政府のサイバーセキュリティに関する予算

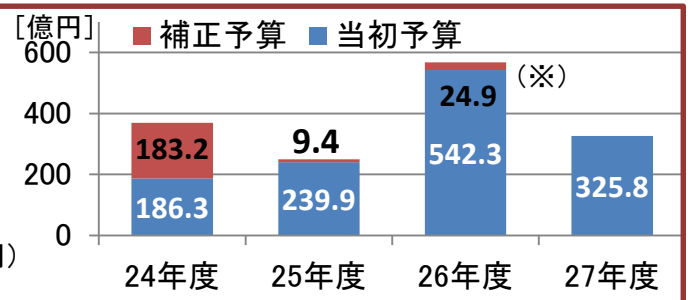
資料５

平成27年度予算額

325．8億円

（平成26年度当初予算額：542．3億円）

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。



施策例及び平成27年度予算額（括弧内は平成26年度当初予算額）

【内閣官房】	内閣サイバーセキュリティセンター予算	16．5億円（9．9億円）
【警察庁】	日本版NCFTAへの参画に伴う経費	1．1億円（―）
【警察庁】	サイバーテロ対策用資機材の増強等／重要インフラ事業者等からの要望に基づくIT障害対応能力を高めるための支援	7．1億円（ 5．7億円）
【総務省】	サイバー攻撃複合防御モデル・実践演習／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	8．1億円（11．1億円）
【総務省】	M2Mセキュリティ実証事業	1．5億円（ ― ）
【外務省】	情報セキュリティ対策の強化	4．2億円（ 4．0億円）
【外務省】	サイバー空間における外交及び国際連携	0．1億円（ 0．1億円）
【経済産業省】	重要インフラのセキュリティ対策促進・IT 製品の評価・認証等（独立行政法人情報処理推進機構（IPA）交付金）	36．1億円（37．4億円）
【経済産業省】	スマートグリッドのセキュリティ評価事業	1．0億円（ ― ）
【防衛省】	ネットワーク監視器材の整備	29．8億円（29．8億円）
【防衛省】	サイバー演習環境（サイバーレンジ）の整備	6．6億円（ 6．6億円）

平成26年度補正予算額

24．9億円

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。

施策例及び平成26年度補正予算額

【内閣官房】	内閣サイバーセキュリティセンター予算	7．3億円
【総務省】	国際連携によるサイバー攻撃予知・即応技術の研究開発	2．0億円
【外務省】	情報セキュリティ強化	0．4億円
【防衛省】	自衛隊の防護・監査システム等の維持・整備等	8．7億円

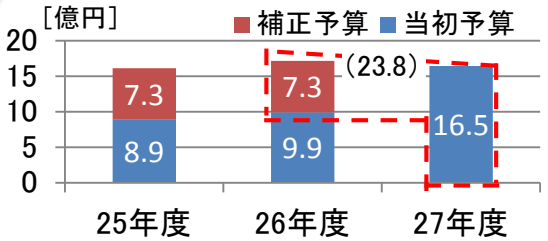
（※）26年度の数値は防衛情報通信基盤（DII）の整備（器材の整備）（クローズ系）（防衛省）、社会保障と税に関わる番号制度の導入に伴うシステム開発（内閣官房）を含む。

内閣官房の施策例

我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針（平成26年11月25日情報セキュリティ政策会議決定）

