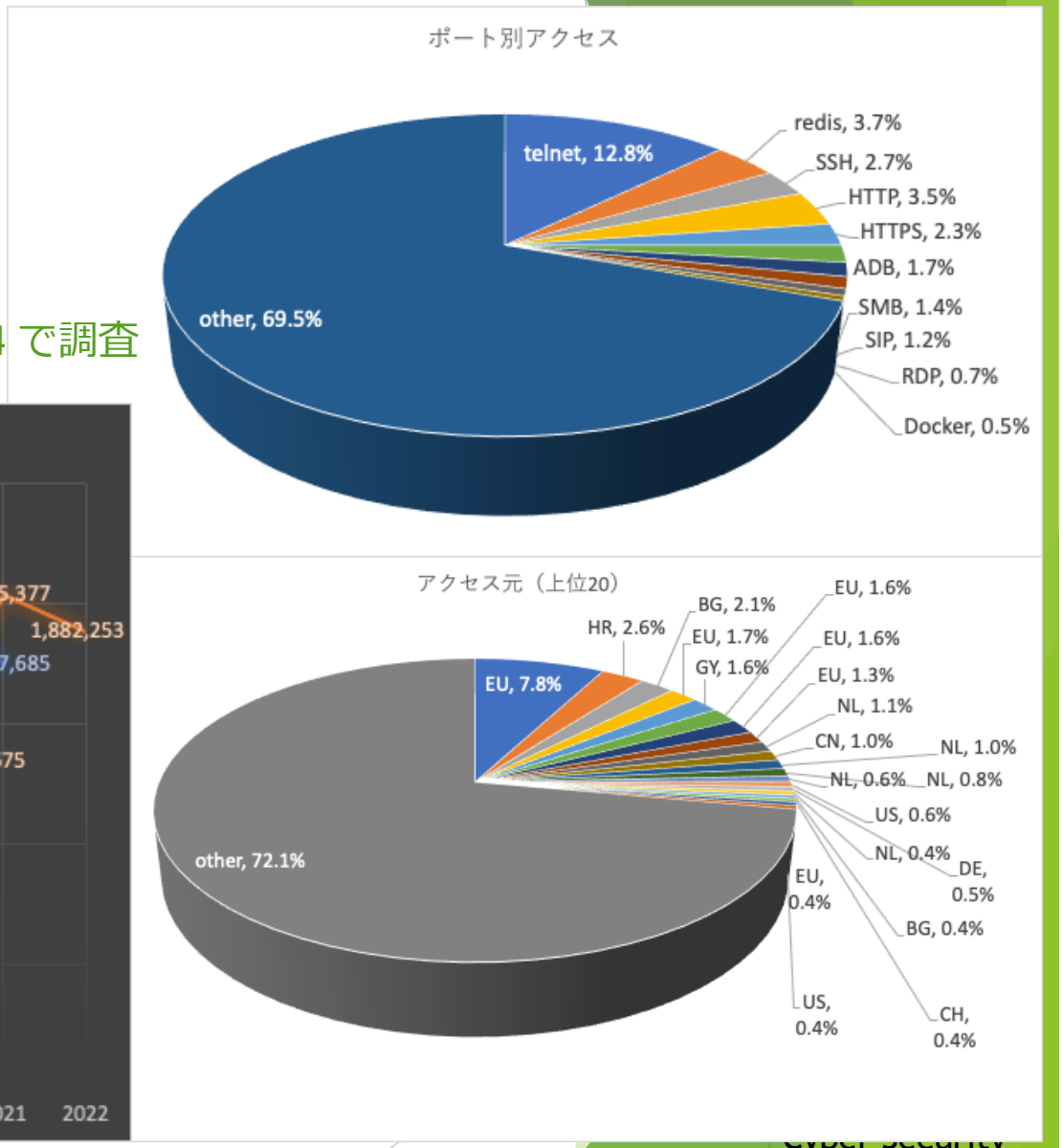
SYNCHRO®
CSCC
Cyber Security Countermeasures Center

