

目 次

	ページ
序文.....	1
1 適用範囲.....	1
2 用語及び定義.....	1
3 セキュリティの諸概念及びその関係.....	4
3.1 セキュリティに関する原則.....	4
3.2 資産.....	4
3.3 脅威.....	5
3.4 ぜい弱性.....	6
3.5 影響.....	7
3.6 リスク.....	7
3.7 セーフガード.....	7
3.8 制約事項.....	8
3.9 セキュリティ要素の関係.....	9
4 目標, 戦略及び方針.....	11
4.1 ICT セキュリティ目標及び戦略.....	12
4.2 方針の階層.....	13
4.3 全社的な ICT セキュリティ基本方針の要素.....	15
5 ICT セキュリティの組織的側面.....	17
5.1 役割及び責任.....	17
5.2 組織における原則.....	20
6 ICT セキュリティマネジメント機能.....	22
6.1 概要.....	22
6.2 文化的及び環境的条件.....	22
6.3 リスクマネジメント.....	22

まえがき

この規格は、工業標準化法に基づき、日本工業標準調査会の審議を経て、経済産業大臣が制定した日本工業規格である。

この規格は、著作権法で保護対象となっている著作物である。

この規格の一部が、技術的性質をもつ特許権、出願公開後の特許出願、実用新案権、又は出願公開後の実用新案登録出願に抵触する可能性があることに注意を喚起する。経済産業大臣及び日本工業標準調査会は、このような技術的性質をもつ特許権、出願公開後の特許出願、実用新案権、又は出願公開後の実用新案登録出願にかかわる確認について、責任をもたない。

JIS Q 13335 の規格群には、次に示す部編成がある。

JIS Q 13335-1 情報技術—セキュリティ技術—情報通信技術セキュリティマネジメント—第1部：情報通信技術セキュリティマネジメントの概念及びモデル

ISO/IEC 13335-2, Information technology—Security techniques—Management of information and communications technology security—Part 2: Information security risk management (審議中)

情報技術—セキュリティ技術— 情報通信技術セキュリティマネジメント— 第 1 部：情報通信技術セキュリティマネジメントの 概念及びモデル

Information technology—Security techniques—Management of information
and communications technology security—Part 1: Concepts and models for
information and communications technology security management

序文

この規格は、2004 年に第 1 版として発行された ISO/IEC 13335-1 を基に、技術的内容及び対応国際規格の構成を変更することなく作成した日本工業規格である。

1 適用範囲

この規格は、情報通信技術 (Information and Communications Technology) (以下、ICT という。) セキュリティのマネジメントについての手引について規定する。この規格群の第 1 部では、ICT セキュリティを理解する上において必要最低限の基本的な概念及びモデルを示し、ICT セキュリティの計画、導入及び運用の成功に極めて重要である。この規格は、マネジメントの一般的な問題を取り上げる。

この規格は、ICT セキュリティへの特定のマネジメントの取組み方を推奨することは意図していない。その代わりに、この規格は、ICT セキュリティのマネジメントに役立つ、概念及びモデルに関する一般的な考え方を示す。この規格が取り上げた事項は一般的なものであり、多くの異なった様式のマネジメント及び組織の環境に適用可能である。この規格が取り上げた事項は、組織の要求及びその組織特有のマネジメント様式に合わせて手直しできようになっている。

注記 この規格の対応国際規格及びその対応の程度を表す記号を、次に示す。

ISO/IEC 13335-1:2004, Information technology—Security techniques—Management of information and communications technology security—Part 1: Concepts and models for information and communications technology security management (IDT)

なお、対応の程度を表す記号 (IDT) は、ISO/IEC Guide 21 に基づき、一致していることを示す。

2 用語及び定義

この規格で用いる主な用語及び定義は、次による。

2.1**責任追跡性 (accountability)**

あるエンティティの動作が、その動作から動作主のエンティティまで一意に追跡できることを確実にする特性 (**JIS X 5004**)。

2.2**資産 (asset)**

組織にとって価値をもつもの。

2.3**真正性 (authenticity)**

ある主体又は資源が、主張どおりであることを確実にする特性。真正性は、利用者、プロセス、システム、情報などのエンティティに対して適用する。

2.4**可用性 (availability)**

認可されたエンティティが要求したときに、アクセス及び使用が可能である特性 (**JIS X 5004**)。

2.5**ベースライン管理策 (baseline controls)**

あるシステム又は組織のために設定されたセーフガードの最低限の組合せ。

2.6**機密性 (confidentiality)**

認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性 (**JIS X 5004**)。

2.7**管理策 (control)**

ICT セキュリティにおいては、“管理策”は“セーフガード”と同義語とすることがある (**2.24** セーフガード 参照)。

2.8**指針 (guidelines)**

方針のなかに設定された目標を達成するためになすべきこと及びその方法を明らかにした記述。

2.9**影響 (impact)**

情報セキュリティインシデントの結果。

2.10**(情報セキュリティ) インシデント (information security incident)**

事業活動又は情報セキュリティを損ねる可能性のある、予期しない又は望んでいない事象。情報セキュリティインシデントの例には、次のものがある。

- サービス、設備又は施設の停止
- システムの動作不良又は過負荷
- 人為的誤り
- 方針又は指針への不適合
- 物理的セキュリティに関する取決めへの違反

- ー 管理されていないシステム変更
- ー ソフトウェア又はハードウェアの動作不良
- ー アクセス違反

2.11

ICT セキュリティ (ICT security)

ICT にかかわる機密性, 完全性, 可用性, 否認防止, 責任追跡性, 真正性及び信頼性の定義付け, 達成及び維持に関連したすべての側面。

2.12

ICT セキュリティ方針 (ICT security policy)

組織及びその ICT システム内において, 取扱いに慎重を要する情報を含む資産の管理・保護・配付を統制する規則, 指示及び慣行。

2.13

情報処理設備 (information processing facility)

情報処理システム, サービス若しくは基盤, 又はそれらを収容する物理的な設置場所。

2.14

情報セキュリティ (information security)

情報又は情報処理設備にかかわる機密性, 完全性, 可用性, 否認防止, 責任追跡性, 真正性及び信頼性の定義付け, 達成及び維持に関連したすべての側面。

2.15

完全性 (integrity)

資産の正確性及び完全さを保護する特性。

2.16

否認防止 (non-repudiation)

ある活動又は事象が起きたことを, 後になって否認されないように証明する能力。

2.17

信頼性 (reliability)

意図した動作及び結果に一致する特性。

2.18

残留リスク (residual risk)

リスク対応の後に残っているリスク。

2.19

リスク (risk)

ある脅威が, 資産又は資産のグループのぜい (脆) 弱性につけ込み, そのことによって組織に損害を与える可能性。これは, 事象の発生確率と事象の結果との組合せによって測定できる。

2.20

リスク分析 (risk analysis)

リスクの重大さを算定するための体系的なプロセス。

2.21

リスクアセスメント (risk assessment)

リスク特定, リスク分析及びリスク評価を組み合わせたプロセス。

2.22**リスクマネジメント (risk management)**

ICT システムの資源に作用する不確かな事象を特定し、制御し、また、それらを除去又は最小化する総合的なプロセス。

2.23**リスク対応 (risk treatment)**

リスクを変更するために方策を選択及び実施するプロセス。

2.24**セーフガード (safeguard)**

リスク対応のための慣行、手順又は仕組み。

注記 “セーフガード” は、“管理策” と同義語とすることがある (2.7 参照)。

2.25**脅威 (threat)**

システム又は組織に損害を与える可能性があるインシデントの潜在的な原因。

2.26**ぜい (脆) 弱性 (vulnerability)**

一つ以上の脅威がつけ込むことのできる、資産又は資産グループがもつ弱点。

3 セキュリティの諸概念及びその関係**3.1 セキュリティに関する原則**

次に示す、高い次元から見たセキュリティに関する原則は、効果的な ICT セキュリティ構想を確立するための基本である。

リスクマネジメント：資産を、適切なセーフガードの採用を通して保護することが望ましい。セーフガードを選択し管理する際には、適切なリスクマネジメントの方法論、すなわち、組織の資産、脅威、ぜい弱性及び発生する脅威の影響を査定して、随伴するリスク及び配慮すべき制約事項を見出すような方法論を基礎に置くことが望ましい。

コミットメント：ICT セキュリティ及びリスクマネジメントへの組織ぐるみのコミットメントが不可欠である。コミットメントを得るためには、ICT セキュリティの展開による利益を明確にすることが望ましい。

