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

「各国における情報セキュリティに対する取り組みに関する調査」

～製品・サービスの情報セキュリティに関する動向～

株式会社三菱総合研究所

2009 年 3 月

目次

図目次

表目次

1. はじめに

1.1. 背景

近年、わが国の国民生活・社会経済活動のあらゆる場面において、ICT への依存度は高まってきている。ICT の利用・活用は、医療、福祉、教育等の多方面において国民生活に不可欠となりつつある。一方、ICT 基盤は、24 時間・365 日、常時世界とつながっているため、わが国のIT基盤に何らかの障害が発生した場合、その影響が諸外国に急速に拡大する可能性がある。逆に、諸外国において ICT 基盤に何らかの障害起こった場合はわが国の国民生活・社会経済活動に負の影響が生じる可能性がある。さらに、海外からの意図的な攻撃は、国境に関係なく容易に国・地域内の重要なビジネスインフラ等に被害を発生させる可能性がある。

このような背景の下、2006 年 2 月 2 日に情報セキュリティ政策会議において決定された「第 1 次情報セキュリティ基本計画」では、セキュリティ立国の思想に基づき、政府組織の情報セキュリティ対策の水準を世界最高のものとするため、政府機関統一基準について、技術や環境の変化を踏まえ毎年その見直しを実施するものとしている。さらに、2007 年 10 月 27 日の情報セキュリティ政策会議で決定された「我が国の情報セキュリティ分野における国際協調・貢献に向けた取組み」においては、「経済関係の深化が進むアジア地域のビジネス環境向上に向けた協調・貢献の推進」「情報セキュリティに係る新しい諸権利に係る検討及び議論への貢献」「サイバー攻撃、ICTに起因する脅威への対応のための取組の推進」「情報セキュリティに係るグローバルなルールや標準の形成への貢献」「様々な国際フォーラム等における提案や議論への積極的な参加」を今後の取組みの方向性としている。また、前記基本計画の下での最終年度である 2008 年度における情報セキュリティ対策の政府の重点施策を定めた「セキュア・ジャパン 2008」が 2008 年 6 月 19 日での情報セキュリティ政策会議において決定された。「セキュア・ジャパン 2008」では、「情報セキュリティ基盤の強化に向けた集中的な取組み」を図り、大きな社会的効果が発現するよう努力を続けることが述べられており、「政府機関・地方公共団体」や、「重要インフラ」、「企業」及び「個人」のそれぞれの領域について具体的施策をあげるとともに、「横断的な情報セキュリティ基盤の形成」や「政策の推進体制と持続的改善の構造」について具体的施策を示している。

1.2. 目的

本調査は、「我が国の情報セキュリティ分野における国際協調・貢献に向けた取組み」(平成 19 年 10 月 27 日情報セキュリティ政策会議決定)に基づき、内閣官房情報セキュリティセンター殿の国際貢献の実現方策を検討するために実施するものである。

本報告書は、「各国における情報セキュリティに対する取り組みに関する調査」のうち、「製品・サービスの情報セキュリティに関する動向編」として、欧米先進国を中心として、ICT 製品・サービスの情報セキュリティに関する政府の取り組みおよび民間・業界団体の取り組み状況を調査することにより、先進国等の取り組み事例を、我が国の情報セキュリティ政策の運営に生かすとともに、急速に変化する情報セキュリティ分野における新たな連携・協力手法を検討するための材料を得ることを目的とする。

2. 各国の製品・サービスのセキュリティに関する動向

2.1. アメリカ

2.1.1. 情報システムのセキュリティに関する政府調達基準

2.1.1.1. 政府調達基準を根拠付ける法律および政策文書

米国の ICT 製品の政府調達基準を規定する法律等に関しては、IT 管理改革法(Information Technology Management Reform Act of 1996[1])及び FISMA(連邦情報セキュリティ管理法:Federal Information Security Management Act of 2002[2])がある。これらの法律を根拠として、連邦情報処理標準 FIPS(Federal Information Processing Standards)が作成されている。

さらに、FIPS 201(政府職員の個人認証に関する標準)のように、IT 管理改革法や FISMA による規定に加えて、国土安全保障大統領令 HSPD-12 や、行政管理予算局(OMB)の政策文書 M-05-24 などを根拠として、政府調達に関する標準文書となっているものもある。

一方、国家安全保障に係わる情報システムの調達を規定した国家情報保証調達ポリシー(National Information Assurance Acquisition Policy)は、コモンクライテリアや FIPS に基づく製品認定制度である CMVP や NPIVP 等で認定された製品の中から調達を行うことを義務付けている。

2.1.1.2. FIPS (連邦情報処理標準)

2.1.1.2.1. FIPSの位置づけ(根拠法)

NIST は、IT 管理改革法に基づき、国防関連以外の連邦政府機関およびその請負業者を対象としたコンピュータシステムの情報セキュリティや相互運用性に関する標準やガイドラインの作成を義務付けられている。これらの標準やガイドラインは、商務長官の承認を経て発行される。

FIPS には、義務免除手続き[3]が記載されており、これにより、連邦政府機関は、情報セキュリティに関する遵守義務を免除されるケースがあった。しかし、2002 年に FISMA が制定されたことにより、FIPS の義務免除手続きにより免除されていた項目についても強制力が発生することとなった[4]。また、NIST は、情報システムに関して連邦政府が参考にできる標準がすでに民間において作成されている場合はそれを採用するが、必要とする標準が作成されていない場合には、FIPS として作成することになった。

FIPS の主なターゲットは連邦政府機関であるが、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、LAN のセキュリティなど、分野別に詳細な基準や要求事項を示した文書は、政府機関のみならず、民間企業にとっても情報セキュリティ対策を考える上で有用である[5]。

2.1.1.2.2. FIPSの構成(SP 800を含む)

2002 年に制定された FISMA は、各連邦政府機関に対して、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の策定、文書化、実装を義務付けるとともに、NIST に対して情報システムのセキュリティ強化のための

---

[1] 連邦政府の IT システムの調達・廃棄に関して規定した法律。クリンガー・コーエン法(Clinger-Cohen Act)として知られている。NIST の FIPS に関する公式サイトでは、Information Technology Reform Act と記載されている。

[2] 連邦政府組織の情報セキュリティ管理とプロセスの改善を規定する法律である。

[3] 連邦政府が FIPS の強制事項の免除を受ける際の手続きを規定したもの。

[4] Computer Security Act of 1987 は、連邦政府の情報システムのセキュリティを強化することを目的とした法律であり、情報セキュリティに関する強制事項の免除に関する規定があった。免除条項の無い FISMA によって代替されたことにより、実質的に強制力が大きくなった。

[5] http://www.ipa.go.jp/security/publications/nist/nist_publications.html#3

標準やガイドラインの策定を義務付けた。NIST は、FISMA の規定を受けて、「FISMA 導入プロジェクト(The FISMA Implementation Project)」(2003 年 1 月) を立ち上げ、FISMA リスクマネジメントフレームワークと呼ばれる情報セキュリティを継続的に改善・向上させるための枠組みや多くの規格、ガイドラインを開発している[6]。

FISMA 導入プロジェクトでは、以下のような段階的計画によりセキュリティ強化を推進する。

フェーズ I (2003-2007)	FISMA 関連のセキュリティ規格(FIPS)およびガイドライン(SP シリーズ)の開発・策定 2007 年 8 月に FISMA 導入プロジェクト関連文書は、ほぼ策定済み。
フェーズ II (2007-2009)	セキュリティ評価機関を認定するプログラムの開発
フェーズ III (2007-2009)	セキュリティ評価ツール検証プログラムの開発 (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 の一部として実施される。ツールとしては既存の IT 製品のテスト・評価・検証用プログラムを利用する。)

図 2-1 は、NIST のリスク管理フレームワークにおける情報セキュリティの対応プロセスを示したものである[7]。

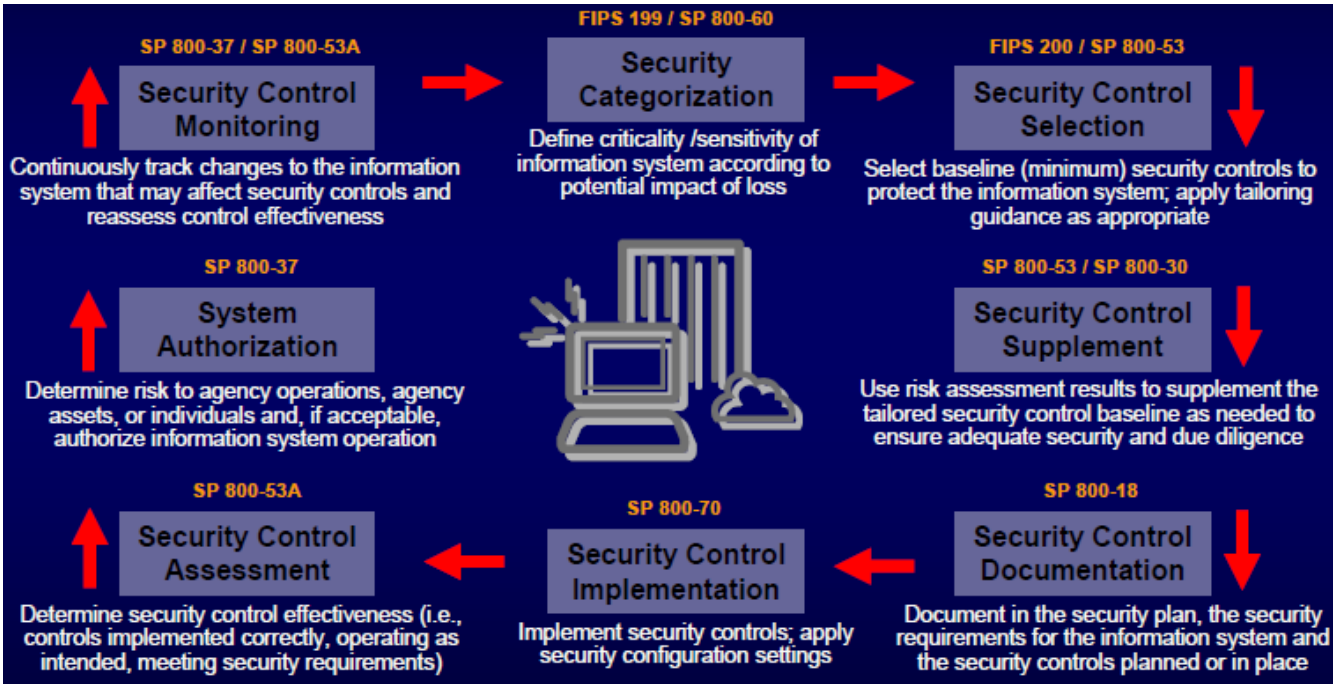

図 2-1:NIST のリスク管理フレームワーク

図 2-1 の NIST のリスク管理フレームワークにおけるプロセスの実施手順は以下の通りである。

(1) セキュリティの分類 ：FIPS 199/SP 800-60
情報資産に対する潜在的な脅威の影響度に基づき、情報システムを低位・中位・高位に分類する。

(2) セキュリティ管理策の選択 ：FIPS 200/SP 800-653
情報システムを保護するための最低限のセキュリティ管理策を(1)で行った低位・中位・高位の分類に応じて

[6] http://www.ipa.go.jp/security/publications/nist/fisma.html
[7] http://csrc.nist.gov/groups/SMA/fisma/framework.html
http://csrc.nist.gov/groups/SMA/fisma/documents/risk-framework-2007.pdf

選択する。

(3) 選択したセキュリティ管理策の調整 ：SP 800-53/SP 800-30
リスクアセスメントを行い、組織の状況、求められる脅威への対策および政府機関それぞれに特有な要件に基づく最低限の管理策を調整する。

(4) セキュリティ管理策の文書化 ：SP 800-18
システムセキュリティ計画において、情報システムのセキュリティ要件の概要を提供し、計画・実施されるセキュリティ管理策を文書化する。

(5) セキュリティ管理策の導入 ：SP 800-70
セキュリティ管理策を導入する(セキュリティ設定チェックリストを適用する)。

(6) セキュリティ管理策の評価 ：SP 800-53A
セキュリティ管理策の有効性を判断する(管理策が正しく導入され、意図した通りに運用され、セキュリティ要件に見合う成果を上げているかなど)。

(7) システムの運用認可 ：SP 800-37
政府機関の業務や資産、人員へのリスクを判断し、リスクが容認可能であれば、情報システムの運用を認可する。

(8) セキュリティ管理策実施状況の監視 ：SP 800-37/SP 800-53A
セキュリティ管理に影響を及ぼす情報システムへの変更を継続的に監視し、管理策の有効性を再評価する。

FIPS の主要な文書を表 2-1 に示す。

表 2-1:FIPS の主要な文書

FIPS 番号	発行日	タイトル(内容)
FIPS 201-1	2006/3	連邦従業員及び委託業者の個人識別情報の検証
FIPS 200	2006/3	連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項
FIPS 199	2004/2	連邦政府の情報および情報システムに対するセキュリティ分類規格
FIPS 198-1	2008/6	鍵ハッシュメッセージ認証コード(MAC)
FIPS 197	2001/11	共通鍵暗号 AES
FIPS 196	1997/2	公開鍵暗号を用いた相手認証
FIPS 191	1994/11	LAN セキュリティ解析のガイドライン
FIPS 188	1994/9	情報転送のための標準セキュリティラベル
FIPS 186-3	2007/12	RSA 強化素数 - DSS
FIPS 185	1994/2	エスクロー暗号標準
FISP 181	1993/10	自動パスワード生成機
FIPS 180-3	2008/10	セキュアハッシュ標準(SHS)
FIPS 140-3	1994/1～2007/7	暗号モジュールのセキュリティ要件(CMVP)
FIPS 113	1985/5	コンピュータデータ認証

2.1.1.2.3. SP 800シリーズ

2.1.1.2.3.1. SP 800シリーズの概要

SP 800 シリーズ(Special Publications 800 Series)は、連邦政府がセキュリティ対策を実施する際に参考文書として利用することを前提として、NIST のコンピュータセキュリティ課 CSD[8]により作成されるガイダンスであり、FIPS の具体的な導入ガイダンスとしての役割を果たす。政府機関だけではなく、民間企業のセキュリティ担当者にとっても有益な文書である。

2.1.1.2.3.2. SP 800シリーズの主要な文書

SP 800 シリーズの主要な文書は表 2-2 の通りである。情報セキュリティマネジメント、リスクマネジメント、情報セキュリティ技術、情報セキュリティの対策状況を評価する指標、情報セキュリティ教育、インシデント対応など、情報セキュリティ全般を幅広く網羅している。

表 2-2:SP 800 シリーズの主要な文書

文書番号	発行日	タイトル(内容)
SP 800-18 rev1	2006/2	連邦情報システムのためのセキュリティ計画作成ガイド 改訂第 1 版
SP 800-23	2000/8	セキュリティアシュアランス(Security Assurance)と調達に関する連邦政府のためのガイドライン
SP 800-30	2002/6	IT システムのためのリスクマネジメントガイド
SP 800-33	2001/12	IT セキュリティのための基本テクニカルモデル
SP 800-34	2002/6	IT システムのための緊急時対応計画ガイド
SP 800-35	2003/10	IT セキュリティサービスガイド
SP 800-37	2004/5	連邦政府情報システムに対するセキュリティ承認と運用認可ガイド
SP 800-40	2005/12	パッチおよび脆弱性管理プログラムの策定
SP 800-42	2005/8	ネットワークセキュリティテストにおけるガイドライン
SP 800-50	2003/10	IT セキュリティの意識向上およびトレーニングプログラムの構築
SP 800-53 rev2	2007/12	連邦政府情報システムにおける推奨セキュリティ管理策(改訂第 2 版)
SP 800-53 rev.2 Annex 1	2007/12	連邦政府情報システムにおける推奨セキュリティ管理策 低位影響レベルのベースライン
SP 800-53 rev.2 Annex 2	2007/12	連邦政府情報システムにおける推奨セキュリティ管理策 中位影響レベルのベースライン
SP 800-53 rev.2 Annex 3	2007/12	連邦政府情報システムにおける推奨セキュリティ管理策 高位影響レベルのベースライン
SP 800-55	2008/6	情報技術システムのためのセキュリティメトリクスガイド
SP 800-60 Volume 1	2006/8	第 I 巻:情報および情報システムのタイプとセキュリティ分類のマッピングガイド
SP 800-60 Volume 2	2006/8	第 II 巻:情報および情報システムのタイプとセキュリティ分類のマッピングガイド付録

[8] コンピュータセキュリティに関する研究やプロトタイプ開発、テスト、セキュリティ標準の策定などを行う部署。
セキュリティ標準は、FIPS、SP 800 シリーズ(情報セキュリティ)、SP 500 シリーズ(情報技術)等として発行される。

SP 800-61 rev1	2008/3	コンピュータセキュリティインシデント対応ガイド(改訂第 1 版)
SP 800-63	2006/4	電子認証に関するガイドライン
SP 800-64	2008/10	情報システム開発ライフサイクルにおけるセキュリティの考慮事項
SP 800-65	2005/1	IT セキュリティの資本計画及び投資管理プロセスへの統合
SP 800-70	2005/5	IT 製品のためのセキュリティ設定チェックリストプログラム -チェックリスト 利用者と開発者のための手引き
SP 800-73 Rev2	2008/9	個人識別情報の検証インタフェース
SP 800-76	2007/1	個人識別情報の検証における生体認証データ仕様
SP 800-83	2005/12	マルウェアによるインシデントの防止と対応のためのガイド
SP 800-85 A	2006/4	PIV カードアプリケーションとミドルウェアインタフェーステストガイドライン
SP 800-85 B	2006/6	PIV データモデルテストガイドライン

この中で製品の情報セキュリティと関連性の高いものとして以下のようなものがある。

- SP 800-23:セキュリティ・アシュアランスと調達に関する連邦政府のためのガイドライン(Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products)
  連邦政府における情報セキュリティ関連 IT 製品のセキュリティ・アシュアランスと調達/検査・評価済み製品の利用に関するガイドライン[9]。
- SP 800-37:連邦情報システムのセキュリティ承認と運用認可のためのガイド(Guide for the Security Certification and Accreditation of Federal Information Systems) [10]
  システムの運用開始前に、リスクを低減するための情報セキュリティ管理と対策がとられていることを保証するためのプロセスを示す。FISMA の情報セキュリティプログラムの一環として、OMB Circular A-130 Appendix III[11] に基づき作成されている。
- SP 800-70: IT 製品のためのセキュリティ設定チェックリストプログラム:チェックリスト利用者と開発者のための手引き(Security Configuration Checklists Program for IT Products: Guidance for Checklist Users and Developers) [12]
  組織および個人ユーザが IT 製品をより適切に保護できるように、セキュリティ設定チェックリストの開発と普及を推進するためのガイドラインである。

2.1.1.3. 国家情報保証調達ポリシー

国家情報保証調達ポリシー(National Information Assurance Acquisition Policy No. 11(NSTISSP No. 11:National Security Telecommunications and Information System Security Policy)) (2000 年 1 月発行)は、国防総省(DoD)が議長を務める国家安全保障通信・情報システムセキュリティ委員会(NSTISSC:National

[9] http://www.niap-ccevs.org/cc-scheme/nist-sp800-23.pdf
[10] 出典:http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf
[11] 連邦政府の情報システムに対するコンピュータセキュリティ法(Computer Security Act of 1987)および FISMA の要件への準拠を義務化する方針を示した米国連邦政府の文書。
[12] 出典:http://checklists.nist.gov/ncp.cfm?special_pub

Security Telecommunications and Information System Security Committee[13] (現 CNSS：Committee on National Security Systems))によって国家レベルのポリシーとして策定されたもので、情報保証(Information Assurance ： IA) [14]と IA 対応の IT 製品の調達に関する国家レベルの方針を規定している。情報保証は、国家安全保障に関わる情報の入力、処理、保存、表示、送信に使用されるすべてのシステムに対する要件とみなされるものである。

このポリシーにより、2001 年 1 月 1 日に、連邦政府が調達する民生品(COTS：Commercial Off-the Shelf)に関して、ISO/IEC[15] 15408 [16] (Common Criteria ： コモンクライテリア(CC))の相互認証協定(MRA：Mutual Recognition Arrangement) [17]、コモンクライテリアに関する評価・認証プログラム(CCEVS(Common Criteria Evaluation and Validation Scheme (2.1.1.4.1 で説明))、FIPS の認証プログラム(CMVP(Cryptographic Module Validation Program (2.1.1.4.2 で説明)、NPIVP(NIST Personal Identity Verification Program (2.1.1.4.3 で説明)等)の制度に従わなければならないこと、および連邦政府機関が情報セキュリティ関連製品および、暗号モジュール関連製品を調達する場合には、CMVP の基で実施される検査制度 Cryptographic Module Testing (CMT)により認定された製品、あるいは CCEVS の基で実施される検査制度 Common Criteria Testing (CCT) により認定された製品の中から選ばなければならないことが規定された。

NSA が開発・製作した通信セキュリティ装置(GOTS ： Government-Off-the-Shelf [18])の代替とされる民生品は、情報セキュリティに関する一定の保証を与える標準化された評価プロセスを通さなければいけない。民間セクターに対しては、認定製品リストから選ぶことが推奨されている。(義務化はされていない)

DoD の情報保証(IA)は、情報の保全や、ソフトウェアのセキュリティを確保するための手段を明確化することで、組織として情報の安全性を保証するという点において、software assurance(ソフトウェア・アシュアランス)[19]のベースとなる概念であると考えられる。

2.1.1.4. FIPS等に基づく政府調達基準

FIPS などの標準に基づき、政府が調達する情報システムを認定製品リストから選択することを義務化する制度としては、以下のものがある。

- 暗号モジュール認定制度(CMVP, FIPS 140-2)
- 個人認証認定制度(NPIVP, FIPS 201)
- 評価・認証プログラム(CCEVS, ISO15408)

これらの認定制度の運用に関する全体的な枠組みを図 2-2 にまとめる。これらの制度は、NIST の製品検査

---

[13] 2001 年 10 月、大統領行政令(E.O.13231)により、重要インフラ防御のため、National Security Telecommunications and Information Systems Security Committee (NSTISSC)を Committee on National Security Systems (CNSS)として再任命した。CNSS の議長は、NSD-42(国家安全保障令 42： 国家安全保証に関する大統領令で、国家安全保障通信情報システムのセキュリティに関する国家ポリシーを規定)に基づき、DoD が務める。

[14] 情報および情報システムの可用性、完全性、認証、機密性、否認防止を確保するための各種対策。 http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

[15] International Electrotechnical Commission： 国際電気標準会議 http://www.iec.ch/

[16] IT 製品が特定の情報セキュリティ要件に準拠しているかどうかを評価・認証するための枠組みおよびその基準に関する国際標準。一般にコモンクライテリア(Common Criteria)と呼ばれる。http://www.commoncriteriaportal.org/

[17] MRA は、コモンクライテリア承認アレンジメント (CCRA, Common Criteria Recognition Arrangement)に改称された。

