製造業へのローカル5G導入に伴うサイバーセキュリティリスク実証実験

～製鉄所を模した環境での侵入経路と被害の実態～

トレンドマイクロ株式会社
セキュリティエバンジェリスト
石原陽平

2021月10日26日現在の情報をもとに作成されたものです。
今後、内容の全部もしくは一部に変更が生じる可能性があります。

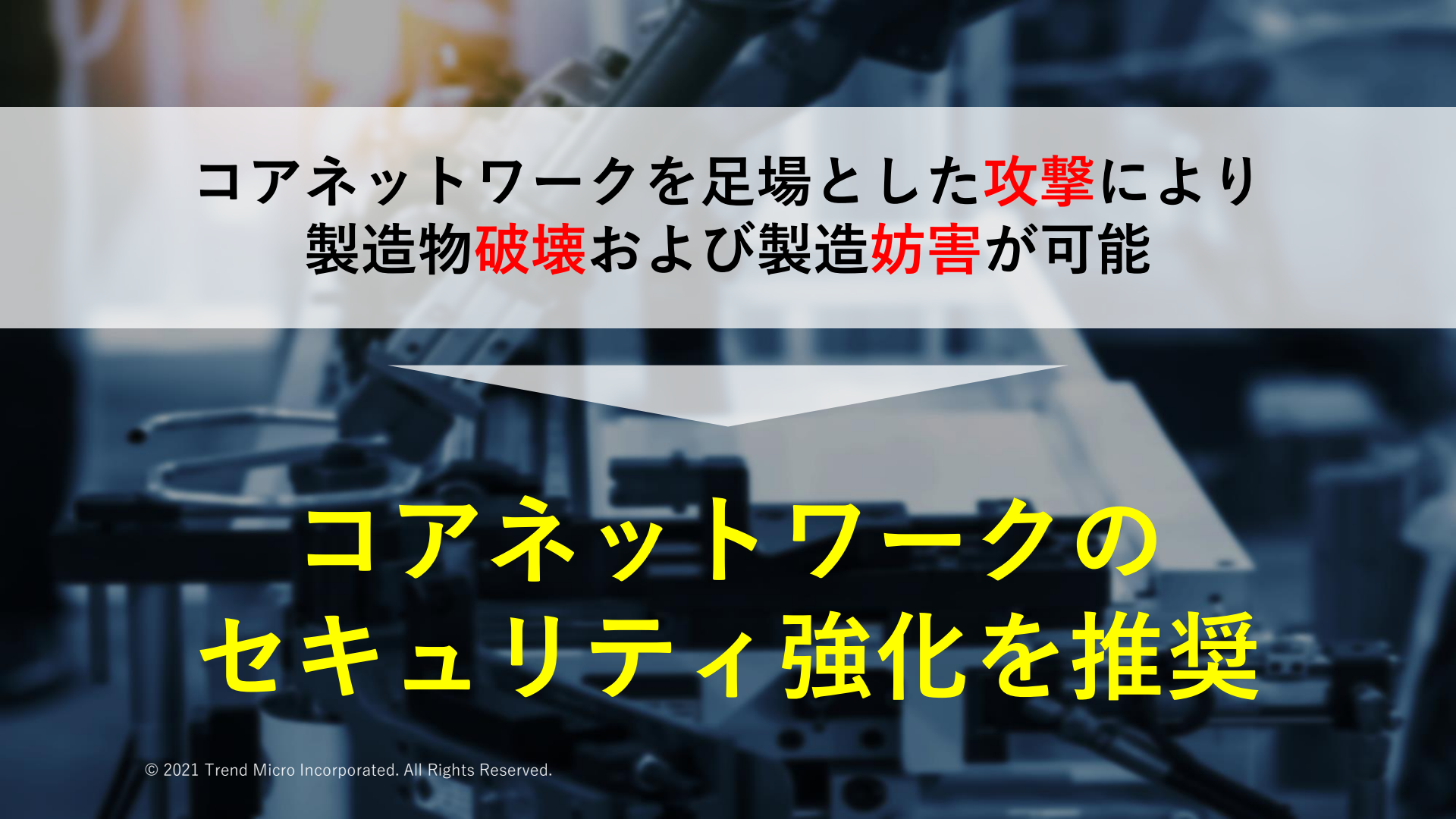
Attacks From 4G/5G Core Networks

Risks of the Industrial IoT in Compromised Campus Networks

Philippe Z Lin, Charles Perine, Rainer Vosseler
Trend Micro Research
Wen-Ya Lin
Institute of Information Industry

