２００２年度
情報セキュリティインシデントに関する
調査報告書

＜第１部＞

情報セキュリティのインシデントに関する調査および被害算出モデル

ＮＰＯ日本ネットワークセキュリティ協会

２００３年3月３１日

目　次

JNSA　政策部会　セキュリティ被害調査ワーキンググループ

ワーキンググループリーダー

山本　匡　　株式会社損保ジャパン・リスクマネジメント

ワーキンググループメンバー（氏名昇順）

大谷　尚通　株式会社 NTT データ
大溝　裕則　株式会社ジェイエムシー
岡田　賢治　ELNIS テクノロジーズ株式会社
日下　昌彦　株式会社損保ジャパン・リスクマネジメント
指田　朝久　東京海上リスクコンサルティング株式会社
佐藤　友治　株式会社インターネット総合研究所
長嶋　潔　　東京海上火災保険株式会社
根本　卓　　株式会社ヒューコム
松谷　幸洋　株式会社ヒューコム
丸山　司郎　株式会社ラック
安田　直義　株式会社ディアイティ
山田　英史　株式会社ディアイティ
（敬称略）

1. はじめに

NPO 日本ネットワークセキュリティ協会(JNSA)では、現在 20 近いワーキンググループが活動を行なっているが、前年に引き続き、情報セキュリティインシデント被害調査をプロジェクトとして行った。

＜第 1 部について＞

JNSA 政策部会「情報セキュリティ被害調査ワーキンググループ」では、JNSA メンバーを中心とした日本の基幹産業を構成する代表企業および、IT 関連企業について、前年に引き続き、アンケート及びヒアリング調査を実施した。

そして、第一部では、これらの企業における情報セキュリティインシデントに係る被害額・投資額などの実態把握および本調査結果を基にしたインシデントによる被害額および対策額の算出モデル策定を目指して検討し、現時点で考えられるモデルの一案を提示している。

今回は、昨年の「算出モデル」を基に更に検討を加えているが、まだ多くの課題を残しているのは事実である。今後さらに調査および考察をしてゆくことが重要である。

しかしながら、リスクマネジメント実施において「被害規模と対策規模」が重要であるにも関わらず、これらの情報関連の被害額や対策額を企業や組織で十分に把握できていない現状を鑑みると、今回の「情報セキュリティ被害額および対策額の算出モデル」によって、これらのコスト算出に指標を与える意義は大きいと考える。

＜第 2 部について＞

算出モデルでは、情報セキュリティがシステム関連の被害にとどまらず、波及的な被害として、損害賠償額などの被害についても言及している。

今回の報告書では、情報漏洩による「損害賠償の可能性」についての検討や考察、企業価値の一端となる「株価への影響」について実例調査なども行った。

本報告書で述べる「損害賠償金額の算出」や「株価への影響額」は、あくまでも当ワーキンググループによる一つの提案であり、確定したものではない。

しかしながら、今後様々な方面の専門家において共通の題材として取り上げられ、企業経営者が考えるべき情報セキュリティのリスク量の把握や行うべき投資判断の一助となれば幸いである。

2. 目的

2001 年の米同時テロ、毎日のように発生する新しいウイルスや情報漏洩事故、システム統合時のシステム不具合の発生など、サイバーテロや重要インフラセキュリティに対する関心は、益々高まり、今まで以上に重要インフラである情報システムにおけるセキュリティインシデントに関する過去の事例や現状についても関心が高まっている。

しかし、これらセキュリティインシデントに関する具体的な事例や被害額についてのまとまった情報は殆ど無い。インシデントの性質上、一般に公表されることが稀であるということに加え、そもそも被害の定義が曖昧であることも、情報が得られない大きな原因となっている。

また、同様なことは、対策の面でも生じており、対策定義の曖昧さにより、対策コストの情報はまだ不足している。

＜第１部＞では、アンケートやヒアリングによって、国内におけるサイバーテロや重要インフラセキュリティインシデントに関する現状を把握するための情報収集を行った。この情報から得られる結果を基に、昨年度提案したセキュリティインシデントの被害額や情報セキュリティの対策投資額を推計するモデルに対し、情報セキュリティマネジメントにおける「リスクの大きさ(被害規模)」と「対策規模」の把握と効果の計測、効率的なマネジメントの実現において、更に精緻なモデルとするため検討を加え、２００２年度モデルとして提案する。

また、＜第２部(別冊)＞では、社会的な反響があり、関連者も非常に多数に上る事故種類の一つとして、今回「情報漏洩」を取り上げた。この「情報漏洩事故」は、どの企業にも共通の脅威であり、個人情報保護法案の進捗を踏まえると、経営者としては当然認知すべきリスクの一つである。

本ワーキンググループでは、「情報漏洩事故」における「損害賠償の可能性」や「株価への影響」について、今後の議論の題材になることや、企業経営者が考えるべき情報セキュリティのリスク量の把握や行うべき投資判断の一助となることを目的として、検討および提案を行う。

主な項目は次頁の通りである。

＜第１部：情報セキュリティのインシデントに関する調査および被害算出モデル＞

(1)「情報セキュリティインシデントに係る被害額・対策の投資費用に関する調査」

アンケートやヒアリングにて調査すべき項目を設定し、実際の企業においてインシデント発生や発生で要した費用(被害額)を調査する。

また、情報セキュリティインシデントの対策として実施されている取り組みへの投資額についても調査する。

(2)「被害額算出モデルの提案」

前年作成した情報セキュリティインシデントに関する被害額の算出モデルについて、更なる検討を加えたモデルを作成する。

具体的には、システム対応者の労務費用だけでなく、損害賠償に要した費用、復旧等に要した人件費、ハードウェア等物理的被害、イメージダウンによる被害、業務の停止による逸失利益などを想定し、被害額を算出するモデルの再検討と提案を行う。

(3)「情報セキュリティインシデント対策の標準モデルと対策費用」

前年調査との対比を交えた現時点で考えられる被害抑制のための標準的なモデルや望まれる対策レベルや予算規模などの提案を行う。

＜第２部(別冊) ：情報漏洩による被害想定と考察(賠償額および株価影響額)＞

(1)「情報漏洩による損害賠償被害額の想定」

２００２年に発生した、情報漏洩事件について調査を実施し、そのインシデント内容を分析した。本分析結果を元に、当ワーキンググループとして、個人情報の価値およびその情報が漏洩した際における賠償金額等について、いくつかの仮定に基づいて被害額を算出する。

(2)「情報漏洩による企業価値への影響(株価面での考察)」

情報漏洩による企業価値低下の一端を探るため、２００２年に情報漏洩事件を生じた企業について、情報漏洩の事故発生と当該企業の株価の動きについて、どの様な関係があるのかを調査し、本結果を元に、当ワーキンググループとして影響額を算出する。

3. 調査結果および分析

3.1 調査対象

・セキュリティ被害調査ワーキンググループメンバーにて調査を依頼し、了解頂いた日本のインフラや基幹産業を構成する企業や組織。

・JNSA メンバー企業を中心とする IT 関連企業。(一部に非 IT 企業含む)

3.2 調査方法

・対象企業に対して、アンケート及びヒアリングにより調査を行う。

・アンケートは、昨年度の調査用紙をより簡便かつ詳細な回答ができるように大幅に修正したアンケート用紙を使用した。(アンケート用紙については、「8.2 アンケート用紙」を参照)

・JNSA メンバーへのアンケートは、JNSA 事務局長の依頼文章と共に送付し、記入後、事務局へ返送、集約を行った。

・JNSA メンバー以外へのアンケートは、ヒアリング担当者より先方へ個別依頼にて収集。

3.3 調査の結果

3.3.1 ヒアリング調査の結果(集約)

「8.1 ヒアリング集約」参照。

3.3.2 アンケート調査の結果(集計表)

「3.4 調査結果の分析と特徴」参照。

3.3.3 アンケート回収率とヒアリング引受率

以下にアンケートの送付数と回答数、及びヒアリングの打診数と承諾数を示す。

	アンケート			ヒアリング		
	送付	回答	回答率	打診	承諾	承諾率
会員	159 (121)	53 (53)	33.33% (41.32%)	17 (20)	9 (11)	52.94% (55.00%)
非会員	20 (5)	13 (4)	66.66% (80.00%)	20 (14)	7 (5)	35.00% (35.71%)
合計	179 (126)	66 (54)	36.87% (42.86%)	37 (34)	18 (16)	48.64% (47.06%)

( )内は昨年度の数値

アンケートの回答率は、約 37%で昨年の約 43%よりも若干落ちてしまっている。母数が少ないことを割り引かなくてはならないが、2002 年はあまり騒ぎがなかったことが反映されていると思われる。JNSA 会員の方がアンケートの回収率が悪かったが、総数では変化していない。反対に、非会員の回収率が高いのは、依頼時にインシデント被害及び被害額の算定についての感心が高い企業を選定していることが挙げられる。

また、ヒアリングの承諾率 50%程度も、被害を情報公開して透明な企業姿勢を示したいという真摯さを感じることができた。確かにヒアリング先では、このような調査がほぼ毎日依頼があるというところ

もあり、全て対応はできないという声も聞かれた。今回の調査は JNSA 単体の取り組みであるにも拘らず、真剣に質疑に取り組んでいただけたのは、セキュリティに関する対応姿勢が徐々にではあるが確実に向上していると感じられた。

3.3.4 アンケート拒否の主な理由

アンケート拒否理由として、下記のような理由があげられていた。

・外資系企業のため、本社の承認が必要、それが得られなかった
・社内ポリシーは外部に公開しないため
・情報セキュリティに対する取り組み方の詳細が把握できることになり、
そのことが会社のセキュリティ強度をイメージすることが可能になる。
それはおおきな脅威（リスク）になりうる。
・アンケートの問いによっては、セキュリティスタンダードの内容そのものに
該当するものもある。それを公開することはできない。
・事故や事件への対策についても、それを開示することは、自らの守り方
を開示するに等しいため、回答できない。被害状況についても同様。

このようなご意見を頂いたが、ここでこれらを細かく考察するだけの情報を聞いていないので、コメントは控えるが、セキュリティを実現することは、金庫に鍵を掛けてしまいこむことではなく、情報公開を行ったうえでシステムとしてどのように守るかが重要であるので、常に説明可能な状態にしておくことが重要であろう。

隠すばかりがセキュリティの本質ではないことをもっと理解しなくてはならない。セキュリティとアカウンタビリティには密接な関係がある。従って情報公開を一律に拒否する反応についてはもう少し慎重に分析していく必要がある。今後の同様な調査でも意識してトレースしていきたい。

3.4　調査結果の分析と特徴

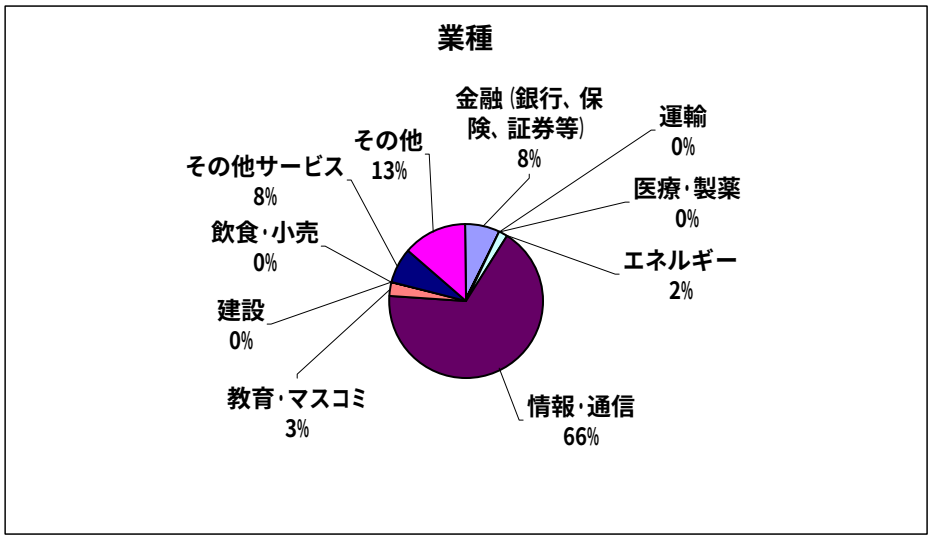
3.4.1 本年調査の調査結果と考察

本項目では、「66 件のアンケート結果を集計」と「ヒアリングの結果」とを照らし合わせながら、各項目に分析や特徴についてコメントを入れている。

A　貴社の事業状況についてご回答下さい。

A-1 貴社が属する主要業種をご回答下さい。（1 つ選択し、○をお付け下さい）

	業種名	件数	割合
1	金融（銀行、保険、証券等）	5	7.6%
2	医療・製薬	0	0.0%
3	運輸	0	0.0%
4	エネルギー	1	1.5%
5	情報・通信	44	66.7%
6	教育・マスコミ	2	3.0%
7	建設	0	0.0%
8	飲食・小売	0	0.0%
9	その他サービス	5	7.6%
10	その他	9	13.6%
		66	100.0%



Note

前年 2001 年度の集計件数 55 件に対し、本年 2002 年度は 66 件と回答者が増えたものの、調査対象が前年と同じく JNSA（NPO 日本ネットワークセキュリティ協会）会員企業中心になった。その結果、業種の比率も前年とほぼ同様になり、情報･通信が最も多くを占めた（66%）。

また、医療・製薬、建設、飲食・小売は前年と同じく本年も未調査であり、実社会を反映させた調査結果を求めるなら、これらの業種も対象にする施策が今後の課題となる。

A-2 貴社の年間売上および従業員数をご回答下さい。

■ 平均値

1	年間売上高（万円）	17,090,186	万円
2	従業員数（人）	1,806	名

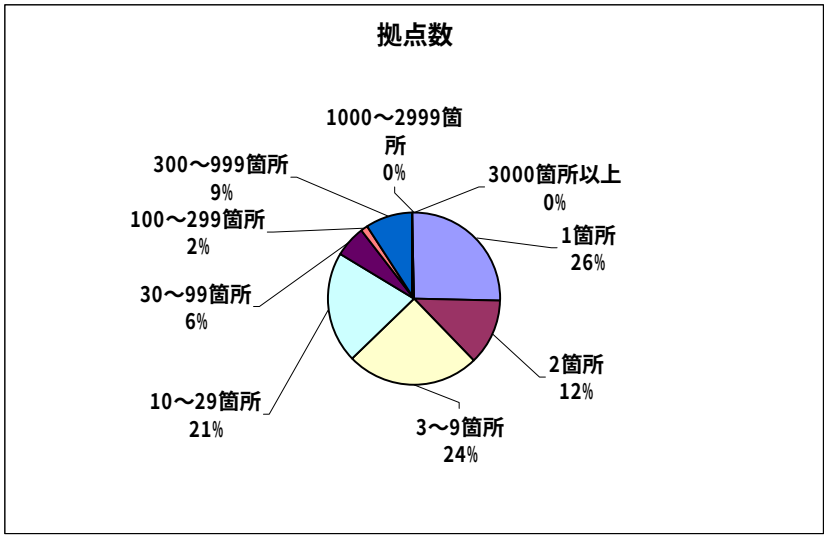
Note

上記数値は対象 66 件の平均であるが、年間売上高の最小値は 100 万円、最大値は 168,694,100 万円、従業員数は最小 1 人、最大 15,470 人と広く分布した。

売上高や従業員数などの規模とセキュリティ対策の関係は特にアンケート結果からは読み取れないが、強いて言えば“C-1 情報セキュリティに関する規定をお持ちですか”の質問に対し「ない」と回答した 7 社の内 6 社が従業員 100 名以下である（残り 1 社は 330 名）ことが挙げられる。

A-3 貴社の拠点数をご回答下さい。

	拠点数	件数	割合
1	1箇所	17	25.8%
2	2箇所	8	12.1%
3	3～9箇所	16	24.2%
4	10～29箇所	14	21.2%
5	30～99箇所	4	6.1%
6	100～299箇所	1	1.5%
7	300～999箇所	6	9.1%
8	1000～2999箇所	0	0.0%
9	3000箇所以上	0	0.0%
		66	100.0%



Note

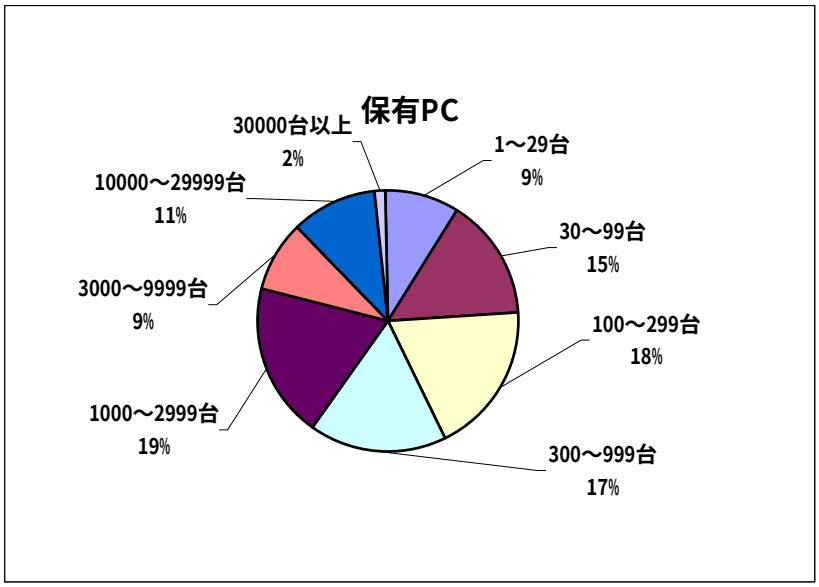
調査対象の 83%が拠点数 29 箇所以下となっている。今回の調査対象には入っていないが、もしチェーン展開しているような飲食・小売業が含まれれば拠点数の分布は大きく変わったと思われる。

ネットワークセキュリティの観点から考えると、拠点数が増えるほどリスクは大きくなると予想されるが、やはり拠点数の比較的多い上記 5～7 に相当する企業は、効率良く情報伝達できるように連絡体制を整備していることがアンケートの結果（C-4）からも読み取れる。

B貴社のシステム状況についてご回答下さい。

B-1 貴社が保有しているパーソナルコンピュータ（PC）の台数をご回答下さい。

	台数	件数	割合
1	1～29台	6	9.1%
2	30～99台	10	15.2%
3	100～299台	12	18.2%
4	300～999台	11	16.7%
5	1000～2999台	13	19.7%
6	3000～9999台	6	9.1%
7	10000～29999台	7	10.6%
8	30000台以上	1	1.5%
		66	100.0%



Note

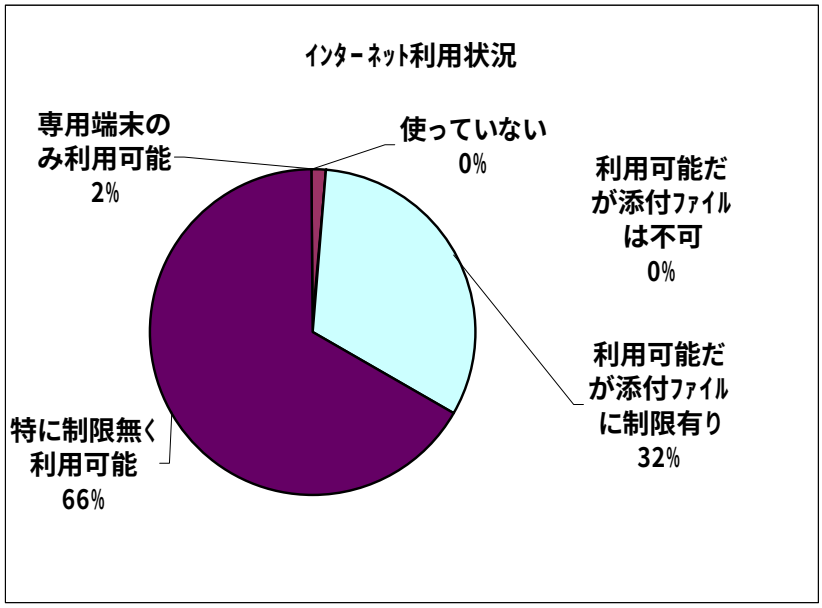
“A-2-2 従業員数”と比較したところ平均的な PC 保有台数は 1 人あたり 1 台以上となった。調査対象の多くが情報･通信業ということも影響していると思われるが、今回調査した範囲ではすべての業種で同様の結果になった。

PC の台数が増えると拠点数の場合と同じくリスクは大きくなると予想されるが、比較的 PC 所有

台数の多い 5～8 に該当する 27 件においても、メールの使用と Web 閲覧に何かしらの制限を設けている「B-2、B-3」は 12 件（44%）であり、アンケートの結果からは顕著な特徴は見出せなかった。

B-2 貴社のインターネットメールの利用状況はどの程度ですか。（1 つ選択）

	利用状況	件数	割合
1	使っていない	0	0.0%
2	専用端末のみ利用可能	1	1.5%
3	利用可能だが添付ﾌｧｲﾙは不可	0	0.0%
4	利用可能だが添付ﾌｧｲﾙに制限有り	21	31.8%
5	特に制限無く利用可能	44	66.7%
		66	100.0%



Note

この質問の場合も調査対象の多くが情報･通信業であるということが影響しているためか、100%がインターネットメールを利用しているという結果となった。

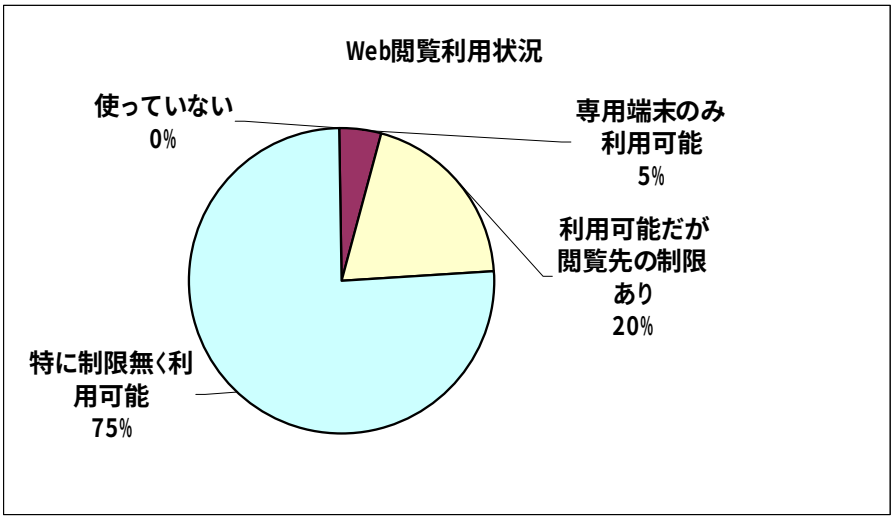
メールの利用率が高ければコンピュータウイルスの感染の危険性も大きくなるが、“C-15 導入済みセキュリティシステム”の調査結果を見ると、1 社を除き「メールサーバでのウイルスチェック」もしくは「全クライアント PC でのウイルスチェック」のいずれか一方あるいは両方を実施しており、メール利用時のリスクを十分理解していることがうかがえる。

ただし、情報漏洩の観点から考えると社内から発信するメールの制限も注意する必要があり、今後のアンケートにはそれを反映させるような質問を盛り込む必要がある。

また、ヒアリングの結果を見ると制限を設けているのはほとんどが容量に対するもので、セキュリティ面というよりネットワーク負荷という実務面での要求によるものと考えられる。

B-3 貴社の Web 閲覧の利用状況はどの程度ですか。（1 つ選択）

	利用状況	件数	割合
1	使っていない	0	0.0%
2	専用端末のみ利用可能	3	4.5%
3	利用可能だが閲覧先の制限あり	13	19.7%
4	特に制限無く利用可能	50	75.8%
		66	100.0%



Note

メールの利用に関する質問の結果と同様、Web 閲覧の利用状況についても利用率は 100%となった。「専用端末のみで利用可能」と「閲覧先の制限あり」を合計すると、何らかの制限を設けている企業は 24.2%となる。業種別で見ると、「専用端末のみで利用可能」と回答した 3 件の内 2 件が金融業で、1 件が地方自治体となっている。

また、「閲覧先の制限あり」と回答した 13 件の内で情報・通信業を除くと、2 件がその他サービス業で 1 件がエネルギー関連、1 件が金融業で 1 件が地方自治体となっている。

「制限」はコンテンツフィルタリングによるもので、アダルト、ギャンブル、株取引、攻撃サイト、掲示板などが対象となっている。また、切符の手配のために人事部門のみ買い物サイトへのアクセスを許可しているといった、細かな設定をおこなっている企業もある。

B-4 貴社が保有している PC（ｸﾗｲｱﾝﾄ）の何割程度がメール、Ｗｅｂ閲覧を利用できますか。

■ 平均値

1	インターネットメール (%)	90%
2	Web閲覧 (%)	85%

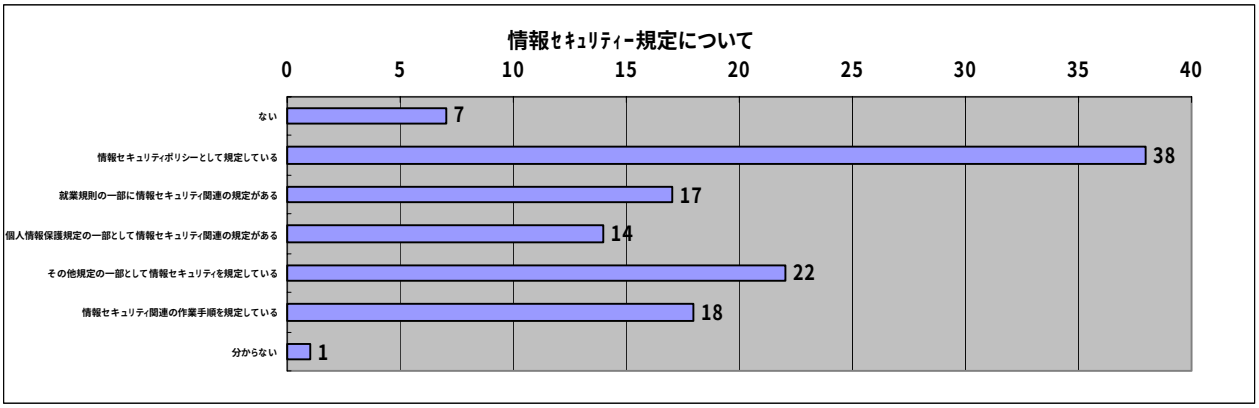
Note

上記の数値は平均値となる。B-2 および B-3 の結果と併せて見ると、金融業や自治体の一部を除きほとんどの企業が各人で直接インターネットを利用できる環境にあると言える。コミュニケーションツールあるいは情報収集ツールとしてインターネットが果たす役割が大きくなっている状況を考えると当然の流れではあるが、メールも Web 閲覧もほとんどの企業が制限無しで利用可能であるという結果を見ると、まだ、セキュリティよりも利便性を優先していることがうかがえる。

