システム監査経験に基づいた情報セキュリティ監査について

Information Security Audit based on System Auditing Experiences

高 橋 良 子，山 田 和 憲，久 米 進 也

要 約 個人情報の漏洩，不正アクセス，コンピュータウイルス等の脅威が社会的な問題として取り上げられている中，情報資産の保有者である企業では，情報セキュリティ対策が適切かどうかを第三者が評価する情報セキュリティ監査の必要性が高まっている．本稿では，経済産業省が制定した情報セキュリティ監査制度に則った監査基準と，システム監査実施で作成された標準を活かすことにより，効果的に実施できた情報セキュリティ監査について，事例を交えて紹介する．情報セキュリティ監査を実施する上で，今後の課題と認識したリスク評価および技術的検証の見解についても述べる．

Abstract Many companies have a substantial need for the information security audit to assess the appropriateness of their own information security measures by third parties, whose information assets are threatened by the privacy information leakage, unauthorized accesses, computer virus attacks, etc, which are now becoming the social concern.

In this paper, presenting business examples, we introduce the information security audit which could been effectively performed by taking advantage of the audit standard based on METI−established information security audit system and NUL proprietary standards developed with corporate system audit practices. We also discuss the future issues, the recognized risk assessment and technological verification viewpoints for implementing the information security audit.

1. はじめに

中央省庁や自治体における業務の情報システム化が急速に進められ，2002年8月には住民基本台帳ネットワークが稼働した．民間市場では，企業活動に必要な資材の調達等のいろいろな分野において電子商取引の導入が進んでいる．さらに，一般家庭での高速なインターネットアクセス回線の普及に伴って，プライベートや仕事でインターネットを利用する人口は急激に増加している．このように，社会全体と国民の生活で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社会問題が生じている．情報システムへの不正侵入や機密情報/個人情報の外部漏洩，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事故の発生である．これらの事故は，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，さらには企業活動の停止といった被害をもたらし，社会的な影響を深刻なものにしている．

このような社会状況のもとで，情報システムの効率性や有効性，さらに企業の戦略性を評価することが，監査の大きな役割の一つである．

そこで，政府や行政体では，業務の電子化を契機に，情報セキュリティ対策の重要度が高まり，事前防止対策として，システム監査，情報セキュリティ監査の必要性を掲げている．経済

産業省は 2003 年 4 月 1 日に情報セキュリティ監査制度を制定し，この中の「情報セキュリティ監査基準」で，「情報セキュリティ対策は，本来的には，企業，団体，自治体等の組織体の責任において遂行されるべきものであるが，情報セキュリティをマネジメントプロセスに組み込んで構築し運用するためには，管理サイクルの見直しにとって情報セキュリティ監査は不可欠な要素となる．さらに，外部利害関係者との影響関係を視野に入れて IT ガバナンスという観点からも，情報セキュリティ監査のモニタリング機能としての重要性はますます高まってきている．」と述べている．

本稿では，情報セキュリティ監査の必要性が増加している中で，当社のシステム監査で作成した標準を利用し，情報セキュリティ監査制度に則って，情報セキュリティ監査を実施した例から考察までを述べる．まず 2 章では，読者の皆様にセキュリティ監査を知っていただくために，一般的な背景や歴史について述べる．次に 3 章で，当社で実施しているシステム監査の標準を利用した情報セキュリティ監査の手順を述べ，4 章で，実施した情報セキュリティ監査の事例を記載する．おわりに，実施事例から得た，今後の課題と考察について言及する．

2. 情報セキュリティ監査の背景

2.1 情報セキュリティ監査の社会的背景

情報システムの利用が増大している社会環境の変化に対して，国では情報セキュリティに関する制度整備を進め，わが国全体の情報セキュリティ対策を重要視する段階に入ってきた．セキュリティ確保の重要性が増す中で，法律，各種規格，制度が以下のように制定されてきた．

- 1998 年　プライバシーマーク制度の創設
- 2000 年　暗号技術の評価（CRYPTREC）の開始
- 2001 年　JIS X 5080（ISO 17799 より）の制定
  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
- 2003 年　情報セキュリティ監査制度の開始
  インシデント情報共有・分析センター（Telecom-ISAC Japan）の設立
  情報セキュリティ監査制度の運営を支援する団体「日本特定非営利法人日本セキュリティ監査協会（JASA）」の設立
- 2005 年　個人情報保護法の施行

これにともない，独立かつ専門的な知識を有する専門家が情報セキュリティ対策の有効性を評価する「情報セキュリティ監査」分野の制度を整備する必要性が問われるようになった．すなわち，

- 運用後の情報セキュリティ対策の継続的な向上手法の有効性
- 経営ガバナンスにおけるリスクマネジメント体制の有効性
- 内部統制の有効性

これらを評価し監査する仕組みをもった制度が必要不可欠であると言及されるようになった．

ここで，前述の制度であり，情報セキュリティ監査を社会に普及させる発端となった「情報セキュリティ監査制度」について述べる．

2.2 情報セキュリティ監査制度

2003 年 4 月に経済産業省は「情報セキュリティ監査制度」を開始した．その特徴は以下の 4 項目にまとめられる．

① 情報資産のマネジメント

情報資産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という視点が「情報セキュリティ監査」には重要である．また監査にあたっては，監査人は情報資産のリスクアセスメントを行う等，被監査部門主体のリスクアセスメントの妥当性を確認する必要がある．

② 監査形態

「情報セキュリティ監査」を実施する場合，定められた基準の全部を行う形態と，対象範囲，コントロールすなわち内部統制の手続きや保証を限定し，ユーザのニーズに合わせてこの基準の一部のみを実施する形態がある．

③ 個人情報保護との関連

個人情報の漏洩は，個人のプライバシーを侵害し，社会的な大問題となっている．情報セキュリティ管理基準でも「8.4 システムファイルのセキュリティ」の「8.4.2 試験データを保護し管理すること」のコントロールに，「個人情報」と限定した言葉で，保護するためのサブコントロールが記載されている．