役割及び責任：組織の全体的管理体制は、資産をセキュリティが保たれた状態に置くことに責任がある。ICT セキュリティのための役割及び責任を明確にして知らせることが望ましい。

目標、戦略及び方針：ICT セキュリティリスクを、組織の目標、戦略及び方針に配慮しつつ管理することが望ましい。

ライフサイクル管理：ICT セキュリティマネジメントは、組織の ICT 資産の全ライフサイクルを通して継続的なものであることが望ましい。

次の細分箇条では、セキュリティマネジメントに関係する主なセキュリティ要素及びそれらとの間の関係について、基本的なセキュリティに関する原則から見たときの概略を示す。それぞれの要素を示し、また、関係する主な要因を上げる。この規格群の第 2 部では、脅威、ぜい弱性及びセーフガードを含むリスクの要素を詳細に規定している。

3.2 資産

資産の適正な管理は、組織の成功にとって必ず (須) であり、経営陣すべての主要な責務である。組織

の資産は、何らかの保護を与えるのに十分な価値があると見てよい。次に示すものが資産に含まれる場合があるが、これに限るものではない。

- 物理的な資産（例：コンピュータ ハードウェア、通信設備、建物）
- 情報・データ（例：文書、データベース）
- ソフトウェア
- 製品又はサービスを提供する能力
- 人材
- 無形財産（例：営業権、企業イメージ）

セキュリティの視点から見ると、組織の資産が識別されていないと、よいセキュリティ構想を実現し維持していくことができない。多くの場合、資産を識別して価値を割り当てる処理は、概観レベルで完了することができ、このときは費用のかかる、また、詳細で時間のかかる作業は必要としない。この作業の詳細さのレベルは、資産価値に対する時間及び費用の点から判断されることが望ましい。どの場合でも、詳細さのレベルは、セキュリティの目標を基に決定することが望ましい。

配慮の必要がある資産の属性には、その価値及び／又は取扱いに要する慎重さ、並びに既存のセーフガードが含まれる。特定の脅威が存在するときのぜい弱性は、資産を保護する要件を左右する。組織がその中で活動する環境、文化及び法制度は、資産及びその属性に影響を与える可能性がある。例えば、個人情報保護を非常に重要とみなす文化がある一方で、この問題にそれほど重要性を置かない文化もある。このような環境、文化及び法律上の多様性は、国際的な組織及び国境にまたがる ICT システムの使用において重要である。

脅威及びぜい弱性、並びにそれらを組み合わせた影響のアセスメントに基づいて、リスクが査定され、そして、資産を適切に保護するためにセーフガードが適用される。資産が十分に保護されているかどうかを決定するために、更に残留リスクのアセスメントが必要である。

3.3 脅威

資産は、多くの種類の脅威にさらされている。ある脅威は資産に損傷を与え、そのことで組織に損害を与える可能性がある。この損傷は、ICT システム又はサービスで処理されている情報に対する攻撃、システム自体に対する攻撃及びその他の資源に対する攻撃、すなわち、データの許可されていない破壊、開示、改ざん、破損、利用不可又は損失を引き起こすことから発生する。資産に損傷を与えるためには、脅威は、その資産に存在するぜい弱性を悪用する必要がある。脅威は、環境に端を発する場合又は人間に端を発する場合があるが、後者の場合は、偶発的なもの又は意図的なものがある。偶発的及び意図的な脅威をともに識別し、脅威のレベル及び発生の可能性を査定することが望ましい。環境的脅威の多くについては、統計データが入手可能である。組織は、脅威を査定するとき、そのようなデータを入手して使用してよい。

脅威の例を表 1 に示す。

表 1—脅威の例

人間		環境
意図的	偶発的	地震 落雷 洪水 火災
盗聴 情報の改ざん システムのハッキング 悪意のあるコード 盗難	誤り及び手ぬかり ファイルの削除 不正な経路 物理的事故	

脅威には、例えば、コンピュータの破壊という形で、組織のある箇所に影響を与えるものがある。その一方で、幾つかの脅威は、例えば、暴風又は落雷による建物の被害という形で、システム又は組織の所在するある立地の周辺に、広く影響を与えることがある。脅威は、例えば、従業員のサボタージュのように、組織の内部から発生する可能性があるし、例えば、悪意のハッキング又は産業スパイのように、外部から発生する可能性がある。損傷の規模は、脅威の発生それぞれによって大きく異なる。損傷には、一時的なもの又は資産の破壊の場合のように永続的なものがある。

脅威には、その他のセキュリティ要素との関係を規定する特徴がある。その特徴には、次のことが含まれる。

- 部内者又は部外者という、その源
- 例えば、金銭的利得又は競争上の優位といった、その動機
- 発生頻度
- 発生可能性
- 影響

幾つかの脅威は、複数の資産に作用する場合がある。この場合、脅威がどの資産に作用するかで、異なる影響を与える可能性がある。例えば、ネットワークに接続されていないパーソナルコンピュータ上のソフトウェアウィルスは、限定的又は局所的にしか影響しない場合がある。しかし、同じソフトウェアウィルスでも、ネットワークに接続されたファイルサーバ上に存在するときは、広い範囲に影響する可能性がある。

組織がその中に位置する環境及び文化は、その組織及びその資産への脅威をどのように扱うかについて、極めて大きく関連し、また、影響をもつ。ある文化では、幾つかの脅威は、危険とみなされない可能性もある。脅威を扱うときは、環境及び文化の側面を考慮する必要がある。

脅威は、脅威のアセスメント結果に基づいて、高、中及び低といった表現で格付してもよい。

3.4 ぜい弱性

一つ以上の脅威が悪用することのできる資産又は資産の集合の弱点は、ぜい弱性として知られている。資産に関するぜい弱性には、物理的配置、組織、手順、要員、マネジメント、管理、ハードウェア、ソフトウェア及び情報における弱点が含まれる。脅威は、ICT システム又は事業目標に損傷を与えるために、ぜい弱性を悪用する場合がある。ぜい弱性は、対応する脅威がない状態でも存在する。ぜい弱性それ自体は損傷を与えず、それは単に、脅威が資産に作用することを許す可能性のある条件又は条件の集合ではない。様々な源から生じるぜい弱性、例えば、資産そのものに内在するぜい弱性であるか、又は外生的なぜい弱性であるかに配慮する必要がある。ぜい弱性は、資産自体が変化して、そのぜい弱性が問題とならなくなるまで、残る可能性がある。ぜい弱性は、あらゆる状況を考慮するために、個別に査定するととも

に集合としても査定することが望ましい。

ぜい弱性の例の一つにアクセス制御の欠落があり、これは、侵入という脅威を許して資産を消失させることがある。

特定のシステム又は組織では、すべてのぜい弱性が脅威を許してしまうわけではない。対応する脅威の存在するぜい弱性が直近の懸念である。ただし、環境は、予想を超えて変化するので、新しい脅威又は再出現した脅威にさらされるぜい弱性を識別するために、すべてのぜい弱性を監視することが望ましい。

ぜい弱性アセスメントとは、識別された脅威によって悪用されるかもしれない弱点を調査することである。このアセスメントでは、環境及び既存のセーフガードを考慮する必要がある。特定のシステム又は資産の脅威に対するぜい弱性の程度は、そのシステム又は資産の損傷の受けやすさで表される。

ぜい弱性は、ぜい弱性アセスメントの結果に応じて、高、中又は低といった表現で格付してもよい。

3.5 影響

影響は、資産に作用する脅威によってもたらされる、情報セキュリティに関してのインシデントの結果である。この影響としては、資産の破壊、ICT システムへの被害、及び機密性、完全性、可用性、否認防止、責任追跡性、真正性又は信頼性を損ねることがある。また、間接的影響として考えられるものに、金銭的損失、市場シェア又は企業イメージの損失が含まれる。

影響を測定することは、インシデントの予期される結果とインシデントを防止するセーフガードの費用との間で均衡をとることを可能にする。

インシデントの発生可能性を考慮する必要がある。これは、一つ一つのインシデントによって発生する損傷が小さくても、長い間の多くのインシデントによる総合効果が危険である場合に特に重要である。