TREND MICRO | research

製造業における
ローカル5G環境導入に伴う
サイバーセキュリティリスクの
実証実験を実施

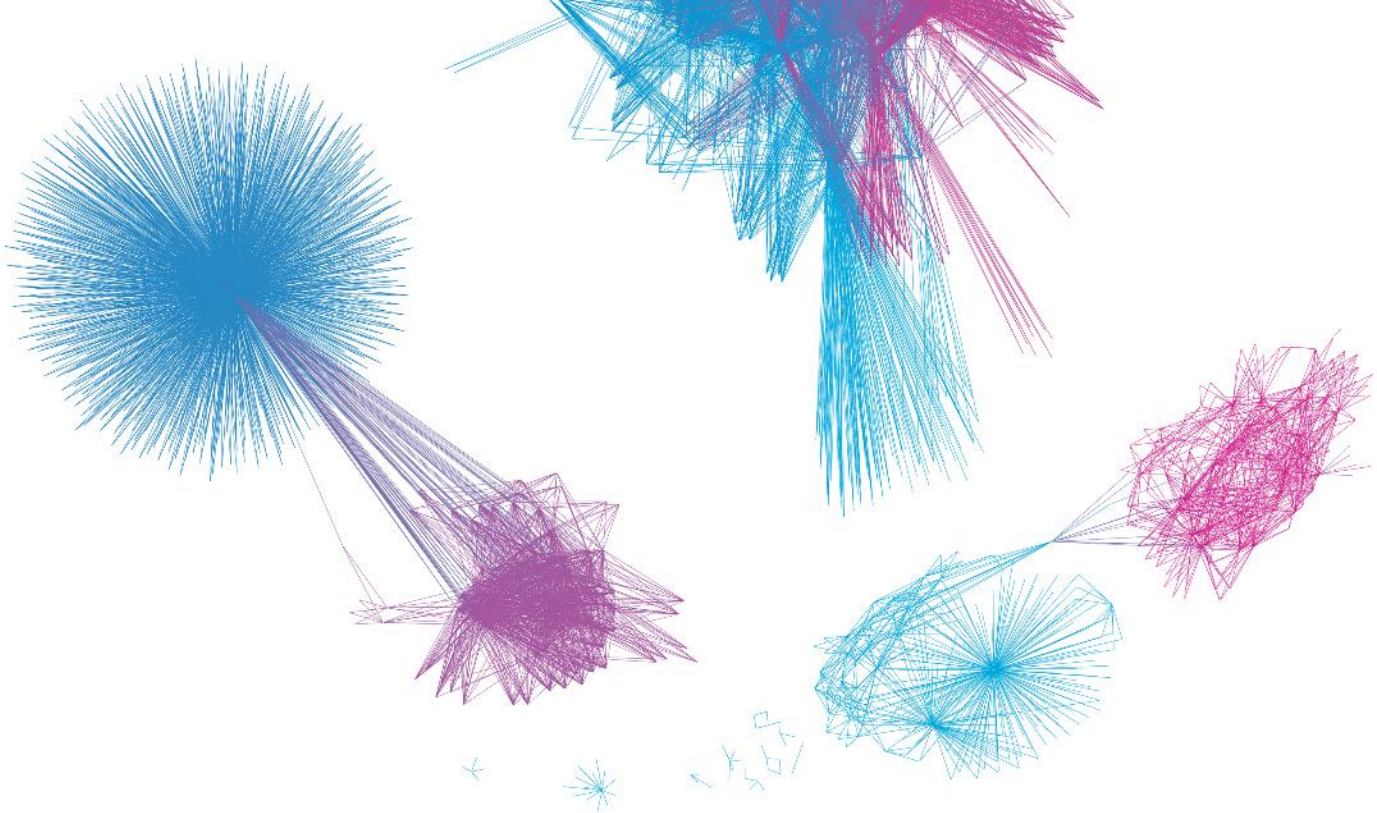


コアネットワークを足場とした攻撃により
製造物破壊および製造妨害が可能

コアネットワークの
セキュリティ強化を推奨

Agenda

1．ローカル5Gの構成要素
2．実証実験の目的と方法
3．実証実験の結果
4．推奨される対策



ローカル5Gの構成要素

移動通信ネットワークとは『ユーザが移動しても通信を継続して行える通信システム』で、三要素から構成される。

コアネットワーク（CN※3）

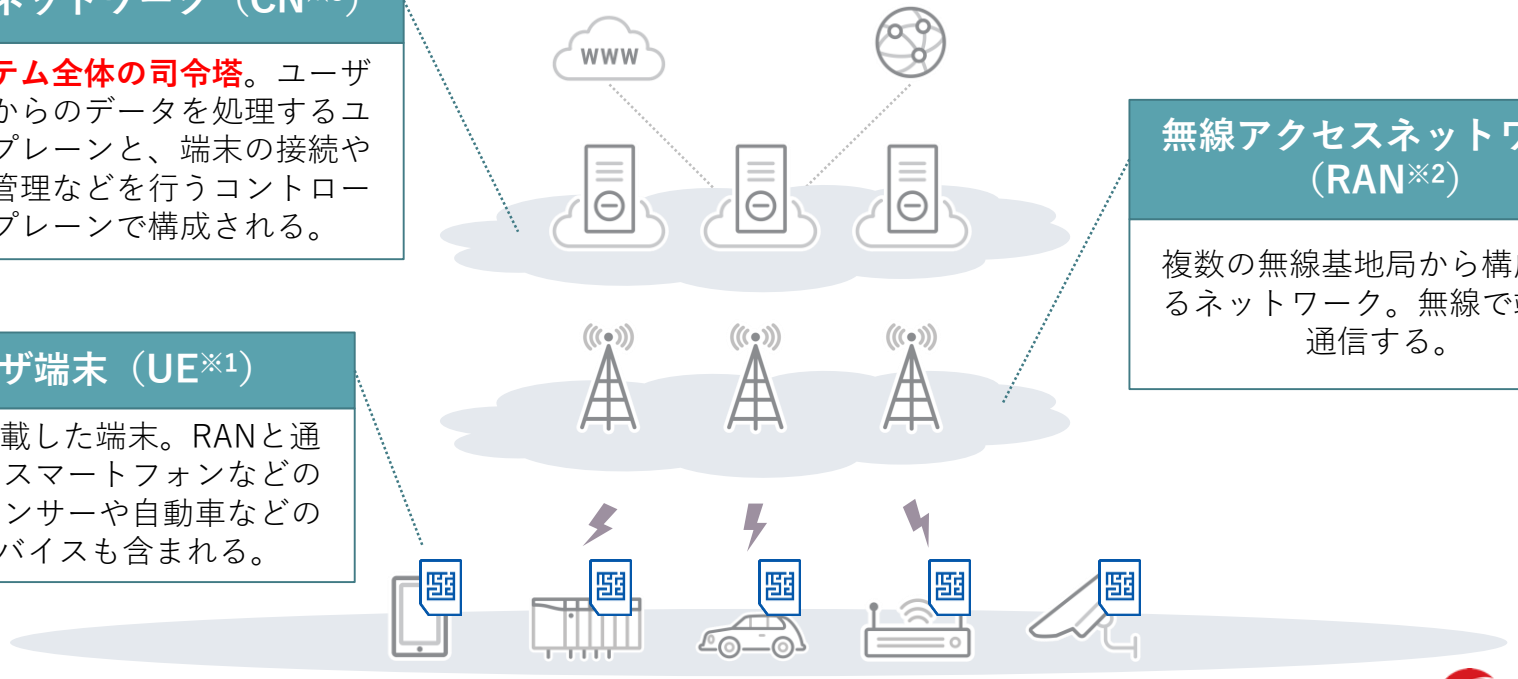
システム全体の司令塔。ユーザ端末からのデータを処理するユーザプレーンと、端末の接続や移動管理などを行うコントロールプレーンで構成される。

無線アクセスネットワーク（RAN※2）

複数の無線基地局から構成されるネットワーク。無線で端末と通信する。

ユーザ端末（UE※1）

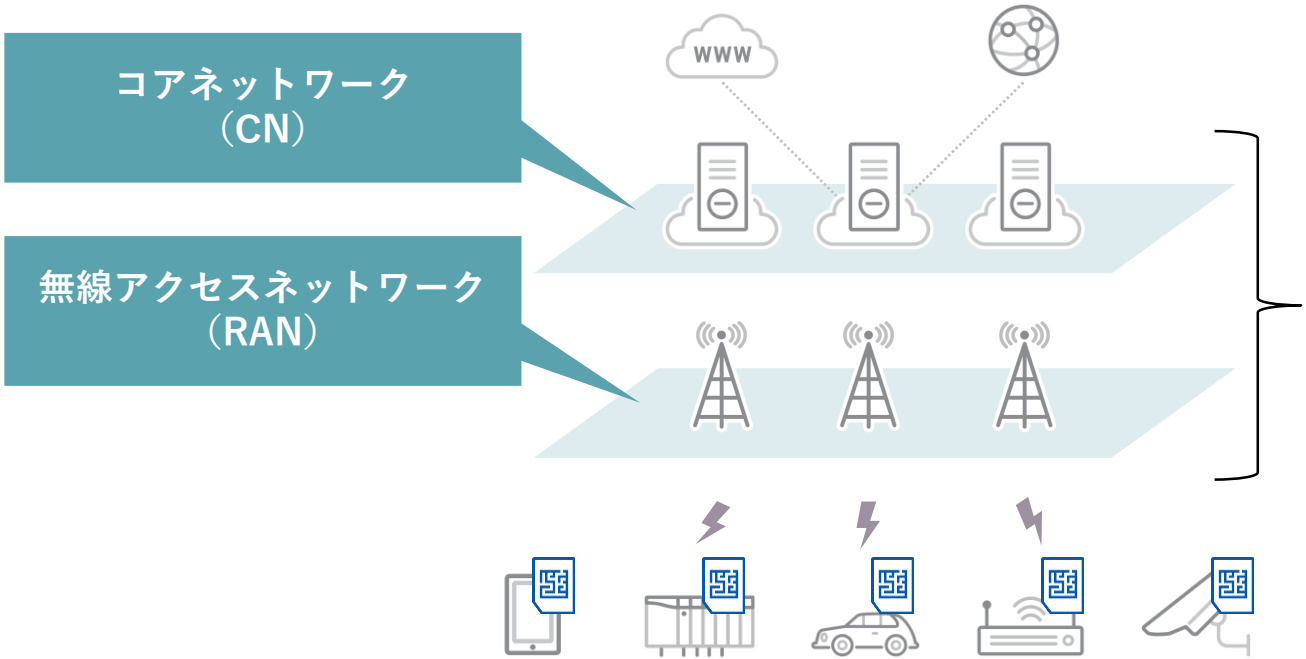
SIMを搭載した端末。RANと通信する。スマートフォンなどの他に、センサーや自動車などのIoTデバイスも含まれる。

