●システム監査学会　第24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取組みの評価･格付け　－2

2009年度
情報セキュリティ監査基準･管理基準　研究プロジェクト(*)報告

2010年6月４日
報告者　研究プロジェクト主査　　木村　裕一

（(*)「情報セキュリティ対策の診断　研究プロジェクト」に名称変更）

目次

当報告は２００９年６月研究大会のプロジェクト報告の続きである

1．研究プロジェクトの目的と検討内容

目的：情報セキュリティ監査の活用

（1）問題提起

企業の情報セキュリティ対策の促進と徹底のための、情報セキュリティ監査の活用をどのように行なうか

（2）これまでの経緯

①企業は、その活動のため情報資産に対する情報セキュリティ確保は必須

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。

②企業は実施している情報セキュリティ対策を適切に評価してもらいたいと望んでいる（対応状況がどの程度であるか知りたい）

→ 企業の立場：顧客・社外へアピール・宣言をする

やっていることは正当に評価されるようにしたい

⇒ 改善のために、今後どのようなことをやればよいか知りたい

③システム監査人としてそのために

→ 情報セキュリティ対策実施内容の評価が必要

→ 情報セキュリティ対策を評価する基準を明らかにする

⇒ その基準により格付けを行なう

1．研究プロジェクトの目的と検討内容

④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） がある

情報資産管理： ISMS（JISQ27001）認証制度 がある

「情報セキュリティ格付」： ㈱アイ・エス・レーティングが実施

しかし、これらは中小企業（中堅企業）には負担が重い仕組みである

（対象企業：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業種の、人数で50人程度以下の企業も対象に考えている ）

→もう少し軽く、しかし、考え方は確立したものを検討

（3）具体的検討事項

①企業に必要な対応内容（レベル）を基準として提示しよう

・評価、監査をすることを提案

（その過程で情報セキュリティ監査の活用を図る）

②方法の考え方

・世間に認められる評価基準を参考にした基準を検討

“情報セキュリティ管理基準、COBIT成熟度モデル、JISQ27001”

1．研究プロジェクトの目的と検討内容

（3）具体的検討事項（続き）

③評価対象・方法

・中小企業、中堅企業
・比較的容易に取り組める方法

a）(自身で評価)自己宣言する

・自社のセキュリティ対策内容を統一基準で評価し、格付けに適合していると公表

あるいは

b）システム監査人による評価

・外から第三者が評価する仕組み

④以上の方法を確立させるための実証実験 （③b）システム監査人による評価）

⇒ ＜企業の情報セキュリティ対策の格付け＞の実施

2. 情報セキュリティ対策
評価・格付けの考え方

（1）基本的な考え方

＜企業の必要性に応じた情報セキュリティ対策の実現度合いの評価＞

- 格付け診断する企業の内部統制のレベルを判断する。（継続性）
  これは情報セキュリティ管理基準、COBITの内部統制レベル付け等の考え方を参考にして行なう。

- 当該企業の業種・業務の状況のヒアリング・調査をする。（現状）
  情報セキュリティ対策の必要性を判断し、対策の実施状況と対比し、評価を行なう。

- この2つの結果をつきあわせ評価・格付けする
  ⇒ 当該企業の情報セキュリティ対策の格付けを決める
  ⇒ 診断結果への対応（情報セキュリティ対策に対する提言）

2. 情報セキュリティ対策
評価・格付けの考え方（続き）

①ステップA　企業の内部統制のレベルを評価する（COBITの成熟度モデルを参考にした1～5の5段階） → 評価の結果： A

②ステップB　必要な情報セキュリティ対策の充足度を評価する。
（0～1．0） → 評価の結果： B

③ ①、②の結果を受け、 格付け ＝ A × B （0．5刻み）を★の数（1～5）で表現する。（SS認定（注）とよぶ）

（注）SS（Security Score）認定：★の数（1から5）で表現する。内部統制のレベルと情報セキュリティ対策の充足度から得た格付けの表示

★☆☆☆☆ ～ ★★★★★（半分の表示 ⋆ もあり）

２．情報セキュリティ対策
評価･格付けの考え方

（２）企業が行なう準備　体制と仕組み作り

ａ)･セキュリティポリシ（基本方針）の策定・公表
- ･情報セキュリティ規程の制定（マネジメントシステムの考えを基本とする）
- ･その運用（マネジメントシステムの実践）
- ･情報セキュリティ規程の運用フォロー

ｂ）準備段階におけるシステム監査人の協力(ニーズに応じる）

（３）情報セキュリティ対策レベル　格付け

ａ）評価･格付け方法を対象企業に適用

ｂ）公表・宣言内容・実施状況を評価する
- ･自己宣言のみ　ランク数の★　（ 第三者による評価なし）
- ･第三者評価　　ランク数の★と期間　（第三者による評価あり）※

