情報セキュリティへの取り組みと企業の社会的責任

Information Security and Corporate Social Responsibility

多　田　　哲

要　約　情報セキュリティをめぐる事件・事故が後を絶たない．2年前にはウイルス被害による企業システムのダウンが頻発，企業では対策に追われた．今でも，PCやインターネットに対する知識不足や認識不足，はたまた，情報の持ち出しやPC盗難などによる情報漏洩事件が頻発している．情報セキュリティに関連するこのような事件（犯人あり）・事故（過失）を防ぐためには，企業における内部統制やコンプライアンス，業務プロセス管理などを行う企業統治と同時に，情報システムサイドとしてもIT戦略策定から設計，開発，テスト，運用のシステムライフサイクルを通した管理統制を行う「ITガバナンス」が必要となる．情報セキュリティ事件や事故は，サーバ停止や企業イメージダウンにとどまらず，事業の一時停止による損失や株価低下による時価総額の縮減など，企業経営に対して非常に大きな影響を及ぼす．事件・事故がおこった後のリスク管理体制だけでなく，多くの企業においてはその予防が重要であり，ITなしには成り立たないと言われる今日の企業経営において，事件・事故の有効な予防策として，企業の内部統制の仕組みと，それを支える情報セキュリティガバナンス[1]を確立することが重要な経営課題であると言っても過言ではない．本稿では，多くの企業においてなぜ情報セキュリティ対策が重要になってきたか，という視点から説き起こし，情報セキュリティを企業の社会的責任（CSR：Corporate Social Responsibility）という視点からとらえたときに重要になってくる事業継続を担保するための計画策定（BCP：Business Continuity Plan）の必要性と策定ポイントについても言及する．

Abstract　There shows no sign of significant decline of information leakage cases and security troubles. Many of the Japanese companies have been almost preoccupied with response to Internet-related viruses and system failure recovery these two years. Today, we can still see the deluge of PC robbery news and the customer information divulgation. To prevent these information-security-related cases and troubles, IT governance establishment through entire IT life-cycle in the organization is essential. At the same time, we should confirm the corporate governance including internal controls, compliance management and business process management. There arising a substantial influence to the bottom line of the company by business interruption, sluggish stock price, and etc. with information leakage. Not only risk management after the affair, but the countermeasures must be taken. It is not an exaggeration to say that information security governance to support internal control mechanism in the firm as effective policy and measures is one of the most important business challenges, since it is said that there is no business administration without IT. This paper starts with the reason why information security comes to be so important in most of the organizations, then discusses the information security with the consideration from the aspect of CSR（Corporate Social Responsibility）. It also discusses the necessity and important items when building a BCP（Business Continuity Plan）as a pledge to business continuation.

1. 企業において情報セキュリティ対策が必要な理由

1.1 情報セキュリティ事故が与える影響は拡大

2005年4月，大手ワクチンソフト開発会社が引き起こした情報セキュリティ事故は記憶に新しい．PCをウイルスから守るはずのソフトウェアが引き金になってPCが実質的に利用できなくなった．ウイルス対策が徹底している企業であればあるほど「パターンファイルの更新」はとにかく早く行うことを遂行しているはずであるが，この場合にはそれがあだになった．PCだけでなくPOS,ATM，大規模サーバにもWindowsが採用されている現状を考えると，この影響度合いを想像するだけで恐ろしく，この事故が土曜日であったことで被害を最小限にとどめられたことは幸いであった．2004年3月に発覚した大手通販会社における顧客情報漏洩では45日にわたって営業活動を自粛し，直接的な売上損失額は150億円と想定された．同年1月に起こったブロードバンドプロバイダでの情報漏洩ではIDやパスワードのずさんな管理の状況が犯罪を招いたと言われ，大きな企業イメージダウンにつながった．こうした事件や事故の影響は，遺失売上や復旧コスト，補償/損害賠償など直接的な影響にとどまらず，社員のモティベーション低下やお客さま満足度への悪影響，企業の信頼度低下など間接的，潜在的に被害を与えるところまで及ぶ．前述の通販会社では事件後，情報セキュリティの専任部署としてコンプライアンス部セキュリティ課を設置，プロフェッショナルを3名育成，社長自身がCISO（Chief Information Security Officer）に就任し，情報セキュリティ文化を会社に根付かせる努力をしている．同社は日経ビジネスが4月25日号[2]で特集した「ビジネスパースンが選ぶ企業ブランド価値」の調査でも「正直である」「経営者に魅力がある」という2項目で2位となり総合評価で昨年の75位から28位に躍進している．従業員にとっては事件が逆バネになり結束力を高め，モティベーションも上がったという．同じく前述のワクチンソフト開発会社では事故のあと，社長が陣頭に立ってテスト方法の改善を実施しているが，今後の誠実な対応が重要であろう．このように事故やリスクをきっかけにして，会社文化や業務プロセスを全面的に見直すことは，トップがリーダシップを発揮すれば可能である．事故の100%防止は実際には難しいが，事故原因の8割を占めるとも言われている「人」に対する教育，啓発，情報セキュリティ文化の定着には，トップの理解とリーダシップ，そして地道なPDCAマネジメントの繰り返しが重要である．

