

政府のサイバーセキュリティに関する予算

資料 3

平成30年度予算政府案

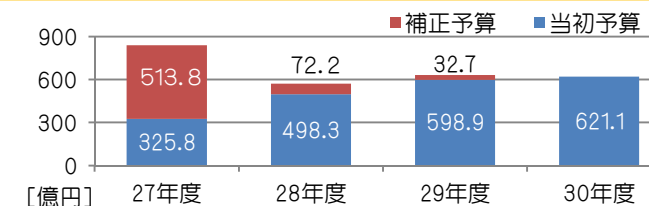
621.1億円

(平成29年度当初予算 598.9億円)

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30年度 予算政府案	平成29年度 補正予算案	平成29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	24.9億円	21.0億円	24.0億円
【警察庁】	サイバーテロ対策用資機材の増強等	5.9億円	—	4.1億円
【警察庁】	デジタルフォレンジック用資機材の増強等	4.4億円	—	1.5億円
【総務省】	ナショナルサイバートレーニングセンターの構築	15.1億円	—	15.0億円
【総務省】	IoTセキュリティ総合対策の推進	6.0億円	—	—
【総務省】	自治体情報セキュリティ対策の強化	0.5億円	—	3.3億円
【外務省】	情報セキュリティ対策の強化	7.2億円	—	6.1億円
【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	19.1億円	—	11.7億円
【経済産業省】	(独)情報処理推進機構(IPA)交付金	49.0億円	—	45.4億円
【経済産業省】	サイバーセキュリティ経済基盤構築事業	22.8億円	—	21.6億円
【防衛省】	移動系システムを標的としたサイバー攻撃対処のための演習環境整備に関する研究	27.9億円	—	—
【防衛省】	人工知能のサイバー・セキュリティへの応用に関する調査研究	0.8億円	—	—
【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・監督体制の拡充及び強化	11.8億円	—	13.3億円
【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	—	0.5億円
【文部科学省】	高等教育機関におけるセキュリティ人材の育成	11.7億円	—	11.0億円
【厚生労働省】	組織、ヒト、ルール、システムの観点から情報セキュリティ対策を強化	34.7億円	—	42.1億円
【国土交通省】	国土交通省CSIRT等や所管重要インフラ事業者における情報セキュリティ対策の強化	0.7億円	—	0.8億円



平成29年度補正予算案

32.7億円

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。

内閣サイバーセキュリティセンターの予算・体制

サイバーセキュリティ戦略

(平成27年9月4日 閣議決定)

サイバーセキュリティ戦略中間レビュー

(平成29年7月13日サイバーセキュリティ戦略本部決定)

内閣サイバーセキュリティセンター予算

平成30年度予算(案)

24.9億円

平成29年度補正予算(案)

21.0億円

<参考> 平成29年度当初予算額 24.0億円 <参考> 平成28年度第2次補正予算額 4.2億円

サイバー攻撃等に対する防御態勢の強化
(2020年オリパラに向けた態勢の整備)

○サイバーセキュリティ対処調整センター
及び情報共有システムの構築

0.3億円

○サイバーセキュリティ対処調整センター
及び情報共有システムの構築

10.5億円

○重要インフラ事業者等に係るリスク評価の
実施支援

6.5億円

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

6.9億円

○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

0.4億円

○各府省庁、独立行政法人、指定法人に
対する監査

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 等

2.9億円

○脅威予測等総合分析の実施 等

1.3億円

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調査 等

2.1億円

○サイバーセキュリティインシデントに係る調査 等

0.9億円

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

0.9億円

※ 平成30年度予算(案)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(2.8億円)を計上

NISCの体制強化

定員増 8人

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29年度当初予算 : 4. 1億円
平成30年度予算政府案 : 5. 9億円

