Part2　ブロードバンド時代のセキュリティ対策

第１０回 『情報セキュリティポリシー』策定のための基本的な考え方

NTTコミュニケーションズ株式会社
先端IPアーキテクチャセンタ
大納　亮一

最近、情報セキュリティポリシーの重要性がますます高まっている。それを受けて情報セキュリティポリシーを導入しようとする企業が増えている。今回は、情報セキュリティポリシーについて、なぜ必要なのか、情報セキュリティポリシーとは何か、またどの点に注意して策定すべきなのか、などについて解説していく。

1．情報セキュリティポリシーとは

情報セキュリティポリシーとは、情報セキュリティの確保に向けた取組みの基本的な考えや、その考えに基づいた対策及び管理運営等の方針を定めた規程である。

単にセキュリティポリシー（情報がつかない）と呼ばれる場合もある。本来、セキュリティとは企業の全資産（人、物、金、情報）に対する保全行為や、安全運用を意味する概念であるが、昨今、セキュリティポリシーといった場合は、情報セキュリティポリシーと同じ概念で使われることが多い。すなわち、情報のセキュリティを確保することを第１の目的としており、その目的を達成する上で関連する人や物などの資産の保護についても対象範囲としている（図１参照）。

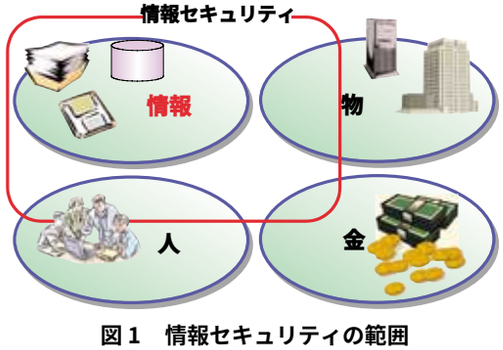

図１　情報セキュリティの範囲

2．情報セキュリティポリシーの必要性

情報セキュリティポリシーが必要になった背景としては、以下のようなことを上げることができる。

①企業経営へのIT利用の影響

ITの進展に伴い、CRMによる顧客情報の活用やSCMによる企業や組織を越えた情報の共有など、情報を企業経営に活用することが盛んに行われるようになってきた。そのため、企業内のいろんな部署でさまざまな重要情報が扱われるようになってきており、企業の一部の管理者だけが情報セキュリティ対策を行えばよいという時代から、ユーザー（社員だけではなく契約社員、派遣社員なども含む）１人１人がセキュリティ意識を持たなければならない時代へと変化した。さらに、インターネットの利用がビジネス上重要な位置を占めるようになり、インターネットと社内情報システムとのシームレスな接続がビジネス遂行上必須となった反面、社内情報システムは常に外部からの不正アクセスや情報漏洩などのリスクに曝されるようになった。

②雇用環境の変化の影響

近年の厳しい経営環境のもと、終身雇用制度の見直しを実施する企業が増えてきている。これに伴い、契約社員や派遣社員などを雇用する企業が増えてきているが、契約社員や派遣社員などは、正社員とは異なる価値観や会社に対する忠誠心を持って働いている。また、正社員でさえも早期退職制度や転職支援制度などの導入によって、企業に対して従来のような高い忠誠心を失いつつあるのが現状である。

厳しい経営環境の中では、終身雇用制度の見直しは仕方のないことではあるが、情報セキュリティの観点からは、内部犯行へのリスクが高まってきていると言わざるを得ない。現代の企業は、情報セキュリティの確保が、より困難な状況に置かれている。

このような状況の中、企業として情報セキュリティを確保するためには、行っている業務や利用しているシステムなどにおけるセキュリティの要求レベルを明らかにし、その要求レベルに向けた、網羅的、体系的な情報セキュリティ対策に組織全体として取り組む必要がある。情報セキュリティの確保に向けてどのようにして取り組んでいくのか、基本的な考えを経営者が示し、その基本的な考えに基づいて具体的な対策を定め、組織全体で取り組んでいくことになる。この中核となるのが情報セキュリティポリシーの策定と言える。

情報セキュリティポリシーは、経営者の情報セキュリティに対する強い意志を表したものであり、「わが社の情報資産をこのように守れ」という経営者から社員に向けた命令書とも解釈できる。

