

情報セキュリティ事故再発防止策についての考察

Analytical Thoughts on Certain Preventative Measures against Repetition of Information Security Incidents

牧 野 英 克

Hidekatsu MAKINO

相 澤 吉 勝

Yoshikatsu AIZAWA

はじめに

「後絶たぬ情報流出：海自の暗号やNTT顧客」「日産—顧客情報が流出：最大538万人分の可能性」。これらは、それぞれ2006年12月13日と12月22日の日本経済新聞の記事見出しから拾ったものである。新聞報道によると、ファイル交換ソフト「Winny（ウイニー）」¹⁾を組み込んだパソコンがコンピュータウイルスに感染し、利用者が気づかない間に個人情報や国の防衛情報などがインターネット上で閲覧できる状態になるケースは現在も官公庁から民間企業に至るまで幅広く続発しているという。2007年1月のある日曜日の朝のこと、テレビの討論会を視聴していると所謂ホワイトカラーエグゼンプション²⁾の導入の可否が熱っぽく論じられていた。導入に理解を示す著名な評論家が、いまや成果主義でIT社会なのだから、職場にいなくともパソコンと携帯電話があればどこでも仕事は可能である。会社にとらわれない自由な時間をもっと楽しむべきであるとの自説を展開していた。職場に居座って残業する必要性も薄れていくはずであると主張していた。果たしてそうであろうか。冒頭の新聞報道にもあるように個人情報保護法が全面的に施行された2005年4月以降から現在に至るも、後を絶たない情報流失事故、とりわけWinnyに関連するものは、会社の顧客情報を職場外に持ち出し、自宅で作業したことから惹起されたものであり、また、自衛隊の秘密扱いの防衛情報がインターネット上に流出したのも隊員の私物パソコンからだといわれている³⁾。この研究は、情報流失事故の背景とその実務的な再発防止策に

ついて考察するものである。なお、この研究は情報流出事故に巻き込まれた苦い経験を有するNECグループ⁴⁾から提供されたデータを参考にしているが、NECグループ関係各社の具体的事例を紹介するものではなく、また関係各社の見解を示すものでもない。

1. 情報流失事故の概要

(1) 情報流失事故の態様

情報流失事故は、情報セキュリティの三大要素である「機密性」、「完全性」および「可用性」のうちの、「機密性」にかかわる事故である⁵⁾。主要な情報流失事故を類型化してみると下記のようなになる⁶⁾。このうち、個人情報保護法の全面施行以降（2005年4月1日から）続発したのが下記①に掲げる「Winnyウイルスによる情報流失」事故である。本研究は主に「Winnyウイルスによる情報流失」事故に焦点をあてたものである。

- ① Winnyウイルスによる情報流出
- ② 外部からの不正アクセス
- ③ 盗難・紛失（ノートパソコン、USBメモリ、書類、携帯電話など）
- ④ 内部犯罪、情報持ち出し（Winny事故に結びつく可能性あり）、目的外使用
- ⑤ 技術的ミス（設定ミス、誤操作、対策不足）

(2) 流失の対象となっている情報資産の種類

個人情報を含めて保護すべき情報は「情報資産」と称されている⁷⁾。これら情報資産のなかには（イ）顧客から預かった情報（個人情報、人事情報、営業情報、購買情報、生産情報など）、（ロ）顧客に提供する予定の情報（作成中の設計書、開発中のプログラムなど）および（ハ）会社固有の情報（技術情報、顧客情報、経営情報、取引情報、従業員情報、リクルート情報など）が含まれる。これらの情報資産はアナログデータとしても管理されているが、IT社会においては利便性の高いデジタルデータの形態をとり、各社のコンピュータシステムの対象となって保管・管理されている。本研究では、主にデジタルデータ化された情報の流失事故を対象として取り扱っている。

(3) 情報流出事故の主たる当事者

従前の情報漏洩・流失事故といえば、産業スパイのような外部からの侵入者による情報の窃取をイメージしよう。また、IT社会においても情報漏洩・流失事故の典型例としてはハッカーなどによる情報の不正アクセスが想起される（「不正アクセス行為の禁止等に関する法律」）。しかしながら、最近の「Winnyウイルスによる情報流出」事件の多くは、社員、派遣社員、業務委託先の契約社員など、会社内部にあるデジタルデータ化された情報資産を、会社の外に持ち出し、自宅の個人所有のパソコンを通じて会社業務を行っているケースから発生している。新聞報道されている情報流失事故からみると、外部に持ち出される情報は、個人情報を含む顧客情報であったり、従業員の人事データなどであったりすることが多い。冒頭でも記述したように、IT社会においては、職場以外でも仕事をすることは容易に可能である。必要な情報をデジタルデータで携帯して持ち歩き、あるいは電子メールを自宅に転送し、深夜や週末にやり残した会社業務を自宅のパソコンを使用して行うことは、一般的なことのように思われる。しかし、皮肉にも情報流失事故は、仕事熱心な社員を巻き込むことが多い。家庭内では家族で同一のパソコンを共用することが多く、家族の誰かが Winny ソフトをインストールし、これがウイルスに犯され、それを知らずに会社業務をその汚染パソコンを使用して行ったことが事故の主な原因となっている。なお、現在、ほとんどの会社は業務用パソコンに Winny ソフトをインストールすることを厳禁しているのが実状である。

2. 情報流出事故の背景

(1) 情報資産に対する認識不足

IT社会が進展していくなかで、「情報」が人、金、物に続く第四の経営資源であるといわれているのは周知のとおりである。しかしながら、最近の企業経営を不祥事という切り口でみると、人、金、物に対する扱いが不十分・不適切なことから多くの問題が続発している。ましてや第四の経営資源である情報については、流失事故を中心にほとんどの企業が問題を起こしているといっても言い過ぎではないであろう。「人」についてみると、生命の軽視が問題となった2005年のJR西日本福知山線事故、セクハラやパワハラに係わる事故の増加、成果主義に便乗するような従業員処遇の劣化や本来の趣旨が怪しいホワイトカラーエグゼンプション問題などである。「金」については、監査法人までも巻き込む粉飾決算、安易な金儲けに走るインサイダー取引、後を

絶たない消費者金融問題などである。「物」については、一流企業も例外ではない。自動車、電池、ガス湯沸かし器、食品などにおける品質問題が多発している。これら有限な人、金、物についての資産としての重要性やリスク管理の必要性は、各企業において以前から取り組んできたことであり、従業員一人ひとりのレベルにおいても、重要性を認識することは比較的容易である。しかしながら、会社固有の情報、顧客から預かった情報、あるいは個人情報については、人、金、物との取扱とは異なり、複製が容易で、持ち運びが簡単であり、その流布も瞬時に世界を駆け巡ることもまれではない。そういった特性を持った情報の取り扱いについて、日本企業全体において、いまだ習熟していないのが現状であろう。従って、情報流失を中心とした事故対応についても、試行錯誤的な面があることも否めない。この点については、さらに、本稿の後半で論じたい。

