政府のサイバーセキュリティに関する予算

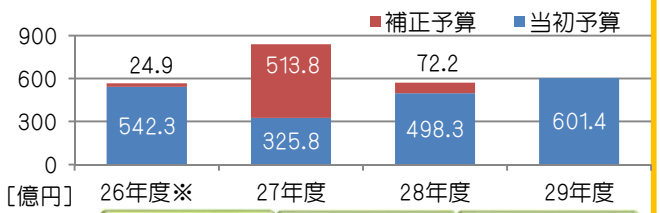
資料10

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次補正予算政府案

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。

内閣官房の施策例

サイバーセキュリティ戦略
（平成２７年９月４日　閣議決定）

内閣サイバーセキュリティセンター予算

	平成２９年度 概算要求額　２８．７億円	平成２８年度 第２次補正予算案　４．２億円	平成２８年度 当初予算　１７．３億円 《参 考》
➢ 各府省庁、独立行政法人、指定法人に対する監査、監視	○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　８．９億円 ○各府省庁、独立行政法人、指定法人に対する監査　９．０億円		○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 ○各府省庁に対する監査　３．０億円
➢ 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等　４．１億円		○脅威予測等総合分析の実施等　２．６億円
➢ 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対応の強化	○サイバーセキュリティインシデントに係る事後調査　等　２．５億円		○サイバーセキュリティインシデントに係る事後調査　等　２．２億円
➢ 各国との協力・連携、信頼醸成	○海外のサイバーセキュリティ関係機関等との協調・連携等　１．６億円		○海外のサイバーセキュリティ関係機関等との協調・連携等　０．８億円
➢ NISCの体制強化	機構・定員増　４人 （機構２・定員２）		定員増　２２人 （新規増１２、省庁間振替１０）

