政府のサイバーセキュリティに関する予算

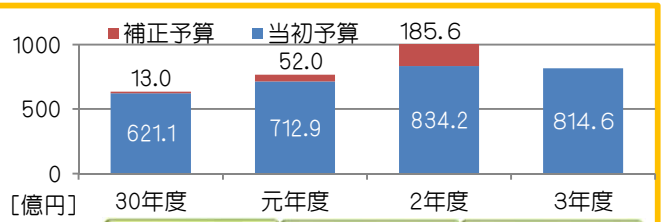
資料4

令和3年度予算政府案

814.6億円

（令和2年度当初予算額　834.2億円）

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。



主な施策例及び予算額

		令和3年度予算政府案	令和2年度補正予算	令和2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	16.7億円	23.5億円	15.3億円
【警察庁】	サイバー犯罪対策用資機材の増強等	2.3億円	3.7億円	9.3億円
【警察庁】	ホットライン業務等の外部委託	1.3億円		1.3億円
【総務省】	地方公共団体の情報セキュリティ対策の推進	0.4億円	31.4億円	1.0億円
【総務省】	サイバーセキュリティ統合知的・人材育成基盤の構築	7.0億円	85.2億円	―
【総務省】	ナショナルサイバートレーニングセンターの強化	12.0億円		15.0億円
【外務省】	情報セキュリティ対策の強化	4.0億円	5.4億円	4.8億円
【外務省】	サイバー空間に関する外交及び国際連携	0.5億円		0.2億円
【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	4.4億円		4.6億円
【経済産業省】	サイバーセキュリティ経済基盤構築事業	19.3億円		20.0億円
【経済産業省】	産業系サイバーセキュリティ推進事業	19.4億円		19.3億円
【防衛省】	防護システムの整備	202.1億円	0.8億円	162.6億円
【防衛省】	情報通信システムの安全性向上	80.9億円		76.4億円
【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	16.2億円		16.3億円
【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	0.9億円		0.8億円
【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、GIGAスクール構想の加速による学びの充実	9.0億円		9.9億円
【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	22.0億円		33.9億円
【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	0.6億円		0.5億円

令和2年度補正予算（第3次補正予算案を含む）

185.6億円

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令和３年度予算重点化方針
（令和２年７月２１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

令和３年度予算案	令和２年度当初予算額
１６．７億円	１５．３億円
＜参考＞令和２年度第３次補正予算額２０．２億円	＜参考＞令和元年度補正予算額４６．１億円

	令和３年度予算案	令和２年度当初予算額
不正な通信の監視・監査・インシデントの事後調査のための経費	**総　額　１．７億円** （主な事業） ○各府省庁、独立行政法人、指定法人に対する監査　０．８億円 ○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 ●ｻﾌﾟﾗｲﾁｪｰﾝﾘｽｸ対応のための技術検証体制構築のための調査　０．１億円	**総　額　２．６億円** ○各府省庁、独立行政法人、指定法人に対する監査　０．８億円 ○サイバーセキュリティインシデントに係る調査　１．２億円 ○クラウドの安全性評価に関する調査　０．７億円
サイバーセキュリティ戦略本部・内閣サイバーセキュリティセンターの運用等のための経費	**総　額　８．９億円** （主な事業） ○NISC統合LANシステムの運用　５．１億円 ○NISCシステムの運用　０．４億円 ○サイバーセキュリティ協議会の運用　０．８億円 ○情報セキュリティ業務補助　１．９億円 ○国際的なｲﾝｼﾃﾞﾝﾄ対応のためのCSIRT機能の構築・運用　０．３億円	**総　額　６．６億円** （主な事業） ○NISC統合LANシステムの運用　０．４億円 ○NISCシステムの運用　２．１億円 ○サイバーセキュリティ協議会の運用　１．０億円 ○情報セキュリティ業務補助　２．０億円 ○国際的なｲﾝｼﾃﾞﾝﾄ対応のためのCSIRT機能の構築・運用　０．３億円
2020年東京大会とその後を見据えた取組のための経費	**総　額　３．０億円** （事業） ○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　２．９億円 ●重要サービス事業者等に係るリスク評価の実施支援　０．０２億円	**総　額　３．０億円** ○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　３．０億円
情報セキュリティに係る研修訓練・広報等のための経費	**総　額　１．６億円** （事業） ○情報セキュリティ緊急支援チーム(CYMAT)要員等の訓練・運用　０．４億円 ○重要インフラ分野横断的演習企画実施支援　０．５億円 ○ｻｲﾊﾞｰｾｷｭﾘﾃｨに係る緊急情報発信・意識啓発の方策の強化　０．５億円 ○ｾｷｭﾘﾃｨ・IT人材（橋渡し人材）へのｻｲﾊﾞｰｾｷｭﾘﾃｨ研修　０．２億円	**総　額　１．６億円** （主な事業） ○重要インフラ分野横断的演習企画実施支援　０．５億円 ○ｻｲﾊﾞｰｾｷｭﾘﾃｨに係る緊急情報発信・意識啓発の方策の強化　０．５億円
国際連携・情勢分析等のための経費	**総　額　１．５億円** （主な事業） ○海外のサイバーセキュリティ関係機関との協調・連携等　０．４億円 ○国際連携によるサイバー攻撃即応態勢の確立　０．４億円	**総　額　１．５億円** （主な事業） ○海外のｻｲﾊﾞｰｾｷｭﾘﾃｨ関係機関との協調・連携等　０．４億円 ○国際連携によるサイバー攻撃即応態勢の確立　０．４億円

※１）○は、継続事業を指す。●は、令和元年度補正予算で計上し、令和３年度当初予算に計上した継続事業を指す。
※２）GSOCの運用及び次期システム構築経費をIT総合戦略室が一括計上している（外数）。 同経費の令和３年度予算案は３５．２億円、令和２年度当初予算は９．３億円である。
又、令和２年度補正予算に４．９億円を計上している。

警察庁の施策例

サイバー犯罪対策用資機材の増強等

令和３年度予算政府案：２．３億円
令和２年度補正予算　：３．７億円
令和２年度当初予算　：９．３億円

概要

相談対応、事件情報の収集活動及び情報の分析等を行うために使用するサイバー犯罪捜査に必要な資機材の増強整備等を行う。

○ 事件情報内偵用資機材の高度化更新

導入分析ソフトウェア

クラウド情報抽出	不正プログラム自動判別	IP・SSID/BSSID位置情報検索
各種クラウドサービス・SNSからデータを抽出	メールに添付された不審な実行ファイルを判別し自動でレポート作成	IPアドレス及び公衆Wi-Fiの SSID/BSSIDから位置情報を検索

twitter　Google　iCloud　etc.

