政府のサイバーセキュリティに関する予算

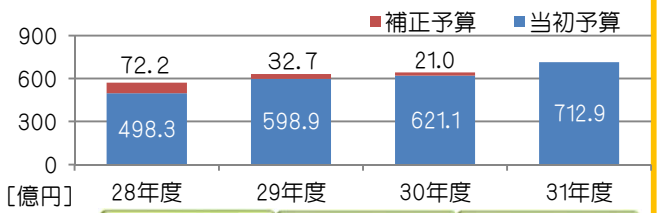
資料7

平成31年度予算政府案

712.9億円

（平成30年度当初予算　621.1億円）

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31年度予算政府案	平成30年度補正予算案	平成30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	13.0億円	24.9億円
【警察庁】	サイバー攻撃対策に係る資機材の整備等	3.3億円	―	1.1億円
【警察庁】	デジタルフォレンジック用資機材の増強等	4.5億円	―	5.9億円
【総務省】	IoTの安心・安全かつ適正な利用環境の構築	14.6億円	―	―
【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	14.9億円	―	15.1億円
【総務省】	自治体情報セキュリティ対策の強化	1.0億円	―	0.5億円
【外務省】	情報セキュリティ対策の強化	5.9億円	―	7.2億円
【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】	サイバー・フィジカル・セキュリティ対策促進事業	3.5億円	―	―
【経済産業省】	サイバーセキュリティ経済基盤構築事業	21.0億円	―	22.8億円
【経済産業省】	産業系サイバーセキュリティ推進事業	19.3億円	―	19.1億円
【防衛省】	航空作戦システムのサイバーセキュリティ対策の強化	4.4億円	―	―
【防衛省】	情報システムのサプライチェーン・リスク対処に関する調査研究	0.9億円	―	―
【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	11.7億円	―	11.8億円
【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	―	0.5億円
【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	10.4億円	―	12.1億円
【厚生労働省】	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情報システム構築に向けた取組	40.4億円	―	36.7億円
【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	0.5億円	―	0.7億円

平成30年度補正予算案

21.0億円

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

サイバーセキュリティ基本法
（平成３０年１２月５日 改正）

サイバーセキュリティ戦略
（平成３０年７月２７日 閣議決定）

サイバーセキュリティ関係施策に関する
平成31年度予算重点化方針
（平成３０年７月25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３１年度予算政府案	平成３０年度第２次補正予算案
２４．９億円	１３．０億円
＜参考＞平成３０年度当初予算２４．９億円	＜参考＞平成２９年度補正予算２１．０億円

	平成３１年度予算政府案	平成３０年度第２次補正予算案
2020年東京大会とその後を見据えた取り組み	○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運用 ３．０億円 ○重要インフラ事業者等に係るリスク評価の実施支援等 ０．１億円	○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運用 ０．９億円 ○重要インフラ事業者等に係るリスク評価の実施支援等 ６．３億円
政府機関等におけるセキュリティ強化・充実	○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 ８．４億円 ○各府省庁、独立行政法人、指定法人に対する監査 ５．１億円 ○サイバーセキュリティインシデントに係る調査 ０．８億円	○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 ０．６億円 ○各府省庁、独立行政法人、指定法人に対する監査 ２．０億円 ○サイバーセキュリティインシデントに係る調査 ０．７億円 ○政府機関等における情報システムのセキュリティ対策の高度化に向けた検討 １．２億円
大規模サイバー攻撃事態等への対処態勢の強化	○脅威予測等総合分析の実施 ０．５億円 ○重要インフラ分野横断的演習企画実施支援　等 ０．７億円	
従来の枠を超えた情報共有・連携体制の構築	○インシデント対応のための連絡調整及びCSIRT機能の構築・運用 ０．８億円	
人材育成・確保、普及啓発	○セキュリティ・IT人材へのサイバーセキュリティ研修 ０．１億円 ○緊急情報発信・意識啓発の方策の強化 ０．３億円	○緊急情報発信・意識啓発の方策の強化 ０．５億円
国際協力・連携	○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	

※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として、４．３億円（平成３１年度予算政府案）、０．８億円（平成３０年度第２次補正予算案）を計上

