情報化社会を生き抜くための企業セキュリティ

鉄鋼システム事業部
ＮＷＳ運用管理センター
ITエンジニア

鈴木　大介

Daisuke　Suzuki

鉄鋼システム事業部
ＮＷＳ運用管理センター
チームマネージャー

松井　聡

Satoshi　Matsui

情報漏洩等に代表されるセキュリティ脅威が増加している近年、企業におけるセキュリティ対策の実現は必須となりつつある。本論文では、具体的なセキュリティ対策方法や、セキュリティ対策において意識すべき点、セキュリティ対策環境の構築・維持にかかる負荷などについて筆者の経験をもとに解説し、効果的な企業のセキュリティレベル向上を実現するための手法について述べる。

1. はじめに

1.1. 近年のセキュリティ脅威の動向

近年、コンピュータやインターネットの普及に伴い、企業においても情報化が急速に進んでいった。しかし、その一方で個人情報の漏洩や不正アクセス、コンピュータウィルスといった企業の情報資産を脅かすセキュリティ脅威も同様に増加し、企業の情報資産を脅かしている状況である。図１に示すように、2004年に発生したセキュリティ事故の増加傾向だけを見ても、個人情報漏洩件数では前年の6.4倍(被害者数15.6倍)[1)]、コンピュータウィルス届数は3倍[2)]、不正アクセス数届数は1.5倍[2)]と、2003年度に比較して著しく増加してきていることがわかる。

企業において、増加するセキュリティ脅威から情報資産を守るためにセキュリティ対策の実現は急務であると言える。

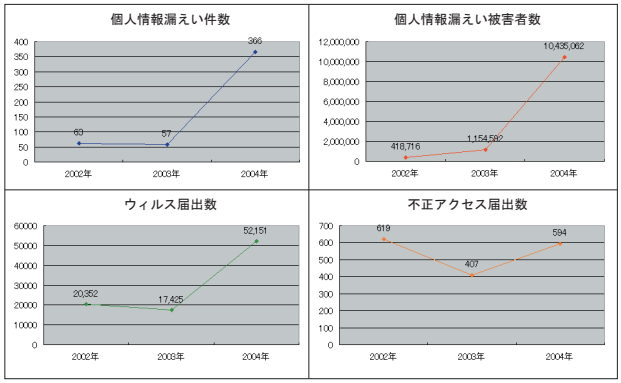

図１　セキュリティ脅威の推移

1.2. セキュリティ対策の現状

セキュリティ脅威が増加する一方で、情報セキュリティマネジメントシステム(ISMS)やプライバシーマークなどに代表されるセキュリティ対策に関する制度が注目され、様々な企業でこれらの認証制度を取得する企業が増加してきている。図2に示すように、2005年9月時点で情報セキュリティマネジメントは1,061社[3)]、プライバシーマークは2,040社[4)]と、多数の企業が認証取得を行っていることがわかる。他にもISO/IEC15408(セキュリティ評価制度)なども存在し、各種企業でセキュリティ対策の一環として活用されている。

これらのことから、企業の情報資産を脅かすセキュリティ脅威の増加に対抗すべく、各種企業は、企業セキュリティの向上について大きな関心を抱いているといえる。

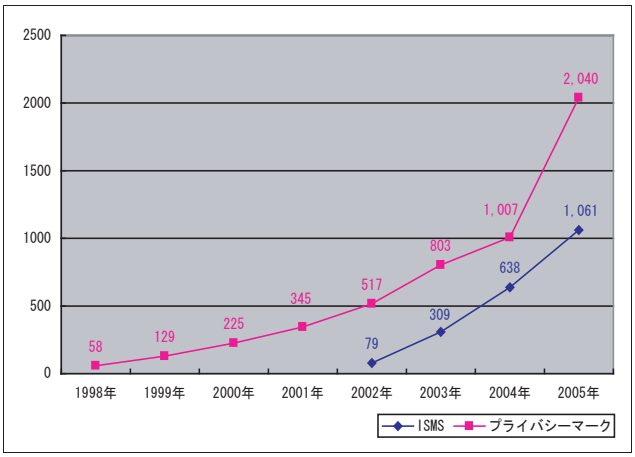

図２　ISMS認証およびプライバシーマーク付与認定 取得事業者数の推移

2. セキュリティ対策の実現

企業においてセキュリティ対策が必須であることは前述のとおりだが、実施すべきセキュリティ対策は多岐にわたっており、正しく理解しなければ効果的なセキュリティ対策を実現することはできない。

本論文では、企業におけるセキュリティレベルを向上するために必要な以下の項目について具体的に解説し、企業におけるセキュリティ対策環境実現のための礎となることを目的とする。

【セキュリティ対策】

(1) ポリシー／ルールの策定
(2) 物理アクセスセキュリティ
(3) 論理アクセスセキュリティ
(4) 人的セキュリティ
(5) セキュリティ検査
(6) 事故管理
(7) ワークプレイスセキュリティ

3. ポリシー／ルールの策定

セキュリティ対策を実現するにあたり、最も基準となるものが「ポリシー／ルール」である。本章では、セキュリティポリシー／ルールを策定する上で必要な事柄について解説する。

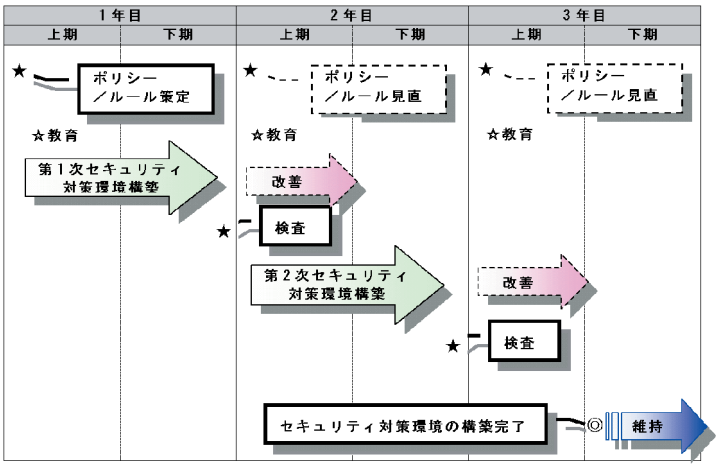

図８　セキュリティ対策環境スケジュール（例）

表３　セキュリティ環境の構築／維持にかかる作業負荷（例）

作業項目	対象	年間 作業負荷	例）頻度 例）対象	例）作業負荷 合計（年間）
セキュリティ設定 の実装	サーバ1台	1人日	初回 200台	200人日
ヘルスチェック および改善	サーバ1台	1人日	年1回 200台	200人日
ユーザID棚卸	1ユーザID	0.01人日	年1回 20,000ID	100人日
セキュリティパッチ 適用	サーバ1台	1人日	適宜 200台	200人日
ワークプレイス セキュリティ定期検査	1ユーザ	0.02人日	年1回 1500人	35人日
合計				**735人日 （約37人月）**

