# 国外の政府レベルのネットワークセキュリティ確立への取り組み

村瀬一郎　（株）三菱総合研究所
murase@mri.co.jp
鈴木裕信　ソフトウェアコンサルタント
hironobu@h2np.net

本稿においては，我が国の電子政府におけるネットワークセキュリティ確保を念頭に置きつつ，国外の政府レベルにおける取り組みの実態を，各国のネットワークセキュリティ対策機関の紹介を中心に述べる．米国においては，クリントン政権とブッシュ政権における取り組み，ヨーロッパやアジア諸国においては，国家全体を統括するネットワークセキュリティ対策機関の設置がなされていることを通して，ネットワークセキュリティ対策の内容および今後の展望について総括する．

## 米国におけるネットワークセキュリティ政策

### ■クリントン政権以前のネットワークセキュリティ対策

米国政府機関は，暗号関連政策以外のネットワークセキュリティ対策に関して，1980年代から取り組みを開始した．クリントン政権以前に活動を開始した機関について主なものを以下に挙げる．

主として，省庁別のCSIRTの設立がなされた．

－ CIAC（Computer Incident Advisory Capability）[1)]

CIACは，1989年にエネルギー省（DOE : Department of Energy）によって設立されたエネルギー省関係機関向けのCSIRT（Computer Security Incident Response Team）であり，ローレンスリバモア研究所傘下のCSTC（Computer Security Technology Center）が運営を担っている．CIACの業務内容は以下の通りであるが，広く政府機関向けに行っているサービスもある．

- インシデント緊急対応支援
- 普及啓発活動，トレーニングと教育
- 脅威，脆弱性等セキュリティ情報の収集と分析
- 技術動向の把握
- Advisories（勧告文書）の発行 等

－ AFCERT（Air Force Computer Emergency Response Team）[2)]

AFCERTは，1992年に設立された米国空軍内のCSIRTである．空軍内の機関向けに，緊急対応支援，侵入検知関連サービス，ネットワークセキュリティ関連情報提供を行い，さらには空軍の意思決定の支援の他に，他政府機関への情報提供も行っている．

－ GAO（General Acounting Office）[3)]

GAOは，1993年に4人のメンバにより，情報セキュリティにかかわる問題への取り組みを開始した．GAOは本来，会計システムの高度化の勧告業務を経て，システムのセキュリティも監査の対象に加えている．

2001年5月22日には，NIPC（後述）に関する監査レポートを発行し，人手不足によりタイムリな情報提供を行っていないことを指摘している[4)]．

### ■クリントン政権における政策

○クリントン政権前期における暗号政策

1993～1996年に至るクリントン政権前期においては，情報セキュリティ政策の中心は，暗号政策であった．1993年4月，クリントン政権は「クリッパーチップ・政府キーエスクロー提案」を発表したが産業界や市民団体の強い反対に遭遇し，計画は何度も変更を強いられた[5), 6)]．

○クリントン政権後期におけるネットワークセキュリティ政策

1997年～2000年のクリントン政権後期においては，情報セキュリティ政策は，その対象を大きく広げた．暗号政策に関しては，規制緩和の方針が徹底され，重要インフラ保護策の一環としてネットワークセキュリティ対策が本格化した．

1996年に，クリントン政権は，ネットワークセキュリティ以外のテロリズム対策も念頭に置き，PCCIP（President's Commission on Critical Infrastructure Protection，重要インフラに関する大統領委員会）と暫定機関であるIPTF（Infrastructure Protection Task Force. インフラ防衛対策委員会）を設置した[7]．PCCIPは，重要インフラに関する状況を以下のように整理した．