C　貴社の情報セキュリティ管理への取組みについてご回答下さい。

C-1 情報セキュリティに関する規定をお持ちですか。（該当全て）

	状況	件数	割合
1	ない	7	10.6%
2	情報セキュリティポリシーとして規定している	38	57.6%
3	就業規則の一部に情報セキュリティ関連の規定がある	17	25.8%
4	個人情報保護規定の一部として情報セキュリティ関連の規定がある	14	21.2%
5	その他規定の一部として情報セキュリティを規定している	22	33.3%
6	情報セキュリティ関連の作業手順を規定している	18	27.3%
7	分からない	1	1.5%



Note

セキュリティポリシーを規定していると回答する企業の半数にあたる 19 件が 3～6 の他の規定も併用している。特に罰則規定など実運用にかかわる部分は、就業規則など既存の規定を適用する例がみられる。

反対に、セキュリティポリシーという専用の規定を定めず、他の規定の一部として制定している企業は 10 件になる。

また、新たな法案として注目される個人情報保護に関して規定を持つと回答のあった 14 件の内

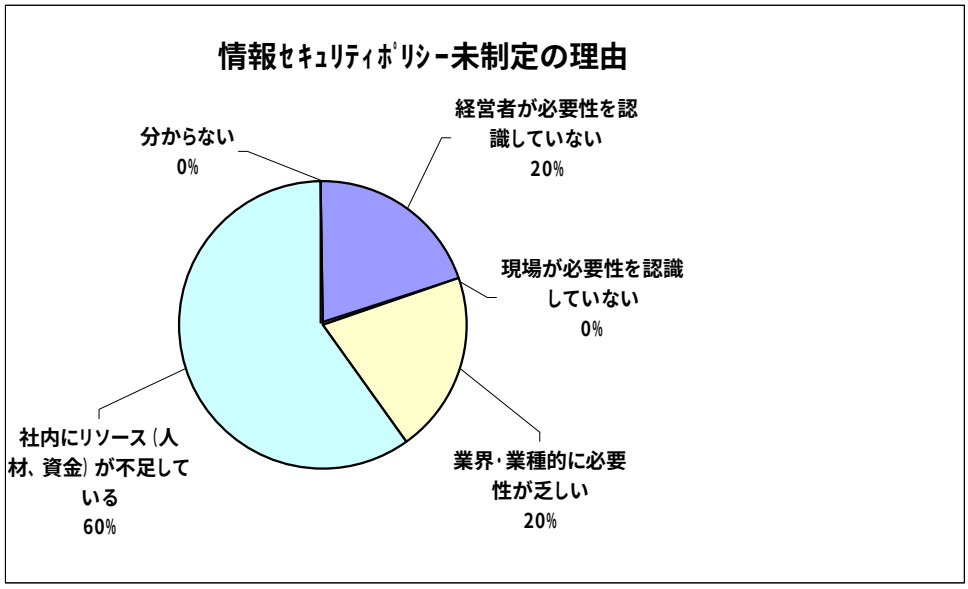
1 件は金融業で 1 件が教育・マスコミで、残りはすべて情報・通信業となっている。

ヒアリングを行なった範囲では、ほとんどの企業がポリシー策定後は従業員に対する教育ならびに定期的なメンテナンスを行い、運用維持のための努力をしていることがわかる。

C-2　C-1 で「1 ない」と回答した方のみご回答下さい。

情報セキュリティに関する規定を制定していない最大の理由をご回答下さい。（1 つ選択）

	理由	件数	割合
1	経営者が必要性を認識していない	1	20.0%
2	現場が必要性を認識していない	0	0.0%
3	業界･業種的に必要性が乏しい	1	20.0%
4	社内にリソース（人材、資金）が不足している	3	60.0%
5	分からない	0	0.0%
		5	100.0%



Note

A-2 の項で述べた通り「規定していない」と回答する 7 社の内 1 社を除き、従業員数が 100 名以下であることが、「社内にリソースが不足している」ということを裏付けている。

C-3 情報セキュリティ管理担当者の人数を教えてください

1	専任担当者 (名)	1.70	＜回答各社の平均人数＞
2	兼任担当者(名)	56.15	＜回答各社の平均人数＞
3	担当役員を選任している	21	件

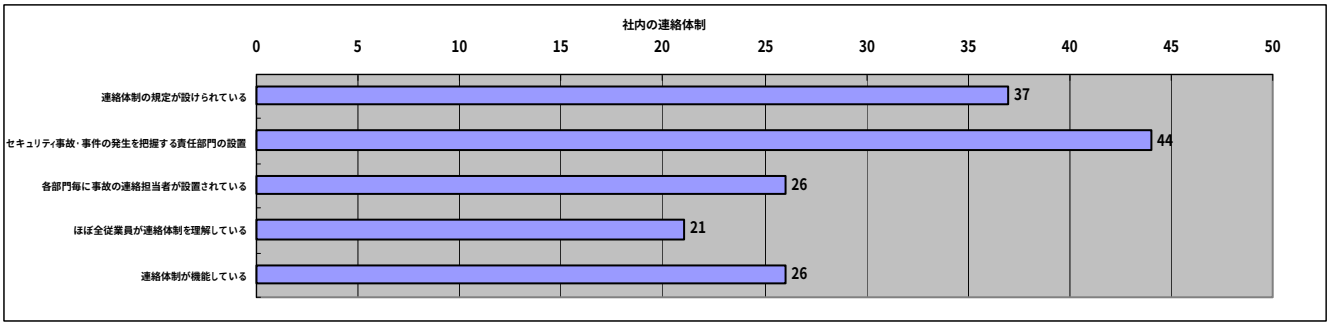
Note

多くの企業が情報セキュリティ担当を兼任で置いている。「予算（C-12)」と同様に情報セキュリティは他の情報システムの一部として運用されていることが分かる。

ヒアリングでは、兼任の場合にセキュリティに関わる業務は全業務中 10%～20%との回答が多かった。

C-4 情報セキュリティ関連の事故や事件が発生した場合の社内連絡体制。（該当全て）

	体制	件数	割合
1	連絡体制の規定が設けられている	37	56.1%
2	セキュリティ事故･事件の発生を把握する責任部門の設置	44	66.7%
3	各部門毎に事故の連絡担当者が設置されている	26	39.4%
4	ほぼ全従業員が連絡体制を理解している	21	31.8%
5	連絡体制が機能している	26	39.4%



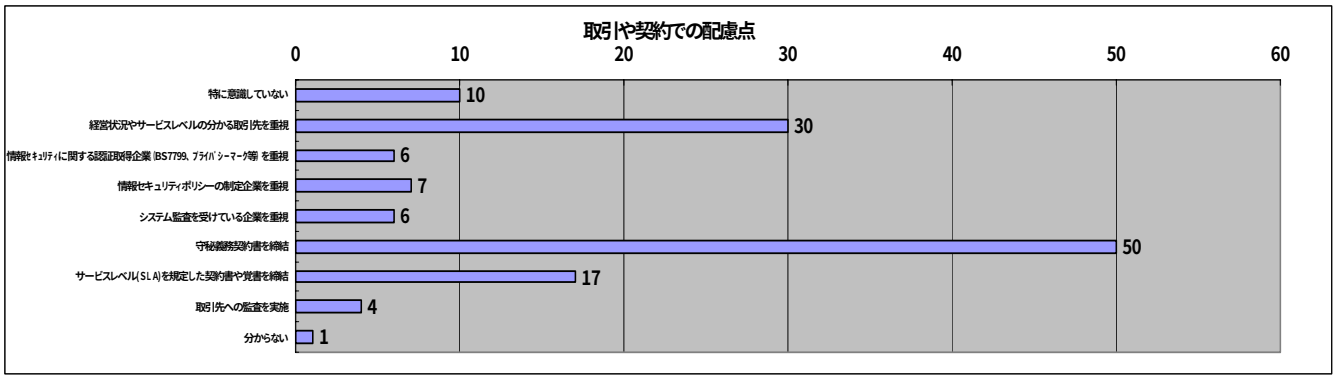
Note

調査対象 66 件中上記項目のどれにも該当しない（体制を持たない可能性あり）のは 4 件で、90%以上の企業が連絡体制を定めていることになる。責任部門は情報システム部門ではなく総務・業務部門が担当していると回答する企業もあり、情報セキュリティを他のリスク管理の一部として認識していることがうかがえる。

また、連絡体制を整備する企業の多くが、教育やリハーサルを反復することによって体制の維持を図っている。

C-5　情報セキュリティの観点から取引先の選定や契約時に配慮している点。（該当全て）

	配慮点	件数	割合
1	特に意識していない	10	15.2%
2	経営状況やサービスレベルの分かる取引先を重視	30	45.5%
3	情報ｾｷｭﾘﾃｨに関する認証取得企業（BS7799、ﾌﾟﾗｲﾊﾞｼｰﾏｰｸ等）を重視	6	9.1%
4	情報セキュリティポリシーの制定企業を重視	7	10.6%
5	システム監査を受けている企業を重視	6	9.1%
6	守秘義務契約書を締結	50	75.8%
7	サービスレベル(ＳＬＡ)を規定した契約書や覚書を締結	17	25.8%
8	取引先への監査を実施	4	6.1%
9	分からない	1	1.5%



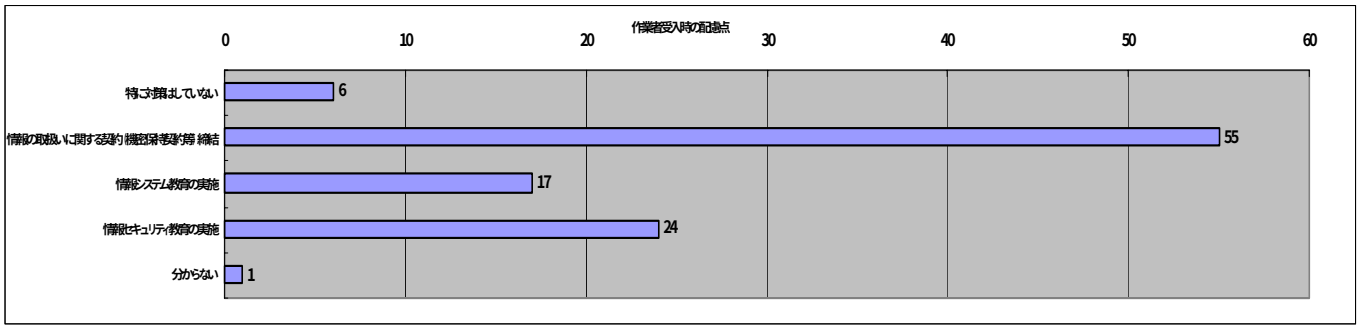
Note

“２経営状況やサービスレベルの分かる取引先を重視”の実施率が高いのは、以前から営業的要求で実施している与信管理を含むことが理由として考えられる。同様に“６守秘義務契約書を締結”も、セキュリティが注目される以前から契約書類に盛り込まれているために実行率が高いと予想される。

逆に取引先から上記の事項を求められることが増えているという回答もあり、「情報セキュリティ対策実施の有無」を取引条件にすることが商習慣として定着しつつあるように思われる。

C-6　派遣社員や常駐作業員受入時の配慮点をご回答下さい。（該当全てに○をお付け下さい）

	配慮点	件数	割合
1	特に対策はしていない	6	9.1%
2	情報の取扱いに関する契約（機密保持契約等）締結	55	83.3%
3	情報システム教育の実施	17	25.8%
4	情報セキュリティ教育の実施	24	36.4%
5	分からない	1	1.5%



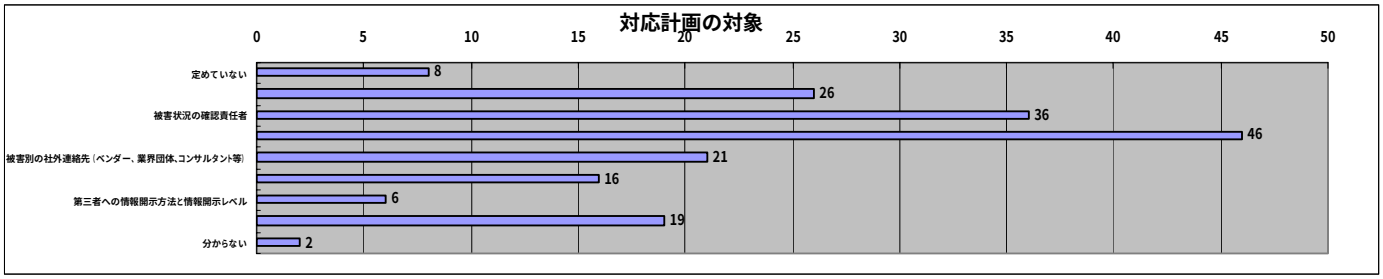
Note

“2 情報の取扱いに関する契約（機密保持契約等）締結”の実行率が高いのは、C-5 でも述べた通り従来からすでに契約内容に盛り込まれているためと思われる。教育については 3 と 4 どちらかが 41%の企業で実施されており、業務全体の問題としてセキュリティに取り組む姿勢がうかがえる。

ヒアリング結果によると、派遣社員に対する教育を実施するのは初期の受け入れ時に実施することが多く、内容的にはシステムの操作規定など具体的な内容までを含む場合が多い。

C-7　被害が発生した時の対応計画の対象をご回答下さい。（該当全てに○をお付け下さい）

	対応計画の対象	件数	割合
1	定めていない	8	12.1%
2	発生事象別の被害状況の確認事項	26	39.4%
3	被害状況の確認責任者	36	54.5%
4	被害発生時の社内連絡体制	46	69.7%
5	被害別の社外連絡先（ベンダー、業界団体、コンサルタント等）	21	31.8%
6	従業員への情報開示方法と情報開示レベル	16	24.2%
7	第三者への情報開示方法と情報開示レベル	6	9.1%
8	復旧時の確認事項	19	28.8%
9	分からない	2	3.0%



Note

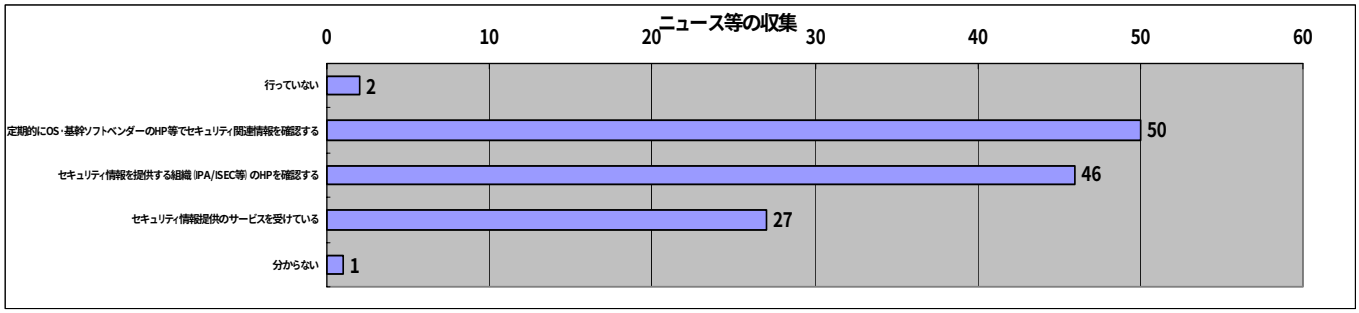
C-4 の結果からもわかる通り社内の連絡体制は今回調査した内の 90%が整備しており、その結果を反映するように 3～5 の項目の実施件数は高い。

しかし、実際に被害を受けた場合は、その後の対応次第で企業イメージの低下につながりかねないことを考えると“7 第三者への情報開示方法と情報開示レベル”が低いことが気になる。

「定めていない」と回答しているものについては、責任部門に被害報告が上がってくる都度経験的に計画を立て対応している、あるいはアウトソーシング先のベンダーがその都度対策を提案し社内で協議して実施している、などのコメントがあった。

C-8　情報セキュリティ関連ニュース等の収集についてご回答下さい。（該当全て）

	収集状況	件数	割合
1	行っていない	2	3.0%
2	定期的にOS･基幹ソフトベンダーのHP等でセキュリティ関連情報を確認する	50	75.8%
3	セキュリティ情報を提供する組織（IPA/ISEC等）のHPを確認する	46	69.7%
4	セキュリティ情報提供のサービスを受けている	27	40.9%
5	分からない	1	1.5%



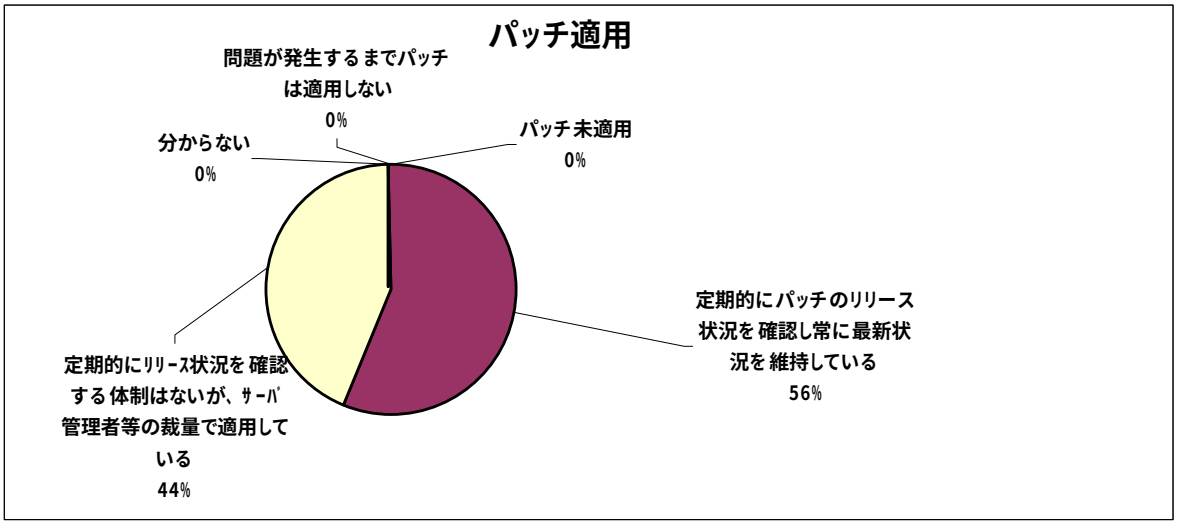
Note

パッチに関する情報は OS メーカーのホームページやセキュリティ関連のメーリングリストを活用し、コンピュータウイルスに関してはウイルス対策ソフトメーカーのホームページから情報を得るという回答が多かった。

また、有償の情報提供サービスについては、パッチの検証まで言及されていることにメリット感じるという意見があった。

C-9　サーバのセキュリティを確保するための各種パッチを適用。（1 つ選択）

	適用状況	件数	割合
1	パッチ未適用	0	0.0%
2	定期的にパッチのリリース状況を確認し常に最新状況を維持している	34	55.7%
3	定期的にﾘﾘｰｽ状況を確認する体制はないが、ｻｰﾊﾞ管理者等の裁量で適用している	27	44.3%
4	問題が発生するまでパッチは適用しない	0	0.0%
5	分からない	0	0.0%
		61	100.0%



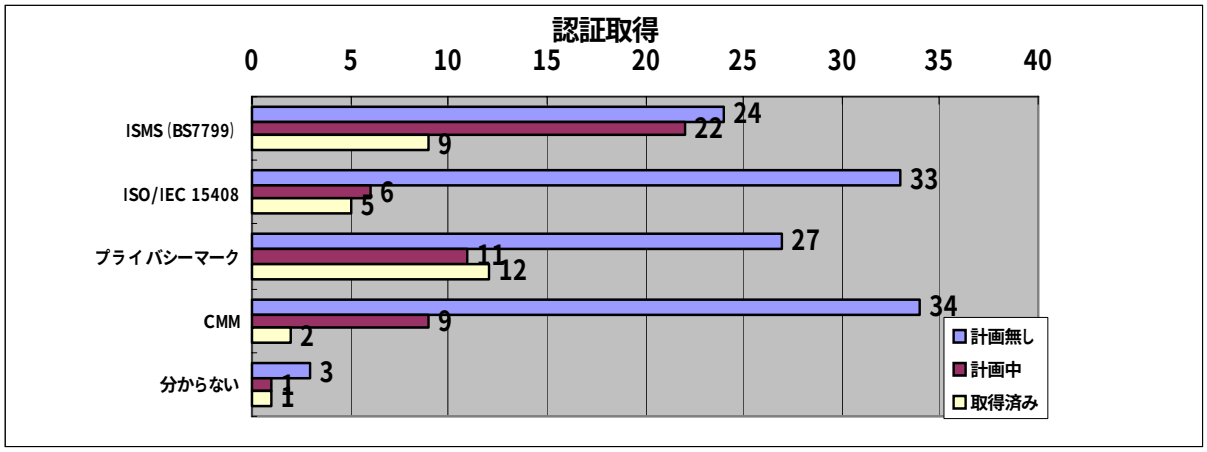
Note

コンピュータウイルスや不正アクセスによる被害が日常化する中で、パッチの適用は基本的な対策として認知されており、それを反映するようにアンケートの結果でも「パッチ未適用」という回答は 0 件であった。

しかし、一方で停止できないサーバへの適用が困難であるとか、DB 系のサーバへの適用は事前検証なしでは心配であるといった意見が多くあった。このような理由から、外部に公開するサーバには適時パッチを適用しているが内部サーバは未着手という例もあった。

C-10 認証取得を「計画中」、または「取得済」の別を右欄に○を付けてご回答下さい。

	名称	計画無し	割合	計画中	割合	取得済み	割合
1	ISMS (BS7799)	24	36.4%	22	33.3%	9	13.6%
2	ISO/IEC 15408	33	50.0%	6	9.1%	5	7.6%
3	プライバシーマーク	27	40.9%	11	16.7%	12	18.2%
4	CMM (Capability Maturity Model)	34	51.5%	9	13.6%	2	3.0%
5	分からない	3	4.5%	1	1.5%	1	1.5%



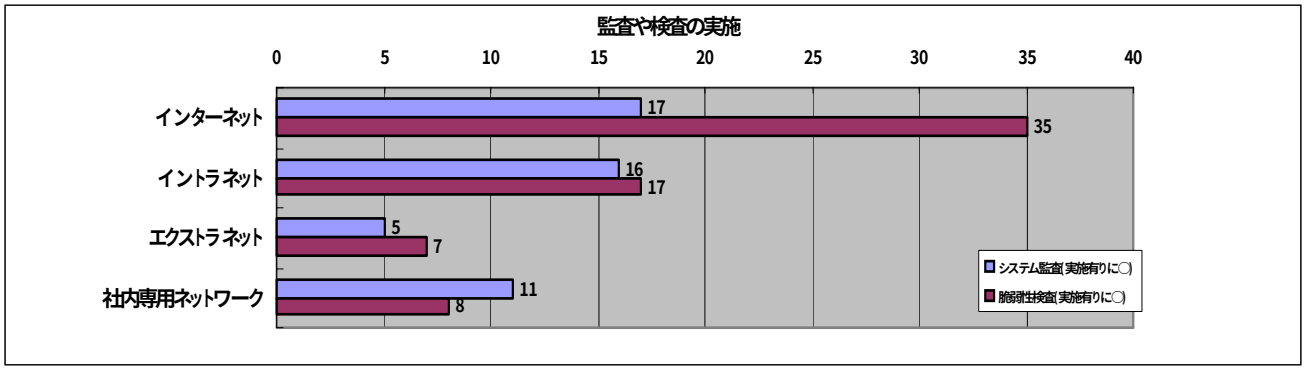
Note

「取得済み」ならびに「計画中」の合計を見ると、ISMS31 件、プライバシーマーク 23 件と高い割合を示す。どちらの認証も、競合との差別化やマーケットニーズという企業戦略的な面で捉えている意見が多い。

対して、ISO/IEC 15408 や CMM は調達要件に盛り込まれるなど、必要性を感じた場合に検討するという回答が多かった。CMM についてはヒアリング時に、その意味を問われるなど、認知度が低いと感じる場面もあった。

C-11 直近１年間でのシステム監査や脆弱性検査(ﾍﾟﾈﾄﾚｰｼｮﾝﾃｽﾄ)の実施状況をご回答下さい。

	項目名	システム監査実施	割合	脆弱性検査実施	割合
1	インターネット	17	25.8%	35	53.0%
2	イントラネット	16	24.2%	17	25.8%
3	エクストラネット	5	7.6%	7	10.6%
4	社内専用ネットワーク	11	16.7%	8	12.1%



