情報セキュリティポリシー運用における課題と対策

Problem and Measures of Information Security Policy Operation

鈴 木 武 俊，真 田 大 志

要　約　企業の情報セキュリティ対策を継続的に推進していくために，多くの企業が情報セキュリティポリシーを策定し運用しているが，情報セキュリティ事件・事故は増加傾向である．昨今のセキュリティ事件・事故を分析した結果，情報セキュリティ事件・事故を発生させる要因の多くは，内部の人員によるミスや認識不足が原因であることが確認された．

つまり，策定した情報セキュリティポリシーの周知徹底と適切な運用がなされていないと考えられる．その理由には，情報セキュリティ組織・体制に関する曖昧な責任・権限の設定や情報資産の杜撰な管理，抽象的で分かりにくい情報セキュリティポリシー等が挙げられる．情報セキュリティ事件・事故を減らすためには，情報セキュリティポリシーを適切に運用しなければならない．それには，情報セキュリティに関する責任・権限の明確化と現場に負荷の掛からない資産管理，整合の取れた文書作成，必要性を理解させる研修等，常に情報セキュリティ意識を向上させる工夫を継続的に行うことが重要である．

Abstract　Although many companies have developed and applied the information security policy in order to promote continuously their own information security measures, information security-relevant accidents and incidents are increasing yearly. The result of analyzing recent security-relevant accidents and incidents shows that these accident and incidents are caused by human mistakes of company employees and a lack of their understanding of the information security.

This means that it is insufficient to keep all personnel within a company informed about developed information security policy and to make its adequate application. The reasons include the ambiguous definition of responsibility and authority for the information security organization, careless management of information assets, and abstract and unclear information security policy, and etc. The adequate application of information security policy is of utmost importance in reducing information security-relevant accidents and incidents. This will require constant performance of devising the increased awareness about the information security, including clarification of responsibility and authority for the information security, the asset management that does not require the workload of people on the line, the coherent document creation, training which leads employees to understand the necessity of the information security.

1. は じ め に

グローバル化や新規事業の開発，M&A による組織の拡大等企業の成長に伴い，情報資産を取り巻く環境は日々変化している．また，情報システムや情報通信・その他の媒体の技術革新により情報資産の取り扱いも常に変化している．その変化によって情報資産に影響を及ぼす新たな脅威や脆弱性が発見されており，情報セキュリティに関するリスクが増大している．そのため，情報セキュリティ事件・事故は，毎年増加傾向にあり，社会的な問題に発展してきている．

この情報セキュリティ事故を防止するため，各企業は情報セキュリティ対策の仕組みである情報セキュリティポリシーを策定し対策を実施しているが，刻々と変化する環境に対応できていないのが実情である．

本稿では，多くの企業が情報セキュリティポリシーを構築し，運用しているにもかかわらず，なぜセキュリティ事件・事故が減らないのか，著者のセキュリティコンサルティングサービス実施の経験や調査結果を基に情報セキュリティポリシーの動向と課題，その課題に対する解決策を考察する．

2. 情報セキュリティポリシーの動向

2.1 情報セキュリティポリシーの策定状況

情報セキュリティポリシーの歴史を振り返る．

2000 年から 2001 年にかけて，官公庁に対するホームページの書き換えや，猛威を振るったコンピュータウイルス「NIMDA」等の情報セキュリティ事件・事故が発生し，社会全体が情報セキュリティ対策の必要性を感じ始めた．

その後，2002 年の地方公共団体における「住民基本台帳ネットワークシステム」の開始に伴い，総務省が「地方公共団体における情報セキュリティポリシー策定に関するガイドライン」を策定し配布したことにより，地方公共団体を中心として情報セキュリティポリシー策定の気運が広まっていった．

一方，民間企業は，頻発する情報セキュリティ事件・事故の影響と，官公庁との取引条件に情報セキュリティポリシーの策定が推奨されたことなどから，情報セキュリティポリシーを策定する企業が増加した（図 1）．また，経済産業省が主導で行っている ISMS 認証制度（現：JISQ27001）による認証を取得する企業が増加したことも情報セキュリティポリシーの普及に拍車をかけた（図 2）．

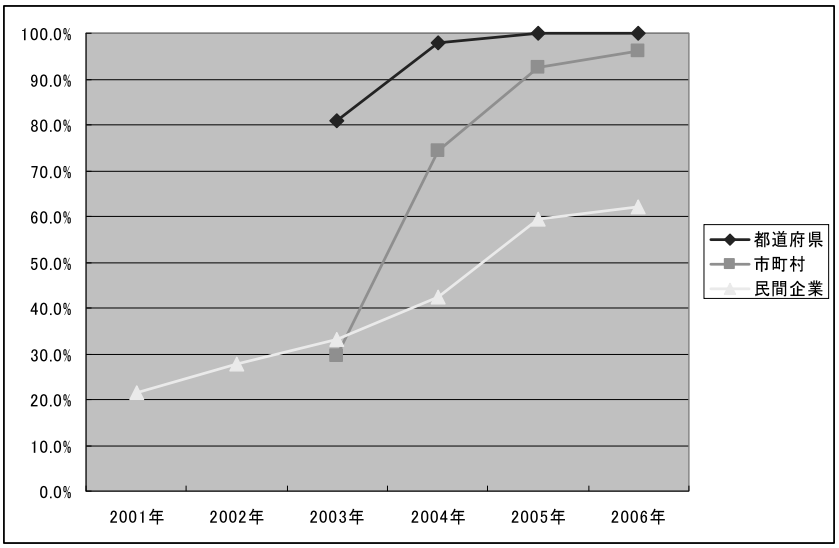

図 1　情報セキュリティポリシー策定状況の推移[1][2]