[18] 国家安全保障に係わるセキュアな通信のためのシステムとして NSA が開発した装置と考えられる。GOTS と同義語として扱われている。 出典：NSTISSP No.11, Revised Fact Sheet National Infoamtion Assurance Acquisition Policy

[19] ソフトウェアに脆弱性が存在しないことおよび意図した通りに動作することに対する信頼性を表す概念。 http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf DoD、DHS などが、その方法論の開発に取り組んでいる。

機関認定プログラム(National Voluntary Laboratory Accreditation Program：NVLAP[20])をベースとしたものであり、検査実施機関は、検査対象の製品に関して第三者の民間組織から選ぶようになっている。

連邦政府の IT 製品セキュリティ評価認証制度の具体的な内容については次章以降で述べる。

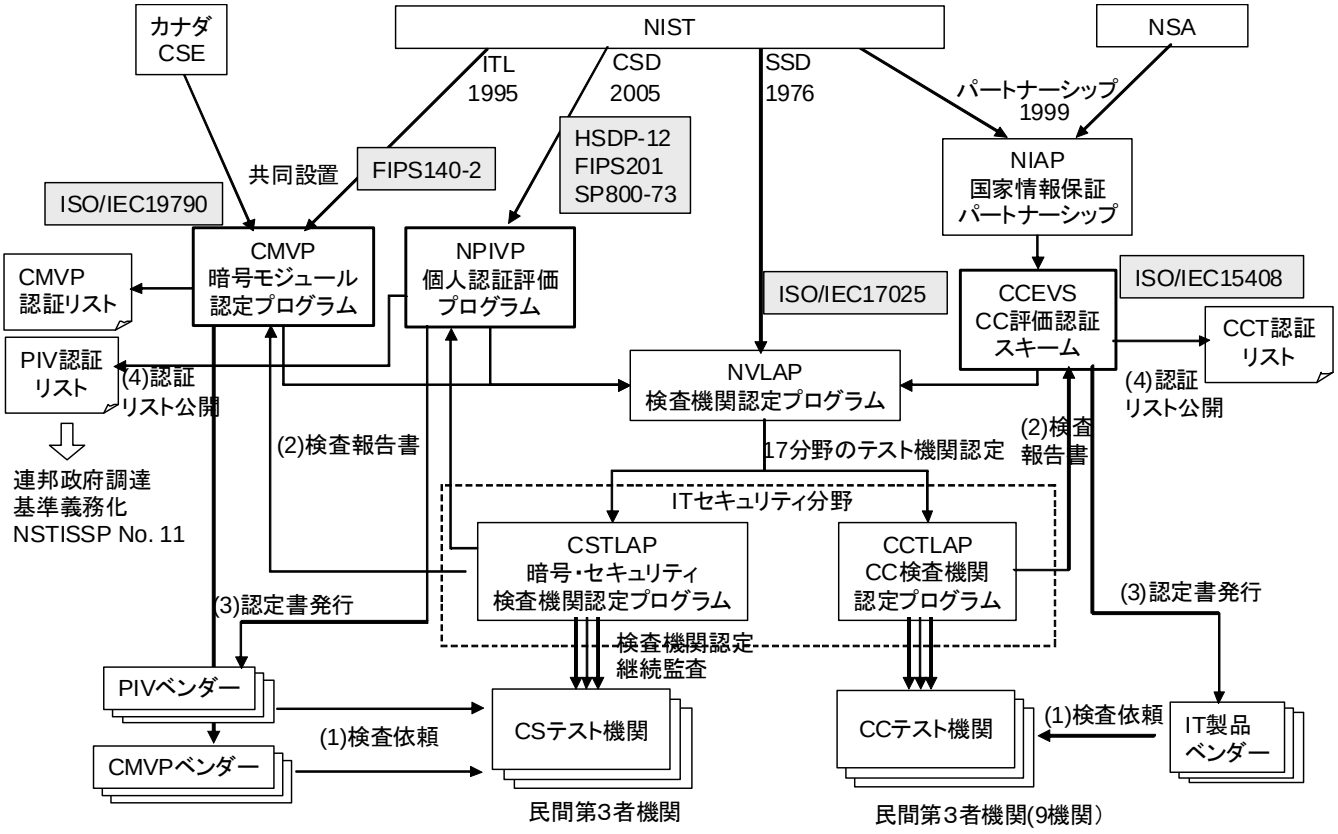

図 2-2：米国連邦政府の IT 製品セキュリティ評価認証制度の構造[21]

図 2-2 中の略語の説明を以下に記す。

- CSE (Communications Security Establishment：通信安全局)：カナダの政府機関で、通信のセキュリティを所管する。
- NSA (National Security Agency：国家安全保障局)：アメリカ国防総省の諜報機関で、暗号技術の規制管理などを行っている。
- ITL (Information Technology Laboratory)：NIST における IT 分野の研究を行う研究所
- SSD (Standard Services Division)：NIST における標準化を推進する部署で、米国標準を国内外で普及させることをミッションとしている。
- NVLAP(National Voluntary Laboratory Accreditation Program)：17 分野の製品について、製品が基準を満たすかどうかに関する評価・認証を行う機関を認定するための制度：2.1.1.4.4 を参照。
- CSTLAP(Cryptographic and Security Testing Laboratory Accreditation Program)：NVLAP の下位プログラムで、暗号・セキュリティ製品の評価・認証を実施する機関の認定制度
- CCTLAP(Common Criteria Testing Laboratory Accreditation Program)：NVLAP の下位プログラ

[20] http://ts.nist.gov/standards/accreditation/index.cfm
[21] 出典：三菱総合研究所資料。

ムで、CC に基づいて製品の評価・認証[22]を実施する機関の認定制度[23]。

- NIAP(National Information Assurance Partnership) [24]:IT ユーザと IT 製品の両方のセキュリティテストのニーズを満たすための米国政府のイニシアチブで、NSA により運用される。コスト効果の高いセキュリティテスト・評価・認定プログラムの利用を通じてユーザの情報システム・ネットワークに対する信頼を高めることを目標とする。
- CMVP(Cryptography Module Validation Program):2.1.1.4.2 を参照。
- NPIVP(NIST Personal Identity Verification Program):2.1.1.4.3 を参照。
- CCEVS(Common Criteria Evaluation and Validation Scheme):2.1.1.4.1 を参照。

2.1.1.4.1. コモンクライテリア評価認証スキーム(CCEVS) [25]

CCEVS(Common Criteria Evaluation and Validation Scheme)は、IT 製品が ISO/IEC15408(コモンクライテリア:CC)に適合する評価・認証を行う連邦政府によるプログラムであり、評価実施機関に対する技術ガイダンスや、認定製品リスト[26,27]を定める。CC の前身である TCSEC は、米国防総省が発行したガイドラインに基づいて国防関係のコンピュータシステムを調達する際の評価・認証基準である。1983 年に作成され、NSA により運用されていたが、2005 年に TCSEC から CCEVS に置き換えられた。CCEVS も NSA により運用される。

CC は、評価・認証の対象となる IT 製品のセキュリティ要件(プロテクション・プロファイル(PP))に関して、製品を開発・製造した機関が規定し、製品の開発・評価プロセスが規定通りに実施されたかどうかを評価するための枠組みである。米国政府向けの PP[28]などが開発されている。

CC では、評価対象の情報セキュリティ水準を 7 段階の評価保証レベル (EAL: Evaluation Assurance Level) [29]で指定する。最も厳しい EAL7 では、形式手法を用いた設計・開発およびテスト[30]の実施が要件となる。コモンクライテリア等の IT セキュリティ要件を規定したハンドブックとしては、NIST ハンドブック 150-20 [31] が公開されている。

製品の評価・認証を実施する機関を認定するプログラムである CCTLAP は、NIST と NSA のパートナーシッププログラムである National Information Assurance Partnership (NIAP)において、IT テストプログラム(Information Technology Testing (ITST) program)の一部として実施される[32]。

ある国で CC に基づき評価・認証された製品を、他の国でも認証済み製品とする国際間の相互承認にかんする国際協定として、コモンクライテリア承認アレンジメント(CCRA : Common Criteria Recognition

---

[22] 厳密には、「CC を満たす製品を検査する」とは、セキュリティ製品が CC の基準を満たすことを第3者検査機関が検査することを指し、「CC の認定を行う」とは、検査機関の検査結果をもとに、NAIP が、製品の認定を行うこと。

[23] 出典:http://ts.nist.gov/Standards/scopes/programs.htm
http://ts.nist.gov/standards/accreditation/index.cfm

[24] http://www.niap-ccevs.org/

[25] http://www.niap-ccevs.org/cc-scheme/

[26] CCEVS 認定製品リスト:http://www.niap-ccevs.org/cc-scheme/in_evaluation/

[27] http://www.niap-ccevs.org/cc-scheme/in_evaluation/

[28] たとえば、U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments Version 1.2 http://www.niap-ccevs.org/cc-scheme/pp/pp_av_br_v1.2/
日本においては IPA が電子政府向け情報システムに関する PP を策定している。

[29] 製品やシステムのセキュリティ評価において、そのセキュティ機能が確実に動作することの保証の度合いを表す指標。
EAL1～EAL7 までの 7 段階があり、数値が大きいほど保証の度合いが大きい(求められる要件が厳しい)。
http://www.ipa.go.jp/security/ccj/cc_tutorial/faq_index.html

[30] 情報システムの設計・開発・テストが、形式仕様記述言語や形式手法を用いて行われていることを指す。

[31] 出典:http://ts.nist.gov/Standards/Accreditation/upload/NIST-HB-150-20-Checklist.pdf

[32] 出典:http://ts.nist.gov/Standards/scopes/cct.htm
http://www.niap-ccevs.org/cc-scheme/cctls/

Arrangement)[33]がある。

2.1.1.4.2. 暗号モジュール評価プログラム(CMVP)

CMVP(Cryptography Module Validation Program)は、FIPS 140-2 [34] に基づく暗号モジュール製品に関する認証制度であり、CMVP プログラムにおける暗号モジュール製品の評価・認定は、検査機関認定プログラム(NVLAP)のうち、情報セキュリティ分野に特化した検査機関認定プログラムである Cryptographic and Security Testing (CST) [35] に基づいて認定された検査機関によって実施される。

2.1.1.4.3. 個人認証評価プログラム(NPIVP : NIST Personal Identity Verification Program)

NPIVP は、FIPS 201-1 が規定する、連邦政府の施設や情報システムにアクセスする連邦政府職員および業務委託先の従業員の個人識別情報の検証(Personal Identity Verification)用コンポーネントの認可を行うためのプログラムであり、2005 年に運用が開始された。

NPIVP に関連する政府機関、文書等の相互関係を図 2-3 に示す。国土安全保障大統領令 HSPD-12 を上位の根拠文書として、FIPS 201-1 および OMB の HSPD-12 導入ガイダンス・ロードマップがその柱となり、SP 800 シリーズなどにより具体的なガイダンスが示される。

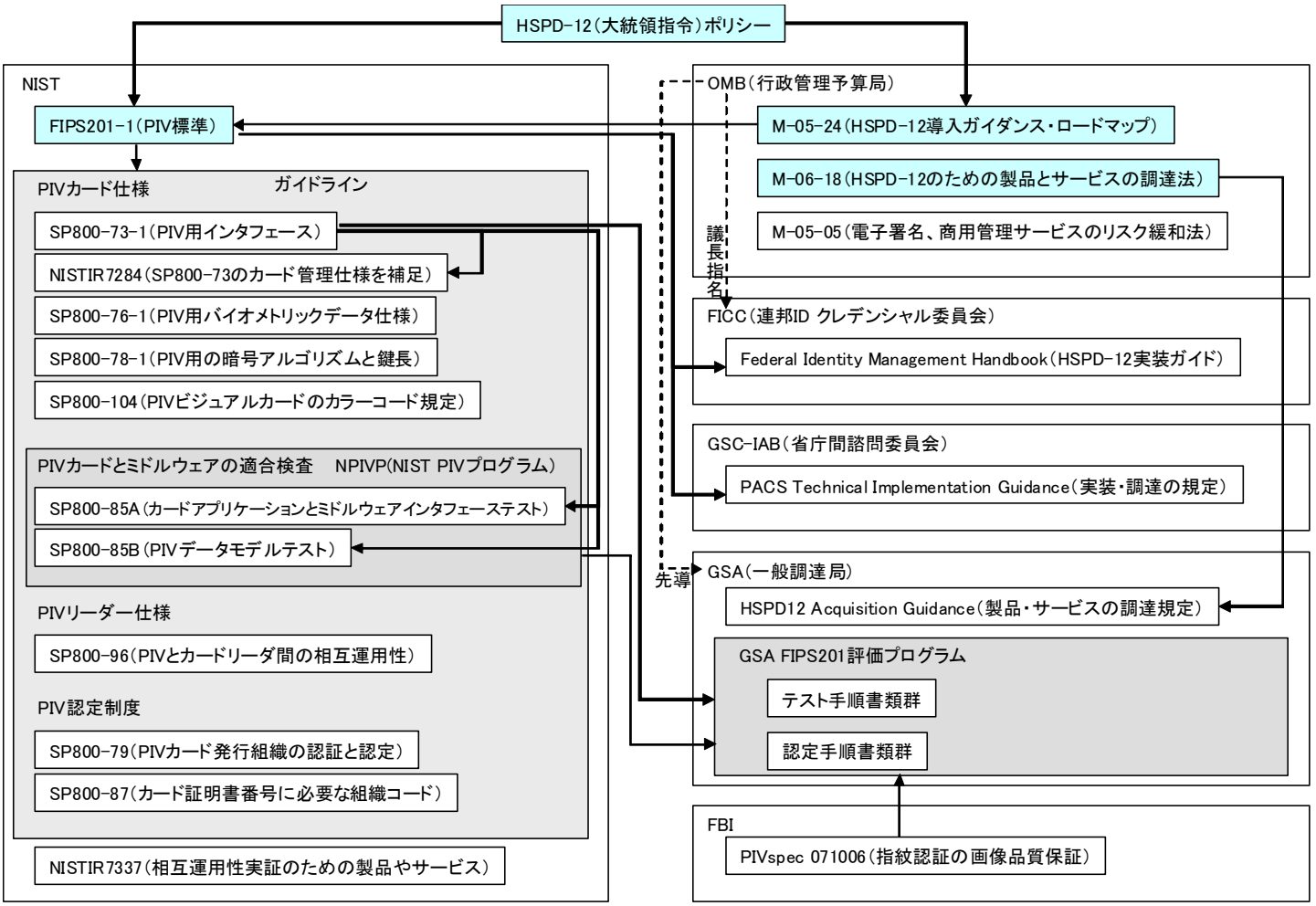

図 2-3:NPIVP に関連する政府機関、文書等の相互関係

[33] http://www.commoncriteriaportal.org/theccra.html

[34] FIPS 140-2 は、ISO/IEC 19790:2006 暗号モジュールのためのセキュリティ要件(Security requirements for cryptographic modules(2006 年 3 月 1 日発行))を作成する際の主要な参考文書となった。

[35] 暗号モジュールが FIPS 140 に準拠しているかどうかに関する評価認証を実施する機関を認定する制度。

2.1.1.4.4. 検査機関認定プログラム(NVLAP) [36]

NVLAP は、各種製品等の検査を実施する能力を持つ検査実施機関を認定する制度であり、1976 年に設置された。IT セキュリティ以外に、一般の製品、化学製品等 17 分野に対して製品検査が実施され、2006 年の時点で 749 の検査実施機関を認定している[37]。検査実施機関は、ISO/IEC 17025(検査実施機関及び校正機関の能力に関する一般要求事項(General requirements for the competence of testing and calibration laboratories)の要件を満たす必要がある。相互認証合意(MRA:Mutual Recognition Arrangements)により、APLAC(Asia Pacific Laboratory Accreditation Cooperation [38]) や International Laboratory Accreditation Cooperation (ILAC) [39] などの検査実施機関認定組織と連携している。

2.1.1.5. CC と CMVP の比較

CC と CMVP を比較したものを
表 2-3 に示す[40]。

表 2-3:CC と CMVP の比較

	CC	CMVP
標準	ISO/IEC15408	FIPS 140-2, ISO19790
規定内容	セキュリティ評価の枠組み(フレームワーク)を提供。 セキュリティ要件は利用者が指定。	セキュリティ要件のリストそのものを規定。
対象範囲	セキュリティ機能を備えた製品	暗号機能を持つモジュール製品(ハード、ソフト、ファームウェア)

暗号系の実装に関する評価は、CC の適用領域外である。暗号モジュールの仕様は、米国政府標準 FIPS 140 などにより規定される。

2.1.2. 米国政府調達基準と WTO 政府調達協定との関係

2.1.2.1. WTO 政府調達協定

WTO 政府調達協定(WTO Agreement on Government Procurement:WTO GPA) [41] は、政府等の調達において、国内の事業者が提供する製品・サービスに対して、海外の事業者が提供する製品・サービスよりも有利な調達条件を設定することを禁止する国際的な取り決めである。このうち、第 6 条の技術仕様に関する条項は、国際貿易上不必要な障害をもたらすような適合性評価手続きを立案・制定することを禁止している。また、技術的規制や政府調達の実施に際して、国際標準(ISO/IEC 等)に準拠することを推奨している。協定の原則を具体化するために、公正で透明性の高い調達手続きを定めること、その手続きが無差別に適用されることを締約国に義

[36] http://ts.nist.gov/standards/accreditation/index.cfm
[37] http://ts.nist.gov/Standards/upload/What-is-the-NVLAP.pdf
[38] アジア太平洋試験所認定協力機構 : アジア太平洋地域内の製品検査機関を認定する組織 http://www.aplac.org/
[39] 国際試験所認定協力機構 http://www.ilac.org/
[40] http://dev.sbins.co.jp/cryptography/CMVP05.html
[41] http://www5.cao.go.jp/access/japan/chans/kyoutei.html

務付けている。なお、国家安全保障の確保に不可欠な調達には適用されないなど、一定の適用除外事由が定められている(23 条 1・2 項)。

適用対象は、中央政府、地方政府、政府関連機関など各国ごとに指定された機関に限定される[42]。対象となる製品・サービスの品目は国ごとに指定されており、規定の調達基準額を上回るものに限定される。

2.1.2.2. WTO 政府調達協定に係わる日米の動向

日本政府は、米国政府に対し、WTO政府調達協定に関連する米国連邦政府の調達について、米国製の製品を優遇するバイ・アメリカン条項を撤廃し、米国企業と外国企業に平等な事業機会を確保することを求めている[43]。この中で、政府調達に関しては、交通標準化法や、WTO 政府調達協定適用外の鉄道を含む大量輸送および高速道路に関する調達の是正を求めているが、IT セキュリティ製品等については言及されていない。

WTO 政府調達協定では不服申し立て制度の設置が義務づけられており、欧米では広く活用されている。日本では 5 件の申し立てがある[44]。最近の日本の政府調達における海外からの不服申し立ての事例には、JR 東日本(WTO 政府調達協定対象組織)の IC カードシステムの調達における Suica の採用に関するものがある。また、コンピュータの基本ソフトウェア(OS)の一つである TRON は、文部省(現文部科学省)と通産省(現経済産業省)が設立したコンピュータ教育開発センター(CEC)によって全国の中学校に導入されるパソコンの OS に指定されようとしていたが、アメリカ通商代表部(USTR)が、スーパー301 条に基づいて貿易障壁に指定したことから、計画が頓挫した経緯がある[45]。

以上に示した例を考慮すると、技術仕様に基づく政府調達基準について、特定の組織や企業によって策定された技術仕様に基づく政府調達基準は、WTO 政府調達協定に抵触するものと考えられる。一方、国際標準等の国や企業等との結びつきがない技術仕様に基づく政府調達基準は、WTO 政府調達協定に整合するものと考えられる。

2.1.2.3. FIPS と WTO 政府調達協定との整合性

NIST が発行する FIPS は、国家安全保障に係わる情報システムを除く情報システムに関する連邦政府の調達基準とみなされるが、外国企業の製品等を排除する規定が無く、WTO 政府調達協定の内外無差別の原則に抵触しないと考えられる[46,47]。また、FIPS に基づく製品認定制度である CMVP、NPIVP や ISO15408(CC)に基づく CCEVS などの制度においては、製品の評価・認証を行う検査機関を国内の機関に限定していないことや、海外の製品についても評価・認証の対象としていることなど、公正で透明性の高い調達手続き[48]を定めているため、WTO の協定と整合していると考えられる。

2.1.2.4. TBT(Technical Barriers to Trade)協定

TBT 協定は、国内規格を国際規格に整合させることにより、特定の企業や国が有利になるような貿易障壁を取り除くことを目的としている。TBT 協定は、WTO 協定の附属書 1A(E)に属する一括受託協定(WTO の全締約

---

[42] 日本については独立行政法人や JR なども含まれる。

[43] 米国の規制改革及び競争政策に関する日本国政府の要望事項 (2008 年 10 月 15 日)
http://www.mofa.go.jp/MOFAJ/area/usa/keizai/kanwa/pdfs/1999recom_j.pdf

[44] 各国の政府調達制度と WTO 政府調達協定との整合性 (JETRO, 2005 年 3 月)
http://www3.jetro.go.jp/jetro-file/search-text.do?url=05000960

[45] 出典:http://www.nhk.or.jp/special/libraly/05/l0008/l0828s.html

[46] 公開情報を調査した限りでは、FIPS を政府調達基準とすることに対する海外からの不服申し立ての事例はない。

[47] WTO 政府調達協定締約国は、調達機関の協定違反行為に対する苦情申し立てを行うことが可能となる。締約国に対して透明性が高く、効果的な手続きを整備することを義務づけているため(同20条2項)、米連邦政府の情報システム調達に関する協定違反に関する申し立て情報を探す手がかりとなる。

[48] WTO 政府調達協定第 17 条 透明性の規定。

国に適用される。）である。TBT 協定によって、各国における国内規格の作成過程の透明性や国内規格と国際規格との整合性が確保され、情報通信など国家間での相互運用性が求められる分野における規格の国際市場性(適合性)(Global Relevance [49])の促進につながると考えられる[50]。

2.1.3. 米国政府によるソフトウェア・アシュアランスの取り組み[51]

2.1.3.1. 全体俯瞰

米国政府によるソフトウェア・アシュアランス[19]の取組みは、企業や重要インフラによって使用されるソフトウェアを主な対象として、主に DHS、DoD、NSA、NIST によって推進されている。政府機関の中でも、早い時期に取り組みを開始した DoD は、政府調達基準における情報保証(Information Assurance [14])の派生概念として、ソフトウェア・アシュアランスという概念を創出したと考えられる。

