平成 20 年度内閣官房情報セキュリティセンター委託調査

各国の情報セキュリティ政策における情報連携モデルに関する調査

株式会社三菱総合研究所

平成 21 年 3 月

目次

本報告書に記載しているURLは、全て2009年5月19日現在、閲覧可能であったことを確認している。

0. 調査概要

0.1. 調査目的

我が国の政府機関及び重要インフラ各分野が所有する情報システムの安全性、信頼性及びそれらが実現するサービスの可用性を確保するべく、政策立案とオペレーションの各レベルにおいて望ましい情報連携の在り方の検討に資することを目的とし、調査対象国における政府機関及び重要インフラ事業者の情報連携に関する取組の動向について調査を実施した[1]。

0.2. 調査対象国

情報セキュリティ対策において先進的な取組を実施している米国、英国、ドイツ、オーストラリア、シンガポール、韓国の 6 カ国を調査対象国とした。

0.3. 調査の枠組

以下に本調査の枠組を示す。

1.（対象国）

1.1 情報連携のフレームワーク

1.1.1. 情報セキュリティ関連組織

対象国の情報セキュリティに関わる政府組織の体制と、各組織の持つ機能を示した。

1.1.2. 法執行機関、防衛機関、情報機関の位置づけ

対象国の情報セキュリティ体制における、法執行機関、防衛機関、情報機関の位置づけを示した。

1.1.3. 情報連携の分類

対象国の政府組織、及び重要インフラにおいて実施されている情報連携に資する取組を、政策レベル(システム構築、マネジメント等)とオペレーションレベルに分類した。（図 0-1 参照）

[1]本調査は各国の調査対象機関のウェブサイトやインターネット上で公開されている文書を中心に調査を行っている。国によって調査結果の内容や記載に濃淡がある点を注意されたい。

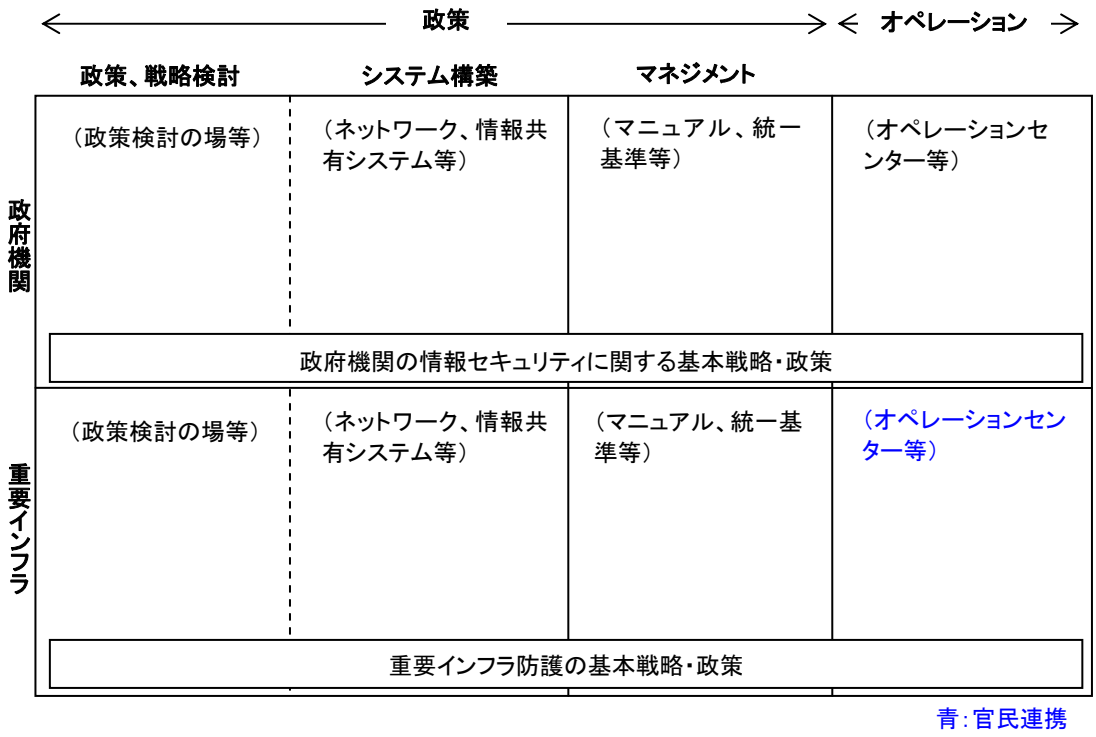


図 0-1 情報連携のフレームワークの分類（例）

1.1.4. 情報連携の関係図

情報連携を行う組織間の関係図及び組織間で共有される情報を、組織の位置づけと目的を軸としたマップ上に分類した。（図 0-2 参照）

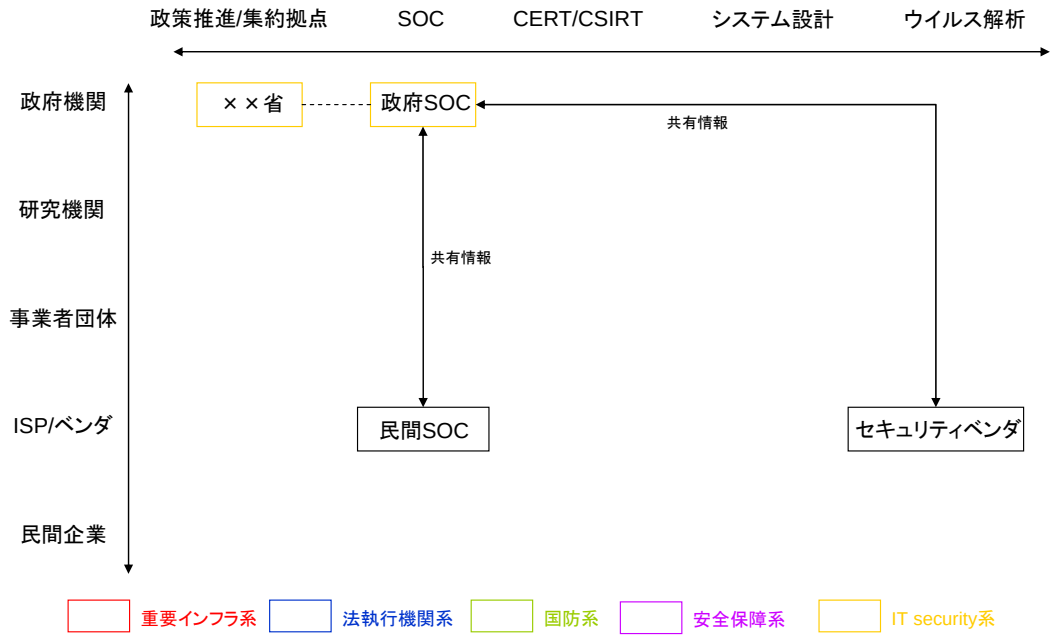


図 0-2 情報連携の関係図（例）

1.2. 政府機関における情報連携

1.2.1. 政策レベル

政府機関における情報連携に関する政策的取組を、政策検討・立案、共有ネットワーク等のシステム構築、規定類の整備等のマネジメント業務に分類し調査を実施した。

1.2.2. オペレーションレベル

対象国における政府機関の情報連携に関するオペレーション上の取組、特に政府機関の情報システムの監視及び情報収集・分析の実施状況や、インシデント対応の体制の整備等を中心に調査を実施した。

1.3. 重要インフラ防護における情報連携

1.3.1. 政策レベル

対象国における重要インフラの情報連携に関する政策的取組、特に政府機関と重要インフラ事業者が連携して重要インフラ防護の施策を検討する機会等を中心に調査を実施した。

1.3.2. オペレーションレベル

対象国における重要インフラの情報連携に関するオペレーション上の取組、特に重要インフラにおける脅威・脆弱性・インシデントに関する情報共有、インシデント発生時のインシデント対応体制等を中心に調査を実施した。

《第 I 部　調査のまとめ》

1. 調査のまとめ

1.1. 各国調査のまとめ

1.1.1. 米国

米国では 2001 年の同時多発テロ以降、米国愛国者法（2001 年）や国土安全保障法（2002 年）等に代表される国家安全保障を基礎としたサイバーセキュリティを目指す大きな流れに沿って、様々な施策が実現されてきた。行政管理予算局（OMB）[2]を主導とした FISMA[3]の策定、国土安全保障省（DHS）[4]を主導としたUS-CERT[5]の設立やISAC[6]等の民主導のオペレーション機能の確立、国家重要インフラ防護計画(NIPP)[7]の策定（2006 年）等、すべて今日の米国のサイバーセキュリティ体制の基礎を築くものである。OMB や DHS によるこのようなトップダウンの施策が着実に進められる一方で、サイバーセキュリティにおける省庁間及び官民との情報連携については取組の遅れが指摘されてきた。[8]こうした状況を受けて、2008 年には連邦政府のサイバーセキュリティに係る新たな政策の策定を目指したイニシアチブとして CNCI[9]が開始された。同イニシアチブでは米国のサイバーセキュリティの体制について、政策及びオペレーション両方の観点から省庁間・官民の連携を軸とした見直しが行われている。

1.1.1.1. 政府の情報セキュリティにおける情報連携

米国の政府機関の情報セキュリティ対策は、OMB 主導の下 2002 年の FISMA 策定を中心に、SP800 関連文書、FIPS の整備により強化されてきた。FISMA は各政府機関の自己監査による自主的な取組に基づくものであるが、2007 年以降は新たな流れとして、統一的なシステム構築による政府機関全体の情報セキュリティレベルの底上げを目指した取組が進められている。代表的な取組が、政府のネットワークの外部接続ポイントを統合し、マネージドサービスを展開する Trusted Internet Connections（TIC）[10]の構築である。TIC は政府機関のネットワークの情報を包括的に管理し、インシデント対応の機能を強化するとともに、連邦政府デスクトップ基準[11]等のサーバや PC 端末レベルにおけるセキュリティ対策の実装基盤となる。TIC の構築を機に、政府機関の情報セキュリティオペレーション体制も大きく変化している。これまでUS-CERTによって整備されてきた政

---

[2] 行政管理予算局（OMB：Office of Management and Budget）、21 ページ参照。

[3] 連邦情報セキュリティ管理法（FISMA：Federal Information Security Management Act of 2002）

[4] 国土安全保障省（DHS：Department of Homeland Security）、22 ページ参照。

[5] United States Computer Emergency Readiness Team、40 ページ参照。

[6] Information Sharing and Analysis Centers、53 ページ参照。

[7] 国家重要インフラ防護計画（NIPP：National Infrastructure Protection Plan）

[8] 2005 年の GAO の報告書“GAO-05-434, Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities”では DHS による省庁間及び官民の連携が進んでいないことを指摘している。(http://www.gao.gov/new.items/d05434.pdf)、2007 年に同じく GAO から出された報告書では、DHS が省庁間及び州政府間の情報連携を目的として整備した土安全保障情報ネットワークが機能していないことを指摘している。詳細については、32 ページ参照。

[9] Comprehensive National Cyber Security Initiative、26 ページ参照。

[10] 27 ページ参照。

[11] 連邦政府デスクトップ基準（FDCC： Federal Desktop Core Configuration）

府ネットワーク監視システム EINSTEIN[12]は TIC 上に再構築され、US-CERT では、政府ネットワークのあらゆる情報に関する巨大なDBを一括管理することとなる。US-CERT のオペレーション機能が拡大したため、従来 US-CERT が行ってきた組織間の調整機能を担う組織として、NCSC[13]、NCRCG[14]が新たに設置されている。NCSC は US-CERT や DoD の JTF-GNO[15]等の法執行機関や情報機関等に元々整備されていた 6 つのオペレーションセンター（OC）の調整役として、各 OC の情報を包括的に分析することで状況認識の同期をとり、DHS 長官への報告経路を 1 本化する役割を果たす。また、インシデントが発生した際には NCRCG が省庁間の調整を行い、US-CERT のインシデント対応業務を支援する。

1.1.1.2. 重要インフラ防護における情報連携

米国において重要インフラ防護は関係者間の連携が必要な分野として認識されており、省庁間、官民の情報連携を目的とした体制が構築されてきた。サイバー犯罪情報については FBI による InfraGuard、一般的な技術情報に関しては CERT/CC 等を通じた情報共有も行われている。中でも、民間主導の情報共有組織として分野別に整備された ISAC が重要インフラ防護における情報連携の中心となっている。しかし、ISAC の活動において競合する企業同士が機微情報を共有することに対する懸念は強く、ISAC の仕組みの中での情報連携の限界が指摘されている。[16]そのため、2006 年に策定された NIPP では、分野間の情報連携を目的とした新たな分野間連携モデルが示され、分野内の情報共有に対して法的枠組を与えることで ISAC が直面した問題を解決しようとしている。分野間連携モデル[17]ではベストプラクティス等の政策に資する情報共有を行うとされており、オペレーション上の技術情報の共有を行うISACとはその機能が切り分けられている。しかし ISAC が政策関係の情報共有活動に関わらないという切り分けに対しては、分野間の連携を担っていた ISAC Council の側から反対の声も出ており、既存の ISAC 及びその取りまとめ機関である ISAC-Council、そして分野間連携枠組における SCC[18]及びその取りまとめ組織である PCIS[19]の位置づけを明確にすることが求められている。

---

[12] 31 ページ参照。
[13] National Cyber Security Center、38 ページ参照。
[14] National Cyber Response Coordination Group、40 ページ参照。
[15] Joint Task Force for Global Network Operations：国防省のネットワークの運用・監視組織
[16] 62 ページの「GAO による ISAC の情報共有に対する指摘」を参照。
[17] 45 ページ参照。
[18] Sector Coordinating Councils、詳細については 45 ページ参照。
[19] 分野間連携モデルで Private Sector Cross-Sector Council として認定された組織、47 ページ参照。

1.1.2. 英国

英国における情報セキュリティに係る取組は、情報保証（IA：Information Assurance）の考え方に基づき、情報保証中央局（CSIA）[20]を中心とした情報セキュリティに関わる省庁(CESG[21]、BERR[22]、CPNI[23])によって戦略的方向性が示されている。英国における IA の考え方は、「情報システムによって取り扱われる情報が、必要な時に正当なユーザによって利用可能であること」であり、政府機関の情報セキュリティ及び重要インフラ防護における情報連携においても、この考え方をとした取組が展開されている。

1.1.2.1. 政府の情報セキュリティにおける情報連携

政府機関の情報セキュリティ対策の枠組は国家の IA に対する取組を包括的に纏めた文書である IA Governance Framework[24]の中で示されているが、これは米国の FISMA のように法的拘束力を持つものではなく、各政府組織における IA 確立のための自主的な体制の構築を求めるものである。システムの面では、1997 年から整備してきた政府のイントラネット GSi（Government Secure Intranet）[25]の機能が拡張され、米国の TIC と同様にネットワーク上でマネージドセキュリティサービスが提供されている。政府機関が GSi に接続する際に満たすべき条件として、CESG が策定した情報セキュリティ基準が指定されており、これらが実質的に政府機関の情報セキュリティ対策に係る文書として機能している。2007 年には、政府ネットワークに対する監視及び政府機関全体のインシデント対応を行う組織として GovCERTUK[26]が CESG の下に設置され、活動を行っている。

1.1.2.2. 重要インフラ防護における情報連携

英国では重要インフラ防護の取組も IA の考え方がベースとなっており、重要インフラ事業者が主体となった自主的な情報セキュリティレベルの向上が最も重要であると考えられている。英国の重要インフラ防護における最高責任者は内務大臣であるが、実際には複数の政府機関に跨る取組であるため、2007 年には調整機関として内務省下に国家インフラ保護局（CPNI）が設置された。CPNI は各政府機関の出向者で組織されており、各職員が親機関の情報集約や調整の役割を担っている。民間部門との情報共有に関しては CSIRTUK[27]が CPNI の下に設置されており、重要インフラに係る脅威・脆弱性・インシデント情報を収集・分析する機能を担っている。CSIRTUK 等で収集・分析されたこれらの情報は、WARPs[28]や Information Exchange(IE)[29]によって民間部門に提供さ

---

[20] 情報保証中央局（CSIA：Central Sponsor for Information Assurance）、64 ページ参照。
[21] 政府通信本部（GCHQ：Government Communications Headquarters）通信機器セキュリティグループ(CESG：Communications-Electronics Security Group)、64 ページ参照。
[22] 英国ビジネス企業規制改革省（BERR：Department for Business, Enterprise & Regulatory Reform）
[23] 国家インフラストラクチャ保護局(CPNI：Centre for the Protection of National Infrastructure)、64 ページ参照。
[24] 68 ページ参照。
[25] 68 ページ参照。
[26] 72 ページ参照。
[27] 76 ページ参照。
[28] 78 ページ参照。

れる。WARPs は中小企業等、自前で CSIRT[30]を持つことができない組織に対して、システムの脅威や脆弱性情報をウェブベースで配信する仕組みである。また、IE は特定の分野に設置されている情報共有の枠組であり、分野の代表者と CPNI 等の政府組織の担当者が参加する非公開のミーティングの中で直接情報交換を行うものである。IA に基づく情報セキュリティ対策を民間部門に確実に普及させるため、IE の取組は官（CPNI）主導で行われており、情報の共有方法やタイミングについても CPNI の管理下で行われている。

---

[29] 76 ページ参照。

[30] CSIRT：Computer Security Incident Response Team
CERT/CC では「コンピュータセキュリティインシデントに関するレポートを収集・分析し、実際にインシデントに対応する一連のサービスを提供する組織」と CSIRT を定義している。サービスは組織ごとに定義される対象者（企業、政府、教育機関、国及び地域、研究ネットワーク、顧客）に提供され、形態としてはインシデント対応専任の組織化されたチームとインシデント対応の必要が生じたときに召集されるアドホックなチームの 2 つのタイプがある。（http://www.cert.org/csirts/csirt_faq.html 参照）
インシデント対応組織の一般呼称として「CERT」が用いられることもあるが、本報告書では「US-CERT」等の固有名詞を除いて「CSIRT」を用いることとする。

1.1.3. ドイツ

ドイツにおける情報セキュリティへの取組の歴史は古く、1990 年には情報セキュリティを専門に扱う連邦情報セキュリティ庁（BSI）[31]が連邦内務省（BMI）[32]の下に設置されている。2001 年の同時多発テロ以降、米国の安全保障政策強化の動きに影響を受けて、大規模テロ等を想定した省庁間及び官民の連携を軸とした情報セキュリティ体制へと改編を行った国が多い中、[33]ドイツでは BSI を中心とした体制を現在まで維持している。BSI は研究者を中心とした組織であり、研究開発から IT の標準策定、重要インフラ防護に至る幅広い範囲の業務を取り扱う。一方で情報セキュリティは国防や、国家安全保障の要素も含むため、全体的な取りまとめ役として内務省が BSI の活動をコントロールしている。オペレーションについては官民の組織に設置された CSIRT がその機能を担っており、CSIRT 間の連携によって情報共有を行っている。

1.1.3.1. 政府の情報セキュリティにおける情報連携

政府機関の情報セキュリティについても BSI が主導で行われている。具体的な情報セキュリティ対策の基準は BSI が策定、改訂を行う IT-Grundschutz[34]の中で細かく規定されており、全ての連邦政府機関で運用されている。システム面では 2002 年から連邦政府の端末の Linux 及びオープンソースへの移行を推進しており、ベンダと製品調達に関する包括的な契約を結んでいる。

オペレーションに関しては BSI の下に設置された CERT-Bund[35]及びその下に設置された政府ネットワークの監視を担当する IT Situation and Analysis Center[36]とインシデント対応を担当する IT 危機対策センターが中心となって業務を行っている。

1.1.3.2. 重要インフラ防護における情報連携

重要インフラ防護の国家戦略検討は BMI の下の重要インフラ保護会議[37]で決められるが、具体的な計画の策定や政策の推進は、BSI が国家重要情報インフラ防護計画（NPSI）[38]に基づいて主導される。ドイツでは英国と同様、重要インフラ防護の基本は民間企業である重要インフラ事業者

---

[31] 連邦情報セキュリティ庁（BSI：Federal Office for Information Security）、83 ページ参照。
[32] 連邦内務省（BMI：Federal Ministry of the Interior）、82 ページ参照。
[33] 例えばオーストラリアでは、同時多発テロ以前は政府の情報セキュリティ対策は、各省庁が機密情報管理のため独自に行っている程度に過ぎなかった。しかし同時多発テロが発生し、オーストラリア全土に散らばる政府の情報システムや重要インフラの保護の必要性が叫ばれ、政府機関・民間企業の双方における情報セキュリティ問題に対する方針策定及び調整を行う政府横断的組織 E-Security 調整グループ（ESCG）が新たに設置された。他にも、政府機関へ情報セキュリティ関する情報を提供しているポータルサイト「OnSecure」(101 ページ参照)の整備や、米国の ISAC にならった重要インフラの情報共有ネットワーク TISN(109 ページ参照)の整備等、様々な情報セキュリティ政策が進められた。
[34] BSI が開発した ISO27000 シリーズにも準拠したリスクマネジメントツール。政府機関だけでなく、多くの民間企業で採用されている。詳細については 87 ページ参照。
[35] 89 ページ参照。
[36] 90 ページ参照。
[37] 通称 KRITIS、詳細については 93 ページ参照。
[38] National Plan for Information Infrastructure Protection：ドイツの重要インフラ防護における情報基盤保護のための包括的戦略を示した文書。詳細については 85 ページ参照。

による自主的な情報セキュリティ対策にあると考えられている。そのため、重要インフラを防護するために官民の情報共有の場を設けるというトップダウンの取組ではなく、各組織が情報セキュリティを強化した結果として、組織間の連携が進み、重要インフラの情報基盤の保護に繋がる、というボトムアップの取組に主眼が置かれている。

BSI の活動としても重要インフラ事業者に対する情報セキュリティ対策の情報提供が重要視されており、その代表例が政府機関でも使われている IT-Grundschutz である。BSI では IT-Grundschutz を企業にも普及させるため専用のソフトウエアや認証制度も整備しており、ドイツに限らず欧州において企業の情報セキュリティ対策、リスクマネジメントツールとして広く活用されている。

オペレーション組織としては官民ともに組織内 CSIRT の設置が推奨されており、各 CSIRT が必要な情報の収集・分析を自主的に行っている。組織内に CSIRT 組織を持つことが難しい中小企業に対しては、脅威や脆弱性情報の提供等の CSIRT のサービスを無償で提供する Mcert[39]等の活動も行われている。そうした CSIRT 組織の情報収集のための場である CERT-Network（CERT-Bund が運営）がドイツにおける実質的な情報連携の場として機能する。

[39] 経済技術省、内務省、IT 関連の業界団体である BITKOM によって設立された中小企業のための CERT。組織内に自前で CSIRT を構築できない組織に対して、脅威や脆弱性、インシデント等の早期警戒情報を提供する。詳細については 91 ページの Mcert の項目を参照。

1.1.4. オーストラリア

オーストラリアはテロや災害を含むあらゆる緊急事態等を想定した全てのリスクに対応する体制（all hazard approach）をとっているため、情報セキュリティに関する取組も、その目的によって司法省（AGD）[40]、予算・行政省、国防省や警察組織等の組織の中で実施されている。そのためそれら組織間で政府の方針を取りまとめる組織として連邦省庁の代表者からなる E-Security 調整グループ（ESCG）が設置されており、政府機関及び民間企業に対する情報セキュリティ政策の基本計画の策定を行っている。

1.1.4.1. 政府の情報セキュリティにおける情報連携

2003 年に公表された“National Counter-Terrorism Plan”[41]では、司法及び行政組織の責任・権限を整理した上で、政府機関が満たすべき基本的な情報セキュリティ基準が示されている。政府機関のセキュリティ対策全般については AGD が定めた Protective Security Manual (PSM)[42] 、政府機関の情報通信システムのセキュリティ対策については国防信号局（DSD）[43]が定めた ISM[44]の中で定められており、政府機関はこれらに準拠する必要がある。また、DSD は情報セキュリティの技術の専門家を多く擁しているため、各省庁に対して暗号やネットワークセキュリティ、情報セキュリティに関するガイドラインやポリシー策定のための人員を派遣している。政府機関のオペレーションについては、DSD の中に設置された INFOSEC[45]が担っており、政府機関の情報セキュリティ対策の技術的サポートや、インシデント情報の収集・分析・配信を行っている。

1.1.4.2. 重要インフラ防護における情報連携

オーストラリアでは重要インフラ防護に対して司法長官に助言を行う司法省(AGD)の元に、官民連携組織 TISN が整備されており、米国の ISAC と同様に分野ごとの情報共有を行っている。2004 年には TISN[46]から重要インフラ防護の国家戦略を示した“Critical Infrastructure Protection National Strategy”[47]が公表され、各ステークホルダ（政府機関、重要インフラ事業者等）に対してこれらに基づいた詳細な計画の策定を求めている。

民間部門に対するインターネット上の脅威、脆弱性情報、分析結果、アラート等の提供は AusCERT[48]によって行われている。ただし、AusCERT はオーストラリア政府から資金援助は受けているが、正式な National CSIRT とは認められていないため[49]、オーストラリアの重要インフラにお

---

[40] 司法省（AGD：Attorney-General’s Department）、97 ページ参照。
[41] 100 ページ参照。
[42] 102 ページ参照。
[43] 国防信号局（DSD：Defense Signal Directorate）、98 ページ参照。
[44] Australian Government Information and Communications Technology Security Manual、102 ページ参照。
[45] Information Security Group、103 ページ参照。
[46] Trusted Information Sharing Network for Critical Infrastructure Protection (TISN)、109 ページ参照。
[47] 104 ページ参照。
[48] 111 ページ参照。
[49] AusCERT は 15 年以上前に設立されており、国際社会においては広くオーストラリアの CERT として認められて

けるサイバー攻撃や脅威に対するオペレーションに関与することはできない。[50]そのような場合は、DSD が情報機関 ASIO[51]とオーストラリア連邦警察（AFP）[52]と正式な Joint Operating Arrangements（JOAs） を結んでおり、それらの協力体制の中で情報収集及びインシデント対応を行う。

いる。しかし、オーストラリア政府の情報セキュリティ政策の枠組みである E-Security では、National CSIRT は GovCERT.au とされており、両組織の機能に重複が指摘されている。詳細については 112 ページ参照。

[50] 2008 年 6 月に AusCERT が公表した“Review of Australian Government's e-Security Arrangements AusCERT Submission”では、国家の重要インフラ及びオーストラリアの情報経済に影響を与えるサイバー攻撃や脅威への対応に、AusCERT のノウハウを活用できていない状況は疑問であると指摘している。

[51] Australian Security Intelligence Organization (ASIO)、98 ページ参照。

[52] オーストラリア連邦警察（AFP：Australian Federal Police）

1.1.5. シンガポール

シンガポールでは情報セキュリティを含むITに係る政策・戦略の立案、策定は情報通信開発庁（IDA）[53]を中心とした複数の省庁の代表者によって構成される首相直轄の国家情報通信セキュリティ委員会（NISC）[54]の調整の下で実施される。施策の具体化及び規制の整備等は全てIDAで実施される。政府機関の情報セキュリティ対策や重要インフラ防護も含め、シンガポール国家のサイバーセキュリティに対する取組の多くは、“InfoComm Security Masterplan”[55]の中で示されている。

シンガポールは事実上、人民行動党(People's Action Party)の一党独裁体制であり、また小国であるが故に、トップダウンによる政策決定やシステム構築が迅速に政府全体に浸透する点が特徴となっている。一方で、政策の実装や情報の伝達において他国のような調整を要しないため、情報連携体制は他国に比べて整備が遅れている。

1.1.5.1. 政府の情報セキュリティにおける情報連携

政府機関の情報セキュリティ対策の基本政策は“InfoComm Security Masterplan”の中で示されており、2005 年版では、政府機関の情報セキュリティ状況のスコア付制度 InfoComm Security Health Scorecard 等の施策が示されている。政策面だけでなく、統一的なIT基盤も整備されており、シンガポール政府ネットワークであるSGNet[56]では電子行政サービス、職員のICカード認証システム等も運用されている。オペレーションについては国家サイバー脅威監視センター（NCMC）[57]が整備されており、サイバー脅威の監視、分析、インシデント対応を行っている。[58]ただし、サイバー攻撃や犯罪に関してはIDA内のGITSIR[59]や警察のTCD（SPF）[60]の協力を得て対応を行う。またNCMC では、その運営に民間ベンダを活用しており、リアルタイムの監視を行うグループ(CWC)[61]では、民間のセキュリティベンダ e-cop 社に運営を委託している。

1.1.5.2. 重要インフラ防護における情報連携

シンガポールでは、重要インフラ防護に特化した政策・戦略文書は策定されていないが、大枠の取組方針については“InfoComm Security Masterplan”の中で示されており、IDA及びNISCが中心的な役割を果たす。

2008 年に改訂されたマスタープランでは限定的な活動ではあるが、情報通信システムのセキュリティアセスメントのために、重要インフラ事業者のシステム担当者が検討を行うプログラム、

---

[53] 情報通信開発庁（IDA：InfoComm Development Authority of Singapore）、114 ページ参照。
[54] 国家情報通信セキュリティ委員会（NISC：National InfoComm Security Committee）、115 ページ参照。
[55] 118 ページ参照。
[56] 118 ページ参照。
[57] 国家サイバー脅威監視センター（NCMC：National Cyberthreat Monitoring Centre）、118 ページ参照。
[58] 118 ページ参照。
[59] Government IT Security Incident Response Team、119 ページ参照。
[60] 115 ページ参照。
[61] Cyber Watch Center、118 ページ参照。

CII-SA（Critical InfoComm Infrastructure Surety Assessment）[62]が開始されている。

[62] 121 ページ参照。

1.1.6. 韓国

韓国における情報セキュリティ戦略は外的な脅威から、政府機関及び主要な公共機関（地方自治体及び学校や医療機関等）の情報通信ネットワークを防護することを基本的な目的としている。具体的な取組方針については 2004 年に公表された国家情報セキュリティ基本方針に示されている。

2008 年の李明博政権の大規模な組織改編によって情報セキュリティに係る組織の構造も大きく変化しており、これまで韓国の情報通信に係る政策を統括していた情報通信部（MIC）が廃止され、それらの機能が複数の組織に分散されている。

1.1.6.1. 政府の情報セキュリティにおける情報連携

政府機関におけるセキュリティは 2005 年に公表された国家情報セキュリティ基本方針の中に基づき、国家情報院（NIS）[63]主導で行われる。システムの面では、公共機関を接続する光ファイバー網 KII-G[64]や、政府機関の情報システムのほぼ全てのデータを管理する共同バックアップセンターを国内 2 箇所に所有しており、政府機関間の情報資源の統合を進めている。2004 年には NIS の一部門として国家レベルでの情報セキュリティ政策の統括、調整、セキュリティ対策促進活動、サイバーセキュリティ上の脅威に関する情報収集、事案対処を行う国家サイバーセキュリティセンター（NCSC）[65]が設置された。政府機関の ISAC である GISAC[66]も脆弱性情報、インシデントの発生情報等を NCSC に提供しその活動を支援している。

1.1.6.2. 重要インフラ防護における情報連携

韓国における重要インフラの情報システムの保護は、2001 年に制定された情報通信基盤保護法によって示されている。また 2001 年には同法を根拠に、首相を委員長とする CPII[67]を設置し、2001 年に制定された情報通信基盤保護法[68]に基づいて重要インフラの情報システム保護における政府横断的な検討を行っている。

国家の重要インフラに大きな影響を与える事故については NCSC で対応がとられるが、国内の情報通信ネットワーク全体の情報収集及び監視、インシデント対応は National CSIRT である KISC（KrCERT）[69]において行われる。また通信や金融等の一部の分野においては米国と同様に ISAC が組織されており、脆弱性、インシデント情報等をデータベース化した形でメンバ間の情報共有を行っている。

---

[63] 国家情報院（NIS：National Intelligence Service）、123 ページ参照。
[64] 韓国政府情報基盤、126 ページ参照
[65] National Cyber Security Center (NCSC)、130 ページ参照。
[66] 132 ページ参照。
[67] Committee on the Protection of Information Infrastructure、134 ページ参照。
[68] 135 ページ参照。
[69] 136 ページ参照。

1.2. 各国の情報連携体制の比較

1.1 で示した各国の情報連携体制の特徴を一覧表として纏めた。

	政府の情報セキュリティ			重要インフラ防護		
国名	主組織	政策レベル	オペレーションレベル	主組織	政策レベル	オペレーションレベル
米国	OMB	予算管理組織である OMB が FISMA に基づき全体の方針を決定し、NIST が規定類を整備するというトップダウンによる取組が行われてきたが、2008 年には CNCI が開始され、政策レベル及びオペレーションレベルでサイバーセキュリティ体制の見直しが行われている。	US-CERT が連邦政府システムの情報収集及び監視を行い、各組織に情報提供を行う。ただし、US-CERT を含めた政府機関の 6 つのオペレーションセンター間の調整及び状況認識の同期は NCSC で行われる。インシデント対応においても実務部分は US-CERT が担当するが、対応・復旧の影響に関する省庁間調整等は NCRCG(DHS)が行う。	DHS	NIPP に基づき DHS が全体的な調整と推進を行う。NIPP の中で示された分野間連携モデルの中で重要インフラの分野ごとの情報共有を目指している。	分野ごとに設置された ISAC が中心となり、主に脅威、脆弱性インシデント情報等オペレーションに関する情報の共有を行う。さらに ISAC 間の調整、情報共有の場として ISAC-Council が整備されている。サイバー犯罪情報については InfraGuard（FBI）、一般的な技術情報に関しては CERT/CC を通じた情報共有も行われている。
英国	CSIA（CESG）	全体的な政策や戦略は CSIA を中心とした情報セキュリティに係る省庁、（CESG、BERR、CPNI）間の検討によって、"IA Governance Framework"に基づき決定される。	政府機関のネットワークに対する監視やインシデント対応は CESG 下の GovCERTUK が一括して行う。	CPNI	重要インフラ防護に係る取組は CPNI を中心に行われるが、活動の中心は民間企業である重要インフラ事業者の自主的な情報セキュリティ対策に重点が置かれている。	全体の脅威、脆弱性、インシデント情報の収集・分析・配信は CPNI 下の CSIRTUK が行う。各分野における情報共有は会議ベースの官民連携体制 IE やウェブベースの WARPs が整備されており、CPNI からのシステムの脅威・脆弱性情報等が共有されている。さらに、通信障害時の緊急対応体制として EC-RRG 構築の準備が進められている。
ドイツ	BMI/BSI	政府機関の情報セキュリティの全体方針は NPSI に基づき BMI によって取りまとめられる。具体的な施策の推進や規定、ツール類の整備は BSI で実施される。	政府機関におけるセキュリティインシデント発生時の対応は BSI の CERT-Bund が行う。さらに CERT-Bund の下に設置された IT Situation and Analysis Center が連邦政府のネットワークの監視、IT 危機対策センターがインシデント対応を担当している。	KRITIS/BSI	重要インフラ防護の国家戦略検討は BMI の下に設置された重要インフラ保護会議で行われ、具体的な施策は NPSI に基づき、BSI によって主導される。	政府機関だけでなく重要インフラに対するオペレーションセンターとしての機能も CERT-Bund が持つ。さらに CERT-Bund の中に設置された IT 危機対策センターでは国内の重要情報システムにおけるインシデント対応を行う。
オーストラリア	AGD DCTIA DSD	政府機関及び民間企業に対する情報セキュリティ政策の基本計画の策定は各政府機関の代表者によって構成され	DSD の中に設置された INFOSEC が政府機関における情報セキュリティ対策のサポートや、インシデント情報の	AGD	重要インフラ防護の戦略や体制については AGD の指揮の下、官民連携モデルである TISN の中で具体	TISN において各分野に設置されたグループの中で情報共有が行われる。国家全体のサイバーセキュリテ

		る ESCG において実施される。ただし、情報セキュリティに関するガイドラインやポリシー策定、人材育成はDSDで行われている。	収集・分析・配信を行う。		的な施策が実施される。	ィに関しては AusCERT が情報収集、監視を行っている。
シンガポール	IDA	政府機関のセキュリティはシンガポールの情報セキュリティ国家戦略である“InfoComm Security Masterplan”の中で示されており、具体的な政策、規定の立案、策定に至るまで全て IDA によって主導される。	政府機関のネットワーク全体の監視及びインシデント対応は IDA に設置された NCMC が行う。特にサイバー攻撃や犯罪に関しては同じ IDA 内の GITSIR や警察の TCD（SPF）の協力を得て、対応を行う。	IDA	重要インフラ防護に関しては NISC が全体的な方針を決定する。各重要インフラ防護活動の取りまとめや調整は”InfoComm Security Master Plan” に基づき、IDA によって行われる。	重要インフラを含め国家全体のサイバーセキュリティの監視は National CSIRT である SingCERT によって行われる。また重要インフラの情報セキュリティアセスメントのプラットフォームとして CII-SA が新たに設置されている。
韓国	MOPAS	政府機関の情報セキュリティは MIC の機能を受け継いだMOPAS やKCC によって主導される。ただし、国家の安全保障に係る事案については情報機関である NIS によって方針が決定される。	政府機関の情報セキュリティに関しては、国家情報セキュリティ基本方針に基づいて NCSC が設置され情報収集、監視、インシデント対応を行う。NCSC とは別に政府機関の ISAC として GISAC が設置されており、収集した情報をNCSC に提供している。その他、サイバーテロ・犯罪に対しては警察の CTRC や ICIC が情報収集や捜査を行う。	CPII	首相を委員長とする CPII、情報通信基盤保護法に基づいて、重要インフラの情報セキュリティ対策及び、計画の策定を行う。	国家全体のサイバーセキュリティの監視は KISC が行う。通信や金融等、一部の分野には ISAC が設置されており、分野内で脆弱性情報やセキュリティ対策についての情報を共有している。

1.3. 各国の政府機関の主要なセキュリティオペレーションセンター（SOC）の比較

各国の政府機関に設置されている主要なセキュリティオペレーションセンターの概要を以下に示す。

国	主要な SOC	上位組織	根拠法	業務内容	予算	職員	民間連携
米国	US-CERT	DHS	FISMA HSPD-7 Homeland Security Act of 2002 National Security Presidential Directive 38 National Strategy to Secure Cyber Space	連邦政府のネットワーク監視、情報収集（EINSTEIN の運用）、インシデント対応 国内のサイバーセキュリティに係る脅威・脆弱性分析、警戒情報の発信	8,300 万ドル[70] （約 83 億 1,000 万円）	CERT/CC からの出向者、セキュリティベンダ等の民間企業の専門家	ISAC への情報共有
英国	GovCERTUK	CESG	不明	政府機関内で発生したインシデント情報の収集及び対応 政府機関の情報システムの脅威・脆弱性に対する助言	不明	不明	CESG の職員
ドイツ	CERT-Bund	BSI	不明	政府機関のセキュリティインシデント対応 脆弱性や脅威に関する情報提供	不明	BSI の職員 10 名程度	重要インフラへの情報提供
オーストラリア	INFOSEC	DSD	不明	政府機関の情報セキュリティ対策サポート インシデント情報の収集、分析、アラートサービス BCP の策定	不明	不明	不明
シンガポール	NCMC	IDA	InfoComm Security Masterplan	政府機関のネットワークの監視、インシデント対応	NCMC のみの予算は不明。2005 年-2008 年のマスタープラン全体の予算は 23 億円。	監視業務を行う CWC は運営を民間委託。（e-cop 社のセキュリティエンジニアとアナリストが勤務）	運営はセキュリティベンダの e-cop 社が行う。
韓国	NCSC	NIS	国家情報セキュリティ基本方針	政府のネットワークの監視、情報収集、連邦政府における情報セキュリティインシデント対応	不明	約 60 人の正規職員と各省庁から出向した専門家 14 人	不明

[70] 1ドル＝100 円で計算（以下同様）

1.4. 各国の調査を通じたベストモデルの検討

1.4.1. 政府機関における情報連携

(1)セキュリティ統一基盤の構築

米国や英国では日本と同様に、政府機関に対する情報セキュリティ対策の基準が定められているが、同時にそれらを実装する基盤としてのシステムの構築にも力を入れている。両国では政府機関向けのネットワークを利用して、各組織のセキュリティを強化するためのマネージドサービスを展開している。特に米国の TIC[71]では、ネットワーク上のファイアーウォールやウイルスチェック機能だけでなく、各政府機関のサーバや PC 端末の OS 設定を規定した FDDC[72]にも準拠しており、システムの末端に至るまで、セキュリティ対策を徹底させることが可能となっている。日本でも、政府機関の情報セキュリティ対策に関して政府統一基準が策定されているが、各国においては、基準の有効性を高めるため、それら基準に準拠したセキュアな基盤システムの構築が進められている。

(2)政府系 SOC、CSIRT におけるインシデント報告の統一窓口の設置

米国、英国、ドイツ、韓国では、政府系 SOC の機能を情報収集や監視機能に限定せず、政府機関の情報セキュリティインシデントの 1 次受付先として機能させる取組が行われている。インシデント情報を1箇所に集中させることで、情報共有の流れが効率化されるだけでなく、各インシデントの対応がノウハウとして蓄積され、政府機関のインシデントへの耐性が高まることが期待される。韓国の NCSC[73]では 60 名の正規職員と各政府機関からの出向者 14 名の人員により、情報収集・監視、分析機能とインシデント対応機能を両方備えた体制が整備されている。「状況室」と呼ばれる部屋では 24 時間体制のネットワーク監視が行われており、一方でサイバー攻撃やインシデントが発生した際には原因調査と復旧支援も行う。さらに、各省庁からの出向者が常駐しているため、政府横断的な事案の調整機能も果たしている。センサ等で収集される情報だけでなく、各政府機関から報告されるインシデント情報も含めた総合的な分析を行うことで、より正確かつ迅速なインシデント対応を実現できると考えられる。

実際に政府のオペレーションを行う機能がインシデント報告を受付け、インシデントの 1 次対応を行うためには、以下のような検討が必要であると考えられる。

- センサ情報を活用した「検知」に留まらず、インシデント対応における適切な「判断」を行うためのオープンソース情報を活用した分析能力の醸成
- 過去に政府組織内で発生したインシデントの件数、内容、対応状況の分析
- 政府組織のインシデントを取り扱うために必要となる人材・能力の確保
- 連絡窓口で受け付けた情報に対する緊急度及び対応の判断方法(トリアージ能力の醸成)

