KATABAMI
技術関連

2019年5月（初版）
2019年9月（社外向け 2.9版）
2022年11月（社外向け 3.5版）

株式会社SYNCHRO　中村 健

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
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

CSCC

Cyber Security Countermeasures Center

CSCC
Cyber Security Countermeasures Center

サイバーセキュリティ対策センタ

CSCC = Cyber Security Countermeasures Center

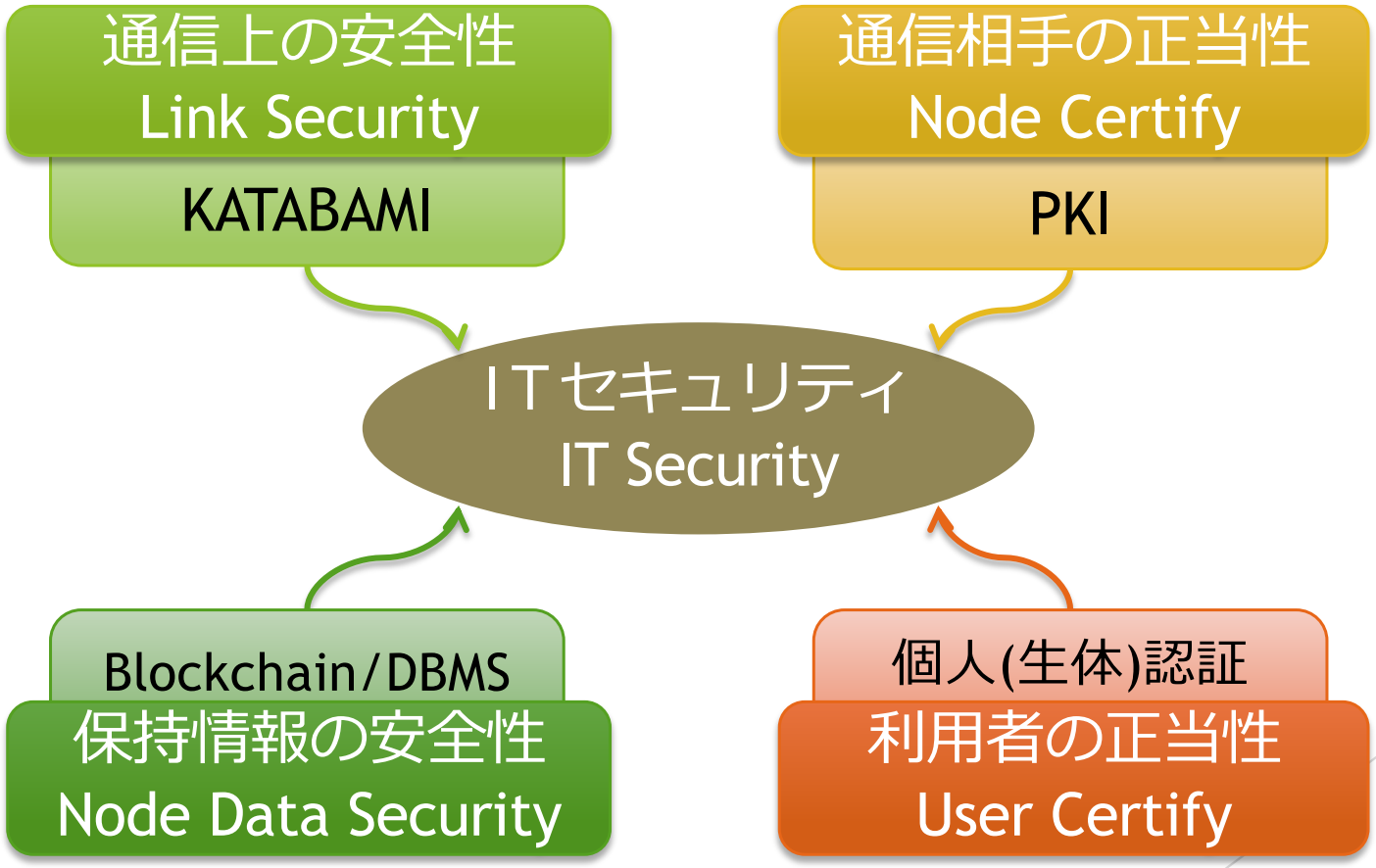
- KATABAMI Series の開発
  - 目的：IP通信のセキュリティ性能向上を図る
  - 思想：WhiteList と E2E での認証＆暗号化
  - 内容：アプライアンス と ソフトウェアシステム を製品化
- コンサルティング
  - ネットワーク設計、構築支援
  - サイバーセキュリティー対策に関するコンサルティング、設計
- IoT機器の脆弱性診断
  - 経済産業省様「開発段階におけるIoT機器の脆弱性検証促進事業」として対応中（2022年7月 - 2023年1月）
- 事業者を対象とした脆弱性診断
  - 2022年は、ニューメディアプラザ山口を中心にセミナ実施
  - 2023年から、KATABAMI VDP を投入し対応開始

