# ２００３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

２００４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
　　佐藤　友治　株式会社インターネット総合研究所
　　佐藤　康彦　株式会社 SRA
　　大谷　尚通　株式会社 NTT データ
　　岡田　賢治　ELNIS テクノロジーズ株式会社
　　杉谷　郁夫　株式会社グローバルエース
　　楠木　秀明　コンピューターアソシエイツ株式会社
　　大溝　裕則　株式会社ジェイエムシー
　　米澤　一樹　セキュアコンピューティングジャパン株式会社
　　遠藤　孝行　セコム株式会社
　　岡本　修一　株式会社損保ジャパン・リスクマネジメント
　　山田　英史　株式会社ディアイティ
　　安田　直義　株式会社ディアイティ
　　長嶋　潔　　東京海上火災保険株式会社
　　指田　朝久　東京海上リスクコンサルティング株式会社
　　佐野　智己　凸版印刷株式会社
　　成澤　晃一　凸版印刷株式会社
　　松谷　幸洋　株式会社ヒューコム
　　丸山　司郎　株式会社ラック

# 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、技術分野から管理分野まで幅広いワーキンググループの活動が行なわれているが、前年に引き続き、３回目となる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、独立行政法人　科学技術振興機構　社会技術研究システム（RISTEX）にご協力頂き、日本の基幹産業を構成する代表企業および、ＪＮＳＡに所属するＩＴ関連企業について、前年を上回る規模でアンケートを行い、さらにその企業の中から面談のご了解をいただいた企業への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を本調査結果として提示する。また、これらの状況を踏まえ、従前より提案しているインシデントによる被害の状況額および対策額の算出モデルについても、現時点で被害として考えるべき損害範囲やモデルの一案として提示している。

＜第２部について＞

被害額の算出モデルでは、情報セキュリティインシデントによる被害がシステム関連のみにとどまらず、波及的な影響として、損害賠償額などに及ぶことについても言及している。

今回の報告書においては、昨年提案した情報漏洩による「損害賠償の可能性」についての検討や考察をさらに進め、個人情報の「プライバシー要素」と「経済的要素」を織り込んだ賠償額を算出するモデルを提案している。また、企業価値の一端となる「株価への影響」について実例調査を再度行った。

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の方々に、共通の題材としてより深く検討していただき、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

毎日のように発生する新しいウイルスや情報漏洩事故、個人情報保護法の一部施行など、情報セキュリティに対する関心は、益々高まり、今まで以上に情報システムおよび情報管理におけるセキュリティインシデントに関する事例や現状調査についての必要性が高まっている。

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まだ少ない。情報漏洩事件については、マスコミなどを通じて公表されることが多くなってきたが、インシデントの性質上、積極的に公表されることがほとんど無く、被害そのものの定義も明確となっていない。このため、被害発生の結果として把握されるべき、被害金額などが算定できない状況である。

また、同様なことは、対策の面でも生じており、対策費用の範囲が明確でないため、一般的な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いその結果を取りまとめている。今年は、独立行政法人　科学技術振興機構　社会技術研究システム（RISTEX）との共同調査を実施し、昨年を大きく上回る規模のアンケートを実施し、多くの回答を得ることができた。この情報から得られる結果と、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よって、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、および効果の計測などについての考察を行った。

また、＜第２部(別冊)＞では、社会的な反響が大きく、関係者も非常に多数に上る事故種類の一つとして、今回も「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。

# 3. 調査結果および分析

## 3.1 調査対象

・JNSA メンバー企業を中心とするＩＴ関連企業。(一部に非ＩＴ企業を含む)
　JNSA 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実施。
・東証１部上場企業より無作為に抽出した 1,000 社。
　独立行政法人　科学技術振興機構　社会技術研究システム（以下 RISTEX とする）より調査を実施。

## 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、「9.1 アンケート用紙」を参照)
・JNSA メンバー企業を中心とする企業へのアンケートは、JNSA 事務局長の依頼文章と共に送付し、回答記入後、事務局へ返送いただき、集計を行った。
・RISTEX にて抽出した対象企業 1000 社については、RISTEX より情報セキュリティご担当者宛に送付し、回収後 RISTEX 事務局で集計を行った。
・また、回答の中で面談可能とのご連絡をいただいた企業に対して、当ワーキンググループメンバーが直接訪問し、具体的な内容について、ヒアリングを実施した。

## 3.3 調査の結果

### 3.3.1 ヒアリング調査

「5. 被害調査ヒアリングレポート」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

以下にアンケートの送付数と回答数を示す。

| | アンケート | | |
|---|---|---|---|
| | 送付 | 回答 | 回答率 |
| JNSA | 190 | 47 | 24.74% |
| RISTEX | 1,000 | 167 | 16.70% |
| 合計 | 1,190 | 214 | 17.98% |

アンケートの回収率は、ＪＮＳＡのアンケートで一昨年の約 43%、昨年の約 37%と比較すると 10%以上落ちて約 25%となった。しかしながら、RISTEX 分と合わせると全体で約 18%の回収率で 214 の有効回答を集めることができた。昨年が有効回答数 66 であったので 3 倍以上の回答数である。

## 3.4　調査結果の分析と特徴

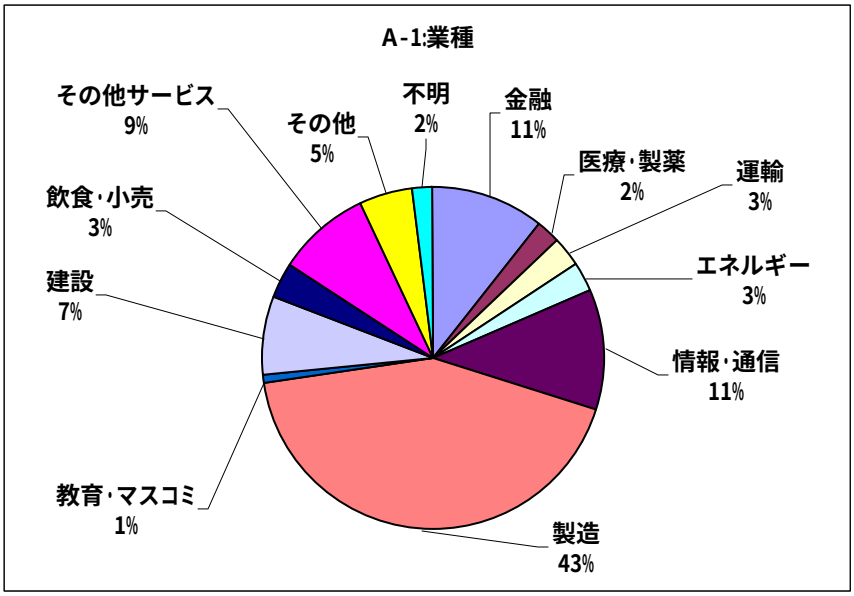
### 3.4.1　本年調査の調査結果と考察

本項目では、214 件のアンケート結果を集計し、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、〇をお付け下さい）**

