NISC National Information Security Center

情報セキュリティの内外の動向と政府の対応

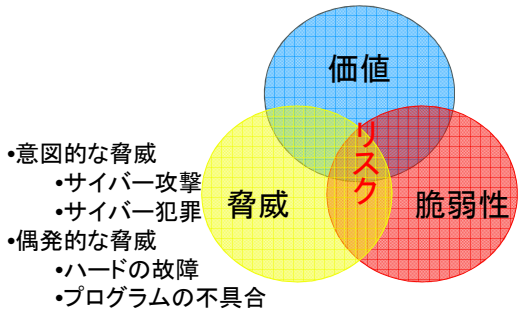
第14回サイバー犯罪に関する白浜シンポジウム
平成22年6月4日

内閣官房情報セキュリティセンター(NISC)
内閣参事官　木本裕司

脅威と脆弱性

NISC

国政上の秘密、個人情報、行政サービス、国家の威信・安心感



- 意図的な脅威
  - サイバー攻撃
  - サイバー犯罪
- 偶発的な脅威
  - ハードの故障
  - プログラムの不具合
  - 人為的な操作ミス
  - 自然災害

- ソフトウェアの脆弱性
- ハードウェアの抗堪性
- 組織マネジメント

1

最近の情報セキュリティに係る脅威の動向

- 最近の情報セキュリティに係る脅威は、ますます大規模化・高度化・複雑化
- 昨年7月には米韓政府機関等に対し大規模なDDoS攻撃が行われるなど、国家規模でのサイバー攻撃の脅威も現実化
- 重要インフラ部門がサイバー攻撃を受けると、国民生活に甚大な影響

2

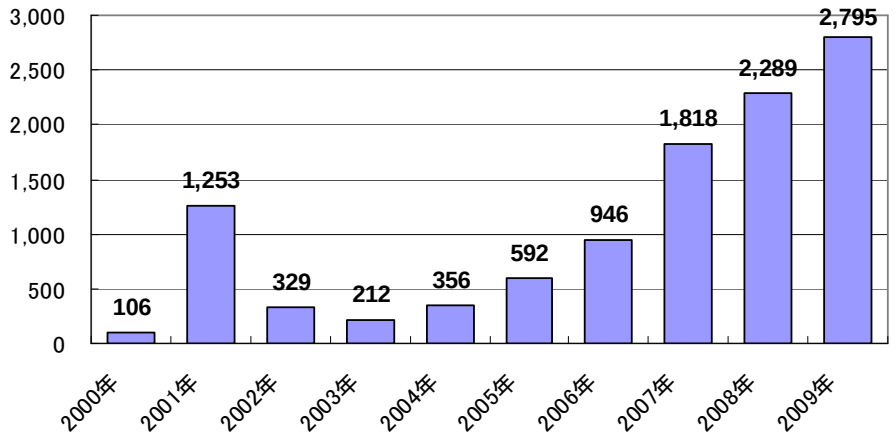
最近の事例

2007.4	エストニア政府機関等へのDDoS攻撃
2007.10	鉄道業A社の自動改札システムで障害。 首都圏約660駅で計4400台の改札機が使用不能に。 260万人に影響
2008.5	金融業B社でシステム障害。 約2万件が約5時間にわたり取引不能に
2008.8	グルジア政府機関へのDDoS攻撃
2008.9	航空業C社でシステム障害。 53便欠航、276便に遅れ。約54,000人に影響
2009.2	D県HPへ大量アクセス 一時閲覧しにくい状態に
2009.4	E省のHP改ざん
2009.4	F省地方支分部局の非公開HPの改ざん
2009.7	韓国、米国政府機関等への大規模なDDoS攻撃
2009末	「ガンブラー攻撃」によるウェブサイト改ざん被害等が増加

