●システム監査学会　第22回研究大会
研究プロジェクト　発表３

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

2007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

２００８年６月６日

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（2006年度からの続き）

（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）2007年度展開

①企業において情報資産（個人情報を含む）活用の基盤に対する情報セキュリティ確保は必須　企業は内部統制の確立を図る。
⇒　情報セキュリティ監査の活用の場を拓く

②企業は情報セキュリティ対策をこれだけ実施している、また対応をする
→　セキュリティポリシにより顧客・社外へアピール・宣言をする
（企業の立場としてはやっていることは正当に評価されるようにしたい）
→ しかし評価がないと対策実施内容の実効性は不明　⇒　格付けを行なう

③評価

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

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

①企業はセキュリティポリシーを公表し対策実施を宣言

（しかし、実施している対策内容は明らかではない。

つまり、セキュリティポリシーの明確な保証はない）

・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（その過程で情報セキュリティ監査の活用を図る）ことを提案

②方法の考え方

・世間に認められる評価基準に則った内部統制の体制・仕組みに基づくもの

・情報セキュリティ管理基準、COBIT成熟度モデル、JISQ27001などを基にした基準内容を検討

③体制・仕組みの評価方法

ａ）自己宣言(自身で評価)(→④）、あるいは　ｂ）システム監査人による評価（→⑤）

④自己宣言

・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

・企業自ら活動する→自ら宣言するためのガイドが必要

・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

⑤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

1．研究プロジェクトの目的と検討内容

（4）当プロジェクトの検討内容と意義

企業の情報セキュリティ対策の取組みの評価・格付け方法の検討

- 企業にとってこの意義とは次のようになる。

1．情報セキュリティ対策は、実施することが先ず重要である。
2．しかし、それだけでは必ずしも十分ではない。
3．我が社はこのように実践していることをビジネス社会に理解してもらう。
4．それによって信用を得て、業務貢献を実現する。
5．更に最高度の評価を得て、他社優位を実現する。

- このような目的を達成するには、自己PR、広報活動だけでなく、社会的に信頼される「格付け制度」が必要である。

２．情報セキュリティ対策実施の表明
情報セキュリティポリシの宣言

（１）（企業による）情報セキュリティポリシー公表
　公表すなわち、社外へのアピール。ではそのポリシーおよび対策内容は？
　①官公庁向けにはガイドラインがある
　　地方公共団体における情報セキュリティポリシーに関する
　　ガイドライン（平成18年9月） 総務省
　②民間部門向けは？　明確なものは無い
（２）ポリシーを宣言することの意味と内容
　（企業は）“何をする”を宣言（⇒　次のことを明確にする必要あり）
　　・宣言のためやることは何か
　　・（何をやっている）を説明する
　　・どのような体制を作っているか（誰が責任をもつのか）
　　・何を対象にするか、どのレベルまで対応するか

