HIPとは？

IDN（Identity Defined Networking）って？

The simplest way to securely network any “thing” to anything, anywhere.

Terilogy　/Takuma Miki

今日のお話し

HIPというプロトコル

×

Identity-Defined Networking（IDN）

ヒップ？

エイチアイピー？

HIPというプロトコル知っていますか？

独自プロトコル？

一覧 [編集]

10進数	16進法	略称	プロトコル	規格
0	0x00	HOPOPT	IPv6 Hop-by-Hop Option	RFC 2460
1	0x01	ICMP	Internet Control Message Protocol	RFC 792
2	0x02	IGMP	Internet Group Management Protocol	RFC 1112
3	0x03	GGP	Gateway-to-Gateway Protocol	RFC 823
4	0x04	IP-in-IP	IP in IP (encapsulation)	RFC 2003
5	0x05	ST	Internet Stream Protocol	RFC 1190, RFC 1819
6	0x06	TCP	Transmission Control Protocol	RFC 793
7	0x07	CBT	Core-based trees	RFC 2189
8	0x08	EGP	Exterior Gateway Protocol	RFC 888
9	0x09	IGP	Interior Gateway Protocol (any private interior gateway (used by Cisco for their IGRP))	
10	0x0A	BBN-RCC-MON	BBN RCC Monitoring	
11	0x0B	NVP-II	Network Voice Protocol	
12	0x0C	PUP	Xerox PUP	
13	0x0D	ARGUS	ARGUS	
14	0x0E	EMCON	EMCON	
138	0x8A	manet	MANET Protocols	RFC 5498
139	0x8B	HIP	Host Identity Protocol	RFC 5201
140	0x8C	Shim6	Site Multihoming by IPv6 Intermediation	RFC 5533
141	0x8D	WESP	Wrapped Encapsulating Security Payload	RFC 5840
142	0x8E	ROHC	Robust Header Compression	RFC 5856
143-252	0x8F-0xFC	UNASSIGNED		
253-254	0xFD-0xFE	Use for experimentation and testing		RFC 3692
255	0xFF	Reserved.		

