エレクトロニックコマース・セキュリティ特集

UDC［681.324：343.45］.001.2

セキュリティポリシー
Security Policy

宮井貴志 Takashi Miyai　武内春夫 Haruo Takeuchi　山本明 Akira Yamamoto

要　旨

セキュリティポリシーは，組織の情報資産を適切に保護するための統一された基本方針である。本稿では，セキュリティポリシーの概念，セキュリティ関連規定における位置付け，標準的な内容，および作成上の留意点について述べる。

1. まえがき

近年，インターネットの普及に伴い世界中の情報を即座に入手できるようになってきたが，その反面，インターネットに接続されている情報システムは世界中から不正アクセスの脅威を受けることになった。図1はFBIとCSIが共同で行なった米国における情報セキュリティの現状調査結果[1]であり，ネットワーク犯罪が増加傾向にあること，外部からのシステム侵入と内部ユーザによる不正アクセスの脅威が大きいことなどを示している。

"CSI/FBI Computer Crime and Security Survey"
2000年3月（調査対象期間は最近12ヵ月間）

◆企業・行政機関などにアンケート調査。全回答数；643組織
　犯罪は増加傾向
◆インターネットからの攻撃；59%　（%は全回答数に対する比率）
◆内部ユーザによる不正アクセス；71%
◆ウイルス汚染；85%
◆ラップトップの盗難；60%
◆情報の盗難；20%
◆損失額；2億6,559万ドル（273組織の合計）
・大きいものから、情報の盗難、お金の詐取
◆犯罪を起こす可能性を持つ者は誰か？
・回答の81%が"社内の不満分子"を挙げている
・以下降順にハッカー、国内競争相手、国外競争相手、外国政府

図1　米国の情報セキュリティの現状
Fig. 1　Status of information security in U. S. A.

情報システムおよびそれが取り扱う情報（合わせて情報資産と呼ぶ）は，企業の運営にとって必要不可欠である。情報資産が盗難，悪用，破壊，妨害されないためには，企業全体の意思統一のもとに，企業構成員1人1人が情報資産の重要性を十分認識し理解した上で，情報資産を保護する必要がある。この情報資産の保護に関する企業全体の意思を定めたものがセキュリティポリシーである。

契約社会・訴訟社会である欧米では，個人情報などの保護に関して裁判に訴えられる危険を回避するための対策の1つとして，セキュリティポリシーが行き渡っている。セキュリティポリシーを備えていればセキュリティに関してしかるべき措置（due care）をとっていると言えるので，セキュリティ上の問題で訴えられた場合に有利である。実際に，米国ではセキュリティポリシーを有する企業の経営者に責任が波及しないと言われている。

一方，日本の金融機関に対するアンケート調査[2]によると，経営者または経営委員会によって承認された


宮井貴志
システムソリューションカンパニー　ビジネスソリューション事業部　ソリューション開発第一部　開発第四チーム


武内春夫
システムソリューションカンパニー　ビジネスソリューション事業部　ソリューション開発第一部


山本　明
システムソリューションカンパニー　ビジネスソリューション事業部　ソリューション開発第一部

セキュリティポリシーが存在する（9％），社内規定等の一部として存在している（25%）という結果であり，約3分の1の金融機関しかセキュリティポリシーを持っていない。金融監督庁が“金融検査マニュアル”[3]の中で金融機関に対してセキュリティポリシーを策定するように指導するなど，日本でもセキュリティポリシーの重要性が次第に認識され始めてきた。

2．セキュリティポリシーの概念

“金融情報等コンピュータシステムの安全対策基準解説書”[4]の中で，セキュリティポリシーは「会社（または組織）の情報資産を適切に保護するための会社としての統一された基本方針」と定義されている。つまり，セキュリティポリシーは，企業の経営方針に基づき，どの情報資産を，誰が，何故，どのようにして守るか，を明確に定義した基本方針であり，企業の経営者が全従業員に与える指針である（図2参照）。

なお，一般的に「セキュリティ」は，「情報セキュリティ」のほかに，「工場やオフィスなどの施設に関するセキュリティ」，「企業経営に関するセキュリティ」なども包含するが，本稿では「情報セキュリティ」に限定する。

情報セキュリティとは，以下の3つの要件を保証することである（“OECD理事会勧告のセキュリティガイドライン”より）。

- 機密性（confidentiality）；アクセスを許されていない者から情報資産を守ること。
- 完全性（integrity）；改ざんや破壊されないように情報資産を正確かつ完全な形態で維持すること。
- 可用性（availability）；情報資産をいつでも利用できるように維持すること。

3．セキュリティポリシーの位置付けと役割

図3にセキュリティに関する規定の体系におけるセキュリティポリシーの位置付けを示す。通常，セキュリティポリシーは数頁以内に簡潔にまとめられ，経営者からトップダウンで全従業員へ提示される。セキュリティポリシーは情報セキュリティに関する企業の憲法であり，なるべく変更しないことが望ましい。改版間隔は3年以上とするのが適当である。

