17－H005

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18年3月

JIPDEC

財団法人　日本情報処理開発協会

KEIRIN

この事業は、競輪の補助金を受けて実施したものです。

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１７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、パネラー及び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18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、BCP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。

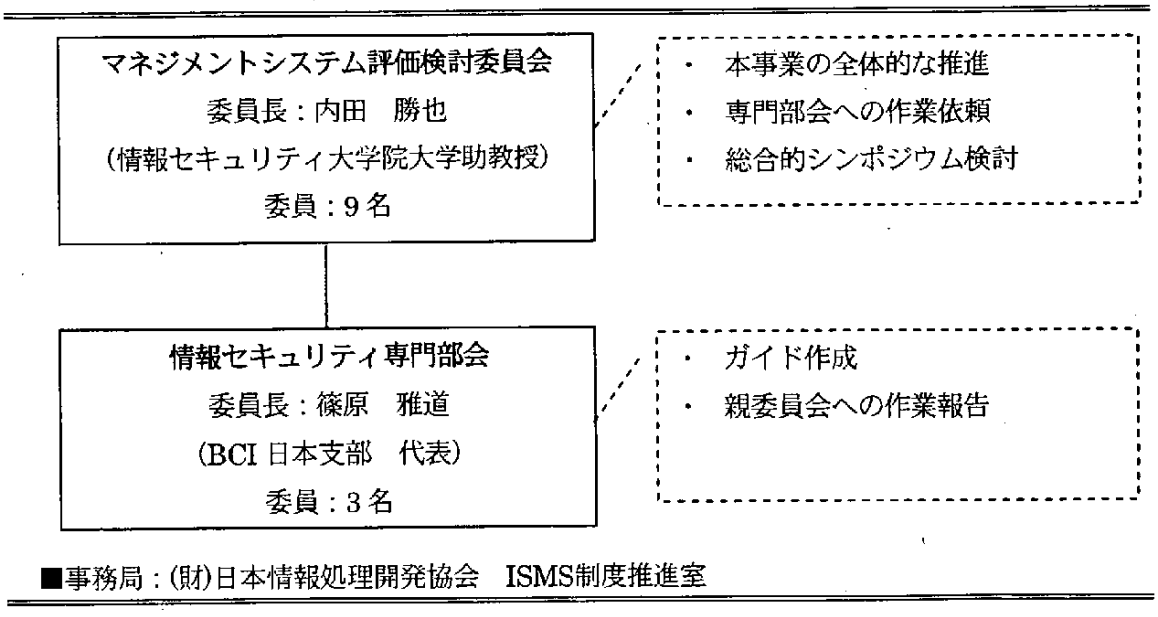


図1.1　検討体制

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

一	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

一	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	BT ジャパン㈱	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	2005.8.3	・実施計画について ・今後のスケジュール
第 2 回	2005.9.6	・事業継続に関するガイドについて ・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	2005.10.11	・事業継続に関する利用ガイドについて ・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	2005.11.22	・事業継続に関する利用ガイドについて ・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5回	2005.12.22	・事業継続に関する利用ガイドについて ・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	2006.1.26	・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7回	2006.2.16	・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8回	2006.3.9	・事業継続に関する利用ガイドについて ・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

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	2005.9.14	・事業継続計画に関する利用ガイドの策定（案）の検討
第2回	2005.10.25	・事業継続計画に関する利用ガイドの策定（案）の検討
第3回	2006.3.1	・事業継続計画に関する利用ガイドの策定の作業依頼
第4回	2006.3.17	・事業継続計画に関する利用ガイドの取り纏め

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）

－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：2006 年 2 月 1 日（水）9 時 30 分～17 時 30 分
－2 日目：2006 年 2 月 2 日（木）9 時 30 分～17 時 00 分

⑤ 会場

－大手町 JA ホール
東京都千代田区大手町 1-8-3

⑥ プログラム

■1 日目　2 月 1 日

時間	内容	講師
9:30～9:40	開会挨拶	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
9:40～10:30	基調講演 事業継続計画策定ガイドライン	経済産業省 商務情報政策局 情報セキュリティ政策室

10:30～10:40	休　憩	-
10:40～11:30	事業継続計画に関するガイドの利用ガイド	財団法人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
11:30～12:30	昼　食　休　憩	-
12:30～13:20	事業継続～重要な情報資産を守る～	富士ゼロックス株式会社 藤本　正代　氏
13:20～14:00	NIST SP800 シリーズに見る BCP と Contingency Planning	独立行政法人 情報処理推進機構 菅野　泰子　氏
14:00～14:10	休　憩	-
14:10～14:40	「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）の策定に ついて 」	(財)金融情報システムセンター 岡崎　洋治　氏
14:40～15:10	「BCM の実際：石油備蓄基地の国家戦略としての危機管理」＋BCM、BCP 雑感	日本セキュリティマネジメント学会 （JSSM） 岡安　邦男　氏
15:10～15:40	インターネットガバナンスと IPv6	(財)インターネット協会 （IA-japan） 高橋　徹　氏
15:40～16:00	休　憩	-
16:00～16:40	設備面からの事業継続	社団法人電子情報技術産業協会 （JEITA） 馬場　敬博　氏
16:40～17:20	BCM 国際規格の理論的支柱 －"BCI Good Practice Guidelines"の考え方	BCI 日本支部 篠原　雅道　氏
17:20～17:30	一日目のまとめ	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

■2 日目　2 月 2 日

時間	内容	講師
9:30～10:30	基調講演 情報セキュリティ人材育成の現場から	情報セキュリティ大学院大学 内田　勝也　氏
10:30～10:40	休　憩	-

10:40～11:20	保証型情報セキュリティ監査への取り組み	NPO 日本セキュリティ監査協会 （JASA） 原田　要之助　氏
11:20～12:00	過去の事件から学ぶ、個人情報漏洩の後始末	日本ネットワークセキュリティ協会 （JNSA） 山田　英史　氏
12:00～13:00	昼　食　休　憩	-
13:00～13:40	情報セキュリティマネジメントの重要性	財団法人日本情報処理開発協会 情報セキュリティ部 ISMS 制度推進室 室長　高取　敏夫
13:40～14:20	事業継続の観点から見た発生事象の傾向	JSOC 西本　逸郎　氏
14:20～14:30	休　憩	-
14:30～15:10	情報セキュリティ対策に関係する法律の紹介 （SOX 法、公益通報者保護法、ｅ文書法、プライバシー侵害）	情報ネットワーク法学会 （IN-Law） 佐藤　慶浩　氏
15:10～15:30	休　憩	-
15:30～16:50	パネルディスカッション 「事業継続とセキュリティ」	コーディネーター：内田委員長 パネラー：（順不同・敬称略） 菅野泰子氏、西本逸郎氏、原田要之助氏、馬場敬博氏、佐藤慶浩氏、篠原雅道氏、井上克至氏、高橋徹氏、等
16:50～17:00	閉会挨拶	財団法人日本情報処理開発協会 専務理事　三平　圭祐

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

479 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 479 名のうちアンケート回答数は、204 名（回答率：42.6%）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

「情報処理」が37%、「サービス」が21%、「コンサルティング」が13%であった。なお、その他の回答としてソフトメーカ、監査機関、広告、財団法人、卸売業、倉庫・運輸が挙げられている。

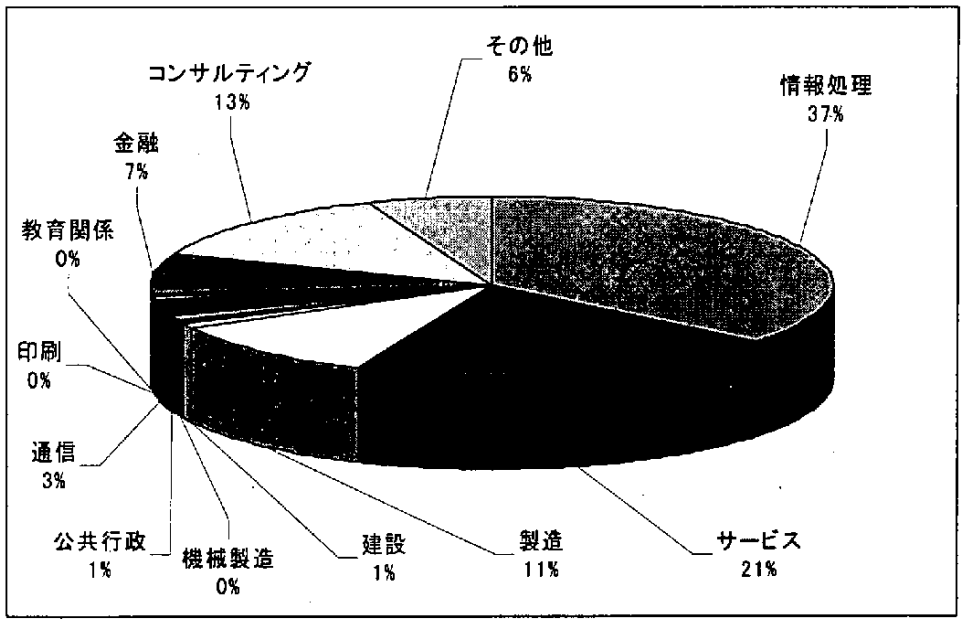


図 2.1 業種

②参加日

「両日」が53%と最も高く、ついで「2日目」が26%であった。

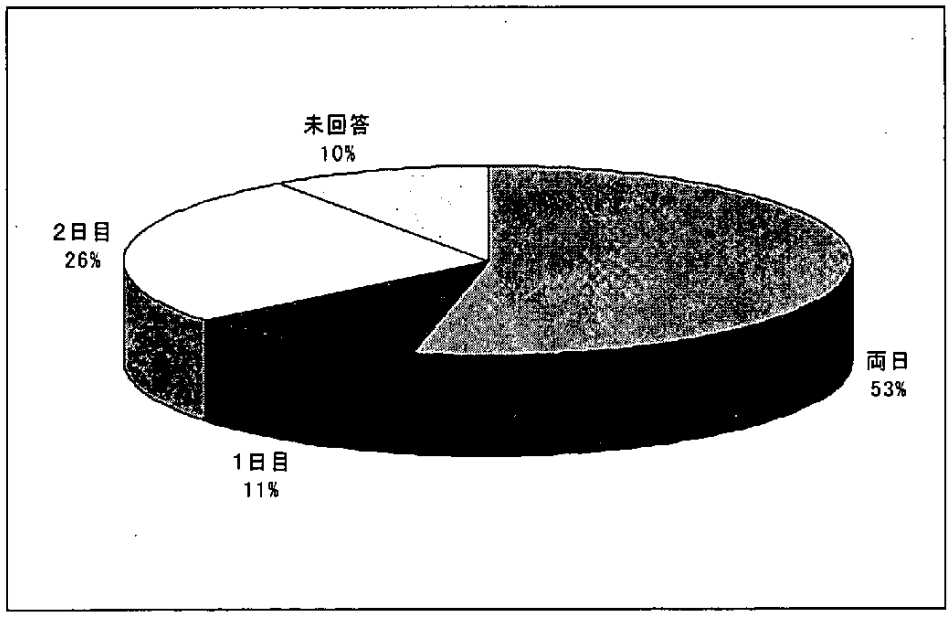


図 2.2 参加日

(2) あなたについてお聞かせ下さい。

①職種

「情報システム」が34%、「企画」が20%を占めている。

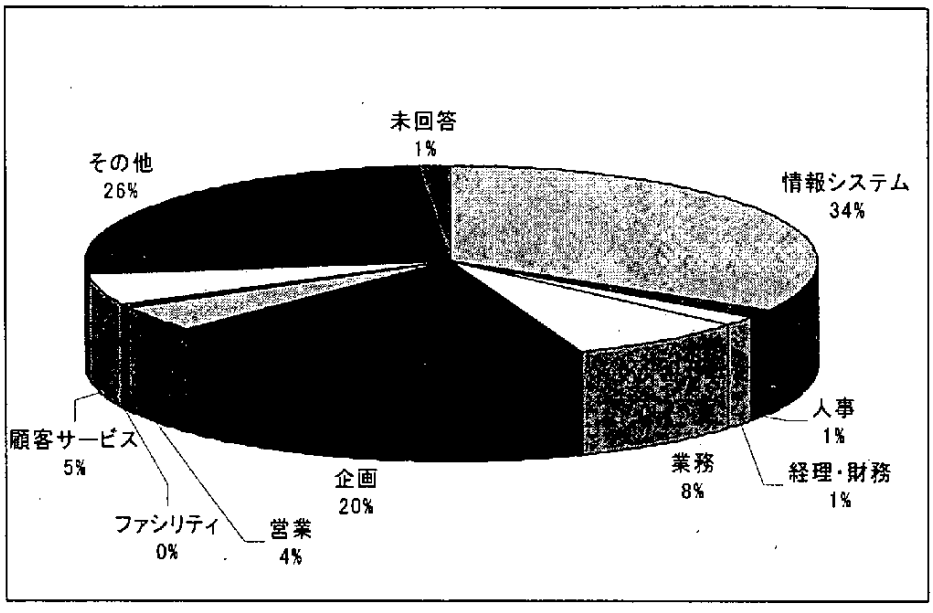


図 2.3 職種

その他の例：

監査(6名)、総務(2名)、ISO事務局(1名)、情報管理(1名)、システム監査(1名)、企業システムの監査業務(1名)、ISMS監査員(1名)、情報セキュリティ責任者(1名)、コンサルタント(1名)等

②役職

「管理職」が39%、「専門職」が27%である。

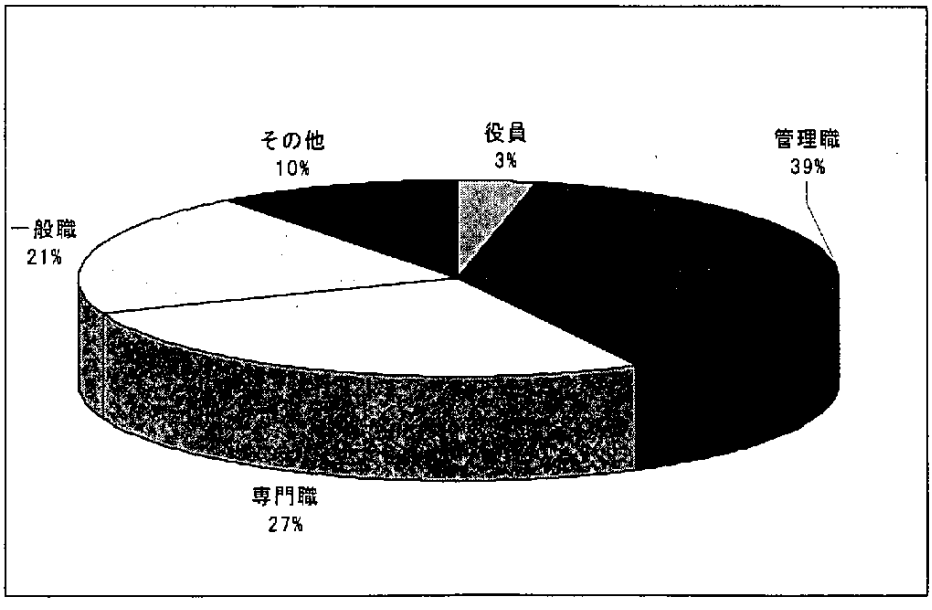


図 2.4 役職

③情報セキュリティに対する立場

「製品・サービスの購入／管理側」が36%、「製品・サービスの販売側」が29%である。

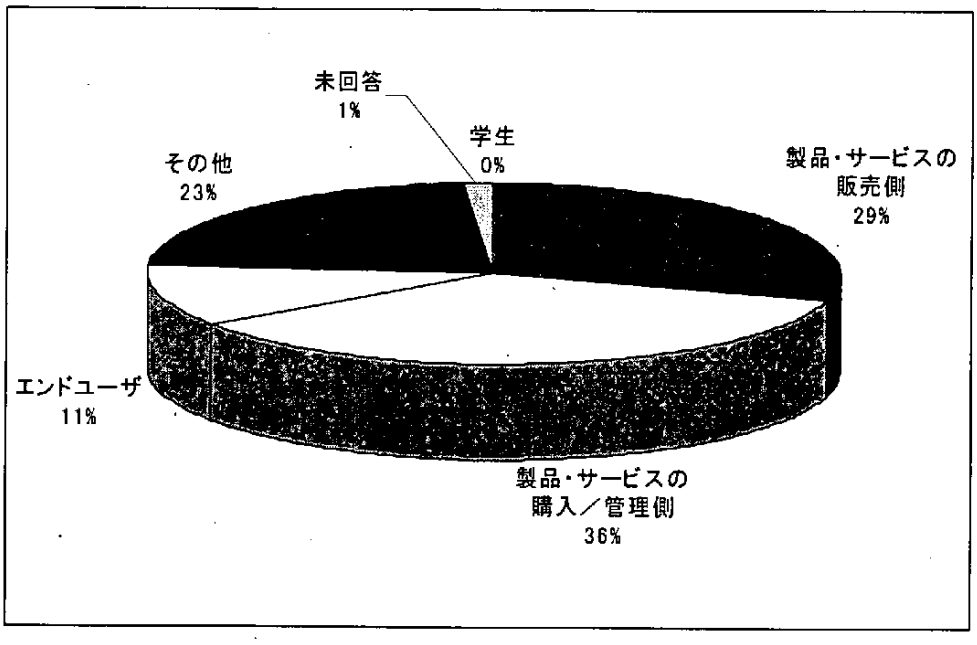


図 2.5 情報セキュリティに対する立場

その他の例：

情報セキュリティ責担当課長,内部監査、ユーザー指導、USMS 管理責任者、ISMS コンサルタント、セキュリティマネジメント、コンサルティング、教員

④本シンポジウムの参加目的

「情報収集」が72%と最も高い。

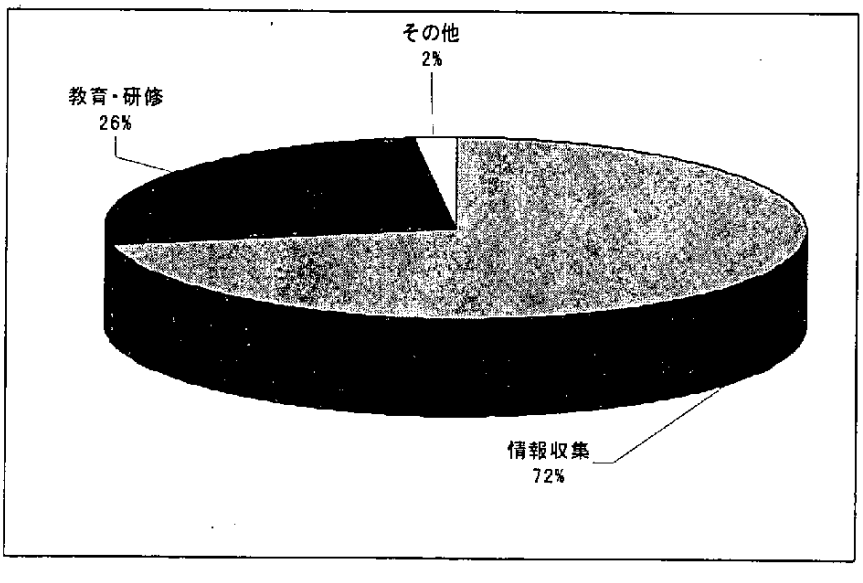


図 2.6 参加目的

(3) プログラムについてお聞かせ下さい

テーマの興味度合いや参考度合いについてアンケート調査した。なお、集計結果図にある番号 1～15 はタイトルを示している。(高 4→1 低)

1：事業継続策定ガイドライン

2：BCM に関するガイドの利用ガイド

3：事業継続～重要な情報資産を守る～

4：NIIST SP800 シリーズに見る BCP と Contingency Planning

5：金融機関等におけるコンティンジェンシープラン（緊急時対応計画）の策定について

6：BCM に関するガイドの利用ガイドの実際：石油備蓄基地の国家戦略としての危機管理

7：インターネットガバナンスと IPV6

8：設備面からの事業継続

9：BCM 国際規格の理論的支柱一"BCI　Good Practice　Guidelines "の考え方

10：情報セキュリティ人材育成の現場から

11：保障型情報セキュリティ監査への取り組み

12：過去の事件から学ぶ、個人情報漏洩の後始末

13：情報セキュリティマネジメントの重要性

14：事業継続の観点から見た発生事象の傾向

15：情報セキュリティ対策に関係する法律の紹介（SOX 法、公益通報者保護法、e.文書法、プライバシー侵害）

①テーマの興味度合い

タイトル 10「情報セキュリティ人材育成の現場から」についての興味度合いの累計が最も高く 186 である。

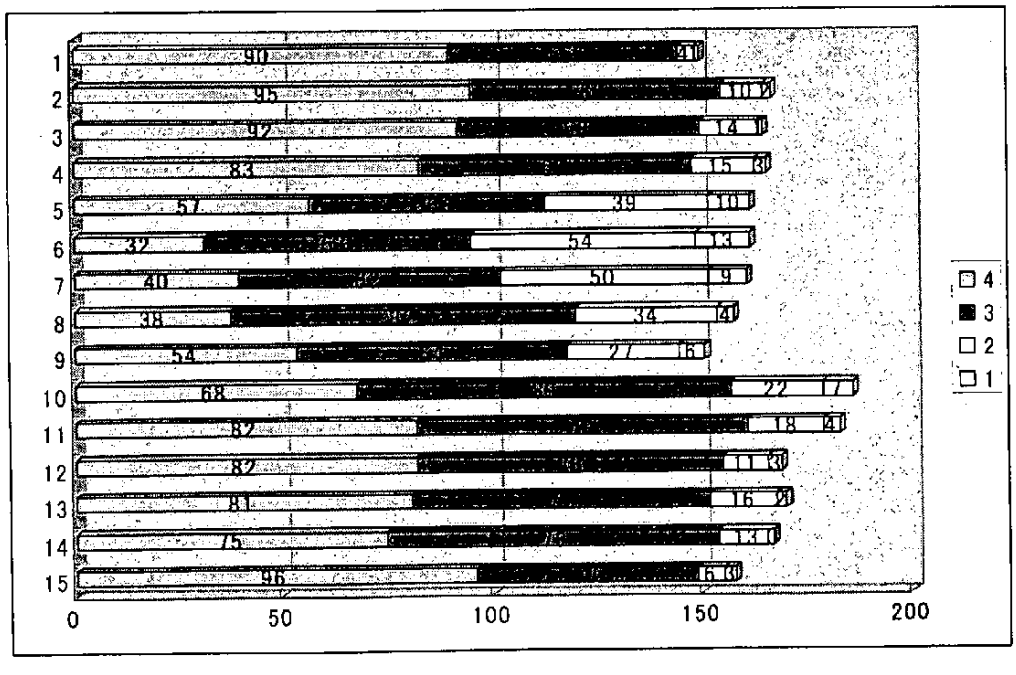


図 2.7 興味度合い

最も興味度合いが高いものは、タイトル 15「情報セキュリティ対策に関係する法律の紹介（SOX 法、公益通報者保護法、e 文書法、プライバシー侵害」の 17 回答であり、ついでタイトル 1「事業継続策定ガイドライン」、タイトル 5「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）の策定について」の 12 回答である。

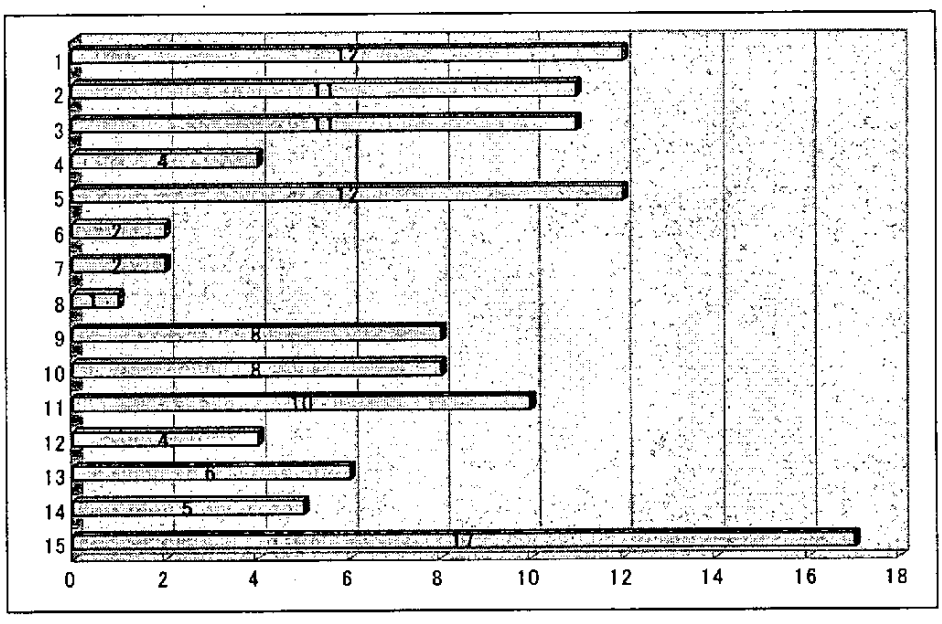


図 2.8 最も興味度合いが高かったテーマ

②テーマの参考度合い

タイトル 2「BCM に関するガイドの利用ガイド」についての参考度合いの累計が最も高く 153 である。

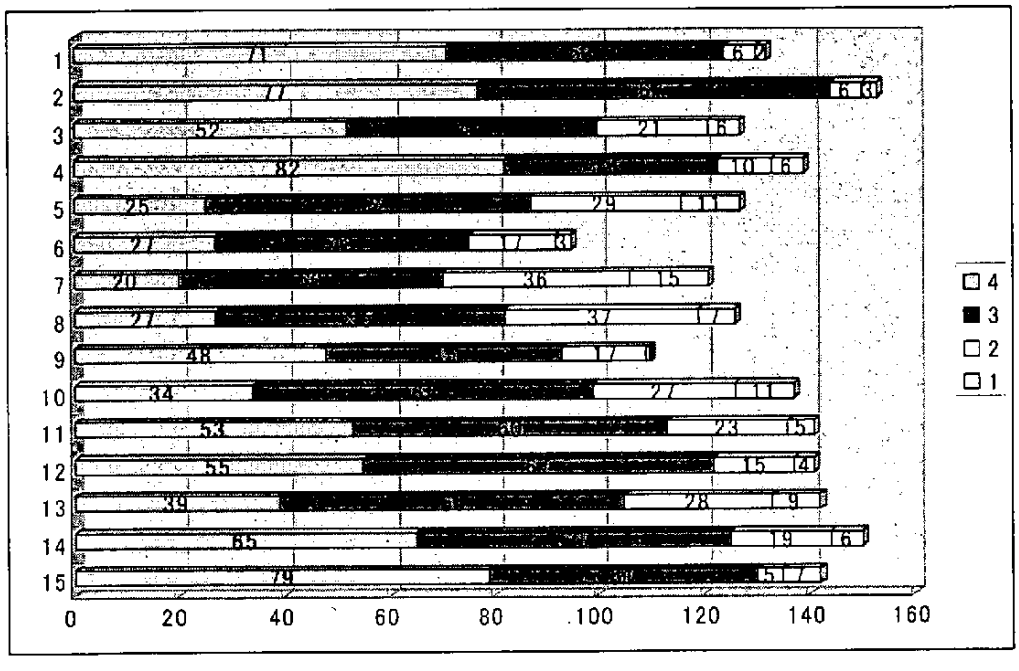


図 2.9 参考度合い

最も参考度合いが高いものは、タイトル 15「情報セキュリティ対策に関係する法律の紹介（SOX 法、公益通報者保護法、e 文書法、プライバシー侵害」の 21 回答であり、ついでタイトル 4「NIIST SP800 シリーズに見る BCP と Contingency Planning」の 12 回答、タイトル 1「事業継続策定ガイドライン」の 11 回答である。

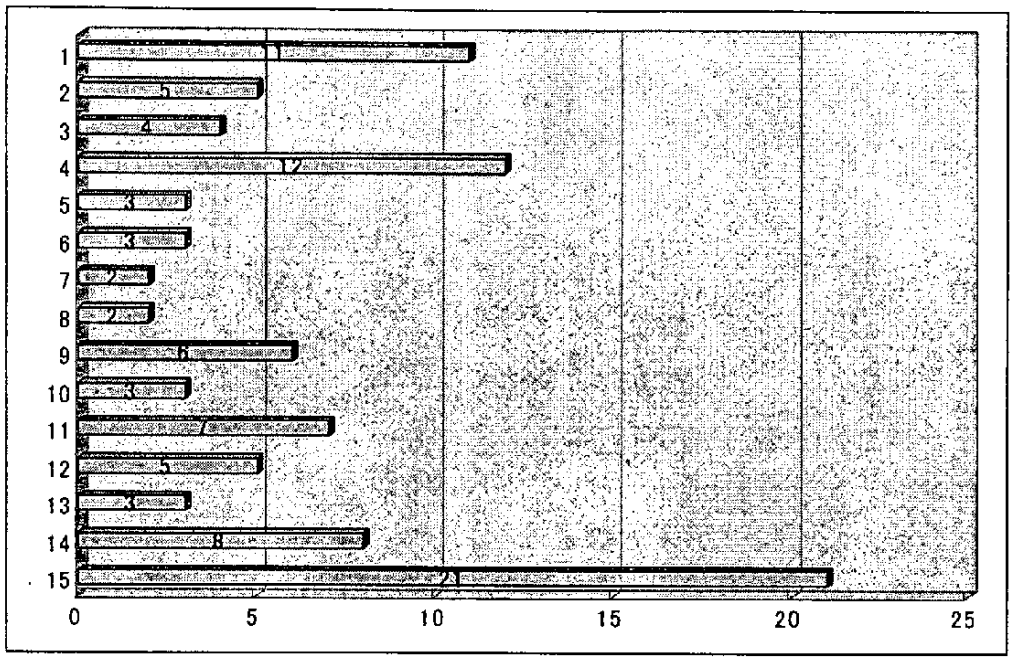


図 2.10 最も参考度合いが高かったテーマ

(4) 事業継続計画（BCP）についてお聞かせ下さい。

①御社の実施状況についてお聞かせ下さい

「策定中」が最も多く 54 回答で 26%を占めており、次いで「検討中」が 47 回答で 23%である。「実施している」は 42 回答で 21%である。（回答数：176）

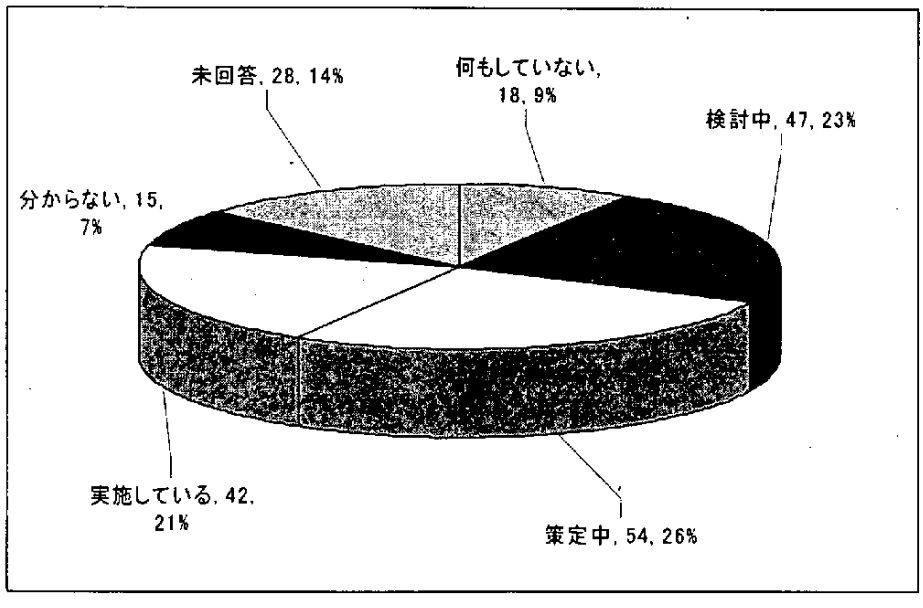


図 2.11 BCP の実施状況

②BCP の訓練を行っていますか

「実施していない」が 105 回答で 52%と約半数を占めている。(回答数：185)

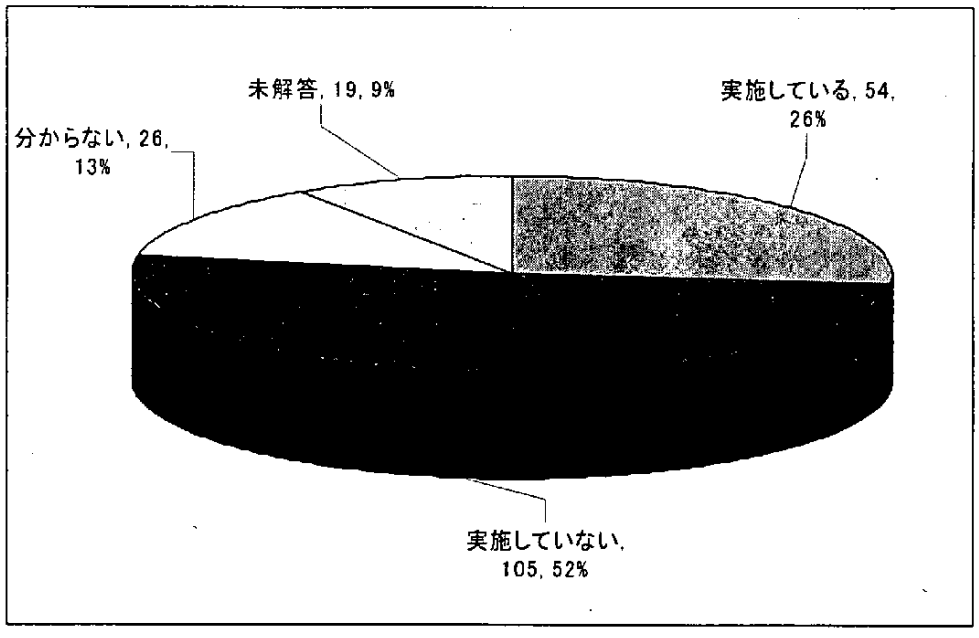


図 2.12 BCP の訓練状況

③BCP を策定する目的についてお聞かせ下さい

1	ISMS 活動の一環
2	顧客のニーズ対応
3	会社の信用維持
4	ISMS の要求事項であるため
5	取引先の要求（契約）
6	顧客のニーズ対応よりいっそうの信頼を得るため
7	サービス停止による顧客維持の回避
8	セキュリティ事故発生に対応することを目的に策定しているが、BCP 作成の経験を繰りかえし、BCM に沿った自社のポリシーを確立していきたい
9	アプリケーションデータを保存するため
10	情報セキュリティベンチマーク
11	情報セキュリティにおけるリスクの数値化（測定方法）手法
12	ユーザ側への提供
13	地震対策
14	ISMS の要求事項として BCP を行うのであれば、少しでも意味のあるものにしたい
15	リスク対応
16	事業を維持するため
17	緊急災害時などにおいて、人命、資産などの被害を最小限に抑え、ステークホルダーに対する絶対的な信頼を確保するため
18	組織（企業）としての信頼、ブランドを継続させるとともに、顧客優先、取引先の対応を実施するため。（もちろん社員の人命は最優先である。）
19	社会的責任、顧客重視
20	現在は、まだまだ不十分なので、よりいっそう充実させ、ブラッシュアップしていく。
21	災害、重大な障害発生時に自社のビジネスを守るため
22	情報セキュリティマネジメントの観点から不可欠と考えるため
23	BCP を策定し、マネジメントの質を高める事で、机上のアピールポイントとした
24	BS7799（ISMS）の記事を取得するため
25	リスクの予防策、企業価値の向上・維持・社会的変化
26	供給する人との完遂
27	製品・サービスを購入/利用されているユーザに対する義務として策定を推進中
28	BCP は大企業だけでなく製品を供給する全てに対して行われなければならない事から
29	災害時復旧がスムーズに行われ社会に混乱を起こさないため
30	企業の存続のため
31	競合、他社との差別化

32	非常時における統制のとれた復旧をステークホルダーに対するタイムリーな対応
33	受託システムを開発、運用している会社であり、危機管理は必要
34	単体のシステムがいくつも導入されるため、個別の問題となり、会社全体としての統制がとれない
35	ISMS 取得目的にあわせ、検討中
36	企業における事業継続保障事項の必須項目である
37	事業継続のため。出来ていないことの物の確認をそれに対するアセスメント実施
38	顧客に迷惑をかけないため
39	1、情報システムの稼動継続　2、データの保全　3、人的保全
40	企業体質強化
41	経営および情報セキュリティマネジメントに必要
42	当社は IT インフラをサポートする事業を行っており、その事業継続が社会的責任の最たるものとの認識のもと、事業継続の構えがなければもしもの時に適切な対応が取れないと考える
43	社の危機管理体制の一環として
44	お客様の業務を守るため
45	事業の継続性の維持
46	顧客ニーズ
47	事業部門内毎のサービス提供責任等
48	企業の発展
49	取り扱う情報が貴重であるため
50	災害を主体として、事件、事故等に対して事業の継続性を確保するため
51	顧客への影響を最小にすることをめざしている
52	ブランドの維持
53	顧客に提案するためのモデルケースとして
54	ISMS 維持
55	ISO27001 の要求事項
56	ISMS の要求事項として
57	ISMS 認定企業、アウトソーシング業でお客様の資産を預かり運用しているため、事業継続の対策が重要課題
58	ISMS 認証のため
59	予防、心構えをすること
60	事業経営におけるリスクの低迷、すみやかな事業開始
61	現状、何も策定されていない→企業として BCP 策定は当然
62	CSR のため
63	現在は、ISMS の認証取得部門が ISMS の ALL（事業継続管理）として実施しているが、会社として取り組むため
64	サービス利用いただいている顧客に迷惑をかけないこと。企業の存在のため
65	会社としても、ISMS の観点からも重要なため

66	ISMS の要求事項（事業継続）としてでなく、これは本来なら、顧客よりの要求でなければならない
67	特に個人情報の保護の見地から、消費者対応の強化や説明責任が増加しているから
68	ユーザ様の業務が最低限継続できるしくみの構築
69	防災対策
70	社会的ニーズ
71	顧客への製品供給責任を課す
72	クライアントの信頼を得ること
73	ISMS 認証取得（継続）及び企業継続の観点から
74	事業をいかに継続するか、スラークホルダーに対する責任をはたすか（取引先、社員、地域）
75	ガバナンスの一環
76	CSR のための一環として ISO/IEC27001 認証
77	社会的責任
78	品質マネジメント系認証（ISO）の取得をきっかけに、事業の安定推進を業務として顧客のデータを扱ってるため
79	ISMS 認証取得
80	サービスの継続顧客 CS 向上
81	事業を中断させるような事態に円滑に対応できるようにする為
82	情報資産の保護は当然ながら、企業責任の関係からもユーザ、取引先へ事業損害を与えない
83	万一事故が発生しても最上の対応をおこなえるよう BCP を策定し（特定資産に対し）訓練を行うことは重要と考えます
84	顧客サービスに対するサービスの安定供給
85	信頼性向上による他社との差別化

(5) その他

①今後も情報セキュリティ総合的普及啓発シンポジウムの開催を期待しますか

「はい」が82%と最も高く、今後の開催も望まれているといえる。

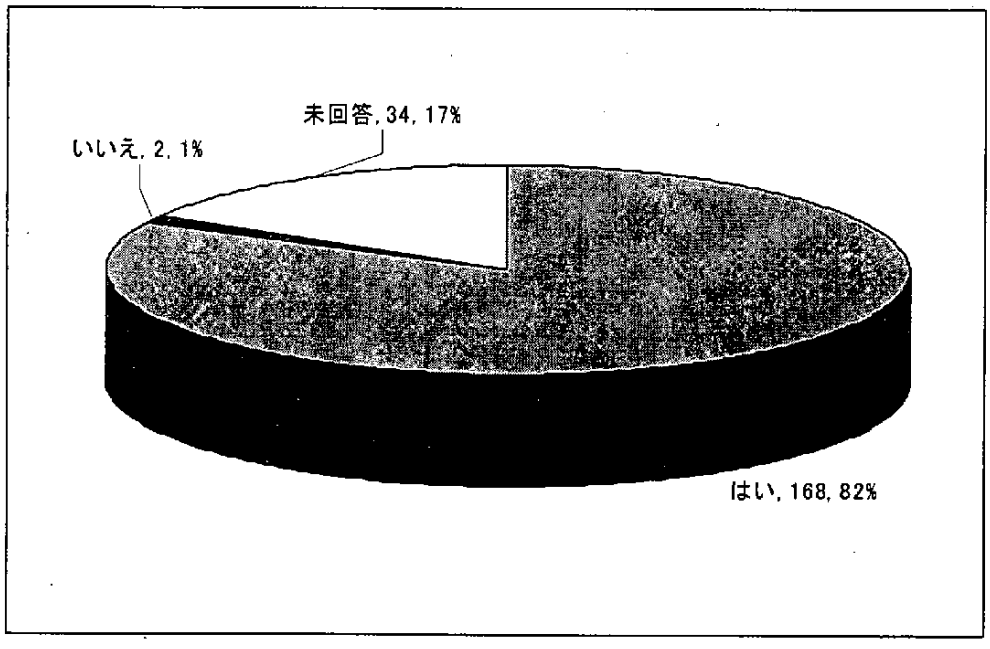


図 2.13 今後のシンポジウム開催希望

②今後取り上げて欲しいテーマをお聞かせ下さい

1	自然災害、地震に対する危機管理で成功例（国内 or 国外）
2	関連法律特集
3	BCP、BCM の導入事例
4	セキュリティ対策の解説　および各規格の解説
5	情報セキュリティベンチマーク
6	情報セキュリティにおけるリスクの数値化（測定方法）手法
7	情報セキュリティ監査と内部監査
8	システム、ネットワークを囲むリスク（攻撃手法、ウィルス）と対応策
9	日本版 SOX 法動向
10	J-SOX 法対応、IT インフラとの関係
11	情報セキュリティに係る実務に於いて、日本銀行のレポートは参考になるものが多いと思います。
12	日銀の専門家の多くの方のお話も伺えるとありがたいと思います。
13	ISMS の PDCA サイクルの中の"Check"に的を絞って、理論および実施の話を聞けると幸いです。
14	リスクの再評価、有効性の監視、内部監査、セキュリティレビュー
15	組織全員への情報セキュリティリテラシー研修
16	IT 技術とセキュリティについて、詳しく知りたいと思う

17	BCP の各社の具体的紹介
18	SOX 法、ITSMS、ISO27001、ISO9001、ISO14001、ISO22000
19	デジタルフォレンジック
20	セキュリティに関する事例発表等がすくないので、このシンポジウムに期待します。
21	SAS70、SOX 法、ISMS、個人情報保護など多岐に渡る規格をどうバランスさせ効率的に実施するか
22	グローバル企業（国内、国外）の取り組み事例の紹介
23	テーマの数を減らして、１つのテーマをもっと深く説明して頂きたい。
24	リスクアクセスメント、リスクの定量化
25	情報セキュリティとの関連法律
26	実地例等の実践が入った内容がもっと聞きたい
27	セキュリティに関する国際情勢など金融関係の BCP，BCM の実例
28	スパムウィルス対策、VCP の具体例
29	具体例な進め方と実例
30	紙ベースのもののセキュリティの考え方を知りたい
31	総合マネジメントの策定について
32	日本版 SOX 法の動向（傾向）
33	情報セキュリティの実証セミナー
34	規格
35	法令、ガイドライン変更時の総合的ポイント
36	今回のテーマの最新動向
37	セキュリティ監査
38	情報サービス産業におけるリスク評価
39	ISO27001
40	事業継続の実例
41	行政の各対策の実例
42	リスクの具体的定量方法
43	内容統制　　日本版 SOX 法対応
44	セキュリティコンサルの観点
45	e-文書法，個人情報保護法の法的観点
46	最新傾向、標準導向
47	情報セキュリティ対策導入の具体的実例
48	日本版 SOX 法への対応を情報セキュリティと会計の両面からアプローチ
49	BCM、BCP にテーマを絞り深く掘り下げて欲しい
50	ISO 対策
51	CSA
52	情報セキュリティガバナンス

53	特定はしないが、そのときに重要視されているテーマをタイムリーに提供してほしい
54	企業におけるリスクマネジメントの実態
55	ISO対策27001評価の実際
56	セキュリティ教育
57	BCMの実地例の紹介
58	BCMの実地例の紹介、具体実例
59	システム監査
60	利便性と機密保護の関係
61	内部統制のあり方（どこまで管理すべきか、性善説ではやっていけない）
62	現場上でのそれぞれのリスク対策など
63	情報セキュリティに関する人材育成
64	EU指令
65	情報セキュリティガバナンスの構築
66	ISO/IEC 27001への対応と実践
67	ITIL、ISMS、ISO27001、SOX法、ITSMS
68	個人情報のセキュリティ対策
69	リスクマネジメント
70	技術的な内容
71	情報セキュリティの総括管理方法
72	J-SOX法
73	ISO/IEC27000シリーズ概要（1日コース）
74	ISMS認証基準(Ver.2.0)との差分
75	メトリックス
76	効果の測定、評価
77	実例毎の対策、レベル別セキュリティ対策セミナー
78	法律との対応、どこまで対応したらよいかの判断
79	効果的な運用（事務局の苦労点）
80	情報法（ITサービス企業における法務対策）
81	セキュリティインシデントレスポンスの分析と対策
82	コーポレートガバナンスとBCP
83	リスクマネジメントと法律との関係
84	ＩＳＯ化
85	法規制最新情報（海外/国内）
86	デジタルフォレンジック　セキュアＯＳ
87	フォレンジック
88	ISMS　Dayとして、種々の論点から（Ｓｔｅｐ毎の重点事項や留意点）ご説明いただきたい

89	またリスク分析の実例も聞きたい。
90	ＪＩＳ２７００１、　内部統制
91	ＩＳＭＳ，ＢＣＭ　内部統制ーＩＴガバナンスー
92	ＣＳＲなど関連する事実を有機的に把えた講演をお願いしたい
93	日本版 SOX
94	アウトソーシングにとって必要なセキュリティの管理
95	ＩＳＭＳ、ＢＣＭ設備に際しての具体的内容について
96	内容統制と情報セキュリティ
97	フォレストシック（コンピュータ、ネットワーク、デジタル）
98	マネジメントシステム　認証、署名等
99	内部統制
100	ＩＳＭＳ内部管理策/17799:2005 のベンチマーク方法論
101	日本型経営上 ISMS の効果的推進方法
102	セキュリティの定着
103	情報セキュリティの安定性とそれに対する損失
104	コストミニマムの情報セキュリティ対策
105	SOX 対応の実例を踏まえたセミナー
106	そのときに応じた情報セキュリティに関する最新の情報
107	システム的（装置主体）情報セキュリティの専門手法
108	個人情報保護に関する具体的な対策