- 重要インフラ相互の依存性が高まっている
- 脆弱性が増している
- 広範囲にわたる脅威が存在する
- 国家的な戦略が欠如している

こうした分析の結果，PCCIPは以下の勧告を行った．

1）教育プログラムの開発
2）産業界の協力と情報共有の促進
3）法律の再検討
4）研究開発プログラムの推進
5）効果的な取り組みの推進

この勧告を基に，国家レベルでのネットワークセキュリティ確保のための組織が多く設立された．こうした動きを総括すると，ネットワークセキュリティ対策に関し，政府機関内の情報集約を図るだけではなく，官民を統合した国家的協力体制を構築することを主眼としていたといえる．以下で，PCCIP勧告に基づいて設立された主な機関について述べる．

－CIAO（Critical Infrastructure Assurance Office）[7]

PCCIP勧告を受けて，1998年にCIAOが設置された．

CIAOの主なミッションは以下の通りである．

- サイバーアタックに対する各省庁の政策を「国家情報システム保護計画」（National Infrastructure Assurance Plan）として整理する
- 重要インフラ保護に関連する政府機関と民間部門を調整する
- 全国的な教育教育プログラムや国民の意識を高めるためのプログラムを策定する

主な活動を以下に示す．

1）ISAC活動支援

ISAC（Information Sharing and Analysis Center）は，業界ごとの情報共有を目的とした民間組織である（2001年10月，金融，情報産業に関して設立が報告されている[8),9)]）．ISACを介して，政府と民間の間でのサイバー攻撃や，潜在的な脅威に関する情報の共有を中心とした関係を構築しようとしている．

