For Business
secured by KATABAMI

2022年1月（初版）
2022年1月（0.2版）

株式会社SYNCHRO　中村 健

SYNCHRO

Company Profile

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

	山口サテライト本社
住所	山口県湯田温泉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 事業内容

① 物理セキュリティ（Physical Security）

手の甲静脈認証装置（開発、製造、販売、システム構築）

顔認証装置（販売、システム構築）

② ネットワークセキュリティ（Cyber Security）

KATABAMIシリーズ（開発、製造、販売、システム構築）

ネットワークセキュリティ・コンサルティング／教育

③ 受託開発事例

大手新聞社向け 一斉同報システム（全国約60箇所への同報）

基本設計、詳細設計、製造、試験（BCP対策を含む）

原子力関連システム 拡声システム／連絡通報システム

基本設計、詳細設計、製造、試験（セキュリティ対策を含む）

④ 主要取引先

(株)アート、(株)アイネット、エス・アンド・アイ(株)、NECエンジニアリング(株)、NECフィールディング(株)、(株)NTTファシリティーズ、(株)クマヒラ、大成建設（株）、高千穂交易(株)、テクノホライゾングループ、東芝テックソリューションサービス(株)、パナソニックシステムソリューションズジャパン(株)、日鉄テックスエンジ(株)、日本フィールドエンジニアリング(株)、(株)日本ロックサービス、(株)ネットワークス、日比谷総合設備（株）、美和ロック(株)、(株)ロックシステム

KATABAMI Series

Zero Trust Network Access

ITセキュリティの作り方

セキュリティを確保するための４要素

通信上の安全性
Link Security

通信相手の正当性
Node Certify

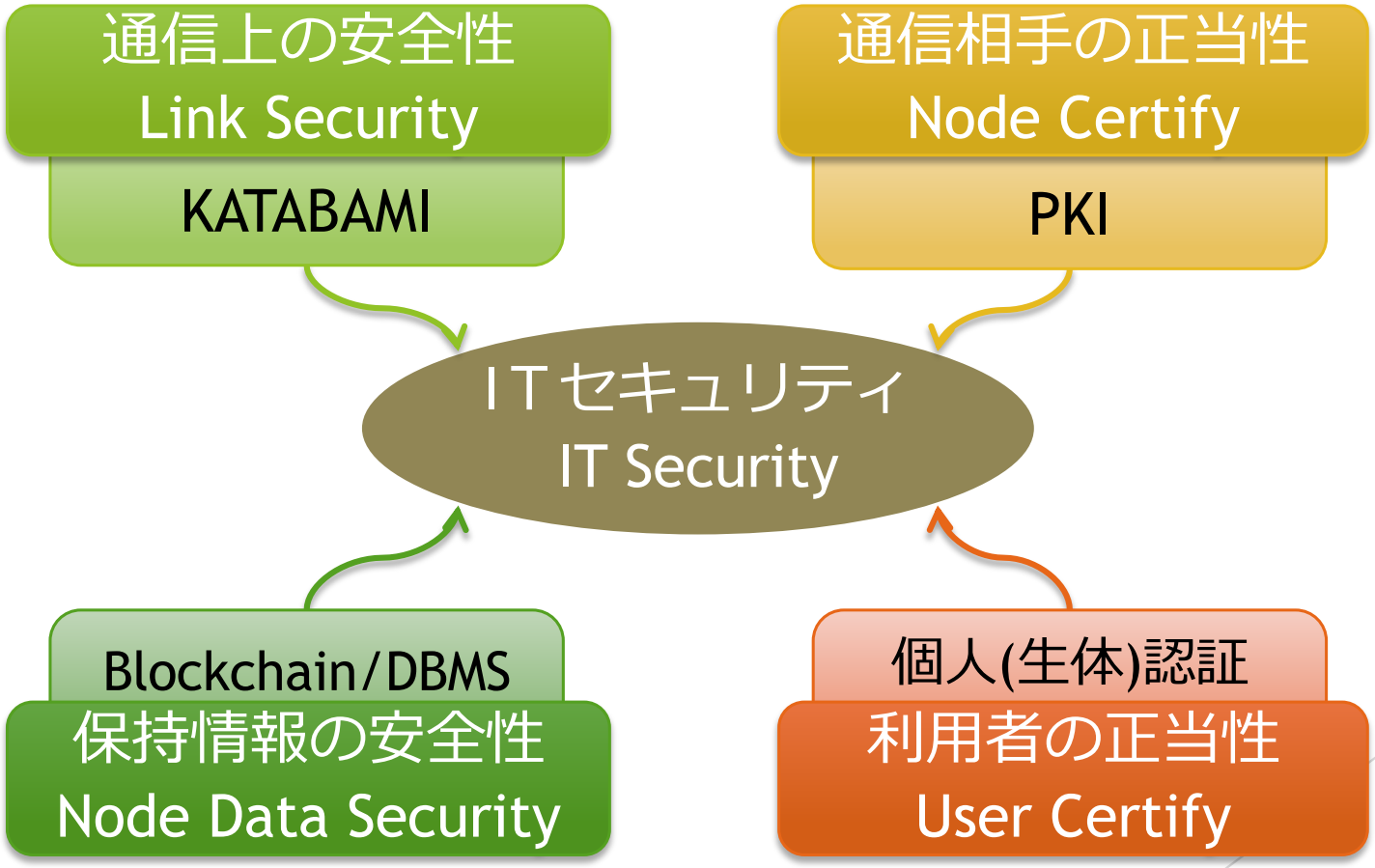
保持情報の安全性
Node Data Security

利用者の正当性
User Certify

SYNCHRO®

ITセキュリティの作り方

４要素 を 構成する要素技術



Zero Trust Security

End Point間の通信の安全性 の 保証 = zero trust

- Zero Trust Security とは
  - 2019年辺りから 流行りだした。M社、C社 の propaganda が火付け役？
  - 2010年に Forrester Research社 が提唱した考え方
  - 決して信頼せず、常に確認する
    - 誰も & 何も、無条件には信用しない という考え方（少し切ない..？）
    - 全てアクセス要求は、認証、承認、暗号化が行われてから許可
  - どこでも 安心 しない
    - オープンな Internet 区間だけでなく、LAN 内でも警戒を怠らない
    - ファイアーウォールで守られていても、その内側に悪者がいるかも知れない
  - デメリットは 利便性の阻害 （そこで、KATABAMI の出番 というストーリ展開）
- Zero Trust Security ⇒ KATABAMI (“Zero Trust Security “ implies “KATABAMI”)
  - KATABAMI は ネットワーク層で Zero Trust Security の要件を充足
    - ペア鍵による認証（認証）
    - 接続相手の IPv6 address の正当性の確認（承認）
    - 楕円曲線暗号、ストリーム暗号の適用（暗号化）
  - さらに、アプリケーション層での認証や権限管理を行う

