●システム監査学会　第25回研究大会　研究プロジェクト報告

情報セキュリティ監査の活用による企業の情報セキュリティ対策の診断

"Evaluation about Corporate Information Security Measures by the Use of Information Security Audit“

2010年度 「情報セキュリティ対策の診断」研究プロジェクト成果報告

2011年6月10日

報告者　研究プロジェクト　　尾崎　孝章

目次

１．研究プロジェクトの目的と検討内容

（１）情報セキュリティ対策の診断　これまでの経緯

中小規模企業の情報セキュリティ対策の促進と徹底のため、情報セキュリティ監査をどう活用するか。情報セキュリティ対策の診断というアプローチによって企業内の実態を把握し、必要な改善を図ってもらうことを軸として研究を進めてきた。

（２）問題提起

企業活動には、情報資産に対する情報セキュリティの確保が必須

- したがって企業は情報資産（個人情報を含む）活用の基盤に対する内部統制の確立を図っている。

これから情報セキュリティ対策に取り組んでいく企業の存在

- 一気に高いセキュリティレベルを目指せない。
- セキュリティ関連の認証取得までに至らなくても、もっと簡単に情報セキュリティ対策を強化したいと考える企業は多い。

顧客をはじめ広く社外へアピール・宣言をしたい企業の立場

- 実施してきた情報セキュリティ対策の活動は、正当に評価されるようにしたい。

企業活動に対するシステム監査人の活躍の場の開拓

- 情報セキュリティ対策を評価する基準を明らかにして、その基準により評価診断を行なう。

1．研究プロジェクトの目的と検討内容

＜既存の評価方法＞

- ✓ 個人情報保護 ： プライバシーマーク認定制度（Ｐマーク）
- ✓ 情報資産管理 ： ＩＳＭＳ（JISQ27001）認証制度
- ✓ 情報セキュリティ対策の格付け ： 「情報セキュリティ格付」制度
  （㈱アイ・エス・レーティングが実施している大企業向けの制度）

上記は中小企業（中堅企業）には、費用を含め負担が重い仕組み

研究プロジェクトのアプローチ

これまで情報セキュリティ対応とは無縁であったような、従業者数で50人に満たない企業も対象として、各企業に適した（必要以上でない）セキュリティ対策を実現させ、対策向上に役立たせることを検討

