資料8

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

2016年3月31日
内閣官房内閣サイバーセキュリティセンター（NISC）

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

IoTシステムのセキュリティの確保

IoT推進コンソーシアム等で検討

企業によるサイバーセキュリティ関連情報の開示の在り方等の検討

NISCにおいてWGを設置して検討

サイバーセキュリティ経営ガイドラインの策定

昨年12月に策定（経済産業省）

サイバーセキュリティ人材育成総合強化方針の策定

サイバーセキュリティ戦略本部決定（3/31）

人材・予算の確保

H27補正・H28本予算、機構定員査定により対応

- ✓ （予算）H27補正：513.8億円（うちNISC68.1億円）、H28当初：499.3億円（うちNISC17.3億円）
- ✓ （機構定員）NISCの定員増22人、12省庁でセキュリティ担当審議官新設等

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

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策の強化

- ✓ 伊勢志摩サミット等での取組の推進
- ✓ 継続的なリスク評価を実施
- ✓ 2019年ラグビーワールドカップ開催時においてオリパラCSIRTを稼働

NISCの業務対象の拡大、連携推進体制の強化

今国会に基本法・情促法改正案を提出（2/2閣議決定）

- ✓ 監視・監査・原因究明調査の対象を中央省庁に加えて独立行政法人、一部特殊法人等に拡大
- ✓ 監視等の業務について、IPA等に委託

攻撃リスク低減のための対策強化

本年夏を目途に統一基準群を改定

- ✓ 独立行政法人等への適用対象範囲の拡大
- ✓ 監査に係る規定の整備

重要インフラに関する取組強化

検討ロードマップをサイバーセキュリティ戦略本部決定（3/31）

- ✓ 重要インフラの対象範囲の見直し等

マイナンバー制度の円滑な導入に向けた対策強化

- ✓ 自治体情報セキュリティクラウドの構築
- ✓ 勧告に対する措置状況報告等を踏まえた厚生労働省に対する追加的監査実施等

「サイバーセキュリティ人材育成総合強化方針」概要

策定の趣旨

「「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、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を示す。