---

[71] Trusted Internet Connections (TIC)、詳細については 27 ページ参照。
[72] 連邦政府デスクトップ基準(FDCC:Federal Desktop Core Configuration)、詳細については 36 ページ参照。
[73] National Cyber Security Center、詳細については 130 ページ参照。

・ 国際的な連携を実施するための能力確保
・ 政府組織に対するインシデント報告組織としての SOC の周知

(3)政府系 SOC、CSIRT への外部専門家の招聘による技術レベルの確保

ネットワーク上の情報収集・監視、分析等のオペレーション業務の遂行には高度な専門知識を要するため、米国やシンガポールの政府機関のオペレーションセンターは、国内の ISP やベンダ等の専門家を取り込んだ体制として構築されている。SOC の業務では、個々の対応を経験する中で得られるノウハウの蓄積が非常に重要であるため、人材の登用に当たっては 5 年程度の比較的長期に亘って業務に従事できる仕組みが構築されている。政府機関のオペレーションについても、民間人材の登用を積極的に行うことで、ISP やベンダのスキル・知見を取り入れ、国内最高レベルのオペレーション及びインシデント対応機能を有する組織が構築されている。

1.4.2. 重要インフラ防護における情報連携

(1)官民の情報共有に対する法的フレームワークの整備

米国やオーストラリアでは、官民連携による情報共有において、企業側からの積極的な情報開示を促進するため、共有された情報が開示されないための仕組みを整備している。特にオーストラリアの TISN では、TISN の活動に参加する企業が提供した情報が公開されるのを避けるため、機密情報に係る証書[74]を整備しており、参加者はこれに署名することで、オーストラリア会社法及びオーストラリア証券取引法の情報公開に関する免除規定が適用される。重要インフラ事業者と政府間の情報共有への協力を活発化させるためにも、オーストラリアのような法的フレームワークによる提供情報保護の仕組みを構築するべきである。

(2)重要インフラのオペレーション担当者による情報共有

重要インフラ事業者の対外的な調整を行う担当者間の情報共有に加えて、オペレーション担当者間の情報共有の機会を設けることが必要である。シンガポールでは、国内の重要インフラの情報システムのセキュリティについて、システムの担当者同士が検討を行うための CII-SA[75]というプロジェクトが開始されている。従来のように、対外的な調整担当者による情報共有は重要であるが、オペレーション等技術的な内容を取り扱う場合には、各事業者がそれぞれのオペレーション担当者に確認する工程が発生し、リアルタイムに正確な情報伝達を行うことは難しい。そのため新たな情報共有の場として、実際に IT 部門(IT-ISAC や CSIRTUK 等のような CSIRT 組織)の担当者間で情報共有を行う体制が構築されている。さらに、この体制では CSIRT 組織の考え方と同様に、担当者を特定個人に限定することで、メンバ間の信頼関係の中での情報共有の機会を提供することが効果的であると考えられる。

---

[74] 機密情報に係る証書(Deed of Confidentiality)、107 ページ参照。
[75] Critical InfoComm Infrastructure Surety Assessment(CII-SA)、121 ページ参照。

(3)重要インフラ事業者の情報セキュリティレベル底上げのための取組

重要インフラ防護を実現するためには情報連携を強化するとともに、重要インフラ事業者が組織として必要な情報セキュリティ対策を徹底することが必要である。英国やドイツでは重要インフラ防護の基本は重要インフラ事業者の情報セキュリティ対策を徹底することにあり、情報システムの信頼性を向上させることによって実現されると考えられている。例えば、ドイツでは政府調達において情報セキュリティに関する認証取得を課したり、リスクマネジメントのツールを提供したりする取組が実際に行われている。[76]重要インフラ事業者を対象としつつ、他の民間企業でも実施できる取組を展開することで、民間の情報セキュリティレベル全体の底上げも期待できる。

[76] IT-Grundschutz、87 ページ参照。

《第 II 部　各国調査》

2. 米国

2.1. 情報連携のフレームワーク

2.1.1. 情報セキュリティ関連組織

米国の情報セキュリティに関わる組織の体制は 2001 年の同時多発テロ以降大きく変化している。2003 年に設立された DHS が国家安全保障をベースとした情報セキュリティ政策の全体調整と指揮を行う。

政府機関のセキュリティに関しては OMB の主導の下、NIST においてシステムや規定の整備が進められている。

重要インフラ防護に関しては 2006 年に公表された National Infrastructure Protection Plan (NIPP)に基づき、DHS が全体的な調整・取りまとめ役となって個々の政策の取組を進めている。

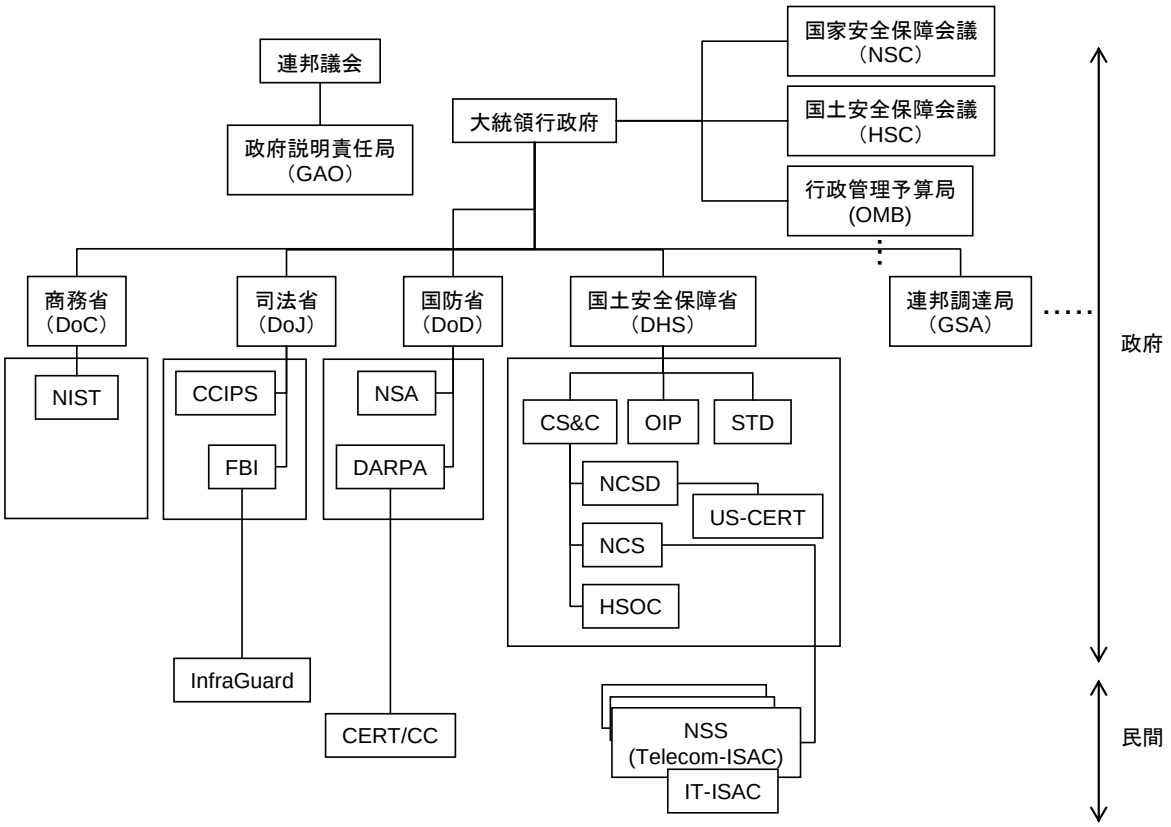


図 2-1 米国情報セキュリティ関連組織

(1)行政管理予算局（OMB：Office of Management and Budget）[77]

連邦政府予算準備及び大統領府局における予算管理支援を行う大統領直轄の組織。各政府機関のプログラムや政策、それら実施手順の効果に対する評価も行う。情報セキュリティに関して

[77] http://www.whitehouse.gov/omb/

は FISMA に基づいた連邦政府機関に対する自己監査実施指針の作成・提示及び結果の分析・評価までを実施している。2007 年からは連邦政府のネットワークサービスを最適化するイニシアチブである Trusted Internet Connections (TIC) の構築を進めている[78]。

(2)国土安全保障省(DHS:Department of Homeland Security)[79]

2002 年 11 月に、同時多発テロを契機に制定された国土安全保障法 (Homeland Security Act of 2002)によって設立された、国家の安全保障に係る事象について分野横断的な管理するための組織である。テロ対策に関わる既存(同省設置以前)の 8 省庁 22 の政府機関・部門が統合されて設立された。職員は約 17～18 万人で 2009 年の年間予算は 505 億ドル(約 5 兆 500 億円)である。国家安全保障に関わるサイバーセキュリティ戦略を立案するとともに、HISN をはじめとした政府横断的な情報連携システムの構築・運営や US-CERT 等の政府機関の SOC としての機能も有する。

(3)Office of Director of National Intelligence (ODNI)

"Intelligence Reform and Terrorism Prevention Act of 2004"によって 16 の省庁にある情報機関を束ねる役割として Director of National Intelligence (DNI)が設置された。DNI は国家保障に係るインテリジェンスの事案について大統領に直接助言を行うことができることになっている。また、DNI をサポートする組織として同法律によって ODNI が設立された。ODNI は 1,500 人の職員を抱え、予算は 435 億ドル(4 兆 3500 億円)と、米国の情報機関の予算を一括で管理している。[80]

(4)国家サイバーセキュリティ庁(NCSD:National Cyber Security Division)[81]

DHS 内に設置された情報システム保護のために国家レベルでのセキュリティ事案への対処の調整や重要インフラ保護のためのリスク管理プログラムの実施等を行う組織。2009 年の年間予算は 2 億 9350 万ドル(約 293 億 5000 万円)である。

(5)連邦捜査局(FBI:Federal Bureau of Investigation)[82]

司法省下の組織で、複数の州に渡る犯罪や、テロ等国家に対する重犯罪、連邦職員の犯罪の捜査を担当する機関。テロ対策として、DHS と国内全土において犯罪者情報及び出入国記録等を共有するシステムを運用している。2008 年 12 月現在、12,977 名の特別捜査官と、18,699 名のサポートスタッフ、計 31,676 名の人員を抱える。2008 年の予算は 6 億 8000 万ドル(約 680 億円)である。

---

[78] http://www.whitehouse.gov/omb/memoranda/fy2008/m08-05.pdf
[79] http://www.dhs.gov/index.shtm
[80] http://www.dni.gov/
[81] http://www.dhs.gov/xabout/structure/editorial_0839.shtm
[82] http://www.fbi.gov/

(6)連邦調達局(GSA:General Services Administration)[83]

1949 年 Federal Property and Administrative Service Act of 1949 に基づき設立された連邦政府の調達における基準策定や支援を行う組織である。情報セキュリティに関しては OMB の定めた政府の情報セキュリティ要求に基づき、各政府機関がそれらに適合する調達を行えるように支援を行う。

2.1.2. 法執行機関、防衛機関、情報機関の位置づけ

2003 年 DHS が設立された際、テロ対策に関連する組織の大半が DHS に統合されたが、連邦捜査局(FBI)、中央情報局(CIA)、国防情報局(DIA)等の主要な情報機関は独立して残ることとなった。ただし、これら情報機関には DHS に対してテロに関する情報共有を実施することが義務付けられている。[84]一方で、DHS 側に情報機関への指揮権はないため、その協力体制に対して疑問の声も上げられてきた。そうした課題の解決策として DHS と情報機関や防衛機関における情報共有の仕組みが幾つか構築されている。DHS と DOJ/FBI の間では、DHS が所有する出入国に関するデータと FBI が持つ犯罪に関するデータを共有している。また、FBI におけるサイバー犯罪に関する活動や、官民連携体制である InfraGuard の活動等でも DHS との情報連携が行われている。

なお、米国の政府機関では、情報の機密度に合わせて図 2-2 に示すような流れで情報が管理されている。国際的な情報機関から提供される最重要機密情報を含む情報は、国内の情報機関が連絡窓口となり管理され、分類が行われる。軍事的な情報は DoD に、それ以外の分類されない情報が DHS や警察に対して受け渡される。[85,86]

---

[83] General Services Administration

[84] 2002 年に制定された国土安全報償情報共有法(Homeland Security Infomation Sharing Act of 2002)によって、テロ関連情報等の国土安全保障に関する情報を情報機関と連邦政府、州・地方政府で共有することが義務付けられた。同法律は DHS の設置法である国土安全保障法(2002)とともに制定された。
(http://www.fas.org/irp/congress/2002_cr/hr4598.html 参照)

[85] http://www.dtic.mil/ndia/2003interop/Lunch.pdf

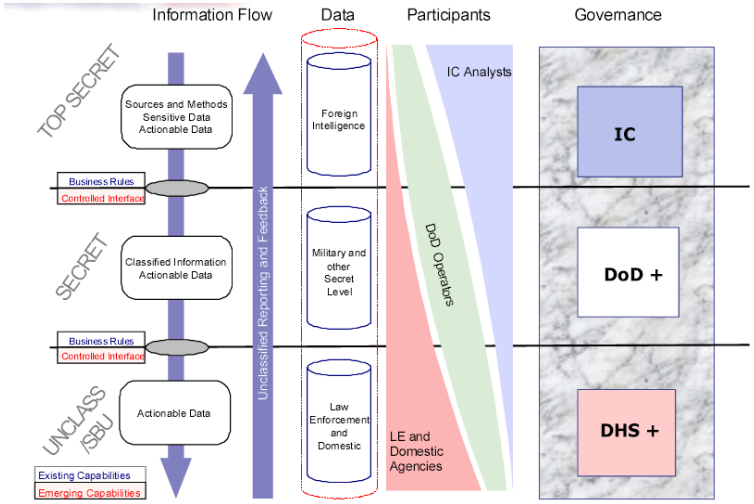


図 2-2 米国における機密情報の流れ[87,88]

2.1.3. 情報連携の分類

米国における情報連携のフレームワークを以下に示す。

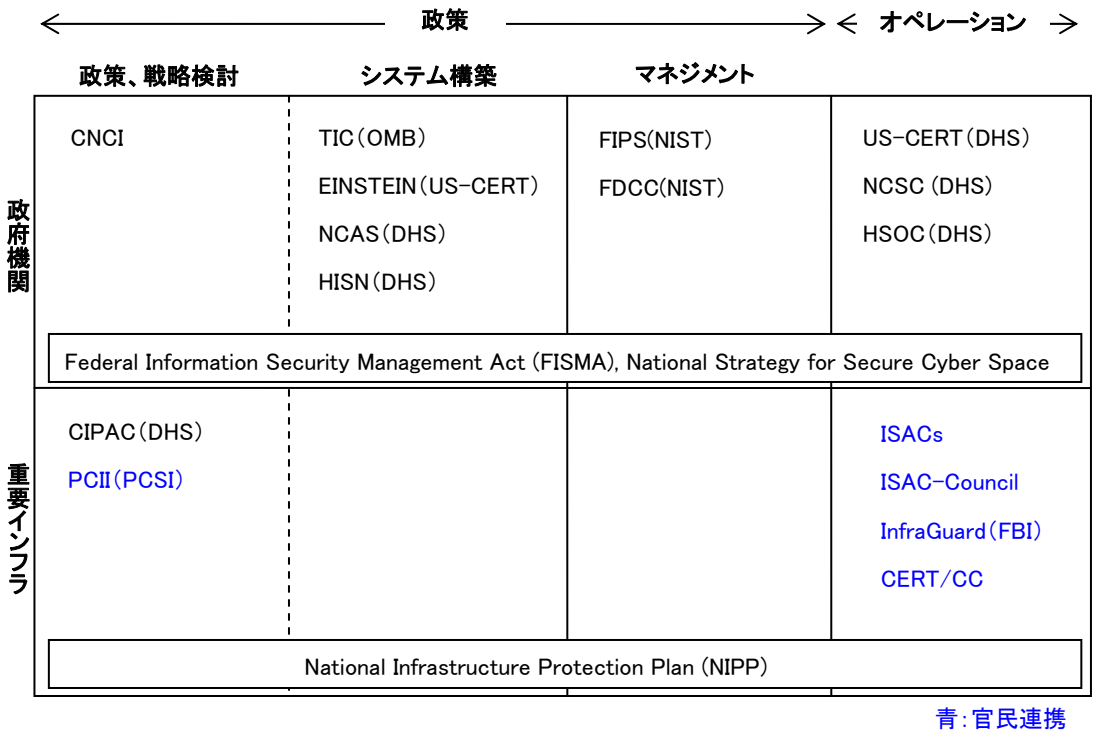


図 2-3 米国における情報連携のフレームワークの分類

[87] http://www.dtic.mil/ndia/2003interop/Lunch.pdf

[88] 図中の IC は Intelligence Community の略で情報機関を指す。

2.1.4. 情報連携の関係図

米国における情報連携の関係図を以下に示す。

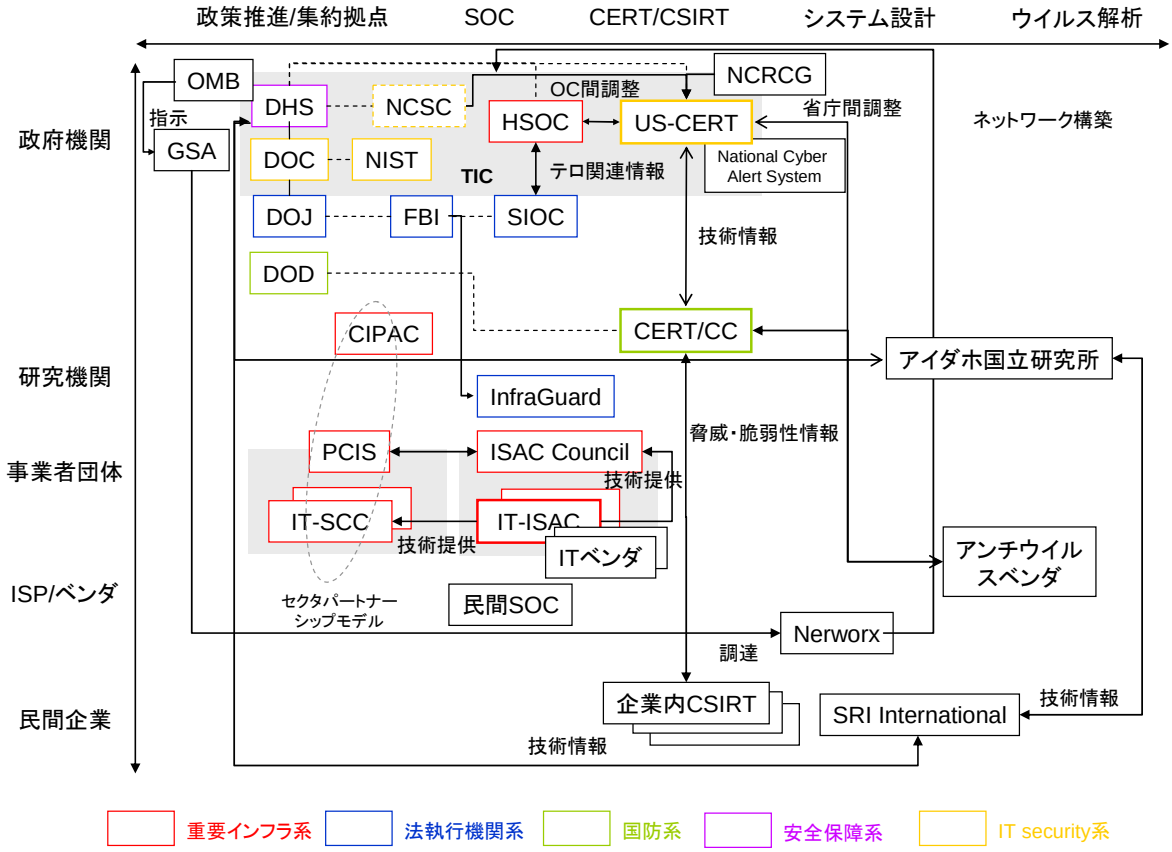


図 2-4 米国における情報連携の関係図

2.2. 政府機関における情報連携

2002 年に制定された連邦情報セキュリティ管理法（FISMA）により政府機関における情報セキュリティ管理が強化されている。政府機関の情報セキュリティ対策の方針決定は OMB が実施しており、標準やツール等の策定は NIST、ネットワークの調達に関しては GSA、IT 関連の製品・サービスの調達に関しては国立衛生研究所の National Information Technology Acquisitions and Assessment Center（NITAAC）が担当する。

2.2.1. 政策レベル

2.2.1.1. 政策・戦略検討

米国における国家安全保障に関わる取組については PDD38 や HSPD-7 等のように大統領や DHS からトップダウンで推進されることが多い。政府の情報セキュリティ政策は、こうした大統領令に基づき、予算決定機関である OMB から具体的な施策として示される。

(1)Comprehensive National Cyber Security Initiative (CNCI)[89]

HSPD-23 及び NSPD-54 に基づいて 2008 年 1 月に開始されたイニシアチブ。連邦政府の情報システム保護のための政策、戦略、ガイドラインの策定を主な目的としている。具体的な活動としては、今後予想される脅威に対して、連邦政府が備えるべき技術的、組織的可用性について検討を行うこととしている。具体的目標としては以下の 12 項目が挙げられている。

（CNCI で示された 12 の目標）

① 統合された連邦政府のネットワークへの移行
② 連邦政府固有の検知システムの構築
③ 侵入防止ツールの開発及び構築
④ 現状の見直し結果を研究開発への投資に結びつけること
⑤ 政府のオペレーションセンターの統合
⑥ 政府全体のサイバーインテリジェンスプランの構築
⑦ 機密通信におけるセキュリティの向上
⑧ サイバー教育の拡大
⑨ 革新技術の明示
⑩ 抑止技術及びプログラムの明示
⑪ サプライチェーンのリスクマネジメントに対して多角的なアプローチの構築
⑫ 民間部門のサイバーセキュリティに対する役割の定義

---

[89] http://www.csis.org/component/option,com_csis_pubs/task,view/id,5157/

CNCIを受け継ぐ形となったオバマ大統領は、大統領選挙戦のキャンペーン中から、サイバーセキュリティの重要性を主張しており、公約として、直接大統領にサイバーセキュリティに関する助言を行う国家サイバーアドバイザーの設置を掲げていた。そのため、就任後の2009年2月9日には CNCI で掲げられた事項が適切に実装されているか、リソース配分されているか、議会及び民間部門との調整が進んでいるかという観点で、省庁間で60日以内に見直すように指示している。

(2)Joint Inter- Agency Cyber task Force (JIACTF)[90]

DNIによって設置されたCNCIの監視と調整を行っており、大統領に対してCNCIの実装状況に関して、4半期に一度報告と助言を行う。

2.2.1.2. システム構築

(1)Trusted Internet Connections (TIC)[91]

2008年OMBが公表した覚書M-08-05 -Implementation of Trusted Internet Connections[92]において連邦政府のインターネット接続点を統合して連邦政府内のデータのトラフィックを監視し、政府のインシデント対応能力の向上を目指す政策実施が宣言された。外部接続点の統合予定として、2009年1月の時点で4,300箇所、5月までに2,758箇所、6月までには目標である100以下(当初の目標は 50)を目指すとしている。個々の外部ネットワーク接続は(Managed Trusted Internet Protocol Services (MTIPS))という規定によって標準化されることになっている。調達は連邦調達局(GSA)の連邦政府のネットワーク調達プログラムNetworxの中で実施されている。Networxによって認定された民間ベンダが"Networx government wide network and telecommunications contract"という契約の下で、ネットワークの機能構築及びサービス提供を行う。また、構築されるネットワークではIPv6や連邦政府デスクトップ基準(FDCC: Federal Desktop Core Configuration)にも対応している。

2008年12月に行われた入札ではAT&Tが最初のMTIPSのサービスプロバイダとなった[93]。OMBは今後もベンダ側からのMTIPSに関する提案書を広く受け付け、2009年の前半に可能な限り多くの入札を行う予定としている。Networx Universalには481億ドル(約4兆8100億円)の予算が用意されているが、Networxプログラムは柔軟な契約形態であるため、各政府機関がMTIPS以外に独自の要件を加える等、自由に調達内容を設定する。

各政府機関は組織の状況に合わせてTIC Access Provider (TICAP)の形態を以下の3つから選択することができる。

・ **Single Service TICAP** (組織内TICを運用可能な大組織向けの形態であり、組織内部のみに

[90] 89と同じ。
[91] http://www.whitehouse.gov/omb/assets/egov_docs/2008_TIC_SOC_EvaluationReport.pdf
[92] http://homeland.house.gov/SiteDocuments/20080228104608-98324.pdf
[93] http://gcn.com/Articles/2008/12/16/GSA-awards-first-contract-for-TIC-service-on-Networx.aspx

サービスを提供する場合に適用される）

- **Multi Service TICAP**（組織内で TIC を運用可能な大組織向けの形態であり、組織の内部、さらに組織外に対しても一部サービスを提供する場合に適用される。）
- **TICAP**（組織内では TIC を運用できない小組織向けの形態であり、共通アクセスポイントの TICAP をネットワークを介したサービスとして利用する。）

（TICAP が提供するサービスの例）

- アンチウイルスマネジメントサービス （AVMS: Anti Virus Management Service）
- 侵入検知／防止システム（IDPS：Intrusion Detection and Prevention Service）
- インシデント対応サービス（INRS：Incident Response Service ）
- マネージド電子認証サービス(MEAS：Managed E-Authentication Service)
- マネージドファイアーウォールサービス（MFS：Managed Firewall Service）
- セキュアマネージドメールサービス（SMEMS：Secure Managed Email Service）
- 脆弱性スキャニングサービス（VSS：Vulnerability Scanning Service）
- マネージド階層セキュリティサービス(MTSS：Managed Tiered Security Services)

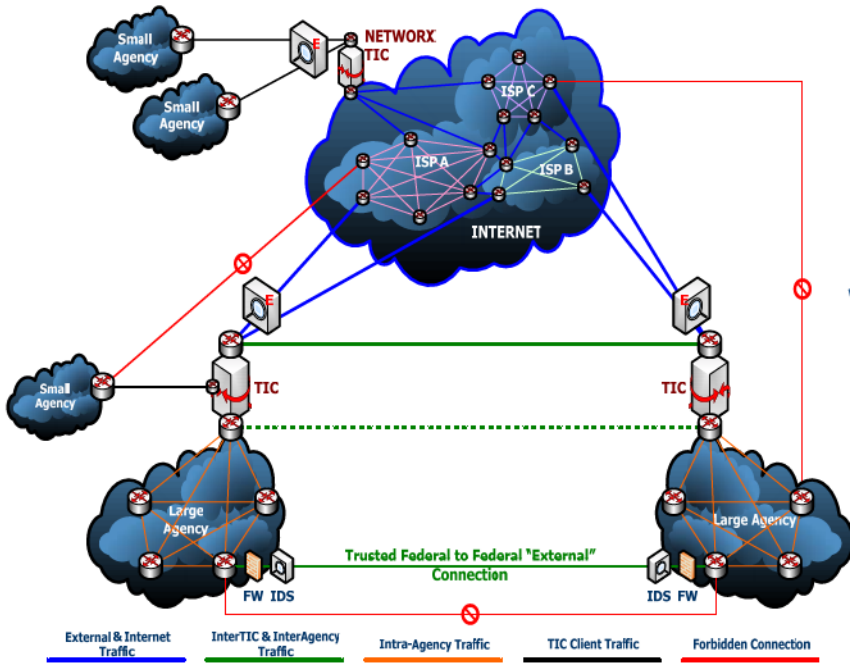


図 2-5 TIC の概要図[94]

[94] http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_OVERVIEW&contentId=16100

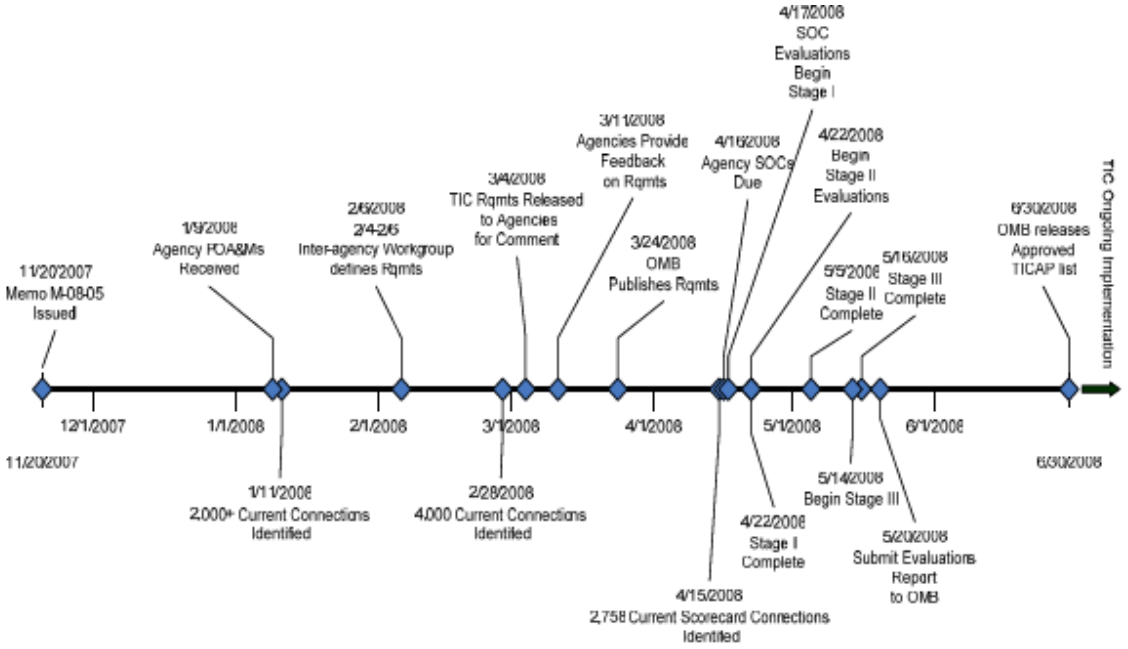


図 2-6 TIC 整備のタイムライン[95]

(2)Networx プログラム[96]

連邦調達局(GSA: General Services Administration)が推進する政府の通信ネットワーク調達プログラムである。表 2-1 に Networx プログラムにおいて認定された事業者が提供する機能及び要件を示す。2007 年にはプログラム参加のための入札が、提供するサービスレベルごとに分けて実施された。実際の落札業者を表 2-2 に示す。

表 2-1 Networx プログラムの提供する機能及び要件

機能・要件	概要
サービス継続性	現在 FTS2001 及びクロスオーバ契約による全てのサービスを対象
競争的価格	全体予算としては FTS2001 より小さい
高品質サービス	信頼性があり連邦政府のミッションに合致した効果的サービスの提供
フルサービスの提供	契約ライフサイクルの中であらゆるサービスを提供する
代替ソース	主要なテレコミュニケーション会社を含む産業サービスプロバイダとの連携
運用サポート	発注、目録管理機能
移行サポート	タイムリーで効果的な移行のための調整と援助
パフォーマンスに基づく契約	契約者のパフォーマンスと品質を確保するための SLA の締結

表 2-2 Networx プログラムの認定ベンダ

[95] 91 と同じ。

[96] http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_OVERVIEW&contentId=16100

契約分類	サービス内容	落札者
Networx Universal （2007 年 3 月 29 日入札）	36 種のサービス[97]に対応 FTS2001 からの継続性確保	AT&T Corp.
		MCI communications Services, Inc. d/b/a Verizon Business
		Qwest Government Services, Inc.
Networx Enterprise （2007 年 5 月 30 日入札）	IIP 中心サービス／9 種のサービス[98]に対応	AT&T Corp.
		MCI Communications Services, Inc. d/b/a Verizon Business Services
		Qwest Government Services, Inc.
		Level 3 Communications, Inc.
		Sprint Nextel Corp.

これまで US-CERT が整備してきた EINSTEIN（(3)参照）は、改めて TIC 上に整備されることになっている。各政府機関に設置された EINSTEIN のセンサから収集された情報は一度 US-CERT に集約された上で、EINSTEIN 以外から収集された情報とともに TIC 上の情報を集中管理するポータル SOC のデータベースに蓄積される。インシデントが発生した際は US-CERT のオペレーションのもと、TIC ポータルのデータベースの情報による情報提供や、各組織の対応への助言がなされる。

[97] 96 と同じ。
[98] 96 と同じ。

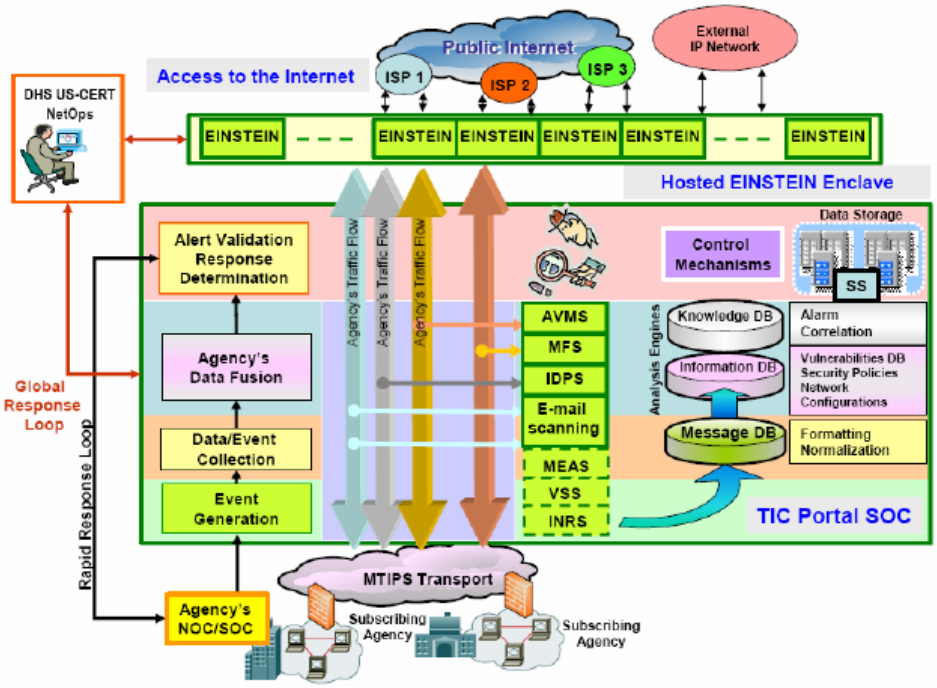


図 2-7 MTIPS による政府機関のトラフィック保護[99]

(3)EINSTEIN Program[100]

US-CERT によって開発された連邦政府のネットワークゲートウェイを監視する侵入検知システム。2002 年の E-Government Act of 2002 等によって進められた政府のインターネットサービス向上を目指す計画の一部として進められている。当初の開発は NIST で行われていたが、その後連邦調達局の連邦コンピュータインシデント対応センター(FedCIRC)に移され、2003 年からは FedCIRC の機能を受け継いだ US-CERT に移された。その後、EINSTEIN 機器は US-CERT によって各政府機関に配備されることとなる。EINSTEIN II からは各政府機関(国防省、情報機関を除く)に設置が義務付けられている。設置は国土安全保障法及び FISMA、HSPD7 によって大枠が示され、2007 年 11 月 20 日の OMB の公表[101]によって具体化された。2008 年時点で 600 以上ある連邦政府機関のうち 15 の機関に設置されている。

また、2007 年から進められている政府ネットワーク TIC の中での運用の準備も進められている。各政府機関に設置された EINSTEIN 機器はアラートやイベント情報を収集し、分析されたデータは US-CERT に送付される。グローバルなセキュリティ脅威が発生した場合は全ての TIC ポータルの SOC と各省庁の SOC に対して電話／メールによって連絡が行われる。

TIC のサービスを提供するサービスプロバイダに求められる要件として①EINSTEIN 機器と US-CERT の間に十分な帯域を確保すること、 ②US－CERT から発信されたアラートを各政府機

[99] 96 と同じ。
[100] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf
[101] http://www.whitehouse.gov/omb/memoranda/fy2008/m08-05.pdf

関の NOC/SOC に対して迅速に伝達すること、③US-CERT から発信されたアラートを既知の脅威として SOC のデータベースで管理すること、等が挙げられている。

参考までに、EINSTEIN 機器が収集するデータを以下に示す。(US-CERT では分析のために必要な情報であれば、これ以外の情報の提出を政府機関に求めることもある。)各政府機関から収集されたデータによる分析結果は US-CERT から機関にフィードバックされる。

(EINSTEIN プログラムにおける共有情報)

- AS 番号[102]
- ICMP のタイプとコード
- パケット長
- プロトコル
- データソースの場所
- IP アドレスの送信元と送信先
- 送信ポートと受信ポート
- TCP フラグ情報
- タイムスタンプ、遅延情報

(4)国土安全保障情報ネットワーク(HISN:Homeland Security Information Network)

連邦政府、州政府、自治体、重要インフラ事業者(電力会社等)、国際機関との間において機密ではあるが明確に分類されていない情報(SBU:Sensitive But Unclassified)を処理するために構築された、セキュアで信頼性を確保したウェブベースのプラットフォームである。元々は、国家の様々な脅威に対する防護・対応・復旧活動を支援する目的で整備されていた既存の情報共有ネットワークを統合するためのインターフェースとして開発された。ウェブベースの技術であるため、機能を柔軟に追加することが可能となっている。また、ステークホルダが整備している既存のシステム間を接続できるため、国内のあらゆる地域との間で、リアルタイムにインタラクティブな情報交換を行うことができる。そのため犯罪捜査や重要インフラ防護まで幅広い分野における情報共有・調整を可能である。以下に HISN が対象とする組織分類及び HISN の基本的な機能を示す。

(HISN が対象とする組織分類)[103]

- インテリジェンス及び分析
- 法執行
- 緊急対応
- 重要インフラ防護

---

[102] 大規模 IP ネットワーク内において各組織が保有・運用する自立したネットワーク(AS)を識別する番号

[103] http://www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm

・その他、何らかの形で HISN の情報共有に協力する組織

（HISN の機能）

・24 時間 365 日体制
・ドキュメントライブラリ
・インスタントメッセージツール
・ウェブ会議
・インシデントレポート
・状況認識及び分析結果（COP：Common Operational Picture）
・地理情報の視覚化（iCAV：Integrated Common Analytical Viewer）
・各種発表(ニュースリリース等)
・タスク一覧
・カレンダー機能
・RSS
・オンライントレーニング

（参考）GAO による HISN に対する指摘

2007 年に GAO が公表したレポート“Homeland Security Information Network Needs to Be Better Coordinated with Key State and Local Initiatives”[104]では、DHS が HISN を有効に活用していないため、省庁間や州政府間における情報連携が機能していないことを指摘している。具体的には DHS 側が提供する情報が、各機関のニーズに合ったものなのか、またどのように使われるべきなのかが示されていないことを問題として指摘している。GAO では、現状の HISN が有効に機能していない理由としては 2001 年の同時多発テロの際に、組織の設立を急いだために HISN における連邦政府と州政府・地域の情報共有イニシアチブにおける位置づけや役割を示しきれず、HISN の機能について十分な理解が得られなかったためと分析している。結果として、州政府において連邦政府からの情報共有が十分に行われないだけでなく、米国全土で情報共有を行う他のシステム（緊急サービスシステム等）の情報共有ツールとの差別化が図られず、州政府側の手間を増やしているとも指摘している。GAO 側の要求としては州政府の役割を明確にするとともに、DHS が所有するその他のネットワークシステムにおいて同様の問題が発生しないようにすることが挙げられている。

[104] http://www.gao.gov/new.items/d07822t.pdf

(5)National Cyber Alert System[105]

US-CERT のシステムの 1 つであり、対象者を限定してリアルタイムの情報を提供するために、分類毎に 6 つのメーリングリストが用意されている。配信される情報は基本的には公開情報である。システム開発は CERT/CC、Symantec 社、Network Associates 社の McAfee 部門で行われ、2004 年から US-CERT で運用が開始されている。サービス対象者に制限はないが、ISAC や ISP、民間企業等幅広いユーザがシステムに登録しており、ユーザ登録数は全カテゴリ合わせて 30 万人に上る。

（NCAS メーリングリストの 6 つのカテゴリ）

- Technical Cyber Security Alerts（http://www.us-cert.gov/cas/techalerts/）
- Cyber Security Alerts（非技術情報）（http://www.us-cert.gov/cas/alerts/）
- Cyber Security Bulletins（http://www.us-cert.gov/cas/bulletins/）
- Cyber Security Tips（http://www.us-cert.gov/cas/tips/）
- Current Activity（http://www.us-cert.gov/current/）
- Vulnerability Notes（http://www.kb.cert.org/vuls/）

(6)DOJ/FBI-DHS INTERIM DATA SHARING MODEL (iDSM)

DOJ/FBI と DHS 間の情報連携のために 2003 年にパイロット的に開始されたプログラム。FBI 側からは指名手配犯等の犯罪者情報、DHS 側からは VISA の発行を拒否された人物や、米国から強制退去させられた人物の情報が提供される。プログラムは共有データコンポーネントと共有サービスコンポーネントからなり、共有データコンポーネントには、両機関が所有する指紋等の生体情報が相手機関で利用可能な形でコピーされる。共有サービスコンポーネントでは、各機関が必要とする情報を取り出すためのサービスであり、指紋情報だけでなく、FBI が所有する犯罪歴のデータ、DHS の持つ出入国に関するデータも抽出することが出来る。

(7)Intelligence Community System for Information Sharing (ICSIS)

ICSIS は情報機関のデータ共有システム(JWICS)や、SIPRNET と呼ばれる DoD の機密用 IP ルータネットワーク、SBU 情報にアクセス可能な Open Source Information System (OSIS)等を通じて、国家安全保障に関わる情報を州政府等、末端組織までに伝達するためのシステムである。

