NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

情報セキュリティの国内外標準や制度の有効な活用方法

JNSA 情報セキュリティ標準調査WG
佐藤慶浩　(日本HP)
http://yosihiro.com/business/

2002 年 11 月 14 日

講師略歴

佐藤　慶浩（さとう　よしひろ）
日本ヒューレット・パッカード株式会社
HPコンサルティング統括本部
セキュリティ・コンサルティング部　部長

1986 年。日本アポロコンピュータ(株)入社。International R&Dに所属。マサチューセッツ州チェルムスフォード市にて日本語環境製品の開発に従事。
1990 年。日本ヒューレット・パッカード(株)入社。新製品のテクニカル・マーケティングとして、OSF／1、分散環境コンピューティング技術、マルチメディア技術、ハイアベイラビリティ技術、インターネット技術をHP社の製品提供と相応して順次担当。この間 1993 年からの 2 年間はカリフォルニア州クパチノ市にてセキュリティ製品の仕様開発に従事。
1996 年、米国駐在中に計画した製品群の出荷が始まったため、現在は主としてセキュリティ・ソリューションのコンサルティングに従事している。
1997 年以後は、通常のコンサルティング活動の他に、ＪPCERT／CCのヒューレット・パッカード対応窓口を担当。また、ＦISC(金融情報システムセンタ)、ＪＩＳＡ（情報サービス産業協会）、ＪUAS（日本情報システム・ユーザ協会）、システム監査人協会や各種有料セミナにて情報セキュリティポリシー策定方法論についての講演をしている。

情報処理学会(www.ipsj.or.jp/)　正会員
日本ネットワークセキュリティ協会(www.jnsa.org/)　理事
情報処理振興事業協会(www.ipa.go.jp/)セキュリティセンター　非常勤研究員
金融情報サービスセンター (www.fisc.or.jp/)セキュリティポリシー研究会　委員
情報処理学会 情報規格調査会(www.itscj.ipsj.or.jp/) SC 27/WG 1小委員会　委員
杉並区住基ネット調査会(www.city.suginami.tokyo.jp/) 技術専門委員
情報ネットワーク法学会(www.in-law.jp/) 理事

 Page 2

標準調査WG発足の背景

発端は技術用語WGにて、用語を各種標準からリストアップしましたが、その訳語が統一されていないことに問題意識を持ったことです。

また、認定制度全体の枠組みが不明瞭であることも、問題だと思っています。既存WGのいくつかは、それぞれの認定に関係していますが、このままでは、それぞれの認定間の位置づけなどが見渡せません。

そこで、認定制度そのものに焦点を置いた、調査WGを新設し、同じ基準で調査をすることが有益であると考えました。

現時点では、成果物を定めない調査WGとして発足していますが、作業がうまく軌道に乗れば、各WGに対して、対応する認定制度についてのインプットを提供できるものと考えています。

 Page 3

標準調査WGメンバー (順不同)

NTTデータ	寺井様
ｼｬｰﾌﾟｼｽﾃﾑﾌﾟﾛﾀﾞｸﾄ	笹井様
日新電機	井上様
横河電気	武智様、武部様、(山田様)
ニューコム	市場様
大日本印刷	半田様
ラック	足利様、宮西様
ｱｲ・ﾃｨ・ﾌﾛﾝﾃｨｱ	小林様
情報数理研究所	伏見様
ｲﾝﾀｰﾈｯﾄ総合研究所	佐藤様、藤野様
日本電気ｴﾝｼﾞﾆｱﾘﾝｸﾞ	茂出木様
東芝情報ｼｽﾃﾑ	石井様
電通国際情報ｻｰﾋﾞｽ	田中様
日本HP	若干名

 Page 4

標準調査WG活動内容

JNSA

個々の標準・認定制度の内容の勉強
各標準・認定制度の相互の位置づけを整理し、体系を確認する
各標準・認定制度の特徴などを、横断的にまとめて整理する
対象として、人に対する試験・認定も含めてみる（努力目標）
法律との関係を調べる（努力目標）

