

Always be Effective,
Always be the best

お客様のニーズへ最適な最先端ネットワーク/セキュリティソリューションを



Tempered Networksご紹介

～IDN (SecureSDN) ・ネットワーク分離・暗号化～

2018年

株式会社テリロジー

スマートビジネス営業部



ステルス化
隠して見えなくする！

ステルス化技術のポイント

デバイスをネットワーク的にステルス化



攻撃対象として認識させない

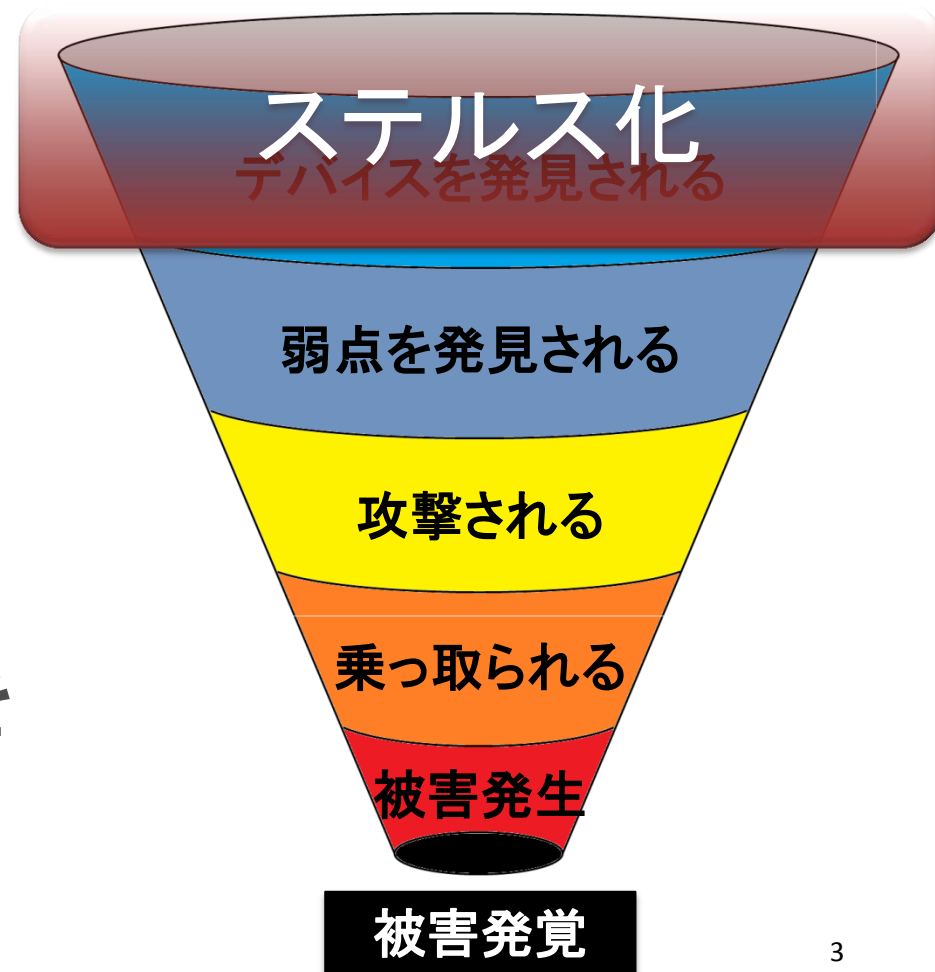
許可デバイス以外とは通信させない
ホワイトリスト化



探索の妨害、被害拡大防止

サイバーキルチェーンを
第一段階から抑制

IoTデバイスの サイバーキルチェーン



TemperedNetworks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)
- 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

