

---

# 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
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

# 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



### 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%)  
※2014年情報通信白書(総務省)

**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%)  
※2014年情報通信白書(総務省)

**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  
※自動車産業のサイバーセキュリティへの取組み  
JIPIC(2013.3/24)

**スマートメーター** 電力会社による開発・導入の開始  
(次世代電力量計) 【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 ⇒ **重要インフラ**への攻撃も増加

**センサー監視等による脅威件数**

年	件数
2011	66万件
2012	108万件
2013	508万件

出典: NISC(2014.7) **5倍**

**重要インフラへの攻撃件数**

年	件数
2012	76件
2013	133件

【重要インフラ分野】  
情報通信、電気、鉄道、航空など13分野 **約2倍**

### 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)**  
リー・ヒョクファース・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。

### 東京五輪に向けた準備

- 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



**Webサーバ** 省庁HP 脆弱性への攻撃  
連続改ざん 2000.1

**フィッシング詐欺** スパイウェア

**DNSキャッシュ** ボイスエンギン

**未検** DDoS 攻撃

**制御システム** Stuxnet 攻撃

**盗撮操作** ウイルス

**米国での** 中国軍関係者 起訴・FBI指名手配

**標的型攻撃** 組織的・高度化による不正送金

**韓国** 大規模 韓吉

**水飲み場型** 米国 ソニーピクチャーズ事件

**誘導型攻撃** の出現

**Gumblar** 猛 威

**9.18** 攻撃

**感染PCに** よる不正送金

**米国** ソニーピクチャーズ事件

**今後の重要な環境変化**

- オリンピック・パラリンピック東京大会
- マイナンバー利用開始
- IoTの広がり
- スマートメーター、自動走行システム等

年次.....2000 | .....2004 | 2005 | 2006 | .....2009 | .....2010 | .....2013 | .....2014 | .....2015 | .....2017 |

**試行錯誤** DoS攻撃、コンピュータウイルス対策

**リスクゼロ社会**

**「事故前提社会」でのリスクベース知策**

**高度なサイバー脅威に即ち、適切な対応が求められる時代**

**情報セキュリティ・サイバーセキュリティ**

**IT利活用**

**国民を守る 情報セキュリティ戦略 (2010.5.11)**  
情報セキュリティ政策会合決定

**サイバーセキュリティ基本法公布 (2014.11.12)**  
サイバーセキュリティ基本法決定

**新・サイバーセキュリティ戦略 (2015.5.4)**  
サイバーセキュリティ基本法決定

**第1次 情報セキュリティ基本計画 (2006.2.2)**  
情報セキュリティ政策会合決定

**第2次 情報セキュリティ基本計画 (2009.2.3)**  
情報セキュリティ政策会合決定

**サイバーセキュリティ戦略 (2013.6.10)**  
情報セキュリティ政策会合決定

**e-Japan 戦略 (2001.1)**

**e-Japan 戦略Ⅱ (2004.1)**

**IT新改革戦略 (2006.1)**

**i-Japan 戦略2015 (2014.1)**

**新たな 情報技術戦略 (2014.1)**

**世界最先端IT国家創造宣言 (2013.6.14)**  
IT総合戦略本部決定・閣議決定、2014.6.24改訂

**「サイバーセキュリティ立国」の実現が急務**

**安全保障**

**国家安全保障戦略 (2013.12.17 閣議決定)**  
サイバー空間の防護は、我が国の安全保障を万全とするとの観点から、不可欠

**成長戦略**

**日本再興戦略 (2013.6.10 閣議決定、2014.6.24 改訂)**  
「サイバーセキュリティ推進体制等の強化」が項目の一つ

# 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

### 「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針(案)」の概要 資料1

#### 1. 機能強化の必要性

- あらゆる活動のサイバー空間への依存の高まりにより、**リスクが深刻化**(基大化・拡散・グローバル化)
- 「**世界最高水準のIT社会**」をIT活用においても実現することが**成長戦略**の柱の1つ
- **国際的な連携の強化が必要な諸外国**においても、積極的な**体制強化**が実施
- **2020年東京オリンピック・パラリンピック**に向けた**対策の強化**が必要