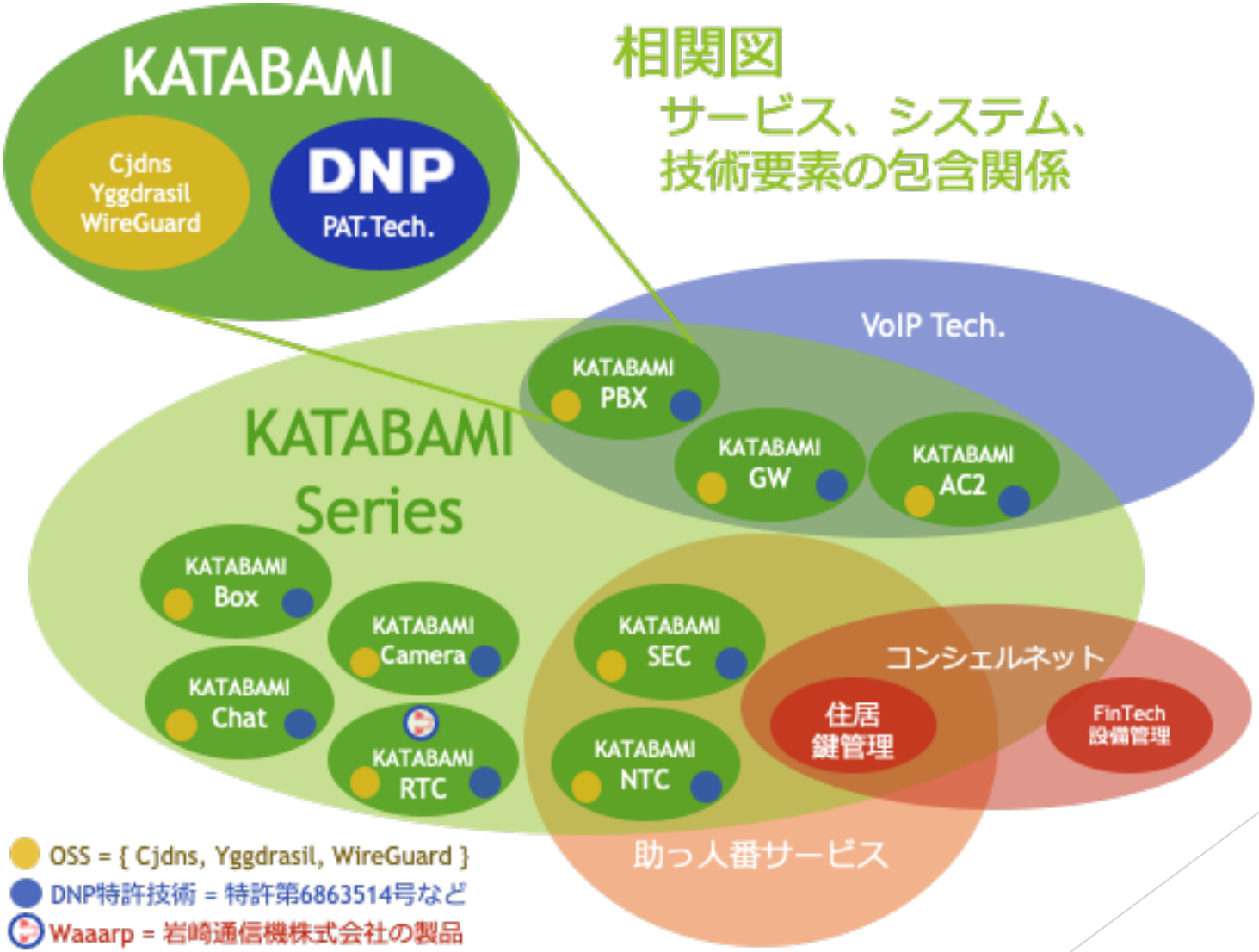
SYNCHRO®

IoTセキュリティ規格への準拠
セキュアIoTプラットフォーム協議会の セキュリティ基準に適合

- 評価の方法
  - 一般社団法人セキュアIoTプラットフォーム協議会（SIoTP）が、国際標準規格である IEC62443 をベースに、実装レベルのセキュリティ仕様をまとめた「IoTセキュリティ仕様書 Ver1.0」(2020年11月にSIOTP協議会より発行)に基づき「SIOTP協議会セキュリティチェックシート」を策定し、評価検証を実施
- 評価の結果
  - 「IoTデバイスの真正性の確保と識別」、「設計・製造から廃棄にいたるプロダクトライフサイクル管理」、「適切なファームウェアアップデート」などIoTシステムに求められるセキュリティ対策が適正に実装され、さらに安全に運用を支援するため管理体制の整備や各種書類の文書化などセキュリティマネージメント観点においても適切に実行されていることを、そのエビデンスを含めて確認