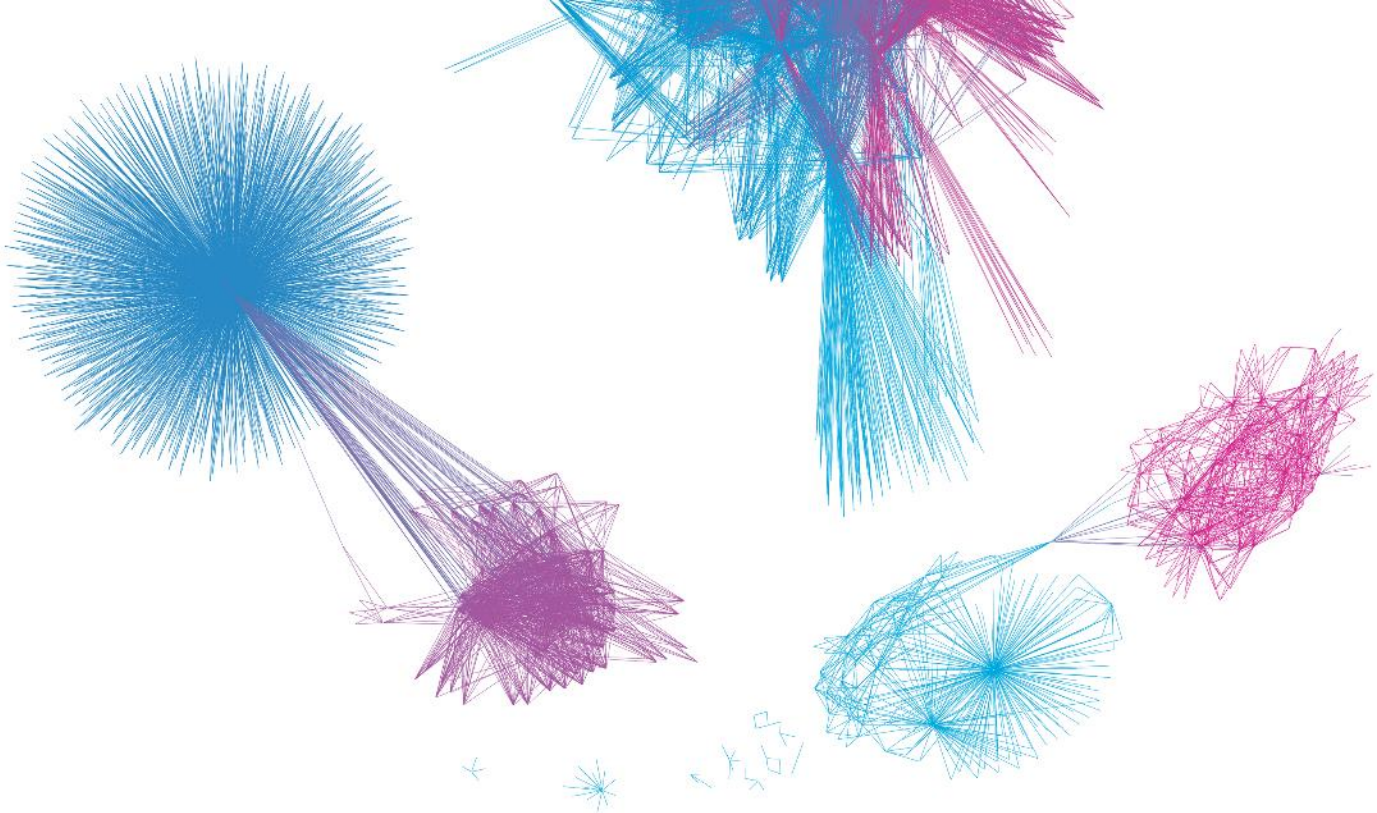


※1 User Equipment
※2 Radio Access Network
※3 Core Network

5G環境も同様の三要素で構成される。
パブリック5Gでは通信事業者がCN・RANの運用主体

ローカル5GではCN・RANをユーザ組織が構築/運用可。つまり、テレコムインフラが組織のIT環境に持ち込まれる





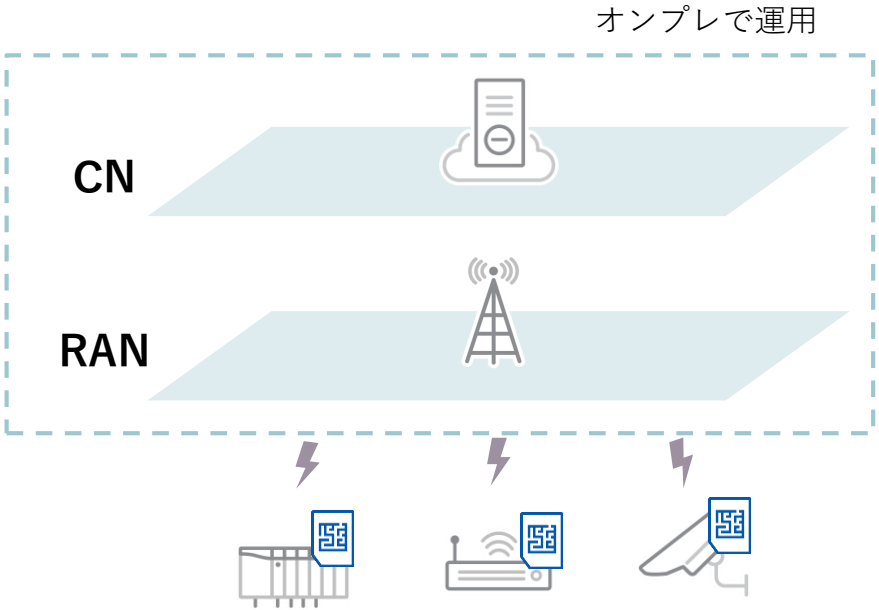
実証実験の目的と方法

製鉄所を模したローカル5G実証環境を構築

コアネットワークを足場とした攻撃を実施

被害をもたらし得るシナリオを特定

コアネットワークとRANを
自前で構築/運用する製鉄業を想定



CN/RANをオンプレで構築

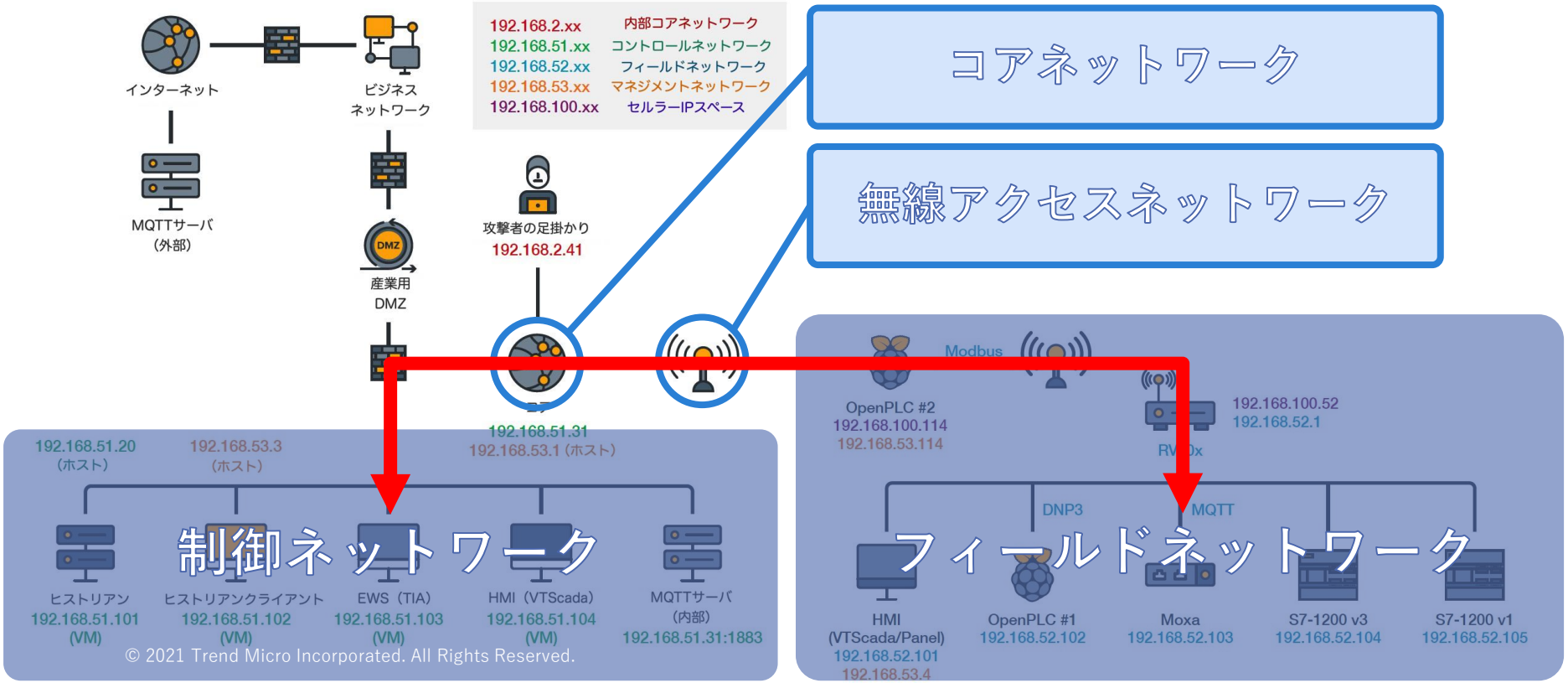
5G NSA※1（ノンスタンドアローン）

PLC※2/HMI※3で工場NWを再現

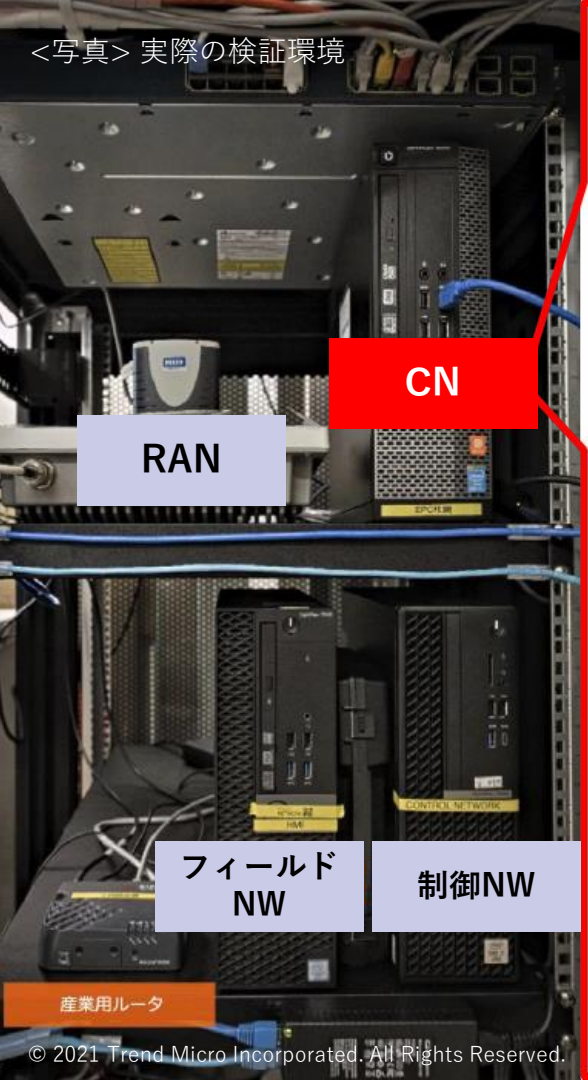