③その他、ご意見をお聞かせ下さい。

1	BCM に関する様々な観点からの講演を聴くことにより、BCM に関する全体像がかなり鮮明になった。
2	BCM の手法はよくわかったが、ISMS との関連をどうするかが課題
3	講師の方が時間を守らない、プログラムに無理があったのではないですか？参考にしてください
4	資料がきちんと用意されていない
5	2 日間は悪い。せいぜい一日。2 回にわけてもらってもよい。
6	最新の ISMS に係る検討状況を総合的に整理することができ大変有意義でした。
7	ありがとうございました。
8	会場の温度が低い（寒い）
9	クローク設置を希望します。貴重な情報ありがとうございました。
10	1テーマ一時間程の割り当てスケジュールで進行してほしい
11	テーマが多すぎる　パネルディスカッションの規定ができない
12	電子ファイルも資料があるといい
13	会場は都内でなくてよいので近県でもう少し広い場所で行って欲しい。
14	ディスカッションは必要ない

15	同じテーマを多人数で特定するため重複が多い。講演者を少なくしてもらったほうが集中して聞くことができる。
16	本会でいうBCPとはIT会社のBCPなのか、一般企業のBCPの中のITなのかまったくわからない。
17	配布資料、できればダウンロードできるようになるとありがたい。貴重な啓発の場ですのでぜひ継続してほしい。
18	机のついている会場でおこなってほしい
19	セミナーやシンポジウムの会場は記録をとったりするので、椅子席だけでなくテーブルを用意してほしい
20	ごく一部講演オーバーがあったものの、全体の進行が時刻とおりで気持ちいい印象でした。
21	講師の皆様が熱心にお話して下さり、問題の重要性が伝わり、認識できました。ありがとうございました。
22	会場のイスが狭い為、2日間大変疲れました。次回ご検討お願いします。
23	会場内が冷房がきいているのかわかりませんが、冷風がきて寒い。
24	できれば机のある会場で行ってほしい。
25	昼食時間が他企業と重なる時間は避けてほしい。
26	1日でもよいと思う。テーマの重複や「つまらないテーマ」を除くと十分可能でしょう。
27	ほとんどのテーマについて実例を紹介しながらわかりやすい内容で有意義なシンポジウムでした。
28	次回も参加したい。
29	非常に密度の高いシンポジウムでした。どうもありがとうございました。
30	今回の資料はあまりにも厚すぎる。2、3冊にわけてほしい。つかれきってしまう。
31	今回のシンポジウムは非常に参考になりました。
32	勉強になりました。ありがとうございました。
33	総合的普及啓発はタイトルがらはずしたほうがよいのでは？
34	終了予定時間に終了してほしい。
35	各テーマが全体のテーマの中でどの様な位置にあるのかを明確にして欲しい。
36	時間管理、資料の整備、音声の適正、会場案内など基本的なところでよく整備されていたと思います。
37	各テーマとも、とても退屈か知ってることばかり、というのがなく、全体的に平均化以上の水準でした。
38	欲を言えば、今回のように長時間の場合は新しい（イスが疲れにくい）会場だとありがたい。
39	説明内容に重複が多いのでもう少し整理していただきたい。
40	テーマと内容が異なるものがあります。できれば事前に精査していただければと思います。
41	実務経験から得た具体的な内容がよい。とても内容の濃いものでした。
42	東京以外の主だった都市でも開催していただきたい。
43	イスが狭すぎて窮屈。1日中講演を受けるには不適切と思われる。
44	インスタントにテーブルが出せるような設備のある会場を希望。
45	すでに実地されているかもしれませんが、今回のシンポジウムの動画配信
46	大変参考になった。会場設定もよかった。
47	メーカやマスコミ主催は規模の点と内容の点で限界があることが多いため、このような総合的なシンポジウムは今後も必要でしょう。
48	参考になりました。ありがとうございます。また参加させていただきたい。
49	資料がきちんと整備されていてよかった。

50	机のないホールで 1 日の研修は厳しい。もう少し、広いスペースと机を用意していただくか、内容を半分に絞りこんでほしい。
51	関東以外での開催。（地方にも広がって欲しい）

3. 事業継続の実際と今後の課題

3.1 情報セキュリティ人材育成の現場から

事業継続計画のお話ですが、最初に企業を取り巻くリスクについて考えてみたものです。実践「危機マネジメント」の資料に追加・編集したものがこのスライドです。

左上の労務リスクから始まり右上まで、企業を取り巻くリスクには多くのものがあります。一番上に情報リスクを書きましたが、情報システム自身が企業の基幹インフラストラクチャーになると共に、企業を取り巻く他のリスクに情報システムリスクが直接・間接関係してきます。各リスクに赤枠をいれましたが、これら全てが情報リスクに関連しています。情報リスクの１つが、関係していることもありますし、あるリスクが発生すると情報リスクに関係してくるものもあります。

地震の発生や台風の来襲は「災害リスク」であると同時に「情報リスク」にもなる可能性があります。また、ウェブから個人情報が漏洩すれば、「法務リスク」、「総務・広報リスク」や「財務リスク」にも関係する可能性があります。

このスライドを利用して、今回のメインテーマである事業継続計画を考える上で、ハイレベルの参考に使うこともにできるのではないかと思っています。

ただ、最近は「経営者に情報リスク、情報セキュリティについて、説明するのが大変だ」という話を、本学の学生（約７割が社会人ですが）とか、セミナー等の参加者から指摘されることがあります。そこで、このスライド使って、経営者を説得してはどうですかとお話をしています。

事業継続計画（BCP）を考えると必ず出てくるのは自然災害ですが、具体的にどんなものがあるかをまとめてみました。

最近は地球温暖化が言われていますが、１つは「集中豪雨」です。去年９月に東京・杉並地区で、１時間に 112 ミリ、総雨量で 264 ミリの雨が降り、ＪＲ阿佐ヶ谷駅近辺や南側を流れる善福寺川近辺で浸水被害がありました。　私はこの近辺に住んでいますが、たまたま犬の散歩で中央線のガード下を歩いていましたが、猛烈な雨でしたので、ちょっと心配をしていましたが、被害がでてしまいました。

それと、少し前になりますが、100 ミリを超えた雨が降って、実際に地下鉄に浸水があり、レールが水をかぶりました。その結果、地下鉄が止まりました。

2000 年９月に名古屋で集中豪雨がありました。「2000 年東海豪雨」と呼ばれていますが、画面右下の地図にありますように、名古屋の西側に新川と庄内川が流れていますが、この流域の西枇杷島地域の堤防が決壊し、名古屋の西側が冠水し、約２万 6,000 棟が床上浸水の被害を受けました。

水の被害を少し調べていますが、調べた限りでは、２万 6,000 棟以上が床上浸水したケースは、あまり多くありません。昭和 30（1955）年代等にはありましたが、最近ではこれが一番大きな

被害だと思います。もし、西側でなく、東側の堤防が決壊したらどうなるかを、数年前に名古屋に行った時に聞いてみたら、東側が決壊したら、名古屋の中心街で相当被害がでて、地下街や地下鉄に水が入ったのではないかとの話もありました。

温暖化の影響が寒冷化としてでてくることもあります。「北極振動」と呼ばれる現象があります。　今年の冬の日本海側は豪雪、太平洋側も3ヶ月予想に反して、厳冬になりました。世界規模で考えると、ヨーロッパやアメリカも寒かったようです。去年の12月に新潟市を中心に約65万戸の停電がありました。大雪で電線に着雪すると、その重みで電線が切れたためです。地球温暖化というと温度が0.2度とか、0.5度程度上がり、暖かくなると思っている方がまだ多いようですが、実際には熱帯型の季候になり、集中豪雨等が起こることになります。

これは、1993年に当時の建設省が、国が管理している主要10河川についてシミュレーションを行いました。前提条件は、200年に一度位発生すると思われる降雨量があり、それぞれの河川について、右岸・左岸の適当な場所で破堤があった場合、どこに、どの程度の被害がでるかを計算したものです。

東京を流れている荒川が破堤した場合に、最も大きな被害になることは想像できると思います。3日間に548ミリの降雨量、この雨量は、1947年に関東地方に来襲し、利根川が決壊した「カスリン台風」の3日間の総雨量446ミリを参考に決められたものですが、その場合に荒川が破堤した場合の被害で最大のものが、この図です。　下流から16.75Kmの右岸、×印がついていますが、赤羽近辺が破堤した場合に浸水深度がどの程度になるかを、2メートル以上を赤色、0.5～2メートルを黄色、0.5メートル未満を青で表示しています。荒川とＪＲ京浜東北線・山手線に囲まれた所は、ほとんど浸水被害が発生します。2メートル以上は、当然ながら3メートルも4メートルも2メートル以上です。最大の浸水深度では、6メートル近くだった記憶があります。

当時の建設省の試算では、被害総額は約38兆円、阪神大震災では約10兆円と言われていますので、約4倍の被害になります。

ただ、3日間で548ミリの降雨を前提としていますが、雨は当然この地区だけでなく、荒川の東側とか、山手線の西側とかにも雨は降ります。当然、この地区以外でも被害は発生します。東京直下型の地震の被害総額が110兆円と言われていますが、このシミュレーションに含まれない東京圏の被害を含めると、直下型地震とあまり変わらないと思っています。

火山の噴火では、1991年、あるいは1980年にフィリピン、アメリカで火山が爆発しています。今年は富士山に雪が少なく、噴火があるのではないかとの噂が流れました。　日本には非常に火山たくさんありますので、どこの火山が噴火しても不思議ではないと思います。　天明3年(1783年)に浅間山が噴火し、大きな被害がありました。　火山の噴火では直接的な被害もありますが、気候に影響を及ぼすと言った間接的な被害もあります。

地震については、中央防災会議を中心に色々な情報提供がされています。2004年のスマトラ沖の大地震とそれに伴う大津波も記憶に新しい所だと思います。

BCPで、自然災害でどこまで考えるかですが、「The Day After Tomorrow」という映画が少し前に公開されました。BCPでは、ここまで考える必要はないと思っていますが、この映画は荒唐無稽ではなく、地球温暖化によって、地球寒冷化、地球全体の気温が下がる可能性も十分あると

いう科学的知見を基に作られた映画です。

水の被害では、東京の例を示しましたが、地下道が浸水して被害がでた例が米国にあります。1992年4月1日、エープリルフールの日にシカゴで発生しました。シカゴに行った方はご存じだと思いますが、シカゴのダウンタウンにループと呼ばれる高架鉄道が走っています。そのループの下に地下道があります。図では赤い線で示しています。昔は暖房用の石炭を運ぶためにトロッコが走っており、この地下道は各ビルの地下と繋がっていました。現在はトロッコは走っていませんが、CATV ケーブル等がこの地下道に敷設されています。この地図では下のほうが東側で、ミシガン湖があります。当時、シカゴ川の改修工事が行われており、コンクリートパイルを打ち込んでいました。そのコンクリートパイルが原因で地下道にシカゴ川の水が漏水していました。一部の人が市に通報したのですが、市は放置し、ある日突然、4月1日ですが、シカゴ川の水が地下道に流れ込みました。

このため、地下道に繋がっているビルにも水が流れ込みました。約1週間と都市機能が麻痺しました。実際には、完全に正常な状態に回復するまでには数カ月かかったと言われています。シカゴには有名なシカゴマーカンタイル商品取引所がありますが、もちろんそこも停止しました。被害総額は、約 20 億ドルと言われています。金額的にはそれほど多い金額ではありませんが、こういうような被害も出ております。

スライド4で、東京での洪水シミュレーションがありましたが、このスライドをもう一度みていただきたいのですが、シカゴと同じ状況が発生したら、東京の浸水地域には地下鉄が走っており、一部のビルは地下道で地下鉄とつながっております。2 メートルを超える浸水深度になると地下鉄・地下街が水没する可能性があるのではないでしょうか？地下に水が入れば、それと繋がっているビルも浸水する可能性があると思っています。

「水が入るとどうなりますか」と言っているんですが、水は高いところから低いところへ流れます。当然ビルにもし水が入ると一番下の階から順番に水没をしていく可能性があります。「ビルの電源や飲料水はどこにありますか」と聞くと、大体地下3階とか、4階ですと回答があります。更に、電源のバックアップはと聞くと、「バッテリー使っています」ですね、多分都心部のビルでは、ほとんどバッテリーのバックアップです。そこで、更に、「バッテリーはどこに置いてありますか」と聞きますと、電源と同じ場所ですと回答されます。電源の供給がなくなると、高層ビルは勿論のこと、ある高さのビルでは屋上に給水タンクを置いていますので、そこまで水を上げることができなくなります。水が無くなるとコンピュータは死にます。

昨日も話がありましたが、現在のインターネットデータセンターでも、空調用に水を相当使っています。昨日の話では、1日約1トンというお話ですが、場合によってはそれ以上必要でしょうね。昨日の話は新潟地震でしたが、10年前の阪神大震災の時に、水の供給が無く、コンピュータを動かすことが非常に困難だった銀行があります。神戸が本店の銀行のデータセンターで、当時まだメインフレームでしたが、水の供給ができなくなり、コンピュータを動かすことができなくなりました。そのため、ビルの側面に穴を開けて地下にある給水タンクに給水車からその穴を通して、水を供給しました。10年前に地震でこのような問題が発生しています。事業継続計画を考える時に、コンピュータが置いてあるビルの環境を考え、対策を検討することは大切だと思っ

ています。

多分、中越地震の時よりは、阪神大地震の時の方がたくさん資料が残っているのではないでしょうか。私は阪神大地震の時には、神戸に行くことが出来ませんでしたが、当時、損害保険会社におりましたので、東京で調べられることは徹底的に調べたり、関西地区に住んでいた友人達からも情報を得て、地震がコンピュータにどの様に影響したかを調査し、報告書にまとめました。ただ、全てが分かった訳ではありませんでした。3～4年前になって、通信回線のケーブルが地下の洞道から、地上に上がる所で損傷があったと言う話を聞きました。この問題については、残念ながら、当時は分かりませんでした。

ただ、過去の問題を可能な限りきちんと調べておくことも非常に大切だと思っています。

自然災害のほかに、米国で、2001年に同時多発テロがありました。情報セキュリティあるいは、BCPを考える上で多くの教訓を残しています。

ただ、同時多発テロ以前のアメリカで発生した事件・事故は、少なくとも私が知っている限り、日本と少し異なった特徴があると思っています。

一つは、少なくともアメリカの大部分の地域、西海岸にはロサンゼルスとかサンフランシスコといった大都市近辺では、地震がありますが、東海岸のニューヨーク、ワシントンＤＣ等の大都市では地震災害はありません。また、米国南部は別ですが、少なくとも東海岸の大都市にハリケーンが来襲したこともありません。このことは、米国東海岸では、大規模な災害が起こった例がないということです。

米系銀行の東京支店に私が勤務していた頃ですから、多分80年代中頃だと思いますが、本店のあるニューヨークのビルの電源設備火災で、そのビルにあったデータセンターが運用できなくなりました。決済システム関係のオペレーションセンターで、処理ができなくなりました。外部のバックアップセンターとの契約がありましたので、即、対応する事は可能でした。

少し話題が外れますが、「日本では、米国のように電源設備からの火災はほとんど起こらない」と指摘される方がおりますが、1990年前後に、大手町にある外資系保険会社のビルで事故がありました。このビルは雑居ビルで、地下にあった電源装置の保守を行っており、最後の段階、多分、保守が終わり、通電した時だと思いますが、電源装置から発火し、保守要員が亡くなりました。月末前の日曜日で、翌日の月末の月曜日に、このビルは全館停電になり、業務ができなくなりました。

２つの外資系の東京支店がこのビルに入っておりました。１行は数ヶ月後に吸収合併される予定でしたので、近くにあった吸収する銀行の支店で、為替関係、いわゆるディーリング業務はそこでやりました。しかし、残りの１行はビルの裏にあるホテルに端末を持って行ってやろうとしましたが、回線の問題とかで処理ができませんでした。

ビルが火災で焼失したと言った事ではなく、ごく小規模の火災でしたが、人が亡くなるとそのビルに入館できなくなると考えておく必要があります。

話を元に戻しますが、コンピュータに関連する事故で人が亡くなったというケースはアメリカではほとんどありません。昔、70年代の中頃に『タワーリング・インフェルノ』という映画がありました、と言っても知らない方がもう随分いるのかもしれません。そのモデルになった高層ビ

ル火災が実際にありましたが、そのビルに入っていた銀行の事業継続計画が非常によく機能しました。そのことにより、その銀行の評判が高まったということがありました。このケースでも、銀行員はほとんど亡くなっておりません。

BCP で考えなければならないことは、人が亡くなった場合で大規模なものは、ワールドトレードセンターを中心とした同時多発テロが唯一ではないかと思っています。

同時多発テロでは、色々なことが起こりました。会社が丸ごと、従業員も含めて全部なくなってしまったとケースもあります。私自身が同時多発テロで一番気になっているのは、PTSD（心的外傷後ストレス障害）です。これは一般の企業ではあまり関係ないかも知れませんが、重要インフラ業種、金融機関、自治体、政府、病院、通信等で事業継続計画を考える場合、BCP で復旧作業を行う人達が、PTSD になってしまったら、どうしますかという話をしています。日本ではあまり、同時多発テロで PTSD の話がでてこないようですので、あえて私はこの話をしています。

PTSD は、かなり前から知られていますし、大地震が起こると PTSD になる方がおりますし、日本では、サリン事件で PTSD になった方がおります。

皆さん方が事業継続計画の中に、PTSD を考える必要がないのですかと問題提起をしています。

コンピュータ室にネズミが入ってケーブルをかじったといったことが昔の動物被害でしたが、最近は、鳥インフルエンザにような問題を考えておく必要があるのかも知れません。新しい伝染病の発生ですね。

鳥インフルエンザについて、少し調べてみました。少なくとも現時点では、鳥インフルエンザが直接人から人に感染することは確認されていないようです。ただ、これはいつ変わるかは分かりません。このため、鳥インフルエンザのようなものが人から人に感染することが起こった場合、どうするかを考える必要があるかも知れません。古い時代に、スペイン風邪で 4,000 万人死亡したとか、アジア風邪で３９万人が死亡したケースもありました。

インフルエンザの流行がどの様に起こるか、感染していくかをテレビで実験していましたが、くしゃみをすると 12 時間ぐらいインフルエンザの菌は残っています、というのをやっていました。インフルエンザのような感染病の大規模な発生は、大都会であればあるほど被害は大きくなります。

業務ミスの件で有名なのは、アンチウイルスベンダーのウイルス対策のパターンファイルに問題があり、コンピュータがハングというか、フリーズしてしまいました。一台一台のクライアントパソコンに導入するアンチウイルスソフトですから、企業によっては数千台、あるいは数万台導入されているパソコンに被害がでました。

この様な問題が発生する可能性もあることを今後とも考えておく必要があります。これも１つの事業継続計画の対象でしょう。

このため、このようなことを避けるためにどうすべきか、もちろん対策として考えておく必要があります。ウイルスあるいはワームというものの最近の状況を見ていると、アンチウイルスソフトだけで解決できません。

ベンダーを複数にするとかして、全部が停止してしまうことを避けることも考えられます。あるいは、ネットワークの構築を工夫することも大切になります。

即ち、１つの防御方法でネットワーク全体を守るのではなく、複数の方法での防御、いわゆる「Security In Depth」とか、「Defence In Depth」とか言われる「多重防御」を考えることも大切になります。

それから、11 月の東京証券取引所の事例では、大々的に報じられましたが、バックアップと本番システムが同一のソフトウェアを前提にしている場合には、ソフトウェアの問題でシステムが停止してしまうと、バックアップは何等役立たないことを明らかにしました。

サプライチェーンのような場合、他社の被害が自分のところにも影響してくることも十分あります。東京証券取引所のトラブルでは、証券会社、あるいは株取引の企業や個人も利用できなくなってしまいました。

この場合には、全てに影響がでましたが、サプライチェーンのような場合、取引ができるサプライチェーンとそうでないサプライチェーンがでる可能性があるかも知れません。

一般的には、一日未満のトラブルであれば何とかしのげるのではないかというような話もありますが、本当にそうなのか、もし競合他社が１時間程度で復旧した場合でも問題ないのかと言ったことも検討する必要があると思います。

昔、損害保険会社にいた時、「地震が起こっても多分損害保険会社のコンピュータは翌日に立ち上げる必要はないだろうね。１週間以上でも大丈夫かもね」というような話をしていました。現在はそれで問題ないかは分かりません。

ただ、計画した通りで問題ない企業・組織と、可能な限り早く立ち上げたほうがいいという企業・組織と色々あると思っています。

全体的には１週間程度でいいかも知れないが、ある業務は数日以内が望ましいと言ったこともありますので、どの程度の期間で立ち上げるのが望ましいかを考えておくことが大切だと思っています。

ただ、現在は問題なくても、来年になったら必要だということもありますので、定期的に見直しをする必要もあります。

今までお話した内容のまとめですが、日本では少なくとも大規模な災害でコンピュータ関係の人達が多数亡くなったケースはありません。

阪神大地震の前に、釧路で地震がありましたが、釧路に昔のお客様がおりましたので、被害状況を聞いてみました。当時のディスプレーは、液晶でなく、ブラウン管でしたが、相当数のディスプレーが机上から落下しまし、筐体（きょうたい）がひび割れたりしましたが、ブラウン管は一台も壊れなかったと言っていました。

ただ、今までの災害で、コンピュータ関係の担当者が亡くなることがないので、担当者が亡くならないという前提で事業継続計画を策定しているとしたら、再考の必要はあるのではないかと思っています。もちろん、PTSD になる事も考慮する必要があります。

それから、同時多発テロでは、ニューヨークでやっていた業務のバックアップを、テキサスのヒューストンでやるというケースがあったようですが、航空機は数日間、飛びませんでした。レンタカーを借りて行くのでも非常に時間がかかることがわかりました。

日本で東京の直下型地震が起こったら、羽田や成田空港は閉鎖されると思っています。少なく

とも民間は使えないことは考えておく必要があります。船をチャーターしてとか言っても港湾設備の被害がないかと言ったことも考える必要があります。

某業界では、「当業界は被災地には絶対行けるお墨付きをもっているから、必ず東京本社には行くことができるから問題ない」との話もあります。でも、大地震だけが、BCP の対象ではないことも考えておく必要があると言っています。

同時多発テロでは多くの資料がでていますし、ウェブでも相当あります。一度は調べておく必要があるのではないかと思っています。

大地震に関して、特に阪神大震災の場合、電気の復旧をかなり急いだとか。地震発生した後2時間か3時間後と記憶していますが、電気を入れたために火災が発生したと言われています。

今後、電力会社は、東京直下型地震や東海、東南海地震等が発生した場合、今までよりも十分時間をかけて電気の復旧を行うだろうと思っています。

電気が早期に復旧しなければ、例えば、1週間電源が入らないとしたら、短時間に回復できるかどうかも検討する必要があります。

一般的に言えば、大地震の発生後、3日後には自治体等も復旧に取りかかると言われてきましたが、電気の復旧がもし3日目だとしたら、今までの考え方で BCP の対応ができるかの検討も必要なのではないでしょうか。もちろん、「当社のコンピュータは1週間後の復旧で十分大丈夫です」であれば、大きな問題はないかも知れませんが。

それから、水に関しては前述しました。「コンピュータ、ソフト無ければただの箱」と言った人がいましたけど、「コンピュータ、水が無ければただの箱」とも言えます。もちろん電源もそうですけども、水が無いと駄目ということが意外と忘れがちです。中型クラスのメインコンピュータでしたが、空調が効かなくなって、部屋の窓や出入口を開けざるを得なかったという経験をしました。空調が効かないために部屋の温度が上昇し、コンピュータ室の窓や出入口を開けて、冷やしました。最悪段階に行く前に空調が復旧したため、大事に至りませんでしたが、真夏に発生していたらと思うと、ぞっとします。

最近のインターネット・データセンター（iDC）の多くは都心にあります。昔のメインフレームの時代には、少なくともバックアップセンターは自分のところから 40 キロ程度離れた場所に置くことになっていました。日本では地震があるので、40 キロ以上離れていれば多分大丈夫というものでしたが、iDCになって、緊急時には近い所にセンターがあった方が便利だとかで、多くの iDC は都心にあると言われています。 一部は関東地区あるいは関西地区というような形で分散しているケースもありますが、バックアップセンターはどこにあるかということを考えておかないと、動かなくなる可能性があると思っています。

参考に書きましたが、ガートナーグループが 2001 年に、40％の企業はコンピュータシステムへの大規模な災害が起こると生き残れないと言っていますが、これは事業継続計画を策定していない企業が大部分だと思います。

また、米国労働省が、災害を経験した企業の 43％は再開できなかったと言っております。更に、再開を果たした企業のうち 29％は 2 年以内になくなってしまったという結果がありますと言っています。

事業継続計画の策定が非常に重要であることを述べているのではないかと思っています。

「米国における情報セキュリティ」としてありますが、2001年に発生した米国中心の問題について述べます。

Code Red やNimdaと言ったワームの出現は、ソフトウェア、特にOSが中心ですが、それらのソフトウェアの脆弱性を放置してはダメで、パッチマネジメントを考えて対応できるようにしなさいというのが最初の層です。

9.11同時多発テロでは、重大な脅威を考えていなかった。事業継続計画、ＢＣＰを策定することが大切であると述べています。

そして、最後には、エンロン、ワールドコムの問題で、サーベンス・オクスリー法（ＳＯＸ法）に従って、経営者が内部統制を率先して行うことが大切であると言っています。

これはその時々の環境の変化、Code Red やNimida等のワームの出現や、同時多発テロ、エンロン、ワールドコム事件のようなものが起こるたびに、自分たちの考えている情報システムに対するリスクが変わってきているので、それらに対する対策を立てていく必要があります。2000年に考えたBCP、あるいは情報セキュリティ対策は、時間や環境が変化するとともに見直しが必要ですということを、この図は示していると考えることもできます。

環境変化を考えながら、事業継続計画の策定・維持を行っていただきたいと思っています。

先ほどのお話とも通じる所がありますが、今、情報セキュリティ大学院大学で、ISMSの講義をしていますが、ISMSや情報セキュリティでは一番重要なものの一つに監査という考え方があると言っています。

監査の考え方では、前述したように環境が変われば、その環境を考慮して行うことが監査だと言っています。

例えば、今、金庫室の中に金庫があります。金庫の鍵と金庫室の鍵が2種類あります。その時、支店長と次長がそれぞれの鍵をそれぞれが持っているという状況が規則で決まっていた場合、検査ではそのルール通りにやっていれば、問題なしになります。しかし、監査ではそのルール自体にリスクがないかをまず調べます。リスクがなければその規則通りやっているかを調べますが、リスクがあれば、それを指摘します、というお話です。

また、右下の図ですが、リスクの大きさは、情報資産、脅威、脆弱性のベクトルの大きさになります。これをRisk Cubeと言っています。

なお、ベクトルの大きさではなく、情報資産、脅威、脆弱性の3つの要素の掛け算ということもあります。

更に、もう一つ時間を考えて四次元にしたほうがいいんじゃないか、というようなお話です。

監査の考えを別の角度からみたものです。

ISMSでは詳細管理策と言われているものが、現在127項目ありますが、127項目を後生大事に持っていたらいけないんですよ、必要に応じて変える必要がありますよとISMSでは言っています。この考え方は非常に重要ですと説明すると「内田、そんなこと当たり前です。」と言われ、内田はなんてばかなことを言ってんだという顔をされることがあります。しかし、この問題を出して反論してくださいと言うとほとんど反論できません。

実際に某コンピュータ雑誌に掲載されていた内容です。ISMS の認証を取れば、個人情報保護法をすべてカバーできるなんて考えるのはおかしいと、その雑誌には書いてありました。本学の ISMS 受講生に初日の講義で質問をしました。今年度は 40 人近くの学生が受講しましたが、正解らしい回答をしたのは一人しかいませんでした。

セミナー等で同じ質問をしても回答した方は今まで一人もおりません。「ISMS の審査員は何人いますか」と質問するとそこそこ手が挙がりますがが、セミナー等だと分かっていても回答しないのかも知れませんが。

これに対する反論は簡単です。環境が変われば、リスクが変わるのであれば、ISMS の詳細管理策も追加できます。個人情報保護法に従った管理策を詳細管理策に追加すれば良いだけです。この記事は、雑誌に書いてあった内容で、本当に本人がこのような事を言ったかどうかは分かりません。BCP でも、環境が変われば、BCP 自身を見直していくことが大切だということになります。以下は宣伝です。今、本学ではこのような講座内容で授業をしております。可能な限りケーススタディ的なものを入れたりしています。受講生と一緒に議論をしたり、あるいはチームで議論をしながら、それぞれでどんなことを考えたかを発表していただいたりしています。

今年、始めて修士過程の人たちが卒業します。まだまだやることはたくさんあると考えていますが、今年から博士後期課程ができ、もう少し充実すると思っています。

修士課程では、平日２、３日と土曜日で修了できる体制になっているので、社会人が修士を目指しております。

最後のスライドの一番下に、アメリカの PITAC (President's Information Technology Advisory Committee) という大統領の諮問委員会が作成した報告書の中に「At U.S. academic institutions today, there are fewer than 250 active cyber security or cyber assurance specialists, many of whom lack either formal training or extensive professional experience in the field.」と書いてありました。

日本では、大学・研究所だけでなく、実務家を含めて、これに該当する人は何人いるだろうかなんて話を調査チームで話をしていました。10%いるだろうかなんて思っております。

ここからは、情報セキュリティや BCP が経営問題だとの認識を経営トップに自覚して頂く方法について、私なりの考えをお話したい思います。

情報セキュリティや BCP のように情報システム関係ですと、多くの経営者は「分からないから、任せる」と言われることが多いようです。私は分からなくても結構です、でも関心だけでも持って下さいと言っています。関心を持ってくれれば、そのものが見えてきますし、あるいは聞こえてきます。BCP や情報セキュリティでの最初の段階はそれが大切なのです。

某人材派遣会社のコマーシャルに、「西遊記編」と言うのがあります。情報セキュリティや BCP に、関心を示さない経営者にぜひ見てくださいと言っております。

東京証券取引所のトラブル等を見ていて感じるのは、あれは、アウトソースじゃなくて丸投げです。経営者は関心も示していないのです。アウトソースと丸投げは違います。BCP 等でも同じではないかと思っています。

---

[1] http://www.staffservice.co.jp/adreview/index.html

3.2 NIST SP800 シリーズに見る情報セキュリティと事業継続計画

3.2.1 はじめに

2004 年、2005 年は、世界的に大規模な自然災害が相次いだ年であった。日本は世界有数の地震国であり、かつ火山の噴火、相次ぐ大型台風、大雪による被害等、災害の爪あとが消える間もなく次々と大規模災害に見舞われている。このような社会情勢を受けてか、2005 年 3 月に、経済産業省より「事業継続策定ガイドライン」が発表され、2005 年 8 月に内閣府中央防災会議より「事業継続ガイドライン第一版」が発表されると、事業継続管理・事業継続計画に対して大きな関心が寄せられるようになった。なお、2005 年 10 月には、内閣府の「事業継続ガイドライン」の理解を助ける補足資料として「事業継続計画の文書構成モデル例 第一版」が発表され、2006 年 2 月には、中小企業庁より「中小企業 BCP[2]策定運用指針」が入門診断、BCP 策定のための様々なテンプレート、実際の策定例とともに発表されている。これらのガイドラインに共通するのは、事業継続計画への取組みをできるところからスタートさせることが重要であると呼びかけ、そのための枠組みや具体例を提示している点である。とりわけ、中小企業庁の指針や文書類は、中小企業が投入できる時間と労力に応じ、その企業なりの BCP が策定できるように細やかな配慮がなされている。

さて、経済産業省と内閣府から時期をほぼ同じくして出された事業継続策定ガイドラインは、BCP の基本的考え方や事業継続計画策定の枠組み設定に大きな違いは無い。また、両者ともその基本部分は、BCP の国際標準策定の動きを睨みながら、欧米の主要な BCP/BCM[3]ガイドラインの考え方を取り入れたものになっている。しかし、ケーススタディでは、経済産業省のガイドラインは、IT 事故を取り上げ、内閣府のガイドラインは（自然災害全般を視野に入れてはいるものの）地震を想定リスクとして BCP の取組みをスタートさせることを推奨している。

内閣府の取組みの核は防災である。そして、防災対策の歴史は古い。内閣府のパンフレット「わが国の災害対策(Disaster Management in Japan)」のなかの「災害対策の歩み」を見ると、防災法制度・体制整備への取組みの年表は、明治 13 年(1880 年)から始まっており、この年に、日本地震学会が発足している。また、災害対策の沿革（戦後）は、昭和 21 年(1946 年)の南海地震から始まり、総合的な防災体制整備の機運は、昭和 34 年(1959 年)の伊勢湾台風を契機として高まったとしている。一方、情報セキュリティ分野の事業継続の取組みは、防災ほどの歴史はないが、IT の始まりとともに芽生え、企業や社会への IT の浸透とともに、その取組みは進化している。

3.2.2 ISO/IEC17799 と NIST SP シリーズに見る情報セキュリティと事業継続計画

情報セキュリティにおける事業継続の取組みは、Contingency Plan（緊急時対応計画）や Computer Security Incident Handling（コンピュータセキュリティインシデント対応）として良く知られている。米国国立標準技術研究所（以下 NIST[4]と言う）は、情報セキュリティに関す

---

[2] BCP: Business Continuity Planning(事業継続計画)

[3] BCM: Business Continuity Management(事業継続管理=事業継続計画策定から導入、運用、見直し、継続的改善を含む事業継続のためのマネジメントを言う)

[4] NIST: National Institute of Standards and Technology

る様々な規格やガイドラインを策定し、発表しているが、1995 年に発表された SP[5]800-12 An Introduction to Computer Security: The NIST Handbook（NIST コンピュータセキュリティハンドブック）の第 11 章は「緊急事態や災害への備え」（PREPARING FOR CONTINGENCIES AND DISASTERS）であり、第 12 章は、「コンピュータセキュリティインシデント対応」（COMPUTER SECURITY INCIDENT HANDLING）を取り上げている。これらは、後年、一冊のまとまったガイドラインとなり、2002 年 6 月には SP800-34 Contingency Planning Guide for Information Technology Systems（IT システムのための緊急時対応計画ガイド）が、2004 年 1 月には SP800-61 Computer Security Incident Handling Guide（コンピュータインシデント対応ガイド）が、2005 年 11 月には、SP800-83 Guide to Malware Incident Prevention and Handling（不正プログラムインシデント防止・対応ガイド）が発表されている。

なお、情報セキュリティにおいて、事業継続という言葉が使われている代表例としては、情報セキュリティマネジメントの国際標準 ISO/IEC17799 が挙げられる。

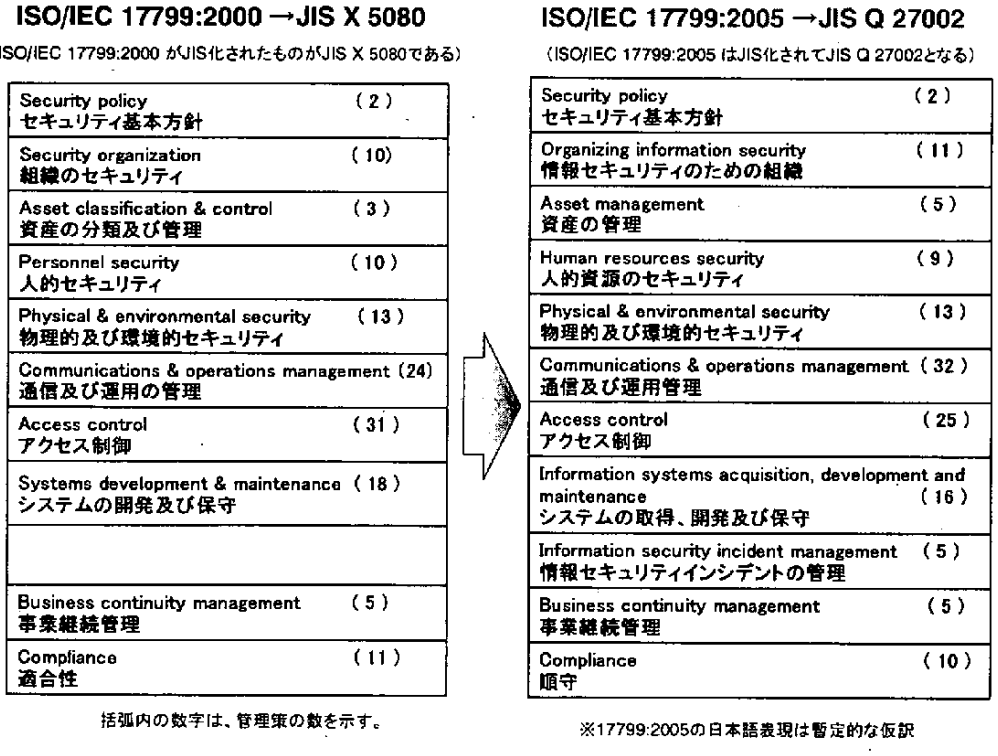


図 3.1　ISO/IEC17799:2000 と ISO/IEC17799:2005 の管理ドメイン

ISO/IEC17799:2000(2000 年発行)には 10 の管理ドメインがあり、9 番目のドメインが事業継続管理（Business Continuity Management）であり、ISO/IEC17799:2005(2005 年発行)では情報セキュリティインシデントの管理(Information Security Incident Management)という管理ドメインが 1 つ増えて管理ドメインが 11 になり、10 番目の管理ドメインが事業継続管理（Business Continuity Management）である。2000 年版と 2005 年版の管理ドメインの名称は事業継続管

[5] SP: Special Publications　NIST が発行する情報セキュリティに関するセキュリティ文書シリーズ。セキュリティ技術、セキュリティマネジメント等、幅広く網羅している。

理と変わらないが、その目的を見ると、微妙な（だが情報セキュリティと事業継続の関係からから考えると大きな）違いが見られる。以下に、2000 年版と 2005 年版より、事業継続管理のカテゴリ名及び目的に関する部分を引用する。

ISO/IEC17799:2000（JIS X 5080）より

> 11. 事業継続管理
> 11.1 事業継続管理の種々の面（Aspects of business continuity management）
> 目的：事業活動の中断に対処するとともに，重大な障害又は災害の影響から重要な業務手続を保護するため。
> 災害及びセキュリティ障害（例えば，自然災害，事故，装置の故障及び悪意による行為の結果）による中断を，予防管理策と回復管理策との組合せによって許容可能なレベルにまで抑えるために，事業継続管理手続を実施することが望ましい。（以下省略）

ISO/IEC17799:2005 より（日本語暫定訳）

> 14 事業継続管理
> 14.1 事業継続管理における情報セキュリティの側面
> （Information security aspects of business continuity management）
> 目的：情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに，それらから重要な業務プロセスを保護し，また，事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。
> 組織への影響を最小に抑えるため，及び予防的管理策と回復のための管理策との組合せによって，情報及び情報処理施設に関連する資産の損失（例えば，自然災害，事故，装置の故障及び悪意による行為の結果の場合がある。）を受容可能なレベルにまで回復するために，事業継続管理手続を実施することが望ましい。この手続では，重要な業務プロセスを識別すること，並びに運用，要員配置，資材，配送及び設備といった点で関連する，情報セキュリティ管理面以外の事業継続の要求事項と情報セキュリティ管理面の事業継続の要求事項とを統合することが望ましい。（以下省略）

2000 年版の事業継続管理にかかわる管理カテゴリは、Aspects of business continuity management（事業継続管理の種々の面）であり、2005 年版のそれは、Information security aspects of business continuity management（事業継続管理における情報セキュリティの側面）である。つまり、2005 年版では情報セキュリティ関連であることが明示されているのに対し、2000 年版ではそうは書かれていない。また、「目的」を比べると 2005 年版では、「情報システムの重大な故障又は災害の影響からの～」と始まり、情報システムにかかわる事業継続管理であることが強調されている。さらには、2000 年版（JIS X 5080）「11.1.2 **事業継続及び影響分析**」では、「業務手続の中断を引き起こし得る事象の特定と、リスクアセスメントには，事業資源及び手続の管理者が全面的に関与することが望ましい。このアセスメントは，すべての業務手続を検討

するものであり，情報処理施設に限定しない。」とあるのに対し、2005 年版では、同じ、事業継続管理の第 2 番目の管理策「14.1.2　事業継続及びリスクアセスメント」で、「事業継続に関するリスクアセスメントは，事業資源及び業務プロセスの管理者の全面的な関与のもとで実施することが望ましい。このアセスメントは，すべての業務プロセスを検討し，情報処理施設に限定しないことが望ましいが，情報セキュリティ特有の結果を含むことが望ましい。」（下線筆者）とある。2000 年版では、組織の全てのビジネスプロセスを対象とした事業継続管理であるのに対し、2005 年版では、事業継続における情報セキュリティの側面を強調しようとする意図が感じられる。

3.2.3 BCP と Contingency Planning[6]（緊急時対応計画）の違い

平成 17 年 3 月付けの INTAP の報告書「平成 16 年度ビジネス継続性技術調査報告書」には、次の記載がある。「現在利用可能なビジネス継続マネジメントのベストプラクティスにはいくつかの方法が存在するが、多くの組織が依然として狭義の対応を行う情報技術の災害復旧（ITDR[7]）とビジネスの復旧、回復、及び計画に必要な情報を提供するだけの官僚的なアプローチのみにフォーカスし続けている。これは、対処的で予防的、更に組織、場合によっては業界全体がリードする包括的かつ統合された広義のビジネス継続マネジメントのプロセスとは対照的である。ビジネス継続マネジメントをビジネスの原動力となるプロセスとして捉えた場合、ITDR 及び復旧計画は、効果的で目的に合ったビジネス継続マネジメントの適合性と実効性を通して組織・業界の耐障害性（レジリエンシー）を推進及び提供するプロセス上の重要な要素として位置づけられる。」

情報セキュリティ（または IT）の世界で推進されてきた事業継続の取り組みは、ITDR（IT 災害復旧計画）であり、IT 緊急時対応計画（IT コンティンジェンシープラン）である。本来、事業継続の取り組みは、すべての業務プロセスを検討し全社的に行ってこそ意味があるものであり、IT に該当する部分でだけ行うものではない。ただ、BCP に関する取り組みが注目されてきたのは、ここ数年のことなので、それまでは、防災は防災のガイドライン、IT は IT 事故対応のガイドラインを策定してきたのも無理からぬことではある。

経済産業省の「事業継続策定ガイドライン」は、INTAP の報告書と時を同じくして発表されているのだが、それは、ケーススタディこそ IT 障害を取り上げているが、その内容は、広範なビジネスを対象とした「事業継続計画」そのものである。この報告書から 1 年たった 2006 年 3 月現在では、「多くの組織が依然として狭義の対応を行う情報技術の災害復旧（ITDR）とビジネスの復旧、回復、及び計画に必要な情報を提供するだけの官僚的なアプローチのみにフォーカスし続けている。」という状況は、もはや鳴りを潜めている。むしろ、「コンティンジェンシープラン」などと言おうものなら、「それは、（事業継続ではない）単なる緊急時対応計画ですね」と言われかねない局面さえある。

だが、事業継続計画と緊急時対応計画はどのように違うのだろうか？そしてまた、情報技術の災害復旧（IT Disaster Recovery）と緊急時対応（IT Contingency Planning）はどのように違うのだろうか？事業継続計画に関連する計画は数多く存在する。「事業継続計画（BCP）」「緊急時

---

[6] Contingency Planning: 緊急時対応計画、コンティンジェンシープラン
[7] ITDR: IT Disaster Recovery　IT 災害復旧

対応計画（Contingency Plan）」「災害復旧計画（Disasters Recovery Plan）」「インシデント対応計画(Incident Response Plan)」などは、馴染みのある言葉である。ところが、これらの計画の共通点は何で、異なる点は何で、どのように相互に関連しているか、となると、明確に分類、整理しているものが少ないように思う。経済産業省の「事業継続策定ガイドライン」では、BCP と Contingency Plan の違いを次のように説明している。以下に該当する部分を引用する。

「BCP と CP（コンティンジェンシープラン）との違いは、想定できるインシデントに対して、発生した場合の対応計画をあらかじめ策定しておくことは同様であるものの、BCP は事業の継続性の観点から事項、手順、体制、資源等の計画を具体化したものであると言える。また、CP は緊急事態発生直後の行動を中心とした計画であるのに対し、BCP は事前にビジネスプロセスの脆弱性を分析（ビジネスインパクト分析）した上で、それに基づいた計画を実施することに特徴がある。」

つまり、BCP は、ビジネスインパクト分析をした上で、コアとなる事業をいかに継続させるかという事業継続により焦点があてられているのに対し、コンティンジェンシープラン（緊急時対応計画）は、緊急事態発生直後の行動を中心とした計画であるという説明である。しかし、NIST SP800-34 の「IT 緊急時対応計画」[8]を見ると、計画を立てる際には、ビジネスインパクト分析から始まり、その手順は、BCP における手順と大きな違いは無い。強いて言えば、それは呼び名の違いであるとさえ思えてくる（もちろん、ビジネス全体に焦点をあてる BCP と IT に焦点をあてる IT 緊急時対応計画には明確な違いがある。それについては後述する。）

同じ経済産業省のガイドラインでは、<2001 年 9 月 11 日 同時多発テロの対応>として、以下の事例が紹介されているので引用する。

「世界貿易センター地域に所在していた金融系会社が、最重要拠点を失ったにもかかわらず危機的状態を見事なまでにくぐり抜け、9,000 人以上の従業員を無事に避難させたばかりか、その翌日からその拠点にあった事業の一部を他の場所で再開した。この会社は、自社の業務状況・リスク状況を分析(ビジネスプロセスの脆弱性分析)に沿って BCP を策定し、BCP のトレーニングを効果的に実施してきた。この BCM の過程では、あらかじめ、どの業務を国内外のどこの拠点に移すことができるか、さらにどの従業員をどの拠点に移すかについて検討をしていた。また、経営層の BCM に対する理解が会社内での BCM 推進に大きな役割を果たしたことは言うまでもない。」