※ 2021年7月21日に SIoTPからプレスリリースが発行されています

DNP社特許技術の適用 → セキュリティ性能強化



Secure Business Environment

For Teleworking

KATABAMI が作る テレワーク環境

ファイル共有も内線通話もいままで通り 機器も使い回し

・チャットでリアルタイム・コミュニケーション
・履歴が残る
　後から参加したメンバも情報共有

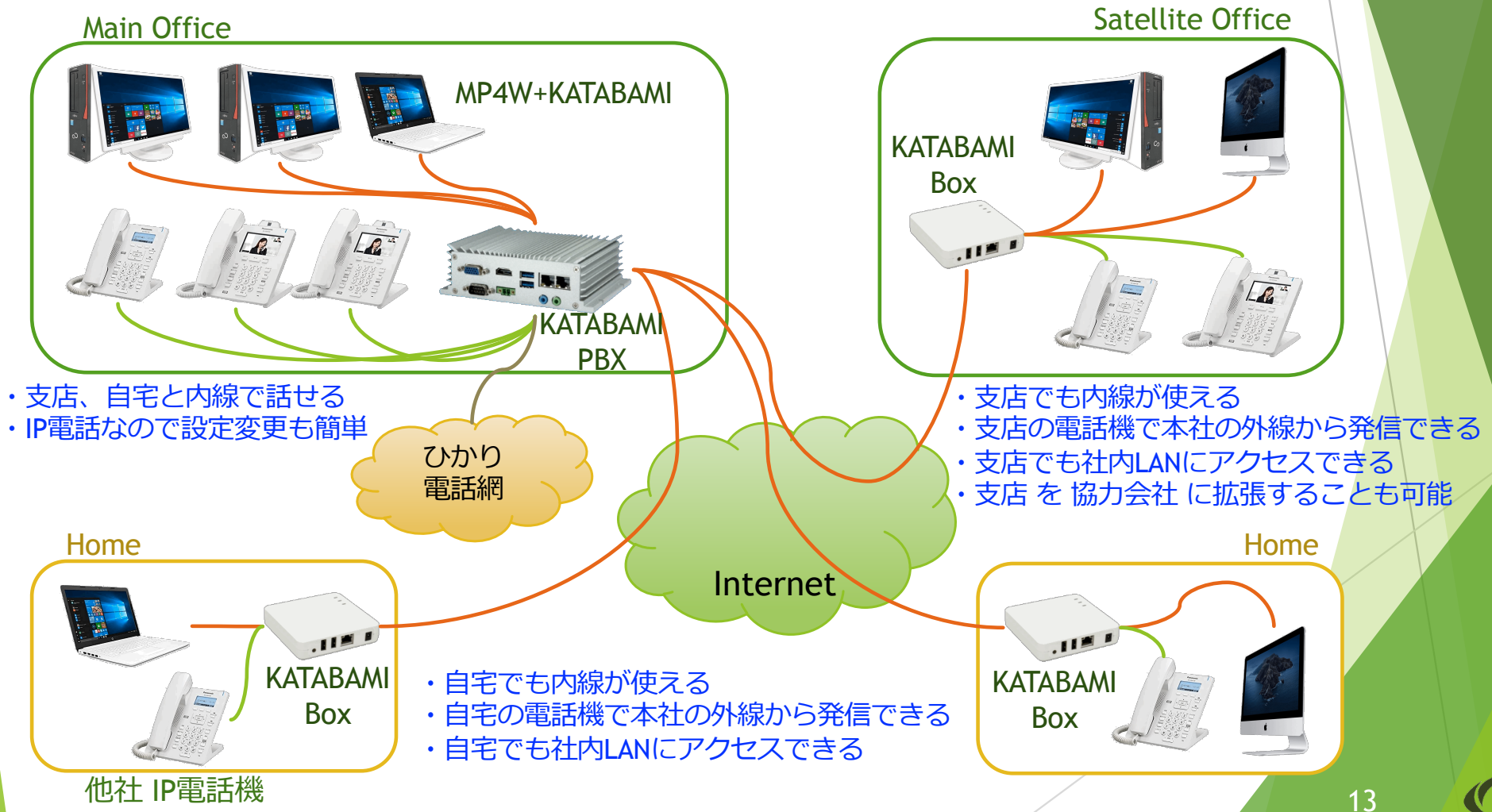
・パートナ会社でもチャットに参加
・ドキュメントやデータも
　セキュアに共有可能
・暗号化の手順を省略 → 効率UP

・自宅、モバイルからもチャットに参加
・添付ファイルも暗号化せずに共有可能
・自宅、モバイルからもＮＡＳにアクセス
・スマホにも対応。移動中もチャット可

※ スマホは Android 8.9.10 に対応

KATABAMI PBX & Box 適用例

KATABAMI で 広域内線システム 構築

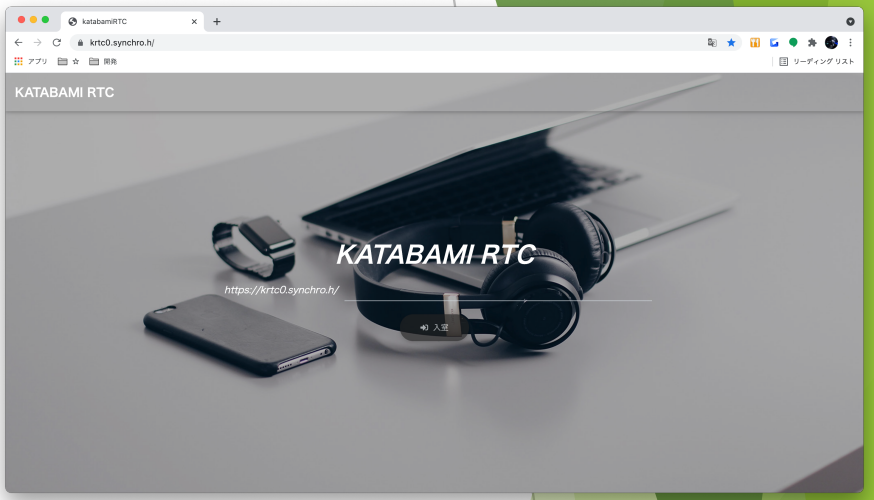


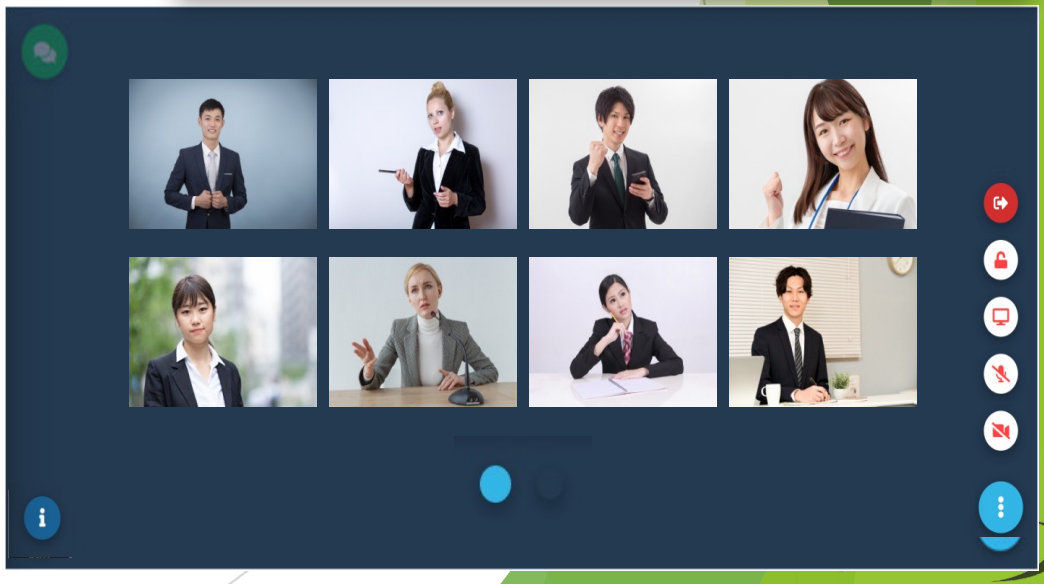
・支店、自宅と内線で話せる
・IP電話なので設定変更も簡単

・支店でも内線が使える
・支店の電話機で本社の外線から発信できる
・支店でも社内LANにアクセスできる
・支店 を 協力会社 に拡張することも可能

・自宅でも内線が使える
・自宅の電話機で本社の外線から発信できる
・自宅でも社内LANにアクセスできる

KATABAMI RTC
ブラウザのみの簡単Web会議、セキュアで高音質





- KATABAMI RTC の 特徴
  - 高いセキュリティ
    - 自社サーバ で 運用可能
      - 機密情報を社外に出さない
    - サーバと通信は KATABAMI で 完全防御
  - 使い易さ
    - ブラウザのみで動作する手軽さ
  - 高音質
    - 最新の CODEC = Opus を採用
  - 幅広い動作環境 (Chrome base)
    - Windows10/11, MacOS
    - Android, iOS, Debian, Raspberry Pi OS
    - Ubuntu, RHEL/CentOS