セキュリティスタンダードは，セキュリティポリシーの意図を具体的な指示に展開したものであり，企業の法律に相当する。セキュリティ業務標準やセキュリティ規定などの名称で呼ばれている。セキュリティスタンダードは情報資産を保護するためのセュリティ対策を含み，技術進歩等によって規定内容に矛盾が生じた場合に改版される。改版間隔はセキュリティポリシーよりも短い。

さらに，各業務部門において，情報資産を保護し業務を円滑に遂行するために，情報システムの実装方法／操作手順／制限事項などを記述したマニュアルや手順書が作成される。

ここでパスワード管理を例として，セキュリティポリシー，セキュリティスタンダード，およびマニュアル／手順書の関係を示す。

- セキュリティポリシー；「利用者に情報システムの使用を許可する前に，利用者を識別・認証しなければならない。」
- セキュリティスタンダード；「利用者を識別・認証する手段としてIDとパスワードを使用しなければならない。パスワードは，各利用者が責任を持

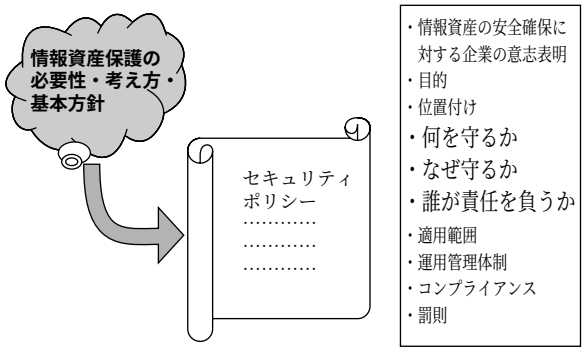

図2　セキュリティポリシーの概念
Fig. 2　Concept of security policy

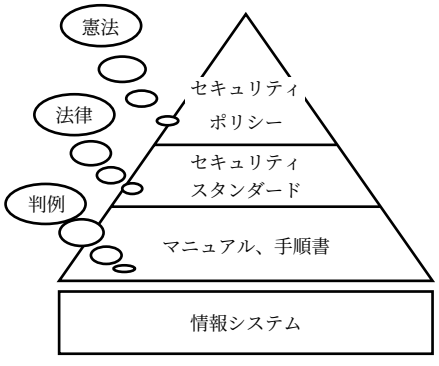

図3　セキュリティ関連規定の体系
Fig. 3　Hierarchy of security regulations

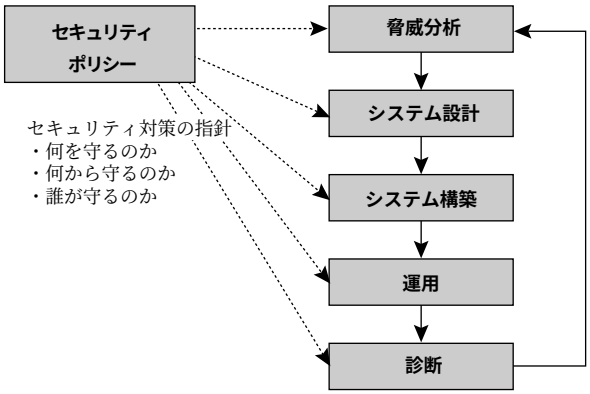

図４　情報システムのライフサイクル
Fig. 4　Life cycle of information system

って管理し，他の利用者に漏らしてはならない。」

- マニュアル／手順書；「IDとパスワードはシステム管理者が生成し，利用者に手渡すこと。パスワードの長さは８文字以上とし，３ヵ月ごとに定期的にパスワードを変更すること。」

このように，規定内容は段階的に具体化される。

図４は情報システムのライフサイクルにおけるセキュリティポリシーの役割を示している。企業情報システムの設計の初期段階で脅威分析を行ない，必要とされるセキュリティ機能を洗い出す。その後，セキュリティ機能を作り込み，システムの運用に至る。運用状況を診断し，セキュリティ上の問題が見つかれば，脅威分析から繰り返す。全ライフサイクルにおいて，セキュリティポリシーに基づいてセキュリティが確保される。

4．セキュリティポリシーの内容

一般的に，セキュリティポリシーには次のような項目が記述される。

1）セキュリティに関する経営者の意思表明；経営者が情報資産の安全性を確保するために何をするかを記述する。

2）目的；企業がセキュリティポリシーをなぜ必要とするか，また，セキュリティポリシーの役割は何かを記述する。一般的に，セキュリティポリシーの目的は次の4つの視点から記述する。

- 経営者の視点；顧客，株主，取引先企業，従業員などに対する社会的責任を遂行すること。
- 情報サービス提供部門の視点；情報の取り扱いに関する曖昧さをなくし，情報や情報サービスに対するセキュリティレベルを維持・向上させ，一貫性を持った情報保護を達成すること。
- 利用者の視点；利用者の責任範囲，利用可能なサービス範囲，遵守すべき行動規準や罰則を明らかにすることにより，情報セキュリティに対する行動規範とモラルの維持を図ること。
- 企業全体の視点；情報や情報サービスに対する意思統一を図り，管理的，人的，物理的，システム的，手続き的にバランスの取れた情報セキュリティを実現すること。

