資料４－１

IoT　セキュリティについて

平成２７年４月２７日

シスコシステムズ

IoE イノベーションセンター東京

木下　剛　(tkinoshi@cisco.com)

最新セキュリティー動向

ビジネスモデルの変革

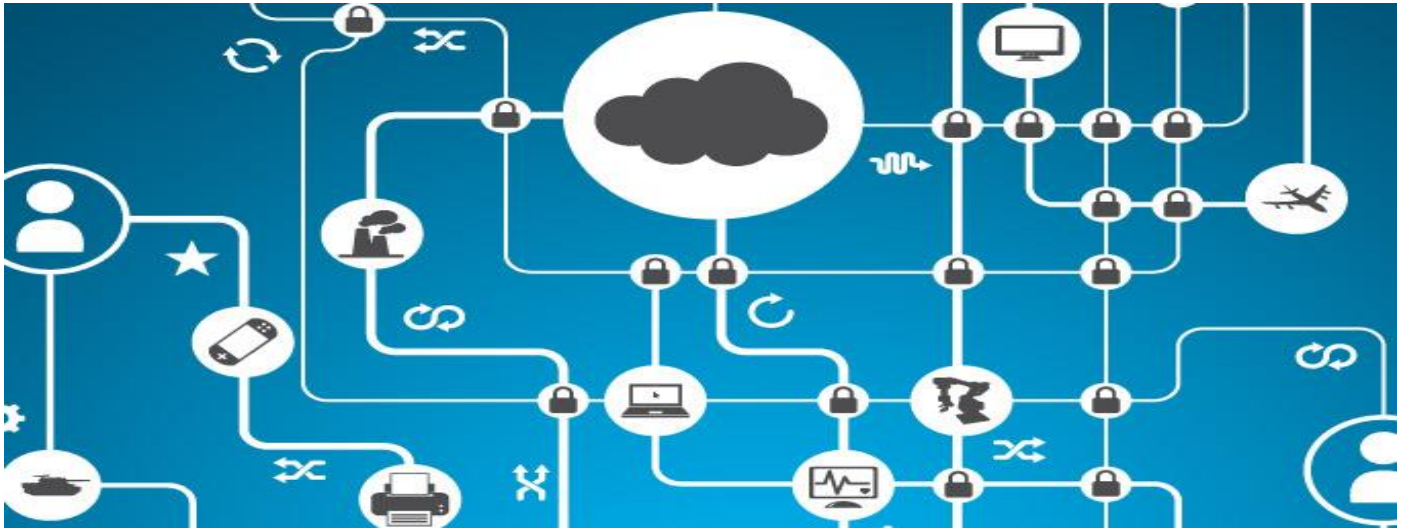
企業を標的とした攻撃が
増加中
クラウド、モバイル

新たな脅威へ継続的な対応が必要

洗練された脅威の
検知が難しい
平均発見日数は80日*

様々な脅威対策環境への適応力

複雑化する
インシデントからの復旧時間
平均解決日数は123日*



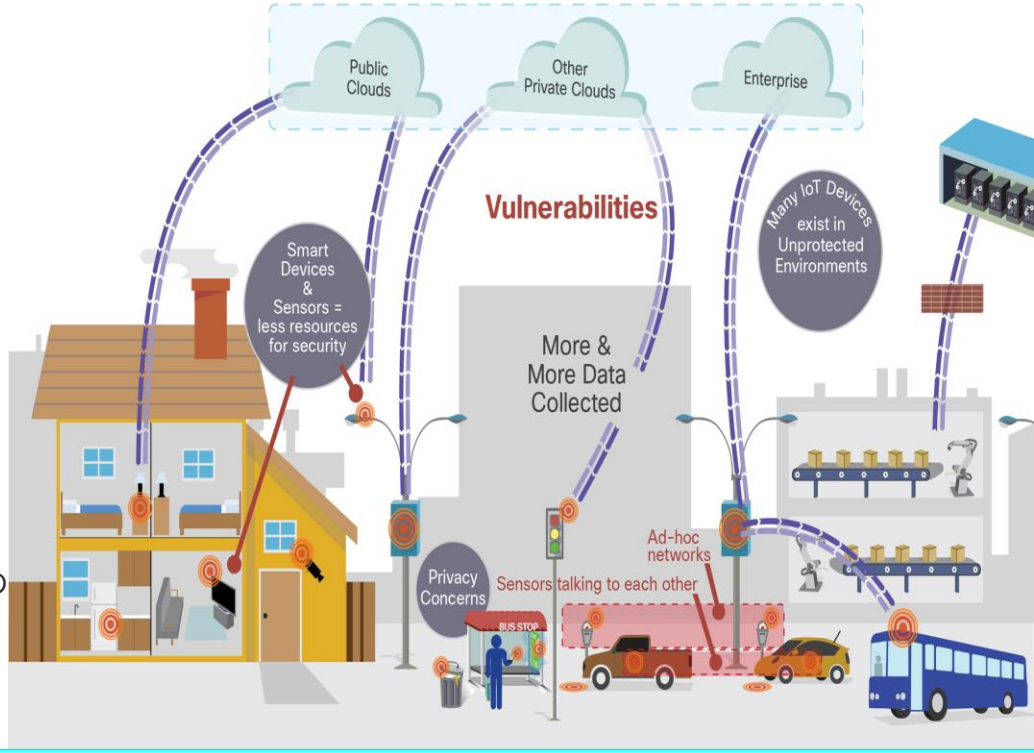
IoTによる新たなセキュリティー対策の課題

- センサーなどIoTにおけるエンドポイントはサイバーセキュリティ対応機能を必ずしも有さない
  また、パッチやアップデートによる対策適用できない