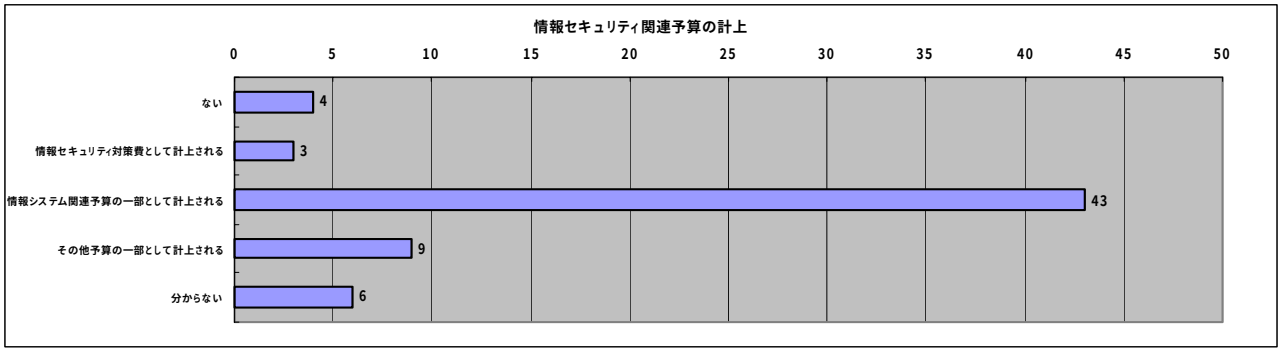
Note

66 件中 40 件（60%）が、全体もしくは一部分で監査や脆弱性検査を実施している。アンケートの結果から見ると、監査は外部・内部の両方を対象として実施するのに対し、脆弱性検査は主に外側部分に対しのみ実施していることがわかる。

実施頻度については、年１回、年２回、ログは毎朝チェックするなど様々である。検査項目を事前に協議する、検査は毎回異なる業者に委託するという回答もあった。

C-12 情報セキュリティ関連予算はありますか。（1 つ選択し、○をお付け下さい）

	予算の計上	件数	割合
1	ない	4	6.1%
2	情報セキュリティ対策費として計上される	3	4.5%
3	情報システム関連予算の一部として計上される	43	65.2%
4	その他予算の一部として計上される	9	13.6%
5	分からない	6	9.1%
<その他>		65	98.5%



Note

C-14 の予算の内訳でもわかる通り、ハードウェア購入や保守など一般のシステムとセキュリティシステムの境界が曖昧なこともあり、「情報システム関連予算の一部として計上される」という回答が最も多い（65.2%）。C-3 でも触れたが情報システム部門がセキュリティ管理を兼任していることが多く、予算も情報システム一般に含み予算管理されている。

C-13 上記回答で 2～4 に○の場合、大まかな数字をご記入下さい。

予算がある場合の平均金額(万円)	1497	(万円)
情報システム予算に対する平均割合(%)	14.8	(%)

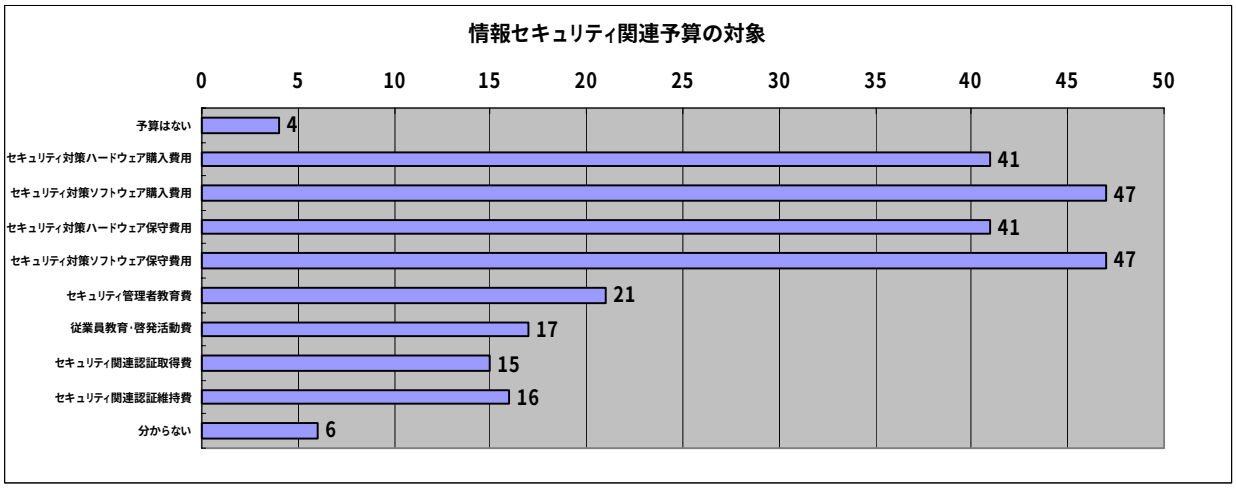
Note

セキュリティ予算と年間売上高の両方について回答があった企業は 26 社で、その 26 件の年間売上高の平均は 9,901,481 万円で、セキュリティ予算金額の平均は 1,596 万円となる。これらの金額から、年間売上高に対するセキュリティ予算が占める割合は 0.016%になる。対象件数が少ないため、この数字の信憑性については議論の余地があるが、情報・通信業中心の調査結果としては極めて低く感じられる。

予算については、調査項目の見直しも含め精度を上げるようなアンケート内容を考えることが今後の課題である。

C-14 情報セキュリティ関連予算の対象をご回答下さい。（該当全てに○をお付け下さい）

	予算の対象	件数	割合
1	予算はない	4	6.1%
2	セキュリティ対策ハードウェア購入費用	41	62.1%
3	セキュリティ対策ソフトウェア購入費用	47	71.2%
4	セキュリティ対策ハードウェア保守費用	41	62.1%
5	セキュリティ対策ソフトウェア保守費用	47	71.2%
6	セキュリティ管理者教育費	21	31.8%
7	従業員教育･啓発活動費	17	25.8%
8	セキュリティ関連認証取得費	15	22.7%
9	セキュリティ関連認証維持費	16	24.2%
10	分からない	6	9.1%



Note

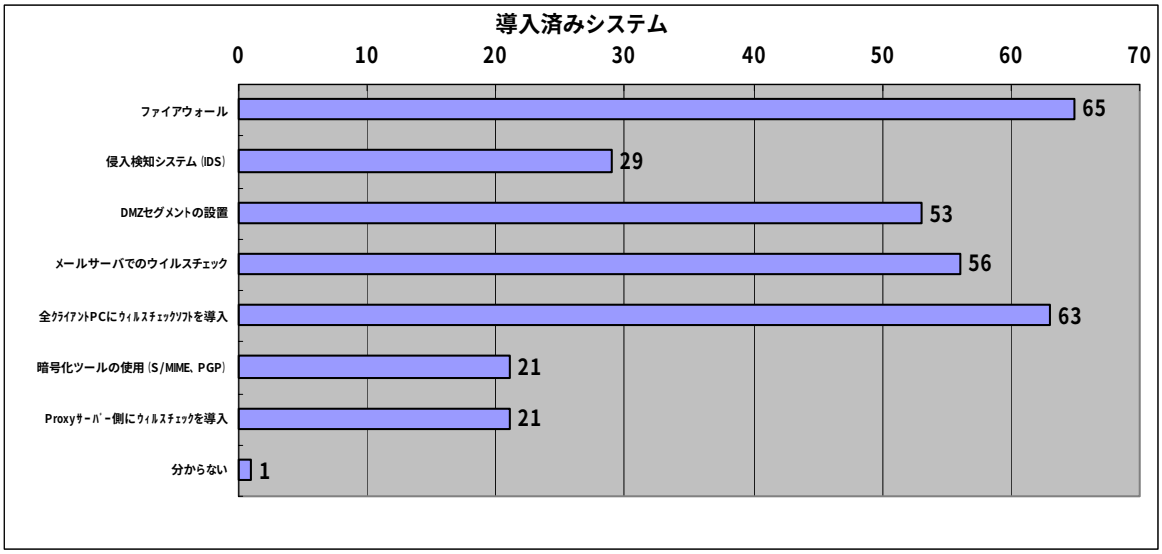
予算の割り当ての中で 2～5 が占める割合が大きいが、いずれもハードウェア・ソフトウェアの購入や保守に関連するもので、例えば新規にセキュリティ製品を購入するのではなくプラットホームとして使用している PC のアップグレードなどもこの中に含まれる。

また、ウイルス対策におけるウイルス定義ファイル更新ライセンスもソフトウェア保守費として計上することが多い。

インシデント発生時にその都度計上するという回答も数件あった。

C-15　情報セキュリティを確保するために導入しているシステムをご回答下さい。（該当全てに○をお付け下さい）

	導入済みシステム	件数	割合
1	ファイアウォール	65	98.5%
2	侵入検知システム (IDS)	29	43.9%
3	DMZセグメントの設置	53	80.3%
4	メールサーバでのウイルスチェック	56	84.8%
5	全ｸﾗｲｱﾝﾄPCにウイルスﾁｪｯｸｿﾌﾄを導入	63	95.5%
6	暗号化ツールの使用 (S/MIME、PGP)	21	31.8%
7	Proxyｻｰﾊﾞｰ側にウイルスﾁｪｯｸを導入	21	31.8%
8	分からない	1	1.5%

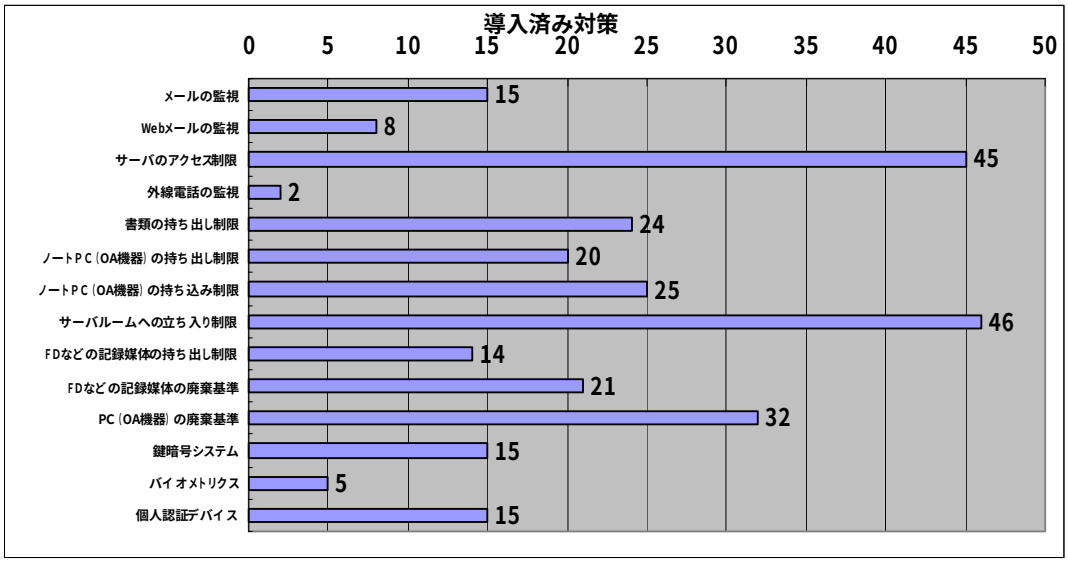


Note

ファイアウォールの導入は、あと 1 社で 100%になる。ウイルス対策についても 1 社を除きサーバ・クライアント・Proxy サーバのいずれかで実施しており、本年の調査先において、インシデントが少なかったのも理解できる。

C-16 情報漏洩を防止するために行っている対策をご回答下さい。（該当全てに○をお付け下さい）

	実施済み対策	件数	割合
1	メールの監視	15	22.7%
2	Webメールの監視	8	12.1%
3	サーバのアクセス制限	45	68.2%
4	外線電話の監視	2	3.0%
5	書類の持ち出し制限	24	36.4%
6	ノートＰＣ（OA機器）の持ち出し制限	20	30.3%
7	ノートＰＣ（OA機器）の持ち込み制限	25	37.9%
8	サーバルームへの立ち入り制限	46	69.7%
9	ＦＤなどの記録媒体の持ち出し制限	14	21.2%
10	ＦＤなどの記録媒体の廃棄基準	21	31.8%
11	PC（OA機器）の廃棄基準	32	48.5%
12	鍵暗号システム	15	22.7%
13	バイオメトリクス	5	7.6%
14	個人認証デバイス	15	22.7%



Note

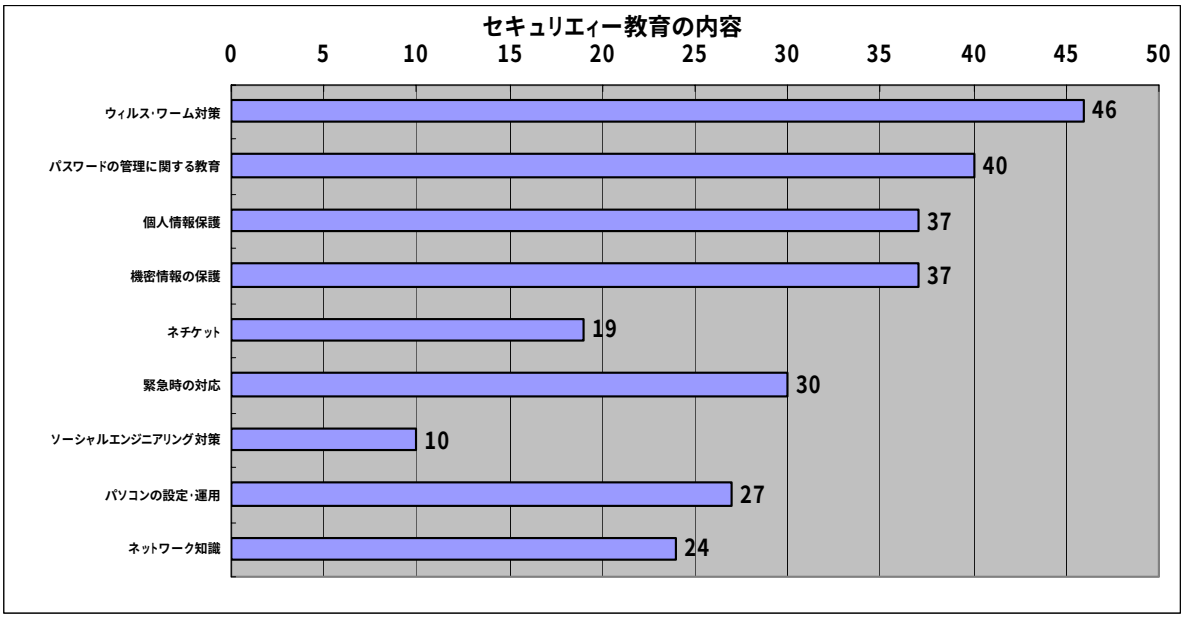
サーバへのアクセス制限ならびにサーバルームへの入室制限はセキュリティの基本として考えられ、約 70%が実施している。次に実施率の高い対策は FD など媒体の廃棄や PC の廃棄に関わる基準で、雑誌等でその危険性が取り上げられる機会が増えたことが一因と考えられる。

書類の持ち出し制限およびノート PC の持ち込み・持ち出し制限を設ける企業も多く、セキュリティに対する取り組みが、単にファイアウォールなどシステムを導入するだけではなく管理プロセスにまで拡大していることがうかがえる。

また、メールの監視はプライバシー問題も関係するため導入が難しいという面を持つが、22%の企業が実施している。メールの内容を直接監視するのではなく、トラフィック量を監視し開発中のプログラムの流出を検知するといったユニークな方法を取っている例もある。

C-17 情報セキュリティ教育の内容をご回答下さい。(該当全てに○をお付け下さい)

	教育の内容	件数	割合
1	ウイルス･ワーム対策	46	69.7%
2	パスワードの管理に関する教育	40	60.6%
3	個人情報保護	37	56.1%
4	機密情報の保護	37	56.1%
5	ネチケット	19	28.8%
6	緊急時の対応	30	45.5%
7	ソーシャルエンジニアリング対策	10	15.2%
8	パソコンの設定･運用	27	40.9%
9	ネットワーク知識	24	36.4%



Note

6 件を除きほとんどの企業で何らかの教育を実施しており、独立したカリキュラムではなく新人教育など他の教育制度の一部として取り入れていることも多い。

少数ではあるが e-ラーニングを採用したり、社内資格制度へ発展させたりと、積極的に取り組んでいる企業もある。

C-18 直近１年間での情報セキュリティ教育の実施状況を教えてください。(該当全てに○をお付け下さい)

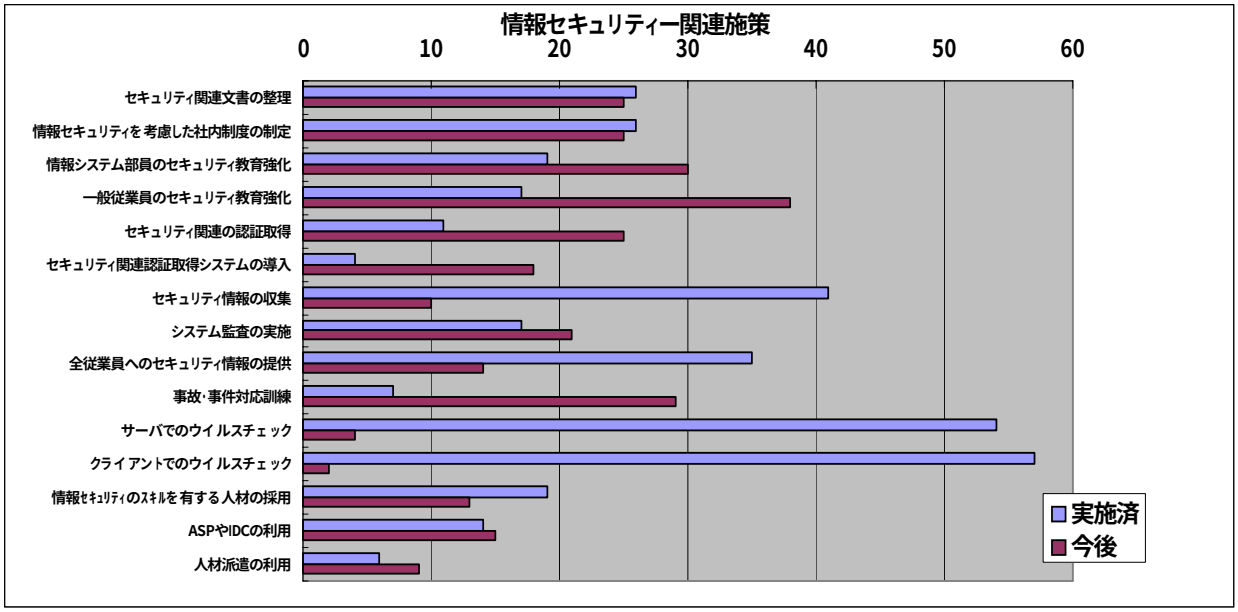
	教　育　内　容	平均人数	平均年回数
1	一般従業員 (ユーザー教育) 向け教育	1775	3
2	マネージャー向け教育	42	2
3	専門家向け教育	62	3

Note

定期的な集合教育だけに留まらずステップアップができる制度を持つ例もある。

C-19 現在実施、また今後実施していきたいと考えている情報セキュリティ関連対策(該当全て)

	対策種類	実施済	割合	今後	割合
1	セキュリティ関連文書の整理	26	39.4%	25	37.9%
2	情報セキュリティを考慮した社内制度の制定	26	39.4%	25	37.9%
3	情報システム部員のセキュリティ教育強化	19	28.8%	30	45.5%
4	一般従業員のセキュリティ教育強化	17	25.8%	38	57.6%
5	セキュリティ関連の認証取得	11	16.7%	25	37.9%
6	セキュリティ関連認証取得システムの導入	4	6.1%	18	27.3%
7	セキュリティ情報の収集	41	62.1%	10	15.2%
8	システム監査の実施	17	25.8%	21	31.8%
9	全従業員へのセキュリティ情報の提供	35	53.0%	14	21.2%
10	事故･事件対応訓練	7	10.6%	29	43.9%
11	サーバでのウイルスチェック	54	81.8%	4	6.1%
12	クライアントでのウイルスチェック	57	86.4%	2	3.0%
13	情報ｾｷｭﾘﾃｨのｽｷﾙを有する人材の採用	19	28.8%	13	19.7%
14	ASP (Application Service Provider) や IDC (Internet Data Center)の利用	14	21.2%	15	22.7%
15	人材派遣の利用	6	9.1%	9	13.6%



Note

コンピュータウイルス対策は約 90%が実施済みで、今後は増設よりも維持に注力すると思われる。

次に実施率が高いのが情報収集および従業員に対する情報提供だが、これは導入・運用コストが低いということとメールや Web など既存のシステムを利用して簡単に導入できることが理由として考えられる。

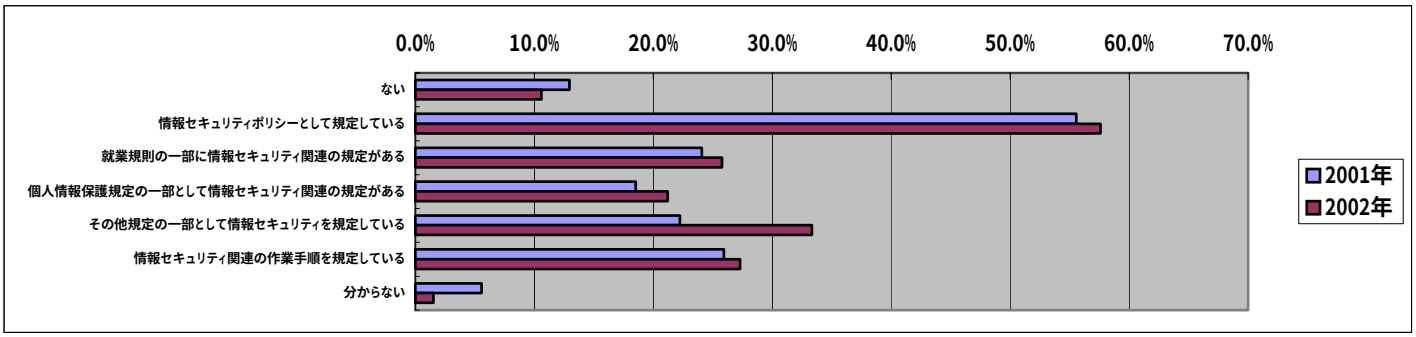
3.4.2 前年度調査結果と今年度調査結果の比較

前年 2001 年度の調査と本年 2002 年度の調査の内、同じ内容で調査した項目について比較し、1 年間でどのような差異が出たのか確認し検証する。

C　貴社の情報セキュリティ管理への取組みについてご回答下さい。

C-1 情報セキュリティに関する規定をお持ちですか。（該当全て）

		2001 年		2002 年	
1	ない	7	13.0%	7	10.6%
2	情報セキュリティポリシーとして規定している	30	55.6%	38	57.6%
3	就業規則の一部に情報セキュリティ関連の規定がある	13	24.1%	17	25.8%
4	個人情報保護規定の一部として情報セキュリティ関連の規定がある	10	18.5%	14	21.2%
5	その他規定の一部として情報セキュリティを規定している	12	22.2%	22	33.3%
6	情報セキュリティ関連の作業手順を規定している	14	25.9%	18	27.3%
7	分からない	3	5.6%	1	1.5%

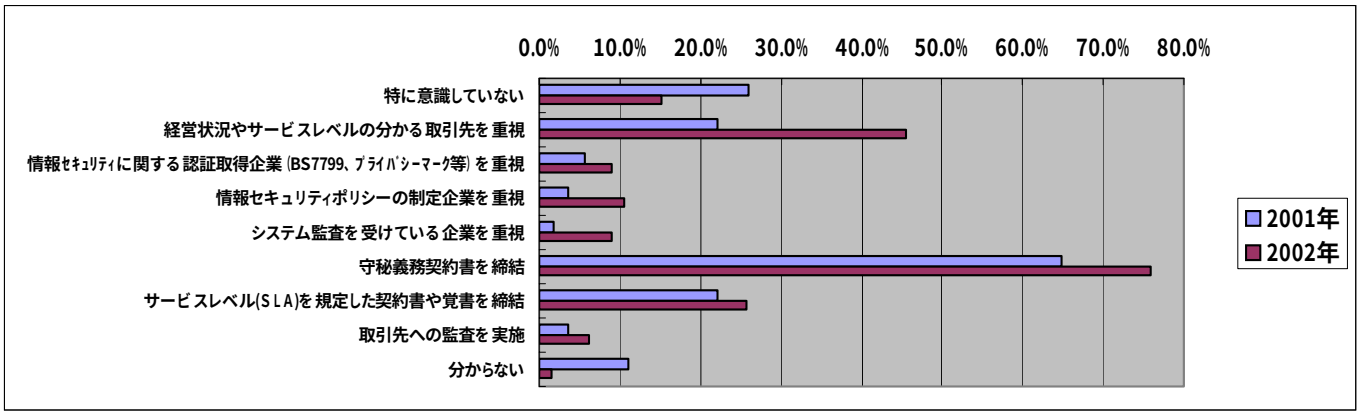


Note

前年と比較するとセキュリティに関する規定類の整備が小幅ではあるが、進捗しているのがわかる。“5 その他規定の一部として情報セキュリティを規定している ”という回答の伸びが大きいのは、ポリシーの必要性は感じるものの専門のセキュリティポリシーではなく、着手しやすい既存の規定（社則など）の拡張により、セキュリティ関連項目を盛り込むという選択をしているのが理由として考えられる。

C-5　情報セキュリティの観点から取引先の選定や契約時に配慮している点。（該当全て）

		2001 年		2002 年	
1	特に意識していない	14	25.9%	10	15.2%
2	経営状況やサービスレベルの分かる取引先を重視	12	22.2%	30	45.5%
3	情報ｾｷｭﾘﾃｨに関する認証取得企業（BS7799、ﾌﾟﾗｲﾊﾞｼｰﾏｰｸ等）を重視	3	5.6%	6	9.1%
4	情報セキュリティポリシーの制定企業を重視	2	3.7%	7	10.6%
5	システム監査を受けている企業を重視	1	1.9%	6	9.1%
6	守秘義務契約書を締結	35	64.8%	50	75.8%
7	サービスレベル(ＳＬＡ)を規定した契約書や覚書を締結	12	22.2%	17	25.8%
8	取引先への監査を実施	2	3.7%	4	6.1%
9	分からない	6	11.1%	1	1.5%