[105] http://www.us-cert.gov/cas/alldocs.html

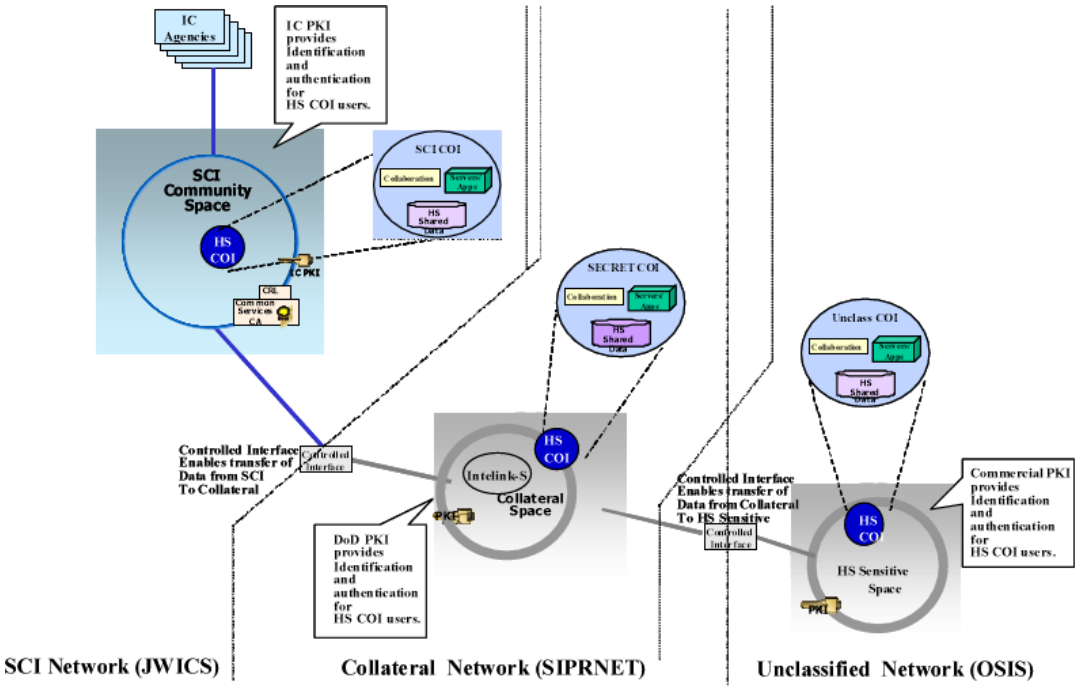


図 2-8 ICSIS の構成[106]

2.2.1.3. マネジメント

(1)連邦情報セキュリティ管理法(FISMA：Federal Information Security Management Act of 2002)

2002 年 12 月に制定された電子政府法の III 連邦情報セキュリティ管理法（FISMA）では、各連邦政府機関に対して、情報及び情報システムのセキュリティを強化するためのプログラムを開発、文書化、実践することを義務付けている。 また、同法は、NIST（米国国立標準技術研究所）に対して、連邦政府が FISMA に準拠するための支援をすることを義務付けている。 そのため、NIST では 2003 年 1 月に「FISMA 導入プロジェクト （The FISMA Implementation Project）」 を立ち上げ、情報システムのセキュリティを強化し安全に運用するための様々な規格やガイドラインを策定している。NIST で進められている FISMA 導入の流れを以下に示す。

フェーズ I ：
FISMA 関連のセキュリティ規格（FIPS）及びガイドライン(SP シリーズ）の開発・策定
2007 年 8 月現在 FISMA 導入プロジェクト関連文書は、ほぼ策定済み。（2003-2007）
フェーズ II ：
セキュリティ評価機関を認定するプログラムの開発。（2007-2009）
フェーズ III:
セキュリティ評価ツール検証プログラムの開発（2007-2009）

[106] 87 と同じ。

（フェーズ III は、単独のフェーズとしてではなく、フェーズ II に組み込まれ、既存の IT 製品のテスト、評価や検証プログラムを利用）

(2)Special Publications 800 Series

SP800 関連文書は、NIST の情報技術研究所（ITL：Information Technology Laboratory）の CSD（Computer Security Division）が発行するコンピュータセキュリティ関係のレポートである。米国の政府機関がセキュリティ対策を実施する際に利用することを前提として纏められた文書となっており、 内容的には、セキュリティマネジメント、リスクマネジメント、セキュリティ技術、セキュリティの対策状況を評価する指標、セキュリティ教育、インシデント対応等、セキュリティに関する幅広い分野を網羅している[107]。

(3)連邦政府情報処理基準（FIPS：Federal Information Processing Standards）[108]

米国商務長官の承認を受けて、NIST が公布した情報セキュリティ関連の文書。SP800 シリーズから FIPS となった文書もある。主な対象は米国政府機関であり、推奨する管理策や要求事項、暗号化やハッシュ化、認証、デジタル署名及び LAN のセキュリティ等、分野別に、詳細な基準や要求事項、ガイドラインを示している。

(4)連邦政府デスクトップ基準（FDCC： Federal Desktop Core Configuration）

2007 年に OMB が公表した覚書[109]に基づく取組。FISMA に従い、連邦政府内で使われる Windows ソフトウエアを「共通セキュリティ設定」に準拠させることで、連邦政府の端末のセキュリティ確保とパッチ当て等に掛かるコスト削減を目指す。「共通セキュリティ設定」は NIST、国防情報システム局（DISA：Defense Information System Agency）、国家安全保障局（NSA：National Security Agency）、Microsoft によって共同で開発された。OS は Windows XP Professional SP2 と Windows Vista に対応している。

(5)Chief Information Officer– Solutions and Partners 2 Innovations （CIO–SP2i）[110]

連邦政府におけるITに係る調達プログラム。国立衛生研究所（NIH：National Institutes of Health）の National Information Technology Acquisitions and Assessment Center（NITAAC）が 2000 年に OMB から Executive Agent[111]として認定され、CIO–SP2i の管理を行う組織となった。

---

[107] http://www.ipa.go.jp/security/publications/nist/nist_publications.html

[108] http://www.ipa.go.jp/security/publications/nist/fisma.html

[109] MEMORANDUM FOR CHIEF INFORMATION OFFICERS, "Managing Security Risk By Using Common Security Configurations"
http://www.cio.gov/documents/Windows_Common_Security_Configurations.doc

[110] http://www.actgov.org/actiac/documents/pdfs/IACLuncheonBriefingPooksHill11708.pdf

[111] 1994 年政府管理改革法（The Government Management Reform Act of 1994）に基づき、OMB は 6 つの業務範囲における政府機関への予算・契約管理業務を、特定の政府機関（Executive Agent）に移譲し、ビジネスとして運

NITAAC では連邦政府の IT に係る調達に対して、CIO-SP2i を含め 3 つの契約プログラムを管理している（他は IW2nd、ECS III）。どのプログラムもビジネスとして運用されており、NITAAC は顧客である連邦政府に対して、IT サービスや機器の調達・契約管理をサービスとして提供し、契約金額の 1%程度を経費として徴収する仕組みとなっている。連邦政府がこうしたプログラムを活用するメリットとして、調達にかかる期間が短いことや、NITAAC 側で調達先情報を一括で管理している点にある。

（CIO-SP2i の業務範囲）[112]
①CIO 業務サポート
②IT アウトソーシング
③IT オペレーション及びメンテナンス
④インテグレーションサービス
⑤重要インフラ防護、情報保証
⑥電子政府
⑦ERP（Enterprise Resource Planning）
⑧調査、研究
⑨ソフトウエア開発

表 2-3 NITAAC が管理する連邦政府の IT に関する調達

	CIO-SP2i	IW2nd	ECS III
契約形態	委託	委託、購買	購買
業務範囲	IT サービス IT ソリューション	IT COTS[113]ハードウエア／ソフトウエア システムインテグレーション IT サービス・ソリューション	IT COTS ハードウエア／ソフトウエア
契約者（民間）	プライム：44 社 サブ：627 社	プライム：24 社 サブ：230 社	プライム：63 社
プログラムのライフプラン	2000 年～2010 年の 10 年間	2000 年～2010 年の 10 年間	2002 年～2012 年の 10 年間
契約総額	195 億ドル（1 兆 9500 億円）	150 億ドル（1 兆 5000 億円）	60 億ドル（6000 億円）
入札に要	7-28 営業日	タスクオーダ：7－21 営業日	1-3 営業日

用させるパイロットプログラムを開始した。
[112] http://nitaac.nih.gov/downloads/ciosp2/CIOSP2_taskdef.html
[113] （COTS：Commertial-off-the-Shel）：既製品で販売やリースが可能となっているソフトウエア製品

する時間		購買：7-10 営業日	
経費	大企業：契約金額の 1% 中小企業：1%以下（規模に応じて）※中小企業を選択することのインセンティブとして経費が引き下げられる。	大企業：契約金額の 1% （中小企業を選択することのインセンティブとして経費が引き下げられる）	契約金額の 1%
マネジメントの特徴	業者に対する業務指示、サポート 委託業務の監視 ウェブベースの情報提供	委託業務の監視 ウェブベースの情報提供	ウェブベースの情報提供

2.2.2. オペレーションレベル

2.2.2.1. 組織

(1)National Cyber Security Center (NCSC)

2008 年 1 月 HSPD-23（Cyber Security and Monitoring）によって設立された政府機関の通信ネットワークの監視・情報収集を行うオペレーションセンターであり、DHS 長官に直接報告を行う。HSPD-23 の大部分は非公開となっており、NCSC の機能が明文化された文書は公表されていない。ただし、2008 年 9 月 15 日に行われた DHS 次官の Paul Schneider の挨拶によると[114]、NCSC は NSA、FBI、DoD そして DHS 等 6 つの政府機関にそれぞれ設置されているオペレーションセンター[115]の中継点となり、連邦政府のシステムに対する包括的な状況認識を実現することを目的としており、さらに、.mil、 .ic、 .gov のドメイン間の調整機能を持つとされている。US-CERT は DHS 管轄下のオペレーションセンターとして NCSC に管理されると同時に、US-CERT の持つ連邦政府ネットワークの監視システム(EINSTEIN 等)から収集した情報を各オペレーションセンターに提供する NCSC の情報ソースとしての役割を果たすという。

HSPD-23 の内容[116]

2008 年に米国で開催された会議“Information Assurance and Enabling Identity Management -Security 2008”のキーノートの中で、米国国家情報局の長官 Steve Chabinsky 氏が説明した内容によると、HSPD-23 では以下の 12 のイニシアチブが示されたとされている。(HSPD-23 の内容は前述の CNCI に与えられたミッションに等しい。)

---

[114] http://www.dhs.gov/xnews/speeches/sp_1222897551951.shtm

[115] オペレーションセンターの 1 つは DoD のネットワークの運用・監視組織である JTF-GNO（Joint Task Force for Global Network Operations）である。その他のオペレーションセンターについては公表されていない。

[116] http://srmsblog.burtongroup.com/2008/11/government-plans-top-secret-hspd-23-program-for-enhancing-information-assurance.html

① 政府機関のインターネット等の外部接続点を現在の 4,500 から 100 以下まで減らし、政府ネットワークの防御対策を統合すること。(⇒TIC の構築)
② 侵入検知システム EINSTEIN II の配備を①の取組の中で進めること。
③ 侵入を防御する Einstein III の配備を進めること。
④ 連邦政府の CTO クラスがサイバー上の活動に関する研究開発に投資するための調整を行うこと。
⑤ サイバー空間の脅威を広く把握するため、政府のオペレーションセンターを相互に接続し、脅威に関する情報を横断的に共有すること。そのために政府機関全体でサイバー防御策を共有し、標準化や規定として整備すること。
⑥ 政府のサイバー上のカウンターインテリジェンス計画を策定すること。
⑦ 機密扱いの情報を取り扱うネットワークの安全性を強化すること。
⑧ サイバーセキュリティ教育を拡大すること。技術やツールやベストプラクティスに関するプログラムを全政府機関に対して実施すること。さらに、国民に対する教育にも拡大すること。
⑨ 先の動向を見据えたセキュリティ戦略及びプログラムを策定すること。常に新技術を着目することで、新たな犯罪に対して事前の対策を打てるようにすること。
⑩ 各分野の専門家を集めて、持続的なサイバー防護戦略とプログラムを策定すること。
⑪ グローバルサプライチェーンに対するリスクマネジメントとして多角的なアプローチを実施すること。この場合の脅威は世界中の小規模／大規模なサプライヤーから供給されるハードウエア／ソフトウエアを含む。またサプライチェーンに対するリスクマネジメント標準も必要である。
⑫ サイバーセキュリティを民間ドメインまで拡大すること。現在進行中の取組を強化すると共に、民間部門と連携してサイバーセキュリティに対する民間部門における取組方法について検討すること。

NCSC の機能について

2009 年 3 月 6 日、およそ 1 年間 NCSC 局長を務めてきた Rod Beckstrom 氏が、NCSC に係る組織間の問題を理由に辞職した。Beckstrom 氏は自身の辞表[117]の中で米国のサイバーセキュリティにおける縄張り争いについて指摘しており、特に NCSC の活動において、NSA がその機能をコントロールしようとしている点を問題点として挙げた。Beckstrom 氏は「諜報／情報(機関＝NSA)の文化と、ネットワーク・オペレーションやセキュリティ(に携わる組織)の文化とはまったく異質だ。加えて言えば、もしも 1 つの機関が(直接的にせよ間接的にせよ)あらゆる政府上級機関のネットワークセキュリティと監視を管轄するならば、我が国の民主主義的プロセスに対するその脅威は非常に深刻なものとなる」と主張しており、米国のサイバーセキュリティにおける情報機関の台頭に懸念を示している。これは、Beckstrom 氏の辞任の前日にオバマ政権で DNI に就任した

[117] http://www.wired.com/images_blogs/dangerroom/files/ncsc_directors_resignation1.pdf(Beckstrom 氏の辞表)

Dennis Blair 氏が議会において、「DHS ではなく、NSA がサイバーセキュリティを担当すべきだ」と発言したことが直接のきっかけになっていると考えられる[118]。一方で、NCSC が DHS から十分な支援とリソースを得られなかったことも指摘しており、NCSC の在り方について疑問を投げかけている。

(2)US-CERT (United States Computer Emergency Readiness Team)

DHS 内に設置された米国の National CSIRT。2009 年の予算は 8,300 万ドル（約 83 億 1,000 万円）である。DHS と CERT/CC の連携によって運営されている。US-CERT は、サイバー攻撃への防御の連携、脅威・脆弱性情報の分析、脅威警報等を行う。CERT/CC は、学術的な連邦政府予算の研究開発センターであり、ベンダに対してサイバーセキュリティ、脆弱性、インシデント対応に関する技術的専門性を提供する。US-CERT は、CERT/CC の技術専門性を活用し、また、ISAC と連携することにより政府向けのインシデント対応の役割を担う。

連邦政府のインシデントマネジメントを担当するとともに、国内のサイバーセキュリティに係る問題を扱う中心組織として機能する。

（US-CERT の根拠法令）

- FISMA
- HSPD-7
- Homeland Security Act of 2002
- National Security Presidential Directive 38
- National Strategy to Secure Cyber Space

(3)National Cyber Response Coordination Group （NCRCG）

13 の連邦政府機関からなるグループであり、国家にとって重大なサイバーインシデントが発生した際に、政府機関のインシデント対応をサポートするために、UC-CERT、法執行機関、情報機関の調整を行う。2006 年に行われたサイバー演習「Cyber Storm」では、NCRCG が中心となって組織間の調整、対応や復旧に影響を及ぼす政策問題の特定、官民の重要情報共有のルートの確認等が行われた。[119]

（NCRCG の主な機能）[120]

- 構成員の組織に対してサイバーセキュリティに係るインシデント及び脅威に関する情報を提供
- 国家のサイバーセキュリティマネジメントにおける、予防、準備、インシデント対応、復旧の各段階に対して、脅威分析のサポート及び、戦略的状況認識の提供
- 構成員の組織に対して提供する情報、政策、推奨されるアクション（連邦政府のリソースの配

[118] http://www.computerworld.jp/topics/gov/138129.html
[119] http://www.dhs.gov/xlibrary/assets/prep_cyberstormreport_sep06.pdf
[120] http://www.learningservices.us/pdf/emergency/nrf/nrp_cyberincidentannex.pdf

分方法等）についての取りまとめ
・ 大統領行政府に対する適切な支援

実際に国家にとって重大なインシデントが発生した際には、NCRCG が HSOC と共同で重要情報の共有の調整を行い、DHS、IAIP、NCSD、US-CERT の業務を支援することとなっている。

(a) 情報共有の担保方法・ルール

DHS の監察総監室（OIP）が 2007 年に公表したレポート“Challenges Remain in Securing the Nation’s Cyber Infrastructure”[121]の中で、民間部門が US-CERT から提供される情報の分類や取り扱いに対して懸念を抱いており、US-CERT に対して民間部門への情報提供に際して明確なルールを作ることを求めたのに対し、NCSD 側の回答の中で「2006 年から US-CERT と IT-ISAC は共同で Concept of Operation(仮題)のドラフト作成を進めており、その中で情報共有の、ルールについても定めている」とし、また NCSD の中の Internet Disruption Working Group においても、「情報共有評価関する文書のドラフトを完成させた」としている。該当する文書は 2009 年 4 月時点で未だ公表されていない。

ただし US-CERT のホームページ上には政府機関向けにインシデントレポートに関する簡単なガイドラインとして、Federal Incident Reporting Guidelines[122]が公開されている。この中で、政府機関が US-CERT にインシデントに関する報告をする際に必要となる情報が示されている。

（インシデントレポートに含めるべき内容）
・ 機関名
・ 連絡先（氏名、電話番号、メールアドレス）
・ インシデントカテゴリタイプ（NIST Special Publication 800-61 に準拠）
・ インシデントの発生日時（タイムゾーン）
・ 送信元の IP アドレス、ポート番号、プロトコル
・ 送信先の IP アドレス、ポート番号、プロトコル
・ OS（バージョン、パッチの適用状況含む）
・ システムの機能（DNS/ウェブサーバ、ワークステーション等）
・ アンチウイルスソフトの導入状況（製品名、バージョン、最新のアップデート）
・ インシデントに巻き込まれたシステムの設置場所
・ インシデントの検知方法（IDS、監査による分析、システム管理者による発見等）
・ インシデントの影響範囲
・ インシデントに対して講じた対策

---

[121] http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-48_Jun07.pdf
[122] http://www.us-cert.gov/federal/reportingRequirements.html

(4)国土安全保障オペレーションセンター(HSOC:Homeland Security Operations Center)

米国内の 35 に及ぶ州や連邦政府の司法、情報機関で構成し、テロ攻撃に対する脆弱性の分析や、脅威評価、分析、国土安全保障省への勧告、事件への対応調整等を365日24時間体制で統合的に運用する組織。

2.2.2.2. National CSIRT と ISP の関係

米国の National CSIRT である US-CERT と ISP の間に直接的な協力関係が強調されることはないが、ネットワーク上ボットに感染したホストのアドレス等のデータベース管理上、密接な情報連携がある。実際に FBI が実施するボット対策作戦の Bot Roast においても、US-CERT や CERT-CC がボットに感染した端末情報の特定等の技術的な協力をしている。また US-CERT が属する CS&C の別組織である NCS は ISP を中心に構成される官民連携組織 NCC(Telecom ISAC)を管轄する立場であるため、ここでも情報が共有されていると考える。

また OMB が新たに打ち出している TIC プログラムでは、ISP を含む民間ベンダが Networx としてネットワークサービスの提供を行う。TIC で構築されるネットワークは US-CERT が運用する EINSTEIN 機器との連携が必要となるため、ネットワーク上のトラフィック情報等の共有が図られている。

2.2.2.3. 職員

US-CERT の職員の大半は CERT/CC の職員である。また、US-CERT(CERT/CC)には民間企業から登用されたサイバーセキュリティの専門的知識を持つ人材が多く配置されている。例としてマルウエア解析の部分では、Trend Micro、McAfee 等のセキュリティベンダの人材を配置しており、情報収集の部分では FBI、シークレットサービス、NSA 等の情報機関の職員が常駐して、業務の支援を行っている。

米国では政府の CIO の多くは民間から移籍してきた人材から登用され、IT コンサルティング会社や、企業内の IT 管理、業務プロセス改革の経験者が多いという[123]。また CIO-SP2i のような CIO 業務を支援するための契約プログラムによって、CIO の実務部分を外注する機関も多い。

(CIO-SP2i における CIO 業務サポート)

- 政府機関の IT アーキテクチャ構築のコンサルティング及び開発サポート
- プログラムの解析(費用対効果解析等)
- 省庁の IT 関連予算の資金マネジメント及び管理アプリケーションの開発
- マーケット調査

---

[123] 第 1 回日米 CIO 会議基調講演(全米知事会州情報化プログラムディレクター トム・C・ルーベル氏)
http://itpro.nikkeibp.co.jp/free/NGT/govtech/20050713/164566/?P=2&ST=govtech

・TCO（Total Cost of Ownership）解析
・ステークホルダの分析
・OMB 通達 A-76「民間サービスマネジメント」への[124]対応
・スタッフマネジメント
・IT 組織の構築

一方で、一部からは US-CERT に与えられた任務に対してリソースが十分でないという指摘も出ている。2007 年 10 月に行われた政府の監視と政府改革に関する委員会情報政策・国税調査・ナショナルアーカイブに関する小委員会における IT-ISAC 代表 John T. Sabo 氏の報告では、US-CERT の体制について以下の点が指摘されている。[125]

IT-ISAC 代表 John T. Sabo 氏による US-CERT及び ISAC council に関する報告
①US-CERT の安定性 US-CERT に期待される機能に見合ったリソース（人員、専門知識、予算等）が割り当てられなければ、与えられた役割を果たすことが出来ないとしている。US-CERT の機能はその人員に大きく依存しているため、ディレクターや主要なスタッフを失うことでオペレーションにも影響が出るとしている。 ②US-CERT に対する予算 現在の US-CERT に与えられている予算が US-CERT 全体のミッションに見合ったものとなっているかの検討を行う必要があるとしている。 ③US-CERT と DHS 下の他の分析組織との役割分担と関係の定義 US-CERT と HITRAC 機能の違いが不明確であり、HITRAC には物理的脅威に関する報告機能、ISAC ではサイバー空間の脅威に関する役割を集中させるべきとしている。 ④企業に対する IT-ISAC への加盟の推奨 ⑤ISAC Council に対する PCIS と同様のサポートの実施 13 の ISAC を束ねる ISAC Council としても PCIS と同様に分野間における協力や情報共有、オペレーションに関わる政策等の協議の機会を与えられるべきとしている。ISAC council では緊急時のコミュニケーションや情報共有において具体的なプロジェクトを実施してきた実績があり、これは 2006 年の NIPP で定められた情報／諜報共通の枠組（正式には PCIS がこれに当たるとされている）として DHS のサポートが必要としている。 ⑥ISAC を通した重要インフラ事業者に対する詳細かつ頻繁なブリーフィングの実施

[124] 1996 年に OMB の Office of Federal Procurement Policy (OFPP).から出された通達。2008 年、「競争調達」から「民間サービスマネジメント」に改名された。政府職員の組織と民間の受託業者を競争させることで、調達の効率化を指示している。政府機関が業務プロセスをどのようにリエンジニアリングしていたか、パフォーマンス、コスト、業務効率化について評価が実施される。なお、政府機関は各機関の資源管理室に 2009 年の「民間サービスマネジメント計画」を提出することを求められている。
（http://fcw.com/articles/2008/07/11/competitive-sourcing-gets-a-new-name.aspx）
[125] http://www.surfacetransportationisac.org/SupDocs/Final_Sabo_Testimony_2.pdf

NIPP の中では ISAC 等が特定分野の脅威分析を行うことになっており、DHS 側から重要インフラ事業者に対する定期的なブリーフィングがなされるべきとしている。現状では、DHS は政策立案代表者に対してこのようなブリーフィングを行うことはあっても、重要インフラ事業者を対象としたものを実施していない。例として 2007 年 8 月に開かれた DHS 主催の National Intelligence Estimate に ISAC が招かれなかったことが挙げられている。

⑦IT 分野と通信分野の協力について

2007 Homeland Security Strategy の中で主張されている、IT と通信が融合した National Cyberspace Security Response System の構築に関して、DHS から IT-ISAC の人員提供の打診を受けていることに触れている。

2.3. 重要インフラ防護における情報連携

2.3.1. 政策レベル

米国における重要インフラの取組は過去に PDD63 や HSPD-7 等で示されてきたが、それらを包含した重要インフラ防護に対する国家戦略として 2006 年に国家重要インフラ防護計画（NIPP：National Infrastructure Protection Plan）が策定された。NIPP に基づき、DHS が全体的な調整や推進役となり、各省庁や民間を含めた取組を行っている。

2.3.1.1. 政策・戦略策定

(1)分野間連携モデル（Sector Partnership Model）

NIPP において提言された重要インフラ防護における官民連携体制。重要インフラの分野毎に官民それぞれのカウンシルを設置し、それらが相互に連携しあう分野間連携モデルが示されている。[126]

①Critical Infrastructure Partnership Advisory Council（CIPAC）

分野間連携モデルでは、重要インフラ／重要資産防護に係る官民の情報共有活動に対して法的なフレームワークを提供することで、情報連携の活発化を図っている[127]。具体的には、国土安全保障法の第 871 節に基づいて、CIPAC のメンバ間の情報共有について、連邦政府諮問委員会法（FACA：Federal Advisory Committee Act）[128]における特別な免除を適用するものである。同免除の下では、メンバ間で共有される情報に対して、一般向けの公開が免除され、活発で相互的な情報共有が可能となる。CIPAC のメンバは SCC（②参照）と GCC（③参照）の代表者で構成される[129]。

②Sector Coordinating Councils（SCC）

重要インフラ防護に係る幅広い活動、問題提起に対して分野内で主導的な立場で政府とのコーディネーションを進めることが求められている。SCC のメンバ構成については分野毎に異なるが、企業の大小に関わらず、幅広い関係者を招集することが求められている。

分野間にまたがる問題、また分野間の相互依存性に関しては民間部門の取りまとめを行う

---

[126] http://www.dhs.gov/xlibrary/assets/niac/NIAC_SPMWGReport_Feb06.pdf

[127] http://www.dhs.gov/xlibrary/assets/NIPP_SectorPartnership.pdf

[128] 連邦政府諮問委員会法（FACA：Federal Advisory Committee Act）
1972 年に制定された、省庁に対する外部からの独立した助言機関としての専門諮問委員会の設立・運営と委員の人選方法を定めた法律（FACA データベース：http://www.fido.gov/facadatabase/）。「政府透明法(Government in the Sunshine Act)」や「政府倫理法(Ethics in Government Act)」等、議会が大統領府の活動を監視し、コントロールするために作られた一連の法律の一つである。委員会の会合は原則公開であるが、例外として、「貿易上の秘密事項」、「国家安全保障や外交政策」、「個人のプライバシー」、「省庁人事規則」に関する会合は、非公開ないし部分的非公開にしてもよいこととなっている。しかし、その場合、委員会は会合予定を公示し、会合のどの部分を非公開にするのか、なぜ非公開にするのかを予め明らかにし、議事録や最終答申・勧告を示さなければならない（http://hideyukihirakawa.com/sts_archive/usregsys/05.html 参照）

[129] http://homeland.house.gov/SiteDocuments/20070726123036-42647.pdf

Private Sector Cross-Sector Council（現在は PCIS）が DHS との協力関係の中で連携を行う。2006 年に公表された“SECTOR PARTNERSHIP MODEL IMPLEMENTATION FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL”では SCC の目的及び機能として[130]、①重要インフラの物理／サイバーセキュリティを向上させるための分野横断の活動やイニシアチブを推進すること、②重要インフラ事業者による DHS や他政府機関への支援を促進すること、③重要インフラに関する活動において政府との連携の窓口となることが挙げられている。

（例）Communications Sector Coordinating Council (CSCC)

CSCC は 2005 年に設立された通信分野の SCC。以下に CSCC の持つ機能を示す。ISAC がオペレーション中心の情報連携を行うのに対して、CSCC では構成員の経験や強みを生かした情報連携を行っているのが特徴である。

（CSCC の機能）

- 重要インフラ／資産に係る政策課題の洗い出しや順位づけ、調整
- 物理及びサイバーに係る脅威、脆弱性、インシデントまたそれらに対する防止策やベストプラクティスの共有の促進
- インシデント発生後の対応、復旧、コミュニケーションにおける政策課題の調整

③Government Coordinating Councils（GCC）

民間部門の SCC に対する、政府側のカウンターパートとして機能する。政府、州政府、地方政府に至るまで、様々なレベルにおける政府の代表を兼ねる。省庁間をまたぐような問題については政府の取りまとめを行う Government Cross-Sector Council が調整機能を果たす。

[130] SECTOR PARTNERSHIP MODEL IMPLEMENTATION FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL
http://www.dhs.gov/xlibrary/assets/niac/NIAC_SPMWGReport_Feb06.pdf

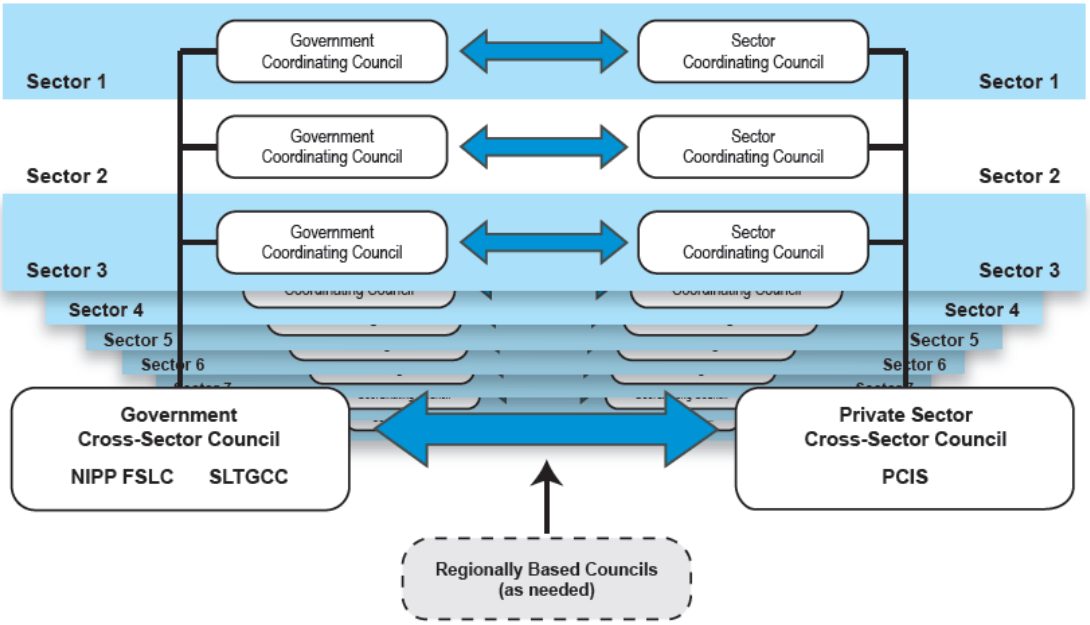


図 2-9 分野間連携モデル[131]

(2)重要インフラ保護パートナーシップ(PCIS:Partnership for Critical Infrastructure Security)

1998 年の PDD63 を受け、1999 年 12 月に米商務長官の進言によって設立された。設立当初は国家計画、研究開発、情報共通、共通ポリシー、オペレーションの 5 つの軸に対して WG を設置し活動を行ってきた。具体的な活動としては、PCII(Protected Critical Infrastructure Information) Program の設立への貢献や"National Strategy to Secure Cyberspace"の民間部門向けのアペンディクス作成への寄与が挙げられる。2006 年に公表された NIPP では分野別の連携モデルの Private Sector Cross-Sector Council として正式に認められている。2006 年以降 Private Sector Cross-Sector Council としての PCIS の主な活動を以下に示す。

(PCIS の活動)

- 分野間の情報共有機能を構築するために民間向けのガイドライン(a guide for the private sector)の作成
- 分野間共通の懸念事項の指摘
  - 演習の計画・調整
  - PCII プログラムの向上
  - 分野間の研究開発や優先事項のギャップに対する解析
- 緊急対応に係る DHS との協力
  - 民間における緊急時対応要員の確保

[131] http://www.dhs.gov/xlibrary/assets/NIPP_SectorPartnership.pdf

- パンデミック対応
- NIPP と SSP の見直し及び実装

(3)The Protected Critical Infrastructure Information (PCII) Program

2002 年重要インフラ情報法によって開始された官民の情報共有を推進するための情報の保護に関するプログラム。民間部門が国家の重要情報に関わる情報を自主的に政府に提供するための枠組となっている。DHS の中に PCII 事務局が設置され、提供された情報の審査や管理を担当している。PCII の活動において民間部門が政府に情報を提供することの利点としては以下の点が挙げられている。

(情報共有における民間部門の利点)[132]

- ビジネス上の機密情報や非公開情報を、重要インフラ防護において同じコミットメントを持つ政府組織間が共有できる。
- 他の重要インフラ事業者と脆弱性やリスクに関する情報を共有することで、自らの組織のリスクを認識できる。
- 重要インフラを防護することで、米国経済に広く影響を与えるインシデントへのセーフガードとなり得る。(2001 年の同時多発テロの際に、経済機能の大半が停止したことを教訓としている)
- 重要インフラ防護の活動に参加、貢献していることが、国民やコミュニティに対してのデモンストレーションとなる。[133]

(a) 情報共有の担保方法・ルール

民間部門から提出された情報に対して、PCII プログラムオフィスでは CII Act(Critical Infrastructure Information Act of 2002)[134] 及び "Procedures for Handling Infrastructure Information; Final Rule ", (6 Code of Federal Regulations Part 29)[135]における連邦情報公開法の適用を免除するための要求事項を満たしているかを判断し、要求を満たす場合は各情報に識別番号が振り当てられる。情報提供要件を満たしていない場合は情報提供者に差し戻される。情報の提出に際しては、以下の書類を提出する必要がある。

---

[132] www.asisonline.org/newsroom/pcii.pdf

[133] プログラムオフィス側が PCII に協力している企業を公表することはなく、あくまで企業側が自らの活動を外側にアピールできる、という意味である。

[134] CII Act:Critical Infrastructure Information Act of 2002
国家安全保障法(Homeland Security Act)の第 II 章のサブタイトル B として 2002 年に成立した。重要インフラの脆弱性や脅威に関して DHS に提供された情報の使用や公開について規定する。

[135] "Procedures for Handling Infrastructure Information; Final Rule" 6 Code of Federal Regulations Part 29 では提供された情報の受付や保管に関する規定を定め、連邦情報公開法(FOIA:Freedom of Information Act)のセクション 214 における情報公開の免除を適用させる。情報公開法セクション 214 には「DHS に対してボランタリーに提供された重要インフラに関する情報は情報公開法の公開義務を免除される」と記載されている。
(http://www.dhs.gov/xlibrary/assets/pcii_final_rule_federal_register9-1-06-2.pdf 参照)

（PCII 活動参加における必要書類）

- CII Act による保護の要求声明
- 認証／承認書
- 提出物の不備が“a violation of 18. U.S.C 1001”によって罰せられる可能性があることへの許諾書

2.3.1.2. システム構築

各分野に設置された ISAC が HP 上で独自に情報共有システム等を展開しているが、元となる情報は DHS（US-CERT）や CERT/CC から提供されている。

重要インフラに対する情報提供は主に国（DHS）によるものと、民間（CERT/CC）によるものが存在する。DHS が主導する重要インフラに対する脆弱性情報の提供は主に ISAC に対するものであり、システムとしては、前述の US-CERT による National Cyber Alert System となる。脆弱性情報提供において、特定の組織を優先するような枠組は公式には存在しない。しかし、実際には ISAC 等に対して、提供する個人を特定した上で非公式に、諜報活動を通じて入手した機密指定されていない機微情報を提供する場合があるとの事である[136]。また、一部の ISAC（Telecom ISAC 等）の、一部のメンバは機密な情報にアクセスするための許可を米国政府から付与されており、このような構成員に対しては、セキュリティレベルに応じた機密情報が提供されている。ただし、このような情報は、ISAC の中で共有されているわけではない。

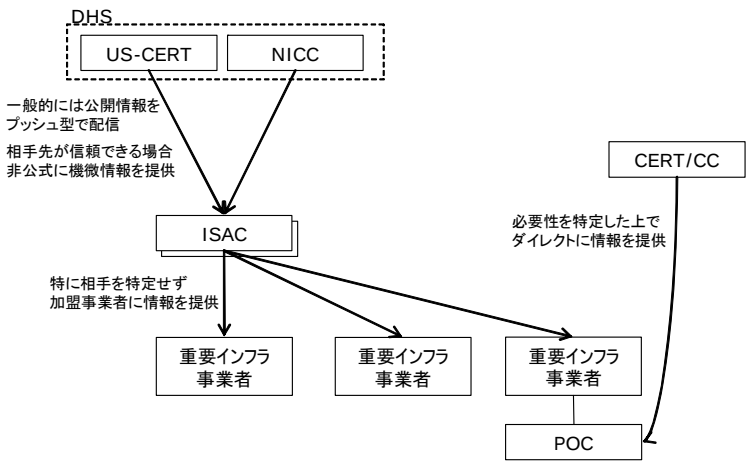


図 2-10 米国における脆弱性情報の優先提供

一方、CERT/CC に関して重要インフラ防護はその業務範囲に含まれないとされているが、実質的な意味で重要インフラ事業者に対する優先的な情報提供を行っている。この場合、情報提供

[136] DHS 及び ISAC に対するヒアリング情報

は、CERT/CC がケース毎に必要性を判断した上で特定の分野の事業者(IT-ISAC 等)の連絡先（Point of Contact （POC））に対して直接に伝達する。この仕組みが有効に機能するためには、

・事業者の連絡先の特定
・事業者がどのような情報（例：特定ルータに関する情報等）を必要としているか を事前に特定しておく必要がある。CERT/CC がこのような仕組みをとる理由は、主に以下の通りである。
・不必要な情報の流通は避けたい（相手先が特定出来ないかつ（または） 必要性のない情報）
・事業者が迅速な対策や回避を行うためには、直接、担当者に連絡出来るパスが必要

従って、CERT/CC は ISAC のような情報共有の枠組では、十分な情報のコントロールが出来ず、また、迅速かつ確実に情報を伝えることが困難であるとの認識を持っている。

2.3.1.3. マネジメント

(1)国家重要インフラ防護計画（NIPP：National Infrastructure Protection Plan ）[137]

2006 年に策定された米国における重要インフラ防護計画。NIPP で示された情報共有体制はこれまでの階層的なものではなく、縦横の情報の交換を可能とするネットワークモデルであり、意思決定機能を分散させている点に特徴がある。このネットワークモデルの目的を以下に示す。

・政府と民間企業の間でセキュアな情報共有を実現することで、無駄なレポートの手間を減らし、情報共有を合理化する。
・全ての重要インフラ防護に関わる関係者（以下、関係者）[138]に対して共通レベルのコミュニケーション、コーディネーション及び情報共有の機能を持たせる。
・関係者に対して、必要な情報共有及びリスク展望、対策を網羅する枠組を提供する。
・関係者に対して脅威、インシデント情報及びベストプラクティス等の包括的な共通手順を提供する。
・関係者に対して適切なタイミングにインシデントの報告及びそのインシデントが重要インフラ・重要資産に与える影響についての情報を付加した形で情報を提供する。
・州政府、地方政府、民間部門を情報循環に組み込むために、情報提供等の役割を与える。
・関係者がそれぞれのリスクを把握し、リスクマネジメントを実施し、セキュリティ対策に資金、リソースを適切に分配するための情報の提供を行う。
・機密情報の完全性、機密性を守る。

---

[137] http://www.fas.org/irp/agency/dhs/nipp.pdf（2006 年版）
http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf（2009 年改訂版）

[138] 重要インフラ防護に関わる関係者（CI/KR partner）には、米国の重要インフラ防護に係わる各組織（DHS、各分野の所管省庁、その他連邦政府機関、州・地方政府機関、各種委員会・評議会、重要インフラ事業者、国土安全保障諮問評議会、教育・研究機関）が含まれる。

図 2-11 NIPP における情報共有に対するアプローチ[139]

(2)重要インフラに関する保護情報の取り扱い説明(Procedures for Handling Protected Critical Infrastructure Information)[140]

Critical Infrastructure Information Act of 2002 の中で規定された、重要インフラに関する提供情報の受け取りや妥当性確認、保存方法等の扱いについて取り決めたルール。州政府や地方機関等全ての政府機関に適用される。

(3)ホワイトハウス"National Strategy for Information Sharing (2007)[141]

国家全体における官民の情報共有に対する戦略文書。基本的に NIPP を踏襲した形であるが、非公開。

(4)CIO-SP2i

NIH の NITAAC が運用する CIO-SP2i の中で連邦政府の IT サービス・ソリューションサービスの業務範囲として重要インフラ防護・情報保証という項目が含まれている。政府機関が有する重

---

[139] NIIP, http://www.dhs.gov/xlibrary/assets/NIPP_InfoSharing.pdf

[140] Final Rule: Procedures for Handling Protected Critical Infrastructure Information http://www.dhs.gov/xlibrary/assets/pcii_final_rule_federal_register9-1-06-2.pdf

[141] http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf.