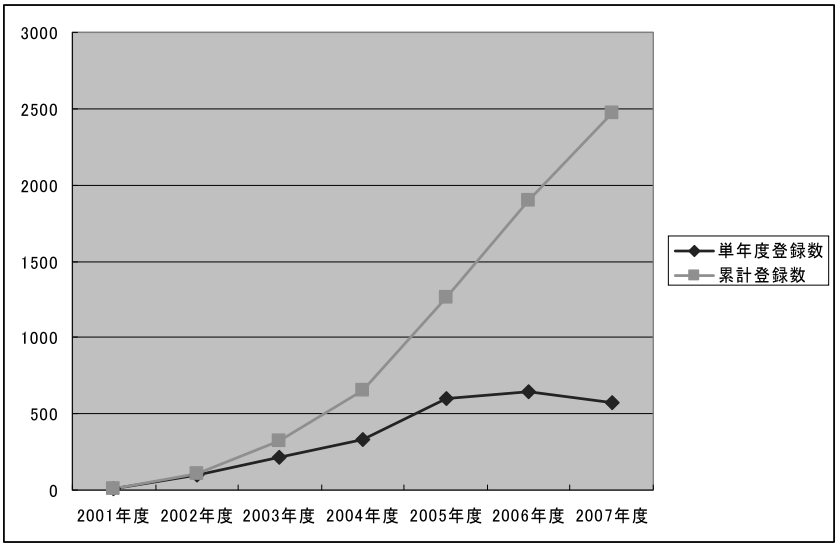

図 2　ISMS 認証取得事業者数の推移[3]

2. 2　日本版 SOX 法（金融商品取引法）の施行

2007 年 9 月に日本版 SOX 法（金融商品取引法）が施行され，株式上場企業は内部統制の仕組みを構築しなければならなくなった．この内部統制の目的とは，「業務の有効性と効率性の構築」「財務報告の信頼性」「法令等の遵守」「資産の保全」であり，言い換えると企業に違法行為やエラー等が発生しないように手続きを定め，それに基づいて監視を行い，記録を取得し，管理を行うことである．

最近の企業は情報システムへの依存度が非常に高いため，この仕組みを構築する上でキーポイントとなるのが IT を活用した統制（IT 統制）である．この IT 統制の対象は，財務報告の基データの作成や更新に関係する業務プロセスやアプリケーションと，それらが動作する IT インフラである．

情報セキュリティポリシー運用に関する活動と内部統制における IT 統制の取り組みは，重なる部分が多い．IT 統制の取り組み手順は，「現状認識⇒整備状況の確認⇒リスクの洗い出しと評価⇒運用とモニタリング⇒評価・改善」であるが，そのほとんどが情報セキュリティポリシー運用に関する活動によって対応可能である．また，情報セキュリティポリシーによって整備された規程関連も，一部見直しは必要であるが，利用できる部分は多い．このように，日本版 SOX 法の対応にも流用できることから，いま多くの企業では情報セキュリティポリシーが見直されている．

3.　セキュリティ事故発生要因の分析

前述のとおり，6，7 年前と現在では比べるまでもなく，現在の方が多くの企業で情報セキュリティポリシーの策定やセキュリティ対策を実施しているにも関わらず，情報セキュリティ事件・事故の発生件数は高い水準を維持している（図 3）．

なぜ情報セキュリティ事件・事故が発生してしまうのか．2008 年 4 月 1 日から 8 月 22 日までに発生した情報セキュリティ事件・事故 427 件[*1] の内容を調査し，要因の分析を行った．

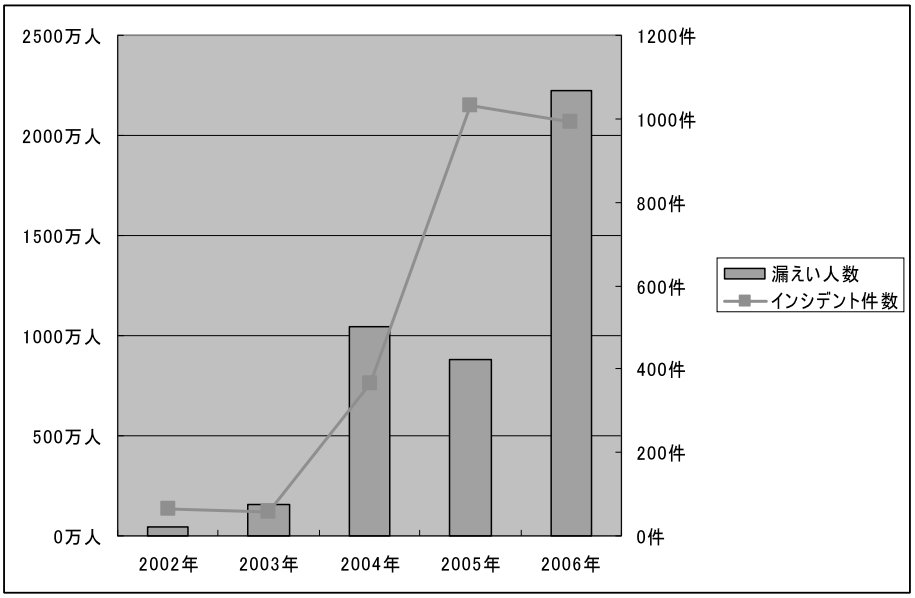

図 3　情報漏洩インシデント件数の推移[4]