ティ環境構築におけるスケジュールの例を示す。

6.2. 作業負荷

セキュリティ環境を構築・維持するためには、様々な作業が発生する。構築段階においては、ポリシー／ルールの策定に始まり、情報システムへのセキュリティ設定の実装や、ユーザIDの初回棚卸、ワークプレイスセキュリティの実施などがある。また、運用段階においても、定期的なポリシー／ルールの見直しや、ルールに従った各種承認業務等の運用、定期ヘルスチェックやユーザIDの再検証が発生する。表３に、システム管理者における作業負荷を明記する。なお、セキュリティ対策環境の構築・維持には、表３に示す以外にも管理者におけるポリシー／ルールの策定・見直しにかかるコストや、物理アクセスセキュリティを実現するための設備投資なども発生する。

表３を見てもらうとわかるように、セキュリティ環境を構築・維持するのは、非常にコストがかかり、決して容易なことではない。しかし、セキュリティ脅威は日々進化しており、セキュリティ対策の実装が遅れれば、その分セキュリティ脅威によるリスクも増大してしまうため、迅速なセキュリティ対策の実現は、企業にとって重要である。

6.1.節で、セキュリティ意識を確実に高めていくために、段階的にセキュリティ対策を実現していくことを述べたが、コスト負荷を低減させるためにも、セキュリティ対策を段階的に実施することは有効である。

フェーズを繰り返して実施することを指す。

セキュリティ対策は、単純にポリシー／ルールを策定しセキュリティ対策環境を構築するだけで完了となるものではない。情報資産を脅かすセキュリティ脅威は日々進化しており、常に新しいセキュリティ対策を講じなければ、情報資産を保護することはできない。また、4.4節 セキュリティ検査でも述べたように、一度適用したセキュリティ対策が、永続的に適用されているとは限らず、定期的に見直しを行わなければならない。PDCAサイクルを繰り返すことで定常的に脆弱性を改善していかなければ、セキュリティレベルを維持することはできず、最終的には、情報資産をまったく保護できない環境となる。

筆者は、セキュリティ対策環境をPDCAサイクルに則って維持・管理していくため年間スケジュールを年度ごとに作成し、スケジュール上で決定したチェックポイントに従って、定期的な責任者への報告や見直しを実施した。スケジュールを作成し、確実に管理することで、セキュリティ対策環境の見直しの漏れを防止した。

5.3. 意識レベルの共通化

セキュリティ対策を行う上では、利用者も管理者も、全て同じセキュリティ意識を持つことが重要である。

セキュリティは、水の入った桶として例えられることがある。水の入った桶は、壁面の一部でも低い箇所があれば、そこから水が漏れ、水面の高さは一番低い壁面の高さまで低下する。セキュリティもこれと同じで、高いレベルのセキュリティ対策を施したとしても、一部の人間のセキュリティ意識が低く、ポリシー／ルールどおりのセキュリティ対策が実現できなければ、そこが脆弱点となり、全体のセキュリティレベルも、その低い部分まで低下してしまう。例えば、いくら推測が困難なパスワードを用いた利用者認証環境を運用しても、一部の人間がパスワードをメモに記録して、コンピュータの横などに貼り付けていれば、そのパスワードを利用されて不正にアクセスされてしまう。

意識レベルの共通化を図るためには、徹底したセキュリティの教育が必要である。しかし、セキュリティ意識を押し付けてしまうことは、逆効果であるため、注意しなければならない。押し付けによる教育は、受講者に対して浸透しにくく、結果的にセキュリティ対策が実施されないでいることがある。そのため、セキュリティ意識の向上のためには、押し付けではなく利用者と管理者が一丸となって「セキュリティレベルを高めていく」ことが重要である。

筆者がセキュリティ対策環境の構築に携わった際は、対象となる地域が広域に渡っていたため、管理者・利用者へのセキュリティ意識の浸透が非常に困難であった。そこで、定期的な教育の他、年間数回の説明会を開催し、発生する作業の必要性や重要度について情報の共有を図り、セキュリティ意識の向上に努めた。

5.4. ログ保管の徹底

重要点の4つ目として、ログ保管の徹底を述べる。

4.2.3.(4)の中でも、様々な記録(ログ)を保管し、検査することを述べてきた。ログの記録は、不正行為を監視する他、その抑止行為になるが、それ以上に有事が発生した際に、その原因を追求し、再発を防止するための最も重要な情報となり得る。

ログを記録するにあたっては、記録が必要なログには何があるかを明確に定義し、その重要度に応じた保存期間を定義し、保存することが重要である。また、ログの中には「誰が」「いつ」「何をした」ということが明確にわかるように記録し、ログを精査することで不正を行った個人まで特定することが可能であることが、ログの記録において重要である。

6. セキュリティ対策環境の構築・維持における負荷

本章では、筆者が過去経験したセキュリティ対策環境の構築および維持における経験をもとに、セキュリティ対策環境の構築・維持にかかる負荷について解説する。

6.1. スケジュール

結論から申し上げると、セキュリティ対策環境を構築するためには非常に長期間の時間が必要となる。なぜならば、5.3節でも述べたとおり、全体的なセキュリティ意識を向上させるためには、押し付けによる教育では効果がなく、管理者側が高い水準のセキュリティ対策を望んだとしても、利用者の意識の向上が追いついてこないためである。

構築を行う環境にもよるが、100台から200台程度の情報システムが稼動する環境においては、定期的な教育・検査を繰り返し、1年から2年程度の時間をかけ段階的にセキュリティ対策を講じていく必要がある。図８に、セキュリ

