１８－Ｈ００５

平成１８年度
マネジメントシステム評価検討及び情報セキュリティの総合的普及啓発に関する
成果報告書

平成 19 年 3 月

財団法人　日本情報処理開発協会

この事業は、競輪の補助金を受けて実施したものです。
http://keirin.jp

はじめに

この報告書は、財団法人日本情報処理開発協会が日本自転車振興会の補助金を受けて実施した平成１８年度情報化の進展に関する補助事業「情報セキュリティ基盤の強化に関する調査研究」事業の一環として取りまとめたものである。

情報セキュリティに関連する取り組みが対象とするリスクは、ますます多様化し複雑化している。一方で、企業等のIT依存度は、かつて無いほど高くなっており、“情報”の処理・流通・保管の形態も紙の文書やソフトウェアなど、さまざまな形態が考えられる。

情報資産の保護という情報セキュリティマネジメントの目的を達成するためには、多様化するリスクについて、顕在化させないための予防策と同様に、顕在化した場合にできるだけ損失を小さくする事故対応策を考えておく必要がある。

特に事故対応策については、ビジネスのサステナビリティへの影響を考慮し、事前に計画を策定しておく、「事業継続計画(BCP)」及びそれをマネジメントにおいて実践する「事業継続管理(BCM)」に焦点をあて、適切な情報資産の保護のあり方について調査研究することが重要である。

そこで、本事業では、国内外の事業継続関連や情報セキュリティの取り組みについて、企業や団体などの活動を調査するとともに、BCPに関するガイドを策定する。

本事業の目的は、わが国における企業や団体におけるBCPの取り組みを推進させるとともに、今後の事業継続活動に資する情報を提供することにある。

また、検討の結果については、昨年度に引き続き実施する情報セキュリティに関する総合的なシンポジウムで報告した。情報セキュリティに関連する取組みは、国をはじめ団体あるいは特定非営利法人（NPO）において、それぞれの視点、立場から行われているが、企業においては、これらの活動や成果に関する情報が個別に提供されるため、相互の関係や位置付けなどが十分理解されない面もあり、また、今後はこれらの活動の相互連携も必要とされている。このため、情報セキュリティに取り組む様々な団体等が協調して、情報セキュリティに関する総合的なシンポジウムを開催した。

このような検討やシンポジウムの実現に当っては、関連する団体の皆様のご協力により実現したもので、この場を借りて講師の方々、関連する団体の皆様に厚く御礼を申し上げる。

また、本報告書の作成にあたり、ご協力頂いた委員の皆様をはじめ原稿執筆頂いた関係各位に対し厚く御礼を申し上げる。最後になりますが、本事業にご支援いただいた日本自転車振興会ならびに日頃からご指導いただいている関係官庁に対して厚く御礼申し上げる。

平成 19 年 3 月

(財)日本情報処理開発協会

目次

1. 事業の概要及び背景

1.1 概要

本事業では、国内外の事業継続関連や情報セキュリティの取り組みについて、企業や団体などの活動を調査するとともに、BCMに関するガイドについて策定する。本事業の目的は、わが国における企業や団体におけるBCPの取り組みを推進させるとともに、今後の事業継続活動や情報セキュリティ対策に資する情報を提供することにある。また、検討の結果については、昨年度に引き続き実施する情報セキュリティに関する総合的なシンポジウムで報告した。

また、情報セキュリティに関連する取り組みは、国をはじめ団体あるいは特定非営利法人（NPO）において、それぞれの視点、立場から行われているが、企業においては、これらの活動や成果に関する情報が個別に提供されるため、相互の関係や位置付けなどが十分理解されない面もあり、今後はこれらの活動の相互連携も必要とされている。このため、情報セキュリティに取り組む様々な団体等が協調して、情報セキュリティに関する総合的なシンポジウムを開催することとし、そのテーマや内容について検討した。

本事業の検討体制は次の図の通りである。

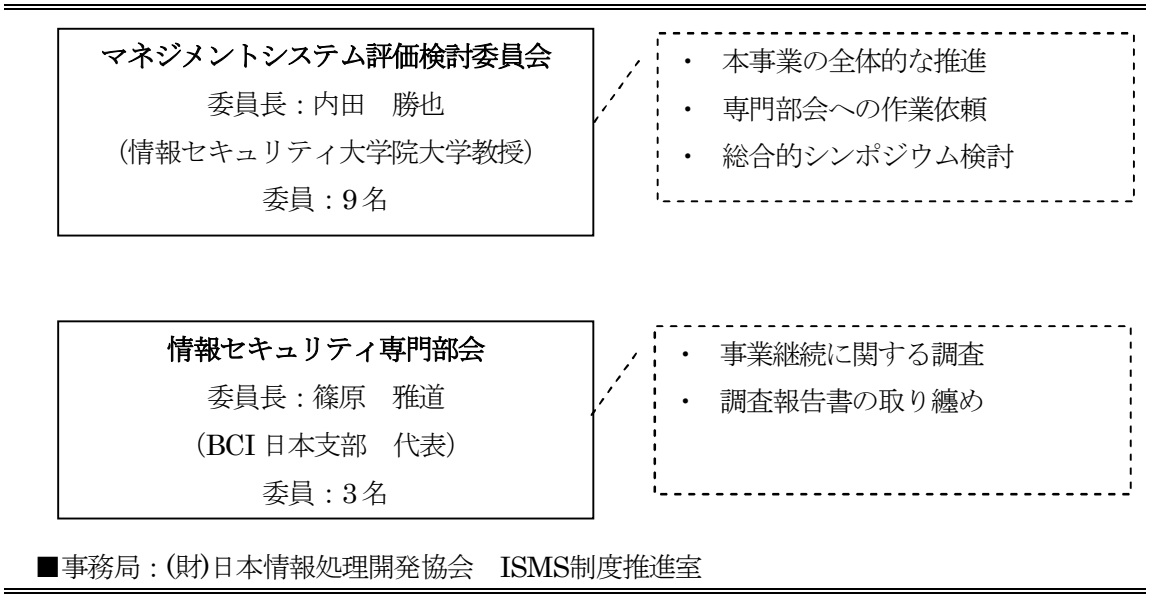


図1.1　検討体制

1.1.1 マネジメントシステム評価検討委員会

本事業の全体的な推進を主な役割とした委員会である。メンバー構成は次の通りである。

表 1.1　委員構成

ー	団体名	委員名
委員長	情報セキュリティ大学院大学	内田 勝也
委 員	JNSA(NPO 日本ネットワークセキュリティ協会)	安田 直義
委 員	JASA(NPO 日本セキュリティ監査協会)	沓澤 徹
委 員	IPA(独立行政法人情報処理推進機構)	菅野 泰子
委 員	㈱ラック内 JSOC(Japan Security Operation Center)	西本 逸郎
委 員	JEITA((社)電子情報技術産業協会)	馬場 敬博
委 員	IA japan((財)インターネット協会)	人見 庸
委 員	IN-Law(情報ネットワーク法学会)	佐藤 慶浩
委 員	BCI　日本支部	小林 誠
委 員	JSSM(日本セキュリティ・マネジメント学会)	井上　克至

1.1.2 情報セキュリティ専門部会

事業継続に関するガイド作成を主な役割とした専門部会である。メンバー構成は次の通りである。

表 1.2　委員構成

ー	所属組織	委員名
委員長	BCI 日本支部／㈱インターリスク総研	篠原 雅道
委 員	㈱アズジェント	駒瀬 彰彦
委 員	㈱KDDI＆BT グローバルソリューションズ	斎藤 俊治
委 員	日本ヒューレット・パッカード㈱	原田 薫

1.2 検討内容

1.2.1 マネジメントシステム評価検討委員会

マネジメントシステム評価検討委員会の検討状況は次の表に示す通りである。

表 1.3　検討状況

回数	開催日	主要テーマ
第 1 回	2006.8.11	・実施計画について ・今後のスケジュール
第 2 回	2006.9.22	・セキュリティ技術国際動向調査について ・情報セキュリティ総合的普及啓発シンポジウムについて
第 3 回	2006.10.26	・事業継続管理に関する調査について ・情報セキュリティ総合的普及啓発シンポジウムについて

第 4 回	2006.12.1	・情報セキュリティ総合的普及啓発シンポジウムについて
第 5 回	2007.1.25	・事業継続に関する原稿執筆について ・情報セキュリティ総合的普及啓発シンポジウムについて
第 6 回	2007.3.12	・情報セキュリティ総合的普及啓発シンポジウムについて ・セキュリティ技術国際動向調査について ・事業継続管理に関する調査について

1.2.2 情報セキュリティ専門部会

情報セキュリティ専門部会の検討状況は次の表に示す通りである。

表 1.4　検討状況

回数	開催日	主要テーマ
第 1 回	2006.9.15	・事業継続管理に関する調査方法の検討
第 2 回	2006.10.20	・各領域の定義の検討
第 3 回	2006.11.30	・各領域の定義の完成
第 4 回	2006.12.21	・各領域の関係性の整理
第 5 回	2007.1.16	・各領域の関係性の整理
第 6 回	2007.1.23	・各領域の関係性の完成
第 7 回	2007.2.5	・調査報告書の検討
第 8 回	2007.3.6	・調査報告書の検討
第 9 回	2006.3.26	・事業継続管理に関する調査報告書の取り纏め

2. 情報セキュリティ総合的普及啓発シンポジウム

2.1 実施概要

本シンポジウムを「情報セキュリティ総合的普及啓発シンポジウム」と題し、次の概要にて実施した。

① タイトル

－情報セキュリティ総合的普及啓発シンポジウム

② 主催

－財団法人日本情報処理開発協会

③ 後援（順不同）

－情報セキュリティ政策会議

－経済産業省

－情報セキュリティ大学院大学

－NPO 日本ネットワークセキュリティ協会（JNSA）

－NPO 日本セキュリティ監査協会（JASA）

－社団法人電子情報技術産業協会（JEITA）

－独立行政法人情報処理推進機構（IPA）

－日本セキュリティ・マネジメント学会（JSSM）

－財団法人インターネット協会（IA-japan）

－Japan Security Operation Center(JSOC)

－BCI 日本支部

－情報ネットワーク法学会（IN-Law）

④ 開催日時

－1 日目：2007 年 2 月 22 日（木）10 時 00 分～17 時 00 分

－2 日目：2007 年 2 月 23 日（金）9 時 30 分～17 時 00 分

⑤ 会場

－日経ホール

東京都千代田区大手町 1-9-5（日本経済新聞社内）

⑥ プログラム

■1日目　2月22日

time	講演時間	内 容	講 師
9：30～10：00	―	受付開始	
10：00～10：05	(5分)	開催コメント	司会者
10：05～10：15	(10分)	開会ご挨拶	財団法人日本情報処理開発協会 常務理事　武田　貞生
10：15～11：05	(50分)	基調講演 我が国の情報セキュリティ政策の 動向について	経済産業省　商務情報政策局 情報セキュリティ政策室 セキュリティ技術係長 金井　秀紀　氏
11：05～11：55	(50分)	講演1 IT ガバナンス時代の セキュリティオペレーション	Japan Security Operation Center (JSOC) 西本　逸郎　氏
11：55～13：00	(65分)	昼食休憩	
13：00～13：50	(50分)	講演2 財務報告に係る内部統制の 評価と監査への対応	情報ネットワーク法学会（IN-Law） 丸山　満彦　氏
13：50～14：40	(50分)	講演3 企業にとってのメールの リスクとその対策	財団法人インターネット 協会（IA japan） 山本　和彦　氏
14：40～14：50	(10分)	休憩	
14：50～15：40	(50分)	講演4 J-SOX と情報 セキュリティ監査	NPO 日本セキュリティ 監査協会（JASA） 岸　泰弘　氏
15：40～16：30	(50分)	講演5 システム管理基準追補版（財務報告に 係る IT 統制ガイダンス）の狙い	日本セキュリティ・ マネジメント学会 (JSSM) 原田　要之助　氏
16：30～17：00	(30分)	質問セッション	コーディネーター 財団法人日本情報処理開発協会

			マネジメントシステム評価検討委員会 委員長　内田　勝也　氏
17：00		終了予定	

■2 日目　2 月 23 日

time	講演時間	内 容	講 師
9:00～9:30	―	受付開始	
9:30～9:35	（5 分）	開催コメント	司会者
9:35～10:25	（50 分）	基調講演 事業継続の必要性と企業への期待 （仮）	内閣府　政策統括官（防災担当）付 参事官(総括担当)付企画官 青木　栄治　氏
10:25～11:15	（50 分）	講演６ 国際規格をリードする BCM 英国規格 ～BCM と他領域との関係整理～	(財)日本情報処理開発協会 情報セキュリティ専門部会 委員長　篠原　雅道　氏
11:15～12:05	（50 分）	講演７ BCM 国際動向について	富士ゼロックス株式会社 藤本　正代　氏
12:05～13:00	（55 分）	昼食休憩	
13:00～13:50	（50 分）	講演８ 事業継続マネジメントの 構築の実際と実務	BCI 日本支部 （BCI-Japan） 小林　誠　氏
13:50～14:40	（50 分）	講演９ IT の脆弱性と BCM	独立行政法人情報処理推進機構 （IPA）セキュリティセンター 小林　偉昭　氏
14:40～14:50	（10 分）	休憩	
14:50～15:40	（50 分）	講演１０ 米国における BCM の実際	NPO 日本ネットワーク セキュリティ協会(JNSA) （株式会社ジュリアーニ・セキュリティ &セーフティ・アジア） 能地　將博　氏

15:40～16:30	（50 分）	講演１１ 情報システムの設備ガイド	社団法人電子情報技術産業協会 (JEITA) 馬場　敬博　氏
16:30～17:00	（30 分）	質問セッション	コーディネーター 財団法人日本情報処理開発協会 マネジメントシステム評価検討委員会 委員長　内田　勝也　氏
17:00		終了予定	

⑦ 申込者数

550 人（システム上 550 名に達した時点で WEB 申込を締め切った。）

⑧ 参加者数

553 名

2.2 アンケート集計

2.2.1 概要

本シンポジウムの参加者数 553 名のうちアンケート回答数は、288 名（回答率：52.1%）であった。アンケート項目の集計結果を「3-2-2 集計結果」に示す。

2.2.2 集計結果

(1) 業種及び参加日

①業種

最も多い参加業種は「情報処理」で 38%、次いで「サービス」15%「製造」10%となっている。近年、様々なビジネスのオペレーションが IT への依存性を高めており、情報処理や IT を中心とするサービスの事業継続管理の構築が急務であること、またサプライチェーンに属している製造業等が物資の供給等に色々な形で関連業務を強化するために関心が強いことがうかがえる。尚、その他の回答としては、「認証審査」「監査」が挙げられている。

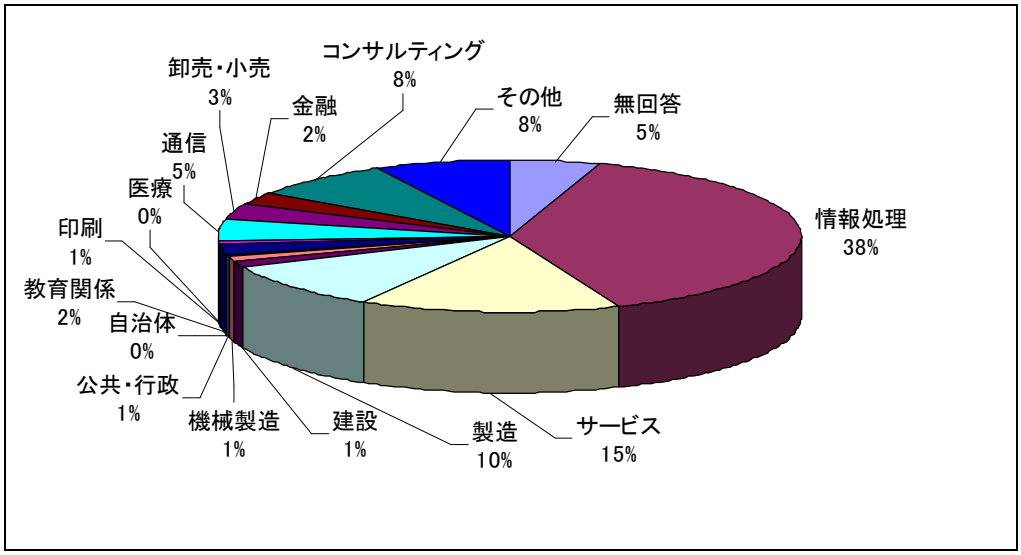


図 2.1 業種

②参加日

「両日」が 45%、「22 日のみ」が 30%、「23 日のみ」が 25%であった。

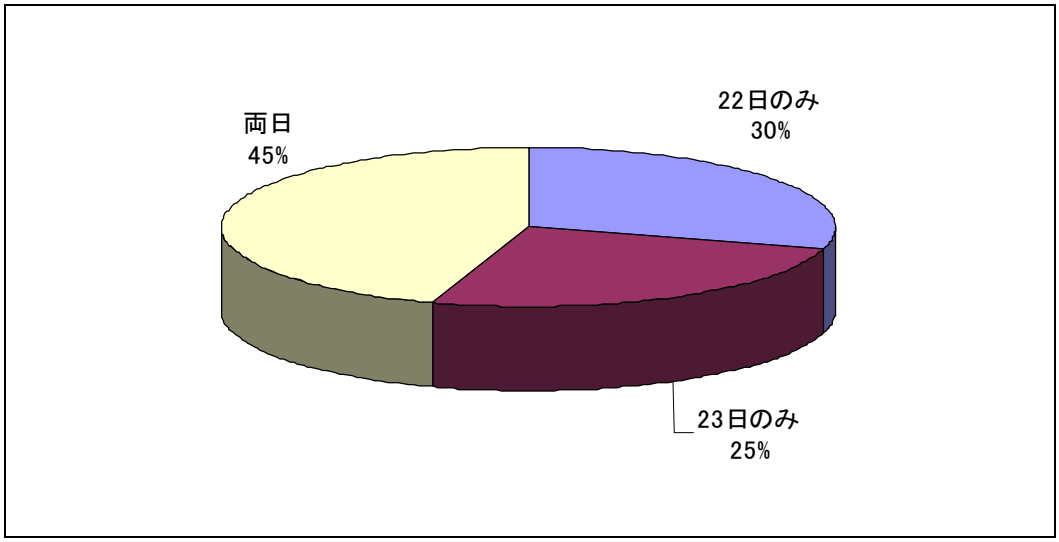


図 2.2 参加日

③従業員数

「1,000 人～5,000 人」が 25%と最も多く、ついで「5,000 人以上」が 24%となっており、大規模企業からの参加が多いといえる。

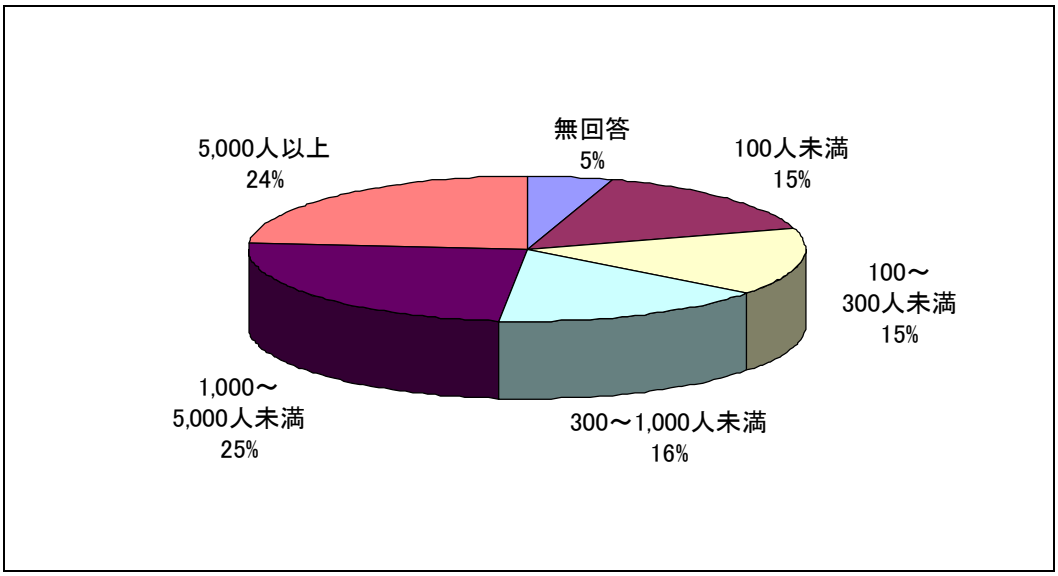


図 2.3 従業員数

④資本金

「50 億円以上」が 28%と最も多く、②の結果からも分かるように大規模企業からの参加が多い。これは、BCP を策定する企業などが年々増加傾向にはあるものの、それらの取組みは大規模企業にまだ限定されている可能性を示唆している。

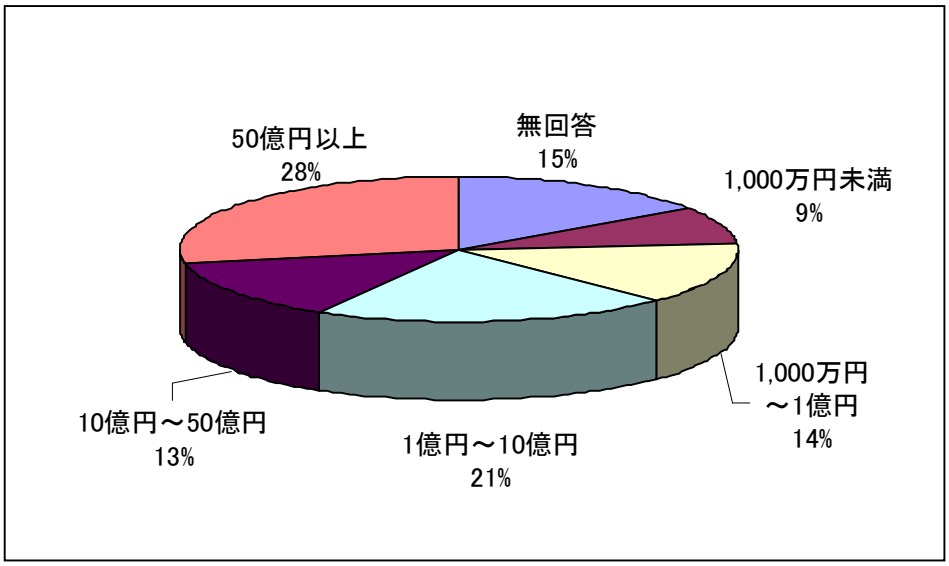


図 2.4 資本金

(2) 参加者について

①職種

「情報システム」が 29%、「企画」が 16%を占めている。

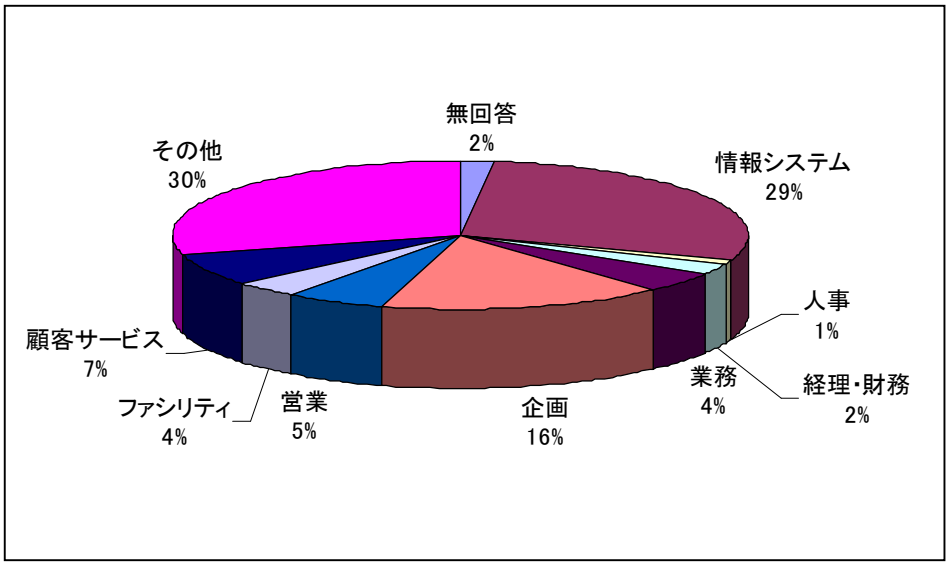


図 2.5 職種

その他の例：

監査・内部監査・情報セキュリティ監査（13 名）
コンサルタント（9 名）

②役職

「管理職」が 38%、「専門職」「一般職」がそれぞれ 24%である。

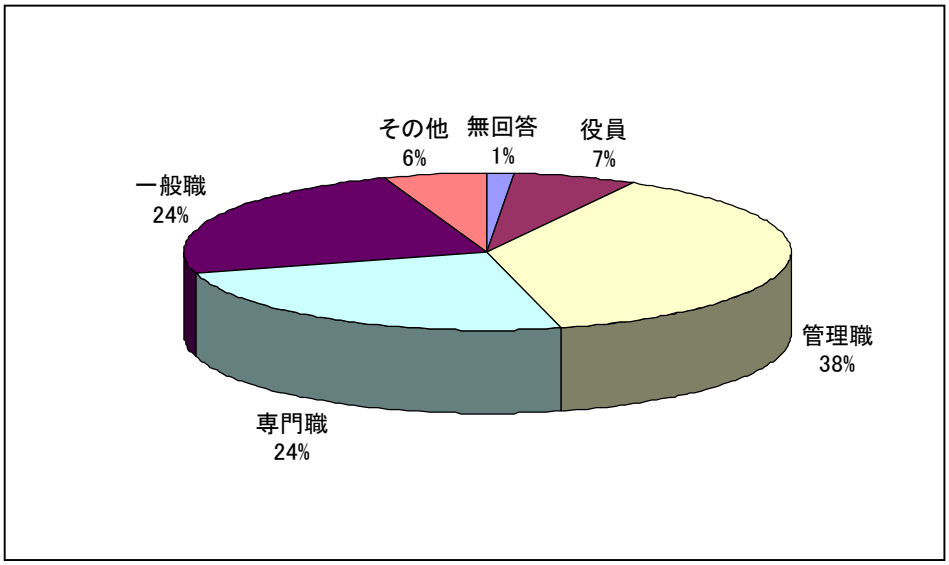
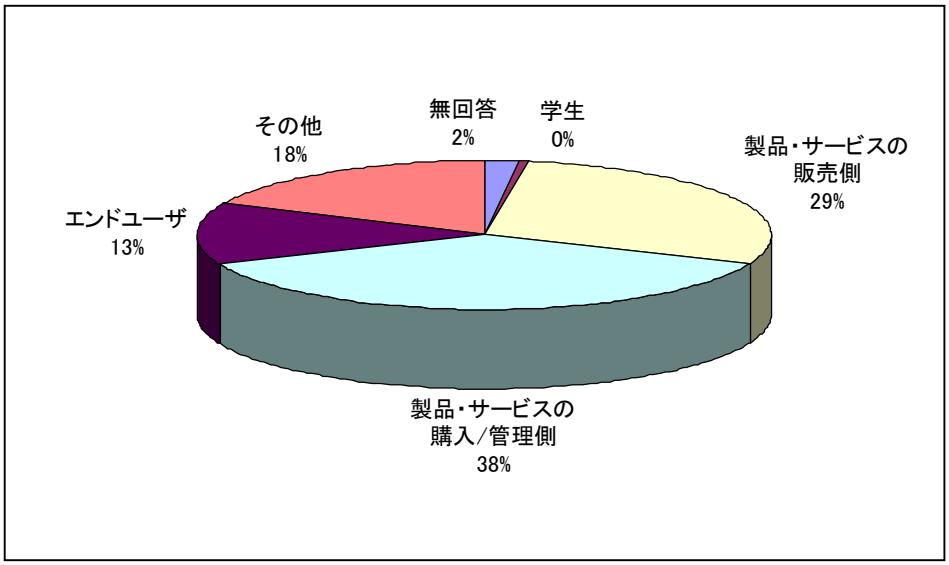


図 2.6 役職

③情報セキュリティに対する立場

「セキュリティ製品・サービスの購入/管理する立場」が 38%、「セキュリティ製品・サービスを販売する立場」が 29%である。



その他の例：

監査する立場（9 名）
提案する立場（4 名）

図 2.7 情報セキュリティに対する立場

④本シンポジウムの参加目的

「情報収集」が 88%と最も高い。

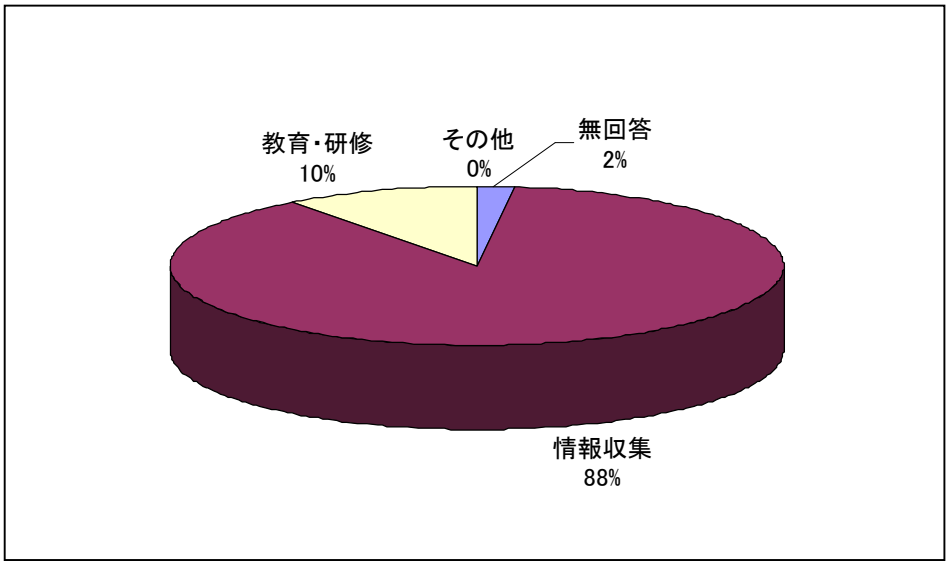


図 2.8 参加目的

(3) 事業継続計画（BCP）・事業継続管理（BCM）について

①BCP・BCM の実施状況

「実施している」が 29%、「検討中」及び「策定中」が 52%であった。

一昨年 2 月、昨年 9 月～10 月に BCI ジャパンが行なった同様の調査と比較して、「実施している」「検討中」及び「策定中」と答えた企業が増加している。

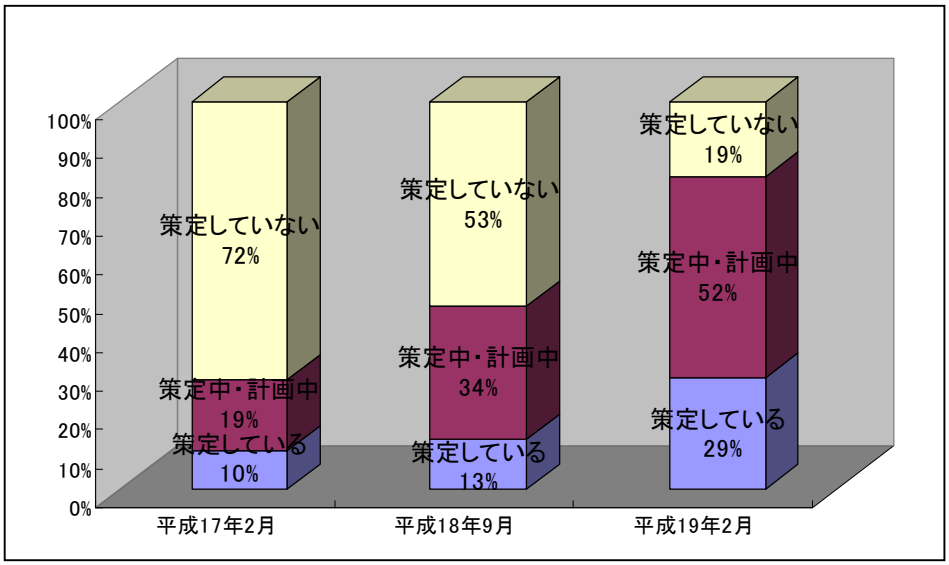


図 2.9 BCI ジャパンが行った同様な調査

前年度のシンポジウム開催時のアンケート結果と比較すると、「実施している」は 3%の増加に留まり、「検討中」「策定中」との回答は 11%減少している。（ただしこの比較は、「分からない」及び「無回答」を有効回答として計数しなかったため、実状とは誤差が生じているものと考えられる。よって、この点についての考慮が必要であると推察する。）

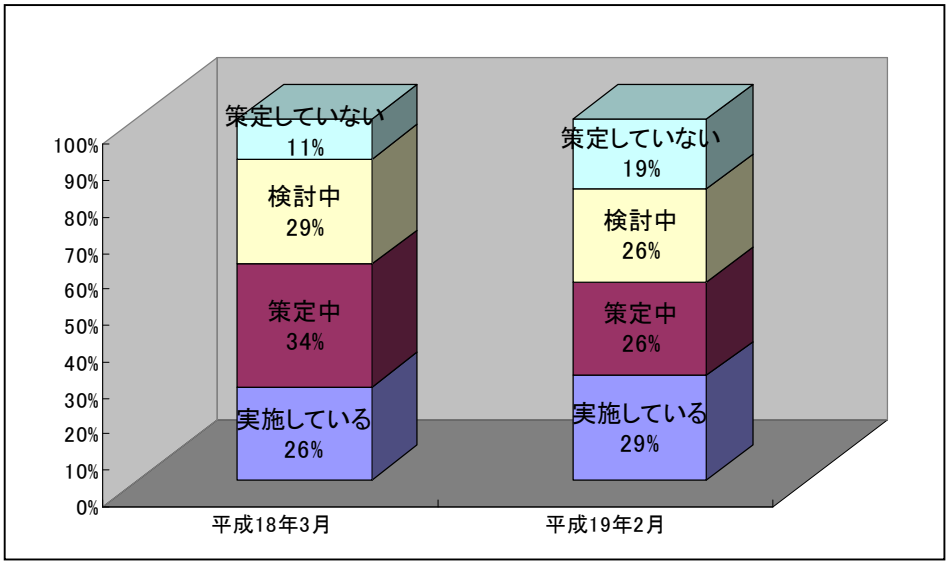


図 2.10 BCP・BCM の策定

②BCP・BCM の策定期間

BCP・BCM を「実施している」「策定中」「検討中」と回答した参加者のうち、最も多かったのが「6 ヶ月～1 年未満」の 34%、ついで「1 年～2 年未満」が 25%であった。尚、最も長く時間を要した企業は、「3 年」であった。

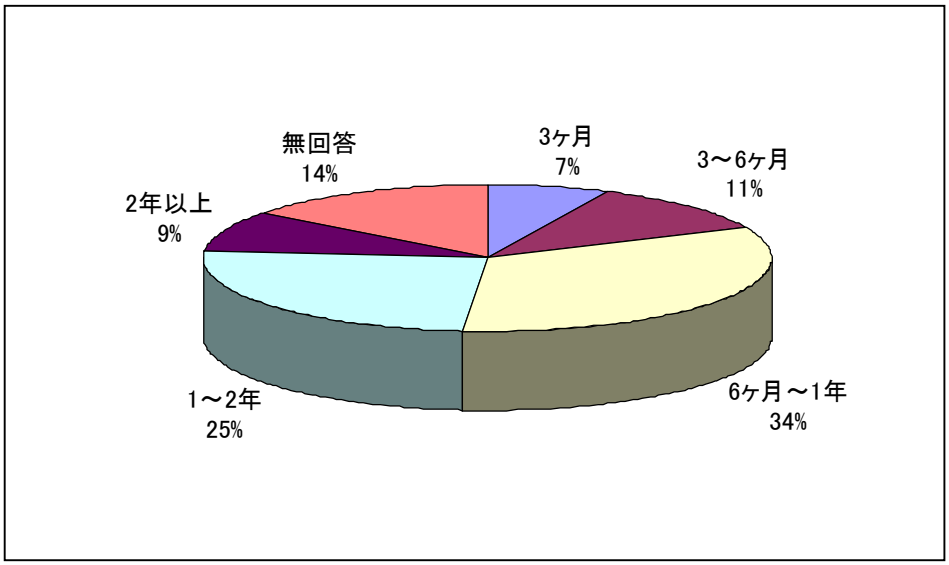


図 2.11 BCP・BCM の策定期間

③BCP・BCM の策定予算

BCP・BCM を「実施している」「策定中」「検討中」と回答した参加者のうち、「1,000 万円～5,000 万円未満」が 18%、「500 万円～1,000 万円未満」が 16%であった。尚、企業が BCP・BCM を実施している（含　策定中、検討中）とは知っていても、どのくらいの予算がかけられているのかは不明とした人は、36%にあたる。BCP・BCM にどこまで投資すれば良いのかは難しい問題である。経営者は、様々な投資案件、償却案件等あるなかで、リスクが顕在化した時のインパクトをある程度経済的な価値で表さなければ、BCP・BCM を構築するための投資判断は困難であるといえよう。

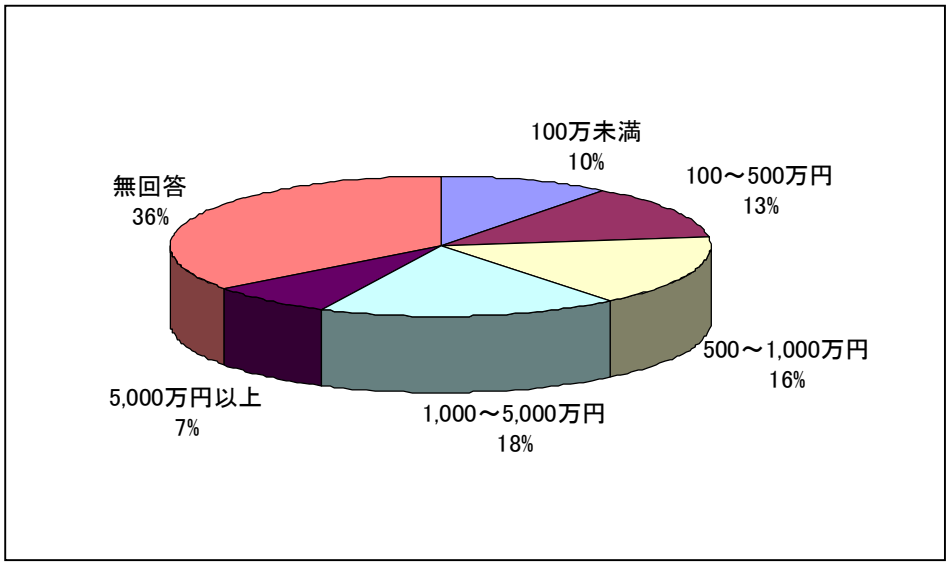


図 2.12 BCP・BCM の策定予算

④BCP・BCM の対象組織（社内組織）

BCP・BCM を「実施している」「策定中」「検討中」と回答した参加者のうち、「全社」を対象としているとの回答が 47%で最も多く、ついで「基幹事業に関わる部分」26%であった。

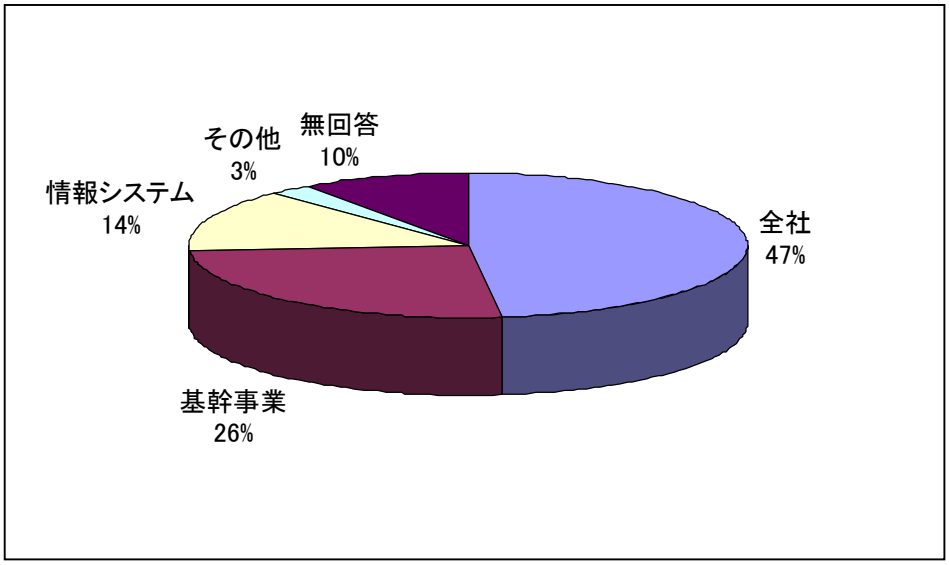


図 2.13 BCP・BCM の対象組織（社内組織）

⑤BCP・BCM の対象組織（社外組織）

BCP・BCM を「実施している」「策定中」「検討中」と回答した参加者のうち、「自社のみ」と回答したのは 39%、「連結対象会社を含む」が 30%であった。

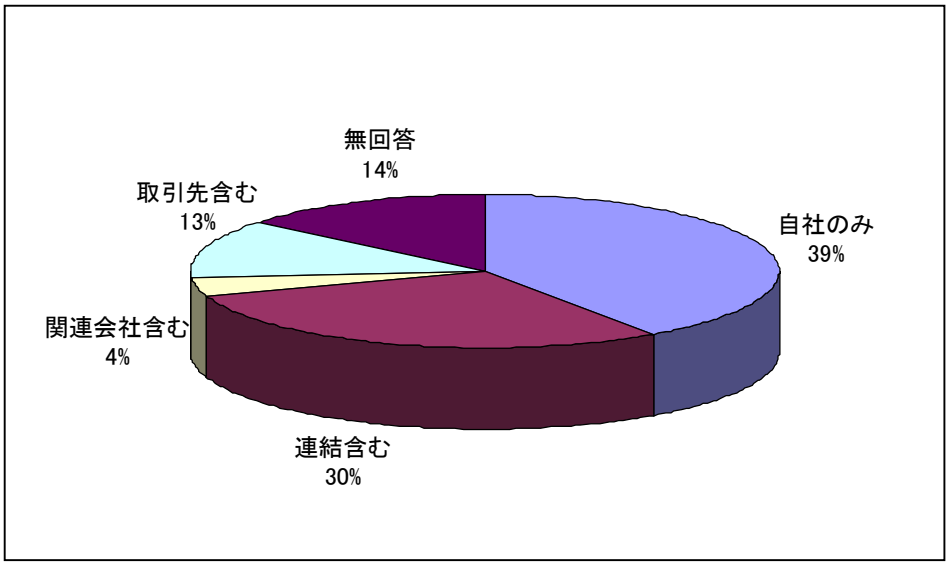


図 2.14 BCP・BCM の対象組織（社外組織）

⑥BCP・BCM を策定する目的

BCP・BCM を「実施している」「策定中」「検討中」と回答した参加者のうち、BCP・BCM を策定する目的として「企存続のため」を選択したものが 18%と最も多く、ついで「ISMS の一環」が 17%、「社会的責任(CSR)」14%、「防災対策」13%、「顧客サービスの向上のため」「企業価値向上のため」各 9%となっている。

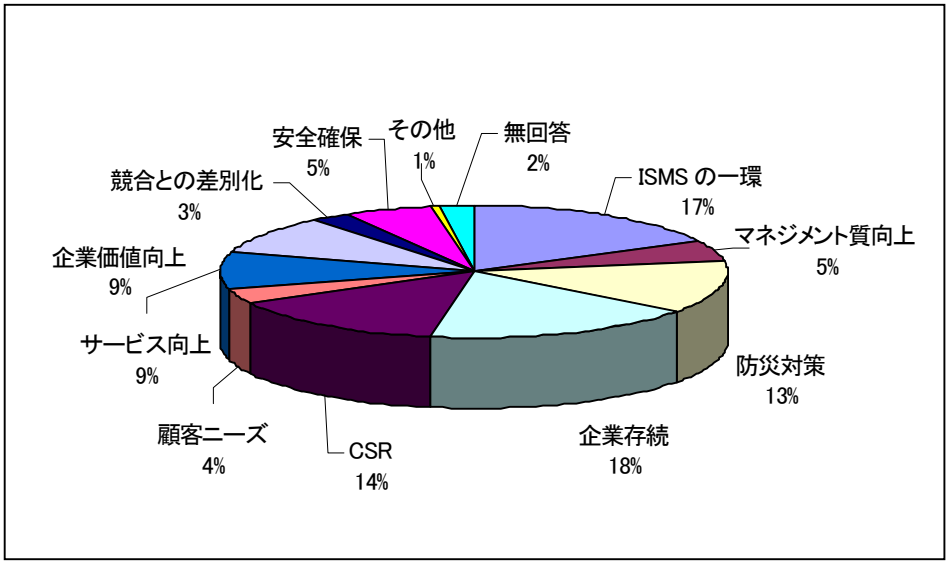
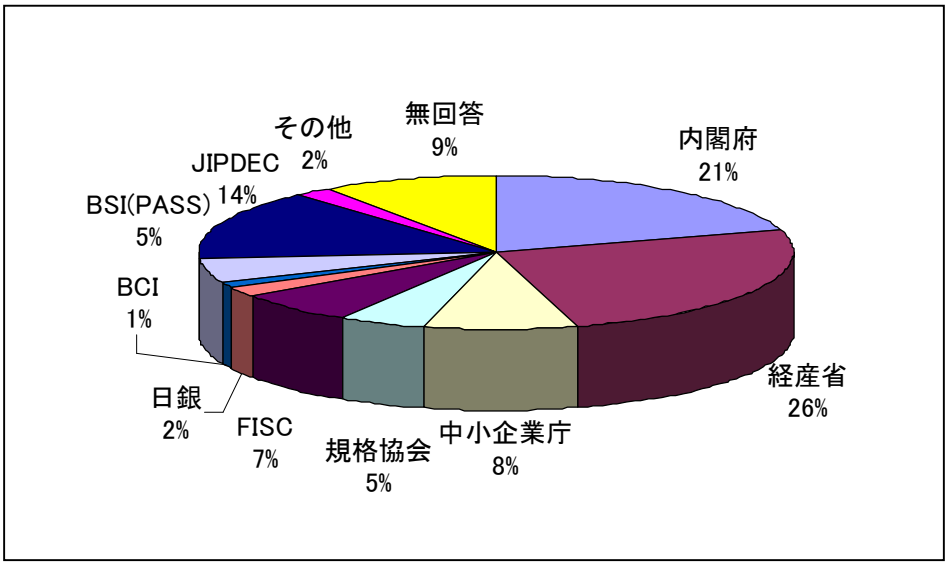


図 2.15 BCP・BCM を策定する目的

⑦BCP・BCM を策定するにあたり参考にしたガイドライン

BCP・BCM を「実施している」「策定中」「検討中」と回答した参加者のうち、BCP・BCM を策定するにあたり参考にしたガイドラインで最も多かったのは「経済産業省　事業継続計画策定ガイドライン」の 26%で、ついで「内閣府　事業継続ガイドライン」(第一版) 21%、「JIPDEC 事業継続管理に関する利用ガイド」14%となっている。

また、いずれかのガイドラインを参考にしたと答えた参加者のうち、73%が複数のガイドラインを参考にしている。



その他の例：
東証 BCP（2 名）　他社 BCP（2 名）
コンサルからのサンプル（1 名）

図 2.16 BCP・BCM を策定するにあたり参考としたガイドライン

⑧BCP・BCM の訓練の実施

BCP・BCM を「実施している」と回答した参加者のうち、訓練も「実施している」と回答したのは 69%、「実施していない」は 9%だった。

前年度のシンポジウム開催時のアンケート結果と比較すると、「実施していない」が激減し、「実施している」が大幅に増えているのがわかる。この結果から、BCP・BCM に対する意識の高まりがうかがえる。

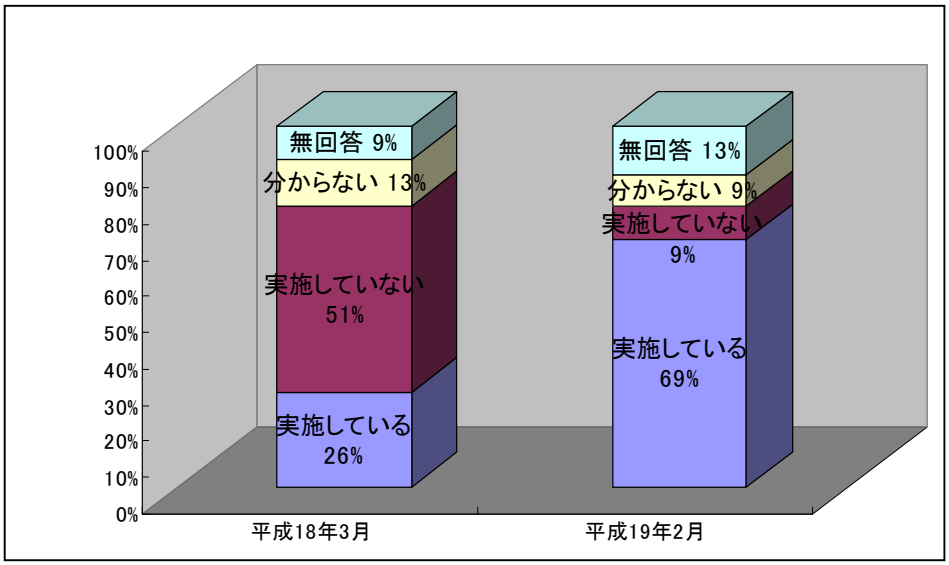


図 2.17 BCP・BCM の訓練の実施

⑨現在最も課題の多いフェーズ

BCP・BCM を「実施している」と回答した参加者のうち、BCP・BCM のＰＤＣＡサイクルにおいて現在最も課題が多いと考えているのは「Ｃ（点検）」のフェーズ 27%、「Ａ（改善）」のフェーズ 21%となっている。

このことは、事業継続計画が最新の情報を取り入れた効果的なものであることを確実にするための定期的な試験、またその試験結果の見直しを通じて問題点を改善していくことの困難さを示唆している。

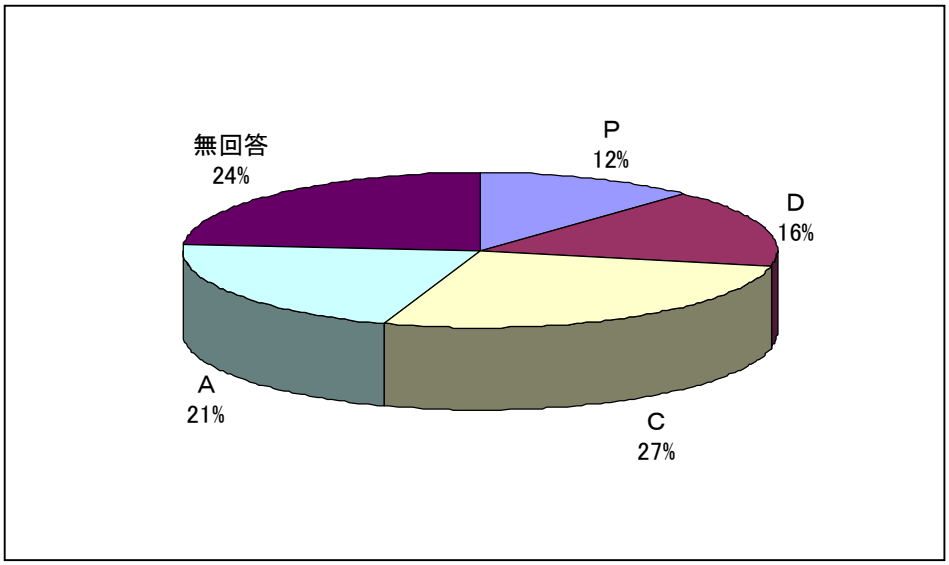


図 2.18 現在最も課題の多いフェーズ

⑩BCP・BCM の今後の取組み

BCP・BCM を「実施している」と回答した参加者が今後の取組みをどのようにしたいと考えているかについての質問には、「もっと向上させる必要がある」と回答した参加者が 57%、逆に「もっと簡略化した方が良い」としたのは 7%であった。

「もっと向上させる必要がある」と考える理由として、「全社へ広げていきたい・浸透させたいから」「経験が浅いから」「訓練が足りないから」という意見があり、各企業において BCP・BCM の本格的な取組みへの準備が整いつつはあるものの、「まだまだこれからだ」という段階にあるといえる。

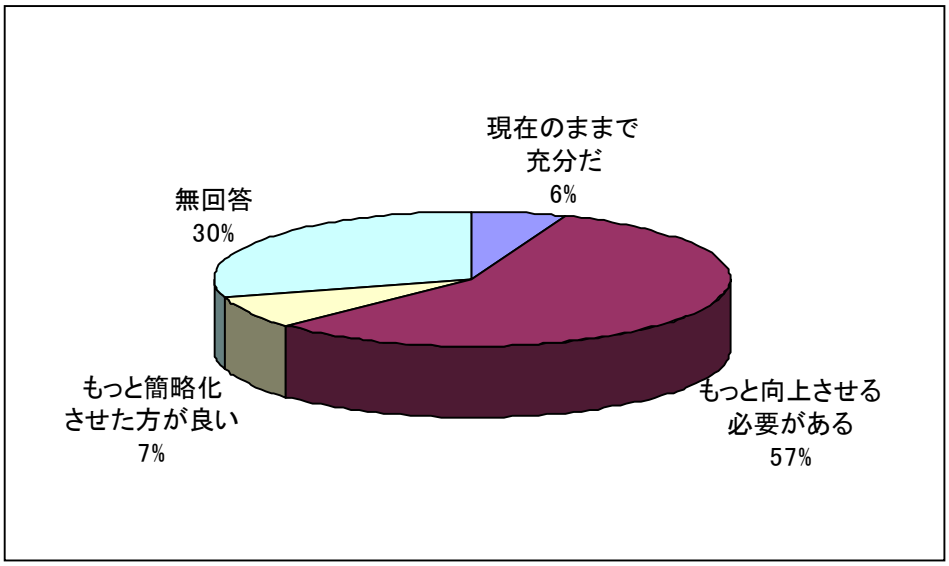


図 2.19 BCP・BCM の今後の取組み

⑪BCP・BCM の取組みにおける障害

BCP・BCM を実施しているとの回答のうち、現在の取組みを一段昇華させるにあたっての障害は、「BCP・BCM そのものの基本的情報不足」「人材不足」がともに 16%で最も多く、ついで「予算不足」13%となっている。

「基本的情報不足」は、今回のようなシンポジウム等を有効に活用することによって解決の一助になればよいと考える。また、「人材不足」については、経済産業省等が実施する人材育成の各種プロジェクトへの積極的参加により解消されることを期待するものである。

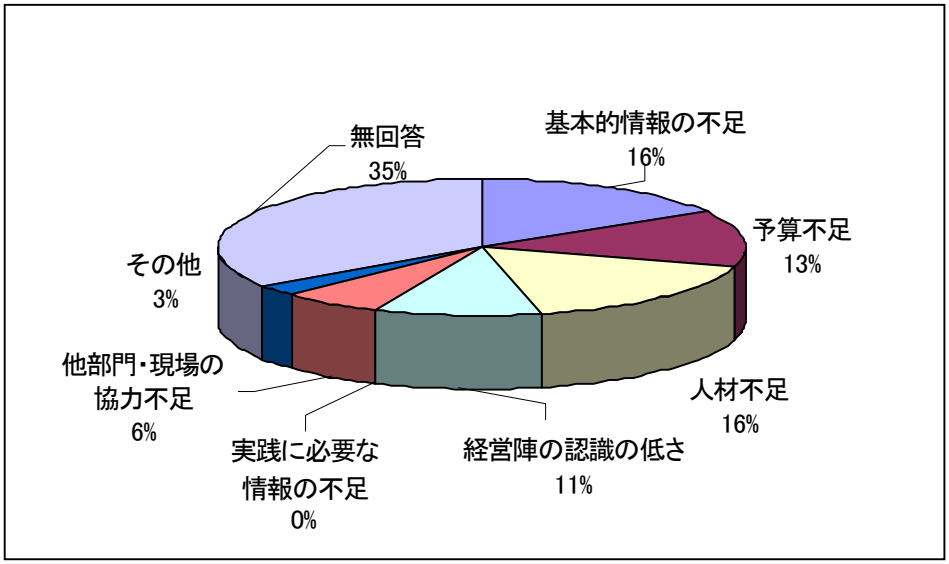


図 2.20 BCP・BCM の取組みにおける障害

(4) 内部統制について

①内部統制の実施状況

「策定中」が最も多く 32%となっている。

これは、金融商品取引法が 2009 年(平成 21 年)3 月期の本決算から上場企業およびその連結子会社を対象に適用となることを受けての動きと考えられる。(⑥の策定目的の回答からもこの傾向が見て取れる。)

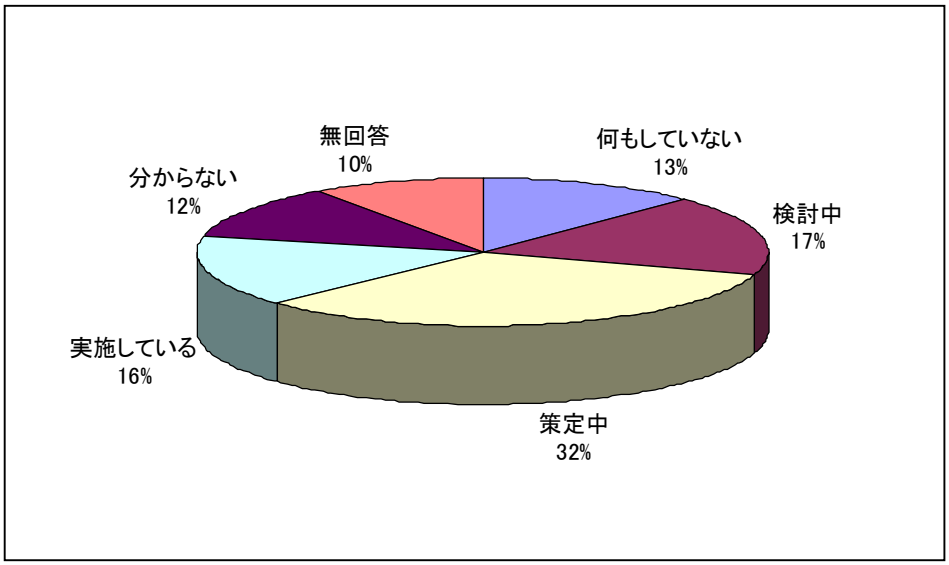


図 2.21 BCP・BCM の取組みにおける障害

②内部統制の策定期間

内部統制を「検討中」「策定中」「実施している」と回答した参加者に、策定にかかった期間（かける予定の期間）について質問したところ、「1 年～2 年」と「6 ヶ月～1 年」がほぼ同比という結果になった。

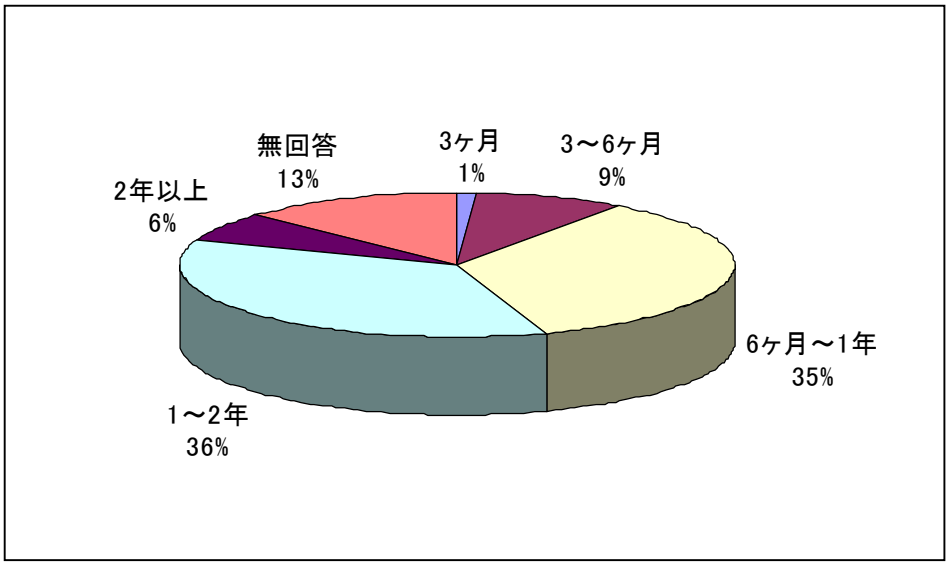


図 2.22 内部統制の策定期間

③内部統制の策定予算

内部統制を「検討中」「策定中」「実施している」と回答した参加者を対象に、策定の為に計上された（される予定の）予算について質問したところ、「1,000～5,000 万円」が 24%と最も多い結果となった。また、「無回答」の中には「予算については知らない、分からない」という回答も多く見られた。

計上された予算については、雑誌などに記載される値と比較すると安価なものであった。

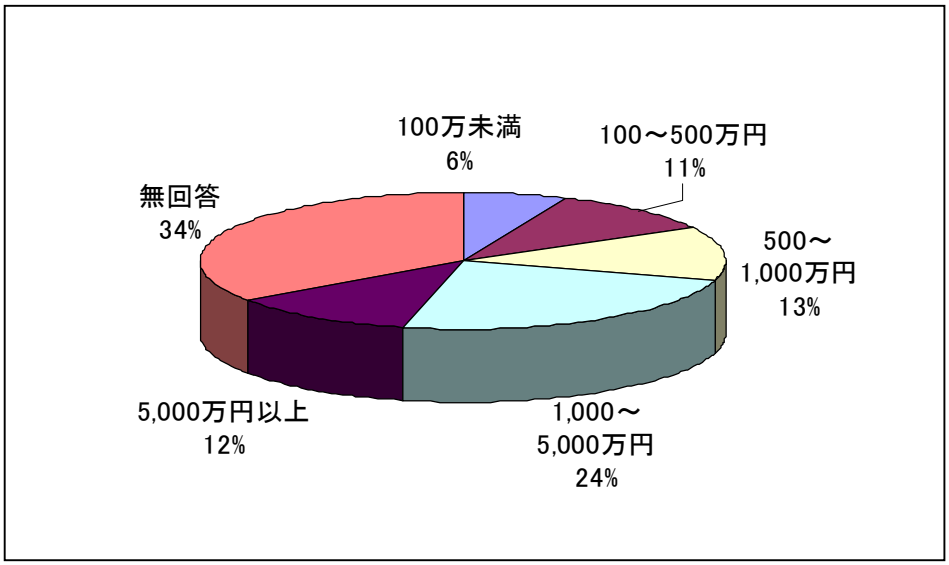


図 2.23 内部統制の策定予算

④内部統制の対象組織（社内組織）

内部統制を「検討中」「策定中」「実施している」と回答した参加者のうち、社内対象組織については「全社」との回答が最も多く、過半数（52%）を占めた。

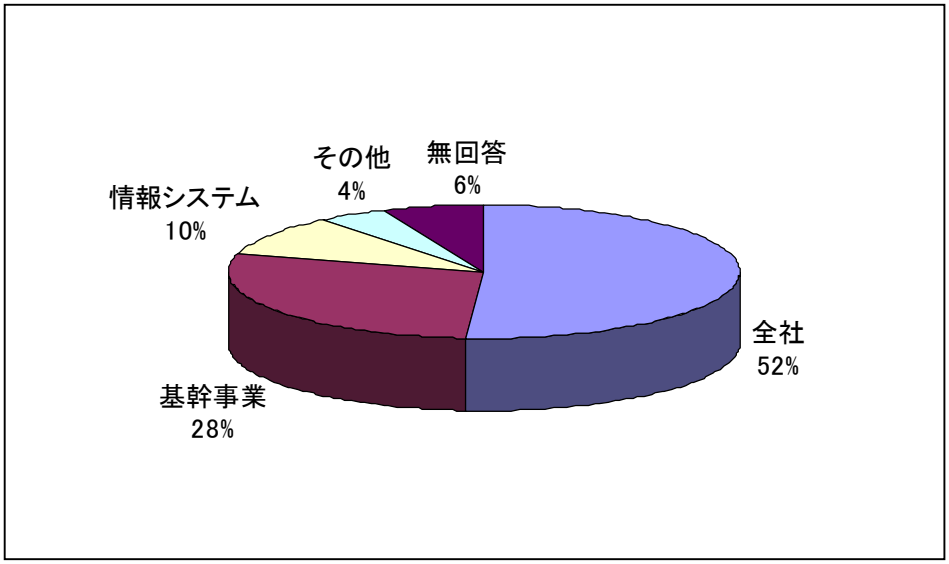


図 2.24 内部統制の対象組織（社内組織）

⑤内部統制の対象組織（社外組織を含む）

内部統制を「検討中」「策定中」「実施している」と回答した参加者のうち、社外対象組織については「連結対象会社を含む」との回答が最も多く、56%を占めた。

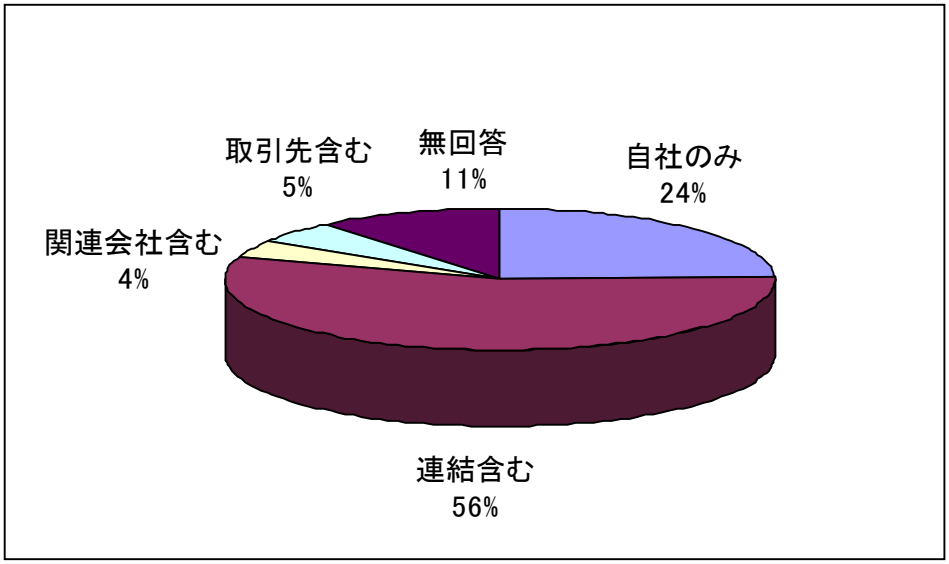


図 2.25 内部統制の対象組織（社外組織を含む）

⑥内部統制を策定する目的

内部統制を「検討中」「策定中」「実施している」と回答した参加者の、策定する目的は「日本版 SOX 法（J-SOX 法）対応」が 27%で最も多く、「社会的責任(CSR)」17%、「企業価値の向上」「マネジメントの質の向上」各 12%と続いている。

①同様、再来年度から適用となる、金融商品取引法を意識しての回答と考察される。

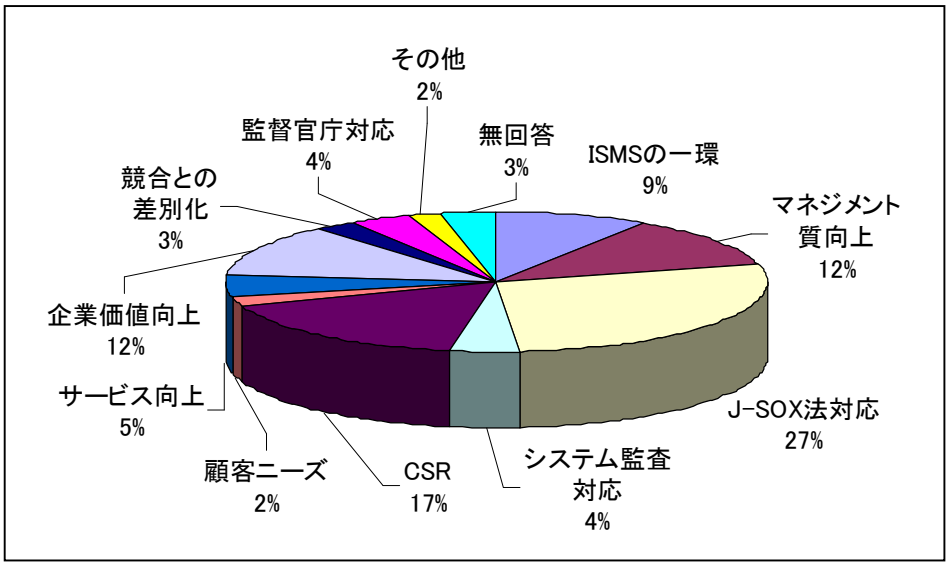


図 2.26 内部統制を策定する目的

(5) その他

①今後の「情報セキュリティ総合的普及啓発シンポジウム」の開催

「期待する」が 77%となり、多くの参加者が今後のシンポジウムの開催を期待しているものと考えられる。

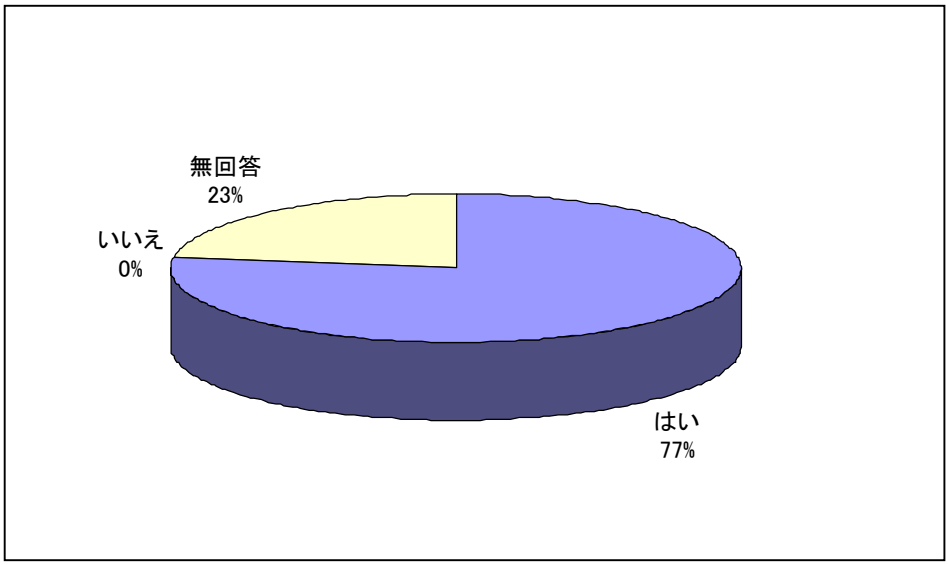


図 2.27 今後のシンポジウム開催について

②今後取り上げて欲しいテーマ

参加者から挙げられた今後取り上げて欲しいテーマは以下のとおりとなっている。

- BCP・BCM（策定及び構築事例、最新動向）
- 統合的マネジメント（BCM、QMS、EMS、ISMS　etc…）
- ISO20000
- ISO27001
- ISO27000 シリーズ
- 内部統制
- J-SOX
- フォレンジック
- 情報セキュリティ監査
- システム監査
- SAS70
- ITIL
- IT ガバナンス
- BS25999
- 個人情報保護
- リスクマネジメントと有効性評価

