IoT/M2M/CPS等の機器認証、データの真正性等のセキュリティ

2015年12月15日

東京工科大学
手塚　悟

目次

1．我が国のサイバーセキュリティ政策

サイバーセキュリティをめぐる状況の変化

NISC

IT依存度の高まり

- **PC**：多くの職場・家庭に普及し、インターネットに接続（2013年末：PC普及率 81.7%、インターネット普及率 82.8%）
- **スマートフォン**：世帯保有率が6倍に急増（2010年末：9.7%→2013年末：62.6%）
- **自動車**：一台に搭載される車載コンピュータは100個以上、ソフトウェアの量は約1000万行
- **スマートメーター（次世代電力量計）**：電力会社による開発・導入の開始
  【主な予定】・東京：2020年度までに2700万台の導入完了
  ・関西：2022年度までに1300万台の導入完了

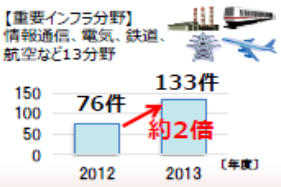
サイバー攻撃の増加

⇒ **6秒に1回**攻撃が発生

センサー監視等による脅威件数

⇒ **重要インフラ**への攻撃も増加

重要インフラへの攻撃件数



国家関与の疑われる攻撃

韓国（2013年4月）

重要インフラ（金融・放送等）に対する大規模サイバー攻撃が発生。韓国当局は北朝鮮の所業と発表。

米国（2014年12月）

ソニー・ピクチャーズ・エンターテインメント社に対するサイバー攻撃が発生。米国政府は北朝鮮に責任ありとし、国家安全保障上の問題として対応。

東京五輪へ向けた準備

- 世界の注目を集める祭典。「ダウンタイム」は許されない。
- 2012年のオリンピック・パラリンピックロンドン大会では、開催期間中、約２億件のサイバー攻撃が発生。
- 英国政府は、6年前からサイバー攻撃対策を準備。

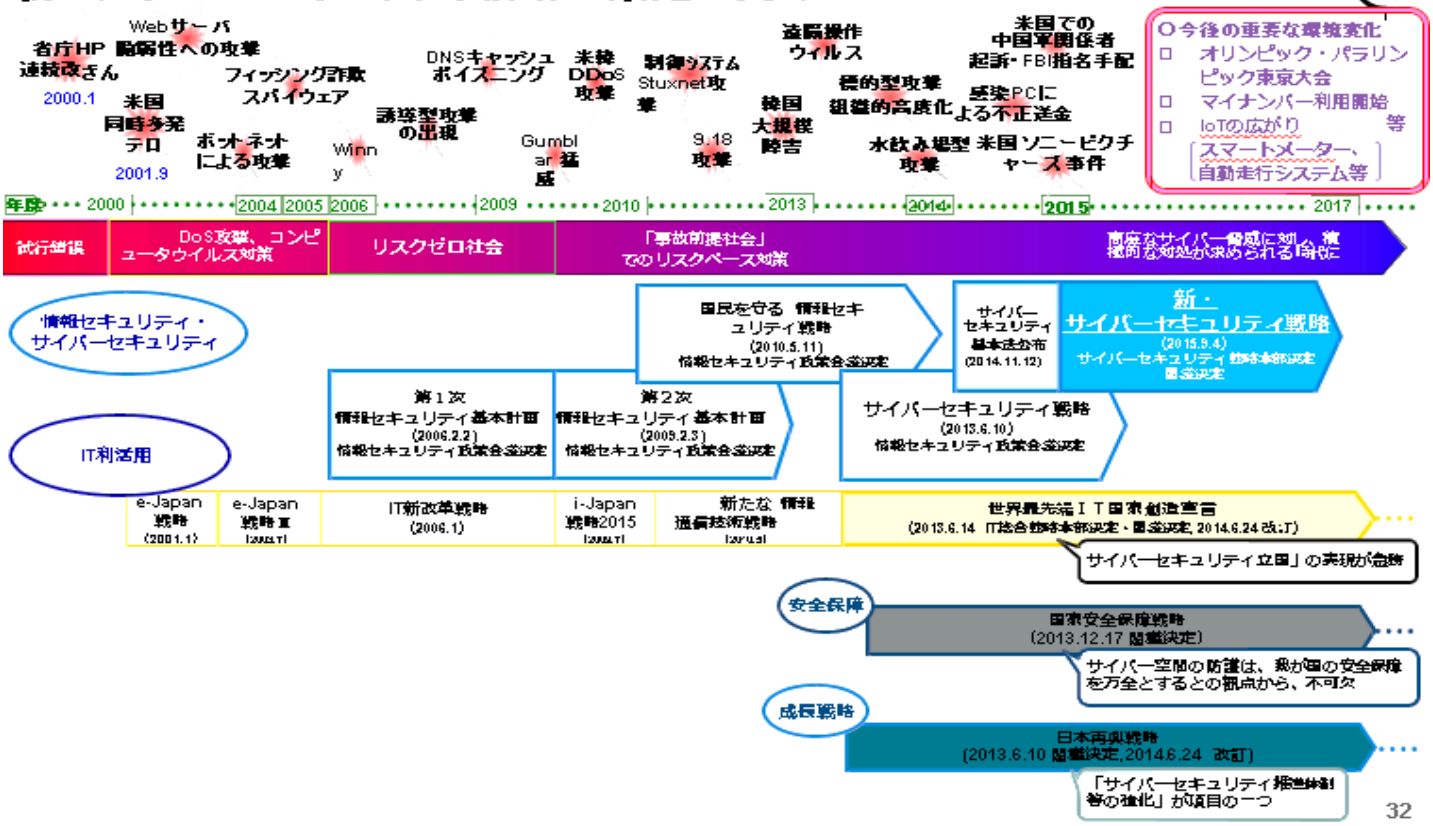
サイバー脅威に対応し、サイバーセキュリティを強化するため、サイバーセキュリティ基本法が成立、施行。

