Orchestrating a brighter world

『IoTセキュリティに関するミニワークショップ』@金沢サテライトプラザ

IoTのセキュリティ確保に向けた取り組み（暗号屋さんの目線から）

2016年03月07日

NECソリューションイノベータ株式会社
北信越支社　北陸支社
齊藤　照夫

Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

目次

１．はじめに

A) IoTとは？
B) IoTとセキュリティ
C) 本日のテーマ

1. IoTとは？

Internet of Things の略語

IoTとは、コンピュータなどの情報・通信機器だけでなく、世の中に存在する様々な物体（モノ）に通信機能を持たせ、インターネットに接続したり**相互に通信する**ことにより、自動認識や自動制御、遠隔計測などを行うこと。

出展：http://e-words.jp/w/IoT.html (2016/02/28)

世の中のすべてをクラウドに蓄積し、活用すること。
そしてそれを実現するためのデバイステクノロジー。

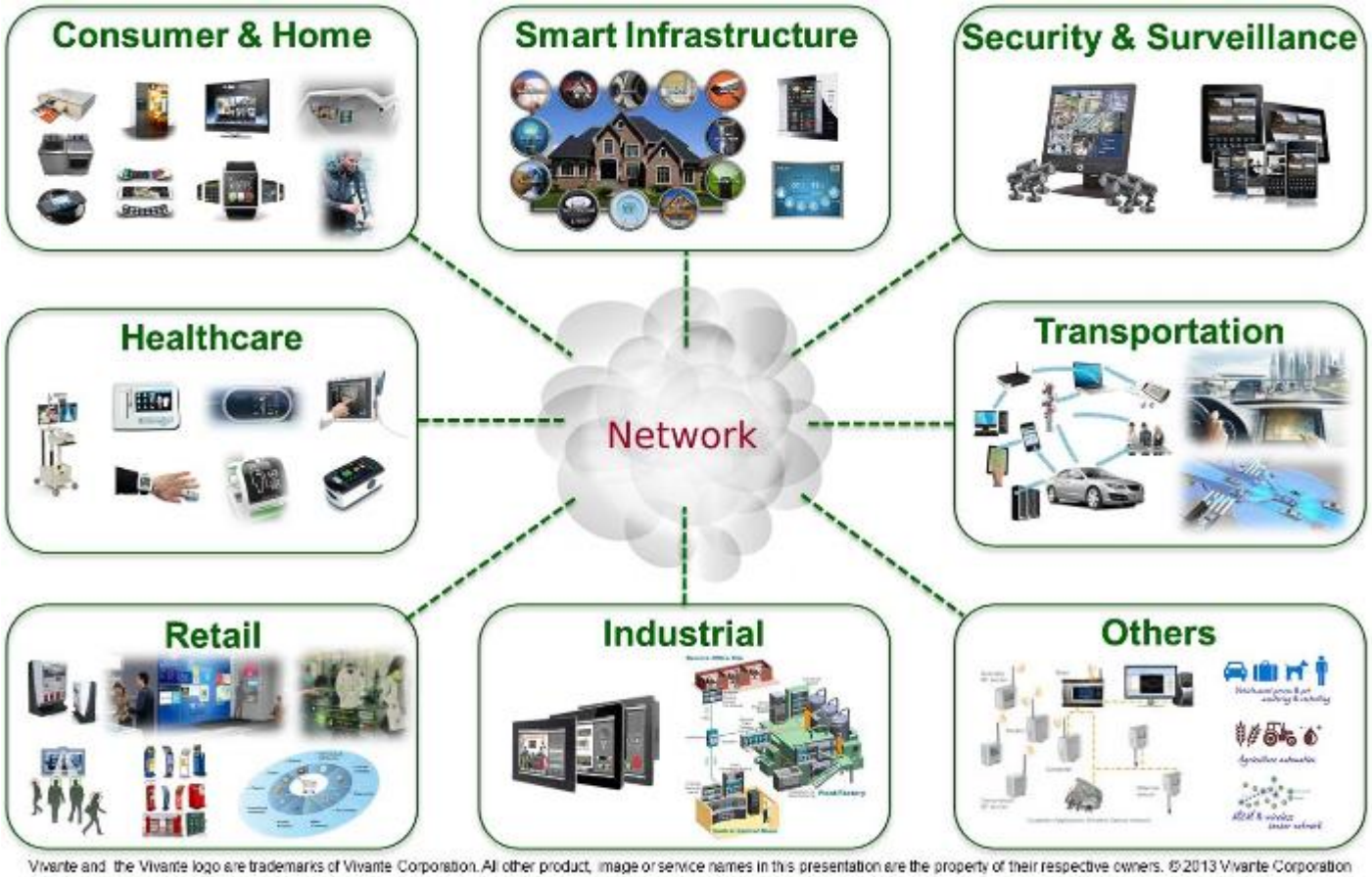
「センシング（すべてのものをクラウドに蓄積する）」されたデータに
「ロジック（解析・整理する）」を加えることによって、
「**フィードバック（私たちが活用できる状態になる）**」が行われる。

現在までに生まれているクラウド技術やビッグデータ解析技術といった
テクノロジをまとめるキーワード

出展：http://japan.cnet.com/sp/iot2014/35049221/ (2016/02/28)

1. IoTと位置づけられるもの

- 交通インフラ、産業機器、物流、ヘルスケアなど、ありとあらゆる繋がる世界
- スマート・グリッドと呼ばれるエネルギー領域もその世界の一つ



出展： http://www.vivantecorp.com/index.php/en/products/internet-of-things.html (2016/02/28)