- リスクアセスメント手順、脅威・脆弱性の対応と対策
- 有効性指標の考え方
- マネジメントではない技術的なテーマ
- 情報セキュリティ関連法制度の説明、コンプライアンス
- セキュリティ人材育成
- ディザスタリカバリ
- 企業内情報管理
- ネットワークセキュリティの最新動向

③その他の意見

「その他、ご意見をお聞かせ下さい」という問いに対し、参加者から寄せられた意見には、開催会場、講演の構成等について等、今後の開催において考慮すべき点を指摘したものがあった。

- 会場に規制が多く、面倒すぎる。（入退場の際の規制、飲食物が持ち込めないことなど）警備員の態度も不快だ。
- 聞きたいセッションだけに参加できるように、各セッションの前後に 5 分程度出入りの時間を設けて欲しい。
- 2 日間のプログラムは長すぎる。テーマ毎に数回に分散して開催して欲しい。（2 日間の講演テーマの中には、今回のテーマにそぐわないものも含まれているように思う。）
- 説明が重複している。講師間の連携を取って欲しい。
- 資料をインターネット公開して欲しい。（本シンポジウムの趣旨(啓発)を鑑み）
- 講演の冒頭の写真撮影は、集中力を欠くので控えて欲しい。
- 場所柄、昼食時は混雑するので時間帯をずらして欲しい。
- 内容が盛りだくさんなのは良いが、1 つ 1 つが短すぎるのが残念だ。

また、以下のような意見も寄せられた。

- システム監査の法的規制を確立して欲しい。
- 広く一般国民に認知させるために、誰にでも分かる日本語を使うようにして欲しい。
- ISMS の審査機関は審査が甘すぎる（ISO27001 になってより一層甘くなったと思う。）ので、先日のおかしメーカーF 社のようにならないためにも、審査のあり方について見直しをして欲しい。

3. 事業継続の実際と今後の課題

3.1 IT ガバナンス時代のセキュリティオペレーション

3.1.1 はじめに

ＪＳＯＸ法対策とはストレートに結びつきませんが、セキュリティオペレーションは IT ガバナンスに必須である、情報セキュリティ対策の中核となるという観点でお話をさせていただきます。

まず、簡単にＪＳＯＣの紹介をさせていただきます。ＪＳＯＣはジャパンセキュリティオペレーションセンターと言いまして、株式会社ラックが営利目的で運営している監視センターです。ＪＳＯＣは、顧客に対するサイバー攻撃やセキュリティ上の事件などを見つけ対応するだけではなく、セキュリティに関連した様々な情報も収集しております。それらの情報をラックの研究機関であるコンピュータセキュリティ研究所（ＣＳＬ）とも協調して分析、結果、傾向分析レポートや、キャッチした様々な脅威に対抗する為の注意喚起などを広く公開することなどを通して、社会貢献を行っております。

3.1.2 IT 活用レベル

元来、情報セキュリティというものは、ＩＴ活用ありきであって、それを安全に安心して使用する手段の一つとして存在するものだと思います。その為、セキュリティを語る上で、そもそも、ＩＴをどの程度どんな目的で使用しているのか、或いは使用していくつもりなのかを理解することが重要なポイントとなります。

そこで、よくメディアなどでも、「社会生活に必須となったＩＴ。よって、どこの組織もセキュリティは必須」などとよく言われていますが、それは本当だろうかということから入っていきたいと思います。

まず、ＩＴをどういう目的で活用しているかということなのですが、まず一つ目には「そろばん」という目的で括っておりますが、例えば、電卓や電話或いは机の代わりなど、基本的には個人の能力増強の目的でＩＴ活用を行っているレベルがあります。 現状では、パソコンを駆使することになるわけですが、表計算やワープロソフトを活用し、様々なドキュメントを作成する。ホームページを検索し様々な情報を収集、メールを駆使して仕事を行う。そういったレベルを「そろばん」と括ってみました。ＩＴの活用レベルとしてはそれほど高くないのですが、それでもメールがないと仕事にならない世の中ですから、このレベルはこのレベルでの統制を行う必要があります。 今後、ＩＴが浸透していっても、やはり５割くらいの企業や人は、このレベルなのかも知れないと思います。 恐らく、中小企業の大半や上場企業の一部も、このレベルに当てはまるのではないかと思います。

次に、「合理化」のためにＩＴシステムを使用するものです。例えば販売管理システム、生産

管理システム或いは会計システムなどを活用するものです。いわゆる基幹システムといわれているようなシステムです。こういった活用レベルは、合理化や、従来のビジネスプロセスの代替とすることが多く、また、多くの企業で企業の基本活動を支えており、システムが止まると仕事も止まってしまう危険性も高くなっています。

昨今、特にＪＳＯＸ法が問うているのは、会計システムや会計を取り巻く営業や購買などの企業の数字を司るシステムの正当性などです。企業の財務報告が、正しいこと。 例えば、改竄（かいざん）を防ぎ、報告内容の信憑（しんぴょう）性をいかに証明していくかということが求められています。その為、このレベルでＩＴを使用している組織は、システムの統制を行うことが必須となるわけです。 また、「そろばん」レベルと同様に、このレベルでＩＴを活用していく組織や個人は今後も、３割くらいはあるのではないかと考えています。現状、多くの上場企業や行政機関、地方自治体などの公共団体などはこのレベルと考えます。

最後は、ＩＴそのものが収益基盤やビジネスモデルを形成するような活用レベルとなります。例えば、コマースサイトなどは、このレベルになると思います。また、安全をＩＴで支えているようなモデルもこのレベルに該当するでしょう。こういった活用レベルは、今後、我々が新しい社会モデルに適応する上でも、政府が推進している我々の生産性を高める上でも、目指すべきレベルかと思います。

金融はずいぶん以前からＩＴがビジネスを支えていたわけですし、ＡＳＰ事業者やネットでビジネスをやられている方は当然ですし、今後益々増えていくことが予想されるｅ-ＸＸＸというのは、まさしくこのレベルを具現化するものと思います。

我々はもっとＩＴを活用していかなくてはいけない。活用して本当にその企業活動とかにインパクトを与えるまで、ＩＴというのを本来は使いこなしていかなくてはいけないのだと思います。しかしながら、多くの日本企業では、ＩＴをそこまで信用していないので、そこまでのＩＴ統制は必要ないというのが本音かもしれません。多くの人が、なんとなく危ないと思っているので、実はそこまで使いこなしていないという後ろ向きの統制が実はかかっているのかもしれません。しかし、今我々は一歩踏み出していかなくてはいけない時代に来ているのだろうと思います。

ＩＴの支える範囲が広がり、進化している現在、もうお分かりだと思うのですが、ほとんど管理限界を超えつつあると感じている方も多いのではないでしょうか。例えば、ある銀行のシステム担当の方が、最近はシステムがスパゲッティになっていると仰っていましたが。 私は昔プログラマーでした。当時、スパゲッティプログラムを書いてはいけない。そういうグシャグシャなプログラムを書くと、後で保守などができないのでダメです、と教え込まれたものです。最近もそういうプログラムは当然作ってはいけないし、開発環境により作りたくても作ることが出来ないようになっているのですが、逆にプログラムを組み合わせたシステムがスパゲティになっている。例えば、かなり以前より、オブジェクト志向を取り入れた、開発手法が主流になっているようです。頭のいい方がしっかり設計をしているうちは良いのですが、保守に入った瞬間その文化･思想が継承されずにグシャグシャになってしまうことが見受けられます。結果、見事なスパゲッティシステムが出来上がり、スパゲッティプログラムより、はるかに危険で大きなクラッシュを引き起こし、リカバリーにも時間がかかってしまうというようなことが起きています。 こういった問

題は、特に運用で、統制が効かなくなったところで発生していることが多いようです。 ある面、現状はＩＴリスクを管理するどころか、ＩＴリスクが爆発しそうだというのが、先端のところでやられている方の危機感ではないかと思います。これはある意味、情報（リスク）ビッグバンともいえるのかもしれませんが、我々はこれを乗り越えていかなくてはいけないと思います。

あらゆる面で、我々はＩＴの活用レベルをさらに上がらないといけないのは、現時点においては間違っていないと思います。昔、自動車で公害問題やオイルショックが起きたときに、エンジン周りで大きな技術革新が図られ、その上でさらなる発展を遂げ、現在の自動車社会が形成されているように思います。そう考えると、現在、知的生産性に関して欧米諸国に劣るといわれていますが、我々は情報ビックバンをいち早く乗り越え、対抗していくことが重要に思います。そう考えますと、現在言われているＩＴ統制や、情報セキュリティというのを真面目にやっていかなくてはいけない時代に入って来たと感じています。

3.1.3 二つのセキュリティ対策

情報セキュリティとは直接関係のない話題ですが、いじめ問題があります。最近、いじめが原因と見られる自殺などが多発して、社会問題となっていますが、その際、両親や校長先生などの管理責任者側は「ＳＯＳを出していたけれど誰も気が付かなかった。」「そんな大きな問題に発展するとは思わなかった。」などのコメントを耳にすることが多いです。

私は、教育の専門家では無く、門外漢ではありますが、責任者側の初動対応が、まずいなあと思うことが良くあります。こういう問題の、根本原因の一つとしては、「いじめが存在していること自体が問題」という風潮があります。見つけると評価が下がるわけですから、この結果、いじめを見つけて対策するということが評価されないし、そもそもいじめを見つけることが出来ないし、見えないという事態、つまり見て見ぬふりが起きることになります。

私ごとで恐縮でございますが、先週の日曜日、車で出かけたところ、国道 15 号線が封鎖されておりました。これは一体何が起きているのですかと聞いたら、「知らないのですか。マラソンです」と言われました。よくよく見てみると、至るところにチラシなどで、何月何日はマラソンがありますと書いてあるのですが、私は全く気がついていませんでした。全く見えないのです。私とは関係ないと思っていまして、興味がないと、もともと気付きようもなく、見えなくなってくるのです。こういったものを見るためには、根本的に問題の原点に帰って行かないといけません。単にオペレーションだけをやっていると、こういった問題は見えてこないし、これは情報の社会においても同様だと思っております。

当事者の方は、「対策をとってきています。」「教師にはこういう指導をしていたのです」などとおっしゃるのですが、対策には正直言って、「形式的な対策」と「本質的、戦略的な対策」の二つがあるのです。「形式的な対策」というのは、例えば、「指示はしていたのですけれど」や「マニュアルはあるのですけれど」などの言い訳が出てくるので、事件が起こったときに良く分かります。かくいう私も、トラブルが発生してしまったときに、お客様にそういう言い訳をしてしまうことはよくあるのですが、こういう二つの対策があるということを分かっていることが大切だと思います。

通常「形式な対策」で許される場合というのは、例えば、他に真犯人がいる、人命に影響がない、社会的責任をとる必要がないなどだと思います。ただ、いじめや、統制といったことは「形式的な対策」では本来済まないのだろうと思います。

3.1.4 セキュリティ対策動機

次に、対策を行う動機というのを少し考えてみます。対策を行う動機で、一番初めに出てくることは、例えば個人情報保護対策やＪＳＯＸ対策でもそうですが、「法律で決まったから」、「取引先から言われて」などです。次に考えられる動機は、「守るべきものが私たちにはあるのだ。だから対策をするのだ」さらに「社会的責任でやるのだ」という場合の二つが存在しています。

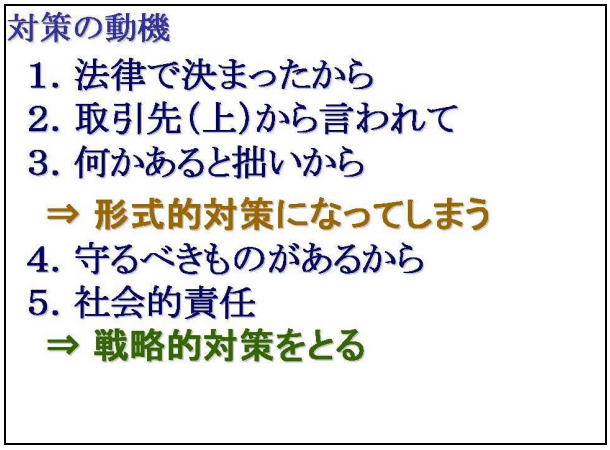


図 3.1　セキュリティ対策の動機

これからいくと、前者は「形式的な対策」にどうしてもなってしまいます。法律が決まったら法律を守ればいいのだ、上から言われたら言われたことをやっていればいいのだというのが対策になってしまいます。後者の、守るべきものがあるとか、責任上やるのだというようなことになると、アプローチとして「戦略的な対策」を本能的にとっていきます。

3.1.5 セキュリティ対策はどこまでやれば良いのか

「対策はどこまでやればいいのか。」ということを良く耳にします。この解には、先に説明した「ＩＴの活用レベル」は重要なパラメータとなります。「そろばん」レベル、「合理化」レベル、「収益基盤」レベルの、ＩＴ活用レベルは、はずすことが出来ません。これは現状だけではなく、今後のＩＴ活用レベルの戦略も含まれます。次のパラメータが、セキュリティ対策動機です。 この二つで考えていくというのは非常に実は大きなポイントです。

ある面、うちは「そろばん」なので、上から言われたので、最低限やるべきことをやればいいという判断は、それはそれで正直正しいと思います。

3.1.6 最近のセキュリティトレンド

図 3.2　200X 年のネット犯罪関係の特徴

２００X年のネット犯罪関係の特徴を三つのキーワードで表現してみました。

狡猾（Shifty）、見えない（Stealth）、標的型（Snipe）の３Ｓです。最近の傾向は愉快犯的な犯罪から、いわゆる金銭目的に代表される、目的志向型の犯罪に変わってきたというのが特徴になっています。

一応、念のためにお話をしておきますが、犯罪というと、「悪いのは犯罪者であるから、我々が対策する必要は無いのではないか」と考える方もいらっしゃると思います。 冷静に考えてみると、犯罪対策をなぜ民間の我々がわざわざお金を出してやらなくてはいけないのだ、「それは国がやるべきだろう」とか、「ＩＳＰとかそういう業者がやるべきだよ」などと、社会的インフラを担っているところに押し付けたいこともあろうかと思います。しかし、今の状況で少なくともＩＴを徹底的に活用していこうとすると、やはり、物理的な世界と違って、例えばネット社会を形成している「情報」の窃盗が法律上成立しないなど、物理世界とは似てはいるが異なることも多いため、単純にはいきません。また、犯罪者にやめてくれと言っても、国も文化も常識も異なる人々に対しては無力なことも多いのです。もちろん、言うことは重要ですが、言っても国境を越えてやってきます。同時に、匿名性も強いので物理社会では抑止がかかっていたものが、日本人であっても従来の常識では図れない行動を取ることもあります。また、コンピュータウイルスのアウトブレイクのようなものは、人間が起こす犯罪というよりむしろ、大規模であるがゆえに、災害のように、統計的・確率的に発生しているような側面もありますので、受けた被害に対して単に犯罪者が悪いというようにはいかないと思います。 ですので、ネット犯罪と聞いて、それは関係ないとはすぐに思わないで、我々自分たちの問題だととらえていく必要があると思います。

3.1.7 最近発生している事件の二つの特徴

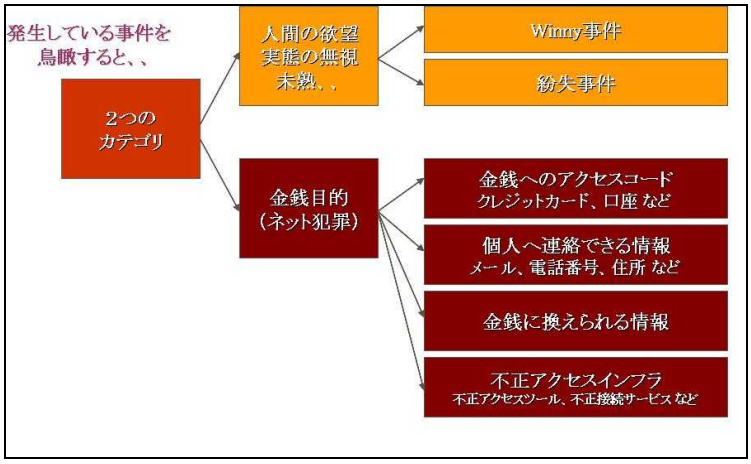


図 3.3　最近発生している事件の二つの特徴

次に、最近発生している事件をみてみます。 大きく二つの特徴があります。一つは人間の欲望であるとか、実態を無視したセキュリティ対策などの無理な運用や未熟などが原因となっている事件と金銭目的で発生していると考えられる事件です。

前者の代表的なものが、Ｗｉｎｎｙに関連した情報漏えい事件です。これはＷｉｎｎｙを使う理由が分かっていないと､Ｗｉｎｎｙを媒体としたウイルスに感染する理由は理解できませんし、対策の施しようもありません。なぜならば、使用理由が人間の欲望に根差したところもあり、さらにパソコン関係の知識もそれなりにある人が対象となっているからです。 ある面、Ｗｉｎｎｙユーザは偶然使用しているのではなく、ある意図を持っているということで、つまり動機がしっかりしているところになります。 よって、禁止するにしてもその背景を分かってないと、形式だけの対策になってしまい、結果、事故を防止できないことになります。

二つ目のカテゴリーは、金銭目的です。しかし、金銭目的というと多くの方は、うちは無関係と捉える人が多いかと思います。なぜならば、クレジットカードなどの金銭に関係する情報を扱っているわけではないし、うちの情報など盗っても仕方がないだろうと短絡的に思ってしまうからではないでしょうか。しかし、何がお金になるか、我々には分からない時代になっているのです。情報の価値は自分たちで決めるだけではだめです。 犯罪者側から見て価値があるかどうかがポイントなのです。

3.1.8 金銭目的で対象となる情報

金銭に関係する情報はいくつか考えられます。最初に考えられる情報は、「金銭へアクセスできる情報」です。クレジットカード情報や口座情報などが当てはまり、誰が見ても金銭に換えられると理解できると思います。

２番目は、「個人へ連絡できる情報」です。住所氏名が全部そろっていなくても、例えばメールアドレスだけでも金銭に換えられる可能性があります。 例えば、健康食品業者に問い合わせを

した人のメールアドレスです。これはこれだけで買いたいと思う人がいそうです。 メールアドレスではなく、電話番号、或いは住所だけでも可能性があるかもしれません。そうなると、これは個人情報法保護法に代表される法律を守れば良いとは一言では片付けられない問題を内包しているといわざるを得ないです。

３番目は、「金銭に換えられる情報」です。例えば、お役所での丸秘の判子がついた書類や、有名企業の次期研究開発にかかわる丸秘がついた報告書などです。さらに、公開前のＩＲ情報（インサイダー情報）や他社が真似できない独自技術なども可能性があります。 こういった情報は、買わないかと持ちかければ、買う人が出る可能性があるからです。

最後は、不正アクセスをするための道具や関連する情報などです。 要するにピッキングツールです。 すぐに侵入可能なサーバのリストと侵入ツールの組み合わせや、大量のメールを出すことのできる踏み台のパソコンを抱えたボットネットなどは、買い手や借り手はあるでしょう。

3.1.9 金銭目的の犯罪へシフトしている理由

金銭目的の犯罪が起きる理由は、端的にいうとその市場があるからです。買い手がいるというのは大きなポイントかと思います。

ノートＰＣや電子媒体を拾った悪意のある人間の行動というのは、明らかに変わってきているというのはご存知だと思います。昔は、単純にＵＳＢメモリーを拾ったら、自分で使えるのだったら使い、パソコンを拾ったら中古ショップに販売する程度でしたが、物理的に売る前に、換金可能な情報が入っているかというのは、悪意のある人間だったら当然考えることです。当然のことながら盗んだ人間は拾った人間と異なり最初から悪意があります。ですから、パソコンを単に盗むというより、中の情報を狙っていると考えるのが妥当だと思います。有名企業や官庁などに勤めている人の個人パソコンは、その手の情報を集めている人から見れば魅力的に見えるでしょう。

さらに、実際にどの程度発生しているか私は情報を持っておりませんが、ショルダーハッキングというのが以前から話題になっています。これまでは企業内などでユーザＩＤとかパスワードを盗み見することで、よく肩越しにパソコンの画面を盗み見する手口です。これが、例えば、通勤途中や出張時の新幹線などで重要書類を見ている肩越しにデジカメや携帯カメラで写真を撮ってしまうようなことも起こるかも知れません。

昔は、誰が盗るのだ。盗っても処分ができない。その為、昔は、プロ以外手が出せなかったのではないだろうか。そんな市場を知っている人間は、所謂その筋の人達であったのではないかと思います。ところが、今は誰でもアクセスできる、ネットで売れてしまう。所謂真面目な人間と、国内外のその筋の人達とをつなぐグレーとかブラック市場というのが、テクノロジーによって拡散し、進行しているということが、ポイントかと思います。 昔から、情報や新技術は、人のために役立てる前に、逆に悪用されてしまうことも多々あったように思います。特に情報は正規の利用方法より、犯罪などへの悪用のほうが、価値がはっきりしており、浸透が早いように思います。技術が本来狙っていることとは逆転しているようなことが、残念ながらあるのかもしれないのです。

3.1.10 脅威の点と線

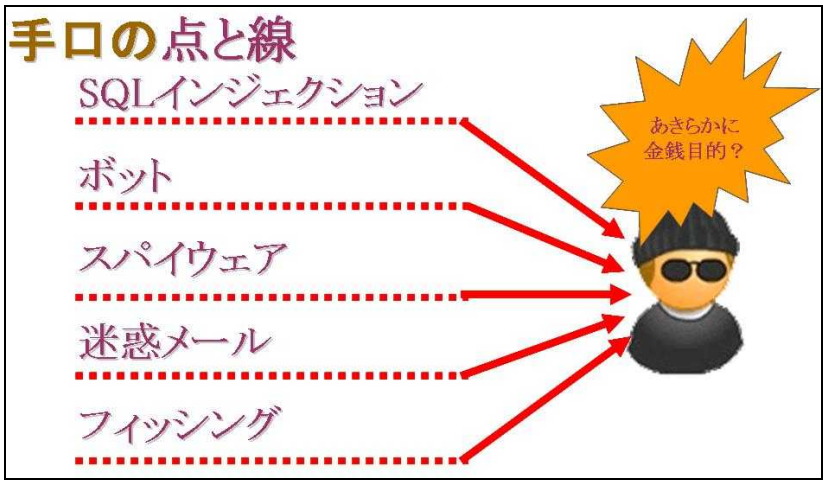


図 3.4　脅威の点と線

ＳＱＬインジェクション、ボット、スパイウェア、迷惑メールやフィッシングなどと脅威となる手口や脅威が多々ありますが、こういった手口は点として単体で存在しているのではなく、線としてつながっているのではないかと推測しています。 どうして、こういうことが起きているのかという構造的な部分をある程度理解していくことが対策を進める上で必要だろうと思います。

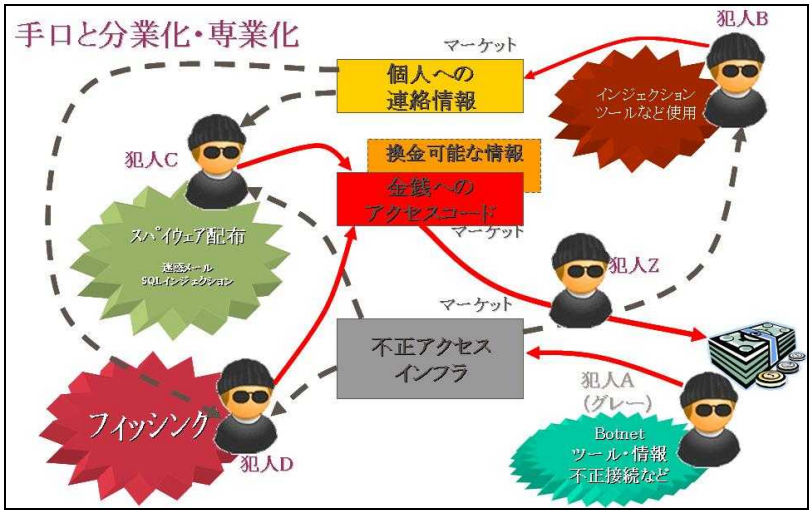


図 3.5　手口の分業化・専業化

犯人のＡは、ちょっとしたマニアで、いろいろなハッキングツールなどを作るのが得意な人。こういった人はハッキングをする上での手ほどきや、侵入ツールなどを売っていくわけです。次にＢはＡから侵入ツール等を購入し、実際にサーバなどに侵入して、個人情報を盗んで売ります。さらにＣは、個人情報とスパイウェアを購入して、金銭のアクセス情報を盗み売る。また、Ｄは個人情報とフィッシングサイト構築ツールを購入し、フィッシングを仕掛け金銭へのアクセス情

報を盗み売ります。

実は、ここまでの間は、金銭被害というのは出ていなくて、こういう悪い人たちの間で金銭のやり取りがされているだけです。最後にＺが、金銭へアクセス情報を入手し、本物のお金に換えていくことで、初めて実害が出る。こういうことが分業化・専業化され機能的に動いているのではないかと思われています。

3.1.11 見えなくなる脅威

こういった背景から、見つけようとしないと見えないのです。なぜなら、向こうは隠れようとしているわけです。見つからないようにしているわけです。

一昨年、ＳＱＬインジェクションなどの手口でホームページ（データ）が改ざんされ、その改ざんされたホームページにアクセスしたクライアントパソコンのウイルス対策ソフトが反応して改ざんの事実が判明したことがありました。ただし、全ての対策ソフトで反応するわけではなく、特定の対策ソフトで反応する。こういった事象から、犯人側は既存の有名な市販の対策ソフトで反応しないことを確認して、仕掛けているのではないかと推測されます。

そういう背景から、明確に見る意思がない限り見えない。 問題が起きないように対策していくのは当然重要なことですが、どうやって見つけますかということは、問題の防止策を検討する前に考えておくことかと思います。

3.1.12 Web アプリケーションの脆弱性

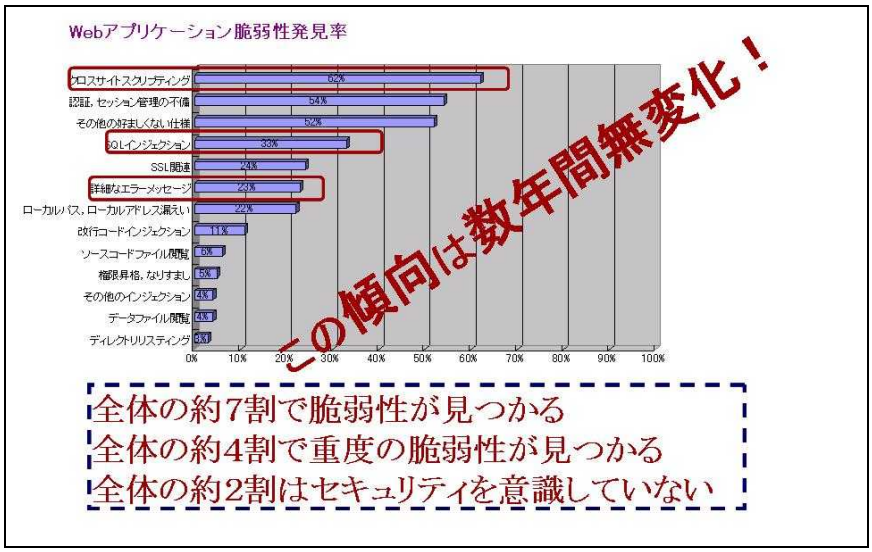


図 3.6　Web アプリケーションの脆弱性

こちらが当社で顧客から依頼されて実施したＷｅｂアプリケーション脆弱性診断においての、見つかった脆弱性の発見率です。私たちに依頼してきたお客さん全体の７割で何らかの脆弱性が見つかります。４割で重度な脆弱性見つかり、２割はセキュリティを意識して作成したとはとても考えられないレベルです。

各々の割合が大きいことも問題ですが、それより大きな問題は、この傾向は数年間変化していないということです。 セキュリティパッチを当てる等の、サーバやＯＳレベルの保守運用については、かなり洗練されてきています。ただ、このユーザが独自に作成するアプリケーションの部分というのは対策状況が基本的に変化していない。私たちがＷｅｂアプリケーションの脆弱性診断を開始した 2000 年から既に７年ほど経過していますが、本当に変化していないのです。同じお客さんでも基本的に変化しない。これがＷｅｂアプリケーションでのセキュリティ対策の大きな特徴かと思います。

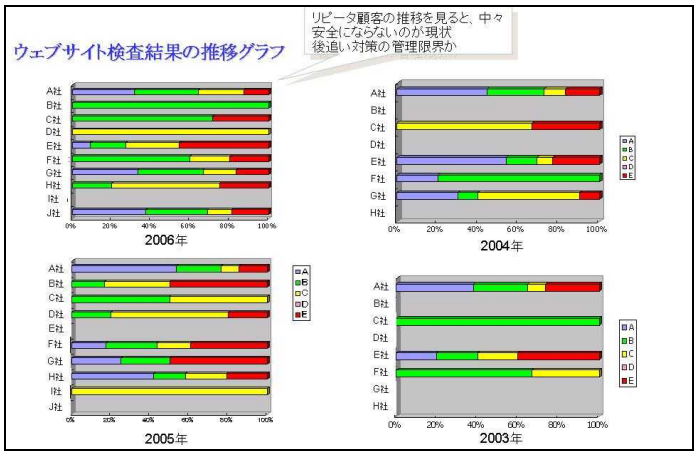


図 3.7　ウェブサイト検査結果の推移グラフ

これは、経年でやられている会社をいくつかトレースをしてみた図なのですが、例えばＡ社が 2003 年と 2004 年ではＥランクは少し減り、2005 年でも少し減りました。でも、その後、それ以上には減っていないのです。例えば、Ｄ社は、最初はかなり悪かったのですが非常に改善してきています。このＡ社とＤ社の違いというのは何かというと、サーバの台数の違いなのです。 20～30 台くらいまでのサーバがあれば、この後追いのセキュリティ、所謂、完成後に脆弱性を指摘し、もぐらたたき的に対策をやっても効果が出ているのですが、それ以上になると単純に後追いだけのセキュリティでは限界があることを物語っていると推測しています。それは、後追いセキュリティの管理限界と考えられ、１００％には到達できず、80 数％で頭打ちになってしまっている理由ではないかと考えています。それは、Ｗｅｂアプリケーションというのは日々変化する必要があるのです。営業に密着したようなシステムで採用されることが多いため、日々変化していかないと競合他社には勝てないのです。そういった中で、安全にし続けていくというのが如何に難しいことかということだと思います。 現実問題として現状では、最初からセキュリティをビルトインで考慮する体制というのは大半のところで築けていないと推測されるのです。

3.1.13 最近の JSOC での観測状況

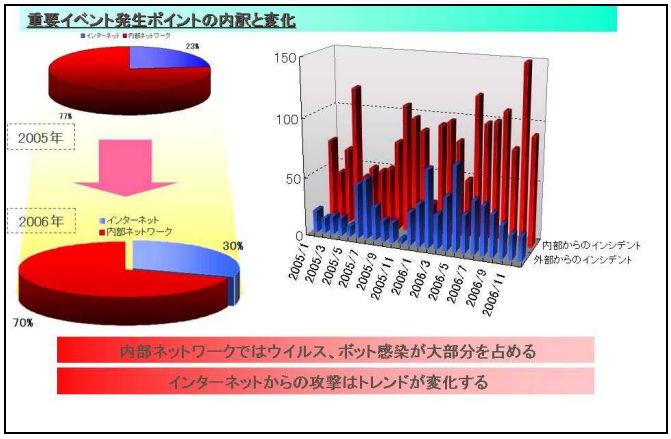


図 3.8　重要イベント発生ポイントの内訳と変化

ＪＳＯＣのほうで観測をした、2005 年と 2006 年での特徴をいくつかお話ししていきます。2005 年では、顧客が対応しなければなかった重要イベントで、インターネットからの攻撃が原因で発生したイベントは全体の 23%でした。イントラネット（内部ネットワーク）で、発生した重要イベントは全イベントの 77%でした。内部ネットワークでの重要イベントとは、ウイルスやボットの感染やＷｉｎｎｙなどの使用が禁止されているＰ２Ｐソフトの使用が大半です。昨年の特徴は、インターネットからの脅威で発生した重要インシデントが従来は減少していたのが増加に変化したことです。 増加理由は、Ｗｅｂアプリケーションの脆弱性が突かれたケースが増えたことと、運用上の不備（脆弱なパスワードの使用や公開フォルダへの不適切なアクセス権限の付与など）を突かれたケースの増加したためです。あと、見逃せない特徴として、ＵＮＩＸ系のサーバの運用に対する油断が散見されます。従来型の攻撃がいきなり通じてしまうのです。恐らく、最近はＵＮＩＸ関係で大きなインパクトのある脆弱性が発見されていない状況で、数年前に運用体制を構築した人たちが異動してしまい、セキュリティ運用に必須の緊張感などの文化が引き継がれていなくて、単にマニュアルだけで次の人たちの世代に渡っているのが大きな理由ではないかと推測しています。新しいサーバを立てる場合にはマニュアルはあるのだが、精神が分かっていないため、当たり前のことがなされず、以前では考えられないような脆弱性が放置され、そこから侵入されてしまうというようなことが、最近散見されます。こういったことから、２００６年はインターネット側からの脅威により発生した重要インシデントが７ポイント増えたとみています。

(1) インターネット側で発生した重要インシデント

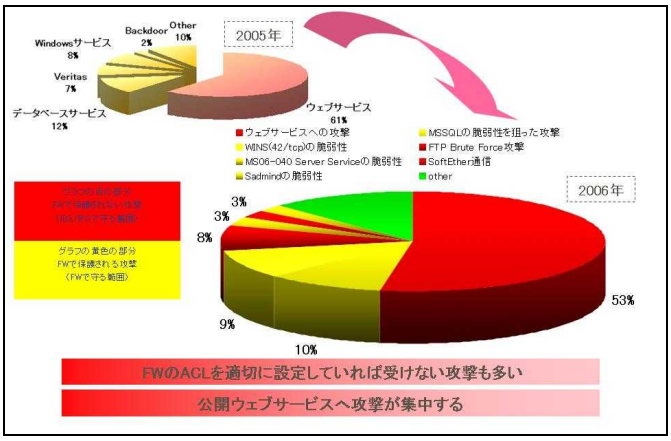


図 3.9　インターネット側で発生した重要インシデント

インターネット側での重要インシデントはＷｅｂサービスを狙ったものが相変わらず主流ですが、中にはずいぶん古いＵＮＩＸ関係の脆弱性が原因であるものも増加しています。

ファイアウォールのＡＣＬを適切に設定するかパッチ運用をしっかり行っていれば、防げたインシデントも相変わらず多いのです。そうなると、防ぐことの難しい脅威の大半は公開Ｗｅｂサービスであると言えます。

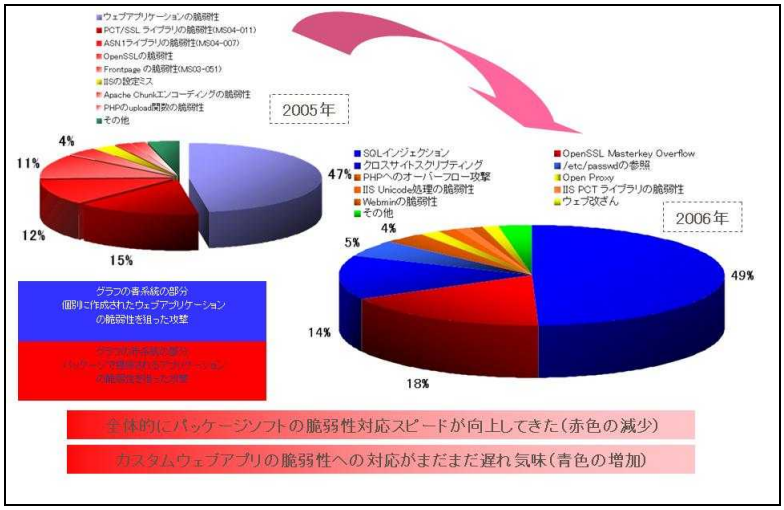


図 3.10　Web サービスへの攻撃の変化

そのＷｅｂサービスへの攻撃の変化ですが、一番多いのはＳＱＬインジェクションです。クロスサイト・スクリプティングも増加してきています。ポイントとしては、同じＷｅｂサービスでもパッケージソフトにおける脆弱性の対応スピードは向上してきています。しかし、ユーザが独自に作成しているＷｅｂアプリケーションの脆弱性への対応が攻撃の増加に比べ遅れているというのがこの資料からもうかがえます。

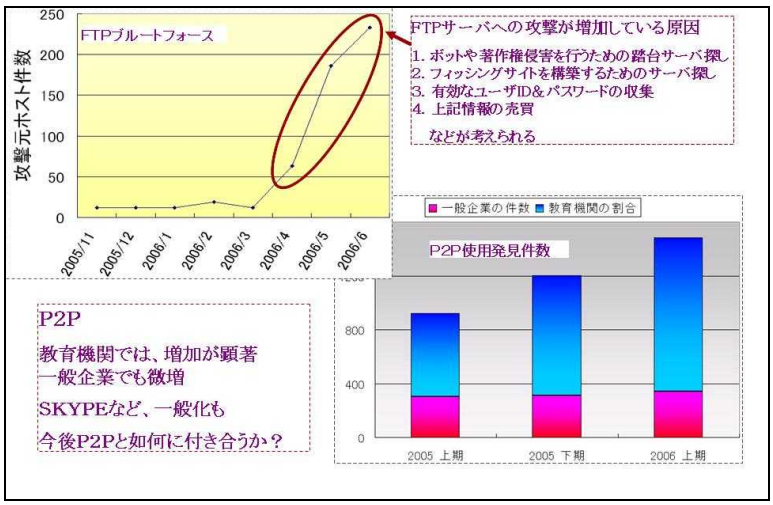


図 3.11　FTP サーバへの攻撃が増加している原因

次に、ＦＴＰとＳＳＨのユーザＩＤとパスワードを調べるブルートフォース攻撃での重要インシデントが増加しました。昨年４月くらいから増えています。 ユーザＩＤとパスワードを収集する攻撃者の目的は現在のところ私たちは掴んでおりません。ボットの活動に悪用するためなのか、著作権侵害を行うための踏み台とするサーバを探しているのか、フィッシングサイトを構築するためのサーバを探しているのか、単に有効なユーザＩＤ、パスワードを収集し売却することが目的なのかは不明です。実際に、こういう攻撃が成功しログインした後の行動を見ても、何をするわけでもないのです。そのまま引き上げていくことが多いのです。

(2) イントラネット側で発生した重要インシデント

内部でのＰ２Ｐ発見数の推移ですが、一般企業は微増でしたが最近は激減してきています。一方、教育機関や研究機関では増加し続けています。特に教育機関等では、Ｐ２Ｐに対する統制がとれていないところが多いと言わざるを得ません。特に著作権侵害や犯罪に直結するようなことは、やってはいけないことは当たり前のことですので、単にセキュリティポリシーを厳守させるという観点だけではなく、教育の観点でも指導が重要と思います。

(3) JSOC でのインシデント発見手段

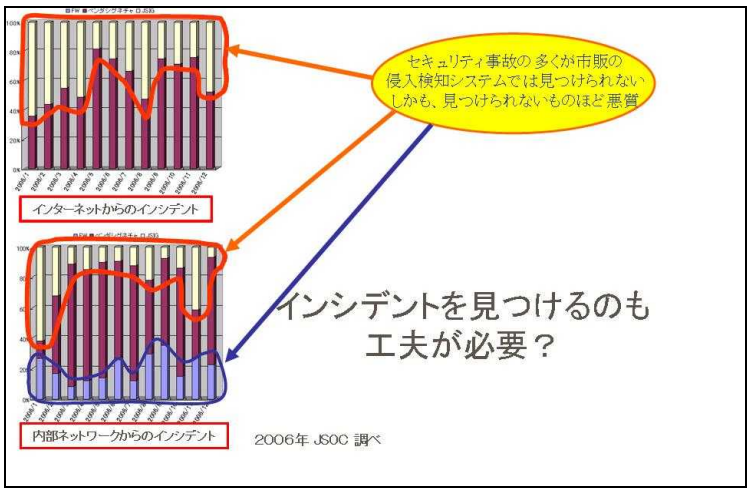


図 3.12　インシデントの発見

ＪＳＯＣでの重要インシデントの発見方法ですが、インターネットからの重要インシデントの約４割がＪＳＯＣオリジナルで作成しているシグネチャ（ＩＤＳやＩＰＳに投入する検出パターン)で見つけています。ＩＤＳベンダから提供されるシグネチャで見つけているのが約６割です。この市販されているパターンで見つけることのできる重要インシデントはどんどん少なくなってきています。当然のことながら市販のパターンでは見つけられない攻撃のほうがむしろ悪質である可能性が高いと見ることができます。

イントラネットでの重要インシデントの発見方法で特徴的なものはファイアウォールで見つけているということです。 従来ファイアウォールではインバウンド、つまり、インターネットからの通信を防ぐのが目的であり、アウトバウンド、つまり外向きの通信に目が向けられることは余りありませんでした。これは、ファイアウォールの設定で、インターネット側のネットワークを「信頼できないネットワーク」、イントラネットを「信頼できるネットワーク」と呼んでいることも、アウトバウンドに目が行っていない証拠とも言えます。 もはやイントラネットは「信頼できるネットワーク」ではなく、特に守るべき情報が格納されているネットワークと捉える必要があり、そこから出ていく通信に目を光らせるのは当然のことです。いずれにせよ、インシデントを見つけていくというのも、工夫が必要な時代に入ってきていると思います。

3.1.14 脅威の対抗策の推移

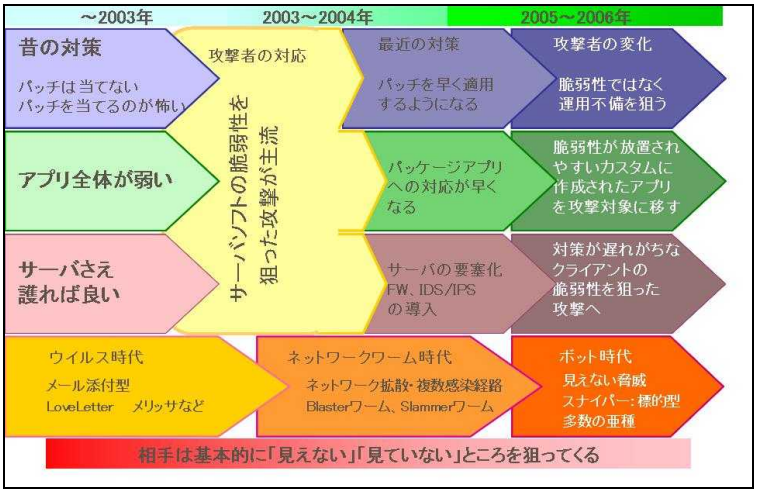


図 3.13　脅威の対抗策の推移

2002 年くらいまでというのは、パッチは当てたくないし、逆にシステムが稼動しなくなるなどの副作用が発生するため、パッチを当てる方がむしろ怖かったのですが、ある面、サーバさえ守ればよかった時代でした。

これが 2003 年～2004 年になりまして、サーバの脆弱性を狙った攻撃が一般化したので、当然パッチを早く適用するようになりました。 パッチを当てて動かなくなるリスクより、当てなくて侵入されてしまうリスクのほうが高くなったのです。 また、パッケージアプリケーションも発見された脆弱性に対して対応も早くなり、サーバの要塞化や、ファイアウォール、ＩＤＳ／ＩＰＳの導入が浸透しました。

最近は、パッチで提供されるような脆弱性ではなくて、運用の不備を狙う攻撃が増えています。例えば、パスワードが脆弱であるとか、設定のミスなどです。 例えば、パッチは当たっているし、ちゃんと運用しているのですが、インターネットに公開しているフォルダへ、インターネットから書き込みが可能となっていたため発生した改竄事件もときどき起きています。やはり、きちんとしている「はず」を確認することが重要であると言えます。

また、ユーザが作成したＷｅｂアプリケーションとクライアントの脆弱性を狙う攻撃へシフトしています。受動攻撃と言いますが、Ｗｅｂブラウザに脆弱性があるために不正なコンテンツを読み込もうとしたときにスパイウェアが組み込まれるなどの攻撃です。攻撃者が能動的に攻撃するのではなく、利用者が脆弱なＷｅｂブラウザなどで不正なコンテンツを受動的に表示することで攻撃を受けてしまうのです。 最近は、Ｗｅｂブラウザに留まらず、ワード、エクセルやＰＤＦなどのビジネスで使用するドキュメントファイルに不正なプログラムを仕込むようなクライアント側の脆弱性を狙った攻撃にシフトしてきています。

攻撃の悪質化と対策はいたちごっこで続いているのですが、攻撃が悪質化する原因の一つに

「対策」があります。 対策を行うと、それを乗り越えることを考え新手の手口が出てくる構造になっています。ですので、私たちは残念ながら、万全の対策をして安心することなど出来ないのです。むしろ「万全」な対策を取れば取るほど相手の攻撃力は増加してしまうジレンマがあるのです。 先日も大手印刷会社で発生した情報漏えい事件は、下請けの元開発会社の人が犯人であったというニュースが出ておりました。 大手印刷会社ですので、相応のセキュリティ対策を行っているはずですが、それでもなぜ犯罪が起きてくるかというと、残念ながら、対策をすればするほど、攻撃者は「出来心」や「ついうっかり」などの素人ではなく、確信犯を作ってしまう構造があるのです。さらに確信犯も模倣犯と筋金入りに分かれます。対策が甘かったころは、たいした努力も必要なく情報が取れる代わりに動機としても弱かったのです。しかし、強い意思を持って確実に狙ってくる筋金入りの攻撃者には大半のセキュリティ対策は無力だともいえます。ですから、「出来心」程度或いは「模倣犯」を防止する或いは抑止する対策と、筋金入りの確信犯を如何に見つけていくか或いは最終的な被害を最小限にしていくかということは分けて考えなければいけません。

3.1.15 セキュリティ対策の課題

対策には、「やる」セキュリティ対策と「やらされる」セキュリティ対策の２種類があります。基本的に、法律で決まったから、仕方が無いので、やるというは「やらされる」セキュリティ対策です。「やる」セキュリティ対策というのは、法律に適応することは最低限であって、守りたいものが明確で、守ることが目的なのです。

冒頭にお話した「形式的対策」は「やらされる」対策です。「戦略的対策」は「やる」対策になります。

この「形式的対策」の問題は、本来手段である対策が目的化するのです。ＩＴを安全に活用したいというためにセキュリティがいるのが本来ですが、「やらされる」対策は本来手段であるべき対策自体が目的になってしまうことが多々あります。しっかりやってほしいがために制定する、規格、ガイドライン、法律はやればやるほど、「形式的対策」が増えてしまうジレンマがあります。

もう一点、法治国家という言葉があります。 私は法律の専門家ではなく、一国民として言うと、ある面、日本は放置される放置国家だったかもしれないと思います。それが、本当の法治国家。つまり一般の人も法律を意識しなければいけない社会制度に今、変わってきているというふうに思います。以前は、普通に真面目に生きていれば法律を意識することは、まず無かったと思います。 これが、法律とお付き合いをしていかなくてはいけないという時代に変わってきたと思います。その時に重要なことは、単に法律を守る、という観点だけでは無く、法律に対するリテラシーを上げていく必要があるのではないかと思います。リテラシーが低いと、法の精神を理解せず、例えば文章に書いているかどうかなどで判断してしまう「形式的対策」で逃れようとするのではないかと思います。

(1) 形式的対策

要求されていることを、やっているかorやっていないか、なので、やっていることの証明が基

本になります。基本的には、どこまでということはありません。やっていれば良いのです。当然、費用はミニマムで実施します。しかし、費用はかけるのです。この費用というのは基本的に捨て金になります。

結局、トータルで考えると、コストパフォーマンスは悪いということに気が付いていきます。個人情報保護をやれと言われてこういう対策をしました。ＪＳＯＸをやれと言われてこういう対策をしました。次、何々をやれと言われてこういう対策をしましたというと、結局、捨て金ばかりが増えていくことになります。最低、実施策と要求事項とのインデックスくらいは作っていかないと割に合わないと思います。

(2) 戦略的対策

当然のことながら己を良く知り（IT をどう使うのか？守るべきものはなにか？自分の弱点は？など）、敵は誰なのか（何から守るのか？どんな手口でくるのか？敵の目的は何か？どうやって見つけるのか？など）を知って、初めて対策を立てることになります。

当然、気付くことなくして作戦は立ちません。 実施されている対策をみると、審判もたてずに、ルールも確認しないで、試合をいきなりしようとしているようなことが良くあります。 何がゴールなのか？どうやれば勝てるのか？どうなると負けなのか？というのを明確にしないとどうしようもないでしょう。 何のために努力しているのでしょうか？ この原点にやはり返らなくてはいけないと思います。

3.1.16 IT の統制で必要なこと

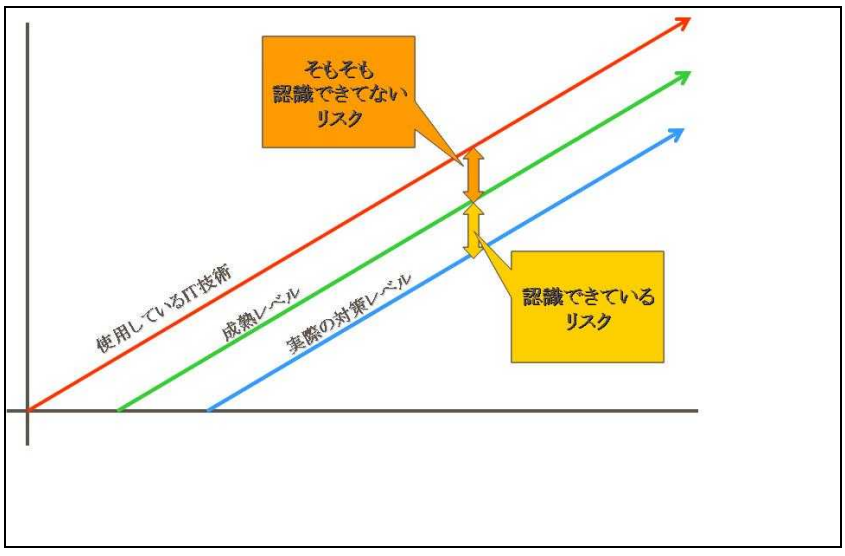


図 3.14　IT 統制で必要なこと

そもそも、我々が使用しているＩＴというのは、我々が理解している以上の機能や能力を持っているのです。さらに、実際の対策レベルは理解できているレベルよりまださらに低いのです。つまり、リスクには分かっているものと分かっていないものがあるということです。分かってい

ないリスクとは、要は何が脅威になるかも分かっていないので、統制以前の問題です。それは、ある面、我々の能力以上の能力を持つことになるからです。

つまりこのわかっていない部分をできるだけ小さくしていかないと、統制というのはできないということになります。端的に言うと、自分の能力を上げるか、乗る自動車の性能を落とすかです。例えば、車のエンジンばかりガンガン性能アップして、知らずに 400 キロものスピードで運転しているのです。でも、運転できていると言っても、制御できているかどうかは別です。自分の身の丈に合ったエンジンに積み替えるかエンジンに手を入れ馬力を落とすなどの対策も必要になるわけですが、自分ではその危険に気づいていないので、誰かが教えてあげる必要があります。

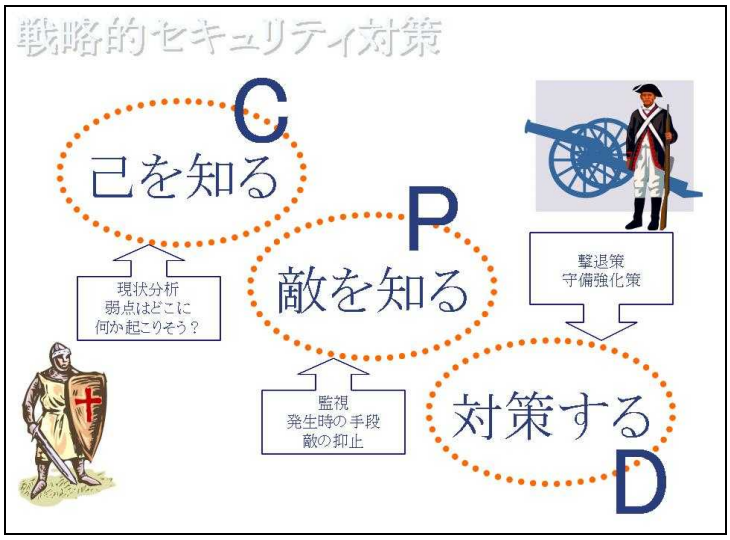


図 3.15　戦略的セキュリティ対策

それで、やはり己を知った上で、敵を知り、その上で対策をするということになるのです。「己を知る」ということは、現状分析が基本になります。守るべきものは何か？どんな弱点があるのか？ IT をどう使用しているのか？どうして行くのか？あたりが最低限必要なことと思います。次に、「敵を知る」ところになります。誰が敵なのか？どういうレベルなのか？ 出来心や模倣犯レベルなのか、国家レベルがバックについた組織なのか？抑止できるのか？見つけることが出来るのか？防ぐことは出来るのか？対策をやる上でもその間の見張りをどうするのか？などを考慮です。その上で対策をします。所謂、ＰＤＣのサイクルをまわしていくわけです。敵から守るために、お城を作るのに、見張りも立てないということは通常ありえません。まず、見張りを立てて、その上でそろそろと体力に合わせて、お城を作っていくというのが普通のアプローチかと思います。ところが、お城を作るのが「形式的」である場合は、見張りは必要ないのです。また、一般的にＰＤＣといいますが、セキュリティは「手段」であるので、ＰＤＣでは考えづらいのです。まずは「Ｃ」が入り、ＰＤと続き、結果的にＰＤＣのサイクルが完成していくと思います。

3.1.17 セキュリティ対策の位置づけ

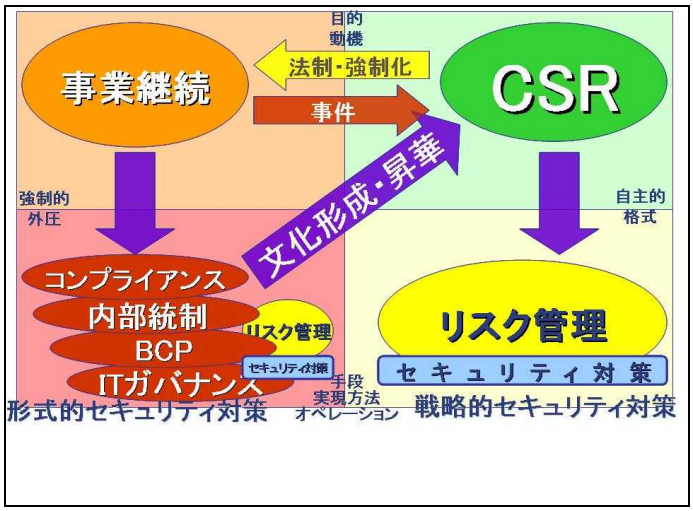


図 3.16　セキュリティ対策の位置づけ

四つのフィールドに分けて整理をしてみました。この縦軸が目的。上のほうが目的であるとか動機です。下がそれを実現するための手段であるとかオペレーション。左側がなぜやるかという動機となります。左側が外圧的、強制的な理由で実施となり、右が自主的に実施となっています。右側は、社会的責任からリスクのマネジメントをしてセキュリティ対策をするというのが本来なのでしょう。

ただ、なかなかそうはいかなくて、外圧でコンプライアンス、内部統制、ＢＣＰ、ガバナンスをやれと、左下の手段としての対策をやります。しかし、せめて、左上の事業継続の為にこの左下を実施するのだ、という理解が必要になると思います。さらに、右上のＣＳＲから左上の事業継続をやろうというようなトップダウンで動いていくようになれば、会社としても既に十分な利益を確保できているということであり、次のステップである社会貢献もしっかり出来ていく体制が出来たということだと思います。

先日、ＪＳＯＣ及び弊社の研究所のほうで、マイクロソフト社製の製品で、特にオフィス関係が攻撃者の標的にされてしまうことが増えている、というレポートを出しました。脆弱性が公になったときに攻撃が発生している若しくは攻撃コードが公開されている状態のことを、ゼロデイといいますが、このゼロデイは、インターネット･エクスプローラは 2005 年、2006 年と横ばいです。2005 年は、ゼロデイでインターネット･エクスプローラが標的となった感があったわけですが、それが 2006 年ではオフィス製品側にシフトしたというのがポイントです。オフィス製品全体で、２００５年は０件だったゼロデイが、2006 年は８件となりました。ワードなどのオフィスドキュメントに不正なコードが仕込まれていて、ドキュメントを開こうとするとスパイウェア等が組み込まれてしまう。そういうことに悪用されるゼロデイが増えています。脅威が広域型から標的型に変化しているのは、こういうゼロデイの変化からもうかがい知ることが出来ます。

ネットに落ちている毒りんごを食べるもの（ソフトウェア）は、Ｗｅｂブラウザやメールソフトに留まらず、オフィス製品やビューワやプレイヤーや、当然のことですがウイルス対策ソフト

などがあります。そろそろ企業の中で、ドキュメントファイルフォーマットごとの管理方法を議論していい時期に来ています。ワード、エクセルやＰＤＦなどのドキュメントをどう管理していくか、また安全確認できていないドキュメントファイルをどう処理していくのかなどは、すぐそこにある危機として対策が必要です。

3.1.18 IT 統制で意識すべきセキュリティオペレーション

まず、第一にファイアウォール周りのアウトバウンドのマネジメントが急務です。もともとファイアウォールというのは、怖い外部から内部を守るのが目的で管理対象はインバウンドが主でした。所謂、入ってくる通信への着目ですが、それと同様に外部に出て行くものもより詳細に見ていきましょうというのがポイントになります。ファイアウォールの外向きの通信を見るだけで、内部に潜んでいるボットやワームとかスパイウェアや使用しているＰ２Ｐの多くを発見することができるのです。さらに、外部にメールやＷｅｂメールその他の方策を使用して情報持ち出しの発見にも大きな役割を果たすことも可能になります。次に考慮したいのは、外部向けの通信を精査する、プロキシサーバ（フィルタリングソフトを含みます）の導入です。

また、Ｗｅｂアプリケーションは、単純に検査して修正するだけではなく、監視などとか組み合わせて、総合的に守っていくという部分が現状すぐに出来る対策です。 さらに、監視していることを告知することも考慮して良いです。外部からやってくる攻撃者は大半が個人レベルですので、見張られているところには近寄らないというのが基本になっていますので、こういうことも非常に大きなポイントだと思います。そうすると、筋金入りの攻撃者は別な方法を考えますので、その対抗策として、別の網を張ることが出来ます。

開発するときからセキュアにするビルトインセキュリティも本気になって考えなければいけない。現場は営業的に追われていますので、早く出せ、即出せといわれて、仕事を詰め込まれている中でセキュリティなんか考えていられませんというのが現状かもしれないのですが、一歩立ち止まり、考えるときにもう来ていると思います。

3.1.19 最後に

ＩＴ統治とかガバナンスというからには、形式で済ますことはあり得ないということです。今、この瞬間に皆さんの会社で事件が発生しました。それを見つけることが出来ますか？内部にスパイウェアが潜んでいる、機密の持ち出しや業務を混乱させる目的で何年も前から社員にとけこみ信頼されているスパイの手下、そういったことは見つけられるのでしょうか。それから、ＩＴにおいて限られた人間に権限やオペレーションが集中していませんか。よく分からないからお前全部やっておけという話はよく耳にします。管理者がユーザ運用まで全部やっているというようなことはありませんか？ このようなことは統制以前の話です。さらに、ＩＴというと、日本の場合、口では重要だと皆様言うのですが、経営レベルで本当に真面目にとらえられている例というのは残念ながらまだ少ないように思います。経営を司る重要人物が、ＩＴの責任者をやっている企業というのはあまり見たことがないと正直思っています。さらに、ＩＴ関係者の社会的地位や待遇の低さというのも、今後改善していかないと、様々な意味で筋金入りの攻撃者に対抗できていけないと思います。それは、開発だけではなく、特にユーザやシステム運用に関係する部分です。開発のチェック。運用のチェック。管理者のチェック。セキュリティオペレーションの位置付け。そういう位置付け。そういったこともよく考えたほうがいいと思います。

手段が目的化していませんか。ときどき原点回帰をしましょう。

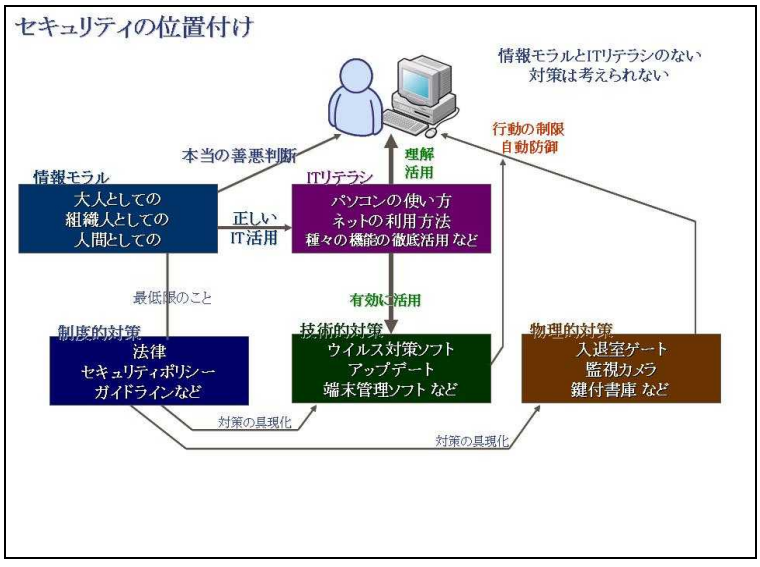


図 3.17　セキュリティの位置づけ

最後に、セキュリティは制度的対策、技術的対策、物理的対策の三つでやるといわれています。ただ、それを支えるためには一般ユーザを含めＩＴリテラシーがないと技術的対策が生きてきません。さらに、情報モラルがないと、制度的対策を生かしきれません。全てを規定していくには無理がありますし、本当に良い事にも思えません。当然のことながら、３つの対策を身の丈にあわせ少しずつスパイラルをもってやるのが基本かと思います。セキュリティを文化として育て、

最終的には人に始まって、人に終わるわけですが、実装にはやはり技術が必須となるわけです。このあたりをバランスして法律への対策であるとか、皆様のセキュリティ対策の中にうまく活用できればありがたいと思っています。

3.2 財務報告に係る内部統制の評価と監査への対応

3.2.1 はじめに

2006 年 6 月 7 日に証券取引法の一部を改正する法律が国会で可決成立し、証券取引法は、その他の金融商品もその対象範囲に含むこととし、金融市場の変化に対応して投資家等の保護をより図るように金融商品取引法と名称を変更することになった。この金融商品取引法では、上場企業等に対し､財務報告に係る内部統制の評価及び監査の制度が導入されることが規定されている。本制度は 2008 年 4 月 1 日開始事業年度の決算から適用されることになる。一方、本制度の導入を見越して金融庁では、企業会計審議会のもとに内部統制部会（部会長：八田進二）を 2005 年に設置した。内部統制部会では、米国等における企業改革法の導入事例等を踏まえわが国にあった制度のありかたを検討し、2005 年 12 月 8 日に「財務報告に係る内部統制の評価及び監査の基準のありかたについて（意見書)」を公表した。この報告書は、内部統制の評価及び監査の制度の枠組みを示しているものであり、財務報告に係る内部統制の評価及び監査の基準案（以下、基準案）を含んだものである。また、実務に適用するためには、より詳細な指針が必要という認識のもと、内部統制部会に作業部会を設置し、実務指針を策定し、基準案の改訂とあわせて「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の設定について（意見書)」を 2007 年 1 月 31 日に公表した。以下、財務報告に係る内部統制の評価及び監査に関する基準を「基準」､財務報告に係る内部統制の評価及び監査に関する実施基準を「実施基準」ということにする。

このように、財務報告に係る内部統制の評価及び監査の制度が始まることになったわけであるが、この制度の導入の背景は、米国におけるエンロン、ワールドコムといった大企業の粉飾決算による企業改革法の導入や日本においても同様の事件が続き、投資家保護をより行っていく必要性が求められることになったからであろう。したがって、そもそもこの制度自体は適正な財務諸表の開示が行われることを担保するための制度である。しかし、一方、現在の財務諸表の作成が IT の活用なしには行い得ないところに､この財務諸表の適正性を担保するための制度と情報セキュリティの接点を見出すことができる。以下、本稿では、財務報告に係る内部統制の評価及び監査の制度の概要、経営者評価について説明し、その後 IT 統制について説明する。IT 統制において情報セキュリティとの接点を説明する。最後に、この制度を効率的に運用していく際のポイントを説明することにする。

3.2.2 制度概要

(1) 制度の概要

エンロン、ワールドコムの粉飾に端を発し米国で企業改革法が議員立法により成立し、一方日本でも鉄道会社や IT ベンチャー企業の有価証券報告書偽造事件等が起こり、投資家が大きな損害をこうむったことから、投資家保護をより磐石なものとするために財務報告に係る内部統制の評価及び監査の制度が導入されることになった。したがって、この制度の本質は投資家の保護である。投資家の保護という観点から日本では従来より、財務諸表に対し公認会計士が監査をし、

監査報告書を有価証券報告書に添付し、公表するという制度があった。いわば財務諸表という投資判断の主要な材料について公認会計士が信頼性を付与する仕組みがあったわけである。しかし、上記のとおり有価証券報告書の偽造事件等がつづくに及び財務諸表だけでなく、その財務諸表を作成する過程における内部統制についての有効性についても経営者が自ら評価し、その結果を報告書（内部統制報告書）として提出し、監査人がその報告書の適正性を監査し、内部統制監査報告書として提出することにより財務諸表等の信頼性を担保する制度を新たに導入することにしたというわけである。なお、内部統制の有効性の評価及び経営者報告書の適正性の監査の基準日は決算日となっている。

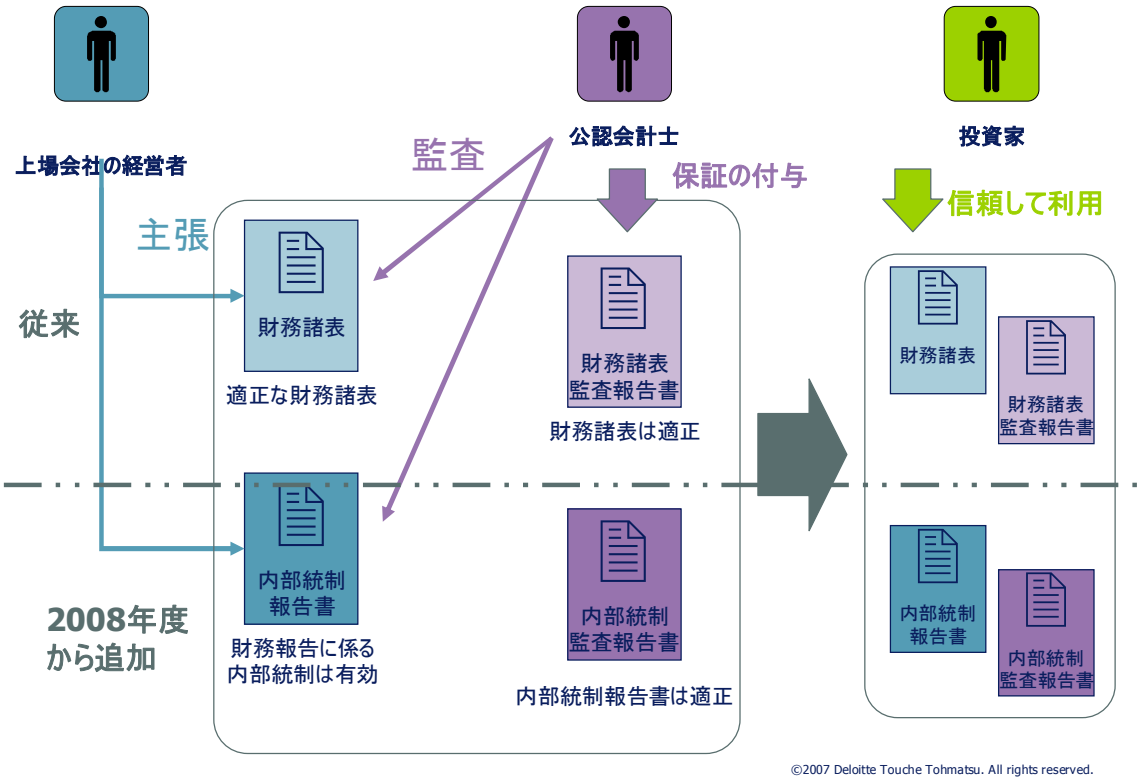


図 3.18　財務報告に係る内部統制の評価及び監査の制度の概要

(2)　全体の枠組み

財務報告に係る内部統制の評価及び監査の制度においては、金融商品取引法において、経営者評価と公認会計士による監査の義務化が行われているが、内部統制の枠組み、経営者評価の仕方、監査の基準については、企業会計審議会で決められている。また、金融商品取引法では一部の詳細な事項が内閣府令に委任されている。このような体系をまとめると図 3.19 のようになる。