影響のアセスメントは、リスクアセスメント及びセーフガードの選択において重要な要素である。

影響の定量的及び定性的な測定は、次のような多くの方法で実施できる。

- 金銭的費用の算定
- 経験に基づいた影響度についての尺度（例：1～10）の割当て
- あらかじめ定義した表から選択した表現（例：高、中又は低）の使用

3.6 リスク

リスクは、ある脅威が資産又は資産の集合のぜい弱性を悪用し、そのことで組織に損傷を与える可能性のことである。一つ以上の脅威が、一つ以上のぜい弱性を悪用する場合もある。

リスク想定は、特定の脅威又は脅威の集合が、資産を危険にさらすように、どのように特定のぜい弱性又はぜい弱性の集合を悪用する可能性があるかを描写する。リスクは、インシデントの発生可能性及びその影響という、二つの要因の組合せで特徴付けられる。資産、脅威、ぜい弱性及びセーフガードのどのような変化も、リスクに重大な効果をもたらす可能性がある。いかなる変化も早期に検知又は認識することは、リスクに対応するために適切な処置をとる機会を増やす。リスク対応の選択肢には、リスク回避、リスク低減、リスク移転及びリスク受容を含む。

リスクを完全に取り除くことはできない。そのセキュリティが組織の要求に合致しているかどうかの判断の一部に、残留リスクの受容がある。影響及びインシデントの発生可能性の見地から、経営陣がすべての残留リスクを認識できるようになっていることが望ましい。残留リスクを受容する決定は、発生するインシデントの影響を容認できる地位にあり、残留リスクのレベルが受容できない場合には、追加のセーフガードの導入を許可できる人が行う必要がある。

3.7 セーフガード

セーフガードは、脅威から保護し、ぜい弱性を減少させ、情報セキュリティに関してのインシデントの

影響を抑制し、インシデントを検知し、復旧を早めることができる、慣行、手順又は仕組みである。効果的なセキュリティには、通常、資産を保護する階層的なセキュリティを提供するための異なるセーフガードの組合せが必要である。例えば、コンピュータに適用されるアクセス制御機構は、監査という管理策、要員管理手順、訓練及び物理的なセキュリティによって支援されることが望ましい。幾つかのセーフガードは、環境の一部又は資産固有のものとして既に存在していることもあるし、システム又は組織内で既に実施されていることもある。

セーフガードを適切に選択することは、セキュリティ構想を適正に実現するために不可欠である。一つのセーフガードが複数の目的達成に貢献する場合もあれば、逆に、一つの機能が多数のセーフガードを要求する場合もある。セーフガードは、次の機能のうちの一つ以上を実現するものとみなしてよい場合がある。

- 予防
- 抑止
- 検知
- 制限
- 是正
- 回復
- 監視
- 意識向上

セーフガードを利用できる領域の例には、次が含まれる。

- 物理的な環境
- 技術的な環境（ハードウェア、ソフトウェア及び通信）
- 要員
- 管理

セーフガードの中には、セキュリティに対する組織の姿勢を強く明確に表明するものがある。この点については、組織がその中で活動している文化及び／又は社会との間で摩擦を起こさないセーフガードを選択することが重要である。

セーフガードの具体例には、次のものがある。

- 方針及び手順
- アクセス制御機構
- ウィルス対策ソフトウェア
- 暗号化
- デジタル署名
- 監視及び分析用ツール
- 予備電源
- 情報のバックアップコピー

3.8 制約事項

制約事項は、通常、組織の管理者によって設定又は認識され、組織がその中で活動している環境によって影響される。配慮を必要とする制約事項の例として、次のものがある。

- 組織に関する事項
- 事業に関する事項
- 財務に関する事項
- 環境に関する事項
- 要員
- 時間
- 法律
- 技術
- 文化・社会

これらの要因を、セーフガードを選択及び導入するときに配慮することが望ましい。既存の制約事項及び新しい制約事項を定期的に見直し、どのような変化も識別することが望ましい。制約事項が、組織の文化とともに変化するだけでなく、時間、地理及び社会の発展とともに変化する場合があることにも注意することが望ましい。組織がその中で活動する環境及び文化は、多数のセキュリティ要素、特に脅威、リスク及びセーフガードと関連することがある。

3.9 セキュリティ要素の関係

ICT システムのセキュリティは、多様な局面からの統制であり、様々な観点から見る事ができる。図 1 は、多くの脅威に資産が潜在的にさらされている状況を示したモデルである。この脅威の集合は、時間とともに絶えず変化し、部分的にしか知られていない。同様に、環境も時間とともに変化し、この変化は、脅威の性質及びその発生可能性に影響する可能性がある。

このモデルは、次のことを示している。

- 制約事項のある環境及び常に変化し一部しか知られていない脅威
- 組織の資産
- それらの資産に関連したぜい弱性
- 資産を保護するために選択されたセーフガード
- 組織が受容し得る残留リスク

少なくとも五つの想定が可能であり、図 1 にそれを示す。これらの想定は、次の内容を含む。

想定 1 — 一つのセーフガード (S) が、リスク (R) を低減することに効果的と見られる場合である。

このときのリスクは、一つのぜい弱性 (V) を悪用できる脅威 (T) と関連している。脅威は、資産がそれに対してぜい弱である場合にだけ効果的である。

想定 2 — 一つのセーフガードが、リスクを低減することに効果的と見られる場合である。このときのリスクは、複数のぜい弱性を悪用する脅威と関連している。

想定 3 — 複数のセーフガードの組合せが、リスクを低減することに効果的と見られる場合である。このときのリスクは、一つのぜい弱性を悪用する複数の脅威と関連している。しばしば、リスクを受容可能なレベルに低減して残留リスクを受容できるものとするために、多数のセーフガードが求められることがある。

想定 4 — そのリスクが受容可能とみなされる場合である。脅威とぜい弱性とが共に存在するとしても、セーフガードは導入されない。

想定 5 — ぜい弱性は存在するが、それを悪用する既知の脅威がない場合である。

ぜい弱性を悪用することのできる脅威が発生していないことを確実にするために、脅威の環境を監視するセーフガードを導入してもよい。制約事項は、セーフガードの選択に作用する。

