NISC National InFormation Security Center

サイバーセキュリティ推進体制の強化について

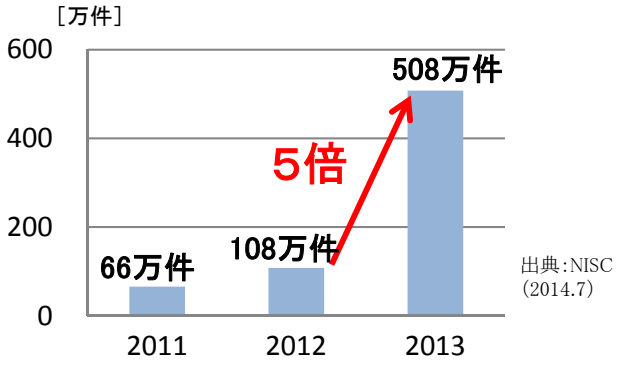
平成26年10月24日
内閣官房情報セキュリティセンター

サイバー脅威の深刻化

政府機関等への攻撃激化

⇒ 6秒に1回攻撃が発生

センサー監視等による脅威件数



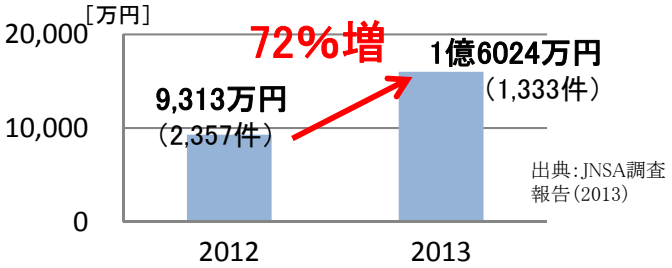
強化①

政府機関の防護・対処能力の強化

攻撃対象の拡大・深刻化

⇒情報漏えい事案の被害額が増加

1件あたりの想定損害賠償額



⇒重要インフラ(情報通信、鉄道等)への攻撃件数が増加

出典:NISCへの通報件数

76件(2012年度) → 133件(2013年度)

約2倍

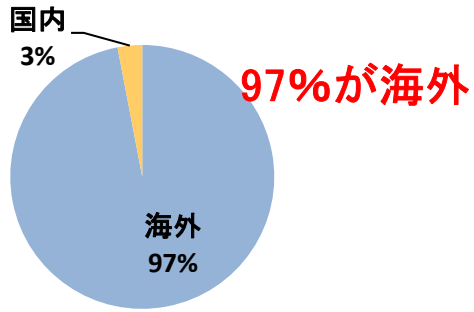
強化②

官民連携の強化

サイバー攻撃のグローバル化

⇒攻撃のほとんどが国境を越える

不正プログラムの接続先(2013)



出典:警察庁(2014.2)

強化③

グローバルな連携強化

政府戦略

以下の各戦略において、サイバーセキュリティ推進体制の強化の必要性が規定。

- 国家安全保障戦略 (H25.12.17 閣議決定)
- サイバーセキュリティ戦略 (H25.6.10 情報セキュリティ政策会議決定)
- 「日本再興戦略」改訂 2014 (H26.6.24 閣議決定)

サイバーセキュリティに係る国家戦略を策定・推進する

司令塔機能の強化や体制整備が急務

東京五輪へ向けた準備

2012年のオリンピック・パラリンピックロンドン大会では、開催期間中、約2億件のサイバー攻撃が発生。英国政府は、6年前からサイバー攻撃対策を準備。

「日本再興戦略」改訂2014＜抜粋＞

サイバーセキュリティ推進体制等の強化

情報の自由な流通の確保及びそのためのITの利用における安全性及び信頼性を確保し、成長戦略を確固たるものとするため、サイバーセキュリティに関する政府の機能について、国自らがリーダーシップを強く発揮できる推進体制への抜本的強化を図る。このため、法制度の在り方も含めて検討を深め、2015年度までに法制上の措置など必要な措置を講ずる。

また、「新・情報セキュリティ人材育成プログラム」（2014年5月 情報セキュリティ政策会議決定）に基づき、サイバーセキュリティに関する人材の量的不足の解消と突出した能力を有する人材の確保のため、情報処理技術者試験の見直しなど、2016年度までに必要な措置を講ずる。