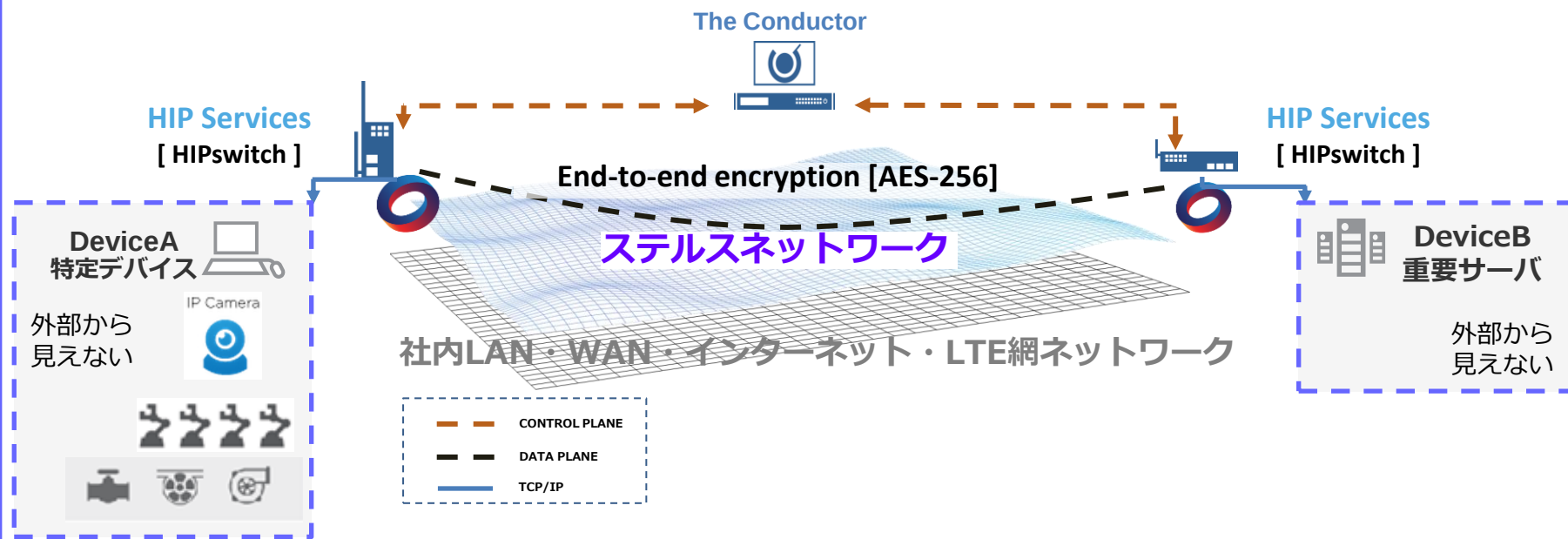
- ▶ 市場での実績

- 米国内で社会インフラや流通系、金融機関など既に約80社以上
- 納入・稼働中

製品コンセプト

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



製品コンセプト:ソリューション背景

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

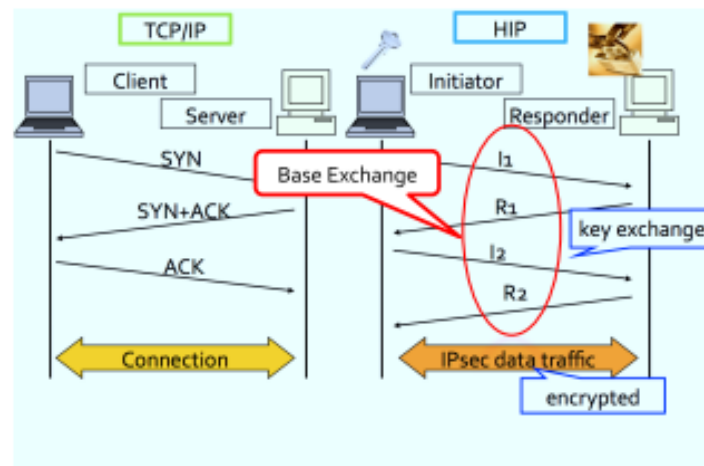
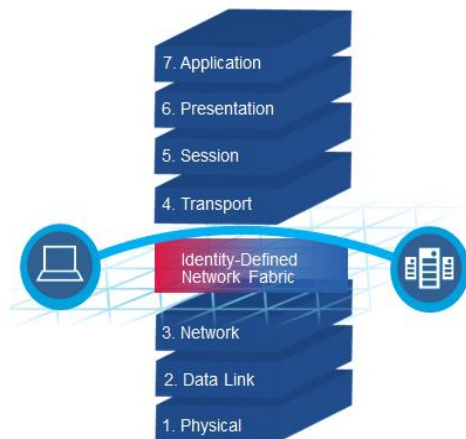


HIP (Host Identity Protocol)とは?



- プロトコル番号 : 139 RFC : 5201/7401
- HIPは識別子（誰が）とロケータ（位置情報）の分離をコンセプト
 - ⇒ホストは2048bit の RSA 公開鍵を使って強力的に暗号化して識別
 - ⇒ロケータは IPv4 または IPv6 アドレスを利用
- 当初からセキュリティを考慮して作られた、HIPで通信する端末間は
端末認証・トンネル・エンドツーエンドで暗号化（ESPモード）される

OSI Model



HIPのポイント

■ IDとロケータの分離

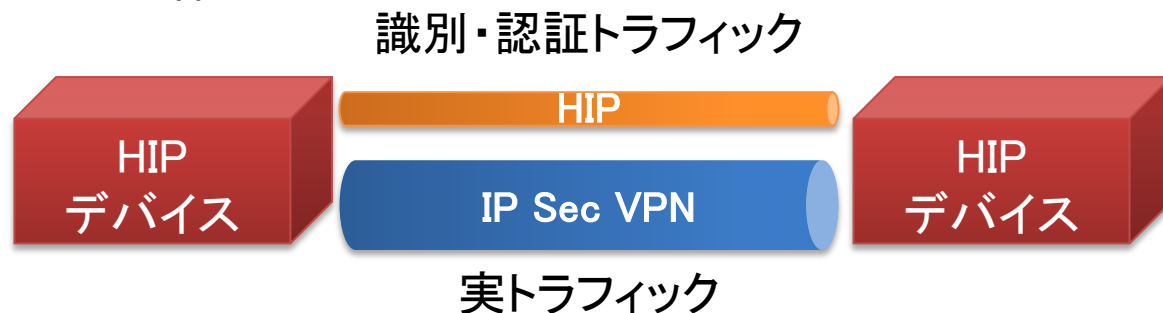
IP通信におけるIPアドレスは、ネットワークにおけるロケータ情報と相手を識別するID情報の2つの役割がある