※　平成２９年度概算要求においては、上記のほか、サイバーセキュリティ戦略本部の運営経費等（２．６億円）を計上

警察庁の施策例

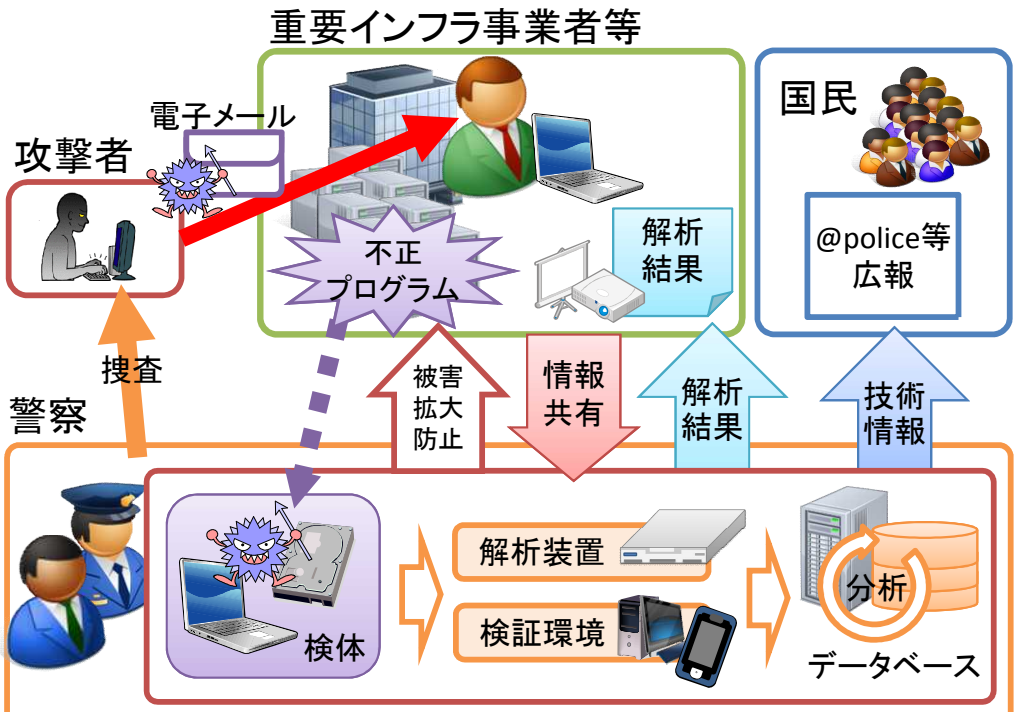
サイバーテロ対策用資機材の増強等

平成２８年度当初予算：４．０億円
平成２９年度当初予算：４．１億円

概要

サイバーテロの被害の未然防止・拡大防止に資するため、サイバーテロ対策用資機材の増強整備等を行う。

○標的型メール攻撃対処用資機材



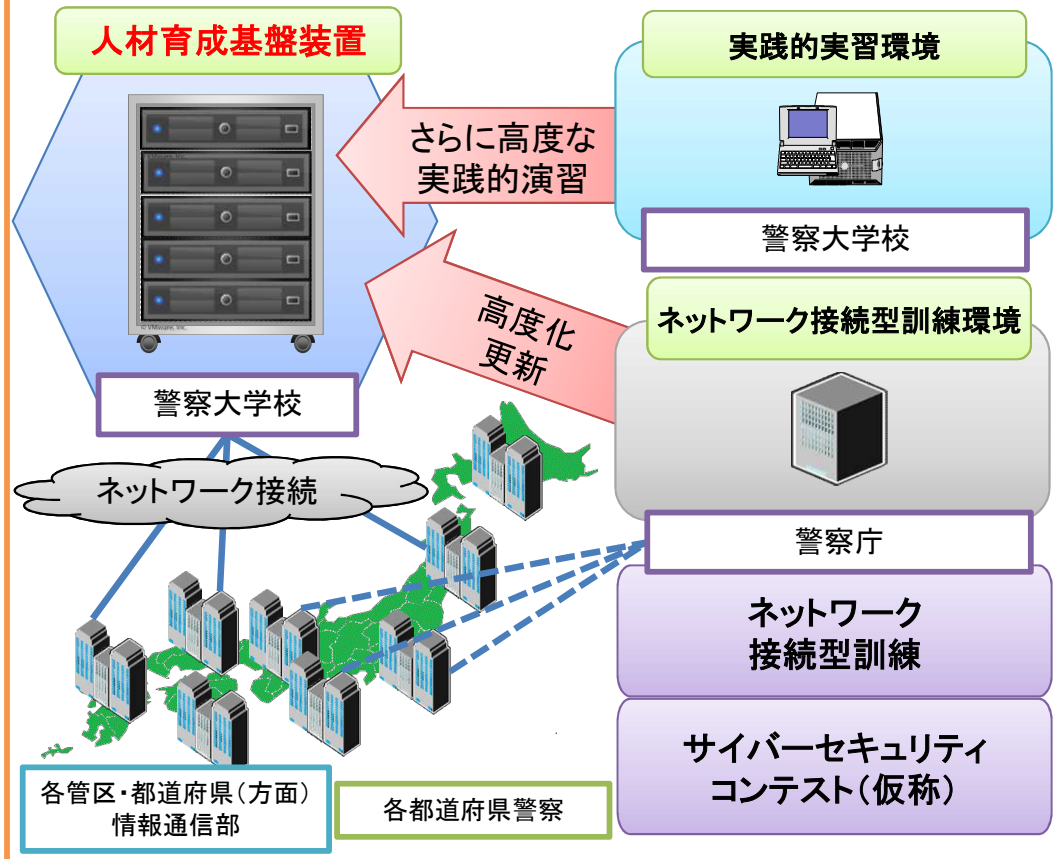
○ 巧妙・複雑化する標的型メール攻撃への対応
○ 攻撃者の推定に資する特徴情報の抽出
○ 重要インフラ等へのサイバー攻撃対策強化

