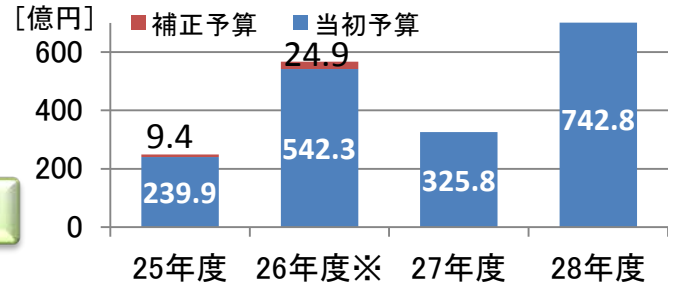
政府のサイバーセキュリティに関する予算

資料３

平成28年度予算概算要求額

742．8億円

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28年度予算概算要求額（括弧内は平成27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	83．0億円＋事項要求（16．5億円）
【警察庁】	日本版NCFTAへの参画に伴う経費	1．2億円（1．1億円）
【警察庁】	サイバー犯罪等の対処能力強化のための実践的実習環境の整備等	0．8億円（0．6億円）
【総務省】	未来志向型ネットワークセキュリティ基盤構築事業	13．0億円（新規）
【総務省】	サイバー攻撃複合防御モデル・実践演習	6．0億円＋事項要求（4．0億円）
【総務省】	自治体情報セキュリティ対策の抜本的強化	4．4億円＋事項要求（新規）
【外務省】	情報セキュリティ対策の強化	4．8億円（4．3億円）
【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）	53．2億円（36．1億円）
【経済産業省】	サイバーセキュリティ経済基盤構築事業	23．6億円（17．7億円）
【防衛省】	情報収集機能や調査分析機能強化	42．0億円（8．4億円）
【防衛省】	ネットワーク監視器材の整備	61．0億円（29．8億円）
【特定保護委】	特定個人情報に係るセキュリティ確保のための監視・監督体制整備（マイナンバー関連）	3．2億円＋事項要求（0．6億円）
【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	62．1億円（新規）

平成27年度予算額

325．8億円

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。

※　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

内閣サイバーセキュリティセンター予算

サイバーセキュリティ戦略（平成27年9月4日　閣議決定）	平成28年度予算 概算要求　83億円	平成27年度（参考） 当初予算　16．5億円
➢ 政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)による検知・解析機能の強化	○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　68．5億円	○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
➢ ペネトレーションテスト等を通じたセキュリティ対策の徹底 ➢ マネジメント監査等を通じた組織の体制・制度の検証・改善、リスク評価に基づく組織的な対策・管理等による組織的対応能力の強化	○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　3．1億円	○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　3．1億円
➢ 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　4．5億円	○脅威予測等総合分析の実施　0．8億円
➢ 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原因究明調査のための取組強化	○サイバーセキュリティインシデントに係る事後調査　1．3億円	○サイバーセキュリティインシデントに係る事後調査　1．1億円
➢ NISCの要員強化	定員増要求	定員増　20人