図 2-4 に米国政府機関によるソフトウェア・アシュアランスの取組みの概観を示す。

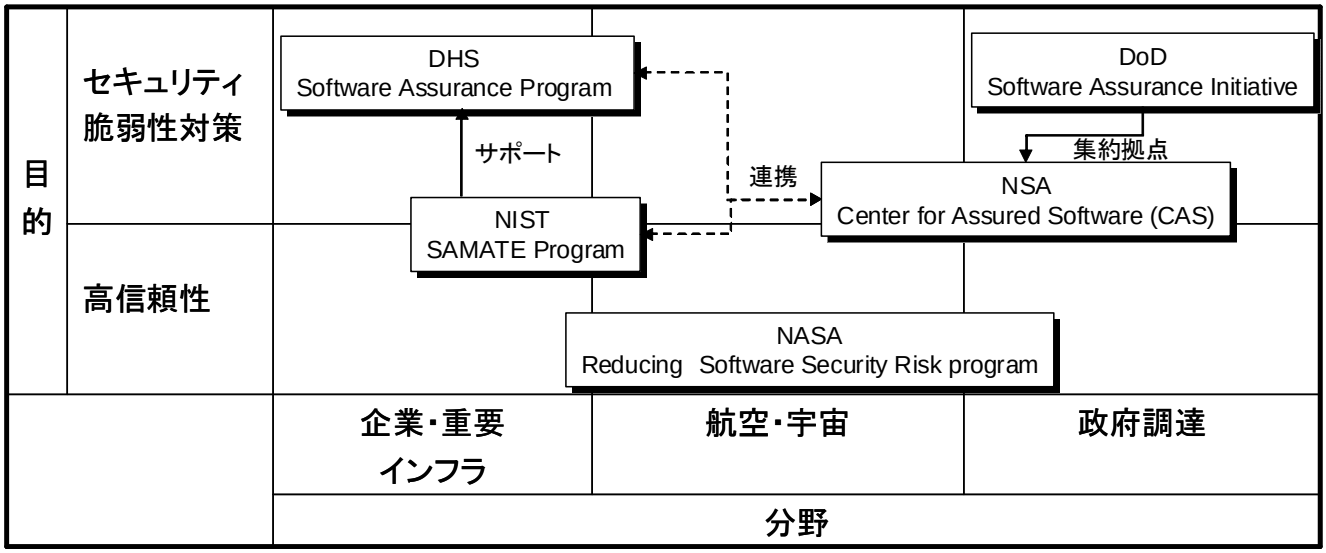

図 2-4:米国の政府機関によるソフトウェア・アシュアランスの取組み(概観)

2.1.3.2. 各省庁における取組み

2.1.3.2.1. DHSのソフトウェア・アシュアランス・プログラム[52,53]

DHS のソフトウェア・アシュアランス・プログラムは、DHS 内の NCSD(National Cyber Security Division：国家サイバーセキュリティ局) [54] により推進されるプログラムで、2007 年 10 月に運用が開始された。企業や重要インフラ事業者の業務に求められるセキュアな高信頼ソフトウェアを実現することを目指し、ソフトウェアの脆弱性削減や悪用の最小化のために、信頼性の高いソフトウェア製品の開発・インストールを促進することを目的とする。

DHS は、「セキュリティパラダイムを従来のパッチ管理からソフトウェア・アシュアラランスに移行させる」、つまり、

[49] 規格や標準が、世界各国において普遍的に適用可能であること。
[50] 出典 http://ja.wikipedia.org/wiki/%E8%B2%BF%E6%98%93%E3%81%AE%E6%8A%80%E8%A1%93%E7%9A%84%E9%9A%9C%E5%AE%B3%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E5%8D%94%E5%AE%9A
[51] Software Security Assurance State-of-the-Art Report http://iac.dtic.mil/iatac/download/security.pdf
[52] https://buildsecurityin.us-cert.gov/swa/
[53] http://www.us-cert.gov/swa/
[54] インターネット上の脅威からの防衛(サイバーセキュリティ)全般を担当する部局。2003 年 6 月に設立。

パッチの適用に頼るのではなく、ソフトウェアの開発の初期段階からソフトウェアの品質とセキュリティを高めるべきであるという考え方に基づいて、産官連携を基礎として、DHS の出資による会議とワークショップを通じて、ソフトウェアの開発者・設計者がソフトウェアの品質[55]や信頼性を向上させるための実践的なガイダンスのベースとなる共通の知識体系の構築を推進している。

政府、産業界、学会の関係者からなる以下のフォーラムやワーキンググループを実施している。

- Workforce Education & Training
  産学官のメンバーに対して適切にセキュリティが確保されたソフトウェアの生産方法を提供する。
- Processes & Practices
  ソフトウェア・アシュアランスの論点整理およびベストプラクティスの共有をミッションとする。
- Technology, Tools & Product Evaluation
  ソフトウェア・アシュアランスのツールと技術を、政府の情報システム調達におけるソフトウェア・アシュアランスの評価・認証のスピードと正確さを向上させる取組みに役立てることをミッションとする。
- Acquisition & Outsourcing
  ソフトウェアの調達者に、ソフトウェア・サプライチェーンのリスクについての情報を提供し、ソフトウェアの調達やアウトソーシングの意思決定に、どのようにソフトウェア・アシュアランスの考えを導入するかを検討する。
- Measurement
  既存の情報保証、ソフトウェア・アシュアランスの強化・調和に向けたアプローチを開発することをミッションとする。
- Business Case
  ソフトウェア・アシュアランスに準拠したソフトウェアとその要求事項についての理解と意識を高めることをミッションとする。
- Malware Attribution
  潜在的に悪意のある動作をするソフトウェアに対する理解を形成することをミッションとする。

2.1.3.2.1.1. Build Security In[56]

NCSD のソフトウェア・アシュアランスプログラムの中の一つのプロジェクトであり、ソフトウェア開発者、セキュリティ技術者などを対象としたプラクティス、ツール、ガイドライン、規則、原則や情報を提供することを目的とする。カーネギーメロン大学(Carnegie Mellon University)のソフトウェア工学研究所(Software Engineering Institute：SEI)が、プロセスと技術分野において支援を提供する。

セキュアコーディングに関する下記のような文書をまとめている。

- CERT C Programming Language Secure Coding Standard
- Top 10 Secure Coding Practices
- Secure Programming Skills Assessment

[55] DHS は明確な定義を行っていないが、ソフトウェアの品質評価に関する国際規格 ISO 9126 では、ソフトウェアの品質を、機能性、信頼性、ユーザビリティ、効率性、保守性、移植性により規定している。

[56] https://buildsecurityin.us-cert.gov/daisy/bsi/home.html

2.1.3.2.2. DoD のソフトウェア・アシュアランス・イニシアチブ[57]

商用ソフトウェア調達時のリスク評価に関する課題を検討するために 2003 年 7 月に設立された。このイニシアチブをフォローするために 2004 年 12 月に、国防総省の Assistant Secretary of Defense for Networks and Information Integration (ASD NII) [58] は、連邦政府が調達する商用ソフトウェアに関連するリスクの影響を低減するための包括的な戦略を開発することを目的として、Software Assurance Tiger Team と呼ばれる組織を設立した。この組織は、国防産業協会(National Defense Industrial Association (NDIA)) [59] と協力して、Software Assurance Summit 会議を開催し、下記のガイドブックを作成した。

名称	**Systems Assurance: Delivering Mission Success in the Face of Developing Threats—A Guidebook[60]**
作成主体	DoD Software Assurance Tiger Team, NDIA Systems Assurance Committee
作成時期	2006年11月
目的	不正に関する懸念、不確実性の低減、合理的な確信の基盤の提供などシステムエンジニアごとに異なる様々な視点に基づく開発のガイドラインを提供する。
経緯	DoDソフトウェア・アシュアランス・イニシアチブの取組みの中で開催されたソフトウェア・アシュアラランスサミット会議において作成された。
概要・特徴	システム工学における開発者ごとの関心の違いについて記述している。ソフトウェアに対する信頼性の基準を与えるとともに、ソフトウェア調達と工学的なアプローチに基づく意思決定法について示している。 十分な情報を持つエンジニアを対象として、基礎的な文書、標準、義務、プラクティスから重要な概念と原則を取り込み、システム・アシュアランスの観点から議論している。
メリット	幅広い視点からのプラクティスを把握することができる。
適用対象	システムエンジニア

ソフトウェアのセキュリティに関するその他のプロジェクトとして以下がある。

- DSB Task Force on Mission Impact of Foreign Influence on DoD Software
- DoDIIS Software Assurance Initiative
- US Army CECOM Software Vulnerability Assessments and Malicious Code Analyse
- Air Force Application Security Pilot and SoftwareSecurity Workshop

2.1.3.2.3. NIST Software Assurance Metrics And Tool Evaluation (SAMATE) [61]

NCSD[54] および DHS をスポンサーとし、NIST により 2004 年秋に開始されたソフトウェア・アシュアランスに関するプログラムである。ソフトウェアツールの評価、効率性の計測、ツールと手法のギャップの特定などのための方法を開発し、ソフトウェア・アシュアランスを改善させることを目的とする。DHS のソフトウェア・アシュアランスにおいて開発されたツールを支援する。

---

[57] DoD のソフトウェア・アシュアランスへの取り組みは、1999 年に Defense Science Board (DSB) により発表された勧告 : Task Force on Globalization and Security's final report に始まる。
[58] http://www.defenselink.mil/cio-nii/
[59] http://www.ndia.org/Pages/Default.aspx
[60] http://www.itaa.org/upload/es/docs/sys_assur_ndia_guidebook.pdf
[61] http://samate.nist.gov/index.php/Main_Page.html

2.1.3.2.4. NSA Center for Assured Software (CAS)

NSA と DoD のソフトウェア・アシュアランスの集約拠点として 2005 年に設立された。DoD の重要システムの脆弱性を低減するためのガイダンスと方法を提供する。DoD の Software Assurance Tiger Team や、DHS の Software Assurance Working Groups (WG)と密接な連携がとられている。また、NIST の Software Assurance Metrics and Tool Evaluation (SAMATE) プログラムとも連携を図っている。

- SSE-CMM(System Security Engineering - Capability Maturity Model)
  米国家安全保障局(NSA)の支援で開発された規格で、セキュアなシステムを開発・運用するための組織のプロセス能力を評価するための規格である。2002 年に ISO/IEC 21827 として国際標準化された。
  製品の評価を主眼とする ISO/IEC15408、組織の評価を主眼とする ISO/IEC/27000、技術ガイダンスであり GMITS の隙間を埋めるものと位置付けられる[62]。

2.1.3.2.5. NASA Reducing Software Security Risk (RSSR) program[63]

高信頼ソフトウェア・システムの開発プロセスにセキュリティを統合するための形式的分析アプローチを規定し、モデル検査手法による要求仕様の検証などについて取り組んでいる。

2.1.4. 民間企業・業界団体による取り組み

2.1.4.1. 概要

民間企業や業界団体によるソフトウェア・アシュアランスに関する取組みは、ソフトウェアベンダーやソフトウェア・サプライヤーなどから構成されるコンソーシアム形態によるものや、金融機関などユーザ系の業界団体などによるもの、これらの団体に大学、政府部門などの組織や個人などが多数参加するものや、官民のパートナーシップによるものがある。

各団体の作成するベストプラクティスやガイドラインは公開されているものが多く、相互に参照・利用されることで、産業界全体のソフトウェア・アシュアランスの水準の向上に寄与するものと考えられる。

2.1.4.2. 主な業界団体の取組み

2.1.4.2.1. SAFECode：Software Assurance Forum for Excellence in Code[64]

ICT 製品・サービスのセキュリティを向上させることを目的として 2007 年に設立された非営利組織である[65]。セキュアなソフトウェア、ハードウェア、サービスの開発・普及のためのベストプラクティスの確立を目指している。メンバー企業によって実践されているさまざまなベストプラクティスから共通部分を抽出し、統一的なベストプラクティスを作成しようという米国でのはじめての試み[66]である。

International advisory board(国際諮問委員会)を設置し、政府や学会からの意見も反映している。政府からの資金提供は無く、政府調達基準とはなっていない。

---

62 http://itpro.nikkeibp.co.jp/word/page/10005179/
63 http://rssr.jpl.nasa.gov/
64 http://www.safecode.org/
65 NCSD のソフトウェア・アシュアランスに関する調査を実施した SRI International の Jeremy J. Epstein 氏は、政府によって規制が行われるのを防ぐために、民間企業が自発的に取組みを行った結果、SAFECode が設立されたのではないかと、同氏に対する現地でのヒアリング調査においてコメントしている。
66 SAFECode の Exective Director である Paul Kurtz 氏へのヒアリングより。

会費は、役員会メンバーが US$50,000、一般会員が US$15,000 となっている。
以下の文書を公開している。

名称	Software Assurance：An Overview of Current Industry Best Practices[67]
作成主体	SAFECode
作成時期	2008年2月
目的	ソフトウェアの信頼性を保証するために、安全な開発手法と完全性(Integrity)管理に関する統一的なベストプラクティスを作成し、SAFECodeメンバーにおいて共有する。
経緯	ソフトウェア・アシュアランスを効率的に達成するために、ソフトウェアの信頼性確保に係る統一的なベストプラクティスを作成する必要があった。
概要・特徴	政府や民間企業に提供される製品の信頼性を保証するために SAFECode メンバーが利用している安全な開発手法と完全性(Integrity)管理に関するベストプラクティスをまとめたもの。
メリット	様々なベストプラクティスからエッセンスを抽出し、総合的なベストプラクティスとして統一することにより、効率的にソフトウェア・アシュアランスが達成される。
適用対象	ソフトウェアベンダー

名称	Fundamental Practices for Secure Software Development
作成主体	SAFECode
作成時期	2008年10月
目的	ベンダーごとに異なるセキュアなソフトウェアの開発手法をベストプラクティスとして統一する。
経緯	ソフトウェアの信頼性確保に係るベストプラクティスが、ベンダーごとに異なっており、業界としての統一的なベストプラクティスを作成する必要があった。
概要・特徴	ベンダーのセキュリティベストプラクティスを収集・分析し、そのコアセットをベストプラクティスとしてまとめている。
メリット	様々なベストプラクティスからエッセンスを抽出し、総合的なベストプラクティスとして統一することにより、効率的にソフトウェア・アシュアランスが達成される。
適用対象	ソフトウェアベンダー

2.1.4.2.2. OMG SwA SIG[68]

OMG SwA SIG は、コンピュータ産業の国際コンソーシアム OMG(Object Management Group)が推進するソフトウェア・アシュアランスに関する取組みである。

OMG プラットフォームおよびドメインタスクフォースや外部民間組織と協力して、ソフトウェアの信頼性向上のための共通フレームワークを作成することをミッションとしている。

共通フレームワークには以下の構成要素が含まれる。

- ソフトウェアの供給者や調達者が、それぞれの要求を満たすソフトウェア部品の仕様を記述するために利用することができるソフトウェアの性質に関するフレームワーク。
- システムインテグレーターが、安全に大規模なシステムを構築する際に使用するソフトウェア部品などの製品の検証。

[67] http://www.safecode.org/publications/SAFECode_BestPractices0208.pdf
[68] http://swa.omg.org/

ソフトウェア・アシュアランスの活動により以下の効果が期待される。

- KDM[69]、SPEM[70]などの関連する OMG 仕様の強化
- セキュアなソフトウェアの開発における OMG の仕様の利用促進
- OMG の仕様との組合せによる、様々な品質の成熟度を評価するモデルを強化するための方法の提示
- ソフトウェアの信頼性(Trustworthiness)向上を目的とした、ソフトウェア・アシュアランスのフレームワーク強化のためのシナリオの特定

ソフトウェア・アシュアランスに関する以下の文書を公開している。

名称	**A White Paper on Software Assurance**[71]
作成主体	OMG SwA SIG
作成時期	2007年2月
目的	ソフトウェアの利用者の観点から、ソフトウェアの安全性を確保するための確信の持てる開発プロセスに関する動向を整理する。
経緯	すべての産業において、業務のソフトウェアへの依存性が高まるにしたがい、ソフトウェアに起因する事故が発生した時のインフラやビジネスへの影響は大きくなる一方である。このような状況において、ソフトウェアの脆弱性の根本的な問題を解決し、ソフトウェアの信頼性を強化することが重要になっている。
概要・特徴	ソフトウェアのパッチのサイクルを短縮することでソフトウェアのセキュリティを向上させるのではなく、ソフトウェアの開発プロセスにおいてセキュリティを考慮するようにすることで、ソフトウェアの安全性を確保するためのプロセスに関する動向をまとめている。
メリット	ソフトウェア・アシュアランスに関するプロセスの状況が把握できる。
適用対象	ソフトウェア・サプライヤー

2.1.4.2.3. OWASP：Open Web Application Security Project[72]

官民組織においてソフトウェアおよびアプリケーションのセキュリティを担当する技術者に対して、高信頼アプリケーションソフトウェアをメンテナンスするための情報を提供することを目的としたプロジェクトである。非営利団体 WASF(Web Application Security Forum)によって実施されている。WASF は、ウェブアプリケーションのセキュリティにかかわる課題を研究し、安全性向上のための情報を共有することにより、適切な対策や構築手段に関する有効な情報を普及啓蒙することをミッションとしている。
ウェブアプリケーションとサービスのセキュリティ構築に関する以下のガイドを公開している。

名称	**A Guide to Building Secure Web Applications and Web Services**[73]

[69] Knowledge Discovery Metamodel： アプリケーションの振る舞い、構造、データを包括的に扱うためのモデル。
http://www.omg.org/technology/kdm/index.htm
[70] Software Process Engineering Metamodel： ソフトウェアプロセスを定義するためのメタモデルで、OMG が承認している UML(Unified Modeling Language)をカスタマイズしたプロファイル。
http://www.omg.org/technology/documents/formal/spem.htm
[71] http://adm.omg.org/SoftwareAssurance.pdf
[72] http://www.owasp.org/index.php/Main_Page
[73] http://www.owasp.org/index.php/Guide_Frontispiece

作成主体	WASF(Web Application Security Forum)
作成時期	2006年2月 (v2.1 Draft 3)
目的	ウェブアプリケーションのセキュリティの設計・構築・メンテナンスに必要な要素技術や、人、プロセス、管理に関する論点についてまとめる。
経緯	プロジェクト開始時には、セキュアコードの書き方に関するガイドはあったが、ウェブアプリケーションのセキュリティに関して広範な技術俯瞰を行う公開されたドキュメントが存在しなかった。
概要・特徴	セキュリティの要求レベル、アーキテクチャ、認証、ユーザセッションの管理、アクセス制御、ログ管理、共通的な問題の回避などについてまとめている。
メリット	ウェブアプリケーションのセキュリティに関する様々な問題についての認識が深まる。
適用対象	ウェブアプリケーションベンダー

他に、以下の文書が公開されている。

- Web Security Certification Criteria[74]
- Spring Of Code 2007： ウェブアプリケーションのコードレビューを行うプロジェクトの報告書

2.1.4.2.4. WASC：Web Application Security Consortium[75]

専門家、企業の技術者、組織の代表者などによって設立された国際的な組織で、WWW のためのオープンソースの広く合意の取れたベストプラクティス・セキュリティ標準を作成することを目的とする。

以下の文書を公開している。

名称	**Web Application Exposure to Risk ： Raising Awareness to Build Confidence and Improve Security**[76]
作成主体	WASC
作成時期	2004年7月
目的	ウェブアプリケーションが脆弱性を持つ可能性を評価し、意思決定者がウェブアプリケーションのどの部分にセキュリティ対策のリソースを割くべきかを判断するための材料を提供する。
経緯	不明
概要・特徴	ウェブアプリケーションが、アーキテクチャ、複雑性、データ操作、ソフトウェアのインストールなどに起因する脆弱性を持つ可能性のことを exposure と定義し、アプリケーションと Exposure の関係、アプリケーションのセキュリティ対策への人的資源配分を決めるための Exposure 情報の使い方などについてまとめている。
メリット	ウェブアプリケーションソフトウェアの脆弱性に関する評価方法が理解できる。
適用対象	ウェブサイト構築事業者

また、以下のウェブアプリケーションのセキュリティに関する文書をまとめている。

[74] 文献 51 に文書名が記載されているが、OWASP のホームページでは詳細情報は得られなかった。
[75] http://www.webappsec.org/
[76] http://www.ntobjectives.com/datasheets/WebApplicationExposureWhitePaper.pdf

- Frequently Asked Questions on Web Application Security (2004 年 1 月) [77]

2.1.4.2.5. National Cyber Security Partnership : NCSP[78]

米国の重要インフラをよりセキュアにするための共通戦略およびプログラムを作成することを目的として、官民パートナーシップとして設立された。

ソフトウェア開発ライフサイクルに関する以下の報告書を発行している。

名称	**Security Across the Software Development Life Cycle**[79]
作成主体	NCSP
作成時期	2004年4月
目的	ソフトウェアの標準、ツール、評価法によって計測可能な脆弱性を明確化することを目的とする。
経緯	ソフトウェアのセキュリティを向上させるために、ライフサイクルの観点からソフトウェアの脆弱性を削減する取り組みを行う必要性が高まった。
概要・特徴	ソフトウェアのための標準、ツールなどにより脆弱性の削減実現する方法、迅速なパッチ適用のための新たなツールと手法、重要インフラ全体に渡るベストプラクティスの適用について検討している。
メリット	重要インフラのソフトウェアのパッチ開発とベストプラクティスの適用法を知ることができる。
適用対象	ソフトウェアベンダー

2.1.4.2.6. VISA USA Payment Application Best Practices (PABP)

VISA は、決済アプリケーションソフトウェアのベンダー(開発者、販売者)が、決済アプリケーションを開発する際に参照するためのベストプラクティスとして、PCI/DSS(Payment Card Industry Data Security Standard)[80]に準拠した Payment Application Best Practices (PABP) [81] を開発した。

PABP の概要は以下の通りである。

名称	**Payment Application Best Practices (PABP)** [82]
作成主体	VISA International
作成時期	2007年1月
目的	決済アプリケーションが満たすべき要件を明確化し、ソフトウェアベンダーが、セキュアな(PCI DSS に準拠した)決済アプリケーションを開発するのを支援する。
経緯	セキュアな決済アプリケーションの必要性が高まった。
概要・特徴	POS(販売時点管理)決済アプリケーションが満たさなければならないセキュリティ要件をまとめたもの。要件は PCC/DSS および PCC/DSS 監査手続きに準拠している。
メリット	決済アプリケーションが満たすべきセキュリティ要件が明確になる。
適用対象	決済アプリケーションベンダー(アプリケーションを開発・販売する事業者)

[77] 文献 51 に文書名が記載されているが、WASC のホームページでは詳細情報は得られなかった。
[78] http://www.cyberpartnership.org/about-overview.html
[79] http://www.cyberpartnership.org/init-soft.html
[80] https://www.pcisecuritystandards.org/
[81] https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml
[82] http://usa.visa.com/download/merchants/cisp_payment_application_best_practices.doc

PABP の管理は、2008 年 1 月より、国際ペイメントブランド共通認定のためのクレジットカード情報保護を目的とした情報セキュリティ基準である PCI SSC(PCI Security Standards Council：PCI セキュリティ基準協議会)に移管された。POS 決済アプリケーションを開発・販売する事業者が対象となっている。