警察庁の施策例

サイバー攻撃対策に係る資機材の整備等

平成30年度当初予算　：１．１億円
平成31年度予算政府案：３．３億円

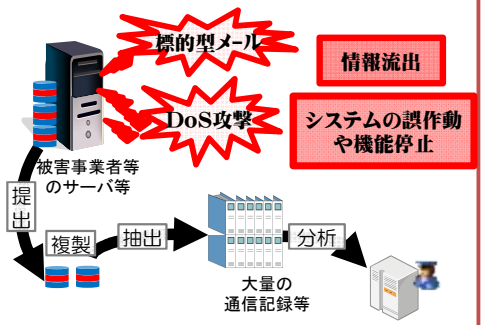
概要

サイバー攻撃への対処や情報収集・分析を行うため、サイバー攻撃対策に関わる資機材の増強整備等を行う。

○ 事案対処能力、情報収集・分析の強化

事案対処能力の強化

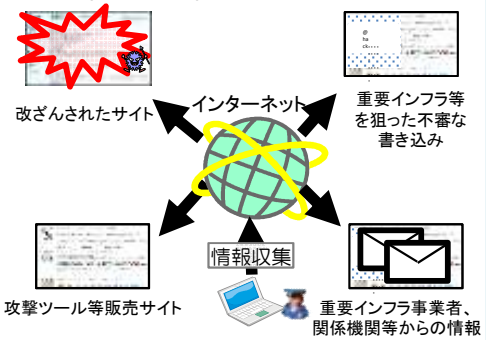
サイバー攻撃事案発生時の初動対処を迅速に実施し、被害の拡大防止を図るため事案対処用の資機材を更新・増強



資機材の更新・増強

情報収集の強化

インターネット上や関係機関等からのサイバー攻撃に関する情報収集を強化し、サイバー攻撃の早期把握・被害の防止を図るための情報収集用端末を更新・増強



情報収集用端末の更新・増強

分析機能の強化

高度化するサイバー攻撃に対応するため、現行のサイバー攻撃分析センター用装置を更新し、セキュリティベンダーの提供サービスと連携し、分析機能を強化

○ サイバー攻撃事案発生時の迅速・的確な対応
○ 早期の実態解明、不審情報発見による被害拡大防止

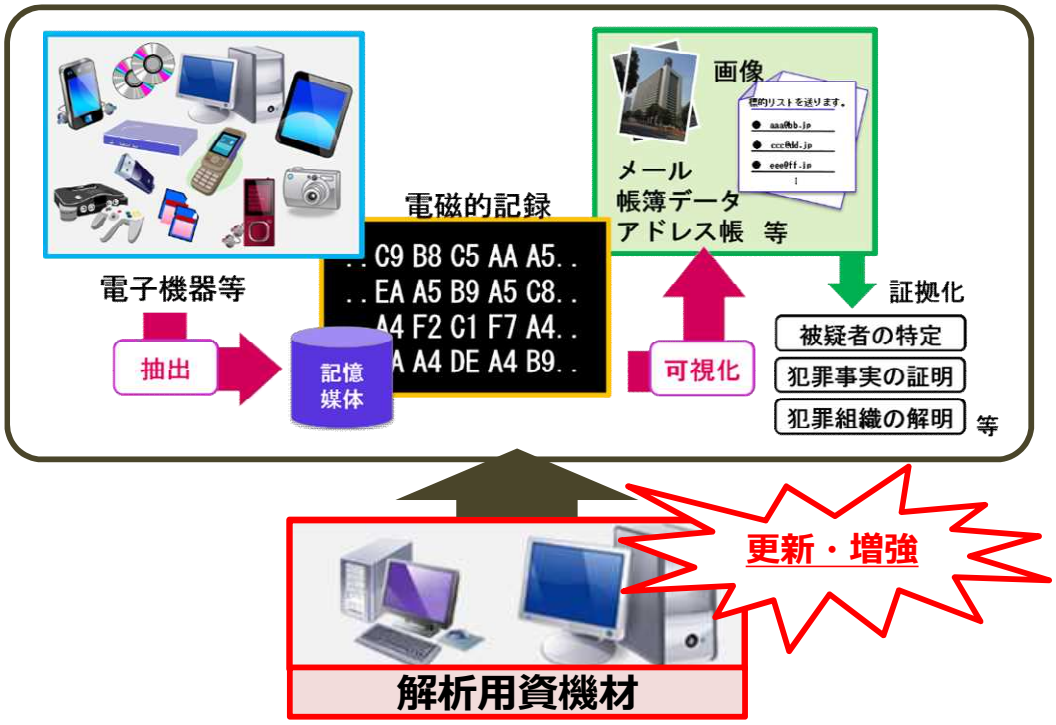
デジタルフォレンジック用資機材の増強等

平成30年度当初予算　：５．９億円
平成31年度予算政府案：４．５億円

概要

効果的かつ効率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更新・増強



○ 都道府県警察が行うサイバー犯罪捜査に対して、電磁的記録等の解析を実施
○ 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

