

情報セキュリティ監査研究会  
報告書

2003年3月26日

経済産業省

## はじめに

中央省庁や自治体における業務や行政サービスのコンピュータ化及びそれらに関連する情報の電子化が急ピッチで進められている。2002年8月には住民基本台帳ネットワークが稼動を開始し、さらに2003年度からは、電子政府/自治体システムの本格的な稼動の開始が予定されている。民間市場においても、企業同士あるいは企業と消費者との間での種々の取引や、企業活動に必要な資材の調達等の様々な分野において電子商取引の導入が進んでいる。また、一般家庭においても、高速なインターネットアクセス回線の普及に伴って、プライベートであるいは仕事でインターネットを利用する人の数は急激に増加している。

このように、中央省庁や自治体の業務やサービス、民間企業の活動の多くにおいてインターネット接続された情報システムが利用されるようになるとともに、一般家庭からのインターネットの利用も増加しており、社会活動と国民の生活が情報システムとインターネットに依存する割合が多くなってきている。

その一方で、情報システムや組織体におけるセキュリティ対策の不備に起因する様々な問題が生じている。すなわち、情報システムへの不正侵入や機密情報/個人情報の外部への漏洩、情報システムに保存されているデータの破壊、ホームページの改竄や情報システムのダウンといった情報セキュリティの事故である。このような事故は、国家や企業の機密情報の漏洩による経済的損害あるいは個人情報の漏洩による人権の侵害、さらにはサービスや企業活動の停止といった被害をもたらし、社会的な影響はより深刻なものとなっている。

こうした環境変化を受け、我が国における情報セキュリティに関する制度整備は着実に進んできている。ISO/IEC15408に基づくITセキュリティ評価認証スキームの創設、暗号技術の評価(CRYPTREC)、情報セキュリティマネジメントの認証制度(ISMS 適合性評価制度)の創設、インシデント情報共有・相談体制(JPCERT/CC、IPA等)の整備などが行われ、今後は、これをいかに利用して、我が国全体の情報セキュリティ確保のレベルを向上させるかという段階に入っているとも言える。また、政府自身についても、内閣を中心として、「情報セキュリティポリシーに関するガイドライン」の策定やその改訂、NIRT(緊急対応支援チーム)の創設などを行ってきているところである。

しかしながら、こうした中、独立かつ専門的知識を有する専門家に、自らの情報セキュリティ対策の有効性の評価を受ける、いわゆる「情報セキュリティ監査」の分野についての制度整備が遅れていることが喫緊の課題として浮上してきた。この「情報セキュリティ監査」は、特に、運用後の情報セキュリティ対策の継続的な向上のための手法として、極めて有効である。また、「情報セキュリティ監査」は、経営のガバナンスとの関連で議論されているリスクマネジメント体制の有効性、内部統制の有効性を確保するためにも必要不可欠なマネジメントプロセスの構成要素と言える。

このような認識を下に、経済産業省において、商務情報政策局長の諮問研究会として「情報セキュリティ監査研究会」を設置し、2002年9月より情報セキュリティ監査の普及と

そのあり方についての検討を行ってきたところである。本分野における民間の有識者に加え、監査を受ける主体となる政府の関係者にもオブザーバーとして参加をいただき、2003年3月まで、精力的に計7回の検討を重ねた。また、2003年1月29日から2月26日まで、報告書案について広く意見を募集し、それを踏まえて内容を修正した(参考資料参照)。

本研究会の成果は、主に以下の3点であると考えている。

- ①「情報セキュリティ監査」のあり方を提示したこと
- ②「情報セキュリティ監査」の標準的な基準と監査を行う主体のあり方の具体案を提示したこと
- ③電子政府の本格稼働に向け、電子政府に対する「情報セキュリティ監査」のあり方を示したこと

政府においては、本研究会の成果を受けて必要な制度整備を行うことを期待したい。また、この成果物が利用され、民間市場、政府関係機関等において、広く「情報セキュリティ監査」が実施されていくことを強く期待したい。

2003年3月  
情報セキュリティ監査研究会委員長  
土居 範久

## 情報セキュリティ監査研究会委員名簿

### (委員長)

土居 範久 慶應義塾大学工学部情報工学科教授

### (委員)

稲垣 隆一 弁護士(日本弁護士連合会コンピュータ研究会委員)  
歌代 和正 株式会社インターネットイニシアティブ技術本部部長  
大木 栄二郎 NPOネットワークリスクマネジメント協会幹事  
喜入 博 KPMGビジネスアシュアランス株式会社シニアアドバイザー  
小林 俊範 (社)電子情報技術産業協会情報セキュリティ監査検討WG主査  
下村 正洋 NPO日本ネットワークセキュリティ協会事務局長  
杉本 隆洋 (財)インターネット協会理事  
鳥居 壮行 駿河台大学文化情報学部教授  
中尾 康二 株式会社KDDI研究所コンピュータセキュリティグループリーダー  
永田 靖人 (社)日本情報システム・ユーザー協会セキュリティ部会長  
堀江 正之 日本大学商学部教授  
本田 実 システム監査学会常任理事  
松尾 明 特定非営利活動法人 IT コーディネータ協会理事  
丸山 満彦 監査法人トーマツ シニアマネジャー 公認会計士  
水野 義嗣 (社)情報サービス産業協会セキュリティ委員会ISMS研究部会長  
山口 英 奈良先端科学技術大学院大学情報科学研究科教授  
和貝 享介 特定非営利活動法人日本システム監査人協会副会長

### (オブザーバー)

内閣官房情報セキュリティ対策推進室  
総務省行政管理局行政情報システム企画課  
総務省自治行政局自治政策課  
情報処理振興事業協会セキュリティセンター  
(財)日本情報処理開発協会  
経済産業省大臣官房情報システム厚生課

### (事務局)

経済産業省商務情報政策局情報セキュリティ政策室

## 目次

<b>1</b>	<b>検討の背景と方向性の整理</b> .....	<b>1</b>
1.1	我が国の情報セキュリティ対策の現状と情報セキュリティ監査の意義.....	1
1.1.1	我が国の情報セキュリティ対策の現状 ～「情報セキュリティマネジメント」確立の必要性	1
1.1.2	情報セキュリティ監査の意義 .....	2
1.2	我が国における情報セキュリティ監査の実施状況と問題点 .....	3
1.2.1	情報セキュリティ監査の実施状況 .....	3
1.2.2	情報セキュリティ監査を巡る問題点 .....	4
1.3	情報セキュリティ監査の普及のために～本研究会の検討の方向性 I .....	5
1.4	電子政府における情報セキュリティ監査の実施～本研究会の検討の方向性 II .....	6
<b>2</b>	<b>情報セキュリティ監査の標準的な基準と主体のあり方を検討するにあたっての基本的な視点</b>	<b>7</b>
2.1	情報セキュリティ監査の対象～システムではなく情報資産 .....	7
2.2	情報資産に対するマネジメントを監査するという視点 .....	7
2.2.1	情報資産に対するリスクアセスメントから始まるマネジメントサイクル構築の思想 .....	7
2.2.2	ISMS適合性評価制度の認証取得組織体の増加 .....	8
2.3	多種多様な組織体の多種多様なニーズに応じた監査制度 .....	8
2.3.1	保証と助言 .....	8
2.3.1.1	保証型監査の要請 .....	8
2.3.1.2	助言型監査の要請 .....	9
2.3.1.3	保証と助言の両者の形態の容認 .....	9
2.3.1.4	助言型監査から保証型監査へ .....	11
2.3.2	多様な主体の多様な活動 .....	12
2.3.3	外部の者による監査の要請 .....	13
2.3.3.1	内部目的か外部目的か .....	13
2.3.3.2	外部の者による監査の要請 .....	13
2.4	インターネット社会における国際的整合性 .....	13
2.5	「情報セキュリティ監査」の定義 .....	14
<b>3</b>	<b>情報セキュリティ監査の標準的な基準の策定</b> .....	<b>15</b>
3.1	情報セキュリティ監査の標準的な基準の位置付け .....	15
3.2	管理基準と監査基準の区分 .....	15
3.3	「情報セキュリティ管理基準」策定の考え方 .....	16
3.3.1	基本～JIS X 5080:2002 をもとに策定 .....	16
3.3.2	JIS X 5080:2002 の細分化 .....	16
3.3.3	成熟度モデル .....	17
3.3.4	「情報セキュリティ管理基準」の位置付け .....	20
3.3.4.1	他の基準等との関係 .....	20
3.3.4.2	「参照元(レファレンス)」としての位置付けと個別管理基準策定ガイドライン .....	20

3.3.4.3	主体別・業種別管理基準の概念と「電子政府情報セキュリティ管理基準」	21
3.4	「情報セキュリティ監査基準」策定の考え方	22
3.4.1	「情報セキュリティ監査基準」の策定方針	22
3.4.2	実施基準ガイドラインの策定	22
3.4.3	報告基準ガイドラインの策定	23
3.4.4	主体別・業種別監査基準の概念と「電子政府情報セキュリティ監査基準」	23
3.5	電子政府への利用	24
3.6	全体像	24
<b>4</b>	<b>情報セキュリティ監査を行う主体のあり方</b>	<b>25</b>
4.1	「情報セキュリティ監査企業台帳」の創設	25
4.1.1	台帳の性質～任意登録制	25
4.1.2	台帳への登録内容(申告内容)	26
4.1.3	台帳への登録主体	26
4.1.4	台帳の公表	26
4.1.5	地域ごとの台帳	26
4.2	情報セキュリティ監査を行う主体の質の確保	27
4.2.1	監査従事者の質の確保	27
4.2.2	監査を行う主体となる企業の質の確保	28
4.3	電子政府監査を行う主体のあり方	28
4.3.1	外観上及び精神上的の独立性	28
4.3.2	高い専門性と倫理性	29
4.3.3	監査業務の再委託	29
<b>5</b>	<b>その他</b>	<b>30</b>
5.1	ISMS適合性評価制度との関係	30
5.1.1	様々なバリエーションがある監査と統一基準のISMS認証	30
5.1.2	ISMS認証取得の裾野を広げる「情報セキュリティ監査」	30
5.1.3	ISMS認証取得後の保証型監査	30
5.2	法的関係についての論点整理	31
5.2.1	監査を行う主体に関する法的関係	31
5.2.1.1	被監査主体に対する法的責任	31
5.2.1.2	監査結果を信頼した第三者に対する法的責任	32
5.2.2	被監査主体に関する法的関係	32
5.3	システム監査(基準)との関係	32
5.4	基準等のメンテナンスのあり方	33

別添資料1：情報セキュリティ管理基準 Ver1.0

別添資料2：個別管理基準（監査項目）策定ガイドライン Ver1.0

別添資料3：電子政府情報セキュリティ管理基準モデル（庁内ネットワークシステム）  
Ver1.0

別添資料4：情報セキュリティ監査基準 Ver1.0

別添資料 5 : 情報セキュリティ監査基準 実施基準ガイドライン Ver1.0

別添資料 6 : 情報セキュリティ監査基準 報告基準ガイドライン Ver1.0

別添資料 7 : 電子政府情報セキュリティ監査基準モデル Ver1.0

参考資料 : 「情報セキュリティ監査研究会報告書 中間とりまとめ」に対する意見募集  
の結果について

## 1 検討の背景と方向性の整理

まず冒頭に、本章において、情報セキュリティ監査についての検討を行う上での背景と、それを踏まえた本研究会における検討の方向性について整理する。

### 1.1 我が国の情報セキュリティ対策の現状と情報セキュリティ監査の意義

#### 1.1.1 我が国の情報セキュリティ対策の現状 ～「情報セキュリティマネジメント」確立の必要性

情報システムを構成するハードウェアやソフトウェアが年々複雑化すると共に、情報セキュリティに関連する状況は日々変化している。また、近年急速に進みつつあるブロードバンド回線の普及<sup>1</sup>や個人情報漏洩の頻発などにより、我が国の企業、政府、自治体等の情報セキュリティ対策の必要性についての認識度をより高めていると言える。