我が国の「サイバーセキュリティ」強化のための推進体制の機能強化が不可欠

#### 2. 機能強化に向けた方針

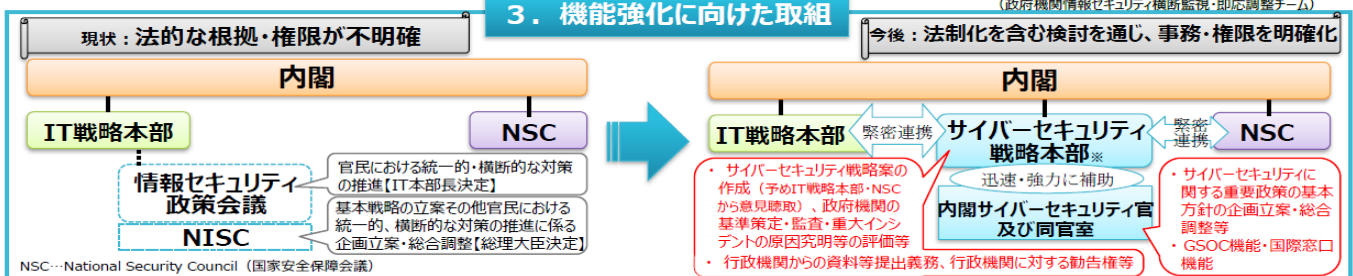
IT社会の形成を目的とし、**民間の主導的役割等を基本理念**とする**IT基本法の基本的枠組み**は今後も堅持することが適当 **国家の安全保障・危機管理上、国の主導的役割**を定め、**マルチステークホルダーの相互連携**による**サイバー空間の防護**が必要

IT社会の形成及びサイバー空間の防護のための**関係者の役割を明確化**し、それが果たされるための**国の基本的施策**が必要

「サイバーセキュリティ」に関する施策を総合的かつ効果的に推進するための体制を整備することが必要

#### 3. 機能強化に向けた取組

GSOC→Government Security Operation Coordination team  
(政府機関情報セキュリティ横断監視・即応調整チーム)



2015年度を目標に「サイバーセキュリティ戦略本部(仮称)」及び「内閣サイバーセキュリティ官(仮称)」へ強化

# 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「産業の新陳代謝の促進⑱」

	2013年度・2014年度	2015年度	2016年度	2017年度	2018年度～	KPI	
		概算要求 概算改訂要望書 秋 年末 通常国会					
ビッグデータ・人工知能等による産業構造・就業構造の変革①	<ITを活用した産業の競争力の強化>	「CPS推進協議会(仮称)」の創設		ビジネスモデルの実証、横断的なルール整備等の推進			
		2020年に日本の最先端の科学技術を世界に発信するための実用化プロジェクトの推進 (次世代都市交通システム、水素エネルギー等)					
		自動走行技術に係る「国家戦略特区」における近未来技術実証の取組推進		必要な措置の実施			
		無人飛行ロボットに係る「国家戦略特区」における近未来技術実証の取組推進		必要な措置の実施			
	・「小型無人機に関する関係府省庁連絡会議」において運用ルール全体の骨子の取りまとめ(2015年6月) ・必要な法整備	必要な法整備も視野に入れた検討			大型無人機に関する必要な法整備等の検討		
		準天頂衛星等宇宙インフラとG空間情報を活用した防災・災害対策や農機・建機の自動運転等の大規模実証・社会実装・国際展開の推進					
		G空間社会の更なる高度化に向けた民間事業者の宇宙関連ビジネスへの参入促進のための関連法制度の整備・実施					

