Tempered Networks製品紹介

TRILOGY
In collaboration with customer

販売パートナー
Direx
JAPAN DIREX CORPORATION
日本ダイレックス株式会社

Agenda

1. Tempered Networks社紹介
2. ネットワークにおけるセキュリティ課題
3. 製品コンセプト
4. HIPとは？
5. 製品構成
6. 製品ラインナップ
7. 適用分野
8. 導入事例

Tempered Networks社紹介

- 会社設立：2014年、本社ワシントン州シアトル

- 創業者CEO：Jeff Hussey（F5の創業者）
  - 社外取締役：Stuart Bailey（Infoblox創業者）
  - Yee May,VP APACJ&Europe：シンガポール
- 製品コンセプト：
  - 既存のIPネットワークから重要な特定ネットワーク通信を隔離/秘匿して外部からステルスモードにして“情報漏えい”や“外部不正アクセス”をシャットアウトさせる
  - IETF標準化団体で承認されたHIPというセキュリティプロトコルを使用して特定のエンド・ツー・エンド通信を暗号化してセキュアにする
- 市場での実績

  米国内で社会インフラや流通系、金融機関など

  既に約50社納入・稼働中

Agenda

1. Tempered Networks社紹介
2. ネットワークにおけるセキュリティ課題
3. 製品コンセプト
4. HIPとは？
5. 製品構成
6. 製品ラインナップ
7. 適用分野
8. 導入事例

ネットワーク業界のセキュリティ課題

- TCP/IP はプロトコルの設計にセキュリティが考慮されていないため、本質的に脆弱であるが広く普及しているため、抜本的な変更が困難
- IP は接続先デバイスの宛先情報と通信経路情報を兼ねているため、モバイル環境などIPが頻繁に変更される構成での相互通信が困難
- モバイルデバイスや RFID、ホームオートメーション機器、医療機器など、2020 年までに5,000 億の「モノ」が接続され（IoT）、デバイス数が急増
- サイバー犯罪者はユーザー間の信頼関係を悪用することに成功。IoT とM2M はマシン間の信頼関係に基づいており、同じリスクを抱えている

Agenda

1. Tempered Networks社紹介
2. ネットワークにおけるセキュリティ課題
3. 製品コンセプト
4. HIPとは？
5. 製品構成
6. 製品ラインナップ
7. 適用分野
8. 導入事例

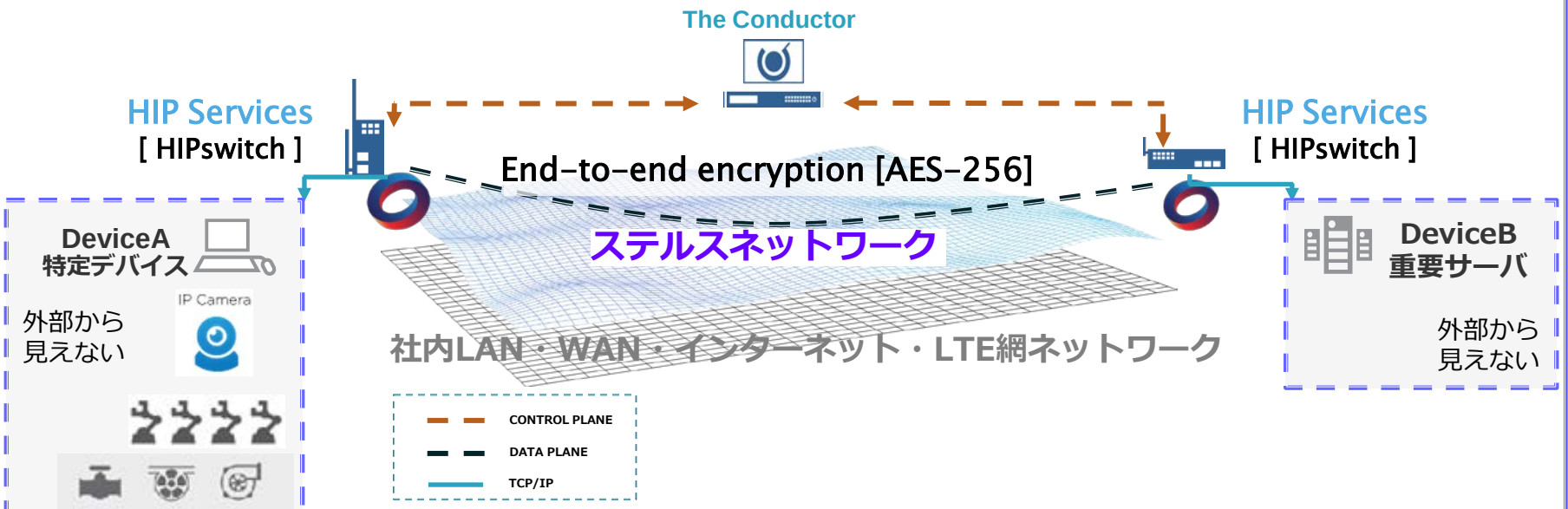
製品コンセプト 1/2

- 重要な資産に対して細分化（小さなセグメント）されたネットワークアクセスを構築
- 共有インフラ上で通信されているデバイスとネットワークを安全に接続
- データセンター間の透過的かつ迅速なフェールオーバ
- 必要に応じてセキュアなネットワークを容易に変更
- 安全なSDNセグメントを構築

製品コンセプト 2/2

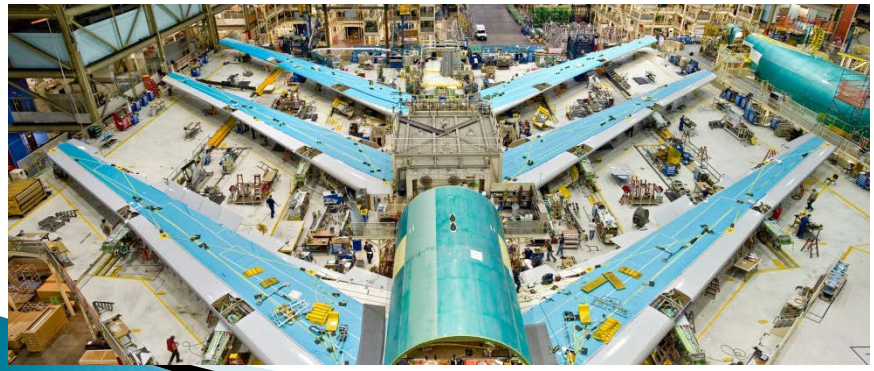
重要なデバイスを見えなくする
～ステルスネットワーク

既存のTCP/IPネットワークから重要な通信を隔離し
外部からステルス（＝見えなく）にして
“情報漏えい”や“外部不正アクセス”をシャットアウト



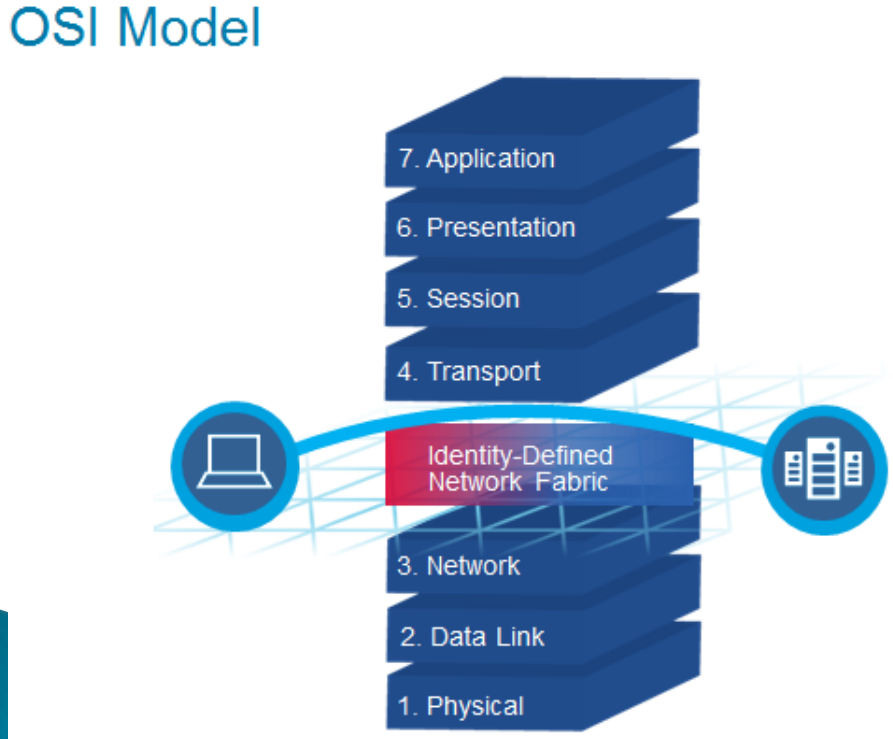
Tempered Networks製品の開発経緯
～技術はボーイング社内から生まれた～

