資料9

サイバーセキュリティ対策の強化に向けた対応について
（追加説明資料）

2016年11月9日
内閣官房内閣サイバーセキュリティセンター（NISC）

0．サイバーセキュリティ政策の概要

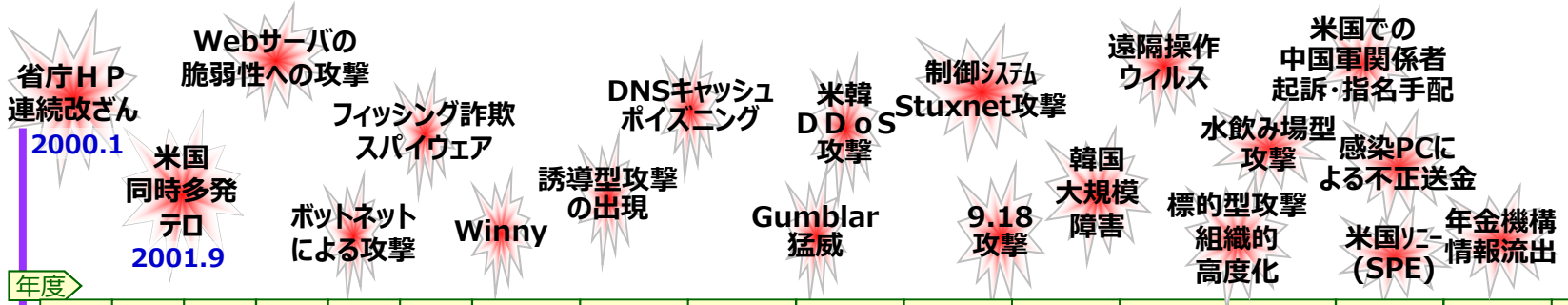
1．重要インフラ防護

2．安全なIoTシステムの創出

3．セキュリティ人材の育成

4．参考資料

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

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

参考：IT利活用

- 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)

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)
- ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略 (2013.6.10 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)

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基本法の概要

2015.1.9施行、2016.10.21一部改正法施行

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政策の推進体制

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

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

※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

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

新たな「サイバーセキュリティ戦略」について（全体構成）

2015年9月4日閣議決定

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

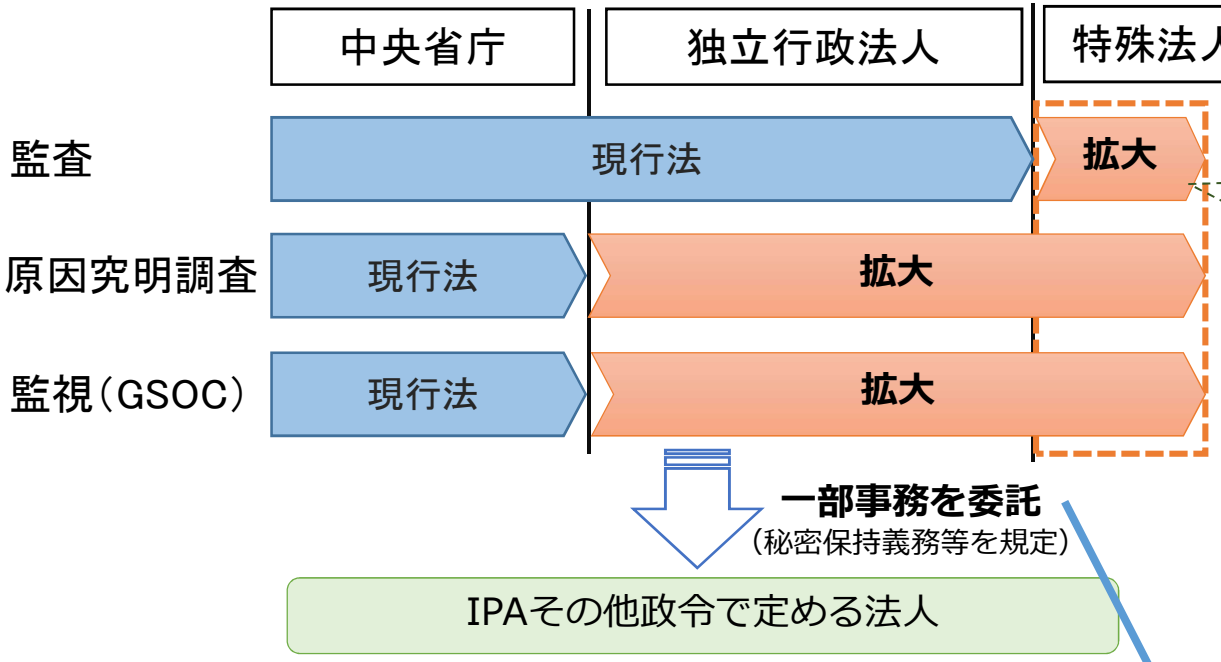
- **研究開発の推進**
  攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発
- **人材の育成・確保**
  ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

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

サイバーセキュリティ基本法の改正法の施行（2016年4月15日成立、4月22日公布、10月21日施行）

■ 国が行う不正な通信の監視、監査、原因究明調査等の対象範囲を拡大
■ サイバーセキュリティ戦略本部の一部事務を独立行政法人情報処理推進機構（IPA）に委託



監視、監査、原因究明調査等の対象となる法人の指定（本部決定）

- ✓ 日本年金機構等の公的年金関係法人（※）及び地方公共団体情報システム機構（J-LIS）を指定。（9法人）

※ 日本年金機構、国家公務員共済組合連合会（KKR）、地方公務員共済組合連合会、地方職員共済組合、都職員共済組合、全国市町村職員共済組合連合会、日本私立学校振興・共済事業団、公立学校共済組合

- ✓ IPAへの委託は「サイバーセキュリティ対策を強化するための監査に係る基本方針」「サイバーセキュリティ戦略本部重大事象施策評価規則」を踏まえて実施

情報処理安全確保支援士制度の開始に伴う規定の整備（情報処理の促進に関する法律の一部改正に伴う政省令の整備）

その他法改正に伴い整備する規則等（本部決定）

- ✓ 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（※前回戦略本部で改定済）
- ✓ サイバーセキュリティ対策を強化するための監査に係る基本方針
- ✓ サイバーセキュリティ戦略本部重大事象施策評価規則
- ✓ サイバーセキュリティ戦略本部資料提供等規則