（平成26年11月12日公布。平成27年１月９日全面施行）

1．我が国のサイバーセキュリティ政策

新・サイバーセキュリティ戦略の策定に向けて

NISC

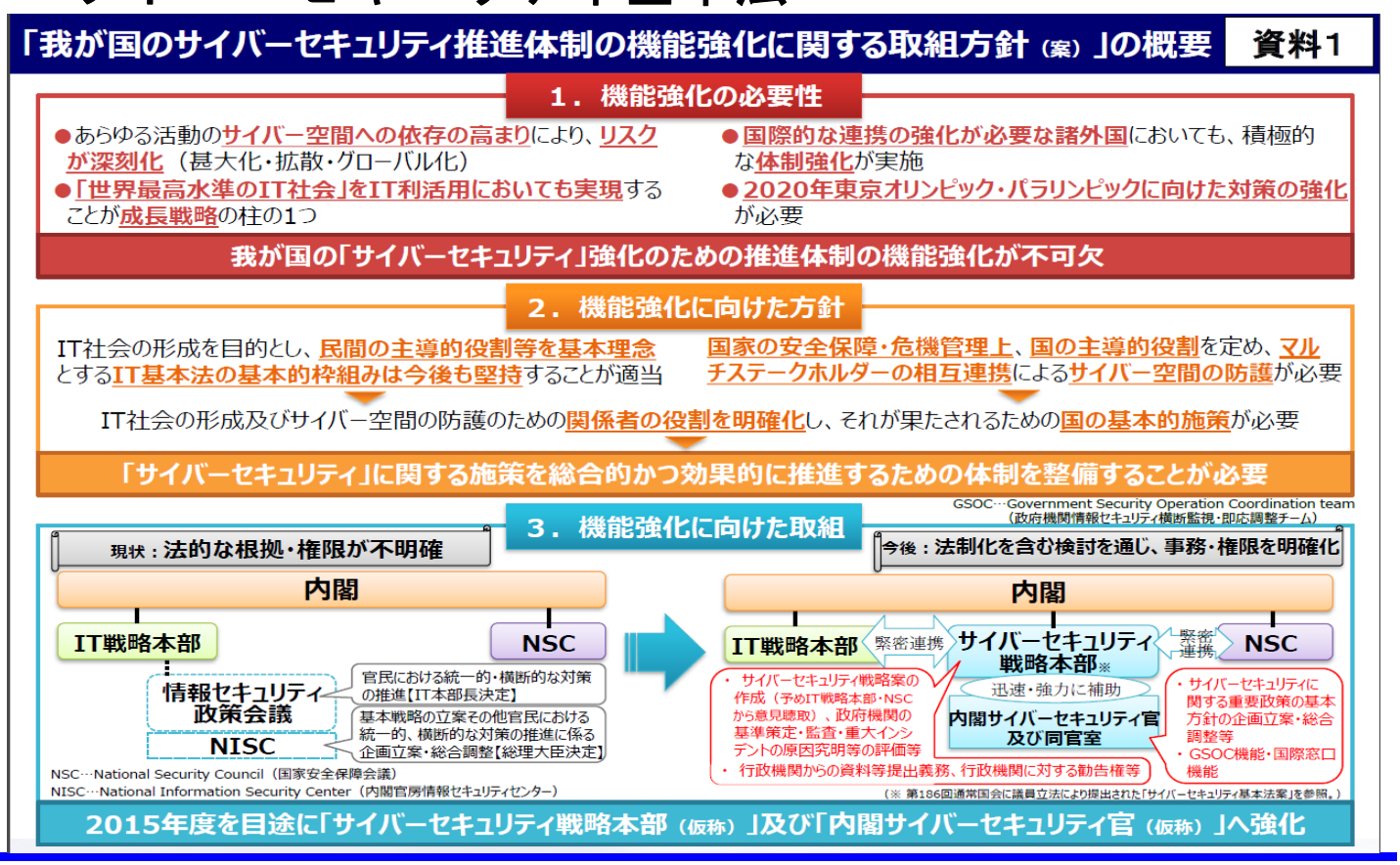


1．我が国のサイバーセキュリティ政策

- サイバーセキュリティ基本法：2014年11月6日成立
- 日本再興戦略改訂2015：2015年6月30日閣議決定
- サイバーセキュリティ2015：2015年9月4日閣議決定