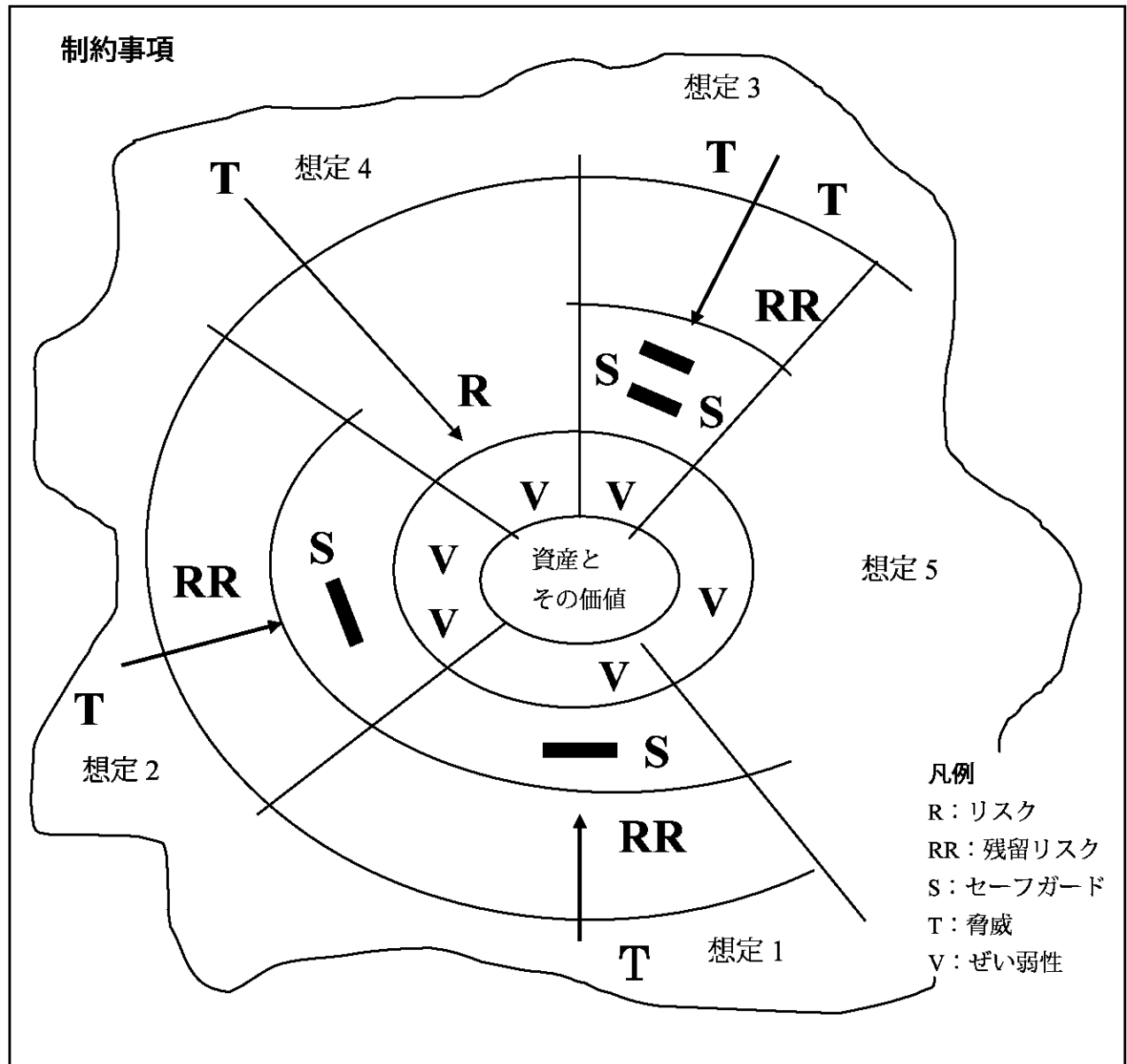


図1ーセキュリティ要素の関係

どのようなICTシステムも、組織の事業成功のために重要な資産（特に、情報であるが、ハードウェア、ソフトウェア、通信サービスなども含まれる。）によって構成されている。これらの資産は組織にとって価値があり、このことは、通常、情報の許可されていない開示、改ざん若しくは否認、又は情報若しくはサービスの利用不可若しくは破壊による事業運営への影響として表現される。最初に、資産の実質的な価値を特定できるようにするために、影響を明らかにする。この段階では、どのような脅威が生じて、その影響をもたらすかは関係ない。次に、そのような影響を及ぼすのはどのような脅威かという問題及びそれらの発生可能性が扱われる。資産が多くの脅威にさらされているかもしれないからである。次に、影響を及

ばす脅威によって悪用されるのはどのようなぜい弱性（又は弱点）かという問題が扱われる。例えば、脅威が資産のもつぜい弱性を悪用するかもしれないからである。これら構成要素のそれぞれ、例えば、価値、脅威及びぜい弱性は、リスクを増大させることがある。したがって、リスクの程度は、保護する必要性の全体的な程度を示すことになり、実際の必要性は、セーフガードの導入によって低くなり又は満たされる。そのようにして実施されたセーフガードは、リスクを低減し、脅威から保護し、ぜい弱性を実際に低減する。

図2に、簡単なモデルで、セーフガードがどのように、リスクの低減に効果を及ぼす場合があるかを示す。多数のセーフガードが、残留リスクを受容可能なレベルに低減するために、しばしば求められる。そのリスクが受容可能とみなされるときは、セーフガードが導入されないことがある。

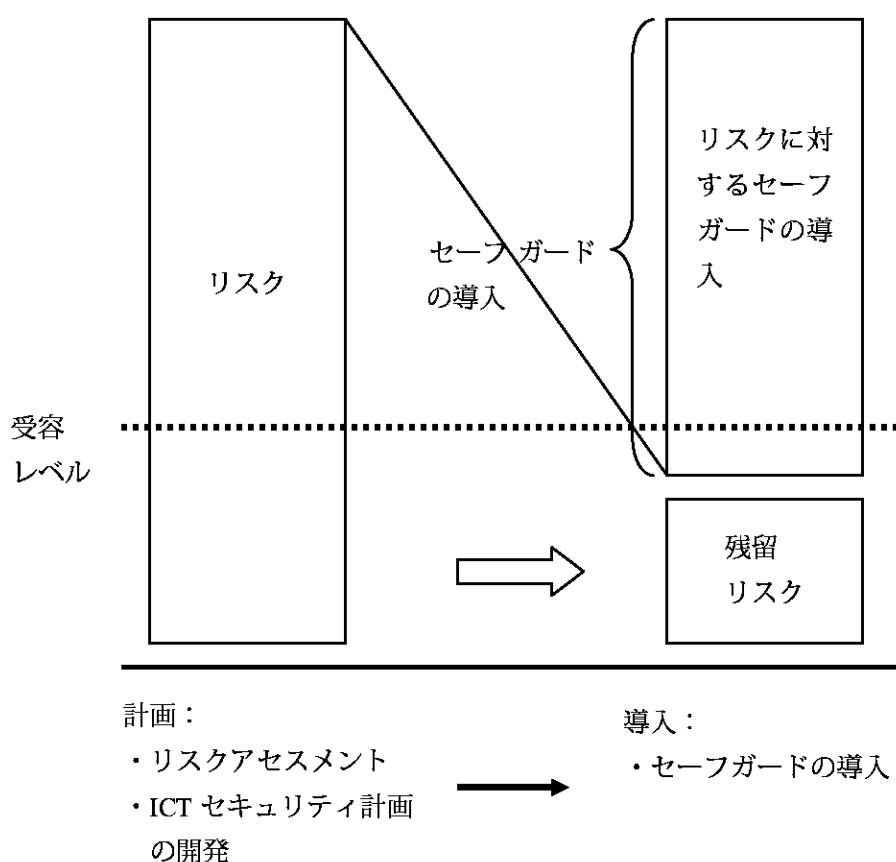


図2—セーフガードとリスクとの関係

4 目標、戦略及び方針

組織内の効果的な ICT セキュリティの基盤として、全社的なセキュリティ目標、戦略及び方針を明確に表す必要がある。目標、戦略及び方針は、事業を支え、そして、一体となってセーフガード間の整合性を確実にする。この整合性を確実にするためには、目標、戦略及び方針をセキュリティ訓練及び意識向上に関する計画の不可欠な一部分として含めることが特に重要である。

全社的なレベルから組織運営のレベルまで階層的に、そして事業部、事業単位又は部課それぞれに対して、目標（達成されるべきこと）、戦略（どのように目標を達成するかの方法）、方針（戦略実行において順守されるべき規則）及び手順（方針を実行するための方法）は、定義し、作成することができる。文書

化を推進する場合は、組織の要求事項を反映し、組織の制約を考慮に入れることが望ましい。(システムハッキング、ファイル削除及び火災のような) 様々な脅威は共通の事業問題なので、関連文書間の整合性(これは考え方の違いに影響される。)及び組織の様々なレベル間の整合性が重要である。

さらに、一般的な全社的目標、戦略及び基本方針は、財務管理、人事管理及びセキュリティ管理のような、組織が関連するすべての分野において詳細で明確な目標、方針及び手順に反映され、具体化されることが望ましい。次に、セキュリティは、セキュリティを構成する部分(人事、物理、情報、ICT など)に分けることが望ましい。文書化の階層は、定期的なセキュリティについてのレビュー(例えば、リスクアセスメント、内部及び／又は外部によるセキュリティ監査)結果及び事業目標の変化に基づいて、保守され、更新されることが望ましい。

ICT システムのセキュリティ目標、戦略、方針及び手順は、セキュリティの観点で ICT システムから期待されていることを表現していることが望ましい。これらは、通常は自然言語を用いて表現するが、何らかの確立された言語を用いて、より形式的な表現が要求される場合もある。セキュリティ目標、戦略、方針及び手順は、組織のセキュリティレベル及びリスク受容のしきい値を確立する。

4.1 ICT セキュリティ目標及び戦略

組織の ICT セキュリティ目標を確立した後、全社的な ICT セキュリティ基本方針を開発する基盤として ICT セキュリティ戦略を開発することが望ましい。全社的な ICT セキュリティ基本方針の開発は、リスクマネジメントの過程が適切で効果的であることを確実にするのに不可欠である。組織内のすべてに及ぶ経営陣の支持は、方針の開発及び効果的な実現に必要である。全社的な ICT セキュリティ基本方針には、全社的な目標及びその組織に固有な部分を考慮することが不可欠である。全社的な ICT セキュリティ基本方針は、全社のセキュリティ方針と事業方針とに連携していなければならない。この連携によって、全社的な ICT セキュリティ基本方針は、資源の最も効果的な使用を助け、異なるシステム環境の範囲をまたがるセキュリティへの首尾一貫した取組み方を確実にする。

