国産セキュリティ「KATABAMI」で進めるSecure DX

第1.0版2025年12月

株式会社SYNCHRO

取締役CMO　北口　順治

Powered by KATABAMI

1. SYNCHROとKATABAMIのご紹介

株式会社SYNCHRO

当社のミッション

飽くなき「パーフェクトアクセスコントロール」を追求するSYNCHRO

- リアル空間に於けるフィジカルアクセスコントロールと、サイバー空間に於けるサイバーアクセスコントロールを徹底する「トータル・アクセスコントロール」と言う概念で、飽くなきパーフェクトアクセスコントロールを追求し、安全安心な社会システムの稼働を支える
- 日本発のセキュリティブランドを志向し、3年後のパブリックカンパニー（IPO）を目指す。

企業案内

「世の中の潜在ニーズにSYNCHRO（シンクロ）する事業の追求」と言う経営理念に基づき
21世紀に必須のセキュリティ課題に対し独自技術の社会実装で社会課題の解決に臨む

- 設立　2001年4月（第二創業）　※初代は1927年宇部電業として創業
- 資本金　315,171千円（2025年4月現在）
- 社員　38名（含　契約社員）（2025年9月現在）
- 代表者　室木　勝行
- 事業所　東京本社　東京都千代田区九段北1-10-9 九段VIGAS5階
  山口支店　サイバーセキュリティ対策センター（CSCC）
  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
- サテライトオフィス　中央大学研究機構
- サイト　https://www.udc-synchro.co.jp/

資格、認定情報

Powered by KATABAMI

直近でのSYNCHROの実績、資格、認定

- **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
- **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

- **一般社団法人セキュアIoTプラットフォーム協議会**
  - SYNCHRO =「セキュアIoTプログラム」指定検証事業者
    - ＊SYNCHRO =指定検証事業者（3社中の1社）
  - 「セキュアIoTプログラム」Gold認定取得　※試験項目「95%」以上

- **日本セキュリティ大賞　優秀賞受賞　2024年10月29日受賞**
  - セキュリティ対策・運用、運用支援、人材育成のベストプラクティスを表彰
  - SYNCHROが日東工器様およびメンテック様で実施した工場DX活動を評価

優秀賞 受賞

- **フォーティネットジャパンとのビジネスアライアンス　2025年8月28日発表**
  - 当社KATABAMIを活用した「Yamaguchi Secure DX Core」を協業で推進し「地方創生」モデルとして全国展開開始

KATABAMIとは？

Powered by KATABAMI

安全な通信経路を軽快かつ安価に提供する国産セキュリティ

※米国の国家安全保障局が2030年まで認める方式で実装

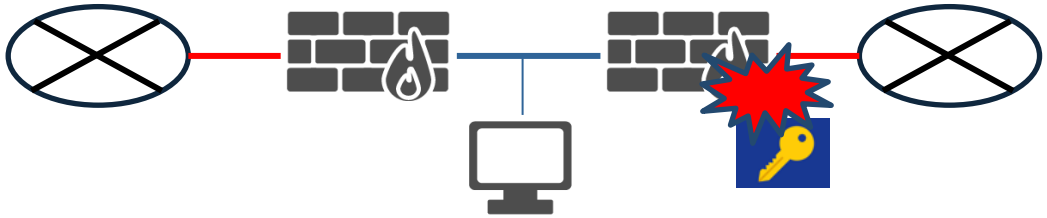
- 高度なセキュリティ
  - エンドポイント間の認証(デバイス認証)を実現
  - End-to-End-Encryption の独自暗号化技術(KATABAMI)
  - 結果、なりすまし、中間者攻撃を理論的に排除
- 利用者にとって優しい実装方式
  - KATABAMIが生成するIPv6 addressで通信するだけ
  - アプリケーション側での認証処理、暗号化処理は不要
- 広い適用範囲
  - KATABAMI は OS上のServiceとして動作するだけ
  - 各種OS(Linux、Windows、MacOS、Android等)に対応
  - KATABAMIは各種の通信機器やデバイス(IoT機器)に設定可能

KATABAMI通信　1/3

Powered by KATABAMI

KATABAMIは、「公開鍵暗号方式」で End-to-End で認証を行います。

インターネットVPNの場合



・VPNはネットワーク間を連接する機能。ネットワーク内での通信を保護する機能はない

KATABAMIの場合

・E2Eでの認証、E2Eでの暗号化を行う
・このような仕組みを ZTNA（Zero Trust Network Access と称する）

KATABAMIは、End-to-End の通信を共通鍵で暗号化

・KATABAMIでは、通信経路上でデータを窃取されることはない

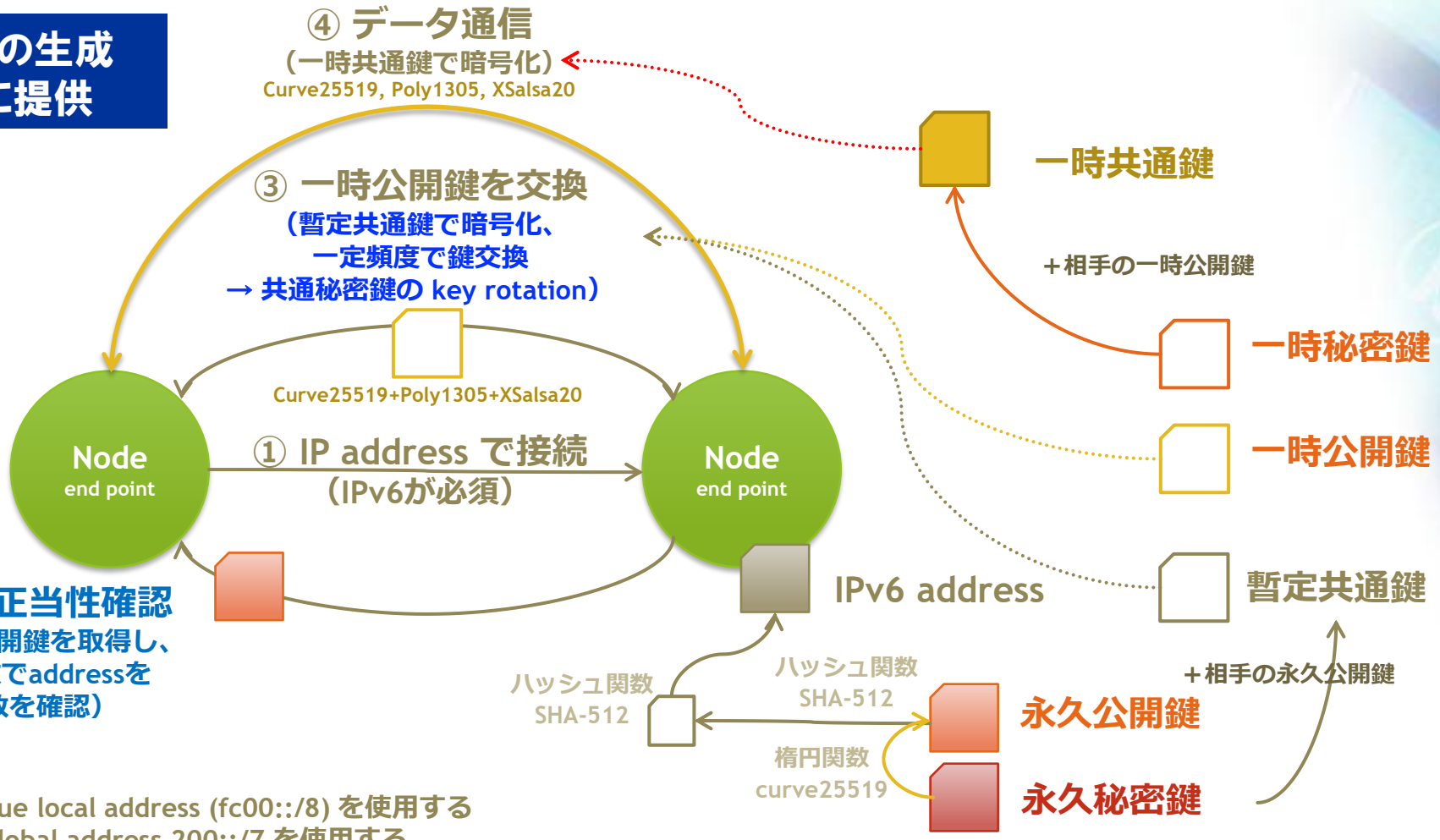
KATABAMI は ゼロトラストセキュリティを実現

・KATABAMI では、IPアドレスを偽装できない。→なりすましを抑止
・KATABAMI では、通信データは共通鍵で暗号化される → 中間者攻撃を抑止
・KATABAMI では、共通鍵は更新される（Key Rotation）→ 前方秘匿性を確保

KATABAMI通信　2/3

Powered by KATABAMI

安全な通信経路の生成
軽快かつ安価に提供

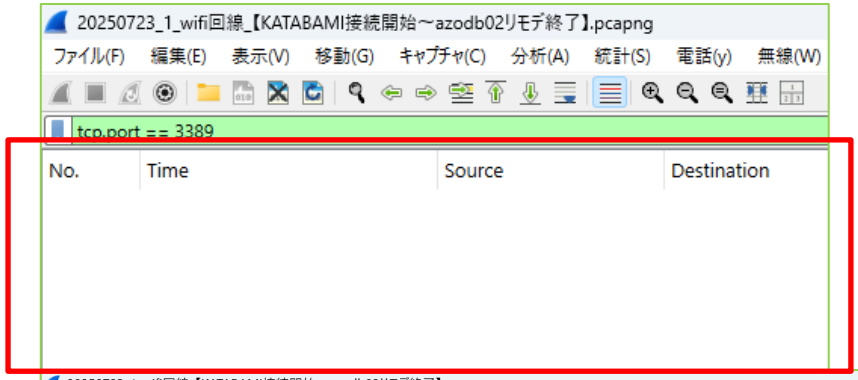


IPv6 address は、
- Cjdns では unique local address (fc00::/8) を使用する
- Yggdrasil では global address 200::/7 を使用する
  - RFC1888 で NSAP に map されたが RFC4048 で非推奨（詳細は RFC4548）
  - Cjdns との競合を回避 → 共存/併用が可能

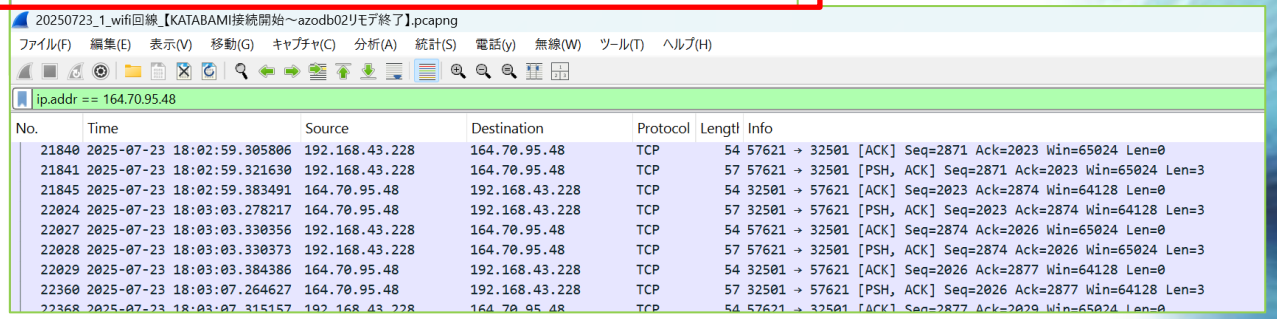
KATABAMI通信　3/3

Powered by KATABAMI

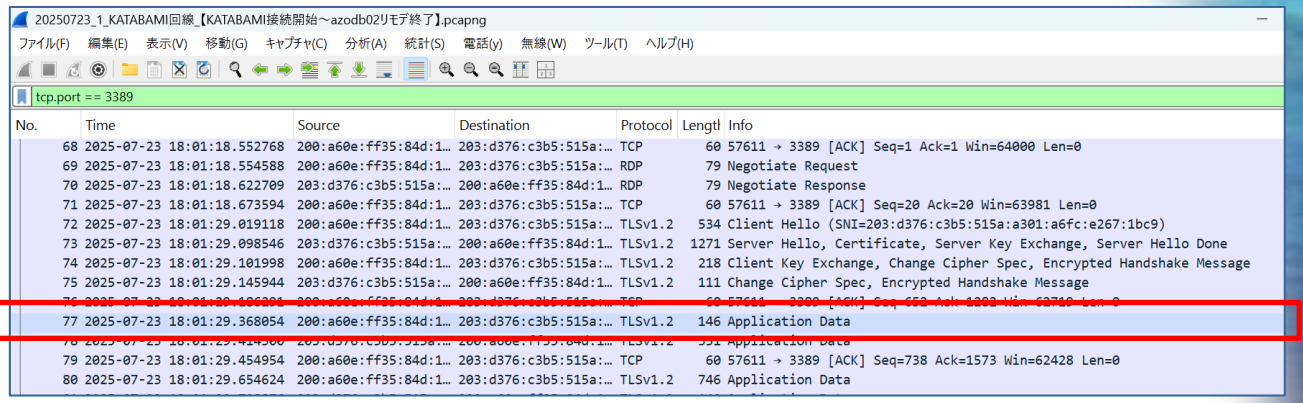
- 通常のネットワーク上では流れているはずの RemoteDesktop の通信を確認できない