※ 本資料は報道ベースで作成

3

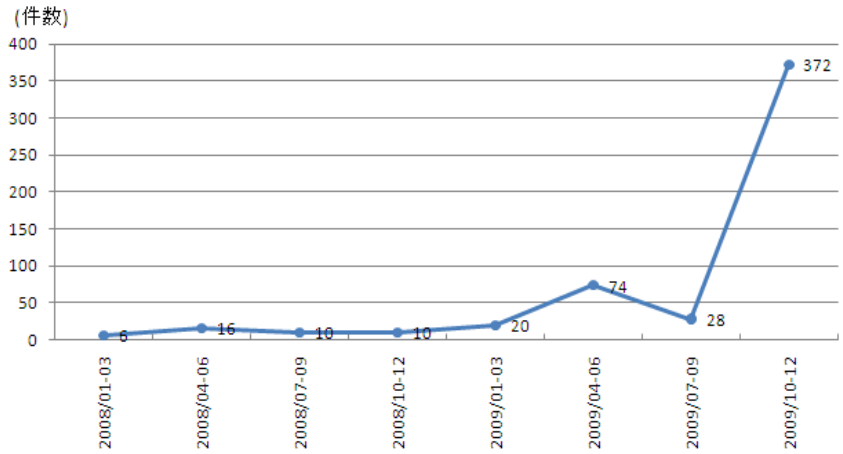
不正アクセス行為の認知状況の推移



【出典】警察庁

4

Web改ざんの届出件数の推移



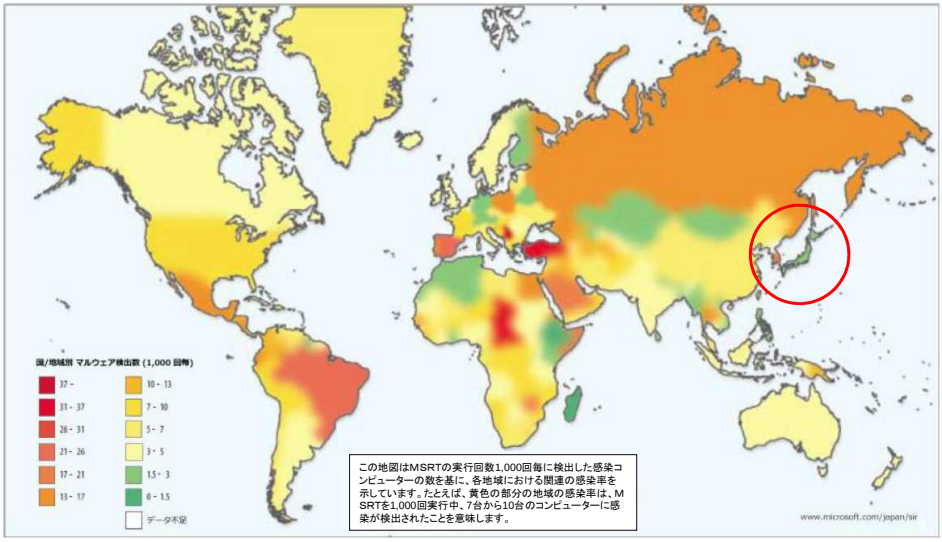
【出典】JPCERT/CC

5

国/地域別マルウェア感染率（2009年上半期）

NISC

日本におけるマルウェア感染率は0．3%（世界平均0．87%）と比較的低い。



マイクロソフト セキュリティ インテリジェンス レポート 第7版（2009年1月～6月）

6

情報セキュリティは経済社会の基盤

NISC

我が国の持続的発展と情報通信技術を活用したより良い国民生活の実現

情報通信技術の利用促進・活性化

- ◆電子政府・電子自治体
- ◆医療・教育の情報化
- ◆情報通信産業と情報通信利用産業の振興

等

情報通信技術の安全・安心の確保

- ◆政府機関等に対するサイバー攻撃
- ◆重要インフラのIT障害
- ◆新たなマルウェアの出現・開発環境の普及

等

情報通信技術を安心して利用できる環境の実現 ：「情報セキュリティ先進国」

政策の枠組み

IT戦略本部の下に「情報セキュリティ政策会議」（議長：内閣官房長官）設置
- ◆「情報セキュリティ基本計画」等を策定
- ◆「国民を守る情報セキュリティ戦略」を策定