これです！

出典: フリー百科事典『ウィキペディア（Wikipedia）』：プロトコル番号一覧

HIP（Host Identity Protocol）は・・・・

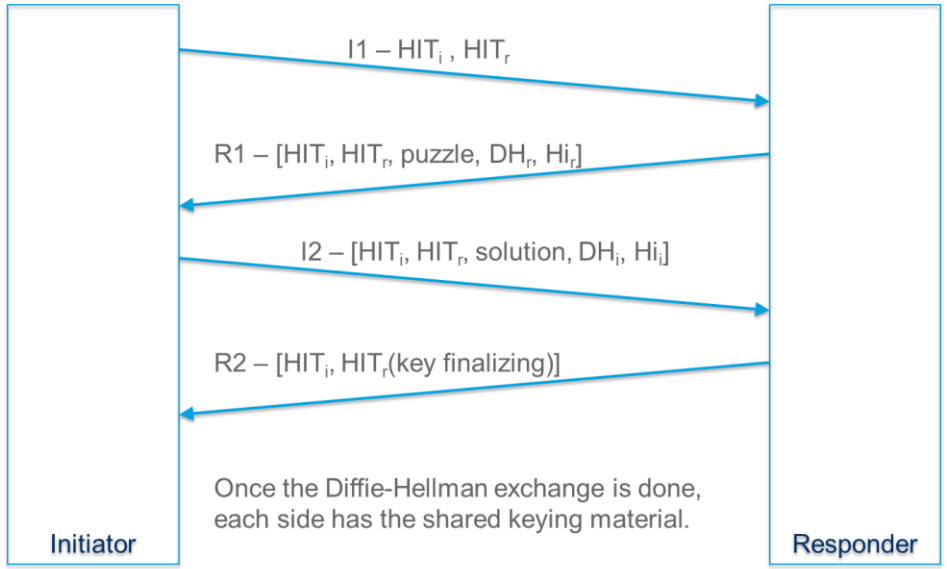
①ID（誰が）と　ロケーター（どこ）の分離をコンセプト

⇒セッションは必ず証明書ベースでのデバイス認証を実施　※誰とでも握手の3ハンドシェイクではない

⇒識別子を2048bit の RSA 公開鍵を使って強力に暗号化して、ユニークなIDとして識別

⇒IDを識別子、認証し、ホワイトリストに登録されたIDの相手のみと通信を実施

②HIPでセッションを張った後は、IPsec同等の暗号化（AES-256）で暗号化通信！



プロトコルにおける課題

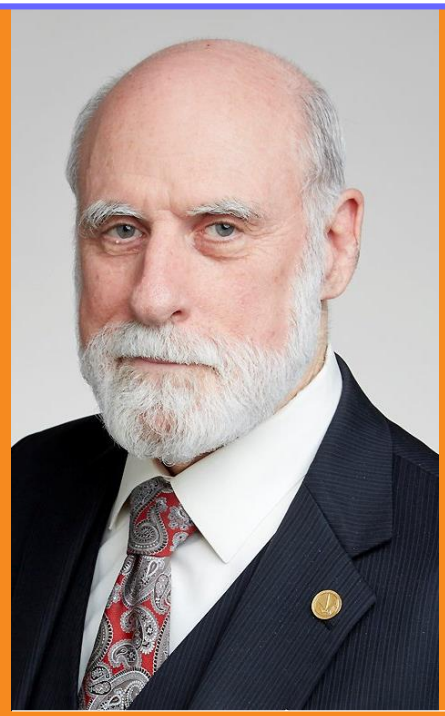
TCP / IPは、セキュリティやモビリティではなく、接続性のためだけに設計されています・・・

この方をご存知でしょうか？
HIPについて語っています！

EVERYTHING USES TCP/IP

BUT TCP/IP IS NOT

- ✕ Private
- ✕ Secure
- ✕ Mobile
- ✕ Simple



「もし時間を遡ることが出来れば、TCPの創生時に信頼できる認証とモビリティについてより良い仕事が出来ただろう。ただ当時、HIPというイノベイティブな考えは全く思いつかなかった」
byインターネットの父

VINT CERF
Co-Creator of the Internet & TCP/IP

TCPは繋げるを優先・・・　HIPはセキュリティを優先！

Internet 2.0 –
“Network everything”

アプリケーション (L5-L7)	IP Address: Port
トランスポート (L4)	IP Address: Port
ネットワーク (L2-L3)	IP Address
物理リンク (L1)	MAC address

UNTRUSTED
Connect First, ・・・ then Authenticate & Authorize

To a secure, mobile and private Internet

Internet 3.0 –
“Network ONLY CRYPTO-IDENTIFIED things”

アプリケーション（L5-L7）	**Host Identity Tag**: Port
トランスポート（L4）	**Host Identity Tag**: Port
Host Identity（L3.5）	**Host Identity Protocol (HIP)**
ネットワーク（L2-L3）	IP Address
物理リンク（L1）	MAC address

TRUSTED
Authenticate & Authorize First, ・・・ then Connect

では、このセキュアな HIPプロトコルを 使っている仕組みは？

“Identity Defined Networking” （ＩＤＮ）

SDNではないです・・・

Identity Defined Networking
（IDN）※通称：SecureSDN

① 簡単にセキュアネットワークを！※既存NW構成OK/IP重複OK!

② HIP による オーバレイNW＆ネットワーク分離 ＆ 暗号化通信

③ オーケストレーション＝センター集中の一元管理

④ 容易なマイクロセグメントを実現　～守りたい重要な個所を～

現在の堅牢なネットワークは、設計は、構築は、、、

セキュリティを気にしながら作られるネットワークは、手間で設定が面倒である

頑張る

ルータ＆ファイヤーウォールで頑張る

```
interface gigabitethernet 0/3
        nameif dmz
        security-level 50
        ip address 192.168.2.1 255.255.255.0
        no shutdown
same-security-traffic permit inter-interface
route outside 0 0 209.165.201.1 1
nat(dept1) 1 10.1.1.0 255.255.255.0
nat(dept2) 1 10.1.2.0 255.255.255.0
router rip
        network 10.0.0.0
        default information originate
        version 2
ssh 209.165.200.225 255.255.255.255 outside
logging trap 5
```

課題

Different:
- IP/DNS Namespaces
- Security Controls
- Networking Context
- Workloads
- Address-Defined

人日工数

VLAN職人によるコンフィグ作業

```
Router>enable
Router>#configure terminal
Router(config)#hostname CORP
ISP(config)#interface serial 0/0/0
CORP(config-if)#description link to ISP
CORP(config-if)#ip address 192.31.7.6 255.255.255.252
CORP(config-if)#no shutdown
CORP(config)#interface fastethernet 0/1
CORP(config-if)#description link to 3560 Switch
CORP(config-if)#ip address 172.31.1.5 255.255.255.252
CORP(config-if)#no shutdown
```

課題

Different:
- IP/DNS Namespaces
- Security Controls
- Networking Context
- Networks
  - Internet
  - MPLS
  - WiFi
  - Cellular