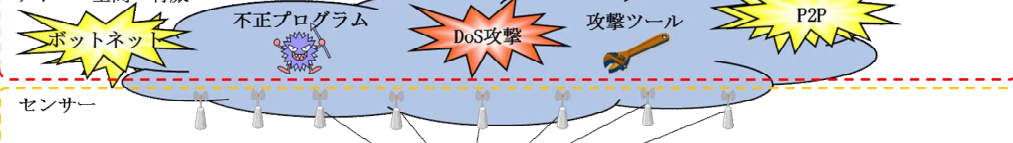
概要

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。

○ リアルタイム検知ネットワーク装置の更新・高度化

インターネット

サイバー空間の脅威



リアルタイム検知ネットワーク装置



観測機能

ボットネット観測

P2P観測

機能強化

定点観測

DoS攻撃観測システム

- 処理能力、ハードディスク等の資源を強化
- 情報技術の進展等に応じた観測機能の強化
- 新たなサイバー攻撃手法へ対応

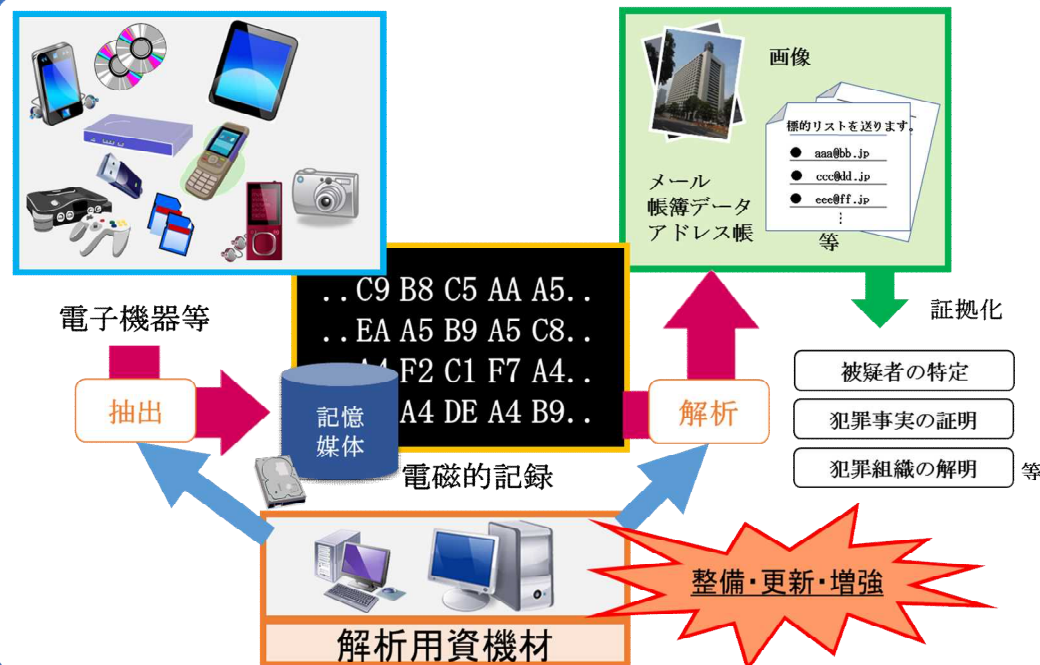
デジタルフォレンジック用資機材の増強等

平成29年度当初予算 : 1. 5億円
平成30年度予算政府案 : 4. 4億円

概要

効率的かつ効果的な捜査等に資するため、デジタルフォレンジック用資機材の増強整備等を行う。

○ 情報技術解析用資機材の増強整備等



- 都道府県警察が行うサイバー犯罪捜査において、電磁的記録の解析等の業務を処理
- 新たな情報通信技術を利用したサイバー犯罪に対応