1. NECの考えるIoTアーキテクチャ5層モデル

- IoTはリアルな世界とサイバー空間が結合され、社会インフラを構成する情報通信が進化したカタチ

- IoTでは、実世界の様々な変化を逃さずにリアルタイムで捉え、新しい価値を創出する

- 従来の3層モデルにエッジコンピューティング層を加え、IoTアーキテクチャを5層モデルとして体系化

1. IoTのセキュリティ課題

- IoTでは、サイバー空間で様々な情報がやり取りされるためサイバーセキュリティは最大のリスクの一つ
- IoTに繋がる全てのデバイスに、データのセキュリティを守るための**十分なリソースがあるわけではない** ▶ ①
- IoTでは、情報の機密性だけでなく、クリティカルデータの完全性、制御システムの可用性、利用者のプライバシー保護の対策も必要
- IoTでは、繋がるモノや環境の多様性、攻撃時のリスクを考慮した**適切なセキュリティ対策が必要**（例：人命に関わるシステムなど） ▶ ②
- 社会インフラがIoTで実現されることによって、攻撃成功時の社会的インパクトが甚大なものになる（例：テロリストの攻撃対象になり得る）

1. 本日のテーマ

① IoTに繋がるデバイスのセキュリティを担保するための技術の一つとして、
軽量認証暗号についてお話しします

② IoTシステム全体のセキュリティを実現するための方法論として、
セキュリティ・アーキテクチャ設計についてお話しします

2．軽量認証暗号

A) 軽量な暗号とは
B) 軽量暗号TWINE
C) 認証暗号OTR

2. 暗号技術と分類

暗号とは一般的に第三者に知られたくない情報を保護する技術です
暗号の機能を大きく分類すると、情報の**秘匿**と**認証**に分けることが出来ます

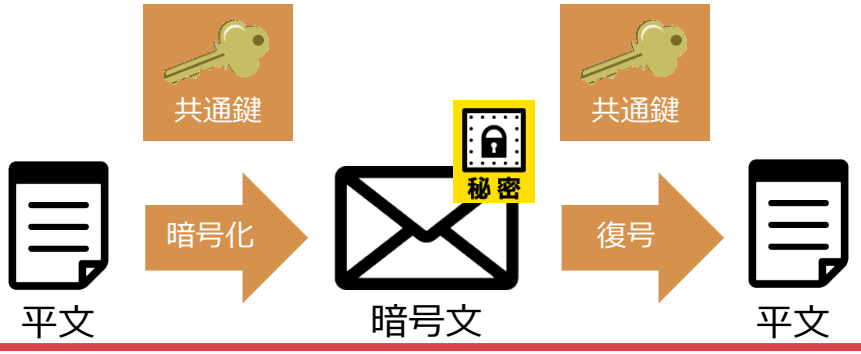
現代暗号を大きく分類すると、公開鍵暗号と共通鍵暗号に分類出来ます
小規模実装と処理速度を重視する場合は、共通鍵暗号を採用します

公開鍵暗号

- RSA, ECC, 等
- 実装規模：大
- 速度性能：低速

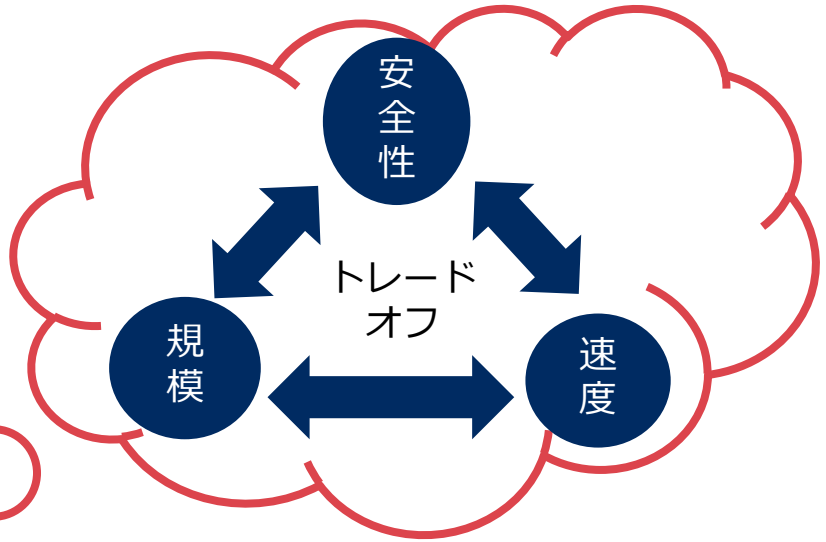
共通鍵暗号

- DES, AES, 等
- 実装規模：小
- 速度性能：高速



2. 暗号のカスタマイズ承ります

- 実装アーキテクチャの特性を考慮した最適な実装が可能です
- お客様ごとの独自カスタマイズが可能
- CIPHERUNICORN-Xシリーズとして開発実績も多数あります
- 皆さんも知らないうちに利用しています