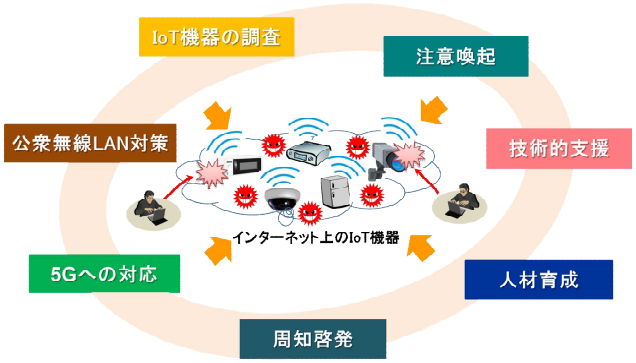
IoTへの信頼を支えるサイバーセキュリティ総合対策

【主な経費】 (1) IoTの安心・安全かつ適正な利用環境の構築　14．6億円<平成31年度予算政府案>
(2) サイバーセキュリティ情報共有推進事業　3．4億円<平成31年度予算政府案>
(3) ナショナルサイバートレーニングセンターの構築　14．9億円<平成31年度予算政府案>

我が国のサイバーセキュリティを強化し、安心・安全な国民生活や社会経済活動を確保

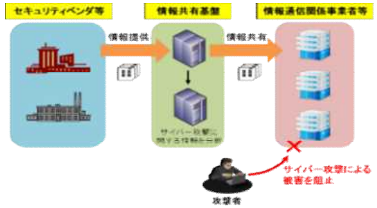
（１）IoTの安心・安全かつ適正な利用環境の構築

・ IoTに係るサイバーセキュリティ対策の強化等のため、(a)IoTセキュリティ対策の推進、(b)地域におけるIoTセキュリティ対策の強化、(c)５Gネットワークのセキュリティ確保に向けた体制整備と周知・啓発等を実施

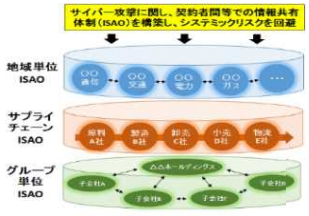


（２）サイバーセキュリティ情報共有推進事業

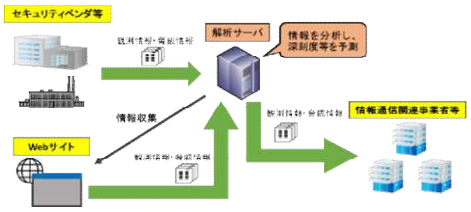
・ サイバー攻撃に関する情報の共有を促進するため、(a)情報共有基盤の高度化、(b)機械学習を用いた高精度な信頼性・深刻度評価を行う実証、(c)契約者間等で情報を共有する体制の構築に向けた取組を実施