（２）遵法精神や倫理観の欠如

情報流失事故の背後にあるものとして見逃せないのは、情報を扱う人間の弱さである。具体的には遵法精神や倫理観の欠如をあげることができよう。情報流出事故を起こした企業のトップが低頭して詫げる姿をマスコミの報道を通して見るたびに、再発防止ができずに、他山の石に学ぶどころか自山の石にも学べない企業が多いことを認識できる。期限切れの原料使用で不祥事を起こした不二家が最近の例であろう。しかし、抜本的な構造変化が日本の経済、社会システム等において実現されない限り、情報流出事故のみならず、企業不祥事を撲滅していくことは容易ではないと思われる。こうした不祥事を引き起こす構造上の問題として、市場シェアの拡大やコスト削減を重視し過ぎてきた企業体質をあげることができる。結局は商売をとりたいたがために、違法な行為として充分認識したうえ、発覚することはあるまいとの希望的観測のもとで、違法行為をやめられないということであろう。また、「他社もやっているから」という理由づけで、自らに言い聞かせ、悪の慣行に逃げ込んでしまうことが多いように思われる。生き残りをかけたグローバルベースの熾烈な競争が今後も続くことは容易に想像でき、こうした中でより一段と厳格な企業倫理を確立していくことは焦眉の急である。

もう一つの不祥事の要因として、目に見える定量的な成果を偏重しがちな能力至上主義がある。社内での競争を勝ち抜くために不正な行為に走ってしまう傾向があることは否めない。事の本質を闇から闇へと葬り、金銭で揉め事を解決しようとする体質が蔓延り、こうした体質が安易な情報の取扱のなかでも散見できる。また、会社の信用を害することが明らかな負の情報は、当然これを隠そうとする。そんな隠蔽体質が

流失した情報を拡散し、事態の収拾をより困難なものとすることが多い。

こうしたことの土壌にあるものとしては、自分が良ければ、それで良いという島国根性、フェアネス精神の欠如、正直者がばかをみるとの思い込みなどが考えられる。かの夏目漱石によると、「国家的道徳というものは、個人的道徳に比べると、ずっと段の低いもののように見える」⁸⁾とのことである。国家と会社は規模や性質が違うとはいえ、個人が会社という大きな組織の中に埋没してしまうと、個人的な道徳が麻痺してしまうことがある。従って会社における道徳や所謂企業倫理というものは、意識的に向上させていく日頃の努力(啓発活動)がないと、結局のところ低レベルのものになってしまうものなのである。ここに、1997年3月に発表されたデータでやや旧聞に属するが、大変興味深い日米でのアンケート調査がある。これは、米国のギャロップ社と日本の読売新聞社との共同の世論調査であり、日米で大きく異なった回答が出ている以下の二つの項目について紹介したい。まず一つは「信頼できる公共機関は何か」との質問についてである。

日 本		米 国	
1. 新聞	33.1%	1. 教会	60.4% (日本の寺社6.1%)
2. 警察・検察	28.7%	2. 病院	39.0%
3. 裁判所	25.6%	3. 軍隊	35.2%
4. 病院	20.1%	4. 学校	30.8% (日本9.2%)
大企業	1.3%	大企業	10.1%

もう一つは「21世紀の指導者に必要な資質は何か」というアンケート調査項目である。

日 本		米 国	
1. 指導力	54.1%	1. 倫理観	63.4%
2. 決断力	52.0%	2. 面倒みのよさ	38.5%
3. 人格・人柄	41.2%	3. 信仰心の厚さ	35.5%
4. 先見性	34.3%	4. 先見性	34.5%
5. 政治理念	20.0%	5. 人格・人柄	29.2%
倫理観	15.1%	決断力	25.8%

上記のアンケート調査結果は、色々な課題を我々に投げかけているように思われる。この調査結果の日米間のズレは、取りも直さず、今後、日本企業が本腰を入れてグロー

バル企業として世界に出て行くときの大きなカルチャー・ギャップになるかもしれない。特に注目したいのは、日本における倫理観に対するウエイトの低さであり（また、米国における教会へのウエイトの高さも注目）、こうした倫理観の低さが、企業不祥事の原因の一つのように思われるのである。

（３）予防法務機能の未整備と弱体な監査機能

情報流失事故の予防としての情報セキュリティ対策としては「管理的および制度的セキュリティ対策」、「物理的および環境的セキュリティ対策」、「技術的セキュリティ対策」、「人的セキュリティ対策」などが有効であることは一般的によく知られている⁹⁾。しかし、人的セキュリティ対策が不十分のため、故意または過失により、他のセキュリティ対策がないがしろにされれば、セキュリティ対策全体が機能しないことになる。従って、人的セキュリティ対策こそが、情報セキュリティ対策の支柱であるとの考えを本研究ではベースにおいている。その意味で、教育の重要性とともに、情報セキュリティ問題の法的対応としての予防法務機能の充実と、情報セキュリティ対策をPDCA¹⁰⁾の形で循環させるためのキーとしての内部監査機能の強化がなされなければ、情報流失事故の未然防止や再発防止は極めて困難なものとなろう。

3. 情報流出事故再発防止に当たっての具体策

情報流失事故に限らず、最近の企業不祥事は内部告発に端を発することが多いといわれている。会社による対応は記者会見を含めて後手にまわることが一般的である。このため、記者会見での経営トップの説明は歯切れが悪い。しかし、会社トップは即座に事故の発生を詫び、そして原因の究明と再発防止に努めることを宣言しなければならない。原因の究明には社外の有識者を中心とする調査チームをスタートさせることが有効な手法とされている。徹底的な原因究明がなされなければ、有効な再発防止策が出てくるはずはない。事故の原因や責任の所在をあいまいにするような企業体質を改革することが求められているといえよう。原因究明と再発防止策に加えて重要なことは、失われた信用回復の対策をどのように構築し、実施していくかである。ここでは、再発防止策に絞って考察してみたい。残念なことに、わが国では不祥事を起こした企業は詳細な再発防止策を文書化することで、再発防止が可能であるかのような錯覚にとらわれることが多く、そうした安直な企業姿勢が次なる不祥事へと繋がっていくといわざるをえない。同様に、現在、2008年度に控えた日本版SOX法の導入に

備えて、上場企業を中心に内部統制システムの構築を急いでいる。しかしながら、社内ルールや業務手続などの文書化（可視化）のみにとらわれすぎると「仏作って魂入れず」ということになるだろう。

（１）行動基準の徹底

ほとんどの会社においては情報セキュリティ基本規程¹¹⁾を制定し、情報セキュリティの維持・向上のための基本事項を定めて、管理体制を整備している。この場合、情報セキュリティとは、情報資産に対し、①機密性（アクセスを許可された者だけがアクセスできることを確実にすること）、②完全性（正確および完全であることを保護すること）および③可用性（アクセスを許可された者が必要な時にアクセスできることを確実にすること）を確保し、維持することをいう。具体的には情報セキュリティ管理責任者（「CIO」など）の任命、委員会の設置などを含む情報セキュリティ管理体制を整備するとともに、情報セキュリティ促進のための全社教育の定期的な実施や自社が保有する情報資産についての定期的なリスク評価（リスク評価とは、情報資産について、脅威に対する脆弱性を分析し、かつリスクが顕在化した場合の事業に対する影響度を評価することをいう）を行うことを義務付けている。