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。

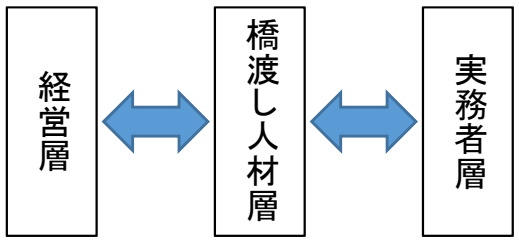
全体構成

第１章　社会で活躍できる人材の育成
第２章　政府機関における人材の育成
第３章　今後の検討の枠組み

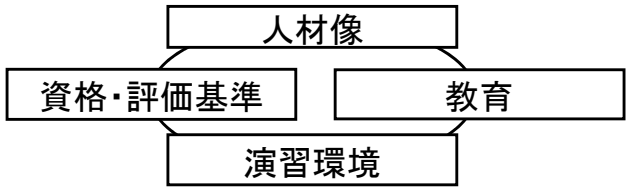
基本的考え方

○人材の需要と供給の好循環の形成

【人材の需要（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

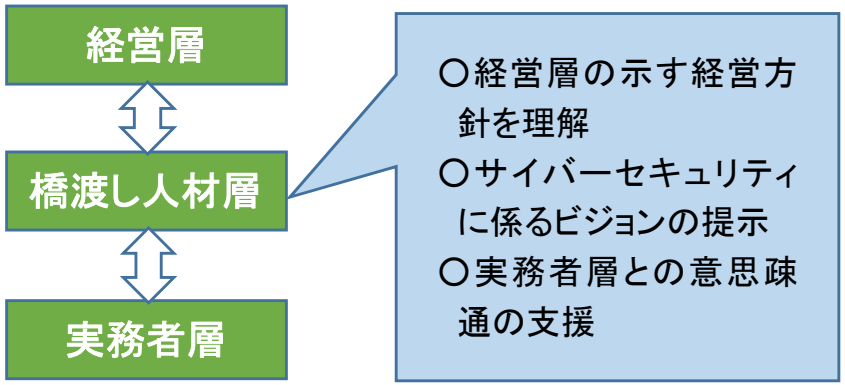


【人材の供給（教育）】
人材育成の循環システム
－確かな知識と実践力の下に、
　様々な業務経験を経て、人材が育成



社会で活躍できる人材の育成

人材の需要面



（1）経営層の意識改革

- 「サイバーセキュリティ経営ガイドライン」（平成27年12月）の普及促進
- 企業等のセキュリティ対策に係る情報発信の方策の検討（平成28年6月を目途）

（2）「橋渡し人材層」の育成（→経営層への働きかけ）

- 経営層への説明用コンテンツの作成（平成28年6月を目途）
- マネジメント能力向上のための演習の実施（平成28年度以降）
- セキュリティと他分野の専門性を併せ持つ教育の推進（社会人向け、継続）

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

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）
- 高専における演習環境の整備等（平成28年度から実施）
- 「職業実践力育成プログラム」制度等の活用による社会人の学び直し促進（継続）

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）
- 制御システムのセキュリティ演習の実施（継続）
- 国立情報学研究所における実践的演習環境の整備（国立大学法人等向けに平成28年度から実施）

能力の可視化
- 情報処理安全確保支援士制度の創設（法改正、平成28年度中に具体的な制度設計、国内外の企業等で行っている演習等も活用し、平成32年までに3万人超の有資格者の確保）

（注）上述に加え、突出人材の発掘・育成を推進（人材発掘の場づくり（継続）に加え、平成28年度から演習基盤の整備等を推進）

政府機関における人材の育成

【課題】
- ○ セキュリティに係る人材の圧倒的不足
- ○ 一般職員の情報リテラシーが不十分
- ○ システム管理や業務改革の知識・経験を有する人材の不足
- ○ 自組織におけるセキュリティ対策等の司令塔機能が弱体

政府一体となって、政府機関においてセキュリティ・IT人材を本格的に確保・育成する第一歩として、以下の取組を実施

1. 各府省庁における司令塔機能の抜本的強化

- ○ 平成28年度から「サイバーセキュリティ・情報化審議官」の新設等により司令塔機能を抜本的に強化
- ○ 「セキュリティ・IT人材確保・育成計画（仮称）」を作成し、これらの審議官等で構成する会議で共有・フォローアップ
- ○ サイバーセキュリティ対策推進会議（CISO等連絡会議）、各府省庁情報化統括責任者（CIO）連絡会議、次官連絡会議においても共有

（CISO:最高情報セキュリティ責任者Chief Information Security Officerの略称、CIO:情報化統括責任者Chief Information Officerの略称）

2. 橋渡し人材（部内育成の専門人材）の確保・育成

（1）体制の整備・人材の拡充
- ✦ 各府省庁の統括部局・一定のシステム所管部局の体制の整備及び人材の拡充

（2）有為な人材の確保
- ✦ 積極的な広報のほか、大学等での出張講義、インターンシップ等を検討　✦ 各府省庁において有為な人材を確保

（3）一定の専門性を有する人材の育成
- ✦ 「セキュリティ・IT人材育成支援プログラム(仮称)」の作成(研修受講、内閣サイバーセキュリティセンター（NISC）等への出向、大学院・民間企業への派遣等を通じた人材育成)　✦ 将来的に一部人材の総務省行政管理局等での採用・一括管理の枠組みの検討

（4）研修体系の抜本的整理
- ✦ 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4年で1千人超規模を目指す）、修了者へのスキル認定の枠組み構築等
- ✦ 管理職向けの実践的演習等　✦ CSIRT要員研修等の活用（CSIRT：情報セキュリティ緊急対応体制　Computer Security Incident Response Teamの略称）

（5）適切な処遇の確保
- ✦ 業務の専門性・特殊性等を踏まえ手当等を新たに支給することによる一定の給与上の評価　✦ 高位ポストまで見据えた人事ルート例（イメージ）の設定

3. 外部人材（即戦力の高度専門人材）の確保

- ○ NISC等において高度セキュリティ人材を採用し監査等で各府省庁に派遣　○情報通信技術（IT）総合戦略室における政府CIO補佐官の積極的活用
- ○ 産学官連携によるセキュリティ・IT人材の育成

