JNSA PKI相互運用技術WG・電子署名WG主催セミナー

PKI Day 2017「IoT・ブロックチェーン時代のPKI」

浅草橋　ヒューリックカンファレンス ROOM1

どこでも公開鍵暗号

2017年4月19日

松本　勉

横浜国立大学　大学院環境情報研究院
横浜国立大学　先端科学高等研究院

アジェンダ

1. IoTのセキュリティ課題

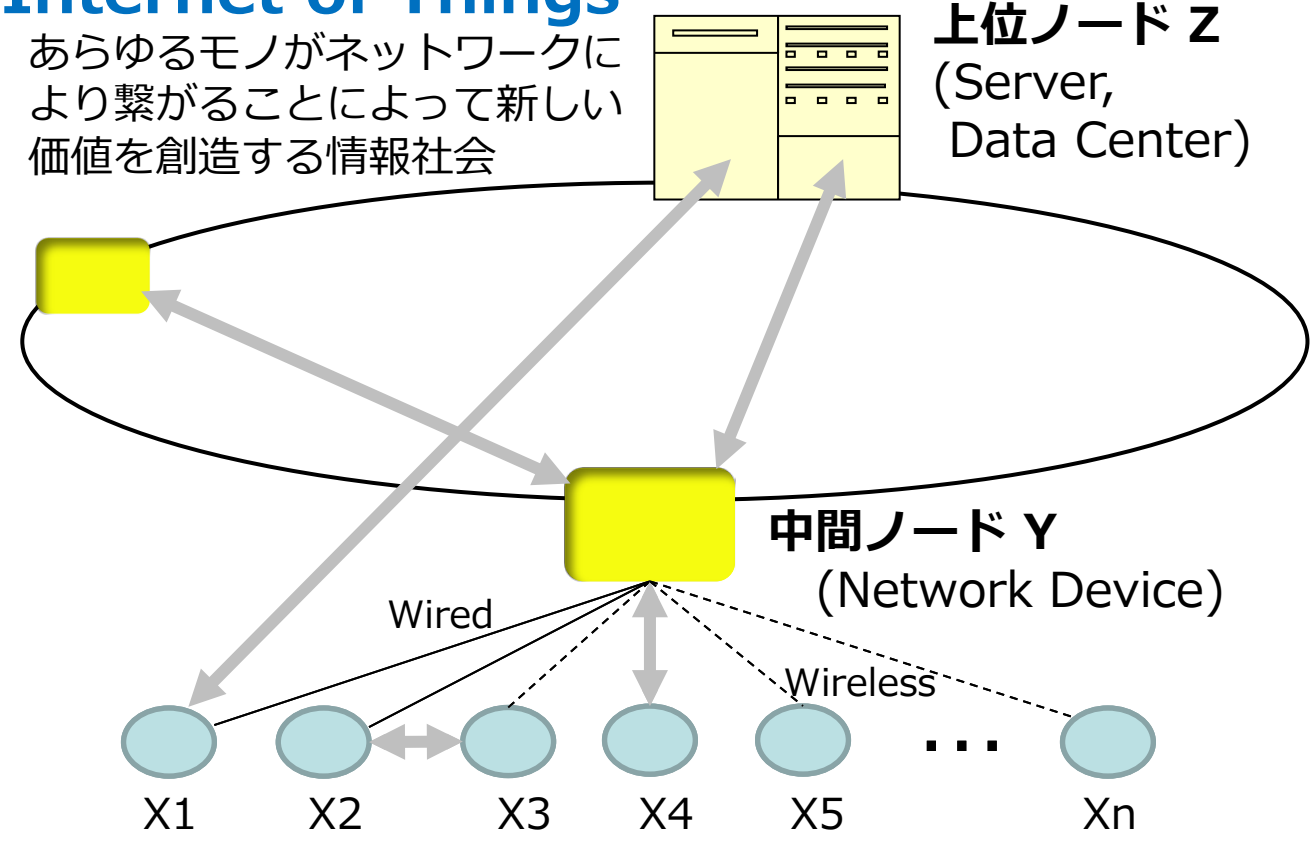
2. どこでも公開鍵暗号

3. さらに高機能暗号導入へ

新しい情報社会の概念が、
Cyber Physical Systemや**Internet of Things (IoT)** といった言葉で語られ、
・物理世界あるいは論理世界からの**データの計測**、・その**通信**、**蓄積**、**処理**を踏まえた
・**利用**（物理世界の**制御**を含む）、・その**結果の確認**、・さらには**保守管理**など
の全ての側面に関し、**適切なセキュティ**が求められる時代が到来しようとしている。

Internet of Things

あらゆるモノがネットワークにより繋がることによって新しい価値を創造する情報社会

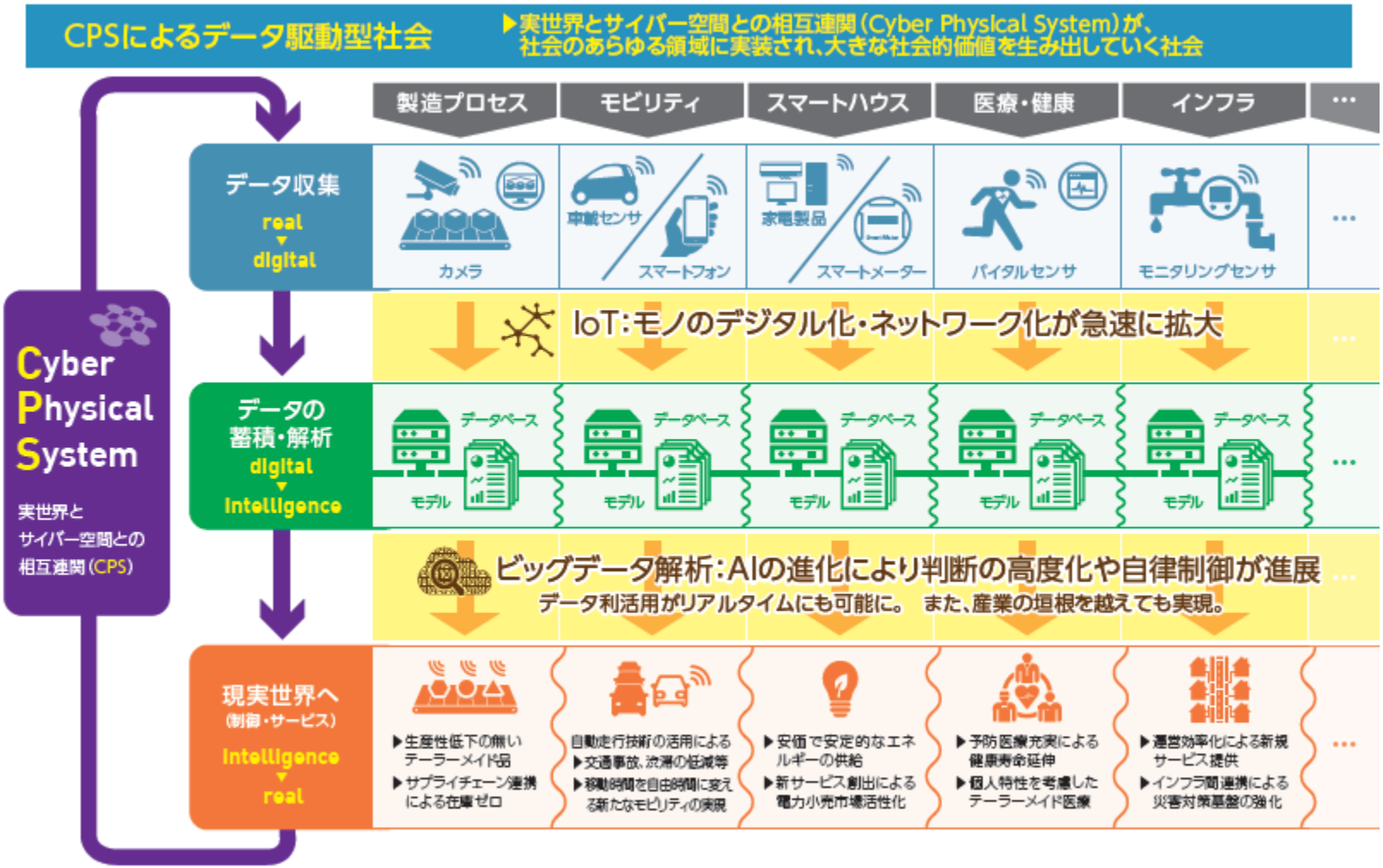


センサ／アクチュエータ, マイコン搭載／非搭載
OS搭載／非搭載, 有線通信／無線通信, 安定な電力供給の有無

主な脅威

- X, Y, Zの改竄、不正な書換え
- X, Y, Zのなりすまし
- X, Yの仕様と機能の乖離
- 不正情報の混入
- 情報漏洩
- 処理に対する攻撃
- 計測に対する攻撃
- 可用性に対する攻撃
- 人命、生活、産業、経済、社会に対する攻撃
- 攻撃側の手先にされる可能性
- ・・・・・

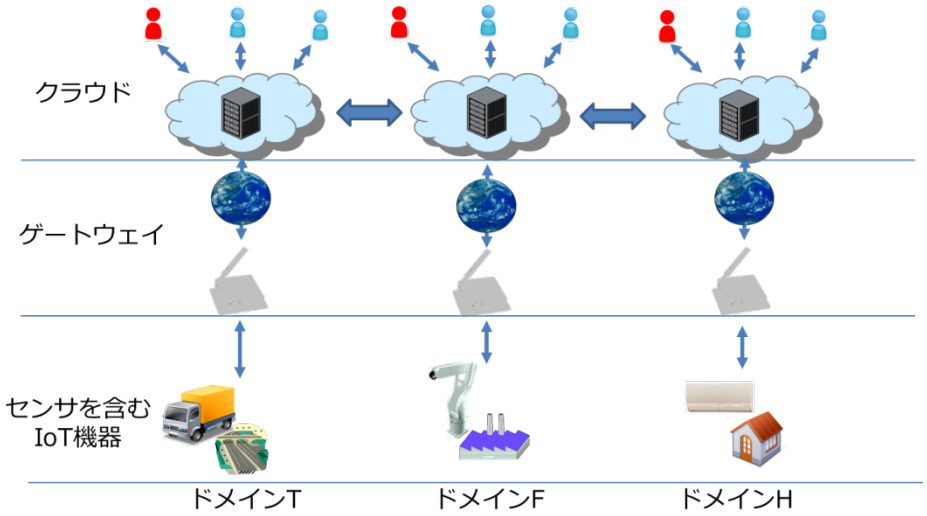
CPS/IoT



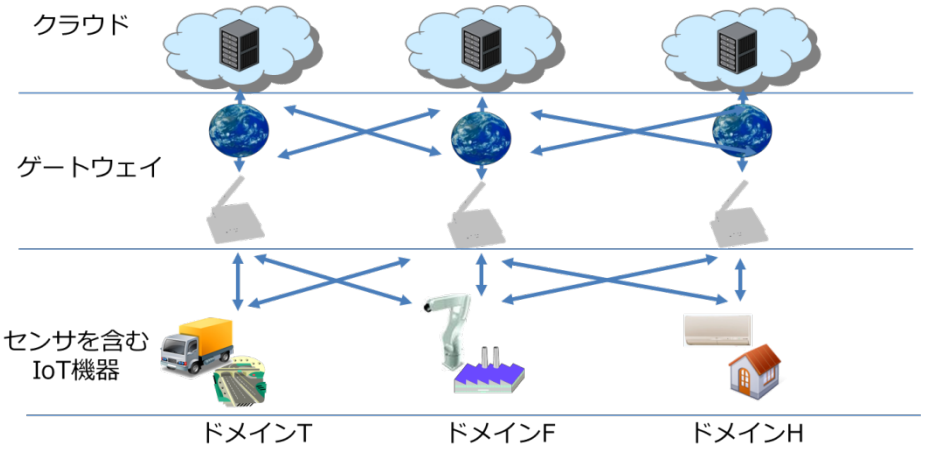
経済産業省・産業構造審議会商務流通情報分科会・情報経済小委員会
「中間取りまとめ ～CPSによるデータ駆動型社会の到来を見据えた変革～」2015年5月21日
http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/report_001.html