3. 1　技術的要因，人為的要因，環境的要因

第一の観点として，何が原因で情報セキュリティ事件・事故が発生したかを分析する．要素としては，IT セキュリティと呼ばれる技術的な要因，人の意識の問題や管理上の不備等である人為的な要因，地震や火災等の環境的な要因である．この分析によって，情報セキュリティ対策とはどのような対策を中心に考え，経営資源を投入すべきかを判断できる．図 4 に示す分析結果から，技術的・環境的な要因は合計しても 2 割強程度であり，ほとんどのセキュリティ事故は人為的な要因により発生していることが分かる．

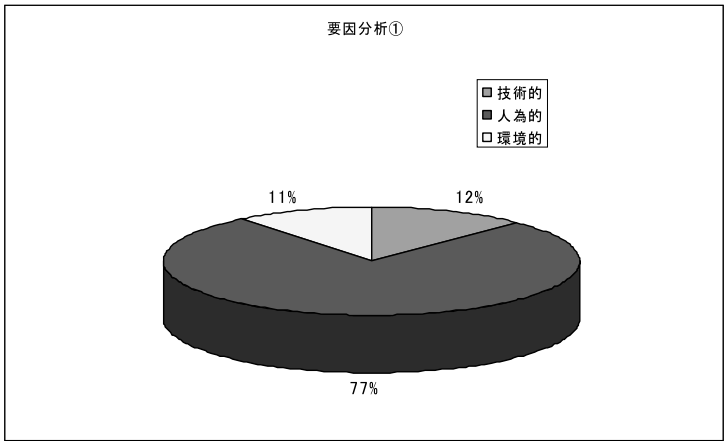

図 4　技術的要因，人為的要因，環境的要因

3. 2　外部要因，内部要因

人為的要因のうち，誰が情報セキュリティ事件・事故を引き起しているのかを調査した．情

報資産を取り扱うことができる対象は，

- 第一者（当該企業の社員）
- 第二者（外部委託先等の利害関係者）
- 第三者（ビジネス上の利害関係のない外部の者）

が考えられる．この分析によって一番の原因となるものがコントロール可能な内部の問題なのか，そうではない外部の問題なのかを判断できる．図5に示す分析結果によると，内部の要因（主に当該企業の社員）がセキュリティ事故を多く引き起しいることがわかる．

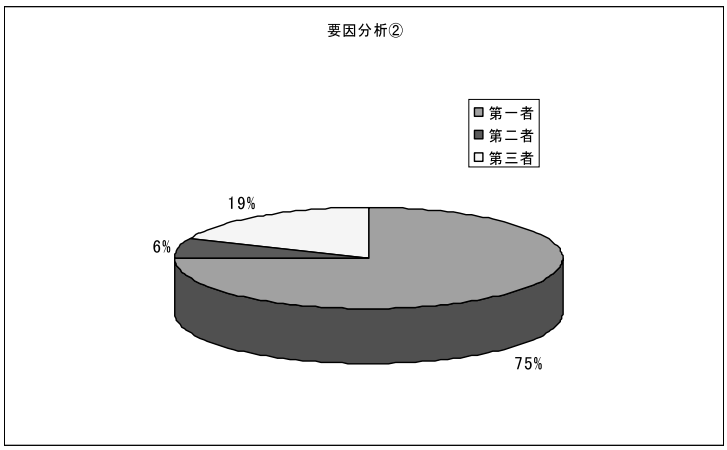

図5　外部要因・内部要因

3.3　故意的な要因，意図しない要因

内部要因（当該企業の社員）がなぜ情報セキュリティ事件・事故を起こしたのか，事故の発生が意図的なものであったかどうかを分析する．要素は，故意的な事故であったか，意図しない要因で事故（ヒューマンエラー）となってしまったのかの二つである．図6の分析結果から，セキュリティ事故を発生させた社員は，意図しないで事故を起こしてしまっていることが分かる．

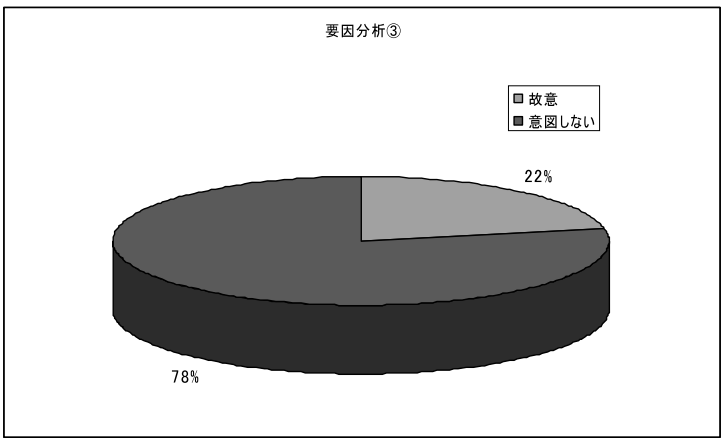

図6　故意的な要因，意図しない要因

3.4　分析結果のまとめ

3.1節から3.3節までの異なる側面から情報セキュリティ事件・事故を分析した結果，事故の発生する要因として最も多いものは「第一者（自社の社員）による人為的な意図しない」ものであることがわかる（図7）．つまり，「自社の社員が，自分が何をしなければならないかを知らないために，ついうっかり事故を起こしてしまった」ということである．