④ 外的目的監査と内部目的監査

外部目的監査（外部監査）は，監査対象の情報資産を保有する企業等の外部企業の監査人に依頼することを推奨し，主として保証型監査である．この企業との利害関係者が利用することを目的とする．また，内部目的監査（内部監査）は，監査対象の情報資産を保有する企業等の内部の監査人（または企業の外部の監査人の場合もある）に依頼することを推奨し，主として助言型監査であり，組織内部権利の対策等に利用することを目的とする．

「情報セキュリティ監査制度」は，これらの特徴を備えた「情報セキュリティ監査基準」や「情報セキュリティ管理基準」を策定することにより，監査人にとって具体的でかつ品質が均一である標準的監査を実施する手がかりとなった．

2.3 日本特定営利法人日本セキュリティ監査人協会設立

2003 年 10 月 16 日に，監査企業や監査人，一般企業や団体などの内部監査実施部門等が一同に会し，「公正かつ公平な情報セキュリティ監査」の確立と普及・浸透を目的とした「特定非営利活動法人日本セキュリティ監査協会（JASA）」が設立された．協会では，標準的な監査手法や監査技術を確立し，ビジネスとして成り立たせるためには，監査の質（高い倫理観，高い専門的な能力）が一定水準以上であることを担保する仕組み作りが必要と言及している．

主な活動は，

- 制度そのものを普及するための定期的なセミナーの開催
- 監査の技術や監査人のスキルアップの支援
- 監査制度そのものの研究や業界別ガイドライン作成支援
- 監査を受けたい企業に対して，監査人を紹介する相談窓口
- 監査人の倫理審査

・　監査人の認定制度の設置

等がある．

このように協会では官民二人三脚で「公正かつ公平な情報セキュリティ監査」を社会に普及・促進させるための活動を実施している．

3.　情報セキュリティ監査を効果的に進めるポイント

当社のシステム監査部門では，情報システムサービスの有効性，信頼性，安全性を点検・評価することを目的とした監査を実施している．本章では，経済産業省が制定した情報セキュリティ監査制度に則った基準と，当社がシステム監査実施で作成した標準を活かした当社の情報セキュリティ監査標準について述べる．

3.1　監査の標準化

監査人の能力や経験に差があっても，監査手順や監査作業の標準化によって，監査結果の均一性を保てる．さらに，標準化された監査マニュアルがあれば，監査作業の実施の有無や進捗状況も確認できるので全体の作業管理や品質管理にも役立つ．このような理由から監査作業に係わる作業説明書，監査計画書や監査報告書等の標準を整備しておくことが重要である．

3.1.1　監査作業説明書と報告書類の雛型の整備

監査の実施工程と各工程の作業について監査作業説明書等で標準の監査作業規定を文書化しておく．作業説明書では，各監査ステップにおける

・　作業概要と作業の実施者
・　作業実施に必要となる文書，情報
・　作業実施結果の成果物

等について記述する．また，監査で扱う文書，例えば，監査計画書，監査調書，監査報告書等について定型書式とその例示を準備しておく．標準書式を利用することで，作業効率の向上，必要事項の記入漏れや監査人による記述レベルのばらつきが少なくなる．

図１は，予備調査工程の作業説明書の例である．作業説明書は，日本ユニシスがシステム開発の品質管理で使用している ISBP（情報システムビジネスプロセス）の業務説明書を利用している．図１のように監査工程毎の作業内容をわかりやすく文書化しておく．

3.1.2　基準と監査手続き

一般的に監査には二つの基準がある．一つは，監査業務の品質を確保し，有効かつ効率的に監査を実施することを目的として監査人の行動規範を規定した「監査基準」である．もう一つは，被監査組織体が自らの管理を規定する根拠であり，同時に監査実施時の判断尺度となる「管理基準」である．システム監査，情報セキュリティ監査ともに，これら二つの基準を規範として監査を実施する．ここで，情報セキュリティ監査制度で定められた情報セキュリティ監査の二つの基準について説明する．

「情報セキュリティ監査基準」は，

・　一般基準：監査人として適格性および監査業務上の遵守事項を規程
・　実施基準：監査計画の立案および監査実施上の枠組みを規程

フェーズ名：	作業名：	作成日：	Rev.	作業番号：
予備調査	予備調査準備	05/3/31	1.0	AB10

作業概要：

(1) 監査調書の作成とレビュー

監査調書とは「予備調査チェック項目表」等を指す。
準備段階で作成した資料を入力として、監査調書を作成する。
作成した監査調書類は、システム監査実施チーム内でレビューをする。
必要な場合は、作成した監査調書類のレビューをシステム監査室内で行う。

(2) 被監査部門への説明会実施

被監査部門に対し、監査調書類を記入してもらうに当たっての説明会を実施する。
説明会の場の設定は、システム監査実施チームが行う。
説明会では、監査調書の記入方法や注意事項だけでなく、システム監査実施の目的等も説明する。
監査調書のうち必要なものを提示して、「「予備調査チェック項目表」記入要領」等で説明する。
記入の期限は、被監査部門責任者と話し合った上で事前に設定しておき、説明会の場で明確に提示する。

役　割	実　施　者
「予備調査チェック項目表」作成	システム監査実施チーム
「予備調査チェック項目表」レビュー	システム監査実施チーム

入力情報（◎は必須）	作成者	用　途	様式No.	標準様式（用例）名
契約資料と監査基準の対応一覧表	システム監査室	監査調書類作成の参考	シ監-FA30-100	「契約資料と監査基準の対応一覧表」
システム監査実施計画書	システム監査室	監査調書類作成の参考	シ監-FA30-200	「システム監査実施計画書」
◎監査対象領域一覧表	システム監査室	監査調書類作成の参考	シ監-FA30-230	「監査対象領域一覧表」
「予備調査チェック項目表」記入要領	標準書式オリジナル	記入要領作成の参考	シ監-FB10-110	「「予備調査チェック項目表」記入要領」