名称	PA-DSS(Payment Application Data Security Standard)
作成主体	PCI SSC(PCI Security Standards Council：PCIセキュリティ基準協議会)
作成時期	2008年4月
目的	PCI DSSに準拠したセキュアな決済アプリケーションの開発を支援する。
経緯	PABPからの移行。
概要・特徴	決済アプリケーションのセキュリティ要件を規定したもので、決済アプリケーションをサードパーティに販売・配布・ライセンス提供するアプリケーションベンダーに適用される。
メリット	決済アプリケーションが満たすべきセキュリティ要件が明確になる。
適用対象	決済アプリケーションベンダー(アプリケーションを開発・販売する事業者)

2.1.4.2.7. ICASI：Industry Consortium for Advancement of Security on the Internet[83]

IT セキュリティをグローバルに推進するために、Cisco、IBM、Intel、Juniper Networks、Microsoft の 5 社が 2008 年に設立した非営利団体。メンバー各社が協力して情報を共有することで、共通するセキュリティ問題を迅速に認識し、効率よく解決することを目標とする。各社のソフトウェア製品に存在する脆弱性や各種の脅威に対して、協力して対応策を検討する。

脆弱性の公開と対応に関する以下の文書を作成している。

名称	**Common Frameworks for Vulnerability Disclosure and Response (CVRF)** [84]
作成主体	ICASI
作成時期	不明
目的	脆弱性情報の交換のための共通フレームワークを構築する。
経緯	不明
概要・特徴	ソフトウェアの脆弱性情報を交換するための共通フレームワークを構築する。産業界の多様なフレームワークを共通の統合化されたアプローチとして拡張・統合する。
メリット	脆弱性情報管理のための統一化されたアプローチを習得することができる。
適用対象	ソフトウェアベンダー

2.1.4.2.8. AMTSO：Anti-Malware Testing Standards Organization[85]

マルウェア対策製品のテストに関する客観性、品質、適切性を改善し、標準やベストプラクティスを作成することを目指して、セキュリティ関連ソフトウェアのベンダーやセキュリティサービスプロバイダ等の約 40 社が参加して 2008 年に設立された団体。

[83] http://www.icasi.org/
[84] http://www.icasi.org/projects.htm#CVRF
[85] http://www.amtso.org/

クラウドコンピューティング(インターネット経由でアプリケーション等のサービスを提供する形態)によって提供されるセキュリティ製品のテストに関するベストプラクティスについて、以下の文書を公開している。

名称	**AMTSO Best Practices for Testing In The Cloud Security Products**[86]
作成主体	AMTSO
作成時期	2009年5月
目的	クラウドコンピューティングを利用して提供されるアンチマルウェア・ソリューションのテストに関するガイドラインを提供すること。
経緯	不明
概要・特徴	クラウドコンピューティングを利用して提供されるアンチマルウェア・ソリューションの正確なテストに関わる課題や、有効かつ有用なテスト結果を得るためにはどのようなテストを設計すべきかについて概観し、テストのガイドラインをまとめている。
メリット	クラウドコンピューティングにより提供されるサービスのテストに関する知見が得られる。
適用対象	アンチマルウェア・ソリューション開発ベンダー

2.1.4.2.9. Software Assurance Consortium (SAC) [87]

2007 年に設立されたコンソーシアムで、既存のソフトウェア・アシュアランス関連の団体に参加していない組織が参加できるようなコンソーシアムとして設立された。多くのセクタの民間企業や政府の CIO などが参加している。

他のコンソーシアムが作成したガイドラインと類似のものを複製するのではなく、OWASP などの団体のガイドラインの成果を要素とする全体フレームワークを作成することを目指す。

現在、SAC のホームページでは、様々な団体が作成したソフトウェア・アシュアランス等に関するガイドラインへのリンク集を提供している。今後、これらのガイドラインを要素とした全体フレームワークを作成すると予想されるが、現時点では、全体フレームワークは公開されていないようである。

2.1.4.2.10. BITS：Financial Services Roundtable Software Security and Patch Management Initiative[88]

BITS は、米国の大手金融機関 100 社をメンバーとするコンソーシアムであり、金融取引におけるセキュリティ、プライバシー、インテグリティを確実なものとし、利用者の信頼・信用を維持することを目的として 1996 年に設立された。

BITS Product Certification Program (BPCP) [89] と呼ばれる、ソフトウェアアプリケーションとインフラストラクチャ製品をテストするためのプログラムで、コモンクライテリアとの整合性を持つプログラムを開発した。 BPCP は、金融サービス業によって確立されたセキュリティベースライン基準に基づいている。

[86] http://www.amtso.org/uploads/amtso-best-practices-for-testing-in-the-cloud-security-products.pdf
[87] http://swaconsortium.org/
[88] http://www.bits.org/
[89] http://www.bits.org/downloads/BPCP/BPCPFAQs.pdf

2.1.4.3. 重要インフラ分野等における情報セキュリティ

2.1.4.3.1. 米国の重要インフラ分野における規制体系(10CFR Part50) [90]

米国の原子力分野における規制は、連邦規則(Title 10, Code of Federal Regulation:10CFR) [91] を最上位の規制として、以下、行政指導等、指針および民間基準等へと細分化される体系に基づいて実施されている。また、最近では、材料や寸法など、明確な合否判定がしやすい「仕様規定」を中心とした規則体系から、本来果たすべき目的や機能を規定する「性能規定」を重視した規則体系となってきている。例えば、原子力発電所において、不十分な保守によって機器の故障が生ずるのを最小限に抑えるために、米国原子力規制委員会[92] (Nuclear Regulatory Commission: 以下 NRC)は、設置者が遵守すべき要件を記載した保守規則(10CFR50.65)を作成している。この中で、保守規則の対象となる構造物、系統、機器については原則的規定のみとなっており、「性能規定」に重点が置かれたものとなっている。

産業界のガイドラインとしては、原子力管理人材協議会(現米国原子力協会:NEI)が作成した、設置者が保守規則に対応する際に参照するガイドライン(NUMARC 93-01)があるが、これを NRC は、ガイドライン「原子力発電所の保守の有効性の監視」(R.G.1.160)の中で容認している。

このように米国の規制は、原則的要件のみを示したものである場合が多く、原則的要件に適合するための手段として何を用いるかについては、設置者の自主的判断に任せるという柔軟なものとなっている。1998 年には行政管理予算局から各連邦政府機関の長官に宛て、「自主規格の作成及び使用に関する連邦政府の関与」という文書(Circular A-119(改訂版))が発信され、民間規格の優先利用、政府規格の民間規格による代替可能性等の提案が示された。これにより、民間規格は、Regulatory Guide、連邦規則(10CFR)、標準審査指針、技術仕様書、一般通達文書などの政府文書において積極的に引用されるようになった[93]。

2.1.4.3.2. Regulatory Guide 1.152 - Criteria for Digital Computers in Safety Systems of Nuclear Power Plants[94]

NRC の「原子力発電所の安全系におけるデジタルコンピュータの使用において高い機能信頼性と設計品質を促進するための規制」に準拠する際に参照されるガイドラインで、原子力プラントの安全系統(安全システム)におけるコンピュータの信頼性と設計品質が規定されている。デジタル計測制御システムは、データ伝送及びプロセス用機器を広範囲に共有しており、これが、アナログ式の制御システムと比較した場合のデジタルシステムの多くの利点のベースとなる一方、異なるタイプの故障に対する脆弱性を高める原因ともなっている。この脆弱性は、たとえば、共用のデータベースとプロセス用機器を使用するという設計によって、冗長な設備に共通に存在する故障原因が伝播される可能性があるというものである。他の脆弱性は、ソフトウェアのプログラミングエラーによって、ハードウェアの構成上の工夫によって達成される、セキュリティ確保のための冗長性が破られるというものである(ソフトウェアによる共通原因故障)。これらの脆弱性を解決するために、機能内及び機能間の共通原因故障の伝播に対して、多重防護を実施する必要性が大きいとされている。

2.1.4.3.3. ANSI/ANS-51.1 Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants[95]

固定式加圧水型原子炉プラントにおけるストラクチャ、システム、コンポーネントの原子力安全性基準及び機能

---

[90] http://www.nrc.gov/reading-rm/doc-collections/cfr/part050/
[91] http://www.nrc.gov/reading-rm/doc-collections/cfr/
[92] http://www.nrc.gov/
[93] 電気評論(Electrical Review) 2007 年 5 月 (ISSN0285-5860)
[94] http://www.orau.org/ptp/PTP%20Library/library/NRC/Reguide/01-152.pdf
[95] http://www.new.ans.org/store/i_240116/r_a

的設計要件に関する基準である。運用、保守、検査要件についても設計規定に影響を及ぼすものについては、この基準の対象となる。これらの安全性基準や設計基準は、他の特殊な設計基準にも関係し、Code of Federal Regulations, Title 10 のエネルギーの Part 50 "Licensing of Production and Utilization Facilities" や Appendix A "General Design Criteria for Nuclear Power Plants" における基準を詳細に説明するものである。

2.1.4.3.4. RTDA DO-178B[96]（航空分野）

1992 年に米国の航空無線技術委員会(RTCA: Radio Technical Commission for Aeronautics)によって作成された、米国における航空用ソフトウェアの開発ガイドラインを定義したもので、事実上の業界基準になっている。欧州では ED-12B と呼ばれている。主にソフトウェアの開発プロセスに関する規格であり、飛行システムと飛行装置に対する 66 項目のソフトウェア認定安全目標が定められている。

DO-178B に準拠していることの認定を受けるには、多数の裏づけ書類や記録の提示が必要であり、必要となる書類や情報の量は受けようとする認定のレベルによって決まる。認定レベルには、ソフトウェアの不具合によって起こる結果(壊滅的、非常に危険、メジャー、マイナー、影響なし)によって A～E の 5 段階があり、レベル A が最も厳しい。66 項目の各安全目標ごとに、認定レベルによってソフトウェアが満たすべき基準が定められている[97]。

[96] http://www.rtca.org/downloads/ListofAvailableDocs_April_2009.htm#_Toc228074101
[97] 出典：高信頼ソフトウェア構築技術に関する動向調査、情報処理推進機構

2.2. EU(欧州連合)

EU における情報セキュリティ政策の担当部局としては、情報社会・メディア総局[98] (Directorate-General for Information Society and Media)、企業・産業総局[99](Directorate-General for Enterprise and Industry)、司法・自由・安全総局[100] (Directorate-General for Justice, Freedom and Security)がある。また、情報セキュリティの分野においては ENISA(欧州ネット・情報セキュリティ機関:European Network and Information Security Agency) [101] が中心的な役割を果たしている。

ICT 製品・サービスの情報セキュリティに関する EU の取組みを以下にまとめる。

2.2.1. 政策的な取組み

2.2.1.1. ネットワーク情報セキュリティ : 欧州指針の提案(COM(2001)298) [102]

ネットワーク情報セキュリティ:欧州指針の提案(Network and Information Security : Proposal for A European Policy Approach)は、電子通信サービスとデータ保護に関するフレームワークを統合し、ネットワーク情報セキュリティを向上させるための欧州の指針を定めている。ストックホルム欧州協議会における要求に基づき、情報セキュリティに対する意識向上、研究開発支援、市場を意識した標準化などに関する一連の具体的な施策をリストアップしている。

2.2.1.2. ITSEC (Information Technology Security Evaluation Criteria) [103]

ITSEC は、英国、ドイツ、フランス、オランダの 4 ヶ国が、情報セキュリティに関する欧州統一評価基準として開発した評価基準で、1991 年 6 月に公開された version 1.2 から運用が開始された。

コモンクライテリアと ITSEC との保証レベルの関係は以下のようになる[104,105]。

コモンクライテリア	ITSEC
-	E0
EAL1	-
EAL2	E1
EAL3	E2
EAL4	E3
EAL5	E4
EAL6	E5
EAL7	E6

2.2.1.3. EN 50129(欧州鉄道信号規格)

IEC 61508 : Functional safety of electrical/electronic/programmable electronic safety-related systems[106]

98 http://ec.europa.eu/dgs/information_society/index_en.htm
99 http://ec.europa.eu/enterprise/index_en.htm
100 http://ec.europa.eu/justice_home/index_en.htm
101 http://www.enisa.europa.eu/index.htm
102 http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf
103 http://www.bsi.de/zertifiz/itkrit/itsec-en.pdf
104 http://www.ipa.go.jp/security/ccj/cc_tutorial/faq_index.html
105 コモンクライテリア、ITSEC 等に関する文献 : http://www.ipa.go.jp/security/ccj/cc_tutorial/cc_history/cc_history.html
106 電気(electric)・電子(electronic)・プログラマブル電子(programable electronic)(E/E/PE)製品の機能に関する安全性を高めるための国際規格。 http://www.iec.ch/zone/fsafety/fsafety_entry.htm

をベースに作成された規格であり、鉄道信号システムの安全性要件とドキュメント管理について規定したものである。信頼性管理、安全性管理、機能および技術的安全性に関して、問題が発生した場合の影響の大きさ、問題の発生頻度等が一定レベル以下であることの証明を求めている。特に信号保安装置等については、最も高い安全性レベルである SIL(Safety Integrity Level)4 [107] が要求されている[108]。

2.2.1.4. 情報セキュリティ証明書手引き[109]

2007 年 12 月に発表された ENISA のレポート「情報セキュリティ証明書手引き: 製品、人、プロセス(Information Security Certifications - A Primer: Products, people, processes)」において、製品、人、プロセスに関して、情報セキュリティの認定と保証(Accreditation & Certification)スキームに基づく評価が行われている。

2.2.1.5. Strategy for a secure information society (COM(2006)251) [110] : 安全な情報社会のための戦略

公的機関、民間企業、個人ユーザの情報セキュリティに関する課題を提示し、その解決のための対話とパートナーシップおよび意識向上によるアプローチや、協議と対話のプロセスの要件を示している。

2006 年 5 月 31 日施行。

2.2.1.6. Common regulatory framework for electronic communications networks and services (Directive 2002/21/EC) [111] : 電子通信ネットワーク・サービスのための共通規制フレームワーク

電子通信ネットワークとサービスの規制に関する共通フレームワークを規定。2002 年 3 月制定。

2.2.1.7. Directive on privacy and electronic communications (Directive 2002/58/EC) : プライバシーと電子通信に関する指令

電子通信分野における個人情報の扱いおよびプライバシー保護に関する規定。2002 年 7 月制定。

2.2.1.8. 消費者保護関連のEU指令

情報セキュリティの観点から、消費者保護に関連すると考えられる EU 指令には、以下のようなものがある。

- Directive 85/374/EEC (1985 年 7 月 25 日) (Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products) [112]

  不良品に関する責任の所在について規定している。ソフトウェアの不具合は、期待される機能から外れた動作であるという点において不良品であると判断されることから、理論的には対象範囲になると考えられる。
- Directive 91/250/EEC (1991 年 5 月 14 日) (Council Directive 91/250/EEC of 14 May 1991 on the

---

107 電子製品の機能安全に関する国際標準 IEC 61508 における安全水準の区分。システムに存在するリスクを4段階に分類し、機能失敗確率(PFD: Probablity of Failure on Demand)として準定量的に定義したもの。SIL の算出手法は IEC 61508 の第 5 部に示されている。

108 高信頼ソフトウェア構築技術に関する動向調査 http://sec.ipa.go.jp/reports/20080606.html

109 http://www.enisa.europa.eu/doc/pdf/deliverables/inf_sec_certification_2008.pdf

110 http://europa.eu/legislation_summaries/information_society/l24153a_en.htm
http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf

111 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:EN:HTML

112 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31985L0374:en:NOT

legal protection of computer programs) [113]
コンピュータプログラムの法的保護などに関する規定。

- Directive 1999/93/EC (1999 年 12 月 13 日) (Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures)[114]
  電子署名のフレームワークに関する規定。

2.2.2. 民間の取組み

2.2.2.1. ISI(The Integral Satcom Initiative)

ISI[115]は、衛星通信ネットワークに関連するステークホルダにより構成される組織であり、EU の研究開発プログラム FP7 において、研究者や産業界などのコミュニティ構築の役割を担う。EU が策定した ISI の戦略的研究アジェンダ[116]において、ISI が取組むべき分野として以下が挙げられている。

- インターオペラビリティと相互ネットワーキング
- 衛星ブロードバンド回線
- 衛星放送
- 移動体衛星サービス
- セキュリティ
- 衛星通信部門の共通プライオリティ

「セキュリティ」分野の重要項目には、異なるプラットフォームを有するホストなどが接続された異質ネットワークにおけるセキュリティの確保、エント・トゥ・エンドでの安全かつ信頼できる通信の確立などがある。25 か国から衛星通信ネットワーク関連の 167 団体が参加している。

113 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0250:EN:HTML
114 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML
115 http://www.isi-initiative.org/
116 http://cordis.europa.eu/technology-platforms/pdf/isi.pdf

2.3. イギリス

2.3.1. 政府の取組み

2.3.1.1. SYS (System level evaluations) [117]

SYS は、IT ソリューションのセキュリティア・シュアランスに関する MOD(英国防衛省)の要求事項を満たすために、CESG(Communications-Electronics Security Group ： 通信機器セキュリティグループ) [118] によって開発された評価手法であり、CC(コモンクライテリア)から派生したものである。防衛省の典型的な IT システムは、様々なベンダーの製品から構成されており、単一のデータセンタに導入されたシステムが、多くのサイトをカバーするエンタープライズレベルのソリューションとして広く使用される場合があることから、このような評価手法が開発された。

2002 年にイギリスの IT セキュリティ評価基準制度(UK IT Security Evaluation Criteria (ITSEC) method)として形式化された。

2.3.1.2. FTA (Fast-track assessments) [117]

FTA は、システムレベルのアプローチにより得られる利益と、そのアプローチが全ての英国政府プロジェクトに対してより広く適用できることを認識した CESG が、特定の製品の評価や特定のコンポーネントの導入といった目的に利用できる、より一般的で有用な fast track 評価スキームとして定義したものである。

事前に評価にかかる期間とコストを予測することができる点が特徴であり、より少ないコストで評価できる、つまり、規模が小さい政府機関の予算でも評価が実施できるように設計されている。

2001 年に、CESG IA サービスとして運用が開始された。

2.3.1.3. CHECK (IT security health checks) [117]

イギリス政府のネットワークおよびソリューションを対象として実施されるペネトレーションテストおよび脆弱性テストに関する基準。もともとは、ネットワークのテストにフォーカスしたものであったが、最近になって、ウェブベースのアプリケーションおよび、複数のソフトウェアパッケージの相互作用、それらの設定状況、カスタマイズされたアプリケーションコードの存在によって顕在化する脆弱性のそれぞれを対象としたテストサービスが新たに追加された。

機密性の高い政府情報システムをインターネットに接続することに関わる全ての英国政府プロジェクトに対して、CHECK サービスの実施が義務付けられる。

FTA とは異なり、CC から派生したものではない。1998 年に運用が開始されている。

2.3.1.4. CAPS (CESG Assisted Products Scheme) [117, 119]

CAPS は、CESG による、ベンダーを対象として暗号技術に関する支援を行う制度である。ベンダーは CAPS のガイドラインに従って政府調達製品を開発し、当該製品を対象として CAPS 基準による評価・認定を受ける。CAPS 認定を受けた製品は、政府調達品としてお墨付きを得ることができる。

CAPS において、製品が有する保護レベル(強度)は、「Baseline(ベースライン)」、「Enhanced(エンハンスド)」、「High Grade(ハイグレード)」の三段階で評価される。ベースラインで保護の対象とされている「Restricted(制限

---

117 http://www.stsc.hill.af.mil/CrossTalk/2007/03/0703SloanOrmerod.html

118 政府調達における暗号製品の仕様の規定・評価を行う政府機関で、GCHQ(政府通信本部)の傘下にある。
Information Assuarance & Consultancy Services(IACS)という製品評価サービスを政府及び公共部門に提供している。
http://www.cesg.gov.uk/

119 http://www.cesg.gov.uk/products_services/iacs/caps/index.shtml

あり)」より機密性レベルが低い「Private(プライベート)」に分類される情報の取扱いには、FIPS 140-2 の適合認定取得製品の使用が奨励される[120]など、米国の FIPS 140-2 が正式に調達要件として採用されている。

CAPS に基づく評価結果は、CC による公式の評価に組み込むことが可能である。[121]。

図 2-5 に、各国政府の情報セキュリティ基準の関係を示す。

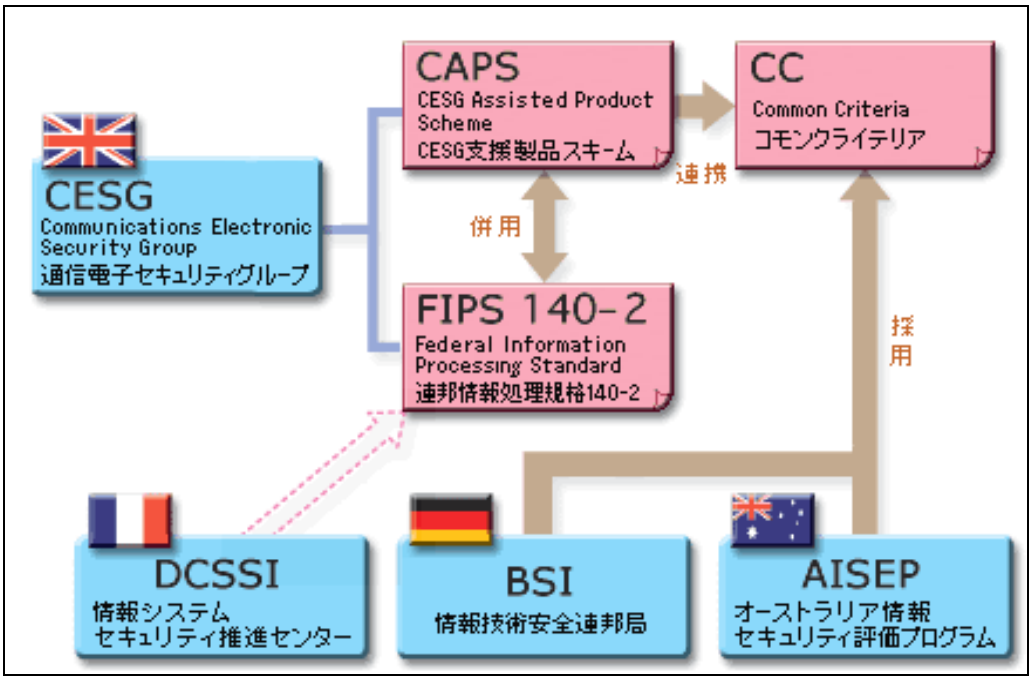

図 2-5:各国政府の情報セキュリティ基準の関係[122]

2.3.1.5. CSIA CCTM(Central Sponsor for Information Assurance Claims Tested Mark) [117]

CESG の支援の基で、CSIA(Central Sponsor for Information Assurance： 中央情報保障局[123])によって策定されたエントリーレベルのアシュアランス・メソッドで、短期間かつ低コストで評価できるのが特徴である。すべてのセキュリティ製品とサービスに対して適用可能であり、イギリス政府調達リストに採用されるためには、最低限この評価を受けることが必要となる。

2005 年にパイロット運用が開始され、現在正式に運用されている。

2.3.1.6. 各情報セキュリティ基準に基づく評価・認証に要する時間とコストの比較 [117]

