

政府のサイバーセキュリティに関する予算

資料5

平成28年度予算政府案

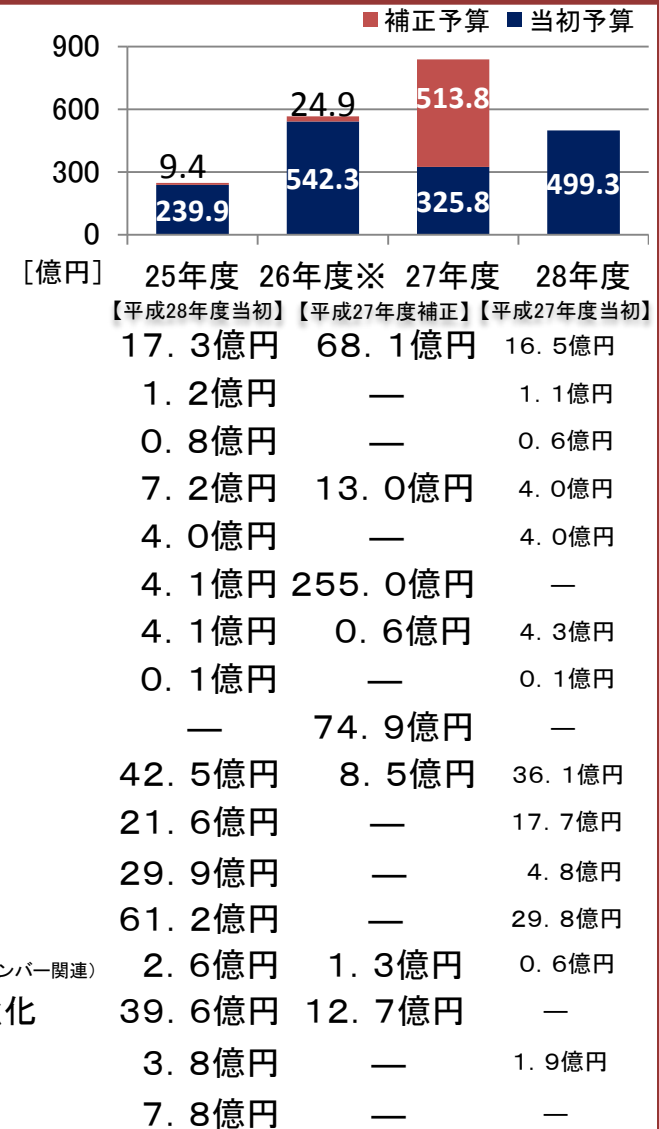
499.3億円

(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

【内閣官房】	内閣サイバーセキュリティセンター予算
【警察庁】	日本版NCFTAへの参画に伴う経費
【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
【総務省】	サイバー攻撃複合防御モデル・実践演習等
【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
【総務省】	自治体情報セキュリティ対策の抜本的強化
【外務省】	情報セキュリティ対策の強化
【外務省】	サイバー空間における外交及び国際連携
【経済産業省】	独法等の監視に係るシステム構築事業等
【経済産業省】	(独法)情報処理推進機構交付金(IPA)交付金
【経済産業省】	サイバーセキュリティ経済基盤構築事業
【防衛省】	サイバー防護分析装置の整備
【防衛省】	ネットワーク監視器材の整備
【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)
【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
【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
【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



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。

内閣官房の施策例

内閣サイバーセキュリティセンター予算

サイバーセキュリティ戦略 (平成27年9月4日 閣議決定)

➤ 政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)による検知・解析機能の強化

平成28年度
予算政府案 17.3億円

平成27年度
補正予算 68.1億円

平成27年度
当初予算 16.5億円
《参考》

○政府機関情報セキュリティ横断監視・
即応調整チーム(GSOC)の運用
6.5億円

○政府機関情報セキュリティ横断監視・
即応調整チーム(GSOC)の運用
6.5億円

○次期システム構築 66.8億円

➤ ペネトレーションテスト等を通じたセキュリティ対策の徹底
➤ マネジメント監査等を通じた組織の体制・制度の検証・改善、リスク評価に基づく組織的な対策・管理等による組織的対応能力の強化