1.2 必要な対策と中長期的にとるべき対策

情報セキュリティの事故にはいくつかのパターンがあり，情報持ちだし，Webからの漏洩，メールによる漏洩，うっかりミス/知識不足，ウイルスによる漏洩などと分類できる．漏洩防止対策として行うべきことはまず，「守るべき情報は何かを知る」ことである．情報資産の洗い出しを行い，その資産が漏洩することによる脅威とぜい弱性を分析，上記のような事故がビジネスに与える影響を分析して，対策を考える．対策にもいくつかの種類があり，物理環境対策，情報管理対策，人・組織対策，情報技術対策の四つに分類できる．ITが直接対策として絡むのは全体の4分の1である（図1）．

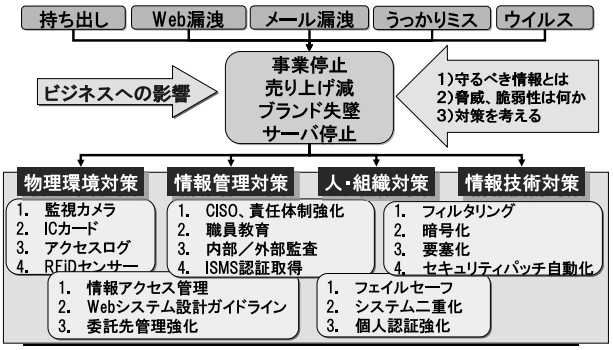


図1　ビジネスへの影響と対策例

対策を短期，中期，長期と分けることもできる（図2，図3）．個人情報保護が重要になっている今，ここに短期策として分類できるもので実施していない企業があればすぐにやるべきである．中長期策としてあげられるものも多くある．これらは業種・業態，オフィス/工場立地，社員の流動性，業界としてのガイドラインなどを考慮して各企業が個別に決めていく必要がある．いずれにしても「何のために情報セキュリティを強化するのか」という目的は明確にしておくことが必要であり，社員にとっては不便になることが多い情報セキュリティ対策では，社員にとっての納得性は重要である．

	必須対策	対応方法
組織的対策	・情報セキュリティ責任者、プライバシー責任者任命。 ・情報セキュリティ基本方針、ポリシーの作成/方針の開示。 ・組織横断的な情報セキュリティ委員会機能強化、組織別委員任命。 ・個人情報保護対応窓口設定、報告体制／手順明確化。	管理的対応
人的対策	・セキュリティ意識/モラル向上教育の実施、自己監査実施。 ・業務委託先契約の見直しもしくは守秘義務条項の強化。	
物理的対策	・入退館管理の強化。 ・コンピュータ室情報管理の強化。 ・執務室におけるマネジメント強化。	
情報管理	・情報の取扱い方針策定(秘密情報の分類方法や情報のライフサイクル等) ・媒体の管理強化	
技術的対策 ●情報漏洩防止 ●不正アクセス対策 ●パスワード管理 ●障害監視	・情報漏洩防止ソフトの導入　・修正プログラムの自動適用 ・サーバのセキュリティ検査実施　・サーバの設定最適化 ・管理者権限パスワードの強化 ・システム監視、ネットワーク監視ソフトウェアの活用	技術的対応

図2　様々な対策案（短期）

【中期】
- ・カメラによる24時間365日監視
- ・セキュリティを考慮したオフィスレイアウトの全面見直し
- ・業務アプリケーションを含めたユーザID・パスワードの全面見直し
- ・セキュリティ方針に準じた教育の実施、人材育成計画の立案
- ・継続的なセキュリティ運用の確立とアウトソーシングの有効活用検討
- ・入退館セキュリティ強化(ガードマンの配置と入退館管理、ICカードetc.)、
- ・PC・メディアに関する保管/持込/持出の制限、廃棄基準見直し、荷物検査
- ・セキュリティ管理区域の設定、
- ・机上のクリアデスク化、紙情報の管理強化
- ・社内諸規定、セキュリティ事件・事故発生時の対応手順の周知徹底