サイバーセキュリティ対策に係る人材育成基盤の整備

平成２８年度当初予算：　０億円
平成２９年度当初予算：　８．７億円

概要

新たに様々な人材育成施策を展開するための人材育成基盤装置を整備する。



○ 実践的シナリオによるハンズオントレーニング
○ リアルタイム演習（攻撃者、防御者）
○ カスタマイズ可能な仮想環境による演習

総務省の施策例

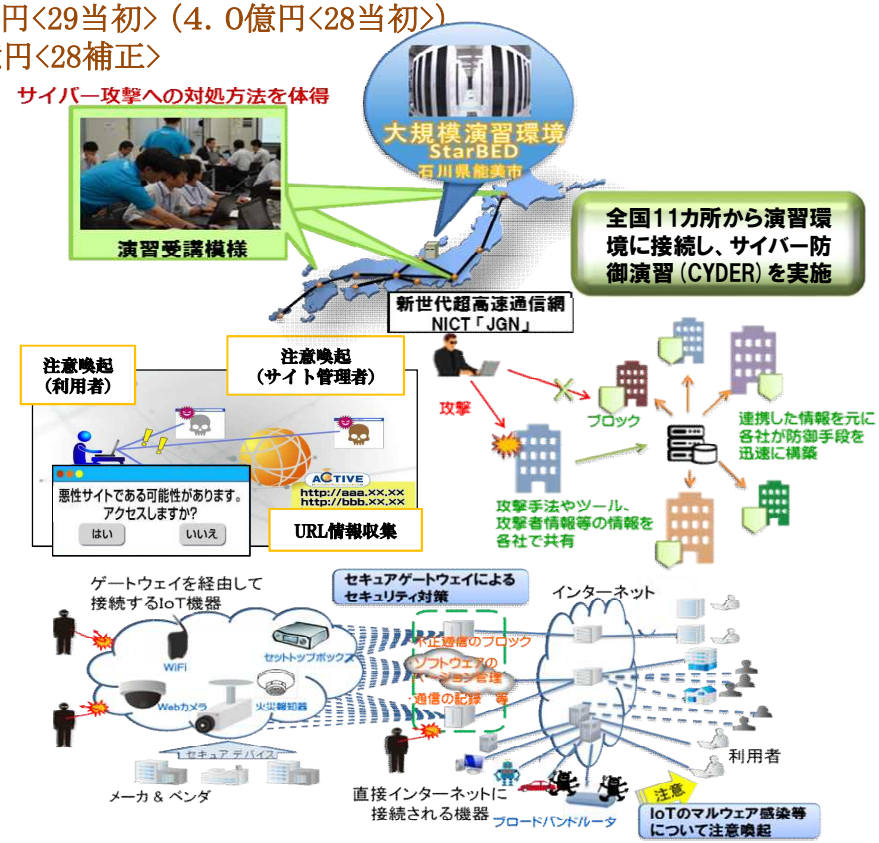
サイバー攻撃への総合的な対応力の向上

【主な経費】 (1) 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<29当初>（7．2億円<28当初>）
(2) 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<29当初>（4．0億円<28当初>）
(3) 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<28補正>

（1）ナショナルサイバートレーニングセンター(仮称)の構築
- 官公庁、地方公共団体、独立行政法人及び重要インフラ事業者等に対するサイバー攻撃について、実践的な演習を実施
- 2020年東京オリンピック・パラリンピック競技大会の適切な運営に向けたセキュリティ人材の育成
- 若手セキュリティエンジニアの育成

（2）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
- 我が国における情報セキュリティ対策基盤を強化するため、①一般のインターネットユーザのウイルス感染を防止するための実証実験、②関係事業者間の情報共有、③サイバーセキュリティにおける国際連携の推進といった各種取組を実施

（3）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
- 新たなサイバー攻撃の脅威にも対応した、①ネットワーク上のIoT機器の脆弱性やマルウェアの感染について、機器の管理者に対し、適切に注意喚起を実施する取組、②IoT機器とインターネットの境界上にセキュアなゲートウェイを設置し、低機能なIoT機器のセキュリティを確保するための取組に関する実証・検証等を実施

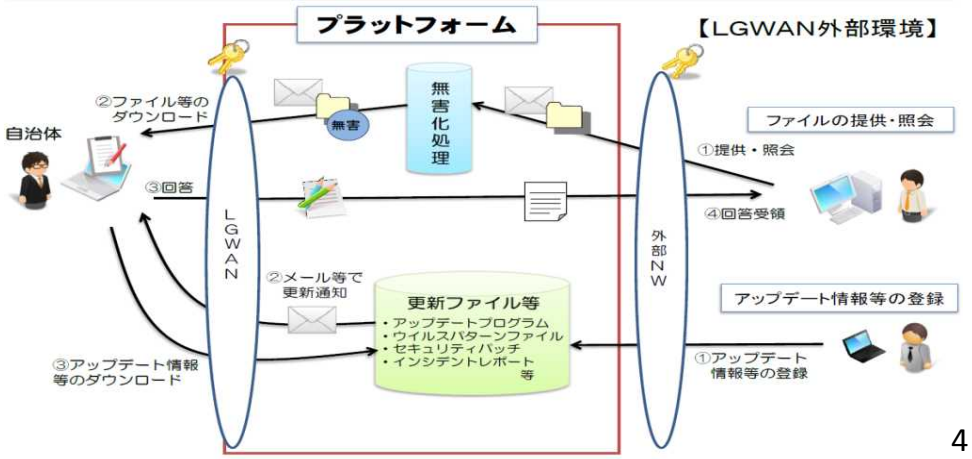


自治体の情報セキュリティ対策の強化

【主な経費】 自治体情報セキュリティ強化対策事業　5．0億円 <29当初>

○ マイナンバー制度による情報提供ネットワークシステムの稼働を踏まえ、LGWAN環境のセキュリティを確保し、地方公共団体で発生しているインシデント対策のノウハウの分析・共有を行い、地方公共団体の情報セキュリティ対策の継続的強化を支援するプラットフォームを構築。

