●システム監査学会　第23回研究大会
研究プロジェクト　発表5

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

2008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

2009年6月12日

報告者　研究プロジェクト主査　　木村　裕一

目次

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うか

（2）これまでの経緯

①企業活動のために、情報資産に対する情報セキュリティ確保は必須
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る。

②企業は実施している、また対応を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

→　顧客・社外へアピール・宣言をする
（企業の立場：やっていることは正当に評価されるようにしたい）

→　対策実施内容の実効性の評価の基準が必要

⇒　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

③評価方法

個人情報保護に関しては プライバシーマーク認定制度（Pマーク）がある

情報資産管理に関しては ISMS（JISQ27001）認証制度がある

しかし、中小企業（中堅企業）には負担が重い仕組みである

→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、中堅企業にとって比較的容易に取り組める方法

a）自己宣言する仕組み(自身で評価)

・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）の内容）

⇒＜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。
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。
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る
⇒ 当該企業の情報セキュリティ対策の格付けを決める

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

（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★　（第三者による保証なし）
- ・第三者評価　ランク数の★と期間　（第三者による保証あり）※

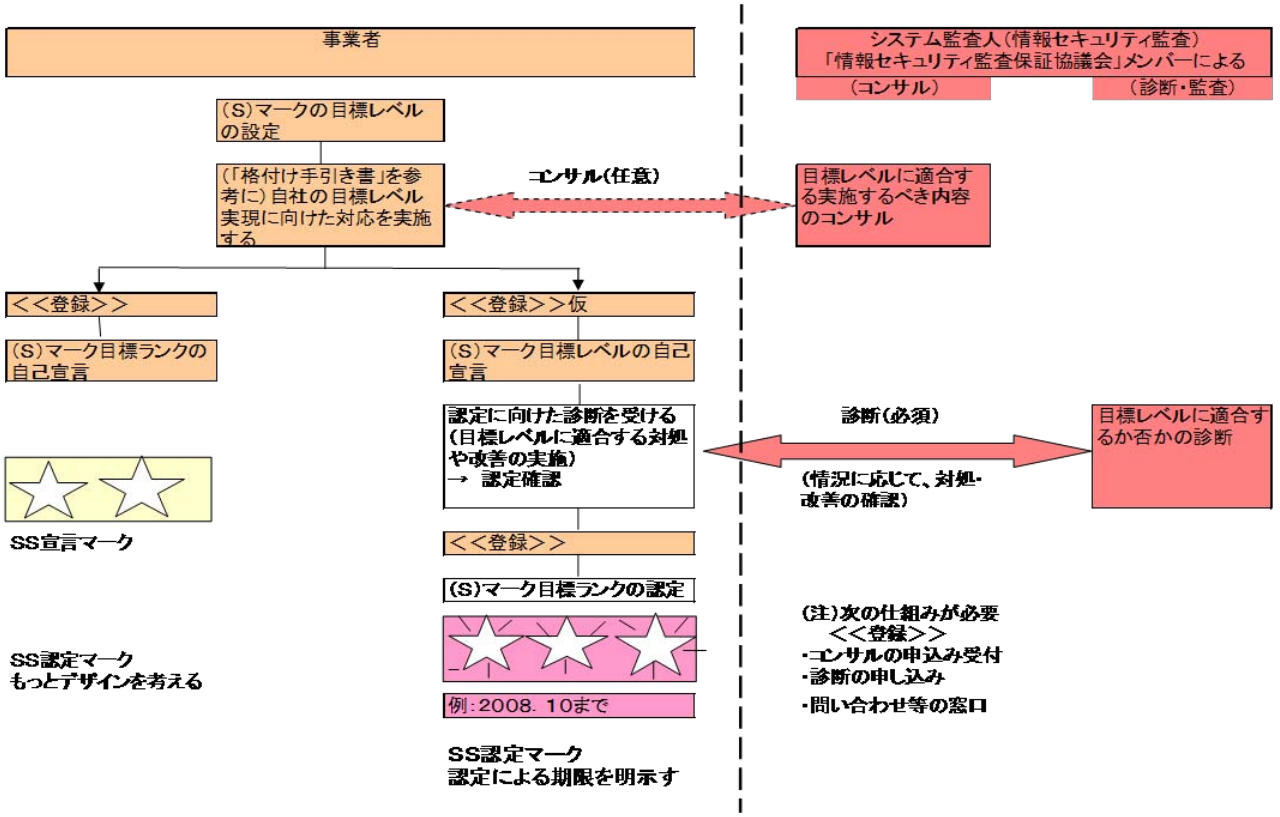
c）情報セキュリティ対策レベルのSS認定結果の表示

※この保証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 （登録・認定）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