政府におけるサイバーセキュリティ確保のための機能強化

サイバーセキュリティ基本法案

［(衆)内閣委員長提案により186回通常国会へ提出。衆院通過後、参院にて継続審査］

NSC（国家安全保障会議） ⇔ 緊密連携

IT総合戦略本部 ⇔ 緊密連携

サイバーセキュリティ戦略本部

（本部長：内閣官房長官）

- サイバーセキュリティ戦略本部の所掌事務を規定
  - サイバーセキュリティ戦略案の作成
  - 政府機関等の防御施策評価（監査を含む）
  - 重大事象の施策評価（原因究明調査を含む）
  - 各府省の施策の総合調整（予算を含む）
- サイバーセキュリティ戦略本部に関する事務は、内閣官房副長官補が掌理

資料等提供義務 ↑　勧告 ↓　勧告に基づく措置の報告聴取 ↓

各府省等

政府における法制の整備

［政府において法制を整備し、新体制を速やかに発足］

政府において本部に関する事務を内閣官房で行わせる等のために必要な*法制*を整備（基本法附則第２条）

内閣サイバーセキュリティセンター

- 内閣サイバーセキュリティセンターの所掌事務を規定
  - GSOCに関する事務
  - 原因究明調査に関する事務
  - 監査等に関する事務
  - サイバーセキュリティに関する企画及び立案並びに総合調整
- センター長には、内閣官房副長官補をもって充てる

＋

戦略本部の事務の稼働状況、東京オリンピック・パラリンピック大会開催に向けた準備、サイバー空間における脅威の増大に対応した追加的な体制強化の必要性等を踏まえつつ、

法制の追加的な整備について引き続き検討

（注） 上記の方向性について、「我が国における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」（情報セキュリティ政策会議決定予定）にて明確化。

2015年度（平成27年度）当初から本格稼働

今後の課題

現在のNISCの位置づけ及びその担当する事務を法制上明確化するにあたっては、2020年オリンピック・パラリンピック東京大会も見据えつつ、主に以下の項目について必要な措置の検討を行い、可及的速やかに結論を得る。

総合調整機能の強化

- 政府機関における対策状況の監査
- 万一、重大なインシデントが発生した場合の原因究明調査

GSOC機能の強化

- 新システムの運用を見据えた体制、機材の整備
- 施設整備に関する具体的計画の策定・推進

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

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

国際連携の強化

- 国際連携・国際協力担当グループの体制整備
- 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

人材の育成及び登用

- 各省庁からの派遣人材を通じ、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

（参考）諸外国における戦略策定・体制強化の状況

サイバーセキュリティに関する国家戦略の策定・体制強化については、欧米諸国等において進展しており、我が国も欧米諸国に後れを取ることなく対応する必要がある。

	戦略策定	体制強化
米	2009年に、包括的国家サイバーセキュリティ戦略を見直し、**省庁間の調整機能の強化**や官民連携による**インシデント対応強化**等の取組を実施	2009年に、関連政策の**統括・調整機能の強化のため**、ホワイトハウスに**サイバーセキュリティ調整官を設置**したほか、同年、官民連携による対策強化のため、国土安全保障省に国家サイバーセキュリティ・通信統合センター（NCCIC※1）を設置
英	2011年に、国家サイバーセキュリティ戦略を見直し、脆弱性情報やサイバー脅威に関する官民の**情報共有パートナーシップの立ち上げ**等の取組を実施	2010年に、**政府横断的な対応強化のため**、内閣府に**サイバーセキュリティ・情報保証部を新設**したほか、2012年のロンドンオリンピックを契機として、2014年3月にCERT-UK※2を内閣府に設立
仏	2011年に、急激に進化する**サイバー脅威の監視・分析**や政府・重要インフラのシステム保護を内容とする情報システム保護・セキュリティ戦略を策定	首相府の下に置かれる国家情報システム・セキュリティ庁の体制を**2015年までに現行の350名から500名に拡充**する旨を公表
EU	2013年に、重要インフラや情報サービス事業者に対する**インシデント報告等の義務付け**（指令案）を含む、EUサイバーセキュリティ戦略を策定	左記指令案において、加盟各国におけるインシデント対応機関の設立や、加盟各国と欧州委員会の間におけるサイバー脅威や**インシデント関連情報共有システムの構築**を規定

※1　NCCIC：National Cybersecurity Communication Integration Centerの略
※2　CERT-UK：Computer Emergency Response Team – United Kingdomの略