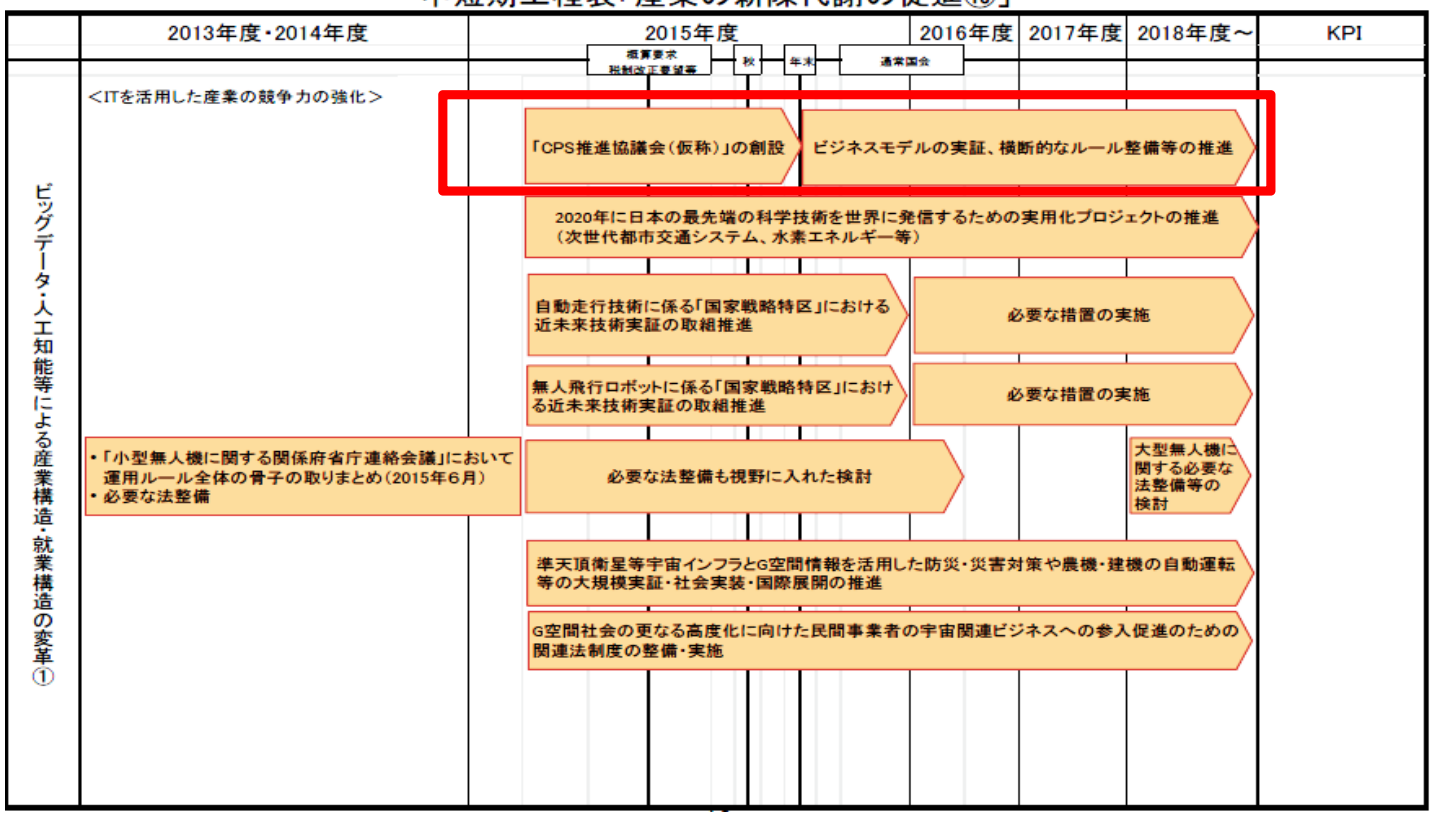
1．我が国のサイバーセキュリティ政策

- サイバーセキュリティ基本法



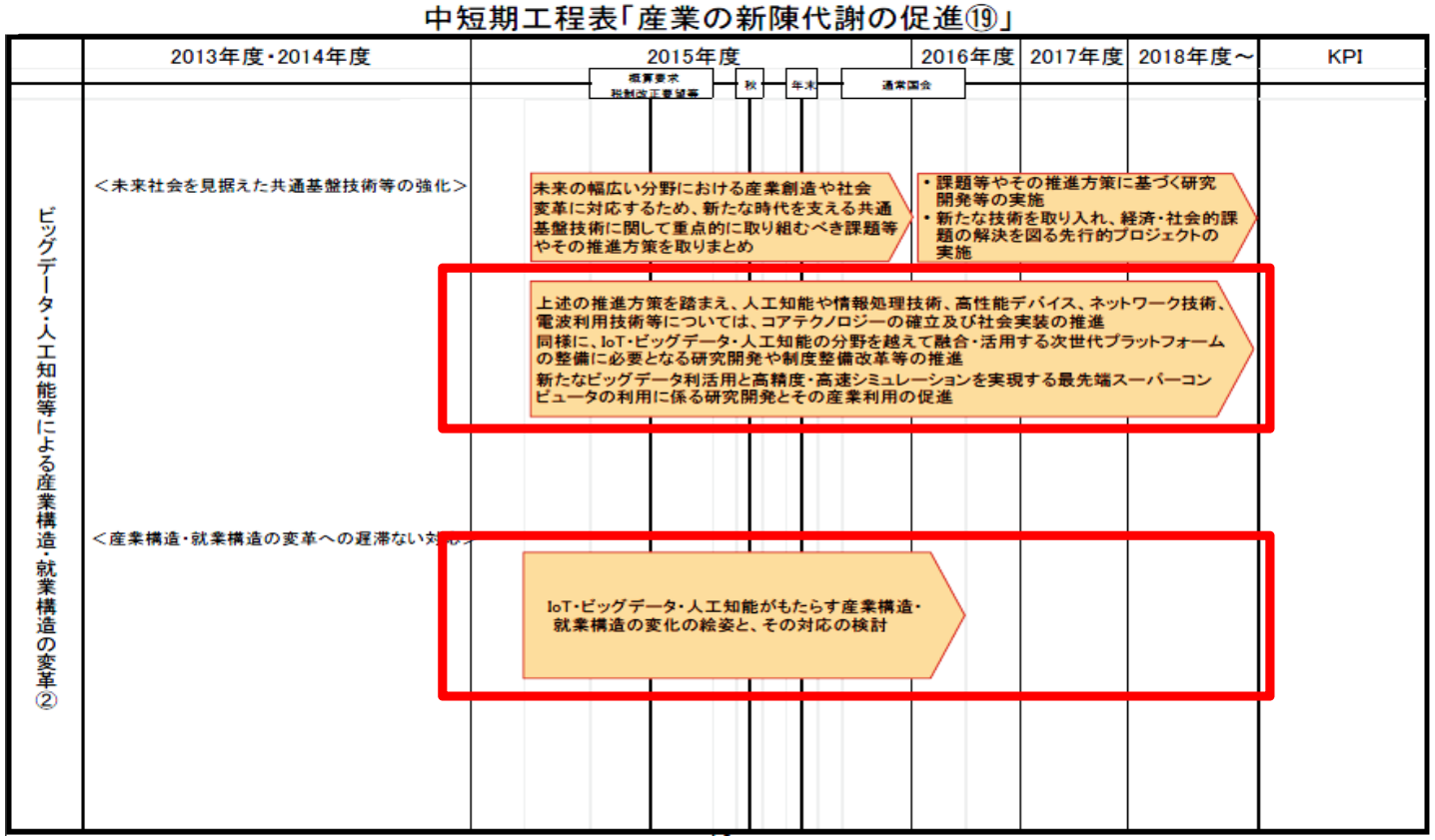
● 日本再興戦略改訂2015

中短期工程表「産業の新陳代謝の促進⑱」



● 日本再興戦略改訂2015

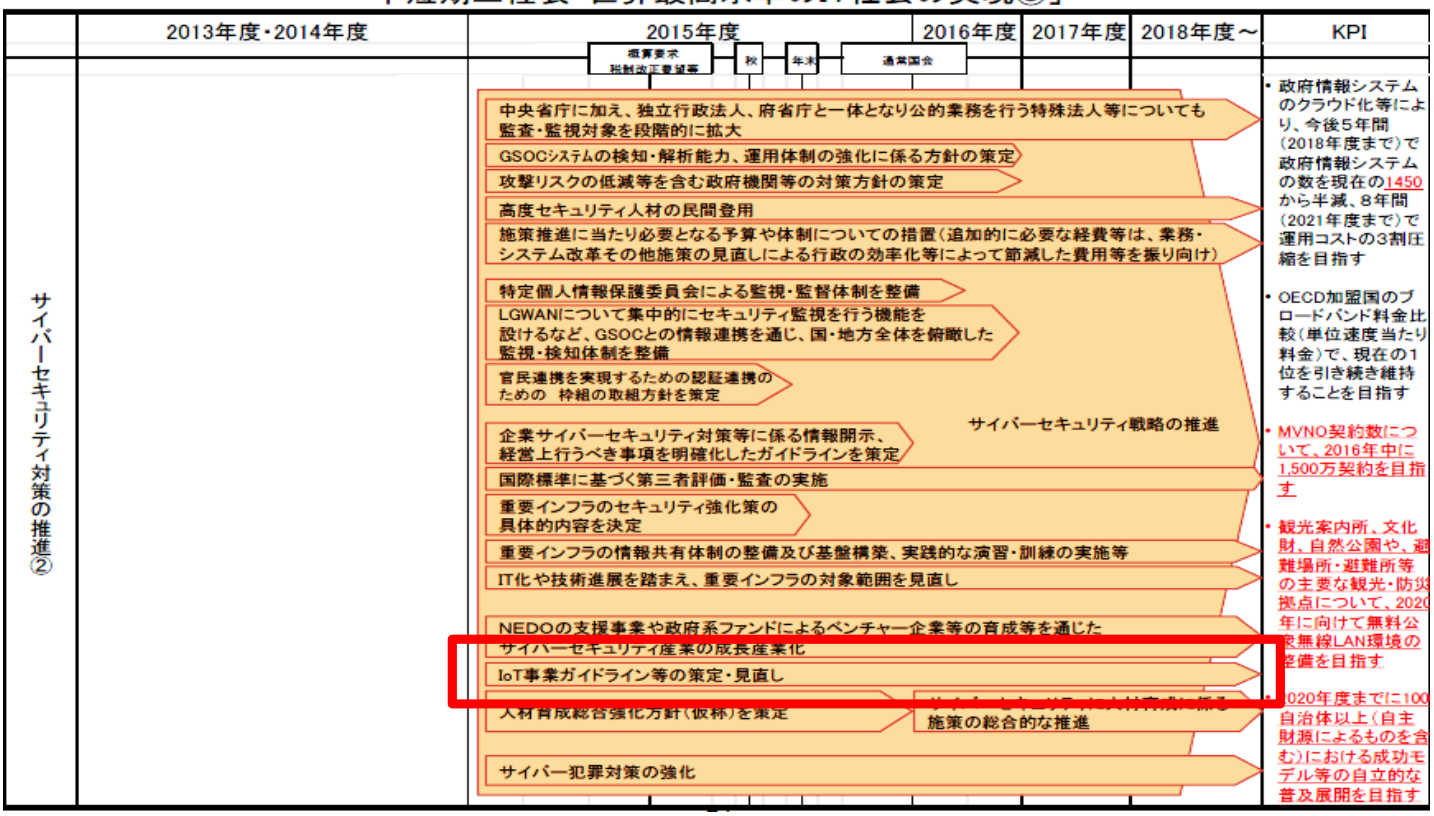
中短期工程表「産業の新陳代謝の促進⑲」



1．我が国のサイバーセキュリティ政策

● 日本再興戦略改訂2015

中短期工程表「世界最高水準のIT社会の実現⑧」