<上図> トレンドマイクロが構築したローカル5G環境の概略図

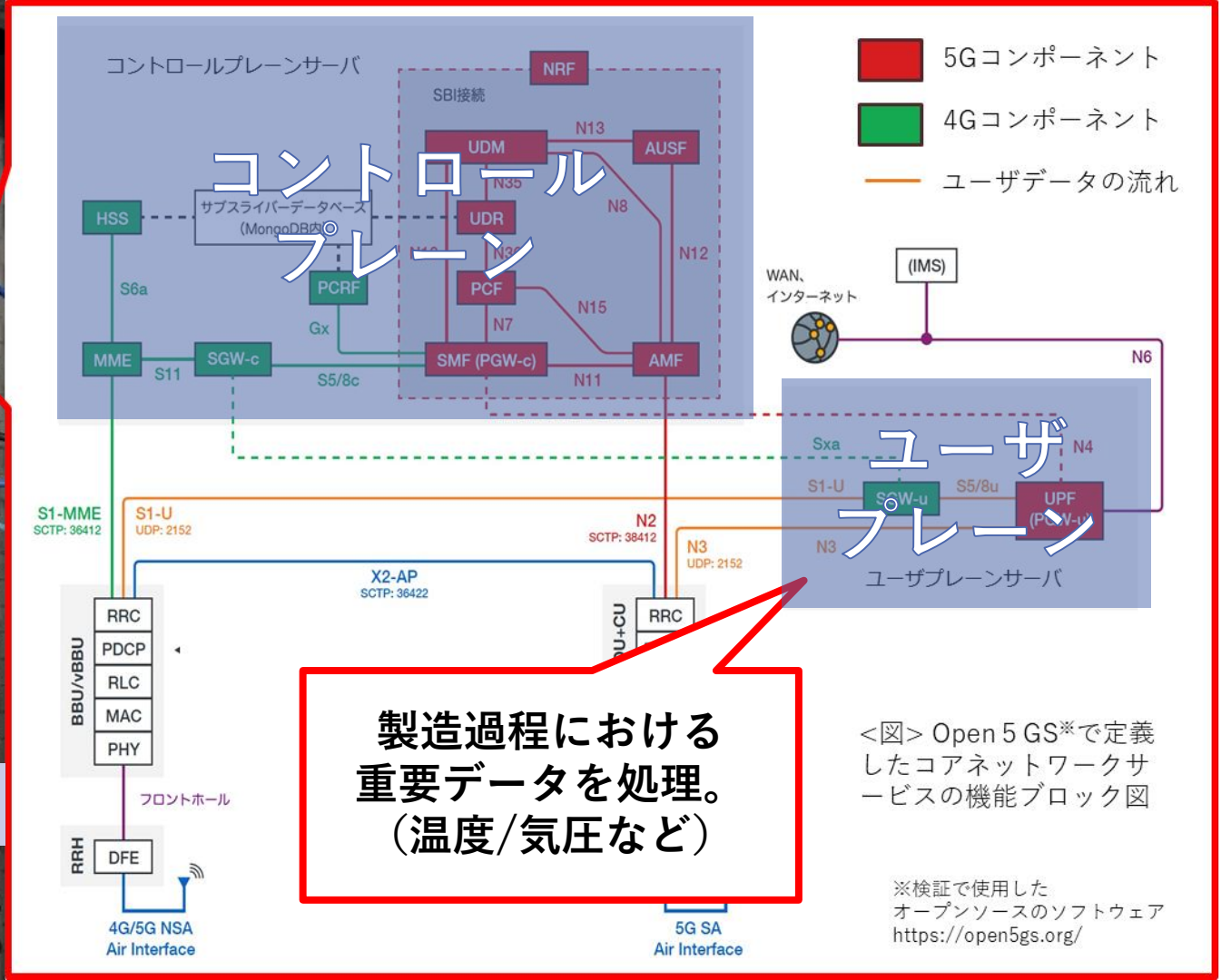
※1 Non Stand Alone：従来の4Gコア設備と5G基地局を組み合わせたシステム構成。
※2 Programmable Logic Controller：ICSで使用される機械を制御するための装置。
※3 Human Machine Interface：システム管理者やオペレーターがシステム全体の状況を確認したり、制御したりするためのインターフェース。

【検証環境ネットワークの概要図】
フィールドNWと制御NWがローカル5Gを介して通信している設定



<写真> 実際の検証環境





製造過程における重要データを処理。（温度/気圧など）

<図> Open 5 GS※で定義したコアネットワークサービスの機能ブロック図

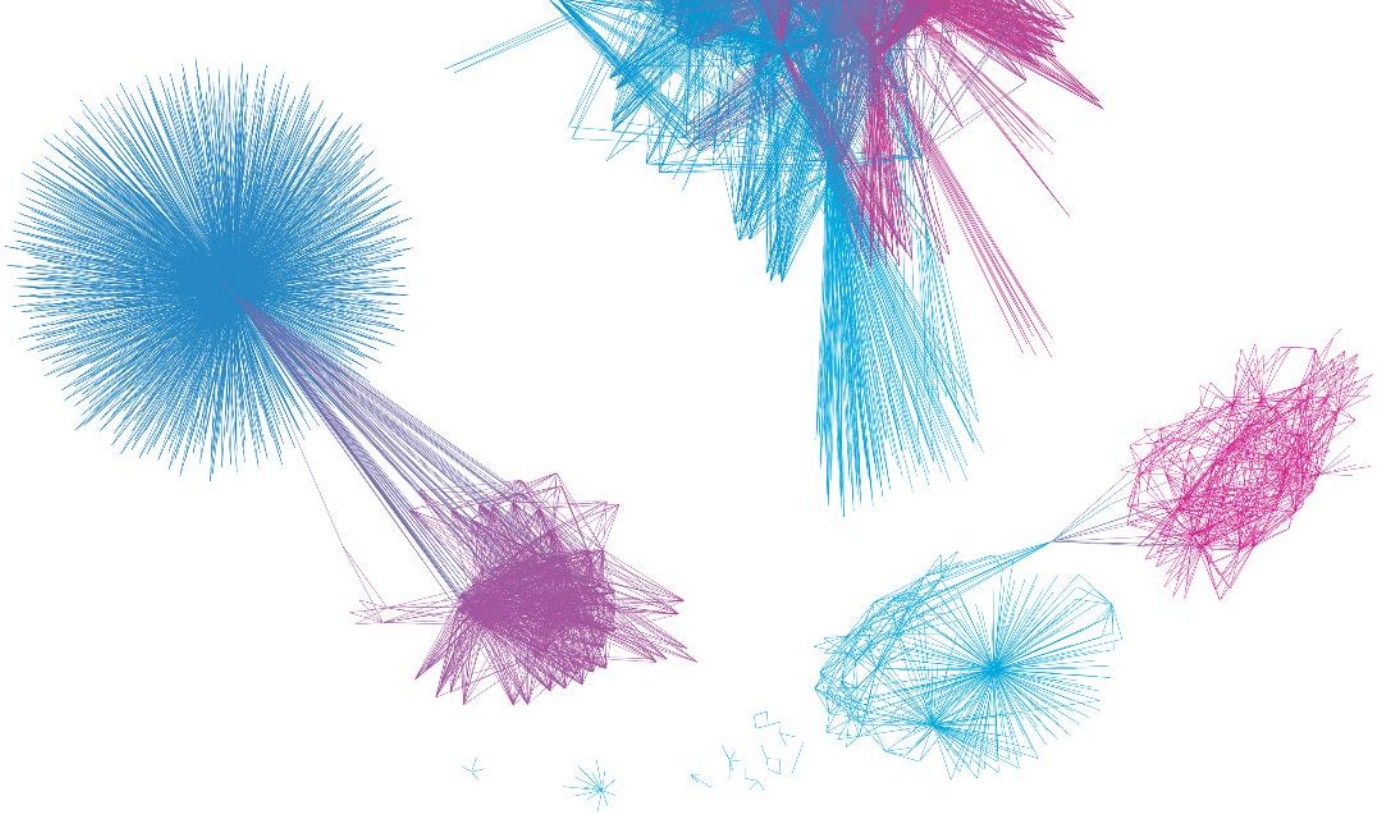
※検証で使用したオープンソースのソフトウェア
https://open5gs.org/