暗号をカスタマイズ

元の暗号（無くても可）

分析 → 設計 → 評価 → 実装

お客様ご要望暗号

<お客様要望>
暗号の
- 小規模（**軽量**）化
- 高速化
- 安全性向上、等

差分攻撃
線形攻撃
高階差分攻撃
暗号評価
統計的評価
乱数検定
○○攻撃

CIPHERUNICORNはNECの登録商標です。

2. 何故、軽量暗号が求められるのか？

- IoTデバイスでは処理能力が貧弱、リソースの制限が厳しい、省電力が求められるなどの実装制約がある

- 2020年、センサー1兆個、機器500億個が繋がると言われるIoTの世界において、ローエンド・マイコンを搭載する機器に暗号技術が必要になる

- 自動運転の実用化、工場やプラントがクラウドとシームレスに繋がる時代には、現時点で暗号技術が利用されていない領域にも利用が広がる

実装上の制約が大きい環境で利用可能な暗号技術が求められる
言い換えれば、実装環境に最適なカスタマイズ暗号の技術が生かせる

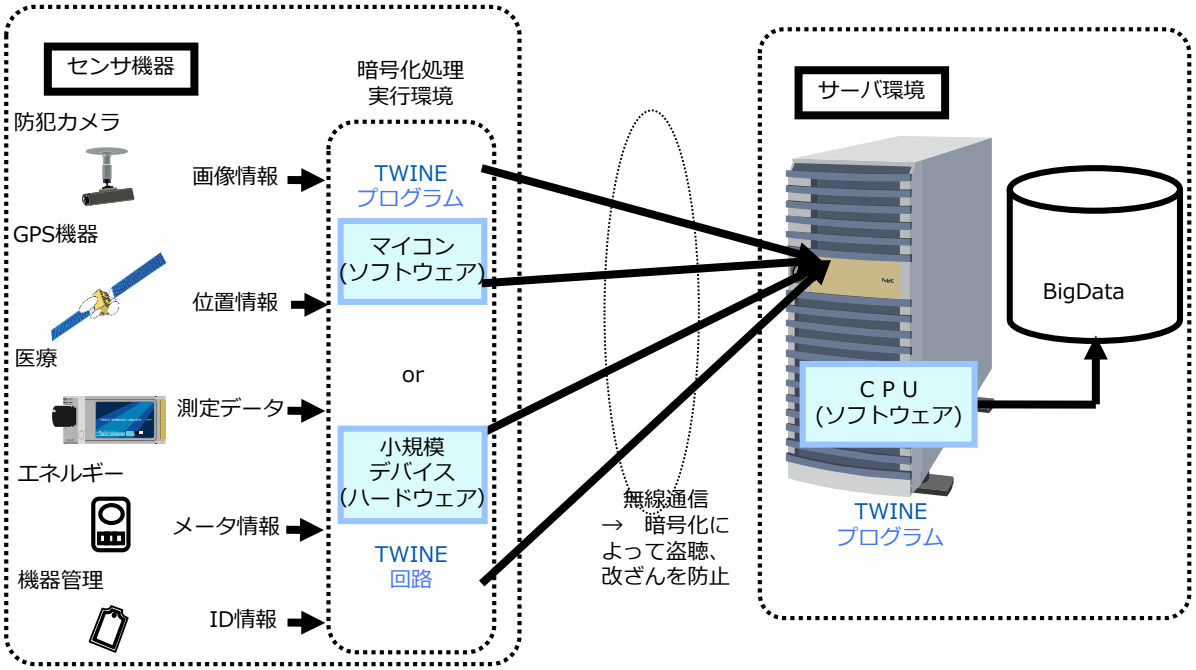
2. 軽量暗号に関する動向

- 2004年～、欧州ECRYPTプロジェクトにおいて、軽量暗号のワークショップ開催や調査レポートの発行などによる研究の活発化
- 2007年～、PRESENTをはじめとする様々な軽量暗号が提案される
- 2009年～、ISO/IEC 29192（Lightweight Cryptography）の規格化が開始
- 2013年～、米国国家安全保障局（NSA）がSIMONとSPECKを提案し、国際標準化活動を開始（ISO/IEC 29192-2へ追加提案）
- 米国国立標準技術研究所（NIST）も軽量暗号に関するワークショップを開催するなど積極的に取り組みを開始
- 日本の電子政府推奨暗号評価機関（CRYPTREC）でも軽量暗号技術の調査を開始

2. 軽量暗号TWINE（トゥワイン）

軽量暗号TWINEはハードウェア/ソフトウェアを問わず、省リソース、省電力、高い処理性能を実現可能

- 2012年、NECは軽量暗号TWINEを開発
- センサ情報の暗号化だけでなく、サーバ処理の暗号化にも適している



ハードウェア回路規模比較

	ASIC (GEs)	FPGA Xilinx Virtex-Ⅱ (Slices)
AES	10,289	3,368
TWINE	1,799	339

小型マイコン実装比較 Atmel AVR

	ROMサイズ (bytes)	1バイトあたり サイクル数
PRESENT（既存）	2,398	1,199
TWINE	1,304	271

2. 軽量暗号TWINEの特長

軽量暗号TWINEは標準暗号AESと同等の安全性（鍵長128ビット）を実現しながら、小規模デバイス、マイコン、サーバのいずれでも高速に動作し、その動作に必要な計算リソースは世界最小クラスで実現しています。

小規模デバイス（ハードウェア）

- 計算リソース（ASIC回路規模）は1,799ゲート
  標準暗号**AESの通常実装の約1/6**
  世界最小クラスの既存軽量暗号PRESENTと比べても同等