IoTアーキテクチャの展開（仮説）

1（2020年頃まで？）



2（2030年頃には）



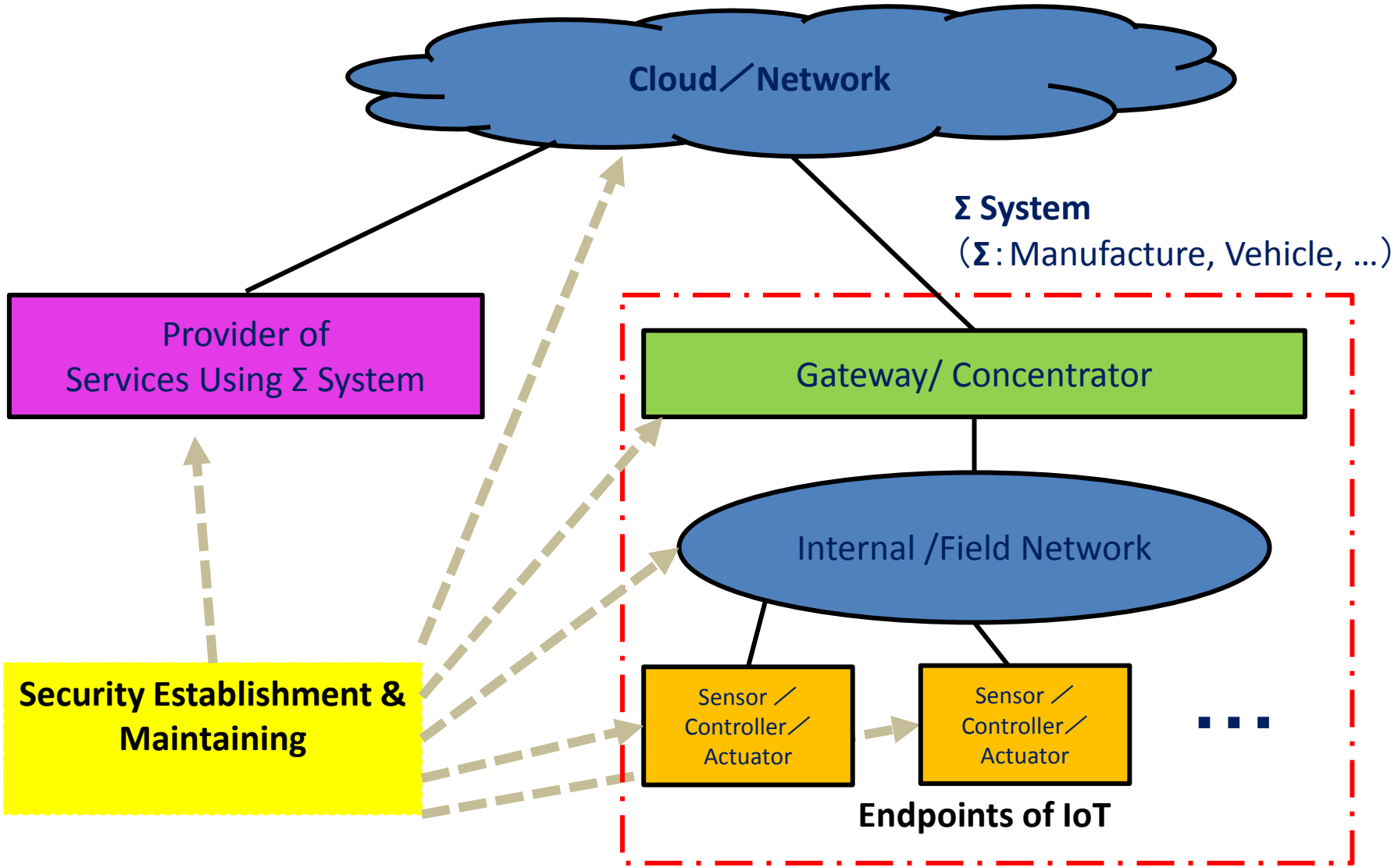
ややIoT

- 現在はドメイン、あるいは事業主毎に、垂直統合でIoTアーキテクチャが構成されている 。
- ドメイン間、あるいは事業主間で、クラウドを介した部分的な情報交換は行われる。

オープンなIoT

- ドメイン、事業主を問わず、 IoTの様々なレイヤ間でデータ流通のメッシュ化、サービスの多層化、仮想化が進む。
- 複数のステークホルダーが多様に繋がる究極のIoTに向かって展開する。

IoTのモデル例



- **今後、IoTシステムへの攻撃事案は飛躍的に増加することが見込まれる。**
- **とりわけ、次の二つの事例については、特に注意が必要である。**

- 重要な資産を保護し特にセキュリティを必要とするIoTシステム（例: 警備, 医療,自動車,ロボット）が攻撃される。

- IoTシステムが、重要な資産を保護し特にセキュリティを必要とする重要インフラ等のシステムに接続していて、IoTシステムの末端機器から侵入を受け、重要インフラ等が攻撃される。

➢ 重要なセキュリティ項目

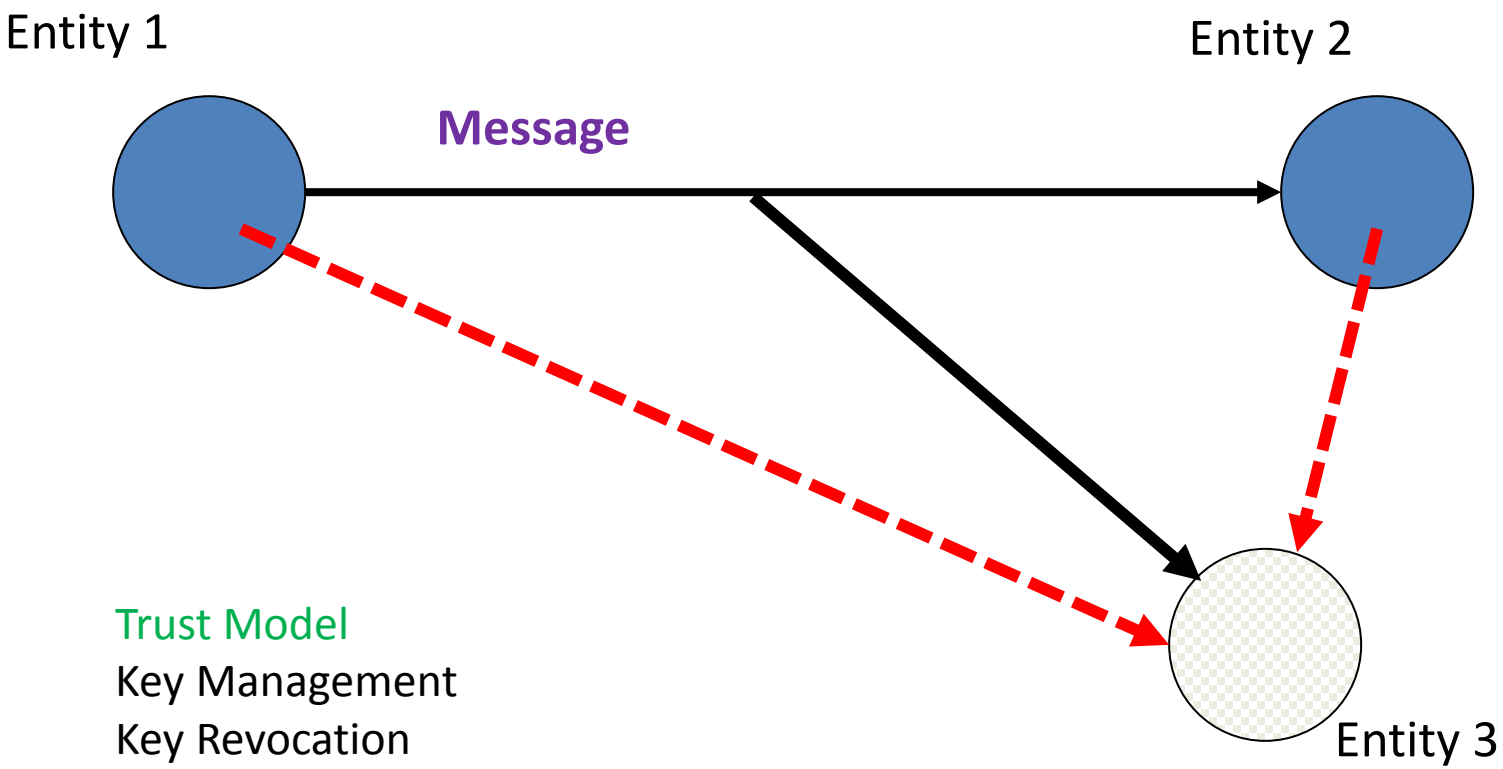
- 守秘性（機密性）Confidentiality:
  「読む」ことに関するセキュリティ

- 一貫性（完全性）Integrity:
  「書く」ことに関するセキュリティ

- 可用性　Availability:
  「使う」ことに関するセキュリティ、
  DoS攻撃への耐性

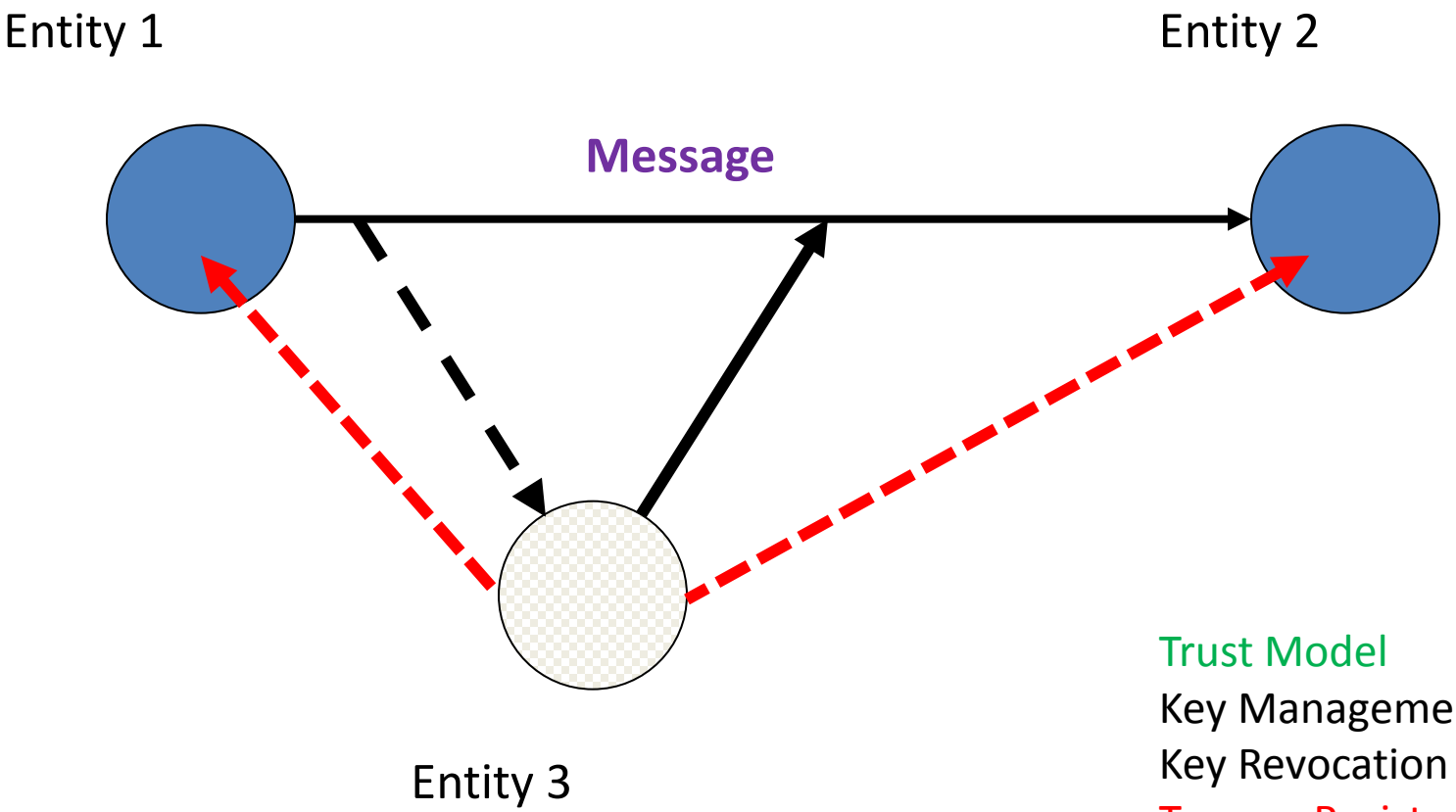
を失わせようとする攻撃が大きな脅威となる。

Confidentiality（守秘性）



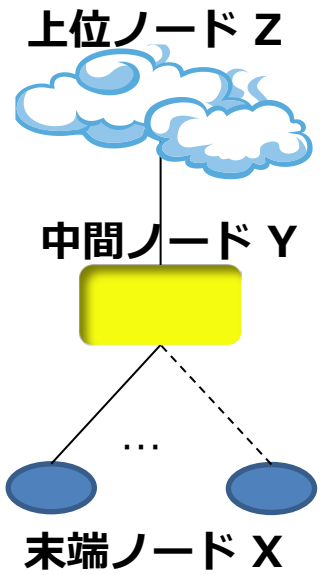
Trust Model
Key Management
Key Revocation
Tamper Resistance
Clone Resistance