これと同じ事例と思われるものが、「企業経営における IT 事故対応に関する調査研究報告書」(2004 年 3 月 ㈱インターリスク総研(経済産業省委託調査)の中で、「第 4 章、4.3 メリルリンチ社」の事業継続の取り組み事例として紹介されている。(http://www.bcijapan.jp/documents/BCM_survey.pdf) この報告で使われている名称は、事業継続の責任者は「グローバル災害計画担当役員」であり、事故が起こった時に動くのは、「全社緊急時対応チーム」であり、災害復旧に威力を発揮した強力なデータベースの名称は、「災害復旧計画システム」である。ここで何を言いたいかと言うと、名称に惑わされてはならないということである。同じ事業継続計画と言っても、それは、内容を確認してみると、IT 事故を対象とした IT 緊急時対応計画の性格をもつものかもしれないし、全社を対象とした事業継続計画である

[8] 正式名称は、NIST SP800-34 Contingency Planning Guide for Information Technology Systems (IT システムのための緊急時対応計画ガイド)。本稿では、以下「SP800-34 IT 緊急時対応計画」又は、SP800-34 と称する。

かもしれない。そして、その反対のケースもあるのである。

視点を変えてみよう。では、ISO/IEC17799 では、管理ドメインの名称をなぜ「事業継続管理」とし、「緊急時対応計画」としなかったのか？情報セキュリティの三要素は機密性、完全性、可用性であるが、「事業継続」は可用性にあたる。そして、管理ドメインの名称を「事業継続管理」としたのは、「可用性」という言葉の背後にある「何のための可用性か？」という目的を強く意識しているためと考えられる。情報システムをいつでも「用いること可」の状態にしておくのは、まさに、ビジネス存続のために必要だからである。また、その名称を「事業継続管理」として「事業継続計画」としなかったのは、BCP を策定し、導入し、運用し、見直すというマネジメントサイクルで考えているからである。IT が社会・経済・政治に深く浸透している現在、IT の関与しないビジネスプロセスは、むしろ少なくなっており、事業継続計画に IT が関与する範囲が拡大しているという事情もある。また、相次ぐ天災により、事業継続が求められるという社会背景がある。例えば、日本では、2004 年 10 月 新潟県中越地震の際に、被災地に製造拠点を置く取引先や子会社などが被災し、サプライチェーンが途絶えたことで親会社や取引先の事業継続に影響が出たケースがあり、CSR の観点からも事業継続管理が求められるようになった。しかも、IT システムの中断がビジネスの中断に直結するという局面も少なくないので、「情報システムの重大な故障又は災害の影響からの事業活動の中断に対処する」一連の活動を「(情報セキュリティにおける) 事業継続管理」と言うのは、時代の趨勢を捉えている。

一方、NIST の様々なガイドラインを読むと、組織のミッションを遂行するために、IT や情報セキュリティがあるという目的意識は明確である。それなのに、NIST SP800-34 IT 緊急時対応計画では、なぜその名称を「IT 緊急時対応計画」とし、「事業継続管理」としなかったのか？ NIST SP800-34「2.2 計画の種類」には、次の記載がある。「一般には、IT 緊急時対応計画とその関連計画領域の定義として、普遍的に受け入れられているものは存在しない。このような定義が存在しないことで、各種の計画の実際の範囲と目的を考える際に、混乱が生じることがある。本項では、IT 緊急時計画に関する共通理解の基盤を提供するため、その他の種類の計画をいくつか特定し、IT 緊急時対応計画と比較してその目的と範囲について説明する」。SP800-34 では、計画の種類として、以下の 8 つの計画を挙げ、定義し、その相互の関連について言及している。

- 事業継続計画 (BCP: Business Continuity Plan)
- 事業復旧 (再開) 計画 (BRP: Business Recovery (or Resumption) Plan)
- 運用継続計画 (COOP: Continuity of Operations Plan)
- サポート継続計画/IT 緊急時対応計画(Continuity of Support Plan/IT Contingency Plan)
- 緊急時コミュニケーション計画(Crisis Communications Plan)
- サイバーインシデント対応計画(Cyber Incident Response Plan)
- 災害復旧計画 (DRP: Disaster Recovery Plan)
- 人員緊急時計画 (OEP: Occupant Emergency Plan)

ここでは、「事業継続計画」の対象範囲は「ビジネスプロセス」と定義され、IT が事業継続計画の対象範囲となるのは、ビジネスプロセスのサポートに IT が関与する場合としている。また、IT 緊急時対応計画は、IT システムの中断を対象とし、ビジネスプロセスに焦点をあてているわけで

はない（not business process focused）、とある。NISTがその文書の名称を「IT緊急時対応計画」とし、「事業継続管理」としなかったのは、それは、この定義に照らし、SP800-34がIT緊急時対応計画を扱ったものであり、事業継続計画を扱ったものではないからである。ここで誤解を避けるために言うと、not business process focusedというのは、責任範囲を明確にしているだけなのであり、ビジネスプロセスを重視していないわけでは無い。「情報システムは通常、ビジネスプロセスをサポートする。しかし、ビジネスプロセスは情報システムに関係しない、他の多様なリソースおよび機能にも依存する」(SP800-34より)ため、IT以外の他の多様なリソースおよび機能に関しては(業務分掌外または権限が無いため)立ち入らないのである。後述するが、IT緊急時対応計画の策定では、最初の段階で事業影響分析を行い、まず、重要なビジネスプロセスを特定し、そのプロセスを動かしている重要なITリソースと関連づけ、そのITリソースが中断した時の影響と停止許容時間を判定した上で、復旧優先度を決定していく。ITはミッション遂行のためにあるのであり、そのために、ITのかかわるビジネスの優先度決定が重要になるのである。もうひとつ大事なことは、SP800-34では、緊急時対応に関する諸計画策定、更新の際には、各計画間の連携を取ることが重要であるとも述べられている点である。つまり、IT緊急時対応計画は、事業継続管理の中の重要な要素として位置づけられており、また、それゆえ、各計画間の整合性を取ることが必要になるのである。このスタンスは、昨年12月に内閣官房情報セキュリティセンターより公表された、「政府機関の情報セキュリティ対策のための統一基準」の「6.3.2 事業継続計画(BCP)との整合的運用の確保」の各項の記載と近い(http://www.bits.go.jp/active/general/pdf/k303-052.pdf)。

3.2.4 参照モデルとしての緊急時対応に関する諸計画の相互関係図

NIST SP800-34では、上の項で述べた、8つの緊急時対応関連の諸計画の相互関係を図示している（図3.2参照)。この図は、計画の相互関係のみならず、どの計画がビジネスプロセスに関与し、どれがIT関連の計画であるか、そして、特に重要な計画が何かも示している。なお、この図を見て、これら全ての計画を策定しなければならないと読んではならない。この図は、優れた分類・整理学を提供しており、各計画が互いの位置づけを理解するための参照モデル（Reference Model）として使える。例えば、ここにあるガイドラインがあるとする。そのネーミングがどうであれ、内容がこの図のどの計画にあたるかを見ていくことで、その計画なりガイドラインの性格が浮き彫りにされる。また、自社の事業継続関連の計画を作る時にも、自分の会社がどの計画をつくろうとしているかの理解を助けてくれる。自社の規模、ビジネスプロセス、想定する事故や災害に応じて、策定すべき緊急時対応関連の計画はそれぞれに違うであろう。自社にとって、どのような種類の計画を策定するのが妥当であるかを考える時、この図は、自社の計画の位置を知らせてくれる。

なお、NIST SP800-34　2.2 計画の種類には、「最終的には、組織は一連の計画を使用して、組織のITシステム、ビジネスプロセス、施設に影響を及ぼす中断に対して対応、復旧、継続の準備をする。」との記載があるが、これは、全ての計画が必要と言っているのではない。この部分の英語の原文は、"Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's IT

systems, business processes, and the facility."(下線筆者)である。下線の部分が shall でも should でもなく would なのは、そういう意味である。ちなみに、最近、SP800-34 の著者の一人である NIST の専門家と話す機会を持ったが、この図を参照モデルとして使うことが可能であること、また、NIST の推奨するセキュリティ管理策においては、事業継続に関する計画として、IT 緊急時対応計画を必須としているのであり、あとの計画はケースバイケースであるとのことであった。

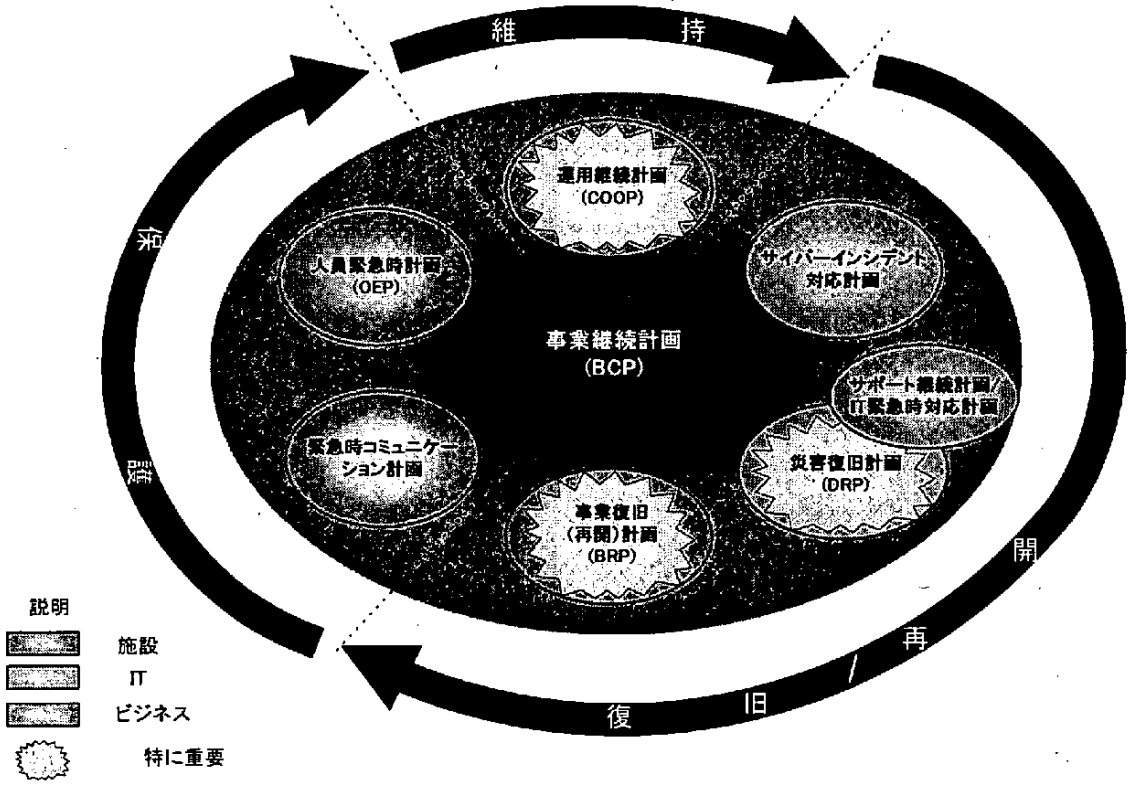


図3.2 緊急時対応に関する諸計画の相互関係図

この図で、事業継続計画が中央に陣取っており、各種計画と重複する部分がある点に注目したい。この図から、事業継続計画は各計画の中心にあり、各計画は、事業継続計画をサポートしていると見て取れる。この図を参照モデルとして使用する時、例えば、経済産業省の「事業継続策定ガイドライン」は、事業継続計画の枠組みと手順を示しており、リスクコミュニケーションに言及し、かつ IT 事故とインシデント対応、広域災害をケーススタディとして取り上げていることから、事業継続計画と IT 緊急時対応計画、サイバーインシデント対応計画、災害復旧計画、緊急時コミュニケーション計画を含むと考えられる。また、内閣府中央防災会議の「事業継続ガイドライン第一版」は、事業継続計画の枠組みと手順を示しており、リスクコミュニケーションに関し言及し、対応するリスクとして「わが国の重大な災害リスクで海外からも懸念の強い「地震」を取り上げていることから、事業継続計画、災害復旧計画、緊急時コミュニケーション計画を含むと考えられる。なお、NIST の定義で、災害復旧計画が対象とするのは、「ほぼ、IT に特化している。影響が長期にわたる大規模災害に限定される。」となっている。

さて、世界各国で策定されているBCP/BCMのガイドラインはこの図にあてはめるとどのあたりに位置するのであろうか？ここでは、国際標準化（ISO化）を目指している2つのガイドラインを取り上げてみる。英国では、BCI[9]の「Good Practice Guidelines」をもとに英国規格協会（BSI）が策定したPAS[10]56 Guide to Business Continuity Managementがある。もうひとつは、米国のNFPA[11]が策定したNFPA1600「Standard on Disaster/Emergency Management and Business Continuity Programs」（2004年版）がある。2つとも、枠組みや手順を示し、リスクを特定していないことから、この図では、中央の事業継続計画にあたると考えられる。ちなみに、リスクを特定していないというのは、リスクについて言及が無いということではなく、原因であるリスクを問うよりも「結果事象」を重要視しているということであり、結果として様々なリスクに対応できることになる。国際標準化を目指すには、万人向け（または森羅万象向け）である必要があるということなのだろう。例えば、NFPA1600の付録A（Annex A Explanatory Material A.5.3.2）には、"The hazard identification should include, but is not limited to, following types of potential hazards:"(リスクは以下を含みかつこれらに限らない)として、地震、津波、火山の噴火、雪害、雪崩、台風、ハリケーン、竜巻、洪水、旱魃、飢饉、疫病、伝染病（SARS、鳥インフルエンザ）、火事、交通事故、ガス爆発、水や空気の汚染、停電、通信障害、テロ、戦争、暴動、ストライキ、誤情報、犯罪、放火、電磁波などなど、およそ考えつくありとあらゆるリスクを掲載している。

3.2.5 誰が事業継続計画を策定するのか？

さて、このように広範な事故・災害・リスクに対応して事業継続計画を策定するのは（またはそれができるのは）誰なのであろうか？米国のDRII[12]は、事業継続及び災害対策関連の計画策定を担当する管理者に対する認定制度である「ビジネス継続プロフェッショナル」などを提供しており、BCIやでは、事業継続の専門家として必要な能力を以下の10項目に分類し公表している。

1 イニシエーションと管理
2 ビジネスインパクト分析
3 リスク評価とコントロール
4 事業継続管理戦略を作る
5 緊急時対応とオペレーション
6 事業継続およびクライシス・マネジメント計画の開発と導入
7 アウェアネスと訓練プログラム
8 事業継続とクライシス・マネジメント計画の維持と実践
9 クライシスコミュニケーション
10 外部エージェンシーとの調整（Co-ordination with External Agencies）

---

9 BCI: The Business Continuity Institute
10 PAS: Publicly Available Specification：一般仕様書。PAS56は、英国標準ガイドラインである。
11 NPA: National Fire Protection Association: 米国防火協会
12 DRII: Disaster Recovery Institute International　災害危機管理の教育・指導・資格認定を行う非営利団体で、1988年に米国で設立

ここで注目したいのは、「外部エージェンシーとの調整」能力である。これだけカバーする範囲が広いと、事業継続の専門家が全てをカバーできるとは考えにくい。よって、例えば情報セキュリティ事故の場合は、情報セキュリティの専門家の協力が、鳥インフルエンザのような疫病の場合は、防疫の専門家の協力が、大規模災害の時には防災の専門家や災害支援のための団体、警察、消防、自治体などの協力が不可欠となり、外部組織との調整能力が重要になるのである。つまり、BCPの専門家には、経営的視点、調整能力、コミュニケーション能力、緊急事態に即した判断能力など、ジェネラリストとしての総合力、指導力が求められることになろう。また、全社的な事業継続計画の策定にあたっては全ての関係者を集めた全社横断的な委員会を組織して策定するのが妥当であろう。但し、これもケースバイケースで、中小企業の場合などは、大掛かりな委員会ではなく、少数の幹部や担当者の合議検討で済む場合もあるだろうし、策定を任されたBCP担当が作成したドラフトを経営者が承認するというストーリーがあるかもしれない。さらには、コアビジネスは誰が見ても明らかにWeb販売であれば、ビジネスインパクト分析を行うまでもなく、Webサイトの中断が想定する最大のリスクとなり、Webサイトの安全のための脆弱性管理も必要となり、情報セキュリティの専門家が関与する余地が大きくなる。

情報セキュリティと事業継続計画の関係について言えば、情報セキュリティは、事業継続計画における重要な部分であり、ITへの依存度が高ければ高いほど、ITの専門家や情報セキュリティの関係者が事業継続計画の策定および事業継続管理に関与する部分は大きくなる。また、すでにIT緊急時対応計画があり、新たに全社的事業継続計画策定の動きがある時には、お互いに連携を取り、二つの計画に矛盾の無いよう、二重に処理を実施することの無いよう、整合性を取るために積極的に協力すべきであろう。

3.2.6 ISO/IEC17799 と SP800-53

さて、いままでは、SP800-34 について述べてきたが、NIST の SP シリーズ文書で、ISO/IEC17799 と並び称されるのは、SP800-53 Recommended Security Controls for Federal Information Systems（連邦政府情報システムにおける推奨セキュリティ管理策）という文書である。ISO/IEC17799 は情報セキュリティ対策におけるベストプラクティスを集めた管理策集であり、SP800-53 は、そのタイトルが示す通り、米国連邦政府が情報セキュリティ対策を行なう際に推奨される管理策を集めたものである。ISO/IEC17799:2005 には、11 の管理領域と 133 の管理策がある、一方、SP800-53 には、17 の管理策ファミリ（管理領域と同様の意味）と 160 を超える管理策がある。ISO/IEC17799:2005 では、事業継続管理に関しては、ひとつの目的と 5 つの管理策があり、SP800-53 の IT 緊急時対応計画に関しては、9 つの管理策が記載されている。

なお、NIST SP 800-53 に示す管理策ファミリは、管理、運用、技術の 3 つの管理策クラスのいずれか 1 つと関連付けられている。しかし、セキュリティ管理策の多くは複数のクラスに関連付けることができるため、クラス分けは便宜的なものであることに留意されたい。たとえば、緊急時対応計画（CP）は運用に分類されているが「CP-1 緊急時対応計画の方針と手順」は運用及び管理両方の特性を持つ。

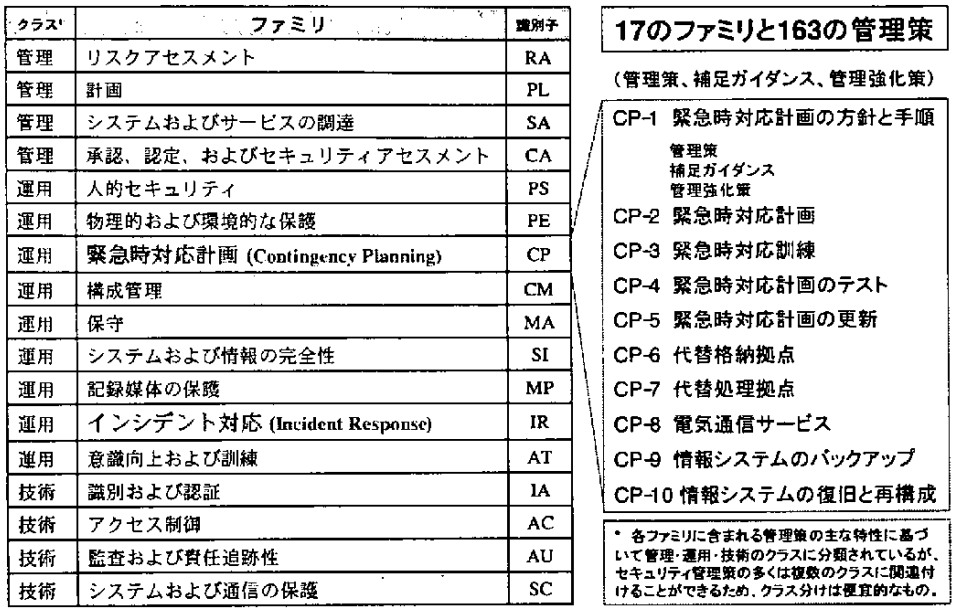


図3. SP800-53の管理策－ファミリ、クラス、識別子(CP関連)

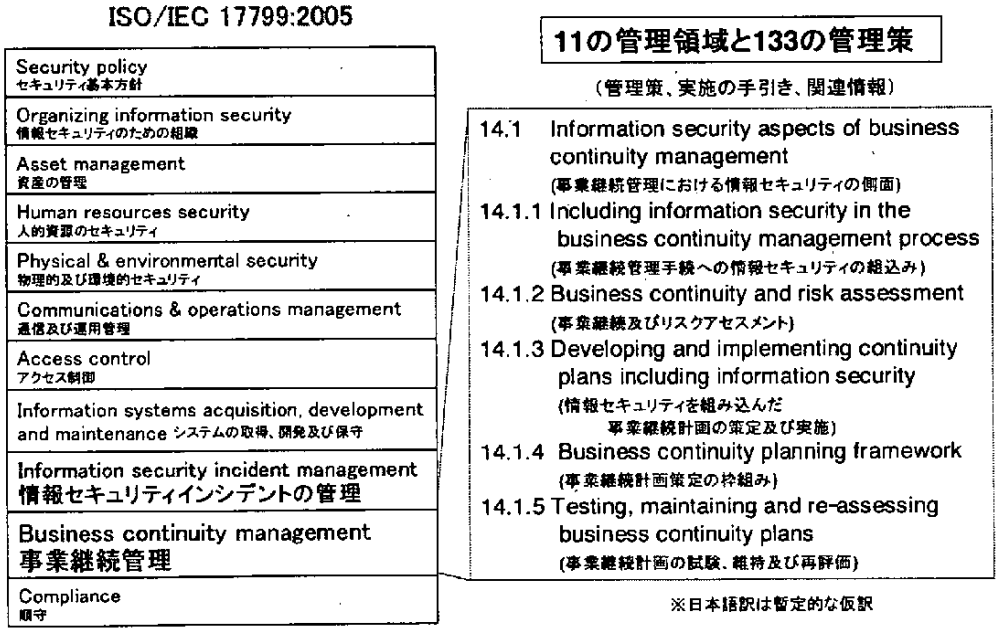


図4. ISO/IEC17799:2005の管理策(BCP関連)

SP シリーズ文書は立体的な構成になっている。管理策集として SP800-53 があり、そのそれぞれの管理策を実行に移すために、より詳細なガイドラインが用意されている。例えば、SP800-53 にはリスクアセスメントの管理策があり、それを実行に移すための詳細なガイドラインには、SP800-30 Risk Management Guide for Information Technology Systems (IT システムのため

のリスクマネジメントガイド)があり、同様に、CP(緊急時対応計画）の管理策を実行に移すための詳細なガイドラインは、SP800-34 Contingency Planning Guide for Information Technology Systems（IT システムのための緊急時対応計画ガイド）が提供し、IR（インシデント対応）の管理策を実行に移すための詳細なガイドラインには、SP800-61 Computer Security Incident Handling Guide （コンピュータインシデント対応ガイド）と SP800-83 Guide to Malware Incident Prevention and Handling (不正プログラムインシデント防止・対応ガイド）がある。

なお、IPA では、海外の情報セキュリティ関連文書等の翻訳・調査研究を NRI セキュアテクノロジーズ(株)と共同で行い、その成果を一般に公開している。2006 年 3 月現在、12 文書の翻訳を公開しているが、SP800-53、SP800-34、SP800-61 の日本語翻訳は双方の Web ページより無償でダウンロード可能であり、SP800-83 も将来翻訳公開する予定である。

3.2.7 SP800-34 IT 緊急時対応計画

SP800-34 は、IT 緊急時対応計画を策定するための、体系的で費用対効果の高いソリューションを提供しており、時間とコストをかけずに、計画策定と運用ができるように、計画管理ツールとしても利用できる図表やテンプレートを含み、巻末付録には、「IT 緊急時対応計画のフォーマット例」や、「事業影響分析の例と事業影響分析テンプレート」も掲載されている。

以下に SP800-34 の特徴を示す。

1. 目的、範囲、対象とする読者が明確（誰が何のためにどのように利用するか明確）
2. 緊急時対応に関する諸計画の相互関係を示し、定義している。
3. 緊急時対応計画とリスクマネジメントプロセスを示している。
4. 緊急時対応計画とシステム開発ライフサイクルを示している。
5. 緊急時対応計画策定プロセスを 7 つのステップにわたり解説している。
6. 豊富なテンプレートと付録が添付され、計画管理ツールとしても利用可能である。
7. 技術的考慮事項と人的考慮事項についても述べている。

3.2.7.1 IT 緊急時対応計画とインシデント対応の想定する脅威

IT システムに対する脅威としては、一般的に以下の脅威が挙げられる。

自然の脅威 － 台風（ハリケーン）、竜巻、洪水、火災など
人的脅威 － 操作ミス、妨害行為、悪意のあるコードの埋め込み、テロ攻撃等
環境的脅威 － 機器故障、ソフトウェアエラー、通信ネットワークの切断、停電等

しかし、SP800-34 IT 緊急時対応計画には、「サイバー攻撃（サービス拒否、ウイルスなど）への対応については取り上げない。これらの種類のインシデントへの対応には、IT 緊急時対応計画の対象範囲外の内容が含まれている。同様に、本ドキュメントでは、不法侵入、サービス拒否攻撃、悪意のあるロジックの注入などのサイバー犯罪に対するコンピュータフォレンジック分析による証拠保存に関連する、インシデント対応についても記述していない。」との注記がある。そして、SP800-34 で取り上げられなかった、サイバー攻撃やサイバー犯罪に対する対応については、先に紹介した「コンピュータインシデント対応ガイド」や「不正プログラムインシデント防

止・対応ガイド」で取り上げられている。但し、これらのガイドラインでは、インシデント対応における方針、手順、訓練、テストを用意することを求めているのであり、インシデント対応計画の策定を求めているわけではない。計画策定が求められるのは、あくまでも IT 緊急時対応計画である。しかし、人的脅威のうちでもサイバー攻撃やサイバー犯罪などの悪意のある攻撃に関しては、予防措置や検知、回復措置にしても、フォレンジック分析や証拠保存にしても、技術的に高度な専門性が求められるため、IT 緊急時対応とは別に詳細なガイドラインを設けているのである。

ちなみに、ISO/IEC17799:2005 では、「情報セキュリティインシデントの管理」と「事業継続管理」の別の管理領域を設けていながら、例えば、「10.4.1　悪意のあるコードに対する管理策」の実施の手引きの中で、「悪意のあるコード感染からの回復のための適切な事業継続計画の策定」を求めている。これは、上の考え方に少し似ている。

3.2.7.2　緊急時対応計画とシステム開発ライフサイクル

SP800-34「2.3 緊急時対応計画とシステム開発ライフサイクル」では、緊急時対応計画とシステム開発ライフサイクルの関係についての記載がある。以下にシステム開発ライフサイクル（SDLC: System Development Life Cycle）のそれぞれのフェーズにおける主な活動を挙げる。

開始フェーズ：　新 IT システムの企画に際し、緊急時対応計画の要件を考慮する

開発/調達フェーズ：緊急時対応策は、運用要件を反映する

導入フェーズ：　緊急時対応策を検証、テストする

運用/保守フェーズ：

- 緊急時対応計画手順を包含する訓練と意識向上プログラムを整備する
- 定期的にバックアップを実施して、オフサイトに保存する
- 必要に応じた緊急時対応計画の保守・更新をする

廃棄フェーズ：

既存システムを撤去し、別のシステムに交換する場合も、緊急事態について考慮する

ここで、「緊急時対策をシステム開発ライフサイクル(SDLC: System Development Life Cycle)のすべての段階で考慮することで、コスト削減や運用負荷軽減に寄与できるが、緊急時対応計画は主に運用/保守段階フェーズの活動に関連する」（要旨）と述べている点は注目に値する。「運用/保守段階フェーズ」の主要な活動として、教育や訓練、バックアップ、計画の保守更新が挙げられている。つまり、緊急時対応計画は、緊急事態発生時に活用できてこそ意味があるのであり、そのためにしっかりした、運用と保守が求められるのである。

3.2.7.3　事業影響分析の実施

事業影響分析は、緊急時対応計画プロセスにおける主要なステップである。事業影響分析は、重要なビジネスプロセスを特定し、そのプロセスを動かしている重要な IT リソースと関連づけ、その IT リソースが中断した時の影響と停止許容時間を判定した上で、復旧優先度を決定していく。そして、この分析結果は、他の緊急時対応関連計画の策定時にも利用できるとしている。

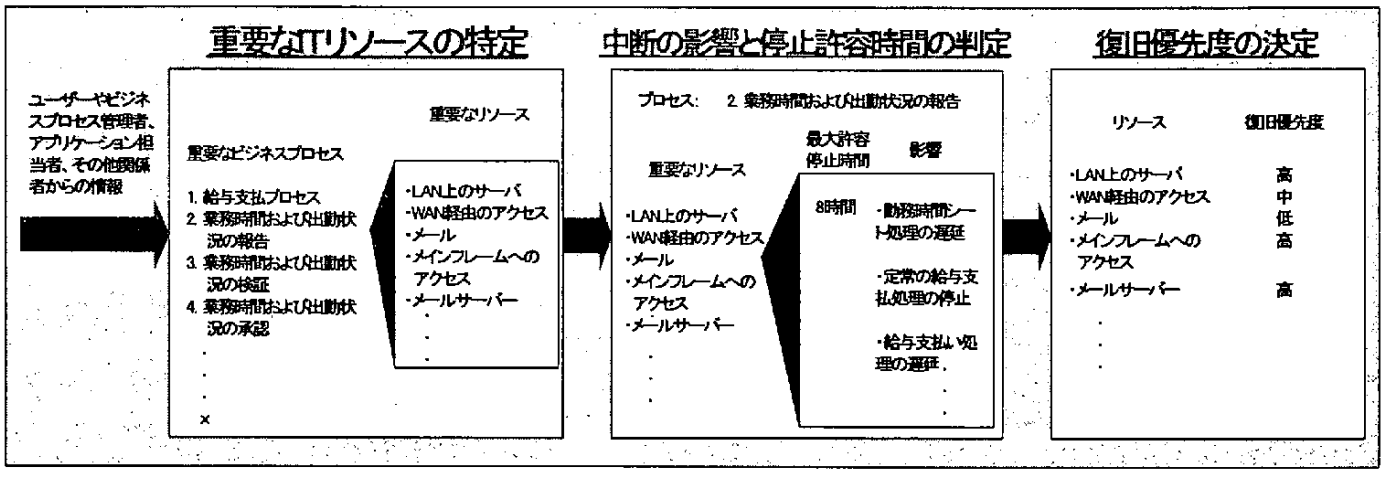


図 3.5　事業影響分析

3.2.7.4　IT 緊急時対応計画の策定

SP800-34 では、緊急時対応計画策定プロセスを以下の 7 つのステップにわたり解説している。

(1)緊急時対応計画ポリシーステートメントの策定

(2)事業影響分析の実施

(3)予防対策の特定

(4)復旧戦略の策定

(5)IT 緊急時対応計画の策定

(6)テスト、訓練、演習の計画

(7)計画の保守

事業影響分析が終わり、予防対策、復旧戦略を策定した後、IT緊急時対応計画を策定する。IT緊急時対応計画の構成については、以下の図3.6を参照されたい。

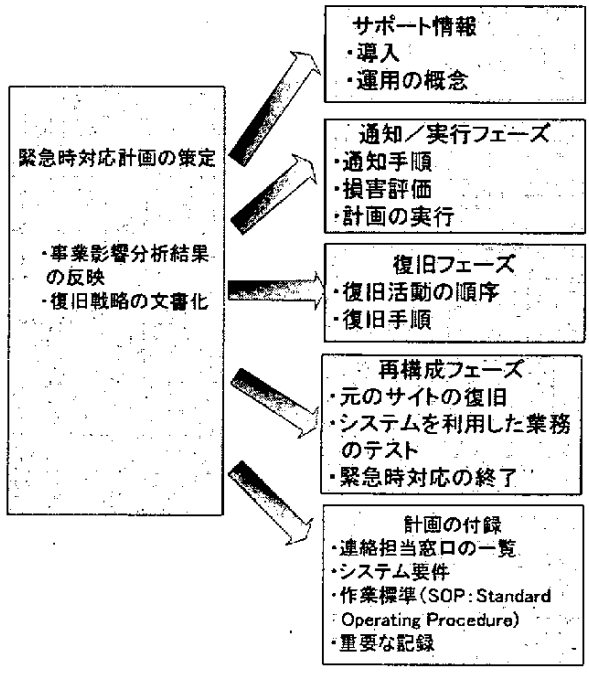


図3.6　IT緊急時対応計画の構成

3.2.8 おわりに

SP800-34の巻末付録Dには、緊急時対応計画における人的考慮事項が記載されている。そこでは、IT緊急時対応計画は、人員緊急時計画、事業継続計画、緊急時コミュニケーション計画などの各計画と整合性をとる必要があると述べられ、特に壊滅的なイベントを想定する場合には、以下の点を十分に考慮することとしている。

・人員緊急時計画：人員の安全性と撤退計画、退去手順、安否確認手順・方法、定期的な避難訓練、退避の際の人員確認の手順、災害後に人員の人数を数えるための手順と何通りかの連絡方法

・地域の消防署、警察署、レスキュー組織との連携し、事前に良好な関係を構築すること。

・コミュニケーション計画: 組織内での内部伝達と外部関係者への伝達窓口や手順

・人員の福利厚生：避難所、就業場所、人材調達、災害後の悲嘆へのカウンセリング

ここで銘記したいことは、深刻な状況下では、人的問題への対処が、事業継続や事業再開よりも優先するということであり、生命の安全等の「人的考慮事項」は最重要課題であるということである。そして、このことは、教育訓練の際にも、緊急事態に遭遇し、判断に迷うことの無いよう（自分の命と事業継続を天秤にかけることの無いよう）きちんと話しておくべきであろう。

参考資料

事業継続策定ガイドライン（経済産業省）
http://www.meti.go.jp/report/downloadfiles/g50331d06j.pdf
企業における情報セキュリティガバナンスのあり方に関する研究会報告書
http://www.meti.go.jp/report/data/g50331dj.html
事業継続ガイドライン 第一版　（内閣府　中央防災会議）
http://www.bcijapan.jp/documents/guideline01.pdf
事業継続計画の文書構成モデル例 第一版（内閣府　中央防災会議）
http://www.bousai.go.jp/MinkanToShijyou/shiryou4.pdf
わが国の災害対策(Disaster Management in Japan)
http://www.bousai.go.jp/panf/saigaipanf.pdf
企業経営における IT 事故対応に関する調査研究報告書　(㈱インターリスク総研)
http://www.bcijapan.jp/documents/BCM_survey.pdf
INTAP「平成 16 年度ビジネス継続性技術調査報告書」(平成 17 年 3 月)
http://www.net.intap.or.jp/INTAP/information/report/16-business-report.pdf
災害発生時における日本銀行の業務継続体制の整備状況について
http://www.boj.or.jp/about/03/data/sai0307a.pdf
金融機関における業務継続体制の整備について（2003 年 7 月日本銀行）
http://www.boj.or.jp/set/03/data/fsk0307a.pdf
当取引所の BCP(緊急時事業継続計画）について(2004 年 6 月 23 日 東京証券取引所)
http://www.tse.or.jp/guide/bcp/bcp2004.pdf
Business Continuity Management Good Practice Guidelines (2005)
http://www.thebci.org/goodpracticeguidetoBCM.pdf
NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs 2004 Edition http://www.state.nj.us/njoem/pdf/nfpa1600.pdf

NIST SP800 シリーズ文書

http://csrc.nist.gov/　http://www.ipa.go.jp/security/publications/nist/
SP800-12 An Introduction to Computer Security: The NIST Handbook
（コンピュータセキュリティハンドブック）(October 1995)
SP800-34 Contingency Planning Guide for Information Technology Systems
（IT システムのための緊急時対応計画ガイド）　(June 2002)
SP800-61 Computer Security Incident Handling Guide (January 2004)
（コンピュータインシデント対応ガイド）
SP800-83 Guide to Malware Incident Prevention and Handling (November 2005)
（不正プログラムインシデント防止・対応ガイド）

SP800-53 Recommended Security Controls for Federal Information Systems (February 2005)
連邦政府情報システムにおける推奨セキュリティ管理策

ISO/IEC17799 関連

JIS X 5080、 ISO/IEC 17799:2000、 ISO/IEC 17799:2005

政府統一基準関連

政府機関の情報セキュリティ対策のための統一基準
http://www.bits.go.jp/active/general/pdf/k303-052.pdf

「政府機関の情報セキュリティ対策のための統一基準（2005 年 12 月版［全体版初版］）」解説書
http://www.bits.go.jp/active/general/pdf/k303-052c.pdf

政府機関統一基準と ISO/IEC17799：2005 等との対応について
http://www.bits.go.jp/active/general/pdf/rel2005_iso.pdf

3.3 「BCMの実際：石油備蓄基地の国家戦略としての危機管理＋BCM、BCP雑感」

3.3.1 最近１０年間の事件・事故

私のこれからやる話は、実際に石油備蓄基地というもののビジネス継続です。石油をちゃんと備蓄して必要なときに出すというビジネスをどう継続的にやっていくかと。日本としては６カ月間の石油の備蓄を持つというのは公約でございまして、今、原油の値段が高いときにさらに積み増しをしようと、それから天然ガスも積み増しをしようというような事態になっておりますが、実はこの危機管理のためのシステムをつくるのに、今、実際にかかってはいるんですが、「やりましょう」という合意が成立するまでに非常に長い時間がかかりまして、ＢＣＭが導入されるにはどのぐらいの過程をふまないと実際にはできないものなのだろうかというのを、ここでお話ししたいと思います。

最近10年間ぐらいの事件・事故のほとんどは、その都度、いったい担当の部署の危機管理はどうなっているんだということが問われた事件です。その都度、あれをやらなければいけない、これをやらなければいけないというのがあって、この阪神淡路大震災以降、1995年というのは非常に悪い年でございまして、１年のうちに３回も事故が起こりました。それで、内閣の中に危機管理監とか、そういった実際に緊急事態に対応する組織をつくったというのは、こういう事件が重なったからです。

今、私がこれから申し上げます大規模の石油汚染事故というのは、実はナホトカ号というこの事件がありまして、これはもう県とか市とかというレベルではなくて、日本海沿岸全体におよんでおり、どうやってそれを太平洋側からサポートするかというような、非常に大きな対策事業であったわけです。このときの被害総額というのは大体350億円になります。もうちょっとうまくマネジメントできたんじゃないか。もうちょっと早く対応できたんじゃないか。もうちょっと早く油を取れたんじゃないか。効率良くできたんじゃないか、というのは常に言われていたんですが、ただこのときに、350億円ですからそのときに１割とか２割改善されていれば、これはものすごいお金なんですね。この金額35億円とか70億円とかあったら、普通でしたら経営者はそれだけ利益を上げたら胸張りますよ。そのぐらいの金額なんですね。それは、実際にはお金が出ていってしまいましたんで、払ってしまうとそれでおしまいになってしまうものなんです。その後、さらにここで大規模石油対策事業で、113億円つくんです。これは事件ですが、これは実際に対策としてつきました。しかし、ここで十勝沖地震が起こってしまった。わずか２年ですか。ですから１年足らずで起こってしまうわけです。

3.3.2 石油備蓄基地の配置状況

こういう事件が起こって、実際に石油備蓄基地というのはどういう配置になっているかと申しますと、全国に10カ所国家石油備蓄基地というのはあります。そのほかに国に依頼されて各石油会社が備蓄している基地があります。この基地の全部でやるのは、5,100万キロリットルという、これは大体６カ月分に相当する原油量なんです。ここで従来どういうことをやったかといいます

と、各備蓄基地は民間の管理会社が引き受けて運営しているわけなんです。こっちは民間の会社がそのまま独自に運営している。独立の会社をつくって、国家石油備蓄基地というのを運営して管理会社がやっている。これは日本の悪いくせなんですが、横並びなんです。ここでは各基地には消防団もあり、コンティエンジェンシープランもあり、危機管理のためのスタッフもそろっているということになっているんですが、ほとんどがマニュアル化されておりまして、例によって紙のマニュアルですよね。この紙のマニュアルというのは、ほとんど実効性は非常に少ないわけなんですが、このような紙のマニュアルを使って、実際には対応している機関と共同で訓練はずっとおやりになってはいたんですが、あまりうまくは実際には運ばなかったというのが実態です。

3.3.3 専門機関の役割と実例

実は、今回私どもがつくったシステムを実際に管理する方は海上災害防止センターというところなんですが、専門機関です。実際にヘルメットをかぶり、長靴を履き、原油に汚れてかなり危険な作業をするところです。ナホトカ号の場合でも、実際に現場で指揮監督して、350 億円の金を使って、最後にプロジェクトのすべての決算やったのもこの機関です。つまり、実際に動く機関。ここでなぜこういう専門機関が必要かということを引き合いに出すのは、今後、皆様方の中でビジネス・コンティニュティ・マネジメントとかプランニングやったときに、こういう専門機関、実際に動く機関が必要なんだということをご理解いただきたいからです。総務の片手間の仕事じゃない。取締役を一人任命すればそれで済むという仕事でもない。ましてや、保険会社とかそういうところを呼んできて、任せてマニュアルを作らせてそれで終わるという仕事でもありません。

仮に、もし頼むのなら、ＮＴＴコミュニケーションとかですね。緊急時に必要なのは情報と通信なんですよ。ですから、少なくとも東証一部のあの株のページをめくって、情報通信のところか、もしくはサービスですか、コンサルティングですから。そういうところから相談先としてお選びになるのが賢明だとは思いますけどね。

実は、この大口径泡放射砲というのがあるんですが、これは大体直径１メートルぐらいにワーッと一気に放射するんですが、これが実は苫小牧の地震、十勝沖の地震のときはなかったんですね。それで、急きょ買ったんですよ。あのときは日本になかった。ではどんな状態で消火をしたのか。これは実際の苫小牧の写真ではなく、イギリスで起きた事故のときの写真です。ご覧になっていただくと分かるんですが、従来のプランでは、これは消防車です。これピュッと出ていますよね。これぐらいでこんな大きなのが消えると思います？　つまり、各管理会社がやっているとこのぐらいで終わってしまうんですよ。これが実態なんです。このタンクですけれど、直径 82 メートル、高さ 24 メートルです。ナフサタンクだと直径 60 メートルの高さ 23 メートル。82 メートルというと、どういうことになるかというと、野球場がすっぽり入っちゃうんですよ。そのぐらいの大きさのものに火がついているのに普通の消火ホースで消そうって、それは無理ですよね。

そうすると先ほども申しましたけれど、何をやったかと言うと、リソースが全国に散らばっている状態の時に、事故はここで起きたわけですから、少なくともこの近くの消火剤なりリソース

なり、それをすべてここに持ってくると。もっと南のほうにある対策要員をスタンバイさせるというようなことをしなくてはならないのですが、これは実はＢＣＭ全体の構造が分かっていれば、そういうプランがつくれるんです。そういうビジネス・コンティニュティのプランが、緊急時のプランがつくれるんです。そのシステムがなかった。それを今つくろうとしているんです。

3.3.4 危機管理導入までに必要な４要素

実は、こういった全国を網羅するような危機管理システムをつくろうじゃないかというのを、私が石油公団とかそういうところに提案したのが 10 年前です。10 年前に提案して、今回の事故が起こって、ついこの間も今治で起こりましたよね。太陽石油のタンクに火がついて、５人お亡くなりになりましたよね。ちょうとヒューザーの小嶋さんが国会でやっていたので、そっちのほうの記事で押されちゃって、全然大きくは取り上げられませんでしたけど、ご覧になってください。これがそれ以前の対策だったんです。ご覧になってちょっと怖いものがありますけれど、提案をして、この苫小牧の事故が起こって、痛い出費をして、あの事故で実際にかかった金が 200 億円ですよ、復旧まで。これもし、考えますよね、１割でもうまくできたら、１割でも削減できたら、20 億円ですよ。

このＢＣＭとかＢＣＰを実際に動かすには、導入までに必要な４つの要素というのがありまして、実に長い孵化期間、教育期間と言ってもいい、自分のリスクに気づく期間です。それだけの非常に長い潜伏期間がある。それと手痛い経験ね。それと、そういう手痛い経験から学ぶのですから、二度目に起こったときには必ず対応できるような専門的な組織。専門の組織です。どこかから取締役呼んできてサインするわけでもない。専門の組織が必要です。先ほど言った、実際にヘルメットかぶって、長靴履いて、軍手して、汚れるのを覚悟の上で実際にできる人たち。要するに、セキュリティマネージャーとか、ビジネス・コンティニュティ・マネジメントというのがあるのであれば、専任のビジネス・コンティニュティ・マネージャーが必要です。それを申し上げておきたい。

もう一つは、基本的な概念設計。危機管理というのは、ここに書いてある要員、資材、施設、地図情報、この４つのデータベースをしっかり持てば、危機管理は必ずできます。なぜかというと、危機というのは必ず場所があります。地図上に落ちます。対策を打つにも、要員、資材、施設、前の３つですが、必ず地図の上に落ちます。地図を使ってどう被害を軽減するか、被害を最小限に収めるか。イギリスだとこういう作業をやる部屋をマッピングルームといいます。これは戦略本部です。ですから、地図情報というものを具体的に自分の組織のとか、ステークホルダーと言っていいんでしょう。ステークホルダーがどういう分布になっているのかというのを一度地図上に落としてみると、実にいいレッスンだとは思っています。

3.3.5 BCM/BCP

ここで、ＢＣＭとかそれの石油業界における手痛い例というのをご紹介したわけなんですが、ただこのＢＣＭというのは、実際には誰のためのＢＣＭなのかというのは、どうも近ごろ私は実は疑問に思っている点がありまして、企業が生き残るためというのですが、これはご異論があれ

ば反論していただいて結構なんですが、結局は消費者のためのＢＣＭなんじゃないか。その部分が抜けてしまうと、基本的な概念が狂ってしまうんじゃないか。それと、昔はフィナンソロフィとか企業貢献とかＩＲ（Investor Relationship）とか、そういうＢＣＭを公開すればIRになります。そういう言葉に置き換えられていた。