しかしながら、例えば、下記の調査結果(表1)に顕著に現れているように、自らは情報セキュリティ対策を行っていると考えている組織体においても、ウイルス対策やアクセス制御に関する製品やシステムを導入すること、またセキュリティポリシーを策定するといった個別対策で留まっている組織体が多く、状況の変化に応じて必要な対策を実施し続けている組織体が少ないのが現状である。

いうまでもなく、情報セキュリティ対策は、日々変化する脅威や技術に応じて不断に見直していくことが必要とされるものであり、こうした見直しを行うための「情報セキュリティマネジメント」が、我が国の各組織体に確立されていくことが強く求められる現状にある<sup>2</sup>と言える。なお、2002年8月に、我が国も参加して策定(改訂)された、OECD(経済協力開発機構)のガイドライン(「情報システム及びネットワークのセキュリティのためのガイドライン」)<sup>3</sup>においても、新たに「セキュリティマネジメントの原則」が盛り込まれているところである。

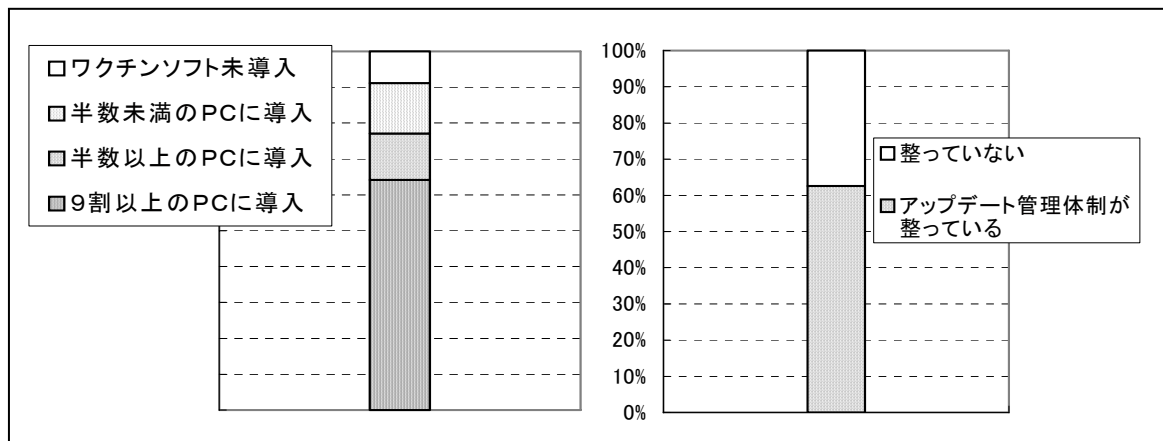
---

<sup>1</sup> 総務省「インターネット接続サービスの利用者数等の推移」  
([http://www.soumu.go.jp/s-news/2002/021227\\_1.html](http://www.soumu.go.jp/s-news/2002/021227_1.html))

<sup>2</sup> 情報セキュリティマネジメントについては、2002年4月より、「情報セキュリティ・マネジメント・システム(ISMS)適合性評価制度」(日本情報処理開発協会)が本格運用を開始し、2003年1月15日現在で、70社が認証を取得しているところである。

<sup>3</sup> OECD Guidelines for Security of Information Systems and Networks(英語と日本語の対訳につき、経済産業省ホームページ参照;<http://www.meti.go.jp/policy/netsecurity/>)

表1: ワクチンソフト導入・ウイルス対策の実施状況 (IPA 調べ)



(資料)国内におけるコンピュータウイルス被害状況調査報告書(平成13年度 IPA/ISEC)

### 1.1.2 情報セキュリティ監査の意義

「情報セキュリティマネジメント」の確立をはじめとした情報セキュリティ対策は、まず第一にその組織体自らが講じていくものであるが、自らの対策のみでは限界がある。こうした中、独立かつ専門的知識を持った者に対して当該組織体の情報セキュリティ対策の評価を依頼する組織体が出始めている。

この「情報セキュリティ監査」<sup>4</sup>は、当該組織体が現時点において適切な情報セキュリティ対策を講じているかどうかといった点に加え、環境変化に応じた対策が可能となっているかといった「情報セキュリティマネジメント」の確立の評価において有効な手法であり、上述したような我が国における情報セキュリティ対策の現状に鑑みると、その普及を促進すべきである。また、独立かつ専門的知識を持った者に、自らの情報セキュリティ対策について、監査を受けた上で「保証」してもらい、それを商取引等において利用したいとのニーズも存在する。

<sup>4</sup> 「情報セキュリティ監査」の正式な定義については後述する(2.5 参照)。

## 1.2 我が国における情報セキュリティ監査の実施状況と問題点

### 1.2.1 情報セキュリティ監査の実施状況

下に、情報セキュリティ監査の実施状況についての調査結果(表2<sup>5</sup>)を示す。ここに現れているように、我が国においては情報セキュリティ監査を実施している組織は未だ少ないのが現状である。

表2: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状況調査結果」)

<sup>5</sup> 総務省「情報セキュリティ対策の状況調査結果」(2002年9月13日発表、[http://www.soumu.go.jp/s-news/2002/020913\\_5.html](http://www.soumu.go.jp/s-news/2002/020913_5.html))

## 1.2.2 情報セキュリティ監査を巡る問題点

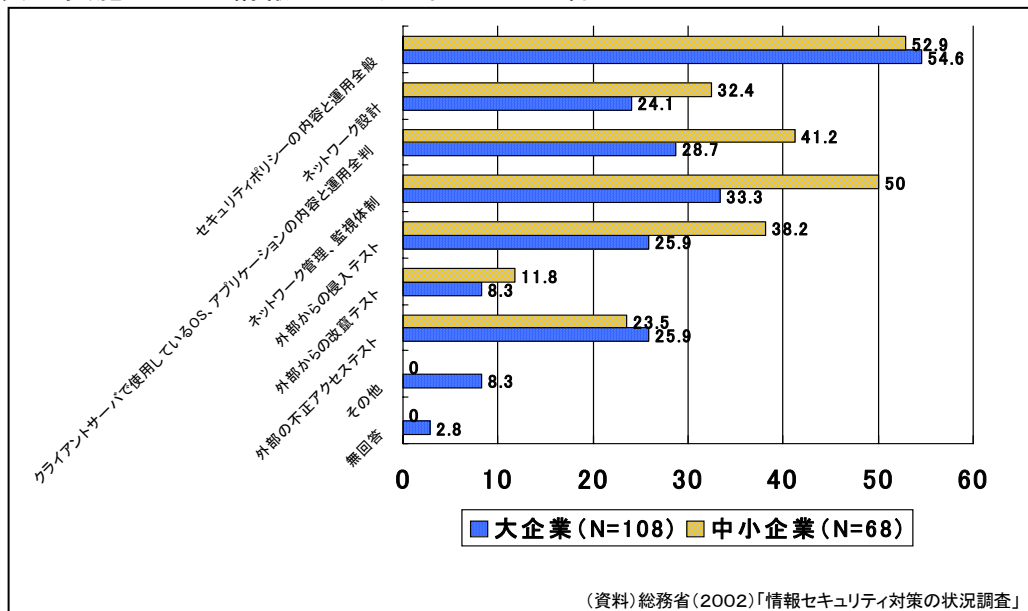
また、同調査において、①実施していると答えた組織体の実施内容(表3)、②実施していない理由(表4)についての調査が行われている。この調査結果に典型的に現れているように、情報セキュリティ監査については、

(1)監査を行う主体としては、監査の正当性を信じてもらえない(「情報セキュリティ監査」とは何かという指針がない)という点、

(2)監査を受ける主体(以下、「被監査主体」という)としては、ア)どのような効果があるか分からない(「情報セキュリティ監査」とは何か不明)、イ)誰に頼めばよいか分からない<sup>6</sup>といった点

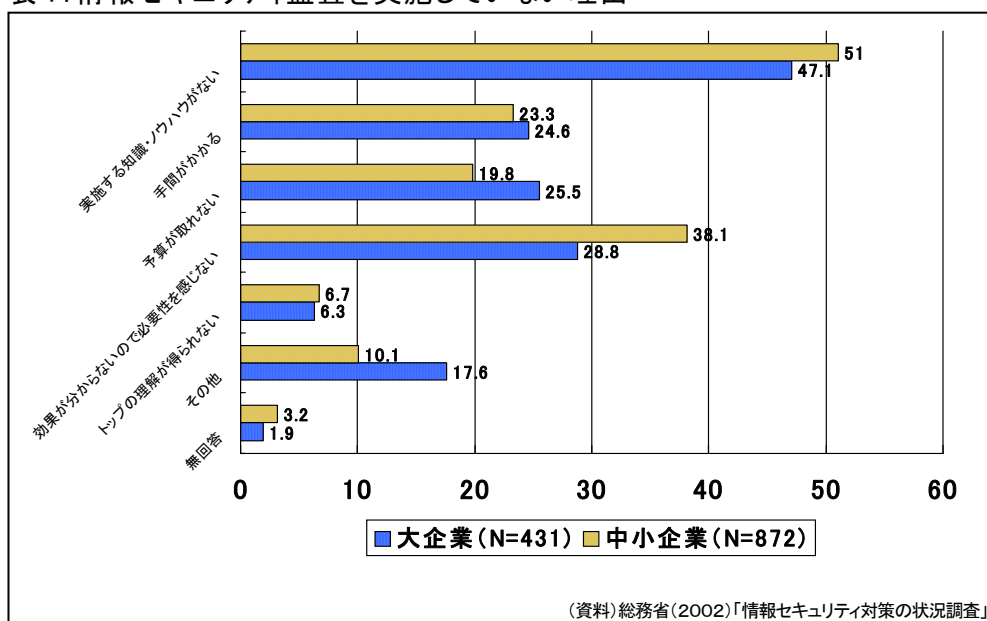
が、問題点として挙げられると言える。

表3:実施している情報セキュリティ監査の内容



<sup>6</sup> 現在、情報セキュリティ監査を行っている外部の監査主体には、監査法人、情報セキュリティ関連のシステム構築等を行うベンダー(情報セキュリティベンダー)、一般のシステム構築を行うベンダー、システムの監視サービス等を行っている情報セキュリティ専門企業、システム監査企業などがある。

表4: 情報セキュリティ監査を実施していない理由



### 1.3 情報セキュリティ監査の普及のために～本研究会の検討の方向性 I

こうした問題点を踏まえ、本研究会においては、情報セキュリティ監査の普及のためには、ユーザー(被監査主体)にとって利用しやすく、また、監査を行う主体にとっても監査を行いやすくなるよう、「情報セキュリティ監査」の標準的・一般的な形態を提示することが適当であると判断した。