Integrity（完全性, 一貫性）, Authentication （認証）



Trust Model
Key Management
Key Revocation
Tamper Resistance
Clone Resistance

IoTにおける信用とセキュリティ



私見：将来のオープンなIoTシステムにおいては
次のような「信用」に係る事項が大きな課題となる。

① **ビッグデータの利用者であるクラウド側（上位ノード）は、一定の水準の「品質」が期待できるデータを入手したい。**
② **ビッグデータの提供側（末端ノード、中間ノード）は、自らが提供するデータの「品質」を利用者側に主張したい。**

- ここで、**データの「品質」**とは、
  データに付随する属性（データ取得に使われたセンサのID、センサ設置環境、使用環境、計測時刻、計測対象など）とその**実態との整合性**を確認できる程度を指すこととする。
- データの品質は、当然、IoTシステムのセキュリティに強く依存する。

IoTセキュリティの現状把握

IoTPOT: Analyzing the Rise of IoT Compromises

横浜国大の研究紹介：
国際会議 USENIX WOOT 2015 (2015年8月、ワシントンDC)において示した事例とその後

Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto (Yokohama National University), Takahiro Kasama (National Institute of Information and Communications Technology), Christian Rossow (Saarland University).

(国際会議論文)
https://www.usenix.org/system/files/conference/woot15/woot15-paper-pa.pdf

(国際会議発表資料)
https://www.usenix.org/sites/default/files/conference/protected-files/woot15_slides_papa.pdf

(情報処理学会論文　Journal of Information Processing, Vol. 24, No. 3, pp. 522-533, May 2016.)
https://www.jstage.jst.go.jp/article/ipsjjip/24/3/24_522/_pdf

(最新の観測結果)
http://ipsr.ynu.ac.jp/iot/index.html

攻撃の観測方法

受動(passive)型：

観測用ネットワークで攻撃が来るのを待つ

- ダークネットモニタリング
- ハニーポット

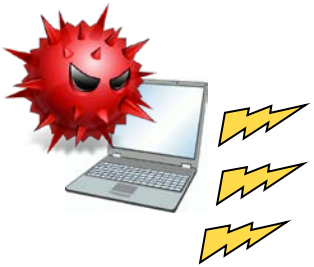
能動(active)型：

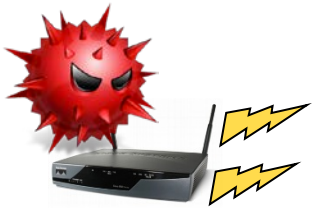
インターネット上の攻撃ホスト情報・脆弱性等を自ら探索する

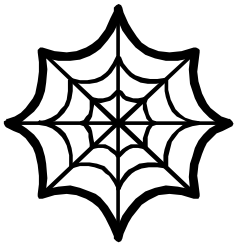
- Web, Telnet, FTP等へのアクセスによる機器、システムの判定
- バックドアポート等の確認

ダークネットによる攻撃の観測

ダークネット：
パソコンや機器等のエンドホストが接続されていないIPアドレス帯





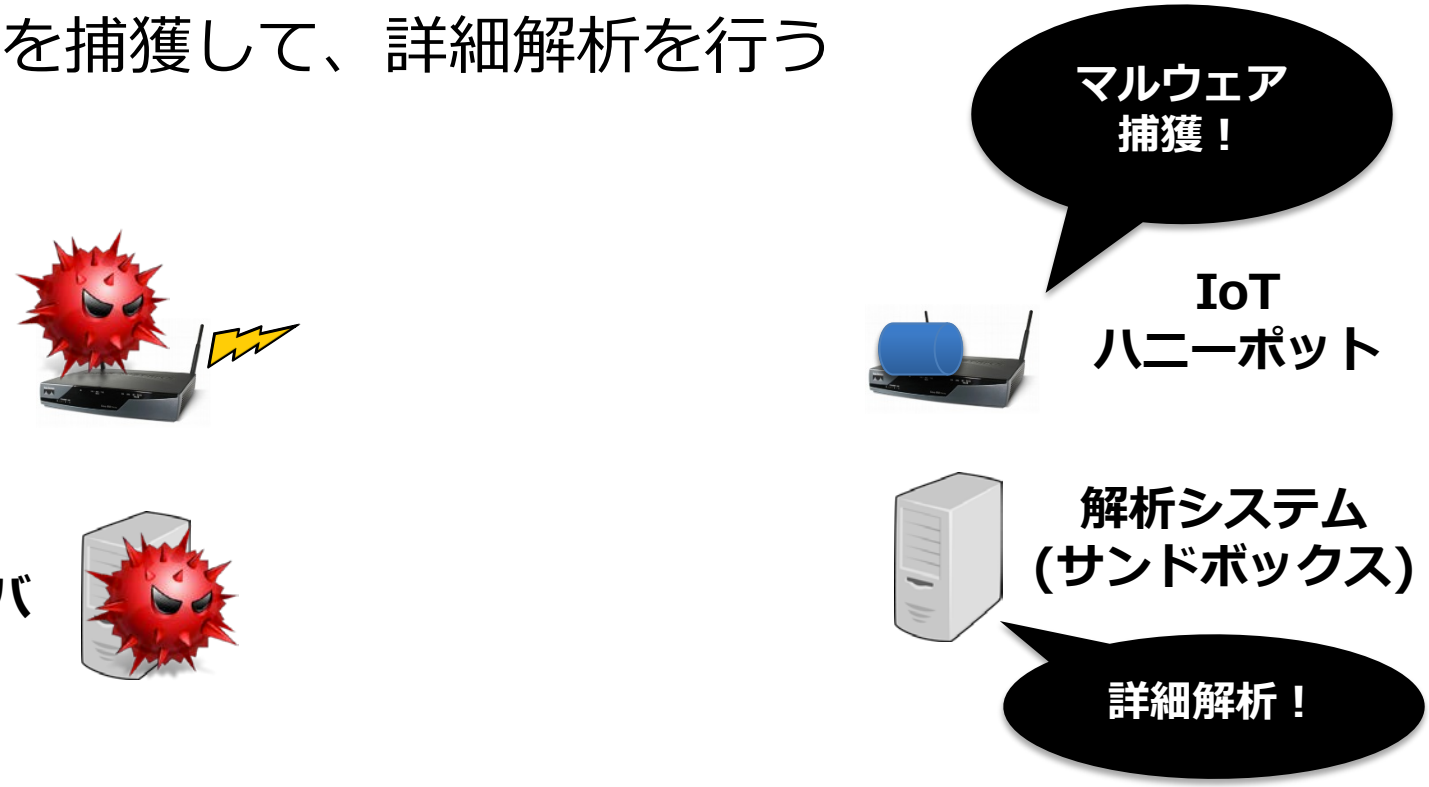


ダークネット

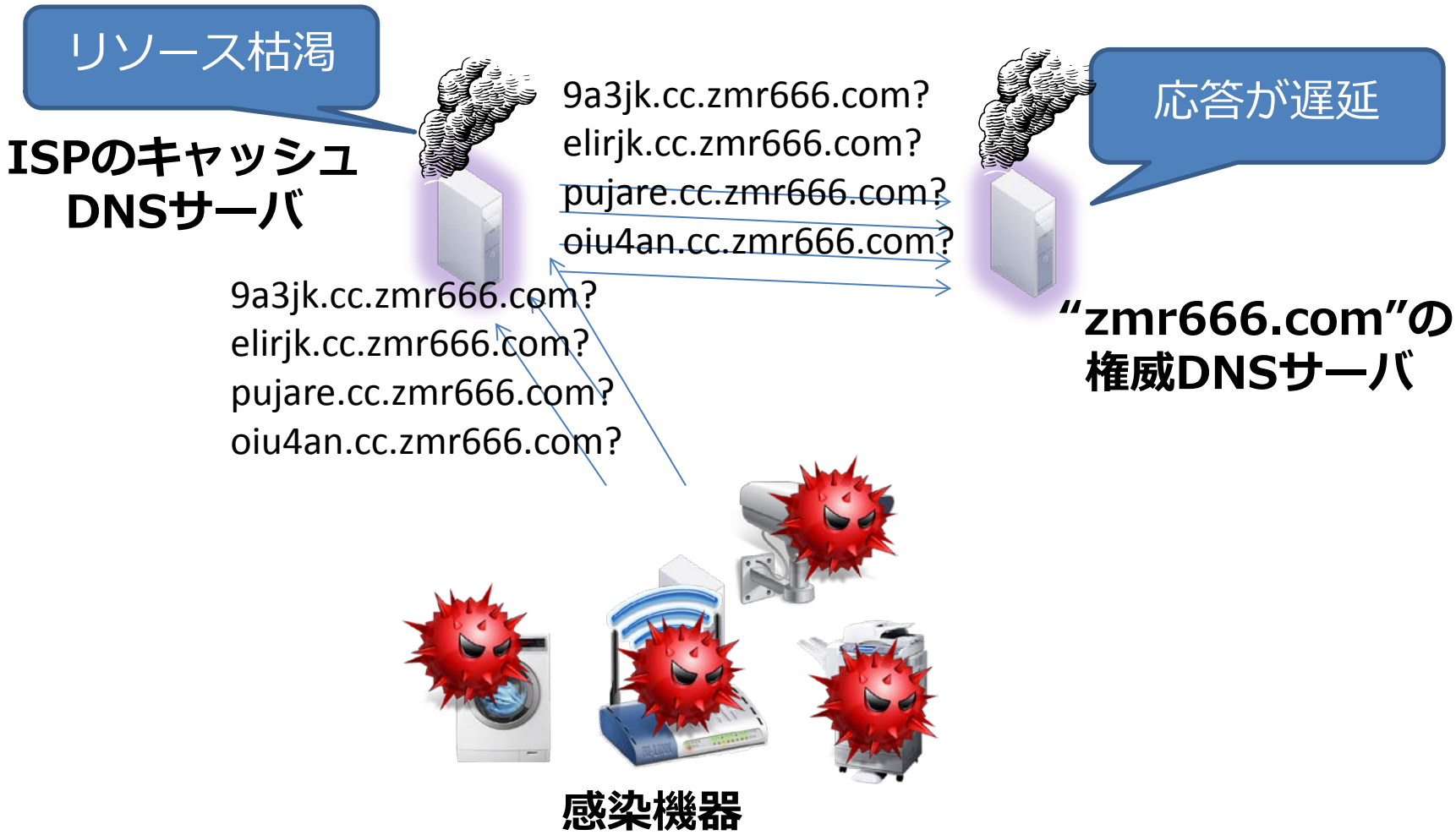
マルウェア(不正プログラム)に感染して外部に無作為に攻撃を行っているパソコン、機器からの攻撃の観測に有効