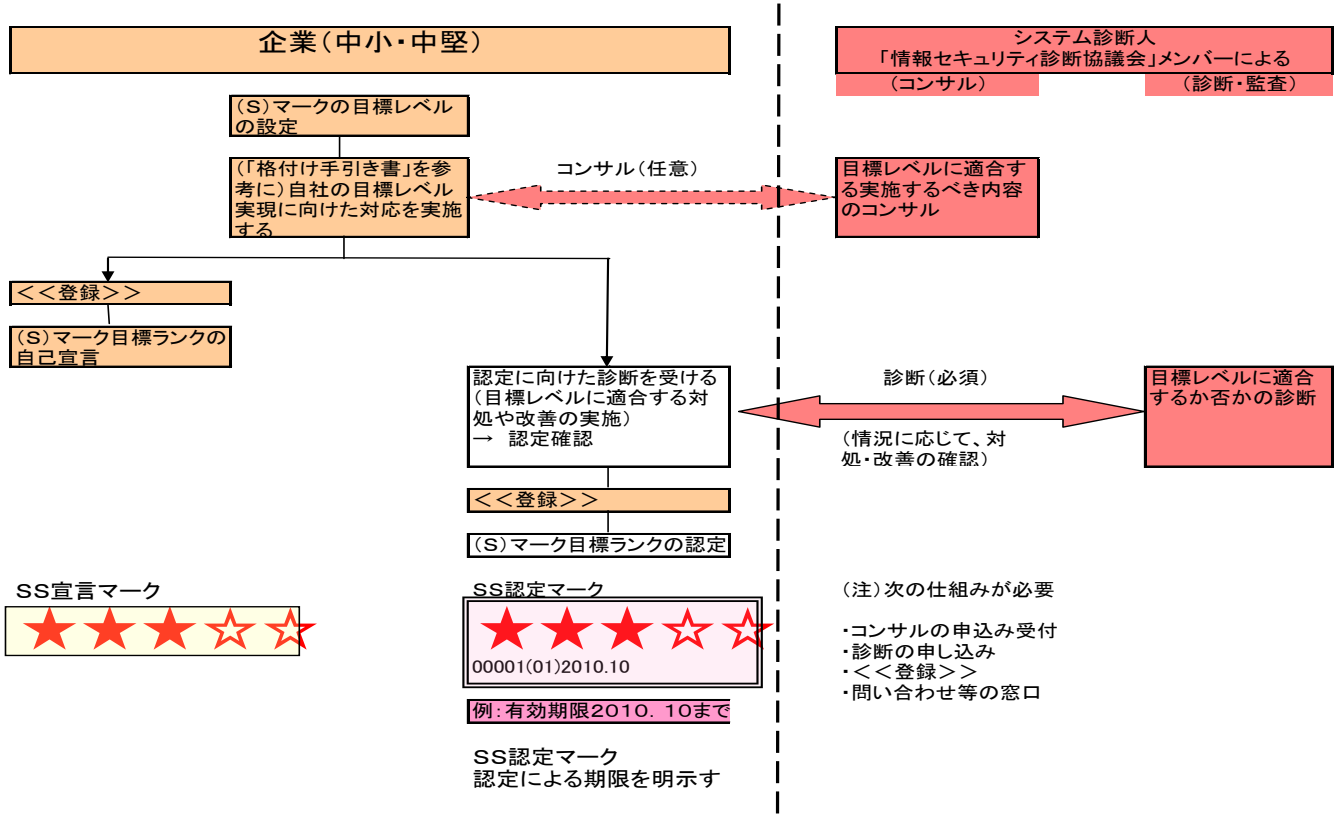
ｃ）情報セキュリティ対策レベルのSS認定結果の表示

※この評価の有無は確実度合いが異なるので、区別して表示する
それを含めた全体のフローは次のとおり

2. 情報セキュリティ対策

評価・格付けの考え方

図：情報セキュリティの格付け　全体のフロー



３．評価・格付けの実証実験

（１） 評価・格付け方法を実地に適用・検証

実証実験の積み重ね→２００９年度１社に対して実施した。

（予備調査を含めて3回の調査による）

- **実施内容を報告書によって紹介する。**
- **課題、今後の進め方を報告する。**

（２）この実証実験を通じて

＜結果＞：

具体的な進め方・手順、質問書などを作成した。

＜課題＞：

実施対象はまだ少なく、今後広く適用させる方法などが課題である。

異なる情報セキュリティ環境の企業を対象に検証する方法は、実施しながら確立させる必要がある。

3．評価・格付けの実証実験

（3）格付けの方法

	机上検討	実証実験(企業）において
情報セキュリティポリシー	①　企業による情報セキュリティポリシの宣言 セキュリティポリシでは、企業が行なう対策内容を明確にする 情報セキュリティポリシの雛形	①情報セキュリティポリシーは、個人情報保護方針として設定済み （昨年度からの変更点） セキュリティポリシの公表・宣言は、一般企業では基本方針のみで、対策基準の公表までは求めない。
評価方法	②　スライド7の方法により格付けする ただし、実施に当たっては次を検討する ・具体的手順 ・質問項目への展開 ・調査結果の報告様式（報告書雛形） ③回答者の立場による考え方の差を評価	②左記のとおり、実施 ③また、IPAの**情報セキュリティ対策自己診断テスト（ベンチマーク）**を立場の異なる3名の方に実施してもらい、その結果も評価の参考にした。 IPA：独立行政法人情報処理推進機構