その実現には、**もう少し軽く、しかし、考え方は確立したものが新たに必要**

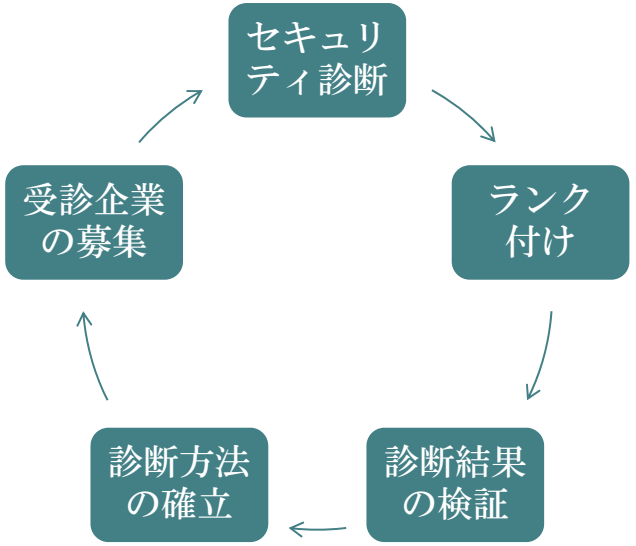
１．研究プロジェクトの目的と検討内容

（３）診断という形の確立へ

① 診断の確立のため、評価、診断を受ける企業を募集し、情報セキュリティ対策の診断を実証実験として行う。

② 診断の過程で情報セキュリティ監査の活用を図る。

③ 企業に必要な情報セキュリティ対策を診断し、ランク付けをする。



２．情報セキュリティ対策　評価・診断の考え方

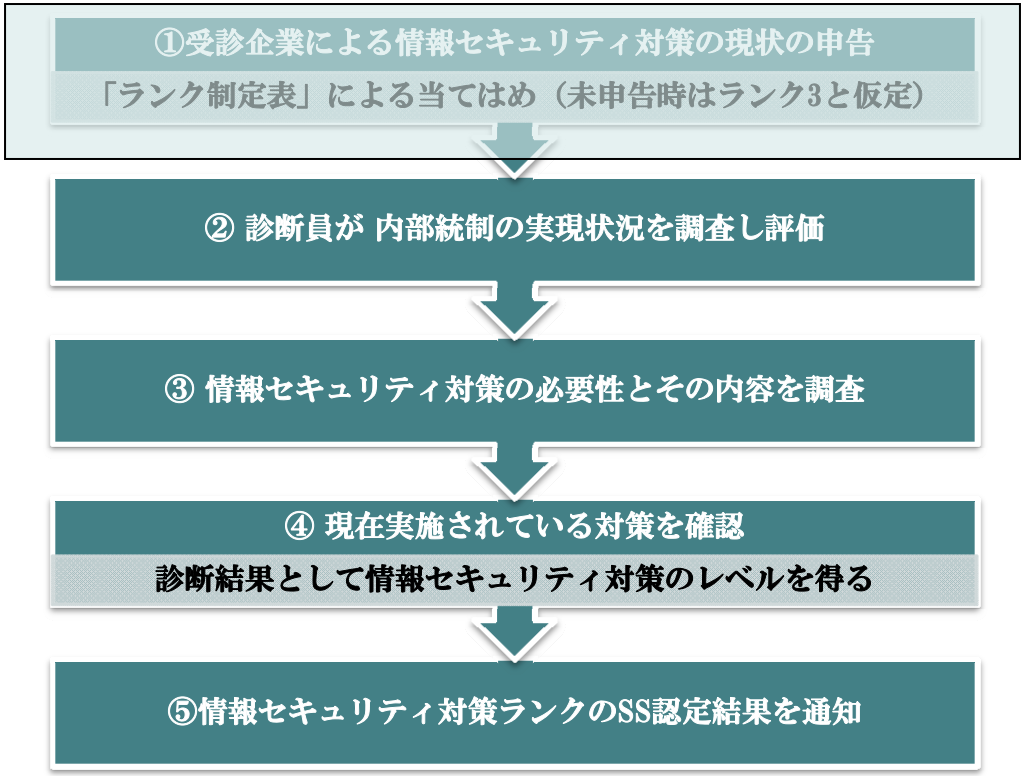
（１）評価・診断の考え方（一律のセキュリティ対策でなく必要性に応じた対策を求める）