　　→　これらを格付けにて確認し、評価し明示する

２．情報セキュリティ対策実施の表明
情報セキュリティポリシの宣言

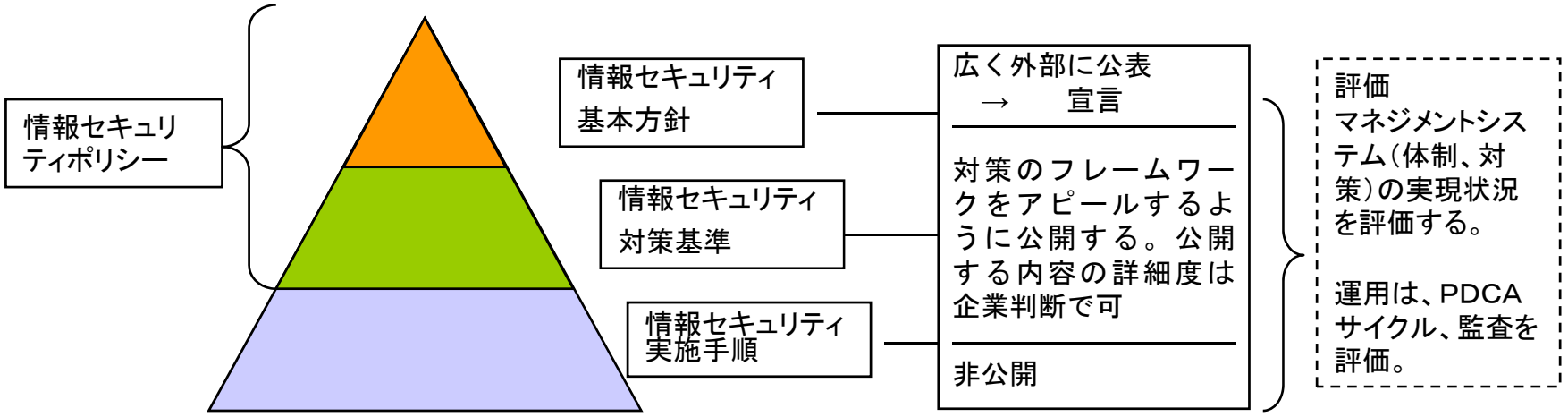
（３）評価実施方法の検討
①格付けの基準内容を明確にする
②セキュリティポリシーの構成（備えるべき項目）を明確にする
セキュリティポリシーの雛形を考える　→　（４）参照
③格付け評価項目を検討する　→　３参照
④評価の仕組みを検討する　→　３参照

評価項目の構成
ａ）**企業の対応体制**
COBITの一般成熟度モデル　＋
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**
（参考：情報セキュリティ管理基準、JISQ27001等）

2. 情報セキュリティ対策実施の表明
情報セキュリティポリシーの宣言

（4）情報セキュリティポリシーとは

情報セキュリティ対策規程（下図）の中で
情報セキュリティポリシーは基本方針と対策基準から構成される。



2. 情報セキュリティ対策実施の表明
情報セキュリティポリシーの宣言

（5）セキュリティポリシー(基本方針）の内容

- 責任者による宣言

〇〇株式会社情報セキュリティ保護宣言

平成〇〇年〇月〇日

代表取締役社長　丸山一郎

〇〇株式会社（以下当社）は情報セキュリティに対する対策を以下のように定めて宣言する。

- 情報セキュリティ対策の目的、企業のやるべき事項
- 目標にする対策レベル（取り扱う情報の範囲）
- 情報セキュリティ対策への取り組み体制
- 情報セキュリティ対策規程体系と概要、レベル
- 情報セキュリティ対策規程内容
- 内部監査責任者の任命と監査結果による適正状況の公表
- 監査責任者名で、情報セキュリティ対策規程に基づく監査結果、適切に運用されていると認めることを公表。
- マネジメントサイクルのCの段階を実施する（実施できているレベル）

など

2. 情報セキュリティ対策実施の表明

- 情報セキュリティ基本方針　　項目の例
  地方公共団体における情報セキュリティポリシーに関するガイドライン（平成18年9月 総務省）より

1.目的
2.定義
3.対象とする脅威
4.適用範囲
5.職員等の遵守義務
6.情報セキュリティ対策
　（1）組織体制
　（2）情報資産の分類と管理
　（3）物理的セキュリティ
　（4）人的セキュリティ
　（5）技術的セキュリティ
　（6）運用
7. 情報セキュリティ監査及び自己点検の実施
8. 情報セキュリティポリシーの見直し
9.情報セキュリティ対策基準の策定
10. 情報セキュリティ実施手順の策定

2. 情報セキュリティ対策実施の表明
情報セキュリティポリシーの宣言

＜参考＞情報セキュリティ監査報告の表明

（システム監査学会の個人情報保護方針を利用して基本方針における表示を例示）

- システム監査学会の個人情報保護方針

システム監査学会は、システム監査に関する会員相互の研究交流、学術的な研究及び調査、専門監査人制度等の学会活動において、会員、並びに研究大会、公開シンポジウム、研究会等イベント参加者の個人情報の適切な管理に努めます。