【参考】今回の実証実験で使用した製品群

項目	見積価格（米ドル）	詳細
ファラデーケージ（Faraday cage）	1,500	電磁波を封じ込めて地域の規制に準拠させる
Gemtek WLTGFC-105	3,750	LTE 基地局
Amarisoft gNB	30,000	5G 基地局
Sysmocom SIM cards	82	10 枚のプログラム可能な SIM カードのパック
Sierra Wireless RV50x	840	広く使われている産業用ルータ
SIM-7000 LTE ハット	60	OpenPLC が動作する Raspberry Pi 用 LTE ハット
ジェネリックサーバ	0	32GB の RAM および 1TB の HDD を搭載した予備
ジェネリックサーバ	0	CISCO 3650 および CISCO 2960 の予備
イーサネットケーブル	0	予備ケーブル
10 SMA ケーブル	400	ファラデーケージに無線機器を接続する際に使用

【上表】検証環境で使用した機器

【上写真】検証に使用した市販のファラデーケージ



実証実験の結果

検証結果のハイライト

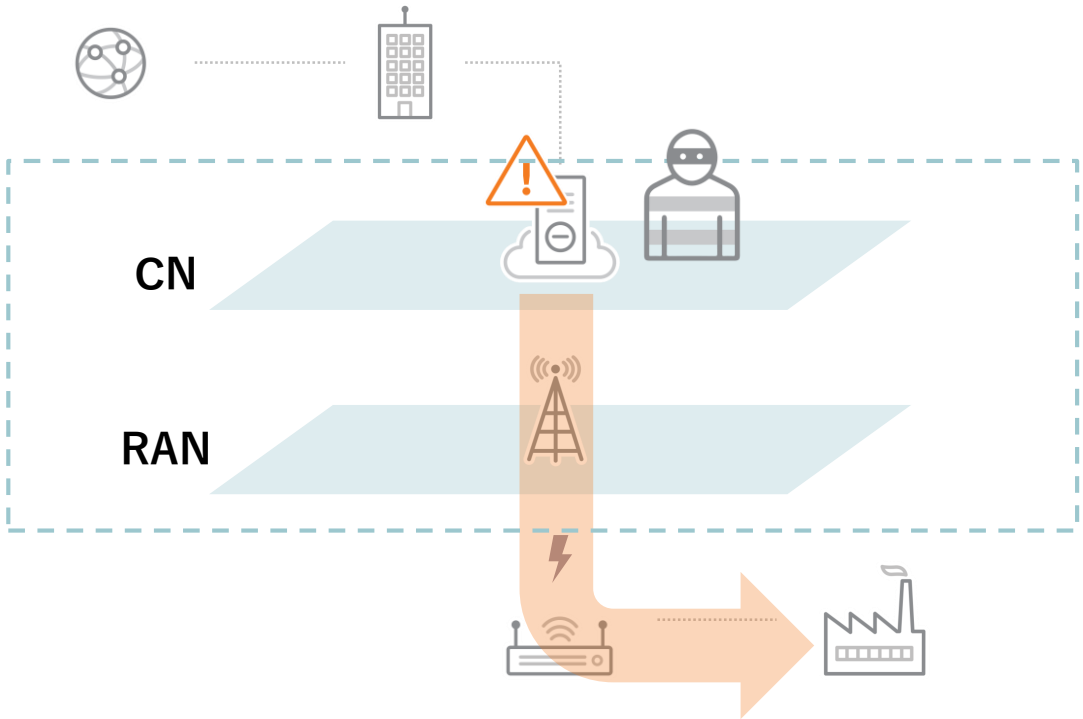
コアネットワークを足場とした攻撃により
製造物破壊および製造妨害が可能

汎用ハードウェアおよびソフトウェアの導入により
コアネットワークへの4つの侵入経路が懸念される

コアネットワーク内部にある3つの傍受ポイントの
いずれかを悪用することで攻撃が可能

【想定シナリオ】コアネットワーク内の攻撃者が通信を傍受/改ざんし製造システムに影響を与える

ITシステムの一部として