- 今年度対応完了予定の「自治体情報セキュリティ強化対策事業」に伴い、LGWAN環境とインターネット環境との分離等が完了する。
- 外部からのメールや、調査・照会システム等における添付ファイルの無害化やインシデント対策のノウハウの分析・共有等を行い、LGWAN環境のセキュリティを確保する。



外務省の施策例

外務省サイバーセキュリティ施策

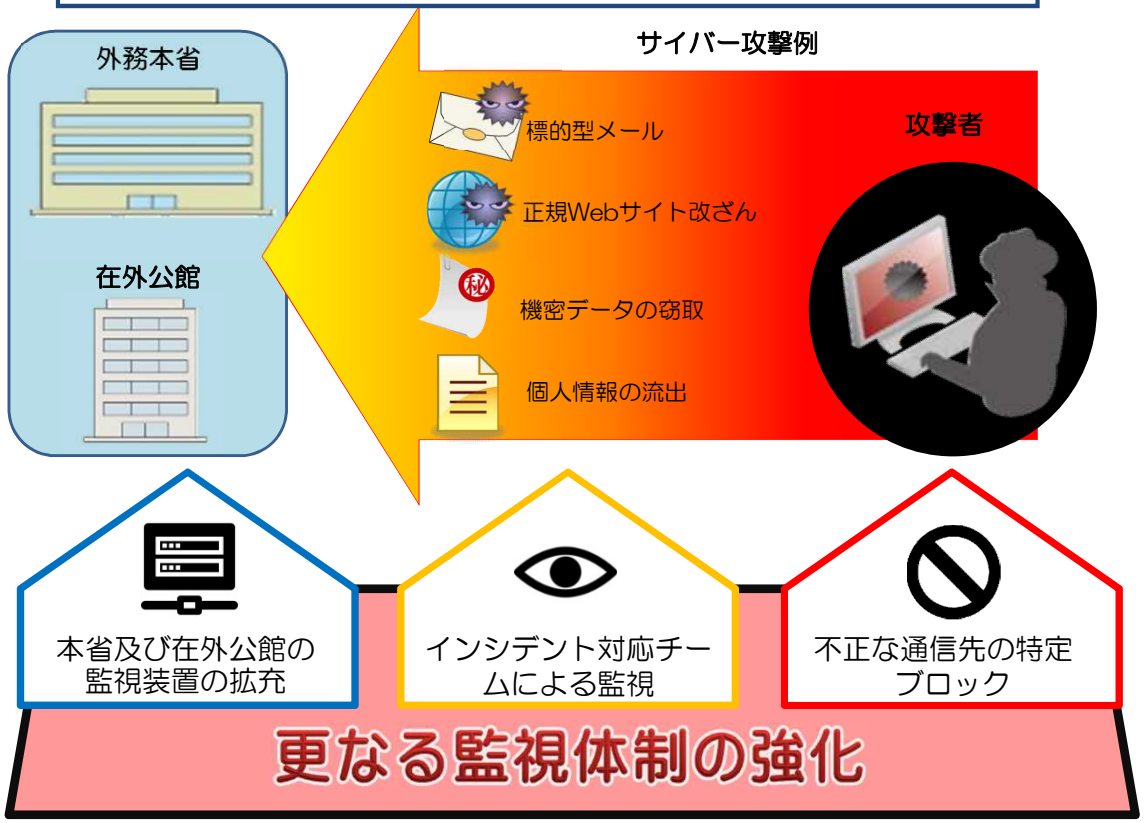
平成２８年度当初予算　：４．２億円
平成２９年度概算要求　：６．５億円

情報セキュリティ対策の強化

平成２９年度概算要求：６．３億円

事業概要･目的

○概要
　巧妙化・多用化するネットワークに対するサイバー攻撃対策を強化すると共に，更なる監視体制の強化を図る。



巧妙化・多様化するサイバー攻撃対策の強化及び更なる監視体制の強化

サイバー空間に関する外交及び国際連携

平成２９年度概算要求：０．２億円

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，国際的なルール作り，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