内閣サイバーセキュリティセンター予算

	平成26年度補正予算（7．3億円）	平成27年度予算（16．5億円）
① GSOC機能の強化 ➢ 新システム（2017年度～）の運用を見据えた体制、機材の整備　等	○政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）機能強化のための調査　31百万円	○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　649百万円
② 総合的分析機能の強化 ➢ 諸外国の政策、サイバー攻撃の脅威情勢及び攻撃に使用された技術等の総合的な分析 ➢ 高度な専門知識と深い知見を有する専門的人材の確保及び資質の向上	○脅威予測等総合分析の実施のためのシステム構築　573百万円	○脅威予測等総合分析の実施　78百万円
③ 国内外の情報集約機能の強化 インシデント情報の集約機能や助言機能等の強化に向けた、 ➢ 官民連携のスキーム強化・構築 ➢ NISC内の体制・システム整備及び能力向上	○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（前倒し分）　117百万円 ○サイバーセキュリティインシデントに係る事後調査　7百万円 ○脅威予測等総合分析の実施のためのシステム構築（再掲）	○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　311百万円 ○サイバーセキュリティインシデントに係る事後調査　114百万円 ○脅威予測等総合分析の実施（再掲）
④ 国際連携の強化 ➢ 緊急対応関連機関とのパートナーシップ構築等による国際的な窓口機能の強化		○国際的なインシデント対応のためのCSIRT機能の構築・運用　86百万円
⑤ 人材の育成及び登用 ➢ 各省庁からの出向等人材を通じ、NISC内の知見・経験を各省庁に還元 ➢ 任期付任用や人事交流の推進等による技能を備えた人材の確保	○定員増10人（任期付職員） ※26年度措置	○定員増　※27年度措置



※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（408百万円）を27年度予算に計上

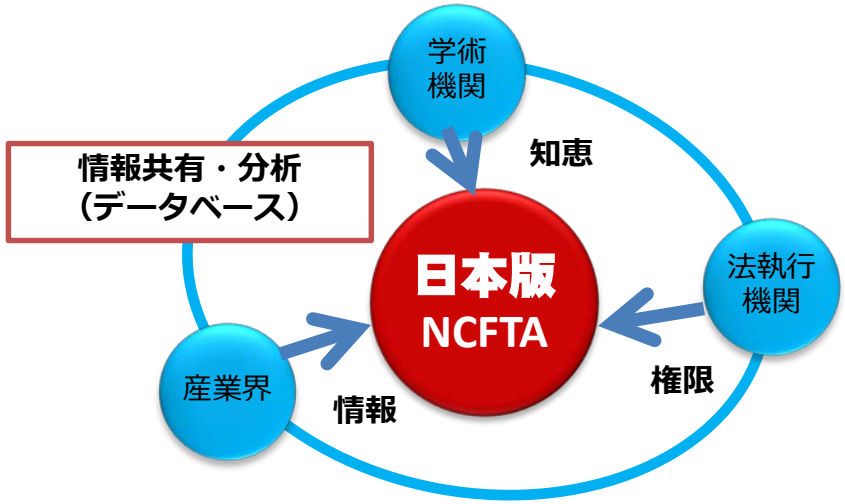
警察庁の施策例

日本版NCFTAへの参画に伴う経費

平成27年度予算： １．１億円

目的

産学官が同じ場を共有し、それぞれが持つ対処の経験等を全体で蓄積・共有するとともに、警察による捜査権限のより効果的な行使を含めサイバー空間の脅威を特定、軽減及び無効化するための**先制的・包括的な対応**を実施



活動

- 情報集約・分析
- トレーニング
- 研究開発
- 海外連携

サイバーテロ対策用資機材の増強等

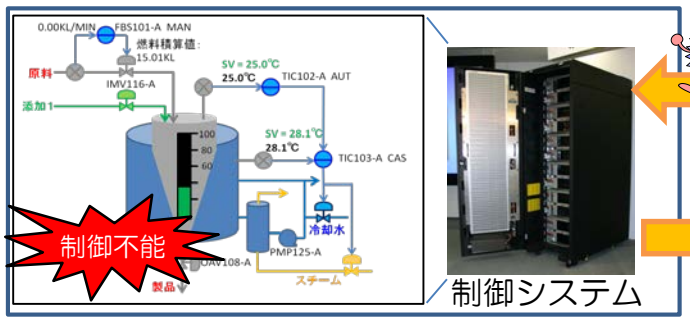
平成27年度予算： ６．３億円

重要インフラ事業者等からの要望に基づくIT障害対応能力を高めるための支援

平成27年度予算： ０．８億円

【情勢】

近年、重要インフラ事業者の基幹システムの動作をつかさどる「制御システム」を狙ったものとみられるサイバー攻撃の兆候が複数発生



【対策】

- 制御システムを模した環境を整備することにより、適切な解析手法等について調査し、稼働中の制御システムに対するデジタルフォレンジック手法を確立
- 訓練用シナリオの作成及び訓練支援業務を委託することにより、制御システムに対するサイバー攻撃対策を適切に実施するための知見を取得