○各府省庁ネットワークに接続されている
コンピュータシステムに対する侵入実験
及び監査 3.0億円

○各府省庁ネットワークに接続されている
コンピュータシステムに対する侵入実験
及び監査 3.1億円

○コンピュータシステムに対する侵入実験
及び監査 1.3億円

➤ サイバーセキュリティに関する情報の収集・分析機能の強化

○脅威予測等総合分析の実施
2.0億円

○脅威予測等総合分析の実施
0.8億円

➤ 政府機関で重大なインシデントが発生した場合等における原因究明調査のための取組強化

○サイバーセキュリティインシデントに係る
事後調査 1.0億円

○サイバーセキュリティインシデントに係る
事後調査 1.1億円

➤ NISCの体制強化

定員増 22人

定員増 20人

※平成28年度予算政府案については、上記のほか、サイバーセキュリティ戦略本部の運営経費やサイバーセキュリティ関連施策の実施に必要な経費等(483百万円)を計上

警察庁の施策例

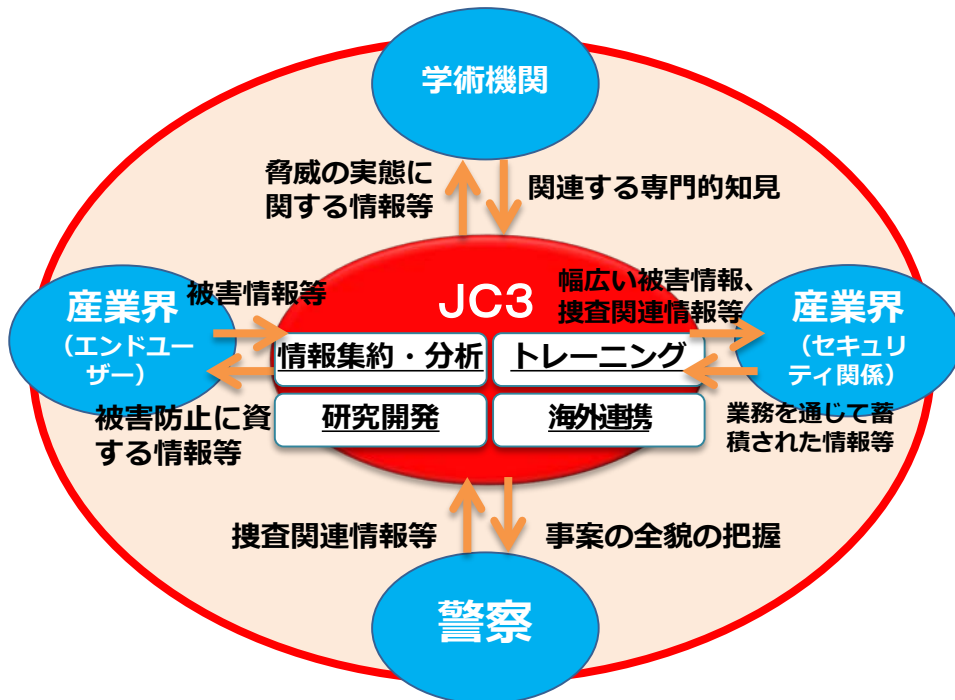
日本版NCFTAへの参画に伴う経費

平成27年度当初予算：1. 1億円
平成28年度予算政府案：1. 2億円

概要

産学官（法執行機関）それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を共有することにより、サイバー空間全体を俯瞰した上で、サイバー空間の脅威の大本を特定、軽減及び無効化し、以後の事案発生の防止に資するための活動を行うための枠組み。

日本版NCFTA^(※)は、平成26年11月、一般財団法人日本サイバー犯罪対策センター(Japan Cybercrime Control Center: 略称JC3)として業務を開始



※ NCFTA(National Cyber-Forensics & Training Alliance)=FBI等の法執行機関、民間企業、学術機関を構成員として米国に設立された非営利団体で、サイバー犯罪に係る情報の集約・分析、海外を含めた捜査機関等の職員に対するトレーニング等を実施。

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

平成27年度当初予算：0. 6億円
平成28年度予算政府案：0. 8億円

概要

捜査員に対して最新の事例を取り入れた高度かつ実践的な実習を行うための環境を整備



【主な経費】

サイバー攻撃複合防御モデル・実践演習等 13.0億円<27補正>

7.2億円<28当初> (4.0億円<27当初>)