- KATABAMI Bridgeとの通信は確認できるが、RemoteDesktop 先の IP やポート、データは秘匿化されている



- KATABAMI の仮想インターフェース上では RemoteDesktop の通信が確認できる
  ネットワーク上では前頁の通り、暗号化されており確認できないが、KATABAMIの機能により
  エンドポイント側では復号されたため確認できる



2. サイバー攻撃の概況

最近のサイバー攻撃事例

アタック件数
平均14件/日

新たな攻撃手口
平均2000件/月

【ランサムウェア攻撃】　（ランサム：身代金　ウェア：ソフトウェア）
コンピュータシステムに不正に侵入し、データを暗号化するなど
使えなくしたうえで、身代金支払いを要求する悪意のある行為

業務妨害　情報漏えい　信頼喪失

2024年ランサムウェアによる被害件数222件（警察庁発表2025/3/13）
2024年ノーウェアランサムによる被害件数22件（警察庁発表2025/3/13）

事例1：名古屋港へのランサムウェア攻撃
2023年7月4日6:30頃発生
全ターミナルの作業が約2日間停止
名古屋港統一ターミナルシステムの全サーバーが暗号化
LockBitの犯行として2名が逮捕（2024年2月）

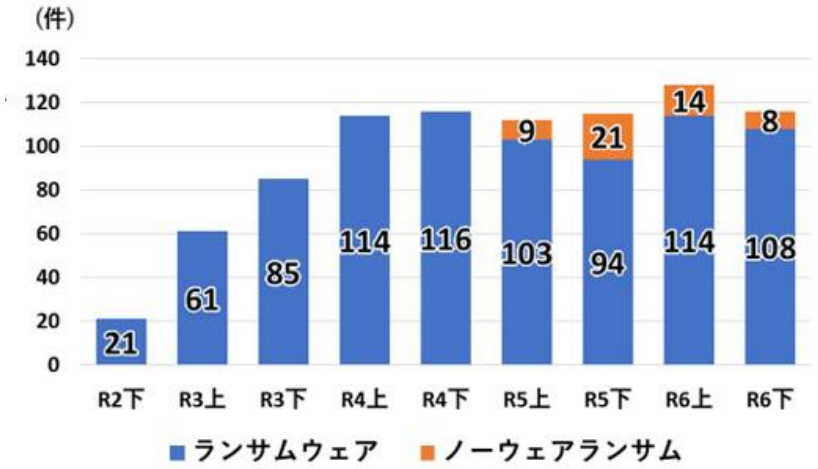
事例2：角川グループへのランサムウェア攻撃
2024年6月8日　発生
「ニコニコ動画」の配信などが停止
7月1日を期限として身代金支払いを要求
サイバー犯罪グループ「Black Suit」による攻撃

事例3：アサヒホールディングスに「Qilin」がランサムウェア攻撃
2025年9月29日出荷停止　11月27日記者会見
①VPN経由の侵入を示唆、脆弱性突かれ被害後に廃止
②攻撃を「EDRで検知できず」
③バックアップは「健全」も、復旧しやすさに課題

増え続けるサイバー攻撃（統計情報）

ランサムウェア攻撃・警察庁の報告
（2025.3.13）
認知件数、手口
被害組織の規模

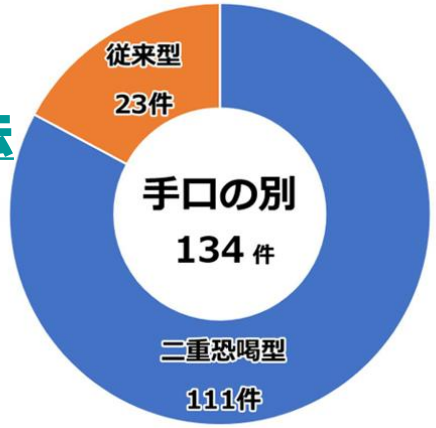
【図表３：ランサムウェア被害報告件数】



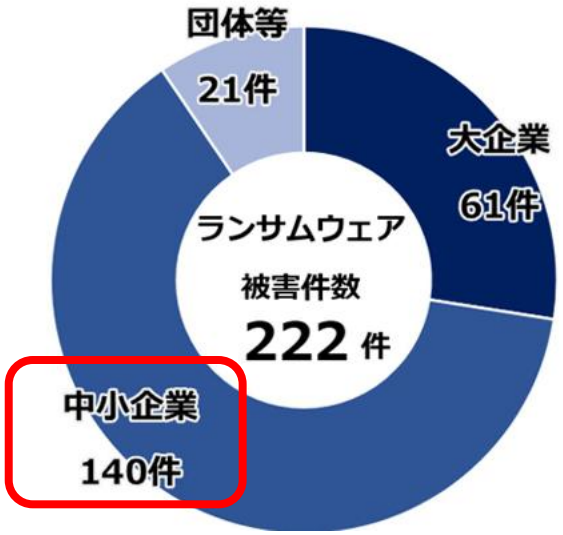
※　ノーウェアランサム：暗号化することなくデータを窃取した上で、対価を要求する手口。令和５年上半期から集計。

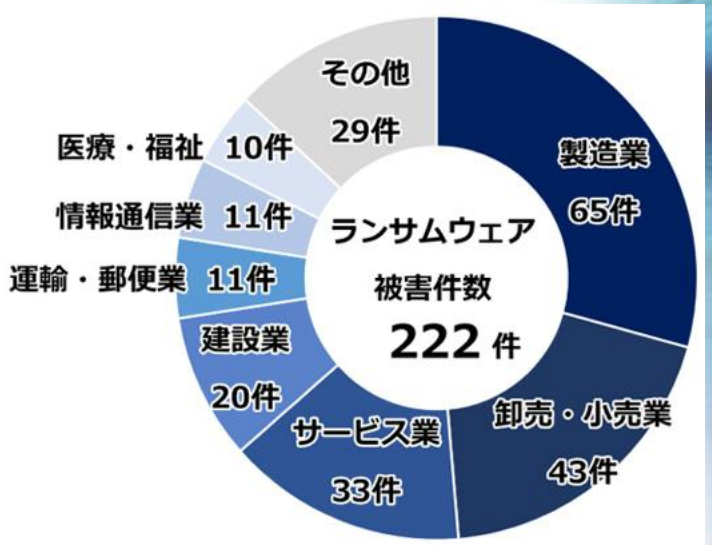
ランサム攻撃（認知）件数の推移

手口、身代金支払方法



被害者の分類





大企業への攻撃は減った一方で
中小企業への攻撃は37％増加

増え続けるサイバー攻撃（統計情報）

ランサムウェア攻撃・警察庁の報告

(2025.3.13)