机上での検討のみでは限界がある。→実施した

- 実施内容を報告書（内容は変更）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が、

＜課題＞：

実施対象がまだ1社であり、異なる情報セキュリティ環境の企業を対象に検証すること、広く適用させる方法などの今後の課題がある。

3. 評価・格付けの実証実験

(3)格付けの方法

机上検討(昨年度)	実証実験において
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 ①'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、対策基準の公表は求めない。(昨年度からの変更点)
② (当研究による)格付け評価基準による評価方法 (a)、b)の結果を組み合わせて格付けを決める) a) 企業の対応体制のレベル (A) 成熟度モデルのレベル/マネジメントサイクルの実践状況 b) 情報セキュリティ対策への対応充足度評価 (B) 業務・規模による対策必要事項と対応実現状況を対比	②左記のとおり、実施 ただし、次を検討しつつ、見直し ・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また、今回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)を企業内で立場の異なる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

3. 評価・格付けの実証実験

実証実験の経緯（内容と直接な関係は無い）

時期	内容		
	右の定例会、打ち合わせの他、各自の検討、メール	定例会 検討会	対象企業との 面談・調査
2008年11月から12月	・対象企業の決定と打ち合わせ	定例会	1H
2009年1月から2月	・予備打ち合わせ、予備調査、 一部資料の受領	定例会	1H
2月	・調査のための検討、 審査員打ち合わせ	定例会 臨時検討会	
2月、3月	・予備調査資料の作成		
3月	・企業調査、および調査調書に基づく整理	定例会	2．5H
3月	・報告書の整理、確認		1H
3月	・調査結果の報告		

4. 実証実験結果

報告書内容（ 目 次 ）

目次、構成は同じであるが、内容は雛形である

はじめに　（注）目的、格付け方法の説明（ここでは省略）
Ⅰ. 総評
Ⅱ. 評価結果の詳細
　1. ステップA 企業の内部統制のレベル
　2. ステップB 必要な情報セキュリティ対策の充足度
　3. IPAベンチマークテストによる結果から　（ここでは省略）
Ⅲ. 評価の背景（貴社の業務と情報システム）
　1. 業務　（注）確認した内容の概要を認識合わせの
　2. 業務遂行の状況　ため簡単に纏める（ここでは省略）

４．実証実験結果
報告書ー１　　Ⅰ．総評

１．格付け評価結果（報告書）

２００９年１月から２月に実施した貴社　株式会社〇〇〇〇の情報セキュリティ対策格付け評価の結果：

認定診断方法による　SS認定マーク：★★ ⋆

（格付けのレベル内容についてはⅡ．１項（ステップA　企業の内部統制のレベル）に記載する。）

２．一般成熟度モデルの考えに基づく貴社の評価

格付けは企業の内部統制のレベルと、情報セキュリティ対策の必要性と充足度によって評価する。

４．実証実験結果
報告書ー２　　Ⅰ．総評

（１）企業の内部統制のレベル （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　２．５レベル　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す。そのレベル付けの考え方は、Ⅱ項で表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
報告書ー３　Ⅰ．総評

（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）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、
②の“情報システムの物理的環境、運用内容”、
⑥外部委託内容、外部委託範囲のセキュリティ
において脆弱性が見られる。