それぞれの ICT システム又はそのうちの幾つかに対するセキュリティ方針を別に開発することが必要な場合もある。これらの方針は、リスクアセスメントに基づき、全社的な ICT セキュリティ基本方針に整合することが望ましい。したがって、関係するシステムに対するセキュリティの推奨を考慮に入れることになる。

ICT セキュリティを管理する過程における第 1 段階として、“組織にとって、広範囲で適用可能な、受容できるリスクのレベルはどの程度か”という問いを考察するのがよい。受容できるリスクの正確な定義、すなわち、セキュリティの適切なレベルの定義は、セキュリティマネジメントの成功のかぎである。必要とする、広範囲で適用可能なセキュリティのレベルは、組織が満たす必要のある ICT セキュリティ目標によって決定される。セキュリティ目標を評価するためには、組織の資産及びその価値を考慮することが望ましい。その価値は、組織の事業を指揮することを支援するために、ICT がもつ重要性によって決定されることが望ましい。ICT そのものの費用は、その価値のほんの小さな部分である。

組織の事業が ICT にどれほど依存しているかを評価するための質問としては、次のようなものがある。

- ICT の支援がないと実行できない事業の重要な要素は何か。
- ICT の助けがなくては得られないタスクは何か。
- ICT によって格納され処理される情報の機密性、完全性、可用性、否認防止、責任追跡性及び真正性に依存している重要な判断は何か。また、この情報がどの程度更新されているか。
- 格納され処理される秘密情報の何が保護される必要があるか。
- 情報セキュリティのインシデントのうち、組織にかかわるものは何か。

これらの質問に答えることは、組織の ICT セキュリティ目標の評価を助ける。例えば、事業上の何らかの重要な又は非常に重要な要素が正確な又は最新の情報に依存するならば、組織の ICT セキュリティ目標の一つは ICT システムにおいて情報が格納され処理されるときに完全性及び適時性を確実にする場合がある。さらに、重要な事業目標及びそのセキュリティとの関係は、ICT セキュリティ目標を評価するときに考慮されることが望ましい。

ICT セキュリティ目標の内容にもよるが、この目標を達成するための戦略が合意されていることが望ましい。選択された戦略は、保護される資産の価値にとって適切であることが望ましい。例えば、上の一つ以上の質問に対する回答が ICT に強く依存することを示すならば、その組織には ICT セキュリティについて高水準の要求があると見ることができ、これらの要求を達成するための十分な戦略を選択することが推奨される。

ICT セキュリティ戦略は、組織がどのようにして ICT セキュリティ目標を達成するかを一般的な表現で概説する。そのような戦略で取り上げることが望ましいテーマは、目標の数、タイプ及び重要度に依存するが、通常は、組織が一元的に取り組むことが重要であるとみなすものが選択される。このテーマは、性格上、特定の領域のものを取り上げる場合又は非常に広い範囲のものを取り上げる場合がある。

特定のテーマの例として、事業特性から、システムのすべてが連続的に利用可能であることを主要なセキュリティ目標にもつことがある。この場合は、一つの戦略のテーマが、組織全体でウィルス対策ソフトを導入することによってウィルスのまん（蔓）延を最小化することに向けられる場合がある。

より広い範囲のものを取り上げたテーマの例としては、ICT サービスを販売する事業をしている場合には、組織が組織自体のシステムのセキュリティが潜在的な顧客にも証明できることを ICT セキュリティ目標にすることがある。この場合には、戦略のテーマが認知された第三者によるセキュリティの妥当性検証となることがある。

これらのほか、特定の目標又はその組合せから ICT セキュリティ戦略のテーマになると考えられるものに、次のようなものがある。

- 組織全体で採用するリスクアセスメント戦略及び方法
- それぞれのシステムの ICT セキュリティ方針
- それぞれのシステムのセキュリティ運用手順
- 組織全体の取扱いに慎重を要する情報に基づく分類体系
- セキュリティ意識向上及び教育・訓練
- 他の組織と接続する前に満足・点検すべき接続についてのセキュリティ条件
- 組織をまたがる標準的な情報セキュリティインシデントの管理体制

一度決定すれば、セキュリティ戦略及び構成するテーマは、全社的な ICT セキュリティ基本方針に包含されることが望ましい。

4.2 方針の階層

全社的セキュリティ方針は、組織全体に対するセキュリティの原則及び指示を含む場合がある。

全社的セキュリティ方針は、個人の権利、法的要求及び規格類を扱っている、広範囲で適用可能な全社的な方針を反映することが望ましい。

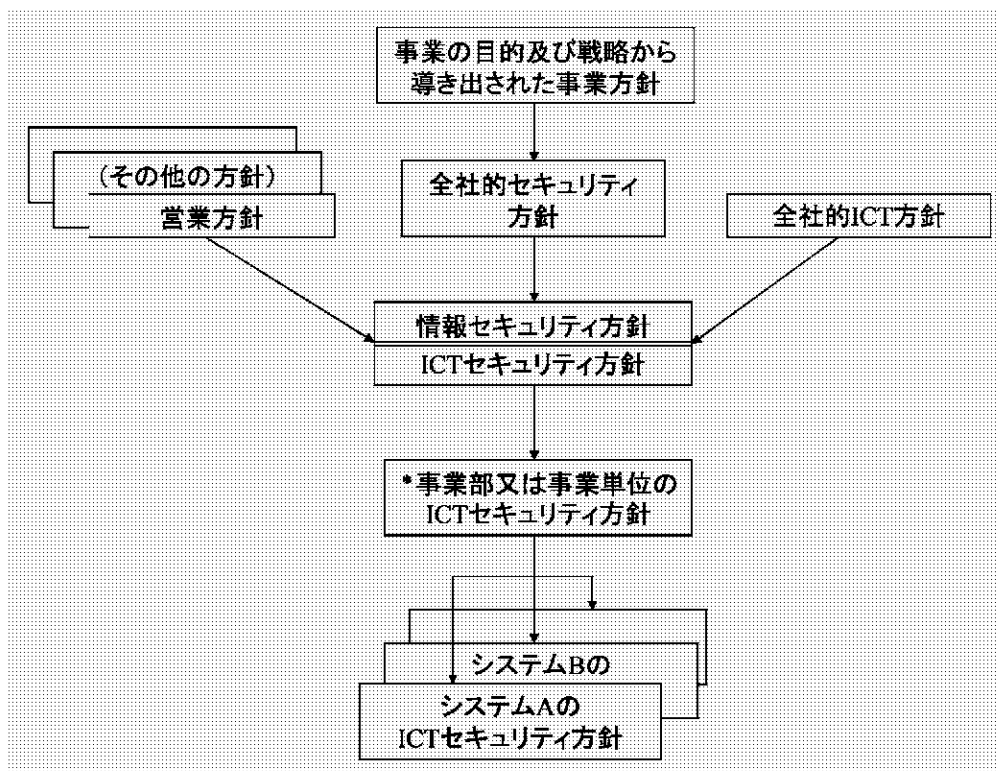
情報セキュリティ方針は、組織にとって取扱いに慎重を要する情報若しくは価値のある情報、又は他の点で重要な情報の保護のための特定の原則及び指示を含む場合がある。そこに含まれる原則は、全社的セキュリティ方針の原則から導かれるので、それとの整合性もあることになる。

全社的な ICT セキュリティ基本方針は、全社的なセキュリティ方針及び情報セキュリティ方針に適用できる、本質的な ICT セキュリティの原則及び指示を反映し、組織内の ICT システムの一般的な利用を反映していることが望ましい。

ICT システムセキュリティ方針は、全社的な ICT セキュリティ基本方針に含まれるセキュリティの原則及び指示を反映していることが望ましい。特殊なセキュリティ要求事項の詳細、実装されるべきセーフガード及び十分なセキュリティを確実にするためにセーフガードをどのように正しく使うかの手順も、含むことが望ましい。すべての場合において、選択された取組み方が組織の事業ニーズに関して効果的であることが重要である。

適切なときは、全社的な ICT セキュリティ基本方針を、全社的な技術方針及び経営管理方針のなかに含めてもよく、これら二つの方針は互いに全社的な ICT 方針の基礎となる。この方針では、セキュリティの重要性について積極的に言及することが望ましく、その方針を順守するためにセキュリティが必要である場合は特にそうである。図 3 は、方針の階層の相互関係の例である。実際の文書及び組織の構造は組織によって異なるだろうが、種々の方針が、様々な記述になっても一定内容を扱っていること及び一貫性を維持していることが重要である。