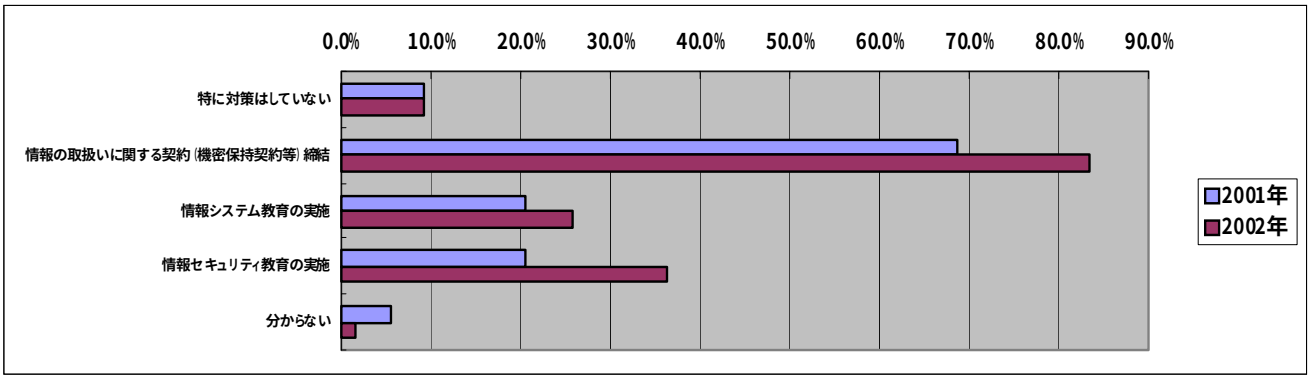
Note

“２経営状況サービスレベルの分かる取引先を重視”が昨年よりも伸びているのは、景気の低迷を反映したものでセキュリティとは直接関連しない可能性が高い、。取引先選定において、認証や監査などセキュリティを第三者的に計測する手段が少ない中で、合理的な選定理由として、本項目を挙げざるおえない企業が多いと考える。

他の項目も若干パーセンテージは上がっているが、認証・ポリシーともに10%程度で外圧がかかるレベルには程遠い。

C-6 派遣社員や常駐作業員受入時の配慮点をご回答下さい。（該当全てに○をお付け下さい）

		2001 年		2002 年	
1	特に対策はしていない	5	9.3%	6	9.1%
2	情報の取扱いに関する契約（機密保持契約等）締結	37	68.5%	55	83.3%
3	情報システム教育の実施	11	20.4%	17	25.8%
4	情報セキュリティ教育の実施	11	20.4%	24	36.4%
5	分からない	3	5.6%	1	1.5%

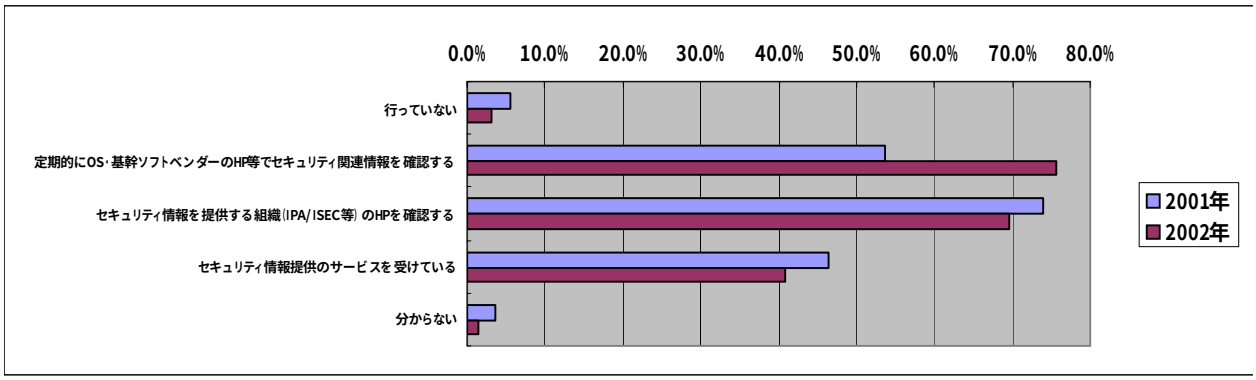


Note

正社員以外にも対策が必要という意識は上がっている。実施率が上がっているのは、調査対象にJNSA の会員企業が多いため、システム的な対応はかなり進み、次のフェーズとして人的な対策に重点が移ってきている可能性がある。あるいは、内部管理面での情報漏洩事故が増加している影響で教育熱が上がっている可能性も大きい。

C-8 情報セキュリティ関連ニュース等の収集についてご回答下さい。（該当全て）

		2001 年		2002 年	
1	行っていない	3	5.6%	2	3.0%
2	定期的に OS･基幹ソフトベンダーの HP 等でセキュリティ関連情報を確認する	29	53.7%	50	75.8%
3	セキュリティ情報を提供する組織（IPA/ISEC 等）の HP を確認する	40	74.1%	46	69.7%
4	セキュリティ情報提供のサービスを受けている	25	46.3%	27	40.9%
5	分からない	2	3.7%	1	1.5%

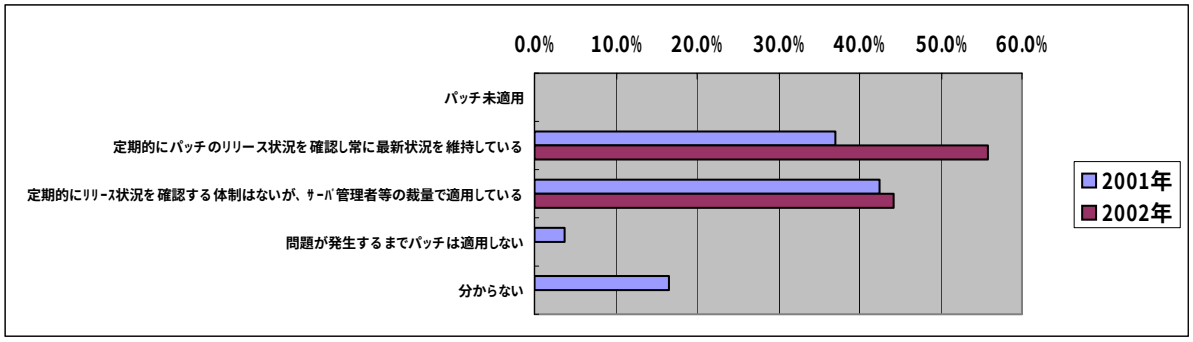


Note

情報の収集方法として“2 定期的に OS・基幹ソフトベンダーの HP 等でセキュリティ関連情報を確認する”のみが増加している。いくつかの情報源を経験した結果、パッチなど直接的に対策に結びつく情報にアクセスする習慣ができたのではないかと思われる。

C-9 サーバのセキュリティを確保するための各種パッチを適用。（1 つ選択）

		2001 年		2002 年	
1	パッチ未適用	0	0.0%	0	0.0%
2	定期的にパッチのリリース状況を確認し常に最新状況を維持している	20	37.0%	34	55.7%
3	定期的にﾘﾘｰｽ状況を確認する体制はないが、ｻｰﾊﾞ管理者等の裁量で適用している	23	42.6%	27	44.3%
4	問題が発生するまでパッチは適用しない	2	3.7%	0	0.0%
5	分からない	9	16.7%	0	0.0%
		54	100.0%	61	100.0%

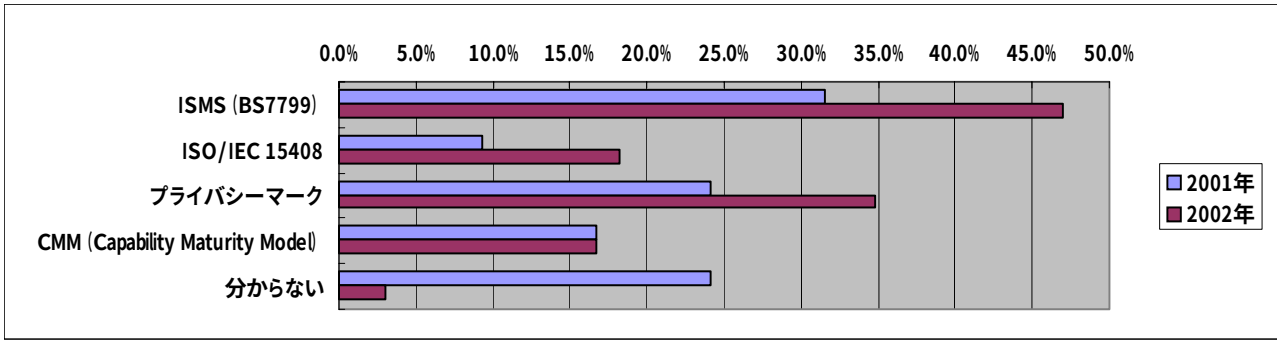


Note

“4 問題が発生するまでパッチを適用しない”と“5 分からない”という否定的な項目が 0%になったのは進展が見られる。“3 サーバ管理者の裁量で適用している”という項目に若干の増加が見られるのはパッチ適用のシビアさを反映しているといえる。

C-10　認証取得を「計画中」、または「取得済」の別を右欄に○を付けてご回答下さい。

		2001 年				2002 年			
	名称	計画中	割合	取得済	割合	計画中	割合	取得済	割合
1	ISMS (BS7799)	14	25.9%	3	5.6%	21	31.8%	10	15.2%
2	ISO/IEC 15408	5	9.3%	0	0.0%	7	10.6%	5	7.6%
3	プライバシーマーク	4	7.4%	9	16.7%	11	16.7%	12	18.2%
4	CMM (Capability Maturity Model)	8	14.8%	1	1.9%	9	13.6%	2	3.0%
5	分からない	13	24.1%	0	0.0%	1	1.5%	1	1.5%



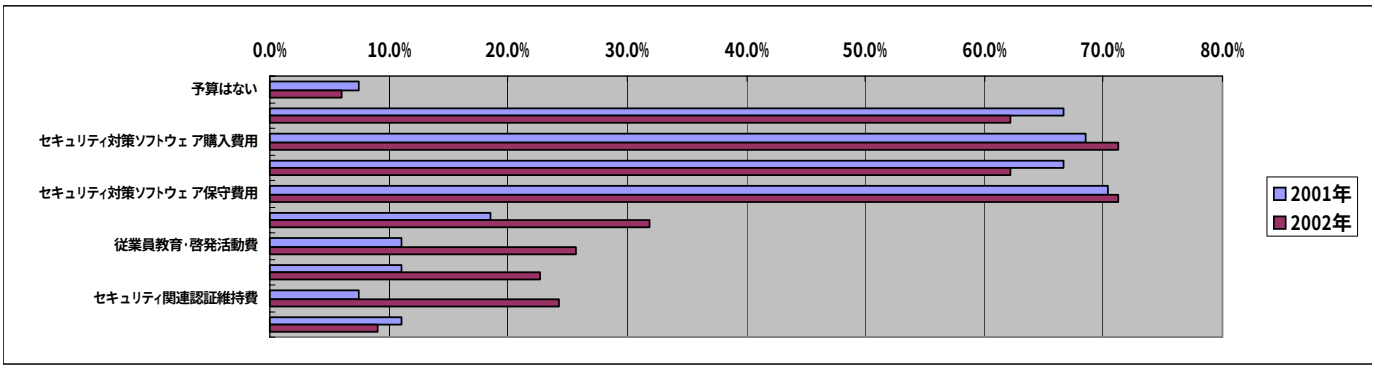
Note

上記グラフは、取得済みと計画中の合計で前年と比較をおこなった。グラフで見ると大きな伸びに見えるが、10%から 15%程度の伸びにおさまっている。

“５分からない”という回答が激減したのは、認証の知名度や関心が大きくなっており、今後の企業活動においても、このような認証取得を検討せざるおえない環境になっていると考えられる。

C-14 情報セキュリティ関連予算の対象をご回答下さい。（該当全てに○をお付け下さい）

		2001 年		2002 年	
1	予算はない	4	7.4%	4	6.1%
2	セキュリティ対策ハードウェア購入費用	36	66.7%	41	62.1%
3	セキュリティ対策ソフトウェア購入費用	37	68.5%	47	71.2%
4	セキュリティ対策ハードウェア保守費用	36	66.7%	41	62.1%
5	セキュリティ対策ソフトウェア保守費用	38	70.4%	47	71.2%
6	セキュリティ管理者教育費	10	18.5%	21	31.8%
7	従業員教育･啓発活動費	6	11.1%	17	25.8%
8	セキュリティ関連認証取得費	6	11.1%	15	22.7%
9	セキュリティ関連認証維持費	4	7.4%	16	24.2%
10	分からない	6	11.1%	6	9.1%

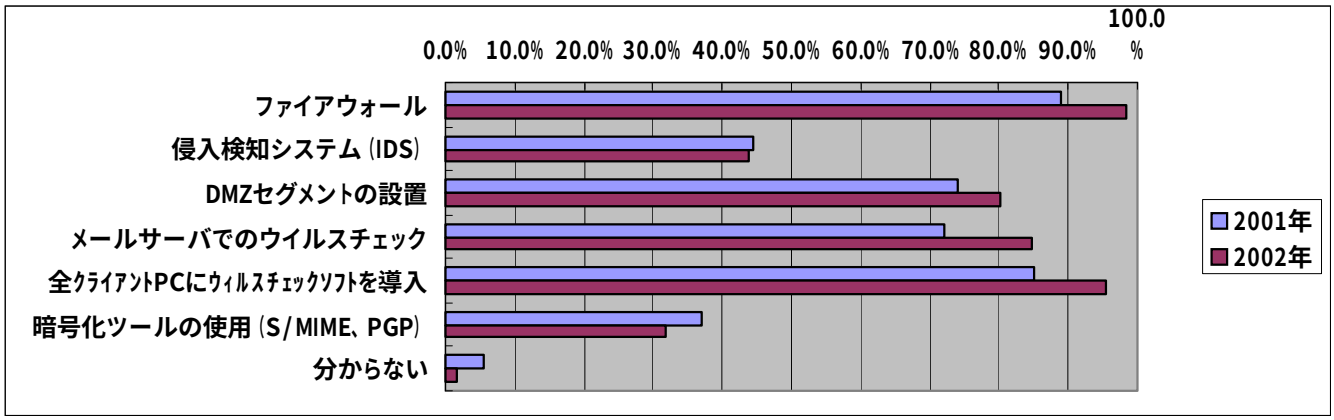


Note

教育費関連が顕著に伸びていることがわかる。認証関連の予算は、認証済み企業が増えていることから当然の結果といえる。

C-15　情報セキュリティを確保するために導入しているシステムをご回答下さい。（該当全てに○をお付け下さい）

		2001 年		2002 年	
1	ファイアウォール	48	88.9%	65	98.5%
2	侵入検知システム (IDS)	24	44.4%	29	43.9%
3	DMZ セグメントの設置	40	74.1%	53	80.3%
4	メールサーバでのウイルスチェック	39	72.2%	56	84.8%
5	全ｸﾗｲｱﾝﾄ PC にウイルスﾁｪｯｸｿﾌﾄを導入	46	85.2%	63	95.5%
6	暗号化ツールの使用 (S/MIME、PGP)	20	37.0%	21	31.8%
7	Proxy ｻｰﾊﾞｰ側にウイルスﾁｪｯｸを導入	-	-	21	31.8%
8	分からない	3	5.6%	1	1.5%

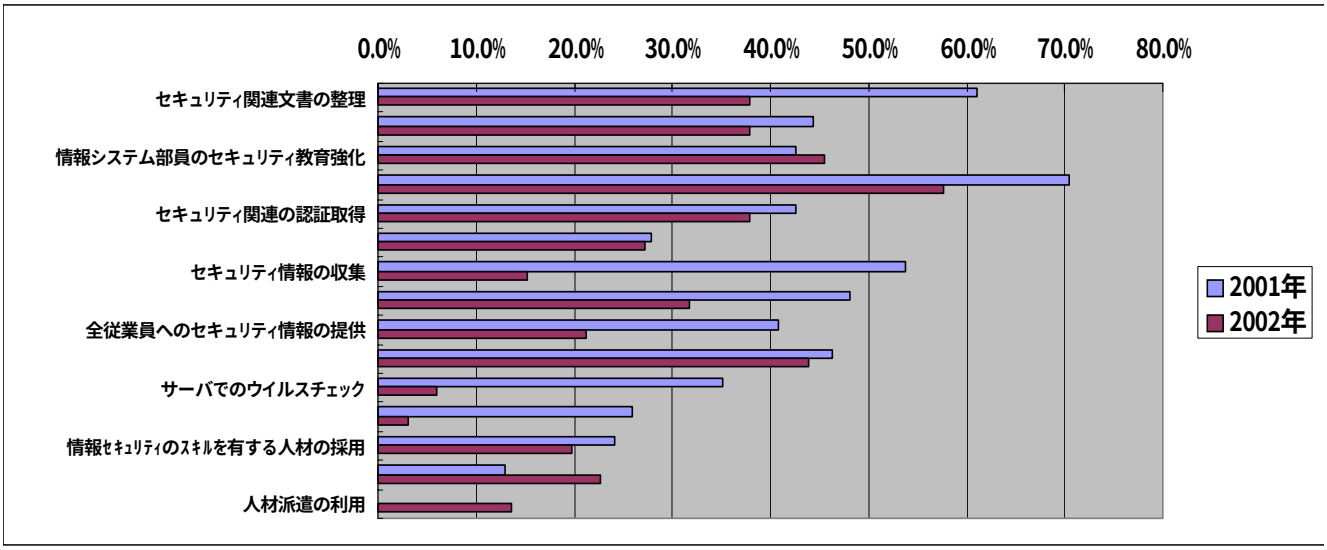


Note

ファイアウォールの導入は、ほぼ 100%となった(未導入は 1 社のみ)。ウイルス対策についても 1 社を除きサーバ・クライアント・Proxy サーバのいずれかで実施しており、調査先における本年のウイルス被害や被害の拡大が抑制できた大きな要因と考えられる。

C-19 現在実施、また今後実施していきたいと考えている情報セキュリティ関連対策(該当全て)

		2001 年		2002 年			
		今後	割合	実施済	割合	今後	割合
1	セキュリティ関連文書の整理	33	61.1%	27	40.9%	25	37.9%
2	情報セキュリティを考慮した社内制度の制定	24	44.4%	26	39.4%	25	37.9%
3	情報システム部員のセキュリティ教育強化	23	42.6%	21	31.8%	30	45.5%
4	一般従業員のセキュリティ教育強化	38	70.4%	21	31.8%	38	57.6%
5	セキュリティ関連の認証取得	23	42.6%	12	18.2%	25	37.9%
6	セキュリティ関連認証取得システムの導入	15	27.8%	5	7.6%	18	27.3%
7	セキュリティ情報の収集	29	53.7%	44	66.7%	10	15.2%
8	システム監査の実施	26	48.1%	20	30.3%	21	31.8%
9	全従業員へのセキュリティ情報の提供	22	40.7%	38	57.6%	14	21.2%
10	事故･事件対応訓練	25	46.3%	9	13.6%	29	43.9%
11	サーバでのウイルスチェック	19	35.2%	56	84.8%	4	6.1%
12	クライアントでのウイルスチェック	14	25.9%	60	90.9%	2	3.0%
13	情報ｾｷｭﾘﾃｨのｽｷﾙを有する人材の採用	13	24.1%	20	30.3%	13	19.7%
14	ASP (Application Service Provider) や IDC (Internet Data Center)の利用	7	13.0%	14	21.2%	15	22.7%
15	人材派遣の利用	0	0.0%	6	9.1%	9	13.6%



Note

上記グラフは、「今後実施したい対策」を比較したものである。ほとんどの項目で前年より低下しており、基本的な対策は整備が完了しており、新規導入は人材などを除き、一段落している可能性がある。

3.4.3 被害状況の概要

前年 2001 年度の被害報告は調査対象 55 件中 33 件（61%）あったが、本年 2002 年度は同 66 件中 11 件（17%）と前年の約 1/4 に大きく減少した。また、被害範囲も低く留まり、被害金額も低くなっている。

① 被害状況（インシデント毎の被害額、被害額順）

No.	人件費／日 (円)	被害額 (円)							合計 (円)	備考
		営業継続費	逸失利益	喪失した情報資産	機会損失	賠償保証	その他関連出費	復旧費		
1	*40,000*						400,000		400,000	注 1
2	30,000		60,000					270,000	330,000	
3	50,000	150,000						25,000	175,000	注 2
4	*40,000*							150,000	150,000	
5	*40,000*	120,000							120,000	注 3
6	*40,000*						20,000	100,000	120,000	
7	50,000							25,000	25,000	注 2
8	*40,000*							15,000	15,000	注 4
9	*40,000*								0	注 5
10	*40,000*									注 6
11	*40,000*									注 7
								総 計	1,335,000	
								平 均	121,364	

■ 算出条件

・被害調査アンケートにて項目 12～19 に被害額が入っているものについてはその数値を採用した。

・項目 12～19 に数値が記述されていないものについては、アンケート項目 5～21 と人件費から予想される数値を算出し表に記入した。

・人件費について回答が無いものは一律一人あたり 40,000 円/日とした。（人件費がイタリック書体になっている箇所）

■ 注釈

(注 1)お詫び行脚（10 人日）×1 日人件費（40,000 円）　で算出。

(注 2) No.3 と No.7 は同一企業。

(注 3)停止時間(1 日)×影響を受けた人数(10 人)×業務低下割合(30%)×1 日人件費(40,000 円)で算出。

(注 4)停止時間(0.125 日)×影響を受けた人数(3 人)×1 日人件費(40,000 円)で算出。停止時間は 1 日 8 時間労働中 1 時間停止として算出。

(注 5)実質の被害無しと回答している。

(注 6)影響を受けた人数のみ記述があり、停止時間等が提示されていないため被害額の算出不可。

(注 7)影響を受けた人数のみ記述があるものの、停止時間を 0 と記述しているため被害額の算出不可。

Note

前述の通り報告割合は前年 2001 年度が 61%なのに対し本年 2002 年度は 17%と大幅に減少。

被害額については、前年の被害総計が 141,478,800 円で平均 4,715,960 円に対し、本年は被害総計が 1,335,000 円で平均 121,364 円と平均値で前年比 の約 40 分の 1 になっている。また、前年の最大被害額が 60,000,000 円に対し本年は 400,000 円と、同じく大幅減となっている。

② インシデント別被害の状況(件数順)

コード No	被害項目	件数	件数比率	金額	金額比率
1	KLEZ (クレズ)	4	36%	310,000	22.88%
7	FLETHEM(フレゼム) 等	3	27%	355,000	26.20%
10	社外から不正アクセス	2	18%	550,000	40.59%
14	ルータ故障 SPAM	2	18%	140,000	10.33%
	合 計	11	100%	1,355,000	100%

Note

前年に比較してコンピュータウイルスによる被害が大幅に低下している。ウイルス被害の割合が 49.08%に対してウイルス以外の被害割合が 50.92%となっている。

③ 被害のあった企業の特徴

被害件数および被害額が大幅に低下したのは、調査の対象がコンピュータウイルスを主眼においた内容であったことと、ウイルス対策については対策手法がある程度確立し、昨年に比較して導入および運用が十分整備されていることが理由と考えられる。

次に、被害報告のあった企業のセキュリティ対策等プロフィールをまとめ、特徴を検証する。

No.	業種	従業員数(人)	事前に取っていた対策	被害の原因
1	情報･通信	1,200	・ポリシー有り ・被害発生時連絡体制有り ・ファイアウォール、IDS、DMZ 設置 ・パッチは最新を適用	DNS 7 台に不正侵入を受けた。原因は未回答。
2	その他	3,700	・ポリシー有り ・被害発生時連絡体制は無いが責任部門は有り ・サーバおよび各 PC でのウイルスチェック実施	エクストラネットで感染。Wondows ファイル共有で被害拡大。被害を受けたのが金曜日であったため業務への支障はなかった。
3	情報･通信	600	・ポリシー有り ・被害発生時連絡体制有り ・サーバおよび各 PC でのウイルスチェック実施	ウイルスチェックは実施していたが、リプレースした PC にウイルスチェックソフトのインストールを忘れたためウイルスに感染。
4	情報･通信	95	・ポリシー無し ・被害発生時連絡体制有り ・ファイアウォール、IDS、DMZ 設置	ファイアウォールの故障。
5	その他サービス	未回答	・ポリシー有り ・被害発生時連絡体制は無いが責任部門は有り ・ファイアウォール、IDS、DMZ 設置	ルータの故障。
6	情報･通信	800	・その他規定でポリシー有り ・被害発生時連絡体制は無いが責任部門は有り ・各 PC でのウイルスチェック実施	マシンパワーの無い PC にてログイン時の自動ウイルススキャンが動作せず感染。共有フォルダで被害拡大。
7	No.3 と同じ			コンピュータウイルス対策メーカの更新ファイルが遅れたため。
8	情報･通信	未回答	・ポリシー有り ・被害発生時連絡体制は無いが責任部門は有り ・サーバおよび各 PC でのウイルスチェック実施 ・ノート PC 持込制限無し	ウイルス対策をしていない自宅の PC に感染。その PC を社内に持ち込み共有フォルダ経由で拡大。
9	金融	134	・ポリシー有り ・被害発生時連絡体制有り ・サーバおよび各 PC でのウイルスチェック実施	原因は未回答。
10	その他	983	・その他規定でポリシー有り ・被害発生時連絡体制無し ・サーバおよび各 PC でのウイルスチェック実施	ウイルス定義ファイルの適用前に感染。
11	その他サービス	2,400	・ポリシー有り ・被害発生時連絡体制有り ・サーバおよび各 PC でのウイルスチェック実施	ウイルス定義ファイルの適用前に感染。