出力情報（◎は必須）	作成者	提出/登録先	様式No.	標準様式（用例）名
◎予備調査チェック項目表	システム監査実施チーム	被監査部門	シ監-FB10-100	「予備調査チェック項目表」
その他の監査調書	システム監査実施チーム	被監査部門	−	−
◎「予備調査チェック項目表」記入要領	システム監査実施チーム	被監査部門	シ監-FB10-110	「「予備調査チェック項目表」記入要領」

備考：

図1　予備調査工程の作業説明書例

・　報告基準：監査報告に係わる留意事項と監査報告書の記載方法を規程

から成り立っている．情報セキュリティ監査の実施にあたっては，これらの規程に基づいて，組織体における情報セキュリティの適否を判断するための尺度が必要である．

「情報セキュリティ管理基準」は，監査対象に対して情報セキュリティ対策に係わる一定の条件を満たしているか否か，あるいは実施状況が適切であるか否かについて検証，評価する際の根拠となる判断尺度である．

情報セキュリティ監査の実施に当たって監査上の判断の尺度を明確にしておくことは，監査人にとって，監査手続と監査意見表明の基礎を確立することになる．一方，被監査部門にとっては，採用すべき情報セキュリティ対策の枠組みを決定でき，情報セキュリティ対策運用上の焦点が絞りやすくなる．さらに情報セキュリティ管理基準には，利用する業種により，それを監督する省庁が作成した個別的な管理基準もある．

①　一般産業向け情報セキュリティ管理基準

「経済産業省　情報セキュリティ管理基準」がある．これは，国際標準（ISO/IEC 17799：2000），国内規格（JIS X 5080：2002）をベースとした，組織体の業種および規模等を問わず適用できる汎用的な管理基準である．

②　金融機関向け管理基準

金融庁の外郭団体である財団法人金融情報システムセンター（FISC）が金融機関を対象に策定した「金融機関等のシステム監査指針」，「金融機関等コンピュータシステム

の安全対策基準」がある．金融情報は，業種の特性として一般産業よりセキュリティ，信頼性を強く求めるため，高度な基準を定めている．これらの基準は，毎年多様化するセキュリティ犯罪への対応や，2005 年に全面施行された個人情報保護法に対応するよう改訂を続けている．金融機関によっては，これらの基準に則り，内部監査を実施し，金融監督局に報告を義務づけられている場合もある．

一般的に「情報セキュリティ管理基準」は，情報セキュリティ対策として実施すべき内容のコントロールと，それを詳細化したサブコントロールの形でまとめている．コントロール，サブコントロールの状況をチェックする際には，監査対象に合った具体的検証内容を監査手続きとして設定しておく．監査手続きは，マネジメント系評価項目と，技術的検証項目に分類できる．マネジメント系評価項目は，システム監査の標準手続きに値する．技術的検証項目の評価は，検証ツールやシステムの設定等を行うといった専門的でかつ高度な技術知識が必要である．

情報セキュリティ監査では，監査手続きを実施する前にリスクを評価するリスクアセスメントを実施している必要がある．

3.1.3　リスクアセスメント

情報セキュリティ監査におけるリスクアセスメントとは，情報資産を洗い出し，それらの資産価値，脅威，脆弱性等からリスクの大きさを分析することである．

監査人は，被監査部門が実施した情報セキュリティ対策の妥当性を評価するために，情報資産のリスクアセスメントに基づき，どのような情報セキュリティ対策を講じているかを知る必要がある．被監査部門の採用しているコントロールが適切であるか否かの判断は，リスクに応じたものでなければならない．リスクが相対的に高い場合にはより強力なコントロールが必要とされるし，逆にリスクが低い場合にはそれ相当のコントロールとなる．このように監査人は，監査証拠を評価する際に，リスクアセスメントの結果を考慮することが重要である．同時に，リスクアセスメントが適切かどうかを判断し，適切でない場合には，被監査部門にリスクアセスメントの再実施を要求することも必要である．

情報セキュリティアセスメントの必要性については，OECD のガイドラインでうたわれ，BS 7799/ISMS や情報セキュリティ監査制度においても，リスクアセスメントの実施が強調されている．しかし，具体的な手法については定義されていないため，リスクアセスメント実施者が最適と判断する方法を選択し実施する必要がある．

表 1 は，日本ユニシスで適用した GMITS による四つのリスクアセスメントアプローチである．これらのアプローチのどれが適切かを判断し，実際のアセスメントに利用する．

3.2　監査実施手順

本節では，図 2 に示す日本ユニシスのシステム監査の標準監査作業工程において，各工程で留意する事項について述べる．

3.2.1　準 備 工 程

準備工程では，監査計画を策定するために必要な監査依頼内容の把握，監査対象の現状調査等を行う．留意事項は以下のとおりである．

表 1 GMITS による四つのリスクアセスメントアプローチ

（出典「システム監査情報セキュリティ監査ハンドブック」より）

リスク分析の種類	用　途	内　容	備　考
ベースラインアプローチ	基本的な対策を短時間で策定する場合	既存のセキュリティ対策基準から，対象の情報資産のコントロールを選択	概括的で簡易ではあるが，対策が過不足する恐れがある．マネジィアルアプローチ
詳細リスク分析アプローチ	対象の情報資産に対して個々の最適なリスク対策を策定する場合	情報資産価値を特定し脅威と脆弱性の評価を実施した上で，設定したリスクの許容レベルのコントロールを実施	個々に適した対策が可能だが，専門技術と，多くのリスク分析の作業が必要．テクニカルアプローチ
非形式アプローチ	対象範囲の規模が小型で適当な場合	対策を実施する対象に合わせて，リスク分析技術者の技術と経験で，コントロールを選択	対策に時間がかからないが見落としや過不足が生じやすい．マネジィアルアプローチ
組み合わせアプローチ	大規模，複雑なシステムの場合，多くのバランスよい対策をとる場合	ベースラインアプローチと非形式アプローチの組み合わせで対策を作成するので，リスクの軽い部分と，影響が重大な場合を判別し，コントロールを選択	重要部分と他の部分のバランスがとれた対策により，適切な対策が可能 折衷型

