情報セキュリティ監査について

セキュリティ監査WG前リーダー
朝賀　康義

2002年9月経済産業省が、「情報セキュリティ監査研究会（以下、「研究会」という。）」が発足し、JNSA下村事務局長が委員として選任されました。JNSA政策部会では、研究会の各種実作業を行うためにセキュリティ監査WGを発足し、「情報セキュリティ管理基準」、「情報セキュリティ監査人スキルマップ」などを作成してまいりました。そして、本年度から「情報セキュリティ監査制度」の運用が始まり、特に初期においては地方自治体からのセキュリティ監査のニーズが多いことを想定し、「電子自治体のためのセキュリティ管理基準」を策定しています。なお、監査WGでは、この基準を使って実際に監査を受けていただける地方自治体を募集しています。
ここでは、情報セキュリティ監査制度とセキュリティ監査WGの活動についてご紹介いたします。

1. セキュリティ監査制度の必要性

情報システムを構成するハードウェアやソフトウェアの高度化や、ブロードバンドの普及、さらには電子政府／電子自治体の進展などもあいまって、情報システムは年々利便性が高いものになっています。一方、複雑化した情報システムにひそむ弱点をついたサイバー攻撃や、個人情報の漏えい、さらにはITを利用した詐欺事件などが多発しています。こうした状況において、企業、政府、自治体の情報セキュリティに関する関心は高まりつつあります。特に政府、自治体においては、今年度は総合行政ネットワーク（LGWAN）への接続や、8月からの住民基本台帳ネットワークの本格稼動があり、情報セキュリティに関する関心は否が応でも高まっています。また民間企業においても相次ぐ個人情報漏えい事件や個人情報保護法の成立を受け、急速に情報セキュリティへの関心が高まっています。

しかし、ウイルス対策ソフトやファイアウォールの導入など、個別的な対策はしているものの、人的・物理的・技術的なセキュリティを総合的に対策している組織体は多くはないようです。またポリシーをつくっていても、その運用状況をきちんと管理し、適切な情報セキュリティ管理をしている組織体は極めて少ないのが現状です。

表1　情報セキュリティ監査の実施状況

	実施している	実施していない	無回答
大企業(N=541)	20.0%	79.7%	0.4%
中小企業（N=951）	7.2%	91.7%	1.2%
地方公共団体（N=172）	4.7%	95.3%	0.0%
病院（N=109）	4.6%	95.4%	0.0%
大学（N=175）	9.1%	90.3%	0.6%
その他学術/研究機関 (N=70)	11.4%	88.6%	0.0%

（資料：総務省「情報セキュリティ対策の実施状況調査結果」）

情報セキュリティは、人的・物理的・技術的対策の最も脆弱な点から破れるものです。また攻撃の手法は日々高度化しています。したがって本来ならば、総合的な情報セキュリティ監査を定期的に実施／受ける必要があるはずですが、実際には、

・監査主体としては、「情報セキュリティ監査とは何か」という指針が無いため、監査の正当性を信じてもらえない
・被監査主体においては、どのような効果があるかわからない、誰に頼めばよいかわからない

といった課題があり、情報セキュリティ監査が普及していなかったようです。

そこで経済産業省情報セキュリティ監査研究会では、

①「情報セキュリティ監査」を考える上での基本的な視点を整理し
②「情報セキュリティ監査」の標準的な基準を策定し
③「情報セキュリティ監査」を行う主体のあり方を提示する

ことにしました。

加えて経済産業省では、この成果を受け、適正な「情

報セキュリティ監査」を受ける主体が増えることにより、日本全体の情報セキュリティのレベルが向上すること、また、「情報セキュリティ監査」の市場が適切に成長していくことを期待しています。

2. セキュリティ監査制度の概要

(1) 基本的な視点

①システムではなく情報資産を監査する

従来からある「システム監査」においてもセキュリティに関する視点はありましたが、あくまでも情報システムとしてのセキュリティの視点でした。現実世界では、システムの弱点だけでなく人の運用上の問題や悪意により情報セキュリティが破れることも多くなっています。そこで「情報セキュリティ監査」では、守るべきものは情報システムではなく情報資産であると考えています。