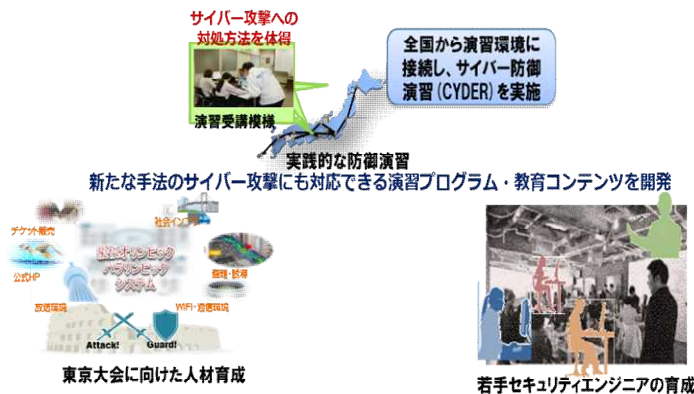
総務省の施策例

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の構築 15.1億円<平成30年度予算政府案>
 (2) IoTセキュリティ総合対策の推進 6.0億円<平成30年度予算政府案>
 (3) サイバー攻撃誘引基盤の構築 国立研究開発法人情報通信研究機構運営費交付金の内数<平成30年度予算政府案>

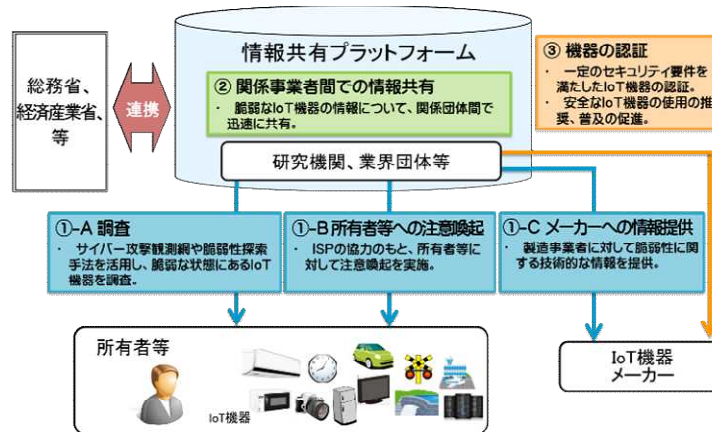
(1) ナショナルサイバートレーニングセンターの構築

- 国の行政機関、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



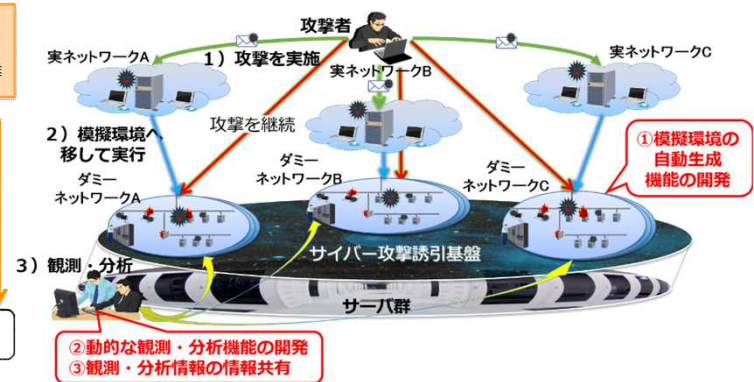
(2) IoTセキュリティ総合対策の推進

- 関係省庁、研究機関、業界団体等の関係主体が連携し、①脆弱なIoT機器の実態調査、注意喚起、②脆弱性情報の共有、③安全なIoT機器の普及促進、などを一体的に実施するIoTセキュリティ総合対策を推進