# 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「産業の新陳代謝の促進⑲」

	2013年度・2014年度	2015年度	2016年度	2017年度	2018年度～	KPI	
		概算要求 概算改訂要望書 秋 年末 通常国会					
ビッグデータ・人工知能等による産業構造・就業構造の変革②	<未来社会を見据えた共通基盤技術等の強化>	未来の幅広い分野における産業創造や社会変革に対応するため、新たな時代を支える共通基盤技術に関して重点的に取り組むべき課題等やその推進方策を取りまとめ		・課題等やその推進方策に基づく研究開発等の実施 ・新たな技術を取り入れ、経済・社会的課題の解決を図る先行的プロジェクトの実施			
		上述の推進方策を踏まえ、人工知能や情報処理技術、高性能デバイス、ネットワーク技術、電波利用技術等については、コアテクノロジーの確立及び社会実装の推進 同様に、IoT・ビッグデータ・人工知能の分野を越えて融合・活用する次世代プラットフォームの整備に必要な研究開発や制度整備改革等の推進 新たなビッグデータ活用と高精度・高速シミュレーションを実現する最先端スーパーコンピュータの利用に係る研究開発とその産業利用の促進					
	<産業構造・就業構造の変革への遅滞ない対応>	IoT・ビッグデータ・人工知能がもたらす産業構造・就業構造の変化の絵姿と、その対応の検討					

# 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」

2013年度・2014年度	2015年度			2016年度	2017年度	2018年度～	KPI					
	概算要求 税制改正要綱等	秋	年末	通常国会								
サイバーセキュリティ対策の推進②	<ul style="list-style-type: none"> <li>中央省庁に加え、独立行政法人、府省庁と一体となり公的業務を行う特殊法人等についても監査・監視対象を段階的に拡大</li> <li>GSOCシステムの検知・解析能力、運用体制の強化に係る方針の策定</li> <li>攻撃リスクの低減等を含む政府機関等の対策方針の策定</li> <li>高度セキュリティ人材の民間登用</li> <li>施策推進に当たり必要となる予算や体制についての措置（追加的に必要な経費等は、業務・システム改革その他施策の見直しによる行政の効率化等によって節減した費用等を振り向け）</li> <li>特定個人情報保護委員会による監視・監督体制を整備</li> <li>LGWANについて集中的にセキュリティ監視を行う機能を設けるなど、GSOCとの情報連携を通じ、国・地方全体を俯瞰した監視・検知体制を整備</li> <li>官民連携を実現するための認証連携のための枠組の取組方針を策定</li> <li>企業サイバーセキュリティ対策等に係る情報開示、経営上行うべき事項を明確化したガイドラインを策定</li> <li>国際標準に基づく第三者評価・監査の実施</li> <li>重要インフラのセキュリティ強化策の具体的内容を決定</li> <li>重要インフラの情報共有体制の整備及び基盤構築、実践的な演習・訓練の実施等</li> <li>IT化や技術進展を踏まえ、重要インフラの対象範囲を見直し</li> <li>NEDOの支援事業や政府系ファンドによるベンチャー企業等の育成等を通じたサイバーセキュリティ産業の成長産業化</li> <li>IoT事業ガイドライン等の策定・見直し</li> <li>人材育成総合強化方針（仮称）を策定</li> <li>サイバー犯罪対策の強化</li> </ul>											
	サイバーセキュリティ戦略の推進											
	政府情報システムのクラウド化等により、今後5年間（2018年度まで）で政府情報システムの数を現在の1450から半減、8年間（2021年度まで）で運用コストの3割圧縮を目指す											
	OECD加盟国のブロードバンド料金比較（単位速度当たり料金）で、現在の1位を引き続き維持することを旨とする											
	MVNO契約数について、2016年中に1,500万契約を目指す											
	観光案内所、文化財、自然公園や、避難場所・避難所等の主要な観光・防災拠点について、2020年に向けて無料公衆無線LAN環境の整備を目指す											
	2020年度までに100自治体以上（自主財源によるものを含む）における成功モデル等の自立的な普及展開を目指す											
	サイバーセキュリティ産業の成長産業化											
	IoT事業ガイドライン等の策定・見直し											
	人材育成総合強化方針（仮称）を策定											
	サイバー犯罪対策の強化											