要インフラの情報システムの分析からインシデント発生時の対応までを、民間事業者に委託できる内容となっている。実際の調達の例を表 2-4 に示す。

（CIO-SP2i の業務範囲 5「重要インフラ防護、情報保証」の具体的業務内容）

- 重要インフラ資産の洗い出し
- 重要インフラ防護の情報保証
- リスクマネジメント
- 重要インフラの事業継続計画策定
- 重要インフラの物理的防護
- 重要システムセキュリティ
- 緊急対応
- 訓練、教育プログラム
- 演習及びシミュレーション
- セキュリティ認証
- 災害復旧
- 暗号システム
- レコードマネジメント
- デジタルライブラリ
- インテリジェント自動データ収集及び解析

表 2-4 重要インフラ防護に関わる CIO-SP2i の利用例[142]

年	発注機関	受注業者	契約件名	契約金額
2008	DOD （陸軍）	SRA International, Inc	Department of the Army (HQDA)Continuity of Operations (COOP) Program Support Task （陸軍のオペレーション継続性プログラム(COOP)のサポート）	$2,650,907.00 （約 2 億 6500 万円）
2007	DHS	Booz-Allen & Hamilton	Cyber Exercise Storm II （サイバーストームIIの実施）	$4,838,822.44 （約 4 億 8388 万円）
2005	DHS	Computer Sciences Corporation/Civil Group	Deployment of Homeland Security Information Network (HSIN) to the Private Sector （HISN の民間部門への整備）	$2,530,372.00 （約 2 億 5303 万円）
2003	DOT[143]	Universal Hi-Tech	Computer System Disaster	$156,592.27

[142] CIO-SP2i を利用した政府機関の調達の内、重要インフラ防護に係わるもの

	（ボルプ全米運輸システムセンター）	Development, Inc	Recovery Services （コンピュータ・システム災害復旧サービス）	（約 1566 万円）

2.3.2. オペレーションレベル

2.3.2.1. 組織

(1)Information Sharing and Analysis Centers (ISACs)

重要インフラの各分野に必要なインシデント、脅威、脆弱性情報を 24 時間体制で確実に提供するための体制。PDD63 の中で ISAC の果たすべき機能の大枠を示されたが、ISAC の詳細な組織体制の在り方については示されなかったため、現在設立されている各 ISAC は基本的な機能は満たされているが、組織の運営体制、ビジネスモデル、資本メカニズム等は各重要インフラ分野によって大きく異なる。また当初、ISAC はサイバーテロに焦点を置いたものであったが、2001 年の同時多発テロ以降、物理テロの重要性を再認識し、ISAC における共有情報は物理的な情報までカバーするように変化してきた。また、ISAC の運用体制に関しても、当初は限定された構成員のみが参加する形態であったものが、会費さえ支払えば誰でも参加出来るオープンな会員制へと多くの ISAC が移行しつつある。会員も会費によってランクが分けられており、ランク別に提供される情報や情報の伝達方法の差別化を図っている。

表 2-5 主な ISAC の機能比較

ISACs	運営体制	共有情報／共有方法
IT-ISAC	非営利の民間団体として設立。ISS[144]が運営を担当する。メンバの勧誘等の広報活動は ITAA[145]によって行われる。会員レベルは無料メンバからプラチナメンバまであり、上位メンバには政府の情報共有政策立案に係る権利（詳細は不明）等の特典が与えられている。（表 2-6 参照）	・一般の情報は IT-ISAC のウェブサイトを通じて行われる。サイバー情報のみならず、事故情報等物理的な脅威についても共有する。 ・メンバ間の情報交換は、一旦 ISS に情報を集約後、匿名化してから共有する ・影響が大きい脆弱性等に関しては IT-ISAC に留まらず、ITAA を通じて広報を行う
ESISAC	電力業界を対象としており、地理的にはカナダもカバーしている。本部は NERC[146]に設置され、費用は全て NERC によって負担されており、メンバの会費は無料。	衛星電話、FAX、メール、ポケベル等を使った情報提供が行われる。詳細な警告情報については会員限定の安全なウェブサイト上で公開される。 物理インシデントに関する情報を中心に DHS に対する報告も積極的に行っている。
REN-ISAC	インディアナ大学、EDUCAUSE、Internet2 を中心として高等教育、研究機関のための ISAC として設立。2007 年 4 月より Microsoft のセキュリティ協	高等教育機関のサイバー空間／物理的脅威を取り扱う。情報の共有方法としては、一般的に公開している統計データや Internet2 Abilene traffic statistics のウェブサイトにおける情報提供に加え関係機関からの提供情

[143] Department of Transportation
[144] Internet Security Systems (ISS、本社・ジョージア州アトランタ)
[145] 米国情報技術協会（ITAA: Information Technology Association of America）
[146] 北米電力信頼度協議会（NERC: North American Electric Reliability Council）

	力制度の下で提携関係を築いている。	報(非公開情報含む)も共有される。共有に際しては情報の分類及び取り扱いについて規定が定められている。
FS-ISAC	民間企業 SAIC が事務局	・機微情報は政府には提供していない ・各社は法律で政府に対する報告義務を負う（DHS に対する報告義務はない）

表 2-6 IT-ISAC のメンバベネフィット一覧[147]

メンバ特典	プラチナ	ゴールド	シルバー	ブロンズ	無料
	$40,000（約 400 万円）	$25,000（約 250 万円）	$10,000（約 100 万円）	$5,000（約 50 万円）	
ウェブサイトにおけるサービス					
最新の脆弱性、ウイルス、ワーム情報へのアクセス	○	○	○	○	
ハッカーの攻撃メトリクス情報へのリアルタイムアクセス	○	○	○	○	
TCP/UDP/ICMP 等のメトリクス情報へのリアルタイムアクセス	○	○	○	○	
IT-ISAC の掲示板へのアクセス	○	○	○	○	
X-Force©のデータベースのサイバーアラート	○	○	○	○	
メンバに対してアラート及び通知を行う権限	○	○	○	○	
メンバが提供する情報へのアクセス	○	○	○	○	
アラート及び e-mail の過去ログアクセス	○	○	○	○	○
IT-ISAC の保護ページへのアクセスのための RSA トークン発行数	15	10	5	3	
一般ページアクセスのための証明書発行数	20	15	10	7	
その他のサービス					
IT－ISAC からの日報メールのアカウント数	15	10	5	5	
暗号化された IT-ISAC のテクニカルメールのアカウント数	10	5	2		
週 2 回のテクニカルミーティング（電話会議）への参加	10	5	2	2	
幹部委員会への参加機会	○	○			
役員就任の機会	○	○			
情報共有に関する政策の関係者との交流の機会	○	○	○		
情報共有に係る政策立案に係る機会	○	○	○		
産業分野における情報共有ポリシー策定に携わる機会	○	○	○		
アラートのカスタマイズ	○	○	○	○	
サイバー及び物理的緊急情報の配信	○	○	○	○	
委員会メンバになる機会	○	○	○	○	
IT-ISAC のチェアとなる機会	○	○	○	○	
毎週ロールアップアセスメントメールの配信	○	○	○	○	○
メールによる IT-ISAC 緊急アラートの配信	○	○	○	○	○

(a) 情報共有の担保方法・ルール

各 ISAC では情報共有に関して独自のルールを設定する。一例として、REN-ISAC における情報共有ポリシー[148]を以下に示す。

[147] https://www.it-isac.org/

[148] http://www.ren-isac.net/docs/information_sharing_policy.html

（参考）REN-ISAC における情報共有ポリシー（2008 年 12 月 19 日版）

（目次）

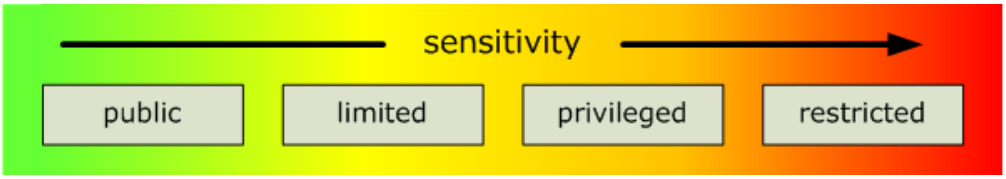
ここでは、3.情報共有の分類及び 9.情報の共有手順について紹介する。

3. 共有情報の分類

カテゴリ	必要条件	目的
機密性	義務	配布範囲の限定
重要度	義務無	緊急性のアピール
信頼性	義務無	反応のタイミングの見極め
ターゲット	義務無	適切な対象者への情報伝達

① 機密性

共有情報は一般利用（public）、限定利用（limited）、特別利用（Privileged）、制限利用（restricted）の 4 段階に分けられる。特別に指定されない場合には Privileged として扱われる。



Public:

レベルとして設定されているだけで、基本的には ISAC の中で共有すべき情報ではない。

Limited:

基本的にはオープンソースから提供される情報だが、悪意のある行為に加担する可能性がない

かの分析が加えられた情報となっている。なお、以下の条件を満たす際には、構成員以外に再配布が認められる。

- 組織のセキュリティ担当者等信頼のおける構成員のみに共有する目的の場合。
- 情報が公的にアクセス可能な環境に置かれないこと（個人的なメーリングリスト等は要注意）。
- 一般公開されていないまたは正当な保護下にない場合には、情報に権限を持たない人の検証が加えられないこと。
- 適当と判断出来れば REN-ISAC のクレジットを出してもよいが、その際に REN-ISAC のチャネル名（メーリングリスト名等）や情報源に関する情報を削除すること。
- 情報共有制限及び免責事項に了承を得ること。

（情報共有制限及び免責事項）
以下の情報は公的に公表されてはいけません。これらの情報はあなたの組織内において情報セキュリティ対策や対応に関係する信頼出来る人のみに共有されるものです。これらの情報を組織内の対策や対応に適用させる際には、情報の正確性に対して一切の保証は行いません。各情報所持者が情報の価値を判断し、それらを使用することのリスクを識別する必要があります。再配布の際には、この文書も一緒に配布されなければなりません。他のいかなる文書も一緒に配布されてはなりません。

Privileged:
REN-ISAC の General 及び Xsec メンバのみに配布される。ただし以下の基準を満たす際には構成員を越えて、当該構成員の組織内で共有することができる。

- 特定の運用の防護や対応の目的のみで共有されること。（状況認識付与や強化等の一般的な目的だけでは共有されることはできない）
- 運用における防護策や脅威の低減をする際に、その情報を知る必要がある人のみに提供されること
- 組織内において最低限必要な情報だけが共有されること。
- 配布されるメンバが信頼するに足る理由があること。
- 一般公開されていないまたは正当な保護下にない場合には、情報に権限を持たない人の検証が加えられないこと。
- 適当と判断出来れば REN-ISAC のクレジットを出してもよいが、その際に REN-ISAC のチャネル名（メーリングリスト名等）や情報源に関する情報を削除すること。
- 情報共有制限及び免責事項に了承を得ること。

Restricted

- REN-ISAC の General 及び Xsec 構成員のみに配布される。ただし以下の基準を満たす際には構成員の組織内で共有することができる。メンバの組織内では共有されることができないた

め、実際の対策、対応策へと落とし込んでから組織内に展開しなければならない。

・ Restricted 情報の内、特定の目的の情報は Xsec メンバより、Referred-Trust Associates に対して共有される可能性がある。

② 重要度

情報の潜在的影響に基づき、対応の迅速性のレベルを示す。

重要度	期待される行動
ルーチン	即時の対応は求められない。一般的に経験される悪意のある行動に対する助言。
重要	特定の攻撃や脆弱性の増加に基づき、特定の脅威に対する対応及び防護を必要とする。
緊急	迅速な行動を必要とする。甚大な影響が想定される情報に付与される。

③ 信頼性

情報のリアルタイム共有を優先して、十分な分析をしていない情報であっても発信出来るようになっている。信頼性のレベルは高い、一般、低い（High, Medium, Low）の 3 段階となっている。

④ ターゲット

情報によって行動や検討を行う人を特定する際に付与される。対象者の例としては、運用／管理層、マネジメント／指揮層、トップ層の 3 段階となっている。

9. 情報の共有手順

① 情報の共有手段は制限されていない。メーリングリスト、IRC、ウェブキャスト、会議電話、対面の会合、Wiki、データフィード、1 対 1 での情報共有等、様々な形態を活用してよい。

② 1 対 1 の情報共有を除いて、各情報共有手段（チャネル）は機密度のカテゴリが定義される。全てのメンバ間で情報を共有する場合は、共有される情報に機微な内容が含まれない場合には Privileged Use と定義される。Privileged Use よりも低い機密性の情報を共有される際も、それらのチャネルを使うことは可能であるが、機密性の低い情報であることが明確に示されていなければならない。

③ 1 対 1 のコミュニケーションの場合、個人的／REN-ISAC の活動の一環であることに関わらず、参加者同士でコミュニケーションのパラメータについて同意を得ることが必要である。

④ 構成員は必要に応じて REN-ISAC に対して、直接的／間接的に帰属が示されていない情報でも提供することが出来る。

⑤ コミュニケーションの手段によらず、メンバは共有する情報の機密性を予め決定するべきである。必要に応じて重要度や信頼性、対象についても示されるべきである。

⑥ 情報の機密性を Privileged 若しくは Restricted と定義する際に考慮すべき点として以下

の点が挙げられる。
－情報を安全に共有するための受取人が必要となる調査の度合い
－情報を安全に共有するための－情報を受け取った組織内での共有範囲
－情報を受け取った人の組織の機能
⑦ 構成員はその判断で提供した情報の分類を低く変更することで、情報の共有範囲を拡大することが出来る。

(2)ISAC-council[149]

2001 年の同時多発テロの際に重要インフラの相互依存性が顕在化したことをきっかけに、2003 年に主要な ISAC によって自主的に設立された。ISAC Council のミッションは、各 ISAC と政府間の相互補完の枠組を策定し、維持することで、北米の重要インフラの物理的及びサイバー上のセキュリティ対策を推進することとしている。

(ISAC Council の機能)

- ISAC 間の問題、特に各 ISAC の運営やその方針に対する調整
- ISAC と政府機関との情報伝達の実現
- オペレーションのデータ等の情報をどのように共有し、また管理するか等といった情報共有のためのプロトコルの開発
- ISAC がそれぞれの分野及び他の分野をサポートするための支援
- 知識やベストプラクティスを抽出し、その情報を広めること

(ISAC Council の具体的活動)

- 各 ISAC と政府機関との情報交換を推進するため、DHS と定期的にミーティングを設けること
- ISAC 間の関係や結びつきを高めるために、各 ISAC の代表者とのミーティングを設けること
- 事例の抽出、またその情報を広めるための討議資料となる白書を作成すること

(IT-ISAC(ISAC Council)と IT-SCC の関係)

ISAC のうち、IT-ISAC は、IT に関する専門的技術力を持つ組織であるため、US-CERT に対する技術的サポートや ISAC Council、分野間連携モデルにおける IT-SCC の活動等分野間の情報連携を担う組織でも中心的な役割を果たしている。

(IT-ISAC が関わっている業務)

- ISAC と US-CERT 間における Concept of Operation の作成
- IT-ISAC ポータルにおけるオペレーションチームによる解析結果の提供
- FS-ISAC と MS-ISAC との間における脅威レベルの関連付け

[149] http://www.hitachi.co.jp/Prod/comp/Secureplaza/sec_trend/ls/is/isac06.html

・ISAC と US-CERT の日時電話会議のホスト、ISAC と US-CERT 間の電話連絡、出版物共有の仲介
・ISAC council 及び IT-SCC のウェブサイトのホスティング及びデータベースの構築
・IT-SCC の主導、IT 分野における情報共有及び分析のメカニズム構築
・サイバーストームへの参加、分析業務の実施及びサイバーストーム II の計画
・ISAC Council の OIIS フレームワークの適用

以下に分野間の情報連携を行う組織として、ここまで紹介した、ISAC Council、PCIS、CIPAC の組織を比較した。

表 2-7 分野間の情報連携を行う組織の比較[150]

	ISAC council	PCIS	CIPAC
メンバ	各 ISAC から 3 名の代表者	SCC の代表者 ISAC Council のチェアも参加	SCC/GCC のメンバ（組織）
目的	コンセンサスの醸成 情報共有（ベストプラクティス、状況レポート等）	分野間のコーディネーション	各分野の重要インフラ事業者と政府のコンセンサスの醸成
スコープ	分野内、分野間のオペレーションに係る問題	分野間のコーディネーション 政策／戦略立案	SSA と DHS に対するコーディネーション及び助言
民／官	民間主導（IT-ISAC）	民間主導（緊急サービス、郵便 SCC は除く）	官／民

Center for Cybersecurity Operations (CCSO)

米国シンクタンクの CSIS(戦略国際問題研究所）がまとめた国家のサイバーセキュリティに関する提言報告書"Securing Cyberspace for the 44th Presidency, Commission on Cybersecurity for the 44th Presidency" において Center for Cybersecurity Operations (CCSO)の設置が提言されている。同報告書の中の提言の幾つかはオバマ政権の中で実際に採用されており、例えば「サイバーセキュリティに関して大統領に直接、助言を行う Cyber Security Chief の設置」という提言に対しては、同様の役割を持つ National Cyber Advisor という役職が新設されている。

CCSO のミッションは重要サイバーインフラに影響するようなオペレーション上の問題を発信することであり、これまでの政府中心の組織とは異なり、政府と企業のジョイントベンチャーのような形を想定している。CCSO の運営は 24 時間 365 日のフルタイム体制とし、人員は政府と民間の両方から提供されるとしている。サイバーセキュリティに係る外部組織や研究機関との連携も重要とされており、特に ISAC とは密接な連携のもと業務を進めるとしている。

(3)InfraGuard

1996 年に開始されたサイバー犯罪分野における民間と学界との連携を目的としたプログラム。1998 年に国家基盤保護センター（NIPC）に吸収されているが、2003 年に NIPC が DHS に吸収さ

[150] http://www.pcis.org/PCISDocuments/PCISPresentationOctober2006-v6.pdf

れた際に、テロ対策とサイバー犯罪における重要なプログラムとして InfraGuard は FBI に残すこととなり、現在まで活動を行っている。現在 Fortune500 企業のうち 350 社が InfraGuard に代表者をメンバとして登録している。メンバは米国全土の 56 の FBI 支局の中に設置されている 80 の InfraGuard 支部の中で活動を行っており、サイバー犯罪が発生した際には事件の関連情報が暗号化されて送信される。現在のところ構成員は米国国民に限られており、個々の構成員については非公表となっている。構成員は InfraGuard に関する情報提供を制限されており、取材等の質問への回答や出版物において InfraGuard の活動について言及する際には事前に許可を取る必要がある。これらは“Interviewing and Publication Policy”というガイドラインに規定されている。[151]

(a) 情報共有の担保方法・ルール

i) InfraGuard Interviewing and Publication Policy（概要）

（共通事項）

- InfraGuard の構成員と FBI 代表者は発表のテーマについて同意を得なければならない。
- InfraGuard の構成員の身元はいかなるときも保護されなければならない。
- 個々の構成員の名前、所属機関はそれら両者の同意を得ずに公開されてはならない。

（質問）

- 全ての質問項目は事前に書面で提示されなければならない。
- 質問項目は InfraGuard のリーダと FBI の地方局の代表者に確認され、回答について同意を得なければならない。また質問を受ける担当者についても適性がチェックされる。
- 可能な場合は FBI 地方局の代表者が同席し、FBI と InfraGuard の協力体制について強調することが望ましい。
- 質問を受けるメンバは回答にあたり、以下の事項を厳守しなければならない。
- シンプルな表現と基本的な事実によって回答し、無関係な内容に誘導されないように InfraGuard のメンバーシップに対して有益な回答をすること。
- 機密情報に関する質問は避けられなければならない。（質問者は回答者の発言を引用する権利があるため）不適切な情報を引き出そうとしている質問には注意を払い、決して質問者と口論してはならない。

（出版物）

どのような資料や出版物であれ、その内容について InfraGuard の地方支部のリーダと FBI の支局の許可を得なければならない。

2.3.2.2. 官民連携体制

米国の重要インフラ防護は ISAC を中心とした官民連携体制の中で推進されているため、民間の活動に対する官側のチェック体制が必要となる。以下に主なチェック体制を示す。

[151] http://infragard.thehandcoders.com/UserFiles/File/Contact%20Us/ipolicy.pdf

(1)DHS

米国の重要インフラ防護の取組全体的指揮をする立場にあり、民間の活動に対しても助言、改善指導を行う。例として 2003 年に食品・農業分野の ISAC に対して行った改善指導がある。

DHS による農業分野への指導、改善命令(Homeland Security Presidential Directive/HSPD-9 (Defense of United States Agriculture and Food)[152]

2003 年 DHS が大統領令 HSPD-9 に基づいて、食品・農業分野の ISAC である Food and Agriculture ISAC(2002 年発足)の体制と情報分析機能の不備を指摘し、その体制の変更を求めた事例である。結果的には DHS インフラ保護室(Office of Infrastructure Protection)の指導の下、食品・農業保護に関する民間 7 分野に対して「Food and Agriculture Sector Coordinating Council」を創設した 。

(2)NIAC (National Infrastructure Assurance Council)

2001 年 10 月の大統領令 13231 によって設立された重要インフラのセキュリティについて、大統領に助言を行う大統領直轄の評議会。全米コーディネータ[153]の推薦に基づき大統領が指名した 30 名の構成員によって構成される。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、特に民間部門との協力が必要とされるものについて、外部の専門家を招聘し、国家戦略形成のための助言を得る。民間部門と政府の情報共有の進展状況についても助言を行う立場にある。

President Committee for Secure Cyberspace

前述の米国シンクタンク CSIS のレポート"Securing Cyberspace for the 44th Presidency", Commission on Cybersecurity for the 44th Presidency" では、サイバーセキュリティにおける官民連携体制への提言の 1 つとして President Committee for Secure Cyberspace の設置が示されている。具体的には既存の National Security and Telecommunications Advisory Committee (NSATAC)及び、NIAC の機能を吸収することが示されている。また、既存の会議のように、政府高官をメンバとするものではなく、重要インフラを所有する企業において適切な人物(go-to person)をメンバとして、連邦政府と民間メンバの信頼関係の中で真の情報共有を実現していくべきだとして主張している。

(3)Government Accountability Office (GAO)

1921 年 Budget and Accounting Act(会計予算法)によって設立された議会からは独立した米国

[152] http://www.dhs.gov/xabout/laws/gc_1217449547663.shtm

[153] National Coordinator for Security, Infrastructure Protection, and Counter-terrorism Presidential Decision: 大統領によって指名され、国内の安全保障、重要インフラ防護、テロ対策に関する行政の調整を行う総責任者。1998 年の Directive No. 63 (PDD-63)によって設置された。

連邦議会の調査実施機関である。2008 年現在 3,150 名のスタッフを抱えており、2008 年の年間予算は 5 億 7,000 万ドル（570 億円）である。どの党派にも属さず、政府がどのように税金を運用したかのチェックを行う。連邦議会の要請に応じて政府の政策や歳出について調査を行う。これまで重要インフラ防護に係る情報連携（特に ISAC の機能）の課題を指摘する報告書を複数公表している。[154]

GAO による ISAC の情報共有機能に対する指摘[155、156]

GAO が ISAC や ISAC council の代表者に対してヒアリングした結果によると ISAC の情報共有においては以下のような課題があると指摘されている。

・企業の重要情報の共有
・Privacy Act による個人情報の取り扱い
・企業の契約及びビジネス情報の情報公開制限
・各ステークホルダ（政府機関、民間企業）の役割
・資金面における ISAC の運営方法

特に、企業の状況の共有に関しては、ISAC に参加する重要インフラ事業者は、反トラスト法、情報公開法、情報開示に伴う様々な影響を懸念し、ISAC に参加する他の重要インフラや事業者政府機関との情報共有に消極的であると指摘している。

[154] http://www.gao.gov/new.items/d04780.pdf（2004 年 7 月）
[155] http://www.gao.gov/new.items/d03173.pdf
[156] http://www.gao.gov/new.items/d04699t.pdf

3. 英国

3.1. 情報連携のフレームワーク

3.1.1. 情報セキュリティ関連組織

情報セキュリティに関わる取組を実施する主な組織は CESG（政府機関向け）、CPNI（重要インフラ向け）、BERR(民間企業向け)と明確な切り分けが行われているが、全ての組織の取組は情報保証（IA：Information Assurance）の考え方を基礎としている。

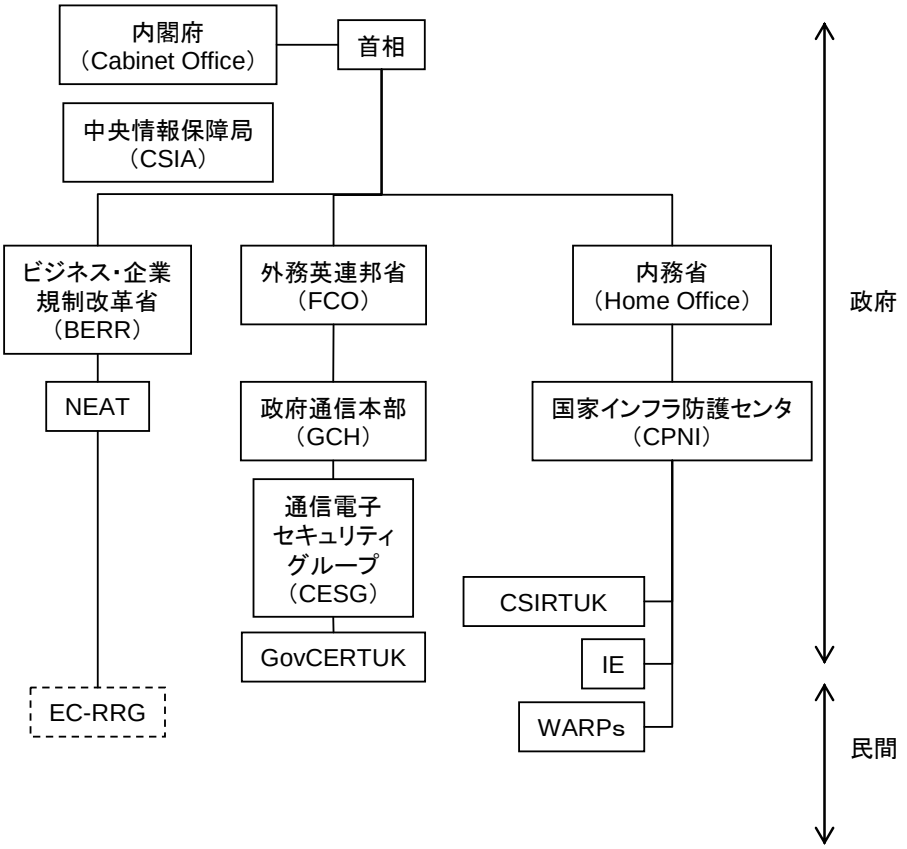


図 3-1 英国情報セキュリティ関連組織

(1)内閣府[157]

政府の戦略策定を行う首相直轄の組織。情報セキュリティに係る組織として内部には以下の組織が設置されている。

・首相戦略ユニット（Prime Minister’s Strategy Unit）

国家戦略の一貫として情報セキュリティに関する方針を策定する。

・情報保証中央局（CSIA: Central Sponsor for Information Assurance）

情報保証（IA: Information Assurance）に関する政策立案、ポリシー策定、民間を含めた英国全体における IA の促進活動等を行う。

・危機計画大学 EPC: Emergency Planning College）

[157] http://www.cabinetoffice.gov.uk/

1989 年より民間緊急事態事務局（CCS：Civil Contingencies Secretariat）内に設置されている。英国政府や政府関係組織における IT セキュリティの専門家を養成するプログラムであり、毎年全省庁から 6,500 名程度の職員が参加する。養成プログラムのコースは、基礎、リスクマネジメント、計画、危機管理、BCM、公共安全等多岐に亘る。

(2)情報保証中央局（CSIA：Central Sponsor for Information Assurance）[158]

内閣府の一組織であり、英国における情報セキュリティの概念である IA に関わる戦略的な方向性の策定と、官民それぞれの組織における IA の活動に対する支援を行っている。 IA に関わる活動を行う他省庁（CESG、CPNI、SOCA 等）と政策の検討において連携を行っている。

(3)通信機器セキュリティグループ(CESG：Communications-Electronics Security Group）[159]

政府通信本部（GCHQ：Government Communications Headquarters）内部の組織であり、情報保証に関する活動を行っている。消費者、企業、安全保障局（MI5）と密接に協力して、政府機関や軍の情報通信システムの重要情報が適切に保護されているかを検証し、政府機関や軍に対してセキュリティについて助言を行う。

(4)英国ビジネス企業規制改革省（BERR： Department for Business, Enterprise & Regulatory Reform）[160]*旧 DTI（貿易産業省）

情報セキュリティの分野では、産業界との緊密で効果的な連携を図ることで、政策の重要分野の競争力を促進する役割を担う。2007 年 6 月のブラウン首相の省庁再編によって、科学・イノベーション庁（OSI）が切り離されると共に、従来は内閣府にあった規制改革担当業務が加えられた。

(5)国家インフラストラクチャ保護局(CPNI：Center for the Protection of National Infrastructure)[161]

英国における重要インフラを、テロ攻撃等をはじめとする脅威から防護し、各インフラの提供するサービスを継続させることを目的としている。具体的な機能としては、CIIP/CIP に関連する部門間調整を行う。各部門から集めた情報を整理し公開することが挙げられている。2007 年 2 月に国家情報インフラ安全調整局（NISCC：National Infrastructure Security Co-ordination Center）と国家セキュリティ顧問局（NSAC：National Security Advice Center）が合併し発足した。CPNI の業務は Security Service Act 1989 に準拠している。

（CPNI の機能の例）

・ 英国の重要インフラに対する脆弱性/情報セキュリティ評価

---

[158] http://www.cabinetoffice.gov.uk/csia.aspx
[159] http://www.cesg.gov.uk/
[160] http://www.berr.gov.uk/
[161] http://www.cpni.gov.uk/

・ 重要インフラ事業者との情報共有及び協力体制の確立
・ 企業における情報セキュリティ意識の向上、ベストプラクティスの提供

(6)英国商務局(OGC:Office of Government Commerce)[162]

IT 製品・サービスを含む政府調達について各省庁に助言し、プロジェクト・プログラムの実施における省庁の能力向上を図る。IT システム、ソリューションの調達は Buying.solution が実施している。2002 年から後述の政府のイントラネット GSi(Government Secure Intranet)計画を推進している。

3.1.2. 法執行機関、防衛機関、情報機関の位置づけ

英国には情報セキュリティに関わる組織が多数あるが、CPNI が情報セキュリティに係る組織の調整を担う組織として機能しており、職員も各省庁(防衛省(Ministry of Defense)、SOCA(Serious Organized Crime Agency)内の e-crime unit 、BERR 等)の出向者であるため、法執行機関及び防衛機関ともに強い連携関係にある。特に National Counter Terrorism Security Office (NaCTSO) は CPNI 内に設置されており、テロ対策の専門家(CTSAs:Counter Terrorism Security Advisers)より、国内のインフラの中で重点的な保護が必要な場所等について助言を受けている。

[162] http://www.ogc.gov.uk/

3.1.3. 情報連携の分類

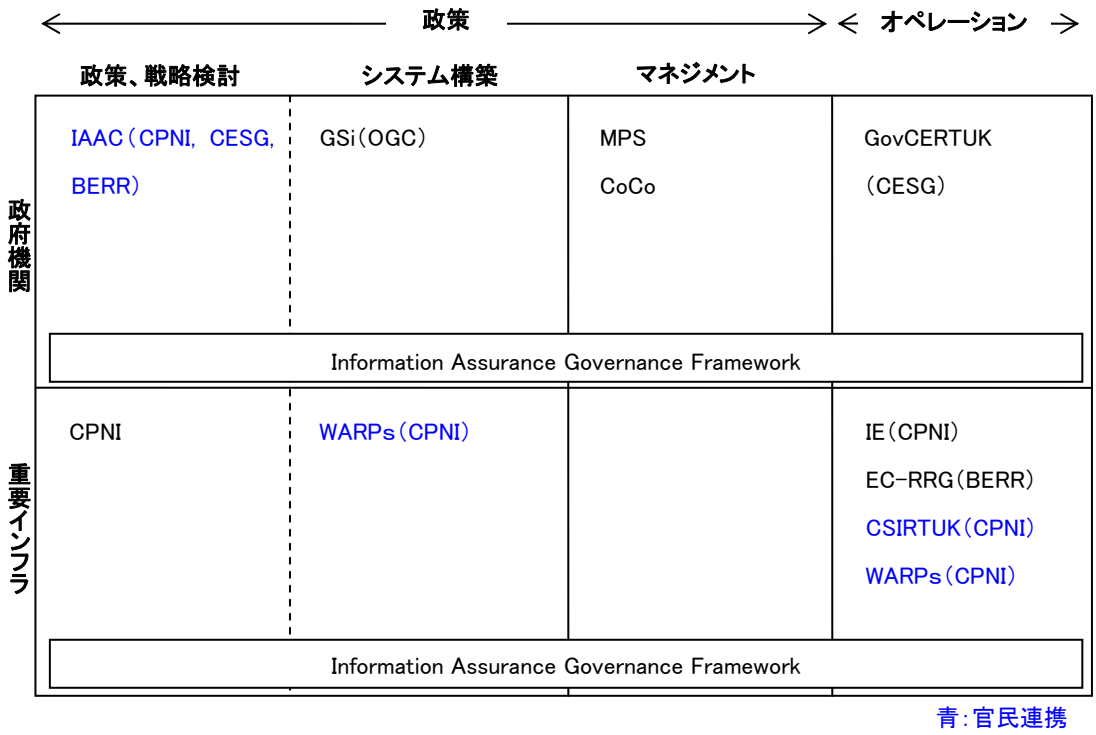


図 3-2 英国における情報連携のフレームワークの分類

3.1.4. 情報連携の関係図

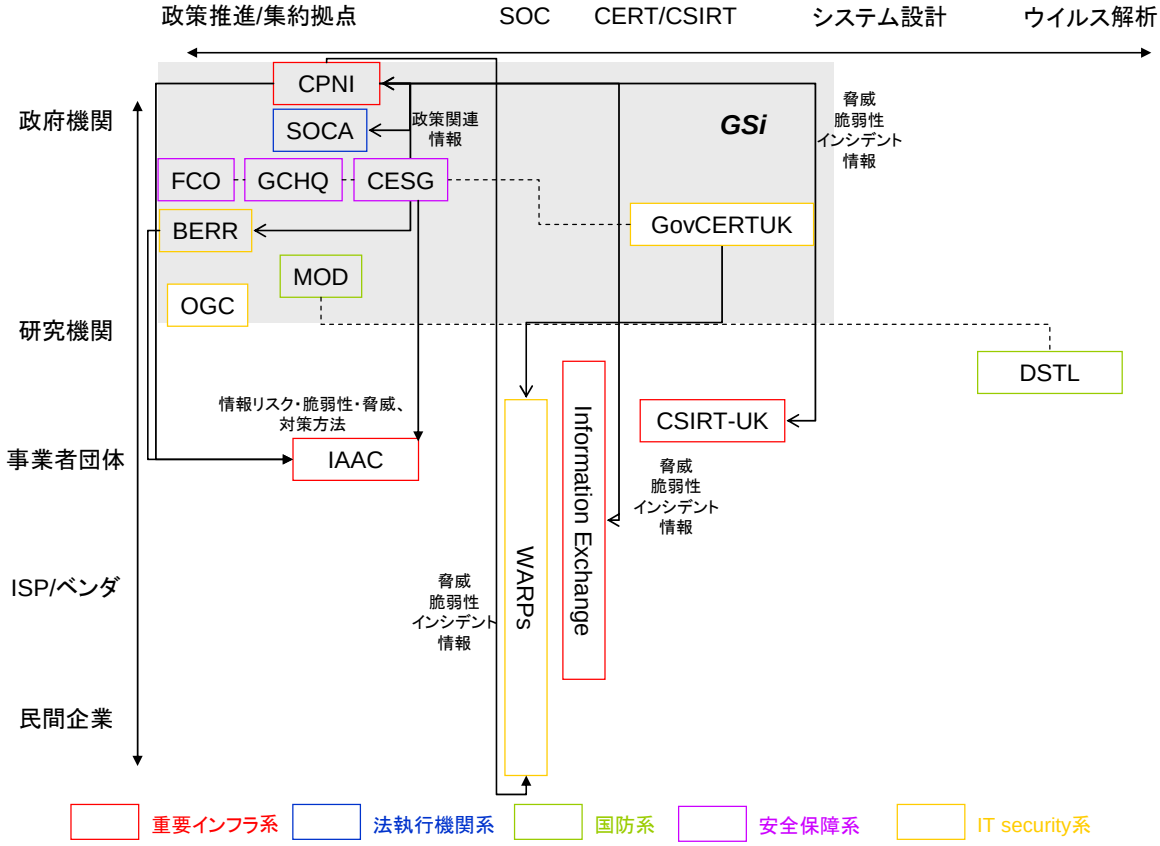


図 3-3 英国における情報連携の関係図

3.2. 政府機関における情報連携

英国における情報セキュリティとは、ISO/IEC17799 に沿って、機密性、完全性、可用性を確保することであり、そのベースとなる情報保証の考え方はこれら 3 つの要素に裏付けされた情報セキュリティを確保することで、情報システムの信頼性を向上させることを目的としている。そのため、政府機関向けの情報セキュリティに関する規定、民間向けの情報セキュリティ普及活動も IA の考え方をベースとしたものになっている。

また、CISA が 2007 年に発表した国家 IA 戦略(National Information Assurance Strategy)[163]の中では、2011 年までに「市民、企業及び政府が、情報システムを利用しその恩恵にあずかることのできる環境を整備すること」というビジョンが掲げられた。このビジョン達成のために以下の 3 つの戦略目標が定められている。

- 政府は ICT を適切に活用することで、より良い公共サービスを提供する。
- 情報及び情報システムをリスクから保護することで、英国国家のセキュリティを強化する。

[163] http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/nia_strategy.pdf

・ 政府、企業及び市民が ICT の利点を理解し、より良い英国経済と社会福祉を実現する。

(1)Information Assurance Governance Framework[164]

英国における IA の考え方や実装のための方策について包括的に纏めた文書であり、政府機関・自治体等の公共部門における IA の導入促進、情報セキュリティ強化を図るための指針となっている。

3.2.2. 政策レベル

3.2.2.1. 政策・戦略検討

政府の情報セキュリティに関する政策の立案及び普及促進はCSIAを中心として、情報セキュリティに係る省庁の間で検討される。また民間企業からなる官民連携組織 IAAC の中でも政策について検討が行われている。

(1)情報保証諮問委員会(IAAC:Information Assurance Advisory Council)

産学官それぞれから資金とメンバを募り 2000 年に設立されたロンドン大学キングスカレッジ内に本部を置く非政府機関。政府からは内閣府、CPNI、CESG 及び BERR が支援を行っている。組織の目標として、公共政策やコーポレートガバナンスと並んで情報リスクや脆弱性、脅威及び、それらに対する対策について構成員内の情報共有と意識啓発が挙げられている。具体的な活動としては、民間部門にサイバー攻撃に関する教育や情報提供を行うプログラム Cyberhoodwatch を CPNI と共同で実施している。信頼性と機密性を保つため、IAAC における議論は一般に公表されていない。[165、166]

3.2.2.2. システム構築

(1)Government Secure Intranet(GSi)[167]

英国商務局 OGCbuying.solutions と民間の ISP(Cable & Wireless UK)の連携によるマネージドネットワークサービス。元々は 1997 年に政府機関のネットワークの相互接続、インターネット接続、メールサービスを提供する枠組として開始された。2004 年から 2009 年の第 2 フェーズではマネージドサービスのコンセプトの下、民間部門も対象とし、情報の機密レベルに合わせたネットワークサービスとして拡大された。現在第 2 フェーズの延長である第 2.5 フェーズとして、英国 ISP 大手の Cable & Wireless がサービスプロバイダとなり運用が行われている。ただし、2012 年 2 月からは外務省が中心となって進める Ocean Programme に統合されることになっている。ちなみに、「GSi」は OGCbuying.solutions が提供するマネージドネットワークサービスの調達の総称であり、個々のネ

[164] http://baobing.googlepages.com/ia_governance_framework.pdf
[165] http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663
[166] http://www.ipa.go.jp/security/fy12/contents/crack/sekitoku/report_USA.pdf
[167] http://online.ogcbuyingsolutions.gov.uk/services/Communications/GSi/

ットワークは、その機密レベル[168]により 5 つのコミュニティに分かれている。(表 3-1 参照)

(GSi が提供するサービス)

- インターネットアクセス
- セキュアメール
- イントラネット(ポータルサイト)
- アンチウイルスサービス
- ファイアーウォール
- リモートアクセス
- ホスティング(シェアードアプリケーションマネージドサービス(SAMS 含む))
- 利用者間の IP 接続
- サポートサービス

表 3-1 GSi の 5 つのコミュニティ

コミュニティ	参加組織とその基準
GSI	RESTRICTED レベルの通信を行う政府機関に提供される。コミュニティへの参加には Manual of Protective Security(MPS)を満たす必要がある。
xGSI	CONFIDENTIAL レベルの情報を共有する政府機関に提供される。GSI と同様に MPS を満たすことが求められる。
GSX	一時的に RESTRICTED レベルまでで保護された情報を収集、格納、処理する必要がある政府機関に提供される。接続されるシステム及びそれらに対するマネジメントプロセスやドキュメントは情報セキュリティポリシー、セキュリティフレームワークのドキュメント、e-Government Security フレームワーク等のビジネス上のベストプラクティスを満たす必要がある。
GCSX	GSX と同様の基準で、主にイギリス雇用年金省の Government Connect に接続するイングリッシュ及びウェールズの地方機関に対して適用される。
GSE	RESTRICTED 及び CONFIDENTIAL レベルにおいて GSi に接続する必要のある民間部門に提供される。官民の共同プロジェクトにおいて政府機関と民間部門、または民間部門どうしで機密情報を共通する必要性がある際に認められる。接続に際しては、後述の Code of Connection (CoCo)と MPS に準拠する必要がある。

[168] 英国の情報の機密レベルは Top Secret、Secret、Confidential、Restricted の 4 段階に分類される。詳細については 71 ページの 3.2.2.3. (1)Manual of Protective Security (MPS)を参照。

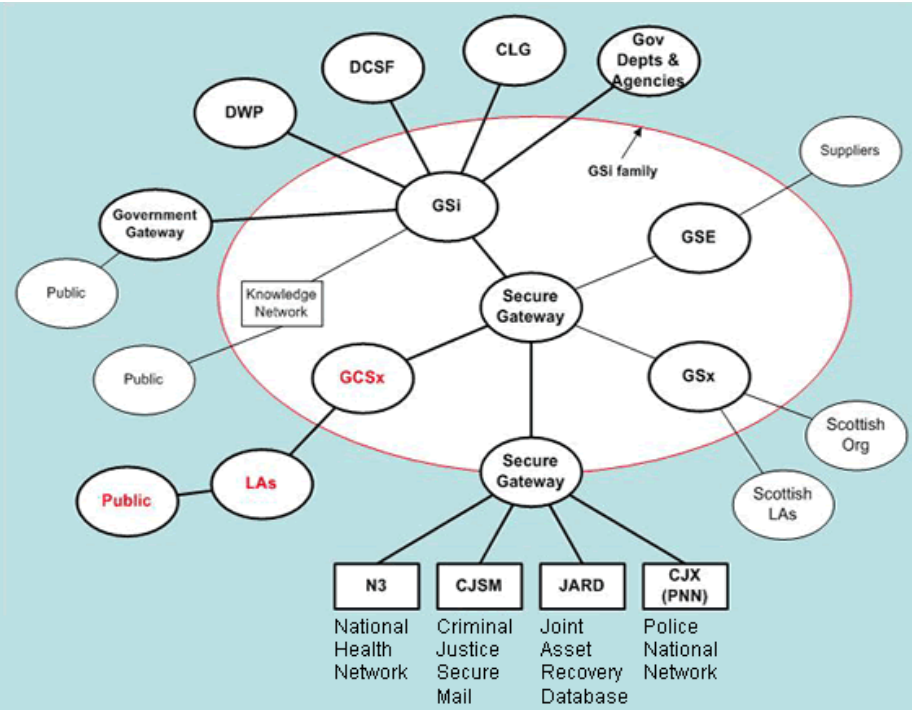


図 3-4 GSi のネットワークの全体図[169]

