資料１－３

我が国のサイバーセキュリティ政策の概要

2017年1月30日
内閣官房
内閣サイバーセキュリティセンター

サイバーセキュリティ政策の経緯

○今後の重要な環境変化
- 2020年東京オリンピック・パラリンピック競技大会
- マイナンバー利用開始
- IoTの広がり　等
  スマートメーター、自動走行システム等

省庁ＨＰ連続改ざん 2000.1
Webサーバの脆弱性への攻撃
米国同時多発テロ 2001.9
フィッシング詐欺 スパイウェア
ボットネットによる攻撃
Winny
DNSキャッシュポイズニング
誘導型攻撃の出現
米韓ＤＤｏＳ攻撃
Gumblar猛威
制御ｼｽﾃﾑStuxnet攻撃
9.18攻撃
遠隔操作ウィルス
韓国大規模障害
米国での中国軍関係者起訴・指名手配
水飲み場型攻撃
標的型攻撃 組織的高度化
感染PCによる不正送金
米国ｿﾆｰ(SPE)
年金機構情報流出

年度: 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 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」でのリスクベース対策 | 国家安全保障・危機管理としてのサイバーセキュリティ　高度なサイバー脅威に対し、積極的な対処が求められる時代に

e-Japan 戦略 (2001.1.22)
e-Japan 戦略Ⅱ (2003.7.2)
IT新改革戦略 (2006.1.19 IT戦略本部決定)
i-Japan 戦略2015 (2009.7.6)
新たな情報通信技術戦略 (2010.5.11 IT戦略本部決定)
世界最先端ＩＴ国家創造宣言 (2013.6.14 閣議決定, 2014.6.24 改定, 2015.6.30 改定, 2016.5.20 改定)

参考：IT利活用

基本戦略
- 第１次 情報ｾｷｭﾘﾃｨ基本計画 (2006.2.2 政策会議決定)
- 第２次 情報ｾｷｭﾘﾃｨ基本計画 (2009.2.3 政策会議決定)
- 国民を守る情報ｾｷｭﾘﾃｨ戦略 (2010.5.11 政策会議決定)
- サイバーセキュリティ基本法公布 (2014.11.12)
- ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略 (2015.9.4 閣議決定)
- サイバーセキュリティ基本法改正公布 (2016.4.22)
- ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略 (2013.6.10 政策会議決定)

年次計画
SJ：セキュアジャパン　JS：情報セキュリティ　CS：サイバーセキュリティ
SJ2006 | SJ2007 | SJ2008 | SJ2009 | JS2010 | JS2011 | JS2012 | CS2013 | CS2014 | CS2015 | CS2016

政府機関対策
- 情報セキュリティポリシーに関するガイドライン (2000.7 情報ｾｷｭﾘﾃｨ対策推進会議決定)
- 政府機関の情報セキュリティ対策のための統一基準
  - 第1版 (2005.12.13 政策会議決定) 第2版 (2007.6.14 政策会議決定) 第3版 (2008.2.4 政策会議決定)
  - 第4版 (2009.2.3 政策会議決定) 平成23年度版 (2011.5.11 政策会議決定) 平成24年度版 (2012.4.21 政策会議決定)
  - 平成26年度版 (2014.5.19 政策会議決定)

重要ｲﾝﾌﾗ対策
- 重要インフラのサイバーテロ対策に係る特別行動計画 (2000.12 情報ｾｷｭﾘﾃｨ対策推進会議決定)
- 重要インフラの情報セキュリティ対策に係る行動計画 (2005.12.13 政策会議決定)
- 重要インフラの情報セキュリティ対策に係る第2次行動計画 (2009.2.3 政策会議決定)
- 重要インフラの情報ｾｷｭﾘﾃｨ対策に係る第3次行動計画 (2014.5.19 政策会議決定, 2015.5.25 戦略本部改訂)

組織体制
- 内閣官房 情報セキュリティ対策推進室 (2000.2設置)
- 内閣官房情報セキュリティセンター (2005.4 設置)
- 情報セキュリティ政策会議 (2005.5 設置)
- GSOC (2008.4 運用開始)
- CYMAT (2012.6 設置)
- 内閣官房内閣ｻｲﾊﾞｰｾｷｭﾘﾃｨｾﾝﾀｰ (2015.1設置)
- サイバーセキュリティ戦略本部 (2015.1設置)

サイバーセキュリティ政策の推進体制

NISC

内閣

内閣総理大臣

高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）

高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進

緊密連携

サイバーセキュリティ戦略本部（2015.1.9 サイバーセキュリティ基本法により設置）

本部長　内閣官房長官
副本部長　サイバーセキュリティ戦略本部に関する事務を担当する国務大臣
本部員　国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣
情報通信技術（ＩＴ）政策担当大臣
東京オリンピック競技大会・パラリンピック競技大会担当大臣※
有識者（７名；10名以下）

閣僚が参画

※平成27年７月22日付け内閣総理大臣決定により本部員に指定

遠藤　信博	日本電気株式会社代表取締役会長
小野寺　正	ＫＤＤＩ株式会社代表取締役会長
中谷　和弘	東京大学大学院法学政治学研究科教授
野原佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
林　紘一郎	情報セキュリティ大学院大学教授
前田　雅英	日本大学大学院法務研究科教授
村井　純	慶應義塾大学教授

重要インフラ専門調査会
研究開発戦略専門調査会
普及啓発・人材育成専門調査会
サイバーセキュリティ対策推進会議（CISO等連絡会議）

緊密連携

国家安全保障会議（NSC）

我が国の安全保障に関する重要事項を審議

（事務局）

内閣官房　内閣サイバーセキュリティセンター（2015.1.9 内閣官房組織令により設置）

内閣サイバーセキュリティセンター長
（内閣官房副長官補(事態対処・危機管理)が兼務）
副センター長（内閣審議官）
上席サイバーセキュリティ分析官
サイバーセキュリティ補佐官

- 政府機関・情報セキュリティ横断監視・即応調整チーム（ＧＳＯＣ）
- 情報セキュリティ緊急支援チーム（CYMAT）

協力

＜重要インフラ所管省庁＞

金融庁	（金融機関）
総務省	（地方公共団体、情報通信）
厚生労働省	（医療、水道）
経済産業省	（電力、ガス、化学、クレジット、石油）
国土交通省	（鉄道、航空、物流）

＜その他関係省庁＞

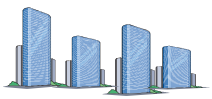
文部科学省（セキュリティ教育）等

協力

閣僚本部員５省庁

- 警察庁（サイバー犯罪・攻撃の取締り）
- 総務省（通信・ネットワーク政策）
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
- 防衛省（国の防衛）

重要インフラ事業者等

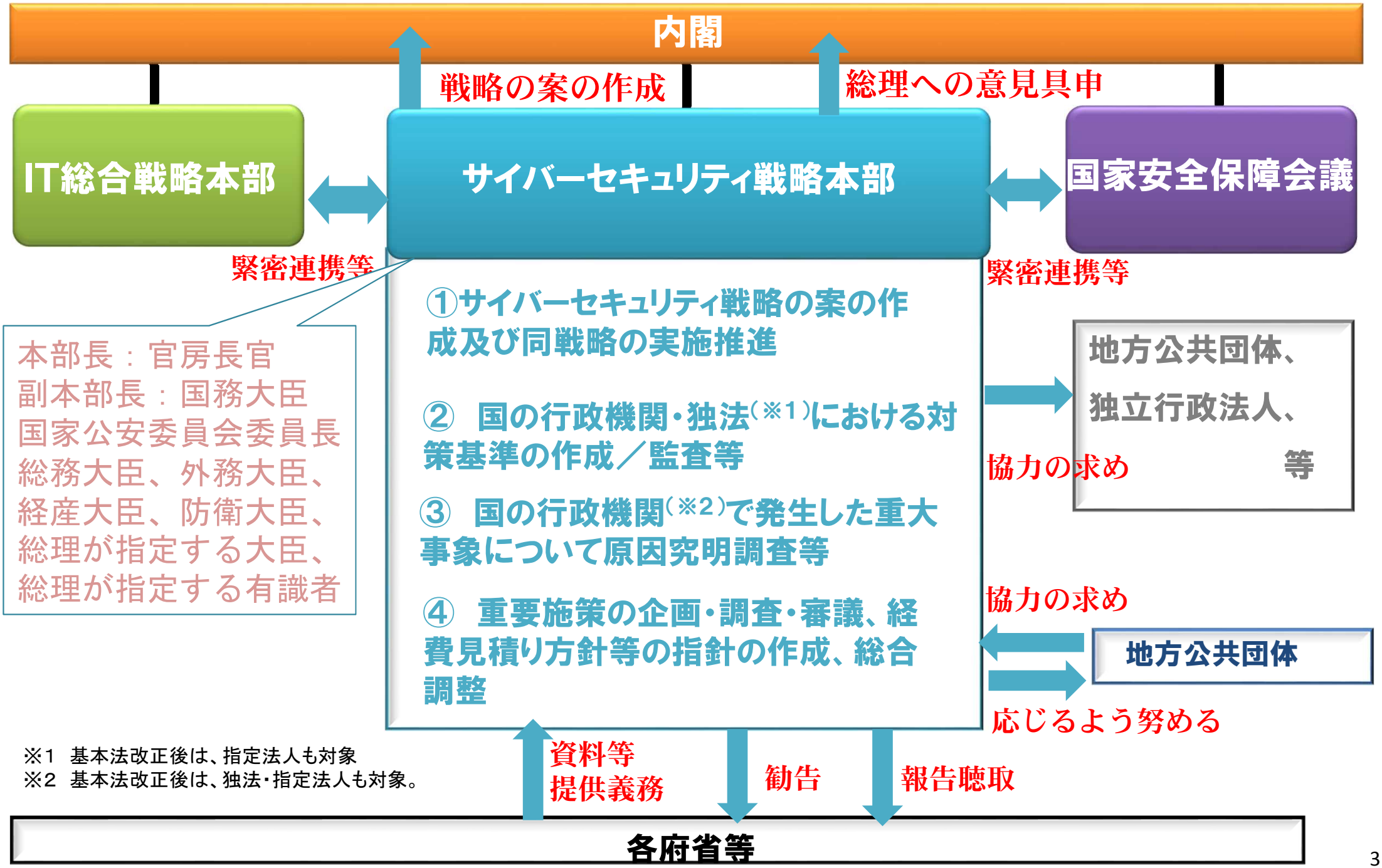


政府機関（各府省庁）

企業

個人

サイバーセキュリティ戦略本部の機能・権限（イメージ）



※1 基本法改正後は、指定法人も対象
※2 基本法改正後は、独法・指定法人も対象。

サイバーセキュリティ基本法の概要（平成28年改正後）

第Ⅰ章．総則

■**目的（第1条）**

■**定義（第2条）**

⇒「サイバーセキュリティ」について定義

■**基本理念（第3条）**

⇒ サイバーセキュリティに関する施策の推進にあたっての基本理念について次を規定

① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応

② 国民１人１人の認識を深め、自発的な対応の促進等、強靱な体制の構築

③ 高度情報通信ネットワークの整備及びITの活用による活力ある経済社会の構築

④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施

⑤ IT基本法の基本理念に配慮して実施

⑥ 国民の権利を不当に侵害しないよう留意

■**関係者の責務等（第4条～第9条）**

⇒ 国、地方公共団体、重要社会基盤事業者（重要インフラ事業者）、サイバー関連事業者、教育研究機関等の責務等について規定

■**法制上の措置等（第10条）**

■**行政組織の整備等（第11条）**

第Ⅱ章．サイバーセキュリティ戦略

■**サイバーセキュリティ戦略（第12条）**

⇒ 次の事項を規定

① サイバーセキュリティに関する施策の基本的な方針

② 国の行政機関等におけるサイバーセキュリティの確保

③ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進

④ その他、必要な事項

⇒ その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

第Ⅲ章．基本的施策

■**国の行政機関等におけるサイバーセキュリティの確保（第13条）**

■**重要インフラ事業者等におけるサイバーセキュリティの確保の促進（第14条）**

■**民間事業者及び教育研究機関等の自発的な取組の促進（第15条）**

■**多様な主体の連携等（第16条）**

■**犯罪の取締り及び被害の拡大の防止（第17条）**

■**我が国の安全に重大な影響を及ぼすおそれのある事象への対応（第18条）**

■**産業の振興及び国際競争力の強化（第19条）**

■**研究開発の推進等（第20条）**

■**人材の確保等（第21条）**

第Ⅲ章．基本的施策（つづき）

■**教育及び学習の振興、普及啓発等（第22条）**

■**国際協力の推進等（第23条）**

第Ⅳ章．サイバーセキュリティ戦略本部

■**設置（第24条）**

■**所掌事務等（第25条）**

⇒サイバーセキュリティ戦略案の作成、国の行政機関、独立行政法人・指定法人に対する監査・原因究明調査等の実施

■**組織等（第26条～第29条）**

⇒内閣官房長官を本部長として、副本部長（国務大臣）、国家公安委員会委員長、総務大臣、外務大臣、経済産業大臣、防衛大臣、総理が指定する国務大臣、有識者本部員で構成

■**事務の委託（第30条）**

⇒独立行政法人・指定法人に対する監査・原因究明調査の事務の一部をIPAその他政令で定める法人に委託（秘密保持義務を規定）

■**資料提供等（第31条～第36条）**

第Ⅴ章．罰則

■**罰則（第37条）**

⇒戦略本部からの事務の委託を受けた者が秘密保持義務に反した場合。1年以下の懲役又は50万円以下の罰金

「サイバーセキュリティ戦略」（2015年9月4日閣議決定）について（全体構成）

1 サイバー空間に係る認識

- サイバー空間は、「**無限の価値を産むフロンティア**」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがネットワークに連接され、実空間とサイバー空間との融合が高度に深化した「**連接融合情報社会**（**連融情報社会**）」が到来
  同時に、サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