また、「情報」そのものに関するセキュリティ、「情報システム」に関するセキュリティ、「人」に関するセキュリティ、取引先等に関するセキュリティ、保管環境に関するセキュリティにつき、遵守事項を定めている。さらに、会社の基本規程では不測の事態に備えた対応策、自主点検、内部監査などにも言及し、経営トップから従業員一人ひとりにいたるまで行動基準を定めている。この点に関し、経営危機管理規程を定めている会社があり、不測の事態が発生したときに、有効と思われるので、その一例を参考までに後掲する¹²⁾。

（２）プロジェクト管理における情報セキュリティ対策の強化

① 基本的な考え方

顧客から受注したプロジェクトに関連して顧客の情報資産を取り扱う場合、基本的な考え方は「情報の入り」の統制である。まず、顧客情報を持ち込まないことが第一の原則である。プロジェクトの遂行上、どうしても顧客情報の持ち込みが必要な場合には、その情報は必要最小限のものに限定し、また顧客情報の拡散を可能な限り防ぐため、顧客情報の取扱者を絞り込み、顧客情報へのアクセスを制限することが肝要である。

② プロジェクト開始時の対応

上記の基本的な考え方のもと、顧客情報の取扱いおよびその管理方法については顧客と合意しておくことが重要であり、契約書その他の書面でその合意事項を明確化しておくことである。顧客情報の授受は顧客とプロジェクト遂行側の顧客情報取扱責任者との間で行い、顧客情報の受領時には「顧客情報の預り証」（個人情報が含まれている場合には「個人情報受領に関する預り証」）を発行し、双方がこれを確認することが必要である。また、顧客情報管理台帳に登録し管理すること、必要に応じて、暗号化やマスクの処理などを行うことも有効である。

③ プロジェクト運用時の対応

顧客情報を使用するときは、必ず顧客情報取扱責任者を通して行うこととし、その情報はペアで利用し、相互牽制の下、外部への持ち出しを防ぐような手立てを講じる。また、プロジェクト用のマシン以外でのデータの使用を禁止し、顧客情報はアクセス制御（特定サーバやパソコンに限定）の下で集中管理を徹底（ドキュメント類は鍵付きのキャビネットなどで集中管理）する。さらに、最重要な顧客情報の管理場所は物理的な立ち入り制限措置も実施すべきである。

④ プロジェクト完了時の対応

使用した情報が不要になったときは、顧客情報取扱責任者がアクセスログを確認し、当該情報が使用を許可された用途以外に使われていないこと、また外部に持ち出されていないことを確認したうえ、その情報を削除し、削除を確認する。顧客情報が不要になった場合は、管理台帳に登録された当該情報を削除し、あるいは顧客に返却する。預り証には、返却した旨を記し、顧客から借用した情報（ICメモリーカードや紙のような媒体）を返却する。最後に顧客情報管理台帳に返却したことを明記する。

（３）技術的・システムのな情報セキュリティ対策強化

技術的・システムのなセキュリティ対策の強化としては、情報漏洩防止のためのIT武装化が必要となる。これには、かなりの額のIT投資が必要となることもあるので、どのような技術的セキュリティ対策を導入していくかについては会社のIT戦略部門との連携が必要である。この面では、外部記憶媒体による流出阻止（外部記憶媒体への書き込み禁止や印刷防止）やネットワークによる流出阻止（電子メールでのガードやダウンロード不可制御）などのセキュリティ対策が考えられる。こうした対策はITの

利便性を制限することにもなり、慎重な対応が必要である。

上記のようなセキュリティ対策に加えて、従来から実施されている一般的な全社セキュリティ対策の継続も必要である。これには、①個人認証基盤の構築による社内システムへのアクセス管理、②パソコンへのソフトウェアのインストール状況の監視（不正ソフトウェアの使用など）、③パソコンの暗号化、④グループ外へのドキュメント流出防止、⑤USBメモリの使用制限（暗号化USBの配布）、⑥サーバーの定期的な脆弱性の検査、⑦ハードウェア／ソフトウェアのたな卸し実施を通じての紛失監理などが含まれる。加えて、SOX法対応の内部統制体制の見直しの過程で、ITアーキテクチャーそのものの再構築が必要となることもあろう。

（４）協力会社における情報セキュリティ管理体制の強化

情報流出事故の防止のためには、自社だけでなく、企業集団としての管理体制の構築が必要なことはいうまでもない。ここでは、これに加えて、下請けなどの協力会社に対する情報の開示および管理の徹底について考察する。なぜなら、協力会社に開示した顧客情報が流出するという事故も起こっているからである。この面でも、顧客情報（顧客のシステム環境バックアップを含む）は、協力会社には開示しないことを基本スタンスにすることが肝要である。特に、個人情報を含む顧客情報については、社内の管理場所から一切外に出さないことに徹し、どうしても協力会社への開示が必要な場合には社内の指定場所でのみ作業させ、情報の持ち出しを認めない。協力会社に顧客情報を開示する場合には、まず顧客の書面による合意を事前に得ることが必要であり、「顧客情報の預かり証」を協力会社から取得する。開示に当たっては、センシティブな情報をマスクする。また、協力会社に開示した情報も、顧客情報管理台帳に登録するとともに、協力会社における管理、返却・消去の実施を継続監視しなければならない。協力会社と締結する業務委託契約等においては、秘密保持義務を課すとともに、契約違反に対する制裁条項も必要となる。さらに、協力会社に対しては、作業に使用するパソコンの暗号化、ファイル交換ソフトの使用禁止、個人パソコンの業務での使用禁止などを明確化することなどが不可欠である。

（５）オフィスセキュリティの強化

これは、所謂物理的情報セキュリティ対策であり、次の３点からの強化策が有効と思われる。また、こうした物理的な情報セキュリティ対策の実施は、会社の機密情報が「営業秘密」として不正競争防止法に基づく保護を受けるという観点からも極めて

重要である⁹⁾。

① ビル・フロアの入場セキュリティの強化

個人別の入退場情報をきめ細かく把握・管理できるセキュリティ・システムを導入する。顧客情報が保管されている特定フロアへの入場制限（入場ドアのセキュリティ、フロアの間仕切りなど）を行うとともに、サーバー室やサーバー・コーナーへの物理的セキュリティ強化が必要である。

② 持ち込み品・持ち出し品の管理

検査員を入退場ゲートに配備し、持ち込み品と持ち出し品の検査を実施する。特に、パソコンなどの社用品の持ち出しに関しては、管理制度を構築し、これを厳格に適用していくことが肝要である。

③ 重要情報の廃棄管理の徹底

文書管理規程を制定するのは最低限必要なことであり、また、そうした社内ルールや顧客との契約上の取り決めに基づき、不要となった会社の秘密情報や顧客情報を含むドキュメント類のシュレッダーによる廃棄の徹底と、これらの情報を含むCD-R等の電子媒体の廃棄管理も徹底しなければならない。

（6）情報セキュリティ教育の充実・強化

人的情報セキュリティ対策の中で、最も重要なものは教育の実施である。これについては全社一律の教育だけではなく、階層別・部門別の教育や、集合教育とWEB教育の併用など、きめ細かい教育メニューを用意し実施していくことがポイントであり、以下がその例である。