面倒

ACLを追加・変更・面倒・・

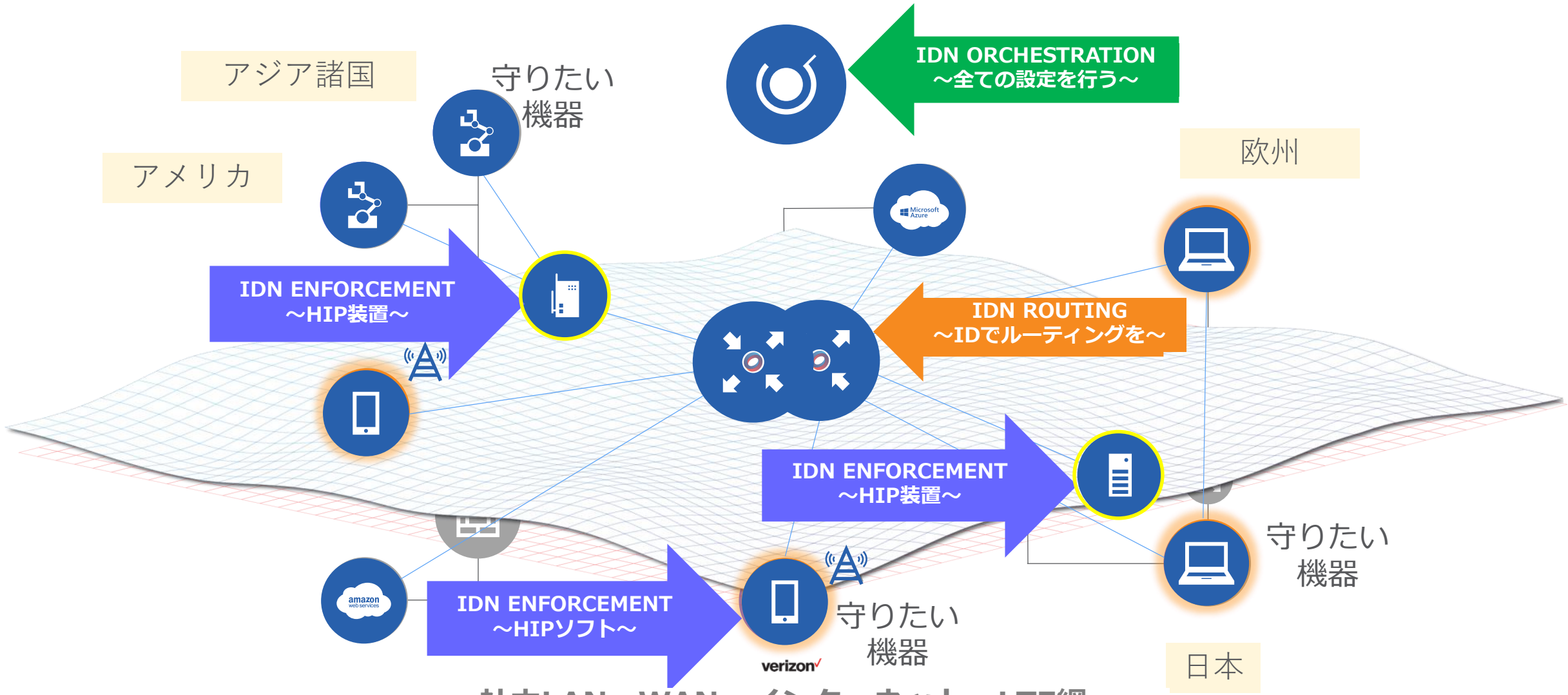
```
device(config)# ip access-list standard Net1
device(config-std-nacl-Net1)# deny host 10.157.22.26
device(config-std-nacl-Net1)# deny 10.157.29.12
device(config-std-nacl-Net1)# deny host IPHost1
device(config-std-nacl-Net1)# permit any
device(config-std-nacl-Net1)# exit
device(config)# int eth 1/1
device(config-if-e10000-1/1)# ip access-group Net1 in
```