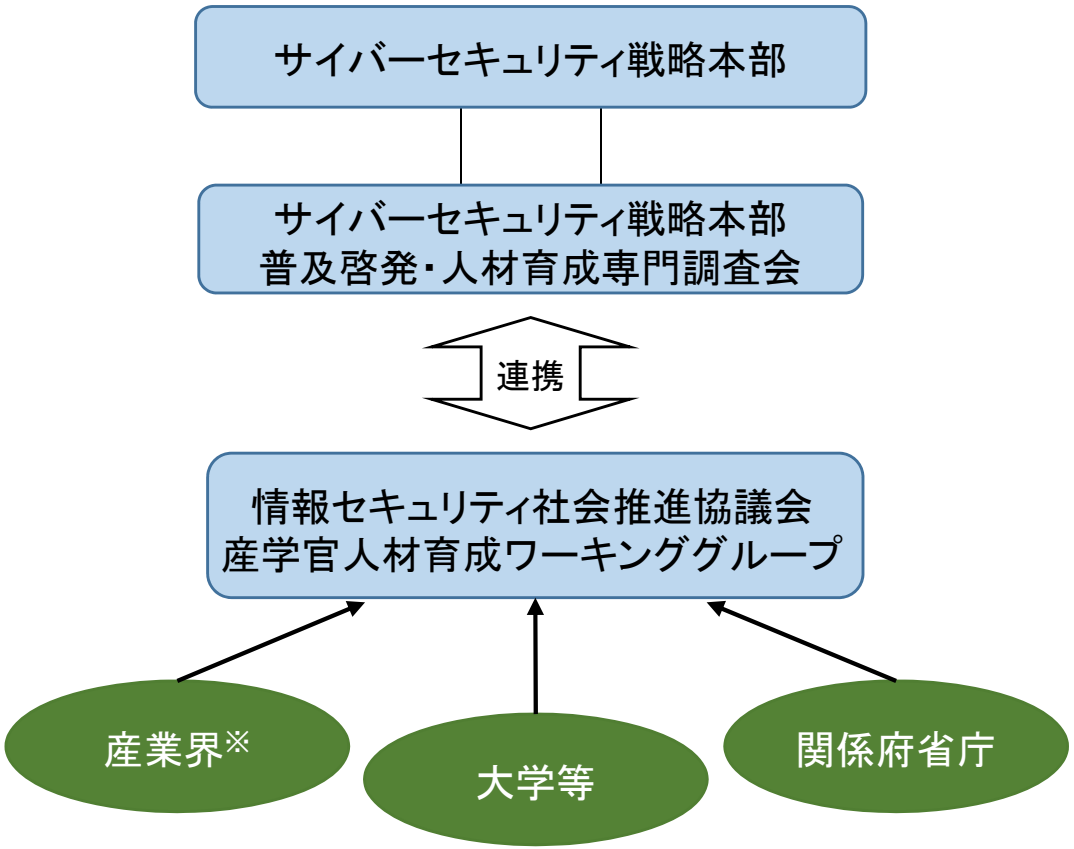
4. 一般職員の情報リテラシー向上

- ○ 各府省庁の新人研修等でのセキュリティ・IT研修実施　○ 新任管理職研修でのセキュリティ・ITの基礎的知識の習得機会提供
- ○ 人事評価マニュアルを改訂し、セキュリティ等に係る行動の評価の着眼点を明示等