（1）個人情報の取得
本学会は、学会活動における個人情報の利用目的を明示して個人情報を適正に取得します。
（2）個人情報の利用
本学会は、取得した個人情報を、予め明示した利用目的の範囲内で利用し、目的外利用にあたっては、事前に本人からの同意を得ます。
（3）個人情報の提供
本学会は、取得した個人情報を、本人の同意がある場合、又は法令の規定に基づく場合を除いて、第三者に提供いたしません。
（4）個人情報の開示・訂正・削除
本学会は、取得した個人情報に対して、本人からの求めがあった場合は、本人を確認の上、学会業務に必要な調査を実施し、学会業務の適正な実施に著しい支障を及ぼさない範囲において開示・訂正・削除を行います。
（5）法令等の遵守
本学会は、個人情報の取扱いに関する法令、国が定める指針その他の規範を特定し参照できる手順を確立し、且つ維持します。
（6）個人情報の取扱いに関する継続的改善
本学会は、個人情報の取扱いに関し、本個人情報保護方針のもとに継続的改善に努めます。
（7）情報セキュリティ監査
本学会は定期的に情報セキュリティ監査を実施し、情報セキュリティの維持、向上に努めます。

2005年4月1日　制定
2007年8月1日　改定
システム監査学会　会長　　森宮　　康

当学会規程に基づく情報セキュリティ監査を実施した結果、適切に運用されていると認められました。
内部監査人・システム監査部　　○○　○○　　2008年6月6日

- 個人情報の取扱いに関するお問い合わせはこちら　　システム監査学会　　電話：03-3432-3166
- E-Mail　info@sysaudit.jp

2. 情報セキュリティ対策実施の表明

情報セキュリティポリシーの宣言

(6)情報セキュリティ対策基準の構成

＜参考＞情報セキュリティ実施手順の例　地方公共団体における情報セキュリティポリシーに関するガイドライン(平成18年9月　総務省)より

3.4. 物理的セキュリティ

3.4.1. サーバ等の管理

(1)機器の取付け

- 情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

(2)サーバの二重化

- ①情報システム管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを二重化し、ミラーリング等により同一データを保持しなければならない。【推奨事項】
- ②情報システム管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。【推奨事項】

３．情報セキュリティ対策

評価・格付けの考え方

（１）基本ステップ

情報セキュリティポリシーの自己宣言・公表
（公表された格付け基準による自己評価）

企業自身の準備
・自らの体制作り仕組みづくり
・対策の実施
・宣言による公表
・（準備段階におけるシステム監査人の協力）

↓

情報セキュリティポリシーの裏づけとなる
情報セキュリティ対策の実施状況の格付け評価
（格付けレベルを第三者が認定する）

・第三者に格付け基準による評価依頼
（方法：情報セキュリティ監査
・（あるいは診断）
・認定評価結果の表示

３．情報セキュリティ対策
評価・格付けの考え方

（２）セキュリティポリシの自己宣言・公表
　a）企業が行なう準備　　体制と仕組み作り
　　その運用（マネジメントシステムの実践）
　　・セキュリティポリシ宣言による公表
　　・情報セキュリティ規程の制定、実施、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
　公表・宣言内容・実施状況の評価を依頼する
　情報セキュリティ対策レベルの格付け（1っ☆～5っ☆）を認定

　　自己宣言のみ　　（第三者による保証なし）
　　第三者による評価済　（第三者による保証あり）※

※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

３．情報セキュリティ対策
評価・格付けの考え方

（４）格付け評価の全体のフロー
（監査人の関与を含めて基本ステップを表示する）。

- 情報セキュリティ対策の格付け評価結果をセキュリティマーク（（Ｓ）マーク）として表示する
- 格付け評価結果は、自己宣言のみと、外部監査人による監査の結果で評価したものとは、確実度合いが異なる。
- 情報セキュリティ対策の格付けは、自己宣言のみと、評価認定済を区別して表示する