3）位置付け；セキュリティポリシーは情報資産を保護するための企業の基本方針であり，セキュリティ関連規定の最上位に位置し，他のセキュリティ規定よりも優先することを記述する。

4）情報資産；何がこの企業の情報資産であるかを定義する。また，情報の漏洩・紛失・破壊，情報システムの停止などによって生じるビジネス上の損失の大きさに応じて情報資産の重要度をランク付けする。さらに，情報資産の重要度に応じて，どのように情報資産を保護するかを抽象的なレベルで記述する。たとえば，重要機密情報は暗号化すること／情報システムの利用者を識別認証すること／アクセス制御によって情報資産を保護すること。

5）適用範囲；情報システム，情報(電子情報やハードコピー)，人(管理者や利用者)など，セキュリティポリシーの適用範囲を明確にする。

6）セキュリティの運用管理体制；企業全体のセキュリティ管理組織とその任務，情報資産ごとの管理者の設置とその責任，情報システムの利用者の責任などを記述する。

図５は，リスク[*1)]のランクに従って段階的にセキュリティ管理を行なう例を示している。リスクが軽微な場合には，業務部門の情報資産管理者がリスクに対応する。リスクが大きく業務部門では十分な対応が取れないと判断された場合は，全社レベルのセキュリティ管理部門が報告を受けて対応する。さらに，一定レベル以上のリスクには経営レベルの判断に従って対処する。

(7）教育・訓練；セキュリティに対する従業員の理解や意識を高めるために行なわれる，セキュリティに関する定期的な教育や訓練について記述する。

＊1）リスクは情報資産が損害を受ける可能性の大きさ。

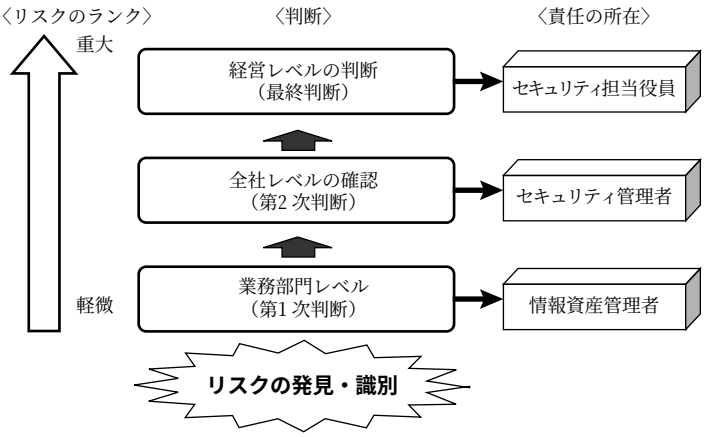

図5　情報システムの運用管理のイメージ
Fig. 5　Operation and management of information systems

（8）監査・レビュー；セキュリティに関する規定が遵守されているかどうかを調べるための定期的な監査やレビューについて記述する。
（9）コンプライアンス；個人情報や知的財産権の保護など，情報資産の利用に関する各種法令にセキュリティポリシーが準拠していることを記述する。
(10) 罰則；セキュリティポリシーに対する違反行為が発生した場合の罰則やルールを記述する。

5．セキュリティポリシー作成上の留意点

- セキュリティポリシーを作成する際は，“規定は必ず守ること，守る意思がない規定や守れない規定は作らないこと”が重要である。
- 保護すべき情報資産の決定は，脅威分析に基づいて行なう。脅威分析は，情報の盗難・破壊・改ざん・悪用や，情報システムの機能停止によって生じるビジネス上の損害の大きさと，損害発生の可能性(リスク)を明らかにするプロセスである。
- 情報資産の損害額とセキュリティ対策のコストのバランスが重要である。対策しない場合の損害額を上回るコストを対策にかけないこと。
- セキュリティ規定は利用者に不便を強いることが多い。制約が大き過ぎると利用者は規定を遵守しなくなるので，制約と利用者の使いやすさとのバランスをとることが重要である。
- セキュリティポリシーを作成するための参考書として，“金融機関等におけるセキュリティポリシー策定のための手引書”[5]や“BS7799”[6]などがある。

6．あ　と　が　き

金融機関を中心として，我が国でもセキュリティポリシー整備の機運が高まっており，セキュリティポリシー作成のためのサービスが求められている。沖電気は米国Atomic Tangerine社（旧SRI Consulting社）との技術提携に基づいて，セキュリティポリシーレビューサービスとセキュリティポリシー作成支援サービスを提供している。

7．参　考　文　献

1）“Computer Security ISSUES & TRENDS”, CSI, SPRING 2000.
2）“金融情報システム平成11年11月増刊46号”, (財)金融情報システムセンター，11.1999
3）“金融検査マニュアル”，金融監督庁，7.1999
4）“金融機関等コンピュータシステムの安全対策基準解説書”，(財)金融情報システムセンター，7.1998
5）“金融機関等におけるセキュリティポリシー策定のための手引書”，(財)金融情報システムセンター，1.1999
（6）“BS7799”，BRITISH STANDARD INSTITUTION, 5.1999