サイバー攻撃とは？

Cyber Attack の実態

SYNCHRO の 独自調査：
2019年から実施。2022年は8月14日に7 IPv4 で調査



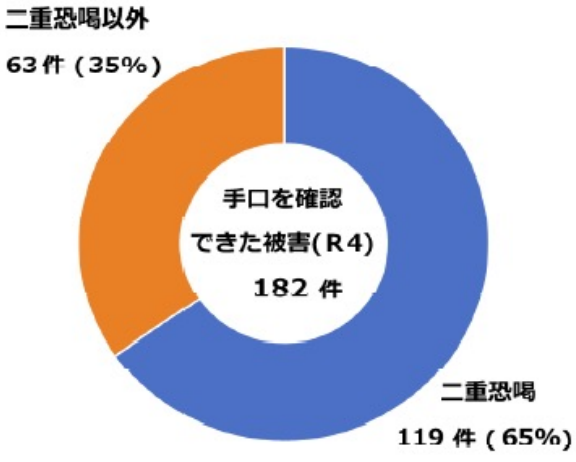


NICTER 観測レポート
＋ *SYNCHRO の global IPv4* で独自調査結果

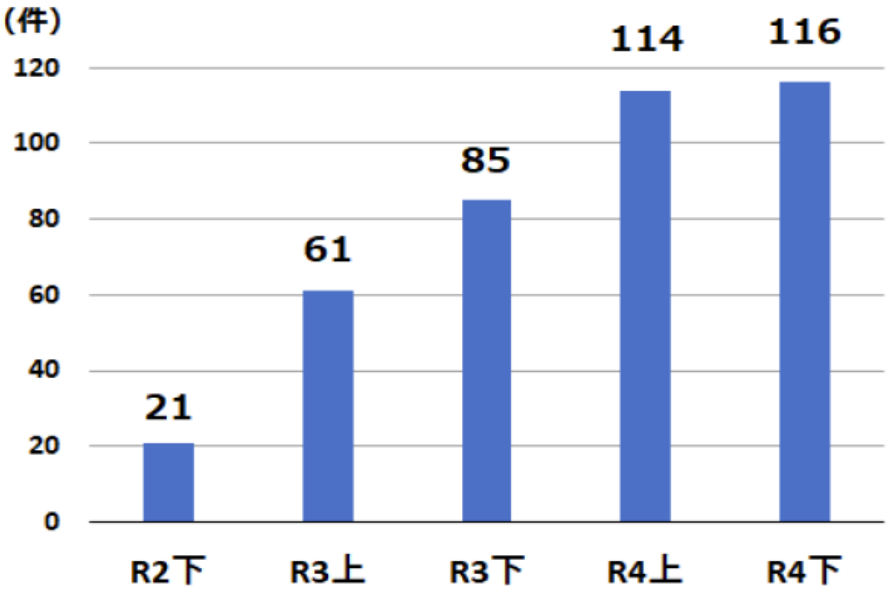
ランサムウェア攻撃・警察庁の報告 (2023.3.16)