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<28当初> (4.0億円<27当初>)

サイバー攻撃への総合的な対応力の向上

◎ サイバーセキュリティ対策を抜本的に強化するため、セキュリティ対策予算の規模を大幅に拡大。

(1) 昨年5月に発生した日本年金機構の情報流出事案を踏まえ、実践的なサイバー防御演習「CYDER」を活用したサイバーセキュリティ人材の育成強化。



(2) 2020年東京大会に向けて、大会を想定した大規模演習環境「サイバーコロッセオ」の整備及び演習の実施

(3) IoT時代を見据え、増大するIoT機器のセキュリティ確保のため、当該機器の脆弱性等に関する調査や利用者への注意喚起等、IoT機器へのセキュリティ対策を促す仕組みの構築・実証及び情報共有組織「Telecom-ISAC」への支援等を実施。

◎ 実践的なサイバー防御演習を、技術・知見を有するNICTが業務として実施するための法整備を検討。

◎ 本年3月を目途に、ISP事業者を中心としたTelecom-ISAC Japanを発展させた「ICT-ISAC」(仮称)を整備し、ICT分野全体にわたる情報共有を実施。

自治体情報セキュリティ対策の抜本的強化 【主な経費】 A 255億円<27補正>+B、C 4.1億円<28当初>

・ マイナンバー制度導入に関連し、標的型攻撃等の新たな脅威に対応可能な情報セキュリティについての抜本的な対策を実施。

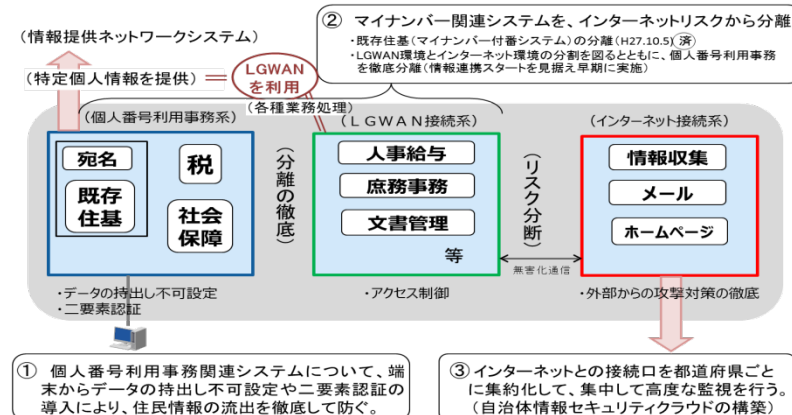
A 以下の三層からなる対策で、情報セキュリティ対策の抜本的強化を図る自治体を支援。

- ・ マイナンバー利用事務系では、端末からの情報持出し不可設定等を図り、住民情報流出を徹底して防止
- ・ マイナンバーによる情報連携に活用されるLGWAN環境のセキュリティ確保に資するため、LGWAN接続系とインターネット接続系を分割
- ・ 都道府県と市区町村が協力して、高度な情報セキュリティ対策を講じるため、自治体情報セキュリティクラウドを構築