な状況に陥ることも考えられるため、独自での行動は禁止し、責任者への報告を第一にするよう運用ルールを定義することが大事である。

4.6. ワークプレイスセキュリティ

ワークプレイスセキュリティとは、ワークプレイス（Work Place）、すなわち勤務場所におけるセキュリティ対策である。今まで解説したセキュリティ対策とは異なり、全ての従業員が意識して行わなければならないセキュリティ対策である。

対策内容は、紙媒体に記録された情報資産などの施錠管理の徹底や、ノートパソコンなどのワイヤーロック、帰宅時の施錠管理など、従業員が扱う情報資産の盗難防止を目的とした物理セキュリティや、コンピュータ起動時の始動パスワードの徹底、離席時のスクリーンロック、廃棄時のHDD完全消去運用など、情報漏洩対策としての論理セキュリティが存在する。ワークプレイスセキュリティは、サーバなどの情報システムへのセキュリティ対策とは異なり、対象となる環境が全従業員である。そのため、すべての従業員への教育や定期的な点検などを徹底しなければならず、従業員のセキュリティ意識が高くなければセキュリティレベルの維持は難しい。

5. セキュリティ対策を行う上での重要点

４章では、セキュリティ対策を実施する上の具体的な対策方法について述べたが、本章では、セキュリティ対策を実現する上で意識しなければならない、４つの重要な点について論じる。

5.1. 性善説と性悪説

従来、日本人は「性善説」（不正はやらないだろう、と信じる）が美徳として考えられてきた。しかし、セキュリティ対策を行う上では逆の視点である「性悪説」（誰でも不正をするだろう、と疑う）の考え方を意識する必要がある。

NPO法人日本ネットワークセキュリティ協会（JNSA）の調査[1)]では、2004年に発生した366件の個人情報漏洩事件のうち、約10%が内部犯行によるものであったと報告している。このことからも、従業員などが不正行為を行う可能性があることは明白であり、「性善説」にたったセキュリティ対策では、十分なセキュリティを維持することができないといえる。セキュリティ対策を行う上では、「性悪説」にたってセキュリティ対策を実現し、外部の人間のみならず、内部からも情報資産を保護することが重要である。４章で述べたセキュリティ対策においては、各種履歴（ログ）の管理や検査が、「性悪説」に立ったセキュリティ対策である。許可を与えられた正規の利用者であっても不正を行う可能性があると考え、利用履歴を記録し検査することは、まさに「性悪説」に立ったセキュリティ対策であるといえる。