(2)Ocean Programme[170]

外務省、OGCbuying.solutions、British Council、内閣府、国際開発省、英国年金労働省、英国歳入税関庁、英国国境局が連携して IT コミュニケーション及びソリューションに関する調達を統一化する試み。GSi、Mts[171]、FTN[172]を統合し、新たに以下の 4 つの業務範囲でサービスを提供する。2010 年からの稼動が予定されており、運営は外務省が行う。

（Ocean Programme における業務範囲）

- ネットワークサービス
- ボイスサービス
- ビデオ・データ補助サービス
- サービスマネジメント及び実装

---

169 http://www.govconnect.gov.uk/about.php

170 http://www.fco.gov.uk/en/about-the-fco/working-for-us/contracts-procurement/contracts/ocean-procurement/

171 OGCbuying.solutions と民間企業 Global Crossing によって、民間部門に提供されるマネージドサービス。TDM 固定電話サービスやモビリティサービス、ビデオ会議サービス等を提供しており、民間部門において 22 万のユーザを抱えている。

172 2000 年より外務省と民間企業 Global Crossing によって提供されているグローバル通信サービス。

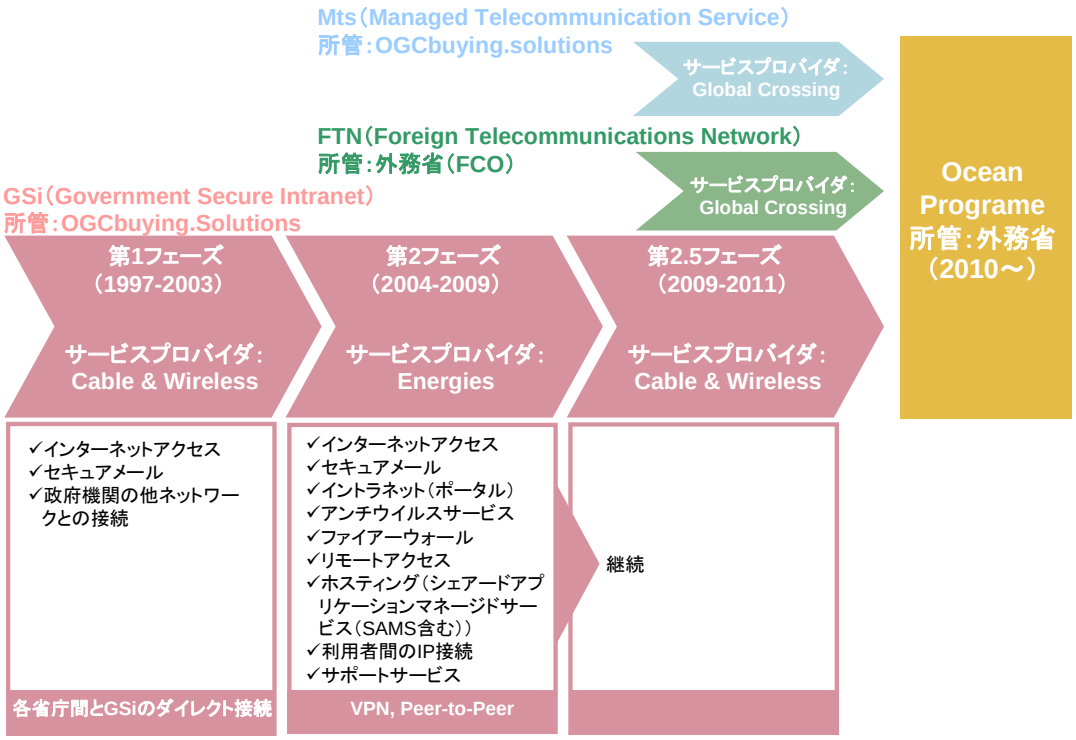


図 3-5 GSi の全体像

3.2.2.3. マネジメント

(1)Manual of Protective Security (MPS)[173]

軍事情報保護法(Officials Secret Act (OSA))に基づいてその詳細を定めた政府の文書。人事選定や機密情報利用許可に関する基準、物理的保管方法、外国政府・企業間での情報交換方法についての規定が示されている。また機密情報取り扱いに関する契約を政府と締結する場合には、MPS に加えて契約内容に固有の情報保全規定が盛り込まれることになっている。

（英国における情報の機密区分）[174]

英国を含めドイツや NATO では以下の 4 段階の機密区分が用いられている。ちなみに、米国では最も低い区分の「Restricted」がない 3 段階の区分となっている。

・ Top Secret

不正な公開によって国家安全保障に「非常に重大なダメージ」を及ぼす可能性のある情報

・ Secret

不正な公開によって国益に「重大な損害」を及ぼす可能性のある情報

・ Confidential

[173] http://www.rosenet.ne.jp/~nb3hoshu/BeiOukigyoHimituho.html

[174] http://badge.lanl.gov/uk-usa_classification.shtml

不正な公開によって国益に「不利な影響」を与える可能性のある情報

・ Restricted

不正な公開によって国益に「望ましくない影響」を与える可能性のある情報

民間人が英国の機密情報の取り扱いを行うためには事前調査で情報取扱者としての資格を受けることが必要となる。上記区分において「Confidential」以下の機密区分情報取扱者の選定は、Security Vetting といった手続きにより、採用対象者の個人情報を企業内で調査を行う必要がある。Security Vetting では、採用に先立ち、親戚・これまでの居住地・国籍・外国との接点・犯罪歴を本人から申告させ、身元保証書を 2 通提出させる。犯罪歴はマイナス要因として考慮される。

「Secret」及び「Top Secret」情報取扱者の選定は政府にて実施され、調査内容は犯罪歴、対テロリストチェックに及ぶ。政府による当該調査は、MI5（英国情報局保安部）により実施され、最長 12 週間を要する。「Top Secret」機密区分情報取扱者の調査は、以上の審査に加え、資産状況の調査と身元保証人の面接が実施され、かなり詳細な点までが確認対象となる。採用対象者の面接も徹底的に行われ、この調査は5ヶ月から6ヶ月を要する。このとき、機密情報取扱者の配偶者が外国人の場合はその点も審査の要素となる。再調査実施間隔は、「Secret」区分の情報取扱者は 10 年毎、「Top Secret」区分の情報取扱者は 7 年毎と設定されている。機密情報取扱資格の付与については、知る必要性（Need to Know）に基づき行われる。例えば、上位に位置する立場の人間であってもアクセス権が付与されない場合がある。国会議員にも自動的に付与されるものではない。また、記者に付与されることはない。[175]

(2)Code of Connection (CoCo)[176]

GSI に接続するために必要な情報セキュリティ要件を定めた規約文書。非公開である。

3.2.3. オペレーションレベル

3.2.3.1. 組織

(1)GovCERTUK[177]

CESG の下に設置された英国政府ネットワークに対する監視及びインシデント対応を行うチーム。CPNI の前組織 NISCC の中に設置されていた Unified Incident reporting and Alert Scheme (UNIRAS)の機能を受け継いでいる。主な業務としては、政府機関内で発生した情報セキュリティインシデントへの対応や、政府機関が管理する情報システム上の脅威や脆弱性に対する助言等が挙げられる。実際の事例として、GovCERTUK はこれまで政府機関の WEB サイトにおける 100

[175] 米欧企業の機密情報保護体制、「新国策」2008 年 2 月 15 日号（国策研究会）
(http://www.rosenet.ne.jp/~nb3hoshu/BeiOukigyoHimituho.html)

[176] http://www.govconnect.gov.uk/implementation/coco.php

[177] http://www.govcertuk.gov.uk/

以上のクロスサイトスクリプティングを指摘している[178]。また、各国の CSIRT やベンダからの提供情報、CESG が独自に行った研究結果を基に、HP 上で警戒情報を提供している[179]。特に CESG の研究結果については独自でテクニカルレポートを纏めており、HP 上で一般に公開している。インシデントが発生した政府機関では、組織のネットワークサポートマネージャまたは ICT プロジェクト及びネットワークサポート技術者によって、GovCERTUK に報告を行う。第 1 連絡は電話で、インシデント報告書様式にインシデントの詳細内容を記入し、メール添付で incidents@govcertuk.gov.uk まで送付する。GovCERTUK で取り扱うインシデントとしては以下のものを想定している。

（GovCERTUK で取り扱うインシデント）

- 不正アクセス
- DDoS
- マリシャスアクティビティ（阻止されたもの、被害を受けたもの両方）
- その他の攻撃

（GovCERTUK で提供しているテクニカルレポート）

- SQL インジェクション[180]

SQL インジェクションに用いられる主要なテクニックについて紹介した上で、それらの攻撃の防御策を紹介している。加えて、ログ管理やセキュアなコーディング等の一般的な対策に関するベストプラクティスも提供する。

- クロスサイトスクリプティング技術とリスク緩和[181]

クロスサイトスクリプティングの脆弱性の一般的な知識、この脆弱性によってどのようにウェブサイトが悪用されるか、組織としてどのような防止策をとるべきか、について紹介する。

- マリシャスコードが含まれる可能性があるファイルの取り扱い[182]

統計的にマリシャスコードが含まれる可能性のあるデータファイルのタイプや、それらへの対処法について紹介する。

(a) 情報共有の担保方法・ルール

GovCERTUK に送付するためのインシデント報告の様式が用意されており（図 3-6）、政府機関の職員は様式に記入の上、メールで専用メールアドレスに送付するルールとなっている。

---

178 http://ezine.ogcbuyingsolutions.gov.uk/ezines/gsi/2008-02/govCertUK.html
179 http://www.govcertuk.gov.uk/alerts.shtml
180 http://www.govcertuk.gov.uk/pdfs/sql_injection.pdf
181 http://www.govcertuk.gov.uk/pdfs/govcert_xss.pdf
182 http://www.govcertuk.gov.uk/pdfs/possible_malicious_content.pdf

GovCertUK Incident Report

General Information	
Reported By:	Date/Time Detected:
Department:	Date/Time Reported:
Title:	Mobile:
Phone:	Fax:
Email Address:	Additional Information:
Postal Address:	
Incident Details	
Type of Incident:	
Status of the Department (total failure, business as usual etc):	Classification of affected System:
Incident Details:	
Site Details:	Site Point of Contact:
Actions Taken:	

図 3-6 インシデントレポート様式(テンプレート)[183]

3.2.3.2. National CSIRT と ISP の関係

英国の政府機関では、民間企業(現在は Cables & Wireless)が運用する政府イントラネット GSi において提供されるマネージドサービスの中で、基本的なセキュリティが確保されている。それらサービスで対応できないインシデントに対しては、政府機関の職員からの報告を受けて GovCERTUK で対応される。

3.2.3.3. 職員

CPNI は情報セキュリティに係る各省庁からの出向者によって運営されている。具体的には、その他、CPNI で政府機関職員に対するセキュリティ専門家育成プログラムが整備されている。

[183] http://www.govcertuk.gov.uk/incident_report.doc

3.3. 重要インフラ防護における情報連携

英国では重要インフラの防護においても、情報保証の考え方に基づき各重要インフラ分野に情報セキュリティレベルの向上が最も重要であると考えられており、その取組も重要インフラの事業者を中心とした民間部門に対して、情報セキュリティ文化を広めることに重きが置かれている。[184] そのため、分野別に設置された IE における情報連携、中小企業を対象とした WARPs の構築にも力を入れて取組んでいる。

3.3.1. 政策レベル

重要インフラ防護に関する取組は CPNI を中心に、民間に関わる部分については BERR や CESG 等の機関と連携した取組が進められている。重要インフラ防護についても、基本的には IA の考え方を基礎としたしており、IE や WARP 等で技術的な情報を共有するだけではなく、民間企業のセキュリティ対策強化のためのガイドラインや評価ツール等の提供や、情報セキュリティに関わる普及啓発活動も積極的に行っている。

3.3.1.1. 政策・戦略検討

重要インフラ防護に関わる政策は CPNI を中心に進められるが、CPNI 自体が情報セキュリティに関わる各政府機関の人材を集めて構成された省庁横断的組織であり、情報連携の場と言える。[185]

3.3.1.2. システム構築

重要インフラ防護に関わるシステムとして WAPRs のシステム構築が挙げられる。詳細については 3.3.2 オペレーションレベル（3）WARPs の項を参照。

3.3.1.3. マネジメント

重要インフラ防護のための情報共有に関して具体的な規定を定めたものはないが、2004 年に制定された民間緊急事態法では、カテゴリ 1 及びカテゴリ 2 という業種区分に分類された民間企業は緊急事態発生時に情報提供の義務を課されることになっている。

また民間企業の情報セキュリティ対策向上を目的として CPNI、BERR、CESG それぞれにおいて情報セキュリティ対策強化のためのガイドラインが公表されている。

(1)民間緊急事態法（CCA：Civil Contingencies Act)[186、187]

英国における戦争、テロ攻撃から自然災害、伝染病まで多様な緊急事態に対応する包括的枠

---

[184] http://www.olis.oecd.org/olis/2006doc.nsf/linkto/dsti-iccp-reg(2006)15-final
[185] 63 ページ、CPNI の項参照
[186] http://www.opsi.gov.uk/acts/acts2004/ukpga_20040036_en_1
[187] http://www.ndl.go.jp/jp/data/publication/legis/223/022301.pdf

組みの構築を目的とする法律として 2004 年に制定された。3 部構成になっており、第 1 部では地方自治体等に対して課される市民保護の義務について、第 2 部ではより大規模な緊急事態に対応して中央政府に与えられる権限について、第 3 部では施行や適用範囲を示している。同法では緊急事態管理に携わる組織を、それぞれの役割の重要度に応じて、以下のようにカテゴリ1と2に分類しており、同法に関するガイダンスの中では、カテゴリ 1、2 に属する機関同士での情報共有が推奨されている。[188]

なお、英国では 2001 年には内閣府の下に民間緊急事態管理局(CCS : Civil Contingency Secretariat)が設置されており、災害、テロ、パンデミック等の健康被害、産業分野の事故や障害(システム障害も含む)の情報管理を行っている。これらの緊急事態に関する情報は UK Resilience homepage で公開されている。[189]

(英国民間救急事態法におけるカテゴリ 1 及びカテゴリ 2 に分類される組織)[190]

カテゴリ 1

- 中央・地方政府(地方政府、中央政府環境局、海上保安局)
- 緊急事態管理サービス(警察、交通警察、消防局、救急サービス)
- 国民保険サービス(プライマリケアサービス、健康保護局、病院、海上衛生局)

カテゴリ 2

- 公共事業(電力、ガス、水道、公共通信)
- 運輸・交通(電車、貨物・旅客輸送、ロンドン交通局、ロンドン市地下鉄、空港、港、高速道路)
- 政府(保険安全局)

3.3.2. オペレーションレベル

3.3.2.1. 組織

(1)CSIRTUK

重要インフラに係る、脅威・脆弱性・インシデント情報を収集・分析し注意情報を配信する。Gov CERTUK が政府ネットワークのみを対象とするのに対し、CSIRTUK では民間部門との調整が必要となる事案を扱う。CSIRTUK で収集された情報は基本的に機密扱いとなるが、個人や企業を特定する情報を除いた形でセキュリティに関する注意として重要インフラ事業者に配信されることもある。

(2)Information Exchange(IE)[191]

特定の分野において設置されている脅威、インシデント、脆弱性情報を交換する非公開のフレ

---

[188] http://www.cabinetoffice.gov.uk/ukresilience/preparedness/informationsharing.aspx
[189] http://www.cabinetoffice.gov.uk/ukresilience.aspx
[190] http://www.opsi.gov.uk/acts/acts2004/ukpga_20040036_en_1
[191] http://www.cpni.gov.uk/products/information.aspx

ームワーク。メンバ間の個人的な信頼関係にベースを置いており、情報共有は非公開のミーティングによって行われる。なお、このミーティングには原則全員参加、代理不可というルールになっている。各 IE には CPNI から議長が配置される。

表 3-2 現在設置されている IE

IE（設立年）	メンバ	共有情報
ADMIE（2006） （Aerospace and Defense Manufacturer's Information Exchange）	英国の宇宙、防衛分野関係組織	宇宙、防衛分野における脅威情報
FSIE（2003） （UK Financial Services Information Exchange）	銀行、保険、証券サービス事業者及び CPNI	金融分野における脅威、脆弱性、対策情報
MSPIE （Managed Service Providers Information Exchange）	英国の重要インフラに IT サービスを提供する事業者	サイバー空間における脅威、脆弱性、インシデントや攻撃情報（重要インフラのステークホルダを含めたメンバ内で共有）
NSIE（2003） （UK Network Security Information Exchange）	IP 事業者、携帯電話・PHS 事業者、通信事業者及び CPNI（英国の 80%以上の通信事業者）	情報通信分野の機密情報
PIIE（2006） （Pharmaceutical Industries Information Exchange）	製薬会社	製薬分野における脅威、脆弱性、インシデント情報
SCSIE（2003） （SCADA and Control Systems Information Exchange）	SACADA システムを利用する企業	SCADA システムやその関連プロセスにおける脆弱性、脅威情報
E-SCSIE (European SCADA and Control Systems Information Exchange)	SACADA システムを利用する企業	SCADA システムやその関連プロセスにおける脆弱性、脅威情報
TSIE（2006） （Transport Sector Information Exchange）	ICT 企業	ICT 産業における脆弱性、脅威
SRIE（2006） （Security Researchers Information Exchange）	ペネトレーション・テスト及び研究部門	ペネトレーション・テスト及び研究部門における脅威情報
VSIE(2005) （Vendor Security Information Exchange）	IT ベンダ	ICT 産業に関わる情報セキュリティ上の脅威

(a) 情報共有の担保方法・ルール

IE における共有情報は基本的に非公開扱いとなる。さらに、メンバは他のメンバの同意を得ない限りは会合で知り得た情報を外に漏らしてはならないという内容のメンバーシップガイドラインに署名する必要がある。[192]

[192] http://www.cpni.gov.uk/Docs/re-20040601-00395.pdf

(3)WARPs[193]

CPNI によって運営されているシステムの脅威/脆弱性情報を提供する枠組であり、現在 19 の WARPsが存在している。英国では政府機関レベルでは GovCERTUK 等の CSIRT 組織が重要インフラ防護の中心的役割を果たしているが、民間企業の多くでは CSIRT 組織を構築するコストや技術がないため、CSIRT の代替組織として中小企業でも実装可能な WARPs のシステムが構築された。各 WARP では 1～2 名の運営責任者が設置され、CPNI 等から提供される情報を構成員に対して配信する。なお、提供される情報自体に各 WARP が事前に設定したフィルタリングがなされており、コミュニティにあった情報が優先的に提供される仕組みとなっている。WARPsが提供する 3 つの主要サービスを以下に示す。

（WARPs が提供する主要サービス）

① Filtered Warning Service

メンバが必要とされる情報がフィルタリングされて提供されるサービス。メンバは配布されたソフトウエアを使って、自由にフィルタ条件を変えることができる。またメンバが独自に作成したツールを他のメンバに提供することもできる。

② Advice Brokering Service

オンラインの掲示板を使った対話型のセキュリティに関する情報共有環境。掲示板に挙げられた情報から、関係のあるメンバを招待したり、機微な情報を取り除いた上で、FWS において構成員に展開したりすることが出来る。

③ Trusted Sharing Service

匿名を原則として、機密情報（インシデント経験等）を共有するための環境。

表 3-3 現在設置されている WARPs

公共サービス			
名前	設立	概要	ステイタス
DSWARP	2006 年 6 月	シドマス大学によってデボンの教育機関のテクニカルスタッフによって構築された WARP。現在は範囲を広げて活動を行っている。	オペレーション：準備中 フィルタ登録：準備中
MODWARP	2008 年 1 月	23 のサブ WARP から集められた情報保証及び、コンピュータネットワーク防護に係る情報を集める。	オペレーション：開始
NWEWARP	2006 年 1 月	北西地域の緊急情報提供サービス	オペレーション：準備中 フィルタ登録：準備中
PolWARP	2005 年 1 月	PITO によって提供される警察用 WARP	オペレーション：開始
地方自治			
名前	設立	概要	ステイタス
EMGWARP	2006 年 6 月	イングランド東中部地方の行政機関のための WARP	オペレーション：開始 フィルタ登録：開始

[193] http://www.warp.gov.uk/Index/%20indexfaq.htm

LCWARP	2003 年 4 月	ロンドン自治区の情報セキュリティに係る情報のための WARP	オペレーション：準備中 フィルタ登録：準備中
NWGWARP	206 年 4 月	北西地方の行政機関のための WARP	オペレーション：開始 フィルタ登録：開始
SWWARP	2007 年 5 月	南西地方の行政機関のための WARP	オペレーション：開始 フィルタ登録：開始
WMCWARP	2006 年 9 月	ウエストミッドランド地方の行政機関のための WARP	オペレーション：開始 フィルタ登録：開始
ビジネス			
名前	設立	概要	ステイタス
ANSWARP	2005 年 11 月	Anite Swift software 社のユーザのための WARP	オペレーション：開始 フィルタ登録：開始
AVWARP	2008 年 10 月	マルウエア対策の研究者のための WARP	オペレーション：準備中
BTRWARP	2006 年 2 月	BT(British Telecom) 内の WARP	オペレーション：準備中 フィルタ登録：準備中
LS1WARP	2008 年 2 月	ロンドンの Law Society のための WARP	オペレーション：開始 フィルタ登録：開始
PENWARP	2007 年 9 月	ジャーナリストのための WARP	オペレーション：開始
SECWARP	2008 年 11 月	様々な分野のセキュリティの専門家ための WARP	オペレーション：開始
ボランティア			
名前	設立	概要	ステイタス
GUWARP	2004 年 6 月	Genealogy Society のための WARP	オペレーション：開始
RAYWARP	2006 年 4 月	アマチュア無線用の非常ネットワーク	オペレーション：開始
ボランティア			
名前	設立	概要	ステイタス
HIWARP	2007 年 5 月	日立の HIRT による WARP	オペレーション：準備中 フィルタ登録：準備中
IE1WARP	2008 年 2 月	アイルランドの中小企業向け WARP	オペレーション：開始 フィルタ登録：開始

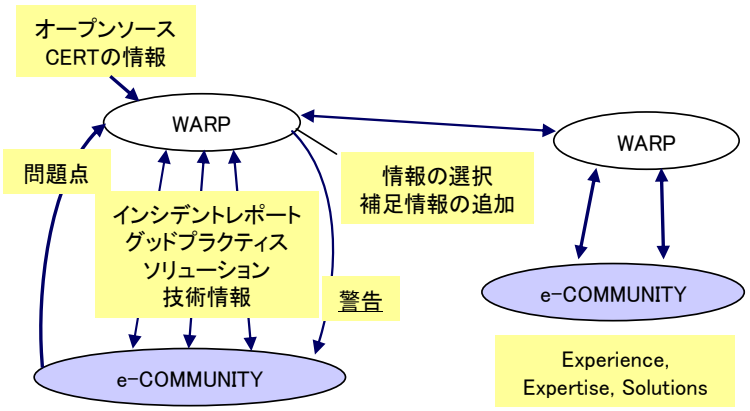


図 3-7 WARPsにおける情報の流れ

(a) 情報共有の担保方法・ルール

WARPs の活動では、参加に際して Code of Practice[194]（第 3 版 2008 年 10 月改訂）に同意することが求められる。Code of Practice では情報共有に対して「守秘性と匿名性を原則としつつ、WARP メンバ、CPNI、他の WARP にとって有益な情報は共有することが推奨される」としている。

(4)Electronic Communications Resilience and Response Group (EC-RRG)[195]

BERR の組織である National Emergency Alerting for Telecommunications (NEAT)の中に設立された、英国内のネットワーク障害における官民連携体制の構築と障害時の対応計画の検討を目的としたグループ。政府側からは CSIA、BERR、CPNI、Ofcom 等から代表者が参加し議長は CSIA から選出される。民間側からは ISP を含む通信関連の企業が参加しており、民間緊急事態法及び ISO27011 を基礎とした検討を進めているが、具体的な枠組はまだ整備されていない。ただし、将来何らかの組織が設置された際には、民間の ISP（国内シェア 10%以上）等でオペレーションの経験がある人物を Qualifying Operators として登用することとしている。

（Qualifying Operators の要件）

- 民間の通信利用者に対してダイヤルトーン、若しくはそれに近いサービスを提供するオペレータ
- 緊急サービスオペレーティングサービスを提供しているオペレータ
- 当局や重要インフラ（例：銀行業務、鉄道、ガスまたは電力）、他の分野で電子通信サービスを使用に提供しているオペレータ
- 放送ネットワークにおいてトランスミッターと通信のリンクを提供するオペレータ
- 一般のインターネットサービスのオペレータ
- 市場占有率 10%以上の会社のオペレータ
- そのほか主要な通信サービスのオペレータ

ECRRG は 75 ページで示した民間緊急事態法をベースとした活動であり、通信分野だけでなく同法においてカテゴリ 1 及びカテゴリ 2 に指定された事業分野においても、緊急時の対応計画を策定することを目的に、それぞれ RRG の取組が進められている。図 3-8 に示すように、現在パンデミックや、2012 年ロンドンオリンピック等の分野に RRG が設置されているが、実際の活動状況は報告されておらず、ECRRG が先行して取組を進めている状況にある。[196]

[194] http://www.warp.gov.uk/BusinessCase/CodeofPracticeV3.0.pdf
[195] http://www.cabinetoffice.gov.uk/media/131474/telecoms_ec-rrg_tor_101108.pdf
[196] http://www.gose.gov.uk/497648/docs/264757/telecomsSeminarGovIndust.ppt

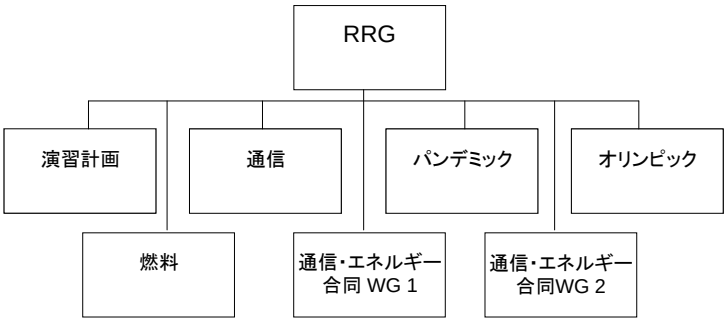


図 3-8 RRG の設置分野

3.3.2.2. 官民連携体制

米国の ISAC の活動は民間主導で実施されるのに対し、英国における官民連携体制は政府機関が主導となる。例えばIE の活動においては民間からは重要インフラ事業者の代表者、官側からは CPNI の担当者が参加し脆弱性情報や研究結果ベストプラクティス等を共有するが、IE 間の情報共有に関しては CPNI がシステムの脆弱性に関する情報の取りまとめ、公開判断等のコントロールを行っている。

4. ドイツ

4.1. 情報連携のフレームワーク

4.1.1. 情報セキュリティ関連組織

ドイツにおける情報セキュリティに関わる取組は BSI を中心として進められる。また、ドイツにおける重要インフラ防護は情報セキュリティだけでなく、テロ対策や国家安全保障の観点も含めた取組となっているため、BKA や BBK との連携の中で進められる部分も多い。そのため、2006 年に公表された“National Plan for Information Infrastructure Protection Plan（NPSI）”の中では重要インフラ防護に関する方針だけでなく、政府機関の情報セキュリティ対策に関する方針も示されている。

政府機関のセキュリティ、重要インフラ防護ともに、実際のオペレーションは各組織の CSIRT を中心に行われる。ドイツでは、BSI に設置された CERT-Bund を中心として 40 以上存在する公共及び民間の CSIRT 組織が整備されており、それらの連携を目的とした CERT-Network が国内の主な情報連携モデルとなっている。

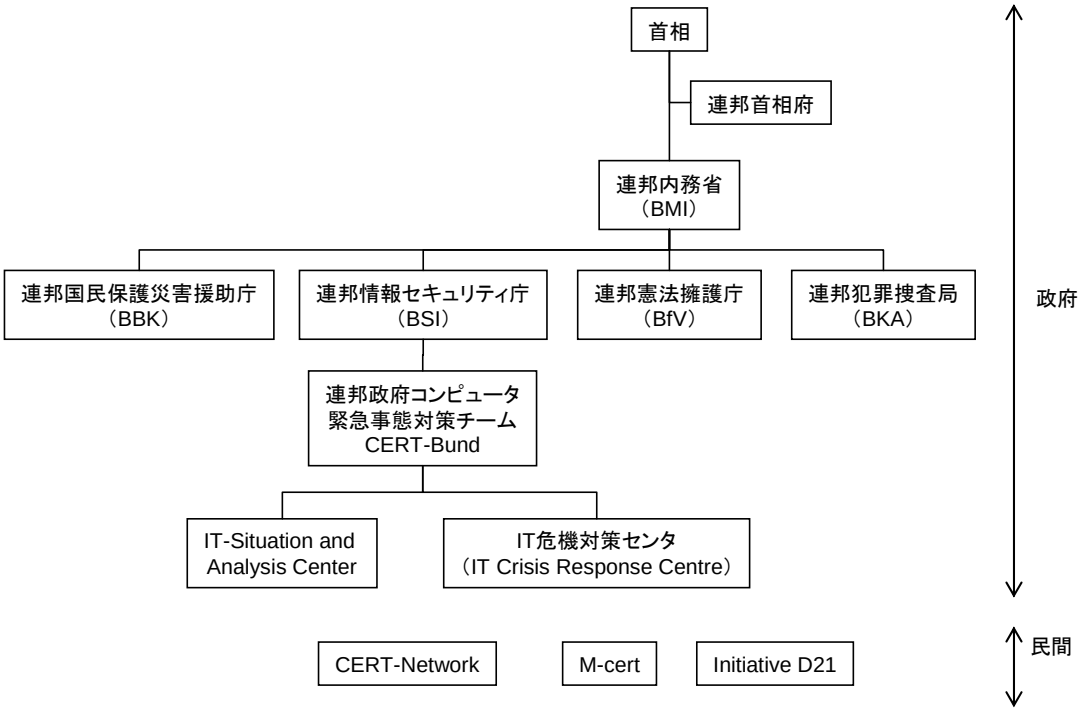


図 4-1 ドイツ情報セキュリティ関連組織

(1)連邦内務省（BMI：Federal Ministry of the Interior）[197]

国内の治安維持を役割としており、連邦全体及び複数の省庁にまたがる情報セキュリティ事案の取りまとめ役として機能している。

197

http://www.bmi.bund.de/cln_145/sid_4742CD00258EDA71850B0E3FF6A2275B/DE/Home/startseite_node.html

(2)連邦情報セキュリティ庁(BSI:Federal Office for Information Security)[198]

1990 年に BSI の設立に関する法律 (BSIG of 17 December 1990)が制定され、BMI 下に設置された。国家レベルにおける情報セキュリティの専門組織であり、暗号を含む IT セキュリティに係るあらゆる研究・開発・普及・啓発・標準の策定やその評価・認証等を行う専門組織である。年間の予算は 5,100 万ユーロ(約 66 億円)[199]でコンピュータの専門家や、技術者等 430 人のスタッフを抱える。

(3)連邦憲法擁護庁(BfV:Bundesamt für Verfassungsschutz)[200]

BMI 管轄の諜報機関であり、国内の極右及び極左の監視、機密情報の管理、要人警護等を行う。BfV の収集する情報の 80%は公開情報である。国家安全保障に対する差し迫った危険を予防・除去する目的で、国内の電気通信の監視、記録を行う権限を与えられている。

(4)連邦犯罪捜査局(BKA:Bundeskriminalamt)[201]

BMI 管轄の犯罪捜査を行う組織。ドイツでは犯罪捜査は各州警察が行うため、主要な業務として州警察と連邦政府との調整を行う。

4.1.2. 法執行機関、防衛機関、情報機関の位置づけ

ドイツで政府機関における情報セキュリティや重要インフラ防護において中心となる組織は BSI である。ただし、図 4-2 に示すように、ITセキュリティ、テロ対策、国家安全保障の業務等は単純に切り分けられないものとされており、IT セキュリティは BSI、国家安全保障は BBK、テロ対策は BKA 等の法執行機関を中心に機能しつつ、各機関の密接な連携が必須となっている。特に BSI と BKA はどちらも BMI 直轄の組織であり、テロ対策の部分等において協力体制をとることが多い。

198 http://www.bsi.de/english/index.htm
199 1 ユーロ=130 円で計算
200 http://www.verfassungsschutz.de/en/index_en.html
201 http://www.bka.de/

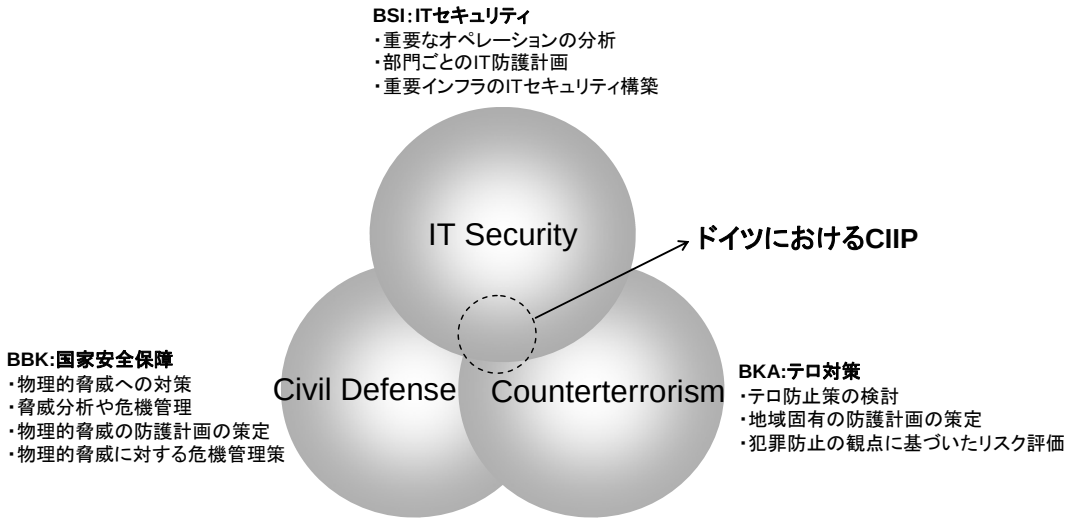


図 4-2 ドイツにおける CIIP の位置づけ

4.1.3. 情報連携の分類

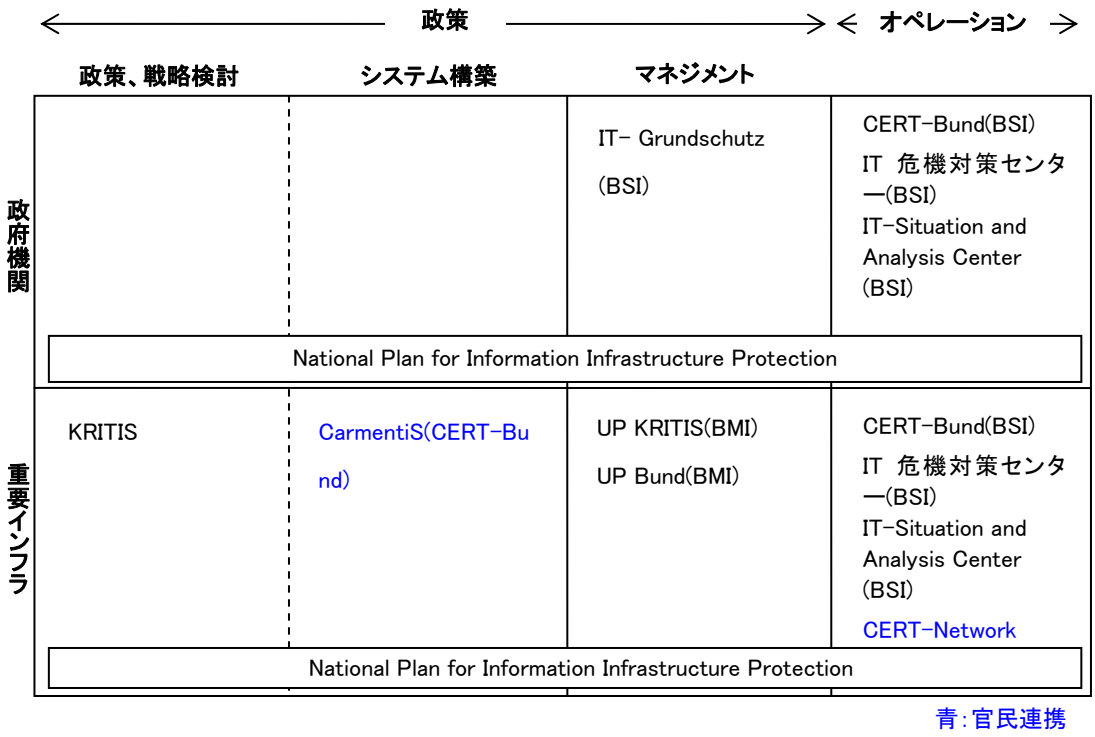


図 4-3 ドイツにおける情報連携のフレームワークの分類

4.1.4. 情報連携の関係図

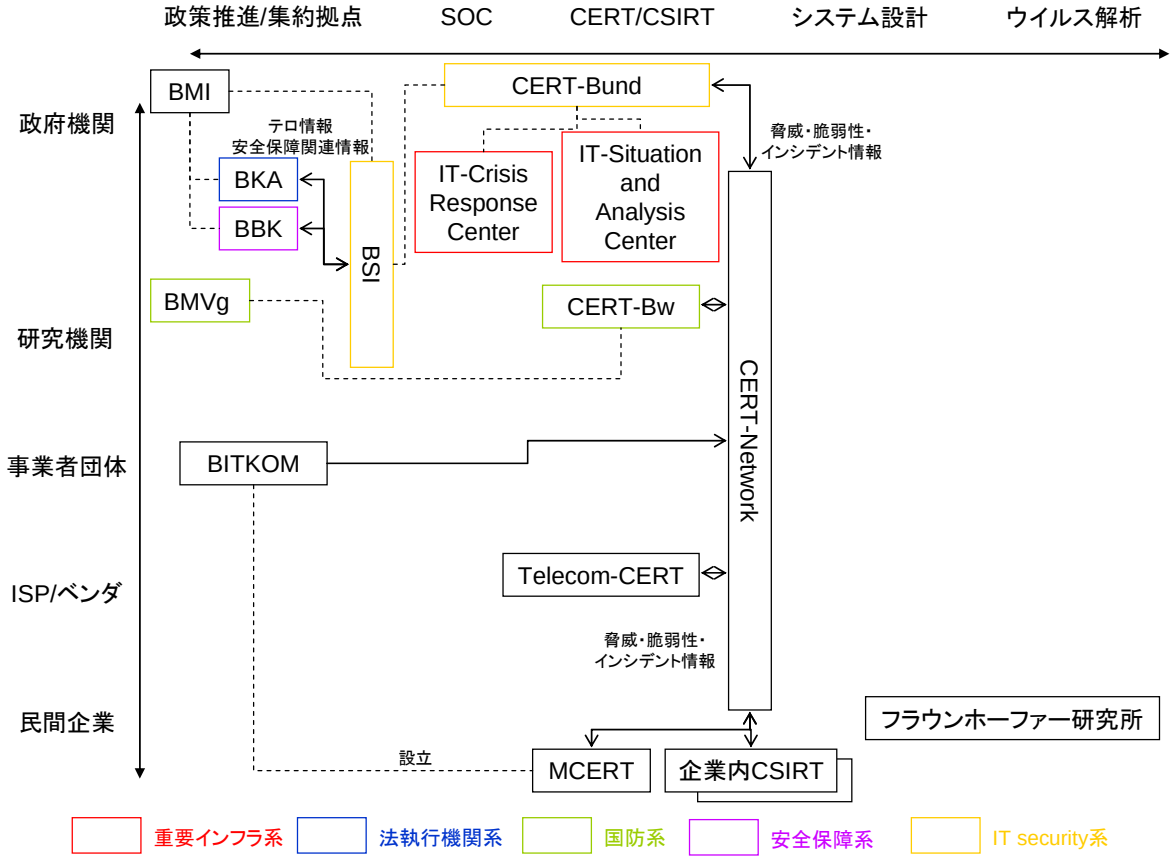


図 4-4 ドイツにおける情報連携の関係図

4.2. 政府機関における情報連携

政府機関における情報セキュリティの方針は NPSI の中で示されており、具体的な基準については IT-Grundschutz の中で規定されている。

(1)National Plan for Information Infrastructure Protection

ドイツの重要インフラ防護における情報基盤保護のための包括的戦略を示した文書。2005 年に BMI から公表されたが、執筆は BSI が行っている。情報基盤保護の戦略目標として以下の視点と個別目標が示されている。

(NPSI の視点と個別目標)[202]

- 予防:情報基盤の適切な保護

202

http://www.en.bmi.bund.de/cln_028/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National_Plan_for_Information_Infrastructure_Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.pdf

– IT 利用に対するリスクの認識を高める（全体）
–IT 製品及び安全な IT システムの利用（全体）
–暗号化等の技術による機密性の確保（政府、企業）
–技術的、物理的、組織的なセーフガードを整備（政府、企業）
–標準等のフレームワークやガイドラインの整備（政府、企業）
–異なる分野のセキュリティ戦略間の調整・連携（政府）
–ネットワークへのセキュリティ対策等における海外諸国及び国際機関との協力関係の構築（政府）

- 準備：IT インシデント発生時の適切な処置
  –インシデントの検知・分析機能の構築（IT 危機対応センターの設置）（政府）
- 持続性：ドイツ全体の IT セキュリティ向上
  –信頼性の高い情報技術の推進及び高信頼性製品利用の奨励（政府、企業）
  –IT セキュリティにおける国家機能向上（政府、企業）
  –学校教育及び専門家トレーニングにおける IT セキュリティ分野の強化（政府、企業、個人）