GMITS (Guidelines for the Management for IT Security)

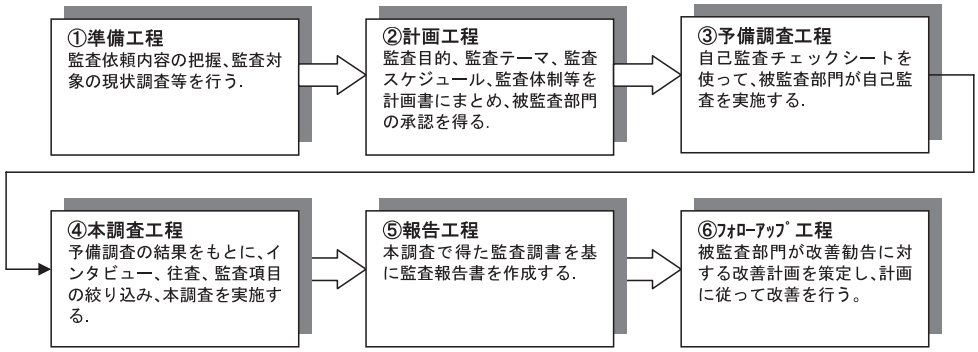

図 2　監査作業工程

① 被監査部門が行ったリスクアセスメント結果を入手し，被監査部門の情報セキュリティのリスクを把握する．同時に被監査部門のリスクアセスメントが適切であるかどうか判断し，適切でない場合にはリスクアセスメントの再実施が必要である．リスクアセスメントは情報資産を把握している被監査部門での実施が望ましい．しかし，リスクアセスメントを被監査部門で実施していない，実施できない場合には，監査部門が支援して簡易的に実施することもある．

② 監査対象に対応した監査手続きを設定する．標準的な監査手続きが，JASA 等から提示されているので，これらをもとに，対象に合わせて監査手続きを追加，削除，変更する必要がある．

③ 個別案件の情報セキュリティ監査の目的は，監査対象の情報セキュリティ対策の欠陥，懸念事項等の問題点を検出し，必要に応じて検出事項に対応した改善提言を行い，情報セキュリティ対策を維持し，セキュリティレベル向上を図ることである．情報セキュリティ監査の実施にあたっては，監査の目的を，説明会等で被監査部門に的確に伝えることが重要である．被監査部門に監査の目的を理解してもらうことにより，監査への協力が得られ，円滑に実施できる．

3.2.2 計 画 工 程

計画工程では，事前におこなった調査結果を元に，監査目的，監査テーマ，監査スケジュー

ル，監査体制等を計画書にまとめ，被監査部門の承認を得る．留意事項は以下のとおりである．

① 内部監査としての情報セキュリティ監査は，中長期的な監査計画のもとで継続的あるいは定期的に実施することが肝要であり，情報セキュリティ対策の運用が形骸化していないかチェックすることが必要である．

② 被監査部門に対し，情報セキュリティ監査，個人情報保護，業務監査等複数の監査が計画されている場合には，類似のインタビューを行ったり，同じ文書・記録やデータの提出を再三求めたりするといった状況を回避すべきである．例えば，各監査の監査項目に共通する部分がある場合には，監査項目を整理・統合すること等が考えられる．

③ 監査業務は，少ないコストで，最大限の効果が期待できるよう実施されるべきである．そのためには監査業務の品質確保が最も重要な要件となる．監査業務の品質確保のため，監査計画，監査調書，監査報告書等のレビュー計画も同時に策定する．

④ 技術的検証を行う場合等専門知識が必要な場合には，ネットワークスペシャリスト，システムアナリスト等専門家の支援を仰ぐことも考慮すべきである．監査計画段階で，これらの専門家を交えた監査チーム体制を整えておく．

3.2.3 予備調査・本調査工程

予備調査では，自己監査チェックシートを使って，被監査部門に自己監査の実施を依頼する．予備調査の結果をもとに，インタビュー，往査，技術的検証項目の内容を絞り込み，監査人が本調査を実施して，監査調査を作成する．留意事項は以下のとおりである．

① 監査証拠は，助言意見の根拠となるものである．関連書類の閲覧，担当者へのヒアリング，現場への往査および視察，システムテストへの立会，テストデータによる検証，脆弱性スキャン，システム侵入テスト等の方法を通じて入手する．そして，その時の状況に応じてもっとも適切な監査手続を選択適用することが重要である．

② 監査人は，入手した資料，テスト結果等を総合的に勘案して，入手した監査証拠を評価し，十分でない場合には追加の点検や調査を実施すべきである．

③ 監査人が入手した監査証拠の評価に当たっては，リスクアセスメントの結果との関連づけを考慮することが望ましい．被監査部門が現に採用しているコントロールが適切であるか否かの判断は，リスクに応じたものでなければならない．リスクが相対的に高い場合にはより強力なコントロールが必要とされ，逆にリスクが低い場合には相応のコントロールとなる．

④ 監査人が実施した監査手続の結果と，監査手続に関連して入手した資料等は，監査の結論に至った経過がわかるように監査調書としてまとめる．情報漏洩や紛失等を考慮し，機密レベルに応じて施錠できるキャビネット等に適切に保管しておく．

3.2.4 報 告 工 程

報告工程では，本調査で得た監査調書を元に報告書を作成し，監査報告会を開催する．留意事項は以下のとおりである．

① 情報セキュリティ監査報告書は，監査の結果を関係者に伝達する手段であるとともに，情報セキュリティ監査人が自らの役割と責任を明確にする手段である．したがって，情報セキュリティ監査の目的に応じて監査人が必要と認めた事項を，明確に記載しなけれ

ばならない.

② アウトソーシングサービスの委託先として内部監査を実施した場合，委託元から報告を要求される場合がある．監査結果は，誤解がなく伝わるものでなければならず，監査報告書に記載した事項については監査人が全面的に責任を負うことに留意する.