EXE

IP 00.00.00.00
0001docomo
xx:xx:xx:xx:xx:xx

○ インターネット上にある違法・有害情報やその他事件に関する情報を安全かつ迅速に収集
○ 収集した情報をインターネット環境が必須となる分析ツールを用いて分析

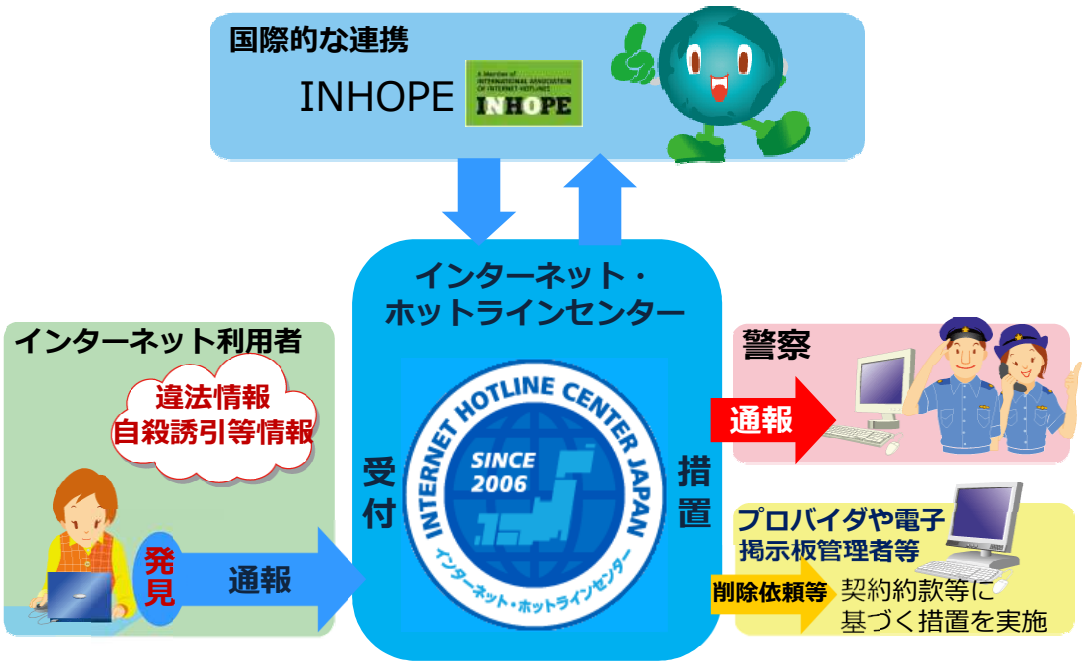
ホットライン業務等の外部委託

令和３年度予算政府案：１．３億円
令和３年度当初予算　：１．３億円

概要

一般のインターネット利用者からの違法情報等に関する通報を受理し、警察への通報やサイト管理者等への削除依頼等を行う。

○ ホットライン業務等の外部委託



○ インターネット上の違法情報として、児童ポルノ、規制薬物の広告に関する情報等を受理
○ 他人を自殺に誘引・勧誘する情報等を受理したときは、サイト管理者に削除依頼を直接行うとともに、緊急の対応を要する場合は都道府県警察に通報

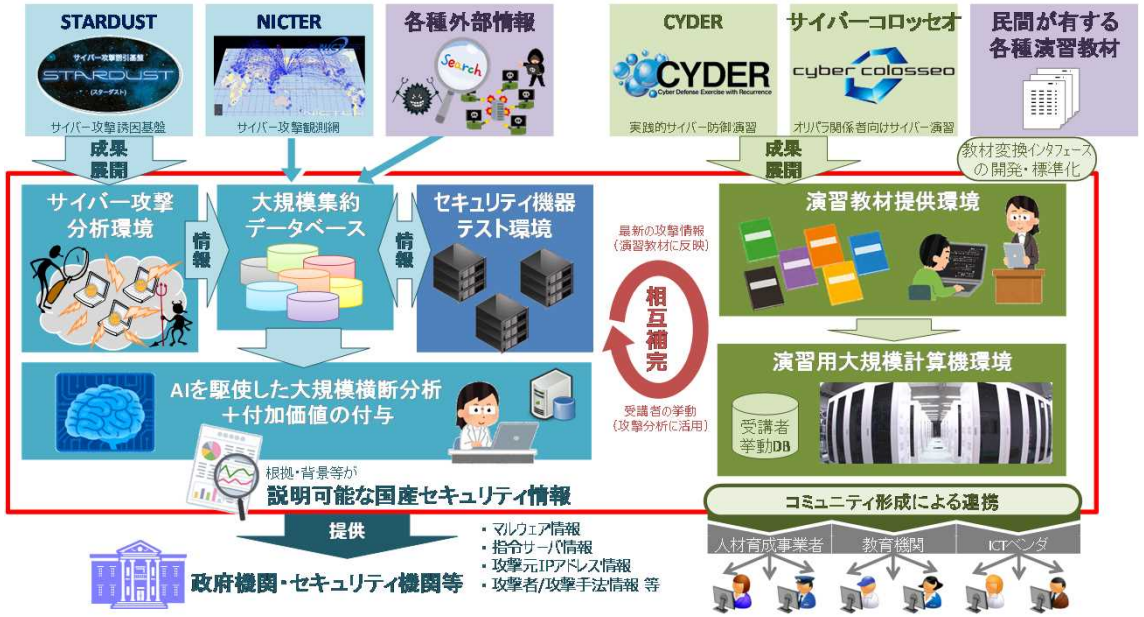
IoT・5Gへの信頼を支える「IoT・5Gセキュリティ総合対策2020」

【主な経費】 (1)サイバーセキュリティ統合知的・人材育成基盤の構築 7.0億円〈令和3年度予算政府案〉 85.2億円〈令和2年度補正予算〉
(2)ナショナルサイバートレーニングセンターの強化 12.0億円〈令和3年度予算政府案〉
(3) IoTの安心・安全かつ適正な利用環境の構築 12.8億円の内数〈令和3年度予算政府案〉