推進体制

内閣官房情報セキュリティセンター（NISC、センター長：内閣官房副長官補）設置
- ◆「情報セキュリティ政策会議」の事務局として、各種戦略を企画・立案
- ◆ 官民連携により、統一的・横断的な情報セキュリティ政策を推進
- ◆ 24時間365日体制で、政府機関ホームページ等への攻撃を監視

省庁HP連続改ざん 2000.1

年度 2000 2005 2006 2008 2009 2010 2012

国民を守る情報セキュリティ戦略

第１次情報セキュリティ基本計画　第２次情報セキュリティ基本計画

内閣官房情報セキュリティ対策推進室（2000.2設置）

内閣官房情報セキュリティセンター（2005.4 設置）

情報セキュリティ政策会議（2005.5 設置）

7

情報セキュリティ政策の推進体制

NISC

内閣官房を中心に関係省庁も含めた横断的な体制を整備

高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）

本部長　内閣総理大臣
副本部長　内閣特命担当大臣（科学技術政策）
内閣官房長官
総務大臣
経済産業大臣
本部員　本部長及び副本部長以外のすべての国務大臣
民間有識者（8人）

（事務局）
内閣官房IT担当室
室長（官房副長官補（内政））

情報セキュリティ政策会議　（2005年5月30日 IT戦略本部長決定により設置）

議長　内閣官房長官
議長代理　内閣府特命担当大臣（科学技術政策）
構成員　国家公安委員会委員長
総務大臣
経済産業大臣
防衛大臣
小野寺　正　KDDI株式会社代表取締役社長兼会長
黒川　博昭　富士通株式会社相談役
土屋　大洋　慶應義塾大学大学院准教授
野原　佐和子　株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英　首都大学東京法科大学院教授
村井　純　慶應義塾大学教授

閣僚が参画

重要インフラ所管省庁
金融庁（金融機関）
総務省（地方公共団体、情報通信）
厚生労働省（医療、水道）
経済産業省（電力、ガス）
国土交通省（鉄道、航空、物流）
その他の関係省庁
文部科学省（セキュリティ教育） 等

（事務局）
内閣官房情報セキュリティセンター（NISC）
センター長（官房副長官補（安危））
副センター長（内閣審議官）2名
内閣参事官5名

協力
協力4省庁
警察庁（サイバー犯罪の取締り）
総務省（通信・ネットワーク政策）
経済産業省（情報政策）
防衛省（国の安全保障）

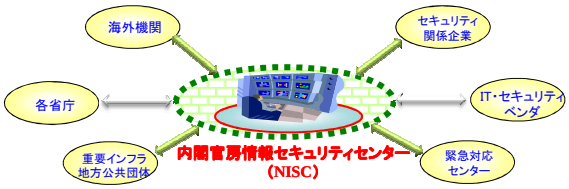
重要インフラ事業者 等　政府機関（各府省庁）　企業　個人

8

「第2次情報セキュリティ基本計画」について

NISC

■ NISCを中心とした新たな官民連携の取組みにより、複雑化・高度化する情報セキュリティ対策に対処
■ 「第2次情報セキュリティ基本計画」（2009～2011年の3カ年計画）に基づく政策の推進



◆ NISCを結節点とした官民連携の強化、我が国全体としての対処能力の最大化
◆ 統一的・横断的な情報セキュリティ対策の推進による底上げ
◆ PDCAサイクルによる持続的改善
◆ 国際連携の強化によるイニシアティブの発揮

政府機関・地方公共団体
「政府機関統一基準」等により情報セキュリティを確保
【主な施策】
① サイバー攻撃等への緊急対応
②情報セキュリティ体制の整備
（最高情報セキュリティ責任者（CISO）の設置など）
③政府機関統一基準の策定
（各省庁が守るべき最低限の対策水準を規定）
④政府機関におけるPDCA

