

# 関連資料集

# 目次

## 1. 各国のセキュリティ関連予算の比較

- 1.1 各国の情報セキュリティ予算の比較…………… A-4
- 1.2 各国のセキュリティポートフォリオの比較…………… A-5

## 2. 米国のセキュリティ政策推進状況

- 2.1 重要インフラを巡る米国のセキュリティ政策動向…………… A-9
- 2.2 PCCIP (Presidential Commission on Critical Infrastructure Protection) …… A-10
- 2.3 PDD-63 (Presidential Decision Directive-63) …… A-11
- 2.4 情報システム保護のための国家計画 Ver1.0 …… A-12
- 2.5 大統領令 13231 …… A-13
- 2.6 サイバースペース安全保障のための国家戦略 …… A-14
- 2.7 米国におけるISACの状況 …… A-15
- 2.8 重要インフラに対するサイバー演習 …… A-16
- 参考文献リスト (PCCIP, PDD63, 大統領令 13231) …… A-20

## 3. 各国のセキュリティ推進体制比較

- 3.1 各国のセキュリティ推進体制比較…………… A-22
- 3.2 米国の情報セキュリティ関連組織…………… A-23
- 3.3 イギリスの情報セキュリティ関連組織…………… A-25
- 3.4 フランスの情報セキュリティ関連組織…………… A-26
- 3.5 ドイツの情報セキュリティ関連組織…………… A-27
- 3.6 韓国の情報セキュリティ関連組織…………… A-28
- 3.7 日本の情報セキュリティ関連組織…………… A-29

## 4. 主権リスク関連資料

- 4.1 欧米と日本、韓国におけるIT製品の市場シェア…………… A-31
- 4.2 GPSに対する主要各国の政策・取り組み方針…………… A-32
- 4.3 各国における暗号政策の要点…………… A-35
- 4.4 ルートDNSサーバの現状…………… A-37

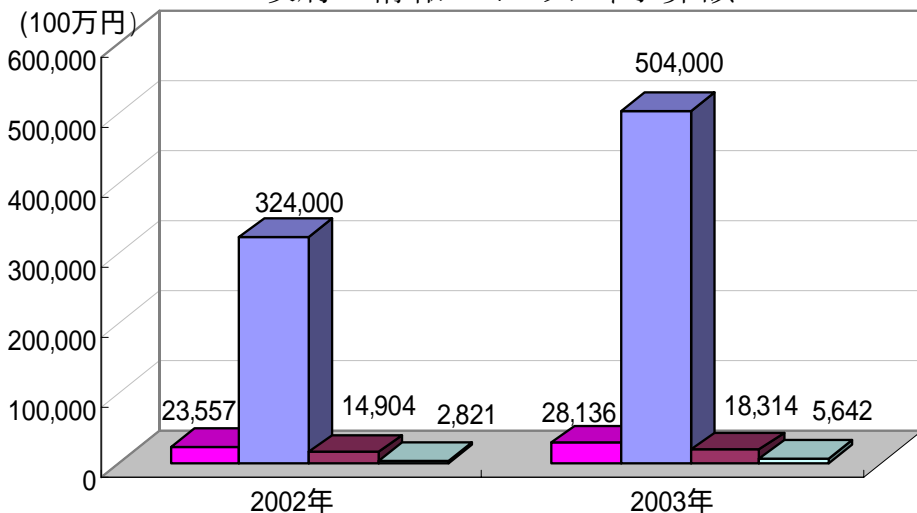
# 1. 各国のセキュリティ関連予算の比較

---

# 1.1 各国の情報セキュリティ予算の比較

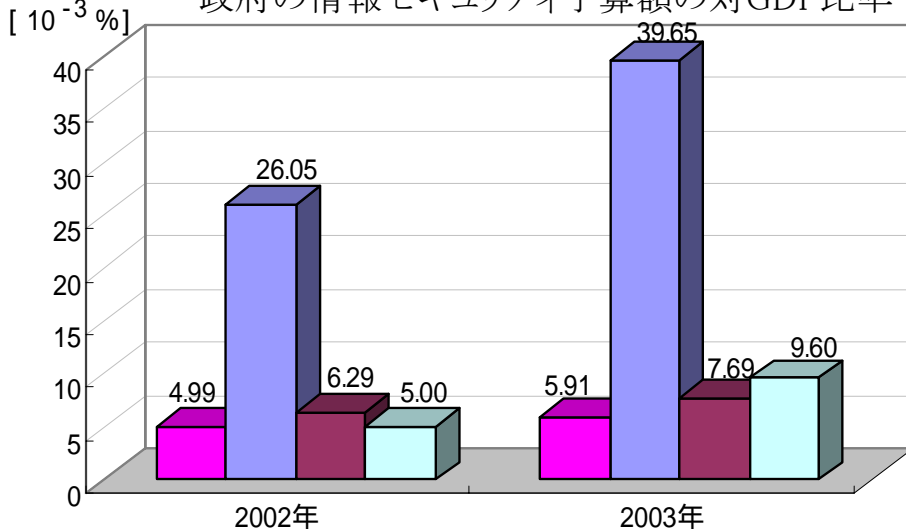
- ▶ 各国政府の情報セキュリティ予算額を比較すると、2002年時点で日本の予算はドイツの約1.6倍、韓国の約8倍の規模にあるものの、アメリカの1割にも満たない。また、2003年には、アメリカでは前年の約1.6倍、韓国では前年の2倍に増額しているが、日本は前年の約1.2倍にとどまる。
- ▶ さらに、対GDP比率で比較すると、日本は、アメリカだけでなく韓国やドイツよりも規模が小さい。

政府の情報セキュリティ予算額



■ 日本 ■ アメリカ ■ ドイツ □ 韓国

政府の情報セキュリティ予算額の対GDP比率

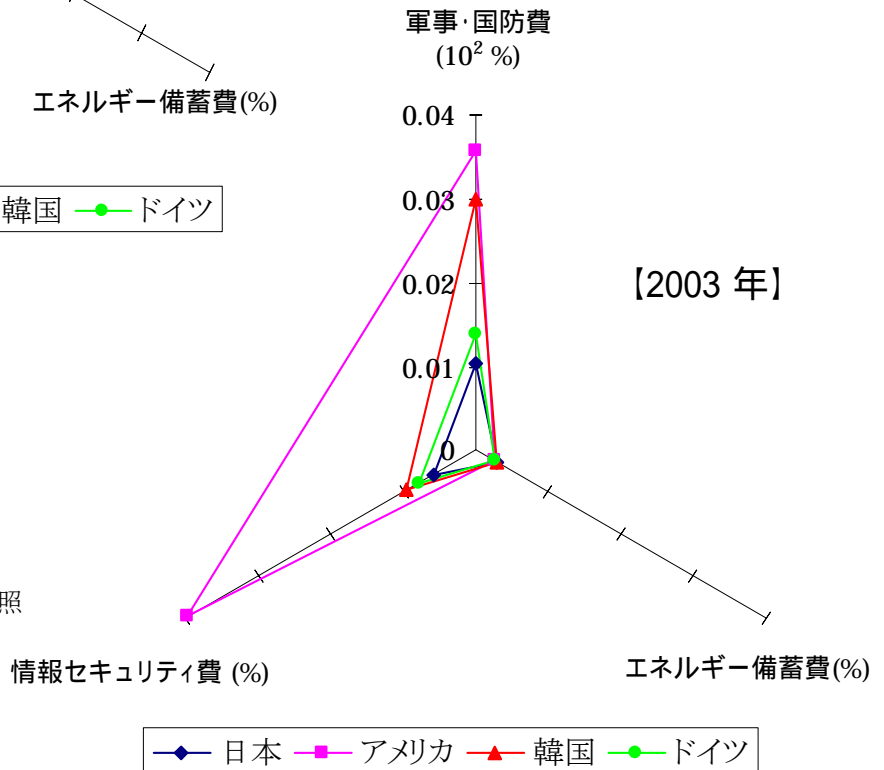
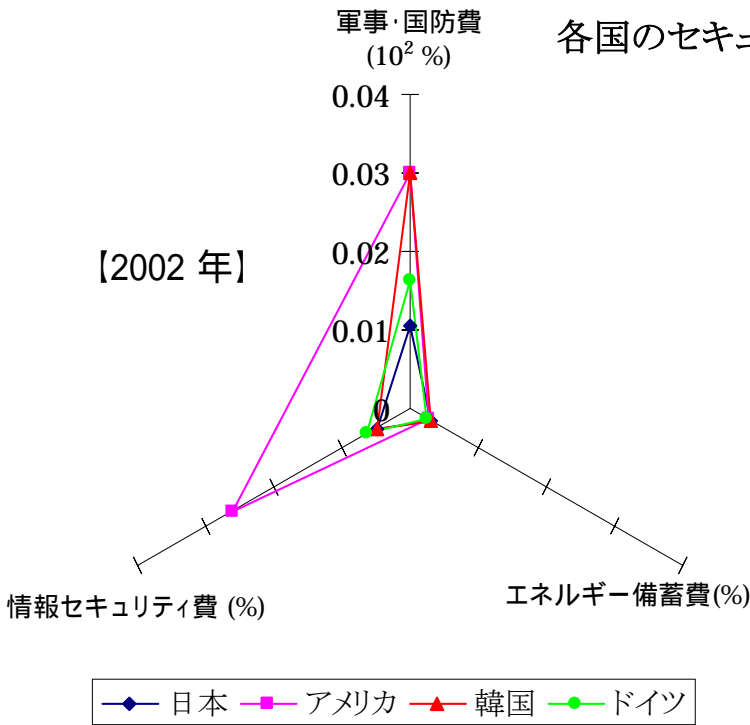


■ 日本 ■ アメリカ ■ ドイツ □ 韓国

## 1.2 各国のセキュリティポートフォリオの比較

- ▶ 各国政府の軍事・国防費、エネルギー備蓄費、情報セキュリティ費の対GDP比率を比較すると、日本の2002年の危機管理予算はアメリカに比べ小規模であり、特に情報セキュリティ費は格差が大きいことがわかる。
- ▶ 2003年の数値を見ると、アメリカ、韓国では軍事・国防費やエネルギー備蓄費に比べ情報セキュリティ費の伸びが著しく、日本との格差がさらに広がっている。

各国のセキュリティポートフォリオの比較(対GDP比)



注) エネルギー備蓄費は、  
石油備蓄量を金額に換算した

各データの正確な数値および出所  
についてはA-6頁およびA-7頁を参照

## (参考) 各国の統計データ一覧

### 各費目の絶対額 (単位:100 万円)

2003年	日本	アメリカ	韓国	ドイツ
軍事費	4,926,500	45,516,000	1,762,022	3,304,000
エネルギー備蓄費	14,242	31,455	1,775	5,807
情報セキュリティ費	28,136	504,000	5,642	18,314

2002年	日本	アメリカ	韓国	ドイツ
軍事費	4,939,500	37,260,000	1,692,000	3,847,900
エネルギー備蓄費	14,240	32,607	1,733	5,821
情報セキュリティ費	23,557	324,000	2,821	14,904

### 各国の GDP

GDP (単位:100万円)	日本	アメリカ	韓国	ドイツ
2002年	472,272,000	1,243,896,000	56,448,000	236,940,000
2003年 (*)	476,049,600	1,271,262,000	58,762,800	238,124,400

(\*) 2003 年の値については IMF による経済成長率の予測値を基に算出

### 各費目の対 GDP 比率

2003年	日本	アメリカ	韓国	ドイツ
軍事費	0.01034871	0.03580379	0.02998533	0.01387510
エネルギー備蓄費	0.00002992	0.00002474	0.00003021	0.00002438
情報セキュリティ費	0.00005910	0.00039646	0.00009601	0.00007691

2002年	日本	アメリカ	韓国	ドイツ
軍事費	0.01045902	0.02995427	0.02997449	0.01623998
エネルギー備蓄費	0.00003015	0.00002621	0.00003070	0.00002457
情報セキュリティ費	0.00004988	0.00026047	0.00004998	0.00006290

# (参考) 出所一覧

## エネルギー備蓄費

IEA 統計 Monthly Oil Survey February 2003 <http://www.iea.org/statist/>

日本 我が国の石油備蓄の現状(資源エネルギー庁) <http://www.enecho.meti.go.jp/info/statistics/>

アメリカ U.S. Crude oil, Energy Information Administration

[http://www.eia.doe.gov/pub/oil\\_gas/petroleum/data\\_publications/  
weekly\\_petroleum\\_status\\_report/current/pdf/table03.pdf](http://www.eia.doe.gov/pub/oil_gas/petroleum/data_publications/weekly_petroleum_status_report/current/pdf/table03.pdf)

<http://tonto.eia.doe.gov/oog/ftparea/wogirs/xls/psw10vwrst.xls>

韓国 内閣府ホームページ 今月のトピック 原油価格高騰に対し比較的弱い中国、韓国

<http://www5.cao.go.jp/keizai3/2003/0317getsurei/topics2.pdf>

日本エネルギー研究所レポート 韓国のエネルギー動向 <http://eneken.iej.or.jp/data/pdf/628.pdf>

## 軍事・国防費

アメリカ 平成14年度防衛白書 [http://jda-clearing.jda.go.jp/kunrei/w\\_fd/2002/honmon/frame/at1401020000.htm](http://jda-clearing.jda.go.jp/kunrei/w_fd/2002/honmon/frame/at1401020000.htm)

平成13年度防衛白書 [http://jda-clearing.jda.go.jp/kunrei/w\\_fd/2001/honmon/frame/at1301020000.htm](http://jda-clearing.jda.go.jp/kunrei/w_fd/2001/honmon/frame/at1301020000.htm)

平成12年度防衛白書 [http://jda-clearing.jda.go.jp/kunrei/w\\_fd/2000/honmon/frame/at1201020000.htm](http://jda-clearing.jda.go.jp/kunrei/w_fd/2000/honmon/frame/at1201020000.htm)

日本 防衛庁 各年度防衛力整備と予算のポイント

<http://www.jda.go.jp/j/library/archives/yosan/2003/point.pdf>

<http://www.jda.go.jp/j/library/archives/yosan/2002/point.pdf>

<http://www.jda.go.jp/j/library/archives/yosan/2001/point.pdf>

韓国 韓国防衛庁ホームページ <http://www.mnd.go.kr/>

## 情報セキュリティ費

日本 高度情報通信ネットワーク社会の形成に関する平成14年度予算について

<http://www.kantei.go.jp/jp/singi/it2/others/14siryu1.html>

アメリカ INPUT 社レポート Federal IT Security Market View 2003年5月発行

韓国 朝鮮日報 2003年1月28日付け記事

[http://japanese.chosun.com/site/data/html\\_dir/2003/01/28/20030128000048.html](http://japanese.chosun.com/site/data/html_dir/2003/01/28/20030128000048.html)

ドイツ IDC 社レポート

IT Security : Government support to private sector in Western Europe 2003年6月発行

\* 政府から民間向けに配分される予算については、IDC 社の推定値を用いた

## GDP

OECD アウトルック概要 <http://www.oecdtokyo.org/theme/macroeconomics/2003/20030424eo73.html>