【長期】
- ・ネットワーク構成を含めたシステム全体の見直し
- ・情報セキュリティ監査の定期的実施によるPDCAサイクル運用の定着
- ・ISMS適合性評価制度などの外部認証の取得検討

図3　中長期対策例

1.3　内部統制と情報セキュリティガバナンスの確立

情報セキュリティ強化を進めると，IT だけでなく企業内での情報管理や内部統制の仕組みとの整合性が重要になる．情報セキュリティが万全でも，処理している情報自身の正当性をどのように担保するかということである．米国企業改革法と訳されるサーベンス・オクスレイ（Sarbanes　Oxley：SOX）法対応では，米国企業はグループ統治の形の整備，財務報告開示と正当性保証，不正防止，ステークホルダーへの説明責任履行などが義務づけられ，経営者の刑事責任明確化が行われている．SOX 法対応のために企業が使った初年度対応費用は売上規模の 0.3% から 1.9% とされ（KPMG 2004 年 12 月調査結果より[3]），一般的な IT 投資費用に相当するほどの膨大な手間と費用がかかっている．日本においては何が問題になるであろうか．まず考えられるのがグループ企業，海外法人，支店と事業部門縦割り組織対応である．企業によって地域別管理もしくは事業部門別管理としている管理の仕組みについて，異なる見方によって強化を図る必要性が出てくる．今までは ERP（企業会計システムなど）を導入していても，支店別には独自の集計を Excel で処理していたり，SFA（営業支援システム）にはリアルタイムで在庫データが送られていないので別途在庫確認をしていたりすることなども，報告内容や処理の正当性保証という意味では問題となる可能性がある．随時行われている経営トップへの財務報告でも，経理担当者の手製 Excel シートによる報告が問題となるかもしれない．正しい会計処理や報告がなされるだけでなく，社内での情報の正当性保証と正当性維持には人による「運用」の介在を許さない IT 活用が不可欠である．定型業務から非定型業務も含んだ業務マニュアル化も必要になり，このような IT 活用による業務の標準処理化は一時的には費用と処理時間の増大になって，企業パフォーマンスの一時的低下も懸念されるが，それを遵守して企業運営を行うことは経営者の責任である．このように考えてくると，業務を支える IT の設計からデータの正当性保証，一貫性保持が重要で，グループ企業としての IT ガバナンスと内部統制を情報セキュリティ面から企業内に構築・運用する情報セキュリティガバナンスの確立が課題となる[1]．企業における内部統制フレームワークとしては COSO（トレッドウェイ委員会による内部統制モデル　http：//www.coso.org/[4]）があり，IT 面からの内部統制モデルとしては COBIT（Control Objectives for Information and related Technology https：//www.isaca.org/Template.cfm?Section＝Obtain_COBIT[5]）が参考になる．

1.4　経済産業省による情報セキュリティ戦略

経済産業省は 2003 年 10 月「情報セキュリティ総合戦略」を策定した．策定された総合戦略は，三つの戦略と 42 の施策からなっている．三つの戦略としては「戦略 1.　しなやかな事故前提の社会システムの構築」「戦略 2.　高信頼性を強みとするための公的対応の強化」「戦略 3.　内閣機能強化による統一的推進」をあげている．（経済産業省ホームページより http：//www.meti.go.jp/policy/netsecurity/strategy.htm[6]）戦略の中で触れられている「企業情報セキュリティ格付け」ついては慎重に検討すべき，という意見もあり，情報セキュリティは，第三者認定や規制という方向ではなく，企業の自主的取組みを促進し，市場の評価が得られるような仕組みとするべき，という考えもある．企業としてはこのような戦略や企業環境を踏まえ，企業としてできることは積極的に取り組む必要がある．その例が先に触れた短期中長期策であり，内部統制と情報システムの仕組みの検討である．日本ユニシスグループでは，経済産業省からの情報セキュリティ総合戦略を受けて，一般企業としての「情報セキュリティ