以下の成果物の作成（努力目標）

標準・認定制度の一覧表
用語WGの用語との整合を計る情報源としたい

一覧表の縦項目

JNSA

名称・規格番号
国際規格か国内規格の別
規格の範囲（対象：製品か運用か等）
規格の作成組織
取り扱い者（誰が規格詳細を習得すべきか）

関連規格、法律
関連情報（URL等）

日本語化の担当組織

国内の認定制度の有無
　認定（審査方法：再審査の有無等）
　認定取得のための費用・期間の目安・考え方

調査対象の規格

ISO/IEC 13335 (GMITS) - JIS TR X0036(No.1 - No.4)
BS7799 Part1, Part2
ISO/IEC 17799 - JIS X5080
ISMS
ISO/IEC 15408 - JIS X5070
SSE-CMM - JIS TR X0021(No.1 - No.9)

CEM (評価機関の認定用規格)
ISO/IEC 17205 (評価機関の運用ガイドライン)
CCRA (国際間相互認証)

経済産業省　安全対策基準
総務省　安全・信頼性基準
プライバシー・マーク - JIS Q15001

 Page 7

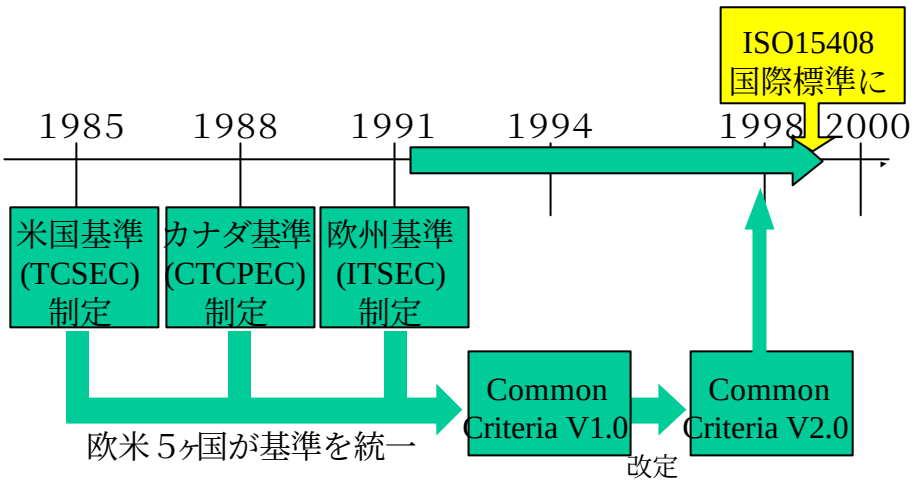
情報セキュリティ標準の解説

ISO/IEC 15408 (JIS X5070)

ISO/IEC 17799 (JIS X5080)

 Page 8

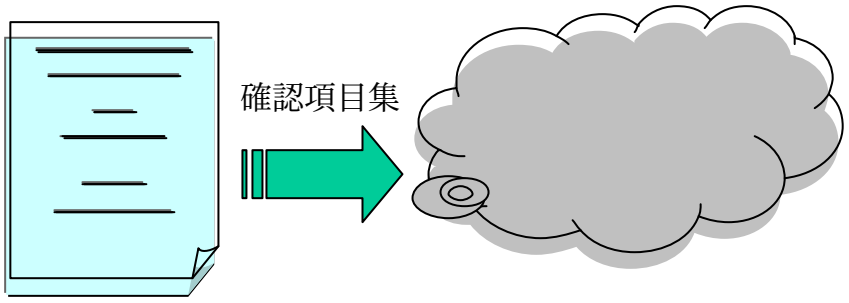
ISO/IEC 15408 (JIS X5070)



 Page 9

ISO/IEC 17799 (JIS X5080)