B 総合行政ネットワークシステム(LGWAN)に関するセキュリティ対策事業

C 情報提供ネットワークシステムに関するセキュリティ対策事業

情報提供ネットワークシステム全体を保護し、より安全な情報連携を実現するための対策を実施



外務省の施策例

外務省サイバーセキュリティ施策

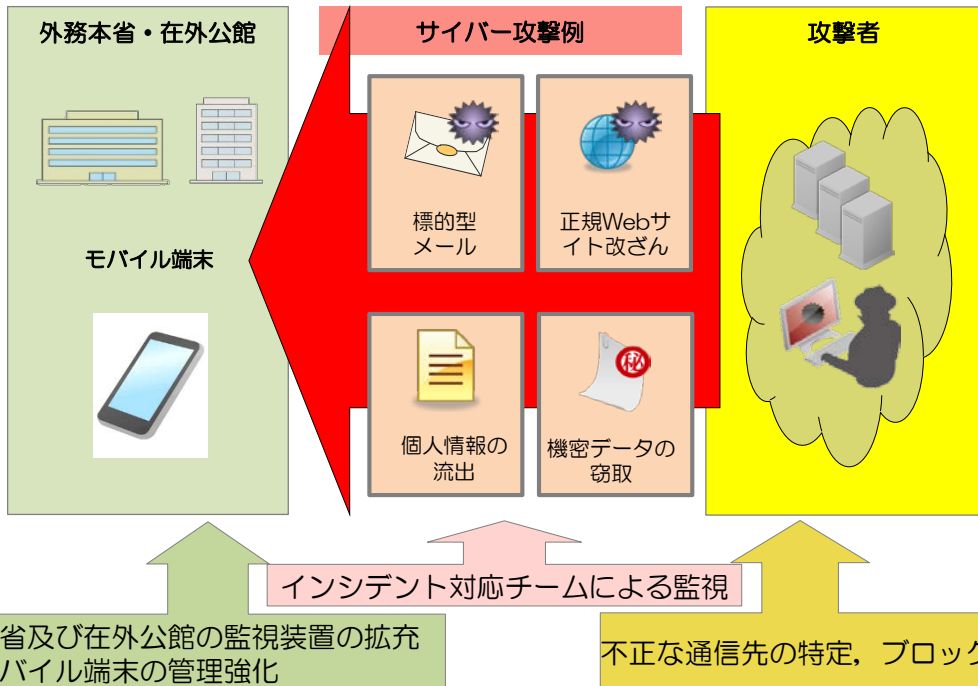
情報セキュリティ対策の強化

平成28年度予算要求：4. 1億円 平成27年度補正予算：0. 6億円

事業概要・目的

○概要

サイバー攻撃は年々巧妙化し、侵入を防ぐことは困難な状況になっており、侵入を前提とした監視・検知の強化などの多重防御による対策強化を図る。



○多様化する攻撃に対する、侵入されることを前提とした防御の多層化

平成27年度当初予算：4. 4億円
平成28年度予算要求：4. 2億円
平成27年度補正予算：0. 6億円

サイバー空間における外交及び国際連携

平成28年度予算要求：0. 1億円

事業概要・目的

○概要

近年増大するサイバー空間の脅威に対し、国際的な規範作り、安全保障面での課題、各国との連携等に取り組んでいく。

○国際会議

- ・サイバー安全保障に関する関係者会議／関連会議
- ・サイバー犯罪条約締約国会議／関連会議
- ・サイバーセキュリティに関する戦略的政策協議



サイバー安全保障に関する関係者会議



サイバーセキュリティに関する協議

経済産業省の施策例

○独法等の監視に係るシステム構築事業 (独立行政法人情報処理推進機構(IPA)交付金)

平成27年度補正予算 : 74.9億円

- ・ NISCの指示の下、独立行政法人情報処理推進機構(IPA)が、監視センターを構築し、独法等の情報システムの監視を行い、対処・警戒態勢の強化を図る。

○重要インフラ等のサイバーセキュリティ対策強化推進事 (IPA交付金)

平成27年度補正予算 : 4.0億円

- ・ 2020年の東京五輪に向けて、重要インフラのサイバーセキュリティ対策を実効性のあるものにしていくことが重要。
- ・ 重要インフラ事業者の対策状況調査やサイバーセキュリティリスク分析等を実施することで、重要インフラにおけるサイバーセキュリティ対策強化を推進。

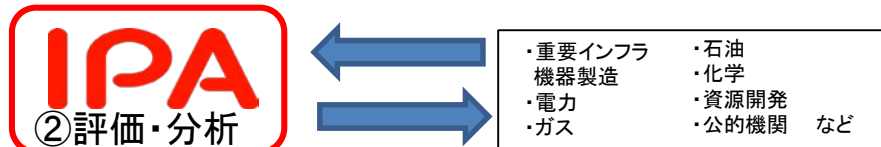
○情報セキュリティ対策促進・IT製品の評価・認証等(IPA交付金)

平成28年度予算案: 42.5億円(36.1億円)

- サイバー攻撃などのセキュリティ関連情報の収集・評価・分析や、対策方法の提案・実施・普及に取り組む。
- また、政府調達等のためのIT製品のセキュリティ評価・認証や、高度セキュリティ人材育成のための研修を実施。