5.2. PDCAサイクル

PDCAサイクルとは、図７に示すように、Plan（計画）、Do（実施）、Check（点検）、Action（処置）の４つの

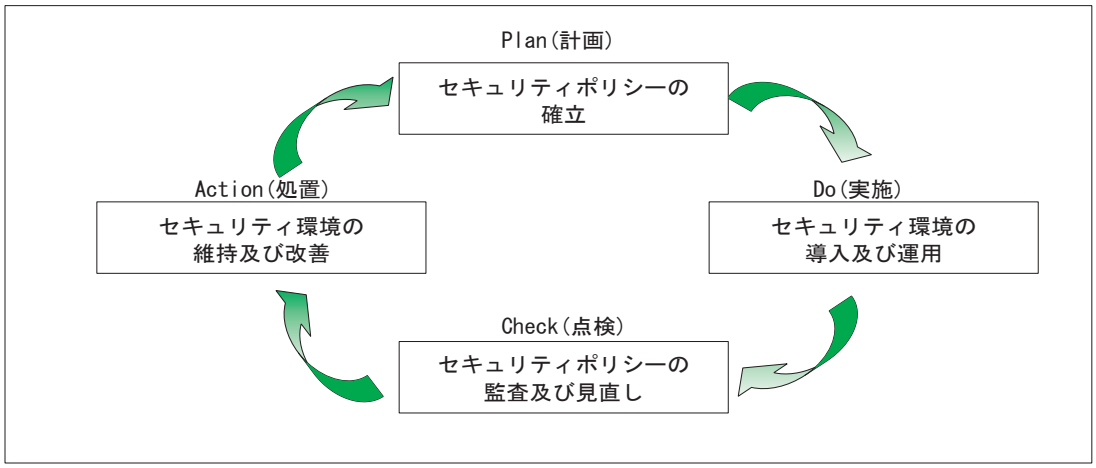

図７　PDCAサイクル

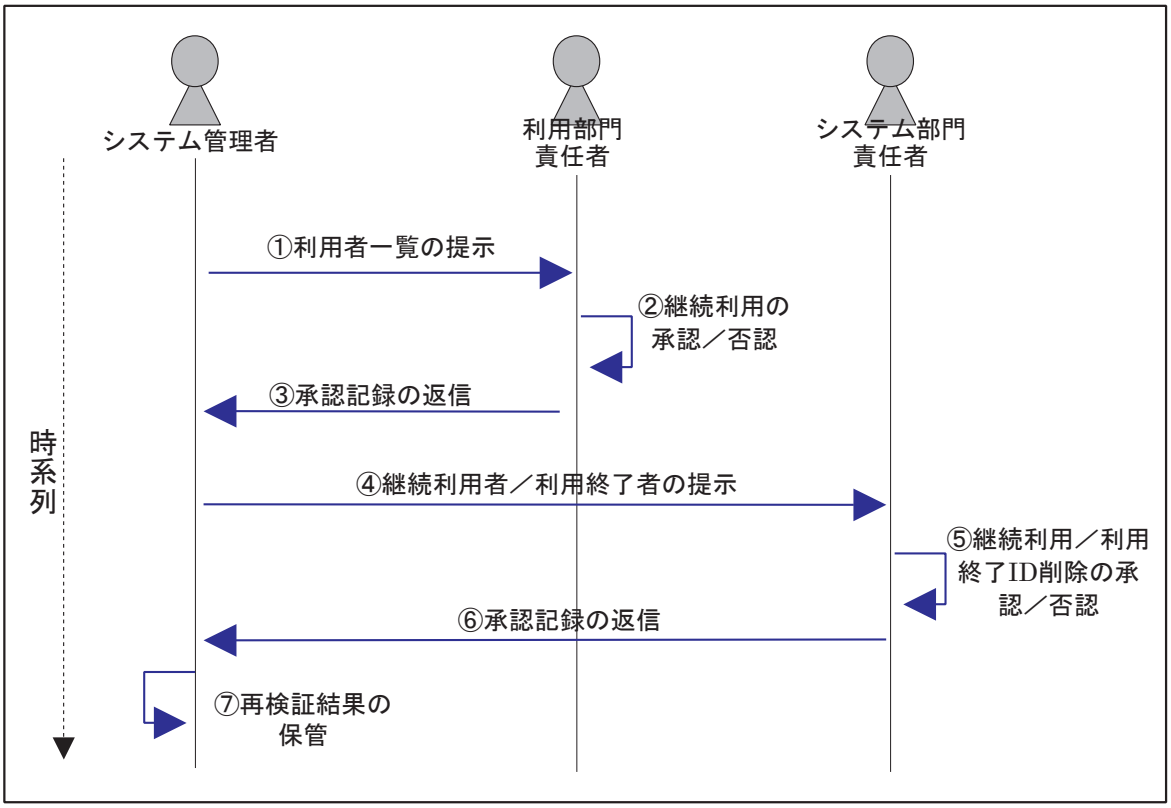

図６　ユーザ ID再検証の流れ

4.4.3. 監査

セキュリティ対策環境においては、ヘルスチェックやユーザID再検証による定期的な検査の他、セキュリティ監査による全体的な検査も必要となってくる。監査では、セキュリティ環境運用が正常に行われているかのチェックの他、ポリシー／ルールに不備はないか等、セキュリティ対策環境全体に対する検査を行う。

監査には、社員が監査員として行う内部監査と、外部の監査機関を利用した外部監査とが存在する。内部監査は、社員を監査員として任命し、セキュリティ環境が正常に運用されているかを監査する。社員による監査のためコスト負荷は少ないが、専門的な判断が難しいというデメリットがある。外部監査は、外部の専門機関への依頼となるためコスト負荷は大きくなるが、専門的な視点で監査されるため、より厳密な検査が可能となる。

短間隔での監査として内部監査を利用し、長間隔での監査として外部監査を併用することで、双方の利点を生かした効果的な監査環境を実現できるとともに、確実なセキュリティ対策環境の維持を実現することができる。

4.5. セキュリティ事故管理

どのようなセキュリティ対策を行っても、情報資産をセキュリティ脅威から完全に防御することは非常に困難である。そこで、事前にセキュリティ事故が発生した際の対応手順を定義しておき、迅速に対応できるようにしておくことが、セキュリティ事故管理である。

セキュリティ事故は、不正アクセスの発生や、ウィルス感染など、多岐にわたって存在する。発生する可能性のあるセキュリティ事故すべてについて明確に運用・報告手順を定義しておくことで、実際に有事が発生した際に迅速に対応することが可能となり、被害を最小限に食い止めることができるとともに、再発防止に繋げることができる。

セキュリティ事故管理を定義する中では、独自での行動を禁止するようにしなければならない。セキュリティ事故の発生に伴い、サービスの停止が発生した場合などは、迅速にサービスを復旧させようと、システム管理者が独自で行動してしまうことがある。しかし、その行為は結果として事故発生原因追求の妨げとなり、再発防止策を講じることができなくなる可能性がある。また、独自で調査することで、不用意に事故原因となる個人・組織に接触し、危険

4.3. 人的セキュリティ

人的セキュリティとは、情報資産の利用者が不正な行為を行わないようにするためのセキュリティ対策である。セキュリティ脅威は、意図的／非意図的に関わらず人を介して行われることが多い。そのため、利用者への教育などによるセキュリティ対策は、物理アクセスセキュリティや論理アクセスセキュリティなどと同様に、重要なセキュリティ対策の一つである。

4.3.1. 教育

人的セキュリティで最も重要なものは、利用者への教育の徹底である。ポリシー／ルールによる厳密な保護対策を定義していたとしても、情報資産の管理者や利用者が、そのルールを認識していなければルールは機能しない。また、セキュリティ対策の重要性を教育し、管理者・利用者がともに高いセキュリティ意識をもつことが、セキュリティを維持していくためには必要となる。

教育では、ポリシー／ルールの通知の他、セキュリティ対策の必要性や重要性を説明することで、利用者のセキュリティ意識を向上させる。また、ログ採取・検査により不正行為の監視を行っている旨、不正行為を行った際の罰則(後述)などについても説明し、利用者が不正行為を行わないよう、予防措置を行っておくことも必要となる。

教育は、ポリシー／ルールの更新の都度実施する。また、更新がない場合であっても、年1回は定期的に実施することが望ましい。

4.3.2. 罰則

利用者への教育に併せて重要となるのが、罰則の定義である。本来であれば罰則により利用者を縛るということは好ましくないのかも知れない。しかし、緩いルールでは、どうしてもルール違反を行う者が出てくるものである。企業における就業規則等と合わせ、セキュリティ違反を行った利用者に対しては、厳重な罰則を与えるよう定義し、セキュリティ違反を犯さない環境を作り上げることが重要である。

4.4. セキュリティ検査

セキュリティ検査は、ポリシー／ルールにより定義された各種運用や、情報システムの設定値が、間違いなく遵守されているかを定期的に検査し、漏れがないように管理することを目的とする。セキュリティ検査には「ヘルスチェック」と「ユーザID再検証」「監査」の３種類が存在する。

セキュリティ対策は、ポリシー／ルールどおりに運用されてこそ、最大の効果を発揮する。そのため、ルール違反がないように定期的な検査を設けることは企業セキュリティを高めていく上で重要な要素である。

4.4.1. ヘルスチェック

ヘルスチェックとは、情報システムにおいて、ポリシー／ルールを遵守するために設定した、パスワードルールや、アクセス権などの各種設定値が、ルールどおりに設定されているかを確認することを指す。情報システムの設定値は、アプリケーションの追加や、例外的な運用で変更されてしまう可能性があり、変更されてしまうと、セキュリティレベルが低下してしまう。そのため、定期的に設定値を確認し、脆弱性を残さないようにする必要がある。

システムの制約等により、どうしてもルールに準拠することができない場合は、4.2.3.(3)で述べたセキュリティパッチの適用と同様、セキュリティ責任者の承認を得た上で運用するなどのルールを定義し、脆弱点が存在することを認識し、運用などでカバーできるよう、フォローすることが重要である。▪

4.4.2. ユーザID再検証

ユーザID再検証とは、4.2.1.項のユーザの識別と認証でも述べた、利用者に付与されたユーザIDの棚卸と退職者検証を指す。図６に、ユーザIDの再検証の流れを示す。