IMF による見通し <http://www.mof.go.jp/jouhou/kokkin/weo1504.htm>

## 2. 米国のセキュリティ政策推進状況

---

## 2.1 重要インフラを巡る米国のセキュリティ政策動向

業界の動き (2.7 参照)	政府の基本施策	サイバーテロ演習
1999年10月 FS/ISAC 設立	1996年7月 PCCIP:「重要インフラストラクチャ保護に関する大統領特別委員会」が設置され、電力、通信、金融、エネルギー、輸送等の重要インフラの保護に向けた活動が開始される(2.2 参照)	1996年3月 <b>The Day After</b> DARPA が実施した机上演習 攻撃発生 ⇒ 対応 ⇒ 対応策の改善の3ステップからなる。 (2.8 ① 参照)
2000年3月 NCC-ISAC 設立 (Telecom-ISAC)	1998年5月 PDD63 (Presidential Decision Directive 63) の発令 米国の重要インフラを支える情報システムの保護を目的として、PCCIP 活動の成果として報告された一連の勧告のすべての発動を命じる大統領令(2.3 参照)	1997年6月 <b>Eligible Receiver</b> NSA のスタッフが、送電システム 国防総省のコンピュータシステムに実際に侵入を試み、成功する。 送電システムについては、送電を止めることも可能だった。 (2.8 ② 参照)
2000年10月 ES-ISAC 設立	2000年1月 「情報システム保護のための国家計画 Ver 1.0」策定 サイバーセキュリティに関する最初の国家計画(2.4 参照)	1999年10月 <b>Zenith Star</b> 1997 年に実施された <b>Eligible Receiver</b> のシナリオに基づく机上演習。コンピュータネットワーク保護に関わる組織間のオペレーションの調整を目的として実施された。 (2.8 ③ 参照)
2001年1月 IT-ISAC 設立	2001年10月 大統領令 13231 発令 PDD 63 の活動の多くを引き継いだもので、重要インフラに対するサイバー脅威に焦点を当てている。(2.5 参照)	2002年7月 <b>Digital Pearl Harbor</b> 重要インフラへのサイバー攻撃の実行可能性と、それによるダメージの程度を見極める事を目的として実施された。 特定の技術を用いることより、金融システムに障害を与える攻撃が可能であることが示された。 (2.8 ④ 参照)
2001年11月 Energy-ISAC 設立	2003年1月 国土安全保障省設立 National Cyber Security Divisionを2003年6月に設置。	
2002年2月 Food-ISAC 設立	2003年2月 「サイバースペース安全保障のための国家戦略」発表 5つの優先事項が示されるとともに、セキュリティに対する組織と個人の責任に言及。 (2.6 参照)	
2002年4月 ST-ISAC 設立		
2002年4月 Chemical-Sector ISAC 設立		
2002年5月 EFS-ISAC 設立		
2002年12月 Water-ISAC 設立		

## 2.2 PCCIP (Presidential Commission on Critical Infrastructure Protection)

### PCCIP の位置付け

- 重要インフラに対する脅威と脆弱性のスコープと性質の評価
- 重要インフラ保護における法的問題及び、ポリシーに関わる問題の明確化
- 重要インフラを物理的攻撃及びサイバー攻撃から保護するための包括的な国家政策と導入戦略の推奨

### PCCIP の活動内容と成果

1. 重要インフラ所有組織と重要インフラ利用組織のそれぞれを対象にインタビュー調査を行い、意見を収集
2. 情報通信、銀行・金融、エネルギー、物資輸送(商品・ガス・石油・水等)、生活必須サービス(水道・緊急サービス・政府サービス)の各セクタを対象とした研究グループを発足させ、それぞれのセクタに存在する脆弱性とそれに対する推奨策を示した(下表参照)
3. 勧告：CIAO, NIPC, ISAC の設置、研究開発の推進、法律の整備  
目標：2003年までに強固な情報システムインフラを確立する

	指摘された問題点	推奨される対策
情報通信	ネットワークの相互依存の度合いが高まるに従い、サイバー攻撃からネットワークを保護することがより困難になる。交換機、伝送システム、共通線信号システム (Common Channel Signaling System)、高度インテリジェントネットワーク：AIN(Advanced Intelligent Network) のそれぞれにサイバー攻撃に対する脆弱性が存在する。	システムセキュリティに関する原則の導入と推進、インシデント報告プロセスの導入、システムのセキュリティアセスメント、セキュリティ意識向上、セキュリティ技術・サービスの開発推進、リスク管理における意思決定演習
銀行・金融	電子バンキングの導入に伴うインターネット接続の増加により、不正アクセスのリスクが増加する。通信・電力業界の規制緩和の結果生じる不安定要因により、システム全体のサイバーリスクが増加する。	情報共有の推進、コンティンジェンシープラン策定、内部脅威の抑止、バックアップ設備の確保、教育
エネルギー	SCADA (Supervisory Control And Data Acquisition：監視制御・データ収集) システムを経由して、基幹システムに侵入され、重要システムのデータやプログラムが書き換えられる可能性がある。	情報通信セクタにおける NSTAC のような CEO レベルのアドバイザリ顧問の設置、研究開発への投資、セキュリティ標準の策定、教育・トレーニング・啓蒙の強化、脅威や脆弱性に関する情報共有センタの設立、
物資輸送	脆弱性評価が実施されていない セキュリティ標準・ガイドラインがない 脅威・攻撃の特定・追跡を行う組織・機関がない サイバー攻撃に関する情報の共有がされていない	セキュリティ標準・ガイドラインの策定、教育プログラムの開発、セキュリティポリシーの導入、暗号・強化ファイアウォールの使用、信頼できるハードウェア・ソフトウェアの使用
生活必須サービス	サービスを提供するシステムのコンピュータへの依存度が増しているにもかかわらず、コンピュータセキュリティのプライオリティが高くない。	情報の収集・分析・共有、指示警告システムの提供、サイバー攻撃の可能性とシステムの脆弱性に対する意識の向上

出所) A -20頁の参考文献リストを参照

## 2.3 PDD-63 (Presidential Decision Directive-63) (The Clinton Administration's Policy on Critical Infrastructure Protection)

### PDD-63 の意図と目標

- 意図：米国のサイバーシステムに対する物理的およびサイバー攻撃による不安定性の排除
- 目標：2003年までに、攻撃から重要インフラを防衛するための以下のような能力を獲得
- ✓ 重大な国家安全保障任務を遂行し、総合的な公衆衛生と公的安全を保障する連邦政府の能力
- ✓ 命令を遵守し、最低限の重要な公益サービスを提供するために必要となる州政府や地方自治体の能力
- ✓ 秩序ある経済活動と、重要な通信、エネルギー、金融および輸送サービスの提供を保障する民間セクタの能力

### PDD-63 で示された指針

- 議会との協調
- 重要インフラの所有者、運営者と政府で責任を分担
- 評価を頻繁に実施する
- 経済的インセンティブの提供と慎重な規制の適用
- 全ての政府の権限、能力、人材の活用
- プライバシーの尊重
- 政府がインフラ保護の最善の達成法に関するモデルとなる
- 民間セクタの自発的な参加の要請と緊密な連絡

### PDD-63 の成果(組織の誕生)

CIAO、NIPC、NIAC の設立、ISAC(2.6 参照)、PCIS の発足

#### NIPC(National Infrastructure Protection Center) ★現在は、国土安全保障省に統合

- コンピュータ捜査・運営セクション(CIOS)      コンピュータシステムへの不正侵入に関する捜査の支援
- 分析・警告発信セクション(AWS)              国内外からの物理的脅威およびサイバー脅威の評価・分析
- トレーニング・啓発・戦略セクション(TOSS)      連邦、州、地方警察機関と民間、学際との共同学習と情報交換の場の提供

#### PCIS(Partnership for Critical Infrastructure Security)

- ミッション：国家および経済の安全保障に対する脅威が増加しても、重要インフラが安定したサービスを保証できるよう、異業種間および官民の活動を調整する。
- ISAC 設立に向けた協議。
- メンバー：通信・IT、金融、エネルギー、運輸などにおける主要民間企業のCIOら。

#### CIAO(Critical Infrastructures Assurance Office) ★現在は、国土安全保障省に統合

- 様々な分野のインフラ計画を一つの国家計画へ統合
- 各連邦政府部局における重要インフラへの依存に起因するリスクの評価
- 国家的な教育/認知向上プログラムの調整・策定
- 官民両セクタにおける重要インフラストラクチャの保証を目的とした、立法・公的活動の調整

#### NIAC(National Infrastructure Assurance Council)

- ミッション：連邦政府による情報セキュリティに関連する活動のうち、特に民間セクタとの協力が必要とされるものについて、外部の高名な専門家を招聘し、国家戦略形成のためのガイダンスを得る。
- メンバー：全米コーディネータの推薦に基づき大統領が指名。(30名以下)

出所) A-18頁の参考文献リストを参照

## 2.4 情報システム保護のための国家計画 Ver 1.0 (National Plan for Information System Protection Version 1.0)

### 国家計画 Ver1.0 の位置付け

PDD63に従い、2000年1月、サイバーセキュリティに関する最初の国家計画として発表された。

### 国家計画 Ver1.0 の目標

**被害最小化・運用継続化：** 重要インフラに対するサイバー攻撃による被害の最小化。

サイバー攻撃を受けた重要インフラの継続運用の確保。

**検知・分析・対応：** タイミングを計り、サイバー攻撃を検知・分離・分析し、攻撃を封じ込め、素早くシステムを復旧／再構築する。

**強固なインフラ：** 重要インフラへのサイバー攻撃を国家レベルで回避、検知および対応可能とするための組織の確立、人材育成、法整備。

### 国家計画 Ver1.0 における連邦政府の重要インフラ保障計画

国家計画 Ver1.0 では、特に国家の重要インフラ保護という視点において行政と連邦議会が密接に協力することの重要性について謳っている。具体的には、連邦計画における以下の2セクションにおいて、重要インフラ保護のための中核的事項を規定している。

#### 「民間機関保護および政府規模政策」:

法の執行を含む民間および連邦政府機関の重要インフラ保護プログラムについて記述。

また連邦政府規模で実施中の政策の概略および、被害規模を縮小する能力を強化するための政策例を提示。具体的には、特定の省における最も重要なインフラの把握、潜在的弱点の評価・修正、独自の重要システムに対する計画的攻撃を認知・回避するための手段を含む。

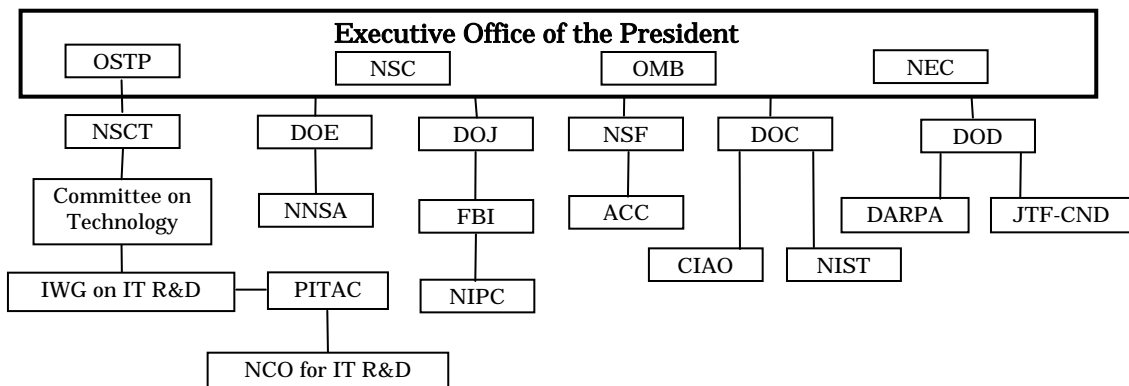
#### 「国防総省インフラ保護計画」:

インフラ防護の先駆者、そして国防という使命の下に国防総省が実施してきた連邦政府計画と民間部門に対する模範政策の詳細を提示。

重要インフラ保護のための枠組み[分析と査定／改善／指示と警告／緩和／対応／再構築]、防衛インフラの範囲、具体的方策等を含む。

### 国家計画 Ver.1.0 の実施に関わる政府機関

各政府機関は、安全保障、研究開発、技術・対策の標準化、人材育成、情報提供・分析等、様々な角度から重要インフラ保護に取り組んでいる。



出所：National Plan for Information Systems Protection Version 1.0 : An Invitation to a Dialogue (2000)

## 2.5 大統領令 13231 ( Executive Order 13231) (Critical Infrastructure Protection in the Information Age)

### 大統領令 13231の位置付け

PDD 63 の活動の多くを引き継いだもので、重要インフラに対するサイバー上の脅威に焦点を当てている。国家計画 Ver 1.0 が、サイバー攻撃の回避・検知・対応およびサイバー攻撃からの早期回復に重点を置いていたのに対し、より広範な視点からの重要インフラ保護の枠組みを提示している。なお、大統領令 13231 は、米国政府内の組織変革に伴い、2003 年 2 月に廃止されている。

### 大統領令 13231 で示された指針

- ✓ **President's Critical Infrastructure Protection Board (PCIPB : 大統領重要インフラストラクチャー保護理事会)** の設置  
PCIPB は、”重要インフラストラクチャーの情報システムを保護するために、ポリシーの推薦とプログラムの調整を実施する” ことを任務とする、
- ✓ PCIPB の活動を補佐する、10 の常設委員会の設置 ( 国家セキュリティシステム、インシデント対応、金融システムインフラ 等)
- ✓ **NIAC ( National Infrastructure Advisory Council)** の設置 ( 下記参照)

### 大統領令 13231 の成果

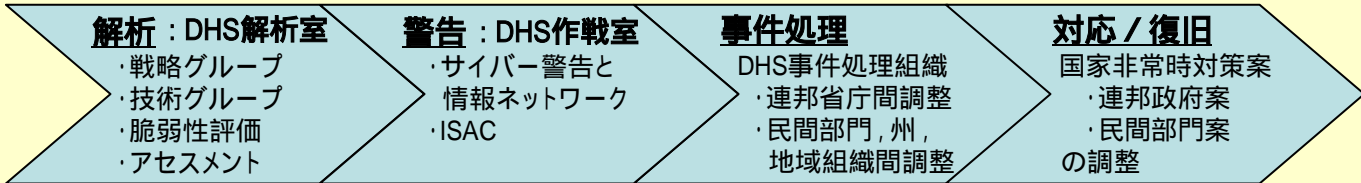
- **PCIPB の役割を明確化することにより、重要インフラ保護政策を進展させた**
  - ✓ 連邦機関の重要インフラの保護と、政府・州・地方自治体・民間企業・学術機関の間での情報共有体制の確立
  - ✓ インシデントハンドリングと危機対応
  - ✓ セキュリティプロフェッショナルの採用と育成のための戦略策定
  - ✓ 研究開発において、OSTP ( Office of Science and Technology Policy : 科学技術政策庁) と協調する
  - ✓ 国際インフラストラクチャーの保護に向けた協調
  - ✓ 重要インフラ保護に関わる法律の制定

