TOSHIBA
Leading Innovation

サイバーセキュリティの課題と脆弱性対策
～ICSとITセキュリティ～

その１：
サイバーセキュリティの新しい研究課題

(株)東芝　研究開発センター

東芝グループは、持続可能な
地球の未来に貢献します。

研究ターゲット

ITセキュリティ全般の研究ではなく、

- **ICS／スマートグリッド固有の機能要求**

および

- **ICSにおいて特に効果の大きい防御技術**

に絞って近未来の研究ターゲットを選択した

(※) ＩＣＳ：Industrial Control System

①メータリング・データのプライバシ保護

課題：

メータ

メータリング・データ
（電力使用量）の収集

サーバ

需要家

生活習慣や使用機器等の
プライバシ情報を
見られたくない

矛盾

事業者

課金や系統制御に必要な
統計情報を知りたい

成果：矛盾した要求を両立させる技術

- ✓月の電力使用総量は判るが各時刻のは判らない
- ✓地域の電力需要は判るが各家庭のは判らない

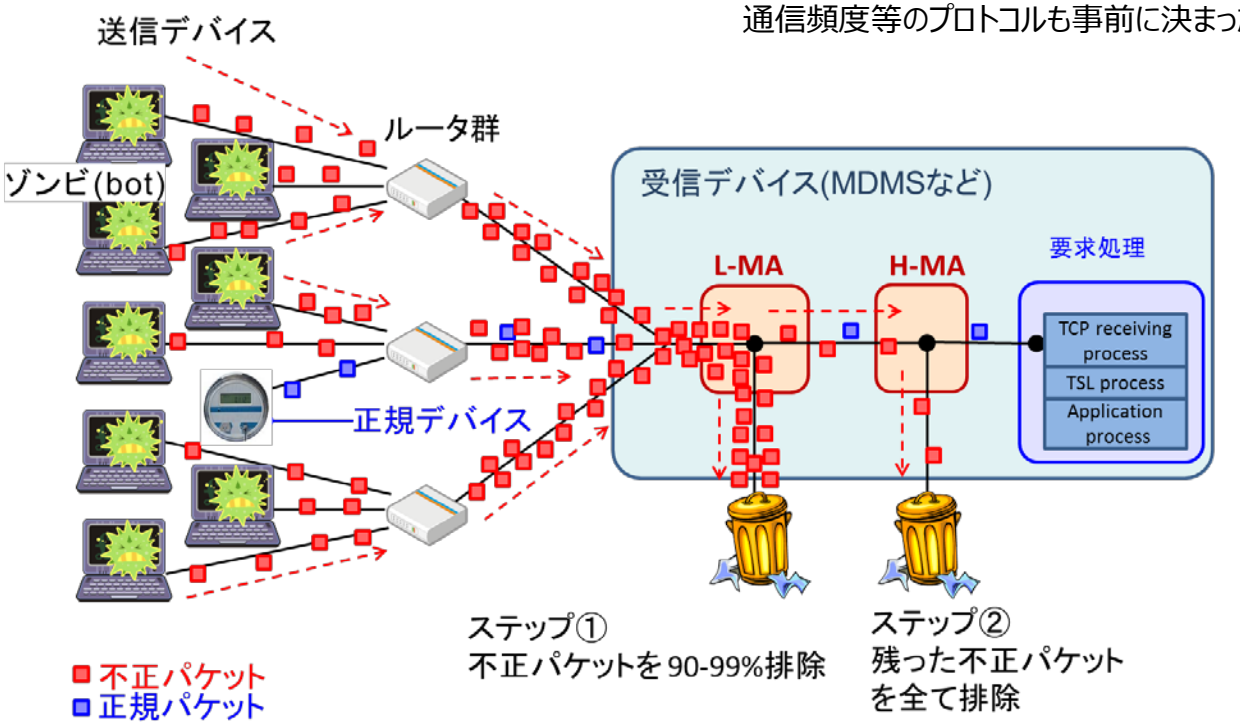
➥「秘密分散技術」および「準同型暗号」を用いる
２つのプライバシ保護手法を開発・実証

② 広域のサイバー攻撃(DDoS)への対抗

課題：サービス継続が保証できるレベルの耐攻撃性実現は理論的に難しかった。

成果：防御専用の超軽量認証(L-MA)と一般的な認証(H-MA)を組み合わせた特殊な認証手順を踏むことで、特定の前提(*)下では完全防御できるICS向けDDoS攻撃防御方式を提案し、検証した。本方式はゼロデイアタック対策にもなる。

(*)事前に定めた機器とのみ通信し、事前に秘密鍵交換済みであり、通信頻度等のプロトコルも事前に決まったものしか使わない



③ AMI網における統一的鍵管理方式

課題：メータアプリケーションに鍵更新の機能がなく
セキュアな稼働が保証困難だった

成果：標準のネットワーク接続認証方式RFC 5191と
メータアプリケーション(ANSI C12.22/C12.19) を統合した鍵更新機能付き鍵管理方式の開発及び検証を行った

➡ RFC 5191はZigBee IP にも採用されている