2 目的

- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「**経済社会の活力の向上及び持続的発展**」、「**国民が安全で安心して暮らせる社会の実現**」、「**国際社会の平和・安定及び我が国の安全保障**」に寄与する。

3 基本原則

① 情報の自由な流通の確保　② 法の支配　③ 開放性　④ 自律性　⑤ 多様な主体の連携

4 目的達成のための施策

①後手から**先手**へ　／　②受動から**主導**へ　／　③サイバー空間から**融合**空間へ

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**
安全なIoT活用による新産業創出

■ **セキュリティマインドを持った企業経営の推進**
経営層の意識改革、組織内体制の整備

■ **セキュリティに係るビジネス環境の整備**
ファンドによるセキュリティ産業の振興

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**
事業者の取組促進、普及啓発、サイバー犯罪対策

■ **重要インフラを守るための取組**
防護対象の継続的見直し、情報共有の活性化

■ **政府機関を守るための取組**
攻撃を前提とした防御力強化、監査を通じた徹底

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**
警察・自衛隊等のサイバー対処能力強化

■ **国際社会の平和・安定**
国際的な「法の支配」確立、信頼醸成推進

■ **世界各国との協力・連携**
米国・ASEANを始めとする諸国との協力・連携

横断的施策

■ **研究開発の推進**
攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発

■ **人材の育成・確保**
ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

5 推進体制

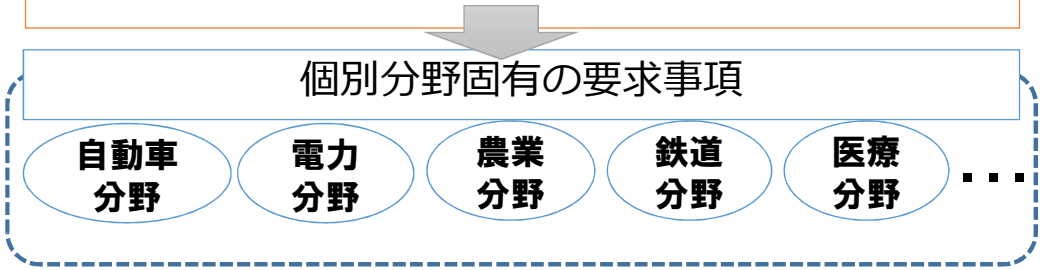
- 官民及び関係省庁間の連携強化、東京オリンピック・パラリンピック競技大会等に向けた対応

安全なIoTシステムのためのセキュリティに関する一般的枠組について（概要）

目的

- IoT(Internet of Things)システムは、従来の情報セキュリティの確保に加え、新たに**安全確保が重要**
- **セキュリティ・バイ・デザイン**の思想で設計・構築・運用されることが不可欠
- 安全なIoTシステムが具備すべき**一般要求事項としてのセキュリティ要件の基本的要素**を明らかにしたもの

安全なIoTシステムのためのセキュリティに関する一般的枠組み（個別分野の標準の**"テンプレート"**）



検討の視点

- 一つのIoTシステムリスクが他のIoTシステムに波及する可能性→**System of Systems**としての捉え方
- **機密性、完全性、可用性に加え、安全性**の要件確保

基本原則

- 関係者間の相互理解及び相互信頼の下、ネットワーク側とモノ側が、一体となり**システム全体としてセキュリティ確保**を図ることが必要。
- **セキュリティ・バイ・デザイン**を基本原則とし、**システム稼働前に確認・検証できる仕組**が必要。
- その際、基本方針の設定、リスク評価、システム設計、システム構築、運用・保守の**各段階の要件定義**が必要であり、以下の項目の明確化が必要。
  - ✓ 定義・範囲
  - ✓ 安全性・機密性・完全性・可用性
  - ✓ 確実な動作に必須事項、障害発生時の回復に必要な要件
  - ✓ 法律等からの要求事項
  - ✓ サイバー攻撃時の機能確保と迅速な復旧
  - ✓ 責任分界点、データの扱い方

取組方針

- **法令等の要求事項の明確化**
- IoTシステムの構成を**適切にモデル化**し、モデルを参照しながらセキュリティ要件を議論
- リスクアセスメントを活用した**セキュリティ対策や実装方法等の明確化**。ただし、リスクに応じた**柔軟な対応が必要**。
- 普遍的な**性能要求**とその時点での有効な手段の具体的方法を示す**仕様要求**の適切な適用
- 技術革新を前提とした**段階的・継続的アプローチ**
- IoTシステムに関連する者の**役割分担**（連携・協調によるセキュリティ確保の在り方や責任分界点の明確化を含む）
- データの利活用と個人情報保護の仕組み、機器認証の在り方などの**運用ルールの明確化**

安全なIoTシステムの創出に向けた取組

【安全なIoTシステムのためのセキュリティに関する一般的枠組】（2016年8月 NISC）

個別分野の標準のテンプレート（基本原則、共通の要求事項）

【前提となる考え方】　セキュリティ・バイ・デザイン
【明確化すべき要素】
◇定義・範囲　◇安全性・機密性・完全性・可用性
◇確実な動作に必須事項　◇法律等からの要求事項
◇迅速な復旧　◇責任分界点、データの扱い方

さまざまな分野がつながる中、共通言語でサイバーセキュリティ対策を進めていくために不可欠。（安全なIoTシステムのためのセキュリティに関する一般的枠組）

代表的なアーキテクチャ・セキュリティの対策事例集
通信系　セキュリティベンダー系　クラウド事業者系　・・・

セキュリティに対する関心の重点が異なる様々な関係者

分野固有の要求事項
自動車分野　電力分野　農業分野　鉄道分野　医療分野　・・・

事業の考え方・内容、文化、用語が異なる中で、個別に発展を遂げてきた各分野

上記体系でサイバーセキュリティ対策を進めるために今後必要な取組例

【国際標準化に向けた取組】

米国等の主要国と連携し、ISOなどの国際標準への提案に向けた取組を検討。今後策定される各分野固有の国際基準等について、標準のテンプレートを踏まえたものにし、我が国の強みを国際標準に反映していく。

【日本国内の基準等への適用】

日本国内の様々な関係者が策定する基準やガイドラインについて、標準のテンプレートをベースとしたものとなるよう促し、展開を図ることで我が国のIoTシステムの国際競争力を高めていく。

重要インフラの情報セキュリティ対策に係る第４次行動計画（案）の概要

１．本行動計画のポイント

◆ 重要インフラサービスを、安全かつ持続的に提供できるよう、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らし、迅速な復旧が可能となるよう、経営層の積極的な関与の下、情報セキュリティ対策に関する取組を推進。（機能保証の考え方）

◆ また、取組を通じ、オリパラ大会に関係する重要なサービスの安全かつ持続的な提供も図る。

２．重要インフラの情報セキュリティ対策の現状と課題

◆ 第３次行動計画に基づく施策群により、自主的な取組が浸透しつつあるが、ＰＤＣＡのうちＣＡに課題。一部で先導的な取組も進展。

◆ 機能保証のため、情報系(ＩＴ)に限らず、制御系(ＯＴ)を含めた情報共有の質・量の改善や、重要インフラサービス障害に備えた対処態勢の整備が必要。

◆ 国内外の多様な主体との連携、情報収集・分析に基づく国民への適切な発信の継続・改善が必要。

３．本行動計画の３つの重点

次の３つを重点として、第３次行動計画の５つの施策群の補強・改善を図る。

①　先導的取組の推進(クラス分け)

■ 他分野からの依存度が高く、比較的短時間のサービス障害でも影響が拡大するおそれがある分野(例：電力、通信、金融)において、一部事業者における先導的な取組（ＩＳＡＣ※の設置やリスクマネジメントの確立等）を強化・推進

※所属事業者間で秘密保持契約を締結するなど、より機密性の高い情報の共有等を目的とした組織

■ 上記先導的な取組みの、当該重要インフラ分野内の他の事業者等及び他の重要インフラ分野への展開による我が国全体の防護能力の強化

②　オリパラ大会も見据えた情報共有体制の強化

■ サービス障害の深刻度判断基準の導入に向けた検討

■ 連絡形態の多様化（連絡元の匿名化、セプター※事務局・情報セキュリティ関係機関経由）による情報共有の障壁の排除。分野横断的な情報を内閣官房に集約する仕組みの検討

※重要インフラ事業者等の情報共有を担う組織

■ ホットライン構築も可能な情報共有システムの整備（自動化、省力化、迅速化、確実化）

■ 情報連絡・情報提供の範囲にＯＴ、ＩｏＴ等を含むことを明確化（ＩＴ障害→重要インフラサービス障害）

■ 演習の改善、演習成果の浸透による防護能力の維持・向上

■ サプライチェーンを含む「面としての防護」に向け範囲の拡大

③　リスクマネジメントを踏まえた対処態勢整備の推進

■ 「機能保証に向けたリスクアセスメントガイドライン」の提供及び説明会の実施等によるリスクアセスメントの浸透

■ 事業継続計画及び緊急時対応計画（コンティンジェンシープラン）の策定等による重要インフラ事業者等の対処態勢の整備

■ 事業者等における内部監査等の取組において、リスクマネジメント及び対処態勢における監査の観点の提供等による「モニタリング及びレビュー」を強化

４．本行動計画の期間

➢　第４次行動計画（案）はオリパラ大会開催までを視野に入れ、大会終了後に見直しを実施。その間であっても、必要に応じて見直す。

サイバーセキュリティ分野における国際連携

サイバー空間に関するグローバルな議論

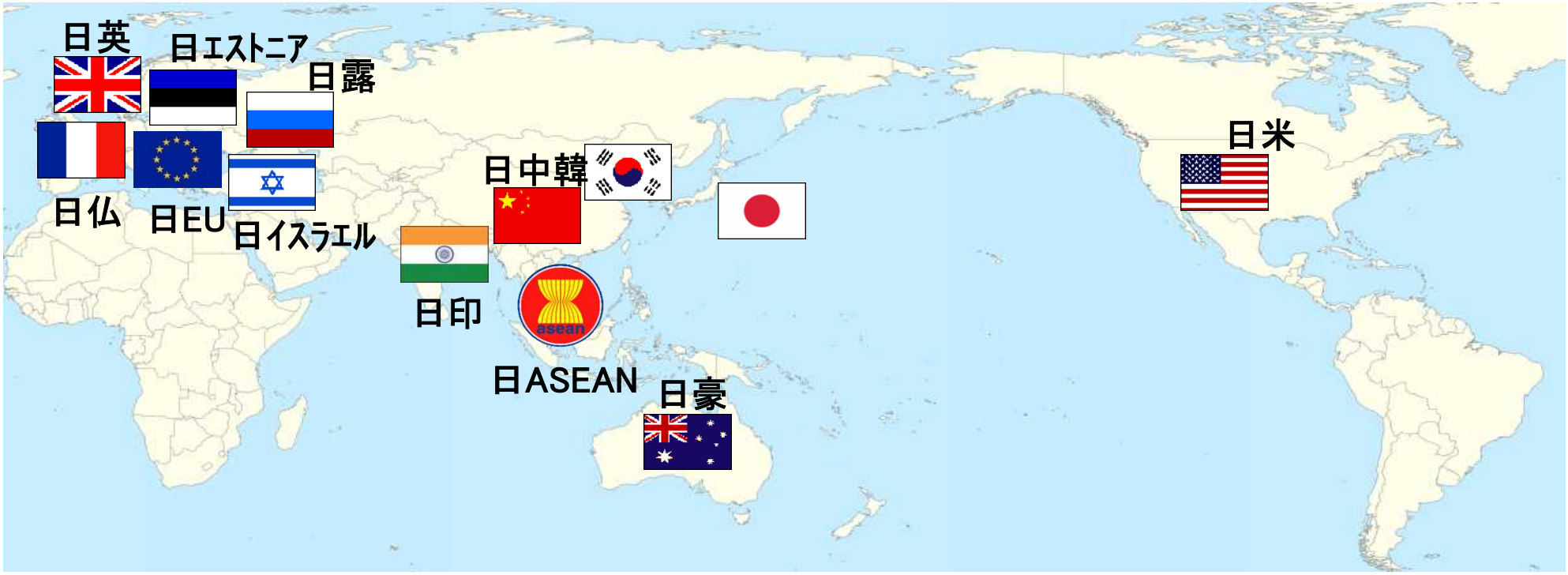
- サイバー空間の国際的な規範形成、最先端の知見の共有、信頼醸成を目的として、国連サイバー政府専門家会合、重要インフラ所管省庁によるMeridian会議、グローバルな情報共有を行うIWWN、産学官の関係者が一堂に会する「サイバー空間に関するロンドン会議」プロセス等に参加。