0．サイバーセキュリティ政策の概要

1．重要インフラ防護

2．安全なIoTシステムの創出

3．セキュリティ人材の育成

4．参考資料

重要インフラ防護のための取組①（現状）

■ 重要インフラ事業者等に対するサイバーセキュリティ対策は、サイバーセキュリティ基本法の規定に基づき、取組を推進。

○サイバーセキュリティ基本法（平成26年法律第104号）

第6条　重要社会基盤事業者は、基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

第14条　国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。

■ 具体的な取組は、「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（※１）」に基づき実施。

※1　2014.5.19 情報セキュリティ政策会議決定、2015.5.25サイバーセキュリティ戦略本部改訂

①　重要インフラの範囲（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（地方公共団体を含む）、医療、水道、物流、化学、クレジット及び石油（それぞれの分野において、サービスの持続的な提供に支障が生じた場合(サイバー攻撃による場合を含む)には、基本的には関係法令により、所管省庁への報告義務がある。）

②　第３次行動計画に基づく施策

- 安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント及び防護基盤の強化
- 情報共有体制については、平時・大規模IT障害対応時それぞれについて、関係省庁や重要インフラ事業者における対応を整理。各分野内、分野間において、内閣官房（NISC）が中心となり、情報共有を図っている。
- 本行動計画に基づき、重要インフラ事業者等が参加する分野横断的演習を実施し、対応能力の向上を図っている。（2015年度は302組織・1168名が参加）
- 重要インフラ事業者は行動計画を踏まえ、自主的な取組の一環として、情報共有・分析機能及び当該機能を担う組織（※２）及びその代表で構成される協議会(セプターカウンシル)を運営し、情報共有を実施。
- 一部の分野では、分野内における情報共有・連携を促進するための組織(ISAC（Information Sharing and Analysis Center）)を設立し、取組の強化を図っている（金融、ICT分野）。

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

重要インフラの情報セキュリティ対策

官民連携による重要インフラ防護の推進

重要インフラにおけるサービスの持続的な提供を行い、
自然災害やサイバー攻撃等に起因するＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、
ＩＴ障害の発生を可能な限り減らすとともにＩＴ障害発生時の迅速な復旧を図ることで重要インフラを防護する

重要インフラ（１３分野）

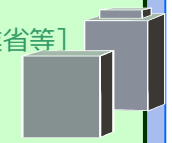
- 情報通信
- 金融
- 航空
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油

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/CC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３次行動計画

H26.5.19 情報ｾｷｭﾘﾃｨ政策会議 決定
H27.5.25 ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略本部改訂

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

ＩＴ障害関係情報の共有による、官民の関係者全体での平時・大規模IT障害発生時における連携・対応体制の強化

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ＩＴ障害対応体制の総合的な強化

リスクマネジメント

重要インフラ事業者等におけるリスク評価を含む包括的なマネジメントの支援

防護基盤の強化

広報公聴活動、国際連携の強化、規格・標準及び参照すべき規程類の整理・活用・国際展開

重要インフラ防護のための取組②（諸外国の状況）

■ 情報共有のための枠組は、脅威情報まで含めた共有を目指し、自主的な取組のインセンティブを目指すもの（アメリカ）と、インシデント発生時における情報共有を主とするもの（欧州）がある。

アメリカ	◆ サイバーセキュリティ法（Cybersecurity Act of 2015） • サイバーセキュリティ脅威情報の官民共有の手続の整備 • 民間主体等について、情報共有に伴う法的責任を免除
ＥＵ	◆ ネットワーク及び情報セキュリティ（NIS）指令（2016） • 加盟国は、重要なサービス提供事業者において深刻なインシデントが発生した場合には、当該事業者が遅滞なく監督官庁への通知を行うための措置を講じること
ドイツ	◆ ITセキュリティ法（2015） • 重要インフラ事業者は、ITシステムに関する重大なインシデントが発生した場合には、情報セキュリティ庁（BSI）に報告する義務を負う。
フランス	◆ フランス国防法典（2013） • 重要インフラ事業者は、インシデント発生時において国家情報システム・セキュリティ庁（ANSSI）に報告する義務を負う。
イギリス	• 情報共有の在り方について政府と業界で検討中

■ 重要インフラの対象分野は、各国の事情により差異。

アメリカ	化学、商業施設、通信、重要製造業、ダム、防衛産業基盤、緊急対応サービス、エネルギー、金融、食料・農業、政府施設、ヘルスケア・公衆衛生、情報技術、原子炉・核物質・核廃棄物、輸送システム、水・排水システム（16分野）
ＥＵ	エネルギー、交通・輸送、銀行、金融、医療、水、デジタルサービス（7分野）
ドイツ	エネルギー、ICT、水、食料、医療、金融、交通、メディア、行政サービス（9分野）
フランス	食糧、医療、水、通信・放送、宇宙、産業、エネルギー、交通、金融、行政、軍事、司法（12分野）
イギリス	通信、緊急サービス、エネルギー、金融サービス、食糧、政府、医療、交通、防衛、原子力、宇宙、化学（13分野）

重要インフラ防護のための取組③（今後の方向性）

- 現行の行動計画は策定後3年に1度見直す必要があるとされており（＝2016年度末まで）、現在見直しに向けた検討を実施中。
- 見直しに当たっては、2020年東京オリンピック・パラリンピック競技大会を見据え、重要インフラ防護の強化を図る必要。

行動計画見直しの方向性

① 重要インフラの範囲

- 重要インフラの対象分野については、諸外国の枠組も踏まえ、国民の安全や知的財産の保護等、防護対象として情報共有等を推進すべき分野についての取組強化を行う。

② 重要インフラ防護のための取組（特に情報共有について）

- 重要インフラサービスの安全かつ持続的に提供（機能保証）という目的を達成するために、最適な情報共有の枠組みを構築。
- 24時間365日、官民間、民民間及び関係省庁間における安全・迅速な情報共有や情報の収集・分析を可能とするシステムの整備（緊急時等におけるホットラインの構築を含む）
- 事案の深刻度のレベル分けや、予兆脅威情報を含む共有すべき情報の明確化

［今後の予定］
✓ 行動計画の見直し（案）を策定・公表（2016年中）、2016年度末までに結論

「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」の見直しのポイント

１．行動計画の目的

重要インフラサービスは、安全かつ持続的に提供（機能保証）することが求められることから、自然災害やサイバー攻撃等に起因するＩＴ障害とそれによるサービス障害の発生を可能な限り減らすとともに、発生時の迅速な復旧が可能となるよう、関係主体において経営層の積極的な関与の下、情報セキュリティに関する取組を推進する。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っていく。

２．重要インフラを取り巻く現状と課題

◆ 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。

◆ サービスの安全かつ持続的な提供のため、情報系(ＩＴ)だけではなく、制御系(ＯＴ)を含めた情報共有の質・量の改善等が必要。

◆ 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．行動計画の見直しの３つの重点

次の3つを重点として行動計画に基づく5つの施策群の取組の深化を図る。

①　先導的取組の推進(クラス分け)

重要インフラ分野が依存し、短時間のＩＴ障害でも影響が大きくなるおそれがある分野(例：電力、通信、金融)において、一部事業者による先導的な取組を進めるとともに、他の事業者、さらには他の分野にも波及させることにより、重要インフラ全体の機能保証の確保を図る。