図 2-6 に、英国において使用されている各種セキュリティ基準に基づく評価・認証に要する時間とコストを比較したものを示す。この図は、所要時間・コストの平均的なレンジを示したものであるが、一般的に評価・認証の基準やプロセスが厳格であるほど、所要コスト・時間が大きくなり、また、評価・認証の対象となるシステムやコンポーネントが大規模で複雑なものになれば、それに比例して所要コスト・時間も増えることになる。

---

120 http://www.cesg.gov.uk/products_services/iacs/evaluations.shtml
121 http://www.cesg.gov.uk/publications/media/iacs.pdf
122 http://dev.sbins.co.jp/cryptography/CMVP05.html
123 内閣府(Cabinet Office)傘下の組織で、公共セクター(中央政府から地方政府機関まで)の情報システムと IT の認定に関して、全市民に対する責任(pan-civil government responsibility)を負う。http://www.cabinetoffice.gov.uk/csia.aspx

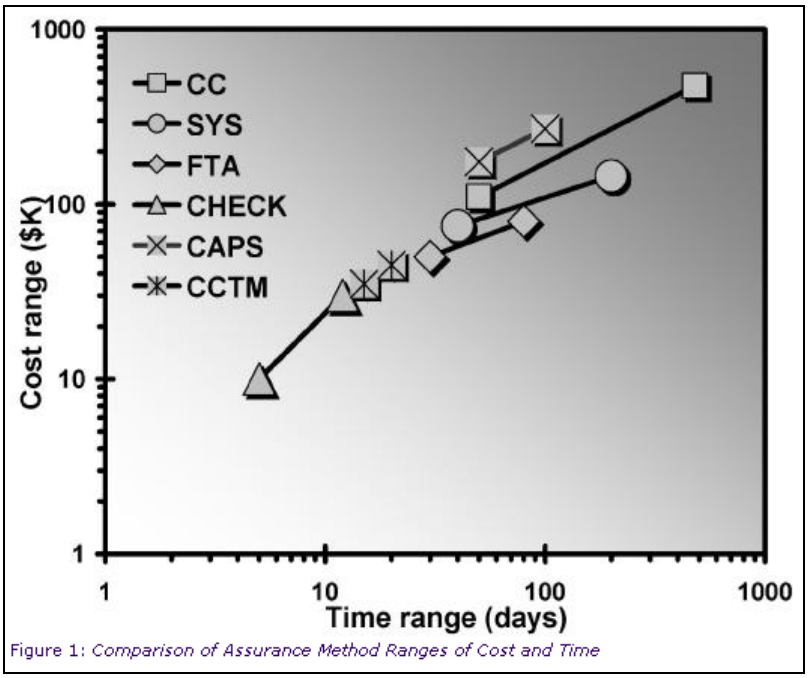

図 2-6:各種セキュリティ基準に基づく評価・認証に要する時間とコスト

表 2-4 は、英国において利用されている各種セキュリティ基準の特徴を整理したものである[117]。

表 2-4:英国で利用されている各種セキュリティ基準の特徴

Assurance Requirement	CC	SYS	FTA	CHECK	CAPS	CCTM
Certified product mark	✔				✔	✔
Mutual recognition	To EAL 4					
High assurance	✔				✔	
Medium assurance	✔	✔	✔		✔	
Low assurance				✔		✔
Pass/fail outcome	✔			✔	✔	✔
Risk enumeration		✔	✔	✔		
Flexible re-use	✔					✔
Project specific		✔	✔	✔		
Deployment specific		✔	✔	✔		
End to end		✔		✔		
Bespoke specific		✔	✔	✔		
Multi-product/vendor	In V 3.1	✔		✔		
Polymorphic products				✔		✔
Architecture/system		✔		✔		
Service delivery						✔
UK national requirements		✔	✔	✔	✔	
Deployment testing		✔		✔		
Open ended/iterative	✔				✔	
Time bounded		✔	✔	✔		✔
Low cost			✔			
Very low cost				✔		✔

2.3.1.7. CPNIのGood Practice Guidelines [124]

CPNI(Centre for the Protection of National Infrastructure：国家インフラストラクチャ保護センター) [125] は、国家インフラセキュリティ調整センター(National Infrastructure Security Co-ordination Centre (NISCC))とMI5 (Military Intelligence 5 ： 情報局保安部)の一部、国家セキュリティアドバイスセンター(National Security Advice Centre (NSAC))が合併して、2007 年 2 月 1 日に設立された政府組織であり[126]、国家の重要なインフラストラクチャへの脅威を払拭するために国家(重要)インフラストラクチャ事業者および組織(政府組織)に対してセキュリティに関するアドバイスを行う。

情報セキュリティの分野では、情報窃盗に対する防御法、個人情報のセキュリティのリスク評価、

[124] http://www.cpni.gov.uk/Products/guidelines.aspx
[125] http://www.cpni.gov.uk/
[126] http://www.cpni.gov.uk/about.aspx

プロセス制御・SCADA のセキュリティ等のグッドプラクティスガイドラインを発行している。

2.3.2. 民間・業界団体における取組み

2.3.2.1. イギリス規格協会(BSI: British Standards Institution)

2.3.2.1.1. BS ISO/IEC 27001:2005 [127]

Information technology. Security techniques. Information security management systems. Requirements

組織のビジネスリスクに関して、文書化された「情報セキュリティマネジメントシステム(ISMS)」を確立、導入、運用、監視、レビュー、保守、改善するための要求事項を規定したもので、政府、民間企業、非営利組織等すべての組織に適用可能である[128]。

BS7799-2:2002 に代わるものとして、ISO/IEC 27001 をベースとして BSI によって発行されたバージョンであり、内容は ISO/IEC 27001 と同一である[129]。2005 年 10 月 18 日に発行された。

2.3.2.1.2. BS ISO/IEC 27002:2005, BS 7799-1:2005, BS ISO/IEC 17799:2005 [130]

Information technology. Security techniques. Code of practice for information security management

組織において情報セキュリティマネジメントを開始、導入、維持、改善するためのガイドラインや一般原則となる国際標準であり、BS ISO/IEC 17799:2000、BS 7799-1:2000 に代わるものとして 2005 年 6 月 16 日に発行された。ISO/IEC 27002:2005 の技術的な内容は、ISO/IEC 17799:2005 と同一である[131]。
ISO/IEC 27002:2005 には、情報セキュリティマネジメントの各種領域におけるコントロール目標およびコントロールのベストプラクティスが含まれる。

時系列に見ると、1999 年に発行された BS 7799-1:1999 から、ISO/IEC 17799:2000(初版)、ISO/IEC 17799:2005(2005 年改訂)を経て 2007 年に ISO/IEC 27002:2005 に改称された。
上記規格の対応関係を以下に示す[132]。

英国規格	国際規格	日本工業規格	備考
BS 7799-2	ISO/IEC 27001	JIS Q 27001	ISMS 要求事項
BS 7799-1	ISO/IEC 17799 → ISO/IEC 27002	JISQ X 5080 → JIS Q 27002	ISMS 実践のための規範

2.3.2.1.3. BS ISO/IEC 27005:2008 [133]

Information technology. Security techniques. Information security risk management

組織における情報セキュリティマネジメントのガイドラインとなる国際標準であり、BS ISO/IEC TR 13335-3:1998、BS ISO/IEC TR 13335-4:2000 に代わるものとして 2008 年 6 月 30 日に発行された。

特に、ISO/IEC 27001 の要求事項をサポートするもので、政府、民間企業、非営利組織等すべての組織に適用可能である。

リスクベースの標準である BS ISO/IEC 27001 を使用する場合、BS ISO/IEC 27005 は、リスクの主体に対する追加的なガイダンスを提供するのに非常に有効である。

---

127 http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030126472
128 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103
129 http://www.bsigroup.com/en/Standards-and-Publications/Industry-Sectors/ICT/Information-Security/BS-ISOIC-270012005-FAQs/
130 http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030166440
131 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297
132 http://ja.wikipedia.org/wiki/ISO/IEC_27002
133 http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030117274

2.3.2.1.4. BS 7799-3:2006 [134]

Information security management systems. Guidelines for information security risk management

ISMS のリスクマネジメントサイクルの全ての観点から、BS ISO/IEC 27001:2005 の要求事項をサポートするためのガイダンスとなるものであり、リスク評価、リスクを扱うためのコントロールの導入、リスクの監視・レビュー、リスクコントロール体制の維持・改善が含まれる。リスクマネジメント活動の実施中のプログラムを通じて、組織のビジネスリスクに対する情報セキュリティを確保することにフォーカスしている。規模や性質によらず、すべての組織に適用することが可能であり、情報セキュリティ管理におけるリスクマネジメント活動に従事するビジネスマネージャーおよびスタッフによる利用を想定したものとなっている。2006 年 3 月 17 日に発行された。

2.3.2.2. MISRA-SA[135]

英国に本部を置く、自動車産業の業界団体 MISRA (The Motor Industry Software Reliability Association)が、MISRA 安全性解析(MISRA-SA)ガイドラインを策定している。これは、ISO 26262 [238] に適合した開発実務を実現するためのガイドラインとして位置付けられる [108]。ISO 26262 の第 6 部に記載されている“ソフトウェア開発プロセス”において、安全性の高いプログラムを作成するための C 言語ガイドラインとして MISRA-C があることが記載されている。

[134] http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030125022
[135] http://www.misra.org.uk/

2.4. ドイツ

2.4.1. 政府における取組み

2.4.1.1. ITS：IT Security Criteria[136]

ドイツの政府系情報セキュリティ機関である BSI(連邦情報セキュリティ室) [137] が、製品・システムの評価・認証を行う際に用いる基準である。米国の TCSEC を参考にして作成されたもので、ドイツにおける最初の国内基準である。本基準は、その後の欧州統一基準 ITSEC のベースとなった。

2.4.1.2. SAGA：Standards und Architekturen für eGovernment-Anwendungen [138]

KBSt(連邦政府調整助言課[139])により作成された、電子政府の相互運用のための、アプリケーションの規格・基準を規定する文書である。省庁における電子調達システムの標準規格としても用いられる。

2.4.1.3. IT-Grundschutz[140]

BSI が開発した、IT システムに関するリスクアセスメント・マネジメントの手法で、標準、脅威/セーフガードカタログ、ソフトウェア、認証制度の 4 つのツールによって構成される。BMI[141]や KBSt などの電子政府に関連する政府組織には IT-Grundschutz の遵守が求められている。

企業に対しても適用が推奨されている。

2.4.1.4. ドイツPL法[142]

(a) 名称

Produkthaftungsgesetz (略称 ProdHaftG)

和訳:ドイツ PL 法(1989 年法)

英語訳:Product Liability Act of 15 December 1989 [BGBl. I 2198], as amended[143]

(b) 経緯

1985 年 7 月 25 日に「1985 年 EC 指令」: Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products(国内法化期限:1988 年 7 月 30 日) が採択され、製造物の欠陥により発生する損害について、故意・過失がなくても、損害賠償責任を負うことを規定する無過失責任(liability without fault [144])の採用について、EC 内の統一的な製造物責任法制を実現することを目指した。

1989 年 12 月 15 日にドイツ PL 法が制定され、1990 年 1 月 1 日から施行された。2002 年 7 月に最終改正が行われている。なお、医薬品に関しては、無過失責任を定めた薬事法(Pharmaceutical Products

136 http://www.bsi.de/zertifiz/itkrit/itgruene.pdf
137 情報セキュリティサービスを提供するだけでなく、独自に IT セキュリティ分野の研究機能を持つ。
138 http://www.cio.bund.de/cae/servlet/contentblob/83732/publicationFile/5155/archiv_saga_1_1_download.pdf
139 連邦政府調整助言庁。IT に係わる標準化、オープンソースソフトウェア(OSS)戦略、電子行政サービスを担当。
140 http://www.bsi.de/gshb/intl/index.htm
141 連邦内務省。重要情報インフラ防護および電子行政サービス、渡航に関する書類、生体認証の管理を担当。
142 米国、英国などにおいても同様の法律が制定されているが、ドイツでは、ソフトウェアについても PL 法の適用対象となる製造物の範囲に含まれるとする解釈があるため、特にドイツの PL 法について述べる。
http://www.consumer.go.jp/kankeihourei/seizoubutsu/file/hokoku.pdf
143 http://www.utexas.edu/law/academics/centers/transnational/work_new/german/case.php?id=1397
144 損害の発生につき、故意・過失がなくても損害賠償責任を負うこと。過失責任主義。アメリカの厳格責任と同様。欠陥の存在と欠陥によって損害が生じたことが必要。製品から損害が生じた場合に常に責任を負う「絶対責任」とは異なる。

Act)が存在するため、適用除外(製造物責任法第 15 条)となった。

c) 特徴

ドイツ PL 法制定の規準となった EC 指令には以下の 3 つのオプションがある。

（1） 開発危険[145]の抗弁の有無

当時の技術水準によって当該欠陥を認識することができなかった場合は製造者を免責しうるものとしている(製造物責任法第 1 条第 2 項第 5 号)。

（2） 第 1 次農産物・狩猟物への適用

（3） 責任限度額の設定

人的損害の責任最高限度額を以下のように設定

同一の欠陥を持つ製品について複数の被害者がいる場合でも、上限額の総額を 8,500 万ユーロとする。

物的損害(個人私用のものに限る)については、500 ユーロまではつねに被害者の自己負担として免責され、請求も減額される。(製造物責任法第 11 条)

ドイツの判例では、伝統的に製造物責任を不法行為(民法)の過失責任原則によって処理してきた。しかし、1968 年の鶏ペスト事件連邦通常最高裁(BGH)判決以後、過失の証明責任を転換して製造者は無過失を立証しない限り、免責されないとするなど、不法行為法上の製造者責任について被害者の挙証責任[146] を軽減しているため、製造物責任法の意味合いはそれほど大きいものではないと言われている。つまり、製造者の行為について故意・過失が無かったことを立証しなければ、製造者が損害賠償責任を負う方向(無過失責任の方向)に修正された。

【参考】

ドイツ民法(BGB)の大原則として、被害者に挙証責任がある。ただし、契約法は、責任に関する挙証責任は転換されるものと明文化されている。また、不法行為法上の製造者責任の場合には、判例が安全義務違反および責任の要件について挙証責任の転換を認めている。(アウスライサー(期待可能なあらゆる措置を取ったにもかかわらず回避し得なかった欠陥)が存在する場合には、製造者は免責されるが、期待可能なあらゆる安全措置(開発事業部の従業員を監督すること等)を取っていたことを立証しなければならないため、事実上このような主張が認められることは稀である)

被害者は当該製品の瑕疵、用法に基づいた使用において発生した損害、瑕疵と損害の間の因果関係を立証する必要がある。判例において、ソフトウェアがウイルスに感染した場合に、ソフトウェアの機能に障害が発生する欠陥は、契約法上の「瑕疵」と認定されている。

(d) 製造物責任法に関する判例

判例は見当たらない。営業利用を目的とした物によって発生した損害が製造物責任法の対象となっていないことから、製造者の責任が一般的に、民法上の不法行為法に基づき判断されているからだと考えられる[147]。

---

145 事故を起こした製品が流通に置かれた時点(引渡し時)の科学・技術知識の水準では、当該製品の存在を認識できなかった場合に認められる製造業者側の抗弁。

146 裁判において証拠を示す責任。PL 法においては、一般消費者である被害者が証拠を示すことの負担が大きいことを考慮し、挙証責任を軽減することで、消費者の権利が強化されている。

147 ドイツ法律特許事務所の弁護士の見解。

(e) ソフトウェアへの適用可能性

製造物責任法第 2 条の「製品」に該当するかどうかで学説の対立がある。

＜最近の主たる学説＞

ソフトウェアに対して製造物責任法を適用しうるものとしている。ただし、製造物責任法 2 条は欠陥製品について「動産」でなくてはならないと規定している以上、学説は、ソフトウェアが何らかの媒体に保存されている[148]こと、また、サービスとしての職務的性質よりも具体的な物である製品としての性質が優先的であると評価されることを要求している。(このような定義は、欧州共同体委員会による 1989 年の意見書でも示されているようである[147]。)

以上のことから、いわゆる Standard software(下記【補足】参照)は、製造物責任法 2 条における「製品」に該当するという主張がなされている。

【補足】

ソフトウェアをその契約形態によって分類すると、Standard software と Individual software の 2 種類に分けられる。(表 2-5 参照)

表 2-5： 契約形態によるソフトウェアの分類

ソフトウェアの種別	定義	関連法
Standard software	完成品[149] として引き渡されるソフトウェア	製造物責任法
Individual software	個別の要求に応じて作成されたソフトウェア	契約法

なお、上記の分類とは関係なく、全てのソフトウェアに製造物責任法の適用を認めている学説もある。

また、プロバイダーがサーバーに保存した情報へのアクセスを可能にすることにより、情報を流通させることは、当該ソフトウェアと内容が同一のものを継続的な利用のために提供することを意味し、それは情報の有形化に足りうるものとして製造物責任法の対象になるという見方がある。もっとも、このような学説においても、当該情報の利用が一時的にしか可能にならない場合[150]には、製品の引き渡しというよりも職務の提供として見なされ、製造物責任法は適用しえないものとしている。

＜その他＞

「技術的作業道具および消費者製品に関する法律(Gesetz über technische Arbeitsmittel und Verbraucherprodukte)」

消費者に人的損害をもたらす危険性が存する場合において、製造者に対しリコール義務等の義務を課す、行政法的性質を有する法律。2004 年 1 月 6 日に施行。

ソフトウェアもこの法律の対象となりうるため、ソフトウェア製造者は、人の身体等に対する危険が存在し、製造者がこの法律が定める義務に違反した場合につき、損害賠償責任を問われることになる。

2.4.2. 民間・業界団体における取組み

2.4.2.1. BITKOM[151] (情報経済・通信・新メディア連盟)

148 ネットワークを介してその機能が提供されるのではなく、記録媒体によって機能が提供されること。
149 改変や追加を行うことなく利用する製品。
150 ASP/SaaS やクラウド形態により提供されるサービスが該当すると考えられる。
151 http://www.bitkom.org/en/Default.aspx

BITKOM は IT、通信、ニューメディア業界の業界団体であり、1,200 以上の会員企業、900 名の個人会員を抱えており、会員企業の売り上げはドイツの ICT 産業全体の売り上げの 90%以上を占める。

情報セキュリティの観点では、主に中小企業を対象として、企業における情報セキュリティ確保の仕方、情報セキュリティ規格導入のためのガイドラインなどについてレポートを発行している。

2.4.3. ガイドライン

2.4.3.1. 国家の全体計画

2.4.3.1.1. Bund-Online 2005 [152]

2000 年に公表された電子政府プログラムで、2005 年までに、市民、企業、行政を対象とする主要なサービス 385 項目をオンラインで提供するというもの。

2.4.3.1.2. DeutschlandOnline [153]

Bund-Online を引き継ぐ形で、政府の全階層(連邦政府機関、16 の連邦、300 以上の地方区、および 13,000 以上の地方自治体)が連携する電子政府の実現を目指している[154]。

2.4.3.1.3. eGovernment 2.0 [155]

欧州の情報化社会推進戦略である i2010 [156] にしたがって、2010 年までに ICT を活用したより便利な電子政府サービスを推進することを掲げた電子政府戦略。電子カードやセキュアな通信基盤による電子政府サービスにおける認証技術、通信における可用性など、情報セキュリティに重点が置かれている。

2.4.3.2. 政府組織向け

2.4.3.2.1. E-Government Manual[157]

電子政府の構築に関わる政府側の人間を対象とした、組織において標準的な情報セキュリティを実現するためのマニュアル。

ドイツ連邦政府の電子政府戦略である Bund-Online2005 をベースとしている。

2.4.3.3. 消費者／製造者向け

2.4.3.3.1. BSI IT Certificates Information for consumers[158]／manufacturers[159]

BSI が作成したセキュリティ認証についての解説文書で、欧州全体のセキュリティ基準である Information Technology Security Evaluation Criteria (ITSEC) [103] や、ISO/IEC 15408といった認証を満たした製品を利用することにより、ユーザにどのようなメリットがもたらされるかを、また、製造者に対しては、認証を取得することによる利点、認証取得に必要な基準及び認証取得手順について解説する文書である。

---

[152] http://www.en.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2001/BundOnline__2005__-__Implementation__plan__Id__22725__en,templateId=raw,property=publicationFile.pdf/BundOnline_2005_-_Implementation_plan_Id_22725_en.pdf

[153] http://www.deutschland-online.de/DOL_en_Internet/broker.jsp

[154] 2005 年以降に開始されたものと思われる。

[155] http://www.verwaltung-innovativ.de/cln_117/nn_684536/sid_95C96B4FDBCFAEC9401DD7A794C6B1BF/SharedDocs/Pressemitteilungen/1125281__english__version__egovernment__2__0.html?__nnn=true

[156] 欧州委員会(European Commission)が、EU 全域において、2005 年から 5 年間の計画で実施するプロジェクト。ブロードバンドの普及と活性化、デジタルデバイド(情報格差)解消等を課題とする。

[157] http://www.bsi.bund.de/english/topics/egov/3_en.htm

[158] http://www.bsi.bund.de/english/publications/fb/F03BSISiconsum.pdf

[159] http://www.bsi.bund.de/english/publications/fb/F03BSISimanufact.pdf

2.5. オーストラリア

2.5.1. 政府の取組み

2.5.1.1. AISEP(オーストラレーシア情報セキュリティ評価プログラム) [160]

AISEP(Australasian Information Security Evaluation Program) [161] は、オーストラリア政府およびニュージーランド政府が調達・利用するITシステムの情報セキュリティの評価認定に関する制度である。1994年にオーストラリア国防省のDSD(Defense Signals Directorate： 国防信号局) [162] によって運用が開始され、当時の名称はAustralian Information Security Evaluation Programであったが、1998年にオーストラリアとニュージーランドの評価認定制度が統合されたことに伴い名称が、Australasian Information Security Evaluation Programに変更された。なお、オーストラリア政府は、1999年にCCRAに加盟している。

評価基準としてはISO 15408とInformation Technology Security Evaluation Criteria (ITSEC)が用いられ、実際の評価は、評価実施機関として認定された民間評価機関にアウトソースされている。認定された製品は、「評価済み製品リスト(Evaluated Products List)」としてウェブサイト[163]で公開される。

AISEP の運営管理は、DSD の下位組織でオーストラリア政府の情報システム保護を担当する Information Security Group(ISG) [164] によって行われている。ISG は、新しい暗号製品の開発に関して、産業界との協力において重要な役割を果たしている[165]。また、ACA(Australasian Certification Authority： オーストラレーシア認証局)が AISEP の監督および実際の認証活動を行う。

2.5.1.2. オーストラリア政府機関のためのオープンソースソフトウェアガイド[166]