- IoTにおける対策対象範囲と数は、大幅に増加、セキュリティ対策における新たなスケーラビリティー要件

- 産業用セキュリティー、物理セキュリティーとサイバーセキュリティーのシステムレベルでの連携が前提
  現状、産業分野環境におけるサイバーセキュリティ脆弱性、脅威は、増加傾向
  - Stuxnet: シーメンス コントロール(USB経由)
  - Shamoon: シュナイダー (Telnet)クライアント
  - Others: Flame, Duqu ,etc.

  また、OT(Operation Technology)環境は、まだAPTのような最新脅威に対する本格的な防御になっていない



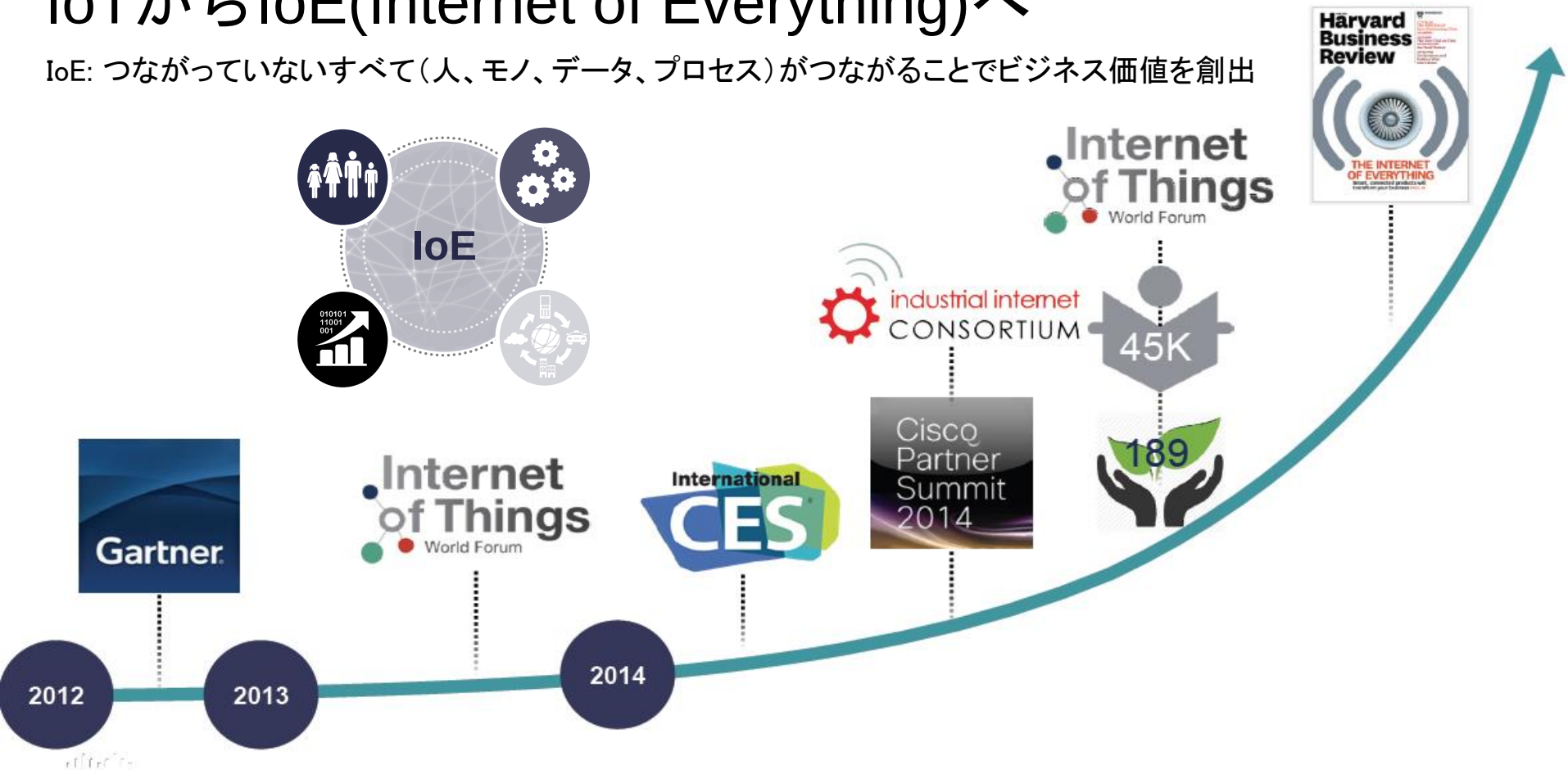
IoT Aware Visibility, Access Controls, Enforcement, Threat Analytics