②　オリパラ大会を見据えた情報共有体制の強化

連絡形態の多様化、事案の深刻度のレベル分け、情報共有システムの整備、情報提供の拡大等により、情報共有を促進するとともに、重要インフラ内外の共有範囲の拡充、制御系を意識した情報共有等を図る。また、演習等の継続・改善等により、障害対応体制の強化を図る。

③　リスクマネジメントを踏まえた対処態勢整備の推進

重要インフラサービスの安全・継続的な提供のため、重要インフラ事業者等へのリスクマネジメントの更なる浸透や、CSIRTやコンティンジェンシープランの整備等を含む対処態勢の整備の推進図る。

行動計画に基づく５つの施策群

安全基準等の整備・浸透

情報共有体制の強化

障害対応体制の強化

リスクマネジメント

防護基盤の強化

４．行動計画の見直しに向けた今後のスケジュール

➢　平成28年中に行動計画の見直し（案）を策定・公表、平成29年3月までに結論を得る。

0．サイバーセキュリティ政策の概要

1．重要インフラ防護

2．安全なIoTシステムの創出

3．セキュリティ人材の育成

4．参考資料

安全なIoTシステムの創出（現状・諸外国の取組等）

■ IoT（Internet of Things）の普及により、新たなサイバーセキュリティ上の課題への対処が必要。

IoTは、
① サイバー空間が物理空間に影響を及ぼすため、安全性の問題が生じる（例：自動車の制御システムのハッキング）
② 各機器のコンピューター性能などの問題によりセキュリティを実装しにくい場合がある
③ 機器の数が多いため、ボット化してしまうとサイバー空間上に悪影響を及ぼす（例：IoTに感染するマルウェアによる大手サービスへの攻撃）
など、新たな課題があり、機器の持つ機能そのものを確保しつつ対処していく必要がある。

■ 他方、安全なIoTシステムの創出のための取組については、各国とも取組が始まったところ。

日本

◆ IoTの一般的枠組み（2016.8）
- サイバーセキュリティ戦略を踏まえ、セキュリティ・バイ・デザインの思想でIoTシステムを設計・構築・運用。
- 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。

◆ IoTセキュリティガイドライン（2016.7）
- 新たなIoTセキュリティ上の脅威を踏まえ、IoT機器やシステム、サービスの提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）における指針を定めるとともに、一般利用者のためのルールを定めたもの。

アメリカ

◆ IIC（Industrial Internet Consortium）がIoTシステムへのセキュリティを組み込むためのフレームワークを策定中。（2015.9～）

◆ GSMA（移動体通信事業者の国際的業界団体）が、IoTの脅威と対策方法に関するガイドライン策定（2016.2）

◆ 米国商務省傘下のNISTがCPSフレームワークを策定。任務保証の考え方に基づき、IoTのシステムのサービス品質を確保するための基本的な考え方と考慮すべき重要なポイントを提示。（2016.5）

◆ NTIAがIoT の利益・課題・政府の役割についてパブリックコメントを実施（2016.4）し、様々な主体が意見を提出。（2016.8に意見募集結果を公表）

ドイツ

◆ 連邦経済エネルギー省（BMWi）が、インダストリー4.0におけるITセキュリティのガイドラインを策定。
- セキュリティ管理者の任命や訓練、ネットワークアクセスポイントのセキュリティ、USBメモリの使用ルール策定、ソフトウェアのアップデートなどの必要性等を列挙。

✓ 我が国が国内外において先導的な取組を行うことで、国際競争力向上につなげていく必要
✓ また、その前提として、考え方や用語などに関して、様々な分野の共通基盤を創ることが必要

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"**）

個別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** | **・・・**

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。

0．サイバーセキュリティ政策の概要

1．重要インフラ防護

2．安全なIoTシステムの創出

3．セキュリティ人材の育成

4．参考資料

諸外国のサイバーセキュリティ政策の動向（人材育成）

■ 「サイバーセキュリティ人材育成総合強化方針」（2016.3）において、民間分野・政府機関双方を対象とする包括的なセキュリティ人材育成のための方針を策定。

- セキュリティ対策は、やむを得ない「費用」ではなく、より積極的な経営への「投資」であるべきとの認識の下、経営戦略と実務者層の間で総合的に調整ができる橋渡し人材の育成を推進。
- 人材の需要（雇用）と供給（教育）の好循環を形成することが必要。
- その際、サイバーセキュリティの素養が様々な層の人材に必須のものとなりつつあることを踏まえ、必要となる人材像を具体化した上で、それに求められる育成施策を検討。

■ 各国とも、民間・政府機関を問わず、サイバーセキュリティ分野における人材育成が急務

アメリカ

◆ 連邦サイバーセキュリティ人材戦略を公表（2016.7）

- 連邦機関におけるサイバーセキュリティ・IT人材不足が防御能力向上の障害となっている一方、現在の施策の履行状況が十分でないという課題に対処するため、4 つの主たるイニシアティブを策定
  - ① 国家サイバーセキュリティ人材フレームワークを使用し、人材のニーズを特定
  - ② 教育・訓練による人材の増強（2017年度予算では6,200万ドルを投資）
  - ③ 多様な人材の採用の促進
  - ④ キャリアパスを構築し、高度なスキルを有する人材の維持・促進
- サイバーセキュリティ・IT人材の採用：2016年度上半期・3,000名、2017年1月まで・3,500名（予定）

EU

◆ EU指令（2016.7）

- EU加盟国に対し、ネットワーク及び情報システムのセキュリティに関する国家戦略を定め、その中で、教育・普及啓発・人材育成に関する施策を含めることを要求。

◆ 人材の需要面では、IoTなどITの利活用が事業全体に拡がる中、事業の「セキュリティ品質」を高め、国際競争力を強化していくためには、従来型の業務系システムのための情報セキュリティエンジニアの育成だけでなく、セキュリティに対して高い意識を持つ経営層の下、様々な専門の実務者がチームでセキュリティの問題を解決できる体制と人材育成が必要。供給面では、人材像の明確化、教育・演習の充実、能力の可視化を推進する。

◆ 政府機関においても、体制整備、キャリアパスの構築等について、各省庁が具体的な取組方策を定め、フォローアップを実施。

（今後の予定）

- ✓ 人材育成プログラムの策定（2016年度中）
- ✓ 各府省庁セキュリティ・IT人材確保・育成計画のフォローアップ・見直し等（2016年度末）

社会で活躍できる人材の育成

人材育成施策について

- 「「日本再興戦略」改訂2015」（平成27年６月閣議決定）、「サイバーセキュリティ戦略」（平成27年９月閣議決定）等を踏まえ、本年3月にサイバーセキュリティ分野の人材育成の具体的な強化方針（サイバーセキュリティ人材育成総合強化方針）を策定。
  - 参考1「日本再興戦略」改訂2015 抜粋
    - ・人材育成に係る施策を総合的に推進するため、本年度中に「サイバーセキュリティ人材育成総合強化方針（仮称）」を策定する。
  - 参考2　サイバーセキュリティ戦略抜粋
    - ・人材育成に係る施策を総合的かつ強力に推進するための方針を策定する。
- 現在、将来の社会・経済やITの利活用の進化を見据えたサイバーセキュリティ人材育成の課題の整理をしつつ、普及啓発・人材育成専門調査会での審議を通じ、人材育成プログラムの策定に向けて検討中。（今年度中に策定予定）