Society5.0を支えるIoT及び5Gのセキュリティ対策、セキュリティ人材の育成、サイバー攻撃への自律的な対応能力の強化等を推進

(1)サイバーセキュリティ統合知的・人材育成基盤の構築

・サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を国立研究開発法人情報通信研究機構（NICT）に構築し、産学の結節点として開放することで、我が国全体のサイバーセキュリティ対応能力を強化。



(2)ナショナルサイバートレーニングセンターの強化

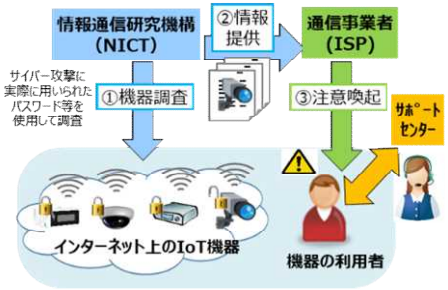
・巧妙化・複雑化するサイバー攻撃に対応できるサイバーセキュリティ人材を育成するため、NICTの「ナショナルサイバートレーニングセンター」において、

① 国の機関、地方公共団体、重要インフラ事業者等の情報システム担当者等を対象とした実践的サイバー防御演習（CYDER）を実施。

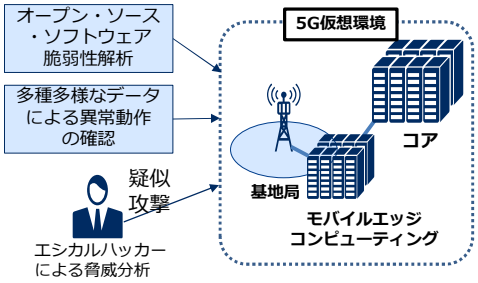
② 25歳以下の若手ICT人材を対象として、新たなセキュリティ対処技術を生み出しうる最先端のセキュリティ人材を育成（SecHack365）。

(3)IoTの安心・安全かつ適正な利用環境の構築

・電波を使用するIoT機器の多様化・急増に伴い、それらに対するサイバー攻撃の脅威が増大していることから、NOTICEの実施や５Gのセキュリティ対策により、国民生活や社会経済活動の安心・安全の確保等を実現。



①「NOTICE」の実施

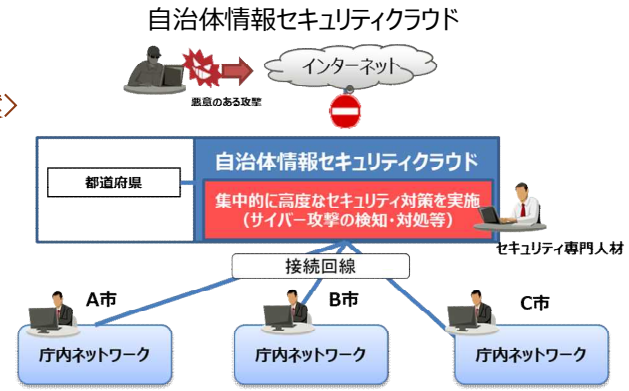


②5Gのセキュリティ対策

地方公共団体の情報セキュリティ対策の推進

【主な経費】 地方公共団体の情報セキュリティ対策の強化に要する経費 0．4億円〈令和3年度予算政府案〉
31．4億円〈令和2年度補正予算〉

○ 次期自治体情報セキュリティクラウドについて、国が設定した高いセキュリティレベル（標準要件）の遵守を図るため、移行に要する経費に対し補助を行うとともに、自治体情報セキュリティ向上プラットフォームの改修を行い、マイナンバー利用事務系のセキュリティソフト更新等を支援する。加えて、サイバー攻撃の高度化・巧妙化や技術の進展を踏まえた自治体情報セキュリティ対策の調査研究を行う。