| | 業種名 | 件数 | 割合 |
|---|---|---|---|
| 1 | 金融 | 23 | 10.7% |
| 2 | 医療・製薬 | 5 | 2.3% |
| 3 | 運輸 | 6 | 2.8% |
| 4 | エネルギー | 6 | 2.8% |
| 5 | 情報・通信 | 24 | 11.2% |
| 6 | 製造 | 91 | 42.5% |
| 7 | 教育・マスコミ | 2 | 0.9% |
| 8 | 建設 | 16 | 7.5% |
| 9 | 飲食・小売 | 7 | 3.3% |
| 10 | その他サービス | 19 | 8.9% |
| 11 | その他 | 11 | 5.1% |
| 12 | 不明 | 4 | 1.9% |
| | | 214 | 100% |




***Note***

前年の調査が JNSA の会員企業中心で情報・通信業が過半数を超えており、医療・製薬、運輸、建設、飲食・小売などの業種が対象に無かったが、今回のアンケートでは製造が 43%と一番多く、全業種が網羅されている。前年と比較すると、かなり実社会に近いアンケート集計が期待できる。

## 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

| | |
|---|---|
| 年間売上高（万円） | 31,895,663 万円 |
| 従業員数（人） | 4,084 名 |

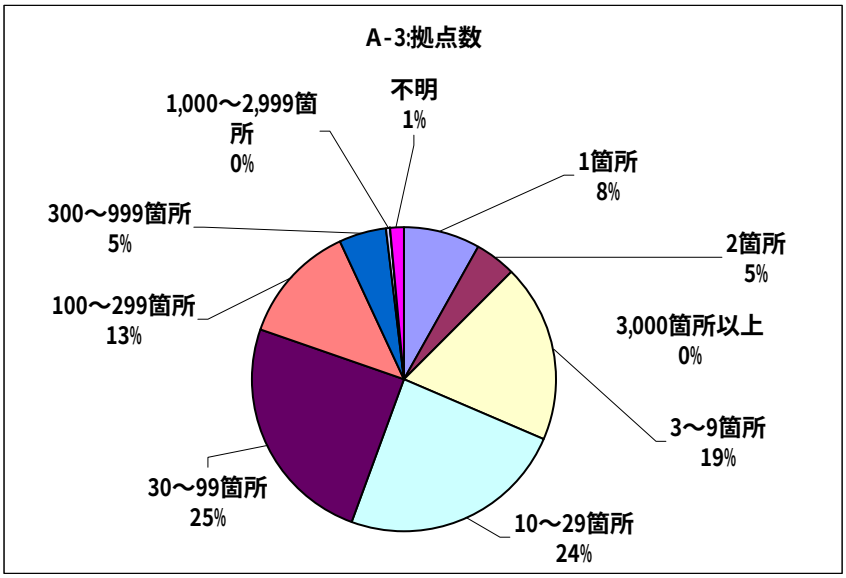
***Note***

上記数値は対象 214 件の平均であるが、年間売上高の最小値は 150 万円、最大値は約 5 兆 2 千億円、従業員数は最小 3 人、最大 14 万人とかなり幅広くなっている。

また、この平均値は、前年の調査と比較すると年間売上高で約 1.9 倍、従業員数で約 2.3 倍となっている。平均値であるので単純には述べられないが、次の拠点数のアンケート結果も考慮すると前年の調査より比較的規模の大きな企業の割合が高い可能性が強い。

## 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 | 7.9% |
| 2 | 2 箇所 | 10 | 4.7% |
| 3 | 3～9 箇所 | 40 | 18.7% |
| 4 | 10～29 箇所 | 52 | 24.3% |
| 5 | 30～99 箇所 | 53 | 24.8% |
| 6 | 100～299 箇所 | 27 | 12.6% |
| 7 | 300～999 箇所 | 11 | 5.1% |
| 8 | 1,000～2,999 箇所 | 1 | 0.5% |
| 9 | 3,000 箇所以上 | 0 | 0.0% |
| 10 | 不明 | 3 | 1.4% |
| | | 214 | 100% |



***Note***

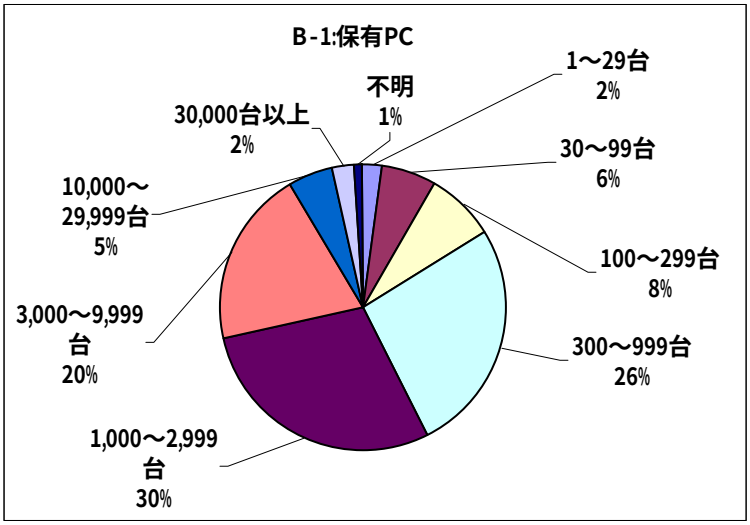
前年の調査では、調査対象の 83%が拠点数 29 箇所以下、62%が拠点数 9 箇所以下となっていた。今回の調査では、調査対象の 56%が拠点数 29 箇所以下、31%が拠点数 9 箇所以下となっており、10 箇所から 99 箇所の拠点数で全体の 49%を占めている。

また、前年には無かった拠点数が 1,000 箇所を超える企業も今回の調査では 1 社あった。

**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。**

| | 保有 PC 数 | 件数 | 割合 |
|---|---|---|---|
| 1 | 1～29 台 | 5 | 2.3% |
| 2 | 30～99 台 | 13 | 6.1% |
| 3 | 100～299 台 | 17 | 7.9% |
| 4 | 300～999 台 | 56 | 26.2% |
| 5 | 1,000～2,999 台 | 62 | 29.0% |
| 6 | 3,000～9,999 台 | 43 | 20.1% |
| 7 | 10,000～29,999 台 | 11 | 5.1% |
| 8 | 30,000 台以上 | 5 | 2.3% |
| 9 | 不明 | 2 | 0.9% |
| | | 214 | 100% |