(3) サイバー攻撃誘引基盤の構築

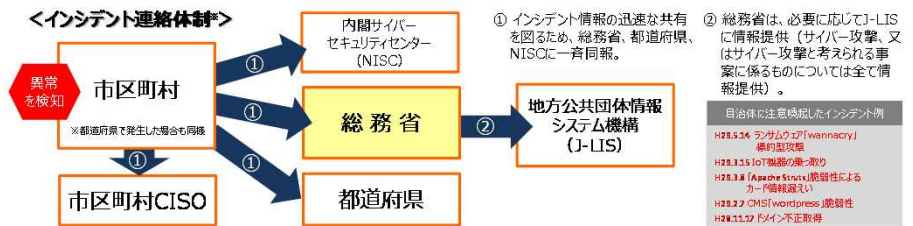
- 新たに出現する未知の標的型攻撃の挙動を早い段階で明らかにするとともに、分析結果をセキュリティ対策機関などと連携し情報共有を図るため、高度で効率的なサイバー攻撃誘引基盤を構築し、我が国のサイバーセキュリティ対策に貢献



自治体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に向けたインシデント対応支援 0.5億円<平成30年度予算政府案>

- サイバー攻撃は年々高度化しており、被害が拡大すると対応コストが甚大になる傾向があるため、最新の予防対策を講じる必要がある。具体的には、A)インシデント情報の収集・分析、B)インシデント対応マニュアルの継続的更新、C)有識者等と連携したQ&Aの検討、D)自治体職員に向けたセキュリティ講座、E)自治体への個別助言等を実施。



管理運用している事業・体制	対象とする団体	事業分類	事業概要
※ インシデント連絡体制 (H28改定)	47都道府県 1,741市区町村	体制	・インシデント発生時の報告体制 (担当者、書式、ルート) ・自治体でインシデント発生した際、総務省や内閣サイバーセキュリティセンター (NISC) へ報告 ・NISCや総務省で自治体のリスクを検知した際、総務省を通じて自治体への注意喚起
情報セキュリティ支援プラットフォーム (H27～)	47都道府県 1,741市区町村	体制	・自治体からセキュリティ専門人材に相談表を使用してオンラインでQ&Aが出来る仕組み。 ・セキュリティ専門人材は、セキュリティベンダー等20社から48名が登録 (H29.8現在)。
情報セキュリティ向上プラットフォーム (H29～)	構築中 (最大47都道府県 1,741市区町村が利用可能)	システム	・LGWANに接続された自治体のシステムや端末にインストールされているOSやウイルス対策ソフトに対してセキュリティパッチやウイルスパターンファイル等を配信する仕組み。

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30年度予算政府案：7.2億円

事業概要・目的

○概要

高度化するサイバー攻撃に対処するため、検知能力・監視能力等を強化するとともに、体制面においても増強を図る。

インシデント対応
チームによる
監視・分析・対処



エンドポイントの
セキュリティ強化



フォレンジック機器
やメール攻撃対策
システムの導入



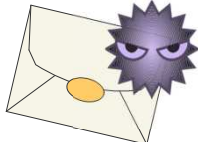
攻撃者



不正サイト



不審メール



平成29年度当初予算：6.2億円

平成30年度予算政府案：7.3億円

サイバー空間に関する外交及び国際連携

平成30年度予算政府案：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、国際的なルール作り、安全保障面での課題の検討、各国との連携、信頼醸成等に取り組んでいく。

○国際会議

- ・サイバーセキュリティ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30年度予算案:19.1億円(11.7億円)

- IPA((独)情報処理推進機構)に設置する産業サイバーセキュリティセンターにおいて、模擬プラントを用いた演習等を通じ、サイバーセキュリティの中核人材を育成。海外から専門家を招致するなど、海外の知見を活用。

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

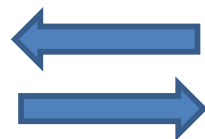
○情報セキュリティ対策促進・IT製品の評価・認証等(IPA交付金)

平成30年度予算案:49.0億円(45.4億円)