# 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（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～	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～
<ul style="list-style-type: none"> <li>■安全なIoTシステムの創出                     <ul style="list-style-type: none"> <li>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】</li> <li>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】</li> <li>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・手帳を実証【経済産業省】</li> </ul> </li> <li>■セキュリティマインドを持った企業経営の推進                     <ul style="list-style-type: none"> <li>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】</li> <li>経営ガイドラインの策定【経済産業省】</li> <li>「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】</li> <li>ISACを活用した情報共有体制の拡充【総務省】</li> </ul> </li> <li>■セキュリティに係るビジネス環境の整備                     <ul style="list-style-type: none"> <li>政府系ファンド等の活用検討【経済産業省】</li> <li>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】</li> <li>制御システムセキュリティ認証の拡大【経済産業省】</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>■国民・社会を守るための取組                     <ul style="list-style-type: none"> <li>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】</li> <li>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】</li> <li>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】</li> </ul> </li> <li>■重要インフラを守るための取組                     <ul style="list-style-type: none"> <li>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】</li> <li>メンバーの監視・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】</li> </ul> </li> <li>■政府機関を守るための取組                     <ul style="list-style-type: none"> <li>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】</li> <li>国の行政機関における統一基準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】</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>■我が国の安全の確保                     <ul style="list-style-type: none"> <li>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】</li> <li>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】</li> <li>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】</li> <li>部外インフラ等、関係主体との連携深化【防衛省】</li> </ul> </li> <li>■国際社会の平和・安定                     <ul style="list-style-type: none"> <li>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】</li> <li>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】</li> <li>各国における能力構築を支援【内閣官房 他】</li> </ul> </li> <li>■世界各国との協力連携                     <ul style="list-style-type: none"> <li>ASEAN諸国との連携を強化【内閣官房 他】</li> <li>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、米国の情報共有を強化【総務省】</li> <li>包括的な日米サイバー防衛の連携【防衛省】</li> </ul> </li> </ul>

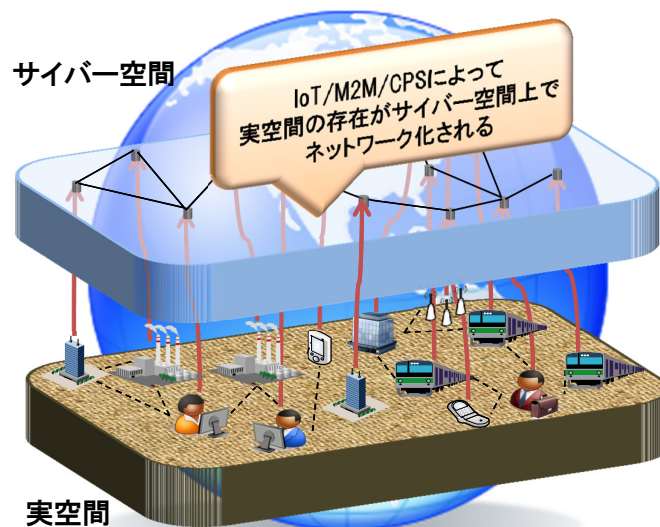
横断的 施策	研究開発の推進	人材の育成・確保
	<ul style="list-style-type: none"> <li>世界最先端のサイバー攻撃観測・分析技術、暗号基盤技術等に関する研究開発を実施【総務省】</li> <li>法律や国際関係、安全保障、経営学等の社会科学的視点も含め様々な領域の研究との連携、融合領域の研究を促進【内閣官房】</li> <li>戦略的イノベーション創造プログラム（SIP）の枠組み等により研究開発を推進【内閣府】</li> </ul>	<ul style="list-style-type: none"> <li>高度なITの知識と経営などその他の領域における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】</li> <li>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】</li> <li>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】</li> <li>サイバー防衛演習を通じた実践的セキュリティ人材の育成【総務省】</li> </ul>