今後の検討の枠組み

【社会で活躍できる人材の育成】

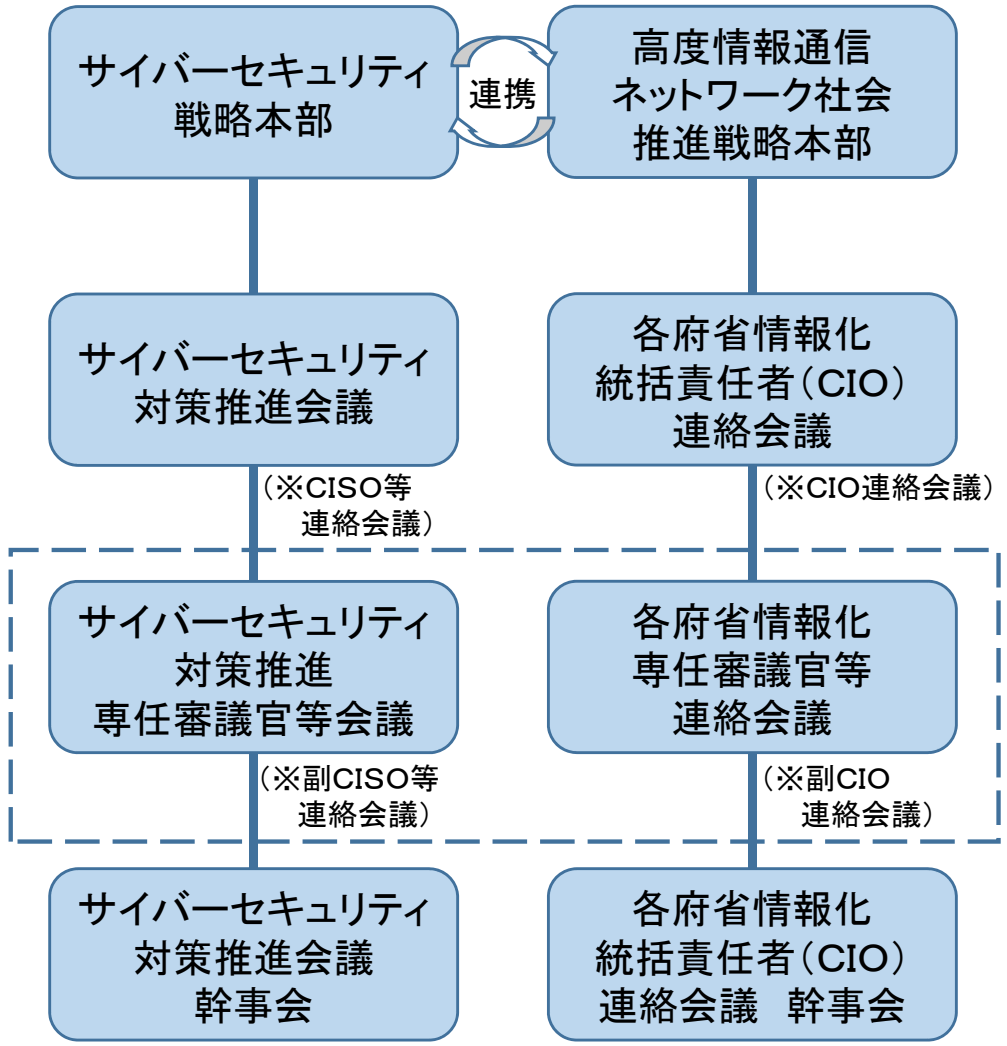
・「産学官の情報共有の場」として情報セキュリティ社会推進協議会 産学官人材育成ワーキンググループで情報共有する。
・次期人材育成プログラムを策定・公表する。（平成28年度中）



※「産業横断サイバーセキュリティ人材育成検討会」との連携を含む。

【政府機関におけるセキュリティ・IT人材の育成】

・平成28年度よりサイバーセキュリティ対策推進専任審議官等会議及び各府省情報化専任審議官等連絡会議を設置する。
・各府省庁において「セキュリティ・IT人材確保・育成計画（仮称）」を作成する。



（CISO:最高情報セキュリティ責任者　Chief Information Security Officerの略称
CIO:情報化統括責任者　Chief Information Officerの略称）

「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に向けたロードマップ」概要

1．行動計画見直しに当たっての基本方針

◆ 重要インフラを標的としたサイバー攻撃の深刻化に伴う重要インフラ防護の必要性が高まっている中、「サイバーセキュリティ戦略」（平成27年9月閣議決定）等に基づき、対策強化に向けた検討課題を整理。その際、「機能保証」の考え方に基づく取組を含める。

◆ 本ロードマップに従い検討を進め、行動計画の見直しについて、平成29年3月末を目途に結論。早急に対処すべき事項については、行動計画の見直しを待たずに対処。

2．考慮すべき環境変化

(1) **ＩｏＴの浸透に伴う制御技術と情報通信技術の相互依存性の高まり**

- 実空間（モノ・ヒト）とサイバー空間（情報）の物理的制約を越えた連接
- サイバー攻撃の対象となり得る機器が我々の身の周りの隅々まで拡散・浸透

(2) **面的防護に向けた情報共有等の連携体制強化の必要性等**

- ＩｏＴシステムを活用した新たなビジネスの創出や既存ビジネスの高度化・高付加価値化に伴うサプライチェーンリスクの高まり

(3) **諸外国における重要インフラへの取組の加速化**

- 官民間の情報共有の枠組みの強化・推進等の取組が進展

（米国「サイバーセキュリティ法」、EU「ネットワーク及び情報セキュリティ(NIS: Network and Information Security)指令」(案)）