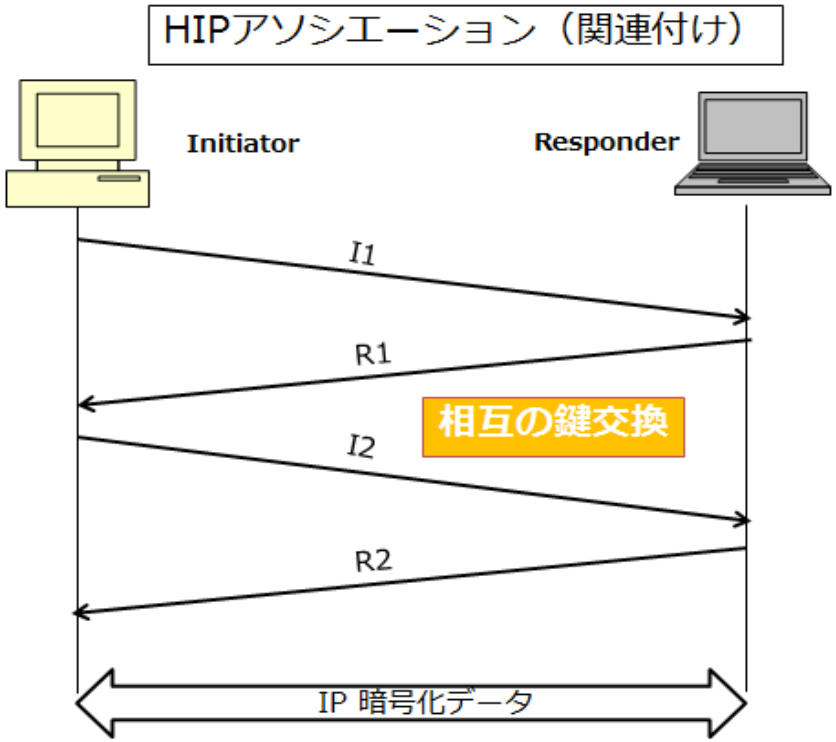
- 1999年：米国海軍が”HIP”を考案
- 2002/3年：IETF標準化団体でHIPを検討
- 2004年：IETF内でHIPのWorking Group組織
  - ボーイングR&DのDavid Mattesも参加
- 2005年：ボーイングプロジェクト開始。その後導入
- 2012年4月：Asguard社設立。商用版リリース
- 2014年10月：Tempered Networks設立



HIPとは?

- Host Identity Protocol (HIP) は、盗聴やその他の脅威に対するセキュリティ面を強化したエンドポイント間で動作するIPレベルでの次世代通信プロトコル
- HIP通信プロトコルは2005年に米海軍で開発。その後ボーイングで改良。IETF RFC5210/4423として業界標準化

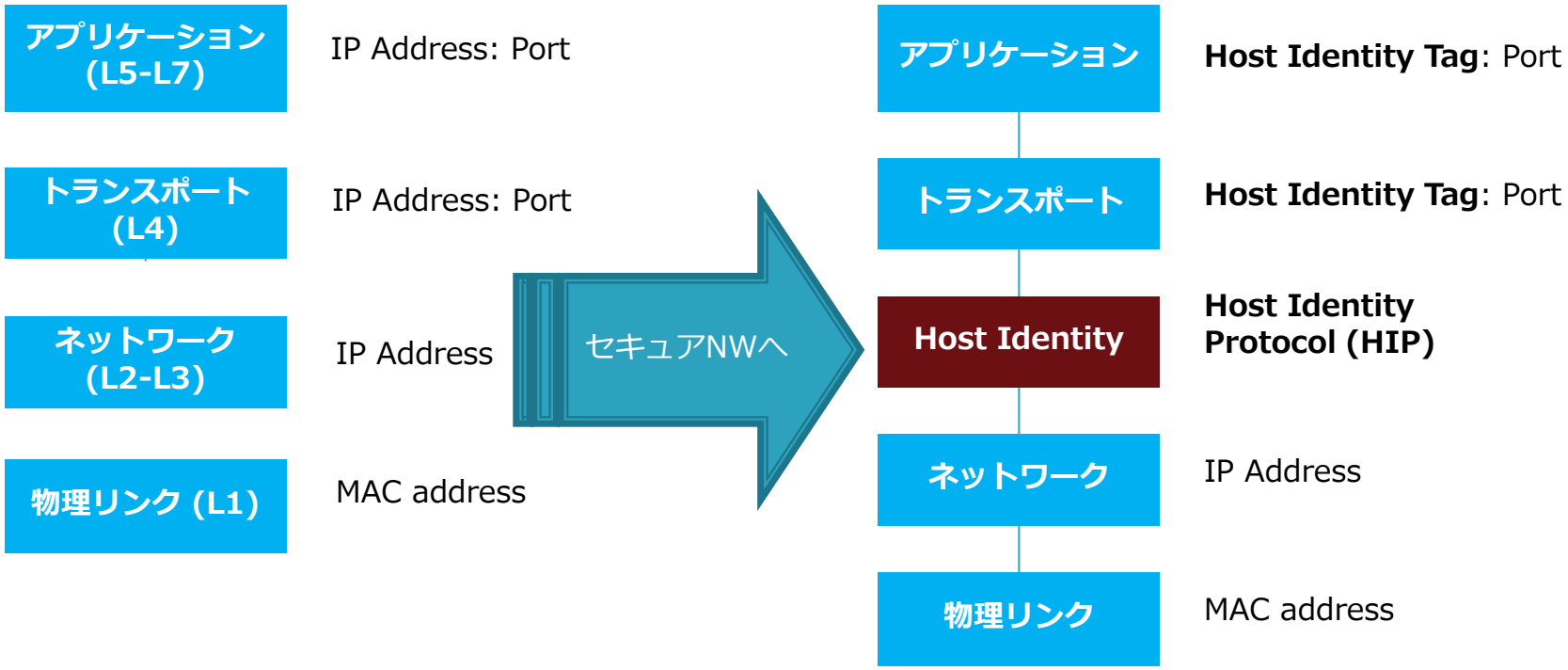




新たなアイデンティティネットワーク（IDN）へ パラダイムシフトが必要

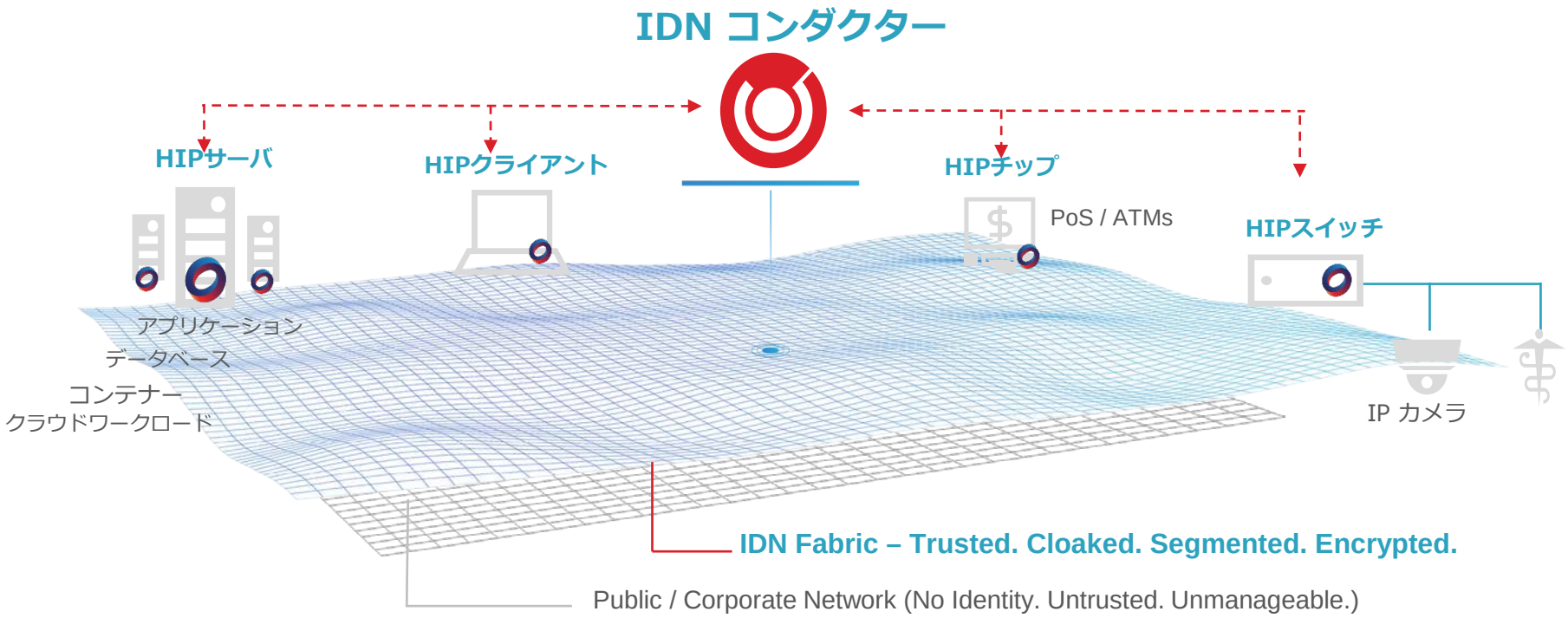
Internet 2.0 –
“Network everything”

Internet 3.0 –
“Network ONLY CRYPTO-IDENTIFIED things”