ユーザID再検証は、利用者の業務上の必要性を定期的に検査するとともに、業務利用以外に使用されないことを保証することにも繋がるため、セキュリティ検査の有効な手段として考えることができる。ユーザIDの再検証においては、特に特権IDの利用状況の管理を徹底して行う必要があり、通常のユーザIDよりも頻繁に再検証を行うことを推奨する。

アクセス権についても、定期的に業務上の必要性を棚卸することを管理基準の中で定義する。アクセス権は必ずユーザIDと紐付くため、ユーザIDの棚卸と同時に実施することで、効率的に実施することができる。

4.2.3. システムセキュリティ

本項では、情報システムを不正アクセス等のセキュリティ脅威から保護することを目的とした、システムセキュリティについて論述する。

システムセキュリティでは、「暗号化」「ウィルス対策」「システム脆弱性対策」「不正アクセス監視」の４点について定義し、運用する。

(1) 暗号化

保護対象の資産価値に応じて、情報資産(ハードディスク)や通信経路を流れる情報資産の暗号化を実現するため、暗号化鍵の長さや利用期間、利用手順等を定義し、情報資産の暗号化による情報漏洩の防止を行う。

(2) ウィルス対策

情報システムへのウィルス対策ソフトウェアの導入を徹底するとともに、定期的なディスクスキャン、定義ファイルの更新を実施して、コンピュータウィルスによるセキュリティ脅威から情報資産を保護する。近年、コンピュータウィルスは非常に頻繁に新種が発生しているため、ウィルス定義ファイルの更新は定期的に実施し、常に最新の定義ファイルが有効となっている状態で運用しなければ効果的なウィルス対策は実現できない。

(3) システム脆弱性対策

定期的にOSなどのセキュリティパッチの適用を徹底し、システムのセキュリティホールを常に排除していくことで、情報システムに保管された情報資産を保護する。セキュリティパッチは、最新のものを適用するだけではなく、過去に公開されたすべてのセキュリティパッチを適用しなければ、すべての脆弱性を排除することができないため、情報システムの構築時にセキュリティパッチをすべて適用するよう、ルールを定義しておくとともに、定期的に情報システムのセキュリティパッチ適用状況の監査を実施して、セキュリティパッチの適用漏れが発生しないように管理することが必要となる。

なお、使用するアプリケーションなどの制約によりセキュリティパッチの適用ができない場合は、セキュリティ責任者へ未適用時のリスクを説明した上で、未適用に対する承認を得ることをルール化し、情報システムが保有するリスクを確実に把握しておくことが重要である。

(4) 不正アクセス監視

アクセスログの定期的な検査により実現する。アクセスログを検査することで、不正アクセスの有無を把握するとともに、不正アクセスに対する抑止効果も期待できる。

4.2.4. ネットワーク管理

情報システム同様、ネットワークも情報資産を保護する上では重要な要素である。特に、多くの企業では社内ネットワーク（LAN）により情報システム間が接続され、インターネットや他企業などの社外ネットワークとも接続していることから、ネットワークについても厳密に管理を行う必要がある。

ネットワークの管理は、社内ネットワークの管理と、社外ネットワークとの接続に関する管理の2通りが存在する。

(1)社内ネットワーク管理

社内ネットワークを安全に管理するため、ネットワーク機器の管理は限定された者のみが行うことが必須である。そのため、情報システムの利用と同様、ネットワークの管理者は限定し、業務上の必要性を加味した承認ルールに則って権限を付与するとともに、定期的な棚卸による管理者の見直しを行う。

(2)社外ネットワーク管理

社外ネットワークとの接続は、社外から社内へのアクセスと、社内から社外へのアクセスの双方を管理する。ここで社外とは、インターネットや他企業との企業間接続などを指す。

社外ネットワーク管理では、接続可能な経路を限定し、許可されていない経路での社外との接続を禁止する。許可されていない経路は、セキュリティが十分に確保されている保証がないため、重大な脆弱性となってしまう。接続方法についても、接続時の認証の徹底や、利用アプリケーションの限定(ファイル転送の禁止など)を定義付け、不要な通信を許可しないことが重要となる。

また、社外ネットワークとの接続ポイントは、特にセキュリティ脅威に晒されやすいため、IDS（不正アクセス検知装置：Impact Detective System）等による攻撃検知環境などによる防御も重要となってくる。

必須だが、削除漏れがないことを確実に確認するためにも、1ヵ月に1回から四半期(3ヶ月)に1回程度の頻度で実施することが望ましい。退職者検証は、人事情報のデータベースなどとシステム的な連携により退職者のユーザIDを自動的に削除するなど処理の自動化も可能である。退職者検証の自動化は、確実な削除の実現と作業負荷の軽減に繋がるため、セキュリティ運用において有効な手段となる。

(3)パスワード管理

利用者認証において、ユーザIDと同様に重要となってくるのが、パスワード等の識別コードである。ワンタイムパスワードなど、常に異なるパスワードを利用する方式であれば問題はないが、文字列によるパスワードを利用する場合は、パスワードが漏洩した際に不正アクセスを引き起こす可能性が高くなるため、その管理も利用者認証においては重要な要素となる。パスワードの管理は、表2に示す5種類の項目を用いて管理すると良い。この5項目は、現在多く利用されている各種オペレーティング・システム(以下、OSとする)で、標準で設定可能な項目であることが多く、容易に実現することができる。

4.2.2. 資源保護

資源保護とは、コンピュータなどの情報システムに保管された情報資産の用途に応じて、必要な利用者へのみアクセス権を付与し、不必要なアクセスから保護することである。情報システムに保管された情報資産は、すべてが同じ用途であることはない。そのため、ユーザIDの付与だけでは厳密に情報資産を保護することはできず、情報資産へのアクセス権による保護が必要となってくる。

(1)情報資産の分類

情報システムに保管される情報資産には、大きく分けて２種類ある。一つは、企業にとって保護すべき機密情報等の「ユーザ資源」と、もう一つはOS等の情報システムが正常に稼動するための「システム資源」である。情報システムに保管された情報資産は、OS等の制御機能により保護されている。そのため、情報システムが正常に稼動していなければ確実に情報資産を保護することはできないため、システム資源についても、機密情報等のユーザ資源同様、厳密にアクセス権を管理する必要がある。