「オーストラリア政府機関のためのオープンソースソフトウェアガイド(A Guide to Open Source Software for Australian Government Agencies)」は、オーストラリア政府情報管理局(The Australian Government Information Management Office：AGIMO[167])が作成した、オープンソースソフトウェアの調達ガイドであり、政府がオープンソースソフトウェアを利用する際に考慮すべき事項に関する網羅的な分析と評価を行っている。結論として、オープンソースソフトウェアが提供する機能が、政府が求める機能にどの程度合っているか(適格性)ということと、同等の機能を提供する商用ソフトウェアの金額とを比較した上で、いずれのソフトウェアを選択するかを決めるべきであるとしている。

2.5.1.3. オーストラリア政府ICTセキュリティマニュアル (ACSI33) [168]

「オーストラリア政府 ICT セキュリティマニュアル(Australian Government Information and Communications Technology Security Manual：ACSI33)」は、オーストラリアの政府機関が所有する情報通信システムを保護するためのアドバイスと情報を提供するために、DSD が発行したマニュアルである。政府機関同士あるいは政府と民間サービスプロバイダ間において、情報交換・データ交換を安全に行う(情報通信をセキュアに行うための情報セキュリティ環境を実現する)ために準拠すべきセキュリティ標準が定義されている。本方針の構成および個別項目は次のとおりである。

- Part 1. 政府内の ICT セキュリティ

---

160 http://www.dsd.gov.au/infosec/evaluation_services/aisep_pages/aisep.html
161 Australasian：オーストラリア、ニュージーランドおよびそれらの周囲の島々からなる地域を指す。
162 http://www.dsd.gov.au/
163 http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html
164 http://www.isg.com.au/
165 http://www.dsd.gov.au/infosec/
166 http://www.finance.gov.au/publications/guide-to-open-source-software/docs/A_Guide_to_Open_Source_Software.pdf
167 http://www.finance.gov.au/agimo/index.html
168 http://www.dsd.gov.au/library/infosec/ism.html

オーストラリア政府 ICT セキュリティマニュアル、セキュリティとリスク管理

- Part 2. ICT セキュリティガバナンス
  ICT セキュリティの役割と責任、セキュリティ文書、ICT セキュリティの評価、セキュリティメンテナンス、セキュリティインシデント
- Part 3. ICT システムのセキュリティ確保
  物理的な安全、通信セキュリティ、システム利用のセキュリティ、製品セキュリティ、メディアセキュリティ、ソフトウェアのセキュリティ、アクセス制御セキュリティ、暗号セキュリティ、ネットワークセキュリティ、ゲートウエイセキュリティ、オフサイトにおける業務のセキュリティ

ACSI33 は、全てのオーストラリア政府機関の保護セキュリティ[169]指針のベースとなっており、各政府機関は、保有する情報システムのセキュリティを維持するために、ACSI 33 に準拠した適切な政策及び手順を策定することが義務付けられている[170]。また、州政府が情報セキュリティ政策を策定する際にも、ACSI 33 に準拠するよう全豪地方自治体協会(ALGA:Australian Local Government Association) [171] が勧告している[172]。

2.5.1.4. 保護セキュリティマニュアル2005 [173]

「保護セキュリティマニュアル 2005(Protective Security Manual 2005:PSM 2005)」は、オーストラリアの公的部門が保有する資源(Official resources) [174] を守るために、オーストラリア政府機関が遵守すべき保護セキュリティに関する方針、原則、標準及び手続に関する指針を定めたもので、2005 年に司法省が発行した。本指針の構成は以下の通りである。

- 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. 職員の安全
- Part E. 物理的な安全
- Part F. 競争入札及び契約のための安全保障の枠組み
- Part G. セキュリティ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

PSM2005 は、政府組織やその契約関係にある組織等を対象として、セキュリティを確保するための最低限の標準を定めたものであり、すべての政府組織に対して一貫したアプローチを提示している。また ACSI33 は、PMS2005 の方針や原則に従い、ICT セキュリティに関する標準をより具体的に示したものであり、各組織が保有する情報や情報システムの機密レベルに応じたセキュリティ対策の実装が行えるような内容となっている。

2.5.1.5. 電子政府戦略、応答性の高い政府:新たなサービスアジェンダ

「電子政府戦略、応答性の高い政府:新たなサービスアジェンダ(2006 e-Government Strategy, Responsive

---

169 政府作成の保護セキュリティ・マニュアル(PSM:Protective Security Manual)において用いられている用語。攻撃からの防御を目的としたセキュリティを指す。
170 司法省が発行した保護セキュリティマニュアル 2005(2.5.1.4 参照)によって、ACSI33 準拠の義務化が規定されている。
171 州政府等の地方政府の代表をメンバーとする協会で、国政に対する意見の提示や、地方政府の政策のガイドなどを行う。
172 http://www.alga.asn.au/about/
173 http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_ProtectiveSecurityManual(PSM2005)
174 政府の職員等の人的資源、インフラ等の資源、情報システムに蓄えられる情報資産などが含まれる。

Government：A New Service Agenda）[175] 」は、2002 年に発行された電子政府戦略“2002 e-Government Strategy, Better Service, Better Government”に続く電子政府戦略であり、2010 年までに、統合された応答性の高い政府を実現するというビジョンの基に策定されたものである。

新しい戦略では、技術を効果的に活用することにより、いかにしてオーストラリア政府が、効率的で、利用者中心の産業部門に変わるかが示されている。つまり、対象とするテクノロジーを絞り、戦略的な投資を行うことで、政府内の重複業務等の削減、省庁間の業務プロセスの共通化・改善が図られ、また、オンラインサービス、電子サービス、音声ベースのサービスが完全に政府のサービス提供基盤に組み入れられることにより、利用者が政府に対してどのような手段でアプローチした場合でも、一貫性のあるサービスが提供されるようになる。

本計画における活動は、以下の 4 つの戦略優先課題に基づいて行われる。

① 利用者ニーズの満足
② 連結されたサービスの提供[176]を可能とするメカニズムの確立
③ バリューフォーマネーの実現
④ 公的部門の能力強化

本戦略では、2006 年からの 5 年間に実施する活動が、初期フェーズ(2006 年～2008 年)と完成フェーズ(2008 年～2010 年)の 2 段階に分けてまとめられている。初期フェーズでは、電子政府サービスの省庁間連携を実現し、利用者が、どのウェブサイトから電子政府にアクセスしても目的とする省庁にコンタクトできるようにする。また、一つの省庁のウェブサイトで登録情報の変更を行った場合、関係する他の省庁のウェブサイトにおいても変更が反映されるような仕組みを実現する。

完成フェーズでは、電子政府サービスが広く利用可能となり、利用者は、政府サービスのコンタクト先の担当者を指定できるようになる等、パーソナライズされたサービスの利用が可能となる。また、非常に簡易なシングルサインオンによる政府サービスの利用が可能となる。

2.5.1.6. 情報セキュリティ(IS18) [177]

クイーンズランド州の政府機関が、情報セキュリティの構築、実装、メンテナンスを行う際に強制的に適用される要求事項(政府が保有する情報に対する不正なアクセスや使用、情報の偶発的な書き換え、情報の喪失、情報漏洩を防止するための明確な方針など)を提供するために作成された情報セキュリティ規格である。

2.5.1.7. ICTポリシーと標準(ビクトリア州政府)

ビクトリア州政府が規定した、「ICT ポリシーと標準 Information and Communication Technology Policies and Standards」[178]は、ビクトリア州政府の ICT に関するポリシーと標準であり、スマートカードガイドラインや政府サービスの継続に関するポリシーを規定している。

2.5.2. 民間・業界団体の取組み

民間・業界団体の情報セキュリティに対する取組みの事例を以下に示す。

---

175 http://www.finance.gov.au/publications/2006-e-government-strategy/index.html
176 各省庁(のウェブサイト)が連携することにより、利用者にワンストップで効率的なサービスを提供すること。
177 http://www.qgcio.qld.gov.au/qgcio/architectureandstandards/informationstandards/current/Pages/Information%20Security.aspx
178 http://www.egov.vic.gov.au/index.php?env=-categories:m408-1-1-8-s-0

2.5.2.1. Australian Information Security Association (AISA) [179]

Information Security Interest Group (ISIG) [180] の下で 1999 年に設立された機関で、情報セキュリティに関する普及啓発、情報セキュリティ産業の専門家の育成などを行っている。

情報セキュリティに関する資格認定制度である CISSP などに関するスタディ・グループのウェブフォーラムや CISSP のトレーニングコースを提供している。

メンバー企業には、以下のメリットがある。

- 産業界の人的ネットワークの構築
- セミナー、パネルなどの専門家育成活動への参加
- 情報セキュリティに関するポータルサイトへのアクセス

2.5.2.2. Australian Security Industry Association Ltd (ASIAL) [181]

オーストラリアのセキュリティ産業の業界団体であり、メンバーの支援、標準の促進、公益の保護をミッションとしている。

情報セキュリティについては、アクセス制御、重要インフラ保護、IT セキュリティ、リスク管理、バイオメトリクスなどを事業範囲としている。

[179] http://www.aisa.org.au/
[180] http://www.isig.org.au/
[181] http://www.asial.com.au/

2.6. 韓国

2.6.1. 政府の取組み

2.6.1.1. 韓国ITセキュリティ評価認証制度(KECS:Korea IT Security Evaluation and Certification Scheme) [182]

韓国の政府系情報セキュリティ機関である KISA(Korea information Security Agency) [183] 傘下の IT セキュリティ評価センター(KISEC:Korea IT Security Evaluation Center)は、独自の IT セキュリティ評価認証制度(KECS:Korea IT Security Evaluation and Certification Scheme)に基づいて、情報セキュリティ関連製品の評価・認証を行う。また、KISEC は、コンピュータセキュリティ標準や評価要件に関する支援サービスや、コモンクライテリア承認アレンジメントに基づく評価保証レベル EAL4 までの製品評価も実施している。

韓国は、2006 年 9 月に CCRA (CC Recognition Arrangement : コモンクライテリア承認アレンジメント)[33]に、認証国(CAP:Certificate Authorising Participant)として正式に加盟している。

2.6.1.2. 情報セキュリティ検査サービス(ISCS : Information Security Check Service) [184]

情報通信ネットワークに対する大規模な侵害の発生を防止することを目的として、主にインターネットサービスプロバイダー(ISP)やインターネットデータセンター(IDC)、民間企業を対象として、ISMS の技術的・管理的な対策基準に適合しているかどうかについての評価・認証を行う制度であり、2004 年 9 月より運用されている。

選定された事業者は、毎年、情報セキュリティコンサルティング事業者による安全診断を受けることが義務付けられている。書面による一次審査に続き、現地での実態調査があり、認証の証明書の発行は KISA が行う。ISCS における具体的な審査内容には、次の事項を含む 48 事項が含まれている[185]。

- 情報セキュリティ対応組織の構成と運営体制(5 事項)
- 情報インフラ資産の管理(2 事項)
- 情報通信インフラの保安維持(21 事項)
- 情報ネットワークの保安維持(3 事項)

2.6.1.3. 情報セキュリティ管理体制の認証制度(Information Security Management System Certification Scheme) [186]

情報セキュリティの確実な管理・運用を目的とした制度で、ISP や IDC などの事業者や民間企業を対象として、情報セキュリティの管理・運用に係る要件を満たしているかどうかという観点からの評価・認証が行われる。認証取得時に 3 年間有効な ISMS 認証証明書が交付される。強制的な認証制度ではない。

評価は、以下のような基準に基づいて、KISA により行われる。

- 情報セキュリティ管理プロセスに関する 14 の要件
  情報保護ポリシーの策定、ISMS の対象範囲の定義、リスク管理、実装、フォローアップ管理に関するプロセスなどに関する要件。
- 文書化に関する 3 つの要件
  文書自体の規定、文書の管理、記録の管理などに関する要件。

---

182 http://www.kisa.or.kr/kisae/kisec/jsp/kisec_6010.jsp
183 http://www.kisa.or.kr/maine.jsp
184 http://www.kisa.or.kr/kisae/iscs/jsp/iscs.jsp、http://www.waset.org/pwaset/v6/v6-4.pdf
185 http://e-public.nttdata.co.jp/f/repo/456_a0703/a0703.aspx
186 http://www.kisa.or.kr/kisae/isms/jsp/isms_06.jsp、http://www.kisa.or.kr/kisae/isms/jsp/isms_07.jsp

- リスクへの対応策に関する 120 の要件
  情報セキュリティポリシー、外部者に対するセキュリティ、情報資産の分類など 15 の分野にわたる要件。

2.6.1.4. サイバー安全予防活動

国家安全保障に対するサイバー攻撃から国家情報通信ネットワークを効率的に保護することを目的として、国家サイバーセキュリティに関する組織体系及び運営に対する事項を定めた『国家サイバーセキュリティ管理規定』(大統領訓令第 141 号)に基づき、国家サイバーセキュリティセンター(National Cyber Security Center : NCSC) [187] が実施している取り組みである。

NCSC は、各政府機関の情報化(情報通信ネットワークの新設・増設など)を推進する際に、ネットワークの監視や脆弱性修正プログラムの配布等を通じて、事前に安全性を確認する。また、サイバー攻撃に対する対応能力を培うため、民・官・軍を結集してサイバー演習を実施している。さらに、国及び公共機関が利用する情報セキュリティ製品の安全性を検証するため、セキュリティ適合性の検証制度を運営している。

2.6.1.5. サイバーセキュリティインシデントの事例分析集

国家サイバーセキュリティセンターは、クラッキング、ワーム・ウイルスなど、国内で発生したサイバーセキュリティインシデントについての状況と事例を総合的に分析した『サイバーセキュリティインシデントの事例分析集』を発行し、政府機関及び企業に配布している。

2.6.1.6. 電子証明書の発行及び利用基盤の管理

公的な電子証明書発行サービス全般における障害の発生防止や認証サービスの安全性強化を目的とした取り組みであり、インターネットバンキングサービスなどに用いられる公的な電子証明書の安全な発給・管理を行うために、最上位の電子証明書認証局として、国内の 6 つの公認認証局を管理する。KISA が推進する。

2.6.2. 民間・業界団体の取組み

2.6.2.1. KF-ISAC[188]

MOFE(Ministry of Finance & Economy:財政経済部)及び金融機関を対象とした ISAC で、金融分野の主要な重要情報インフラ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。MoFE の承認を受けて Koscom[189]社が運用を行っている[190]。
2002 年 12 月に運用が開始された。

---

187 公共セクタにおける情報セキュリティ政策の統括を目的として 2004 年 2 月に国家情報院(NIS)傘下の組織として設立。
188 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(2009 年 NISC)
http://www.nisc.go.jp/inquiry/pdf/renkei_model.pdf
189 証券市場のコンピュータ化を目的として、韓国財務省と証券取引所によって 1977 年に設立。 http://english.koscom.co.kr/
190 http://english.koscom.co.kr/intro/comp/outline/index.jsp

2.7. 中国

2.7.1. 政府の取組み

中国政府による情報セキュリティ政策は、以下の組織が中心となって推進されている。

- 国家情報化指導グループ
- 情報セキュリティ国家重点実験室
- 国家情報センター
- 公安部情報安全等級保護評価センター
- 国家コンピュータネットワーク応急処理技術調整センター

中国における製品・サービスに関する情報セキュリティの取り組みを以下にまとめる。

2.7.1.1. ITセキュリティー製品の強制認証制度

2008 年 1 月に公布された IT セキュリティ製品の強制認証制度(China Compulsony Certification: CCC) [191] は、外国企業が製造する IT 製品のセキュリティ機能の適切性・確実性を中国政府が審査し、審査に合格した製品を認証する制度である。不合格の場合、その製品を中国国内で販売することができず、現地生産も許されない[192]。外国の企業は、審査を受ける際に製品の設計情報やソースコードを開示しなければならない可能性があることから、日米欧の政府が反発している。

2008 年 1 月の公布時点では、審査対象として、ファイアウオール、IC カード、基本ソフト、データベース、ルータなど IT セキュリティ製品 13 品目がリストに掲載されていた[193]。

当初は、2009 年 5 月施行予定であったが、日米欧の政府や企業の強い反発により延期され、2010 年 5 月 1 日から実施する予定であることを発表している。

国際的に認知されている情報セキュリティ認証制度である ISO／IEC15408(コモンクライテリア ：CC)には 7 段階の評価保証レベル(Evaluation Assurance Level：EAL) [29] があり、CC においても製品の評価を受ける際には、製品の情報を開示することが求められるが、たとえば、最も条件が緩い EAL1～2 では各種 IT 製品の「マニュアル」や「機能仕様」など、必ずしも機密とはいえない情報の開示にとどまり、EAL3 で「詳細な設計仕様」、EAL4 で「実装ソースコード」の開示が求められる等、情報開示の度合いは認証レベルに応じたものとなっている。

なお、中国政府は、2009 年 3 月現在、CC 承認アレンジメント [33] に加盟していない。

本制度運営のため、国の認証許可業務を統括する国家認証認可監督管理委員会(CNCA)が新たに設立された。

2.7.1.2. WAPI (Wireless LAN Authentication and Privacy Infrastructure) (GB15629.11／1102)

WAPI は、ワイヤレス LAN に関する中国独自のセキュリティ規格である。2003 年 11 月 26 日に国家標準化委員会が「ワイヤレス LAN の強制的国家規格実施に関する公告」を発表し、2004 年 6 月 1 日以降、中国国内のすべてのワイヤレス LAN 製品を対象として WAPI 規格の採用を義務付けるとしていた。しかし、米国政府

---

191 中国の安全認証制度には、中国へ輸出される電気・電子製品の規制を目的とした「CCIB 認証」と、中国国内で販売される電気・電子製品の規制を目的とした「CCEE 認証」の 2 つの制度が存在していたが、2001 年 11 月の WTO 加盟に伴い従来の二重認証制度が統合され、中国強制認証(CCC)に統一された。第一次強制認証実施製品として 19 分類 132 品目が指定されている。この強制認証制度の認証を取得しない限り、海外の企業による中国への輸出、中国国内での製造・出荷・販売、その他営利目的の使用が禁止されることとなった。http://www.suzuden.co.jp/gijyutu/pdf/bell43/pdf43_07.pdf

192 http://www.yomiuri.co.jp/net/frompc/20081218nt0c.htm

193 http://jp.fujitsu.com/group/fri/report/china-research/topics/2009/no-112.html

および企業からの圧力により、中国政府は WAPI 規格の導入を無期限で延期している。

一方、財政部、国家発展改革委員会、情報産業部が共同で発表した「ワイヤレス LAN 製品の政府調達にかかる実施意見」は、国家機関、事業単位(政府系機関)、団体・組織が公的資金を用いて、ワイヤレス LAN 製品やワイヤレス LAN 機能を搭載したコンピュータなどの製品を購入する場合、WAPI に合致する製品を優先的に購入しなければならないとしている。

このようなことから、WAPI の適用に向けた動きが停止したわけではないと考えられる[194]。

2.7.1.3. ゴールデンカードプロジェクト

電子政府推進政策の一貫として、IC カードの普及を国家重要施策に位置付け、社会保障カードとして導入するというものである[195]。2008 年までの数年間は、年間の IC カード発行量は 1 億枚を超えるとともに、年成長率は 30ー40%にも達した。地方政府では、何枚の IC カードを配ったかという数値的な実績のみを重視する傾向があるが、他の都市でも使用可能となるよう地方保護主義を改めることが重要である。

中国の電子政府プロジェクトにおいて、IC カードは重要なツールとして認識されているが、複数の IC カードフォーマットが林立しており、IC カード相互間の相互運用性が確保されていないことが問題となっている。

[194] アジア情報化レポート 2007 中国 (CICC)
[195] http://e-public.nttdata.co.jp/f/repo/236_a0409/a0409.aspx

2.8. シンガポール

2.8.1. 政府の取組み

2.8.1.1. 標準ICT業務環境（SOE：Standard ICT Operating Environment）[196]

IT に係る政府調達の一括管理を行うことを目的として、パソコン環境とネットワーク環境の統一化を図るプログラムであり、IDA(Infocomm Development Authority of Singapore）[197] により推進される。

標準 ICT 業務環境の導入により、最新の ICT サービスの導入にかかる時間、コストや仕様が異なるシステムの互換性の問題などが軽減されると共に、脆弱性修正プログラムの適用プロセスを共通化することができるといったことにより、効率的にセキュリティの向上を図ることができる。

IDA は、政府職員 140000 席分の情報システムのプラットフォーム、セキュリティアプリケーションを共通化することを目指している[198]。IDA は、このプログラムにより年間の ICT 運用コストを 3 割削減できると試算している。

2006 年から 2008 年にかけて各省庁に導入され、2007 年から 2009 年にかけて、法定機関[199]や学校に導入される予定である[200]。

2.8.1.2. コモンクライテリア(ISO 15408) による認証

シンガポールは、2005 年 3 月に CCRA[33] に加盟しており、同国の ICT 関連製品がコモンクライテリア(ISO 15408)による認証を取得するケースが増加すれば、海外市場における競争力が向上するものと期待されている[201]。

2.8.1.3. 認証局のためのセキュリティガイドライン（Security Guidelines for Certification Authorities）[202]

民間事業者を対象とした、認証局運用に関するセキュリティ指針であり、CA 認証サービス、データ・システムの機密性、完全性、可用性を確保するため、認証局の運用・管理に関する統一的なセキュリティフレームワークおよびセキュリティ要件を規定している。

IDA により作成され、2003 年 9 月に運用が開始されている。

2.8.1.4. 電子取引法（Electronic Transactions Act 1998）[203]

電子商取引における本人認証と文書の改ざん防止のための法体系の構築を目的とした法律。

法律は、下記の実現を目指すものである。

1. 電子商取引をサポートするための商業規定の制定
2. PKI： 公開鍵基盤の提供
3. 公的セクタを対象として、電子アプリケーションとライセンスを活用できるようにする
4. 第 3 者が保有するコンテンツに対するネットワークサービスプロバイダの責任の明確化

---

196 http://www.ida.gov.sg/Programmes/20060419145341.aspx?getPagetype=34

197 競争力の高い情報通信産業を育成することをミッションとするシンガポール政府の法定機関であり、1999 年に国家コンピュータ局とシンガポール通信公社との統合により設立された。 http://www.ida.gov.sg/home/index.aspx

198 IDA Infocomm Security & Trust Division Deputy Director Clement Leong からのヒアリング情報。

199 法定機関：法律に基づき設立された政府関連機関で、その機能、業務範囲、権限なども法律で定められている。法定機関は、監督省庁の管下にあり、監督省庁を通して国会に責任を持つ。

200 出典：http://www.clair.or.jp/j/forum/compare/pdf/0607-4.pdf

201 出典：http://e-public.nttdata.co.jp/f/repo/449_a0702/a0702.aspx

202 http://www.ida.gov.sg/Policies%20and%20Regulation/20060425155704.aspx

203 http://www.ida.gov.sg/Policies%20and%20Regulation/20061023155715.aspx

2.8.1.5. 電子商取引(認証局)規則 (Electronic Transactions (Certifications Authority) Regulations 1999)[204]

シンガポール国内での電子署名認証局の運営については、認証局規制局(Controller of Certification Authorities(CCA)) [205] からライセンスの発行を受ける必要があることから、電子商取引規則は、電子署名認証局の運営に関わる申請手続きや審査基準等を明確化するものである[206]。