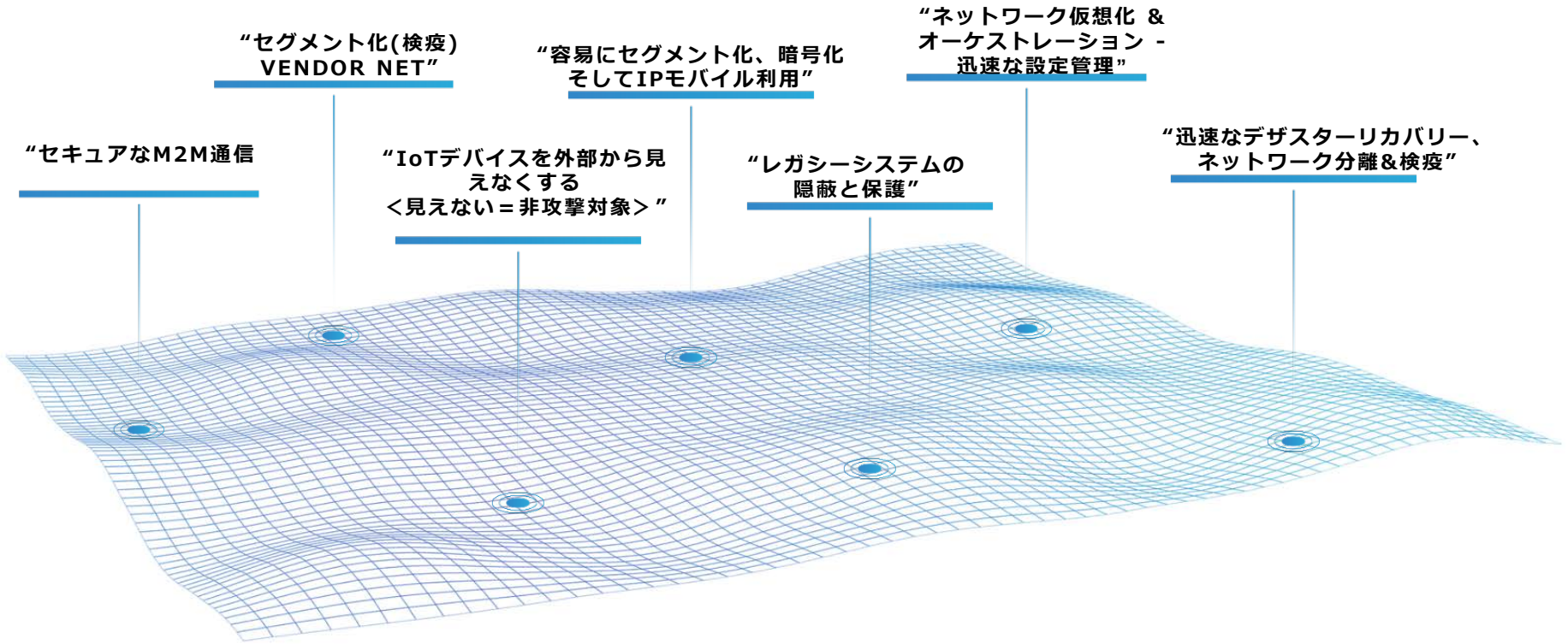


Identity-Defined Networking (IDN)

ネットワーク接続されたすべての**モノ**にユニークな暗号化IDを付けてコントロール。シームレスな導入、IDベースの簡単なポリシー設定によるオーケストレーションを実行。　IDNの暗号化ファブリック内でのセキュアな接続、クローク、スモールセグメント化、隔離・取り外し、移動、フェールオーバを迅速に。



TemperedNetworksソリューション用途



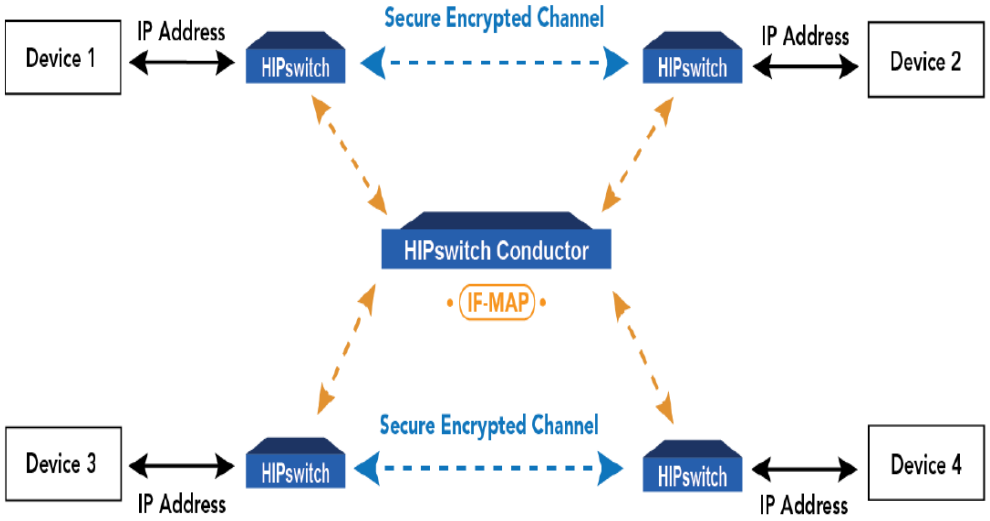
Agenda

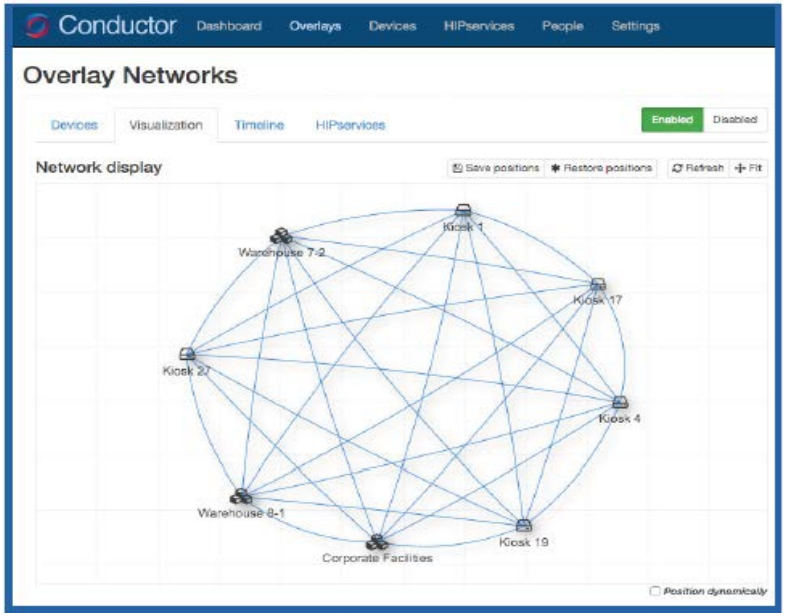
1. Tempered Networks社紹介
2. ネットワークにおけるセキュリティ課題
3. 製品コンセプト
4. HIPとは？
5. 製品構成
6. 製品ラインナップ
7. 適用分野
8. 導入事例

製品構成 1/2

- オーバレイネットワークはHIPスイッチとHIPスイッチコンダクターで管理
- オーバレイネットワークを通じてユーザが保護したいデバイスに関してより堅牢なセキュア通信を提供

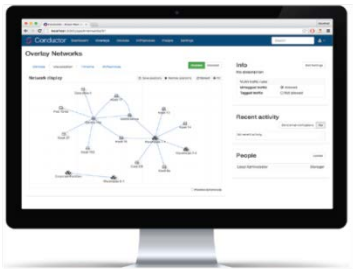
(注）オーバレイネットワークとは IPアドレスが指定されていない目的地へルーティングメッセージを送出すること可能にするための仮想ネットワーク





製品構成 2/2

- **IDNコンダクタ**
  - HIPスイッチ間でオーバレイネットワークを構築して、HIPスイッチ、デバイス、セキュリティポリシー、ユーザアカウントを含むコンポーネントを管理するオーケストレーションエンジン。IF-MAPサービス機能を実装しており、これによって各HIPスイッチにリアルタイムでセキュリティメタデータをデリバーする
- **HIPスイッチ**
  - HIPを実装したスイッチ。HIPスイッチにLAN上の保護したいホストデバイスを接続。オーバレイネットワークを介してHIPスイッチ間で暗号化通信を行う
- **HIPクライアント**
  - Windows版(7/8/10)、MAC/OS版（予定）、Linux版（予定）
- **HIPサーバ(Windows)**
- **HIP chip Firmware（IoT組込み型）**



CONDUCTOR
CENTRALIZED
ORCHESTRATION

IDENTITY-ENABLED HARDWARE

IDENTITY-ENABLED CLOUD
& HYPERVISOR PLATFORMS

IDENTITY-ENABLED
CLIENTS & SERVERS

SIEMENS RUGGEDCOM

PoE
SWITCH

IDENTITY-EMBEDDED MODULES

HIPオーバレイと既存VPNとの比較

- 既存VPNの機能
  - VPNトンネルを構築するためには複雑な鍵交換手順(実情)
  - LAN上の特定セグメント間の暗号化通信が出来ない
  - マルチサイト間でのVPNトンネル変更が難しい
  - マルチサイトとのトンネルは設定できるがマルチトンネルとの同時アクセスは出来ない。
- HIPオーバレイネットワーク
  - 対抗に安価なHIPスイッチとマルチサイトを一元管理するHIPスイッチコンダクタアプライアンスを設置
  - 必要な時にプライベートオーバレイネットワークを容易に構築変更・追加が可能
  - それぞれのLAN上で隠匿したい特定セグメント間の暗号化通信が可能
  - HIPスイッチコンダクタのポリシング設定によりメッシュ網でのプライベートオーバレイネットワークで暗号化通信設定可能