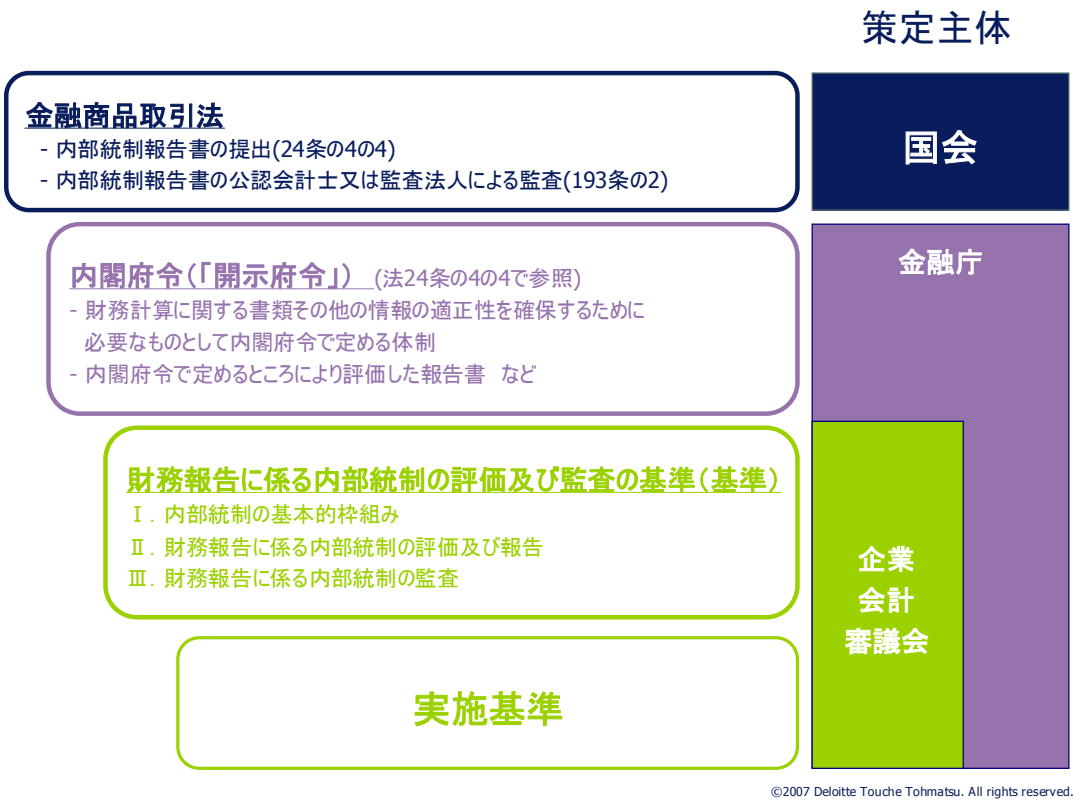


図 3.19　制度全体の枠組み

(3) 法的根拠

財務報告に係る内部統制の有効性を経営者が評価し、その結果を内部統制報告書として提出することは金融商品取引法第 24 条の 4 の 4, 内部統制報告書の適正性について公認会計士が評価することについては金融商品取引法第 193 条の 2 第 2 項により規定されている。

参考　金融商品取引法

第 24 条の 4 の 4

第二十四条の四の四第二十四条第一項の規定による有価証券報告書を提出しなければならない会社（第二十三条の三第四項の規定により当該有価証券報告書を提出した会社を含む。次項において同じ。）のうち，第二十四条第一項第一号に掲げる有価証券の発行者である会社その他の政令で定めるものは，事業年度ごとに，当該会社の属する企業集団及び当該会社に係る財務計算に関する書類その他の情報の適正性を確保するために必要なものとして内閣府令で定める体制について，内閣府令で定めるところにより評価した報告書（以下「内部統制報告書」という。）を有価証券報告書（同条第八項の規定により同項に規定する有価証券報告書等に代えて外国会社報告書を提出する場合にあっては，当該外国会社報告書）と併せて内閣総理大臣に提出しなければならない。

第 193 条の 2 第 2 項

金融商品取引所に上場されている有価証券の発行会社その他の者で政令で定めるものが，この法律の規定により提出する貸借対照表，損益計算書その他の財務計算に関する書類で内閣府令で定めるものには，その者と特別の利害関係のない公認会計士又は監査法人の監査証明を受けなければならない。ただし，監査証明を受けなくても公益又は投資者保護に欠けることがないものとして内閣府令で定めるところにより内閣総理大臣の承認を受けた場合は，この限りでない。

なお、金融商品取引法の附則第 15 条によりこの２つの条文は、平成 20 年（2008 年）4 月 1 日開始事業年度の決算より適用されることが定められている。

２つとの条文とも適用除外等詳細についての規定は内閣府令に委任されているが、2007 年 3 月 17 日現在、内閣府令は公表されていないため、どのよう場合に適用除外が受けられるか等の詳細は不明である。

(4) 基準及び実施基準

金融商品取引法では、経営者が内部統制報告書を提出し、公認会計士が内部統制監査報告書を提出することが義務付けられているだけで、実際にどのようにそれを行うべきかは規定していない。どのように行うべきかの枠組みについては、企業会計審議会のもとに設置された内部統制部会により検討され、企業会計審議会により基準及び実施基準として定められた。基準及び実施基準は三部構成となっている。第一部「内部統制の基本的枠組み」は、内部統制の枠組みをしめしたもの、つまり、内部統制の有効性を評価する際にどのような場合に内部統制が有効かを判断するための基準となっている。第二部「財務報告に係る内部統制の評価及び監査」は、経営者が財務報告に係る内部統制を評価する際に従うべき基準である。経営者は、基準及び実施基準の第二部に従って経営者評価をし、その結果として内部統制の有効性についての意見を内部統制報告書に表明することになる。第三部「財務報告に係る内部統制の監査」は、公認会計士が内部統制報告書の適正性を監査する際に従うべき基準である。基準及び実施基準の目次項目を示せば図 3.20 のとおりとなる。

図 3.20　基準及び実施基準

本稿では、おもに第二部の経営者評価に関する部分について簡単に説明することにする。

■コラム（基準における内部統制の基本的要素）

日本の基準及び実施基準の内部統制の枠組みでは、トレッドウェイ委員会組織委員会による内部統制報告書（以下、COSO 報告書という）の内部統制の枠組みにおける構成要素と異なり、基本的要素という用語を使い、「IT への対応」を加えていることが特徴となっている。これは、「COSO 報告書公表後の IT 環境の飛躍的進展により、IT が組織に浸透した現状に即して「IT への対応」を基本的要素の 1 つに加えている。」と説明されている。ただし、「IT への対応」は、内部統制の他の基本的要素と必ずしも独立に存在するものではないが、組織の業務内容が IT に大きく依存している場合や組織の情報システムがＩＴを高度に取り入れている場合等には、内部統制の目的を達成するために不可欠の要素として、内部統制の有効性に係る判断の規準となるとされている。

基準における内部統制の基本的要素とその定義は図 3.20 のようになる

IT への対応と他の基本的要素との関係は図 3.21 のようになる。

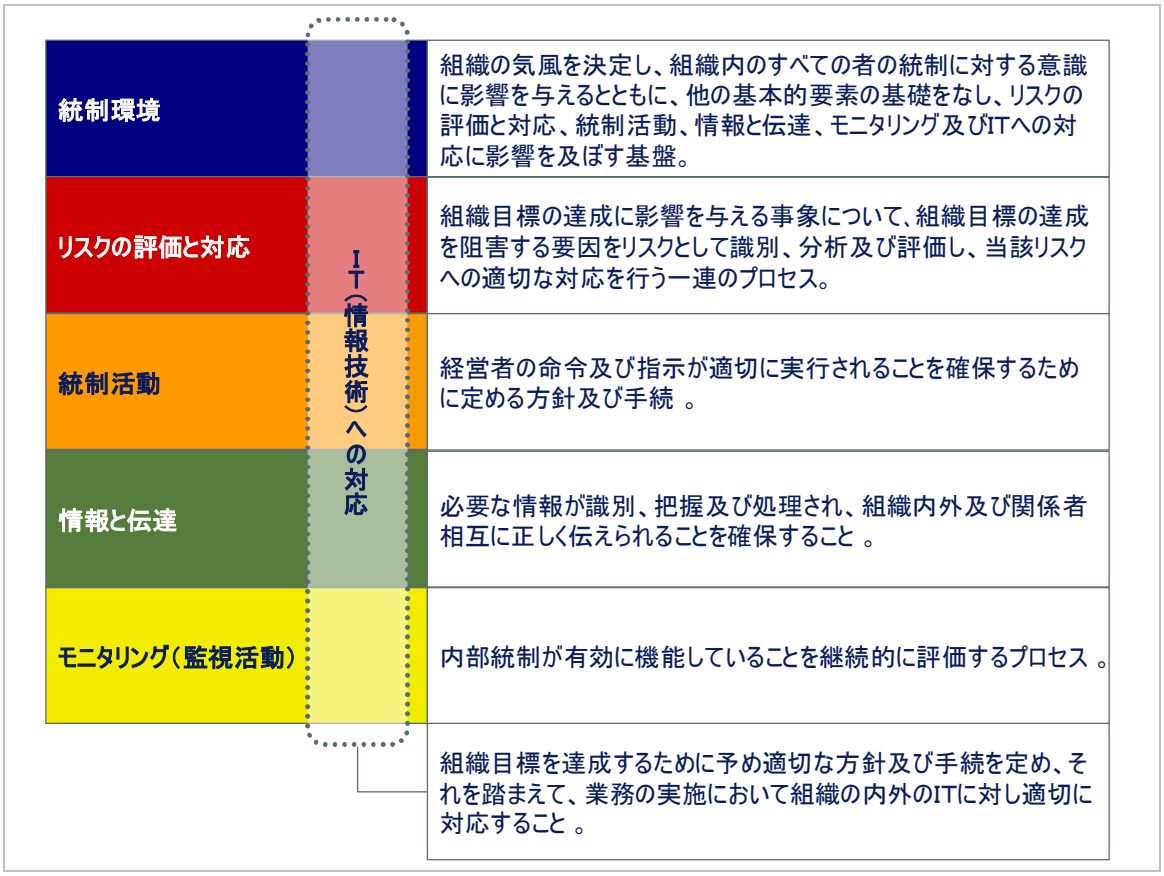


図 3.21　IT への対応と他の基本的要素との関係

3.2.3　経営者評価

(1)　評価の対象となる内部統制の範囲

財務報告に係る内部統制の評価及び監査の制度においては、対象となるのは財務報告に係る内部統制に限定される。このことをまず念頭におく必要がある。なお、財務報告は財務諸表のみならず財務諸表の信頼性に重要な影響を及ぼす開示事項（財務諸表に記載された金額、数値、注記を要約、抜粋、分解又は利用して記載すべき開示事項、関係会社の判定、連結の範囲の決定、持分法の適用の適否、関連当事者の判定その他財務諸表の作成における判断に密接に関わる事項）のことである。有価証券報告書は連結ベースで作成されることから、海外子会社に存在する内部統制も業務プロセスに重要性があれば評価の対象となる。なお、財務報告につながる重要な業務プロセスが内部統制の評価の対象となることから業務委託を行っている場合に委託先に委託した業務も内部統制の評価の対象となりうる。例えば、会計システムの運用を企業グループ以外に委託している場合であっても、評価の対象となりうる。

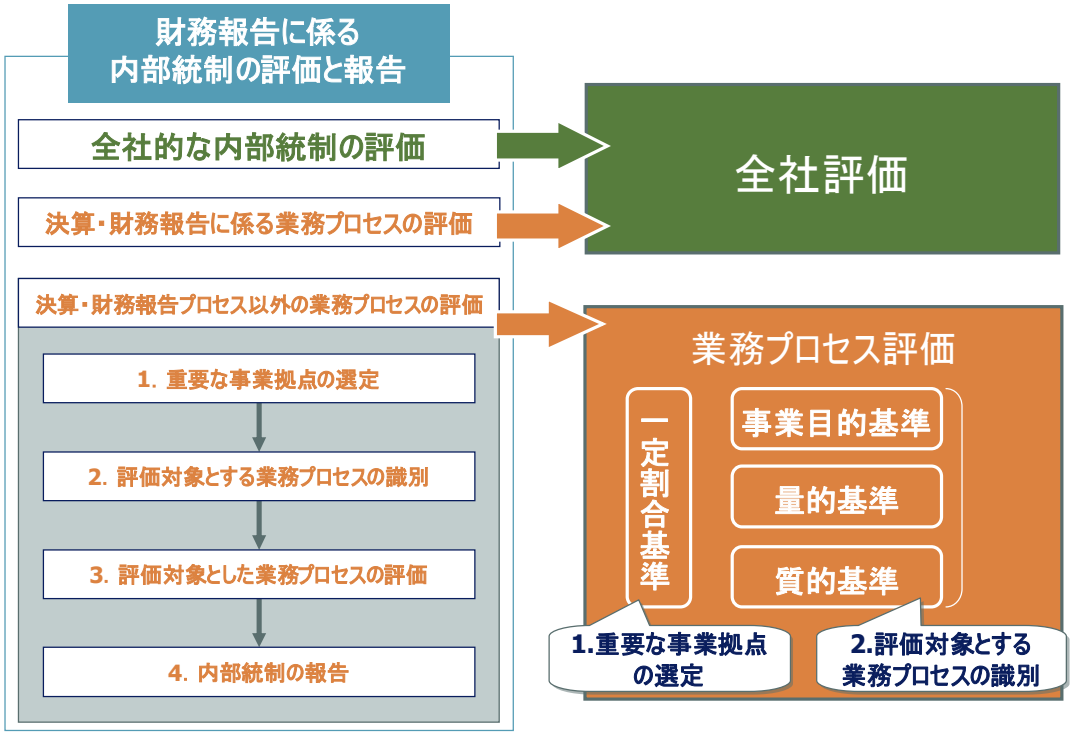
(2)　評価プロセスの概要

財務報告に係る内部統制の評価については、基準及び実施基準の第二部で規定されている。こ

こでは、評価プロセスの概要について説明する。

経営者評価を行う場合は、トップダウンによるリスクアプローチを採用していることから、まず連結ベースの財務報告全体に重要な影響を及ぼす「全社的な内部統制」を評価し、その後で、業務プロセスに組み込まれ一体となって遂行される内部統制である「業務プロセスに係る内部統制」を評価することが原則となる。ただし、業務プロセスに係る内部統制のうち決算・財務報告プロセスに係る業務プロセスは、全社的な観点から全社ベースで評価されることになる。業務プロセスに係る内部統制の評価においては、そのすべての業務プロセスを評価の対象とするのではなく、量的な重要性（一定割合基準）の観点から事業拠点を絞り、さらに事業目的との関係性（事業目的基準）並びに量的及び質的な重要性（量的基準及び質的基準）の観点から重要なプロセスを絞り評価範囲を決定し、評価していくことになる。

評価プロセスの全体像については図 3.22 のとおりとなる。



（出典：内部統制部会第16回会議資料2）

図 3.22　経営者評価プロセスの全体像

(3) 内部統制の評価

①整備状況の評価と運用状況の評価

内部統制の評価は基本的に、整備状況の評価と運用状況の評価にわけて行う。整備状況の評価は、財務報告の虚偽記載につながるリスクを一定水準以下に低減するように内部統制が設計されて導入されているかを確認することになる。運用状況の評価は、導入されている内部統制が継続

的に運用されていることをサンプル等を抽出して評価することになる。

②全社的な内部統制の評価と業務プロセスに係る内部統制の評価

全社的な内部統制の評価は、質問書による質問やその質問に対する回答についての裏づけ証拠等を査閲することにより内部統制が有効に整備及び運用されていることを評価することになる。以下に実施基準で示されている全社的な内部統制の評価項目例を示す。

統制環境

- 経営者は，信頼性のある財務報告を重視し，財務報告に係る内部統制の役割を含め，財務報告の基本方針を明確に示しているか。
- 適切な経営理念や倫理規程に基づき，社内の制度が設計・運用され，原則を逸脱した行動が発見された場合には，適切に是正が行われるようになっているか。
- 経営者は，適切な会計処理の原則を選択し，会計上の見積り等を決定する際の客観的な実施過程を保持しているか。
- 取締役会及び監査役又は監査委員会は，財務報告とその内部統制に関し経営者を適切に監督・監視する責任を理解し，実行しているか。
- 監査役又は監査委員会は内部監査人及び監査人と適切な連携を図っているか。
- 経営者は，問題があっても指摘しにくい等の組織構造や慣行があると認められる事実が存在する場合に，適切な改善を図っているか。
- 経営者は，企業内の個々の職能（生産，販売，情報，会計等）及び活動単位に対して，適切な役割分担を定めているか。
- 経営者は，信頼性のある財務報告の作成を支えるのに必要な能力を識別し，所要の能力を有する人材を確保・配置しているか。
- 信頼性のある財務報告の作成に必要とされる能力の内容は，定期的に見直され，常に適切なものとなっているか。
- 責任の割当てと権限の委任がすべての従業員に対して明確になされているか。
- 従業員等に対する権限と責任の委任は，無制限ではなく，適切な範囲に限定されているか。
- 経営者は，従業員等に職務の遂行に必要となる手段や訓練等を提供し，従業員等の能力を引き出すことを支援しているか。
- 従業員等の勤務評価は，公平で適切なものとなっているか。

リスクの評価と対応

- 信頼性のある財務報告の作成のため，適切な階層の経営者，管理者を関与させる有効なリスク評価の仕組みが存在しているか。
- リスクを識別する作業において，企業の内外の諸要因及び当該要因が信頼性のある財務報告の作成に及ぼす影響が適切に考慮されているか。
- 経営者は，組織の変更やＩＴの開発など，信頼性のある財務報告の作成に重要な影響を及ぼす可能性のある変

化が発生する都度，リスクを再評価する仕組みを設定し，適切な対応を図っているか。

・ 経営者は，不正に関するリスクを検討する際に，単に不正に関する表面的な事実だけでなく，不正を犯させるに至る動機，原因，背景等を踏まえ，適切にリスクを評価し，対応しているか。

統制活動

・ 信頼性のある財務報告の作成に対するリスクに対処して，これを十分に軽減する統制活動を確保するための方針と手続を定めているか。

・ 経営者は，信頼性のある財務報告の作成に関し，職務の分掌を明確化し，権限や職責を担当者に適切に分担させているか。

・ 統制活動に係る責任と説明義務を，リスクが存在する業務単位又は業務プロセスの管理者に適切に帰属させているか。

・ 全社的な職務規程や，個々の業務手順を適切に作成しているか。

・ 統制活動は業務全体にわたって誠実に実施されているか。

・ 統制活動を実施することにより検出された誤謬等は適切に調査され，必要な対応が取られているか。

・ 統制活動は，その実行状況を踏まえて，その妥当性が定期的に検証され，必要な改善が行われているか。

情報と伝達

・ 信頼性のある財務報告の作成に関する経営者の方針や指示が，企業内のすべての者，特に財務報告の作成に関連する者に適切に伝達される体制が整備されているか。

・ 会計及び財務に関する情報が，関連する業務プロセスから適切に情報システムに伝達され，適切に利用可能となるような体制が整備されているか。

・ 内部統制に関する重要な情報が円滑に経営者及び組織内の適切な管理者に伝達される体制が整備されているか。

・ 経営者，取締役会，監査役又は監査委員会及びその他の関係者の間で，情報が適切に伝達・共有されているか。

・ 内部通報の仕組みなど，通常の報告経路から独立した伝達経路が利用できるように設定されているか。

・ 内部統制に関する企業外部からの情報を適切に利用し，経営者，取締役会，監査役又は監査委員会に適切に伝達する仕組みとなっているか。

モニタリング

・ 日常的モニタリングが，企業の業務活動に適切に組み込まれているか。

・ 経営者は，独立的評価の範囲と頻度を，リスクの重要性，内部統制の重要性及び日常的モニタリングの有効性に応じて適切に調整しているか。

・ モニタリングの実施責任者には，業務遂行を行うに足る十分な知識や能力を有する者が指名されているか。

・ 経営者は，モニタリングの結果を適時に受領し，適切な検討を行っているか。

・ 企業の内外から伝達された内部統制に関する重要な情報は適切に検討され，必要な是正措置が取られているか。

・ モニタリングによって得られた内部統制の不備に関する情報は，当該実施過程に係る上位の管理者並びに当該

実施過程及び関連する内部統制を管理し是正措置を実施すべき地位にある者に適切に報告されているか。

・ 内部統制に係る重要な欠陥等に関する情報は，経営者，取締役会，監査役又は監査委員会に適切に伝達されているか。

ＩＴへの対応

・ 経営者は，ＩＴに関する適切な戦略，計画等を定めているか。

・ 経営者は，内部統制を整備する際に，ＩＴ環境を適切に理解し，これを踏まえた方針を明確に示しているか。

・ 経営者は，信頼性のある財務報告の作成という目的の達成に対するリスクを低減するため，手作業及びＩＴを用いた統制の利用領域について，適切に判断しているか。

・ ＩＴを用いて統制活動を整備する際には，ＩＴを利用することにより生じる新たなリスクが考慮されているか。

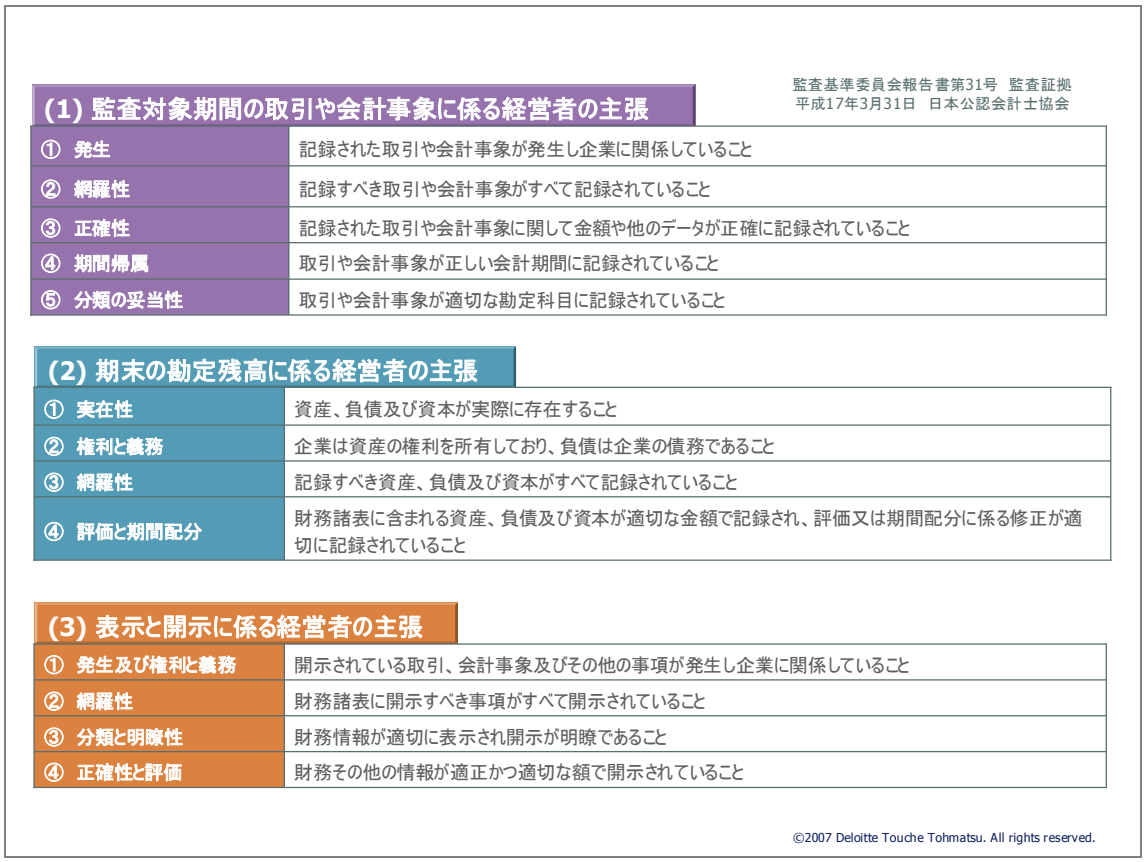
・ 経営者は，ＩＴに係る全般統制及びＩＴに係る業務処理統制についての方針及び手続を適切に定めているか。

一方業務プロセスに係る内部統制の評価は、業務プロセスに組み込まれた内部統制活動を評価することになるが、財務報告の虚偽記載につながるリスク、例えば、架空売上の計上、たな卸し評価損の未計上、減価償却費の計算誤りを予防又は発見し修正する統制活動を具体的に評価していくことになる。この際にリスクをある程度分類して考えると内部統制を効率的に評価できるため、架空計上というリスクに対しては「実在性」、未計上というリスクに対しては「網羅性」、という名前をつけ、実施基準では「適切な財務情報を作成するための要件」といっている。勘定科目についてこの「適切な財務情報を作成するための要件」が適切に整備、運用されていることを確認することになる。なお、実施基準で示されている適切な財務情報を作成するための要件とその内容は図 3.23 のとおりである。

表 3.1　適切な財務情報を作成するための要件

適切な財務情報を作成するための要件	内容
a. 実在性	資産及び負債が実際に存在し，取引や会計事象が実際に発生していること
b. 網羅性	計上すべき資産，負債，取引や会計事象をすべて記録していること
c. 権利と義務の帰属	計上されている資産に対する権利及び負債に対する義務が企業に帰属していること
d. 評価の妥当性	資産及び負債を適切な価額で計上していること
e. 期間配分の適切性	取引や会計事象を適切な金額で記録し，収益及び費用を適切な期間に配分していること
f. 表示の妥当性	取引や会計事象を適切に表示していること

なお、「適切な財務情報を作成するための要件」は、「経営者の主張」、「アサーション」、又は「監査要点」と呼ばれることがある。日本公認会計士協会 監査基準委員会報告書 第 31 号 監査証拠では、この「経営者の主張」を以下のように整理している。



監査基準委員会報告書第31号　監査証拠
平成17年3月31日　日本公認会計士協会

(1) 監査対象期間の取引や会計事象に係る経営者の主張

① 発生	記録された取引や会計事象が発生し企業に関係していること
② 網羅性	記録すべき取引や会計事象がすべて記録されていること
③ 正確性	記録された取引や会計事象に関して金額や他のデータが正確に記録されていること
④ 期間帰属	取引や会計事象が正しい会計期間に記録されていること
⑤ 分類の妥当性	取引や会計事象が適切な勘定科目に記録されていること

(2) 期末の勘定残高に係る経営者の主張

① 実在性	資産、負債及び資本が実際に存在すること
② 権利と義務	企業は資産の権利を所有しており、負債は企業の債務であること
③ 網羅性	記録すべき資産、負債及び資本がすべて記録されていること
④ 評価と期間配分	財務諸表に含まれる資産、負債及び資本が適切な金額で記録され、評価又は期間配分に係る修正が適切に記録されていること

(3) 表示と開示に係る経営者の主張

① 発生及び権利と義務	開示されている取引、会計事象及びその他の事項が発生し企業に関係していること
② 網羅性	財務諸表に開示すべき事項がすべて開示されていること
③ 分類と明瞭性	財務情報が適切に表示され開示が明瞭であること
④ 正確性と評価	財務その他の情報が適正かつ適切な額で開示されていること

図 3.23　経営者の主張

売掛債権の実在性を確保するための内部統制は業務プロセスの中に複数組み込まれている。たとえば、「あらかじめ与信の承認した顧客以外には掛売できないようにシステム上でロックがかかる」、「契約書の内容を査閲し、実在する取引であることを確認する」、「未回収債権の内容を査閲し、回収可能であることを確認する」、という内部統制はいずれも、売掛債権の実在性に関連する内部統制である。内部統制の評価を行う場合、このすべての評価する必要はない。このうち、経営者の主張が保証できるだけの内部統制の評価ができればよいことになる。評価の対象とする統制を実施基準では「統制上の要点」としている。

③有効性評価

評価範囲が適正で、評価範囲に含まれる内部統制がすべて有効に整備され運用されていれば「財務報告に係る内部統制は有効である」と判断される。しかし、内部統制に不備があり、その内部統制が単独または他の内部統制の不備とあわせて重要な記載誤りの可能性が高いと判断される場合は「財務報告に係る内部統制は有効でない」と評価されることになる。

(4) IT 統制とその評価

①IT への対応の概要

「IT への対応」は、組織目標を達成するために予め適切な方針及び手続を定め、それを踏まえて、業務の実施において組織の内外の IT に対し適切に対応することをいう。

この「IT への対応」はさらに「IT 環境への対応」、「IT の利用と統制」に分類される。また、IT の利用と統制には、「IT の利用」と「IT の統制」に分類され、「IT の統制」は、「IT に係る全般統制（以下、IT 全般統制という）」と「IT に係る業務処理統制（以下、IT 業務処理統制という）」の２つに分類されている。IT の業務処理統制は IT の統制に含まれているが、IT を利用した統制である。「IT 全般統制」実施基準においては図 3.24 のようになる。

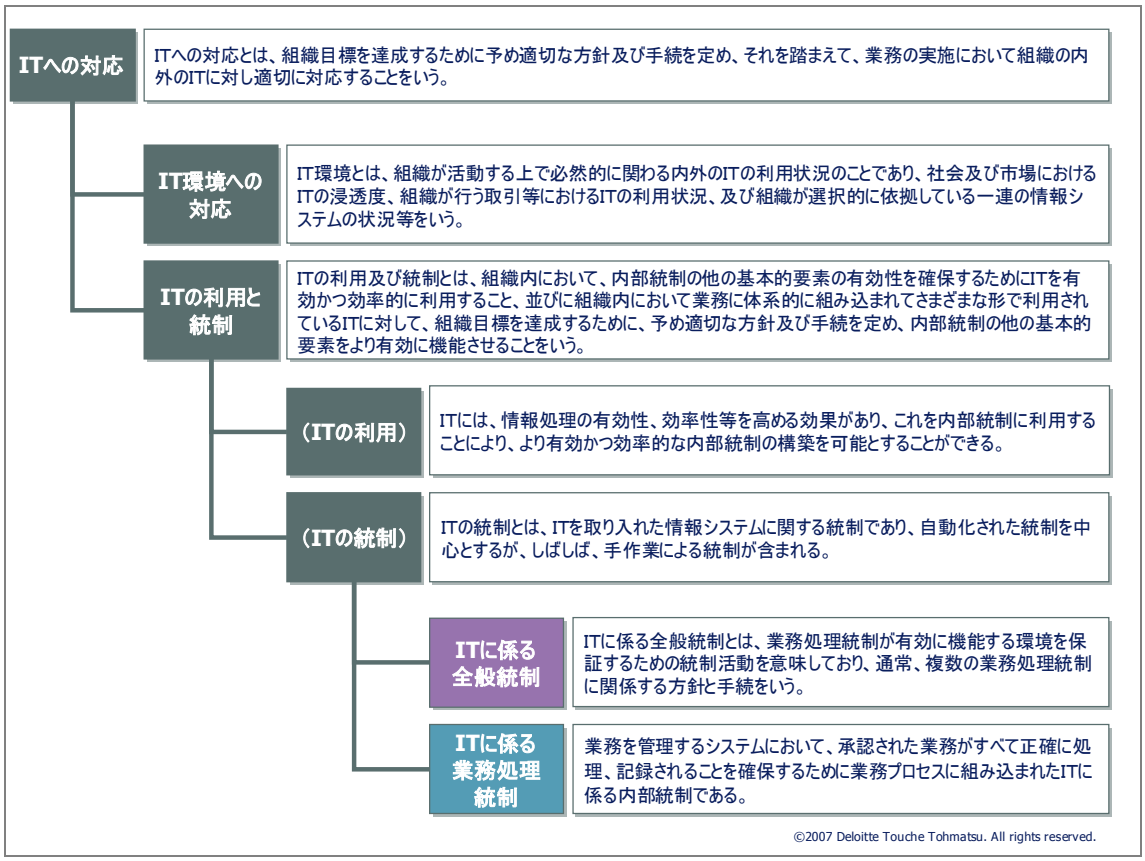


図 3.24　IT への対応

財務報告に係る内部統制の評価に際しては、全社的内部統制として主に「IT の統制」以外の部分を評価し、業務プロセスに係る内部統制として「IT 全般統制」と「IT 業務処理統制」を評価することになる。

②IT 統制の評価

ここでは、業務プロセスに係る内部統制のうち IT の統制に関する評価について概説すること

にする。

会計システム、販売システムや購買システムといったアプリケーション・システムは、IT を活用して、効率的に運用されている。しかも、そのアプリケーション・システムに売掛債権の実在性を保証するような内部統制がプログラム化されて組み込まれている場合もある。例えば、あらかじめ顧客マスターに登録している顧客以外では販売処理ができない、一定金額以上の販売には課長の承認がなければ出荷指示が出せないようにシステム上制限されている場合がある。このようなプログラム化された統制（つまり、IT 業務処理統制）が有効に機能するためには、情報システムの開発、運用等が適切に行われていなければならない。このような IT 業務処理統制が有効に機能する環境を保証するための統制活動は IT 全般統制であるが、これが有効に整備され、運用されていることを評価しなければならない。

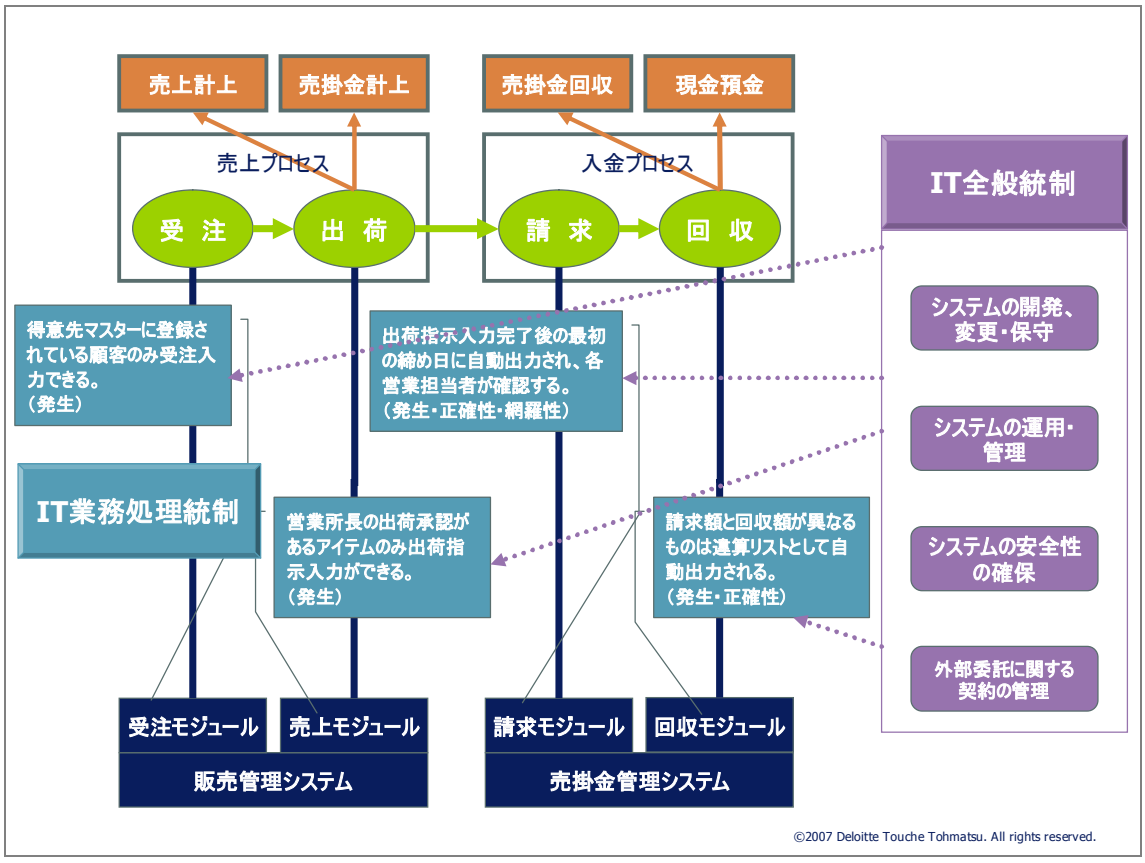


図 3.25　IT 統制の評価

③IT 全般統制の評価

IT 全般統制は、複数の業務プロセスについて共通の IT 処理環境があるため、それを共通して評価することが効率的である。例えば、汎用機を利用した開発手法、運用、保守については、販売システム、原価計算システム、購買システムともすべて同じであれば、販売システム、原価計算システム、購買システムそれぞれについて別々に評価するのではなく、同じ IT 処理環境として評価すればよい。このように IT 全般統制を評価する場合は、評価を効率的に行うために評価

単位を適切に設定することが重要となる。

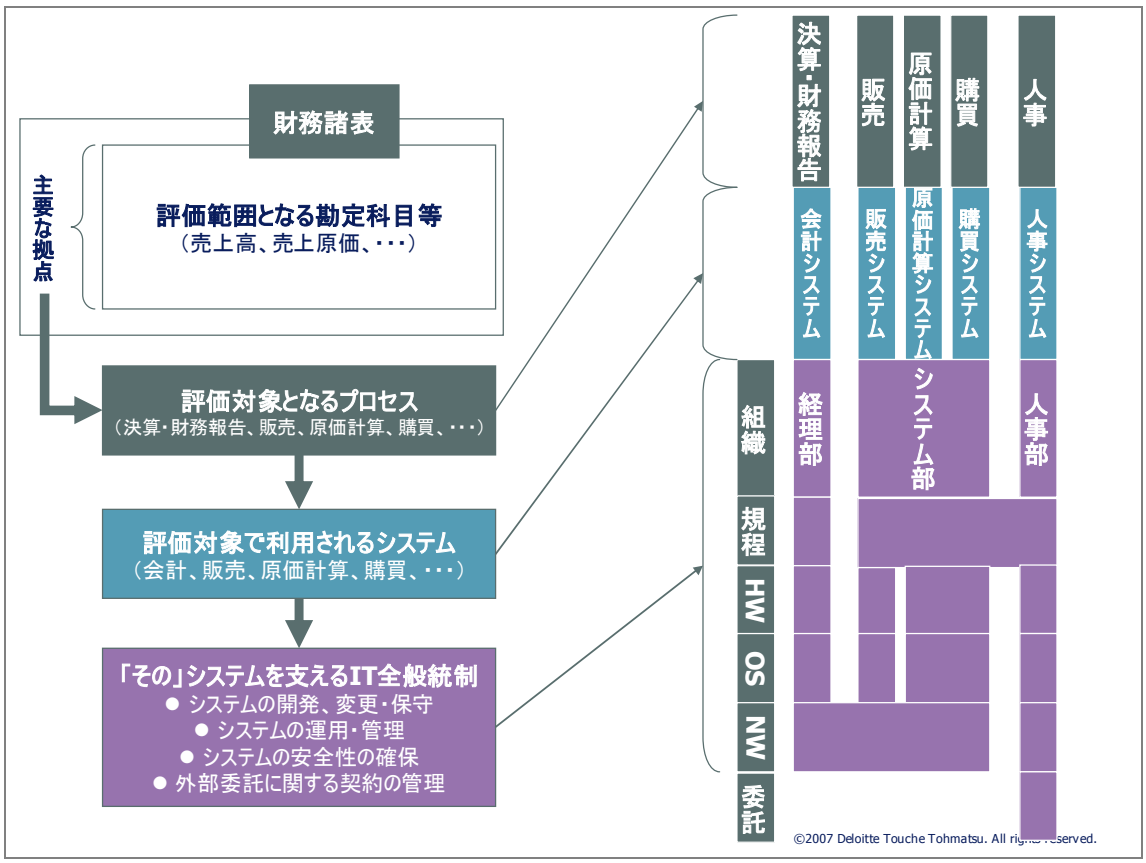


図 3.26　IT 全般統制の評価

④IT 全般統制の評価の視点

IT 全般統制の評価の視点は実施基準においては、第三部の監査の基準に記述されている。その概要については、図 3.27 のとおりである。

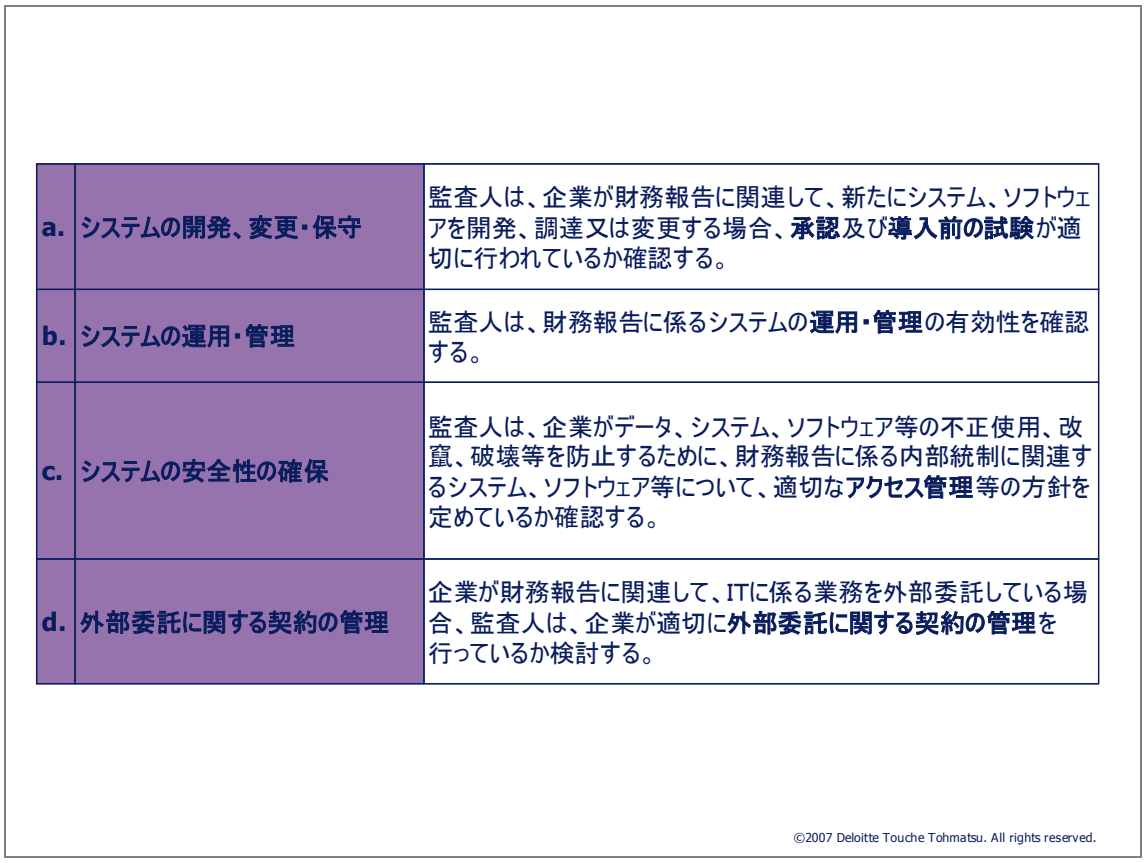


図 3.27　IT 全般統制の監査のポイントの例示

なお、「システムの開発、変更・保守」及び「システムの運用・管理」については、より具体的な評価のポイントが記述されている（表 3.2）。

表 3.2　システムの開発、変更・保守及びシステムの運用・管理の評価項目のポイント

	IT 全般統制の分野	評価上の留意点の例示
a.	**システムの開発，変更・保守**	監査人は，企業が財務報告に関連して，新たにシステム，ソフトウェアを開発，調達又は変更する場合，**承認**及び**導入前の試験**が適切に行われているか確認する。その際，監査人は，例えば，以下の点に留意する。 ● システム，ソフトウェアの開発，調達又は変更について，事前に経営者又は適切な管理者に**所定の承認**を得ていること ● 開発目的に適合した適切な**開発手法**がシステム，ソフトウェアの開発，調達又は変更に際して，適用されていること ● 新たなシステム，ソフトウェアの導入に当たり十分な**試験**が行われ，その結果が当該システム，ソフトウェアを**利用する部門の適切な管理者**及び**IT部門の適切な管理者により承認**されていること ● 新たなシステム，ソフトウェアの**開発，調達又は変更**について，その**過程が適切に記**

		録及び保存されるとともに，変更の場合には，変更前のシステム，ソフトウェアに関する内部統制の整備状況に係る記録が更新されていること ● 新たなシステム，ソフトウェアにデータを**保管又は移行**する場合に，**誤謬，不正等を防止する対策**が取られていること ● 新たなシステム，ソフトウェアを利用するに当たって，利用者たる従業員が適切な計画に基づき，**教育研修**を受けていること
b.	**システムの運用・管理**	監査人は，財務報告に係るシステムの**運用・管理**の有効性を確認する。その際，例えば，以下の点に留意する。 ● システムを構成する重要なデータやソフトウェアについて，障害や故障等によるデータ消失等に備え，その内容を**保存し，迅速な復旧**を図るための対策が取られていること ● システム，ソフトウェアに障害や故障等が発生した場合，**障害や故障等の状況の把握，分析，解決等**の対応が適切に行われていること

以上は、監査人が監査をする視点であるが、経営者もこれを意識して評価しなければならない点に注意にしなければならない。

3.2.4 情報セキュリティとの関係

(1) IT 全般統制と情報セキュリティ

さて、情報セキュリティ対策と内部統制の関係について考えてみよう。情報セキュリティとは、JIS Q 27001：情報技術－セキュリティ技術－情報セキュリティ・マネジメント・システム－要求事項によると次のように定義される。

情報の機密性，完全性及び可用性を維持すること。さらに，真正性，責任追跡性，否認防止及び信頼性のような特性を維持することを含めてもよい。

なお、機密性、完全性、及び可用性は以下のように定義される。

可用性；認可されたエンティティが要求したときに，アクセス及び使用が可能である特性 機密性；認可されていない個人，エンティティ又はプロセスに対して，情報を使用不可又は非公開にする特性 完全性；資産の正確さ及び完全さを保護する特性

簡単にいえば、情報セキュリティは、情報や情報システムの機密性、完全性、可用性が維持できなくなるというリスクをコントロールするものである。

一方、内部統制は、組織内部におけるリスクをコントロールすることであるといえる。情報セキュリティに係るリスクをコントロールという意味で情報セキュリティ対策は内部統制の一部ということになる。また、情報セキュリティのコントロールには情報の完全性を保証することも含

まれる。財務諸表に記載されている内容も情報である。したがって、財務報告に係る情報の完全性を保証することが財務報告に係る内部統制ともいえることから、情報セキュリティのうち完全性を保証するような対策は、財務報告に係る内部統制と深く関係してくることになる。主に関係するのは IT 全般統制のうち、「システムの安全性の確保」の部分である。財務情報及びそれを取り扱うシステムのプログラム等が承認なく変更等されないように適切なアクセスコントロールが必要となる。

このことは、既に情報セキュリティ・マネジメント・システム（以下、「ISMS」という。）などの認証取得をしている企業も多いと思うが、その活動も財務報告に係る内部統制の評価の際には活用できうることを意味している。また、反対に、既に ISMS 認証を取得している企業は、その ISMS に財務報告に係る内部統制により要求される事項を組み入れていかなければならないことを意味している。

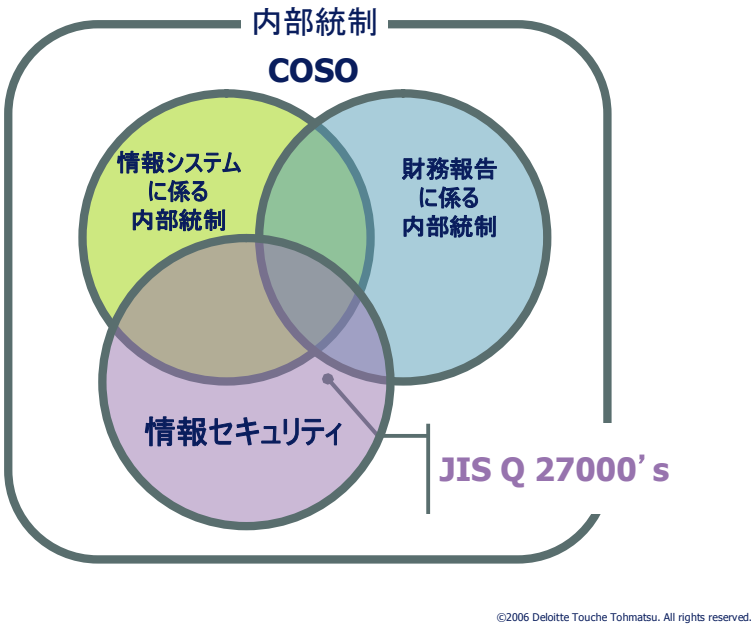


図 3.28　情報セキュリティと内部統制

(2) JIS Q 27001 付属書 A と財務報告に係る内部統制

情報セキュリティ・マネジメント・システムの要求事項である JIS Q27001 の付属書 A は管理策（すなわち、内部統制）のリストとなっている。このうち情報及び情報システムに関する完全性に係る部分が、財務報告に係る内部統制に関係しうることになる。その関係について、以下の考え方に基づいて対応を考えてみた。

マッピングにあたりまず、財務報告に係る内部統制との関連性の深さに基づいて判断し、関連性がほとんどないと思われるものを「－」とした。次に、関連性があると考えられるものを３段階に区分した。多くの場合評価の対象となりうると考えた項目を「●」に、財務報告に係る業務

プロセスにおいて IT の利用程度が高い場合評価の対象となりうると考えた項目を「◎」に、財務報告に係る業務プロセスにおいて IT の利用程度又は他の統制が有効でない場合の代替的な統制として評価の対象となりうると考えた項目を「○」とした。

内部統制の基本的要素との関係については、次の考え方によった。すなわち、統制環境には、倫理観、組織構造、責任と権限、教育・訓練等に関する項目を、リスクの評価と対応には、目的や方針の設定、リスクの評価に関する項目を、情報と伝達には、外部・内部への報告、調整等に関する項目を、モニタリングには、その他の内部統制の有効性をレビューすることに関する項目が該当するものとして割り当てた。

表中の「環」、「リ」、「活」、「伝」、「モ」は、それぞれ内部統制の基本的要素の、「統制環境」、「リスク評価と対応」、「統制活動」、「情報と伝達」及び「モニタリング」を表している。

なお、分類及び内部統制の基本的要素との関係付けは、筆者の私見に基づくものである。また、関係が深い場合であっても、そもそも財務報告の信頼性を確保する観点からその情報システムの重要性が高くない場合は評価する必要がないことに留意しなければならない。

表 3.3　JIS Q27001　付属書 A の項目と内部統制の基本的要素との関係

JIS Q 27001 付属書 A				環	リ	活	伝	モ
A.5	セキュリティ基本方針							
	A.5.1	情報セキュリティ基本方針						
		A.5.1.1	情報セキュリティ基本方針文書		◎			
		A.5.1.2	情報セキュリティ基本方針のレビュー					◎
A.6	情報セキュリティのための組織							
	A.6.1	内部組織						
		A.6.1.1	情報セキュリティに対する経営陣の責任	○				
		A.6.1.2	情報セキュリティの調整				○	
		A.6.1.3	情報セキュリティ責任の割当て	○				
		A.6.1.4	情報処理設備の認可プロセス			○		
		A.6.1.5	密保持契約				—	
		A.6.1.6	関係当局との連絡				○	
		A.6.1.7	専門組織との連絡				—	
		A.6.1.8	情報セキュリティの独立したレビュー					●
	A.6.2	外部組織						
		A.6.2.1	外部組織に関係したリスクの識別		○			
		A.6.2.2	顧客対応におけるセキュリティ			—		
		A.6.2.3	第三者との契約におけるセキュリティ			—		
A.7	資産の管理							
	A.7.1	資産に対する責任						
		A.7.1.1	資産目録		○			

		A.7.1.2	資産の管理責任者	○				
		A.7.1.3	資産利用の許容範囲		○			
	A.7.2	情報の分類						
		A.7.2.1	分類の指針		○			
		A.7.2.2	情報のラベル付け及び取扱い		○			
A.8	人的資源のセキュリティ							
	A.8.1	雇用前						
		A.8.1.1	役割及び責任	○				
		A.8.1.2	選考			○		
		A.8.1.3	雇用条件			○		
	A.8.2	雇用期間中						
		A.8.2.1	経営陣の責任	◎				
		A.8.2.2	情報セキュリティの意識向上，教育及び訓練	◎				
		A.8.2.3	懲戒手続	○				
	A.8.3	雇用の終了又は変更						
		A.8.3.1	雇用の終了又は変更に関する責任	—				
		A.8.3.2	資産の返却			—		
		A.8.3.3	アクセス権の削除			●		
A.9	物理的及び環境的セキュリティ							
	A.9.1	セキュリティを保つべき領域						
		A.9.1.1	物理的セキュリティ境界			○		
		A.9.1.2	物理的入退管理策			◎		
		A.9.1.3	オフィス，部屋及び施設のセキュリティ			○		
		A.9.1.4	外部及び環境の脅威からの保護			○		
		A.9.1.5	セキュリティを保つべき領域での作業			—		
		A.9.1.6	一般の人の立寄り場所及び受渡場所			—		
	A.9.2	装置のセキュリティ						
		A.9.2.1	装置の設置及び保護			—		
		A.9.2.2	サポートユーティリティ			—		
		A.9.2.3	ケーブル配線のセキュリティ			—		
		A.9.2.4	装置の保守			—		
		A.9.2.5	構外にある装置のセキュリティ			—		
		A.9.2.6	装置の安全な処分又は再利用			—		
		A.9.2.7	資産の移動			—		
A.10	通信及び運用管理							
	A.10.1	運用の手順及び責任						

		A.10.1.1	操作手順書			●		
		A.10.1.2	変更管理			●		
		A.10.1.3	職務の分割			●		
		A.10.1.4	開発施設，試験施設及び運用施設の分離			○		
	A.10.2	第三者が提供するサービスの管理						
		A.10.2.1	第三者が提供するサービス			●		
		A.10.2.2	第三者が提供するサービスの監視及びレビュー					●
		A.10.2.3	第三者が提供するサービスの変更に対する管理			●		
	A.10.3	システムの計画作成及び受入れ						
		A.10.3.1	容量・能力の管理			○		
		A.10.3.2	システムの受入れ			●		
	A.10.4	悪意のあるコード及びモバイルコード3)からの保護						
		A.10.4.1	悪意のあるコードに対する管理策			○		
		A.10.4.2	モバイルコードに対する管理策			○		
	A.10.5	バックアップ						
		A.10.5.1	情報のバックアップ			◎		
	A.10.6	ネットワークセキュリティ管理						
		A.10.6.1	ネットワーク管理策			◎		
		A.10.6.2	ネットワークサービスのセキュリティ			◎		
	A.10.7	媒体の取扱い						
		A.10.7.1	取外し可能な媒体の管理			—		
		A.10.7.2	媒体の処分			—		
		A.10.7.3	情報の取扱手順			◎		
		A.10.7.4	システム文書のセキュリティ			◎		
	A.10.8	情報の交換						
		A.10.8.1	情報交換の方針及び手順			◎		
		A.10.8.2	情報交換に関する合意			◎		
		A.10.8.3	配送中の物理的媒体			○		
		A.10.8.4	電子的メッセージ通信			●		
		A.10.8.5	業務用情報システム			●		
	A.10.9	電子商取引サービス						
		A.10.9.1	電子商取引			●		
		A.10.9.2	オンライン取引			●		
		A.10.9.3	公開情報			●		
	A.10.10	監視						
		A.10.10.1	監査ログ取得			●		

		A.10.10.2	システム使用状況の監視			○		
		A.10.10.3	ログ情報の保護			●		
		A.10.10.4	実務管理者及び運用担当者の作業ログ			◎		
		A.10.10.5	障害のログ取得			◎		
		A.10.10.6	クロックの同期			○		
A.11	アクセス制御							
	A.11.1	アクセス制御に対する業務上の要求事項						
		A.11.1.1	アクセス制御方針			●		
	A.11.2	利用者アクセスの管理						
		A.11.2.1	利用者登録			●		
		A.11.2.2	特権管理			●		
		A.11.2.3	利用者パスワードの管理			●		
		A.11.2.4	利用者アクセス権のレビュー			●		
	A.11.3	利用者の責任						
		A.11.3.1	パスワードの利用			●		
		A.11.3.2	無人状態にある利用者装置			—		
		A.11.3.3	クリアデスク・クリアスクリーン4)方針			—		
	A.11.4	ネットワークのアクセス制御						
		A.11.4.1	ネットワークサービスの利用についての方針			◎		
		A.11.4.2	外部から接続する利用者の認証			●		
		A.11.4.3	ネットワークにおける装置の識別			◎		
		A.11.4.4	遠隔診断用及び環境設定用ポートの保護			◎		
		A.11.4.5	ネットワークの領域分割			◎		
		A.11.4.6	ネットワークの接続制御			◎		
		A.11.4.7	ネットワークルーティング制御			◎		
	A.11.5	オペレーティングシステムのアクセス制御						
		A.11.5.1	セキュリティに配慮したログオン手順			●		
		A.11.5.2	利用者の識別及び認証			●		
		A.11.5.3	パスワード管理システム			●		
		A.11.5.4	システムユーティリティの使用			●		
		A.11.5.5	セッションのタイムアウト			◎		
		A.11.5.6	接続時間の制限			◎		
	A.11.6	業務用ソフトウェア及び情報のアクセス制御						
		A.11.6.1	情報へのアクセス制限			●		
		A.11.6.2	取扱いに慎重を要するシステムの隔離			◎		
	A.11.7	モバイルコンピューティング及びテレワーキング5)						

		A.11.7.1	モバイルのコンピューティング及び通信			●		
		A.11.7.2	テレワーキング			◎		
A.12	情報システムの取得，開発及び保守							
	A.12.1	情報システムのセキュリティ要求事項						
		A.12.1.1	セキュリティ要求事項の分析及び仕様化			◎		
	A.12.2	業務用ソフトウェアでの正確な処理						
		A.12.2.1	入力データの妥当性確認			●		
		A.12.2.2	内部処理の管理			●		
		A.12.2.3	メッセージの完全性			●		
		A.12.2.4	出力データの妥当性確認			●		
	A.12.3	暗号による管理策						
		A.12.3.1	暗号による管理策の利用方針			◎		
		A.12.3.2	かぎ（鍵）管理			○		
	A.12.4	システムファイルのセキュリティ						
		A.12.4.1	運用ソフトウェアの管理			●		
		A.12.4.2	システム試験データの保護			—		
		A.12.4.3	プログラムソースコードへのアクセス制御			●		
	A.12.5	開発及びサポートプロセスにおけるセキュリティ						
		A.12.5.1	変更管理手順			●		
		A.12.5.2	オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー			◎		
		A.12.5.3	パッケージソフトウェアの変更に対する制限			◎		
		A.12.5.4	情報の漏えい			—		
		A.12.5.5	外部委託によるソフトウェア開発			●		
	A.12.6	技術的ぜい弱性管理						
		A.12.6.1	技術的ぜい弱性の管理			○		
A.13	情報セキュリティインシデントの管理							
	A.13.1	情報セキュリティの事象及び弱点の報告						
		A.13.1.1	情報セキュリティ事象の報告				◎	
		A.13.1.2	セキュリティ弱点の報告				◎	
	A.13.2	情報セキュリティインシデントの管理及びその改善						
		A.13.2.1	責任及び手順			◎		
		A.13.2.2	情報セキュリティインシデントからの学習	○				
		A.13.2.3	証拠の収集			◎		
A.14	事業継続管理							
	A.14.1	事業継続管理における情報セキュリティの側面						

		A.14.1.1	事業継続管理手続への情報セキュリティの組込み		—			
		A.14.1.2	事業継続及びリスクアセスメント		—			
		A.14.1.3	情報セキュリティを組み込んだ事業継続計画の策定及び実施			—		
		A.14.1.4	事業継続計画策定の枠組み			—		
		A.14.1.5	事業継続計画の試験，維持及び再評価			—		
A.15	順守							
	A.15.1	法的要求事項の順守						
		A.15.1.1	適用法令の識別		—			
		A.15.1.2	知的財産権（IPR）			—		
		A.15.1.3	組織の記録の保護			●		
		A.15.1.4	個人データ及び個人情報の保護			—		
		A.15.1.5	情報処理施設の不正使用防止			○		
		A.15.1.6	暗号化機能に対する規制			—		
	A.15.2	セキュリティ方針及び標準の順守，並びに技術的順守						
		A.15.2.1	セキュリティ方針及び標準の順守					◎
		A.15.2.2	技術的順守の点検					◎
	A.15.3	情報システムの監査に対する考慮事項						
		A.15.3.1	情報システムの監査に対する管理策			◎		
		A.15.3.2	情報システムの監査ツールの保護			◎		

3.2.5 制度対応後のポイント

多くの上場企業では、財務報告に係る内部統制の評価と監査の制度の導入に向けた準備を始めているところであろう。この制度の適用が 2008 年 4 月 1 日開始事業年度の決算日であることから、対応の時間も十分ではなく、効率的な制度対応の重要性を認識しつつも、内部統制の不備の是正及び評価体制の構築に自体を優先しているために、効率的な評価をするための準備が十分にできていないと思われる。これは、米国の場合も同様であり、導入２年目以降に効率的な評価を考慮した改善に取り組んでいく例が多いようである。そこで、ここでは評価の効率性及び経営の有効性を高めるという２つの視点から、制度導入後の課題をまとめておく。

(1) 効率的な評価のために（１）集中化、標準化とモジュール化

内部統制の評価を効率的に行うためには、評価単位をできる限りすくなくすることが効果的である。そのためには、業務プロセスや内部統制をできる限り標準化しておく必要がある。また、あらたな業務プロセスを導入する際にも一から内部統制を設計するのではなく、すでにある内部統制の手法を使いまわしできるようにしておく必要がある。例えば、ERP の導入やアイデンティティ管理の集中化という手法の活用が有効といえる。また、システム開発手法、システムリリー

ス手続、システムの運用等を標準化することもまた有効である。

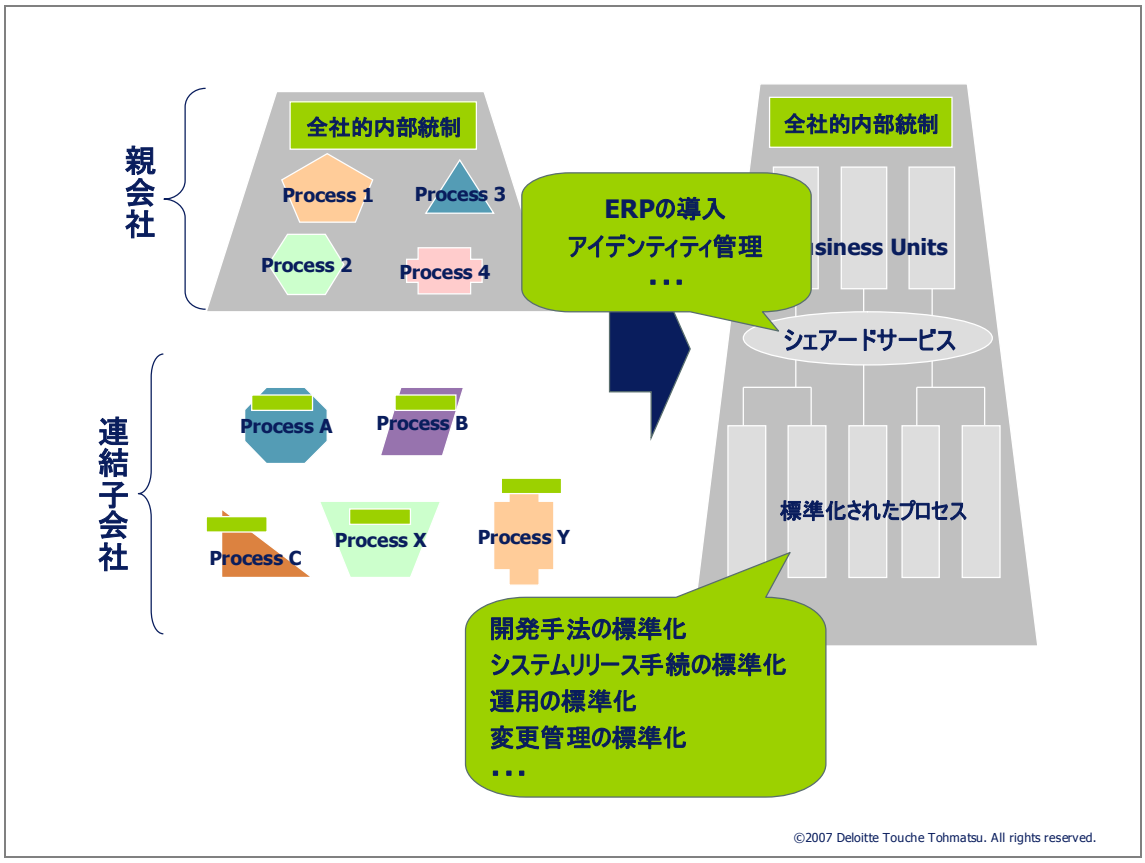


図 3.29　集中化、標準化及びモジュール化

(2) 効率的な評価のために（2）IT の活用

IT を利用して自動化された内部統制は、実施基準では、一度内部統制が設定されると、変更やエラーが発生しない限り一貫して機能するという性質があるため、年度に内部統制の不備が発見されずに有効に運用されていると評価された場合、評価された時点から内部統制が変更されてないこと、障害･エラー等の不具合が発生していないこと、及び関連する全般統制の整備及び運用の状況を確認及び評価した結果、全般統制が有効に機能していると判断できる場合には、その結果を記録することで、当該評価結果を継続して利用することができるとされている。したがって、IT 業務処理統制等は、IT 全般統制の評価をすることにより基本的には過年度の結果を利用して運用テストを省略することが可能となるために、サンプル数が減少し、効率的な評価につながる。例えば、日々行われる多数の承認を手で行っている場合で、運用状況の評価として毎年 25 件のサンプルを評価している場合、サンプル 1 件あたりの評価作業が 30 分であれば、1 つの内部統制あたりの評価時間に 12.5 時間かかっていることになる。このような内部統制が 100 あれば 1250 時間かかっていることになる。IT で置き換えられるとすると年間 1250 時間の節約となる。

(3) リスクマネジメントとの融合

この制度の導入で期待されるもっとも大きな効果は、内部統制の評価基盤ができることである。

この制度での評価の対象は財務報告の信頼性に関係する部分のみであるが、企業グループ全体に内部統制の評価の基盤ができることになる。この基盤にのせて評価する対象を財務報告の信頼性に関係する部分からコンプライアンス、業務の有効性及び効率性を高めること等に拡張していくことにより、グループ全体のリスクマネジメント体制を構築していくことができる。

社長が知らないところで、社長の意に反して談合等の不正が行われていないことを確かめるための基盤ができる意義は大きい。今回の制度の導入には多額のコストが係るのは避けられない。しかし、この制度で構築させるグループ全体に及ぶ内部統制の基盤を活用して、コンプライアンス経営の強化、その他のリスクマネジメントへの拡張を図ることにより基盤に投資した費用は回収できるはずである。その中に情報セキュリティに関する項目もいれることができる。それができれば、グループ企業全体としての情報セキュリティガバナンスを確立することができるだろう。

3.2.6 おわりに

財務報告に係る内部統制の評価と監査の制度の導入が 2008 年 4 月 1 日開始事業年度より始まることはすでに確定している。まずは目先の制度対応が重要であることには違いない。そのためには、制度内容をよく理解して対応することが重要である。一方、個人情報保護法の対応等により情報セキュリティ対策が強化されている上場企業も多いであろう。そのような上場企業の場合は、その基盤がある程度今回の制度でも利用できるであろう。しかし、今回の制度は財務報告の信頼性を確保するための制度であるが、この制度で確立した内部統制の基盤を活用して、情報セキュリティガバナンスを確立することが重要といえるであろう。

3.3 企業にとってのメールのリスクとその対策

3.3.1 はじめに

私は IAjapan の迷惑メール対策委員会1に参加しておりまして、その迷惑メール対策委員会を代表といっては僭越ですけれども、今日は迷惑メールに限らずメールのリスクについてお話ししたいと思います。