① 新人教育

Winnyの利用者は、30万人から50万人いると推計されており、その中心は高校生、大学生といわれている。この観点から、まず、新卒社員については入社前の内定教育の段階で情報セキュリティ教育を開始することが有効である。また、入社時に実施される新入社員教育プログラムの中に情報セキュリティ教育を組み込み、特に顧客情報の取扱にあたっての秘密遵守につき、誓約書を提出させる。なお、最近では、こうした誓約書を電子的に行うことも一般化されてきている。しかしながら、細かな誓約条件を読まずに「誓約する」欄をクリックする者も多く、この面では集合教育の方が有効といえよう。

② 中途入社社員等への教育

中途入社社員への教育については、定期的に行われている次回の社内教育の時期まで引き延ばされることが多いという現実があり、手遅れになるケースも考えられる。従って、たとえ中途入社社員が一人でも情報セキュリティ教育を実施する教育体制の構築が必要であり、新入派遣社員や新規構内請負社員への教育をふくめて、受け入れ時に教育を実施することが情報セキュリティ事故の未然防止に役立つものである。

③ 階層別教育

新たに会社に加わった者への教育に加えて、定期的な全社教育が情報セキュリティ分野においても必要なことはいうまでもない。集合教育の実施に当たっては、例えば、部門別の教育メニューを用意したり、あるいは担当者コースと管理者コースというような区分での教育を行い、情報の取扱に当たっての管理責任のレベルに合わせた教育プログラムを用意したりするなどのきめ細かさが必要である。なお、役職者については、その昇格時に行われる課長研修や部長研修の場で、情報セキュリティ教育を実施するのが適当である。

④ 協力会社への教育支援

前述したように協力会社における情報セキュリティ管理体制の整備も急務となっている。協力会社に対してはセキュリティツールを提供するなどの支援に加えて、情報セキュリティ教育や啓発活動にも積極的に支援していくことが必要となる。具体的には、協力会社での教育に当たっての講師派遣や自社での社内教育に協力会社社員も受け入れるなどの支援が考えられよう。

⑤ 教育内容、実施方法

情報セキュリティ教育は、WEB教育と集合教育の併用によることが最も有効と考えられる。教育内容としては、(a) 基本方針、基本規程など関係規程類の理解、(b) 個人情報保護法の遵守、(c) 「営業秘密」の管理、(d) 電子マナー、(e) 技術・システムセキュリティ、(f) 顧客システムのセキュリティ、(g) 事故事例の分析・検討、(h) セキュリティ資格取得の推進（社内におけるセキュリティ専門家の育成）などである。また、多くの会社ではCSR教育は企業行動教育などを通じて、企業倫理の確立や行動規範の徹底などに努めており、こうした教育とも連動させることが望ましい。

(7) セキュリティ事故関係者に対する処分

情報セキュリティ事故には業務多忙のため、会社情報を自宅に持ち出し、私用のパソコンで仕事をしたことが原因であることが多いといわれている。たとえ善意からでた行為とはいえ、こうした行為は社内ルールに反する行為であり、情報流出事故が会社に与える影響は極めて大きい。とりわけ、顧客からの信用失墜のダメージは深刻であり、事故が発生すると、事故の外部発表は必須で（ときには記者会見）、個人情報からみでの関係官庁への説明、二次被害の防止など、事故の対応には多大の労力と出費を伴うことになる。従業員に対する懲戒処分は基本的には就業規則に基づき行われ、その適用は厳格でなければならない。事故の関係者に対しては、個人業績評価（成果主義に基づくもの）や関係者の属する部門の業績評価において、事故を招いた責任を反映させることになる。また、顧客との関係では、事案の機密性を考慮したうえということになる。社内に対して事案の内容を公表するとともに、場合によっては関係者の氏名の公表も必要となろう。さらに、事件の直接の発生原因が派遣会社や協力会社にある場合には、契約の解除、損害賠償請求、あるいは取引停止などを行うことになる。関係する契約条項の内容が不明確のために、そうした会社との間に新たなトラブルを生むことにもなるので、契約締結に当たっては法務部門のチェックを事前に受けておくことが必要なことは当然である。

(8) モニタリング活動の強化

① 個人情報保護状況に関する監査

社内の各部門が保有している個人情報の管理体制については、個人情報保護管理規程において定めている会社が多いと思われる。通常、こうした管理体制の監査については内部監査部門が担当する。問題は監査部門がどれだけの陣容を抱えているかで監査の頻度や監査レベルが定まってくる。監査部門の監査活動は、個人情報管理体制の監査だけでなく、その他の監査もカバーしているうえ、スタッフの員数が少数である会社が多い。社内の各部門を最低でも年1回の監査を実施すべきであり、理想的には半期に1回としたいものである。成果主義が主流の現在、各部門の業績評価は、部門の売上と利益をベースにするのが一般的である。今後は情報セキュリティ体制に問題のある部門の業績は厳しく評価されなければならないであろう。そのためには、業績評価の指標に情報セキュリティのレベルを盛り込むことが不可欠である。例えば業績評価が半期ごとに行われるのであれば、監査部門による情報セキュリティ監査も半期ごとでなければならぬ。監査部門に関する一般的な問題としては、監査部門をより陽の当たる部署として位置づけ（閑散部門であってはなら

ない)、監査部門を経験した者の人事上の評価ポイントを大幅に上げてはどうかと提案したい。また、監査の過程で明らかになった問題点を改善活動につなげていくためには、所謂トレーサビリティが確保されなければならず、これによって、モニタリング活動の実効性が高まっていくこととなろう。

② 重要プロジェクトのセキュリティ監査

顧客情報を扱っている重要プロジェクトのセキュリティ監査は、技術的情報セキュリティのチェックが中心となることもあり、通常の内部監査部門による監査では対応しきれない面があり、こうした監査は社内の品質管理部門や技術管理部門が適当であろう。こうした監査結果も、関係部事業部門の業績評価に適切に反映すべきものと思われる。

③ 自主点検

各事業部門は自部門における情報セキュリティの確保・維持について最低半期に1回の頻度で自主点検を行い、その結果を踏まえた自主的なセキュリティ強化施策を推進していくことが望ましい。自主点検の対象となる事項については、本社の情報システム部門などが全社基準を設定し、社内に周知徹底していくことになる。この場合、自主性を重んじすぎると、手拔きの点検に陥る可能性も高いので、注意を要する。

(9) 予防法務機能の強化

情報セキュリティ事故の再発防止のために不可欠なものとして、法務部門の充実・強化を忘れてはならない。法務部門には、臨床機能、予防機能および戦略機能があるが、いまだ、問題が起こってから法務部門の出番となる会社が多い。痛い目に遭わないと、日本の経営者はなかなか予防法務の重要性を認識できないようである。こうしたことの背景としては、予防法務活動の成果の測定が難しいことがあるように思われる。確かに、大きな法律問題をかかえていないことが予防法務活動の成果なのか、たまたまそういう状況にあるのかの判断は難しい。他方、発生した複雑な法律問題を手際よく処理した際の手腕は、ビジュアルで、トップに対するアピール度も高い。要は、トップに対するパフォーマンスが評価の尺度になりやすいのである。能力主義を中心とする最近の人事制度の下では、確かな眼力に基づき成果を公平に評価するシステムが担保されなければ、法的リスクの予防を使命とする法務スタッフのやる気を失わせることになろう。限られた人的資源を最大限活かした法務部門におけるマネジメントが確立されなければならない。もちろん法務部門が万能ということはない。従って、