2つの結果を突き合わせて対比し、評価をする。

評価「ＳＳ（Security Score）」認定：★の数（１から５）で表現
★☆☆☆☆ ～ ★★★★★（半分の表示「★」（小さい星）もある）

2．情報セキュリティ対策　評価・診断の考え方

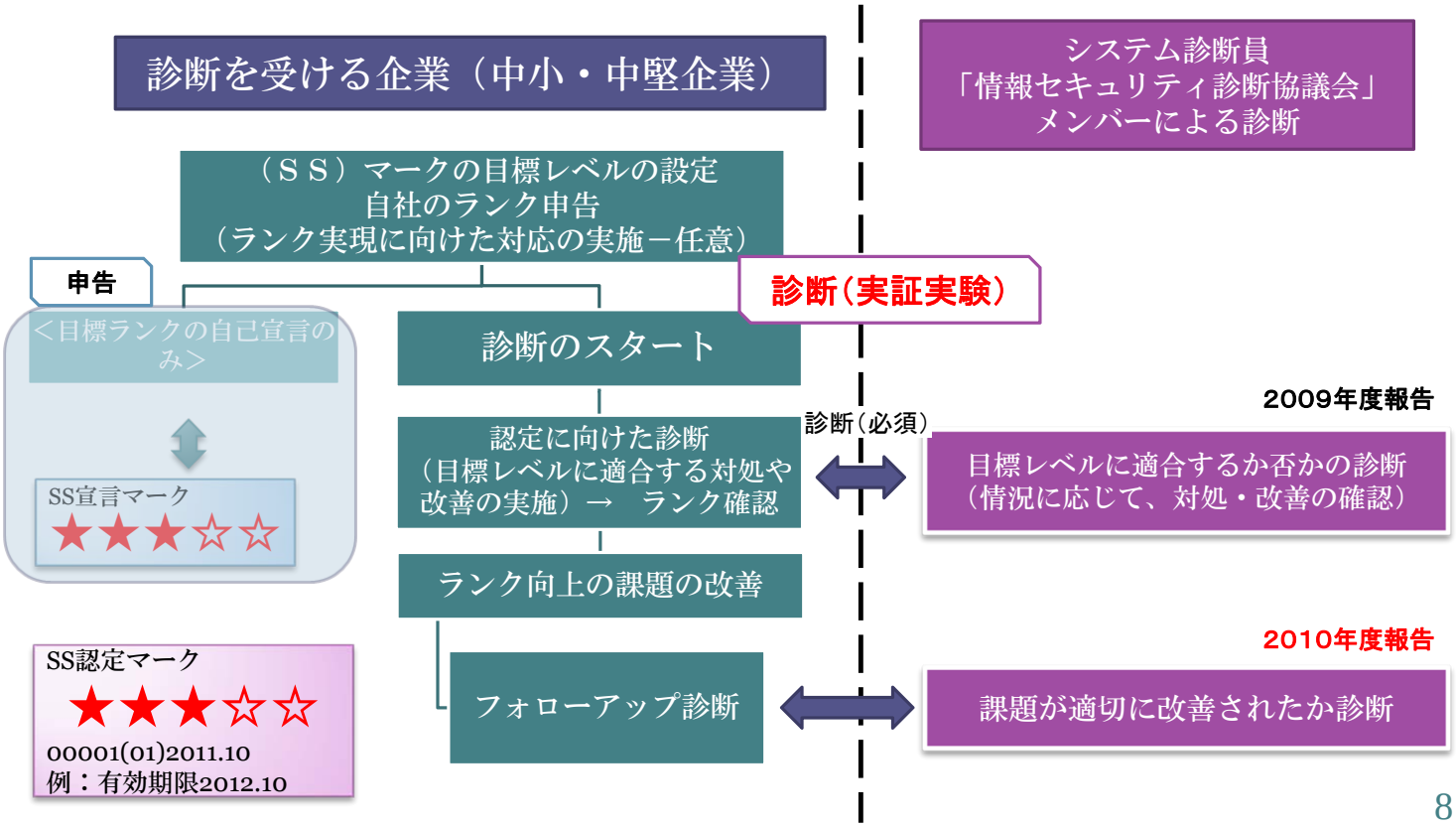
（2）情報セキュリティ診断の流れ



※現在未実施

2．情報セキュリティ対策　評価・診断の考え方

図：情報セキュリティ対策の診断　全体スキーム



３．２０１０年度の研究事項

（１）研究項目

2009年度の実証実験により、受診企業から得られたニーズと課題

ニーズ	• 受診企業は“改善に向けて何をしたらよいのか”具体的な取り組み方法を求めている。
ニーズ	• 規定の改善、あるいは規定策定の体系構築も含めた、基礎からの提案が望まれる。
課題	• 診断をうけた後に、改善実施結果を確認するフォローが必要であり、「フォローアップ診断」方法の体系化が必要。

企業はセキュリティ対策の診断結果を踏まえて、当然に現状からさらによい状態に進めたいと考えている。⇒診断のみでは企業の要求に対応できていない。

３．２０１０年度の研究事項

（２）フォロー診断

２０１０年度の実証実験として、２００９年度に診断を実施した１社を含むフォロー診断の実施を進める中で、次を研究事項として検討を進めた。

研究事項　①　情報セキュリティ対策が必要な業務分野の把握の確立

- 診断の内容を事業者の業務内容（対策の必要性）に適合させる方法の整備（手さぐり的な方法からの改善）

研究事項　② 情報セキュリティ対策分野ごとに必要な規定体系の整備

- 対象企業の中には、規定の整備も始めたばかりの企業もあり、これから本格的に情報セキュリティ対策を進める企業が想定され、ＰＤＣＡの仕組みも十分に出来ていない場合もある（＝規定体系の整備が必要になる）。