3．強化すべき取組の方向性

1）サイバー攻撃に対する体制強化

➢ **経営層における取組の強化の推進**
- 機能保証の考え方に立脚し自らの経営責任を全うする観点からのセキュリティ経営資源投入の推進（情報開示の在り方）
- 経営層のセキュリティ意識改革を促す環境の整備（インセンティブの在り方）

➢ **情報共有の強化**
- 予兆脅威情報を含む共有すべき情報の範囲の見直しと情報共有の活性化
- 法令に基づく義務的な報告又は補完的な報告の着実な実施、安全基準や報告事項の基準等の見直し

➢ **内部統制の強化の推進**
- 自ら若しくは第三者による監査等の推進（マネジメント監査、侵入試験等）
- リスクマネジメントの推進強化

➢ **マイナンバー制度の運用に係るセキュリティの確保に関する取組**

➢ **2020年東京オリンピック・パラリンピック競技大会等大規模イベントの情報共有・対処体制のモデル化**

2）重要インフラに係る防護範囲の見直し

➢ **情報共有範囲の拡大**
- 相互依存性等を考慮した情報共有体制に組み込むべき主体の拡大

➢ **分野横断的な情報共有の強化**
- スマートシティ、自動車等、従来の業態の枠に収まらない情報共有のための体制の検討（既存の情報共有体制との連携の在り方を含む）

➢ **国の安全等の確保の観点からの取組**
- 重要インフラに属さないものの、我が国の知的財産や営業秘密を保全する観点から情報共有等を推進すべき分野の取組強化（研究機関、大学等を含む）

3）多様な関係者間の連携強化

➢ **国際連携**
・海外ＩＳＡＣとの連携（共同演習、情報共有を含む）の促進
・二国間・地域間・多国間の枠組みを活用した国際連携の継続

➢ **人材育成**
・人材育成強化方針に基づく重要インフラに係るセキュリティ人材の育成支援

4．行動計画の見直しに向けた今後の検討スケジュール

➢ 平成28年夏期に行われる評価を踏まえ、秋頃に行動計画の見直し骨子（案）を策定

➢ 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

➢ 上記検討は、2020年東京オリンピック・パラリンピック競技大会に係るサイバーセキュリティ確保のための施策と緊密に連携

強化すべき取組の方向性(具体的施策)

◆ 本ロードマップでは、**検討時期(結論を得る時期)を可能な限り具体化**。
◆ **早急に対処すべき事項**については、**行動計画の見直しを待たずに対処**。

１）サイバー攻撃に対する体制強化

➢ **経営層における取組の強化の推進**

○ 制御系（ＯＴ）と情報系（ＩＴ）のシステムの融合を踏まえ、「機能保証（任務保証）」の考え方に立脚し、事業継続を意識して経営層が自らの経営責任を全うする観点からセキュリティに係る経営資源が投入されるよう取り組む（情報開示の在り方について検討を行い、平成28年秋までにその方向性を明確にするとともに、「サイバーセキュリティ経営ガイドライン」の普及推進を継続的に実施。）

○ 経営層のセキュリティ意識改革を促す環境整備を図る（平成28年度中に具体策について一定の結論を得る。）

➢ **情報共有の強化**

○ 予兆脅威情報を含む共有すべき情報の範囲の見直しと情報共有の活性化（平成28年度末までに一定の結論を得て、その後も継続的に見直しを行う。報告事例集の作成は、平成28年度上期に実施。）

○ 法令に基づく義務的又は補完的な報告の着実な実施、安全基準や報告事項の基準等の見直し（平成28年度末までに具体的な方針について結論を得る。）

➢ **内部統制の強化の推進**

○ 自ら又は第三者による監査等の推進（マネジメント監査、侵入試験（情報システムに対する擬似的攻撃による評価（監査））等）（平成28年度末までに推進策についての結論を得る。）