二国間協議

- 2012年の英国及びインドをはじめ、米国、EU、中韓、イスラエル、仏、エストニア、豪州及び　ロシアとの間でサイバー協議を開始。各国との間で年1回程度の頻度でサイバー空間に関する政府横断的な政策協議を継続的に実施。我が国のサイバーセキュリティ政策を紹介しつつ、具体的トピックを議論（協議全体は外務省が取りまとめ）。

地域連携・セキュリティレベル底上げ

- セキュリティマネジメント体制の確立、維持、改善などを目的として日ASEAN情報セキュリティ政策会議等を実施。



社会で活躍できる人材・政府機関における人材の育成

人材の需要面

経営層
↕
橋渡し人材層
↕
実務者層

○経営層の示す経営方針を理解
○サイバーセキュリティに係るビジョンの提示
○実務者層との意思疎通の支援

（1）経営層の意識改革

（2）「橋渡し人材層」の育成（→経営層への働きかけ）

人材の供給面

人材像の提示
➢産業界で求められる人材像の明確化（平成28年度中）

↓

教育の充実
➢enPiT等の大学教育の充実（平成28年度から大学学部にも拡大）、等

↓

演習環境の整備
➢NICTにおける実践的なサイバー防御演習（CYDER）の拡充（法制度の整備を含む）、等

↓

能力の可視化
➢情報処理安全確保支援士制度（平成32年までに3万人超の有資格者の確保）

政府機関における人材の育成

○各府省庁における司令塔機能の抜本的強化

サイバーセキュリティ・情報化審議官等の主導の下、人材の着実な確保・育成を図るため、採用、人材育成、将来像等にわたる具体的な取組方策を定めた**「セキュリティ・IT人材確保・育成計画（仮称）」**を**本年8月までに**作成

民間等におけるセキュリティ・IT高度専門人材* ⇔ 橋渡し人材管理職 ⇔ 一般行政部門*

○橋渡し人材の確保・育成

セキュリティ・ITの一定の専門性と所管行政の知識・経験を有し、民間等におけるセキュリティ・IT高度専門人材と一般行政部門との橋渡しをする人材を確保

○研修体系の抜本的整理等

➢ 新たに役職段階別に研修体系を抜本的整理（**橋渡し人材の受講者数を今後4年で1千人超規模を目指す**）、修了者にスキル認定を行う枠組みの構築
➢ 管理職に実践的な演習等に係る研修を実施

enPiT：「成長分野を支える情報技術人材の育成拠点の形成」事業　Education Network for Practical Information Technologiesの略称（「エンピット」と読む）
NICT：国立研究開発法人情報通信研究機構　National Institute of Information and Communications Technologyの略称
CYDER：実践的なサイバー防御演習　CYber Defense Exercise with Recurrenceの略称

2020年東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ確保のための取組

大会の運営に大きな影響を及ぼし得る重要システム・サービスを対象としたリスクアセスメントに基づく対策の促進や、大会組織委員会を含めた関係組織との情報共有の中核的組織としての対処体制（オリンピック・パラリンピックCSIRT）の整備に向けて検討を実施。

東京オリンピック・パラリンピック競技大会に向けた取組

リスクアセスメントに基づく対策の促進
（事前対応のための取組）

○ 大会の開催・運営に影響を与える重要サービス事業者等を選定し、リスクアセスメントの実施を依頼。各事業者等は、10～12月の期間でリスクアセスメントを実施中。

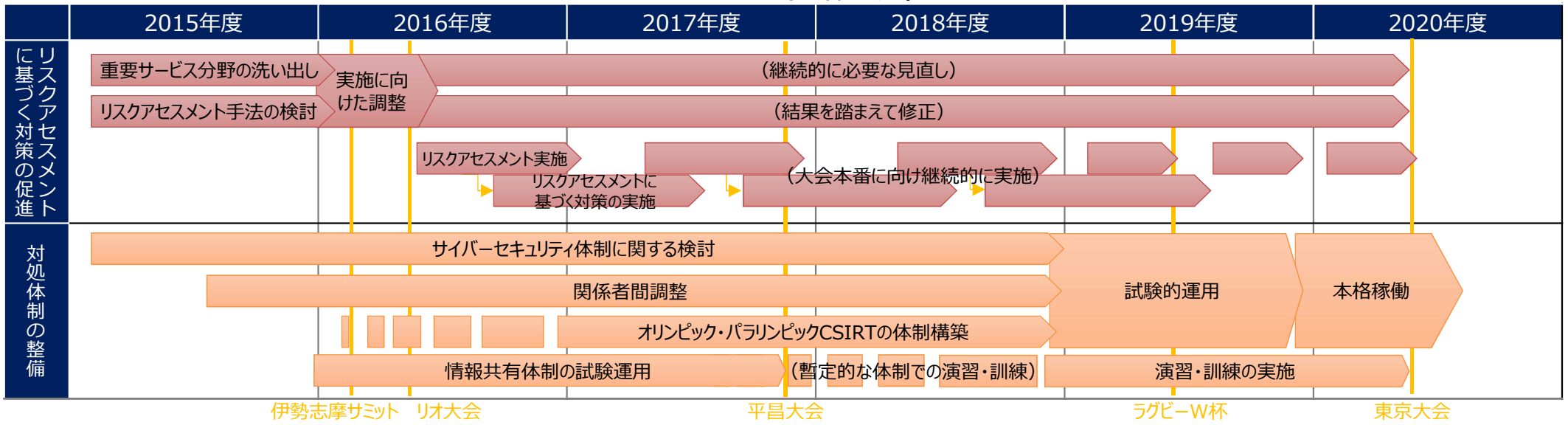
○ 事業者等が実施するリスクアセスメントの手順書をNISCにおいて作成。現在、NISCでは事業者等からの手順に関する問合せへの対応を実施。

対処体制の整備
（事案発生時の迅速かつ的確な対処のための取組）

○ 関係組織に対して対処のための的確な情報共有を担う中核的組織としての対処体制（オリンピック・パラリンピックCSIRT）の構築に向け、2020年東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ体制に 関する体制検討会において、具体的な体制を検討。

○ G7伊勢志摩サミット及びリオ大会において、現地に連携要員を派遣。情報共有手段として同検討会メンバーを中心とした体制の試験運用を実施。

スケジュール（全体想定）



2020年東京オリンピック・パラリンピック競技大会のサイバーセキュリティの確保に向けたリスク評価への取組状況

◆ 重要インフラ事業者を含む、東京大会の円滑な運営に不可欠なサービスを提供する事業者等を選定。NISCが作成した手順に基づき、東京23区内の事業者等を対象に第1回目のリスク評価を実施。
◆ 来年度以降は、東京圏、地方会場に関連する事業者等に拡大しつつ、2020年までにリスク評価を計６回実施予定。

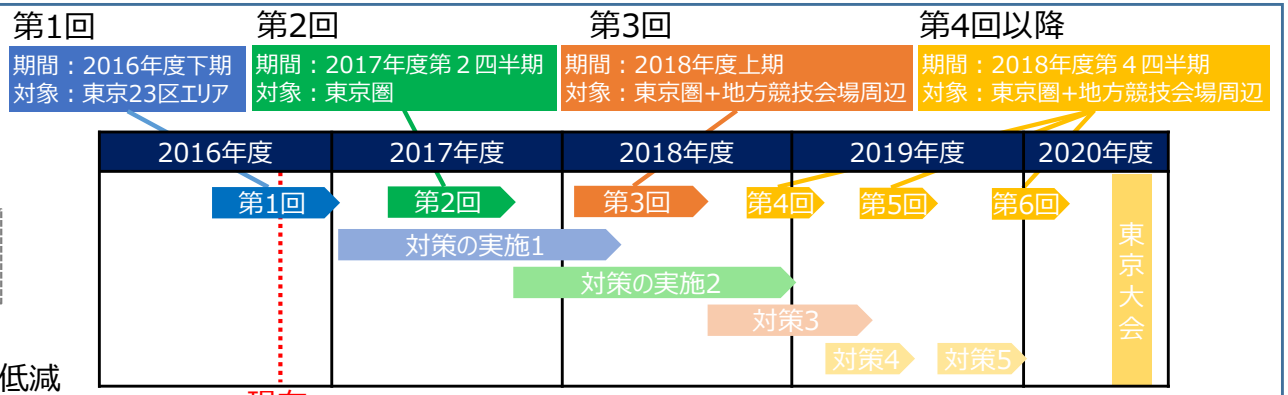
リスク評価の取組概要

○ リスクマネジメントの促進のため、サイバーセキュリティリスクを特定・分析・評価する手順をNISCで作成（添付資料を参照）

○ 東京大会の開催・運営に影響に与えうる重要サービス分野を、関連する所管省庁と調整の上で選定

通信、放送、金融、航空、鉄道、電力、ガス、上水道、物流、クレジット、行政サービス（地方自治体）、下水道、空港、道路・海上・航空交通管制、緊急通報、気象・災害情報、出入国管理、高速道路、熱供給　計19分野

○ 東京大会に向けて、継続的に複数回実施することを想定
- 事業者等：PDCAサイクルを繰り返すことで、リスクを継続的に低減
- NISC：対象とする事業者等の拡大、手順の充実化



東京大会に向けたリスク評価の取組スケジュール

2016年度の取組状況

＜これまで（第１回）の取組状況＞

○ 東京23区エリアの事業者等がリスク評価を実施
- これまでに約70組織から実施結果を受領
  このほかの事業者等は、組織の事情に応じた時期に実施を予定
- ９月に説明会を６回に分け開催。所管省庁・事業者等から計215名が参加
- 11月に情報交換会を開催。事業者等の担当者ら51名が参加

＜今後の予定＞

○ リスク評価により明らかになったリスクへの対策実施を依頼

○ 第２回以降の取組に向けて準備と改善を実施
- 第１回で受領したレポートをもとにしたリスク評価の手順の見直し
- リスク評価を実施する事業者等の拡大
  - 対象地域を拡大し、東京23区外の地方競技会場周辺を追加
  - 大会計画の更新をもとに、対象の重要サービス分野を見直し
- 組織委員会等との継続的な意見交換により、大会開催時に要求されるサービス提供レベルを明確化
- 事業者等との情報交換を継続的に実施

第１回目（2016年度）の実施スケジュール


事業者等向けの説明会（9月）の様子


事業者等との情報交換会（11月）の様子

2017年「サイバーセキュリティ月間」（2/1～3/18）について（案）

【実施概要】
○国民のサイバーセキュリティに関する意識を向上させるため、行事の開催や広報等の普及啓発活動を集中実施。
○昨年度から引き続き<u>メディアとのタイアップ</u>や<u>競技形式の訓練（NATIONAL 318（CYBER） EKIDEN）</u>、<u>日替わりコラムの掲載</u>等を実施。
○さらに、サイバーセキュリティの普及啓発のために<u>体験型イベント</u>を開催するとともに、<u>官民のコラボ</u>を積極的に実施。