4. 実証実験結果

報告書内容（ 目 次 ）

Ⅰ. 本編 「情報セキュリティ対策診断報告書」 （内容は雛形である）
 1. 実施概要
 2. 診断所見
 3. 診断結果
 4. 診断結果のレーダーチャート
 5. 診断結果への対応
Ⅱ. 添付資料
 1. 業務
 2. 業務遂行の状況

報告書はⅠ.本編とⅡ. 添付資料からなり、Ⅱは企業との認識合わせのため、確認した内容を簡単に纏める（ここでは省略）

4. 実証実験結果

本編　　1. 実施概要　　2. 診断所見

1. 実施概要

研究プロジェクトは IX株式会社 の依頼を受けて、情報セキュリティ対策についての診断を行ないましたので、報告します。

(1)診断対象組織

業種･業態：情報サービス産業、システム設計･開発他

個別診断対象のテーマ：内部統制

2. 診断所見

(1)マネジメントシステム診断

(2)個別診断対象のテーマ：内部統制

(3)情報の取扱い状況診断

(4)情報セキュリティ運用･定着診断（実施作業･記録）

4. 実証実験結果

本編　　2. 診断所見（続き）

（1）マネジメントシステム診断 （ステップA）

- 情報セキュリティを中心とした一般成熟度モデルの考え方からみて、貴社の位置づけは　１．０　である。

- これはCOBITの一般成熟度モデルの考え方を参考にし、情報セキュリティ対策に関する視点を加えて評価したものである。その考え方は、Ⅱ 添付資料で表A1－1，表A1－2 に示す。（なお、3レベルは業界平均レベル）

4. 実証実験結果

本編　　2. 診断所見（続き）

（2）セキュリティ対応必要性とその対応充足度　（ステップB）

- 8つのセキュリティ検討軸（次ページ1~8項）の必要性、充足度のランクにより評価する。

貴社では8つのセキュリティ検討軸のうち、
4項の“情報システムへの利用、依存度、通信システムの危険性”、
8項の“教育”（教育の実施、従業員の説得性、信頼性)等
において脆弱性が見られる。

総合的な対応状況充足度は後に示すように 0. 89 である。
（この評価の考え方は、Ⅱで〔表BB－1〕に示す。）

4. 実証実験結果

本編　　2. 診断所見（続き）

（3）セキュリティ検討軸

1. 取り扱う情報の性質、情報量
2. ①情報システムの物理的な環境
   ②情報システム運用内容
3. 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
4. 通信システムへの利用、依存度、通信システムの危険性
5. （紙等物理媒体の）情報取扱いセキュリティ
6. 外部委託内容、外部委託の範囲
7. 情報システムの開発、保守、アプリケーションシステムの信頼性
8. 教育（ルール、役割の周知徹底）、従業員の流動性、従業員の信頼性、従業員の絶対数