復旧期間、復旧費用、感染経路

復旧期間

復旧費用

感染経路

増え続けるサイバー攻撃（統計情報）

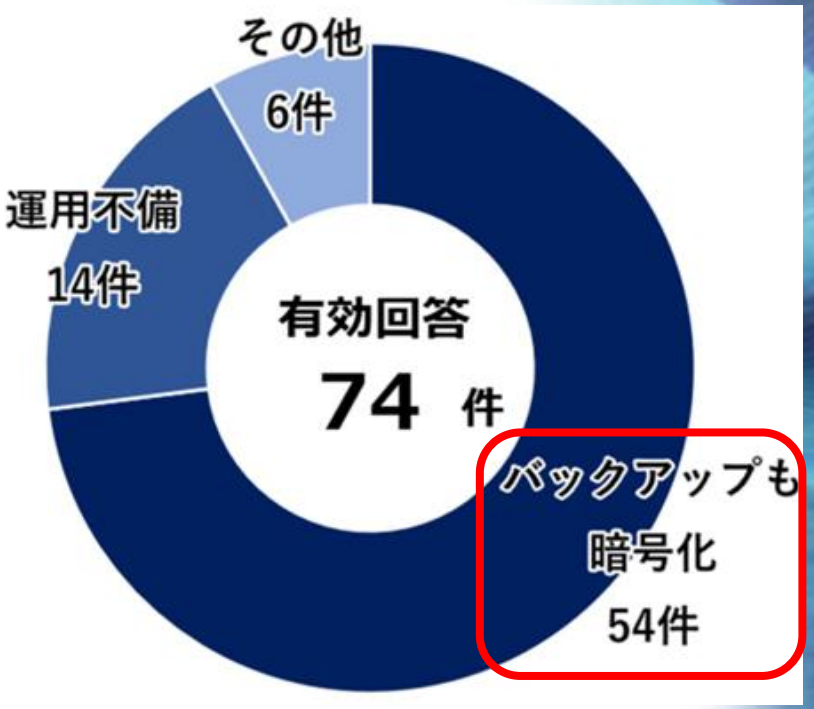
ランサムウェア攻撃・警察庁の報告

（2025.3.13）

バックアップの有効性

バックアップの有無

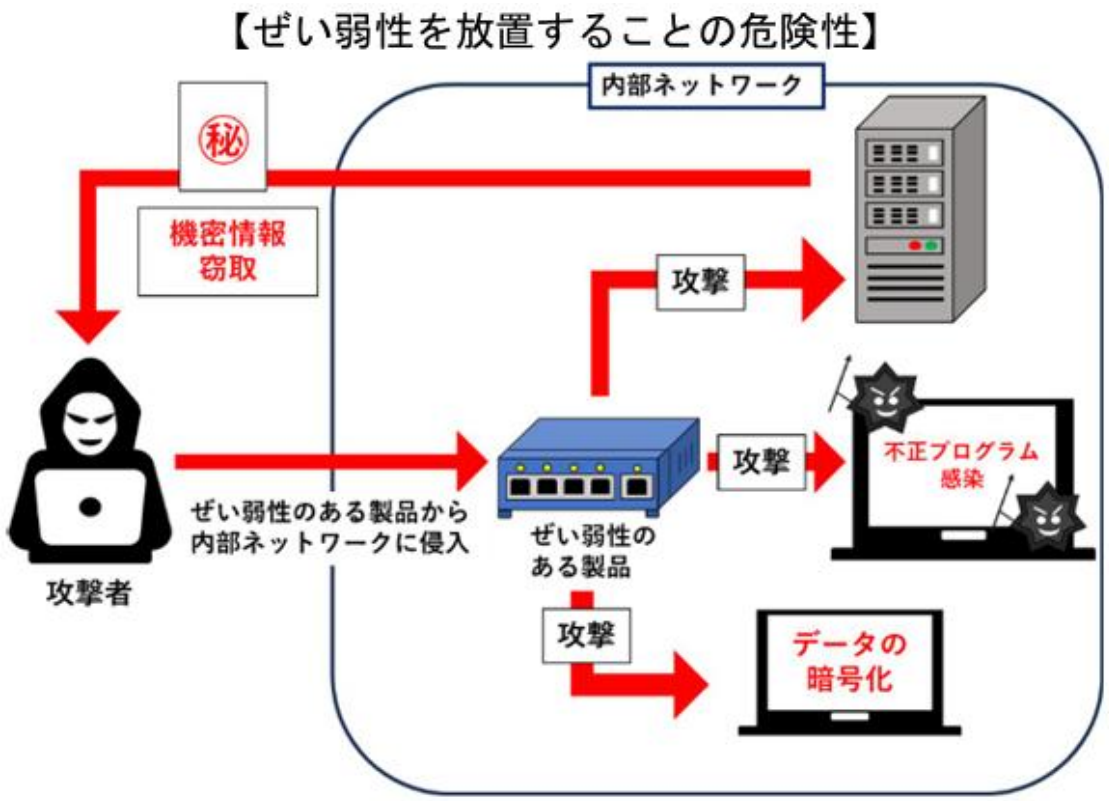
バックアップからの復旧

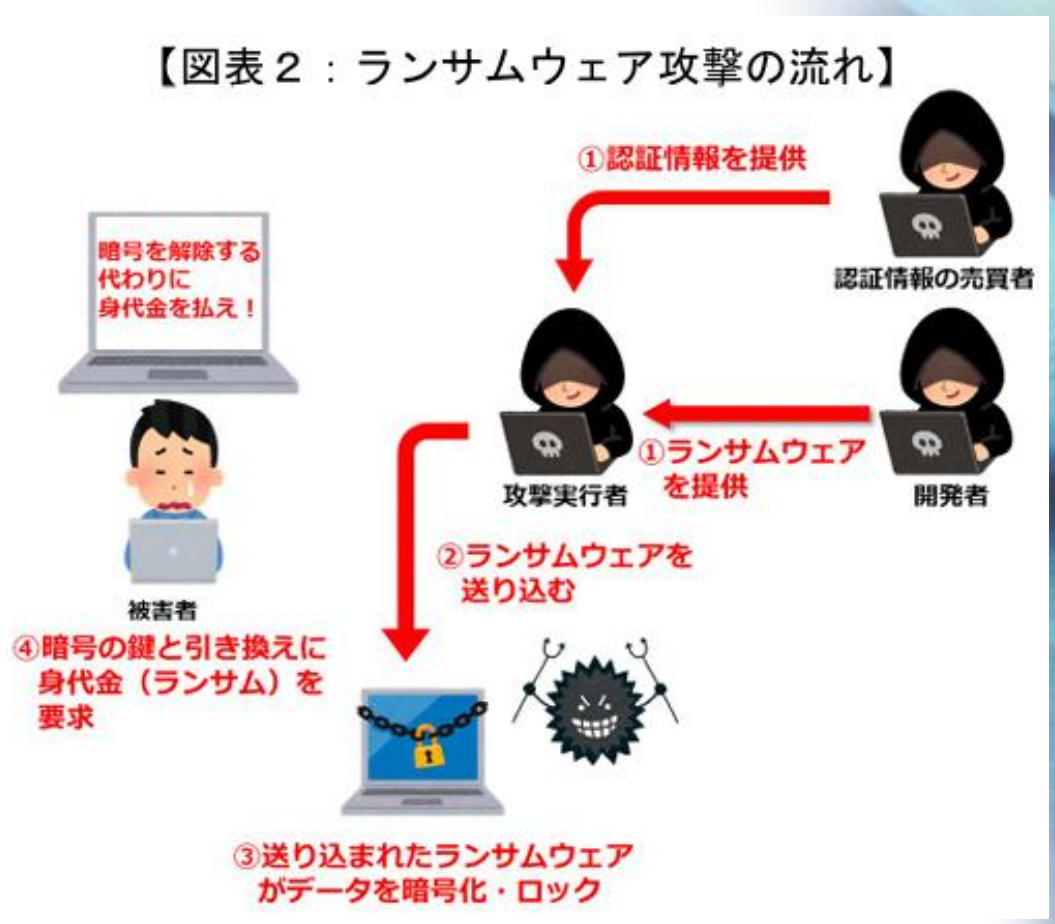


復旧出来なかった理由

増え続けるサイバー攻撃（危険性と手口）

ランサムウェア攻撃の手口
（サイバー企画課　公表2025.3.13）





出典：警察庁サイバー企画課　2025年3月13日公開資料より

企業のためのセキュリティアクション

経産省　５段階格付け　サプライチェーン攻撃への対策　2026年10月開始予定

サイバーセキュリティ対策の5段階格付け概要

レベル	対象	要件	認定方法
1-2	中小企業	アクセス制限 ソフトウェア更新	自己宣言
3-4	取引先と供給網を構築する企業	情報管理の強化 責任者の配置	自己宣言 第三者機関
5	重要インフラ関連企業	官民共有 復旧手順の事前策定	第三者機関

出典：日本経済新聞社　2024年4月5日記事

- **★3：Basic：全てのサプライチェーン企業が最低限実装すべきセキュリティ対策として、基礎的なシステム防御策と体制整備　を中心に実施（自己評価（25項目））**
- ★4：Standard：サプライチェーン企業等が標準的に目指すべきセキュリティ対策として、組織ガバナンス・取引先管理、**システム防御・検知、インシデント対応等包括的な対策を実施（第三者評価（44項目）※）**
  ※第三者評価を原則とするが、評価コストの負担を抑える観点から、詳細は今後検討予定。
- ★5：サプライチェーン企業等が到達点として目指すべき対策として、国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施（第三者評価（対策項目は今後検討予定））

出典：経済産業省　2025年4月14日公表

3. SECURE DXの推進

Powered by KATABAMI

DX推進によるサイバーリスク

セキュリティ人材の
不足数は約11万人

中小企業における人材と運用の現状

出典：日本国内の中小企業のサイバーセキュリティに関する実態調査2024年版（2024.8）パロアルトネットワークス株式会社

89%

サイバーリスクが
自組織に与える
ビジネス上の影響を懸念

1位	得意先への悪影響	48%
	社会的な信用下落	
3位	得意先・取引先からの信用下落	45%
4位	取引先への悪影響	44%
5位	知財やノウハウの外部流出	35%