情報セキュリティ管理施策の規範



情報処理学会 情報規格調査会(www.itscj.ipsj.or.jp/) SC 27/WG 1小委員会

 Page 10

着目すべき観点

ISO/IEC 15408

適用対象範囲 → SSE-CMM
司法取引の前提

ISO/IEC 17799

試験対策勉強による本末転倒
項目＝教科に喩えられる
例外対応能力の欠如

 Page 11

ガイドライン・法令等

監督官庁ｶﾞｲﾄﾞﾗｲﾝの例

通商産業省
- 情報ｼｽﾃﾑ安全対策
- コンピュータウィルス対策
- 不正ｱｸｾｽ対策基準

JIPDEC
- プライバシ・マーク

警察庁
- 情報ｼｽﾃﾑ安全対策指針
- ｺﾝﾋﾟｭｰﾀｳｨﾙｽ等不正ﾌﾟﾛｸﾞﾗﾑ対策指針

FISC
- 安全対策基準
- ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定手引書
- 個人ﾃﾞｰﾀ保護取扱指針（改訂版）

総務省総合通信基盤局
- 情報通信ﾈｯﾄﾜｰｸ安全・信頼性基準（H13.3.22改正案）

（一部出典：高橋　郁夫先生）

法令等の例

関係法令の例
刑法典上の犯罪
- 電子計算機詐欺罪（246条の2）
- 電磁的記録等毀棄罪（258条、259条）
- 電子計算機損壊等業務妨害罪（234条の2）
- 電磁的記録不正作出罪（161条の2）

特別法上の規制
- 不正競争防止法
- 著作権法
- 不正アクセス禁止法

（出典 **石井　徹哉先生**）

関係法令の例（追加）
- 個人情報保護基本法→個人情報保護法
- IT基本法
- 特定電子商取引円滑化法
- プロバイダー責任法

＊被害を受けないことばかりではなく、加害者にならない配慮も重要

 Page 12

まとめ

①標準を偏重しないようにしたい
　情報セキュリティ施策に 9＋ 3／ 4番線ホームはない

②売るためには、何でもしてよい。のではなくしたい
　必要なものをちょうど良く売る
　マッチ・ポンプにバケツ

③できる協力はしたい

 Page 13

 Page 14

	表作成担当者
ISO／IEC 13335 (GMITS)	HP 永沼
JIS TR X0036 (No.1-4)	(NTTDATA 寺井様)
ISMS	NTTDATA 寺井様
BS7799 Part1,Part2	横河電気 山田祥子様
ISO／IEC 17799	横河電気 山田祥子様
経済産業省 安全対策基準	HP 山口
総務省 安全・信頼性基準	HP 山口
ISO／IEC 15408	日新電機 井上様
JIS X5070	日新電機 井上様
CEM 評価機関の認定用規格)	ラック 宮西様
ISO／IEC 17025 評価機関の運用ガイドライン)	ラック 宮西様
CCRA (国際間相互認証)	ラック 宮西様
SSE－CMM	HP 佐藤
JIS TR X0021 (No.1-9)	(NTTDATA 寺井様)
プライバシー	
JIS Q15001	シャープ 笹井 隆志様
Pマーク	シャープ 笹井 隆志様

シャープ 笹井 隆志様

(欠席)ニューコム 市場ちよ様
(欠席)大日本印刷 半田様

名称(英語/日本語)	SSE-CMM (Systems Security Engineering Capability Maturity Model)
規格番号	なし
国内での認定制度の有無	有
~~制定年度~~	2000/5月？
国際か国別	米国
対象者（ユーザ・ベンダー・人）→誰が勉強すべきか	ベンダー（エンドユーザ）
規格の範囲・分類（何に対するものか：物か運用か等）	運用
規格の作成組織	米国防総省予算 ISSEA(International Systems Security Engineering Association)
~~(改訂頻度の有無)~~	できたばかり
所管官庁（色付けだけの場合あり）	経済産業省
日本語化の組織	IPA公募案件で情報数理研究所
認定審査方法・組織（認定発行と審査の別などの仕組みも含め）	国内は検討中（リンクする）
認定取得費用の目安	不詳
認定取得期間の目安（対象規模の想定を記載する）	6-12ヶ月
認定取り消しの基準の有無	なし？
認定の再監査の期間（有効期限）	なし？
関連規格	CMM JIS TR X0021 (No.1-9)
認定のポイント→解説書	http://www.ipa.go.jp/security/ccj/download.htm
関連する法律	
関連URL	http://google.yahoo.com/bin/query?p=SSE-CMM&hc=0&hs=0 http://www.sse-cmm.org/ http://www.issea.org/ssecmm.html http://www.imslab.co.jp/SSE-CMM/SSE-CMMseminor.html http://www.software.org/quagmire/descriptions/sse-cmm.asp http://www.issea.org/Notes_May00.html