IoTセキュリティー関連特許申請状況

出展元：Cisco Tech Radar　https://techradar.cisco.com

IoTからIoE(Internet of Everything)へ

IoE: つながっていないすべて（人、モノ、データ、プロセス）がつながることでビジネス価値を創出



IIC Founder Companies

INDUSTRIAL INTERNET CONSORTIUM

An Open Membership Consortium **now 140** companies strong

IoTリファレンス・モデル

レベル

7 **コラボレーション & プロセス**
(人々を巻き込む&ビジネスプロセス)

6 **アプリケーション**
(レポート,分析,コントロール)

5 **データ抽象化**
(集約 & アクセス)

4 **データ蓄積**
(ストレージ)

3 **エッジ コンピューティング**
(データエレメント分析 &変換)

2 **コネクティビティ**
(コミュニケーション&処理ユニット)

1 **物理デバイス &コントローラー**
(IoTにおける”モノ”)

Data at Rest
（蓄積されるデータ）

Data in Motion
（流れるデータ）

IoTWF Steering Committee Working groups

Vertical Working Groups

Education

Health

Manufacturing

Energy

Retail

Transportation

Smart City

Horizontal Working Groups

Security, Privacy, Compliance

Standards & Interoperability

Architecture, Management, Analytics

Innovations, Start-Ups

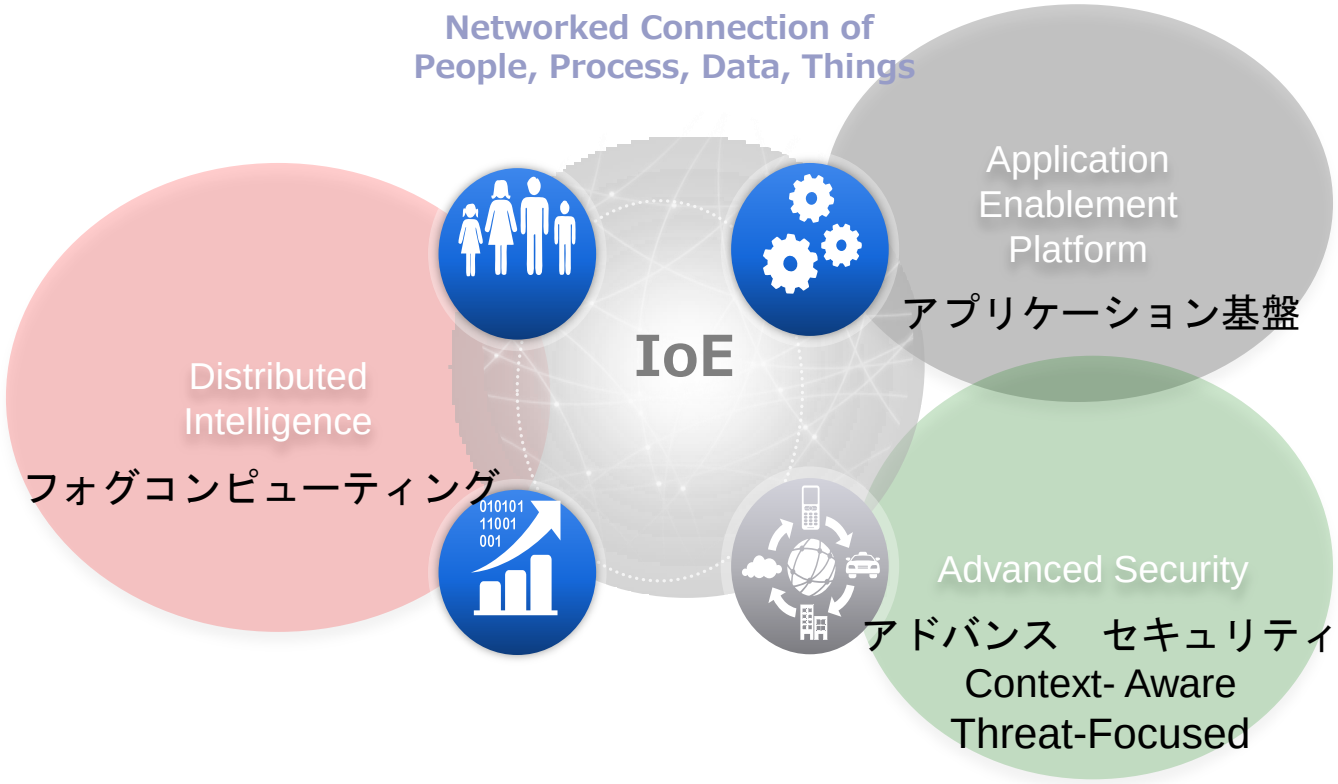
Sensors & Embedded OS

GTM: New Business Models

Marketing

104 IoTWF Steering Committee Members

IoTからIoEにおける
ネットワーク基盤としたシスコ　IoEアーキテクチャアプローチ



エンドポイントの多様化、仮想化,CPSにより従来の情報セキュリティー対策を高度化させるニーズが新たに台頭

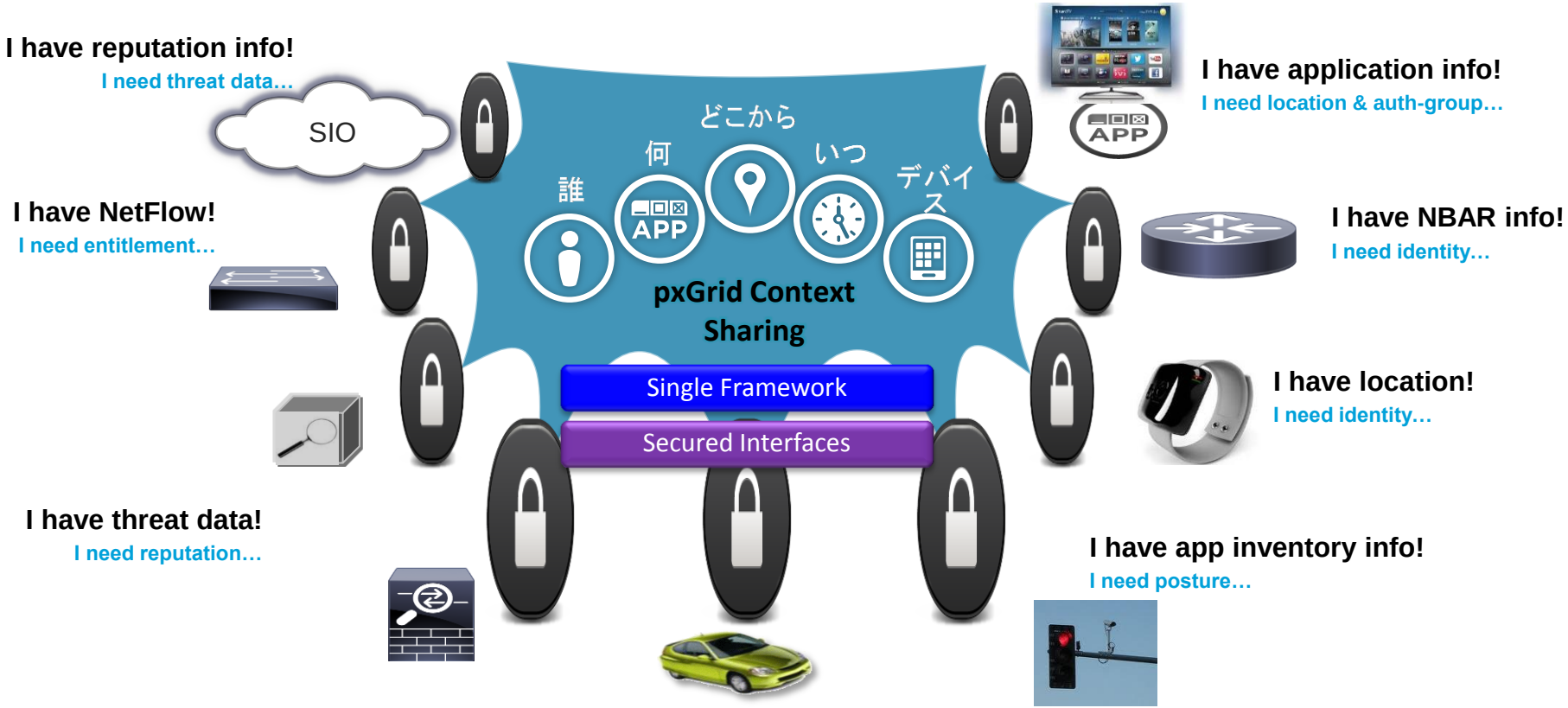
セキュリティ機能のベースラインがそろわないエンドデバイスは、
ｎｘｎ で接続される混在環境