3．情報セキュリティ確保に求められる情報セキュリティ対策

セキュリティと聞いたときにシステムやネットワークに対することや技術的な対策だけを思い浮かべる人がいるかもしれないが、それだけではない。「ファイアウォールやウィルスソフトを導入しました」、「暗号化を行っています」などの対策でシステムやネットワークだけをいくら守っていても、重要な情報がプリントアウトされた紙が机の上に放置されていたり、パスワードの管理が不適切で第３者に漏れてしまったりすれば、簡単に情報漏洩につながる。システムやネットワークに対する技術的な対策だけでなく、クリアディスクやユーザーへのセキュリティ教育などの物理的環境的セキュリティ対策や人的セキュリティ対策などを含めた網羅的、体系的な情報セキュリティ対策が必要である。

情報セキュリティ対策を企業活動全般の観点から網羅的・体系的に国際規格としてまとめたのがISO17799である。企業が情報セキュリティ対策を網羅的・体系的に検討する上で、ISO17799は参考にできる。この国際規格は127個の具体的な情報セキュリティ対策項目を10の大分類（セキュリティ領域）で体系化したベストプラクティス集である。いずれの対策項目も情報セキュリティを確保する上で国際的に実施が強く推奨されている事項である（表１参照）。企業で情報セキュリティポリシーを策定する際にISO17799の内容を意識する事例が増えている。

表１　ISO17799の概要

大項目（セキュリティ領域）	中項目（セキュリティ目的）
セキュリティ基本方針	情報セキュリティ基本方針
組織のセキュリティ	情報セキュリティ基盤 第三者によるアクセスのセキュリティ 外部委託
資産の分類及び管理	資産に対する責任 情報の分類
人的セキュリティ	職務定義及び雇用におけるセキュリティ 利用者の訓練 セキュリティ事件・事故及び誤動作への対処
物理的及び環境的セキュリティ	セキュリティが保たれた領域 装置のセキュリティ その他の管理策
通信及び運用管理	運用手順及び責任 システムの計画作成及び受入れ 悪意のあるソフトウェアからの保護 システムの維持管理 ネットワークの管理 媒体の取り扱い及びセキュリティ 情報及びソフトウェアの交換
アクセス制御	アクセス制御に関する業務上の要求事項 利用者のアクセス管理 利用者の責任 ネットワークのアクセス制御 オペレーティングシステムのアクセス制御 業務用ソフトウェアのアクセス制御 システムアクセス及びシステム使用状況の監視 移動型計算処理及び遠隔作業
システム開発及び保守	システムのセキュリティ要求事項 業務用システムのセキュリティ 暗号による管理策 システムファイルのセキュリティ 開発及び支援過程におけるセキュリティ
事業継続管理	事業継続管理の種々の面
適合性	法的要求事項への適合 セキュリティ基本方針及び技術適合のレビュー システム監査の考慮事項

4．情報セキュリティポリシーの構成

企業が情報資産を保護するためには、様々な情報セキュリティ対策を網羅的・体系的に実行しなければならない。多様な情報セキュリティ対策を多数の社員に的確に

実施してもらうために、組織としては基本的な考えの提示だけでなく、その考えに基づいた具体的な指示書などの整備が必要となる。情報セキュリティポリシーを整備するとき、記述レベルの異なるこれらの文書類を階層的に構成していくのが一般的である。図2はその一例である。

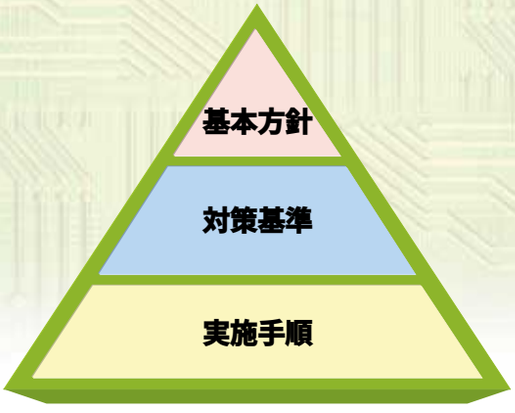

図2　セキュリティポリシー構成例

①基本方針

経営者の情報セキュリティの確保に向けた取組みの基本的な考えを示したもの。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。

②対策基準

基本方針の意図を具体的な指示に展開したもの。情報セキュリティに関する企業の法律に相当する。技術の進歩などによって内容に矛盾が生じた場合は改定される。

③実施手順

対策基準に基づき詳細な手順やガイドラインを記述したもの。

ここでパスワード管理を例として基本方針、対策基準、実施手順の関係を示す。

◆基本方針:「情報資産を不正なアクセス等から適切に保護するため、情報資産への適切なアクセス制御が行われなければならない。」

◆対策基準:「システム、サーバ等へのアクセスに際しては、IDとパスワードによる認証を行う機能を設けること。」

◆実施手順:「パスワードの長さは８文字以上としアルファベットとそれ以外の文字が混在すること。３ヵ月ごとに定期的にパスワードを変更すること。」

ただし、第1階層を指して情報セキュリティポリシーと呼ぶ場合もあれば、第2階層までを含めて呼ぶ場合、或いは全ての階層を指して呼ぶ場合もある。各階層の文書の策定では、多くの人や組織が関わるのが通例なので、情報セキュリティポリシーと呼ぶ範囲、階層ごとの記述の詳細加減などは、策定作業前に当事者間で理解を揃えることが必要である。