※　記載事項は月間中に予定されている取組。

今年度実施予定の取組

●『情報セキュリティハンドブック』の普及

情報セキュリティハンドブックの最新版を公開。身近な話題からサイバーセキュリティに関する基本的な知識を紹介し、一緒に学んでいただくことを目的に作成。

←イラスト例

（本ハンドブックの目次）
プロローグ　サイバー攻撃ってなに？
第1章　基本のセキュリティ
～ステップバイステップでセキュリティを固めよう～
第2章　セキュリティを理解して、ネットを安全に使う
第3章　スマホ・パソコンのより進んだ使い方やトラブルの対処の仕方
第4章　被害に遭わないために、知らない間に加害者にならないために
第5章　自分を守る、家族を守る、災害に備える
エピローグ　来たるべき新世界
※第1章以外を平成28年12月15日に新規公開。

●メディアを通じた普及啓発活動

国民に親しみやすいメディアの影響力に着目し、サイバーセキュリティ対策の重要性を国民一人一人に訴求していくことを期待。

<u>著名な作品の活用を通じた官民連携</u>

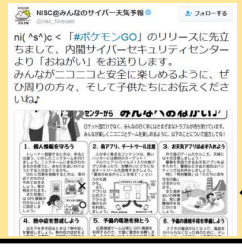
今年度は『劇場版 ソードアート・オンライン －オーディナル・スケール－』とタイアップし、サイバーセキュリティに興味を持ってもらう取組を官民連携で展開。その取組の一つとして、ポスターやバナーを作成し、関係機関等で貼付してもらい、多くの方々へ月間周知を行うとともに、サイバーセキュリティ対策の重要性を訴求。

↑2017年版ポスター

●キャッチフレーズ「＃サイバーセキュリティは全員参加」

月間中は「＃サイバーセキュリティは全員参加」をつけて、様々な情報を発信。引き続き、みんなのサイバー天気予報ではセキュリティ関連情報やブログ等の読み物も情報発信。

参考：みんなのサイバー天気予報
フォロワー 8,700以上（twitter）、60,000以上（LINE）※平成29年1月19日時点



NISC@ みんなのサイバー天気予報

↑アイコン

←ツイート例
（NISCからの注意喚起）

●「サイバー攻撃を目撃せよ！2017」（仮称）の開催

一人でも多くの方にサイバーセキュリティに関する意識を高めていただくために、ウィルス感染によるパソコンの乗っ取りの実演やVR／AR機器の展示・体験などを、官民のコラボを通して、３月４～５日の２日間秋葉原にて実施。



2016年の様子↑→

トップメッセージ発信

月間に関するメッセージを発出。記者会見、 Webサイト等を活用し周知。

↑2016年のメッセージ

キックオフ・シンポジウムの開催

月間のキックオフイベントとして毎年開催。今年度は「IoT時代のサイバーセキュリティ」をテーマに企業の直面している課題等について議論。


↑2016年の様子

コラムの掲載

コラム「サイバーセキュリティ　ひとこと言いたい！」を掲載。

↑2016年のコラム執筆者

NATIONAL 318 (CYBER) EKIDENの開催

各府省庁対抗による、競技形式のサイバー攻撃対処訓練を実施。


実績：（2016年）
官房長官表彰　警察庁
総務大臣表彰　厚生労働省
遠藤国務大臣表彰　文部科学省

ロゴマークの活用

前回に引き続き、ロゴマークを活用して国及び国民全体の活動として一体的に推進。

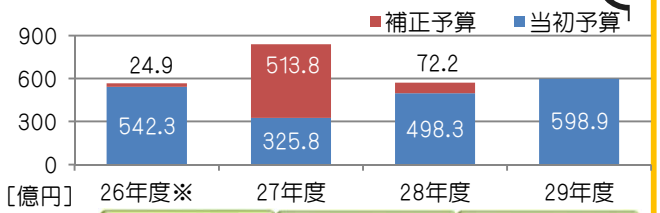
政府のサイバーセキュリティに関する予算

平成29年度予算政府案

598.9億円

（平成28年度当初予算額　498.3億円）

サイバーセキュリティに関する予算として切り分けられない場合には計上していない。



主な施策例及び予算額

		平成29年度予算政府案	平成28年度第2次補正	平成28年度当初予算
【内閣官房】	内閣サイバーセキュリティセンター予算	23.9億円	4.2億円	17.3億円
【警察庁】	サイバーテロ対策用資機材の増強等	4.1億円	—	4.0億円
【警察庁】	サイバーセキュリティ対策に係る人材育成基盤の整備	8.7億円	—	—
【総務省】	ナショナルサイバートレーニングセンター（仮称）の構築	15.0億円	—	7.2億円
【総務省】	ICT環境の変化に応じた情報セキュリティ対応方策の推進事業	3.8億円	—	4.0億円
【総務省】	IoT時代におけるサイバーセキュリティ総合対策実証事業	—	5.0億円	—
【総務省】	自治体の情報セキュリティ対策の強化	3.3億円	—	—
【外務省】	情報セキュリティ対策の強化	6.1億円	—	4.1億円
【外務省】	サイバー空間に関する外交及び国際連携	0.1億円	—	0.1億円
【経済産業省】	産業系サイバーセキュリティ推進事業	11.7億円	25.0億円	—
【経済産業省】	（独）情報処理推進機構（IPA）交付金	45.4億円	4.0億円	42.5億円
【経済産業省】	サイバーセキュリティ経済基盤構築事業	21.6億円	—	21.6億円
【防衛省】	作戦システムセキュリティ監視装置の整備	7.0億円	—	—
【防衛省】	サイバー攻撃等への対処能力を強化するサイバーレジリエンス技術の研究	7.0億円	—	—
【個人情報保護委】	特定個人情報（マイナンバーをその内容に含む個人情報）に係るセキュリティの確保を図るための委員会における監視・監督体制の拡充	13.3億円	—	2.6億円
【厚生労働省】	本省及び日本年金機構等の関係機関における情報セキュリティ対策の強化	42.1億円	1.8億円	39.6億円
【文部科学省】	大学や高専におけるセキュリティ人材の育成	4.4億円	—	3.8億円
【文部科学省】	国立大学法人等における情報セキュリティ体制の基盤構築	8.0億円	—	7.8億円
【金融庁】	金融業界横断的なサイバーセキュリティ演習の実施	0.5億円	—	0.3億円
【国土交通省】	重要インフラ事業者等に対する情報セキュリティ強化策	0.6億円	—	0.3億円

平成28年度第2次補正予算

72.2億円

サイバーセキュリティに関する予算として切り分けられない場合には計上していない。

※　平成26年度の数値は、社会保障と税に関する番号制度の導入に伴うシステム開発（内閣官房）等も含む。

2020年及びその後を見据えたサイバーセキュリティの在り方について

【検討の背景】

現在

2014年度	2015年度	2016年度	2017年度	2018年度	2019年度	2020年度
▲基本法制定（'14/11）	▲NISC発足（'15.1）	▲現行戦略決定（'15.9）	▲改正基本法施行（'16.11）			▲2020東京大会（'20.7）

見直し検討（基本法・・・）★

見直し検討（戦略・・・）

施行後二年以内に同法の施行状況等を踏まえ、同法見直しの必要性を検討。その結果に基づく必要な措置を講ずる（付帯決議）

今後3年間に実施すべき施策の基本的な指針を示す

◆ サイバーセキュリティ戦略の期間（～'18年9月）及び改正基本法の見直し期限（～'18年10月）まで1年余り

◆ 2020年東京大会に向けた抜本的対策を見据えた取組の必要（当該取組はその後も見据えたもの）

【脅威の変化】

脅威の一層の複雑化
- 攻撃手法の高度化・大規模化
- 攻撃の「サービス化」
- 重要インフラのIT化の進展

防護対象の拡大
- 防護対象の面的増加
- マイナンバーの利活用の拡大
- 先端技術保有者への脅威の増大

脅威のグローバル化
- IoT機器の指数関数的増大と拡散
- 同時多発的なグローバルなサイバー攻撃等の増加

2020年及びその後に向けて更なる取組が必要

【課題と検討事項（例）】

IoTセキュリティの強化

◆ セキュアなIoTシステムの実現
◆ 日本発技術の開発・普及

（検討事項例）
- ✓ IoTｾｷｭﾘﾃｨ対策の官民連携体制強化
- ✓ IoTｾｷｭﾘﾃｨの国際標準化の推進　等

国際対応の強化

◆ 米国等との情報共有・連携の強化

（検討事項例）
- ✓ 先進国等との脅威情報等の共有・連携の強化
- ✓ 日本発製品・サービスの海外展開支援
- ✓ 途上国への政府開発援助等を通じた支援　等

重要インフラ等に関する取組強化

◆ 検知・判断・防御体制（重要ｲﾝﾌﾗ等）の強化
◆ 危機管理体制との連携強化

（検討事項例）
- ✓ 重要ｲﾝﾌﾗ等の障害・事故、脅威情報　の総合的な情報共有　（ﾊﾞｰﾁｬﾙｻｲﾊﾞｰ脅威情報集約ｾﾝﾀｰ構築、情報共有ｼｽﾃﾑ・ﾎｯﾄﾗｲﾝ構築）
- ✓ 最新技術を活用した政府機関等の監視システムの高度化
- ✓ 警戒体制の整備　（深刻度の場合分け・警戒レベルの設定）
- ✓ 危機管理体制との連携強化　（物理ｾｷｭﾘﾃｨに連動した緊急対応計画の策定等）　等

その他の主体に関する取組強化

◆ 地方公共団体における対策の一層の促進
◆ 研究開発法人、大学法人等における対策の促進

（検討事項例）
- ✓ 地方公共団体のｾｷｭﾘﾃｨ水準向上支援
- ✓ 先端技術保有者（大学等）のｾｷｭﾘﾃｨ水準向上支援　等

東京ｵﾘﾝﾋﾟｯｸ・ﾊﾟﾗﾘﾝﾋﾟｯｸ競技大会等に向けた対策の強化

◆ 2020東京ｵﾘﾊﾟﾗ大会を見据えた対処体制の強化

連　携

（検討事項例）
- ✓ ｵﾘﾊﾟﾗ対処調整ｾﾝﾀｰの整備、重要ｲﾝﾌﾗ事業者のﾘｽｸ分析の促進、十分な演習・訓練の実施　等

（参考）
サイバーセキュリティ戦略

1 サイバー空間に係る認識
2 目的
3 基本原則
4 目的達成のための施策
- 経済社会の活力の向上及び持続的発展
- 国民が安全で安心して暮らせる社会の実現
- 国際社会の平和・安定及び我が国の安全保障
- 研究開発の推進、人材の育成・確保

5 推進体制

【今後の予定】

2017年1月25日	戦略本部（第11回）	検討方針等
今年度末目途	戦略本部（第12回）	方針の骨格の決定
来年度夏頃	戦略本部（第13回）	方針の決定
～2018年6月	可能な施策から段階的に実施（1年以内の完全実施）	

この間、有識者会合の開催（随時）

参考資料

重要インフラの情報セキュリティ対策に係る第４次行動計画（案）

官民連携による重要インフラ防護の推進

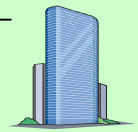
重要インフラにおいて、機能保証の考え方を踏まえ、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する。

重要インフラ（１３分野）

- 情報通信
- 金融
- 航空
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油

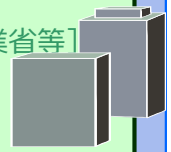
ＮＩＳＣによる調整・連携

重要インフラ所管省庁（５省庁）



- 金融庁　［金融］
- 総務省　［情報通信、行政］
- 厚生労働省　［医療、水道］
- 経済産業省　［電力、ガス、化学、クレジット、石油］
- 国土交通省　［航空、鉄道、物流］

関係機関等



- 情報セキュリティ関係省庁［総務省、経済産業省等］
- 事案対処省庁［警察庁、防衛省等］
- 防災関係府省庁［内閣府、各省庁等］
- 情報セキュリティ関係機関［NICT、IPA、JPCERT等］
- サイバー空間関連事業者［各種ベンダー等］

重要インフラの情報セキュリティ対策に係る第４次行動計画（案）

安全基準等の整備・浸透

重要インフラ各分野に横断的な対策の策定とそれに基づく、各分野の「安全基準」等の整備・浸透の促進

情報共有体制の強化

連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化

障害対応体制の強化

官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化

リスクマネジメント及び対処態勢の整備

リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの支援

防護基盤の強化

重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等の推進

第４次行動計画（案）の基本的考え方・要点

「重要インフラ防護」の目的

重要インフラにおいて、機能保証の考え方を踏まえ、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現すること。