### NIAC の概要と役割

- ✓ PDD 63 により設置された **National Infrastructure Assurance Council : NIAC** の後継機関 ( NIAC の名称にある Assurance が Advisory に変わった)
- ✓ 30人以下のメンバにより構成される大統領補佐機関で、銀行・金融、輸送、エネルギー、製造、緊急政府サービスの各インフラストラクチャーを支える情報システムのセキュリティについて、大統領に助言を与える
- ✓ メンバは大統領が任命し、銀行・金融、輸送、エネルギー、通信、緊急政府サービスの各業界の情報セキュリティを担当する CEO から選出される。
- ✓ 民間セクタにおける ISAC の進展状況を監視する

## 2.6 サイバースペース安全保障のための国家戦略

### 優先事項 : 国家セキュリティ対応システムの構築



1. 国家レベルの事象に対応する官民協力体制の構築
2. サイバー攻撃分析、脆弱性評価の戦術・戦略の提供
3. サイバースペースの健全性を概観する民間部門の能力開発支援
4. Cyber Warning and Information Network (CWIN) を拡張し、DHS(国土安全保障省)の危機管理をサポート
5. 国家危機管理の改善
6. 国の官民連携・緊急時対策の開発について、任意参加のプロセスを調整
7. 連邦システムのサイバーセキュリティ連続計画の実施
8. サイバー攻撃・脅威・脆弱性管理に関連する官民情報共有体制の改善と強化

### 優先事項 : 脅威/脆弱性軽減の為のプログラムの実施

1. サイバースペース攻撃の防止と訴追に関する司法当局の権限強化
2. 脅威・脆弱性の潜在的帰結をより詳しく把握するための国家的脆弱性評価プロセスの創設
3. プロトコル/ルーティングの改善によるインターネットメカニズムの保全
4. 高信頼デジタル制御システムと監視制御およびデータ収集(SCADA)システムの利用を助成
5. ソフトウェア脆弱性の低減と改善
6. インフラの相互依存関係を把握し、サイバーシステム・通信の物理的セキュリティを改善
7. 連邦サイバーセキュリティ研究開発に関する議題を優先
8. 新規(emerging)システムの評価とセキュリティの確認

#### 社会的ルール

法執行強化,  
 脅威/脆弱性評価手続き,  
 脆弱性開示手続きの仕組み

#### ソフトウェア

セキュアなOS・コード開発  
 ソフトウェア産業の主導によるセキュリティの促進

#### 物理基盤

物理的セキュリティ向上, プロトコルのセキュア化,  
 ITセキュリティ研究開発への助成, 新技術評価

### 優先事項 : 啓蒙教育プログラムの実施

1. 企業、労働者、国民にサイバースペースの安全性向上を促す啓蒙プログラムの推進
2. 啓蒙・教育プログラムへの助成
3. 既存の連邦サイバーセキュリティトレーニングプログラムの効率性向上
4. 専門サイバーセキュリティ認証制度への民間部門サポートの推進

産業界における  
 セキュリティ  
 貢献者の表彰

#### 啓蒙

ホームユーズ  
 中小企業  
 大企業・大学

#### 教育

初等中等教育プログラム  
 奨学金・育成フェローシップ  
 犯罪捜査訓練プログラム  
 セキュリティ資格プログラム

### 優先事項 : 電子政府のセキュリティ向上

1. 連邦サイバーシステムに対する脅威・脆弱性を継続的に評価
2. 連邦サイバーシステムのユーザ認証管理を行う
3. 連邦サイバーシステム内の無線LANシステムの安全確保
4. 連邦政府の外注・調達におけるセキュリティ向上
5. 州・地方政府の情報技術セキュリティプログラム構築及び、同様の政府組織群との間で情報共有を行うための情報共有/分析センター(ISAC)への参加促進

#### 州政府

ITセキュリティ計画立案  
 ISAC参加奨励

#### 利用者

アクセス管理/認証  
 (アクセス制御ツール評価)  
 無線LANのセキュア化

#### 連邦政府

脅威管理ツールの導入  
 不正接続監視システム設置  
 NIAPの見直し

### 優先事項 : 国家安全保障と国際協力

1. サイバー関連の諜報活動強化
2. 攻撃元の特定および反撃能力の向上
3. サイバー攻撃への対処に向けた国家安全保障共同体内部の結束強化
4. 業界内の連携や国際機関を通じ、情報インフラストラクチャの保護およびグローバルな「セキュリティ文化」の発展にフォーカスした、国際的な官民の対話とパートナーシップを促進
5. 国際的な監視・警報ネットワークの設置を推進し、サイバー攻撃検知・防止能力を向上させる
6. 欧州評議会「サイバー犯罪条約」への加盟、または、各国の法制度・訴訟手続きにおける包括性確保を奨励

#### 国際協力

グローバルなセキュリティ文化の育成  
 サイバー犯罪条約批准推奨  
 国家安全保障共同体内部の調整

#### 安全保障

FBI 対敵情報活動/情報共有  
 攻撃者特定

## 2.7 米国における ISAC の状況

ISAC 名称	運用開始時期	PDD 63 で規定された推進機関	メンバ資格、メンバ企業
FS/ISAC	1999年10月	財務省	銀行、証券会社、保険会社、金融機関
NCC Telecom - ISAC	2000年3月	商務省	* ネットワークサービス・機器・ソフトウェアを提供している企業、CLEC、ISP、連邦機関、州機関、地方自治体機関 * AT&T, Bell South, Boeing, Cisco, CSC, EDS, Lockheed Martin, Lucent, Nortel, Qwest, SAIC, Sprint, Verizon
ES - ISAC (Electricity Sector - ISAC)	2000年10月	エネルギー省	* 北米(アメリカとカナダ)の電力会社、連邦の電力機関 * 独立系の電力業者、州や市の公益事業者 * 電力売買事業者、エンドユーザ
IT - ISAC	2001年1月	商務省	* IT製品、ソリューション、サービスを提供するベンダ、メーカ、プロバイダ * IT・インターネット・電子商取引をベースとするサービス提供事業者 CSC, Veridian, Cisco, HP, IBM, MS, Oracle, Verisign, EDS 等
Energy ISAC	2001年11月	エネルギー省	* 石油会社、天然ガス会社 * 電力会社 * 化石燃料の精製／輸送／貯蔵等に関わる企業
Food Industry ISAC	2002年2月	-	* FMI (Food Marketing Institute) のメンバである企業 * FMI によって承認された組織
ST - ISAC (Surface Transportation - ISAC)	2002年4月	運輸省	鉄道、船舶、トラック等、地上輸送及び海上輸送に関わる組織
Chemical Sector ISAC	2002年4月	-	化学製品製造業者、化学製品販売業者
EFS - ISAC (Emergency Fire Services ISAC)	2002年5月	FEMA (Federal Emergency Management Agency)	全米の消防署長と各地域の消防署・救急施設
Water ISAC	2002年12月	環境省 水資源保護タスクフォース	* アメリカの全ての上水道システム及び下水道システム * ユーザは、シニアマネージャ以上の役職者でなければならない。 * IDの数と会費は、サービスを提供している人口によって決まる。
Inter State ISAC	-	-	全米50州の CIO
Emergency Law Enforcement Services	-	-	全米の法執行機関

## 2.8 重要インフラに対するサイバー演習

## The Day After

- ▶ 実施時期 1996年3月
- ▶ 演習の目的
  - ✓ 米国の情報セキュリティ基盤を拡充するために必要となる研究開発議案への提言作成
- ▶ 実施主体 DoD(DARPA : Defense Advanced Research Projects Agency)
- ▶ 演習の概要
  - ✓ 約60名の政府、大学、報道などの情報インフラ関係者による約半日の机上演習
  - ✓ 西暦2000年に起こると仮定された中東危機を背景とし、重要インフラに対してサイバー攻撃の発生を想定(ページ下部にシナリオの一部を抜粋)。
  - ✓ 演習のプロセス
    - “The Day of” (STEP 1) サイバー攻撃の発生
    - “The Day After” (STEP 2) 対応策の実践
    - “The Day Before” (STEP 3) 攻撃による被害を最小化するために対応策を改善
- ▶ 提言内容
  - ✓ 分散型の適応型セキュリティアーキテクチャ、早い回復力を有する戦略とシステム構築など
- ▶ シナリオの抜粋

5月11日 夕方	NCC がホワイトハウスへ、以下の報告を行う。 ①「カリフォルニア州北部とオレゴン州の電話回線にトロイの木馬が仕掛けられ、回線が不通になった。」 ②「ワシントン州フォートリスの軍事基地の基幹回線がDOS攻撃を受け、通信システムが数時間に渡り、機能不全に陥った。」
5月20日 夕方	全米ネットおよび地方ネットのイブニングニュースが、「陸軍および海軍のLANや電話回線がサイバー攻撃されたため、湾岸地区における米軍の活動に支障をきたしている。」と報道。
5月24日 午後	ワシントンで緊急に国家安全保障会議が開催されることになったが、電話回線が不通のため、大統領は関係者を召集できない。

出所) "Strategic information warfare : a new face of war",  
Roger C. Molander, Andrew S. Riddile, Peter A. Wilson, Rand Corporation

## 2.8 重要インフラに対するサイバー演習

## Eligible Receiver

### ▶ 実施時期および期間

- ✓ 1997年6月 3カ月の準備期間の後に約2週間の攻撃を実施

### ▶ 実施主体

- ✓ NSA

### ▶ 演習の目的

- ✓ アメリカ国内のすべての電力システムおよび電話のシステムのスイッチを切る方法を見つけること
- ✓ 国防省の中にあるコンピュータシステムに不正侵入を試みること

### ▶ 演習の概要

- ✓ NSA のスタッフ35人がハッカーに扮し、合衆国内の3チームと太平洋上の船舶を拠点とする1チームの計4チームが実際にサイバー攻撃を実施

### ▶ 攻撃の成果

- ✓ 米国の9つの市の送電網に侵入し、スイッチを切るサインを残した。
- ✓ DoD のネットワークへの侵入に成功した回数が36回(スーパーユーザーとしてアクセス権を得た)
- ✓ DoD のシステムへの侵入のうち、DoD のシステム管理者が検知できたのは2回

### ▶ 演習後の対策(国防省)

- ✓ コンピュータネットワークの24時間監視体制の確立
- ✓ 800 あるネットワーク全てに IDS およびファイアウォールを設置
- ✓ コンピュータ犯罪について研究するための研究所の設置
- ✓ 最も機密性の高いネットワークに対する公開鍵インフラの整備

出所) CSIS所長(前国防副長官)の John Hamre 氏によるスピーチ

<http://www.iftech.or.jp/00.08.09/CSIS.html>

Global Freedom Institute

<http://www.geocities.com/globalfreedominstitute/AmericasGreatestThreatInfowar.html>

## 2.8 重要インフラに対するサイバー演習

Zenith Star

- 実施時期および期間 1999年10月13～14日の2日間
- 実施主体 IATAC (Information Assurance Technology Analysis Center)
- 演習の目的
  - ✓ Computer Network Defense (CND)コミュニティが、組織間の調整等、その目的を達成するために必要となるプロセスと道具の洗い出し
- 演習の概要
  - ✓ Eligible Receiver のシナリオをベースにして実施された机上演習
  - ✓ 演習のプロセス
    - Eligible Receiver をベースに新CND 組織化のルールや役割分担を理解する
    - Agency 間の要求事項の理解
    - JTF-CND(Joint Task Force CND)と他のサポート機関(例えば NIPC, Intel)に対する調整活動の試験
    - 各チーム(インテリジェンス、法の執行、カウンターインテリジェンス、オペレーション)によって指摘されたポイントの改善
  - ✓ 演習の構造
    - ✓ チーム・プレーを強調
    - ✓ 参加者は、機能的な 4 チームに分割された政府関係者55名
    - Operations チーム(SPACCOM、JTF-CND およびそのコンポーネント)
    - インテリジェンスチーム(CIA、DIA、NSA)
    - 法執行・スパイ防止活動チーム(Defense Criminal Investigative Operations、NIPC)
    - 他のチーム (Joint Staff、国防長官の[OSD]のオフィスチーム)
    - ✓ チーム間のコミュニケーションツールは安全な電話ユニット、STU-III、Face to Face、ファクスと電子メールに限定

出所) IA Newsletter Vol 3. Number 3 “Zenith Star”

## 2.8 重要インフラに対するサイバー演習

Digital Pearl Harbor

- 実施時期および期間 2002年7月24～26日
- 実施主体 Gartner, U.S Naval War College
- 演習の目的
  - ✓ 重要インフラへのサイバー攻撃の実行可能性とそれによるダメージの程度を見極める
- 演習の概要
  - ✓ 主催者から仮想シナリオ(予算、準備期間、人的リソース等) が与えられる
  - ✓ 仮想シナリオに基づいて、電力網システム、通信インフラストラクチャ、インターネット、金融サービスのそれぞれに対して、コンピュータセキュリティの専門家が4つのチームに分かれて攻撃手法を検討する
  - ✓ 実際にシステムに対して攻撃を実施するのではなく、実行可能な攻撃方法と、攻撃が成功した場合に生じると予想されるダメージを机上で考察する
- 演習の結果
  - ✓ 電力網システム : SCADA (\*) システムから侵入して攻撃を実施することが可能であるが、実現性は低い。
  - ✓ 通信インフラストラクチャ : 攻撃に必要な情報が内部者以外には入手困難であることから、攻撃の実現性は低い。また、内部者による攻撃が成功した場合でも、システムの冗長性によりダメージは限定される。
  - ✓ インターネット : peer-to-peer のファイル共有技術と同様の技術を用いた攻撃手法には現実性がある。
  - ✓ 金融サービス : 攻撃者がバックアップファイルをどれだけ破壊できるかによって、システムに重大なダメージを引き起こせるかどうかが決まる。  
インターネットチームが考案した攻撃手法を用いれば、バックアップファイルの破壊も可能である。

(\*) SCADA : Supervisory Control And Data Acquisition 遠隔からシステムの監視制御・データ収集を行うための装置

出所) Gartner : Digital Pearl Harbor: Is It Only a War Game ? (2003)

The Register : Mock cyberwar fails to end mock civilization (2002)

<http://www.theregister.co.uk/content/55/26675.html>

Navy News Week : Navy Wargame Finds Danger Of 'Digital Pearl Harbor' To Be Small (2003)

<http://www.law.uoregon.edu/faculty/shoar/033103/article8.pdf>

# 参考文献リスト (PCCIP, PDD63, 大統領令 13231)

## ➤ PCCIP

- ・Opinion Survey of Infrastructure Owners and Users (1998)
- ・Summary Report on Critical Infrastructure Interviews (1997)
- ・Critical Foundations - Protecting Americas Infrastructures Appendix A.,  
Sector Summary Report (1997) [http://www.ciao.gov/resource/pccip/pccip\\_documents.htm](http://www.ciao.gov/resource/pccip/pccip_documents.htm)