85%

自組織のセキュリティへの
取り組みに課題があると認識

支援サービスが必要

1位	対策に従事する人材の不足	47%
2位	予算が限られている	42%
3位	対策が十分かわからない	33%

63%

セキュリティ製品・サービスの
運用・保守業務を外部に委託

29%

外部に委託している
運用・保守内容を把握していない

KATABAMIの解決方法

Powered by KATABAMI

現場の課題

- 予算不足
- IT人材の不足
- 防御システムの整備不足

KATABAMIの解決方法

業界最安値での提供

- 1台月額750円～で毎月定期検診

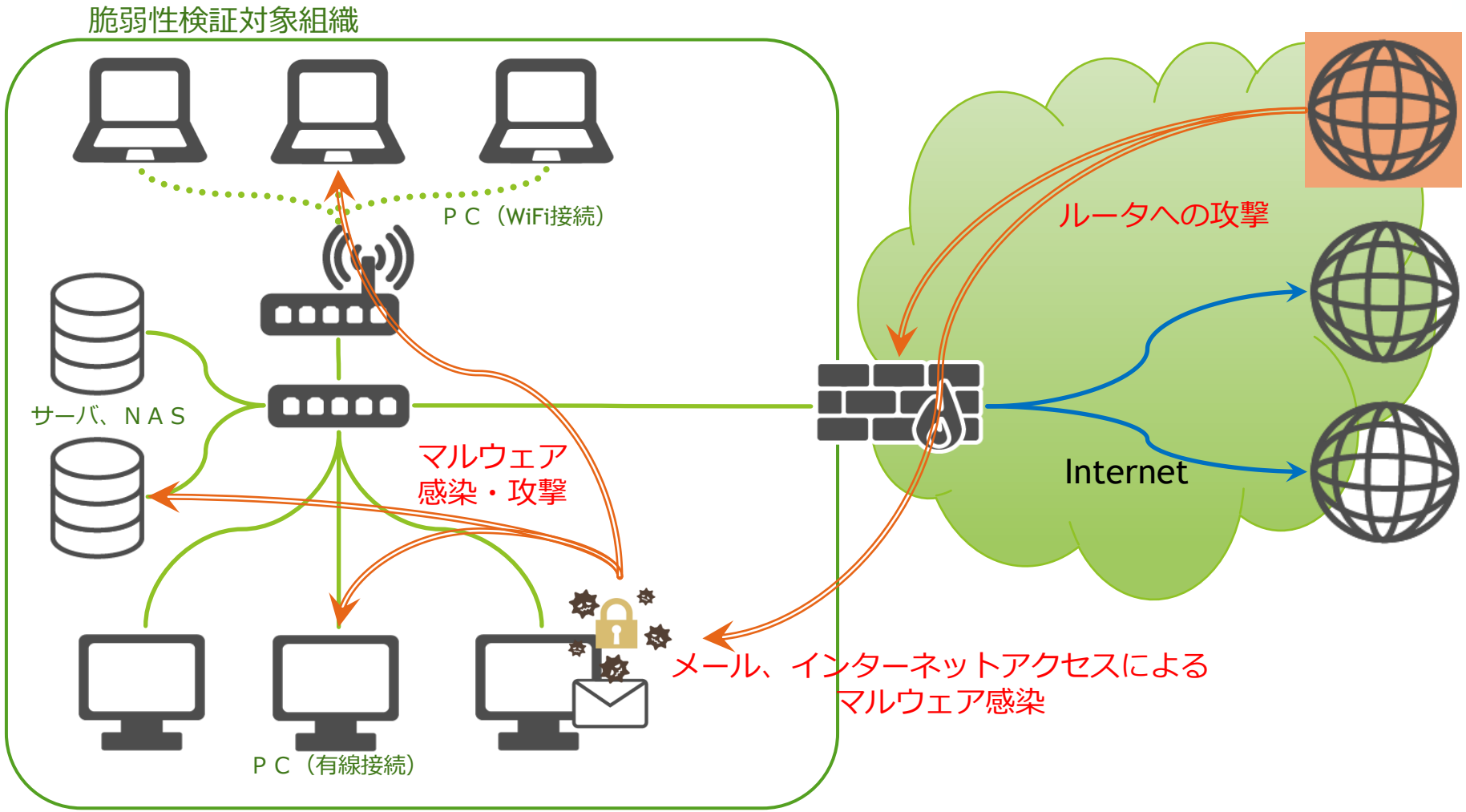
セキュリティ人材の育成

- 定期報告会で社内の人材を育成

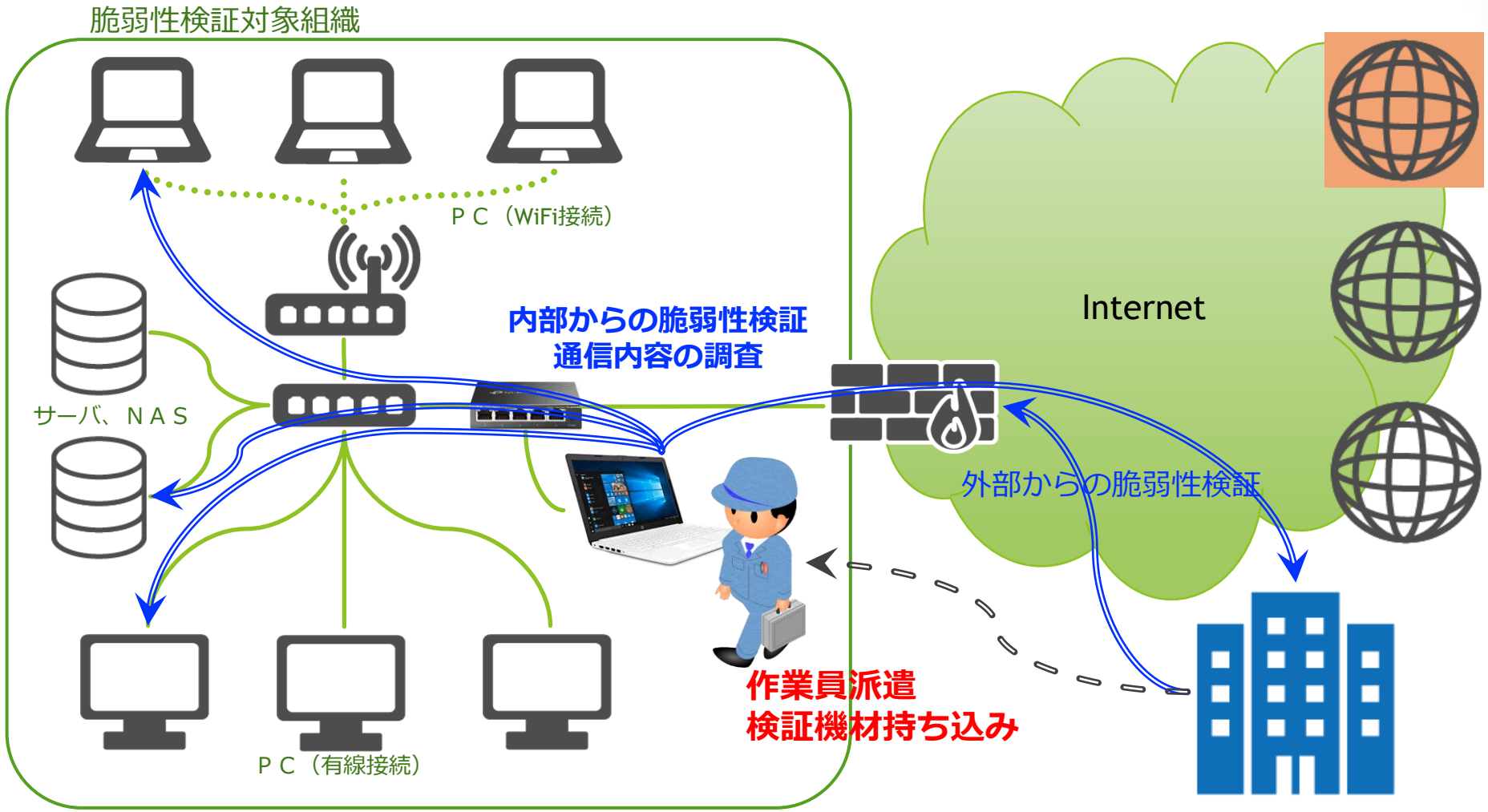
遠隔からの安心サポート

- KATABAMIで安全に遠隔サポート

組織へのサイバー攻撃



一般的な脆弱性診断の方法

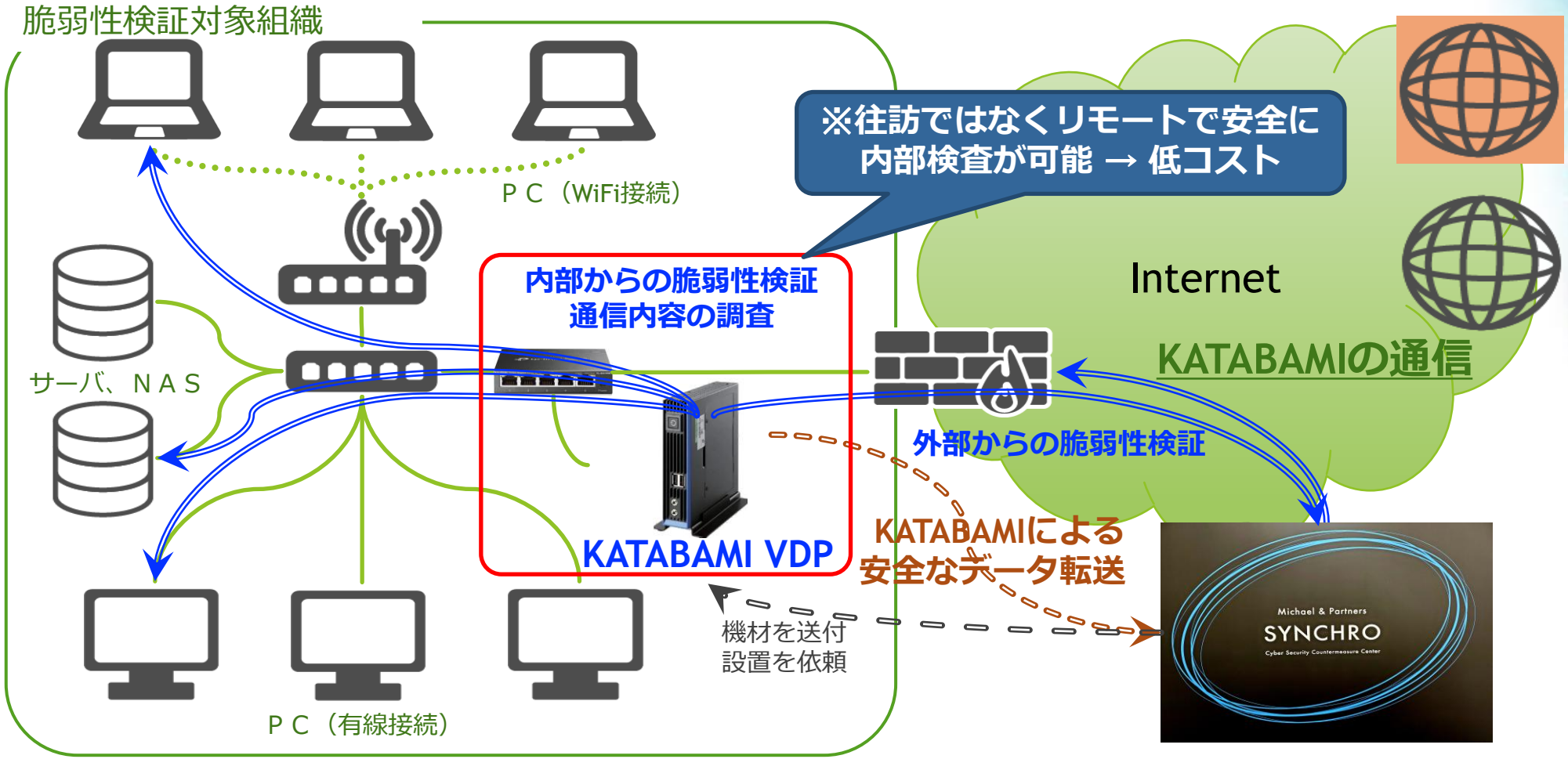


【VDP】 定期的な「脆弱性診断」でリスクを可視化

KATABAMI VDP

リモートからネットワーク内を定期検診　脆弱性を発見し改善策を提示

国際標準（IEC62443、CVSS）に準拠した方法で内部から定期検診



「脆弱性診断（VDP）」での指摘事例（上位7事例）

	脆弱性	対象機種	件数／対象機器	件数／対象組織	比率／対象組織	問題点	影響
1	ユーザ名／パスワードが初期設定のまま	複合機	45(73)	14(14)	100%	該当機器のマニュアルなど公開情報に記載されているユーザ名／パスワードを利用している	該当の機器を踏み台にネットワーク内のリソースにアクセスされるおそれがある
2	脆弱性のあるファームウェアの使用	-	-	9(15)	60%	ルータや複合機等の機器が既知の脆弱性に該当している	既知の脆弱性を悪用されるおそれがある
3	ユーザ名／パスワードが初期設定のまま	ルータ、L3スイッチ、L2スイッチ、AP	16(58)	8(15)	53%	該当機器のマニュアルなど公開情報に記載されているユーザ名／パスワードを利用している	ネットワーク設定や通信ログの改ざんのおそれがある
4	ユーザ制限がされていない、推測しやすいパスワードが使用されている	ファイルサーバ、NAS	11(14)	8(15)	53%	認証なし（または、空ユーザ名／空パスワード）やよく使用されるパスワード（123456やpassword等）で共有フォルダにアクセス可能である	機密情報を窃取やランサムウェア攻撃による被害のおそれがある
5	インターネットからアクセスが可能	-	-	7(15)	47%	ネットワーク内のルータやサーバにインターネットからアクセス可能である	不特定多数からネットワーク内のリソースにアクセスされるおそれがある
6	TELNET が使用されている	ルータ、L3スイッチ	25(35)	6(15)	40%	現在非推奨である TELNET プロトコル（暗号化しない通信方式）を使用している	通信内容から認証情報などの機密情報が窃取されるおそれがある
7	サポートが終了したOSの使用	PC	-	2（直近6社中）	33%	セキュリティアップデートやパッチの提供が行われない	既知の脆弱性を悪用されるおそれがある

ユーザ名／パスワードを乗っ取られるとデータを暗号化される自社被害だけでなく連携先への攻撃など二次被害も助長します。弊社は具体的な対策をご説明する中で人材育成にも寄与します。

「脆弱性診断レポート」の内容（1/8）

本書の構成について

1章　エグゼクティブ・サマリーを記載します

2章　検証の概要を記載します

3章　検証の結果と検出した脆弱性、セキュリティグレードを記載します

4章　検証結果の詳細を記載します

5章　特記事項を記載します

月１回の頻度で対象機器およびネットワークの定期検診を実施。診断レポートは左記の構成で、約200ページ前後のレポートを作成し課題と対策方法を解説します。

「脆弱性診断レポート」の内容（2/8）

#1.　エグゼクティブ・サマリー
#1.1.　エグゼクティブ・サマリー

E

重大な脆弱性があります

**エグゼクティブ・サマリーでは、A～Eの5段階判定結果とリスクの内訳を記載します。
問題内容は3章、内容詳細は4章、推奨対策は別紙に記載します。**

貴社ネットワーク環境に潜在するセキュリティ上の脆弱性を確認することを目的とします。
今回の検証で発見した脆弱性は下記のとおりです。

HIGH 2 件、MEDIUM 1 件、LOW 0 件、INFO 17 件

上記の内、即時対応可能な HIGH の脆弱性は 1 件です。
それぞれの脆弱性の内容は、3 章に記載しております。
今回行った検証内容の詳細は、4 章に記載していますのでご確認ください。
各脆弱性の対策は、別添の「推奨対策リスト」をご確認ください。
検証対象機に対するポートの調査結果は、別添の「ポートスキャン結果」をご確認ください。
報告書内の用語・報告書の解説について、別添の「解説書（仮称）」をご確認ください。

9

「脆弱性診断レポート」の内容（3/8）

1.2. 総合評価の判定基準について

総合評価は下記の表に基づき判定されます。また、検出された問題のリスクレベルは、現実的なシナリオを想定した場合の悪用の可能性に基づいています。

検出された問題とリスクレベルの詳細については、3 章検証結果をご確認ください。
なお、本評価は期間内に検証が完了した項目をもとに行っています。

総合評価	判定基準
A	問題は検出されなかった
B	LOW の問題が 1 件以上検出された
C	MEDIUM の問題が 1 件以上検出された
D	複雑な対応を要する HIGH の問題が 1 件以上検出された
E	即時対応可能な HIGH の問題が 1 件以上検出された

経営層にわかりやすいA～Eの5段階で弊社が判定しますが、根拠はCVSSを活用しています。（詳細は次ページに記載）

「脆弱性診断レポート」の内容（4/8）

脆弱性評価において世界的に活用されているFIRST（Forum of Incident Response and Security Teams）が公開するCVSS（Common Vulnerability Scoring System）の「共通脆弱性評価システム CVSS v3 概説」に基づき、SYNCHROが**5段階で診断**

国際標準（IEC62443、CVSS）に準拠した診断方式であり経済産業省も2025年度から本方式での企業格付けを開始

【5段階での点数評価】

総合評価	判定基準
A	問題は検出されなかった
B	LOW の問題が 1 件以上検出された
C	MEDIUM の問題が 1 件以上検出された
D	複雑な対応を要する HIGH の問題が 1 件以上検出された
E	即時対応可能な HIGH の問題が 1 件以上検出された

【改善プロセスの実践】

- 未改善の場合は対策を再検討
- 改善済ならD判定 → 当社保険加入
- 当月Eランクの課題に対処 → 翌月の定期診断時に結果を確認

【ご参考：CVSSスコア】

リスクレベル	CVSSスコア	概要
重要（HIGH）	7.0～10.0	緊急または重要に該当する問題を確認。早急に対策する必要があると考える。
警告（MEDIUM）	4.0～6.9	警告に該当する問題を確認。対策の実施について検討が必要と考える。
注意（LOW）	1.0～3.9	注意に該当する問題を確認。バージョン更新等のタイミングで対策検討が必要。
INFO	-	問題とはみなされないが、セキュリティ上好ましくない、など懸念点として分類したもの。

「脆弱性診断レポート」の内容（5/8）

3. 検証結果
3.1. 総評

CVSSリスクスコアに基づいた診断結果を表示

1(+1) 件	1 件	0 件	4 件
HIGH	MEDIUM	LOW	INFO

X か月目の検証結果、弊社の判定基準からセキュリティグレードは E（重大な脆弱性があります）と判定します。

今回の検証で前回報告した HIGH の脆弱性 1 件、MEDIUM の脆弱性 1 件、INFO の脆弱性 1 件が解消されたことを確認しました。

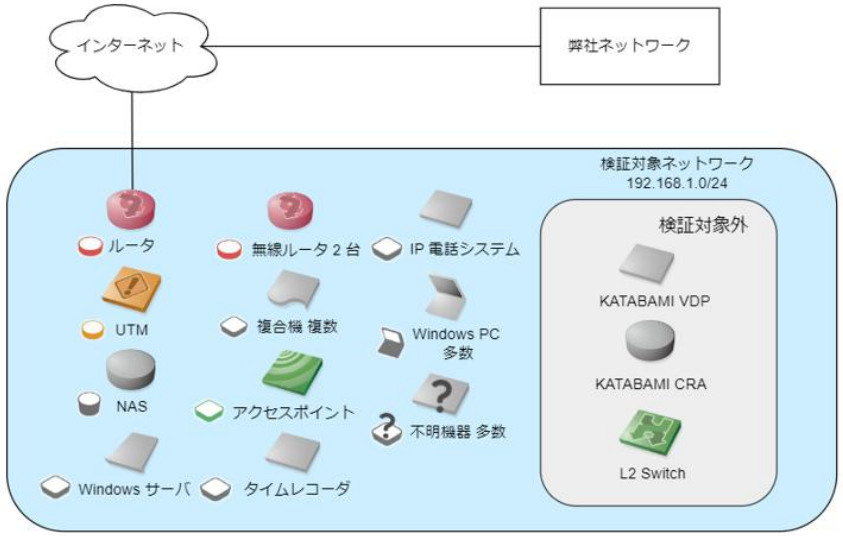
しかし、引き続き HIGH の脆弱性が 2 件確認されています。内の 1 件は即時対応可能な脆弱性のため、別添の「推奨対策リスト」を参考に対策を実施することを推奨します。

リスクレベルの分類について、別紙【説明書 p.11-12】にて詳しい記載があります。ご不明な点がありましたら、併せてご一読お願いいたします。

次項から、検証目標に対する結果を記載します。

「脆弱性診断レポート」の内容（6/8）

ネットワーク構成図



顧客企業様のネットワーク構成図を作成

#3.3. 解消された脆弱性の一覧

先月から解消した脆弱性

今回の検証で解消した脆弱性の一覧を以下に示します。

項番	検証ポイント	脆弱性	リスクレベル
4.2.1.	IMM2	Web 管理画面にログインが可能	HIGH
4.2.2.	RTX1210	TELNET サーバにログインが可能	HIGH
4.2.3.	Windows サーバ	Microsoft RPC に該当する複数の CVE	INFO
		Microsoft Terminal Service に該当する複数の CVE	INFO

詳細は上記の項番からご参照ください。

次項から検出した脆弱性の一覧を記載します。

#3.4. 検証結果の詳細
#3.4.1. 検出脆弱性の一覧

残存する脆弱性

検出した脆弱性の一覧を示します。

赤色部は新たに発見した脆弱性または、報告内容に変化があった脆弱性です。

項番	検証ポイント	脆弱性	リスクレベル
3.4.2.	Windows サーバ	サポートが終了した OS の使用	HIGH※2
3.4.3.	Windows サーバ	SMBv1 が有効（CVE-2017-0143）	HIGH※1
3.4.4.	HDL6-H18	Web サーバステータスの閲覧が可能	MEDIUM
3.4.5.	PR-500MI	Jetty に関する CVE	INFO