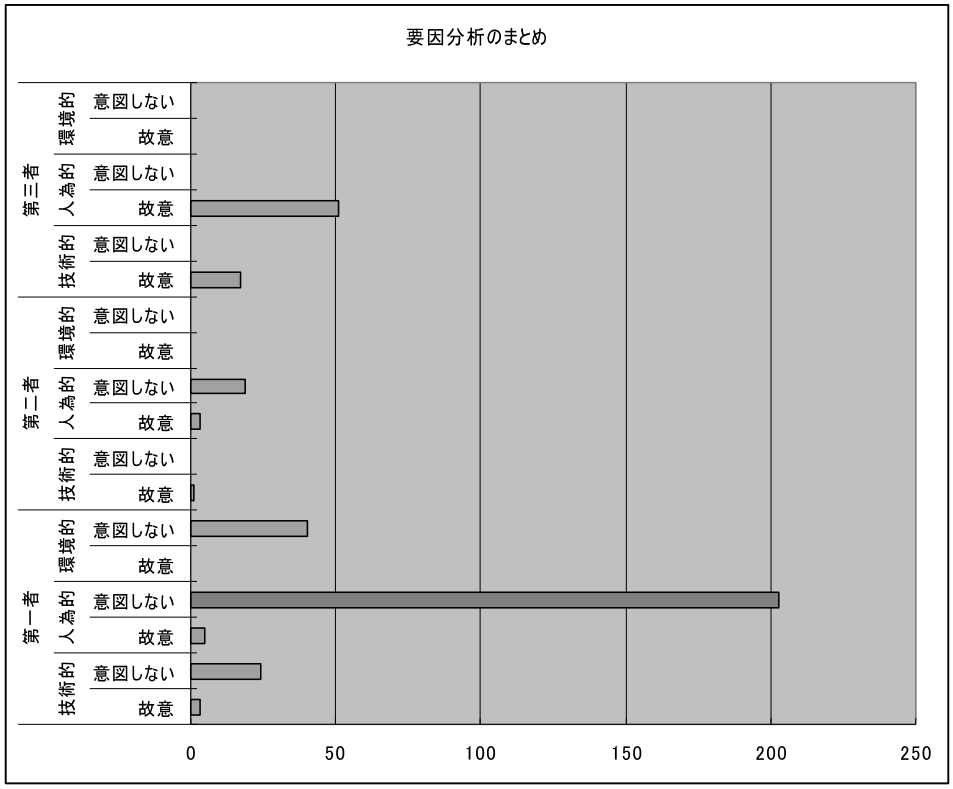

図7　要因分析のまとめ

このような要因が最も多いという分析結果から，意図的に攻撃する外部要因に対する技術的セキュリティ対策や物理的セキュリティ対策については，比較的実施されているが，内部社員の情報セキュリティに関する啓発等が不十分であり，各個人の情報セキュリティ意識も低い状態であるといえる．したがって，このような状態では，各個人が実施しなければならないルールが遵守されないため，情報セキュリティポリシーが適切に運用されていない可能性が高いと推測される．

4.　情報セキュリティポリシーが適切に運用されていない理由

前章で，情報セキュリティ事件・事故の起こる要因から，情報セキュリティポリシーが適切に運用されていない可能性が高いことが推測されたが，その具体的な事象はどのようなものであろうか．著者の情報セキュリティポリシーの策定やISO/IEC27001認証取得の支援を実施した経験から，課題を抱えている企業には多くの共通点があることが分かった．その共通点のうち最も多い5点に関して考察を行う．

4.1　情報セキュリティ組織・体制における課題

情報セキュリティ組織・体制とは，一般的に情報セキュリティにおける最高責任者である「CISO（Chief Information Security Officer)」，決議機関である「情報セキュリティ委員会」とその構成員である「情報セキュリティ委員」「情報セキュリティ担当者」，情報セキュリティ委員会の運営・その他手続きを行う「情報セキュリティ委員会事務局」等から構成される．通常，企業の情報セキュリティに関する活動は，全てこの組織で管理・運用される．情報セキュリティポリシーが適切に運用されていない企業は，情報セキュリティ組織が機能していないことが多い．その原因として，以下の項目が考えられる．

4.1.1　経営陣の情報セキュリティに対する消極的な姿勢

情報セキュリティ組織の体制上，「CISO」として経営陣が参画しているが，名前だけが記されているだけで，内容に関してはあまり係っていないことが多い．

4.1.2　特定部門のみによる情報セキュリティ組織の構成

情報セキュリティの特性上，情報システムに関するリスクや対策が多く発生する．そのため，情報セキュリティに関しては，情報システム部門に全て任せてしまい，情報システム部門だけで情報セキュリティ組織を構成している企業も多い．