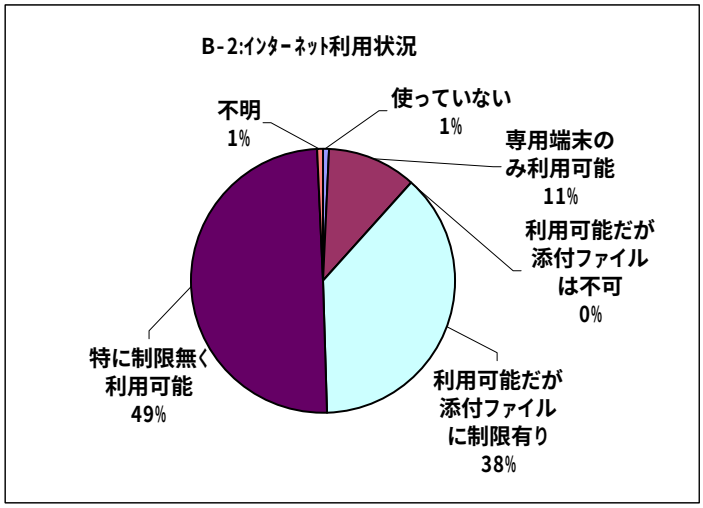



***Note***

従業員数との比較はないので、PC の一人一台環境がどの程度進んでいるかはわからないが、”B-5 貴社業務の IT 化はどの程度進んでいますか“ で 90%近くが ”多くの業務がコンピュータ化されている“ となっている状況と合わせると、業務に PC が不可欠な現状になっていることが推測される。

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 | 2 | 0.9% |
| 2 | 専用端末のみ利用可能 | 23 | 10.7% |
| 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 | 81 | 37.9% |
| 5 | 特に制限無く利用可能 | 106 | 49.5% |
| 6 | 不明 | 2 | 0.9% |
| | | 214 | 100% |




***Note***

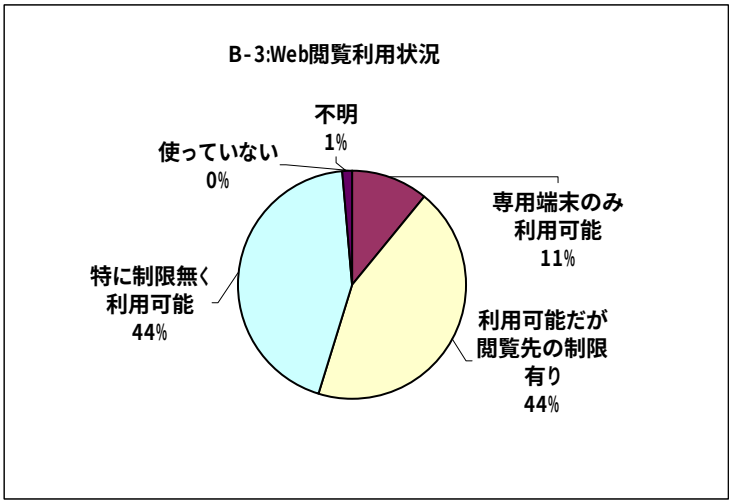
インターネットメールの利用では、2 社が「使っていない」と回答、また「専用端末のみ利用可能」も 23 社となっている。今回の調査では金融業が 23 社あり、いわゆる“ IT 化が進んでいない ”という状況ではなく、情報セキュリティ面からウイルスの感染などのリスクに対応した結果だと推測される。金融や社会の重要インフラを担う企業の場合は、セキュリティ面に万全を期すために利便性より安全を選択するのは、正しい選択と言える。

メールの添付ファイルを不可にしている企業はなく、これは前年の調査と同様の結果となった。添付ファイルに制限をつける企業は 38%と前年の 32%より上回った。

これは、情報セキュリティ面からのメールのフィルタリングと、画像などファイルサイズの増大化に対応した結果と思われる。

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 | 23 | 10.7% |
| 3 | 利用可能だが閲覧先の制限有り | 94 | 43.9% |
| 4 | 特に制限無く利用可能 | 94 | 43.9% |
| 5 | 不明 | 3 | 1.4% |
| | | 214 | 100% |




***Note***

Web 閲覧の利用率は 100%となった。これは、前年の調査と同様である。また「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 54%と半数を超える。これは、前年のの調査では 25%であったのと比較すると倍増している。

Web 閲覧とインターネットメールの利用状況は、約半数の企業が制限を設けており、約半数の企業が制限なく許可しているというのが、現在の利用状況であり、何らかの制限を加えている企業が増加傾向にある。

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

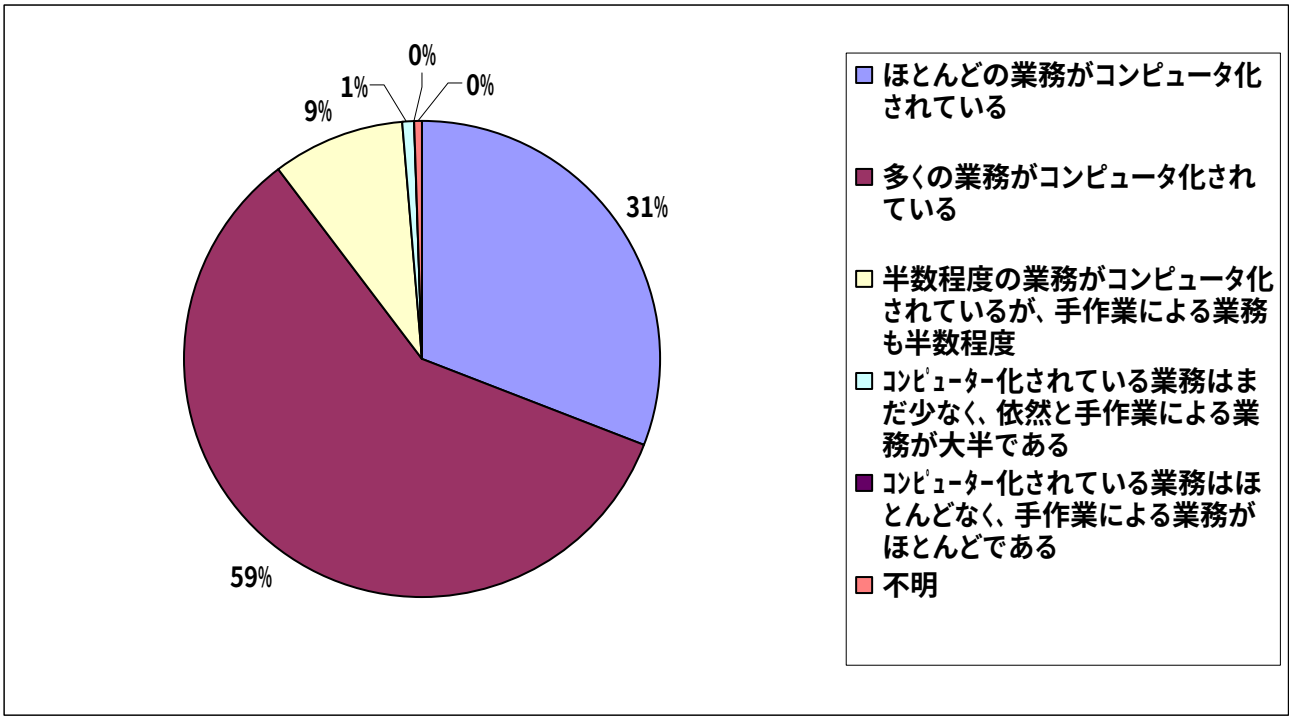
| | | | |
|---|---|---|---|
| 1 | インターネットメール (%) | 79 | % |
| 2 | Web 閲覧 (%) | 75 | % |