総合的な対応状況充足度は次のページに示すように　０．９１である。
（この評価の考え方は、Ⅱで〔表ＢＢ－１〕に示す。）

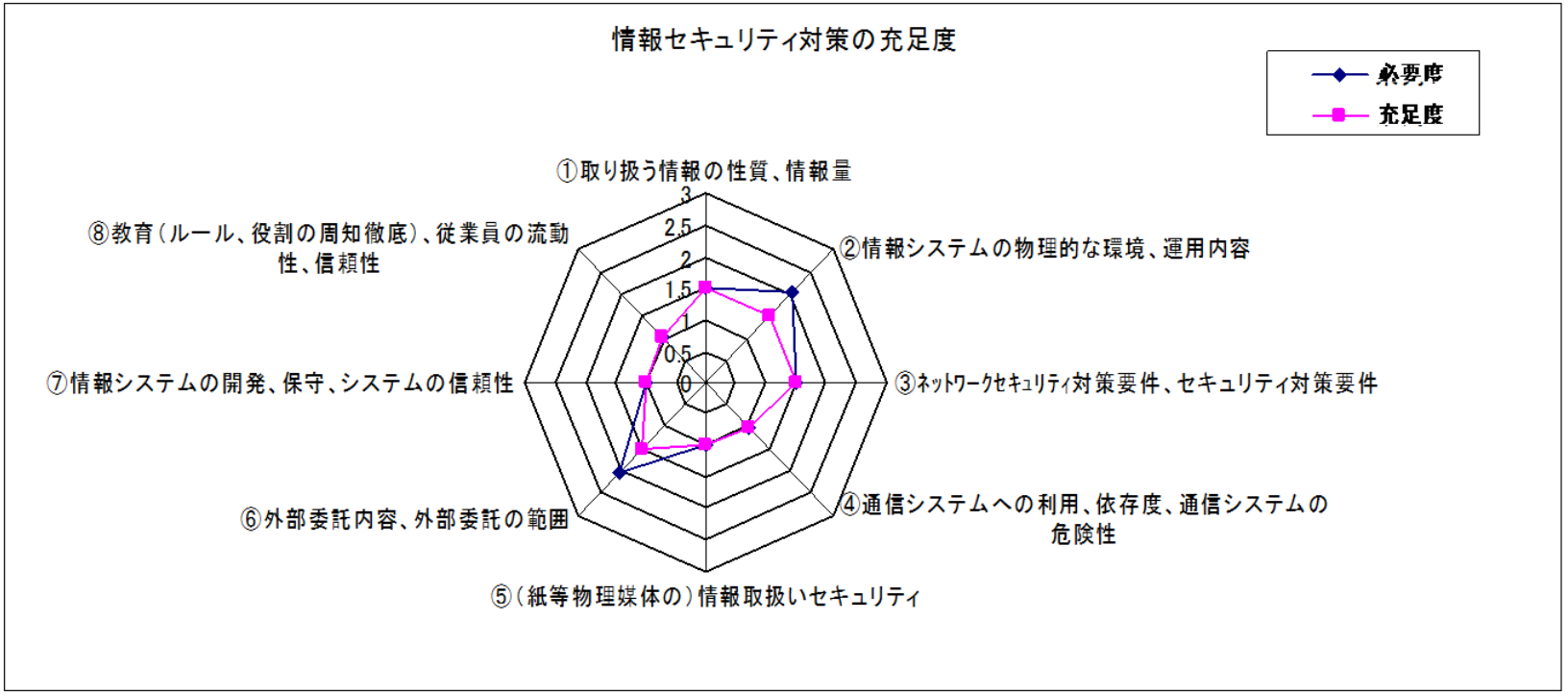
４．実証実験結果
報告書―４　　Ⅰ．総評

- 情報セキュリティ検討軸による評価　　必要度 ： 充足度
  （ランクは１～３（０．５刻み））　　ランク　　ランク

①取扱う情報の性質、情報量	１．５	１．５
②情報システムの物理的環境、運用内容	２．０	１．５
③セキュリティ対策要件	１．５	１．５
④通信システムの利用、依存度、危険性	１	１
⑤（紙等物理媒体の）情報取扱いセキュリティ	１	１
⑥外部委託内容、外部委託範囲のセキュリティ	２．０	１．５
⑦情報システム開発、保守、信頼性	１	１
⑧教育、従業員の役割、信頼性、従業員の流動性	１	１
①～⑧　対応状況充足度総合判定	１	０．９１