5．情報セキュリティポリシーの目的

情報セキュリティポリシーの主な目的は、以下である。

◆情報セキュリティの確保に向けた基本的な考えや方針を定めることで、組織の情報セキュリティの強化を行う。

◆情報セキュリティに取り組む考え方を明らかにすることで、顧客、株主、取引先企業、社員などに対する企業としての社会的責任を果たす。

◆ユーザーに対して、責任、行動基準、罰則などを明らかにし、情報セキュリティに対する意識の向上やモラルの維持を図る。

◆組織として情報セキュリティに対する意思統一を図り、組織全体で同一レベルの情報セキュリティ対策を実施する。

◆実施する対策の基準を定め、効率的で無駄のない情報セキュリティ対策を実施する。

6．情報セキュリティの策定手順

情報セキュリティポリシー策定の基本的アプローチは、まず、どの範囲を対象とするかを明確にし、対象となる範囲のリスク分析を行い、その結果に基づく対策を情報セキュリティポリシーとして定めることである。

リスク分析とは、対象範囲の情報資産を洗い出し、その情報資産の重要度を評価するとともに、どのような脅威（漏洩、改ざん、消去、破壊、故障等）にさらされているか、そしてその発生確率がどの程度あるかを推測し、そのリスク（危険度）を定性的、定量的に評価することである。

リスク分析の結果に基づき、誰が、何を、何から、どのようにして守るのかを情報セキュリティポリシーとして定めることになる。情報セキュリティポリシーの策定では、組織の実態に合わせた内容にすることが大切であり、組織が抱える情報セキュリティ上の弱点を洗い出すための実態調査は、情報セキュリティポリシー策定手順のカギとなる。

7．情報セキュリティポリシーを策定する際の留意点

情報セキュリティポリシーを策定する際、留意することとしては、以下のような点がある。

①経営者の支持を得ていること

情報セキュリティには組織全体が一丸となって取り組まなければならない。組織の一部にセキュリティの弱点があるとそこから綻びるからである。組織の隅々までこのような統制を行き渡らせ、情報セキュリティを組織に根付かせるには、経営者主導の強い意志を組織全体に示すのが良い。最近では、情報セキュリティポリシーの中で経営陣の情報セキュリティに対する取組み姿勢を明確にすることが、重要視される傾向にある。ISO17799を初めとする各種情報セキュリティ規格においても、経営層の取組み姿勢の明確化が、他の情報セキュリティ対策よりも優先的な推奨事項に位置付けられるようになってきた。情報セキュリティポリシーは経営者の支持を得た上で制定すべきであり、姿勢の明確化の手段として情報セキュリティポリシーの中に社長による取組み宣言文を含めるなどの工夫も考えられる。

②組織の実態に合わせた内容になっていること

最近では、情報セキュリティポリシーのサンプルやひな形が、多数出版されるようになった情報セキュリティに関する書物やホームページ*1に掲載されている。そのサンプルやひな形を参考にして情報セキュリティポリシーを策定することは、作成時間の短縮という意味では有効な手段ではある。しかし、ひな形をそのまま自組織の情報セキュリティポリシーとするのは、注意が必要である。ひな形のなかには、組織にとってリスクのほとんどないものへの対策が記述されていたり、組織にとってリスクの高いものへの対策が抜ける可能性があるからである。組織の実態に即していない情報セキュリティポリシーは、ユーザーからそっぽを向かれることになる。この意味で、組織の実態を知るためのリスク分析は、極めて重要である。

＊1:日本ネットワークセキュリティ協会
URL:http://www.jnsa.org/

③簡潔で明確な記述となっていること

情報セキュリティポリシーは、簡潔で明確な記述となっていなければならない。セキュリティコンサルティングの業界では、このことを例えて「12才程度の子供が読んでも分かる記述」と言うことがある。

情報セキュリティポリシーの読者は、知識や経験といったバックグラウンドの異なる多数の社員である。それぞれの知識や経験に基づき読まれるので、誰が読んでも同じ認識が得られる記述とすることが重要である。少なくとも５W1Hの原則を忘れずに記述することが必要である。