重要インフラ
「重要インフラ行動計画」に基づく官民連携による重要インフラ防護
【主な施策】
① 安全基準等の整備
② 情報共有体制の強化
③ IT障害の波及の最小化
（共通脅威分析、演習等）
※重要インフラ（10分野）
情報通信　金融　航空
鉄道　電力　ガス
行政サービス　医療
水道　物流

企業・個人
普及啓発の推進
【主な施策】
①「情報セキュリティ月間」の実施
②情報セキュリティガバナンス確立の支援

横断的取組
● 情報セキュリティ技術戦略の推進
● 情報セキュリティ人材の育成確保
● 国際連携・協調の推進
● 犯罪の取締り、権利利益の保護救済

9

「国民を守る情報セキュリティ戦略」について（平成22年5月11日策定）

NISC

（注）「第2次情報セキュリティ基本計画」を包含する新たな情報セキュリティ戦略（2010年度から2013年度）

現状の課題

- 大規模なサイバー攻撃事案等の脅威の増大
- 社会経済活動の情報通信技術への依存度の増大
- 急速な技術革新の進展
- グローバル化の進展

● **重要インフラ等の国民生活に直結するサービスのIT化により、脅威は着実に増大**
● 情報セキュリティ上の攻撃手法が多様化・高度化・複雑化しており、従来の取り組みでは対応が困難

課題に対応する新戦略の必要性

「国民を守る情報セキュリティ戦略」

基本的な考え方

安全・安心な国民生活を実現

- サイバー空間上の我が国**安全保障・危機管理**の確保
- 情報通信技術の利活用を促進し、我が国の経済成長に寄与

具体的な取組

大規模サイバー攻撃事態への対処態勢の整備

- **■対処態勢の整備**
  - ・初動対処態勢の整備
  - ・初動対処訓練の実施
  - ・官民連携の推進
  - ・サイバー攻撃に対する防衛分野での体制強化
  - ・サイバー犯罪の取締
- **■平素からの情報収集・共有体制の構築・強化**
  - ・対処に資する情報収集・分析・共有体制の強化
  - ・諸外国等との情報共有体制の構築・強化

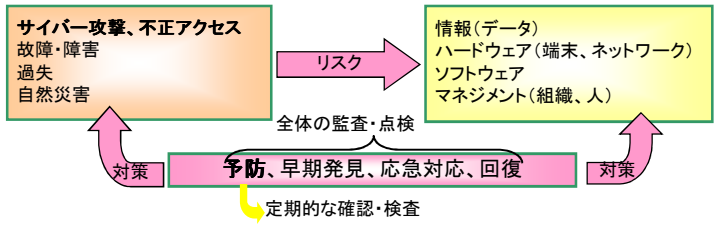
新たな環境変化に対応した情報セキュリティ政策の強化

- **■国民生活を守る情報セキュリティ基盤の強化**
  - ・政府機関等の基盤強化
  - ・重要インフラの基盤強化
  - ・その他の基盤強化
- **■国民・利用者保護の強化**
  - ・普及啓発活動の充実・強化
  - ・情報セキュリティ安心窓口（仮称）の検討
  - ・個人情報保護の推進
  - ・サイバー犯罪に対する態勢の強化
- **■国際連携の強化**
  - ・米・ASEAN・欧州等
  - ・APEC・ARF・ITU等国際会合通じた情報共有体制の強化
  - ・NISC窓口機能の強化
- **■技術戦略等**
  - ・研究開発の戦略的推進
  - ・人材の育成
  - ・情報セキュリティガバナンスの確立
- **■制度整備**
  - ・サイバー空間の安全性・信頼性向上の制度の検討
  - ・各国の情報セキュリティ制度の比較検討