HIPはID情報をHIPプロトコルで識別・認証を行い、IPアドレスとID情報をリアルタイムで紐付けることで、ロケータ情報をID情報を分離

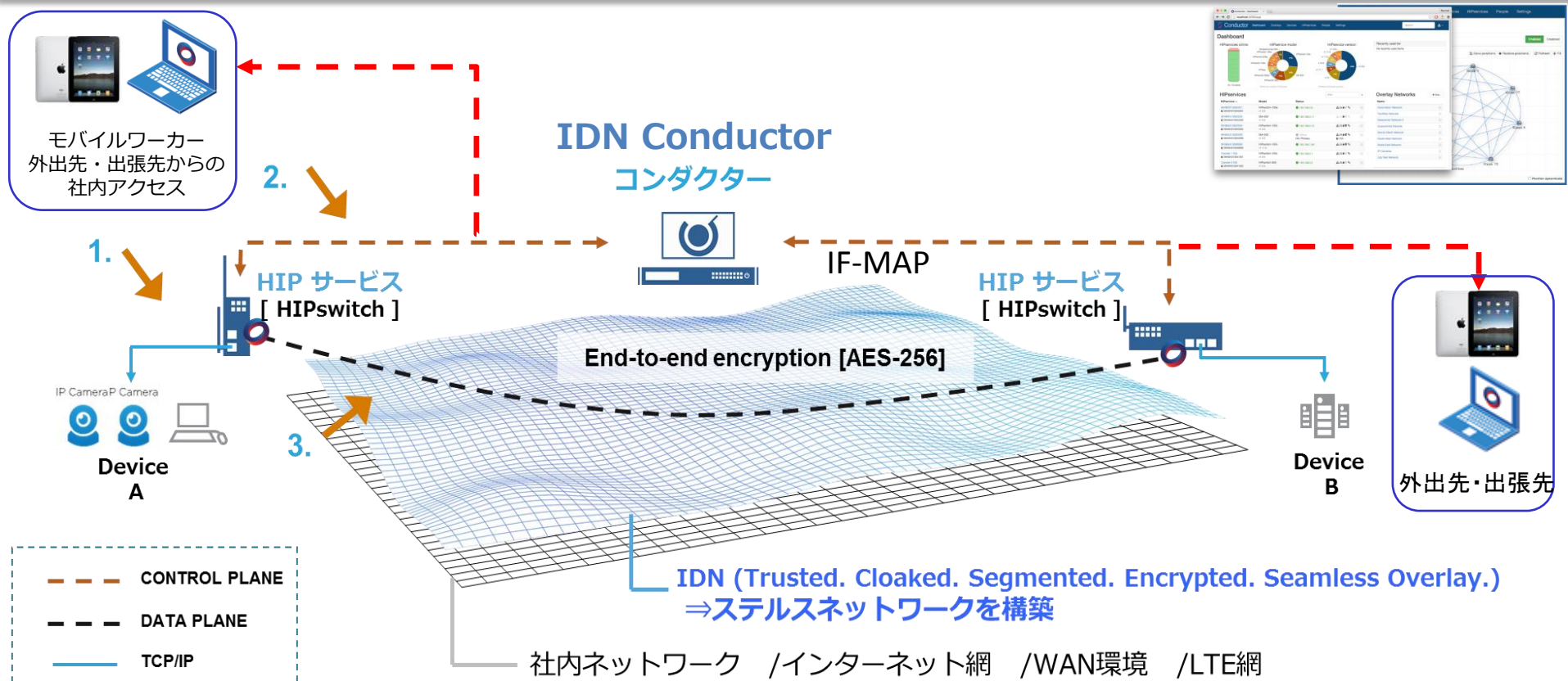
■ ID情報と実通信の暗号化

TCP/IPベースの通信は標準では暗号化はされず、全てオプション

HIPの場合、標準でID情報（独自）と実通信（IPSec）による暗号化を行うことで、安全性を確保



ソリューション構成



1. HIPサービスの配下で保護されたIoTデバイスの設定

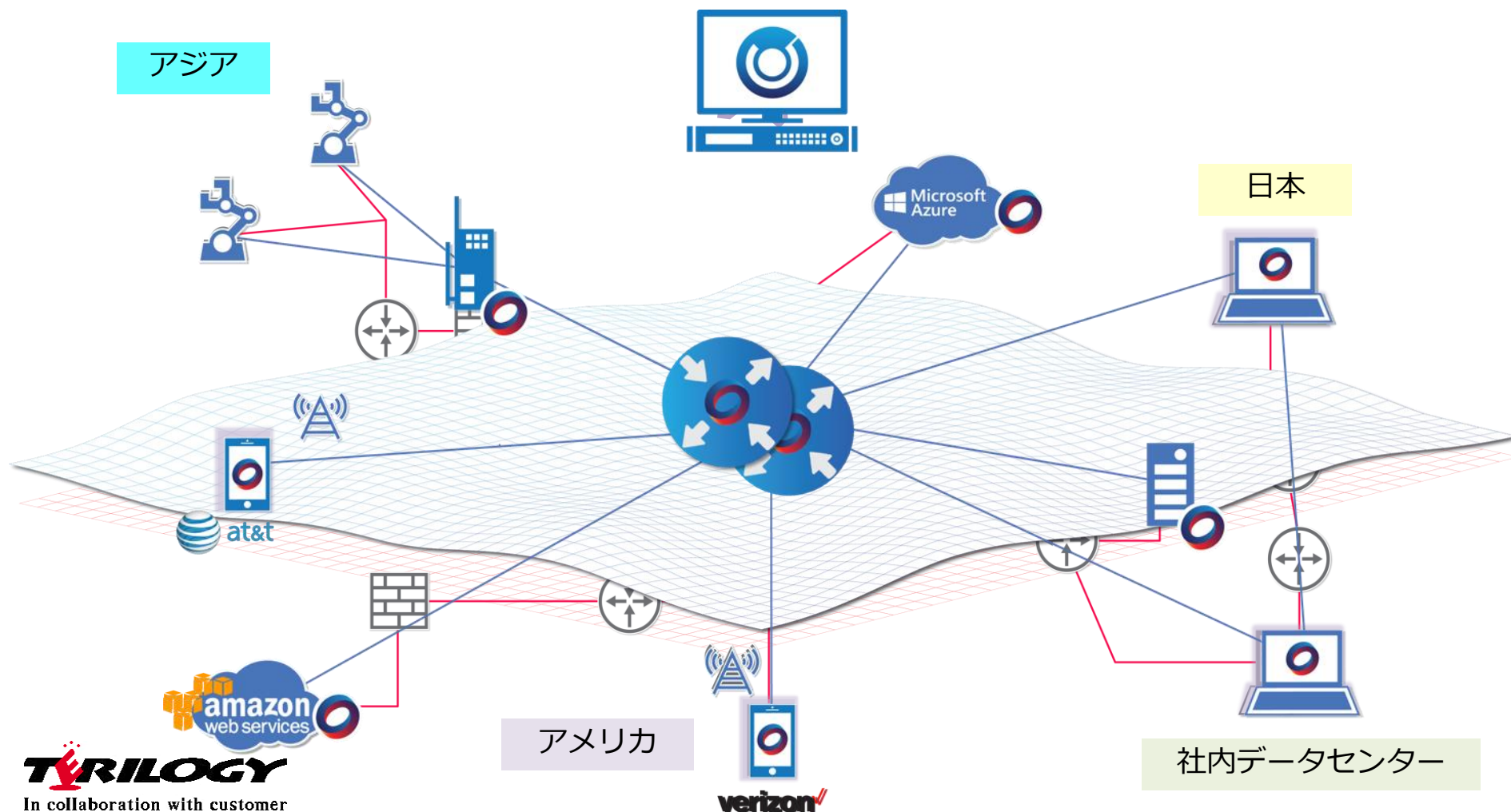
2. 認証可能なアイデンティティに基づく構成とポリシー管理を簡単に推進します

3. HIP サービスは、互いに認証・証明書ベースのカプセル化セキュリティペイロード（ESP）で保護されたトンネルを構築します。

認証による通信先の識別 /ステルス化によるデバイスの保護 /暗号化によるセキュアな通信

ソリューション構成 : HIP-Relay

- IDNルータとして機能。HIPService間で直接のIPリーチャビリティがない環境においてもRelayが通信を中継しHIP通信を可能にする
- Cloud版/VA版/HIPswitch400にアドオン



TemperedNetworksソリューション用途

“マイクロ
セグメンテーション
VENDOR NET”

“容易にセグメント化、
暗号化そしてIPモバイル利用”