KATABAMI Series

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



KATABAMI Series
appliance & software

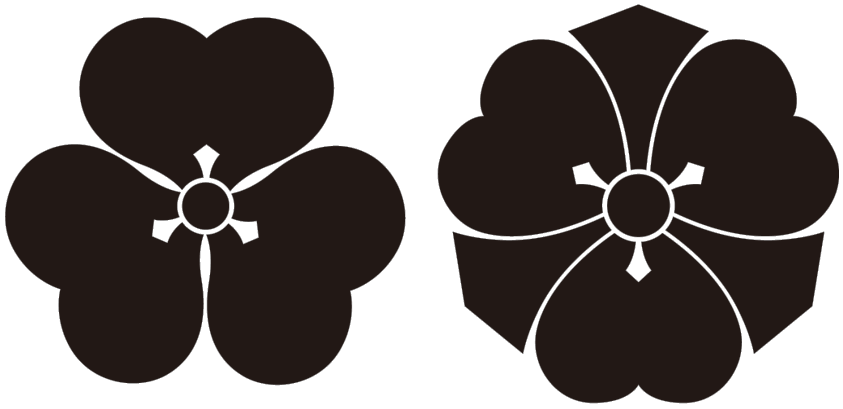
- 製品の種類
  - アプライアンス製品（IoT機器）
    - KATABAMI Box（ルータ）、KATABAMI AC2（VoIP端末）
    - KATABAMI PBX（IP-PBX）、KATABAMI Camera（IP Camera）
    - KATABAMI VDP（脆弱性検証用装置）

  - ソフトウェア製品
    - KATABAMI Chat（ビジネスチャットサーバ）
    - KATABAMI RTC（Web会議サーバ）、KATABAMI Bridge（ゲートウェイ）
    - KATABAMI PCS（認証サーバ）

- コンセプト
  - 既存ネットワーク上で仮想閉域網を構成
  - E2E の 認証・暗号化により、ゼロトラストネットワークアクセスを実現
  - OSS を活用することによりコストの最小化を図る