10

情報セキュリティ対策の基本的な考え方

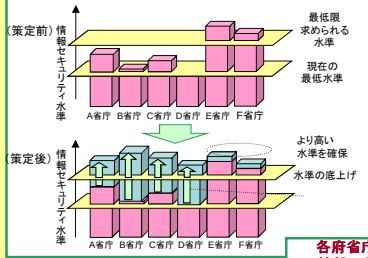
NISC



政府機関における情報セキュリティ対策（「政府機関統一基準」等による対応）

＜政府機関統一基準の目的＞

各府省庁が守るべき最低限の対策水準を定め、情報セキュリティ水準の向上を図る。



各府省庁は、統一基準に準拠した情報セキュリティポリシーを策定。

＜政府機関統一基準の主な内容＞

1. 情報（データ）
   情報の取扱い、暗号、電子署名
2. ハードウェア（端末、ネットワーク）
   端末、電子メールサーバ、webサーバ、ファイルサーバ、通信回線、アクセス制御、踏み台対策、ウィルス感染対策、物理的防護措置
3. ソフトウェア
   アプリケーションの脆弱性
4. マネジメント（組織、人）
   組織・体制の整備、教育、自己点検、監査、障害・事故対策、外部委託

＜NISCによる、その他の主な取り組み例＞

①重点検査
ハードに係る対策の検査

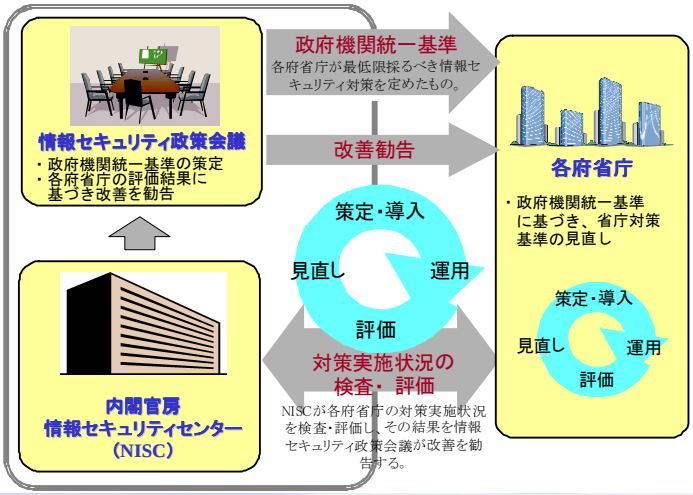
②サーバ集約化
ハード、組織・体制に係る対策

③対策実施状況報告
組織体制、自己点検、教育

11

政府機関における持続的な情報セキュリティ確保のための枠組み

○ 各政府機関は、「統一基準」を踏まえてそれぞれ対策を実施。**P（計画）-D（運用）-C（評価）-A（見直し）サイクルに基づいて、毎年、その実施状況を検査・評価**。これを踏まえて、情報セキュリティ政策会議が改善を勧告
○ **「統一基準」自体も、**各省庁における対策の定着状況や技術の変化等を踏まえつつ、**随時改訂**することにより、持続的に情報セキュリティを向上・改善（2005年12月13日初版決定、現在は第4版）