具体的には、

- 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(第2章)、
- ②「情報セキュリティ監査」の標準的な基準を策定し(第3章)、
- 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(第4章)

こととした。

加えて、関連する論点として、「情報セキュリティマネジメントシステム(ISMS)適合性評価制度」(以下、「ISMS 適合性評価制度」という。)との関係、法的関係についての論点整理、システム監査(基準)との関係、ここで策定した基準等のメンテナンスのあり方について提示することとした(第5章)。

そして、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、我が国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するものである。

## 1.4 電子政府における情報セキュリティ監査の実施～本研究会の検討の方向性 II

政府における業務や行政サービスの IT 化及びそれらに関連する情報の電子化が急速に進められている。さらに、2003年度からの電子政府の本格稼働が予定されており、個人情報や企業情報等の保護や国家安全保障の観点からも、政府における情報セキュリティ対策の重要性は言を待たない。

こうした中、政府における「情報セキュリティ監査」実施の必要性も声高に指摘され、一部実施に移されているところ<sup>7</sup>である一方で、現在のところ、いかなる「情報セキュリティ監査」を行うべきかを示した指針は出されていない。

したがって、本研究会の成果が、政府において指針として利用されることを想定した検討も行い、2003年度以降の利用に耐えうる必要な基盤を用意することも、あわせて本研究会の目標としたところである。

---

<sup>7</sup> 「電子政府の情報セキュリティ確保のためのアクションプラン(2001年10月10日 情報セキュリティ対策推進会議決定)」においては、「内閣官房は2002年夏を目処に…セキュリティ監査等につき実施手法の模範例(ベストプラクティス)を提示する」とされている。また、「住民基本台帳ネットワークシステムの稼働について」(2002年7月29日 総務省報道発表資料)においては、「住民基本台帳ネットワークシステムを稼働するに当たり、以下の措置を新たに講ずることとする。……3. 外部監査によるシステム運営監査 全地方公共団体を対象に監査法人等による外部監査を実施する(稼働後できるだけ早期に、全団体に対して、運営面でのチェックリストを配布し、その回答状況を点検するとともに、監査法人等により個別に監査を行う方法を検討)」とされている。

## 2 情報セキュリティ監査の標準的な基準と主体のあり方を検討するにあたっての基本的な視点

本章では、本研究会において、我が国において「情報セキュリティ監査」を考える上での基本的な視点、すなわち、第3章及び第4章において示すこととなる、「情報セキュリティ監査」の標準的な基準と監査を行う主体のあり方を検討するにあたっての基本的な視点を整理する。

### 2.1 情報セキュリティ監査の対象～システムではなく情報資産

「情報セキュリティ監査」は、「情報技術」(IT)に関連するいわゆる情報システムのセキュリティだけではなく、より広く「情報資産」(information assets)全体のセキュリティの確保を目的とすることが適当である。

### 2.2 情報資産に対するマネジメントを監査するという視点

「情報セキュリティ監査」においては、その時点における「情報セキュリティの強度」そのものではなく、当該組織体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判断するものであるという点が重要である。情報セキュリティの確保を脅かすリスクは多様化かつ複雑化し、さらには日々変化していくものだからである。

#### 2.2.1 情報資産に対するリスクアセスメントから始まるマネジメントサイクル構築の思想

情報資産に対するリスクのマネジメントを効果的に実施するにあたっては、情報資産に対するリスクアセスメントを行い、それにしたがって適切なコントロール<sup>8</sup>を割り当てることが出発点となる<sup>9</sup>。

したがって、「情報セキュリティ監査」においても、監査を行う主体は、当該組織体において情報資産に対するリスクアセスメント自体がそもそも行われているかどうかを判断することが重要である。さらに、当該組織体がリスクアセスメントを行っていた場合であっても、そのリスクアセスメントの内容が適切なものであるかを判断するため、監査を行う主体としても、当該組織体に対するリスクアセスメントを実施し、監査を行うことが望まれる。

<sup>8</sup> 「コントロール」とは、最も広義には、ある特定の目的を達成するために、何らかの影響力を行使することを意味するが、ここでは情報セキュリティを確保するための具体的な対策を指す言葉として用いている。したがって、マネジメントサイクルに組み込まれた個々の情報セキュリティ対策をいう。

<sup>9</sup> 2002年8月に策定(改訂)されたOECDのガイドライン(「情報システム及びネットワークのセキュリティのためのガイドライン」)においても、「リスクアセスメントの原則」が、8原則のうちの1つとして盛り込まれている。(英語と日本語の対訳につき経済産業省ホームページ参照; <http://www.meti.go.jp/policy/netsecurity/>)

## 2.2.2 ISMS適合性評価制度の認証取得組織体の増加<sup>10</sup>

情報資産に対するリスクのマネジメントについては、2002年4月からISMS適合性評価制度の本格運用が開始され<sup>11</sup>、マネジメント体制が構築されている組織体に対して認証を与える制度が、(財)日本情報処理開発協会により運用されている<sup>12</sup>。

上に述べたように「情報セキュリティ監査」が情報資産に対するリスクのマネジメントを効果的に行うことを促す制度であることに鑑みると、「情報セキュリティ監査」の普及により、ISMS 適合性評価制度による認証取得組織体の裾野を広げ、結果として認証取得組織体も増加していくという相乗効果を生むものと期待される。

## 2.3 多種多様な組織体の多種多様なニーズに応じた監査制度

「情報セキュリティ監査」を実施すべき組織体は、民間分野においては大企業から中小企業まで、また政府関係分野においては、中央省庁から都道府県、市町村まで、その人員規模、情報システムの態様、拠出可能な予算の規模など様々である。また、被監査主体のニーズも、自らの情報セキュリティ対策の不備の指摘を目的としているものから、商取引の相手方等との関係から情報セキュリティ対策の有効性についていわゆる「お墨付き」を得たいというものなど、一様ではない。

こうした被監査主体のニーズに応じ、監査を行う主体と監査内容を柔軟に選択できるようにし、一過性のものではなく継続的に監査を導入する環境を整備していくことが適当である。

### 2.3.1 保証と助言

#### 2.3.1.1 保証型監査の要請

「情報セキュリティ監査」を受けるニーズとしては、まず、第三者－民間企業であれば取引先や顧客、政府関係機関においては国民等－に対して、自らの情報セキュリティ対策についての「お墨付き」を得ることを目的とすることが考えられる。例えば、EC サイトを運営する企業が、加盟店に対して自らの情報セキュリティ対策が安全であることを提示したい場合などが典型的な事例である。このように、監査の対象となる組織体の情報セキュリティに関するマネジメントや、マネジメントにおけるコントロールが監査手続を実施した限りにおいて適切である旨(又は不適切である旨)を伝達する監査の形態を、「保証型監査」と呼ぶ。

なお、この場合、「保証」といっても、結果としてインシデントが発生しないという絶対的な保証ではなく、一定の判断の尺度に従って監査手続を行った範囲における合理的な保証となることに留意が必要である。

<sup>10</sup> 情報セキュリティ監査とISMS適合性評価制度との関係については、5. 1参照。

<sup>11</sup> ISMS適合性評価制度は、2001年4月からパイロットプロジェクトとして情報処理サービス業を対象として開始され、2002年4月から全業種に対象範囲が拡大されて運用されている。

<sup>12</sup> 同様の制度として、BSI(英国規格協会)によるBS7799-2に基づく審査登録制度がある。

### 2.3.1.2 助言型監査の要請

一方で、マルかバツの評価だけではなく、ある尺度に照らしたときに、それとの乖離(ギャップ)を指摘したり、改善の方向性を示してもらうことも、「情報セキュリティ監査」に求められる重要なニーズである<sup>13</sup>。現在我が国で行われている多くの「情報セキュリティ監査」がこの方式で行われており、また国際的に見ても「情報セキュリティ監査」の一形態として、この方式が主流で行われているのが現状である。このように、監査の対象となる組織体の情報セキュリティに関するマネジメントや、マネジメントにおけるコントロールの改善を目的として、監査対象の情報セキュリティ上の問題点を検出し、必要に応じて当該検出事項に対応した改善提言を行う監査の形態を、「助言型監査」と呼ぶ。

この際、監査の主体が組織体の外部者である場合、マネジメント体制構築や情報システム構築といったコンサルティング業務との違いは明確化しておく必要がある。すなわち、監査はあくまで独立した者による客観的な評価業務であり、特定の製品やサービスを販売・斡旋することに関与してはならない。例えば、継続的に監査を行う場合に、前回の助言型監査の際に導入を提言した特定の製品やサービスが組み込まれている場合に、その点について独立した観点から評価を行うことが困難になるケースが想定されるからである。したがって、①客観的に提示した一定の尺度<sup>14</sup>との乖離(ギャップ)を指摘した後で(検出)、②それを改善するための方向性(改善提言)を示すことにとどめることが適切である。

### 2.3.1.3 保証と助言の両者の形態の容認

以上より、多種多様な被監査主体の多種多様なニーズに応じた「情報セキュリティ監査」が行われる市場とするためには、当面、保証型監査と助言型監査を自由に選択できる制度とすることが適当である。

加えて、一部分の保証、保証と助言の混合型といった形態も認められるべきである。ただし、一部分の保証—例えば、外部委託の項目のみの保証—を行うような際には、監査の対象として選択されなかった他の項目と有機的に結びついてはじめて有効に機能することも多い点に、十分に留意が必要である。

なお、保証型監査、助言型監査両者において、監査である以上、監査を行う主体は独立性を確保することが必要であるが、昨今、会計監査において問題とされている<sup>15</sup>ように、特に保証型監査においては、厳格な独立性が要求されることに

<sup>13</sup> 現在行われている「システム監査」においては、ここでいう助言型監査の形態が基本である。「システム監査基準」(昭和60年通商産業省策定)においても、情報システムの有効性、安全性等を保証し、保証に係る監査意見を表明するという概念はない。「システム監査基準」において、システム監査とは「監査対象から独立かつ客観的立場のシステム監査人が情報システムを総合的に点検及び評価し、組織体の長に助言及び勧告するとともにフォローアップする一連の活動」と定義されている。

<sup>14</sup> 第3章で提示する、「情報セキュリティ管理基準」をもとに策定される個別組織体の管理基準がそれに当たる。

<sup>15</sup> 米国で発生したエンロン、ワールドコム不正経理事件等を契機に、会計監査とコンサルティング業務の分

留意する必要がある。したがって、「情報セキュリティ監査」においても、保証型監査の独立性<sup>16</sup>の厳格性について、今後検討が要求されることも視野に入れておく必要がある。

また、保証をするにも助言をするにも、監査を行う上での判断の尺度が明示されていることが必要であり、我が国において標準的に用いられるべき尺度について、第3章で提示する<sup>17</sup>こととなる。

---

離についての規制等の導入が検討され、実際に行われている。

<sup>16</sup> 第3章で示す「情報セキュリティ監査基準」は、保証型監査、助言型監査に共通に求められる規範として、監査を行う主体に対して「外観上」及び「精神上」の独立性を要求している。