研究事項　③ 内部統制状況のわかりやすい把握方法の確立

- ランク制定表の表現（ランクの考え）がわかりづらく、企業の理解が得られるわかりやすいランク制定表へ見直しを行う。

４．研究結果（研究事項１）

情報セキュリティ対策が必要な業務分野の把握の確立

（１）企業のセキュリティ活動を１０分野に分類をして考える。

例

1. 情報セキュリティ管理体制
   情報セキュリティマネジメントシステムの基本的な規定
   情報資産管理のための基本的な規定など
2. 情報資産の取扱いに関する管理
   取得、利用、伝送、保管、消去・滅却およびそれらの記録）
   アクセス制御、運搬(手持ち)、送付
3. 雇用管理　(採用―雇用―退職・退場)
   社員や関連する従業員の人的な業務管理規定

（全体項目は次スライドに記載）

（２）受診企業に対して具体的な業務分野を明示する。
業務フローなどを元に、情報セキュリティ対策が必要な分野（業務内容）とその関係を明示し、１０分野を意識した業務概要図を作成する。

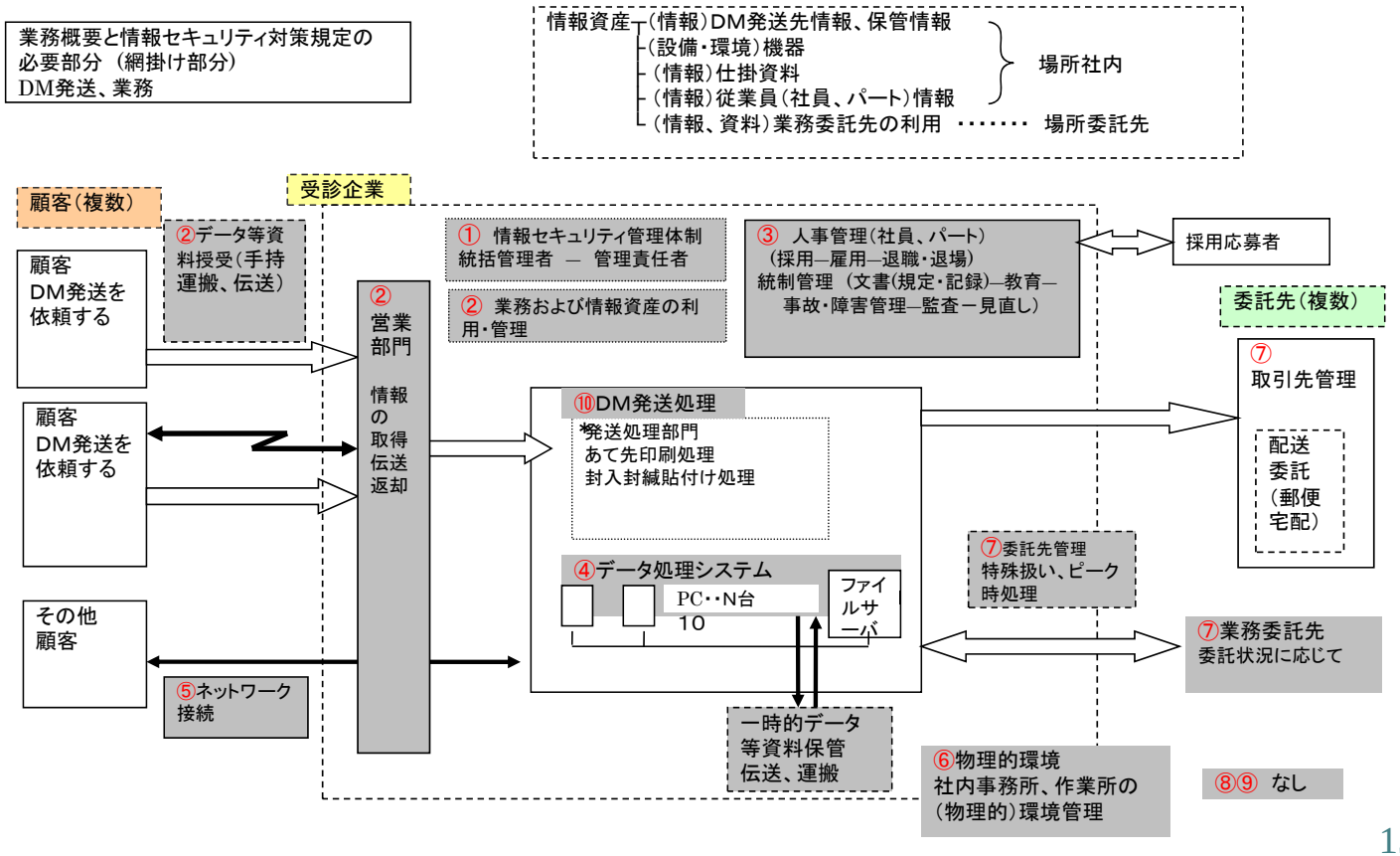
（３）各分野における情報資産取り扱いのリスクを把握する（リスク分析）。

情報セキュリティ対策が必要となる業務分野

分野	業務
①企業組織の統括管理業務分野	・情報セキュリティの基本業務（方針策定、情報資産特定） ・マネジメントシステム（ＰＤＣＡ）運営
②業務及び情報資産の利用・管理分野	・会社の基本業務に関する情報（従業者、顧客、取引情報）の取扱いに関するインフラ管理
③従業員管理業務分野	・従業員の雇用管理 ・従業員への教育、事故、管理
④情報システムの運用管理分野	・会社の情報システムの運用環境（インフラ）の管理
⑤ネットワーク接続管理業務	・ネットワーク接続環境の管理
⑥物理的環境管理	・施設、設備環境の管理、設備、施設管理