## ➤ PDD63

- ・The Clinton Administration's Policy on Critical Infrastructure Protection :  
Presidential Decision Directive 63 (1998)
- ・「重要インフラにおけるセキュリティ対策の事例調査」(2000年1月) 情報処理振興事業協会
- ・Partnership for Critical Infrastructure Security, April 17, 2002  
<http://www.pcis.org/getDocument.cfm?urlLibraryDocID=17>
- ・PCIS membership application (2002年12月)  
<http://www.uschamber.com/NR/rdonlyres/et36qwph5sgeuevozaoli5ctmqgobu43ew7agd7sy3m2uv2cr3s6e6e4nub63mm7l2j7mkmeizpeyjwlcvw66ka7wth/pcis%2emembershipapp2.pdf>
- ・Executive Order 13130, National Infrastructure Assurance Council, July 14, 1999 (CIO Council)  
[http://www.cio.gov/documents/natl\\_infrastructure\\_assurance\\_council\\_jul\\_1999.html](http://www.cio.gov/documents/natl_infrastructure_assurance_council_jul_1999.html)
- ・CIAO ホームページ <http://www.ciao.gov/>
- ・NIPC ホームページ <http://www.nipc.gov/>

## ➤ 大統領令 13231

- ・Executive Order 13231 : Critical Infrastructure Protection in the Information Age (2001)  
<http://www.ciao.gov/resource/eo13231.html>
- ・GAO : Critical Infrastructure Protection -  
Challenges for Selected Agencies and Industry Sectors - (2003)  
<http://www.gao.gov/new.items/d03233.pdf>

## 3. 各国のセキュリティ推進体制比較

---

# 3.1 各国のセキュリティ推進体制比較

	政策立案・推進 省庁間調整	製品評価・認証	人材育成	セキュリティ関連 技術開発	暗号
イギリス	<p>政府通信司令部 (GCHQ)</p> <p>国家インフラストラクチャ安全調整局</p> <p>各組織 / 機関が個別に実施</p>			<p>通信電子セキュリティグループ (CESG)</p> <p>人員数: 300人 予算: 不明</p>	
フランス	<p>国防総事務局 (SGDN)</p> <p>人員数: 273名 (調整部門 158名)</p>			<p>情報システムセキュリティ中央局 (DCSSI)</p> <p>人員数: 90人 予算: 11億円</p> <p>研修センター      実施部門      科学技術部門</p>	
ドイツ	<p>内務省内 ITセキュリティ室等 (IT-Stabas/KBSSt)</p> <p>人員数: 不明</p>			<p>連邦情報技術安全局 (BSI)</p> <p>人員数: 390人 予算: 63億円</p> <p>人材育成に関しては、企業向けに人材育成マニュアルを作成しているのみ。他に人材育成を担当する機関があるかどうかは不明。</p>	
韓国	<p>情報通信部 (MIC)</p> <p>人員数: 不明 予算: 不明</p> <p>国家情報院</p> <p>人員数: 不明 予算: 不明</p>			<p>韓国情報保護振興院 (KISA)</p> <p>人員数: 約 300人 予算: 40億円</p> <p>電子通信研究院 (ETRI)</p> <p>人員数: 不明 予算: 不明</p> <p>国家保安技術研究院 (NSRI)</p> <p>人員数: 約 100人 予算: 不明</p>	
アメリカ	<p>国土安全保障省 (DHS)</p> <p>人員数 IA&amp;IP: 1,000名 NCSD: 60名 予算 IA&amp;IP: 1,000億円 NCSD: 60億円</p>			<p>国立標準技術研究所 (NIST)</p> <p>人員数: 50人 予算: 18億円</p> <p>全米科学財団 (NSF)</p> <p>人員数: 不明 予算: 30億円</p> <p>国家安全保障局 (NSA)</p> <p>人員数: 不明 予算: 不明</p> <p>情報インフラ保護研究所 (I3P)</p> <p>人員数: 不明 予算: 不明</p> <p>DARPA</p> <p>人員数: 不明 予算: 60億円</p>	
日本	<p>内閣官房 情報セキュリティ対策推進室 (9名)</p>	<p>経済産業省 (NITE/IPA)</p>	<p>経済産業省 (IPA)</p>	<p>経済産業省 (IPA/AIST)</p> <p>総務省 (TAO/CRL)</p>	<p>経済産業省 (IPA) / 総務省 (TAO)</p>

## 3.2 米国の情報セキュリティ関連組織

## 組織の概要

### <情報セキュリティ関連組織とそのミッション>

- 国土安全保障省 (Department of Homeland Security : DHS) 情報分析/インフラストラクチャ保護部 (Information Analysis and Infrastructure Protection : IA&IP) : 脅威分析・脆弱性評価・警告発出/国家安全保障の観点からの重要インフラ保護/セキュリティ対応システムの構築/コンピュータシステム・ネットワークの保護/政府機関と民間セクタとのパートナーシップの確立/人材育成
- 重要インフラストラクチャ保証局 (\*) (Critical Infrastructures Assurance Office : CIAO) : 重要インフラを攻撃から保護し、重要インフラが提供するサービスの継続性を確保するために業界横断的に活動を行う。
- 連邦捜査局 (Federal Bureau of Investigation : FBI) : コンピュータ犯罪の捜査、NIPC との協調による情報インフラの保護
- 連邦コンピュータ事故対応センター (\*) (Federal Computer Incident Response Center : FedCIRC) : コンピュータセキュリティ事件の報告、対応、解決策の提示
- 国家通信システム (National Communications System : NCS) (\*) : 国家安全保障と非常時対応を目的として、通信システムのセキュリティ確保および高機能化を推進
- 国家サイバーセキュリティ部門 (National Cyber Security Division : NCSD) : DHS 内の IA&IP 配下の組織で、CIAO, NIPC, FedCIRC, NCS の機能を統合した役割を果たす情報セキュリティに関する専門部署。各 ISAC の管轄も行う。
- 全米科学財団 (National Science Foundation : NSF) : 2002年に成立したサイバーセキュリティ R&D 法に基づいて、情報セキュリティ関連の研究開発、情報セキュリティ分野の専門家の育成を実施する。
- 情報共有分析センタ (Information Sharing and Analysis Center : ISAC) : 2.7 参照

- 国家安全保障局 (National Security Agency : NSA) : 高度暗号/セキュアネットワーク管理/セキュア OS 等の研究開発および諜報活動
- 国立標準技術研究所 (National Institute of Standards and Technology : NIST) : 暗号標準策定/暗号応用、セキュリティ研究、製品評価・テスト・認証、情報セキュリティガイドライン策定、情報セキュリティ教育、人材育成
- 国家インフラストラクチャ保護センター (\*) (National Infrastructure Protection Center : NIPC) : 重要インフラをサイバー攻撃から護るための各種活動。脅威分析、警告発出、情報共有の推進。
- 国防総省高等研究計画局 (Defense Advanced Research Projects Agency : DARPA) : 国防総省配下の研究機関。国防に関連する情報セキュリティ/コンピュータ技術の研究開発を実施する。
- 情報インフラ保護研究所 (Institute for Information Infrastructure Protection : I3P) : 学術機関、産業界、政府と協調しながら、情報インフラ保護のための研究開発を行う
- 会計監査院 (General Accounting Office : GAO) : 連邦省庁のコンピュータシステムを対象とした情報セキュリティ監査の実施、監査結果レポートの発行、情報セキュリティ監査基準の策定
- 行政管理予算局 (Office of Management and Budget : OMB) : 各省庁の情報セキュリティに関する政策・基準・指針の開発・実施・監督および、情報セキュリティ監査結果の議会への報告

\* CIAO, FedCIRC, NIPC, NCS については、DHS 内の IA&IP 部門配下の NCSD への統合が進められている。

<各組織のスタッフ数> DHS 全体で 17万人。このうち、情報セキュリティに関連する組織については以下の通り。

IA&IP : 1000人 NCSD : 60人 CIAO : 65人 NCS : 91人 NISAC : 2人 NIPC : 20人 FedCIRC : 19人 NIST : 50人

<各組織の予算> DHS 全体で総額 362 億ドル (約4兆円) [http://www.dhs.gov/interweb/assetlibrary/FY\\_2004\\_BUDGET\\_IN\\_BRIEF.pdf](http://www.dhs.gov/interweb/assetlibrary/FY_2004_BUDGET_IN_BRIEF.pdf)

IA&IP (情報分析とインフラストラクチャ保護)部門全体で 8.3 億ドル(約1,000億円)。情報セキュリティ分野の内訳については、次頁参照。

これには、重要インフラ (核施設、通信ネットワーク、水道、輸送システム等)のアセスメント費用 5億ドル(約600億円)が含まれる。

NCSD に対しては、5,470万ドル(約 66 億円)を拠出。(OMB に対するヒアリングによる)

I3P : 予算は公表されていないが、PCAST(大統領科学技術諮問委員会)は最低 120億円が必要であるとしている。

NSF : IT 関連研究開発に 260 億円、そのうちサイバーセキュリティに 24億円。( [http://www.nsf.gov/bfa/bud/fy2004/pdf/fy2004\\_8.pdf](http://www.nsf.gov/bfa/bud/fy2004/pdf/fy2004_8.pdf))

別途サイバーセキュリティ R&D 法に基づく予算枠有り。(次頁参照)

DHS に統合される前の部門別の 2003年度予算

(出所 : <http://www.whitehouse.gov/deptofhomeland/book.pdf>)

CIAO : 32 億円 NCS : 186億円 NIPC : 181億円 FedCIRC : 23 億円

NIST : 2002年度 13億円、2003年度 18億円。

別途サイバーセキュリティ R&D 法に基づく予算枠有り。(次頁参照)

DARPA : コンピュータシステム/通信の研究に 500億円

このうち情報セキュリティ分野に 60億円

(出所) <http://www.darpa.mil/body/pdf/>

FY04\_FY05BiennialBudgetEstimatesFeb03.pdf

NSA の予算は公開されていない。

### <各組織の設立経緯>

1901 NIST 設立 1908 FBI 設立 1921 GAO 設立(1982 情報管理技術部設置)

1950 NSF 設立 1952 NSA 設立

1958 最新技術を軍事に应用することを目的として、DARPA 設立

(軍が実施する研究開発とは完全に独立している。)

1963 ケネディ大統領が、緊急事態発生時にも政府内のセキュアな通信を

確保することを目的として NCS を設立

1996 NIST, CIAC(エネルギー省のコンピュータセキュリティ関連組織)、

CERT/CC が共同で FedCIRC を設立

1998 PDD 63 に基づいて、CIAO, NIPC を設置 1999 最初の ISAC (金融) 設立

2001 1998年の PCAST の勧告とその後の検討を経て、政府出資の非政府系

サイバーセキュリティ研究所 I3P 設立

2002 DHS 設立 CIAO, FedCIRC, NIPC, NCS は、DHS 内の IA&IP

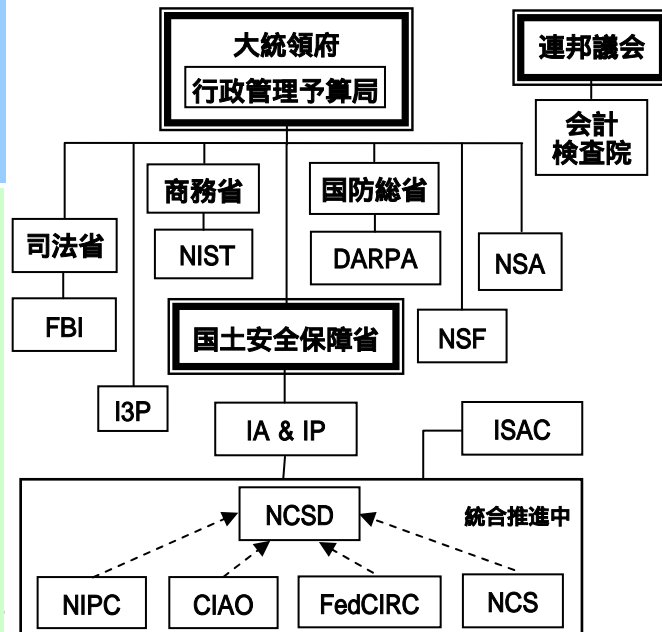
(Information Assurance & Infrastructure Protection) 部門配下となる。

2003 DHS の IA&IP 部門に、情報セキュリティを専門に扱う国家サイバー

セキュリティ部門(NCSD) が設置され、CIAO, FedCIRC, NIPC, NCS の

各機関の機能を同部門に統合すべく、作業が進められている。

図 1 米国の情報セキュリティ関連組織



## 3.2 米国の情報セキュリティ関連組織

## 予算の詳細

2004年度の国土安全保障省の IA&IP 部門の予算のうち、情報セキュリティに関連する項目を表1に示す。上院の予算案報告書では、「情報・警告発令システム」に割り当てられた予算 6,970万ドルのうち、3,280万ドルを物理的なインフラストラクチャと情報インフラストラクチャの統合的な監視・調整に、また、「リスク改善・保護対応プログラム」に割り当てられた予算 3億8,300万ドルのうち、6,570万ドルを情報セキュリティに充てるよう勧告している。

表1 2004年度 IA & IP 部門の予算

重要インフラストラクチャに対する脅威の発見と評価	3,200 万ドル (38.4 億円)
情報・警告発令システム	6,970 万ドル (83.6 億円)
インフラストラクチャの脆弱性・リスク評価	9,500 万ドル (114 億円)
リスクの改善・保護的対応プログラム	3億8,390 万ドル (460.7 億円)
国家通信システムの確保・改善	1億5,500 万ドル (186 億円)

出所)  
下院 予算審議書 Report 108-169 :

[http://thomas.loc.gov/cgi-bin/cpquery/R?cp108:FLD010:@1\(hr169\):](http://thomas.loc.gov/cgi-bin/cpquery/R?cp108:FLD010:@1(hr169):)

### サイバーセキュリティ R&D 法に基づく予算

出所) : <http://www.house.gov/science/hot/cyber/hr3394.pdf>

2002年に成立したサイバーセキュリティ R&D 法は、2003年度から2007年度にかけて、NSF (National Science Foundation) および NIST を通じて、サイバーセキュリティに関する研究開発や人材育成を強化することを定めており、総予算は、約8億7800万ドルと試算されている。

### NSF 向け

> コンピュータ & ネットワークセキュリティ研究費 (暗号技術、無線セキュリティ、サイバー犯罪捜査等 9分野のセキュリティ研究に対する助成金)

2003年度	2004年度	2005年度	2006年度	2007年度
3,500万ドル (42億円)	4,000万ドル (48億円)	4,600万ドル (55億円)	5,200万ドル (62億円)	6,000万ドル (72億円)

> コンピュータ & ネットワークセキュリティ研究センタ (研究者・専門育成のための研究センタの設立)

2003年度	2004年度	2005年度	2006年度	2007年度
1,200万ドル (14億円)	2,400万ドル (29億円)	3,600万ドル (43億円)	3,600万ドル (43億円)	3,600万ドル (43億円)

> コンピュータ & ネットワークセキュリティ教育 (学士及び修士プログラムのための大学への助成金)

2003年度	2004年度	2005年度	2006年度	2007年度
1,500万ドル (18億円)	2,000万ドル (24億円)	2,000万ドル (24億円)	2,000万ドル (24億円)	2,000万ドル (24億円)