○産業系サイバーセキュリティ推進事業（IPA交付金）

平成28年度補正予算　：25.0億円
平成29年度当初予算　：8.0億円

- IPA（（独）情報処理推進機構）に「産業系サイバーセキュリティ推進センター（仮称）」を創設。世界的な専門人材を招聘し、攻撃対応演習等を実施。

演習のイメージ

①セキュリティ、ネットワーク、制御システムの基礎
ネットワークやシステム構築の演習

②多様な攻撃パターンへの対応訓練

③講師が作成したシナリオに基づく演習

④演習シナリオを研修員自らが作成、実践

○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年度補正予算：4.0億円
平成29年度当初予算：45.5億円（42.5億円）

- 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

IPA
②評価・分析

・重要インフラ　・石油
機器製造　・化学
・電力　・資源開発
・ガス　・公的機関　など

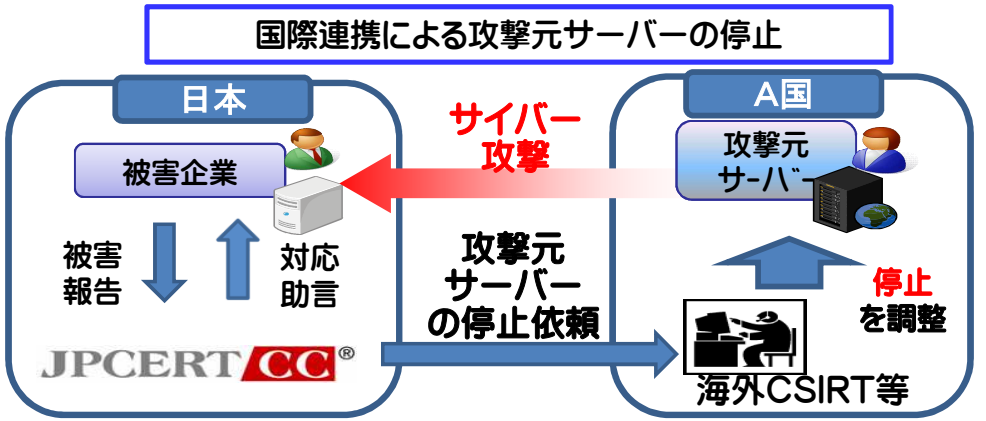
③対策方法の提案・実施・普及

○サイバーセキュリティ経済基盤構築事業

平成29年度当初予算：23.5億円（21.6億円）

- 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。

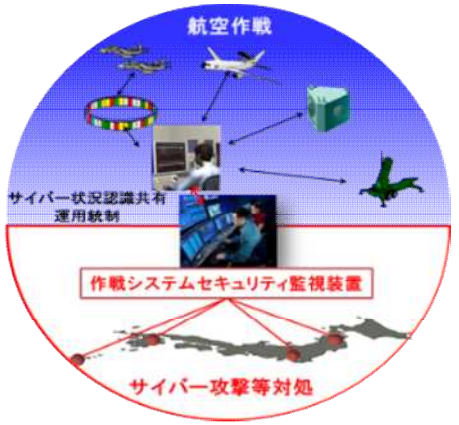


防衛省の施策例

作戦システムセキュリティ監視装置の整備

平成29年度当初予算　：　7億円

航空自衛隊の作戦システムに対するサイバー攻撃等を迅速に察知し、的確に対処するため、セキュリティ監視装置を整備



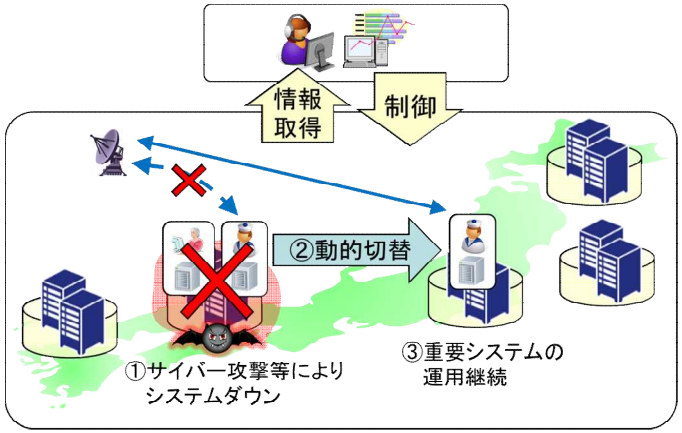
作戦システムセキュリティ監視装置（イメージ）

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

平成29年度当初予算　：　7億円

サイバー攻撃時においても、防衛省・自衛隊の情報通信基盤の運用継続を実現する研究を実施

※　サイバーレジリエンス：サイバー攻撃等によって指揮統制システムや情報通信ネットワークの一部が損なわれた場合においても、柔軟に対応して運用可能な状態に回復する能力