総合戦略」を策定，3 カ年計画として実施中である．

1.5　ISMS 認証，P マーク取得が示す企業の取り組み姿勢

企業内での情報セキュリティへの取り組みが一定の水準で行われているかを客観的に判定する手段としては，JIPDEC（日本情報処理開発協会）による ISMS（Information Security Management System）認証とプライバシーマーク（P マーク）がある．これら認証や P マーク取得の有無により，情報セキュリティレベルを維持するための，PDCA マネジメントを行っていることが分かるため，ビジネスを始める際にパートナーとしての取引基準として ISMS 認証と P マーク取得を上げている企業も増えている．ISMS 認証取得事業者は 2005 年 6 月 10 日時点で 893 社あり，P マーク取得者は同時点で 1543 社である．（http：//www.jipdec.jp/より[7]）

2.　企業の社会的責任（CSR）と情報セキュリティ

2.1　日本企業の社会責任とトリプルボトムライン

CSR では「トリプルボトムライン」が重要といわれている．それは経済，社会，環境の三つである．つまり，企業の責任としては経済的に売上を伸ばし利益を出すだけではなく，社会的貢献や環境への配慮が必要で，それらがバランスよく達成されて初めて一人前の企業である，というものである．しかし CSR の状況は，欧米と日本では相当事情は異なると筆者は考えている．欧州では EU 統合から EU 経済圏拡大の時代を迎え，EU や政府主導で CSR への取り組みが進んでいる．「経済」問題では雇用確保や東西格差解消が課題であり，「社会」としては人権問題や女性の役割，生活の質向上，「環境」としては温暖化防止やリサイクル推進があげられる．米国では企業中心に CSR 的取り組みが進んでいる．9–11 のテロ事件があり，エンロン・ワールドコムの企業不祥事を受けてサーベンス・オクスレイ法が発効し，「経済」面では経営者倫理や内部統制が最重要課題となっている．「社会」としては多民族と多様性の受容，家族価値観の重視，「環境」としては自然保護や資源確保が大きな課題であろう．日本においてはどうであろうか．70 年代の公害問題，80 年代の過労死問題，90 年代の新卒失業問題，2000 年になっては情報隠蔽問題や現在の安全安心問題と時代毎の問題を抱えてきた日本の社会である．「経済」の側面ではコンプライアンス経営やリスク管理は当然として，日本企業の強みを再認識しそれを発揮することが重要となっている．「社会」面では少子高齢化や過疎化，地域格差，財政赤字などがあげられ，「環境」では京都議定書批准に伴う目標達成やリサイクル，資源確保があげられる．日本に主たる活動の場を持つ日本企業として CSR に取り組むためには，上記のような国際的な地域特性を踏まえ，戦略立案をする必要がある．

2.2　リスク管理，コンプライアンスと情報セキュリティ，そして CSR

コンプライアンスという言葉にはどこまでの範囲を含めて考えるべきであろうか．法令遵守から始まって，社会規範や常識を守ること，企業内の規則，規定を守ること，社内で培われている倫理観に従うこと，このあたりまでが，企業内に設置されている「コンプライアンス委員会」での討議事項であろう．CSR 施策を検討する際にはこうしたコンプライアンス施策に加えて，企業価値を高める方向の積極的社会貢献施策を考えることになる．リスク管理としては，企業における「リスク管理委員会」が設置され，突発的に発生するリスクに機動的に，かつ，必要な場合には経営トップ自身が指揮を執れるよう組織化されており，どちらかというと事後

的緊急処理対応の性格が濃い．昨今の情報漏洩事故や個人情報保護法施行を受けて，情報セキュリティ委員会機能を強化する企業も増えている． 先ほどの ISMS 認証や P マークを取得し，社内の情報セキュリティレベルを向上させるため CISO （Chief Information Security Officer）や CPO（Chief Privacy Officer）を設置，予防的，発見的だけでなく，事後処理的にも情報セキュリティ強化をしていこうという動きである．こうした委員会と同期して，もしくは既に実施済みの活動を CSR の視点から束ね CSR 戦略として推進していこうという動きも 2003 年あたりから出てきている．環境推進プログラムやメセナ，お客さま対応，IR（Investors Relation）対応，お客さま満足度向上，ボランティア活動促進などを活動範囲とし，上記委員会の機能も含めて CSR 活動戦略とする動きである．そして何をおいても CSR 活動として最大の活動は企業の本業そのものであり，本業の中でどのような社会貢献をしているかを認識し，さらに積極的に貢献を進めることである．