4. 実証実験結果

報告書ー5　Ⅰ. 総評



４．実証実験結果

報告書ー６　Ⅰ．総評

（３）格付け評価

貴社のSS認定マーク（星の数）

＝ Ａ×Ｂ ＝ ２．２７５（＝ ２．５ × ０．９１）

（１、２、２～５は0.5刻み））

＝ ★★ ⋆

（評価幅：５＝５～４，７　４．５＝４，７未満～４，２

４＝４，２未満～３．７ 、、、、）

４．実証実験結果
報告書ー7　Ⅰ．総評

格付評価結果から見た情報セキュリティ対策に対する提言

- 貴社の情報セキュリティ対策の必要性充足度は、表〔BBー１〕に示す０．９１と高く評価できるが、その中で貴社の対策の現状は　2つの分野（②“情報システムの物理的環境、運用内容”、　⑥“外部託内容、外部委託範囲のセキュリティ”分野）において脆弱性が　見られる。
- ただ、当面緊急に必要な対策は特にない。
- 現状、これらの対応が十分でないために、　〇〇〇〇〇〇の脅威に対して弱い点があり、リスクとして□□□□　　□□□□　の状況がある。
- 顧客情報を扱う事業者としては、事務所内の更なるセキュリティレベルの向上のために□□□□　　□□□□を図ることが望ましい。
- 現状、これらの対応が十分でないために、　外部からのアクセスの脅威に対して弱い点があり、リスクは低いが顧客の機密情報、個人情報の漏洩　リスクがある。
- 顧客情報を扱う事業者としては、事務所内の更なるセキュリティレベルの向上のために事務所内の４S（整理、整頓、清潔、清掃）の導入を図ることが望ましい。

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

- 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
- 顧客に対して、また企業行動として、安心・安全の確認 (必要性がある)
- 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

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

- 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。そして、安価に現状把握が出来、レベルアップの方向を見極められる
（他の方法はそこそこの準備と、費用が必要、結果は0か１かである）
- 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
- セキュリティ対策の現状、目指すべきところを明らかにする。
要望により、コンサル対応も行なうも。

- この（１）（２）を実現させるため以降を進めてゆく。

５．情報セキュリティ対策の評価・格付けの特徴

（３）企業自身による格付け評価

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。

更に評価の確実性向上のために、次を考える。

⑤システム監査人による評価・診断あるいは監査を依頼する。

⑥ 評価した結果は、認定済みとして公表する。→（４）

５．情報セキュリティ対策の評価・格付けの特徴

（４） 第３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、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（ー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

①格付け結果を登録、公表する。

②宣言内容は定期的に見直しする。

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）

情報セキュリティ監査保証協議会 (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回に報告）

②格付け基準

③実証実験　手引書、質問書、誓約書

（２）これからの課題 （ ２００９年度　今年度の予定）

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求める運用の仕組み 「情報セキュリティ監査保証協議会」の位置付け、審査員、運用方法、その他

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（学会ニュースでの募集）

当研究プロジェクト（連絡先）

主査　木村　裕一　(info@sysaudit.jp)

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/download / を参照されたい

・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）

赤尾嘉治 足立憲昭 石渡博一 大井正浩 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 （50音順）

ご清聴を有難うございます。

＜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　　①評価点(A)を求める

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　　：体制評価点　　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

#	レベルの説明および質問	判定＊ 左記の質問、説明以上を○とする	基準
1	＜レベル０＞コントロール不在		
（１）	①マネジメント層がサービスレベル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。	①（○） ②（○） ③（○） ④（○） ⑤（○） ⑥（○）	全て○→ 仮レベル＝０とし、次の＃（２）へ
（２）	＜レベル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顧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○→ 仮レベル＝１とし、次の＃（３）へ
（３）	＜レベル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（○）	全て○→ 仮レベル＝２とし、次の＃（４）へ
（４）	＜レベル３＞定められたプロセスがある ①業務手順書、マニュアルが標準化され周知されている。（技術、ノウハウの共有化→外部委託分について把握し、管理している） ②業務遂行で標準化に従うか否か、業務管理は各自が判断して行う。 ③標準化された手続は、既存の内容であって最適化はされていない。	①（○） ②（○） ③（○）	全て○→ 仮レベル＝３とし、次の＃（５）へ