内容は４部構成になっておりまして、最初にメールにかかわる素朴な疑問について考えてみます。企業に属している社員が私用メールを使ってしまった。これは余りリスクとは直接は関係がないのですけれども、それが許されるのかどうかということ。皆さんはあまりクリアではない状態で使っていらっしゃると思いますので、そういった素朴な疑問についてまずお話ししたいと思います。

それから、本題のメールに関するリスクについて、3 つにまとめています。まず、「情報漏洩」です。それから、「メールアドレスの詐称」。これも避けて通れない問題で、携帯電話では難しいですが､インターネットのメールはとても簡単です｡これを悪用した犯罪も起こっていますので、どうやって防止するかについて説明していきたいと思います。3 つめが「迷惑メール」です。たくさんの迷惑メールが届いていまして、今年も急増していますので、これも少し考えてみたいと思います。

本報告の内容は、私がプログラム委員を務めた Email Security Conference2で議論された内容を踏まえています。この中で、法律関係は高橋弁護士（IT 法律事務所）3からたくさん有益な情報をいただいており、今日の法律関係のお話は、それを踏まえていることをあらかじめご了承ください。

3.3.2 素朴な疑問

(1) 社員のプライバシと権利

社員のプライバシと権利ということで、私用メールは許されるのかということです。他の会社の友達に、今日飲みに行かないかというメールを書いたとしたら、これは違法なのかということなのですが、これは許されています。ただし、常識的な範囲に限るという但し書きが付きます。

常識的な範囲とは、就業規則等に「就業中は私用メールを使ってはならない」といった特段の定めがなく、メールを書いていたとしても業務遂行のために支障とならない程度で使っているということ。つまり、会社に過度の負担をかけていないといことがクリアされるのであれば、私用メールは許されるということです。

高橋弁護士の言葉を借りると、これは息抜きのお茶と同じということになります。大抵の場合、お茶は会社が買ってくれているし、それを飲むという機会もあるはずです。そうしたところで会社に怒られるということはない、だから、常識的な範囲であれば私用メールは許されています。

---

1 http://www.iajapan.org/anti_spam/

2 2006 年 11 月 28 日、29 日に開催された Email 運用におけるセキュリティ対策に特化した専門イベント

3 http://www.comit.jp/

これについては、グレイワールドワイド事件4という裁判が起きています。日に数通のメールを書いていた女子社員が、それは会社にとって迷惑はかけていないのでそれで罰することはおかしいという判例が出ていますので、皆さん安心して使ってください。

(2) 企業の権利

会社の権利として社員のメールをモニタリングするのは合法かということですが、これは合法です。これにもやはり常識的な範囲ではという但し書きがついていて、特定の企業秩序違反の疑いがある人に対してモニタリングするということは合法ということになります。逆にいいますと、社員全員を何の疑いもないのにモニタリングしてしまうとこれは違法になってしまいます。判例としては、日経クイック事件とフィッシャー社事件5というのが出ています。

また、厚生労働省や経済産業省から社員のモニタリングに関わるガイドライン6が出ています。高橋弁護士によれば、私用メールもモニタリングも、用法と用量を守っている限り問題はないということです。

(3) 証拠としてのメール

メールに証拠能力があるか。これも SOX 法との関連で興味があるところではないかと思います。

「証拠能力」とは、法的には証拠の方法として用いることが可能か、裁判官が目にすることができるかということなので、メールは保存しておけば証拠能力があるということになります。これに対して、我々が証拠能力と思っているのは実は「証明力」です。事実認定に役立つ度合いのことを証明力といいます。

記録として保存しているのであれば、メールには証拠能力はあります。SOX 法では保存しておけばよくて、検索する作業は他に任せてよいことになっています。アメリカにはディスカバリーサービスプロバイダという職業もあります。また、第三者が保存しているなら証明力は高いですが、当事者が保存している場合は裁判官の判断にゆだねられるということになります。

3.3.3 企業にとってのメールのリスク

次に、企業にとってのメールのリスク、情報漏洩とアドレス詐称、それから迷惑メールについて考えます。

- ■ 情報漏洩：ウイルスによるまき散らし、内部犯行、宛先間違い
- ■ アドレス詐称：フィッシング（高度な詐欺）、虚偽情報の流布

---

[4] 東京地判平 15.9.22 労判 870-83）

[5] インターネット協会第 11 回セキュリティフォーラム資料 31 ページ
<http://www.iajapan.org/bukai/isec/forum/2002/20021107koushi1.pdf>

[6] 労働者の個人情報保護に関する研究会報告書
<http://www2.mhlw.go.jp/kisya/daijin/20001220_01_d/20001220_01_d.html>
経済産業省の個人情報ガイドラインについて
<http://www.meti.go.jp/policy/it_policy/privacy/kojin_gadelane.htm>

■ 迷惑メール：大切なメールの見落とし、受信サーバのマヒ、迷惑メールの送信

(1) 基本的な対策

お手持ちの PC に「ウイルス検疫ソフト」を入れることよって、大切なファイルがウイルスによってまき散らされてしまうということを防止します。それから、メールの送受信サーバには、「ウイルスフィルタ」を入れます。受け取るほうにはウイルスフィルタを入れているが、送るほうに入れていないという企業もあると思いますので、帰られてからチェックされたほうがよろしいかと思います。

受信サーバには、大切なメールの見落しを防止するために迷惑メールフィルタを入れます。それから、受信サーバで「通数制限」を行ないます。これによって、大量の迷惑メールを送りつけられることによって、受信サーバが麻痺するということを防止します。

これ（図 3.30）は「Outbound Port 25 Blocking、略して OB25B」といいます。正式な送信サーバからメールが出て行く場合は OK だけれども、それ以外の PC からは出さないようにフィルタリングしてしまうという技術です。これによって社内から迷惑メールを送られるということを防止するということですが、多くの企業には、ファイアウォールという形でこのフィルタリングはすでに設置されています。

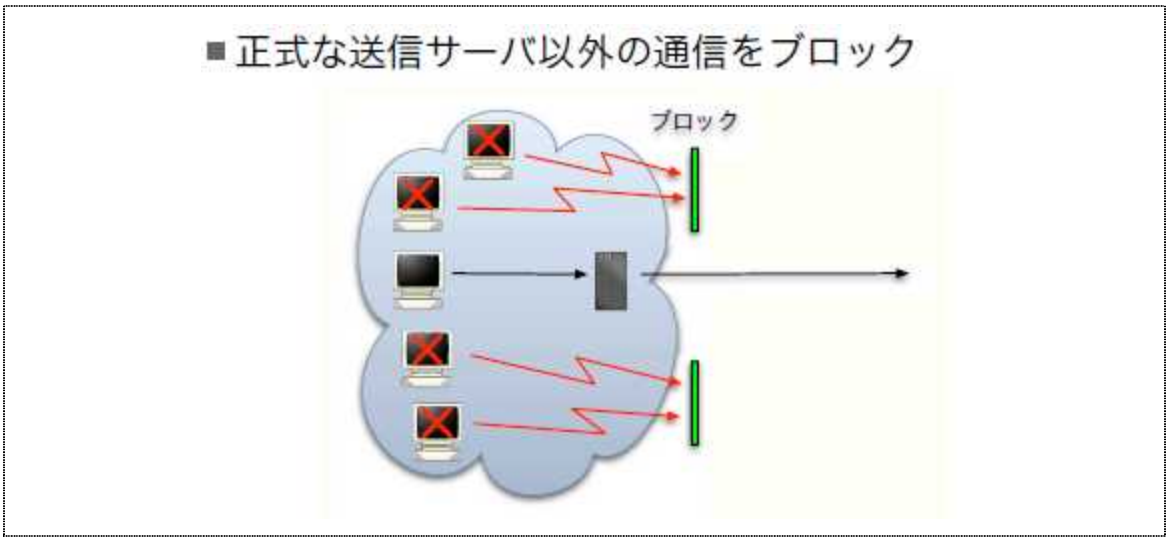


図 3.30 Outbound Port 25 Blocking (OP25B)

(2) 情報漏洩

①内部犯行

内部犯行ですが、これは悪意をもって社内の人が情報を漏洩してしまうという問題です。

高橋弁護士はヤフーBB の情報漏洩事件を取りあげました。この裁判では、注意義務違反ということになりました。データベースにアクセスするパスワードの管理が不十分で、外部からそのデータにアクセスできてしまった。外部から不正アクセスを防止するための措置を怠ったということで、注意義務違反を問われました。

こういうことを守る指針として「最小権限」という鉄則[7]があるのですが、これを守っていないということが問題です。弁護士の視点では、これからの企業はメールのリスクに対しても注意義務を問われる時代になっていくのではないかと推測されるそうです。どういうことに気を付けなくてはいけないかというと、辞めた社員のアカウントはすぐに消去するとか、社外からのメール利用を制限するなどメールアカウントの管理です。メールで受け取った見積書を社外からアクセスするということは、これからは許されないかもしれません。

②宛先間違い

悪意はなくともメールアドレスを間違って情報漏洩してしまうという問題について考えます。幾つかの会社に聞いてみたところ、これが情報漏洩の一番の原因だということです。

例えば、宛先のメールアドレスを入れるとき、一部だけ入れて補完してしまう。自分はAというアドレスを入れたつもりなのに、Aダッシュになってしまい違うところに送られている。それから、Bcc すべきところをうっかり Cc して、誰に送ったかを漏洩してしまうというようなことです。これからは注意義務違反を負う可能性があります。

こういったことに対してどういった対策があるかといいますと、既にこういった技術対策を組み込んだ製品というのは出てきているのですが、ユーザに「アドレス帳の使用を強要」します。つまり、アドレスは最初に一回入力するだけ、それ以降はアドレス帳から選んで使う。補完は絶対にしないということが、これからは必要になってくるかもしれません。

それから「送信先制御」です。これは社員ごとに送れる宛先というものを制限してしまうということです。この技術ももうできていますので、納入している会社があるかもしれません。

それから、「送信メールの内容フィルタ」です。外部に社外秘というような文字列を含んだメールというのが出て行くことが絶対にあってはならないので、そういった内容を見て、社外秘というような文字列を見つけたら止めてしまうという技術も実はもうできています。製品やサービスを買えばできるわけですが、こういったことが必要になってきます。

それから、「遅延配信」です。メールはなるべく早く届かなければいけないといような考え方もあるとは思うのですけれども、メールというものは送った瞬間に、「あ、間違った」と気付くことも多いかと思います。送ってもサーバから 5 分間は出さないというような対策を講じることによって、5 分程度だったら許される範囲だと思いますので、5 分以内に気付けばやり直しや取り消しが効くというような対策も必要かもしれません。

(3) アドレス詐称

次に、アドレス詐称の問題について考えてみたいと思います。アドレス詐称を巧みに利用した詐欺をフィッシングというのですけれども、フィッシング・メールは迷惑メールの一部です。フィッシングというのは釣るという意味です。フィッシングの「釣る」という意味には、だますという意味もあるそうですので、高度な詐欺を行うメールをフィッシング・メールといいます。

---

[7] Need to Know

①フィッシング・メール

これ（図 3.31）は、実際に私が受け取ったフィッシング・メールですが、UFJ 銀行を騙ったものです。アドレスを詐称して、本文は UFJ 銀行がお客様に送っているような内容になっています。大体パターンは一緒なのですけれども、セキュリティを向上したいのでアカウントを管理してくださいみたいなことが書いてあるわけです。ここには、ufjbank.co.jp と書かれていますので、大抵の人は、ここをクリックすれば UFJ 銀行に飛ぶのだと思うわけです。ぼくは専門家ですので、これはフィッシングだと分かっていますが、やはりクリックするときはドキドキします。クリックしてみるとこういったサイト（図 3.32）に飛びます。


UFJ銀行

こたえていくチカラ。

UFJ銀行ご利用のお客様へ

UFJ銀行のご利用ありがとうございます。
このお知らせは、UFJ銀行をご利用のお客様に発送しております。

この度、UFJ銀行のセキュリティーの向上に伴いまして、
オンライン上でのご本人確認が必要となります。

この手続きを怠ると今後のオンライン上での操作に支障をきたす恐れがありますので、一刻も素早いお手続きをお願いします。

https://www.ufjbank.co.jp/ib/login/index.html

また、今回のアップデートには多数のお客様からのアクセスが予想されサーバーに負荷がかかるため、下記のミラーサイトを用意しております。上記のリンクが一時期不可能になっている場合は、下記をご利用ください。

https://www.ufjbank.co.jp/ib/login/index2.html

https://www.ufjbank.co.jp/ib/login/index3.html

お客様のご協力とご理解をお願いいたします。

UFJ銀行

図 3.31 フィッシング・メール

皆さん、これが高度な詐欺をしている、つまり皆さんをだまそうとしているページだということを見抜けますか。実はこれはある時点での UFJ 銀行のホームページをコピーして作られていますので、全く一緒です。実際に UFJ バンクに飛んでみても、このフィッシング・サイトを見ても全く同じなのです。初心者というか、普通の利用者の方には見抜けません。専門家が怪しいと思うのは、多くの人は見ないと思いますけれども、このアドレスバーとか URL バーとかいわれているところがありますけれども、ここに「ufjbank」とは書かれていなくて、IP アドレスが出ているということです。

ですから、https://www.ufjbank.co.jp/ib/login/index.html をクリックして、後にここを見ればおかしいとわかるのですけれども、大抵の人は見ないので思わない。ここに何か入れてログインすると、いよいよフィッシングのページ（図 3.33）になりまして、「こういったものを入力してください。あなたのセキュリティが向上します」というふうにうたっているわけです。

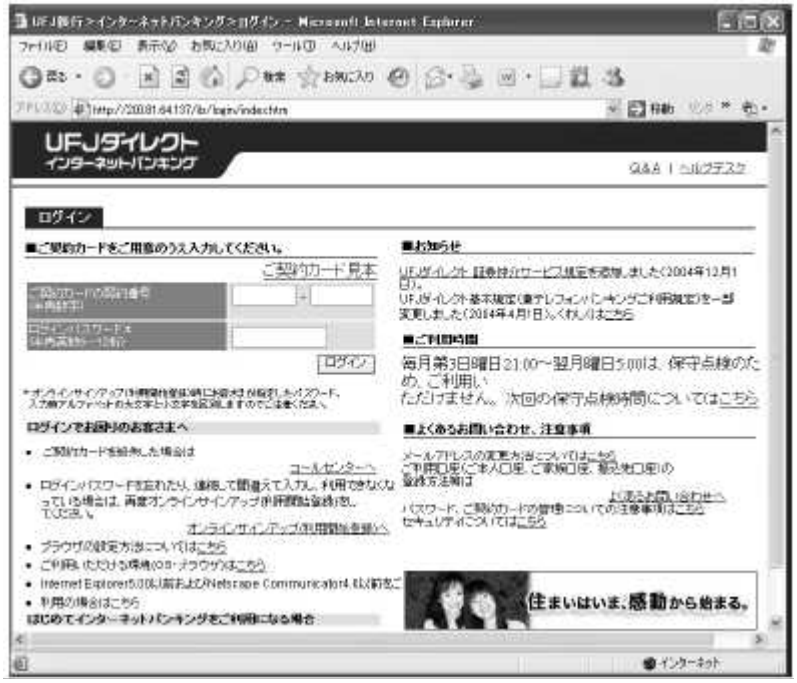


図 3.32　フィッシング・サイト

当然、入れますといろいろ番号を取られて、パスワードも取られます。取られてしまうとあとは他の人が、悪い人があなたのアカウントから、銀行口座からお金をどこかに転送してしまう。パスワードを盗まれますから。こういうことをやるわけです。これがフィッシングの典型的な例です。

図 3.33　フィッシングのページ

②フィッシングへの対処

幸いなことに日本では、フィッシングの被害というのはまだあまり起こっていません。なぜ起こらないかというと、ある分析によれば日本にはもっと効率よく稼げる詐欺があるからです。そうです、振り込め詐欺があるので、フィッシングというのはこういうふうにいろいろな作業が必要で、いろいろなサーバを用意したりしないといけないので、手間ひまがかかるのです。ですから、詐欺する人もコストパフォーマンスというのを考えますので、よりコストが少なくて稼げる口があればそちらを使うのです。

もし、振り込め詐欺が、これから銀行 10 万円以上振り込ませないといような対策を取りますと、フィッシングというものがはやってくるかもしれません。アメリカやブラジルではもうすごい被害が起きています。

皆さんは、まだフィッシングに遭うことはないかもしれませんけれども、かなりフィッシングに対する対策というのは進められておりまして、是非これを覚えてお帰りください。こういったフィッシングを見つけたらどうすればよいかというと、日本にはフィッシング対策協議会[8]というのがあります。この URL にいっていただくとページが見られますけれども、そこには事例一覧もありまして、先ほどの UFJ 銀行の例も載っていました。日本では現時点で見つかったもので 30～40 くらいの事例が載っていたと思いますので、興味がある場合は見てください。実は皆さんの会社を騙ったフィッシングの例というのが見つかるかもしれません。

それから、フィッシングで被害に遭ったらどうするのかとよく聞かれるのですけれども、警察にフィッシング 110 番[9]というのがあります。各県の警察の電話窓口が書かれていますので、もしフィッシングで被害があったときはそこに相談してくださるといいと思います。

警察の対策としてはすごく画期的でして、すぐに動けるのです。通報するとすぐに動いてくれます。どういった理由で警察が動けるかといいますと、まず、業務妨害罪です。明らかに業務を妨害しているので、そういった理由で調査を始められる。それから、先ほども見て明らかなように著作権を侵していますから、著作権法違反ということで警察が動いてくれます。何に比べてこれは画期的であるといっているのかというのは後ほど分かると思います。

③アドレス詐称の法的な位置付け

さて、フィッシングのメールというのはアドレスを詐称しているわけですけれども、アドレス詐称の法的な位置付けというのも明らかになっています。日本には迷惑メールに対する法律として、特定電子メール送信適正化法[10]というものがございます。多分、皆さん名前はご存じないと思いますけれども、いわゆる「未承諾広告」というのが一時期はやったと思います。ダイレクトメールを出す場合、宣伝のメールを出す場合は、必ず未承諾広告というのを件名に入れましょうというのを定めている法律です。これは、2002 年 7 月に施行されまして、どういうことを目的に

8 STOP!フィッシング詐欺 <http://www.antiphishing.jp/>
9 <http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm>
10 特定電子メールの送信の適正化等に関する法律
<http://www.soumu.go.jp/joho_tsusin/top/meiwaku.html>

していたかというと、ダイレクトメールを送るときのルールを作りましょう。それを守らないものは迷惑メールとして取り締まりましょうということだったわけです。

罰則が重要ですけれども、なんと違反した迷惑メールを出したら、相手がもし特定できれば総務省から警告メールがいくのです。それを無視した場合は措置命令。つまり業務停止命令がいき、場合によっては 50 万以下の罰金が科せられます。迷惑メールを送る人に警告メールを送るというのがこれで動くのかどうかかなり怪しいのですけれども、この 3 年間で措置命令の発出というのはたったの 3 件です。私は 1 日に数百通の迷惑メールを受け取っていますが、そういう時代なのに 3 年間でたったの 3 件です。

逮捕者の数はゼロです。まだまだこれは問題がありまして、少し専門用語になってしまいますけれども、SMTP というインターネットのメールを対象にしていましたので、携帯電話のショートメールサービス。これは対象外です。それから、個人宛だということを規定していましたので業務用のメーリングリスト <info@…>というのに来る迷惑メールは対象外だったわけです。それから、未承諾広告に限っていましたので、後ほど説明しますけれども本文はないけれども、他の攻撃に使うメールというのは迷惑メールとはされなかったわけです。

それで、これは明らかにザル法ですので、3 年の時限が切ってありまして必要があれば、改正しなさいということでしたので、もちろんあまり役に立っていませんでしたから改正されました。

2005 年に改正されて 11 月に施行され、問題点は改善されました。罰金は 50 万円から 100 万円に引き上げられました。先ほどフィッシングの捜査が画期的だったというのは、これまでの迷惑メールに対する法律では、警察が動く余地がなかったのです。しかし、フィッシングに対してはいきなり動けるというところが画期的で、今回の改正によって、迷惑メール一般に対しても警察が動けるようになりました。それは、直罰化ということを決めたからです。どういうことをしたら警察がすぐに動けるかといいますと、差出人を詐称したらすぐに警察は動いてくれます。では、差出人の詐称というのは何か、メールのヘッダの From を詐称したらそれは詐称か、皆さん疑問がわくと思うのですけれども、詐称の定義を公開してしまうとすり抜けてしまう。穴を見つけてすり抜けようとする人が出てくるのでお答えしませんというのが政府の立場です。詐称の定義というのは、我々ISP みたいなところには知らされているのですけれども、一般の人には公開されていないということがあります。

直罰化の後に、ようやく初めての逮捕者が出ました。多分新しいので記憶にある方もいらっしゃると思います。今年の 1 月、タクミ通信の経営者が捕まりました。この人は 1 日あたり 9000 万通の迷惑メールを配信していたそうです。中国に拠点を持って、そこから配信していて 1 ヵ月あたり 1 億 2000 万円の収入があったということです。

逮捕したのはめでたいのですけれども、月に 1 億 2000 万円を稼いでいる人に 100 万円の罰金でいいのでしょうか。100 万円というと、日本の法律ではかなり厳しい罰金ですけれども、本当にこれが妥当なのかというのは議論されるところです。民事に行っても、不特定多数の人に送っているわけで誰が訴えるのかということもあります。この人は多分出所したらまたやるだろうなというのが、みんなが思っているところです。

④アドレス詐称の防止

アドレス詐称の話をしてきましたけれども、幾つかアドレス詐称を防止する技術が出てきております。

まず、電子署名。これは本当に私が書きましたというものを社員が各メールに対して署名していくという技術です。それぞれの社員がやるのが S/MIME11、会社全体でやるのが DKIM12です。それから、署名ではなくドメインを認証してしまおうという技術もございます。深い話は飛ばしますけれども、メールアドレスというのは、アットマークの前がユーザ名で、アットマークの後がドメイン名です。このドメイン名を認証する。サイトからサイトにメールが送られるときに、ドメイン認証をしてしまう。サイト内でユーザがメールを出すときはユーザ認証をする（図 3.34）。この二つの認証をもって、アドレスの詐称を防止するという技術ができています。あとは普及を待つだけです。

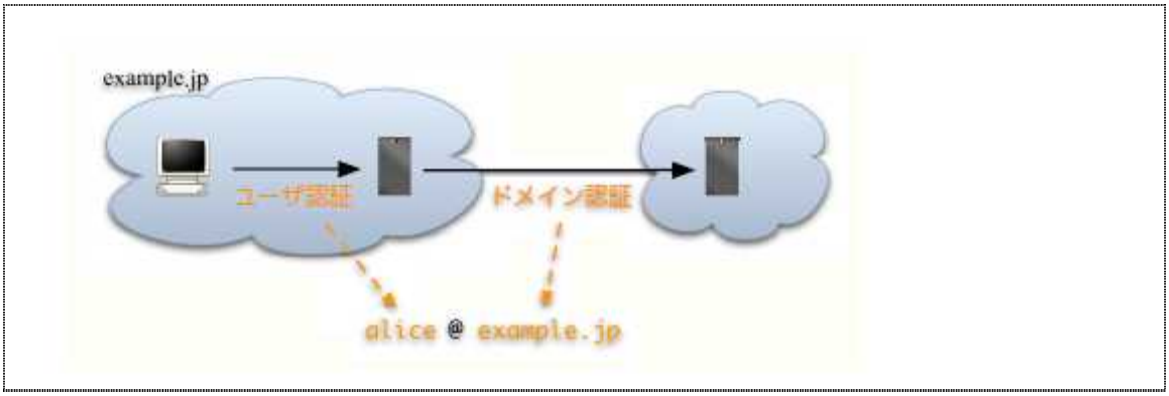


図 3.34　アドレス詐称の防止

例えば、ドメイン認証の技術を皆さんの会社に導入すると、他の人が皆さんの会社を名乗って出すメールがうそつきだということが分かります。また可能性があるのは、内部から他のユーザを騙ってメールを出すことです。例えば、悪い社員が社長の名前を騙ってメールを出す。ドメインは詐称しないけれども､ユーザ名を詐称するということです｡これを防止するのは簡単でして、ユーザ認証をすればよいわけです。ユーザ認証の一般的な技術はパスワードです。それから、できれば「送信通数制限」も行ってください。社長をかたって 1 日に 500 万通内部からメールを出されると困りますので、パスワードがばれたときもそんなにメールが出せないようにしておかなければいけません。

ですから、これからはメールを送るときはパスワードを聞かれる時代になります。メールを受け取るときにパスワードを皆さん入れていると思いますけれども、これからは、送るときもパスワードを入れるという時代になるということをご理解ください。

3.3.4 迷惑メール

迷惑メールについてお話ししたいと思うのですけれども、最近、ようやく迷惑メールの送信手

11 <http://www.ipa.go.jp/security/fy12/contents/smime/email_sec.html>
12 < http://www.iajapan.org/anti_spam/portal/Tech/kiso09.html#92 >

法というものが分かりだしたのです。

(1) 迷惑メールの送信手法

日本にはインターネットと携帯電話網というものがあり、発信するほうと受け取るほうに携帯とインターネットがありますから、2×2 の表が書けるわけです。

まず、携帯電話から携帯電話向けの迷惑メールというのは、携帯電話に届く迷惑メールのほとんど 100%を占めていたわけですけれども激減しました。最近、携帯電話に迷惑メールが来なくなったと思いませんか。それは、それぞれの携帯電話会社がたくさんの対策を講じたからです。DoCoMo さんの発表によりますと、ピークだった 2003 年には 1 日当たり、1 ユーザ 1.8 通です。もちろん片寄りがありますから、受け取る人は数百通受け取るといようなときがあったわけですけれども、2005 年 6 月には 1 日当たり、1 ユーザ 0.02 通と 99%削減されたということです。送信通数制限とかいろいろな手段を講じまして、これを撲滅することに成功したということです。

携帯からインターネットに向けて迷惑メールを送るというのは、コストがかかりますので見合わないということで、これはほとんど存在しません。

インターネットからインターネットに向けて迷惑メールを送る行為。これは皆さん今、困っている問題かと思いますけれども急激に増加中です。これには、「Bot」という技術が使われています。後ほど説明します。それから、インターネットから携帯向けという迷惑メールもありまして、これも増えつつあるのですけれども、これには日本特有の「渡り」という技術が使われます。

(2) Bot の機能

まず、この Bot といものを説明したいのですが、Bot というのは PC に感染して見つからないように裏で動くプログラムのことです。ここに挙げているような、いろいろな機能があって、すごく高度なプログラムなのです。

- 感染機能：複数の脆弱性
- 攻撃：DDOS、迷惑メールの中継
- 制御機能： IRC[13]、Web、DNS
- 情報収集： アカウント情報、メール、プロダクトキー
- 自己防衛： アンチウイルス製品対策、デバッガ対策

図 3.35 を見たほうが早いと思います。Bot というものは何らかの手段で PC に感染します。ウイルスというのは一つの脆弱性を作ることしかしないのですけれども、Bot というのはたくさんの脆弱性のデータベースをもっていまして、ありとあらゆる手段で感染しようと試みます。感染すると、あらかじめ乗っ取っていたウェブサーバ。これも Bot なのですけれども、ウィンドウズにはウェブサーバになる機能とかありますので、乗っ取った後にウェブサーバ化しているのですけれども、ここから本体をダウンロードします。

---

[13] Internet Relay Chat

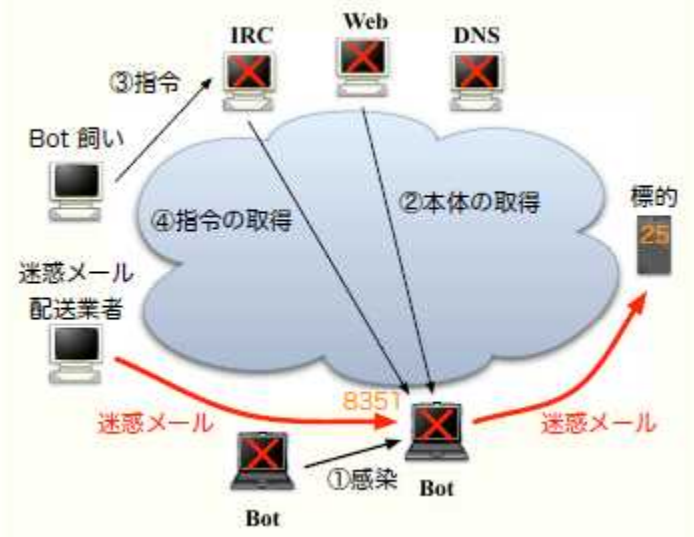


図 3.35　Botnet

Bot を飼っている人はチャットのチャンネルを使って指令を送っておきます。この指令が何かというと、ある番号につないできたらメールを転送する転送サーバになりなさいということをいうのです。Bot 飼いはこれで目的を果たしました。Bot 飼いは実は迷惑メール配送業者ではなく、迷惑メール配送業者に Bot を貸し出しているのです。1Bot あたり 3 ドル/日みたいな宣伝を見たことがありますけれども、3 ドルくらいで貸し出すわけです。すると迷惑メール配送業者はこの番号を教えてもらって、つないで、そこからここを踏み台にして迷惑メールを出すというようなことを最近はやっているわけです。

(3) 渡り

渡りという技術は何かといいますと、日本にはフレッツという技術がありまして、例えば、NTT 東につないでいると上流の ISP を自由に選べるわけです（図 3.36）。今日は ISP a、明日は ISP b というふうに選べるのでどんどん接続を変えて携帯事業者に接続し、迷惑メールを送るということをやります。

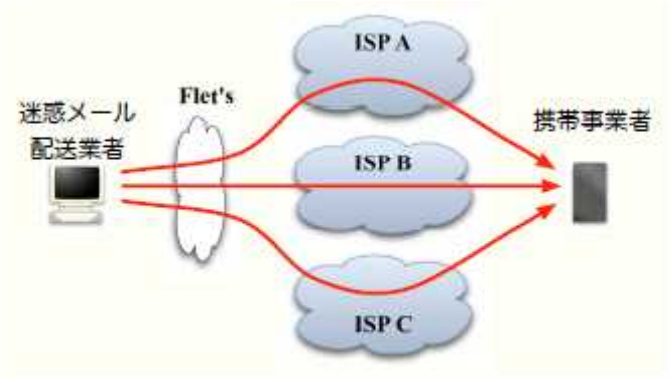


図 3.36　渡り

Bot のほうは世界的規模で誰がやっているかよく分かりませんけれども、この渡りのほうは日本のやくざがやっているのだろうということは言われています。

先ほども言いましたけれども、現在では、ISP が OB25B という技術で、正式なサーバ以外からのメールの送信をブロックするということをやり始めています。また、これからはユーザ認証とか、ドメイン認証とか対応していきますので、日本では迷惑メールが出しにくい状況にどんどんなっていきます。

これまでずっと、迷惑メール発信国として日本はトップテンに入っていたのですけれども、この OB25B が去年すごく普及したので、その結果トップテンから日本が落ちました。何位かよく分からないのですけれどもそういった効果が出ています14。これから少し不便になりますけれども、必ず正式なサーバにつないで、パスワードを打って、メールを出すという時代になっていきます。迷惑メールを撲滅していく過程ですので、少し不便になりますけれども、皆さんご理解をいただいて使うようにしてください。

繰り返しますけれども、ISP は今、実施中ですけれども、多くの企業はファイアウォールで OB25B は導入済みだと考えていただいて結構です。

(4) 迷惑メールの送信

さて最後に、実は皆さんも知らない間に迷惑メールを送信してしまうという可能性があるということを指摘して、まとめに入りたいと思います。まず、この現象を知るには、宛先がない場合に戻ってくるエラーメールの仕組みについて知らないといけないのですけれども、昔はこういうシステムでした（図 3.37）。

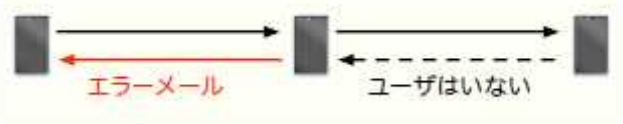


図 3.37　一般的なエラーメールの仕組み

この人がメールを出します。中継されます。最終点に届きました。ここにユーザがいないと、ユーザがいませんということを通知します。すると、真ん中のサーバがエラーメールを返していたのです。ユーザがいないというところが、エラーメールを返すのではなくて、その 1 個手前が返していたわけです。つまり、ユーザがいる、いないということを、相手が、最終点が答えていたわけです。

最近はハーベスティング攻撃という攻撃があります（図 3.38）。これは、迷惑メールを送りたい人が、そのドメインにどういうユーザがいるかというのを確かめるときに使う方法なのです。Alice はいますかと言って、いますと答えると「あ、Alice はいるのだ」となったり、Bob はいますかと言って、いないと答えられたら「いないんだね」と分かりますね。こういったものをハーベスティング攻撃といって、接続した後に、この人いる、この人いると聞いていくわけです。

14 <http://www.sophos.co.jp/pressoffice/news/articles/2007/01/secrep2007.html>

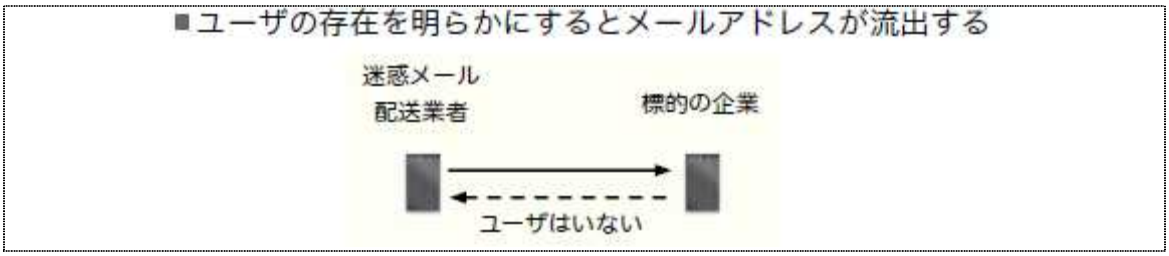


図 3.38　ハーベスティング攻撃

すると、こういうふうな昔ながらのサーバですと、メールアドレスは流出してしまうわけです。私のメールアドレスはインターネットに掲示したことがないのに、何でばれてしまうのだろうという人がいるかもしれませんが、こういうサーバを運用していると、すぐにばれてしまうわけです。これを防止するために、最近はユーザがいるいないといわない、そういう設定をする企業が増えました。つまりどんなメールも受け取る。受け取ってユーザがいなければ、自分でエラーメールを生成するというようなことをやるようになりました（図 3.39）。これが時代の変化なわけです。

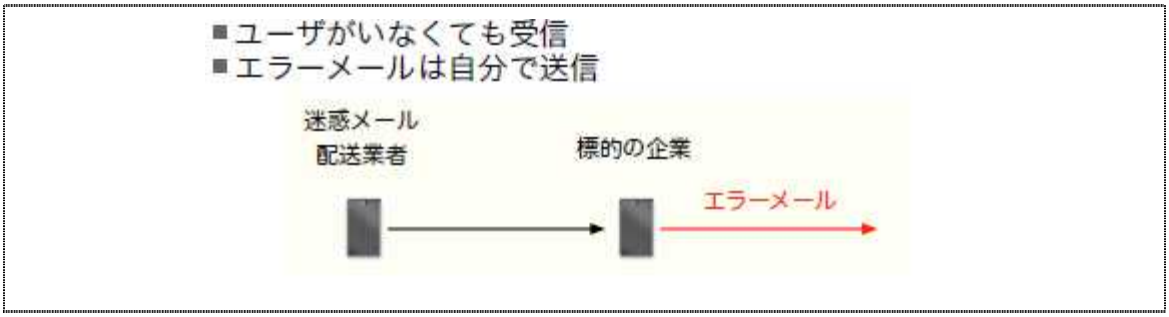


図 3.39　ハーベスティング攻撃の防御

こうなってくると、不要なエラーメールを送信してしまうという可能性があります（図 3.40）。まず、迷惑メールが皆さんの企業に届いたとしましょう。多分、差出人を詐称しています。受け取る人がいなければエラーメールを返しますので、差出人に対して、差出人を宛先に替えます。差出人は自分に替えて送ります。すると、詐称された罪のない企業にエラーメールが戻ってしまうわけです。このときに、迷惑メールですから、何かエッチな宣伝とか書いてあって、それをコピーして返そうものならこれはもうまさに迷惑メールなわけです。

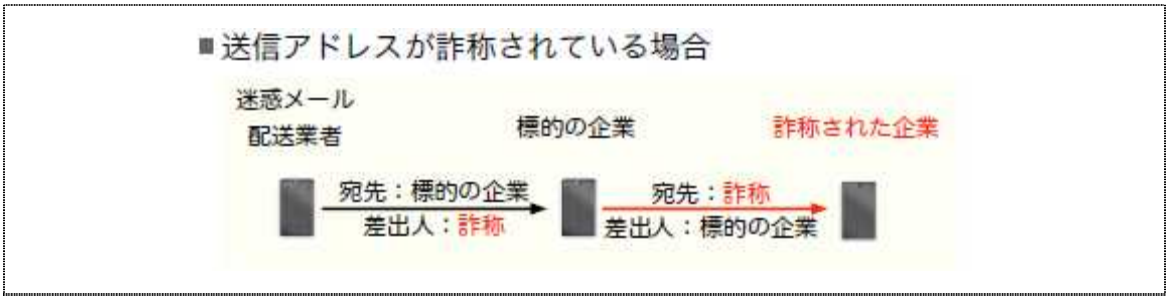


図 3.40　不用なメールを送信してしまう

そうすると、受け取った企業はこの人は迷惑メールを送る悪い人だということで、みんなが作

っているブラックリストのデータベースに登録します。すると、登録してしまうとこの企業から他の企業にメールを送ろうとすると、そのブラックリストを参照していれば、受け取り拒否ということをされますので、まずいよねということです。私は何も悪い事をしていないのに、他の人が受け取ってくれなくなったという事態が起こっているのです。今、実際に。

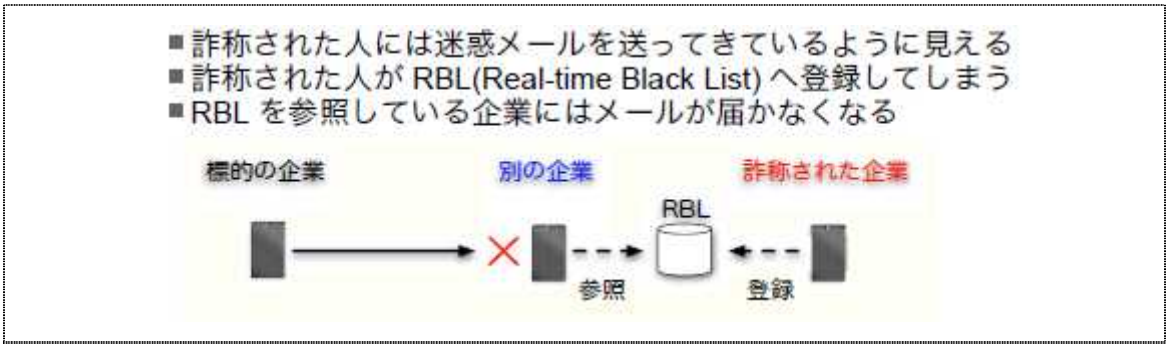


図 3.41 不用なメールを送信すると…

これを防止する技術というものも最近提案されていますので、是非、次にメールサーバを入れ替えるとか増強するというときは、この技術を納入業者に要求してみてください。どうするかというと、先ほどドメインは認証できると申しました。そういう技術はもうございますので、詐称かどうかは分かるわけです（図 3.42）。

図 3.42 ドメイン認証により送信アドレスを判定

悪い人が送っているかどうかは分かるので詐称であって、しかも受け取るユーザがいなければ、エラーメールを返す必要はありません。ユーザがいないとしても、相手が詐称しているのであれば、エラーメールを返す必要がないので、返さないということをする。こうするとドメイン認証が活発に使われて、ドメイン認証自体も普及しますし、皆さんのリスクも軽減されますので、是非、メールサーバを増築とか入れ替えるときにはこの技術を要求してください。

3.3.5 まとめ

メールのリスク管理というのは本当に専門家しかできないような時代になっています。高度化して専門化していますので、大企業の方であれば、専門の人をおいてずっと勉強していただいて、追いついていくということも可能でしょうけれども、中小企業の場合は人員も割けないですし、こういった専門的な知識を習得している時間があれば他の仕事をして欲しいということも多いと思います。これから、メールの運用というのは外注する時代になってくるのかということが言えると思います。

最後に、皆さんはユーザとしてメールを使うと思いますけれども、発想を変えていただきたいというお願いをします。

これからは、メールを送る際にパスワードが要求される時代になります。これは少し不便ですけれども、迷惑メールをなくそうという大きな目標の第一歩ですので、是非ご理解いただいて、もし皆さんの企業がまだパスワードなしでメールを送れるようなシステムであれば、パスワードを打たないとメールが送れないというシステムへ転換していただきたいと思います。

3.4 JSOX と情報セキュリティ監査

私は、あらた監査法人というところでシステム関係の監査であったりコンサルティングをやっておるのですが、ここ数年は、あらた監査法人というのがプライスウォーターハウスクーパースのメンバーファームということで、外資系や日本の SEC 登録企業が米国のＳＯＸ法 404 条に対応する際に、監査人としてそれを評価したり、監査顧客ではない企業に対して、いろいろなアドバイザリーを行ってきています。いわばここ数年は、ずっとＳＯＸ漬けの状態です。

ですから頭の中もずっとＳＯＸ状態になっているわけですけれども、そのＳＯＸについての経験を踏まえて本日はお話を差し上げよう、その中で情報セキュリティ監査についてもどう有効利用ができるかということも含めてお話を差し上げようと考えております。

ＪＡＳＡというところを代表してきて言うのも苦しいのですが、Ｊ－ＳＯＸにおいて、情報セキュリティ監査をやっていればそれですべて足りるかというと、さすがにそういうことにはなりません。どういう役割ができるかを考えると結構厳しいところがございます。そういう意味では、この私の説明の中でも残念ながら情報セキュリティ監査に触れる部分は実はそんなに多くなくて、大半はＪ－ＳＯＸそのもののところにかかわる部分が多くなっています。

私は実践としてやってきていますので、なるべくセオリーではなくて実際に近い話を差し上げたいと考えております。

一応この流行、ブームに乗って『内部統制とＳＯＸ法』という本を昨年の 12 月に出したのですけれども、残念ながらこの１月にこの本を出した出版社が倒産してしまいまして、入手不可能な状態にあります。私も原稿執筆料はゼロ円ですので、いくらお買いいただいても全然お金は入ってこないということになります。もし万が一本屋で見かけるようなことがあったら、非常に貴重品ですのでご購入をいただいてもいいかと思います。

それでは本論に入りたいと思います。まず、Ｊ－ＳＯＸの概要ですが、この辺は色々なところで説明されていますので、そんなに詳しくは説明しません。一般的に、Ｊ－ＳＯＸに対応するためには会社内の内部統制の整備ということが必要なわけです。その内部統制のフレームワークというのが、世界的に見ると、ＣＯＳＯというものしかありません。日本版においては、実施基準の中で、そのＣＯＳＯを流用しながらも、若干の変更を加えています。

次に経緯ですが、これについても皆さん、よくご存知と思いますので、あまり詳しくは述べません。すでにいろいろご存知の状況がある中で、一番最新のところとしては、経産省のシステム管理基準の追補版というのが出ています。それからさらに後で、財務報告にかかわる内部統制の評価および監査に関する実施基準ですが、これは昨年パブリックコメントが出ていたものに対して、この２月に最終版が出ています。

あとは、3 月に本当に出るかどうか分かりませんが、日本公認会計士協会のほうからの実務指針というものが出ると予想されております。それが出てしまうと、ほぼＪ－ＳＯＸに関しての公から出てくるようなものはすべて出尽くすということになります。その後は、結局、企業や外部監査人が自分たちで考えていかなくてはいけないため、実際には詳細が決まらずに手探りでやらなくてはいけない状況というのが今後も続くのだろうと予想されます。

全体的な話としては当たり前のところなのですけれども、もう一度おさらいとして申し上げます。Ｊ－ＳＯＸというのは新たな法律です。

会社の経営者が、財務諸表作成に係る内部統制を自分で評価をして、報告書にまとめるという行為をしなくてはいけないというのがまず一つです。それともう一つは、その評価の内容や方法について、外部監査人が監査をするという点です。

そのときの外部監査人の監査というのが、経営者の評価内容について評価をする行為なのですが、米国のＳＯＸ404 条には、それ以外にダイレクトレポーティングというものがあります。それは、外部監査人が財務諸表の作成にかかわるプロセスの内部統制を直接評価することで、日本版では大変になるから外しましょうということになったと聞いています。ところが実施基準の監査人に係るパートを見ると、監査人が評価する内容は経営者による評価、つまり経営者の評価が適切にできているかどうかだけではなくて、内部統制を直接評価するような内容が書かれています。ですから結果として外部監査人はダイレクトレポーティングという意見表明はないですけれども、実作業としては内部統制の評価を行うことになります。外部監査人というのは、要は会計監査人ですから、会計監査の正しいアプローチという中には財務諸表を作成するにかかわるプロセスの内部統制の評価というものが入っており、そこで直接内部統制を評価するという考え方のようです。

このような会計監査の一環としての内部統制評価は、今までは必ずしも十分に行われてきたわけではないと思いますが、こうして実施基準に明記されてしまいますと、監査人としてもやらざるを得ないということになります。何を言いたいかといいますと、ダイレクトレポーティングはないと言いながらも、実際には外部監査人は、経営者による内部統制の評価の内容や方法だけを見るのではなくて、実際の内部統制のほうもやはり見るのだというところは念頭に置いていただいたほうがいいと思います。

次に内部統制の枠組みですが、ここもすでに、皆様方、嫌というほどご覧になっていますので、あまり説明はしません。アメリカではこのＣＯＳＯキュービックをベースにしていますが、日本版では五つの内部統制の構成要素に対して、さらにもう一つ、「ＩＴへの対応」が付け加えられているのと、三つの内部統制の目的に対してさらにもう一つ、「資産の保全」が付け加えられています。ただ J-SOX 対応上においては、結局フォーカスする目的は、財務報告であることにご留意願います。

五つの構成要素及び「ＩＴへの対応」というのはどういうことかということを書いていますが、この辺は説明がいろいろなところに出ていますので説明を割愛したいと思います。

私がなるべくフォーカスしようと思っているのは、私の専門はＩＴですので、内部統制全部というよりは、基本的にＩＴに絡むところです。そのＩＴにかかわる内部統制の評価というのは、もうすでにご存知のように３種類あるわけですね。内部統制は、実施基準においても、全社的な統制と業務処理統制、ＩＴ全般統制というものに分かれています。さらにはこの中で、ＩＴにかかわる全社的な統制とか、ＩＴ業務処理統制、そしてＩＴ全般統制というように分かれているわけです。

まず、おさらいとして申し上げますと、会社レベルの統制、全社的な統制というのは会社全体

の組織構成、経営者の考え方、風土とか、そういったことを含んだ非常に広範にわたるような概念で、具体的な個別統制とは大分違って、ある意味ではより評価が難しい部分です。

そういったものがまず一つ分類としてあって、次に業務処理統制があります。これは具体的な財務諸表、財務報告を作るプロセスであり、それを業務と呼んだ場合に、その業務上で実施されている財務報告を信頼すべきものにする、または歪めないようにするための統制、コントロールのことを指しています。

その中には人間が行うマニュアル的な統制以外に、アプリケーションプログラムが行うＩＴアプリケーション統制、ＩＴ業務処理統制というものがあるわけです。そうすると、そのＩＴ業務処理統制というのが、どれだけ信頼ができるかということを考えるためには、ＩＴ全般統制が必要であるということになります。

全社レベルの統制、全社的統制の中にはＩＴ全社的統制というのがあります。それは、一般的にはここに書かれているように、ひとつはＩＴの方針が含まれます。金融機関などのように、ＩＴ、もしくはシステムリスク管理方針のようなものを作っている会社もあります。一般的な企業においては、どこでもそういうものがあるわけではありませんが、基本的にはそういったものを含めて、会社においての IT の全社的な方針です。セキュリティポリシーは必ずしもＩＴのことだけ書いているとは限りませんが、内容によっては含まれると思います。

このような IT の全体的な方針において、IT 委員会やステアリングコミッティーなどの IT に係る経営委員会の位置づけや、どういう部門がＩＴの開発、運用を担当し、どういう部門が利用しているとか、その中でシステムの管理者、セキュリティの管理者はどういう位置付けの人でありというようなことが規定されている場合もあると思います。また、会社としてシステムの開発や運用を自社中心で行うのか、アウトソースを中心とするのか、さらには OS やプラットフォームの方針などが規定されている場合もあると思います。

このような方針というのは絵に描いたもちでは非常にまずいので、会社で、特に関係する人たちがちゃんと把握するようにする仕組みも重要です。例えば、方針そのものが誰でもがアクセスできるイントラネットの掲示板にあるとか、あるいは定期的な研修の場において方針の内容を必ず説明するとか、新入社員の入社時に説明するとか、そういった仕組みがあることが重要となります。

モニタリングというのは、その周知がちゃんと成功しているかどうかをオブザーブすることです。社員が IT に関する全社的方針を知っているかどうかをちゃんと確認するということです。内部監査部門において、そのような点を評価項目に入れているかどうかがポイントだと思います。

それから最終的には、その状況がどうであるかということを経営者がちゃんと把握しているかが重要になります。経営陣の集まるような委員会や取締役会等で、IT の全社的方針について、策定時に諮られていたり、浸透状況が報告されているかどうか。こういったところがＩＴ全社的統制というものになると思います。

ＩＴ業務処理統制も概念的にはすでに皆様方ご存知だと思うのですが、業務処理に係る自動化された統制のことです。この対象となる業務は、財務諸表を作成するプロセスですが、これは取引の発生のところから、実際に総勘定元帳に登録されるまでの全体のプロセスになります。もち

ろん、最も重要な期末財務報告プロセス、決算プロセスも含まれます。これらプロセスの中で、取引データであったり、それが保存された元帳データというのが信頼できるものでないといけないわけです。

信頼できるものにするために、いろいろな統制があり、それを業務処理統制と呼びます。その業務処理統制の中で、特にＩＴにかかわるものをＩＴ業務処理統制と言います。その中でも概念的には、ここには書いていないですけれども、2 種類考えられます。システムと人間のする行為が両方必要なものを、ＩＴ依存統制、システムだけで全部やってしまうのがＩＴ統制というように分類されます。

ＩＴ依存統制ですが、例えば、システムからリストが出てきて、そのリストを基に人間が何かの照合作業を行うという処理があります。この時、人間が行う照合作業をマニュアル統制として考え勝ちですが、もしシステムから出力されるリストそのものに間違いがあった場合、照合作業自体に影響を与えてしまいます。したがって、その統制が正しく実行されているかどうかを評価するにあたっては、厳密に言えば、まずはシステム上でリストを出す機能が正しくできているのかどうかということが、ポイントの一つとなります。その次に、人間がちゃんとチェックしているのかがポイントになるわけです。つまり、ＩＴ部分とマニュアル部分の両方の評価をしなくてはいけないのがＩＴ依存統制です。

それに対して、ＩＴ統制は、システム上に統制そのものが実装されているケースを指します。よく例に挙げられるのが、システム間でデータ転送を行う場合に、それが正しく実行できたことを確認する統制があります。

業務処理統制というものの理解は大変難しく、色々な業務によって異なります。今現在、実施基準においては、あくまで主要なものが例示されているだけであり、そこに書かれている内容に合致しないものは、一切関係ないということにはならないと思いますので、その点に注意して洗い出しを行う必要があります。

次はＩＴ全般統制です。財務報告の信頼性をゆがめるリスクを軽減するために適切な統制が行われているかどうかを評価するというのがＳＯＸ404 条であったり、Ｊ－ＳＯＸの考え方です。その場合に、なぜＩＴの開発とか運用の統制を評価する必要があるのかが理解できないと思われます。

理解できないのは当然なのですけれども、今後実際に会社として評価していくためには、それを理解しないといけないわけです。理由としては大きく二つあって、一つは最終的に自分で評価をするのですから､そのときにこのＩＴ全般統制と言われる開発や運用にかかわる評価を行って、何らかの問題が発見されたときに、その問題というのは重要な問題なのかそうじゃないのかということを判断するために理解する必要があります。これが一番重要な理由です。

もう一つは、やはり自分で評価をするといったときに、どの会社もそうですけれども、効率的にやりたい。つまり、やらなくていいことはなるべくやらない、または、やる必要があることだけにフォーカスしたいと思うわけです。そうすると何がやる必要があることなのだろうと考えるときには、なぜこれをやらなくてはいけないかということを理解しないとできないので、IT 全般統制の必要性を理解する必要があるわけです。

それをすべて細かい点まで本日ご説明するのは非常に難しいのですが、どういうようにこのＩＴ全般統制が財務報告の信頼性にかかわっているかということですと、根本的にはこの図に行き着きます。この図は、ＩＴＧＩ／ＩＳＡＣＡのＣＯＢＩＴをベースにしたＳＯＸ404 条のためのＩＴにかかわる説明の資料から抜き取ってきています。

重要な勘定科目に係る業務プロセスにおいては、通常、業務アプリケーションが利用されています。この業務アプリケーションは、ダイレクトに財務報告の信頼性にかかわる統制を提供している可能性があるわけです。そうすると、まずそのＩＴ業務処理統制が重要かどうかということが第一のポイントになります。必ずしもすべての企業において、重要なＩＴ業務処理統制が数多くあるとは限りません。金融機関などは絶対避けて通れませんが、小さい企業であれば、極端な話、IT に少し位間違いがあっても、マニュアル統制、つまり人間による統制が非常に徹底していて、取引の量があまり多くないので必ず原票と比べているとか、もしくは何らかの間違いがあったら必ず取引相手に発見されるから正すことができるとか、いろいろなやり方があると思うのです。とにかくまずは、ＩＴ業務処理統制というのが重要かどうかを見極めることです。そしてＩＴ業務処理統制が重要となった場合、つまりコンピューター処理が間違っている場合に非常にリスクがあるといったときに初めて、ＩＴ全般統制というのが必要になってくるわけです。

ではそのＩＴ全般統制がなぜ必要ですが、例えばＩＴの開発・保守にかかわる統制があります。ではなぜこの項目が必要かと言いますと、IT 業務処理統制の説明として、IT が、システムが重要な統制を提供しているという話をしました。しかしその IT 業務処理統制の信頼性を脅かすリスクが二つあります。

一つは、個々の IT 業務処理統制機能は実際に業務をつかさどる人たち、つまりユーザーが必要だと考えたから存在するのですから、そのシステムの機能がユーザーの要件通りに本当に作られているのかどうかがポイントになります。もし異なって作られていたら、それは間違いである可能性が高いことになります。そのため、IT 全般統制の中で、ユーザーの要件どおりにシステムを開発するための統制が必要になります。例えば、要件定義書のようなものを作ったらユーザー部門に見せて、本当に自分達の要求とあっているという確認をした上で、部長印を押してもらうというような統制が考えられます。それ以外には、実際に開発をした後で、当然単体テストや結合テストといった直接的にシステム開発者がやるテストもありますが、その後で最終的に、最近ですとＵＡＴ、ユーザー・アクセプタンス・テストとかユーザー受け入れテストという言い方をしますけれども、そうしたユーザーが評価するようなテストも重要な統制となります。

もしこうした統制がないとなると、極端な話は、特にその機能をリリースしたばかりの頃には、ユーザーが思っていることと異なる結果となるリスクがあります。もちろんそんなに高いわけではないのでしょうけれども、そういうリスクがあるので、そういった観点からは、やはりユーザーが開発にちゃんと関与しているかどうかというのが大切です。

一方でもう一つのリスクは、ユーザーはちゃんと関与しているが、システムの開発がいい加減で、要求された機能が正しく実現できないということが考えられます。このようなリスクに対しては、適切な開発手法が会社の中で確立していたり、その開発手法の中で、担当者が仕様書を作った後には上位者がレビューをするといったようなチェック機能があるかとか、適切なテストを

しっかりやるような仕組みになっているとか、そういった統制が必要になります。

このように、IT 業務処理統制に繋がるリスクを適切に理解した上で、その項目、統制を洗い出したり評価することが重要になります。

運用についても同様です。運用においては、ユーザーの要求通りにシステムが作られているかどうかというよりは、運用するにあたって間違いが起こらないかがポイントです。極端なケースとして、運用管理がすごくいい加減で、毎日正しく動くはずのバッチジョブが動いていなかったがゆえに、何らかの資産がちゃんと計上されないような事態が起こってしまったら、大きな問題となります。そういう観点から運用の統制を評価する必要があります。

アクセス管理については、アプリケーションプログラムへのアクセスとデータへのアクセスの二つがポイントとなります。

せっかくＵＡＴも適切に行われていて、プログラム開発の統制も非常に素晴らしいという状況にもかかわらず、じゃあ本番リリース後に、そのプログラムの内容にものすごく詳しい開発者がひそかにプログラムを改ざんしてしまっても誰も気づきませんでしたというと非常にまずいわけです。ですから、プログラムに対してちゃんとアクセスコントロールができているかということが非常に重要になります。

同じように本番のデータは、開発者だけに限らずオペレーターを含む運用部門や利用部門、さらには社外のインターネット経由のアクセスも含めて、すべての人たちから適切に保全されているかどうかということを検討しなくてはいけないということになります。

外部委託というのは、今回Ｊ－ＳＯＸの実施基準でわざわざクローズアップされている項目です。最近は開発や運用が外部委託されているケースが目立ちますが、その場合であっても財務報告の信頼性に係るリスクの管理責任から逃れることはできません。自分たちは一切そういうことは知りません、外部に任せているのだから外部の会社次第ですという考え方は、許されないということです。この外部の会社は十分な統制を備えているのかを、評価する必要があるということです。

このように、IT 全般統制について考える場合においても、まず何のためにやるのか、つまり財務報告の信頼性を担保するためであり、直接的には IT 業務処理統制（この場合はデータの保存も含みますが）に依拠するために評価を行うのだということを理解することが大変重要だと思います。その理解の上で、では必要最低限はどれだけのことを行うべきか、というように考えていくということです。

では、情報セキュリティとはどう関係があるか。やはりこれも無駄なことをやらないためとに、ちゃんと理解する必要があると思います。ポイントは、情報セキュリティに含まれながらも、ＳＯＸの外に出ている部分です。ここの部分を非常に注意していただきたいと思います。まず、情報漏えいですね。別に漏えいしたから、個人情報が外に出たからといって、財務報告の信頼性に直接的には関係するわけではありません。もちろん間接的には株価には影響するかもしれないけれども、株価が変動したからって財務諸表の信頼性が損なわれるわけではありませんから、そういう意味では、漏えいは関係がないのだということです。

データの改ざんは関係するのですけれども、財務諸表作成プロセスに関係ない部分のデータの

改ざんは、やはり関係がありません。

ＢＣＰも一応は対象外だと考えられます。ただ、バックアップがちゃんと取られているか、というようなところは関係します。それはなぜかというと、システムというかデータのバックアップをちゃんと取っていなくて、システムがダウンしてそれまでの会計記録が一切ありませんとなると期末財務報告が作れなくなりますので、当然バックアップは重要になります。

一方でシステム処理の不正確性とか要件のミスマッチなどの開発関連の部分は、一般的には情報セキュリティ側には入りません。情報セキュリティについて、よくＩＳＭＳなどでもＣＩＡという言葉を使われますが、コンフィデンシャリティ、インテグリティ、アベイラビリティという観点からしますと、J-SOX にはコンフィデンシャリティが一番関係なさそうな感じですね。インテグリティは圧倒的に関係が深いと思います。ただしあくまで財務諸表関連のデータだけに限ってです。もちろん、この時の財務諸表関連のデータとは、END TO END のプロセス全体に渡る広い範囲ではありますが。アベイラビリティというのもある程度関係していますが、あくまで財務諸表関連のデータおよびシステムに限ってということになります。

ここからは、J-SOX に対応するために実際にどんな作業をやるのかということの説明ですが、色々なところで説明されていますので、詳しくは説明しません。簡単に言うと、最初にちゃんとスコーピングをして、文書化をして、そして統制の設計の評価、運用の評価をやって、最後の評価をする前までは問題があれば修正をして、最後に報告書を作るという流れです。

まず体制ですが、一般的には文書化をするチームというのは実際の業務の担当者で、評価をするのは、どちらかと言うとそこから独立した側ということになります。ここでは評価・テスト責任者と書いていますけれども、一般的に一番多いと思われるのは、評価側は内部監査部門が担当する場合ということになるのでしょう。実際に今、日本においては内部監査部門の人数が足りなかったりスキルが不足していたりということで、この辺をどうするかということが非常に問題になります。必ずしも内部監査部門ではなくて、臨時のチームを組成してやるというようなことも考えられます。

次にシステムの特定です。やはりこれについても重要なのは、Ｊ－ＳＯＸに対応するにあたってなるべく無駄なことはやらないという方針であれば、対象のシステムを限定することです。限定するためには、上流からいかないといけません。

一番最初は、その企業においての特に重要な勘定科目です。一般事業会社においては、売上、売掛金及び棚卸資産となっていますが、金融業等、明確になっていない業種もあります。今後、日本公認会計士協会の発表する実務指針などで明確にされていくと思いますが、特に重要な勘定科目は何かというのが決まったら、ではそれにかかわるプロセスが特定されます。そうすると、次にそのプロセスで使っている情報システムは何かというのを特定していくというのが、スライドで示しているマッピングの表です。こうした表は、ほぼ間違いなく作ったほうがいいと思います。

そのときに重要なのは、そのプロセスで使われている情報システムが全部対象になるのではなく、当然のことながら、その使われ方がキーポイントになります。その使われ方というのが財務諸表の信頼性に非常に大きく関係しているかどうか、なのです。非常に抽象的な言い方をしてい

ますが、それがすべてのキーです。

対象となる業務において、例えば取引はすべてあるシステムに入力する場合であっても、システムから出力された取引は、その後すべて取引先と照会して内容を全部確認するような統制、もしくは取引先から請求書のような書類が来て、その内容と比べるようなマニュアル統制がある場合には、そこで１回確認されます。したがって、その後でまた別のシステムに取引データが転送される場合には、それより前のシステムは切ってもいいということになります。ですから、そういったようなことを分析をして、なるべく対象のシステムを外す、少なくするというのが非常に重要なポイントになります。

それはなぜかというと、対象となったシステムに関しては、それら全てをカバーするＩＴ全般統制の評価をしなければいけなくなるからです。ＩＴ全般統制を実際に評価して、問題点をなくしていくというのは簡単ではありません。工数もかかるわけですので、対象のシステムが少なければ少ないほど楽になります。

ですから対象システムの特定をちゃんと行うということが、非常に重要なポイントになるのです。その後は、文書化、評価という大きな作業ステップがありますが、本日は時間もあまりありませんので、ごく簡単に説明したいと思います。

文書化フェーズにおいては、基本的には、よく言われているような三点セットというようなものを作ります。要は、統制の洗い出しとその説明の文書を作成するのです。それが作られたところで、今度は統制の設計の評価と運用の評価というものを行います。設計の評価というのは、本来あるリスクを文書化された統制で十分低減できているかという観点から評価をする行為です。そして十分でないと考えられる場合には、規定を作ったり書き換えたりと、ルール側のほうを直していきます。

運用の評価というのは、ルールは十分だったとしても、実際にその通りにやっていないかもしれないので、やっているかどうかをチェックするというものです。

こうした一連の作業を行った後で、ちゃんとできていませんでしたという問題が出た場合には、それは内部統制の不備なのか重要な欠陥なのかということを評価しないといけません。ここが非常に難しいところで、私もここでどうやればいいですということを一言で言うことはできません。もしこういう問題が出た場合には、相当悩んで、ほとんどの問題は内部統制の不備であって、重要な欠陥でないと結論付ける形になると思います。

不備は多分ものすごい数が出るので、重要なのは、不備を一切なくそうなどという完璧主義者みたいな考えは起こさずに、不備はいくらあってもいい、重要な欠陥でなければいいという考え方を持つことです。重要な欠陥は内部統制報告書に載ってしまいます。

次のスライドはアメリカのＳＯＸ1 年目の結果ですが、どこまで正確なのかは保証できませんが、6%から 8%程度は企業として非常にシリアスな問題が発見されたということのようです。具体的な欠陥の内容としては、全社的統制としてシステム関連の主要な方針がなかったとか、アクセスコントロールができていなかったとか、バックアップが全然ないとか、変更の仕方が適切でないがゆえにユーザーが全然承認していないといったところが挙がっています。

次に情報セキュリティ監査の活用です。情報セキュリティ監査というのは、私どもＪＡＳＡは、

経産省が作ったルールに基づいてそれを推進しようとしています。

会社が情報セキュリティ監査を受けた場合に、報告書が出ます。先ほど情報セキュリティとJ-SOXの関連を説明しましたが、共通している部分があります。そのような共通部分も情報セキュリティ監査の報告書に評価結果が載っていますので、それを流用することができる可能性があるわけです。

可能性と言っているのは、今現在、公的な基準上はこれを使いなさいとか使ってもいいですということは一切明示されていませんし、今後も簡単にはされないと思うのです。ただ最終的には外部監査人がOKと言ってくれればいいわけですから、外部監査人と交渉して情報セキュリティ監査の結果を流用できるのであれば、マネジメントテストの中で、自分でやる部分を減らすことができるということと、情報セキュリティ監査そのものの元々の効果もありますから、一石二鳥になります。ただ残念ながら私が大丈夫ですとは言えません。それぞれの会社の方は、自社の外部監査人と相談をしてOKかどうかということを確認してからやっていただきたいと思います。

それからもう一つ、情報セキュリティ監査のやり方というのはＪＡＳＡを筆頭にいろいろなところで細かい情報が出ていますので、結構マネジメントテストに流用できると思います。

まとめです。すでにいろいろ言いましたので重複する部分もありますが、まずはスコーピングがＩＴ全般統制において重要になるということですね。それから標準化。これは説明しませんでしたが、先ほどの話で、なるべく対象のシステムを絞ったとしても、まだ対象システムが 10 個あるといった場合に、その 10 個を個別に全部評価していくとすごく時間がかかります。開発のやり方も運用のやり方もアクセスコントロールも全部同じであるというように、標準化ができれば一まとめに評価できます。1回やるのと10回やるのでは全然違いますから、標準化は非常に重要です。ただ標準化できない場合もあるでしょうから、その場合には個別に評価しないといけません。しかし 1 年目に間に合わないとしても、2 年目、3 年目に間に合わせるために標準化していくと考えてもいいと思います。

それから、対象となったシステムについては、システム部門が所管しているか所管していないかとは関係なく評価しないといけません。今まで見ている限りにおいては、システム部門が所管していないシステムの評価はうまくいっていない場合が多いですので、そこは非常に気をつけていただいたほうがいいと思います。

業務処理統制については、洗い出すときにシステム担当者がかかわらないとよく失敗していますので、システムも含めて洗い出しを行うことが重要です。

外部委託している場合にどうするのかというと、大きく言えば二つしかありません。外部委託先に自分で評価に出かけるか、もしくは外部委託先から第三者によって評価した結果をもらうか。後者の仕組みがここで説明しているSAS70です。日本版は、監査基準委員会報告書第18号と言います。これは外部委託先、つまりアウトソーシング受託企業が自分の外部監査人を使って監査をした報告書を開示してもらい、それを会社のマネージメントテストや外部監査人の監査に利用するというものです。アウトソーシングの規模が大きい場合など、直接会社を訪問して評価をするのが大変になりますので、SAS70（18号）をもらう方式をお勧めします。

3.5 システム管理基準追補版（財務報告に係るＩＴ統制ガイダンス）の狙い

3.5.1 企業における IT 統制とシステム管理基準

先般金融庁より発表された、財務報告にかかわる金融商品取引法の実施基準は 2 月 15 日にフィックスされた。これに対し、経済産業省は、そのＩＴ統制にかかわる部分をもう少し具体化したほうがいいのではないか、少なくとも企業が財務報告にかかわるＩＴ統制を実施するときに少しでも楽になるような方法を提供する必要があるのではないか、ということで緊急会を持ち、よく知られているシステム管理基準について、「システム管理基準追補版」という形で、これと整合性を取った上で、ガイダンスを作ってきたものである。

本稿はこの「システム管理基準追補版」についてまとめたものである。現実には、本報告書中の関連する報告等も総合して、各企業でどのようにしていくのかということを決めていくのがよいと考える。ここで発表するものはあくまでもシステム管理基準というものをベースにしてきた企業が、ＩＴ統制をどうやっていくのか、そのときの参考にしてもらうという位置付けであるので、その点をご理解いただきたい。

本稿ではまず、追補版の構成、ＩＴ全社的統制、ＩＴ全般統制、ＩＴ業務処理統制といったものの内容に少し触れる。その後、(他の報告中にもあるためざっくりとだが) 経済産業省サイドはどう考えているかという観点から、財務報告にかかわるＩＴ統制の評価について述べる。最後に「システム管理基準」をどうやって使っていくのかについて述べる。

まず、システム管理基準だが、これは昭和 60 年、今から二十数年前に最初に作られた基準で、コンピューターシステムを開発していくとき、どのようにしていくのかをまとめた基準である。どうやっていくかということが書いてあって、ちょうど 2 年ほど前に改訂されている。