④修正を前提に、まずは制定すること

①～③の内容を読むと、「情報セキュリティポリシーの策定は難しい」、「制定するのに時間がかかる」と感じられた方が多いのではないだろうか？確かに、完璧を目指すと手間も時間も必要となる。特に、大企業では、組織の実態を把握するためとはいえ、現状調査を詳細に行っていたのでは、いつ制定できるのか予想もつかない。

完璧を期して策定に多くの時間を費やすより、まずは制定してみるぐらいの割り切りが必要である。制定することによって、ユーザーの反応や効果などを計ることも可能となるので、その状況をみて悪いところは直していけばよい。３回ぐらい修正すれば、良いものになっていくようである。

8．民間企業における情報セキュリティポリシーの策定状況

ここで、情報セキュリティポリシー策定の実状を把握するため、2002年９月に総務省が発表した「セキュリティ対策の状況調査」の中から民間企業における情報セキュリティポリシーの策定状況について示しておく。

情報セキュリティポリシーを策定している企業は、図３のとおり、全体の約29％にとどまっている。しかし、「現在、策定中である」と「策定を検討中である」を合わせて60％に達していることから、今後、企業における情報セキュリティポリシーの策定が着実に進むものとみられる。

また、情報セキュリティポリシーが機能しているかどうかについては、図４のとおり、策定済み企業の10％程度しか「十分機能している」と回答しておらず、機能しない理由としては、図５のとおり、「内容が抽象的で理解しにくいため」、「情報の重要度の定義があいまいで、どの対策を採用すればいいのか分からないため」、「セキュリティポリシーを保障する手段がなく実効性を欠くため」などが主なものである。前述した策定時の留意点を意識するだけでも、「十分機能している」情報セキュリティポリシーが増える。

9．まとめ

情報セキュリティポリシーについて、必要性、策定の手順や留意点などを説明してきた。

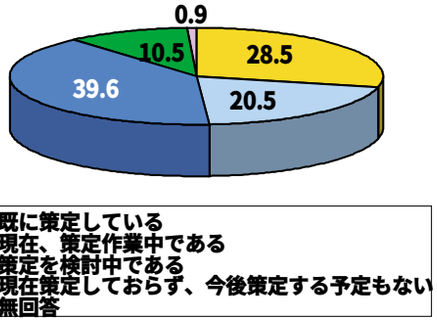

図３　情報セキュリティポリシーの策定有無（民間企業）

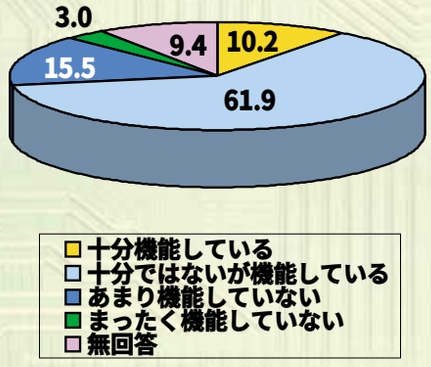

図４　情報セキュリティポリシーの機能の有無

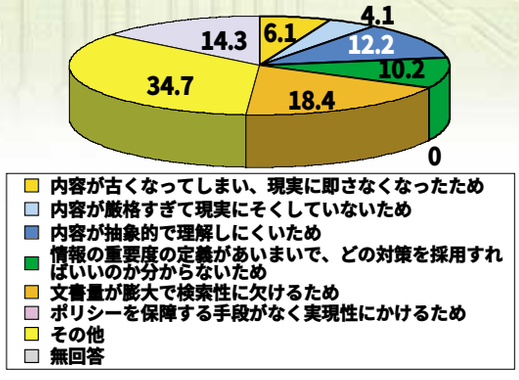

図５　情報セキュリティポリシーが機能していない理由

総務省の調査結果からもわかるように、多くの企業で情報セキュリティポリシーが策定されることが予想されるが、情報セキュリティポリシーは、情報セキュリティを確保する上での基本的な考えや方針を定めた単なる文書にすぎない。したがって、策定するだけでは、十分な効果は得られない。

組織の実態に即した情報セキュリティポリシーに基づき継続的な対策を実施することが、情報セキュリティを確保する上で、大切なことである。そのためには、情報セキュリティに係わるPDCAサイクル（Plan、Do、Check、Actionの4段階のマネジメントサイクル）を組織内に確立することが重要であり、情報セキュリティポリシーの策定は、そのPDCAサイクルを確立するための、第１歩である。

本連載へのご意見・ご感想は、弊誌編集部TEL:03-3507-0560、またはE-mail:bcm@bcm.co.jpまでご連絡願います。