どうもだんだん新しい概念というと英語でやっているような、英語でやると分かったような分からないような気持ちになるということがあるんだと思うんですが、実はこの下に書いてある百年目とか味噌蔵とかは、円生の落語なんですよ。この円生の落語の中に「百年目」というのがありまして、皆さん古典落語お好きな方は帰って読んでいただきたいんですが、檀那、百年目、栴檀、南縁草、年季奉公、屋号。これ考えてみますと、檀那の修業というのは、ビジネス・コンティニュティ、要するに、マネージャーの修業なんです。檀那というのは、実は栴檀と南縁草がかかって「ダン・ナン」なんですね。栴檀の木というのは、その根元にある南縁草という汚い草があってこそなんです。檀那の木というのは大きくて、明け方に露を落とす。その露で南縁草が育って、その南縁草が肥やしになって栴檀が育つと。だから檀那というのは“落とす”んだよと。

先ほどマネージャーという話をしましたけれど、こういうマネージャーを育てるのは、ただ単に任命すれば済むんじゃなくて、それこそ年季奉公とか屋号とか襲名させるとか、そういった形でビジネスのコンティニュティをつくると。これは落語の中にあるんです。

それで最後に、のれん分けというのは実にうまい危機管理の方法でありまして、仕入れ先、売り場、それからお得意、経路、すべてをのれん分けで分けているわけですから、１軒が駄目になっても、みんなリカバリーが利くわけですよ。ネットワークでサポートシステムが出来上がっているわけですから。こういうところからもうちょっと学んでもいいんじゃないかと。

「味噌蔵」というのは、「焼けてきました、焼けてきました」と言って、田楽のにおいでうちの味噌蔵に火が入ったというオチの落語ですけれど、その中にも「うだち」とかですね。うだちとは防火壁ですよね。災害のためのプランというのがちゃんとつくってある。こういうふうに、かなり江戸時代の古い檀那衆の檀那ぶりといいますかね、老舗の、そういう人たちの中に、日本で使えるような、変な、分かったような分からないような英語を使うんじゃなくて、日本の心情的にも納得がいくような、いわば腑に落ちるというのですか、そういったもので実際に、ビジネス・コンティニュティとは言いません。お店（たな）の世継ぎがちゃんとできていくのではないかと思っています。

「ＴＩＭＥ2005年の顔」というのは、これはビジネス・コンティニュティがあまりにも大きくなりますと、ビジネス・コンティニュティをどういうふうにやるかというと、『ＴＩＭＥ』の2005年の顔、『ＴＩＭＥ』の一番年間の最終号に出てくる去年の顔は、ビルゲイツ夫妻、それからＵ２のボーノ。これは３人並んでいるんですけれど、Ｕ２のボーノは皆さんご存じないと思いますけれど、ロック・スターですよ。世界で最も寄附とか、ここで言うところの最後にここに書いてある布施餓鬼、ドネーション。先ほど言いました、栴檀の露を落とした人なんです。そのお三方がタイムの最終号の顔でした。

先ほど言いました、檀那ぶりと言いましたけれど、ビジネス・コンティニュティとかビジネス・マネジメントを考えるかというと、当然その企業の責任者の方ですから、こういう方がどのよう

な檀那になればいいのかというのは、はっきり言いたくはないんですが、英語で学ばなくてもいいんじゃないかと思っています。

3.4 情報セキュリティ侵害事案を対象とした事業継続計画導入について

3.4.1 「可用性」以外を要因とする事業計画発動

事業継続計画は、通常、事業の継続に必要不可欠な何らかのリソースが“使用できなくなる”ことによって発動される。これは、情報セキュリティの三要素（機密性、可用性、完全性）に照らして言えば、当該リソースの可用性が損なわれた場合に該当すると言える。通常良く話題に上がる事業継続計画発動の場面は災害であることもこれを端的に表しているものと言えるだろう。逆に言えば、事業継続に不可欠なリソースの可用性を直接的に損なうおそれのある代表選手が災害であるということである。したがって、災害発生を対象とした事業継続計画についてはこれまでもよく研究され事例の蓄積も多々ある。しかしながら、今日、事業の遂行に必要不可欠なリソースが使用不能になるきっかけは必ずしも直接的に当該リソースの可用性が損なわれた場合だけとは限らなくなってきていると言える。

まず、情報の機密性に問題が発生した場合で、事業継続に大きな影響を及ぼす場合について述べる。機密性に問題が発生した場合、という端的な例は情報漏えいである。最もわかりやすい例で言えば、情報システムに何らかの脆弱性が有ったが故に、当該情報システムが扱っている情報の機密性が損なわれた場合、特にそれが顧客にとって重要な情報である場合には、最悪の場合、原因が判明し機密性が回復できるまでシステムの運用を止めて原因究明にあたらねばならないことになりかねない。これは実際に通信販売会社が顧客情報の漏えい事故発生に際して、一旦すべての業務を止め、原因究明にあたった実例がある。もちろん、その間の売上はゼロになる。しかしながら、この例の場合には潔く業務をすべて止めて原因究明を徹底的に行った企業の姿勢が好感される等の状況もあり、結果的には事業の継続に成功した、と言えるだろう。この例に学ぶ最も重要なことは、どこまでの損失ならば倒産せずに耐えられることができるのか、そのために業務を停止できる限界はどこまでか、を見極めることにあると言える。このような対応は、業務の停止によって発生する損失がそれなりの精度で計算でき、自らのコントロールの範囲内である場合にのみ実行できることに注意すべきである。情報漏えいであっても、以下の例のように事業継続が非常に困難になる場合も容易に想定できる。

昨今話題の個人情報漏えい事故を想定する。想定する状況は、非常に多数の一般消費者の個人情報を保有し、取り扱う大企業が、これら個人情報の取り扱いを含む情報システムの運用管理を外部の会社に委託している場合であって、この受託業者が、さらに外部の業者から人を雇い入れてその運用業務にあたっているという場面で、この再委託先従業者（多くの場合このような事業者は中小または零細事業者である）の故意または過失によって大量の個人情報が漏えいした状況である。個人情報の漏えいによって、この委託元大企業は多くの緊急時対応作業を行わねばならなくなる。漏えいした情報の内容、その量といった状況の把握、漏えいした情報による本人への最大リスクの検討・評価、本人への通知（場合によってはお詫びの品を送付する等）、苦情受け付け、原因究明と再発防止策の検討・実施、報道発表の準備と発表後のマスコミ対応、主務大臣（監督官庁）への報告等々である。さらに、一次受け企業も原因究明、報道発表等これに準じた対応

の必要に迫られる。数万人規模の情報漏えい事故の場合、これら対応に要する経費は数千万～億単位になる場合がある。これら経費は、一連の対応が終了し収束してきた時点で、発注元から一次受けへ損害賠償として請求される。一次受け企業は、再委託先の企業に対し、自社の責任範囲に相当する費用は減額するものの自社の対応経費のうち幾ばくかは加算されて、再委託先企業へ損害賠償請求をする。業務受委託契約の内容にもよるが、損害賠償請求額が業務受委託契約金額の上限を越えるようなことが発生した場合、この末端の中小・零細企業にとってはとても払いきれない金額の損害賠償を請求されることになりうる。このことは、この業者にとっては直ちに債務超過となり倒産の危機を迎えることになりかねない。

このような、情報漏えいをきっかけとする事業継続の危機状態は中小企業にのみ起こるものではもちろんない。機密情報の漏えいをきっかけとする顧客からの信頼を失うことによる事業機会の喪失、これの積み重ねによる売上減、事業損失の増大が事業継続に重大な影響を及ぼしかねないことは、大企業であっても十分に起こりうると考えられる。企業そのものの倒産という事態にまで発展せずとも、当該事業からの撤退を余儀なくされる等の状況も発生しうる。

情報の完全性が損なわれた場合にも、事業継続の危機は起こり得る。情報の完全性が損なわれるとは、情報の改竄などがそれに当たるが、情報の完全性に問題が発生し、このことが企業の経営に影響を及ぼした実際の例としては以下のようなものがある。

米国のとあるバイオサイエンス企業のホームページが改ざんされ、偽のニュースリリースが掲載された。このニュースリリースには同社が買収されると書かれており、NASDAQ に上場されていた同社の株価は一時前日比 50%上昇した。

これは２０００年の２月に米国で起こった例である。偽のニュースリリースによって株価が上昇するならば逆に下降する場合もあり得ることは容易に想像できる。

このほかにも、国内のショッピング情報サイトが、あるページを閲覧するとウイルスがダウンロードされるように改ざんされ、原因の除去のために同サイトが一時的に閉鎖された例もあり、完全性が損なわれた場合も事業継続に影響を及ぼしかねない状況も現実に発生しつつある。

また、情報システムの可用性が損なわれたために事業継続に影響を及ぼした事例であっても、可用性が損なわれた原因が地震、火災、水害といった災害だけでなく、オペレーションミスのような人的原因によるものや、設計時の容量を大幅に上回る処理要求の発生によるシステムダウンなどを原因とするものも多くなっている。

3.4.2 情報セキュリティに対する認識・理解

このように、情報技術が発達、情報の持つ価値が増大し、企業活動の多くが情報技術によって支えられている現在、情報および情報システムのセキュリティが損なわれることが企業の事業継続に大きな影響を与えかねない危険性はより一層高まってきていると言える。加えて、企業の経営陣における情報セキュリティ侵害に対する警戒、すなわち発生しうる損失の大きさ（＝リスクの高さ）に対する認識は十分なものとは言えない。特に、情報セキュリティは鎖のような“連鎖”であって、その最も弱い輪が切れたらすべて終わりであるという認識を十分にしているかどうか、残念ながらはなはだ疑問である。しかも、災害にくらべ先に挙げたような状況はより発生頻度が

高いことも考えられる。しかしながら、事業継続計画の策定に際し、このような要因によって事業の継続に影響を与えうることはあまり考慮されていないように見受けられ、ここに課題があると考える。

実際の事業継続計画の策定に際してもまだ様々な課題が存在すると考えられる。リスクの分析・評価が体系的に行われていないために、手を打つ優先順位に妥当性が欠けていたり、そもそも自社業務を支える情報システムの重要性の順位付けもされていなかったり、昨今電子メールシステムを代表とする情報系（インターネット系）システムの重要度が増しているにもかかわらずこれに高い優先順位を与えていなかったりする企業も多々あると考えられる。自社の情報システム中、どのシステムがクリティカルなのか、まずはここから考える必要があるだろう。

また、事業継続計画を策定しても、これが実際に効果を発揮できる内容になっているかどうか、訓練や演習によって確かめる必要がある。その際には、発生している状況をシナリオとして作成するメンバと、事業継続計画に従い、アクションを起こしていくメンバとを分けて行うことは効果があると考えられる。

3.4.3 緊急時対応、危機管理についての「心構え」

事業継続計画発動の契機となるインシデントについては、台風、水害、一部のコンピュータワームのように発生の前兆を観測できる場合と、地震、火災、不正アクセス、情報漏えいなど突然やってくる場合があり、また、突然発生型であっても、その発生直後にはその影響の大きさが判然としなかったりする場合など、様々な状況があり得るが、いずれの場合においても、初動対応では常に最悪の事態も想定した上で取り組む心構えが必要であると同時に、もし“空振り”に終わった場合であっても、無駄なことをした、と悪い方向に考えてはいけない。緊急時対応や危機管理にも同じことが言えるが、いわゆる“オオカミ少年”と思っては絶対にいけない。“どうせまた空振りだろう”という意識は、せっかく立案し訓練した計画を台無しにしてしまいかねない。このことは訓練を通して等、この活動に携わるメンバをよく教育しなければならない。たとえ“ぼや”でも消防車は出動しなければならない。逆に“ぼやで終わって良かった”と考えるように動機づけなければならない。日本においてはこの点の教育にも力を入れるべきである。さらに、この、緊急時の対応を行うメンバは専担である必要がある。情報セキュリティ確保のための様々な行動は、日常の業務活動の中にごく当たり前に組み込まれることが最終的に望まれる状況であり、そうなるように業務プロセスを修正していかなければならない。これが完全に達成された暁には情報セキュリティを推進する特別なチームは不要になるのかもしれない。しかし、緊急時の対応は別である。消防活動が、専担の消防署員と応援の地元消防団といった形で構成されるのと同様、専担で常に準備を欠かさず万一に備えるチームと、平時は他の業務に就いていても、緊急時にはこの対応にあたるメンバをアサインしておく構成を取らねばならない。さらには、地震、台風などの広域災害や大規模なコンピュータウイルスなどは各所で同時に発生することにも注意が必要である。特に、もし緊急時対応の要員を外部に委託することを考えているような場合には特に注意が必要である。

3.5 インターネットガバナンスと IPv6

3.5.1 初心・基本に帰ること

私は日本のインターネットを始めた人間の一人、インターネットを日本に持ってくる仕事をやった立場の人間として、「インターネットガバナンス」と「IPv6」に焦点をあてて話をすすめたい。

インターネット企業と事業継続性との関係を言うとき、この問題は避けて通れない。ネット企業といわず、インターネットを使っている企業が全部関係しているわけだが、ネットの仕組みをよく理解しているかどうか、というのが重要な問題である。例えば最近問題を起こしたネット企業が、インターネットはどうして動いているとかということをよく理解しているとは到底思われない。

私たちは、ネットの初心ともいうべきものを大事にする、それを Go back to the Fundamentals と呼ぶようになっている。ただ単に「基本に帰れ」と言うだけでなくネットが無数のひとびとの努力の積み重ねから成り立っていることを忘れず、その善意の巨大な集合体にたいする畏敬の念をもって、ありうべき未来の Fundamentals を模索することを言うのである。

IP ネットワーク上ですべてが動くこと、Everything over IP ということをわれわれは昔から言ってきているが、インターネットの資源管理というものを自覚的にとらえてインターネットを企業活動の神経網に使うということが、まず前提として必要なことだと思う。それは、インターネットガバナンスと IPv6 を今ここでテーマにする理由になると考えている。現在使っているインターネットがどうして動いているのか、を知ることは重要である。

IP アドレスとドメイン名なしにはインターネットが成り立つわけもなく、それらの管理の重要性を知ってはじめてインターネットを使う環境が成り立つ。そこでのインターネットは公物、コモンズ Commons であり、誰の所有でもない人類の共有財産、公共のものである。この常識が常識でないところに、さまざまの事件が起こり、公共物をみんなが使えるようにするというモラルが守れないために、不都合が生じる。考えてみただけでも、腹立たしい毎日である。

インターネットガバナンスというのは、1998 年の ICANN の設立から始まったのではなく、1988 年の IANA の顕在化が IP アドレスとドメイン名の管理を浮かび上がらせてからずうっと議論されてきた事柄である。このところは、インターネットの歴史を紐解いてもらいたい。

2003 年、国連の事務総長の下で WSIS(World Summit on the Information Society)というのが開催されて、2003 年のジュネーブから始まって 2005 年の 11 月のチュニスまでこれが続いて、インターネットガバナンスが議論された。国連が主導して、ITU が主な担当になって、この中で現在インターネットガバナンスを担っている ICANN という組織があって、ICANN が透明性と公平性を確保しているかということが途上国から疑問視されたという経緯がある。しかしながら途上国の発言は、ほとんど ICANN の実体を知らないまま、つまりインターネットの実体を知らないままに問題視をしていたということが判明した。そこで、世界中の国々の人々が、インターネットガバナンスの、つまりインターネットの現実を学ぶ機会が生じたという。11 月のチュニスの会合には、竹中総務大臣が出席しているが、このとき何と 23,000 人もの人々が、インターネットガバナンスの主題だけではないけれども、そこに集まったということがあった。

3.5.2 インターネットの資源管理

インターネットガバナンスというのは、インターネットの資源管理の問題である。IP アドレスとドメイン名がインターネットの最重要な資源であることは強調しすぎることがない。IP アドレスは、現行が 32 ビットの IP アドレス体系：IPv4 であって、これは残りが少なくなってきている。今後は IPv6 で 128 ビットになり、無限にあるようなものと考えられている。米国の DOD（国防総省）が 2008 年までに全面的に移行するということを表明しており、中国も IPv4 が足りないままで、いきなり IPv6 で行こうということを表明している。

携帯の IP 電話化は、IPv6 でいくかどうかということが一番の焦点になっていて、IPv6 でないとソリューションにならない。IPv6 による携帯 IP というのは、今中国で盛んに開発されているというところで、日本の技術が中国市場にどうささっていくかということが大きな問題のところである。

ドメイン名は、gTLD(generic Top Level Domain)をどんどん増やしていくということを ICANN ではやっているが、「.com」「.org」「.it」などというドメイン名から始まって、「.biz」とか「.museum」などに拡大されてきた。「.xxx」というのはポルノ系のコンテンツのプロバイダーに対して与えたらどうかということが、現在 ICANN では議論になっていて、アメリカや ICANN の理事会がこれに対しては反対しているので、議論がまだ続いている。

また「.jp」などの ccTLD、カントリーコードのトップレベルドメインというのは、あれこれ転用される場合があって、「.tv」というツバル共和国のドメインはテレビ業界などにどんどん売られている。そういうことが、いろんなビジネスモデルを誘発して、またそのある場面では混乱の元になるということもある。

そもそもインターネットは誰のものか。誰がどこのお金で誰のためにつくったか。ということが、インターネットガバナンスの議論では問題になっていて、アメリカ政府が最初のカネを出したから米国のものなのか。所有権、知的財産権はどこにあるのかということがしばしば議論されてきたが、ほとんど Commons（共有財産）であるということで合意にするほかにない。これは誰にも属さない共有のものであるということで、いろんな主張がまとまってきている。

ところが、誰が運用管理してメンテナンスするのか。例えば一番肝心の Root DNS Server というのが世界中に主要なものが 13 個あり、アジアでは日本に 1 個ある。それぞれの団体の管理者が力を寄せ合ってその 13 個のルートサーバの管理をやっている。日本にはこのルートサーバの Mサーバというのがあって、WIDE プロジェクトがこれを管理している。ものが置かれている場所は大手町の KDDI のビルの中にある。誰も命令せずにそういうものが動いているというのがインターネットの現実であって、所有者は誰もいない。これは Commons という考え方になっている。実際の運用担当者は、もちろんそのことを知っている。

実際にインターネットの管理を担ってきたのは、最初から IANA(Internet Assigned Numbers Authority)である。南カリフォルニア大学の情報科学研究所(ISI)のジョナサン・ポステル(Jonathan Postel)博士が IANA を献身的に運営していたが、当初から国防総省との契約があったとされている。Jon Postel は、IP アドレスの配布のシステムを考案し、ドメイン名管理の方策を

考慮した。

手短に言うと、IANA でまかないきれなくなって、ICANN を形成した。ICANN は、インターネットの各種資源を全世界的に調整することを目的として、1998 年 10 月に設立された民間の非営利法人である。民間の会社、それも非営利の会社であることは重要である。米国の西海岸カリフォルニア、ロサンゼルスの近くにあるが、まずドメイン名と IP アドレスおよび AS 番号というのがあって、プロトコルポート番号およびパラメーター番号というのがその管理の対象になっている。

ルートサーバについては、その運用および展開の調整も ICANN で行うとしている。ICANN には、ルートサーバのアドバイザリ・コミッティーというのがあって、それの委員長が村井純になっている。これらの技術的業務に関するポリシー策定の調整というのも ICANN で行うということで、民間主導で全世界的に行うことを目的としている。その活動は全世界に開かれたものとなっていて、関心のある人は誰でも参加できるという組織になっている。

ICANN の考え方は、これまで通りインターネットのカルチャーというものを受け継いでいて、インターネットカルチャーというのは、とくに IETF（Internet Engineering Task Force）に象徴されるようなものとすれば、それは多数決原理ではなくて、実質を重視するということである。「ラフ、コンセンサス、ランニング・コード」(Rough Consensus And Running Code)ということで表現されるように、最後まで決めこまないで大まかな合意を採って進める、その際に、いま動いているコードを大切にするという、実態に即した考え方になっている。これには、米国特有のプラグマチズム(Pragmatism)のよき伝統が反映しているように思われる。

元よりオープンシステム、オープンソースの考え方であるから、良いものはみんなが使ってもっと良くなっていくというのが、ＵＮＩＸを始めとして、オープンシステムのカルチャーである。オープンシステム、オープンソース。当然ボトムアップであって、トップダウンではない。分散環境で危険も分散する。Internet is for Everyone（インターネットは万人のために）というのが標語になっている。

しかし、スケールの拡大と商用インターネットの性格の曖昧さが、Jon の設定した枠組みを超えて、さまざまな問題を引き起こすようになった。それは、一般ドメイン名、.com, .net, .org の登録管理をネットワークソリューション社（NSI）に委託したところ、手数料として 50 米ドルを請求するようになったところから始まった。First Come, First Serve の原則、要するに早いもの勝ちで、ドメイン名の登録を受け付けていたこともあって、投機的な先行取得が流行り、先にドメイン名を取得したものがそれを必要とするものに高値で売りつけることが日常化する、Cyber Squatter とよばれる状況になっていた。これは、社会問題化してきた。

ドメイン名の扱いを当初は米国防総省、後に商務省から委託された IANA で、Jon は、ドメイン名の名前空間の拡大を考えた。IESG、IETF のインターネット技術を中心にしたグループの本来の議論とは違った局面の問題である。Jon は、150 ぐらいの一般トップレベルドメイン名（gTLD）を増やしたらどうかと考えていた。どういう手続きでこれを増やしていくのか。

Jon は、インターネットコミュニティの自主的な管理を、社会的に認知させる道を選んだ。それが，International AdHoc Committee（IAHC）の提唱となった。IAHC と呼ばれた委員会

である。当初から村井さんがそのボードメンバーに入っており、JPNICの理事会でサポートしようということになった。

記憶が曖昧だが、第４０回のIETFで、Jonの新たなIANAの組織的イメージが語られたりしていたが、そこではすでにICANNの骨格を成すドメイン名、IPアドレス、プロトコルの３つの管理組織作りが挙げられていて、プロトコルの管理組織の中にはWIDEの名もあった。

IAHCはインターネットコミュニティの意思を反映して進められた。その傍ら、IAHCの在り方についてJonは米国商務省でインターネット戦略をクリントン大統領の下で担当する上級顧問のIra Magazinerと相談を始めていた。IAHCの運動を世界中に広め、ドメイン名を中心にして改革に携わろうとする人々を集めて、COREというグループが結成された。私は東京インターネットからそれに参加するようになった。ドメイン名の新規ビジネスが始まるところに参加しておきたい、と考えたからである。

COREの流れで、何回もの会合が持たれたが、東京でも1997年に開かれた。ISOCがこの流れを推進しようとしていた。WIPO（世界知的財産権機構）も参加して、ITUからRobert Showが出席していた。日本からCOREグループに参加したのは、数社であった。東京インターネットから私とセコムの新事業企画担当者、国際調達情報（PSI）からRobert Connellyさんがいて、いつもの会議で一緒だった。韓国からはKRNICの人々が来ていた。COREの事務局が認定した会員番号が、東京インターネットは88番だった。それを見た西海岸在住の中国系の人が、中国人がほしがる番号なので、譲ってほしいと、冗談か本気かわからないようなことを言っていた。

IAHCから、COREを始めPOCやいくつかのグループが生まれて、お互いに会費として資金を出し合って活動を開始していた。しかし、米国商務省DoCがその方向を認めるというようには進まなかった。DoCには、Ira Magazinerという男がいて、IANAのJon Postelと新しいIANAを作る相談をしていた。

それでDraft Bylaws（規約案）のバージョンがどんどん重ねられて、10月にICANNができた。村井さんが最初のBoardのメンバーになった。

ICANNの構造としては、IPアドレスを担当する部門と、ドメインネームの担当部門と、プロトコル担当部門というふうになっている。そのほかにAt Largeという一般会員の制度を持っていて、地域ごとにその候補者を決めて選ぶということをやってきた。At Largeの選挙というのは、皆さん覚えておいでかどうか、日本から加藤さんという富士通の公務でワシントン事務所におられた、富士通の知的財産権本部長が、この人が当選するときに、日本政府というか当時の郵政省が推進して競争をあおったということがあった。中国ではCNNICが投票した人間に抽選でパソコンを景品につけたということがあった。そんなことでいいのかという問題だった。

今のICANNはたくさんの問題を抱えている。多言語ドメイン名の問題、これは英語だけではなくて、ほかの言語でドメイン名を表記できるようにしようということになってきた。日本語でもドメイン名をつくれる。今ＪＰＲＳに依頼すると、例えば「高橋徹.jp」というドメイン名がつくれる。誰でも自分の母国語で表現ができ、必要に応じて翻訳するという当然の世界が、実現できることが望ましい。

ルートサーバ問題というのは、村井さんや東大の加藤朗さんが努力しているが、いまだに途上

国からの要求や何かで、13個のうちの10個がアメリカに集まっていて、あとの2個がヨーロッパにある。そのこと自体がけしからん、アメリカ中心主義ではないかと指弾する。それに応えて、同じミラードサーバをどんどん世界中に増やしていって、みんなが便利に使えるようにしようということが進んでいる。

At Large 一般会員のあり方はいまだに議論が継続になっていて、解決がついていない。会津泉さんたちがAt Large のグループで一生懸命がんばっているが、まだめどがたたない。

英語以外の言語の使用というのはどんどん進んできている。地域のレジストリ、例えばJPNICとICANNとの間の契約関係が成り立っているが、ほかの国ではなかなか進んでいないところもある。ＩＰアドレスを扱うレジストリがRIRs（Regional Internet Registries）となっていて、世界に5ヶ所ある。北米のARIN、南米とカリブ海のLACNIC、欧州のRIPE-NCC、アジア-パシフィックのAPNIC、それにアフリカのAfriNICである。これらもICANNとの契約が成り立ってきている。

また、どの会議に行っても英語を話す法律家が中心になっていて、日本語でものを考えるのには全然ふさわしくない環境になっている。これを何とか変えたいという思いがあるのは当然であろう。

現在のインターネットガバナンスの問題は、アメリカの指導によるインターネットガバナンスに対する批判がある。これはICANNが大体アメリカ政府の許認可によって存在する、アメリカの西海岸に存在するではないかというような批判である。それは現在の世界秩序が、アメリカによる支配形態というのが変わらなければならないと感受している人々がいて、そう訴えかける国々が途上国を中心にたくさんあることを映し出している。たとえばBRICsと呼ばれるブラジル・ロシア・インド・中国などの国々の、イラク戦争に対する態度の反映であったり、われわれが9.11の後の時代にいるという認識が、こういうところに現れてくる。それをPax Americana、（アメリカによる平和）というものの終焉であるか、これはおしまいになっていいのだと言う人もいる。日本にとっては日米同盟も終わりなのか、ということは問題になっていないようだが、途上国勢からするとそうではない。そういう勢いがICANNのような組織のありかたに疑問を投げかけてやっていると、私は感受する。インターネットガバナンスにそういう国際情勢すべてが影響してきているように見える。

WSIS（World Summit on the Information Society）という、世界情報社会サミットというのが開かれて、チュニスの 11 月の会議で終わったが、合意形成が非常に難しかったということである。11月16日に会議が始まる前に合意形成が何とか進んで、その結果、Internet Governance Forumというものを国連のもとに5年間継続して行うことになり、そこで議論を継続しようということになった。

日本の立場は、現在のICANNが民間の努力でやっていることを基本的に支持するということである。政府の関与は小さい方がよいといっている。BRICsというのが実際に力を持っていて、それにヨーロッパの連中は譲歩したように見えるが、それもこれも全部今後のIGF(Internet Governance Forum)の議論を待って進めましょうということになっている。

WSISの元にインターネットガバナンス・ワーキンググループ(WGIG)というのが設けられて、

坂巻さんという総務省のデータ通信課課長が委員に選出されていたが、また、その坂巻さんが登場する場面があるかもしれない。民間では、私たちは IGTF - J(インターネット・ガバナンス・タスクフォース・ジャパン)というのを JPNIC, IAjapan, JAIPA, JPRS の 4 組織を中心につくって、会津泉さんを事務局長に、毎回の WSIS の会議に対して日本からの意見を出して、世界中から注目を集めたので、一定の成果をおさめたと言えよう。

3.5.3 IPv6 の世界

さてそのインターネットプロトコル(IP)というのがすべての基礎であり、現在、Everything over IP と言われている。IP はパケットを配送する機能を持っている。IP パケットのヘッダーに IP アドレスがあって、その IP アドレスを見てルーティング(経路制御)などの処理が行われる。ルーターがルーティングを行うのは、その IP アドレスを見て宛先を識別し、宛先に向けてパケットを送り出す。現在まで IPv4(バージョン 4)を使っており、これからは IPv6 であると決まっている。IPv6 をどんどん採用しないと、世界の趨勢に遅れるということだ。IPv4 は 40 億とちょっとしかないので、IPv6 にならざるを得ないわけであり、この IPv6 の開発・実装というのは、日本がリードしてきたのである。128 ビット、2 の 128 乗の数だけあるわけで、これは 40 億という IPv4 の数に比べると天文学的な数字です。こういうところに情報がたまっていますが、私はインターネット協会の IPv6 ディプロイメント委員会の代表ということで、これを推進する立場にある。IPv4 アドレスというのはいつなくなるかという問題があって、この図がその予測を示している。(図入る)どんどんこのカーブが急になってきた。最初はリニアの予測で 10 年持つ予測だったが、どんどん前倒しになってきた。

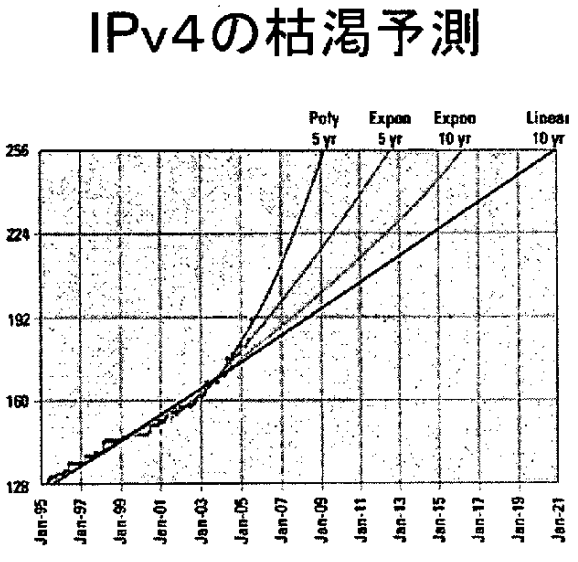


図 3.7 IPv4 の枯渇予測

最近の調査によると、あと 5 年ぐらいで危ないぞということが指摘されて、5 年足らずで枯渇

がどんどん近づいてきたことが明らかになってきた。そういう進行状態がある。

このIPv6の採用を日本政府のIT戦略に決めたのは、村井純さんが森総理の周辺に「IPv6というのがあるんだけど」と言ったら、「それは何だ」という話になって、IPv6を説明した。そのときに、日本が技術開発で先行していることがわかり、それで行こうと決まった。それをユビキタス社会の創出に使おうということになっていった次第である。

いま、OSやルーターなどのIPv6対応はできているが、日本がイニシアチブをとってきたことに対して、米国、EUおよび中国が急速に後から追いかけてきている。とくに米国の国防総省のディプロイメントが2008年とはっきりしているものだから、それに対して日本はどうするのか。日本の技術が標準化を推進していく中核にあり続けることができるか、その大きな課題を担っていけるのかということが日本の技術戦略上の問題である。

IPv6はモバイル関係とか移動体通信、自動車のITSに使われて、IPv6のインプリメントが進んでいる。家電のネット対応でIPv6を使うことも日本発で進んできている。いろんなセンサーネットワークが細密化されて、どんどん進むが、これは各センサーにIPv6アドレスを振って連携して使うという意味で、IPv6がないとうまくいかない。ベッドの各所にセンサーを置いて、生体の異常検出にIPv6を使うというふうな、あらゆる場面でIPv6のアドレス体系がうまく使われていくだろう。

私たちは2000年の暮れから毎年IPv6サミットをやってきている。地域サミットというのもやっている。2003年と2005年の12月にはInternet Weekでテクニカル・サミットを開催した。その間、2004年にはビジネス・サミットというほうに焦点があたってきたが、2006年の2月15、16日に秋葉原のコンベンションセンターでGlobal IP Business Exchangeが開催された。これには、実際にディプロイメントした事例とか、具体的な話がどんどん出てきている。いろいろな産業分野でIPv6を取り込んだ事例が出てきた。地域サミットはいろんな展開をしていますが、3月には富山でやるということになっています。国際的にも先週は東京でＡＰＡＮの会議が行われて、その中でアジアパシフィックのＩＰｖ６タスクフォースの会議も行われました。今月はオーストラリアのパースでＡＰＲＩＣＯＴの会議が行われて、これは去年、京都でやって大成功した流れがあるので、日本からも参加者をたくさん出したいところだ。

IPv6普及・高度化推進協議会の提供による資料を講演では使ったが、http://www.v6pc.jp/に多くの資料が置かれている。米国の話が最初にあって、これで見るように2008年までということで進んでいる。今すぐ対応しないと、日本は米国政府のネットワークから5年分遅れるということになってしまう。

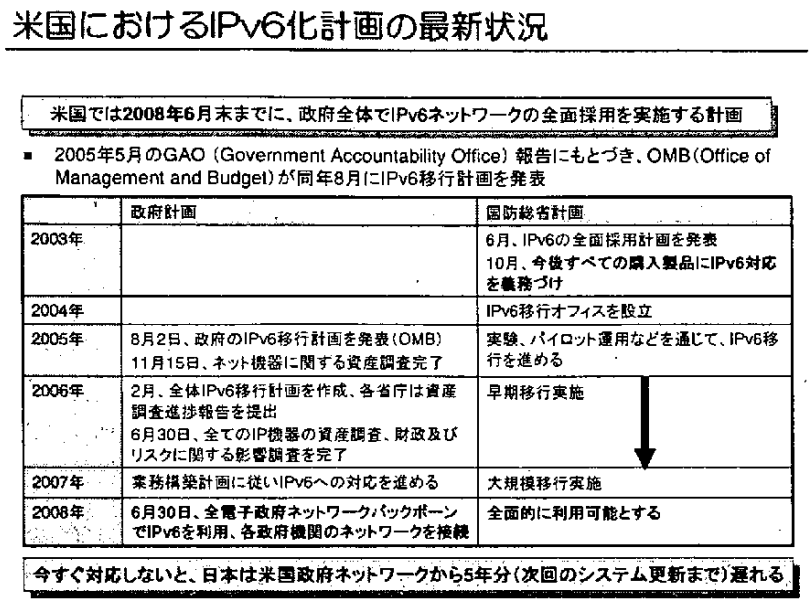


図 3.8　米国における IPv6 化計画の最新状況

また、IPv6 を採用するメリットとしてはセキュリティなどがある。IPv6 で実現する E2E のセキュリティなどが含まれる。アドレスの配布数が非常に大きいため、少ない IP アドレスを節約するのに NAT を使わなくてもいいということが大きなメリットになってくる。NAT が IPv4 のプライベートアドレスを内部で使い、外部に出て行くときだけグローバルアドレスに翻訳して使う。NAT を多用すると元のアドレスが何か分からなくなるということがおきる。そのため IETF では NAT is Evil などと言われたりしていた。IPv6 を使えば、そんな NAT を排除できる。

IPv6 と IPv4 の IP 電話の場合の対照表ができている。IP 電話の v6 移行の基本イメージがこのように読み取れるのである。

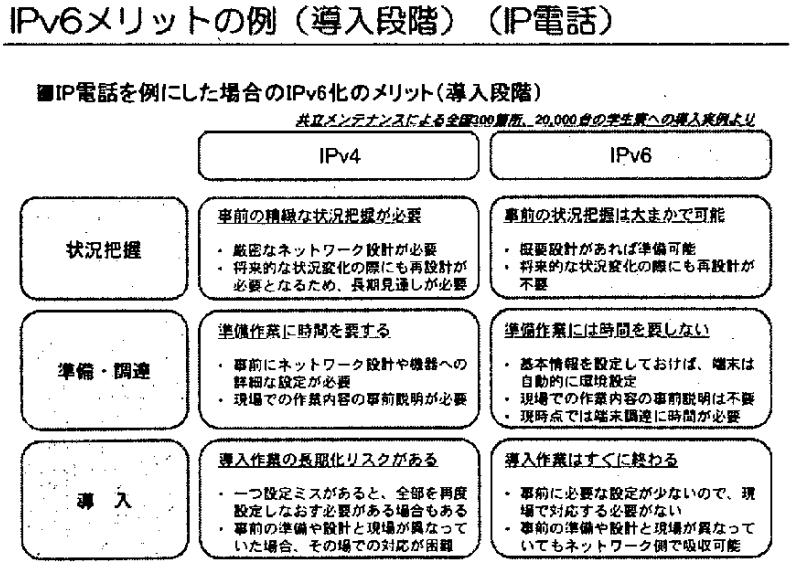


図 3.9　IPv6 メリットの例（導入段階）（IP 電話）

環境分野でも取り組みが進んでいる。そのひとつにLive E! プロジェクトが総務省の予算でもって行われていて、「デジタル百葉箱」の実験がある。多くの学校などの施設にデジタル百葉箱を置くと、地域の気象データが克明に採取できる。

そのほか防災分野でのＩＰｖ６の必要性というのがある。これは行政機関の縦割りシステムを横にくし刺しにしてきちんとやろうという話になってきている。

それから、移行実証実験として医療関係、たくさんの事例がある。ほかにもいろんな実験が行われている。ぜひ見て欲しいものだ。

3. 6 コンピュータ関連設備からの事業継続

現在、情報処理は IT 機器の安定稼動に拠るところが多大である。コンピュータの安定稼動に必要な条件、設備設計に当たり考慮すべきことを述べてみたい。

現実には、事業継続を考える場合、運用が中心になり必要不可欠である関連設備の検討が最後になるか忘れがちになるのが現状である。関連設備の不具合が生じた場合、その原因を見つけるのに多大な時間を費やし、復旧作業にもかなりの時間を要する。場合によっては、付帯設備そのものの入れ替えも行わなければならなくなる。以上のことから事業継続が不可能になる事が想定され、自社のみならず関連各企業にも多大な迷惑を掛けることになる。関連設備の不具合の発生とバックアップ及びその対応について注意しなければならない項目を説明述べさせていただきますので参考にしていただき、事業継続に役立てていただきたい。

3.6.1 建屋関連

1.1 建屋を選択する条件は

1)落雷の少ない場所

2)地震の被害が少ないと想定される場所

(第一種地層――岩盤――の上が理想的)

3)過去に水の被害があった場所

(湖沼の近くや河川の近くを避ける)

4)崖等の下

5)電気事情が良い所

6)近辺にレーダー等の施設が無い場所

7)社員等の交通手段が確保できる場所

等の場所を避けることが必要です。

しかし日本国内では避けることが不可能な場所もあり対策の検討が必要になります。

その対策に関しては各項目で述べさせていただきます。

1.2 落雷の少ない場所とは

これらを見極めるには理科年表等を利用し年間における雷の発生等を調べます。

1.3 地震の被害が少ないと想定される場所とは

日本国内において地震が発生しない場所は皆無と言っても過言ではないでしょう。日本は地震国であり、国内至る所で活断層の存在が確認されています。　最小限これらの活断層の上または近辺を避けるべきでしょう。

1.4 過去に水の被害があった場所とは過去に水害や河川の氾濫があった場所であり、その被害を調べ、極力避けるべきです。

1.5 崖等の下とは自然の崖、造成地によって出来た崖であり、土砂崩れ等の被害を避けるため崖の下や近辺の建物は避けるべきです。　以上が自然に対しての建物選択の最小条件です。

1.6 電気事情が良い所を選択するために電気が安定して供給される場所を選ぶことが必要です。コンピュータ機器の稼動には電気が欠かせません。 日常的に電圧の変動や低下が有っては安定稼動に影響をきたすからです。

1.7 近辺にレーダ等の施設が無い場所とは、航空機用レーダ等が有る場所をいい、この影響によりコンピュータの動作に影響が出るからです。 レーダのアンテナの回転により間歇的に機器の誤動作が起こります。これを防ぐためには建物の電磁シールドを行う必要があり、対応が難しいです。

1.8 社員等の交通手段が確保できる場所を選択しなければならないのは、彼らが通勤するための手段が悪ければ、意欲的に働かなくなるからです。 従業員の高い質と意欲が無ければ企業活動は落ちること確実です。

以上が建物を建てる場所等の条件になります。

3.6.2 建物における対策

2.1 建物は、上記 1.の条件に加え防火２21 対策、防犯・防災対策が必要になります。

2.2 防火対策

建物に於ける防火対策の最初は近隣からの延焼を考えなければならない。 その対策とは、建築基準法に定められている建物間の離隔距離である。 この離隔距離を守ることにより類焼を免れるのである。

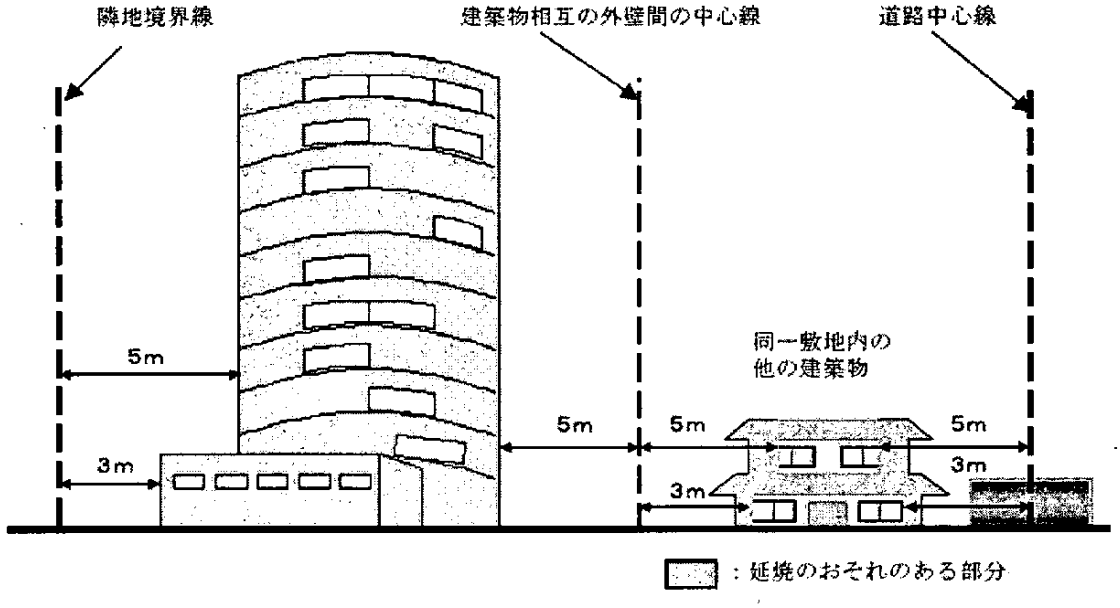


図 3.10 離隔距離のイメージ図

次に考える事は、建物が耐火構造物でなければならない－建築基準法（第２条９の２）－事である。

その基準とは；

耐火性能に関する技術基準（建築基準法施行令第１０７条）

次の表に掲げる建築物の部分にあっては、

当該部分に通常の火災による火熱がそれぞれ次の表に掲げる時間加えられた場合に、構造耐力上支障のある変形、溶融、破壊その他の損傷を生じないものであること。

表3.1 建築基準法施行令第１０７条

建築物の階 / 建築物の部分		最上階及び最上階から数えた階数が２以上で４以内の階	最上階から数えた階数が５以上で１４以内の階	最上階から数えた階数が１５以上の階
	間仕切り壁（耐力壁に限る）	１時間	２時間	２時間
壁	外壁（耐力壁に限る）	１時間	２時間	２時間
柱		１時間	２時間	３時間
床		１時間	２時間	２時間
はり		１時間	２時間	３時間
階段		３０分間		
屋根		３０分間		

その他参考法令等；

建築基準法　第２条

〃　第６条

〃　第７条第５項

建築基準法施行令第１０７条

〃　第１０８条

〃　第１０８条の２

〃　第１０８条の３

〃　第１０９条

消防法施行　第二款

〃　第三款

2-3 外部からの水による被害を考慮する；

立地条件及び設置環境を考慮し、水による情報システムへの被害を防止し事業継続を確保することが必要になるからです。

具体的には下記の項目に注意しなければならない；

1)建物の選定にあたっては、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での設置を避ける。

2)電源室及び空気調和室等の関連設備は、地下室内に設置することを避ける。

3)建物開口部に防水扉を設ける。

雨水に対する対策も考慮する必要がある

1)建物は、十分な防水性能を確保する。

2)屋根、外壁及び窓等は、防水施工を行う。

・屋根、外壁等を貫通する吸排気口、ダクト、配管等の周りは防水施工を行う。

・排水口及び配管等でつまり、逆流防止の対策を講じ、排水性能を確保する。

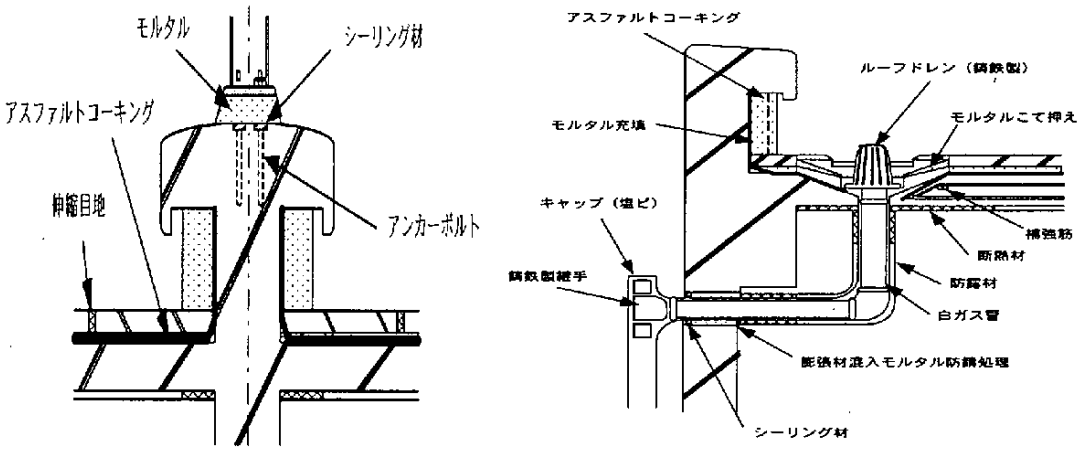


図 3.11　防水工事の施工例

2.3 建物における地震の考え方は；

建物周辺の地盤の強弱、活断層の有無等の立地条件と建物の構造（剛構造か柔構造等）を把握し、必要な対策を講じ、地震による情報システム等への被害を防止することを目的に対処することになる。