ハニーポットによる攻撃の観測とマルウェアの捕獲・詳細解析

脆弱なIoT機器を模擬した**囮システム(ハニーポット)**
IoTPOTにより攻撃元と通信を行い、攻撃を観測し
マルウェアを捕獲して、詳細解析を行う



IoT機器に感染した マルウェアはDoS攻撃に加担



他の機器の探索・感染

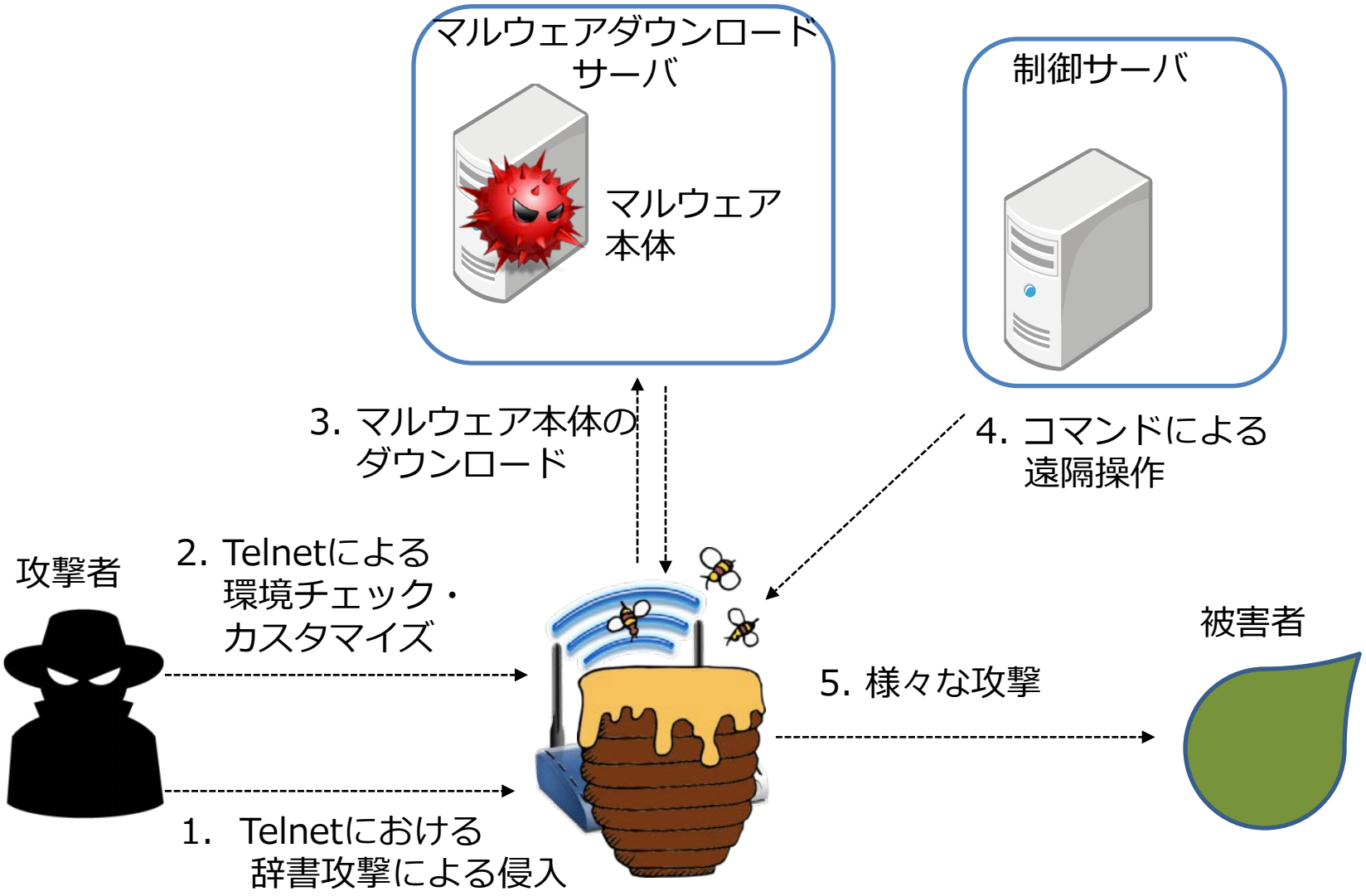
同様のTelnetサービスが動作する機器を探索し感染を広める





感染機器

Telnetベースのマルウェア感染の流れ



IoTPOT(横浜国大発案のIoTハニーポット)で観測して判明した感染機器の種類 19

<500種類以上>

機器はWebおよびTelnetの応答から判断

- 監視カメラ等
  - IP カメラ
  - デジタルビデオレコーダ
- ネットワーク機器
  - ルータ・ゲートウェイ
  - モデム、ブリッジ
  - 無線ルータ
  - ネットワークストレージ
  - セキュリティアプライアンス
- 電話関連機器
  - VoIPゲートウェイ
  - IP電話
  - GSMルータ
  - アナログ電話アダプタ
- インフラ
  - 駐車管理システム
  - LEDディスプレイ制御システム
- 制御システム
  - ソリッドステートレコーダ
  - インターネット接続モジュール
  - センサ監視装置
  - ビル制御システム
- 家庭・個人向け
  - Webカメラ、ビデオレコーダ
  - ホームオートメーションGW
  - 太陽光発電管理システム
  - 電力需要監視システム
- 放送関連機器
  - 映像配信システム
  - デジタル音声レコーダ
  - ビデオエンコーダ/デコーダ
  - セットトップボックス・アンテナ
- その他
  - ヒートポンプ
  - 火災報知システム
  - ディスク型記憶装置
  - 医療機器(MRI)
  - 指紋スキャナ

国内メーカの機器の感染事例も複数確認。感染機器情報はJPCERT/CC、NISC (内閣サイバーセキュリティセンター)に提供、または、メーカに直接提供。

IoTPOTなどを用いた観測から

IoT機器の大量マルウェア感染は深刻

- **感染機器数は増加(侵入に使用するid/passwordも急激に増加)**
  500種類以上
- **2016年夏ごろから急増。横浜国大では9月に100万超**
- **IoT機器が標的のマルウェアMiraiの影響が大と想定**
- **国内の感染機器数も増加**
- **国内メーカの感染事例を複数確認**
- **大規模サービス妨害攻撃への加担を確認(600Gbps超の攻撃も)**
  2016年10月に米国では、インターネットのインフラ(DNSサービス)
  を提供するDynへの大規模攻撃あり

アジェンダ

1. IoTのセキュリティ課題

2. どこでも公開鍵暗号

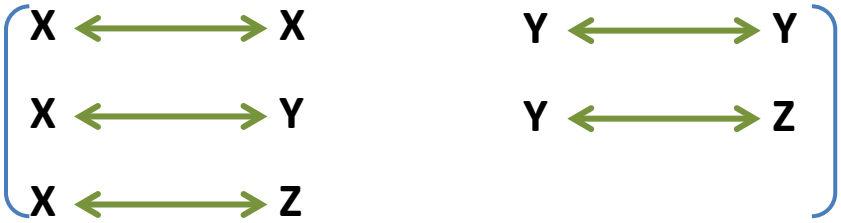
3. さらに高機能暗号導入へ

さて、どうするか？

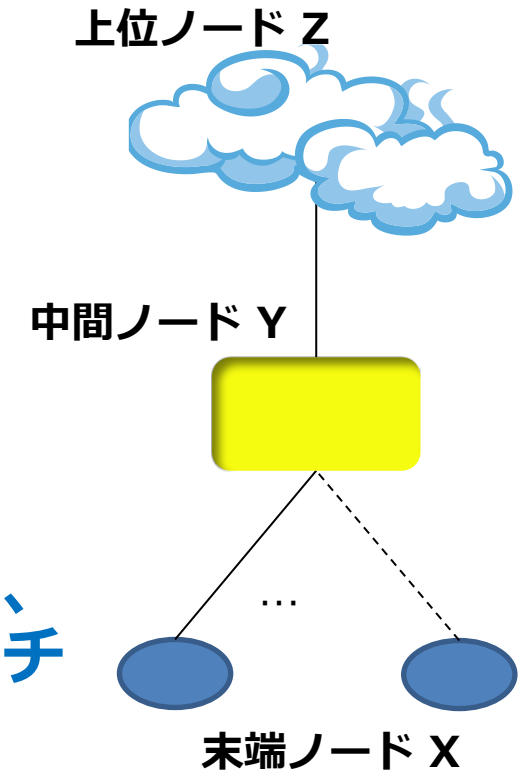
この状況に対し、telnetなどは使わせないようにするというアプローチがある。しかし、徹底できるのか？

アプリケーションや管理プロトコルが動作する場として、

- **ノード X, Y　の保護・監視、および、**
- **チャネル**



を通るデータの保護が重要。



２つの方向性

1. **中間ノードおよび上位ノードで対策する、つまり、多層の境界防御を行うアプローチ**
2. **末端ノードを強くするアプローチ**
   - **リソース制約**
   - **厳しい環境**

➢ IoTセキュリティ実現に向けて 中間ノード等で対策するアプローチの有効性と限界

- 中間ノードが末端ノードを保護する
  - ✓ 中間ノードYと末端ノードXの間のセキュリティは別途手当されるとの仮定が必要
- 既存の末端ノードを変更しないで対応できる場合がある

➢ 短期的には現実的かつ有効なアプローチである

- 技術的には、
  異常検知技術（不正挙動、不正トラフィックの監視）
  ホワイトリスト方式など
  が中心となる
  - ✓ 検出の見逃し／過剰検知は避けられない
  - ✓ End-to-endのセキュリティが達成できない

➢ このアプローチだけではIoTに係る脅威に対処しきれない

- 末端ノードを強くするアプローチ
- IoTシステムのセキュリティ確保には、本質的に**暗号技術**を利用した**構成機器間の(相互)認証**と**データ保護**が必須である。耐タンパー性も確保も重要である。

- ✓ **しかし現状は、**実際のIoTシステムにおいて、**暗号による機器間相互認証やデータ保護が実現されている事例は少ない**。2014年7月HP社調査によれば、IoTシステム構成機器の内、**暗号機能を使用していない比率は70%** とされる。
- ✓ 暗号技術（共通鍵方式、公開鍵方式）のうち、共通鍵暗号すらまだあまり使われていない。

- 末端ノードへの暗号導入が困難であることの要因（推定）
  - ✓ 計算リソース(含むエネルギー)不足
  - ✓ 耐タンパー技術を導入する余裕がない
  - ✓ 鍵等の管理のコスト
  - ✓ システムに影響が及ぶ
  - ✓ 機器の価格に見合わない
  - ✓ ・・・

末端ノードへの暗号導入の困難性を解消に向けた方針

- ✓ 計算リソース(含むエネルギー)不足
  - **軽量暗号**
  - **ハードウェア暗号エンジン**
- ✓ 耐タンパー技術を導入する余裕がない
  - **耐タンパーソフトウェア**
  - **ハードウェア上の工夫**
- ✓ 鍵等の管理のコスト
  - **ホワイトボックス暗号**
  - **公開鍵暗号の導入**
- ✓ **システムに影響が及ぶ**
  - **ハードウェア化**
- ✓ 機器の価格に見合わない
  - **ローエンドマイコンにデフォールトで暗号技術を組込む**
- ✓ ・・・

大規模IoTシステムで公開鍵暗号が自在に活用できたならば

1.	「共通鍵暗号」しか使えない場合に比べ、 ディジタル署名の検証が秘密でない公開鍵で行える、 メッセージの暗号化が秘密でない「公開鍵」で行える等の、 格上のセキュリティを達成可
2.	多数の末端ノードの鍵管理・セキュリティ管理コストを圧倒的に削減可
3.	大規模IoTの利便性とセキュリティの両立に大きく貢献
4.	「高機能暗号(※)」のIoTへの導入の足掛かりとなる ※ 秘匿検索（暗号化されたデータベースの検索）や集約署名（多数のディジタル署名が一括検証可能な方式）などの、公開鍵暗号よりさらに機能性の面で進んだ先端暗号技術

公開鍵暗号技術のアイディア
Eg. Digital Signature Generation

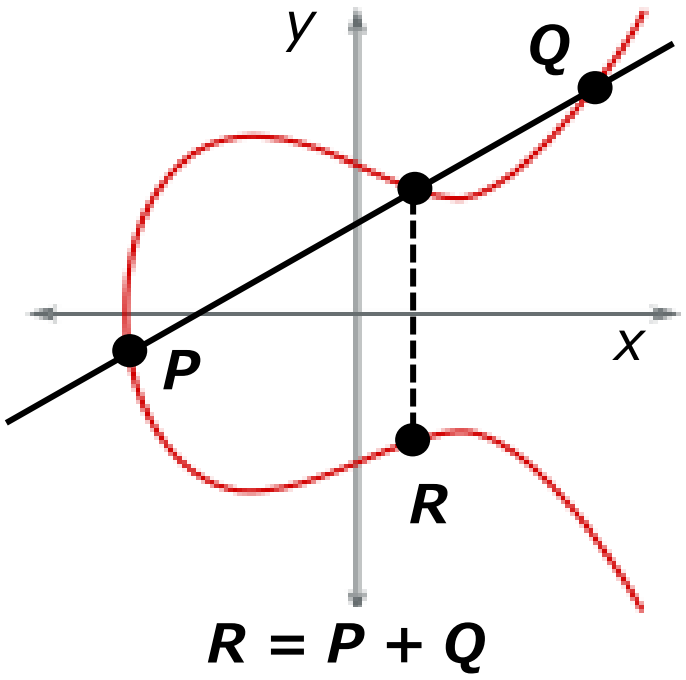
■ Key $K=(K_1,K_2,\ldots,K_{256})$ Message $M=(M_1,M_2,\ldots,M_{256})$
Functions $G_1,G_2,\ldots,G_{256}$
Signature $S=(S_1,S_2,\ldots,S_{256})$

$$\begin{cases} S_1 = G_1(K_1,K_2,\ldots,K_{256},\ M_1,M_2,\ldots,M_{256}) \\ S_2 = G_2(K_1,K_2,\ldots,K_{256},\ M_1,M_2,\ldots,M_{256}) \\ \\ S_{256} = G_{256}(K_1,K_2,\ldots,K_{256},\ M_1,M_2,\ldots,M_{256}) \end{cases}$$

■ Design $G_1,G_2,\ldots,G_{256}$ so that solving the system of equations to get K is extremely difficult.