オンプレで運用



<上図> トレンドマイクロが構築したローカル5G環境の概略図

ローカル5G環境は汎用HW/SW活用が見込まれるため コアネットワークへの4つの侵入経路が懸念される

一般的なx86サーバのため
OSなどの**脆弱性**を悪用可能

今回の研究で**脆弱性を新たに発見**

②VM/コンテナ

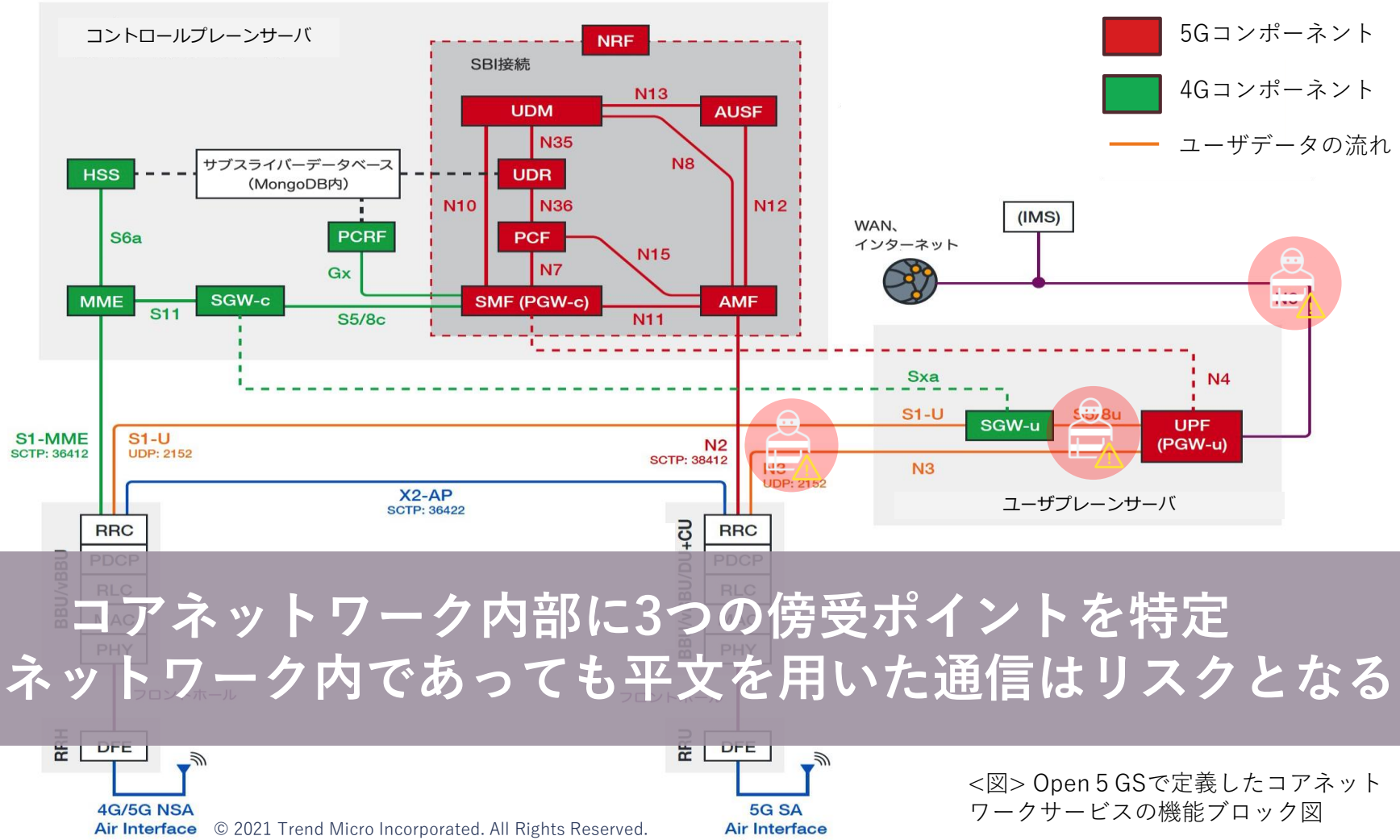
コアネットワークサービスでは
仮想化技術が**多用**される

ルータ・スイッチ・FW・アプライアンスなどの**脆弱性や設定ミス**

④基地局

①CNホスティングサーバ

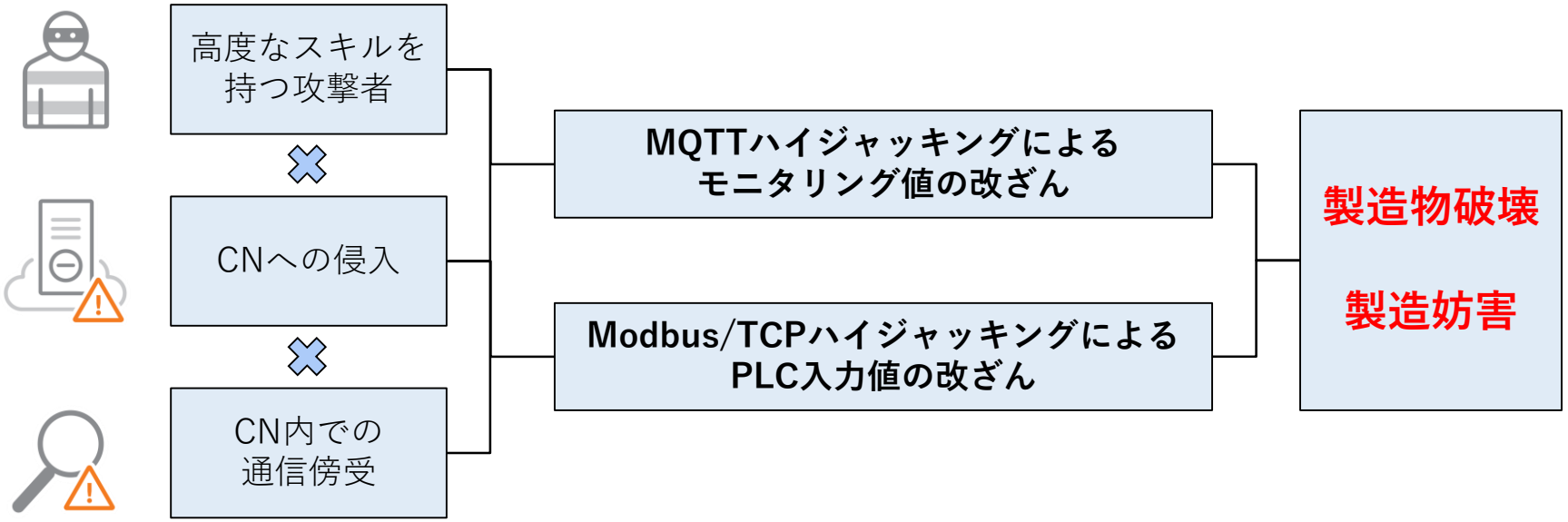
③ネットワークインフラ



コアネットワーク内部に3つの傍受ポイントを特定
コアネットワーク内であっても平文を用いた通信はリスクとなる

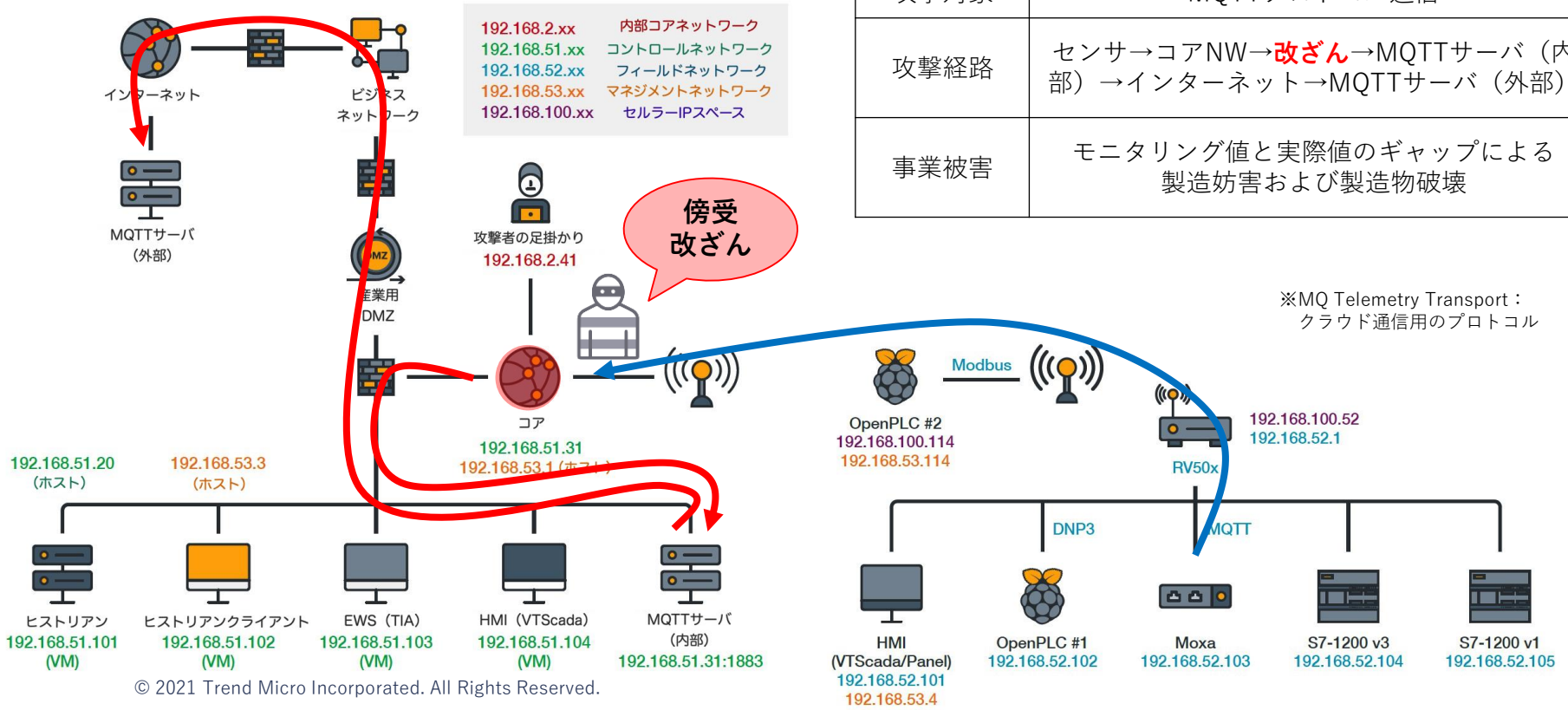
<図> Open 5 GSで定義したコアネットワークサービスの機能ブロック図

製造環境に影響を及ぼす攻撃シナリオ



① MQTT※ハイジャッキングによるモニタリング値の改ざん

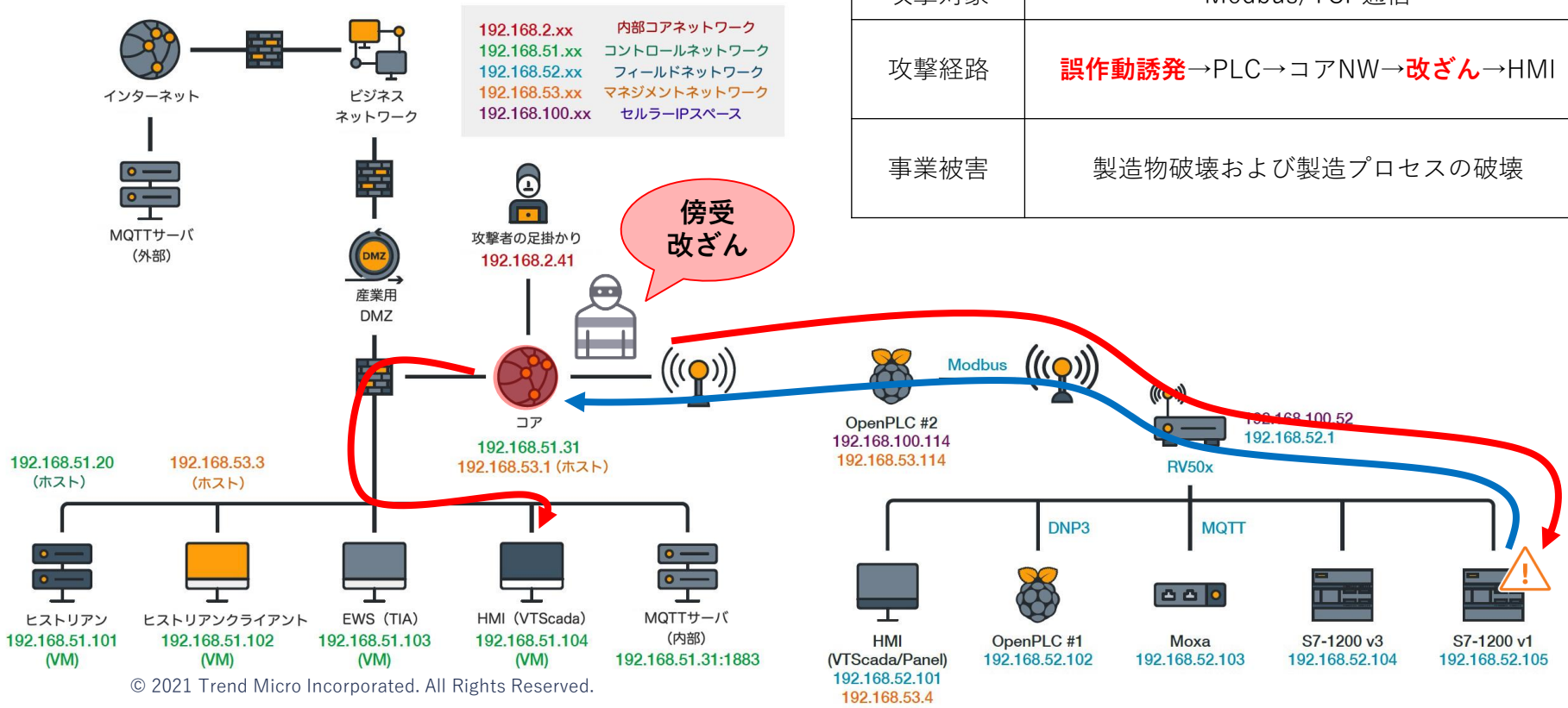
分析要素	説明
目的	製造プロセスの妨害
攻撃拠点	コアネットワーク（ユーザプレーン）
攻撃対象	MQTTプロトコル通信
攻撃経路	センサ→コアNW→**改ざん**→MQTTサーバ（内部）→インターネット→MQTTサーバ（外部）
事業被害	モニタリング値と実際値のギャップによる製造妨害および製造物破壊