汎用小型マイコン（ソフトウェア）

- 計算リソース（メモリサイズ）はROM728バイト、RAM335バイト
  世界最小クラスのメモリサイズ
- 処理速度は271サイクル／バイト

サーバCPU（ソフトウェア）

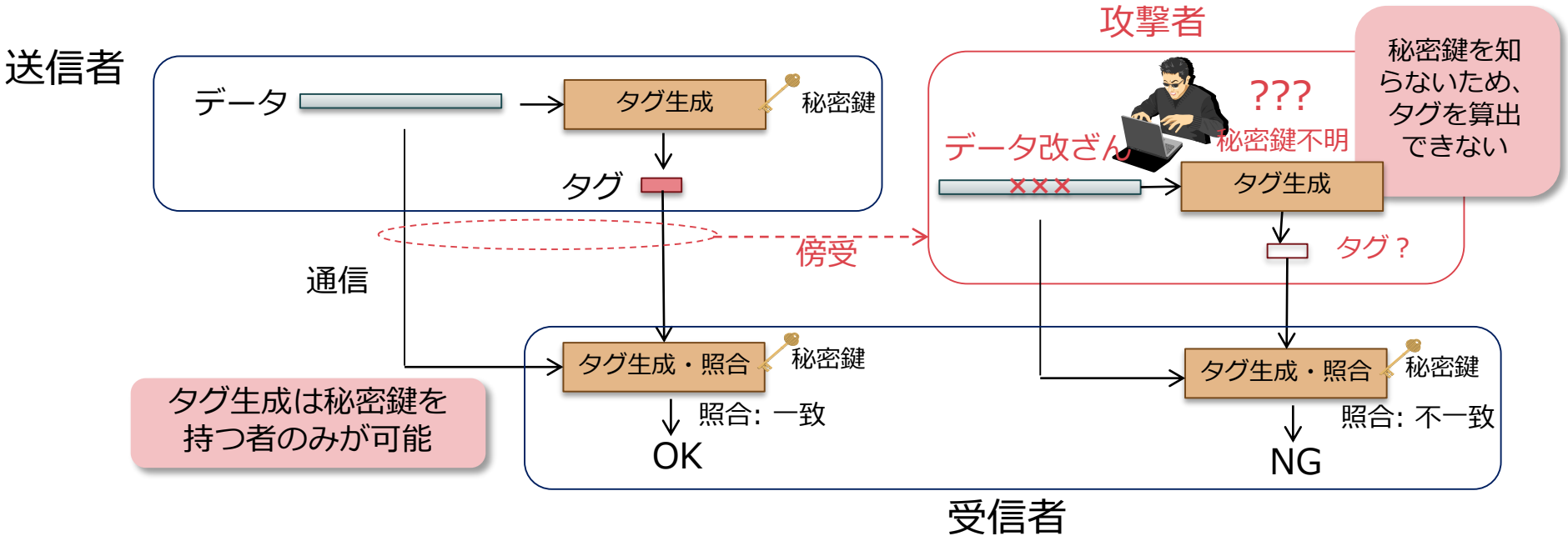
- 処理速度は5.55サイクル／バイト（2.8GHzCPUで2.76Gbpsのスループット）
  AES（C言語実装）の約2.5倍高速

2. 何故、認証暗号が求められるのか？

暗号化（秘匿）だけでは不十分

- 暗号化されていて攻撃者が改ざんの影響の予測が困難であっても、改ざんデータがそのまま処理されると予期しない制御に結びつく可能性あり
- 暗号化の方法によっては暗号化データに対しても意図通りの改ざんが可能となる（データの特定のビットを反転させるなど）