- 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



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

③対策方法の提案・実施・普及

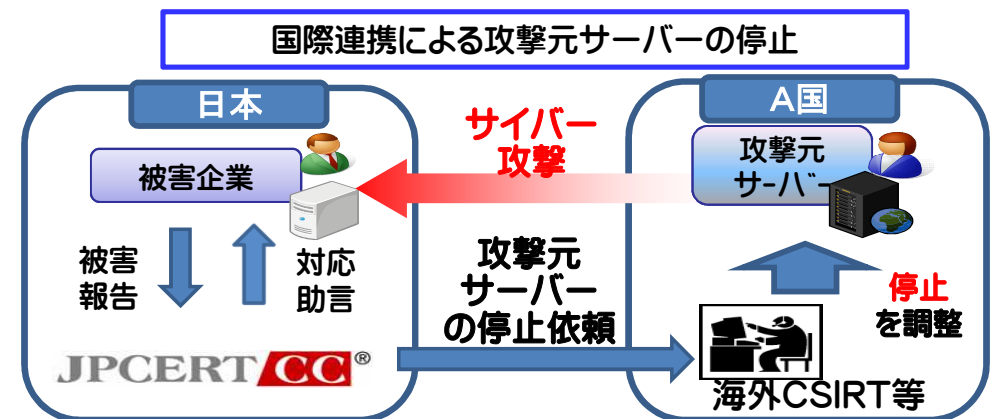
○サイバーセキュリティ経済基盤構築事業

平成30年度予算案:22.8億円(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。

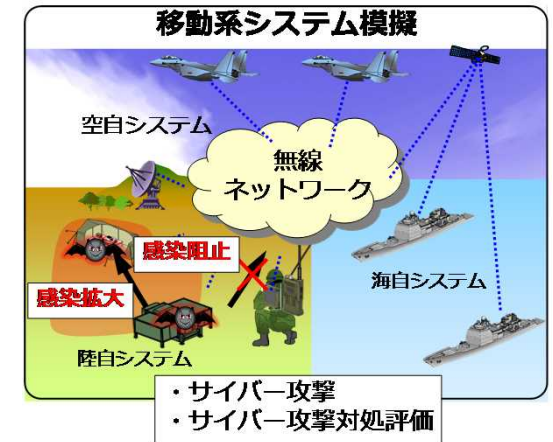


防衛省の施策例

移動系システムを標的としたサイバー攻撃対処のための演習環境整備に関する研究

平成30年度予算政府案 : 27.9億円

防衛省・自衛隊の移動系システムを標的にしたサイバー攻撃への効果的な対処手法の検討・評価に資する、移動系サイバー攻撃対処技術に関する研究を実施

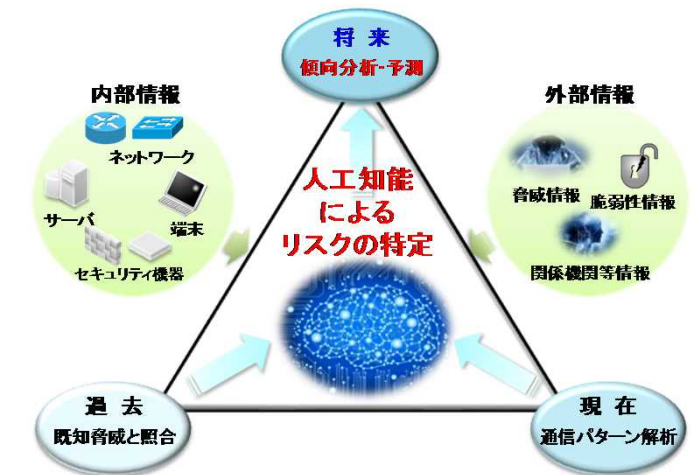


移動系システムを標的としたサイバー攻撃
対処のための演習環境整備に関する研究
(イメージ)

人工知能のサイバー・セキュリティへの応用に関する調査研究

平成30年度予算政府案 : 0.8億円

サイバー防衛隊による防御の実効性を高めるため、深層学習等のサイバー・セキュリティへの応用に関して調査し、防衛省のネットワーク防御に人工知能を活用したソフトウェア等を応用するための調査研究を実施