(2)アクセス権の付与

アクセス権は、ユーザIDの付与同様に業務上の必要性に応じて上長の承認のもとで付与する。システム資源は、通常IDの利用者がアクセスする必要はないため、システム管理者、すなわち特権IDを保有する者にアクセス権の付与を限定する。

(3)アクセス権の棚卸

表２　パスワード管理ルール

項目	説明
有効期間	パスワードの有効期間。パスワードの定期的な変更を促し、パスワード漏洩による不正アクセスの可能性を低減する。 短期間では運用を妨げる要因となり、長期間では有効性が低い。
最小文字数	パスワードに使用する文字数の最小数。文字数を増やすことでパスワードの推測を困難にする。 少ない文字数では効果が低いが、多すぎてもパスワードを記憶することが困難になり、紙媒体などへのメモなどを助長する要因となる。
使用文字種	パスワードに使用可能な文字の種類。英字だけでなく数字や記号、大文字／小文字の使用を強制することで、パスワードの推測を困難にする。 最小文字数同様、厳しすぎるルールでは、記憶することが困難になるため注意が必要。
再利用禁止回数	過去に使用したパスワードの再利用を禁止する回数。有効期間と併用し、定期的に異なる文字列へのパスワード変更を強制する。
ロックアウト	無効なパスワードを複数回連続で入力した際に、ログインを禁止するルール。パスワードの推測による不正ログインの実行を防ぐ。 ロックアウトまでの回数が短すぎると、単純な入力ミスでさえロックアウトしてしまうため、運用に支障を来たす。

保護すべき可搬記憶媒体は、入室制限エリア内や施錠可能な棚等への保管を定義する。

(2)管理方法

可搬記憶媒体の管理では、媒体管理台帳を作成し、保護対象となる全ての媒体について台帳管理を行う。

また、保管場所への入退室や施錠管理方法を定め、物理的に情報資産を保護する。保管場所への入退室や施錠棚の開閉については、入室制限エリアへの入退室同様、管理責任者により業務上の必要性に応じた入退室・保管棚の鍵貸し出し許可の付与を管理するとともに、入退室・利用履歴の記録・検査を実施する。

(3)移送手順

可搬記憶媒体は、サイズが小さいことから情報資産の遠隔地保管などを目的とした移送を行うことがある。移送時における紛失などを防ぐため、移送前には、実施者・実施日時・目的・媒体名・媒体本数・移送先などを移送履歴として、移送先での受信時は、受信者・受信日時・媒体名・媒体本数・移送元などを受信履歴として記録し、定期的な記録の検査を実施することで媒体紛失の防止を徹底する。

(4)定期的な棚卸

可搬記憶媒体の棚卸では、媒体名や媒体数を再確認することで媒体の紛失がないことを確認するとともに、保護対象となる媒体の見直しを行う。保護対象を定期的に見直すことで、保護すべき情報資産の確実な保護を実現するとともに、保護不要な媒体に対する過剰保護などによる無駄な運用負荷を削減する。

4.2. 論理アクセスセキュリティ

論理アクセスセキュリティとは、コンピュータ等の情報システムに保管された情報資産へのアクセスを管理することで、情報資産を保護するためのセキュリティ対策である。情報化が進む昨今では、紙などの物理媒体以上に、情報システムに保管される電子的な情報資産の量は増加する一方である。そのため、厳密なルールのもとで情報資産へのアクセスを管理しなければ、情報資産を保護することはできない。また、インターネットなどの通信手段が多様化している現状では、電子化された情報資産は容易に世界中へと飛散する可能性が高い。そのため、論理的に情報資産を保護することは、企業セキュリティにおいて非常に重要である。

4.2.1. ユーザの識別と認証

まず、情報資産を論理的に保護するために重要となってくるのは、情報資産へアクセスするための認証である。許可された者のみが情報資産へアクセスできるように管理するためには、ユーザIDとパスワードなどの識別コードによる利用者認証を行う必要がある。

(1)ユーザIDの付与

利用者認証による利用者制限を行うために必要となってくるのが、ユーザID付与に関するルールの定義である。ユーザIDの付与は、業務上の必要性を判断する必要があり、上長の承認などが必要な運用ルールを定義することが望ましい。

ユーザIDは、大きく分けて2種類存在する。情報システムを利用するためのユーザID（以下、一般IDとする）と、情報システムを管理するためのユーザID（以下、特権IDとする）である。特権IDはシステムの各種設定を操作することが可能であるため、より厳密に行う必要があり、ユーザID付与とは別にシステム管理権限付与のためのルールを定義する必要がある。システム管理権限の付与は、ユーザID利用者の上長による承認だけではなく、利用する情報システムの管理責任者による許可を設け、より厳しく管理することが重要である。

なお、ユーザIDを付与する際は、個人に対してのみ付与するよう徹底することを忘れてはならない。なぜならば、複数の利用者によりユーザIDを共有していた場合、セキュリティ事故が発生した場合に、アクセスログ等の履歴からでは、個人を特定することができないためである。

(2)ユーザIDの棚卸

ユーザIDについても物理アクセスセキュリティにおける入室許可者同様、定期的に業務上の必要性を判断し、棚卸を行うことは必須である。ユーザIDの棚卸は、最重要の情報資産を管理する情報システムのユーザIDについては、1ヶ月ごと、中レベルの資産価値を持つ情報資産であれば、四半期(3ヶ月)に1回、それ以外の低レベルの資産価値であれば年1回～2回実施するなど、管理する情報資産の価値に応じて実施することが望ましい。

また、定期的な棚卸とは別に、退職者検証を定期的に行うことも重要である。退職者検証とは、ユーザIDの利用者が退職によりユーザIDを利用しなくなっていないかを定期的に判断するための確認作業である。退職者が利用した

理領域を保護しなければ、電子情報であっても完全に防御することはできないため、物理アクセスセキュリティを高めることは、情報資産を守る上で重要である。

4.1.1. 入室制限エリアの明確化

本項では保護すべき情報資産が保管されている物理領域のレベル分けについて説明する。

保護すべき情報資産は、必ずどこかの物理領域の中に存在する。そこで、物理領域を数段階のレベルに区分し、レベルごとに実施するセキュリティ対策のレベルを分けるとともに、設置する保護対象を分ける。例えば、図5に示すように「ハイレベル管理エリア」「管理エリア」「それ以外」のように3つのレベルに物理領域を区分けし、保護対象となる情報資産を保管する。入室制限エリアを明確にし、レベル分けを行うことで、施錠設備などの設置などを行う箇所を限定し、情報資産の保管も、その資産価値に応じて区分することができることから、効果的に設備投資を行うことができる。