外務省の施策例

外務省サイバーセキュリティ施策

令和２年度当初予算額　　：５．０億円
令和３年度予算政府案額　：４．５億円
令和２年度補正予算額　　：５．４億円

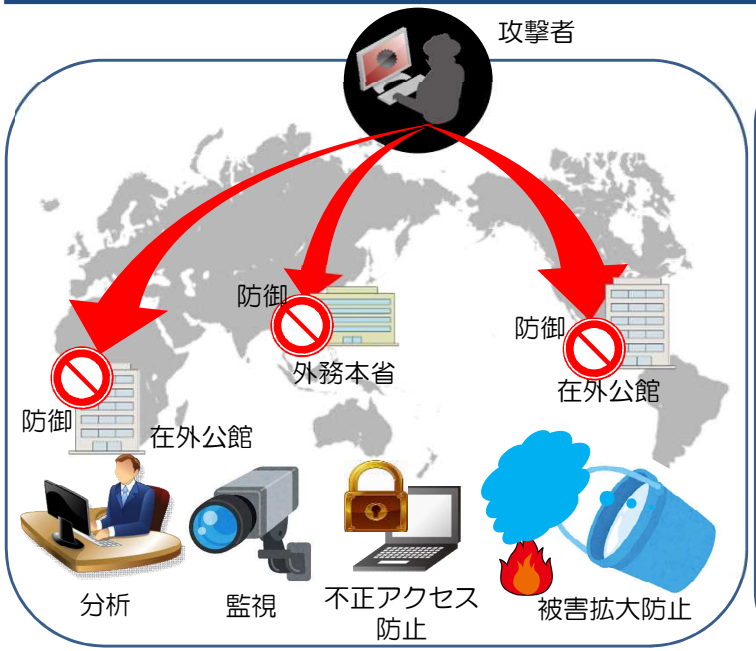
情報セキュリティ対策の強化

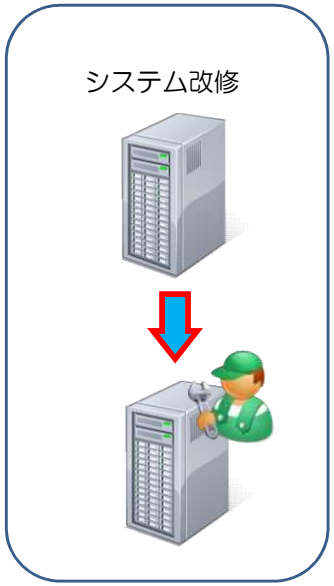
令和３年度予算政府案額：４．０億円
令和２年度補正予算額　：５．４億円

事業目的･概要

○目的
　脅威やインシデントの予兆を早期に検知・対応し、被害の回避・最小化を図るとともに、不正アクセス対策を強化する。

○事業概要
・不正通信の監視及びメールフィルタやエンドポイントでの未知の不正プログラム対策。
・ログ分析、フォレンジック等による事案解明及び対処。
・サーバ、ネットワーク機器入替等に伴う一部システムの改修。
・ログイン認証強化（令和2年度第３次補正予算）





サイバー空間に関する外交及び国際連携

令和３年度予算政府案額：０．５億円

事業目的･概要

○目的
　近年増大するサイバー空間における脅威及びサイバー問題の重要性を背景に、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、開発途上国における能力構築支援等に取り組んでいく。

○事業概要
　･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
　･開発途上国におけるサイバーセキュリティに関する能力構築支援

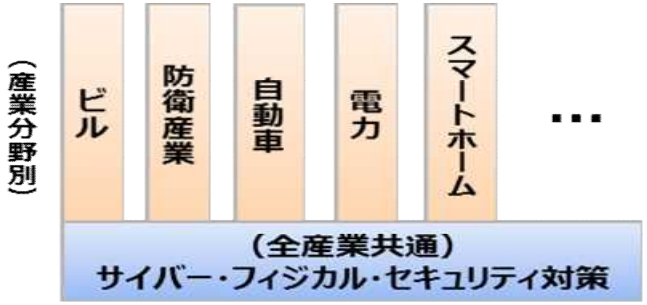
サイバーセキュリティに関する協議

経済産業省の施策例

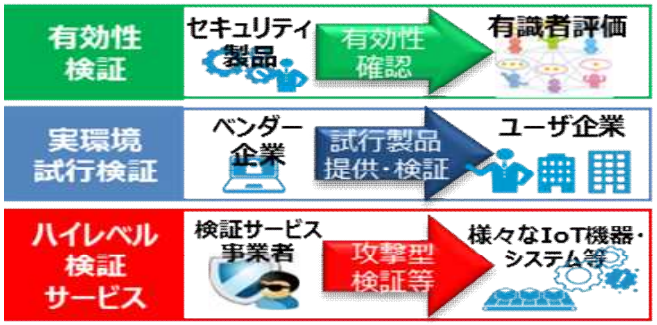
金額は令和3年度予算政府案額
（（）内は令和2年度当初予算額）

○サイバー・フィジカル・セキュリティ対策促進事業　：　4.4億円（4.6億円）

・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等の策定やセキュリティ対策の確認の仕組みの構築を推進。
・セキュリティ人材の職務・役割を必要な知識・技能や資格と紐づけ、企業と人材のマッチングを促進。
・包括的なサイバーセキュリティ検証基盤の構築等を通じて、我が国のセキュリティビジネスの成長を促進。



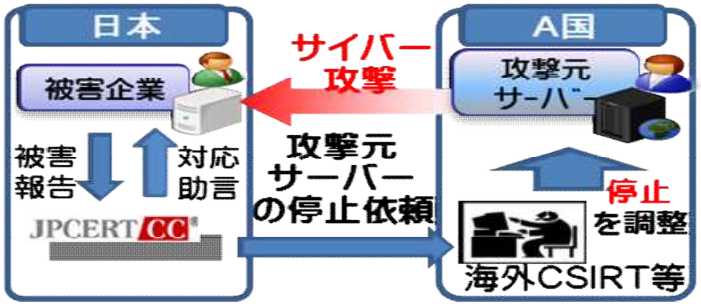
産業分野別の対策検討（イメージ）



包括的なサイバーセキュリティ検証基盤の構築（イメージ）

○サイバーセキュリティ経済基盤構築事業　：　19.3億円※うち6.5億円はIPA交付金（20.0億円）

・各国の攻撃情報の集約・対応を行う機関（窓口CSIRT）との間で情報共有を行うとともに、国境を越えて行われるサイバー攻撃への共同対処を実施。
・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。