次項からそれぞれの脆弱性について記載します。

「脆弱性診断レポート」の内容（7/8）

3.5.2. RTX1200（ルータ）
[Web 管理画面に管理ユーザとしてログインが可能]

8.8 HIGH	攻撃元区分	条件の複雑さ	必要な特権レベル	利用者の関与
	隣接	低	不要	不要
	影響の想定範囲	機密性への影響	完全性への影響	可用性への影響
	変更なし	高	高	高

調査結果と評価基準8項目（CVSS）に基づきリスク評価を行います。

概要

次頁に記載されている機器は Web 管理画面に管理ユーザとしてログインが可能です。

影響

機密情報の漏洩やシステムに関する設定が改ざんされるおそれがあります。

推奨する対策

一般ユーザ、管理者パスワードを変更することを推奨します。詳しい方法は、4 章に記載の対策をご参照ください。

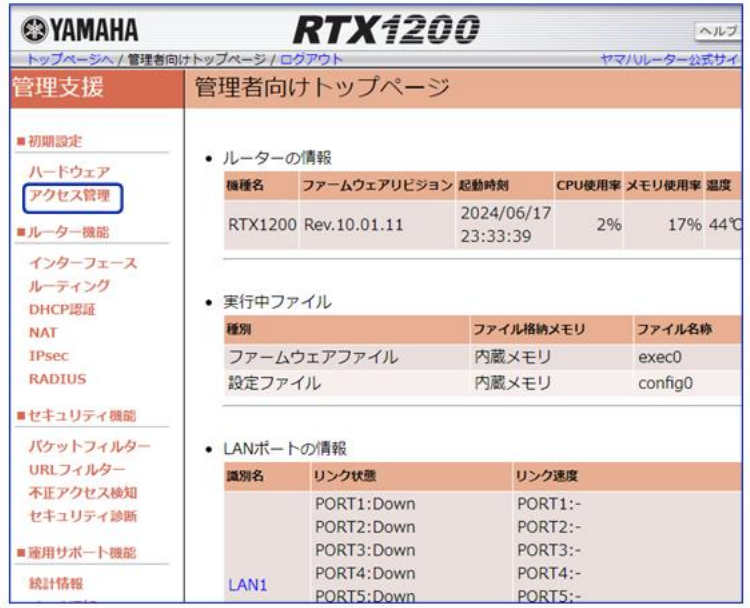
「脆弱性診断レポート」の内容（8/8）

具体的な対策を説明

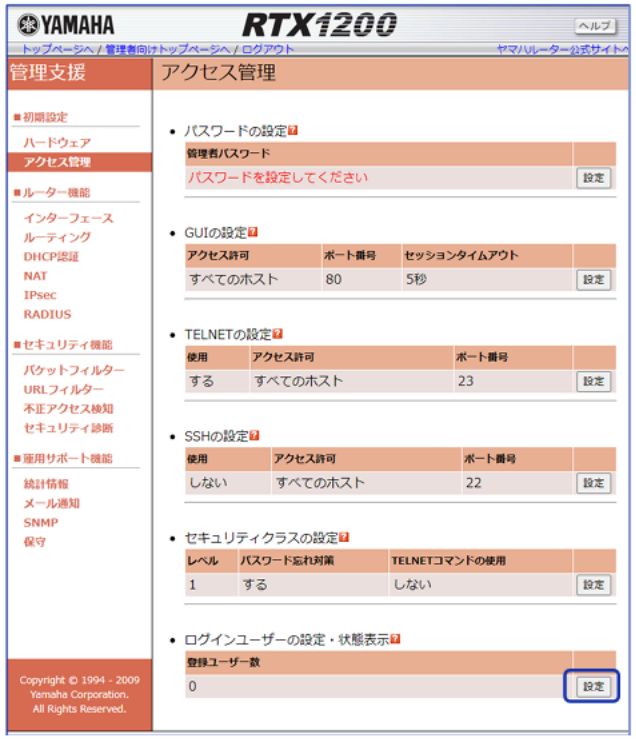
RTX1200ルータのケース

▶一般ユーザのパスワードの設定

① 管理者としてログイン後、「アクセス管理」をクリックします。



② アクセス管理画面から「ログインユーザーの設定・状態表示」の「設定」をクリックします。



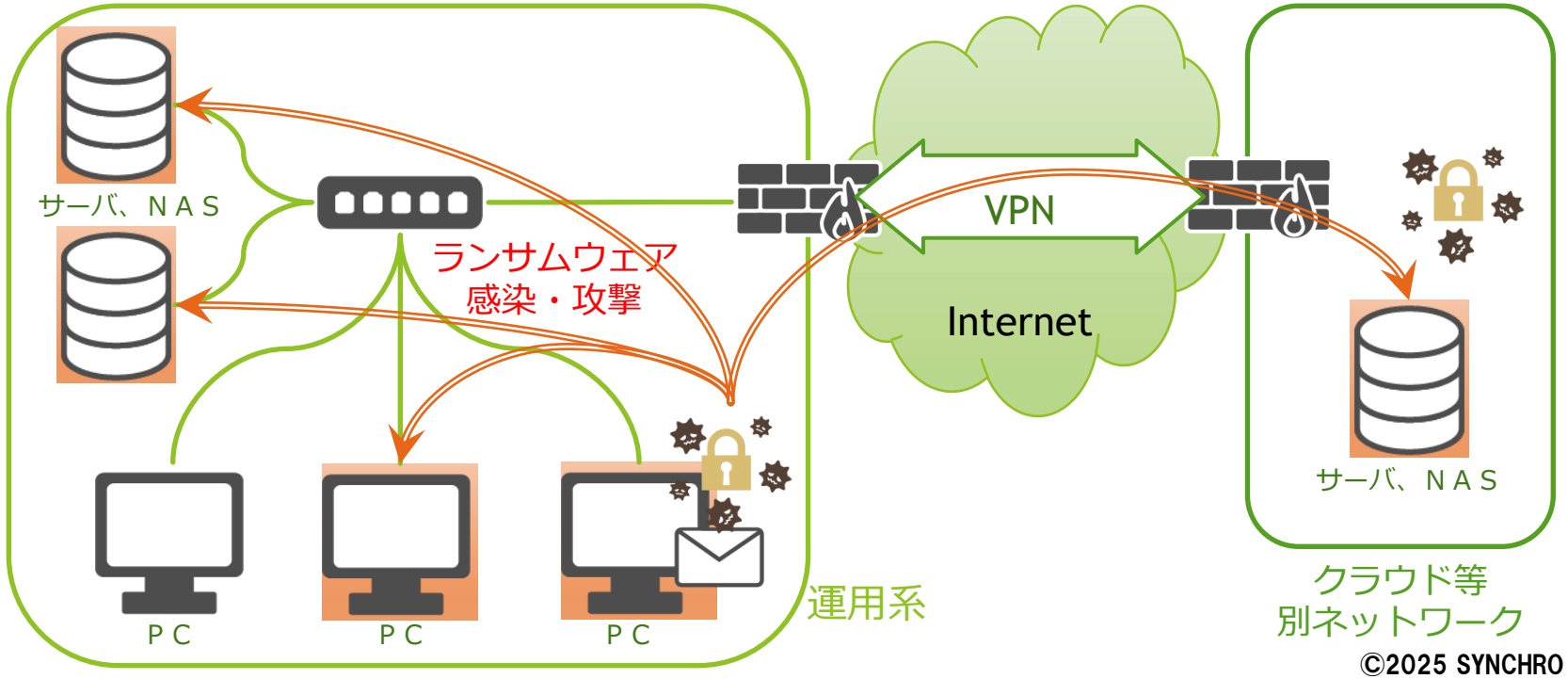
操作方法を詳しく説明

お客様に伴走する体質改善

従来のバックアップ vs ランサムウェア攻撃

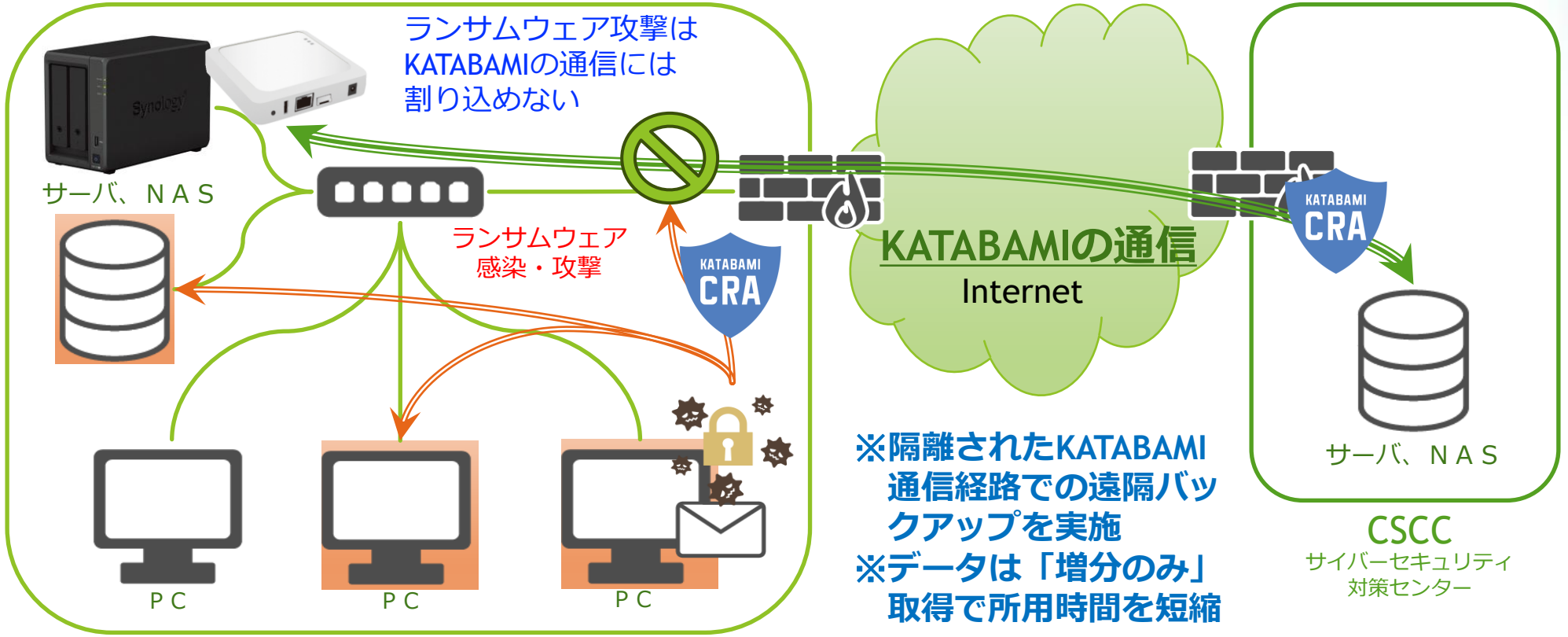
従来のバックアップでは防げない

- ランサムウェア攻撃の対象
  - 感染したPC/サーバ等から、ネットワーク内の NAS/サーバ等を攻撃
  - クラウド等 別ネットワークにバックアップ先を置いても
    ネットワークが繋がっていれば攻撃されてしまう



【CRA】リスクを最小化する「バックアップサービス」

データを「人質」にした「身代金要求」への対策としてのデータ・バックアップ
遠隔地でのバックアップデータまで「ランサムウェア」に攻撃された事例有
対策としては「バックアップ経路の通信も隔離」すること ⇒ KATABAMIの利用



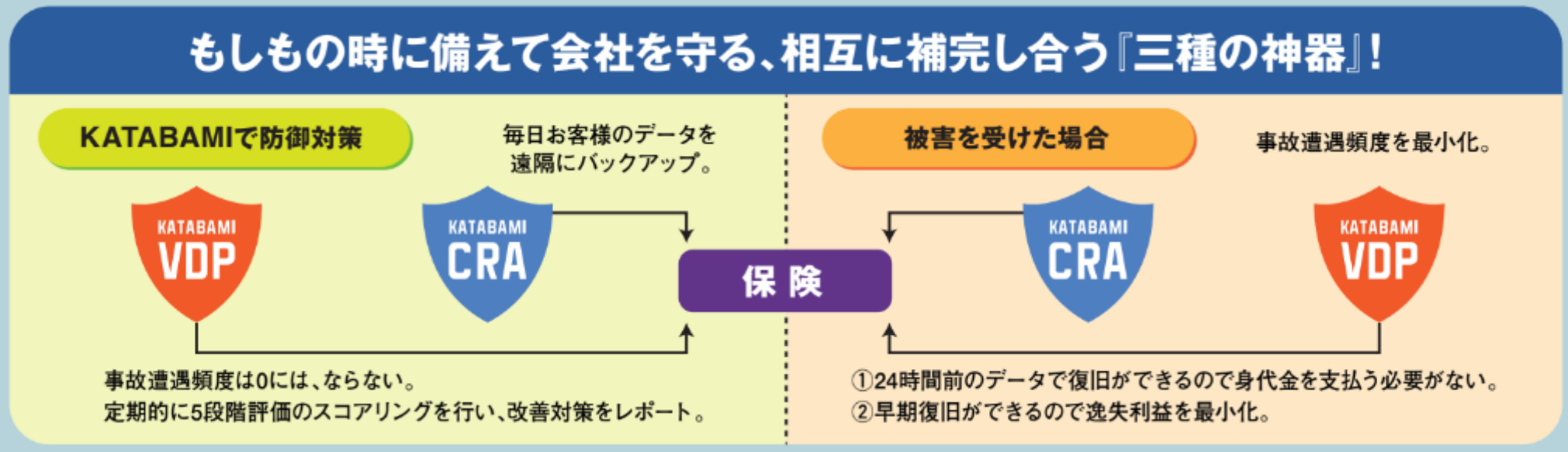
【保険】サイバーセキュリティ保険を自動付帯

保険種類	サイバーセキュリティ保険
支払限度額	賠償損害 1 億円、費用損害 3,000 万円
免責金額	なし
保険期間	「KATABAMI VDP/CRA」の契約期間に準じる（1 年間）
保険金をお支払いする場合	※対象となる損害は次のとおりです。 1.賠償損害 ①損害賠償金 ②争訟費用 ③権利保全行使費用 ④訴訟対応費用 2.費用損害 ①事故対応費用 ②事故原因・被害範囲調査費用 ③広告宣言活動費用 ④法律相談費用 ⑤コンサルティング費用 ⑥見舞金・見舞品購入費用 ⑦クレジット情報モニタリング費用 ⑧公的調査対応費用 ⑨コンピュータシステム等復旧費用 ⑩被害拡大防止費用 ⑪再発防止費用 ⑫サイバー攻撃調査費用