人材育成の基本的考え方

○人材の需要と供給の好循環を形成

人材の需要面（雇用）

適切な認識の下で、雇用・キャリアパスを確保
－経営戦略上の「投資」
－サイバー攻撃への対処の必要性

- 経営層 ○「経営層」のリーダーシップ
- 橋渡し人材層 ○組織内の関係部局間の総合調整や実務者層をまとめリード
- 実務者層 ○情報部門にとどまらず、事業部門、法務部門、工場など**セキュリティの範囲の広がり**

人材の供給面

人材育成の循環システム
－確かな知識と実践力の下に、
様々な業務経験を経て、人材を育成

- 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）等

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

「各府省庁セキュリティ・IT人材確保・育成計画」の作成状況等について
～政府機関におけるセキュリティ・ＩＴ人材の育成～

総合強化方針

◎政府機関におけるセキュリティ・ＩＴ人材育成総合強化方針
（平成28年3月　サイバーセキュリティ戦略本部決定※）
（平成28年3月　サイバーセキュリティ対策推進会議・各府省情報化統括責任者(CIO)連絡会議）

≪一部抜粋≫
１．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、組織規模や所管するシステム等の実情を踏まえつつ、人材の着実な確保・育成を図るため、速やかに、**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）」を作成し、各府省庁のサイバーセキュリティ・情報化審議官等で構成する会議において共有の上、フォローアップを実施する。**

（※）サイバーセキュリティ人材育成総合強化方針の第2章として

作成状況

・8月31日までに、対象の全府省庁において作成。
・9月8日　「副CISO等連絡会議/副CIO連絡会議合同会議」において各省計画を共有。

各省計画の内容

①体制の整備
　各府省においては、統括部局のセキュリティ部門を中心に、必要な強化を図るため、一定数の増員要求がなされ、審議官などの機構要求も含め、本省全体で約100人の要求が行われている。

②人材の拡充
　それぞれの府省の業務面の必要性や人材の脆弱性を踏まえた拡充方針を示している。

③有為な人材の確保
　府省の規模やシステム数等に応じ、素養や関心も踏まえ、相応の人材を確保する。

④セキュリティ・IT人材育成支援プログラム
　総務省等の研修に橋渡し人材の規模に応じて相応の人数を参加させる。（29年度府省全体で約2000名が行政管理局が行う情報システム統一研修を受講予定。）
　半数を超える府省では、府省の実情を踏まえた独自の研修も実施する。
　NISC、総務省行政管理局、個人情報保護委員会事務局等へ一定数の人材を出向させる。