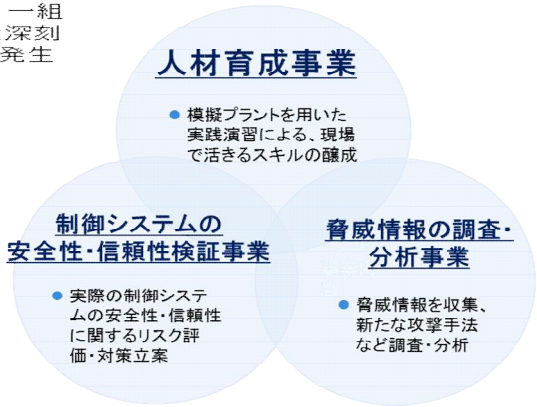


国際連携による攻撃対処

サイバーレスキュー隊の活動

○産業系サイバーセキュリティ推進事業（IPA交付金）　：　19.4億円（19.3億円）

• 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

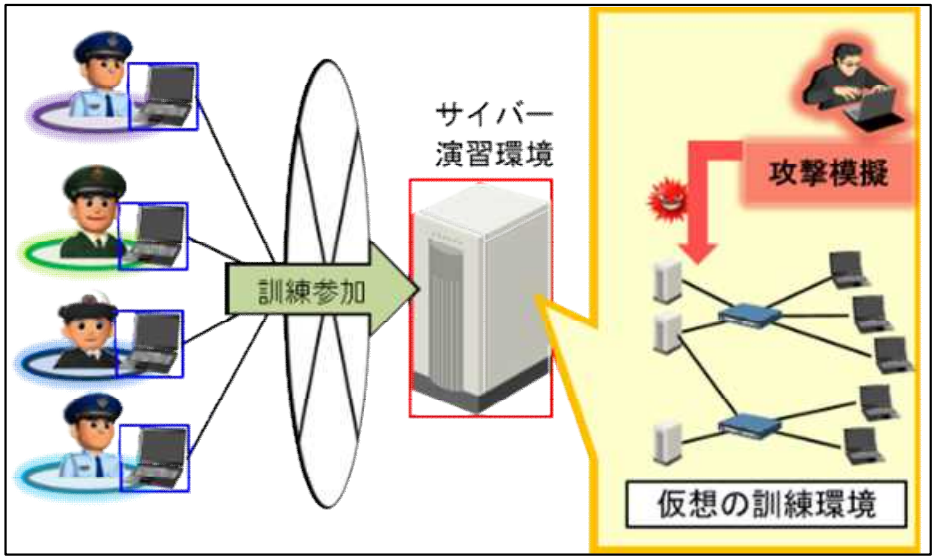
防衛省の施策例

防護システムの整備　令和3年度予算政府案額：202．1億円（令和2年度　当初予算額：162．6億円、補正予算額：0．8億円）

（令和3年度予算案事業の具体例）

◆　サイバー防護分析装置の整備
　サイバー攻撃に関する手法等を収集・分析し、防衛省・自衛隊に対するサイバー攻撃に対処するための装置を整備

◆　サイバー演習環境の整備
　サイバー攻撃等への実戦的な対処訓練を行うため、自衛隊の全てのサイバー関連部隊が利用可能な装置を整備



サイバー演習環境の運用（イメージ）

情報通信システムの安全性向上　令和3年度予算政府案額：80．9億円（令和2年度当初予算額：76．4億円）

（令和3年度予算案事業の具体例）

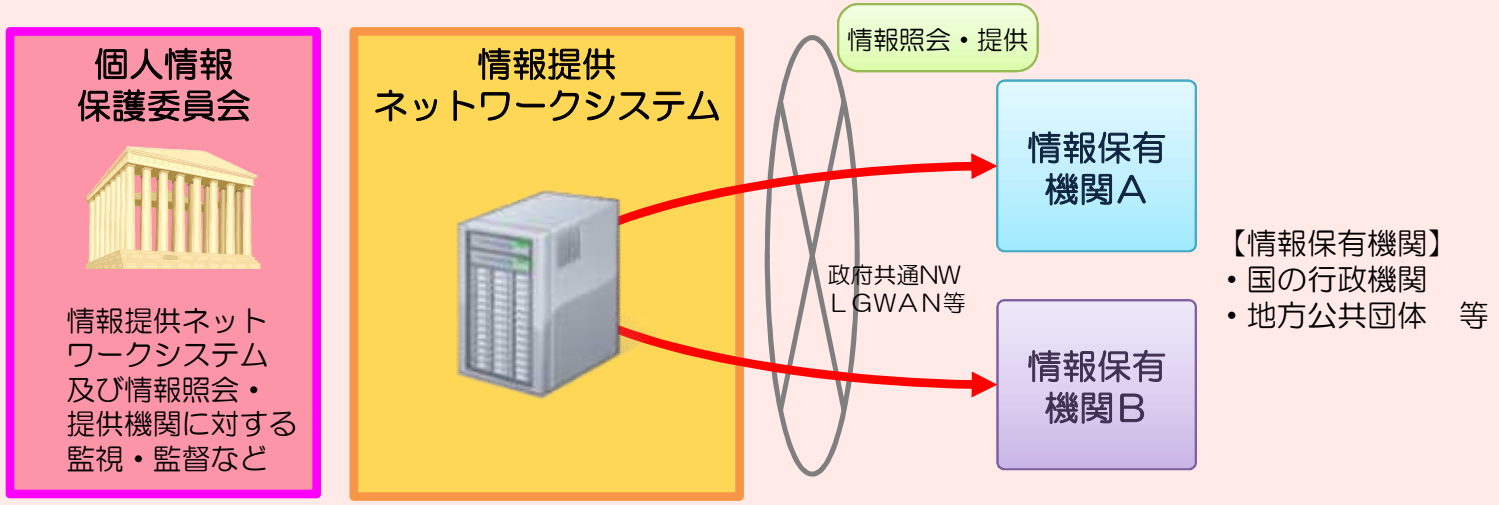
◆　防衛情報通信基盤（DII）の整備（クローズ系）
　内部侵入等によるサイバー攻撃からの防護のため、防衛情報通信基盤（DII）のクローズ系システムを整備