企業の経営戦略に合わせてＩＴを使用していこうという点と、ＩＴのリスクにまつわる提言をして、ＩＴ統制をやろうということがベースになっている。したがって今回のＩＴの内部統制の構築、評価にはシステム管理基準が役に立つのではないかと考えて、今回、追補版としてガイドラインを経済産業省のほうでは作ったということである。

3.5.2 経済産業省　対補版の構成

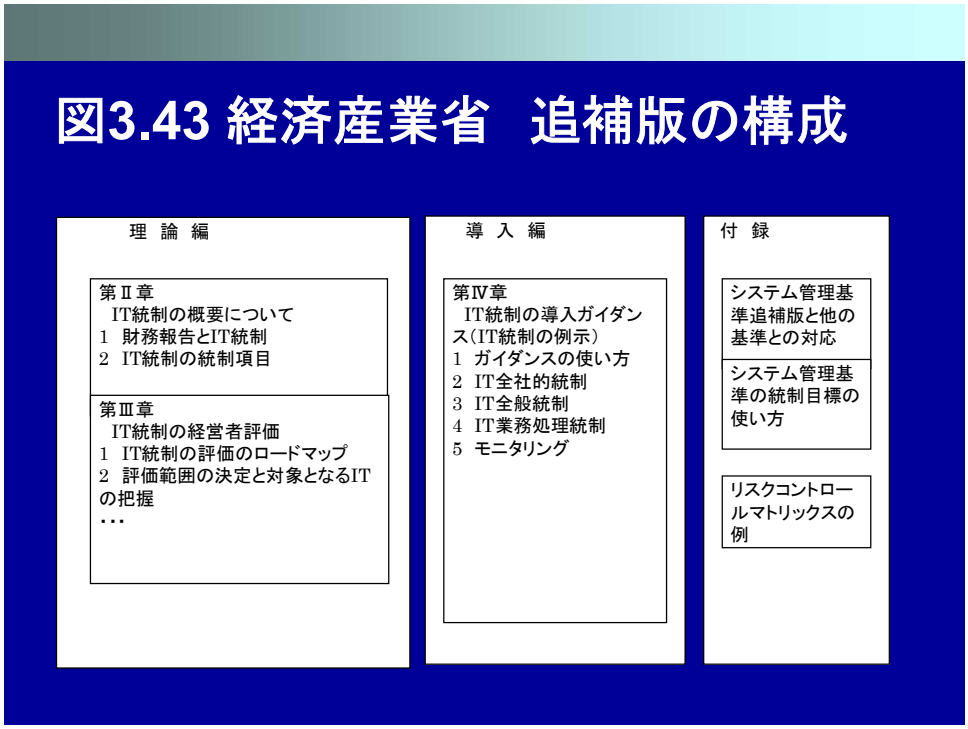
次に、構成について簡単に紹介する(図 3.43)。第Ⅰ章は用語などが記述されている。第Ⅱ章ではＩＴ統制の概要をざっくりと、金融庁の金融商品取引法実施基準との関係で触れている。第Ⅲ章は一番内容的には難しいところであるが、企業にとってＩＴの経営者評価をやれ、内部統制報告書を書け、と言われているので、この部分をどのようにしていくのかという趣旨の内容を記述している。

続いて「導入編」という形で、ここはどちらかと言えばＩＴ部門の方々が主に使うことを想定して記述している。企業のＣＩＯおよびＩＴ部門が、経営者からの諸々の指示を受けて実際に経営者評価につなげるために、具体的にはどのように実施していくのかを記述している。

次に「付録」であるが、これがこのガイダンスの一番の目玉になるところであると思う。経済

産業省としてはシステム管理基準ということでこれまで進めて来ているが、今、世の中の多くの企業では、特に米国のＳＯＸ法対応を行われたところではＩＳＡＣＡ（情報システムコントロール協会）が出しているＣＯＢＩＴ（Control Objectives for Information and related Technology）を参照していると思うが、これとの対応なども今回この付録の中で明示してあるので、読者諸氏がお使いになるときにこれらの対応が取りやすいように考慮した。

それからシステム管理基準追補版を使うときの統制目標といったものも付録に挙げてある。最後にリスクコントロールマトリックスであるが、どんな形でリスクコントロールマトリックスを作っていくのかといった内容のやや具体的な事例を挙げさせていただいた。



3.5.3 IT 統制の概要について

次に、より具体的に、どのような内容が記述されているのかを述べる。

まずⅠ章では全体の構成と用語の解説を記述している。実は、金融庁の実施基準の中ではＩＴ統制は全般統制と業務処理統制の二つしかない。しかし、今回の検討委員会でいろいろと議論していく中で、やはり全社的統制というものを入れたほうがいいのではないかという結論に至り、ＩＴ統制というものは三つあるというように記述した。なお、実施基準には「会社として」の統制は全社的統制、全般統制、それから業務処理統制と三つあると書かれている。

金融庁の実施基準で、ＩＴ統制については全般統制と業務処理統制があると書かれているが、今回の検討委員会の中では、セキュリティポリシーや開発標準といったものは、全般統制よりも全社的統制に分類しておいたほうがいいのではないかという考えがあり、ＩＴ全社的統制というものを今回のシステム管理基準追補版中では謳っている。

ただ、このシステム管理基準追補版は、必ずしもこのガイダンスにしたがってやらねばならな

いというものではないので、このあたりは使用する各企業で判断していただく必要がある。

3.5.4 IT 統制の経営者評価

それから経営者評価の中では具体的にどんなことを挙げているかについて述べる。ＩＴ統制の評価のロードマップをどのようにやっていくのか。最初にちょっと触れておきたいのだが、ＩＴから見たときにこの金融商品取引法の関係でシステムをゼロから作るということはまずないと今回の調査検討委員会では考えている。やはり各企業において、実際の業務ですでにシステムを使用し、運用している中で、新しいコンプライアンスプログラムが出てきたという状況である。そういう中でどのように対応するのか。既存のシステムに足らないところを手当てしていくというのが一般的に考えられる対応だと考えられる。そういうことで作成側としては、このロードマップの中では今まであるシステムを全部捨ててゼロから作れということをここで訴えているわけではないことに注意されたい。

システム管理基準というもの自体は情報システムを作っていくために使える基準である。この情報システム管理基準等をベースに作っている中で、さらに何が必要なのか。そういった意味で「追補版」という言い方を今回しているので、この点を承知しておいていただきたい。このためにシステムを、経済産業省として、新たに作り直せとか、既存のものは捨てろということを言っているわけではない。

したがって、システム管理基準に今回新たに追補版という形で追加するが、これを参考にする等してシステムを構築し、その中で足りない部分として今回の追補版に挙げられているプロセスをもって評価し、実行していただければいいのではないかと考える。このような考え方であるので、あくまでも本稿で述べているガイダンスというものは、情報システムをスクラップ&ビルトして作り直せということではなく、足りない部分にどのように手当てをしていくのかを考えて欲しいという意図である。さらには、今後新しいシステムを構築していくときには最初からこの追補版にあるような観点も入れて構築していただくような形で、参照していただければよいという発想であるので、この点をご理解いただきたい。

3.5.5 IT 統制の導入ガイダンス

本稿では目次編の詳しい解説は省略するが、実は、ＩＴ部門の方々にとって、第Ⅳ章だけ読めば使えるようにしようという考えに基づき、この章の中には意図的に目次を設けてある。その中でガイダンスの使い方、ＩＴ全社的統制、ＩＴ全般統制、（ＩＴ）業務処理統制、それからモニタリングという順序で記述してある。したがって、ＩＴ部門の方々においては第Ⅳ章をじっくり読んでいただければ、私たちがこの委員会で言いたかったことが伝わると考えていただければと思う。

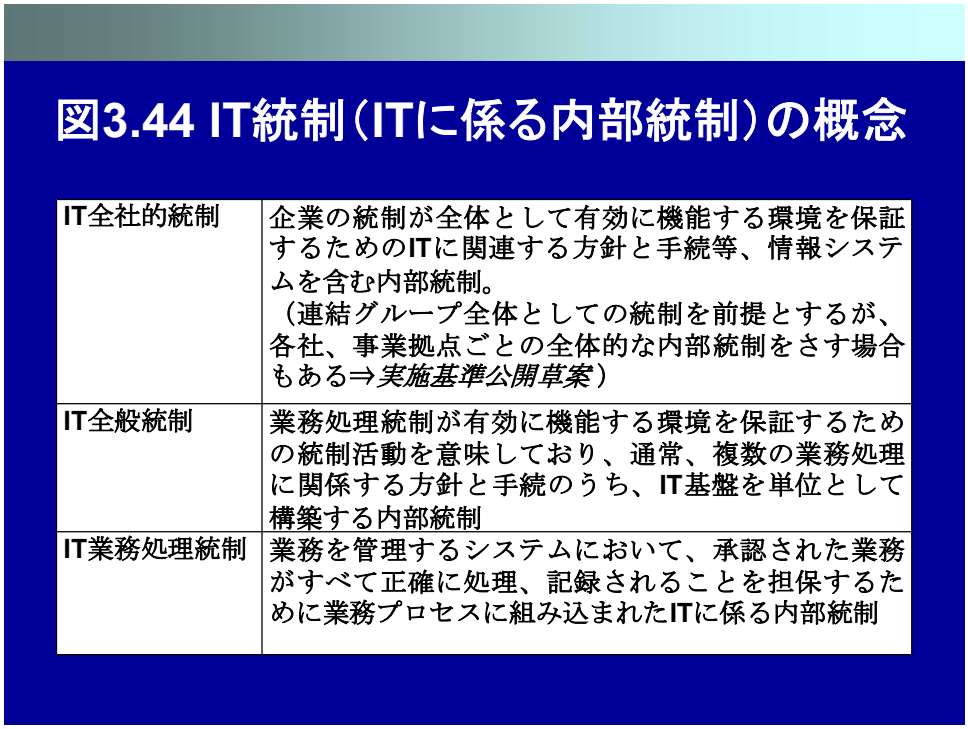
今回の追補版では、付録がたくさんついている。2007 年 1 月 19 日～2 月 19 日の期間にパブリックコメント募集ということで公開した。本報告の読者におかれてもダウンロードしてお読みいただいた方々もたくさんおられるのではないかと思うが、約 150 ページあり、金融庁のものに比べても「何かボリュームがある、すごい項目だ、やれるのか」という懸念をお持ちの方も多い

と思い、本稿では、「ここに書かれていることをすべて行わねばならない」と言っているわけではなく、各自のリスクに応じて適切に（取捨選択して）実施するものであるということをご理解いただければと思う。

3.5.6 IT 統制（IT に係る内部統制）の概念

まず最初に用語の定義である（図 3.44）。先ほど触れたように、今回、ＩＴ統制というものをわざわざ区別するために頭に全て「ＩＴ」と付けて区別をしている。ＩＴ全社的統制、ＩＴ全般統制、ＩＴ業務処理統制という言い方を採らせていただいた。これについてはこの追補版独自の言葉で、特に全般統制の中でＩＴにかかわるものをＩＴ全般統制と呼んでいるとご理解いただきたい。

全般統制というのは、金融庁が言っている広い話だが、その中のＩＴに関わる部分を取り出して今回の委員会で議論したいということで、このような定義をしている。



3.5.7 財務諸表監査と内部統制監査

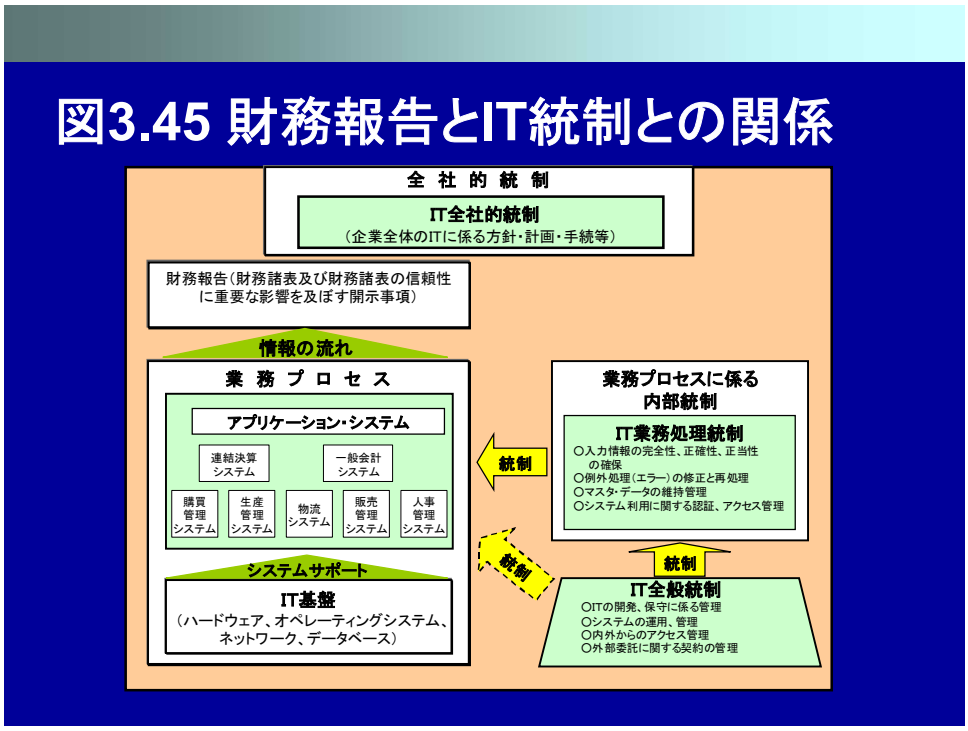
詳細は本報告書中の他稿にあるため詳細は割愛するが、いわゆる財務諸表監査と内部統制監査を公認会計士が実施し、そして同じ形で発表していくことになるということなので、（実態としては）各企業の公認会計士にＩＴも見てもらうということになる。

その中で私どもが一番懸念しているのは、公認会計士はなかなか多忙で、ＩＴまで手が回らないというのが現状ではないかということであり、そのような状況において（監査を実施する）公認会計士が、どうしても厳しい方向へ行ってしまうのではないか、ということである。そういう中で、企業として「ここまでやっている」ということを何か明言できれば少しでも（監査人であ

る）公認会計士に説明できるだろうし、また逆に公認会計士もどのような形で（実際に）やっているのかということを理解してもらえる。このようなことに使えるという目的で今回のガイダンスがあると考えていただければと思う。

3.5.8 財務報告と IT 統制との関係

さて、図 3.45 はＩＴ統制がどういう関係にあるかという図である。これは、情報システムコントロール協会が出している図を委員会でじっくり研究し、委員会の中では、日本版のＳＯＸから考えるとこういう理解のほうがいいのではないかということでまとめたものである。



まず業務プロセスがあり、いろいろなアプリケーションシステムがある。例えば購買システム、生産管理システム、物流システム、販売管理システム、人事管理システム、それから一般会計システム、連結決算システム等である。これが今回の財務諸表にかかわるコアになるシステムである。そのシステムはご存知のようにオペレーティングシステム、ネットワーク、データベースというハードウエアで運用されている。そしてこういったシステムにおいてＩＴが何にかかわるか。このシステムをどのように開発しているか。どのようにデータを入力し、運用しているのか。ここでのマスターデータをどう管理しているか。そういったことが大事になる。そういうところでの管理が業務プロセスにかかわる内部統制である。その中にＩＴの部分としてあるのがＩＴ業務処理統制というように理解していただければよいと思う。

ここでちょっとグレーな部分は、コンピューターに人がタイプインするが、これが人なのか、情報システムなのかという点である。金融庁の発想では一応情報システムに入れるというところ

なのだが、従来経済産業省等で考える情報システムの範ちゅうには入っていない。このあたりが若干グレーであり、含めて考えないといけないのではないか。情報システムにデータ入力するときのインターフェイスも少しは（含めて）考えようというような話がここに入ってくる。

それからこのような業務システムに対してどのように開発するのかという点ではここで関係してくるかと思う。システムの開発をどうするか、とか保守をどうするかという点である。このシステムの業務処理統制がどううまくいくことによって、このアプリケーションシステムがきっちりと統制されるのか、という話になる。

点線で書いてあるのはアクセス制御についてである。いわゆるＩＴ全般統制でネットワークにログインして、そのログイン ID でアプリケーションシステムが使えるかどうか、そういうアクセスコントロールをするというところがこの統制に当たるという考え方で整理している。

そしてこういったものを全体的につかさどるというか、企業全体のＩＴの方針、自社において、ＩＴシステムをどうするのか、例えば会計系であればＳＡＰを使うとか自社システムを特注で作るとか、いろいろな方針があると思う。そういう方針だとか計画、それから開発するときにはこうやって開発するのだといったいろいろな手続きがあるはずだと考える。それがＩＴ全社的統制である。また、情報セキュリティポリシー等もここに入ってくると考えている。

そういうわけでこの点に全社的統制があると考えている。今このＩＴ全社的統制をこういった形で分けている理由は、これも公認会計士の方々等と委員会で議論していく中で、例えば、ある会社の子会社が例えば 100 社あるとする。100 社全部を連結で見ようと思うと結構大変なことになる。そうするとある程度サンプリングして見ていくことになる。そのサンプリングするときの単位は、多分ここの IT 全社的統制の方針が同じであるものを単位としていくのであろうというところにある。

例えば、会計系にＳＡＰを使っているようなグループと、そうではなくて既存のホストを使っているグループ、それから、ちょっとしたパッケージでやっているグループ等、そういったいくつかのグループができるだろう。そしてそういうグループについての方針等である程度色分けして、その中からサンプリングをして検査をするといった形がとれるだろう。そういうときにこのＩＴ全社的統制が役に立つという発想である。

例えばセキュリティポリシーが同じであればセキュリティポリシーにかかわるここのいわゆるアクセス管理の部分等も範囲を絞り込むことができるだろう。例えばグループに対するセキュリティポリシーがもし何もなければ、やはりそこの企業の子会社はかなり念入りに見ていかないといけない。

そういう判断に使いたいというのがあり、このＩＴ全社的統制という概念を今回置いたとご理解いただきたい。そういう意味では（金融庁の）実施基準の全社的統制、業務処理統制、全般統制とちょうど対応する形になっている。そういうことでこのような概念がおかれているということをご理解いただければと思う。

3.5.9 財務報告とアプリケーション・システムの関係

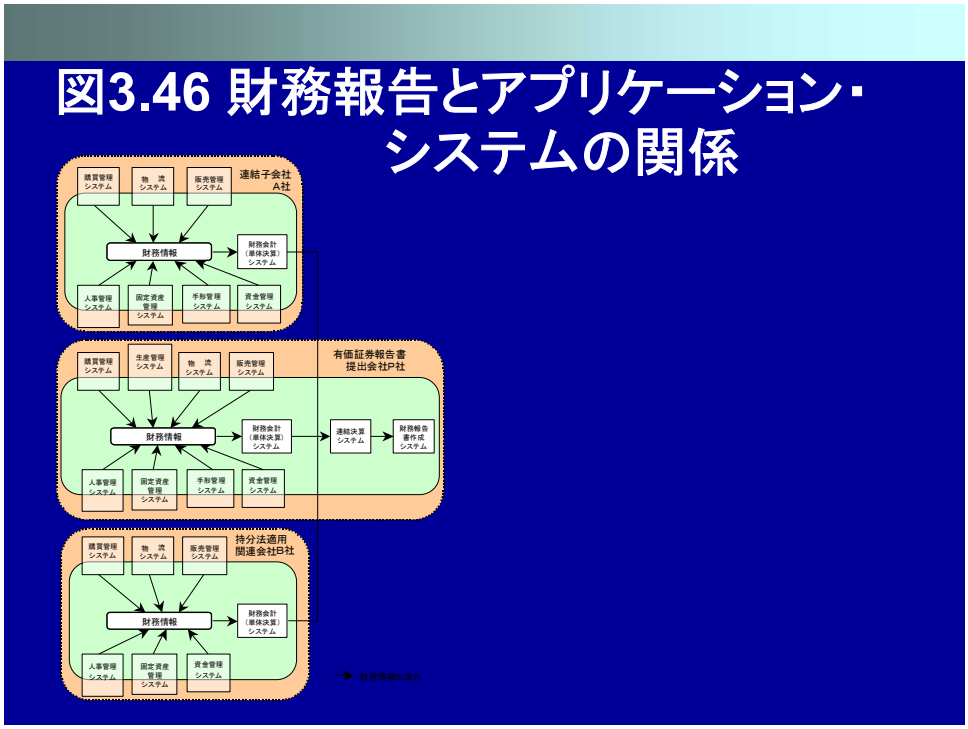
それから財務報告とアプリケーションシステムの関係であるが、図 3.46 のような関係でかなり

いろいろなシステムがかかわってくる。それも全部ではなく、財務報告にかかわる部分がシステムとしてかかわってくるのだとご理解いただきたい。そしてある１社の中での会計処理がこれで完結する。その連結という形で連結親会社のところでシステムとしてまとまってくるという形になる。

この追補版について寄せられたコメントを見ると、財務情報という言葉を我々が定義してしまったために分かりにくいというところもあったようである。財務情報というのは財務にかかわる情報一般、全部を一体として呼んでいるので、何か財務情報とかかわると金融商品取引法にかかわるデータの根本か何かそんなものだと思っていただければよいかと思う。

例えば販売情報だったら売り上げデータとか、価格情報とかそういったものになると思う。生産管理システムだと何台作ったとか原価がいくらだとかそういう情報が上がってくるが、これらが財務情報だというようにご理解いただければと思う。

そして会計の決算にかかる一番重要な情報はこういう財務会計システムのところに入ってくる。ここの情報はさらに重要になってくると理解いただきたい。



なぜこのようなことに触れたかというと、（詳細後述するが）リスクアプローチで我々はとらえている。リスクアプローチからするとやはり最後に一番大事になるのは財務報告の情報である。ここのデータが改ざんされていたり、例えば虚偽の数字だったりすると問題である。そうするとこのシステムにおいてはそのリスクが一番大きいということになる。では生産管理システムの原価情報はどうか。これはもうほとんどサブの情報になる。そうするとリスクというものは、ここの情報についてのリスクとここの情報についてのそれは違いますということになる。すると当然、

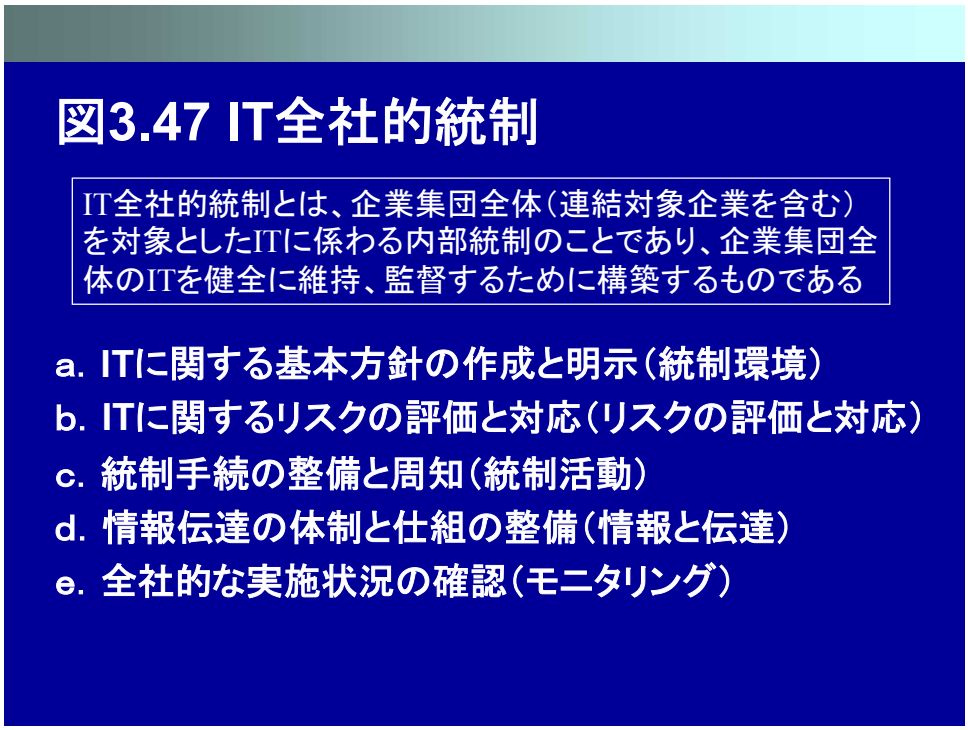
こういうシステムに対するリスクの考え方も変わってくる。それをご理解いただければよいと思う。

財務報告にかかわるからすべて強力な内部統制が要るのかという点も、リスクに応じて各企業で考えていただければよいという説明になる。ただし問題なのはそれを公認会計士がきちんと分かってくれるか、そこが私たちの一番頭の痛いところである。

3.5.10 IT 全社的統制

先述のように、ＩＴ全社的統制はどのような項目があるかというと（図 3.47）、他の報告でもあるように、これはもともとＣＯＳＯモデルから来たもので、ＩＴの場合はＩＴに代わる基本方針、リスクの評価と対応、それから統制の手続きと整備の周知、どうやって従業員に周知しているか、それから情報伝達、これは財務情報がタイムリーに経営者に入るかどうかとかいう点がポイントである。

それから一番大事なのがモニタリングである。モニタリングが一番ＩＴ部門にとっては気になるところだと思う。これについては後述する。



3.5.11 IT 全般統制

こういったものが全社的統制で、全体図を示す、ということである。全般統制（図 3.48、49）は多分、ＩＴ部門の方々には一番なじみがあるところだと思っている。

図3.48 IT全般統制

・IT全般統制とは、財務情報の信頼性に直接関連する業務処理統制を有効に機能させる環境を実現するための統制活動
・ITの企画・開発・運用・保守というライフサイクルの中で、リスクを低減するための統制を適切に整備・運用

- ITの開発、保守に係る管理、
- システムの運用・管理、
- 内外からのアクセス管理等のシステムの安全性の確保、
- 外部委託に関する契約の管理

図3.49 IT全般統制の考え方

- 新規のプログラム
  - 信頼性がテストされ、承認されて本番環境に移行
- プログラムの保守
  - 信頼性がテストされ、承認されて本番環境に移行
  - 旧システムから変換されて、新システムに移行されるデータも同様の過程を経て、本番環境に移行
- プログラムの運用
  - 未承認の処理や不正な処理が防止
- プログラムとデータへのアクセス
  - あらかじめ承認された者だけにアクセス権限を設定（予防的統制）
  - アクセス違反をモニタリング：プログラムとデータの改ざんが防止（発見的統制）。
- 開発・保守・運用を外部委託
  - 委託先で、プログラムとデータの信頼性が確保

開発、保守をどうやっていくか、また、運用管理、アクセス管理、そして外部委託はどうか。このような点でいろいろとヒアリングをしたのだが、やはりＩＴ部門の方々が一番責任を持ってやるのがこのＩＴ全般統制だと思う。ここが、全体をきちんと作るという意味では一番大事にな

ってくるということなので、これが一つのキーになってくると考えていただきたい。

全般統制については、なぜこのようなものが出てきたということについて、以下のような発想で考えられているとご理解いただきたい。まず新規のプログラムというのはどんなものだろうか。新規のプログラムに対する統制とは何だろうか。それは、ここで言う信頼性、すなわち数値が正しいことである。そしてその信頼性というものがテストされて承認されて本番環境に移行する。この点にはまたなかなか難しいところもある。本番環境に移行するときにどうするのか。これも後述するが、これを本当に真面目にやっているとアメリカのように大変なことになってしまう。アメリカのＳＯＸなどではこの本番環境への移行はＩＴ部門がタッチしてはいけないなどという話になる。

ただ日本の場合、本番環境に移行するときにＩＴ部門の人がいなくてできるだろうかというと、現実にはほとんどできない。ではどうしたらいいのか、については後述する。

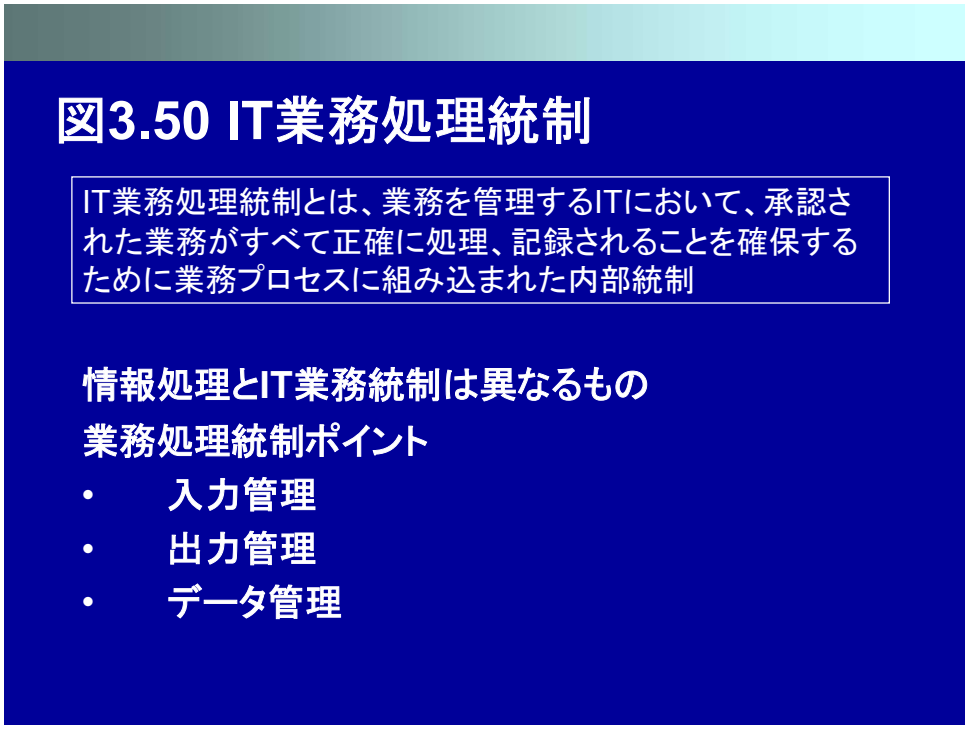
次に、本番環境でプログラムを運用している間、プログラムは保守しなくてはいけない。保守するということは、実際には何をするのか。卑近な例で言うと、ウィンドウズアップデートがある。ウィンドウズのシステムだと、例えばＯＳにパッチを当てなくてはいけない。これらが保守にあたると考えて欲しい。ＯＳにパッチを当てて、また本番できちんと試験をして運用する、といったようなことをやりなさいという話になってくる。これらについても、どこまできっちりとやるのか、またこれを（監査人である）会計士がどこまで要求するか、この点（プログラムの保守）についても大きな問題になってきて結構大変なところだと考える。

次に運用についてだが、運用というのはコンピューターを毎日、日時運用していくときに、誰かが何か承認されていないデータを打ち込んだとか不正なことをやってしまったとか、データを入れ替えてしまったとか、そういったことがないように運用しなければいけない。そのためにはプログラムとデータへのアクセス権限の設定が必要である。これが一つの開発から運用までの全般統制の考え方のステップである。

こういうところでもっていわゆる財務情報にかかわる部分の統制、すなわち不正がないようにしていくというのが一つの考え方である。では、それを外部委託しているときはどうするのか、外部委託先をどうやってチェックするか。これらの項目が全般統制に含まれるものであり、これが全般統制の考え方であるので、いわゆるパッケージプログラムを対象として考えた場合、一部が省略されることはあり得ると考えていただきたい。

3.5.12 IT 業務処理統制

次に業務処理統制について述べる（図 3.50）。



これはＩＴ部門がやっている会社もあるし（IT 部門は）手を出していないところ等、会社によっていろいろな形態がある。業務処理はあくまでも実際の事業部がしっかりと面倒を見るのだという整理をしているところもある。

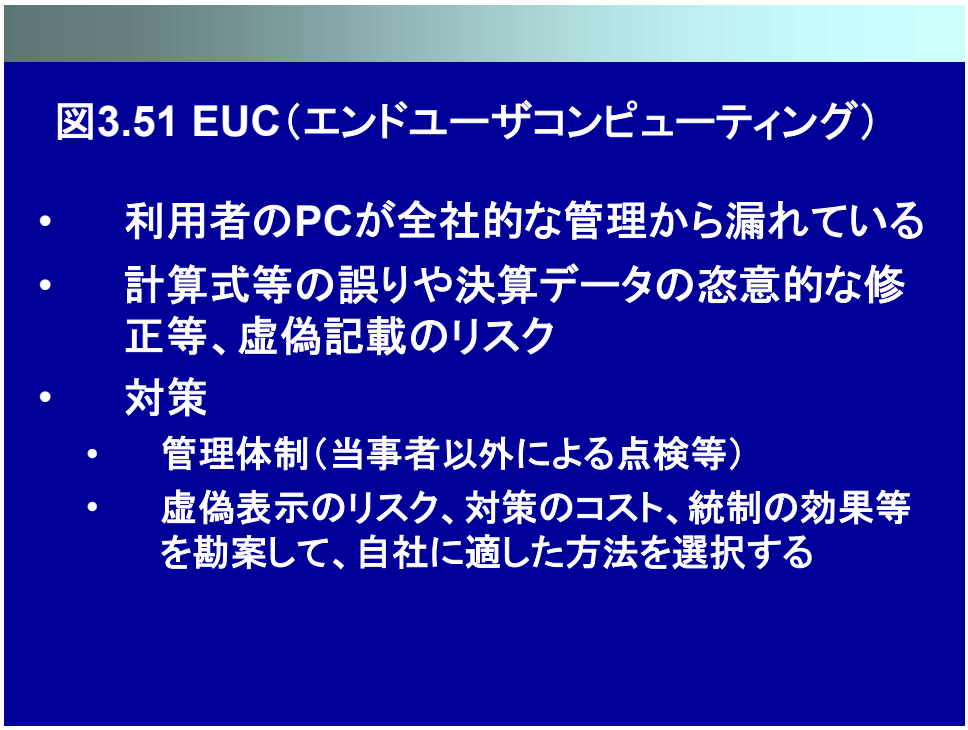
ここでのポイントはデータをどう入力するか、それから例えば、システムに入力したデータを他のシステムに移さなくてはいけないようなとき、例えば他のシステムでそのデータを活用するという場合もある。そのような場合、出力管理というのが一つポイントになってくる。つまり入力と出力、ここが一つのポイントである。

それから 3 番めにデータ管理がある。内部でどう処理しているか、内部に不正がないかが着目点である。これは開発のところで見る形になるのだが、この三つをポイントとして実行する。したがってこのデータ管理の部分が、例えば情報システム部が開発しているときは情報システム部が担当し、システム開発をして渡す。あとは業務処理部門が運用する。運用するときはこの入力と出力を管理する。このような形になってくると思う。

これらについても、入力、出力を自動化していくような場合、例えばウェブでも自動的に入力が入ってくる場合や、ＢｔｏＢで受発注が自動的に入ってくるような場合、ほとんど業務処理部門が入力に触ることもない。出力もデータになって、例えば暗号化されて次のシステムに渡される等の形になってくると、これら業務処理統制のポイントが実を言うと軽減されていく。ではこれは誰が面倒見るのか。全般統制のほうで面倒を見るという形になってくるというようにご理解いただきたい。

3.5.13 EUC（エンドユーザーコンピューティング）

それから今回、私ども委員会で相当な議論したのがエンドユーザーコンピューティングのところである（図 3.51）。



特に大きく二つあり、一つは本当にパッケージなどを業務部門が勝手に入れて運用しているような場合で、二つめがエクセルみたいなものの場合である（システム管理基準中ではスプレッドシートと表現している）。

そうしたときにどんな統制をやらなければいけないか。あくまでも先述のとおり、不正がないようにしなければいけないということが一つの大きいポイントになる。もう一つ一番問題になってくるのが、例えばコンピューターというと、アクセス制御にしても何に関しても、普通は情報システム部門が大部分を管轄しているのだが、ＥＵＣの場合「これは財務で使うのだから自身の、いわゆる財務部門だけでいい」などということで管理が漏れている場合がたまにある。

こういったときに例えば公認会計士（監査人）等がこういったシステムを見るといろいろとコメントがでるかもしれない。だからこのあたりは少し考えておいたほうが良い、というような意味で注意喚起している。

それから二つめとして、スプレッドシート（エクセル等）のような場合、これが特に決算データの最後の作り込みなどのときに結構エクセル等を頻繁に使うというケースが多いようである。エクセルを使ってはいけないのかと言われてしまうと、多くの企業は困ってしまう。ではどこまでやるのか、情報システムの開発と同様な厳しいことをやらなければいけないのか。厳密にはそこまでやったほうがいいのだろうけれども、そこまでやると結構大変だということで、では（現

実的に）どのあたりまで必要なのかというところを今回、この追補版では記述した。

パブリックコメントとして出てきた意見には両方あり、今後、経済産業省のほうで最終的にどこまで落とし込むかというのは（講演実施時点では）まだ決まってはいないのだが、何らかの表記は残るだろうと考えている。あくまでもやはり計算式の誤りとかデータが勝手に変えられないという点は重要である。例えばＣＦＯとか、財務担当が「うーん、ちょっと黒字にしよう」などと勝手に数字が入れられないような何か統制が必要である。それは別に自動的に行われなければならないということではない。誰か人的なチェックでもいい。それから例えばもしそれができないのであればエクセルのフォーム自体を、データは入れられるけれどもいわゆる計算式を変えられないといったようなことでもやっておいたらどうか。委員会での検討中に行ったヒアリングしている中で興味深かった話がある。普通マニュアルでこういうＢＳとか決算データとかを扱うときは概ね数表を作る。縦横計算をして、縦横で大体合っていると、みな検算も兼ねて行う。ところがエクセルだと縦で計算してしまって決算、答えが出てしまう。横をやっていないとかがあって、チェックしていないというの例が結構ある。

少なくともチェックはしたというぐらいのことはやってほしいというのがここでの思いである。ただ、そうかと言って、ではこのエクセルでやっているのを全部ドキュメントにして書いて文書化せよ、と、そこまではやらなくてもいいのではないかと思っている。ただこれも公認会計士がだめだと言ったら、企業としてはやらなくてはいけなくなるかもしれない。ただしそのときに、我々は経済産業省のガイドラインに従って、こう書いてあるのでそういうことだけはやっていると言ってもらえれば少しは免れるかもしれない。そんな理由もあり、こんなところをわざわざ書いたと理解いただければと思う。

このあたりの虚偽表示のリスクへの対応、統制をどうやっていくかについては、各企業の“思い”で決めてもらうことになると思う。そのあたりはエクセルとかを使うときに何かのルールを決め、そしてそれに従って、例えばそのチェックはきちんとやっているというようなところがあれば､それなりにものの分かる公認会計士であれば聞いてもらえるかと思っているところである。

3.5.14 財務報告に係る内部統制構築のプロセス

財務報告にかかわる内部統制のプロセスをどうやって進めていくのかという点についてその概要を述べる。

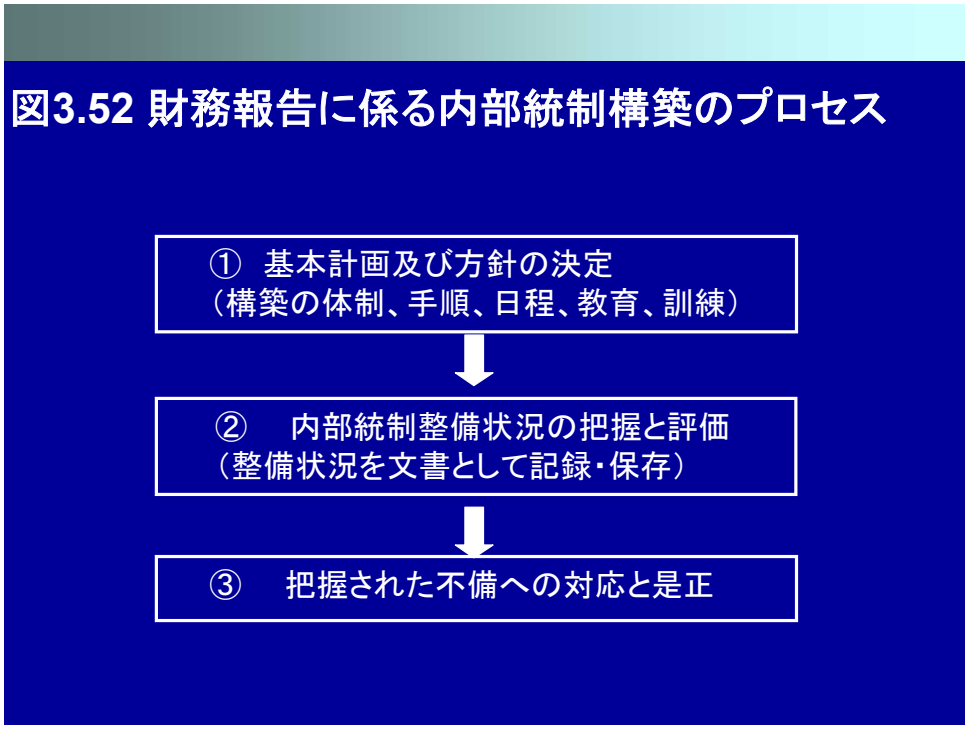


図 3.52 に挙げているのは実施基準に書かれている通りのものである。基本計画を作り、内部統制整備状況の把握と評価、このようなことをやりなさいということである。一番大変なのがこの、整備状況を文書として記録、保存せよ、というところで、文書化ということで今皆が大変苦労しているのはここだと思う。ここの文書化にしてもいろいろとやり方はあると思う。やり方については、ある程度公認会計士とも相談する必要はあると思う。ただし公認会計士の言う通りにやるととんでもないことになる場合もあるので、それなりに各企業自らポリシーを持ち、ここまでは我々はやるのだ、これで十分リスクには対応しているのだということを言えば、少しは（負荷が）軽減されるかもしれない。この点については後述する。

この過程で分かった不備への対応と是正をやる。これに関して、不備が出てきたとき、直ちに直さなければいけないか、については、不備があったら不備があるということを内部統制報告書のほうに書けばいいということになっているので、この点を理解する必要がある。

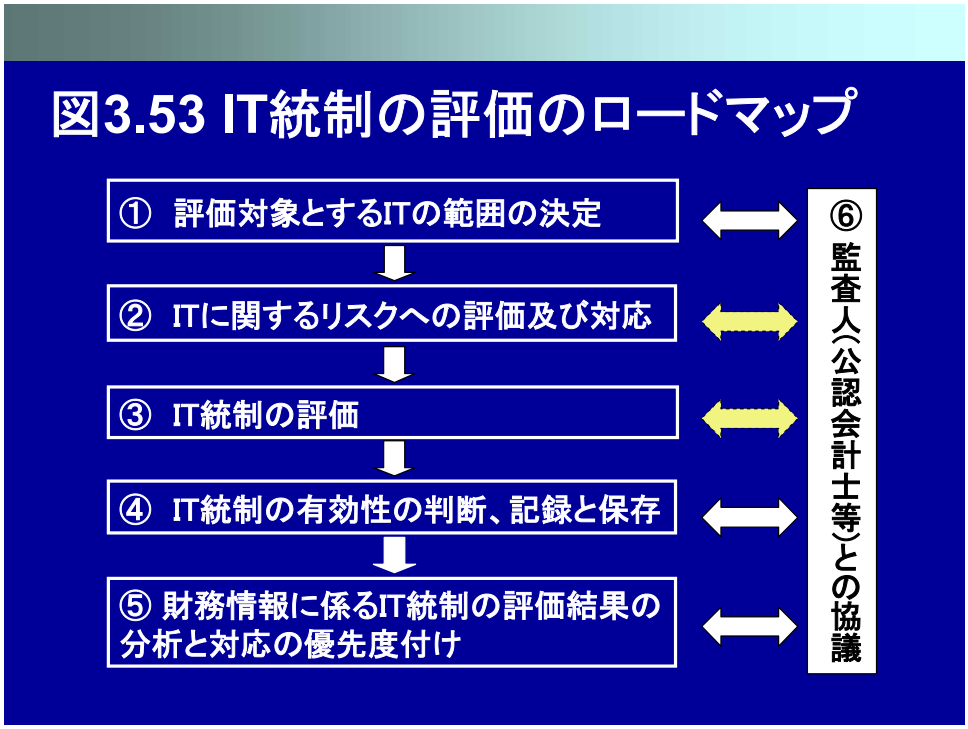
例えば、システムの不備があったとしよう。即このシステムを何とかしなくてはいけないが、あと 1 年ちょっとしか準備期間もない、やれない、大変だ、となってしまうかもしれない。この場合、本当に財務情報の信頼性に極めて大きい影響があるというシステムはそれなりにやらないといけないかもしれないのだが、それほど影響も少ないし、2 年後にはお払い箱にするシステムだということであれば、不備なのだけれどもこういうことで影響は少ないというようなことを、例えば内部統制報告書に書けば、それなりにまだ許される世界だと思っている。

そして、例えばそれは 2 年後にリプレイスするというようなことで会計士と相談していただければいいのだろうと考えている。内部統制構築で一体何をどうするかというのはなかなか難しい問題がある。すべて文書化しなければいけないとかすべてシステムを直さなければいけないとか、

すべて不備を来年の 3 月 31 日までにやらなければいけないということではないということをご理解いただければと思う。

3.5.15 IT 統制の評価とロードマップ

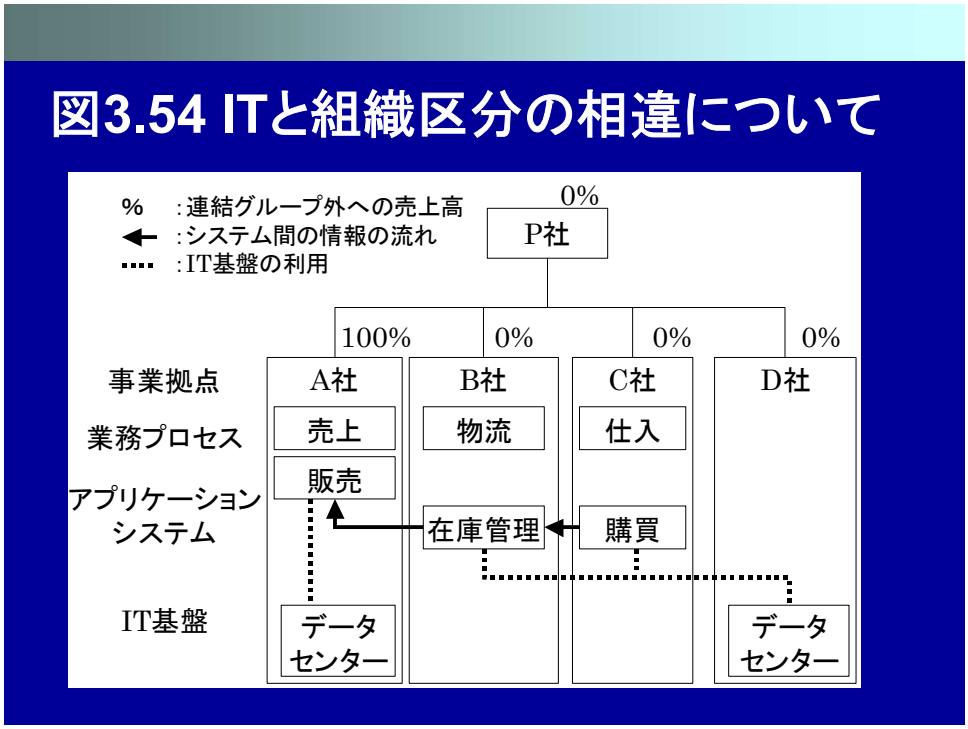
次にＩＴ統制について述べる（図 3.53）。



ＩＴ統制の中でどのように評価していくかという課題がある。実を言うとこの実施基準では、この1から5の項目の中で監査人と対応しなさいというのは1番と5番ぐらいしか書いていない。ただ私ども、実を言うと 2 番め、3 番め、4 番め、ここも場合によると会計士と意見が違ったらちょっと問題だということで、一応全項目公認会計士とそれなりに相談しなさいと追補版では書いている。

実施基準の中で書かれていない話で、私たちが一番気にしてこの中で触れた話として、（これはいろいろなコメントが来ているので言い方が変わるかもしれないが）パブリックコメント募集時の時点では、以下のような例（図 3.54）を挙げた。例えば、A社は連結子会社がいくつもある。例えば在庫管理、それはほとんどＢ社というところに依存している。しかしＢ社は 0%ですという場合のときに、Ｂ社は連結対象ではない。だからここの情報システムは関係ない。でもここの在庫管理の情報が例えば改ざんされたら、カネボウ事件ではないけれど、ここの在庫情報が違ってしまったらA社の財務諸表は大きく変わってしまう。数%（程度の差）だったらまだいいかもしれないが、これが数十%等影響があるようなときに、ここの在庫管理のシステムが、「いや、これはA社とは関係ありません。だからここのシステムは我々見ておりません」というように、こ

このシステムは関係ありません、と言えるかというと多分言えないのだろうという結論でこういう話を書いている。



したがって、ＩＴから見たときに、いわゆる実施基準で書かれている範囲と必ずしも一致しないかもしれない。そのケースがすこし懸念されるということで、挙げてある。

このような形で、例えば、いろいろなシステムが外出しになっていて、さらにハードウエアはD社というデータセンターに入っていて、自分のところのシステムはほとんどなく外注しているので自分は関係ない、ＩＴはどうでもいいのだと本当に言い切れるかというのは正直言って分からないというのが、今回のこのガイダンスの中で挙げているところである。

したがってここに関しては、場合によれば公認会計士と相談の上、本稿で述べたように対象範囲とするＩＴの範囲、これが、「あれはもう連結対象ではないのだから自分の評価対象にしていない。でも自分の売り上げの 80%ぐらいがそのシステムにかかわっている。それでも関係しない。自分は信用している」というのでは、ちょっと会計士に、「それは評価してもらわないと困ります」なんて言われてしまうと後々で困ってしまうかもしれない。そういう意味では、実施基準に明確に書かれてはいないのだが、こういったところのＩＴの範囲を決めるという意味では会計士と早めに相談しておく必要があると考える。

そのとき、「教えてください」と言うと会計士は教えられないので、教えてもらうのではなくて、「だから私たちは対象範囲としません、これでよろしいですね」という聞き方になると思う。そうすると「いや、それは対象範囲と考えます」と言われると思うので、こうして範囲を決めていくという形になる。

公認会計士は監査人なのでアドバイスはできないので、そこは理解して欲しい。だから、企業

として、評価対象範囲としては、例えば「A社のシステムだけにとらえております。私どもの在庫管理の情報はほとんどがB社に依存しております。でもB社はこういう会社で100%信頼できるので私どもは特段、評価対象の範囲にしておりません」というように明確に言い切ってしまえば、「いや、違います」と言われると思うので、それで分かるだろう。

これと同様に、ＩＴにかかわるリスクの評価や対応、ＩＴ統制をどう評価していくか。ここのＩＴ統制の有効性の判断、それから記録と保存をどうするか。これは多分、監査人、特に公認会計士の方々はＩＴに詳しい人ばかりではないので、分からないからこの辺りがすごくぶれてくる恐れがある。企業としては、ＩＴにかかわるリスクを、「我々はこのように考えてこのようにやりたいと思っています。これでよろしいですね。これで内部統制報告書に書くつもりです。これでよろしいですね」ということで聞けば、多分会計士は、「ちょっと持ち帰って検討します」というような形になって、後日教えていただける、という話になるのではないかと思っている。

やはりＩＴの部分というのは会計士のほうもあまり経験がない。新しい分野であるので、対応はちょっと念入りに行ったほうがいいのではないかと考えている。

3.5.16 IT の統制目標とアサーション／有効性評価

それからＩＴ統制の中で、特にこの有効性評価のところが大変難しいと思う。統制評価をどうするか、特に会計士はアサーションという言い方をする。アサーションにつながるものはというと、財務情報の完全性、正確性、正当性という三つのことを必ずいう（図 3.55）。

図3.55 ITの統制目標とアサーション

ITの統制目標	アサーション
完全性	網羅性、期間配分の適切性、
正確性	実在性、評価の妥当性、期間配分の適切性、表示の妥当性
正当性	実在性、権利と義務の帰属、評価の妥当性

そしてその中に、網羅性というと難しく聞こえるのだが、要するに取り引きのデータが全部入

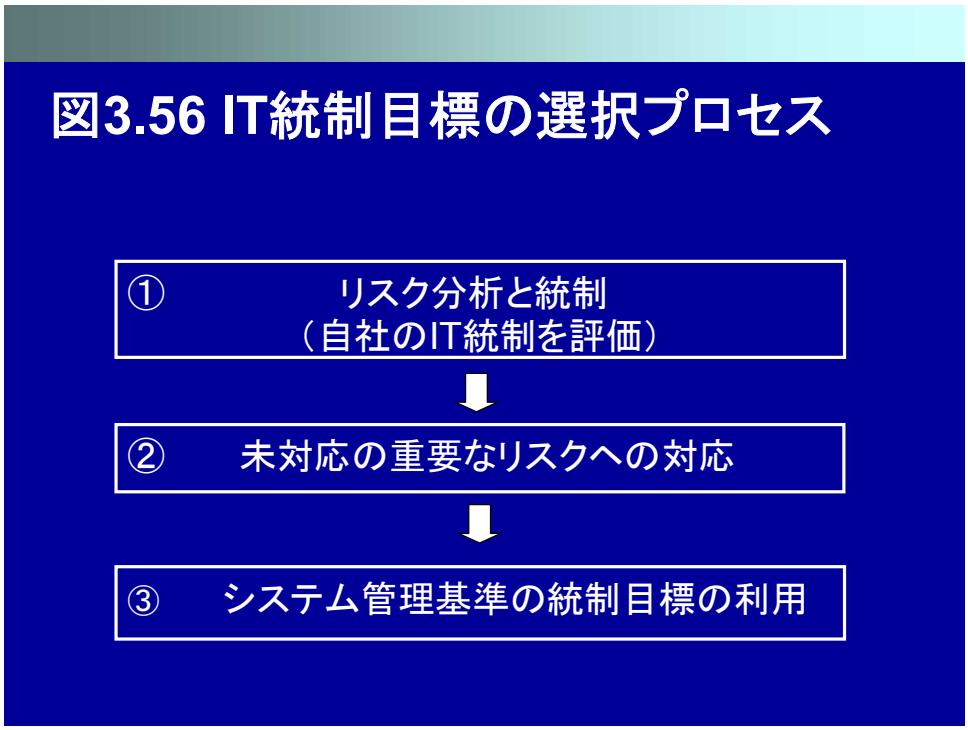
っている、という意味である。それから期間配分の適正性である。これは財務のかかわる事象、売り上げ（いつ売り上げたとかいつ販売したとか）、等々が決算期間の中に正しく入っている、という話である。

また、実在性（その取り引きがあった）等、いろいろと難しい言葉がたくさんあるが、こういったもので評価をしないといけない。それを経営者がちゃんとまとめてアサーションしなければいけないという話がある。ここが一番経営者にとってみると難しいところで、大変だろうと思う。このあたりはある程度、場合によるとコンサルタントに頼まないといけないかもしれない。

この辺が分かっている内部監査人の方がいれば、内部監査人を活用いただければと思う。経済産業省のほうのガイドラインもここまで踏み込んだものはなく、ここはちょっと手が出ていないというところである。

3.5.17 IT 統制目標の選択プロセス

さてこのガイダンスにおいて、後半では、ＩＴ統制目標をどのようにして決めていくかという話をメインにしている。統制目標の選択プロセスは概ね以下のような流れになる（図 3.56）。



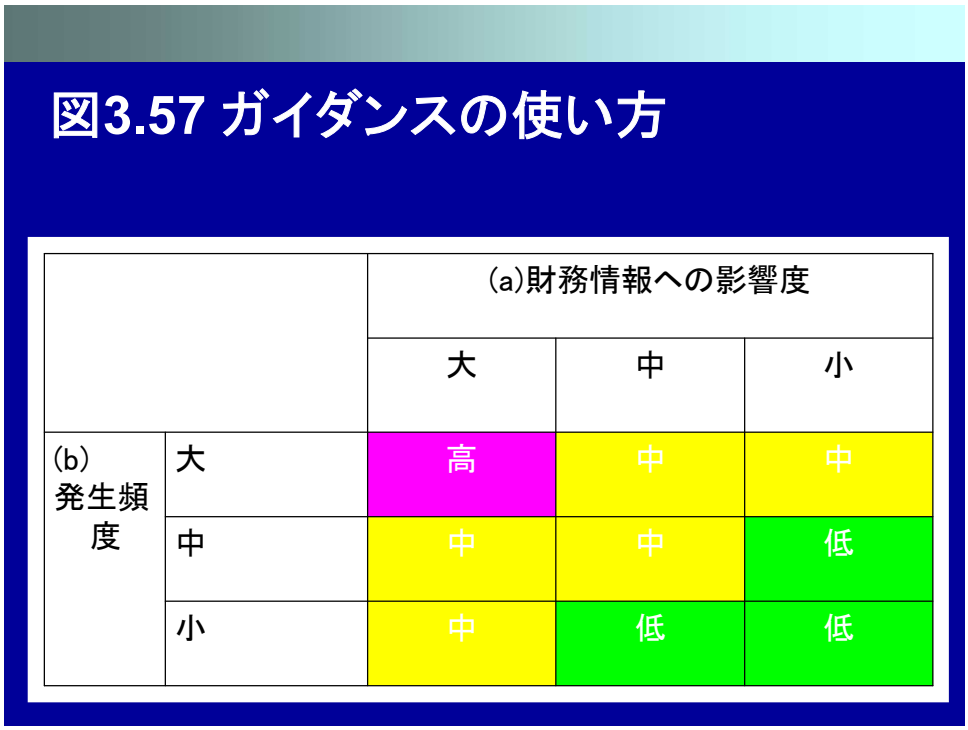
まず財務システムを見直し、その中で、いわゆる虚偽につながるとか財務報告が狂ってしまうとかエラーが出てしまうとか、そういう観点でもう一度リスクを見直していただきたい。財務報告のリスクをＩＴで見直して、中でデータが間違っていない、大丈夫だということを確認するようなことをやっていく形になると思う。

その中で特に、やはり「リスク」というのが大事になってくる。これは売上高で見るとかいろ

いろな見方があると思う。これは各企業のご判断で決めていただければいいのかと思う。

考え方としては、図 3.57 にあるような従来よくあるリスク分析である。そのリスク分析も財務情報への影響度、例えばいわゆるエラーが発生する頻度や虚偽が発生する頻度、それの大、中、小ぐらいを決めて、どのあたりまでやるかを考える。このあたりは、いわゆる通常のリスクマネジメントを想定していただければいいのではないかと考えている。

そしてリスクの分析等を行い、自社のＩＴ統制がどうなのかを考える。よく「文書化」と言われるが、では文書化とはどこで出てくるのというと、「ＩＴ統制は中でどうやっているのかは何も分からない。だから文書が要るのだ」というような話になってくると思う。



例えば過去に開発したシステムでよく会計士等に言われるのが、このシステムは一体どんな処理をやっているのかが分からないと言われてしまったときには、やはり文書化を何かやらないといけない。そのシステムの中でどういうデータがどのように作られているか、それを文書化する。米国のＳＯＸではその受け入れテストと同じテストをもう１回やる。それによってブラックボックスだけれども中でやっていることが間違いないということが保証できる。そのどちらかしかないと思うのだが、そんなことをここで考えていくことになると思う。

3.5.18 未対応な重要なリスクへの対応

この中で一番重要なのは、未対応の重要なリスクというのを見つけていくことであると思っている。経済産業省においてガイダンスを作っていく作業の中で、いろいろとヒアリングをさせていただいたのだが、企業の中で今回Ｊ－ＳＯＸの対象になる上場会社などは、大体情報システム

を入れるときにリスクを考えてそれなりのことをやって入れておられるようである。

何でもいいから買ってきて、などということはまずなく、日本の企業はやはりそれなりに優れた会社が多くて、それなりに考えてやっておられるので、私はここはリスク分析をやって抜けているところ、パッチワークを探せばいいのかと思っている。抜けているところ、「財務情報をそこまでちょっと考えていなかった。もうちょっと統制入れたほうがいい」というところの未対応のリスク、これを探すのが一番だと考えている。未対応のリスクが見つかったとき、それをどうやって埋めるかという段階になってくる。そうするとシステム管理基準みたいなものを引っ張ってくるということになる。

例えば、開発でちょっとチェックしていなかったとか、開発のときのテストがちょっと不十分だった、では開発のテストをそれなりにちゃんとやりましょうというようなことで開発のリスクが分かるという形になる。そうするとシステム管理基準の開発の部分を持ってきて開発をちょっと考えればいい。このような使い方をしていただきたいということで、今回システム管理基準を持ってきたところである。

であるので、例えばリスク分析をして、財務情報にかかわる重要なリスク、例えば「エクセルシートで何もチェックもしないでやっていた、どうも縦横の計算とかちゃんと合っているのだろうか。その確認はしよう」といったようなことを考えればよく、その確認をしたら“誰が”確認をしたのか、どういう表になっていてそれがあといついつのどのバージョンになっているのか、それを使ってもらえれば一応チェックはできている、だから統制は取れている、というようなことをやっていっていただければいいというようになると思う。

そういう形であとリスクがどうなのだというのを、もうちょっと網羅的に見ようと思うと、リスクコントロールマトリックス（後述）というものを使っていただくという形になると思う。そんな形で今回のシステム管理基準の追補版を作っている。

本稿では、システム管理基準だけを使えというように論じてはいるのだが、実はセキュリティの部分はシステム管理基準ではなくて､情報セキュリティ管理基準というものを持ってきている。ここで触れておきたいのは、別にシステム管理基準で足らなかったら他の基準を持ってきてもいいということである。

セキュリティ管理基準でもいいし、ＣＯＢＩＴのほうがいいと言われる方もあるかもしれない。ＣＯＢＩＴでもいいと思う。いわゆるこういった管理基準を持ってきて、リスクを減らせ、財務情報の信頼性が保てている、誰も改ざんできない、虚偽ができないということをちゃんと説明できる、そういうことがポイントになるので、そこをご理解いただければと思う。

よく、何かもうちょっと使いやすいものが欲しい、追補版も分かる、追補版と言っても、やはり 300 ほどの項目があり、これをチェックして全部最初からやるのかということを聞かれるのだが、そのようなことを一切我々は考えていない。

あくまでも各企業のシステムで財務にかかわるリスクがどこにある、それを見つけていただきたいと思っている。そのリスクを見つけるやり方がどうも分かりにくいというために一つ例示を入れているというように考えていただいたらよい。

システム管理基準追補版の中に表（統制に関する指針、統制目標、リスク）が入っており、こ

んなリスクの場合はこんなことをする、というのがいくつかある。これをそのまま使ってくれという意味で入れているわけではなく、これを参考にしてやっていったらいいよ、ということの例示に過ぎない。こういった項目だったらこんなことをやるのだということで、それは各企業に任されているところであって、これがそのままぴったり当てはまる場合はそのまま使っていただいて特に問題ない。

ただし、これを読んで全部やらなければいけないかということではなくて、各自のリスクに合っていればこれを使える、という形で表を作っている。たくさん表があって、これを全部やるのかというのがパブリックコメントでも挙がってきているが、一切そういうことは考えていない。

各企業がリスクを見て、その中でどんな統制が要るのか、「この統制がやはりできていない」と思ったときにそれを使っていただくという形になるので、この点はご理解いただきたい。

システム管理基準については、2004 年に経産省から改訂公表されたガイドラインで、300 ぐらいのことが挙がっている（図 3.58）。

図3.58 システム管理基準について

2004年に経済産業省から改訂・公表されたガイドライン

(1)	入力管理ルールを定め、遵守すること。	業務	情報システムへのデータ入力に伴う一連の作業について手順、検証方法、承認方法を明文化する	4-(1)-①	C	入力データの作成、授受、検証、入力の実施、入力後の確認、保管等、情報システムへのデータ入力に伴う一連の作業について手順、検証方法、承認方法を入力管理ルールとして明文化し、遵守する必要がある。
(2)	データの入力は、入力管理ルールに基づいて漏れなく、重複なく、正確に行うこと。	業務	入力データに欠落、二重入力等の誤りが発生しない	4-(1)-②	S	情報システムにデータを入力する際は、入力データに欠落、二重入力等の誤りが発生しないように入力管理ルールに記載されている手順に従い、正確に行う必要がある。
(3)	入力データの作成手順、取扱い等は誤謬防止、不正防止、機密保護等の対策を講じること。	業務	入力データの作成、取扱い等での不正を防止する		S	入力データの作成、取扱い等を正確に行ない、不正を防止するため、データの作成手順、取扱い等は、誤びゅう防止、不正防止及び機密保護等の対策を講じる必要がある。

記載内容は、入力管理ルールを定め順守すること、データ入力は入力管理ルールに基づいて漏れなく重複なく正確に行うこと、というような話しか入っていない。それに対して今回この管理目標というものを加えた。これは一体何をするためかというと、情報システムのデータ入力に伴う一連の作業について手順、検証方法、承認方法を書くことである。こういったことができていなければやらなければいけないということを書いた。これを見ていただき、基準としてどれを使うかというような発想で使っていただければと思っている。

3.5.19 リスクコントロールマトリックス

リスクコントロールマトリックス（図 3.59）について触れる。これはやや複雑なのだが、経営者のアサーションというところがあるが、これにどういったものがあるかというのは、先述したように例えば実在性、実際その取り引きがあったかというものに対して、例えば業務ごとにこのような表を作っていくというのがリスクコントロールマトリックスというものである。これは業務ごとに実際の業務の流れが本当に統制が取れているかということの検証のために用いる表である。コンサルタントが入って行うときにこういった表を作って、薦められると思う。

経済産業省がこれを載せた理由は、（コンサルタント業に関わる方々には申し訳ないが）コンサルタントがこういう表を１枚作るだけで数百万取ったりするというケースを聞いていて、経済産業省として、ちょっとそれは取りすぎではないかと。企業も自身で作成してみて、どうしてもできなければコンサルタントに任せて作ってもらったらいいのではないか、このような情報を渡しておけば、いわゆる売り手相場にならなくて済むのではないかという話で入れたものである。

これをやらなければいけないということを経産省が言っているわけではなくて、こういったものを使ってコンサルタントが業務システムについてきちっとチェックしていかないと、（彼らが）システムを網羅的にチェックしたとは言えないという形になる。

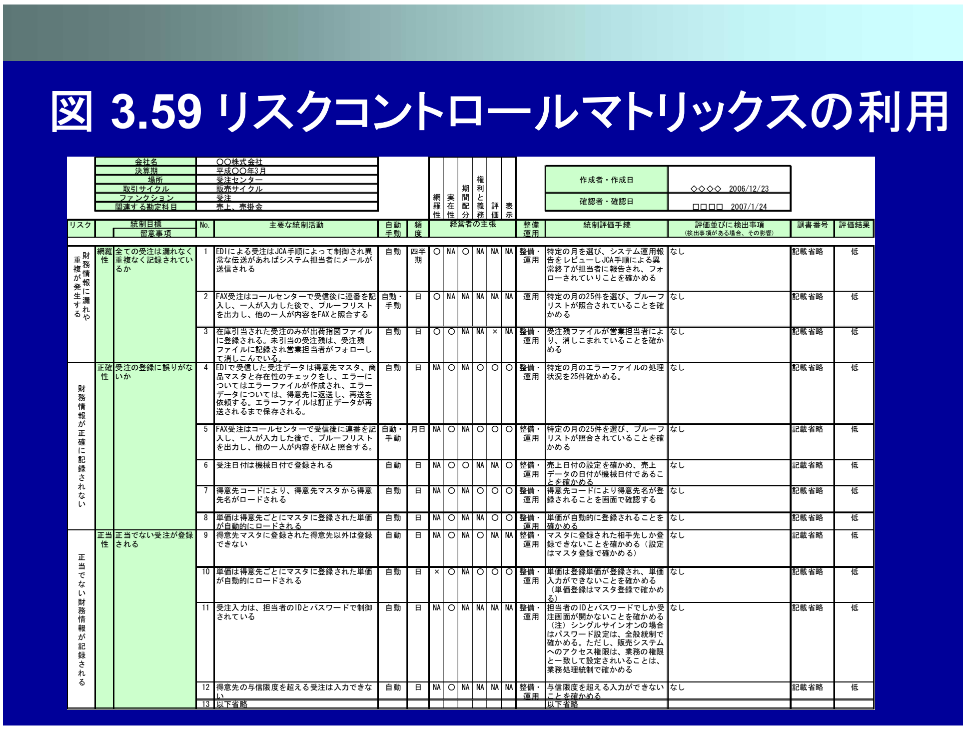


図 3.59 リスクコントロールマトリックスの利用

会社名	○○株式会社
決算期	平成○○年3月
場所	受注センター
取引サイクル	販売サイクル
ファンクション	受注
関連する勘定科目	売上、売掛金

作成者・作成日	◇◇◇◇ 2006/12/23
確認者・確認日	□□□□ 2007/1/24

リスク	統制目標	留意事項	No.	主要な統制活動	自動手動	頻度	経営者の主張：網羅性	実在性	期間配分	権利と義務	評価	表示	整備運用	統制評価手続	評価並びに検出事項（検出事項がある場合、その影響）	調書番号	評価結果
財務情報に漏れや重複が発生する	網羅性	全ての受注は漏れなく重複なく記録されているか	1	EDIによる受注はJCA手順によって制御され異常な伝送があればシステム担当者にメールが送信される	自動	四半期	○	NA	○	NA	NA	NA	整備・運用	特定の月を選び、システム運用報告をレビューしJCA手順による異常終了が担当者に報告され、フォローされていりことを確かめる	なし	記載省略	低
			2	FAX受注はコールセンターで受信後に連番を記入し、一人が入力した後で、プルーフリストを出力し、他の一人が内容をFAXと照合する	自動・手動	日	○	NA	NA	NA	NA	NA	運用	特定の月の25件を選び、プルーフリストが照合されていることを確かめる	なし	記載省略	低
			3	在庫引当された受注のみが出荷指図ファイルに登録される。未引当の受注残は、受注残ファイルに記録され営業担当者がフォローして消しこんでいる。	自動	日	○	○	NA	NA	×	NA	整備・運用	受注残ファイルが営業担当者により、消しこまれていることを確かめる	なし	記載省略	低
財務情報が正確に記録されない	正確性	受注の登録に誤りがないか	4	EDIで受信した受注データは得意先マスタ、商品マスタと存在性のチェックをし、エラーについてはエラーファイルが作成され、エラーデータについては、得意先に返送し、再送を依頼する。エラーファイルは訂正データが再送されるまで保存される。	自動	日	NA	○	NA	○	○	○	整備・運用	特定の月のエラーファイルの処理状況を25件確かめる。	なし	記載省略	低
			5	FAX受注はコールセンターで受信後に連番を記入し、一人が入力した後で、プルーフリストを出力し、他の一人が内容をFAXと照合する。	自動・手動	月日	NA	○	NA	○	○	○	整備・運用	特定の月の25件を選び、プルーフリストが照合されていることを確かめる	なし	記載省略	低
			6	受注日付は機械日付で登録される	自動	日	NA	○	○	NA	NA	○	整備・運用	売上日付の設定を確かめ、売上データの日付が機械日付であることを確かめる	なし	記載省略	低
			7	得意先コードにより、得意先マスタから得意先名がロードされる	自動	日	NA	○	NA	○	○	○	整備・運用	得意先コードにより得意先名が登録されることを画面で確認する	なし	記載省略	低
			8	単価は得意先ごとにマスタに登録された単価が自動的にロードされる	自動	日	NA	○	NA	NA	○	○	整備・運用	単価が自動的に登録されることを確かめる	なし	記載省略	低
正当でない財務情報が記録される	正当性	正当でない受注が登録される	9	得意先マスタに登録された得意先以外は登録できない	自動	日	NA	○	NA	○	NA	NA	整備・運用	マスタに登録された相手先しか登録できないことを確かめる（設定はマスタ登録で確かめる）	なし	記載省略	低
			10	単価は得意先ごとにマスタに登録された単価が自動的にロードされる	自動	日	×	○	NA	○	○	○	整備・運用	単価は登録単価が登録され、単価入力ができないことを確かめる（単価登録はマスタ登録で確かめる）	なし	記載省略	低
			11	受注入力は、担当者のIDとパスワードで制御されている	自動	日	NA	○	NA	NA	NA	NA	整備・運用	担当者のIDとパスワードでしか受注画面が開かないことを確かめる（注）シングルサインオンの場合はパスワード設定は、全般統制で確かめる。ただし、販売システムへのアクセス権限は、業務の権限と一致して設定されいることは、業務処理統制で確かめる	なし	記載省略	低
			12	得意先の与信限度を超える受注は入力できない	自動	日	NA	○	NA	NA	NA	NA	整備・運用	与信限度を超える入力ができないことを確かめる	なし	記載省略	低
			13	以下省略										以下省略			