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】

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

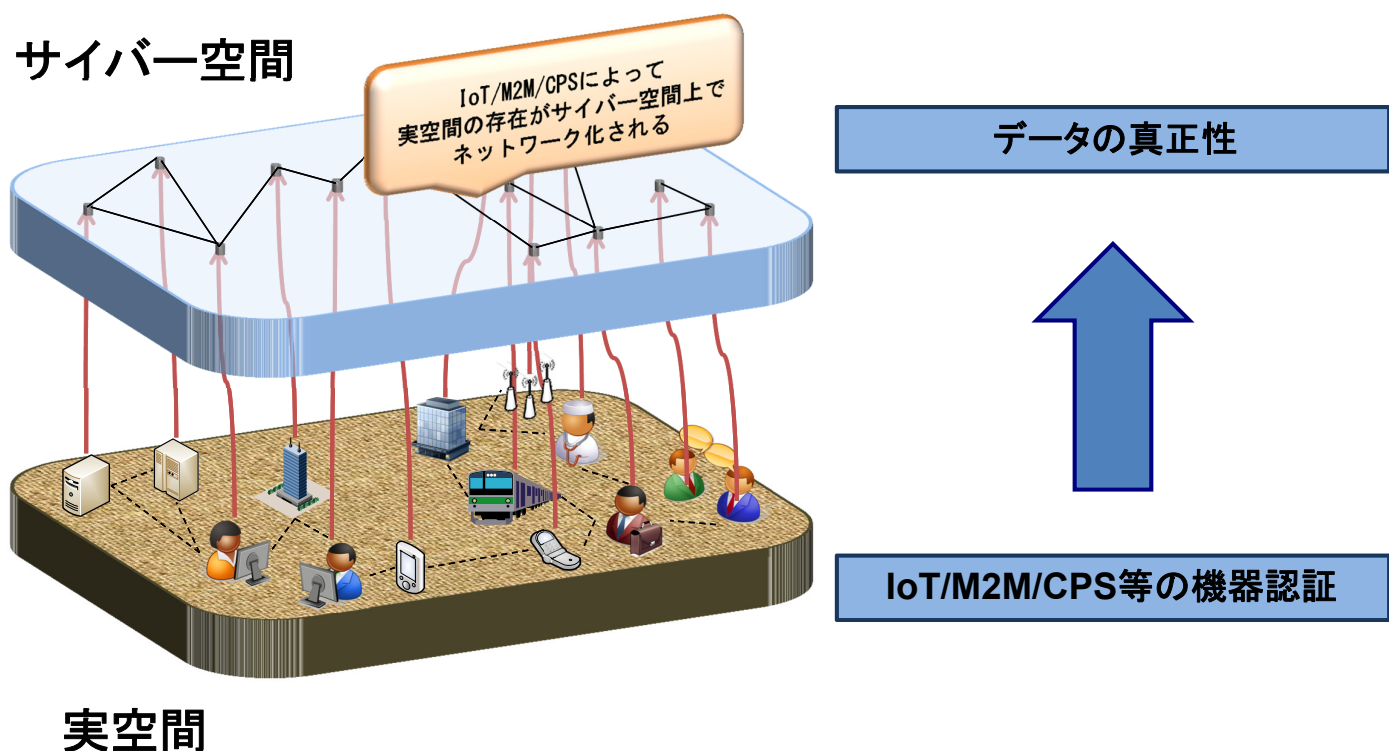
膨大なIoT/M2M/CPS等の機器が接続されたことで、サイバー攻撃に対するリスクが増大、複雑化し、影響範囲も広域化