標的型サイバー攻撃情報の共有

①セキュリティ関連情報の収集

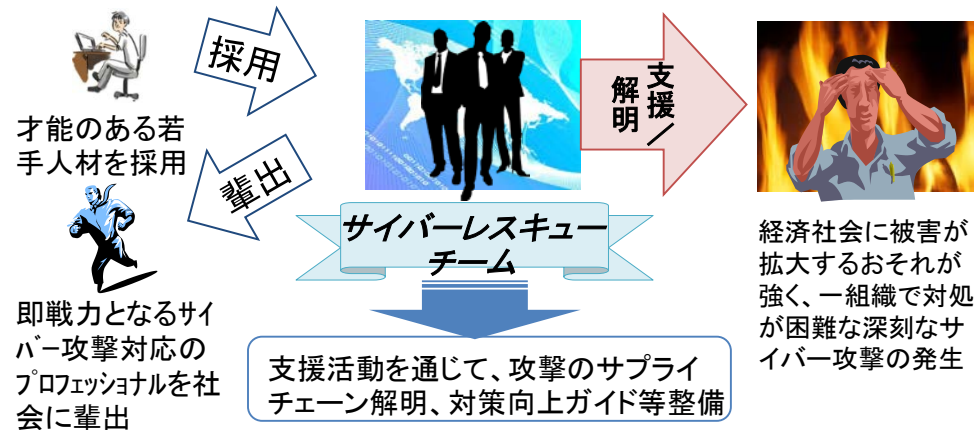


③対策方法の提案・実施・普及

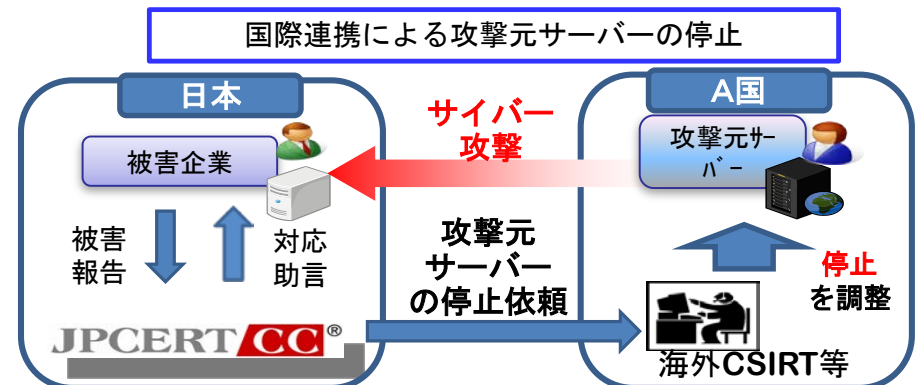
○サイバーセキュリティ経済基盤構築事業

平成28年度予算案: 21.6億円(17.7億円)

- ・ 経済社会に被害が拡大するおそれが強く、一組織で対処困難なサイバー攻撃について、IPAのサイバーレスキュー隊により、被害状況を把握し、被害拡大防止の初動対応を支援。