サイバー攻撃対策サービス
KATABAMI VDP/CRAに
あいおいニッセイ同和損保の
サイバーセキュリティ保険を付帯した
「KATABAMI VDP/CRA安心安全
パッケージ1」を
2024年8月8日より提供開始

賠償損害1億円、費用損害3,000万円

【保険】 防御とバックアップと保険の相互補完関係



- 防御は「毎月（年12回）」の定期検診（脆弱性診断）
- データバックアップは「毎日（24時間毎）」に実施
- 保険は事故遭遇時の復旧費用と損害賠償を補償
- しかし、「身代金」と「逸失利益」は保険の補償対象外
- 定期検診とデータバックアップが重要かつ有効な防御策

【価格】 費用対効果に優れた価格帯

1. 脆弱性診断サービス

①定期的な脆弱性診断　～診断を毎月実施し診断レポートを作成～

②安全なKATABAMI通信を利用し遠隔で診断　～外側からだけでなく社内ネットワークの内側も診断～

	提供価格	診断方法	診断結果	アフターフォロー
KATABAMI VDP	900,000円/年 （100ノード単位）	内側からも診断 12回の定期診断	定期検診＆ 毎月改善レポート	免疫力強化 自社での無償の対策を優先
D社	3,000,000円/回	内側からも診断 一回のみ	結果報告は1回のみ	製品やソリューション コンサルティングを販売

2. バックアップサービス

①バックアップを毎日、増分のみ取得　～お客様業務の負担を軽減～

②安全な閉域網であるKATABAMI通信を利用しランサムウェアの侵食を遮断

	提供価格 （初期費用）	提供価格 （年額費用）	バックアップ方法	商品付帯保険
KATABAMI CRA	480,000円 （機器と設定作業費）	360,000円/年 （8TB単位）	閉塞された通信経路経由の イミュータブルバックアップ	費用補償 30百万円 損害賠償　1億円
C社	5,000,000円	2,600,000円/年	同上	費用補償 10百万円

【まとめ】費用対効果に優れたSecure DXサービス

サイバーレジリエンス強化策を強力にご支援します

業界最安値での提供

- 1台月額750円～で毎月定期検診

セキュリティ人材の育成

- 定期報告会で院内の人材を育成

遠隔からの安心サポート

- KATABAMIで安全に遠隔サポート

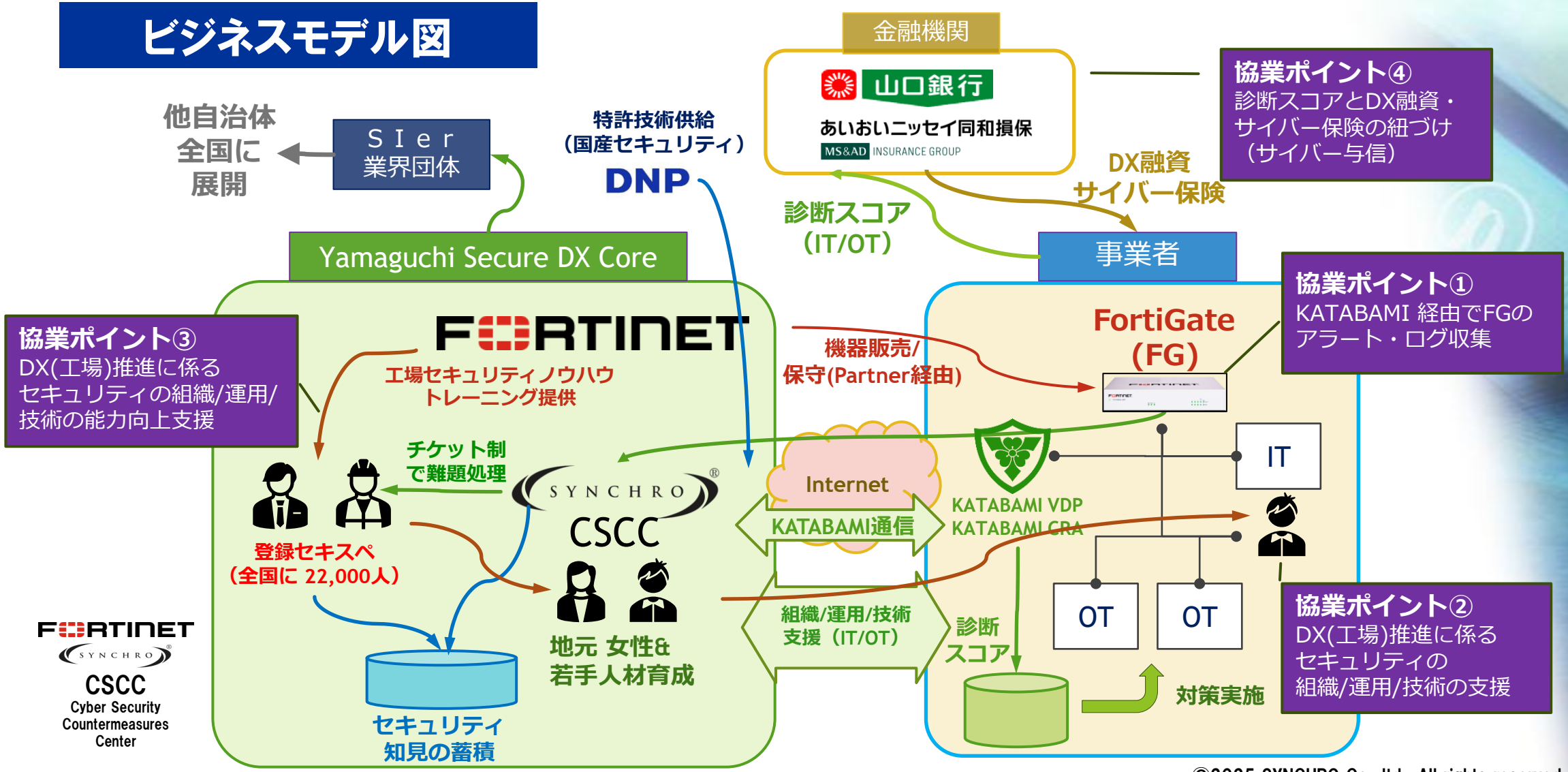
サイバー攻撃への免疫力向上（サイバーレジリエンス強化）の
鍵を備えた国産セキュリティでSecure DXをサポートいたします

4. お客様サポート力向上のための提携促進

Powered by KATABAMI

1. フォーティネットジャパンとの提携～Yamaguchi Secure DX Core～

ビジネスモデル図



1. フォーティネットジャパンとの提携～Yamaguchi Secure DX Core～

Secure DX 推進サービス一覧

2025年8月28日発表

サービス項目		内容	メリット	参考価格
ITシステム脆弱性 診断・分析 サービス	KATABAMI VDP ＋商品付帯保険	・継続的脆弱性診断 ・抗ランサムウェアバックアップ ・サイバーセキュリティ保険	ITセキュリティ リスク低減 （販売中）	KATABAMI VDP **900,000円～/年** （Node数に依存）
	FortiGate 通信健康診断 サービス （KATABAMI経由） **放置されているFortiGateを KATABAMIがリモート・ケア**	・機器運用サポート（**FWアップデート**） ・ユーザ特化のサイバーセキュリティ関連 ニュース配信 <Option> Op1: セキュリティポリシ設定／変更 Op2: 継続的脆弱性診断 Op3: 脆弱性を解消できない機器の隔離	ITセキュリティ リスク低減 ＋ ネットワーク 管理強化 （新規サービス）	**600,000円～/年** （Node数に依存） Op1：要見積もり Op2：→KATABAMI VDP Op3：Node数に応じて 18,000円/年～
セキュア工場DX推進 組織・運用・技術サポートサービス		登録セキスペによるセキュアDX推進支援の **人的サポート** ・経済産業省工場セキュリティガイドライン チェックリストを活用した現状把握 工場セキュリティの組織、運用、技術の 改善活動の支援サポート ・DX人材向けセキュリティ教育プログラム ・セキュアDX相談（よろず相談）	セキュアDX 推進のための 人的サポート （実証済）	工場セキュリティ改善サ ポートサービス **2,000,000円～/拠点** セキュアDX人材教育 **500,000円～/年8回 x 2h** セキュアDX相談 **80,000円～/月1h**

2. CyLeagueと医療機関向けセキュリティサービスを共同開発

医療機関向け「CyLeagueサイバーレジリエンス・パッケージ」を2025年11月より提供開始

～実効性ある体制を実現し、診療継続を守る事前契約型インシデント対応ソリューション～

SYNCHRO® × CyLeague

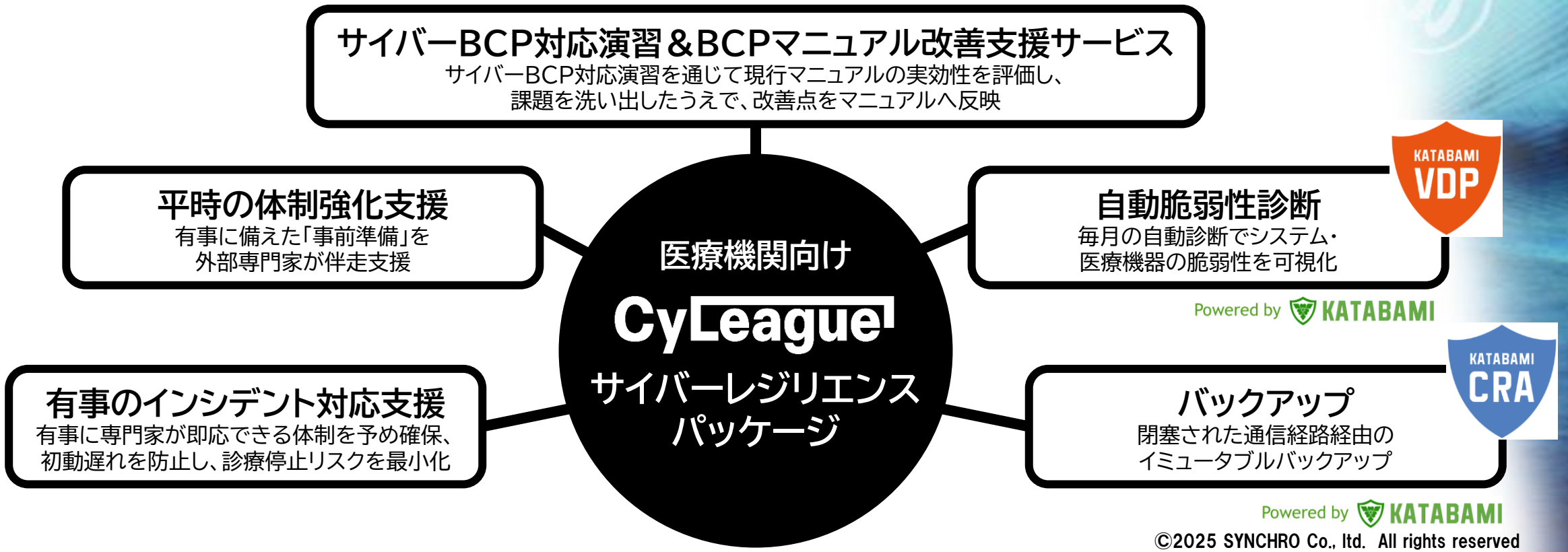
サイリーグホールディングス株式会社について

サイリーグホールディングス株式会社は、株式会社チェンジホールディングスの子会社で、日本の企業や組織のサイバーセキュリティを高めることを使命とする持株会社です。M&A、業務提携、自社サービスの開発を通じて、ITインフラやネットワークの安全性を確保しつつ、事業の成長と発展を支えます。「リーグ（League）」の精神のもと、グループ企業やパートナーと切磋琢磨し、日本のサイバーセキュリティ業界を牽引します。セキュリティ人材育成にも注力し、企業が抱えるサイバー脅威に迅速に対応できる体制を構築。デジタル社会の安心・安全に貢献する総合的なサイバーセキュリティ企業を目指します。