＜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

成熟度属性項目（視点）											
レベル	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	
#		＊		＊		＊		＊		＊		＊
レベル＝3 貴社の評価	対応の必要性が理解されている。(=) マネジメント層は、より正式化および構造化された方法で周知を図っている。(=) （注）情報セキュリティの重要性とその周知を指す。 (=)：実際には○、×、△などの判断を入れる		優れた実践基準が使用され始めている。 鍵となるすべてのアクティビティについて、プロセス、ポリシー、および手続が定義され、文書化されている。(=) ビジネス上のプロセス実行に関する明確な役割と実行責任、および成果測定手法がある。		プロセスを自動化するため、ツールの使用方法と標準化に関する計画が定義されている。(×) ツールはその基本目的に合わせて使用されているが、合意済みの計画に完全には従っていない場合や、他のツールと統合されていないことがある。(=) (根本的に)ツールと自動化は当社に必要か		すべての領域についてスキル要件が定義され、文書化されているか。 正式な研修計画が作成されているが、。。。(=) 業務に関する専門知識の文書化はまだなされていない。(=)		プロセスの実行責任と説明責任が定義されており、プロセスオーナが特定されている。(=) 実行責任を果たすために必要な全権限を、プロセスオーナが保有していない可能性が高いことに注意して確認。		有効性の達成目標および測定指標がいくつか設定されているが、周知されていない。(=) ビジネス達成目標との明確な関連付けは存在する。 (=) 成果測定プロセスが作成され始めているが、一貫して適用されていない。(=)	
貴社の固有状況	＜対象企業の状況を判断し、状況を記載する＞ 例：貴社で扱う情報は、。。。。	例：5	＜対象企業の状況を判断し、状況を記載する＞ 例：業務に関するワークフローから判断すると、。。。。	例：4	＜対象企業の状況を判断し、状況を記載する＞ 例：ツールを使用できるか、不可かの検討は。。。。自動化には今のところ該当しない。まだその必要性が明確でない。	例：— 非該当	＜対象企業の状況を判断し、状況を記載する＞ 例：社内の個人情報保護研修が。。。。	例：4	＜対象企業の状況を判断し、状況を記載する＞ 例：社内組織が業務対応に構成されており、。。。。	例：5	＜対象企業の状況を判断し、状況を記載する＞ 例：ビジネス達成目標は、。。。。	例：4

＜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：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

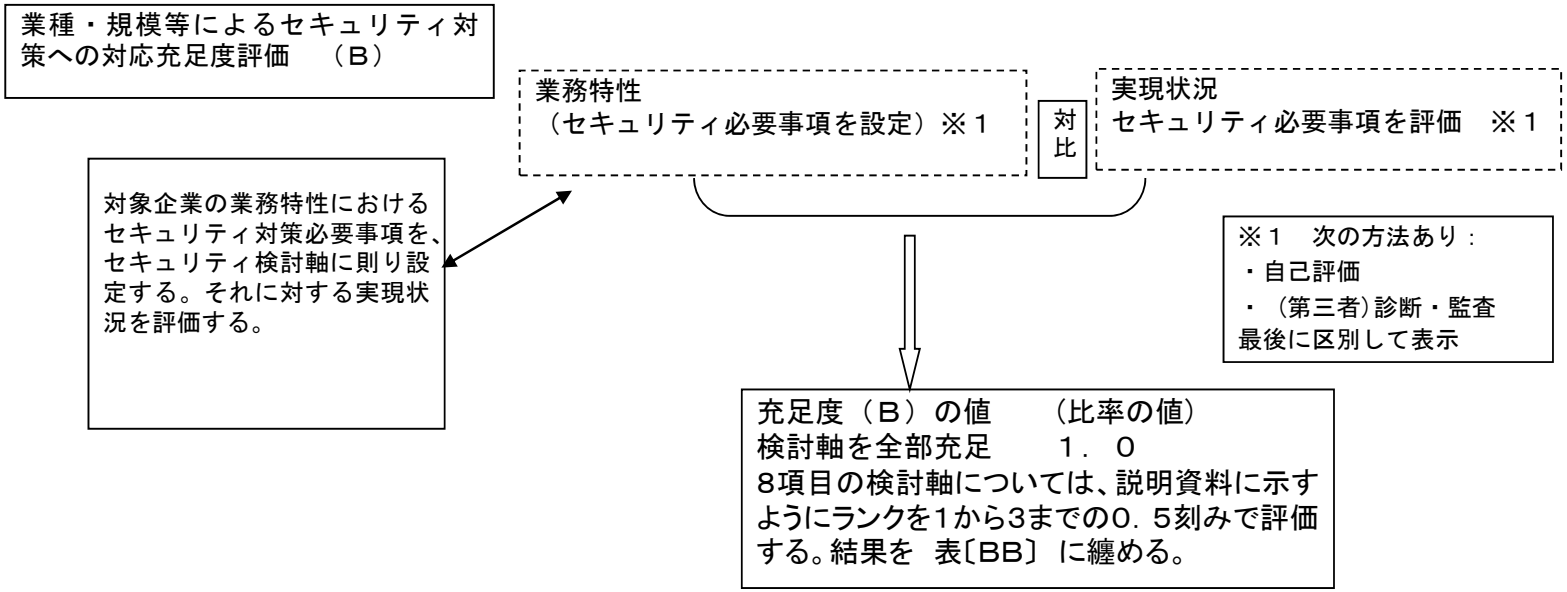
格付けのレベル		格付け対象外		格付けに値する成熟度モデルの範囲			
マネジメントシステム（ＭＳ）実施状況	ＣＯＢＩＴ一般成熟度モデル	0 不在	1 初期／その場対応	2 再現性はあるが直感的	3 定められたプロセスがある	4 管理され、測定が可能である	5 最適化
体制整備（整備＝機能していること）	不十分	—	—	—(ありえない)	—(ありえない)	—(ありえない)	—(ありえない)
	軽度の不備	—	—	1	3	4	4
	整備	—(ありえない)	—(ありえない)	2	4	5	5
規程整備	不十分	—	—	—(ありえない)	—(ありえない)	—(ありえない)	—(ありえない)
	軽度の不備	—	—	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	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。＝3			

