大目標・ビジョン：産業競争力 UP!

サイバー犯罪が世界経済損失 年間53.4兆円
（インターネット創造価値の15～20%程度）
McAfee and CSIS 2014

国内インフラ産業規模：180兆円
市場規模マップ2015

インフラ産業の損失低減 ← 守り

サイバーセキュリティの確保

攻め → **インフラ産業の規模拡大**

勘所となるセキュリティ製品・技術の国内自給を確保

重要インフラ産業の価値を上げる

国内市場180兆円・2015年

＋ 30兆円・2020年

第６回経協インフラ戦略会議

重要インフラのサイバーセキュリティ対策

社会実装（重要インフラ）

政府系

通信・放送

エネルギー

交通

本計画

コア技術

制御・通信機器, IoT機器の
セキュリティ確認技術

システムの
動作監視・解析・防御技術

社会実装技術

認証制度の設計

情報共有・評価
検証プラットフォーム技術

重要インフラ
セキュリティ
人材の育成

マルウェア分析

物理セキュリティ

内部統制

データセキュリティ

ファイアウォール

入口出口対策

現在広く取り組まれている対策技術

既存の認証制度
（EDSA, JISEC, JCMVP, ・・・）

ICTや金融のISAC

IT人材

コア技術：セキュリティ確認技術の役割

構築時のセキュリティの作り込み

履歴書の内容チェック

ソフトウェア

不正機能検出

入試合格、採用合格

適合性確認

「信頼の基点」を機器に作り込み

身分証明書、実印の準備

運用時のセキュリティ監視と対処

入国時・入館時の身分証明書確認

システム起動時にセキュリティを確認

確認後になりすまされる可能性

いつでも！身分証明書の確認

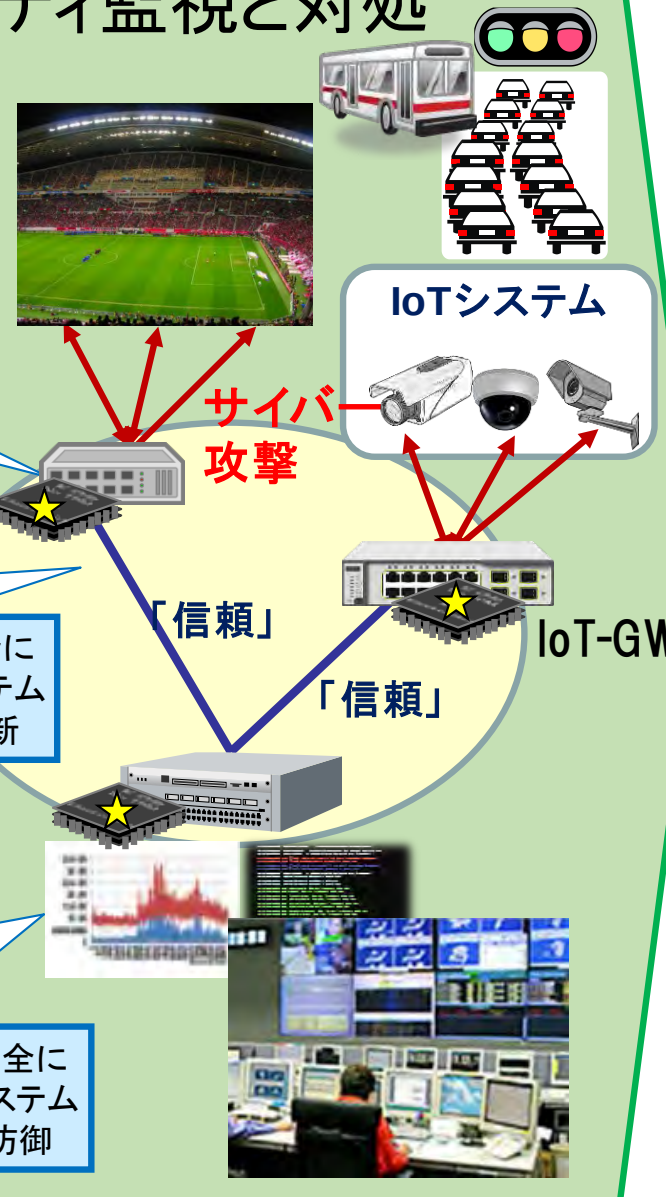
運用時にもセキュリティ確認

安全にシステム更新

確認後に侵害される可能性

正しい健康診断！

動作監視・解析

「信頼」できる機器での分析により迅速対処

安全にシステム防御