③ 助言意見の表明に当たっては，助言の内容は情報セキュリティ監査人の自由裁量で行われるものではなく，あくまでも“選択した管理基準”に照らして検出された問題点の指摘と改善提言であることに留意する.

④ 助言意見は,“選択した管理基準”等に照らした欠陥および懸念事項を検出事項として提示することに留まらず，検出事項に対応した改善提言があって初めて効果的なものとなる.

⑤ 監査報告書における検出事項の記載は，あくまでも被監査部門による継続的な改善活動を前提とした助言として行われるものであって，情報セキュリティ対策の重大な欠陥等に基づく限定的な監査意見にならないことを留意しなければならない．したがって，監査報告書において保証を付与するかのような誤解を与える表現を用いてはならない.

⑥ 監査人が指摘した助言事項に基づいて是正措置を採用するか否かは，あくまでも監査依頼者または被監査部門の判断であって，監査人はそれを強制することはできない.

3.2.5 フォローアップ工程

フォローアップ工程では，改善実施部門が，改善事項に対して改善計画（見積りを含む）を策定し，計画に従って改善を行う．監査部門は，改善の実施状況を把握し，改善結果の点検・評価を行う．留意事項は以下のとおりである.

① 改善計画が策定され，改善が実現されてはじめて監査目的を達成したといえる．改善終了報告を受け，監査人は改善効果の評価を行う必要がある.

② 被監査部門で改善ができない是正項目が存在した場合，戦略的，かつ被害に対する費用対効果等を，十分に被監査部門と検討する必要がある.

4. 情報セキュリティ監査実施事例

本章では，情報セキュリティ監査（内部監査）を行なった事例について述べる.

事例の被監査部門は，金融顧客の構内イントラネットとインターネットを接続する接続ポイントを提供するアウトソーシングサービスを実施している．具体的なサービス内容は，システム運用/障害対応/機器構成管理/不正アクセス監視/セキュリティ診断等である.

4.1 準 備 工 程

① 監査依頼内容の把握

1回目の監査（初回監査）を実施する前には，被監査部門へ監査についての事前説明会を開催し,内部監査の必要性/目的/実施手順/スケジュール等を説明した.これは,3.2.1項の準備工程で述べたように，監査実施計画の策定前に被監査部門と監査ニーズや監査目的の意識合わせをし，円滑に実施できるようにするためである.

② 現状調査

監査実施計画を策定するために，提案書/サービス基本契約書/サービス仕様書/SLA

等を入手した．また，「内部監査事前調査表」を被監査部門に記述していただき，対象システム，関連組織および監査範囲を明確にした．業務内容は，顧客ネットワークとインターネットを接続するネットワーク基盤の構築と，運用・管理業務の受託である．サービス時間は，24 時間 365 日であり，提供している主なサービスは，

・システム運用サービス
・不正アクセス監視

等である．

③　リスクアセスメント結果の入手

前章で述べたように，情報セキュリティ監査を実施するためには，監査実施前にリスクアセスメントが必要である．例えば，ISMS 認証基準では，リスク識別（情報資産の洗い出し，脅威・脆弱性の明確化）を実施してから，リスク分析とリスク評価をする手順がある．事例案件は準備工程時点でリスクアセスメントを実施していなかった．

そこで，監査人が簡易リスクアセスメントを実施し，当社のシステム監査標準の自己監査チェックシートを被監査部門に記載してもらうこととした．自己監査チェックシートは，情報セキュリティ管理基準が 10 項目の管理項目と 132 項目のコントロールで構成されている．さらに，管理項目には 36 項目の管理目的，コントロールには 955 項目のサブコントロールがある．この情報セキュリティ管理基準をベースとして，各コントロールに対して，

・　被監査部門がわかりやすいように，補足説明を追加
・　情報資産に相当する関連資料を記載する項目を追加
・　状況欄に被監査部門が記載することで，リスクを把握

を記載した予備調査チェックシート（表 2）を作成し，これを簡易リスクアセスメントとした．また，ISMS 認証基準では，リスク識別をした後，リスクアセスメントを実施するが，今回は，リスクアセスメントを実施しながら，情報資産の洗い出しを同時に実施した．事例からの考察としてリスクアセスメントやリスク把握は，リスクに対する意識向上のために，情報資産を保有する被監査部門が実施することを推奨する．万一，監査実施までにリスク分析がされていない場合は，表 2 のような予備調査チェックシートによる簡易リスクアセスメントや，被監査部門の所有する情報資産一覧や推定リスク一覧等の資料を入手し，リスク分析する方法が考えられる．

④　監査対象に合致した監査手続を設定する

監査/管理基準の選定としては，金融分野のアウトソーシングが監査対象であることから，FISC の「金融機関等のシステム監査指針」を選択することも考えられたが，サービスの内容がインターネットデータセンターの機能の一部を提供するものであるため，被監査部門とも合意の上で経済産業省の「情報セキュリティ管理基準」を選定した．

監査手続を設定する場合，標準的な手続を監査対象に合わせて修正（追加/削除/変更）する必要がある．監査範囲についての当監査部門の方針として，初回監査では管理基準の全てを確認することにしている．このため，情報セキュリティ管理基準の全管理項目を監査対象として手続きを設定した．また，監査手続きに大きな影響を及ぼす技術的監査項目ついて，監査対象にあわせた対応を取る必要がある．事前調査の結果，被監査部門において，技術的な検証が年 3 回行われていることが分かったので，それらの検証結