個人情報保護委員会の施策例

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

（令和３年度予算政府案額：16.2億円（令和２年度当初予算額:16.3億円））

○ 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

令和３年度予算政府案額：0.9億円（令和２年度当初予算額：0.８億円）

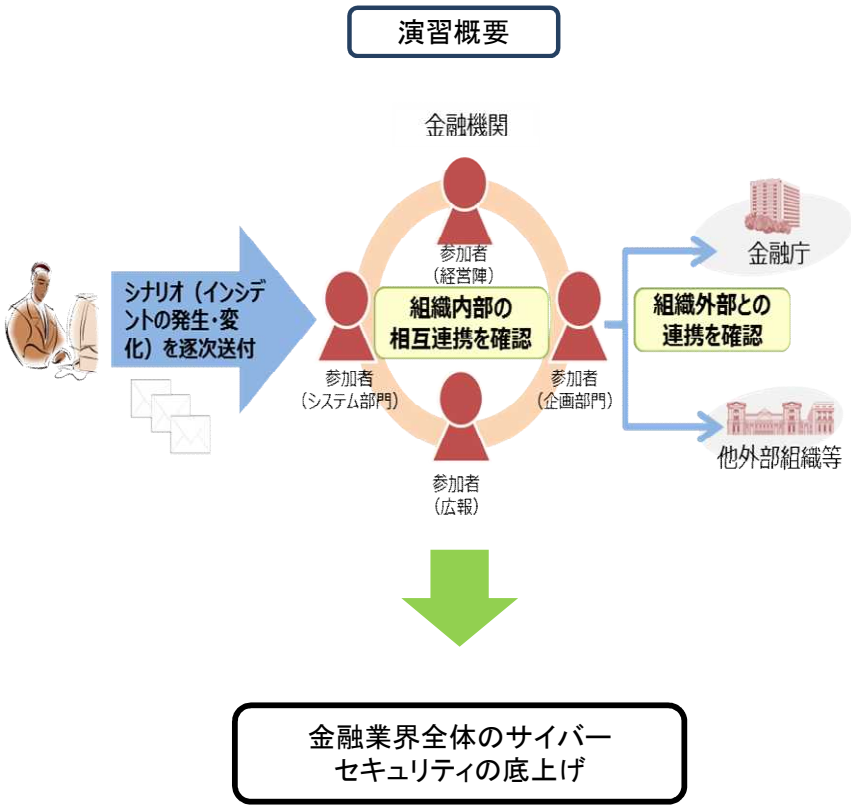
事業概要

- 金融分野におけるサイバー攻撃の複雑化・巧妙化が進む中、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、30年10月アップデート）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、令和２年度、５回目の「金融業界横断的な演習」（Delta Wall Ⅴ）を実施。

  （参考）令和２年度演習は、対象業態を拡充のうえ、約１１０先が参加（前回は約１２０先）。

- 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、令和３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



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

○Society5.0に対応した高度技術人材育成事業
成長分野を支える情報技術人材の育成拠点の形成
（enPiT-Pro）

【令和3年度予算政府案額：1．1億円（2．9億円）】

事業概要

産学連携による実践的な教育ネットワークを形成し、Society5.0の実現に向けて人材不足が深刻化しているサイバーセキュリティ人材をはじめとする情報技術人材といった、大学等における産業界のニーズに応じた人材を育成する取組を支援する。

○国立高専における情報セキュリティ人材の育成

【令和3年度予算政府案額：3．7億円（4．4億円）】

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。

GIGAスクール構想の加速による 学びの充実

【令和3年度予算政府案額：4．2億円（2．6億円）】

事業概要

「GIGA スクール構想の実現」の着実な実施に向けて、児童生徒１人１台端末の環境におけるICT の効果的な活用を一層促進する取組を実施。あわせて、新学習指導要領において、「情報活用能力」が全ての学習の基盤となる資質・能力として位置付けられたことを踏まえ、その育成及び把握のための調査研究等を実施。

- 「ＩＣＴ活用教育アドバイザー」等による整備・活用推進
- 児童生徒の情報活用能力の把握に関する調査研究
- 情報モラル教育推進事業

※令和3年度においては、令和2年度「小・中・高等学校を通じた情報教育強化事業（情報モラル教育推進事業、児童生徒の情報活用能力の把握に関する調査研究）」及び「「新時代の学びにおける先端技術導入実証研究事業」（「ICT活用教育アドバイザー」の活用事業）」を整理・統合している。

注：（ ）内の金額は令和2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。

令和3年度予算政府案額：22．0億円
（令和2年度当初予算額：33．9億円）

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　　21．0億円（32．9億円）

○　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　　1．0億円（1．0億円）

○　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

令和３年度予算政府案額：0.6億円
（令和２年度当初予算額：0.5億円）

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）

○ 国土交通省情報セキュリティポリシー及び関係規程に関する準拠性監査業務　　等
（政府統一基準との準拠性の監査）

(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.重要インフラ事業者を含む所管分野事業者のサイバーセキュリティ対策への自主的な取り組みを進めるため積極的に支援する