「基本的な考え方」

情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施するものである。
重要インフラ全体の機能保証の観点から、官民が一丸となった重要インフラ防護の取組を通じて国民の安心感の醸成を目指す。

- 重要インフラ事業者等は事業主体として、また社会的責任を負う立場としてそれぞれに対策を講じ、また継続的な改善に取り組む。
- 政府機関は、重要インフラ事業者等の情報セキュリティ対策に関する取組に対して必要な支援を行う。
- 取組に当たっては、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは多様な脅威への対応に限界があることから、他の関係主体との連携をも充実させる。

各関係主体（重要インフラ事業者等、政府機関、情報セキュリティ関係機関等）の在り方

- 自らの状況を正しく認識し、活動目標を主体的に策定するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況を把握し、相互に自主的に協力する。
- 重要インフラサービス障害の規模に応じて、情報に基づく対応の５Ｗ１Ｈを理解しており、重要インフラサービス障害の予兆及び発生に対し冷静に対処ができる。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携、統制の取れた対応ができる。

重要インフラ事業者等の経営層の在り方

- 情報セキュリティの確保は経営層が果たすべき責任であり、経営者自らがリーダーシップを発揮し、機能保証の観点から情報セキュリティ対策に取り組むこと。
- 自社の取組が社会全体の発展にも寄与することを認識し、サプライチェーン（ビジネスパートナーや子会社、関連会社）を含めた情報セキュリティ対策に取り組むこと。
- 情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと。
- 上記の各取組に必要な予算・体制・人材等の経営資源を継続的に確保し、リスクベースの考え方により適切に配分すること。

第４次行動計画（案） 施策①：安全基準等の整備及び浸透

重要インフラ防護能力の維持・向上を目的として、セキュリティ対策のPDCAに沿って「指針」及び「安全基準等」の継続的改善を推進する。

※安全基準等・・・関係法令、業界標準／ガイドライン、内規等の総称
※指針・・・・・・安全基準等の策定・改定に資するため、分野横断的に必要度の高い対策項目を収録したもの

現状の課題

- 自主的に見直しの必要性を判断し改善できるサイクル自体は重要インフラ事業者等の行動規範として浸透しつつあるが、PDCAサイクルのCheck（確認）及びAct（是正）における取組の定着が課題である

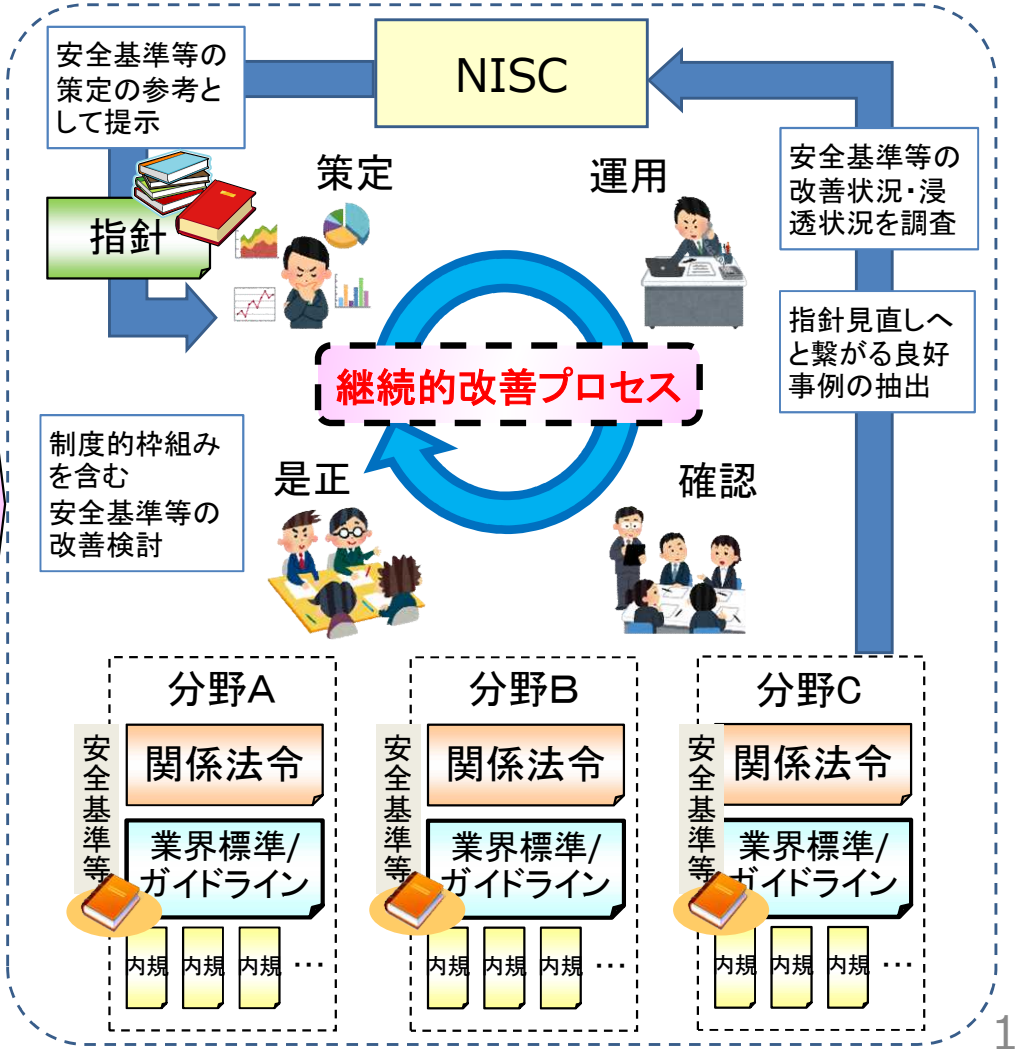
行動計画期間中の施策

（１） 指針の継続的改善
- 情報セキュリティ文化の醸成やPDCAサイクルの実行に責任を持つ経営層が認識すべき事項及び行動を指針改定時に詳細化
- 機能保証の考え方を踏まえた事業継続計画・コンティンジェンシープラン等の対処態勢整備の必要性を指針改定時に明記

（２） 安全基準等の継続的改善
- セキュリティ対策のPDCAサイクルに沿った業界標準/ガイドラインの改善プロセスの推進
- 情報セキュリティの取組の保安規制への位置付けや、関係法令等におけるサービス維持レベルの具体化等、制度的枠組みを含めた検討の実施

（３） 安全基準等の浸透
- 重要インフラ事業者等への毎年のアンケート調査により、セキュリティ対策状況を把握するとともに、アンケートへの回答を通じ、事業者等が対策の課題、解決策等を認識可能となるよう支援

第４次行動計画に基づく取組



第４次行動計画（案） 施策②：情報共有体制の強化

個々の重要インフラ事業者等が日々変化する情報セキュリティ動向に迅速に対応できるよう、官民間や分野内外間における情報共有の強化に取り組む。

現状の課題

- 情報共有を行う意義・必要性の訴求
- 迅速かつ効果的な情報共有体制の検討
- 共有すべき情報の理解・浸透・活性化
- 民間の自主的取組に関する普及・促進　　等

行動計画期間中の施策

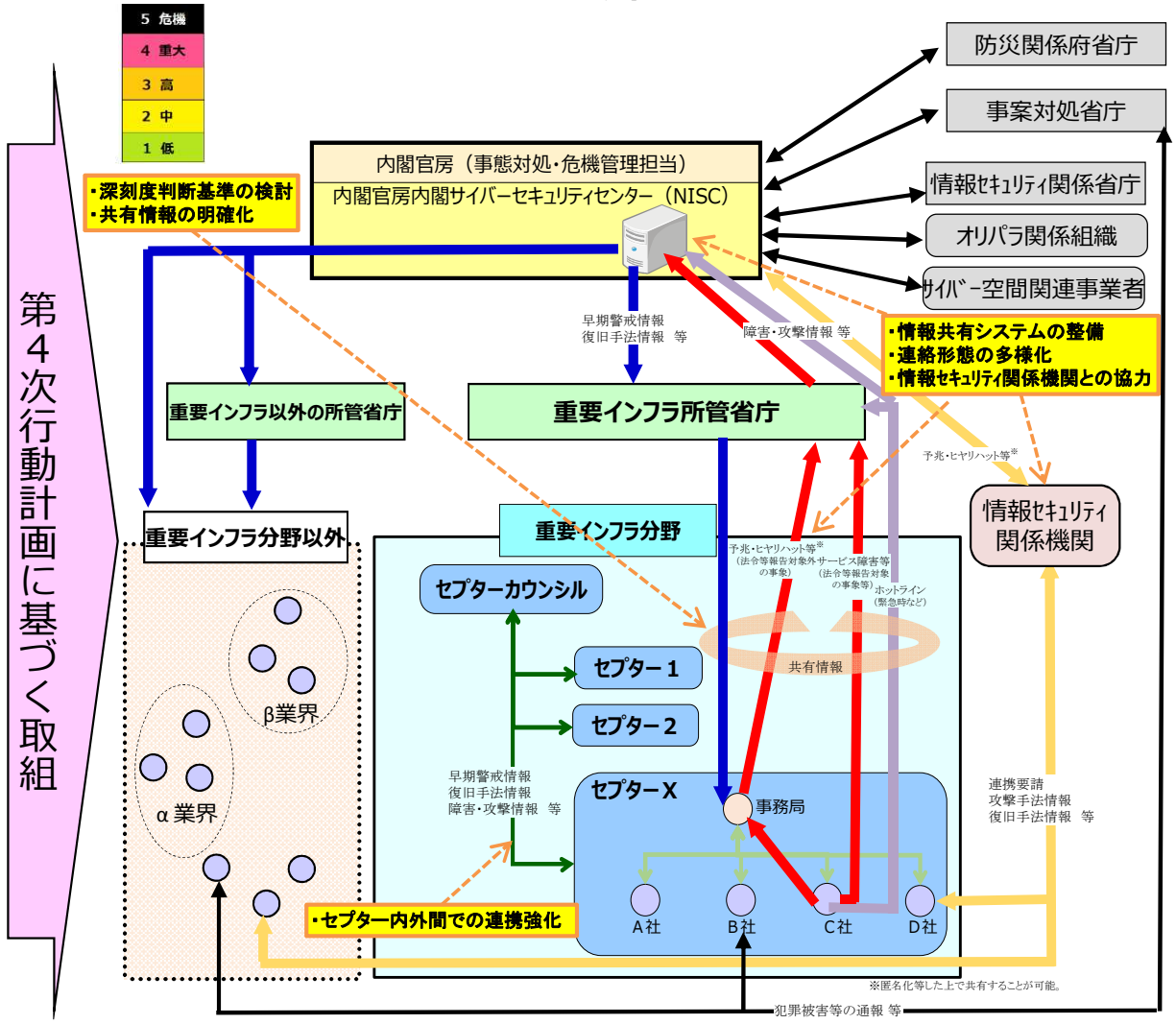
（１）情報共有体制の充実
- 新たな連絡形態(セプター事務局経由)の導入
- オリパラ大会等を見据えた情報共有システムの整備
- 情報セキュリティ関係機関との積極的な協力