1．我が国のサイバーセキュリティ政策

● サイバーセキュリティ2015

「サイバーセキュリティ2015(案)」の概要について　資料１－１

新たなサイバーセキュリティ戦略に基づく最初の年次計画として、2015年度に実施する具体的な取組を戦略の体系に沿って示したもの（以下は主な施策例）。

経済社会の活力の向上及び持続的発展
～ 費用から投資へ ～

■安全なIoTシステムの創出
- IoTに係る大規模な事業に対し、セキュリティ・バイ・デザインに必要な働きかけを実施【内閣官房】
- M2M機器・IoTのセキュリティに係る横断的なガイドラインの策定【総務省及び経済産業省】
- エネルギー分野のガイドラインとして、スマートメーターのセキュリティ評価技術・手順を実証【経済産業省】

■セキュリティマインドを持った企業経営の推進
- サイバー攻撃によるリスクを投資家に開示することの可能性を検討【内閣官房及び金融庁】
- 経営ガイドラインの策定【経済産業省】
- 「橋渡し人材層」としての能力向上を図るセミナー等を実施【内閣官房及び経済産業省】
- ISACを活用した情報共有体制の拡充【総務省】

■セキュリティに係るビジネス環境の整備
- 政府系ファンド等の活用検討【経済産業省】
- 著作権法におけるリバースエンジニアリングに関する適法性を明確化【文部科学省】
- 制御システムセキュリティ認証の拡大【経済産業省】