Agenda

1. Tempered Networks社紹介
2. ネットワークにおけるセキュリティ課題
3. 製品コンセプト
4. HIPとは？
5. 製品構成
6. 製品ラインナップ
7. 適用分野
8. 導入事例

製品ラインナップ　HIPスイッチ

HIPswitch-100 シリーズ

HIPswitch-100 シリーズは、小型の物理アプライアンスで、セキュアな接続のスループットは 8 Mbps に達します。DIN レールまたは壁掛け (オプション) で設置でき、様々な電源で動作し、有線・無線ネットワーク、携帯電話回線などで接続できます。
HIPswitch-100v は仮想 HIPswitch です。ラップトップやデスクトップ PC にインストールし、高度にセキュアなリモートアクセスを可能にします。

スループット : 8 Mbps
外形寸法 : 3.19" L x 1.77" W x 3.74" H
形状 : IP-30、DIN レール、壁掛け
電源 :　- デュアル 12-48 VDC 4 ピンターミナルブロック
　　- IEEE 802.af PoE PD
　　- 3 つの入力全てで自動フェイルオーバー
動作温度 : -40° C ~ +80° C
湿度 (結露無し) : 5% ~ 95%

物理アプライアンス	ネットワーク I/F
HIPswitch-100e	2 x RJ45 10/100
HIPswitch-100w	2 x RJ45 10/100, 1 x 802.11 b/g/n
HIPswitch-100g	2 x RJ45 10/100, 1 x Cellular
仮想アプライアンス	**OS 要件**
HIPswitch-100v	Windows 7/8

HIPswitch-200 シリーズ

HIPswitch-200 シリーズは、中型の物理アプライアンスで、セキュアな接続のスループットは 15 Mbps　に達します。DIN レールへの設置が可能 (オプション) で、様々な DC 電源で動作し、有線・無線ネットワーク、携帯電話回線などで接続でき、これらの異なるネットワークを跨いだフェイルオーバーをサポートします。

スループット : 15 Mbps
外形寸法 : 4.1" L x 7.0" W x 1.6" H
形状 : 20ga メタルケース、DIN レール
電源 : PoE またはバレルジャックからの 8-48VDC 入力
動作温度 : -40° C ~ +85° C
湿度 (結露無し) : 20% ~ 90%

物理アプライアンス	ネットワーク I/F
HIPswitch-200e	2 x RJ45 Gig-E
HIPswitch-200w	1 x RJ45 Gig-E, 1 x 802.11 a/b/g/n
HIPswitch-200g	1 x RJ45 Gig-E, 1 x 3g cellular

HIPswitch-300 シリーズ

HIPswitch-300 シリーズは、データセンター向けの 1U サイズの物理アプライアンスで、セキュアな接続のスループットは 100Mbps に達し、デバイスネットワーク用に 4 ポート、共通ネットワーク用に 2 ポートを持っています。
HIPswitch-300v は仮想 HIPswitch です。データセンターやクラウドにインストールし、高度にセキュアなリモートアクセスを可能にします。

物理アプライアンス	ネットワーク I/F
HIPswitch-300	6 x RJ45 Gig-E
仮想アプライアンス	**OS 要件**
HIPswitch-300v	VMWare ESXi 6.x, Hyper-V (Microsoft Windows Server 2012 R2)

スループット : 100 Mbps
外形寸法 : 9.8" L x 17.2" W x 1.7" H
形状 : 19" ラックマウント、1U
電源 : 200W 電源、100 - 240VAC、50 - 60Hz
動作温度 : 0° C ~ +35° C
湿度 (結露無し) : 8% ~ 90%

HIPswitch-400 シリーズ

HIPswitch-400 シリーズは、データセンター向けの 1U サイズの物理アプライアンスで、セキュアな接続のスループットは 1.3Gbps に達し、デバイスネットワーク用に 4 ポート、共通ネットワーク用に 2 ポートを持っています。

物理アプライアンス	ネットワーク I/F
HIPswitch-400	6 x RJ45 Gig-E

スループット : 1.3Gbps
外形寸法 : 25.6" L x 17.2" W x 1.7" H
形状 : 19" ラックマウント、1U
電源 : 500W 電源、100 - 240VAC、50 - 60Hz
動作温度 : 0° C ~ +35° C
湿度 (結露無し) : 8% ~ 90%

仮想アプライアンス版有り
（ESXi Hyper-V）

HIPスイッチConductor ・ Client

HIPswitch　Conductor

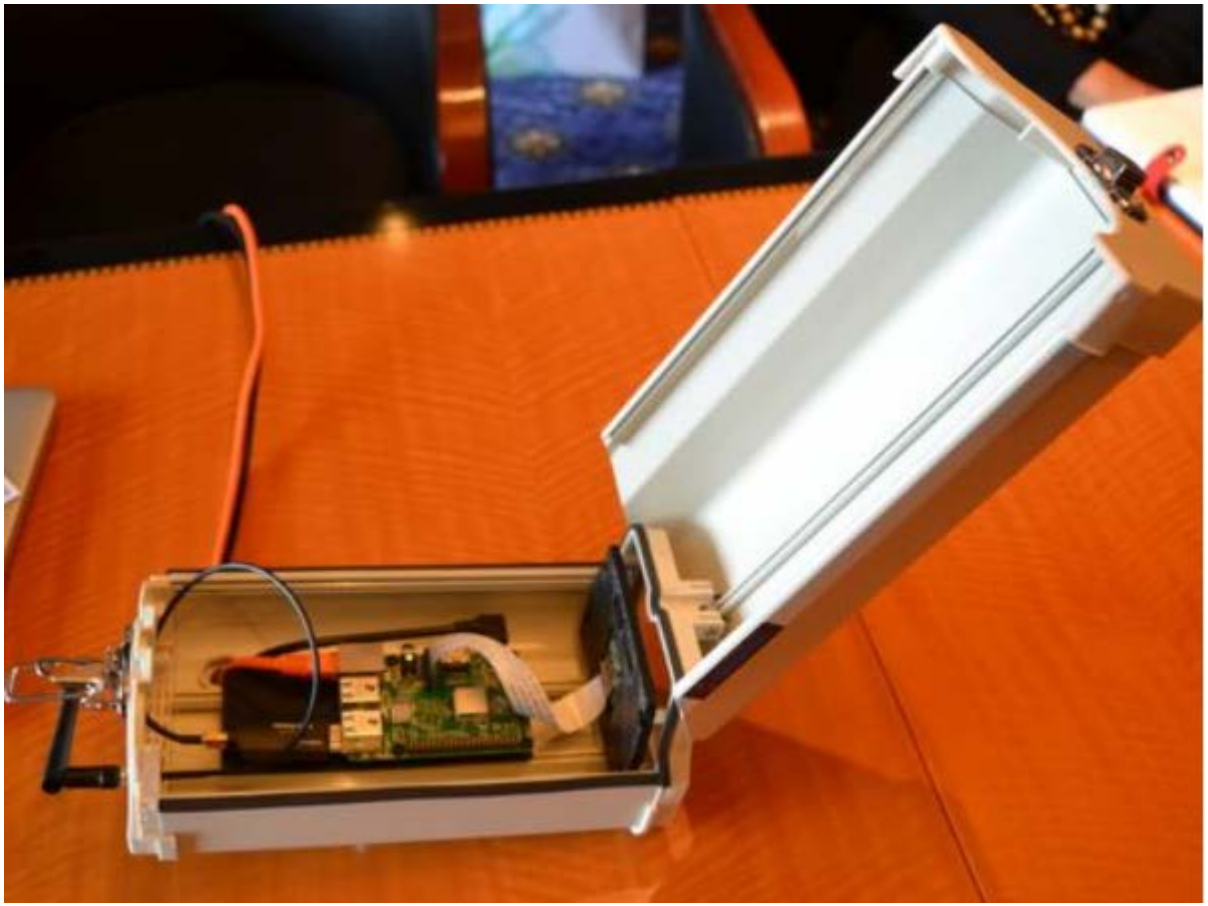
HIPswitch　Conductor for AWS

Windows(7,8,10)版
MAC/OS版（予定）
Linux版（予定）

HIPスイッチ Embedded （組込み型）

- HIPchip firmware
  - カスタムハードウエアへの組込み開発。
  - The minimum hardware requirement to run the HIPchip firmware is a 500 MHz MIPS processor and 64 MB of RAM.
  - 既にフィリピン銀行でのPoE装置（数千のIPカメラを接続する）：Certis Cisco社（セキュリティ警備サービス会社）
  - Siemens Ruggedcom社産業用イーサネットスイッチ