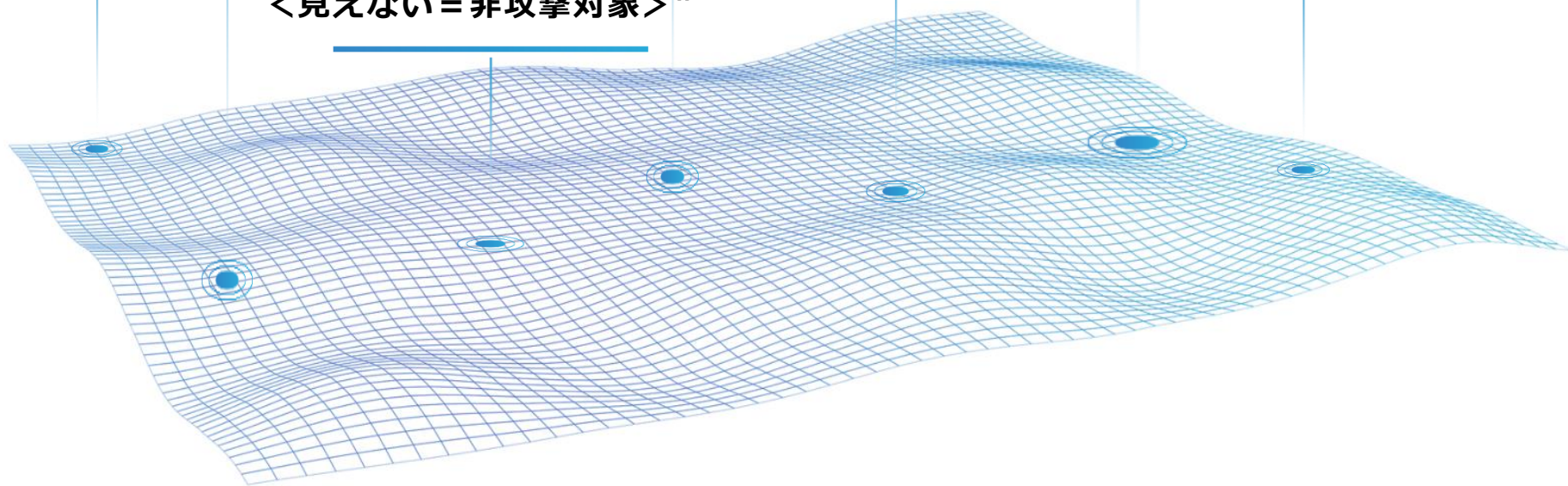
“ネットワーク仮想化 & オーケストレーション - 迅速な設定管理”

“セキュアな
M2M通信

“IoTデバイスを外部から見えなく
く見えない = 非攻撃対象>”

“レガシーシステムの
隠蔽と保護”

“迅速なデザスタリカバリー、
ネットワーク分離&検疫”



製品ラインナップ



IDN Conductor
IDN Conductor for AWS
IDN Conductor for ESXi



HIPswitch 100
(10M)



HIPswitch-250
(10M/25M/50M/100M)



HIPswitch-400
(1G/3G)



HIPswitch-500
(1G/3G/5G)



HIP switch /1G
for AWS (Cloud)
for Azure (Cloud)
for Google (Cloud)
for Hyper-v (VA版)
for ESXi (VA版)



HIPclient
Windows 7, 8 or 10
Macintosh X / iOS



HIPserver for
Windows Server 2008 R2, or 2012 R2
Linux

～ Subscription (HW・年間ライセンス) ～

- ・ Subscriptionライセンスにはメンテナンスサポートが含まれます。
⇒ (後出しSB/QA対応/バージョンアップ版の提供)
- ・ ハードウェア1台に付き、1subscription必要。※予備機に関してはライセンスフリー (無償)

適用分野

- 製造分野（重工業メーカー、自動車メーカー等）
 - 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：**（PCI-DSS準拠）**
 - 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

本ソリューションのターゲットユーザ

NISCでは、下記を重要インフラとして13分野を特定

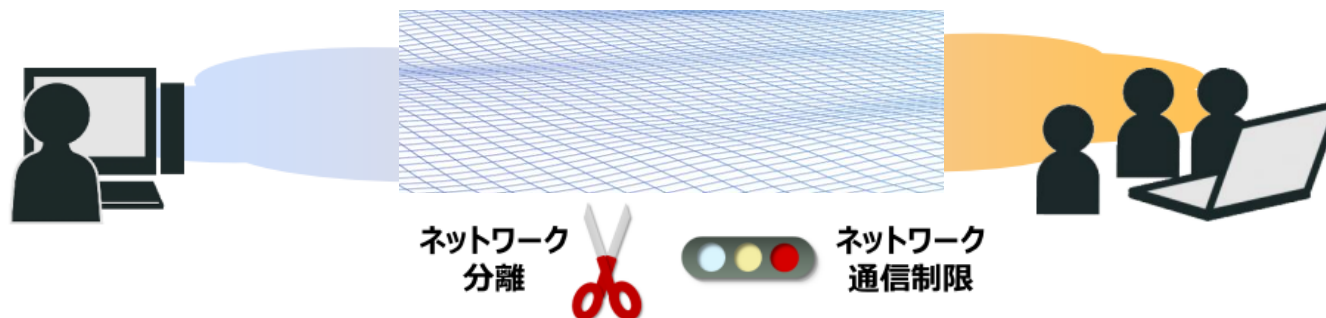
⇒「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」