その対処方法は；

地震による被害のおそれのある地域での立地を避けることが最良ですが現実味はありません。

ではどの様な対策を考えるか？

2-3-1 建物の構造・機能での対策を講じる事になります

1)建物の構造及び機能面において地震対策（耐震・免震・制震構造）を講じる

2)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－設置階の話

また、上記対応と共に考慮することは

1)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する

2)地震感知器を設置し、監視システムと連動させる

3)装置及び機器において地震対策を講じる

4)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

5)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

等忘れてならない項目があります。

参考までに過去の大きな地震を記す。

地震名または震源地	発生年	地震の規模 マグニチュード（M）	地震計		
			設置場所	震央地までの距離（km）	測定値（gal=cm/s²）
エルセントロ	1940	6.7	エルセントロ	8	NS;341.7 EW;210.1 UD;206.4
タフト	1952	7.7	タフト リンカーンスクールトンネル	43	NS;152.7 EW;176.0 UD;102.9
十勝沖	1968	7.9	八戸港湾	179	NS;311.7 EW;206.2 UD;135.4
宮城県沖	1978	7.4	東北大学建設系研究棟	116	NS;258.2 EW;202.6 UD;153.0
兵庫県南部	1995	7.2	神戸海洋気象台	直下型	NS;818 EW;617 UD;332
平成15年（2003年）十勝沖	2003	8.0	幕別町本町	138.8	NS;754.2 EW;874.2 UD;217.0
新潟県中越	2004	6.8	川口町川口	2.5	NS;1141.9 EW;1675.8 UD;869.8
福岡県西方沖	2005	7.0	前原市前原西	20.7	NS;386.1 EW;706.1 UD;302.2
宮城県沖	2005	7.2	宮城川崎町前川	未入手	未入手

図 3.12　過去の有名な地震

さらに忘れてはならない対策は、振動に対策です。

地域の選択による；

1.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。

1)鉄道の近傍に建物が設置されている

2)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

3)機械プレス、油圧機等が稼動している特定施設が建物に隣接して設置されている

建物の構造体等による対策；

2.建物の構造・機能面での対策を講じる。

1)建物の構造上から耐震設計を図る。

2)室の床を振動の影響を受けにくい免震床構造とする。

3)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。

表 2-3　振動規制対象の発生源

1	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以上のもの)　　d.鍛造機 e.ワイヤーフォーミングマシン(原動機の定格出力が37.5kw以上のもの)
2	圧縮機(原動機の定格出力が37.5kw以上のもの)
3	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)
4	織機(原動機を用いるもの)
5	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)並びに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が10kw以上のもの)
6	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以上のもの)
7	印刷機械(原動機の定格出力2.2kw以上のもの)
8	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、原動機の定格出力30kw以上のもの)
9	合成樹脂用射出成形機
10	鋳型用造型機(ジョルト式のもの)

2.4 建物を電磁環境から保護する；

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事を目的とし対策を立てます。

その対策の例は；

1)電界及び磁界からの被害のおそれのある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

2)建物の構造・機能面での対策

□建物全体に電磁遮蔽

□各室で電磁遮蔽

□信号ケーブルは、シールド付を使用

□電力ケーブルは、金属管配線として信号ケーブルと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る

その他影響が考えられる物に携帯電話が

ある。　携帯電話の出力等は；

表 3.2　携帯電話基地局、ＰＨＳ基地局の代表的な電界環境（計算値）

無線基地局アンテナ	代表的出力	アンテナから距離１００ｍの電界強度（ｄＢ）	周波数
携帯電話基地局	９６Ｗ	１１５（0.54V/m）	９００MHｚ帯
ＰＨＳ基地局	２Ｗ	９８（0.08V/m）	１．９GHｚ帯
大出力ＶＨＦテレビ放送局	８５kW	１４４（16.0V/m）	９０－２２０MHｚ帯

(総務省　電波防護指針)

落雷に関しての注意事項；

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。

2-5 腐食性ガスの対応も必要である

建物の近隣に科学工場等が存在する場合、

排出される恐れのある腐食性ガスの対策を考慮する必要がある。　その目的は、大気汚染による情報システムへの被害を防止する事である。

その対策は；

1.大気汚染からの被害を受けやすい地域を避ける。

1)化学物質・粉塵等の被害を受ける恐れのある地域

2)排気ガス等の被害を受ける恐れのある地域

3)塩害の恐れのある地域

4)火山・温泉地域

2.建物の構造・機能面から対策を講じる。

1)腐食性ガスの除去装置を設置

2)集塵装置を設置

3.情報システムに影響を与える因子；

1)腐食性ガス（亜硫酸ガス、一酸化炭素、塩素、オゾン等）

2)化学物質（酢酸、クロオフォルム等）

3)塵埃

4)海塩粒子 ある。

表 3.3　腐食性ガスの種類と発生源

発　省　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	二酸化硫黄（SO_2）

場の排出ガス ・ゴミ焼却場排出ガス	
・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,NOx)
・化学工業、製紙工業の排出ガス ・上水処理場の大気	塩素 (CI2)
・化学肥料工業の排出ス ・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（O3）

2-5 今までは建物自体での対応を中心に述べてきましたがこれ以降は建物の防犯・防災を中心に事業継続に必要な対策を考えてみたい。　初めに、不法侵入等の犯罪による被害を受けない措置を講じる方法と考え方を述べる。

1.敷地における対策(不法侵入等);

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

2.建物における対策;

1)外部に面する壁、扉及び扉枠は、容易に破壊されない構造

2)隣接する建物等から屋上、窓等への侵

入を防ぐ対策

3)非常口は、防犯錠を使用し、不法侵入

を監視する設備

4)窓等の開口部は、防犯ガラスを使用

5)出入口以外で、１階等で外部から侵入

の恐れがある窓には、防火戸又は防犯センサーを設置

6)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

3.建物、室の機能、用途が外部から察知されないための対策

1)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。

2)室の入口に室名を表示しない。

3)館内、エレベータ等の案内板に室の位置を表示しない。

4)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。

2-6また、注意を払わなければならないことは；

1.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

2.駐車場、駐輪場等からの不法侵入に対しても配置し構造等に留意する。

3.監視設備についても考慮する

4.パンフレットやホームページに室の位置がわかる図面を掲載しない。

5.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し、樹木や植栽の成長にも留意する。

2-7入退館管理を実施することにより立地条件、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

その方法とは；

1.入退者を認証し記録する機能

1)機械による場合は、次の機能を有する設備

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

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

2.許可された者だけを通過させる機能

1)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。

3.制御機器、電気錠は、停電対策を講じる

上記対策とともに考慮する項目があり、

あわせて対応をしていただきたい。

1.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

2.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

3.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

4.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
5.入退管理設備の配線は、ノイズ・切断等
の対策をする
6.自動扉の場合は、非常電源を設置する
7.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。
・監視機能付のフラッパーゲート、ター
ン式ゲートを設ける。

図 3.13　フラッパー・ターン式ゲート

8.機器類の保守点検についてあらかじめ
メーカと検討しておく

参考

1.個人識別の方法

1)生体認証・・・・
網膜・指紋・静脈・顔等による識別

2)筆跡認証

3)媒体認証

①接触式・・・・
磁気カード式、ホログラムカード式、
ＩＣカード式

②非接触式・・・
ＲＦＩＤ式

③テンキー（個人認証ができるもの）

上記管理方法を図に纏めると添付図になる

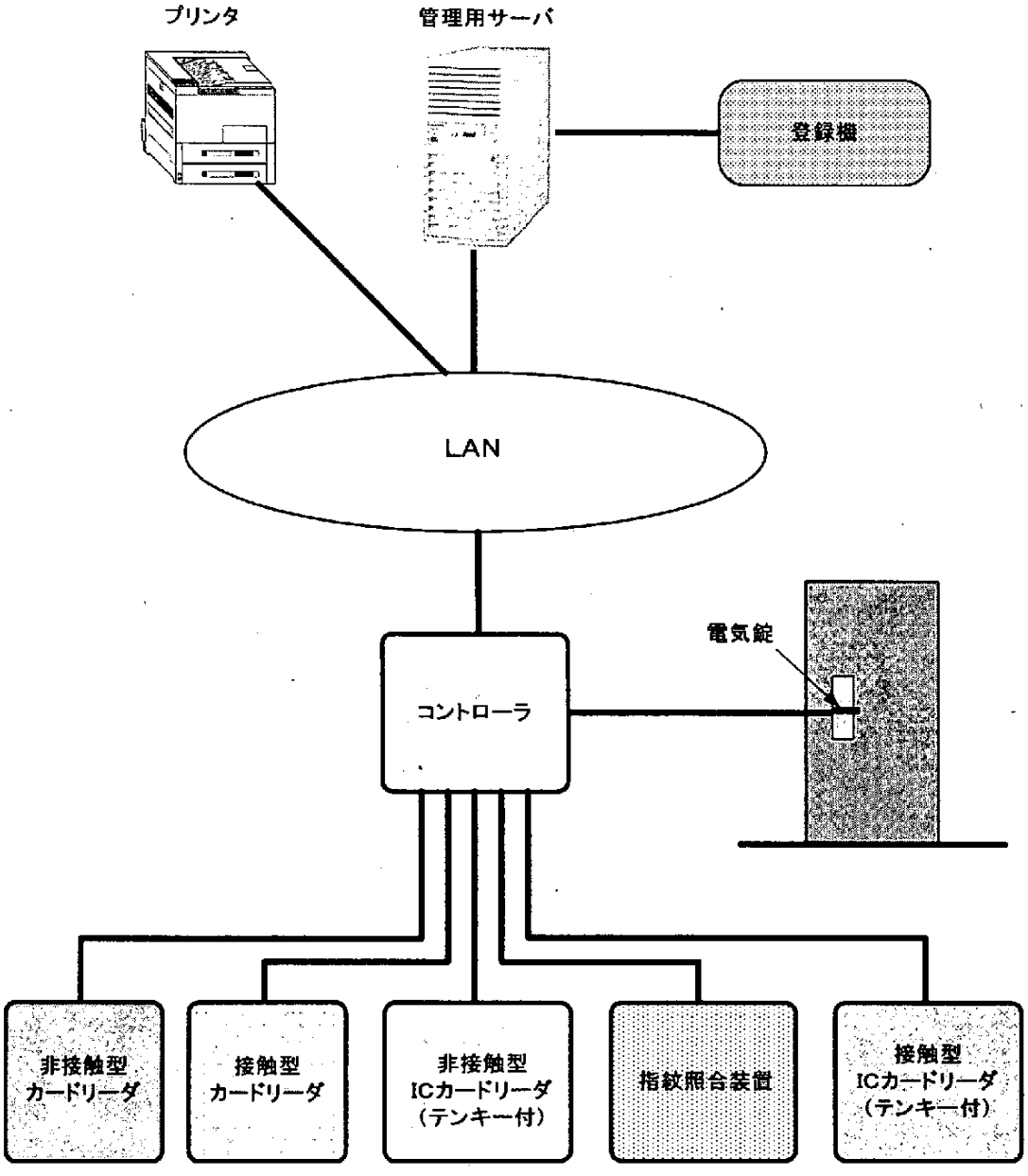


図 3.14　入退管理イメージ図

その上、災害及び犯罪を監視する措置も考
慮する必要がある。

考慮することは；

1.防災設備からの警報（火災・地震・
漏水）を監視する設備

2.防犯設備からの警報（ガラス破壊・不法侵入・扉と窓の開放）を監視する設備

上記設備に関しては以下のことに注意；

1.常時監視し、速やかに対応できる体制

1)監視設備を防災センター 、中央監視室等に設置

2)監視の場所が無人となる場合は遠隔監視などの代替監視の処置

3)ビル管理会社、警備会社等と連携する。

2.定期的に巡回し、異常を監視する

同じ監視でも電源や空気調和設備の監視等

は詳細に渡ってくる。 その対策は；

1.稼働状況（定常・異常）を記録する

1)電源設備：電圧・電流・周波数

2)空調設備：温湿度・風量・圧力・液面警

報・漏水

2.異常が発生した場合の警報受発信

1)設備設置場所での警報（ランプ・ブザー）

□設備設置場所でのランプ、ブザーによる警報

□監視設備設置場所での警報受信

□管理責任者への発報

3.定期的に巡回する

1)稼働状況の確認と記録

2)管理責任者への報告

以上を確認し建屋側から見た事業継続を図らなければならない。

対応策の令として；

1.情報システムのバックアップセンターを

設ける

2.情報システムのデータ等を別の場所に

保管する

2-8通信関連の考慮点

ネットワーク機器及び関連設備は、外部からの影響を考慮しその対策を行わなくてはならない。 そ

の対策と考え方は；

1.浸水対策

1)架空配線

2)防水加工を施した埋設管路、ピット、トラフ、共同溝に配線

3)防水加工をしたコルゲートケーブル等を直接埋設

2.火災対策

1)金属管を用いて配線

2)難燃性ケーブルを用いて配線

3)ケーブルには延焼防止剤の塗布／不燃材を用いて養生

3.電磁界の対策

1)光ケーブルを用いて配線

2)金属管等でケーブルをシールド

3)シールドケーブルを用いて配線

4.雷対策

1)光ケーブルを用いて配線

2)アレスタを設置（通信系・電源系）

3)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（機器の接地とは接続しない）

5.地震の対策（別途記載あり）

1)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

2)搭載している機器の移動／落下（飛び出し）防止対策

3)配線は余長を持たせ整理し固定

上記内容に下記のことを加味した対策；

1.寒冷地の管路内凍結でケーブル断線

2.屋外無線通信は降雨,積雪,濃霧等の気象条件による通信障害の対策

3)電波塔,レーダーアンテナ,高圧線等

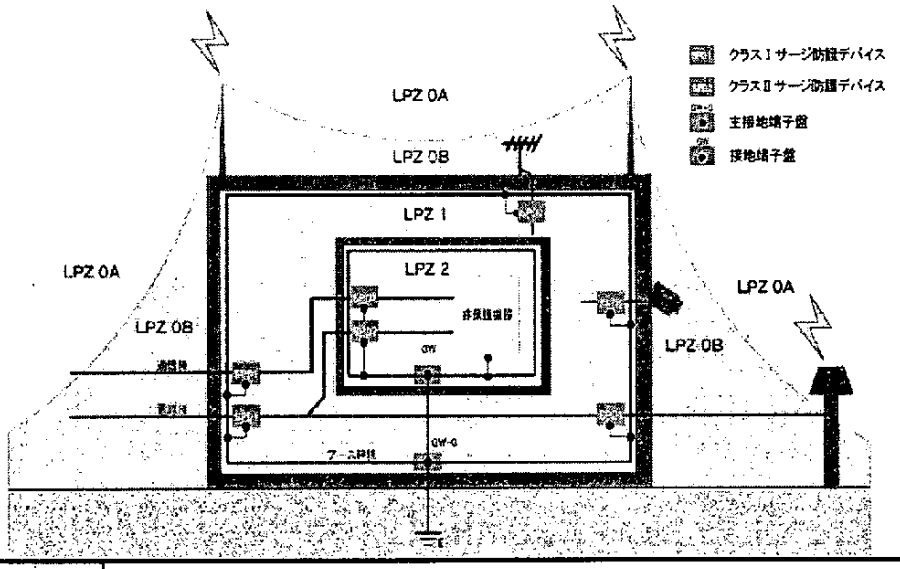
4)ラックの地震対策とはラック自体の移動・転倒防止とラックの強度

5)腐食性ガスの影響

6)用途により難燃性ケーブルを選択

7)建物の重要度に応じた雷保護レベルについても考慮する。また建物内をいくつかの雷保護領域（ゾーン）に区分けし、ゾーン毎にアレスタを選択

下記の図は雷対策の例として記す。



LPZ 0A	直撃雷にさらされ、全雷電流が流れる可能性がある領域
LPZ 0B	直撃雷にはさらされないが、発生する電磁界は減衰しない領域
LPZ 1	外壁内など直撃雷にさらされない領域で、この領域内の導電性部分に流れる電流は、領域0Bに比べて減少する。
LPZ 2	コンピュータールームなどのように、電流及び電磁界の影響をさらに減少させる必要がある場合には、建物内に遮蔽を施した部屋を形成した空間。さらに保護を強化する場合はLPZ3などを設定する。

図 3.15　雷とアレスタの関連

また、室内に設置されているネットワーク機器と内装にも配慮が必要である。

室内はコンピュータ室と同様不燃物又は準不燃物を用いた内装で、特定者以外の者が機器や配線に近づけない方法を取る必要がある。

同時に、ネットワーク機器への安定した電気の供給が必要になる。

その方法とは；

1.負荷変動の激しい機器と共用しない

2.重要なネットワーク機器の電源は；

1)ＵＰＳと自家発電設備

2)ＵＰＳを使用

3)情報システム専用の変圧器を使用

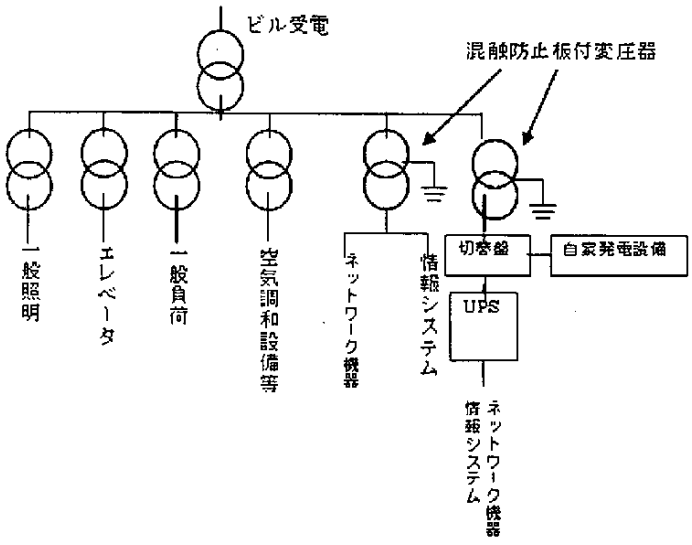


図 3.16　安定運転用電源イメージ

2-9 イメージ図の電源を使用するときの留意；

重要なネットワーク機器の電源は；

1.ＵＰＳと自家発電設備

2.ＵＰＳを使用

3.情報システム専用の変圧器を使用

4.停電回復時に商用電源の安定供給を確認すると共にＵＰＳバッテリの充電時間を考慮し自家発電設備を停止

5. ＵＰＳのバックアップ時間は情報システム側が要求しているＵＰＳバッテリのバックアップ時間に準じる

6.相互にノイズ・負荷変動・もらい事故等のシステムのリスクを考

2-10 熱溜（ラック内）に留意する

近年ラックに搭載するサーバー機器の発熱量が増大している。　そのため、ラック内に熱溜が出来機器に重大な影響を与えるケースが増えている。　これを解消しなければ事業継続に重大な影響を与える要因の一となる。　正しい処理の方法として；

1.ガラリに拠る対応

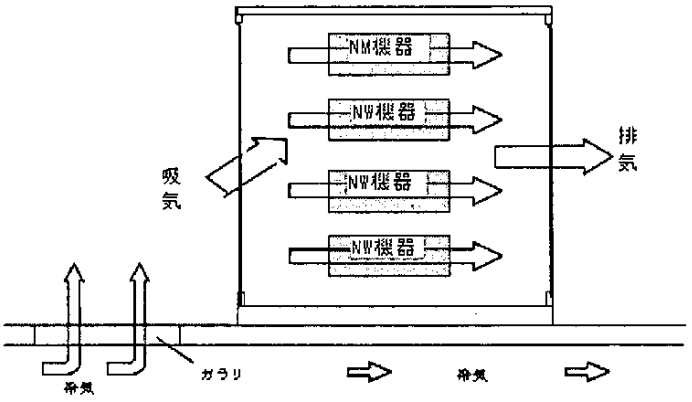


図 3.17　2.ファン内蔵型ラック

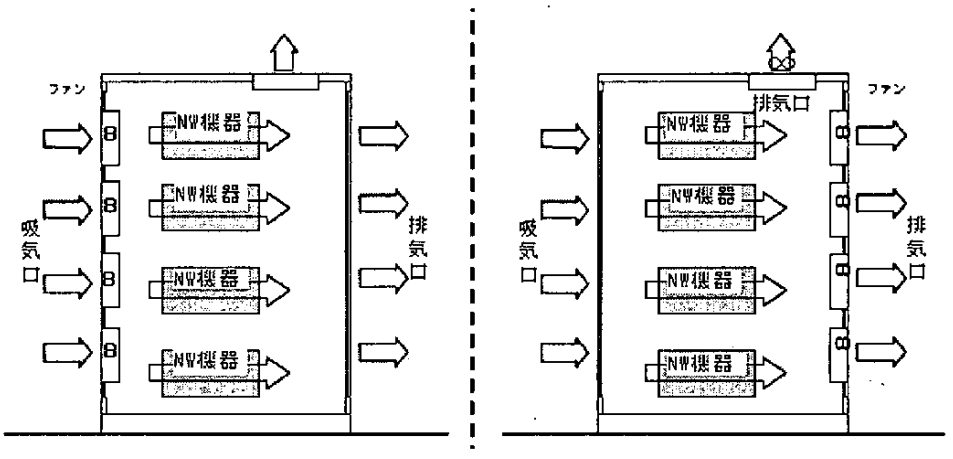


図 3.18　吸気ファンの例　排気ファンの例

3.最新情報では冷水を利用したラックにより熱を取り除く様になってきている

4.給気口を向かい合わせて設置した例

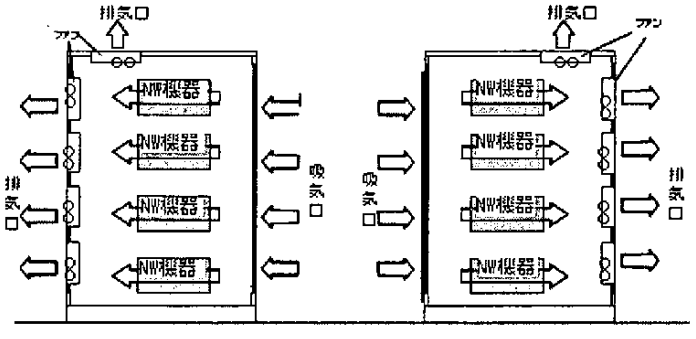


図 3.19　給気口を向かい合わせて設置した例

3.6.3 コンピュータ室における対応

（外部からの浸水、振動による被害、電界及び磁界の被害、外部からの腐食性ガス等は説明を省く）

3-1 コンピュータ室は独立した専用の部屋とし　　て、入退室管理を行い許可された人以外の出入りによる影響（防犯等）を排除する

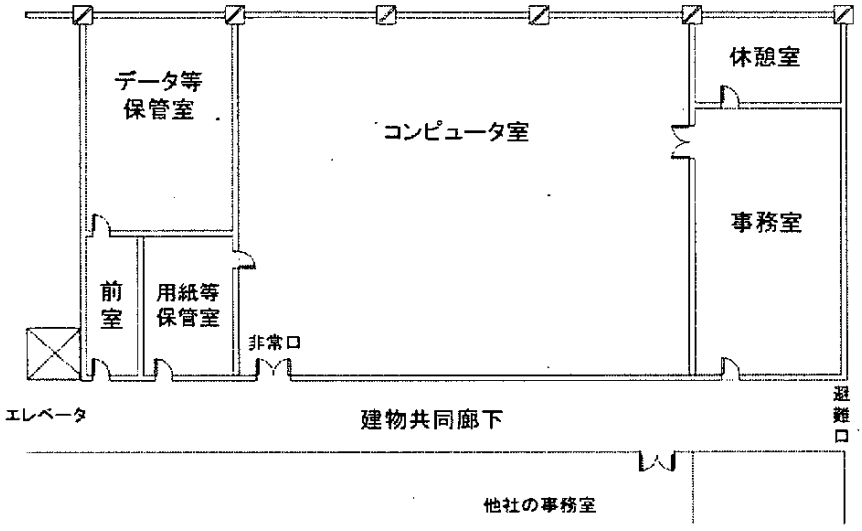


図 3.20　独立した部屋の例

3-2 不法侵入や危険物投げ込みの対応

外部及び共用部に面した開口部からの侵入　　や危険物の投げ込みからの被害を防止する対策を講じ、機器への影響を排除し事業継続を確保する。　その対策は；

1.外部に面した窓等の開口部は

1)無窓

2)防火シャッター、防火戸、鉄扉を取り付ける

3)耐火ボードで覆う

4)外部から見えない様な措置を講じる

2.共用部に面した開口部の対応

外部に面した開口部と同等に対応が必要

3.室は建築基準法で定められた防火区画

1)壁は耐火構造とし上下階のスラブまでを区画とする

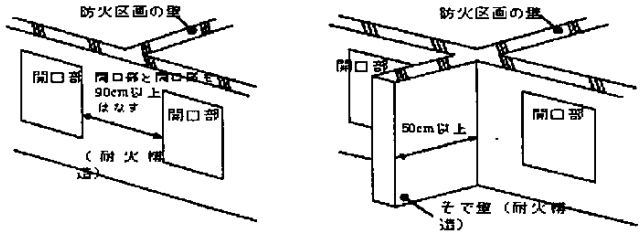


図 3.21　耐火壁の例

4.コンピュータ室は非常口を設けなければならない。　室に２箇所以上の非常口を設けることにより、災害時の避難を容易にし、人的資源の確保を行い事業継続に必要不可欠な人員を確保する事が可能である。

5.室の内装等は不燃材、準不燃材を用い延焼等を防ぎ安全を確保する。

6.室にはウイスカが発生する恐れがある部材を使用しない（特に電気亜鉛メッキを施した部材はウイスカが発生しやすく、ウイスカが機器内部に入り込むと電気的影響が発生する）。

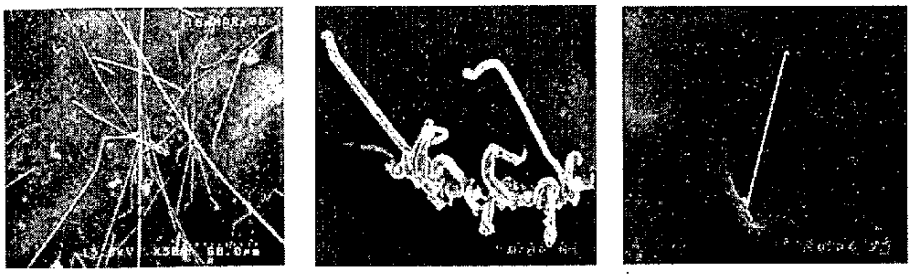


図 3.22　ウイスカの写真

ウイスカの大きさは太さ約２μ、長さ２mm以上に成長する（一般のフィルタは通過ししまい機器への浸入は止められない）

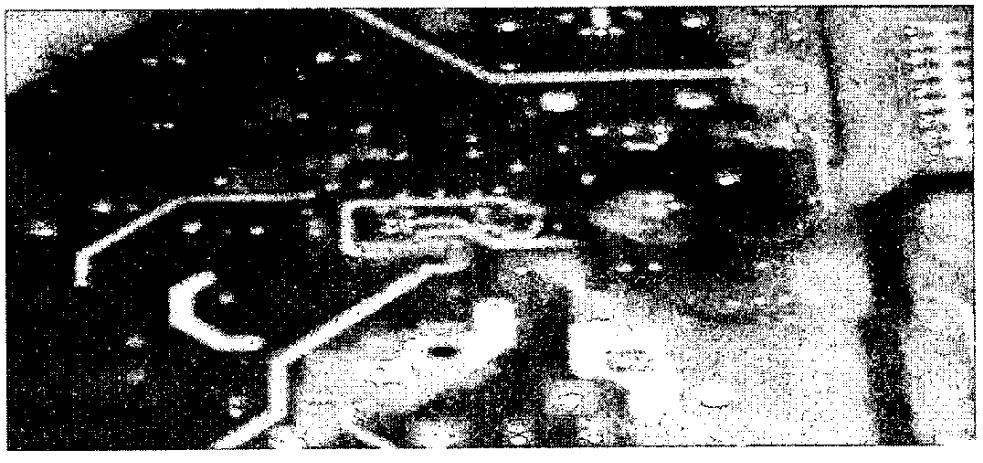


図 3.23　ウイスカの影響を受けた短絡事故例

一般的にウイスカによる障害は一過性の原因不明障害として処理されることが多い。

ウイスカの対策は；

1)ウイスカの発生しない部材に入れ替えるか、新たに室を作る

2)床下等の清掃による対応（２年周期での清掃がひつようになる）

3)清掃＋養生（支柱等ウイスカの発生している部材にカバーを掛けて対応）

大別して３通りの対策がある。

7.室内の温湿度を管理し静電気の影響を排除すると同時に床パネルに帯電防止の措置を講じ、

放電による影響を排除する必要がある。 この放電による影響は電気的に弱い処に現れるため原因不明の障害になり、事業継続に影響を与える原因の一つになる。

8.地震による影響を排除する必要がある。

1)天井、照明器具、間仕切壁、二重床は地震により倒壊しない対策を施し、人身及び情報機器への影響を排除し事業継続を可能にする。

対策は；

1)照明器具の固定例

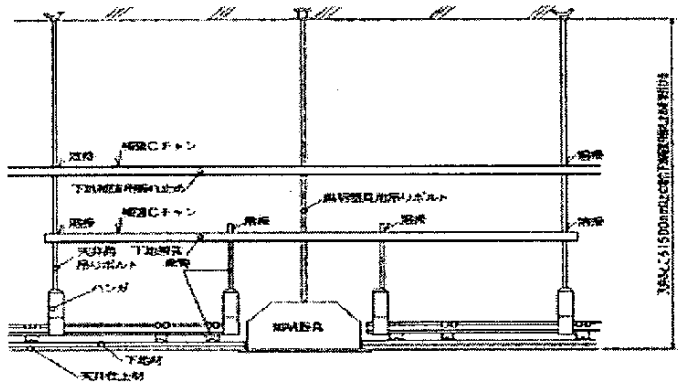


図 3.24　照明器具固定例

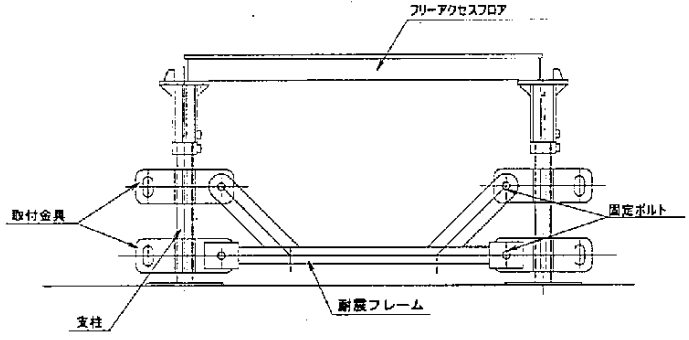


図 3.25　床支柱耐震対策例

9.コンピュータ機器の移動転倒防止

機器の移動転倒防止対策を行い機器の安定稼動を図り人身の安全と機器の安定稼動を確保することが必要である。　この対策は、機器設置階に於ける想定入力加速度を基準に対策を考える必要がある。

1)免震ビルに設置する

2)免震床に設置する

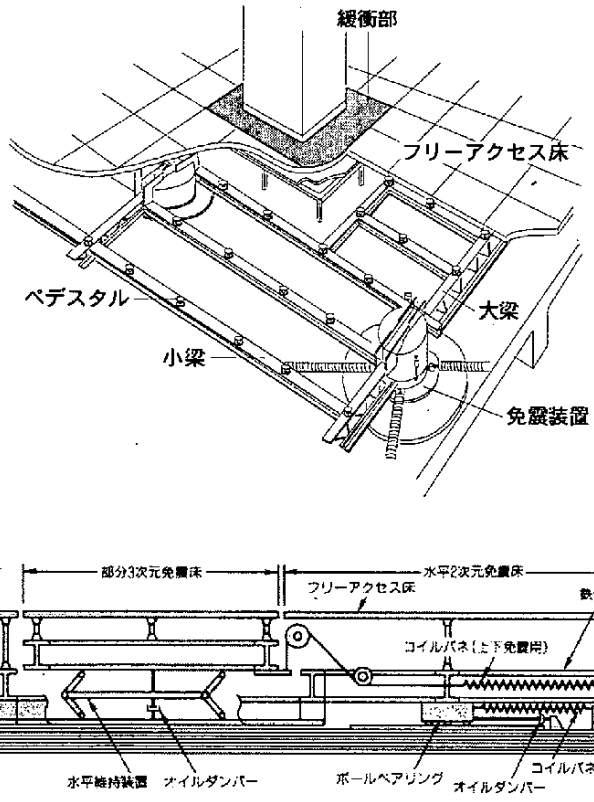


図 3.26　免震床の例

3)制震台等による対応例

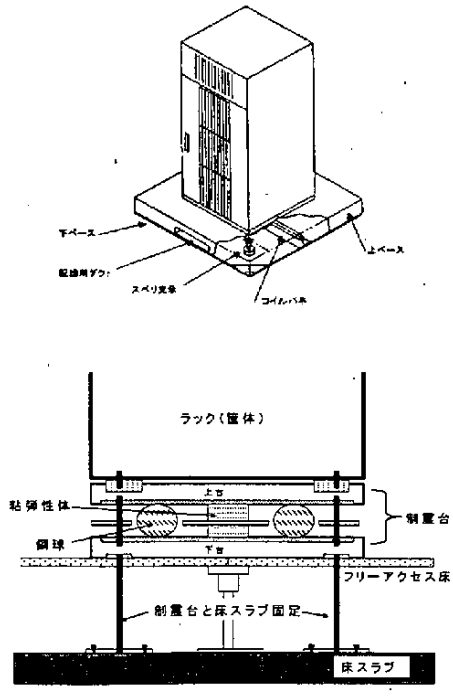


図 3.27　免震台設置例

3)機器により適切な方法（メーカ推奨方式）を選択し対応する

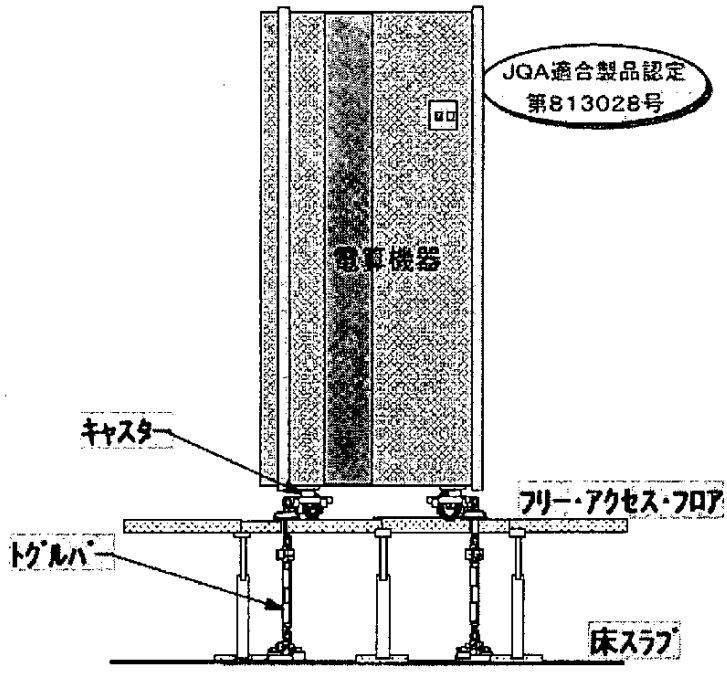


図 3.28　メーカ方式　の例 1

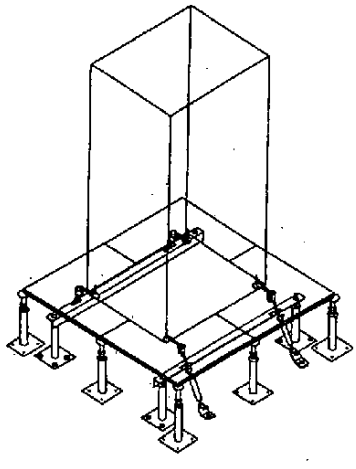


図 3.29　メーカ方式　の例 2

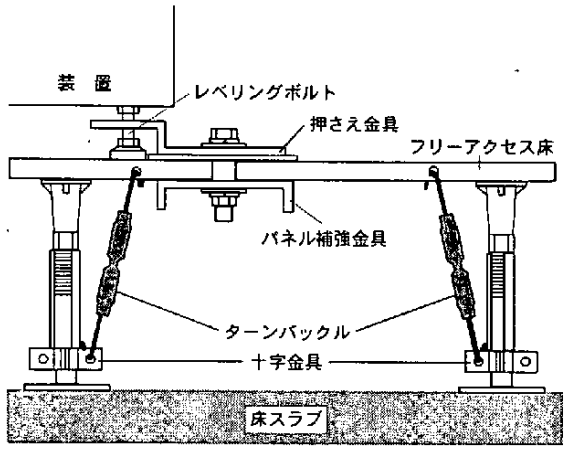


図 3.30　メーカ方式　の例 3

この様な対応は必要であるが機器の運用を続けるかの判断基準は地震感知システムとの併用で判断するべきである。

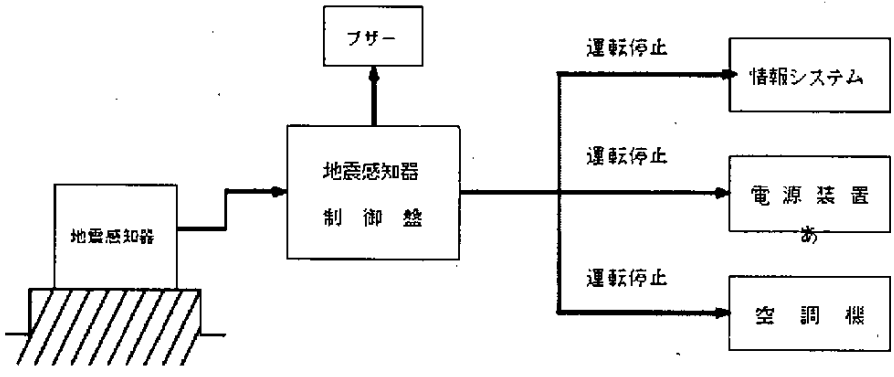


図 3.31　地震感知システム例

10.コンピュータ室には携帯電話を持ち込ませない措置が必要である。　携帯電話を使用し、機器に影響を与えた事例が報告されている。　何気なく持ち込んだ携帯電話の影響で業務遂行が出来なくなり原因究明にかなりの時間が費やされた事例がある。　また、外見では携帯電話とＰＨＳとの差は判断できないので持込禁止にするべきである。　持込禁止にした場合、コンピュータ室内で使用している内線電話の使用許可を出すべきである。　最近では内線電話にＰＨＳを使用している企業が増えている。　携帯電話とＰＨＳの出力の違いによりＰＨＳ（携帯電話の約十分の一の出力）の影響を受けないからである。

11.端末やネットワーク機器からの漏洩電波による情報漏えいも考慮しなければならない。対策は電磁シールドをどの様に選択するかであり詳細検討が必要。

12.情報システムにノイズ誘起されないよう

配線等に電磁遮蔽を行い、原因不明のシステム障害の発生を防ぐ。

13.電気の質を一定に保つことが必要。

瞬停、瞬低、停電、周波数の変動に注意　し、機器の要求する電気の質を確保し、障害を未然に防ぐような措置が必要である。

14.万が一漏洩電流が感知されても、電路を遮断しないような措置が必要である。

遮断した場合、システム全体が止まる可能性があるからである。　その対応は、漏電遮断器を用いず漏電警報機で対応するのがよい。

15.コンピュータシステムの接地は確実に設け、他の機器からのノイズ等を排除し、機器の安定稼動を図る。　接地の現状は

専用接地を施しているが国際標準の取りこみ（ＪＩＳに取り込まれた）で共用接地方式に注目が集まっている。

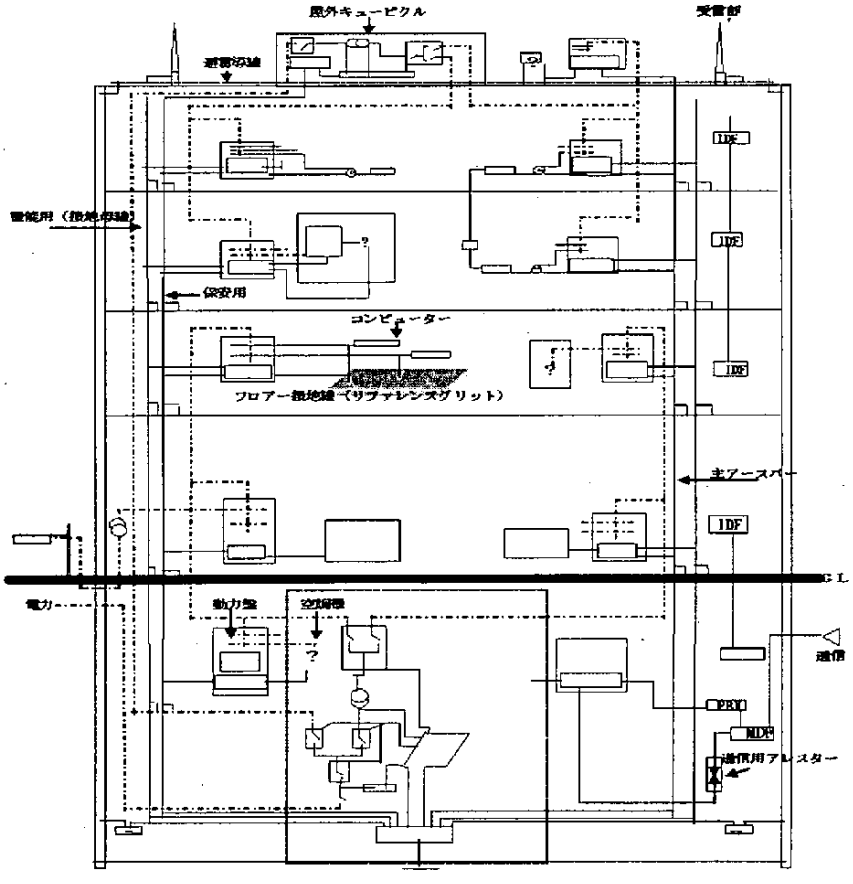


図3.32　ＪＩＳ　Ｃ０３６４総合接地例

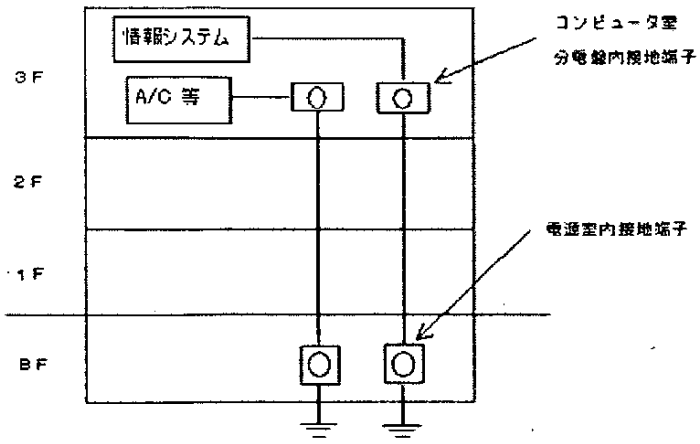


図 3.33　従来の専用接地例

16.コンピュータ室の熱溜

コンピュータ室は機器の配置により熱溜が発生する。　熱黙りにより機器への影響が出るので解消しなければならない。

解消法は；

1)機器の前後にガラリヲセットする

2)空気のリターンを調整する

3)冷水使用の機器で対処する

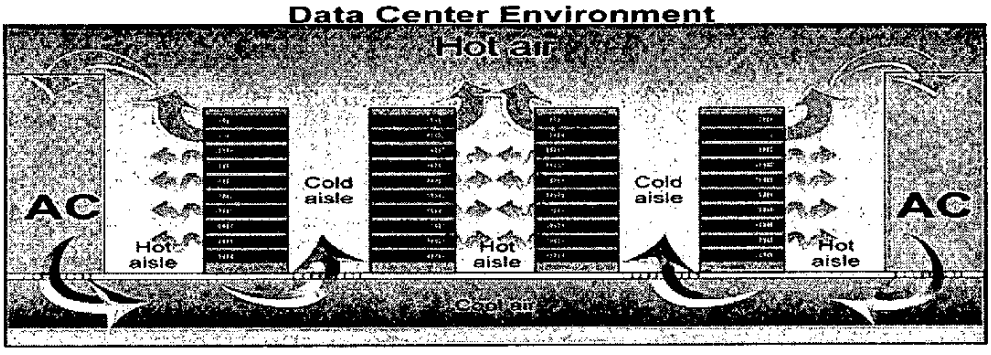


図 3.34　熱溜の例

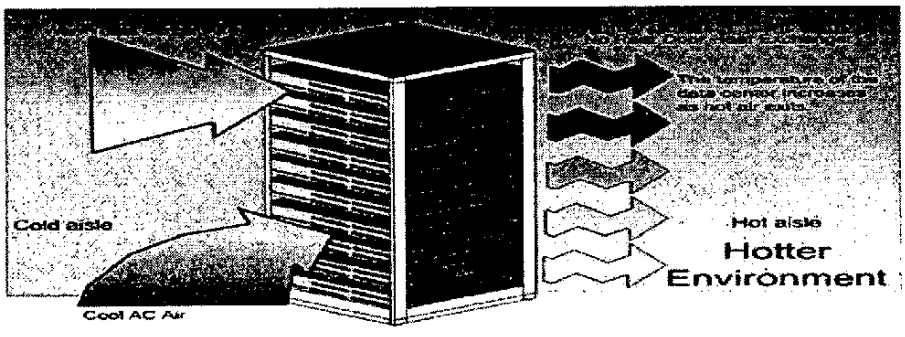


図 3.35　機器と熱の関連例

3.6.4 電気室、空気調和室

両方の室も耐震対策、入退室管理が必要になる。　両方の室が何らかの原因で被災等の被害を受けるとコンピュータの運用に支障をきたし、事業継続に重大な影響を与えるからである。対応は、建屋、コンピュータ室と同等である。