表2　予備調査チェックシート（セキュリティ管理基準チェック項目表）の一部

項番	項目	コントロール	補足説明	記入者	監査結果	状況	関連資料(例)	備考
1.	セキュリティ基本方針							
1.1	情報セキュリティ基本方針	1）基本方針文書は，経営者によって承認され，適当な手段で，全従業員に公表し，通知すること	宣言されたセキュリティポリシーは，経営レベルの課題としての組織の情報セキュリティ確保に向けた取り組みを示すものであり，外部の者を含む全ての関係者に徹底されているか.				・情報セキュリティ基本方針（情報セキュリティポリシー） ・教育資料 ・情報セキュリティ指導書	
		2）基本方針には，定められた見直し手続に従って基本方針の維持および見直しに責任を持つ者が存在すること	組織の運営環境を変更等により，組織の運営実態に合わなくなったセキュリティポリシーは機能しないだけでなく有害にもなる．このため，セキュリティポリシーは，常にその妥当性が維持されているか.				・基本方針更新手続書	
2.	組織のセキュリティ							
2.1	情報セキュリティ基盤	1）セキュリティを主導するための明りょうな方向付けおよび経営者による目に見える形での支持を確実にするために，運営委員会を設置すること	組織の情報セキュリティ確保には経営陣の参加が不可欠である．このため，情報セキュリティの確保にかかる活動に経営陣の実効的な参画が行われる仕組みが確立されているか.				・組織体制図	
		2）運営委員会は，適切な責任分担および十分な資源配分によって，セキュリティを促進すること	運営委員会は，適切な責任分担および十分な資源配分によって，セキュリティを促進されているか.				・議事録等	
		3）大きな組織では，情報セキュリティの管理策の実施を調整するために，組織の関連部門からの管理者の代表を集めた委員会を設置すること	大きな組織においては，組織の情報セキュリティの確保には組織運営に係わる多くの業務が関係するため，さまざまな部門の連携が必要となる．このためには，関係する部門同士が情報セキュリティ対策の実施に関しお互いに連携できる仕組みが構築されているか.				・組織体制図	
		4）個々の資産の保護に対する責任および特定のセキュリティ手続きの実施に対する責任を，明確に定めること	情報セキュリティの確保は多くの関係者が係わる．定められたセキュリティの確保にかかるさまざまな施策が適切に機能するようにするためには，保護対象資産に対する保護責任や，セキュリティプロセスの実施責任等の組織内における情報セキュリティの確保についての責任分担が明確にされ，それが当事者に周知されているか.				・体制図 ・役割分担表	
		5）新しい情報処理設備に対する経営陣による認可手続を確立すること	不用意な情報処理関連施設や設備の導入は，サイトのセキュリティを脅威にさらす．このようなことを避けるためには，情報処理関連施設や設備の導入にあたっては，十分なチェックがなされるよう，導入についてのルール・手続きの確立とその適切な運用が行われているか.				・情報処理設備管理手順書	
		6）専門家による情報セキュリティの助言を内部又は外部の助言者から求め，組織全体を調整すること	情報セキュリティの確保には，高度の専門知識やスキルが必要となる．このため，必要に応じ情報セキュリティの専門家の支援が得られるような体制の整備ができているか.				・サポート体制図	

果を評価する手続きとした.

4.2 計 画 工 程

4.2.1 計画の策定

① 監査実施計画書の作成

監査作業について，事前に行った調査結果に基づき，監査の目的，内容，スケジュール等を記載した監査実施計画書を作成した．また，監査業務の品質を確保するため，以下のタイミングでのレビューを計画書に盛り込んだ.

・事前準備終了時
・予備調査終了時
・本調査終了時
・監査報告書作成時

情報セキュリティ監査においては，さらに以下の内容を監査実施計画書に明示すべきである.

・リスクアセスメントの手法

監査実施計画書にリスクアセスメントの手法を明示する．事例では『被監査部門で記入した「自己監査チェック項目シート（情報セキュリティ用）（表 2 と同じもの）の結果とヒアリングを組み合わせて行う』とした.

・技術的検証の範囲

監査実施計画書は技術的検証の範囲を明示する.

被監査部門で技術的な検証が行われていたため，『技術的検証は，被監査部門で実施されている技術的な検証の結果を基に再評価』とした.

② キックオフミーティング

監査作業について，監査実施計画書に基づいて被監査部門と合意をするためにキックオフミーティングを開催した．監査の実施期間中は，被監査部門が客先のサービスを実施していたため，計画変更となることが多いので，余裕を持った作業計画が必要とされた.

4.3 予備調査工程

① リスクアセスメントの評価

被監査部門に自己監査チェックシートによる自己監査を依頼した．また，被監査部門が ISMS 認証取得のリスクアセスメントを実施し作成した以下の ISMS 関連資料を入手した.

・ギャップ分析結果
・リスク分析
・情報リスクアセスメント報告書
・適用宣言書

これらの資料より以下のことが確認できた.

・被監査部門は，ISMS 認証取得を目的としているため，ベースラインアプローチと詳細リスク分析アプローチを組み合わせたリスクアセスメント手法を実施していた.

・事例の監査の方がISMS適用範囲より広いセキュリティ範囲である．
・ギャップ分析結果は本監査の参考にできる．

当該監査範囲でありながら，適用宣言書で適用外となっている項目を中心に簡易リスクアセスメントを実施（自己監査結果に対するヒアリング）することにより，問題が見つかった．このような問題点を本調査における重点項目として採用した．

② 本調査で重点をおく項目の選出

本調査を効率よく行うための準備として，本調査チェック項目表を作成した．本調査チェック項目表は，予備調査で検出された問題点/指摘事項/確認必要事項等を整理し，確認方法をまとめたものである．事例では以下の項目を選択した．

・契約書に記載されているサービス項目に関連するコントロール
・予備調査チェック項目表における疑問点に係わるコントロール
・問題点であると判断している事項に係わるコントロール
・リスクアセスメント結果から対処が必要と判断されたコントロール
・ギャップ分析結果から再確認が必要であると判断された事項に係わるコントロール

③ 技術的検証

一般的に，監査対象のコントロール項目等から技術的検証の必要性を判断し，検証手順を定める．事例は，顧客のイントラネットとインターネットを接続するサービスを提供するだけであるため，被監査部門が実施した技術的な検証で十分であるとし，以下の検証報告書の妥当性を確認した．

・ネットワークセキュリティ診断
・サーバログ解析

4.4 本調査工程

4.4.1 インタビュー

インタビューには，以下のような項目があり，効率良く，被監査部門が負担にならない時間で実施する．事例では，本調査チェック項目表にインタビュー項目を記載し，それを利用した．