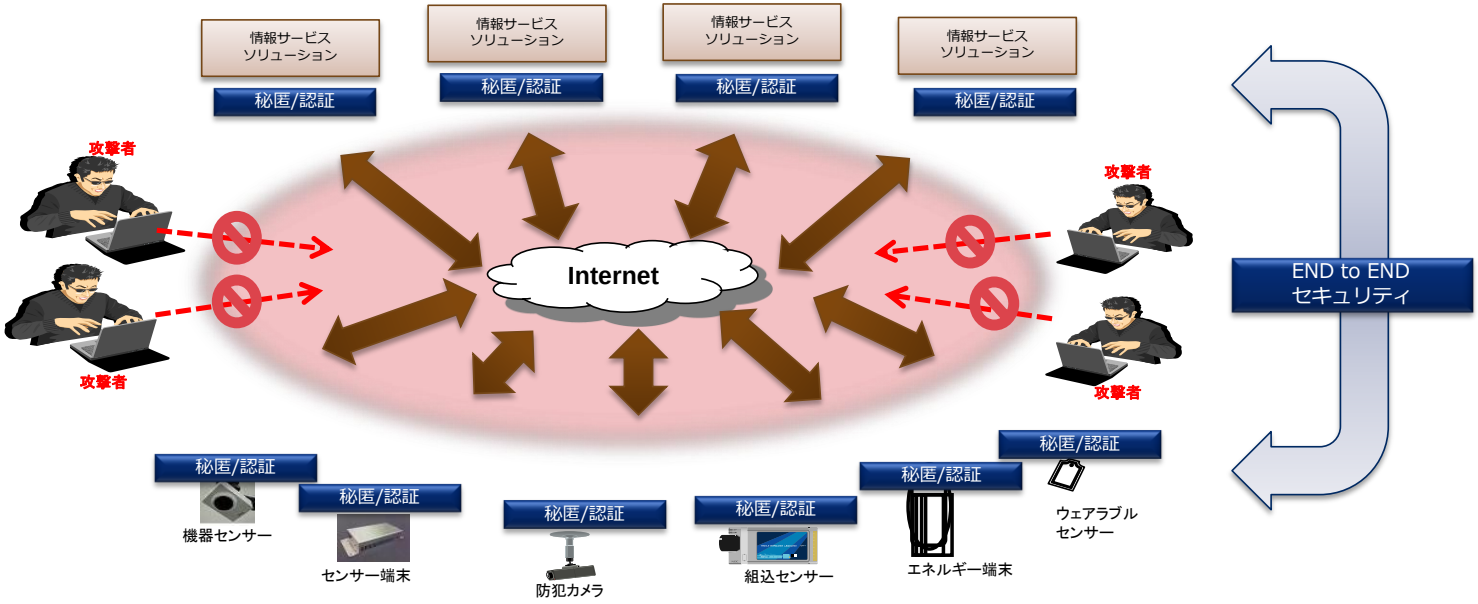
メッセージ認証で改ざん検出の対策



2. 認証暗号OTR

データ保護のためには、情報漏えい防止とともに改ざん検出も重要
認証暗号OTRは、暗号化とメッセージ認証を高効率で同時に行う暗号技術

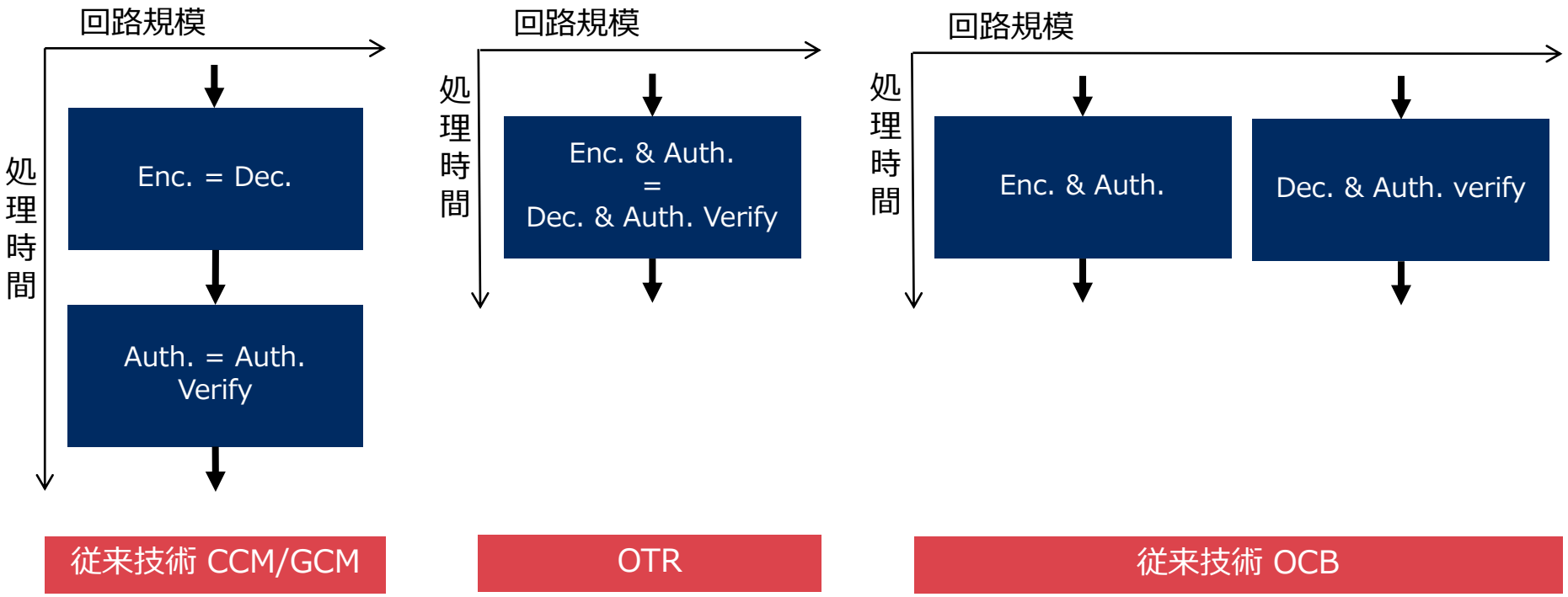
- 2014年、NECは認証暗号OTR (Offset Two-Round) を開発
- 認証暗号とは、機密性と完全性を保証する共通鍵暗号技術
- OTRは、NIST が出資する国際的な認証暗号コンペティションである CAESAR の候補として提案中（2015年7月に一次選考を通過）



2. 認証暗号OTRの特長

認証暗号OTRは、従来技術と比較して2倍高速に処理が可能、かつ、実装規模を1/2に削減できる

- OTRは従来技術CCM/GCMと比べて**2倍高速**に処理が可能
- OTRは従来技術OCBと比べて**回路規模を1/2**に削減可能
- OTRは高速性と省リソースを同時に実現可能とした初めての技術



2. 今後の目標・課題

- TWINEを超える軽量暗号の開発
- CAESARコンペ最終候補選定に向けたOTR提案活動
- IoTシステムでの利用を想定したNEC軽量暗号ライブラリの開発・実用化

3．セキュリティ・アーキテクチャ設計

A) セキュリティ・アーキテクチャ設計の重要性
B) 衛星システムにおける実績
C) V2Xシステムにおける実績

3. セキュリティ・アーキテクチャ設計の重要性

- セキュアなIoTシステムを構築するためには、各層のセキュリティを個別に検討していても安全性を担保できる保証はない
- IoTシステムの前提条件やスコープを明確にしておかないと、発生しうる脅威も正確に把握できない（適切な対策が打てない）
- 実装環境のリソース制約や投入コストなどを踏まえた上で、必要十分なセキュリティ要件を抽出しなければならない（ただ安全サイドに倒せば良い訳ではない）
- 抽出されたセキュリティ要件もアーキテクチャに応じた適切な配置が重要！配置を間違えればシステム性能が大幅に劣化するかもしれない