情報共有基盤の高度化



契約者間等で情報を共有する体制の構築



機械学習を用いた信頼性・深刻度評価

（３）ナショナルサイバートレーニングセンターの構築

・ NICTのナショナルサイバートレーニングセンターにおいて、実践的な対処能力を持つセキュリティ人材の育成を実施

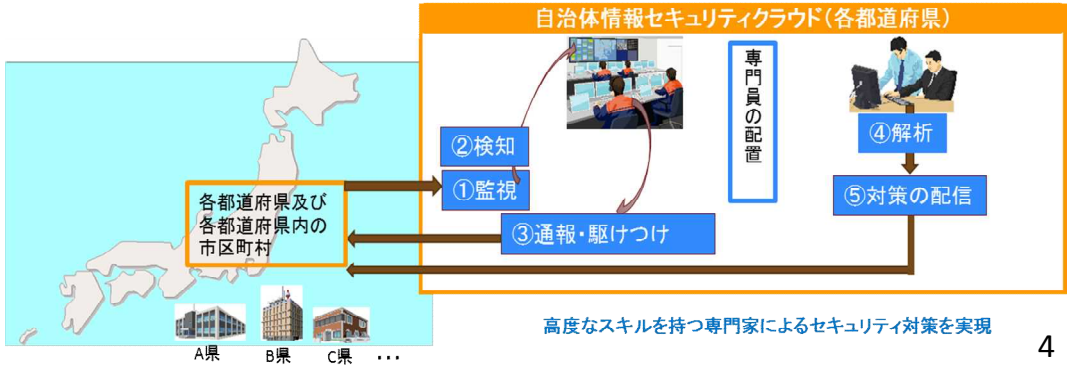
サイバーコロッセオ

SecHack365

自治体情報セキュリティ対策の強化

【主な経費】 集中型の新たなセキュリティクラウドの仕組等自治体情報セキュリティ対策　1．0億円 <平成31年度予算政府案>

○ 地方公共団体においては、「三層の対策」により情報セキュリティの強化が図られたところであるが、これを踏まえた情報セキュリティ対策を更に推進していくため、自治体行政の標準化・共通化を見据えた集中型の新たなセキュリティクラウドの仕組やセキュリティレベルを維持しつつ、操作性の向上を図ることのできる新しい技術の適用等に関する調査研究を実施



高度なスキルを持つ専門家によるセキュリティ対策を実現

外務省の施策例

外務省サイバーセキュリティ施策

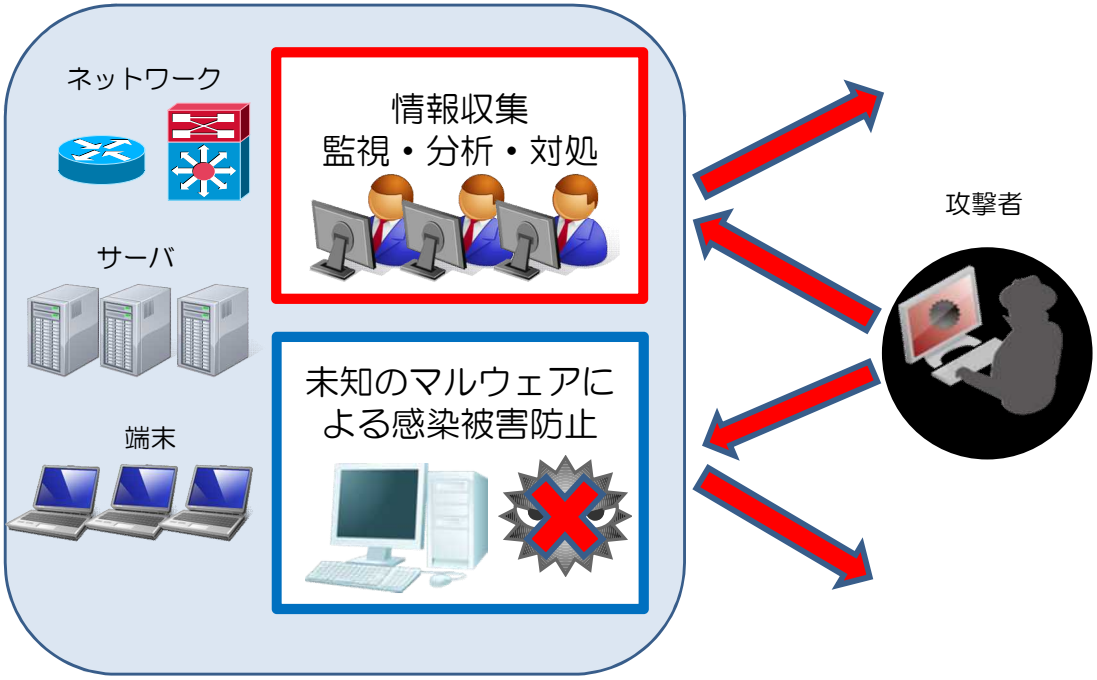
平成３０年度当初予算　　：７．３億円
平成３１年度予算政府案　：６．０億円

情報セキュリティ対策の強化

平成３１年度予算政府案：５．９億円

事業概要･目的

〇概要
　サイバーセキュリティ戦略本部において，「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（平成30年度版）」が決定されたところ，同統一基準群を踏まえ，防御能力の向上を図っていく。