12

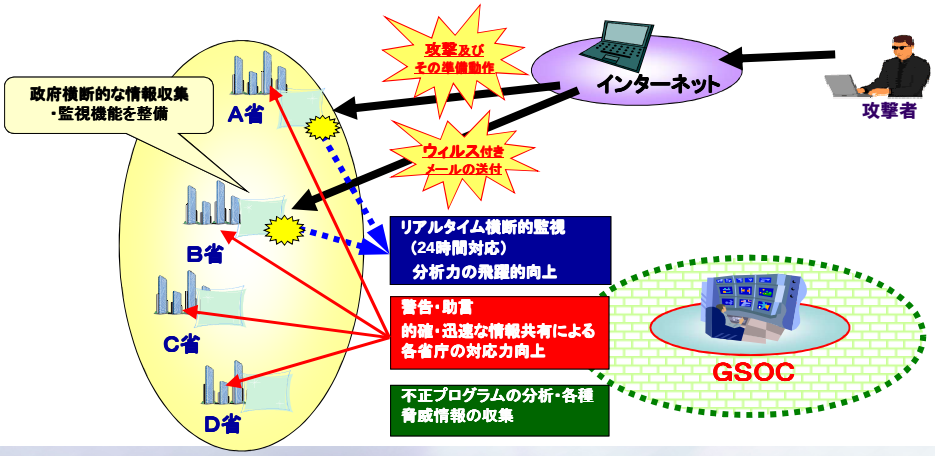
政府横断的な情報収集・分析システム（GSOC）

（注）Government Security Operation Coordination team

目　的

■ **情報セキュリティ問題（外部からのサイバー攻撃など）に対して、政府機関の緊急対応能力強化を図るために整備・運用**

（経緯）
2008年4月～　運用開始
2009年1月～　24時間運用開始　（注）なお、現時点では、本府省省庁のシステムのみを監視対象としている



13

重要インフラの情報セキュリティ対策

官民連携による重要インフラ防護の推進

重要インフラにおけるIT障害が国民生活、社会活動に重大な影響を及ぼさないことを目指す
①予防的な対策と再発防止対策の両側から対処（具体的には、安全基準の整備、情報共有体制の強化など。）
②重要インフラ事業者等における情報セキュリティ対策の浸透状況や急速な技術進展等を踏まえたPDCAの促進

重要インフラ（10分野）
- 情報通信
- 金融
- 航空
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流

NISCによる調整・連携

重要インフラ所管省庁（5省庁）
- 金融庁 [金融分野]
- 総務省 [情報通信分野、行政分野]
- 厚生労働省 [医療分野、水道分野]
- 国土交通省 [航空分野、鉄道分野、物流分野]
- 経済産業省 [電力分野、ガス分野]

関係機関等
- 情報セキュリティ関係省庁
- 事案対処省庁
- その他関係機関

重要インフラの情報セキュリティ対策に係る第2次行動計画

①情報セキュリティ対策の向上（安全基準等の浸透）

重要インフラ各分野に横断的な「指針」に基づいて、「安全基準」等の浸透を図る

②情報共有体制の強化（経験の共有・広範で迅速な対応）

情報の共有により、個々の主体による孤立した対応から、社会全体としての対応を促進

③IT障害の最小化

（1）共通脅威分析

複数分野に共通する潜在的な脅威を発見

（2）分野横断的演習

防護対策向上のための課題抽出

14

分野横断的対策（安全基準等）と官民における情報共有の推進

官民の情報共有体制

セプターカウンシル（2009年2月設立）
重要インフラの各分野により構成される共助活動の場

物流 / 医療 / 鉄道 / 航空 / 損害保険 / 自治体 / 水道 / 放送 / 生命保険 / 証券 / ガス

通信セプター / 銀行等セプター / 電力セプター

情報提供 / 提供情報 / 情報連絡

重要インフラ所管省庁 / 重要インフラ所管省庁 / 重要インフラ所管省庁

NISC

情報セキュリティ関連情報等

情報の共有による迅速な対処と被害拡大の防止等

IPA（注5）
JPCERT（注6）
その他の情報セキュリティ関係機関

分野横断的対策の向上（各分野における安全基準等）

サイバー攻撃をはじめとする意図的要因（ウイルス攻撃、DDoS攻撃等）

（注5）独立行政法人 情報処理推進機構（Information-technology Promotion Agency）
（注6）一般社団法人 JPCERT コーディネーションセンター

分野横断的演習の展開

日本における演習

机上演習 ＋ 機能演習

分野横断的演習

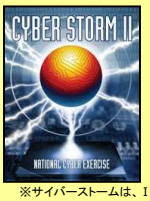
『重要インフラの情報セキュリティ対策に係る行動計画』に基づき、IT障害発生時の重要インフラサービスの維持・復旧や事業継続に向けた課題抽出を目的として、2006年度より毎年実施している。