※平成28年度予算概算要求については、上記のほか、サイバーセキュリティ戦略本部の運営経費やサイバーセキュリティ関連施策の実施に必要な経費等（565百万円）を計上

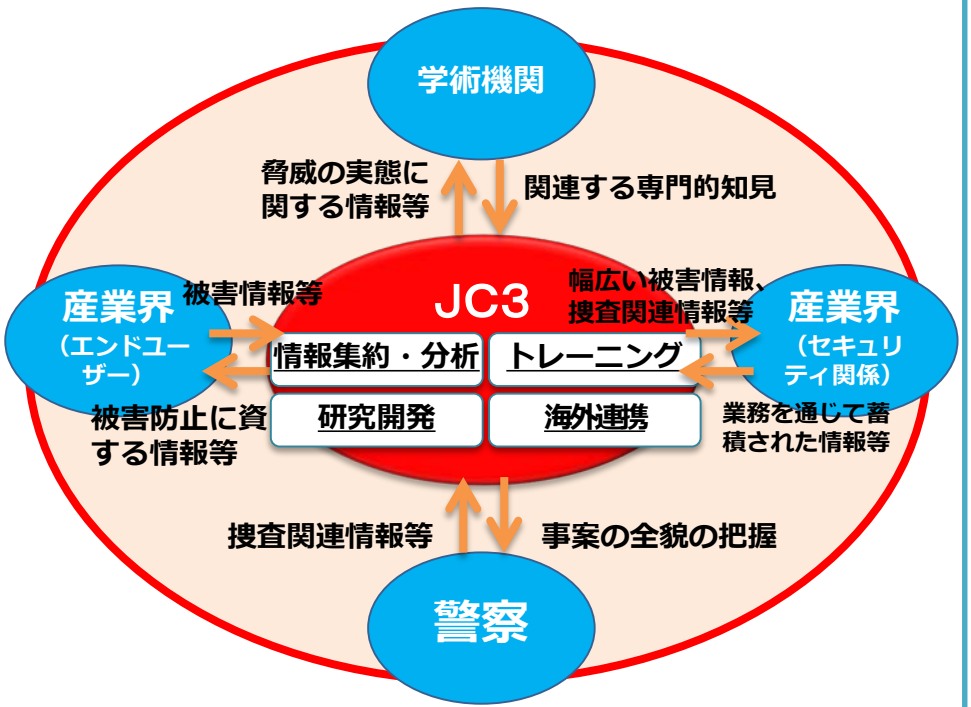
警察庁の施策例

日本版NCFTAへの参画に伴う経費

平成27年度予算： １．１億円
平成28年度予算概算要求： １．２億円

概要 産学官（法執行機関）それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を共有することにより、サイバー空間全体を俯瞰した上で、サイバー空間の脅威の大本を特定、軽減及び無効化し、以後の事案発生の防止に資するための活動を行うための枠組み。

日本版NCFTA(※)は、平成26年11月、一般財団法人日本サイバー犯罪対策センター（Japan Cybercrime Control Center：略称JC3）として業務を開始



※ NCFTA(National Cyber-Forensics & Training Alliance)＝FBI等の法執行機関、民間企業、学術機関を構成員として米国に設立された非営利団体で、サイバー犯罪に係る情報の集約・分析、海外を含めた捜査機関等の職員に対するトレーニング等を実施。

サイバー犯罪等の対処能力強化のための実践的実習環境の整備等

平成27年度予算： ０．６億円
平成28年度予算概算要求： ０．８億円

概要 捜査員に対して最新の事例を取り入れた高度かつ実践的な実習を行うための環境を整備

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】未来指向型ネットワークセキュリティ基盤構築 事業　13億円（新規）

- 2020年東京オリンピック・パラリンピック競技大会を見据え、更に巧妙化・複合化するサイバー攻撃に備え、将来の我が国における安心・安全なサイバー空間を実現し、もって安全な社会経済基盤の実現を図るため、以下の取組を推進する。
  - ① 実践的能力を有する人材の育成に向け、2020年東京大会関連システムの模擬も可能な大規模演習基盤を構築・運用するとともに組織の人材育成に対する支援を行う。
  - ② サイバー攻撃や脆弱性等の情報を収集・解析し、ISPやセキュリティベンダ等の関係者間で共有することで、適切な対策を促す仕組みの構築・実証を行う。
  - ③ 増大するM2M・IoT機器の安全性の確保のため、セキュリティ技術開発や運用ガイドラインの策定等、当該機器への対策を促す仕組みの実証を行う。

サイバー攻撃複合防御モデル・実践演習【主な経費】サイバー攻撃複合防御モデル・実践演習6．0億円 ＋ 事項要求（4．0億円<27当初>）

- 近年、巧妙化・複合化する標的型攻撃※について、攻撃の解析・防御モデルの検討及び実践的な防御演習を実施し、我が国における標的型攻撃に対する対処能力を向上させる。
  大規模実証環境を活用し、以下の取組を推進する。