<sup>17</sup> 第3章で示す「情報セキュリティ管理基準」がそれに当たる。

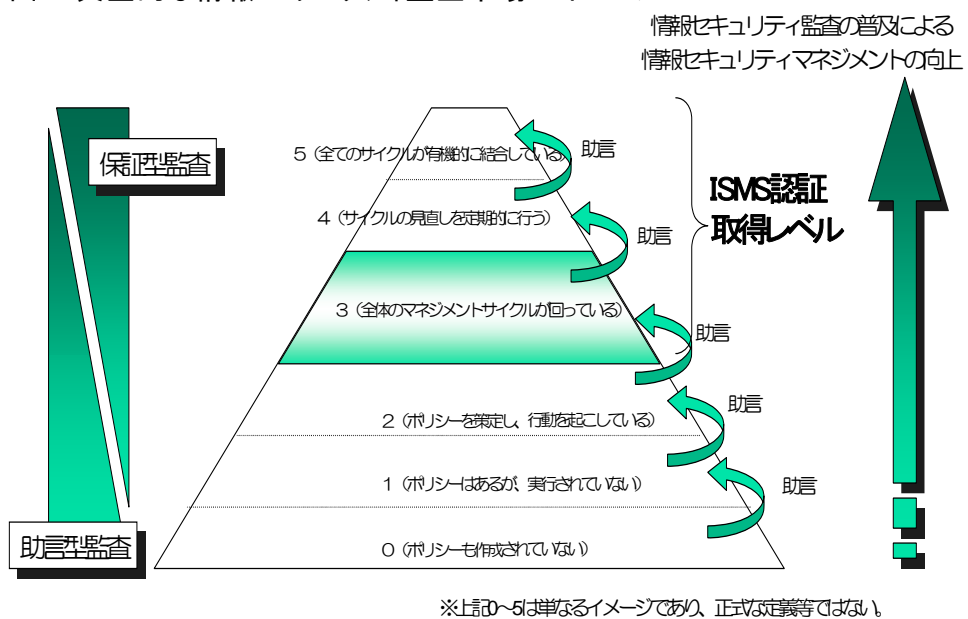
### 2.3.1.4 助言型監査から保証型監査へ

我が国の各組織体における情報セキュリティ対策の現状に鑑みると、当初は、助言型監査が主流となってくると考えられる。監査の際の判断の尺度として提示されるものはベストプラクティスとして示されるものとなる<sup>18</sup>ため、保証をしようとしても、このベストプラクティスに照らせば、「できていない」ことを保証することとなる可能性も否定できない。「できていない」ことの保証を受けることは現実的ではなく、そのようなニーズは極めて少ないと考えられるからである。また、たとえ保証できたとしても、対象範囲を限定した一部分の保証にならざるを得ないと考えられるからである。

したがって、各組織体に対する監査のあり方としても、まずは、助言型監査によって徐々にそのレベルを向上させ、また必要に応じて一部分の保証を加えながら、ある段階に来たときに保証型監査を行うといった利用のされ方になるものと想定される。また、市場全体を考えれば、当面は助言型監査中心の市場が形成され、我が国における組織体の情報セキュリティのレベルが向上してきた段階で、保証型監査中心の市場へ移行していくものと想定される。そして、保証型監査中心の市場となれば、会計監査の市場がそうであるように、監査とコンサルティング業務との役割分担が明確となり、「情報セキュリティ監査」の定義自体を変更する必要性も出てくることが考えられる。

以上をまとめると、当面想定される情報セキュリティ監査の市場のイメージは、以下の図(図1)のようになるものと考えられる。

図1:典型的な情報セキュリティ監査市場のイメージ



<sup>18</sup> 第3章で示す「情報セキュリティ管理基準」参照。

### 2.3.2 多様な主体の多様な活動

「情報セキュリティ監査」を行う主体は多様であることを前提として捉えることが望ましい。この市場は、我が国においては未だ創成期の市場であり、多様な主体が多様な活動を通してサービスの質を向上させる段階にあり、また、上に述べたように助言型・保証型など、被監査主体の多種多様なニーズに応じるためには、監査を行う主体もその特性に応じてサービスを行うべきだからである。

実際、現在「情報セキュリティ監査」のサービスを行っている監査を行う外部の主体には、監査法人、情報セキュリティ関連のシステム構築等を行うベンダー（情報セキュリティベンダー）、一般のシステム構築を行うベンダー、システムの監視サービス等を行っている情報セキュリティ専門企業、システム監査企業など様々である。これらの主体が、それぞれの得意分野を活かしながら、競争を行い、専門性を高めていく市場であることを期待したい。

また、組織体における内部監査部門等が経営管理の要請によって実施する「情報セキュリティ監査」も有用な監査の在り方として位置づけられることから、かかる監査態勢を整備強化し、早急に普及定着させることも重要である。組織体の内部監査人による「情報セキュリティ監査」と、組織体の外部主体による「情報セキュリティ監査」との二層構造に基づく監査形態、あるいは両者の共同監査という監査形態もあり得ないわけではない。

しかしながら、それぞれの主体が何の規律もない中でサービスを行っているのは、ユーザー（被監査主体）側の混乱を招き、結果として市場が適正に発展しないこととなる。第3章及び第4章で提示する「情報セキュリティ監査」に関する標準的な基準と監査を行う主体のあり方についての制度が、これらの主体が従うべき一定の規律となる。

### 2.3.3 外部の者による監査の要請

#### 2.3.3.1 内部目的か外部目的か

「情報セキュリティ監査」を実施する(受ける)目的には、①経営者等が経営判断に利用する場合(内部目的)と、②経営者等が外部の利害関係者に対して当該監査結果を示すことに利用する場合(外部目的)の両者があり得る<sup>19</sup>。助言型監査は主に内部目的に利用され、保証型監査は主に外部目的に利用されることとなる。

#### 2.3.3.2 外部の者による監査の要請

一般に、外部目的のための監査は外部の者によって行われることが原則となるが、内部目的のための監査を行う主体は、外部の者であっても内部の者<sup>20</sup>であってもよく、原則として被監査主体の選択に委ねられることとなる。

しかしながら、政府・自治体といった公共性の高い被監査主体においては、国民の権利等を守るという目的が付加されることから、たとえ内部目的の監査であっても、外部の主体による監査を受けることが望ましい。

また、民間企業に対する「情報セキュリティ監査」においても、事例の蓄積や保険ビジネスの発展により、監査を受けることが訴訟リスクをはじめとするリスク分担に繋がること<sup>21</sup>等が共通認識となれば、外部の主体による監査を受ける企業が増加することが見込まれる。

したがって、本研究会としては、外部の者による「情報セキュリティ監査」の有効性を認識し、この外部の者による監査の市場を育成しつつ、内部主体による「情報セキュリティ監査」との有機的な連携を図り、もって我が国における「情報セキュリティ監査」を普及定着させることが肝要であるとの認識を基本的なスタンスとした。

## 2.4 インターネット社会における国際的整合性

世界的にインターネットの利用が広がり、企業においても国際取引が、政府においても他国との交渉がインターネットを経由して行われるようになってきている。こうした中、「情報セキュリティ監査」についても、我が国の独自性は認識しつつも、国際的に整合性のとれた制度として設計され、我が国において行われた監査の結果が、広く国際的に認知されるものであるべきとの視点が重要である。

<sup>19</sup> 公認会計士又は監査法人による企業等の財務諸表の監査は、投資家等の外部利害関係者保護を目的とした監査であり、外部目的監査である。

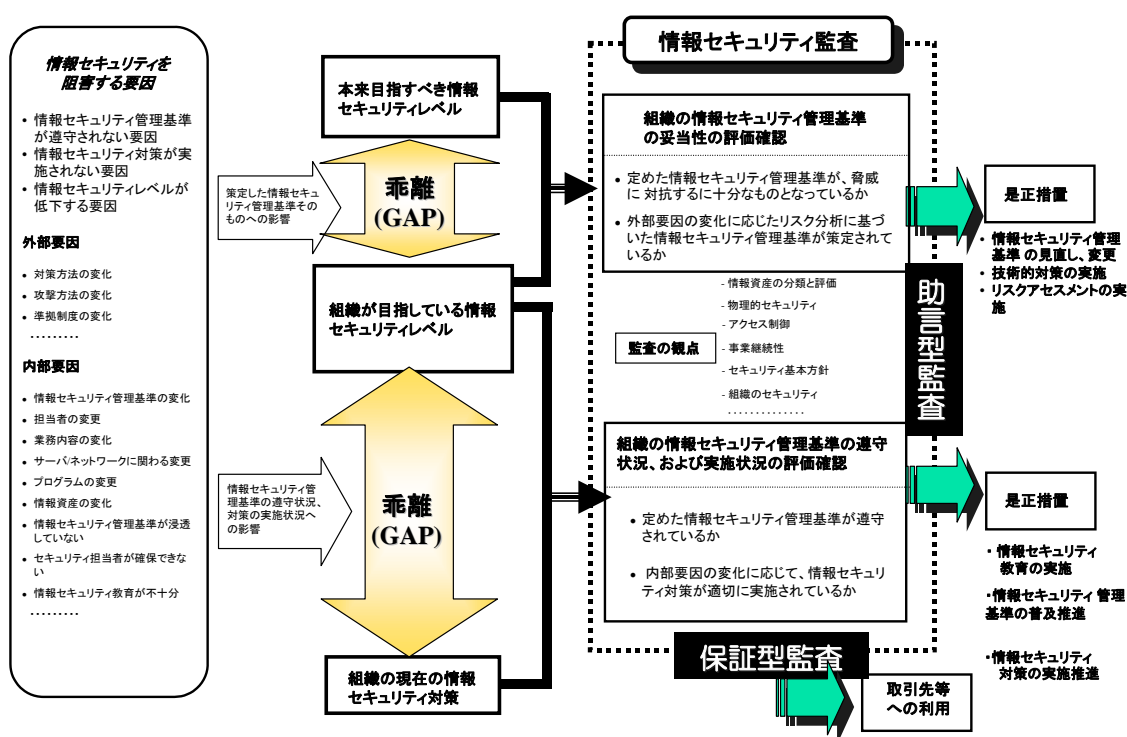
<sup>20</sup> 例えば、企業等においては、監査部、検査部、考査部等に所属する監査専属の従業員がこれに該当する。また、広い意味では、監査役会又は監査委員会もこれに該当する。

<sup>21</sup> 監査を受けることによる法的責任論については、5.2 参照。

## 2.5 「情報セキュリティ監査」の定義

以上より、本研究会において「情報セキュリティ監査」の外縁は、「情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査を行う主体<sup>22</sup>が独立かつ専門的な立場から、国際的にも整合性のとれた基準に従って検証又は評価し、もって保証を与えあるいは助言を行う活動」と定義できる。全体の位置付けを概略で示すと、以下の図(図2)となる。

図2: 情報セキュリティ監査の位置付け



<sup>22</sup> 本報告書においては、「監査を行う主体」と記載するが、基準等においては「情報セキュリティ監査人」との用語を用いることとする。

### 3 情報セキュリティ監査の標準的な基準の策定

前章に示した基本的視点に基づき、本章では、「情報セキュリティ監査」の標準的な基準の策定についての考え方とその具体案を示すこととする。

#### 3.1 情報セキュリティ監査の標準的な基準の位置付け

『情報セキュリティ監査』の標準的な基準は、多様な主体が監査を行い、多様な主体がそれぞれのニーズに応じて監査を受けるにあたり、一定の規律を付与する性格のものである。そして、これを利用する主体は、政府機関、民間企業問わず、我が国のあらゆる組織体が想定される。また、内部目的、外部目的を問わず利用されるものとするべきである。