サイバー空間に関する外交及び国際連携

平成３１年度予算政府案：０．１億円

事業概要･目的

〇概要
　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。

〇国際会議
　･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

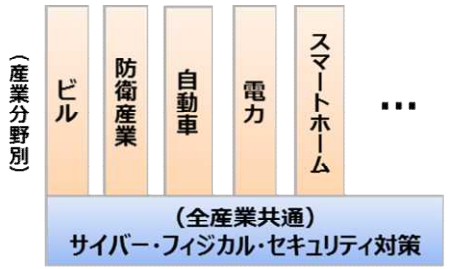
経済産業省のサイバーセキュリティ施策

（（）内の金額は30年度当初予算額）

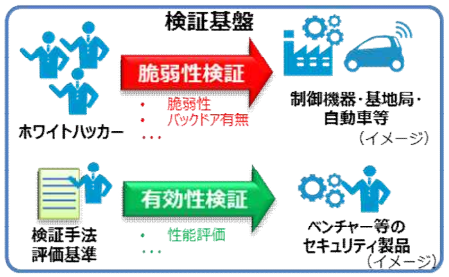
○サイバー・フィジカル・セキュリティ対策促進事業
平成31年度予算政府案　：　3.5億円（新規）

・産業分野別のサイバー・フィジカル・セキュリティ対策に関するガイドラインの策定、情報共有の仕組みの検討等を推進。

・我が国の状況に応じたサイバーセキュリティビジネスのエコシステムを構築するために、実戦的サイバーセキュリティ検証基盤を整備。



産業分野別の対策検討（イメージ）

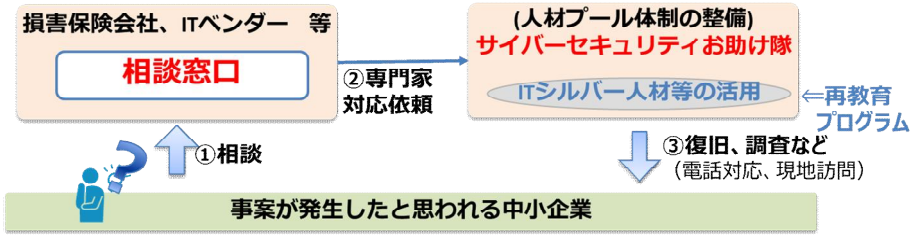


実戦的サイバーセキュリティ検証基盤構築(イメージ)

○中小企業等強靭化対策事業
平成30年度第2次補正予算案　：　**15.0億円の内数**

・中小企業に対し、セキュリティ対策の普及啓発を行うとともに、専門家を派遣して、マネジメント指導を実施。

・サイバー攻撃によるトラブル時に相談対応や現場派遣を担う支援サービスの提供体制を整備するなど、ニーズに沿ったセキュリティ技術・サービスの実証事業を実施。

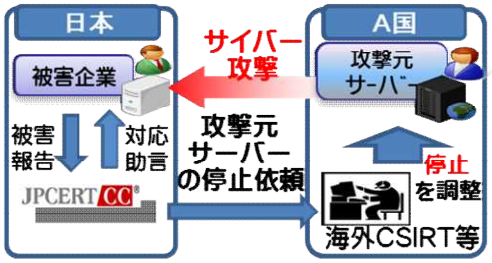


支援サービスモデル（サイバーセキュリティお助け隊）

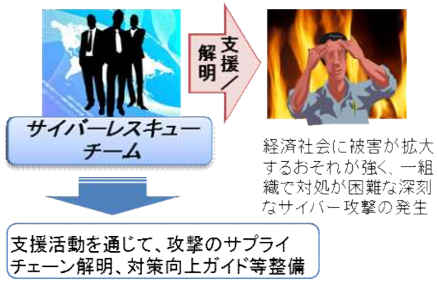
○サイバーセキュリティ経済基盤構築事業
平成31年度予算政府案　：　21.0億円（22.8億円）

・各国の攻撃情報の集約・対応を行う機関（窓口CSIRT）との連携により、国際的なサイバー攻撃基盤を共同駆除する活動の支援。

・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対する初動対応を行う独立行政法人情報処理推進機構（IPA）の「サイバーレスキュー隊」の運営。



国際連携による攻撃対処



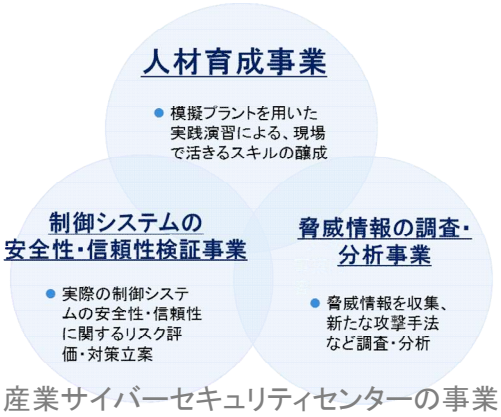
サイバーレスキュー隊の活動

○セキュリティに係る情報共有や対策促進（IPA交付金）
平成31年度予算政府案　：　46.0億円の内数（49.0億円の内数）

・重要インフラ事業者や企業等に対するサイバー攻撃による被害の未然防止や低減を図るための情報共有基盤の運営やサイバーセキュリティ経営支援ツールの整備を推進。

○産業系サイバーセキュリティ推進事業（IPA交付金）
平成31年度予算政府案　：　19.3億円（19.1億円）

• IPA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、米国等との国際連携により、情報システムと制御システムの両方に精通したサイバーセキュリティの中核人材の育成や制御システムセキュリティの強化を支援。