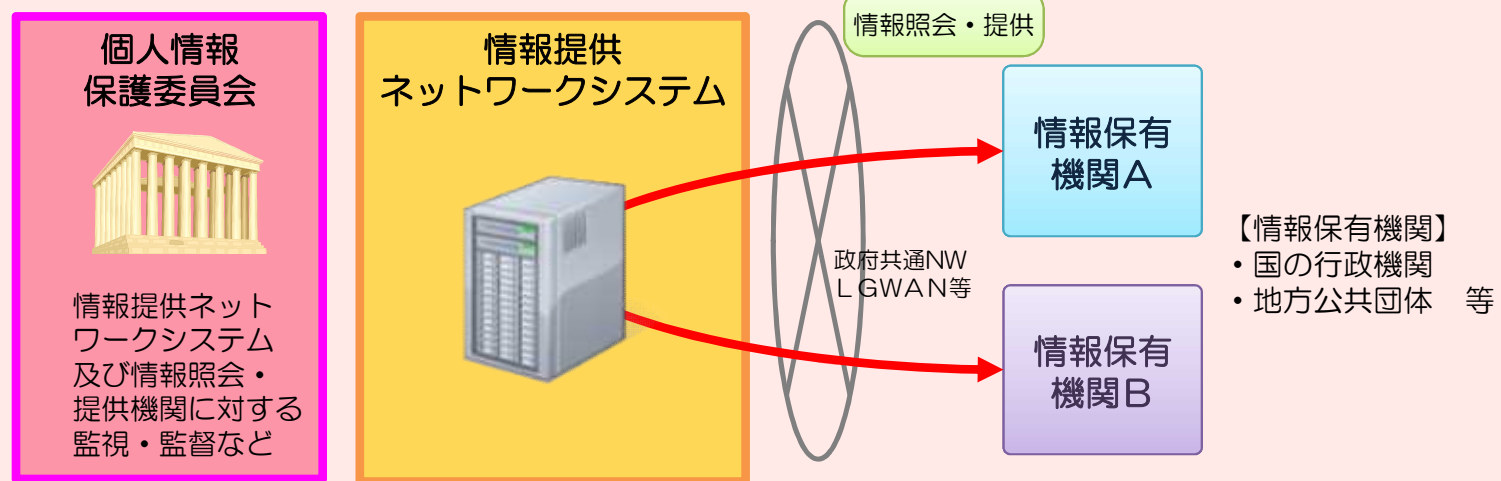
人工知能のサイバー・セキュリティへの
応用に関する調査研究(イメージ)

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・監督体制を拡充及び強化

平成29年度当初予算：13.3億円、平成30年度政府案：11.8億円
平成30年度機構定員：新規増2名を含む3名の増員

○ 情報提供ネットワークシステムに係る監視・監督体制の整備



○ 監視・監督に係る業務体制の拡充及び強化

- ・ 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
- ・ 報告徴収・立入検査等により入手した情報の活用