KATABAMI Chat

Slack clone を使って 協働の効率向上 を図る

- KATABAMI Chat の 特徴
  - 高いセキュリティ
    - 自社サーバ で 運用可能
      - 機密情報を社外に出さない
    - サーバと通信は KATABAMI で 完全防御
  - 使い易さ
    - 機能、操作性は Slack と同様
      - ∵ Slack clone (OSS) が base
    - 社外（パートナ）との連携も可能
  - クライアント動作環境 (Chrome base)
    - Windows10/11, MacOS
    - Android, iOS, Debian, Raspberry Pi OS
    - Ubuntu, RHEL/CentOS

Slack vs KATABAMI Chat
比較

項目	Slack	KATABAMI Chat
利用開始	○ サービス利用	△ サーバ構築が必要 （構築サービス＝有償）
メッセージ数	× 10,000件まで（無料） ○ 無制限（課金）	○ 無制限（環境に依存）
ストレージ容量	△ 課金に依存	○ 無制限（環境に依存）
セキュリティ	△ サービスに依存	○ KATABAMI で担保
サーバ	△ クラウド（Slack社）	○ オンプレミス
対応OS	○ Linux, Windows, MacOS iOS, Android, Windows Phone	△ Linux, Windows, MacOS Android, iOS
日本語対応	○ 可	○ 可
サポート	有（有償・プラン依存）	有（有償・プラン依存）
アカウント	無料 ～ 800 or 1,600円/人月	無料
カスタマイズ	不可	可（有償）

SYNCHRO®

Visual Contact Center

For Local Government

基本コンセプト

音声、動画、画面共有。より緊密なコミュニケーション

- やりたいこと
  - 音声のみの対応からの進化形
    - プラス 動画 = 相手の顔をみながらの対話
      - 相手の様子が分かる
      - ジェスチャーも伝わる、手話での会話も可能
    - プラス 画面共有 = 資料や操作画面を共有しながらの対話
      - 操作方法のなどの円滑な伝達
  - セキュリティ は万全にしたい
    - 共有情報の データは保護したい（リアルタイムでも履歴でも）
    - システム への 侵入は防ぎたい
  - 簡単に使いたい
    - 自宅、出先 など どこから でも 接続したい
    - 面倒なこと（インストール、設定、複雑な操作）は 避けたい

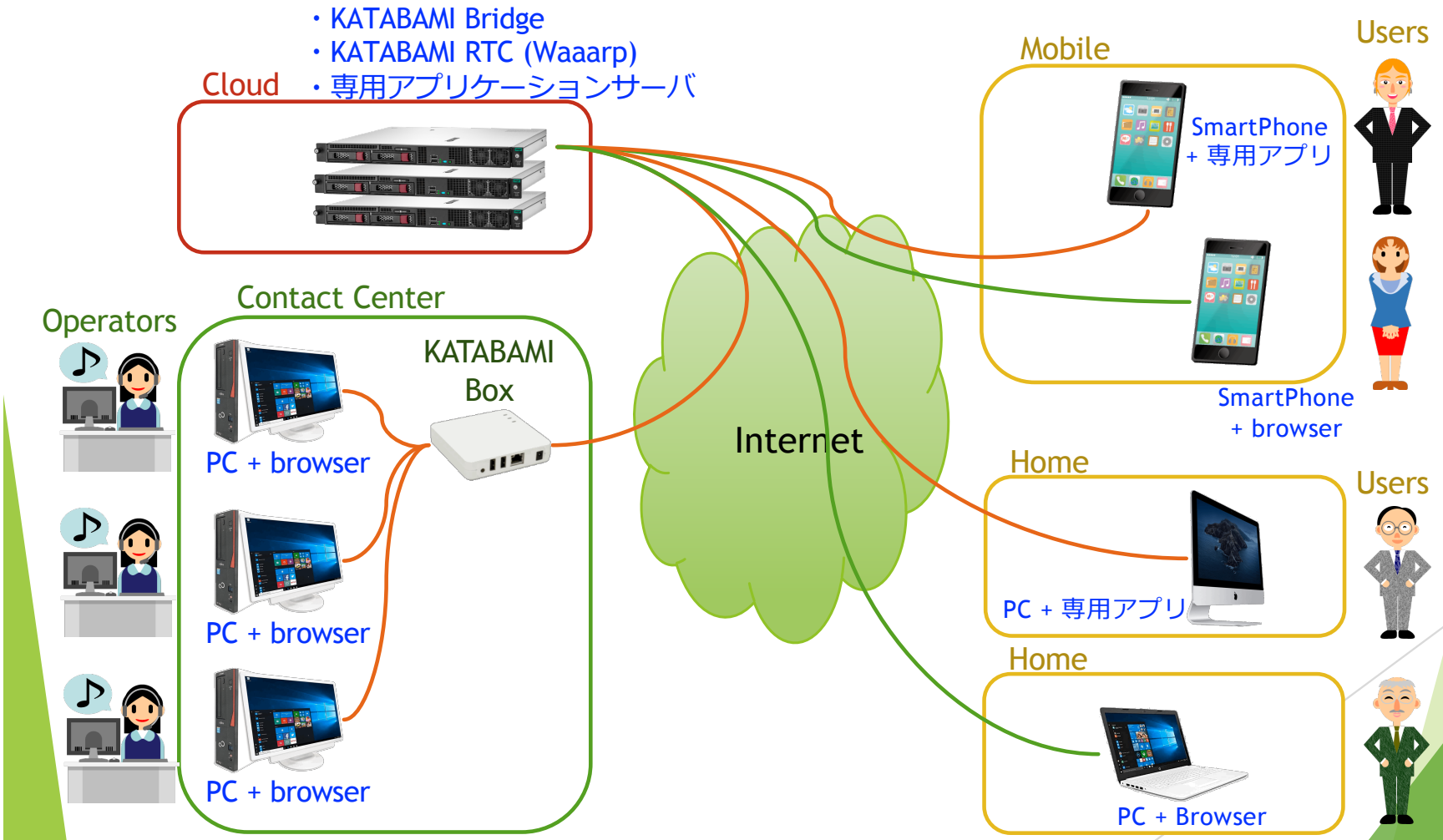
適用場面

有効活用できるアプリケーション例

- 自治体の窓口業務を遠隔でも可能化
  - 問合せ対応
    - 資料を画面共有しながら分かり難い書類作成のアドバイス
  - 悩み相談、トラブル相談
    - 相手の様子・反応をみながら適切なカウンセリングを実現
- メーカ、サービサのユーザサポート
  - 問合せ対応
    - 資料を画面共有しながら操作方法などのアドバイス
    - システム、機器情報を参照しながらトラブルシューティング
- 施設利用者の遠隔サポート
  - 受付、トラブル対応、アドバイス などを遠隔で実施
    - 接触機会を大幅に低減 → 感染症対策
    - 業務効率向上 → 人件費の圧縮