3.6.5 自然災害等による広域災害に見舞われてときの対応

1) 電源の確保

①電源の確保は自家発電装置

②最低でも３日分の燃料を備蓄

③２系統受電　等

2) 通信手段の確保

①ネットワーク配線取り入れは多重化

②ネットワークの切り替えは自動化

③ネットワーク用電源の確保　等

3) 企業としての社会的責任

①災害に備え近隣地域への配慮

・各種公共団体（地方自治体を含む）の対応と連動

・３日分の生活必需品の備蓄（自社の分と近隣の分、乳幼児対策と共に老人対策――老人用オシメ等――も考慮？？）

②金融（支店等）では小銭の用意が必要（高額紙幣は使用しにくい状況になっている）

最後に；

上記各項目を参考に、社会的立場から、事業継続に対する取り組みを考慮し、企業内で最低限必要な設備の確保をしていただきたい事をお願いし終わりとさせていただきます。

3.7 BCI Good Practice Guidelinesの考え方-BCM国際規格の理論的支柱-

3.7.1 BCIについて

BCI（Business Continuity Institute）は、世界最大のＢＣＭに関する普及啓発団体で、その概要は次のとおりである。

3.7.1.1 組織

BCIは、1994年に設立され、世界50カ国に2,500名以上の会員を有している。本部は英国にあり、世界で有名な企業の多くが会員になっている。世界の支部については、欧州各国、米国、カナダ、アジア、豪州などにあり、日本は2003年12月に三井住友海上グループのインターリスク総研がＢＣＩ日本支部になり、現在に至っている。

BCIの目的は次の３つにまとめられる。

(1)ＢＣＭの普及啓発

企業や政府官公庁などの組織に対して、ＢＣＭの重要性を訴えていく活動をしている（後記参照）。これが主たる目的である。

(2)ＢＣＭに関する専門家の支援・育成

BCIの会員は、いくつかのグレードに分けられる。トップの会員になるには、グレードごとに一定のノウハウやBCMに関する実務経験が必要でグレードを上げるために資格試験などを受ける必要がある。

(3)ＢＣＭに関するガイドラインの提供

BCIは、「ＢＣＩ Good Practice Guidelines」というBCMに関するガイドラインを提供しており、2005年に最新版を公表した。

3.7.1.2 BCMに関する法規制・基準作りへの貢献

英国では、ＢＣＭに関するCivil Contingencies Actという法律が施行されている。また、シンガポールでは２種類のＢＣＭに関するガイドラインが発行された。その他、香港、オーストラリア、さまざまな国においてBCMのガイドライン等の策定が行われてきたが、その多くにＢＣＩのノウハウが生かされている。

3.7.1.3 BCIの普及啓発活動

ＢＣＩは先に述べたようにBCMに関する普及啓発活動に非常に力を入れている。例えば、毎年Business Continuity Expoが英国で開催されている。直近では2006年３月に２日間開催された。参加者はおよそ３千人、世界の政府官公庁、民間企業、大学、研究機関などから参加してい

る。日本人も最近増加してきており、日本でもBCMに対する関心が高まっていることを伺わせる。テーマはＢＣＭに関する幅広い事項を取り上げている。例えば、英国ＢＣＭの国家規格化に関する話題、ＩＳＯ化、ＢＣＭに関する実際の取り組み事例などである。

その他、同じようなイベントが英国では年数回開催されている。また、ＢＣＭに関するトレーニングもワークショップ形式で頻繁に開催されている。こうしたイベントの主催者や後援者になっているのがBCIである。アジアでもこれまでタイ、シンガポール、マレーシアなどでBCMに関するコンファレンスが開催されてきたが、ＢＣＩが主催者として関与している。このようにＢＣＩは、世界的な活動を展開、強化している。

また、ＢＣＩに関するホームページ（http://www.thebci.org）も最近一新され、非常にユーザーインターフェースがよくなった。そのウェブサイトからBCIのガイドラインも無料で入手することができる。日本では、BCI日本支部が中心となり、BCIの趣旨に賛同した企業が「ＢＣＩジャパンアライアンス」という任意組織をつくっており、そこがホームページを立ち上げている（http://www.bcijapan.jp）。このウェブサイトでは、BCIジャパンアライアンスの活動や日本におけるBCMの動向に関する情報を発信するとともに、英国のBCM専門誌「Continuity Central」と提携し、世界のBCMに関する情報を提供している。

3.7.2 ＢＣＭを取り巻く環境

3.7.2.1　日本企業のBCM取組状況調査

株式会社インターリスク総研が日本の全上場企業を対象に、2005年の３月にBCMの取組状況についてアンケート調査を実施した。その結果を紹介する。

(1)許容できる停止時間

組織の基幹業務が停止した場合に、許容できる停止時間について、全産業の半分以上が１日未満と回答している。つまり、１日以上業務が止まってしまっては困るというわけである。

(2)BCMの導入状況

これに対して、ＢＣＭの導入は非常に残念な状況にある。図3.36は、海外企業と国内の企業の対比をしたものである。左側が回答企業全体、右側の図が売上高20億円以上の企業における比較である。全体の場合は国内上場企業のＢＣＭ導入割合は9.8%。一方、海外企業は47%である。売上高20億円以上になると、国内上場企業は全体の場合とほとんど変わらないが、海外企業は69%の企業が導入している結果となっている。これは非常に大きな差である。企業の半分以上は１日以上事業が止まってしまっては困ると考えているにもかかわらず、企業ではＢＣＭがほとんど導入されていないというのがわが国の現状といえよう。

ただし、調査は2005年３月に行われた。その月には経済産業省から、ＩＴを対象にした事業継続計画策定ガイドラインが公表された。また、８月には、内閣府から事業継続ガイドライン第一版が公表された。こうしたことを考慮すると、日本企業の導入状況は現在もう少し改善されて

いると推測される。

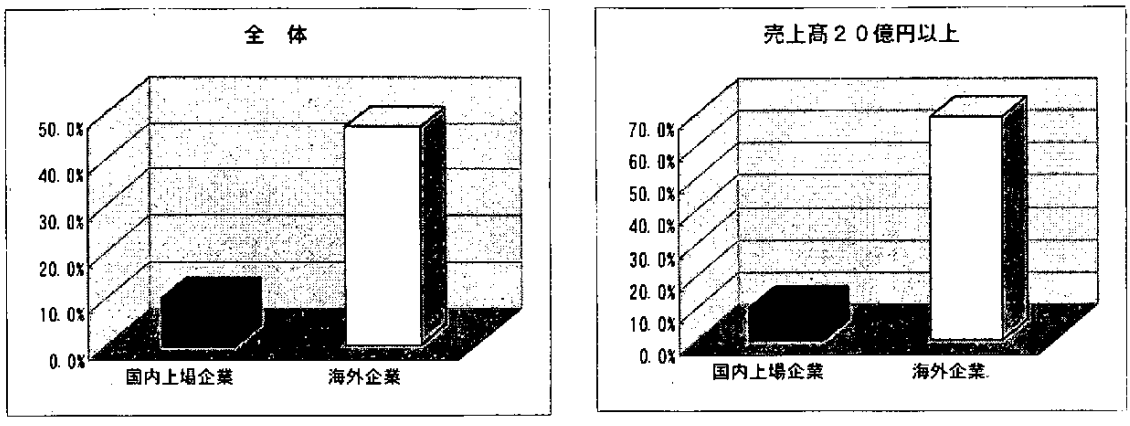


図 3.36　BCM 導入状況国際比較

(3)ICT への依存度

企業が ICT にどの程度依存しているかという質問に対しては、70～80％という回答をした企業が最も多かった。ICT の事業継続に対する影響は非常に高くなっており、その重要性がますます増しているという状況にある。

製造業でも、例えばICTがストップすると、在庫状況が全く分からなくなったり、生産計画が工場にタイムリーにいかなかったりするなどの事態が発生して、数日間生産部門では対応できなくなるという状況が生まれることが懸念されている。

3.7.2.2　事業継続にかかる悪循環

もしＢＣＭをやっていなかった、もしくはＢＣＭをやっていたにもかかわらず、まったく訓練等をやっていなかったという場合にはリスクが顕在化してしまう可能性が高くなる。このリスクには、ICT 事故、地震、鳥インフルエンザ等様々なものが考えられる。リスクが顕在化すれば、事業の継続が不能になり、タイムラグはあるが利益の低下、そして事業価値の低下が起きる。最悪の場合には、金融機関から資本、資金の調達ができなくなってしまう。最悪の場合には企業倒産に至ってしまう。これを「事業継続にかかる悪循環」という。これを断ち切るのがＢＣＭである。

3.7.2.3　BCM はなぜ必要か

現在、世界的にサプライチェーンの緻密化、発展化が非常に進んでいる。その中で、ある企業に ICT 事故、火災、地震などが発生すると、万一その企業がサプライチェーン上のボトルネックであると、サプライチェーン全体に影響を与えてしまうことになる。例えば、日本企業の爆発事故によって、ブラジルの企業の操業に大きな影響が出てしまったという事例もある。

こうした「サプライチェーンで仕事をする」状況の中では、自社だけが万全な対策をしていても、取引先が事故や災害にあえば、その影響を受けてしまうのである。このため、今サプライチェーン全体でＢＣＭをつくっていかなければならい。現実にわが国でもそうした流れが見られる

ようになった。サプライチェーン全体でＢＣＭを構築するといっても、企業ごとにつくる場合、ＳＣＭの一環として協調的にＢＣＭをつくる場合など方法はさまざまである。例えば、自動車業界では、「ＢＣＭやっていますか」「ＢＣＰ持っていますか」と取引先に照会し、協調的に BCM 構築をすすめているところがある。

さらに、海外企業では、このＢＣＭを経営戦略の一つとしてとらえているところが増えており、企業価値の向上という観点で、ＢＣＭの取組状況を取引先に説明している企業がかなり増加しているというニュースも入ってきている。

3.7.2.4 BCMを取り巻く世界の動き

海外、日本含めてかなりＢＣＭの重要性が叫ばれており、ＢＣＭのガイドラインが次々に生まれている。はじめに世界の動きを概括したい。

(1)国・地域別の動き

①英国

英国では、ＢＣＩが 2002 年に世界で初めてＢＣＭに関する包括的概念を示したガイドライを公表した。このガイドラインを３年間、企業、政府、官公庁に使ってもらい、その意見をフィードバックさせて 2005 年２月に全面改訂を行った。

この BCI のガイドラインをもとに、今年の７月に BSI(英国規格協会) が PAS56 の改訂版を公表し、それを国家規格にしていくというスケジュールが正式にリリースをされている。現在、英国ではＢＣＭは国家規格の前段階まできているといえよう。

一方、Civil Contingencies Act という法規制がすでに施行されている。これは司法当局、社会基盤企業、警察、病院など社会に密着する機関、会社については、事故が起こった際の万全の準備としてＢＣＰ（事業継続計画）を策定しなければならないという法律である。これがわが国でも注目を集めており、防衛庁等も関心を持っているようである。

②ISO（国際標準化機構）

BCM の標準化は現在ＩＳＯの場で検討をされており、近い将来、ＩＳＯ化されるだろう。

今年の４月、ＥＰ（Emergency Preparedness：緊急時計画）に関する規格作成のためのワークショップが開催される（米国ニューヨーク大学)。これはＢＣＭのことである。主催は ANSI（米国規格協会）である。ここで各国のＢＣＭに関する案が出される予定になっており、日本案も提案される予定である。この中でもＢＣＩのガイドラインが世界の企業で一番使われているので、ISO の場でも大きな役割を果たすと思われる。

国際規格として公表されるのは 2008 年夏ごろと予定している。ＢＣＭがＩＳＯ化されると、ＢＣＭが「企業間取引の条件」として大きく加速されることに加えて、トップマネジメントの責任の増大、将来的には「企業存続の必須条件」になっていくと考えられる。

③アジア・日本

アジアは日本よりも進んでいる国が見られる。もっとも進んでいるのはシンガポールである。シンガポールは ICT が非常に発展している関係上、ＢＣＭに対する取り組みももっとも早かった。

一方、最近急速に取組が進み始めたのが日本である。政府や官公庁がＢＣＭの重要性を今非常に大きく訴え、ガイドラインも整備されてきた。例えば、経済産業省、内閣府からBCMに関するガイドラインが発行されている。さらに今年２月には中小企業庁も中小企業に対するＢＣＭのガイドラインを公表した。中小企業庁ではこれ以外に、ＢＣＰを持っている企業については貸出金利の低減を行う施策を実施している。したがって、BCM は大企業だけの課題ではなく、中小企業にも必要な管理手法となってきた。今後、特定の企業だけではなくて、産業界全体でＢＣＭが展開されていくと思われる。

(2)BCMに関する規格・ガイドライン

イギリス、アメリカ、オーストラリア、シンガポールなどでBCMに関するガイドラインが発行されている。ＢＣＭのガイドラインは大きく次の２つに分けられる。

○リスクを問わない大局的な指針

例えば、ＢＣＩのガイドライン、ＰＡＳ56、シンガポールのガイドライン、ＮＦＰＡ(National Fire Protection Association）のガイドラインである。

○特定リスクを対象にした指針

わが国の経産省の事業継続策定ガイドラインはICT事故を中心にしており、また、内閣府の事業継続ガイドラインは地震リスクを念頭に置いたガイドである。

このようにリスクを問わない大局的な指針と、日本のように国のリスク状況に応じてリスクを限定した指針が公表されている。おのおののガイドラインの特徴を理解していきながら、うまくこれを取り入れて、ＢＣＭを効率的につくることが必要である。

3.7.3 ＢＣＭ国際規格の理論的支柱－BCIガイドライン

ＢＣＩのガイドラインには、次の４点に特徴がある。

○世界のＢＣＭの指導的役割を果たしてきたBCIの集大成であること

○災害復旧の領域だけではなくて事業、ビジネスの継続・再開に大きな力点を置いていること

従来のガイドラインは、コンピュータシステムやネットワークの復旧に力点をおいた「災害復旧（Disaster Recovery)」を主に扱っており、ビジネスそのものの継続や再開は付随的なものとされてきた。

○事業継続を経営課題として取り組むこと

○BCMを企業の文化として定着させることを重要視をしていること

ＢＣＭは、組織を脅かす潜在的なインパクトを認識し、利害関係者や取引先を初めとしたステークホルダーの利益、名声、ブランド及び価値創造活動を守るため、復旧力及び対応力を構築するために有効な対応を行うフレームワークであり、包括的なマネジメントプロセスと定義することができる。この「復旧力及び対応力」をいかに構築していき、災害、事故・事件が発生した場

合でも、適切に対応できるようにするのがポイントである。

3.7.3.1 BCI ガイドラインの基本理念

BCI ガイドラインにおける BCM の手順は、図 3.37 に示すとおりである。手順は、５つのフェーズに分かれており、事業の理解から始まり、ＢＣＭの戦略、ＢＣＰを中心とした危機への総合的な対応、そしてＢＣＭ文化の発展・確立、最後に訓練、継続的改善、監査と続いていく。BCI のガイドラインには、フェーズごとに取るべきプロセスが記載されており、結果と成果物のありようが示されている。

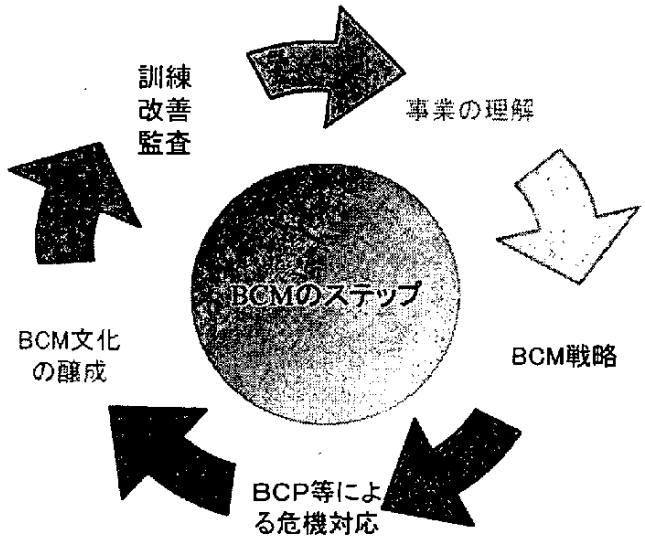


図 3.37　BCI ガイドラインの BCM のステップ

(1)事業の理解

はじめの手順は、「事業の理解」である。企業体が大きくなればなるほど自社の事業全体を理解することは難しくなる。どの事業、業務、機能を優先的に守っていかなければならないかを知ることが BCM の始まりである。

(2)BCM 戦略

わが国では、災害発生時に全事業部門が一斉に復旧をはじめることが普通であるが、再開時期を一層早めなければならない場合には、経営資源を優先的に再開するものに集中的に投入していかなければならない。このどの事業を優先的に守るのかということを決めるのが「BCM 戦略」である。このために重要なのは、ビジネスインパクト分析である。ビジネスインパクト分析とは、業務の流れ、重要な業務機能の洗い出し、目標とすべき復旧時間などを分析する手法であり、これにもとづいて優先すべき業務機能と復旧時間の目標などを会社全体で決めていく。優先順位を決めるに当たっては、財務、人命、供給責任、ブランド、シェア喪失される顧客との関係悪化に対する影響を勘案しながら、総合的に判断して、企業としての基幹業務（Mission Critical Activities）を特定する。

その際に大事なことは経営トップの推進でマネジメントプロセスを推進していくことである。推進体制における役割や責任を明確にし、企業としてのＢＣＭに関する基本方針を策定していくことも重要なことである。日本企業にもＢＣＭの方針を策定して、実際にホームページで公開しているところがみられるようになった。

(3)BCP 等による危機対応

こうした事業の継続にかかる重要事項が決まったら、危機管理計画や BCP（事業継続計画）を

策定していくことになる。危機管理計画とは、事業継続に陥らないような大きなリスクを対象にした計画のことを指す。例えば、危機管理計画の対象としては、テロや戦略的買収などの際の広報対応がそれに該当する。BCP だけでなく、企業としての危機に総合的に対応していくというコンセプトを持っているのが、BCI のガイドラインの特徴である。英国の Civil Contingencies Act もこの BCI ガイドラインをもとに作られている関係から、危機管理計画を持ちながら、ＢＣＰを適切に策定することを規定している。

計画策定に当たっては、事業再開に際しての時間的な制約条件、阻害要因などの「ボトルネック」を明らかにしておくことが重要である。このボトルネックを特定したうえで、対策を立てていく必要がある。企業のボトルネックとしては、例えば、ICT、データ、キーパーソン、取引先、物流、生産体制など様々なものが考えられる。当然、「基幹システムのバックアップがない」ということもボトルネックになる。キーパーソンについていえば、属人的に業務をしていると当人がダウンした場合にボトルネックになりかねない。こうしたことをリストアップして対応しなければならないのである。

BCP のフェーズは、ＢＣＰの発動フェーズ、緊急時フェーズ、業務再開フェーズ、業務回復フェーズ、全面復旧フェーズの５つに分けられる。こうした時系列で対策本部や従業員の行動マニュアルを策定していくことが必要である。

(4)BCM 文化の醸成

ＢＣＭ文化の構築、醸成とは、BCM の普及啓発活動の現状を把握し、従業員がＢＣＭに対してどのように感じているか、実際に行動できるのかなどを分析し、社内に BCM を定着させ、さらに発展させていくための諸活動をしていくことを指す。従って、社員教育や研修、キャンペーンなどが中心的なものであり、その達成度を評価しながらすすめていくことが重要となる。

(5)訓練・改善・監査

PDCA サイクルでいえば、C（Check）に該当するフェーズであるが、チェックや評価をしながら継続的な改善を図ることが重要である。BCM のＩＳＯ規格化に際しても、このフェーズは重要で、特に監査は不可欠になると考えられる。この BCI ガイドラインのステップは、ＰＤＣＡサイクルそのものといってもよく、企業には受け入れられやすいものであると思う。

3.7.3.2　企業価値を高めるための理論

ＢＣＭを構築したら非常時の対応がスムーズにいくというだけであれば、どのガイドラインでも同じである。BCI ガイドラインの特徴は、「事業継続から企業価値へ」を指向している点にある。実際に世界で発生した企業が関わった災害事故・事件を「うまく事業継続ができた企業」と「できなかった企業」に分けてみると、いずれも事件事故が発生した直後の５日間ぐらいは企業価値下がっているが、「企業継続がうまくできた企業」ではその後反転して企業価値が上がっていることが分かってきた。一方、「できなかった企業」は、企業価値が下がっているのである。株価で見れば、250 日たった後も 15％ぐらい下がった事例もある。こうしたことを考慮して BCI ガ

イドラインでは、企業価値のバリュードライバーを管理するために危機管理計画の策定という要素が入れられている。その他、ＢＣＭを企業の経営課題として位置づけ、適切な対応を取ることで、企業の復元力（レジリアンシー）を維持・強化する要素がガイドラインの各所にちりばめられており、ＩＳＯ化に際しても必ず理論的な支柱として採用されていくと考えている。

3.7.4 提言

事業継続を妨げるリスクはさまざまである。リスクには予測可能なものもそうでないものもある。中には新型インフルエンザなどの感染症のように発生が予測不可能であっても企業が事業停止に追い込まれるリスクの出現もありうる。

企業は、事業停止リスクに遭遇した際に、基幹業務を継続させるための行動基準、すなわち「BCP」を策定しておく必要がある。日本経済の中枢を担う国内上場企業のおいても、実践的なBCPを策定している企業は１割に満たない。欧米を中心とする海外企業では、ＢＣＭは経営戦略の一環として不可欠な取り組みであるという認識が産業界に広がっており、導入企業はますます増加している。

世界的に自然災害やテロ、大規模事故のリスクが増大している中、実践的なＢＣＭを確立しているか否かが企業の命運を左右すると言っても過言ではない。ＢＣＭによる企業の復元力・対応力の向上が企業選別基準や他社との差別化に影響するなど、市場競争力向上に直結することを日本企業の経営者は早急に認識する必要がある。また、個々の企業の事業継続力の向上が、ひいては日本社会の災害耐力を高めることになる。東海地震、東南海・南海地震など大地震の発生が切迫していると言われる中、企業がリスクを限定しないＢＣＭの必要性に目覚め、実行に移すことが、日本社会全体の復旧・復興力を高めることにつながるのである。

3.8 保証型情報セキュリティ監査への取り組み

昨今の個人情報保護、認証局の準拠性監査、日本版 SOX など情報セキュリティの水準やマネジメントに対して保証を求める保証型情報セキュリティ監査への社会的要請が高まってきているなか、これまで特定非営利活動法人日本セキュリティ監査協会*1（以下、JASA と呼ぶ）が重点テーマとして取り組んできた「保証型情報セキュリティ監査」について紹介する。

3.8.1 情報セキュリティ監査について

まず、情報セキュリティ監査を実施する上で規範となる制度について触れておく。2003 年 3 月、経済産業省・商務情報政策局長の諮問研究会の「情報セキュリティ監査研究会」より、情報セキュリティ監査の普及とそのあり方に関する答申案が出された。これを受けて 2003 年 4 月、経済産業省から以下の内容が盛り込まれた「情報セキュリティ監査制度」*2が告示された。

・「情報セキュリティ監査」のあり方
・「情報セキュリティ監査」の標準的な基準と監査を行う主体のあり方
・電子政府に対する「情報セキュリティ監査」のあり方

その中で、情報セキュリティ監査について以下の定義がなされた。「情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を情報セキュリティ監査が行う主体が独立かつ専門的な立場から、国際的にも整合性のとれた基準に従って検証又は評価し、もって保証を与えあるいは助言を行う活動」とある。これまでの監査の概念である保証型監査に加え、助言型監査という新しい概念が盛り込まれた。

3.8.2 情報セキュリティ監査の実施・普及状況

情報セキュリティ監査には、前述した助言型と保証型があるが、都道府県では、助言型の情報セキュリティ監査が一巡し、情報セキュリティレベルの向上が図られており、今後、情報セキュリティがある一定の水準に達すれば、現在の助言型中心の監査から保証型監査に移行していくものと考えられる。

---

*1 特定非営利活動法人日本セキュリティ監査協会：2003 年 4 月、経済産業省による「情報セキュリティ監査制度」が施行され、この制度を着実に浸透させていく為の運営体として、2003 年 10 月に設立。情報セキュリティ監査を実行しようとしている企業・組織・監査人が会員となり、情報セキュリティ監査の「あり方」や「やり方」を研究、ならびに監査と監査人の質の確保を行うことにより、「公正かつ公平な情報セキュリティ監査」が実施され、情報社会にとって有益なものとして情報セキュリティ監査が機能することを目指している。http://www.jasa.jp/

*2 http://www.meti.go.jp/policy/netsecurity/audit.htm

平成 17 年 10 月総務省が発表した調査結果によると、都道府県レベルでは過半数の 26 都道府県で情報セキュリティ監査が実施されており、残る都道府県においても検討中が多い。市町村でも実施と検討中を含めると 3/4 に達するなど、総務省の指導もありかなり普及しているといえる
また、監査の種別は、都道府県では外部監査が多く、市町村では内部監査が多い。

一方、民間企業では、情報セキュリティ監査企業台帳の集計結果によると、8 割は助言型監査であり、地方自治体と同様に、まだまだ保証型監査は浸透していない状況である。

3.8.3 助言型監査と保証型監査の違い

情報セキュリティ監査は、助言型監査から始まり今後は保証型監査へとその中心がシフトするものと思える。この保証型監査は「監査対象となる情報資産に対するリスク対策のコントロールの実施状況について評価し、監査意見を表明すること」が主目的であるが、助言型監査は「監査対象となる情報資産に対するリスク対策のコントロールの実施状況について評価した上で、そのギャップを埋めるための助言をすること」に重きを置いている点が大きな違いといえる。

情報セキュリティ監査のプロセスは、「リスク認識」「コントロールの整備状況」「コントロールの評価」「報告」の 4 段階に分かれるが、この 4 段階のうち、助言型監査と保証型監査では、コントロールの評価から報告の段階が大きく異なる。つまり、助言型監査ではコントロールの評価を行った上で問題があれば、それを改善するための意見を述べることに重点を置くが、保証型監査ではコントロールの評価を行って、その客観的な評価を監査意見として報告書にまとめることが主目的となる。また、助言型監査の場合は情報資産のリスク全般を対象にすることが多いのに比べ、保証型監査では対象とする情報資産・情報システムを限定することが多い。

更に特徴的なのは、助言型監査は監査の対象となる組織と監査人の 2 者関係であるのに対して、保証型監査ではその 2 者に加えて監査の結果、つまり報告書を利用・活用する第 3 者が関わることにある。この点が、監査対象を限定することが多い理由の一つにもなっている。例えば、保証型監査に対して寄せられる要望には、「業務委託契約に保証型監査の枠組みを適用したい」「一部の業務や情報システム対する保証は可能か」、或いは日本版 SOX 法との関わりから「経営に与えるリスクと管理状況を評価する監査は可能か」といったことからも理解できる。

次に、保証型監査の報告者を誰が利用するのかという観点で説明を加える。図 3.38 に示す様に、企業 B 社が A 社のサービスを利用したり、業務委託を検討する際に、B 社が A 社に対して監査の実施とその報告書を要求するケースが考えられる。この場合、B 社が監査費用を負担しても A 社に監査を受けるよう要求することもある。もう一つのケースは図 3.39 に示す様に、企業 B 社のユーザが、B 社が業務委託している A 社について情報セキュリティで信頼できる企業であるかを求めた場合、B 社は A 社の監査結果を利用してユーザに対する説明責任を果たすケースが考えられる。

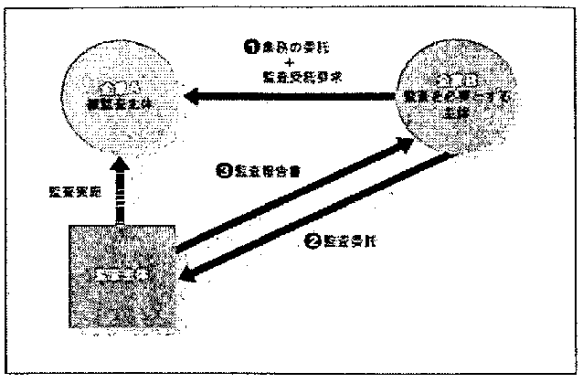


図 3.38　B 社が A 社に監査を要求するケース

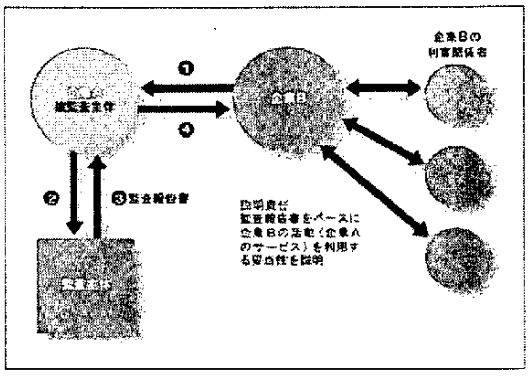


図 3.39　B 社が A 社の監査結果を利用・ユーザへの説明責任を果すケース

そこで、監査報告書にも保証型監査と助言型監査で大きな違いが出てくる。保証型監査では第 3 者の利用を前提としているので、地方自治体などでの監査は住民請求があるためその第 3 者利用のケースとなる。ただ、助言型監査の場合では第 3 者開示を前提としていないため、検出事項や改善事項などが公開されると脆弱点が外部に開示されてしまう問題が起こるので、公開する際には契約段階でも開示情報の範囲と対象をしっかりと決めておく必要がある。

更に監査人の責任に於いても大きな違いがある。保証型監査の監査人は監査結果に対して第 3 者への責任が伴うので、監査結果の内容に問題があれば、場合によっては監査報告書を利用した第 3 者に損害賠償を求められることにもなる。

3.8.4 保証型監査に対する誤解

ここで保証型監査に対してよくある誤解について解説しておきたい。それは監査報告書あるいは監査人は「将来」に渡って監査結果を保証するものではないことである。つまり、監査報告書で問題が指摘されなければ、将来に渡っても問題が生じないことを意味するものではない。これは、どんな分野の監査でも共通することで、監査は実施時点における評価であり、将来に渡っての予測や責任を持つものではない。ただ、将来問題が発生して責任の追及を受けた場合、これだけの情報セキュリティ対策を実施していたという事実認定に役立つことには違いない。こうした誤解が生じるのは「保証型」という言葉を使っていることに起因していると思われるが、海外の情報セキュリティ監査では助言型・保証型の区別はなく、一般的に監査は保証型監査のことを言い、「保証」＝guarantee とは言わず「確信」＝assurance と表現している。これは専門家である監査人が評価した結果、大丈夫であると確信したとの意味からくるものである。

3.8.5 海外における保証型監査の実情

次に、実際にどのような保証型監査があるのか、海外の事例を中心に紹介する。まず、Web Trust*3検証報告書の例として、米国とカナダの公認会計士協会が協力し共同開発・管理運営し

*3 http://www.webtrust.org/

ている電子商取引保証規準に基づくものがあり、公認会計士がWeb Trust原則及び規準に照らして監査を行い、問題がないと認定した企業に対してWeb画面にWeb Trustシールを付与するものである。

また、DHS（米国の国家安全保障省）*4の入出国者管理システムでの情報セキュリティ監査があり、これは米国市民と入国管理者を管理するデータベースシステムのセキュリティの状況を監査したもので、特徴的なのは、監査の結果をWebで一般に公開している点である。核心部分は、どのシステムのどんな問題かは分からないようになっているが、監査した結果、これ以外の問題が無いことを知らせるために公表している。また、評価を簡潔に表記して報告書を読む第3者が容易に理解できる工夫もみられる。欧米の監査では保証型監査しかないと前述したが、この監査では改善の提言も述べられ、さらに監査人の意見と被監査組織の意見も併記することで、意見の一致、不一致が第3者にも容易に分かるようにしているなど、様々な工夫がこらされている。

米国でも監査報告書の形態にはさまざまなものが存在し、改善勧告が述べられているものもあれば、非常に簡素なものなど、米国に限らず海外全般を見ても今なお研究中であり、試行錯誤を続けているのが現状と言えよう。

3.8.6 JASAによる保証型情報セキュリティ監査への取り組み

(1) 言明による保証型情報セキュリティ監査について

JASAでは、海外をはじめ他業界に於ける監査の枠組みの調査研究を行い、日本の保証型情報セキュリティ監査をどうやって進展させるかをテーマに、保証型情報セキュリティ監査の類型の一つとして、経営者などによる言明による保証型情報セキュリティ監査の枠組みについて検討してきた。これまでの検討状況を以下に紹介する。

---

*4 http://www.dhs.gov/dhspublic/

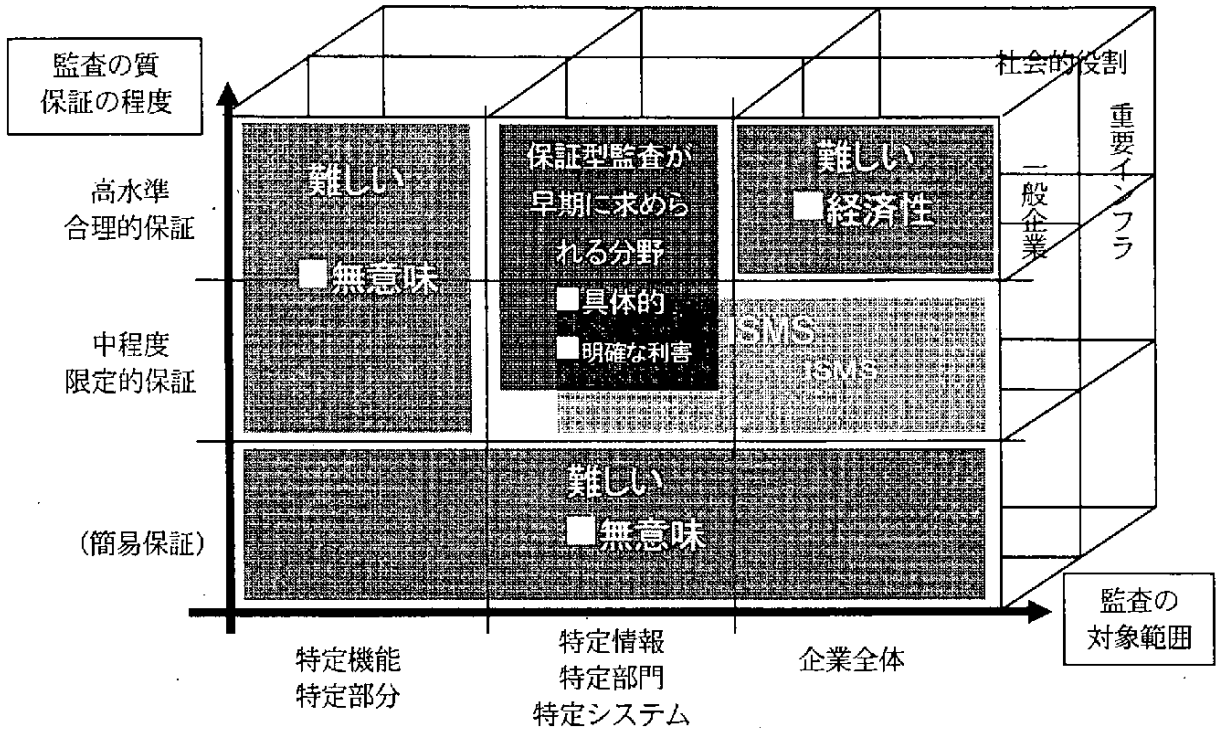


図 3.40　監査に於ける保証の程度と監査の対象範囲

上の図 3.40 に示す中心の青の部分が保証型情報セキュリティ監査の主要な対象と想定している。つまり、特定の情報や部門などを対象に、ある程度以上の保証を与えるものである。よく質問される ISMS 適合性評価制度と較べると、ISMS 適合性評価制度は一般に企業全体など比較的広範な部分を対象にある程度限定された保証を行うことを前提としている。中程度の保証の部分では相互に関連するが、より高水準の保証を求めるなら保証型監査になるものと考えている。

実際の保証型監査でユーザが求めるのは、この業務、あるいはこのシステムや情報資産がしっかりとセキュリティ管理が行われていることを保証して欲しい、あるいは証明したい、それを何らかの文書に残したいというものである。

現在 JASA が考えている「言明による保証型情報セキュリティ監査」は、当該業務においてリスクに対する対策を行い「有効な情報セキュリティマネジメントを行っている」と、まず経営者が言明し、その言明を受けて監査人が具体的なセキュリティ対策が存在しているか、リスクに対する対策をしっかりやっているかを検証した上で、保証を行う監査である。

(2) 言明による保証型情報セキュリティ監査の定義

保証型情報セキュリティ監査は、ひとつの定義にしばられるものではなく、多様なものがイメージできる。その中で、現実的な情報セキュリティ監査における保証型監査の定義のひとつとして、言明方式「『監査対象の経営者が言明した情報セキュリティマネジメントのリスク対策』の全てが存在し、機能していることについて、合理的な方法と証拠に基づき監査人が意見を述べること」を取り上げ、具体的な意味づけを行うことを提言する。

□ 何を監査するのか

監査対象の経営者が言明した情報セキュリティのリスク対策の全てが存在し、機能していること。

(注)「機能している」ということの定義は別途行う

『解説』会計監査では経営者の責任で作成された「財務諸表」が実態を適正に反映していることを、実態から集められた客観的証拠により判断している。つまり、会計監査は実態としての財務状況を判断しているものでもなく、またそれに基づくリスクを判断するものでもない。情報セキュリティ監査では、実態を判断するというイメージがある。例えば、「保証意見を述べた後に事故が起こったらどうするか?」というような問いが発せられる。しかし、実態に対する判断(そのリスク低減策で安全か否かなど)は別の主体(例えば、被監査主体へ情報サービスを委託する者、あるいは公的な主体など)が行うものと考える。

情報セキュリティ監査においても、会計監査と同じように、経営者の責任で外部に提示された情報(この場合は言明)が、実態と乖離しているか否かを判断するものである。

□ 言明とは何か

監査対象の経営者が監査報告書の利用者に対して行う、「監査の対象となる組織体において情報セキュリティに関するマネジメントとコントロールを適切に行っている旨」を内容とする表明

□ 保証の定義

監査対象の経営者が発した上記の言明に対し、監査人が合理的な方法と証拠に基づき、監査の対象となる組織体の情報セキュリティに関するマネジメントとコントロールが監査手続きを実施した限りにおいて、適切である旨(又は不適切である旨)の意見を述べること

『解説』合理的とは、経済的合理性、技術的合理性、社会的合理性などを意味する。利害関係者の監査に対する合理的な期待に応えるための目的合理性、監査の質を担保する手続的合理性、監査人の責任を規定する制度的合理性も含まれる。

□　何を意見として述べるか？

「リスク対策の全てが存在し、機能している」ことを内容とする経営者の言明が、事実と照らして適正であるかについて

『解説』経営者が情報セキュリティマネジメントのリスク対策について言明していることが監査の前提となる。言明は「情報セキュリティ報告書」「情報セキュリティに関する契約」などを通じて行われる。公的な機関が制定した基準への適合性宣言なども、言明となる。これらはすべて経営者の責任において行われていることが必要である。

（参考）保証業務の定義（公認会計士協会　財務以外の保証業務等に関する実務指針（公開草案）より）

公認会計士等が業務実施者として行う保証業務とは、主題に関わる業務対象の作成者または実施者（以下「主題に責任を負うもの」という。）が、一定の規準によって主題を評価又は測定した結果を表明する情報（以下「主題情報」という。）について、又は、主題それ自体について、それらに対する保証報告書の利用者（以下「想定利用者」の信頼の程度を高めるために、業務実施者が自ら入手した証拠に基づき規準に照らして判断した結果を結論として報告する業務をいう。

（コメント）今回の定義は会計士協会の定義のうちの一部、主題情報に限定したものと解釈できる。

ここでいう言明とは、情報セキュリティ報告、情報セキュリティに関する契約、公的な機関が制定した規準への適合性宣言などが含まれるが、言明書に記載すべき項目、記述レベルなどは今後明確にしていきたい。

(3)　保証型情報セキュリティ・パイロット監査について

JASA では、この言明による保証型情報セキュリティ監査を進めるにあたって、現在トライアルとしてパイロット監査の準備を進めている。パイロット監査を通じて、本当に「言明」という監査のやり方が良いのか、日本の情報セキュリティ監査に適合できるのかなどを検証すると共に、保証型監査に対するユーザニーズなどを吸い上げていきたい。

パイロット監査を行う上で、以下の様な保証型情報セキュリティ監査の類型パターンの整理を行った。

・業務委託契約で管理要件を定めているケース

現在内閣官房（NISC）が進めている政府機関の情報セキュリティ対策のための統一基準[*5]に基づき外部委託契約をする場合などが相当する

[*5] http://www.bits.go.jp/active/general/pdf/k303-052.pdf

・被監査組織が管理要件を定めて宣言しているケース
　民間企業などが独自に管理要件を定めて、宣言し運用している場合などが相当する
・業界団体などが定めた標準要件が存在するケース
　医療情報システムの安全管理に関するガイドライン[*6]など、業界団体が定めた基準などが存在する場合が相当する

現在、上記の類型パターンを基に３つのタスクにて保証型パイロット監査の準備を進めている。

(4)　言明以外の保証型情報セキュリティ監査について

こうしたパイロット監査を通じて、経験・ノウハウを蓄積し、今年中には「言明による保証型情報セキュリティ監査」の枠組みを明確にする予定である。言明以外の保証型情報セキュリティ監査については、例えば、このシステムは運用を含めて本当にセキュリティは大丈夫なのか、という様な第３者（利害関係者など）からのニーズにも応えられる保証型情報セキュリティ監査の枠組みの検討も進めている。

3.8.7 情報セキュリティ監査の品質確保に向けたJASAの取り組み

保証型監査において監査人は第３者に対して責任が伴うなど、監査人はある一定以上のスキルや資質が要求される。このニーズに応えるため、JASAで取り組んでいる制度について紹介する。

(1)公認情報セキュリティ監査人資格制度(CAIS)[*7]

情報セキュリティ監査人に求められる知識・経験・技術に応じて、公認情報セキュリティ主任監査人、公認情報セキュリティ監査人、情報セキュリティ監査人補、情報セキュリティ監査アソシエイトの資格認定を行っている。資格認定には、監査人としての能力（知識・経験・実証された能力）、監査人としての適切な行動（倫理基準への遵守）が求められており、この資格制度を運営するために、ISO/IEC17024（適合性評価－要員の認証を実施する機関に対する一般要求事項）に則り、協会内の独立した機関として資格認定委員会を設けて、資格制度の運用と資格に係るレベル認定を行っている。

更に、情報セキュリティ監査人に求められる知識・経験・技術を維持向上する為に、監査実績、監査人教育、JASA活動への参加、社会貢献などの観点で３年毎の更新時にその資格要件を見定めて資格維持可否の判断を行っている。

(2)審査委員会制度[*8]

審査委員会制度は、紛争審査制度、監査品質審査制、倫理審査制度の３本柱からなる。

[*6] 厚生労働省 http://www.mhlw.go.jp/shingi/2005/03/s0331-8.html
[*7] http://www.jasa.jp/qualification/qualify.html
[*8] http://www.jasa.jp/shinsa/shinsa.html

紛争審査制度は被監査主体より提起される苦情を契機として、現に行われた監査に対し、情報セキュリティ監査制度に基づき、その監査に用いられた基準及び倫理基準等協会の定める基準に示された監査水準に適合するか否かを審査するものである。

監査品質審査制は会員より申請のあった、又は協会として独自の判断により選択した現に行われた監査について、情報セキュリティ監査制度に基づき、その監査に用いられた基準及び倫理基準など協会の定める基準に示された監査水準に適合するか否かを審査するものである。

倫理審査制度は被監査主体より提起される苦情を契機とする紛争審査や現に行われた監査を対象とする監査品質審査によらず、JASA 会員及び公認情報セキュリティ監査人資格制度(CAIS)資格登録者について倫理基準に違反する事実が判明したとき、その事実について懲戒処分を行うべきか否かを審査するものである。

以上の様な制度運営により、JASA 会員及び公認情報セキュリティ監査人資格制度（CAIS）の資格登録者が行う情報セキュリティ監査の信頼性が一定水準以上であることを担保し、JASA 設立の趣旨でもある「公正かつ公平な情報セキュリティ監査」の普及浸透を目指して社会に貢献できるものと考えている。

3.9 過去の事件から学ぶ～個人情報漏えいの後始末

事業継続計画（BCP）では、地震・暴風雨など自然災害や火災・爆発などの事故、システム障害、電力や通信回線などのインフラ障害さらにはスタッフの長期不在などの人的要因まで、あらゆる事業継続の阻害要因を想定しそれらが事業に与える影響度を分析することにより、ミラーサイトの設置やバックアップの遠隔地保管などの復旧計画を立案する。事業継続計画は、組織の戦略的な計画であるが、コンティンジェンシープラン（緊急時対応計画）やインシデント対応などその他の個別緊急時計画とも整合させる必要がある。反対にコンティンジェンシープランやインシデント対応など個別対応計画は、事業継続計画の目的（復元、復旧）を意識した内容にしなければならない。

以下に、事業継続計画における個別対応計画を策定する際の一助になることを期待し、インシデント対応の策定手順の例を挙げる。事業継続計画および個別対応計画は、組織の事業内容や特性により内容が異なるが、ここでは、多くの組織で共通の心配事であり、また個人情報保護法完全施行後も後を絶たない個人情報漏えいを題材にする。

3.9.1 過去の事例の分析

阻害要因が事業継続へ与える影響度を分析する場合、想定されるインシデント（事件・事故）のシナリオを沢山考え出せるほど分析結果の精度が向上する。しかし、想像だけでシナリオを考えることには限界があり、またあまりにも現実離れしたシナリオでは分析する労力が無駄になってしまう。その点で、過去の事件・事故を参考にすることは有意義であり、様々なケースが含まれているし何より実際に発生したことであるので説得力もある。

NPO 日本ネットワークセキュリティ協会（JNSA）では、2001 年から毎年、国内のメディアに公表された個人情報漏えいインシデントを集計し評価している。その評価結果を紹介しつつ、過去の事例の分析方法を解説したい。

3.9.1.1 2004 年の個人情報漏えいインシデントの集計と評価

（1）漏えい件数

表 3.4 漏えい件数

2004 年	2003 年	2002 年
366 件	57 件	62 件

2002 年・2003 年と比較すると 2004 年は漏えい件数が約 6 倍と大きく増加している。2004 年は個人情報保護法完全施工を前にマスコミが多く取り上げたことと、それまでは単なる事務所荒らしや車上荒らしなど盗難事件とされていたものが、たまたま個人情報の記録された書類や PC が被害にあった場合、この時期には“個人情報の盗難”と報道されたことも一因と考えられる。