3. 過去に取り組んだ実績

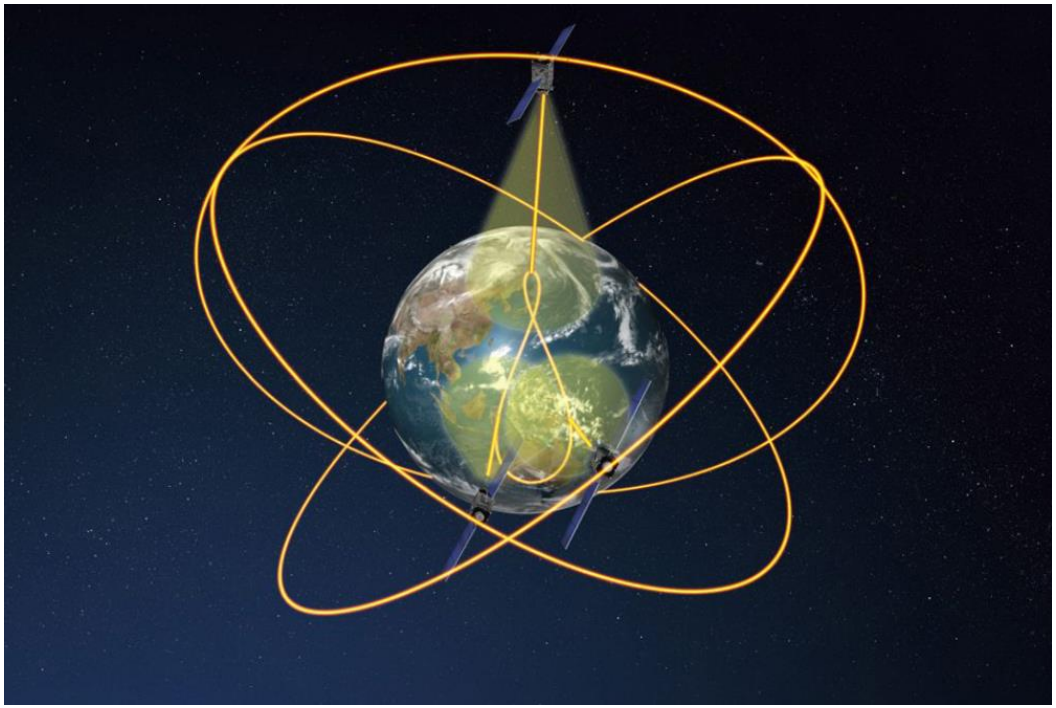
- 衛星システム（どの衛星かは言えない）
- V2X（車車間通信および路車間通信）システム
- And a few more …

3. 衛星もIoTシステムとして考えられる

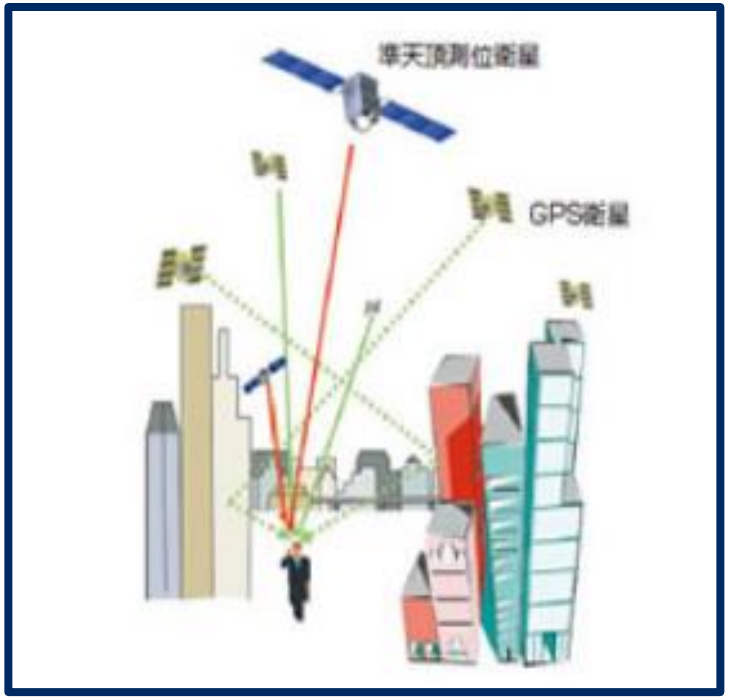
（参考）準天頂衛星システム（QZSS）

- QZSSは、日本のほぼ天頂（真上）を通る軌道を持つ衛星を複数機組み合わせた衛星システムで、常に1機の衛星を日本上空に配置することができます。衛星がほぼ真上に位置することで、山間部や都心部の高層ビル街など、GPS衛星の電波が測位を行うために必要な衛星数が見通せない場所や時間においても、準天頂衛星の信号を加えることによって測位ができる場所と時間を拡げることができます

出展：http://qzss.jaxa.jp/01.html (2016/03/05)



出展：http://www.satnavi.jaxa.jp/project/qzss/index.html (2016/03/05)



出展：http://www.jaxa.jp/projects/sat/qzss/index_j.html (2016/03/05)