### NIST 向け

> コンピュータシステムのセキュリティ研究プログラム (ポストドクおよび上級研究者に対する奨学金)

2003年度	2004年度	2005年度	2006年度	2007年度
2,500万ドル (30億円)	4,000万ドル (48億円)	5,500万ドル (66億円)	7,000万ドル (84億円)	8,500万ドル (102億円)

表2 主な省庁の IT 予算と情報セキュリティ予算 (2003年度)

	情報セキュリティ予算	IT予算	割合*
農務省	6,400万ドル (77億円)	21億3,000万ドル (2556億円)	3%
商務省	6,400万ドル (77億円)	13億6,000万ドル (1632億円)	4.7%
国防省	19億4,300万ドル (2332億円)	277億ドル (3兆3240億円)	7%
教育省	2,060万ドル (25億円)	4億1,000万ドル (492億円)	5%
エネルギー省	1億2,700万ドル (152億円)	25億ドル (300億円)	5%
保健福祉省	1億3,800万ドル (166億円)	47億5,000万ドル (5700億円)	3%
住宅都市開発省	560万ドル (6億7千万円)	3億5,400万ドル (425億円)	1.5%
内務省	3,400万ドル (41億円)	8億5,200万ドル (1022億円)	4%
司法省	2億2,300万ドル (267億円)	19億ドル (2280億円)	11.7%
労働省	7,800万ドル (94億円)	4億4,300万ドル (532億円)	17%
国務省	1億9,140万ドル (230億円)	8億5,200万ドル (1022億円)	22%
運輸省	1億400万ドル (125億円)	27億ドル (3240億円)	3.8%
財務省	8,050万ドル (96億円)	25億6,000万ドル (3072億円)	3%
退役軍人省	1億2,480万ドル (150億円)	14億2,000万ドル (1704億円)	8.8%
環境庁	800万ドル (9億6千万円)	4億3,200万ドル (518億円)	1.9%
緊急管理庁	880万ドル (10億6千万円)	5億8,200万ドル (698億円)	1.5%

### 主な省庁の IT 予算と情報セキュリティ予算

2003年度の連邦政府省庁の IT 予算と ITセキュリティ予算を表 2 に示す。

2003年度の連邦政府省庁の ITセキュリティ予算は、42億5000万ドルで、連邦政府の IT 全体予算の7%を占め、2002年度の27億ドルから約57%の増加となっている。

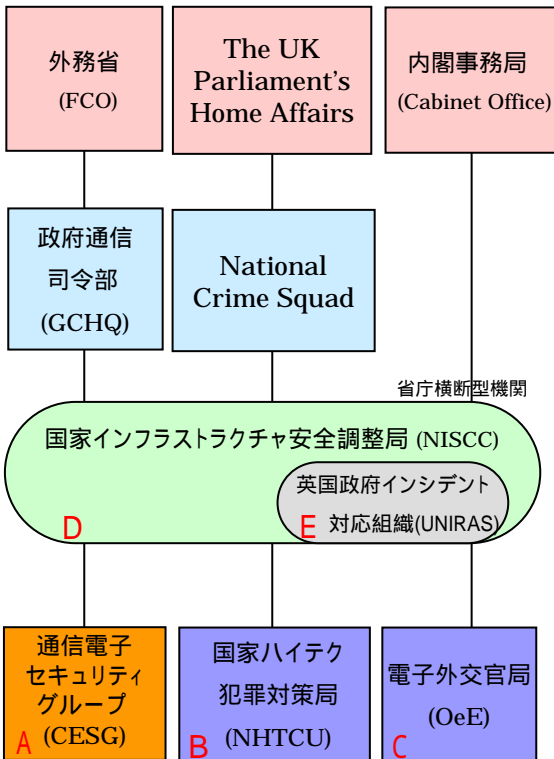
2004年度の ITセキュリティ予算は、47億ドルに上る予定で、連邦政府省庁の IT 予算全体の8%を占め、2003年度比で11%増加する見通しである。

1 ドル = 120 円で換算

\* IT 予算に対する 情報セキュリティ予算の割合

出所) : [http://www.whitehouse.gov/omb/info/foreg/2002gisra\\_report.pdf](http://www.whitehouse.gov/omb/info/foreg/2002gisra_report.pdf)

# 3.3 イギリスの情報セキュリティ関連組織



出所) GCHQおよび上記A~Eの機関のHPを基にNRI作成

## 上位組織 政府通信司令部 (GCHQ : Government Communications Headquarters)

- ・ 国家機密、軍事行動と法執行のフィールドにおいて、政府の決断を支援するために、情報を提供する部門。  
おもにテロリズムに関連する情報や重大犯罪防止のための情報を提供する。
- ・ 予算、人員数とも不明  
出所) GCHQのHP

## 中心組織 ▲ 通信電子セキュリティグループ (CESG : Communications Electronics Security Group)

### <設立背景>

GCHQ の一部門で、前身は第一次世界大戦前の暗号研究学校 (GC&CS : the Government Code and Cipher School) にさかのぼる。1997年より情報セキュリティサービスを本格的に開始。政府機関・組織に対して、通信やITシステムのセキュリティに関する支援・アドバイスをを行う。情報セキュリティに対する政府の取り組みおよびGCHQの機能は、Intelligence Services Act 1994、Security Service Acts 1989 および 1996 (改訂版) にて定義されている。職員数は約300人、Director は Richard Walton 氏。

※ 組織体制、予算は公表されていない

出所) CESGのHP

当局で、情報システムセキュリティにおける【人材育成】、【技術開発】、【技術評価・認証】、【暗号】の機能を担っている。具体的には以下のとおりである。

### <人材育成> Partnerships with Industry (PWI) Initiatives

- ・ 政府使用の暗号製品開発支援 (対民間) と、訓練コースの運営

### <技術開発> Tempest , Applied Security Technologies

- ・ 電磁波による攻撃を考慮した製品設計、保証要求
- ・ 国家重要インフラ保護や、情報セキュリティのための技術研究を実施

### <暗号> Cryptographic Services

- ・ 政府使用の暗号製品の開発

### <技術評価・認証> Infosec Assurance and Certification Services (IACS)

- ・ ITセキュリティ製品の認証と認定を実施

## その他関連機関のミッション、組織および予算

### B 国家ハイクテック犯罪対策局 (National Hi-Tech Crime Unit : NHTCU)

▶ ハイクテック犯罪に対抗する活動の支援および指導、重要度の高いインフラに対する脅威および攻撃に関する調査、諜報機関の設立、法執行機関に対する支援および協業、法執行機関、産業界、IT関連企業に対する情報提供。

▶ 予算は2001年~2004年までの3年間で2,500万ポンド(約50億円)の政府予算が計上されている。

内訳 : National Center of Excellenceの設立費 : 1,500万ポンド(約30億円)

ハイクテック犯罪対策を目的とした、イングランドおよびウェールズの警察組織の統合費 : 1,000万ポンド(約20億円)

▶ 組織の人数は40名だが、早急に50名に増員される予定(2003年5月現在) Head of NHTCU : Len Hynds

以下の4つの組織により構成される。

① TTS (Tactical and Technical Support : 戦術的技術的支援) : 国際的なハイクテック犯罪における英国側の窓口。

国内の警察組織を統合する形で CCU (Computer Crime Unit) を設立。

② Intelligence Unit (諜報機関) : ハイクテック犯罪に対する対策の立案、運用管理部門に対する支援

③ Operations Unit (捜査機関) : 警察組織と協力し、ハイクテック犯罪の捜査を行う

④ Digital Evidence Recovery (電子的証拠の復元) : ハイクテック犯罪の法廷闘争で、電子的証拠を復元する。

### C 英国電子外交官局 (Office of the e-Envoy : OeE)

行政サービスのオンライン化、政府間ゲートウェイの構築、情報セキュリティ、異なるシステム(省庁、地方自治体、民間企業間)での相互接続の実現。組織の人数は250人。予算は公表していない。

### D 国家インフラストラクチャ安全調整局 (National Infrastructure Security Co-ordination Center : NISCC)

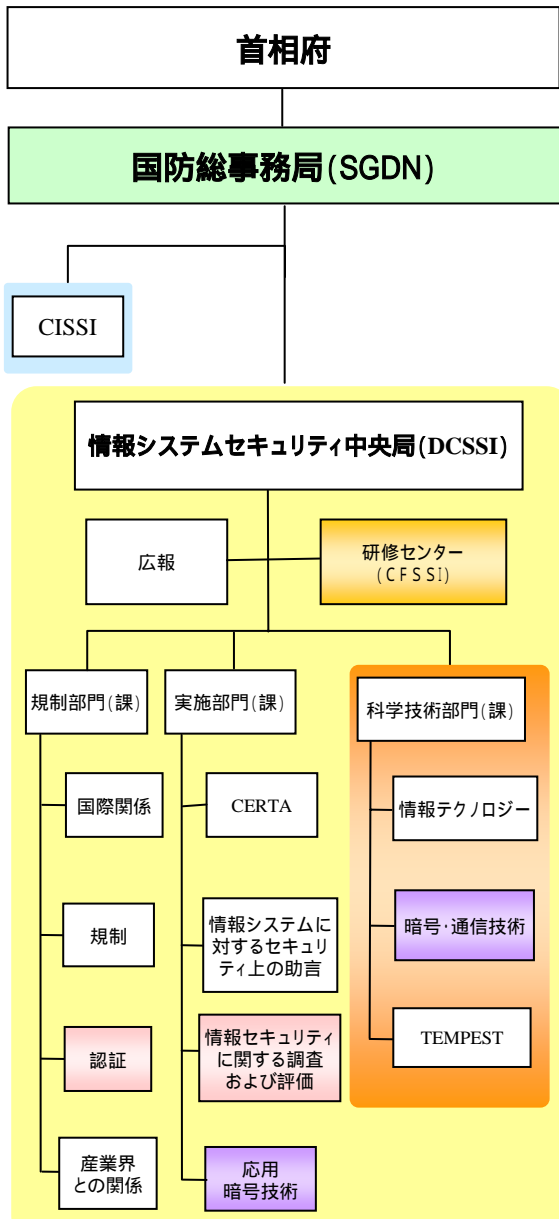
デジタルアタックに関する調査および評価。 人員数、予算は公表していない。

### E 英国政府インシデント対応組織 (Unified Incident Reporting and Alert Scheme : UNIRAS)

デジタルアタックおよびITセキュリティインシデント対応、脆弱性に関する警告、情報収集。

人員数、予算は公表していない。

# 3.4 フランスの情報セキュリティ関連組織



出所) [www.cnrs.fr/Infosecu/Catalogue\\_CFSSI2002.pdf](http://www.cnrs.fr/Infosecu/Catalogue_CFSSI2002.pdf) および、「欧州における暗号政策および暗号評価機関に関する調査報告 - 電子署名法における暗号政策の調査報告書 -」(平成13年3月 情報処理振興事業協会)

## その他関連機関のミッション

**情報システムセキュリティに関する省庁間委員会 (CISSI)**  
 2001年7月31日に発出された政令により、情報システムセキュリティに関する唯一の審議機関として設置され、各省庁の関連組織が CISSI のもとに再編された  
 ⇒目的:組織構造の簡素化&活動の活性化  
 出所) 'N° 68 SENAT SEDDION ORDINAIRE DE 2002-2003 Annexe au proces verbal de la séance du 21 novembre 2002 RAPPORT GENERAL」

## 上位組織 国防総事務局 Secretariat General de la Defense Nationale (SGDN)

- SGDN は情報セキュリティを含む広範囲の国防問題に関して首相に対してアドバイスや助言を行う。
- DCSSI を管轄するSGDNの職員数変遷および予算(ならびに2002年度予算申請額)は下表の通りである。組織運営に関わる費用は政府予算でまかなわれているが、情報セキュリティ製品の評価・認定に伴うコストは公表されていない。

SGDN 職員数変遷			SGDN 予算			
	2002	2003		2002	2003	
		予算法案	人員予測		予算法案	支出管理
省庁間調整機能 部門	158	158	158	11	21	11
政府通信機能 部門	3	3	3	3	6	6
DCSSI	86	91	87	8	8	8
防衛民間プログラム	18	18	18	6	8	7
情報に関する省庁間委員会	8	8	8	5	5	5
TOTAL	273	278	274	33	48	37

出所) 'N° 68 SENAT SEDDION ORDINAIRE DE 2002-2003 Annexe au proces verbal de la séance du 21 novembre 2002 RAPPORT GENERAL」

## 中心組織 情報システムセキュリティ中央局 Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI)

**<設立背景>**  
 DCSSIは1978年1月に発足した国防総事務局(SGDN) 付属の6機関のうちの1つである。DCSSIの前身であるSCSSI(Service Centrale de la Sécurité des Systèmes d'Information)は1986年に発足し、1996年にSGDNの付属機関となった。なお、DCSSIは現在もSCSSIと呼称されている。DCSSIは、SGDN 管轄下においてフランス政府の情報セキュリティ政策を支援している。情報セキュリティ管理を首相管轄のSGDNに委譲する法的根拠(SCSSIの設立根拠、権威付け)は政府官報「Journal Officiel de la République Française du 8 mars 1986 page 3592. Décret No 86-318 du 3 mars 1986. 「Central service of the Security of the Systems of information」にて確認することができる。また、法令「N° 901/DISSI/SCSSI le 2 mars 1994 Chapter 4, Article-17」において、情報セキュリティに関するSCSSIの機能が定義されている。また、1999年の暗号規制緩和 (décret n° 99-200)により、利用可能な暗号鍵の鍵長が40bit から128bit に変更され、暗号製品利用の自由度が他国と同等となるように図られている。当局で、フランス情報システムセキュリティにおける【人材育成】、【技術開発】、【技術評価・認証】、【暗号】の各機能を担っている。具体的には以下のとおりである。

### <人材育成> CFSSI (研修センター) 出所: <http://www.formation.ssi.gouv.fr/formation/catalogue2003.pdf>

要員育成の骨格:情報システムセキュリティの啓蒙活動、システム構築における情報セキュリティに関する評価・助言、国家資格交付、研修の実施

### <技術開発> (DCSSI 科学技術部門)

フランス政府の情報セキュリティ政策への貢献、情報セキュリティに関する調査・研究(専門研究所にてSSIに関する科学技術リサーチを行っている)

### <暗号> (DCSSI 科学技術部門)

暗号鍵の作成および公共団体および民間団体への配布、技術サポート

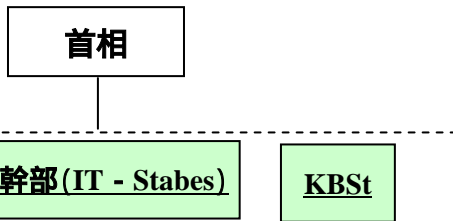
### <技術評価・認証> (DCSSI 実施部門)