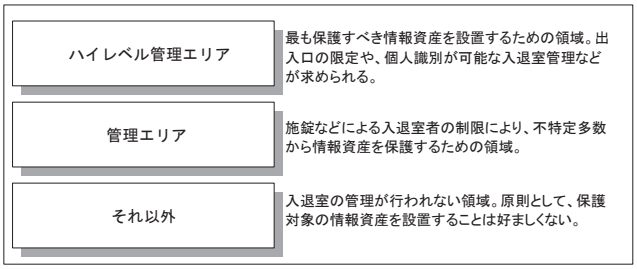

図5　入室管理エリアの明確化

4.1.2. 入退室管理

入退室管理とは、4.1.1項で定義した入室制限エリアへの入退室を行う際のルールを定義し、管理することを指す。

入退室管理は、まず管理責任者となる入退室管理者を、管理すべき入室制限エリアごとに定義する。入退室管理者は、対象の入室制限エリアへの入退室および入退出管理基準の維持管理についての責任を負い、定義した入退室管理手順に沿って、入退室希望者の承認／否認を行う。

入退室管理手順においては、入退室履歴の記録方法や、入室許可条件などを定義する。

(1)入室許可の付与

入室許可を与える際は、希望者が業務上の必要性が本当にあることを確認し、慎重に承認を行うべきである。入室許可を与えた者については、定期的に業務上の必要性を判断し、不必要な者が長期に渡って入室することがないよう棚卸を行うことも必要である。

また、入室許可の付与についてルール化する際には、ベンダのヘルプ要員の入室など臨時での入退室許可の付与についても定義する。臨時入退室も定常的な入退室許可同様、業務上の必要性をもとに入退室管理者による承認を運用する。

(2)入退室履歴の記録と検査

入室制限エリアへの入退室は、入室許可の付与だけではなく、入退室に関する履歴を記録し、定期的な検査を実施する。入退室履歴の記録では、入室者名・入室／退室日時・入室目的などを記録する。複数名での入室の際は、入室制限エリアのレベルに応じて代表入室者情報の記録、もしくは全入室者情報の記録を使い分け、必要以上に運用負荷をかけないことが望ましい。

入退室履歴の検査は、入室許可を与えられていない人間は入室できないため、不要と思われがちだが、許可された人間が不正な行為を行っていないことを監視する、もしくは行為そのものを抑止するため、定期的に入退室のログを検査し、不必要な入退室が繰り返されていないかなどを調査することが、物理アクセスセキュリティを確保するためには重要となってくる。

4.1.3. 可搬記憶媒体管理

可搬記憶媒体管理とは、磁気テープに保管されたバックアップ情報や、フロッピーディスク・CD-ROM・USBメモリなどに記録された情報資産を、セキュリティ脅威から保護するための管理プロセスである。以前より、磁気テープなどへの情報資産の記録は頻繁に行われているが、更に昨今ではUSBメモリなどの可搬容易な媒体へ情報資産を記録する機会が増えており、可搬記憶に対する管理はより重要な要素となってきている。

可搬記憶媒体は、同じ情報資産が記録されるコンピュータなどの筐体とは異なり、サイズが小さく、紛失・盗難の可能性が高い。そのため、持ち出し等を把握することが可能な施錠区域を保管場所として指定するとともに、保護の必要性や本数の定期的な棚卸、持ち運びの際の責任者承認および履歴の記録を行うことが重要な要素となってくる。

(1)保管場所の定義

4. 具体的なセキュリティ対策

ポリシー／ルールの中で定義されるべき、セキュリティ対策手段は、図４に示すとおり、大きく分けて６種類が存在する。本章では、そのセキュリティ対策について具体的に解説する。表１は、本章で述べるセキュリティ対策とそれを定めるべきセキュリティ基準文書の対応表である（なお、表中の管理文書は一般的な名称であり、実在するものとは限らない）。

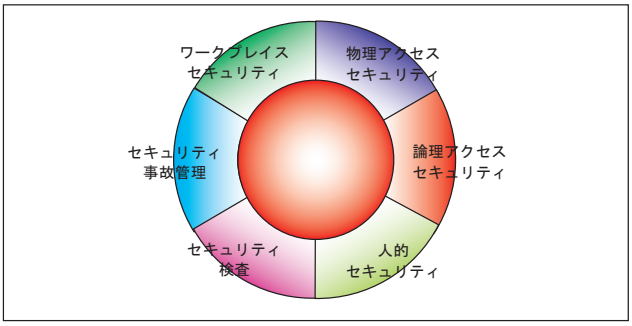

図４　セキュリティ対策

4.1. 物理アクセスセキュリティ

物理アクセスセキュリティとは、保護すべき情報資産を物理的に保護するためのセキュリティ対策である。「情報」という単語から、電子的な情報を想像しがちではあるが、情報資産には磁気テープなどに保管された情報も含まれる。電子データが保管されたコンピュータ、二次媒体および物

表１　セキュリティ対策と管理文書

セキュリティ対策	詳細対策		管理文書
物理アクセスセキュリティ	入室制限エリアの明確化	－	入退室管理基準書
	入退室管理	入室許可の付与	
		入退室履歴の記録と検査	
	可搬記憶媒体管理	保管場所の定義	可搬記憶媒体管理基準書
		管理方法	
		移送手順	
		定期的な棚卸	
論理アクセスセキュリティ	ユーザの識別と認証	ユーザIDの付与	ユーザID管理基準書
		ユーザIDの棚卸	
		パスワード管理	
	資源保護	情報資産の分類	
		アクセス件の付与	
		アクセス権の棚卸	
	システムセキュリティ	暗号化	情報システム運用管理基準書
		ウィルス対策	
		システム脆弱性対策	
		不正アクセス監視	
	ネットワーク管理	社内ネットワーク管理	ネットワーク管理基準書
		社外ネットワーク管理	
人的セキュリティ	教育	－	（セキュリティ基本方針で定義）
	罰則	－	（就業規則にて定義）
セキュリティ検査	ヘルスチェック	－	情報システム運用管理基準書
	ユーザID再検証	－	ユーザID管理基準書
	監査	－	（セキュリティ基本方針で定義）
セキュリティ事故管理	－	－	セキュリティ事故管理基準書
ワークプレイスセキュリティ	－	－	情報システム利用基準書