⑦取引先管理業務分野	・取引先(顧客、委託先)の管理
⑧開発業務環境分野	・開発業務の情報システム環境
⑨設計書、リソース等資料管理	・開発業務に関わる情報及び資料の管理
⑩業務固有分野	・業務固有の管理

業務概要図

図はＤＭ発送業者を例示



４．研究結果（研究事項２）

情報セキュリティ対策分野ごとに必要な規定体系の整備

（１）具体的な規定の整備および規程内容について確認し、提示

① マネジメントシステムに必要なＰＤＣＡを動かす規定が、どのように策定されているか、確認する。

② 情報資産の取り扱いに必要なセキュリティ規定がどのように策定されているかを確認する。

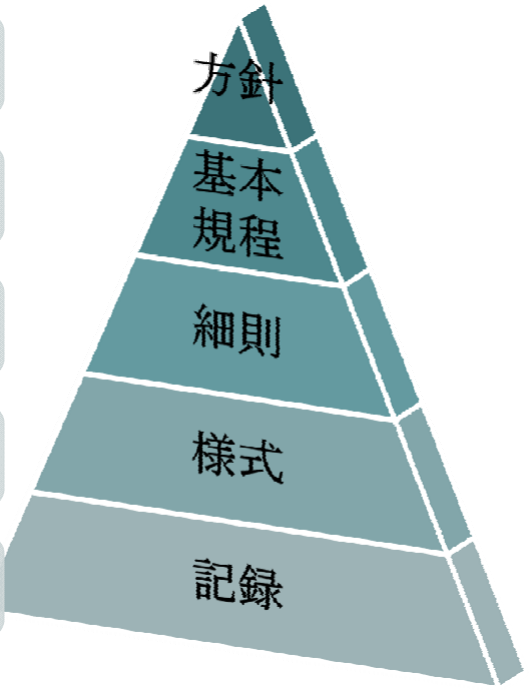
③ 各分野ごとにリスク分析結果を考慮して、必要な規程を決定する。

- 規定がない場合、規程をどのように策定するかについて示すことが必要
  - マネジメントシステムに関する規定は、JISQ15001、JISQ27001を参考
- 規定の構成（体系）は、方針、基本規定などの５階層を想定（次スライド）
- セキュリティ診断の結果、整備が必要な規定は業務分野と関係付けて「ランク制定表」の申告ランクのレベルを考慮して指摘
  - 改善点を明確化し、企業がなすべきことを提示

４．研究結果（研究事項２）

（２）規定の体系

方針	・セキュリティポリシーとし、マネジメントシステム（ＭＳ）に基本をおいて、情報資産のセキュリティ確保を実現させることを、宣言する。
基本規程	・ＭＳの規定、及び安全管理規定の基本事項を策定する。管理策マニュアルも該当する。
細則	・基本規定に基づく、現場での実施規定、手順などを具体的に策定する
様式	・基本規定、細則により実施されるセキュリティ活動で使用する各種様式
記録	・基本規程や細則に従って様式に記入した文書やデータ