（２）情報共有の更なる促進
- 重要インフラサービス障害の深刻度判断基準の検討
- 共有すべき情報の明確化※

※情報系だけでなく制御系やIoTシステムも対象となること等を明示

（３）民間活動の更なる活性化
- セプター内、セプター間の情報共有の更なる充実
- 先進的な取組を行うISAC等の活動の展開

【本行動計画期間で取り組む情報共有体制】



第４次行動計画（案） 施策③：障害対応体制の強化

重要インフラ事業者における重要インフラサービス障害対応の実態や演習ニーズに適合した演習・訓練の充実による重要インフラ防護能力の維持・向上。

現状の課題

- より効果的で実用的な分野横断的演習の企画推進
- 参加者拡大や、重要インフラサービス障害発生時の関係主体間の在り方に適合した演習成果の普及・浸透

行動計画期間中の施策

（１）分野横断的演習の継続と改善

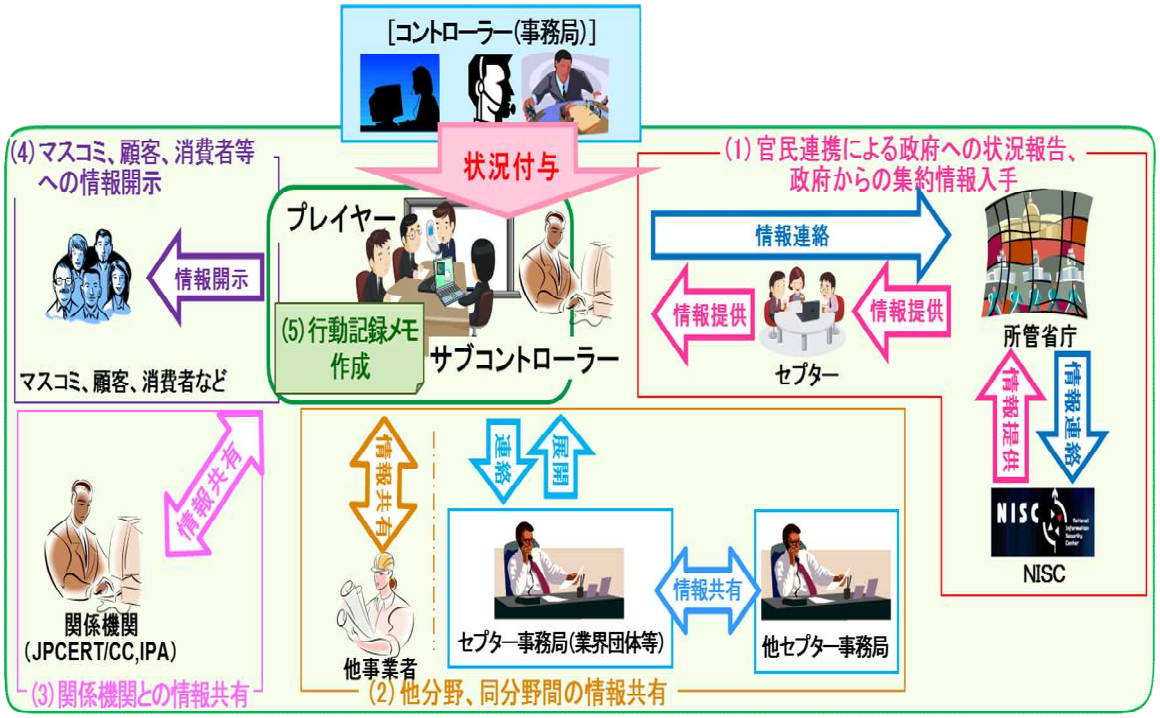
- 重要インフラ事業者の実態に即した演習企画
  - ・重要インフラ事業者の演習ニーズ取り込み
  - ・最新の攻撃手法を考慮した演習シナリオ整備
  - ・外縁の事業者や密接に関連する関係主体の参画

（２）参加者大幅増に即した演習成果の浸透

- 新規参加への促進
- 他演習・訓練との相互連携
- 経営理解増進に寄与する演習企画
- 自社演習実施に資する演習ノウハウの還元
  - ・仮想的な演習環境の提供　等

第４次行動計画に基づく取組

分野横断的演習の概要（ステークホルダー相関図）



分野横断的演習の継続と充実

- より実態に即した演習企画
- 外縁の事業者も含めた新規参加の促進
- 他演習・訓練との相互連携
- 経営理解増進に資する演習企画
- 演習ノウハウの還元

重要インフラ防護能力の維持・向上

第４次行動計画（案） 施策④：リスクマネジメント及び対処態勢の整備

重要インフラサービスの安全・持続的な提供に向けて、重要インフラ事業者等が実施するリスクマネジメント及びこれを踏まえた対処態勢整備を推進する。

現状の課題

- リスクアセスメントの重要性については認識が広まりつつあるが、その考え方や実施方法については十分に浸透していない。
- 重要インフラサービス障害が発生した際に備えた対処態勢整備の必要性が高まっているが、具体的な方向性・支援策等が示されていない。

行動計画期間中の施策

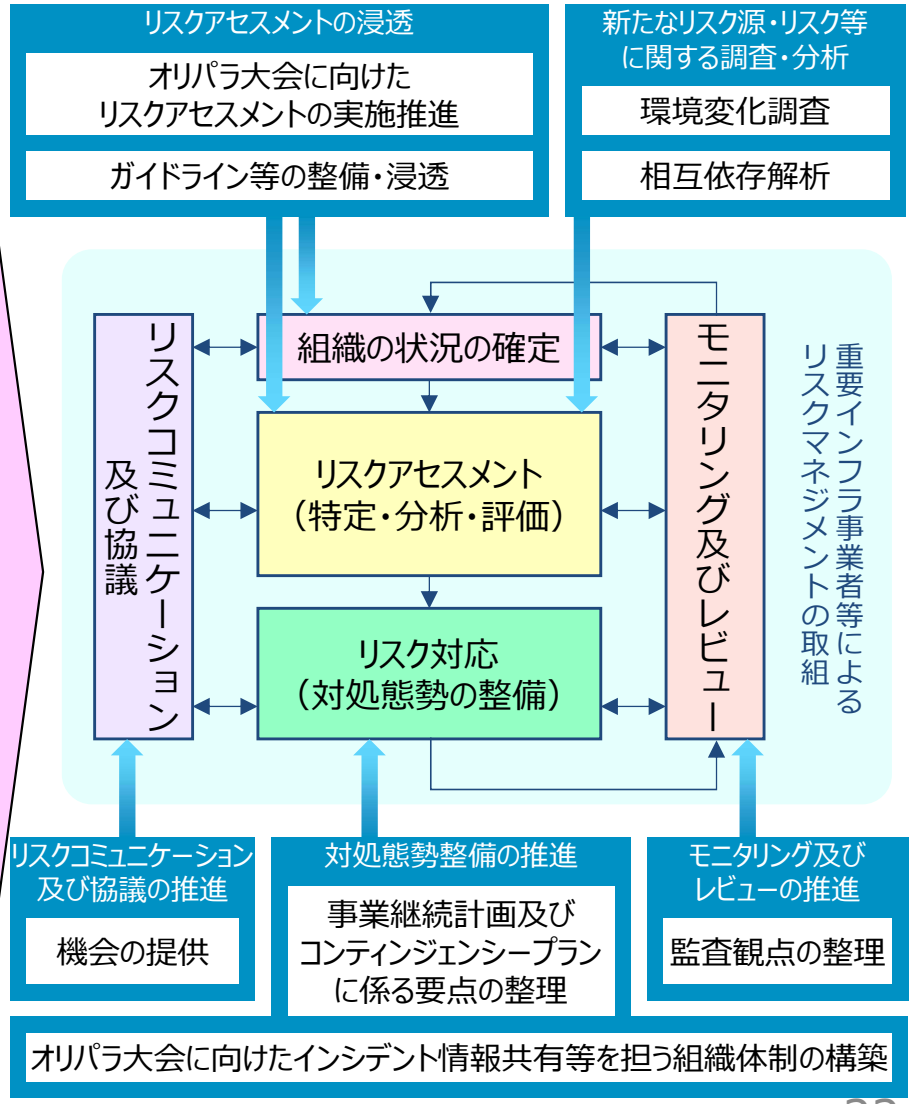
（１）リスクマネジメントの標準的な考え方

（２）リスクマネジメントの推進

- リスクアセスメントの浸透
  - ・オリパラ大会に向けたリスクアセスメントの実施推進
  - ・機能保証の考え方に立脚したリスクアセスメントガイドライン等の整備・浸透
- 新たなリスク源・リスク等に関する調査・分析
  - ・環境変化調査　・相互依存性解析
- 対処態勢整備の推進
  - ・機能保証の考え方を踏まえた事業継続計画及びコンティンジェンシープランの要点の整理
  - ・オリパラ大会に向けたインシデント情報共有等を担う組織体制の構築
- リスクコミュニケーション及び協議の推進
  - ・内部ステークホルダー間、関係主体間での情報・意見交換の機会の提供
- モニタリング及びレビューの推進
  - ・重要インフラ事業者等が自主的に行う内部監査等の監査観点の整理

（３）本施策と他施策との相互反映プロセスの確立

第４次行動計画に基づく取組



第４次行動計画（案） 施策⑤：防護基盤の強化

防護範囲の見直し、広報広聴、国際連携、規程類の整備、経営層への働きかけ、人材育成等、重要インフラ防護の全体を支える共通基盤的な取組を強化する。

現状の課題

- 環境変化を踏まえた面としての防護
- 広報広聴活動の一層の充実
- 国際的な情報セキュリティ対策水準の向上
- 情報セキュリティに関する経営層の意識向上
- 情報セキュリティ人材の質的・量的な充実