***Note***

平均値で見ると、インターネットメール、Web 閲覧ともに 80%弱の利用率になっている。

B-5 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）

| | システム依存度 | 件数 | 割合 |
|---|---|---|---|
| 1 | ほとんどの業務がコンピュータ化されている | 66 | 30.8% |
| 2 | 多くの業務がコンピュータ化されている | 126 | 58.9% |
| 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 | 19 | 8.9% |
| 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 | 2 | 0.9% |
| 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 | 0 | 0.0% |
| 6 | 不明 | 1 | 0.5% |
| | | 214 | 100.0% |




***Note***

「ほとんどの業務がコンピュータ化されている」と「多くの業務がコンピュータ化されている」の 2 項目で 90%、「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」まで入れると 99%と業務のコンピュータ依存度は高くなっている。

B-6　情報セキュリティ管理担当者の人数を教えてください

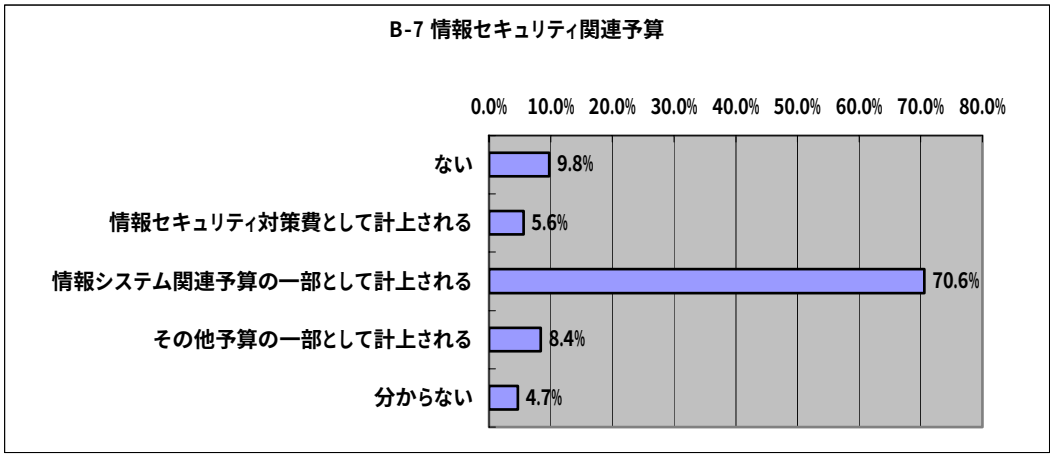
| | | | |
|---|---|---|---|
| 1 | 専任担当者 (名) | 2.0 | 専任者を置いている会社の平均人数 |
| 2 | 兼任担当者(名) | 22.0 | 兼任者を置いている会社の平均人数 |
| 3 | 担当役員を選任している | 32.7% | 選任している会社の割合 |

***Note***

上記の人数は、専任担当者・兼任担当者に関しては、担当者を置いている企業の平均人数、担当役員については今回のアンケート回答全体を母数とした割合である。実際にヒアリングした内容から兼任担当者には、情報システム部門内の人と社内各部門の情報セキュリティ委員などを加味した人数になっている場合が多い。

B-7　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）

| | 情報セキュリティ関連予算 | 件数 | 割合 |
|---|---|---|---|
| 1 | ない | 21 | 9.8% |
| 2 | 情報セキュリティ対策費として計上される | 12 | 5.6% |
| 3 | 情報システム関連予算の一部として計上される | 151 | 70.6% |
| 4 | その他予算の一部として計上される | 18 | 8.4% |
| 5 | 分からない | 10 | 4.7% |
| | | 212 | 99.1% |




***Note***

情報セキュリティ予算は、単独で計上されているのが 5.6%で、70.6%の企業が情報システム関連予算の一部として計上している。理由としては、ウイルス対策ソフトのように情報セキュリティに特化したプロダクトやサービスだけでなく、機能の一部としてセキュリティに関連したルータなどもあるため分けるのがむずかしいと考えられる。