被害の未然防止・拡大防止に係る技術的な研究や対処要員の育成を行い、制御システムに対するサイバー攻撃への対処能力を強化

総務省の施策例

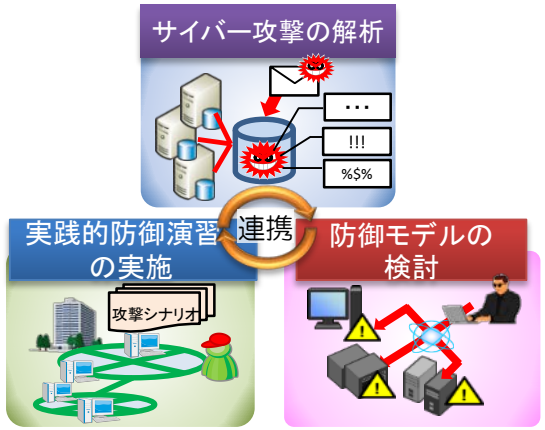
課題

標的型攻撃	個人のマルウェア感染	分散型サービス妨害攻撃（DDoS攻撃）
標的型攻撃等の巧妙化するサイバー攻撃により、政府機関、民間企業等において機密情報漏えい等の被害が発生する事態が頻発。	個人利用者においても、ウェブサイト等からのマルウェア感染により、ネットバンキングの不正送金などの実被害が発生。	海外を主な発信源とするDDoS攻撃により、政府機関等のウェブサイトのアクセス障害やネットワークの輻輳が頻発。

対策

サイバー攻撃複合防御モデル・実践演習

標的型攻撃等の新たなサイバー攻撃の解析による実態把握、防御モデルの検討、官民参加型の実践的な防御演習の実施。 平成26年度当初予算　：４．５億円
平成27年度予算　：４．０億円

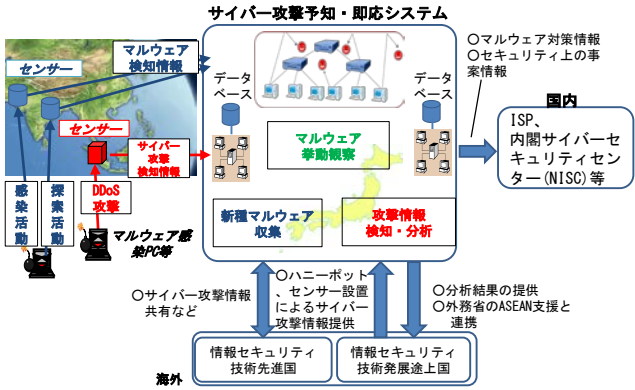


ICT環境の変化に応じた情報セキュリティ対応方策の推進事業

ISP等と連携し、インターネット利用者を対象に、マルウェア配布サイトへのアクセスの未然防止や利用者の行動特性に基づいた不正通信検知技術の開発など総合的なマルウェア感染対策を行うプロジェクト。 平成26年度当初予算　：６．６億円
平成27年度予算　：４．１億円

国際連携によるサイバー攻撃予知・即応技術の研究開発

諸外国と連携してサイバー攻撃に関する情報を収集するネットワークを構築し、サイバー攻撃の発生を予知し即応を可能とする技術の研究開発及び実証実験。平成26年度当初予算　：３．０億円
平成２６年度補正予算　：２．０億円



新規

M2Mセキュリティ実証事業

ICTの基盤である通信インフラの情報セキュリティを確保する横断的取組

IoT（Internet of Things）環境の本格的な到来により、今後の急速な普及が見込まれる機器間通信（M2M）について、M2Mの特徴に合致した通信プロトコル・暗号通信技術等の情報セキュリティ技術の開発・実証を実施。