行動計画期間中の施策

（１）重要インフラに係る防護範囲の見直し
- 「面としての防護」に向けた取組、国の安全等の確保の観点からの取組

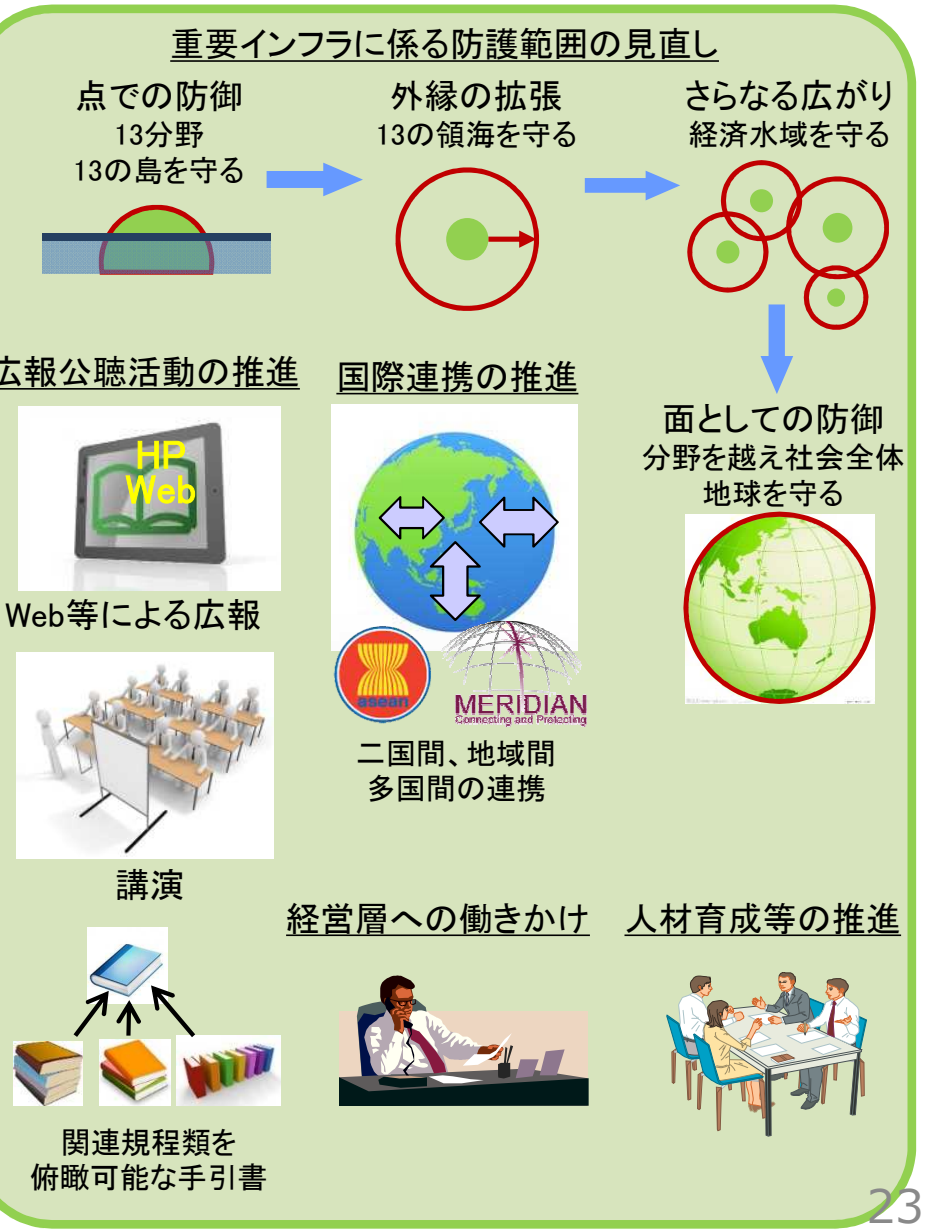
（２）広報広聴活動の推進
- 行動計画の枠組みや取組等の国民への積極的な発信

（３）国際連携の推進
- 国際的な情報セキュリティ対策の水準向上のための積極的な寄与

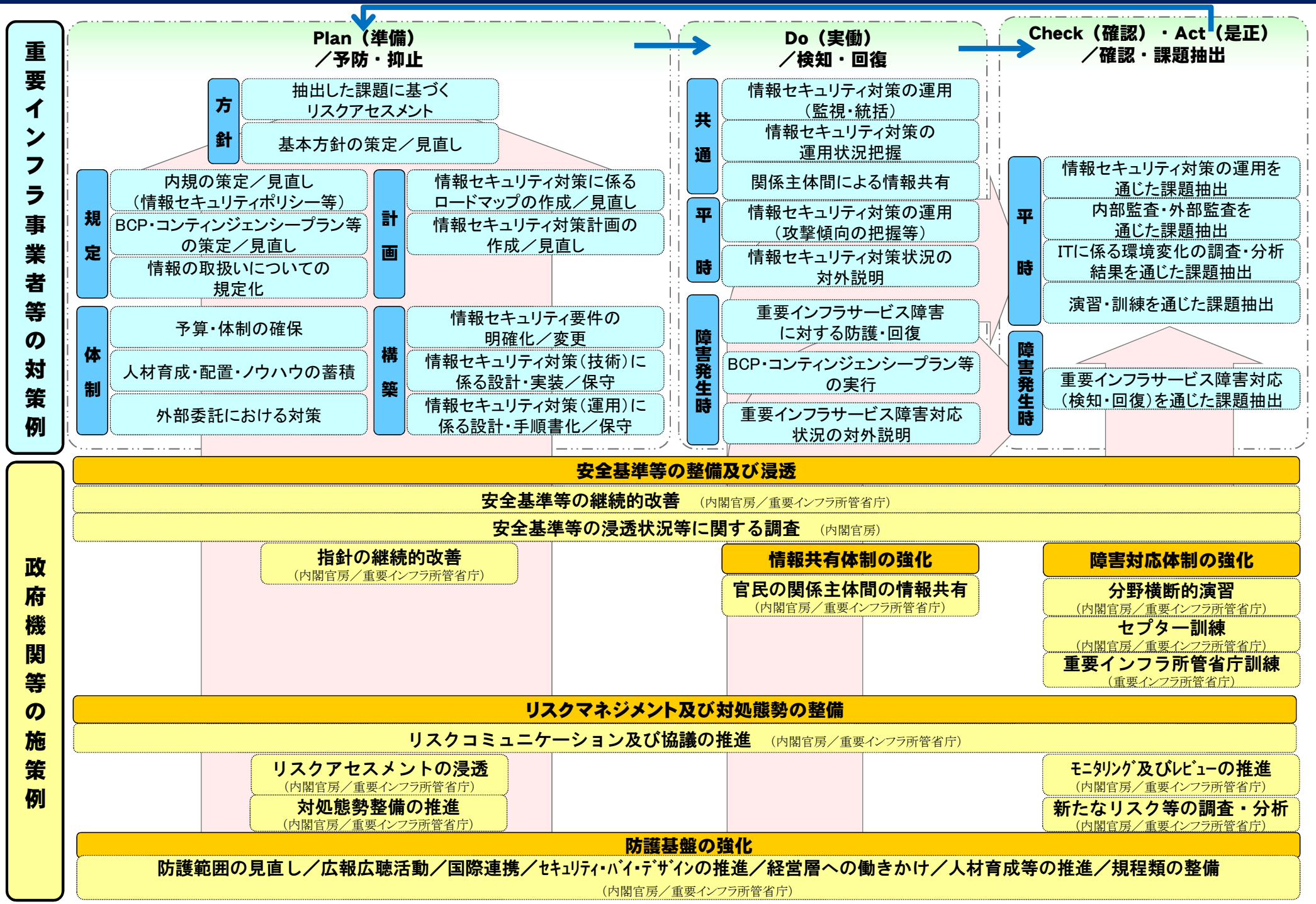
（４）経営層への働きかけ
- 情報セキュリティに関する意識向上のための経営層への働きかけ

（５）人材育成等の推進
- 橋渡し人材の育成、演習や教育の実施、人材交流の推進等

第４次行動計画に基づく取組



「重要インフラ事業者等による対策例」と各対策に関連する「政府機関等の施策例」



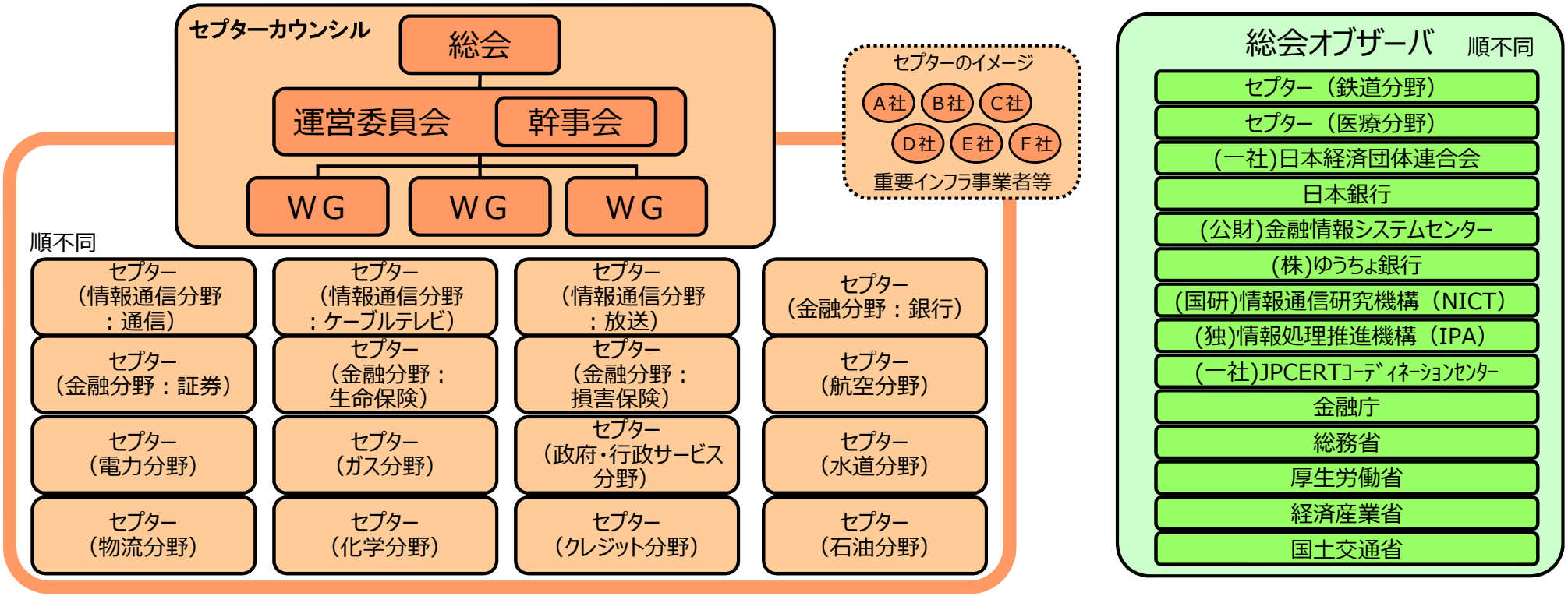
セプターとセプターカウンシル

セプター（ＣＥＰＴＯＡＲ）Capability for Engineering of Protection, Technical Operation, Analysis and Response

- 重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。
- 重要インフラサービス障害の未然防止、発生時の被害拡大防止・迅速な復旧および再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係者間で情報を共有。これによって、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資する活動を目指す。

セプターカウンシル

- 各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。
  政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
- 分野横断的な情報共有の推進を目的として、２００９年２月２６日に創設。



情報共有体制の強化・防護範囲の見直しに関する取組状況

2016年9月末日現在

■ セプターの拡充等

重要インフラ分野	情報通信			金融				航空	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	航空	鉄道	電力	ガス	政府・地方公共団体	医療	水道	物流	化学	クレジット	石油
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	金融CEPTOAR連絡協議会 銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR	航空分野におけるCEPTOAR	鉄道CEPTOAR	電力CEPTOAR	GAS CEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR	化学CEPTOAR	クレジットCEPTOAR	石油CEPTOAR
事務局	(一社)ICT-ISAC	(一社)日本ケーブルテレビ連盟	(一社)日本民間放送連盟	(一社)全国銀行協会 事務・決裁システム部	日本証券業協会 ＩＴ統括部	(一社)生命保険協会 総務部組織法務グループ	(一社)日本損害保険協会 ＩＴ推進部品質グループ	定期航空協会	(一社)日本鉄道電気技術協会	電気事業連合会 情報通信部	(一社)日本ガス協会 技術部	地方公共団体情報システム機構 情報化支援戦略部	厚生労働省 医政局 研究開発振興課 医療技術情報推進室	(公社)日本水道協会 総務部総務課	(一社)日本物流団体連合会	石油化学工業協会	(一社)日本クレジット協会	石油連盟
構成員（のべ数）	24社・団体	333社	194社 1団体	1,433社	260社 7機関	41社	29社（オブザーバ3社含む）	14社 1団体	22社 1団体	12社 2機関	10社	47 都道府県 1,741 市区町村	1グループ 6機関	8水道事業体	6団体 16社	13社	28社（10.1時点）	14社・グループ
2014年4月時点	28社・団体	252社	193社 1団体	1,411社	251社 7機関	43社	30社（オブザーバ3社含む）	2ｸﾞﾙｰﾌﾟ 3機関	22社 1団体 1機関	12社 2機関	10社	47 都道府県 1,742 市区町村	1グループ 2機関	8水道事業体	6団体 16社	—	—	—
NISCからの情報の展開先（構成員以外）	399社・団体										38社		375社・機関	内容に応じ1,361事業体へ展開				
	その他（核物質関連事業所等（内容に応じ展開先を選定）、ビルディング・オートメーション協会、サイバーディフェンス連携協議会、大学等（内容に応じ展開先を選定））																	
事務局の民間移行	航空分野（国土交通省航空局 → 定期航空協会）、鉄道分野（国土交通省鉄道局 →（一社）日本鉄道電気技術協会）																	