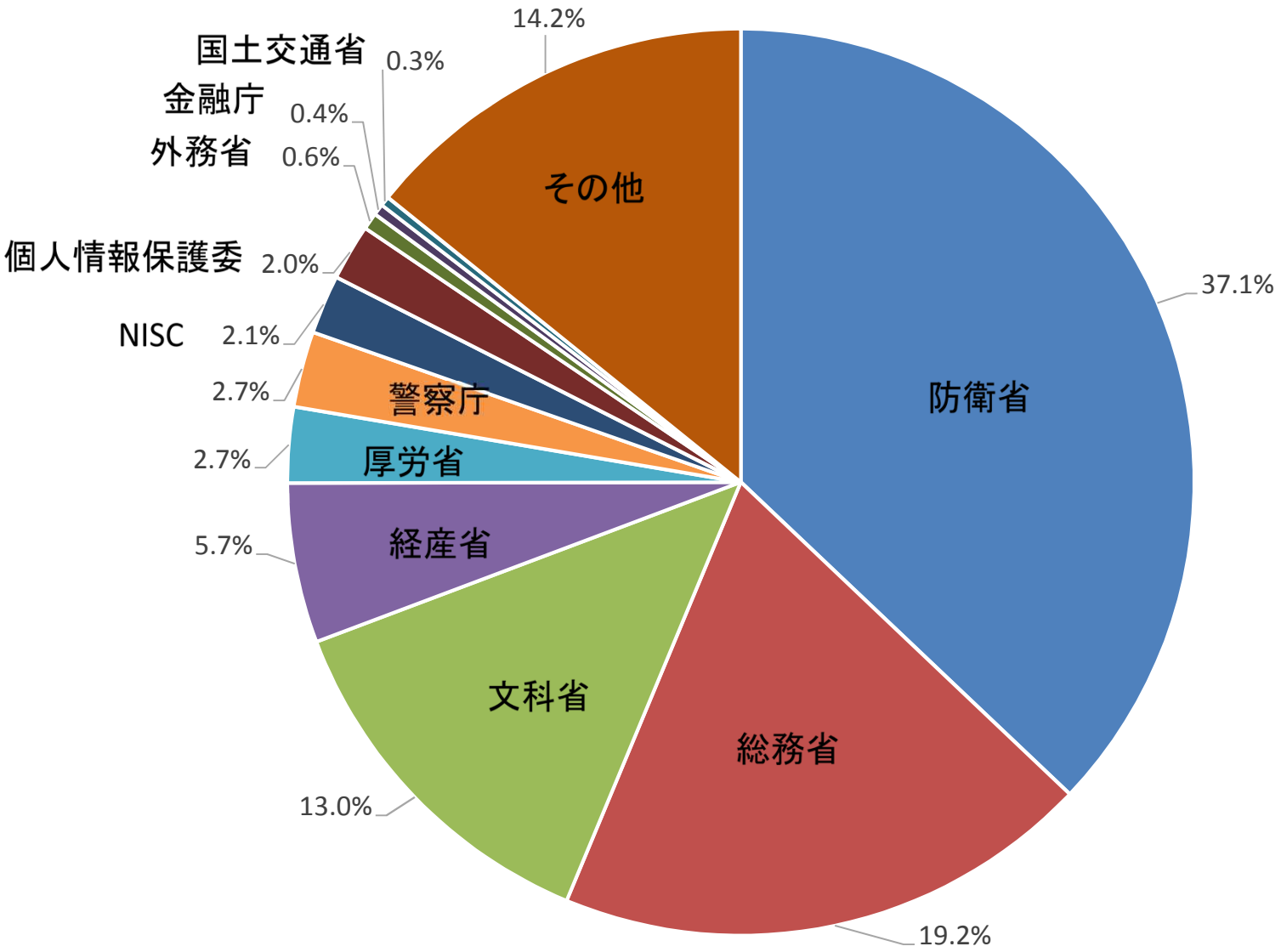
○ 重要インフラ分野における情報セキュリティ確保に係る安全ガイドライン策定業務
（新たなデジタル技術への情報セキュリティ対策に対応するための改定に向けた検討）
（国土交通省の所管重要インフラ分野：航空・空港・鉄道・物流の４分野）

各府省庁等のサイバーセキュリティに関する予算

令和3年度予算政府案

814.6億円

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。



予算重点化方針分野別一覧

令和3年度予算政府案

814.6億円

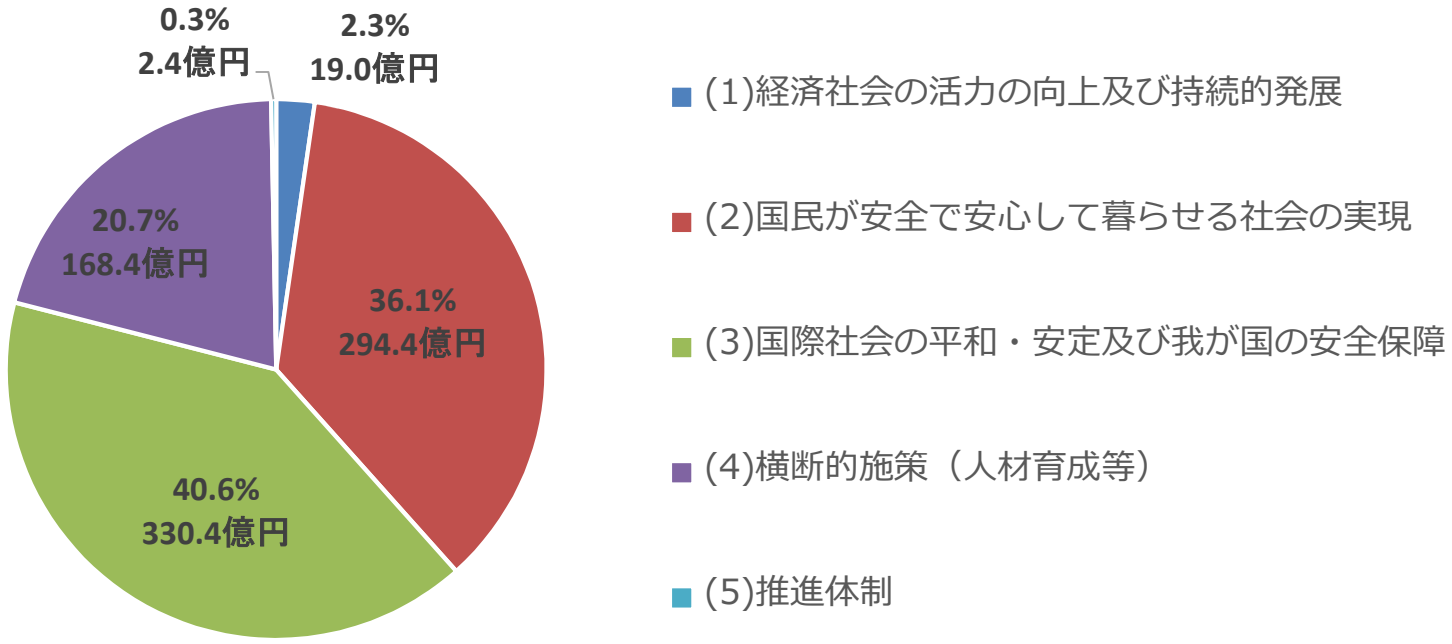
サイバーセキュリティに関する予算として切り分けられない場合には計上していない。

○　サイバーセキュリティ関連予算に関しては、「サイバーセキュリティ関係施策に関する令和３年度予算重点化方針」（令和2年7月21日サイバーセキュリティ戦略本部決定）において、サイバーセキュリティ戦略に定める「目標達成のための施策」に掲げる政策領域ごとに重点化を図るべき分野を示している。