産業サイバーセキュリティセンターの事業

防衛省の施策例

航空作戦システムのサイバーセキュリティ対策の強化

平成31年度予算政府案　：　4.4億円

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

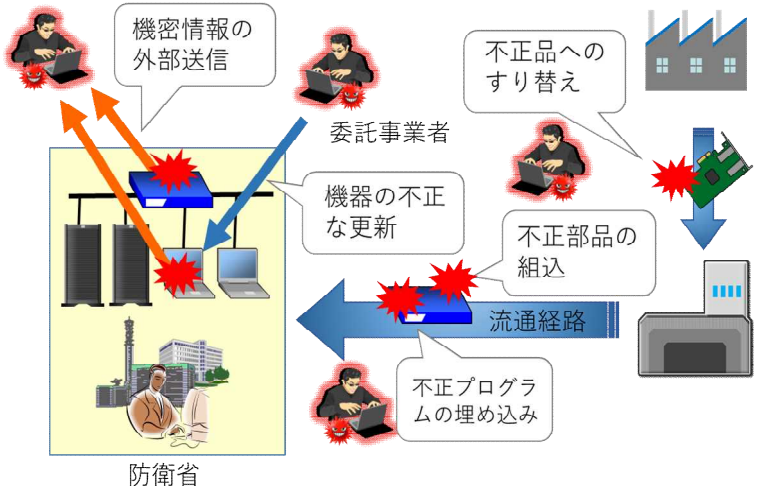
作戦システムセキュリティ監視装置（イメージ）

情報システムのサプライチェーン・リスク（※）対処に関する調査研究

平成31年度予算政府案　：　0.9億円

不正なチップやソフトウェアをサプライチェーンにおいて混入される等の攻撃に対し、それらを検知し排除するための手法・対策について調査・研究を実施

※　サプライチェーン・リスク：発注者へ情報システムや機器等が納入されるまでの開発や製造に係る一連の工程に加えて、当該情報システムや機器等の運用・保守・廃棄を含むライフサイクル全体に存在するリスク



