# 企業のセキュリティポリシーの制定に関する考察

5W－4

雨宮　俊一　　西尾　秀一
株式会社　ＮＴＴデータ

## 1. はじめに

近年，ネットワーク機器等様々な製品のセキュリティ機能が強化されているにもかかわらず，プライバシー侵害や不正アクセス等のコンピュータ犯罪が後を絶たない．取引先とのネットワーク接続等，企業情報へアクセスできる範囲が拡大しているため，セキュリティ対策を施す個所が多様化，分散化し，セキュリティは複雑な問題となっている．そのような環境においては単にセキュリティ製品のインテグレーションだけではなく，その企業の体制，運用，教育等を含めた組織的かつ包括的なセキュリティへの取り組みが必要となる．

このような取り組みを示すものとして，セキュリティを重要な業務と位置付け，セキュリティの目標を定めそれに向かってどのような行動をとるべきかを明確に示したセキュリティポリシーが重要となっている．

本稿では，企業の情報資産，人，体制について包括的に定めたセキュリティポリシーのモデルを示し，そのようなセキュリティポリシー制定にあたって留意すべき事項や有効な運用方法を示す．また，その効果を把握するため，現在検討中であるセキュリティポリシー遵守状況管理システムの概要について紹介する．

## 2. セキュリティポリシーの内容

図１は，人が情報資産を利用して業務を遂行する過程において，セキュリティポリシーとして定めるべき項目を示したモデルである．

- 人に関する役割，責任に関する方針
- 情報資産に関する方針
- 情報資産の利用を支える各種セキュリティ技術の適用，運用管理等のプロセスに関する方針
- セキュリティポリシーの有効性を維持するために企業として取り組むべき事項に関する方針

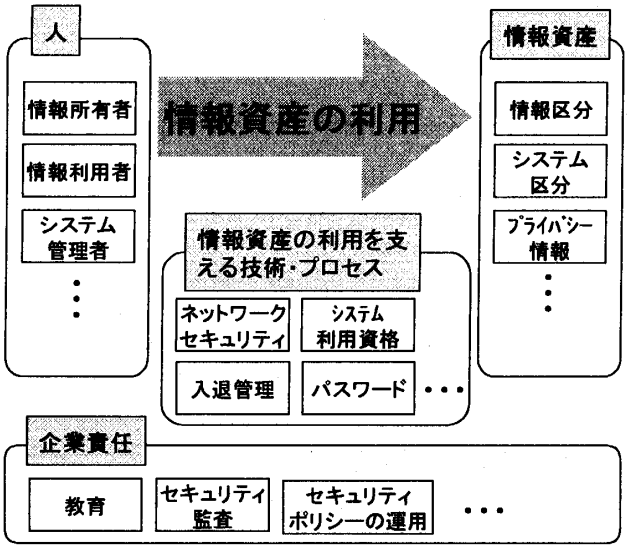


図１：セキュリティポリシーモデル

## 3. セキュリティポリシーの制定

本節では，図１に示したような幅広い項目について定めるセキュリティポリシーが企業に定着するために，制定にあたって留意すべき事項について述べる．

- セキュリティポリシーはあるべき姿
  セキュリティポリシーは，単に現状を記述するものでもないし実現不可能な願望を記述するものでもない．セキュリティに関する時間，コスト，技術，環境，法制度等の様々な制約を考慮し，企業においてあるべき姿や実現可能な目標を定める．
- 企業固有のセキュリティポリシー
  セキュリティポリシーを制定する上では，その企業の業務内容，経営方針，保護すべき情報資産，リスク，企業文化等の固有条件を考慮して従業員が受容可能なものを定める．
- 利便性とセキュリティ
  セキュリティを強化するあまり，情報資産の利便性，運用性が大幅に損なわれないように，バランスのとれたものを定める．
- 法制度等との適合性
  既存の法制度と矛盾しないようなものを定める．
- 経営者による積極的推進
  経営者の積極的な推進，指導のもと，システム部門

A Study on Establishing Practical Corporate-Level Security Policy
Shunichi AMEMIYA, Shuichi NISHIO
NTT DATA CORPORATION
1-21-2, Shinkawa Chuo-ku, Tokyo 104-0033, Japan
E-mail : {amemiya, nishio}@rd.nttdata.co.jp