- ・ 攻撃対応連絡調整窓口(窓口CSIRT)の連携により、サイバー攻撃の温床となっている国際的攻撃基盤を共同駆除。

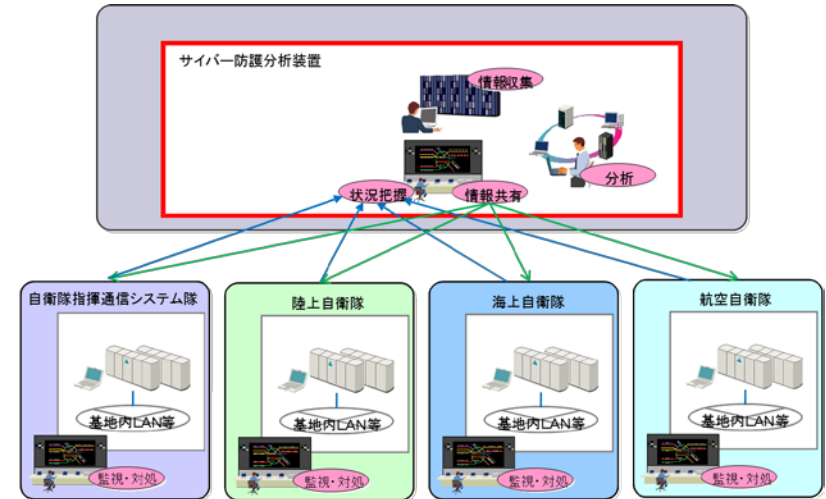


防衛省の施策例

サイバー防護分析装置の整備

平成28年度予算政府案 : 29.9億円

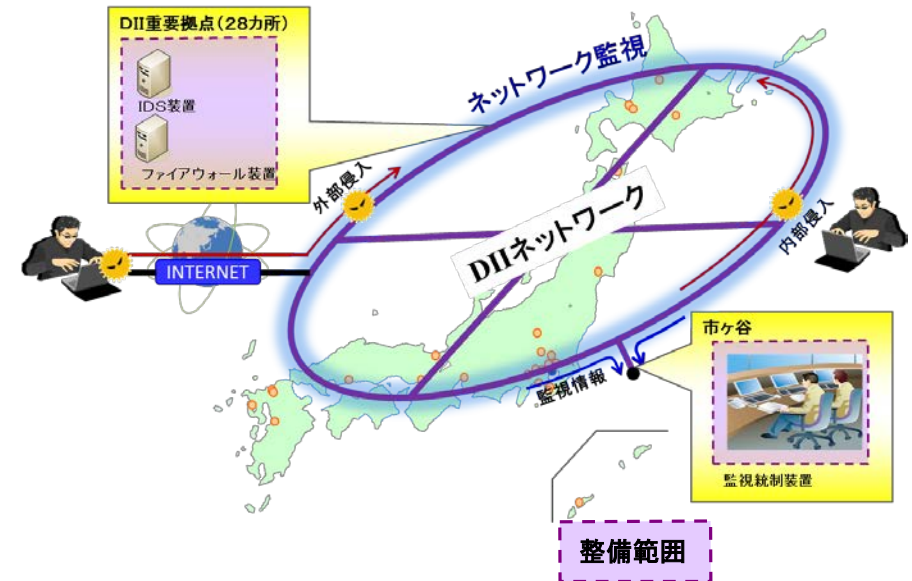
サイバー攻撃手法の高度化・複雑化に対応するため
器材を最新化し、ウイルス解析能力等の機能を向上



ネットワーク監視器材の整備

平成28年度予算政府案 : 61.2億円

サイバー攻撃等に対する状況把握能力を維持すると
ともに、サイバー攻撃等発生時における被害局限化、
早期復旧等対処能力の維持を図るため、防衛情報通信
基盤（DII）の各拠点に整備した監視器材を維持



個人情報保護委員会

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、委員会における監視・監督体制を整備

平成27年度当初予算：0.6億円、平成27年度補正予算：1.3億円、
平成28年度当初予算案：2.6億円
平成28年度機構定員：参事官1、企画官1を含む11名の増員

○ 監視・監督に係る業務体制の整備

- ・ 関係機関と連携し、専門的・技術的知見を有する監視・監督体制を整備
- ・ 情報提供ネットワークシステムに係る監視・監督体制の機能拡充
- ・ インシデント発生時の事案分析等における専門機関の知見の活用による効果的執行
- ・ 報告徴収・立入検査等により入手した情報の管理を含む、適切かつ効率的な執行を支えるための環境整備

「特定個人情報の適正な取扱いに
関するガイドライン」の継続周知・見直し

執行で得られた知見を、
「特定個人情報の適正な取扱いに
関するガイドライン」及び同Q & Aに反映

特定個人情報に係る
セキュリティの確保

厚生労働省の施策例

情報セキュリティ対策の強化

平成28年度予算案:39.6億円(新規)、平成27年度補正予算:12.7億円

日本年金機構における不正アクセスによる情報流出事案を踏まえ、日本年金機構をはじめ、厚生労働省及び関係機関の情報セキュリティ対策の一層の強化を図り、安全・安心で国民に信頼されるシステム構築に向けた取組を進める。

情報セキュリティ対策強化の4つの視点

組織、ヒト、ルール、システムの観点から、それぞれ対策を強化

組織的対策

(体制の強化)

- 情報セキュリティ対策の専門性や即応性向上のための組織強化

人的対策

(意識改革、人材育成)