2. 医療機関向けCyLeagueサイバーレジリエンス・パッケージ

「形式的な整備」から「診療を継続できる体制」へ

サイバーBCP対応演習、マニュアル評価・改訂、自動脆弱性診断、バックアップ、有事対応までを網羅した、
医療機関向けのワンストップソリューション「CyLeague サイバーレジリエンス・パッケージ」。
ガイドライン準拠を押さえつつ、現場で本当に機能する体制を構築します。



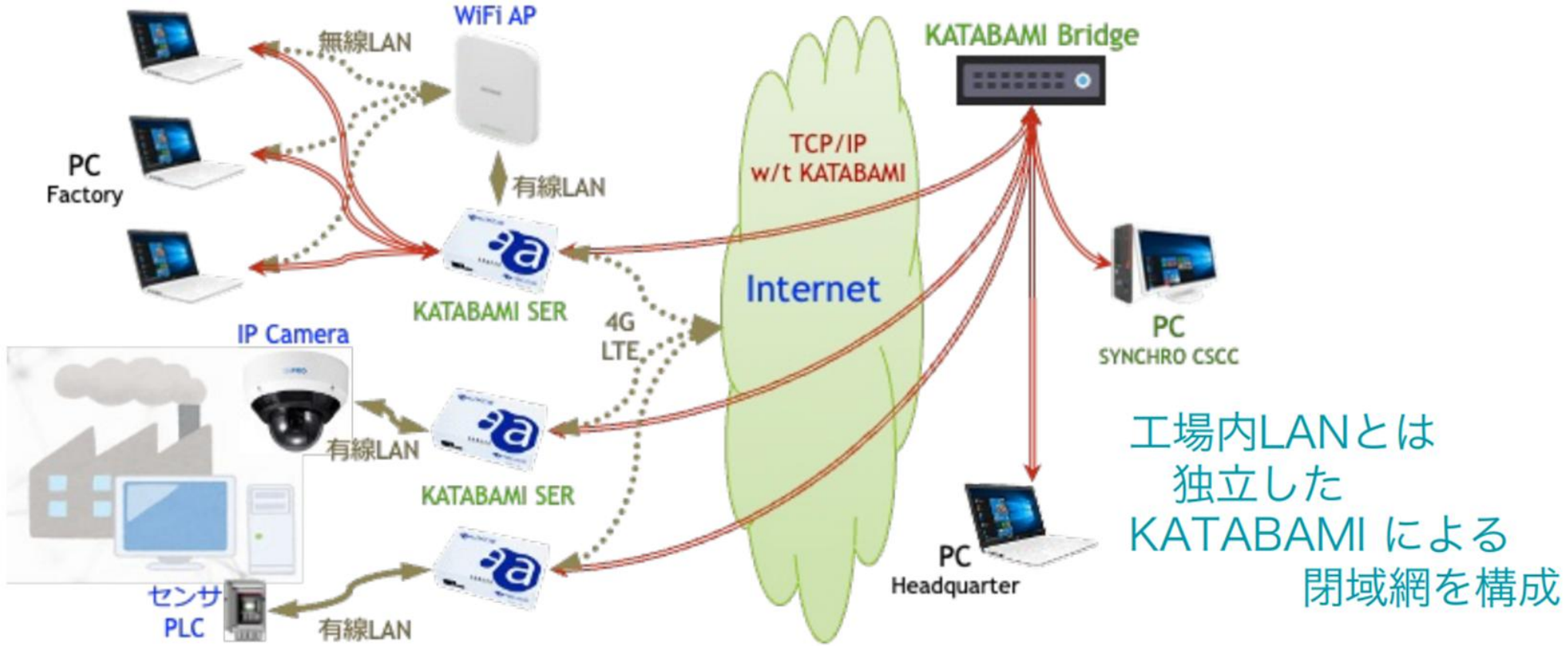
5. KATABAMI導入事例（応用編）

Powered by KATABAMI

お客様導入事例①：工場DXへのKATABAMI適用

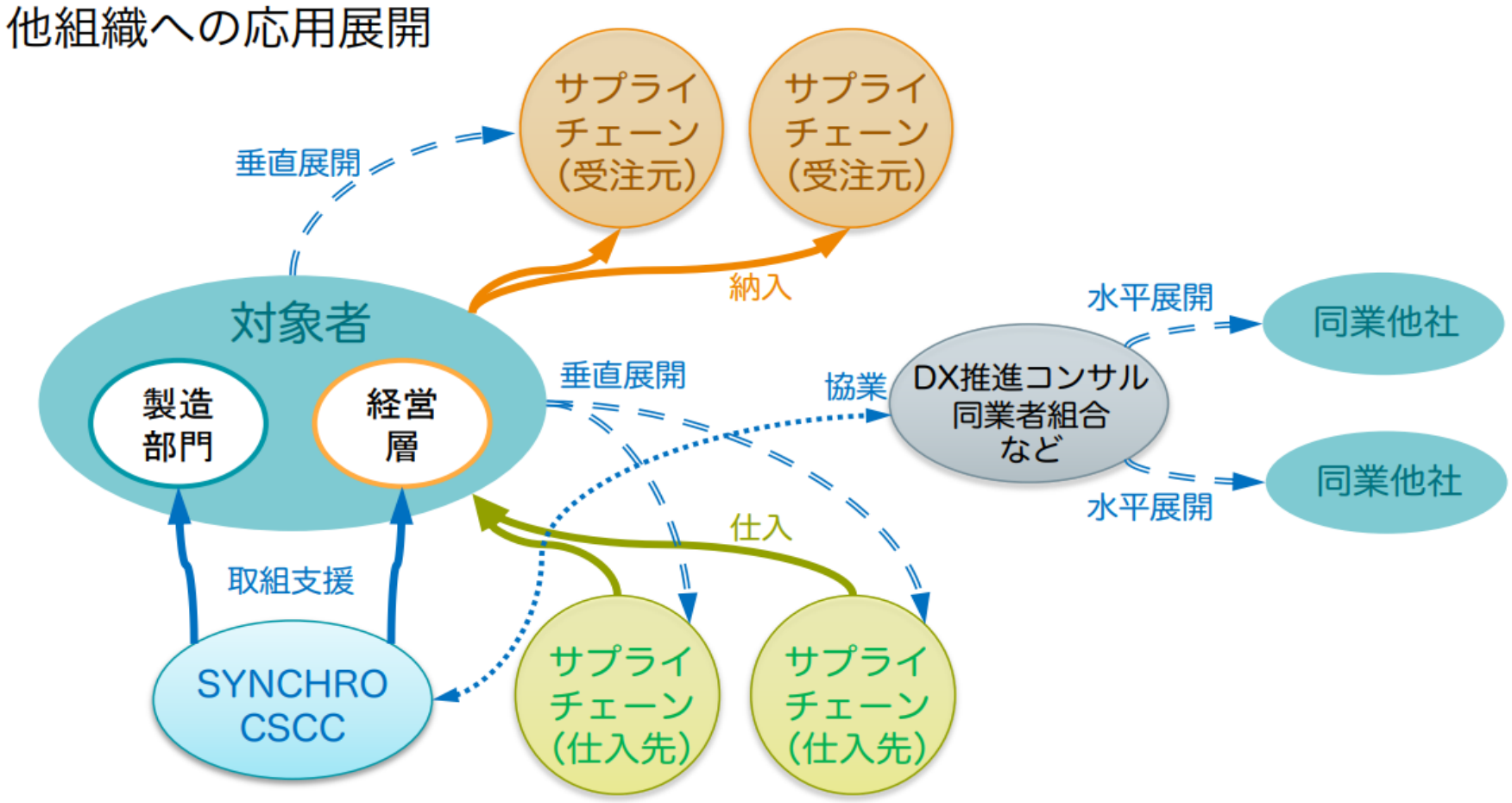
流体継手メーカでの取り組み

KATABAMI SER を利用した監視カメラシステム



5

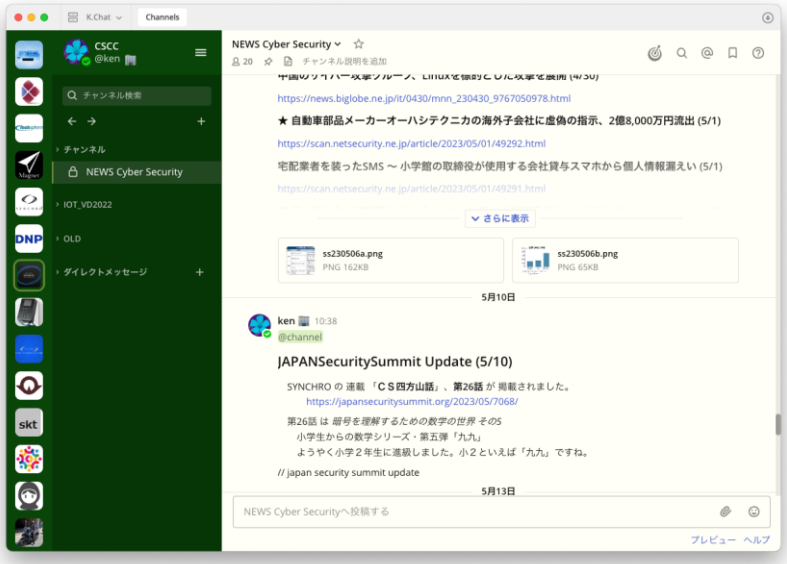
お客様導入事例②：TPRMへのKATABAMI活用（準備中）

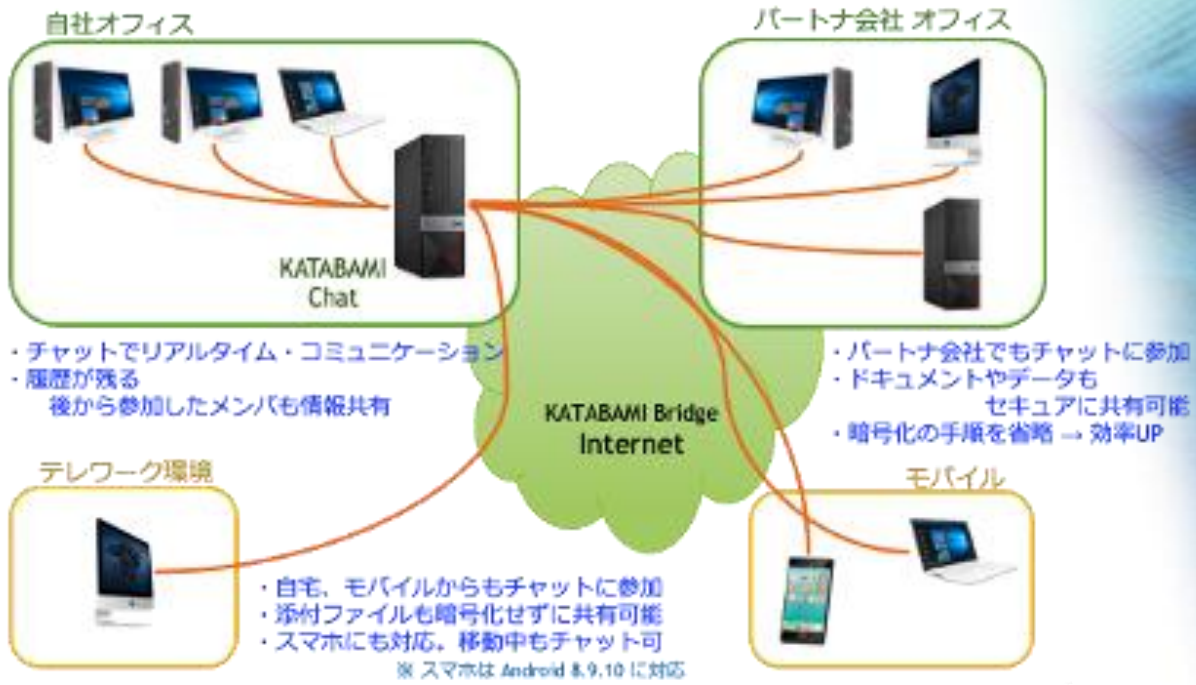


お客様導入事例③:KATABAMI Chatとしての利用

KATABAMI化できない 装置 や アプリケーション を KATABAMI化
Slack クローンと呼ばれる Mattermost の通信をKATABAMI化

- Slack clone と呼ばれる Mattermost がベース
  - オープンソースなのでライセンスフリー
- サテライト、パートナ企業との連携も可能
  - KATABAMI Bridgeで Internet経由で接続
- セキュリティは powered by KATABAMI で万全
  - なりすまし、中間者攻撃は完全に排除　・Internet経由でも安心接続
  - 添付ファイルもKATABAMIと自社サーバでガード
- カスタマイズ
  - カスタマイズ機能の他、OSS故に改修も可能





お客様導入事例④:KATABAMI VDP dawn

- **管理しきれていない内部ネットワークのリモート調査**
- **対象ネットワーク上の機器の洗い出し**
  - どんな機器が存在するか（ by arp-acan, nmap ）
  - どんなサービスが提供されているか（ nmap ）