認証局規制局は、シンガポール国内での認証局運営について、電子取引法、電子取引規制、認証局のためのセキュリティガイドライン等に基づき、ライセンスの発行を行う。

1999 年 2 月に運用が開始された。

2.8.1.6. Internet Banking Technology Risks Management Guidelines[207]

インターネット・バンキング技術リスク管理ガイドライン(Internet Banking Technology Risks Management Guidelines)は、銀行システムに関するサイバー脅威や攻撃に対する防御に関するガイダンスである。2008 年 6 月に改訂されている。

金融機関や産業界が、顧客に対して、インターネットや他のコンピュータネットワークを介して提供されるオンライン金融サービスに関する便益とリスクについて積極的に啓発することを推奨している。リスク管理に関する高いレベルの標準による情報開示のプロセスを通じてオンライン金融システムに対する信頼性を高めることについて言及している。

本ガイドラインでは、リスク管理のフレームワーク、インターネット金融サービスの種類、セキュリティの原則と慣行、システム開発とテスト、リカバリーと事業継続、アウトソーシング管理などについてまとめている。

2.8.1.7. 情報通信セキュリティに関するベストプラクティス(Infocomm Security Best Practices)

サイバー空間のセキュリティに関するシンガポールの戦略(Singapore's Strategy in Securing the Cyberspace)において引用されたベストプラクティスで、情報システムを利用する組織が対象となる。

情報通信セキュリティマスタープラン 2(Infocomm Security Master Plan 2)では、国際的な連携を図るために本ベストプラクティスの普及を図るとしている。

2.8.1.8. ICTセキュリティ健全性スコアカード(Infocomm Security Health Scorecard)

ISMP(Information Security Master Plan)の中で掲げられた公共機関の情報セキュリティ対策の準備レベルを測定するための制度で、2005 年 2 月発表されたものである[208]。政府共通の検討課題が抽出し、弱点を取り除くためにが払拭されるようにし、公的部門のセキュリティに関する俯瞰的な状況を確認することができるようにすることを政府横断的に適用可能なスコアカードの策定に結びつけることを目指している[209]。

2.8.2. 民間企業・業界団体の取組み

2.8.2.1. 事業継続/災害復旧サービスプロバイダのためのシンガポール標準

事業継続/災害復旧サービスプロバイダのためのシンガポール標準(Singapore Standard for Business

---

[204] http://www.ida.gov.sg/Policies%20and%20Regulation/20060425154627.aspx
[205] http://www.ida.gov.sg/Policies%20and%20Regulation/20060508170238.aspx
[206] 出典:アジア情報化レポート 2007 シンガポール, CICC
[207] http://www.mas.gov.sg/legislation_guidelines/banks/guidelines/Internet_Banking_Technology_Risk_Management_Guidelines.html
[208] 出典:http://www.ida.gov.sg/Programmes/20060925100740.aspx?getPagetype=36
[209] 出典:http://www.ida.gov.sg/News%20and%20Events/20050717164621.aspx?getPagetype=21

Continuity/Disaster Recovery(BC/DR) Service Provider)[210] は、BC/DR サービスを提供する企業のための基準を定めたシンガポール規格。世界で初めての BC/DR サービス事業者の国家規格である。この規格に適合する企業の認証を、PSB の子会社である PSB Certificate が実施しており、Equinix、HP、IBM、NCS、SCS、SingTel EXPAN 及び StarHub の 7 社が認証を取得している。2005 年 4 月にウィーンで開催された ISO/IEC JTC1 /SC27 において、ICT 災害復旧サービス(Information and communications technology disaster recovery services)のガイドラインに関する国際規格の新規業務計画(NWIP)の提案を行った。2004 年 8 月策定。

2.8.2.2. TrustSg マークプログラム

インターネットを経由する電子商取引を促進するため、公正にセキュリティが保護されているインターネットサイトには「TrustSg」マーク[211]の貼り付けを認め、利用者が安心して電子商取引を行うことができるようにする制度である。国家信用カウンシル（National Trust Council[212]）が規定したオンライン事業者が守るべき情報システムに関する規範を審査基準とする[213]。2001 年 3 月に運用が開始されている。

2.8.2.3. PSB情報セキュリティマネジメントシステム認証スキーム

PSB 情報セキュリティマネジメントシステム認証スキーム(PSB Information Security Management System Certification Scheme)は、製品・サービスのセキュリティのを向上させることを目的として、情報セキュリティマネジメントシステムの認証取得を支援する制度である。TÜV SÜD PSB Certification Pte. Ltd.により実施される認定制度である。このスキームの下で、ISO27001 や BS7799 などの認証を取得している企業がある[214],[215]。2006 年 3 月に、SPRING[216]傘下の PSB Certification がドイツの IT サービスプロバイダである TÜV SÜD 社に買収されている。2001 年に運用が開始されている。

2.8.2.4. データ保護規則モデル(Model Data Protection Code for the Private Sector)

個人情報を電子的データの形式で保有する企業を対象として、電子データの保護に係る規約を規定したものである。民間企業における個人情報保護の推進を目的としている[217]。2003 年 6 月に NIAC[218]が策定した。

データ保護に関する規約には、以下のようなものが挙げられている[219]:

- 個人データを組織の管理下に置き、責任者を任命すること。
- 個人データ収集の目的を特定すること。
- 個人データの収集、利用、開示に関する知識と合意を形成すること。
- 個人データの収集は目的の範囲に限定すること。

---

[210] 出典：http://www.continuitycentral.com/news01712.htm
[211] 出典：http://www.trustsg.com/trustsg/c/portal/layout?p_l_id=1
[212] NTC：http://www.trustsg.com/radiantrust/tsg/rel1_0/html/TrustCouncil.html
[213] 出典：http://www.trustsg.com/radiantrust/tsg/rel1_0/html/whatistrust.html
[214] 出典：www.bellua.com/bcs/asia08.materials/bcs08-ng.ppt、
[215] 出典：http://www.isms.jipdec.jp/doc/ismsintre.PDF
[216] SPRING（シンガポール生産性・標準化庁）：生産性向上のための標準を作成する機関である。
[217] 出典：http://www.ida.gov.sg/News%20and%20Events/20061120095852.aspx?getPagetype=20
[218] NIAC(National Internet Advisory Committee:国家インターネット諮問委員会)：シンガポールのインターネット利用等に関する助言を行う国家委員会である。
[219] 出典：http://www.agc.gov.sg/publications/docs/Model_Data_Protection_Code_Feb_2002.pdf

2.9. マレーシア

政府機関および民間企業における ICT 製品やサービスを対象とした情報セキュリティに関する評価認証制度や認証基準についての政策は、以下の組織を中心に進められている。

- CyberSecurity Malaysia[220]
- MAMPU (MODERNISATION AND MANAGEMENT PLANNNING UNIT)[221]
- Government Computer Emergency Response Team(GCERT)[222]

2.9.1. 政府の取組み

2.9.1.1. CyberSecurity Malaysia

CyberSecurity Malaysia には、情報セキュリティ評価や情報セキュリティ基準準拠サービスを提供するセキュリティ保証部門がある。セキュリティ保証部門では、情報セキュリティ対策に対する専門的な助言や、ISO15408/Common Criteria 及び主要な国際標準に基づく ICT 製品・システムのセキュリティ評価を実施している[223]。

2.9.1.2. 公的部門情報通信技術セキュリティ管理ハンドブック(MyMIS)

電子政府は、MAMPU（現代化・管理計画ユニット: MODERNISATION AND MANAGEMENT PLANNNING UNIT)によって推進されてきており、電子政府システムの調達からシステムのライフサイクルにおける情報セキュリティの確保についても MAMPU が担当している。

公的部門の情報通信技術セキュリティに関する管理ハンドブック(Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS)[224])が公的セクタにおける ICT 利用におけるセキュリティ管理について広く参照できるハンドブックである。

MyMIS の構成は以下のとおりである。

公的部門情報通信技術セキュリティ管理ハンドブック(MyMIS)の構成

1. はじめに
2. 管理セーフガード
    - 公的部門 ICT セキュリティポリシー
    - ICT セキュリティのシステムライフサイクルへの導入
    - ICT セキュリティ・アシュアランス
3. 基本オペレーション
    - 情報分類
    - ICT セキュリティオフィサー
    - 電子施設
    - 電子メール
4. 技術オペレーション
    - 法的事項

[220] http://www.cybersecurity.org.my/en/
[221] http://www.mampu.gov.my/
[222] http://www.mampu.gov.my/perkhidmatan/gcert
[223] http://www.cybersecurity.my/en/services/security_assurance/about/main/detail/230/index.html
[224] http://www.mampu.gov.my/mampu/pdf/MyMIS/MyMIS.htm

第 2 章『MANAGEMENT SAFEGUARDS』には、プログラムマネジメントの重要性と組織における ICT セキュリティ管理についての記述がある。また、『2.1 公的部門 ICT セキュリティポリシー』では、中央政府、各省庁、各部門におけるポリシーについて、『2.2 公的部門 ICT セキュリティプログラム管理』では、中央政府における ICT セキュリティプログラム管理と運用レベルのセキュリティプログラム管理についての記述がある。『2.4 ICT セキュリティのシステムライフサイクルへの導入』では、公的セクタにおける ICT 活用は必須であるため、公的セクタにおける ICT セキュリティ計画を最初に考慮することが重要であるとの指摘がされている。『2.5 ICT セキュリティ・アシュアランス』では、セキュリティ保証を必要とする人およびどのタイプのセキュリティ保証が必要なのかという観点から、設計と実装における保証と運用における保証についての記述がある。『2.5.1 設計と実装における保証』では、テストと認証、信頼性の高いアーキテクチャ、安全な利用法、評価とレビューなどについてまとめられている。

また、第 3 章の『基本オペレーション』の『3.2.4 ICT セキュリティオフィサー』において、ICT オフィサーの役割と責任がまとめられている。

2.9.1.3. PRISMA[225]

重要インフラの情報セキュリティの確保に対しては公的分野のための ICT セキュリティ担当部門がある。PRISMA と呼ばれる政府 ICT セキュリティ指令センターがあり、ネットワークシステムと公的 ICT をサイバー脅威から監視するためのプロジェクトである。以下の目的のもと設立されている。

- ネットワークシステムと ICT 資産モニタのための定期的脆弱性スキャンニングシステムの提供
- セキュリティ侵害インシデントの検知とサイバーセキュリティ脅威の阻止
- サイバー攻撃や脅威の予測や警告

2.9.1.4. GCERT

MAMPU の Government Computer Emergency Response Team(GCERT)とは、公的セクタの ICT インフラにおけるインシデントを組織横断的に対応するものであり、各省庁には Agency CERT が置かれている[226]。

[225] 出典：http://www.mampu.gov.my/perkhidmatan/prisma
[226] 出典：http://gcert.mampu.gov.my/

2.10. 国際機関

ICT 製品・サービスの情報セキュリティに関連する、国際機関における標準化等の動向についてまとめる。

2.10.1. ICT 分野

2.10.1.1. コモンクライテリア(CC)承認アレンジメント (CCRA) [227]

CC 承認アレンジメントは、1998 年 10 月に発効した CC に基づくセキュリティ評価・認証の相互承認に関する協定で、CC に基づく認証制度を持つ国(認証国)で評価・認証された製品を他の CCRA 加盟国においても CC 認証製品として扱うことができることを規定したものである。CCRA 加盟国のうち、CC に基づく認証制度をもつ国(CCRA 認証国(Certificate authorizing participants (CAP))については、それぞれ認証製品リストを公開している。2000 年 5 月に CCRA の規定が改定され、CC に基づく認証制度を持たない国であっても、他の加盟国で認証されている製品をその国において認証済みの製品として受け入れることを許容するのであれば、CCRA に加盟できるようになった。そのような国は、受入国(CCP:Certificate consuming participants)と呼ばれる。

CC 承認アレンジメント加盟国には、フランス、ドイツ、イギリス、オランダ、スペイン、スウェーデン、米国、オーストラリアなどがあり、日本は、2003 年 10 月に CCRA に認証国として加盟した。シンガポール、マレーシアは CCRA 受入国である。中国は、2009 年 3 月時点で、CCRA に加盟していない。

2.10.2. 鉄道分野

2.10.2.1. IEC 62278 [228] (鉄道システムの信頼性、可用性、保守性、安全性に関する規格)

本標準の正式名称は、『Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)』であり、リスク解析に基づいて、鉄道システムのライフサイクルにおける信頼性、可用性、保守性、安全性を確保するためのプロセスおよび実施するべき内容を規定している。ただし、日本とヨーロッパでは鉄道システムのが異なっていることや、日本の安全性基準が海外と比較して厳格であること、安全性の価値観が異なるといった事情により、日本は規格化に反対したという経緯がある [97]。

2.10.2.2. IEC 62279 [229] (鉄道用ソフトウェア)

本標準の正式名称は、『Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems』であり、鉄道の制御・保護ソフトウェアに関する規格である。各ライフサイクルにおいて安全性確保のために要求される SIL[107] が満たされていることを明らかにするためのプロセスを規定している。例えば、安全性が確保されていない要素を排除するための C 言語の使用禁止や、SIL4 のシステムに C 言語を使う際の、「ルーチン内に埋め込んだプログラムのドキュメント化」、「セキュアコーディングに関する教育の実施」を規定している [97]。

IEC 62279 のベースとなった IEC 61508[106] では、ソフトウェア開発(詳細設計)において採用すべき技法(図 2-7 参照)やプログラミングに使用すべき、あるいは使用すべきでない言語(24 種類)などが定義されており、合計で 100 ほどの技法がベスト・プラクティスとして規定されている。図 2-7 の 1c では、形式的手法を使用することを規定している。IEC61508 の中で、形式手法の言語として、OBJ, VDM, Z, HOL などを推奨している。

---

227 http://www.commoncriteriaportal.org/theccra.html

228 http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=english&wwwprog=pro-det.p&progdb=db1&He=IEC&Pu=62278&Pa=&Se=&Am=&Fr=&TR=&Ed=1#Ass

229 http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=english&wwwprog=pro-det.p&progdb=db1&He=IEC&Pu=62279&Pa=&Se=&Am=&Fr=&TR=&Ed=1

	技術／手法	SIL 1	SIL 2	SIL 3	SIL 4
1a	構造化手法	HR	HR	HR	HR
1b	半形式的手法	R	HR	HR	HR
1c	形式的手法	–	R	R	HR
2	コンピュータ支援による設計ツール	R	R	HR	HR
3	防衛プログラミング	–	R	HR	HR
4	モジュラー・アプローチ	HR	HR	HR	HR
5	設計及びコーディング規約	R	HR	HR	HR
6	構造化プログラミング	HR	HR	HR	HR
7	信頼ができて検証された モジュールなどの使用	R	HR	HR	HR

図 2-7:ソフトウェアの詳細設計において用いるべき技法

(R: Recommended, HR:Highly Recommended)(出典:IEC 61508)

2.10.2.3. IEC 62280-1 [230] / IEC 62280-2 [230] (鉄道用通信規格)

本標準の正式名称は、62280-1 :『Railway applications - Communication, signaling and processing systems - Part 1: Safety-related communication in closed transmission systems』および 62280-2 : 『Railway applications - Communication, signaling and processing systems - Part 2: Safety-related communication in open transmission systems』であり、物理的に独立した専用の有線回線と、物理的に独立していない無線回線やインターネットなどの回線を対象として、データ伝送の安全性に関する技術的な要件を規定している。例えば、鉄道が利用する WAN は、クラス 4(伝送システムの性質は未知、信頼できるネットワークのみを使用[231])であり、「なりすまし」以外の全ての脅威を考慮しなければならない。

2.10.3. 原子力分野

2.10.3.1. IEC 61513 [232] (原子力発電所 - ハードウェア設計要求)

本標準の正式名称は、『Nuclear power plants - Instrumentation and control important to safety-Hardware design requirements for computer-based systems』であり、原子力発電所の安全性確保のために重要な役割を果たす計装制御設備(instrumentation and control systems equipment : I&C システム)に関する一般的要件[233]に関する基準を定めたもので、IEC 61508[106]における基本的安全基準に類似した表示書式、全般的な安全性ライフサイクルフレーム、システムライフサイクルフレーム、IEC 61508 パート 1、2、4 を核応用分野に採用している。

2.10.3.2. IEC 60880 [234] (原子力発電所で使用されるコンピュータシステムのソフトウェア : カテゴリA)

---

230 http://www.iec.ch/online_news/justpub/jp_2002/jp2002.htm
231 平尾ら「鉄道信号の安全性技術規格の動向」
232 http://www.iec.ch/zone/fsafety/61513.htm
233 機能安全に関する国際標準 IEC 61508 の第1部に相当する。これ以外に、第3部にソフトウェアの信頼性などソフトウェアに関する要求事項が示されている。
234 http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=cat-det.p&progdb=db1&wartnum=036058

本標準の正式名称は、『Nuclear power plants -Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category』であり、原子力発電所におけるコンピュータを用いた計装制御設備(I&C システム)で使用されるソフトウェアのうちカテゴリ A に分類されるソフトウェア(高信頼性ソフトウェア)の要件について、ソフトウェア生成と要件、仕様、設計、実装、検査、検証、運用を含むドキュメンテーションを開発ステージごとに定義している。

2.10.3.3. IEC 62138 (原子力発電所で使用されるコンピュータシステムのソフトウェア ： カテゴリB及びC) [235]

本標準の正式名称は、『Nuclear power plants - Instrumentation and control important for safety - Software aspects for computer-based systems performing category B or C functions』であり、原子力発電所向けソフトウェアのうち、カテゴリ B 及び C 機能に分類されるソフトウェアを対象としたものである。具体的には、コントロールルーム、自動制御、サービスシステムのソフトウェアのヒューマンマシンインタフェースを提供するソフトウェアを対象とする規格で、コンピュータ化されたコントロールルームと I&C システムを体系的に扱うための標準である。将来的には、コンピュータ化されたコントロールルームのハードウェア及びソフトウェアの国家規格やガイドラインを策定することにより、単なる信頼性の改善だけではなく、ライセンス供与による公に対する説明責任の改善を目的としている。日本では耐震設計要件の追加が検討されている。

2.10.3.4. 原子力発電プラントにおける高い安全性が要求されるソフトウェアのライセンシング基準

EC と WENRA(Western European Nuclear Regulators' Association)による計装制御に関する規制と安全性に関する WG の検討内容をまとめた European Commission Nuclear Safety and the Environment 『Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorized technical support organizations (Revision 2007) 』[236]は、原子力発電プラントの安全を確保するための設計と高い安全性が要求されるソフトウェア(safety critical software)の運用におけるライセンス供与問題に関する共通な技術的立場を解説している。2000 年 5 月に発行された EC コンセンサス文書である共通の立場と勧告事項の改訂版であり、『Common position of nuclear regulators for the licensing of safety critical software for nuclear reactors (EUR 19265 EN.2000)[237]』に記載されている"共通の立場と推奨されるプラクティス"は、このレポートに含まれる。

内容は以下のようになっている。(下線を記してある項目は情報セキュリティに関するものである)

Part 1: Generic Licensing Issues
1.1 Safety Demonstration
1.2 Safety Categories, Classes and Graded Requirements for Software
1.3 Reference Standards
1.4 Use and Validation of Pre-existing Software (PSW)
1.5 Tools
1.6 Organisational Requirements
1.7 Software Quality Assurance Programme and Plan
1.8 Security

[235] http://www.iec.ch/news_centre/release/nr2006/nr1006.htm
[236] http://www.stuk.fi/ydinturvallisuus/lahialueyhteistyo/en_GB/wenra/_files/12222632510024502/default/PART_1_and_2_Version_18.pdf
[237] http://www.info.ucl.ac.be/Bienvenue/PagesPersonnelles/courtois/Courtois/eur19265.pdf

1.9 Formal methods
1.10 Independent Assessment
1.11 Graded Requirements for New and Pre-existing Software (PSW) of Safety Related Systems
1.12 Software Design Diversity
1.13 Software Reliability
1.14 Use of Operating Experience

Part 2: Life Cycle Phase Licensing Issues
2.1 Computer Based System Requirements
2.2 Computer System Design
2.3 Software Design and Structure
2.4 Coding and Programming Directives
2.5 Verification
2.6 Validation & Commissioning
2.7 Change Control and Configuration Management
2.8 Operational requirements

「1.8 セキュリティ」では、IT セキュリティの目的、定義、課題をまとめている。また、"共通の立場(Common Position)"として、原子力発電所の建設をライセンス化することなどを挙げている。

「1.13 ソフトウェア信頼性」では、ソフトウェアの信頼性向上は、製品の検査だけでは達成できず、生産工程における品質管理が重要であることや、品質管理に関する課題がまとめられている。

2.10.4. 自動車関連分野

2.10.4.1. ISO/CD 26262 [238] (Road vehicles – Functional safety : 自動車を対象とする機能安全規格)

自動車に搭載される電子製品(主として組込みソフトウェア)が仕様通りに動作することを認定する際に用いられる機能安全規格である。IEC 61508 をベースとして作成された規格であり、ドイツ、フランスの主導により標準化が進められている。現在、Committee Draft の状態である。

システムの特性に応じて、ソフトウェアの安全度水準を規定するもので、求められる安全度水準 SIL[107] に応じて、使用が推奨される技術、ソフトウェア開発手法、テスト環境等が規定されている。自動車特有の条件が考慮されており、安全度水準としては ASIL(Automotive Safety Integrity Level)[239]が用いられる。

[238] http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_ics_browse.htm?ICS1=43&ICS2=040&ICS3=10&development=on 項目ごとに Part1 から Part10 に分かれている。

[239] ISO/CD 26262 に規定されている安全度水準で、A から D までの 4 段階に分けられている。それぞれの段階ごとに、ソフトウェアの安全性、設計、システム分析、生産管理などについての基準を定めている。

3. 今後の方向性と提言

3.1. 政府および民間における取り組みのまとめ

ICT 製品・サービスの情報セキュリティ確保に向けた最近の取り組みとして、以下のようなものがある。

- 製品や情報システムの政府調達基準の活用
  政府機関が調達する ICT 製品やシステムは、その金額が非常に大きいため、製品・システムを開発・販売するシステム構築事業者やベンダーに対する影響力も非常に大きい。したがって、政府が、製品・システムの調達基準に情報セキュリティに関する基準を規定することにより、システム構築事業者やベンダーの情報セキュリティ対策に関する取り組みが促進され、結果的に製品・サービスの情報セキュリティが向上することが期待される。
- 業界における開発方法論・ノウハウの共有化
  SAFECode を初めとする業界のベストプラクティスなど、各企業が持つノウハウを業界全体で整理し共有することで、相互にメリットを享受する。
- 重要インフラ事業等に対する政府規制・自主ガイドライン
  米国を中心に重要インフラ事業に対する政府による規制や業界の自主ガイドラインにより、重要インフラのセキュリティを確保するための取組みが行われている。

製品・サービスの情報セキュリティは、その推進主体によって、政府機関と業界団体に、また、その対象となる分野や目的によって、主に以下の 4 つのカテゴリに分類することができる。