4.1.3　形骸化する情報セキュリティ委員会

情報セキュリティ組織を策定し，セキュリティ委員会も定期的に開催する旨を情報セキュリティポリシーに記載されているにも拘わらず，策定時に一度だけ開催し，その後開催していない企業が多い．その原因として，情報セキュリティ委員会に関する事務局機能がないことがあげられる．また，事務局としての機能はあるが，なにをすればよいか分からないというケースもある．

4.1.4　担当者による情報セキュリティ委員会の構成

情報セキュリティ委員会を構成する要員が，IT 技術や知識に長けているという要件のみに傾注しすぎて，責任権限を考慮せずに現場の担当者レベルで構成されていることがある．このような構成によって，情報セキュリティ委員会で決定された事項にまったく強制力がないという状況が発生している．

4.1.5　情報セキュリティ専門人材の不足

情報セキュリティに関しては，IT に関する知識やセキュリティに関する知識等広範な知識が要求される．また，日々新たな脅威や脆弱性が発見されるため，常に情報収集していなければ，自社がいつ被害に遭うか分からない状況である．よって，少人数でも情報セキュリティに関しての知識を持つ専門家を育成することが望ましいが，ほとんどできていないのが実情である．また，情報セキュリティ組織を策定し，各部門に情報セキュリティ担当者を設置しても，知識レベルにバラツキがあり，適切な統制が取れていない場合が多い．

4.2　情報資産の管理における課題

情報資産の管理とは，企業で保有している重要な情報資産を明確にして重要度を分類し，重要度に応じた取り扱いのルールを定め，それに基づき情報資産を取り扱うことである．情報資産の管理は情報セキュリティにおけるキーポイントであり，適切に行われなければ，直接，情報漏洩等の事故につながる可能性が高い．しかし，日々増減する情報資産の管理ができていない企業が多い．その原因として，以下の項目が考えられる．

4.2.1　情報資産の分類およびラベル付けにおける課題

企業が情報セキュリティポリシーを策定する際，重要なポイントになるのが情報資産の分類である．一般的な手順としては，先ず全ての情報を洗い出し，その後情報の種別や業務内容等によってグループ化を行い，その後重要度の分類を行う．重要度の分類は，「最重要情報」「重要情報」「社外秘情報」「一般情報」の４段階や「最重要情報」を除いた３段階に分類するようなルールを策定している企業が多い．４段階に分類する場合の基準例としては，

・最重要情報：企業の保有する情報資産のうち，漏洩又は毀損・滅失が発生した場合，極めて重大な影響を及ぼす情報.
・重要情報　：企業の保有する情報資産のうち，漏洩又は毀損・滅失が発生した場合，重大な影響を及ぼす情報.
・社外秘情報：企業の保有する情報資産のうち，漏洩又は毀損・滅失が発生した場合，軽微な影響を及ぼす情報
・一般情報　：企業の保有する情報資産のうち，社外に公開可能な情報.

のような定義づけが一般的であるが，このような分類基準は情報資産が与える影響を指標としており，経営層の視点から見ると理解しやすいかもしれないが，実際に情報を取り扱う従業員には，不明確で理解しにくく，人によって判断の基準がぶれてしまうケースが多い．

また，多くの企業が，この分類基準に応じて「ラベルづけ」を行うことをルール化している．具体的には，文書に「社外秘」と記載したり，ファイル名の先頭に「【重要情報】」と付加する等である．しかし，手間が増えることや分類基準を迷ってしまうことから，適切にラベルが付加されずに社外秘の情報を公開してしまったり，提携先へ公開すべき情報が提供されずに情報が有効に活用できていない場合が多い．

4.2.2　情報資産のライフサイクルに応じた対策の欠如

情報資産のライフサイクルとは，情報の「作成」「入手」から始まり，その後「利用」「保管」され「廃棄」される一連の流れである．このライフサイクルに応じたセキュリティ対策をルール化し，適用するのが一般的な手順であるが，「入手」「利用」「廃棄」という用語の定義が理解しにくく，現場ではこれらを組み合わせた様々なケースが発生しているため，現場の担当者が実際の状況にあてはめられない場合が多い．

4.2.3　情報資産の重要度とリスクに応じた対策の欠如

情報資産は，時間と処理のプロセスに応じて変化するものである．時間に関する変化については，ある期間まで機密度が高く，その日を過ぎると公開情報になるような情報に対して，公開情報になっても厳格管理をしていることがあり，管理負荷になることがある．処理のプロセ

スおける変化については，紙の情報が情報システムに入力されて利用され，バックアップテープに保管される等，処理のプロセスに応じて媒体が変化する．その変化に応じてリスクの度合いも変化する．そのリスクに応じた対策が実施されていない場合が多い．

4.3　情報セキュリティ関連文書における課題

情報セキュリティ関連文書とは，情報セキュリティポリシーとそれに関連する規程（文書管理規程，個人情報保護規定等）である．情報セキュリティポリシーは，一般的に経営者による情報セキュリティに対する考え方を示す「情報セキュリティ基本方針」，全ての組織において実施する情報セキュリティ対策の基準を網羅的に記載した「情報セキュリティ対策基準」，情報セキュリティ対策基準を実現するための具体的な手続き・手順が記載された「情報セキュリティ実施手順」から構成される．情報セキュリティポリシーが策定され始めたのは 2002 年頃からであり，元来存在していた企業の内部規程類に溶け込めていないケースが多い．その原因として，以下の項目が考えられる．