国民が安全で安心して暮らせる社会の実現
～ 2020年・その後に向けた基盤形成 ～

■国民・社会を守るための取組
- マルウェアに感染したユーザーを検知し、マルウェアの除去等を促す取組を実施【総務省】
- 安全な無線LAN環境の整備に向けて、必要となる対策の検討、周知啓発を実施【総務省】
- 通信履歴等の保存の在り方について、ガイドラインの解説の改正を踏まえ対応【警察庁及び総務省】

■重要インフラを守るための取組
- 東京オリンピック・パラリンピック競技大会に重大な影響を与えるサービス・事業者・分野の候補を選定【内閣官房】
- マイナンバーの監視・監督体制や、LGWANにおける集中的なセキュリティ監視機能の整備【特定個人情報保護委員会、内閣官房及び総務省 他】

■政府機関を守るための取組
- 各府省庁の情報システムに対してペネトレーションテストを実施【内閣官房】
- 国の行政機関における統一基準群等に基づく施策の取組状況に関する監査制度を設計するとともに、試行的な監査を実施【内閣官房】

国際社会の平和・安定及び我が国の安全保障
～ サイバー空間における積極的平和主義 ～

■我が国の安全の確保
- 情報収集・分析機能の強化に加え、サイバー攻撃対策に係る訓練を実施【警察庁】
- カウンターインテリジェンスに係る取組の推進【内閣官房】
- サイバー攻撃時においても持続的な部隊運用を確保するための取組を継続【防衛省】
- 部外インフラ等、関係主体との連携深化【防衛省】

■国際社会の平和・安定
- 二国間協議や多国間協議に参画し、国際法の適用や国際的なルール・規範作り等に積極的に関与し、我が国の意向を反映【内閣官房及び外務省】
- 国際テロ組織の活動等に関する情報の収集・分析の強化【内閣官房、警察庁及び法務省】
- 各国における能力構築を支援【内閣官房 他】

■世界各国との協力連携
- ASEAN諸国との連携を強化【内閣官房 他】
- インターネットエコノミーに関する日米政策協力対話にて一致した、米国との情報共有を強化【総務省】
- 包括的な日米サイバー防衛の連携【防衛省】

横断的施策

■研究開発の推進
- 世界最先端のサイバー攻撃観測・分析技術、暗号基盤技術等に関する研究開発を実施【総務省】
- 法律や国際関係、安全保障、経営学等の社会科学的視点も含め様々な領域の研究との連携、融合領域の研究を促進【内閣官房】
- 戦略的イノベーション創造プログラム（SIP）の枠組み等により研究開発を推進【内閣府】

■人材の育成・確保
- 高度なITの知識と経営などその他の領域における専門知識を併せもつ人材の育成【文部科学省及び経済産業省】
- 初等中等教育に携わる教員等を対象とした研修、情報交換【文部科学省】
- 情報処理技術者試験において実践的な能力を適時適切に評価するための更新制度の導入の検討【経済産業省】
- サイバー防御演習を通じた実践的セキュリティ人材の育成【総務省】