認知件数、手口
被害組織の規模

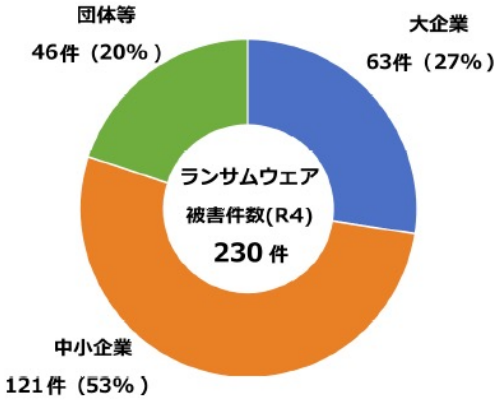
【図表２：ランサムウェア被害の手口別報告件数】



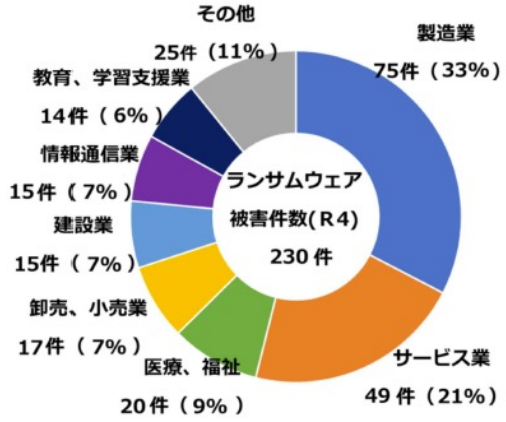
【図表１：企業・団体等におけるランサムウェア被害の報告件数の推移】



【図表４：ランサムウェア被害の企業・団体等の規模別報告件数】



【図表５：ランサムウェア被害の企業・団体等の業種別報告件数】

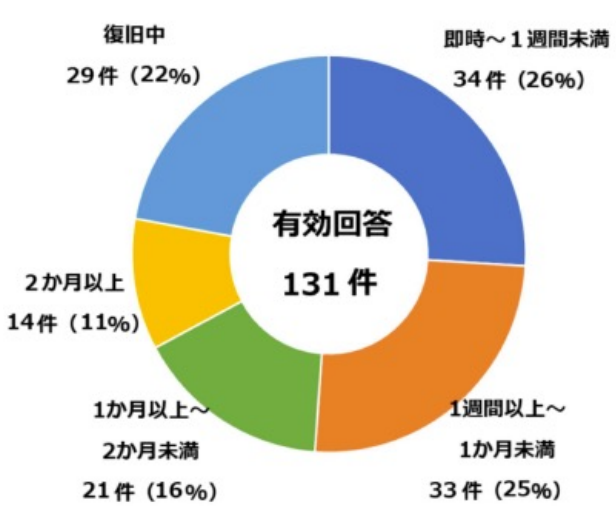


SYNCHRO®
CSCC
Cyber Security
Countermeasures
Center

ランサムウェア攻撃・警察庁の報告 (2023.3.16)