こうして、我が国で広く一定の規律として利用されるものであるから、この基準は、政府の告示等において公的な位置付けが与えられることが望ましい。

一方で、「情報セキュリティ監査」は、現時点では、法定の義務付け監査に位置付けられるものではなく、この基準に準拠して監査を行うかどうかについては任意である。今後、情報セキュリティ監査が、経済社会上の要請を受け、例えば公共性の高い組織体に対して義務づけされるような状況となれば、この基準に準拠して行うことが統一的に求められることも想定される。

#### 3.2 管理基準と監査基準の区分

情報セキュリティ対策は、まず各組織体の自己責任において行われることが必要である。したがって、①各組織体が自らの管理基準等(情報セキュリティ基本方針<sup>23</sup>を含む)を規定する場合の拠り所となり、同時に、②「情報セキュリティ監査」の際には判断の尺度<sup>24</sup>を定めることが有益である。この判断の尺度を、「情報セキュリティ管理基準」と呼ぶこととする。

また、監査の際の判断の尺度とは別に、監査の際に監査を行う主体が従うべき行為規範を定めることが有益である。この行為規範を「情報セキュリティ監査基準」と呼ぶこととする。

あえて、一括りに「情報セキュリティ監査基準」とせず、「情報セキュリティ管理基準」と「情報セキュリティ監査基準」の2つの基準をあわせて、「情報セキュリティ監査の標準的な基準」と呼んでいるのは、両者の違いを明確にするためである<sup>25</sup>。

<sup>23</sup> 「情報セキュリティ基本方針」は、「情報セキュリティ管理基準」(別添資料1)上の用語。「情報セキュリティポリシー」という用語は、組織のトップポリシーを指して使われる場合や、より詳細な規定も含んだものを指して使われる場合など様々であり、ここでは用いない。

<sup>24</sup> 判断の尺度となるものは「規準」(クライテリア)と表記する場合もあるが、「基準」は「規準」を包含する概念であると考え、ここでは「基準」と呼ぶこととする。

<sup>25</sup> 現行「システム監査基準」(昭和60年経済産業省策定)においては、監査の際の判断の尺度と監査人の行為規範が混在しているとの指摘がある。

### 3.3 「情報セキュリティ管理基準」策定の考え方

#### 3.3.1 基本～JIS X 5080:2002 をもとに策定

前章で示したように、「情報セキュリティ監査」は、①「情報システム」ではなく「情報資産」<sup>26</sup>を対象とし、②リスクのマネジメントが有効に行われているかどうかという点を評価することが重要な視点である。また、基準の策定に当たっては国際的な整合性も図られていなければならない。

この観点から、「情報セキュリティ監査」にあたっての判断の尺度となる「情報セキュリティ管理基準」は、JIS X 5080:2002(情報技術－情報セキュリティマネジメントの実践のための規範)<sup>27</sup>をもとに策定することが適当である。

なお、JIS X 5080:2002 のもととなっている ISO/IEC17799:2000 (Information technology－Code of practice for information security management) は、現在見直しのプロセスに入っているが、修正が加えられ JIS にも反映されれば、同時に本管理基準も見直されることが必要となる。

また、ISMS適合性評価制度の認証基準も、JIS X 5080:2002 を参照して策定されていることから、「情報セキュリティ監査」とISMS適合性評価制度の判断の尺度は、整合性が図られる<sup>28</sup>こととなる。

#### 3.3.2 JIS X 5080:2002 の細分化

「情報セキュリティ管理基準」をJIS X 5080:2002 をもとに策定するとした場合、「情報セキュリティ監査にあたってJIS X 5080:2002 を参照する(JIS X 5080:2002 をそのまま基準化する)」との位置付けをするだけでは、1)管理策(コントロール)<sup>29</sup>が複数化している場合、2)管理策(コントロール)の曖昧度が高い場合があり、監査に利用しにくい。したがって、監査を行う主体にとっても被監査主体にとっても利用しやすいものにするために、この管理策(コントロール)を可能な限り細分化することが有益である。

細分化にあたっては、以下のように体系化することが適当である。

- 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

<sup>26</sup> 現行「システム監査基準」(昭和60年経済産業省策定)は、「情報資産」ではなく「情報システム」を対象としている。

<sup>27</sup> JIS X 5080:2002 は、国際規格であるISO/IEC17799:2000 を国内規格化したものである。

<sup>28</sup> 情報セキュリティ監査とISMS適合性評価制度との関係については、5.1 参照。

<sup>29</sup> JIS X 5080:2002 は、「セキュリティ領域(security domain)－目的(security objective)－管理策(controls)－管理策のガイダンス」という階層構造になっている。

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。

### 3.3.3 成熟度モデル

JIS X 5080:2002をもとに策定する「情報セキュリティ管理基準」は、その性質上、全てのコントロールとその体系性がベストプラクティスを示したものとなる。したがって、我が国の現状に鑑みると、そのベストプラクティスの水準のみを判断の尺度とすると、保証型監査においては肯定型の保証が困難となり、また助言型監査においては指摘する乖離(ギャップ)が大きくなりすぎるという問題点がある。

ここで、「情報セキュリティ監査」の際の判断の尺度を、例えば、①コントロールを整備していない、②コントロールを整備している、③コントロールを運用している、④継続的に改善されているといったように、段階に区切り、達成度に応じて組織体を評価するという考え方があり得る。この達成度を示す指標(成熟度モデル)につき、本研究会において一つのモデルを示し、「情報セキュリティ管理基準」の中に盛り込むことも検討したが、どのような成熟度モデルが適切かどうかの実績が少ない中で、現時点で一つのモデルを示すことは適当でないという結論に達したところである。したがって、成熟度モデルを利用して監査を行う場合は、当面は、監査を行う主体の判断によって、そのモデルを選択していくこととなる。

なお、現在国際的にも認知されている成熟度モデルとして、NIST<sup>30</sup>、COBIT<sup>31</sup>、SSE-CMM<sup>32</sup>のモデルがあり、以下(表5)に参考までにその内容を示す。

表5: 成熟度モデルの例

**○Security Self-Assessment Guide For IT Systems(NIST)のITセキュリティアセスメントフレーム**

**ワークのモデル**

Level 1; Control objective documented in a security policy.

コントロール目標がセキュリティポリシーに文書化されている。

Level 2; Security controls documented as procedures.

セキュリティコントロールは手続として文書化されている。

Level 3; Procedures have been implemented.

手続は導入されている。

Level 4; Procedures and security controls are tested and reviewed.

手続とセキュリティコントロールはテストされ見直されている。

Level 5 ; Procedures and security controls are fully integrated into a comprehensive program.

手続とセキュリティコントロールは包括的なプログラムに完全に統合されている。

<sup>30</sup> NIST "SP 800-26 Security Self-Assessment Guide for Information Technology Systems", November 2001 (<http://csrc.nist.gov/publications/nistpubs/index.html>)

<sup>31</sup> ISACA "Cobit Ver3" (<http://www.isaca.org/cobit.htm>)

<sup>32</sup> 情報処理振興事業協会仮訳「セキュリティ評価・認証 SSE-CMM関係」(平成13年度、<http://www.ipa.go.jp/security/ccj/download.htm#SSECMM>)

## ○Cobit Ver.3 の成熟度モデル

### 0 Non-Existent (存在しない)

実施すべき手順が完全に欠落している。組織は対応すべき問題が存在しているにも関わらず、そのための手順を導入していない。

### 1 Initial (初歩的)

問題が存在し、対応する必要があると組織が認識していることを裏付ける証拠は存在する。しかし、標準化された手順は存在せず、個人ごと、あるいはケースバイケースによる思いつきによる手順が実施されている。

### 2 Repeatable (繰り返し可能)

この段階では、手順が確立され、同じ業務を持つ異なる担当者が良く似た手順を実施している。しかし、標準的な手順についての訓練や伝達は存在せず、個人が責任を負うという状況である。個人の知識に依存している程度が高く、過ちが発生しがちである。

### 3 Defined (定義されている)

プロセスは標準化され、文書化され、訓練により伝達されている。しかし、このようなプロセスは個人に依存しており、逸脱が存在する可能性がある。プロセスは、洗練されていないが、実際に行われている規範として公式化されている。

### 4 Managed (管理されている)

プロセスに対する遵守状況のモニターと測定が可能で、プロセスが有効に機能していない場合には修正が行われる。プロセスは継続的に改善されており、良い実践規範が提供されている。しかし、自動化の程度とツールの利用は限定的であり、統合されずに利用されている。

### 5 Optimised (最適化)

継続的な改善と他の組織の成熟度との比較の結果により、プロセスは最良の実践規範のレベルとなっている。IT は業務フローを自動化するための統合化された方法として利用され、品質と有効性を改善するためのツールとなっており、組織は IT により適時に(環境変化に)対応することができる。

## ○OSSE-CMM 2.0(ISO/IEC 21827)の成熟度モデル

### Level 1、“Performed Informally、”(非公式に実施されたレベル)

プロセスエリアの基本プラクティスはだいたいにおいて実施されている。これらの基本プラクティスの実施は厳密に計画されたり追跡されたりしていない。実施は個人の知識と努力に依存する。プロセスエリアの作業生産物が実施の証拠となる。組織の中の諸個人は活動を認識しており、要求に応じてこの活動が実際されるという点で意見が一致している。プロセスエリアには、それとわかる作業生産物が存在する。

### Level 2、“Planned and Tracked、”(計画され追跡されたレベル)

プロセスエリアの基本プラクティスの実施は、計画され追跡されている。特定の手順に従った実施が検証されている。作業生産物は特定の標準と要求事項に適合している。測定がプロセスエリアの実施状況の追跡に使用される。このようにして組織は実際の実施状況に基づいて活動を管理することができる。「能力レベル1 非公式に実施されたレベル」との主な違いはプロセスの実施が計画され、管理されているということである。

**Level 3、“Well Defined、”（明確に定義されたレベル）**

基本プラクティスは、標準化され文書化されたプロセスを修正しまた承認したものを使用した、明確に定義されたプロセスに従って実施される。「能力レベル2 計画され追跡されたレベル」との主な違いは、プロセスは組織全体の標準プロセスを使用して、計画され管理されているということである。

**Level 4、“Quantitatively Controlled、”（定量管理されたレベル）**

詳細なプロセス実施の測定値が収集され、分析される。これは、プロセス能力の定量的な把握と、プロセス実施の予測能力の改善とを可能にする。プロセス実施は客観的に管理され、作業生産物の品質は定量的に把握される。「能力レベル3 明確に定義されたレベル」との主な違いは、定義されたプロセスは定量的に把握され、制御されているということである。

**Level 5、“Continuously Improving、”（継続的に改善しているレベル）**

プロセスの有効性と効率に対する定量的な実施目標（対象）が設定される。これらは組織のビジネスゴールに基づいている。これらの目標に対する継続的なプロセス改善は、定義されたプロセスの実施と、革新的なアイデアと技術の実行からの定量的フィードバックによって可能にされる。「能力レベル4 定量管理されたレベル」との主な違いは、定義されたプロセス及び標準プロセスが、これらのプロセスに対する変更の影響の定量的把握に基づいた継続的な改良及び改善を受けるということである。