4.3.1　不明確な役割，責任・権限

情報セキュリティポリシーの文書において，情報セキュリティ組織の役割，責任・権限，特に情報セキュリティに関するイベント（リスク評価・点検・監査等）を実施する際の起点となる組織と主体となる組織が明確になっていないと，情報セキュリティポリシーが形骸化してしまう場合が多い．

4.3.2　情報セキュリティポリシー関連文書との不整合

実態に合わない情報セキュリティ対策基準を策定すると，下位文書である情報セキュリティ実施手順及びその他の規程との整合がとれない場合が多い．上位文書と下位文書が整合されていないため，技術的文書に特化する等網羅性に欠け，形骸化する場合が多い．

4.4　情報セキュリティマネジメントシステムの運用における課題

情報セキュリティマネジメントシステムの運用とは，Plan（計画），Do（実行），Check（チェック），Act（見直し）を行い，継続的に運用することである．具体的には，Plan フェーズで計画を策定し，Do フェーズで計画に基づいて情報セキュリティ対策を実行する．Check フェーズでは，情報セキュリティ対策の実行状況を点検・監査という形で確認を行い，Act フェーズで，ルールや対策・運用方法を見直していく．情報セキュリティポリシーを運用するためには，この仕組みを適切に運用することが重要であるが，各フェーズにおいて以下の課題が散見される．

1)　Plan フェーズ

- 情報セキュリティにおける年間計画を策定していない．
- 情報セキュリティにおける年間計画を経営者が承認していない．
- リスクアセスメントを実施していないため，実態との乖離があるルールが策定されている．

2） Do フェーズ
・リスク管理ができていないため，発見されたリスクをそのままの状態にしている．
・情報セキュリティポリシーに関する教育が実施されていない（4. 5 節にて後述）．
3） Check フェーズ
・内部監査員を内部監査部門の要員のみで構成してしまっているため，一般部門の参加意識が低い．
・海外拠点等の監査ができていない．
・情報システムの脆弱性検査を実施していない．
4） Act フェーズ
・リスクアセスメントの結果や内部監査の結果，事件・事故の結果等を経営者へ報告するマネジメントレビューを実施していないため，正しく経営資源の配分がされない．
・情報セキュリティポリシーの見直しを実施していない．

4. 5 情報セキュリティ教育・研修における課題

情報セキュリティ教育・研修とは，情報セキュリティポリシーを周知させるための教育と情報セキュリティに関する基本的な知識・一般動向を周知させる研修，また，情報セキュリティ担当者を育成するための研修や管理者，経営層向けの研修等役割に応じて様々である．この情報セキュリティ研修に関しては，以下の課題がある．

4. 5. 1 不十分な情報セキュリティポリシー研修

情報セキュリティポリシー策定後，グループウエア上に文書を添付し，アナウンスを行うだけで，特に研修（集合研修や管理者による研修等）という形式では実施されていない場合や，情報セキュリティポリシー策定後一度研修を実施しただけで，その後実施されていない場合も多い．

4. 5. 2 情報セキュリティ上の役割を考慮していない研修

情報セキュリティの組織や役割についてそれぞれが意識する必要がある．CISO には，組織全般の方針に関する事項や事業継続に関わる事項についての教育が必要であり，情報セキュリティ委員会及び情報セキュリティ委員会事務局には，情報セキュリティに関する一般情報や他社の事故情報，法令等に関する教育も必要である．情報セキュリティ管理者や担当者は，一般的な情報セキュリティに関する知識と情報セキュリティポリシーの内容，申請手順等を確実に理解する必要がある．

4. 5. 3 情報セキュリティの必要性を認識させられない研修内容

情報セキュリティ研修に関しては，実施方法というより内容に課題があることが多い．特に一般部門員が興味を示す内容の研修を行うには，必要性を理解してもらえるよう工夫をしなければ難しい．一般的な内容の集合研修や e- ラーニング等のコンテンツは様々あるが，実施しても期待する効果は得られない場合が多い．

5. 継続的かつ効果的に情報セキュリティポリシーを運用するポイント

前章にて挙げた要因は，全ての企業において同様な状況となる可能性を秘めている．情報セキュリティポリシーを適切に運用するにあたって，どのような観点に主眼を置けばよいのであろうか．

5.1 情報セキュリティ組織・体制を機能させるポイント

情報セキュリティポリシーを適切に運用することは，企業における情報セキュリティリスクの予防・検知に絶大な効果を発揮する．それには，経営陣が積極的に参画し，情報セキュリティ組織を牽引することが効果的である．定期的に実施される点検や監査，情報セキュリティ事件・事故の報告等により収集されたリスクを経営陣がきちんと見極め，是正・予防することにより，大きな事件・事故を防ぐことが可能になる．情報セキュリティ組織・体制を効果的に機能させるポイントは以下のとおりである．