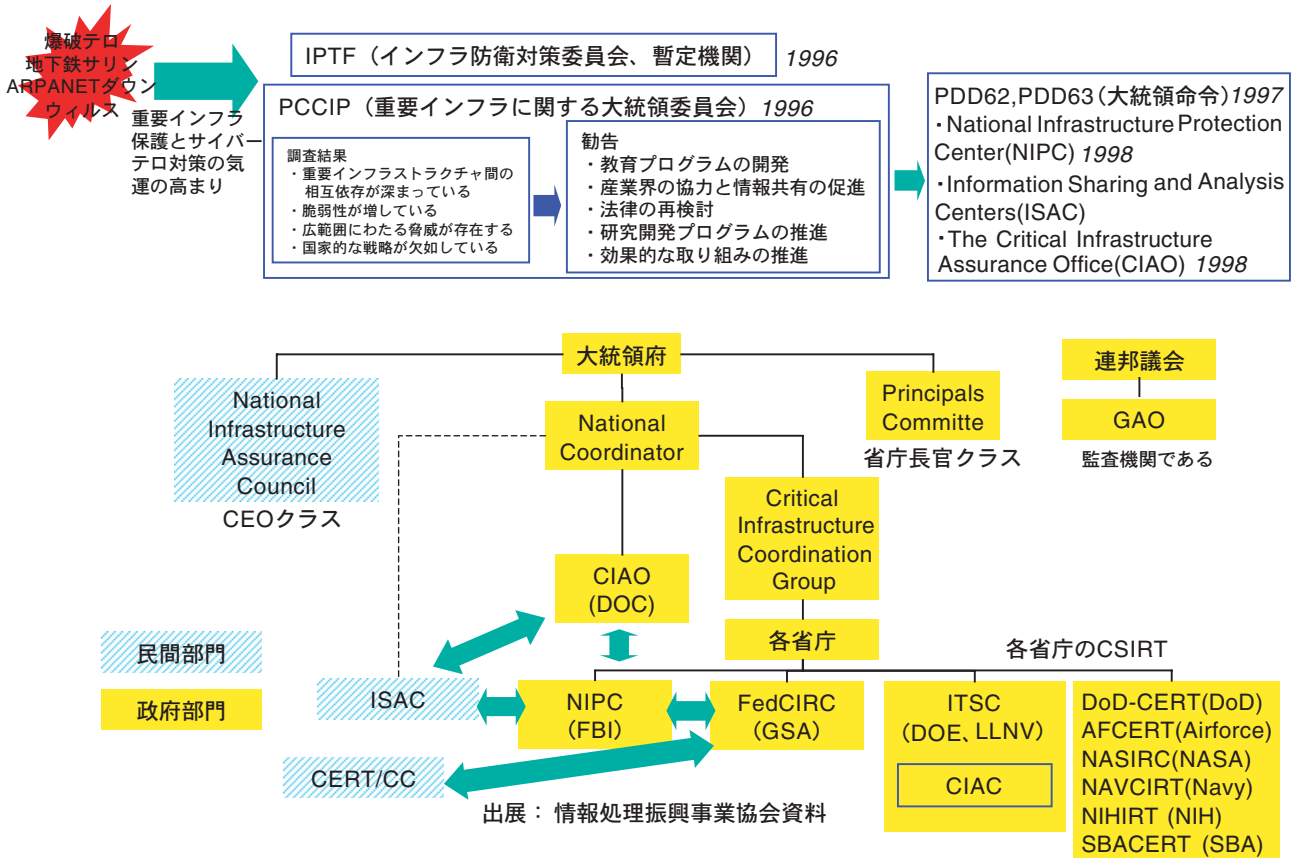


図-1　米国におけるネットワークセキュリティ対策の概要

2)「国家情報システム保護計画」の作成

国家情報システム保護計画の目的は以下の通りである.

- 連邦政府組織をネットワークセキュリティの規範として整備すること
- 国のインフラストラクチャ防衛のために官民のパートナーシップを育成すること

以上を総括するとCIAOは，官民にかかわらず米国全体のネットワークセキュリティ対策に関する調整機関である.

－FEDCIRC（Federal Computer Incident Response Center）[10]

FEDCIRCは，PDD63を受け1998年にGSA（General Services Administration）傘下に設置された．米国の軍以外の連邦政府機関全体に対してのCSIRTという位置づけであり，インシデント検出，防御．復旧支援に関する協力および情報集約のための拠点の役目を果たしている．インシデント・レスポンスは，CMU内に設置され数十名の技術専門家から構成される（CERT/CCとの密接な連携体制を整えていることが伺える).

具体的には，連邦政府機関に対して，以下の業務を行っている.

- 基本サービス（インシデントレスポンス インシデント処理・分析セキュリティ速報，アドバイザリ，分析ツールへのリンク等）
- 有料サービス（オンサイトコンサルティング，復旧支援，オンサイト監査分析，リスク分析，侵入テスト，非常事態対策，ネットワークセキュリティプロファイリング，トレーニング）

－NIPC（National Infrastructure Protection Center）[7]

NIPCは，PDD63を受けて，FBI（Federal Bureau of Investigation）下の一組織として，国家の重要インフラへの脅威や攻撃に関し，調査分析を行い対応策を関連機関に通知するための政府機関としてNIPCが設置された. NIPCは，2001年初頭に，暗号化メールを利用した侵入警戒ネットワークFIDNetを発表した．FIDNetは，連邦政府機関のネットワークが不正侵入・システム破壊などの攻撃にあった際にそれに関する詳細をNIPCに報告するためのメカニズムの提供を目的としていた．しかし，産業界や大学から反対の声が上がり，FIDNetは，2001年には話題に上らなくなっている.

## ■ブッシュ政権における政策

2001年にブッシュ政権が誕生し，ネットワークセキュリティ関連政策はいくつかの変更がなされている模様である.

同時多発テロ事件への対応も考慮し，ホワイトハウスは，2001年10月16日に新しい重要インフラ対策を発表した[11]．ここに，ブッシュ政権の関連政策概要が示されているため詳述する.

基本方針として，以下の2つが掲げられている.

(a) 重要インフラを保護するためには，非常時通信手段と，システムの物理的なバックアップを含む，セキュアなシステムの構築（GOVNetと呼ばれる構想であり，インターネットとは切り離したクローズドなネットワークを構築しようとするものである）が必要である.