※上記3つの基準の邦訳は経済産業省仮訳である。

### 3.3.4 「情報セキュリティ管理基準」の位置付け

以上の考え方にに基づき策定される「情報セキュリティ管理基準」(別添資料1)は、「情報セキュリティ監査」を行う際に原則として用いられるべき判断の尺度となる。その際、以下の点に留意することが必要である。

#### 3.3.4.1 他の基準等との関係

「情報セキュリティ監査」においては、本管理基準を監査上の判断の尺度として用いることを原則とするが、監査の要請または目的によって、本管理基準以外の適切な尺度を追加して用いることもできる。例えば、国内基準であれば、経済産業省の「システム監査基準」<sup>33</sup>、「情報システム安全対策基準」<sup>34</sup>、「コンピュータウイルス対策基準」<sup>35</sup>、「コンピュータ不正アクセス対策基準」<sup>36</sup>、総務省の「情報通信ネットワーク安全・信頼性基準」<sup>37</sup>、警察庁の「情報システム安全対策指針」<sup>38</sup>などがある。

今後、情報セキュリティ監査の実績が蓄積された段階で、これらの基準の内容を「情報セキュリティ管理基準」に反映していくことも検討すべきである。

#### 3.3.4.2 「参照元(レファレンス)」としての位置付けと個別管理基準策定ガイドライン

「情報セキュリティ管理基準」は、全てのケースにおいてこれを網羅的に利用するものではなく、あくまでも個別組織体の管理基準(監査項目)を策定するにあたっての参照元(レファレンス)である。すなわち、監査にあたっては、本管理基準を基礎として、必要な項目を追加し、あるいは該当しない項目を削除して、あるべき個別組織体の管理基準<sup>39</sup>を策定し、活用する性質のものである。

本研究会においては、個別組織体の管理基準(監査項目)を策定する際に、どのようなプロセスを踏んで策定されるべきかという方法論につき、「個別管理基準(監査項目)策定ガイドライン」(別添資料2)として提示することとする。

なお、個別組織体に情報セキュリティに関する管理基準等(情報セキュリティ基

<sup>33</sup> 経済産業省「システム監査基準」(昭和60年1月制定、<http://www.meti.go.jp/policy/netsecurity/systemauditG.htm>)

<sup>34</sup> 経済産業省「情報システム安全対策基準」(平成7年8月29日制定、<http://www.meti.go.jp/policy/netsecurity/downloadfiles/esecu03j.pdf>)

<sup>35</sup> 経済産業省「コンピュータウイルス対策基準」(平成7年7月7日制定、<http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm>)

<sup>36</sup> 経済産業省「コンピュータ不正アクセス対策基準」(平成8年8月8日制定 <http://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm>)

<sup>37</sup> 総務省「情報通信ネットワーク安全・信頼性基準」(昭和62年、[http://www.yusei.go.jp/whatsnew/kokuji/network\\_2001feb.html#r-1](http://www.yusei.go.jp/whatsnew/kokuji/network_2001feb.html#r-1))

<sup>38</sup> 警察庁「情報システム安全対策指針」(平成9年9月18日制定、[http://www.npa.go.jp/hightech/antai\\_sisin/kokuji.htm](http://www.npa.go.jp/hightech/antai_sisin/kokuji.htm))

<sup>39</sup> 概念としては、これが各組織のあるべき「セキュリティポリシー」と一致する性質のものである。

本方針<sup>40</sup>を含む)が既に存在する場合は、①組織体の現状がその管理基準等に準拠しているかという準拠性の監査と、②あるべき個別組織体の管理基準(監査項目)と現に有する管理基準等との乖離(ギャップ)の両者の視点による監査が行われることが一般的であると考えられる。

#### 3.3.4.3 主体別・業種別管理基準の概念と「電子政府情報セキュリティ管理基準」

上に示したように、個別組織体は「情報セキュリティ管理基準」を基礎として、個別組織体のあるべき管理基準を策定して監査を実施することとなるが、全ての個別組織体がバラバラに管理基準を策定するよりは、例えば、電子政府や金融、医療といった主体別・業種別に、その特性を反映した統一的な管理基準が策定されていることが望ましい。

これについては、各業界団体等において独自に策定されることが適当であるが、本研究会においては、「個別管理基準(監査項目)策定ガイドライン」を利用し、電子政府における一般的な庁内ネットワークシステムを想定して<sup>41</sup>、「電子政府情報セキュリティ管理基準モデル(庁内ネットワークシステム)」(別添資料3)を策定し、電子政府用の主体別・業種別管理基準として利用可能なモデルを提示することとする。

---

<sup>40</sup> 脚注23参照。

<sup>41</sup> 一般的な電子政府においては、その代表的なシステムとして、①庁内ネットワークシステム、②公開サーバーネットワークシステム、③認証局システム、④インターネット以外の外部接続システムの4システムが挙げられる。ここでは、この4つのうち「庁内ネットワークシステム」を選択し、このシステムとその運営に関わる要員を対象範囲として、管理基準のモデルを提示したものである。

### 3.4 「情報セキュリティ監査基準」策定の考え方

#### 3.4.1 「情報セキュリティ監査基準」の策定方針

「情報セキュリティ監査基準」は、「情報セキュリティ監査」を行う主体の行為規範を定めるものである。その際、前章で示したように、

- ① 多様な主体（監査法人、情報セキュリティ関連のシステム構築等を行うベンダー（情報セキュリティベンダー）、一般のシステム構築を行うベンダー、システムの監視サービス等を行っている情報セキュリティ専門企業、システム監査企業等）が共通に利用するものであること、
- ② 外部の主体及び内部の主体が共通に利用するものであること、
- ③ 内部目的、外部目的ともに利用するものであること、
- ④ 保証型監査、助言型監査ともに利用するものであること

に留意した基準であることが必要である。

この観点から、「情報セキュリティ監査基準」は、

- ① 監査を行う主体としての適格性及び監査業務上の遵守事項を規定する「一般基準」、
- ② 監査計画の立案及び監査手続の適用方法を中心に監査実施上の枠組みを規定する「実施基準」、
- ③ 監査報告に係る留意事項と監査報告書の記載方式を規定する「報告基準」の3部構成とし、現行「システム監査基準」を基本とし、内部監査人協会（IIA）の基準、情報システムコントロール協会（ISACA）の基準等を勘案して策定することが適当である（別添資料4）。

#### 3.4.2 実施基準ガイドラインの策定

「情報セキュリティ監査」を実施するにあたっての留意事項や実施上の手順について、「情報セキュリティ監査基準」の「実施基準」において示された基本的な考え方に基づき、「実施基準ガイドライン」（別添資料5）を策定することが適当である。

ここにおいて、前述した、

- ① 監査における「情報セキュリティ管理基準」の位置付け（3.3.4）、
- ② 保証型監査と助言型監査の選択（2.3.1）、
- ③ リスクアセスメントの実施（2.2.1）、
- ④ 成熟度モデルの利用（3.3.3）

などの重要な点を規定することで、監査の際に、監査を行う主体がこれらの視点を共通に持つことを求めることとする。

### 3.4.3 報告基準ガイドラインの策定

同様に、監査の報告にあたっての留意事項や報告書の雛形について、「情報セキュリティ監査基準」の「報告基準」において示された基本的な考え方にに基づき、「報告基準ガイドライン」(別添資料6)を策定することが適当である。

ここにおいて、保証型監査と助言型監査の場合の監査報告書の違い、保証型監査の類型などについて規定することで、監査の際に、監査を行う主体がこれらの視点を共通に持つことを求めることとする。

### 3.4.4 主体別・業種別監査基準の概念と「電子政府情報セキュリティ監査基準」

「情報セキュリティ管理基準」と個別組織体の管理基準との関係と同様、個別組織体は「情報セキュリティ監査基準」を基礎として、個別組織体のあるべき監査基準を策定して監査を実施することとなるが、全ての個別組織体がバラバラに監査基準を策定するよりは、例えば、電子政府や金融、医療といった主体別・業種別に、その特性を反映した統一的な監査基準が策定されていることが望ましい。

これについては、管理基準と同様、各業界団体等において独自に策定されることが適当であるが、本研究会においては、電子政府における一般的な組織体を想定して、「電子政府情報セキュリティ監査基準モデル」(別添資料7)を策定し、電子政府用の主体別・業種別監査基準として利用できるモデルを提示することとする。

### 3.5 電子政府への利用

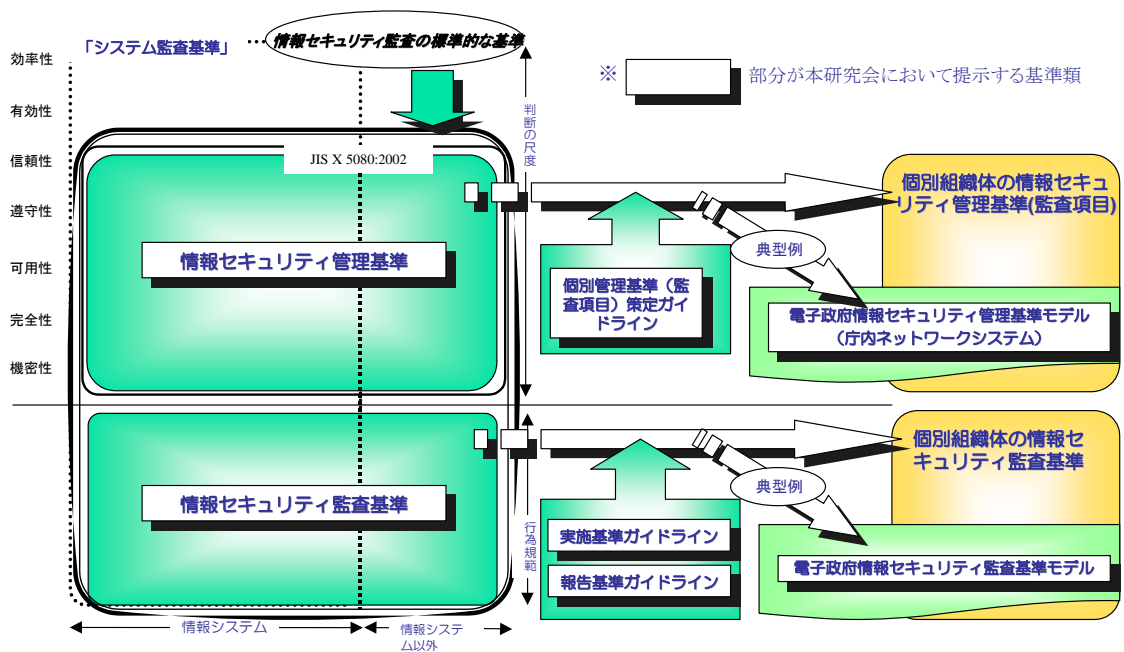
前述(1.4)したように、政府における「情報セキュリティ監査」実施の必要性が声高に指摘され、一部実施に移されているところである一方で、現在のところ、政府においていかなる「情報セキュリティ監査」を行うべきかを示した指針は出されていない。

本研究会においては、電子政府用のモデルとして、「電子政府情報セキュリティ管理基準モデル(庁内ネットワークシステム)」「(別添資料3)」、「電子政府情報セキュリティ監査基準モデル」(別添資料7)を提示しているが、この基準モデルが広く政府において利用され、効果的な「情報セキュリティ監査」が行われることを期待したい。