名称（英語/日本語）	ISO／IEC 15408	JIS X5070
規格番号	ISO／IEC 15408	JIS X5070
国内での認定制度の有無	有	有
制定年度	1999年	2000年7月
国際・国内かの別	米・英・仏・独・加・豪/NZ、他7カ国	国内
対象者（ユーザ・ベンダー・人）	ﾍﾞﾝﾀﾞｰ	ﾍﾞﾝﾀﾞｰ
規格の範囲・分類（何に対するものか：物か運用か等）		
規格の作成組織　スポンサー		
改訂頻度の有無		
所管官庁（色付けだけの場合あり）	経済産業省	経済産業省
日本語化の組織		
認定審査方法・組織（認定発行と審査の別などの仕組みも含めて）		独立行政法人製品評価技術基盤機構
認定取得費用の目安		
認定取得期間の目安		
認定取り消しの基準の有無		
認定の再監査の期間（有効期限）		
関連規格	ISO/IEC 17025	JIS Q 17025
認定のポイント→解説書		http://www.nite.go.jp/asse/its/index.htm
関連する法律		
関連URL	http://csrc.nist.gov/cc/ccv20/ccv2list.htm	

名称	CEM（15408に基づく評価手法）
規格番号	
国内での認定制度の有無	なし
（制定年度）	
国際・国内かの別	
対象者（ユーザ・ベンダー・人）→誰が勉強すべきか	人（評価者）
規格の範囲・分類（何に対するものか：物か運用か等）	15408に基づく評価手法
規格の作成組織（スポンサー？）	CC作成グループCCIBMのCEMグ
（改訂頻度の有無）	
所管官庁（色付けだけの場合あり）	
日本語化の組織	IPA
認定審査方法・組織（認定発行と審査の別などの仕組みも含めて）	
認定取得費用の目安	
認定取得期間の目安（対象規模の想定を記載する）	
認定取り消しの基準の有無	
認定の再監査の期間（有効期限）	
関連規格	ISO/IEC15408
認定のポイント→解説書	
関連する法律	
関連URL	http://www.ipa.go.jp/security/ccj/ninshou/cc&mra.htm#cc_project

名称	CCRA（15408の相互承認協定書）
規格番号	
国内での認定制度の有無	なし?
（制定年度）	1998年10月
国際・国内かの別	相互承認参加国間
対象者（ユーザ・ベンダー・人）→誰が勉強すべきか	相互承認参加国
規格の範囲・分類（何に対するものか：物か運用か等）	15408に基づいた認証書の有効範囲
規格の作成組織（スポンサー？）	
（改訂頻度の有無）	2000年5月に一度改定
所管官庁（色付けだけの場合あり）	（日本は不参加）
日本語化の組織	
認定審査方法・組織（認定発行と審査の別などの仕組みも含めて）	
認定取得費用の目安	
認定取得期間の目安（対象規模の想定を記載する）	
認定取り消しの基準の有無	
認定の再監査の期間（有効期限）	
関連規格	ISO/IEC15408
認定のポイント→解説書	
関連する法律	
関連URL	http://www.ipa.go.jp/security/ccj/ninshou/cc&mra.htm#cc_project

名称	ISO／IEC 17025 「試験所及び校正機関の能力に関する国際規格」
規格番号	
国内での認定制度の有無	
（制定年度）	
国際・国内かの別	国際
対象者（ユーザ・ベンダー・人）→誰が勉強すべきか	
規格の範囲・分類（何に対するものか：物か運用か等）	
規格の作成組織（スポンサー？）	
（改訂頻度の有無）	
所管官庁（色付けだけの場合あり）	
日本語化の組織	
認定審査方法・組織（認定発行と審査の別などの仕組みも含めて）	
認定取得費用の目安	
認定取得期間の目安（対象規模の想定を記載する）	
認定取り消しの基準の有無	
認定の再監査の期間（有効期限）	
関連規格	JIS Q 17025 ISO/IEC Guide25
認定のポイント→解説書	
関連する法律	
関連URL	http://www.sonytek.co.jp/Customer_Service/cs_aboutG25.html