⑤人事ルート例（キャリアパスのイメージ）
　具体的な部署・ポスト、出向先、研修内容等を勤務年数に応じて明記したキャリアパスを提示している。

⑥一般職員の情報リテラシー向上
　全職員、新採職員等を対象とした各種の研修を実施する。

今後

・今年度末　「副CISO等連絡会議/副CIO連絡会議合同会議」において、各省計画のフォローアップ、見直し等。

0．サイバーセキュリティ政策の概要

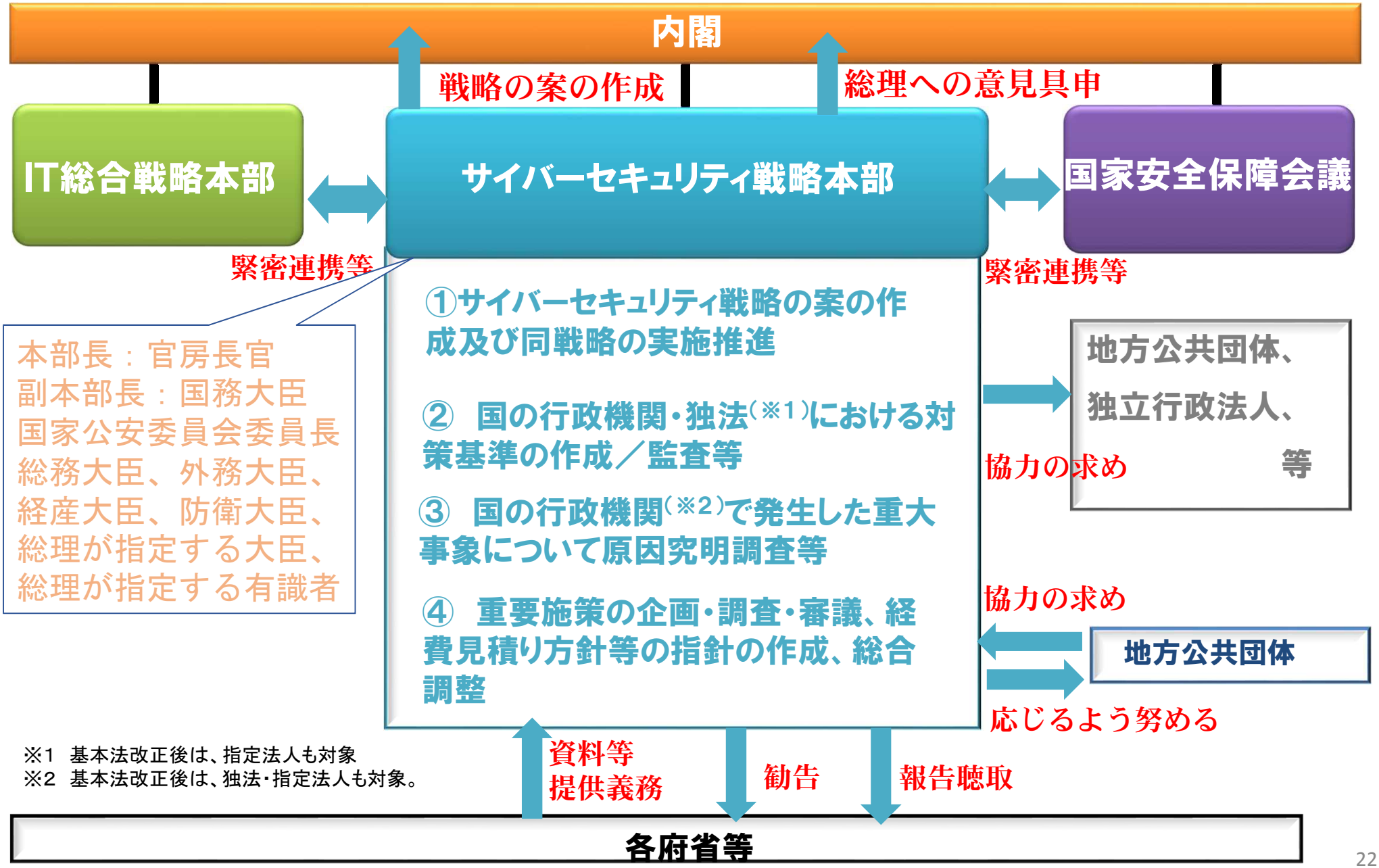
1．重要インフラ防護

2．安全なIoTシステムの創出

3．セキュリティ人材の育成

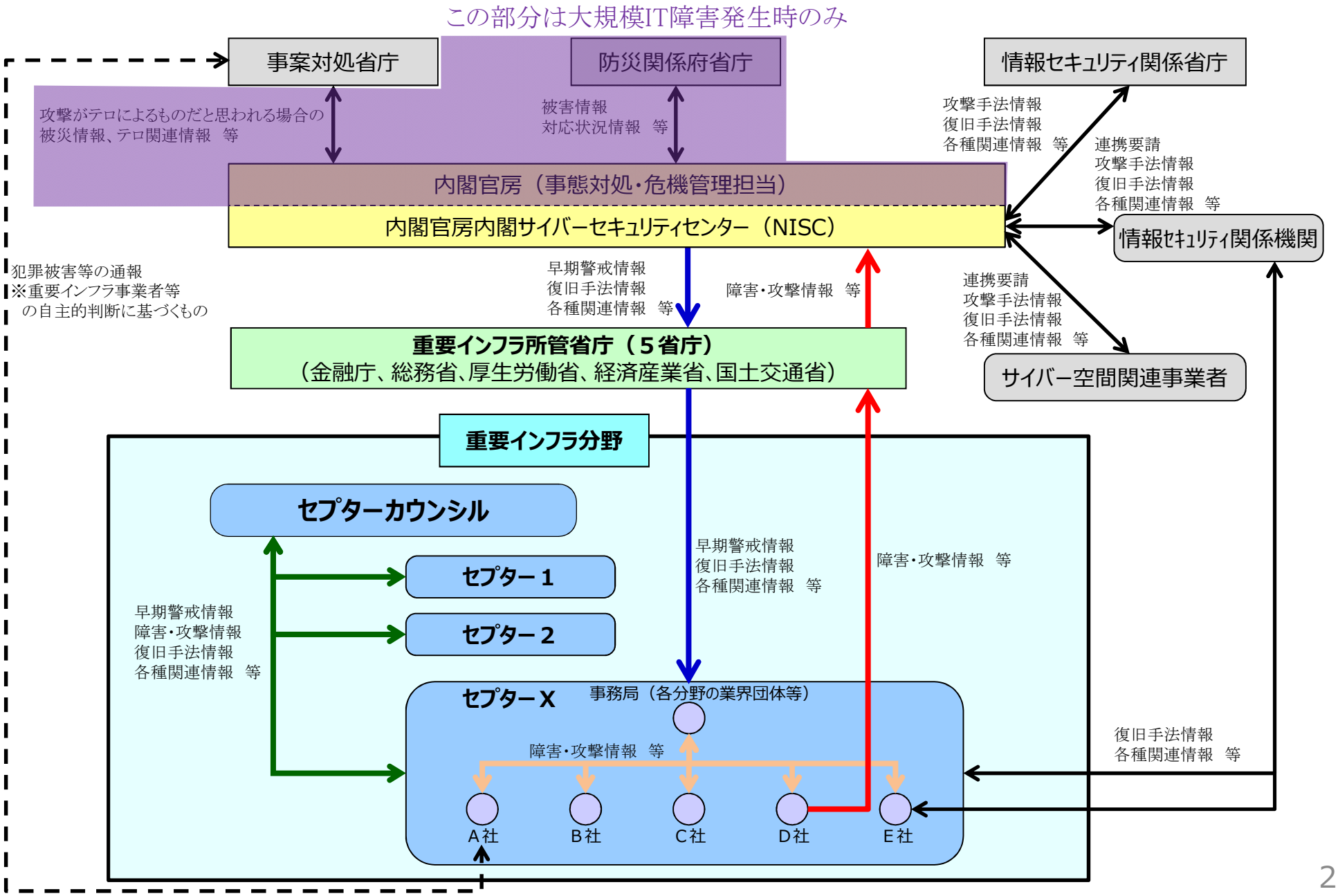
4．参考資料

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。

（参考）情報共有体制


この部分は大規模IT障害発生時のみ
事案対処省庁
防災関係府省庁
情報セキュリティ関係省庁
攻撃がテロによるものだと思われる場合の
被災情報、テロ関連情報　等
被害情報
対応状況情報　等
攻撃手法情報
復旧手法情報
各種関連情報　等
連携要請
攻撃手法情報
復旧手法情報
各種関連情報　等
内閣官房（事態対処・危機管理担当）
内閣官房内閣サイバーセキュリティセンター（NISC）
情報セキュリティ関係機関
犯罪被害等の通報
※重要インフラ事業者等
の自主的判断に基づくもの
早期警戒情報
復旧手法情報
各種関連情報　等
障害・攻撃情報　等
連携要請
攻撃手法情報
復旧手法情報
各種関連情報　等
重要インフラ所管省庁（５省庁）
（金融庁、総務省、厚生労働省、経済産業省、国土交通省）
サイバー空間関連事業者
重要インフラ分野
セプターカウンシル
セプター１
セプター２
セプターＸ
事務局（各分野の業界団体等）
早期警戒情報
障害・攻撃情報
復旧手法情報
各種関連情報　等
早期警戒情報
復旧手法情報
各種関連情報　等
障害・攻撃情報　等
障害・攻撃情報　等
復旧手法情報
各種関連情報　等
Ａ社
Ｂ社
Ｃ社
Ｄ社
Ｅ社