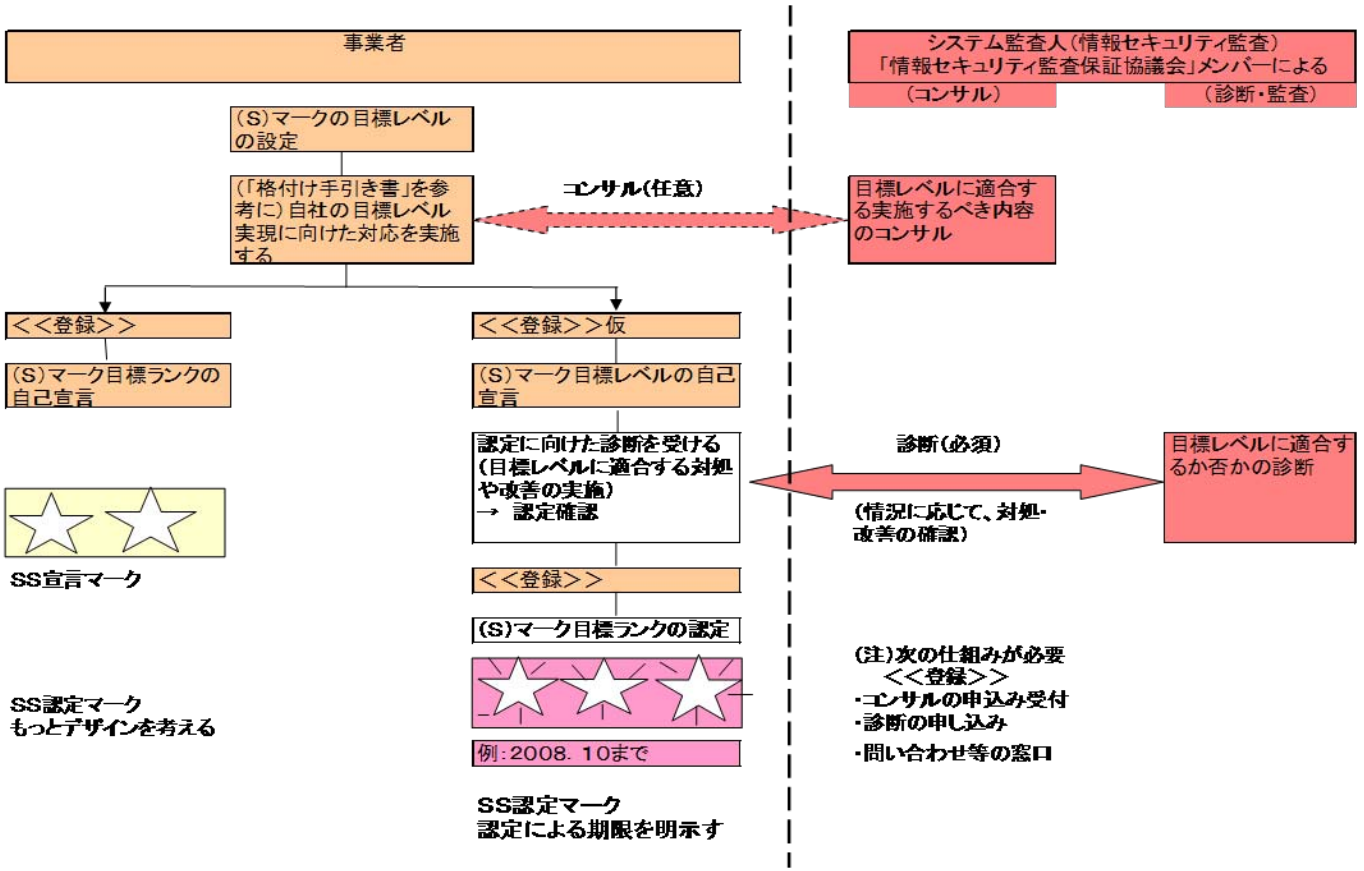
- 自己宣言　　ランク数の☆　　(ＳＳ宣言マーク)
- 評価認定済　　ランク数の☆と期間(ＳＳ認定マーク)