平成27年度予算：１．５億円

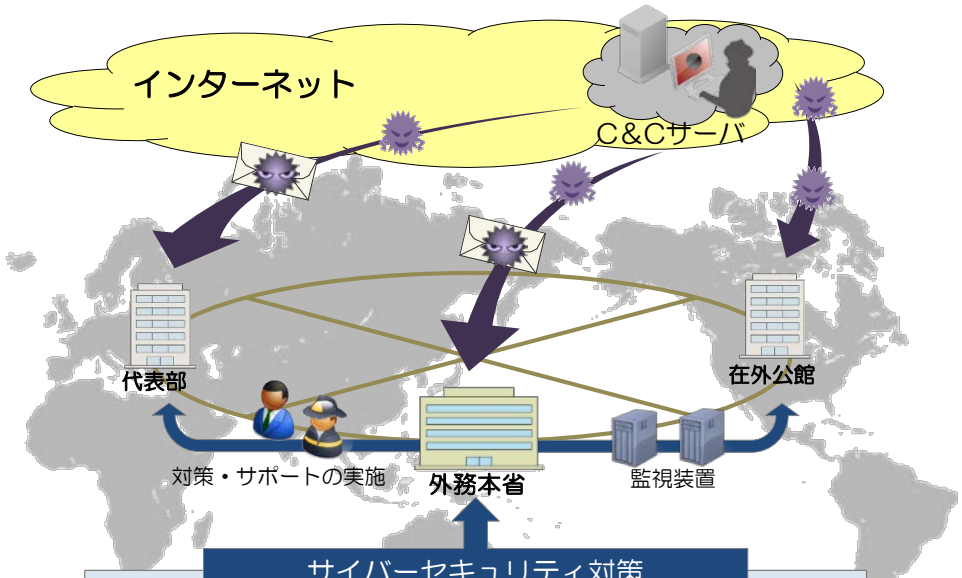
外務省の施策例

情報セキュリティ対策の強化

平成26年度当初予算　：４．０億円
平成27年度予算　：４．２億円

事業概要･目的

○概要
　サイバー攻撃の手口は益々巧妙化･多様化し，標的を絞り込んだ上で周到に準備が行われており，脅威は一層増大していることから，これら脅威に迅速に対応するための対策強化が必要不可欠である。



サイバーセキュリティ対策

･インシデント対応チームの強化
･本省及び在外公館の監視装置の拡充
･人材育成及び啓発の強化

サイバー空間における外交及び国際連携

平成26年度当初予算　：０．１億円
平成27年度予算　：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
･サイバーセキュリティに関する戦略的政策協議
･国際テロ・組織犯罪関連条約に関するワークショップ

平成26年度補正予算

情報セキュリティ強化

平成２６年度補正予算　：０．４億円

事業概要･目的

○概要
　ネットワーク機器のリプレイスに伴うログ管理システム改修費用。

経済産業省の施策例

○重要インフラのセキュリティ対策促進・IT製品の評価・認証等
（独立行政法人情報処理推進機構（IPA）交付金）

平成26年度当初予算　：37.4億円
平成27年度予算　：36.1億円

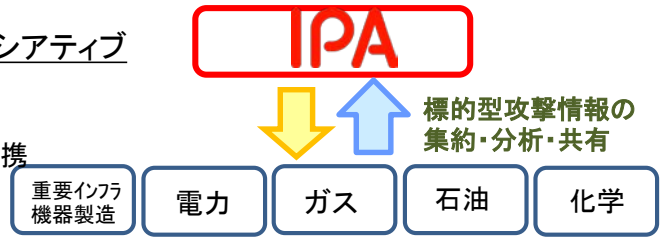
重要インフラへの標的型攻撃に関する情報共有、セキュリティ対策の分析・普及啓発やIT製品の評価・認証等を実施。