今回被害を報告した企業は、ポリシー策定、連絡体制の整備、ファイアウォールの設置、ウイルスチェックといった基本的なセキュリティ対策は実施している。そのため被害が発生した場合も小

さな規模におさまったと考えられる。

被害発生の原因は以下のように分類できる。

（ア）不可抗力的な原因

- システムの故障。
- コンピュータウイルス提供メーカの更新ファイルリリースの遅れ。

（イ）運用上の問題

- ウイルス定義ファイルの適用遅れ。
- エクストラネット経由で外部からウイルス感染。
- PC リプレース時のインストールミス。
- マシンパワーの不足。
- ウイルスに感染した PC の持込。

一定水準のセキュリティ対策は実施されているため、被害をもたらすのは外部要因ではなく、故障など不可抗力的なものや運用手順上の問題に起因する場合に限定された結果となった。

システムの故障やメーカの対応遅れといった、ユーザがコントロールできないような事象に伴う被害については、事後処理のための連絡体制や手順書の整備といったことが被害の範囲を左右する。

また、運用上の問題においては、人為的なものに起因する場合は、手順の徹底やチェック機能の強化、あるいは可能であれば自動化することで効果が得られると考えられる。

3.5 調査結果の分析と特徴

IPA（情報処理振興事業協会）の統計によるとコンピュータウイルス届出件数は、昨年に比較して約 16%減少し 10,352 件となり、実被害を受けたという報告も昨年に比較して半減している。2001 年に感染力の高い Sircum や Nimda が猛威を振るったことが経験となり、ウイルスに対する認識が上がり、対策が進んだものと考えられる。それを反映するように当被害調査においても被害額は昨年に比べ大幅に減少している。

コンピュータウイルス対策ソフトメーカ数社に確認をしたところ、昨年に比較して販売実績は確かに伸びているが、何よりもユーザがウイルス定義ファイルの更新を徹底していることが被害を低く抑える要因になっているのではないかというコメントがあった。

今回のアンケートによると各社のセキュリティ対策については、ファイアウォールやコンピュータウイルス対策は約 100%が配備し、侵入検知システム（IDS）も 43.9%が導入しているという結果となった。また、パッチの適用も 100%が実施している。

ファイアウォール、ウイルスチェック、IDS などの導入により、不正侵入・コンピュータウイルスへの技術的対策は定着してきたが、昨今問題になっている情報漏洩については設定ミスや関係者による不正といった人的要素が高く、技術的対策よりも管理・運用面の対策が求められる傾向にある。

運用面については、ポリシー等規定を設定している企業は 87.9%になり、連絡体制の整備、教育の実施も高い比率で実施している。このように、技術面・運用面の整備が進んだことが今回の調査で被害額が低く抑えられる結果に結びついたと考えられる。

しかし反面、被害を受けたと回答した企業も同様に技術的対策やポリシーの策定は実施しており、教育の徹底やチェック機能の強化に再考の余地があることを明らかにした。利便性とのバランスを考慮しながらも、罰則規定など強制力を伴う運用ルールや管理体制の強化が企業にとって今後の課題となるだろう。

予算面に関しては、65.2%の企業が情報セキュリティに割り当てる予算を情報システム関連予算の一部として計上しており、また、売上高に占めるセキュリティ予算の割合も非常に低く、企業活動の中でセキュリティ対策が優先順位の低い位置にあることを示唆している。

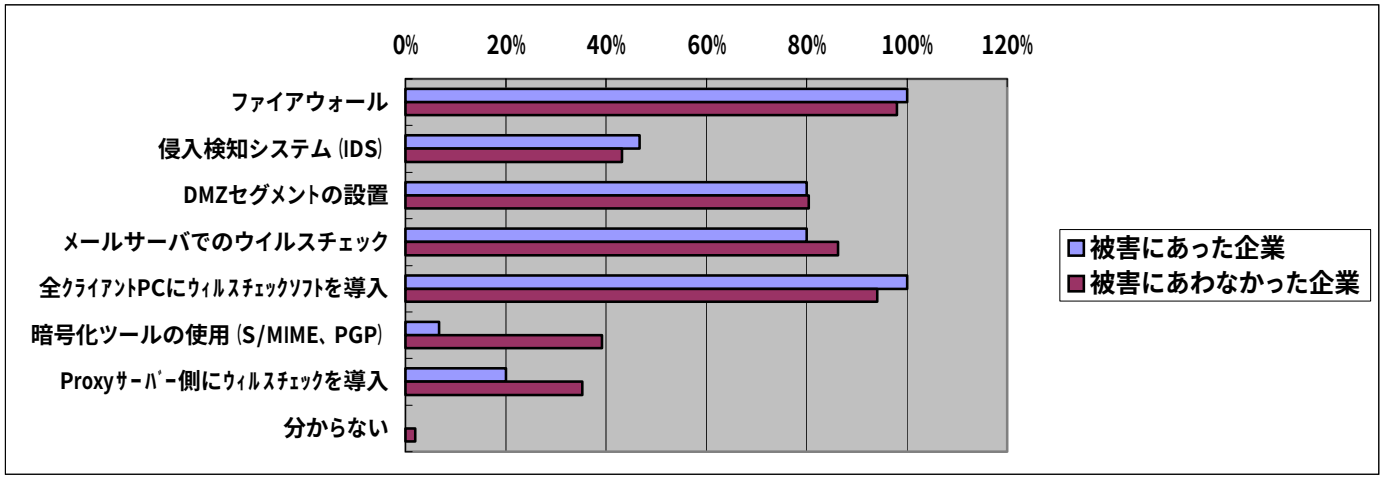
セキュリティ対策は効果が見えにくいというのも予算が確保できない理由のひとつと考えられるが、今後のアンケートおよびヒアリング内容については、導入しているセキュリティ技術がインシデント発生率にどのような影響を与えているのか、また、連絡体制などの対策が被害発生後の対応にどれだけ効果を発揮しているのかを、定量的にまたコスト的に把握するような質問項目を検討していく必要があるだろう。

4. 情報セキュリティインシデント対策の標準モデルと対策費用

4.1 被害発生を抑止している情報セキュリティインシデント対策の状況

本年度の「情報セキュリティインシデントが発生した企業のグループ」と「被害にあわなかった企業のグループ」について、「情報セキュリティを確保するために導入しているシステム」項目のアンケート結果をもとに対策などの差異を把握するために分析を行った。

情報セキュリティを確保するために導入しているシステム		被害にあった企業 15社		被害にあわなかった企業 51社	
1	ファイアウォール	15	100%	50	98%
2	侵入検知システム (IDS)	7	47%	22	43%
3	DMZ セグメントの設置	12	80%	41	80%
4	メールサーバでのウイルスチェック	12	80%	44	86%
5	全ｸﾗｲｱﾝﾄ PC にウイルスﾁｪｯｸｿﾌﾄを導入	15	100%	48	94%
6	暗号化ツールの使用 (S/MIME、PGP)	1	7%	20	39%
7	Proxy ｻｰﾊﾞｰ側にウイルスﾁｪｯｸを導入	3	20%	18	35%
8	分からない	0	0%	1	2%



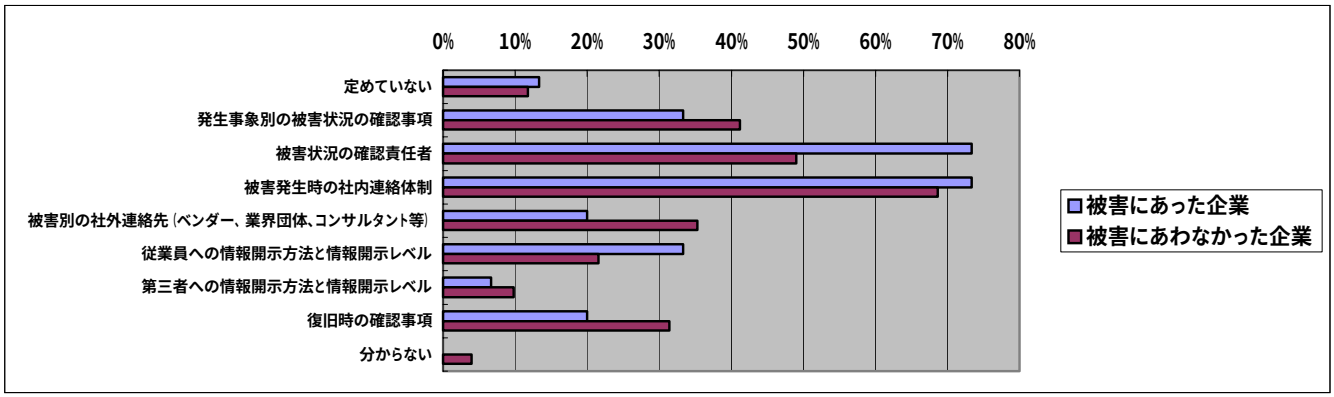
各グループの特徴を見ると、特に大きな差異は見つからない。暗号化ツールや Proxy サーバー側にウイルスチェックという項目では、被害にあわなかったグループの導入率が高い点がグラフでは見られる。

しかしながら、今回発生のインシデント内容から、これらが原因とは考えにくい。

今回のアンケート結果からは、「セキュリティ対策システムの導入比率」と、「被害を防いでいる比率」は特に関連性が見られない結果になった。

技術的な項目では差異がなかったため、「被害が発生した場合の体制」や「セキュリティに関する教育」「派遣社員の受け入れ体制」などについて、「セキュリティに対する企業の意識に関連するアンケート項目」を「被害にあわなかったグループ」と「被害にあったグループ」で比較を行い、次の 4 個のグラフを作成した。

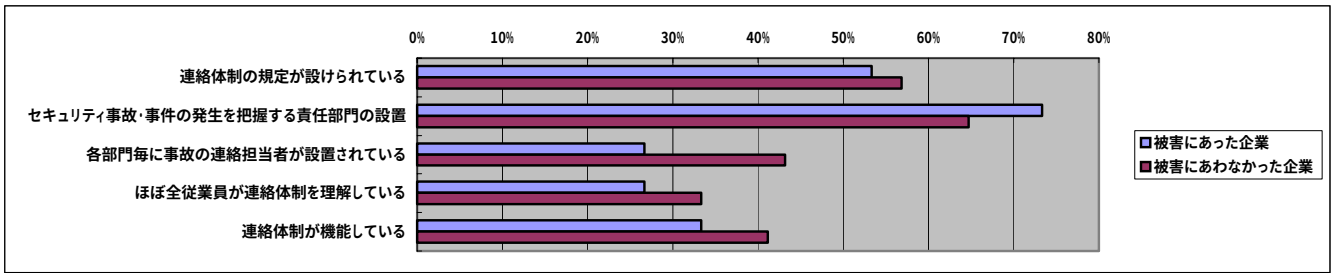
①被害が発生した時の対応計画の対象



上記のグラフからは、顕著な差があるのは、被害にあったグループのほうが、被害状況の確認責任者を決めている比率が高い。事故発生と責任者設置の時期についての情報が無いため、安全対策の状況としては逆になった。

この点については、被害を受けた経験によって、確認責任者を設置の必要性を感じ、事後対策として導入した可能性がある。

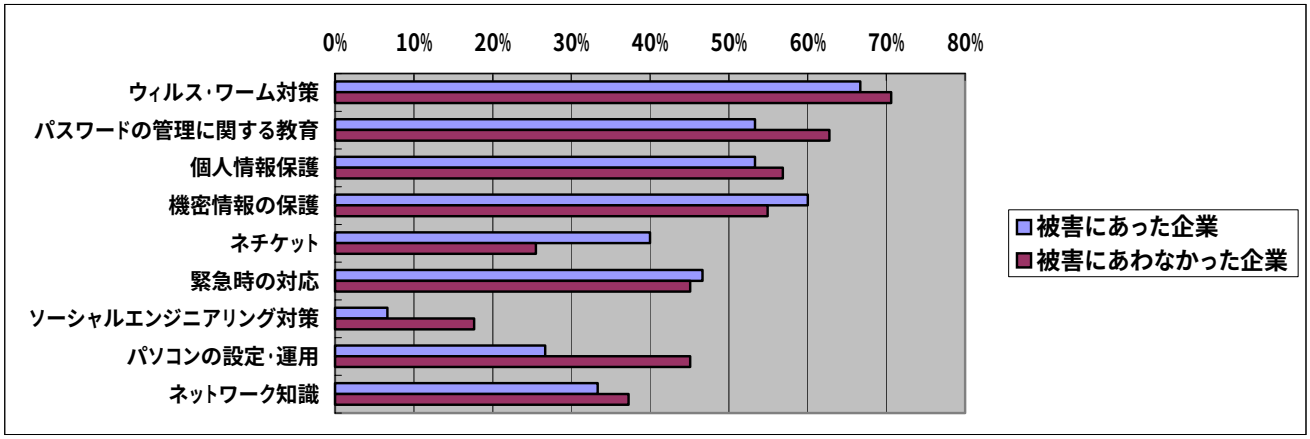
②情報セキュリティ関連の事故や事件が発生した場合の社内連絡体制



インシデントが発生した後の連絡体制について、被害にあったグループの法が「インシデント発生を把握する責任部門の設置」がやや多いものの、その他の項目では被害にあわなかったグループの比率が高くなっている。

前述の「責任者を設置」と同様に「責任部門の設置」の必要性を感じて、事後対策として導入した可能性がある。

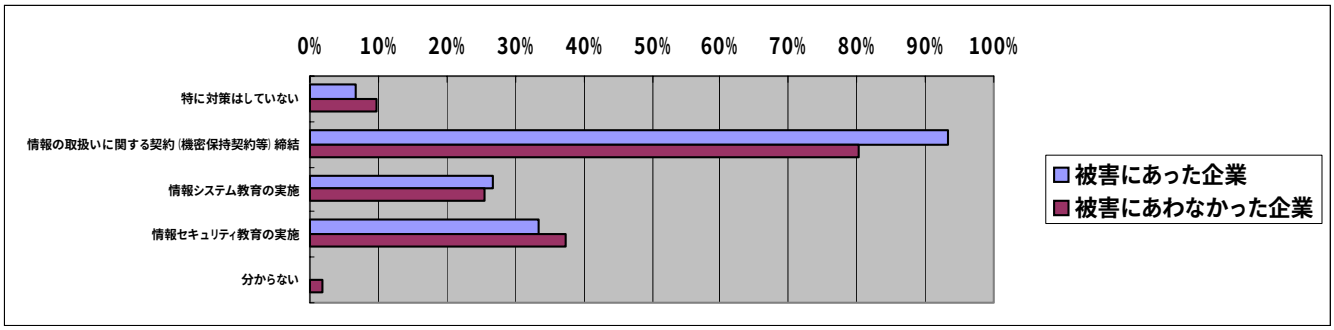
③情報セキュリティ教育の内容



情報セキュリティ教育に関しては、ネチケットとパソコンの設定・運用の項目に差異があるが、インシデント被害との関連性はあまり見られない。

全 9 項目のうち 6 項目で「被害にあわなかったグループ」のほうが、相対的に取り組み割合が高く、情報セキュリティ教育に対してより熱心であるということが考えられる。

④派遣社員や常駐作業員受け入り時の配慮点



派遣社員などの受け入り時の配慮については、大きな差異はなかった。

本章全体を通して、情報セキュリティインシデント被害を抑止している情報セキュリティ対策をアンケートの集計から考察すると、ファイアウォールやウイルスチェックソフトなどのセキュリティ対策システムの導入比率との相関関係は、残念ながら特に見出せなかった。

ただし、情報セキュリティインシデント被害を受けた後に、すぐにシステム的な対策を実施したことも考えられるため一概に無関係とは結論付けられない。

また、今回のアンケート及びヒアリング先における「セキュリティ対策システムの導入率」は、一般と比べるとかなり高いと考える。そのため、これにより情報セキュリティインシデント被害の発生自体を低く押さえる効果を発揮していると判断できる。

セキュリティ対策におけるシステム以外の対策では、「情報セキュリティ教育」や「インシデント被害対策体制」がインシデント被害の抑止に、貢献している傾向が見て取れる。

4.2　抑止モデルの情報セキュリティ関連予算の実際

本年度の調査で、情報セキュリティインシデントが「発生した企業」と「発生しなかった企業」を二つのグループに分けて、その中で「情報セキュリティ関連予算」について、アンケート回答のある企業のみを取り出し、傾向を分析する。

①被害にあったグループ（７社）

No.	従業員数 (人)	セキュリティ予算 (万円)	予算の割合 (%)	一人あたりの予算 (円)
1	100	20	1.0%	2,000
2	15,470	1,000	0.1%	646
3	983	500	-	5,086
4	800	200	8.0%	2,500
5	95	500	30.0%	52,632
6	6,487	5,000	0.5%	7,708
7	3,700	7,500	40.0%	20,270
合計	27,635	14,720	-	90,842
平均	3,948	2,103	13.3%	12,977

②被害にあわなかったグループ（２３社）

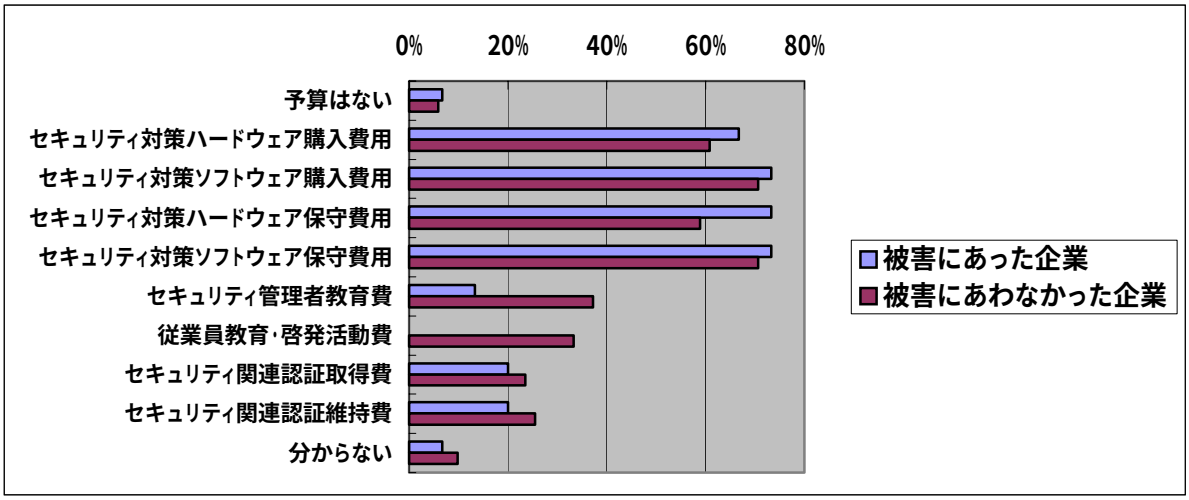
No.	従業員数 (人)	セキュリティ予算 (万円)	予算の割合 (%)	一人あたりの予算 (円)
1	1	30	10.0%	300,000
2	30	500	10.0%	166,667
3	140	1,100	65.0%	78,571
4	400	500	30.0%	12,500
5	400	1,000	-	25,000
6	6,000	1,000	1.0%	1,667
7	1,112	1,000	20.0%	8,993
8	80	400	25.0%	50,000
9	34	150	20.0%	44,118
10	32	800	10.0%	250,000
11	130	150	20.0%	11,538
12	980	1,000	3.0%	10,204
13	120	3,000	50.0%	250,000
14	220	3,000	-	136,364
15	5,000	10,000	3.0%	20,000
16	650	3,000	9.0%	46,154
17	250	400	2.5%	16,000
18	56	300	-	53,571
19	551	1,000	7.0%	18,149
20	900	400	3.0%	4,444
21	2,800	1,200	2.0%	4,286
22	330	256	5.0%	7,758
23	2,100	5,500	3.0%	26,190
合計	22,316	35,686	-	1,542,174
平均	970	1,552	14.9%	67,051

インシデント被害の「発生した企業」と「発生しなかった企業」の企業規模が違うので単純に総額では比較できないため、各グループの従業員数とセキュリティ予算を合計して「一人あたりのセキュリティ予算」を比較すると、「被害にあわなかったグループ」の一人あたりの情報セキュリティ予算が 15,991 円に対し「被害にあったグループ」の予算は 5,327 円と 3 倍の差が出た。

「情報セキュリティ予算」は、企業規模が大きくなれば一人あたりの金額は少ない傾向があり、情報セキュリティ予算の定義が明確ではない点を考慮すると、今回表れた「3 倍の差」を単純に判断できないが、来年度以降の調査においても継続的に傾向を分析していきたい結果となった。

次に、情報セキュリティ予算の内訳を各グループごとに比較してみる。

	情報セキュリティ関連予算の対象	被害にあった企業		被害にあわなかった企業	
1	予算はない	1	7%	3	6%
2	セキュリティ対策ハードウェア購入費用	10	67%	31	61%
3	セキュリティ対策ソフトウェア購入費用	11	73%	36	71%
4	セキュリティ対策ハードウェア保守費用	11	73%	30	59%
5	セキュリティ対策ソフトウェア保守費用	11	73%	36	71%
6	セキュリティ管理者教育費	2	13%	19	37%
7	従業員教育･啓発活動費	0	0%	17	33%
8	セキュリティ関連認証取得費	3	20%	12	24%
9	セキュリティ関連認証維持費	3	20%	13	25%
10	分からない	1	7%	5	10%



比較の結果、顕著ではないが「セキュリティ対策ハードウェア／ソフトウェアの購入費用／保守費用」ともに「被害にあったグループ」のほうが「情報セキュリティ予算の対象にしている比率」がやや高い傾向になっている。

また、教育・啓発活動費については、逆に「被害にあわなかったグループ」のほうの比率が、格段に高くなっており、この傾向は、「4.1 被害発生を抑止している情報セキュリティインシデント対策の状況」の結果と合致している。

これは、最近の情報セキュリティインシデントが発生している原因が、技術的な対策をすり抜けるような不可抗力であったり、人為的な不注意からであることが多いという点が考えられる。

つまり、情報セキュリティインシデントの発生を抑える要因として「教育・啓発・被害対策」の体制作りが必要と考えられる。

4.3　望まれる対策レベルと予算規模の提案

情報インシデント被害状況では、依然コンピュータウイルスによる被害が多くなっている。

技術的な対策としては、アンチウイルスソフトの導入率がかなり増加しており、企業ではクライアント、サーバ、ゲートウェイなど多面的な対策を実施するのが当然になってきている。

コンピュータウイルスの傾向もシステム障害を起こすというものから、他のコンピュータやサーバを攻撃したりコンピュータの保存しているファイルを添付して、情報漏洩を起させようとしたり、他のメールアカウントを偽装するような多岐にわたるようになってきているため、防御をする側も、被害に遭わないことだけでなく加害者にならない事も考えなければならなくなっている。

実際の情報セキュリティインシデントの例を見ても新種のコンピュータウイルスの侵入や、感染しているノートパソコンの社内ネットワークへの接続による感染など、多面的技術的にアンチウイルスソフトで防御していても、コンピュータウイルスに感染している。

これらの感染を防ぐにはセキュリティポリシーで、メールの添付ファイルの取り扱いに注意したりノートパソコンの持ち込み、持ち出し制限をかける対策が必要になり、万一インシデントが発生し、外部に感染したメールを発信してしまった場合の危機対策マニュアルの作成も重要になる。

今回の調査先では、外部からの不正侵入に対し、ほぼ１００％ファイアウォールが導入されており、それほど多く被害は生じていない。

セキュリティパッチの実装も意識が高くなっており、全般的に「不正侵入対策に対して何をすべきか」という知識と意識が浸透し、これに応じた運用が行われてきていると考えられる。

これには、情報漏洩事故がニュースなどに取り上げられることが多く、Web の改ざん防止といった愉快犯対策ではなく、情報漏洩を防ぐことの重要性と、万一情報漏洩事故を起した場合の対応を準備する必要性を強く感じていることに起因していると考えられる。

①現状で考えられる最低限の対策レベル

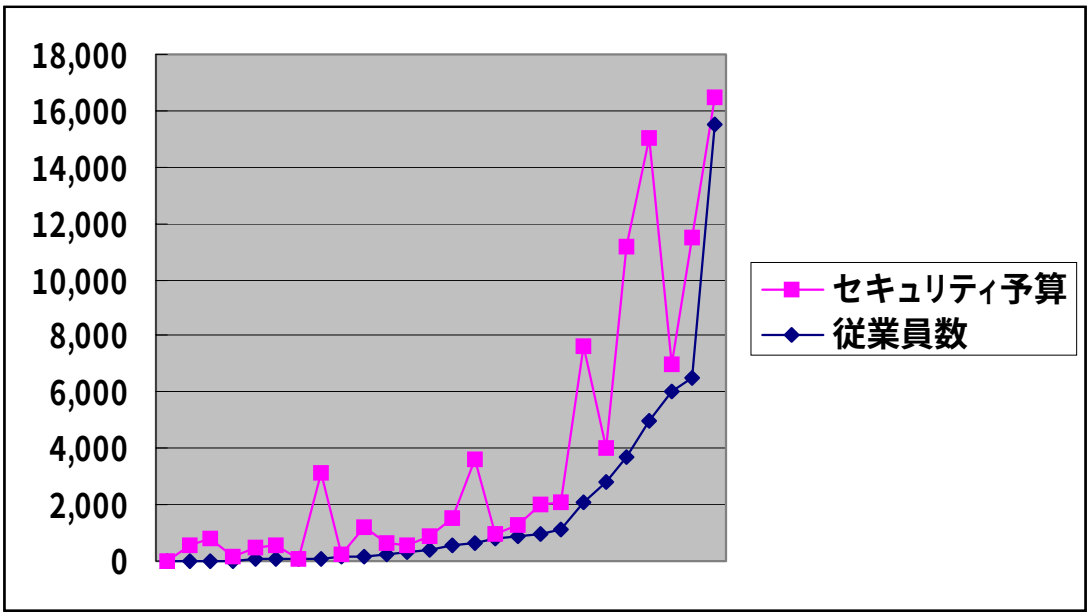
このような事故事例や調査結果をもとにすると、「理想論やあるべき論」は別にして、現状で考えられる最低限の対策レベルとしては、下表の「運用上の対策をユーザに浸透させるセキュリティ教育・啓発活動の実施レベル」までを推奨したい。