法務部門が情報システム担当部門と緊密に連携することにより、より有効な情報セキュリティ対策が実施可能となるように思われる。

(10) 組織体制等の強化

情報流失事故に代表される情報セキュリティ事故の再発防止のためには情報セキュリティ・マネジメント・システム (Information Security Management System: ISMS) を確立することが急務である。ISMSは情報セキュリティを維持・管理するためのマネジメント・システムのことで、国際標準 (ISO/IEC 17799) に準拠し、日本情報処理開発協会 (JIPDEC) を中心に「ISMS適合評価制度」が運営されている¹³⁾。しかしながら、マネジメント・システムを構築することにエネルギーを費やし、構築そのものが達成のゴールとなり、その後の運営がおろそかになる例が多い。こうした傾向は、今ホットな話題となっている内部統制システムの構築についてもいえることである。組織を作り、規程類を整備し、マニュアル化をはかることが達成目標ではない。大切なことはPDCAのサイクルを回していくことである。新しい制度に魂を入れ、運用し、またこれを改善し、再運用を図っていくことが基本である。その意味で、情報資産や情報セキュリティの重要性、コンプライアンス、そしてCSR推進の意義を経営トップから従業員一人ひとりまで理解する企業風土の醸成が必要であろう。では企業風土とはどういうことであろうか。最後にその点を考察して、本稿のむすびとしたい。

むすび

情報セキュリティの重要性を全社で浸透させていくためには、情報を資産として認識し、情報資産をしっかり管理していく企業風土の醸成が必要である。「企業の社会的責任」(CSR) の一つに企業倫理を確立して不祥事を未然に防止し、社会に貢献していくという活動が含まれていることは大方の一致する見方である。企業不祥事には、故意による違法行為そのものが引き起こす悪質なものと、過失や不注意などによる事故であるが結果として深刻な事態にいたるものがある。いずれにしても、どの企業も不祥事を起こすまいと日々努力をしているにもかかわらず、昨今の報道からみても明らかのように、依然として不祥事が続発しているのが現実である。過去数年の間に不祥事に巻き込まれていない一流企業を探すのが難しい。不祥事を報道するマスコミ機関もまた例外ではなく、ここでも不祥事が起こっている。企業の大半は株式会社とい

う組織形態の法人である。法人とは我々自然人以外で、法律上の権利義務の主体となるものをいう。簡単に言うと法が作った人という意味である。自然人は目に見える存在であり、血も涙も、心もあり、そして程度の差はあるにせよ、良心や倫理観を持ち合わせている。これに対して法人には社名や社屋があっても、法人そのものは不可視であり、法人がみずから意思を有し行為することはできない。しかし、組織の構成員である個々の人間とは別に、法人としての「企業倫理」の確立が求められ、また企業市民としての良識ある行動が期待されているのである。そうはいつでも結局のところ、目に見える社長をはじめとする経営陣や個々の従業員、すなわち自然人の行為そのものが法人の行為と世間には見えることになる。

従前から、社風や企業風土という言葉はごく普通に使われている。企業風土とは、その企業特有の行動様式や文化のことを意味するという。家風とか校風という言葉も同じような意味に使われていると思われる。「こんな会社で働きたい」というある雑誌記事の中でも、企業風土への共感が会社選択の主要項目の一つに挙げられていた。一般的に、企業不祥事の有効な防止策として「風通しの良い企業風土」の醸成が必要といわれている。では、企業風土はどのような過程を経て醸成されていくのであろうか。企業風土は、経営理念やそれを実現するための経営方針の実施や社員一人ひとりによる行動規範の遵守を通じて、ある程度の時間の経過があって、徐々に創生されるものではないかと思われる。企業風土を醸成するのは企業を構成する経営トップから末端の社員一人ひとりである。従って、組織の規模が大きくなるほど、遵法経営の徹底を図り、企業倫理を社内に普く浸透させていくことは難しくなる。この面での王道はないように思われる。レベルの高い倫理観を共有し、また風通しの良い、健全な企業風土を醸成していくためには、その場限りでない地道な啓発活動や社会貢献活動の実践なども不可欠であろう。そうした啓発活動や社会貢献活動は反復、継続されて、はじめて成果をもたらすものである。2006年11月末に来日した米国証券取引委員会（SEC）のウィリアム・ドナルドソン前委員長は日本経済新聞社のインタビューに応じて、内部統制には「倫理観」が重要だと述べていた¹⁴⁾。情報セキュリティ事故の再発防止においても、人的情報セキュリティ対策、即ち企業倫理の確立や法遵守の徹底を中心とした人間系の対策が最も重要であるというのが、本研究の結論である。

注

- 1) Winnyは、インターネットを通じて、音楽や動画などのファイルを共有する「ファイル共有ソフト」の一種で、開発者は日本人である。無料で手に入るが、コンピュータウイルスに感染する危険性が高く、官庁・企業や個人のPCからの情報流出が一昨年あたりから続発している。なお、昨年 Winny の開発者に対して著作権侵害行為を助長したとして京都地裁で罰金150万円の有罪判決があった（日経新聞 2006年12月13日夕刊）。
- 2) 一定条件を満たす会社員を労働時間規制から外す「日本版ホワイトカラー・エグゼンプション」を導入するための労働基準法改正案については、2007年1月25日召集の通常国会への提出は見送られた（日本経済新聞 2007年1月17日）。
- 3) 防衛省が Winny 対策として開発した暗号化ソフトについては、日本経済新聞 2007年1月19日を参照。
- 4) NECグループの中核子会社で、IT事業に従事しているNECソフト株式会社の人事総務部から多大の協力を得た。
- 5) 中央青山監査法人編『情報セキュリティマネジメント』（中央経済社・2006年）p.4
- 6) 宮崎貞至「企業情報はこんな手口で盗まれる」（東洋経済新報社・2005年）p.56
- 7) 下記11) 情報セキュリティ基本規程（サンプル）第2条（3）および情報の安全・安心研究会「情報資産とセキュリティ管理」（生活情報センター・2006年）を参照。
- 8) 夏目漱石「私の個人主義」
- 9) 経済産業省「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（平成16年10月）P10以下
- 10) 「PDCA」とは、「Plan, Do, Check, Action」, すなわち計画⇒実行⇒点検⇒処置のサイクルのことをいう。
- 11) 情報セキュリティ基本規程（サンプル）

情報セキュリティ基本規程

（目 的）

第1条 本規程は、当社の「情報セキュリティ基本方針」に掲げる理念を実現するために、情報セキュリティ管理体制、従業員等の責務その他の情報セキュリティの維持・向上のために基本となる事項を定めることにより、当社における情報セキュリティ・マネジメントシステム（情報セキュリティの維持・向上のための施策を立案・運用・見直し・改善すること）を確立することを目的とする。