4.2.2. 政策レベル

4.2.2.1. 政策・戦略検討

情報セキュリティ政策の実務を担当するのは BSI であるが、情報セキュリティに関わる取組の全体的な取りまとめは BSI の親組織である BMI によって行われる。

4.2.2.2. システム構築

BMI は 2002 年 6 月より IBM とドイツ連保政府の Linux 及びオープンソフトウエアへの移行を支援する包括的な協力契約を結んでいる。同契約によって連邦、州、地方の各行政府は、有利な価格で Linux 搭載の IBM 製ハードウエア及びソフトウエアを購入できるようになった。具体的な例として、ドイツの SuSE Linux AG が販売する Linux OS をプリインストールした eServer 等が提供されている。

BMI では 2001 年の同時多発テロ以来、IT インフラのセキュリティレベルを高めるため、官民とのセキュリティ連携の枠組を重視している。当時の BMI 大臣であるシリー氏は IT インフラのセキュリティレベル向上として、システム／ソフトウエアの信頼性を重視しているとした。 一方、IBM ドイツの CEO、エルヴィーン・シュタウト氏は、「連邦行政府でのオープンソース製品の採用は、州及びコミュニティの将来的な方向性を示すだけでなく、ドイツ IT 業界への貢献にもなる」と主張している。[203]

[203] http://www.itmedia.co.jp/enterprise/0206/06/02060608.html

4.2.2.3. マネジメント

(1)IT-Grundschutz[204]

IT-Grundschutz はITシステムにおいて適切なセキュリティレベルを確保するためにBSIが開発したリスクアセスメント/マネジメント手法である。具体的には組織、個人、インフラ、技術的標準、セーフガードを適切に利用することによって目的を達成するものである。IT-Grundschutz は IT-Grundschutz Standards(標準)、IT-Grundschutz Catalogues(脅威/セーフガードカタログ)、IT-Grundschutz GSTOOL(ソフトウエア)、IT-Grundschutz Certification(認証制度)の 4 つのツールによって構成される。以下にそれぞれの機能を示す。

①IT-Grundschutz Standards

IT-Grundschutz は段階的な IT セキュリティの実装を行う手法であり、実践の中で IT セキュリティマネジメントの構築及び運用の方法が示されている。この標準の中では IT セキュリティマネジメントの確立及び組織体制を構築することが最大の目標となっているため、IT-Grundschutz では実践的なITセキュリティのコンセプトを設定し、コンセプトに適した対策の実施手法について、詳細に記載してある。また組織の中で既に構築されている IT セキュリティの体制の改善方法についても同様に詳細な記述がされている。IT-Grundschutz の内容は ISO 13335、17799 及び 27001 によって網羅されているが、それらの要求事項をユーザが実際に理解し、実践できるように、詳細な解説と、専門的背景及び実例を沿えて分かりやすく解説している点が特長である。

②IT-Grundschutz Catalogues

IT-Grundschutz Standards の要求事項に対して想定される脅威や対策等をカタログとして纏めた文書。IT-Grundschutz Threat Catalogues と IT-Grundschutz Safeguard Catalogues から構成される。また対策として「何をすべきである」という情報のみを提供するのではなく、実際にその対策を実施するには、どういったプロセスや情報が必要になるかも含めて詳細に説明しているため、文書は全体で 3,000 ページに及ぶ。文書は BSI のサイトから自由にダウンロードが出来る。

IT-Grundschutz Threat Catalogues

IT システムにおいて具体的に想定されうる脅威について以下の項目で詳細なカタログとしてまとめたもの。

- 不可抗力(15 項目)
- 組織的不備(101 項目)
- 人為的ミス(76 項目)
- 技術的障害(52 項目)
- 物理的な/IT を活用した意図的攻撃(126 項目)

---

[204] http://www.bsi.de/english/gshb/index.htm

IT-Grundschutz Safeguard Catalogues

Threat Catalogues の想定脅威に対して、インフラ、組織、人、BCP 等の観点から詳細な対策を纏めたカタログとなっている。組織におけるケーススタディ等も取り込まれている。

- インフラ(60 項目)
- 組織(306 項目)
- 人(42 項目)
- ハードウエア/ソフトウエア(232 項目)
- コミュニケーション(121 項目)
- 事業継続管理(95 項目)

③IT-Grundschutz GSTOOL

IT-Grundschutz の要求事項をベースとした IT セキュリティを実際のシステムに実装するためのソフトウエアであり、BSI のサイトの中において有償で提供されている(1 ライセンス 76,500 ユーロ(約 995 万円[205]、大学は半額))。30 日の試用版及びマニュアルは BSI のサイトからダウンロード可能となっている。[206]GSTOOL がサポートする主な機能を以下に示す。

(GSTOOL の機能)

- IT-Grundschutz に沿ったシステムのモデリング
- IT システム記録及び構造分析
- アプリケーションの記録
- セーフガードの実装
- コスト分析
- 要件決定
- レポート機能
- システム修正サポート
- 基本的なセキュリティチェック
- IT-Grundschutz 認証対応

(GSTOOL のパフォーマンスの特徴)

- 複数のセキュリティコンセプトを 1 つのツールで管理
- ネットワークの可用性
- 2 カ国語対応(英語／ドイツ語)
- ユーザが自由に設定したデータの外部送信に対する暗号化

---

[205] 1 ユーロ＝130 円で計算。

[206] http://www.it-grundschutzhandbuch.de/english/gstool/gstoolmanual.pdf

・ 基本的パフォーマンスの向上
・ 過去履歴の保存
・ モダンで人間工学的なデザイン
・ インターネットやメールを通じて簡単にアップデート可能なデータベース機能
・ Versions 2.0 1998-2000 からのインポート機能

④IT-Grundschutz Certification

企業や政府機関における IT セキュリティに関する活動を対外的にアピールするための認証制度。IT-Grundschutz のユーザに対して BSI が 3 段階の資格を与えており、実際に認証を与えるかを判断する監査は BSI から認定された監査法人によって行われる。監査の基準については BSI が公開する IT-Grundschutz Manual の中の"Audit Scheme for Auditors"の中に明記されている。

(2)E-Government Manual

ドイツ連邦政府の電子政府戦略である BundOnline2005 をベースとした、電子政府を構築する政府側の立場の人間を対象とした標準的な情報セキュリティを実装するためのマニュアル。

4.2.3. オペレーションレベル

4.2.3.1. 組織

(1)連邦コンピュータ緊急事態対策チーム(CERT-Bund)[207]

2001 年に BSI 内部に設置された政府機関のセキュリティインシデント対応チーム。前身は BSI ーCERT である。主に政府職員、政府機関(州政府等を含む)を対象とする CSIRT であり、BSI の第 1 局第 2 課が運営している。情報の共有は主に目的別に整備されたメーリングリストによって行う。また、組織内部に IT-Situation and Analysis Center という組織を持っており、そこでは政府ネットワークを対象として監視を実施する SOC としての機能も持つ。

また CERT-Bund 内部に別に設置されている IT 危機対策センターでは政府機関のみならず、重要インフラの脅威や脆弱性に関する情報提供やインシデント対応も行う。

(CERT-Bund の主な機能)

・ 政府機関の SOC(IT-Situation and Analysis Center)
・ 24 時間体制の連絡窓口
・ IT 危機対策センターの運営
・ 詳細なセキュリティ事案、脆弱性情報等の分析
・ インシデントの調査と復旧のサポート
・ インシデント対応及びマルウエアレポートの連動

[207] http://www.enisa.europa.eu/doc/pdf/other/2nd_cert_ws/enisa_german_activities.pdf

・情報セキュリティに関する対策、助言及び普及・啓発活動
・警告情報の提供
・連邦政府機関の緊急時対応
・IT 危機対策センターの運営警報

（CERT-Bund が連邦政府機関に対して配信するメーリングリストの例）[208]
・ウイルス、ワーム、脆弱性に関する情報配信用リスト（=virinfo）
・システム内の IT セキュリティギャップに関する情報配信用リスト（=kurzinfo）
・セキュリティ関連事件及びその適切な対処方法配信用リスト（=advisories）

(2)IT Situation and Analysis Center

ドイツにおけるIT セキュリティの状況を監視し、情報を収集・分析した上でドイツにおけるIT セキュリティ全体の状況を可視化している。集めた情報はターゲットごとに加工され、政府機関、重要インフラ事業者、一般ユーザに対して提供される。[209]

(3)CERT-Verbund （CERT-Network）[210]

CERT Network はドイツにおける CSIRT 組織の連携体制であり、現在官民を含め 19 の CSIRT が所属している。組織の主な目的は、異なる組織間の強力な連携により、情報の収集・分析力を強化することであり、そのために国家の IT ネットワーク保護体制の確保とセキュリティインシデントに対して迅速な対応能力を提供している。また、参加メンバの中では情報連携を支援するシステムやツールに対する研究開発も実施されている。以下に CERT-Verbund によって開発されたシステムの一例を挙げる。

（CERT-Verbun によって開発されたシステム）
・CarmentiS
・Deutsches Advisory Format (DAF)
  - 独の CSIRT 機関のニーズに沿ったセキュリティ情報交換様式
・Common Model of System Information (CMSI)
  - CSIRT 間の協力を改善するために開発
  - IT システムを説明するための共通モデルを提供
  - モデルは完成済み、データベースを構築中
・System for Incident Response in Operational Security (SIRIOS)
  - CSIRT におけるインシデント対応及び脆弱性管理のための枠組

[208] http://www.bsi.de/certbund/index.htm
[209] http://www.bsi.bund.de/english/topics/kritis/aufgabenwahrnehmung.htm
[210] http://www.ipa.go.jp/security/fy18/reports/fraunhofer/documents/abstract.pdf

表 4-1 CERT-Network のメンバ

官	民
CERT-Bund, BSI Bayern-CERT, Landesamt für Statistik und Datenverarbeitung（バイエルン州） CERT Baden-Württemberg, Innenministerium Baden-Württemberg（バーデン・ヴュルテンベルク州） CERTBw, Bundeswehr（軍）	BFK Consulting GmbH CERT-NRW, Landesamt für Datenverarbeitung und Statistik NRW CERT-VW, Volkswagen AG CERTBw, Bundeswehr CERTCOM AG ComCERT, Commerzbank AG DFN-CERT Services GmbH GNSec IBM BCRS PRESECURE Consulting GmbH RUS-CERT, Universität Stuttgart S-CERT, SIZ Informatikzentrum der Sparkassenorganisation GmbH Secunet Security Networks AG Siemens-CERT, SIEMENS AG Telekom-CERT, CERT-NRW, Landesamt für Datenverarbeitung und Statistik NRW CERT-VW, Volkswagen AG CERTCOM AG ComCERT, Commerzbank AG

(a) 情報共有の担保方法・ルール

19 以上の官民 CSIRT 組織が集まる CERT-Network では、情報共有に際して“Code of Conduct[211]” 及び NDA に署名する必要がある。Code of Conduct の中では、情報提供はあくまで任意であり、ビジネスに係る部分や顧客データの守秘を高いプライオリティとして置いている。

(4)CERT Working Group (CERT-Arbeitsgruppe)

ドイツ国内で整備されている 30 以上の CSIRT 組織が集まる非公開の会合。2 年に 1 回開催される。

(5)Mcert （M-Computer Emergency Response Teams）[212]

2002 年に発行された「インターネットのセキュリティと信頼」（“Security and Trust in the Internet”, a product of the project CERT Infrastructure Germany）の中では、ドイツの既存の企業内 CSIRT である、dCERT 、DFN-CERT 、S-CERT secu-CERT 、Telekom-CERT、CERT-Bund 等 と同様に、中小企業向けの CSIRT を設立すべきだと主張されている。これを受けて 2003 年には経済技術省、内務省、IT 関連の業界団体 BITKOM によって中小企業のための CSIRT として Mcert が設立された。設立に当たってはドイツ国内の IT 大手企業もスポンサーとして参加している。

[211] http://www.cert-verbund.de/coc.html （ドイツ語サイト）
[212] M はドイツ語の「中小企業」“Mittelstand” の頭文字

現在、実際の運営は BITKOM の子会社である Mcert German IT security 社が行っている[213]。提供するサービスのタイプは企業規模によって 2 つに分類されており、具体的には「内部に IT セクションを持たない小規模な企業」と、「従業員 50 人以上で内部に IT セクションを持つ企業」という基準でサービスの切り分けが行われている。構成員は、最初の 3 年間は出資者の支援により、無償でサービスを受けられるが、その後は自己負担となる。

参加企業は最初に企業の IT プロファイルを Mcert に提出し、Mcert 側ではそのプロファイルに基づき、各企業の必要とする情報を分類分けする。その上で、CERT-Network や企業等、外部機関から提供された早期警戒情報を独自に取りまとめ、中小企業の担当者でも分かりやすいように解説や助言を添えた形で、各企業のニーズに合わせたパッケージとして提供する[214]。

4.2.3.2. National CSIRT と ISP の関係

ドイツの National CSIRT である CERT-Bund はドイツにおける官民 CSIRT 組織の連携体制である CERT-Network の運営を行っており、同組織に参加している ISP を中心に組織された Telecom-CERT とも情報共有を行っている。

4.2.3.3. 職員

BSI の 430 人(2006 年時)の人員の内、およそ 8 割は研究者である。CERT-Bund における職員は常時 10 名程度で、BSI の職員が配属される。ただし、必要に応じて BSI の別のセクションと連携をして活動を行うことも多い。役割分担としてはチームリーダ 1 名、シニアアドバイザー3 名、セキュリティ専門家 5 名、秘書 1 名となっている。

---

[213] http://www.ecom.jp/results/h18seika/02_%E6%B5%B7%E5%A4%96%E3%81%AB%E3%81%8A%E3%81%91%E3%82%8BEC%E6%8E%A8%E9%80%B2%E7%8A%B6%E6%B3%81%E8%AA%BF%E6%9F%BB%E5%A0%B1%E5%91%8A%E6%9B%B82006.pdf

[214] http://www.oecd.org/dataoecd/54/32/31453706.pdf

4.3. 重要インフラ防護における情報連携

ドイツにおける重要インフラ防護の取組は古く、1997 年に設立されたKRITIS の設立以来続いている。現在実際に政策を推進するのはBSIである。現在の取組は2006 年に公表されたドイツの最初の重要インフラ防護計画である National Plan for Information Infrastructure Protection（NPSI）[215]を基礎とした活動を行っている。

4.3.1. 政策レベル

4.3.1.1. 政策・戦略検討

(1)重要インフラ保護会議（KRITIS）

KRITIS は米国の PCCIP の設立を受け、1997 年に内務省の中に重要インフラ総合研究作業部会として設立された。WG メンバには内務省の代表、運営委員、BSI からなる。AG KRITIS の主な目的を以下に示す。

- ドイツにおける脅威シナリオの作成
- ドイツの重要インフラにおける脆弱性分析
- 対策の提案
- 早期警戒連携の計画

AG KRITIS では 1998 年の前半に、ドイツの重要インフラにおける国家戦略、各重要インフラにおける IT 依存度、想定されるリスクアセスメントに関する調査を行っている。以下に、これらの調査の結果を示す。[216]

（AG KRITIS の調査結果）

- IT における脅威の認識は組織毎に大きく異なる。
- 調査実施対象者は IT セキュリティにおける脆弱性を調査することに非協力的である。
- IT システムにおいてハッキングとデータへの不正アクセスが最も重大な脅威として認識されている。

KRITIS における活動はドイツにおける重要インフラ防護の基礎を築いたが、実務的な役割は現在 BSI に引き継がれている。

4.3.1.2. システム構築

(1)CarmentiS[217]

重要インフラ防護の目的のために国内に設置されたセンサから得られたデータを、センサ設置協力者や CSIRT 内で、収集、共有、分析するためのシステム。CERT-Bund によって開発された。

---

[215] 独語では Nationaler Plan zum Schutz der Informationsinfrastrukturen と表記するため。

[216] http://www.iwar.org.uk/cip/resources/Kritis-12-1999.html.

[217] http://www.first.org/conference/2006/papers/junger-sander-slides.pdf

現在未だ試験的な段階にあり、脅威情報を効率的に集める体制を構築するためのテストベッドでもある。参加する協力者はセンサ情報を提供し、CSIRT 組織は収集データの解析を行う。現在試験段階であるが、センサ BOX の設置地点の増加と情報提供者の確保が課題となっている。[218]

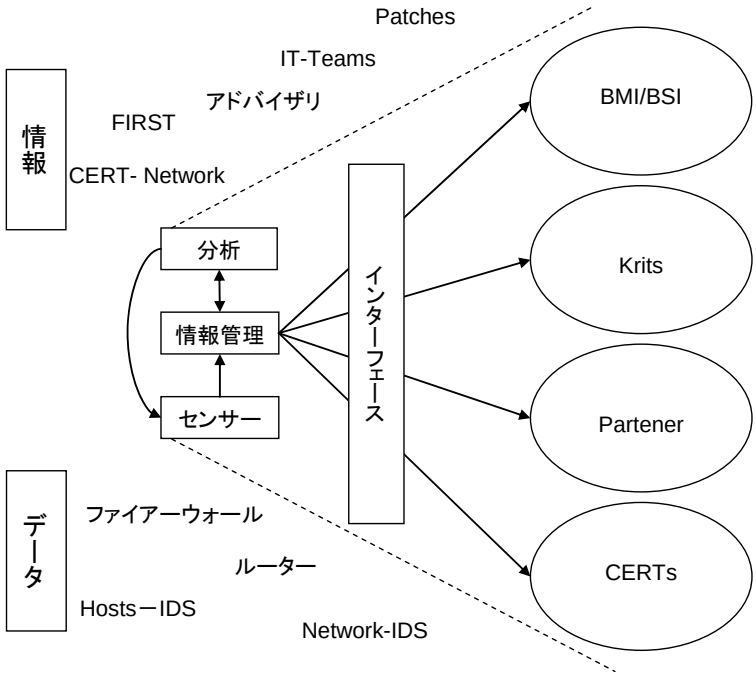


図 4-5　CarmentiS における情報の流れ[219]

218

http://www.eu2007.bmi.bund.de/nn_1034550/Internet/Content/Common/Anlagen/Themen/Europa_Internationales/Veranstaltungen/IT_Security/Tag_1/Forum_II/Sander_Tag2,templateId=raw,property=publicationFile.pdf/Sander_Tag2.pdf

219 218 と同じ。

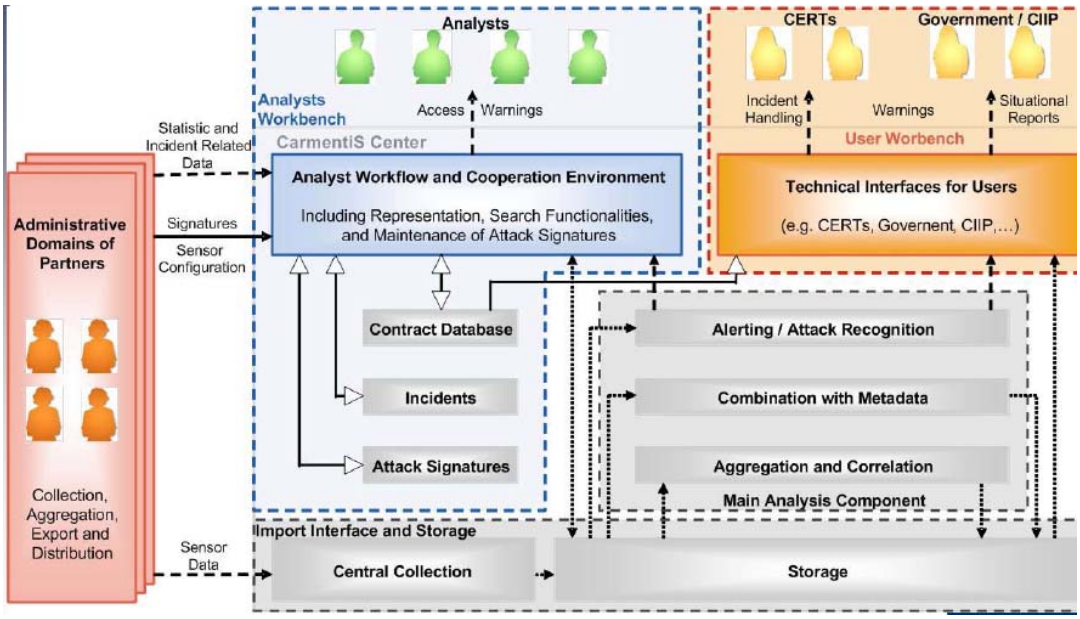


図 4-6 CarmentiS における情報の流れ[220]

4.3.1.3. マネジメント

(1)Implementation Plan for Critical Infrastructure Protection 2007(UP-KRITS)(2007)

2005 年の NPSI を企業や団体に実装するための文書。重要インフラ防護と同様に高レベルの情報セキュリティの確保にも主眼を置いている。

(2)Implementation Plan for the Federal Administration(UP Bund)(UP KRITIS)(2007)

NPSI を政府機関において実装するためのガイドライン。各政府機関における実装については、各省庁にその実施の権限が委ねられている。

4.3.2. オペレーションレベル

4.3.2.1. 組織

CERT-Bund は政府機関だけでなく、重要インフラに対するオペレーション機能も持つ。中でも CERT-Bund の中に設置された IT 危機対策センターは重要インフラにおけるインシデント対応を目的として設立されている。

(1)IT 危機対策センター(IT Crisis Response Center)[221]

情報システムに重大な損害を与えるような国家危機に備える目的で CERT-Bund の中に設置された対策センター。2006 年に公表されたドイツの重要インフラ防護計画 National Plan for

[220] 218 と同じ。

[221] http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663

Information Infrastructure Protection (NPSI)の中で設立が提案された。国内の情報セキュリティに係る状況に対して信頼性の高い分析を行う管理・分析センターとしての役割を担っており、様々な危機状況に対応して、その被害を防ぐために IT 危機管理を発動させ、被害の潜在的対象者に対して警戒を行う。さらにインシデント発生時には連邦政府機関において対応を実施し、被害を受けた情報システムのオペレーションを再開するための調整機能も持つ。

4.3.2.2. 官民連携体制

ドイツには、ISAC のような官民連携を軸とした重要インフラ防護における情報共有を目的とした組織は存在しない。一部の分野を除いて、競争関係にある関連機関同士で情報を共有するには限界があると考えられている。一方で、組織の自主的な取組である CSIRT の設立は盛んで、現在 CERT-Bund や企業で構築されている CSIRT も含めドイツでは 40 以上の CSIRT 組織が整備されている。それらは CERT-Network 等の活動等を通じて密接に連携している。

(参考)ドイツにおける官民 CSIRT 設立の流れ

1991 Micro-BIT (University of Karlsruhe)

1993 DFN-CERT (German Research Network)

1994 BSI-CERT / CERT-Bund (BSI)

2002 CERT-Bw (ドイツ陸軍)

2003 Mcert (中小企業)

2005 Bürger-CERT (国民のための CSIRT)

今後～ CSIRT が整備されていない分野における CSIRT の整備

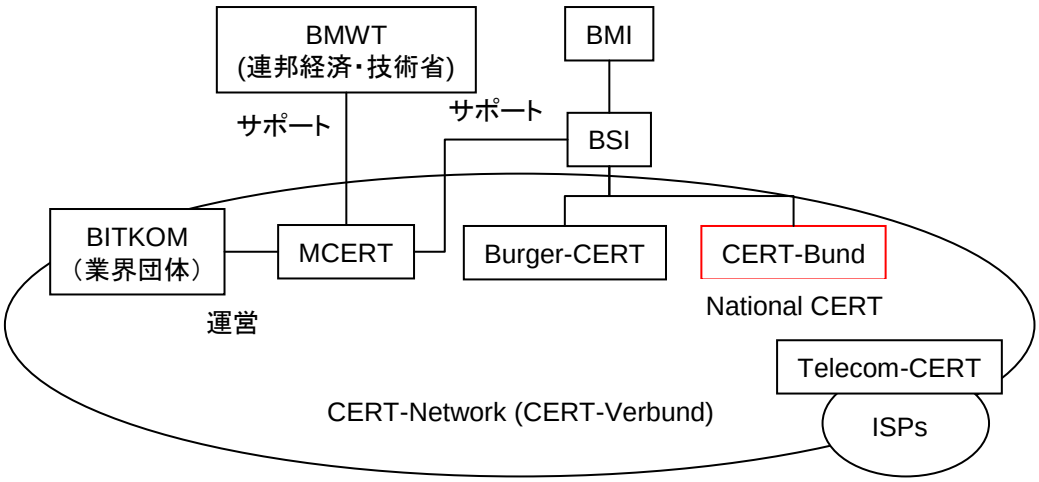


図 4-7 ドイツ内の CSIRT の関係図(CERT-Network)

5. オーストラリア

5.1. 情報連携のフレームワーク

オーストラリアはテロや災害を含むあらゆる緊急事態を想定した全てのリスクに対応する体制（all hazard approach）をとっているため、情報セキュリティに関する取組も、その目的によって司法省、予算・行政省、国防省や警察組織等、多数の組織の中で実施されている。

重要インフラ防護に関しては司法省の主導の下、米国の ISAC にならった官民連携組織の TISN の中で分野別の情報共有の取組が進められている。

5.1.1. 情報セキュリティ関連組織

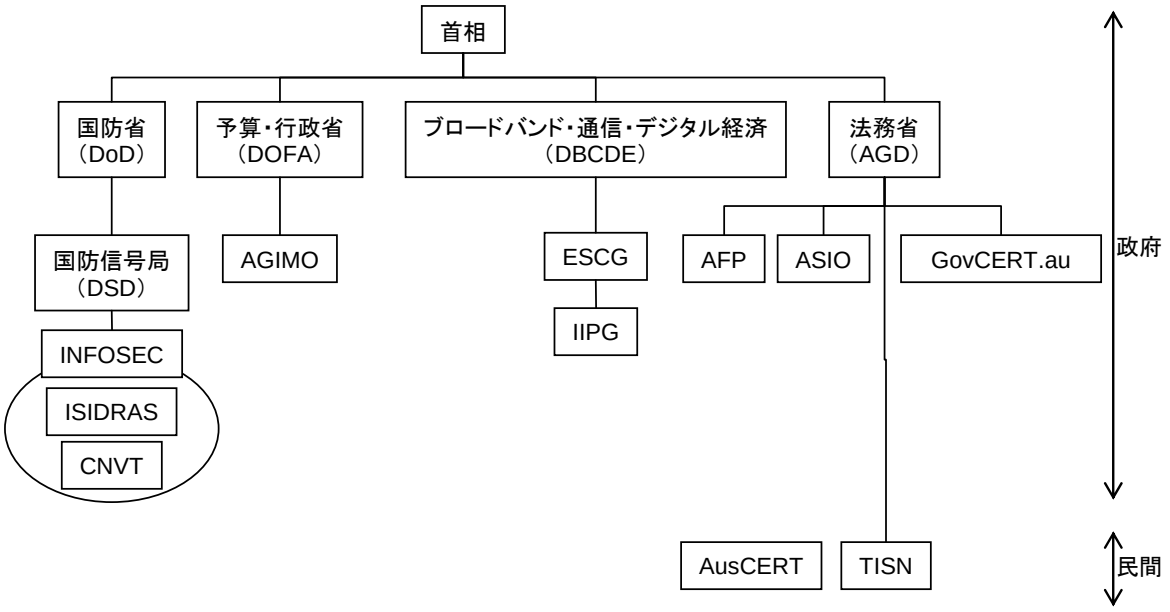


図 5-1 オーストラリア情報セキュリティ関連組織

(1)司法省（AGD：Attorney-General's Department)[222]

国家安全保障の観点から重要インフラ保護の指針を策定、推進する。情報セキュリティ政策の具体的な推進役を担っており、重要インフラ保護に関して、各連邦機関の調整機能を持つ。オーストラリア連邦政府の情報セキュリティ対策の標準を規定するとともに、重要インフラのセキュリティ対策のためのプロジェクト推進及び対策手法の開発も行っている。

[222] http://www.ag.gov.au/

(2)ブロードバンド・通信・デジタル経済省（DBCDE：Department of Broadband, Communications and the Digital Economy）

電気通信事業を始とする情報技術関連のサービス事業者を所管する省庁である。2007 年 11 月の総選挙により通信・情報技術・芸術省（DCITA：Department of Communications, Information Technology and the Arts）から改組された。現在ブロードバンド網の構築に特に力を入れている。

(3)国防信号局（DSD：Defense Signal Directorate）[223]

DSD は情報セキュリティ及び信号インテリジェンス機関であり、オーストラリア国家の情報及び通信システム防護において重要な役割を果たしており、各省庁に対して暗号やネットワークセキュリティ、情報セキュリティに関するガイドラインやポリシー策定のための専門家を派遣している。具体的には政府の情報システムの保護指針を示した ISM の策定やメンテナンス、また後述の政府機関における情報セキュリティインシデントの情報収集及び分析を行うなうためのスキームである ISDRAS の運営をしている。民間企業とは新しい暗号の開発等の活動で協力をしている。

(4)Australian Government Information Management Office（AGIMO）[224]

2004 年の設立当初は旧 DCTIA（現 DBCDE）に設置されたが、現在は予算行政省（DOFA：Department of Finance and Administration）の下に移された。政府への ICT の利用促進を図ることが主な役割となっている。AGIMO のトップはオーストラリア政府の CIO としての機能を果たすとしている。また gov.au ドメインは AGIMO が管理を行っている。

(5)Australian Security Intelligence Organization (ASIO)[225]

オーストラリアの国防諜報機関。1949 年 H.V.エヴァットの助言によりチフリー内閣によって創設された。1956 年には法律が整備され、ASIO は国家の安全に関わる情報の収集のための権限を与えられている。現在は 1979 年の Australian Security Intelligence Organization Act 1979 においてその機能が規定されているが、1999 年の改正では、民間のコンピュータ・システムが「安全保障事項」に関連すると考えられる正当な理由があるならば、これを合法的にハッキングすることの他、データのコピーや変更をも認可出来るという内容が追加されている。[226]ASIO は専らスパイや反政府活動に対する安全政策が任務であるが、英国の MI5 や米国の CIA のような他の連合国の諜報機関と協力関係を維持している。

---

[223] http://www.dsd.gov.au/

[224] http://www.finance.gov.au/agimo/index.html

[225] http://www.ajf.australia.or.jp/aboutajf/publications/sirneil/dict/AustralianSecurityIntelligenceOrganizationASIO.html

[226] http://wiredvision.jp/archives/199912/1999120703.html

(6)Australian Government Computer Emergency Readiness Team (GovCERT.au)[227]

海外の National CSIRT との連絡窓口として 2005 年に設立。実際のオペレーションというよりは、重要インフラにおけるオーストラリア政府の政策のサポートや、重要インフラ事業者に対する情報提供やファンディング（後述の CNVA）等を行う。

(7)重要インフラ諮問委員会（The Critical Infrastructure Advisory Council）

重要インフラを有する省庁、州政府、地域政府、全国の対テロ委員会及び、政府機関の代表者からなる委員会。会議は司法長官に対して、オーストラリア国家の重要インフラ防護及び対テロ対策について関連する事項に対して忠告を行う。

5.1.2. 法執行機関、防衛機関、情報機関の位置づけ

国家の情報システムに影響を与えうるインシデントに対しては国防信号局 DSD、警察 AFP そして情報機関の ASIO が Joint Operating Arrangement の下、情報収集や分析において協力体制をとっている。

5.1.3. 情報連携の分類

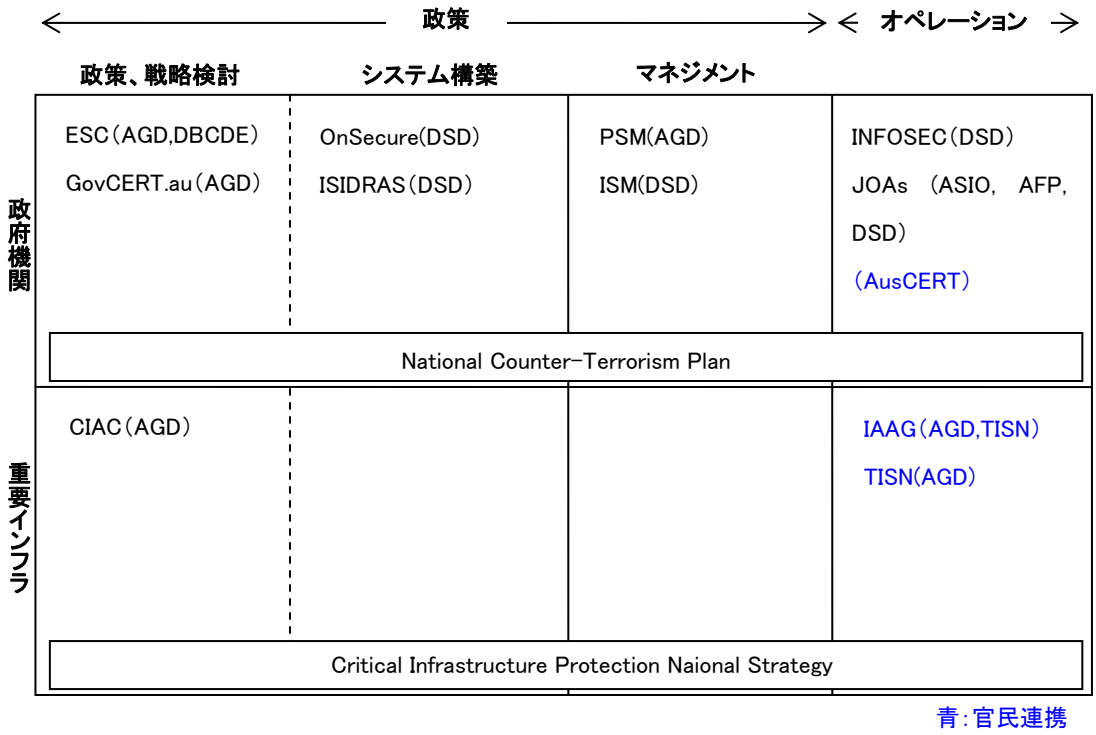


図 5-2 オーストラリアにおける情報連携のフレームワークの分類

[227] http://www.ag.gov.au/govcert

5.1.4. 情報連携の関係図

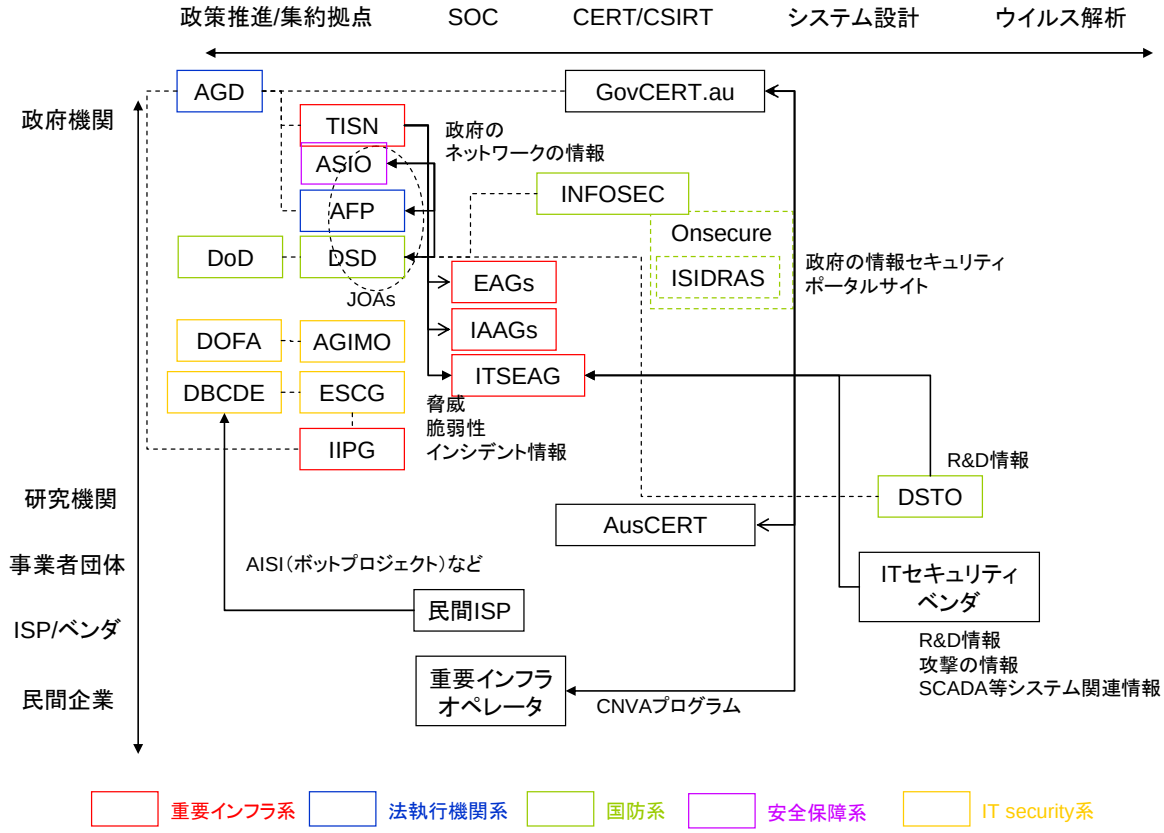


図 5-3 オーストラリアにおける情報連携の関係図

5.2. 政府機関における情報連携

オーストラリアはテロ、災害、人為的な要因の全てのリスクに対応する体制（all hazard approach）をとっているため、情報セキュリティが物理セキュリティも含めた国防や国家安全保障の枠組で捉えられており、基本的方針は 2003 年に公表された“National Counter-Terrorism Plan”[228]に基づくとされている。情報セキュリティが多くの省庁にまたがる課題として捉えられているため、情報セキュリティに関わる政策の取りまとめを目的として各政府機関の代表者によって構成される E-Security 調整グループ（ESCG）が設置されている。

228

http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(3273BD3F76A7A5DEDAE36942A54D7D90)~National+Counter-Terrorism+Plan+-+Alert+System+Changes+October+2008+PDF.PDF/$file/National+Counter-Terrorism+Plan+-+Alert+System+Changes+October+2008+PDF.PDF

5.2.1. 政策レベル

5.2.1.1. 政策・戦略検討

情報セキュリティ政策の立案や国家横断的な情報セキュリティの問題に対処するための組織として、DBCDE の組織下に E-Security 調整グループ(ESCG)が設置されている。グループのメンバは AGD をはじめとした複数の政府機関の代表者によって構成されている。

(1)E-Security 調整グループ(ESCG: E security Coordination Group)

2001 年に AGD 長官と DBCDE 大臣から設立が発表され、DBCDE の NOIE(情報経済局)の下部組織として設置されている。官民双方にとっての安全で信頼出来る IT 環境作りのために、国家情報システム防護、経済及び地域社会に影響を与える情報セキュリティ問題に対する方針策定及び調整を行う。14 の連邦省庁の代表者とから構成される。ESCG の主な活動としては以下の 4 つが挙げられる。

(ESCG の主な活動)

- 公的機関、民間企業の双方に対する情報セキュリティの普及啓発
- 産業界やサービスプロバイダとの情報共有の促進
- 情報セキュリティ活動に関する国際対応
- 情報セキュリティ関連技術やその研究開発に関する事項

5.2.1.2. システム構築

(1)OnSecure[229]

OnSecure は、DSD と財務管理省下のオーストラリア政府情報管理局(AGIMO : Australian Government Information Management Office)との共同プロジェクトにより 2003 年 12 月に誕生した。本サイトの第一目的は、オーストラリアの公共サービス向上のために、セキュリティインシデントに関する情報を収集することであるが、その情報をワンストップで提供するオーストラリア政府のポータルサイトとしても重要な役割を担っている。

OnSecure が整備されるまでは、オーストラリアの政府機関が情報セキュリティインシデントについて報告する場合、文書を郵送或いは FAX で送る方法しかなかった。同サイトの整備により、各政府機関は迅速且つ安全にオンラインでインシデントの報告が実施できるようになり、またそれらを受ける DSD 側にとっても、それぞれのインシデントを監視し、その発現パターンを分析することにより、インシデントの管理がより効率的に行えるようになった。[230]

[229] http://www.onsecure.gov.au/(非公開)

[230] http://e-public.nttdata.co.jp/f/repo/547_a0805/a0805.aspx より引用

(2)Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS)

DSD が運用する情報セキュリティインシデントのレポート及び解析スキーム。政府の情報システムに影響を与えるようなセキュリティインシデントに関する情報収集を目的としている。政府機関で検知されたインシデントは所定の様式によって、前述の OnSecure サイトを通じて提出される。

5.2.1.3. マネジメント

(1)Protective Security Manual (PSM)[231]

AGD の Protective Security Policy Committee (PSPC)によって管理されているオーストラリア政府機関向けの情報セキュリティに関するポリシー。オーストラリアの公的資源を守るために、オーストラリア政府機関が遵守すべき防御策に関する原則、標準及び手続きについて記載している。

(PSM の構成)

Part A. 防御セキュリティ政策
Part B. セキュリティリスク管理指針
Part C. 情報セキュリティ
Part D. 職員のセキュリティ
Part E. 物理的セキュリティ
Part F. 競争入札及び契約のためのセキュリティの枠組
Part G. セキュリティに関するインシデント及び調査に関する指針
Part H. 在宅勤務に関するセキュリティ指針

特に情報セキュリティに関しては、下記(2)の Australian Government ICT Security Manual と内容が重複することがないよう、機密情報(電子的・紙ベース両方)の保護に関する最低限の防御標準を提供している。[232]

(2)Australian Government ICT Security Manual (ISM)[233]

DSD が作成したオーストラリア政府機関における情報通信システムにおける情報の保護を目的とした情報セキュリティポリシー及び標準。2007 年までは Australian Government Information and Communications Technology Security Manual (ACSI33)という名称で公表されていた。オーストラリアの政府機関は前述の PSM において ISM に準拠することが義務付けられている。

---

[231] http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_ProtectiveSecurityManual(PSM2005)
[232] http://e-public.nttdata.co.jp/f/repo/547_a0805/a0805.aspx より引用
[233] http://www.dsd.gov.au/library/infosec/ism.html

5.2.2. オペレーションレベル

5.2.2.1. 組織

(1)Information Security Group（INFOSEC）[234]