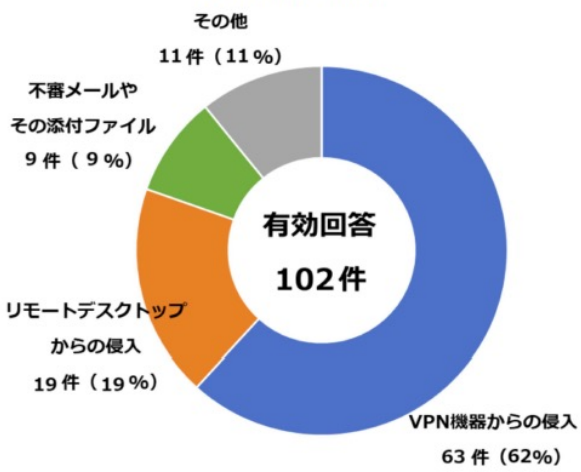
復旧期間、復旧費用、感染経路

【図表７：復旧に要した期間】



【図表８：調査・復旧費用の総額】

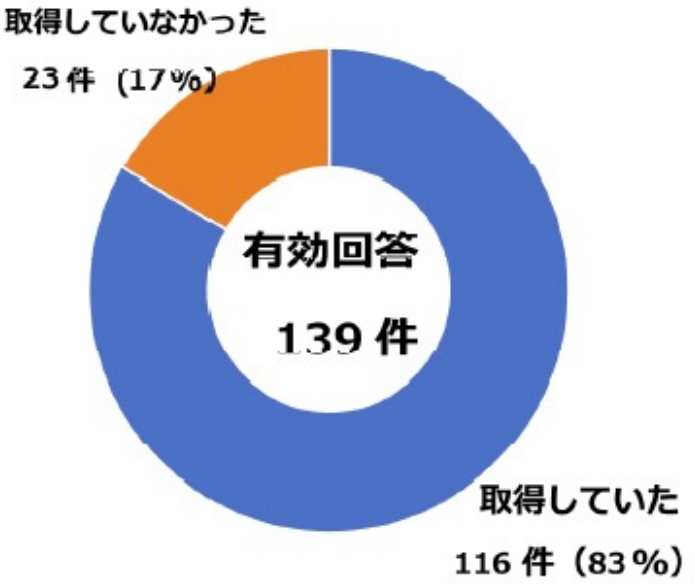
【図表６：感染経路】



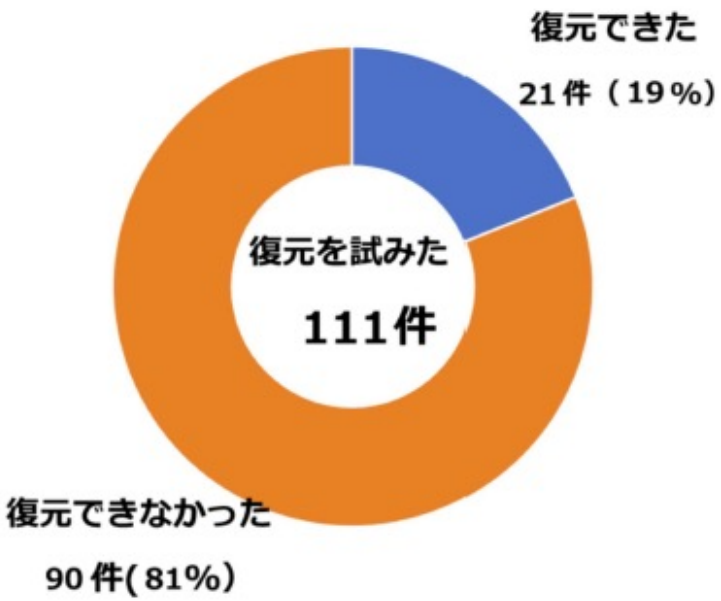
SYNCHRO®
CSCC
Cyber Security
Countermeasures
Center

ランサムウェア攻撃・警察庁の報告 (2023.3.16)
バックアップの有効性

【図表９：バックアップ取得の有無】



【図表10：バックアップからの復元結果】



SYNCHRO
CSCC
Cyber Security Countermeasures Center

サプライチェーン攻撃
名称 と 直近の事例

- サプライチェーン攻撃
  - 本来は「サプライチェーンに対するサイバー攻撃」
  - このパターンの攻撃が増加している
  - →「サプライチェーン攻撃（Supply chain attack）」と縮約
- 2022年に発生した日本企業での事例
  - 株式会社デンソー
    - ドイツの現地法人がランサムウェア攻撃に遭う
    - 設計図や発注書の画像、メールやプリンターの印刷データなどの計157,000件超のデータが窃取
  - 株式会社ブリジストン
    - 米国子会社がランサムウェア攻撃を受けた
    - その対応で、複数の工場が約１週間操業を停止したと発表しています。
  - 小島プレス工業株式会社
    - 国内子会社がランサムウェア攻撃を受けシステム障害が発生
    - （対策として）外部とのネットワーク接続の遮断を行った
    - 結果、トヨタ自動車、日野自動車、ダイハツ工業が生産を見合わせ、14工場の計28ラインが停止し、約13,000台の生産を見送ることとなった

医療機関へのサイバー攻撃
直近の事例

- 2021年 徳島県 つるぎ町立 半田病院
  - 2021年10月：
    - ランサムウェア(LockBit2.0)攻撃により電子カルテシステムなどが暗号化 → 診療を大幅に制限
    - LockBit が犯行声明を出し身代金を要求
  - 2022年1月：　東京の専門事業者が復号したデータなどにより復旧。通常の診療を再開
  - 2022年10月：　専門事業者が LockBit に身代金を支払った疑惑が浮上
- 2022年 大阪府 大阪急性期医療センター
  - 2022年10月：
    - ランサムウェア(Phobos亜種)攻撃により電子カルテシステムなどが暗号化 → 診療制限（外来受入休止など）
  - 2022年12月：　電子カルテシステムが復旧。新規患者の外来診療を再開
  - 2022年1月：　検査、会計、給食システムも再開し完全復旧。原因究明と再発防止はこれから
- 2022年サイバー攻撃を受けた医療機関（未公表事案も含む）
  - 公表：
    - 青山病院(大阪府)、鳴門山上病院、田沢医院(沼津市)、大阪府急性期医療センター、金沢西病院
  - システム障害として公表：　日本歯科大学病院、春日井リハビリテーション病院
  - 未公表：
    - 東北地方眼科有床診療所、九州地方胃腸科外科診療所、関東地方歯科診療所、
    - 愛知県産科有床診療所、東邦大学医療センター大橋病院

SYNCHRO CSCC Cyber Security Countermeasures Center

サイバー攻撃の影響と経営責任

SYNCHRO®

CSCC

Cyber Security Countermeasures Center

企業リスクマネジメントの一部としてのサイバーセキュリティ

経済産業省
「サイバーセキュリティ経営ガイドライン」Ver.3.0」から引用

サイバーセキュリティ対策は「投資」(将来の事業活動・成長に必須な費用) と 位置付けることが重要である。

直接的な収益を算出することは困難ではあるが、企業の価値を維持・増大していく上で、企業活動におけるコストや損失を減らすために必要不可欠な投資であるとともに、サイバーセキュリティリスクを組織の経営リスクの一環として織り込み、その観点からサイバーセキュリティリスクを 把握・評価した上で対策の実施を通じてサイバーセキュリティに関する自社が許容可能とする水準まで低減することは、企業として果たすべき社会的責任であり、その実践は経営者としての責務である。