(b) 重要インフラの混乱を最小限に留めることが最重要であり，そのためには官民の協力が必須である.

これらの基本方針のもとに，新機軸として，PCIPB（President's Critical Infrastructure Protection Board），NSTAC（National Telecommunication Advisory Council）とNIAC（National Infrastructure Advisory Council）の設立が宣言された.

○PCIPB

1）役割

PCIPBは，情報インフラを保護するための政策や省庁間の共同プログラムを検討する．そのための具体策として，以下が述べられている.

(a) 重要インフラを形成する民間部門や地方州政府を視野に入れたコンサルティング業務

(b) 政府機関の情報システム運用チームと各ISACとの間の情報共有，およびFEDCIRC，NIPC,他の関係機関の間での情報共有の推進

(c) 緊急時におけるNCS，NIPCおよび他の関係機関との調整

(d) OPM（Office of Personnel Management，人事管理局）との連携による，各省庁の担当者のリクルート，育成

(e) 関係各機関との連携による研究開発の推進

(f) NIPCおよびシークレットサービスとの連携を中心とした法執行機関との協調

(g) 世界的な協調の推進

(h) 関連法整備の推進

(i) OHS（Office of Homeland Security,本土安全保障局）との協調

OHSは，2001年9月11日の同時多発テロを受けて，PCIPBは新しく誕生した部局であり，そことの協調を掲げている.

2）組織

PCIPBのメンバは，軍関係以外の各省庁の局長クラスおよび大統領補佐官から構成される．議長は，サイバー空間セキュリティ担当大統領顧問が就任すると定められている．また，以下の委員会を設置することになっている.

- 民間部門および地方自治体
- 軍事部門を除く中央官庁の情報セキュリティ
- ナショナルセキュリティシステム
- 緊急時対応
- 研究開発
- ナショナルセキュリティと非常時通信システム
- 物理的セキュリティ

・相互連携インフラストラクチャ
・国際連携
・金融部門
・その他

○NSTACとNIAC

NSTACとNIACは，1982年に設立されたが，今回の大統領においてその役割が強化された．特に，産業界における重要インフラのセキュリティに関するアドバイスが重要とされる．メンバは，民間，大学および地方自治体から選抜することになっている．NIACの機能は，以下の通りである．

1）重要な情報システムを守るために官民の協力関係を構築し，大統領に対して関連する報告を行う
2）重要な情報システムや通信システムに対する定期的なリスク評価方法を開発して，民間に提案する
3）ISACの状況をモニタするとともに，ISAC，NIPCおよび他連邦政府機関の間の協力関係の方法について，PCIPBに提案する

■クリントン政権とブッシュ政権の比較

ブッシュ政権が誕生して，最も大きな変化は，GovNet構想とPCIPBの設置であろう．Govnetは，クローズドなネットワークであり，インターネットとは分離される予定である．しかし，現時点で以下の問題点があると筆者は考えている．

1）インターネットと分離されたネットワークを構築することにより，国民の多数が利用するインターネット上での情報公開との二重投資が必要となること
2）セキュアなネットワークの必要な業務が明確になっていないこと

今後，連邦政府・議会・産業界・一般市民を巻き込んだ議論が展開されるものと予測されるが，現時点ではGOVNETの実現性には，疑問符を付けざるをえない．

体制面では，PCIPBの設置が大きな動きであるが，クリントン政権との違いは明らかになっていない．特に，クリントン政権により設置されたCIAO，NIPC，FEDCIRCの扱いが焦点となろう．

## 欧州におけるネットワークセキュリティ対策

■英国

英国においては，GCHQ（Government Communications Headquarters，政府通信本部）管轄下に，1978年にCESG（Communications Electronics Security Group）が設置された．CESGは政府の情報セキュリティ全体に責任を負っている．主な業務は，以下の通りである[12]．