B-8 上記回答で２～４に○の場合、大まかな数字をご記入下さい。

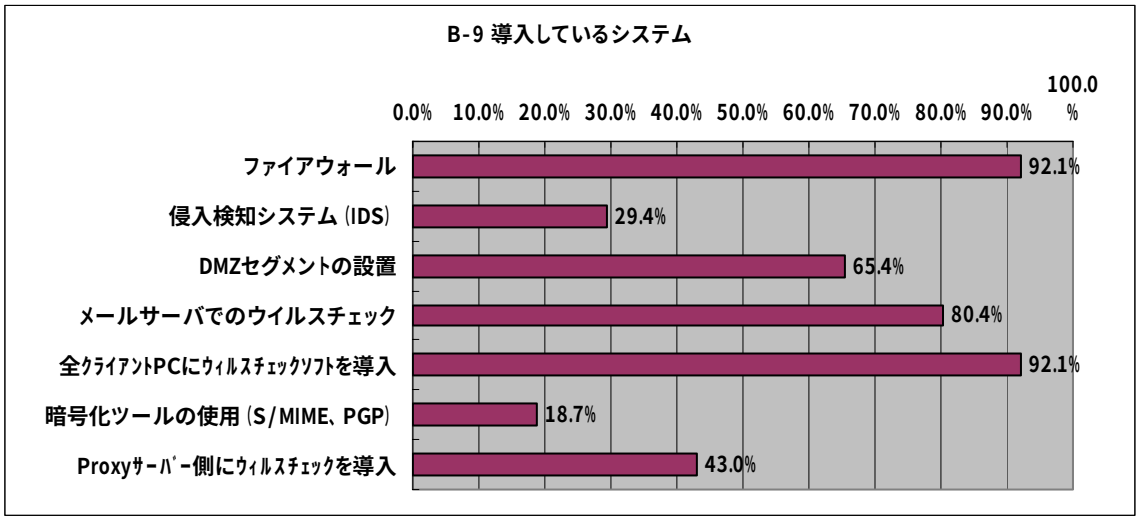
| | | |
|---|---|---|
| 予算がある場合の金額(万円) | 5,573 | 平均金額(万円) |
| 情報システム予算に対する割合(%) | 6.1 | 平均割合(%) |
| 増減額 | 567 | 平均金額(万円) |

***Note***

情報セキュリティの予算規模は、最小で 50 万円から最大で 20 億円と幅広く、最小の場合は一人あたり 16 万 7 千円で最大の場合は一人あたり 4 万 5 千円と約 4 倍の差が出た。企業規模が大きいほど一人あたりの予算が少なくなるのは理解できる。

B-9　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）

| | 導入しているシステム | 件数 | 割合 |
|---|---|---|---|
| 1 | ファイアウォール | 197 | 92.1% |
| 2 | 侵入検知システム (IDS) | 63 | 29.4% |
| 3 | DMZ セグメントの設置 | 140 | 65.4% |
| 4 | メールサーバでのウイルスチェック | 172 | 80.4% |
| 5 | 全ｸﾗｲｱﾝﾄ PC にウイルスﾁｪｯｸｿﾌﾄを導入 | 197 | 92.1% |
| 6 | 暗号化ツールの使用 (S/MIME、PGP) | 40 | 18.7% |
| 7 | Proxy ｻｰﾊﾞ側にウイルスﾁｪｯｸを導入 | 92 | 43.0% |
| 8 | 分からない | 0 | 0.0% |

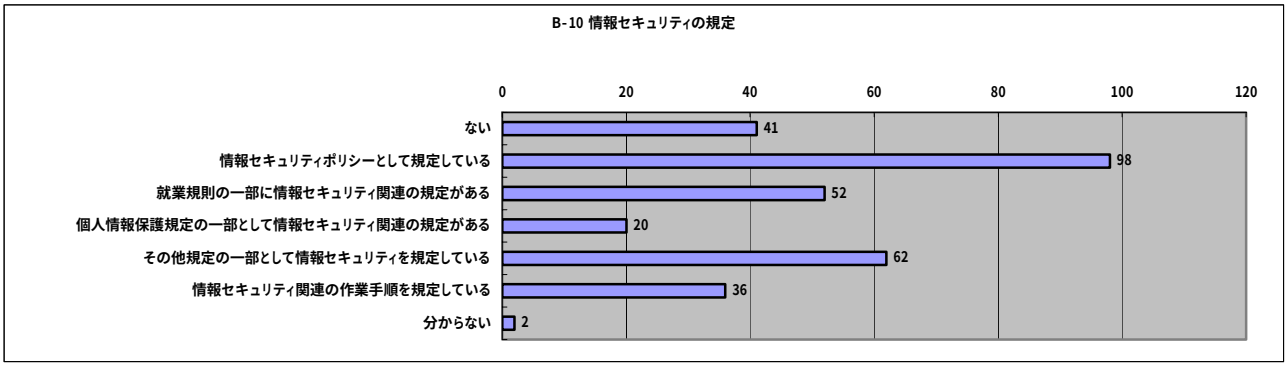



***Note***

ファイアウォールとクライアント PC でのウイルスチェックは 92.1%とかなり高い水準で導入されている。インターネットを使う以上、この対策は企業として常識になってきたのであろう。次いで導入が多いのがメールサーバでのウイルスチェックで、企業においてはウイルス対策が最重要項目であることがうかがえる。

B-10 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）

| | 情報セキュリティの規定 | 件数 | 割合 |
|---|---|---|---|
| 1 | ない | 41 | 19.2% |
| 2 | 情報セキュリティポリシーとして規定している | 98 | 45.8% |
| 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 | 52 | 24.3% |
| 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 | 20 | 9.3% |
| 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 | 62 | 29.0% |
| 6 | 情報セキュリティ関連の作業手順を規定している | 36 | 16.8% |
| 7 | 分からない | 2 | 0.9% |

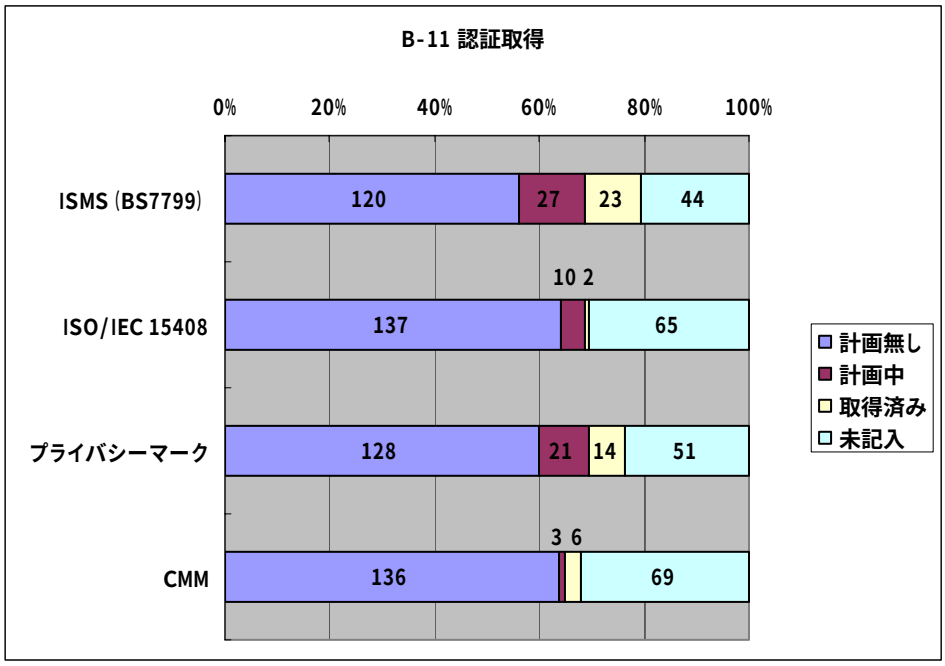



***Note***

セキュリティポリシーを規定している企業は、45.8%と全体の約半分である。重複回答があるので確実ではないが、何らかの規定に情報セキュリティ関連の規定があるとの回答をすべて集めると100%を超えている。これは、企業として情報セキュリティに対する関心の高さをうかがえるアンケート結果になった。