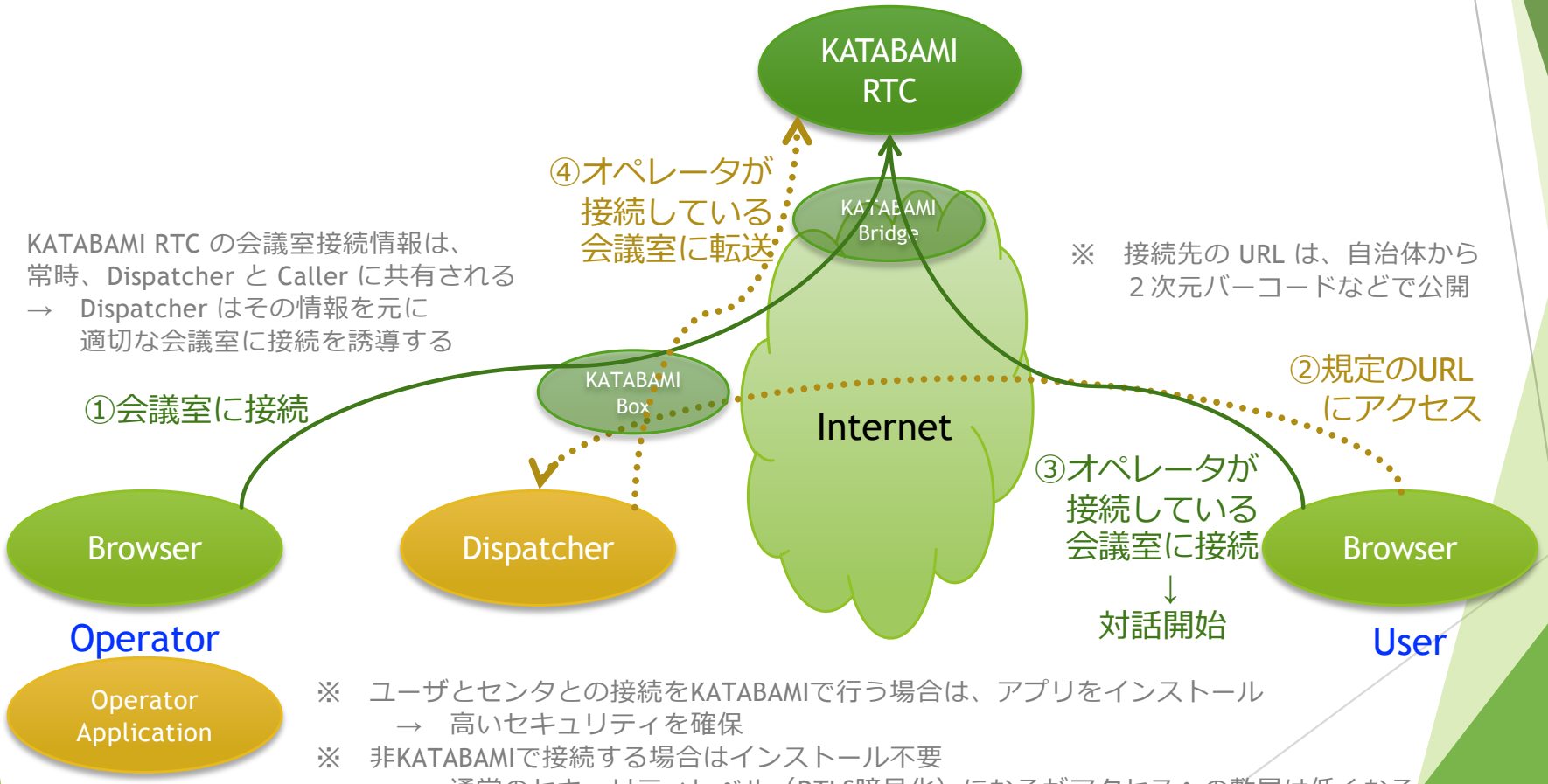
構成イメージ

問い合わせ対応、相談窓口



動作イメージ

ユーザからの接続 → 空いているオペレータに接続



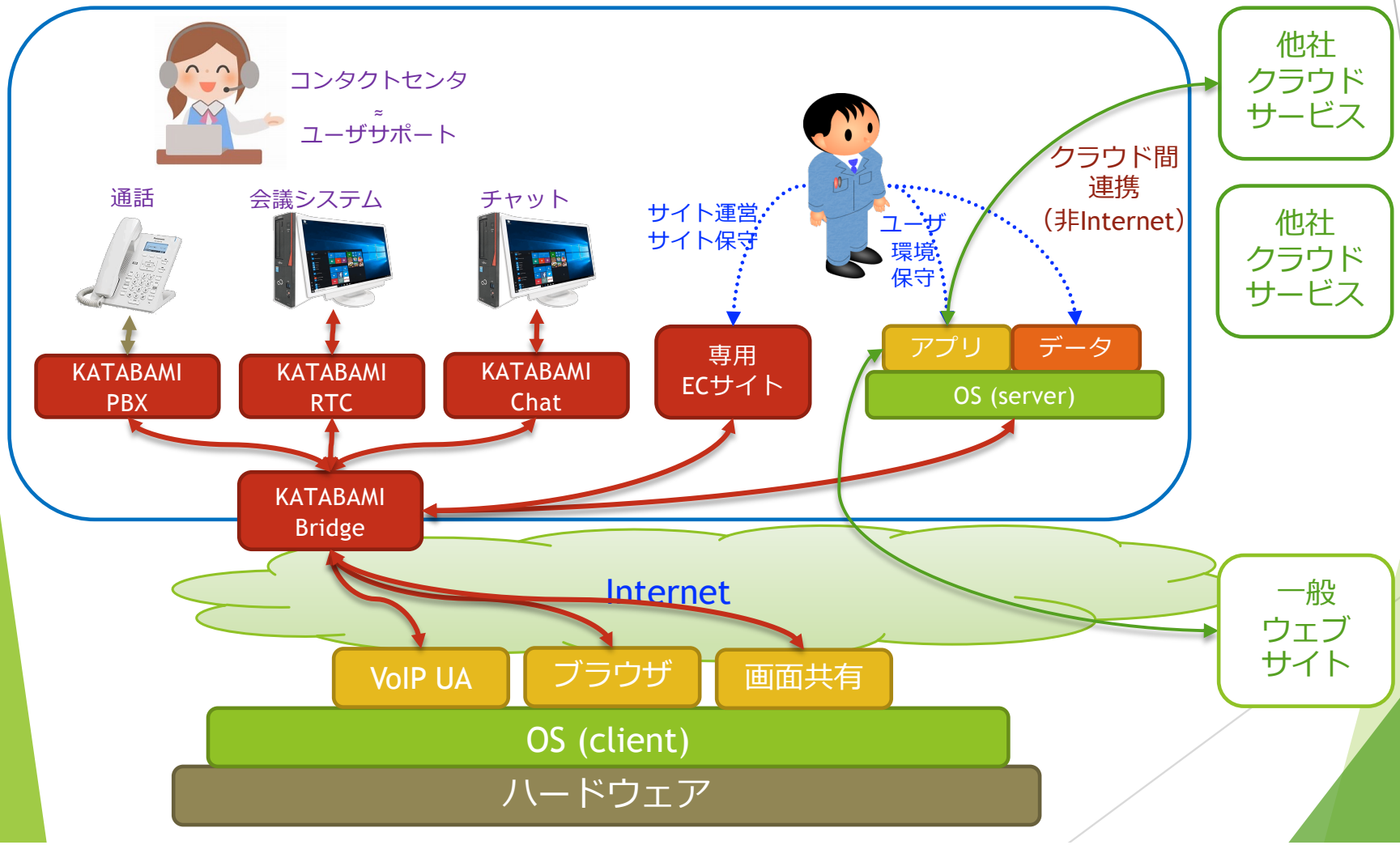
※ ユーザとセンタとの接続をKATABAMIで行う場合は、アプリをインストール
→ 高いセキュリティを確保
※ 非KATABAMIで接続する場合はインストール不要
→ 通常のセキュリティレベル（DTLS暗号化）になるがアクセスへの敷居は低くなる

Neo Thin Client

For Teleworking

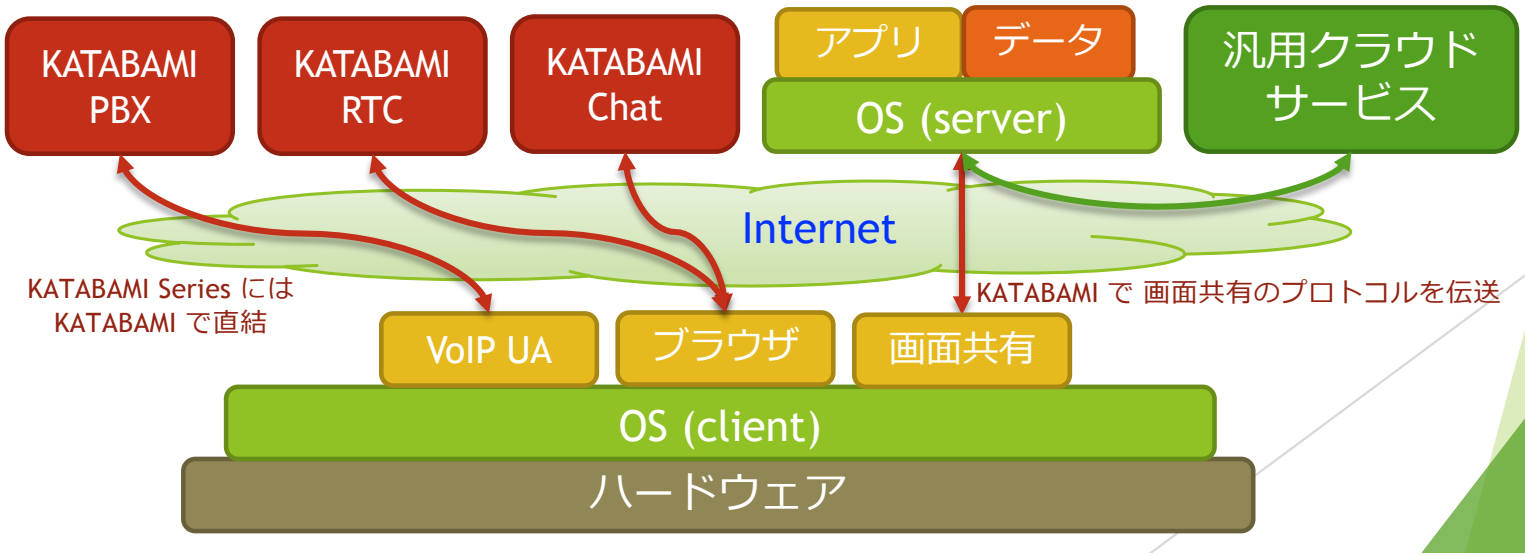
Neo Thin Client

KATABAMI が作る高セキュリティ ＆ 充実サポート



Neo Thin Client
これからのプラットホーム

- 概要
  - Client = コンパクトなタブレット型（Linux ベース）
    - WiFi接続（4G/LTE は検討中）、通信は KATABAMI でガード
    - アプリケーション = ブラウザ (Chrominium)、VoIP Client (SIP)
    - Bluetooth で keyboard & mouse を接続 + HDMI出力 → PC的な利用も可能
  - Server = Windows、MacOS、Linux
    - 一般アプリ の 主処理、データは全てクラウド側 → データ漏洩リスクを低減
    - 通信は server で扱える画面共有プロトコル を KATABAMI で伝送
      - 画面共有プロトコル = Miracast、Anycast、VLC、X2go



Neo Thin Client
いままでとは違うニュータイプ

- いままでのシンクラ（なぜ普及しなかった）
  - 重くてお買い得感がない
    - ＰＣベースのシンクラ
      - stand-aloneでアプリを動かせる能力があるがアプリを動かせない → 矛盾 → 不満
  - 通信が貧弱だと何もできない
    - シンクラ・サーバに接続できなければ機能しない → 不満
    - 通信速度が低いとレスポンスが悪い → 使い勝手が悪い → 不満
- Neo Thin Client では
  - 軽く、タッチ操作が可能なタブレット（H/Wの進化の恩恵）
    - コンパクトな OS (Linux) と 軽量なアプリ のみを実装
    - 固有アプリ：画面共有クライアント、ブラウザ (Chrominium)、VoIPクライアント
    - 作業内容によっては、ディスプレイ／キーボード／マウスで武装も可能
  - 通信速度の向上（インターネット接続環境充実の恩恵）