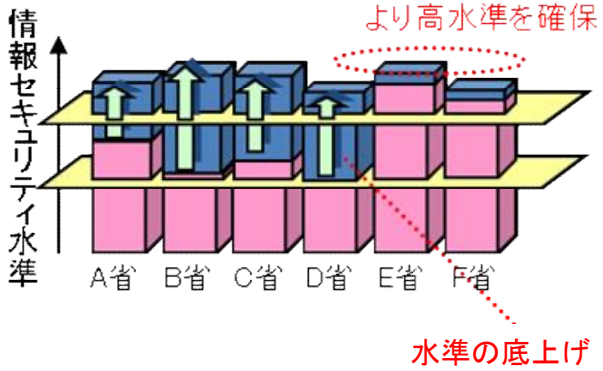
■ その他

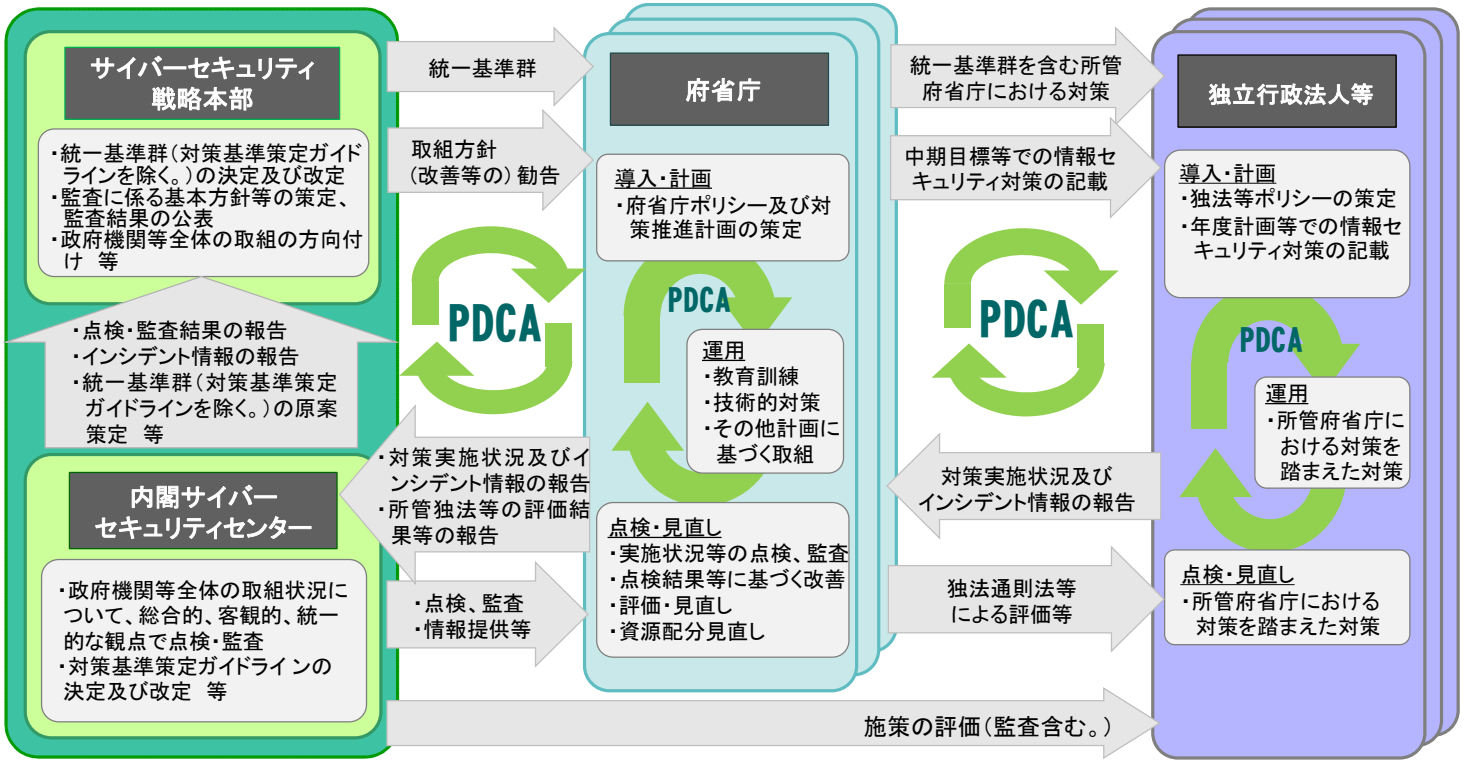
既存事業領域を越える連携等	情報通信（Telecom-ISACの活動を新たに設立されたICT-ISACに移行し一部の放送事業者が加盟）、電力（ISAC設立を模索）、化学（石油化学工業協会と日本化学工業協会の情報共有・活動連携）、クレジット（ネットワーク事業者への拡張）、制御システム（JPCERT/CCが提供するConPaS等） J-CSIP（IPA：標的型攻撃等に関する情報共有）、サイバーテロ対策協議会（重要インフラ事業者等と警察との間で連携、47都道府県に設置）、早期警戒情報WAISE（JPCERT/CC: 情報セキュリティに係る情報全般）

（※）本頁は、2016年9月時点の状況を示すものであり、セプターの構成員に関する情報は、定期的（２回/年）に更新し、内閣ｻｲﾊﾞｰｾｷｭﾘﾃｨｾﾝﾀｰのＨＰ（http://www.nisc.go.jp/）に掲載。

政府機関等の情報セキュリティ対策のための統一基準群

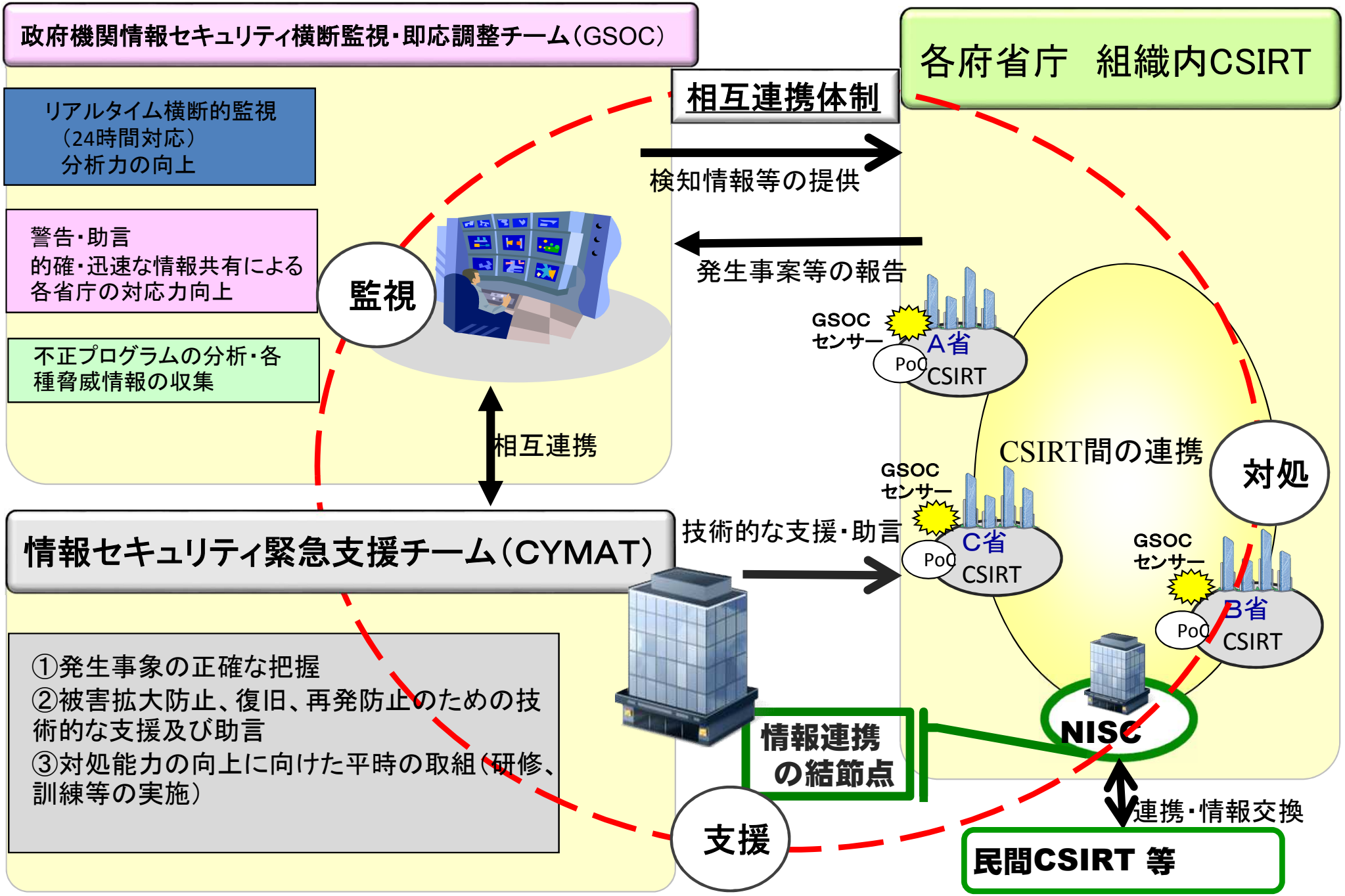
- 政府機関等の情報セキュリティ対策のための統一基準群（以下「統一基準群」という。）は、政府機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組み。
- 統一基準群では、府省庁及び独立行政法人等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定している。
- 統一基準群の運用により、個々の組織のPDCAサイクルや政府機関等全体のPDCAサイクルを適切に回し、政府機関等全体としての情報セキュリティを確保する。





※平成28年度版統一基準群案の決定（次回戦略本部で決定予定）を前提として記載

政府機関における情報集約・支援体制の枠組み



サイバーセキュリティに関する研究開発

達成目標

戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」
H27（2015）年度～H31（2019）年度（予定）、H27年度予算：5億円

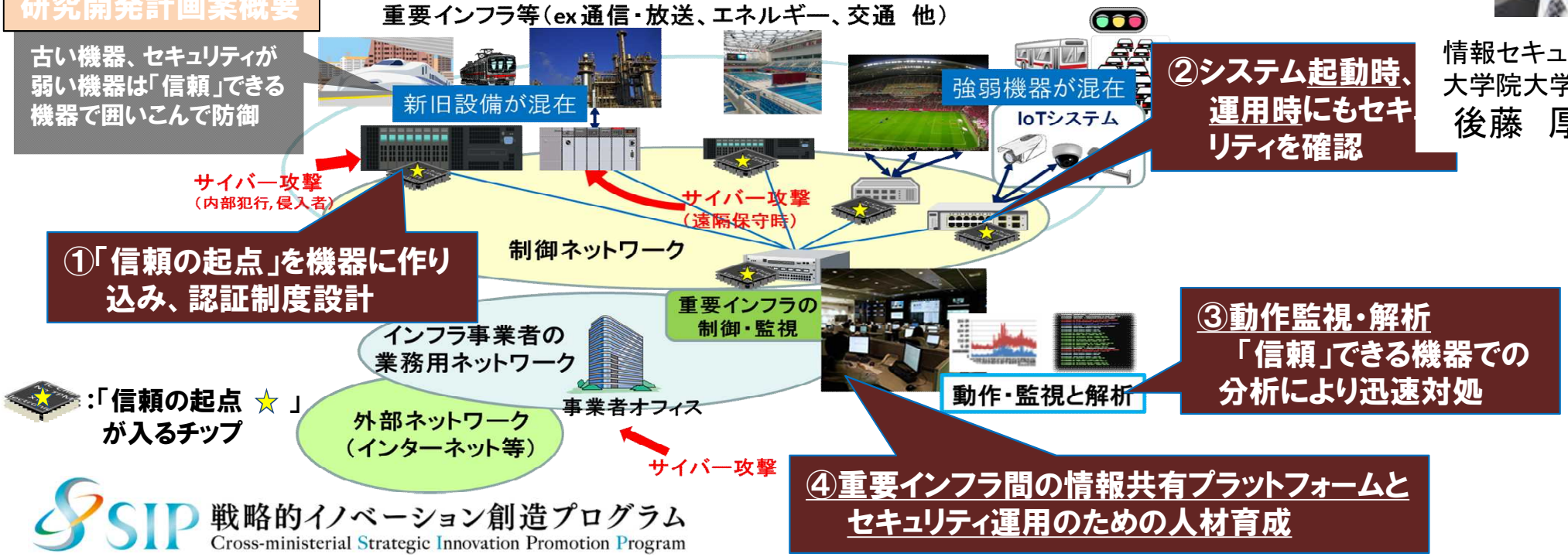
- **悪意のある機能を“持ち込ませない”、悪意のある動作を“いち早く発見する” システムの実現**
- **国産セキュリティ技術を確立。重要インフラ産業の競争力強化、安全な社会基盤実現に貢献**

⇒ **2020年五輪大会の安心安全な開催**

PD

情報セキュリティ大学院大学教授
後藤　厚宏

研究開発計画案概要



SIP 戦略的イノベーション創造プログラム
Cross-ministerial Strategic Innovation Promotion Program

- **また、安全なIoTシステムの創出、我が国製品の海外展開を念頭に置いたIoTセキュリティの国際標準化も行う予定**

2020年東京オリンピック・パラリンピック競技大会に向けた取組

2020年東京オリンピック・パラリンピック競技大会（以降、大会）を成功へと導くためには、大会の開催・運営を支える重要サービスにおけるサイバーセキュリティを確保し、安定したサービスを供給することが不可欠との認識の下、関係機関と連携し取組を検討。

【検討体制】

東京オリンピック競技大会・東京パラリンピック競技大会推進本部
（本部長：安倍総理）

2020年オリンピック・パラリンピック東京大会関係府省庁連絡会議
（議長：杉田副長官）

セキュリティ幹事会

座長	– 内閣危機管理監
座長代理	– 内閣官房オリパラ事務局長、内閣官房副長官補（内政）、内閣官房副長官補（事態対処・危機管理）、警察庁次長
構成員	– 関係省庁の局長級
オブザーバー	– 東京都、組織委、警視庁、東京消防庁の幹部
事務局	– 警察庁、総務省、外務省、経産省、国交省、防衛省の協力を得て内閣官房（内政・事態・NISC）において処理

テロ対策ＷＴ

座長	– 内閣審議官（事態・内政）
座長代理	– 内閣審議官（オリパラ事務局） 警察庁審議官
構成員	– 関係省庁の課長級
オブザーバー	– 関係機関の幹部
事務局	– 警察庁、国交省、防衛省の協力を得て内閣官房（事態・内政）において処理

サイバーセキュリティＷＴ

座長	– 内閣審議官（NISC副センター長）
座長代理	– 内閣審議官（オリパラ事務局） 警察庁審議官
構成員	– 関係省庁の課長級
オブザーバー	– 関係機関の幹部
事務局	– 警察庁、総務省、外務省、経産省、防衛省の協力を得て内閣官房（NISC）において処理

2020年東京オリンピック・パラリンピック競技大会における
サイバーセキュリティ体制に関する検討会

【大会の開催・運営を支える重要サービスのイメージ】