４．研究結果（研究事項２）

（３）策定検討規定の一覧分野

分野ごとのリスクに対応した規定があるか、規定内容がセキュリティ項目を満たしているかを確認する。なお、一覧全体とはJISQ27001（詳細管理策）との項目対比を行い、対応を確認している。

分野	関連する規定
①企業組織の統括管理業務分野	マネジメントシステム、内部組織管理情報資産
②業務及び情報資産の利用・管理分野	取得、利用、伝送、保管、消去・滅却およびそれらの記録）、アクセス制御、運搬(手持ち)、送付
③従業員管理業務分野	雇用管理　(採用－雇用－退職・退場) 統制管理規定　(文書(規定・記録)－教育－事故・障害－見直し)
④情報システムの運用管理分野	(業務分野に関する情報システムの基本規定を含む) （ウイルス対策、セキュリティソフト、グループウェアなどのほかソフトウェアライセンス管理）
⑤ネットワーク接続管理業務	インターネット環境、(業務分野に関する情報システムの基本規定を含む)
⑥物理的環境管理	情報及び情報処理施設の入退管理、アクセス管理、各種災害等の脅威への対策管理
⑦取引先管理業務分野	委託先、委託業務の委託実態に応じて策定すれば良い
⑧開発業務環境分野	システム設計書、設計書等資料管理
⑨設計書、リソース等資料管理分野	設計書等資料管理
⑩業務固有分野	業務対応の規定

４．研究結果（研究事項３）

内部統制状況のわかりやすい把握方法の確立

（１）「ランク制定表」を中小規模の企業の実態に適合した分かりやすい表現に見直しする（企業に対してランクアップへの行動を明確に示す）。

以前のランク表示

- 業務標準、プロセスの確立をベースに判断するが、企業にとってどのレベルに位置しているのか、明確ではない。
- 成熟度別の情報セキュリティ対策の説明（ツール、スキル要件、プロセス、自動化など）が、中小規模の企業ではあまり使わない用語を記述をしていた。

見直したランク表示

- 企業のルール及びトップ/ミドル/ローの認識・行動を確認するものへと展開
- 中小規模の企業における管理や内部統制の状況を、企業の該当者が読んでわかる表現へ

４．研究結果（研究事項３）

（2）「ランク制定表」(部分) 確認対象（一般成熟度モデルの分類は変えていない）

	一般成熟度モデル（０～５）
ルール	・業務に関する内部統制 業務手順書などによる業務継承方法)の確立 ・情報セキュリティの内部統制の確立
トップ（代表者）	情報セキュリティに関するトップの考え方とその具体的表現実施
ミドル（管理者） ➢業務管理者 ➢マネジメントシステムの管理者 ➢情報システムの管理者	ミドルの状況と活動結果 マネジメントシステムの管理者の活動状況、定着状況 情報システムのセキュリティ対策の定着状況
ロー（担当者）	従業者の情報セキュリティ対策の意識、行動、ルールの徹底状況

参考資料（新ランク制定表）※抜粋

分類　ランク表示	ランク０	ランク１	ランク２	ランク３	ランク４	ランク５
一般成熟度モデル（０～５）	プロセスが確立していない初期段階（不在）	プロセスは特定のリーダ・技術者に依存している（その場対応）	首尾一貫したプロセスがあるが、標準になっていない	プロセスは標準化され、文書化されている（定められたプロセスがある）	プロセスのPDCAが確立して、是正が行われている	継続的改善、予防活動によりプロセスが最高水準に最適化できている
ルール 業務に関する内部統制						
ルール 情報セキュリティの内部統制の確立						
トップ 情報セキュリティに関するトップの考え方とその具体的表現実施	情報セキュリティ方針が存在しない。	情報セキュリティ方針がない、または有っても明確にはオーソライズしていない。	情報セキュリティ方針がトップの責任で明文化されている。方針の具体的展開の指示が存在する。	情報セキュリティを含んだ教育計画とその定期的な実施を確認できる トップが関与したＰＤＣＡの運用記録あり。	定期的な情報セキュリティマネジメントシステムの見直しの機会があり、機能している（見直しの記録や成果がある）。	全社が参画するＰＤＣＡの効果的な運用記録（活動結果）がある。
ミドル ミドルの状況と活動結果	情報セキュリティに関する活動実績（記録）はない。	情報セキュリティルールが、一部の業務について作成されているが、必要なすべてはカバー出来ていない。	情報セキュリティ対策を実施した記録に、規定された範囲での結果が確認できる。	セキュリティルールを遵守している範囲を明示し、その運用結果を求めに応じて提示できる。	ＰＤＣＡが機能し運用されていることが記録としてある。発生した問題が適切に対処されている。	ＰＤＣＡが機能し運用されている記録の中に、業務改善の成果も確認できる。
ロー（従業員） 従業者の情報セキュリティ対策の意識、行動、ルールの徹底状況	特に情報セキュリティ活動に関して業務実施記録がなくともよい。	周知されたルールにより業務を遂行した記録がある。	ルールが整備されている範囲での業務実施記録を確認できる。	ルールが整備されている範囲での業務実施記録を確認できる。	異常事項も含めてルールに従って適正に業務を実施しており、対処が出来ている。	ＰＤＣＡを運用した結果および実施した改善活動を明確に提示できる。