SYNCHRO
CSCC
Cyber Security Countermeasures Center

経営における情報セキュリティ対策の責任

経産省、内閣官房、経団連 が 明確な定義を表明

- 「サイバーセキュリティ経営ガイドライン」 Ver.3.0　経済産業省
  - 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を認識し、リーダーシップによってリスクと企業影響を考慮した対策を進めることが必要
  2. 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対する総合的なセキュリティ対策が必要
  3. 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、ステークホルダ（顧客・株主等）および事業上の関係者との適切なコミュニケーションによる信頼構築が必要
- 「企業経営のためのサイバーセキュリティの考え方」 内閣官房
  - 企業経営における基本的認識
  1. サイバーセキュリティは、利益を生み出し、ビジネスモデルを革新するものであり、新しい製品やサービスを創造するための戦略の一環として考えていく必要がある。
  2. 全てがつながる社会において、サイバーセキュリティに取り組むことは、社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与することとなる
- 「サイバーセキュリティ経営宣言」 一般社団法人 日本経済団体連合会
  - 経営宣言
  1. 経営課題としての認識
  2. 経営方針の策定と意思表明
  3. 社内外体制の構築・対策の実施

CS対策は
経営責任

CS対策
not コスト
but 投資

SYNCHRO
CSCC
Cyber Security
Countermeasures
Center

サイバー攻撃への影響
予想以上に大きい

- 一次被害
  - 直接被害
    - 逸失利益：売上ダウンによって失う利益
    - 機会損失：見込み成長率分のダウン
  - 間接被害
    - 謝罪文、謝罪訪問、見舞品などの実費発生
    - 広報費用
    - 問い合わせ窓口運営
    - 業務継続費用
- 二次被害
  - 顕在化被害
    - ブランド力の低下
    - 取引先からの信用の低下
    - 無関係な勤務者のモチベーション低下
    - 漏洩した個人情報を再利用した 詐欺事件の発生、賠償など

SYNCHRO
CSCC
Cyber Security Countermeasures Center

経営における情報セキュリティ対策の責任
急がれる体制作り

- セキュリティインシデントが発生した場合
  - 経営者によって企業の情報セキュリティ方針(ポリシー) が明確化されていない
  - 方針(ポリシー) が組織や供給者へ発信されていない
  - 方針(ポリシー) に基づいて、対策が計画・実行がされていない
  - 情報資産および個人情報が把握できていない
  - 経営者の積極的関与の報告(記録) が無い
- などの状態が確認された場合は 行政指導を含むペナルティが発生する可能性があります！

CS対策を
怠ると
ペナルティ

SYNCHRO
CSCC
Cyber Security
Countermeasures
Center

サイバー攻撃の影響と経営責任

SYNCHRO®

CSCC

Cyber Security Countermeasures Center

KATABAMI VDP
導入の狙い

SYNCHRO®
CSCC
Cyber Security
Countermeasures
Center

KATABAMI VDP導入
その目的

- 基本的な目的
  - 対象事業者さまをサイバー攻撃から守ること
  - 結果、サイバー攻撃による 負の影響 を抑止すること
  - 対象事業者さまの 従業員、顧客、パートナ、株主(出資者) を守ること
  - ひいては、対象事業者さまの経営者を守ること
- 直接的な目的
  - ① 対象事業者のネットワークの構造、接続する機器を把握すること
  - ② 対象事業者のネットワーク、機器を検査し、脆弱性を検出すること
  - ③ 検出した脆弱性に対する対策案を提示すること（対策実施は対象外）
  - ④ ①～③を継続的に実施すること（新たな脆弱性が日々発見・報告される）
  - ⑤ ①～④に基づき、ネットワーク構造の再設計、機器の見直しなどを含み改善策を提示すること