2.3 情報セキュリティ，CSR 戦略と費用対効果

情報セキュリティ推進や CSR を進めるにはお金がかかる．評価の基準を定めなければ企業活動とは言えないし，情報セキュリティ戦略，CSR 戦略が成功したかどうかも評価できない．警察庁による「不正アクセス行為等の実態調査」2003 年 12 月[8]によると，大手，中堅企業における情報セキュリティ投資の障害として「費用対効果が見えない」「どこまで行えばよいか基準が示されていない」が上位 2 位を占めている．また，「売上高の何%程度を CSR 活動や情報セキュリティに費用もしくは投資として計上すべきか」という質問をよく受けるが，企業規模や業種により異なる，としかお答えできない．さらに，評価軸は企業の経営理念や経営戦略に合致していなければ意味がなく，経営トップに認識されていなければ継続性は保証されない．CSR 戦略として，企業によっては焦点を当てているステークホルダーが違うケースがあり，それぞれの企業では評価軸が異なるはずである．ここには筆者が考える評価軸設定と運用のポイントを上げる．

- 経営理念や企業戦略に合致していること
- 客観的な指標であること
- 情報セキュリティ戦略，CSR 戦略実施前に宣言すること
- PDCA マネジメントのレビューのポイントとすること
- 評価指標間の関連性があり，施策実施により結果が異なると想定できること
- 経営者，社員とも納得できること

2.4 目指したい企業イメージと経営者の戦略

情報セキュリティにしても CSR 戦略にしてもやるべき施策とやった方が良い施策がある．この義務的施策と積極的施策については，施策を取りやめたり対応を間違った事例もたくさんある．日本経済が拡張していたバブルの時代に，スポーツに取り組んだ企業がたくさんあった．また，メセナ活動として収益を文化事業等へ投資するなどが行われたが，バブル崩壊後の日本経済停滞の中，いくつかの企業では業績不振などによりそれらの活動から撤退した．こうした企業の半数以上で，景気が回復しても再開しないとしている．また，企業が ISO 認定や ISMS 認証取得に先走り，認証取得企業，認定企業としての価値創出に失敗している事例もある．ISMS や ISO を経営面でどう活かすか，規格要求の意図するところを十分理解せず認証，認定を取

得した企業が多いためである．これらはどちらも義務的施策ではなく積極的施策での失敗例である．福井県の原子力発電所では 2004 年 8 月に，給水管が突然破裂し大量の蒸気がタービン室内に放出した事故があり，4 人が事故当日に死亡，他 7 人のうち 2 人が重症となった．原子力発電所が設備の定期点検を怠ったためとされている．大手スポーツアパレルメーカーが未成年者を雇用していた海外企業に生産を依頼していたため，企業のブランドイメージの低下を招いたという報道もあった．こうした事例は義務的施策を十分に実施していなかった，もしくは意識できていなかったため起こったと考えられる．情報セキュリティ戦略や CSR 施策の考え方としては，事業活動が大きくなれば，バランスするように施策規模も大きくならざるを得ない，という一方で，施策には継続性や企業経営哲学，ポリシーが必要ということを先ほどの失敗例は示している．情報セキュリティ戦略や CSR は企業の義務的行動と積極的行動をバランスさせながら持続可能な発展を実現させることであり，特に CSR 戦略は企業経営そのものである．

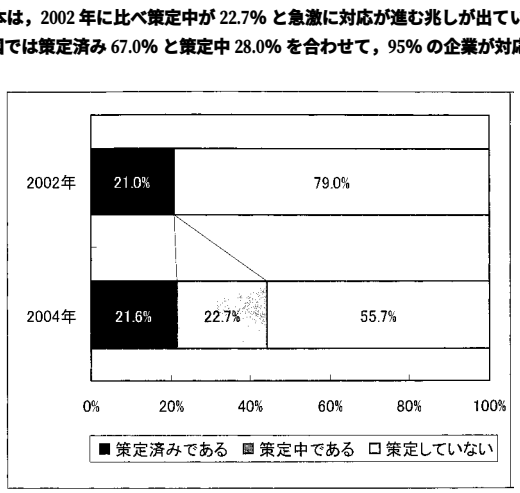
3. 情報セキュリティから事業継続管理（BCM : Business Continuity Management）へ

3.1 想定すべき事態と対応策

KPMG ビジネスアシュアランスの調査によると，米国企業では 2003 年の調査時点で 9 割以上の企業で BCP を策定済み，もしくは策定中である．一方日本企業では 2004 年調査でも 2 割程度の企業でしか BCP を策定していないという調査結果になっているが（図 4），日本経済新聞の経済教室欄でも 2005 年 5-6 月「防災と企業価値」が連載され[9]，注目され始めているのは事実である．BCP 策定時に日本企業が想定すべき緊急事態とは何であろうか．KPMG ビジネスアシュアランスの同調査によると米国での業務中断理由は，①停電②自然災害③通信の故障④機器故障⑤ウイルス感染や不正アクセス，という順である．日本での BCP 策定において対象とする緊急事態は①地震②火災③地震以外の自然災害の順となっている（図 5）．2004 年 10 月の新潟県中越地震の際，ある大手電機メーカーの子会社は大きな被害を被った．同社はその被害と影響を発表，直接被害額で 503 億円，販売機会損失で 370 億円とした．同社は地震保険には入っていなかったのですべて自社による負担となった．