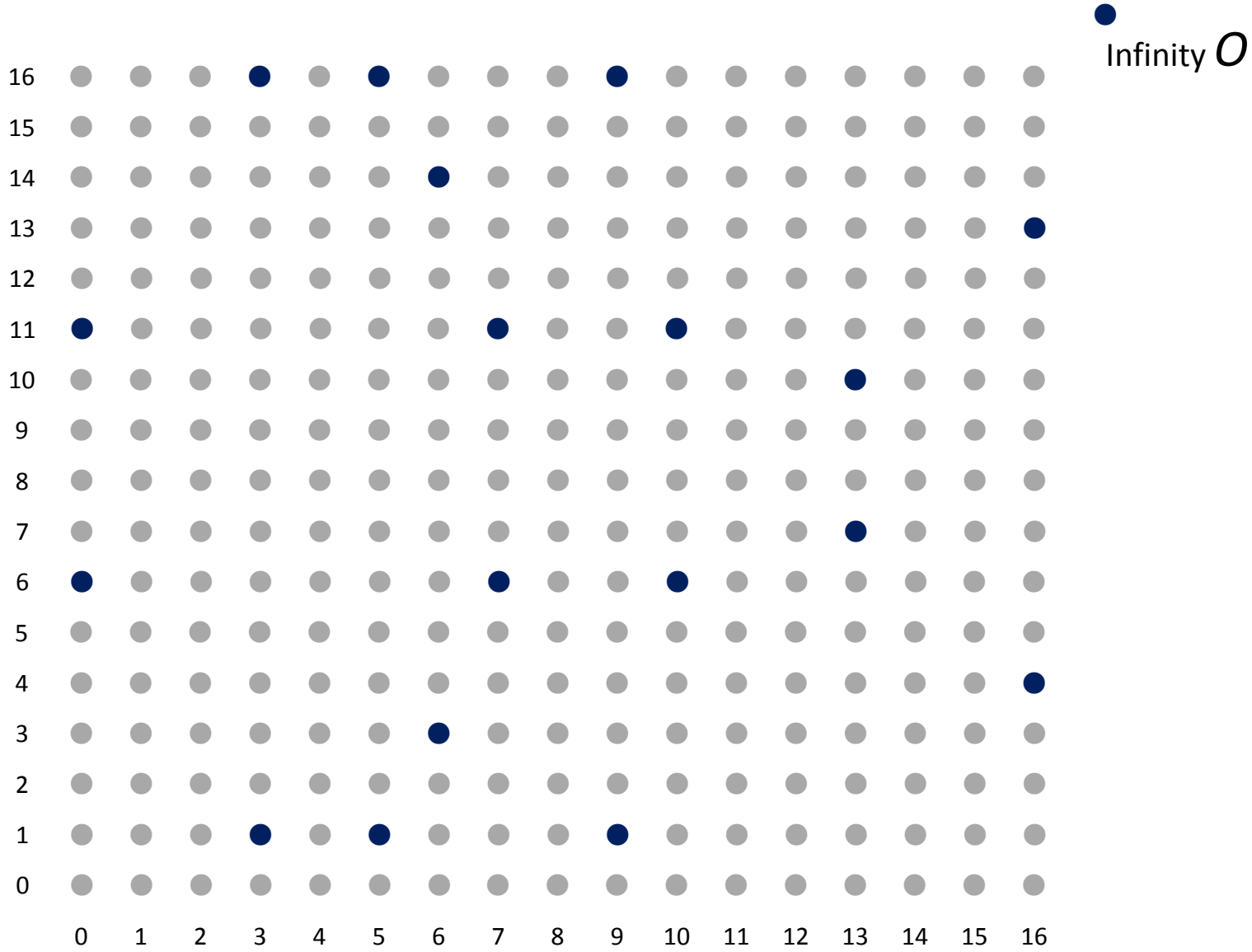
低電力実装・長期使用に適した楕円曲線暗号

- 公開鍵暗号のクラス **楕円曲線暗号** は、広く使われてきたRSA暗号に比べ、小型で低電力実装ができ、かつ長期使用に対し有利であり、今後のIoTに適している。鍵共有、ディジタル署名、認証、暗号化のための**楕円曲線暗号標準**も充実している。

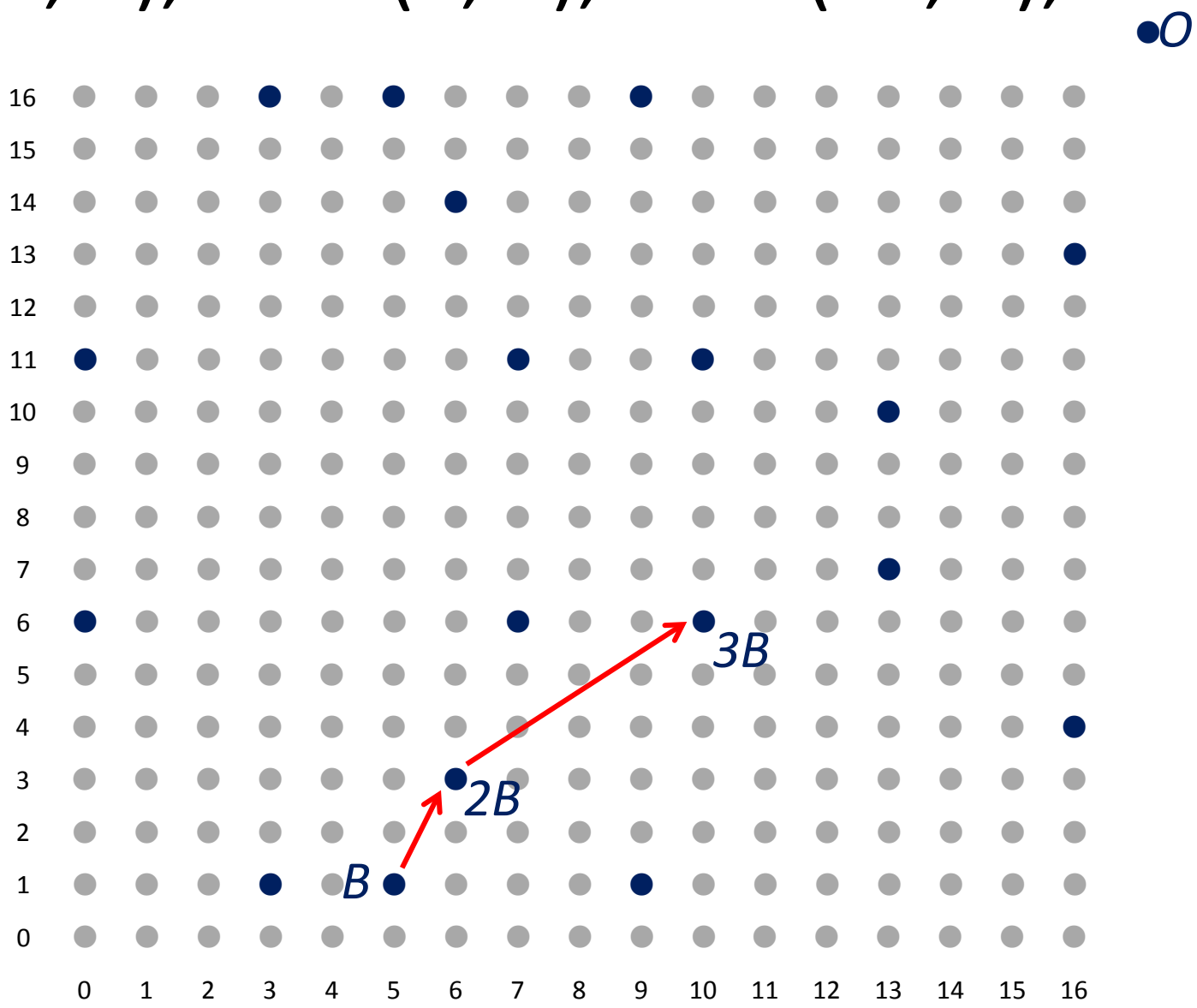


楕円曲線G：有限体**K**上の指定された3次の定義方程式を満たす点と無限遠点からなる集合で、**加算に関して群**をなす。楕円曲線暗号に用いる**G**は、点 ***A***, ***B***に対し, ***B*** = *s****A*** なるスカラー (**離散対数**) *s* を求めることが困難であるように選択される。
K は256 ビット程度のサイズ。

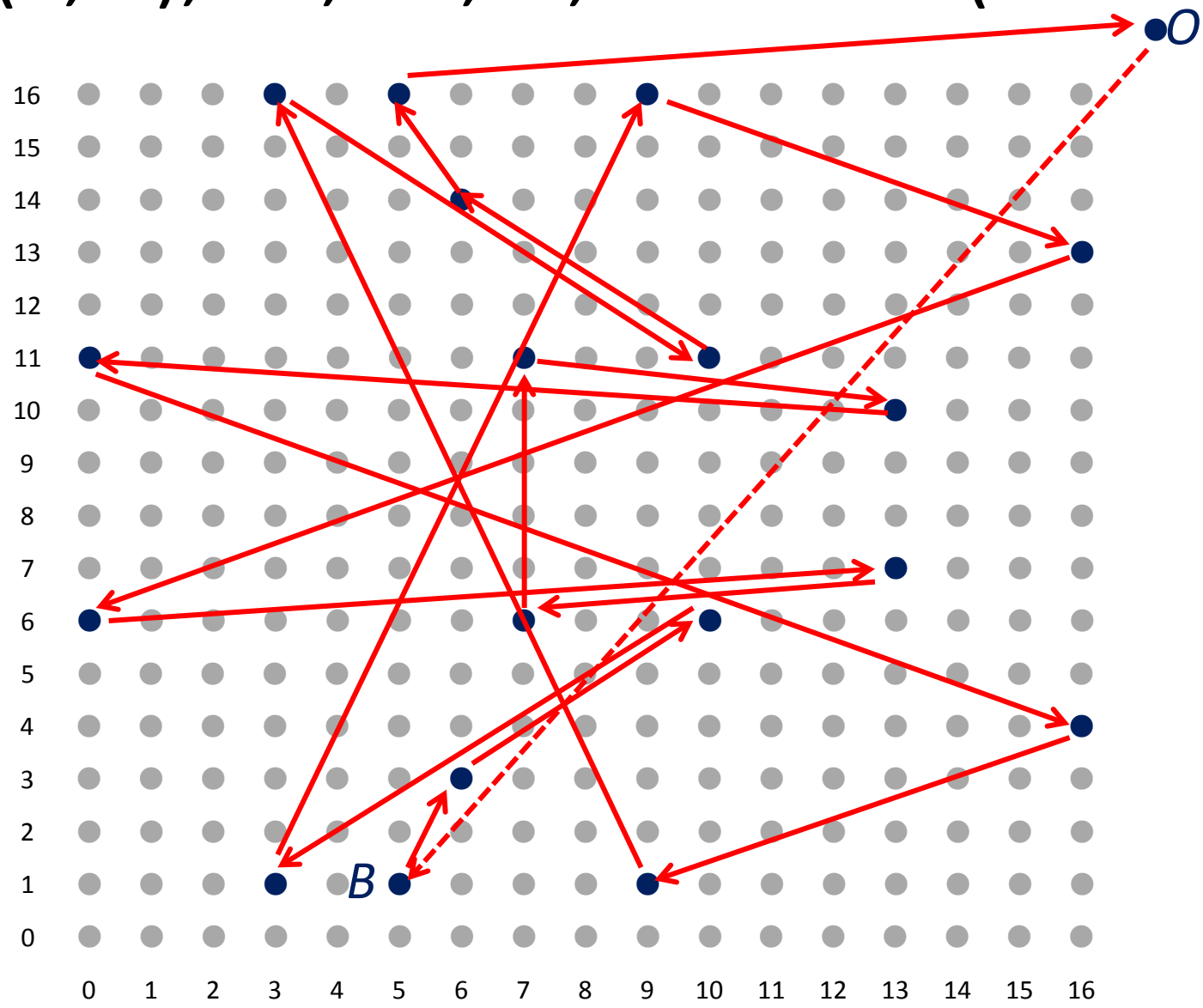
Elliptic Curve : $y^2 \equiv x^3+2x+2 \pmod{17}$ (19 points)