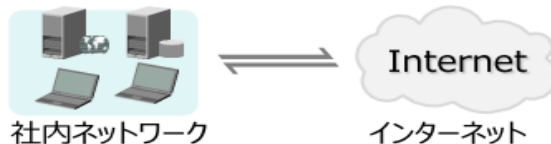
セキュアでステルス（見えない）なネットワークを提供

NW分離・暗号化通信を必要とされるお客様

- ✓ セキュリティ管理のためにセキュリティレベルの異なるネットワークを分離して通信を制限する



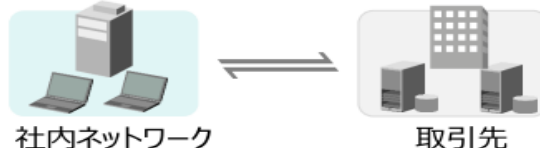
- ✓ インターネットとの接続



- ✓ 制御システムネットワーク接続



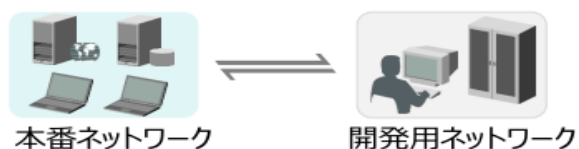
- ✓ 企業間接続（B2B接続、保守用途）



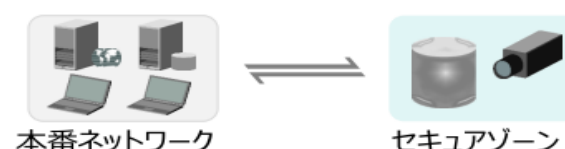
- ✓ 研究開発ネットワーク（最重要機密）



- ✓ 本番環境と開発環境の接続



- ✓ 機密情報管理ネットワーク（大量機密）



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
- 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（ソフトウェア版）