4. 実証実験結果

本編　　3. 診断結果

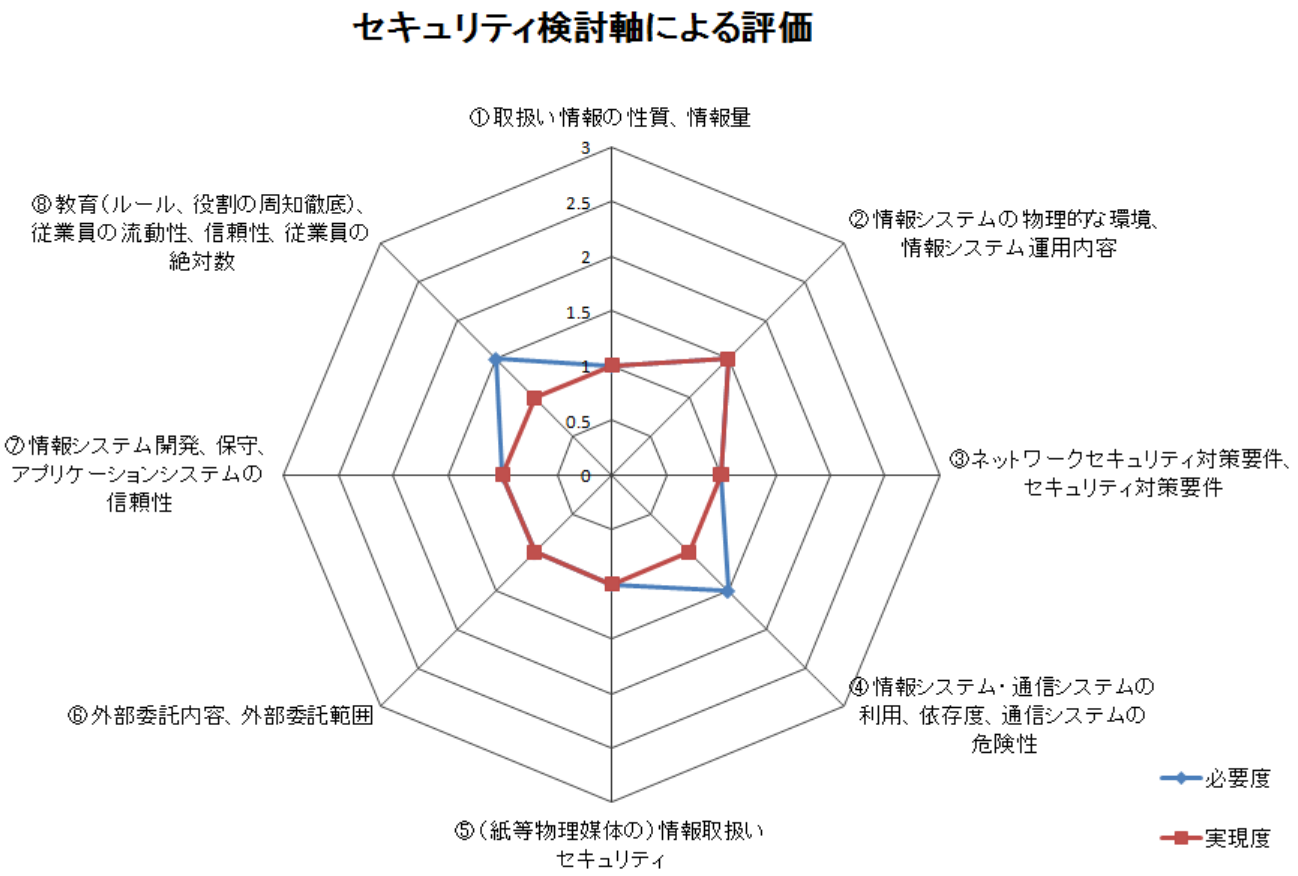
- 診断結果

診断結果	★☆☆☆☆	（1．0）

- 企業の内部統制評価：1．0
  ①一般成熟度モデルに関して：1．75
  ②マネジメントシステム実施状況評価：1．0
- 情報セキュリティ対策の充実度：0．89

4. 実証実験結果

本編　4. 診断結果のレーダーチャート



4. 実証実験結果

5. 診断結果への対応（提言）

◆評価

①規定化が十分でない。マネジメントシステムが継続的に運用されることが体制面、規程面で確認できない。

②情報セキュリティ環境面の安全性確保、計画に基づく教育実施と、記録による確実化が必要

◆具体的な対応

①規定を整備する。例えば、情報資産管理規程、監査規程、マネジメントレビュー規程、文書管理規程、教育規程

②体制（責任と権限）を明確にする

③運用記録を残す

5. 情報セキュリティ対策の評価・格付けの特徴

（1）評価・格付けの対象企業

情報セキュリティに関して、次のような企業

- レベルアップしたい意思を持つ会社（関心がある）、何とかしたい、どうしたらよいかと考えるところはどこでも
- 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、評価の対象とできる。
- 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
- HPをもち、メールを利用し、ファイルサーバを持つ企業であれば、どこも対象にできる

- 情報セキュリティ対策方針が未策定の企業もある。そのレベルから対象に含める。対策方針策定の指導も含めることが必要である。

5. 情報セキュリティ対策の評価・格付けの特徴

（2）我々の取組みの目標

- 企業が、容易に安価に情報セキュリティ対策の現状把握が出来る
- ゼロからのスタートが出来る (取組みが容易）
  一言で言って「ゼロからスタートできるセキュリティ評価、格付け」
- レベルアップの方向、目指すべきところを見極められる
  要望により、コンサル対応も行なう。

(注）（他の方法は相応の準備と、費用が必要、結果は0か1かである）
この（1）（2）を実現させるため以降を進めてゆく。

（3）企業自身による格付け評価を可能とする

①企業自らが評価できるよう、格付け評価基準を「格付け手引き書」として当研究会で作成・公表する。

②企業自身が、対応体制評価、対応充足度評価を行なう。
その結果をもって“SS宣言”（（S）マーク公表）を行なう。

③評価資料、結果はSS認定の証拠として企業が保管する。

④自己宣言の維持のため、企業は定期的見直しする。

5. 情報セキュリティ対策の評価･格付けの特徴

（4） 第三者による評価（評価基準による診断･監査）

①企業からの要望に応じて（監査人が）診断、コンサル、監査を行なう

・ 情報セキュリティ監査保証協議会（＊→6項）による診断･コンサル

・その意義ー情報セキュリティ対策内容、企業の独自解釈によるレベルの違いを是正
ー第三者による確実性ある解釈、判断を行なう等

② 診断･監査を行えるように「格付け手引き書」を整備
（監査人は診断･監査どちらでも実施できるようにする）

・監査は保証型監査の内容を考える（一定期間仕組みが継続機能要）

（5）格付けレベルの公表と管理 (課題)