○　各府省庁は、この予算重点化方針に留意して概算要求を行うこととしており、今回の調査においては、令和３年度予算政府案における予算重点化方針の反映の状況についても調査を行った。

○　令和３年度予算政府案におけるサイバーセキュリティ関連予算は、令和２年度当初予算額に比べて19.6億円減少し、814.6億円となっており、そのうち、予算重点化方針において特に重点を置くべき施策として示した施策の内訳としては、（２）国民が安全で安心して暮らせる社会の実現が約４割、（３）国際社会の平和・安定及び我が国の安全保障が約４割を占めている。

○　サイバーセキュリティ戦略を的確に実施するため、毎年度、年次計画及び年次報告を作成することとしており、重点化方針の反映状況も含めた年次報告について、次年度の年次計画に反映する。



予算重点化方針分野における施策例①

（１）経済社会の活力の向上及び持続的発展

①サイバーセキュリティに関する品質の高いモノやサービス等の実現につながる施策

○サイバーセキュリティ統合知的・人材育成基盤の構築（総務省）・・・・・・・・・・・・令和３年度予算政府案　7.0億円

※事業概要については、Ｐ４の『総務省の施策例』に記載。

②中小企業のサイバーセキュリティ対策に資する施策

○サイバー・フィジカル・セキュリティ対策促進事業（経済産業省）・・・・・・・・・・令和３年度予算政府案　4.4億円

※事業概要については、Ｐ６の『経済産業省の施策例』に記載。

（２）国民が安全で安心して暮らせる社会の実現

①深刻な社会問題となっているサイバー犯罪への対策のための施策

○サイバー犯罪対策用資機材の増強等（警察庁）・・・・・・・・・・・・・・・・・・・・令和３年度予算政府案　2.3億円

○ホットライン業務等の外部委託（警察庁）・・・・・・・・・・・・・・・・・・・・・令和３年度予算政府案　1.3億円

※事業概要については、Ｐ３の『警察庁の施策例』に記載。

②官民の枠を超えた訓練・演習の実施による障害対応体制の強化に資する施策

○ナショナルサイバートレーニングセンターの強化（総務省）・・・・・・・・・・・・・令和３年度予算政府案　12.0億円

※事業概要については、Ｐ４の『総務省の施策例』に記載。

○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（厚生労働省）・・令和３年度予算政府案　1.0億円

※事業概要については、Ｐ１１の『厚生労働省の施策例』に記載。

○金融分野のサイバーセキュリティ対策向上（金融庁）・・・・・・・・・・・・・・・・令和３年度予算政府案　0.9億円

※事業概要については、Ｐ９の『金融庁の施策例』に記載。

③政府機関、独立行政法人等におけるセキュリティ強化・充実に資する施策

○GSOCシステムの構築（内閣官房（IT室が一括予算計上））・・・・・・・・・・・・・・令和３年度予算政府案　26.5億円

新たなサイバー攻撃から政府情報システムの被害の発生と拡大を防止するため、最新の技術や手法を取り入れた新たな機能を設けたGSOC （政府機関情報セキュリティ横断監視・即応調整チーム）システムを構築し、政府横断的な監視を行う。

④大規模サイバー攻撃事態等への対処態勢の強化に資する施策

○サイバーセキュリティ経済基盤構築事業（経済産業省）・・・・・・・・・・・・・・・令和３年度予算政府案　19.3億円

※事業概要については、Ｐ６の『経済産業省の施策例』に記載。

予算重点化方針分野における施策例②

（３）国際社会の平和・安定及び我が国の安全保障

①サイバー空間における国際的な法の支配に積極的に貢献する施策

○サイバー空間に関する外交及び国際連携（外務省）・・・・・・・・・・・・・・・・・・・・令和３年度予算政府案　0.5億円

※事業概要については、Ｐ５の『外務省の施策例』に記載。

②我が国の防御力・抑止力・状況把握力の強化に資する施策

○防護システムの整備（防衛省）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・令和３年度予算政府案　202.1億円

○情報通信システムの安全性の向上（防衛省）・・・・・・・・・・・・・・・・・・・・・令和３年度予算政府案　80.9億円

※事業概要については、Ｐ７の『防衛省の施策例』に記載。

③国際協力・連携に資する施策

○産業系サイバーセキュリティ推進事業（経済産業省）・・・・・・・・・・・・・・・・・令和３年度予算政府案　19.4億円

※事業概要については、Ｐ６の『経済産業省の施策例』に記載。

（４）横断的施策（人材育成等）

①人材育成・確保に資する施策

○国立高専における情報セキュリティ人材の育成（文部科学省）・・・・・・・・・・・・・令和３年度予算政府案　3.7億円

○Society5.0に対応した高度技術人材育成事業（文部科学省）・・・・・・・・・・・・・・令和３年度予算政府案　1.1.億円

○GIGAスクール構想の加速による学びの充実（文部科学省）　・・・・・・・・・・・・・・令和３年度予算政府案　4.2.億円

※事業概要については、Ｐ１０の『文部科学省の施策例』に記載。

②サプライチェーンリスクへ対応するための施策

○ＩｏＴの安心・安全かつ適正な利用環境の構築（総務省）・・・・・・・・・・・・・・・令和３年度予算政府案　12.8億円

※事業概要については、Ｐ４の『総務省の施策例』に記載。

（５）推進体制

①サイバーセキュリティ対策を推進するための施策

○情報セキュリティ業務補助（内閣官房（NISC））・・・・・・・・・・・・・・・・・・・・令和３年度予算政府案　1.9億円

民間企業等に蓄積された技術的知見・ノウハウ等を有する者を積極的に活用し、政府における情報セキュリティ分野の国家戦略の立案・対策を推進する。