B-11 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 | | 未記入 | |
|---|---|---|---|---|---|---|---|---|
| ISMS (BS7799) | 120 | 56.1% | 27 | 12.6% | 23 | 10.7% | 44 | 20.6% |
| ISO/IEC 15408 | 137 | 64.0% | 10 | 4.7% | 2 | 0.9% | 65 | 30.4% |
| プライバシーマーク | 128 | 59.8% | 21 | 9.8% | 14 | 6.5% | 51 | 23.8% |
| CMM | 136 | 63.6% | 3 | 1.4% | 6 | 2.8% | 69 | 32.2% |




認証取得年度

| 名称 | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 |
|---|---|---|---|---|---|---|
| ISMS (BS7799) | | | | 2 | 6 | 12 |
| ISO/IEC 15408 | | | 1 | | | 1 |
| プライバシーマーク | 1 | 1 | 4 | 3 | 2 | 2 |
| CMM | | | | | 1 | 1 |

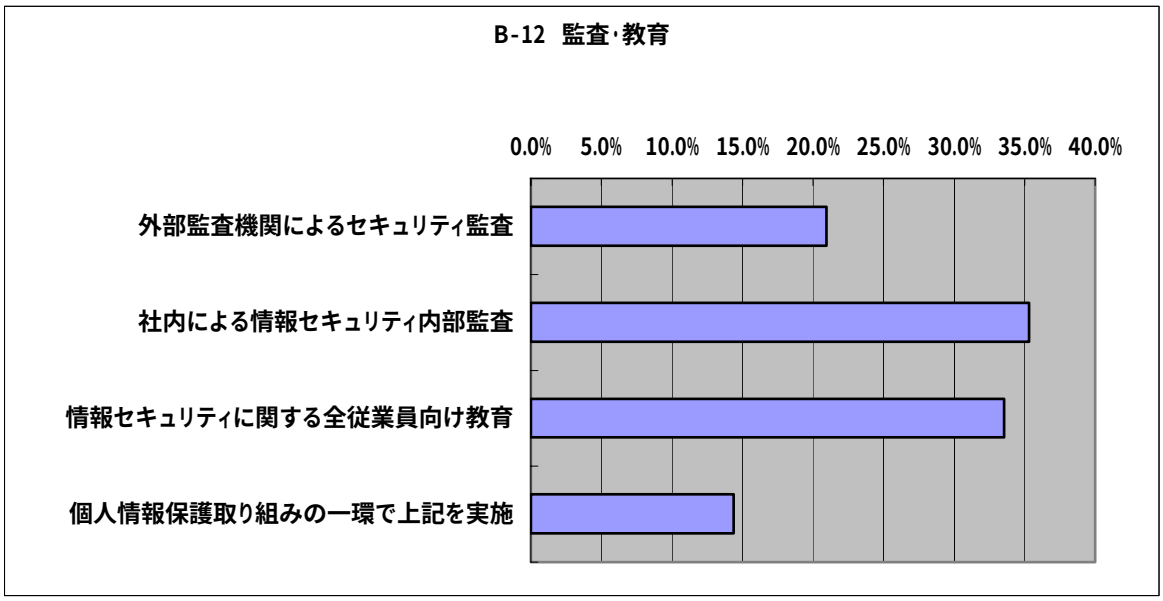
***Note***

「取得済み」が多かったのが ISMS の 23 件であった。また、「計画中」も 27 件あり、取得年度の変化から増加傾向にあるのがわかる。

次に「取得済み」が多いのがプライバシーマークの 14 件で、「計画中」も 21 件あり個人情報保護法の影響で 2004 年度以降は取得が増えると思われる。また、ISO/IEC 15408 や CMM は「取得済み」「計画中」共に低い水準になっている。

B-12 情報セキュリティに関する監査、教育についてご回答ください。（該当全てに○をお付け下さい）

| 監査･教育 | 実施している | 実施していない |
|---|---|---|
| 外部監査機関によるセキュリティ監査 | 21 | 79 |
| 社内による情報セキュリティ内部監査 | 35 | 65 |
| 情報セキュリティに関する全従業員向け教育 | 34 | 66 |
| 個人情報保護取り組みの一環で上記を実施 | 14 | 86 |




***Note***

このアンケート項目は、RISTEX が実施したアンケートのみ設定された項目である。情報セキュリティに関する内部監査、全従業員向け教育は 30%を越えているが、外部に委託したセキュリティ監査は、20%と比較的低い水準である。

## 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（JNSA のアンケート）。

### 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）

| | 情報セキュリティの規定 | 件数 | 割合 |
|---|---|---|---|
| 1 | ない | 6 | 12.8% |
| 2 | 情報セキュリティポリシーとして規定している | 31 | 66.0% |
| 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 | 14 | 29.8% |
| 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 | 6 | 12.8% |
| 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 | 7 | 14.9% |
| 6 | 情報セキュリティ関連の作業手順を規定している | 12 | 25.5% |
| 7 | 分からない | 0 | 0.0% |

### 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）

| | 情報セキュリティの規定 | 件数 |
|---|---|---|
| 1 | 経営者が必要性を認識していない | 0 |
| 2 | 現場が必要性を認識していない | 0 |
| 3 | 業界･業種的に必要性が乏しい | 1 |
| 4 | 社内にリソース（人材、資金）が不足している | 2 |
| 5 | 分からない | 0 |

***Note***

このアンケート項目以降からは、JNSA の会員企業を中心としたアンケート集計である。C-1 に関しては B-10 と同じ内容なので、解説は割愛するが、情報セキュリティの規定を制定していない理由として、「必要性が乏しい」と「リソースが不足している」の 2 点が上げられている。