＜参考＞報告書Ⅱ．格付けの方法と評価基準

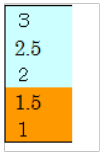
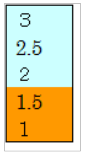
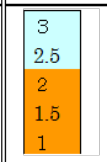
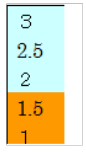
（2）企業の対応体制評価　②評価点(B)を求める

（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

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 ＜例示＞	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） ＜例示＞	残存リスクの状況、許容度 ＜例示＞	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（差を表示）
①	取り扱う情報の性質 情報量	守るべき情報資産として ・（顧客から預かる）組織人事業務組織、処遇、人事制度情報など ・業務情報は長期間保有するものは少ないが、全体で約２０００件程度を保有する。これらを電子ファイル、あるいは紙媒体として事務所を中心に安全に利用、保管する。情報セキュリティ対策はこれを満たす必要がある。	情報の種類 右に同じ 預かり情報 （１）顧客からの預かり情報の種類と内容 （２）社内情報の管理状況		必要性状況をステップBの質問票から判断する。 		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	・情報管理は事務所内にサーバを設置し、主たる利用は事務所内で行なう集中型である。外部との通信は。。。。。 ・この環境で（相互には独立な）顧客情報のセキュリティ確保を図る必要がある。 情報システム環境・運用へのリスク対応要件は限定的。	①業務用サーバ１台を本社に設置し社内ＬＡＮを構築している。 業務上インターネット利用で顧客企業情報を収集するが、。。。。 安全管理手順等は整備され実施されている。 ・入退管理、保管、情報システム、におけるセキュリティー対策の必要性状況、適切性が十分検討されていない。 例：地震、火災、等の災害対策、ケーブル配線等。	・情報セキュリティーの観点から守るべき資産は何か、サービスが停滞し、顧客サービス面に与える影響度、事業収益に与える影響等の検討はなされていない。 機密性、完全性、可用性の面からリスクを認識し必要なシステム構成、安全対策が十分とは言えない。			0

＜参考＞格付け会社（株アイ･エス･レーティング）

関連事項

- 格付け会社（株アイ･エス･レーティング）が発足し格付け実績もある
- 当研究内容との違い

	当研究プロジェクトでの格付け評価方法	情報管理体制の格付け会社 「株式会社アイ・エス・レーティング」 （2008.4.9日経新聞記事、インターネット情報による）
目的	企業の情報セキュリティ対策の評価・格付け （情報セキュリティ監査の活用）	情報管理体制の格付け 情報の管理体制や法令順守への取り組みを第三者機関からのお墨付きを得て、事業拡大につなげる。
特徴（狙い）	比較的安価、容易に取組み出来る	1件あたり100万～400万円？
対象	中小・中堅企業（事業所単位から） ＩＳＭＳやプライバシーマーク認定取得には費用的に手が届かない企業にも容易に取り組める	大手企業やその取引先（自動車や金融、流通など個人情報を多く扱う業種） 企業単位や事業部門単位
内容・方法	自己宣言 自己宣言内容を診断し、認定する 情報セキュリティ監査、情報セキュリティ診断を活用	機密や情報の取り扱いについて現地調査や幹部への聞き取りを行なう。 第三者による格付けの診断、監査 情報セキュリティ監査
格付け表現	セキュリティポリシーとセットにした☆マーク。☆の数で評価結果のランクを表す。 対応体制の充足度、セキュリティ対応必要項目に対する実現度	全体としては16段階の格付け 項目ごとの評価を「トリプルＡ」から「Ｂ」をつける ISO27001に加え、組織等の情報セキュリティレベルをランク付けする
システム監査人のかかわり	情報セキュリティ監査、情報セキュリティ診断を実施する。依頼によりコンサルに応ずる。	（情報セキュリティ）監査