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（イメージ）

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・監督体制を拡充

平成28年度当初予算： 2.6億円、平成29年度概算要求：14.3億円、
平成29年度機構定員要求：新規増２名を含む22名を要求

○　監視・監督に係る業務体制の拡充

- 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

厚生労働省の施策例

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

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。

平成29年度当初予算：47．1億円、平成28年度補正予算：1．8億円

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）	人的対策 （意識改革、人材育成）	業務運営対策 （ルールの見直し、徹底）	技術的対策 （システムの強化）
• 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	• 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	• 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	• 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
■個人情報を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
■個人情報を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２９年度概算要求額：4.5億円（3.8億円）

（１）成長分野を支える情報技術人材の育成拠点の形成（enPiT）セキュリティ分野における人材育成

事業概要

- 産学連携による教育ネットワークを形成し、大学学部学生を主な対象として課題解決型学習（ＰＢＬ）等の実践的な教育を推進することで、セキュリティ分野の人材の育成機能を強化する。

【平成２９年度概算要求額：１.８億円※（1.5億円）】
（※成長分野を支える情報技術人材の育成拠点の形成（enPiT）の内数）

（参考）成長分野を支える情報技術人材の育成拠点の形成（enPiT）
【平成29年度概算要求額21.8億円（6.5億円）】
大学学部学生を主な対象とする人材育成の取組に加え、社会人学び直しを進めるため、現役IT技術者などを主な対象とした情報技術分野を中心とする体系的で高度な実践教育プログラムの開発・実施を推進する。

（２）高専における情報セキュリティ人材の育成

事業概要

- 企業等と連携し、情報セキュリティの教材開発や達成目標の構築を継続実施するとともに、平成28年度より新たに全国の高等専門学校学生がアクセス可能なサイバーレンジ（実践的な演習環境）の整備を進める。

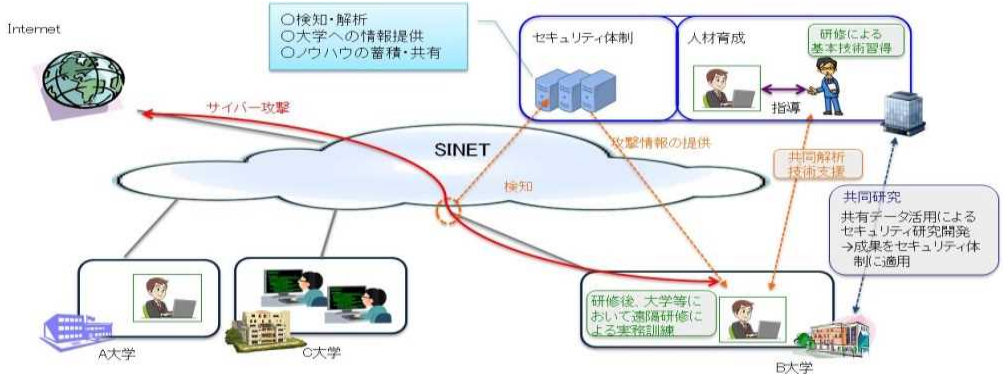
【平成２９年度概算要求：2.7※億円（ 2.3※億円）】
（※国立高等専門学校機構運営費交付金の内数）

○ 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（参考）

平成２９年度概算要求：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/ＩｏＴ/サイバーセキュリティ統合プロジェクト

平成29年度概算要求：96.4※億円（新規）
（※JST運営費交付金中の推計額含む）

- 理研AIPセンターにおいて、革新的な人工知能基盤技術の研究開発を推進するとともに、関係府省等と連携することで研究開発から社会実装までを一体的に実施。あわせて、JSTの戦略的創造研究推進事業において、人工知能等の分野における独創的な若手研究者や、新たなイノベーションを切り開く挑戦的な研究課題の支援を実施。
- その際、サイバーセキュリティに関する研究テーマも実施する。