（用語の定義）

第2条 本規程における用語の定義は、次の各号に定めるとおりとする。

- （1）「情報」とは、当社が保有する一切の情報（当社固有の情報のほか、契約

情報セキュリティ事故再発防止策についての考察

その他正当な権原に基づいて顧客その他の第三者から取得した情報を含む。)をいい、有形・無形を問わない。

- (2) 「情報システム」とは、情報を取り扱う機器、ソフトウェア、伝送路等により構成される電子システムをいい、情報に関連する一切の資産および処理方法を含む。
- (3) 「情報資産」とは、情報および情報システムの総称をいう。
- (4) 「リスク」とは、ある脅威（情報資産に対して損害を与える要因をいう。以下同じ。）が、情報資産に対して損害を与える可能性をいう。
- (5) 「リスク評価」とは、情報資産について、脅威に対する脆弱性を分析し、かつリスクが顕在化した場合の事業に対する影響度を評価することをいう。
- (6) 「情報セキュリティ」とは、情報資産に対し、①機密性（アクセスを許可された者だけがアクセスできることを確実にすること）、②完全性（正確および完全であることを保護すること）および③可用性（アクセスを許可された者が、必要な時にアクセスできることを確実にすること）を確保し維持することをいう。
- (7) 「対象情報」とは、リスク評価の結果、情報セキュリティの確保・維持が必要と判断した情報をいう。
- (8) 「対象情報システム」とは、リスク評価の結果、情報セキュリティの確保・維持が必要と判断した情報システムをいう。
- (9) 「対象情報資産」とは、対象情報および対象情報システムの総称をいう。
- (10) 「不測事態」とは、情報セキュリティの確保・維持に重大な影響を与える災害、セキュリティ障害などの事態をいう。
- (11) 「従業員等」とは、当社の役員および従業員ならびにこれらに準じる者（顧問、嘱託、臨時従業員、パートタイマー等、当社との間に委任契約または雇用契約が成立した者）をいう。
- (12) 「事業部」とは、事業部門およびスタッフ部門をいう。
- (13) 「管理責任者」とは、事業部の長をいう。
- (14) 「社規類」とは、規程、細則およびマニュアルをいう。

(適用範囲)

第3条 本規程は、従業員等に適用する。

(情報セキュリティ管理体制)

第4条 情報セキュリティの維持・向上に関する全社統括責任者は、別に定める「情報セキュリティ委員会規程」により設置される情報セキュリティ委員会の委員長とする。

2. 情報セキュリティ委員会は、情報セキュリティの維持・向上のための全社の基本方針、施策等の審議、評価および情報共有を行う。
3. 情報システム部門長は、当社における情報セキュリティの維持・向上のための推進責任を負う。
4. 情報システム部門長は、情報セキュリティ委員会の審議の結果および本規程に従い、情報セキュリティの維持・向上のために必要な社規類を制定し、これらの周知徹底、運用および見直し・改善を図るとともに、全社の情報セキュリティ管理体制を構築し、情報セキュリティに関する情報共有の全社展開ならびに不測事態が生じた場合の連絡体制を整備、運営および見直し・改善を行う。
5. 管理責任者は、自事業部が保有する対象情報資産の情報セキュリティに関する一義的な管理責任を負う。
6. 管理責任者は、自事業部における情報セキュリティの維持・向上のために必要な情報セキュリティ管理体制を構築し、情報セキュリティ委員会の審議の結果および情報システム部門長により制定された社規類に従い、自事業部における情報セキュリティの維持・向上のために、これらの周知徹底および運用を行う。
7. 管理責任者は、自己の管理責任において、管理推進者を1名または複数名選任し、第6項に定める役割を代行させるものとする。
8. 管理責任者は、管理推進者を選任後、すみやかにその役職、氏名等を情報システム部門長に届け出るものとし、管理推進者を変更する場合も同様とする。
9. 情報システム部門長は、情報セキュリティの確保・維持のために必要と判断した場合、管理責任者に対して、当該事業部の情報セキュリティ管理状況の報告を求めることができる。

(教 育)

- 第5条 情報システム部門長は、人事部長その他の関係部門長と協議のうえ、情報セキュリティの促進のために必要な全社教育を従業員等および派遣社員に対して定期的
に実施する。
2. 管理責任者は、必要に応じ情報システム部門長その他の関係部門長と協議のうえ、自事業部の従業員等および派遣社員に対し、その情報セキュリティ管理体制および社規類を理解させるために必要な教育を実施する。

(リスク評価)

- 第6条 管理責任者は、自事業部が保有する情報資産について定期的にリスク評価を実施し、常に自事業部が保有する対象情報資産を把握しなければならない。
2. 情報システム部門長は、総務部門長その他の関係部門長と協議のうえ、事業部がリスク評価を実施するために必要な社規類を作成し、情報セキュリティ委員会の審議に付す。

情報セキュリティ事故再発防止策についての考察

3. 情報システム部門長は、情報セキュリティ委員会の審議の結果に従い、前項の社規類を制定し、この周知徹底、運用および見直し・改善を図る。
4. 管理責任者は、前項に基づき制定された社規類に従い、自事業部においてリスク評価を適切に行うために、周知徹底および運用を行う。

(対象情報に関する情報セキュリティ)

第7条 従業員等は、自己が扱う対象情報を適切に管理しなければならない。

2. 従業員等は、対象情報の管理にあたり、「企業秘密管理規程」、「個人情報保護管理規程」その他情報セキュリティに関連する社規類を遵守しなければならない。
3. 情報システム部門長は、総務部門長その他の関係部門長と協議のうえ、従業員等が対象情報を適切に管理するために必要な事項等を定めた社規類を制定し、この周知徹底、運用および見直し・改善を図る。
4. 管理責任者は、前項に基づき制定された社規類に従い、自事業部の従業員等が自事業部の対象情報を適切に管理するために、周知徹底および運用を行う。

(対象情報システムに関する情報セキュリティ)

第8条 管理責任者は、自事業部が管理する対象情報システムについて、その設計・開発から導入、運用、保守を通じ、対象情報システムの重要度や特性に適合した情報セキュリティの確保・維持のための施策（コンピュータ・ウイルスからの保護、記録情報のバックアップ、情報システムの運用の記録、ネットワークの管理、情報システムの付属媒体の管理、電子メールのセキュリティ、アクセス制御を含むが、これらに限らない。）を講じるものとする。

2. 従業員等は、対象情報システムの利用および管理に際し、「インターネット等使用規程」、「企業グループイントラネット利用管理規則」その他情報セキュリティに関連する社規類を遵守しなければならない。
3. 情報システム部門長は、関係部門長と協議のうえ、対象情報システムを適切に管理するために必要な事項等を定めた社規類（対象情報システムの外部への持出しに関する細則等を含む）を制定し、この周知徹底、運用および見直し・改善を図る。
4. 管理責任者は、前項に基づき制定された社規類に従い、自事業部の対象情報システムを適切に管理するために、周知徹底、運用および見直し・改善を図る。

(人に関する情報セキュリティ)