①格付け結果を登録、公表する。
登録･認定を考えているが、この仕組みは未定

5. 情報セキュリティ対策の評価・格付けの特徴

（6）前回対象企業による感想と今回の対応

- 課題
  報告書を中心に分かりやすい方法、内容にする必要がある。（中小企業・中小規模を対象にする場合の重要なこと）
- 経営者の望むところ ⇒ 改善のためのコンサルを望む
  (他社の例、良い例の紹介など）
  報告書では改善の筋道を示して欲しい

⇒ 課題への対応

- 報告書の構成を分かりやすい構成に改訂
- 企業として整備が必要な規程体系、名称等を提示
- ステップAの評価結果が1～2に偏る。（別なインセンティブのある指標も共に用いる必要があるか）

６．検討したこと／これからの検討課題

（１）検討したこと（検討中含む）

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格付け基準

③実証実験　手引書、質問書、誓約書

（２）これからの検討課題　（２０１０年度）

①内容・仕組みの体系化

「格付け手引き書」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）

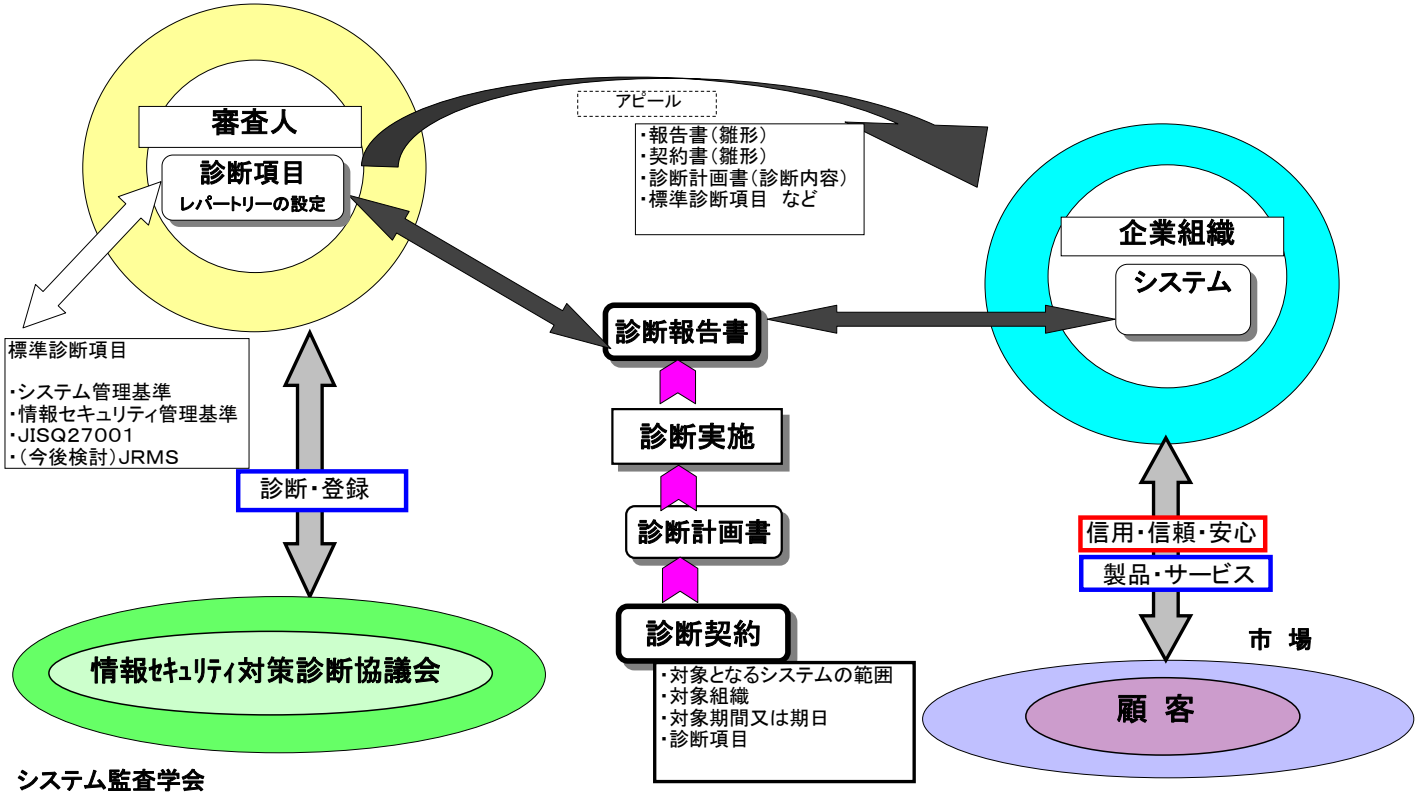
②システム監査人の活動の場を拡げる仕組み

「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

③既診断企業の再評価によるスパイラルアップ方法　等

6. 検討したこと／これからの検討課題

「情報セキュリティ対策の診断」の枠組み



診断実施を推進する
（診断をアピールする仕組み）

- 今後この診断を推進するための、具体的な改善提案や診断実施効果をアピールする仕組みづくり

①診断企業に分かりやすい評価基準

②情報セキュリティ事故による影響（取引き停止、売上減、賠償、対応工数等）を認識してもらう

③情報セキュリティ対策規程体系の提示

④「JRMS2010」（リスクマネジメントシステム（注））の質問項目等の利用

（注）JIPDECに設置されたリスク評価指針検討委員会が2010年5月発表

など

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。
  まだ課題があるので、一緒に研究を進めたい。
- 原則月１回夜間の研究会合を中心にすすめています。
  当機械振興会館内の会議室にて開催
- 対象企業の更なる募集