○重要インフラへの標的型攻撃に関する情報共有（開始以降、400件以上を共有。）

○セキュリティ関連情報（脆弱性、ウイルス、不正アクセス）の収集・分析・対策の実施。

○政府調達等のためのIT製品のセキュリティ評価・認証　等

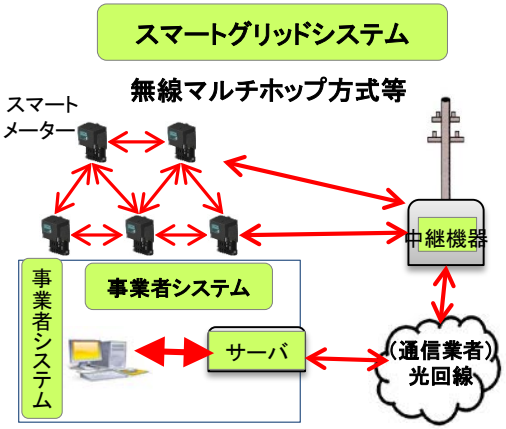
サイバー情報共有イニシアティブ（J-CSIP）
・IPAがハブ
・セプターカウンシルとも連携



○スマートグリッドのセキュリティ評価事業（新規　1.0億円）

・スマートメーターや中継機器のなりすましによる、スマートグリッドシステム上のデータ改ざん・不正取得が問題。

・スマートグリッドシステムのサイバーセキュリティの評価技術・手順を策定し、その有効性を実証。

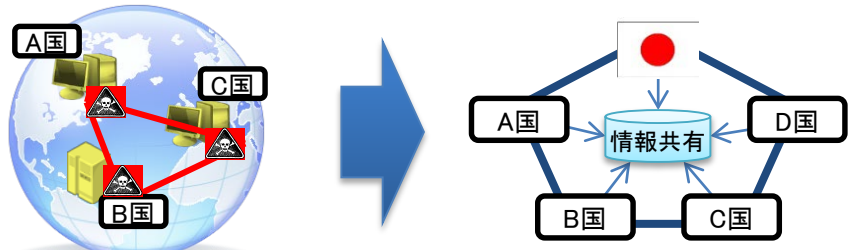


○サイバーセキュリティ経済基盤構築事業

平成26年度当初予算　：17.4億円
平成27年度予算　：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、再発防止を支援。

・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。



攻撃者は、各国に散らばった遠隔操作マルウェア感染端末等の攻撃基盤を用い攻撃。
→攻撃の巧妙化・大規模化の温床

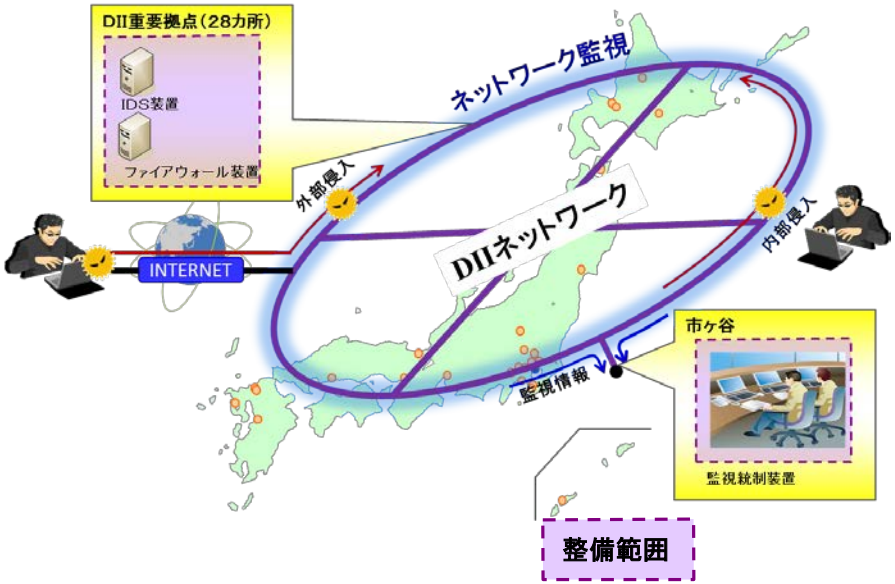
各国の窓口CSIRTが、攻撃基盤に係る情報を共有し、共同対処。

防衛省の施策例

ネットワーク監視器材の整備

平成27年度予算 ： 29．8億円

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



サイバー演習環境（サイバーレンジ）の整備

平成27年度予算 ： 6．6億円

サイバーセキュリティの常時確保のため、防衛省・自衛隊のシステムへのサイバー攻撃等に対する実戦的な訓練を行うためのサイバー演習環境（サイバーレンジ）を整備