従って、 つながる共通リソースとなるネットワークを高度化セキュリティー対策と基盤として活用することを指向

- Consistent Control
- Advanced Threat Protection
- Superior Visibility
- Complexity Reduction

ネットワーク基盤とした新しいセキュリティモデル

Platform Exchange Grid (pxGrid), Network-Wide Context-Aware Security Platform



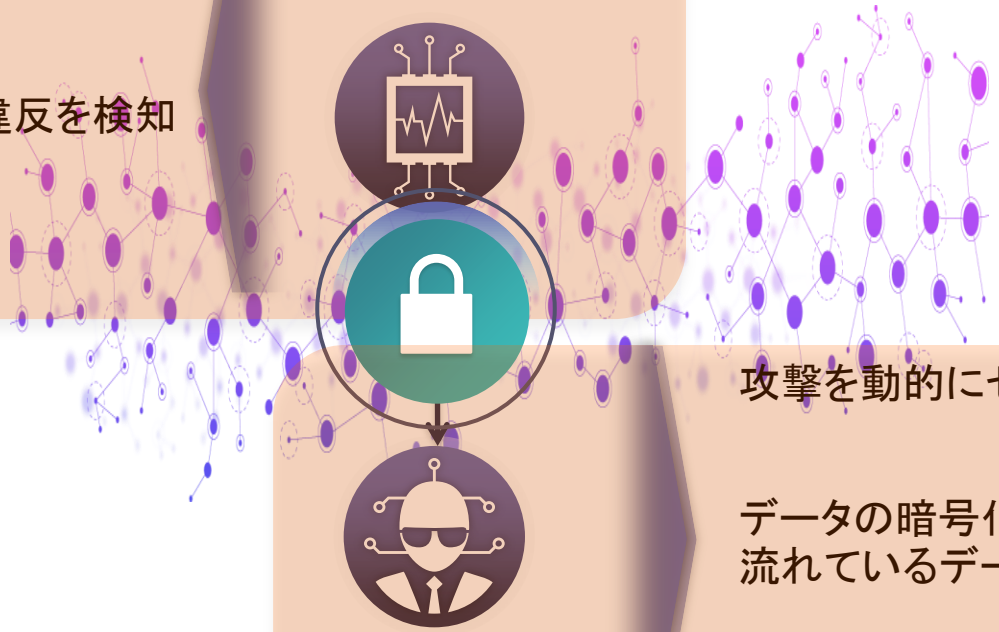
ネットワーク基盤とした新しいセキュリティモデル
Internet of Things (IoT): Malware Defense

異常なトラフィックを検知

アプリ利用やポリシー違反を検知

不正デバイス等を検知

Network As A Sensor (NaaS)



Network As A Enforcer (NaaE)

攻撃を動的にセグメンテーション

データの暗号化から
流れているデータを保護

直接インターネットアクセスを持つ
拠点をセキュアにする

TOMORROW starts here.

セキュリティ脅威の変遷と防御策の進化

APT

仮想化
端末の多様化

マルウエア

ワーム

現在

インテリジェンス
アナリシス
APT対策

2010

コンテキスト認識
アイデンティティ
多要素認証

2005

コンテンツ認識
アプリケーションセキュリティ

2000

アクセス制御
DMZ,アンチウイルス

境界が中心

システム全体での対処