① サイバー攻撃の解析：標的型攻撃の解析及び解析結果のデータベース化を通じ、標的型攻撃の特徴情報の体系化及び解析手法の確立を図る。

② サイバー攻撃防御モデルの検討：①の結果を踏まえ、サイバー攻撃が発生した際のインシデントレスポンスについて検討を行い、防御モデルの確立を図る。

③ 実践的防御演習：②で確立した防御モデルを踏まえ、官公庁・大企業等のLAN管理者を対象にしたサイバー攻撃への対応能力向上のための実践的防御演習を実施し、対処に必要なスキル項目の体系化を図る。

自治体情報セキュリティ対策の抜本的強化【主な経費】自治体情報セキュリティ緊急対策事業4．4億円＋事項要求（新規）

- マイナンバー制度導入に関連し、標的型攻撃等の新たな脅威に対応可能な情報セキュリティについての抜本的な対策を実施。

① 組織体制の再検討、職員の訓練等、インシデント即応体制の整備とあわせて、自治体の情報システムに係るインターネットのリスクへの対応として、以下の取組を推進する。

（ア）攻撃に強い内部ネットワーク等の構築

情報提供ネットワークシステムの稼働を見据え、機密性はもとより、可用性や完全性の確保にも十分配慮された攻撃に強い内部ネットワーク等の構築を図る。

（イ）自治体情報セキュリティクラウドの構築

自治体における不正通信の監視機能の強化等への取組に際し、より高い水準のセキュリティ対策を講じるため、インターネット接続ポイントの集約化やセキュリティ監視の共同利用等を図る。

② 総合行政ネットワークシステム（LGWAN）に関するセキュリティ対策事業

③ 情報提供ネットワークシステムに関するセキュリティ対策事業

情報提供ネットワークシステム全体を保護し、より安全な情報連携を実現するための対策を実施

外務省サイバーセキュリティ施策

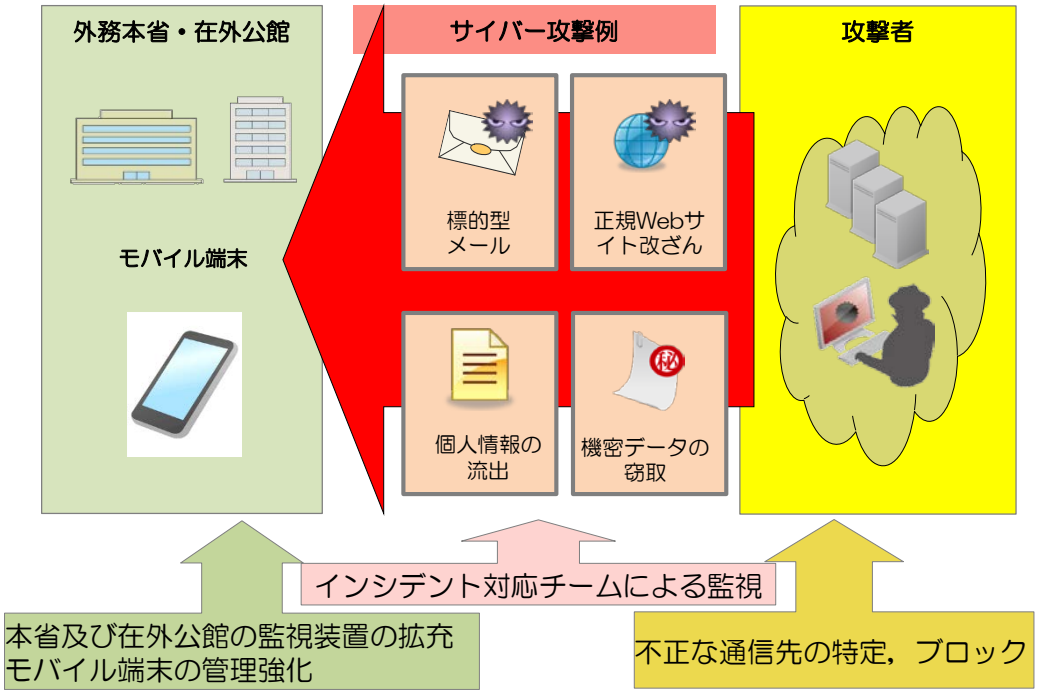
平成２７年度当初予算　　：５．０億円
平成２８年度予算概算要求：４．９億円（うち事項要求０.６億円）