・政府の情報セキュリティポリシの策定
・政府および公的機関のオフィシャルユーザに対するアドバイス／コンサルティングの提供
・暗号製品開発
・産業界との連携
・トレーニングコースの運用
・政府向け暗号製品／システムの提供
・ITSEC（Information Technology Security Evaluation Criteria）の運営

また，政府系のCSIRTとしては，JANET-CERTが存在する．JANETは，英国の研究開発テストベッドであり，UKERNA（United Kingdom Education & Research Network Association）が運営主体である．JANET-CERTは，インシデント対応支援，ネットワークセキュリティの普及啓蒙に関する刊行物の発行，教育訓練コースの運用，各種イベントの開催等を行っている．

なお，2000年2月中旬には不正アクセス等の調査分析を行うための特別対策本部 Sicheres Internet が，BSI，内務省，経済技術省，司法省，犯罪調査局の協力により設置された．

■フランス

フランス政府は，1986年3月の政府命令により国家の情報セキュリティにかかわる以下の首相直轄組織を設置している[13]．

・国防事務局（SGDN：Secretariat General De la Deffense Nationale）

SGDNは国家安全保障の責任者として関連組織を統括することを目的として設立された．1996年以降はCISSI（次項）の運営支援業務も行っている．

・情報システムセキュリティに関する省庁間委員会（CISSI：Commission Interministerelle pour la Securite des Systemes d' Information）

情報セキュリティにかかわる行政と民間のニーズに対応することを目的に設置され，暗号，通信妨害，ネットワークセキュリティ一般等における検討を行っている．

・中央情報システム安全部（SCSSI：Service Central de la Securite des Systems d' Information）

SCSSIは，国防省の管轄下にある組織であり，国全体にかかわる情報セキュリティの強化の推進，公共団体および民間団体の職員を対象とする専門家トレーニング等を行っている．

■ドイツ

ドイツ連邦政府による情報セキュリティ対策は1986年から開始された．当初は，暗号管理が中心であったが，1991年に連邦政府の情報セキュリティ確保を任務とするBSI（Bundesamt fuer Sicherheit in der Informationstechnic，連邦安全情報局）が設立された．BSIは，セキュリティ評価認

証制度にかかわる業務およびBSI-CERTによる緊急対応支援業務を担っている．BSI-CERTは，1991年に設立され，連邦政府機関向けに，緊急問題解決支援・侵入テストおよび不正アクセス検知・パッチプログラムの調達と供給・関連調査分析評価等を行っている[14]．なお，2000年2月中旬には不正アクセス等の調査分析を行うための特別対策本部 Sicheres Internet が，BSI，内務省，経済技術省，司法省，犯罪調査局の協力により設置された．

## アジア・オセアニアにおけるネットワークセキュリティ対策

### ■韓国

韓国では，情報セキュリティ関連のあらゆる問題に対応する組織として情報通信省の傘下に，1996年4月韓国情報セキュリティセンタ（KISA：Korea Information Security Agency）が設立された．現在，KISAは，傘下に多くの組織を抱えている．主な組織と業務は，以下の通りである[15]．

1）CERTCC-KR

CERTCC-KRは，官民を問わず韓国国内の情報システムのネットワークすべてを対象としており，インシデントの予防および対応サービスを提供している．

2）CONCERT（CONsortium of CERTs）

国内のCSIRT間の調整組織である．

3）Computer Virus Incidents Response Coordination Center

コンピュータウイルス関連のインシデントの対応組織である．

4）Anti-Intrusion Consult & Assistant Center

不正アクセスおよびウィルス対策，インシデントの対策の相談窓口である．

### ■シンガポール

1999年12月に，通信情報技術庁（MCIT）管轄の政府機関としてIDA（Information Development Authority of Singapore）が設立された．IDAはシンガポール政府と国家の情報セキュリティの関連問題のすべての責任を権限を担う組織であり，主な業務の内容は以下のとおりである[16]．