対策レベル		具体例
対策レベル1	技術的対策	アンチウイルスソフト
		メール監視ソフト
		ファイアウォール
		IDS
		認証デバイス
対策レベル2	運用上対策	入退室管理
		セキュリティ管理責任者の任命
		情報セキュリティに関する規定作成
		セキュリティ事故対応マニュアル
対策レベル3 (推奨レベル)	情報セキュリティ教育・啓発	コンピュータウイルス教育
		パスワード管理教育
		機密情報保護教育
対策レベル4	セキュリティ監査・第三者認証	ISMS・BS7799
		P マーク

②従業員数とセキュリティ関連予算額の相関

今回のアンケートでは、情報システム予算における情報セキュリティ関連予算の割合は、最大６５％（従業員数 140 名）から最小０．１％（従業員数 15,470 名）まで多岐にわたり、平均で１４．５％になった。

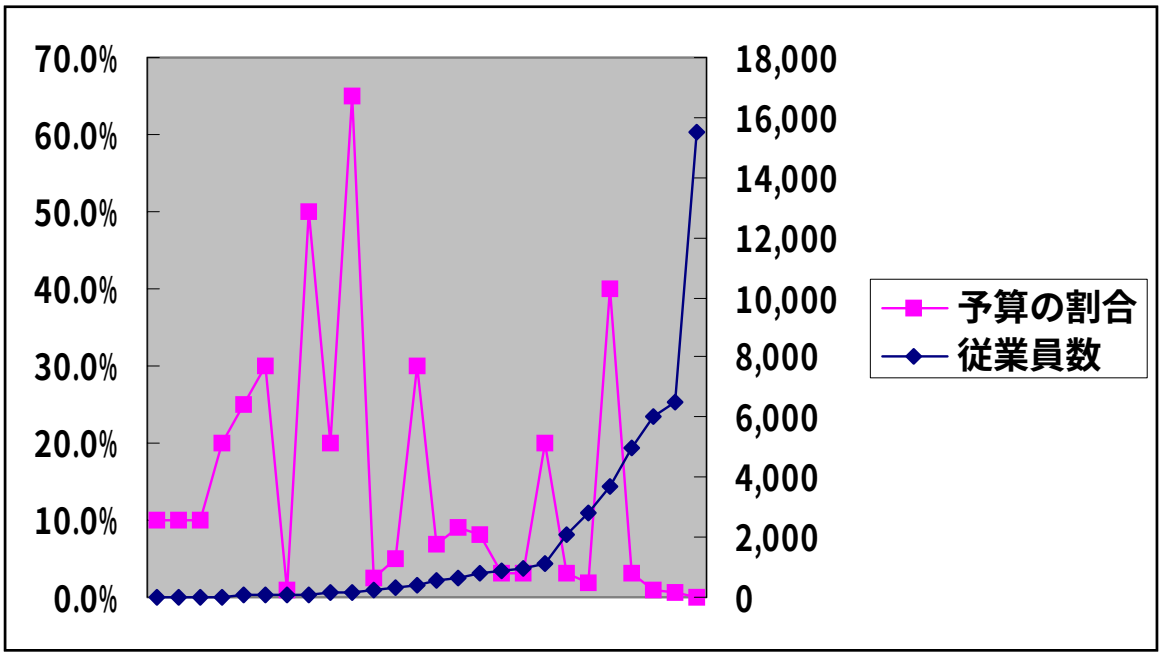
下記の図のように従業員数とセキュリティ予算額は、ほぼ比例している。



③従業員数と情報システム予算における情報セキュリティ関連予算の割合の比較

従業員数と情報セキュリティ予算の割合は、下記の図のように反比例傾向にはあるものの、振れ幅が大きい。ヒアリング時、ほぼ毎回のように「何をセキュリティ関連予算に含めるか」という単純な質問が出ていた。たとえば「ルータはセキュリティ機器か通信機器か」という点一つを考えてもセキュリティ予算額判断の難しさが挙げられる。

このように、予算定義の曖昧なもの以外にも、新規にハードウェア、ソフトウェアを導入した場合は、一時的に大きな予算を取る場合があり、経費予算に占める情報システムの予算額も業種、企業規模、時期によって大きく変わるということも考えられる。



また、「ほとんどの企業では情報システム予算の○○%」というような考え方は持っておらず、ヒアリング結果から考えると、必要に応じて予算申請、予算執行を行っているのが現状である。

このような難しい点や企業規模でのばらつきが見られるものの、おおよその企業では「情報セキュリティ関連の保守費、運用対策費、セキュリティ教育費」などを必要に応じ、情報システム予算の５～１５%を目安にセキュリティ関連費用として計上している。

教育に関わる「セキュリティ教育啓発活動」に関しては、年間スケジュールを立案し計画的なセキュリティ対策の運用が重要となる。

5. 2002 年度情報セキュリティインシデント被害額算出モデルに関する検討

ここでは、昨年度モデルをもとに、今年度の情報セキュリティインシデントに関する被害額の算出モデルの作成を検討する。

システムやネットワークに対する情報セキュリティインシデントに関する被害の構成要素には、損害賠償に要した費用、復旧などに要した人件費、ハードウエアなど物理的被害、イメージダウンによる被害、業務の停止による逸失利益など、様々な要素がある。

これらの様々なインシデント被害を２つに分類する。

まず、一つ目は、比較的算出が容易で一般的な「直接的な被害：逸失利益や費用発生モデル」「間接的な被害：補償・補填・損害賠償モデル」で構成される「表面化被害」とする。２つ目として、業務効率の低下などによる通常表面化しない「潜在化被害」とに分ける。

これら２つの被害の合計によって、インシデントによる被害額算出モデルを検討する。

なお、２００２年度モデルにいおて修正を行った箇所については、緑色で表示している。

5.1 表面化被害

インシデント被害の結果として生じる逸失利益や企業が実際に支払う金額については、企業が被害額として認識しやすい。被害が金額として認識できるものを、「表面化被害」と呼び、この表面化被害について、１次的なものと、２次的なものを考える。

5.1.1 直接被害額

電子商取引サイトなどのように業務、またはサービスの 100%がネットワークシステムに依存している場合には、インシデントによってシステム、またはネットワークの停止した期間を逸失利益の被害額として、比較的容易に算定できる。

この場合、インシデントによりシステムないしネットワークが停止していた期間の売上はゼロであり、当該期間に利益が挙げられなかったと見なす。

被害額は逸失利益の考え方により下記式により算出される。

逸失利益=時間あたりの売上による利益×システムないしネットワークの停止していた時間

「時間あたりの売上による利益」は、システムないしネットワークがインシデントにより停止していなければ得られていたであろう利益金額を設定する。電子商取引サイトの場合であれば、一日あたりの利益金額から算出することが考えられる。

また、直接的な被害としては、復旧に要したコストも算入する必要がある。電子商取引サイトが不正アクセスを受け、ウエブページの改ざんを受けた場合には、復旧するまでの期間の逸失利益と、復旧に要したコスト（ハードウエア、ソフトウエア、人件費）を下式のように加算し、直接的な被害で生じる被害額を算出する。

直接被害額=逸失利益+復旧に要したコスト+営業継続費用+喪失情報資産+機会損失

5.1.2 間接被害

業務またはサービスがインシデントにより停止したことにより、間接的に金銭的な被害が発生している場合には、その対価を被害額に計上する必要がある。

各種の補償・補填や損害賠償請求・謝罪広告費用などが挙げられる。被害額の算定は難しいが風評被害による利益の減少もこれにあたる。

間接被害=補償、補填、損害賠償など、間接的に生じた被害

5.2 潜在化被害

前述の表面化被害の算出モデルでは、いずれもインシデント被害が具体的な金額として表出するため、被害額を把握する事ができる。

これに対し、インシデントが対外的な業務やサービスに影響を明確な影響を及ぼさない場合には、潜在化してしまい、被害額が表出しにくい。このため、この部分のインシデント被害額についてはこれまであまり論じられることがなかった。

ここでは、これらの潜在化している被害を「潜在化被害」と捉え、被害額の算出モデルを考える。

5.2.1 潜在化被害額

インシデントによりシステムないしネットワークが停止した場合でも、業務遂行におけるシステム依存度が大きいほど、業務効率が大きく落ちる。

業務自身は、システムを使用しない業務フロー（発注業務の場合は、電話や FAX を利用する、等）に切り替えて業務を継続したり、システムの復旧後の残業などにより、処理能力低下をカバーし、金銭的な被害の発生を抑止している。

このケースの場合、業務自体はシステムを使用しないで継続してしまっているので金額的な被害は発生していない。しかし、業務効率がダウンしたり、システムの復旧後にデータを再投入したり、あるいは残業でリカバリーしたりなど、目に見えないコストが発生しているのである。

今回の調査で我々は、業務効率の低下自体もインシデントによる被害と考え算出する事を検討した。

また、このような「業務に関わる潜在化被害」に対し、企業イメージのダウン＝ランド価値の低下など「業務外の潜在化被害」も潜在化する被害の一つと考えられる。

しかし、企業イメージのダウンなどを金額に置き換えることは非常に難しく、業種業態、被害発生の理由などによっても、発露する影響が大きく異なる。

このため、「業務外の潜在化被害」は、今回のモデルの項目に組み込んでいるが、具体的な金額算出のモデル化については、ここでは特に言及しないこととする。

これらの議論を踏まえると、潜在化被害額は下式で算出できる。

潜在化被害額＝業務にかかわる潜在化被害＋業務外の潜在化被害
＝（固定費（人件費）×インシデントによる影響を受けた人数
×IT 感応度（業務依存度）×停止時間）
＋業務外の潜在化被害(ブランド価値の低下など)

5.3　インシデント被害額算出モデル

前述の議論をふまえ、下記のように「表面化被害」と「潜在化被害」を統合した「インシデント被害額算出モデル」を提案する。

インシデント被害額
＝表面化被害+潜在化被害
＝直接被害＋間接被害＋潜在化被害
＝逸失利益（直接的な被害）
+復旧に要したコスト（ハードウエア、ソフトウエア、工数）
+営業継続費用+喪失情報資産+機会損失
＋補償、補填、損害賠償など(間接的な被害)
＋（固定費（人件費）×インシデントによる影響を受けた人数
×IT 感応度（業務依存度）×停止時間）
＋業務外の潜在化被害(ブランド価値の低下など)

＜各項目補足＞

・固定費（人件費）

インシデントにより影響を受けた従業員の時間あたり人件費単価を設定する。

・インシデントにより影響を受けた人数

インシデントを受けたのがクライアント PC であれば、その台数を設定する。
インンシデントを受けたのがメールサーバやファイルサーバなどのサーバの場合には、そのサービスを利用している人数を設定する。

・IT 感応度（業務依存度）

インシデントを受けたシステムないしネットワークの業務に対する影響度を０～１の範囲で設定する。システムやネットワークへの業務依存度が高いほど、この係数は高くなる。業務に全くの影響を及ぼさなかった場合にはゼロを設定することになり、コストベースの損害は発生しなかったことになるが、通常は前述のように被害は実効効率の低下となって現れる。システムないし

ネットワークを利用した場合に１時間で１００件処理できたものが、利用しなかった時に８０件しか処理できなかった場合には、業務依存度は０．２となる。

また、システム停止時の代替え手段を充実させることで、万一の実行効率の低下を抑制することができる。実際の適用では、このような代替え手段も考慮して、業務依存度を決定する事が必要である。

なお、２００１年の調査・検証の結果、一般企業における実務上の参考値としては、「ＩＴ感応度０．２」を用いることで、幅広く対応できる可能性が大きい。

・停止時間

インシデントによりシステムないしネットワークが停止していた時間と、システムないしネットワークの復旧後に業務効率が通常レベルに戻るまでにかかった時間を設定する。復旧後にデータの再入力や残業を行ってリカバリーした場合には、そのリカバリー処置が完了するまでの間は、実効効率は IT 感応度で設定した実効効率が有効であると考える。

以上の４項目を掛け合わせたものに、業務外の潜在化被害額、ハードウエア・ソフトウエア・工数などの復旧に要したコストと、発生しているのであれば逸失利益（直接的な被害）と補償・補填・損害賠償（間接的な被害）を加えたものがインシデント被害額算出モデルとなる。

このモデルの特徴は、インシデントによる業務の実効効率の低下に着目している点にある。
インシデントによる金銭的な被害が具体的に発生していない場合でも潜在している被害額を算定することが可能である。

被害額を極小化するには、システムとネットワークを、被害を極小化できるように構成し配置すること（影響範囲の極小化）と、業務継続性の高い水準で維持すること（業務依存度の極小化）にある。

インシデント被害額の算定に対するこのアプローチは、企業の情報システムにリスク分析にも有効であろう。

6. 今後の課題

6.1 モデルの課題

今回、前年度のモデルに検討を加え、被害額算出方法についてのモデルのレベルアップを試みた。

検討の過程では、昨年モデルにおける言葉の定義や取り込むべき対象被害の確認や範囲の拡大が議論され、よりきめの細かいモデルにすることができた。

しかしながら、これらの対象被害の確認や範囲は、概念としては理解できるが、未熟な点が少なくない。モデルをより精緻なものとするため、今後克服すべき課題を検討する。

6.1.1 2002 年度情報セキュリティインシデント被害額算出モデルの課題

「5. 2002 年度情報セキュリティインシデント被害額算出モデルに関する検討」で、今年度の検討結果をもとに、新モデルを提示し、各項目について補足を記述した。今年度の検討においても、実際の算出業務を行う場合、現実に数値を算出しにくい項目が、まだ多い。

昨年から課題となっている「IT 感応度」については、今年度の見直しで十分な材料が無く、前回提案と特に大きな進歩を遂げることができなかった。今後は、企業毎に大きく異なるシステムの導入状況や業種などの情報で、ある程度数値化できる仕組みが本モデルの幅広い利用のために必要と考える。

6.1.2 情報セキュリティインシデント対策の標準モデルの課題

「4. 情報セキュリティインシデント対策の標準モデルと対策費用」にて、本年度「情報セキュリティインシデントが発生した企業のグループ」と「被害にあわなかった企業のグループ」について、実施されている対策全般について分析および標準的な対策モデルの提案を行った。

今回のアンケートから得られた情報によって、各種分析を行ったが、インシデントの発生企業が少ない点や発生後の対策実施などにより、表面的に大きな差は見られなかった。

事故の発生時期とアンケート時期のタイムラグにより、事故発生と対策の相関を掴むためには、対策の導入時期までも踏まえたものにする必要も考えられる。

予算については、必要性に応じた予算取りを行っているため、システム予算との区別が行いにくい状況が数多く見られたが、以前よりも具体的な数字を入れる企業が増えており、今後に期待したい。また、セキュリティ専門家からの費目提示が行えた場合には、企業担当者の意識形成において役立つ可能性は大きいと考える。

6.2 調査の課題

6.2.1 アンケートの課題

今回の調査では、昨年の冗長なアンケート項目を見直し、十分な議論を重ねてポイントを絞ったアンケートの作成を行った。

しかしながら、今年ののアンケートにおいても、まだ問題点や課題は残っており、内容について下記に示す。

- 被害状況の調査シートへの記載例などを記載し、これらの項目を記入していただいた回答者も見られたが、全体的には、担当者自身が未確認の項目が多く、ブランクとなっているものがほとんどであった。現実の企業や組織では、システム担当者周囲で発生した対応や被害しか掴めておらず、被害を金額化して回答を頂くことはまだまだ難しい状況である。
- アンケートを大幅修正したため、昨年回答との比較が非常に難しかった。今後はできる限り、本スタイルの内容でアンケートを行い、同じ項目について定点観測できるアンケート実施が好ましい。

6.2.2 ヒアリングの課題

今回のヒアリング調査先は、昨年と同じくアンケート回答した JNSA 加入企業、および調査に同意していただいた少数の企業や組織に限られている。継続的にご協力いただいた企業も多く、ヒアリング調査に対しては、全般的に協力的であった。

ヒアリング調査に関する問題点や課題を下記に示す。

- 昨年と同じく、セキュリティに関わる部分であり、調査先はワーキンググループメンバーの属人的な繋がりで調査に同意いただいた企業や組織に限られた。
- 昨年協力を頂いた先においても、今年度調査を断られる企業もまれにみられた。セキュリティ管理が強化されると共に、このような調査を行いにくい側面があると考える。
- ワーキングメンバー２名１組で調査を行ったが、何分人手と時間が少なく、十分なヒアリングスケジュールの日程調整が難しかった。

7. 最後に

前年に続き、JNSA 会員を中心に主要企業をある程度含んだ形で、情報システムのインシデントに関する調査や検討を行い、今回は公表された情報漏洩事故にも検討の対象を広げて議論した。今年もインターネット関係の被害調査や脆弱性に関する調査は、日本でも多く実行され、情報処理振興協会(IPA)や警察庁など、アンケートの着眼点も被害額の把握が取り入れられている。

しかしながら、調査先からの被害金額の聴き取りは、被害範囲の定義やその把握方法が定型化されていないため、まだまだ調査先の担当者の直感に頼る部分が多い。

NPO 日本ネットワークセキュリティ協会(JNSA)では、このような現状を鑑み、昨年に引き続いて、JNSA のセキュリティワーキンググループの作業により、JNSA 会員企業を中心に日本の基幹産業を調査対象被害額や対策費用を含んだ調査を行った。

この調査の目的は、情報セキュリティインシデントに関する現状を把握し、情報セキュリティ分野におけるリスクマネジメントにおける非常に重要な基礎的な情報を収集することである。

JNSA の調査は、アンケート調査だけではなく直接ヒアリングも行い精度の高い結果を得るとともに、被害額を推計するモデルの構築や、対策の有無による被害発生の差の把握を目標とした。

調査にあたっては、アンケート内容を大幅に見直すなどの工夫を行ったが、アンケート、ヒアリングともに、回答できない企業もまだまだ多いのが現状であった。

アンケートやヒアリングに関しては、継続実施の企業も多く協力的な反応が多く、この場をお借りしてお礼を申し上げたい。

ご協力を得られなかった企業では、ポリシー等の対策を理由に挙げる企業が少なくない。セキュリティポリシーと相反する調査協力をについては、調査活動の上でどの様に対応するのかが、今後大きな課題となる。

一方、今回の調査では、第２部(別冊)において、今後の議論の題材とするため、公表された情報漏洩事故について検討を加え、賠償による被害額の想定や企業価値の一端を示す株価への影響について、本ワーキンググループとして数値を示した。ごく少数での討議・検討の結果であり、法律問題など我々の専門分野以外の要素が多く、弁護士を交えて議論をしたが、現時点ではまだ精緻な数値でないことは否めない。

しかしながら、これらの被害の数値算出および算出課程を明示したことで、専門家を巻き込んだ今後の議論の題材なる可能性を示すことができた。各異分野専門家の共通の話題として取り上げられ、情報システムのリスクアセスメントで必要な「リスク量の把握」における把握モデルの構築が前進し、安全な情報化社会の形成に役立つことを期待したい。

最後に今回のチャレンジは、年度末などの多忙期にプロジェクトメンバーに各種作業を要求するとと

もに、ヒアリングにご協力いただいた企業の方々にも、多くの率直なご意見をいただき、大変感謝している。本報告書およびワーキンググループの活動は、継続的に勧めることに大きな意義があり、定期的かつ繰り返して実施していく。合理的な対策実施へのニーズが高まる中、今回の結果を踏まえ更に実情にあった情報を提供できるように努力してゆきたい。

8. 参考資料

8.1 ヒアリング集約

ヒアリング調査を行った調査先において聴取した内容について、アンケート項目別に簡単にまとめています。

PC台数などシステム状況について(アンケートB-1関連)
・クライアント150台、サーバ（メール2台、Web1台、ファイル1台） ・開発用のサーバが10台程度
約900台
内部サーバ（DNS、SMTPなど）5～6台、ファイルサーバ30～50台
・クライアント約5,000台、サーバは数百台。 ・管理はQNDを使用している。
700台弱(1人1台制、常駐先PC除く)
1500台(1人1台制)、部門サーバ80台
約8000台（オンライン、オフライン計）、業務サーバ数台、その他部門サーバ400台
・クライアント約800台(1人1台以上、ノートPC比率約30%)、サーバ台数約80台（Unix20台）
3000台。管理職一人一台、事務職はグループ利用
・PC900台（一人一台）、サーバ20台（社内メール用、業務用） ・基幹系ホストは除く。
PC約3,500台、社内サーバ約300台、他外向けWEBサーバ
30000台以上(社員、派遣・SEは一人一台以上)
メール用＆業務用端末で一人1.5台程度、ファイルサーバ8台、その他Webサーバ 3台、メール 1台、財務会計用サーバ 1台。

メール利用状況について(アンケートB-2関連)
添付ファイルのサイズ制限 ウイルスチェック をおこなっている 社外のメールアカウントの禁止は現在おこなっていない
・添付ファイルの容量制限10MB ・グループ全体のフィルタリングの詳細はわからない（たぶん親会社がやっていると思う）
・容量制限をかけている。（MAX2MB） ・メールアドレス名は、入社時に会社側で決めている。 メーラーはNotesを使用、OEを使っている場合もある。
サイズに制限あり。過去に大きなファイル（プログラム）の送受信があり大きな影響を受けたため。 メールサーバは自社に設置。Linux sendmail使用。 POPは外部からも利用可能。暗号化はしていない。A-POPなどセキュリティの適用も検討しているが、各人のメーラーが統一されておらず設定変更が困難。
・メールはMax3MBの容量制限をかけている ・e-メール利用は、ほぼ全員に近い（希望者のみ）
独自仕様のWebメール（IMAP）を7,000人が使用。 サーバは千葉センター 1箇所に設置。

・メールの制限は添付ファイルにexeファイルは不可 ・メールフォルダー50MBに制限（一人） ・メールアドレスは一人ひとつだが、「業務」で共有アドレスあり ・メールアドレス名で女性とわからないようにしている
特に制限なく利用。インタネットメールは登録制で２０００ID、Ｗｅｂはフィルタリングソフト利用
利用可能だが添付ファイルに制限あり（500KBを目安だがシステム的に制限をかけていない。） 利用メール（サーバ、クライアントともにノーツのみ利用、社員の70%程度メール使用）
特に制限なく利用（添付2～3MBとしているがシステム的には制限していない。） ・PC配布は情シで行っているため、Outlookといったメールソフトは使用していない。 ・グループウェア（ノーツ利用） ・メールは、キーワードチェックを行っている。
利用可能だが添付ﾌｧｲﾙに制限有り Microsoft Exchange Serverを利用。(Outlookベースのメールシステム) POP3、IMAPも利用可能。社員1人1メールアドレス。派遣・SESは、要申請。
1フロアに1台専用端末があり、それを利用。庁内LANとは接続していない。各端末ごとに共有のメールアドレスがある。メールが届いたことは気が付いた人が受信者に通知。添付ファイルは、FD経由で持ち出す。

Web閲覧の利用状況について(アンケートB-3関連)
特に制限をかけていないが、ルールとしてはギャンブル、株などは禁止している
フィルタリングツールを検討中。掲示板への書き込み、Web経由ウイルス感染防止、セキュリティ監査ワーキンググループで制限を年1回改訂
Web閲覧はプロキシサーバ経由で制限
・URLフィルタリングを実施。（規制は割合緩い）
特に制限なし。開発業務に支障がありポート制限無し。 Proxy未使用。NAT利用。 ファイアウォールでアクセスログ収集。半年～1年はHDに保存(その後CD-ROM保存) ログ解析の頻度は多くない。Nimda、CodeRed、Slammerなどが拡大した際には意識して確認している。
・Webフィルタリングを利用。（アダルト、ドラッグ、出会い系サイトなど、警告実施は１０回以下）
専用端末のみ利用可。利用可能ＰＣは全社で約450台。
・Web閲覧にはコンテンツフィルターを使用(フィルタ内容は、ｱﾀﾞﾙﾄ、ｷﾞｬﾝﾌﾞﾙ、株取引などで社内公開) ・違反はあるが、故意性は低く、たまたま見てしまったケースが多い状況。 ・四半期一回の会議で、要注意人物をﾋﾟｯｸｱｯﾌﾟしている。(ﾌｨﾙﾀｰの運用ノウハウとしても、本業に活用)
基本的に利用可能だが閲覧先の制限あり。切符購入などは行えるが、買い物サイトは人事のみ利用可。
特に制限なく利用可能（WEB利用の申請制度有り）
特に制限なく利用可能。（ガイドラインとして、業務以外のサイト閲覧を禁止）
利用可能だが閲覧先制限有り。 接続時に認証パスワードが必要。 URLフィルタによる制限。有害サイト(犯罪教唆)や攻撃サイト(Nimda等のブラウザの脆弱性を狙うもの)に配慮している。

メール端末によるWeb閲覧。フィルタ制限は未設定。

メールおよびWeb閲覧利用か可能なPCの割合(アンケートB-4関連)
メール100%・Web閲覧100%
メール： 82.5%（7000台/8000台） Web： 5.7%（450台/8000台）
メール80%、Web閲覧50%
メール　90% Web閲覧　30～40%
ﾒｰﾙ　90% Web閲覧　90%
ﾒｰﾙ50%、Web閲覧50%
メール　5%、Web 5%