ユースケース①: 医療

◆マイクロセグメンテーションによる医療データの保護

課題

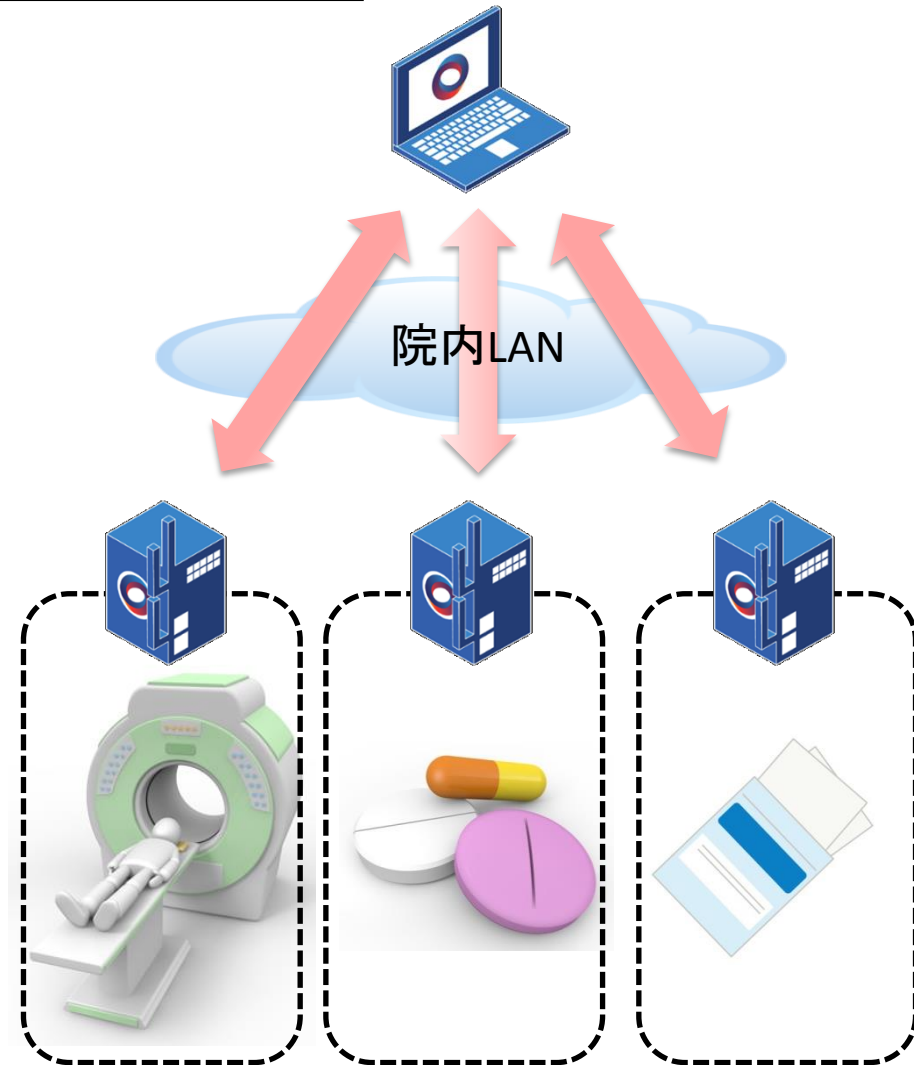
- カルテや医療機器のIT化が進んだが、患者の医療データを安全に扱いたい

ソリューション

- HIPスイッチによる医療システム単位でマイクロセグメンテーション化

ポイント

- HIPスイッチを設置するだけで医療システム単位でのマイクロセグメンテーション化が可能



ユースケース②: 端末のNW分離

◆ HIPクライアントによるマイクロセグメンテーションとNW統合

課題

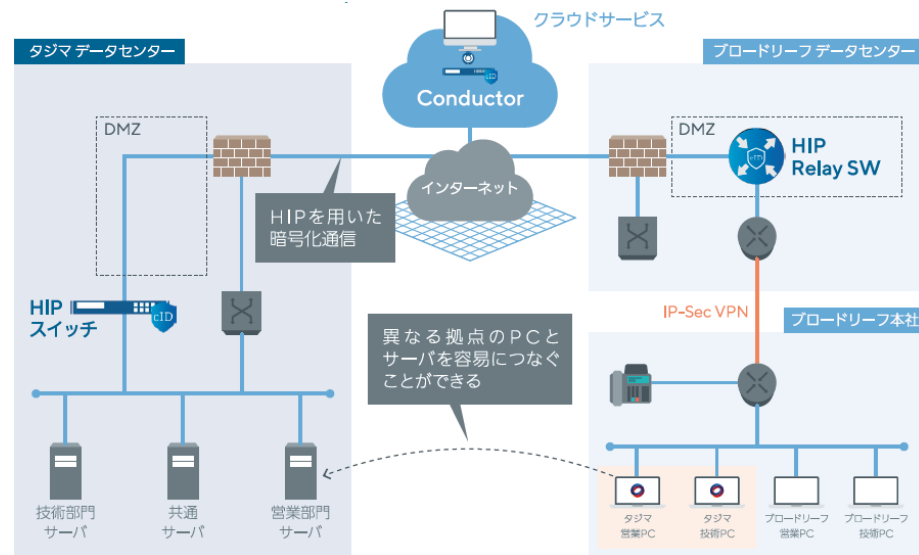