3. 衛星もIoTシステムとして考えられる

（参考）宇宙太陽光発電システム（SSPS）

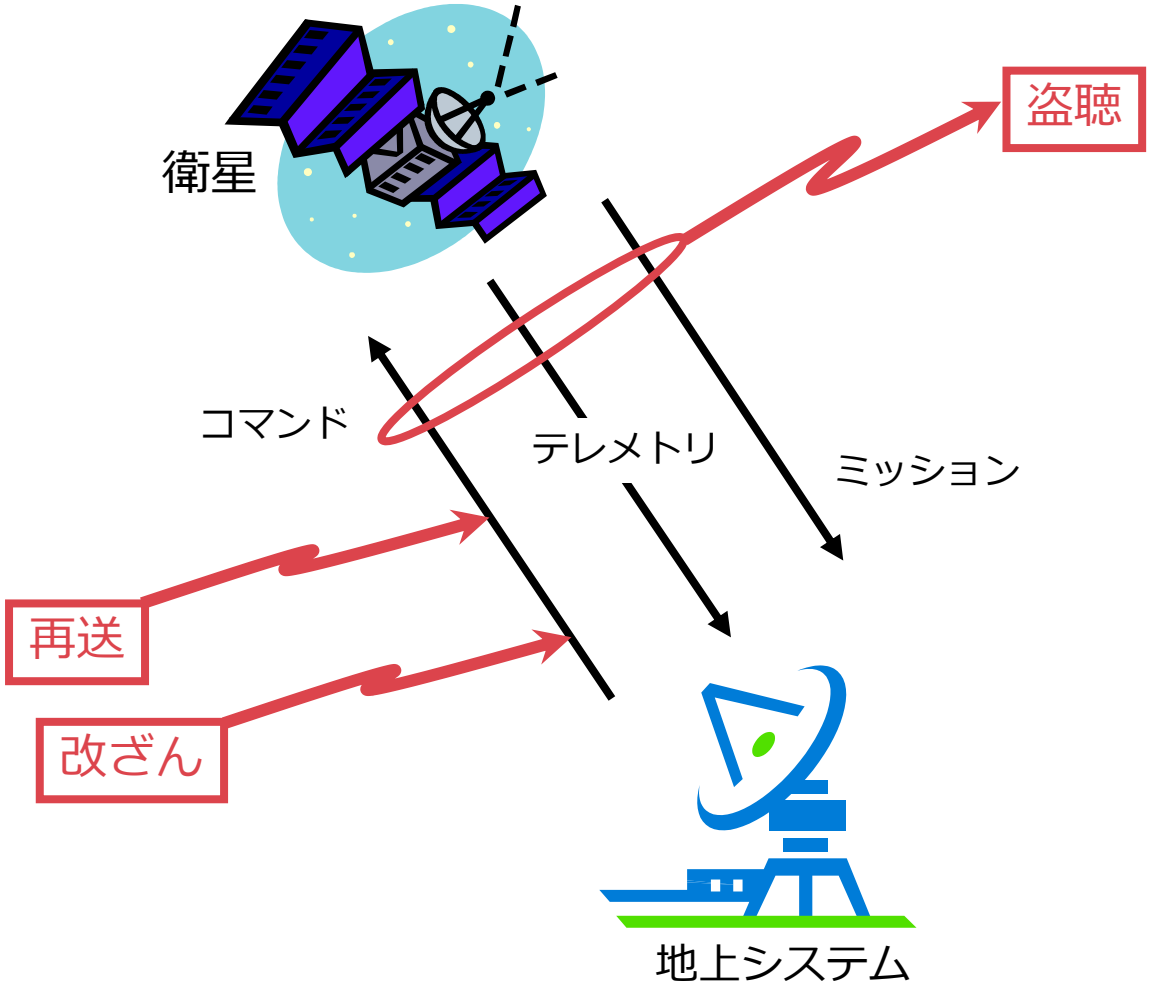
- SSPSとは、宇宙空間において太陽光エネルギーをマイクロ波、またはレーザーに変換して地球に伝送し、電力として利用するシステムであり、エネルギー、気候変動、環境等の人類が直面する地球規模課題の解決の可能性を秘めています

出展：http://www.ard.jaxa.jp/research/hmission/hmi-index.html (2016/03/02)

出展：http://www8.cao.go.jp/space/seminar/dai1/meti-7.pdf#page=2 (2016/03/02)

3. 衛星システムにおける脅威

- 衛星を制御するコマンドに対する不正な操作が脅威として起こり得る
- 衛星から地上に伝送される情報を盗聴される恐れがある



3. 衛星システムにおける制約

- 衛星搭載機器ではリソース制約が大きい（搭載できる機器容量が限られている）
- 衛星地上間の通信レートには制約が大きい（衛星回線の帯域限界やミッションデータのサイズが大きい）
- 新規技術に導入障壁がある（衛星打ち上げ後の変更が出来ないため過去の実績を重視する）
- システム運用期間が長いため、暗号危殆化（きたいか）への考慮が必要（打ち上げ後に暗号が解読されるケースを否定できない）

3. 衛星システムにおけるセキュリティ要件

- リソース制約に対しては、実装環境における最適化技術のノウハウを生かして、省リソースな実装方法の適用やアーキテクチャの配置を行う
- 転送レートの制約に対しては、パケット長が変化しない暗号化方式の選択や、パケットに組み込む改ざん検知用コードのサイズの調整や、適切な鍵更新頻度の設定によって対処する
- 外部評価機関による十分な評価が確認されており、衛星搭載実績のある暗号技術を導入する
- 暗号危殆化の問題に対しては、非公開アルゴリズムの採用や複数種類の暗号方式を搭載する

要件定義を適切に行っても、セキュリティ・パラメータを細かく調整しないとクリティカルなミッションシステムとして機能しない

3. V2Xシステムにおけるセキュリティガイドライン

自技会ガイドの策定には
NECも関わっており、既に
Tier1メーカに対して脅威
分析の実績があります！

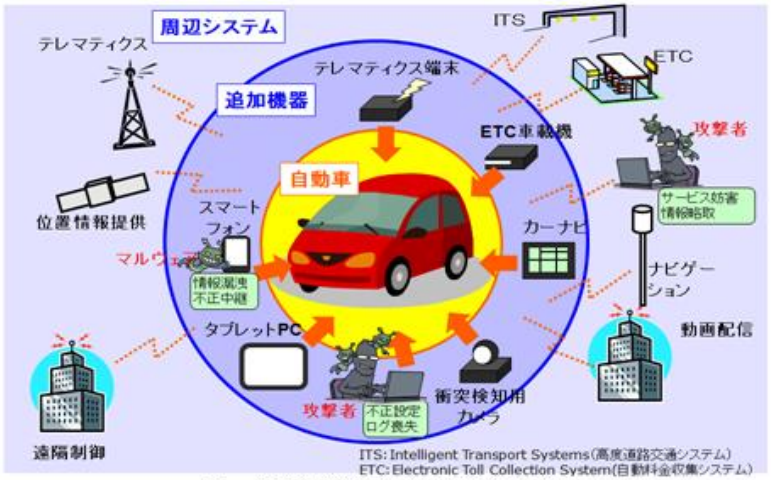


図1：自動車を取り巻く機器・機能や脅威

出展：自動車技術会
『自動車－情報セキュリティ分析ガイド』
http://tech.jsae.or.jp/hanbai/list.aspx?category=522
(2016/03/05)