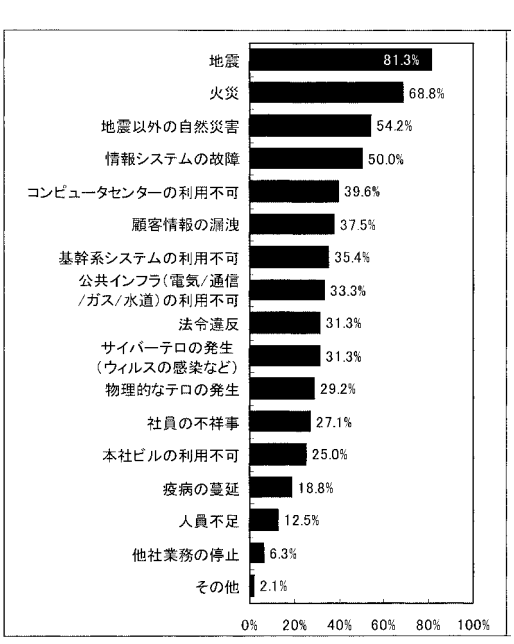
こうした理由以外にも欠陥車販売や食品中毒などの会社製品による緊急事態も存在し，このような場合には直接的な被害と言うより信用問題による事業継続危機が起こる．2000 年 6 月に起こった大手乳飲料メーカーの加工乳中毒事件では，会社対応の不手際や経営トップの不適切発言もあり世間の不評を買ってスーパー，コンビニからの製品撤去が相次ぎ売上は激減した．直後の中間決算では売上は前年同期の 3 分の 2，経常利益は前年同期比マイナス 314 億円，事件による特別損失も加えた当期利益は前年同期比マイナス 445 億円となった．当該年度決算ではさらに経常利益で前年同期比マイナス 709 億円となり，優良会社といわれた同社にも資金ショートが発生した．別の乳飲料メーカーは 1955 年にヒ素ミルク事件を起こしているが，当時の利益は前年同期比マイナス 5 億円で止まっている．同社は 1970 年までヒ素混入と中毒の因果関係を認めなかったが，事業継続問題にまでは発展していない．現在のマスコミの力，消費者の力，スーパー，コンビニの力と当時の違いが大きく影響しているのではないかと考える．2005 年現在，IT が企業経営の中核を担う状況を深く認識すれば，情報セキュリティを原因とする様々な事態を想定しておくこと，直接被害だけでなく，信用低下や販売機会損失など川下被害も想定すること，事故による資金ショート問題が深刻な問題であること，情報システム自

身をビジネスとする企業においては，情報漏洩や IT を原因とする事件が事業継続を危うくする事実を理解しておくことなど，こうした現状をしっかり認識した BCP 策定が重要である．



出典：ビジネス継続計画マネジメント（**BCM**）サーベイ
2005 年 4 月　KPMG ビジネスアシュアランス(株)

図 4　BCP の策定状況（日本）



出典：ビジネス継続計画マネジメント（**BCM**）サーベイ
2005 年 4 月　KPMG ビジネスアシュアランス(株)

図 5　BCP で対象とする緊急事態（日本）

3.2　企業戦略と BCP 立案

2001 年 9 月に起こった米国同時多発テロでは，事故の翌日から事業再開ができた企業があり，日本企業を驚かせた．メリル・リンチ社である（図 6）．BCP と日頃からの BCM の成果だったが，この結果同社への信頼は圧倒的に高まった．同社では数ヶ月前従業員避難計画を見直したところで，そのため航空機が衝突したとき，従業員は全員避難ルートを知っていた．また，2000 年問題の後，メリル・リンチ社は全世界の事業拠点に災害復旧計画システムの使用を義務づけていた．こうしたことは経営トップの BCM へのコミットメントなしには実現できない企業戦略そのものであり，事件後の同社への信頼の高まりは戦略の成功を物語っている．日本においても，金融機関だけではなくすべての企業で BCP 策定と BCM が必要として，経済産業省は 2005 年 6 月 BCP のガイドラインを公開した．
（http：//www.meti.go.jp/policy/netsecurity/downloadfiles/6_bcpguide_gaiyou.pdf）[10].