当研究プロジェクト（連絡先）
主査　　木村　裕一　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 情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムー要求事項

・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 簗島邦男 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。

＜参考＞
報告書添付資料．格付けの方法と評価基準

添付資料１　ステップＡ　企業の内部統制について
添付資料２　ステップＢ　必要な情報セキュリティ対策の充足度
添付資料３　IPAのベンチマークテストによる結果から
添付資料４　会社概要・業務概要と取扱情報（評価の背景）

＜参考＞添付資料1

1．ステップA 企業の内部統制のレベルを求める。

- 表A1－1：一般成熟度モデル
- 表A1－2：成熟度属性表（表A1－1をさらに補足）
- 表A2－1：情報セキュリティマネジメントシステムの実践状況（略）
- 表AA　：体制評価

に纏める。

＜参考＞報告書Ⅱ. 格付けの方法と評価基準

ステップA 表A1－1 一般成熟度モデル

表Ａ１－１：一般成熟度モデル

判定 ＊：○（クリアしている、もっと良い）、×（それ以外）

#	一般成熟度モデル 説明および質問	判定＊ 左記の質問、説明以上を○とする	基準	判定コメント 貴社に関する評価、判定の根拠、状況などを記載
1 （0）	＜0＞コントロール不在 ①マネジメント層がサービスの定義プロセスの必要性を認識していない。 ②組織がＩＴセキュリティの必要性を認識していない。 ③セキュリティを確保するための実効責任および説明責任が割り当てられていない。 ④ＩＴセキュリティ管理を支援する対策が実施されていない。 ⑤ＩＴセキュリティに関する報告およびＩＴセキュリティ違反発生時にとるべき対応プロセスが存在しない。 ⑥システムのセキュリティ管理プロセスと呼べるようなものが全く存在しない。	全て○	次の（1）の確認へ	左記事項には「情報セキュリティ規定」にて定めている。特に問題なく、質問事項はクリアできる。
（1）	＜1＞コントロール初期／その場対応 ①組織がＩＴセキュリティの必要性を認識している。セキュリティの必要性に関する意識は、主として個人に依存している。 ②ＩＴセキュリティへの取り組みは爾後対応という形である。 ③ＩＴセキュリティの成果測定は行なわれていない。 ④責任の所在が明確でなく、ＩＴセキュリティ違反が発見された場合、責任のなすり合いが起こる。 ⑤ＩＴセキュリティ違反への対応は予測できない。	①（○） ②（○） ③（○） ④（○） ⑤（○）	全て○→次の（2）の確認へ	特に問題なく、質問事項はクリアできる。会社としての意識は高い。 ③についてはこれまで必要性はなく、今回の診断が最初となる。 ⑤小規模の企業で、社長および幹部により全体を把握しているとの回答があった。 全般に適用する規定として「情報セキュリティ規定」がある。ただ、会社規定としてその策定が正式な手順（文書規定がない）に則らない、周知徹底に不十分さが残る。
（2）	＜2＞再現性はあるが直感的 ①当該企業の業務内容に相応した業務手順が統一化されている部分がある。しかし、手順書の整備が（必要な）全業務には亘っていない。 ②出来ている手順書について積極的、徹底的な教育、研修、訓練はまだ行なわれておらず、知識、技術の共有化が出来ていない。 ③手順書に従うか否か個人任せ。 ④業務上の誤り、事故は時々ある。	①（△） ②（○） ③（○） ④（○）	一部△はあるが、次の（3）の確認へ	①業務手順はあるようだが、手順書としての整備は確認できない。「情報セキュリティ規定」以外に重要な規定が整備されていない。 ②積極的に教育･研修を行なっているようであるが、徹底的･体系的な状況ではない。