推進体制　➢ 伊勢志摩サミットにおけるサイバーセキュリティの確保や東京オリンピック・パラリンピック競技大会に向けた対策の検討【内閣官房】

目次

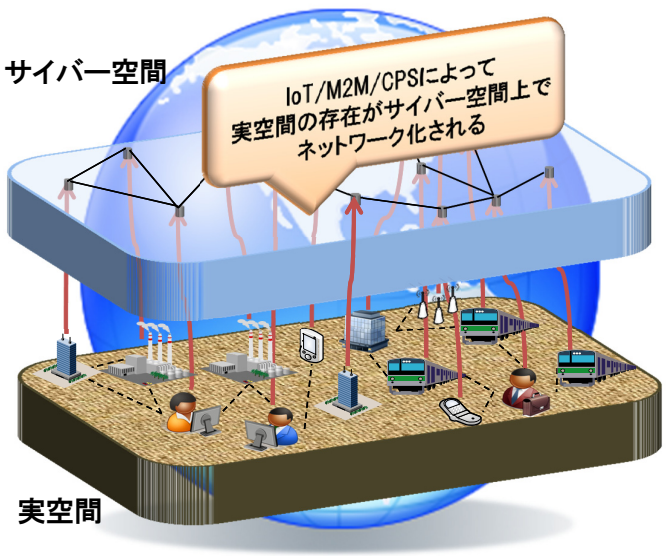
1. 我が国のサイバーセキュリティ政策

2. IoT/M2M/CPS等の課題と対策

3. 今後のサイバー空間の安心安全

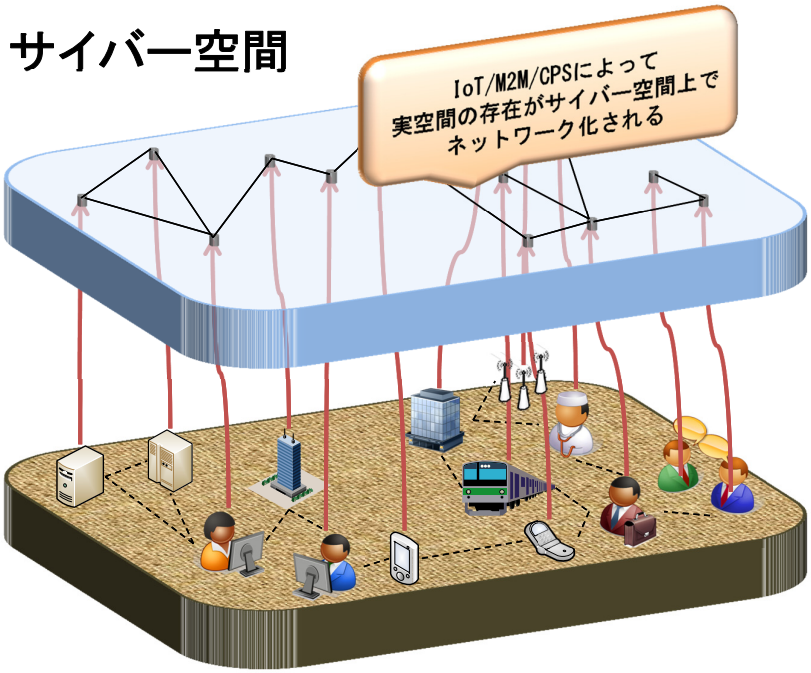
2. IoT/M2M/CPS等の課題と対策

膨大なIoT/M2M/CPS等の機器が接続されたことで,
サイバー攻撃に対するリスクが増大、複雑化し、影響範囲も広域化



センサ等の多種多様な機器や、他機関、他国のシステムとも
接続されたIoT/M2M/CPS等のシステムを守る

● IoT/M2M/CPS等の機器認証、データの真正性

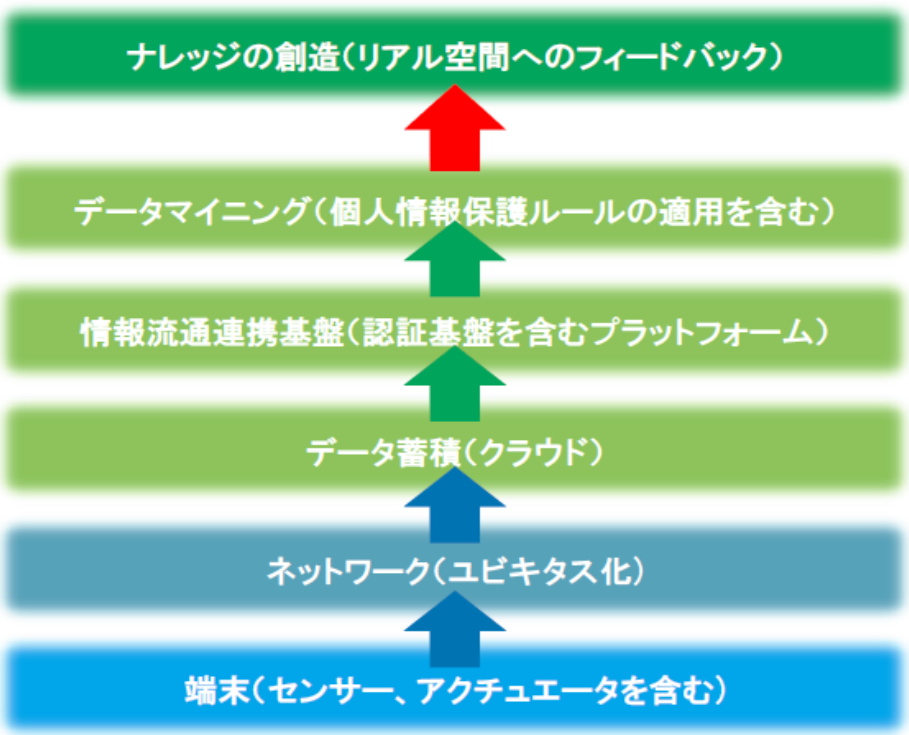


データの真正性

IoT/M2M/CPS等の機器認証

IoTセキュリティに関する検討事項（例）

NISC



検討事項（例）

- ■自律・分散・協調型NW（インターネット網に類似）→マルチステークホルダーによる検討が必要。
- ■Security by Designの徹底
- ■異NW間の責任分界点とインターフェースの共通化
- ■端末認証の仕組み
- ■インシデント情報の共有体制（連鎖の拡大への対応）
- ■個人情報保護の仕組み

２．IoT/M2M/CPS等の課題と対策

● 課題

1. IoT/M2M/CPSシステムではセキュリティ対策のスキームが未整備であること
   - 従来のPCベース環境を利用したICTシステムは、Windows、Linuxなどのベースにしている。
   - 供給者責任による脆弱性対策の提供や、ウィルス対策ソフトウェアや脆弱性検査ツールおよび脆弱性情報公開により、セキュリティ対策のスキームが整備されているが、IoT/M2M/CPSシステムにおいては、そのスキームは未整備である。