- それを含めた全体のフローは次のとおり

3. 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



４．格付けの方法と評価基準の検討

（１）格付けの方法

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（前出）

② （当研究による）格付け評価基準による評価方法
（次のａ）、ｂ）の評価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

③セキュリティポリシで明確にする内容や対策を確実なものとするため、必要であればシステム監査人にコンサルを依頼する。
（システム監査人の関与）

４．格付けの方法と評価基準の検討

（2）企業の対応体制評価　①評価点(A)を求める

体制評価点Ⓐの値　企業が自社の置かれた立場を、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。

格付けのランク		格付けに値せず		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）実践状況	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　〇	—（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　〇			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Ⓐ		———	———	１～５の値を得る。　例示：３ または－（条件を満たさず）			

評価点Ⓐの値は、該当する（ＭＳ）の数値の最低値を与える

４．格付けの方法と評価基準の検討

（2）企業の対応体制評価　　②評価対象

対応体制評価の対象とする情報セキュリティポリシー等の内容

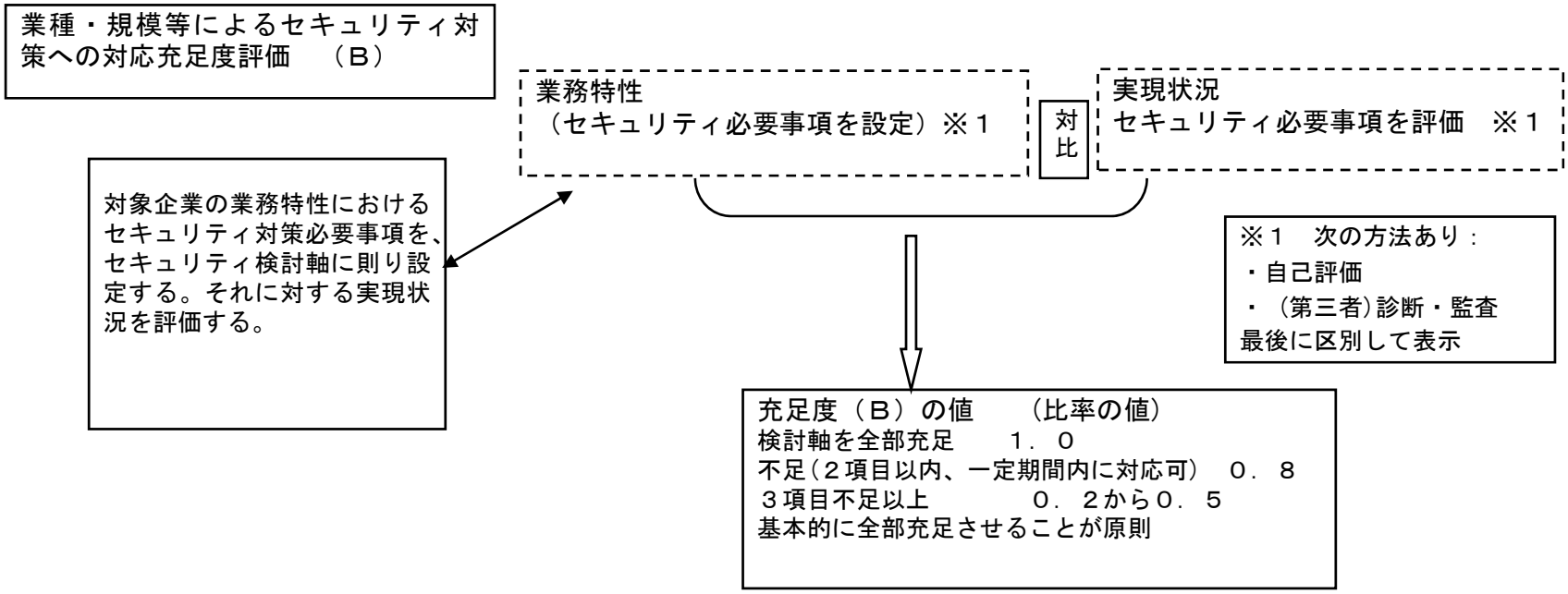
(企業が整備し実施する内容は、最初から完全なものを準備できないことも考慮する。
下図のように企業の対応水準を第１段階から第４段階に必要に応じて高めてゆく。)