- M&Aにより事務所の統合をしたが、システムが異なるのでユーザー単位でNWを分離したい

ソリューション

- HIPスイッチとクライアントによりユーザー単位でのマイクロセグメンテーション化

ポイント

- HIPスイッチとHIPクライアントを利用するだけなので既存NWに変更を加えず短期間でマイクロセグメンテーション化が可能



ユースケース③: 監視カメラのステルス化

◆ステルス化による監視カメラの保護

課題

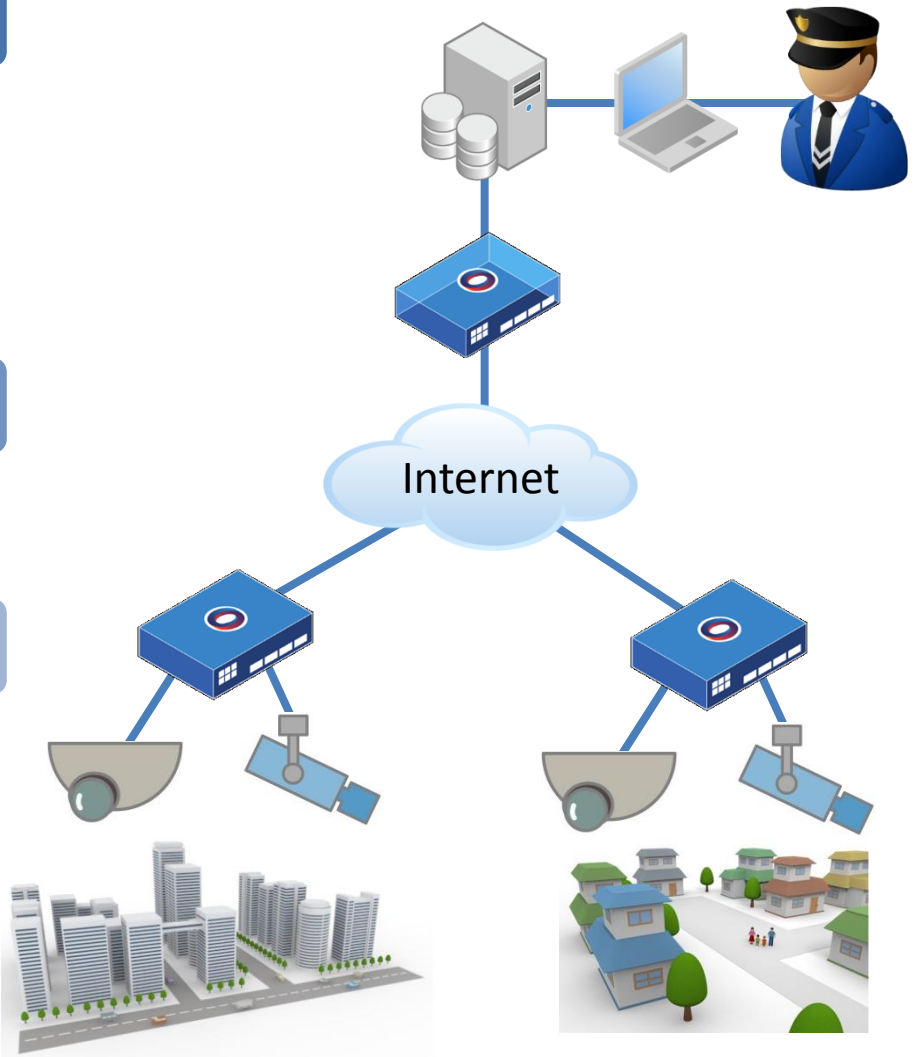
- 大量に存在する街頭の監視カメラをサイバー攻撃から守りたい
- 安価な回線を使用しつつ監視センター間の通信をセキュアにしたい