- 経営陣が積極的に参画し，情報セキュリティに会社として取り組む姿勢を社員へ提示する．
- 情報セキュリティ委員会を定期的に開催し，報告は経営層に対して行う．
- 情報セキュリティに関するイベント（リスク分析，内部監査等）の管理や部門間における連絡・連携の補助等を行う情報セキュリティ委員会事務局を設置する．
- 情報セキュリティに関する分野は幅広く，習得しなければならない知識も多いため，学習期間が必要なことから，情報セキュリティに関する活動が軌道に乗るまで，コアメンバは固定する．
- 情報セキュリティに関する活動には全社横断的な参画を求める．情報システム部門等の特定の部門による技術的な情報セキュリティ対策に傾注しすぎずに，総務・人事部門による外部委託管理や入退室管理等の対策も考慮し活動することが望ましい．
- 情報セキュリティ委員会を構成するメンバは各部門をまとめセキュリティ対策を実行させる責任がある．したがって，ある程度の権限をもち，自部門の要員に対して行動を強制できる役職（役員・部長等）が望ましい．

5.2 情報資産の取り扱いにおけるポイント

情報資産の取り扱いは，情報セキュリティポリシーの適用範囲における全ての要員が毎日必ず行わなければならない基本的な事項である．したがって，情報の分類，ラベル付けの方法，取り扱いルールは，わかりやすく実行しやすいものでなければならない．

まず，情報の分類については，分類基準を詳細に詰めてみても，定義としては正しいが実際には分類できない基準ができあがってしまう．分類基準の定義を現場へ説明しても「では，具体的にこの文書は何に分類するのか」と困惑されることが多い．したがって，定義を厳密に策定するよりも具体例を提示し，その判例に従ってもらう方法が有効である．

ラベル付けについては，単純にファイル名の先頭に分類名を表示したり，紙面の右上に分類名を記入するというルールのみの対策ではなく，書類の雛形を作成し，ファイルの背景色やフッターの表示によって分類名の表示を行う等，運用で補助する方法や，分類名を明記する文書管理システムを導入する方法が効果的である．

取り扱いルールについては，情報を入手・作成した場合の取り扱いフローを作成することが

重要である．これによって，現場での具体的な情報の取り扱いとルールを照らし合わせ，現実味をもって現場へ周知することができる．ただし，全ての業務について取り扱いフローを作成する作業は非常に負荷がかかるため，重要な情報を取り扱う業務や取り扱いが複雑な業務のみを対象として実施することが有効である．その他の業務については基本的な取り扱いルールを遵守することでセキュリティレベルは維持できると考える．

情報資産の取り扱いにおけるポイントは以下のとおりである．

・各部門が保有しているファイルや文書を閲覧させてもらい，主なファイル名・文書名を選出し，例を示す．

例）情報システム部門の最重要情報は，システム仕様書，ソースコード，設定情報等
人事部門の最重要情報は，履歴書，社員個人情報等
総務部門の最重要情報は，個人株主情報，入退出管理システムの指紋情報等

・選出する主なファイル・文書は，部門内の誰もが知っており，イメージしやすいものにする．

・背景色等によって分類を詳細に判別できる様式（赤：極秘，青：社外秘，黄：NDA 締結先のみ公開，緑：顧客のみ公開等）を用意して積極的に公開し，情報の利活用を促進する．

・重要な情報を洗い出した後に，その重要な情報が関連する業務を選定して取り扱いフローを作成する．取り扱いフローはルールとの不整合がないかを検証した後に現場へ周知する．

5. 3　効果的な情報セキュリティ関連文書策定のポイント

情報セキュリティポリシーを適切に運用するためには，情報セキュリティポリシー関連文書に各者の役割分担・責任権限を明確にすることが必要である．また，他の規程と整合を取る場合には，その規程を所管している部門の担当者を策定及び見直しのメンバに含めるとよい．規程を策定して運用していくと，当初想定していなかったことが発生し，ルールやプロセスを改訂したり，効率化を図るためにプロセスを省略したということが頻繁に出てくる．他の規程の背景を知る担当者に，策定の初期段階から内容を確認してもらうことにより，不整合や重複による余計な手間を防ぐことが可能になる．

各業界で発行されている情報セキュリティ対策ガイドラインと自社の情報セキュリティポリシーを対比し，自社の情報セキュリティポリシーがガイドラインに準拠しているか，文書の整合表を作成し確認すれば，より確実性を増す．

5. 4　有効な情報セキュリティ対策実施のポイント

情報セキュリティ対策は，何処までやってもきりがないとよく言われるが，守るべき情報資産を明確にし，リスク評価を行うことにより，企業として何処まで対策を行えばよいかの判断は可能と考える．

5. 4. 1　定期的なリスク評価の実施

情報資産に対するリスクは，社会情勢や情報セキュリティ技術の流行等によって変化するため，定期的に見直しを実施する必要がある．また，組織改編による業務内容の変更や他社との

業務提携等が実施された場合には，情報資産の公開する範囲が変更されるため，リスクが大きく変動する可能性がある．したがって，リスク評価は定期的な見直しだけではなく，企業活動に大きな変化がある場合にも実施する必要がある．具体的なケースは以下のとおりである．

・組織改変により，情報資産の所在が不明確になったり，引継ぎされていない媒体が放置される場合
・M&A，業務提携等により会社間でのセキュリティレベルの不整合が発生する場合
・グローバル展開により，多国間で情報の受渡しが発生する場合，等