2. IoT/M2M/CPSシステムがサイバー攻撃の対象になり得ること
   - サイバー攻撃の対象は、従来のPCベースの環境にとどまらない。
   - Android、iOSなどをOSとする環境、さらには組込み機器、制御機器も攻撃対象になり得る。

3. サイバー攻撃が物理空間にも影響を及ぼすこと
   - 重要インフラや自動車等がサイバー攻撃により物理的影響を受ける事態は避けなければならない。

２．IoT/M2M/CPS等の課題と対策

● 対策

1. 現状の脆弱性の洗い出しと、今後のセキュリティ対策
   - 現状で運用されているIoT/M2M/CPSシステムのセキュリティ点検は急務
   - その上で今後、ウェアラブル等のリソース制約のある機器への軽量暗号の実装
   - PC・スマホと異なり常時接続ではないシステム（車など）へのソフトウェアアップデートのためセキュアなプロトコルの整備

2. IoT/M2M/CPSシステムをUpdatableとする技術、枠組みの整備

3. IoT/M2M/CPSシステム向けにソフトウェアや暗号鍵の更新を行うためのセキュア通信プロトコルの開発

目次

3. 今後のサイバー空間の安心安全

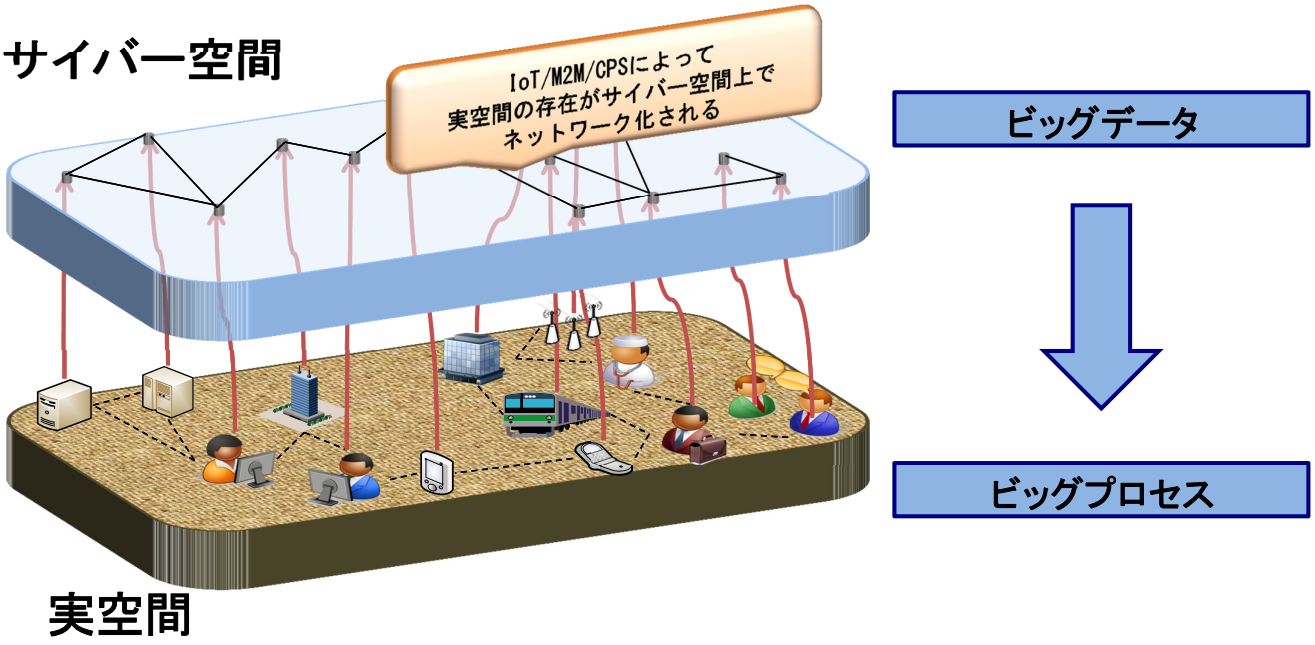
●情報セキュリティとは

組織にとって価値ある情報資産を、
機密性、完全性、可用性の観点において維持するもの

●通称「セキュリティのCIA」と呼ぶ

機密性 Confidentiality	アクセス許可されたものだけが情報にアクセスできることを確実にすること
完全性 Integrity	情報及び処理方法が、正確であること及び完全であることを保護すること
可用性 Availability	許可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること

３．今後のサイバー空間の安心安全



- TSDI(Trusted Social Data Infrastructure)　：ビッグデータ
- TSPI(Trusted Social Process Infrastructure)：ビッグプロセス