その他に、特定のシステム及びサービス用、又は ICT のシステム群及びサービス群用に、より詳細化した ICT セキュリティ方針が必要になる。これらは通常、ICT システムのセキュリティ方針と呼ばれる。ICT システムのセキュリティ方針の適用範囲及び境界線が明確に定義されていること、並びにこれら適用範囲及び境界線が事業、技術上の両方の理由に基づいていることは、経営管理上重要なことである。



注* 階層の深さ（階層の数）は、組織の規模など多数の要因による。

図 3—方針の階層

4.3 全社的な ICT セキュリティ基本方針の要素

全社的な ICT セキュリティ基本方針は、合意された全社的 ICT セキュリティの目標及び戦略に基づいて策定するのが望ましい。全社的な ICT セキュリティ基本方針は、法制度、事業、セキュリティ及び ICT 方針に矛盾しないよう確立し、維持する必要がある。

事業目標を満足することを確実に支援するために、組織の ICT 依存度が高くなればなるほど ICT セキュリティが一層重要となる。全社的な ICT セキュリティ基本方針を立案する場合、文化、環境及び組織の諸特性を念頭に置くのが望ましい。なぜなら、それらの特性がセキュリティへの取り組み方に影響を及ぼすためである。例えば、ある環境では容易に受け入れられる可能性があるセーフガードであっても、別の環境では全く受け入れられない場合がある。

全社的な ICT セキュリティ基本方針に記述されるセキュリティ関連業務は、組織の目標及び戦略、以前のセキュリティのリスクアセスメント及びマネジメントレビューの結果、並びにフォローアップ業務の結果に基づくことができる。フォローアップ業務とは、例えば、実施されたセーフガード、日々使用される ICT セキュリティの監視・監査・レビュー及びセキュリティインシデントの報告書のセキュリティ順守状況の点検である。これらの業務中に検知された重大な脅威又はぜい弱性は、全社的な ICT セキュリティ基本方針で規定された組織の総合的なセキュリティ問題の取扱い手法に沿って、取り上げる必要がある。詳細な処置については、様々な ICT システムセキュリティ方針又はその他の支援文書、例えば、セキュリティ操作手順などで示す。

全社的な ICT セキュリティ基本方針の策定に当たっては、次に示す職務の代表者が参加するのが望ましい。

- 監査
- 法務
- 財務
- 情報システム（技術者及び利用者）
- ユーティリティ・施設（例えば、建物の構造及び設備、電力、空調に責任をもつ人）
- 人事
- セキュリティ
- 事業経営陣

セキュリティの目標及びそれらの目標を達成するために組織が採用した戦略に従って、全社的な ICT セキュリティ基本方針の詳細な適用レベルを決定する。全社的 ICT セキュリティ基本方針には、次に示す一般的な事項を記述するのが望ましい。

- その範囲及び目的
- 法制度上の義務に関するセキュリティの目標及び事業の目標
- 情報の機密性、完全性、可用性、否認防止、責任追跡性及び真正性に関する ICT セキュリティの要求事項
- セキュリティ基本方針の基となった標準の参照
- 組織及び個人の責任並びに権限を網羅する情報セキュリティの管理
- 組織が採用したリスク管理手法
- セーフガードの実施の優先度を決定するための手段
- 経営陣が必要とする、広範囲で適用可能なセキュリティ及び残留リスクのレベル

- アクセス制御のための一般的な規則（建物、部屋、システム及び情報への物理的アクセス制御と同様な論理的なアクセス制御）
- 組織内部のセキュリティ意識向上及び教育・訓練の手法
- 広範囲で適用可能な、セキュリティの点検及び維持のための手順
- 一般要員のセキュリティ事項
- セキュリティ方針を関係者全員に伝達するための手段
- セキュリティ方針をレビュー又は監査するのが望ましい状況
- セキュリティ方針の変更を管理する方法

組織は、状況に最も適した特定のテーマを決定するために、要求事項、環境及び文化を評価するのが望ましい。このテーマには、次のものを含む場合がある。

- 機密性、完全性、可用性、否認防止、責任追跡性、真正性及び信頼性といった観点からの、ICT セキュリティの要求事項。特に、資産の所有者としての視点からの要求事項
- 組織的な基盤及び責任の割当て
- システムの開発段階及び調達段階でのセキュリティの組込み
- 情報を分類するための方法及び分類の定義
- リスクマネジメント戦略
- 事業継続計画
- 要員問題（信頼が必要な要員、例えば、保守要員及びシステムアドミニストレータのような地位につく要員には、特別の注意を払うことが望ましい。）
- セキュリティ意識の向上及び教育・訓練
- 法制度上の義務
- 外注管理
- 情報セキュリティのインシデントの取扱い

この箇条で規定したように、以前実施したリスクアセスメントのレビュー結果、セキュリティ順守状況の点検及び情報セキュリティのインシデントは、全社的な ICT セキュリティ基本方針に影響を及ぼすことがある。また、このために、以前に定義した戦略又はセキュリティ基本方針のレビュー又は再定義が必要となる場合もある。

すべてのセキュリティ関連措置のための適切な支援を確保するために、全社的な ICT セキュリティ基本方針は、経営者の承認を得るのが望ましい。

全社的な ICT セキュリティ基本方針に基づいて、これをすべての管理者及び従業員に義務付ける指示書を作成することが望ましい。指示書は、組織内でのセキュリティに対する従業員各人の責任を規定した文書に各人の署名を要求してもよい。さらに、責任を周知させるために、セキュリティ意識向上及び訓練のための計画を策定し、実施することが望ましい。

全社的な ICT セキュリティ基本方針に責任をもち、組織の要求事項及び実際の状況をそのセキュリティ基本方針に反映させることができる人物を選ぶのが望ましい。この責任者は、全社的な ICT セキュリティ責任者ということになり、数ある業務の中でもフォローアップ業務に責任を負うのが望ましい。フォローアップ業務には、セキュリティ順守状況の点検・レビュー・監査、インシデント及びセキュリティの弱点の取扱い、並びにこれらの業務結果によって必要となる可能性がある全社的な ICT セキュリティ基本方針の

変更を含む。

5 ICT セキュリティの組織的側面

5.1 役割及び責任

5.1.1 組織における役割及び責任

効果的なセキュリティには、説明責任、並びにセキュリティの責任の明確な割当て及び承認が必要である。経営陣は、リスクマネジメントの意思決定を含むセキュリティマネジメントのあらゆる側面に対して責任をもつことが望ましい。組織の性格、組織化の形態、組織の規模及び構造のような多数の要素が、どのレベルにその責任を割り当てるかを決定する。ICT セキュリティは多くの分野にまたがるテーマであり、あらゆる ICT プロジェクト及びシステムと関係があり、組織内のすべての ICT 利用者と関係がある。説明責任並びに特定の役割及び責任の適切な割当て及び区分けは、すべての重要業務を完了すること、並びにそれらが効果的及び効率的に遂行することを確実にすることが望ましい。小規模な組織にとっては、経営者がセキュリティの全役割を担ってもよいし、他の管理者が二つ以上のセキュリティの役割を担ってもよい。このような場合、独立したレビューは、利害の衝突を避け、また、役割の適切な分離を確実にするために重要である。

この目標は、組織の規模及び構造によって変わる様々な組織の体制を通して達成できるが、どのような組織でも、次の役割を含むことが必要である。

- 特に多くの分野にまたがる課題を解決し、戦略について助言及び提言し、並びに方針及び手順を承認する ICT セキュリティ委員会
- 組織内の ICT セキュリティのすべての側面について、中心となって活動する全社的 ICT セキュリティ責任者

ICT セキュリティ委員会及び全社的 ICT セキュリティ責任者の両者とも、明確に定義されておりあいまいではない職務を担うことが望ましく、また、全社的な ICT セキュリティ基本方針に責任をもてるような十分に上層の職員がこれに就くことが望ましい。組織は、全社的 ICT セキュリティ責任者のために、情報提供、責任及び権限に関する明確な方針を打ち出すことが望ましく、この責任者の職務は、ICT セキュリティ委員会において承認されることが望ましい。これら職務の履行は、外部コンサルタントを利用することで補完することもできる。