特に、文書がないというようなシステムだと、業務の流れを見て、どんなシステムでどういう情報が取られてどうなっているか、そのリスクがどうなっているか、それについての対応が取れているか、こういうのをまとめていくのがリスクコントロールマトリックスである。

通常情報システムを作るときにはこのようなことを大体はやっているはずである。だからこれ

を新たに作るというのは普通はないのだけれど、結局文書がないとか設計が分からないとなるとこういうのを作ることになる。そうするとその分（費用が）高くなってしまうということなので、できれば自社で作るといいということで入れてある。

3.5.20 モニタリング

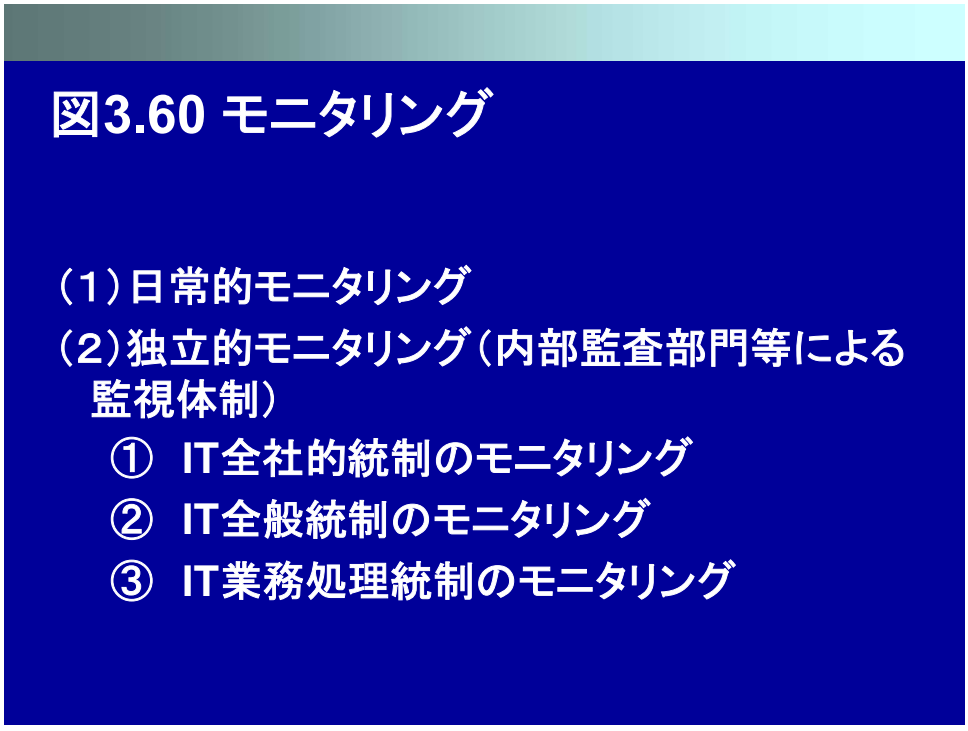
モニタリング（図 3.60）は、これがやはり今回新たに大きく入ってきた重要な点である。日常的なモニタリングと独立的なモニタリングの二つがある。日常的なモニタリングというのはどちらかと言うと IT 部門の業務に近い、いわゆるログ情報の取得等を言う。

2 番めの独立的モニタリングというのは、内部監査部門といったようなところにチェックをしてもらうことを言う。これら二つあるということをご理解いただきたい。

このモニタリングでどれだけログを保管しておかなければいけないとかいうのは、経済産業省としてはさすがに何も言えないところである。もし経済産業省が言ってしまうと関係各方面に多大な負担をかけてしまうかもしれない。経済産業省としてどう考えているかというと、各企業のリスクに応じて情報を保存しておけばいい、という言い方でしかない。

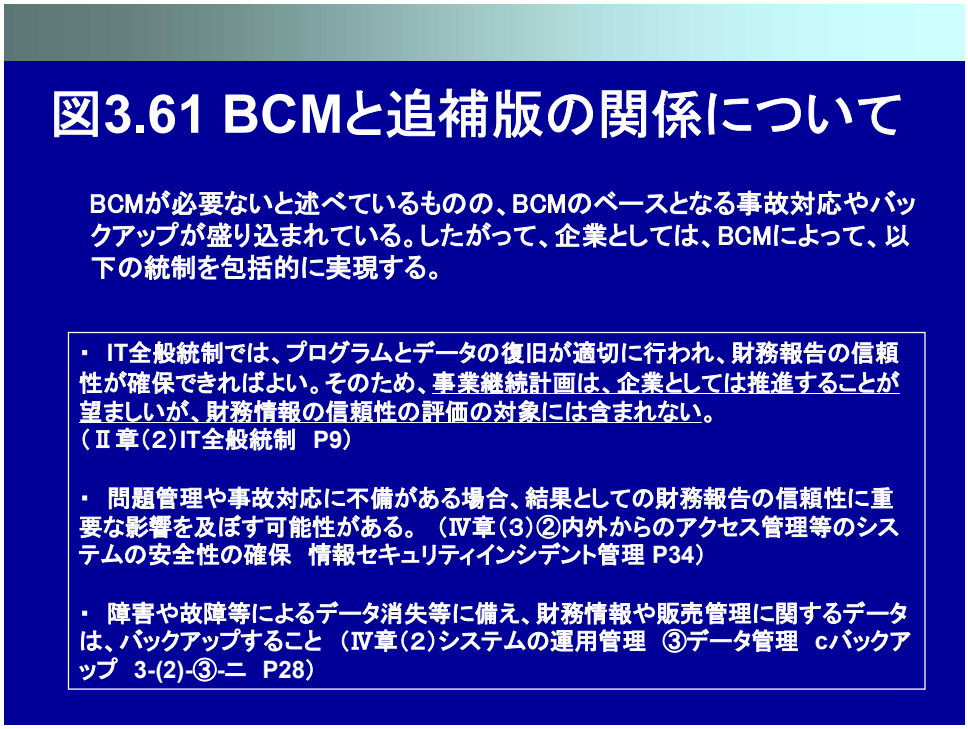
例えば何年間、この部分のデータを全部などというと何十ギガ、何百ギガバイトといったデータを取っておかなければならないという話になってしまう。これは、将来的に何か不正があったときにこのシステムのログがないと困ってしまう、そういうリスクに応じてモニタリングを考えていただければいいというメッセージとご理解いただきたい。

書いてしまうことは簡単ではあるが、各企業が自らのリスクに応じてどれだけのデータをどれだけの期間、どの種別、どう取っておくか、そこはお考えいただければという発想である。



3.5.21 BCM と追補版の関係について

最後に、ＢＣＭと追補版の関係について触れておく。



ＢＣＭというのはあくまでも各企業の、いわゆる大きい意味でのリスクマネジメントであり、ＩＴのリスクマネジメントもこれに含まれてくるものである。今この財務情報にかかわる部分でこれをやらなければいけないかというと、違うという判断を示している。

追補版本文中には図 3.61 のような書き方をしている。ＩＴ全般統制ではプログラムとデータの復旧が適切に行われ、財務報告の信頼性が確保できればよいということである。そのため事業継続計画は企業としては推進することが望ましいが、財務情報の信頼性の評価の対象には含まれない。だから財務情報の信頼性には、やっていればいいけれどもそのために事業継続計画をやれ、ということは言わない。こういう言い方になっている。

では何をしなければいけないか。バックアップは取っておいて欲しい。財務情報がなくなって消えてしまった、売上情報も何もかも消えてしまった、これでは正しい財務報告作れない。これはやはり困る、ということで、このデータ消失に備え財務情報や販売管理に関するデータをバックアップすること、これをご理解いただければと思う。ただしこのＢＣＭをやってはいけないということではなくて、企業としてＢＣＭに取り組むのは当然だと思っている。ただしいわゆる財務情報の信頼性にとって、ＢＣＭがなかったらだめだということではないという意味なので、そこの履き違いをしないでいただければと思う。

少なくともバックアップが取れていて、その財務情報が正しく作れていれば構わないということである。いわゆるＢＣＭがないとまずいのです、なんてことをいわれることがあり、管理基準にも事故の報告、記録、対応ルールと手順などと書いてあるので、この管理基準を持ってくると

やはりＢＣＭをやっておいたらいいかなんて思ってしまう方がおられる。

しかしそれはあくまでも企業のリスクで考えて、財務情報がなくなってしまったらやはり困るので、どうしてもＢＣＭが要ると思われれば入れられたらいいし、いや、うちはバックアップで十分だとお考えになるのであればそれで十分だということである。この財務情報の信頼性の観点で、どうしてもＢＣＭが必要だということは一切言っていないので、この点は十分にご理解いただきたい。

最後に、この追補版の意味を簡単に述べる。金融商品取引法に対応した実施基準があり、その実施基準の中にＩＴ統制というものが出ている。そのＩＴ統制をやはりやらないと財務報告の信頼性というものをなかなか信用してもらえない。公認会計士がそれを信用しない。そして内部統制報告書を書いていても承認してくれないということがあると困るので、ＩＴ統制としてどうやっていったらいいのか、金融庁が出しているものはそれなりに書かれてはいるが、まだあいまいなので、もう少し書いてみようか、というところにある。

ただ、この基準がこれだけあるから、これ全部やらなければいけないかということではなく、先述のとおり、各自の企業の中でのリスクを考え、そのリスクの中でどうしても要るものを取ってくればよい。その考え方として、追補版としてこういうものがあるのだと理解いただければと思う。

あくまでもシステム管理基準を全部やれというようなことは一切申し上げていない。財務諸表に係るリスクに対して何をやらなければいけないか。その統制をきちっとやっていただければいい。それを公認会計士に説明してご理解いただければいいのであって、これを全部やっていたら公認会計士がいいと言うかというと、そうとは限らない。あくまでもリスクに対応できていることが重要である。

3.6 事業継続マネジメントの構築の実際と実務

3.6.1 はじめに

本稿では、実際に BCP を作るときの留意点を中心まとめる。大きなポイントは次の３つである。

①事業継続マネジメントの基本的な考え方

②BCP 策定において誤解しやすいこと

③BCP 策定の進めかた、BCP の作り方

3.6.2 事業が 10 日間止まったら

BCP 策定を検討する場合に前提となるのは、「事業が 10 日間止まってしまったら」の元になる事象ではなく、その結果の想定である。発生事象が地震、台風、IT 事故等なんであろうと、事象の検討はとりあえず置いておくとのが事業継続マネジメントの基本的な考え方である。これは欧米の結果管理（Consequence Management）から出た考え方で、わが国では、原因からはいる「原因主義」に対して、「結果主義」と呼ばれることがある。

これが BCP の基本的な考え方である。この考え方を取り入れているために、BCP は想定外の事象に対応できるのである。

しかし、原因を想定せずに結果を制御することに、わが国の企業は慣れていないところがある。どうしも原因事象を考えてしまうので、いくつかの「想定外」事象について見ながら、結果主義の重要性を確認してみたい。

(1) 停電事故

昨年８月に東京で停電があった。水や電気は、わが国では止まらないというのが常識的な考え方であったが、思いがけない小事故で停電が起きてしまった。停電時間はわずか約５時間であったが、首都圏の事業継続に影響を与えるとともに、想定外事象への備えの必要性が再認識された。

この事故のちょうど３年前の同じ日にニューヨークで大停電が起きている。そのときは 29 時間も停電していたが、わが国では「対岸の火事」とみなし、真剣な対策は取られなかった。ほんの 5 時間停電が起きて初めて、わが国でも停電対策の必要性を認識したのではないだろうか。いわゆるビジネスフォン等を使用していた企業では、停電用電話機が役に立ったということで停電対策の見直しをしているようだ。

5 時間だから停電用電話でよいが、「事業が 10 日間止まったら」どうすべきなのかを考えなければならない。

⑵ 地下鉄、バス同時テロ事件

2005 年 7 月に、ロンドンの地下鉄やバスが同時に爆弾テロ攻撃を受けた（概要は右欄のとおり）。

事件後、各企業で BCP の検証が行われ、報告書が公表されている。

大きく、BCP の課題が 2 つ浮き彫りになった。

①エスカレーションの検討不足

②BCP の発動の明確化

ロンドン同時多発テロ事件概要

2005 年 7 月 7 日午前 8 時 50 分頃、ロンドンの地下鉄トンネル内の 3 カ所でほぼ同時に地下鉄の車両が爆発した。最初の爆発から 3 個目の爆発までわずか約 50 秒足らずであったといわれている。

また、同日の午前 9 時 47 分頃、大英博物館のあるラッセル広場近くのタビストック・スクエアを走行中の 2 階建てバス 1 台が爆発し、屋根を含めて 2 階部分が完全に吹き飛んだ。

この事件によって 56 名が死亡。ただし、その中に実行犯 4 名が含まれていた。地下鉄車両は完全に破壊され、施設にも被害を受けた。この事件について、捜査当局はテロリストによるテロと発表したものである。

⑶ 津波

わが国では、多くの企業が大地震のための BCP を策定しはじめたが、そのときの大地震による影響は主に「地震動」による被害に限定されているのではないだろうか。しかしわが国で起きうる地震は、首都圏直下地震だけではなくて、東海地震や東南海、南海地震など津波の被害があるものも心配されているのである。

例えば、2004 年の暮れに発生したスマトラ沖地震は、インド洋大津波と呼ばれる非常に激しい津波を起こし、平均で高さ 10m に達する津波が数回、インド洋沿岸に押し寄せたという。地形によっては 34m に達した場所もあったようだ。

津波とは、水の力によって物や人が壊れることで、大地震を考える時に沿岸部にある事業所の BCP では当然想定しておかなければならない事象である。大地震の BCP 策定において、津波に対する事業継続対策を考えて対応策は講じているか、疑問である。

津波によって、「事業が 10 日間止まったら」どうすべきなのかを考えなければならない。

⑷ 台風・豪雨災害

日本が誇るスーパーコンピューターである「地球シミュレーター」が、日本の夏の豪雨日数を予測した結果によると、1 日 100 ミリ以上の雨が降る日は、2000 年以降、急激にその日数が増加していくと出た。地球温暖化の影響ということになろうが、これによって事業中断がないとは限らない。

この台風や豪雨災害で、「事業が 10 日間止まったら」どうすべきなのかも考えていかなければならない。

⑸ 鳥インフルエンザ

鳥インフルエンザと BCP が何の関係があるのかという人がいるかもしれないが、外資系企業を中心に BCP において鳥インフルエンザ対策が講じられている。鳥インフルエンザは、今はま

だ人から人にうつるという事態になっていない。WHO のレベル分けによると、レベル 3 という状態であるが、今年世界的に大変心配された事象であった。パンデミックとか Avian Flu とかいわれる。

1918 年にスペイン風邪が大流行し、感染者約 6 億人、うち死んだ方が 4000～5000 万人に上る「大災害」が起きた。当時の人口が 8 億人から 12 億人なので、世界の人口のほとんどが感染したといってよい。また、第二次世界大戦での戦死者が 1500 万人、軍人が 2500 万人ということになっているので、スペイン風邪の死亡者数は戦争よりも多かった。これが新型インフルエンザの大規模感染、つまり「パンデミック」といわれ、心配されているものである。鳥インフルエンザがその新型インフルエンザになりうるという心配である。

わが国でも大感染が発生し、かなりの死亡者を出した。日本災害史をひも解くと、当時の役所から国民に対して、「手を洗いましょう、マスクをしましょう、うがいをしましょう、感染者が出たら隔離をしましょう」と、今と同じような安全衛生上の対策の呼びかけが行われていた。

このスペイン風邪の後に、1923 年に関東大震災が起きて、14 万人以上が死亡し、その後いろいろな経済的なインパクトが起きて、戦争に至ったという、忌まわしく、かつ前兆的な出来事であったわけである。鳥インフルエンザが大流行した後に首都圏直下型地震が起きるというのと、非常に似たところがあるのではないかと思う。

事業所で鳥インフルエンザ患者が発生したら事業所を閉鎖しなければならないかもしれない。それによって「事業が 10 日間止まったら」どうすべきなのかを考えておくべきだろう。

3.6.3 想定外を想定する（Expecting the Unexpected）

このように考えてみると、思いもよらないことが最近次々に起きていることが分かるだろう。2001 年のニューヨーク同時多発テロ事件の際に、「Expecting the Unexpected」という、予期しないことにどう対応していくのかということが、議論された。

日本でも、想定していなかったということが言い訳になる時代は終わった。想定し得ないことにどのように対応していくのかということを、危機管理の基本として、検討していかなければいけない時代になったのである。

BCP は、実際に起きてしまった時の対応策が中心であり、事前に災害の予防をどうするのかという「防災」とは大きく違うことを改めて認識すべきである。これが最初に述べた結果主義である。

「結果」から考える、「結果」をコントロールしていくことが重要で、「結果」のもとである「事象」を予防するのは、防災や防犯というジャンルでやればよい。

3.6.4 BCP について誤解しやすいこと

BCP 策定や検討の際に、誤解しやすいことを次にまとめる。

(1) BCP はマニュアルではない

BCP は、Business Continuity Plan の略称で、「計画」である。この計画をマニュアルと間違

っているケースが多く見られる。

マニュアルは、「BC マニュアル」である。BCP は、いわゆる対応マニュアルや手順書とは違うことを理解する必要がある。

いわゆる対応手順は、SOP（Standard Operating Procedure 標準手順書）としてまとめられるが、そうした標準手順書と、今後どのように BCP の活動していくのかという活動推進計画、対策整備計画、緊急時の活動計画などとは同じではない。

これらをすべて含んだものを本来 BCP というのである。わが国ではその中の標準手順書のところだけに、フォーカスが当たってしまっているのではないだろうか。

海外の BCP はどんな目次になっているのかについて、各種テンプレートや書籍等を見ると、BCP のプロジェクトを始める方法、推進体制、予算、企業の事業リスク、緊急事態のインパクト評価、その後にはじめて緊急事態への準備や DR（現場の復旧）方法、BC（事業の復旧）などが書かれている。

そのうち緊急事態への対応と復旧の部分が、いわゆる対応マニュアルであるが、それだけが BCP ではない。その前後の計画のテスト、教育訓練、計画のメンテナンスと等を含めていかなければならない。これが計画である。

対応マニュアルはもちろん重要である。しかし BCP の PDCA を回していくときに、事業継続に関する推進計画や整備計画がないと、PDCA は回らない。対応のためのマニュアル（手順書）を作っただけでは、活動が継続しない筈である。対応マニュアルを策定したあとに、それを従業員に周知徹底をして改善をしていくという、Plan、Do、Check、Act のプロセスがあって初めて、継続的な活動ができるのではないだろうか。

BCP の P（lan）の意味が曖昧なために。最近では P を外して、BC などと言っている向きがある。では BCM は Business Continuity Management ではなく、BC マニュアルの略かなどという妙な議論を耳にしたりする。

例えば消防計画とか経営計画はマニュアルではないだろう。これから防火や経営において何をしていくのか、どういうふうにやっていくのか、いつまでに何をやるのかが主として書かれたものであろう。決して消防マニュアルや経営マニュアルではない。

(2) BCP は大規模地震対策ではない

わが国の企業は、例えば東京湾北部地震が起きたときに、被災事業所を短期間で復旧するために策定するのが BCP であると誤解しているところが多く見られる。しかし大規模地震では、自分の事業所だけで解決し得ない問題（特に、社会インフラの早期復旧）が多い。例えば、電力復旧には、6 日間かかる、ガス、水道は 1 ヵ月以上かかるという状況の中で、被災事業所をどのようにしたら短期間で復旧できるであろうか。欧米の BCP の前提は代替拠点での業務再開であり、大地震発生時に被災事業所を短期間で復旧しようという考え方自体に矛盾があると考える。

大地震にこだわらずに、パンデミック、テロ、大規模停電等すべての不測の事態を念頭に入れて BCP の策定を行うべきである。大事なことは不測の事態の予防ではなく、結果の抑制、つまり経済的損失をいかに軽減していくのかに着目することである。これが BCP の基本的な考え方

である。

BCP は大規模地震対策ではない。不測の事態というのは、IT 等の事故、テロ、サボタージュ、生産ライン停止、自然災害等極めて多岐にわたる。地震は、その中のひとつでしかない。BCP で対応すべき事態は、これらのすべての事態であるが、1 事象ごとに BCP を作るのは大変なので、結果の抑制に注目して、BCP を作るというわけである。

当然リスク分析は当然実施すべきプロセスであり、その中で自社にとって重要なリスクを限定して、それらについて詳細マニュアルを作るのはまったく問題ないが、BCP の推進体制や整備対策を実施する際には、すべての事象をやはり考えていかないと、対策に漏れがでてしまうのではないだろうか。

(3) 最悪事態だけ想定してはいけない

危機管理では、「最悪事態を想定して行動せよ」といわれる。これ自体は誤りではないが、BCP において最悪事態だけを想定していると、結局は的確な対応をすることができなくなることがある。BCP では、対応すべき事態のレベル分けを行っておくことが重要である。例えば、IT 事故の場合、火災の場合、大規模災害の場合ごとに事態のレベル分けをして、そのレベルごとの最悪事態を想定するのである。すべての災害の中で、最大規模である事態だけを想定して BCP を策定すべきではない。

少しずつ情報が入ってくるに従って、災害の規模も大きくなってくる事態が起きたときに、その災害規模の展開に応じた形で対応を考える。これがエスカレーション（段階的拡大）という戦術である。

エスカレーションを考える場合には、現場で対応できること、会社全体で組織的に取り組むこと、そしてマスコミ対応を含めた危機広報まで検討する必要がある。BCI の BCP に関するガイドラインでは、対応レベルを 3 段階に分けている。レベル 1 は、いわゆる危機広報である。風評リスクが顕在化しないように、マスコミ対応を的確に行うレベルである。そして、会社全体で復旧のところを考えるレベル 2，部門別で対応するレベル 3 がある。事態の進展に伴って、レベル 3 から 2、1 と対応を段階的に拡大していくことが重要である。それぞれのレベルで事態を抑えることがもちろん目的である。

中小企業庁の BCP のガイドラインでは、エスカレーションを「緊急事態の進展に合わせて、対応体制を拡大したり、判断者をより上位者に移行したり、対策内容を高めていったりすること」と定義している。

このエスカレーションで段階的に対応を拡大していくが、なるべく下位のレベルで収束するように対応することが重要である。

(4) 「はじめて」BCP に取り組む場合には BIA は簡便に

誤解を生むことを承知の上で言えば、BCP に「はじめて」取り組む企業では、ビジネスインパクト分析（BIA）は、簡単にすませる方がよい。本格的な BIA は大変ロードのかかるプロセスである。確かに重要なものであるが、本格的な BIA の後に BCP の策定に入ると息切れするおそれ

がある。自社の中で何が重要な業務か、それがどのくらいの影響を与えるのかなど社内調整が大変である。

大企業や組織的な意志決定手続きとして BIA が不可欠な企業では、本格的な BIA はもちろん必要であり、その場合には、BIA 実施後に計画策定を行うべきであることはいうまでもない。

3.6.5 BCP の取り組み方

中小企業庁の BCP ガイドラインに基づき、段階的に BCP の簡単な取り組み方を紹介する。ガイドラインを読む場合には、指針の背景にあるものが最も重要であることに留意したい。つまり、何が書いてあるかではなく、「なぜこう書いてあるのか」という視点を常に持ってほしい。

(1) BCP サイクル

本来、PDCA を回す仕組みは BCM(Business Continuity Management)であるが、中小企業庁のガイドラインでは、それを「BCP サイクル」と呼んでいる。

この BCP サイクルとは、「事業の理解」、「BCP の準備」、「BCP の策定」、「文化の定着」、「維持更新」という要素から構成されている。

①事業の理解

「事業の理解」とは、妙な言葉と感じるだろうが、自社のすべて知っている人は数少ないと思う。

そこで BCP 策定の最初に、「自分の会社は何をやっているのだろうか」について改めて整理してみることが重要である。例えば、財務状況やいざというときの運転資金の状況などを整理してみるのである。

②BCP の準備

BCP では、被災事業所を復旧することが主ではなく、無被害の他事業所や代替拠点等での事業再開策、いわゆる代替策の決定が必要である。代替策の決定に当たって、事前に必要な準備をしておくことがこのプロセスの意義である。

③BCP の策定

実際に BCP の発動基準等の整理や BCP の文書化等を行うプロセスである。

④文化の定着

BCP を総務部なり現業部門で作っただけでは、機能しない。BCP を実行する従業員に周知していかなければならない。その際に、BCP を無理やり押し付けるのではなく、従業員が「もっともだ、なるほどな」と思う、つまり自社の“カルチャー”として定着するのが、ベストである。

BCP の「文化」と言うものの、これはいわゆる「文化」ではなく、自社に根付くという意味である。

⑤BCP の維持更新

BCP を自社に根付いたものにするには、教育・訓練が必要である。また、PDCA を回していくために、現状の BCP でいいのかなどをチェックし、維持更新をしていくことも必要である。

(2) コース別 BCP

中小企業庁のガイドラインでは、BCP 策定を基本コース、中級コース、上級コースの三つのステップに分けられている。

基本コースは BIA を除くと、１日か２日あればプランできるもの、中級コースは、１週間くらいあればできるもの、上級コースは、中級コースに飽き足らない企業や非常に複雑な組織などが自分たちで考えるべきものである。

初めに基本コースでまず外形的に BCP を作り、それをステップアップして、中級コースに至ることを想定している。このため基本コースと中級コースでは、項目が少し変わっている。中級コースのほうが難易度が上がっているので、自社のレベルに応じて、基本コースから始めるのか中級コースから始めるのかを決めればよい。

BCP 策定が最優先であり、「とにかく作ろう」というのが背景にある考え方である。このガイドラインは中小企業向けであるが、初めて BCP に取り組む企業であれば規模の大小は問わないと位置付けている。

①初動対応の考え方

BCP の中の対応マニュアルの部分だけで取ってみると、大きく二つに分けられる。何か起きたときの初動対応とその後の復旧対応又は業務の再開対応である。

ある規模以上の企業では、火災や地震発生時の初動対応については計画しているところが多い。緊急事態が起きたときに、それを認識して、二次災害の防止措置を講じたり、従業員を招集したり、従業員の安否や被災状況を把握したり、ということを決めていると思われる。

しかし初動対応は、復旧を見据えたものにしなければならない。例えば、地震対策の初動対応マニュアルでは、地震により施設が壊れた場合、その施設内での業務を復旧することまでを考えて初動対応を規定しているのかを検証してみる必要がある。企業にとっての初動対応は、事業の復旧、再開など復旧対応の手段であるという位置付けをすべきである。事前準備、初動対応、復旧という一連のプロセスの中で災害時にはじめに行うのが初動対応なのだという認識が必要である。

はじめて BCP に取り組むときには、復旧を見据えた初動対応についてのみ規定してもかまわない。その際に復旧、再開を目的にしている初動対応なのだという自覚が必要である。例えば、地震対策で安否確認の必要性がいわれるが、安否確認は何のためにするのだろうか、ということを例に挙げよう。

安否確認というのは復旧に従事できる無事な人間が何人いるのか、誰が出てこられて誰が出てこられないのかを把握するために、本来企業としては実施すべきものであると考える。従業員の

人道上の問題でやるわけではない。(死亡や負傷した従業員に対しては自社の福利厚生としてやらなければいけないのは当然のことであるが、安否確認とは別問題である)

②復旧対応の考え方

初動対応の後に、お客様や関係会社への連絡や自社の中核業務の継続方針策定などを行う必要がある。これが、第２段階の復旧対応である。

第２段階の復旧対応は、次の三つに分けられる。

・お客様、協力会社向けの対策
・従業員、自社の資産の対策
・財務対策

これらの復旧対応にかかる対策が既存のBCPに含まれているか、点検することが必要である。

③復旧対応策策定上の留意点

- 自社の中核事業の継続方針や継続体制を確立しておく必要がある。どれだけの期間で復旧するのかという目標を決め、そのための対策や方針を決めるのである。例えば、鳥インフルエンザの患者が１名でも出ると、事業所は閉鎖しなければならなくなると思われる。そうした状況では、ものは壊れていないにもかかわらず、代替の拠点を設置して業務を続ける必要が出てくるだろう。
- 協力会社等が被災して、自社が無傷なのに仕事ができない場合には、取引調整が必要となる。場合によっては、被災した協力会社の復旧支援をしなければならないことまで視野に入れて対策を講じていく必要がある。
- 従業員や資産の保護については、従業員が被災した場合の生活支援も検討すべき事項である。
- 財務上の対策として、決済、不渡り対策も必要である。これもBCPの一部となる。また、仕入れの支払いや従業員の給与支払いも重要な対策である。
- 復旧資金の調達もあらかじめ検討しておきたい対策である。

(3) 文化の定着

①文化の定着のための３つの質問

BCP文化が定着しているというためには、次の３つの質問に自信を持って「はい」と言えなければならない。

○BCP活動を実施することに従業員が賛成している、賛同しているか。

企業のBCP研修は、まだ従業員にBCPを知ってもらうことが主体になっているように思われる。文化が定着しているということは、従業員が自らBCPを理解して、賛成しているという状況である。

○緊急時、出社可能な従業員は会社に来てくれるか、くれそうか。

不測の事態が起きて出社できない状況になっても、業務遂行に使命感を持って、従業員は出社し事業復旧に従事してくれるかどうかということである。

○従業員は何を行うべきか、理解しているか。

マニュアルがなくとも、緊急時になすべきことを体で覚えている状況が望ましい。そうなってはじめて BCP が社内に定着したと言えるだろう。従って対応マニュアルは、社員が指示されなくとも自動的に行動できる「自動的行動」を主体としたものにすることが望ましい。そのために重要なのが、教育である。BCP の重要性を理解させたり、BCP の技術や技能を習得させておく必要がある。

また、訓練や点検も重要である。緊急事態は頻繁に起きるものではないので、訓練や点検が必要なのである。訓練や点検を PDCA サイクルの中に位置付け、定期的に実施することが重要である。その際、従業員のレベルに合わないことを実施しても仕方がないので、習熟レベルに応じた訓練、点検の方法を確立しておく必要がある。

検討したい訓練の種類には次のようなものがある。

・机上訓練

地震等でいういわゆる図上訓練やシナリオシミュレーション

・情報連絡訓練

テロのような少しずつしか情報が入ってこない場合に非常に重要になる。

・代替施設への移動訓練

バックアップ拠点にどういうふうに人を配置するのか。例えば被災事業所に 1000 人いたとしたら、1000 人をバックアップ拠点に遣ってしまったら、被災事業所の復旧をどうするのか等を検証する。

・バックアップ情報の回復訓練

データバックアップ、プログラムのバックアップ等を元に戻してみる訓練である。

・防災訓練への参加

事業所や地域の防災訓練への参加からはじめるのもよい。

②文化の醸成において求められること

文化の醸成に際しては、経営者と従業員それぞれが意識しなければならないことがある。

経営者には従業員の安全や雇用を守る姿勢が必要である。これを是非前面に押し出して BCP を推進してほしい。

一方、従業員は、BCP が企業の存続にとって不可欠であるということを自覚しなければならない。中小企業庁では、BCP を「緊急時企業存続計画」と呼んでいる。その趣旨は、中小企業の場合には、何か非常事態が起きて、事業継続が難しくなると企業の存続そのものに影響が出てしまうと考えられているためである。それだけ財務体質等が弱い企業が多いのであろう。

③BCP コミュニケーション

取引先や協力会社を意識しながら、サプライチェーン全体で事業継続を図っていかなければならない時代になっている。このために BCP コミュニケーションとして、関係会社や地域を含め、BCP に関する情報共有や共同作業を行っていくことも必要である。

④BCP の診断、維持・更新

中小企業庁のガイドラインの中に BCP 自己診断チェックリストがある。継続方針、運用体制、事業の理解等に関して１０数項目設定されているので、一度チェックすることを勧める。

3.6.6 おわりに

中小企業庁で議論した際に、「身の丈サイズの BCP」を作ることが重要だという認識を共有した。自社でできる範囲やレベルを見極め、自社の「身の丈サイズに合った」BCP づくりを進めることによって、BCP は無理なく組織に定着できる。

また、初めから完璧を求めないことも重要である。初めから完璧なものを作ったら、PDCA のサイクルが緩くなってしまう。継続的改善を図りながらレベルアップすることが重要である。

最後に、BCP を検討していく中で迷いが出てきたら次のことを自問自答してみたい。これを考えるプロセスが BCP を作り上げていく中で、一番大事なことだろうと考える。

・自分たちは会社の何を守ろうとしているのか
・会社を何から守ろうとしているのか
・会社をどのように守ろうとしているのか

3.7 ＩＴの脆弱性とＢＣＭ

3.7.1 はじめに

IT の脆弱性と BCM（事業継続管理）について、特にセキュリティ・インシデントを考慮した BCM への対応を中心に説明します。

また、独立行政法人 情報処理推進機構（略して IPA）という組織が、セキュリティ・インシデントに対して何をしているかも説明します。ひょっとしたら「IPA の者ですけれども、御社の WEB サイトに脆弱性の問題があります」という連絡が行く可能性もありますので、そのような時に「IPA ってどこの者だ」とならないようにしたいためです。

なお、BCP とか BCM の詳細は、ほかの説明を参考にしてください。

セキュリティ・インシデントに対応して、具体的にどのようなことを考えていく必要があるかをまとめています。

海外も含めて重要インフラとか、社会をきちんと守っていこうということで、どのような活動がなされているかということも説明します。

(1) IT 依存の進展

図 3.62 は、多様化するリスクということで、家庭・個人、ビジネス・企業、コミュニティ・社会に対するいろいろなリスクがあるということを示し、これがますます複雑化し、増加しています。このような多様なリスクに対してきちんと対応していかないと、事業を継続できないということです。

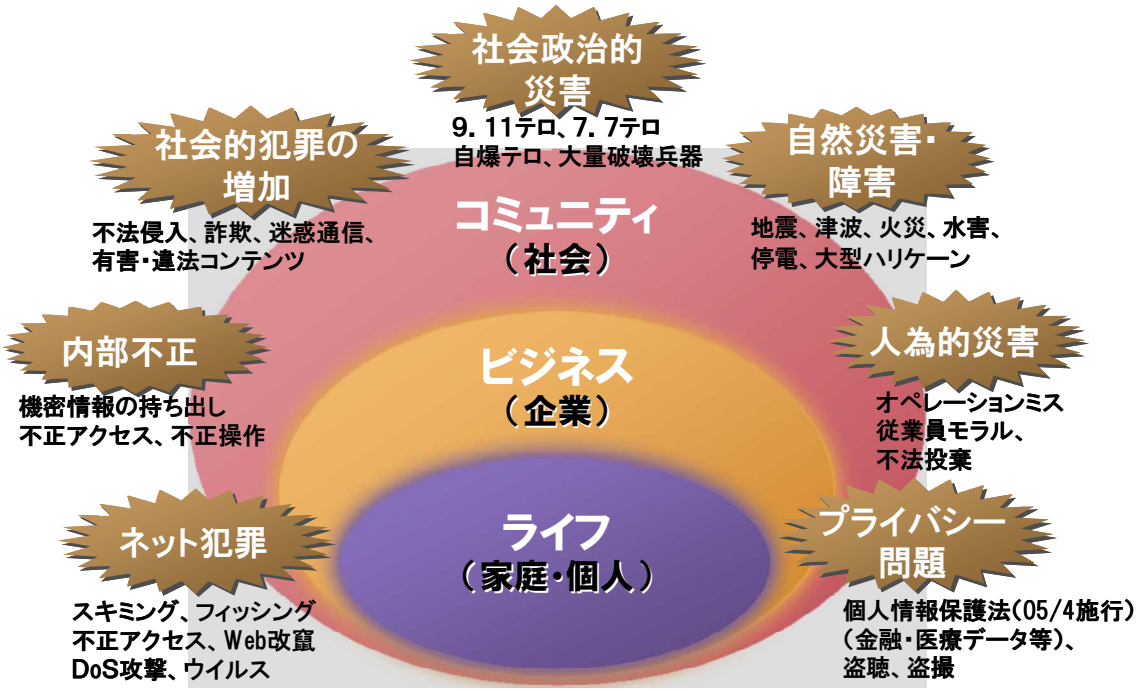


図3.62　多様化するリスク

IT システムへの依存増加についてですが、自分の作った「システムを止めない」、バグを出さないということがこれまでは一番の目的だったと思います。しかし、今や経営の視点からは、「ビジネスを止めない」ということで、「ビジネスの重要なプロセスについては、可能な限り停止しない。できれば一瞬たりとも停止しないこと」ということが要求されています。IT システムはそのビジネスプロセスの中で、経営にも直結している基盤となってきています。すなわち、「IT を利用した経営」というものになってきているということを、皆さんも認識されていると思います。

(2) BCP/BCM とは

経済産業省が 2005 年 3 月に、「事業計画策定ガイドライン」を出しました。筆者は、この中の IT 関係のところの作業に、ワーキンググループ委員として参加しました。

また、情報処理相互運用技術協会、INTAP の事業継続性技術委員会の委員長として、BCP について 3 年間ほど IT 事業者の視点で調査し、「ビジネス継続性技術調査報告書」としてまとめました。

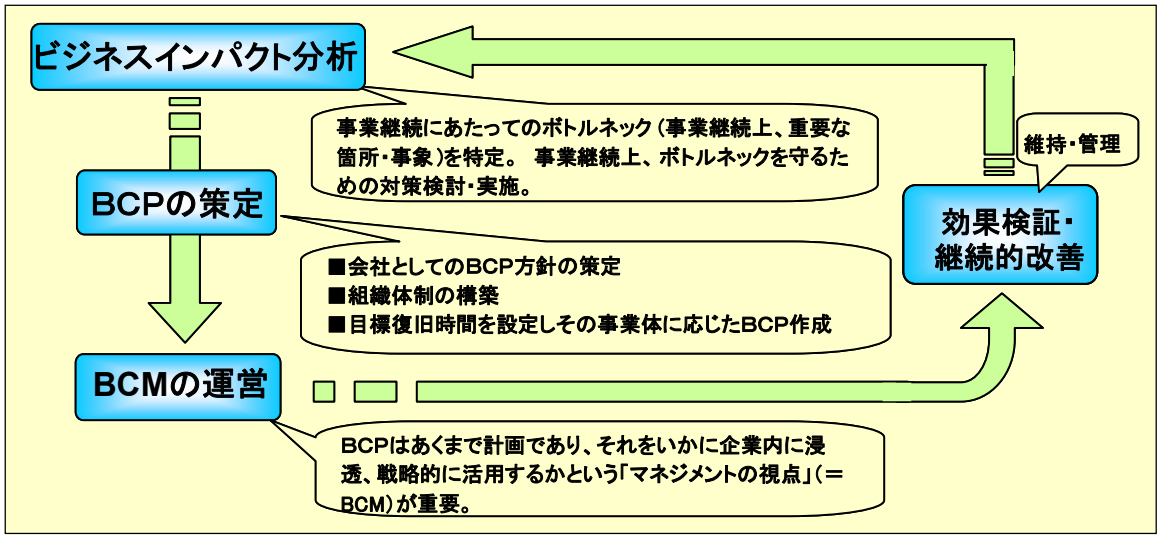
参考文献

事業継続策定ガイドライン（経済産業省）（2005年3月）
http://www.meti.go.jp/report/downloadfiles/g50331d06j.pdf
事業継続ガイドライン第一版（内閣府中央防災会議）（2005年8月）
http://www.bousai.go.jp/MinkanToShijyou/guideline01.pdf
中小企業BCP策定運用指針（中小企業庁）（2006年2月）
http://www.chusho.meti.go.jp/bcp/
ビジネス継続性技術調査報告書(情報処理相互運用技術協会)（2005年3月）
http://www.net.intap.or.jp/INTAP/information/report/16-business-report.pdf

図 3.63　BCP の参考資料

以降の説明では、経済産業省の「事業計画策定ガイドライン」の用語や内容を使って説明しています。

BCP の構築、運用の PDCA サイクルについて図 3.64 に示します。P - D - C - A のサイクルのできるところから、IT 関係についてもできるところから、BCP にチャレンジしていくことが大切だと思います。



出典：経済産業省報告書

図3.64　BCPの構築・運用のPDCAサイクル

IT システムに対する一般的な BCP では、本社とか支社、事業所のシステム構成に対して、どこのネットワークを二重化しようか、データセンターを利用する場合には、データセンターを東京と大阪に分散させ、そこの間でのバックアップをどうするかとか、広域災害が起きたときにどうするかとか等を対象として考えると思います。本稿の以降の説明では、このような IT システムに対してではなく、多くの企業で使用されていて、いろいろな業務が稼動するウエブアプリケーションとそのシステム（以降ウエブサイトと呼ぶ）についての BCP についてです。ウエブサイトは、社外の方とのポータルという位置付けで、企業の情報を発信します。企業のイメージ、ブランドを発信するということになってきています。このウエブサイトでのセキュリティ・インシデントが発生したときの BCP について以降説明します。

詳細の説明は別の章で行いますが、BCP ではまず適用範囲を決めます。ウエブサイトのセキュリティ・インシデントの適用範囲の例は、以下のようです。

＊ソフトウェアの脆弱性を悪用した不正アクセス、コンピュータ・ウイルス感染やウエブ改ざん等により業務の停止・低下、個人情報の漏洩や情報の改ざんなどの発生により顧客・協力会社や社会から信頼を失い、経営に重大な影響を及ぼすことを想定した BCP を策定する。

次に、ビジネスインパクト分析をします。すべてのウエブサイトに対してではなく、例えばオンラインショッピングをしているのであれば、オンラインショッピング系のウエブサイトの優先順位を高くするとか、事業とどう関係するかで、目標復旧時間というものを設定するとかを分析していきます。たとえば、４時間以内に再立ち上げしないとまずいとか、あるいは１日ぐらいだったら我慢できるとか、こういう分析をします。

3.7.2 セキュリティ・インシデントと BCM

(1) IT 脆弱性とは

脆弱性という言葉、なかなか難しい言葉です。セキュリティ・ホールと脆弱性は、意味的には同じですけれども、この認知度を去年の 11 月に調査しますと、セキュリティ・ホールが 63.6%の人が知っている。脆弱性というと、なかなか難しい漢字で初めてだとどう読むのか、キジャクセイとかいろいろ読むケースもあるのですが、49.8%でした。50%未満ということです。脆弱性についての認知度がまだ低いということが分かります。

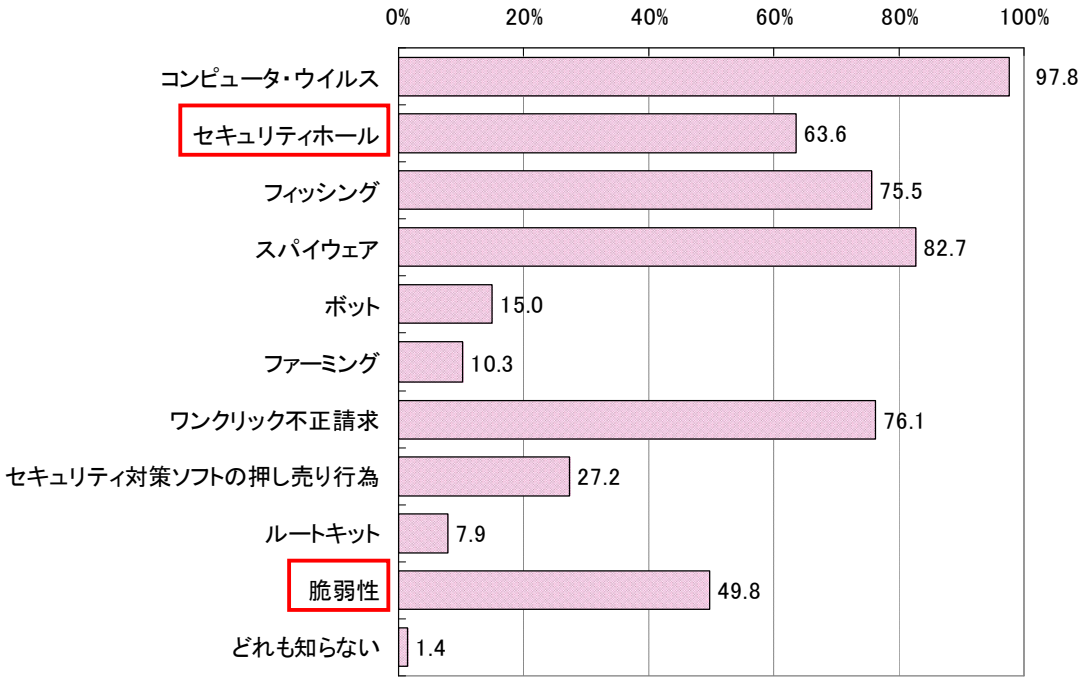


図3.65 情報セキュリティに関する言葉の認知度 [回答者全体:5，316](複数回答)
調査方法 ： ウェブアンケート調査　　調査期間 ： 2006年11月15日～11月16日
調査対象 ： 15歳以上のPCインターネット利用者

脆弱性とはどういうものかというのが、経済産業省の告示に定義してあります。「ソフトウェア等においてコンピュータ・ウィルス、コンピュータ不正アクセス等の攻撃により、その機能や性能を損なう原因となり得る安全性上の問題箇所」と定義されています。ウエブアプリケーションについても、同じように「安全性が欠如している状態を含む」となっています。

脆弱性は、より簡単に説明しましょう。インターネットは良い人だけが使っているわけではなくて、必ず悪い人がいます。50 年前、私が子供のとき、田舎でしたら家に鍵もかけず開けておいても、周りの人は良い人だから、家には悪意を持って入って来ないのですけれど、最近ではそういうことをすると、悪者（攻撃者）がそのような無防備な所にどんどん入って来てしまいます。攻撃者、悪意の人から見た始点では、「セキュリティ上の弱点」のようなイメージでとらえていただくといいのではないかと思います。

目的とする機能･性能･品質を実現すれば良いというのが、今までのコンピューターシステム、IT システムで重要な点でした。しかし、今や機能･性能･品質だけではなく、攻撃者からいろいろ

な攻撃をされても困らないようにするということが、これから皆さんが、頭を悩ます重要なポイントになってきているということではないかと思います。

本稿でのもう一つ、重要で覚えていただきたいのは、「情報セキュリティ早期警戒パートナーシップ」です。

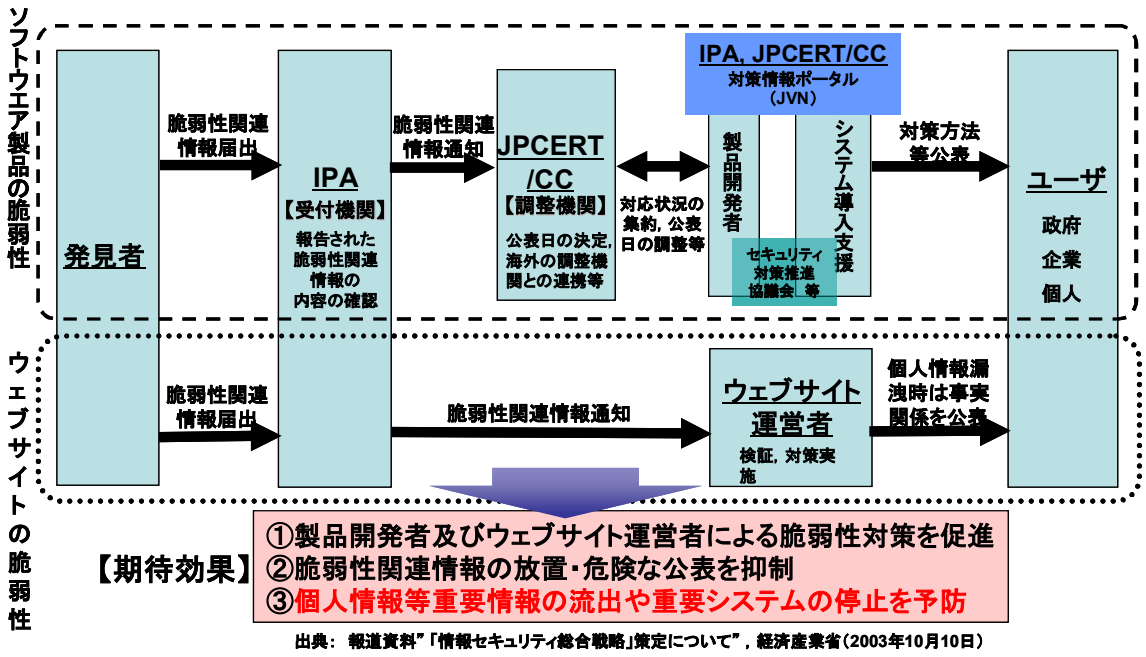


図3.66　情報セキュリティ早期警戒パートナーシップ

図 3.66 に示しますように、発見者、セキュリティの研究者とか、セキュリティの製品を扱っている人が、「この製品あるいはウエブサイトには、セキュリティの弱点があります。攻撃を受けますよ。」という状態を見つけて、それを脆弱性の受付窓口である IPA に報告します。IPA は届出を受け付け、それが脆弱性かどうかを分析します。

① 製品であれば JPCERT/CC に通知します。JPCERT/CC は、製品開発者に連絡し、調整作業をします。解決したとき、その対策情報（対策パッチ等）を IPA と共同で公表します。

② ウエブサイトの場合は、IPA がその発見者からの情報を受け付けると、ウエブサイトの運営をしている窓口に、「お宅のウエブサイトには脆弱性が指摘されています。」という通知をします。ウエブサイトの対策をしてもらうとともに、個人情報の漏えいがある場合には、その事実の公表をするようお願いをしている。依頼がある場合は、IPA は修正したウエブサイトの修正完了確認も無償で実施しています。

図 3.66 中の JVN(JP Vulnerability Notes)は、脆弱性の対策情報などを蓄積する場所（データベース）です。この JVN を定期的に見て、必要な脆弱性対策をすることが、これから重要になってきます。

(2) IT の脆弱性取り扱いの状況

どのくらい脆弱性が発見され届けられているかというと、この制度が開始されてから２年半経っているのですけれど、2006 年末現在で、1,166 件の脆弱性が届けられております。図 3.67 のグラフの下がウエブサイトに関する届け出で、上がソフトウェア製品に対する届出件数です。これの内訳を見ますと、トータルではウエブサイトが合計 704 件で、製品が合計 462 件ということで、ウエブサイトのほうの脆弱性がかなり多く指摘されているということです。ただこれだけしか脆弱性がないということではなくて、氷山の一角だと思っていただくのが良いと思います。必ず皆さんの持たれているウエブサイトには脆弱性があると思ったほうが良いくらいです。

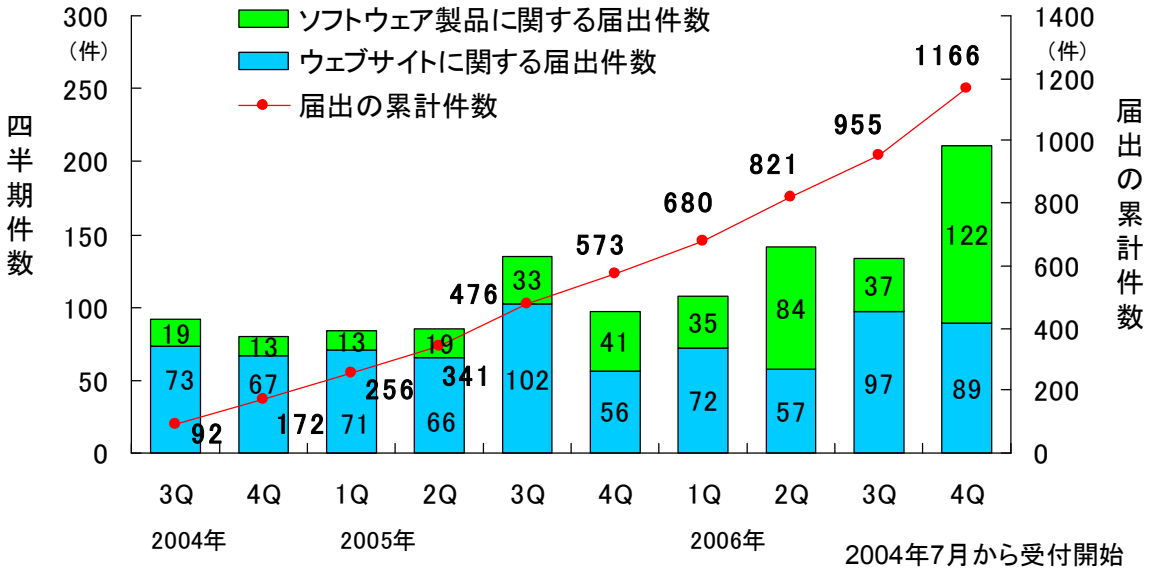


図3.67　脆弱性の届出件数の四半期別推移

それをもう少し分析すると、ウエブサイトの運営者は企業が多いということ。それから、どういう問題が指摘されているかといいますと、クロスサイト・スクリプティングとか、SQL インジェクションが多いです。脅威別ではどうかといいますと、一番多いのが本物サイト上への偽情報の表示です。御社の WEB サイトが書き換えられてしまうということです。重要なことは、「信頼される企業」としては、こういうことにならないように、きちんと対応しているということを企業姿勢としても見せていかないと、顧客やステークホルダーから継続して信頼を受けられなくなってしまうということです。ここにも事業継続として意識しなければいけない点があります。

(3) 具体的な脆弱性事例

具体的な事例をいくつか説明します。

１）クロスサイト・スクリプティング（図 3.68）というものです。

悪意のある人が運営するウエブサイト（②）があります。このウエブサイト（②）に悪意のある人がメール等で、ユーザ（ひょっとしたらこの企業（④）のユーザかもしれない）にアクセスするように仕掛けます。このウエブサイト（②）に入ると脆弱性のあるウエブサイト（④）にリンクするページを返し、アクセスするように誘導させます。同時に不正な処理をするスクリプト

（命令語みたいなもの）もそのリンク情報に埋め込んでおきます。脆弱性のあるウエブサイト（④）がそのスクリプト（命令語）をさらにユーザから見える企業 A のページ（⑤）に埋め込みます。このスクリプトがユーザのパソコン上（⑥）で実施されてしまい、認証情報や個人の情報等が悪意のある人に送られてしまうことがおきます。このユーザから見ると、企業Aのウエブサイト（④）の脆弱性があったおかげで、自分の情報（⑥）が漏えいしてしまったと思うケースとなります。

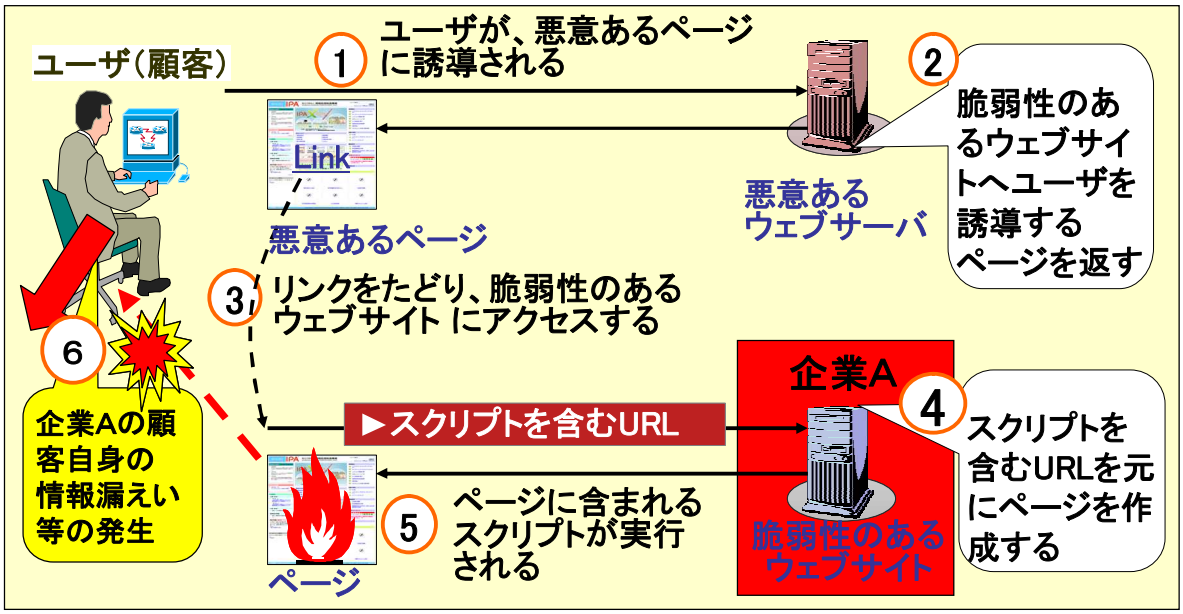


図3.68　事例：クロスサイトスクリプティング

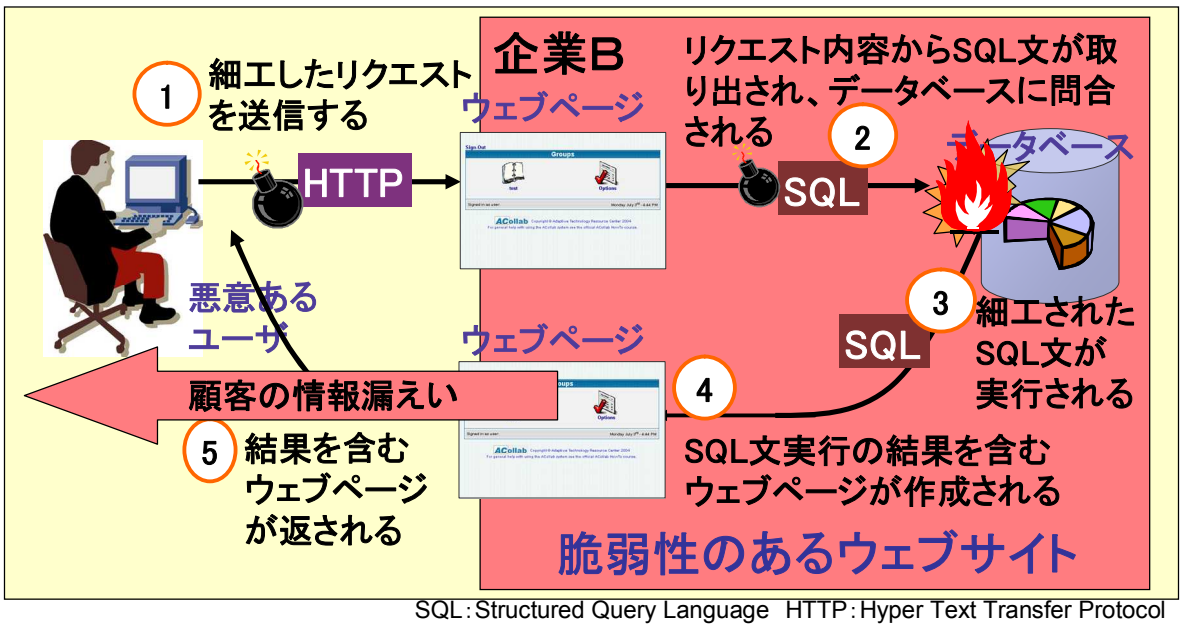
このような脆弱性を持つウエブサイトを運営していることにより、顧客に損害を与えてしまうこと、自社のブランドがダメージを受けるということが起きてしまいます。このようなセキュリティ・インシデントが起きたときには、企業はウエブサービスを停止することが必要です。まずすぐに停止できるのだったら、被害拡大防止のために停止する。基本的には停止しなければいけないと思うのですけれど、企業の方からみると、それが重要なオンラインショッピング等ですと、どれくらいの間にサイトを立ち上げなければいけないとか、いろいろ考えなければいけないということです。

参考ですが、IPA では「安全なウエブサイトの作り方」という冊子を公開しております。この冊子の後半に各脆弱性に対する対策に関するチェックリストを載せています。ウエブサイトの脆弱性対策をする時に、たとえば、皆さんが発注してウエブサイトを作る場合など、この「安全なウエブサイトの作り方」のチェックリストにしたがって、一応脆弱性対策についてチェックするとか、そういうことを発注の条件にして、検収時にそれを確認するということをされるのが良いのではないかと思います。

2）SQL インジェクション（図 3.69）です。

これは悪意のあるユーザ（①）が、脆弱性を持つウエブサイト（③）に対して問い合わせを入力するとき、不正な処理をする SQL 文を入力する（②）と、この企業のウエブサイト（③）が

持っている個人情報とか重要な企業情報が、悪い者（④）に流れて行ってしまうというものです。



SQL：Structured Query Language　HTTP：Hyper Text Transfer Protocol

図3.69　事例：SQLインジェクション

特に個人情報流出になる可能性もありますので、最近はそういうことを起こすと、新聞でも非常に大きく出てしまいます。企業として脆弱性をほったらかしないようにウエブサイトを運営すること、情報漏えいなどを起こさないようにするということが、「信頼できる企業」として認められるためには非常に重要なことだと思っております。

これもIPAの調査ですが、復旧対策とか対外経費とかそういうもので1億円を超えるケースもあります。売り上げ減ですが、たとえば数ヶ月間ウエブサイトを閉鎖して対策をすると、数億円から数十億円の売り上げ減が起きることもあるという調査もあります。

事象（セキュリティ・インシデント）が起きた場合には、被害状況の調査をきちんとする。それから復旧作業をする。それから対外説明等をきちんとするということが大切です。対外説明等のリスク・コミュニケーションについては、よくメディアなどもウォッチしておりますので、ここでブランド失墜にならないように、きちんとした対応をするということが、「信頼される企業」ということで重要ではないかと思います。

やはり起きてから焦ってバタバタする。それで後悔して、社内体制をきちんとしておくべきだったなということではなくて、できればBCP的にはこういう災害が起きることを想定して、セキュリティ・インシデントへの対応を行う社内体制を事前に整備しておくということも必要ではないかと思います。

3）ボット（図3.70）、ロボットのボットと言われているものです。

これは最近いろいろな場所でおきています。これは企業だけが悪いのではないのですけれど、利用者が自分で変なところ（危険なウエブサイト等）にアクセスして、ボットを埋め込まれてしまうケースが多いようです（①）。最近は、有名スターの関係する周辺のウエブサイトに行くと、ボットを埋め込まれることがあります。しかし、企業Xに脆弱性があると、この企業Xにアクセ

スをすると、ボットを埋め込まれてしまうことがあります（②）。

ボットを埋め込まれると、ボットの仲間に組み込まれます（③）。実はこのボットというのは、悪意を持つ人（④）にコントロール（指示）されるわけなのです。たとえば、この悪人（④）が一斉攻撃しろという、サービス拒否攻撃の指示をすると、あるウエブサイト（⑤）に向かって一斉に攻撃をします。このボット化しているパソコンが今、台数的に 40 万と言われています。海外では、シャドウ・クルーと呼ばれるボット運営組織は各国に 4000 人のメンバーを擁して、クレジット詐欺等により数百万ドルを稼ぐということで、もう犯罪に直結しているものです。

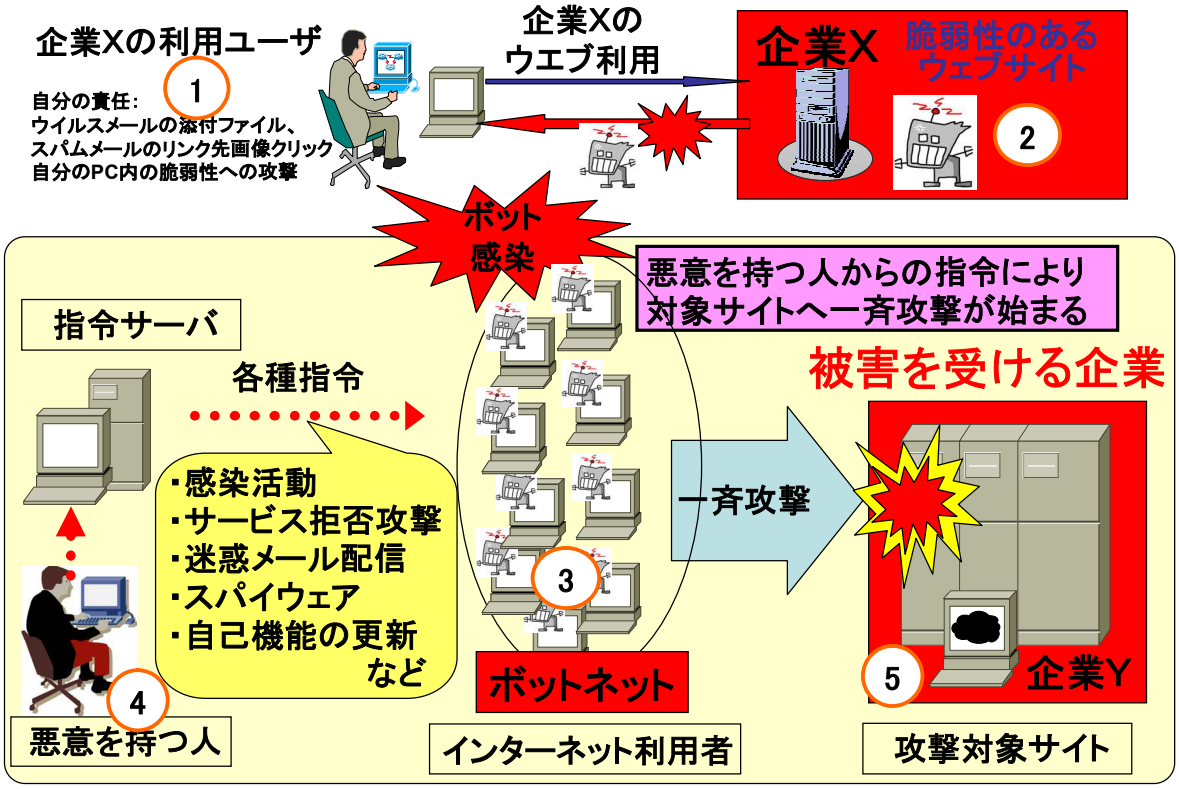


図3.70　事例：BOTの脅威

これらの対策としまして、先ほど 40 万台と言いましたが、40～50 人に 1 台、台数的にも 40～50 万台ということで、皆さんの家庭でもたぶん、ブロードバンドということで、メガというオーダーの帯域を使っているので、この台数に掛ける（X）メガ（Mbps）で行きますと、ものすごい帯域を使うということで、恐ろしいことになります。こういうことを防ぐためにも、サイバークリーンセンター（CCC）というものが立ち上げられております。IPA も CCC のメンバーとして活動しております。