組込み型の例



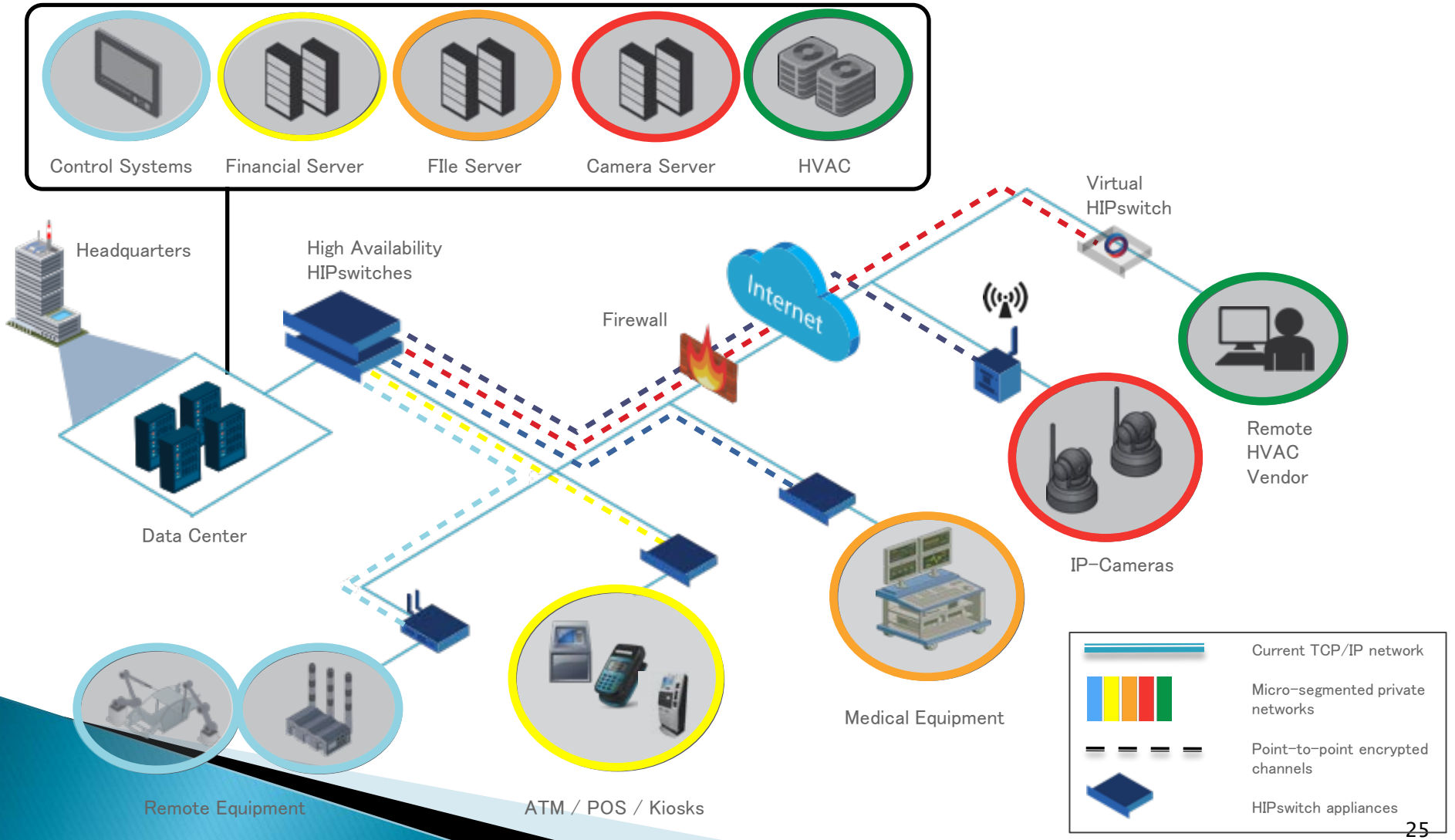
Agenda

1. Tempered Networks社紹介
2. ネットワークにおけるセキュリティ課題
3. 製品コンセプト
4. HIPとは？
5. 製品構成
6. 製品ラインナップ
7. 適用分野
8. 導入事例

適用分野

- 製造分野（重工メーカ、自動車メーカ等）
  - 自動化に伴う生産重要インフラネットワーク
- 金融・流通分野
  - ATM/POS/Kiosk等店舗のネットワーク
- 社会インフラ分野
  - 電力/ガス/水道/交通/監視カメラの重要インフラ
- 研究機関分野
  - 学術ネットワークおよび研究プロジェクトの秘匿性
- インターネット利用のセキュアな通信分野
  - 既存VPNサービスの新たな選択肢

展開例


Control Systems
Financial Server
FIle Server
Camera Server
HVAC
Headquarters
High Availability
HIPswitches
Firewall
Internet
Virtual
HIPswitch
Remote
HVAC
Vendor
Data Center
IP-Cameras
Medical Equipment
Remote Equipment
ATM / POS / Kiosks
Current TCP/IP network
Micro-segmented private networks
Point-to-point encrypted channels
HIPswitch appliances

Agenda

1. Tempered Networks社紹介
2. ネットワークにおけるセキュリティ課題
3. 製品コンセプト
4. HIPとは？
5. 製品構成
6. 製品ラインナップ
7. 適用分野
8. 導入事例

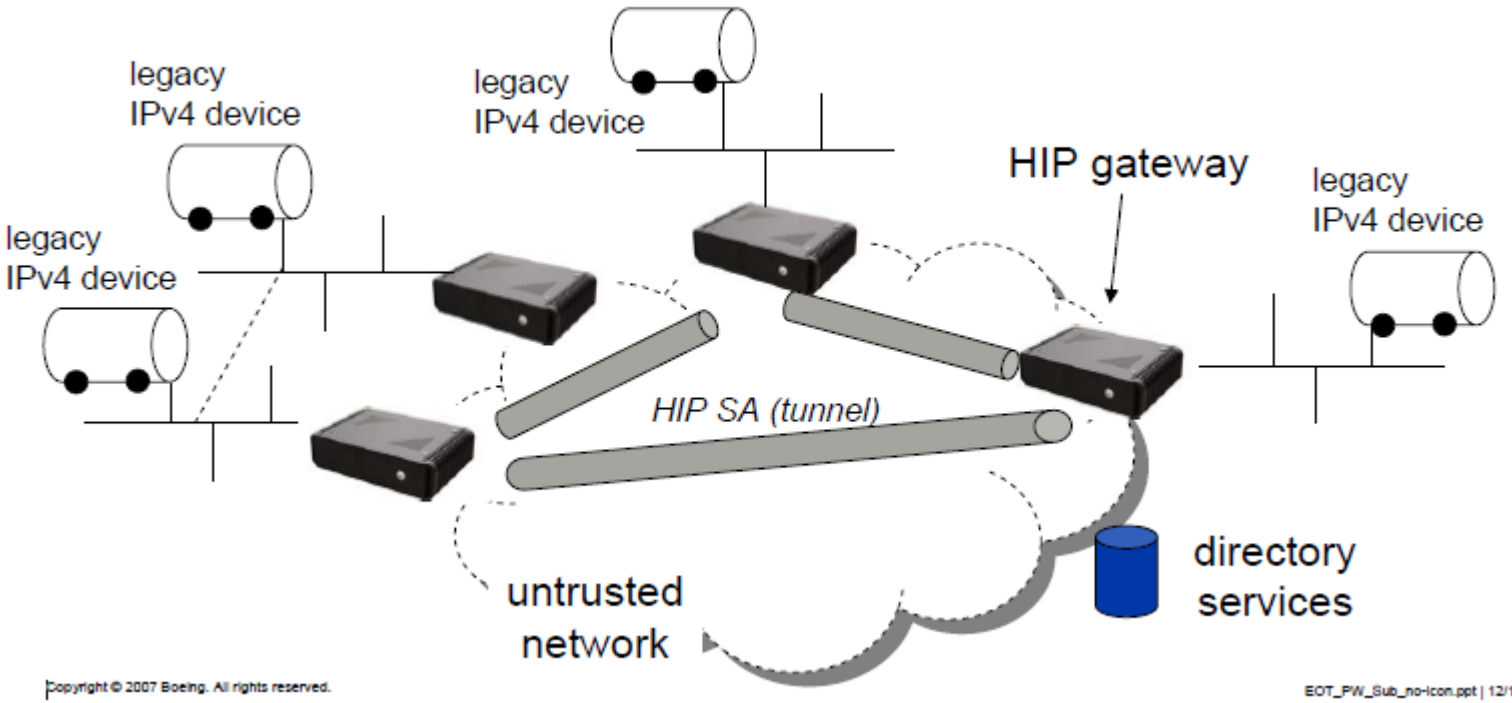
Boeingの事例（1）

- Boeing is using HIP as part of a Secure Mobile Architecture (SMA)implementation
- Provides secure connectivity to SCADAnet equipment over an untrusted factory wireless network

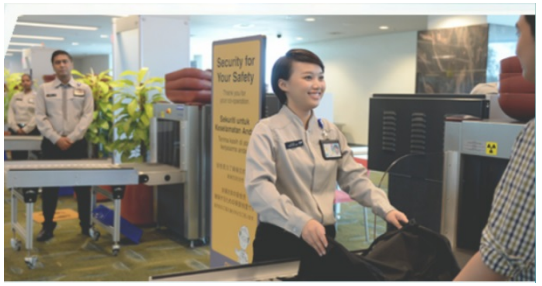
- 777 assembly line, Everett WA
- Supported by HIP overlays