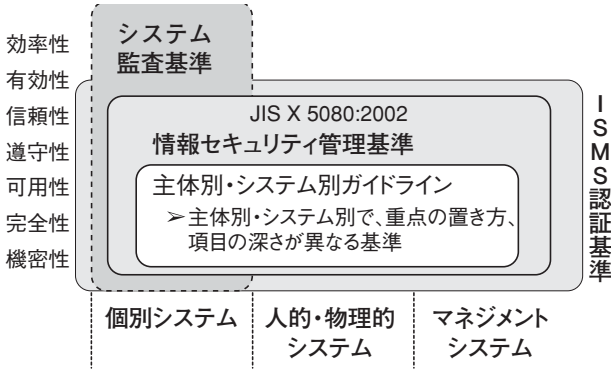
②セキュリティの強度ではなく情報資産に対するマネジメントを監査する

情報セキュリティを脅かすリスクは日々変化・高度化しています。ある時点におけるセキュリティ対策が明日も有効であるという保証はありません。そこで「情報セキュリティ監査」においては、ある時点における「情報セキュリティの強度」ではなく、その組織において情報資産に対するリスクのマネジメントが効果的に実施されているかどうかを監査すべきと考えています。

③マネジメントサイクルの視点

情報セキュリティリスクをマネジメントするには、情報資産に対するリスクアセスメント(評価)を行い、その評価を基に適切な管理策(コントロール)を割り当て、その管理策が適切に実施されているかどうか、そもそもリスクアセスメントが適切であったかどうかを評価する必要があります。情報セキュリティ監査では、このような評価を行い、情報セキュリティ対策を改善するのに役立つものになります。

図1　情報セキュリティ監査の対象



(2) 多種多様な監査ニーズに対応した監査制度

①保証型と助言型の選択制

監査には、監査結果を被監査主体の外部に対する“お墨付き”とする保証型監査と、改善課題を内部的に利用したり、責任の限界を外部に示すための改善提案型監査の二つがあります。

保証型監査では、監査人は、基準に照らして適合しているか否かについて意見を表明します。保証型監査の代表例は会計監査です。不適切な監査意見を表明したりすると賠償責任を問われたり資格を剥奪されるなどします。ただし(会計監査を含め)保証型監査といえども絶対の安全を保証するものではなく、監査人が見た範囲についての“合理的な保証”となっています。

改善提案型監査では、基準に対する適合性を○か×かで意見表明するのではなく、基準とのギャップを指摘したり、改善の方向性を示すことを目的としています。改善提案型の監査の代表例として、システム監査が挙げられます。

「情報セキュリティ監査」では、被監査主体のニーズにより、保証型監査でも改善提案型監査でも、どちらでも選択できるようにしています。これは、被監査主体としては、“お墨付き”を得たいというニーズがある一方、そのような第三者に対して保証を提供できる独立性や責任能力のある監査組織が少ないこと、またそもそも“お墨付き”が得られるほどの情報セキュリティ管理体制ができている組織が少ない現状において、“不適合意見”を得るために監査を受ける組織は無いであろうことから、「情報セキュリティ監査」を広めていくために、両方のタイプの

監査を選択できるようにしています。

②全部と一部の選択性

「情報セキュリティ監査」では、監査の対象範囲も自由に選択できます。もちろん、組織の全ての領域と全ての情報資産を対象とした方が望ましいのですが、対策ができた(あるいはできていない)部門から監査を受けるとか、ネットワークを使った外部からの攻撃への対策だけ先行して監査を受けるなど組織や情報資産の一部だけについて監査を受けることも可能とされています。