SYNCHRO
CSCC
Cyber Security Countermeasures Center

KATABAMI VDP導入
そのメリット

- 基本的なメリット（Sales Talk）
  - 機器を含む自身のネットワークの弱点を顕在化できること
  - 顕在化した弱点に対する対応方法を提示してもらえること
  - 弱点に対する対策実施で、サイバー攻撃のリスクを低減できること
  - 上記を、継続的に、かつ、安価に実現できること
- 直接的なメリット
  - KATABAMI VDP を適用することでネットワーク内から検査ができること
    - インターネット越しの検査では検出できない脆弱性を顕在化できる
      - メール添付、ダウンロード、USBメモリなどで持ち込まれるマルウェアに対する防御は、ネットワークと機器の内部対策が必用
      - この問題の把握は、外部からの調査ではあぶり出せない
  - KATABAMI VDP の適用で高レベルの検査を低コストで実現できること
    - ネットワーク内の検査のための人員を定期的に派遣するとコストが増大する
    - KATABAMI VDP がコスト増大を抑止する

SYNCHRO®
CSCC
Cyber Security Countermeasures Center

SYNCHRO & KATABAMI

CSCC

Cyber Security Countermeasures Center

SYNCHRO 基本情報

会社名	株式会社SYNCHRO
設立	2001年 4月
従業員数	14名（契約社員を含みます）
資本金	230,171千円
売上高	302,330千円（2019年度）
事業	物理セキュリティ（静脈認証、顔認証）製品 ネットワークセキュリティ製品 ソフトウエア設計・開発・保守・運用
代表者	室木勝行
住所	東京都千代田区九段北1-10-9 九段VIGAS 5階
電話／FAX.	Tel.03-4570-3291 Fax.03-4570-3292
ホームページ	https://www.udc-synchro.co.jp

	サイバーセキュリティー対策センター
住所	山口県山口市熊野町１−１０ニューメディアプラザ山口６階
電話／FAX.	Tel.083-902-2518

	山口サテライト本社
住所	山口県山口市湯田温泉３丁目2-7 セントコア山口 1階
電話／FAX.	Tel.083-902-2818 Fax.083-902-2819