DSDの中に設置されたINFOSECではオーストラリア政府機関に対する情報セキュリティ対策の支援を実施しており、インシデント情報の収集・分析、警告サービス、セキュリティ対策、BCP の策定も行う。また、DSD は後述の ASIO と AFP と正式な Joint Operating Arrangements（JOAs） を結んでおり、オーストラリアの情報システムの完全性に影響を与えうるインシデントに対して脆弱性分析や対応の面で協力体制をとっている。

5.2.2.2. 職員

各オーストラリア政府機関には DSD において養成された情報セキュリティの専門家が派遣され、暗号やネットワークセキュリティ等の技術的な指導と、情報セキュリティポリシーの整備等の体制の構築を行っている。

[234] http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663

5.3. 重要インフラ防護における情報連携

オーストラリアでは重要インフラ防護に対して司法長官に助言を行う AGD が官民連携組織 TISN の指揮をとっており、司法省下に重要インフラ防護組織が組み込まれるという体制をとっている。

5.3.1. 政策レベル

2004 年に発行された Critical Infrastructure Protection National Strategy の中でオーストラリアの重要インフラ防護戦略が示されている。この中で、オーストラリアの重要インフラ防護に関しては各ステークホルダの役割が明確に示されている。

（オーストラリアにおける重要インフラ防護における各ステークホルダの役割）

①オーストラリア政府の役割

- オーストラリアにおける重要インフラ防護の戦略的な主導及びオーストラリア国内全土における重要インフラ防護への取組を展開し、実装するための調整
- 連帯的な責任が発生する場合の主導及び調整
- 重要インフラ防護の構築における州政府、準州政府との連携
- オーストラリア政府の重要サービス、（国防、外交、議会等）の確実な保護
- 重要インフラ防護に携わるステークホルダに対する情報提供
- オーストラリア政府が定める重要インフラ分野における防護策の徹底
- 海外にあるインフラや資産、複数の司法権利が関わる重要インフラに対する防護策の徹底
- 国家の重要インフラに対するデータベースの開発及び整備
- 重要インフラ防護に係る事項について海外と調整を行うリアゾンとしての役割
- 条約の義務に従って、国際組織に求められた情報を提供すること
- 重要インフラ防護を国家の主要研究課題と位置づけ
- オーストラリアにおける重要インフラ事業者に対する防護策の構築、確認、監査等の援助の実施
- 研究開発や技術面も含め、国家の情報セキュリティの強化
- 国家レベルにおける公開情報やメディアの管理

②州政府、準州政府の役割

- 国家の重要インフラ防護の取組を各州で構築、実装するための主導と調整
- 結果管理とコミュニティの回復能力の強化
- 重要インフラ事業者の防護策の構築の支援とサービスの継続性の確保
- 管区の中の重要インフラに関するデータベースを整備
- 州及び準州政府における重要サービス（公共施設や設備）の確実な保護
- 管轄区における重要インフラの脅威レベルに応じた対応について合意
- 重要インフラ事業者の防護策の構築、確認、監査の支援

・重要インフラ防護におけるオーストラリア政府との連携と協力
・管区内の好評とメディア管理

③国家対テロ委員会の役割
・重要インフラをテロから防護するための国家戦略の策定
・対テロの演習の中に重要インフラを取り込むこと
・CIAC に対する要注意事項に関する助言

④州及び準州警察の役割
・管区における重要インフラ防護を支援し、対テロに対する戦略を構築
・管区の重要インフラ事業者に対する関連する脅威情報の提供
・各州及び準州のリアゾンとして重要インフラ事業者を管理すること
・得られた情報の関連する組織への伝達
・重要インフラ防護に係る訓練への参加

⑤地方自治体の役割
・管区における、コミュニティベースの重要インフラ防護策の実装の調整
・重要インフラ防護の重要性の理解促進
・重要インフラ防護策の実施支援（訓練契約、使用電力、建築物に対する制限）、及びアセスメントの実施
・重要インフラ事業者の防護計画がステークホルダにとって関連ある項目として整備されていること
・地域の重要インフラ防護枠組の中における被害管理と回復能力の強化のための支援

⑥重要インフラ事業者
・所有する資産に対する適切なセキュリティの確保
・計画プロセスの中にリスクマネジメント技術を適用
・定期的なリスクマネジメントアセスメントと計画の見直しを行う
・インシデントや疑わしい行為に関して州警察に連絡
・BCP の策定と定期的な見直しの実施
・政府機関で行われる訓練への参加

⑦CIAC
・重要インフラ防護の国家戦略の方針を司法長官に助言
・重要インフラ防護における TISN の活動を監視
・TISN の分野から出される相互依存性の問題に関する検討

⑧専門組織

・各組織の専門領域の中で重要インフラ防護を推進し、ガイドラインやベストプラクティスの作成や情報共有を支援する。

⑨監査組織

・市場規制の中で強固な重要インフラへの投資の必要を議論する。

⑩Standards Australia International

・危機管理、コーポレートガバナンス、BCP、セキュリティに関する標準を普及させる。

5.3.1.1. 政策・戦略検討

重要インフラ防護に関する省庁横断的な政策立案と技術的な対処を行う組織としてESCGの小委員会という位置づけでInformation Infrastructure Protection Group(IIPG)が設置されている。委員会の主導権はAGDが持つ。

(1)Information Infrastructure Protection Group(IIPG)

ESCG と同様、複数の政府機関の代表者から組織されており、オーストラリアの重要インフラ防護に関して、重要度の特定と助言を提供する責任を負う。

5.3.1.2. システム構築

技術的な情報提供はAusCERTを通じて行われる。

(1)National Information Technology Alert Service

AusCERT が運用している企業や一般のコンピュータユーザに対してコンピュータネットワーク上の脅威や脆弱性情報を配信する無料のメーリングリストサービス。

5.3.1.3. マネジメント

TISN(後述)の情報共有における論点について、関係機関(通信局(Australian Communications Authority)、諮問規制局(Australian Prudential Regulation Authority)、自由競争消費者委員会(Australian Competition and Consumer Commission)、安全投資委員会(Australian Securities and Investment Commission)、証券取引所(Australian Stock Exchange))による協議において以下のような方向性が示された。

TISN における情報共有は競争阻害行為に当たるか。

1974 年取引慣行法パート 4 第 45 節

・市場における競争を抑制する影響を持つ契約及びその準備行為を禁止

⇒セキュリティ上の脅威及び脆弱性に関する議論を行うことは問題ない。

⇒ただし価格設定や事実上の業界標準の決定に影響がある情報ならば問題がある可能性。

企業が TISN で情報を共有する際に、オーストラリア証券取引所上場規則に則って、それらの情報を公開することを求められないか。

2001 年会社法第 6CA 章

オーストラリア証券取引所上場規則 3.1A 及び 3.1B

・株価の価格または実際の価値に影響を及ぼす情報は公開されなければならない。

・ASX が市場が株価を誤ることを予想し、企業にその誤りを防ぐように求めた際には、企業側はそれらを防ぐための情報を公開しなければならない。

例外）

ASX が公表しないことを容認した情報

・仮定レベル、不確かな情報

・内部管理のための情報

⇒ Deed of Confidentiality を策定

連邦政府はどのように企業から TISN に提供される情報を保護するか。

⇒以下の法律で保護される。

・1914 年犯罪法第 70 節　連邦政府の非公開義務

・1982 年情報公開法第 43 節　ビジネスに係る文書に対する例外

・1988 年プライバシー法

機密情報に係る証書（Deed of Confidentiality）[235]

商業上の機密情報の取り扱いに対する懸念に応える形として、機密情報に係る証書を策定している。この証書は TISN の信頼性と透明度の高い環境の中におけるセーフティネットとして機能している。具体的には以下の事項について規定している。

①情報共有

TISN 内における情報共有を容易にするとともに、TISN 参加企業が法律に抵触しないように配慮がなされており、商業的機密情報の使用に関して強固な防衛策を敷くことを主な目的としている。

②法的義務

証書は TISN 参加企業が、各企業のセキュリティ手順及び脆弱性の提供を行う際に、2001 年会社

[235] http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/About_the_TISN

法（Corporations Act 2001）及びオーストラリアの証券取引所の上場規則に対して準拠するように配慮されたものである。オーストラリアの会社法及び証券取引所の上場規則の中では、株価に具体的な影響を及ぼす可能性のある情報は投資家に開示する義務がある。また非上場企業であっても、株価に影響を与える情報については ASIC に提供することが要求される。ただし上場規則の中には、免除規定があり、この証書は TISN において扱われる情報に対してその「免除」を適用させようとするものである。参加者は他の参加者がこの証書に署名したということに同意した上で TISN の活動に参加することが求められる。ただし、共有されている情報の正確性は会社法と上場規則の免除になるかの非常に重要な観点であり、個々の情報に対する分析は個々の企業によって行われる必要があるとしている。

③証書の構造

機密情報の受取人のみが、証書の当事者となる平型捺印証書の構造となっており、これによって機密情報を不当なプロセスを経ずに管理することができる。一般の契約では当事者でない人は契約内容の対象とはならないが、この構造の場合は当事者でない人間であっても証書に基づいて訴訟を起こすことができる。つまりこの証書への署名は署名者が TISN の中で共有される情報の機密性を維持するために、他の全ての証書の署名者と契約を結ぶという形式となる。情報の公開者は情報の受取者に対して直接的な契約関係にあり、守秘義務に関する違反があった際には直接訴えることができる。そもそも、TISN への参加は任意であり、提供する情報の判断も参加者の判断に任されている。そのため、この証書によって情報の強制的な提供を求められることはない。

④機密情報について

TISN の中で共有される全ての情報が機密情報であるということではない。この証書は情報が機密性を保つことが必要で、その配布が制限されなければならない際のみに適用される。つまり、この証書は機密情報ではないものには適用されない。この証書が守るべき機密情報は、一般的には機密情報であり、TISN の参加時にのみ利用出来るようにされている情報である。ちなみに、ここでの機密情報の定義は連邦政府の Protective Security Manual (PSM)に規定される「機密情報」とは異なる。PSM の機密情報は TISN で扱われるような商業的な情報というよりは、国家機密のようなものである。TISN の相互依存性に関する調査結果によっては全ての参加者に関係する情報については、証書に署名しなかった参加者には共有されない可能性がある。

⑤一貫したアプローチについて

AGD は証書に対する一貫したアプローチを保証する。証書が情報の機密性を維持するために一定の義務を参加者に課していることから、AGD も首尾一貫した姿勢が必要となる。そのため証書の変更が必要な場合は参加者全員の同意を得る必要がある。企業が証書への署名を拒否した場合でも個人として署名をすることもできる。ただし、その場合その個人が知り得た情報を所属する企業内で共有することはできない。

⑥政府代表について

この証書は民間部門の構成員のみに適用される。政府代表者は情報の取り扱いに対する、より広範囲な法令への遵守義務があるため署名を要求されない。ただし、TISN に参加する全ての政府代表者は「政府代表者機密確認事項」に署名することが要求される。

5.3.2. オペレーションレベル

5.3.2.1. 組織

(1)Trusted Information Sharing Network for Critical Infrastructure Protection (TISN)[236]

政府及び民間の重要インフラに影響を及ぼすセキュリティ問題に関する情報を一括して収集することを目的とした情報共有組織であり、以下の 9 グループ(分野)にまたがっている。オーストラリア政府の重要インフラに対する役割と責任は、研究開発及び技能基盤を含む情報セキュリティ保護に対する国家能力の強化としている。また TISN 内には DBCDE が事務局として組織された Information Technology Security Expert Advisory Group (ITSEAG)と Communications Sector Infrastructure Assurance Advisory Group (CSIAAG)という 2 つの特別グループが設置されている。

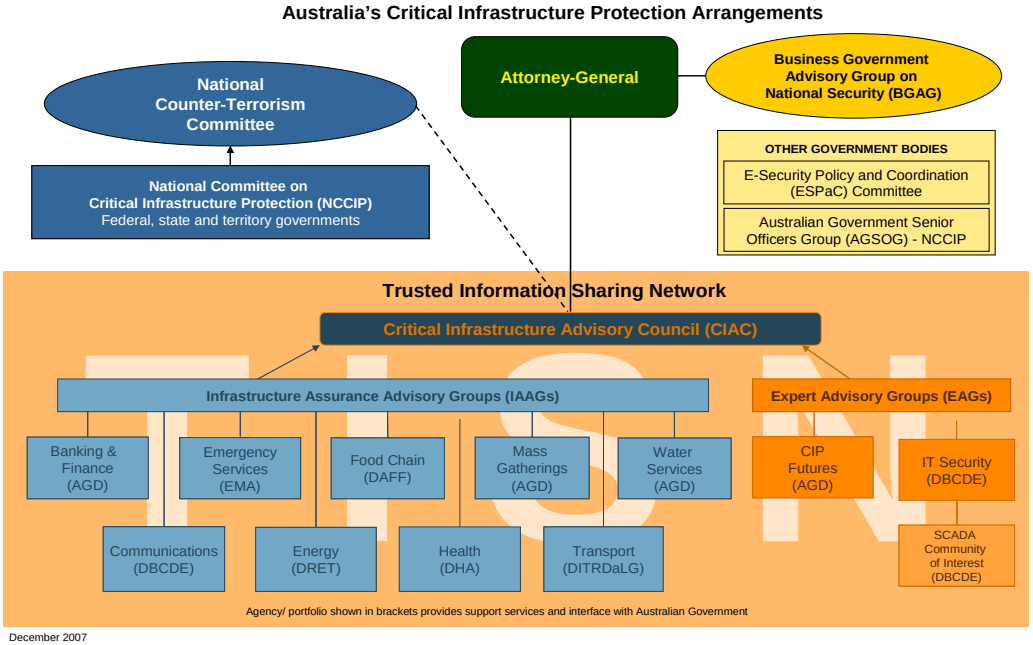


図 5-4 TISN の組織図[237]

[236] http://www.tisn.gov.au/

[237] http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(E794A048FF84C896A06E1D7EC63DF5A4)~TISN+diagram+Dec+07.pdf/$file/TISN+diagram+Dec+07.pdf

（TISN の 9 分野）

- 金融分野
- 緊急時対応分野
- 食品チェーン分野
- 大衆集会分野
- 水道分野
- 通信分野
- エネルギー分野
- 医療保健分野
- 輸送分野

①Information Technology Security Expert Advisory Group (ITSEAG)

グループに対して非定期に公表されるレポート等によって重要インフラにおける IT セキュリティに関わる情報を提供する。ITSEAG は国内の IT セキュリティベンダや研究機関、さらに IT／e-security の分野における政府の代表者によって構成される。過去にはワイヤレスセキュリティ、VoIP アプリケーションにおけるセキュリティ、DDoS 攻撃、IT セキュリティガバナンス等に関するガイダンスを提供してきた。現在は IT サービスプロバイダに対してアウトソーシングを行う際の IT セキュリティマネジメントや SCADA システムの向上に関するプロジェクト等が遂行されている。ITAESG が Brisbane, Sydney, Melbourne, Adelaide, Perth の 5 都市で開催した National SCADA Workshop では SCADA システムを保有する重要インフラ事業者等合計 326 人が参加し、SCADA システムの知識やスキルを共有するとともに、脆弱性に関する注意喚起を行った。オーストラリアの SCADA に関する情報共有ポータルとして SCADA COI information portal（http://www.scadacoi.com.au/）というサイトが整備されていたようだが現在はアクセス出来ない状態となっている。

②Communications Sector Industry Assurance Advisory Group (CSIAAG)

情報通信分野に関連するセキュリティに関する情報を収集する。リスクマネジメントフレームワーク（RMF）との連携によってオーストラリアの重要インフラにおけるリスクや脆弱性の検討を行う。また RMF の中で指摘されたリスクを想定したシナリオを基礎としたの机上演習等を実施している。現在はリモートアクセスにおけるセキュリティや放送分野の事業継続に関する机上演習等のプロジェクトが実施されている。

(a) 情報共有の担保方法・ルール

TISN ではメンバ間における情報共有について、法的な論点において関係省庁を含めて検討を行っており、それらの検討の一部を反映する形で、Deed of Confidentiality を整備している。

(2)Australian Computer Emergency Response Team（AusCERT）[238]

クイーンズ大学内に設置されているコンピュータ事故対応チームである。連邦政府からの資金援助を受ける非営利・独立組織である。セキュリティ対策のための情報収集、分析、提供を行っている。1992 年に設立された最も古い CSIRT の 1 つであり、オーストラリア内におけるインターネット侵害事故対応の国際窓口としての役割を担っている。

（AusCERT の提供するサービス）

- 早期警戒サービス
- メンバ限定のウェブサイトコンテンツ
- セキュリティ情報のメール配信サービス
- メンバ限定のフォーラムへの参加
- インシデントマネジメントサービス
- 脅威、脆弱性監視・分析・注意情報の配信

(3)Computer Network Vulnerability Assessment Program（CNVA）

GovCERT.au によって運営されているプログラムであり、重要インフラ事業者に対して、重要インフラの情報システムの中の脆弱性や攻撃を受けた際の体制についてアセスメントを行うことを推奨し、ファンディングを行うことを目的とする。CNVA 側でもネットワーク脆弱性アセスメントの専門家をコンサルタントとして設置しており、プログラムへの応募者に対してサポートを行っている。
プログラムの成果は AGD に提出され機密情報として取り扱われることになっているが、参加者側の承諾が得られれば、機微な情報を含まない形で、オーストラリア政府の中の認識向上のための材料として活用される。[239]

5.3.2.2. National CSIRT と ISP との関係

オーストラリア政府と ISP との直接的な連携として、以下の AISI の活動が挙げられるが、このイニシアチブにおいて AusCERT は直接的な関与はしていない。

(1)The Australian Internet Security Initiative (AISI)[240]

2005 年 11 月、オーストラリア通信局と国内の 6 つの ISP（BigPond, OptusNet, Westnet, Uecomm, Pacific Internet, West Australian Networks.）によって設立された、国内のボット等のマルウエア感染を減らすための活動を行っている。AISI では 24 時間体制でボットネットの監視を行い、ボットに感染したコンピュータのインターネットアドレスを ISP に提供する。ISP は提供されたリストからコンピュータの持ち主に連絡し、改善策の助言を行う。そこで、問題が解決されない場合には ISP ごと

[238] http://www.auscert.org.au/
[239] http://www.ag.gov.au/www/agd/agd.nsf/Page/GovCERT_ComputerNetworkVulnerabilityAssessmentProgram
[240] http://www.acma.gov.au/WEB/STANDARD/1001/pc=PC_310317

に定めた Acceptable Use Policy（AUP）[241]の下で、ネットワークを遮断することができる。2006 年の試験プログラムを経て、新たに 19 の ISP が加わり活動を続けている。AISI では今後も参加する ISP の数を増やす意向で、HP 上で ISP に参加を呼びかけている。この活動への ISP の参加は無料となっている。

（AISI に参加している ISP）

・ AAPT	・ EZ ADSL	・ Nowires Pty Ltd
・ Access Net Pty Ltd	・ GCOMM	・ OneWire
・ Adam Internet	・ Global Dial	・ Optus Internet
・ Albury Local Internet Pty Ltd	・ Grapevine	・ Overflow
・ All Hours Communications	・ HaleNET	・ Pacific Internet (Australia)
・ AOL	・ Highway 1	・ Reynolds Technology
・ Aussiewide Internet	・ Hotkey	・ Riverland Internet
・ AUSTARnet	・ HugoNET	・ (The) Smelly Black Dog Company
・ Bekkers	・ IDL Internet	・ Soul Communications
・ Bendigo Community Telco	・ iiNet	・ Speedweb Internet
・ Central Data	・ Internode	・ Spin Internet
・ Chariot	・ IntraPower	・ Telstra Bigpond
・ Chilli Internet Solutions	・ iPrimus	・ TPG Internet
・ Comcen	・ ispONE	・ TSN Communications
・ Dodo Australia	・ KDDI Australia	・ Uecomm
・ Dreamtilt	・ Neighbourhood Cable	・ Unwired
・ EscapeNet	・ Netspace	・ West Australian Networks
・ Exetel Pty Ltd	・ NetYP	・ Westnet
	・ Nextep	・ Wideband Networks

5.3.2.3. 官民連携体制

民間の情報セキュリティインシデント対応を行う AusCERT はオーストラリアの代表的な CSIRT として位置づけられており、その活動に対して連邦政府から資金援助を受けている。ただし、活動の内容として国家の重要な情報システムに対してネットワーク情報の脅威や脆弱性を警告や情報提供する機能を有するが、政府内部において情報セキュリティインシデント対応に直接関与することはない。

（AusCERT と GovCERT.au について）[242]

2008 年 6 月に AusCERT が公表した“Review of Australian Government's e-Security Arrangements AusCERT Submission”において、AusCERT と GovCERT.au の役割についてコメントが出されている。その中では、GovCERT.au の機能について①海外の危機対応チームのリアゾン、②オーストラリアのサイバーセキュリティにおいて、重要インフラやビジネス分野の係る部分の調整、③オーストラリアの重要インフラ防護の観点による政策に対する助言等の機

[241] ネットワークを利用する際の利用目的を制限する規則。ボット等悪意のある目的でのネットワークの利用を制限する。

[242] www.auscert.org.au/download.html?f=286

能が挙げられているが、①におけるビジネスに対する両者の機能が重複している点、また GovCERT.au が一般的な National CSIRT が持つべき、セキュリティ脅威の監視・助言機能や、オーストラリアの組織がサイバー攻撃を受けた際の対応(現在は実質的には AusCERT が担当)、セキュリティ脅威や攻撃に対する分析機能を持たない点を指摘している。その上で、CSIRT 組織は政府や民間の各分野、ISP やアンチウイルスベンダ等の様々な関係者を取り込んだ分野横断的組織であるべきで、その意味でも AusCERT は CSIRT コミュニティの中で 15 年以上の活動実績があり、国際的にも「National CSIRT」として広く認識されていると主張している。提案として、オーストラリア政府は e-Security 戦略の中で、現在の状況を把握し、2 つの組織の役割を明確に定義すること、オーストラリアの National CSIRT を海外に対する 1 つに統一するべき(AusCERT に National CSIRT の機能を持たせる)としている。具体的な解決策として、国家のサイバー脅威や脆弱性を取り扱うフレームワークである Joint Operating Arrangement (JOAs)に、オペレーション担当として AusCERT が参加すべきと主張している。

6. シンガポール

6.1. 情報連携のフレームワーク

6.1.1. 情報セキュリティ関連組織

シンガポールでは、情報通信開発庁（IDA）が情報通信に関する政策、規定の立案から策定、重要インフラ防護、また民間部門との連携に至るまで、シンガポールにおけるICTに関する施策を主導する立場にある。IDAの下に設置されたNCMCは政府機関のネットワークのSOCとして2006年より運用が開始されている。

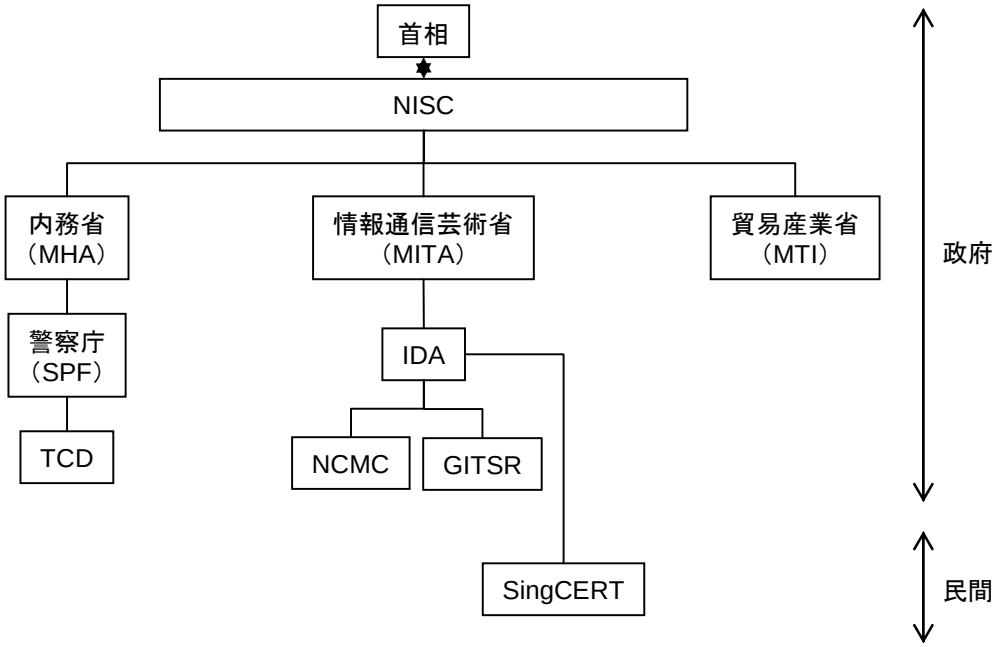


図 6-1 シンガポール情報セキュリティ関連組織

(1)情報通信開発庁（IDA：InfoComm Development Authority of Singapore）[243]

1999 年に国家コンピュータ委員会（NCB：National Computer Board）とシンガポール通信局TAS：Telecommunications Authority of Singapore が合併する形で設立された。現在は情報通信技術・芸術・文化庁（MICA）傘下の組織となっている。NISC と協力し、シンガポールにおける情報通信及び施策の具体化及び実施に当たって中心的役割を果たす。主要な業務はシンガポールにおける競争的 IT 産業の育成を行うことであるが、シンガポール政府の最高情報責任者（CIO）としての役割も担っており、InfoComm Security Division (iSec)では、公共機関における ICT セキュリティ対策実装の監視を行っている。民間企業に対しては ICT 標準を整備することで、企業の情報セキュリティの向上を図っている。

[243] http://www.ida.gov.sg/home/index.aspx

(2)国家情報通信セキュリティ委員会(NISC:National InfoComm Security Committee) [244]

国家レベルでサイバーセキュリティに対する政策や戦略的方針を策定する機関として設立された。各政府機関からの出向者で構成されている。NISC の事務局は IDA 内に置かれ IDA が事務局運営の役割を担っている。

(NISC に人材が出向している政府機関)

- 内務省(Ministry of Home Affairs)
- 国防省(Ministry of Defense)
- 情報通信・芸術省(Ministry of Information, Communication and the Art)
- 財務省(Ministry of Finance;)
- DSO 国家研究所[245]
- 国防科学技術庁(DSTA:Defense Science and Technology Agency)

(3)シンガポール警察技術犯罪部門(Singapore Police Force, Technology Crime Division:TCD)[246]

シンガポール警察犯罪調査部門の一組織として設立された。コンピュータ不正使用禁止法(Computer Misuse Act)で規定されたサイバー犯罪の捜査、法的証拠の検査及び起訴を担当する。また、シンガポールの各警察支部に対して、高度犯罪の調査のための分析やフォレンジックサービスを提供する。特に高度な分析を要する事案に関しては、科学技術犯罪捜査班(TCIB:Technology Crime Investigation Branch of the Singapore Police Force)で捜査が行われる。

6.1.2. 法執行機関、防衛機関、情報機関の位置づけ

政策の面では情報セキュリティに関する取組は一貫して IDA によって主導されている。オペレーションの面では、IDA の NCMC が監視情報収集、インシデント対応を行うが、サイバーテロ等の犯罪行為の捜査、立証については、シンガポール警察技術犯罪部門の TCD が担当しており、NCMC が TCD に対して関連する情報を提供する。

---

[244] http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663

[245] DSO National Laboratories:国防省下の国家研究所。900 名以上の研究者を抱える。(http://www.dso.org.sg/)

[246] 244 と同じ。

6.1.3. 情報連携の分類

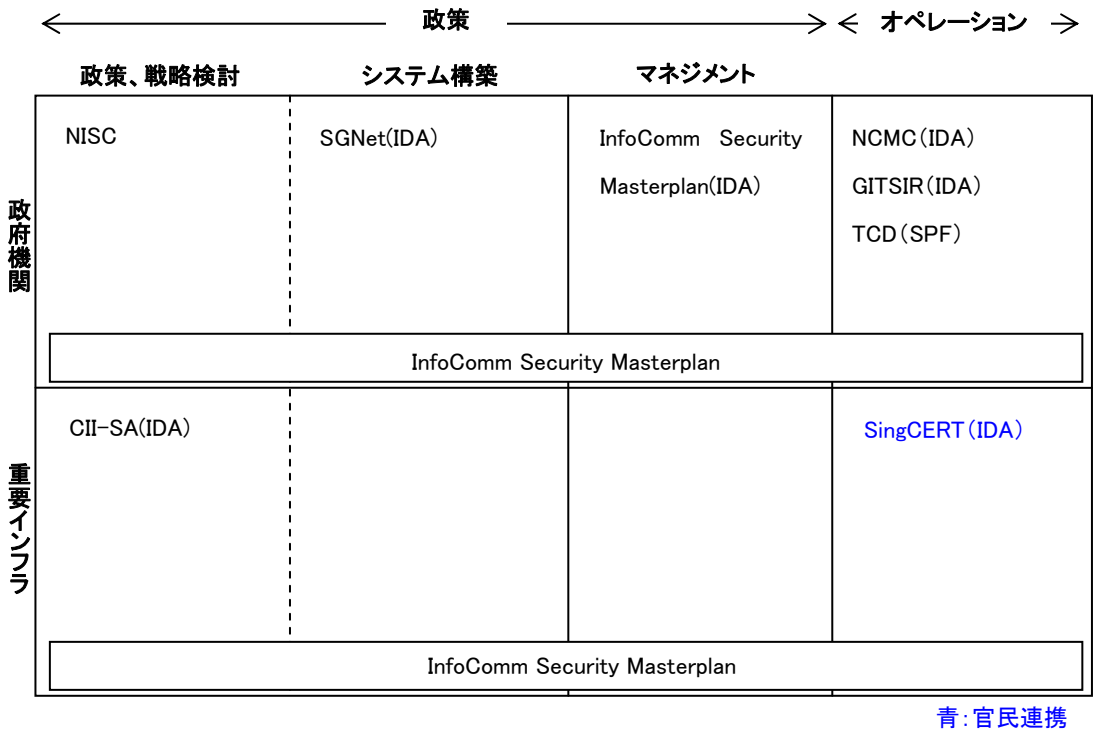


図 6-2 シンガポールにおける情報連携のフレームワークの分類

6.1.4. 情報連携の関係図

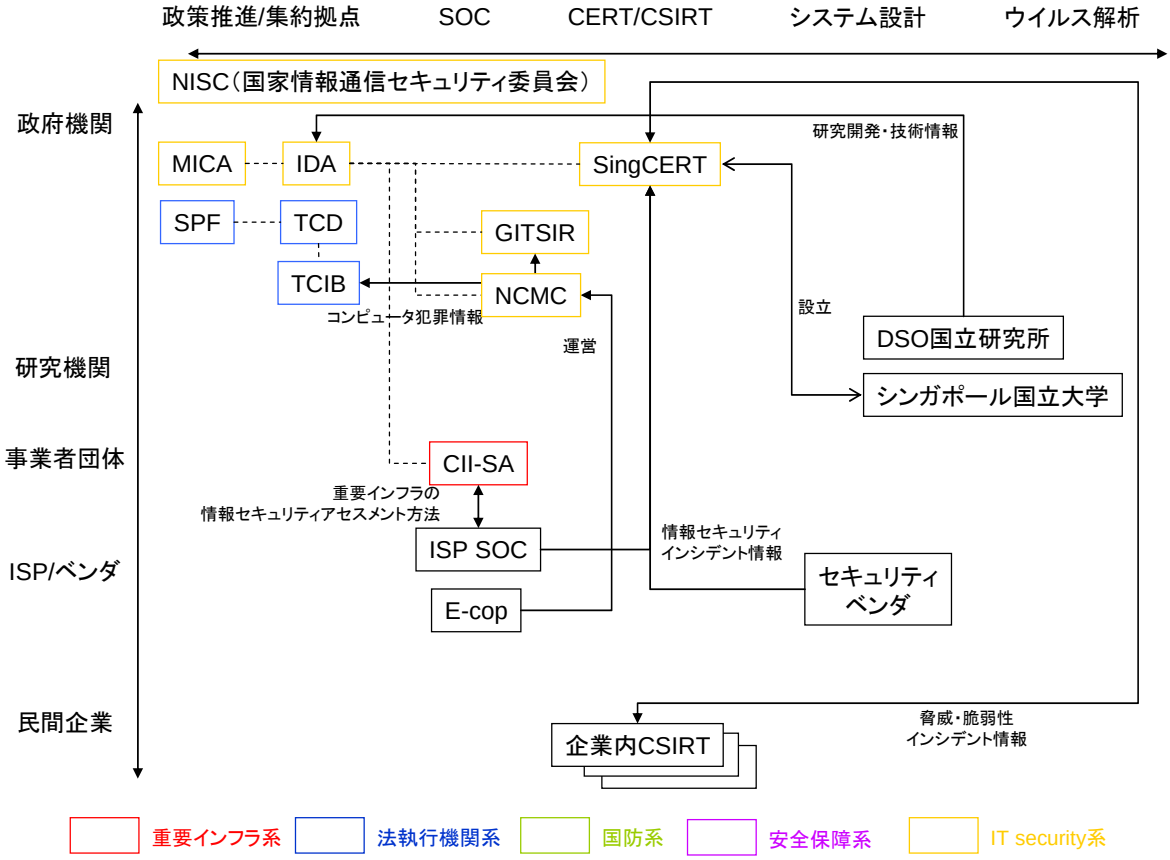


図 6-3 シンガポールにおける情報連携の関係図

6.2. 政府機関における情報連携

6.2.1. 政策レベル

6.2.1.1. 政策・戦略検討

シンガポールにおける情報セキュリティに関わる取組は、全て IDA 主導の下に決定されている。その方針を示したのが、2005 年に公表された“InfoComm Security Masterplan”である。

(1)InfoComm Security Masterplan（2005-2007）

国家全体としてのサイバーセキュリティの確保を目的として 2005 年に策定された。3 年間の予算は 3,800 万シンガポールドル（約 23 億円）[247]である。具体的な施策としては国民の意識向上プログラム、国家認証基盤の構築、コモン・クライテリア(CC)認証スキームの確立等を示しており、以下の 7 つのプログラムを実施することとしている。

[247] 1 シンガポールドル＝60 円で計算。

（InfoComm Security Masterplan 2005-2007 で示されたプログラム）

- サイバーセキュリティ意識向上プログラム（個人向け）
- 国家認証基盤の整備
- CC（Common Criteria）認証スキームの確立
- 事業継続対策評価フレームワークの確立
- セキュリティスコアカード制度（政府機関の情報セキュリティの状況に対する評価制度）の確立
- NCMC の設立
- 国家重要インフラの情報通信に関わる脆弱性の調査

6.2.1.2. システム構築

(1)Singapore Government Network（SGNet）

2000 年シンガポール政府ネットワークとして構築が開始され、入札の結果 Newbridge Networks 社がサービス提供権を取得した。政府ネットワークにはほぼ全ての政府機関が接続されており、各種電子行政サービス、職員の IC カードの認証システム等も SGNet を基礎として構築されている。セキュリティに関しては Newbridge 130 Secure VPN Client、 Newbridge 830 Secure VPN Management Suite、Newbridge 230 series of Secure VPN Gateways 等 VPN の技術が導入されている。

6.2.1.3. マネジメント

(1)InfoComm Security Masterplan （ISMP）2005-2008[248]

政府機関情報セキュリティに対しては、InfoComm Security Health Scorecard(公共部門における情報セキュリティ状況を把握し、共通の問題等を特定・改善するためのスコア付け制度)等が示されている。

6.2.2. オペレーションレベル

6.2.2.1. 組織

(1)国家サイバー脅威監視センター（NCMC：National Cyberthreat Monitoring Center）

“InfoComm Security Masterplan”に基づき、政府のネットワークと情報セキュリティを強化するために設立された政府のネットワークを 24 時間 365 日体制で監視する組織。サイバー攻撃を分析することに特化したサイバー脅威分析センター（TAC）及びリアルタイムのサイバーセキュリティ検知を行うサイバーウォッチセンター（CWC）の 2 つの組織で構成される。緊急的な対応が必要となる脅威が報告された場合、進行中の攻撃が検知された場合は、関連する組織に対して対処方法と再発防止策が通知される。事件間の相関分析技術（Security Events Correlation Technology）等の最先端技術を備え、政府のオンラインサービスに対するサイバー攻撃に対しても、摘発を行

[248] http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663

う。

CWC は専任のセキュリティエンジニアとアナリストの 12 名のスタッフから構成される。実際の運営はシンガポールのセキュリティベンダ e-Cop[249]社が 2006 年～2010 年の 5 年契約を約 11 億円で請け負っている。[250,251]

(2)GITSIR (Government IT Security Incident Response Team)[252]

政府機関に対するサイバー攻撃に関する情報を収集するために IDA の下に設置された組織。情報収集に際してはTCDの科学技術犯罪捜査班(TCIB:Technology Crime Investigation Branch of the Singapore Police Force)の協力を得ることもある。ただし現在ポータルサイト(http://gitsir.ida.gov.sg/)へのアクセスが無効になっているため、現在も組織として存続しているかは不明である。

6.2.2.2. 職員

シンガポールの政府機関 SOC として稼動し始めた NCMC では民間ベンダの e-cop 社に実際のオペレーション業務をアウトソーシングしており、職員も民間の人材を利用している。

---

[249] マネージドセキュリティサービス、セキュリティに関するコンサルティングサービスの業務を行う企業。タイやインド等アジア地域で広く SOC を展開。

[250] http://www.infocommsingapore.sg/home/index.php/web/success_stories/e_cop_awarded_contract_to_develop_cyber_watchcentre_cwc_for_singapore_government

[251] http://www.zdnetasia.com/techguide/security/0,39044901,39434719,00.htm

[252] http://www.clair.or.jp/j/forum/compare/pdf/0607-4.pdf

6.3. 重要インフラ防護における情報連携

重要インフラ防護に関しては、NISCとIDAが中心的組織として機能している。シンガポールにおける重要インフラ防護の方針は“InfoComm Security Masterplan”の中で示されており、2008 年の新マスタープラン発表に際してNISCの議長が行った講演では、重要インフラ防護における官民連携の重要性について強調している。

6.3.1. 政策レベル

6.3.1.1. 政策・戦略検討

(1)National Critical Infrastructure Assurance (NCIA) Program[253]

重要インフラにおける脆弱性解析、またはそれに対応する対策を実行する目的で 2002 年に策定された。またこのプログラムは重要インフラ防護における官民連携体制の支援機能としての役割も持つ。

6.3.1.2. システム構築

本調査では、特に確認できなかった。

6.3.1.3. マネジメント

重要インフラに対する細かい規定は定められていないが、国家の重要インフラ防護に対する取組の大枠の方向性は Information Security Masterplan の中で示されている。

6.3.2. オペレーションレベル

6.3.2.1. 組織

(1)SingCERT（Singapore Computer Emergency Response Team）[254]

シンガポールにおける National CSIRT であり、1997 年に情報通信開発庁（IDA）のプログラムとしてシンガポール国立大学と共同で設立され、現在は IDA の一組織として活動している。ハッキングやコンピュータウィルスなどの情報セキュリティに関して発生したインシデント情報を民間企業等から収集・分析し、ホームページやメーリングリストによって公開する。SingCERT の主な活動内容を以下に示す。

（SingCERT の活動内容）

- セキュリティパッチに関する情報の配信
- セキュリティ講習やセミナー、ワークショップを通じたセキュリティ啓発活動
- セキュリティインシデントの解決におけるベンダや他 CERT 組織との連携

---

[253] http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663

[254] http://www.singcert.org.sg/

（インシデントレポートに含めるべきとされている情報）

1.人命に関わる活動

2. 以下に示すようなインターネット上のインフラに対する攻撃

－ルートネームサーバ

－ドメインネームサーバ

－主要なアーカイブサイト

－ネットワークアクセスポイント

3. インターネットサイトに対する広範囲な自動攻撃

4. 新しい脅威に対する新たな攻撃手法

(2)Critical InfoComm Infrastructure Surety Assessment（CII-SA）[255]

シンガポールの情報及び通信インフラの情報セキュリティのアセスメントを評価するために IDA によって開始されたプロジェクト。国内の重要インフラ事業者のシステム担当者が一緒に検討を行うためのプラットフォームとなっている。

6.3.2.2. National CSIRT と ISP の関係

National CSIRT である SingCERT に対して、ICT ベンダ、セキュリティベンダ、ISP からネットワーク上の情報セキュリティインシデント情報が提供される。それらの情報は SingCERT に収集・分析された上で、SingCERT の HP[256]上で公開されている。

6.3.2.3. 官民連携

シンガポールでは、重要インフラ防護に関わる取組も IDA 主導の下で推進されており、情報共有を行う官民連携体制は存在しない。

[255] http://www.ida.gov.sg/Programmes/20060925100740.aspx?getPagetype=36

[256] http://www.singcert.org.sg/

7. 韓国

7.1. 情報連携のフレームワーク

7.1.1. 情報セキュリティ関連組織

韓国では 2008 年 2 月に李明博政権の政府機関の大規模な組織改編によって、情報セキュリティに係る組織の構造も変化した。大きな変化として、情報通信部（MIC）が廃止され、その機能は公共政府安全部（MOPAS）[257]、韓国知識経済部（MKE）[258]、放送通信委員会（KCC）[259]に引き継がれた。

韓国では政府機関、民間部門の情報セキュリティ、重要インフラ防護等情報セキュリティに関わる施策は前 MIC によって全体的な指揮がとられており、MIC の下部組織であった KISA が実務対応を行っていた。今後政府機関の情報セキュリティは MOPAS、認証等の技術的な部分や研究は KCC の機能として移行されると考えられる。