＜参考＞報告書Ⅱ．格付けの方法と評価基準

ステップA 表A1－2 成熟度属性表

評価＊各項５～１の判断：

５：(満たしている+)　４：(満たしている)　３：(満たしているー)　２：(満たしていない)　１：(不充分)　－：非該当

	成熟度属性項目（視点）											
段階	認識および周知	＊	ポリシー、標準、および手続	＊	ツールと自動化	＊	スキルと専門知識	＊	実行責任および説明責任	＊	達成目標の設定および成果測定	＊
２ あるべき状況	対応の必要性が意識されている。 経営層は、全体的な課題について周知している。		類似した共通のプロセスが採用され始めているが、個人の専門知識に依存しており、大部分において直感的である。 個人の専門知識により、プロセスのいくつかの局面は再現可能である。ポリシーと手続の一部が文書化されているか、非公式であるが認識されている場合がある。		ツールの使用に関する共通のアプローチは存在するが、主担当者が作成した対応策を基にしている。 ベンダーツールが入手されていたとしても、主担当者が作成した対応策をもとに使用されている。 ベンダーツールが入手されていたとしても、正しく適用されていない場合や、使用されていない場合がある。		重要な領域に関するスキルの最小要件が特定されている。 研修は、合意のみの計画に沿って形ではなく、必要に応じて行なわれており、実地での非公式な研修が行なわれている。		責任に関する公式な合意が得られておらず、個人が各自の実行責任を想定し、説明責任を負っているものと認識されている。 問題発生時には実行責任に関する混乱が生じ、責任転嫁が発生しがちである。		達成目標の設定が多少行なわれており、いくつかの財務対策が作成されているが、経営幹部にのみ周知されている。特定の領域のみにおいて、一貫性の無いモニタリングが行なわれている。	
貴社の状況と評価	貴社開発業務は顧客の人事・総務関連のソフトウェアであるため、そこで扱う情報は顧客の生データである。このようなデータ取扱いの重要性を社員に幹部から直接(同一プロジェクトで)伝え意識教育している。周知のツールとしてＧＷ（グループウェアペンギン）を利用している。従業員は十分認識していると思われる。	4	情報セキュリティポリシー、業務標準はこれまで幹部から直接従業員に伝えていたために文書化、標準化などは後回しになって不十分であった。今回の診断を機に整備し始めた。プロセスの広がりは限定的で再現可能と思われる。	3	開発業務用としてマンティスを補助ツールとして独自に利用している。また、クライアントＰＣに情報を残さないなどの対応を標準にしている。 ただ、自動化には今のところ該当しない。まだその明確な必要性がない。	3	従業員はすべて入社時に業務スキル要件を満たす者が採用されている模様である。したがって業務およびセキュリティに関しての専門知識の研修は実地での非公式な研修が主体である。他にＣ社と合同でセキュリティ教育を実施している。	4	少人数の企業で社長自身が情報保護統括責任者を務めるなど、現場と管理層の乖離はない状況であり、責任の認識で問題はないものと判断できる。	4	達成目標の設定という点では不透明であり、ビジネス達成目標の明確な設定は存在することが認められなかった。一般消費者を対象とするＡＳＰサービスなどの計画もあるようだが、きちんとした目標になっているかも不明確である。	3

＜参考＞報告書Ⅱ. 格付けの方法と評価基準

ステップA 表AA 体制評価点

表ＡＡ による評価は、ステップ Aの結果を纏め、企業の内部統制を求めるものである。
企業の内部統制Aの値は貴社の状況を、一般成熟度モデル → マネジメントシステム実施状況 順に評価する。
表ＡＡによって、条件を満たす体制評価点として、該当する数値の中の最低値を採用する。
表ＡＡ：体制評価点 （表頭：表Ａ１－１、表側：表Ａ２－１の判定を適用）

今回の評価結果

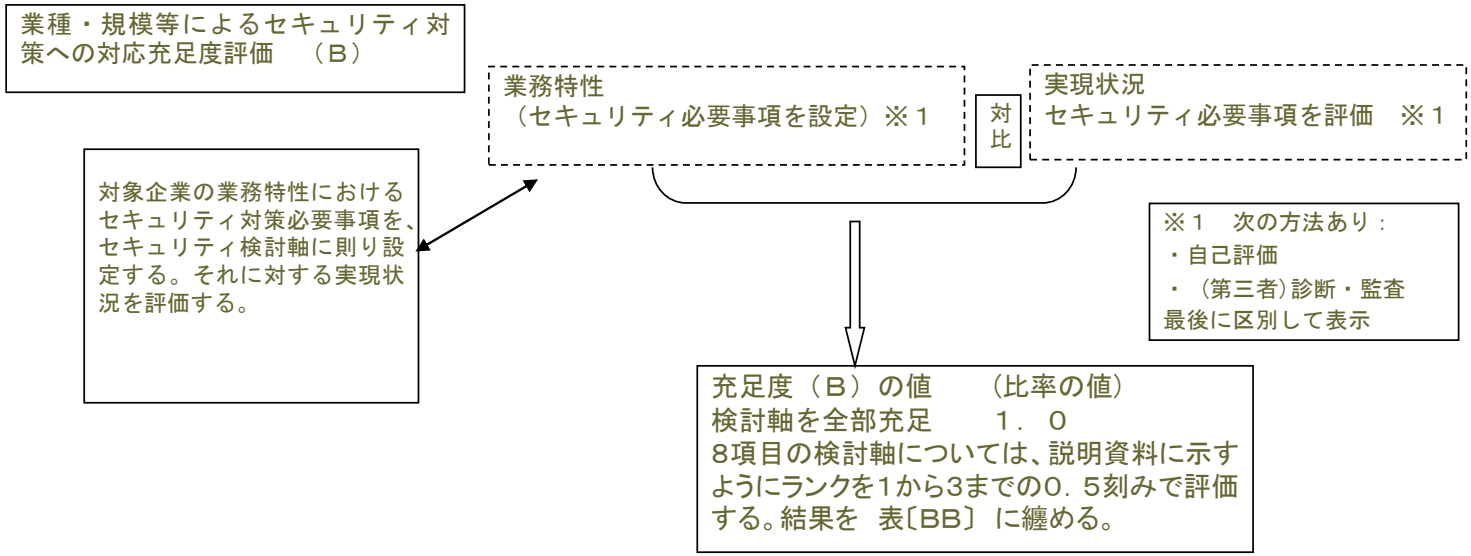
格付けの		格付け対象外	格付けに値する成熟度モデルの範囲				
マネジメントシステム（ＭＳ）実施状況	ＣＯＢＩＴ一般成熟度モデル	0 不在	1 初期／その場対応	2 再現性はあるが直感的	3 定められたプロセスがある	4 管理され、測定が可能である	5 最適化
体制整備（整備＝機能していること）	不十分	—	—	—(ありえない)	—(ありえない)	—(ありえない)	—(ありえない)
	軽度の不備	—	1	1	3	4	4
	整備	—(ありえない)	—(ありえない)	2	4	5	5
規程整備	不十分	—	—	—(ありえない)	—(ありえない)	—(ありえない)	—(ありえない)
	軽度の不備	—	—	1	3	4	4
	整備			2	4	5	5
ＰＤＣＡサイクルの運用実施	１廻りがまだ	—	—	—	—(ありえない)	—(ありえない)	—(ありえない)
	１回り	—(ありえない)	—(ありえない)	１－２	１－２	２－３	３－４
	複数廻り実施	—(ありえない)	—(ありえない)	１－３	３－４	３－５	４－５
監査、法令順守	曖昧な実施	—(ありえない)	1	1	1	—(ありえない)	—(ありえない)
	適格な実施	—(ありえない)	—(ありえない)	3	３－４	３－５	４－５
体制評価点		———	表ＡＡの値を得る。＝１				