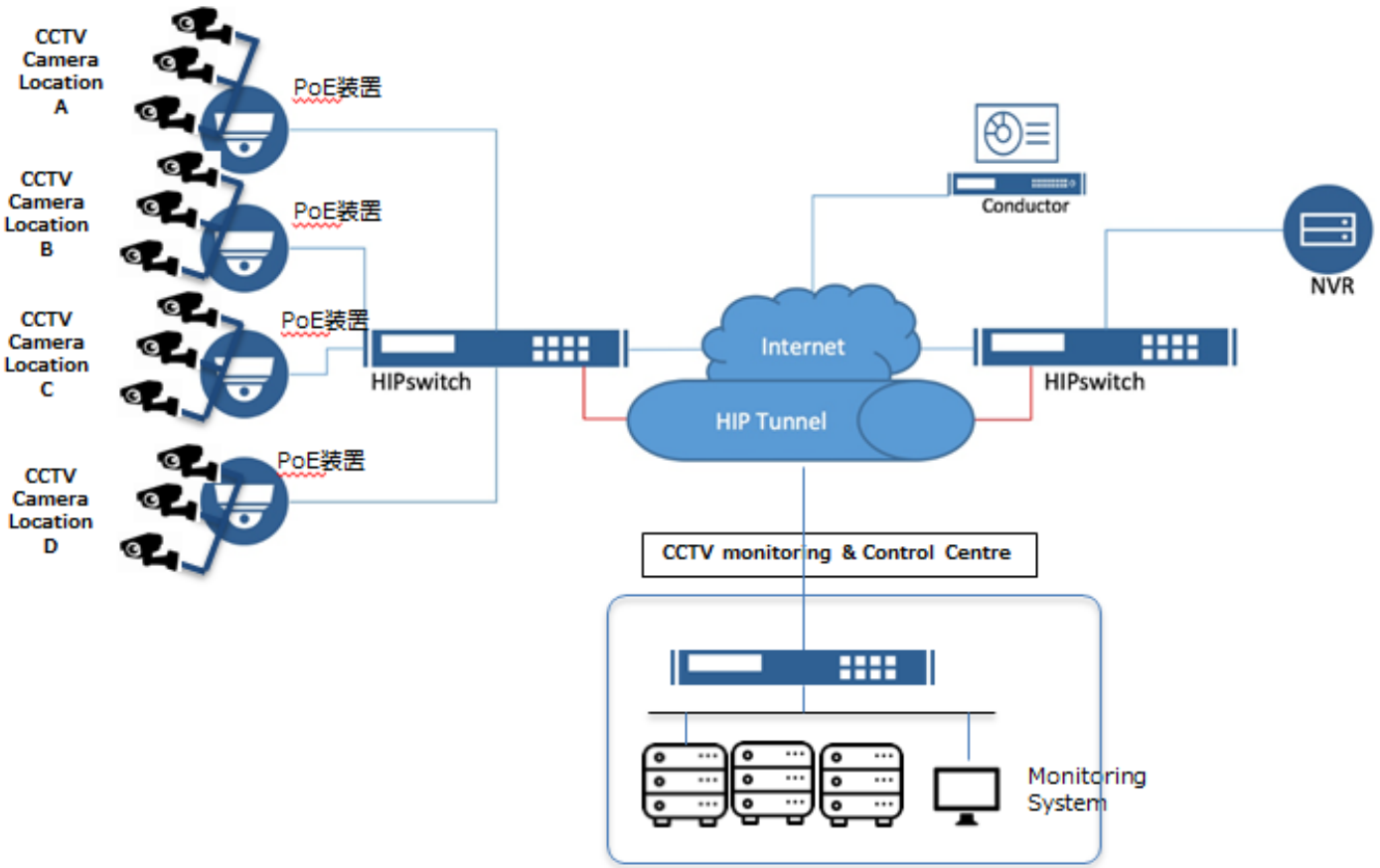
Boeingの事例（2）

- Provide layer-2 connectivity between SCADAnet (IPv4) devices

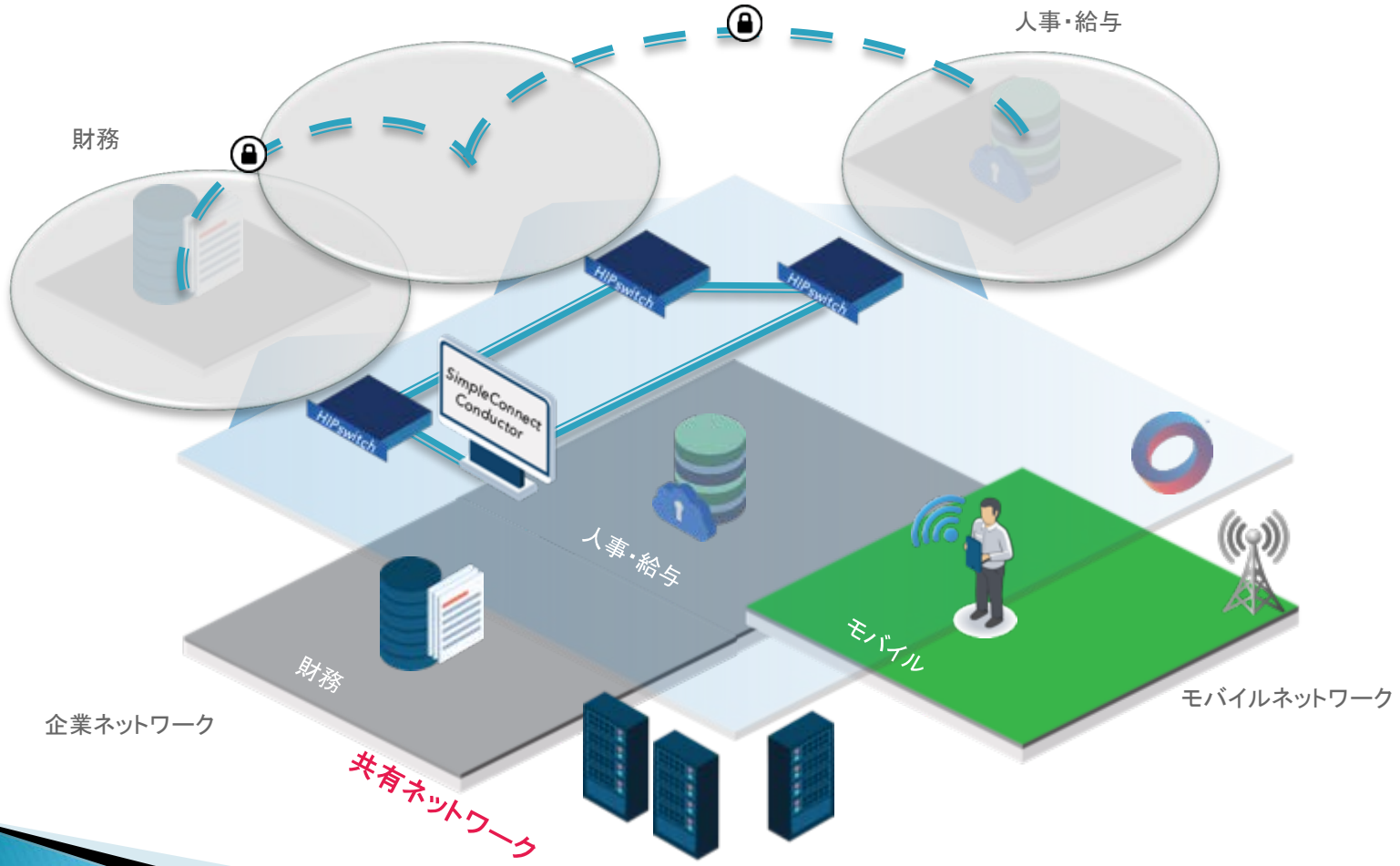


Certis Cisco（シンガポール警備保障）の事例





企業への導入例：人事と給与をクローキング（隠蔽）



Use Case:
アジア某銀行ATM/支店間のセキュア通信

課題

- ハッカーにとって容易でかつ価値ある攻撃ターゲットである
- 現状の脆弱の露出は銀行取引やコアシステムへの直接アクセスをハッカーに提供してしまう
- 不十分なネットワークレベルの暗号化とセキュアでないアクセス制御を使用して展開されることが多い
- 数千のエンドポイントを管理しているがセキュアでない
- 複雑なデータセンタのインフラで脆弱な穴がある
- レガシーシステムの維持と管理にはコストがかかる
- 既存のセキュリティシステムでは、十分な防御が出来ない場合がある

Tempered Networks の 価値提案

- ATM/銀行支店の重要なエンドポイントをセグメント化して隠す – トラステッドなシステムユーザ以外のユーザには見えない
- 攻撃の矛先を断ち切りセキュリティ環境とコンプライアンスを向上する
- １つのソリューションで複数の課題を解決 – AES-256暗号化とMACアドレスのロックダウン（封じる）によりセキュアな有線とセルラーの通信を実現
- オーケストレーション機能により設定・管理が簡単である
- データセンター運用の複雑さを軽減して既存環境のROIを守る
- 高価な専用線をインターネットに置換え支店/ATM本店間の通信をセキュアにしてコストを削減する
- 色々なユーザニーズに応える多様なHIPデバイス（アプライアンス、ソフトウエア、組込み型）を提供