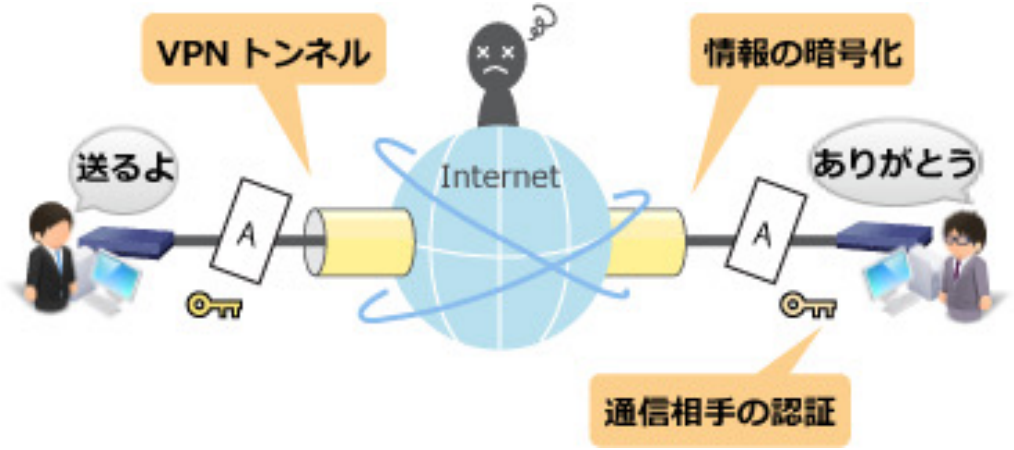
VPN
VS
KATABAMI

comparison

VPN とは？

現時点では最も普及しているセキュアアクセスの手段

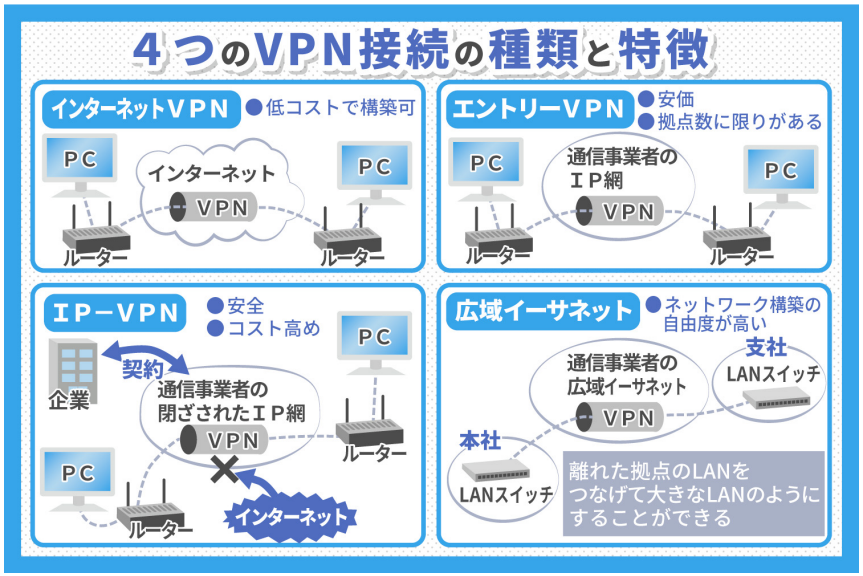
- VPN = Virtual Private Network
- 仮想的に Private Netwrok = LAN 接続を可能とする仕組み
  - １世代（２世代？）前の概念でいえば、
    専用線の代わりに「仮想」で LAN間 の接続を行う仕組み
  - ネットワークを守る防壁（firewall など）を超えて接続する仕組み
- VPN の セキュリティ
  - 接続認証 と 通信の暗号化 によって その接続を保護



VPN の種類

最も普及しているのはインターネットVPN

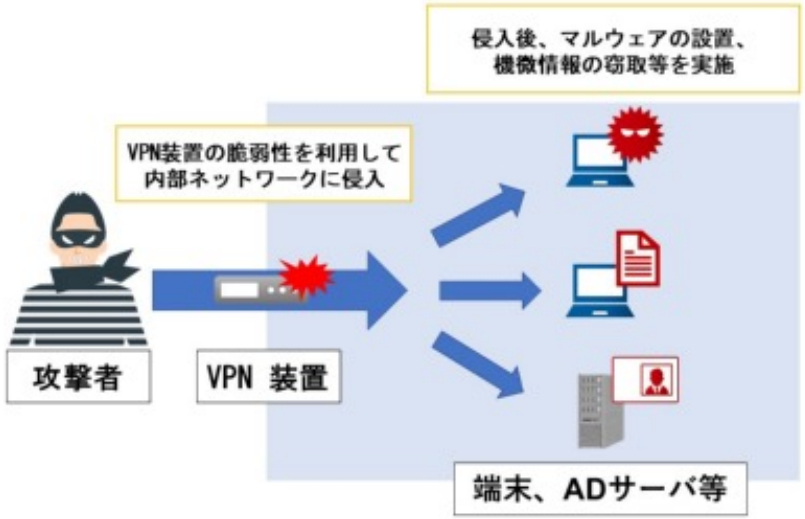
- ４種類の VPN
  - Internet利用
    - インターネットVPN　最も普及　∵低コストで構築可能（安いが偉い）
  - 通信事業者のネットワーク利用
    - エントリVPN　　比較的安価、セキュリティは高め
    - IP-VPN　　閉域網利用、コストは高め、高セキュリティ
    - 広域イーサネット　専用LAN、コストは高め、高セキュリティ
- KATABAMI の ライバル は インターネットVPN



VPN 装置の脆弱性

VPN router の F/W (firmware) の 脆弱性 を突く

- 2019年 VPNルータの脆弱性に関する情報公開
  - 米パルスセキュア（Pulse Secure）、米フォーティネット（Fortinet）、
  - 米パロアルトネットワークス（Palo Alto Networks）
- 米パルスセキュア（Pulse Secure）
  - 世界全体で、約14,500 サーバ。日本国内で、約 1,500サーバ
- 対策（F/W update）を行わないと攻撃は止まらない。2020年も攻撃例あり