	情報セキュリティポリシーの公表					結果のランク
評価対象 企業レベル	基本方針の公表	対策基準の整備、公表	PDCA サイクルの実行	きちんとした監査実施の公表	実施手順の整備	
第１段階	○	(○)				☆
第２段階	○	○	(○)			☆☆
第３段階	○	○	○	(○)		☆☆☆
第４段階	○	○	○	○	(○) ～○	☆☆☆～ ☆☆☆☆☆

○　：公表、対応あり　　(○)：完全でなくとも対応する
不足する事項に関しては、診断により不足を明らかにして、企業に対応をもとめ、満たすようにさせる。
コンサル、あるいは事業者との共同作業型で、結果としての情報セキュリティ対策強化を図る方法を作っておく。
Ｋ社の例：　公表事項は第４段階で、評価点（Ａ）の☆☆☆☆　を満たしている。

４．格付けの方法と評価基準の検討

（3）対応充足度評価(B)　①考え方



評価方法は次のスライド。「セキュリティ検討軸」の評価項目はＣＯＢＩＴや、情報セキュリティ管理基準、ＪＩＳＱ２７００１等を参考にするもので、内容（概要）を「格付け手引書」にまとめる。

４．格付けの方法と評価基準の検討

（3）対応充足度評価(B)　②評価方法

業種・規模等による対応評価の方法　　記入例

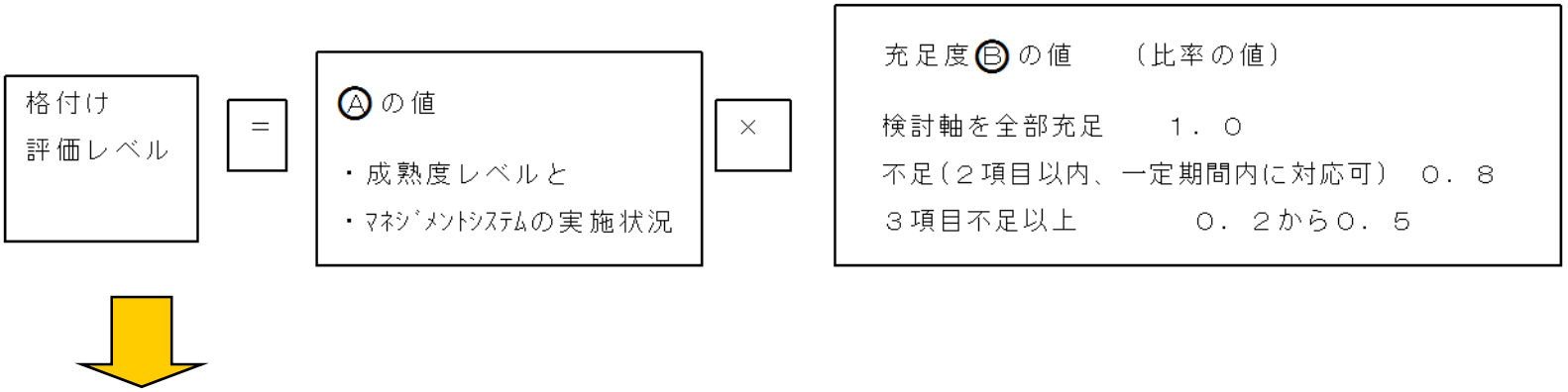
				必要度			実現状況			充足度
	セキュリティ検討軸（＊） （これに対する対策内容を見る）	要因	指標内容	1	2	3	1	2	3	
1	取り扱う情報の性質 情報量	管理対象の量、質、期間、範囲	機微情報、機密情報の比率 小　→　大、量（小→大）		○		○			不足
2	情報システムの物理的な環境 情報システム運用内容	物理的安全性、	集中　→　広域、分散		○			○		OK
3	ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ対策要件 セキュリティ対策要件	論理的安全性、 アクセス管理	危険度　小　→　大		○			○		OK
4	通信システムへの利用、依存度、 通信システムの危険性	通信システム関連の指標	モバイル利用、通信依存度の危険性		○			○		OK
5	（紙等物理媒体の）情報取扱いセキュリティ	移送、授受管理、保管、媒体変換	手作業取扱い等の危険度 小　→　大	○				○		OK
6	外部委託内容 外部委託の範囲	情報取扱いの外部委託の安全性	外部委託内容の重要度、比率、危険度　小　→　大			○		○		不足
7	情報システムの開発、保守、システムの信頼性	システムの安定性	システム更新、変更の頻度、障害の頻度		○		○			不足
8	教育（ルールの周知徹底）、従業員への役割の徹底	構成の流動による対応必要性	正社員、臨時社員比率など流動度合い　小　→　大		○			○		OK