### C-3　情報セキュリティの制定時期についてご回答下さい。

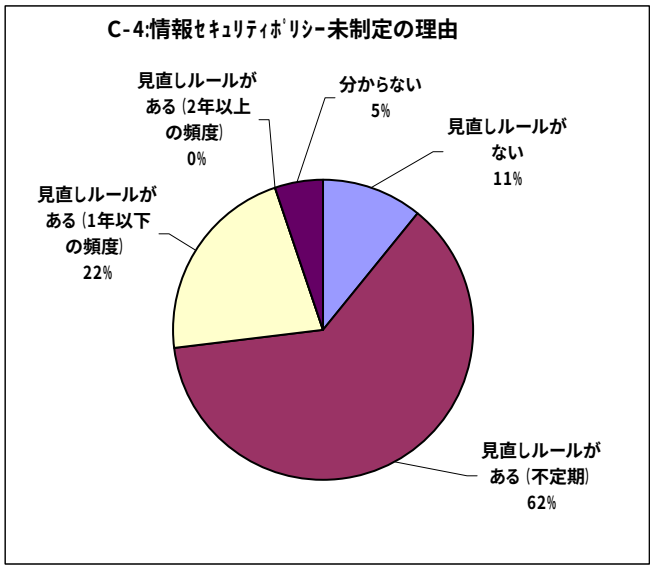
| 1994 | 1995 | 1996 | 1997 | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | - | - | - | 2 | - | 5 | 6 | 11 | 9 |

***Note***

古くは 1994 年に制定している企業が 1 社あるが、大半は 2000 年度以降に制定されている。ISMS の認証取得が 2002 年、2003 年に多く見られたのと同様に情報セキュリティの規定もこの 2 年間が多くなっている。

C-4 情報セキュリティに関する規程の見直し状況についてご回答ください。（1 つ選択）

| | 情報セキュリティの規定の見直し | 件数 | 割合 |
|---|---|---|---|
| 1 | 見直しルールがない | 4 | 10.8% |
| 2 | 見直しルールがある（不定期） | 23 | 62.2% |
| 3 | 見直しルールがある（1 年以下の頻度） | 8 | 21.6% |
| 4 | 見直しルールがある（2 年以上の頻度） | 0 | 0.0% |
| 5 | 分からない | 2 | 5.4% |

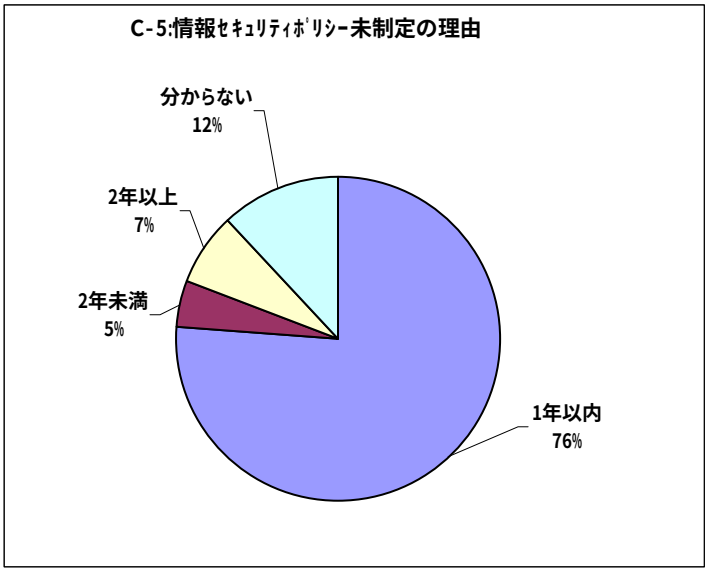



***Note***

このアンケートは、情報セキュリティの規定があると回答のあった企業に対して行った。「見直しルールがない」という回答は 4 件だけで、ほとんどの企業で見直しルールがあるとなっている。見直し時期は、不定期というのが 62%と多く、見直さなければならないタイミングで見直しが実施されているとすると、効果的に運用されていると解釈できる。

C-5　前回の見直し時期（見直していない場合には制定時期）についてご回答ください。（1 つ選択）

| | 前回の見直し時期 | 件数 | 割合 |
|---|---|---|---|
| 1 | 1 年以内 | 32 | 76.2% |
| 2 | 2 年未満 | 2 | 4.8% |
| 3 | 2 年以上 | 3 | 7.1% |
| 5 | 分からない | 5 | 11.9% |

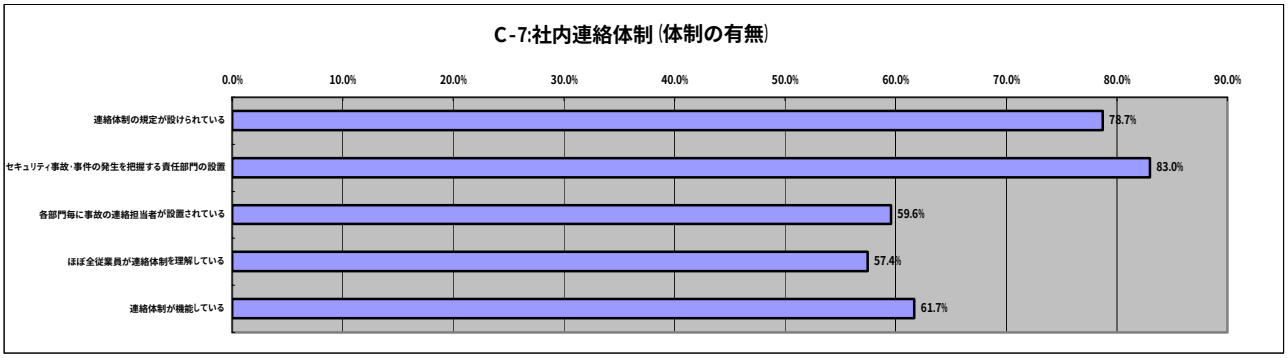



***Note***

情報セキュリティの規定の見直しは、一年以内に実施されているのが 76%と多くの比率になっている。これはC-4 で解説したように短期間で見直されて、運用されていることがうかがえる。

C-7　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。（体制の有無）（該当全て）

| | 社内連絡体制 | 件数 | 割合 |
|---|---|---|---|
| 1 | 連絡体制の規定が設けられている | 37 | 78.7% |
| 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 | 39 | 83.0% |
| 3 | 各部門毎に事故の連絡担当者が設置されている | 28 | 59.6% |
| 4 | ほぼ全従業員が連絡体制を理解している | 27 | 57.4% |
| 5 | 連絡体制が機能している | 29 | 61.7% |




| | 社内連絡体制（最近 1 年以内に設置） | 件数 | 割合 |
|---|---|---|---|
| 1 | 連絡体制の規定が設けられている | 9 | 19.1% |
| 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 | 8 | 17.0% |
| 3 | 各部門毎に事故の連絡担当者が設置されている | 4 | 8.5% |

| | 社内連絡体制（事故を契機に設置） | 件数 | 割合 |
|---|---|---|---|
| 1 | 連絡体制の規定が設けられている | 1 | 2.1% |
| 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 | 0 | 0.0% |
| 3 | 各部門毎に事故の連絡担当者が設置されている | 2 | 4.3% |