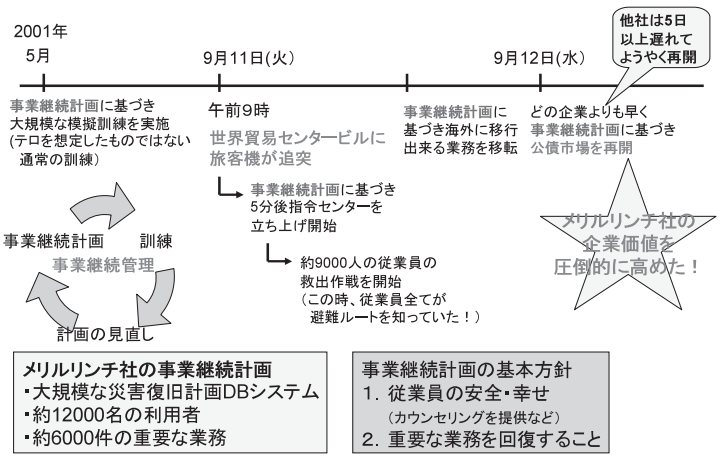


図 6　ビジネス継続計画と管理の有効性
（事例：9.11 におけるメリルリンチ社）

3.3　BCM を行うための PDCA

BCM はどのような企業でも検討することが必要なのであろうか．業界の特性や企業の置かれた環境，お客さまのニーズ，企業の戦略を踏まえて，必要な事業継続のあり方を考える必要があると筆者は考える．この際，意思決定を行うのは経営トップの仕事である．検討すべき項目は次の通りである．

■CSR の視点からみた BCM
　―社会的責任：社員の安全確保，雇用確保，地域貢献，リスク時コミュニケーション
　―地域・環境責任：二次災害防止，危険物漏洩防止
　―経済的責任：製品サービスの継続供給
■BCM として計画すべき範囲
　―BCM として想定する災害，リスク定義
　―指揮権，指揮系統確立/維持（代行者含む）
　―本社機能，事務所機能のバックアップ
　―情報システムのバックアップ

―製品サービス提供の代替手段確保

■BCP 策定のポイント

―コア業務の選定：復旧の策定対象（ファシリティ，業務，リスク）を定義する

―復旧方針，目標（時間と割合）策定：各業務の優先度を定義，目標を設定する

―災害，リスクなど被害想定：対象となるリスクを評価，被害の程度を想定する

―ビジネスインパクト分析：業務への影響度を分析，業務代替手段，代替経営資源を確保する

- お客さまに許容いただける，サービスの停止時間.
- 事業中断による被害総定額算定（1 時間，1 日，1 週間）.
- 事業中断による企業信頼低下，ブランド価値低下の想定.
- 事業中断により生じる会社責任.
- 再開を優先すべきサービス，顧客.

このようにして策定した BCP をマネジメントシステム（PDCA）として会社の仕組みに組み込み，方針，計画，点検，監査，見直し，マニュアル，シナリオを想定した緊急時行動計画を定義，訓練により計画の有効性を検証する，緊急時行動計画書の見直し方法を定義するなどを繰り返し行うこと，これが BCM である（図 7）.

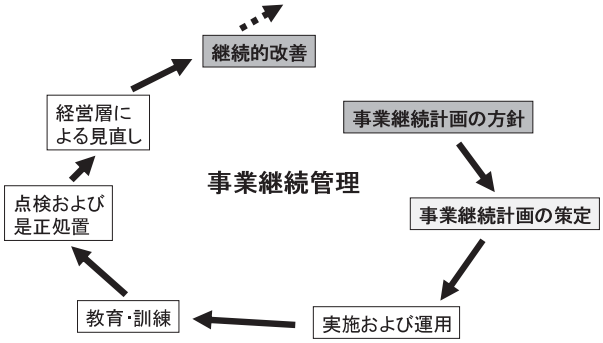


図 7　BCP/BCM の実現方法とポイント

3.4　社員は納得するか

メリル・リンチ社で避難訓練を行う際に，社員が「なぜ，このようなことをしなければいけないのか」と疑問に思い，訓練に参加しなかったらどうなっていただろうか．また，従業員避難計画が適時見直されていなかったらうまく避難できたであろうか．何のための情報セキュリティ強化であり，どのような経営目標のための BCM であるか，社員が合意し納得できていなければうまくはいかない．最重要ポイントは経営トップのコミットメントとメッセージである．