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



KATABAMI

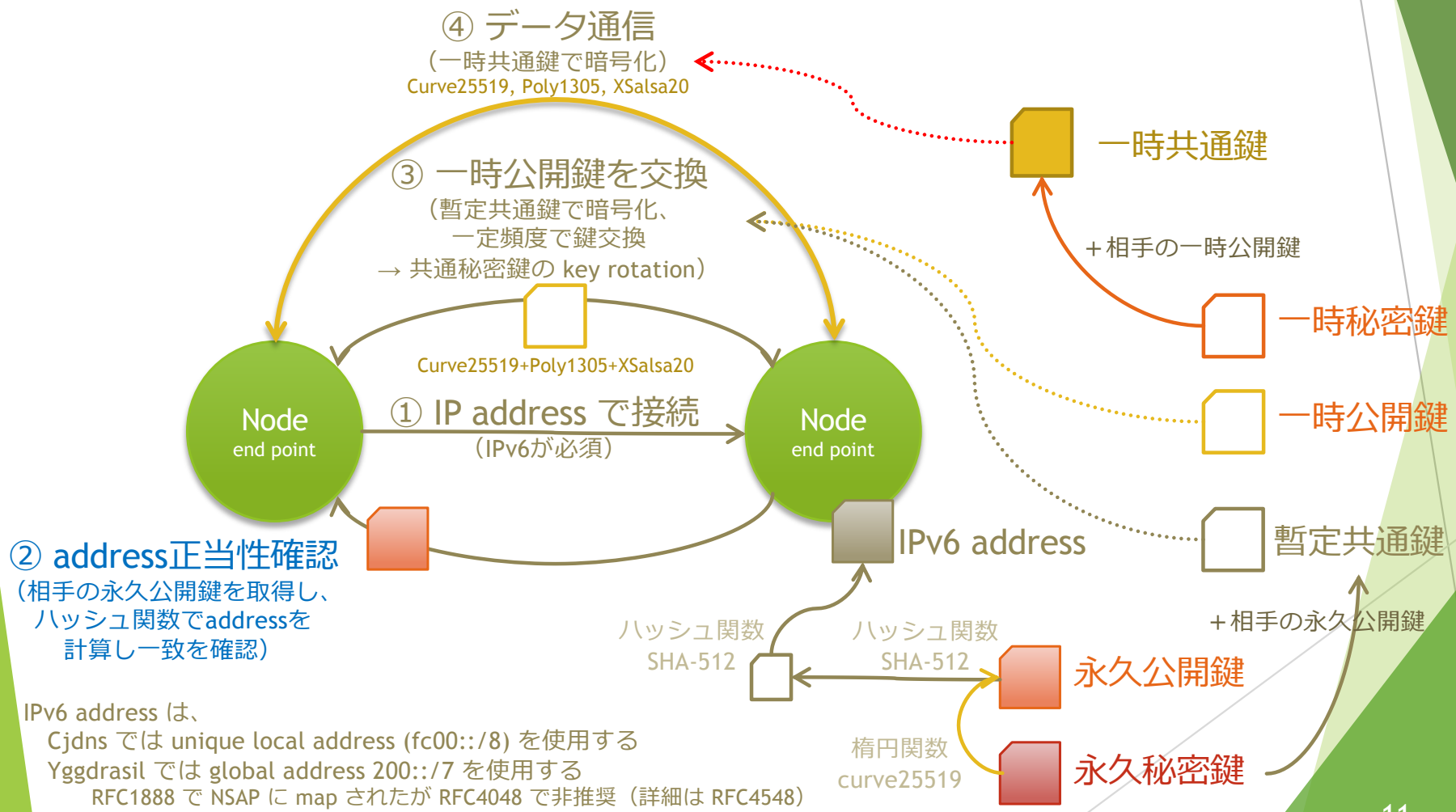
Base Technology

KATABAMI's features

Relationship between IPv6 and private key

- 目的 = なりすまし／中間者攻撃の封止
  - KATABAMI の IPv6 address は、永久公開鍵 から生成
  - 処理手順
    - ① 双方、永久ペア鍵（永久公開鍵、永久秘密鍵）を持つ
    - IPv6 address で node A が node B に接続
    - ② node A は node B の 永久公開鍵を取得 → IPv6 address との突き合わせ
    - 双方、相手の永久秘密鍵と自分の永久公開鍵で 暫定秘密鍵 を生成
    - ③ 双方、一時ペア鍵（一時公開鍵、一時秘密鍵） を生成
    - 暫定秘密鍵を使った暗号通信で一時公開鍵の交換を実施 → 成立すれば なりすまし は無い
    - ④ 双方、相手の一時公開鍵 と 自分の一時秘密鍵 で 一時共通鍵 を生成
    - この 一時共通鍵 で データを暗号化して授受
    - ※ ③ の手順を定期的に実施 = 一時共通鍵 の key rotation
      - 目的は、セキュリティ強度 と 処理効率 のバランス取り