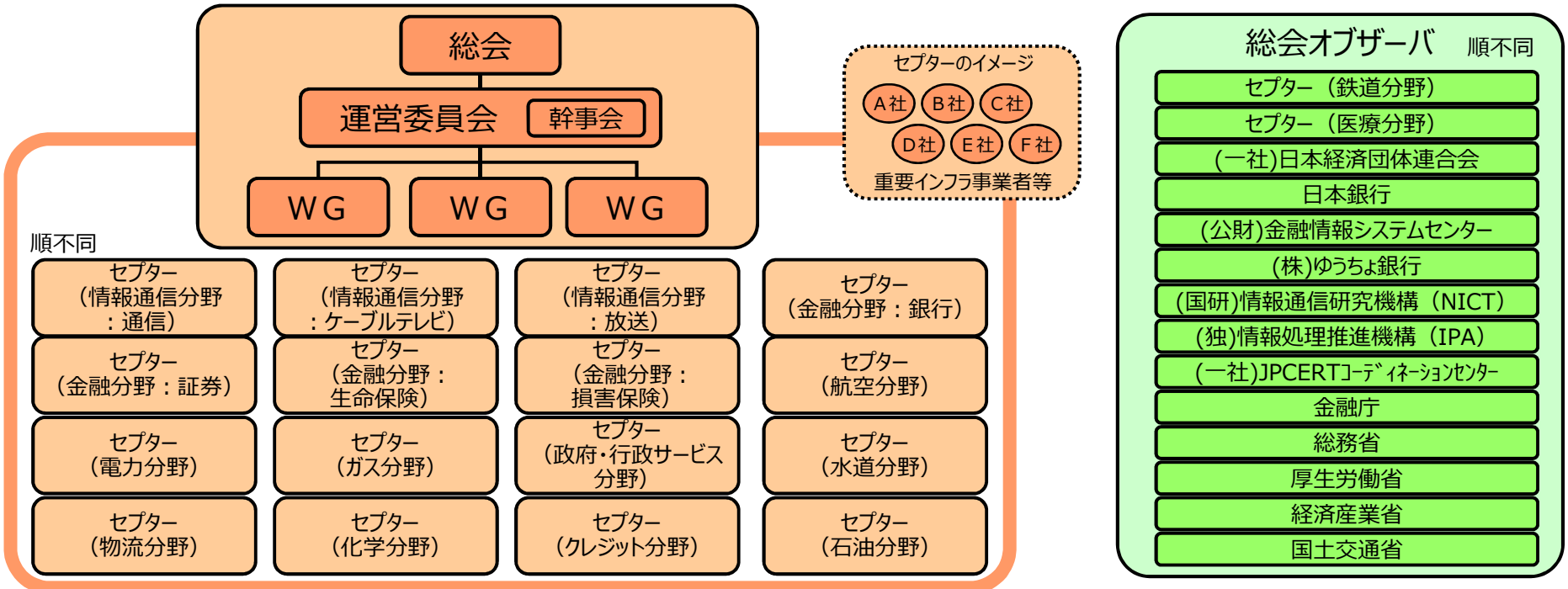
（参考）セプターとセプターカウンシル

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。
- IT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。



（参考）各分野のセプター一覧

2016年3月末現在

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CEPTAOR	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	(一財)日本データ通信協会 テレコム・アイザック推進会議	(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推進部共同システム開発室	国土交通省 航空局 安全企画課	国土交通省 鉄道局 総務課 危機管理室	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（内訳）	24社・団体 （固定系のﾈｯﾄﾜｰｸｲﾝﾌﾗを設置する電気通信事業者、ｱｸｾｽ系の電気通信事業者、ISP事業者、携帯電話事業者等）	332社 ((一社)日本ケーブルテレビ連盟の正会員ケーブルテレビ事業者)	194社 1団体 （日本放送協会、地上系民間基幹放送事業者、(一社)日本民間放送連盟）	1,446社 （銀行、信用金庫、信用組合、労金、商工中金、農協等）	255社 ７機関 （金融商品取引業者、取引所等証券関係機関）	41社 ((一社)生命保険協会の定款に定める社員および特別会員）	29社 （オブザーバ３社含む） ((一社)日本損害保険協会 情報システム委員会参加会社）	2グループ 3機関 （航空運送事業者、定期航空協会、官庁［航空局、気象庁］）	22社 1団体 1機関 （鉄道事業者22社、1団体、官庁［鉄道局］）	12社 2機関 （一般電気事業者、日本原電(株)、電源開発(株)、電気事業連合会、電力中央研究所）	10社 （主要な一般ガス事業者10社）	47 都道府県 1,741 市区町村	1グループ 6機関 （医療機関、(公社)日本医師会、四病院団体協議会((一社)日本医療法人協会、(公社)日本精神科病院協会、(一社)日本病院会、(公社)全日本病院協会）、保健医療福祉情報システム工業会）	8水道事業体 （会員水道事業体のうち会長都市並びに地方支部長都市） [補足]障害の内容によって、構成員を通じ、全国の日本水道協会の会員水道事業体(1,361事業体)へ情報を提供	6団体 16社 （日本物流団体連合会、日本船主協会、日本内航海運組合総連合会、日本港運協会、日本倉庫協会、全日本トラック協会及び主要な物流事業者16社）	11社 （主要な石油化学事業者）	18社 （主要なクレジットカード会社等）	14社 ・グループ （主要な石油精製・元売会社）
緊急窓口	2007年4月運用開始	2012年12月運用開始	2007年4月運用開始										2008年4月運用開始			2015年1月運用開始	2014年4月運用開始	2014年12月運用開始
情報の取扱ルール	2007年1月制定	2012年11月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2006年9月制定	2007年3月制定	2007年3月制定	2008年3月制定	2008年3月制定	2008年3月制定	2014年12月制定	2014年４月制定	2014年１２月制定
情報と連絡手段	障害事例情報等 メール、電話	障害事例情報等 メール、電話	障害事例情報等 メール、電話、FAX、WEB	障害事例情報等 メール、電話、ＷＥＢ	障害事例情報等 メール、電話、FAX、WEB	障害事例情報等 メール、電話、携帯、WEB	障害事例情報等 メール、電話	障害事例情報等 メール、電話	障害事例情報等 メール、電話	脆弱性に関する情報等 メール、電話携帯、FAX、電子会議室TV会議、会議体	障害事例情報等 メール、電話、携帯、AX	障害事例情報等 メール、電話、WEB	障害事例情報等 メール、電話、携帯、衛星電話、FAX	障害事例情報等 メール、電話、携帯、衛星電話、FAX	障害事例情報等 メール、電話、携帯、FAX	障害事例情報等 メール、電話、携帯電話	障害事例情報等 メール、電話	障害事例情報等 メール、電話

（注） 本マップは、各セプターの自主的な整備状況を把握し、マップとして取り纏めたもの。

第3次行動計画の見直しのポイント

① 重要インフラ事業者の先導的取組の推進（相互依存性等を踏まえたクラス分け）

重要インフラ事業者の情報セキュリティ対策における先導的取組を推進するとともに、重要インフラ事業者以外の事業者についても情報セキュリティ対策レベルの向上を図る。

重要インフラ事業者

先導的取組を行う事業者	その他の事業者
電力分野	
◘ 一般送配電事業者　等	◘ 左記以外の電気事業者
情報通信分野	
◘ 主要電気通信事業者　等	◘ 左記以外の情報通信事業者
金融分野	
◘ 主要都市銀行　等	◘ 左記以外の金融機関
✓ 他の重要インフラ事業者からの依存が大きい ✓ 比較的短時間のIT障害であってもその影響が大きい	◘ 他の重要インフラ分野の事業者