3.1. リスク分析

セキュリティポリシー／ルールを策定する場合、まずリスク分析を行う必要がある。リスク分析とは、保有する情報資産に発生しうるリスクを分析し、求められるセキュリティレベルを決定するものである。

セキュリティ対策は、企業に対して直接的な利益を生むことがなく、「負の資産」とも言われている。そのため、セキュリティレベルと必要なコストとのバランスが重要である。過剰なセキュリティ対策を施せば、企業財政を圧迫する要因になり、コストを下げるために十分なセキュリティ対策を施せなければ、セキュリティ脅威から十分に情報資産を保護することができなくなる。

3.1.1. 保護対象の明確化

リスク分析は、まず「保護対象の明確化」から行う。企業の保有する情報資産は、すべて保護すべきものであるとは限らないため、保護すべき資産を明確にしなければ、効果的なセキュリティ対策を実現することはできない。

「保護対象の明確化」は、企業が保持するすべての情報資産を洗い出し、漏洩や、サービス停止した場合に損失が発生する情報資産とは何があるのかを調査することで実施される。すなわち、「保護対象の明確化」とは保有する情報資産の棚卸を行うことから始まる。

3.1.2. 資産価値の算出

保護対象を明確にした後は、その情報資産がどの程度の資産価値を持っているかの算出を行う。資産価値は、その情報資産が漏洩や、サービス停止などのセキュリティ被害にあった場合に企業に与える損失と、セキュリティ脅威を受ける危険性の高さをもとに算出する。

保護対象として洗い出された情報資産は、保護すべきであることに違いはないが、すべてが同じ価値を持っているわけではない。例えば、保護すべき対象である個人情報においても、給与情報や身体情報のような情報資産と、E-Mailアドレスリストなどの情報資産とでは、漏洩した際の被害は大きく異なることは明確である。保護対象が持つ資産価値を明確に把握してこそ、効果的なセキュリティ対策を実現することができる。

に情報資産を区分することを推奨する。レベル分けすることにより、後に実施するセキュリティ対策をレベルごとに定義し、スムーズに対策を実施することが可能となる。

3.2. ポリシー／ルールの策定

リスク分析が完了したら、分析結果をもとに実施すべき対策を決定する。それがポリシー／ルールの策定である。

ポリシー／ルールは、図３に示すとおり、大きく分けて３種類のドキュメントにより管理される。

なお、ポリシー／ルールの策定後は、運用状況を踏まえた上で定期的に見直しを実施することが重要である。ポリシー／ルールの見直しは、年度ごとに実施することが望ましい。

(1) セキュリティ基本方針文書

セキュリティ対策を実施する上で大前提となる基本方針（ポリシー）である。この方針文書の中で、保護対象の定義や実施するセキュリティ対策のレベルを定義する。

(2) セキュリティ基準文書

セキュリティ方針で定義されたポリシーをもとに、より具体的な対策を定義し、管理するための文書（ルール）である。例えば、「ユーザID管理基準」や「入退室管理基準」などがそれにあたり、情報システムのパスワードルールや、管理領域への入退室方法など、すべての保護対象にとっての基準となるルールを定義する。

(3) 手順書

保護対象ごとに定義する最も詳細な文書であり、各種基準書をもとに具体的な運用／操作手順を定義するために作成される。例えば、「ユーザID管理基準」をもとにAシステムの「セキュリティ運用管理手順書」を作成し、その中でAシステムにおいて「ユーザID管理基準」を遵守するための各種設定方法や、具体的な運用管理方法を定義する。この手順書は、システム単位、環境単位で作成されるため、文書数としては非常に膨大な数となる。

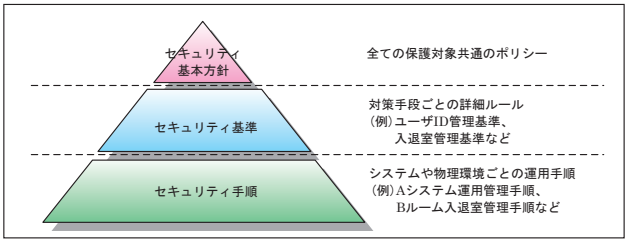

図３　ポリシー／ルールの種類

筆者は、コスト負荷の低減のため各種ツールによる運用の自動化を図ることで、ヘルスチェックやユーザID棚卸、セキュリティパッチの適用といった毎年定期的に発生する高負荷作業の効率化を実現した。これにより、コスト負荷が低減するとともに、精度向上にも寄与した。

7. おわりに

セキュリティ対策環境を実現するということは、前述のように、多くの時間とコストが必要となる他、セキュリティ対策を講じることで利便性が低下してしまう、導入効果が見えにくいなど、企業においては導入を敬遠してしまいがちになることが多い。また、5.3.節においても意識レベルの共通化が重要である旨は述べたが、いくら技術的に優れたセキュリティ対策を講じたとしても、セキュリティに対する意識が低ければ、企業にとってのセキュリティレベルは向上せず、企業におけるセキュリティレベルを向上させることは、決して容易なことではない。

しかし、情報化が進み、様々なセキュリティ脅威が発生している昨今においては、企業が保有する情報資産を保護するためにセキュリティ対策を講じることは必須となってきている。

企業としてセキュリティレベルを向上させ、最終的には利用者・管理者双方が、セキュリティを高めていくということを理解し、「意識せずとも高いセキュリティレベルを維持できる企業」となっていくことが、今後の情報化社会を生き抜いていくためには必要なことである。

参考文献

1) NPO法人 日本ネットワークセキュリティ協会（JNSA）. http://www.jnsa.org/
2) 独立行政法人 情報処理推進機構（IPA）. http://www.ipa.go.jp/
3) 財団法人 日本情報処理開発協会（JIPDEC） ISMS制度推進室. http://www.isms.jipdec.jp/
4) 財団法人 日本情報処理開発協会（JIPDEC） プライバシーマーク事務局. http://privacymark.jp/

＜問い合わせ先＞

NWS運用管理センター

運用管理チーム

Tel 03-3217-3908　鈴木 大介

E-mail: daisuke-suzuki@exa-corp.co.jp