第9条 管理責任者は、社規類に従い自事業部の情報セキュリティ管理体制における役割および責任を規定する。

2. 人事部門長は、その採用の時に、情報セキュリティの確保・維持に関する必要な事項を定めた誓約書等を当該従業員等から取得するものとする。
3. 管理責任者は、派遣社員の受入の時に、情報セキュリティの確保・維持に関する必要な事項を定めた誓約書等を当該派遣社員から取得するものとする。

4. 情報システム部門長は、人事部門長および資材部門長と協議のうえ、従業員等および派遣社員の受入に関する社規類において、前2項に定める誓約書等の取得のために必要な事項等を確保するとともに、これにかかる周知徹底、運用および見直し・改善を図る。

(取引先等に関する情報セキュリティ)

第10条 管理責任者は、対象情報資産を取引先等の第三者に開示する場合、対象情報資産を第三者に預ける場合、その他第三者が対象情報資産を知り得る場合は、当該第三者との間で情報セキュリティの確保・維持のために必要な契約を締結する等の適切な措置を講じなければならない。

2. 管理責任者は、前項の場合、当該第三者による当該対象情報資産の適切な情報セキュリティの確保・維持のために必要な監督に努めるものとする。
3. 情報システム部門長は、資材部門長、総務部門長その他の関係部門長と協議のうえ、取引先等の第三者との契約に関する社規類において、第1項に定める適切な措置を講じるために必要な事項等を確保するとともに、これにかかる周知徹底、運用および見直し・改善を図る。

(保管環境に関する情報セキュリティ)

第11条 管理責任者は、自事業部の対象情報資産を保管する建物、区画、書棚等について、当該対象情報資産につき不当なアクセス、紛失、盗難等を防止するための適切な措置を講じるものとする。

2. 情報システム部門長は、人事部門長および総務部門長と協議のうえ、事業場等の入退出管理その他対象情報資産に対する不当なアクセス、紛失、盗難等に関する社規類において、これらの防止のために必要な事項等を確保するとともに、これにかかる周知徹底、運用および見直し・改善を図る。

(不測事態対応計画)

第12条 管理責任者は、不測事態が生じた場合においても、自事業部の事業活動に支障を来さない、または支障を最小限化するための計画（以下「不測事態対応計画」という。）を立案、策定、周知および見直し・改善を行うものとする。

2. 管理責任者は、自事業部の対象情報資産について不測事態が生じた場合またはその兆候を知った場合は、直ちに不測事態対応計画を実行するとともに、当該不測事態の原因究明を行う。
3. 管理責任者は、不測事態対応計画の実効性について定期的に見直し、必要に応じ改善を図るものとする。
4. 総務部門長は、関係部門長と協議のうえ、管理責任者が不測事態対応計画の策定等を行うために必要な事項等を定めた社規類を制定し、この周知徹底、運用および見直し・改善を図る。

情報セキュリティ事故再発防止策についての考察

(不測事態の報告等)

第13条 従業員等は、不測事態の発生または発生の兆候を知った場合、直ちにこれを所属する管理責任者に報告するものとする。

2. 管理責任者は、前項の報告を受けた場合、前条第2項に基づきすみやかに不測事態対応計画を実行するとともに、不測事態の発生等につき、総務部門長に報告し、総務部門長は直ちにこれを全社統括責任者に報告するものとする。
3. 総務部門長は、全社統括責任者の指示に基づき、関係部門長と協議のうえ、管理責任者とともに当該不測事態の対応を行い、事態の収束を図るものとする。
4. 総務部門長は、不測事態の再発防止の観点から、不測事態への対応結果につき、必要に応じ情報セキュリティ委員会に報告する。

(自主点検)

第14条 管理責任者は、自事業部における情報セキュリティの確保・維持について定期的に自主点検し、改善を図らなければならない。

2. 管理責任者は、前項の自主点検の結果をすみやかに情報システム部門長および監査部門長に提出する。
3. 情報システム部門長は、前項により提出を受けた自主点検の結果を評価し、その結果に応じ、改善を図るために必要な指導を管理責任者に対して行うものとする。
4. 情報システム部門長は、監査部門長その他の関係部門長と協議のうえ、管理責任者が第1項の自主点検を実施するために必要な事項等を定めた社規類を制定し、この周知徹底、運用および見直し・改善を図る。

(監 査)

第15条 監査部門長は、本規程ならびに本規程に基づき情報システム部門長等が制定する社規類の遵守状況を監査する。

2. 情報システム部門長は、前項の監査の結果に応じ、管理責任者に対して改善を図るための指導を行うものとする。

(規程等の遵守)

第16条 従業員等は、情報セキュリティの重要性を認識のうえ、本規程（本規程に基づき制定される社規類を含む。）、関係法令その他の規範および第三者との契約条件を遵守しなければならない。

(規程等の見直し・改善)

第17条 情報システム部門長は、本規程および本規程に基づき制定された社規類の実効性を確保するために、第13条に基づき報告を受けた不測事態の発生原因等を考慮のうえ、定期的にこれらを見直し、必要に応じ改善を図るものとする。

2. 管理責任者は、社規類の実効性を確保するために、第14条に基づく自主点検ま

たは第15条に基づく監査の実施により顕在化した対象情報資産に対するリスク等を考慮のうえ、定期的に運用を見直し、必要に応じ改善を図るものとする。

3. 情報システム部門長は、管理責任者に対し、前項の見直し・改善が確実に行われるように指導する。

(違反時の措置)

第18条 本規程および本規程に基づき情報システム部門長等が制定する全社基準に違反した場合は、従業員就業規則等に基づき懲戒処分その他の処分に付することがある。

12) 「経営危機管理規程」(サンプル)

経営危機管理規程

(目 的)

第1条 この規程は、第4条に定義する経営危機に関する会社の基本対応について定める。

(役員の責務)

第2条 役員は、経営危機管理の重要性を的確に認識するとともに、率先垂範の上、管理の徹底に努める。

(行動基準)

第3条 経営危機の予防や経営危機が発生したときの対応にあたり、役員および社員（以下「社員」と総称する）は、この規程の定めに従って冷静、かつ、整然と行動しなければならない。

(経営危機の定義)

第4条 この規程において「経営危機」とは、次の各号に定める事態の発生またはその虞のある場合をいう。

- (1) 会社の信用を大きく毀損または会社の存続に影響を与える不祥事および製品・サービスなどに関する事故もしくは会社に著しい損害を及ぼす事象
- (2) 会社の事業継続に重大な影響を与える地震、火災、水害などの自然災害および戦争、紛争、テロ行為などの人的災害
- (3) 社員の生命・身体の安全に影響を与えまたは社会全体に重大な影響を与える緊急事態
- (4) 重大な法制改革や急激な景気変動などの経営環境の劇的な変化
- (5) 前各号に定める事件、事故、災害または緊急事態に準じる不測の事象

(適用範囲)

第5条 この規程は前条で定義された経営危機についてのみ適用され、経営判断や事業運

情報セキュリティ事故再発防止策についての考察

営そのものに起因する業績不振などのいわゆる「経営の危機」すべての対応に適用されるものではない。

(対応の基本原則)