$B = (5, 1), 2B = (6, 3), 3B = (10, 6), \ldots$

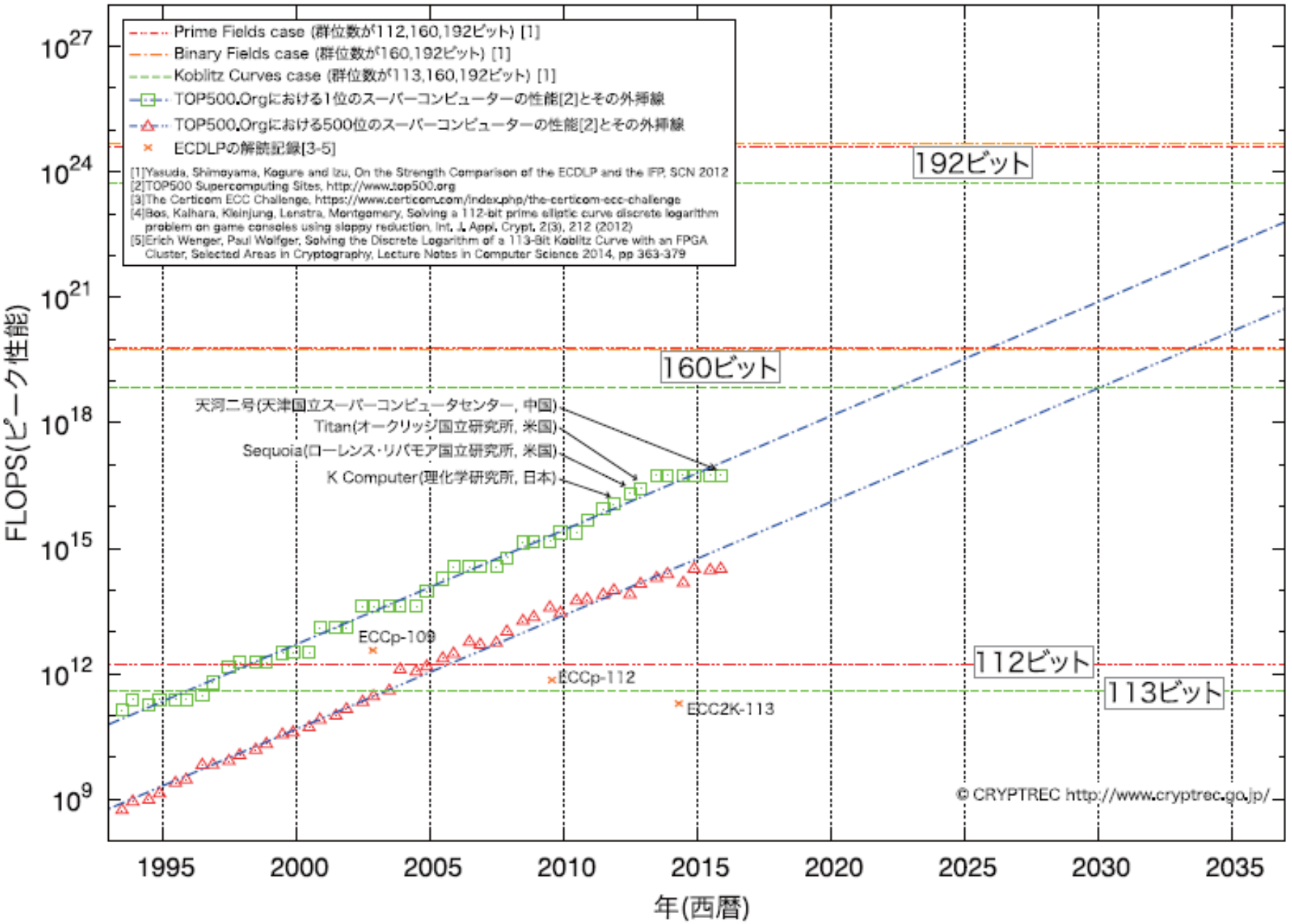


$B = (5, 1), 2B, 3B, \ldots, 19B=O \quad (20B = B)$



CRYPTREC Report 2015 より抜粋

ρ法でECDLP を1 年で解くのに要求される処理能力の予測(2016 年2 月更新)



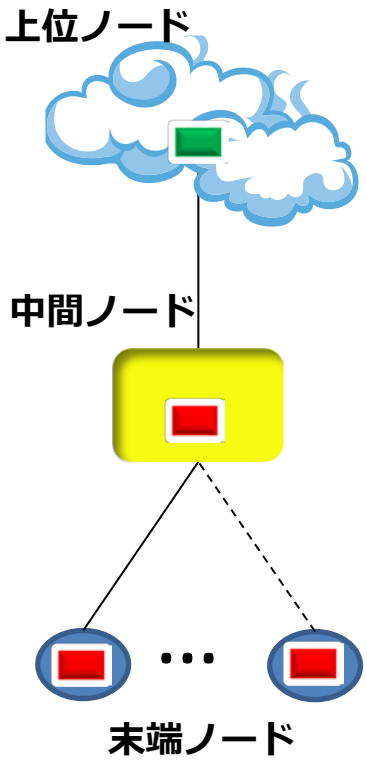
「SIP 重要インフラ等におけるサイバーセキュリティの確保」 IoTのセキュリティを実現する超低電力暗号実装技術

研究代表者　松本

どこでも公開鍵暗号を！

Secure Cryptographic Unit SCU

末端ノードでも公開鍵暗号の自在な活用を可能としIoTのセキュリティ実現に貢献



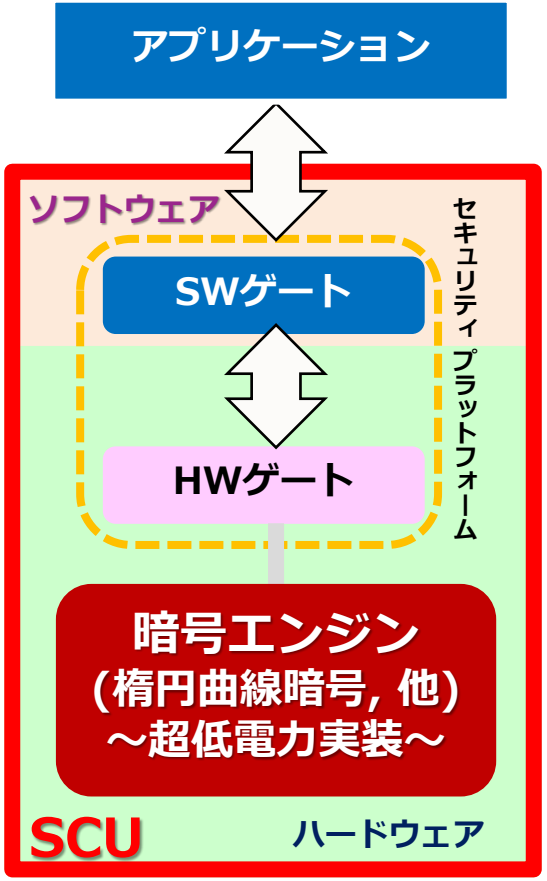
① **セキュア暗号ユニットSCUの開発**

② **社会実装に向けたSCU導入分析 およびモデルシステムによる実証**

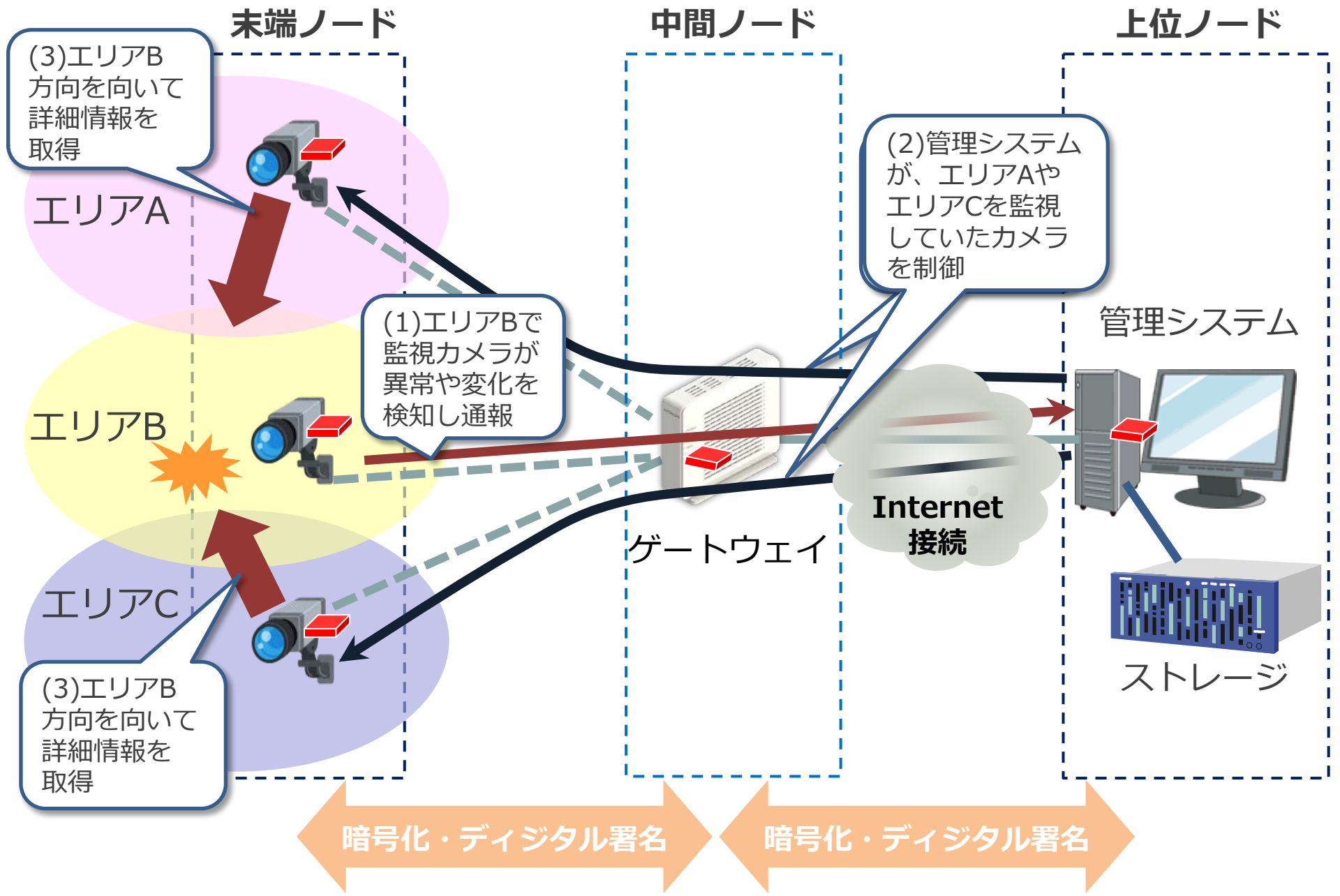
③ **ハードウェアトロイ対抗技術の研究**

性能の目標は、256ビット楕円曲線暗号処理/ディジタル署名の生成・検証処理において、
末端ノードでは1ミリワット級の超低電力および十キロゲート級の小面積・低コスト
中間ノードでは10,000回／秒以上の超高速動作に至るスケーラビリティを備えることとし、
実用性の高い暗号エンジンの構築技術を開発する。

さらに、セキュア処理の信頼の基点となるデバイス真正性と耐タンパー性を確保する暗号ユニットの構築法を確立し、
セキュア暗号ユニットをプロトタイプ実証する。



セキュア暗号ユニット 適用例：監視カメラシステム



総合科学技術イノベーション会議　**戦略的イノベーション創造プログラム（SIP）**
「重要インフラ等におけるサイバーセキュリティの確保」プログラムディレクタ　後藤厚宏