情報セキュリティに関する規定について(アンケートC-1関連)
・96年に情報セキュリティポリシーを作成。 ・ポリシー違反者に対する処罰規定は有り。
・コンサルティング会社による監査＆作成 ・メンテナンスは毎年実施 ・年1回社内全体の方針にもとづいているかポリシー運用状況を確認 ・構成は、前半：一般編　後半：管理者編
・3年前の2000年頃前にセキュリティポリシーを策定。 ・ヒアリングなどに基づき、年に1回メンテナンスを実施。 ・外部へのポリシー公開は未実施（理由は特にないが、公開要求も特にないため） ・違反の罰則は服務規程で定義。
過去一度、全社向け説明。 新入社員には入社時の説明と同意書の取り付け有り。 ポリシー上の罰則はなく、社則に準拠して運用。
・セキュリティポリシー改定は未実施。 ・ポリシー見直しで、提出文書のログが未取得だったことが判明した。（文書管理規定と電子データ管理規定の不一致があった。） ・違反者の処罰規定は特にない
・1999年にﾎﾟﾘｼｰ的なものを作成したが、全社には広まらず、改めて2000年度にポリシーを策定(全社に広めた、分量は60ページ程度）。 ・関連会社であるが、システム開発業務などがあり、親会社と別ポリシーで制定。 ・事故発生や損害の予見時に、ポリシーを見直し適時実施だが、2001年に大きな見直し実施。 ・ポリシーは社外公開のみ。 ・罰則は、就業規則の規定を使用している（過去一度オークションサイト利用者に適用有り） ・セキュリティポリシーは、有益と感じている。(会社のセキュリティに対する方向性が明確できた。文書・メールの取り扱い手順が明確になった。開発業務にも反映し本業にも好影響あり)
情報セキュリティポリシーを規定(リスク管理部が制定)。電子媒体については情報システム部。罰則は「場合がある」という表記にとどまり、人事諸規定との連動は特にない。
その他規定の一部として情報セキュリティを規定している。（社内規定の一部として）
セキュリティポリシー作成中。情報システムで仮運用中。

･セキュリティポリシー策定を始めたころには、国内で他にポリシー策定しているところがなく、逆に周囲を気にする必要が無かったため、苦労は少なかった。 ･ メンテナンスは年1回実施。 ･ ポリシーの外部公開はしていない。 ･ ポリシー違反者については、社員就業規則をふまえて、処罰を行う規程がある。 ･ ポリシー策定や認証取得の効果については、社員のセキュリティ意識の向上やビジネス上有益な点が上げられる。
外部のコンサルタントの協力により、ポリシー策定予定(2003年度)。 重要な個人情報へのアクセスにはID毎に権限を付与。ネットワークへのログインIDのログ管理は、課の単位で実施。(課単位のIDなので個人レベルのログは取得できない) 入退室管理は既に規定として明文化。(マシンルームへの入室時の記録や外部来訪者の入退室記録など) ホストに関するシステム障害対応手順については明文化。ルータやHUBなどネットワーク機器については経験的に対処。ベンダー連絡含む連絡体制は整理されている。

情報セキュリティ管理の体制について(アンケートC-3関連)
IT系10名　総務系10名　マネージャー以上
選任担当者のセキュリティ業務の業務割合は、全業務の80～90%。各部門にセキュリティ管理者を設置(部門長)しているが、セキュリティ業務の業務割合は10未満。
合計4名。担当部門は総務の業務関連部署。 ネットワーク担当が兼務なので主な業務はネットワークのメンテナンス。 セキュリティ関連では、MSのパッチ情報の告知、アカウント管理、SNMP監視などを実施。
･兼任者のセキュリティ業務の割合は4時間/月程度。 ･各部門のセキュリティ担当者は、部門長が行っている。(役割としては、情報資産の機密レベルの指定など)
兼任　8人(社員2名、ベンダー6名)
･各部門のセキュリティ担当は部門長が兼務。 ･セキュリティ兼任担当者の業務としては、1人が全体の40%、2人が全体の20%程度の割合である。
1名(情報システムの副部長クラス)
兼任担当者　2名(業務割合は全体の20%未満) システム担当者　70名(業務割合は全体の5%未満)
兼任担当者　2名(業務割合は全体の約10%)
･ 兼任者のセキュリティにおける業務割合は20%
月1回ファイアウォールのログチェックを実施(外部のベンダーの保守範囲で実施) アンチウイルスのパターンファイル更新は、夜間自動実施。ネットワーク監視は始業時に記録確認。

事故や事件が発生した場合の社内連絡体制について(アンケートC-4関連)
事故に対しては、緊急対応チームを設置
･コンテンジェンシープランを策定済み。 ･訓練も実施。 ･セキュリティ事故DBを作成し、事故記録を保管している。
責任部門は総務部門の業務担当。ただし、緊急対応の手順の規定は無い。

・社内の連絡体制について、年一回訓練を実施し、実効性を確認している。（土曜日夜間に、サイバーテロが発生した場合を想定し、実際に連絡を行う）
ヘルプデスクの常駐ベンダで対応する。
・事故や事件が発生した場合は技術グループが担当する。 ・試行的な体制であったが、事故の経験を重ね近年は機能するようになってきた。
連絡体制規定、セキュリティ事故の把握責任部門設置、従業員への連絡体制周知などを実施。(但し、各部門の連絡担当員は無い)
危機管理を去年設置し、連絡体制規定、事故発生の責任部門、各部門の連絡担当者、従業員への連絡体制の周知を行っている。
連絡体制規定、事故発生の責任部門を制定している。基本的に情報システム部門に連絡。
トップダウン方向の連絡体制は機能しているが、ボトムアップ方向の連絡体制には不十分な面がある。先日のSlammer発生時の発生調査依頼の時は、1日以内にほぼ全社から報告があり、指示・報告の伝達時間がだいぶ早くなってきている。
情報部門が責任部署となっており、各課長クラスが現場のセキュリティ責任者。 今まで、システムがストップしても通常1時間程度で復旧、最悪でも半日以内で復旧している。おおよそ1年間に2～3回ホストやネットワークに障害が発生するが、連絡体制は上手く運用できていると考えている。

取引先の選定や契約時に配慮している点について(アンケートC-5関連)
外注先との守秘義務契約書はある場合と無い場合がある
取引先の経営＆サービスを重視し、守秘義務契約書やサービスレベル(ＳＬＡ)を規定した契約書や覚書を締結している。
営業レベルで確認（与信）。 逆に取引先から求められることもある。プライバシーマーク取得準備中。
セキュリティの観点ではないが取引先の信用調査を実施。
＜依頼先選定の配慮点とポイント＞ ・経営状況やサービスレベルの分かる取引先を重視取引先については、過去取引や帝国データバンクなどを活用している。 ・守秘義務契約やサービスレベル(ＳＬＡ)については、基本契約に入れている。 ＜顧客から要求される事項＞ ・ポリシー作成、守秘義務契約やサービスレベル(ＳＬＡ)、親会社からの監査などがある。
守秘義務契約を締結。法務部がチェックする。
守秘義務契約書を締結している。
守秘義務契約書を締結している。
顧客から要求があれば取引先にも対応を求める。それ以外の場合はコストパフォーマンスを重視。 認証を取得しているような取引先は現実問題として少ない。
サービスの購入は提案コンペで決定することが多い。 データ入力の委託先には年1回の監査を実施し、バックアップテープを保管している倉庫を年に数回査察している。

派遣社員や常駐作業員受入時の配慮点について(アンケートC-6関連)
機密保持契約、セキィリティー教育の実施は行っている。内容については、イントラネットで常時公開している。 機密漏洩等、紙のドキュメントの取り扱いにランク付けをしているが、数が多く一覧表を見ないで回答するのは難しい。
・派遣社員などの教育も社員と同等に行っている ・グループ会社に派遣会社があり、ある程度信用している
セキュリティ教育は、配属部門で実施している。教育内容は、社員と違い業務内容に関連した内容だけである。
契約時に誓約書に一筆もらう。主に利用規定（インターネット利用、社内LAN利用など）。
・派遣社員のセキュリティ教育は、社員と同一レベルで実施している ・派遣社員のNDAは部門の裁量によるが、個人レベルで取っている部門もある
千葉センターは社員カードに入室可能エリアが登録され、入室制限がされている。
・派遣社員などのNDAは会社対会社で取っている(受け入れ先の部門管理) ・正社員よりは少ないが、現場ベースでｼｽﾃﾑ&ｾｷｭﾘﾃｨ教育は行っている。
契約を締結。賠償額は年間の委託料が上限。
派遣契約は特に行っていないので、教育も特に不要。(機密保持程度)
派遣社員では特に意識していない。機密保持程度
派遣には情報セキュリティ教育を実施している。 教育は派遣元に依頼する。
業務委託をしている場合はNDAを取っている。 個人情報保護に関しては、年に一度教育を実施している。

被害が発生した時の対応計画の対象について(アンケートC-7関連)
発生から、復旧までをおおよそ全て規定。 今まで大きな事故はないが、社外からの問い合わせは個別にくる
特に決めていない。 発生時には一般に総務部門の業務へ連絡が入り、カバーできない場合は協力を仰ぐ。 ウイルス検知時にはIPAへ報告している。
・危機管理マニュアルを作成している
定めていない。都度ベンダーが対策を提案する。
・不正アクセス、ウイルス、その他(紛失)などの連絡票を使っている
第三者への情報開示方法は定めていない。それ以外はすべて実施。
・ウイルスを社外に送付した場合。 ・ホストPCが停止した場合。
特に明文化していない。
被害報告は求めるが、細かな確認事項までは定めていない。 IPA等への報告は行う。

情報セキュリティ関連ニュース等の収集について(アンケートC-8関連)
情報収集先は、ベンダーなど無料の情報が多い。
・セキュリティ事業の提携先からセキュリティ情報提供サービスを受けている。 しかし、社内にその情報を提供しても、各部門のセキュリティ責任担当者全員が理解できるとは思えない。
セキュリティ関連の情報は、CERT、MSのセキュリティ情報などを収集している
有償のサービスを受けている。パッチの検証なども書いてあるので判りやすい。
情報提供サービスは無料サービスを利用。 大半はＯＳなどのバグ関連なので、サイトのパッチで対応。 Linux関連は情報提供サービスから情報を収集している。
ベンダーHPから毎日情報収集している。SunやORACLEが中心。Windows系はあまり熱心に行っていない。
・情報セキュリティ関連の有料情報は利用していない ・情報の不足はないが、内容が多く自社で適用すべき情報であるか選別するのが大変である
メーリングサービスを利用あり。ファイアーウォール購入時のサービスを受けている。
ＩＰＡなどのサイトで収集し、今のレベルで対応できていると思う。
ベンダーによるメール配信サービスを受けている。
セキュリティサービスの情報提供を受けているが、提供までの時間が遅く、独自収集の情報と内容的に大きな違いがない。
業務委託しているSEが、セキュリティ関連情報を見ている程度。（ネットワーク系3名、ホスト系2名）

各種パッチの適用状況について(アンケートC-9関連)
パッチ情報がでても、停止できないサーバもあり、各サーバの管理者の裁量に任せるしかない。 管理者の対処のレベルが把握できないクライアントで、知らない内にサーバ機能が動いている場合があり、クライアントPCを含めた資産管理を徹底しないといけないと感じている。 資産管理のシステム構築・運用（利用・更新）が非常に難しい。
・セキュリティパッチに関しては、パッチを当てるのに不安要素がある場合は連絡を貰う。(ベンダーから？) ・特にデータベース系のサーバは、パッチをあてることが厳しい場合がある
社内のネットワークに接続していない各部門のサーバは、各部門で管理している。顧客環境に併せている場合もあるので、常に最新にできない部分もある。
ファイアウォールに対するパッチは保守契約の範囲で提供を受けている。 ソフトを販売する関係で、パッチは各種OSで試し、結果をユーザへアナウンスしている。 Internet公開サーバはLinuxベースで20台弱ある。 社内サーバはWindowsベースで常用は約50台。その他開発用の一時的なサーバがあるため、全適用は難しい。 業務用サーバのパッチは各部門で対応し、パッチ情報のアナウンスは総務部門の業務から行っている。
メールサーバについては必要に応じて適時行っている。 本番機と検証機に分けて、パッチ検証を実施後、本番機に入れている。
・基幹システムには、自動的にパッチをあてる方式を構築中（MS系） ・開発系サーバ、ＤＢ系、ﾃﾞｨﾍﾟﾝﾄﾞしているＰＣのセキュリティ確保が難題と考えている。 ・テスト環境はあるが、時間的な余裕が少なく、活用は限定的となっている。

メーカーの維持保守サービスを受けている。マイクロソフト関連は重要度で選別し、それ以外は1ヶ月に一回。対象はサーバーのみとなっている。
最低限必要なパッチ以外は当てていない。 また、DMZネット内サーバ等は、アウトソーシングしているため、対応の詳細は不明。
外部向けのサーバには積極的にパッチを当てているが、残念ながら、内部サーバについては手つかずの状態。 パッチの収集は、アウトソーシングしている関係子会社に任せている。
セキュリティ委員会の管理しているサーバ類は常に最新に保っている。 それ以外は、各部門ごとに、定期的にパッチのリリース状況を確認し、責任者の了承を得て、ｻｰﾊﾞ管理者がパッチを適用している。 保守は、主に社内(社員、SES等が実施)で実施している。 実施のについては、基本的に各事業部の裁量に任せており、セキュリティ委員会が危険度の高いセキュリティホール等を発見した場合は、各部門へ対策指示を行う。1～2日後には、対策を終了させる体制となっている。 外部接続点や最上位のWeb Serverなど、セキュリティ委員会の管理しているサーバ類は、検証用のサーバでパッチ等の検証を行った後、パッチ当てを実施している。(パッチによってシステムトラブルを生じることもあるため)
委託先のベンダーの提案によって、各種パッチを適用している。

認証の取得や計画について(アンケートC-10関連)
・セキュリティ認証取得は部門レベルで必要な規定を取得している。 ・ISMSはセキュリティ関連の事業部門、プライバシーマークは広報部門で計画中。
プライバシーマークを取得する方向で準備中。 CMMは開発部門から人員を出して推進中（取締役をトップにし、支店担当も集まり半月毎に会議を実施）
・ISMSなどの認証は、良い面があるが「まず文書管理ありき」となっている様に感じる。セキュリティー技術とのバランスが悪いように思われる。 ・Pマークは個人情報保護のために必要かもしれない(親会社ﾃﾞｰﾀの取り扱いでの情報漏洩が心配)
特に計画なし。関連会社でプライバシーマークを取得済み
今のところ、すべて計画無し。
今のところ、すべて計画なし。
各種取得を他社との差別化や業務上の必要性、マーケットニーズなどで取得した。 取得資格には、初のものがあり差別化の効果が大いにあった。

直近1年のシステム監査、脆弱性検査の実施について(アンケートC-11関連)
インターネットのシステム監査、脆弱性検査については、毎年定期的に実施し、重点テーマを委員会で決定している(今年テーマは資産管理)
システム監査は年に一回実施し、脆弱性検査は不定期。(外部依頼)
設定変更時（バージョンアップ、パッチ適用など）に実施している。 脆弱性検査については、ダイヤルアップで外部からポートスキャンし、LAN側からファイアウォールのログを確認する方法で行っている。
・脆弱性検査は外部を使い3回実施（毎回違う会社を選定した）
ログの確認により、毎朝不正アクセスの点検を実施。

・社内の技術者によるペネトレーションテストを実施。 ・システム監査は社内＆親会社で、インターネット&イントラで実施した。
インターネットと社内専用ネットワークについてシステム監査実施。脆弱性検査については、アタック検知運用会社による年2回のチェックを実施。システム改訂時にセキュリティホールがあることを発見した。
未実施。これから考えていきたい。
インターネット、イントラネットともに、ヒアリングレベルでの診断は受けたことがある。 また、ネットワークベースのスキャナを利用した定期検査は実施している。
基本的に社内で実施。 インターネットの脆弱性検査は、外部1社に委託。 社内専用NW・システム(セキュリティ)監査は、社内および外部1社に委託。 調査会社選定理由としては、技術・信用・コストのバランス。 但し、脆弱性検査においては、コストよりも技術・信用を重要視。
・システム監査は来年度実施。詳しい担当が不在のため、運用に問題がないかどうか確認のために実施。 ・セキュリティポリシー策定。 ・主要業務ネットの範囲でペネトレーションテスト実施。

情報セキュリティ関連予算について(アンケートC-12関連)
セキュリティ予算については、部門ごとに管理しているのでわからない。
情報システム関連予算の一部として計上されている。
システム関連予算に含まれる。
・セキュリティ関連として、毎年必要に応じ予算化している。
運用委託先ベンダーへの保守費として計上している。
・セキュリティに関連する経費についての満足度は65～70%程度
システム関連予算の一部として計上している。
情報システム関連予算の一部として計上。ファイアウォール、ウイルス（ゲートウェイ、クライアント）。
クライアント用ウイルスソフトなどを予算化。WEBフィルタリングは検討中。
セキュリティマネージメントシステムの維持、関連システムの開発、ウイルス関連ソフトの購入、教育・啓蒙など、主にソフト方面へ支出している。 FWなどのハードウェア関係は、情報システム関連予算に含まれている。(ただし、情報システム関連予算の中のセキュリティ関連費として管理している部分もあり、通常のネットワーク設備費と分類が難しいものもある) 十分な情報セキュリティ対策費が取れている。ただし設備系の費用は現状厳しい。 ・経費についての満足度合いは、全体として70%程度と考えている。
金額回答したものは、ウイルスパターンファイル更新などセキュリティ関連と明確なもののみの費用で、監査費用などは含んでいない。

現行セキュリティ予算の金額やシステム予算に対する割合などについて(アンケートC-13関連)
・ライセンス更新料としては、スキャンやウイルス関連で年間更新料等200万円程度計上。 ・FWについては、今後外部保守を検討している。
予算の大枠はあるが、セキュリティ関連に関しては必要に応じて予算を要求している。
特に区分けがない。
5,000万円を挙げているが、運用委託先ベンダー　6名分の委託費。

詳細は不明
予算は400万円でシステム全体に対する割合は約3%
予算は40億円で、予算に対する割合は2.5%
システム予算に対する予算の割合は8～10%前後
セキュリティ対策については、現在上層部の理解があり、予算は取りやすい。

情報セキュリティ関連予算の対象について(アンケートC-14関連)
ライセンスの更新は毎年 今年導入する製品
ファイアウォールの保守費などは明確。アンチウイルスのライセンスなども年間予算で計上。 ハードウェアにかかる費用は主にPCのパワーアップ。
ベリサインへの証明書継続費用など。
ハード、ソフトの購入費、保守費である。IDSサービス導入をしている。教育予算がないのに気づいている。
各部門毎に認証取得している場合は、各部門の予算内に含まれる。 (全社的な取得認証はない)
ウイルスパターンファイル更新

情報セキュリティを確保するための導入システムについて(アンケートC-15関連)
ファイアウォール、DMZセグメントの設置、メールサーバでのウイルスチェック、全ｸﾗｲｱﾝﾄPCにウイルスﾁｪｯｸｿﾌﾄを導入などを実施済み。 Linix,Solarisなどにおけるセキュリティ確保するシステムは知識が少なく不安を感じる。
アンチウイルスを導入済み。システムのアップグレードレベルは月1回CD-ROMで入手。定義ファイルは毎日更新し、ドメインサーバへ登録し、ログイン時に各ユーザへ配布している。 サーバは毎夜自動スキャンし、ウイルス検知で管理者にアラーム通知される。 自宅でもウイルスチェックを義務付け、評価版でも良いから実装するように勧めている。さらに年末などは注意を呼びかけるメールを送信。
・暗号化について、一部SSLを使用している
・ユーザ向けホームページでSSLの使用を行っている。
・暗号化は計画中である ・IDSの手前レベルとして、パケットは見ている。
暗号化以外すべて導入済みで、暗号も検討中であるが問題はコスト。
ファイアウォール、DMZセグメントの設置、メールサーバでのウイルスチェック、全ｸﾗｲｱﾝﾄPCへのウイルスﾁｪｯｸｿﾌﾄは導入済み。 外部との接続は、RAS、国際フレームリレーを利用している。
ファイアウォール、侵入検知システム（IDS）、DMZセグメントの設置、メールサーバでのウイルスチェックを導入済み。 全ｸﾗｲｱﾝﾄPCやProxyｻｰﾊﾞｰ側のウイルスﾁｪｯｸｿﾌﾄは一部を除き、導入済み。
Web Trafficに対するパターンフィルタは実施可能
ファイヤーウォールは、セグメントごとに導入(他ネットとの切り分け) 各端末のウイルスファイル更新は、夜間に自動電源オンによる自動更新) 個人情報を扱う端末については暗号済み。

情報漏洩を防止するために行っている対策について(アンケートC-16関連)
対策実施の内容、状況ノートＰＣ（OA機器）の持ち込み制限は、チェックすることはほぼ不可能。(入館時にノートPCを起動させるわけにもいかない。)
無線LANも使用しているが、ESSID、WEP、電波の漏洩などに注意するようにしている。
ルータのトラフィック監視を実施。(以前3Dオンラインゲームで帯域を圧迫された経験がある) 特に外に出て行くトラフィックを見ることで、プログラムの流出などを検知。(派遣社員が自宅で作業するために持ち出すことがあるため)
・個人認証は現在はIDとパスワードだが、来年度はICカードを導入する予定である
・行政からの指示でメールの保存を実施。 ・情報資産（紙・データ）は厳密に管理。 ・各部署にセキュリティ担当を設置。毎月ランダムに部署を決めサンプル的に監査を実施。
・ノートPCのネット接続は禁止(業者の持ち込みはチェックについては詳細不明)
書類、ＰＣの持ち込み持ち出しは規定により禁止、サーバールームへの立ち入りはIDカード、ＦＤなどの持ち出し破棄は規定上の禁止事項、メール監視は検討中、ＷＥＢメールは２００３年度から全面禁止。
部門の共有サーバは、各フロアで設置管理
書類、ノートＰＣ、ＦＤなどの記録媒体の持ち出し制限は、社内規定にあるが、現実は守られていない。
・書類の持ち出し制限については、明文化はされていない。 ・ノートPCの持込制限については、運用規定の中の「私物の持ち込み制限」を適用。 ・FD等持ち出し制限については、PCのドライブに制限をかけることで実施。(ただし、チェック機能は無し) ・記憶媒体の廃棄については、PC廃棄時にハードディスククラッシャーで処理。 ・PCの廃棄は、年度末に一括廃棄処分（ハードディスククラッシャー使用）。リース品はディスク消去ツールで内容を削除。 ・入退室はキー入力で制限。

情報セキュリティ教育の内容について(アンケートC-17関連)
・教育は、社内のイントラWebを使っている ・入社時にセキュリティ教育をしている
中途採用者にも教育実施が望まれるが、IT部門、営業部門などの部門でバラツキが大きい。 人事部門・担当者で説明することは難しい。
入社時に教育し、社内にe-ラーニングの仕組みがあり利用している。
ウイルス対策については、対処法をメールで提供。(情報提供がメイン) 緊急対応については、ヘルプを求められた都度指導している。 PC運用は、新規購入時の設定マニュアルを共有フォルダで公開し、設定は各ユーザに任せている。
セキュリティに特化したものではなく、システム教育の一環として実施している。
・緊急時用の訓練はしていない ・緊急時対応の教育としては、連絡ルートの周知等がある。 ・ネチケットやソーシャルエンジニアリング教育を課題と考えている。(とくに事務、営業)
全国規模の教育は９９年に実施。その後はできていない。情報に関する社内資格を導入し、出先については有資格者が教育することとなっている。
情報セキュリティの専門教育は行っていない。セキュリティポリシーができた段階で考えたい。

担当としては、機密保持を重要視している。 アクセスコントロールやスクリーンロックなどセキュリティに関する設定・運用の教育は行っている。 (一般的な設定技術などの教育は対象外。)
個人情報管理についての教育は採用時に実施。 情報システム課内でも実施。

直近1年間のセキュリティ教育の実施状況について(アンケートC-18関連)
一般向け500名、管理職向け100名の規模で、年一回定期的に行っている。 社内のセキュリティ教育ツールで学習し、合格後　メールアカウント発行する。 当初は、出版系のe-Learningを使用したが、技術者向けであるため、一般職員には不適切な内容であった。この経験を踏まえ、社内で作成し、4～5日くらいかけて新しい内容で再実習をおこなう予定。
セキュリティ教育をグループ全体で行っている（30分程度）
新入社員教育の一環で実施。 各種フォロー教育の一環で実施。 カリキュラムは人事が作成し、実施は総務部部門の業務が担当している。
・教育は集合教育で年に1時間程度行っている(欠席者は上位職から説明) ・理解度については、セルフチェックできる仕組みがある（WBTの仕組み） ・マネージャには4半期ごとにセキュリティに関する委員会で報告をしている(2～2.5時間程度)
システム管理者70名について、年1回実施。
専門家向け教育を年一回20名程度で実施。
e-ラーニングを実施。新入社員・中途採用社員には集合研修とe-ラーニング。 教育は、100%実施が難しい。休職者や出向者など。(休職者は、業務に携わっていないため不要) 出向者の受講は可能だが、出向先管理下となるため、出先の教育方針に任せている。
情報関連部署で年一回年度の始めに実施。

現在実施または今後実施を考えている情報セキュリティ関連対策について(アンケートC-19関連)
セキュリティ委員は、部門長、サーバ管理者で構成され、そこから全従業員へのセキュリティ情報の提供が行われている。 各々の理解度は不明である。 社外への連絡体制、フローは、今後の要検討課題。
・認証取得では、個別フローの文書化が実務として負荷が大きい。
情報システム部門員と協力会社について、月１－２回集合教育で最新情報を教育している。今後は一般社員の教育を実施したい。
今後の課題としては、情報セキュリティを考慮した社内制度の制定、情報システム部員のセキュリティ教育強化、事故・事件対応訓練、情報ｾｷｭﾘﾃｨのｽｷﾙを有する人材の採用などが挙げられる。
今後の課題としては、セキュリティ関連文書の整理、情報セキュリティを考慮した社内制度の制定、情報システム部員のセキュリティ教育強化、一般従業員のセキュリティ教育強化、システム監査の実施、全従業員へのセキュリティ情報の提供、クライアントでのウイルスチェックなど、多岐に渡る。
・セキュリティ監査を今後実施したい。 ・セキュリティ関連の認証取得は、マーケットニーズによって実施する可能性がある。 ・IDCは信頼しきれない。
各対策については、ポリシー策定の際に検討の予定。