だけが携わるのではなく様々な組織の有識者が検討に係わるような体制で定める．

## 4. セキュリティポリシーの運用サイクル

セキュリティポリシーを制定するだけではなく，制定後に適切に運用することが必要である．図2に示すような運用サイクルに基づいて継続的に運用することにより，実効的なものとなる．

① 制定プロジェクトの発足，ドラフトの起案
② 経営者の承認，制定
③ 施行によるセキュリティ対策の実践
④ すべての従業員に対する教育，啓発
⑤ 遵守状況の把握
プロジェクトやシステム毎の特殊事情等によりセキュリティポリシーを遵守できない場合，当該ケースを分析し，代替案，条件を明確にしてリスクを許容することが重要である．
⑥ 遵守状況や環境変化に応じた見直し

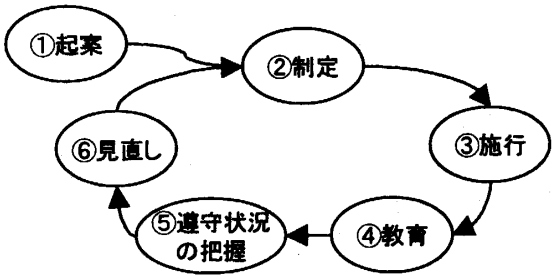


図2：セキュリティポリシーの運用サイクル

## 5. セキュリティポリシー制定，運用の効果

セキュリティポリシー制定，運用の効果を示す．

(1) 情報セキュリティについての判断基準の提供
- セキュリティに関する従業員の権限，責任，義務の明確化
- 保護すべき情報資産の明確化

(2) 従業員のセキュリティに関する意識，知識の向上
(3) セキュリティレベルの向上
(4) 適切なリスク管理の実現
- リスクの把握
- 対処すべきリスクのプライオリティ決定

(5) お客様に対する説明責任の確保

リスク管理における適切な意志決定，及び従業員に達成度を示し意欲を高めるため，以上の効果を可視化する必要がある．そこで我々はセキュリティレベルの測定や効率的なリスク管理を実現するしくみとしてセキュリティポリシー遵守状況管理システムを提案する．

## 6. セキュリティポリシー遵守状況管理システム

セキュリティポリシーを運用していく中で，プロジェクトのリソースの問題等により遵守できない場合が生じる．その際，経営者はリスクのプライオリティを明確にしてどのリスクに対して投資するのか，どのリスクについて許容可能とするのかという意志決定をしなければならない．このような意志決定に必要な情報を効率的かつリアルタイムに提供するしくみとしてセキュリティポリシーの遵守状況管理システムについて検討している．

遵守状況管理システムは以下に示す項目を達成することを目的とする．

- セキュリティポリシー遵守状況の把握，リスクの所在の把握
- セキュリティレベルの測定
- 対処すべきリスクのプライオリティ決定の支援

表1：遵守状況管理システムの主要な機能

| | 機能名 | 概要 |
|---|---|---|
| 1 | プロジェクト把握機能 | プロジェクトの重要性を判定する． |
| 2 | セキュリティレベル表示機能 | プロジェクトの現在のセキュリティレベルを，過去の実績，他のプロジェクト等と比較可能なように表示する． |
| 3 | リスクのプライオリティ判定機能 | 各プロジェクトが抱えるリスクのうちから，事業内容，規模等，リスクの影響度を考慮してプライオリティを判定する． |
| 4 | レポート作成機能 | リスクに応じた代替案や推奨事項等をレポートする． |
| 5 | セキュリティ機能 | ユーザ認証，暗号化等． |

## 7. おわりに

本稿では，効果的なセキュリティポリシーのモデルを示しその制定,運用の意味及び効果について考察した．また，検討中であるセキュリティポリシーの遵守状況を把握するシステムの概要について報告した．

今後は，リスクのプライオリティ判定方法やセキュリティレベル測定方法について検討し，遵守状況管理システムを構築する．

## 参考文献

[1] ISO/IEC TR 13335-3 Guidelines for the management of IT Security, 1998
[2] 財団法人金融情報システムセンター，「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」，1999
[3] グレン・ブルース他，「分散コンピューティングセキュリティ」，プレンティスホール，1998