（2）被害者数

表 3.5　被害者数

2004 年	2003 年	2002 年
10,435,061 人	1,554,592 人	418,716 人

2004 年は被害者数も大きく増大している。2004 年はある通信事業者からの 450 万人分の情報の漏えいや、ある信販会社からの 160 万人分の情報漏えいなど大きな事件が発生したものの、前述した漏えい件数の 1 件当たりの被害者数の平均は 2003 年・2004 年とも約 3 万人で変化が見られないことから、2004 年の被害者数の増加は報道の増加に伴うものと考えられる。

（3）個人情報の漏えい原因

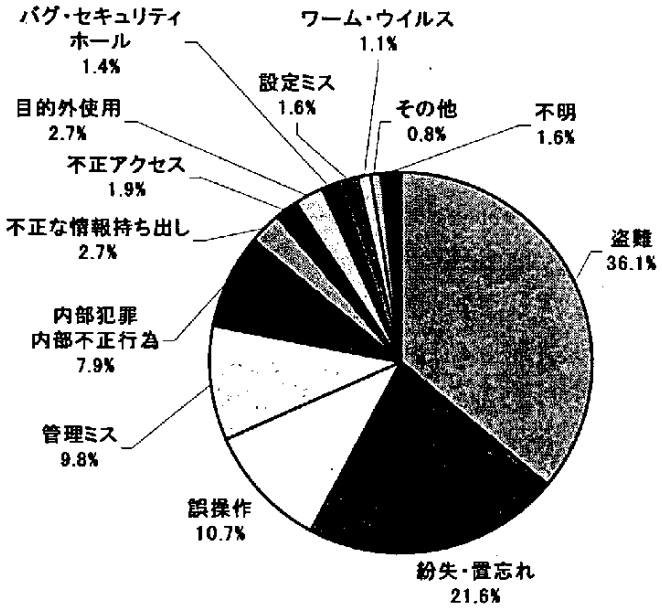


図 3.41　2004 年 個人情報漏えいの原因

図 3.41 は 2004 年の個人情報漏えいインシデントを原因別に集計した結果である。「盗難」「紛失・置忘れ」が全体の 57.7%を占める。先に述べたとおり今までは単なる事務所荒らしや車上荒らしが個人情報漏えいと結びつけて報道されたことも一因と考えられるが、数字の信憑性はさておき、内訳を見ると「網棚に置いた鞄が盗まれた」「パチンコしている間に車上荒らしで鞄が盗まれた」「事務所荒らしで数台のノート PC がまとめて盗まれた」「居酒屋で預けた鞄がなくなった」など身近な行動にリスクが潜むことが分かる。

（4）個人情報の漏えい経路

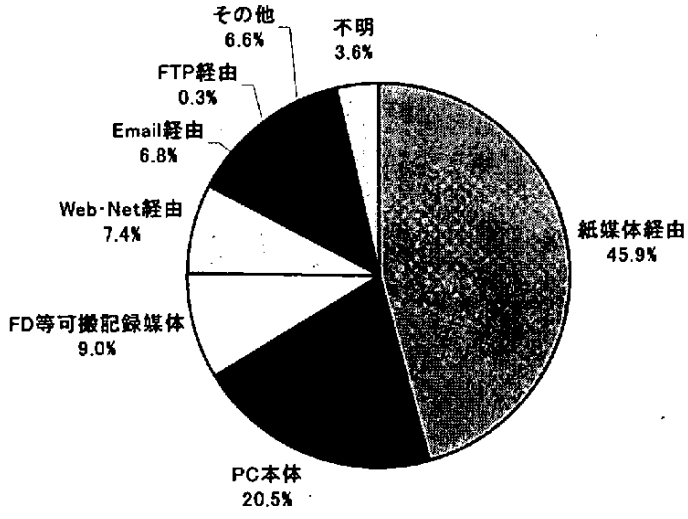


図 3.42　2004 年 個人情報漏えいの経路

図 3.42 は 2004 年の個人情報漏えいインシデントを経路別に集計した結果である。「紙媒体」「PC 本体」が全体の 66.4%を占める。漏えい原因と関連付けて考えるとやはり、盗難にあった鞄に個人情報が記録された書類や PC が入っていたためと分析できる。

（5）個人情報漏えい原因別の被害者数

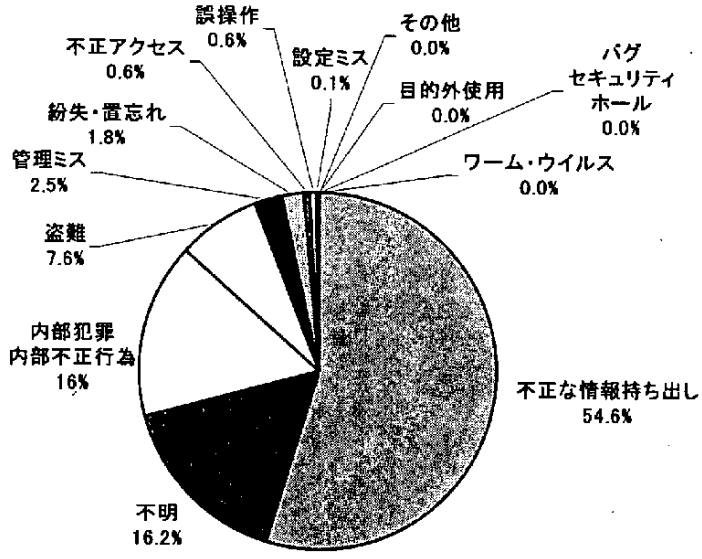


図 3.43　2004 年 個人情報漏えい原因別の被害者数

図 3.43 は個人情報漏えい原因別の被害者数を集計した結果である。グラフ 1 では 10.6%にしかすぎなかった「内部犯罪・内部不正行為」「不正な情報持ち出し」が、被害者数で集計しなおすと全体の 70.6%を占めるようになる。ここでいう内部犯罪・内部不正行為・不正な情報持ち出しとは、組織の従業者や業務委託先従業者など個人情報を取り扱う業務従事しそれらの情報にアクセスする権限を持つ者が故意に情報を持ち出し結果漏えいしたというものである。この結果から、内部のものが関わる情報漏えいは、発生する確率は低いものの（10.6%）、一度発生すると被害が大きい（70.6%）という分析ができる。権限者は機会も多く時間もかけられるということが原因と予想される。

（6）個人情報インシデントから学べること

2004 年の個人情報漏えいインシデントを分析・評価して学べることは、移動中に持ち歩いている情報はリスクが高いということと、権限者による不正はインパクトが大きいということだ。

予防策としては、情報持ち出しの制限とその徹底、持ち歩くデータの暗号化、権限者のアクセス記録（ログ）の収集、従業者からの秘密保持誓約書等の取得などが考えられるが、事業継続計画またはインシデント対応としては、それらのインシデントが発生した場合のリカバーの手順を明確にすることが求められる。そのためにはさらに事例を深く分析することが求められる。

なお、JNSA セキュリティ被害調査ワーキンググループでは過去の事例を分析し、適切な事後対応、不適切な事後対応をまとめているので参考に記述しておく。

a. 適切な事後対応例

- すばやい対応

- 被害状況の把握
- 事件の公表
- 状況の逐次公開(ホームページ，メール，文書)
- 被害者に対する事実周知，謝罪
- 被害者に対する謝罪(金券の進呈を含む)
- 顧客に与えるであろう影響の予測
- クレーム窓口の設置
- 漏えい情報回収の努力
- 通報者への通報のお礼と顛末の報告
- 顧客に対する補償
- 経営者の参加による体制の整備
- 原因の追究
- セキュリティ対策の改善
- 各種手順の見直し
- 専門家による適合性の見直し
- 外部専門家の参加による助言や監査の実施

b. 不適切な事後対応例

- 指摘されても放置したままである
- 対応が遅い
- 繰り返し発生させている
- 対策を施したが、有効でない
- 虚偽報告

3.9.1.2 個人情報漏えいインシデントの詳細分析

過去のインシデントから学び、事業継続計画あるいはインシデント対応に役立てるため、ある事例を詳細に分析した例を挙げる。

対象とした事例は少し古く、今のように個人情報漏えいが頻繁に公表される以前のものであり、まだ事後対応について世の中全体に経験が浅い頃のものである。そのため、当該組織がどのようにインシデントを評価し行動に移したかが分かるためサンプルには適していると考え取り上げた。

事例を分析する場合は、当該組織がどのような行動を行ったか時系列で追跡し、それぞれの行動のどこが良くてどこが悪かったのかを評価することと、被害者がどのような行動を起こしたかがポイントになる。

（1）事例

漏えい情報	会員カードの会員情報　約56万人分 氏名・住所・性別・生年月日・自宅電話番号・携帯電話番号
経緯	0日　会員3名からの問い合わせ 「貴社の会員登録のみに提供した宛先に不審なダイレクトメールが届いた。貴社から情報漏えいが有ったのではないか。」 1日　社内調査開始 9日　別の会員からの問い合わせ 10日　顧客情報の流出を確認 流出先業者が保有する会員情報を消去 14日　調査委員会発足・警察への相談 社外取締役との打合せ、社外弁護士を委員長とする調査委員会を発足 15日　個人情報保護委員会発足 個人情報保護委員会を発足し、専門家をアドバイザーとして起用 アクセスログの強化、情報の外部利用の制限、入退出の二重チェックなど管理を強化 17日　Web上で情報公開 会員へお詫び状と商品券（500円）を発送 後日　外部委託先のシステム開発会社のシステムから、故意に盗まれた可能性が高い。 システムにアクセス可能な人物はある程度絞られたが特定は困難と発表。

（2）事例分析

事例を分析した結果の要点をあげてみる。

・漏えい情報

漏えい規模は、全会員数の版数にあたる56万と想定され、影響が非常に大きい。漏えい情報の内訳で悪用される可能性があるのは氏名と連絡先で、予想される会員への被害としては迷惑メールの増加、架空請求、インターネット掲示板への公表などが考えられる。

・漏えいの検知

被害者からの通知で漏えいが発覚、組織は自ら検知する能力はなかった。

・レスポンス

通報が入って翌日には社内調査を開始していることは評価される。その後の対応として、調査委員会発足が2週間後というのは評価が分かれるところであろう。当時の状況とは違うため、現在であれば対応組織はすでに用意されていることが望まれる。

・対応の内容

警察に相談し、調査委員会の委員長に社外弁護士を採用するなど、外部に協力を求めたことは評価できる。身内だけで解決を図ると、どうしても手加減してしまうし、世間もそのように見るので、取り組みに対する信用度を上げるためにも外部の専門家を利用することは望ましい。

その後、個人情報保護委員会を社内に発足させ、継続的な取り組みをしようとする努力は評価できる。

・原因の特定

漏えい原因が、外部委託先の故意によるものであるという所までは追跡できたが、人物（犯人）は特定できなかった。ログの内容および記録期間が十分であったか、ログの評価分析は十分であったか等の課題が残る。これらの課題はいまだに多くの組織での懸案となっている。先にも述べたが、権限者の不正の予防（抑止）のためにはログは重要な要素であるので、十分考慮する必要がある。

・被害者への保障

本件の実被害としてはDMが増えた程度であるが、デジタルデータは一度流通すると回収は不可能である。今後別の目的で悪用されることも予想される。その際、組織として被害者に対しどのような救済措置がとれるのか検討しておく必要があるだろう。

本件ではお詫びとして全会員に500円のプリペイドカードを配布している。最近のインシデントにおいてもお詫びに500円というのは相場になっているようだが、ある弁護士によると、被害者数が少なければ数千円の菓子折りでも持参して一軒ずつに足を運んでお詫びをするだろうところを、500円金券を一斉に配布して済ますのは企業の怠慢であると評価している。

現実にはタイムリーに迅速に対応しなければ効果も薄く、企業としてはその費用対効果といった経済的な判断に基づくものであるので、左記のような評価を甘んじて受けることは出来ないと思うが、右へ倣えで500円ではなく、各事案毎のインパクトを分析した上での対応が求められる。

なお、幾つかの事例では被害者が漏えいした組織を相手に訴訟を起こしているものもあり、判例が増えれば訴訟の可能性も高くなるため、組織としてもそれに備えた対応計画も必要になるであろう。

さて、上記のようにひとつの事例であっても多くの教訓が得られることがご理解いただけたと思う。今後も引き続き特徴的なインシデントが報道されたら、是非分析を試みていただきたい。

3.9.2 個人情報漏えい発生！　その時組織は何をするのか？

これまで様々な事例を分析した結果から、個人情報漏えいに対し組織が備えておくべきこと、また発生後に取るべき行動をまとめたので、インシデント対応手順を策定する際の参考にしていただければ幸いである。

3.9.2.1　インシデント発生時の対応フロー

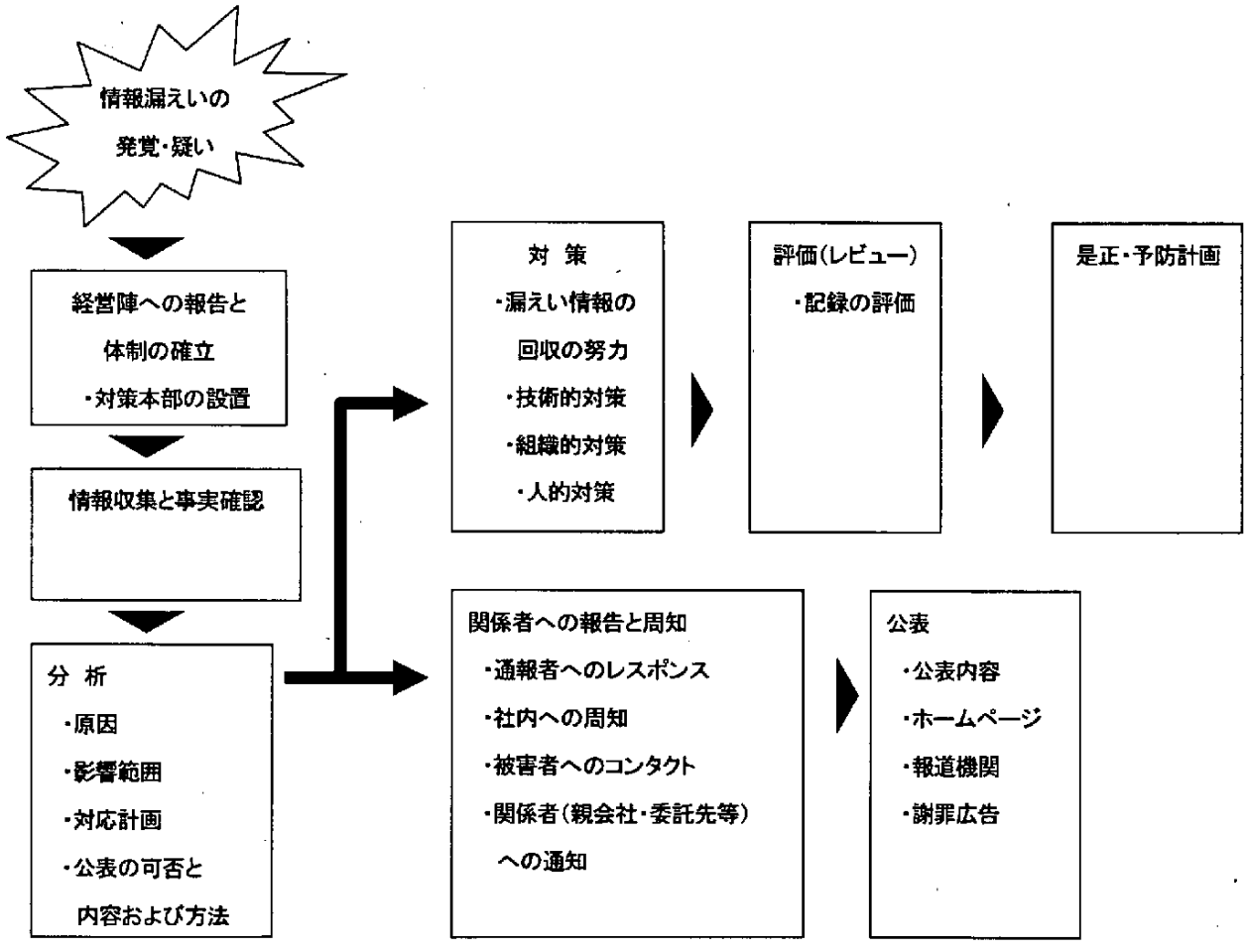


図 3.44　インシデント発生時対応フロー

インシデント発生後の行動は、「対策」と「周知」の二つのフローに分かれる。

3.9.2.2　インシデント対応の目的

インシデント対応を実施した結果、何をもって成功とするかの判断基準とするために、目標を明確にしておく必要がある。

インシデント対応の目指すところとしては、被害の最小化、現状の復旧、信用回復、予防などが挙げられる。

3.9.2.3 インシデントの定義

何をもってインシデントと判定するのか、その判断基準がなければインシデントを検知できないし、発見者が届けることもできない。インシデントには、業務・サービス障害、人的リソースの欠如、情報障害、セキュリティ侵害・障害、それらの疑いなどが考えられる。定義の方法は組織によって異なるが、事象を例示する方法や、ベースライン（正常な状態）を定義しそこから逸脱しているかどうかにより判断する方法など様々な方法が考えられる。

ここでは個人情報漏えいとう事象にフォーカスした内容となっている。

3.9.2.4 インシデント対応組織と体制の確立

ここから以降は先に記した対策フロー図に沿った実施項目について解説していく。

速やかかつ整然とインシデントに対応するためには、予め対応組織を確立し役割を明確にしておく必要がる。

（1）対応窓口の設置

内外からの通報や問い合わせに対応するための対応窓口を設置し、もたらされる情報をキャッチする。窓口は、インシデント受付、被害者への対応、関係者への対応、報道機関への対応などの機能が期待される。

（2）連絡体制の整備

インシデントの発生を速やかに周知するため、予め連絡網を整備する。連絡網には当社従業者、委託先、社外関係者（関連会社、取引先、弁護士など）、行政機関（監督官庁、警察など）、報道機関を含む。

（3）意思決定機関ならびに対策本部の設置

インシデント対応では場面に応じた承認・意思決定を行うことになるので、意思決定機関を設定しておく。意思決定については、委員会など専門組織の設置や弁護士など外部の専門家の支援も考慮する。また重大事案に対応するために経営陣を中核とした対策本部の設置も必要となるが、対策本部を設置する必要があるか否かの判断基準も設けておく。

3.9.2.5 情報の収集と事実確認

インシデントが発見または発生した場合、適切な判断を行うための材料をそろえるため、まず情報の収集を行う。

（1）情報の収集

誰が、いつ、どのように、何をしたか、その結果の被害者数は、漏えいした情報の内訳は何かを把握する。

（2）事実確認

できる限り当事者にコンタクトし事実確認を取る。又聞きは憶測のもととなる。例えば当事者である上司を通して情報を得ると、保身や思い込みからバイアスがかかる可能性がある。

個人情報漏えいの場合は、自組織が所有する個人情報と漏えい情報を照らし合わせ、自組織から流出した可能性を判定する。

後の公表に備え、事実と推測を明確に分けて整理しておく。

3.9.2.6 インシデントの分析と評価

収集し確認した情報に基づきインシデントの分析と評価を行う。

（1）原因の究明

原因の分析のために、アクセスログの分析、関係者へのヒアリング、リスク分析に基づく原因の洗い出しを実施する。原因が特定できない場合は、想定されるシナリオをできる限り洗い出す。その際、1章で述べたように過去の事例研究が役に立つ。

例えば、“机の上に置いたはずのCD-ROMが無くなった”という事象が発生した場合、推測できる原因は1つではない。「ゴミ箱に落ちて、誤って捨てた」「搬送中紛失または盗難にあった」「誤送信された」「別の資料にまぎれた」「悪意のある社員が盗んだ」「外部の者が侵入して盗んだ」など複数のシナリオが考えられる。その中でも可能性が高いケース、またインパクトの大きいケースを想定して対応計画を立てる。

（2）影響範囲の特定

インシデントが、被害者または自組織に与える影響を検討する。想定される最大の被害者数の把握、風評被害などで影響を及ぼす先の特定、被害者にかかる負担の認識、情報の流出先の予測・特定などを行い、対応のために投入すべき人的リソース、コスト、時間的猶予などを算定する。

（3）公表の判断

インシデントの事実を外部に公表すべきかどうか判断する。判断にあたっては、被害者の希望、法的責任、社会的責任、影響度合い、公表することのメリット・デメリットを考慮する。

3.9.2.7 関係者への報告と周知

インシデント対応の一方のフローである周知について解説する。

連絡網で述べたとおり周知すべき対象には通報者、社内、被害者、関係者、行政機関、報道機関などがある。通報者には適切なレスポンスを返さないと、協力者であったはずが敵対者になる危険性がある。「あの会社はせっかく教えてやったのに対応が悪い。掲示板に書き込んでやろう。」などという事態を招くことも考えられる。

また、社内に関してはインシデントの事実を周知徹底する必要がある。被害者からは社内のどこにアクセスがあるか予想ができないため、被害者からの電話を受けた社員が的を外した対応をすると信用を失ってしまう。

3.9.2.8 公表

インシデントの事実を公表するか否かの判断は前述したとおりであるが、公表すると判断した場合は公表する内容や方法を決めて実施していくことになる。

（1）公表する項目と内容の特定

公表すべき項目を特定する。項目としては、謝罪、被害者の特定方法、漏えい情報の種類、影響範囲、対応窓口の案内、被害者への保障、経緯、原因、対策体制、対策内容などが挙げられる。また、公表にあたっての優先事項も決定しておくと良い、優先度の判断は、被害者の立場に立って何を知りたいかを検討する。おそらく被害者が知りたいのは、何が発生したか、だれが被害者か、漏えい情報は何か、どのような影響が考えられるのか、どこに相談すればよいのかといったことであろう。

（2）公表方法

公開方法は、影響度などの判断基準の設定し決定する。一般的な公表媒体としては、ホームページ、新聞・雑誌など刊行物などがある。随時タイムリーな情報を公開する場合はホームページを利用するが、インシデントの影響が大きく不特定多数に広くお詫びあるいは周知する場合は全国紙などに掲載することが多い。公表方法についてはコストも判断基準のひとつになるだろう。

公表媒体については、新聞社の連絡先などをリスト化しておくとすばやい対応が可能になる。

3.9.2.9 インシデント対策

対応フローのもう一方のフローである対策について述べる。

（1）漏えい情報の回収　（の努力）

一度漏えいしたデジタルデータは、事実上回収は不可能と考えるべきである。しかし、何も手を打たないというのは信用問題にもなるので、可能な範囲で努力はしなくてはならない。実際にとれる行動としては、名簿屋からの買い戻し、プロバイダーやネット掲示板運営者への削除依頼などであろうか。

（2）被害者の救済の検討

実際にどのような被害を被ったかにより、救済の方法とその実現性は違ってくる。例えば、クレジットカード番号やメールアドレスが漏えいした場合、漏えい情報を悪用されないように、被害者は様々なサイトに登録しているそれらの情報の変更を試みるかもしれない。そのような作業は大変な負担を強いるものであるが、そのような負担を漏えいした組織が肩代わりするのは現実的ではないだろう。しかし、被害者救済の一手段として検討だけでもしておく。

（3）緊急対応と長期的な対応

対策を計画する場合、緊急のものと長期的な展望のもと実施するものに分けて考える。緊急対応としては、被害拡大を防ぎ、２次被害を予防するということが目的になる。

長期的対応としては、現状復旧が目的になる。

3.9.2.10 インシデントの記録

インシデントは、その経験を後に役立てるため記録されなければならない。

記録は、すべてのインシデント対応活動について残されていなければならない。また、記録はその信憑性が要求されるため、改ざんや紛失から保護されなければならない。

3.9.2.11 インシデントのレビュー

インシデントは、その記録をレビューし学ばなければ、組織は同じ過ちを繰り返すことになる。インシデントの発生状況、原因、結果、容認・是正・予防の判断、また、是正・予防すると判断した場合の是正・予防処置の内容をレビューし承認する。

以上、事業継続計画の一部としてのインシデント対応について、その策定手順の方法を記述した。例として取り上げたのは個人情報漏えいであるが、各項目と検討事項は他のインシデントにも応用できるはずなので、各組織が重要と考える情報資産やそれに対するインシデントに読み替えて利用いただければ幸いである。

3.10 事業継続の観点から見た発生事象の傾向

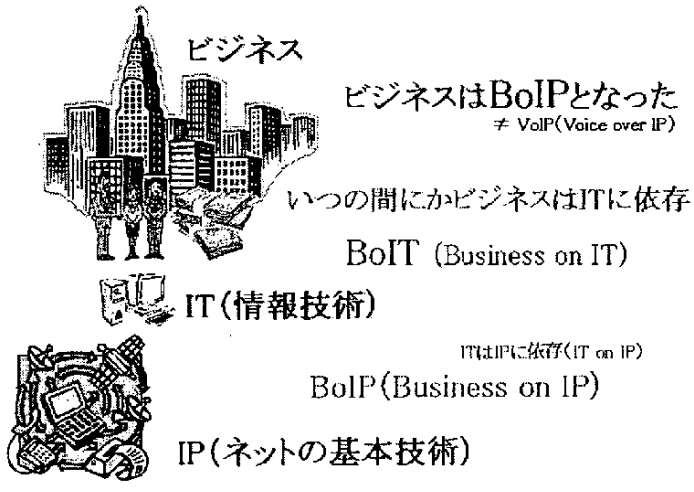
3.10.1 はじめに

ＪＳＯＣというのは、株式会社ラックという民間の会社が運用しているセキュリティ監視センターになります。ビジネスとしてお客様から対価を頂戴してサービスを行う以外に、実際に発生している攻撃の傾向や実際の事件などに関するレポートや注意喚起の発行などにより、皆様のセキュリティ向上に貢献しています。今回は、事業継続という観点から見た、特にセキュリティインシデント（ネット犯罪者やコンピュータウイルスなど）の傾向と対策のポイントに関して述べさせていただきます。

3.10.2 ２００６年情報 Security キーワード

「情報 Security キーワード」というより「ネット犯罪キーワード」と言った方が良いと思いますが、傾向として次の３点だと考えます。 一つ目として、Shifty （狡猾）が上げられます。これは単純な犯罪から、益々、巧妙というか狡猾になってきており、こちら側の対策の少し先をいく傾向が強くなってきています。２つめは Stealth（見えない）ということです。これは、大規模で目立つ愉快犯や自己顕示欲的犯罪から、金銭目的となってきているため見えなくなってきていること。何も起こっていないから大丈夫とはいえなくなってきていることが上げられます。三つ目は Spear/Sniper（槍/狙撃手）と言っていますが、犯罪が広域で無差別的にではなく、狙いを絞り限定的になってきている傾向が上げられます。これは最近、様々なメディアでも愉快犯から、金銭目的への犯罪のほうにシフトした等の報道も増えてきています。総括すると、２００６年は上記で示したような３つのＳとなり、続けると「狡猾で見えない槍や狙撃手」となり、従来の「単純で見える雨」よりはるかに厄介な状況になってきていることは事実と感じます。このことは、逆に言えば、ネットが単なる道具から、お金のなる木へ成長したことを物語っています。

3.10.3 背景



背景としては、そもそもＩＴやネットというものがビジネスに直結していなければ、情報セキュリティや IT システムと事業継続といった課題は出てこないわけです。所謂、ＶｏＩＰ（Voice over IP）という言葉があります。インターネット（IP：インターネットプロトコル）上に音声を通す技術、所謂、IP 電話のことになりますが、現在は、実は電話だけじゃなくて、

ビジネスがＩＰの上に乗っている、つまりＢｏＩＰ（Business over IP）になってしまっていることが、重要なことだと思います。ビジネスが IP の上に乗っているわけですから、いわばＩＰを足払いするとビジネスがこけてしまうというような状況に、いつの間にか、なっていると言えます。過去、実験的に拡大していったネットは、同時にオープンシステム化や、ダウンサイジング或いはエンドユーザーコンピューティング等のキーワードとともにビジネスの中に組み込まれていき、単に生産性を高めたりする従来の基幹システムだけではなく、新たな事業モデルを支える基盤となるようなネットサービス関係のシステムも出てきており、従来の基幹システム以外も事業継続を真面目に考える必要が出てきたということでしょう。現実に、ある大手の不動産会社の方は、（実は、不動産会社さんだからネットのセキュリティそんなに関係ないでは？と勝手に想像していました）マンション販売の８割以上はすでにネットからとなり、その為、無視できないエリアに発展し、同時に情報セキュリティ対策も重要な課題となったとおっしゃっておりました。それほど、ネットというのがお金になるようになってきているし、そこを中心としたビジネスモデルというのがどんどん誕生し変化しているというのは、皆さんご存じの通りだと思います。

3.10.4 業務中断リスク

そういった背景の中、事業中断リスクということを考えてみますと、昔から災害や、テロなどに関しては指摘をされておりますが、ＩＴ化によって、考慮すべき新たな脅威が出てきたということが重要なポイントです。一般的に、例えばネットでビジネスを展開している方というのは、昔から、ＤｏＳ（Denial of Services）は意識をされていました。ＤｏＳというのは、所謂サービス妨害と言われている攻撃です。例えば、最近は多くのデートレーダーといわれる方々がいて、個人で株の取引を行っているわけですが、彼らは、投資している株や興味のある株の動向が大変気になるわけです。その為、様々な情報を入手し、場の動きを察し、自分なりに判断し取引を行うわけです。毎朝９時になると、証券取引所がオープンするわけですが、そういった方々は一斉に証券会社のホームページにアクセスして、常に最新の情報を表示させるためにカチカチカチカチ（クリック）しながら情報を見ているわけです。こういう状況の中、何らかのニュースなどと重なると従来の常識をはるかに超えたアクセスが集中し、本人達は、意識は無いと思いますが、結果的にＤｏＳ状態等になり、運営している会社にクレームとして入ってくることになります。当然のことながら投資家としては、買いたいときに買うことが出来ない、逆に売りたいときに売ることが出来ないために大きな損失がでたり、儲けそこなったりするわけですから必死です。また、海外では、ギャンブルサイトなど止まると大きな損失が発生してしまうサイトに対し、わざと大量のデータを送りつけ営業妨害をし、その後、脅迫するような事件も報道されています。このＤｏＳは従来から言われている、情報セキュリティに関係する業務中断リスクですが、どちらかというと、力づくであり、物理的に近いリスクといえます。

ところが、今後、意識すべき業務中断リスクはこのような力づくだけではなく、むしろ論理的なリスクのほうが大きくなると考えられます。ネット犯罪などによる個人情報の流出、例えば、ホームページに外部から犯罪者が侵入し、個人情報が漏れた可能性があるような事件が起きると、事業が止まります。システムの再発防止策を取らずに運用を継続することはあり得ないわけです。

以前のように、ホームページが何者かに改ざんされるような侵入事案が発生しても、戻せば大丈夫、ということではすまなくなったのです。システムの弱点によって個人情報が流出した場合には、原因究明等を行い、再発防止策が取れない限り、原則再オープンは出来なくなっているのですね。　あと、昨年実際に発生しましたが、利用者がホームページを閲覧するとスパイウェアがダウンロードされてしまったというような、不正ソフトをばらまくための踏み台になったケースも放置するわけにはいかず、止めざるを得なくなっているのです。こういったことが、論理的な事業中断リスクとなり、最近非常に多くなっています。実際にこういった事件を起こされた方の大半は、こんなことで業務を中断せざるを得なくなるとは、思っていませんでした。

そういう観点で考えると、単に法律を守ればいいのかとか、そういうことではなくて、企業姿勢であるとか、従来の（悪い意味での）日本的やり方というのが本当に通用しなくなってきているのを感じます。

3.10.5 ２００５年の状況

3.10.5.1　報道された主な事件のトレンド

2005年、去年報道された主な事件を見てみますと、大きく２つのカテゴリに分かれます。一つ目は、情報の紛失や流出です。直接的な原因として Winny 上のコンピュータウイルスで機密情報が流出したケースやパソコンの紛失や盗難といったものですが、この種の事件での根本的な原因は３つあります。

(1) 実態を無視したセキュリティ対策（無理な対策）
　個人パソコンの持込使用の黙認、同時に機密情報持ち出しの黙認
　現実問題、予算の関係から支給されていない、編実問題、仕事を家庭に持ち込まないと対応できないなど。

(2) 人間の欲望
　海賊版・違法・アダルトコンテンツや海賊版ソフトへの根強い需要

(3) 無知・未経験・リテラシの低さ
　自己防衛の知識不足、他人事の脅威、コンピュータ操作などへの知識不足

２つめのカテゴリは金銭目的の事件です。通常金銭目的というと、クレジットカード情報のように金銭に直接アクセスできる情報を思い浮かべる方は多いと思いますが、それだけではなく、メールアドレスなどの個人にアクセスできる情報だけでも事件として発生しています。

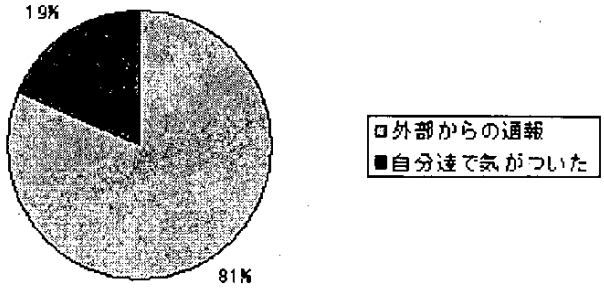
いずれのカテゴリで発生している事件も、物理的な社会でのそれと似ていますが、決定的に異なるのは圧倒的な匿名性とボーダーレスという特徴を持っていることにあります。こういう特徴は、仮想的な出稼ぎ犯罪に悪用されていると考える必要があります。

3.10.5.2 JSOCにおける緊急対応事案におけるトレンド

ＪＳＯＣでは通常はお客様のセキュリティ監視をしているのですが、契約のないお客様から「どうも侵入されたようだ」、「個人情報が漏えいしたのではないかと利用者から問合せが来たが、どうすればよいか」などの依頼を受け、緊急に出動し、対応や対応支援なども行っています。昨年、相談を受けたのは８０件を超え、実際に緊急出動した回数は 20 件を超え、過去最高となりました。

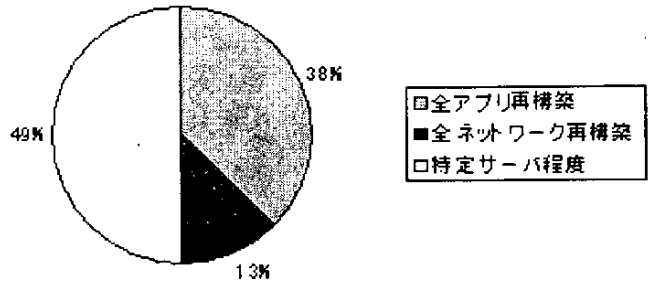
手口は右記の通りですが、2004 年では０件だったいわゆるＳＱＬインジェクションというデータベースに侵入する手口が 2005 年では全体の 50％を超えました。この SQL インジェクションでは、単に情報が取られただけではなく、スパイウェアのばらまきの踏み台を作るためにも悪用されていました。また、昨年の後半から増加しているのは、最近、日本でも時折報道がなされていますが、海外の金融機関等のフィッシングサイトになっていたという事案です。逆に単なるこれまでよくあった単純なホームページ改ざんでの緊急出動は０件でした。そういったレベルのものは、皆さんも依頼をしなくなったということだと思います。

あと、所謂最新のセキュリティパッチがあたっておらず侵入された事案も相変わらずありますが、相対的には減っています。それより増加傾向にあるのが、ＳＳＨブルートフォースというやつです。ＳＳＨは管理者が安全にサーバのメンテナンスをするために使う仕組みですが、そのパスワードをクラッキングされ侵入を許してしまう事件です。パスワードを犯人に破られ、入られるということは正規の管理者のアクセスと区別がつかず通常の防御システムが機能しないため、その後の調査も困難となります。私たちが対応した事案では、特に海外からのフィッシングサイト構築のための手口の大半はＳＳＨブルートフォースでした。

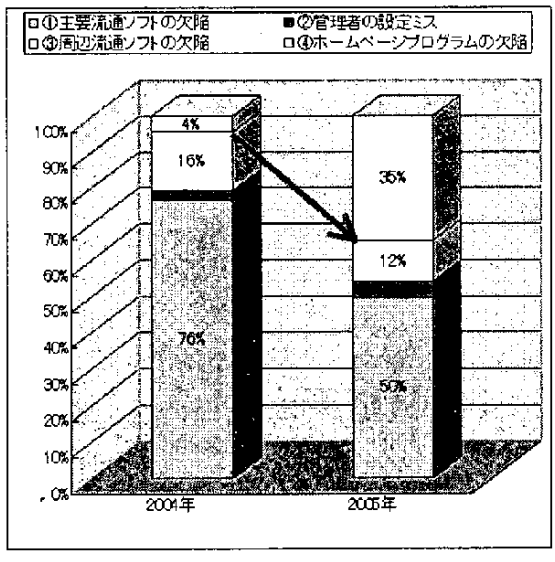


続いて、特徴的なことは、事案に自分達で気がつかないということです。実際、侵入されたお客様の８割は、自分たちで気がついていません。例えば、その利用者の方からの連絡をうけ、初めて異変に気がついたり、雑誌社などのメディアからの問い合わせで発覚したりしたケースがありました。

続いて、２００５年の事案で特徴的だったことは、再開するのが以前にも増して大変になったことです。特にＳＱＬインジェクションで侵入されたケースでは、データベースシステムに侵入されている関係で、ただ単にサーバを再インストールするだけではすまなくて、データベースのどこが改ざんされているか分からない為、全てのデータの完全性を確認することが求められます。しかも、データベースを使用しているシステムということは、事業に直結をしているようなサイトであることが多く、経営者としても再開が遅れると、会社存続の危機に直面してしまう恐れもあって、思ったより事態は深刻化します。実際に、昨年は約半数の事案で、すべてのコンピュータプログラムの作り直しやネットワークの再構築を行っており、特定のこのサーバだけの対応で済んだのは、全体の半分となり、これも２００４年とは大きな違いが出ています。



3.10.5.3　JSOCにおけるセキュリティ監視におけるトレンド



次は、攻撃者の、日々の攻撃行動というのは如何でしょうか、という話題になります。２００５年一年間で実際にJSOCで監視をしている中で、攻撃者は様々な攻撃を仕掛けてきます。通常の攻撃は、別に恐れることはないし、実際何の脅威にもならないのですが、時折、有効な攻撃や侵入された疑いが高いケースに遭遇します。そういう有効に効いてしまった攻撃を集計したのが「有効な手口の推移」となります。これによると、2004年では、例えばウインドウズやアパッチというウェブサーバなどの主要流通ソフトの欠陥によるものと、例えばデータベースソフトやバックアップソフトなどの周辺流通ソフトの欠陥によるものが主流でした。ところが、２００５年では前述の緊急対応事案と同じように、ホームページプログラムの欠陥、いわゆるＳＱＬインジェクションというのが有効な攻撃手口として非常に増えています。前年の８倍です。重要なことは、攻撃そのものの急増も脅威ですが、それより有効となる攻撃が急増していることはもっと着目する必要があります。

2004年

No.	Attack	Rate
1	IIS PCT/SSL BufferOverflow Attack	30%
2	Vulnerability Scan	16%
3	OpenSSL MasterKey BufferOverflow	15%
4	FrontPage Server Extensions BufferOverflow Attack	12%
5	Telnet login Overflow Attack	6%
6	Windows LSASS BufferOverflow Attack	5%
7	Apache Chunked Encoding Attack	4%
8	Cross Site Scripting Attack	4%
9	OpenSSH Challenge Respose BufferOverflow Attack	3%
10	FTP Brute Force Attack	3%

2005年

No.	Attack	Rate
1	SQL Injection Attack	32%
2	IIS PCT/SSL BufferOverflow Attack	16%
3	OpenSSL MasterKey BufferOverflow Attack	11%
4	Veritas Backup Exec BufferOverflow Attack	11%
5	MS SQL BufferOverflow Attack	7%
6	Cross Site Scripting Attack	6%
7	FrontPage Server Extensions Attack	5%
8	Microsoft ASN1 BufferOverflow Attack	4%
9	Microsoft WINS BufferOverflow Attack	4%
10	Web Defacement	4%

左の表は少し細かくした攻撃の傾向ですが、いずれにせよ Web サーバが一番狙われているという傾向は変わりませんが、2004 年ではいわゆるバッファ・オーバーフロー等の脆弱性を付く攻撃が１番でしたが、２００５年では２番目に落ちました。逆に２００４年では欄外だったＳＱＬインジェクションが２００５年では全体の 32％を占めるようになり、トップの座に着きました。「ワースト手口 of 2005」はやっぱりＳＱＬインジェクションだったということです。引き続き多いのがＳＳＬ関係です。安全に取引をするため、所謂「https」を実現するためのためのプログラムです。ここを狙ってくる攻撃というのが非常に高位置を実はキープしております。というのが、２００５年での有効な攻撃の観測状況です。続いて、ＳＱＬインジェクションをかけてくる推測攻撃元は８割が中国からでした。残りはアメリカ、韓国といった部分です。現状では、ほとんど中国からと言っても過言ではありません。

3.10.5.4　セキュリティ検査での対策状況におけるトレンド

今度は、実際の対策状況はどうでしょうかということになります。２００４年は実際に１２２のサイトに対して Web アプリケーションの脆弱性診断を行ったところ、約４割のサイトでＳＱＬインジェクション等のインジェクション系の欠陥が見つかりました。あとは、クロスサイトスクリプトと言われる欠陥が約７割のサイトで見つかりました。２００５年になり、個人情報保護法も施行され、様々な事件も発生し、特にＳＱＬインジェクションが危ないと、メディアや、関係省庁や関係機関において、一生懸命啓蒙活動をやられましたが、それでも実際は変わっていない、改善されていないということです。２００４年と２００５年を比べてみますと、インジェクション系については同じです。セッション管理不備は多少改善しているものの、ほとんど誤差と捉えていいくらいだと思います。クロスサイトスクリプティングも誤差の範囲かと思います。基本的には残念ながら、ほとんど改善していないのが現実です。

欠陥内容	2004年	2005年
インジェクション系	39%	39%
セッション管理不備	61%	59%
アクセス制御不備	39%	7%
クロスサイトスクリプト	67%	54%
仕様上の問題	56%	52%
設定上の問題	16%	16%
その他	52%	43%
母数	122	155

原因ですが、大きく３つあると考えています。一つ目は、駄目だった実態や対策ノウハウが共有できていないことが上げられます。例えば、Ａ社が診断を申し込みます。そうしたら、次にＡ

社が別なサイトで診断するときには少しは改善されているだろうと考えるのですが、実は改善されることは少ないのです。毎回、改善されていない。原因として、その Web サイト開発プロジェクトとしては脆弱性がないことが確認できれば基本的には目標を達成して完了してしまい、結果、情報は共有されることなく同じ過ちを繰り返しているのではないかと考えられます。こういった理由から問題を指摘されてもそれが共有されることはなく、共有しようとしても、逆に自分たちの恥になると考える人もいて、共有されることは残念ながら少ないようです。

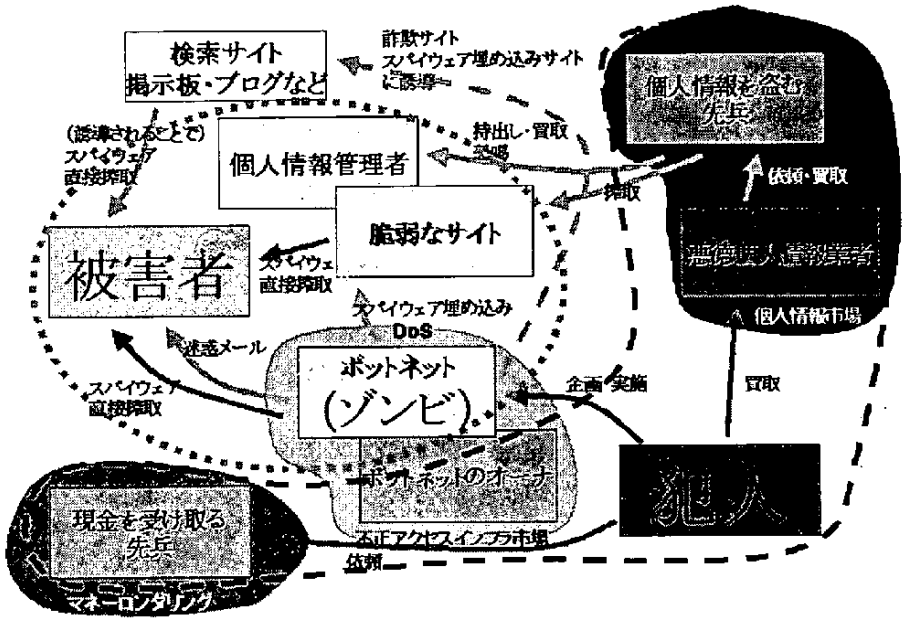
2つ目は、開発業者もセキュリティを組み込んだ提案をしづらいということです。そういう提案をすると、ユーザからは当たり前のように言われ返って収益を悪化させかねないことさえ、考えられます。別にセキュリティ関係で特に有効な営業的差別策になっていないということですね。逆にセキュリティの提案をしたために、責任を取らされたり、お金も負けさせられたりする、事例も多いようです。

3つ目は、そもそも気がついていないケースです。気がついていないという人は本当に多いです。特に、（メールアドレスのみを含む）個人情報を保持しているサイトの管理者は Web アプリケーション点検を行ったことがあるかどうか、ログの確認を行ったことがあるかどうか、チェックしてください。

これらの3つの要因が絡み合って、改善されていないという、現状が残念ながらあるように思います。その為、個人情報取り扱い事業者のサイトなどは、個人情報保護責任の観点で責任を問うような動きも、今後非常に重要でないかと思います。

3.10.6 様々な脅威は何故発生しているのか？

今メディア等で、さまざまな脅威の話が出てきます。前述のＳＱＬインジェクション、ボットネット、スパイウェア、迷惑メール、フィッシング、ＤｏＳなど、こういう脅威を個別の点としてとらえ、対抗していく考えもありますが、何故このような点としての脅威が存在するのか？ それを点ではなく線としての関連を理解することは、点そのものを見ることより重要なことと考えます。