- 開発技術
- プロセス管理
- 評価・認証・基準
- 普及啓発

これらの分類に基づき、製品・サービスの情報セキュリティに関する代表的な取組みを整理すると、図 3-1 のようになる。

政府による取組みは、IT 製品の情報セキュリティに関する評価・認証が主であり、国際標準や各国が独自に定めた基準をベースとした評価・認証が主流となっている(図 3-1 の右上の円で囲まれた領域)。一方、民間企業による取組みは、セキュアな製品やサービスを開発するための技術や運用プロセス管理における情報セキュリティに軸足が置かれており、業界全体で取り組みを推進するためのベストプラクティスや自主ガイドラインが作成されている(図 3-1 の左下の円で囲まれた領域)。特に米国においては、一般的に政府による規制や法律の策定を回避するために[240]、業界団体等が自主的に取り組みを推進する傾向が強いが、今回の調査でも米国においては、他の国と比較して民間部門における取り組み事例が多いことが明らかとなった。

[240] 規制や法律を遵守するために要するコストよりも自主的な対策を行うのに要するコストの方が低いこと、また、法律や規制によってビジネスを展開する上での自由度やスピードが阻害される懸念があることが理由として考えられる。

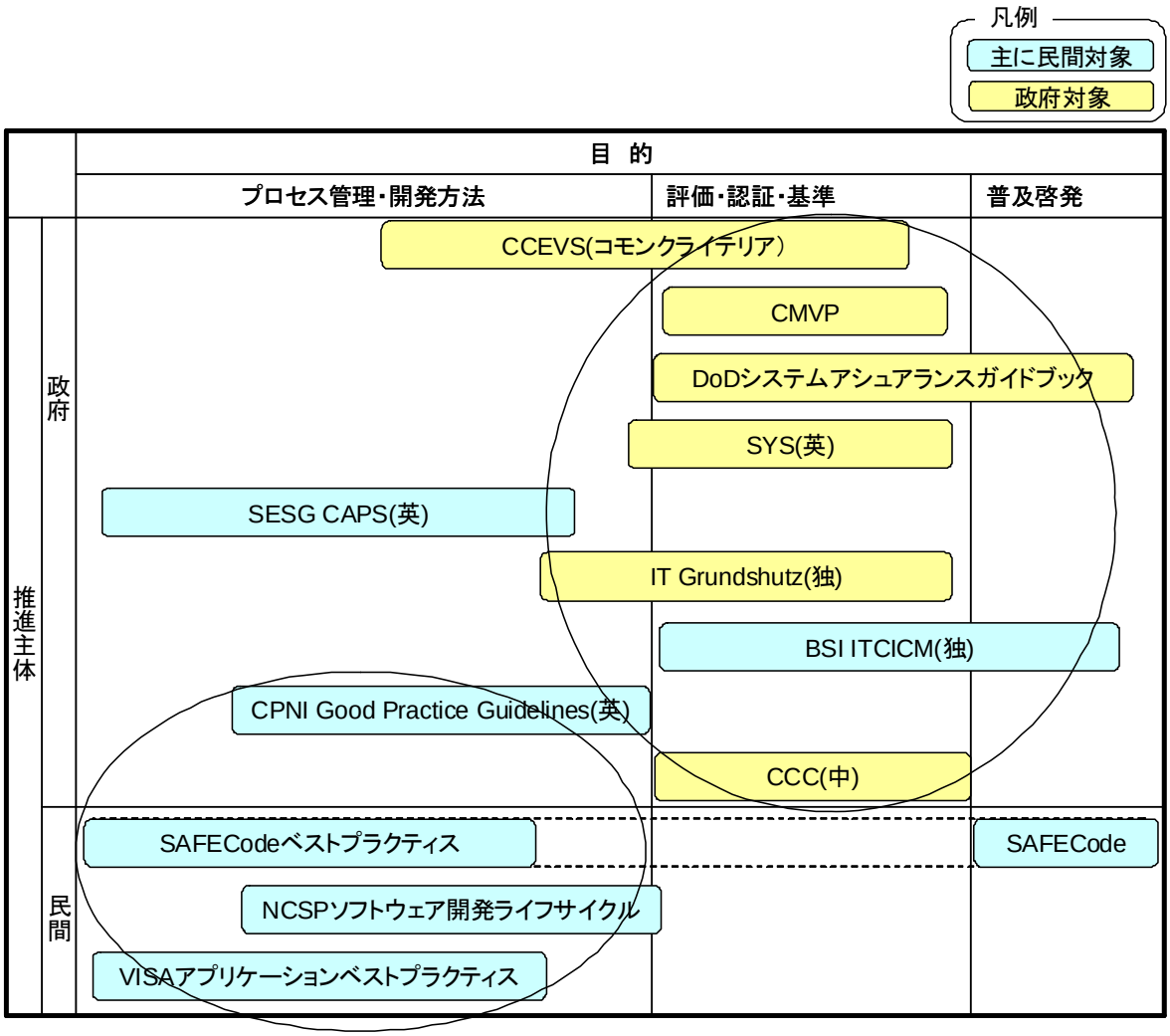

図 3-1:製品・サービスの情報セキュリティに関する主な取組み

3.2. 日本の政策に関する提言

各国におけるICT製品・サービスを対象とした情報セキュリティに対する取組み状況を踏まえ、我が国の情報セキュリティに関する政策の方向性についての提言をまとめる。

3.2.1. 日本型ソフトウェア開発方法論の国際標準化

近年、コモンクライテリア(ISO/IEC 15408)や電子機器の機能安全(IEC 61508)、自動車の機能安全[241]などの情報セキュリティに関する評価・認証に係わる国際標準や、鉄道システム[242]、航空機システム[243]、原子力[244]などの重要インフラ分野において使用される電子機器やソフトウェアの信頼性の評価・認証に関する国際標準において、欧米諸国による激しい主導権争いが繰り広げられている[245]。このような競争の背景には、自国の技術を国際標準とすることにより、グローバルな産業競争において優位性(自国の企業がビジネスを有利に進めることができる等)を確保することができるという事情がある。また、WTO 政府調達協定では、国際標準のような中立的な基準を政府調達基準に採用することを前提としているため[246]、政府調達政策における影響力においても国際標準はプレゼンスを増している。

国際標準となった評価・認証基準においては、研究や実用化において欧米が先行しているフォーマルメソッド(形式手法) [247] の適用[248]が規定されており、フォーマルメソッドの分野において欧米企業に遅れをとっている日本企業は、海外へ製品を輸出する場合や WTO 協定が適用される政府調達において、不利な状況に立たされることが懸念されている[249, 250]。

今後さらにグローバル化が進む経済活動において競争力の維持・向上を図るためには、他国主導によって策定された国際標準によって日本企業の競争力が阻害されることがないよう、また、日本企業がこれまでに培ってきた高い品質基準が、グローバルなビジネスにおいてそのまま活用できるよう、国際標準に対する取り組みを推進することが極めて重要である。日本の企業は、情報家電の組込みシステムやテレマティークス[251]、鉄道システムなどの分野において、独自の製造ノウハウや品質管理手法を構築し、高品質の製品を生み出してきた実績がある[252]。日本のソフトウェア産業において実証されている高い信頼性を要件とする基準を国際標準化するためには、客観的で透明性の高い評価基準を示すことが求められる。特に、日本が技術優位性を持つ組込みシステム等における情報セキュリティの国際標準化が候補と考えられる。国際標準化の推進においては、日本政府および企業の経験および国際的な合意形成の能力は十分とは言えない。日本政府には、国際標準化活動の主体となる企業および国立研究所などに対して、関連技術情報の提供や戦略構築支援を行うための施策が期待される。

---

241 http://keng.ke.ohost.de/ISOWD26262(AutomotiveE.ESicherheitsengineering).html
242 http://webstore.iec.ch/webstore/webstore.nsf/artnum/029178
243 http://www.stsc.hill.af.mil/crosstalk/1998/10/schad.asp
244 http://webstore.iec.ch/webstore/webstore.nsf/artnum/026810
245 IEC 61508 は、イギリスを中心とする欧州諸国により標準化が進められた。現在、IEC 61508 に基づく認証を実施している機関は、イギリスの Sira とドイツの TUV のみである(2007 年)。ISO/IEC 15408 は、1970 年代に米国において標準化が進められた TCSEC、1990 年代に欧州で開発された ITSEC をベースとする標準である。
246 http://www.wto.org/english/tratop_e/gproc_e/gp_gpa_e.htm
247 ソフトウェアや情報システムの仕様を厳密に定義された形式言語により記述することにより、ソフトウェアや情報システムの要求仕様や機能仕様を正しく満たしているかどうかを論理的かつ網羅的に検証し、それらの安全性(仕様通りに動作すること)を保証する技術。フォーマルメソッドを用いることにより、従来のテストケースに基づく検査では検証が困難な動作タイミングや並列処理等に係る安全性を満たすかどうかを検証することができる。
248 コモンクライテリア(ISO/IEC 15408)における評価保証レベル EAL6,7 や、機能安全(IEC 16508)における要求水準 SIL2,3,4 において、フォーマルメソッドの適用が規定されている。
249 TOPPERS プロジェクト 名古屋大学 高田広章 http://www.kumikomi.net/article/report/2006/11topper/01.html
250 標準化戦略 日本工業標準調査会 標準部会 (平成 13 年 8 月 31 日)
251 テレコミュニケーション(Telecommunication： 通信)とインフォマティクス(Informatics： 情報工学)から作られた造語。で、自動車などの移動体を対象として、携帯電話などの移動体通信システムを利用してサービスを提供する機能のこと。
252 Software Development Worldwide：The State of the Practice, Michael Cusumano, IEEE Software 2003

また、国際標準として認められるためには、日本の提案に対する賛同国・賛同組織を増やすことが重要である。ASEAN 諸国や中東、アフリカ等の国々は、提案されている手法・スキームが自国のメリットになるかどうかという観点で判断を行う傾向が高く、これらの国々からの賛同を得られるかどうかによって国際標準となるのかの帰趨が決する場合がある。従って、日本企業の技術や手法、ノウハウを国際標準にしようとする場合、これらの国々に対する日頃からの国際協力・援助を通じて、良好な関係を構築しておくことにより、日本の提案に対する潜在的な賛同国を増やしておくことが有効であると考えられる[253]。

3.2.2. 高信頼ソフトウェアに係わる人材の育成

情報セキュリティや高信頼ソフトウェアに関する国際標準において、フォーマルメソッドの使用に関する規定が取り入れられる動きが進展している。フォーマルメソッドは、欧米では、早くから研究が進んでいる分野であり、現在では、実際の設計・開発への適用が進んでいる[254,255,256]。フォーマルメソッドの応用研究のコミュニティにおいては、設計段階からセキュリティの組込みおよび検証を行うことが重視されている[257,258,259,260]ことから、NISC が提唱する SBD(Security By Design)の政策目標と合致する技術である。欧米における科学的なソフトウェア開発アプローチは、1968 年の NATO ソフトウェア工学会議[261]にまでさかのぼる事ができ、以後継続的な取り組みが行われている。日本では、専門家による研究は行われているが[262]、研究者の数は欧米に比べて非常に少ないため、欧米の手法をベースとしたフォーマルメソッドに基づく情報セキュリティ評価・認証スキームが国際標準となった場合、日本は迅速に対応することができないことが懸念される。また、ソフトウェアに関する国際標準は、ICT 分野だけでなく、電子機器やソフトウェアを利用する多くの産業に影響が及ぶことが予測されることから、日本には、国際標準となる前の段階から、欧米諸国の標準化活動の状況や研究開発動向に関する情報の収集等を行うことにより、フォーマルメソッドへの準拠を規定している国際標準に基づいて設計・開発を行うことができるように準備をするとともに、日本の高い品質基準を、フォーマルメソッドのような国際的に受け入れられやすい科学的な手法に基づき、国際標準とすることにより、欧米主導による国際標準という現状から脱却するための取り組みを推進することが求められる。日本発の国際標準に向けた活動の方向性としては、日本の企業がこれまで培ってきた独自の設計・開発・製造手法を用いることによっても同様に電子機器やソフトウェアの情報セキュリティを確保できることを示すことにより、フォーマルメソッド以外の手法により設計・開発された電子機器やソフトウェアが、フォーマルメソッドに基づいて設計・開発された電子機器やソフトウェアと、セキュリティ・アシュアランスの点において互換性を持つということを各国に理解してもらうための施策を実施することが重要である。

日本がこのような多面的な対応を行うためには、フォーマルメソッドに基づいて設計・開発を行う能力を有する人

---

253 技術標準化における途上国などの浮動票国への無償技術提供の例として、UWB(Ultra Wide Band： 超広帯域無線)の標準化における米 XtremeSpectrum の関連特許無償提供などがある。
http://techon.nikkeibp.co.jp/members/NEWS/20031107/100424/?ST=bbint

254 World Congress on Formal Methods in the Development of Computing Systems, 1999

255 T. Lacomte, T. Servat, G. Pouzancre：Formal Methods in Safety-Critical Railway Systems, Proceedings of Brazilian Symposiumon FormalMethods: SMBF 2007, pp26-30 (2007)

256 Formal Methods:State of the Art and Future Directions, ACM Computing Surveys, 1996

257 Masaki Ishiguro, Ataru T. Nakagawa, Proof Abstraction with Parametric Specifications and Views in CafeOBJ, Joint Workshop on Calculemus and Types/ User Interface for Theorem Provers, The Netherlands, July, 1998

258 Masaki Ishiguro, Ataru T. Nakagawa, Proof Assistance for Algebraic Specifications Based on Proof Obligations in CafeOBJ, "Cafe: An Industrial-Strength Algebraic Formal Method",pp.79-96, Elsevier Science Ltd, 2000

259 石黒正揮 モデル検査による組込みソフトウェア検証とモデリング・パターン化の研究開発　経済産業省 新世代情報セキュリティ研究開発シンポジウム(2009 年 3 月)

260 石黒正揮「形式手法の概観とモデル検査法の応用」、第 12 回組込みシステム開発技術展 ソフトウェアエンジニアリング専門セミナー

261 SOFTWARE ENGINEERING, Report on a conference sponsored by the NATO SCIENCE COMMITTEE, http://homepages.cs.ncl.ac.uk/brian.randell/NATO/nato1968.PDF

262 フォーマルメソッドの潮流 情報処理学会誌 (2008 年 5 月)

材と、日本独自の設計・開発・製造手法の国際標準化に向けた取り組みを推進する人材が必要となる。前者については、フォーマルメソッドは、従来のソフトウェア開発やプログラミングとは異なり、数理論理学の基礎的な素養を必要とするため、企業が提供する研修だけでは十分な人材を育成するのは難しく、大学・大学院等の高等教育機関におけるカリキュラムに組み込むことが必要となる。欧米では、大学・大学院等の高等教育におけるフォーマルメソッドに関する教育が充実していることが、専門家の育成に寄与している[263]。従って、日本においても、フォーマルメソッド等のソフトウェアのセキュリティや信頼性の分野における専門家・技術者を育成するための高等教育機関あるいは国立研究所等における教育・研修コースの拡充を行うと同時に、日本独自の設計・開発・製造手法のメリットを各国に理解してもらい、最終的に国際標準に関する議論の場で各国の賛同を得られるようにするために必要なスキルを有する人材の育成にも取り組むことが求められる。

3.2.3. 外部不経済[264] の内部化[265] と産業振興をバランスさせる情報セキュリティ保険

ソフトウェアの不具合に起因する情報セキュリティの問題点は、消費者がソフトウェアを購入する時点では認識できない場合が多く、また、問題点が全くないソフトウェアは、技術的にも経済的にも現実的ではない。現状では、問題点を修正するために、ベンダーから修正プログラム(パッチ)がリリースされるたびにユーザ自身が対象となるソフトウェアに適用しなければならないが、実際に全てのソフトウェアに修正プログラムが適用されることは期待できず、パッチが適用されていない PC がマルウェアに感染してボットの構成要素となる、DDoS 攻撃に加担させられるなど[266,267]、ソフトウェアを開発した主体以外に対して何らかの不利益を生じさせる状況となっている[268]。このような状況は、一般的に外部不経済(Externality)と呼ばれ、解決するためには、たとえば、市場メカニズムを機能させるようにする等の処置を行うといったなんらかの政策的手段を講じることが必要である。

製品・サービスの情報セキュリティ水準は、製品・サービスに情報セキュリティに起因する問題が発生した場合にどれだけの被害・影響が生じるかの度合いに応じて決定されるべきであり、航空宇宙分野など、一つの事故が大きな被害を招く可能性のある分野や自動車・医療機器などの人命に係わる可能性のある分野など、特定の分野にはきわめて高い情報セキュリティ水準が求められるが、情報処理等の一般的な業務に使用される情報システムに関しては、リスクとコストのバランスに見合う情報セキュリティ水準が確保されれば十分であると考えるのが通常である。想定されるリスクに見合う情報セキュリティ水準以上に高い水準の情報セキュリティを求めることは、開発コストの増加に伴う製品価格の上昇や、その分野からベンダーが撤退することによる技術革新や産業活力の停滞を招く可能性がある。

米国では、情報システムの不具合に起因する事故への対応が事前に考慮されているが、たとえば、ソフトウェアの不具合を修正するためのアップデートの作業の実施は、ユーザの責任となっている。米国でソフトウェアが製造物責任法の適用対象外となっている理由としては、このような背景があるものと考えられる。

グローバルにも、情報システムの多少の不具合は受け入れつつ、それを上回るベネフィットの方を高く評価しようという考え方が主流である[269]。

情報システムのセキュリティに係わるコストの問題に対処するために、情報セキュリティ保険の導入が有効であ

---

263 http://spinroot.com/spin/whatispin.html

264 ある経済主体の活動が、市場メカニズムを通さずに、他の経済主体にとってネガティブな影響を及ぼすこと。たとえば、工場が発生する公害は、工場で生産される製品の取引市場を通さずに、工場周辺の住人に健康被害を与えることなど。

265 外部不経済を解消するために、税制や規制などの導入により市場メカニズムが機能するようにすること。

266 Masaki Ishiguro, Yoichi Shinoda," An Internet Threat Evaluation Method based on Access Graph of Malicious Packets", 19th Annual FIRST Security Conference, 2007

267 Masaki Ishiguro et al, "Proposal on Collaboration of Internet Threat Monitoring and Analyses using 3D Visualization System", APCERT Annual Conference, March 11th, 2008

268 企業における情報セキュリティガバナンスのあり方に関する研究会 第1回議事要旨

269 次世代IT産業論考　浜口友一 http://it.nikkei.co.jp/business/column/hamaguchi_it.aspx?n=MMIT2z000018042008

ると考えられる。理由は以下の通りである。

- ソフトウェアの不具合に起因する損害が発生した場合に、損害を適度なコストで補填することができ、過剰な情報セキュリティ対策コストを負担する必要がないため、産業活力を失うことを回避することができる。
- 一般に保険への加入は任意であるが、情報セキュリティ保険の保険料を、コモンクライテリアなどにより規定される情報セキュリティ対策水準に応じて定められた額に相当する拠出金(税金)としてベンダーから徴収することにより、外部不経済を解消するための費用負担の仕組みを市場メカニズムに組み込むことができる。

現状では、情報システムの不具合に起因するリスクについては十分な認識・理解がされておらず、リスクが現実化した場合の損害を補償するための情報セキュリティ保険は十分には活用されていない[270,271,272,273,274]。業務や産業ごとにどの程度の情報セキュリティが求められるのかに関する研究や、ソフトウェアの脆弱性の削減手法に関する調査研究などを実施することにより、情報セキュリティ保険と情報セキュリティ対策水準との関係をより明確化し、情報セキュリティ保険が有効な情報セキュリティ対策として活用されるようにすることが重要である。

3.2.4. CIO、CISO の権限と責任の強化

米国においては、民間企業および政府機関の CIO や CISO の権限および責任が明確化され、情報システムの調達において情報セキュリティに係わる要件を明確化する傾向が強い[275]。一方、日本においては、政府および民間企業における CIO・CISO の責任が明確になっていないため、情報システムやソフトウェアの調達、システム構築のアウトソーシングにおいて、情報セキュリティに関する要件を明確化することなく、委託先企業に丸投げする傾向が強いといわれている[276]。

情報システムやソフトウェアの情報セキュリティ水準を向上させるためには、CIO・CISO の責任、権限を強化し、より大きな裁量を持って情報セキュリティ対策を推進できるようにすることが必要である。一方、CIO・CISO にも、情報セキュリティに関する広く深い専門知識を持つと同時に、CIO・CISO の下で業務に従事する人材を育成するという役割を果たすことも求められる。

3.2.5. 政府調達基準の実効性強化

米国では、FISMA および IT 改革法を根拠として、FIPS を米国連邦政府の情報システム調達基準とすることが義務化されており、情報システムの最大のバイヤーとしての連邦政府が、政府調達基準に情報セキュリティに関する基準を導入することで、製品・サービスの情報セキュリティ水準の向上に寄与していると考えられる。一方、日本においては、CRYPTREC[277]、JCMVP[278]、JISEC[279]などの調達基準に係わる製品認定制度が運営されて

---

270 Masaki Ishiguro, Hideyuki Tanaka, Kanta Matsuura, The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market, Workshop on the Economics of Securing the Information Infrastructure, Washington DC(WESII 2006)

271 Gordon, L. A. and M. P. Loeb, "The Economics Information Security Investment," ACM Transactions on Information and System Security, November 2002.

272 石黒正揮 IT 事故と情報セキュリティ対策の企業価値に与える影響分析　経済産業省 リスク定量化ワークショップ（2007 年 3 月 25 日）

273 石黒正揮、松浦幹太、田中秀幸　情報セキュリティ対策による企業価値向上に関する影響分析　暗号と情報セキュリティシンポジウム 2009 (2009 年 1 月 21 日)

274 Cyber Insurance and IT Security Investment: Impact of Interdependent Risk, Hulisi Ogut, Workshop on Economics of Information Security, 2005

275 JEITA ソフトウェア事業委員会「ソフトウェアリソースの最適活用に関する調査報告書」(2008 年 3 月)

276「システム・インテグレータの時代―究極のアウトソーシング戦略」 社団法人 情報サービス産業協会「特サビ実態調査」

277 http://www.cryptrec.go.jp/

いるが、政府調達基準としての義務化はされていないため、セキュアな製品・ソフトウェアの普及という観点からは、米国ほどの実効性は発揮されていない。

日本政府の情報システムの調達額は、2001 年度で 2.2 兆円[280](中央省庁、地方自治体の合計)であり、情報システムを開発する事業者に対する影響力は非常に大きい。このような調達者としての影響力の大きさを考えれば、政府調達基準に情報セキュリティに関する要件(JCMVP、CRYPTOREC 等)を組み込むことは、製品・サービスの情報セキュリティを向上させる上で非常に効果的であり、製品・サービスの情報セキュリティの向上に実効性を与えることができることが期待できる。

278 http://www.ipa.go.jp/security/jcmvp/
279 http://www.ipa.go.jp/security/jisec/
280 http://www.rieti.go.jp/jp/events/03020501/pdf/kishimoto_p.pdf