### 3.6 全体像

以上により策定する基準等の全体像は、以下(図3)のように整理できる。

図3: 基準等全体像



## 4 情報セキュリティ監査を行う主体のあり方

本章では、「情報セキュリティ監査」が健全に普及するために、監査を行う主体に対して用意することが必要な制度等について示すこととする。

### 4.1 「情報セキュリティ監査企業台帳」の創設

前述(2.3.2)したように、監査を行う外部の主体は、監査法人、情報セキュリティ関連のシステム構築等を行うベンダー(情報セキュリティベンダー)、一般のシステム構築を行うベンダー、システムの監視サービス等を行っている情報セキュリティ専門企業、システム監査企業など、多種多様な主体であることを想定している。こうした中、ユーザー側(被監査主体)からすれば、監査を行う主体を選定する際の目安となる制度が用意されていることが有益である。

しかし、我が国における「情報セキュリティ監査」は未だ創成期であることから、現段階では、事前規制はせず、必要な情報開示を求めることで、ユーザーの選択を助けるという視点に立った制度とすることが適当である。

この観点から、一定の開示情報の内容を定めた任意登録制の「情報セキュリティ監査企業台帳」を創設することが適当である<sup>42</sup>。

#### 4.1.1 台帳の性質～任意登録制

「情報セキュリティ監査企業台帳」は、一定の要件を満たせば登録が可能な、任意登録制の台帳とする。登録可能な企業は、

- ① 他人の求めに応じて、「情報セキュリティ管理基準」及び「情報セキュリティ監査基準」にしたがって「情報セキュリティ監査」を行う企業であること、及び
- ② 独立かつ専門的な立場から「情報セキュリティ監査」を行う企業であることを自己宣言していること

を要件とすることが適当である。

また、

- ① 登録は毎年度行うものとし、
- ② その際に前年度の監査実績等を申告し、
- ③ 申告内容に虚偽があった場合等は台帳からの登録抹消が行われる性質のもの

とすることが適当である。

---

<sup>42</sup> 現在、「システム監査企業台帳に関する規則」(平成3年通商産業省告示第72号)に基づく「システム監査企業台帳」が存在するが、これとは別個のものとして位置付ける。

#### 4.1.2 台帳への登録内容(申告内容)

登録に際しての申告内容は、以下のものとし、様式を定めて提供することが適当である。

- ・当該企業の概要
- ・監査の実績(※初年度は、関連する今までの実績で可)
- ・当該企業が属する団体等の名称
- ・情報セキュリティ監査従事者の概要
- ・その他(特色など)

#### 4.1.3 台帳への登録主体

登録主体は企業であるが、個人として「情報セキュリティ監査」を業とする者も当然に登録可能である。「情報セキュリティ監査企業台帳」とする趣旨は、個人としての監査従事者を登録する制度ではないことを示すためである。

#### 4.1.4 台帳の公表

台帳は、毎年度ごとに経済産業省において取りまとめ、経済産業省の WEB ページ等で、速やかに公表されるものとするのが適当である。

#### 4.1.5 地域ごとの台帳

地域の企業や地方公共団体に対する継続的な監査提供の要請に応える観点から、地域ごと(全国9ブロック)に分け、そのブロックに本店又は支店がある企業が登録可能な「情報セキュリティ監査企業台帳(〇〇地域版)」を同時に整備することが適当である。

## 4.2 情報セキュリティ監査を行う主体の質の確保

「情報セキュリティ監査」を行うことのできる人材の裾野を広げ、また監査を行う主体の質を確保・向上させていく仕組みが必要である。監査を行う主体の質の確保を行うためには、①情報セキュリティ監査に従事する個人(以下、「監査従事者」という。)の質の確保、②監査を行う主体となる企業としての質の確保の両面からの手当が必要である。

### 4.2.1 監査従事者の質の確保

監査従事者の質の確保にあたっては、資格制度の存立が有効な仕組みの一つとして考えられる。現在、「情報セキュリティ監査」に関連する国家資格(システム監査技術者、情報セキュリティアドミニストレータ)及び民間資格(公認システム監査人、ISMS 主任審査員、公認情報システム監査人(CISA)等)が存在する(表6参照)も、いずれの資格も、今般整備する情報セキュリティ監査制度と完全に親和性をもつものではない。一方で、資格の乱立は望ましいものではなく、政府は、今後、現存する資格制度を最大限活用しつつ、「情報セキュリティ監査」を行う人材の資格制度のあり方について検討を行う必要がある。

その際、単なる一過性の試験制度ではなく実務的なスキルも加味した仕組みのあり方や、新たな技能の獲得のための継続教育(研修)の必要性などについても、検討を行うことが適当である。

また、上記国家資格については、来年度の試験から、「情報セキュリティ監査」に関するスキルを加味する方向で検討を行うことが適当である。

表6: 関連する主な資格制度(2002年10月現在: 経済産業省調べ)

	資格名称	資格要件	資格抹消	人数等	所管団体
個人	システム監査技術者	試験	なし	4,700名程度	日本情報処理開発協会
	情報セキュリティアドミニストレータ	試験	なし	2,111名	日本情報処理開発協会
	公認システム監査人	システム監査技術者資格+実務経験 or 特定認定(ex. 公認会計士&特別認定講習)	不適切な行為による取り消し	会員755名	日本システム監査人協会
	CISA(公認情報システム監査人)	試験	継続教育の要件を満たさない及び職業倫理規定に違反した場合等	465名	ISACA(情報システムコントロール協会)
	ISMS主任審査員	審査員補&審査の実務経験	なし	92名	日本情報処理開発協会
	ISMS審査員	審査員補&審査の実務経験	なし	31名	日本情報処理開発協会
	ISMS審査員補	実務経験あるいは試験&研修	なし	71名	日本情報処理開発協会
組織	システム監査企業台帳	システム監査を行っていて、登録を行った組織	主に経済産業省の指導による	74団体	日本情報処理開発協会

#### 4.2.2 監査を行う主体となる企業の質の確保

監査を行う主体となる企業の質の確保にあたっては、例えば、「情報セキュリティ監査企業台帳」に掲載された企業が加盟する機関等において、

- ① 監査従事者のための継続教育
- ② 監査企業のピアレビュー
- ③ 監査のノウハウの蓄積
- ④ 今般策定する基準類の改訂・改善の提案
- ⑤ 監査に係る紛争処理

等を行うことが有効であり、政府は、今後、こうした仕組みの整備について検討を行う必要がある。

#### 4.3 電子政府監査を行う主体のあり方

国民の権利・プライバシー、国家の安全保障や、国民の社会生活及び企業活動の安定的運営を確保する観点から、電子政府の「情報セキュリティ監査」を外部の第三者が行う際には、①外観上及び精神上的の独立性、②高い専門的能力、及び③高い倫理性を有していることが求められる。本研究会では、電子政府の「情報セキュリティ監査」を行う第三者の要件について、素案を提示することとする。

##### 4.3.1 外観上及び精神上的の独立性

電子政府の「情報セキュリティ監査」を行う外部の第三者である主体は、自らの行為を自らが監査するようなことがあってはならず、具体的には、以下の要件に該当しないことを、自ら宣言し、証明しなければならないものとするのが適当である。

- ① 企業としての独立性
  - (ア) 当該企業が、現在又は過去において、当該被監査主体(X省)における、当該監査対象となる情報システム(関連業務を含む)の企画、開発、運用、及び保守に係る業務を行っている場合
  - (イ) 当該企業が、現在又は過去において、X省における、当該監査対象となる情報セキュリティのマネジメントや、マネジメントにおけるコントロール(関連業務を含む)の企画、開発、運用、及び保守に係る業務を行っている場合
- ② 監査従事者としての独立性
  - (ア) 監査従事者の中に、現在又は過去において、X省の在職者である者が含まれる場合
  - (イ) 監査従事者の中に、現在又は過去において、X省における、当該監査対象となる情報システム(関連業務を含む)の企画、開発、運用、及び保守に係る業務を行っている者が含まれる場合

- (ウ) 監査従事者の中に、現在又は過去において、X省における、当該監査対象となる情報セキュリティのマネジメントや、マネジメントにおけるコントロール(関連業務を含む)の企画、開発、運用、及び保守に係る業務を行っている者が含まれる場合

#### 4.3.2 高い専門性と倫理性

電子政府の「情報セキュリティ監査」を行う外部の第三者である主体は、高い専門性と倫理性を有していることが必要である。

現時点における資格制度等を前提とすると<sup>43</sup>、具体的には、以下の要件を満たしていることを必要とすることが適当である。

① 企業としての高い専門性と倫理性

新設する「情報セキュリティ監査企業台帳」記載企業であること<sup>44</sup>

② 監査従事者としての高い専門性と倫理性

(ア) 監査責任者は、以下のいずれかの資格を有する者であること

- ・システム監査技術者
- ・情報セキュリティアドミニストレータ
- ・ISMS 主任審査員／審査員
- ・公認システム監査人
- ・公認情報システム監査人(CISA)

(イ) 監査チームの中に、監査責任者の他、上記有資格者を複数名以上(※監査対象の規模によって判断)含めること

#### 4.3.3 監査業務の再委託

電子政府の「情報セキュリティ監査」にあたっては、原則として監査業務の再委託は認めないことが望ましい。

しかしながら、十分かつ適切な監査証拠を入手する観点から、他の専門職(技術士、弁護士、公認会計士等)の支援を仰ぐことが必要な場合もあり、その場合は、当該再委託先に、上記と同様の要件を課した上で、これを可能とすることが適当である。なお、当該他の専門家からのアドバイスや監査手続の補助又は代行があっても、監査の結果についての責任は監査を行う主体にあることはいうまでもない。

<sup>43</sup> 今後、新たに適切な資格が創設された場合は、それを追加することを検討する必要がある。

<sup>44</sup> 「当該企業がISMS適合性評価認証を取得していること」を要件とする案も考えられるが、その構築の経験を有することを意味し、監査を行う能力があることには必ずしもならないため、監査を行う主体の要件とすることは適当でないとの整理。

## 5 その他

### 5.1 ISMS 適合性評価制度との関係

第3章で示したように、今般策定する「情報セキュリティ管理基準」は、JIS X 5080:2002 をもとにするものである。ISMS 適合性評価制度の認証基準も、JIS X 5080:2002 を参照して策定されていることから、「情報セキュリティ監査」と ISMS 適合性評価制度の判断の尺度は、整合性が図られることとはなるが、一方で、その役割分担について整理することが必要となる。

#### 5.1.1 様々なバリエーションがある監査と統一基準の ISMS 認証

ISMS 適合性評価制度は、ある組織体が情報セキュリティマネジメントを行っていることについて ISMS 認証基準という一定の基準に準拠しているか否かについて認証を与えるものである。一方で、前述(3.3.4)したように、「情報セキュリティ監査」は、「情報セキュリティ管理基準」を原則として用いながら、その一部分のみ、また他の基準なども利用しながら、保証又は助言を行っていくという、幅広い評価業務を視野に入れている。

#### 5.1.2 ISMS 認証取得の裾野を広げる「情報セキュリティ監査」

「情報セキュリティ監査」においては、監査の内容については基本的に被監査主体の選択の自由度が高い。「情報セキュリティ管理基準」の項目の一部のみの監査を受けることも可能である。例えば技術的な部分について、客観的に評価をしてもらいたいと思えば、「アクセス制御」の部分についてのみ、重点的に監査を受けることも可能である。またこれらの積み重ねで ISMS 準拠性監査を行い、ある段階で ISMS 認証を取得するといったことも考えられる。