省略

階層別の評価

分かりやすい表現

参考資料（旧ランク制定表）※抜粋

分類　ランク表示	ランク０	ランク１	ランク２	ランク３	ランク４	ランク５
一般成熟度モデル（０～５）	プロセスが確立していない初期段階（不在）	プロセスは特定のリーダ・技術者に依存している（その場対応）	首尾一貫したプロセスがあるが、標準になっていない	プロセスは標準化され、文書化されている（定められたプロセスがある）	プロセスのＰＤＣＡが確立して是正が行われている	継続的改善、予防活動によりプロセスが最高水準に最適化できている
情報システムの物理的な環境、情報システム運用内容	—	命令指示系統は曖昧で、場あたり的に人に業務を依頼する状況であり、各人の担当作業量は各人でしか把握できない。	中間	各人への業務の依頼状況が書面で管理され、第三者に担当の人間を示すことができる。	中間	仕事のバランスに応じて、適時、担当者の増減を調整した場合にもアクセス権限等が最新化され、適切な業務環境を各人に付与することができる。
ネットワークセキュリティ対策要件、セキュリティ対策要件	—	ネットワーク構築は各業務における必要性に応じて勝手に増設するなど、ネットワーク管理は個人任せ。	中間	ネットワーク構成手続きがあり、書面等により、情報の経路やアクセス制限等、ネットワークのセキュリティ要件を設けていることを第三者に説明できる。	中間	業務等の変化に応じて、適時、ネットワークの要件基準を見直し、且つネットワークの利用状況等を把握して、増強等を実行している
通信システムへの利用、依存度、通信システムの危険性	—	業務に対するネットワーク依存の度合いを明確にしておらず、利用できない場合は各人に対応を委ねている。	中間	業務ごとの切断許容時間を書面等で明らかにし、許容時間に応じたネットワークの代替手続きを整備して実行できる。	中間	ネットワーク切断時の代替や回復の方法を整備し、可能な範囲での復旧手順を整備している。
（紙等物理媒体の）情報取扱いセキュリティ	—	紙の保管や廃棄は各人に任せ、責任者は保管場所や廃棄有無の状況を把握できない。	中間	保管、廃棄の実施手順があり、手順に従って実施をしている。	中間	保管や廃棄の管理は、その対象情報に応じた適切な手順を設けている、また手順に従った保管、廃棄をチェックし、徹底を図っている。
外部委託内容	—	人的関係等による信頼の中で委託をし、委託完了条件等の契約書はないなど、管理者の個人的判断で委託可否を判断している。	中間	開発、保守の作業手順は文書化され、業務中断への許容時間に応じた復旧手順もある。手順に従って実施をしている。	中間	担当者間で手順の共通化が浸透し、また過去の保守作業履歴等から問題点の共通認識や作業の改善が継続的に行われている。

５．今後の課題、進め方

（１）実証実験の更なる充実

従来の受診企業に対する考え方の見直しが発生

受診企業の状況に関するこれまでの前提

- 受診企業にマネジメントシステム規程を策定し運用する体制が確立している。
- 企業の基本業務の取扱いは確立している（業務手順書がある）。

評価・診断の対象企業を再定義

上記の前提を確認し、評価する必要性が発生

- レベルアップしたい意思を持つ中小規模の企業
  - 専門家はおろか、専任者もいないが、何とかしたい、どうしたらよいかと考えている。
  - 情報セキュリティ対策がゼロであっても、対策を考えようという経営者の意向があれば、評価の対象となりえる。
- 顧客に対して、また企業行動として、安心・安全の確認の必要性がある企業
- ＨＰをもち、メールを利用し、ファイルサーバを持つ企業