さらには、前述の保証型監査と改善提案型監査を組み合わせることもできるとされています。例えば、オフィスエリアの人的セキュリティについては改善提案型監査を受けて、ネットワークセキュリティについては保証型の監査を受けるといった混合型監査も認められています。

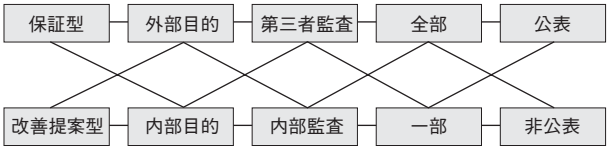
③多様な監査企業

「情報セキュリティ監査」には、経営、人的オペレーション、建築、ネットワークセキュリティ、法律など、幅広い領域の知識や経験が必要とされます。この全ての領域をひとりでカバーできているような人はもちろん、企業としても少ないのが現状です。「情報セキュリティ監査」を普及するためには、一握りの専門家や専門企業を監査主体として認めるのではなく、部分的でも一定の知識･経験を持つ主体を監査主体として取り込むことで、監査サービスの向上、被監査主体の満足が得られると考えられています。そこで、セキュリティソリューションベンダーのみならず、システム監査企業、監査法人、その他様々な業種の参入を認めています。

とはいえ、何の制限もない中では被監査主体が監査主体の選定に戸惑ったり、監査サービスの質の向上が期待できないことから、「情報セキュリティ監査企業台帳」に過去の実績などを公開することを最低条件とし、被監査主体が監査主体を選べるようにしています。

また今後、NPO日本セキュリティ監査協会(JASA、設立準備中)において、監査人として必要な資質や受けるべき研修などの基準を明らかにしていくことになるでしょう。

図2　情報セキュリティ監査は組み合わせ自由自在



3. 管理基準と監査基準

研究会では、半年間の活動の成果物として

①「情報セキュリティ管理基準」

②「情報セキュリティ監査基準」

を発表しました。

「情報セキュリティ管理基準」は、各組織が自らの情報セキュリティポリシー策定やセキュリティ対策を検討する際の拠り所であり、監査をする際のチェック項目ともなるものです。

また「情報セキュリティ監査基準」は、監査を行う際に監査主体が従うべき規範を定めたものです。

(1)「情報セキュリティ管理基準」

研究会では、「情報セキュリティ監査」制度におけるチェック項目である管理基準について、そのベースとして、JIS X 5080:2002を選びました。これは、

・情報システムではなく情報資産を対象とする

・リスクマネジメントの有効性を評価する

・国際的な整合性

の観点から、ISO/IEC 17799:2000をローカライズしたJIS X 5080:2002が最適と考えたためです。

情報セキュリティ管理基準は、JIS X 5080:2002をベースにしていますが、これをチェックリストとしてより使いやすくするために以下のような方法で体系化しています。

① 目的

② コントロール

「JIS X 5080:2002 の管理策(コントロール)」において、管理すべき内容が複数ある場合はそれを細分化する。

③ サブコントロール

「JIS X 5080:2002 の管理策(コントロール)のガイダンス」の内容を項目化し、内容に応じて上記のコントロールごとに振り分けする。

(2) 情報セキュリティ管理基準の使い方

情報セキュリティ管理基準を使って監査を実際に行う場合には、

・「コントロール」を判断尺度として使う

・組織の事業内容や規模により、「コントロール」を取捨

選択したり、追加したり、あるいはその業界の用語に読み替える

などの注意が必要です。

管理基準を見ると、一見「サブコントロール」がチェックすべき項目のように思えてしまいますが、そうではありません。「サブコントロール」は、統制目標である「コントロール」を達成するための手段の例示であり、その全てを実行することが求められているわけではありません。

また、取り扱っている情報資産の内容や業界特有の表現や規制にも配慮して運用することが必要です。例えば、個人情報取扱事業者においては、個人情報保護法に対応するために、管理基準で求められている以上の対策が必要な場合もあるでしょうし、自治体など行政機関では、“従業員”を“職員”に読み替えたり、“経営陣”をその組織の実態に合わせて読み替える必要があるでしょう。