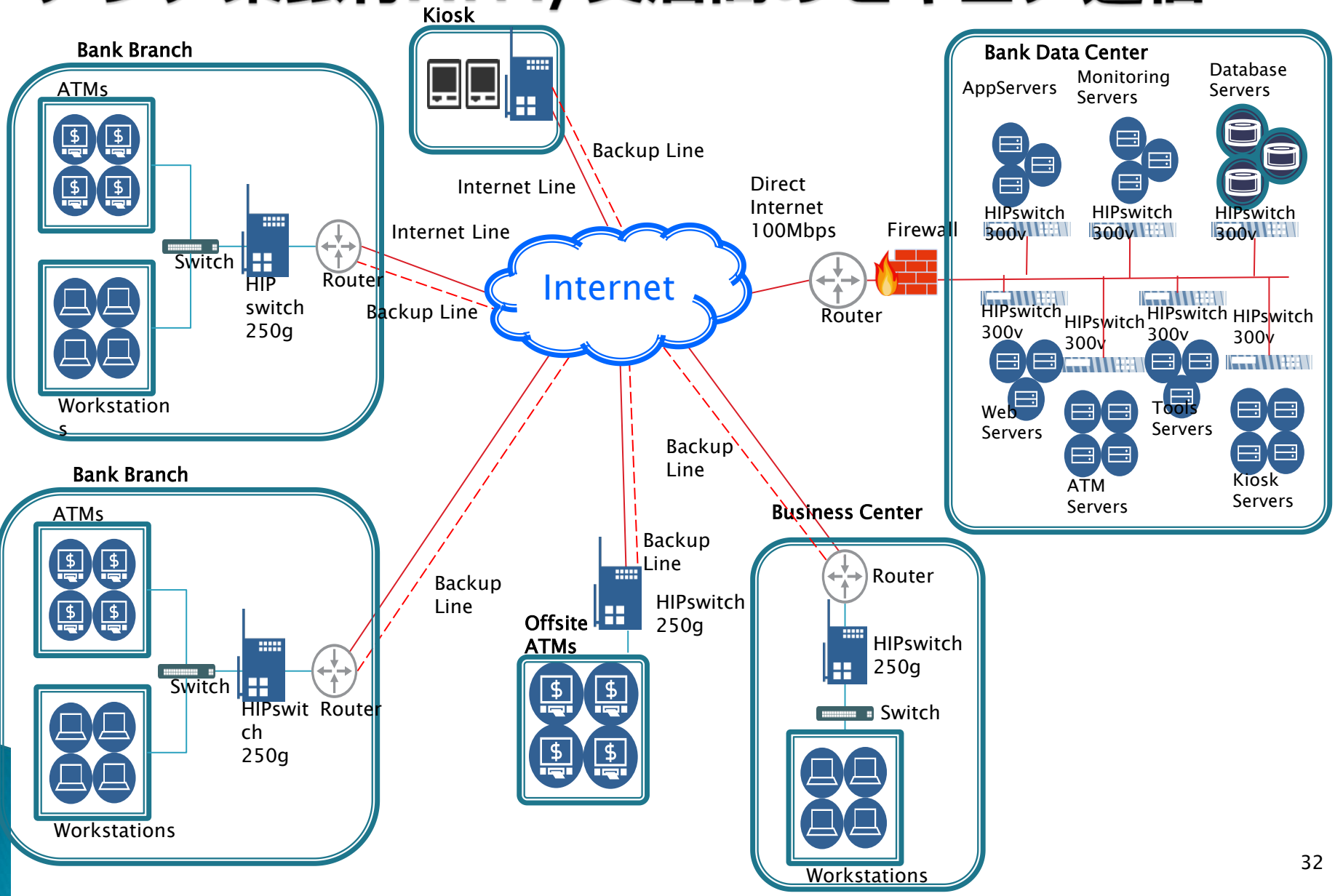
対応可能な市場

- 世界銀行の調査では、2014年、アジアでは160万以上の銀行ATMが設置されていると推定
- 設置が簡単で色々と応用できるソリューションアーキテクチャ
- アジアの銀行ではATMのネットワーク化が急速に拡大している
- ますます多くの機能がATMにプッシュされるので、システム環境に依存せずかつ容易な対応が可能なセキュアなソリューションニーズが必要
- 高度な手口による攻撃によって従来型のソリューションでは効果的に対処出来ないセキュリティ問題が発生

対象ターゲット

- 大規模なATMネットワークと拠点数の多い支店のある大手銀行
- 地理的に遠隔地に分散している拠点の多い銀行/ATM拠点
- 多額の維持・管理コストがかかっているレバシーシステムを使用している銀行
- 銀行インフラのセキュリティ対策の積極的に推進している政府系および一般の金融機関
- コンプライアンスの規制を必要としているところを探す
- 最近ATMハッキングされた金融機関/ATM

Use Case:
アジア某銀行ATM/支店間のセキュア通信



Use Case：
セキュアなPoS通信

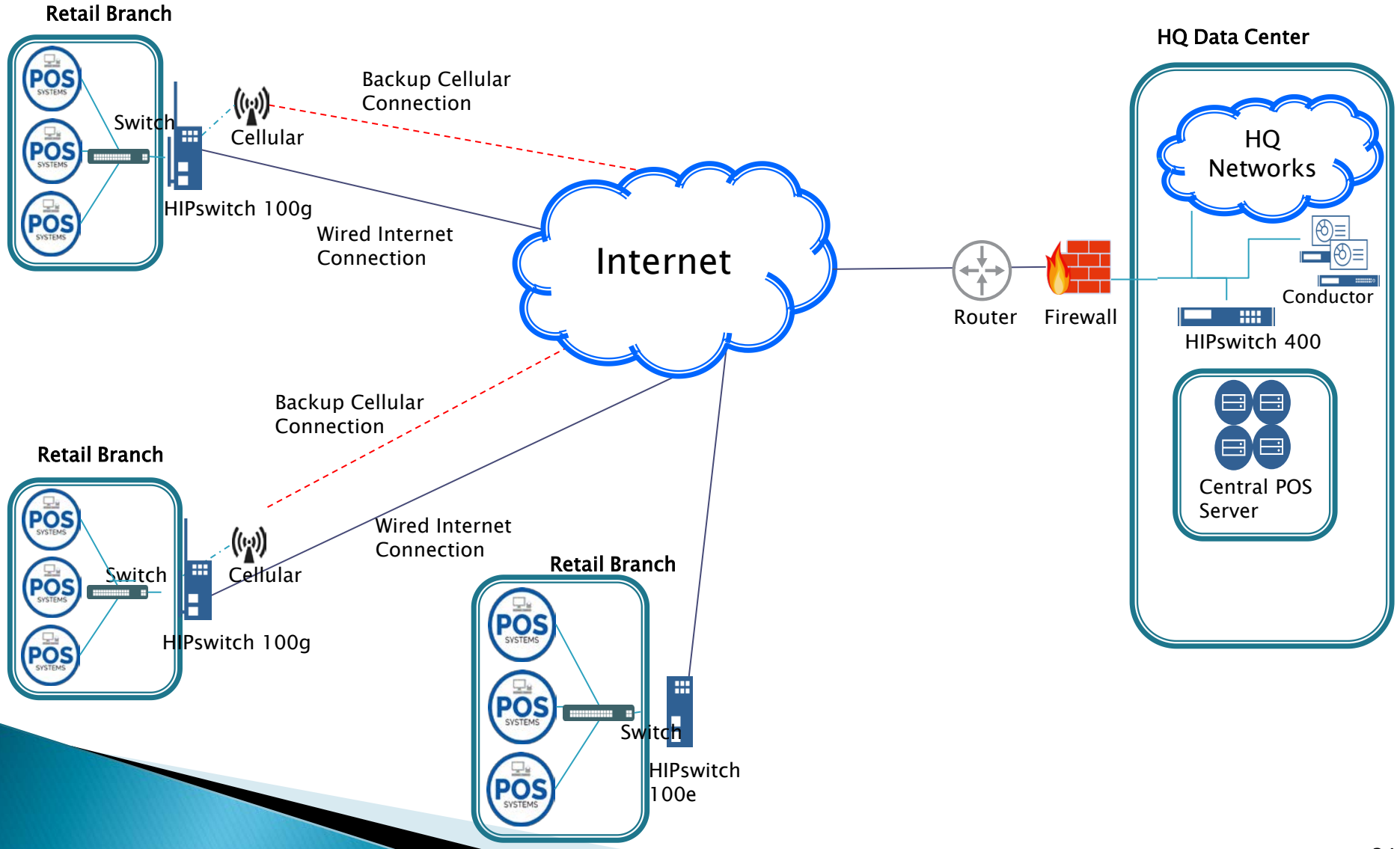
課題
- PoSシステムはハッカーにとって攻撃しやすく大きな損害を与えるターゲット
- ハンドヘルドPoSデバイスは簡単に盗難されたり、置き忘れやすくかつ紛失しやすい可能性があり、セキュリティ上のリスク増大につながる
- 貴重な資産情報の漏洩の可能性 (例：クレジットカード、顧客情報等)
- PoSシステムの脆弱性により中央決裁システム、取引データとか運用データに直接不正アクセスされやすい
- 多くの場合、遠隔地などの広大な地域に分散されておりセキュリティ管理が大変である
- 不十分なネットワークレベルの暗号化、不十分なアクセス制御とか脆弱なOSレベルでセキュリティ防御対策を展開している場合が多い
- 数千以上のエンドポイントのセキュリティ管理は大変である
- データセンターインフラのセキュリティ管理が複雑である
- 既存のセキュリティシステムは、しばしば、適切な防御および保護を提供しない場合がある

Tempered Networksの価値提案
- PoSエンドポイントのセグメント化と隠蔽（クローク）– ハッカーを含む他のユーザには検知されないので安全
- 攻撃アプローチの排除およびセキュリティ環境とコンプライアンス強化の向上
- １つのソリューションで複数の課題を解決 – AES-256暗号化とMACアドレスのロックダウン（封じる）によりセキュアな有線とセルラーの通信を実現
- オーケストレーション機能により設定・管理が簡単である
- データセンター運用の複雑さを軽減して既存環境のROIを守る
- 色々なユーザニーズに応える多様なHIPデバイス（アプライアンス、ソフトウエア、組込み型）を提供