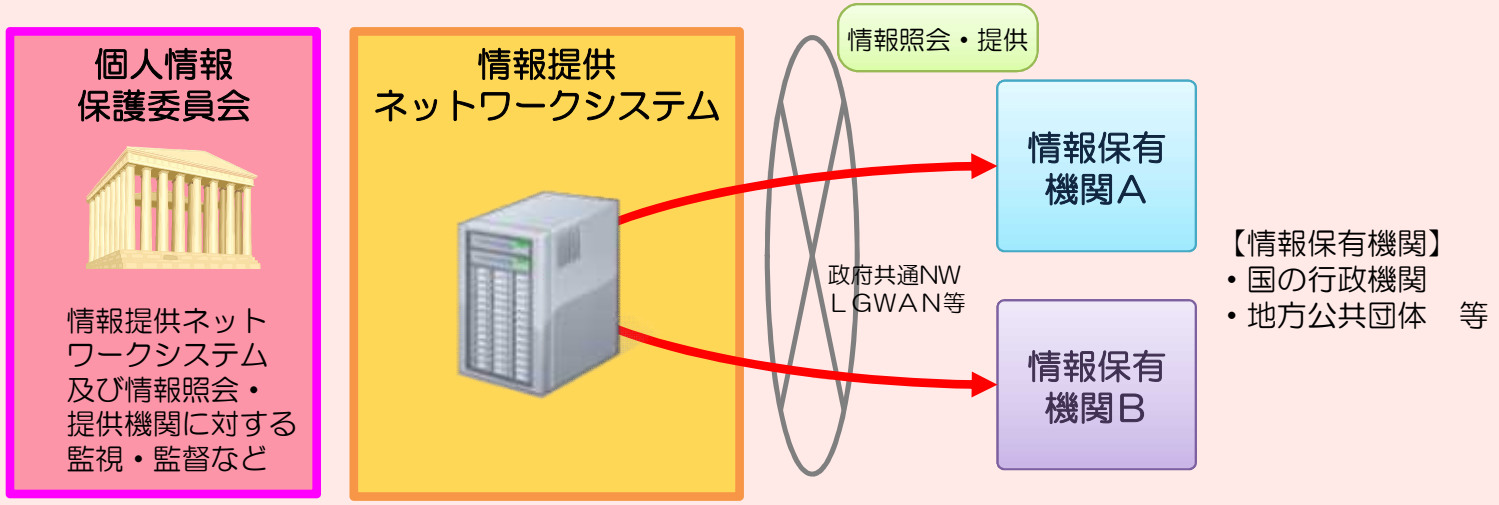
情報システムのサプライチェーン・リスク（イメージ）

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31年度予算政府案：11.7億円
平成31年度機構定員：新規4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

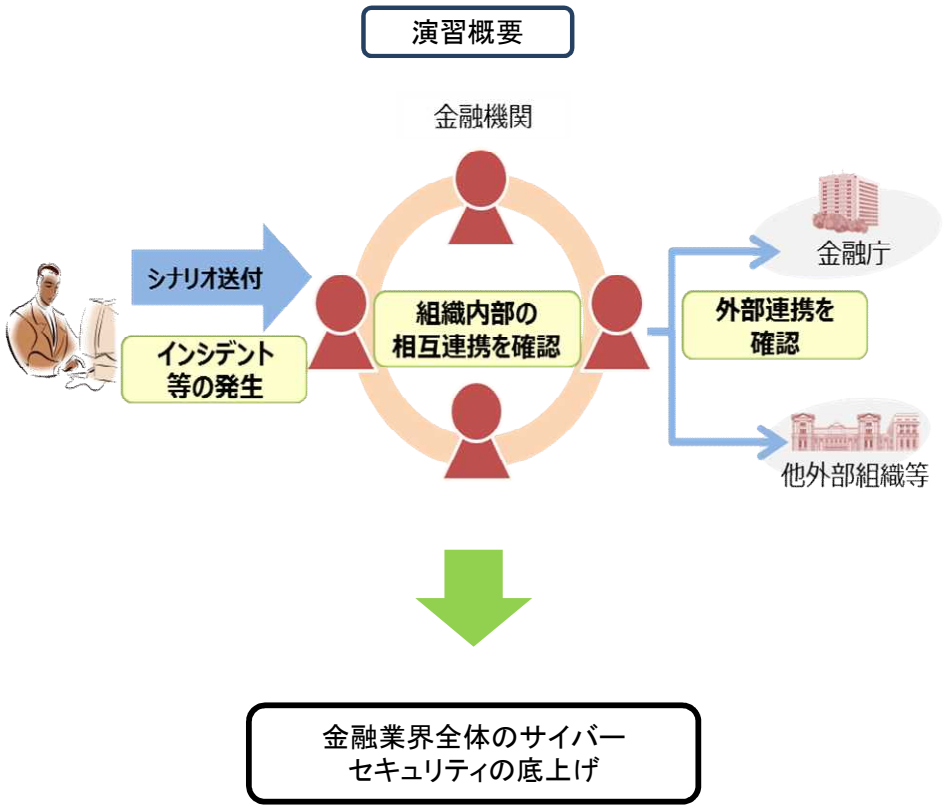
平成31年度政府予算案：0.6億円（平成30年度当初予算：0.5億円）

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月策定・30年10月改訂）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30年度、３回目の「金融業界横断的な演習」（Delta Wall Ⅲ）を実施。

  （参考）平成30年度演習においては、中小金融機関の底上げを目的に、参加金融機関の対象業態を拡充のうえ、約100先が参加。

- サイバー攻撃へ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かを確認するなど、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31年度も、引き続き演習を実施予定。



文部科学省の施策例

高等教育機関におけるセキュリティ人材の育成

○Society 5.0に対応した高度技術人材育成事業
成長分野をさせる情報技術人材の育成拠点の形成（enPiT）

【平成31年度予算政府案：7．4億円（8．1億円）】

事業概要

産学連携による課題解決型学習(PBL)等の実践的な教育の推進により、大学における情報技術人材の育成強化を目指す。

○国立高専における情報セキュリティ人材の育成

【平成31年度予算政府案：4．0億円（4．0億円）】

事業概要

サイバーセキュリティに関する知識やスキルの習得に加え、高い倫理観やITリテラシーを習得する教材・教育プログラムの展開と、社会ニーズを踏まえた実践的な演習環境の高度化を図る等、教育環境を整備することにより、情報セキュリティ人材の育成を推進する。