また，このリスク評価によって，企業の情報セキュリティ対策状況が把握できると共に，どこまで対策するべきかの経営判断が可能となり，過度なセキュリティ対策の抑制にもなる．

5. 4. 2　必要性を理解させる教育の実施

情報セキュリティ教育は，その役割によって遵守しなければならないルールや知識が異なるため，個別の教育を行う必要がある．また，情報セキュリティ教育の一番の目的は情報セキュリティの必要性を認識する意識向上であるため，情報セキュリティ知識の習得に傾注した内容とならないように注意する必要がある．具体的には，「なぜ情報セキュリティ対策をしなければならないか」「自社においてどんなリスクがあるのか」「なぜそのルールを策定したか」を，社員全員に理解させるような教育を行うことである．教育を行う上での具体的なポイントは以下のとおりである．

・情報セキュリティ上の役割に応じた教育を定期的に行う．
　1）情報セキュリティ管理者や役員
　2）情報セキュリティ専門家
　3）一般社員，派遣社員
・アンケートとテストを行い，基準点以下の場合は再試験を受けさせる．
・重点的な情報セキュリティ対策をポスターに掲示し，自覚を高める．
・部門長の評価に，要員の教育の実施状況や点数を連動させ，教育に関する部門長の責任を明確にする．
・他の教育（個人情報に関する教育や環境に関する教育等）との調整を行い，連続して教育が行われたり，繁忙期に研修が行われないようにする．
・集合研修や e- ラーニング等の机上研修だけではなく，擬似ウイルスメールを送信し正しい対応が実施できるかの抜き打ち検査を実施する[*2]．

6. お　わ　り　に

十数年前までは，多くの企業において，IT 技術の導入等による情報の利活用のみが促進されてきた．しかし，個人情報漏洩事故の被害拡大から，企業は情報セキュリティ対策を適切に行い，情報セキュリティ事件・事故を未然に防ぐ必要がでてきた．これは，企業の社会的責任であり，企業が成長するにつれて，その責任は重大になってきている．

企業が総合的な情報セキュリティ対策のルールである情報セキュリティポリシーの構築を考えた場合，現在では，各種発行されている具体的なガイドラインを単に適用するだけで，容易に目的を果たすことはできる．ただし，利便性の向上を優先し利活用してきたところへ，型どおりの情報セキュリティに関するルールが適用されると，現場にとっては面倒な手順ばかりが

増えるだけになる．情報セキュリティ事件・事故の分析結果からもわかるとおり，情報を取り扱う要員のセキュリティ意識が低いままルールを適用しても，形骸化することは必然であると考える．したがって，情報セキュリティポリシーを形骸化させずに効果的かつ継続的に運用するためには，現場の負荷を取り除き，意識を向上させる工夫が必要不可欠である．

本稿では，筆者が情報セキュリティポリシーの構築支援等の現場で得た，有効と考える工夫のポイントを述べてきた．これらの内容が，同様の課題を持つ企業の役に立てば幸いである．

＊1　情報セキュリティ事件・事故のデータは，ニュースガイア株式会社が提供するセキュリティニュースサイト SecurityNEXT（http://www.security-next.com）のデータベースによる．

＊2　擬似ウイルスは危険性のないテスト用ウイルスを使用する．また，抜き打ち検査は混乱を招かないように問い合わせ対応等の準備を適切に行う必要がある．

参考文献

［1］ 不正アクセス行為対策等の実態調査 調査報告書，警察庁，2001 年－2006 年

［2］ 地方自治情報管理概要，総務省，2007 年

［3］ ISMS 認証取得事業者数の推移，財団法人日本情報処理開発協会（JIPDEC）

［4］ 2006 年 情報セキュリティインシデントに関する調査報告書，NPO 日本ネットワークセキュリティ協会（JNSA），2006 年

［5］ 情報セキュリティ白書，独立行政法人情報処理推進機構，2008 年 6 月

［6］ セキュリティポリシーの作成と運用，トーマス・R・ペルティア（著），Thomas R. Peltier（原著），三輪信雄（翻訳），ISPP 翻訳有志（翻訳），2001 年 12 月

［7］ 市場の失敗事例で学ぶ情報セキュリティポリシーの実践的構築手法，打川和男（著），ジェイエムシー（編集），2003 年 4 月

執筆者紹介

鈴　木　武　俊（Taketoshi Suzuki）

情報セキュリティ専門企業にて，セキュリティサービス開発，セキュリティプロダクト導入等コンサルティング業務に従事した後，2005 年日本ユニシス(株)入社．現在は共通利用技術部システム管理技術室に所属し，大企業向け情報セキュリティ実装支援，情報セキュリティ診断，情報セキュリティ監査等のコンサルティング業務に従事．CISSP, ISMS 審査員補．

真　田　大　志（Hiroshi Sanada）

大手データセンタにおいてネットワークの構築・運用業務に従事．その後，情報セキュリティ専門企業にて，情報セキュリティ脆弱性診断業務・不正アクセス監視業務を経て 2006 年日本ユニシス(株)入社．現在は共通利用技術部システム管理技術室に所属し，情報セキュリティ実装支援，情報セキュリティ診断，情報セキュリティ監査等のコンサルティング業務に従事．CISSP.