【ISMS制度との関係】

情報セキュリティ監査制度の兄貴分にあたる制度として、「ISMS適合性評価制度」があります。情報セキュリティ管理基準がベースとするJIS X 5080は、元々は英国規格BS7799のベストプラクティス集であるpart1をベースにしているのに対し、ISMS適合性評価基準は、BS7799の認証基準であるpart2をベースにしています。したがって2つの基準は、個別システムではなく情報資産を組織としてトータルに保護するためのマネジメント体制を評価するという基本的な視点において整合性が取れています。制度として異なる点は、ISMS制度は認証するかしないか(マークを与えるか否か)の審査をするのに対し、情報セキュリティ監査制度は、前述のように「保証－改善提案」、「全部監査－一部監査」などを被監査主体が選択できるようにしている点です。

現時点においては、対外的なブランディングのためにはISMS制度、段階的な改善のためには情報セキュリティ監査制度を利用するなど、目的によって制度を使い分けることができるかもしれません。

4. JNSAセキュリティ監査WGの活動

【JNSAセキュリティ監査WGの活動】

JNSA政策部会では、情報セキュリティ監査研究会の発足を受けて、昨年9月にセキュリティ監査WGを発足しました。昨年度は、サブWGを2つつくり、監査基準サブWGでは、JIS X 5080ベースのセキュリティ管理基準の作成を支援し、セキュリティ監査人スキルマップ・サブWGでは、セキュリティ監査人に必要と考えられるスキルを洗い出しました。そして今年度は、電子自治体のためのセキュリティ管理基準モデルを策定し、パブリックコメントを募集いたしました。

セキュリティ管理基準は、経済産業省に正式に採用され、WEBでも公開されていますので、ここでは「セキュリティ監査人スキルマップ」と「電子自治体のセキュリティ管理基準(JNSA案)」をご紹介します。

(1) セキュリティ監査人スキルマップ

研究会の報告書でも指摘されている通り、監査人の質の確保が、「情報セキュリティ監査」制度が普及するかどうかを左右すると考えられます。そこでJNSA監査WGでは、セキュリティ監査人に要求されるスキル要件を洗い出すことにしました。この洗い出し作業には、ISMS認証取得コンサルティングの経験を持つコンサルタントを中心に、リスクアセスメントや内部監査など、ISMS構築の現場経験を踏まえて検討しました。

検討に当たっては、

- 日本情報処理開発協会　ISMS審査員研修コース基準2.2履修目標
- 日本情報処理開発協会　JITEC 情報処理技術者スキル標準～システム監査技術者

に示されるISMS審査員およびシステム監査技術者としてのスキル要件との比較をすることにより、情報セキュリティ監査人としてのスキル要件を浮彫りにしました。

またJNSA教育部会スキルマップWGの成果物「セキュリティ技術者スキルマップα.1版」も参考にしました。

この検討を通じて明らかになったのは、

- マネジメントシステム、技術的セキュリティ、人的セキュリティ、物理的セキュリティ、監査技術はそれぞれ独立した高度な知識である
- ISMS審査員およびシステム監査技術者のスキル要件では、技術的セキュリティ、人的セキュリティ、物理的セキュリティ、に関する要求が不十分である
- 特に技術的セキュリティについてのカバーが不十分である

ということでした。

特に、従来IT関連の監査の主流であった情報セキュリティ監査技術者の資格要件にセキュリティ技術に関する要件が少ないこと、またISMS審査員の研修基準においても（また実際の研修においても）セキュリティ技術に関する要件が少ないことから、今後「情報セキュリティ管理基準」を理解し、監査現場で技術的な確認をするには、追加の研修等が必要となることが予想されます。