第6条 会社は平時においては常に適切な対策を講じて経営危機の発生を予防するとともに、万一経営危機が発生した有事の場合には迅速な対応によってその被害を最小限に抑えるとする。また、会社は再発防止のための適切な対策を講じ、社会への迅速で的確な情報の開示と説明責任を果たすものとする。

2. 関係各部門は、リスクマネジメント委員会が策定する基本方針に従って常に適切な対策を講じて経営危機の発生予防と、有事の場合を想定した被害や損失を最小限に抑えるための事前準備に努めなければならない。また、会社は積極的に広く社会とのコミュニケーションを行い、適時に企業情報を公正に開示する。

(人命の尊重)

第7条 社員の身体・生命にかかわる経営危機への対応にあたっては、会社は、その生命の保護・救出を最優先しなければならない。

(関係官庁等への届出)

第8条 経営危機に関して、関係官庁等への届出が必要な場合には、総務部長または関係の部門長が速やかに所管官庁等に届け出る。

(部門長への報告)

第9条 社員は、経営危機に関する情報や経営危機につながる情報を入手したときは、次に掲げる事項を正確、かつ、迅速に部門長に報告しなければならない。

- (1) 情報の内容
- (2) 情報の入手先
- (3) 情報を入手した日時、場所など

(社長への報告)

第10条 部門長は、部下から受けた情報を直ちに社長および関係の役員に報告しなければならない。

(情報の収集)

第11条 関係各部門は、すべての合法的な情報ルートを利用し、日頃から経営危機に関する情報の収集に努めるものとする。

(対策本部の設置)

第12条 経営危機が発生した有事のときは、社長またはこれに代わる者の指示により、直ちに対策本部を設置する。

2. 対策本部を設置したときは、直後の取締役会に報告する。

(対策本部の業務)

第13条 対策本部の業務は次のとおりとし、対策本部設置後の経営危機に関係する情報の

収集・発信は対策本部に一元化する。

- (1) 情報の収集・分析
- (2) 対応策の検討・決定・実施
- (3) 再発防止策の検討・決定・実施
- (4) 関係機関との連絡・調整
- (5) 報道機関への対応の基本方針の策定
- (6) その他、経営危機の対応に関すること

(対策本部の組織)

第14条 対策本部の組織は、本部長、事務局長（事務局員を含む）および本部員により組織される。

(対策本部の人員体制)

第15条 対策本部の人員体制は、次のとおりとする。

- (1) 本 部 長 ―― 社長またはこれに代わる者
- (2) 事務局長 ―― 総務部長
- (3) 事務局員 ―― 事務局長が指名する適任の社員。
- (4) 本 部 員 ―― 本部長が指名する関係役員および適任の社員

(対策本部員の責務)

第16条 各部員は、会社が置かれている状況を正しく認識し、経営危機の解決、克服もしくは回避のために全力を尽くすものとし、その任務の遂行上知りえた機密を無断で漏洩してはならない。

(第三者の助言)

第17条 対策本部は、必要に応じ、経営危機の対応にあたって、法律顧問その他の専門家に助言を求める。

(対応策の決定)

第18条 対策本部は、経営危機への対応策の決定にあたっては、人命の尊重を最優先するとともに、次に掲げる事項に十分留意する。

- (1) 会社の信用の保持およびその回復
- (2) 顧客、株主、地域社会その他のステークホルダーの利益

(対策本部の解散)

第19条 経営危機が収束し、かつ、再発防止策を講じたときは、対策本部は解散する。

- 2. 対策本部の解散は、本部長が決定する。
- 3. 対策本部が解散したときは、取締役会に報告する。

(対応策の実施責任者)

第20条 対策本部で決定した対応策を実施するときは、実施責任者を置く。

- 2. 実施責任者は、本部長が指名する。

情報セキュリティ事故再発防止策についての考察

3. 実施責任者は、対応策の目的が完全に達成されるようにこれを実施しなければならない。

(取締役会への報告等)

第21条 対策本部は、経営危機の対応状況を随時、取締役会に報告するものとし、報告にあたっては次に掲げる事項を含めるものとする。また、対応策の実施にあたって取締役会の決議をするものについては事前にこれを取得するものとする。

- (1) 実施した内容
- (2) 実施にいたる経緯
- (3) 実施した時期
- (4) 実施した体制
- (5) 実施した効果

(説明責任の遂行)

第22条 会社は経営危機の対応にあたり、その状況を必要に応じて適時これを公表し、会社としての十分な説明責任を遂行する。

(報道機関への対応)

第23条 経営危機に関する報道機関からの取材の申し入れに対しては、誠実に対応する。

(報道機関への対応責任者)

第24条 報道機関への対応は、社長その他の関係役員があたるものとし、会社としての事務窓口は総務部長とする。

2. 社員は、無断に報道機関の取材に応じたり、関係の情報を提供したりしてはならない。

- 13) 国際セキュリティ標準とISMSについては、田渕治樹『国際セキュリティ標準ISO／IEC 17799入門』（Ohmsha・2001年）および鳩原恵二・浅川浩『よくわかるISMSとプライバシーマーク』（日本実業出版社・2004年）を参照。

- 14) 日本経済新聞 2006年12月1日

参考文献

岡村久道『個人情報保護法』（商事法務・2004年）

田村善之『不正競争法概説（第2版）』（有斐閣・2003年）

長内健『企業秘密保護法入門』（民事法研究会・2005年）

井戸田博樹『情報セキュリティ・マネジメントの理論と実践』（白桃書房・2004年）

- 船木春仁・峰岸一彦『「知の共有」と情報セキュリティマネジメント』（ダイヤモンド社・2004年）
- 監査法人トーマツ編『セキュリティ・マネジメント戦略』（日本経済新聞社・2003年）
- 古川泰弘『情報セキュリティマネジメント』情報セキュリティ（かんき出版・2002年）
- 島田裕次『情報セキュリティ監査の実践』（同文舘出版・2006年）
- 瀬戸洋一編著『ユビキタス時代の情報セキュリティ技術』（日本工業出版・2003年）
- 大塚寿昭『コーポレート・セキュリティ』（ダイヤモンド社・2001年）
- 酒巻久『最新情報漏洩防止マニュアル』（ASCII・2006年）
- 高野一彦『情報管理とコンプライアンス教育』（九天社・2006年）
- 持丸浩二郎『会社の情報漏洩を防ぐ鉄則』（C & R 研究所・2006年）
- 原田泉ほか『情報セキュリティで企業は守れるのか』（N T T 出版・2005年）
- 森山満『顧客情報漏えいの予防プログラム』（商事法務・2004年）
- 土屋敏子『企業の情報セキュリティに秘策あり』（日経B P 企画・2005年）
- コクヨ S & T (株) セキュリティ推進室ほか『セキュリティ時代の文書管理』（日経B P 企画・2006年）
- 高橋善樹・松村幸生『営業秘密管理マニュアル&契約書作成の手引』（日本法令・2006年）
- 森末伸行『ビジネスの法哲学』（昭和堂・2006年）
- リン・シャープ・ペイン（鈴木主税・塩原通緒 訳）『バリューシフト』（毎日新聞社・2004年）