また、マネジメントの監査を正面から実行したとして、助言型監査を用いて、そのレベルを徐々に ISMS 認証取得レベルに向上させていくという利用のされ方が考えられる(図4参照)。

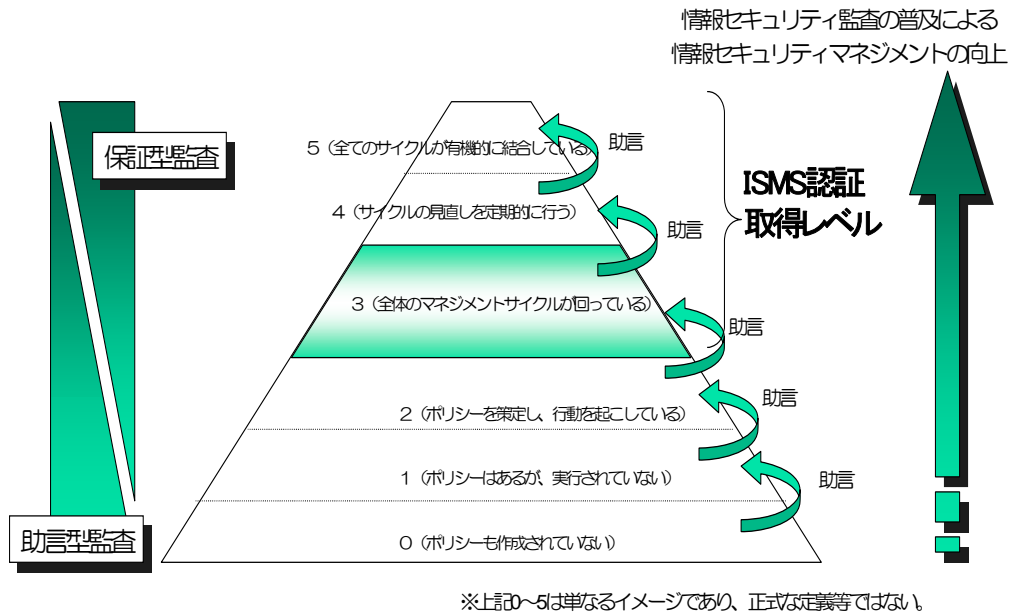
したがって、「情報セキュリティ監査」の普及は、ISMS 認証取得組織体の裾野を広げ、結果として認証取得組織体も増加していく相乗効果を生むものと期待される。

#### 5.1.3 ISMS 認証取得後の保証型監査

ISMS 認証取得後も、ISMS 認証基準に定められる「監査」とは別に、「情報セキュリティ管理基準」及び「情報セキュリティ監査基準」に基づいた「情報セキュリティ監査」を行うことが考えられる。例えば、取引先等の特定の相手方から、マネジメントシステムの認証である ISMS 認証に加え、技術的なコントロール(例えばアクセス制御など)についての監査結果を求められ、こうした部分的なコントロールについての重

点的な保証型監査を受けるといった場合である。

図4:「情報セキュリティ監査」とISMS との関係のイメージ図(図1再掲)



## 5.2 法的関係についての論点整理

ここでは、「情報セキュリティ監査」が実施された場合の、法的関係についての論点の概略を整理する。法的関係についての論点は、「情報セキュリティ監査」を行う主体に関するものと、監査を受けた被監査主体に関するものに分けられる。

### 5.2.1 監査を行う主体に関する法的関係

「情報セキュリティ監査」を行う主体に対しては、①被監査主体に対する法的責任、②監査結果を信頼した第三者に対する法的責任が発生する可能性がある。

#### 5.2.1.1 被監査主体に対する法的責任

監査を行う主体は、監査の依頼者である被監査主体に対する契約上の責任と、不法行為責任を負う可能性がある。このうち、契約上の責任を明確にするためには、①契約の書面化、②契約における監査の判断の尺度の具体化が有益であると考えられる。すなわち、前述(3.3.4)したように、「情報セキュリティ管理基準」以外の判断の尺度を追加して用いるような場合は、その旨を契約上明確化しておくことが有益であると考えられる。これは、保証型監査であるか助言型監査であるかを問わず言えることであると考えられる。

### 5.2.1.2 監査結果を信頼した第三者に対する法的責任

監査を行う主体の第三者に対する責任は、監査結果・監査意見に対する第三者の信頼のうち、保護に値するものを害したことによって発生し、賠償範囲は、これによって通常生ずべき損害であると考えられる。監査結果・監査意見に対する第三者の信頼のうち保護に値するものが何かは、抽象的には論じ得ず、被監査主体、監査を行う主体及び第三者の関係なども踏まえて具体的に確定していくほかにないものと考えられる。

### 5.2.2 被監査主体に関する法的関係

「情報セキュリティ監査」を利用した情報セキュリティマネジメントの確立は、訴訟リスクを軽減する可能性があると考えられる。

紛争の終局的解決は裁判所の判断によるため、本スキームに基づく「情報セキュリティ監査」も、これによっていることそれ自体をもって、直ちに訴訟上の免責を導くものではないと言える。とはいえ、責任の基礎としての過失の判断においては、一般人の能力、具体的には、事故当時において一般的に求められる行為の水準が決め手となる。そのため、本スキームによって示される情報セキュリティマネジメントに共通する枠組みは、裁判所の過失の判断に大きな影響を与え、これに従うことは、有責のリスクを軽減することとなると考えられる。すなわち、本スキームに従った適正な手法によるリスクアセスメントの結果にもとづく合理的なセキュリティ対策の選択とマネジメント体制構築の努力は、責任の軽減に貢献することになる可能性があると言える。

## 5.3 システム監査(基準)との関係

前述(2.1)のように「情報セキュリティ監査」は、「情報資産」(information assets)全体のセキュリティの確保を目的としており、情報資産の分類やそのライフサイクルに沿った枠組みで構成されることが原則となる。この点、現行の「システム監査基準」(昭和60年経済産業省策定)は、「情報システム」のライフサイクル(企画、開発、運用、保守)にしたがって、情報システムの信頼性、安全性及び効率性を検証するという体系となっている。したがって、第3章で提示した「情報セキュリティ監査」の標準的な基準と「システム監査基準」は、その体系が異なることとなる。

一方で、情報資産は情報システム上で運用されることが多く、また、現在行われている実際のシステム監査の業務においては、その手法として情報資産のリスクアセスメントを出発点としているものも存在する。したがって、体系が異なると言っても、「情報セキュリティ監査」と「システム監査」とが排他的になるものではない。

なお、「システム監査基準」については、インターネット環境等現在の情報システムの体系に対応できていない等の問題点も指摘されているところである。したがって、今後、IT ガバナンスやリスクマネジメントの観点を踏まえ、あるべき「システム監査」とは何かということを検討し、今後定められる「情報セキュリティ監査」の一連の基準類等との関係も含めて、「システム監査基準」の見直しを行うことが必要である。

## 5.4 基準等のメンテナンスのあり方

今般策定する一連の基準類については、全て「初版(Ver.1.0)」としての策定を想定しており、これらが利用される状況等を確認しながら、適宜改訂の検討を行っていくことが必要である。

これらの基準類は、技術的側面の陳腐化等の度合いにより、大きく以下の3階層に分けられると考えられ、改訂の頻度や検討体制も、これに見合ったものとする必要がある。

- ①「情報セキュリティ管理基準」「情報セキュリティ監査基準」
- ②「実施基準ガイドライン」「報告基準ガイドライン」「個別管理基準(監査項目)策定ガイドライン」「電子政府情報セキュリティ管理基準モデル(庁内ネットワークシステム)」「電子政府情報セキュリティ監査基準モデル」
- ③「電子政府情報セキュリティ管理基準モデル(庁内ネットワークシステム)」における「技術的検証項目リスト」<sup>45</sup>

---

<sup>45</sup> 「電子政府情報セキュリティ管理基準モデル」においては、必要なサブコントロールについて「技術的検証項目リスト」を策定している(「個別管理基準(監査項目)策定ガイドライン」(別添資料2)参照)。「技術的検証項目リスト」はその全てを研究会開催期間中(本年度内)に策定することは困難であることから、継続的に検討を行い、2003年秋を目処に全体版を策定することとすることが適当である。また、本リストは技術的側面の陳腐化が最も早いものであり、策定後も継続的に見直しを行い、提供方法もWEBサイトにて行うことが適当である。

## おわりに

我が国における「情報セキュリティ監査」の市場は、未だ創成期である。「情報セキュリティ監査」を導入する組織体が増加することで、我が国全体の情報セキュリティ確保のレベルが向上していくことが期待されるとともに、この「情報セキュリティ監査」の市場自体を、今後の成長市場として捉えていくことも必要である。本研究会では、その創成期の市場に一定の規律を与えながらも、政府による規制によって活力がそがれないことに留意して、一連の制度を提案している。

一方で、「情報セキュリティ監査」は、経営のガバナンスという観点からも、その導入を迫られていく流れにある。特に、政府機関においては、国民や企業情報を保有するという立場から、その導入を一層強く求められていくことになるであろう。

我が国において「情報セキュリティ監査」が根付き、有効な制度として機能するためには、その監査事例や紛争処理案件の積み重ねが必須である。また、監査を行う主体の裾野を広げ、その専門性を高めていくことが必要である。「情報セキュリティ監査」を担う主体は、様々な主体であることから、互いにその連携を深め、事例の蓄積、監査を行う主体のスキルの向上などが、有機的に行われていく体制が構築されることを期待したい。

本研究会で策定した基準類は、現時点で最善と考えられ、評価・認知度が確立されている制度をもとに策定したものである。したがって、今後の監査事例や紛争処理案件を踏まえて、適宜見直していくことが望ましい。その際、「情報セキュリティ監査」を導入するユーザーの意見や監査を行う主体のノウハウが、基準類の見直しに有効に反映されるような体制が構築されることも、あわせて期待したい。

## (参考)検討の経緯

第1回:2002年9月5日

1. 本研究会の検討課題について
2. 情報セキュリティ監査の現状について

第2回:2002年9月25日

1. 情報セキュリティ監査の位置づけについて
  - (1)内部・外部論の整理
  - (2)保証型・助言型の整理
2. 情報セキュリティ監査の標準的な基準案の策定について

第3回:2002年10月29日

1. 標準的な基準策定の考え方について(再整理)
2. 監査を行う主体のあり方について

第4回:2002年11月15日

1. 情報セキュリティ監査基準について
2. 情報セキュリティ管理基準全体像と電子政府向け管理基準の考え方について
3. 監査を行う主体のあり方と情報セキュリティ監査企業台帳について
4. 名称について

第5回:2002年12月19日

1. 監査を行う主体のあり方と情報セキュリティ監査企業台帳について
2. 成果全体像と基準等のメンテナンス体制について
3. 情報セキュリティ管理基準について
4. 情報セキュリティ監査基準及び関連ガイドラインについて
5. 電子政府情報セキュリティ管理基準及び電子政府情報セキュリティ監査基準について

第6回:2003年1月21日

1. 情報セキュリティ監査研究会報告書(中間とりまとめ～パブリックコメント版)(案)について

第7回(最終回):2003年3月14日

1. 「中間とりまとめ」に対する意見募集について
2. 「情報セキュリティ監査研究会報告書(案)」について