出展：ITS情報通信システム推進会議
『運転支援システムに関するセキュリティガイドライン』
http://www.itsforum.gr.jp/Public/J7Database/p41/ITS_FORUM_RC009V1_0.pdf (2016/03/05)

出展：IPA『自動車の情報セキュリティへの取組みガイド』
http://www.ipa.go.jp/security/fy24/reports/emb_car/index.html
(2016/03/05)

3. V2Xシステムにおける脅威

- 繋がる車は、様々な通信機器を備え、多様なITサービスを提供する存在になる
- 繋がる車は、様々なIT機器の特徴を持つので多くの脅威に晒される

3. V2Xシステムにおける制約

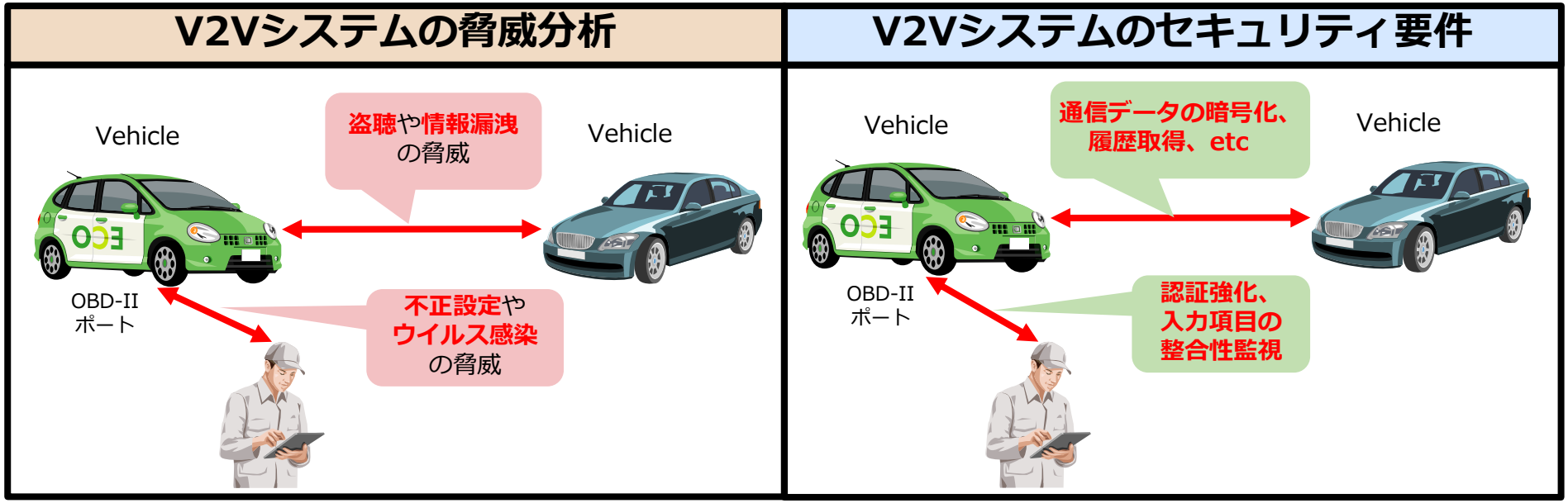
- 機能安全（ISO26262）フレームワークの適用が必須（Safetyの概念）
- 情報セキュリティ確保に関するフレームワークは未だ確立されていないが、
  人命に関わるシステムであるため、開発メーカとしての説明責任は大きい
- CAN（Controller Area Network）の通信レートが非常に低いという制約がある
- V2Xシステムとしての利用シーンは今後広がっていくことが予想されるため、
  利用シーンの広がりを見据えた鍵管理方式が未だ確立されていない

3. V2Xシステムにおけるセキュリティ要件

- V2V（Vehicle to Vehicle）通信システムにおいて、セキュリティ脅威分析を行った事例（左下図）

- システム構成要素の保護資産を規定し、下記5W1H法にて脅威を抽出
  - どのインタフェースから（Where）、誰が（Who）、いつ（When）、どのような動機で（Why）、どのような脅威を（What）、どのような攻撃手段で（How）引き起こすか

- 各脅威に対するFT（Fault Tree）分析を元に基本事象を列挙し、基本事象ごとにセキュリティ対策を洗い出す（右下図）



3. 今後の目標・課題

- V2Xシステムの領域において、セーフティとセキュリティを同時に実現するフレームワークの構築（SafSecハイブリッド認証の考え方）
- その他IoTシステム（組み込み制御機器）におけるセキュリティ確保に向けた取り組みを強化
- 繋がる世界が広がっていく場合、前提条件をどこにおいて評価するべきか？ノード間が相互通信を始めると利用シーンは無限大？

４．まとめ

4. まとめ

まとめ

- IoTシステムに利用可能な軽量認証暗号の技術をご紹介しました
- セキュリティ・アーキテクチャ設計の重要性をお話ししました

見えている課題

- IoTシステムの領域や利用シーンはどんどん広がっていく
- セキュリティ技術者の体制強化やフレームワークの確立が必要

今後の取組み・目標

- IoTシステムで利用可能な、高性能で実用性の高い暗号技術を開発する
- セキュリティの担保されたIoTシステムを実現し、安心安全な社会に貢献する


Orchestrating a brighter world
NEC