情報セキュリティ対策の強化

平成２８年度予算概算要求：４．８億円（うち事項要求 ０.６億円）

事業概要･目的

○概要
　サイバー攻撃は年々巧妙化し，侵入を防ぐことは困難な状況になっており，侵入を前提とした監視・検知の強化などの多重防御による対策強化を図る。



○多様化する攻撃に対する，侵入されることを前提とした防御の多層化

サイバー空間における外交及び国際連携

平成２８年度予算概算要求：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／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

○重要インフラ等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27年度予算　　：36.1億円

平成28年度概算要求　：53.2億円

○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。

○特に、平成28年度はNISCとの連携を強化し、重要インフラを含む官民の重要施設・機関に対する標的型サイバー攻撃情報の共有体制等を抜本的に拡充。

○さらに、政府調達等のためのIT製品のセキュリティ評価・認証や、官民で連携した高度セキュリティ人材育成のための合宿研修を引き続き実施。

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

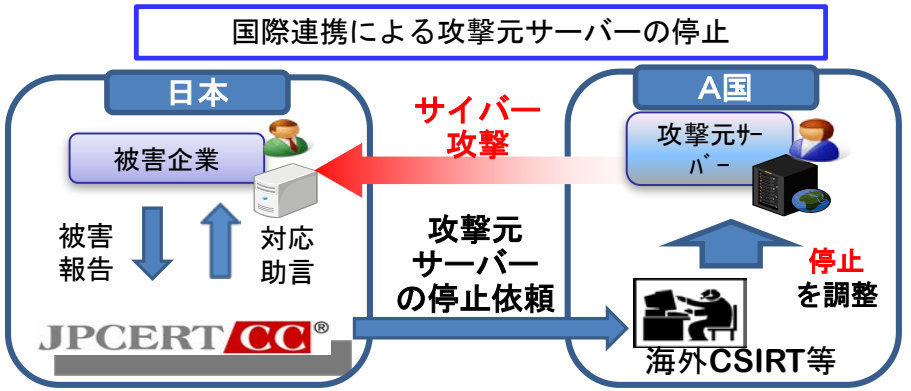
○サイバーセキュリティ経済基盤構築事業

平成27年度予算　　：17.7億円

平成28年度概算要求　：23.6億円

・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。

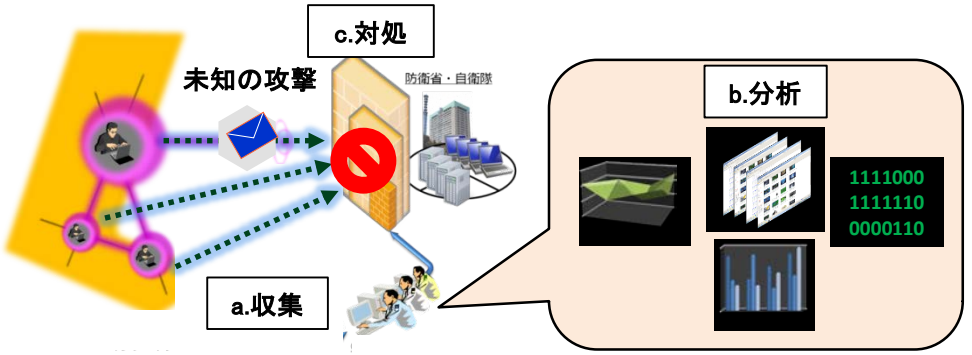


防衛省の施策例

情報収集機能や調査分析機能の強化