金融庁の施策例

金融分野のサイバーセキュリティ対策強化

○ 金融業界横断的なサイバーセキュリティ演習の実施

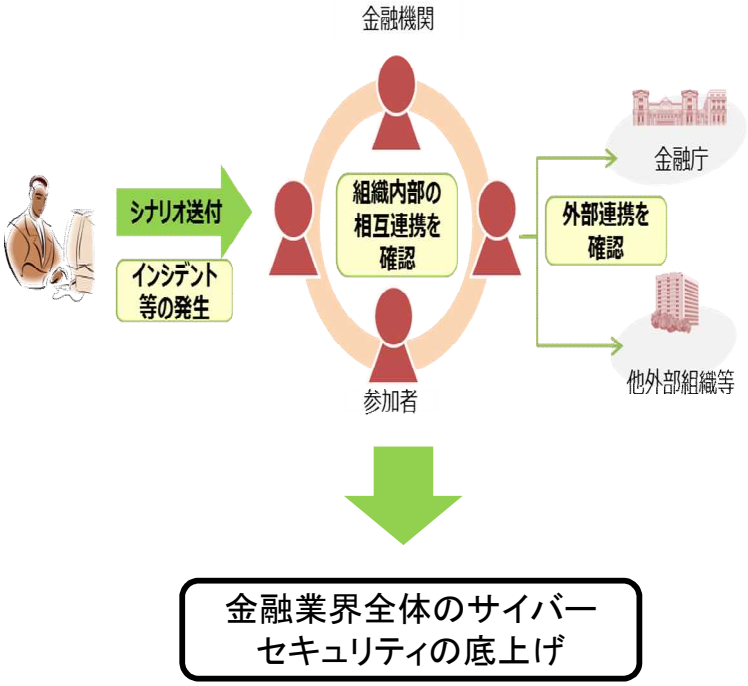
平成29年度当初予算：0.6億円（平成28年度当初予算：0.3億円）

事業概要

- 金融分野におけるサイバー攻撃の高度化が進む中、サイバーセキュリティの確保は、金融システム全体の安定のため喫緊の課題。
- 平成28年度より、「金融分野におけるサイバーセキュリティ強化に向けた取組方針」（27年７月公表）に基づき、金融業界全体のサイバーセキュリティの底上げを図るため、金融業界横断的な演習を実施。
- サイバー攻撃へ的確に対応するためには、演習を通じてサイバー攻撃への対応能力を向上させ、現在の対応態勢や手順の有効性を確認するなど、ＰＤＣＡサイクルを機能させることが重要。
- 29年度は、参加金融機関の対象や規模を拡充し実施する予定。

（注）本演習は、金融庁と参加金融機関の双方で負担（28年度、29年度）

演習概要

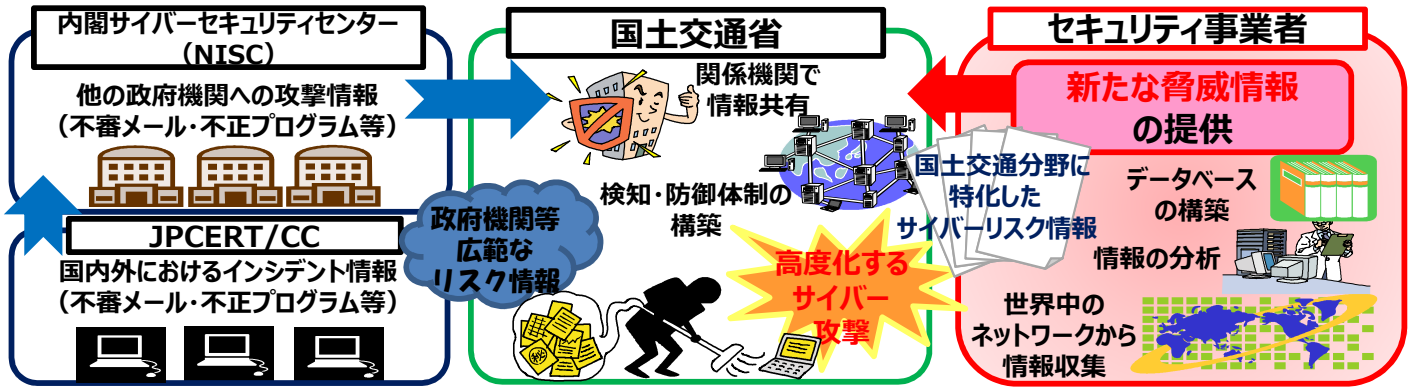


国土交通省の施策例

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 ○平成29年度当初予算要求額：２．２億円（平成28年度当初 0.3億円）

1．脅威情報収集・分析機能の強化

◆国土交通省や重要インフラ事業者をはじめとする国土交通省所管事業者の多くは、サイバー攻撃等によってIT障害が発生した際に国民の生命や社会経済活動に重大な影響を及ぼすおそれのあるシステムを運用している。
→サイバーセキュリティ戦略（閣議決定）に基づき、国土交通省所管の各分野に特化した脅威情報を入手し、カウンターサイバーインテリジェンスを含む、情報収集・分析機能の強化を図る。