Secure Network
function of KATABAMI



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

Crypt engine on KATABAMI
Curve25519, Poly1305, XSalsa20

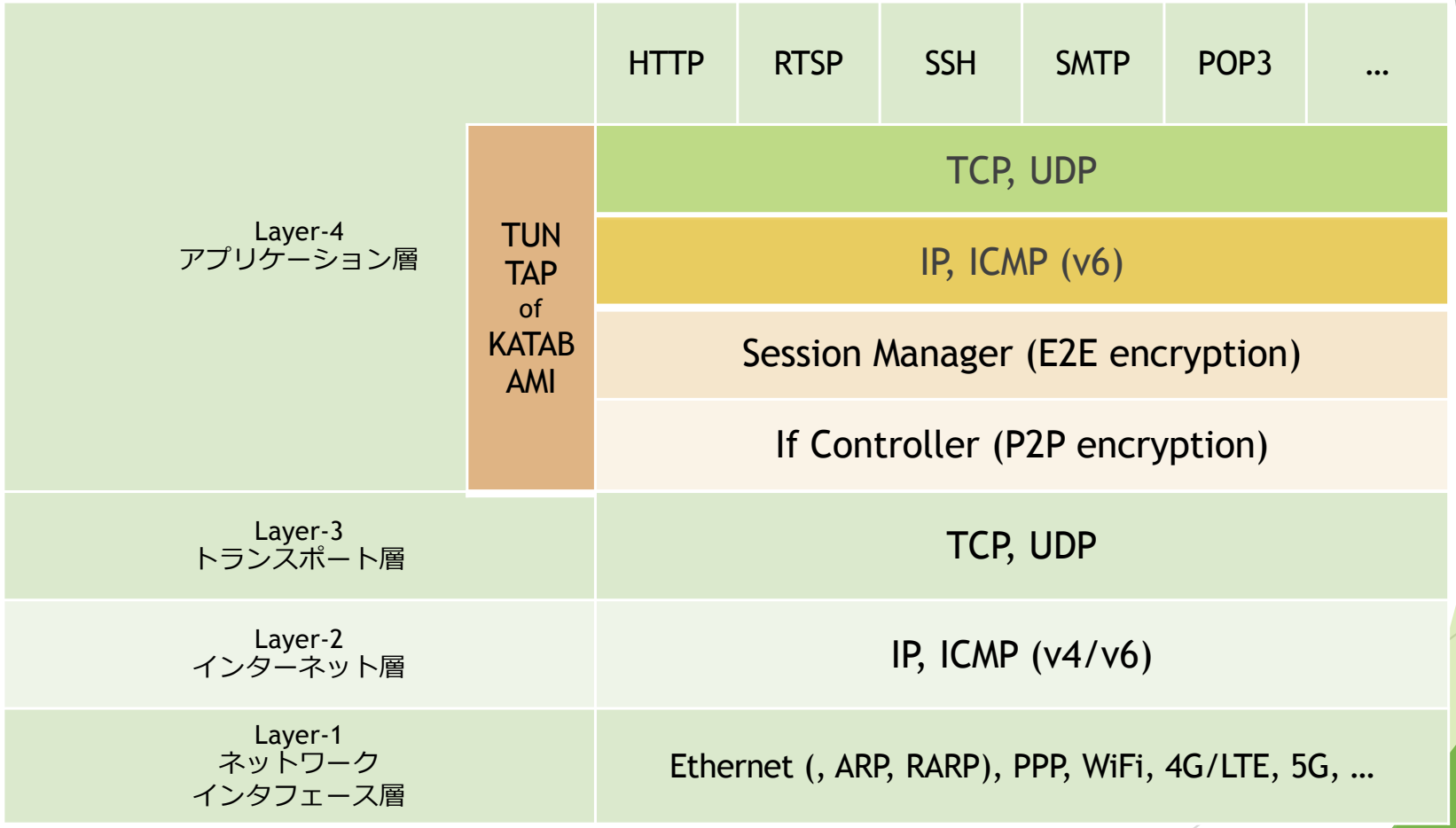
- 概要
  - Curve25519（楕円曲線暗号）
    - 秘密鍵 256bits、公開鍵 256bits。暗号化強度 = 128bits
      - AES256 の 暗号化強度 = 128bits
  - Poly1305-XSalsa20（ストリーム暗号）
    - 鍵 128bits、追加鍵 106bits、nonce 192bits
      - Xsalsa20 は Salsa20 の拡張（nonce が 128bits から 192bits に拡張された）
- 特徴
  - 高暗号強度
    - Salsa20 は 同じ bit数の AES よりもセキュリティが高いことが実証されている
  - 低処理負荷（ソフトウェア処理に向いている）
    - 処理負荷 は Poly1305-Salsa20 : AES ≒ 1 : 3
      - AES は AES-NI があれば速く処理可能であるが、AES が無いと処理負荷が大きい
        - AES-NI は Intel, AMD の CPUに実装されているが、ARM には非実装 → AES は IoT に不向き
        - IoT への適用が多い ARM では Curve25519+Poly1305+XSalsa20 が適している
  - ライセンスフリー
    - Curve25519, Poly1305, XSalsa20 いずれも、既出願の特許には関連していない