○ 演習の取組強化（平成28年度中に仮想演習環境の構築に向けての検討を開始し、平成２９年度末までに結論を得る。）

○ リスクマネジメントの推進強化（平成28年度中に推進強化策についての結論を得て、平成２９年度以後に推進を行う。（手順書については、平成２７年度の取組成果を平成28年度半ばに提供する。その他前倒し可能な取組は、結論を得た後に速やかに取り組む。））

➢ **マイナンバー制度の運用に係るセキュリティの確保に関する取組**

○ マイナンバーの利用に係るサイバーセキュリティの確保に関する取組を継続的に実施する。

➢ **2020年東京オリンピック・パラリンピック競技大会等大規模イベントの情報共有・対処体制のモデル化**

○ 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情報共有・対処体制の整備についてのノウハウ等のモデル化（各年度の取組成果について、翌年度を目途に公表）

➢ **安全基準の不断の見直し等**

○ 業法によってサービスの維持及び安全確保に係る水準が求められている分野の安全基準の見直し等（継続実施）

２）重要インフラに係る防護範囲の見直し

➢ **情報共有範囲の拡大**

○ 相互依存性等を考慮した情報共有体制に組み込むべき主体の拡大（平成28年度末までに一定の結論を得て、その後も継続的に見直しを行う。）

➢ **分野横断的な情報共有の強化**

○ スマートシティ、自動車等、従来の業態の枠に収まらない情報共有のための体制の検討（既存の情報共有体制との連携の在り方を含む。）（平成28年度中を目途にＩｏＴシステムに関する分野横断的な情報共有の在り方についての検討を行う。）

➢ **国の安全等の確保の観点からの取組**

○ 重要インフラに属さないものの、我が国の知的財産や営業秘密を保全する観点から情報共有等を推進すべき分野の取組強化（研究機関、大学等を含む）（平成28年度末までに一定の結論を得て、その後も継続的に見直しを行う。）

３）多様な関係者間の連携強化

➢ **国際連携**

○ 海外ＩＳＡＣとの連携（共同演習、情報共有を含む。）に向けた取組の促進（継続実施）

○ 二国間・地域間・多国間の枠組みを活用した国際連携を継続し、我が国の取組を積極的に公表（平成28年度以降、継続的に実施。）

➢ **人材育成**

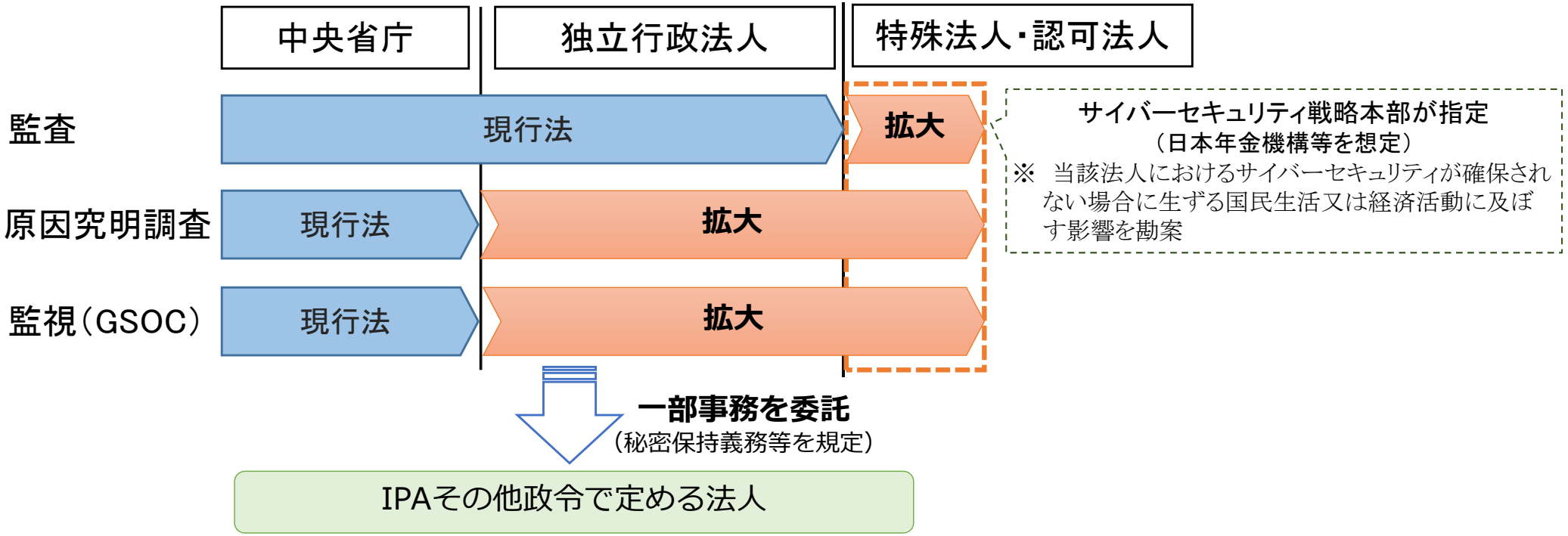
○ 人材育成強化方針に基づく重要インフラに係るセキュリティ人材の育成支援、官民人材交流、資格取得促進（平成28年度以後継続実施）

サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案の概要

日本年金機構の情報流出事案等を踏まえ、政府機関等のサイバーセキュリティ対策の抜本的強化を図るため、サイバーセキュリティ基本法等の改正を行う必要。

■ 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）等に委託

基本法



情促法

■ サイバーセキュリティ対策の強化に係る観点から、以下の規定の整備を行う。
- 本部から委託を受ける事務に係るIPAの業務追加
- 情報処理安全確保支援士制度の創設（名称独占、更新制、秘密保持義務等）
- ソフトウェアの脆弱性情報等の公表の方法・手続を整備

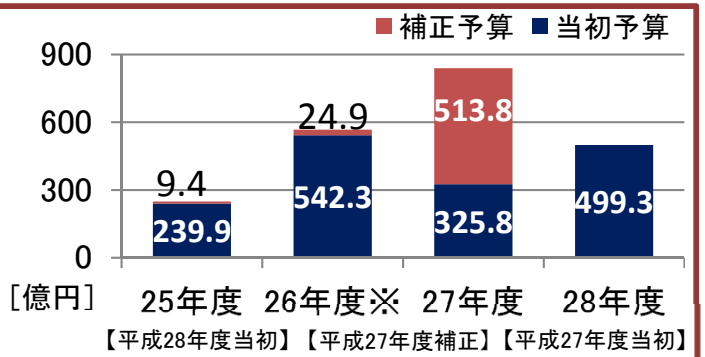
政府のサイバーセキュリティに関する予算

平成28年度予算政府案

499．3億円

（平成27年度当初予算額　325．8億円）

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要求額

		【平成28年度当初】	【平成27年度補正】	【平成27年度当初】
【内閣官房】	内閣サイバーセキュリティセンター予算	17．3億円	68．1億円	16．5億円
【警察庁】	日本版NCFTAへの参画に伴う経費	1．2億円	—	1．1億円
【警察庁】	サイバー犯罪等の対処能力強化のための実践的実習環境の整備等	0．8億円	—	0．6億円
【総務省】	サイバー攻撃複合防御モデル・実践演習等	7．2億円	13．0億円	4．0億円
【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】	自治体情報セキュリティ対策の抜本的強化	4．1億円	255．0億円	—
【外務省】	情報セキュリティ対策の強化	4．1億円	0．6億円	4．3億円
【外務省】	サイバー空間における外交及び国際連携	0．1億円	—	0．1億円
【経済産業省】	独法等の監視に係るシステム構築事業等	—	74．9億円	—
【経済産業省】	（独法）情報処理推進機構交付金（IPA）交付金	42．5億円	8．5億円	36．1億円
【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	—	17．7億円
【防衛省】	サイバー防護分析装置の整備	29．9億円	—	4．8億円
【防衛省】	ネットワーク監視器材の整備	61．2億円	—	29．8億円
【個人情報保護委】	特定個人情報に係るセキュリティ確保のための監視・監督体制整備（マイナンバー関連）	2．6億円	1．3億円	0．6億円
【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	39．6億円	12．7億円	—
【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	3．8億円	—	1．9億円
【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	7．8億円	—	—

平成27年度補正予算

513．8億円

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。

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