貴社業務のIT化進捗、システム依存度について(アンケートC-20関連)
・システム依存の割合は把握していない
・ホストシステムと情報系システム（メールなど）は分離しているので、仮にインターネット接続が止まっても業務が停止するということは無いと考える。
日常業務の利用としては、交通費精算など。 承認印をもらう関係で紙での運用は減らせない。電子認証は、まだ抵抗があり教育が難しい
多くの業務がコンピュータ化されている。
ほとんどの業務がコンピュータ化されている。
多くの業務がコンピュータ化されている。(人事、経理系はほぼ全て) CRM（顧客対応）はあまりされていない。
金融のように中心となる基幹業務がないため、単純にコンピュータ化の度合いを推定することは難しい。 企画、提案、設計などが主業務であり、コンピュータはそれを作成する手段でしかない。 コンピュータ化・NW化された業務としては、人事・財務があるが主業務ではない。 提案書、設計書などの書類作成はコンピュータを使っているが、NW停止が影響しない場合がある。 また、入札時のNW停止のように数億規模の被害を及ぼす場合も考えられ、NWが止まった時間での被害の定量化は難しい。 業務上大きな影響を受けるシステム 5年前は、停止すると業務上大きな影響を受けるシステムは考えられなかった。現在は、インターネット(電子申請)やメールがクリティカルなシステムといえるかもしれない。
・発行に関する業務には、コンピュータがダウンしてしまうと、業務が完全にストップするものがある。（人手による作業が不可能で依存度が高い）

被害状況など(過去事例含む)
＜Fromの詐称メールを送信するウイルスのため、問い合わせ対応が必要になった＞ ・パブリックへのメール問い合わせは、一次対応窓口は広報だが、内容によりIT部門につながれる。 ・影響を受けた3名は従業員 ＜メールの運用面＞ ・全社メールは、メールGWで一旦チェックしている ・添付ファイルサイズの制限をしているが、営業のメーリングリストにサイズの大きいファイルを添付する事故がたびたび起こる
インターネットの接続を2日間止めたので、メールなどは全従業員が影響を受けた。
＜KLEZ＞ 1台のPCに感染。 共有フォルダに感染した時点で検知。最終的に30台程度に感染。 20通の感染メールを発信したことをログから発見し、お詫びした。 PCのパワーが無く、ログイン時の自動スキャンが動かず見逃したのが原因。

本年度は特に被害なし。 ＜過去事故＞ H12年にx97M_DIBIV（Excelマクロ系）に感染。社内で約400クライアントと1サーバに被害。 社員が自宅で感染したファイルをFDで持ち込み、汚染されたファイルを掲示板に挙げたため被害が拡大。メールはウイルスチェックされていたため、その社員が自宅から社内へ送信したファイルは排除されたが、同時にFDで持ち込まれたため防御できなかった。 このインシデント以降、情報系サーバにもウイルス対策ソフト導入。 復旧は3人が2ヶ月対応。センターからリモートで作業、駆除と定義ファイル更新を同時に実施。 当初1～2人程度の感染であったため発見が遅れた。 各端末の定義ファイルは自動更新ではなく、手動で毎日更新。 メールはウイルスチェックされているため、外部への感染は防げた。
２００２年度は被害なし。ＳＱＬは対策が間に合った。 ＜過去事故＞ ２００１年８月７日にコードレッドで被害あり。この結果二重か対策とセキュリティ対策を強化した。特に代理店関連と社内システムとセキュリティ対策が異なっていたが一本化した。
ウイルス被害あり(内容不明) 自宅のFD経由で感染（部門のシステム担当者により対応し、二次感染はなし） 復旧費用　20,000円、一日あたりの人件費　20,000円が発生。
＜過去事故＞ 94年　Yankee Doodle　がＦＤ経由で感染（100～200台) ・復旧に一日 ・その他詳細は不明
1年間あたり数件(予想：5件程度)のKlez関連のインシデントが発生。 現場のNW管理者対応＋セキュリティ委員会(本社組織)対応の稼動、あわせて、合計年100万円程度の稼動費用を費やした。 賠償・お詫びなどの費用発生は特に無いと考える。
ウイルスソフト会社のパターン配信が遅れたため侵入。ウイルスパターンファイル更新後にウイルス削除した。
ウイルス対策はしていたが、パターンファイルが配布される前に感染してしまった。
日時不明　インドネシアの関係会社で　ＫＬＥＺに10～20台感染。 ・日本から技術者2名を派遣し復旧。またすべての端末100台をチェック。 ・Ｅメールの連絡が2日出来なかったが、日本は休暇中だったこともあり、業務への影響は少なかった。 ・復旧作業量　8人日 ・復旧費用　240,000円＋交通費 ・一日あたりの人件費　30,000円
＜過去事故＞ 2002年末　Brade ウイルスに20台感染。共有ファイルで被害が広がった。 ・金曜の夕方に感染したため、業務への影響は少なかった。 ・エクストラネットで感染し、復旧に9人日。 ・復旧費用　270,000円 ・対策費　300,000円 ・一日あたりの人件費　30,000円

その他コメント
・以前退社した社員にソースコードを持っていかれたことがあったが、実害はなかった ・利便性とセキュリティのバランスがむずかしい
暗号化メールが検討にあがっているが、暗号化したデータやMUAによる分割送信は、メールGWウイルスチェックができくなったり処理が重くなるため、すぐに導入できない
・スラマーでSQLサーバ3台が被害にあった、復旧は2人で3～4時間かかった ・無線LANは禁止している
・自社のセキュリティ評価、セキュリティの客観的なレベルが知りたい。 ・セキュリティ教育を今後どうやっていくかが悩みである。
・業務ネットワークは、社内ネットワークと接続していない ・業務の利便性を追求していくと安全性（セキュリティ）がどうなるか判断がむずかしい ・無線LANは使用していない
・メールサーバ、基幹（決済）システムは二重化（冗長構成）にしている ・被害報告は損害額を入れ、経営に伝えている。 ・klezで自社のドメインを語られた被害にあった ・理想的には、クライアントとサーバは違ったメーカのアンチウイルスソフトを入れたいがコストの面がネックである(たまたまクライアントに別ソフトが入っており、予防できた時有り) ・業務上大きな被害を受けるのは、メール(回線2重化、5Mのパラ)と経理決済(コールドスタンバイ、出先に設置) ・情報資産については、大中小は付けているが、金額的な置き直しはしていない。 ・２００２年は比較的平穏であった。
無線ＬＡＮのセキュリティ問題は大きい。次回の調査の対象とすべし。社外の対策は重点をおいているが、社内対策がパッチをあてにくいこともあって今後の課題である。グループウェアを用いているのでワームには強いが、エクセルに添付には弱い。
・社内のウイルスチェックソフトで個人データをウイルスチェックしようとする者がいる。 ・お客様にメールを送ってからセキュリティに敏感になって、対策を行うようになった。
・メールサーバでウイルスチェックを開始してから、ウイルス感染は防御できている。 ・経営陣を巻き込んでのセキュリティ対策が難しい。新聞等に取り上げられたりした場合の方が動きやすい。
ここ1年は、ぽつぽつとメジャーなウイルスの感染報告、対処事案あり。 1件当たり約70～80人(台？)が感染している。ただし、直近1年は以前のNimdaのような大きな被害なし。 前回のSlammerの際も、調査した結果、感染事例は認められなかった。 インターネット接続点に対するDoS攻撃発生については、直近1年はなし。ただし、昨年度は、スパムメール事件があり、数時間にわたってメールサーバが停止した。 今年1年は平穏な年だった。 大きなウイルス被害は2年周期なので、3月から来年度以降が心配。戦争などの情勢不安も重なるので、注意が必要。
現在行っている課単位IDでのネットワークにログインについて、問題有りと考えている。

8.2　アンケート用紙

情報セキュリティ被害調査アンケート

本調査は情報セキュリティの管理者(責任者・担当者)を対象としております。お手数ですが該当する方に転送下さるようお願いします。また、回答は本用紙に直接ご記入下さい。

A　貴社の事業状況についてご回答下さい。

A-1　貴社が属する主要業種をご回答下さい。(1つ選択し、○をお付け下さい)

1	金融（銀行、保険、証券等）		6	教育・マスコミ	
2	医療・製薬		7	建設	
3	運輸		8	飲食・小売	
4	エネルギー		9	その他サービス	
5	情報・通信		10	その他	

A-2　貴社の年間売上および従業員数をご回答下さい。

1	年間売上高（万円）		万円
2	従業員数（人）		名

A-3　貴社の拠点数をご回答下さい。(1つ選択し、○をお付け下さい)

1	1箇所		6	100～299箇所	
2	2箇所		7	300～999箇所	
3	3～9箇所		8	1000～2999箇所	
4	10～29箇所		9	3000箇所以上	
5	30～99箇所				

B貴社のシステム状況についてご回答下さい。

B-1 貴社が保有しているパーソナルコンピュータ（PC）の台数をご回答下さい。
（1つ選択し、○をお付け下さい）

1	1～29台		5	1000～2999台	
2	30～99台		6	3000～9999台	
3	100～299台		7	10000～29999台	
4	300～999台		8	30000台以上	

B-2 貴社のインターネットメールの利用状況はどの程度ですか。（1つ選択し、○をお付け下さい）

1	使っていない		4	利用可能だが添付ﾌｧｲﾙに制限有り	
2	専用端末のみ利用可能		5	特に制限無く利用可能	
3	利用可能だが添付ﾌｧｲﾙは不可				

B-3 貴社のWeb閲覧の利用状況はどの程度ですか。（1つ選択し、○をお付け下さい）

1	使っていない	
2	専用端末のみ利用可能	
3	利用可能だが閲覧先の制限あり	
4	特に制限無く利用可能	

B-4 貴社が保有しているPC（ｸﾗｲｱﾝﾄ）の何割程度がメール、Ｗｅｂ閲覧を利用できますか。

1	インターネットメール（%）		%
2	Web閲覧（%）		%

C 貴社の情報セキュリティ管理への取組みについてご回答下さい。

C-1 情報セキュリティに関する規定をお持ちですか。(該当全てに○をお付け下さい)

1	ない	
2	情報セキュリティポリシーとして規定している	
3	就業規則の一部に情報セキュリティ関連の規定がある	
4	個人情報保護規定の一部として情報セキュリティ関連の規定がある	
5	その他規定の一部として情報セキュリティを規定している	
6	情報セキュリティ関連の作業手順を規定している	
7	分からない	

<その他>

C-2 *C-1で「1 ない」と回答した方のみご回答下さい。*

情報セキュリティに関する規定を制定していない最大の理由をご回答下さい。(1つ選択し、○をお付け下さい)

1	経営者が必要性を認識していない	
2	現場が必要性を認識していない	
3	業界･業種的に必要性が乏しい	
4	社内にリソース(人材、資金)が不足している	
5	分からない	

<その他>

C-3 情報セキュリティ管理担当者の人数を教えてください

1	専任担当者(名)		名
2	兼任担当者(名)		名
3	担当役員を選任している(選任の場合○をお付け下さい)		

C-4 情報セキュリティ関連の事故や事件が発生した場合の社内連絡体制をご回答下さい。（該当全てに○）

1	連絡体制の規定が設けられている	
2	セキュリティ事故･事件の発生を把握する責任部門の設置	
3	各部門毎に事故の連絡担当者が設置されている	
4	ほぼ全従業員が連絡体制を理解している	
5	連絡体制が機能している	

C-5 情報セキュリティの観点から取引先の選定や契約時に配慮している点をご回答下さい。（該当全てに○）

1	特に意識していない	
2	経営状況やサービスレベルの分かる取引先を重視	
3	情報ｾｷｭﾘﾃｨに関する認証取得企業（BS7799、ﾌﾟﾗｲﾊﾞｼｰﾏｰｸ等）を重視	
4	情報セキュリティポリシーの制定企業を重視	
5	システム監査を受けている企業を重視	
6	守秘義務契約書を締結	
7	サービスレベル(ＳＬＡ)を規定した契約書や覚書を締結	
8	取引先への監査を実施	
9	分からない	

<その他>

C-6 派遣社員や常駐作業員受入時の配慮点をご回答下さい。（該当全てに○をお付け下さい）

1	特に対策はしていない	
2	情報の取扱いに関する契約（機密保持契約等）締結	
3	情報システム教育の実施	
4	情報セキュリティ教育の実施	
5	分からない	

<その他>

C-7　被害が発生した時の対応計画の対象をご回答下さい。（該当全てに○をお付け下さい）

1	定めていない	
2	発生事象別の被害状況の確認事項	
3	被害状況の確認責任者	
4	被害発生時の社内連絡体制	
5	被害別の社外連絡先（ベンダー、業界団体、コンサルタント等）	
6	従業員への情報開示方法と情報開示レベル	
7	第三者への情報開示方法と情報開示レベル	
8	復旧時の確認事項	
9	分からない	

<その他>

C-8　情報セキュリティ関連ニュース等の収集についてご回答下さい。（該当全てに○をお付け下さい）

1	行っていない	
2	定期的にOS・基幹ソフトベンダーのHP等でセキュリティ関連情報を確認する	
3	セキュリティ情報を提供する組織（IPA/ISEC等）のHPを確認する	
4	セキュリティ情報提供のサービスを受けている	
5	分からない	

<その他>

C-9　サーバのセキュリティを確保するためにどのようにして各種パッチを適用していますか。
（1つ選択し、○をお付け下さい）

1	パッチ未適用	
2	定期的にパッチのリリース状況を確認し常に最新状況を維持している	
3	定期的にﾘﾘｰｽ状況を確認する体制はないが、ｻｰﾊﾞ管理者等の裁量で適用している	
4	問題が発生するまでパッチは適用しない	
5	分からない	

<その他>

C-10 認証取得を「計画中」、または「取得済」の別を右欄に○を付けてご回答下さい。

	名称	計画無し	計画中	取得済み
1	ISMS (BS7799)			
2	ISO/IEC 15408			
3	プライバシーマーク			
4	CMM (Capability Maturity Model)			
5	分からない			

＜その他の情報セキュリティ関連認証(名称)＞

C-11 直近１年間でのシステム監査や脆弱性検査(ﾍﾟﾈﾄﾚｰｼｮﾝﾃｽﾄ)の実施状況をご回答下さい。

	項目名	システム監査(実施有りに○)	脆弱性検査(実施有りに○)
1	インターネット		
2	イントラネット		
3	エクストラネット		
4	社内専用ネットワーク		

<その他>

C-12　情報セキュリティ関連予算はありますか。(1つ選択し、○をお付け下さい)

1	ない	
2	情報セキュリティ対策費として計上される	
3	情報システム関連予算の一部として計上される	
4	その他予算の一部として計上される	
5	分からない	

<その他>

C-13 上記回答で２～４に○の場合、大まかな数字をご記入下さい。

予算がある場合の金額(万円)		**万円**
情報システム予算に対する割合(%)		**%**

C-14 情報セキュリティ関連予算の対象をご回答下さい。(該当全てに○をお付け下さい)

1	予算はない		6	セキュリティ管理者教育費	
2	セキュリティ対策ハードウェア購入費用		7	従業員教育･啓発活動費	
3	セキュリティ対策ソフトウェア購入費用		8	セキュリティ関連認証取得費	
4	セキュリティ対策ハードウェア保守費用		9	セキュリティ関連認証維持費	
5	セキュリティ対策ソフトウェア保守費用		10	分からない	

＜その他＞

C-15　情報セキュリティを確保するために導入しているシステムをご回答下さい。
(該当全てに○をお付け下さい)

1	ファイアウォール		5	全ｸﾗｲｱﾝﾄPCにウイルスチェックソフトを導入	
2	侵入検知システム(IDS)		6	暗号化ツールの使用(S/MIME、PGP)	
3	DMZセグメントの設置		7	Proxyｻｰﾊﾞｰ側にウイルスチェックを導入	
4	メールサーバでのウイルスチェック		8	分からない	

＜その他＞

C-16 情報漏洩を防止するために行っている対策をご回答下さい。(該当全てに○をお付け下さい)

1	メールの監視		8	サーバルームへの立ち入り制限	
2	Webメールの監視		9	ＦＤなどの記録媒体の持ち出し制限	
3	サーバのアクセス制限		10	ＦＤなどの記録媒体の廃棄基準	
4	外線電話の監視		11	PC(OA機器)の廃棄基準	
5	書類の持ち出し制限		12	鍵暗号システム	
6	ノートＰＣ(OA機器)の持ち出し制限		13	バイオメトリクス	
7	ノートＰＣ(OA機器)の持ち込み制限		14	個人認証デバイス	

<その他>

C-17 情報セキュリティ教育の内容をご回答下さい。(該当全てに○をお付け下さい)

1	ウイルス･ワーム対策		6	緊急時の対応	
2	パスワードの管理に関する教育		7	ソーシャルエンジニアリング対策	
3	個人情報保護		8	パソコンの設定･運用	
4	機密情報の保護		9	ネットワーク知識	
5	ネチケット				

<その他>

C-18 直近１年間での情報セキュリティ教育の実施状況を教えてください。(該当全てに○をお付け下さい)

	教 育 内 容	人数	年回数
1	一般従業員(ユーザー教育)向け教育		
2	マネージャー向け教育		
3	専門家向け教育		

C-19 現在実施、また今後実施していきたいと考えている情報セキュリティ関連対策をご回答下さい。（該当全てに○をお付け下さい）

		実施済	今後			実施済	今後
1	セキュリティ関連文書の整理			9	全従業員へのセキュリティ情報の提供		
2	情報セキュリティを考慮した社内制度の制定			10	事故･事件対応訓練		
3	情報システム部員のセキュリティ教育強化			11	サーバでのウイルスチェック		
4	一般従業員のセキュリティ教育強化			12	クライアントでのウイルスチェック		
5	セキュリティ関連の認証取得			13	情報セキュリティのスキルを有する人材の採用		
6	セキュリティ関連認証取得システムの導入			14	ASP (Application Service Provider) や IDC (Internet Data Center)の利用		
7	セキュリティ情報の収集			15	人材派遣の利用		
8	システム監査の実施						

<その他>

C-20 貴社業務の IT 化はどの程度進んでいますか。大まかなシステム依存度をご回答下さい。（1 つ選択し、○をお付け下さい）

1	ほとんどの業務がコンピュータ化されている	
2	多くの業務がコンピュータ化されている	
3	半数程度の業務がコンピュータ化されているが、手作業による業務も半数程度	
4	ｺﾝﾋﾟｭｰﾀｰ化されている業務はまだ少なく、依然と手作業による業務が大半である	
5	ｺﾝﾋﾟｭｰﾀｰ化されている業務はほとんどなく、手作業による業務がほとんどである	

<その他>

D 貴社の情報システムに生じた被害の状況をご回答下さい。

回答の難しい項目については空欄でも構いませんが、大まかな状況や数字をできるだけご教示下さい。

①被害コードについては次頁をご参照下さい。

②用紙は３事故分を添付していますが、必要な場合にはコピー対応をお願いいたします。

＜記載例＞

	被害コード →		1		
1	＜事故状況＞ クレズに感染したE-Mailを受け取った職員が、本メールを開封して感染した。当該職員の所属部門の共有サーバーのドライブにコピーされ、当該部門のＰＣが感染した。各職員が定期的にパターンファイルを更新する事となっていたが、本職員他、部門メンバーが更新を怠っていたため、ほぼ部門ＰＣ全部に感染するに至った。他部門サーバーへの感染は、ウイルスチェックソフトで防止できたが、社外メールへの送信を防げず、確認出来た件数で３００件ほどが感染メールを社外に送信してしまった。				
2	発生日時	２００２年　８　月　３０　日　　時間（２０：００）			
3	被害システムについて メールサーバー、ファイルサーバー等、全５台				
4	被害システムの種類について(該当システムの右欄に○をお付け下さい。)				
	(1)インターネット(DMZを含む)	○	(4)社内専用ネットワーク		
	(2)イントラネット		(5)ＥＣ（BtoB）		
	(3)エクストラネット		(6)ＥＣ（BtoC）		
5	停止時間		５		時間
6	影響を受けた従業員の人数		８０(社外は不明)		人
7	システム停止時の業務処理量の低下割合		３０		%
8	システムの年間売り上げ（EC関連の場合）		ー		円
9	システムの年間収益（EC関連の場合）		ー		円
10	被害を受けたサーバーの数		５		台
11	被害を受けたクライアントの数		７０		台
12	営業継続費		特になし		円
	代替手段	＜対応方法をご記入下さい＞ ・電話、ｆａｘなどの通信手段。 ・他部門のＰＣでの作業継続			
13	逸失利益(確実利益を逃した分)		１,０００,０００(見積り遅れ)		円
14	喪失した情報資産		０		円
15	機会損失(見込み利益で逃した分)		不　明		円
16	賠償・補償金額		０(謝罪のみ)		円
17	その他関連出費（ブランド価値の維持費用）について				
	(1) お詫び広告		特になし		円
	(2) 謝罪出状		１００,０００(郵便＋人件費)		円
	(3) お詫び行脚		１０(１００件分)		日人工

＜被害コード一覧表＞

被害ｺｰﾄﾞNo.	種類	被害項目	概　要
1	ﾜｰﾑ型ウイルス	KLEZ (ｸﾚｽﾞ)	大流行したニムダと類似した活動を行い、E-Mailと共有ドライブへのコピーで増殖し、実行可能形式ファイルへのウイルス感染を行う別プログラムも作成。プレビューによる「ダイレクトアクション活動」有り。
2	ﾜｰﾑ型ウイルス	BADTRANS (ﾊﾞｯﾄﾞﾄﾗﾝｽ)	ワームに分類される「トロイの木馬型」不正プログラム。WORM_BADTRANS.A の亜種になります。自身のコピーをメールに添付して送信し、ネットワーク上で自己増殖します。また、侵入したマシン上でのキー入力を記録するハッキングツール的活動も行う。プレビューによる「ダイレクトアクション活動」有り。
3	ﾌｧｲﾙ感染型ウイルス	NIMDA (ﾆﾑﾀﾞ)	直接感染のファイル感染型ウイルス。単体で「トロイの木馬」としても活動する。感染活動の他にメール送信、ネットワークドライブへのファイルコピー、IISのセキュリティホールを利用した侵入などで自身のコピーをネットワーク上で頒布するワーム活動も行う。プレビューによる「ダイレクトアクション活動」。
4	ﾌｧｲﾙ感染型ウイルス	MAGISTR (ﾏｼﾞｽﾄﾗ)	PE形式のファイルに感染するメモリ常駐型ミューテーション型のファイル感染型ウイルス。自身の感染ファイルをメールに添付して送付するワーム活動も行う。
5	ﾏｸﾛ型ウイルス	LAROUX (ﾗﾙｰ)	EXCELのマクロ型ウイルス。EXCEL文書内に"laroux"マクロモジュールを作成し他文書に感染を広める。
6	ﾜｰﾑ型ウイルス	BUGBEAR (ﾊﾞｸﾞﾍﾞｱｰ)	ワーム分類のトロイの木馬型不正プログラム。ワームとしてメールに自身のコピーを添付して送信するマスメーリング活動、共有ドライブへの自身のコピーを頒布する。活動の際にウイルス対策ソフトなどの強制終了を試み、情報漏洩型、バックドア型のハッキングツールとしての機能も持つ。
7	その他ウイルス被害		上記以外のウイルス被害。ウイルス名等については、事故状況欄にご記入下さい。
8	風評被害		ウイルス感染や情報漏洩などの2次的な被害
9	誤操作によるﾃﾞｰﾀの消失やｼｽﾃﾑﾀﾞｳﾝ		手順誤りなどヒューマンエラーなどによるトラブル
10	社内外からの不正ｱｸｾｽ		アクセス権を持っていない者による外部からの不正なアクセス
11	DoS攻撃等でｻｰﾋﾞｽ停止		アクセス集中等などによるサービス低下や停止
12	社外公開ﾎｰﾑﾍﾟｰｼﾞ改竄		外部者による不正なホームページの書き換え
13	社内情報の漏洩や改竄		媒体による情報の不正な持ち出しを含む
14	その他		☆内容について、ｱﾝｹｰﾄにご記入いただきますようお願いいたします。

D-1事故状況

1	被 害 コ ー ド →			
	＜事故状況＞			
2	発生日時	年 月 日 (:)		
3	被害システムについて	事故時の対策について		
4	被害システムの種類について(該当システムの右欄に○をお付け下さい。)			
	(１)インターネット(DMZを含む)		(４)社内専用ネットワーク	
	(２)イントラネット		(５)ＥＣ（BtoB）	
	(３)エクストラネット		(６)ＥＣ（BtoC）	
5	停止時間			時間
6	影響を受けた従業員の人数			人
7	システム停止時の業務処理量の低下割合			%
8	システムの年間売り上げ（EC関連の場合）			円
9	システムの年間収益（EC関連の場合）			円
10	被害を受けたサーバーの数			台
11	被害や影響を受けたクライアントの数			台
12	営業継続費(代替システム設置、人手の処理など)			円
	代替手段	＜対応方法をご記入下さい＞		
13	逸失利益(ｼｽﾃﾑ売上×停止時間、確実な利益の逸失分等)			円
14	喪失した情報資産			円
15	機会損失(見込み利益で逸失分、売上増分の逸失など)			円
16	賠償・補償金額			円
17	その他関連出費（ブランド価値の維持費用）について			
	(1) お詫び広告			円
	(2) 謝罪出状			円
	(3) お詫び行脚			日人工
18	復旧作業量（システム部門他）			日人工
19	復旧費用（業者等への支払額）			円
20	貴社従業員の一日当たり人件費			円／日