依存関係

重要インフラ事業者以外

- ◘ 重要インフラ事業者の主要関係先や外部委託先
- ◘ 先端技術等の知的財産や営業秘密を保持する企業、研究機関、大学等
- ◘ 安全保障上重要な企業

◆ 行動計画に基づく取組

安全基準等の整備・浸透

情報共有体制の強化

障害対応体制の強化

リスクマネジメント

防護基盤の強化

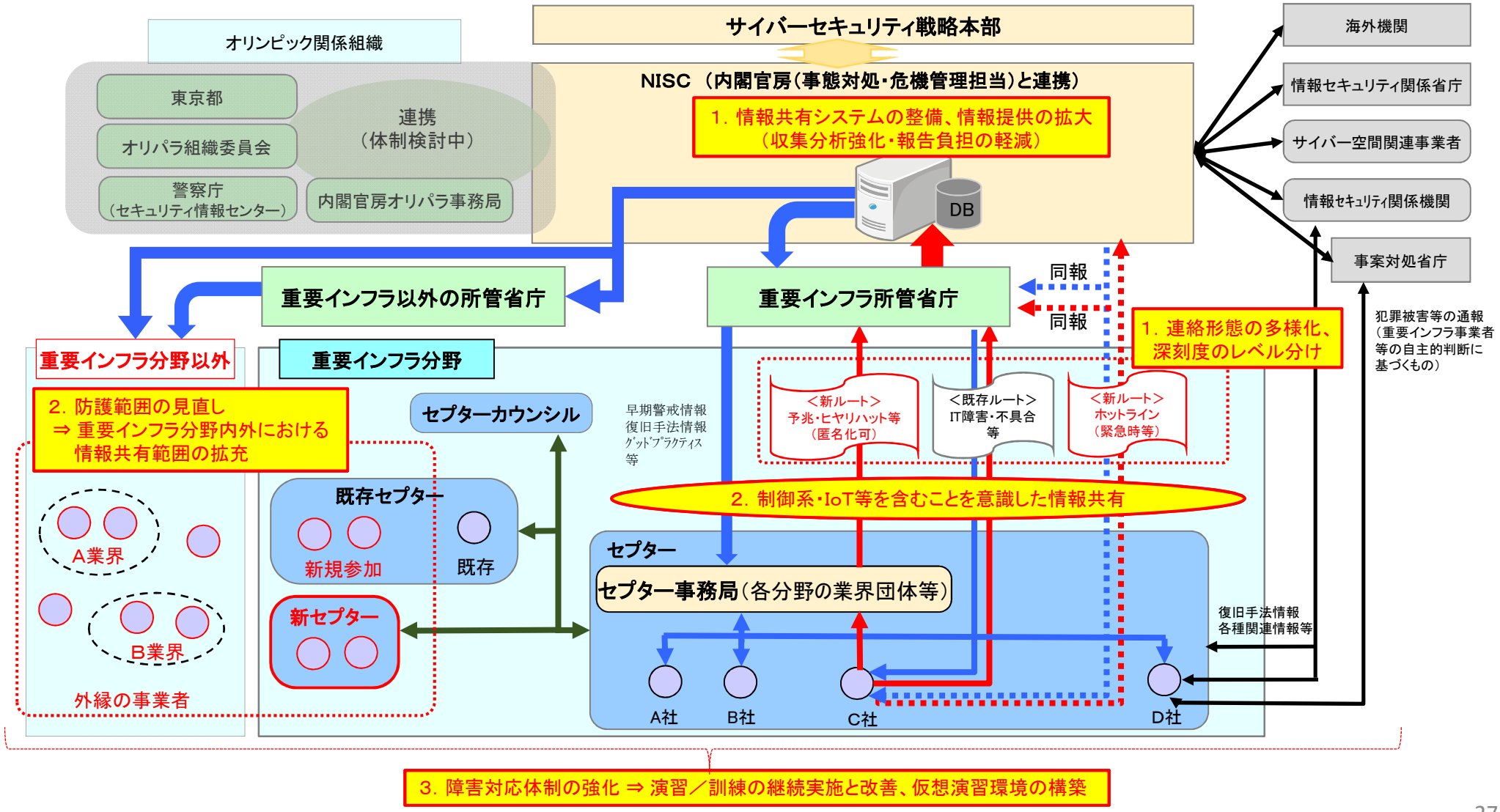
◆ 個々の事業者において情報セキュリティ対策を実施

今後の取組

- ➢ 先導的取組の実施(例)
  - ◆ISACの設立・加盟
  - ◆侵入テストの実施
  - ◆リスクマネジメントの重点化
  - ◆NISCとのホットライン構築
  - ◆浸透状況調査結果を踏まえた対策の深化
- ➢ 先導的取組を実施していくための体制づくり
- ➢ NISC又は所管省庁からの情報提供を開始
- ➢ NISC又は所管省庁への情報連絡、その他の情報セキュリティに係る取組について、組織内の体制が確実なものとなった後に開始