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

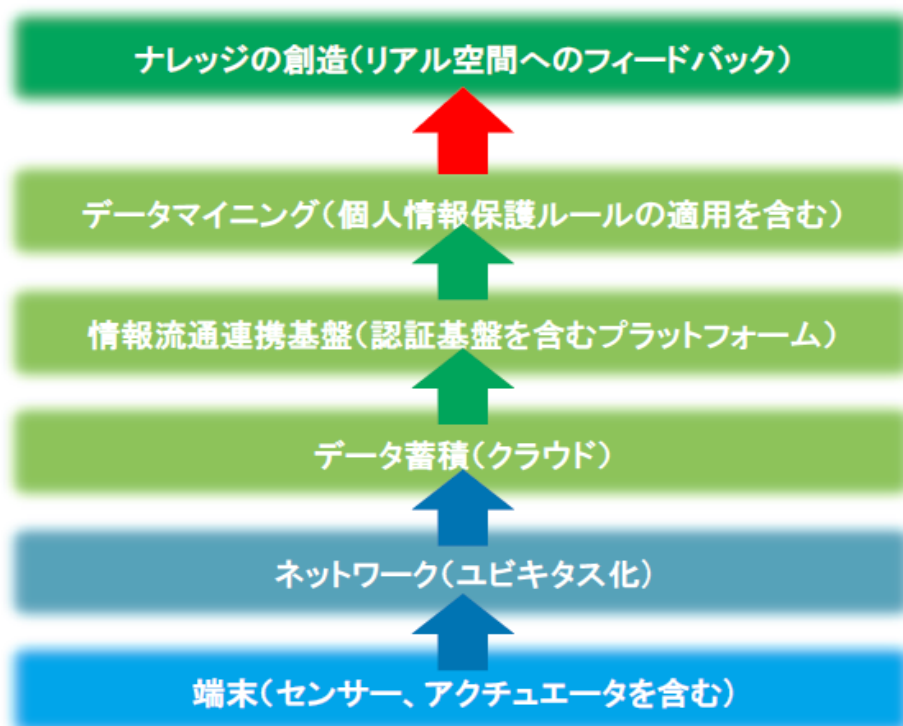
## 2. IoT/M2M/CPS等の課題と対策

### ● IoT/M2M/CPS等の機器認証、データの真正性



## 2. IoT/M2M/CPS等の課題と対策

### IoTセキュリティに関する検討事項 (例)



#### 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OSをベースにしている。
  - 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



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

## 3. 今後のサイバー空間の安心安全

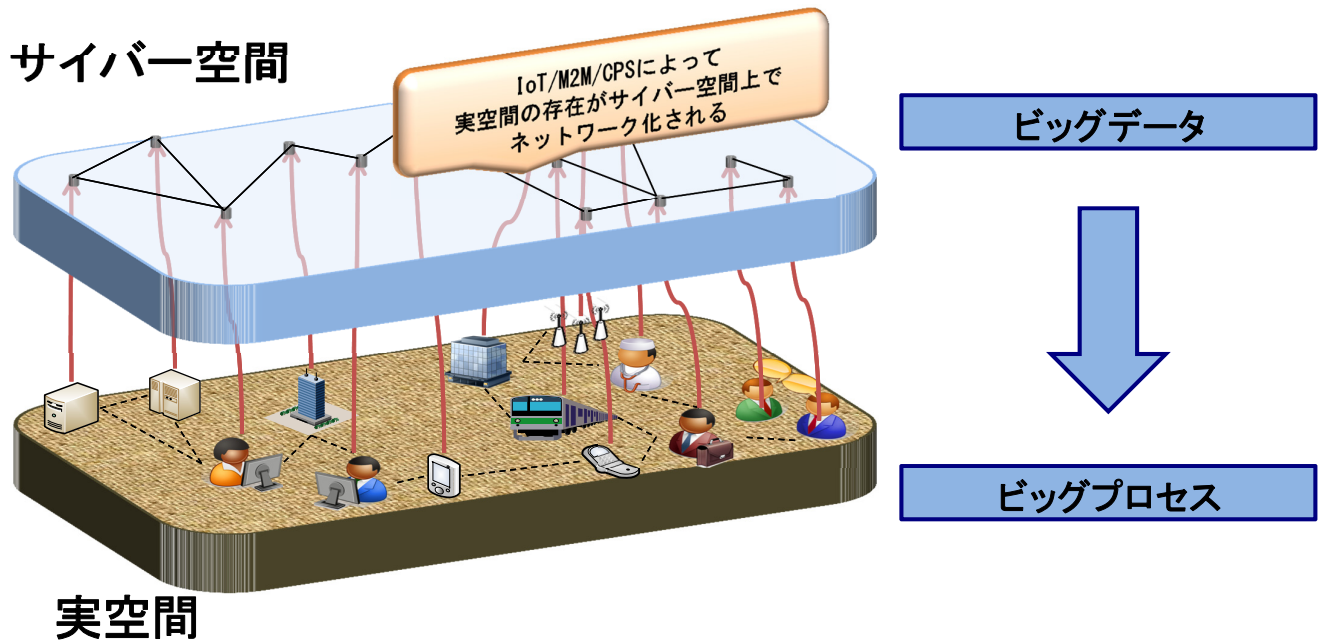
### ●情報セキュリティとは

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

<b>機密性</b> 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
<b>完全性</b> 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
<b>可用性</b> 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