2009年度は、広域停電の発生を想定した演習を実施し、重要インフラ事業者等のシステムについて停電時の対応に関する課題を抽出し、関係者で共有した。

参加者：重要インフラ事業者（10分野）、関係省庁、有識者等

国際連携

サイバーストームとの連携



サイバーストームⅢ

米国の国土安全保障省（DHS: Department of Homeland Security）が主催する大規模なサイバー演習（2010年秋開催予定）

参加者：米国政府、米国民間企業、米同盟国、国際機関（IWWN等）

※サイバーストームは、Ⅰを2006年に、Ⅱを2008年に開催した。（2年毎の実施）

IWWNのメンバーとして、各国と共に演習に初参画

International Watch and Warning Network（IWWN）

サイバー空間の脆弱性、脅威、攻撃に対応する国際的な取組みを促進する場（机上演習や情報連絡演習を実施）

参加国：先進国15カ国（米国、欧州、日本等）

16

最近の政府機関の取り組み

- サーバの集約化
  - 中央省庁の保有する公開webサーバ(1,000台)、mailサーバ(1,900台)を4年間で半減する
- スピアメール対策
  - DNSサーバへのspfレコードの設定。SMTPサーバの設定。
- ブラウザ, OSの更新の呼びかけ
  - InternetExplorer6の更新。Windows 2000, XP SP2, Vista RTMの更新。
- 各省庁の取り組みの確認と自律的な取り組みのための枠組み作り
  - 対策実施状況調査 → 98%の職員が必要な措置を実施。
  - 重点検査 → 全府省において端末、webサーバ、mailサーバに必要な対策を完全実施。
  - 情報セキュリティ報告書→ 22年度より、各府省は自律的に内部検査、改善に取り組む。
- システム調達、設計段階でのセキュリティの作り込み
  - Secure by Design (SBD)

17

（参考）重要インフラの情報セキュリティ政策に関する日米比較

日本（NISC）	米国（DHS）
■「重要インフラの情報セキュリティ対策に係る第2次行動計画」（2009年2月　情報セキュリティ政策会議決定）に基づき対処	■NIPP*（国家重要インフラ防護計画）（2009年2月国土安全保障省改訂（2006年6月策定））に基づき対処（情報セキュリティは重要インフラ防護の一側面） *National Infrastructure Protection Plan
■重要インフラの対象分野（情報セキュリティ） 情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流の10分野	■重要インフラの対象分野（防護全般） 農業・食糧、防衛産業基盤、エネルギー、健康・公衆衛生、国定記念物・建築物、銀行・金融、水、化学、商業施設、重要製造産業、ダム、救急サービス、原子力、情報技術（IT）、通信、郵便・物流、交通システム、政府施設の18分野
■NISCが中心となって重要インフラ所管省庁と情報共有を推進するとともに、重要インフラ分野ごとのセプター（情報共有・分析機能）やセプターの集まりであるセプターカウンシルを構成し、官民の情報共有体制を構築	■GCC（Government Coordinating Council）やSCC（Sector Coordinating Council）といった政府関係者、重要インフラ事業者の集まりを整備し、官民の情報共有体制を構築
■分野毎の安全基準等の継続的な改善を促進することにより、情報セキュリティ対策等の向上を図る	■分野毎に安全対策に関する評価・見直しを行う枠組を構築し、情報セキュリティ対策等を含め継続的な向上を図る
■IT障害上の脅威を原因事象とした分野横断的演習を実施（毎年開催）	■大規模サイバー演習（サイバーストーム）を実施（2年に1回開催）

18

情報セキュリティ政策の国際的連携の推進

国際的連携の推進の基本的な考え方

（1）**日本におけるPOC（Point of Contact）**としてのNISC（内閣官房情報セキュリティセンター）
（2）**世界の脅威動向の把握**
（3）**アジア**における情報セキュリティ水準の向上
（4）**経済活動のグローバル化**に対応した情報セキュリティの確保
（5）標準化をはじめとする**戦略的国際貢献**
（6）**情報セキュリティ文化**のグローバルな醸成