ITSEC と CC(Common Criteria : 共通セキュリティ評価基準)に基づく、暗号製品の評価・

### <その他の情報セキュリティ実施機関> CERTA(情報部門委員会)

- 目的:システムの脆弱性の指摘・問題解決、将来の障害に対する準備
  - ミッション:① 行政機関および公共サービス機関を対象とする ② 技術的な監視 ③ 信頼性の高いネットワークの構築 ④ 世界的なネットワークを持つインシデント対応チームであるCERTと連携しながら、(必要であれば)問題解決をシミュレートする(擬似訓練を行う)。
- 出所) 'N° 68 SENAT SEDDION ORDINAIRE DE 2002-2003 Annexe au proces verbal de la séance du 21 novembre 2002 RAPPORT GENERAL」

# 3.5 ドイツの情報セキュリティ関連組織



## 上位組織 内務省 Federal Ministry of the Interior (BMI : Bundesministerium des Innern)

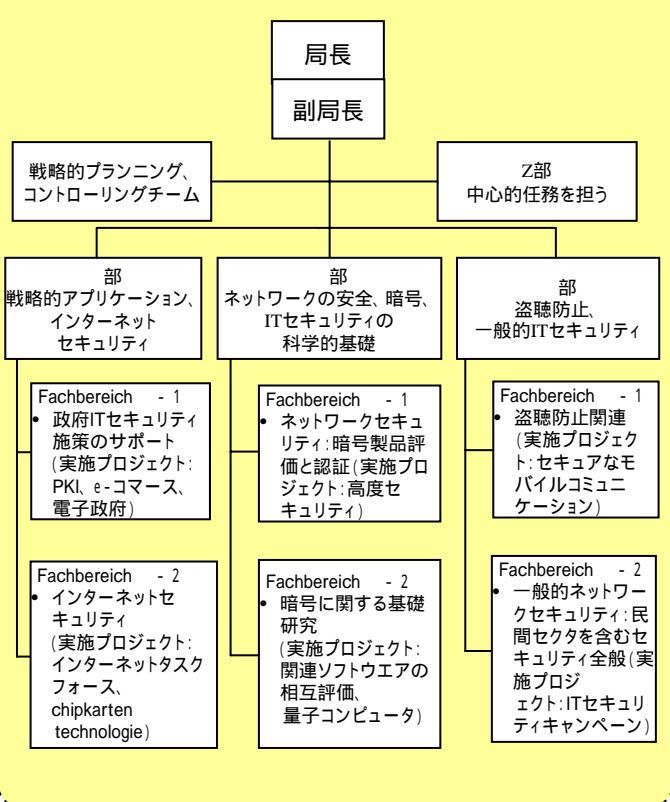
内務省内のセキュリティ室 (IT-stabes) 出所) ドイツ内務省ホームページ

- 内務省の一部門で、IT戦略、IT政策、ITセキュリティに関する業務を行っている。また、BSIの監督もこの部門が行っている。
- 当室の役割の重点は、ドイツ連邦議会および経済界に対する連邦内務省のIT関連所轄任務のコーディネイト(マネジメントや下部組織(主にBSI)への助言活動)を行うことにある。
- この他に、連邦中央政府のITインフラストラクチャ(IVBB, IVV, ポータル連合)構築、そして、情報技術における安全性確保や問題解決の役割を担っている。(i.e. 電子署名またはインターネットセキュリティ)

KBSSt 出所) ドイツ内務省ホームページ

- 各省庁が情報技術施策を実行する際の省庁間の調整および各省庁に対する助言を行う。
- KBSStはIT-stabesの管轄であるBSIと共同で毎年トレンド分析を発行する。
- トレンド分析の中で、特に成功したIT解決策をベストプラクティスレポートとして紹介する。
- 標準化を行う国内委員会および国際委員会において、連邦政府を代表する。

## 連邦情報技術安全局(BSI) 出所) BSIホームページ



## 中心組織 連邦情報技術安全局 BSI (Bundesamt für Sicherheit in der Informationstechnik)

<設立背景>

連邦情報技術安全局(BSI)は1991年に設立され、ドイツ政府のIT施策の中心機関として活動している。ITセキュリティ全般のサポートならびに、セキュリティ製品の評価と認証を実施する。  
1990年12月のBSI設立に関する法(Law about the erection of the federal office of security in the information technology :BGBl. I S. 2834 ff)の第3章、4章に、ドイツ連邦政府の情報セキュリティ施策に関する記述がある。

<ミッション> 出所) BSIホームページ

ITセキュリティに関する最新動向の分析結果等をもとに、ITに関する連邦政府の政策助言および、ITSECとCCに基づいた製品認証における国際協調の推進を担う。インシデント対応では、CERT-Bund (Computer Emergency Response Team für Bundesbehörden)を設置し、不正アクセスウイルスに関する情報の収集・分析を実施している。 出所) BSIホームページ

<事業実態> 出所) ドイツ内務省ホームページ

- 政府予算: EUR 45,215,000 (financial year 2003) で運営されている。
- <組織概要> 出所) ドイツ内務省ホームページ
- 職員数: 388.5 人 (financial year 2003) President : Dr. Udo Helmbrecht
- 【技術開発】、【暗号】、【技術評価・認証】に関する取り組みを行っている。

<技術開発> PKIの運用基盤構築。電子署名に関する研究開発。IDカードを利用したデジタルサービス

<暗号> 暗号システムの開発。暗号製品評価と認証

<技術評価・認証> 情報セキュリティ製品の評価と認証。セキュリティリスクの評価とセキュリティの検証。

## その他の機関の動き

### 【調達におけるセキュリティ対応について】

#### 内務省調達部の動き

- 内務省調達部(BeschA)のホームページには、暗号、特殊技術の調達をしているという記載があるが、詳細についての記載はない。

#### e-procurement flagship project の動き

- また、内務省(IT幹部)が中心となり「e-Procurement 2005」(2005年までに連邦のすべてのサービスをオンラインで提供すること(電子政府の実現)を目標にしているプロジェクト)を実施している。当プロジェクトの内の一つのプロジェクトとして、Ministry of Economics and Technology が中心となって実施している e-procurement flagship project がある。e-procurement flagship project は BSI と協力してセキュリティレベル向上に努めている。

出所) <http://www.wmrc.com/businessbriefing/pdf/ifpmm%202003/publication/goerdeler.pdf>

### 【人材育成について】

基本的に情報システムセキュリティに関する人材育成を担う組織は存在しないようであるが、BSIのホームページおよび関連するホームページに以下のような記述がある。

- BSIにおいて、企業向けの情報システムセキュリティマニュアルおよび人材育成マニュアルを作成している。 出所) BSIホームページ
- BSI が採用する人材は、大学、専門大学で数学、情報学、物理学を専攻した者である。 出所) BSIホームページ
- 教育省とBSIは相互協力している。教育省は情報学における研究開発の助成を、不正操作防止信頼性およびバグのないプログラムの作成(ソフトウェアの品質保証)に重点をおいている。
- 教育省の研究助成はREMO(安全なITシステムに対するレファレンスモデル)およびKORSO(正しいソフトウェア)に集中して行われている。 出所) マインツ大学の連邦助成プログラムの情報工学に関する記述

# 3.6 韓国の情報セキュリティ関連組織

## <情報セキュリティ関連組織の位置付けと機能>

- ▶ **国家情報院(National Intelligence Service)** : 諜報機関である KCIA を前身とする大統領直轄組織。情報セキュリティの計画・調整、政策樹立や、政府自治体を対象とした情報システムのセキュリティ対策支援、情報通信インフラの保護等をミッションとする。
- ▶ **情報通信部 (MIC : Ministry of Information and Communication)** : 情報通信全般を管轄する省レベルの組織。民間部門の情報保護業務に対する情報保護政策及び法制度の樹立・施行、情報セキュリティ産業の育成及び人材育成を担当。KISA および ETRI を管轄。
- ▶ **情報保護振興院 (KISA : Korea Information Security Agency)** : MIC 配下の組織で、情報セキュリティ全般を担当する。暗号技術開発、セキュリティ評価、情報セキュリティ技術開発、人材育成をミッションとする。暗号技術開発では、独自の暗号方式とデジタル署名アルゴリズムを開発済みである。情報セキュリティ技術開発では、侵入検知や動的セキュリティといった実用化に近い領域を担当する。基礎的な研究や技術開発は ETRI および NSRI が担当するという分担になっている。セキュリティ評価では、CC(Common Criteria) に基づいた製品/システムの評価のみを行い、製品/システムの認証は、国家情報院が実施している。人材育成では、企業、政府、公共機関等を対象とした情報セキュリティトレーニングコースを開催している。
- ▶ **電子通信研究院 (ETRI : Electronics and Telecommunications Research Institute)** : 暗号、セキュリティ通信、情報セキュリティインフラに関する研究を行う。国家保安技術研究院を管轄する。
- ▶ **国家保安技術研究院 (NSRI : National Security Research Institute)** : 情報インフラの安全を確保するための国家的対応・体制構築、国家的情報セキュリティ政策の研究、国家用暗号理論・体制の研究、暗号分析技術の研究を行う。
- ▶ **CERT/CC-KR** : コンピュータ事故対応チーム

出所)各機関のホームページ

## <KISA の設立経緯>

- 1996 MIC の出資により、Korea Information Security Center として設立
- 1998 FIRST(Forum of Incident Response and Security Team) のメンバとなる
- 1999 韓国 CA(Certification Authority) センタ開設
- 2000 個人情報保護センタ及び、アンチハッキング・ウイルス相談センタ開設
- 2001 Agency に格上げされ、名称を Korea Information Security Agency に変更

出所) KISA ホームページ

[http://www.kisa.or.kr/english/about\\_kisa\\_02.html](http://www.kisa.or.kr/english/about_kisa_02.html)

## <KISA のミッション>

- 情報セキュリティポリシー調査
- 暗号技術開発 : SEED(128 ビットブロック暗号) および KCDSA (Korean Certificate based Digital Signature Algorithm)
- 高度システム/ネットワークセキュリティ技術開発
- 情報セキュリティ技術の標準化
- IT セキュリティ製品評価
- 国家 PKI 管理
- CERT/CC-KR の運営
- ハッキング/ウイルスへの対応
- Anti-Hacking and Virus Consulting Center の運営
- 重要情報インフラに対するセキュリティコンサルティング
- 情報セキュリティ産業サポートセンタの運営
- 個人情報保護
- 人材開発

出所) KISA ホームページ [http://www.kisa.or.kr/english/team\\_project\\_01.html](http://www.kisa.or.kr/english/team_project_01.html)

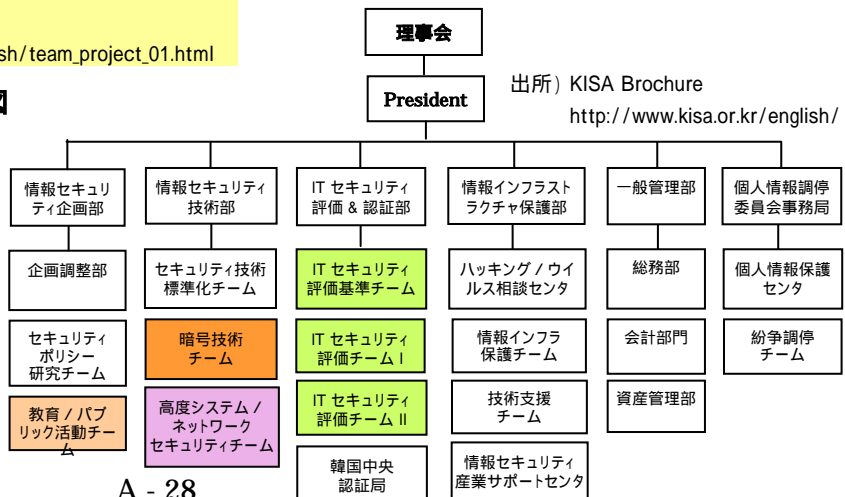
## <KISA のスタッフ数>

- 約 300名。部門別の最新の数値は不明。
- IPA の 1999年の調査によると、以下の通り (<http://www.ipa.go.jp/security/fy11/report/contents/crypto/crypto/report/AsiaSurvey/survey.html#2.4.4>)
- ✓ 一般 : 100人~299人
- ✓ 暗号研究グループ : 10人~29人
- ✓ その他情報セキュリティ研究グループ : 5人

## <KISA の予算>

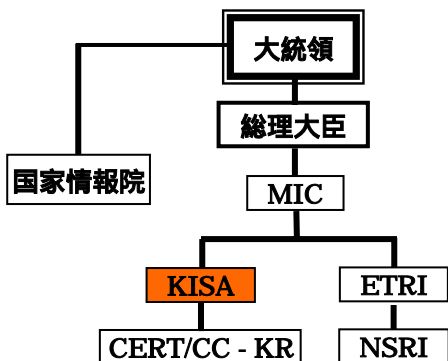
- 2001 年 440億 6,100万ウォン 約 45億円
- 2002 年 379億 2,900万ウォン 約 39億円
- 参考 : MIC の2003年度予算 約 8081億円