Bridge of KATABAMI
for no-transparent network

- KATABAMI は Layer2 透過 なネットワークでは 自動で peering
  - KATABAMI は beacon を broadcast して接続対象を探索し peering
  - Layer3 Switch（L3 SW、NAT）が存在すると、その先には接続できない
- IPv4通信 を Layer2 として KATABAMI による通信を行う
  - Internet を経由したLAN間の接続が可能（拠点間 & モバイル）
- 方式
  - IPv4 TCP/UDP による tunneling
  - 接続には以下の情報が必要
    - IPv4 の (Global) IP address & Port
    - Login ID & password
    - KATABAMI node の 公開鍵

KATABAMI Network

KATABAMI network structure



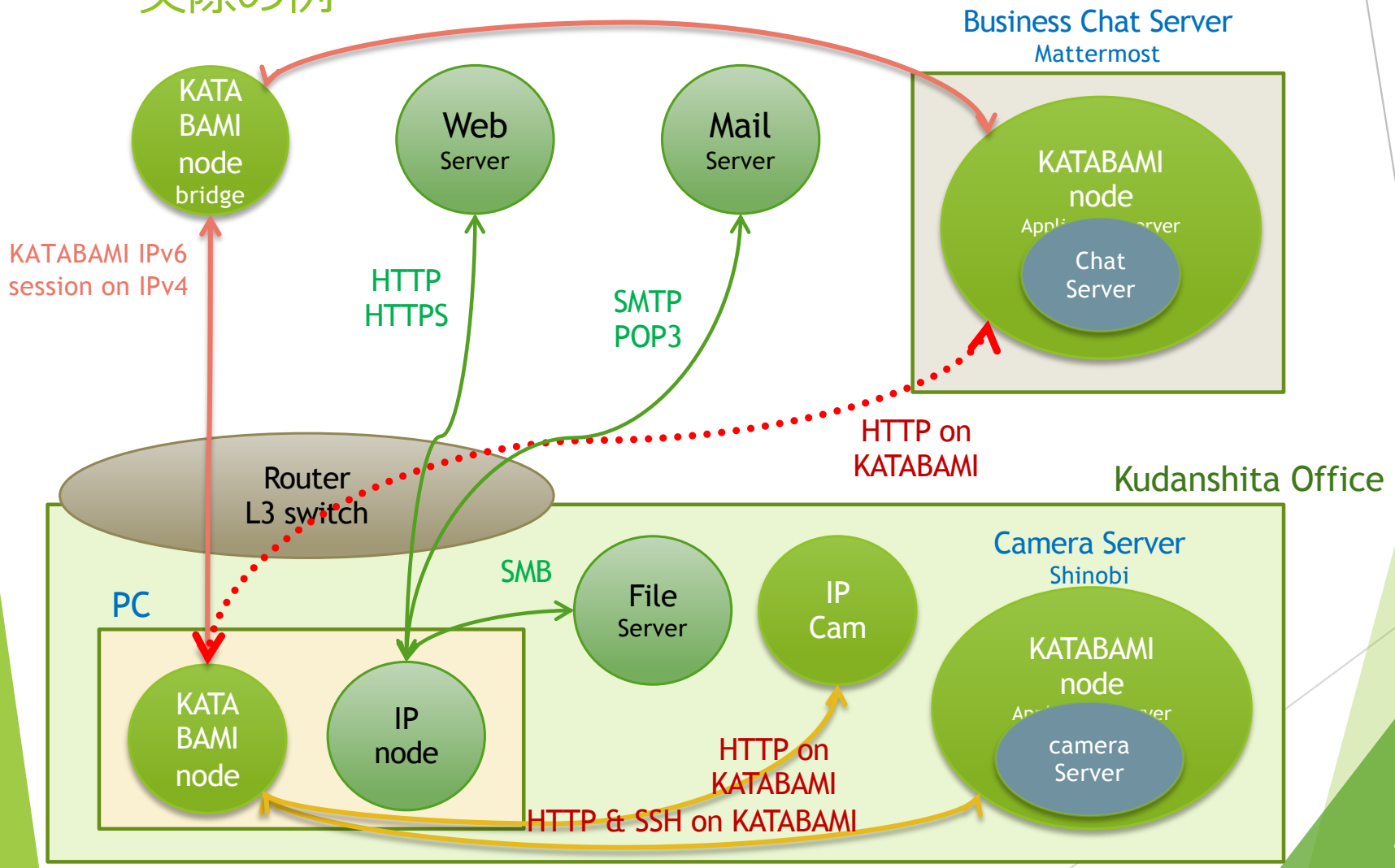
※ TUN = TUNnel, TAP = Terminal Access Point, IP Address = IPv6unique local address (fc00::/8)

KATABAMI node with normal IP node

Mixed Environment

混在可能な normal IP & KATABAMI

実際の例



KATABAMI Environments

KATABAMI の 環境
動作環境、技術標準

- 対応OSの拡充（対応済み、最近対応、一部別方式で対応）
  - Ubuntu 16.04 LTS, 18.04 LTS, 20.04 LTS, 22.04 LTS
  - Windows 10, 11、Windows Server 2016, 2019, 2022
  - MacOS 10.13.x, 10.14.x, 10.15.x, 11.x, 12.x, 13.x
  - RHEL/CentOS 7.x、RHEL 8.x、Debian 9.x, 10.x, 11.x、その他 linux
  - Android 8.1, 9, 10, 11, 12、iOS、iPadOS、Raspberry Pi OS

- セキュリティ規格 への対応
  - IEC62443 = 産業向け IoT の セキュリティマネージメント規格
    - SIoTP様 のご協力の下、2020年にチェックリストを作成し評価を実施
      - SIoTP = 一般社団法人 セキュアIoTプラットホーム協議会
  - JAHIS 製造業者/サービス事業者による医療情報セキュリティ開示書
    - 2021年3月から対応作業中
      - JAHIS =一般社団法人 保険医療福祉情報システム工業会