図 4 は、全社的 ICT セキュリティ責任者、ICT セキュリティ委員会、及び組織内の、例えば、他のセキュリティ機能、利用者組織及び ICT とかかわる要員といった他の領域からの代表者の相互関係の例を示す。このような関係は、ラインの管理又は機能上の場合もある。図 4 に示した ICT セキュリティの組織の例では、三つの組織レベルが想定されている。この例は、広い範囲で適用可能なように、会社又は事業単位・本社部門・部課のような古典的な組織構造に基づいているが、組織のニーズによってレベルを追加又は削除することで、どのような組織でも容易に採用できる。中小規模の組織では、セキュリティに関するすべての役割をもつ責任者として全社的 ICT セキュリティ責任者を選任する場合がある。このように機能が統合される場合は、一人の手に過度の責任が集中して他からの影響又は管理が及ばなくなることがないように、適切な抑制及び均衡が保たれることを確実にすることが重要である。

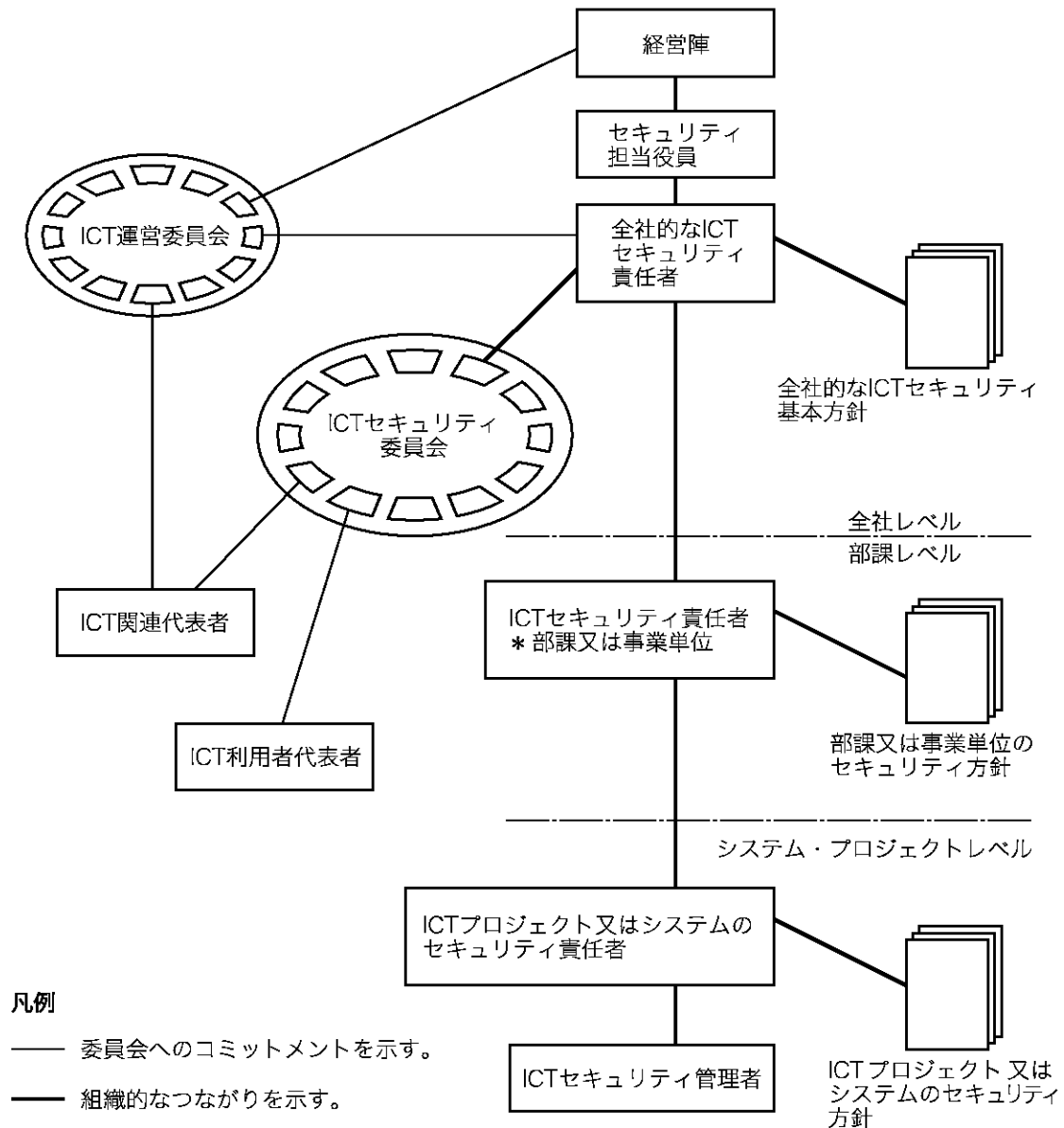


図 4—ICT セキュリティのための組織の例

5.1.2 ICT セキュリティ委員会

このような委員会は、戦略についての助言及び提言、セキュリティ要求事項の特定、方針類の策定、全社的なセキュリティ構想の作成、実施結果のレビュー及び全社的なICTセキュリティ責任者への指示をするのに必要なスキルをもつ者をメンバとすることが望ましい。このような目的に利用できる委員会組織が既に存在する場合もあろうし、それとも、独立のICTセキュリティ委員会を別に置く方がよい場合もある。このような委員会の役割は、次のとおりである。

- ICT運営委員会に対する、戦略的なセキュリティ構想に関する助言
- ICT戦略に裏打ちされた全社的なICTセキュリティ基本方針の策定、及び設置済みならばICT運営委員会からの承認の取得
- 全社的なICTセキュリティ基本方針からICTセキュリティ構想への展開

- － 全社的 ICT セキュリティ構想の実施状況の監視
- － 全社的な ICT セキュリティ基本方針の有効性の見直し
- － ICT セキュリティ問題についての意識向上の推進
- － 計画プロセス及び ICT セキュリティ構想の実施のために必要な経営資源（要員，資金，知識など）についての助言
- － 二つの分野にまたがる事項の解決

委員会が効果的であるために、ICT システムのセキュリティ及び技術面にバックグラウンドをもつ者、並びに ICT システムのプロバイダ及び利用者の代表者をメンバに含めることが望ましい。このような領域から得られる知識及びスキルは、実用的な全社的な ICT セキュリティ基本方針の開発に必要である。

5.1.3 全社的 ICT セキュリティ責任者

ICT セキュリティに対する責任を特定の個人に割り当てることが望ましい。全社的 ICT セキュリティ責任者は、組織内の ICT セキュリティ関連すべての側面に対する中心として活動することが望ましい。しかし、全社的 ICT セキュリティ責任者は、役割の幾つかの側面を委任してもよい。この ICT セキュリティの責任を追加的に課してもよい者が既に存在する場合があるが、中規模から大規模な組織では専任のポストとして設置することが望ましい。大規模組織では、事業単位及び部課のための ICT セキュリティ責任者のネットワークがある場合もある。全社的 ICT セキュリティ責任者及び事業部・事業単位の ICT 責任者には、セキュリティ及び ICT についてのバックグラウンドをもつ人々を選任することが望ましい。全社的 ICT 責任者の主な役割は、次のとおりである。

- － ICT セキュリティ構想の実施に対する監督
- － ICT セキュリティ委員会及びセキュリティ担当役員との連携及び報告
- － 全社的な ICT セキュリティ基本方針及び指示書の作成及び維持
- － インシデント調査の調整
- － 企業全般にわたるセキュリティ意識向上プログラムの運営管理
- － 基本方針から導き出された ICT セキュリティ目標及び基準の設定
- － セキュリティ管理策の有効性のレビュー，監査及び監視
- － 組織を通した ICT セキュリティ手順に合っているかのレビュー，監査及び監視

5.1.1 に規定したように、組織の規模、セキュリティシステムの複雑さ及びその他の関係する要素によっては、役割を分割することができる。

委任される可能性のある機能の例は、次のとおりである。

ICT セキュリティプロジェクト責任者：個々のプロジェクト又はシステムにもセキュリティについて責任をもつ者を置くことが望ましく、これは、ICT セキュリティプロジェクト責任者と通常呼ばれる。これは、フルタイムの職務でなくても実施可能である。これら責任者の職務を指揮管理することは、全社的 ICT セキュリティ責任者の責任であることが望ましい。これら責任者は、あるプロジェクト、あるシステム又はシステム群におけるセキュリティ関連すべての中心的役割を果たす。ICT セキュリティプロジェクト責任者の主な役割は、次のとおりである。