図 2 KISA 組織構成図



出所) KISA Brochure <http://www.kisa.or.kr/english/>

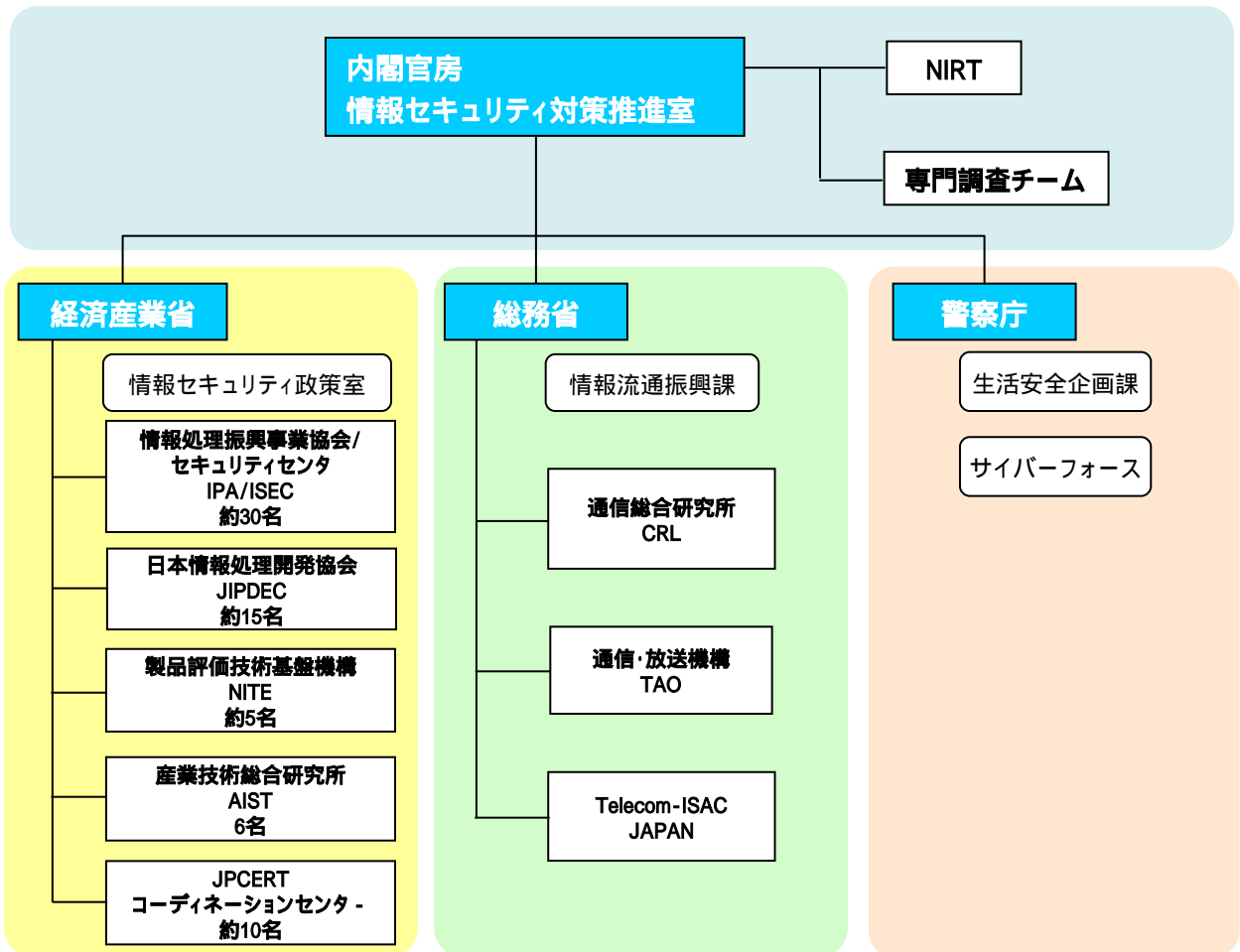
図 1 韓国の情報セキュリティ関連組織関係図



# 3.7 日本の情報セキュリティ関連組織

< 設立 / 活動経緯 >	< 組織の体制 >
1996 コンピュータ緊急対応センター (JPCERT/CC)が発足	< 内閣官房 > 情報セキュリティ対策推進室: 9名 NIRT(National Incident Response Team) : 17名(非常勤) 専門調査チーム: 11名(非常勤)
1997 情報処理振興事業協会(IPA)にセキュリティセンター(IPA/ISEC)設立	< 経済産業省 > 情報セキュリティ政策室: 8名
2000 CRYPTREC プロジェクト開始	< 総務省 > 情報流通振興課 通信規格課
2001 警察庁 サイバーフォース設立	< 警察庁 > 生活安全企画課 技術対策課 サイバーフォース
2002 NIRT 設立	
2002 Telecom-ISAC Japan 設立	
2003 JPCERT/CCの中間法人化	
2004 IPAの独立法人化(予定)	

図1 日本の情報セキュリティ関連組織



## 4 . 主権リスク関連資料

---

## 4.1 欧米と日本、韓国におけるIT製品の市場シェア

	サーバ OS	クライアント OS	ブラウザ	ルータ	
日本	<p>UNIX Linux Windows (78%) Others</p>	<p>Mac OS Windows (99.0%)</p>	データなし	<p>Juniper Redback Cisco (54%) Fujitsu Nortel Others</p>	
アメリカ	<p>Windows (64%)</p>	<p>OS/2 Windows (99.1%)</p>	データなし	<p>Nortel Cisco (95%) Enterasys</p>	
イギリス	<p>Windows (64%)</p>	ヨーロッパ全域でのシェア	データなし	<p>Juniper Nortel Cisco (85%) Redback Others</p>	
フランス	<p>Windows (63%)</p>		<p>Windows (99.9%)</p>	データなし	<p>Juniper Redback Cisco (82%) BinTec Others</p>
ドイツ	<p>Windows (60%)</p>		データなし	<p>Juniper Nortel Cisco (79%) BinTec Others</p>	
韓国	<p>Windows (67%)</p>		データなし	データなし	<p>Redback Others Cisco (55%) Juniper</p>
全世界	<p>Windows (69%) Others</p>	<p>Mac OS Windows (95.0%) Others</p>	<p>Netscape Others Internet Explorer (94.9%) Opera</p>	<p>Fujitsu Juniper Cisco (80%) Hitachi Furukawa Others</p>	

### 出所一覧

\* クライアント OS

世界：IDC 2002

日本、米国、ヨーロッパ：

Gartner Research Note, 2003

\* サーバ OS

ガートナー Dataquest 2003

\* ルータ

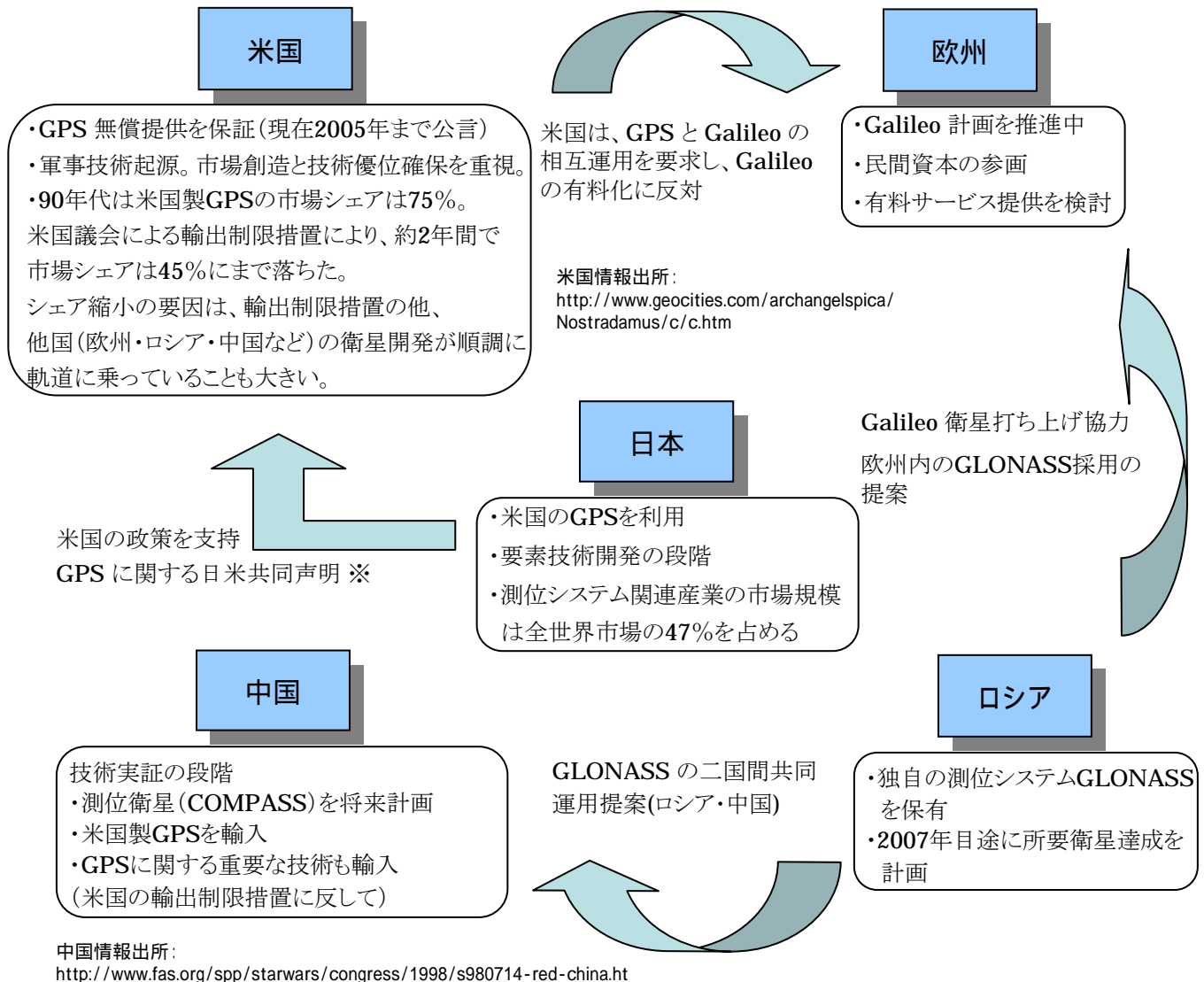
日本、米国、イギリス、フランス、ドイツ：

ガートナー Dataquest August 2003

韓国：ガートナー Dataquest March 2003

\* ブラウザ WebSideStory 2002

## 4.2 GPSに対する主要各国の政策・取り組み方針



### ※GPS 日米政府間協議 (日本経済新聞 1996年9月10日(火)朝刊)

「米国政府は、カーナビゲーションやミサイル誘導など民生・軍事両面の衛星による測位技術「全世界衛星測位システム」(GPS)を高度化するため、日本政府に二国間協定の締結を要請。日本が米国の新技術を国際標準にする共同開発に応じれば、米国は「実用化から二十年程度」をメドに日本企業に新技術の無料利用を保証する内容。この技術を普及させ、関連機器の輸出拡大を狙う米国の新たな対外経済政策で、日本も要請を受け入れる見通しだ。日本に協定締結を申し入れたのはホワイトハウスと国務、運輸、国防各省による米政府のプロジェクトチーム。日本の郵政、通産などの関係省庁に10～12月中に本格協議を始めたいとの意向を示した」

出所: 第3回宇宙開発利用専門調査会説明資料  
<http://www8.cao.go.jp/cstp/tyousakai/cosmo/haihu03/siryu3-2.pdf>

## 4.2 GPSに対する主要各国の政策・取り組み方針

### ●日本のGPS要素技術開発 — 国家レベル

米国連邦航空局(Federal Aviation Administration,FAA)の提案を受けた国連の世界民間航空機構(International Civil Aviation Organization,ICAO)の1995年3月の会議において、GNSSへの移行が国際的に合意されたことを受け、関連システムの開発が、次の2方面で全世界的に着手されている。

①広域システムとして衛星航法補強システム(Satellite Based Augmentation System, SBAS)

②局地システムとしては地上型補強システム(Ground Based Augmentation System, GBAS)

- 衛星航法補強システム(SBAS) DGPS(Differential GPS)の誤差補正情報を衛星を用いて放送するシステム。米国・欧州・日本が分担して開発。相互運用により全世界をカバーする予定。
- 地上型補強システム(GBAS)航空機の進入着陸誘導のために、衛星からの信号を地上局で補強するシステム

### ●日本のGPS要素技術開発 — 民間レベル ※

- 超高感度GPSアルゴリズムの開発 : マゼランシステムズジャパン株式会社
- GPSを用いた超高精度位置検出に関する研究 : (株)キャンパスクリエイト
- マルチGPSによる測位精度の向上に関する研究 : (株)キャンパスクリエイト

GPSを活用したサービスは行われているが、合衆国GPS政策により、GPSのコア部分に直接携わるような技術開発は行われていない模様

出所: <http://www.re-gis.com/ipa/ipa.html>

[http://www.crc.uec.ac.jp/japanese/h14\\_ken.html](http://www.crc.uec.ac.jp/japanese/h14_ken.html)

### 米国のGPS政策

1996年3月29日に公表された政策文書“U.S. Global Positioning System Policy”により、将来にわたる無償利用の保証、SA(Selective Availability: 選択利用性)廃止による民生用精度の向上、敵性利用対策の開発等の方針を明示。

- GPS民生市場でも米国技術・製品が世界をリード。
- 全世界的に直接利用者に無料でGPSサービス提供の継続を保証。
- 敵性利用の防止手段を開発した上で、10年以内に民生向けSAを廃止。
- 他国の類似システムに対し、GPSが国際標準となるよう主張し、他国と調整する。

出所: <http://www.drc-jpn.org/tamama-j.HTM>

	2000年	2001年	2002年	2003年	2004年	2005年	2006年	2007年	2008年	2009年
GPS	SA廃止		WAAS(*) 一部稼働		WAAS完成	第3周波数追加				
衛星数	29	29	33	38	38	38	38	38	38	38
GLONASS			M型衛星打ち上げ開始		24衛星完成					
衛星数	9	9	9+	9+	9+	24	24	24	24	24
GALILEO	システム設計	試験システム建設			実用システム建設開始			システム完成	正式運用開始	
衛星数	0	0						36	36	36
準天頂衛星				事業開始					実証衛星打ち上げ予定	
衛星数									1	3

\* WAAS: Wide Area Augmentation System

現行GPSシステムの欠点を補うための、静止衛星を利用した補強システム

## 4.2 GPSに対する主要各国の政策・取り組み方針

### 交通管理におけるGPS利用の今後の課題

欧州では、航空、鉄道、船舶、自動車等の分野における衛星測位システムの利用を視野に入れるとともに、ITの交通における応用という形で広範囲の議論を展開中。衛星測位システムの開発は高度情報化社会のツールの1つという位置づけなので、民間利用も含めた議論が展開できる。

- ・ 米国のGPSが誤作動した場合、これを利用する交通機関で事故が起きる可能性がある。GPSの利用が無料ということもあってか、その場合に米国に責任を問えないことになっている。法整備などが必要な領域である。
  - ・ 米国のGPSに関しては将来課金されることは有り得る。携帯電話にもGPSが装着されるようになってきており(※)、有料化された場合には、ITS機器の800万台とともにGPS付きの携帯電話等すべてに課金されることも想定される。
- ※ 米国では緊急通報のために、連邦通信委員会が携帯電話会社にGPSの装着を要請
- ・ 次世代衛星測位システムの応用については、日本の国土、都市、港湾等の事情を充分考慮した技術開発が必要である。我が国が次世代衛星測位システムに関して、自前の技術を持たない場合、応用面での技術開発の独自性がどれだけ確保できるか不明。

### 日本の衛星測位システム開発・利用状況

利用面では、衛星測位関連の日本の市場規模は世界の47%を占め、カーナビゲーションシステムの現在の稼働台数は約800万台。

- ・ 日本では米国のGPSを無料で利用している。日米間のGPS利用に関する枠組みとして「GPS利用に関する日米共同声明(1998年9月22日)」があり、下記の項目で合意がされている。
  - － 米国政府は、平和的・民民主的・商業的及び科学的利用を目的としたGPS標準測位サービスの利用には課金しない。
  - － 日本政府は、GPS標準測位サービスの利用を促進するために、米国と密接に活動する。
  - － 日米両国政府は、GPS技術・機器及びサービスの運用基準の互換性確保、十分な周波数帯域割り当てのための効果的な方法の開発を支援し、両国の関心事項の情報交換の促進および協力を実施する。
  - － 年1回全体会合を開催する(2001年2月5日に第1回日米GPS全体会合を開催)
- ・ 国内の技術開発面では、「我が国における衛星測位技術開発への取り組み方針について」(平成9年3月、宇宙開発委員会計画調整部会衛星測位技術分科会答申)において、以下を結論。
  - 1) 当面はGPSの利用を基盤とする。
  - 2) 最も基礎となる3技術(衛星搭載原子時計・時刻管理技術・高精度軌道決定技術)に重点を置く。
  - 3) 複数衛星による宇宙空間における実証を行う。

出所: 第3回宇宙開発利用専門調査会説明資料 <http://www8.cao.go.jp/cstp/tyousakai/cosmo/haihu03/siryu3-2.pdf>