５．今後の課題と進め方

（２）学会としての研究会の位置付けの見直し

- 多くの企業に適用する方法を検討し、システム監査学会として、今後広く展開したいと考えてきた。

<u>これについては、</u>

- システム監査学会としては、当診断の継続的な実行体制の問題もあり、診断し、認定することはなじまない。
- 監査結果を通じて、コンサルテーションの意味合いを多く持つようになり、システム監査と直接関わらない部分が含まれつつある。

<u>そのため</u>

- 現在、正式なランク付けとしての当診断がおこなわれておらず、実証実験の範囲でとどまっている。
- システム監査学会においては、新たな評価・診断方法の実証実験の場として、確立済みの評価・診断に基づくランク付けは別途、組織を作ることを検討している。

６．今後の課題と進め方

（３）今回の報告以外に検討したこと
① 評価・格付けの実施体制（構想）
　情報セキュリティ対策診断協議会　（コンサル／診断／監査を含む）
情報セキュリティ管理基準等に基づきシステム監査等を実施できるシステム監査人で構成する組織(第２１回大会に「情報セキュリティ監査保証協議会」として検討報告)
② 評価・診断の基準
③ 実証実験　手引書、質問書、誓約書

（４）これからの検討課題　（2011年度）
① 評価・診断方法の推進
② 内容・仕組みの体系化
　「診断手引き書」の整備と、ブラシュアップ
・実際に適用して実施　→　見直し(そのため更に実践が必要)
③ システム監査人の活動の場を拡げる仕組み
　「情報セキュリティ対策診断協議会」の位置付け、審査員選定条件、運用方法、有償化をはかる
④ 既診断企業のフォロー診断によるスパイラルアップ方法　等

募集

- **今年度の当研究プロジェクトへの参加を募集しています。**
  - 課題に対する研究（新しい評価方法の検証）を通じた、セキュリティ監査の勉強。
  - 実証実験を通じた企業とのコミュニケーションの勉強。
  - 原則月１回、研究会合（当会館内の会議室）による様々な立場からの意見交換。

- **対象企業（原則都区内・近郊）の更なる募集をしております。**
  - 情報セキュリティ対策内容を無償で評価します（評価の検討・試行期間中）。
  - 自己では気付かない点について、レポートによる第三者の評価･解説を得られます。
  - 企業が必要とする情報セキュリティ対策を明らかにします。

当研究プロジェクト（連絡先）
主査　　木村　裕一　、尾崎　孝章　まで
（研究プロジェクトへのお問い合わせは、システム監査学会HP
「問合せフォーム」からお願いします。

http://www.sysaudit.gr.jp/toiawase/index.html

参考資料等

＜参考資料＞

- 情報セキュリティ監査基準、同管理基準
- ＪＩＳＱ２７００１　情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項
- ＣＯＢＩＴ ４日本語版（2007年3月）

(注) COBITは、米国IT Governance Institute (ITGI)の著作物であり全ての著作権を有している。本プレゼンテーションでは、その日本語訳（日本ITガバナンス協会訳）を引用している。COBITの日本語訳は日本ITガバナンス協会のウェブサイト経由で誰でもダウンロード可能となっている。
http://www.itgi.jp/cobit/index.html

- 情報セキュリティ対策診断（ＩＰＡ：独立行政法人情報処理推進機構）
組織の情報セキュリティ対策自己診断テスト　～情報セキュリティ対策ベンチマーク～ http://www.ipa.go.jp/security/benchmark/index.html

＜研究プロジェクトメンバー＞　（実証実験参加メンバーはこの一部）（５０音順）

赤尾嘉治　足立憲昭　石渡博一　大井正浩　尾崎孝章　木村裕一　沢恒雄
清水政幸　平真寿美　田附喜幸　玉井学　築島邦男　中山照義　馬場孝悦
林兵江　福田健　福徳泰司　福原幸太郎　牧野豊　村上進司　山下幸三

ご清聴を有難うございます。