VPNのルールをガリガリ・・・

作業・作業・作業

Identity Defined Networking

～いつでも、どこでも、容易にIDベースでセキュア接続を実現～



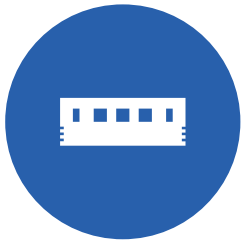
Identity Defined Networking platform

～容易にセキュアネットワーク接続・ネットワークセグメンテーション・NW管理を実現～

オーケストレーションエンジン

設定・変更を一元的に

IDN ORCHESTRATION

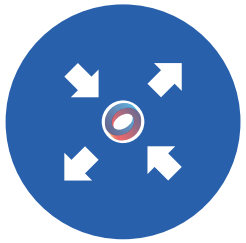


HIP通信機器＆ソフト

既存NWトラスペアレント

各デバイス/セグメントに配備

IDN ENFORCEMENT



IDルータ

復号化せずにプライベートまたは非ルーティングエンドポイント間のピアツーピア暗号化接続を許可します

IDN ROUTING

HIP × IDN

こんな使い方どうでしょう

こんなところで使えます！

マイクロ
セグメンテーション

End-to-End
暗号化ネットワーク

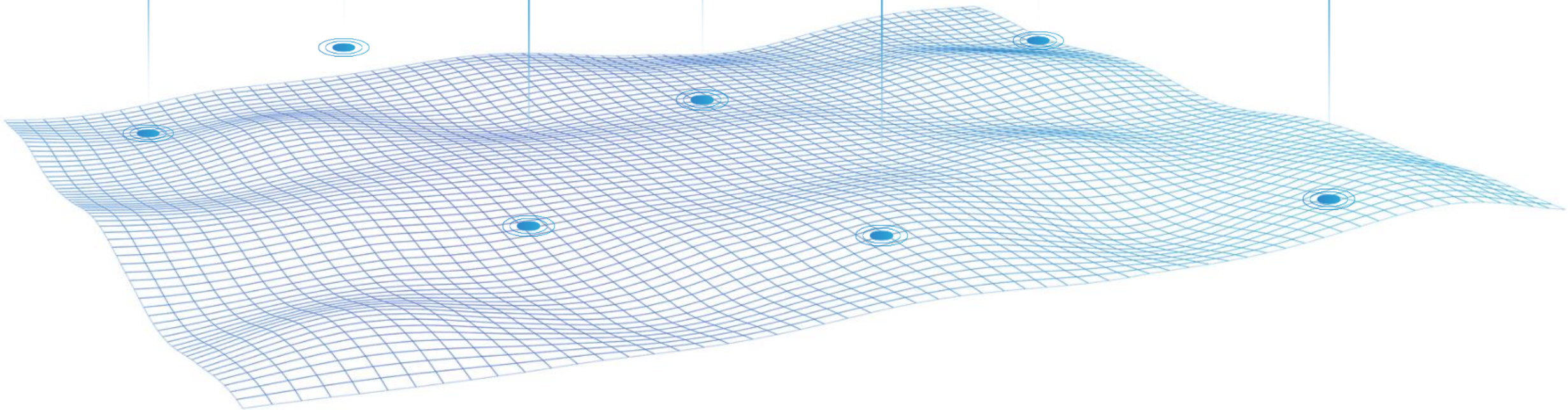
“セキュアネットワーク仮想化
& オーケストレーション

“セキュアなM2M通信

インターネットで
プライベートNWを

テンポラリ
セキュアネットワーク

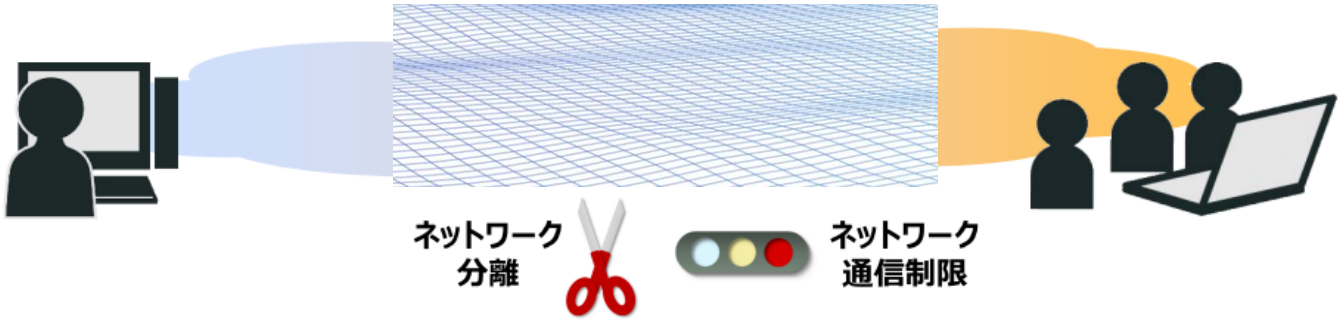
IoTデバイス向け
セキュリティ



こんな場合に簡単なセキュアネットワークのご利用！

～NW分離・暗号化通信を必要～

✓ 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）

Fin.

詳細及びご質問は下記までご連絡を

tmiki@terilogy.com　/　in 九段下