ここで、一つの仮説をお話します、まずは、被害者と犯人が存在すると仮定します。ここでいう被害者はお金を取られる人で、犯人というのは取ったお金を得る人です。この犯人はどんなものがほしいでしょうか？

やはり、何かやろうとすると、個人情報がやっぱり欲しいですね。特に個人にコンタクできるメールアドレスはほしいでしょう。さらに、このコンタクトする人たちがどんな特徴（例えば、３０歳代独身男性、健康食品をネットで買ったことのある人など）を持った人たちかが分かるとさらに良いですね。緊急事案にて出動し、被害にあったサイトの管理者に「当社はクレジットカード情報などの、お金に絡む情報は扱っていないので大丈夫だと思っていました」と言われることが、よくあります。そうじゃないです。犯人側は別にクレジットカード情報などのお金に絡む情報だけが欲しいわけではないのです。こういった個人にコンタクトできる情報も重要なので価値が生じるのです。その為、個人にコンタクトできる情報だけを盗む人が出てくるわけで、脆弱なサイトに侵入しメールアドレスを取りに来るのです。この種の人たちの目的はクレジットカード情報ではないかもしれません。

次に、最近よく言われているボットネットや不正アクセスツール或いは、アクセスを中継するような仕掛けはどうでしょうか？こういったものを使用して、迷惑メールを効果的に出したり、フィッシングサイトを構築したり、侵入して個人情報をとったり、DoS をしかけたり、スパイウェアを埋め込んだりできる道具も価値が出てきますね。次に、こういったものを悪用し、被害者にスパイウェアを埋め込み、銀行へのアクセスコード、やクレジットカード情報などの金銭へのアクセスコードを盗み取り、基本的にはお金を取っていくのではないかと考えられます。一人で全部やることも考えられると思いますが、全ての犯人が金銭を直接盗むという危険なことをするのではなく、点で見れば比較的安全なグレーな行為で金銭を稼いでいく人もいると考えるのが自然かと思います。そういうことで言えば、ネット犯罪は益々分業化・専門化が進んでいくと考えるのが自然です。 この図で、緑点線で囲った部分と黒点線で囲った部分があるわけですが、黒点線部分は基本的に悪い人ですね。（グレーを含め）悪いことをしようと、基本的に思っている人です。ところが、緑点線で囲った部分の中はすべて被害者なのですが、ある面でボットに感染したパソコンや SQL インジェクションで個人情報を抜かれるサイトなどは、ある面被害者でありながら加害者側に加担をしている側面も持っています。

特にここで重要なのが、所謂、犯人は最終的に例えばクレジット情報が欲しかったりとか、銀行へのアクセスコードが欲しかったりするわけですが、それを取り巻いて市場というのができるわけです。例えば、これは個人へのアクセス可能な情報の市場です。メールアドレスだけ取れば、売れるという市場がそこにあるわけです。だから、別に決済情報を持ってないサイトでも、メールアドレスというのがこの犯人にとって売れそうな情報であれば、被害にあってしまう恐れがあるということです。

ですので、よくＳＱＬインジェクションという点としての脅威の話をしても他人事で対策の必然性を理解できない方は多いです。しかし、経営者には、点としての脅威が他人事でないことは、それを点ではなく線として捉えると理解はしやすいようです。それだけ、ネットがお金になるという時代になり、自分達もそこが重要な場所であることは皆様よくご存知です。その為、そこには自分達以外にもお金を求めてくる人が現実的にいるということです。そのあたりをよく理解するというのは非常に重要なことだと思います。前述の仮説の場合ですと、単にメールアドレスだけでも市場が出来上がるということです。これはワンノブの話であり、まだいろいろな市場が考

えられます。

3.10.7 まとめ

２００６年のキーワード Shifty（狡猾）、Stealth（見えない）、Spear/Sniper（槍/狙撃手）の３つですが、この背景は、多くの情報セキュリティ事件は事業継続に大きなインパクトが現実的に出ることを意味しています。ポイントは、自分は関係ないということはないということです。やっぱり一番は気がつくことというのはスタートラインです。気がつかなければ、事業継続も何もひったくれもありません。どれだけ早く気がつくかという、ここを考えるというのは非常に一番大きなポイントだと思います。この発想なくして、通常の管理システムだとか、そんなのを買っておいても何の得にもなりません。気が付くためには見る努力が必要なのです。所詮見えなければ気が付くことはありえません。

基本的に、対策には安心策と安全策があるとよく言われます、特に日本では安全策が重要視されているように思います。それは、当然ですが問題は、安全策を施して安心していることです。実はそれでは安心できないのです。安心するためには、いざ何かがあっても対応できる、こういうときはこうする、ということが明確であれば、危険でも安心できるかもしれません。

いずれにしてもそれをやるというのは、見えるようにするというのがスタートラインです。「見える化」があり「気が付くことが出来」手が打てるのです。その仕組みをいかにつくっていくか。しかも、現在は、これまで言ってきたように相手は狡猾で槍/狙撃手です。つまり地域限定型、広範囲に起きないので自分のとこだけでも起きるのですね。さらに、見えない。なぜ見えないかというと、相手はいずれにせよ金銭目的の犯罪者なので、見られたくないし隠れたいわけです。隠れているのだから、当然見る努力なくしては見ることはできません。ですので、この製品を買ってきたらとか、この製品で全部守れるのかとかというのはありえないのです。なぜかというと、基本的に彼らはそれを逃れようとしているからです。

一般的に言えば、今の犯人たちというのは高度な技術を持っているわけではなく、自分たちの持っている道具で入れるところを探します。今のところ、日本では、例えば、あそこに何が何でも侵入したいなどという目的は基本的には持っていないのですね。そうではなくて、自分たちの道具で取れる情報をとり、市場に流していくと考えるのが自然です。そう考えるとセキュリティ対策はある程度足並みをそろえた方が有効と言えます。人が対策していることはちゃんとやっておく、今流行っている手口についてはちゃんと対抗しておく、ことが極めて重要なのです。突出した対策はある面手口の悪質化を加速させる働きを持っていることも意識しつつ、ぜひ情報セキュリティの対策、事業継続経営・計画を合理的に、有効に実施していただきたいと思います。

3.11 情報セキュリティに関係する法律の紹介

情報セキュリティに関係する法律として、個人情報保護法と、ｅ文書法、ＳＯＸ法、公益通報者保護法について紹介する。

3.11.1 個人情報保護法

ここでは、個人情報保護法の条文解説ではなく、同法以外の法令等の再確認と、同法とプライバシー保護の関係に着目した要点を紹介する。

個人情報保護法は個人情報の保護に関する法律であり、内閣府のＷＥＢページ（※１）にて、法律の全文を参照することができる。

図3.45:個人情報保護に関係する法令等

個人情報保護法
「個人情報の保護に関する法律」
http://www5.cao.go.jp/seikatsu/kojin/index.html

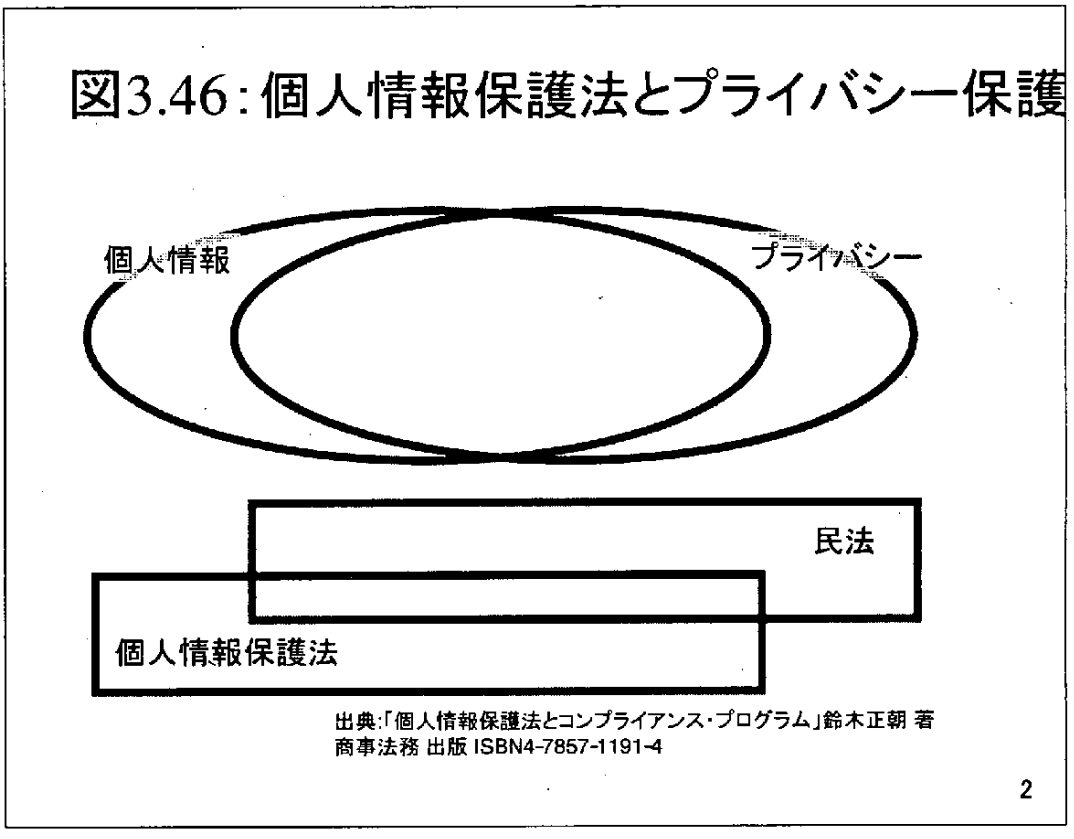
省庁	日付	内容
総務省	-	迷惑メールに係る対応方策の検討について(論点整理)
	-	独立行政法人などの保有する個人情報の保護に関する法律に係る行政手続における情報通信の技術のりように関する法律施行規則
	-	行政機関等個人情報保護法(個人情報保護関連5法の概要)
	-	放送受信者等の個人情報の保護に関する指針
	-	電子タグに関するプライバシー保護ガイドライン
	-	損害保険会社に係る個人情報保護指針(個人情報指針)について
	H16.9.14	「行政機関の保有する個人情報の適切な管理のための措置に関する指針」及び「独立行政法人等の保有うする個人情報の適切な管理のための措置に関する指針」
	H16.8.13	「放送分野における個人情報保護の基本的な在り方について」の公表
		特定電子メールの送信の適正化等に関する法律
経済産業省	H14.6.21	特定商取引に関する法律施行規則の改正について(電子メールによる一方的な商業広告の送りつけへの対応)
財務省	H16.10.25	財務省の所管する事業者等.個人情報の保護に関する法律(個人情報の取得等、管理etca0

1

図 3.45 には、個人情報に関係する法令等の一部を一覧にしたが、企業における個人情報に関しての法令順守対策として、個人情報保護法だけを検討したのであれば業種業態によっては不十分な場合がある。個人情報保護法の中で個人情報は利用目的を通知又は公表し、その利用目的の範囲内で利用するとしているが、それと同種の管理義務を求める法律は個人情報保護法だけではない。たとえば、総務省による特定電子メール送信の適正化等に関する法律や経済産業省による特定商取引に関する法律施行規則の改正、いわゆる迷惑メール防止という観点の法律などもある。

実際には、個人情報保護法の定めは、これらの法令等とも密接な関係を持っているため、企業あるいは組織においては、個人情報保護のための対策として、複数の法律の対応を取っていなければならない。万が一、個人情報保護法しか見なかったという場合には、法令順守を達成してい

るとは言えない可能性のある状態なので、業種業態に応じた再確認をしなければならない。



次に個人情報保護法とプライバシー保護との関係について要点を説明する。図 3.46（※２）は、個人情報保護とプライバシー保護は、全く一致するものではないということを示している。いわゆる個人情報についての問題が生じる際に関係する観点として、図中の左側で示した個人情報保護法と、右側で示したプライバシー保護といっている部分に関しては、ほとんどのものが重なるが、全く一致しているわけではない。

それならばプライバシー保護法というのがあるかというと、日本の場合にはそのための個別の法律はない。憲法の中でもプライバシーという用語は直接使われていない。実際には民法の中で損害賠償に関することとして解釈されることがある。いわゆるプライバシーが侵害されたということを損害だと主張する形で民法の損害賠償請求が起こるという考え方であり、今のところはこの損害賠償問題の中で問われるのが多くの場合である。

こちらの図ででは、左側のところは個人情報保護法に違反するか否かで、法的責任が問われるが、若干、右側のところにはみ出た部分がある。この部分というのは、個人情報保護法の範囲ではないが、受け手がこれは自身にとっては嫌なことだったというふうに思えば、それはプライバシーの侵害、あるいは個人情報の不適当な取り扱いになるという形で民法の損害請求が起きる領域である。したがって、個人情報保護法だけをかっちりやっていたからといって、個人情報に関する企業の訴訟リスク対策がそれで十分だということにはならないということが、この図で示されている。

図3.47：個人情報保護法とプライバシー保護

この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

「個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号）」より転載

3

図3.48：個人情報保護法とプライバシー保護

プライバシーの侵害による不法行為の成立要件

公開された内容が私生活の事実またはそれらしく受けとられるおそれのある事柄であること

一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められること

一般の人々に未だ知られない事柄であること

その他、被害者が公開により不快、不安の念を覚えること

『宴のあと』事件」判決（東京地判昭和39年9月28日）より
出典：新保史生先生 http://hogen.org/research/paper/jp/

4

個人情報保護とプライバシー保護の違いを確認することにする。図 3.47 が、個人情報保護法が定めている個人情報である。それに対してプライバシーの保護として問われているものが図 3.48 である。

個人情報法が定めた個人情報とは、会話言葉でいう「いわゆる個人情報」に関して、幾つかのポイントをふまえるとよい。まず、電子、非電子を問わないため紙の書面も電磁的記録も対象となる。それから、個人情報というと顧客情報がすぐに連想されるが、従業員のことに関しても対象となる。例えば、従業員に自宅の電話番号について利用目的を示さずに聞くということは、この法律では問題となる。自宅の電話番号を聞くにはその利用目的を従業員に示している場合が適法であり、そうでなければ違法でない場合もあるがグレーとなる。これら２つのポイントはプライバシー保護でも相違はない。それに対して次の２つのポイントはプライバシーとの大きな違いとなる。法人等の連絡先情報も個人情報保護法の場合には、個人の名前と結び付いてしまえば、基本的には個人情報として扱う。いわゆる名刺に書いてあるようなことも個人情報の対象になる。このことは、プライバシー保護とは異なる。さらに違いが顕著なのは、個人情報保護法では公知の情報も対象となる点である。企業のホームページに掲載されている社長の名前とその企業の住所という組み合わせも、同法では個人情報の対象となる。

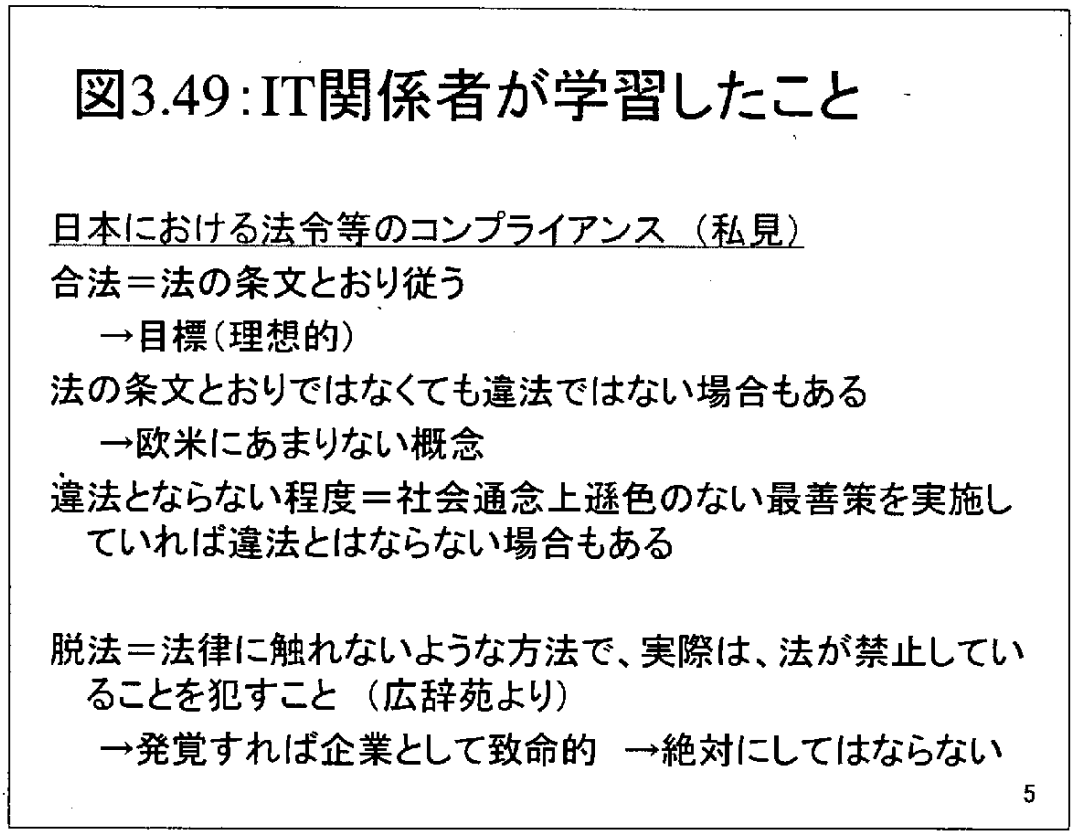
図 3.48 であるが、プライバシーの侵害というのは先ほど述べた通り、日本の場合には明確な定義はない。現在国会を通じて憲法改正議論があり、その中で日本もプライバシーというものを憲法の中に盛り込むことの是非についての議論はあるが、今のところは明確に定義されていない。ただ、今のところ裁判になった場合にプライバシーの侵害という言葉を使われた場合には、昭和 39 年の判決文に書かれた図 3.48 の文章の定義が、日本におけるプライバシー侵害の定義として使われると考えられる（※４）。これは判決文をベースにしているので、この後、万が一、別の判断が示されれば、この内容は変わるかもしれない。そういうことでは困るから、憲法等で明文化してもよいのではないかという議論がなされているわけである。

判決文の３番目に記載されているとおり、「いまだ知られていない事実」という点については、個人情報保護法の定義とは異なり、公知の情報に関してはプライバシー侵害にはならない。それから、法人等の連絡先みたいなものも業務上、お互いの同意に基づいて交換しているようなものはプライバシーの侵害ということには該当しないということになる。このような違いが若干あるものの、ほとんどのことは大体かぶるというところが、先の図 3.46 に示されている。

ただ、ここで注意しなければいけないことは、プライバシー保護の考え方の多くが欧米から日本に輸入されてきていることである。欧米でいっているプライバシー保護プログラムの中には法人等の連絡先、それから公知の情報を保護するという発想はない。その部分に関しては注意しないと、日本の個人情報保護法の範囲との違いを見落とすことになる。

参考までには、米国ですと法人等の連絡先というのは個人情報（Personal Information）とは区別して、コンタクトインフォメーション（Contact Information）と呼ぶ。また、法人として契約を締結するために住所と氏名を書く場合がある。そのような場合には、実際にはその住所が本人の所在地ではなく、契約書上住所を書かなければいけないので、法人が契約書を書く際に記載

する場合などである。支店の住所ではなくて本社の住所を書くという運用をしている場合もあると考えられる。そのため本来は本人の連絡先の住所としては特定されていないわけですけれども、そういうようなものは欧米ですと、管理情報（Administrative Information）という呼ばれ方をしており、これら以外の特定可能個人情報（PII: Personal Identifiable Information）とは区別した情報管理規程を設けている場合がある。ただ、日本の個人情報保護法の定義によると、それら名刺に書いてあるものも、それから契約書に書いた名前も区別することなく個人情報ということになっているということについて注意しないと、欧米の施策をそのまま使っても不整合が出る可能性がある。



このように、根拠となる法令等や価値観が異なれば、法令等に準拠するために講じる措置には違いが生じる可能性に注意をしなければならない。また、私見であるが、欧米での法令のコンプライアンス策を参考にする場合には、日本においては合法、違法、脱法ということについても考察をした方がよいということを図3.49に示した。

合法というのは法の条文通りやるということである。書いてある一言一句をちゃんとやるということだ。これは目標である。ただ日本の場合、この法の条文通りではなくても違法ではない場合もある、というふうに考えることができる。この発想は実は欧米にはあまりない。法律に、やれと書いてあることは必ずやらなければならないし、禁止と書いてあることは一切やってはならないのである。ただ日本の場合には、実施義務や禁止行為が書いてあっても、社会通念上遜色の

ない最善策としての行為であれば違法とはならない場合もある。

例えば、先ほど名刺の内容は個人情報に該当すると述べた。日本の社会慣習上、社員が退社する際には今持っている名刺などは持っていく場合も考えられる。ただ、これは個人情報保護法の条文通りですと、前職の企業から次の企業に第三者提供をしたということになってしまいかねない。まったくの合法とするには、本人からの事前の同意を得ないといけないことになる。そのため、退職する直前に、もらっている名刺の人、全員に連絡をして、「私はこのあと別の会社に行くので、その会社に持っていっていいですか」という同意を得ないと違法ということになるかもしれない。ただ、そんなことまでをするかどうか、あるいはそこまでしないからといって違法を問われるかというところに関しては、日本の場合、若干あいまいだ。前職の名刺を持ち出すことは、営業機密の観点で、企業としては禁じることがあるだろうが、それは個人情報保護法のためでは本来ないはずだ。したがって、名刺を持っていくことは社会通念上遜色のない最善策であれば、許される場合もある。ただ、それが非常に大きな問題を起こせば、全く同じ行為であっても違法だと言われることもあるかもしれない。

このあたりのサジ加減が難しいということについて、個人情報保護法に企業が対応する際に、学習したことと書いた。法令にコンプライアンスするということは、単純なことではないということだ。ただ、そこで一つ言えることは、脱法はまずいと考えられる。つまり、法律に触れないような方法で、実際は法が禁じていることを犯すことはしてはならない。図では広辞苑を引用したが、「法律に触れないように、法が禁じていることをする」という日本語として何か成り立っていないようにも思える説明となっている。これがまさに日本のコンプライアンスのとても難しいところである。

難しいことではあるが、発覚すれば企業として致命的だ。場合によっては倒産するかもしれない。違法を絶対にしてはならないかというと、違法の定義は実はあいまいで絶対とは言い切れない状況も出てくると考えられるが、脱法は絶対にやらないようにしないといけない。

具体例で申し上げると、例えば企業がお客様からアンケートを採って、抽選で何かプレゼントを差し上げるというアンケート用紙をつくったとします。その場合、個人情報保護法上はそのアンケートの中に利用目的を記載しないとならないため、「当選者の方に景品を発送するためだけに使います」と仮に書いたとしましょう。ただ、会社のホームページには「当社のアンケートにお答えいただいた方には、製品の案内などのダイレクトメールを送ります」と書いておいたとしましょう。そうすると、この個人情報保護法は通知もしくは公表すればいいということになっているので、アンケートには抽選のためだけだと書いておきながら、ホームページにはダイレクトメールを送りますと書いていれば、法律上許されるという解釈をすることも可能かもしれません。

ただ、これを読んでお分かりのように、明らかにそれは法の条文の揚げ足取りです。通知または公表という揚げ足取りをして、お客さんにダイレクトメールではないような印象を与えつつ、実際にはホームページで公表はしているよと開き直るということを故意にすれば、脱法という形で問われる可能性がある。そのため、違法は問われないとしても、脱法と解されないように注意しなければいけないということが重要なのである。

3.11.2 e文書法

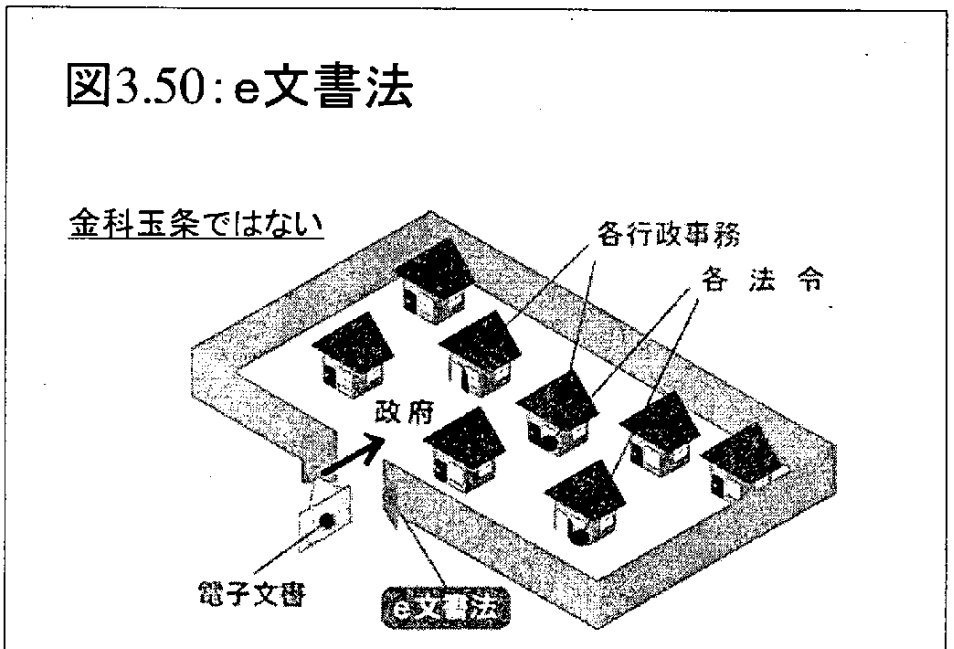
e文書法は、個人情報保護法と同じ、２００５年の４月１日に施行されたが、個人情報保護法が非常ににぎわったためか、その陰に隠れてしまった感がある。最近になって、ＩＴ業界でも動きがありますので、これに関して触れておく。

e文書法というのは通称であり、法律の正式な名称は、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（以下、通則法）」と「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律(以下、整備法)」という２つの法律のことである。通則法が、行政文書を電子化することについて許容した法律である。

日本の場合には、行政文書はどう扱うべきかというのは、それぞれの法律で定めている場合もあるため、一つの法律をつくるだけでは行政文書を電子化することはない。そのために整備法というものを用意して、この中で既存の法律のここの部分に関してはこういうふうに解釈をしてもいいというものを箇条書きに、実際にはe文書整備法の場合約 70 の法律に該当するが、それらの法律に対して、書面といっているものは電子書面でも構わないということを書き連ねるというようなことをして、それぞれの法律の内容を再定義するという構造になっている。

e文書法自体は、そのような呼び方がわかりやすいということで、先の２つの法律だけのためによく使われるが、これに関連する法律は、実際には日本として初めての法律ではなく、ＩＴ基本法（高度情報通信ネットワーク社会形成基本法)、電子署名法（電子署名及び認証業務に関する法律)、ＩＴ書面一括法（書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律）という伏線があった上で、最後にｅ文書法が制定された。これらの法律の条文そのものは、ＷＥＢページを記載した、首相官邸のホームページ（※３）にまとめられている。

図3.50:e文書法



ｅ文書法だが、昨今、ｅ文書法対応ソリューションという言葉をときどき目にするが、この言葉は注意して受け止めるべきだ。まず、このｅ文書法は金科玉条ではない。箱庭のような図で示しているが、政府が扱う行政文書があるとすると、実際にはそれらの行政文書は各行政事務の各法令で決まっている。今まで個々の法令において、書面には電磁的記録、すなわち電子書面を含まず、書面は紙であるという明記や暗黙の解釈があったために、行政文書は電子文書について特段の認めをしていない限り、原則は紙文書のみとなっていた。つまり、箱庭の門が電子文書に対して閉じており、門前払いであったような状態だった。ｅ文書法によって、一番先頭の門戸が開放された。つまり、電子文書が、原則除外から、原則認めるに変わったものの、このあと本当に行政事務のところで、電子文書としてそれを受け付けるかどうかは、各法令がその手順手続き等々を明確に定めていくという必要がある。

そのような時点において、ｅ文書法対応という言葉は、何に対応しているのかを確認する必要がある。例えば税務申告の書類であれば、税務申告書類に関しての行政文書対応ソリューションという言葉はよいが、ｅ文書法対応という言葉は本来正確ではない。ただそう言うと分かりやすいというだけで使っている状況が散見される。実際の部分に関しては、このあと各法令などの運用の中で決まっていくと考えるべきである（※５）。

では、その個別の要件がないと何が問題になるのかであるが、経済産業省から 2004 年に「文書の電磁的保存等に関する検討委員会報告書」（※６）が公開されている。これは、通称、ｅ文書法ガイドラインと呼ばれている。ガイドラインの中で、見読性、完全性、機密性、検索性などを要件として示している。例えば、見読性では解像度について、モノクロの文書に関しては 150dpi 以上でスキャンすることなどということが記載されているが、これを 150dpi のスキャンをすればｅ文書法対応ソリューションだと解釈するのは正確ではない。

このｅ文書法ガイドラインが記載しているのは、十分条件ではなく必要条件を書いているだけで、少なくともこの報告書が書いてある必要条件よりも下回る条件では、今までの門前払いと同様だということに過ぎない。これらの条件は必要条件であって十分条件ではない（※７）ということが重要である。

例えば見読性というのは、文字が読める程度にスキャンしなければならないということだが、それならば文字が読めればいいのかというと、そう単純ではない。それは提出する側の観点だけでしかない。受理する側の観点からすれば、スキャンする前に改ざんがされていないかの有無を確認できる程度の解像度を必要とすることになる。そのため文字を読める程度のスキャンでは、受理してもらえない可能性がある（※８）。受理してもらうための十分条件は、行政文書ごとに決まると考えるべきである。ここでは、見読性における解像度のことだけを例に示した。これに限らず、ガイドラインにある要件は必要条件として対応をしなければならない。その上で、ｅ文書法対応ソリューションと称しているものについては、どの点において対応しているかを判断して導入する必要がある。

3.11.3 SOX法

米国のＳＯＸ法の詳細はここでは申し述べないが、サーベンス氏とオクスレー氏が議会立法したのでＳＯＸ法と呼ばれるが、正式な名称は、Corporate and Criminal Fraud Accountability Actというものだ。米国企業改革法と訳されることもあるが、もとの英語の意味は、企業改革法ということでもない。企業及び犯罪の不正行為の説明責任についてというような名称である。このとき、日本版ＳＯＸ法対応ソリューションという言葉を使った場合に、それが何を意味するのかというのは注意が必要だ。日本版ＳＯＸ法が決まっていない時点で、その対応ソリューションというものに何を期待すべきかには注意すべきだろう。

アメリカにおいてＳＯＸ法は何を目的にしたかと言うと、企業における財務諸表、すなわち、頭の中にエクセルの表のようなものを思い浮かべていただければよいが、財務諸表に書いてあるそれぞれの数字が正しいということを何をもって担保するのかを、説明できる体制を構築することが、大きな目的のひとつである。

そのため、アメリカにおいては例えば経理の仕組み、それから帳票を処理する仕組み、それから民間同士の取引における証拠性の問題というものも、すべてアメリカのいろいろな環境とか法整備の上にのっとった上で、足りない部分をＳＯＸ法として補う形で、財務諸表という紙を見たら、その財務諸表の紙の中の数字がすべて正しいということが担保できることを企業に求めた。その前提部分がまず日本の場合違うため、日本版ＳＯＸ法というのが今までの日本の商取引、あるいは担保の仕方という考え方を根底から変えようとしているのかということが決まらないと、アメリカにおけるＳＯＸ法対応ソリューションのどの部分が日本で再利用可能かが決まらない。今の時点で、何をもってして日本版ＳＯＸ法の定義とするのかというのは、あいまいな要素が多い。

ただし、いずれに決まるとしても、財務諸表の内容に間違いがあると問題になるということは事実なので、財務諸表の内容が正しく積み上げができていることの説明責任を果たす取り組みを見直すきっかけは日本で始まることになる。それのための準備は、日本版ＳＯＸ法ができるかできないかとは別に、各企業は取り組んでおくべきだ。

これは財務諸表が関係する話ですから、少なくともＩＴエンジニアだけの視点でのソリューションには注意が必要だ。財務諸表のここの数字はどういう数字で出来上がるのかということが、その経理のフローとしてちゃんと分かったら、そのフローのそれぞれに対して、いわゆる内部統制と呼ばれるものを注入するということによって、財務諸表という表の中に出てくる数字が現場の実体と一致しているということが担保されて、それによって財務諸表の内容が、紙だけ見れば会社の実態が分かることが担保されるという三段論法なのである。

ＳＯＸ法対応ソリューションと言っているのは、少なくとも米国で成功したソリューションが日本で成功するとは限らない。限らないというのは、成功するかもしれないが、成功しないかもしれないということで、その時点で、日本版ＳＯＸ法対応ソリューションという言葉には注意するべきである。

3.11.4 公益通報者保護法

公益通報者保護法が、２００６年４月１日から施行される。わかりやすく言うと、内部告発者を保護するための法律ということになるが正確ではないことについて紹介する。企業の中の組織人、従業員等がうちの会社は何かおかしなことをやっているということを気づいて報告する際に、それを報告することによって報告者に不利益が与えられないようにしようというものだ。それを保護するという考えがない環境でそんなことをしたら、ただ単にクビになるか左遷されるか、もしかするともっと大変なことになるかもしれない。そのような不利益を与えてはいけないということを法律で定めたのが、公益通報者保護法だ。

同じようなものは、アメリカには 1989 年と古くからあり、内部告発者保護法（Whistleblower Protection Act ）と呼ばれている。不正なことを組織がやっているということであれば、それを内部告発した際に、内部告発した人に不利益なことをしてはいけないと定めています。

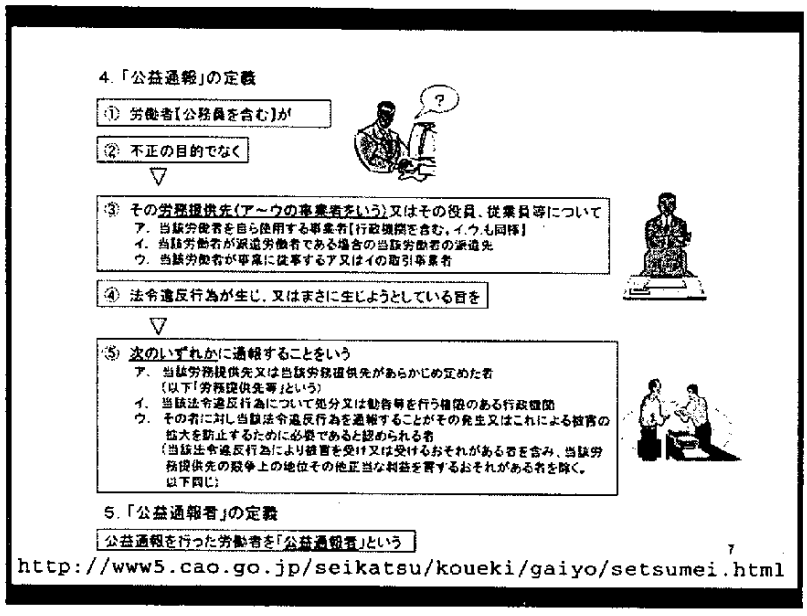
位置づけや違いについて幾つかポイントがあるが、まず先ほどのＳＯＸ法も、この内部告発者保護法にも支えられている部分が大きくある。いくら何をやっても組織全体で丸ごと財務諸表をでたらめなものをつくろうと断固一致していたら、これを外部からだけで防ぐのは容易ではない。ただ、そういうことをすれば中には正義感のある人が一人でもいてくれれば、それが告発されればいいだろうというようなバランスの上に成り立たすと防ぎやすくなる。その意味で、ＳＯＸ法に関して内部告発者保護法は一つの大きな礎を築いている。

日本の公益通報者保護法は、米国の内部告発者保護法とまったく同じではない。何が違うかについて紹介するが、結論だけ言うと、それぞれの法律名は内容をちゃんと表していて、日本のものは、公益に供するような通報をした人を保護するものである。かたや、アメリカのものは、内部で何かの告発をした人を保護するというものだ。

図3.51：公益通報者保護法

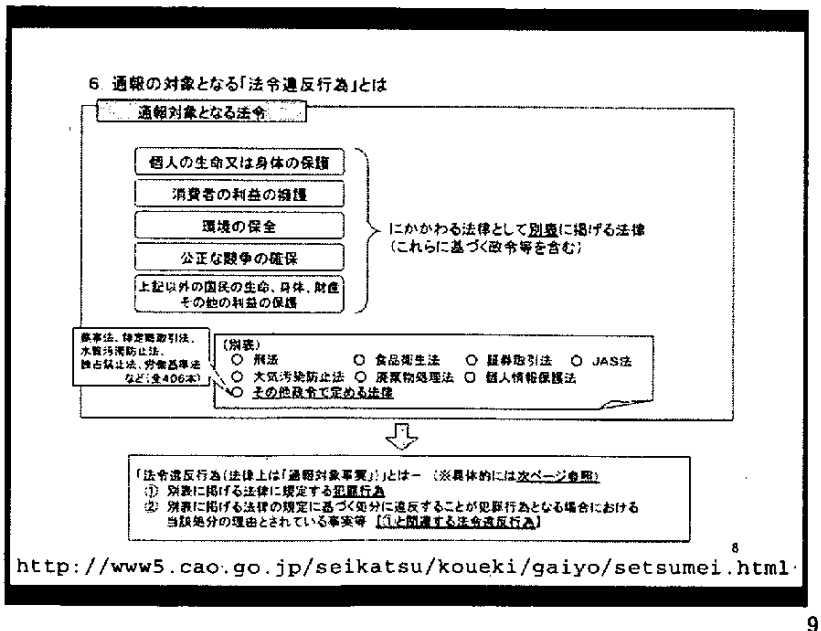
内閣府のＷＥＢページ（※９）はよく整理されたポータルサイトになっており、公益通報者保護法の関係のことがすべて網羅されている。そこに公開されている「公益通報者保護法説明資料」（図 3.51、※１０）を引用して紹介する。

図3.52：公益通報者保護法



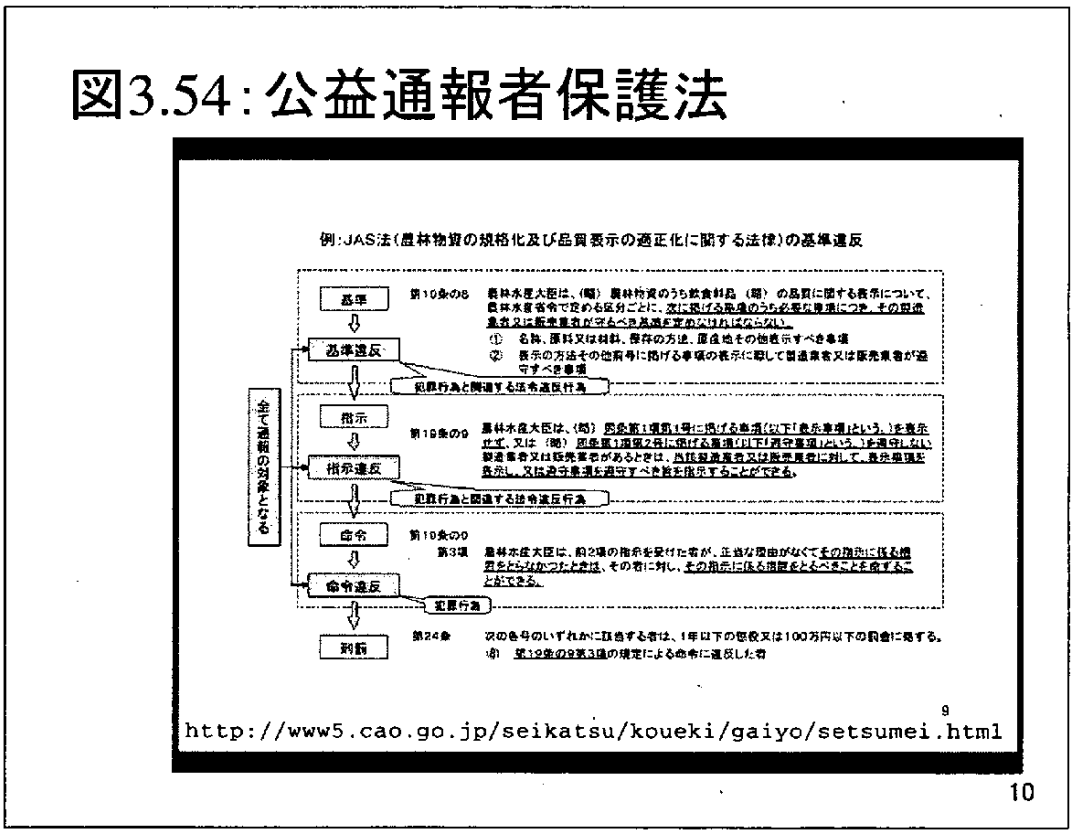
8

図3.53：公益通報者保護法



9

まず、この公益通報の定義というのが細かく決まっている（図 3.52）。ここでは定義の内容について解説はしないが、細かな定義があるということが一つポイントである。それと、通報したときにその行為が保護される対象が、厳密に定義されている（図 3.53）ということである。この法律は消費者保護政策の中に位置付けられたのが出発点になっているという背景があり、企業の不正を暴くということは、消費者を保護するために必要なことであるという位置づけがある。



保護の対象の定義では、通報した内容が企業として法令違反に限られる。先ほどの社会通念上まずいだろうとか、いわゆる脱法みたいなこととかが、本当に違法になるのかというのは微妙なところである。説明資料ではＪＡＳ法を例（図 3.54）に出してあるが、この例だと、自分の会社が今やっている悪いことは、ＪＡＳ法の第 19 条の８に違反するということまでがはっきりと分かった上で通報しないと、場合によっては返り討ちに遭うということだ。やっていることが明確に違法でないことを通報した場合には、この保護法の保護の対象にならない可能性がある。そのため、保護対象が限定されているということについて注意しなければならない。これに対してアメリカの内部告発者保護法は、内部告発という考え方そのものを保護しようということから出発しているため、保護対象が若干広い。

さらに、公益通報者保護法は、違法した行為に関する証拠だけを提出するということを通報者に求めている。例えば、違反した証拠を提出しようとしたときに、その違反行為とは関係のない

会社の営業機密が含まれていたりすると、その部分に関しては通報者が保護されない。つまり、その部分の営業機密については通報者の不正開示の責任が問われるかもしれないということになり、通報者側に証拠を限定するための負担がかかる可能性がある。ただこれは運用で決めていく内容なので、日本においても、アメリカの内部告発者保護法と同じように通報者の負担がより少ない運営になればよいと思われるところである。通報が保護されるか否かは、そのあと裁判などになってみて、企業が違法を問われてくれたとき初めて確定するというのでは困る。そして、違反行為と関係ない情報が交ざらないようにしておかないと、違反行為を通報したということに関しては保護されるが、会社の機密情報を裁判所に出したという部分に関しての情報漏えいだけは、問われてしまうということでは、実際の通報は萎縮してしまうことが懸念される。

ＳＯＸ法に習って日本版ＳＯＸ法をやるときに、米国の内部告発者保護法に相当するものとして、日本は公益通報者保護法が施行されているから、それで十分だという考え方をしてはならないということだ。

なお、公益通報者保護法では、組織の中にそれの通報窓口を設けている場合には、まずそこに届け出るということになっており、いきなり会社の外に言いつけるようなことに関しては、次のステップということになっている。これは言葉の裏を返すと、公益通報者の窓口体制を設けていない企業は、いきなり外に言われても文句が言えなくなると考えることもできる。従業者の誤解によって、外部に通報されて世間で騒がれたりしたら、それが後から誤解だと判明しても、風説による企業へのダメージは小さくないだろう。したがって、すべての企業は公益通報者の窓口を設けて、まず最初に、通報者への説明をできるようにする体制を設けるべきである。

参考・引用文献等
※１：Ｗｅｂページ「http://www5.cao.go.jp/seikatsu/kojin/index.html」
※２：書籍「個人情報保護法とコンプライアンス・プログラム」鈴木正朝 著、商事法務 出版 ISBN4-7857-1191-4
※３：Ｗｅｂページ「http://www.kantei.go.jp/jp/singi/it2/hourei/link.html」
※４：Ｗｅｂページ「http://hogen.org/research/paper/jp/」新保史生
※５：Ｗｅｂページ「http://www.itmedia.co.jp/enterprise/articles/0512/19/news002.html」
※６：報告書「文書の電磁的保存等に関する検討委員会報告書」2004 年経済産業省（http://www.meti.go.jp/press/20050506001/20050506001.html）
※７：Ｗｅｂページ「http://www.itmedia.co.jp/enterprise/articles/0512/19/news002.html」
※８：Ｗｅｂページ「http://www.itmedia.co.jp/enterprise/articles/0601/17/news004.html」
※９：Ｗｅｂページ「http://www5.cao.go.jp/seikatsu/koueki/index.html」
※１０：Ｗｅｂページ「http://www5.cao.go.jp/seikatsu/koueki/gaiyo/setsumei.html」
上記のうち、Ｗｅｂページについては、「http://yosihiro.com/go/2006-02-02-inlaw」にリンクの一覧を設けてあります。

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事業継続を主なテーマとして調査や検討、及びシンポジウムの実施を行ってきました。これに伴い僭越ながら、事業継続に関する３つの提言をさせていただきます。

- 【業界自主基準の策定】
  - 業界の自主基準として考えていって欲しい。

- 【国としての政策的な戦略としての事業継続】
  - 国として事業継続のために安全な場所という考え方の調査研究が必要ではないか。
    - 例えば、米国ではある特定の場所に比較的多くのデータセンターが集まっている。我が国においても、何が安全であるのか、その安全についての様々な要素は何であるのかを含めて十分に調査研究していくことが政策的にも必要なのではないのか。

- 【地方自治体として事業継続の活用：都市再生との連携】
  - 都市整備して誘致しようという「都市再生」と上手く結び付けていくといったことも考える。
    - 例えば、地方自治体が策定した危機管理対策にあわせ、各企業の事業継続が可能か検討し、自治体と協業し都市整備・再生に協力することが考えられる。この場合、各企業への優遇策の検討が必要。

最後になりますが、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いる。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る。しかし、情報のセキュリティの分野は国内においての認知度が低い。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。

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 18 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18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

17－H005