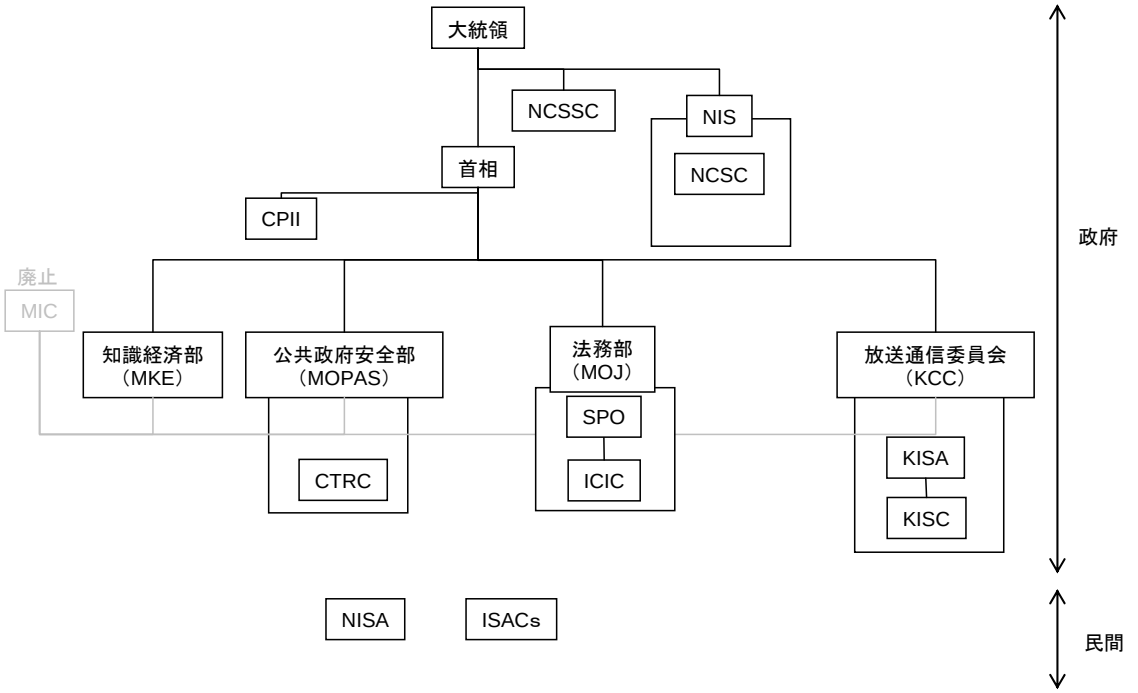


図 7-1 韓国情報セキュリティ関係組織

[257] Ministry of PublicAdministration and Security

[258] Ministry of Knowledge and Economy、情報通信部、科学技術部、財政経済部の機能を統合して 2008 年 3 月に発足。自動車、造船、鉄鋼、石油化学、機械の 5 代主力産業の付加価値を高めるとともに、サービス産業、バイオ、ロボット、太陽光発電等の新産業を新たな成長エンジンとして育成することを目指している。

[259] Korea Communication Commission、韓国放送通信委員会：2008 年 2 月「放送通信委員会の設置及び運営に関する法律」を基づき設立。米国の連邦通信委員会（FCC）をモデルにしており、放送、通信、周波数に関する各種政策立案を行う。

(1)国家情報院(NIS:National Intelligence Service)

1961 年に韓国の諜報機関として設立され、同じく諜報機関である中央情報部(KCIA)を前身とする大統領の直轄組織。国家・公共部門における安全保障に関わる業務を総括する。情報システムのセキュリティ対策の計画、調整、政策策定及び国家・公共部門を対象とした情報システムの対策支援、重要インフラ保護、情報セキュリティシステムの認証等を主な業務内容とする。情報通信基盤保護法及びその施行令により国家保安業務機関として指定されており、国家機関または地方自治体の長及び情報通信基盤保護委員会の委員長が重要インフラ施設の保護の必要性を認めた場合、対象とする重要インフラ施設に対する保護対策の確立、侵害予防及び復旧業務に対する技術的支援を要請される。

(2)National Cyber Security Strategy Council (NCSSC)

2004 年に公表された国家情報セキュリティ基本方針に基づいて設置された大統領直轄の委員会。サイバー攻撃に対する国家レベルの総合的かつ体系的な対応力を強化するため、国家サイバー安全政策を策定すると共に、情報セキュリティの関連制度に関する検討を行っており、国家全般のサイバーセキュリティ政策の総合的な調整を行っている。

(3)Ministry of Public Administration and Security (MOPAS、前 MIC)

2008 年の行政改革の結果、電子政府の担当省庁と公共サービスの省庁が CIIP(後述)を含めた韓国における情報セキュリティ政策の中心的な役割を担うこととなった。具体的には MOPAS 内の情報化戦略オフィスが情報セキュリティに係る事案を取り扱うこととなっている。MOPAS 情報化戦略オフィスの主な機能としては以下が挙げられる。

(MOPAS 情報化戦略オフィスの機能)

- 民間企業向けの情報セキュリティ政策の立案
- ユーザプライバシーの強化
- 電子認証
- 堅実なインターネット文化の醸成

(4)Korea Information Security Agency (KISA)

前 MIC の傘下にあった組織であり、インターネット上の事案対応支援、主要な情報通信インフラの脆弱性分析・評価、スパム対応、情報セキュリティ産業の支援、情報セキュリティ教育の促進等、国家レベルでの情報セキュリティ対策を総合的に推進する。

(KISA の機能)

- 情報セキュリティ政策及び制度に関する調査研究
- 暗号技術開発

・ 先進的システム及びネットワークセキュリティ技術の開発
・ 情報セキュリティ技術の標準化及び基準の開発
・ CC（Common Criteria）に基づいた情報セキュリティ製品/システムの評価
・ 電子署名認証管理
・ インシデント対応（CERT-CC/KR 及び Cyber118 の運営）
・ 重要インフラ保護支援
・ 個人情報保護のための対策研究
・ 人材育成（広報及び教育訓練）

7.1.2. 法執行機関、防衛機関、情報機関の位置づけ

情報セキュリティの全体的な施策は MOPAS や KCC によって実施されるが、政府機関の情報セキュリティ及び重要インフラ防護の中でも、特に国家・公共の安全保障に関わるサイバーテロ等に対する事案は NIS によって主導される。その際、サイバーテロの捜査や取り締りについては NPA の Cyber Terror Response Center(CTRC)が、立件に関する情報収集に関しては MOJ の Internet Crime Investigation Center(ICIC)が実務を行う。

7.1.3. 情報連携の分類

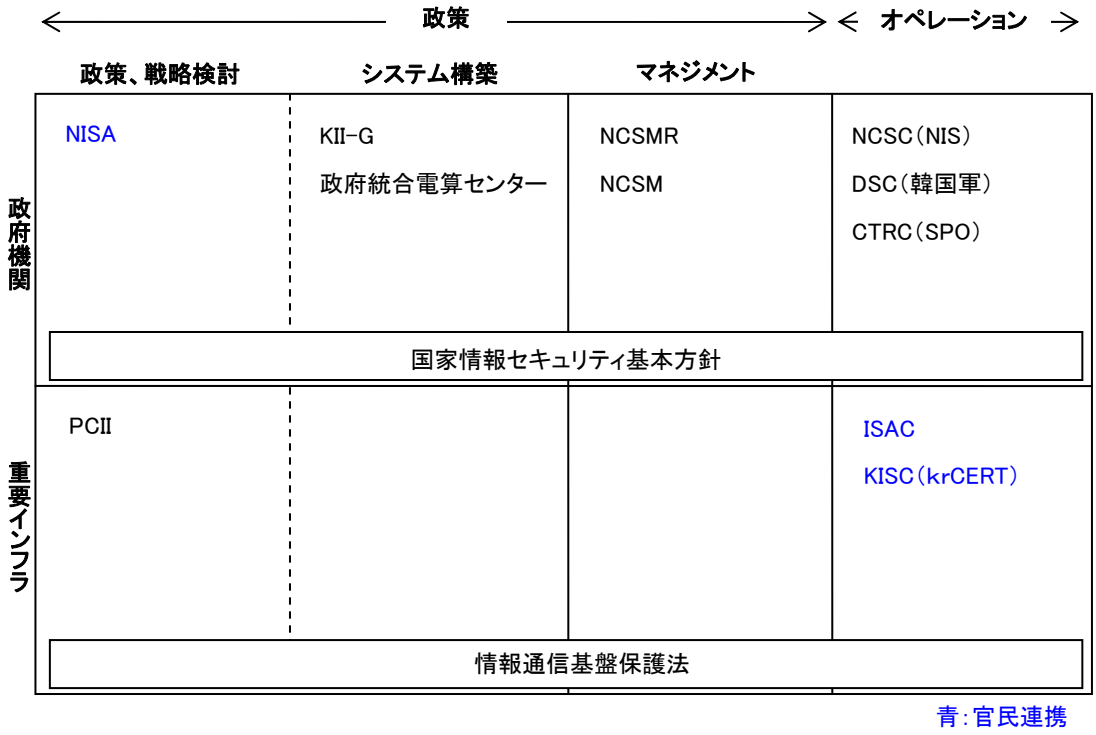


図 7-2 韓国における情報連携のフレームワークの分類

7.1.4. 情報連携の関係図

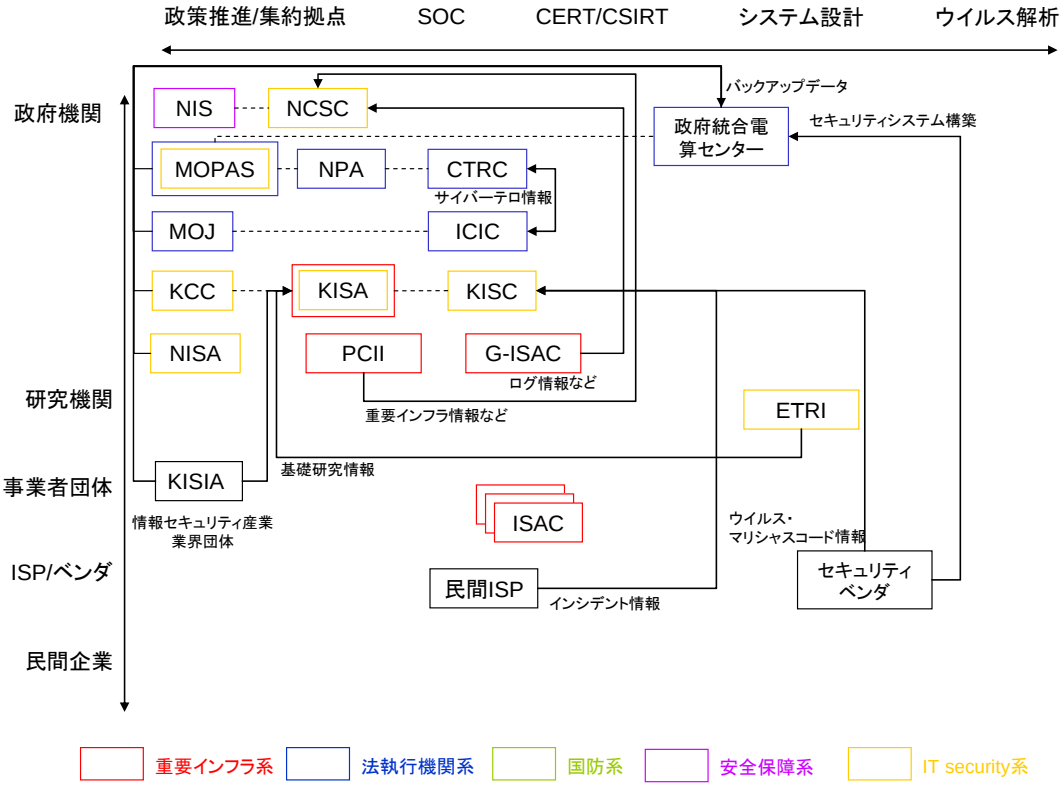


図 7-3 韓国における情報連携の関係図

7.2. 政府機関における情報連携

韓国の政府機関におけるセキュリティの基本方針は 2005 年に NIS から公表された国家情報セキュリティ基本方針の中で示されている。

(1)国家情報セキュリティ基本方針 (NCSMR：National Cyber Security Management Regulations)[260]

国家の情報システムのサイバーセキュリティ管理体制の整備と事案発生時の迅速な対応を可能にするために策定された基本方針。NCSSC、NCSC[261]の設置もこの基本方針の中で示された。中央政府の長に対してサイバー攻撃への対策の徹底を求めている。

7.2.2. 政策レベル

7.2.2.1. 政策・戦略検討

(1)国家情報保安協議会（NISA：National Information Security Alliance）

官民の情報共有や政策の立案、及び省庁間の連携を強化することを目的とした協議会。2002 年 4 月、国家情報院後援により、国家保安情報技術研究所（NSRI）が開催した「国家情報セキュリティ業務発展セミナー」において、効率的なサイバーテロ対応体制の構築のため、政府・公共機関をカバーする協議会の必要性が議論された。これを受けて同年 9 月、国家機関・公共機関・産学官の協力で情報セキュリティ協議会が結成され、これらの連合体として国家情報セキュリティ協議会が同年 10 月に発足した。事務局は国家保安技術研究院内に置かれている。NISA のメンバは、国家機関情報保安協議会、公企業情報保安協議会、産学官情報保安協議会から構成され、協議会間の協力関係を強化するために、各協議会の会長及び副会長から構成される役員会を設置している。 参加企業・参加者は、国防部、産業資源部等の 23 の国家機関の情報セキュリティ担当官 29 名、韓国電力、道路公団等 25 の機関の情報セキュリティ担当者 25 名、KT、韓国情報保護学会等の関係機関から 24 名が参加している。[262] NISA は情報セキュリティ関連省庁、企業の情報セキュリティ責任者、産業・教育・研究分野における情報セキュリティの専門家による重役会議のような位置づけとなっている。

7.2.2.2. システム構築

(1)韓国政府情報基盤（KII-G）[263]

1993 年に発表された韓国情報基盤計画（KII：Korea Information Infrastructure Initiative）のうち、国家情報通信網部分を担う事業で 1996 年より事業化されている。 1987 年、国家の電算化支援と行政電算網事業管理を目的に設立され、1995 年情報化促進基本法第 10 条を根拠法に、

---

[260] http://www.oecd.org/dataoecd/25/10/40761118.pdf

[261] National Cyber Security Center、130 ページ参照。

[262] http://www.ipa.go.jp/security/fy16/reports/korea_security/documents/korea_security_2004.pdf

[263] 262 と同じ。
http://www3.jpc-sed.or.jp/cisi/pdf_file/korea05.pdf

公共機関の情報化促進支援及び電子政府関連施策立案支援機関として機能することになった。1995 年～2000 年にかけて既に全国の 144 地域(国内の全通話区域)を、約 19,611km の光ファイバーケーブルと ATM 交換機により、伝送速度 155 Mbps～40Gbps で接続しており、政府機関、地方自治体、教育機関、研究機関等が回線を利用している。整備に当たっては、政府が通信事業者に構築目標を提示し、設備投資額を支給することにより構築した。整備費は 3,953 億ウォン(約 367 億円)となっている。

(2)韓国公用情報基盤(KII-P)

企業や各家庭等の一般国民が広く利用可能なブロードバンド情報通信サービス。需要と経済性を反映して、FTTH、xDSL、HFC(ケーブルインターネット)、衛星通信、3B-WLL(Broadband Wireless Local Loop)等様々な方式を採用し、全国的なブロードバンド通信網を民間投資により構築している。各通信事業者は、一般国民向けのブロードバンド情報通信サービスのバックボーンとして、超高速国家情報通信網(KII-G)のバックボーンを論理的に分割して利用している。韓国通信とデイコムは、KII-P の展開も考慮して超高速国家情報通信網(KII-G)の整備を行っている。

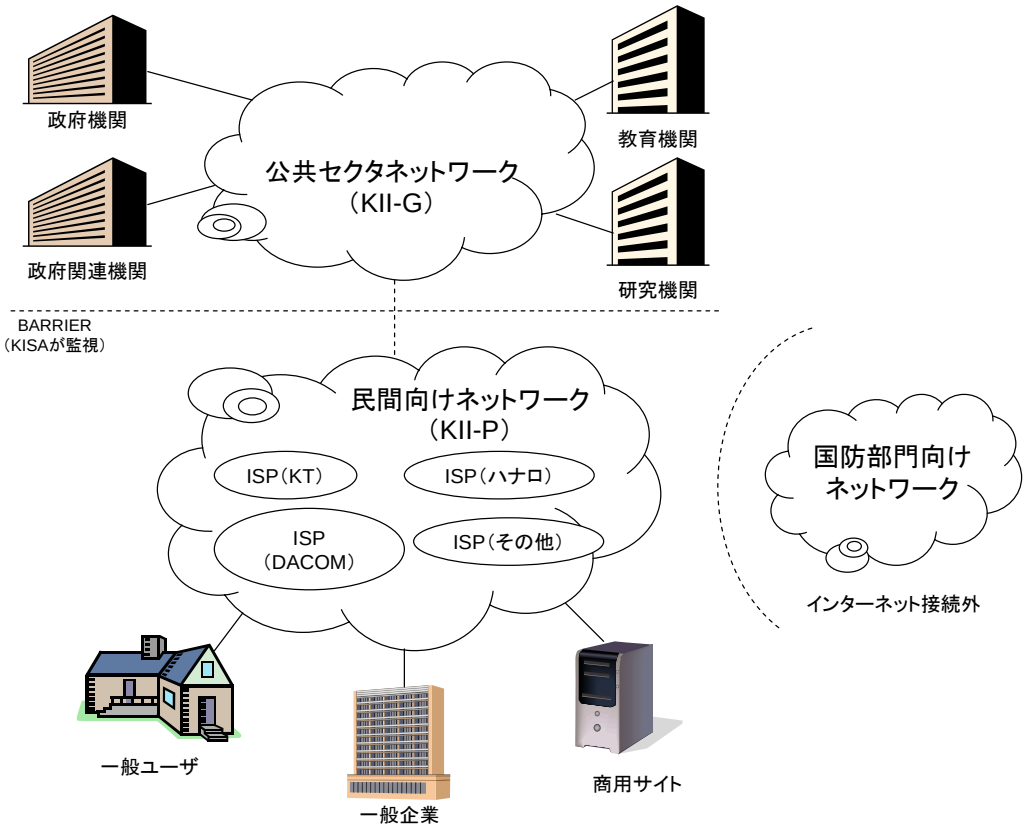


図 7-4 韓国における官民のネットワーク

(3)国家機関情報システムバックアップセンター

2001 年の米国同時多発テロを受けて設立された、情報通信部と行政自治部が共同で推進する

韓国政府の情報システムの共同バックアップセンター。2001 年から 2006 年の第 1 フェーズでは同時多発テロを契機に、幾つかの国家の重要システムの安全確保を効率的に行うため、急遽計画化されたものであり、2003 年から現在に至る第 2 フェーズでは、2003 年の電子政府ロードマップ及び 2004 年の基本計画に基づき、「政府統合電算センター構築事業」として実施されている。

政府統合電算センター構築事業では 48 の政府部署を 24 ずつ 2 つのグループに分け、各グループの保有するシステムを 2 つのセンター(大田市、光州市)に各々移転・運営させている。バックアップシステムには強固なセキュリティ対策を敷いてあるため、各情報システムの信頼性や、事業継続性を確保できる。また、政府機関の情報資源を統合することで、政府機関間の情報の共有及び効率性が向上することも期待されている。なお、センターのシステムの情報セキュリティ対策の調達は韓国のセキュリティベンダの Secuve が受注し、セキュア OS システム等を導入している。[264]

7.2.2.3. マネジメント

(1)国家情報通信セキュリティ基本方針

政府機関を対象とする情報セキュリティガイドラインであるが、詳細な内容は非公開となっている。

(2)National Cyber Security Manual(NCSM)

政府機関・自治体の情報セキュリティ担当者向けのサイバーセキュリティガイドライン。国家安全保障会議事務所、国防部、情報通信部、国家保安技術研究所、韓国情報保護振興院等との共同制作となっており、民間・公共・国防部門の情報システム管理責任者及びシステム管理者が状況別に正しく業務を遂行できるよう、実務指針としても危機対応マニュアルとしても活用できるものとなっている。図 7-5 に示すように平常時であっても NCMC を中心として国防情報戦対応センターやインターネット侵害事故対応支援センター等と脅威情報等を共有している。また、実際に事故が発生した際には、図 7-6 に示すように国家安全保障会議の指示の下に、NCMC が中心となり各組織間で状況が共有される。一方で、サーバやルータ、OS 等のシステム別のセキュリティ管理要領等の技術的な内容についても記載している。

[264] http://www.secuve.co.kr/pressroom/pressroom1_view.htm?idx=391&idx2=595(韓国語サイト)

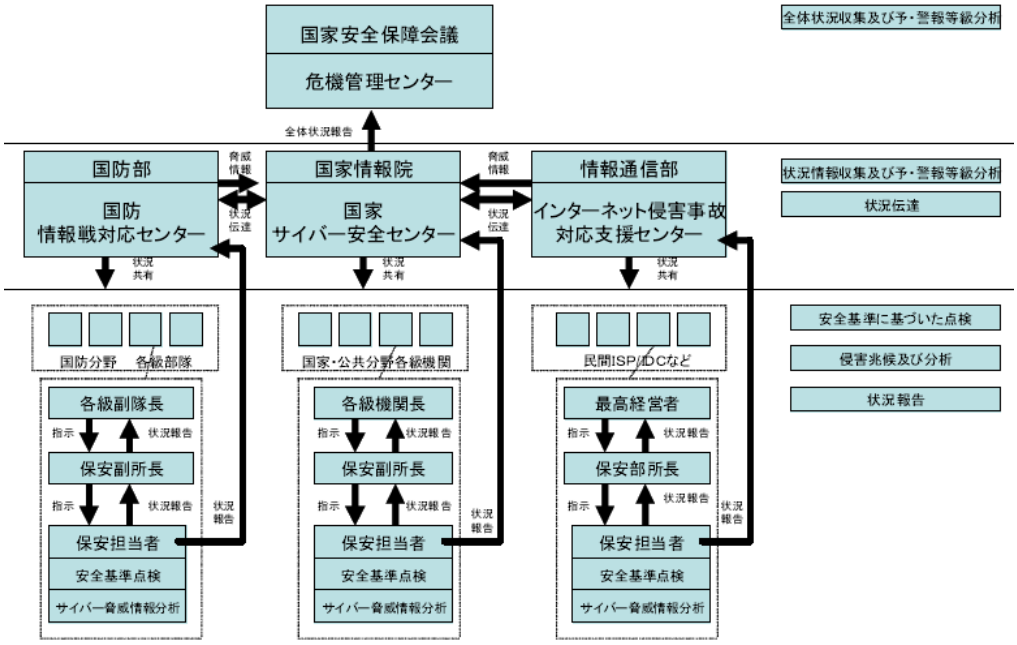


図 7-5　National Cyber Security Manual における平常時の業務フロー[265]

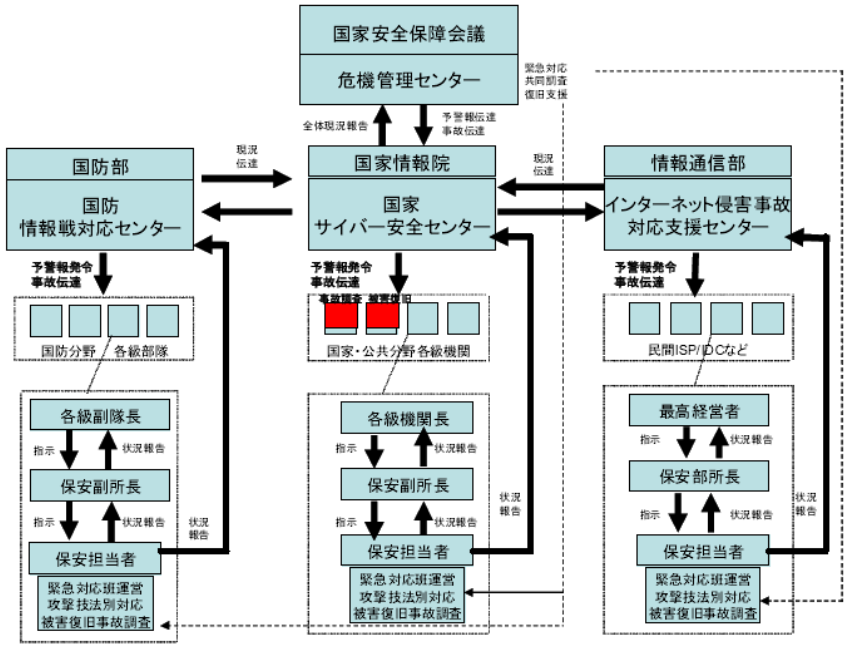


図 7-6 National Cyber Security Manual における事故発生時の業務フロー[266]

[265] 262 と同じ。
[266] 262 と同じ。

7.2.3. オペレーションレベル

7.2.3.1. 組織

(1)National Cyber Security Center (NCSC)

2004 年に公表された国家情報セキュリティ基本方針に基づいて設置された政府のサイバーセキュリティに関するオペレーションセンター。大統領直轄の情報機関である国家情報院の一部門として国家レベルでの情報セキュリティ政策の統括・調整、セキュリティ対策促進活動、サイバーセキュリティ上の脅威に関する情報収集、事案対処を行っている。

約 60 名の職員に加え、財政経済省、国防省、行政自治省、情報通信部、検察庁、警察庁、国家情報保護振興院、国家保安技術研究所から出向した専門家 14 人が勤務している。組織は 12 の大型スクリーンから国家情報通信網を 24 時間監視する「状況室」と関係省庁、KISA、NSRI から出向した専門家が常駐する「協力官室」に分けられる。「状況室」には 27 の主要電算網と 150 の国家機関を含む国家情報通信網への全てのサイバー脅威レベルが時間帯別に正常状態と比較されて表示される。危険度によって平時(緑)、注意(青色)、警告(黄色)、危険(赤色)の 4 段階で警報が発令される。「協力官室」には、行政、国防、通信、金融等、分野別の管制のための各省庁からの出向者及び KISA、NSRI からの出向者が常駐する。KISA は民間部門の支援、NSRI は技術面と研究開発の支援が主な役割となっている。[267]

NCSC の主な機能を以下に示す。

①サイバー安全予防活動

各政府機関の情報通信網の新・増設等政府機関の情報化の事業推進の際に、セキュリティに対する検討を実施する。また、具体的な活動としてはサイバー攻撃対応能力を強化するため、官・民・軍を結集してサイバー演習を実施している。さらに、国及び公共機関のネットワークで利用する情報セキュリティ製品の安全性検証のため、保安適合性の検証制度を運営している。

② 国家サイバー脅威に関する情報の総合収集・分析・発信

総合分析処理システムを運営し、政府機関のネットワークに対する不正侵入事故、トラフィック情報等を収集・分析する。脅威の兆しを探知した場合、政府機関に対して適切な対応を行うことで被害の最小化に努める。サイバー攻撃に対する体系的な対応のため以下の図のようにサイバー攻撃の危険度・被害規模等を考慮し、国家サイバー脅威の警報体系を設定している。

---

[267] 262 と同じ。

図 7-7 サイバー脅威段階別発令警報

③侵害組織での緊急対応、調査及び復旧

サイバー攻撃が発生した際には事故原因の調査と共に速やかな復旧を支援することにより、被害の拡散を防ぎ、システムを安定化させる安全診断等を通じて、類似事故の再発を防いでいる。サイバー攻撃による被害が深刻である場合、関係する中央行政機関と協議し政府合同調査及び復旧支援チームを構成・運営する。

④国内外サイバー脅威情報共有及び共助対応

米国、日本、ヨーロッパ等の各国と協力体系を築き、海外専門家の招請等を行っている。さらに、財政経済部、国防省行政自治部、旧情報通信部、法務部(最高検察庁)及び警察庁等国家保安技術研究所（KISA）と緊密な協力体制を維持している。

⑤サイバー脅威関連情報資料発刊

クラッキング、ワーム・ウイルス等、国内サイバー侵害事故についての一現況と事例を総合分析した『サイバー侵害事故の事例分析集』を発刊し、関連機関及び企業に配布している。

(2)国軍情報司令部（DSC：Defense Security Command）

国防省の対諜報活動を担当する組織。サイバーセキュリティに関連する機能としては以下が挙げられる。

①サイバー攻撃対応

国防省及び各軍の CSIRT と連携し、各軍に設置されている侵入探知システム及び侵入遮断システムから情報収集を行い、全軍のIPアドレスとその使用者をDB化しハッキング及びウイルスによる事故を早期に探知・対応している。遠隔制御・復旧、脆弱性診断デジタル証拠収集も行っている。

②インターネット上の事故への対応

国防省等、軍におけるインターネットホームページを対象とした攻撃の予防と国家サイバー安全センターに情報を提供している。

③国防分野侵害事故の発生時の緊急対応・調査及び復旧の支援

各種のサイバー脅威及び攻撃に対する保安勧告文及びワームやウイルス情報、情報セキュリティのニュース、攻撃事例及び情報セキュリティ資料等の国防サイバー安全関連情報を各軍に伝え、対策を講ずるよう支援している。また、攻撃発生時に軍の専門要員が事故原因の調査と迅速な復旧を支援している。

④国防情報セキュリティ学術行事の開催

KISA、高麗大と共同で約 800 名の情報セキュリティ専門家による国防情報セキュリティカンファレンスを催している。

(3)Cyber Terror Response Center (CTRC)

韓国警察下の組織。国内・海外におけるサイバーテロの事件追跡・捜査及び警報等の初動措置、サイバーテロの対応捜査機関としての役目を担当している。さらに、サイバーテロ申告受付及び相談、関係法令及び制度研究、国内・外サイバー捜査協力、サイバーテロ捜査、ハッカー動向把握、サイバー捜査企画及び指導、不法サイト検索、サイバーテロの予防及び捜査技法研究、サイバー捜査等を幅広く支援する。

(4)Internet Crime Investigation Center (ICIC)

新種のサイバー犯罪の捜査、動向把握、電子商取引を利用した詐欺、個人情報の侵害等のハイテク犯罪に関する情報の収集を行う。

(5)GISAC

国家主要情報資源の管理効率を高めるために、政府機関におけるサイバーインシデント対応を集約した政府機関の ISAC として 2002 年に設置され、現在は MOPAS が運用している。ウイルスやハッキング等、韓国政府ネットワークに対するサイバーテロが発生した場合、各政府組織機

関が独自に対応する既存の方式から一括監視へと対応体系が整えられた。調査・分析結果やログを NCSC に提供すること等で活動を支援している。

（GISAC の主な活動）

- サイバー攻撃に対する予防活動
- 情報セキュリティ事案発生時の対応及び支援
- 政府機関内のセキュリティ情報共有

7.2.3.2. 職員

韓国政府の SOC である NCSC には、MOPAS や KCC 等、各省庁から出向した専門家 14 人が勤務している。国家的サイバーテロ脅威が予想される場合、NCSC 内には脅威レベル（段階）を決定し、対応方法策定のための実務協議機構が設置されるが、その際各部門・機関から出向している所属職員が構成員として参加し、所属機関を代表してその意見を反映し、機構の中で決定された脅威レベル・対応措置を所属機関に伝達し、体制を構築する責務を負う。[268]

[268] 262 と同じ。

7.3. 重要インフラ防護における情報連携

韓国における重要インフラの情報システムの保護は、2001 年に制定された情報通信基盤保護法によって示されている。

7.3.1. 政策レベル

7.3.1.1. 政策・戦略検討

(1)Committee on the Protection of Information Infrastructure（CPII）

2001 年に情報通信基盤保護法によって設立された重要情報通信インフラ防護について検討する政府横断的な委員会。重要情報通信インフラの防護に当たって、サイバー攻撃を防止するためのセキュリティ対策の実施、事案発生時の対応体制等を定めている。また、同法を根拠に、国防、通信、金融等、主要な重要インフラの情報通信インフラのセキュリティ対策並びに計画を策定している。

①サイバー攻撃に対する予防活動

- 類似事案の発生防止のための予防対策
- ワーム・ウイルス感染の除去、ウイルスに汚染された電子メールの遮断、スパムの受信拒否
- 主要な政府情報システムに対する不正アクセスへの予防措置及び遮断
- 不正アクセスの探知・遮断、攻撃発信アドレスの遮断、事案探知及び対応

②情報セキュリティ事案発生時の対応及び支援

- ワーム・ウイルス蔓延に対する警告の発信
- ウイルスやサイバー攻撃等の有害トラフィックの動向、サイバー脅威の発生状況及び被害状況等の調査・分析
- NCSC へのログ提供及び共同対応
- サイバー脅威に対する対策措置実施結果の把握及び NCSC による事案調査の支援

③政府機関内のセキュリティ情報共有

- GISAC ホームページを通じた脆弱性情報、事案発生事例、ウイルス情報、セキュリティに関する注意情報、緊急警報の発信等、電子政府ネットワークの利用組織に対して、最新のセキュリティ情報の提供
- 電子政府に関するニュース、月毎のクラッキング・ウイルス動向、セキュリティニュース及び主要なトピック等を含む、月刊セキュリティウェブマガジンの発行

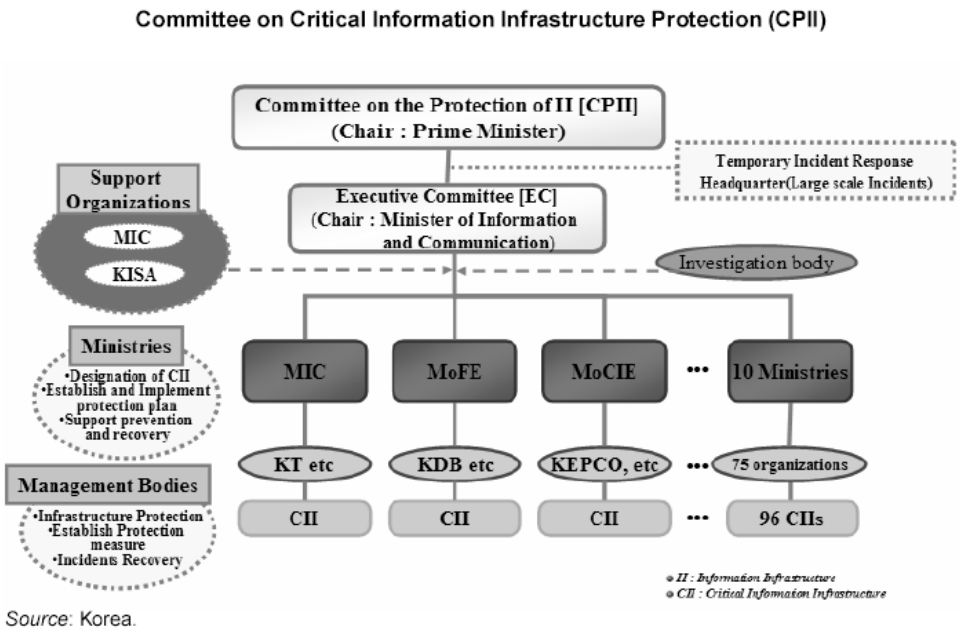


図 7-8 CPII の体制（ただし政府機関は 2008 年の再編以前のもの）[269]

7.3.1.2. システム構築

重要インフラの情報共有のためのシステムは、分野別に設置される ISAC(後述)の運用主体によって構築される。基本的はISACごとにメンバのみが閲覧可能なHPを通じた情報共有が行われる。

7.3.1.3. マネジメント

(1)情報通信基盤保護法[270]

情報セキュリティの脅威から、国家レベルで重要な情報通信基盤を保護することを目的に、情報通信部が「情報通信基盤保護法」を立案、2001 年 1 月に制定、同年 7 月 1 日に施行された。 なお、情報通信基盤保護法は、米国の PDD63（Presidential Decision Directive 63）を参考に作られている。

（情報通信基盤保護法の主な項目）

- 重要インフラ（情報通信基盤施設）の指定
- 情報通信基盤保護委員会(CPII)の設置及び機能
- 重要インフラ保護対策・計画策定、保護支援体制
- 重要インフラ保護対象施設の指定

[269] http://www.olis.oecd.org/olis/2006doc.nsf/linkto/dsti-iccp-reg(2006)15-final

[270] 262 と同じ。

・ 重要インフラに関わる脆弱性分析・評価の義務
・ 重要インフラ保護及びインシデント対応
・ 保護指針/保護措置命令/侵害行為の禁止/インシデントの通知/復旧措置/
・ 対策本部の構成/情報共有・分析センター(ISAC)構築
・ 情報共有・分析センター(ISAC)構築の推奨
・ 情報セキュリティ専門業者の指定及びその業務範囲の指示
・ 技術支援及び民間協力の推進
・ 罰則

7.3.2. オペレーションレベル

7.3.2.1. 組織

(1)Korea Internet Security Center (KISC)[271]

2003 年に設立されたインシデント対応チーム。安全なインターネット及び通信環境を構築するために、民間情報通信ネットワークの防護機能を持つ組織である。組織内部はインシデント分析チーム、インシデント対応コーディネーションチーム、ハッキング対応チーム、スパム対応チーム、ボットネット対応チーム、ネットワーク監視チームの 6 つのグループに分かれて活動を行っている。KISC の主な機能を以下に挙げる。

(KISC の主な機能)

・ サイバーインシデントの防止のための技術的サポート
・ サイバーインシデントの分析、マリシャスコードの分析及び対応策・復旧策の検討
・ ネットワークトラフィックの分析による脆弱性や国家の情報セキュリティレベルの監視
・ 最新のハッキングツール及びインシデント対応対策に関する分析
・ スパムの解析
・ 他国の CSIRT 組織との連携
・ フィッシング等に関する情報提供による国内の CSIRT の活動の活性化と、民間部門における意識向上

[271] http://www.certcc.or.kr/english/main.htm

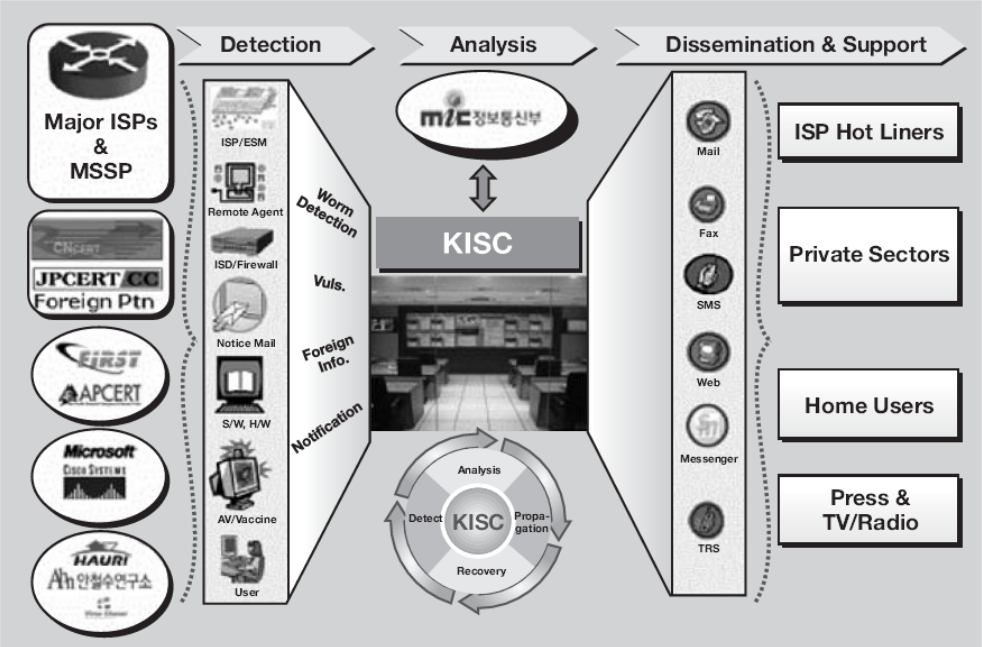


図 7-9 KISC におけるワークフロー[272]

(2)Information Sharing and Analysis Center (ISAC)

2001 年の情報通信基盤保護法の第 16 条に基づき設立された、各重要インフラ分野の企業や、所管省庁との情報共有によって、情報システムに対する攻撃を防止することを目的とした組織。現在以下の 4 つの ISAC が存在する。

①G-ISAC

前述の通り。

②KS-ISAC

韓国で最初に設立された ISAC。分野は特に限定しておらず、サイバーインシデント、脆弱性、パッチに関する情報をデータベース化し、オンラインで構成員に情報を提供する。

③KF-ISAC

2002 年 12 月に設立された MOFE(Ministry of Finance & Economy:財政経済部)及び金融機関を対象とした ISAC。MOFE の承認を受けて Koscom 社が運用を行っている。金融分野の主要な情報システムに対して定期的な脆弱性分析・評価、セキュリティ対策及びセキュリティ計画の策定を行う。

---

[272] http://www.itsc.org.sg/pdf/6thmtg/Korea-Malaysia-Singapore-S.pdf

④Korean Telecommunication ISAC

2001 年 2 月に設立され、韓国の通信事業者の共同体である KTOA（Korea Telecommunications Operators Association:韓国通信事業者連合会）が運営している。CERT/CC-KR と同じ建物にあり、密に連携がとられている。12 の民間の通信事業者から構成されており、以下に示すような活動を行う。

（Korea Telecom ISAC の機能の例）

- 会員企業向けの情報セキュリティ関連の情報共有体制、インシデント対応体制の構築
- 会員企業における情報セキュリティシステムの状況に関する調査
- 会員企業間の情報セキュリティ協力体制の構築

7.3.2.2. National CSIRT と ISP の関係

韓国の National CSIRT である KISC ではインシデントに関する情報を国内の ISP（KT、Dacom 等）や国内外の CSIRT 組織、及び OS 製造企業（Microsoft 等）、さらにウイルス対策、マリシャスコード対策に係る企業から収集している。KISC 自体でも 24 時間 365 日体制で韓国のインターネットの監視を行っている。KISC では ISP から提供されたインシデントに関連する情報や、主要なウェブサーバの状況、ISP の DNS サーバに対するクエリパケットの種類と、ハニーポットから得られた脆弱性やワームに関する情報、情報セキュリティ関連企業から報告される最新の攻撃のトレンド等を収集しており、それらの解析結果を基に韓国におけるインターネットの状況を判断している。インターネット上で危機的な状況が発生した際には緊急警報を発令し、被害を受けた／受けることが想定される企業に対する情報提供等も行う。

7.3.2.3. 官民連携体制

情報通信基盤保護法によって設置が規定されている ISAC は米国と同様に、あくまで民間主導の体制として構築されており、その運営も民間側に任されているが、現時点では 3 つの分野でしか設置が実現されていない。実際に、重要インフラにインシデントが発生した際には、政府の省庁横断的組織である CPII によって対策本部が設置され、各重要インフラは所管省庁に報告を行い、報告を受けた所管省庁からの意見を取りまとめた上で対策本部において方針が決定される。