ＷＧでは、こうした課題を解決するために「セキュリティ監査人スキルマップ案」とともに、以下の提言を経済産業省に提出しました。

- 独立した高度な知識を幅広く一人の人間が保有することは困難であるため、大組織に対する監査においては、複数の専門家による監査チームを編成することが望ましい
- 地方公共団体や中小企業など、監査予算規模が小さいが対象数が膨大な組織のために、必要要素を網羅した人材を育成する専門教育プログラムの開発が必要である
- 開発される専門教育プログラムは、カバーすべき範囲が広範であるため、受講者の既存資格や経験を考慮し、不足している領域のみを効率的に提供できるようにモジュール化することが望ましい

JNSA情報セキュリティ監査人SkillMAp α.1版
領域：技術的セキュリティ

情報セキュリティ監査人スキルマップ	
中分類	小分類
ファイアーウォール	ネットワークポリシー設計
	DMZ等構成の設計
	NAT (StaticNAT / DynamicNAT / IPマスカレード)
	ファイアーウォールのルーティング
	アクセスコントロール技術（PacketFilterling / Circuit Level Gateway / Application Level Gateway）
	ファイアーウォールの基礎的役割
侵入検知システム	IDS負荷分散
	HoneyPot
	IDSの弱点（FalsePositive ・ FalseNegative ・ 暗号環境での未検出 ・ Stick攻撃 ・ 取りこぼし）
	管理者への通知方法
	防御機能（TCPリセット/ルータ・ファイアウォールでの遮断）
	検知アルゴニズム（不正検出・異常検出）
	侵入検知システムの分類（NetworkIDS/Host IDS/ハイブリッドIDS）
	侵入検知システムの基礎的役割（ファイアウォール防御技術との違い）
ウィルス対策	防御システムの構築(ウイルスからの防御システム構造)
	対応ポリシー（感染時）
	設定ポリシー
	ウィルス対策個所の設計
	スキャン方式と検出方法
	感染媒体の種類と感染方法
	ウィルスの分類および定義の理解
	定義ファイルのアップデート
OSセキュリティ	アカウントの管理（ユーザ、パスワード）
	アクセス権の管理（ネットワーク、ディレクトリ・ファイル）
	ファイルシステム
	耐タンパー

情報セキュリティ監査人スキルマップ	
中分類	小分類
ネットワーク技術	ルーティング制御
	プロトコル制御
	アクセスコントール制御
	端末認証
	暗号化方式（SSL、IPSecなど）
	NAT
	運用管理（ログ、ＳＮＭＰ、設定ツール）
	無線ＬＡＮ
	ネットワーク基本知識
	ネットワーク設計技術(セキュア)
暗号	暗号アルゴリズム
	共通鍵暗号方式
	公開鍵暗号方式
	ハイブリッド方式
	暗号アルゴリズムの種類(ブロック暗号、ストリーム暗号)
署名	メッセージダイジェスト
	デジタル署名の仕組み
	デジタル署名の利点
認証	ワンタイムパスワード
	認証トークン(ICカード等)
	バイオメトリクス
	チャレンジ&レスポンス
	ID ・パスワード
攻撃手法	TCPスキャン
	UDP スキャン
	その他偵察行為
	Sniffing,盗聴行為
	パスワードクラック
	DoS攻撃
	DDoS攻撃
	バッファオーバーフロー
	Format String Bug
	トロイの木馬

Trusted OS	工事中
PKI(認証局の構築と運用)	認証局の運用形態
	認証局の構築
	秘密鍵管理(HSMN、アクセラレータ)
	認証局運用規程(CPS)
	証明書ポリシー(CP)
(PKIの定義)	認証機関
	証明書リポジトリ
	証明書失効
	鍵のバックアップと回復
	自動鍵更新
	鍵履歴
	相互認証
	否認防止のサポート
	タイムスタンプ
(PKIが提供するサービス)	認証
	データの完全性(否認防止)
	データの秘匿性
サーバーセキュリティ (Web)	一般的なWebシステム構成
	基本認証
	PAM認証
	SSL
	http通信・webサーバ・ブラウザの基本機能
	HTTP通信で利用される言語(html/XML)
	Webサーバの設定により脆弱になってしまう個所
	Webサーバ上でのファイルのパーミッション(wrxの付け方、umask
	サーバプログラム実行権限
	Chroot
	クライアントアプリケーション(プラグイン、ヘルパー、ActiveX)
	ログ管理
	ロジック爆弾
	メール爆弾
	Spyware
	バックドア
	不正アクセスの隠蔽(ログ改ざん等)
	古典的不正アクセス技法(サラミ)
	クロスサイトスクリプティング
	最新不正アクセス手法
	情報収集
	偵察行為
	攻撃後処理
その他	最新の攻撃手法・脆弱性情報の入手方法に関する知識