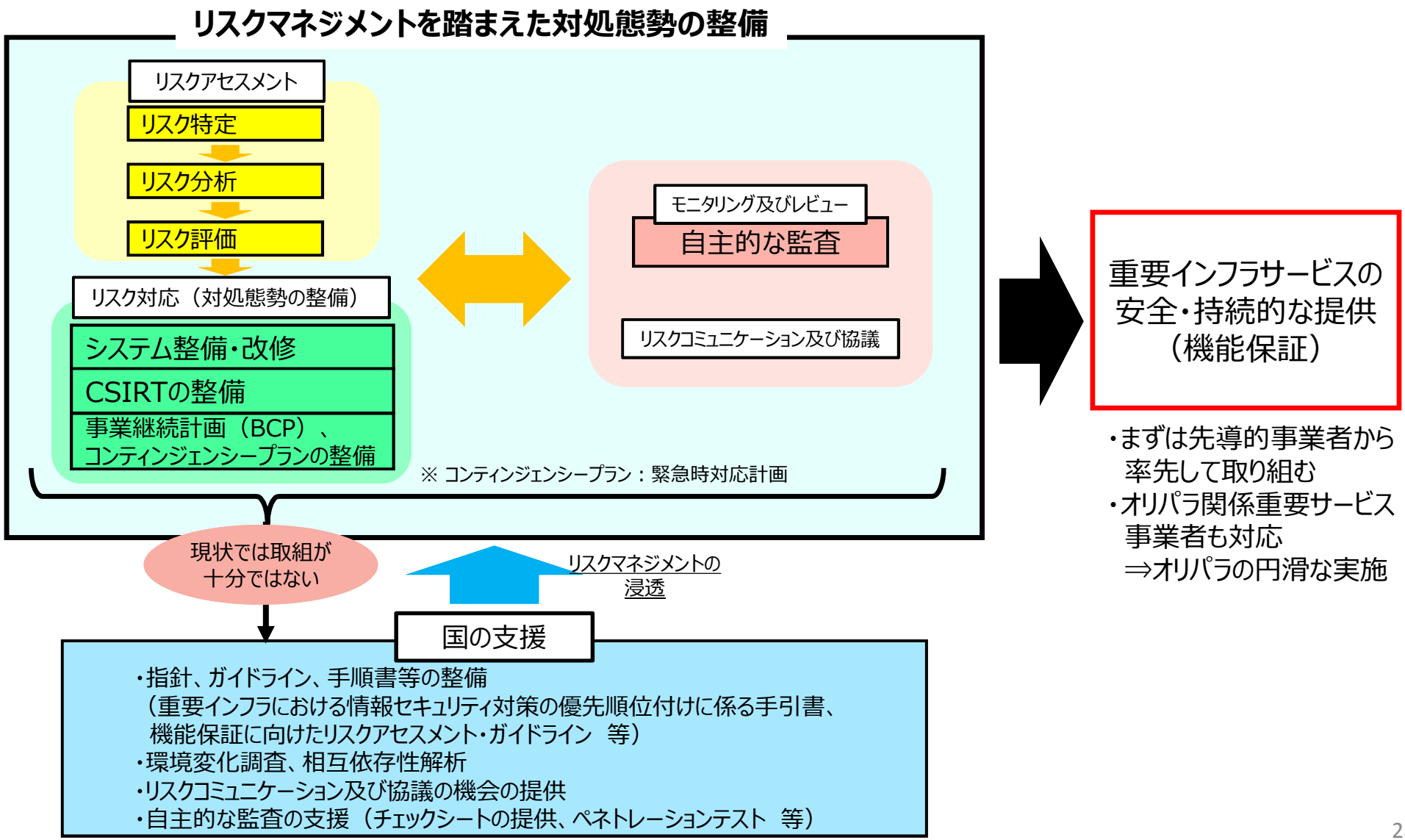
第3次行動計画の見直しのポイント
② オリパラ大会を見据えた情報共有体制の強化

1．情報共有の更なる促進 ⇒ 連絡形態の多様化、事案の深刻度のレベル分け、情報共有システムの整備、情報提供の拡大
2．防護範囲の見直し ⇒ 重要インフラ分野内外における情報共有範囲の拡充、制御系・ＩｏＴ等を含むことを意識した情報共有
3．障害対応体制の強化 ⇒ 演習／訓練の継続実施と改善、仮想演習環境の構築



第3次行動計画の見直しのポイント
③ リスクマネジメントを踏まえた対処態勢整備の推進

重要インフラサービスを安全・持続的に提供できるよう、重要インフラ事業者等によるリスクマネジメントを踏まえた対処態勢整備を推進する。



第3次行動計画の見直しのポイント
④　第３次行動計画の施策群の主な見直し事項

第3次行動計画の目標（理想とする将来像）と評価

◆ 重要インフラ事業者等が自主的に見直しの必要性を判断し改善を図るサイクルが浸透しつつあるが、ＰＤＣＡのうちＣＡについてはいまだ十分とは言えない状況。
◆ 官民、民民間の情報共有が着実に進展。演習等により防護能力が向上。脅威の深刻化を踏まえ、情報共有の質・量の改善、ＩＴ障害対応経験等を将来に活かす取組が必要。
◆ 国民への取組内容の発信を実施。しかし、国民の不安感はぬぐい切れていない。引き続き、国内外の多様な主体との連携、情報収集・分析、国民への適切な発信の継続が必要。
◆ 2000年以降、行動計画として策定・公表、定期的な評価・見直しが行われている。これに基づく継続的取組により対策が着実に進展。同計画の基本的枠組みの維持が妥当。
◆ 重要インフラ防護の目的に照らし、機能保証の観点から取組を進めることが重要。また、一部で先導的な取組も進められており、これを適宜展開していく。

第３次行動計画の施策群	見直しの方向性（案）	具体化に向け検討すべき事項
①安全基準等の整備及び浸透	○経営層に期待される認識・行動、内部統制の強化、ＯＴを視野に入れた人材育成等について追記し、指針を充実 ○情報セキュリティへの取組を業法における保安規制に位置づける等、制度的な枠組みの検討・整備 ○安全基準等の浸透状況調査を通じた重要インフラ事業者の情報セキュリティ対策レベルの底上げ	○経営層に期待される認識・行動を受けた重要インフラ事業者による内規見直しの進め方 ○現状の制度的枠組みの再確認、課題整理
②情報共有体制の強化	○情報共有の更なる促進 ・連絡形態の多様化（セプター事務局経由の省庁報告ルート（匿名化）） ・事案の深刻度のレベル分け ・迅速な共有プラットフォーム整備（ホットライン含む） ・制御系・ＩｏＴ等を含むことを意識した情報共有 ・情報提供の拡大　　等	○その他の情報共有の促進方策
③障害対応体制の強化	○重要インフラ事業者の実用性を重視した分野横断的演習及びセプター訓練の継続実施・改善	○重要インフラ事業者等が検証できるような仮想演習環境の構築
④リスクマネジメント	○施策のスコープを拡大し、機能保証の観点から、リスクアセスメント結果を踏まえた対処態勢の整備支援に係る取組（オリパラも見据えた取組を含む。）を追加	○リスクアセスメント結果を適切に経営意思決定に反映させるための内部統制の強化（自主的な監査の強化等）に対する支援の在り方
⑤防護基盤の強化	○重要インフラ分野内外の情報共有等を行う範囲の見直し ○情報セキュリティ対策への経営層の関与の推進 ○国際会議等で得た情報の関係主体への積極的な提供 ○人材育成の支援（IT、OT両方に対応できるハイブリッド人材を含む。）	○拡充を図る重要インフラ分野内外の情報共有先（外縁等）

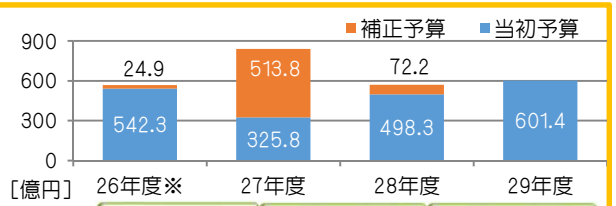
政府のサイバーセキュリティに関する予算

平成29年度予算概算要求額

601.4億円

（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年度概算要求	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	28.7億円	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	35.1億円	—	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	4.0億円	—	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	5.0億円	—	—
【外務省】	情報セキュリティ対策の強化	6.3億円	—	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	0.2億円	—	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	8.0億円	25.0億円	—
【経済産業省】	（独）情報処理推進機構（IPA）交付金	45.5億円	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	23.5億円	—	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	14.3億円	—	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	47.1億円	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	4.5億円	—	3.8億円
【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	0.6億円	—	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	2.2億円	—	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。