NEDO

委託

研究開発責任者
松本　勉 (横浜国立大学)

ルネサスエレクトロニクス株式会社

電子商取引安全技術研究組合
研究グループ事務局
[組合員：日立製作所、
ルネサスエレクトロニクス、
NTTデータ、東芝、凸版印刷、
共同印刷、ECSEC Laboratory]

再委託

セコム株式会社

共同実施

横浜国立大学　（松本　勉）
東京大学　（池田　誠）
電気通信大学　（﨑山一男）
神戸大学　（永田　真）
東北大学　（本間尚文）
奈良先端科学技術大学院大学　（林　優一）
産業技術総合研究所（菊地克弥）

セキュア暗号ユニットSCUの要件

➢IoTに必要とされる条件で楕円曲線暗号を実装

- リソースに乏しい末端ノードに適した低電力性
- 多様なアプリケーションに対応できる高速性
- 様々な楕円曲線に対応できる汎用性
- 「信頼の起点」として必要な耐タンパー性

➢ローエンドマイコンでのソフト実装における困難性

- 省電力性、処理速度に大きな制約
- 暗号プログラムがアプリに割けるメモリを圧迫
- 耐タンパー性実装のオーバーヘッド大

➢ソフトウェア実装の困難性をハードウェアで解消

- 演算アーキテクチャと半導体技術の協奏

セキュア暗号ユニットSCUの活用

SCUは、**IoTの各ノードに搭載**し、IoTシステムの末端ノードが扱う価値ある情報を守りながら、IoTシステムのセキュリティを確保するために幅広く利用される可能性を有する技術である。

末端ノードの主体は、低価格・低リソースのローエンド機器であり、SCUの研究開発には次の条件を考慮している：

1）国際的に認知されたセキュリティ業界標準に準拠し、第三者認証にも対応できるセキュリティ技術であること。

2）ローエンドMCUからハイエンドMPUまでへの搭載にスケーラブルに対応できる技術であること。

3）あらゆるユースケースに親和性が高く、利活用の容易性が高く、インターオペラビリティに優れていること。

4）導入や活用のための方法や手順が明確であること。

本プロジェクトはこれらを考慮した戦略を立て開発を進めている。

加えて重要な点は、

IoTに適した楕円曲線暗号ベースの公開鍵基盤PKIの普及である。

セキュア暗号ユニットSCUの特長

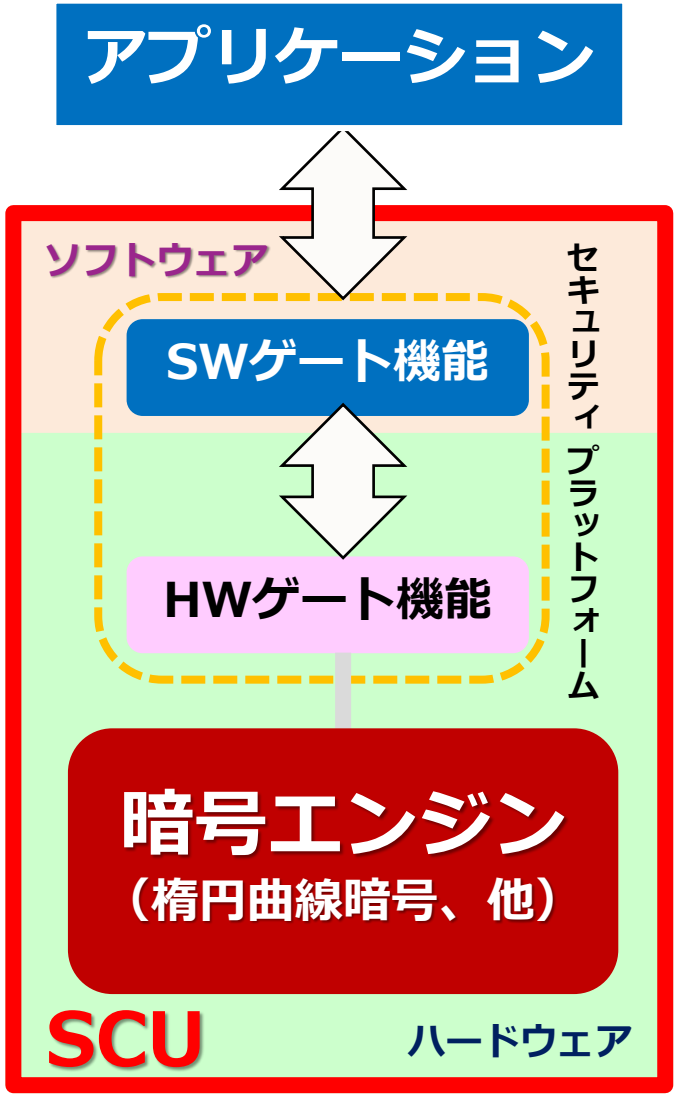
ハードウェア暗号エンジン

256ビットの楕円曲線暗号の処理につき
・末端ノード向きには
　1ミリワット級の超低電力および
　十キロゲート級の小面積・低コストを達成
・中間ノード向きには
　10,000回/秒以上の超高速動作を達成

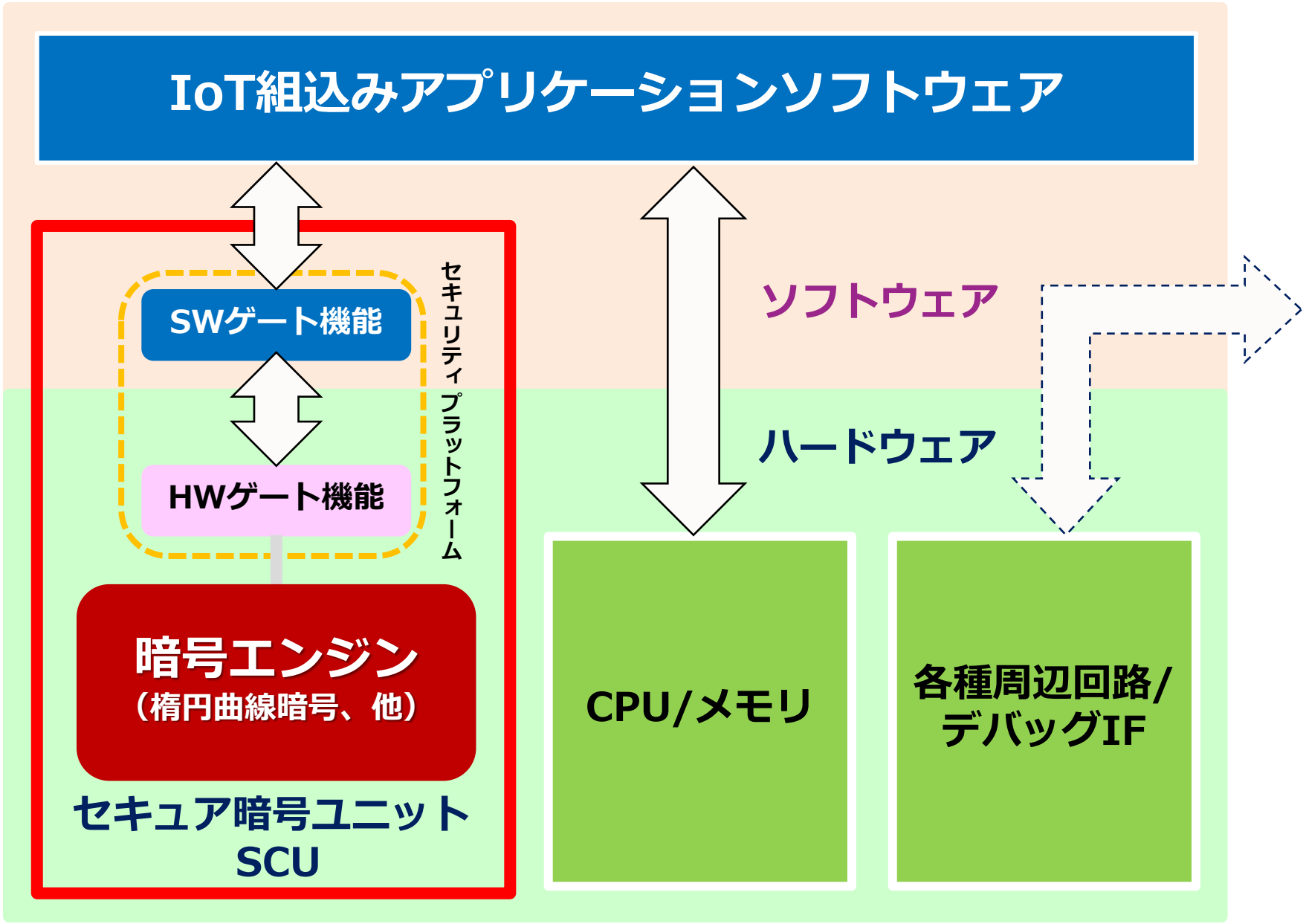
共通鍵暗号等も実装する

セキュリティプラットフォーム

仮にアプリケーションが不正に改変され、暗号エンジンへの不正アクセスを試みたとしても、SWゲート機能とHWゲート機能から構成されるセキュリティプラットフォームが、そのような試みを確実に検出し、アクセスを阻止する



セキュア暗号ユニットSCU内蔵マイクロコントローラの例



セキュア暗号ユニットSCUのプロトタイプと評価ボード

SCU (ハードウェア部分)	**KM10 シリーズ** KM11, KM12,…	・小型・省電力・低レイテンシを最適化する性能指向設計 ・一般的な成熟プロセスから先端CMOSプロセスまで搭載可能 ・ローエンドのマイクロコントローラへの集積化を指向	将来的には、技術統合や、技術ラインナップ化、ユーザによる選択肢化が可能
	KM20 シリーズ KM21, KM22,…	・高スループット・スケーラブル設計 ・先端実装による SiP (System-in-Package)集積化を実現 ・高耐タンパー性の獲得も視野に	
SCU評価ボード	各SCUに共通に(ピンコンパチブルで)使用できる評価ボード		

研究開発スケジュールと活用の展望

2016年 1月 → 2018年 3月 → 2020年 3月 → 2030年

ＳＩＰ研究開発期間

成果の活用

①セキュア暗号ユニット(SCU)

②モデルシステム

③ハードウェアトロイ

暗号エンジン開発
セキュリティプラットフォーム開発
ＳＣＵ試作・改良

評価ボード開発
SCU評価ボード

モデルシステム設計
モデルシステム

ソフトウェア開発
SCU導入や活用のための方法

社会実装のためのTF活動の発展

現実的シナリオでのハードウェアトロイの脅威分析と対策方法考案

用途別ＳＣＵのマイコン等への組込み・製品化

製品版SCUの多様なIoTシステムへの適用

IoTセキュリティの実現

大規模IoTで公開鍵暗号を自在に使えるようにする

1	共通鍵暗号しか使えない場合に比べ、格上のセキュリティを達成可
2	多数の末端ノードの鍵管理・セキュリティ管理コストを圧倒的に削減可
3	大規模IoTの利便性とセキュリティの両立に大きく貢献