- － 全社的 ICT セキュリティ責任者との連携及び報告
- － セキュリティ構想の開発及び実施
- － ICT セーフガードの実施及び使用状況の日々の監視

ー インシデント調査の開始及び支援

ICT セキュリティ監督者：中規模及び大規模組織において、委任された監督業務の役割がある。これらには、次のものが含まれる。

- ー ICT セキュリティ手順の作成及び適用
- ー システム及びネットワークセキュリティの監督
- ー ウィルスツール、ソフトウェアの更新版、ソフトウェアパッチなどのような特定のセキュリティプログラムの更新
- ー バックアップ、アクセス制御リストなどのような特定のセキュリティ管理策の監督

セキュリティ監督者は、特定の活動及びツールを監督するための適切な訓練を受けなければならない。

5.1.4 ICT 利用者

利用者は、次の責任をもつ。

- ー ICT の方針、業務指針及び手順に適合した ICT 資源を使うこと
- ー ICT セキュリティ方針、業務指針及び手順に適合した ICT 業務資産を保護すること

5.2 組織における原則

5.2.1 コミットメント

企業の資産の適切な保護を実現しようとするならば、ICT セキュリティへの経営陣のコミットメントは不可欠である。このようなコミットメントが実際にはないか、又は目に見えるほどでなかった場合、全社的 ICT セキュリティ責任者の立場に影響を与え、脅威に対する企業の防御をかなり弱めることになる。経営陣からの目に見える支援は、全社的セキュリティ方針から導き出され、正式に合意されて、文書化された全社的な ICT セキュリティ基本方針になることが望ましい。これらの方針及びそれらの主要な要素の存在は、経営陣の関心及び支持を得ているとして、定期的にすべての従業員及び契約相手に適切に伝えられることが望ましい。

ICT セキュリティの目的に向けた企業全体のコミットメントには、次のものが含まれる。

- ー 組織の全社的な必要性に対する理解
- ー 組織内の ICT セキュリティの必要性に対する理解
- ー ICT セキュリティへのコミットメントの意思表示
- ー ICT セキュリティの必要性に取り組む意志
- ー 経営資源を ICT セキュリティに割り当てる意志
- ー ICT セキュリティの意味又は構成（適用範囲、限度）について最高レベルでの意識付け

ICT セキュリティの目標は、組織全体に公表されるべきである。従業員又は契約相手それぞれは、ICT セキュリティに対する自分の役割、責任及び貢献を認識して、この目標達成に対する任務がゆだねられることが望ましい。

5.2.2 一貫性のある取組み方

ICT セキュリティに向けた一貫性のある取組み方を、計画・導入及び運用の活動すべてに適用することが望ましい。情報及び ICT システムのライフサイクルの、計画から取得、試験及び運用に至るまでの全体を通して、防御が確実になされることが望ましい。

図 4 に示したような組織構造は、組織全体に及ぶ ICT セキュリティに向かう、調和のある取組み方を支

えることができる。この取り組み方は、規格を活用することによって推進することが必要である。規格としては、国際・国内・地域・産業界及び企業の規格又は規則を考えることができるが、組織の ICT セキュリティの必要性によって選択及び適用することになる。規格は、その実施及び使用に際して、規則及び指針によって補足する必要がある。

規格を利用することの利点は、次のとおりである。

- 統合されたセキュリティ
- 相互運用性
- 一貫性
- 可搬性
- 規模の経済性
- 組織間の相互作用

5.2.3 ICT セキュリティの組み込み

ICT セキュリティのすべての活動は、組織全体にわたって一様で、ICT システムのライフサイクルの最初から開始された場合に、最も効果的である。ICT セキュリティプロセス自体が大規模な循環的活動であり、ICT システムのライフサイクルのあらゆるフェーズにこれを組み込むことが望ましい。セキュリティは、新規のシステムに最初から組み込んだ場合に最も効果的であるが、過去から引き継いできたシステム及び事業活動にセキュリティを組み込んだ場合でも、その時点から効果を得ることができる。

ICT システムのライフサイクルは、四つの基本フェーズに分けられる。これらのフェーズは、それぞれ次のように ICT セキュリティと関連する。

- 計画：すべての計画及び意思決定の活動において、ICT セキュリティの必要性を取り上げることが望ましい。
- 取得：システムの設計・開発・購入・更新・構築のプロセスに ICT セキュリティについての要求事項を組み込むことが望ましい。将来ではなく適切なときにこれらの活動にセキュリティの要求事項を組み込むことは、費用対効果で優れたセキュリティ形態を確実にシステムにもたらす。
- 試験：ICT システムの試験は、ICT セキュリティの構成、形態及びサービスのテストを含むことが望ましい。新規の又は変更したセキュリティ機能部は、意図したように動作することを確実にするための独立試験を行い、次に、その運用環境の中で試験することが望ましい。というのは、その機能部の ICT システムへの組み込みがセキュリティの特性及び形態に影響を与えないことを確実にするためである。試験は、システムの運用のライフサイクルの間に定常的に組み込まれることが望ましい。
- 運用：ICT セキュリティを運用環境に組み込むことが望ましい。ICT システムは、意図した目的を遂行するために使用され、維持されるうちに、新しいハードウェアの構成部品の購入又はソフトウェアの変更若しくは追加を含む一連の更新を経験するのが通常である。加えて、運用環境は頻繁に変化する。このような環境変化は、システム上に新たなぜい弱性を発生させることがあり、それについては分析及び査定を行って、対策をとるか、又は受容するかを決定を行うことになる。同様に、システムを安全に廃棄又は譲渡することも重要である。

ICT セキュリティは、ICT システムのライフサイクルの各フェーズ内及びフェーズ相互間での多くのフィードバックを伴った、継続的なプロセスであることが望ましい。多くの場合、フィードバックは、ICT セキュリティのプロセスでの大きな活動のすべて及び活動相互間でも発生する。このフィードバックによって、ICT システムのライフサイクルの各フェーズを通して、ICT システムのぜい弱性、脅威及びセーフ

ガードに関する情報が途切れることなく伝達される。

組織の中の事業領域ごとに独自の ICT セキュリティに対する要求事項が認識される可能性があることにも注意する価値がある。そのようなときは、事業領域の間でセキュリティにかかわる情報を共有し、お互いの事業領域及び組織全体の ICT セキュリティのプロセスを支援することが望ましく、このような情報は、経営者の意思決定プロセスを支援するために利用できる。

6 ICT セキュリティマネジメント機能

6.1 概要

ICT セキュリティマネジメントが成功するためには、多くの活動を実行する必要がある。これらの活動には、周期的な方法で実行すべき次のものが含まれる。

- 計画
 - 組織の ICT セキュリティ要求事項の決定
 - 組織の ICT セキュリティ目標、戦略及び方針の決定
 - 組織内における役割及び責任の識別
 - ICT セキュリティ計画の開発
 - リスクアセスメント
 - リスク対応の決定及びセーフガードの選択
 - 事業継続計画
- 導入
 - セーフガードの導入
 - ICT システムの承認
 - セキュリティ意識向上プログラムの開発及び実施
 - セーフガードの導入及び運用についてのレビュー及び監視
- 運用及び保守
 - 構成管理及び変更管理
 - 事業継続管理
 - レビュー、監査・監視、及びセキュリティ順守状況の点検
 - 情報セキュリティインシデントの管理

6.2 文化的及び環境的条件

情報セキュリティマネジメントの機能的活動は、その下で組織が運営されている文化及び環境について考慮する必要がある。なぜならば、セキュリティに対する取組み方の全般に、文化及び環境が重大な影響を及ぼす可能性があるからである。さらに、また、組織の特定箇所の保護について責任がある人々に対しても、文化及び環境が影響を及ぼすことがある。ある場合には、政府の方に責任があるとみなされ、法律の制定及び施行によってその責任を免除する。他の場合には、責任があるとみなされるのは、所有者又は管理者の方である。この問題は、採用する取組み方にそれなりの影響を及ぼす。

6.3 リスクマネジメント

リスクマネジメントは、切れ目のない活動である。新規のシステム及び計画段階のシステムについては、設計及び開発工程の一部にリスクマネジメントを組み込むことが望ましい。既存のシステムについては、どの適切な時点からでも、リスクマネジメントを導入することが望ましい。重要なシステム変更を計画するときは、リスクマネジメントを、この計画立案過程の一部分に組み込むことが望ましい。組織内の

すべてのシステムを考慮に入れて、あるシステムを切り離して対象にしないことが望ましい。リスクマネジメントの過程に関しては、この規格群の第 2 部（**JIS** 化未定）に示す。