IP アドレス	MAC アドレス	ベンダ名	詳細
192.168.150.	ac:44:f2	YAMAHA CORPORATION	詳細へ →
192.168.150.1	f8:b1:56	Dell Inc.	詳細へ →
192.168.150.	d8:9e:f3	Dell Inc.	詳細へ →
192.168.150.3	ce:fe:a4	プライベート MAC アドレス	詳細へ →
192.168.150.	00:16:3e:	Xensource, Inc.	詳細へ →
192.168.150.5	00:16:3e:	Xensource, Inc.	詳細へ →
192.168.150.1	00:e0:4c:	REALTEK SEMICONDUCTOR CORP.	詳細へ →
192.168.150.113	a4:77:f3	Apple, Inc.	詳細へ →
192.168.150.	00:1f:f2:	VIA Technologies, Inc.	詳細へ →
192.168.150.1	ec:79:49	FUJITSU LIMITED	詳細へ →
192.168.150.1	28:00:af	Dell Inc.	詳細へ →
192.168.150.	7c:c2:c6:	TP-Link Systems Inc	詳細へ →
192.168.150.1	e0:51:d8:	China Dragon Technology Limited	詳細へ →
192.168.150.1	00:16:3e:	Xensource, Inc.	詳細へ →
192.168.150.1	e8:1b:4b	amnimo Inc.	詳細へ →
192.168.150.2	18:66:da:	Dell Inc.	詳細へ →
192.168.150.2	14:b3:1f:	Dell Inc.	詳細へ →
192.168.150.2	00:04:5f	Avalue Technology, Inc.	詳細へ →
192.168.150.2	34:73:5a	Dell Inc.	詳細へ →
192.168.150.2	c4:36:c0	BUFFALO.INC	詳細へ →
192.168.150.2	00:04:5f	Avalue Technology, Inc.	詳細へ →
192.168.150.2	00:04:5f	Avalue Technology, Inc.	詳細へ →
192.168.150.2	68:45:f1	TOSHIBA CLIENT SOLUTIONS CO., LTD.	詳細へ →
192.168.150.21	94:83:c4	GL Technologies (Hong Kong) Limited	詳細へ →
192.168.150.2	00:16:3e	Xensource, Inc.	詳細へ →
192.168.150.2	ec:f4:bb:	Dell Inc.	詳細へ →
192.168.150.2	00:16:3e:	Xensource, Inc.	詳細へ →
192.168.150.2	d4:2c:46:	BUFFALO.INC	詳細へ →

192.168.150.113		機器一覧に戻る →
ポート／プロトコル	ステータス	サービス
22/tcp	open	ssh
88/tcp	open	kerberos
445/tcp	open	microsoft-ds
5000/tcp	open	unknown
5900/tcp	open	unknown
7000/tcp	open	unknown
49183/tcp	open	unknown

お客様導入事例⑤:FortiGate 通信健康診断サービス

- **FortiGateを放置させないリモート健康診断サービス**

Service Menu

Basic Plan

- Basic Plan ［ FortiGATE + KATABAMI VDP dawn ］
  - ご利用状況把握、保守期限到来通知
  - 新FWリリース通知 → 遠隔での FG FW update 実行
  - 接続機器の洗い出し by KATABAMI VDP dawn
  - ユーザに特化したサイバーセキュリティ関連ニュース配信
- Option service
  - 遠隔での FG Security Policy 設定/変更
  - 脆弱性診断（内部検査）［+ KATABAMI VDP ］
  - 脆弱性を解消できない機器の隔離 ［+ KATABAMI Isolator ］

FortiGate
(FG)

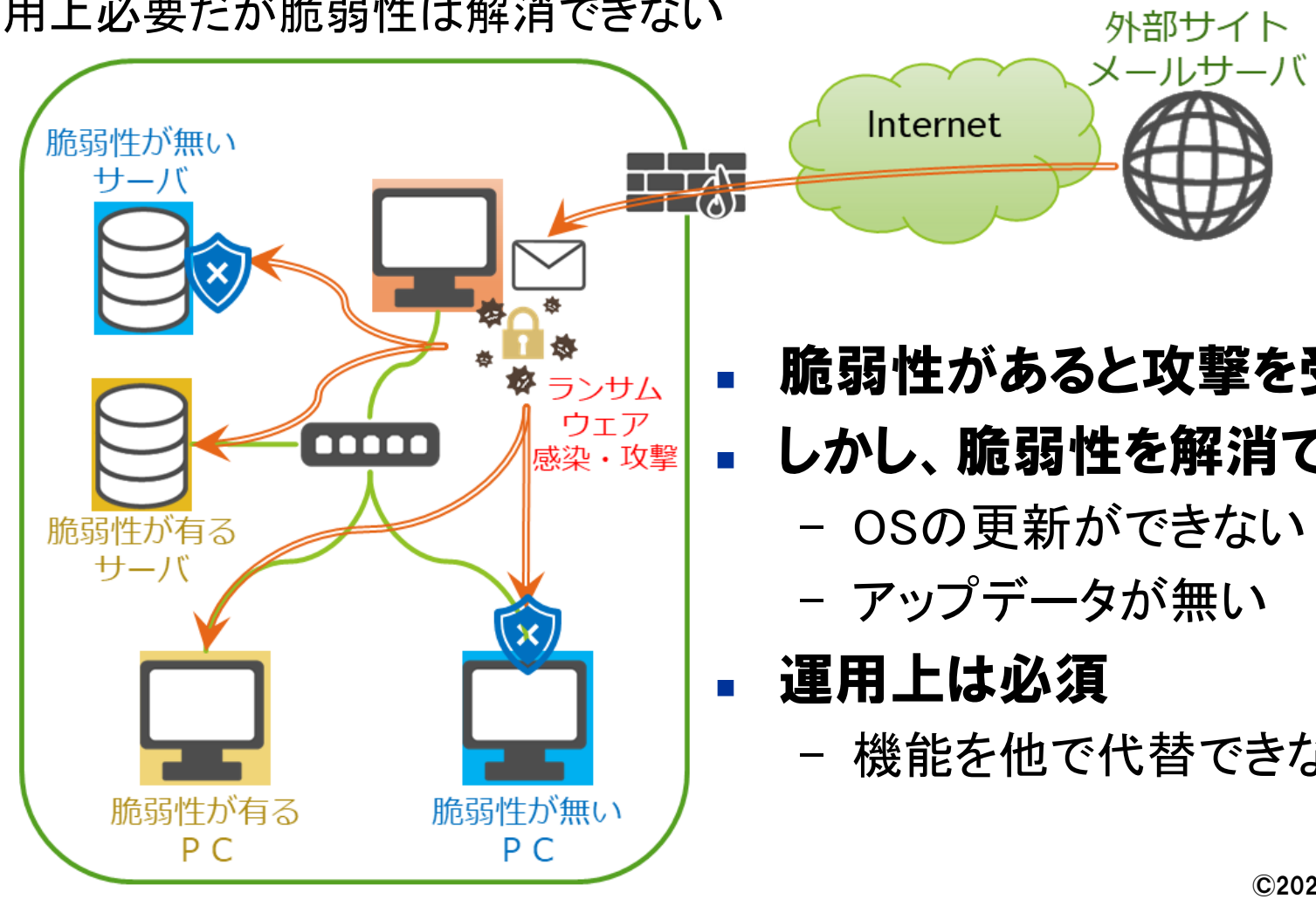
KATABAMI VDP
dawn

SYNCHRO CSCC

FORTINET SYNCHRO CSCC
Cyber Security
Countermeasures
Center

お客様導入事例⑥:KATABAMI Isolator

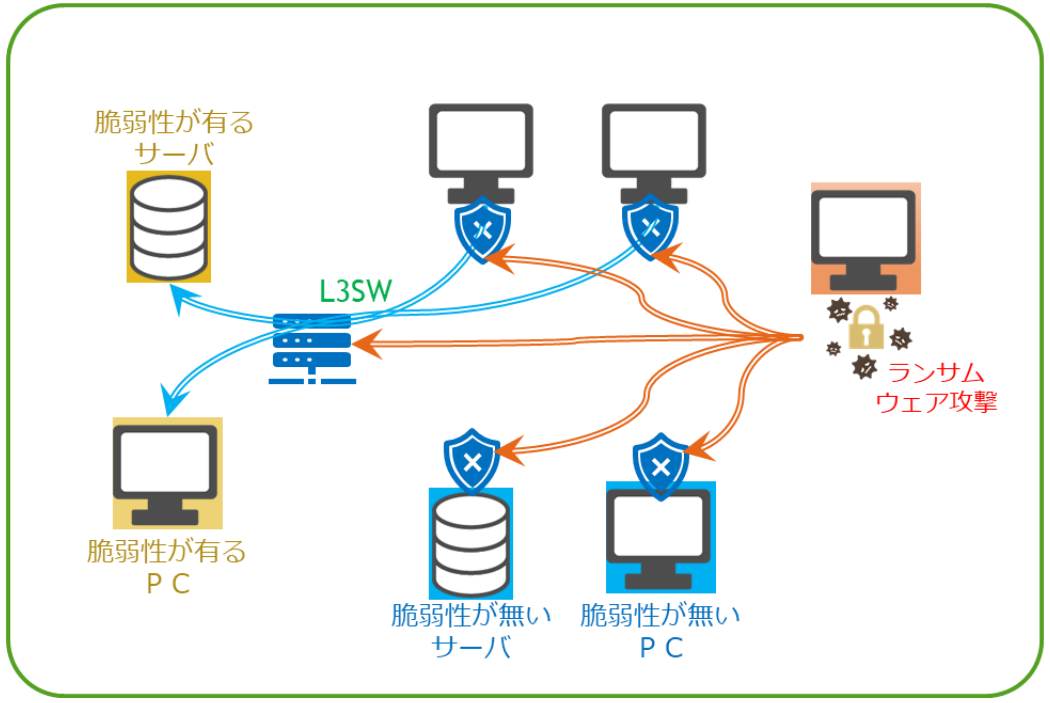
- **脆弱性が解消できないnode**
  - 運用上必要だが脆弱性は解消できない



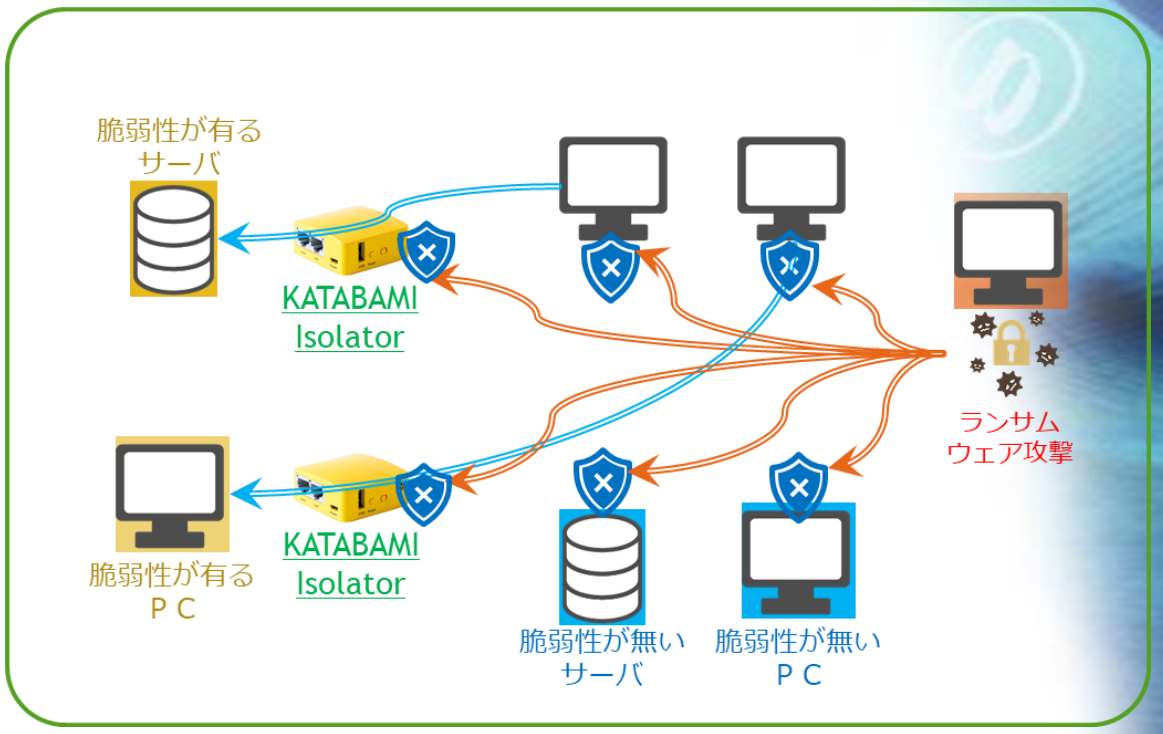
- **脆弱性があると攻撃を受けやすい**
- **しかし、脆弱性を解消できない**
  - OSの更新ができない
  - アップデータが無い
- **運用上は必須**
  - 機能を他で代替できない

お客様導入事例⑥:KATABAMI Isolator

- **一般的な対策方法**
  - セグメントを分けて、L3 S/W でアクセス制御



- **KATABAMI Isolator を用いた対策方法**
  - 個々の node 毎に K.Isolator を配置



ご静聴ありがとうございました

～ご説明動画（YouTube）はこちらからご覧いただけます～

＜お問合せ窓口＞
株式会社SYNCHRO　北口順治（CMO）
EMAIL：katabami@udc-synchro.co.jp
電話番号：03-4570-3291