後日part 1～５を横に並べる

名称	ITセキュリティマネジメントガイドライン（GMITS:TR13335）
規格番号	ISO/IEC TR 13335 (*)
国内での認定制度の有無	TR (Technical Report)
~~制定年度~~	1991年～（）
国際・国内かの別	国際
対象者（ユーザ・ベンダー・人）→誰が勉強すべきか	人
規格の範囲・分類（何に対するものか・物か運用か等）	運用（ITセキュリティのマネジメント）
規格の作成組織	ISO　JTC 1/SC 27
~~改訂頻度の有無~~	
所管官庁（色付けだけの場合あり）	経済産業省
日本語化の組織	JISC(日本工業標準調査会)
認定審査方法・組織（認定発行と審査の別などの仕組みも含め	
認定取得費用の目安	
認定取得期間の目安	
認定取り消しの基準の有無	
認定の再監査の期間（有効期限）	
関連規格	
認定のポイント→解説書	
関連する法律	
関連URL	http://www.iso.ch/iso/en/StandardsQueryFormHandler.StandardsQueryFormHandler?languageCode=en&keyword=&lastSearch=false&isoNumber=13335&isoPartNumber=&ICS=&stageCode=&stageDate=&committee=ALL&subcommittee=&scope=CATALOGUE&sortOrder=ISO
	http://www.jisc.org/jis1.htm

(*)

ISO/IEC TR 13335-1:1996
Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security

ISO/IEC TR 13335-2:1997
Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security

ISO/IEC TR 13335-3:1998
Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security

ISO/IEC TR 13335-4:2000
Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards

ISO/IEC TR 13335-5:2001
Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security

名称（英語・日本語）	JISQ15001	Pマーク
規格番号	JISQ15001	JISQ15001
国内での認定制度有無		認定制度あり
制定年度	平成11年4月	平成10年4月
国際・国内かの別	国内	国内
対象者（ユーザ・ベンダー・人）	個人情報利用事業者	プライバシーマークの付与を申請できる事業者は、国内に活動拠点を持つ民間事業者であって、定められた諸条件を満たしている民間事業者
規格の範囲・分類（何に対するものか：物か運用か等）		プライバシーマークの付与は、事業者（法人）単位を原則とします
規格の作成組織	JIPDEC	JIPDEC
改訂頻度の有無		
所管官庁（色付けだけの場合あり）		
日本語化の組織		
認定審査方法・組織（認定発行と審査の別などの仕組みも含めて）		
認定取得費用の目安		
認定取得期間の目安		
認定取り消しの基準の有無		
認定の再監査の期間（有効期限）		
関連規格		
認定のポイント→解説書		http://www.jipdec.or.jp/security/privacy/yoryo.html
関連する法律		
関連URL		http://www.jipdec.or.jp/security/privacy/

名称	ISMS適合性評価基準（Ver0.8）
規格番号	特に無し
認定制度の有無	有
制定年度	Ver1.0をH14.4に公開予定
国際・国内かの別	国内
対象者（ユーザ・ベンダー・人）	ベンダー（情報処理サービス業）
規格の範囲・分類（何に対するものか：物か運用か等）	情報セキュリティマネジメント
規格の作成組織	JIPDEC
改訂頻度の有無	（まだVer0.8）
所管官庁（色付けだけの場合あり）	経済産業省
日本語化の組織	（もともと日本語）
認定審査方法・組織（認定発行と審査の別などの仕組みも含めて）	ISMS適合性評価制度
認定取得費用の目安	（会社にいけばわかります）
認定取得期間の目安	（会社にいけばわかります）
認定取り消しの基準の有無	無
認定の再監査の期間（有効期限）	3年間
関連規格	ISO/IEC17799、BS7799Part2
認定のポイント→解説書	ISMSガイド
関連する法律	？
関連URL	（ISMS適合性評価制度）http://isms.jipdec.or.jp/