(参考) システム監査人コア知識・スキル	
中分類	小分類
情報技術一般	ソフトウェアに関する知識
	ハードウェアに関する知識
	ネットワークに関する知識
	コンピュータ設備に関する知識
情報技術の動向	Web技術(インターネット、イントラネット、エクストラネット)
	認証局(CA)、認証技術(PKIなど)
	暗号
	VPN(バーチャルプライベートネットワーク)

(2) 電子自治体のセキュリティ管理基準(JNSA案)

監査WGでは、「情報セキュリティ監査制度」に対応した地方自治体向けのセキュリティ監査における監査項目(セキュリティ管理基準モデル)を作成いたしました。

情報セキュリティ監査制度では、情報セキュリティ管理基準をもとに、被監査組織・業界ごとに実態に合った項目・表現に修正した管理基準を作成し、運用することを求めています。そこでJNSA監査WGでは、まず初めに電子自治体の推進、特に住基ネットの本格稼動を控え、情報セキュリティ対策の確立を強く求められている地方自治体向けの管理基準モデルを作成し、提案することにいたしました。

作業にあたっては、以下の自治体向けの情報セキュリティ関連のガイドラインを参考にしました。

A：地方公共団体における情報セキュリティ対策に関する調査研究報告書(H14.2)
http://www.soumu.go.jp/singi/security.pdf

B：情報セキュリティティポリシーに関するガイドライン(H14.11.28一部改定)
http://www.bits.go.jp/sisaku/2002_1128/ISP_Guideline_20021128.html

C：住民基本台帳ネットワークシステム及びそれに接続される既設ネットワークに関する調査表
http://www.soumu.go.jp/c-gyousei/daityo/021107_1.html