ソリューション

- HIPスイッチで監視カメラをステルス化しサイバー攻撃を阻止

ポイント

- HIPのステルス化によりインターネットから監視カメラの不可視化
- ホワイトリストと暗号化による映像データの保護



ユースケース④：異なるポリシーのNW接続

◆マイクロセグメンテーションとHIPトンネルによるNW接続

課題

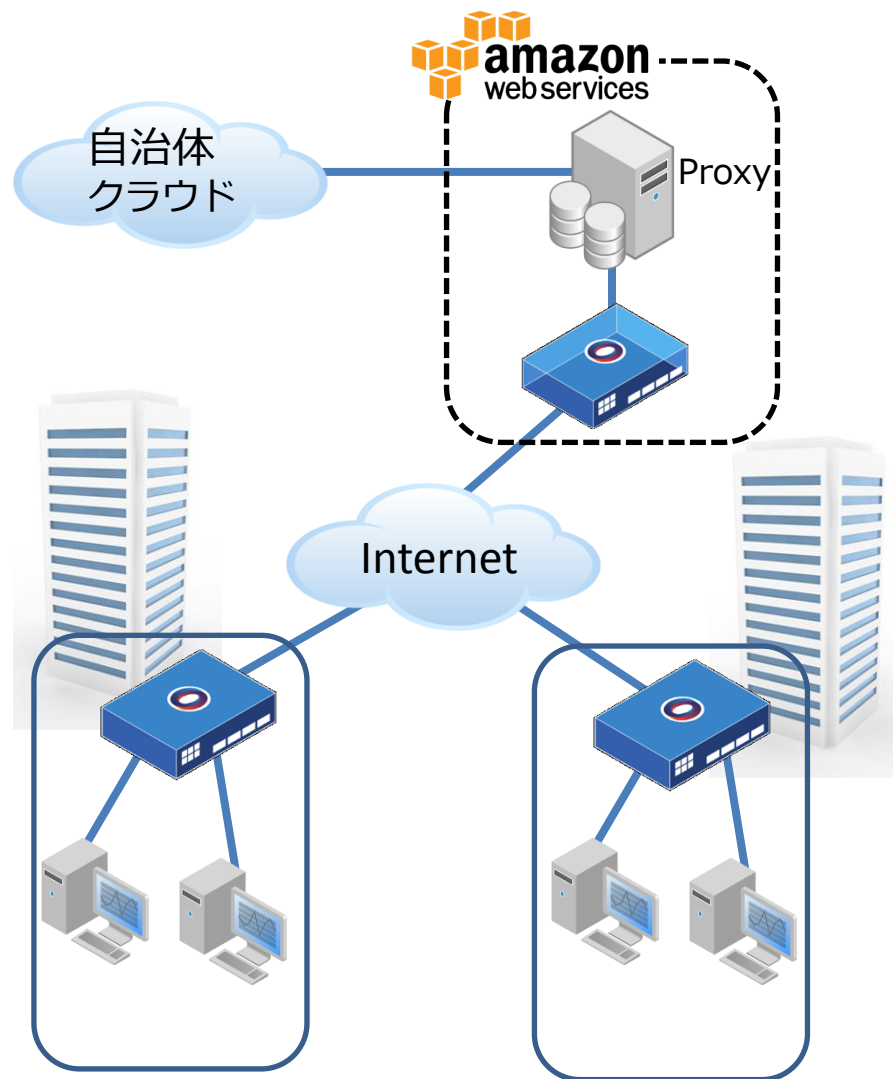
- 自治体システムの運営を委託されているが、自治体側と自社の異なるセキュリティポリシーを共存させる必要がある

ソリューション

- HIP Switchによる機器のマイクロセグメンテーションとホワイトリスト設定による通信端末の限定

ポイント

- 既存NWを使用したまま、NW分離の実現
- AWS環境を利用したサーバレス構成



ユースケース⑤:LTE網を利用したSD-WAN

◆ステルス化とLTE網によるガントリークレーンの制御と集中管理

課題

- ガントリークレーンへの貨物データの配信や制御の為、個別にUTM及びWifi網を設置していたが運用コストが高い上に個別の設定ミスによる事故を心配

ソリューション

- UTMからLTE対応のHIPスイッチへ置き換え

ポイント

- マイクロセグメンテーション化による安全性の向上と集中管理による運用コスト低減と設定ミス防止の両立