一度，情報漏洩など事故が起こると一大事である（図 8）．警察，マスコミ対応や監督官庁への説明，お客さまへの説明，従業員への説明とモティベーション維持など説明責任を果たす対応に終われる．原因究明と再発防止策を緊急に立案する，起こってしまったリスク対応のための様々な対策に追われる，など迅速かつ誠実な対応が必要になる．こうしたことをまずは起こさないための対策が重要であり，何か不測の事態を想定したときの BCP が必要，ということを社員に説明し，納得の上 BCM を行っていくことが重要である．

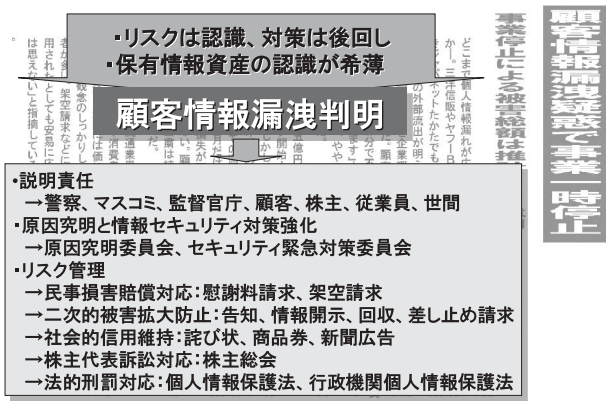


図 8　情報流通の恐怖--事業継続を脅かす被害

4. おわりに

情報セキュリティ向上のための実効ある IT ガバナンスを確立する際に重要なポイントをまとめると次の通りである．（技報 82 号「顧客価値創造特集号」顧客価値創造企業になるためにより[11]）

① 経営トップの IT 投資へのコミットメント
② 情報セキュリティへのリーズナブルな経営資源配分
③ 組織的対応
④ 人（社員や協力企業社員も含む）への教育
⑤ 継続し成長させるマネジメントの仕組み

企業における情報システムの重要性を考えると，情報セキュリティを CSR の側面からも捉えることの重要性も述べた．この視点から考えても，情報セキュリティで重要な IT ガバナンスは企業統治の重要な一部である．また，企業の内部統制の仕組みを情報セキュリティの観点から企業内に構築・運用していくという情報セキュリティガバナンスの確立が非常に重要になってくる．

本「情報セキュリティ特集号」では，まず，日本ユニシスグループで実施している情報セキュリティ総合戦略を紹介し，BCM，個人情報保護法対応という視点からの論文を紹介する．続いて，システム監査，ならびに情報システム構築，リスク分析を情報セキュリティの側面からどのように捉える必要があるか，そして情報セキュリティに関する人材教育について紹介する．事例としては，IC カードによる実証実験を紹介する．情報セキュリティにたずさわる方，CSR 活動戦略を検討している方の参考になれば幸いである．

参考文献
［1］ 企業における情報セキュリティガバナンスのあり方に関する研究会報告書　経済産業省　平成 17 年 3 月
［2］ 日経ビジネス　4 月 25 日号
［3］ KPMG ビジネスアシュアランス社　ビジネス継続マネジメントサーベイ　2004 年 12 月調査
［4］ COSO（トレッドウェイ委員会による内部統制モデル　http：//www.coso.org/）
［5］ COBIT（Control Objectives for Information and related Technology https：//www.isaca.org/Template.cfm?Section＝Obtain_COBIT）

［6］ 経済産業省ホームページより　http：//www.meti.go.jp/policy/netsecurity/strategy.htm
［7］ JIPDEC ホームページより　http：//www.jipdec.jp/
［8］ 警察庁による「不正アクセス行為等の実態調査」 2003 年 12 月
［9］ 日本経済新聞　経済教室　2005 年 5–6 月「防災と企業価値」連載
［10］ 経済産業省 BCP のガイドライン
http：//www.meti.go.jp/policy/netsecurity/downloadfiles/6_bcpguide_gaiyou.pdf
［11］ 技報 82 号「顧客価値創造特集号」 顧客価値創造企業になるために

執筆者紹介　多　田　　哲（Tetsu Tada）
1977 年大阪大学工学部卒業．同年日本ユニシス(株)入社，流通/製造業の顧客システム設計開発を担当，95 年オープンソフトウェア事業部マーケティング部長，98 年から 2000 年まで米国スタンフォード大学客員研究員，2003 年ビジネスコンサルティング統括部長，2005 年 CSR 推進室長．