・自由応答型　「なぜそのようにしていますか」等，自由に回答できる質問
・直接型　　「先月の残業時間は何時間でしたか」等の質問
・選択型　　「はい」,「いいえ」の回答を引き出す質問．

4.4.2 現場視察

予備調査によって絞り込まれた重点項目について,効率良く4箇所の現場視察をするために,チェックシートを準備し実施した．

4.4.3 監査調書

監査調書は，閲覧資料/担当者へのヒアリング結果，現場への視察・インタビュー結果，証跡等と，各監査工程での発見事項や調査した事項等を，コントロール単位で整理した資料群である．表3は監査調書の項目の一部である．この特徴は各監査工程状況をコントロールレベルで容易に再確認できることであり，監査報告書をまとめる際に有効である．

表3　監　査　調　書

項番	項目	コントロール	補足説明	記入者	監査結果	状況	関連資料	ヒアリング結果	予備調査結果			リスクアセスメント結果	視察・インタビュー				実査証跡		発見事項		指摘事項	
									問題ない	問題点	判断保留		1	2	3	4	ISMS 適用範囲	本監査範囲	ISMS 適用範囲	本監査範囲	ISMS 適用範囲	本監査範囲
1.																						
1.1		1）基本方針文書は，経営者によって承認され，適当な手段で，全従業員に公表し，通知すること																				
		2）基本方針には，定められた見直し手続に従って基本方針の維持および見直しに責任を持つ者が存在すること																				
2.																						
2.1		1）セキュリティを主導するための明りょうな方向付けおよび経営者による目に見える形での支持を確実にするために，運営委員会を設置すること																				
		2）運営委員会は，適切な責任分担および十分な資源配分によって，セキュリティを促進すること																				
		3）大きな組織では，情報セキュリティの管理策の実施を調整するために，組織の関連部門からの管理者の代表を集めた委員会を設置すること																				

4.5 報 告 工 程

① 報告書の作成

図3および図4は，監査報告書に記載する項目と概要の例である．図4は，図3の「2―4　人的セキュリティ」の詳細内容である．【監査の視点】では，該当する管理目的を記載し，【状況】では，監査の視点ごとの良い点，悪い点についての状況を記述する．【指摘事項】では，指摘事項がある場合に情報セキュリティ管理基準のコントロール番号と発見した指摘事実を記載する．

Ⅰ 監査の概要
　監査対象、監査目的、監査基準、監査日程、視察場所などについて、監査の概要を記載する。
Ⅱ 監査対象
　監査対象となるアウトソーシングサービスの委託元顧客名、提供しているサービス、契約の期間と提供サービスの規模などについて概要を記載する。
Ⅲ 監査結果
　1．監査結果の概要
　　監査の全体総評、主要指摘事項、改善勧告について記載する。
　2．管理項目別監査結果
　　以下の「情報セキュリティ管理基準」の管理項目別に、状況と指摘事項を記載する。
　　2－1　セキュリティ基本方針
　　2－2　組織のセキュリティ
　　2－3　資産の分類および管理
　　2－4　人的セキュリティ
　　2－5　物理的および環境的セキュリティ
　　2－6　通信および運用管理
　　2－7　アクセス制御
　　2－8　システム開発および保守
　　2－9　事業継続管理の種々の面
　　2－10　適合性

図3　情報セキュリティ監査報告書の概要

【監査の視点】

① 職務定義および雇用におけるセキュリティを確保するために，人による誤り，盗難，不正行為，又は設備の誤用のリスクを軽減させているか.

② 利用者の訓練によって，情報セキュリティの脅威および懸念に対する利用者の認識を確実なものとし，通常の仕事のなかで利用者が組織のセキュリティ基本方針を維持していくことを確実にしているか.

③ セキュリティ事件・事故および誤動作による損害を最小限に抑えるため，並びにそのような事件・事故を監視してそれらから学習しているか.

【状況】

① XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.
② XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.
③ XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

【指摘事項】

① 特になし.

② XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX【コントロール 4.2.1】

③ 特になし

図4　人的セキュリティの報告形式

② 事実確認会および報告会の実施

監査報告書（案）が作成された段階で，被監査部門と事実確認会を開催する．事実誤認を排除し，被監査部門の意見を報告書に反映するためである．その後，監査人は，監査報告書の提出に合わせて，監査依頼部門および被監査部門の責任者に対する報告会を開催する．事例においても，事実確認会と報告会を実施した.

4.6　フォローアップ工程

事例では4件の改善勧告を行った．被監査部門が策定した改善計画書を入手し，改善計画書のスケジュールに合わせて，フォローアップ監査を実施した.

5.　情報セキュリティ監査の今後の課題

実際に情報セキュリティ監査を実施する上で，今まで経験してきたシステム監査の標準では考慮しておらず，かつ標準化しにくい問題があることがわかった．それは，リスク評価するリスクアセスメントと技術的検証である．これらは，JASA や他の監査関連団体等でも検討中の内容である.

① リスクアセスメント

事例では，被監査部門で実施している ISMS 認証取得のためのリスクアセスメントの結果と，自己監査および監査人のヒアリングによる簡易リスクアセスメント結果を利用している．しかし，被監査部門がリスクアセスメントを実施していない場合，自己監査チェックシートを用いた簡易リスクアセスメントでは，情報資産を監査項目から洗い出すため，予備調査工程までリスクが把握できず不足しやすい．被監査部門が準備工程までにリスクアセスメントを実施していることが最適である.

情報セキュリティ監査において，被監査部門における詳細なリスクアセスメントは必要であるが，一般的な詳細リスクアセスメントには，多大な時間がかかる（ISMS 構築において，情報資産の洗い出しからリスクアセスメントを行う工数は約1人月と見積もられている）．リスクアセスメントの標準化により少しでも工数を削減することが必要である.