※MQ Telemetry Transport：
クラウド通信用のプロトコル

② Modbus/TCPハイジャッキングによるアラートの無効化

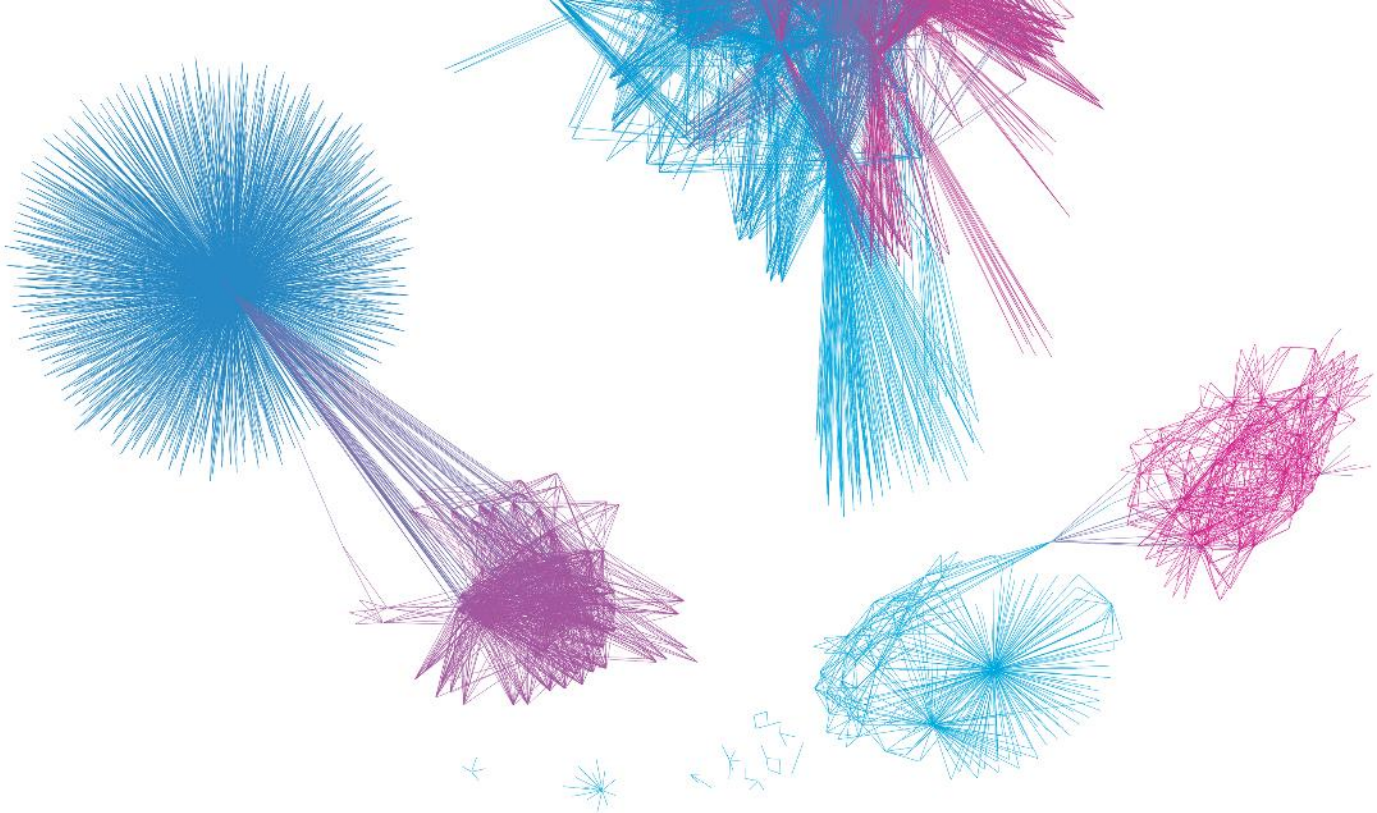
分析要素	説明
目的	製造プロセスの破壊
攻撃拠点	コアネットワーク（ユーザプレーン）
攻撃対象	Modbus/TCP通信
攻撃経路	**誤作動誘発**→PLC→コアNW→**改ざん**→HMI
事業被害	製造物破壊および製造プロセスの破壊



～今回実証した製造システムに対する攻撃手法～
CN内でユーザデータを改ざんすることで物理的被害を誘発

	攻撃名	手法	想定される被害
1	MQTTハイジャッキング	センサー測定値であるMQTTメッセージを**傍受/改ざん**し、実際値とは異なる値を送信する。	**製造物破壊** **製造プロセスの破壊**
2	Modbus/TCPハイジャッキング	Modbusファンクションコードおよびデータ値を**傍受/改ざん**し、HMIに反映される温度値などを偽装する。	**製造物破壊** **製造プロセスの破壊**
3	PLCのファームウェアリセット	PLCとTIA※1間のパケットを**傍受/改ざん**し、PLCを強制的にリセットする。	**製造物破壊** **製造プロセスの破壊**
4	DNSハイジャッキング	PGW※2またはルータにアクセスし DNSクエリを傍受し、レコードを変更する。	機密情報の窃取 機器へのマルウェア混入
5	リモートデスクトップの悪用	RDP/VNC※3ポートをスニッフィングして、 キーストロークとパスワードを窃取する。	機密情報の窃取 権限昇格による水平移動