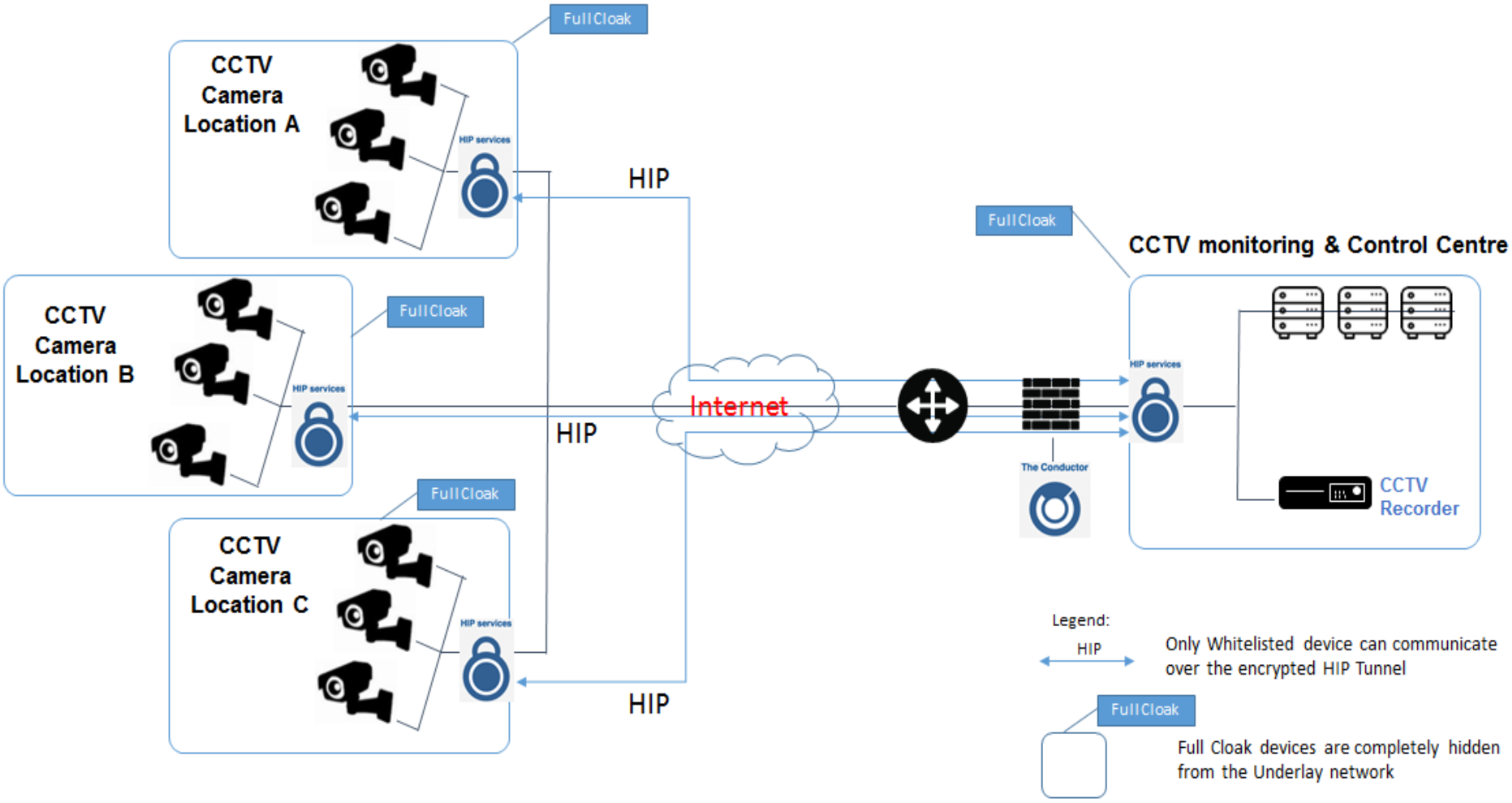
対応可能な市場
- アジア市場では流通のPoSシステムが急速に拡大
- 大手の流通チェーンは大都市では平均50～100の拠点あり
- PoSシステムは伝統的にセキュリティ対策が遅れている
- 最近、米国大手流通業者**Target**のPoSシステムで大規模なセキュリティ被害が発生。この事件が引き金になりPoSセキュリティニーズが高まった
- PoSのセキュリティ上の懸念を取り除くソリューションアーキテクチャを容易に構築したいニーズ

対象ターゲット
- 大規模流通チェーンとフランチャイズ店
- 地理的に遠隔地に分散している多数の拠点をもつ流通事業者
- 多額の維持・管理コストがかかっているレバシーシステムを使用している流通事業者
- セキュリティ対策の積極的に推進している流通インフラ
- コンプライアンス等の規制を必要としている流通事業者
- 最近PoSハッキングされた流通事業者

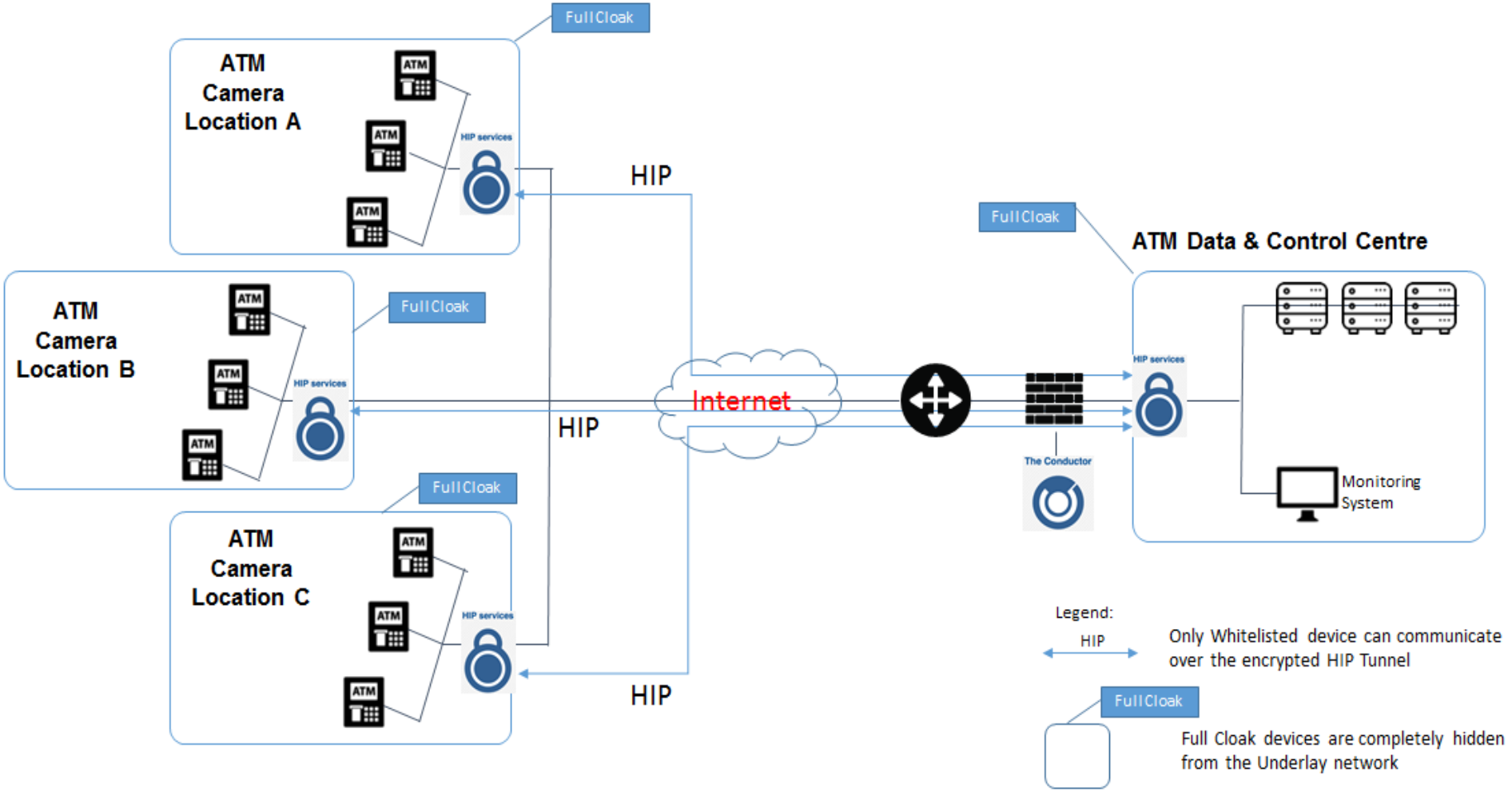
Use Case：
セキュアなPoS通信



ユーザ事例:
米国企業監視カメラのサンプル例



ユーザ事例:
米国金融関連監視カメラのサンプル例



まとめ

- オーバレイネットワークを通じてユーザが保護したいデバイスをホワイトリスト化してより堅牢なセキュア通信を提供（**Secure SDN**）
- 既存のIPネットワークからは完全に隔離され、登録したホストを“見えない”状態にする
- IP 通信(TCP/IP)に伴うセキュリティ問題を解決したはじめてのソリューション
- HIP標準プロトコルを業界で初めて商用製品に実装したベンダー
- 現行のVPNとは異なり設定手続きが簡単で、かつ1:1と1:anyでのメッシュ網による暗号化オーバレイネットワーク通信が可能
- ボーイング社内プロダクションで10年以上の稼働実績あり
- モバイルとかIoT分野にもビジネス展開可能（ソフトウエア版）

販売パートナー

Direx
JAPAN DIREX CORPORATION

日本ダイレックス株式会社 認証取得ISO900
東京都江東区青海2-4-32 タイム24ビル4F

■日本ダイレックスについて
日本ダイレックスは日本ではじめてのネットワーク・システム・インテグレータとして、
創業以来40年以上にわたり、情報通信ネットワーク・システムの未来を研究し、
独自のネットワーク商品を研究開発してまいりました。

お問合せ
TEL 03-3242-3157
Email sales@direx.com

TRILOGY
In collaboration with customer