SYNCHRO
CSCC
Cyber Security Countermeasures Center

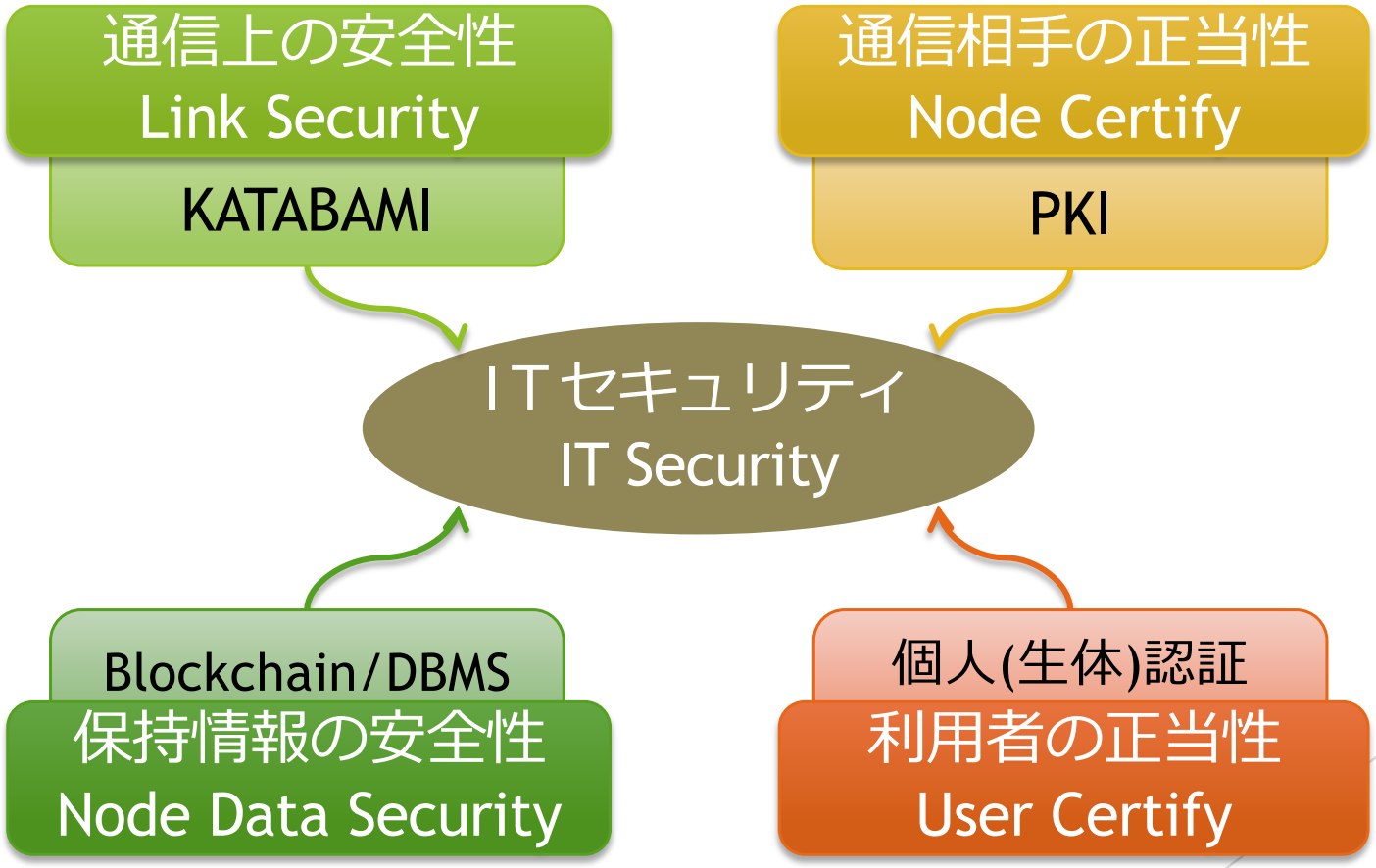
資格、認定など
直近でのSYNCHROの実績、資格等

- 経済産業省 令和３年度補正予算（実施=2022年7月～2023年1月）
  - 開発段階におけるIoT機器の脆弱性検証促進事業
    - SYNCHRO = 検証事業社（12社中の１社）
    - 全155製品中、13製品を SYNCHRO で担当
- セキュアIoTプラットフォーム協議会
  - 「セキュアIoTプログラム」Gold認定
    - KATABAMI、KATABAMI Box、助っ人番SSB、助っ人番サービス
- 経済産業省「情報セキュリティサービス基準審査」
  - KATABAMI VDP（事業社のサイバー環境の脆弱性検証）
  - 2023年６月登録（予定）
- 独立行政法人情報処理促進機構(IPA)「サイバーセキュリティお助け隊」
  - KATABAMI VDP（事業社のサイバー環境の脆弱性検証）
  - 登録(参入)手続き中

SYNCHRO®
CSCC
Cyber Security Countermeasures Center

ITセキュリティの作り方

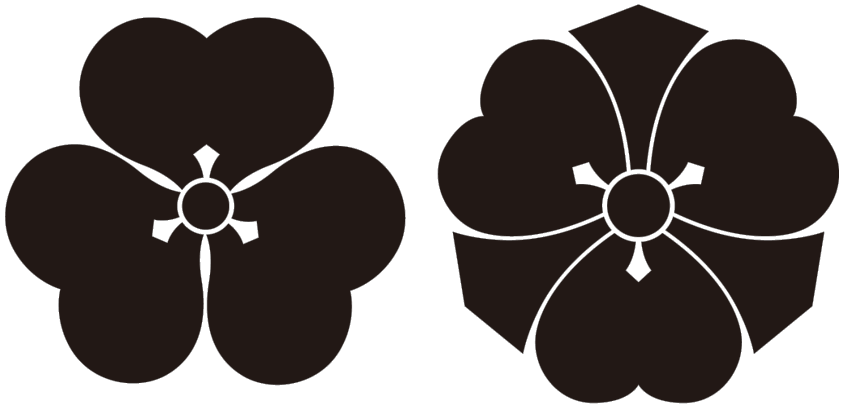
４要素 を 構成する要素技術



SYNCHRO
CSCC
Cyber Security Countermeasures Center

なぜ、KATABAMI
命名の由来

- KATABAMI = カタバミ（片喰）
  - 被子植物、バラ類、カタバミ目、カタバミ科
  - 駆除が難しいと言われる雑草の一種
  - 球根、地下茎も持つが、匍匐茎（ほふくけい）を持ち地表に広がる
- 匍匐茎がネットワークっぽいので KATABAMI と命名
- 家紋にもなっている



SYNCHRO®
CSCC
Cyber Security Countermeasures Center