名称	BS7799 第 1部 :情報セキュリティ管理実施基準 (Part1 Code of practice for information security management) 第 2部 :情報セキュリティ管理システム仕様 (Part2 Specification for information security management	ISO/IEC 17799
規格番号	BS7799-1、BS7799-2	
国内での認定制度の有無	有	無
制定年度		
国際・国内かの別	英国	国際
対象者（ユーザ・ベンダー・人）	ユーザー	ユーザー
規格の範囲・分類（何に対するものか :物か運用か等）	運用	運用
規格の作成組織	英国規格協会(British Standards Institute)	ISO
改訂頻度の有無	無	無
所管官庁（色付けだけの場合あり）	?	？
日本語化の組織	日本規格協会	
認定審査方法・組織（認定発行と審査の別などの仕組みも含め	BSIジャパン	
認定取得費用の目安	? 初回認証時 申請料 10万円　（現時点での単価、以下同じ）、 1人日の単価（現在22.5万円）に必要工数（人日数）を乗じた審査料 その他審査員の移動、宿泊に関わる費用等 年間維持料（認証取得後） 11万円 定期審査料（認証後も、半年ごとの頻度でシステムの運用状況等の審査があります。 審査料は初回審査と同じ計算方法になります。）	
認定取得期間の目安	半年～ 1年	
認定取り消しの基準の有無	?	
認定の再監査の期間（有効期限）	?	
関連規格		
認定のポイント→解説書	PD3000	
関連する法律		
関連URL	http://www.bsi-j.co.jp/	

名称	情報システム安全対策基準	情報処理サービス業情報システム安全対策実施事業所認定制度
規格番号	―	-
規格・認定かの別	認定	認定
制定年度	平成7年度	
国際・国内かの別	国内	国内
対象者（ユーザ・ベンダー・人）	エンドユーザ（情報システムを利用している企業全般？）	エンドユーザ
規格の範囲・分類（何に対するものか：物か運用か等）	設置施設・情報システム・運用	
規格の作成組織	経済産業省（作成時は通商産業省）	
改訂頻度の有無	改訂あり（最終改訂平成9年度）	
所管官庁（色付けだけの場合あり）	経済産業省	
日本語化の組織	―	
認定審査方法・組織（認定発行と審査の別などの仕組みも含めて）		現在はISMS？
認定取得費用の目安		
認定取得期間の目安		
認定取り消しの基準の有無		
認定の再監査の期間（有効期限）		
関連規格	システム監査基準/コンピュータウイルス対策基準	
認定のポイント→解説書		
関連する法律		
関連URL	http://www.meti.go.jp/kohosys/topics/10000098/esecu03j.pdf	

名称	情報通信ネットワーク安全・信頼性対策実施要録規程
規格番号	-
規格・認定かの別	認定
制定年度	昭和62年度
国際・国内かの別	国内
対象者（ユーザ・ベンダー・人）	エンドユーザ（第2種電気通信事業向け）
規格の範囲・分類（何に対するものか：物か運用か等）	情報通信ネットワーク
規格の作成組織	総務省（作成時は郵政省）
改訂頻度の有無	？
所管官庁（色付けだけの場合あり）	総務省（作成時は郵政省）
日本語化の組織	-
認定審査方法・組織（認定発行と審査の別などの仕組みも含めて）	総務大臣。規程上に記述あり
認定取得費用の目安	
認定取得期間の目安	
認定取り消しの基準の有無	有
認定の再監査の期間（有効期限）	3年
関連規格	情報ネットワーク安全信頼性基準
認定のポイント→解説書	http://www.soumu.go.jp/joho_tsusin/whatsnew/kokuji/network_2001feb.html
関連する法律	電気通信事業法
関連URL	http://www.soumu.go.jp/joho_tsusin/whatsnew/kokuji/network_2001feb.html