- 政府セキュリティ方針の策定
- 国内標準およびガイドラインの作成
- 情報セキュリティ技術の研究開発および産業界との連携
- 緊急事態対応の方針と計画の作成
- 普及啓蒙活動
- 国内CSIRTであるSingCERTの運営支援 等

### ■オーストラリア

オーストラリアでは，1986年に国防総省管轄の政府機関としてDSD（The Defence Signals Directorate ）が設立された．DSDは，主として，連邦政府向けに以下の業務を行っている[17]．

- ITセキュリティ製品の選択および使用についてのアドバイス
- 適切なセキュリティ政策に関するコンサルテーションサービス
- リスクアセスメント調査の支援
- 情報セキュリティートレーニングおよび普及啓発活動
- ITセキュリティ（IT Security）に関係のあるプロジェクトについてのアドバイス
- 情報セキュリティプロダクト評価
- インシデント報告

## 今後の展望

海外における，国家全体の情報セキュリティ対策を推進する機関について報告した．我が国においても電子政府のセキュリティ確保のため，NIRT（National Incident Response Team）の設置が提案されている[18]が，NIRTの組織化に当たり，諸外国における情報セキュリティ対策の国家的体制を参考にし，官民連携と国際協調の枠組みを構築することが重要である．

**謝辞**　本稿は，情報処理振興事業協会の「電子政府情報セキュリティ技術開発事業」において，株式会社三菱総合研究所が受託した「電子政府情報セキュリティ技術支援に関する調査と技術開発」の成果に基づいている．関係各位に感謝する．特に，三菱総合研究所の牧野京子，石黒正揮，井上信吾の各氏には有用な情報を提供していただいた．深く感謝する．

**参考文献**

1) CIAC Webページ，http://www.ciac.org/ciac/
2) AFCERT Webページ，http://afcert.kelly.af.mil/index2.html
3) GAO Webページ，http://www.gao.gov/
4) Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities.,GAO-01-323,April 25.，http://www.gao.gov/new.items/d01323.pdf
5) 長谷川英一：米国における暗号政策と技術の現状（その1），電子工業月報/平成9年9月号／通巻419号，http://it.jeita.or.jp/jhistory/document/geppou/kaigai/ny97-9.html (1997).
6) 長谷川英一：米国における暗号政策と技術の現状（その2），電子工業月報/平成9年10月号／通巻420号，http://it.jeita.or.jp/jhistory/document/geppou/kaigai/ny97-10.html (1997).
7) 重要インフラにおけるセキュリティ対策の事例調査（および追補），情報処理振興事業協会，http://www.ipa.go.jp/security/fy11/report/contents/intrusion/infrasec_pts/infrasec_pj.pdf (1999).
8) FS/ISAC Webページ，http://www.fsisac.com/
9) High-Tech Industry Announces New InformationSharing and Analysis Center for Information Security，http://www.itaa.org/news/pr/PressRelease.cfm?ReleaseID=979672846 (2001).
10) FedCIRC Webページ，http://www.fedcirc.gov/
11) Executive Order on Critical Infrastructure Protection，http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html (2001).
12) CESG Webページ，http://www.cesg.gov.uk/
13) SCSSI Webページ，http://www.scssi.gouv.fr/
14) BSI Webページ，http://www.bsi.bund.de/aktuell/index.htm
15) KISA Webページ，http://www.kisa.or.kr/en-kisa/
16) IDA Webページ，http://www.ida.gov.sg/Website/IDAhome.nsf/Home?OpenForm
17) DSD Webページ，http://www.dsd.gov.au/
18) 高度情報通信ネットワーク社会推進戦略本部情報セキュリティ対策推進会議,電子政府の情報セキュリティ確保のためのアクションプラン，http://www.kantei.go.jp/jp/it/network/dai7/pdfs/7siryou13.pdf (2001).

（平成13年11月12日受付）