大学等に対する研修・実践的な演習

【平成31年予算政府案：0．3億円（0．2億円）】

事業概要

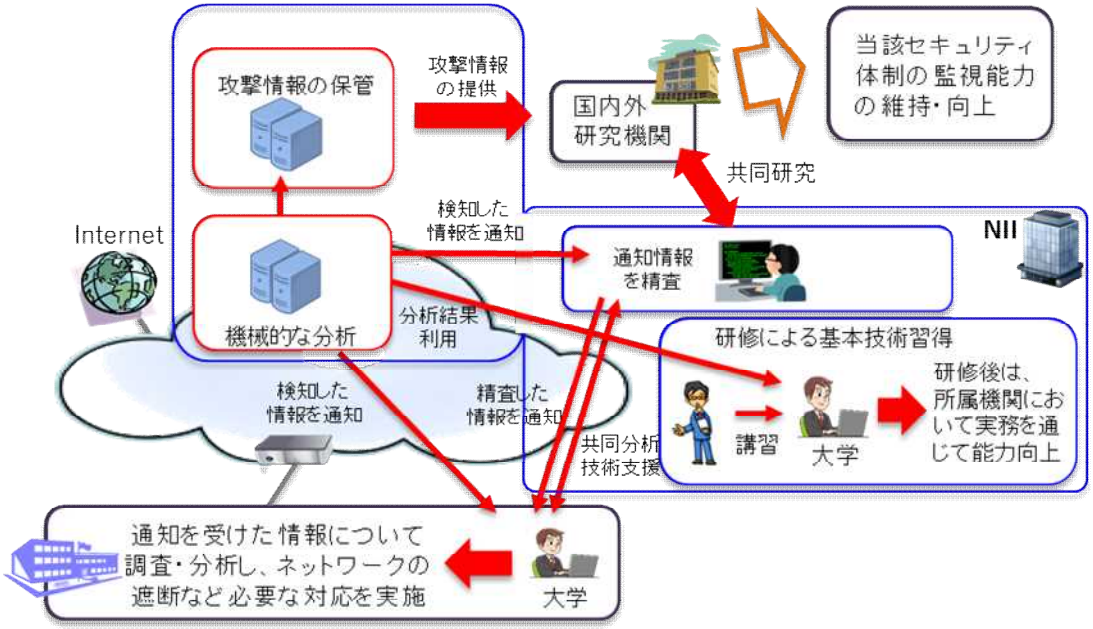
大学等のCISO、戦略マネジメント層、CSIRT構成員、情報セキュリティ監査担当者等に対して、統一基準群やポリシー等のマネジメントに関わる知識、サイバー攻撃に係る攻撃手法と防御方法、情報セキュリティインシデントへの対応等に関する研修や実践的な演習を行う。

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31年度予算政府案：国立大学法人運営費交付金の内数（8．2億円）】

事業概要

・国立大学法人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等の連携に基づき、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整備する。
・国立大学法人等で発生したサイバー攻撃の情報をもとに匿名化を施したベンチマークデータを作成し、セキュリティ対策の研究や取組の高度化に活用する。



注：（）内の金額は平成30年度予算額

厚生労働省の施策例

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情報システム構築に向けた取組を進める。

平成31年度予算政府案：40．4億円

1　厚生労働省（日本年金機構を含む）における情報セキュリティ対策の推進　39．3億円

○　CSIRT支援
- ・外部事業者を活用した情報セキュリティコンサルティング業務（情報セキュリティインシデント対処等）の実施

○　情報セキュリティ監査
- ・情報セキュリティ対策にかかる実効性の向上を図るための外部事業者を活用した監査遂行能力の拡充

○　情報システムにおける情報セキュリティ対策
- ・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対策等の実施

2　重要インフラ（医療・水道）の情報セキュリティに関する取組の強化　1．1億円

○　リスクに基づく実践的訓練
- ・サイバー攻撃を検知した際の国への報告及び事業者内の対応について、リスク分析・評価に基づく実践的な訓練の実施

○　その他重要インフラ防護の取組
- ・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等の実施

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３１年度予算政府案：0.5億円
（平成３０年度当初予算：０.7億円）

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2020年度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。

交通ISAC（仮）のイメージ

政府のサイバーセキュリティに関する予算

平成31年度予算政府案

712.9億円

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。