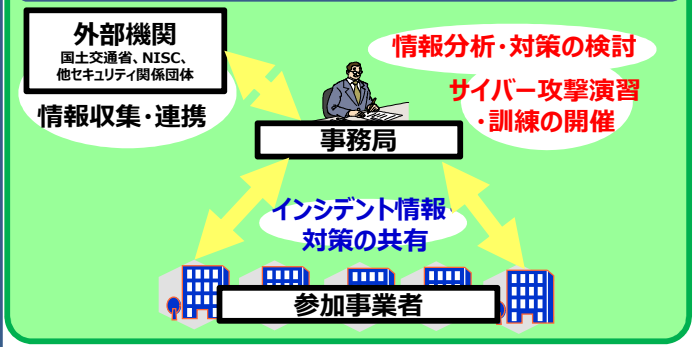


2．ISAC（アイザック）検討調査

◆重要インフラ事業者における情報セキュリティ対策を推進するため、国土交通分野における情報共有・分析及び対策を行う組織として、国土交通省所管重要インフラ分野におけるISACの創設の検討及び組織立ち上げの支援を行う。

ＩＳＡＣの役割

高度化・巧妙化していくサイバー攻撃に対し、同業種・業態の組織・人々が結集し、自ら組織を運営して脅威に対抗する



3.外部専門家の知見を活用した情報セキュリティ対策強化

◆2020年の東京オリンピック・パラリンピック競技大会に向けて、重要インフラ事業者に対するサイバー攻撃の高度化・巧妙化が想定されることから、外部専門家の知見を活用して、情報セキュリティインシデント発生時の支援・助言、リスク評価の実施等を行う。

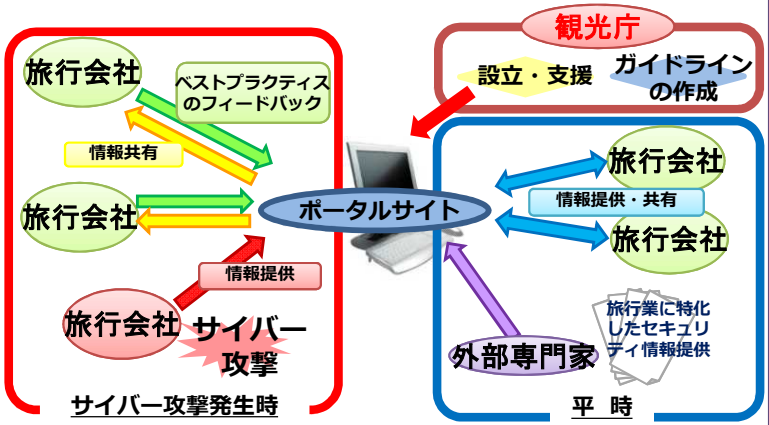
情報セキュリティ関係規定の作成等
○重要インフラ分野の安全ガイドラインの改正
○交通関連事業者等を対象としたセキュリティ対策マニュアル等の作成

情報セキュリティインシデントへの対応
○重要インフラ事業者等で情報セキュリティインシデントが発生した場合、事案の内容の把握・分析を行い、対応方針や再発防止策の策定等について支援及び助言を実施

情報セキュリティに関するコンサルティング
○重要インフラ事業者等への対策支援・助言、交通関連事業者等を対象とした講演会の実施
○2020年オリ・パラ東京大会に向けた重要インフラ事業者等へのリスク評価の実施

4．旅行業者における情報セキュリティ対策強化

◆旅行業者に対する相次ぐサイバー攻撃により、多数の個人情報漏えいの可能性が疑われており、また、2020年の東京オリンピック・パラリンピック競技大会に向けて、早急な対策が求められているため、旅行業者間でサイバーセキュリティ情報を共有するための仕組みの構築支援及び旅行業サイバーセキュリティガイドラインの作成・普及を図る。



5．オリパラに向けた情報セキュリティ対策強化

◆2020年の東京オリンピック・パラリンピック競技大会に向けて、各事業者等のサイバー攻撃に対する対処能力の強化を推進するため、大会の周辺環境を担うバス事業者、宿泊施設等の情報セキュリティ対策を調査し、調査結果から講ずべき情報セキュリティ対策のチェックリストを作成するとともに、事業者向けの講習会を実施する。