	充足状況　　必要度・実現度を自己評価　　→	充足度　5／8 充足度率（B）＝０．８
	充足状況　　必要度・実現度を診断・監査　→	—

（＊）セキュリティ検討軸は、ＣＯＢＩＴ、ＪＩＳＱ27001の要素を参考に集約したもの。

４．格付けの方法と評価基準の検討

（４）格付け評価レベル
　格付けの評価は、セキュリティマーク（（S）マーク）として☆の数で表示する



(S)マークのランク(☆の数）＝（A）の値×（B）の値　(小数点以下切捨て）
K社の例：　３　<＝　４　×　０．８　＝　３．２

４．格付けの方法と評価基準の検討

（５）企業自身による格付け評価

①前記格付け評価基準により、企業自らが評価できるよう当研究で作成する「格付け手引き書」を利用する。

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“（Ｓ）マーク公表”（ＳＳ宣言）を行なう。

③評価資料、結果は“（Ｓ）マーク公表”格付け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が必要。

更に評価の確実性向上のために、次を考えることは良い。

⑤システム監査人による診断あるいは監査を依頼する。

④ 評価した結果は、認定済みとして公表する。→（６）

４．格付けの方法と評価基準の検討

（６） 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

･診断･コンサルの体制 （情報セキュリティ監査保証協議会）（昨年報告）

･保証型監査の契約による

②第三者による診断･評価の意義

情報セキュリティ対策内容、レベルの違いを是正
一確実性あるものにする（解釈の相違、顧客の立場で見る等）

③診断･監査を行う内容(前記「手引き書」による）

（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して機能する必要がある）

④自己宣言レベルと診断･監査結果のレベルで差が出た場合、どちらを表示するかは各企業の判断による

（７）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。登録サイトから登録者へリンク可能とする。

②宣言内容は定期的に見直しする。

５．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監査・診断の内容（保証型情報セキュリティ監査）

監査契約書(雛形）

保証内容

②コンサル／診断／監査の体制

情報セキュリティ監査保証協議会　(構想段階です）

③格付け基準

（２）これからの課題

・「格付け手引き書」の整備

・実際に適用して実施　→　見直し(そのため実践が必要）

・運用の仕組み（組織）を作ること

・第１歩としてモデルの仕組みを作り、実証を行うこと。

5. 検討したこと／これからの検討課題

（3）関連事項

- 格付け会社（株アイ・エス・レーティング）が発足している
- 2007年7月　計画の発表あり（知らずにいた）
- 2008年4月　格付け会社が発足したとの新聞報道
- 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

募集

- 当研究プロジェクトへの参加を募集いたします。
  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、当機械振興会館内の会議室にて開催
- 対象企業になることの募集

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、JISQ15001、
  地方公共団体における情報セキュリティポリシーに関するガイドライン
  （平成18年9月）総務省　他

・研究プロジェクトメンバー

赤尾嘉治　大井正浩　金子長男　木村裕一　沢恒雄　清水政幸
田附喜幸　玉井学　築島邦男　馬場孝悦　林兵江　平真須美
福田健　福原幸太郎　牧野豊　村上進司　（50音順）

- ご清聴を有難うございます。