アジェンダ

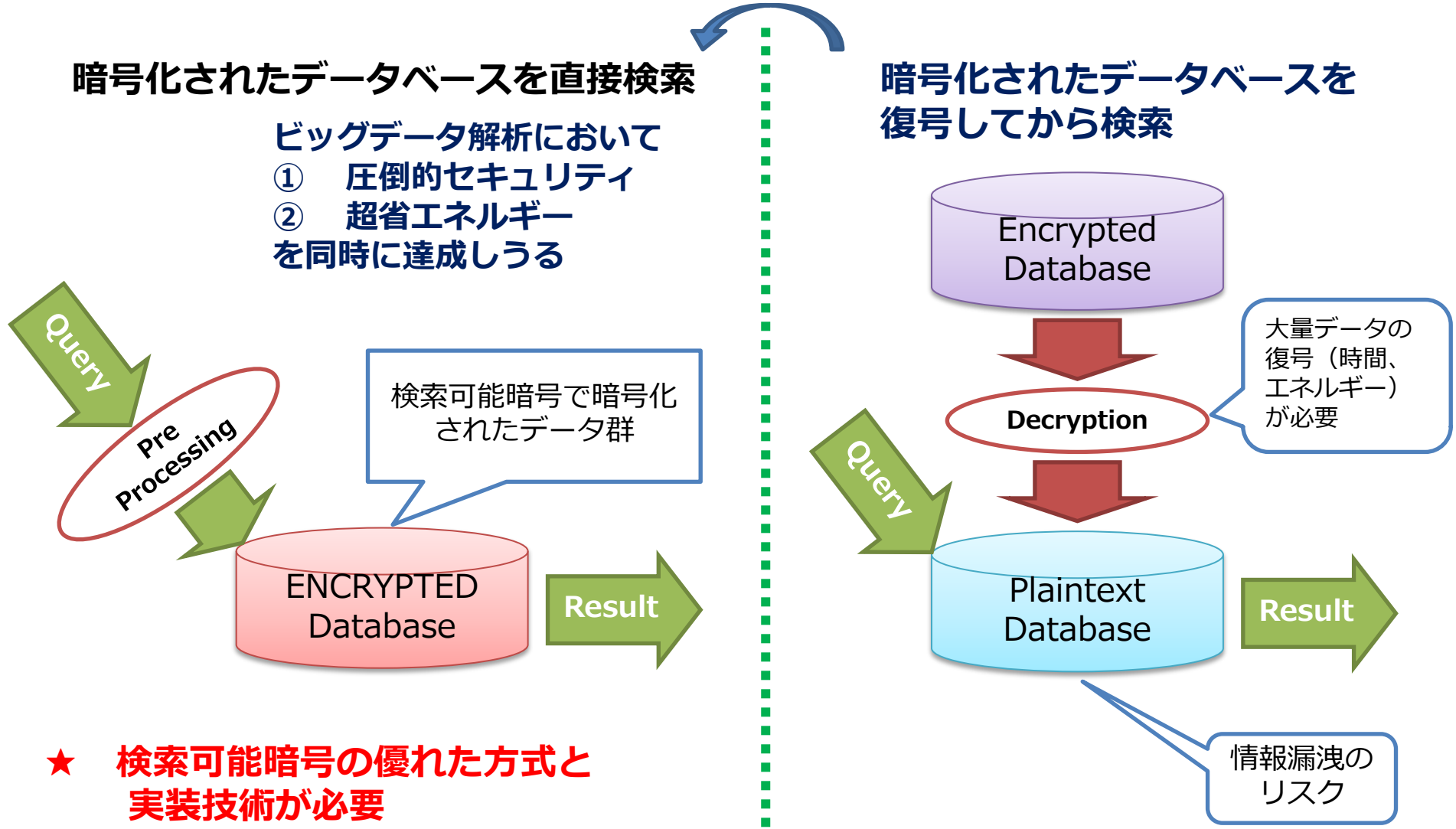
1. IoTのセキュリティ課題

2. どこでも公開鍵暗号

3. さらに高機能暗号導入へ

暗号技術は，**共通鍵暗号**，**公開鍵暗号（含む，ディジタル署名）**から，
さらに多様な機能を実現する**高機能暗号**へと進歩を続けている．

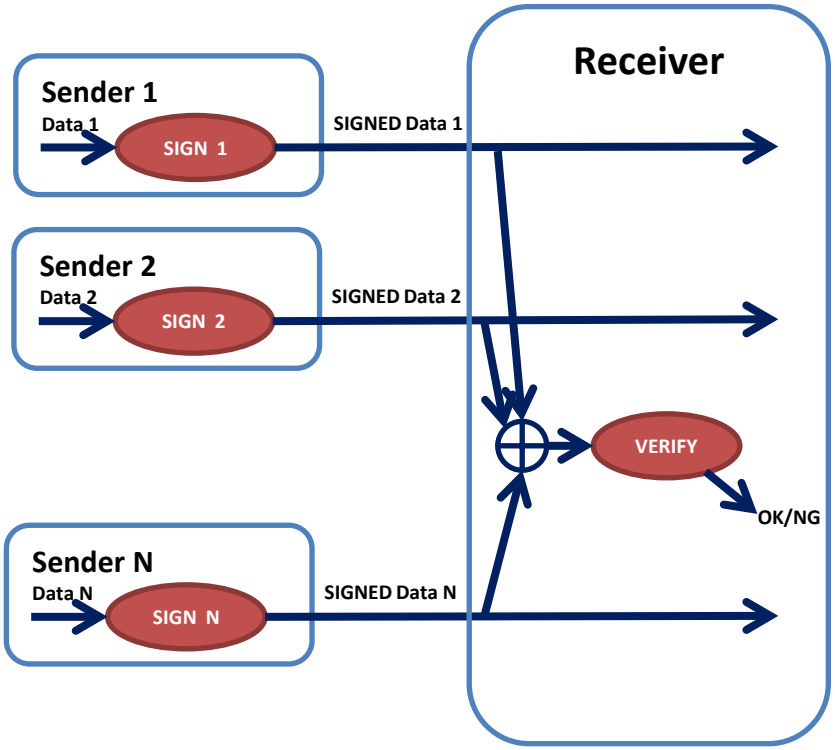
高機能暗号の例１：検索可能暗号（Searchable Encryption）



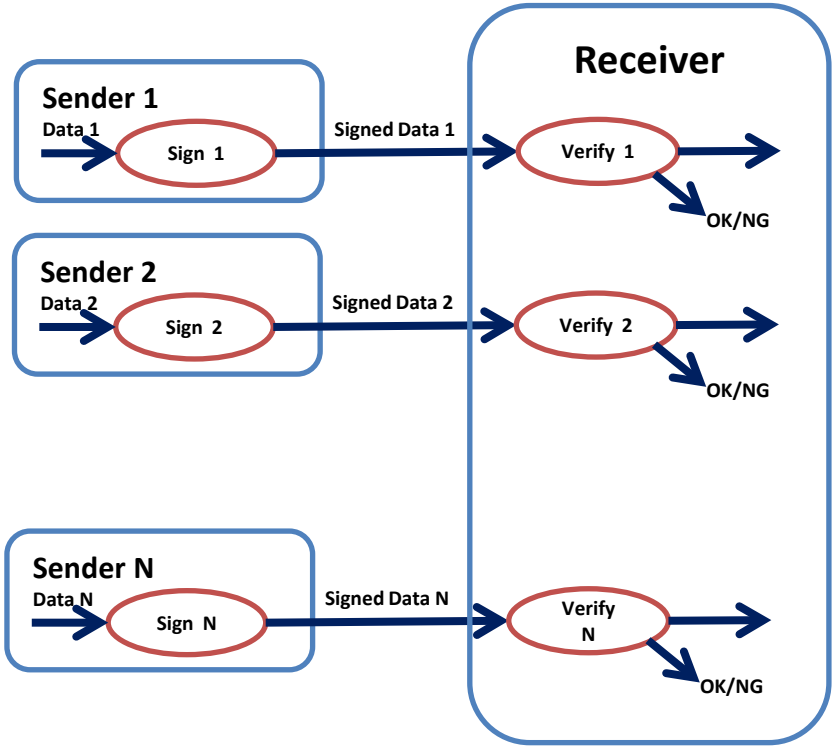
★ **検索可能暗号の優れた方式と実装技術が必要**
← **ペアリングにより可能**

高機能暗号の例２：集約署名（Aggregate Signature）

集約署名による大量の署名データの一括検証



古典的なディジタル署名の個別検証



✓ 署名生成処理 SIGN *i* と Sign *i* の計算量は，同程度.

✓ 署名検証処理 VERIFY は Verify *i* に比べて計算量がかかるが，１回だけでよい.

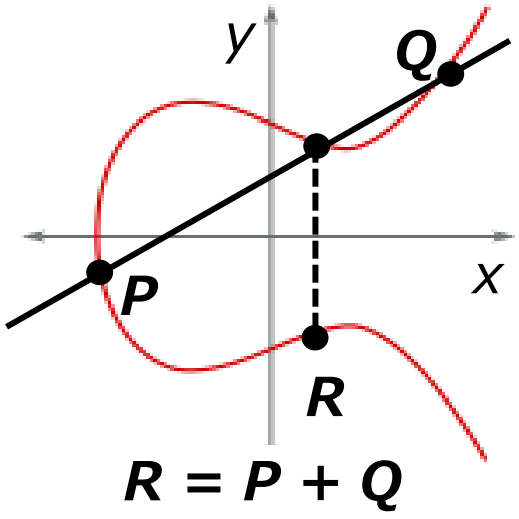
★ **集約署名の優れた方式と実装技術が必要 ← ペアリングにより可能**

ペアリングにより実現可能な高機能暗号の例

暗号方式	機能
属性暗号	データ秘匿したまま、復号するエンティティの属性に合わせてアクセス制御が可能な暗号
検索可能暗号	暗号化されたままデータ検索が可能な暗号
代理再暗号化	暗号文の指定復号者を変更する際に暗号文を別の暗号文に復号することなく変換する方式
放送暗号	データ秘匿したまま、復号するエンティティのアクセス制御が可能な暗号
しきい値暗号	しきい値以上のデータにより復元可能な暗号
漏洩耐性暗号	鍵漏えいに対する耐性のある暗号
タイムリリース暗号	時刻による復号制御が可能な暗号

署名方式	機能
属性ベース署名	属性による検証制御ができるディジタル署名
しきい値署名	しきい値以上の個数の署名データにより検証可能となるディジタル署名
グループ署名	ユーザの匿名化ができるディジタル署名
ブラインド署名	署名者に対してメッセージを秘匿するディジタル署名
多重署名，集約署名	署名のセキュアな圧縮、複数の署名文の一括検証が可能なディジタル署名
漏洩耐性署名	鍵漏えいに対する耐性があるディジタル署名
タイムリリース署名	時刻による検証制御が可能なディジタル署名

楕円曲線とペアリング：　高機能暗号実現の構成要素



有限体 **K**上の3次方程式

$y^2 = x^3 + ax + b$

を満たす点(x, y)と無限遠点からなる集合が**楕円曲線G** である.

G上の点には加算が定義でき，**G**は加法群をなす．**G**上の点Aを整数s倍（**スカラー倍**）した点をsAと書く．暗号技術で用いられる**G**は，

点A, Bに対し，$B = sA$ なるスカラー（**離散対数**）sを求めることが極めて困難であるようにパラメータ **K**, a, b を選ぶ．

ペアリングe とは

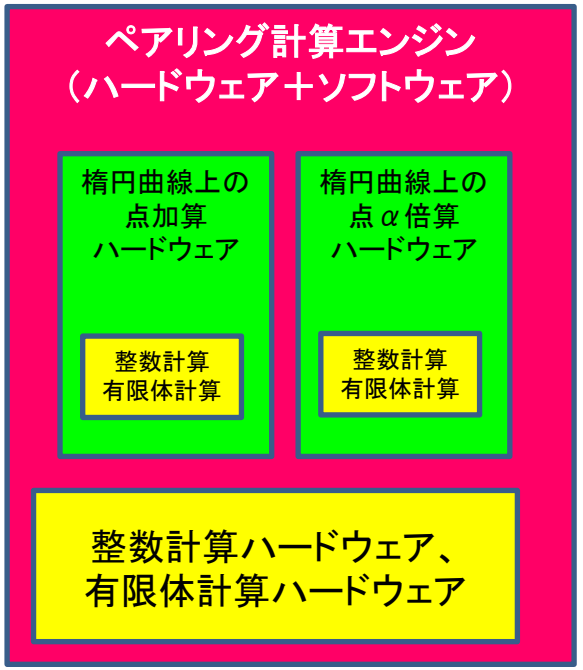
楕円曲線**G**の**加法**部分群$\mathbf{G}_i$　　有限体**K**の拡大体の**乗法**部分群$\mathbf{G}_T$

$$e: \mathbf{G}_1 \times \mathbf{G}_2 \rightarrow \mathbf{G}_T$$

なる写像であり，**双線形性** $e(sA, tB) = e(A, B)^{st}$ を満たす．

ペアリング⇒高機能暗号の実現の汎用ツール

- しかし，ペアリングは非常に複雑な写像である．
  例えば，**K**が256ビット程度のときペアリングeの計算には，
  Kの乗算10万回以上相当の計算量がかかる．
- ペアリングの活用と，高度実装を可能とするアーキテクチャ等の研究開発が必要である．



まとめ

1. IoTのセキュリティ課題

2. どこでも公開鍵暗号

   Secure Cryptographic Unit

   末端ノードでも公開鍵暗号の自在な活用を可能としIoTのセキュリティ実現に貢献

3. さらに高機能暗号導入へ