② 技術的検証

事例では，情報セキュリティ管理基準内の技術的監査項目について，対応した結果を記載している．しかし，実際の検査は被監査部門が実施していたため，検証報告書から文書上の正当性監査を実施するにとどまった．情報セキュリティ監査制度では，技術的監査項目の監査手続（サブコントロール）を定めているが，それをどのように検証するか具体的検証手段が決まっていない．また，システムの HW/SW 構成がそれぞれに異なるため，検証方法を一律に定義し具体化することは困難である．検証ツールの開発や技術監査のできる組織作りが必要である．

6. おわりに

情報セキュリティに対する会社の関心は高まってきてはいるが，実際に情報セキュリティ監査はどの程度実施されているのか．表 4 はシステム監査普及状況調査の一部として，情報セキュリティ監査の普及状況について 2004 年に JIPDEC が実施した調査の概要である．

表 4　調査の概要

調査の目的	システム監査の普及状況を監査担当部門に対して調査し，現状と問題点を把握するとともに，今後のシステム監査の普及促進に役立てることを目的として実施．
調査の対象	JIPDEC が隔年で実施している「システム監査普及状況調査」の母集団４０業種，４０００事業体を対象．
調査時期	調査票発送：　平成 16 年 11 月 19 日 回収締切　：　平成 17 年 1 月 21 日
回収状況	発送数　　：　４０００件 回収数　　：　５０７件（回収率：１２．７％）
回収事業体の平均従業員数	２２４４人

この調査結果では，経済産業省の「情報セキュリティ監査基準」，「情報セキュリティ管理基準」については約 80% の事業体が認識している．一方，情報セキュリティ監査を受けたことがある，または情報セキュリティ監査を受ける予定がある事業体は 30% 弱となっている．これは，情報セキュリティ監査を受ける費用対効果やメリット，必要性などを事業体が十分に認識していないためであり，その結果として情報セキュリティ監査を受ける事業体が少ないと考えられる．

また，監査を外部委託したいと考えている事業体は 50% 強となっている．理由としては，事業体内に情報セキュリティ監査ができる人材がいない，監査体制が整っていないこと等が考えられる．情報セキュリティ監査は，まだまだ社会全体に普及しているとはいえない．

今後は，JASA のワーキンググループ活動に参加するなどにより，情報セキュリティ監査の普及に貢献するとともに，監査のスキル・技術の向上に努め，お客様が満足できるような情報セキュリティ監査を目指していきたい．

参考文献 ［1］ NPO 日本システム監査人協会「改修：システム監査情報セキュリティ監査　ハンドブック」秀和システム
［2］日本セキュリティ監査協会「公認情報セキュリティ監査人研修テキスト」
［3］日本セキュリティ監査協会「Security Eye　創刊号」
［4］経済産業省「情報セキュリティ管理基準　Ver 1.0」
［5］経済産業省「情報セキュリティ監査基準　Ver 1.0」
［6］経済産業省「システム監査基準」
［7］日経 BP　　情報セキュリティ対策集中講座
［8］小林　誠（主査研究員）インターリスク総研「今求められる BCM－事業継続経営－とは？」
［9］特定非営利活動法人　日本セキュリティ監査協会「平成 16 年度　情報セキュリティ監査制度利用促進等事業実施報告書」平成 17 年 3 月 31 日
［10］三井業際研究所　技術部会　情報セキュリティ調査研究委員会「情報セキュリティ調査研究委員会　報告書」2005 年（平成 17 年）3 月
［11］土居範久他「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　報告書」平成 17 年 3 月
［12］「情報セキュリティ・ビジネスの発展と官民連携のあり方に関する調査研究会　報告書」平成 14 年 7 月 1 日
［13］財団法人　日本情報処理開発協会「2005－2006 年版　システム監査白書資料　システム監査普及状況調査（Ⅰ）被監査部門対象　集計結果」平成 17 年 3 月
［14］財団法人　日本情報処理開発協会「2005－2006 年版　システム監査白書資料　システム監査普及状況調査（Ⅱ）被監査部門対象　集計結果」平成 17 年 3 月
［15］経済産業省：「情報セキュリティ監査基準実施ガイドライン」，2003 年 3 月
［16］地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書別添 3
［17］NPO 日本セキュリティ監査協会平成 15 年度情報セキュリティ監査制度普及啓発活動報告技術部会 WG 2「最新の情報技術に対応するセキュリティ監査手法の調査研究」（http：//www.jasa.jp/about/pdf 2003/dist_techwg 2.pdf）
［18］情報セキュリティ・個人情報保護のための内部監査の実務　（日科技連）
［19］NPO 日本セキュリティ監査協会　ホームページ（http：//www.jasa.jp/index.html）

執筆者紹介　高　橋　良　子（Nagako Takahashi）
1978 年東京女子大学卒業．同年日本ユニシス(株)入社．業務 AP のコンバージョン，製造パッケージ開発，通信系システム開発・品質管理のリーダおよびマネジメント職に従事．2003 年 4 月より全社品質管理リーダ，システム監査室室長を経て，現在監査の品質向上・促進活動に従事．NPO 日本セキュリティ監査協会幹事，情報サービス産業協会システム監査研究会委員，ISMS 審査員補．

山　田　和　憲（Kazunori Yamada）
1980 年北海道工業大学卒業．同年日本ユニシス(株)入社．中型機の通信関連ソフトウェアの開発/保守業務を担当．1985 年より，オープン系サーバにおける通信関連ソフトウェアの開発/保守のリーダを経験．その後，情報セキュリティ構築の営業支援を行い，2004 年 4 月よりシステム監査業務に従事．NPO 日本セキュリティ監査協会技術部会会員．

久　米　進　也（Shinya Kume）
1983 年関西学院大学卒業．同年日本ユニシス（株）入社．ユニシス汎用機の基本ソフトウェアの客先出荷前検査業務を担当．1992 年より，TCP/IP プロトコルを使った通信系プログラムの開発・保守を担当．その後，通信キャリア向けパッケージソフトウェアの客先提案業務を行い，2003 年 12 月よりシステム監査業務に従事．公認情報セキュリティ監査人，ISMS 審査員補．