(4)　IT の脆弱性への BCM 適用例

これから少し、具体的に適応事例といいますか、こんなことを考えたらどうですかと言うことを書きます。これはまた後でも出てきますので。

1）まず、脆弱性関連情報についてです。先ほどから脆弱性、脆弱性といっていますが、それ

をどうやって入手するかということですが、公的なセキュリティ機関から入手するということで、先ほども言いましたが JVN というポータルがあります。この JVN には IPA や JPCERT/CC が受け付けをした脆弱性情報および海外、米国の CERT/CC とか、英国の CPNI(旧 NISCC)、こういうところからの脆弱性情報を入れております。

それ以外にもっと多くのセキュリティ専門ベンダーからの脆弱性情報サービス、有料になるかもしれませんが、のようなものがあります。現在 IPA では、過去のものを含めて約 3000 件以上、それから国内外のベンダーの脆弱性情報なども入れるような形で、整備していこうということで、これも４月頃を予定しています。定期的にこのような脆弱性情報を入手し、タイムリーに対策をしていくことが BCP の中でも考えていただくことがよいと思います。特にパッチのような対策については、当然迅速に対策をしなければいけないのですけれど、ユーザから見るとシステムをいじりたくないので、なかなかやりにくいのですが、ある計画や方針でやっていただくのがいいと思っております。

２）先ほどもちょっと言いましたが、脆弱性の存在指摘連絡時の対応についてです。最近は発見者も IPA に届け出、IPA からウエブサイトの運営の方に、こういう脆弱性が発見されましたよということで通知をするようになっています。IPA から見ますと、外部から指摘されたことをその企業のしかるべき部署が受け付けて、それを社内に迅速に展開するような体制が、それぞれの企業、中小企業ですとなかなか難しいのですが、ある程度の規模のところは、まず持っていただくと脆弱性対策への対応が早くなります。このようなセキュリティ・インシデントへの対応体制としては、CSIRT（Computer Security Incident　Response Team）と呼ばれる対応体制がいくつかの企業で設立されて、活動しています。できれば、この CSIRT を構築していただくといいかと思います。

それから自社で発見するケースも当然あると思いますけれども、自社の他のウエブシステムに対策するだけではなくて、他社のウエブサイトに影響するかも知れないというケースの場合には、IPA に届け出をしていただくと非常に助かると思っております。

３）それから演習ということです。だいたい BCP では、最終的には、テスト、テスト、テストで、日常の行動の中に組み込めということです。セキュリティ演習の参考事例は、まだ国内には余りありません。内閣官房情報セキュリティセンター　（NISC）では、総合的演習の実施ということで、10 の重要インフラの事業者と官が集まりまして、２月７日に IT 障害に対する机上演習を実施したという発表があります。たぶんレポートみたいなのが近々出されるのではないかと思いますので、こういうレポートなどを見ながら、IT 系やウエブシステムではどういうことを考えれば良いか参考にすることができると思います。想定外の脆弱性というか弱点を、いかに早く見つけ、対策をしていくかということが、今後ますます重要になると思います。

４）リスクコミュニケーションということで、やはりメディアとの関係をよく考慮して、それからステイクホルダというんですか、いろいろな関係者に、正しい情報を継続的に出すかということです。この事例としては、２００６年の１２月１３日に DDoS 攻撃という攻撃があって、日銀のウエブサイトへのアクセスが困難になるという事件がありました。それを 13、14 日以降、遂次状況を連絡しながら、東京のウエブサイトがなかなかアクセスしにくかったら、大阪のほう

に行ってくださいとか、利用者への適切な誘導をするための情報発信をしている。別の事例としては、同じく２００６年１２月２７日の台湾沖地震の場合です。ここで皆さんに頭に入れておいて欲しいのは、トップページで分かりやすく状況を伝えるということです。利用者から見ると、どこで何が起きているかということを、なるべく１クリック、あるいは２クリックとかで容易に入手できることです、あまりクリック数が多いと、探しに行ってもなかなか見つからないということもありますので、この辺は考慮していただきたい。

(5) BCM ベストプラクティスまとめ

そういうことで、ベストプラクティスのまとめというような形で、セキュリティ・インシデントに対する考慮すべき項目例を、例えば皆さんが自社でウエブサイトに対する BCP を作るときに、この辺のキーワードを使いながら、まずたたき台みたいなものが作れるといいなということを想定しまして、ここにまとめております。全体のまとめイメージは図 3.71 のようになります。

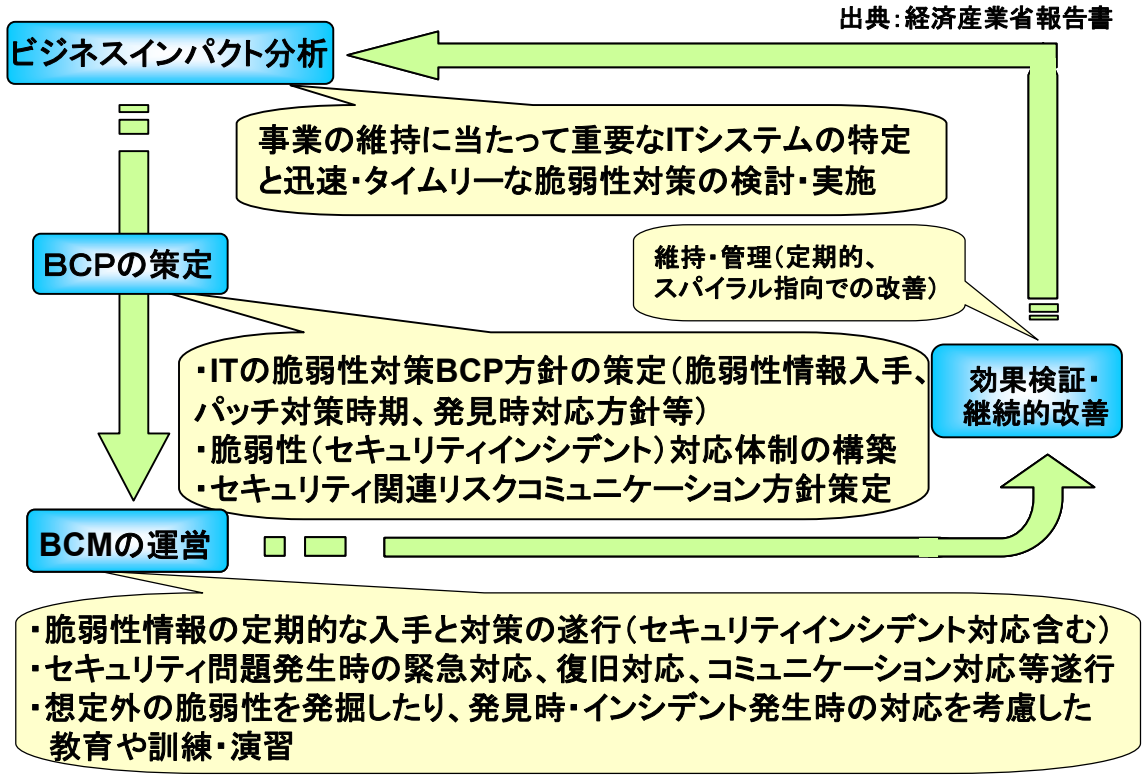


図3.71　BCPのPDCAサイクルと脆弱性への対応

１）適応範囲とビジネスインパクト分析、これは先ほども最初に説明しましたけれど、図 3.72 を参考にしてください。

適用範囲とビジネスインパクト分析：
・ソフトウエアの脆弱性を悪用した不正アクセス、コンピュータウイルス感染やWeb改ざん等より業務の停止・低下、個人情報の漏洩や情報の改ざんなどの発生により顧客・協力会社や社会から信頼を失い、経営に重大な影響を及ぼすことを想定したBCPを策定する。
・本BCPで対象とする情報システムは、たとえば、オンラインショッピングサイト。
個々の情報システムの目標復旧時間（RTO）の設定。たとえば、システム停止をしてから脆弱性対策を実施し、システム再開までの目標復旧時間を決める。4時間とか1日。

図3.72　考慮すべきベストプラクティスまとめ（その1）

2）BCP の策定（図 3.73）、今までいろいろ言ってきましたけれども、できましたら社内体制を整備する。これはどちらかといいますと、経営者に直結するような形でやるようなことが大切です。できればセキュリティの技術が少し分かるような人がいたほうが、たぶん動きが良くなるでしょう。社外との関係もありますので、この辺をいろいろ、常日頃から付き合いをするとか、誰が世の中で信頼できるかとか、そういうことが重要ではないかと思います。

BCP策定：
・社内対応体制、社外機関との連携活動方針を決める。たとえば、社内の連絡体制と各連絡先の文書化。社外機関との連携では、脆弱性情報を定期的にIPAとJPCERT/CCが共同運営するJVNから入手したり、セキュリティサービス事業者から最新インシデント情報等を入手する等の方針を決める。
・個人情報の漏えいの可能性があるときのリスクコミュニケーション方針や、Webサイトを停止するときの公表方法等の方針を決める。
・外部からのセキュリティインシデントに対する指摘をスムーズに対応するため、社内の適切なセキュリティ担当者に情報が正確に伝わるよう、社内のWeb窓口やコールセンターとの連携方法を決めておく。
・Web開発時に脆弱性を作りこまないように確認すべき項目を明確にすること、脆弱性発見時の対策方法を契約時にどう記載するかを明確にする。

図3.73　考慮すべきベストプラクティスまとめ（その2）

それから、個人情報の漏えいの可能性のあるときには、これはもう、いち早く皆さんやられたと思いますけれど、いろいろ外部とのコミュニケーションをどうするのか。どこに連絡するのか。たぶん重要なのは、きちんと電話番号と氏名等が書かれているということです。どこどこの新聞社に連絡するとか、そんなふうに言われても、緊急時にじゃあどうすればいいんだといっても、ドタバタするだけなので、具体的な電話番号、氏名というものを書くということが重要です。

ウエブサイトの指摘を受けたときには、これも社内の適切なセキュリティ担当者に情報が正確に伝わるようにするということを、常に頭に入れて、ウエブの社外窓口の方とか、コールセンターの方と連携をすることが大切になります。どうもあちこちたらい回しになってしまって、対応が遅れるということで、ブランドを傷つけるようなケースもあります。できれば、セキュリティについての窓口はここですとかしていただくと迅速に情報が伝わるかなと思います。

開発時は先ほども言いましたけれど、「安全なウエブサイトの作り方」とかを利用することです。

1） それからBCPの運用（図3.74）ということです。

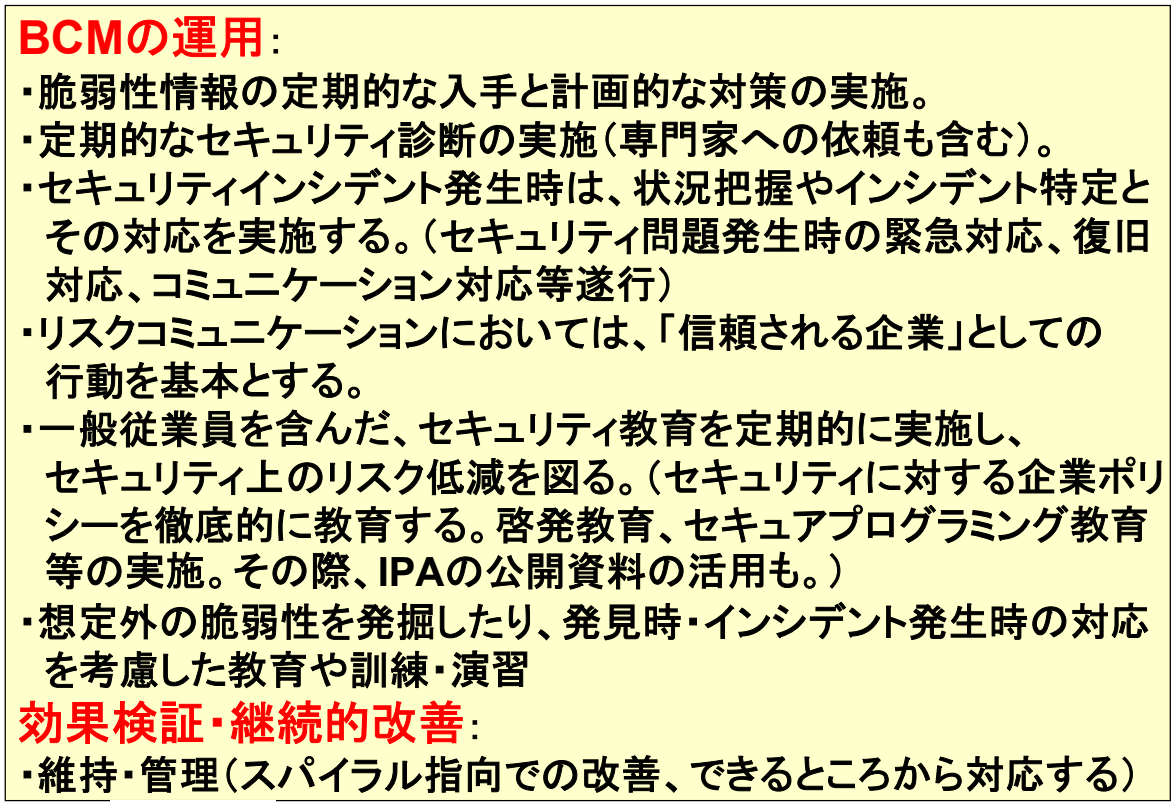


図3.74　考慮すべきベストプラクティスまとめ（その3）

まず、定期的に脆弱性情報を入手することです。

お金がかかりますが、セキュリティ診断の実施ということも忘れてはいけないことです。例えばどこかから１件、脆弱性があると指摘されたときに、他のウエブサイトも全部チェックしないと、大体同じようなものが他のウエブサイトにもあります。それ以外のものもあるということで、この診断のための費用を予算に入れることも忘れないようにすべきです。ウエブサイトの構築をどこかに外注したときには、必ずこういうスキャンチェックみたいなことを、検収でするとかをしたらいいのではないかと思います。

「信頼される企業」ということを常に頭に入れていただきたい。だから教育、教育ということです。そして、やはりスパイラル思考での改善ということで、できるところからどんどんやっていくのが良いのではないかと思います。

今言ったようなことを、うまくガイドラインのような形式で作成して、それでまずスタートするということをやっていただくといいかと思います。

IPA の活動についてですが、「情報セキュリティ白書 2006－加速する経済事件化－」というもの、これは 2006 年版から出版したのですけれども、を出して社会的影響の大きな 10 大脅威をまとめています。現在 2007 年版を作っているところです。もうひとつは、「情報セキュリティ教本」というもので、この中では、パソコンをどこかに置き忘れてしまったケースでの BCP の説明が書かれています。この教本も参考になるのではないかと思います。

3.7.3 重要インフラ・産業界横断的な IT 障害に対する取り組み

具体的な相互依存の事例

CIP/CIIP のモデル化

米国・日本での取り組み状況概要

3.7.4 まとめのようなもの

以降、３番目ですが、海外とかもう少し重要インフラ系とか、この辺の話を簡単にご説明したいと思います。

これは、一番最初に申しましたが、INTAP というところで、３年間いろいろ調査したときに、重要インフラ産業界が、相互に依存しているのではないかと、それをどうまとめるかということで、これは 2003 年８月北米の大停電があった時。ここの赤のところが原因ですけれども、木が倒れたとか、それから SCADA という、これは監視制御システムと言うんでしょうか、Supervisory Control And Data Acquisition system というのですが、制御系の監視システムと思っていただければいいと思うのですけれど。それのシステム障害とか、ヒューマンエラーとか、ちょっとこういう複合的なものが重なりまして、本当に広域、カナダとか北米で事故が起きた。この電力事業者の災害が起きた。それがいろいろな業種のところに影響を与えているということを、実はどう表現すればいいかというのを、ちょっとまとめたものです。これはもう少し具体的なのですが、今ので例えばニューヨークの地下鉄が停止して、一時数千人が閉じ込められた。ゼネラルモーターズの 20 工場が操業停止に陥ってしまうとか、大リーグのメッツ、ジャイアンツ戦が中止になるとか、いろいろ被害が起きたということです。

２番目の事例が、2004 年の５月末です。大手町の電源設備の故障がキャリアで起きまして、当然キャリアのサービスが止まってしまって、それを受けて別の通信事業者、あるいは IT サービスの事業者、官公庁のサービスとか、こういうものが影響を受けた。こういう相互依存性のところが、どう依存しているのか、どこに相互依存のポイントがあるのかとか、その辺をきちんと抽出するということが、非常に重要ではないか。これは航空管制システムですが、これは 2003 年と 2004 年の２度ほど起きているのですが、乗客が非常に困るとともに、たぶん物流関係も非常に影響を受けるという事例です。

こういうことから、皆様一企業の BCP から、複数企業間、後で言いますけど、SCM 的なものです。複数企業できちんと全体の流れ、サービスを実現するためにどうすればいいか。それからさらに業界内から業界間横断の社会基盤の BCP。よくここを、Critical Infrastructure Protection とか Critical Information Infrastructure Protection とか、こういう言い方で、特に政府とか重要インフラ系のところの、サービスの継続を目的にしたいろいろな検討とか研究がされております。これもここの、自分の部門から全社的に行って、他との関連、そして社会の一員としてどうするかというのを、ちょっとマンガっぽく書いたものです。

米国はやはり、金融系が非常に進んでいます。ニューヨーク、これも INTAP で調べた。こういうところですね。こういう情報交換をするような場もあって、金融系が主体で、ちゃんとキャリアさんだったらキャリアさんの、ケーブルが実際にどこの土管の中を通っているかとか、そう

いうところまでいろいろ確認しているということです。

これは、CIP　CIIP について、どういうふうに、先ほどから言っている依存関係のポイントを洗い出すとか、それをどういうふうに被害なり災害が伝わっていくのかというようなことを、いろいろ研究されているところがあります。一つの例ですが、三階層モデルということで、下が？ブツリレーヤーですね。真ん中がサイバー、上がオーガナイゼーションレーヤー、組織的なということで、この辺がイントラネットと同じように、イントラのディペンデンシーがどうなっているか。ほかの業界との間で、インターディペンデンシーがどうなっているかということ。こんなことをベースに、いろいろな議論がされている。

もう少し今のを整理してみますと、物流輸送というのはいろいろ海底ケーブルとか、鉄道とか橋とか、ここでいろんな災害が起きる。その影響は、その上で動いている銀行間決算のシステムとか、航空管制とか、先ほども SCADA という制御系の監視システム、こういうところに影響を及ぼすケースもある。あるいはこのいろんなバグとか、ウィルス系のやつで何かおかしくなるとか、それがまた上に影響する、という形で経営を実際にやるところにどう影響するか。あるいは、ここから外部の別のところにサービスを提供しているのですが、この辺のサービスのところにどう影響を及ぼすか。というかたちで、いろいろこういうモデルです。ここの事業者さんに何か障害が起きて、別のサービスに影響を及ぼしたときに、そのまた次の人がどう影響を受けて、ほかにサービス停止とかそういうことを引き起こすか。こんなことを、ちょっとこれはポンチ絵にしただけなのですけど、重要なのはこういうことの中で、やはり情報共有ということと、定期的にいろいろ、先ほども言いましたが机上演習、あるいは実際に障害を起こして、それで演習するというケースもあると思うのですが。それにしても、いろいろな所で情報を共有するというような活動が重要かなということです。

これは先ほど言いました、SCM のものですけれど、長岡の地震の時も、あるところが地震で災害を受けたのです。以降のところの SCM が止まってしまった。というかたちで、この辺もみんなで連携するような形で、一連の連帯をいかに持続していくかということが大切で、そのためには情報共有のコミュニティが必要だろうということです。

そういうことを日本ではどうしているかというので、内閣官房が進めている、第２次提言です。第１次提言は、国のいろいろなシステムです。第２次提言で重要インフラということで、今当初七つだったのですけれど、ここで三つ追加されて、水道、医療、物流ですか。全部で十の重要インフラ分野です。これにつきまして、ここで事業継続性に関係するキーワードを赤で書いたのですけれど、こういう形でいろいろ検討が進められております。

これが第２次提言の主な結論という形で、先ほどこの演習というところをご説明しました。これが２月７日にありました。ここが、相互依存性解析検討会というのが実は開かれておりまして、ここで 10 の重要インフラ事業者が集まりまして、相互にどういう依存関係があるかというのを、情報共有するということで、いろいろ意見交換をして、この辺のことも、年度ですから、今まとめられている状況だと思います。

もう一つ、情報共有がこれから非常に重要だということで、この部分ですが、これにつきましては、米国では ISAC Information Sharing and Analysis Center と言うことで、情報共有をする

仕掛けが動いている。うまく行っていないという人もいるのですけれど、一応それぞれの重要インフラ業種ごとに、こういう ISAC というのがあって、その ISAC の上に、ISAC 全体の連絡会議をするようなもの。日本の場合には、ここをセプターという名前で、セプターの略語は忘れましたけど、こういうセプターという形で、先ほど言いました 10 の重要インフラ事業者間に、情報を共有する場を作ってもらうということで、たぶん今年度中には、もう全部の業種でこういうものができて、その上にこういうセプターのカウンセルみたいなものができて、情報共有ができるようになる。これは先ほど言った、内閣情報セキュリティセンターというところがコアになって、いろんな情報、何かインシデントが起きたら報告する、あるいは外部からインシデントの情報があれば、それが流れてくる。ここのところにあるのが、たぶん IPA とか JP サート分、こういうところで、いろいろ、ひょっとしたら海外から「こういうシステムに重要な問題がありそうだ」という場合には、それが特に重要インフラ事業者に関係する場合には、迅速にここに連絡して対策をするとか、いうようなことを考えております。

それから、CIIP 関連で、海外でどういう動きがあるかというのは、最近の例だけなんですが、先ほど欧州の CIIRCO (critical information infrastructure research coordination project)、それから IFIP という、情報処理国際連合、ここの中に実は去年ぐらいにチリで、critical infrastructure protection session というようなものが、こういう学会の中でも持たれ始めてきて、実は今年の 3 月 19 か 21 日です。一つのワーキンググループになって、そこで初めて critical infrastructure protection の学会が集まるということで、海外、欧州にしましても、特に米国は DHS です。国土安全保障省とか、あの辺が巨額のファンディングをして、大学にこういう研究を、CIP、CIIP についての研究にお金を出すとか、学会の立ち上げをしているということなので、たぶん日本もこういうことがこれから必要になるのではないかと思います。

まとめのようなものですが、まず一緒にやっていきましょう。一人ではできないということです。というのは、先ほどの 4000 人のカードの ID を盗むようなことを、向こう側のビジネスで、そういうことをやっているのに、一人で対応しようとしてもできませんので、彼らは 24 時間、365 日。それから時差を利用して、夜中でも攻撃してくる。一人ではできないと言う認識で、先ほどから言っている情報共有とか、いろいろそういう信頼できる仲間作りをするということで、やっていく必要があるのではないか。

もう皆様分かっていると思うのですが、WEB というのはこれからますます重要になってくると思いますので、WEB にしても、インターネットにしても、元々は研究者で、信頼できる仲間でやっていたのですけれど、だんだん信頼できる人だけじゃなくて、先ほどの攻撃者だとか、そういう、いつでも攻撃してきますということで、作り込まない。作り込ませない。外注して WEB の開発をしてもらうときにも、ちゃんと IPA の安全な WEB サイトの作り方とか、そういうものを見てチェックをして来るのだよと、そして開発し終わったら、いろんな脆弱性のスキャナーとかそういうものを確認するとか、そういうことを徹底させるとか、そういうことをやっていただかないといけません。

これは米国のある研究者が言っているのですが、2010 年には 10 万件／年、これは日にすると、300 件ぐらいです。現在我々の処理能力の平均値は、2004 年の 7 月にサービスを開始しましてか

ら、実際に働く日で平均しますと、１日当たり２件の脆弱性を受け付けているということになっています。多いときには、１週間で 20 件を越すようなケースもあって、非常に分析をする人間も忙しく働いているという状況です。こういうことで、IPA のほうから「御社の WEB サイトに脆弱性がありました」とメールが行かないように、お互いに頑張っていきたいなと思っています。以上です。どうもありがとうございました。

3.8 米国における BCM の実際

米国においては、2001 年 9 月 11 日の米国同時多発テロ以降、BCM 策定が加速している。2006 年に KPMG が実施した調査によると、BCP 策定済みの米国企業は 62%に上るのに対して、日本企業は 15%という状況である。本章では、導入が進んでいる米国企業が実際の導入、策定で気づき、得られたポイントを述べたいと思う。日本企業の今後の導入の参考にできるところを見つけ出していただければ幸いだ。

3.8.1 BCM コンセプト

まず初めに BCM と BCP を大まかに理解していただきたいと思う。全体像を理解することで、BCM と BCP のイメージがより鮮明になるだろう。

BCM、BCP を端的に理解するには、定義を確認するのが有効だ。定義については、「PAS 56」や昨年末に発行された「BS25999-1」に記載されているので、この内容を見たことがある方も多いことだろう。しかし、「定義」は概要を理解する目的で見られることが多く、その全体像を把握する目的では見られることは少ない。ここでは、「PAS 56」の定義を「BCM、BCP の全体像」を把握する目的で見てみたいと思う。

BCM（Business Continuity Management）
組織を脅かす潜在的なインパクトを認識し、①「利害関係者の利益、名声、ブランド及び価値創造活動を守る」ため、②「復旧力及び対応力を構築」するための有効な対応を行う③「フレームワーク、包括的なマネジメント プロセス」

BCP（Business Continuity Plan）
潜在的損失によるインパクトの認識を行い実行可能な継続戦略の策定と実施、事故発生時の事業継続を確実にする継続計画事故発生時に備えて開発、編成、維持されている④「手順及び情報を文書化」した事業継続の成果物

*数字と「」は筆者が加筆

この短いセンテンスには、BCM を構築するやり方や目的が記載され、BCM と BCP の関係も述べられている。

① 目的（及び構築後に得られるメリット）
「利害関係者の利益、名声、ブランド及び価値創造活動を守る」
② 方針
「復旧力及び対応力を構築」
③ アプローチ方法

「フレームワーク、包括的なマネジメント プロセス」

④ やるべきこと

「手順及び情報を文書化」

そして、この「PAS 56」の定義に具体的なビジネス上の目標として次の点を加えるとより一層BCM/BCP が明確になるだろう。

①’ 目標

ビジネス活動の中断に際し、

「従業員の安全を確保する」

「事業継続し、売上減少をさせない」

③にあるように、BCM はプロジェクト活動のようなものではなく、プロセスになるため、ある程度構築できたら終了というものではない。継続的にレビューを行い、その時点で現実にそぐわない点があったら修正を加えていき、不測の事態が発生した際に活用できるように絶えず更新し続けなければならない。したがって、この「プロセス」であるという点は、BCP 策定を開始した後も十分に意識し、実践しなければならない。このことはよく語られることではあるが、米国においてもなかなか実践されていない現状がある。しかし、一度策定した BCP の有効性を維持し、その効果を期待するのであれば、必ず行わなければならない作業となることを肝に銘じておく必要がある。

3.8.2 BCM プロセス構築のポイント

実際に BCM を構築する上で、意識して行うとよいと思われる点を紹介したい。ここでは、BCM 構築フェーズ（図 3.75）を簡単に説明するとともに、各フェーズで実際に BCM、BCP を使えるもととするポイントを説明していく。

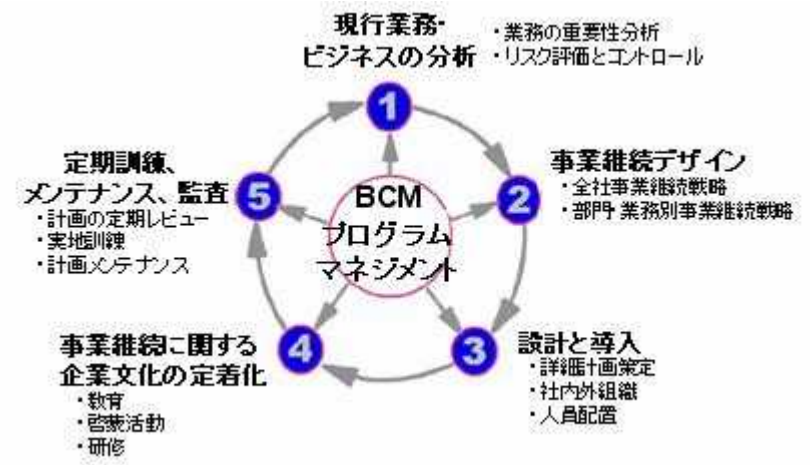


図 3.75. BCM 構築フェーズ PAS 56」より

(1) BCM フェーズ 0.　基本方針

構築ポイント「人命の安全確保を最優先にする」

何のために BCP を策定するのかを意識することが重要になる。策定を進めていく上で、コストやリソースの兼ね合いを考慮しなければならないことも当然発生する。その際、策定するメンバーが判断基準となる目的に基づいたプライオリティ付けができるよう、BCP 策定の目的を明確化しなければならない。そして、その中で最も重きを置き、目的のトップに挙げなければならないのが、「人命の安全確保」である。人道的な理由は論ずるまでもないが、「人」は、重要なリソースの一つになるからだ。不測の事態が発生した際、「人」がいない場合には、BCP を完璧にまとめていたとしても機能はおぼつかない。ドライにリソースの一つと考えても、確保する手段を最優先で考えておかなければならない。

米国同時多発テロ事件（9.11）の陣頭指揮を執ったジュリアーニ前ニューヨーク市長は、「緊急対応において、企業は人命救助と BCP の準備をしておく必要がある。まず、従業員を避難させるプランを作らなければならない。また同時にオフィスを別の場所に移してすみやかに事業を再開・継続することが企業の命運を握る。」と、講演の中で述べている。このように、人命の安全確保と BCP を分けて考えるのもいいだろう。

避難計画は安全確保の手段として最も効果が有効のものになる。有事の際に従業員を迅速に避難させることの重要性については、9.11 の際、ワールドトレードセンターに入居していた大手金融機関であるメリルリンチとモルガンスタンレーの例が参考となる。両社は、9.11 発生前から実際に入居階から地上に降りる訓練を数度に渡って行っていた。だからこそ事件が起きた際にあわてずに、従業員を避難させ、数日後にすぐにビジネスを再開することができた。この結果、他社に先行し、その後の両社のビジネスの飛躍に貢献したのは、よく語られるところである。

また、米国では、9.11 を教訓とし、非常用階段の全幅が条例により拡大されたり、勤務する身体障害者を安全に避難させる事前の訓練なども意識的に行われるようになっている。

BCP 策定と考えるとこの観点や項目は語られないことも多い。人命確保のための施策も BCP 策定の際には考慮すべきであろう。

(2) BCM フェーズ 1.　現行業務・ビジネスの分析

構築ポイント「リスクマネジメントのリスク評価方法」

構築ポイント「リスクシナリオタイプ検討」

最初に行うことは、自社の現行業務を理解し、最優先すべき事業の要件を定義することだ。その後、現行業務プロセス、フローを把握しながら、想定されるリスクならびに被害を検討するわけだが、ここでリスクマネジメントのリスク評価方法を採用するとよいだろう（図 3.76)。つまり、リスクを「市場リスク」、「信用リスク」、「事業リスク」、「オペレーションリスク」の 4 つに分類して対策を検討するのだ。企業には非常に多くのリスクが存在するため、BCP 策定をするためにリスク評価を開始すると、BCP の範疇外となってしまうリスクも存在する。その際に、見出しされたリスクをそのままにするのではなく、各リスクにふさわしい方法で対処することを同時

に検討すると、より広範囲のリスクに適切に対処することが可能になる。ちなみに、BCP が有効になるのは、オペレーショナルリスクに該当するリスクで、災害、事故、過失、犯罪などに関連するリスクが対象になる。

ここで見出されたリスクは、リスクシナリオに基づき、マトリックス化を行い、対応方法をある程度パターン化することを行う。例えば地震のリスクシナリオを考える場合、ファシリティがどうなるか、情報システムは使用し続けられるか、スタッフはオフィスに来られるかなどを考える。震度 6 の地震が発生した場合、電気が供給されなくなり、情報システムは使用できなくなり、電車が運休しているためスタッフは出社できない可能性があるといった感じだ。この点は、「テロ被害の場合と類似点が多い」といった考え方により、対応方法をパターン化しておく。もちろん細かい部分では違う部分も存在するだろうが、被害や対応方法に類似する点が多いという点がポイントになる。この点に注目することで、危機に際し柔軟性や応用力が発揮される。

ニューヨーク市では、9.11 の前にニューヨーク市では大まかな想定シナリオが 20～30 存在していた。その中には飛行機がビルに激突するというシナリオはなかったが、発生した状況から判断すると、ビル火災とテロに対する対応を行えばいいと見当がついた。そこで、ニューヨーク市の危機管理室長のリチャード・シェアーがまず行ったことは、マンハッタンにかかる橋を直ちに閉鎖したことだった。なぜ彼が即座にそのような行動がとれたのか。それは、彼が事前にシナリオ毎の対応方法を熟知しており、被害状況から類似しているシナリオをイメージし、その対応パターンをとることができたからである。

そして、このフェーズの最後では、この検討結果を元にビジネス影響度分析（BIA：Business Impact Analysis）を導き出し、目標復旧時間（RTO：Recovery Target Objective）を決定する。

図 3.76　リスク評価方法

(3) BCM フェーズ 2.　事業継続デザイン

構築ポイント「リスクマネジメント・アプローチ」

このプロセスでは、BIA と RTO を元に、代替リソースを考慮しながら、リスクマネジメント思考による事業継続の方向性を検討する。災害発生を想定しながら、現行オペレーションを継続するための要求事項とリソースをリストアップし､代替リソースによる実行が可能かを検討する。これらのリソースには､インフラ､ファシリティ（工場やオフィスなど)､情報システム（データ、アプリケーションなど)、従業員、取引業者、原材料/外部サービスが含まれ、業務を構成する全リソースについて検討する必要がある。その際、必要リソースについては、災害発生時から時間経過とともに、検討していくとよいだろう。

なお、代替リソースの選択は、想定コストと BIA を比較しながら、ROI（Return on Investment：費用対効果）を意識して行う。代替リソースの採用が時間的、コスト的に現実的でなかった場合は、リスクマネジメントのアプローチにより、他の手段も検討するのが有効だ。

図 3.77 はリスクが存在した場合、それをどう処理するかをマトリックスにしたものだ。リスクの頻度・緊急性と被害規模により対処方法が分かれてくる。まず､『リスク移転』だが、損失の負担の可能性を他者と共有する方法だ。代表的な例が保険で、めったにおこらないが、起こると被害が大きいというリスクに対して有効な手段となる。次に､『リスク回避』だが、ここにプロットされるリスクは、発生頻度も高く、被害規模も大きいものになる。例えばある業務では、頻繁にミスが発生し、注意喚起をするが一向に減る気配がない。よくよく調べてみると、人的に無理な工程があることが判明したなどのケースだ。この場合には、ミスが発生した際の対処を考えるよりも、その工程自体を変更してしまった方がよいことが多い。そうすることで、ミス自体を発生しない仕組みに変更できるからだ。『リスク保有』は、リスクがあるとしてもそれを認識して受容してしまう方法になる。リスクの発生頻度が低く、被害金額も少ないため、発生した際のコストと対策コストの観点から何も行わない選択をするといった具合だ。最後に､『リスク防御』だが、リスクが発生する確率を減らしたり、リスクが顕在化しても被害を最小減にすることを行う。具体的には、BCP 策定や危機管理対策を行い、予めそのリスクに備え、準備をしておくことが特徴になる。

以上のように､リスクマネジメントのアプローチを BCM/BCP においても取り入れることにより、幅広い最適なリスク対策の選択肢をえられることになる。BCM/BCP 策定をする段においては、兎角ビジネスが中断した場合の準備を如何にするかに意識がいってしまうが、リスク移転、回避、保有なども考慮にいれるとよいだろう。

図 3.77　リスクマネジメント・アプローチ

(4) BCM フェーズ 3.　設計と導入

「フェーズ 2.事業継続デザイン」において決定された方法、コスト、スケジュールに基づき、実際のドキュメントとしての BCP を策定する。この際には、経済産業省のガイドラインに記載された次の内容を検討するとよいだろう。

<『2.2.5 事業継続計画の策定』より抜粋>

重要な要素をいかに防御するか、また重要な要素が万一被災した場合にどのように対応をするかの二つの観点から実施することが必要である。企業が災害時に実際に事業を継続していくためには、以下の項目が特に重要である。

1　.指揮命令系統の明確化
2.　本社等重要拠点の機能の確保
3.　対外的な情報発信および情報共有
4.　情報システムのバックアップ
5.　製品・サービスの供給

これらを考慮し、不測の事態発生時に実施すべきアクション、必要とするリソースなど、行動する際に参照するための文書を作成する。したがって、内容は、何を行えばいいか、誰にコンタクトすればいいかなど明確に記載するように心がける。また、同時に緊急時に確認し、実施できるようチェックリストも作成しておくとよいだろう。

(5) BCM フェーズ 4.　事業継続に関する企業文化の定着化

策定した BCP を機能させるためには、実際に緊急対策を行う従業員が正しく BCP を理解し、対応できることが必要になる。また、策定したシナリオ以外の不測の事態においても従業員が適切に行動できるよう訓練をしておく必要がある。そのためには、危機状況を想定し、実際に想定

した行動が行えるかどうか、また策定した BCP に問題点はないかなどを事前に確認しておくことが必要だ。同様に BCP の教育、訓練を通して BCP の重要性、知識と理解を深めることも重要になる。

(6) BCM フェーズ 5.　定期訓練、メンテナンス、監査

構築ポイント「定期的な訓練」

事業継続マネジメント（BCM）では、一連のライフサイクルの最後にこの「定期訓練、メンテナンス、監査」を位置づけている。それは、BCM は日々変化するビジネス環境に適応した危機管理対策でなければ意味を成さないからである。BCP の内容は、ビジネスを支える多くのリソース（従業員、取引先、ファシリティ、原材料）に依存しているため、最新の情報を元にした計画でないと機能しない。また、BCP は、あくまでも想定されるリスクに対し、机上で検討した計画であるため、実際に機能するかは未知数になる。そのため、定期的に危機的状況を疑似体験することで、現行の BCP が実際に機能するのか、リファレンスドキュメントとして分かりやすく書かれているかなど、確認し続ける必要がある。特に、ドキュメントとしての使い易さは、実際に使用してみないと分からないことが多い。日本人の特質上、膨大な報告書を作成しがちであるが、ポイントは「緊急時に参照するに足る情報が列記されているかどうか」、また「すぐに必要とする情報を探し出せるか」であることを、この訓練において確認するとよい。実際に使ってみて、必要項目が探しにくいようであるなら、思い切って内容を減らすとか体裁を変更するなどを検討したほうがいい。

ニューヨーク市の例ばかりで恐縮だが、同市では 9.11 以前以降も何度も訓練を実施している。訓練を行わないと、非常事態が発生した際に行動できないことを痛感しているからだ。是非、BCP は策定したらおしまいというのではなく、何度も訓練を実施していただきたいと思う。実際に階段から降りるなどの訓練もそうだが、机上訓練を行うことでも新たな発見があるだろう。

3.8.3 BCM 導入事例

BCM 導入で先行している米国では、参考となる導入事例も多い。ここでは、一般に公開されている導入事例を紹介したいと思う。この中からポイントとなりうる情報を見出していただければと思う。詳細については、英語になるが、下記 URL を参照いただければと思う。

(1) Workers Compensation Fund(労働者補償基金)

Source：http://www.avaya-apac.com/downloads/casestudies_US/ef-svc2175-02.pdf

同基金は、ユタ州最大の労働者補償基金として、3 万名以上の労働者に休職時や失業時の賃金の補償、再就職の斡旋などを行っている。日本におけるハローワーク（公共職業安定所）のような団体ではあるが、日本とは制度やシステムが異なり、独立して運営を行っているのが特徴だ。在職中に支払われる雇用保険の徴収、その資金運用は複数の独自アプリケーションで行われ、3 万人の労働者の過去から現在に及ぶ就業データも同基金のメインフレーム上で管理されていた。

このように IT 依存が高くなる状況において、扱うデータは労働者の生活に密接に関わる給付

など金銭にからむものである。そのため、万が一のダウンタイムがますます許されない状況になってきた。そこで、システムの可用性を再確認する意味においても BCP の導入を真剣に行うことになった。

BCP 策定を開始したところ、複数の改善すべき点がすぐに見つかった。まず、システムの状況を調査したところ、ビジネスプロセスとデータが全く紐づいていないことが判明した。同基金では、当然のことながらホストコンピュータのリストア対策などは万全であったが、ただデータを丸ごとバックアップしているだけで、どのデータがどのアプリケーションで使用されるかなどの紐付けは一切行われていなかった。BCP 策定においては、緊急事態が発生し、コンピュータがダウンしてしまった場合、複数あるアプリケーションの中からどのアプリケーションを最初に復旧させるべきかなど優先順位付けを行う。その際、アプリケーションは起動できても、肝心なデータはすぐに見つけられない状況になっていた訳である。

また、災害シナリオを想定していくとオペレーションやスタッフをソルトレイクシティ（ユタ州の首都）から移す必要があった。しかし、一切その具体的な計画は検討されていなかった。この段になり、災害プランや復旧対策はやっていたつもりであったが、BCM や BCP の観点に立ってみると、その計画がビジネスオペレーションと紐付いていない点が多々見受けられるようになってきた。

IT 以外の点についても発見はあった。部署のオペレーションを調査していたところ、部署の担当者の経験やスキルに依存しているプロセスがかなりあることだ。平時においては、その担当者が数日休んだところで、そのオペレーションを後日やる段取りにしていれば問題はない。しかし、緊急時には、担当者が出勤できず、そのオペレーションのためにその他のオペレーションも止まってしまう可能性もある。個人のスキルに依存しているオペレーションは、システマティックにワークフローとしてドキュメントに残し、他のスタッフでも行えるようにしておかなければならない。同基金では同様のケースが複数の部署で見受けられたため、外部コンサルタントの協力を得て、ビジネステクノロジーとプロセスのレビューをした後、プロセスの機能解析とリスト化を実施した。

最後に、IT を中心とした BCP 策定を行っていたが、より整合性の高い BCM を構築しようと思った場合には、物理インフラを考慮しなければいけないことにも気づいた。IT セキュリティをより確実な状態にしようと思った場合、物理セキュリティも確実に行わなければならなくなってきているのは、米国において常識になりつつある。米国の公開企業の半数以上に CSO（Chief Security Officer）がおり、IT、物理セキュリティ両方が責任範囲になっているのもその現れである。

このように発見された問題点を改善しながら BCM を構築した同社は、結果得られた効果を次のように挙げている。

① 緊急事態毎の対策確立
② 分析やアセスメントを通じて、ビジネスオペレーションの把握
③ 対応手段が人から部署に変更

④　その結果、ビジネスリソース、時間、予算の最適化などコストセービングが可能に

BCM 構築は外部コンサルタントに依頼しても、内部リソースを使用して行った場合でも当然のことながらコストがかかる。しかし、その見返りとして、災害発生時の早急なるビジネス復旧を確立し、損害を最小限にとどめることも可能になる。また、金額換算は難しいが、リピュテーション（評判）を維持することも可能だ。そして、BCM 構築プロセスを通じて、ビジネスオペレーションを見直すことで、非効率な部分を効率化させることも可能になる。この金額的メリットは会社規模にもよるが、数億円を超える場合も報告されている。

(2) Sprint Nextel Corporation（スプリント・ネクステル）

Source：http://www.strohlsystems.com/Events/_files/BCAwareness/NextelCaseStudy.pdf

同社は、個人、法人合わせて 5300 万人の契約者を抱える米国の携帯電話大手企業として、BCP を策定する必要に迫られていた。通信企業として、多数の契約顧客数を有するため、ビジネス中断の影響力が計り知れないからだ。また、携帯電話は緊急時のファーストレスポンスとして最も利用されるコミュニケーション手段であるため、ライフライン維持という社会的な意味合いにおいても、ビジネス中断は許されない状況にあった。そのため、同社では、現行の BCP を見直し、より信頼性の高い BCP に変更に着手した。

現行の BCP の問題点は、部署毎に策定されており、全く全体統合がされていないことだった。そのため、部署間の BCP 精度のレベルの差を均等化させ、整合性をとる必要があった。また同時に、全社リソースを統合し、シングルポイントで管理をしながら、即座に問題解決ができる体制に変更する必要があった。

そこで同社では、人事担当上級副社長を BCP 担当役員兼務とし、策定チームを立ち上げると共に、社員の BCP に対する意識を向上させるために、ロゴとインターナルサイトを立ち上げた。そして、BCP の目的は、「(家族を含めた) 社員の安全を確保する」ことで、続いて「ビジネスの復旧」「ビジネスの継続」を目指すという、同社の BCP のプログラム・ミッションを決定した。

実は、このプロセスには重要な意味が含まれている。役員が BCP 担当に任命されることで、経営者のコミットメントを表すことができる。また、BCP を成功させるというリーダーシップも期待できる。そして、社員の安全確保を第一優先事項とすることで、社員の共感とインボルブメントも期待することができる。このようなプロセスを最初に行うことで、BCP 策定をスムーズに行うことが可能になるのだ。

つづいて、アメリカ国土安全保障省（DHS）、アメリカ連邦緊急事態管理局（FEMA）のモデルを参考に緊急対策計画を策定した。これら公共セーフティと同様のアプローチをとることで、潜在的な災害への対応をスムーズになると考えたからだ。そして、このプロセスにおいて、通常オペレーションから大災害時までのレスポンス方法、エスカレーション方法を 5 段階の対応方法として策定した。さらには、緊急対応にあたるメンバーが集結する危機管理室（EOC: Emergency Operation Center）を構築した。メンバーが一同に会し、集められた情報を元に判断を下すことは非常に重要なことだ。緊急時においては、情報は集約され、全体的思考において適切に指示さ

れないといけないからだ。

同社はBCP策定後に3年間で、ウイルス被害、停電、ハリケーン被害など17件の緊急事態を経験し、

① EOCでセンター統合していた場合、スムーズにリソースのアロケーションが可能になる

② 具体的なビジネス継続方法は実務がわかる現場が行うべきだが、EOCのようなHUBが必要である

③ 即座に対応することを考えるBCPソフトなどソフトウェア使用した方が効果的である

をポイントとして挙げている。

3.8.4 まとめ

日本においては、冒頭に記載したように、BCP策定はまだ導入期にある。しかし、米国企業を顧客として、あるいはコンペチターとしてワールドワイドで活動している日本企業も少なくない。これらの企業は、米国企業並みのBCPを求められることあるだろ。グローバリゼーションが益々進む今日、BCPは策定しておいた方が得策である。そのためには、まず社内にチームを発足させ、取り組みの第一歩を踏み出すことが重要であろう。

3.9 ＢＣＰと情報システムの設備

現代の情報システム重要性は周知の通りであり、情報システムの安定稼働は当該会社の企業運命を左右することもお解りの事と思います。このシステムの安定稼働に必要不可欠な物は、情報システム関連付帯設備とその安定稼働の為の運用と管理である。この点を考慮し、安定稼働に必要な情報システム用設備は何であるかを考えてみたい。

その説明は下記の順で説明させて頂きたい。

１：火災対策（延焼）
２：水損対策（水害）
３：地震・振動対策（建物、室）
４：電磁界対策（遮蔽）
５：雷害対策（同電位、共用設置）
６：入退館管理（不法侵入等）
７：ネットワーク対策

3.9.1 火災対策

建物間は建物の立地条件や設置環境を考慮し、火災による情報システムへの被害を防止することを目的に選択しなければならない。

その、選択の具体的な対策は

（1）炎症の被害を受ける恐れのある場所を避ける。　延焼の恐れのある場所とは建築基準法第二条に規定してある場所である。
また、建物の近傍にガソリンスタンド等可燃物、危険物を大量に貯蔵している場所も避けなければならない。

（2）建物は、構造・機能面で建築基準法に適合する耐火建築物でなければならない。
また、建物の開口部には防火戸を設置・消防法に規定されている警報設備や消火設備・外気取入れ口に防火ダンパを設置しなければならない。

そのために留意することは；

（1）建物の同一区画内には、危険物の貯蔵設備を設けない。
（2）消防法に規定されている自動火災報知器を設置し、監視システムと連動させる。
（3）建築基準法における延焼のおそれのある部分について延焼のおそれのある部分は、隣地境界線、道路中心線又は同一敷地内の二以上の建築物相互の外壁間の中心線から、一階にあっては３メートル以下、二階以上にあっては５メートル以下の距離にある建築物の部分をいうと定義されている。
ただし、防火上有効な公園、広場、川等の空地若しくは水面又は耐火構造の壁その他これに類するものに面する部分を除く。

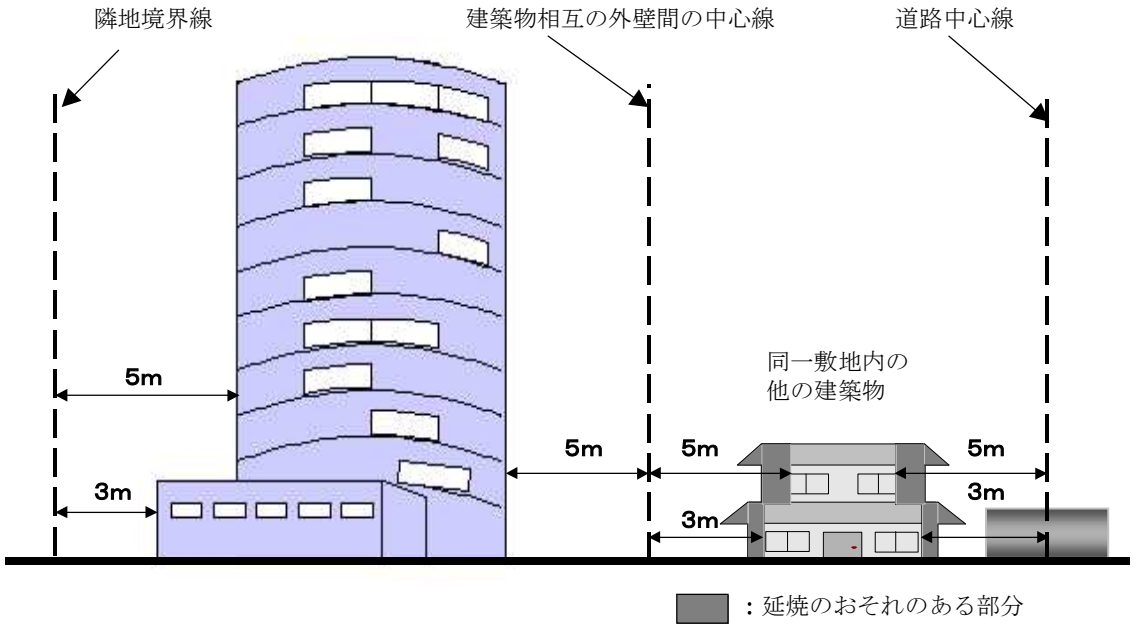


図 3.78　離隔距離のイメージ図

3.9.2 水損対策

水による被害は付帯設備をはじめ、情報処理機器に多大な影響を与えます。　水損を受けると復旧にかなりの時間を要しＢＣＰの観点から視た影響は計りきれません。

その被害を最小限に抑えるためには；

立地条件や機器等の設置環境を考慮し情報システム等への対策を講じなければならない。

その対策は；

建物の選定に当たっては、過去のデータから出水被害の有無を調査し、被害を受ける危険性がある場所を避けなければならない。

また、電源室や空気調和室等の関連は地下室内に設置することを避ける事を考慮すべきである。その他、建物の開口部分への対策を忘れてはならない。

その対策は；

開口部には防水扉・防水堤を設けると共に雨水に対する対策を施す必要がある。

建物には十分な防水性能を確保し屋根・外壁や窓等は防水施工を行う必要がある。

また、屋根・外壁を貫通する吸排気口・ダクト・配管等の周りには防水施工を施す必要がある。また、忘れてはならない項目の一つには排水口・配管等の詰りによる逆流防止対策を講じ、排水性能を確保しておかなければならない。これらの対策を取るに当たり、考慮する点が幾つか有る。

低地や海抜ゼロメートル地帯等の排水の悪い場合では十分な対策の検討が必要であり、出水による被害が懸念される場合は、室を防水区画とする必要がある。情報システム等を設置する室・データ等保管室・サーバ等が設置される事務室については、室外から水が入らないための対策を講じることが望ましい事も忘れてはならない。漏水検知器を設置し、監視システ

ムと連動させることが望ましい。防水加工を施した部分は経年変化による機能低下に注意・屋上排水口はゴミ詰りによる排水機能の低下に注意・屋上や屋根の平らな部分だけではなく立ち上がり部分の防水処理に注意・コンクリート目地部分の破損や防水層の劣化、破損、コンクリートの亀裂に注意・屋根（屋上）に工作物を設置する場合は、防水施工部分を破損しないように注意する必要がある。

図 3.79 は防水施工例である。

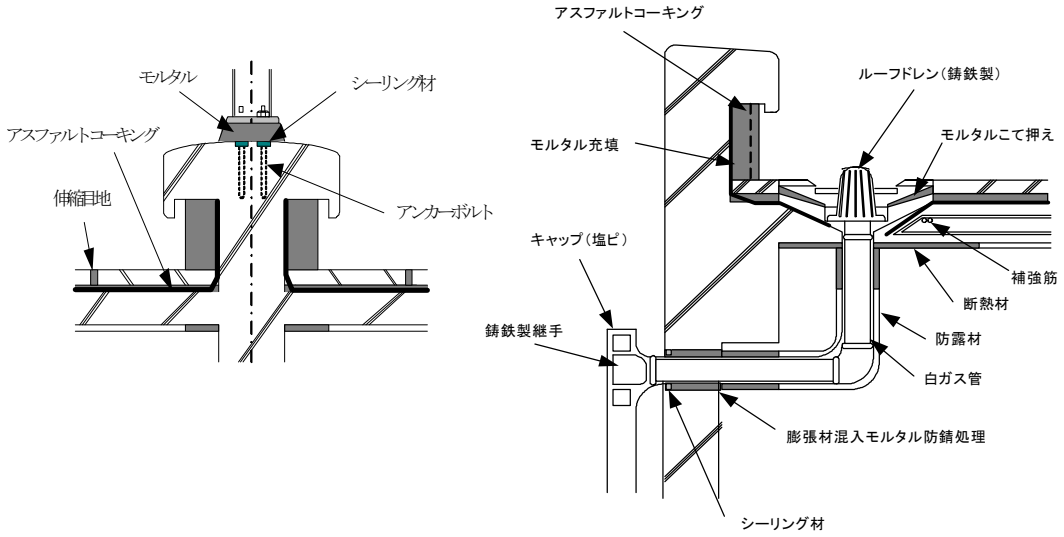


図 3.79　防水施工例

3.9.3 地震・振動対策（建物、室）

建物周辺の地盤の強弱・活断層の有無の立地条件と建物構造（剛構造か柔構造等）を把握し条件に即した対策を講じ地震による情報システムへの被害を最小限にする事が必要になる。

その対策の例は；

地震による被害の怖れがある地域は避ける事・建物の構造や機能での対策（耐震・免震・制震構造）・室の構造及び機能面において地震対策（耐震・免震）を講じる事である。

この対策を講じる時の考慮点は、避難施設、救出器具の確保等人身被害の防止策についても併せて検討・地震感知器を設置し、監視システムと連動させる・装置及び機器において地震対策を講じる・地震感知器で感知しにくい長周期の地震動による被害防止にも留意する・重量物の設置箇所、フリーアクセスフロアのカット部分の補強のため、補助支柱を考慮する事を考慮する必要がある。

振動

立地条件及び設置環境を考慮し、振動（衝撃を含む）による情報システムへの被害を防止しなければならない。

その対策例は；

振動による被害のおそれのある以下の地域での立地を避ける必要がある。

鉄道の近傍に建物が設置されている場合・高速道路及び交通量の多い道路の近傍に建物が設

置されている場合・機械プレス、油圧機等が稼動している特定施設（留意事項参照）が建物に隣接して設置されている場所を避ける事。　ただしこのような場所を選択した場合は、建物の構造・機能面での対策を講じる必要がある。

また、振動の発生源に応じて下記の対策を組み合わせて適用する必要がある。

◆建物の構造上から耐震設計を図る。

◆室の床を振動の影響を受けにくい免震床構造とする。

◆装置及び機器において振動対策を講じる。

振動規制法において振動の発生源と見なされる特殊施設とは、以下のものが規定されており、規制の対象となっている。

◆金属加工施設

a.液圧プレス(矯正プレスを除く)

b.機械プレス

c.せん断機(原動機の定格出力 1kw 以上のせん断機)

d.鍛造機

e.ワイヤーフォーミングマシン(原動機

◆定格出力が 37.5kw 以上のもの)

◆圧縮機(原動機の定格出力が 37.5kw 以上のもの)

◆土石用、鉱物用の破砕機、摩砕機、ふるい、分級機(定格出力 7.5kw 以上のもの)

◆織機(原動機を用いるもの)

◆コンクリートブロックマシン(原動機の定格出力の合計が 2.95kw 以上のもの)並びコンクリート管製造機械、コンクリート柱製造機械(原動機の定格出力の合計　10kw 以上のもの)

◆木材加工機械

a.ドラムバーカー

b.チッパー(原動機の定格出力 2.2kw 以のもの)

◆印刷機械(原動機の定格出力 2.2kw 以上のもの)

◆ゴム練用または合成樹脂練用のロール機(カレンダーロール機以外のもので、原機の定格出力 30kw 以上のもの)

◆合成樹脂用射出成形機

◆鋳型用造型機(ジョルト式のもの)

特定建設作業とは、振動規制法において以下の通り規定されている。

建設工事として行われる作業のうち、著しい振動を発生する作業であって政令で定めるものを「特定建設作業」として規制の対象とする。

振動規制法による特定建設作業は以下のものである。

１：くい打機(もんけん及び圧入式くい打機を除く)、くい抜機(油圧式くい抜機

を除く)又はくい打くい抜機(圧入式くい打くい抜機を除く)を使用する作業
２：鋼球を使用して建築物その他の工作物を破壊する作業
３：舗装版破砕機を使用する作業(作業地点が連続的に移動する作業にあっては、１日における当該作業に係る２地点間の最大距離が５０ｍを超えない作業に限る)
４:ブレーカー(手持ち式のものを除く)を使用する作業（作業地点が連続的移動する作業にあっては、１日における当該作業に係る２地点間の最大距離が５０ｍを超えない作業に限ると規定されている。

機器等の地震対策
各コンピュータメーカの指導の下に対策を考慮する必要がある。
１：機器による対策
２：設備による対策（免振ビル、免振床、メーカ推奨方式等）
３：冷水設備（空調用配管、冷水使用機器関連等）

3.9.4 電磁界対策(遮蔽)

立地条件及び設置環境を考慮し、電界及び磁界による情報システムへの被害を防止する。
その対策例は；
電界及び磁界からの被害のおそれのある以下の施設が近隣にある地域での立地を避ける。
・電波塔
・マイクロ波アンテナ
・レーダ施設
・送電線
・強電実験棟等に隣接する地域を避ける事。

建物の構造・機能面での対策は；
◆建物全体で電磁遮蔽を行う。
◆各室で電磁遮蔽を行う。
◆信号ケーブルは、シールド付とする。
◆電力ケーブルは、金属管配線として信号
ケーブルとの電気的隔離をはかる。
◆ＣＶＣＦ、絶縁トランス及びMG等の
外部電源装置を設けて電磁誘導ノイズの除去をはかる。

3.9.5 雷害対策 (同電位、共用接地)

建物の設置環境及び立地条件を考慮し、落雷による情報システムへの被害を防止する事が必要である。
その対策例は；

年間の雷雨日数等を調査し、落雷による被害のおそれのある地域を避け、必要な付帯設備工事により雷対策を講じる。

◆避雷設備を設置する。

◆地中ケーブルとする。

◆通信ケーブルは、可能な限り光ケーブル

又は無線化する。

対策を講じる時の留意事項は；

建築基準法では「高さが２０ｍを超える建築物の場合、避雷設備の設置が義務付けられているが、２０m以下の建物であっても雷の多発地帯の場合は、避雷設備を設置することが望ましい」と記載してある事に留意する必要がある。