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

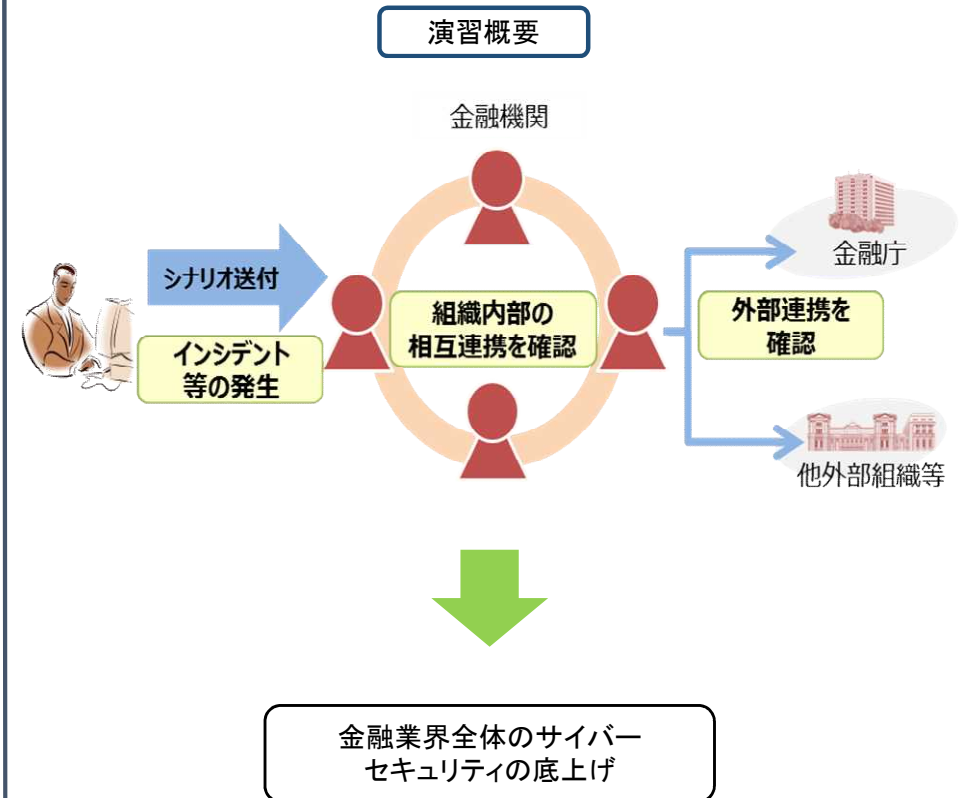
○ 金融業界横断的なサイバーセキュリティ演習の実施

平成30年度予算政府案：0.5億円（平成29年度当初予算：0.5億円）

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。
- 「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、金融業界全体のインシデント対応能力の更なる向上を図るため、平成29年度、2回目の「金融業界横断的な演習」（Delta Wall II）を実施。
（参考）平成29年度演習においては、中小金融機関の底上げを目的に、参加金融機関の参加枠および対象業態を拡充のうえ、約100先が参加（前回は77先）。
- サイバー攻撃への的確に対応するためには、演習を通じて、現在の対応態勢が十分であることを確認するなど、PDCAサイクルを回しつつ、対応能力を向上させることが有効。
- 金融分野のサイバーセキュリティ強化には、官民が一体になって取り組んでいくことが重要であり、平成30年度も、引き続き演習を実施予定。

（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）



厚生労働省の施策例

組織、ヒト、ルール、システムの観点から情報セキュリティ対策を強化

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30年度予算政府案:34.7億円

情報セキュリティ対策強化の4つの視点

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層防御の取組
- 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

- 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
- 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(関係機関を含む)
- 組織体制、保有するシステム等に対する情報セキュリティ監査の実施
- 医療分野におけるサイバーセキュリティ対策の実態調査

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
- 情報管理対策本部・機構CSIRTの体制強化
- 年金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
- 情報セキュリティ対策(技術面)に対する情報セキュリティ監査の実施

国土交通省の施策例

○国土交通省CSIRT等や所管重要インフラ事業者における 情報セキュリティ対策の強化

平成30年度予算政府案：0.7億円
(平成29年度当初予算：0.8億円)

1. 国土交通省CSIRT(注1)の強化等を行うことにより、当省における情報セキュリティインシデントへの対応能力等の向上を図る

- 情報セキュリティ体制強化支援業務 (外部専門家による国土交通省CSIRT等の支援) 等

(注1) Computer Security Incident Response Teamの略。国土交通省における情報セキュリティインシデントに対処するための組織。

2. 所管する重要インフラ事業者(航空、鉄道、物流)が情報の共有・分析や対策を連携して行う体制(「交通ISAC」(仮称))(注2)の創設に向けた検討を支援する

- ISAC検討調査業務

(注2) Information Sharing and Analysis Centerの略。