※1 Totally Integrated Automation：完全統合オートメーション。
※2 Packet Gateway module ：インターネットに接続するためのゲートウェイ。
※3 Virtual Network Computing：遠隔からコンピュータをリモート制御するためのツールの1つ。



対策

【攻撃者の視点】
なぜコアネットワークを狙うのか？

製造工程の機密性/可用性/完全性に直接影響する情報を扱う基盤となるから

一度構築すると改修や修正が難しく、侵害された際の影響が大きいため

セキュリティ・バイ・デザインが必要

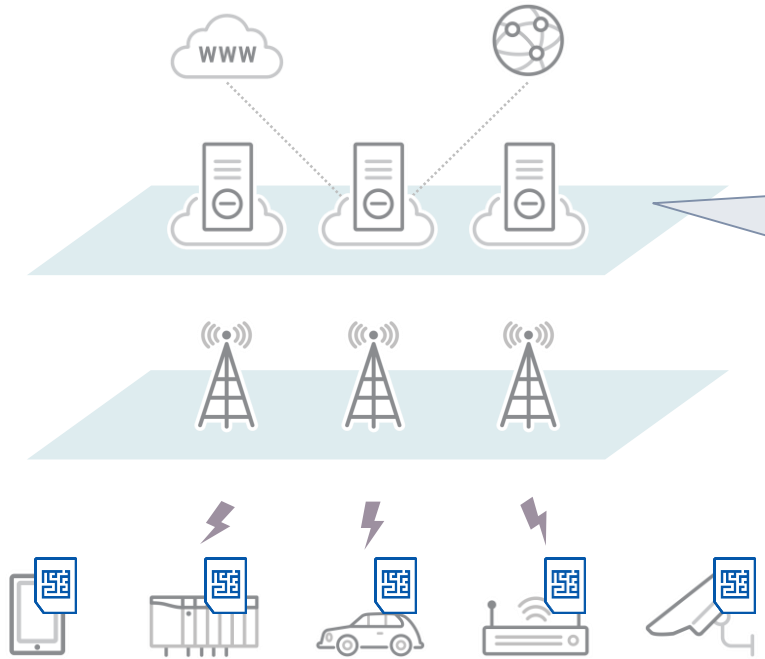
侵入を前提としたセキュリティ対策を

コアネットワーク内の暗号化・認証/認可

PoC段階でのセキュリティ検証の実施

早期に異常を検知できる体制

コアネットワークはユーザデータを扱う重要システム。
まずはローカル5G環境における攻撃対象領域を把握する



今回の研究で
重要データを扱う
ユーザプレーンを含む
コアネットワークに
攻撃対象領域を発見

コアネットワーク内の暗号化・認証/認可でリスク減

	攻撃名	想定される被害	技術的対策
1	MQTTハイジャッキング	製造物の破壊 製造プロセスの破壊	ユーザ名、パスワード、証明書のピン留めを有効にした上でMQTTS(**暗号化**したMQTT)を使用する。
2	Modbus/TCPハイジャッキング	製造物の破壊 製造プロセスの破壊	リモートサイトと制御ネットワーク間で**VPN**を設定する。
3	PLCのファームウェアリセット	製造物の破壊 製造プロセスの破壊	リモートサイトと制御ネットワーク間で**VPN**を設定する。PLCを導入する際に「読み取り/書き取り」の保護を設定する。チャレンジ＆レスポンス**認証**をサポートする新しいファームウェアを導入する。
4	DNSハイジャッキング	機密情報の窃取 機器へのマルウェア混入	不審なIPアドレスを検知できるEDRやネットワーク監視ツールを導入する。暗号化や証明書のピン留めが可能な産業用プロトコルを使用する。
5	リモートデスクトップの悪用	機密情報の窃取 権限昇格による水平移動	VNCの場合は**TLS暗号化**と証明書のピン留めを有効にする。クライアント**認証**を有効にする。MS RDPの場合はバージョン10以上が推奨される。

ユーザ組織はインテグレータと協働し
設計段階からセキュリティ要件を明確にする

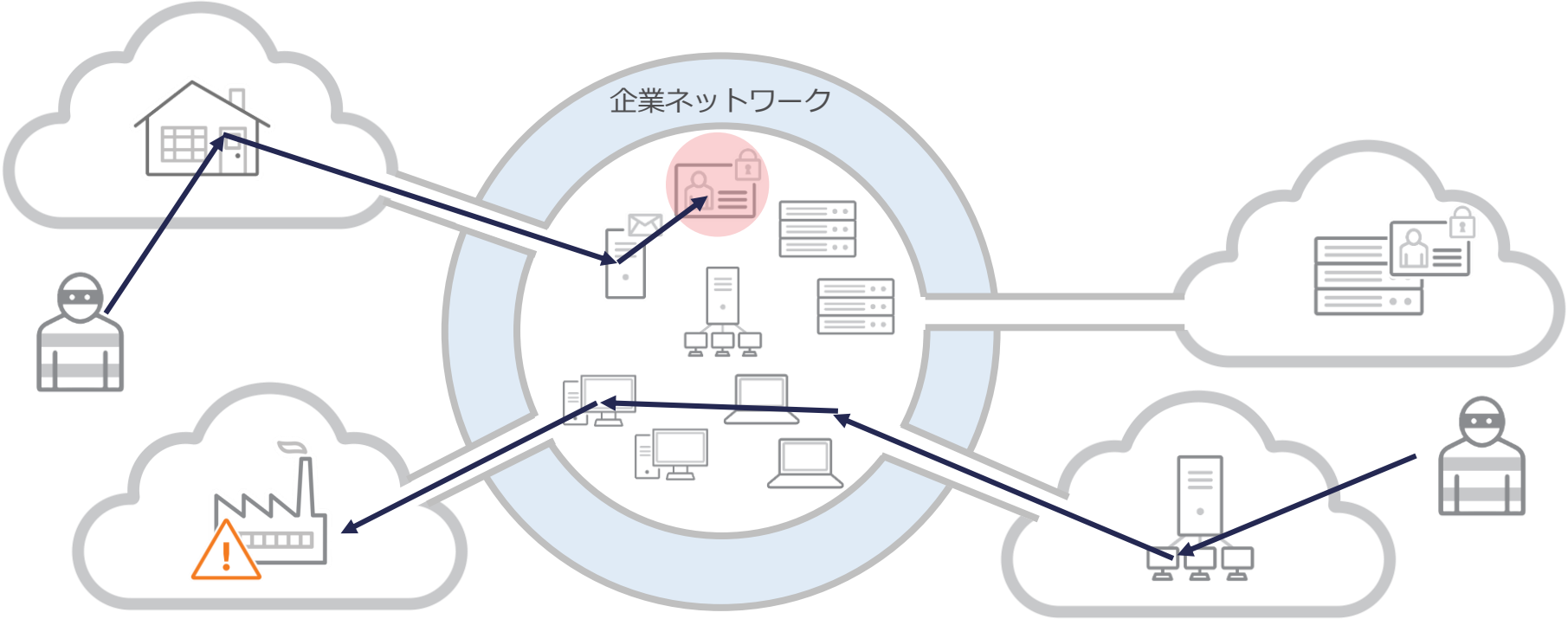
暗号化　証明書　認証認可　NW監視　脆弱性対応

暗号化　脆弱性対応

端末保護　SIM管理

ローカル5GのPoCを
実施する際に
セキュリティ要件も
含めて検証すべき

多様な環境を跨いだ複雑な攻撃を前提とした対策が推奨される。
制御システムへのサイバー攻撃はIT経由が多数



【XDR：See more, respond faster】
クロスレイヤーの検知で迅速な対応を目指す

本日のまとめ

製造過程に関わるデータを扱うコアネットワークが
ローカル5Gセキュリティの鍵。

コアネットワークを足場とした攻撃により
製造物破壊および製造妨害が可能となる。

ローカル5G環境の構築の際には
PoC段階でセキュリティ要件も含めて検証すべき。

THE ART OF CYBERSECURITY

An Innovative Approach to Cybersecurity

Automated hybrid cloud workload protection in Japan via API calls to Trend Micro's cloud security platform. **Created with real data by Trend Micro threat researcher and artist Jindrich Karasek.**