- 情報セキュリティ教育の充実
- 実践的なセキュリティ訓練の実施
- 専門人材の確保

業務運営対策

(ルールの見直し、徹底)

- 情報セキュリティポリシーやインシデント対処手順書等の見直し

技術的対策

(システムの強化)

- 標的型攻撃に対する多重防御の取組
- インターネット接続環境下での情報取扱の厳格化

主な取組

厚生労働省・関係機関

- 高度な標的型攻撃を想定した入口・内部・出口の情報セキュリティ強化対策
- 厚生労働省CSIRT(Computer Security Incident Response Team)の体制強化
- 個人情報インターネット環境に置かないためのシステム上の措置
- 標的型攻撃に対する実践的訓練の実施
- 厚生労働省が保有するシステム及び所管法人等に対する情報セキュリティ監査の実施

日本年金機構

- 高度な標的型攻撃を想定した入口・内部・出口の情報セキュリティ強化対策
- 機構版CSIRT(Computer Security Incident Response Team)の創設
- 個人情報インターネット環境に置かないためのシステム上の措置
- 標的型攻撃に対する実践的訓練の実施
- 情報セキュリティ監査の実施

文部科学省の施策例

○ 大学や高専におけるセキュリティ人材の育成

平成28年度予算案：3.8億円（1.9億円）

(1) 成長分野を支える情報技術人材の育成拠点の形成(enPiT)

事業概要

- 産学連携による教育ネットワークを形成し、大学等における課題解決型学習（PBL）等の実践的な教育を推進する。これにより、セキュリティ分野をはじめとした情報技術人材の育成機能を強化する。
- これまでの実施してきている大学院生向けの人材育成の取組に加え、平成28年度からは新たに学部生を対象とする取組を実施する。

【平成28年度予算案：1.5億円（1.0億円）】

(2) 高専における情報セキュリティ人材の育成

事業概要

- 教材開発や達成目標の構築を継続実施するとともに、全国の高専に所属する学生が共同で利用できる実践的な演習環境（サイバーレンジ）を平成28年度に新たに構築する。

【平成28年度予算案：2.3※億円（0.9億円）】
（※国立高等専門学校機構運営費交付金の内数）

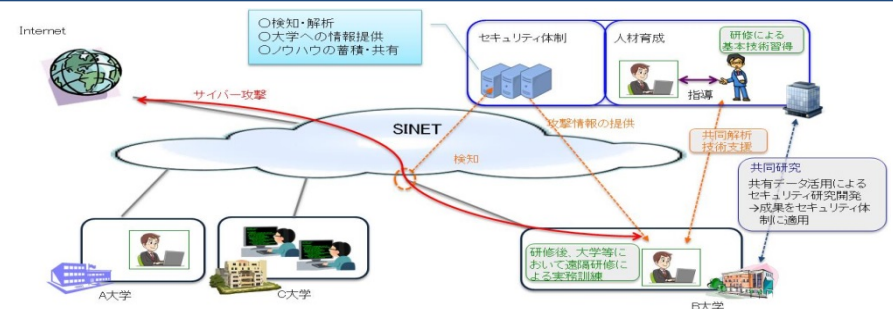
○ 国立大学法人等における情報セキュリティ体制の基盤構築

平成28年度予算案：7.8※億円（新規）

（※国立大学法人運営費交付金の内数）

事業概要

- 国立大学等に対するサイバー攻撃に対処するため、SINETを運用する国立情報学研究所と各大学の連携に基づき、攻撃を検知しその内容を各大学等において解析できる体制を構築する。
- また、SINETの実環境においてサイバーセキュリティに携わる技術職員を対象とした研修を実施し、攻撃の解析技術など最新の技術を習得し、高度化する攻撃に的確に対応できる人材を育成する。



(参考) AIP:人工知能/ビッグデータ/サイバーセキュリティ統合プロジェクト

平成28年度予算案：54.5※億円（新規）

（※関連する既存事業28.5億円を含む）

- 世界最先端の人材が集まる革新的な人工知能等の研究開発拠点を理化学研究所に新設するとともに、新たなイノベーションを切り開く独創的な研究者を支援。
- その際、AIP事業の一環として、高度なセキュリティ知識と管理能力を持つサイバーセキュリティ人材を大学との幅広いネットワークにより育成する。