主な取組みの例

アジア・太平洋

日ASEAN情報セキュリティ政策会議

○セキュアなICT利用（ビジネス）環境構築に向けた協力
○政府SOC（セキュリティオペレーションセンター）の連携
○情報セキュリティ政策の推進　等

APEC（TEL等）　ARF

先進国

日米サイバーセキュリティ会合

○重要インフラ分野における官民連携に係る知見の共有
○政府機関情報セキュリティ対策
○普及啓発対策　等

IWWN　OSCE

グローバル

MERIDIAN

○重要インフラ防護に関する知見の共有
○各国政策当局との直接対話
○グローバルな動向の情報収集
等

FIRST National CSIRT会合　ITU

19

（参考）主な国際会合の概要

NISC

アジア・太平洋

日ASEAN情報セキュリティ政策会議

ASEAN諸国の情報セキュリティに関する政策について、情報連携や具体的な協力関係などを議論する場で、経済および通信規制省庁が参加する。我が国は、第一回政策会議を主催し、主導的役割を果たしている。

アジア太平洋経済協力（APEC（TEL等））

電気通信作業部会セキュリティ繁栄分科会に参加。経済および通信の行政的な議論の場を土台として、21の国と地域が参加する情報セキュリティにフォーカスした会合。我が国は、情報セキュリティ政策に関するPoCとして活動すると同時に、ワークショップの主催や日本での会合を実施。

ASEAN地域フォーラム（ARF）

安全保障を中心に議論する会合で、ASEAN諸国と日本、および米中韓の外務省、法執行機関、通信規制省庁やCERT組織が参加する。地域内で情報を共有するための、Virtual Working Groupを設立することに合意。

先進国

日米サイバーセキュリティ会合

重要インフラ防護政策を中心とした政策的な対話を、NISCと米国国土安全保障省（DHS）が共に毎年実施している。

国際監視警戒ネットワーク（IWWN）

グローバルな重要情報インフラに関するインシデントに対応するため、欧州を中心とする先進15ヵ国から重要インフラ保護のための「政策策定機関」「コンピューター危機管理チーム（CERT）」「法執行機関」が一堂に集まる。我が国は連絡体制に関する演習(ComCheck)を実施するなど積極的に関与しており、次回会合の日本招致も表明している。

欧州安全保障協力機構（OSCE））

56ヶ国の防衛関連省庁が参加し、「サイバーセキュリティに関する脅威」「国内外のグットプラクティスの共有」「サイバーセキュリティを向上させる民間部門の役割」「サイバーセキュリティの向上を推進するOSCEのアプローチ方法」などについて議論する場。

グローバル

メリディアン（MERIDIAN）

重要インフラ防護政策や取組の情報交換を行う場として、G8を中心に欧州・アジアの重要インフラ担当者が参加する、重要インフラ防御の分野では最大規模のカンファレンス。NISCは、プログラム委員として積極的に関与している。重要インフラを所管する省庁および法執行機関が出席している。

FiRST

コンピューター危機管理チーム(CERT)のグローバルなフォーラムで、世界各国の官・民CERTが参加し、インシデント対応事例の紹介など、CERT機関同士の情報交換が行なわれる。我が国は政府機関の危機対応組織として参加している。

国際電気通信連合（ITU）

世界190を超える加盟国が、電気通信に関する標準化および規格を検討する場。我が国は、サイバーセキュリティに関する取り組みについて、我が国で開発した技術等を規格や標準へ反映させる取り組みを実施している。

20

参考資料・URL

NISC

- 内閣官房情報セキュリティセンター（NISC） http://www.nisc.go.jp
- 国民を守る情報セキュリティ戦略
  http://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf
- 政府機関の情報セキュリティ対策のための統一基準
  http://www.nisc.go.jp/active/general/pdf/K303-091.pdf

21