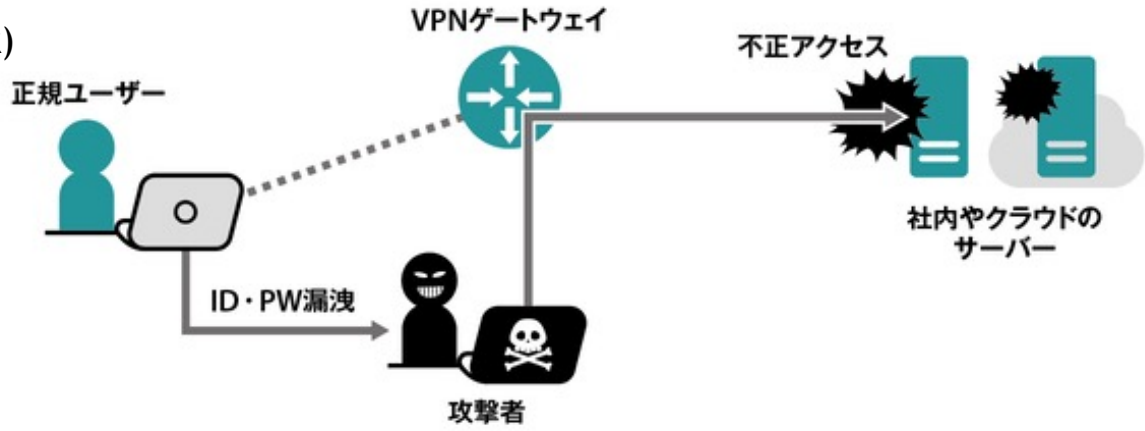


VPN 自体は安全か？
方式そのものの課題

- VPN 接続に必要な情報
  - 接続先の IPアドレス（、ポートを変更していれば ポート番号）
  - 共有鍵、ID、パスワード（IPSec VPN の場合）
- 突破方法
  - IP address/Port →「port scan」などで割り出すことが可能
  - 共有鍵、ID、パスワード
    - 「dictionary attack」などで割り出すことが可能
    - 故意、過失による漏洩もあり得る
- VPN を突破すれば..
  - そこは 保護対策のない LAN (local network)
  - LAN 内の サーバ や PC は攻撃に晒される
- 防壁 を 突破されると 為す術なし

日経新聞*(2021.1.13)*

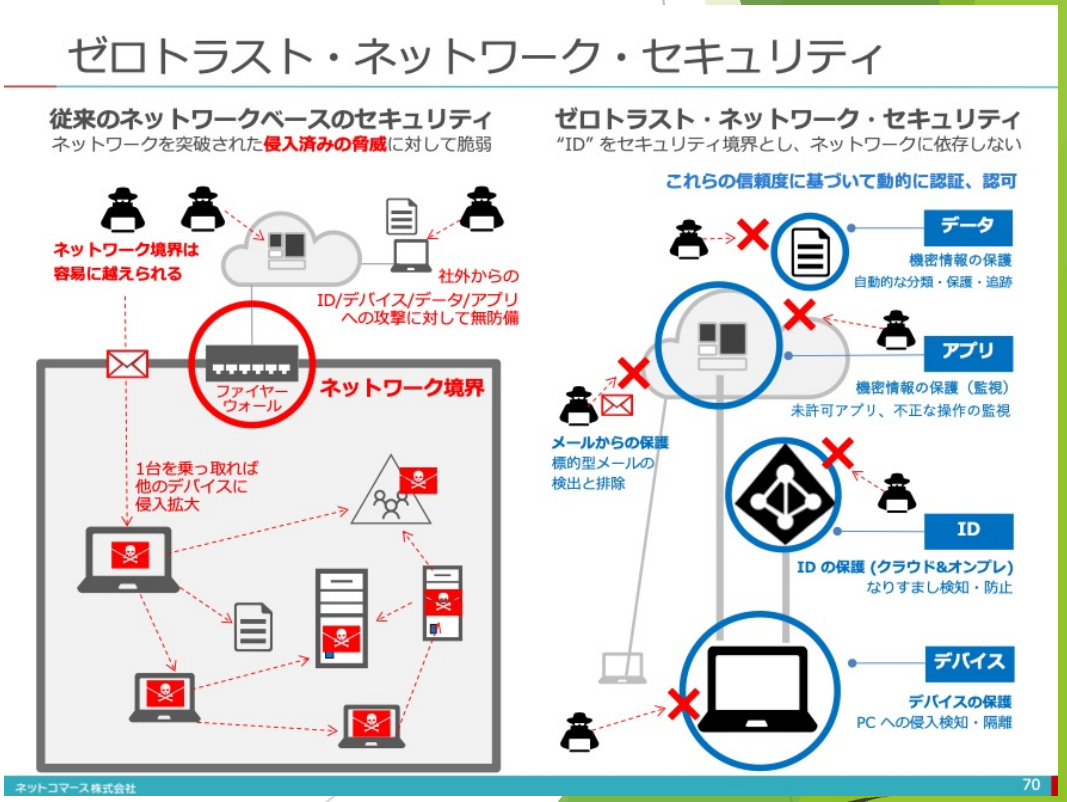
海外拠点を経由した攻撃の被害	
企業名（公表時期）	概要
川崎重工業（20年12月）	タイ拠点などから侵入され、情報漏洩の可能性
NTTコミュニケーションズ（20年5月）	シンガポール経由の攻撃で被害。延べ892社の顧客情報が流出した恐れ
三菱電機（20年1月）	19年3月以降に中国経由で被害。防衛関連情報が盗まれた恐れ
MS&Consulting（18年6月）	海外子会社のサイト経由で攻撃され、個人情報約57万件が流出の恐れ
日立製作所（17年5月）	ランサムウエア「ワナクライ」に欧州拠点の機器が感染、世界に被害が拡大



防壁方式へのアンチテーゼ

Zero Trust Security

- Zone Defense の弱点を克服
  - Zone 内の node を全て 仲間 (friend) と見なすことは止める
  - 誰も信じない = Zero Trust
- テレワーク推進の流れが追い風になる
  - Zone Defence の課題の認識が広がる
  - 2019年頃から活性化 → 2020年 に加速
  - 市場規模も急速に拡大
    - 2019年の市場規模 = US$156億
    - 2024年には US$386億 との予測
- ZTNA = Zero Trust Network Access



VPN, Zero Trust Security ∋ KATABAMI

- VPN と Zero Trust の違いは？
  - VPN は ユーザの権限 を管理
  - Zero Trust Security は ユーザ と サービス（アプリ）の利用権 を管理
- Zero Trust Security の手法としての IAM と KATABAMI との違い
  - 権限の数（∝ 設定の面倒さ）
    - IAM は ユーザ & ユーザ と サービス利用 の権限を一元管理
    - KATABAMI は、ユーザ と サービス利用 の権限を分離して管理
      - サービス利用の権限 は サービス を実行するサーバへの アクセス権で管理
    - 権限が分離していることで KATABAMI は面倒にならない？
      - 権限の数 = ユーザ数 × サービス数（これは、IAM でも KATABAMI でも同じ）
      - 手間（＝面倒さ）が 権限の数 に線形に比例するのはOK（指数的に増大しなければOK）
  - 管理の対象
    - IAM は あくまでも ユーザ を基点とした管理
    - KATABAMI は ユーザ だけでなく、ユーザが使う端末（end point）も管理
      - End point は 固有の IPv6 address を持ち、この IPv6 でも アクセスを制御可能

SYNCHRO®