平成28年度概算要求額 ： 42億円

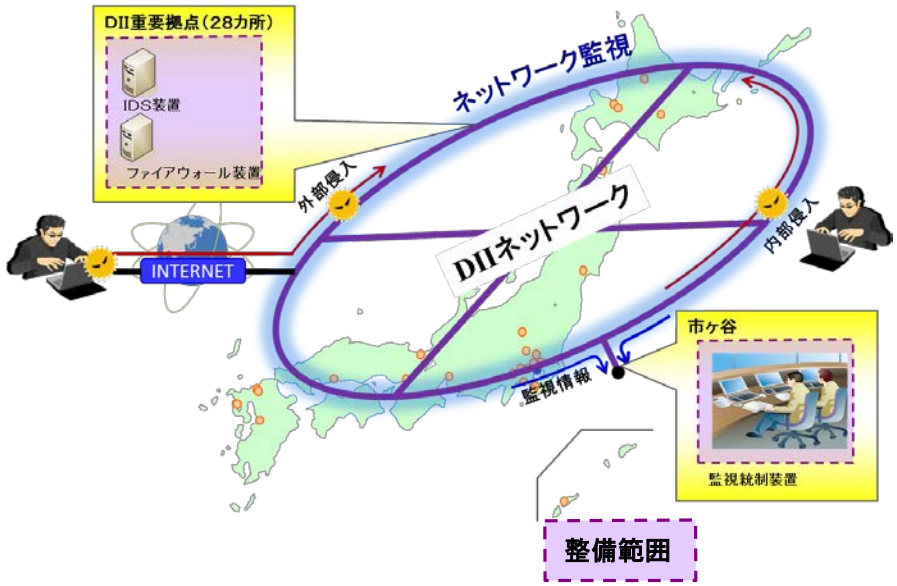
○　サイバー防護分析装置の整備（３８億円）
　　サイバー攻撃手法の高度化・複雑化に対応するため器材を最新化し、ウイルス解析能力等の機能を向上
○　サイバー攻撃情報の収集機能の整備強化（４億円）
　　サイバー攻撃対処に資するため、サイバー攻撃の兆候を検知・分析する機能を整備強化



ネットワーク監視器材の整備

平成28年度概算要求額 ： 61億円

　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



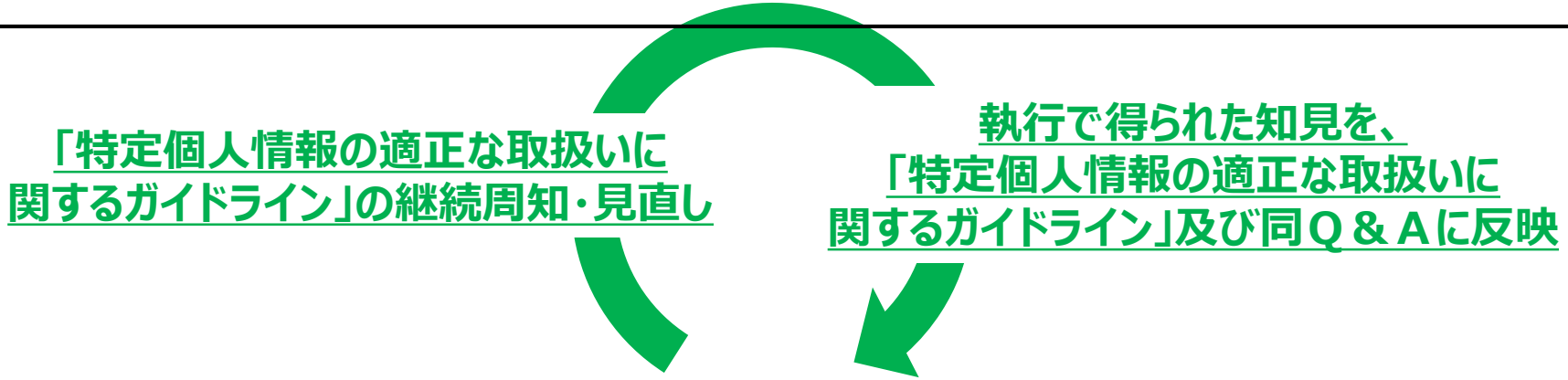
特定個人情報保護委員会の施策例

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・監督体制を整備

（平成27年度当初予算：63.7百万円、平成28年度予算要求：320.4百万円＋事項要求）

○　監視・監督に係る業務体制の整備

- 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

情報セキュリティ対策の強化

平成28年度概算要求：62．1億円（新規）

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。

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）
• 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	• 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

主な概算要求事項

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
■セキュリティ監査の実施