図 3.80 は供用接地を使用した対策の例（IEC で採用されている共用接地）

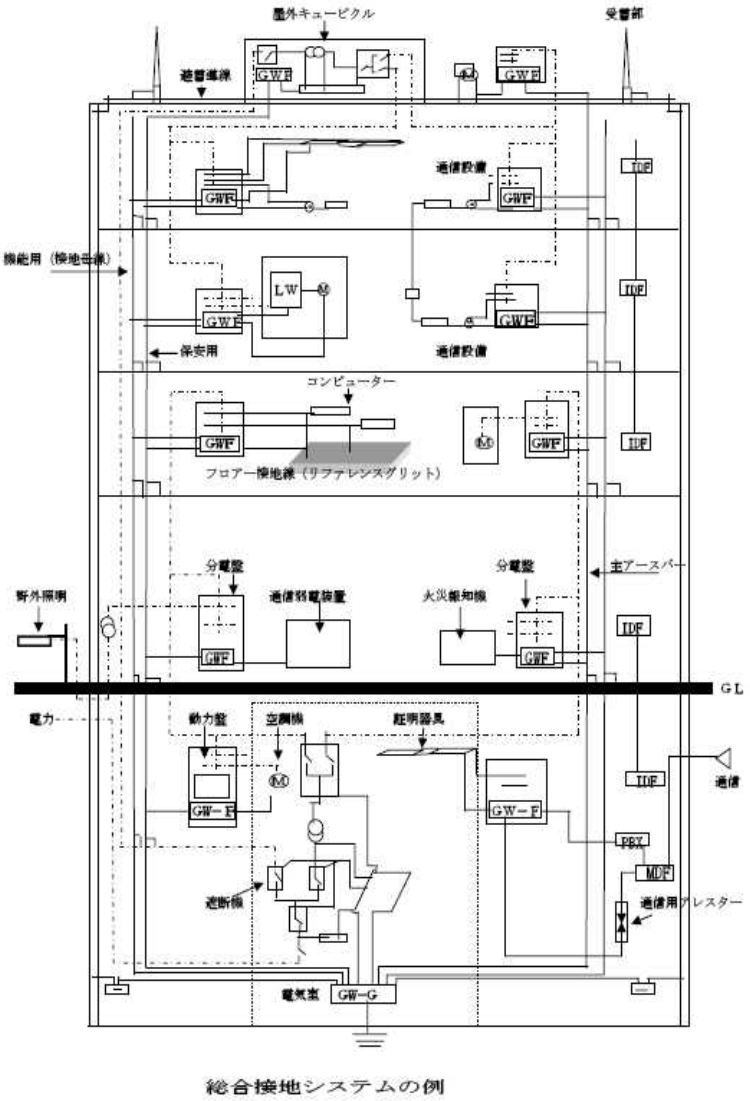


図 3.80　供用接地を使用した対策の例（IEC で採用されている共用接地）

図 3.81 は通信用の供用接地の対策例

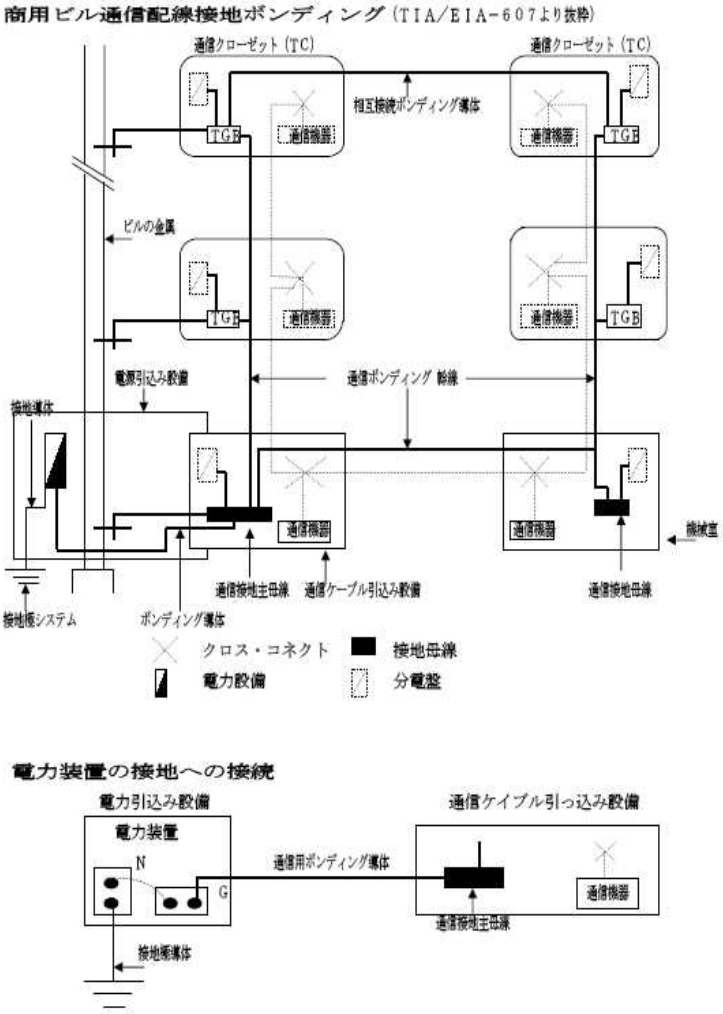


図 3.81　通信用の供用接地の対策例

最新の雷関連の情報は図 3.82 のＩＣＬＰ２００６に記載されている。

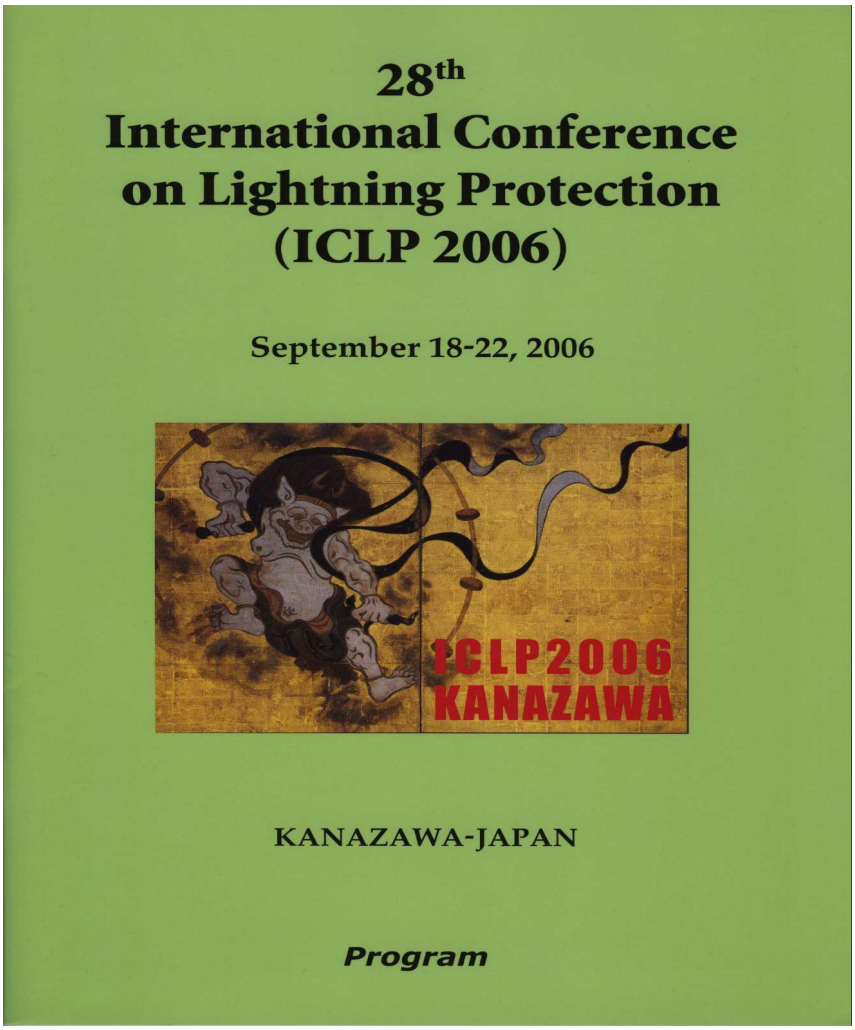


図 3.82　第 28 回 ICLP2006

3.9.6　入退館管理の対策

立地条件、敷地の条件及び建物の構造等を考慮し、建物への入退館管理を強化することにより情報システムへの被害を防止する事を目的にしなければならない。

その対策例は；

１：入退者を認証し記録する機能

機械による場合は、次の機能を有する

設備とする

①入退館資格者（ＩＤ）を登録する機能。

②入退館資格者（ＩＤ）を識別する機能。

③入退館資格者（ＩＤ）、日時／場所

（入・出）を記録する機能。

２：受付けによる場合は、次の機能を有する設備とする。

①入館者の本人及び用件確認できる機能。

②入館者の氏名、日時／場所（入・出）を記録する機能。

③緊急時（不審者等）は警備室等へ連絡できる機能。

３：遠隔操作による場合は、前記２）に加え音声及び映像により識別し扉を解錠する機能を有する設備とする。

許可された者だけを通過させる機能

扉

①認証により解錠する。

②自動的に閉扉する。

③自動的に施錠する。

④緊急時（停電、火災等）は解錠し、扉を手動で開閉する。

⑤制御機器、電気錠は、停電対策を講じる。

上記対策を実施する場合の留意事項は；

◆敷地の出入り口においても電気錠やオートゲートなどで規制することが望ましい。

◆敷地・建物の出入り口において、監視カメラ等を設置して対策を講じることが望ましい。

◆禁止されている物品等の持ち込み、持ち出しを防止する対策を講じることが望ましい

◆機械による入退館管理を行う場合は、不正アクセス、機器の故障・破壊行為、扉のこじ開け等に対する警報を発報し、警備担当部門に通報することが望ましい。

◆入退管理設備の配線は、ノイズ・切断等の対策をすることが望ましい。

◆自動扉の場合は、非常電源を設置することが望ましい。

◆共連れ、すれ違い防止設備を設ける。

◆アンチパスバック機能を設ける。

◆ラッパーゲート、リングゲート等を設ける。

◆機器類は、定期的に保守点検を実施する。

1）定期保守（予防保守）

2）障害保守（障害修復）

事に留意し対策を講じる事が必要である。

図 3.83 は入退管理に用いた例である

図 3.83　入退管理

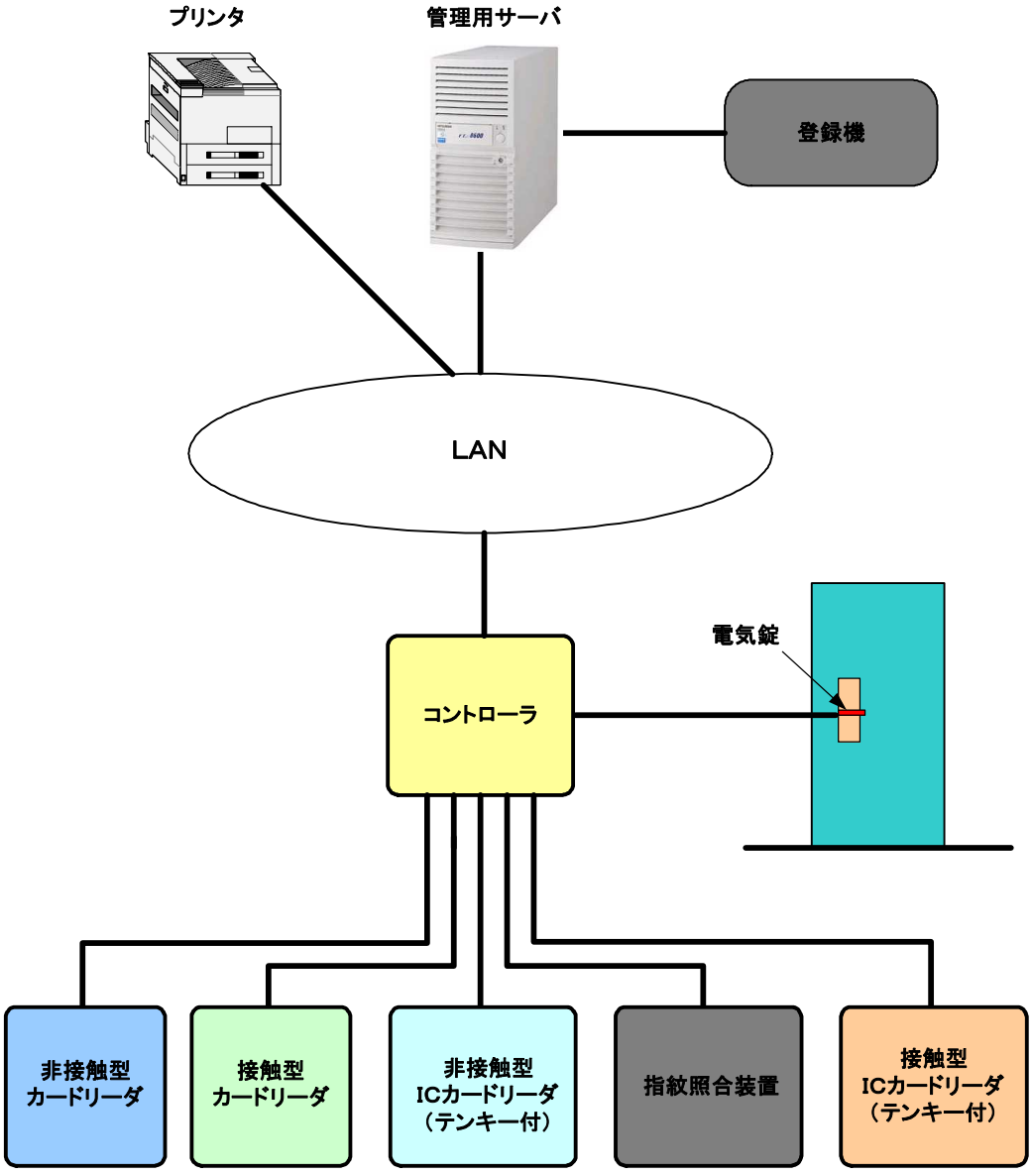


図 3.84　機器管理の例

ネットワークに対する対策は；

ネットワーク機器及びケーブル配線は、外部からの影響を受けない措置を講じネットワーク機器への障害を防止し機器の安定稼動を確保する事を目標に対策を講じる必要が有る。

その対策例

浸水対策

◆架空配線とする。

◆防水加工を施した埋設管路、ピット、トラフ、共同溝に配線する。

◆防水加工をしたコルゲートケーブル等を直接埋設する。

火災対策

◆金属管を用いて配線する。

◆難燃性ケーブルを用いて配線する。

◆ケーブルには延焼防止剤の塗布／不燃材を用いて養生する。

電磁界の対策

◆光ケーブルを用いて配線する。

◆金属管等でケーブルをシールドする。

◆シールドケーブルを用いて配線する。

雷対策

◆光ケーブルを用いて配線する。

◆アレスタを設置する。（通信系・電源系）

◆メッセンジャワイヤー、テンションメンバー（鋼線）、金属管の接地を行う。
（機器の接地とは接続しない）

地震の対策

◆ネットワーク機器を収容するラック及びケーブルラックの地震対策を行う。

◆搭載している機器の移動／落下
（飛び出し）防止対策を行う。

◆配線は余長を持たせ整理し固定する。

コンピュータ室・データ保管室の対策は；

１：地震と振動対策

２：腐食性ガス対策

３：防犯、防災対策

４：コンピュータ室で使用する部材

５：携帯電話、電波漏洩対策

６：水関連対策

７：小動物による被害防止対策　が必要である。

地震と振動対策（室と設置階）

地震による移動及び転倒を防止する措置を講じ、情報システムを構成する機器等の移動・転倒を防止し、人身の安全を確保する事を目的にした対策を取らねばならない。

その対策例は；

建物全体での対策

・免震ビル

・制震ビル

コンピュータ室での対策

・免震床

・部分免震床（免震台・制震台等含む）

機器固定による対

・床スラブに固定

・耐震床（パネルの浮き上がり防止を含む）に固定。

・機器は固定した机や棚に載せたうえ耐震固定具や耐震固定バンド等で落下防止対策を行う。

メーカ推奨方式による対策

具体的な対策方法は各メーカに確認する事。

また、天井・照明器具・間仕切壁等及びフリーアクセス床は地震により損壊しない構造とする。

地震による天井・照明器具・間仕切壁・窓・フリーアクセス床の損壊により人身及び情報システム等への被害を防止いなければならない。

その対策例は；

1) 天井、間仕切壁及びフリーアクセス床は、地震により損壊しない耐震措置を講じる。

天井は上階スラブに吊りボルト等で固定する。（天井、照明器具の固定方法）

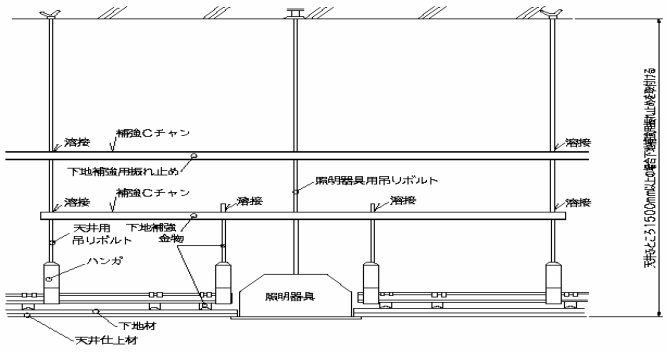


図 3.85　耐震措置例

2)防火区画を構成する間仕切壁は

①上部は、上階スラブに固定する。

②下部は、床スラブに固定する。

③壁・柱に固定した補強材に固定する。

3)間仕切壁（簡易間仕切壁を含む）は

①上部は、天井等に固定する。

②下部は、補強したフリーアクセス床等に固定する。

4)窓及び簡易間仕切り等で使用しているガラスは、破損・飛散を防止する措置を講じる。

① 網入りガラスを使用する。

② 合せガラスを使用する。

③ ガラスに破損、飛散防止フィルムを貼る。

5)フリーアクセス床の耐震は、下記の①、②いずれかの対策を適用する。

①フリーアクセス床の固定は

a. 支柱は下記の対策を選択して適用する。

ｱ. 耐震用の支柱を使用し、床スラブに固定する

ｲ. 支柱間を連結し床スラブに固定する

b. ボーダ部のパネル、支柱を補強する。

c. 切り欠き等開口部を補強枠又はストッパで補強する。

d. 避難通路の耐震補強を行う。

ｱ. パネルを固定する。

②免震構造のフリーアクセス床を設置する

(2)照明器具等は、落下防止措置を講じる。

1)照明器具等は、天井の下地鉄骨にボルトで固定するか、又は上階スラブに吊りボルトで固定する。

この対策を取る為の留意事項は；

(1)耐震強度を算出する際には設置階の応答加速度(フロアレスポンス)によって行う。

(2)フリーアクセスフロアの耐震設計は、設置する機器等の最大重量を想定して行う。

(3)照明器具の防眩ルーバ、カバー等の落下防止措置に留意する。

図 3.86 は建物の応答加速度を示した例

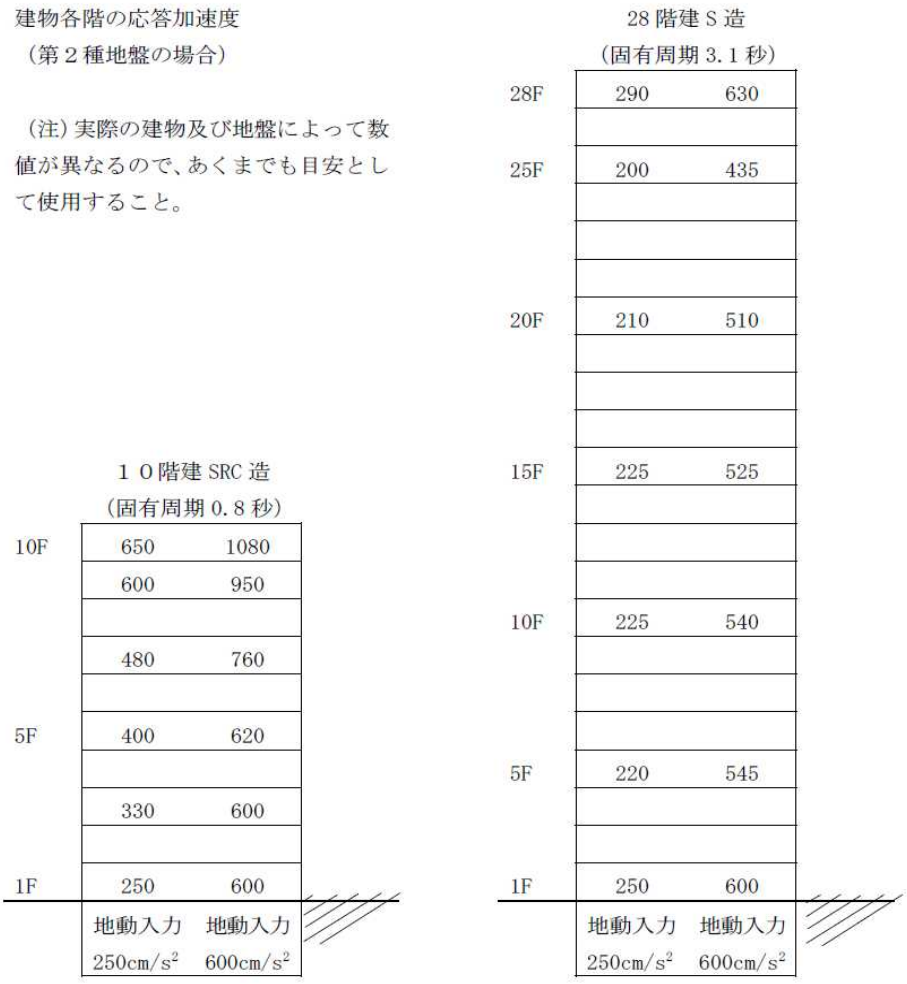


図 3.86　建物の応答加速度を示した例

機器等の地震対策

各コンピュータメーカの指導の下に対策を考慮して下さい。

１：機器による対策

２：設備による対策（免振ビル、免振床、メーカ推奨方式等）

３：冷水設備（空調用配管、冷水使用機器関連等）

腐食性ガス対策

立地条件及び設置環境を考慮し、大気汚染による情報システムへの被害を防止することを目的に対策を講じる必要がある。

これを実施する対策例；

大気汚染からの被害を受けやすい以下の地域を避ける。

・化学物質・粉塵等の被害を受ける恐れのある地域
・排気ガス等の被害を受ける恐れのある地域
・塩害の恐れのある地域
・火山や温泉地域
・室を腐食性ガスの侵入がない位置に設ける。
・腐食性ガス等の侵入を防止する設備を設ける。

建物の構造・機能面から対策を講じる。
・腐食性ガスの除去装置を設置する。
・集塵装置を設置する。

これを実施するための留意事項
情報システムに影響を与える因子としては、以下のものがあげられる。
・腐食性ガス（亜硫酸ガス、一酸化炭素、
塩素、オゾン等）
・化学物質（酢酸、クロオフォルム等）
・塵埃
・海塩粒子　これらに留意し対策を考慮する必要がある。
例として上記を表にしたものが表 3.4 である。

表 3.4　情報システムに影響を与える因子

発　生　源	腐食性ガス
・石油精製、ガス工業、アンモニア工業、製紙工業、製鉄工業の排出ガス ・火山、温泉地帯の大気 ・下水処理場の大気	硫化水素（H_2S）
・石油、石炭を燃料・原料とする燃焼、ガス化設備工場の排出ガス ・製鉄工業、非鉄精錬工業、硫酸工業、硫黄精錬工業、製紙工業等の工場の排出ガス ・ゴミ焼却場排出ガス	二酸化硫黄（SO_2）
・固体燃料ボイラの排出ガス ・硫酸工業の排出ガス ・自動車等内燃機関の排出ガス	窒素酸化物 （NO、NO_2）
・化学工業、製紙工業の排出ガス ・上水処理場の大気	塩素（Cl_2）
・化学肥料工業の排出ガス ・フェノール樹脂	アンモニア（NH_3）
・光化学スモッグ ・電気式集塵装置	オゾン（O_3）

防犯、防災対策
　立地条件や敷地の条件及び建物の構造等を考慮し、外部から危険物の投げ込みや不法侵入等の犯罪による情報システムへの被害を防止することを目的に対策を講じなければならない。
その対策例は；

敷地における対策。

周辺状況や施設配置に応じて守るべき領域の境界に十分な高さや形状を確保した囲障（フェンス、門扉等）を設ける。

建物における対策。

◆外部に面する壁、扉及び扉枠は、容易に破壊されない構造とする。

◆隣接する建物等から屋上、窓等への侵入を防ぐ対策を実施する。

◆非常口は、防犯錠を使用し、不法侵入を監視する設備を設ける。

◆窓等の開口部は、防犯ガラスを使用する。

◆出入口以外で、１階等で外部から侵入のおそれのある窓がある場合は、防火戸又は防犯センサー等を設置する。

◆敷地境界、建物等は、監視カメラ、外灯（防犯ライト）等の威嚇警報設備を設置する。

建物、室の機能、用途が外部から察知されないための対策。

◆建物の機能、用途が分かるような看板、案内図等は外部に掲示しない。

◆室の入口に室名を表示しない。

◆館内、エレベータ等の案内板に室の位置を表示しない。

◆警備室や防災センターの内部が外部から直接見えない措置を講じる。

対策を実施するための留意事項は；

出入口等で外部から直接車両等の突入の恐れのある場合は、車止め等の防護対策をとることが望ましい。

駐車場、駐輪場等からの不法侵入に対しても配置や構造等に留意する。

監視設備については十分に検討する。

パンフレット、ホームページ等に室の位置がわかる図面を掲載しない。

樹木を利用した建物内への侵入、植栽により生じる死角に留意する。（樹木、植栽の成長にも留意する）上記内容は防犯の観点から忘れてはいけないことです。

不法侵入、危険物の投げ込みの恐れのある窓等の開口部は被害防止の措置を講じ、外部及び共用部に面した開口部からの侵入、危険物の投げ込み等による被害を防止することを目的に対策を実

施する必要がある。

その対策例は；

外部に面する窓等の開口部を設ける場合は、下記の対策を選択して適用する必要がある。

◆無窓とする。

◆開口部に防火シャッター、防火戸、鉄扉を設ける。

◆耐火ボードで覆う。

◆ブラインド等を設け、外部から見えない措置を講じ、不法侵入、危険物の投げ込みの恐れのある窓等には格子、強化ガラス及び不法侵入を検知する設備を設ける。

共用部に面する窓等の開口部を設ける場合は、

下記の対策を選択して適用する。

◆無窓とする。

◆開口部に防火シャッター、防火戸、鉄扉を設ける。

◆耐火ボードで覆う。　等の対策を実施する必要がある。

コンピュータ室で使用する部材

内装等は不燃材料又は準不燃材料とし、火災の拡大から情報システム及びデータ等を保護する事を目的に対策を取らねばならない。

その対策例は；

◆内装等(フリーアクセス床を除く)の仕上げ材料は、不燃材料又は準不燃材料とする。

◆フリーアクセス床の主要部材(床パネル、支柱等)は、不燃材料とし下記の全ての対策を適用する。

◆床パネル表面にカーペットを貼る場合は消防法に規定する防炎性能を有するものを使用する。

◆ウッドコアの床パネルは、鉄板等で全面を覆ったものとする。

◆カーテン、ブラインド、カーペット等は、消防法に規定する防炎性能を有するものを使用する。

◆什器、備品（机、椅子、作業テーブル、ロッカー、棚、キャビネット、台車、運搬用ワゴン等）の主要部材は、金属等の不燃材料又は準不燃材料とする。

これらの対策に対する留意事項は；

◆ボーダ部は床パネルと同じものか、金属等を用いて施工することが望ましい。

◆「内装仕上げ材料」として以下のものを使用することが望ましい。

・スラブの断熱材（グラスウール・ロックウール)。

・壁、柱の表面仕上げ（石膏ボード・スチール壁、吹き付け塗装)。

◆ウィスカの発生する恐れがある部材は使用しない。　ウィスカによる情報システム等機器の障害を防止し、機器の安定稼働を確保する事を目的にした部材の選択等を考慮し対策を取らねばならない。

その対策例は；

◆アルミダイキャスト製など、ウィスカが発生しない物を使用する。

◆ウィスカの発生しないメッキを施した部材を使用する。

◆ウィスカが飛散しない処置を行う。

・部材の表面を難燃性プラスチック
（UL 規格　UL94 V－0 相当）の板等で覆い　　ウィスカの飛 散を抑える処置を講じる。

対策に対する留意事項は

◆電気亜鉛メッキを施した床パネル、支柱、ストリンガー、落下防止枠等にウィスカの発生が確認されている。

◆分電盤のブレーカにウィスカが発生し電気的な障害が報告されている。

◆電気亜鉛メッキを施したものにウィスカの発生する確率が高い。

JEITA ホームページ参照「亜鉛のヒゲに注意」

（URL　http://it.jeita.or.jp/infosys/info/whisker/index.html）

◆ウィスカの発生は亜鉛だけとは限らないので十分な注意が必要になる。

◆錫、カドミウム等もウィスカを発生させることが知られている。

◆NASA のホームページ参照「Other metal whisker」

（URL　http://nepp.nasa.gov/whisker/other_whisker/）

図 3.87 はウイスカの顕微鏡写真です。

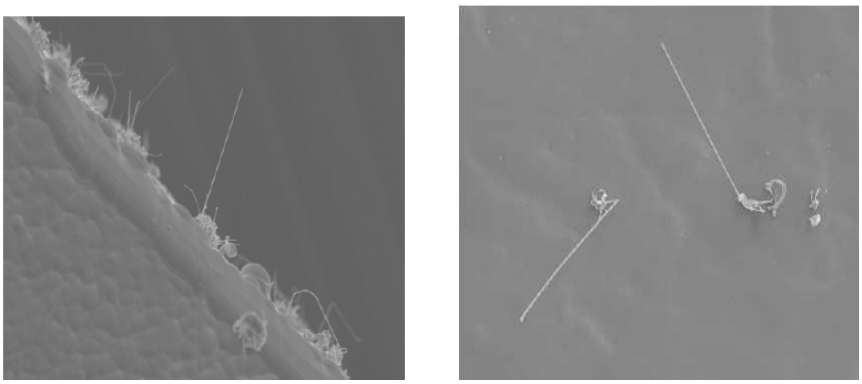


図 3.87　ジンクウイスカの写真

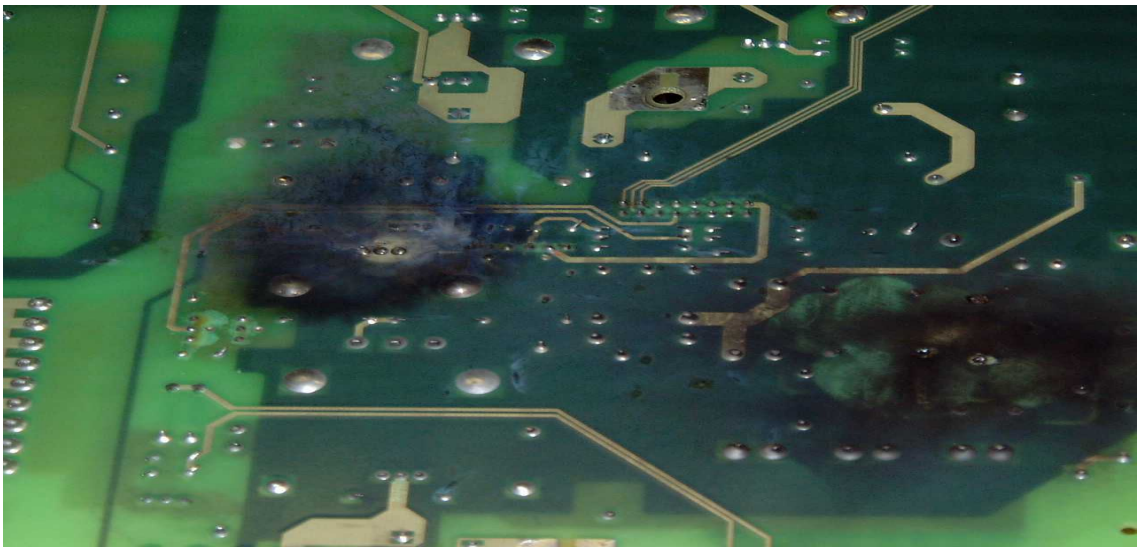


図 3.88　ジンクウイスカの影響を受けた部品

（電源回路で使用している部品）

携帯電話、電波漏洩対策

携帯電話機、トランシーバはコンピュータ室に持ち込ませないで携帯電話機や
トランシーバ等から出力される電波による誤動作を防止する事を目的に対策を講しる事を考慮すべきである。

その対策例は；

携帯電話機、トランシーバは、コンピュータ室への持ち込みを禁止する。

この対策への留意事項は；

◆携帯電話機、トランシーバは、コンピュータ室への持ち込みを禁止をする目的の注意のポスターや文書をコンピュータ室の出入り口や近傍の見易い位置に掲げる。

◆携帯電話機、トランシーバ以外の携帯無線端末については、電磁波セキュリティーガイドライン(新情報セキュリティー技術研究会）参照。

◆携帯電話機の写真撮影機能やメール機能による重要情報の漏洩に留意する。

◆ＰＨＳは外観では電話と識別ができないのでコンピュータ室に持ち込まないことが望まし等を留意し実施しなければならない。

コンピュータ、端末機及びネットワーク
装置からの漏洩電磁波による情報の漏洩
を防止する措置を講じ漏洩電磁波により
情報が外部に漏れることを防止するのを
防止することを目的に対策を講じる必要
がある。

その対策例対策例は；

◆建物、室及び情報システムは、周波数、
強度に応じた電界及び磁界の遮蔽措置を講じる。

◆ネットワーク配線は、下記の対策を選
択して適用する。

◆属管工事、可とう金属管工事、金属線ぴにより配線する。

◆光ケーブルを用いる。

上記に対する留意事項；

◆窓についても電界及び磁界の遮蔽措置
を講じる。

◆無線ＬＡＮのアンテナを設置する場合
は、室外への漏洩を防止する対策を検討する。

小動物による被害防止対策は；
小動物、昆虫による被害防止の措置を講じ、小動物（ねずみ、鳥等)、昆虫の被害から情報システム等を保護する。

この対策例は；
◆外部との境にある開口部等は塞ぐ。
　ねずみ、昆虫が侵入しないように網等を張る。
　不必要な穴は、充填材等で埋める。
◆ケーブルは忌避剤の混入したケーブルを使用するか忌避剤をケーブルに塗布する。

この対策への留意事項；
◆室は、比較的温湿度が一定しており、ねずみが好んで侵入することがある。
　特に、室が人間の生活居住区、ゴミ集積場、食品穀物集積所、飲食店等に近いところに位置している場合は注意する。
◆殺虫剤を使用する場合は、非導通性でかつ非腐食性のものを使用する。
◆各室（コンピュータ室、電源室等）の小動物対策も本項の対策を適用する。
◆定期的にねずみの生息、昆虫の侵入の痕跡を調査し、適切な対策を行う。
　尚、薬剤を使用する場合は上記と同等のものとする。
◆外部にあるケーブルダクト、室外機等への小動物の被害にも注意する。

電気室での対策
専用の室とし被害の波及や犯罪を防止し、運用環境の整備を容易にする。

上記の対策例
◆電源室は他の室と共用しない。
　情報システム専用の電源室とする

（ＵＰＳ等を設置する室）

事業所専用の電源室とする。

建物専用の電源室とする。

キュービクル式高圧受電設備を屋外

(屋上を含む)に設置する場合は、日本工業規格(ＪＩＳＣ　４６２０)に準拠するキュービクルとし，次の条件を全て満たすこと。

◆特定者以外の者が容易に近づけない

措置を講じること。

避難通路、避難階段の避難に支障とならない位置に設置する。

◆屋上に設置する場合は、出入口は防火

戸とし，施錠する。

屋上に面して他の室の窓がある場合は、侵入センサ、網入りガラス，ガラス破壊センサまたは面格子等を設置する。

◆建物構造体、コンクリート,鉄鋼の堅

固な基盤にアンカーボルト等に固定すること。

◆ガソリンスタンド，危険物貯蔵設備,

焼却炉，ボイラ設備等火災の恐れのある場所、腐食性ガスの侵入等外部からの被害を受けるおそれの少ない位置に設置すること。

◆浸水のおそれのない位置に設置するこ

と。

◆避難上支障とならない位置に設置する

こと。

◆消火器を付近に設置すること。

電源の質は

情報システムの電源は、専用とする。

・情報システムの電源設備の電気容量は、

機器の負荷を考慮して余裕を持たせる。

・情報システムの配線にノイズが誘導し

ないよう、電磁遮蔽の措置を講じる。

・情報システムの電源設備は、電圧およ

び周波数の変動に対する措置を講じる。

・設備不平衡による障害の防止措置を講

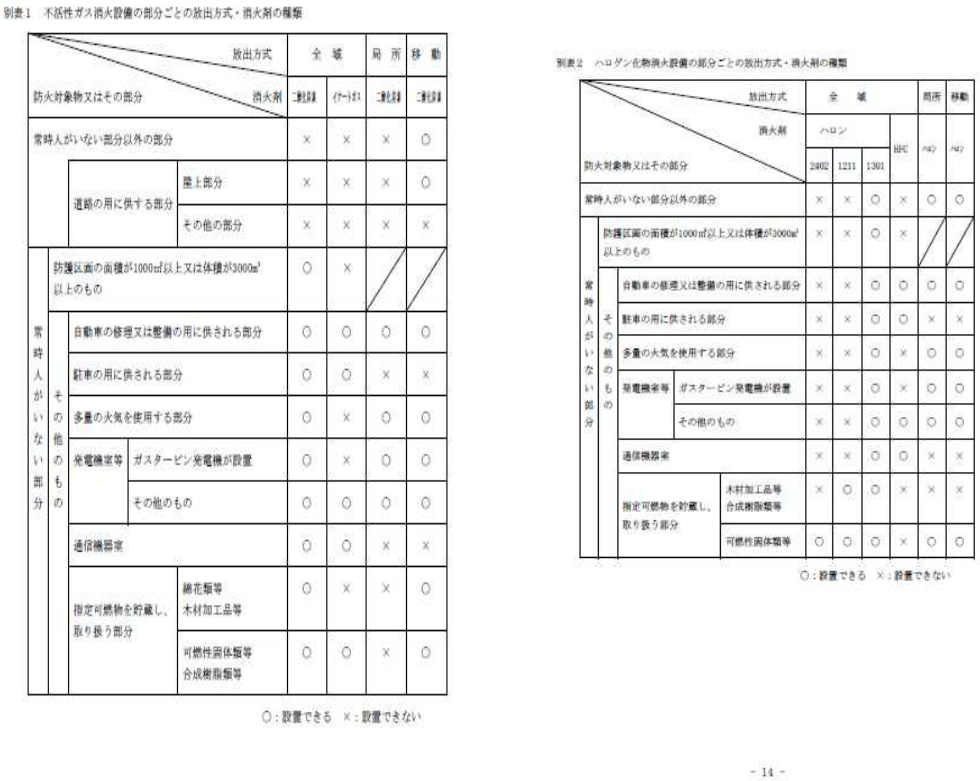
じる。　等を満足することを目的とした設備を用意しなければならない。

・自動火災報知設備および消火設備を設

置する。

・建築基準法に規定する防火区画とする
と共に容易に破壊されない構造とする。

・ガス系の消火設備に関しては消防施工
令１０２（平成１３年3月３０日
参照）



別表1　不活性ガス消火設備の部分ごとの放出方式・消火剤の種類

防火対象物又はその部分 ＼ 放出方式・消火剤			全域		局所	移動
			二酸化炭素	イナートガス	二酸化炭素	二酸化炭素
常時人がいない部分以外の部分			×	×	×	○
	道路の用に供する部分	屋上部分	×	×	×	○
		その他の部分	×	×	×	×
常時人がいない部分	防護区画の面積が1000㎡以上又は体積が3000㎥以上のもの		○	×		
	その他のもの	自動車の修理又は整備の用に供される部分	○	○	○	○
		駐車の用に供される部分	○	○	×	×
		多量の火気を使用する部分	○	×	○	○
		発電機室等 ガスタービン発電機が設置	○	×	○	○
		発電機室等 その他のもの	○	○	○	○
		通信機器室	○	○	×	×
		指定可燃物を貯蔵し、取り扱う部分 綿花類等 木材加工品等	○	×	×	○
		指定可燃物を貯蔵し、取り扱う部分 可燃性固体類等 合成樹脂類等	○	○	×	○

○：設置できる　×：設置できない

別表2　ハロゲン化物消火設備の部分ごとの放出方式・消火剤の種類

防火対象物又はその部分 ＼ 放出方式・消火剤			全域				局所	移動
			ハロン			providC	ﾊﾛｹﾞﾝ	ﾊﾛｹﾞﾝ
			2402	1211	1301			
常時人がいない部分以外の部分			×	×	○	×	○	○
常時人がいない部分	防護区画の面積が1000㎡以上又は体積が3000㎥以上のもの		×	×	○	×		
	その他のもの	自動車の修理又は整備の用に供される部分	×	×	○	○	○	○
		駐車の用に供される部分	×	×	○	○	×	×
		多量の火気を使用する部分	×	×	○	×	○	○
		発電機室等 ガスタービン発電機が設置	×	×	○	×	○	○
		発電機室等 その他のもの	×	×	○	○	○	○
		通信機器室	×	×	○	○	×	×
		指定可燃物を貯蔵し、取り扱う部分 木材加工品等 合成樹脂類等	×	○	○	×	×	×
		指定可燃物を貯蔵し、取り扱う部分 可燃性固体類等	○	○	○	×	○	○

○：設置できる　×：設置できない

- 14 -

図 3.89　不活性ガス／ハロゲン化物消火設備の部分毎の放出方式・消火剤の種類

出入り口の管理

・出入り口には錠を取付け、入退の管理
ができる措置を講じなければならない。

地震による移動および転倒を防止する措置を講じる必要がある（前項と同様の対策が必要である）。

空調室関連の対策

空調設備の外気取入口及び排気口は、雨

水が侵入しない構造とする事が必要である。　その他下記の対策も講じる。

・扉には、錠を取付ける。

・屋外に設置される空調設備には、特定

者以外の者が容易に近づけない措置を講じる。

・空調設備の電源の地絡を検知し、警報

を発する措置を講じる

・自動火災報知設備及び防火ダンパを設置する。

コンピュータ機器と発熱の関係

近年コンピュータ機器からの廃熱

（発熱）処理が問題になって来ている。その問題になってきている原因の一つは

１：機器の高速化に伴い発熱量が増えてきた

２：機器のサイズが小さくなり単位面積当たりの設置代数が多くなってきた

３：配置により熱溜りが発生することが増えている

との説が強い。

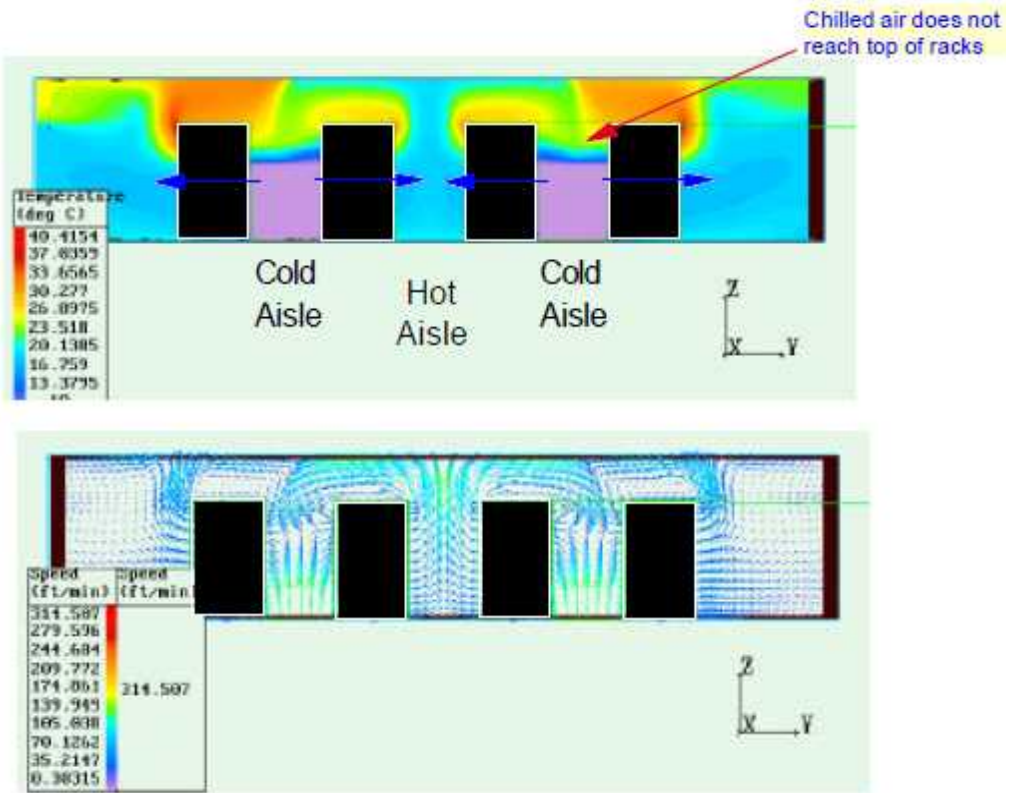


図 3.90　機器の排熱と熱だまりの関連

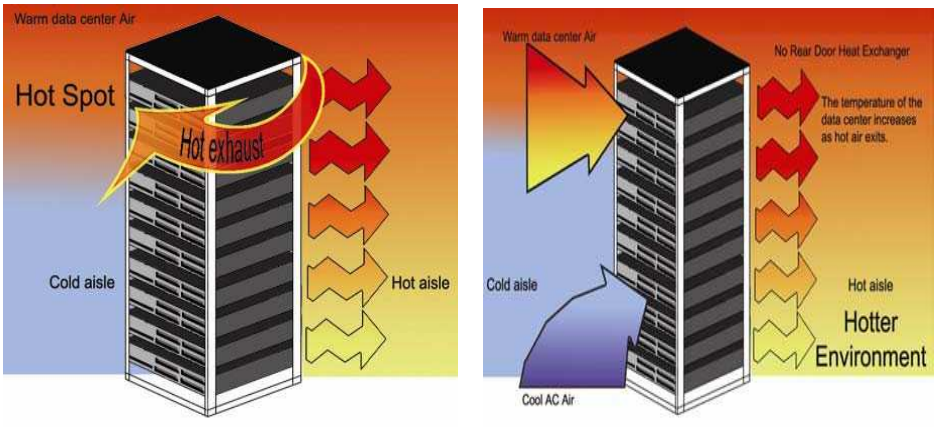


図 3.91　機器と排熱の例

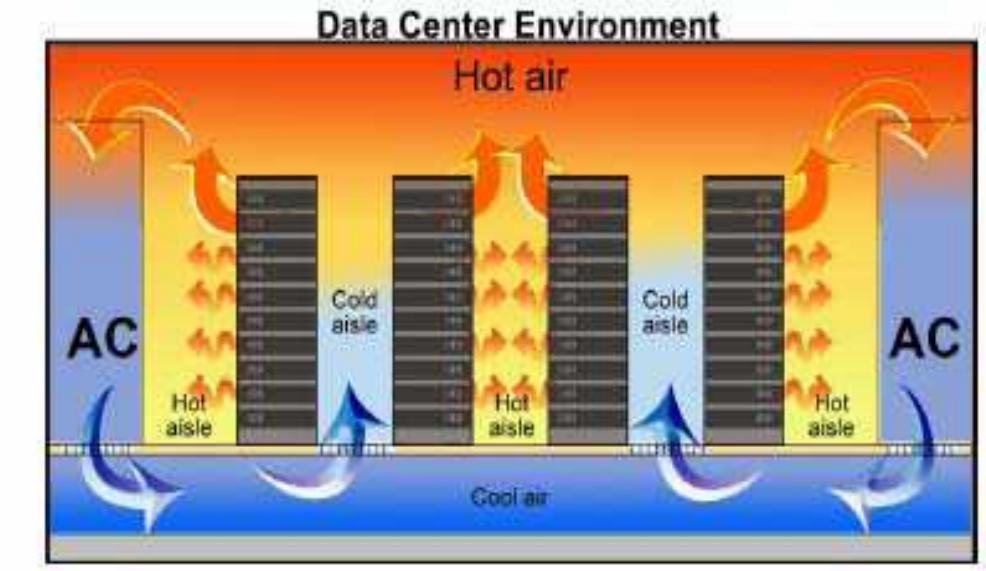


図 3.92　空調と機器の関連

図 3.92 のように空調を適切に配置し熱溜まりの解消を図らなければならない。

災害時の対応も重要な項目の一つである

・一般的にコンピュータ関連業務は企業
　の中枢を担っている。

・現在はシステム稼動が２４時間対応で

あり、システムが停止することは企業の業務継続に多大な影響を与えることになる。　このため、最小時間のシステム停止で障害の回復が出来るかが課題である。　そのために、システム関連の設備は二重化し短時間で切り替え可能でなければならない。

◆電源設備　◆空調設備　◆通信回線

◆システムのバックアップ等

・これらをいかに早く切り替え、回復さ
せるかが重要になってきてい。

・広域災害の場合の詳細対応も検討しておく必要がある。

サーバ室と事務室の対応も重要な項目になってきている。

サーバ室はコンピュータ室と同等な設備が必要になる。　その代表的なものは；

・外部からの影響を受けない設置環境と
する。

・専用の区画とする。

・出入口、窓等は直接外部から被害を受
ける恐れのない場所に設ける。

・出入口は、入退管理設備を設け扉に錠
を取付ける。

・静電気の帯電を防止する措置を講じる。

・天井、照明器具、間仕切壁及び床は、
地震により損壊しない構造とする。

・地震によるサーバ等の移動・転倒を防
止する措置を講じる。

・分電盤は専用とする。

・発煙を早期に発見できる措置を講じ、
消火設備、消火器等を設置する。

・什器、備品の主要部材は、不燃材料又
は準不燃材料とする。

・漏水の検知及び防水措置を講じる。

・異常を検知し、通報する措置を講じる。

この様な対策が必要になるのはコンピュータ機器の発熱が益々増加傾向にある為である。

事業継続をいかに考えるかでどのような設備を構築して行くかが決まり、将来の拡張に対応できる設備（余裕度を持たせて有るか等）を構築するかの参考資料としてお使い頂きたい。

3.10 IT ガバナンス FAQ

3.10.1 ＰＣのハード、ＯＳに依存しないセキュリティ機能を盛り込んだ新しいＯＳの進行状況、実現性

■Q：ＰＣのハード、ＯＳに依存しないセキュリティ機能を盛り込んだ新しいＯＳの進行状況、実現性について教えてください

■A：質問の趣旨と少し異なるかも知れませんが、私の推測ですと、セキュアＯＳの様なものを想定しているのではないかと思います。どの程度の進捗かについては、あまり詳しくありませんが、企業での導入を考える場合、サーバーであれば、ウェブサーバー、メールサーバーと言ったアプリケーションも含めて考えないとなりません。また、オフィスでの導入を考える場合、そこで利用している、あるいは、利用するソフトウェアについても考える必要があります。この辺りは、あまり簡単に考えないほうがいいと思っています。

少し前に、私の周りにいた方々から、『オフィスソフトウェアなんて簡単にこのソフトウェアで代替できる』と言われました。でも、その方々に、『マクロが完全に動作しますか』と聞くと、否定的な回答しか返ってきません。要するに個人が趣味で利用している場合にはいいのですが、他社とのデータ交換とか、マクロを利用したアドインソフトウェアなどを利用している場合には、それらが動かないとオフィス中では役に立たないこともあります。

もう、20 年位前になりますが、某社の表計算ソフトの互換ソフトウェアの日本語化について、アドバイスやテスターを依頼されたことがありますが、単純な計算だけであれば、あまり問題がおきませんが、マクロの実行になると正しく動作しないことがありました。この様な経験がありますので、単に OS ができたから問題ないと考えない方がいいと思っています。

3.10.2 対策インデックス

■Q：対策インデックスの意味について教えてください

■A：これは例を示すことで、お分かり頂けると思います。例えばウイルス対策をやるとか入退室管理をやるとか、そういう具体的な対策と要求されている項目です。この問題はどこに該当するのかと言ったインデックスですね。丸、バツ、三角等で示すマルバツ表の様なものを想定して頂ければ理解できるのと思います。最低限作っておくべきもので、それによって他の要求事項が出てきた場合にも応用できますし、きちんとした整理ができるので効果的、合理的な対策ができることになります。

簡単に検索・参照できる仕組みを作っておきなさいということになりますね。

3.10.3 J-SOX 関連の評価方法

■Q：J-SOX に関連して、「過年度の評価結果利用に関して」、２度目以降、前年度の評価を利

用するという他に、ISMS 等、他で用いた結果を活用することも可能なのでしょうか？

■A：－過年度の評価結果というのはＳＯＸにおいてということでしょうか。

－これは、例えば内部監査でのサンプリングは 25 件やればいいということですが、当然そこで問題がなく、組織あるいは、システム的に変更がなければ次の年にはもっと少なくて済むのではないかという趣旨のご発言でした。この考えを敷衍すれば、ISMS 等、他の評価結果を活用してもいいのかという質問です。

－これは厳密には、1 年目できちんと評価をした時に、2 年めで特に IT 部分、IT 業務処理統制部分に変更がなければ、極端な話、変更がないことだけ確認すればその年は何もしなくても済むという考え方が採れるということです。ただポイントは変更がないということの確認方法で、この辺りが、多分議論になる可能性があります。米国 404 条の場合には厳密にタイムスタンプを確認する等という厳しいことが出ていますが、もう少し緩めに取れば IT 全般統制でプログラム変更等の統制がきちんとしていれば、変更がないということは自己申告的なレベルでも許されるのではないかと言えるかもしれません。変更なしのチェックが厳しいか緩いかについて、どのレベルで落ち着くかは、現時点では、外部監査人に確認をするしかありませんが、アメリカよりもここを積極的に採用していこうという考えであれば、基準が緩めになるのではないかと思っています。

－現時点では、監査人との相談が基本だと考えて欲しいですが、事例がたくさん出てくればまた変わってくると考えてよろしいでしょうか。

－まだスタートしていないので、推測の域にしかありませんが、事例が積み重なってくれば、一定の基準がでてくるということになりますね。

－現時点では、ISMS 等について、経済産業省の中でも議論をしましたが、やはり異なるものということで、入ってはいません。ただ、企業側がマネジメント体制が確立しており、それで管理している。きちんと体制が確立しており、整斉とやっているとの心証を監査人に与えることはできると思います。企業が積極的に監査人に対して発言していき、会計士に任せないで行うことが大切だと思います。ここまでやっており、残っている部分を実施すればいいのかを確認する方がいいと思います。

－それに関連していますが、まさに私の所でも説明をしましたが、ISMS だけではなく、情報セキュリティ監査では、報告書が作成されますので、まさに原田さんのお話のように、きちんと担当会計士と相談して、こういうことを我々はやっているのだから、それを利用していいですよねと言った働きかけを行っていくべきだと思います。

－私の研究室にいる社会人学生の勤務先で、ISMS の認証を取得しているそうですが、J-SOX 対応について、ISMS でやっている内容の説明をして、これで問題ないかを公認会計士に確認したら、何も言うことはありませんとの回答が返ってきたという話もあります。この辺りは多分、ISMS や情報セキュリティ監査等での体制について、相応の実績を作るというか、企業側が対応できるだけの体制を構築し、運用を整斉とやり、それを外部監査人に正確に説明することが大切だろうと思っています。

3.10.4 内部統制の監査

■Q：内部統制の４つの項目の内、①合理的、効率化、②信頼させる財務報告、等が挙げられていますが、監査法人は②にばかり注力しているのでしょうか

■A：内部統制の４つの項目の内、①合理的、効率化、②信頼させる財務報告、等が挙げられていますが、監査法人は②にばかり注力しているとの噂がありますという質問ですが。

－あくまでJ-SOXの目的は財務報告は信頼されるものということです。もちろん会社として内部統制に注力するという意味では②だけでなく他も全部やらなくてはいけないのですけれども、今回 J-SOX でフォーカスが当たっているのはそこだけなので、J-SOX対応にはそこだけをやっていれば特に問題は出ないということですね。ですから会社は一般的には全部やらないといけないとは思います。

－会社法の中で考えるとやはり全部やっていただくことになると思います。システム管理基準も①の合理化、効率化等、全部入っています。企業として今回、J-SOX対応でということになれば、②になります。監査法人も現時点では①は到底見られませんと言うと、監査人に対して失礼かも知れませんが、まずは②だと思います。

－優先順位の問題ですね。①あるいは③、④が必要ないということでなく、最初に見るのは②ですと理解したらいいですか。

－ただ企業としては、①は話だけで済むわけではないと思いますので、そこは自然体でなさっていいのではないかと思います。

3.10.5 証拠としてのメール

■Q：証拠としてのメールについて、日本では、どういう場合に裁判に於ける法的根拠になり得るのでしょうか？

e.g　J-SOX の文書化に関して、とりあえずメールで送ればいいという考え方。刑事/民事を問わず、同じ考え方でよいのでしょうか？

■A：質問の意味を正確に理解していない面がありますが、刑事であれ、民事であれ、裁判所がどう判断するかではないかと思います。

－最近の例として、ホリエモン事件では、フォレンジック関係のものは何一つ出てこなかったようですし、また、日興コーディアル証券の社長だかのメールが全部消えていたとの話もあります。しかしながら、当然サーバーかクライアントPCを押収してコンピュータフォレンジックで、ハードディスクの内容を全て調べているだろうと思います。あくまでもしらを切れば、調査内容を証拠として提出してくる可能性はあると思っていますが、そこまでの裁判になるかは、別の話だと思います。本当に必要であれば、きちっとやっておくべきだと思っています。上記にお話について、私は法律家ではありませんので、あくまでも個人的な見解です。この辺りも何をやっておくかということになれば、きちんとした対応をしたほうがいいということになります。先ほどのJ-SOXで言えば、監査人に、これをやる必要がありますかと聞けば、絶対やる必要がありますと答えます

と言われています。これと同じだと思っています。

－ご質問の趣旨に合っているかどうか分からないですけれども、証拠としてのメールという意味でいくと、評価をするときのエビデンスにメールが使えるか。それはメールに対するアクセスコントロールというのがちゃんとできていて、エビデンスとして簡単に削除ができないような仕組み、もしくは改ざんができないということになれば、一般的に改ざんは普通簡単ではないので、証拠としては十分使えると思います。

3.10.6 メールを送る際のパスワード

■Q：メールを送る際はパスワードが必要とのことについて、それは各社員が毎回送る際に意識するのか、あるいは一度設定すればＯＫなのでしょうか？

■A：パスワードというより、ユーザーＩＤ、即ち、個人認証をしてメールを送っていることが大切になると私は判断をしたのですが、私は PC 端末を使う場合、必ずユーザーＩＤ、パスワードを入れ、その後にメールソフトを起動して、メールの送受信を行うという手順がある訳ですが、この最初の個人認証が行われていることをパスワードが必要と言ったと判断していますが。

国内企業・組織の中には、個人毎にユーザーID、パスワードを設けてクライアント PC を使う仕組みになっていない企業がたくさんあります。このため、誰が送ったか分からないメールはダメというと解釈しています。

3.10.7 事業継続管理の規格 BS25999

■Q：英国規格 BS25999:2005 が国際標準化されると日本企業は何か新たな対応を求めるようになるのでしょうか？また、国内ガイドラインに対応していけば新たな対応を求められることはないという理解でよいでしょうか？

また、国内での第三者認証制度の可能性について教えてください。

■A：BS25999 ですが、認証規格になる予定になっております。英国と取り引きがある企業では、その認証規格を要求される可能性があるので、今から英国の認証を取る準備を始められたという話はあります。まんざら関係ない話ではないとは思います。

－基本的にはいくつかのケースが考えられます。BS25999 が ISO 化されるのか。ISO 化された場合には、どのような体制での対応になるかが一つあります。

ISO 化されない場合には、国内で BS25999 を第三者認証の仕組みとしてやる考えがあるとしたら、どこの組織がこれをやるかということがあります。勿論、BS25999 を本当に日本企業で必要としているかということが、一番最初にないと、どこかがやる、もっとはっきり言えば、JIPDEC はユーザーからの要求がないのにやる可能性は少ないと思っております。

BS25599 の ISO 化では、二つの考え方があると思います。第三者認証を含めた形で ISO 化される場合と、第三者認証がない形での ISO 化です。

第三者認証を含めて ISO 化されると、ISO は早期に JIS になる可能性が高いので、認

証機関、審査員も考える必要があります。認証機関とか審査員に関してどのように計画がありますかという質問については、これらのことを踏まえて考える必要があります。以上のことを考え、その動向を見定めてから、質問を考えるのでも遅くないと思っています。これは、私の個人的な考え方であるとご理解ください。多分、JIPDEC の方々の考えもあまり大きなブレはないと思っています。

3.10.8 BCM の演習

■Q：BCM の演習について、火事の予行演習みたいなもので、地震や火災などを想定しているという理解でよいでしょうか？

■A：日本語で演習というときには多分ドリル（Drill）の日本語訳です。実際に体を動かして何かの訓練を指しているので、避難訓練とかそういったものも含まれるということです。日本語は不便な言葉で、みんな訓練しかないのです。向こうの場合はいろいろなバリエーションが、エクササイズ（Exercise）だとかドリルだとかそういう細かい分け方になっています。それを単純に訳したものだと思います。

ー一般的にはドリルと言っているケースが英語では多いですね。当然、日本だと火災では、防火訓練をやったり、地震では、９月１日に防災訓練をやっていますが、あれをご想像いただければいいのかもしれません。ただしもちろん IT の場合は、少し違います。IT 関連であれば、実際にバックアップセンター等を利用して行います。私は米系の銀行にいましたので、実際に外部のデータセンターを使って業務の一部を動かすということをやってきました。

3.10.9 BCP への取組み状況

■Q：BCP の取り組み状況について、日本企業の取り組みの「策定している」企業数が、2005 年と比較して 2006 年の策定している企業の数が減っているのはなぜなのでしょうか？、また、BS25999-1 で記載されているステークホルダーとは誰を指すのでしょうか？

■A：2005 年の調査のときには BCP という言葉はあまり一般的ではなくて、アンケート調査をした企業の回答者の方が、これが BCP だろうと思っていたのに丸をしてくださっている状況です。しかしながら、策定している中身を見てみますと、ほとんど初動対応マニュアルばかりでありました。１年ぐらいたって 2006 年になりますと、やはり BCP には、復旧とか業務再開等が入っていないとおかしいと考える企業が多くなり、今まで BCP を策定していると思って回答していた方が、出来ていないということで取り組み中が増えてきたのだろうと推測しています。2005 年のレベルですと BCP と BCM の区別もついていなかった状況だと思っています。

ーステークホルダーに関しては、当然いろいろなケースが考えられますね。

ー利害関係者ということで、広い意味で地域住民だとか社会まで含めてだろうと思います。それは各社自分で考えればいいということだろうと思います。

3.10.10 欧米と比較した日本企業の BCP 取組み状況

■Q：日本企業のＢＣＰ対応は欧米と比べ遅れているのでしょうか？、遅れているとしたら何がどの程度遅れているのでしょうか？、地震対応は日本が進んでいるといえるのでしょうか？

■A：取り組みという点では日本はまだ始まったばかりで、色々なガイドラインが出てきたのでようやく皆さん取り組み始めたということですね。今後、策定率が上がり中身の改善等が行われればいいと思っています。遅れているという意味合いがよく分かりませんが、そう悲観するものではないかと思っています。

ー全体的なパーセンテージから言えば少し、中身はちょっと分かりませんが、少ないことは事実です。米国ワールドトレードセンターが 1993 年 2 月に地下が爆破されました。当時、日本の銀行がたくさん入っていたのですが、日本の銀行はアメリカの連銀の検査で、BCP、当時はディザスターリカバリーと言っていたかも知れませんが、訓練をやっていないとアメリカにある支店は追放させました。このようにかなり厳しい業界もありましたが、国内では金融機関はあまり BCP に対して厳格に対応したくないという面はありました。ただ、テロとか災害等を考えても、どの程度日本と欧米の相違があるのか、それによってリスクを考えると、どの様に対応するのはを考えておくことが大切だと思っています。そこまで考えると、一概に遅れているということにはならないのではないでしょうか。ただ、サプライチェーン的なものが出てくると BCP を立案・実行しているどうかを要求されることも当然ありますので、その辺りまで含めて考えておく必要があると思っています。後半のどの程度遅れているかですが、簡単に答え難いですね。地震対応は日本が進んでいますが、当たり前です。地震に関して言えば、今先進国の中で地震があるのは日本とアメリカ西海岸程度ではないでしょうか。日本の特殊性があると理解しています。

3.10.11 パンデミックインフルエンザ

■Q：日本では鳥インフルエンザの脅威はそれほど注目されていないように思います。本日の基調講演でも、まず地震から始めようという話がありましたが、地震の脅威と比べて日本におけるパンデミックな脅威はいかがでしょうか？

平成 19 年 1 月 19 日に厚生労働省が公表した新型インフルエンザ対応で企業に在宅勤務体制構築を求めていますが、個人情報保護等の関係で在宅勤務体制が構築できない場合はどうすべきか？

■A：日本ではいわゆる健康問題というのは労働衛生上の問題というとらえ方が多くて、海外の場合はこれを BCP ととらえる。それは位置付けの問題だけで、では海外のパンデミック BCP の内容は何かというと、そんなに事細かに事業継続のことを書いてあるわけではありません。基本は労働衛生のことで、手を洗いましょう。マスクをしましょう。タミフルを飲みましょう的な所が中心になっていますので、日本の場合ですとやはり労働衛生から BCP を始めればそんなに遅れるとは思いません。

それから地震と新型インフルエンザのどちらのリスクが高いのか。発生確率なのか大きさなのかということがあろうかと思います。地震は、例えば首都圏直下、今後 30 年以内に 70%と言われています。鳥インフルエンザが今 WHO のレベル３ということ。これが数年以内に起きるというように予測されていて、今年は大丈夫かと思っていますが来年だめではないかという話もある。そういうのを比べますと、必ずしもどちらが大きい、小さいという比較は単純にはできないのではないと思っています。

例えば宮城県沖地震は、今後 10 年、20 年でほぼ 100%ですから、そういったものと比べますと地域ごとによって若干の差はあるというようには思います。

ーいわゆる鳥インフルエンザというか、新型インフルエンザですが、現在の感染レベルは、レベル３とのお話がありました。レベル５になって人から人への感染が非常に激しくなるような状況になったときには、僕は自分自身が生きている可能性は偶然の確率しかないだろうと思っています。厚生労働省のホームページに今この新型のインフルエンザに関してのパブリックコメントを求めていますので、ご興味というよりはぜひ見ていただきたいです。それと国立感染症研究所の岡田晴恵さんという研究員が、新型インフルエンザに関していろいろなところに書いております。書籍も出ています。少なくともそれを見ている限り、個人レベルで 14 日間の水と食料の備蓄が必要と言っています。14 日間の備蓄をやろうとすると、水だけでも、１人１日２リットル 14 日間。家族４人がマンションに住まいであれば、ほぼ備蓄は不可能です。電力や水も来ない可能性があるとすれば、新型インフルエンザが大規模に発生したら、そこで生きていける可能性は、私は偶然ではないかと思っています。このような状況で、備蓄しなければならないものは、水や食料だけでなく、薬とかマスク等の医薬費、防災用ラジオや乾電池等の日曜品も含まれます。

平成 19 年１月 19 日に厚生労働省が公表した新型インフルエンザ対応は在宅勤務体制の構築を求めていますと言っています。これは在宅勤務にしなければ多分日本崩壊になる恐れだってあるのだろうというレベルを考えてみていただきたい。例えば、アメリカでは、多くの人が自家用車を使って通勤しています。このことは通勤時間、自宅から勤務先までに他人と接触する機会は限りなくゼロですが、日本では首都圏等の大都市圏では、ほとんどが電車通勤をしています。通勤電車の中で、片手を出して触れる距離に何人いるでしょうか。鳥インフルエンザでは潜伏期間が８日ですから、８日間に往復したり、仕事で外出した時、何人と接触するかを考えると、相当の数になります。リスクマネジメントの講義で、本学の学生と １ ヶ月位前に議論をしました。非常に悲観的な状況になった時には、生き残れるかどうかは確率論の問題になると考えています。個人情報保護等の問題以前の事柄ではないかと思っています。

3.10.12 日本と海外との BCM の違い

■Q：日本と海外の BCM で一番違う点はどのような点でしょうか?

BCM に関するソフトウェアツールの日本での導入実績はどのくらいでしょうか、またど

のような機能を有しているのでしょうか？

■A：違う点は、１つは、特定のリスクに特化したBCPを作っているのかというもの。もう１つは、責任者の体制ですか。BCマネージャーみたいな人たちが積極的に推進していくという体制がまだできていないというところでしょうか。詳細な部分については、いくらでもありますが、大きな点ではこの２つだと思っています。

また、ソフトウェアツールについて、海外には色々あり、BIA（Business Impact Analysis）のツール。この関係のソフトウェアは必ずしも自動的に分析してくれるわけではなくて、アンケートやインタビューのソフトといったものや、BCPの策定ツールですね。それから、例えば、個人の情報だとか緊急連絡網の情報だとかそういうデータベースですね。そういったもののツールが特にアメリカなどではたくさん出ています。

3.10.13 BCP策定に係る費用

■Q：大企業については、いろんな対策できる金銭的余裕があると思いますが、中小企業にとっては、そればかりに資金をつぎ込むと事業に差し障りがでてきます。そこで、売り上げの何%くらい投資するのが適当なのかといった目安について教えてください

■A：東京商工会議所で今、中小企業のためのBCPの推進というのを進めていまして、アンケート調査で、BCPが必要かとか、地震対策は必要か等です。皆さん総論賛成なのですけれども、では対策整備をするのにどのぐらいお金をかけられますかとお聞きしましたら、最大30万円という答えでした。これではコンサルタントは雇えませんので、来年度以降、どの様なことを考えるかですが、例えば、安価なシステムを東京商工会議所で作って会員の皆さんに公開する等を企画しています。中小企業が対象です。30万円が限度なのかなという気はしています。

3.10.14 公的支援

■Q：リアルタイムバックアップ（リモート）は費用が高い。公的支援がないのか（サービスする側、受ける側）

■A：それはないのではないか。

－そうでしょうね。そのため、例えば外部のISPあるいは、ASP等を使って行う仕組みを作るしかないのかも知れませんね。リアルタイムバックアップは以前から比べればクライアントサーバー方式でも比較的簡単にできるようになってきましたが、それでも決して安くはないと思います。ただ、リアルタイムバックアップ方式を採用する必要があるリスクがあるのかを考えるべきですね。リアルタイムバックアップ方式をやるかやらないかではなく、企業の存続に関係するのであれば、それに見合う費用をかけてやる必要があります。リスクを検討し、決める話だと思います。やらなくても、大した問題にはならないのであれば考える必要はありません。

－最近BCPの策定に伴って融資制度というのが都市銀行等でスタートしていて、地銀等でも行っております。防災投資は、何もリアルタイムバックアップだけではなく、耐震

補強等も含めてやっていく。BCP は作っているということであれば低利で融資を受けられるということは民間、それから公的なところを問わず今進みつつ、整備されつつあります。

3.10.15 はじめの BCP

■Q：はじめて BCP を実施するときは、BIA をやらないほうが良いとのことでしたが、その代わりに何をどのようにやれば良いのか教えてください。
緊急時に社員を出社させるための策を教えてください。例えば、都内に家賃補助とか。

■A：初めて BIA をやると大変なのですね。手順を考えると、まず社員全員にアンケートを取り、あなたの仕事の優先度は？何日で復旧できますかとか？何日で復旧しないといけないですか？、とか、インパクトはどの程度ですか？ とかそういうのを聞く必要があります。それから社内のキーパーソン全員にインタビューして同じようなことを聞いて、それを集計して自分の会社における業務の優先順位などをつけていかないといけない。初めての会社でこれが可能でしょうか？むしろ、社内の主要部門の方々に集まって頂き、そこで一応仮決めすとという合意形成を行うのです。BIA で優先順位をつけようとすると、自分の仕事が一番だと思っていますからなかなか社内でまとまらないのです。これをやると、時間や労力等が非常にかかり、入り口で終ってしまう可能性が高いので、仮決めで代表者だけにインタビューというかブレーンストーミングをして決めてしまうということでスタートしたらいかがですかというご提案です。
緊急時に社員を出社させるのにどうしたらいいですかについては、地震のことを考えていらっしゃると思うのですけれども、少なくとも首都圏では M7.3 が出たら社員の出社は無理です。ところが例えば宮城県や東海地震等の地方の場合では出社はある程度可能だろう。それ以外の事象になりますとそんなに難しくはないと思っています。首都圏でやるとしたら環 7 の内側に社宅を建てていただく。あるいは近くの人をいわゆる被災時直行社員か何かに任命して、10 キロ圏内の人間を集める仕組みを作っていっていただくというのが現実的だろうと思っています。
－本社等の近隣に緊急時の本社的なものを作っておき、緊急時には、そこに出社するというのもありますね。
－あります。

3.10.16 サイバーテロ対応

■Q：サイバーテロ対応は、日本は英国に比べ進んでいるのでしょうか？
２月７日の演習は何社参加してどのような訓練が実施されたのでしょうか？

■A：サイバーテロ対応について、進んでいるかいないかいう話でなく、米国には CERT/CC というのがあります。それから英国には NISCC というのがあります。CERT/CC は、Computer Emergency Response Team/Coordination Center の略称です。英国では、NISCC（ナイシー）と言い、National Infurastructure Security Co-ordination Center

の略称ですが、これらの組織は、色々なサイバーインシデントに対応しています。これらの組織と一緒に活動しているのが、国内では、JPCERT/CC（Japan Computer Emergency Response Team/Coordination Center）があります。そこがお互いにセキュリティにインシデントが起きたときには、自国だけで対応できないことが多いので、情報交換を行うことにより、攻撃がどこの国／地域からのものかとかを相互に連携しながらやっています。情報共有や連携して対応していると考えて下さい。

－2007 年の演習というのは内閣官房情報セキュリティセンターがやった演習ですね。重要インフラの企業が集まって行った机上演習ですね。

－はい。内閣官房のホームページ（http://www.nisc.go.jp/）にニュースリリースが出ています。参加者は、重要インフラ 10 業種とそれらを管掌している省庁、及び有識者で、約 90 名が参加したようです。ただ、残念ながら、英国もサイバー演習をやっていますが、詳細は外部にでてきておりません。数日前に会合があり、何らかの形で実施した内容を取りまとめたらどうかとの話がでましたので、どこかのタイミングで出てくる可能性はあるかもしれません。内閣官房のホームページをウォッチしていただきたいと思います。

－アメリカでは 90 年代の中頃から 2002 年位までの間にいくつかのサイバー演習をやっています。例えば、1996 年 3 月に、DARPA（米国国防省高等研究計画局）が、RAND 研究所に委託して、机上演習を行いましたが、その報告書「The Day After... In Cyberspace」が有名です。その他、サイバー演習については、「エリジブル・レシーバー（Eligible Receiver）」とか、「デジタルパールハーバー（Digital Pearl Harbor）」等があります。ご興味があれば、Web で検索すれば、これらの資料を参照できます。国内では、経済産業省が 2000 年前後に、「大規模プラント・ネットワークのセキュリティについて ～重要システムへのサイバーテロリズム・クラッキング対策のあり方～」に関連して、「大規模プラント・ネットワーク・セキュリティ対策委員会」が開催され、実証実験の報告書（http://www.ipa.go.jp/security/fy11/report/contents/intrusion/plant-security/index.html）が公開されています。ただ、個人的には、平成 18 年 8 月に東京大停電が発生しました。サイバーテロではありませんが、荒川と多摩川にかかる高圧電線と、北から東京に入ってくる高圧電線の三系統をショートさせたら東京はどうなるだろうと考えたほうが簡単です。私がサイバーテロリストでも、サイバーテロを選ぶよりは大停電を起こすほうが簡単だろうと思っています。

3.10.17 情報セキュリティインシデント

■Q：被害を届け出ない企業も多いと思うが、実際はもっと事件は起っているのでしょうか？
ボット防止のウイルスソフトで有効なものを教えてください。
被害の届出は誰が行うことが多いでしょうか？
どうやって発見したのでしょうか？

■A：「被害を届け出ない企業も多いと思うが」というのは、その通りだと思います。ただ最近

は個人情報漏えいでは、積極的に外部に公表するようになってきていると思います。いい方向に向かっているとは思っています。ボット対応ソフトで有効なもの。ボットの説明をしましたが、亜種だけでも非常に変化があります。更に、「見えない化」と言っていますが、従来のウイルスのようにその場ですぐ影響が出るのではなく、じっと隠れており、なかなか検出できない。このため、経済産業省、総務省、IPA、JPCERT/CC、Telecom-ISAC等が一緒に、ボット対策のプロジェクト、サイバークリーンセンターを作りました。ISP（Internet Service Provider）がボットの可能性がある自社の利用者に連絡して対策をお願いするとか、ボットの状態をこのサイバークリーンセンターに集め、早期に対策のツールを作ると言った検討を行っている最中です。

－簡単に言えばボットに対して、完全な対策はありませんということですね。

－極論を言うと非常に厳しいです。

－ウイルス対策だって 100%完璧はありません。ボットでも同じと考えたほうがいいと思います。

－届け出は色々な人がやっています。ただ、届け出ででして被害ではありません。IPA も届出と被害の関連の報告はしています。時々、届出を被害と考えている方がおりますが、誤解しないでくださいと一言付け加えておきます。

4. おわりに

この一年マネジメントシステム評価検討委員会では、当報告書で報告させていただいた通りITガバナンスを主なテーマとして事業継続関連やJ-SOX法関連について調査や検討、及びシンポジウムの実施を行ってきました。

最近の情報セキュリティの問題は、情報セキュリティマネジメントシステム（ＩSMS）といった、広い視点でとらえられる重要な分野となってきており、ＣＳＲといったような形で少しずつ社会的認知がされつつあります。しかし、情報セキュリティの分野は国内においての認知度が低く、認知度を高めるためには、情報セキュリティというものに取り組んでいる企業を積極的に評価してくれるような仕組みを実現してゆくべきであり、この実現に努めていかなければならないのではないのかと思います。

最後になりますが、今後ともこのような企画をさらに進め、皆様とともに情報セキュリティに関する意識を互いに高め、課題に対する解決の方策などを検討してまいりたいと思います。ご協力ご支援をお願い申し上げます。

平成19年3月
マネジメントシステム評価検討委員会
財団法人日本情報処理開発協会

平成 19 年 3 月発行

発行者：財団法人　日本情報処理開発協会
東京都港区芝公園 3-5-8　機械振興会館内　〒105-0011
TEL:03-3432-9386
E-mail:info@isms.jipdec.jp

印刷所：山　陽　株　式　会　社
東京都千代田区神田神保町 1-18
TEL:03-3293-5411

１８－Ｈ００５