監査WGでは、これらのガイドラインを参考にしつつ、

検討メンバーの現場経験を通じた自治体の現状や個人情報に関する機密性の要求度合いを考慮して、管理基準について下記のようにチェックしました。

●判定基準の定義

記号	ガイドラインなどで求めている	JNSAとして必要と考えるか
○	求めている	必要
□	求めていない	必要
△	求めている	不要
×	求めていない	不要

目的	コントロール		サブコントロール	管理基準	JNSA提案
7.3 利用者の責任					
認可されていない利用者のアクセスを防止するため	1) 利用者は、パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うこと	○	11) すべての利用者に、利用者が複数のサービス又はプラットフォームにアクセスする必要があって、複数のパスワードを維持することが要求される場合、そのサービスが保管したパスワードを適切に保護しているときは、利用者は一つの質の良いパスワードを用いてもよいことを助言すること	7.3.1.11	□
	2) 無人運転の装置の利用者は無人運転の装置が適切な保護対策を備えていることを確実にすること	○	1) 無人運転の装置が利用者の作業領域に取り付けられている装置（例えば、ワークステーション、ファイルサーバ）は、長期間無人のまま放置される場合、認可されていないアクセスから特別な保護をすること	7.3.2.1	□
			2) 無人運転の装置の保護を実施する責任と同様に、その装置を保護するためのセキュリティ要求事項及び手順についても、すべての利用者及び請負業者に認識させること	7.3.2.2	□
			3) 無人運転の装置の利用者に、実行していた処理（session）が終わった時点で、接続を切るように助言すること	7.3.2.3	×
			4) 無人運転の装置の利用者に、処理（session）が終了したら、汎用大型コンピュータをログオフするように助言すること	7.3.2.4	×
			5) 無人運転の装置の利用者に、パーソナルコンピュータ又は端末装置は、使用していない場合、キーロック又は同等の管理策（例えば、パスワードアクセス）によって認可されていない使用からセキュリティを保つように保護するように助言すること	7.3.2.5	□
7.4 ネットワークのアクセス制御					
ネットワークを介したサービスの保護のため	1) 利用者には、ネットワークサービスへのセキュリティが確保されていない接続は、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること	○	1) ネットワーク及びネットワークサービスの使用に関し、個別方針を明確に設定すること	7.4.1.1	○
			2) ネットワークサービスの使用についての個別方針には、アクセスすることが許されるネットワーク及びネットワークサービスを対象にすること	7.4.1.2	○
			3) ネットワークサービスの使用についての個別方針には、誰がどのネットワーク及びネットワークサービスへのアクセスが許されるかを決めるための認可手順を対象にすること	7.4.1.3	□
			4) ネットワークサービスの使用についての個別方針は、ネットワーク接続及びネットワークサービスへのアクセスを保護するための管理策及び管理手順を対象にすること	7.4.1.4	□
			5) ネットワークサービスの使用についての個別方針には、業務上のアクセス制御方針と整合していること	7.4.1.5	□
ネットワークを介したサービスの保護のため	2) 利用者端末と利用者がアクセスすることを認可されているサービスとの間に、指定された経路以外の経路を、利用者が選択することを防止すること	○	1) 指定された経路以外の経路を、利用者が選択することを防止するために、通常、経路の異なる接続点において幾つかの制御を実施すること	7.4.2.1	○
			2) 指定された接続経路には、専用線又は専用電話番号を割り当てること	7.4.2.2	△
			3) 指定された接続経路では、指定された業務システム又はセキュリティゲートウェイのポートに自動接続すること	7.4.2.3	○

情報セキュリティ監査について

今回作成した電子自治体情報セキュリティ管理基準（JNSA案）は、情報セキュリティ管理基準の中で電子自治体において必要と考えられる監査項目の抽出のみをしており、管理基準の詳細項目（サブコントロール）の表現を自治体向けの表現に置き換えるなどはしておりません。従いまして、本管理基準案をご覧いただくにあたり、従業員_職員、経営陣_首長／幹部などと読み替えていただく必要があります。

今後に残された課題としては、

・自治体向けの表現に置き換える（特に個人情報の保護を重視した表現への置き換えや、コントロールの追加を検討する）
・インタビューや資料の確認だけでなく、技術的なチェックを加えるべき項目を洗い出す

さらには、

・実際に自治体の監査で使ってみる

等が必要と考えています。

特に、自治体の監査における試行を通じて、基準の読み替えや技術的チェック項目や方法の標準パターンを作っていくことが重要と考えます。

現在、JNSAのホームページにて、この「電子自治体情報セキュリティ管理基準（JNSA案）VER.0.8」についてパブリックコメントを募集し、また実際に本管理基準での監査にご協力いただける自治体を募集しています。ご協力いただける自治体の方、自治体をご紹介いただける方は、是非JNSA事務局までご連絡ください。

【参考サイト】

経済産業省　情報セキュリティ政策、署名認証のページ
http://www.meti.go.jp/policy/netsecurity/index.html
経済産業省　「情報セキュリティ監査企業台帳」申告についてのおしらせ
http://www.meti.go.jp/policy/netsecurity/audit_register.start.html
JNSAスキルマップWG「情報セキュリティプロフェッショナル育成に関する調査研究」
http://www.ipa.go.jp/security/fy14/reports/professional/ikusei-seika-press.html
JNSA監査WG　電子自治体情報セキュリティ管理基準（JNSA案）VER.0.8
http://www.jnsa.org/active7_030715.html