＜参考＞報告書Ⅱ．格付けの方法と評価基準

（2）企業の対応体制評価 ②評価点(B)を求める

（3）対応充足度評価(B) ①考え方

- **表BBによる評価は、それぞれの企業における（業種・規模等による事情を考慮した）情報セキュリティ対策の必要性を把握し、その対策に対する充足度を求める。**



＜参考＞報告書Ⅱ．格付けの方法と評価基準

(2)企業の対応体制評価

業種･規模等による情報セキュリティ対応の評価

表ＢＢ　業種・規模等による情報セキュリティ対応の評価

＊＊：ランク３までの枠内に貴社のランクを　で示す。リスクの度合いは　ランク１＜ランク２＜ランク３

No.	セキュリティ検討軸（＊）（これに対する対策内容を見る）	必要性状況 問診による貴社の情報セキュリティ対策を必要とする業務、情報システム、環境等の背景	実施状況 貴社が情報セキュリティ対策に関して実施している対策内容と根拠事項 （審査側から見た結果）	残存リスクの状況、許容度	必要度判断ランク（＊＊）	審査による実現状況評価 実現度ランク	充足度評価（差分）
①	取り扱う情報の性質 情報量	・委託元（顧客）から預かる個人情報はなく、法人情報は1000件以内であること。 ・機密度の高い個人情報や金融情報等を処理することはないこと。	・個人情報は取引先（300件）、自社社員に限定される。これらを電子データ、あるいは紙媒体として事務所内で利用、保管する。 ・テストデータは自社で生成し、実データの取得はない。プロジェクト毎に取引先との契約に基づいてデータを消去している。顧客構内での機密情報の扱いは契約書で定める。 ・情報セキュリティ方針で、預かり情報を特定することを決めている。ただし、特定する手順は定めていない。	・方針に則った、機密情報の特定を実施していないため、左記に確認した情報以外が社内で認識なく管理されている可能性が残る。ただし、取得する情報を限定しているため、現時点ではその可能性も低く、許容範囲。	必要性状況をステップBの質問票から判断する。 3 2.5 2 1.5 1	3 2.5 2 1.5 1	0
②	①情報システムの物理的な環境 ②情報システム運用内容	・従業者数が限定され、社長の目の届く範囲で、集中的、独立的管理が可能であること。 ・関係者は固定され、容易に特定できること。	・社内開発はヒアリング時には２名が実施。開発用サーバはなく、自社のクライアントＰＣで開発し、データはファイルサーバで管理する。深夜残業等はなく、一人での単独作業はない。 ・ファイルサーバはNAS型のハードディスク。机上に設置している。 ・社外開発では、セキュリティ環境は委託元の環境に依存（自社より厳しい）。自社からの持ち込みはない。 ・フロア解錠のICカードは毎月の棚卸をしている。	・第三者の入室はできないため、リスクは限定的であるが、他社とフロアを共有し、他の社員が行き来する通路から見える（近い）位置に、全情報（NASサーバ、バックアップ用USBメモリ）を机上に置いていることは、情報漏洩等の危険性を認識した管理記録を残す仕組みが必要である（業務を委託する顧客の立場で考える）。	3 2.5 2 1.5 1	3 2.5 2 1.5 1	0