### ヨーロッパにおける衛星測位システム計画 ~ GALILEO ~

- < 主要出資国 > イタリア、ドイツ、フランス、英国
- < 全参加国 > EU15カ国(ギリシャ、ルクセンブルクを除く)とノルウェー、スイスで構成されるESA(欧州宇宙機関)
- < 主要国出資比率 > 主要出資国4カ国が各々17.38% ずつ出資  
他に、スペインが9%+追加金1%=10%(600万ユーロ)を出資
- < 開発投資資金額 > 第一段階 ESA: 5億4700万ユーロ+追加金600万ユーロ EU: 5億5000万ユーロ  
総投資額 ESA: 32億~36億ユーロ  
(これで衛星30機によるネットワークをベースとするガリレオシステムを完成する予定)

## 4.3 各国における暗号政策の要点

## 各国比較

	輸出規制	暗号標準	鍵預託(第三者による解読の可否)
アメリカ	<p>1994年 鍵長40ビット以下の製品が認可無しで輸出可能となる。</p> <p>1996年 鍵長 56 ビット以下の製品が許可制で輸出可能となる。</p> <p>1997年5月 金融機関向け暗号製品の輸出規制を緩和。</p> <p>1998年9月 特定45カ国の金融/医療機関向けに限り、鍵長制限を撤廃。</p> <p>1999年9月 鍵長56ビット以下の製品の輸出規制を撤廃。鍵長64ビット以下の製品についてもテロ支援国を除いて輸出を自由化。</p> <p>2000年1月 鍵長制限の撤廃が特定45カ国以外にも認められ、全ての暗号製品は技術審査の後、テロ支援国以外の全ての国に対して輸出可能となる。</p>	<p>1977年 連邦政府の暗号調達標準 (FIPS 46)として、DESを認定。</p> <p>1997年 NIST、AES(次世代暗号標準)の策定開始を宣言、アルゴリズムを公募。</p> <p>1998年 AES 一次選考でアルゴリズム候補が15に絞られる。</p> <p>1999年 AES 二次選考で、5個のアルゴリズムが最終候補として残る。</p> <p>1999年11月 DESの強度低下に伴い、Triple DESをFIPS 46-3として認定</p> <p>2000年10月 AESにRijndaelが選ばれ、FIPS 197として認定される。</p>	<p>1993年4月 クリッパーチップによる鍵預託イニシアティブ (EEI)が大統領令として施行される。鍵の預託先として財務省とNISTを指定。</p> <p>1996年 暗号鍵の預託先として政府機関以外の第三者機関を選択可とする鍵リカバリ方式の運用開始。</p> <p>1998年9月 製品輸出時の暗号鍵リカバリ要件を特定45カ国に限り撤廃。</p> <p>2000年 製品輸出時の暗号鍵リカバリ要件を、テロ支援国家を除き完全撤廃。</p>
イギリス	<p>1998年 12月に改正されたワッセナーアレンジメント(WA)に従い、共通鍵暗号については鍵長56ビット以上、公開鍵暗号については鍵長512ビット以上の製品について輸出を規制。</p>	<p>- 欧州委員会の暗号技術評価プロジェクト NESSIEにおいて暗号方式を公募</p> <p>- 2000年9月 公募開始。10以上の国から42の暗号アルゴリズムが提出された。</p> <p>- 2001年9月 42の候補から24のアルゴリズムが選定された。</p> <p>- 2003年2月 最終的に下記の12のアルゴリズムに絞られた。共通鍵暗号はいずれもブロック暗号である。</p> <p>ストリーム暗号は6個が提出されたが、いずれも基準をパスしなかった。</p> <p>共通鍵暗号： MISTY1(日本)、Camellia(日本)、SHACAL-2(フランス)</p> <p>公開鍵暗号： ACE Encrypt(スイス)、PSEC-KEM(日本)</p> <p>MAC アルゴリズム/ハッシュ関数： Two-Track-MAC(ベルギー、ドイツ)、UMAC(米国)、Whirlpool(ブラジル)</p> <p>デジタル署名関数： ECDSA(米国)、RSA-PSS(米国)、SFLASH(フランス)</p>	<p>1997年 CA、第三者預託機関 (Trusted Third Party : TTP) 等の暗号サービス提供事業者に免許取得を義務付け。</p> <p>1999年 鍵預託をライセンスの条件に結びつける施策を撤廃。</p> <p>2000年 電子通信法制定</p> <p>強制的な鍵預託は廃止されたが、犯罪捜査のための暗号鍵の開示に関する規定は残された。</p> <p>1996年 政府承認組織への暗号鍵預託を義務付け。</p> <p>1998年 40ビット以下の暗号鍵については、第三者預託機関 (Trusted Third Party : TTP) に預託する必要がなくなった。</p> <p>1999年1月 暗号鍵の預託を強制しないとする法案提出。ただし、法執行機関の要求に応じて、暗号化文書の元の文書を提出する規定あり。</p> <p>1997年 鍵預託を随意で使用することを認める。</p> <p>1999年6月 「ドイツ暗号政策のコーナーポイント」において、政府の情報傍受能力が低下することがないように、法執行能力および安全保障機関における技術的能力の向上に務めるとの記述がなされる。</p>
フランス	<p>1996年 EU 域外への輸出について、原則として政府の許可を得ることを義務付け。</p> <p>1998年 12月に改正されたワッセナーアレンジメント(WA)に従い、共通鍵暗号については鍵長56ビット以上、公開鍵暗号については鍵長512ビット以上の製品について輸出を規制。</p> <p>1999年 これまでの規制を大幅に緩和する法案が提出されるが、WAに基づく暗号製品輸出規制は残される。</p>	<p>共通鍵暗号： MISTY1(日本)、Camellia(日本)、SHACAL-2(フランス)</p> <p>公開鍵暗号： ACE Encrypt(スイス)、PSEC-KEM(日本)</p> <p>MAC アルゴリズム/ハッシュ関数： Two-Track-MAC(ベルギー、ドイツ)、UMAC(米国)、Whirlpool(ブラジル)</p> <p>デジタル署名関数： ECDSA(米国)、RSA-PSS(米国)、SFLASH(フランス)</p>	<p>1997年 鍵預託を随意で使用することを認める。</p> <p>1999年6月 「ドイツ暗号政策のコーナーポイント」において、政府の情報傍受能力が低下することがないように、法執行能力および安全保障機関における技術的能力の向上に務めるとの記述がなされる。</p>
ドイツ	<p>1998年 12月に改正されたワッセナーアレンジメント(WA)に従い、共通鍵暗号については鍵長56ビット以上、公開鍵暗号については鍵長512ビット以上の製品について輸出を規制。</p> <p>1999年8月 経済省が、一般市場向けの暗号製品に対する輸出規制を必要最小限とすると発表。これにより、鍵長56ビット以上の製品について、輸出が自由化された。</p>	<p>1998年 国内標準として、128ビットブロック暗号 SEED およびデジタル署名方式 KCDSAを開発。</p> <p>2000年 KCDSAの楕円曲線版を開発。</p>	<p>1999年7月 電子取引基本法において、国家安全保障を目的として、政府が暗号化された情報の原文へアクセスできることを明示。</p>
韓国	<p>1998年 12月に改正されたワッセナーアレンジメント(WA)に従い、共通鍵暗号については鍵長56ビット以上、公開鍵暗号については鍵長512ビット以上の製品について輸出を規制。</p>	<p>1998年 国内標準として、128ビットブロック暗号 SEED およびデジタル署名方式 KCDSAを開発。</p> <p>2000年 KCDSAの楕円曲線版を開発。</p>	<p>1999年7月 電子取引基本法において、国家安全保障を目的として、政府が暗号化された情報の原文へアクセスできることを明示。</p>
日本	<p>1996年 5万円以上の暗号製品を輸出する場合には、政府の認可が必要。</p> <p>1998年 12月に改正されたワッセナーアレンジメント(WA)に従い、共通鍵暗号については鍵長56ビット以上、公開鍵暗号については鍵長512ビット以上の製品について輸出を規制。</p> <p>2000年 通産省、インターネットで使用する暗号ソフトウェアに対する規制を緩和する意向を発表。</p>	<p>2000年 電子政府向け暗号評価プロジェクトCRYPTRECを立ち上げ、国内外から広く暗号アルゴリズムを公募。</p> <p>2003年2月 電子政府推奨暗号リストを公開。公開鍵暗号、共通鍵暗号、ハッシュ関数、疑似乱数生成系について、計29のアルゴリズムが選定される。</p> <p>今後も継続的に評価作業が行われる予定。</p>	<p>現段階で、公式の場での決定事項はない。</p>

## 4.3 各国における暗号政策の要点 参考文献

1. 暗号技術に係る政策動向調査報告書 (2000年 2月 IPA)
2. 欧州における暗号政策および暗号評価機関に関する調査報告 (2001年 3月, IPA)
3. 外務省調査月報 国家による暗号政策 - 暗号の戦略性と輸出管理 - (2001年 No.1, 外務省)  
[http://www.mofa.go.jp/mofaj/annai/pr/pub/geppo/pdfs/01\\_1\\_2.pdf](http://www.mofa.go.jp/mofaj/annai/pr/pub/geppo/pdfs/01_1_2.pdf)
4. キーリカバリー構想を巡る最近の情勢について (1997年, 日本銀行)  
<http://www.imes.boj.or.jp/jdps/97-J-08.html>
5. Crypto Law Survey 2002  
<http://rechten.uvt.nl/koops/cryptolaw/index.htm>
6. The Cryptography Project  
<http://www.cosc.georgetown.edu/~denning/crypto/>
7. Advanced Encryption Standard (AES) Development Effort  
<http://csrc.nist.gov/CryptoToolkit/aes/index2.html>
8. New European Schemes for Signatures, Integrity, and Encryption (NESSIE)  
<https://www.cosic.esat.kuleuven.ac.be/nessie/index.html>
9. 暗号技術評価報告書(2002年度版) (CRYPTREC Report 2002)  
(2003年 3月, 情報処理振興事業協会, 通信・放送機構)  
[http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030401\\_report01.html](http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030401_report01.html)
10. Global Internet Liberty Campaign  
<http://www.gilc.org/crypto/>

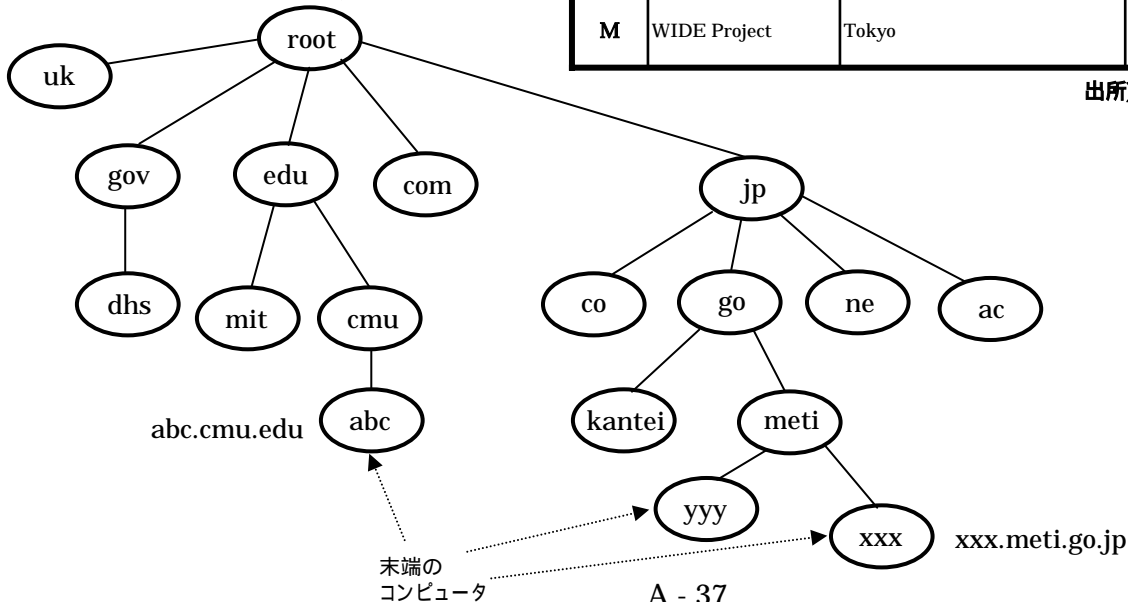
# 4.4 ルート DNS サーバの現状

## ルート DNS サーバ 一覧

Server	Operator	Locations	IPv4 Address [ IPv6 Address ]	Home ASN
A	VeriSign Global Registry Services	Dulles VA	198.41.0.4	19836
B	Information Sciences Institute	Marina Del Rey CA	128.9.0.107 [2001:478:65::53]	tba
C	Cogent Communications	Herndon VA; Los Angeles	192.33.4.12	2149
D	University of Maryland	College Park MD	128.8.10.90	27
E	NASA Ames Research Center	Mountain View CA	192.203.230.10	297
F	Internet Software Consortium	Ottawa; Palo Alto; San Jose CA; New York City; San Francisco; Madrid; Hong Kong; Los Angeles; Rome; Auckland; Sao Paulo; Seoul; Johannesburg	192.5.5.241 [2001:500::1035]	3557
G	U.S. DOD Network Information Center	Vienna VA	192.112.36.4	568
H	U.S. Army Research Lab	Aberdeen MD	128.63.2.53 [2001:500:1::803f:235]	13
I	Autonomica	Stockholm; Helsinki	192.36.148.17	8674
J	VeriSign Global Registry Services	Dulles VA; Mountain View CA; Sterling VA (2locations); Seattle WA; Amsterdam; Atlanta GA; Los Angeles CA	192.58.128.30	26415
K	Reseaux IP Europeens Network Coordination Centre	London; Amsterdam	193.0.14.129	25152
L	Internet Corporation for Assigned Names and Numbers	Los Angeles	198.32.64.12	20144
M	WIDE Project	Tokyo	202.12.27.33 [2001:dc3::35]	7500

出所) <http://root-servers.org/>

### DNS の階層構造



### DNS (Domain Name System)

✓ インターネットにおけるドメインネーム(meti.go.jp 等)とIPアドレスとの対応を維持管理する、**インターネットの基盤システム**

✓ 大元の管理サーバ(ルートDNSサーバ)から、末端の一台のコンピュータまでを**階層的に管理**

例: xxx.meti.go.jp というコンピュータであれば、"jp" 中の "go" の中の "meti" の中の "xxx" というコンピュータとして管理 (下図参照)

現在、ルートDNSサーバは、右表に示すように**米国に10台**、イギリスに1台、スウェーデンに1台、日本に1台の**計13台**あり、A-M の記号で区別されている。そして、それぞれにつき、ミラーサーバが別途置かれている場合がある。

ルート DNS サーバには、

- 物理アクセス制限
- 無停電電源装置及び自家発電装置による停電対策
- 多様なインターネット接続手段の確保

といったセキュリティ対策及び障害対策が施されている。

日本にあるルート DNS サーバは、WIDE プロジェクトにおいて管理が行われている。