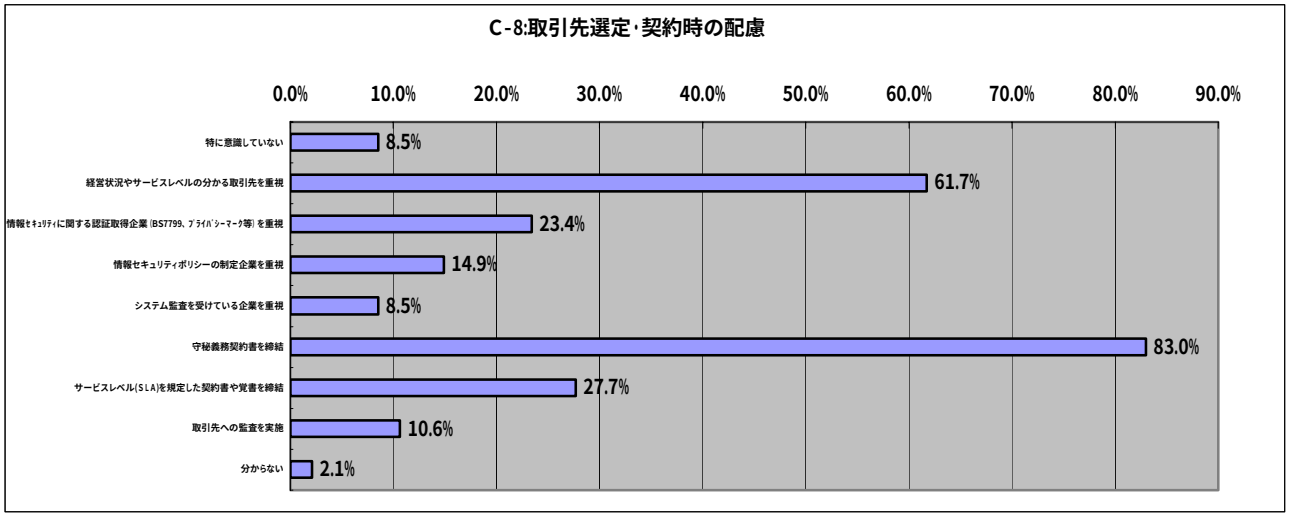
***Note***

情報セキュリティ関連の事件や事故が起きた場合の体制については、連絡体制の規定と責任部門の設置が 80%前後と高い。

それに比較して全従業員の理解度と連絡体制が機能しているかについては、60%前後であり 20%程度の開きがある。これは件数にして 10 件程度である。この差の 10 件は最近 1 年以内に連絡体制が設置された件数とほぼ合致する。事故対応に関する規定の浸透度には時間がかかることが伺われる。

C-8　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）

| | 取引先の選定や契約時に配慮 | 件数 | 割合 |
|---|---|---|---|
| 1 | 特に意識していない | 4 | 8.5% |
| 2 | 経営状況やサービスレベルの分かる取引先を重視 | 29 | 61.7% |
| 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 | 11 | 23.4% |
| 4 | 情報セキュリティポリシーの制定企業を重視 | 7 | 14.9% |
| 5 | システム監査を受けている企業を重視 | 4 | 8.5% |
| 6 | 守秘義務契約書を締結 | 39 | 83.0% |
| 7 | サービスレベル(ＳＬＡ)を規定した契約書や覚書を締結 | 13 | 27.7% |
| 8 | 取引先への監査を実施 | 5 | 10.6% |
| 9 | 分からない | 1 | 2.1% |

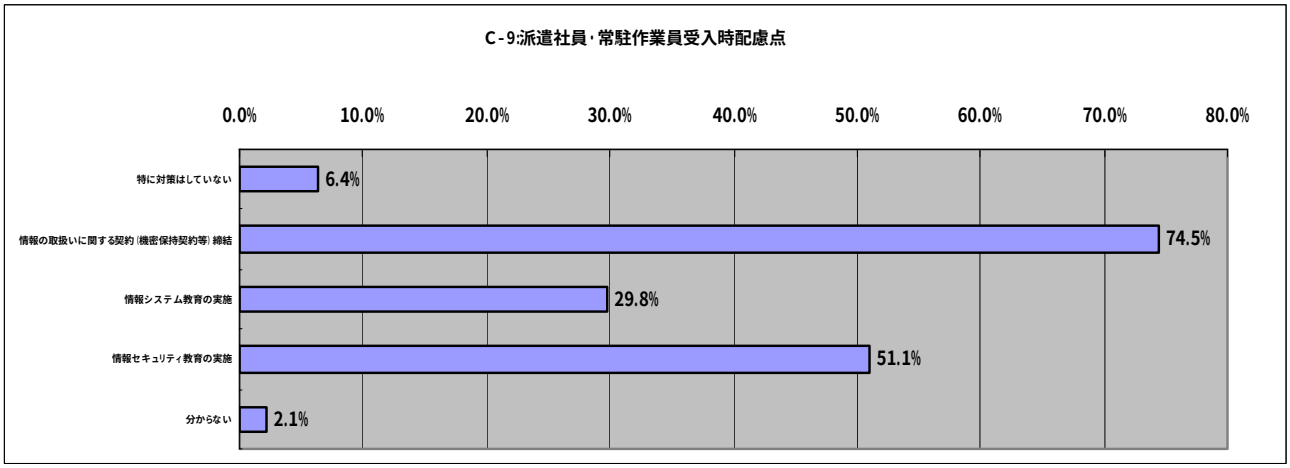



***Note***

取引先に対する考慮では、守秘義務契約書が一番多く 83%を占める。次は、経営状況やサービスレベルが 62%と続き、安定した取引を重視していることがわかる。その他の項目では、いずれも 30%にも満たない件数で、重視しているとは言えない状況である。

C-9　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）

| | 派遣社員や常駐作業員受入時の配慮点 | 件数 | 割合 |
|---|---|---|---|
| 1 | 特に対策はしていない | 3 | 6.4% |
| 2 | 情報の取扱いに関する契約（機密保持契約等）締結 | 35 | 74.5% |
| 3 | 情報システム教育の実施 | 14 | 29.8% |
| 4 | 情報セキュリティ教育の実施 | 24 | 51.1% |
| 5 | 分からない | 1 | 2.1% |

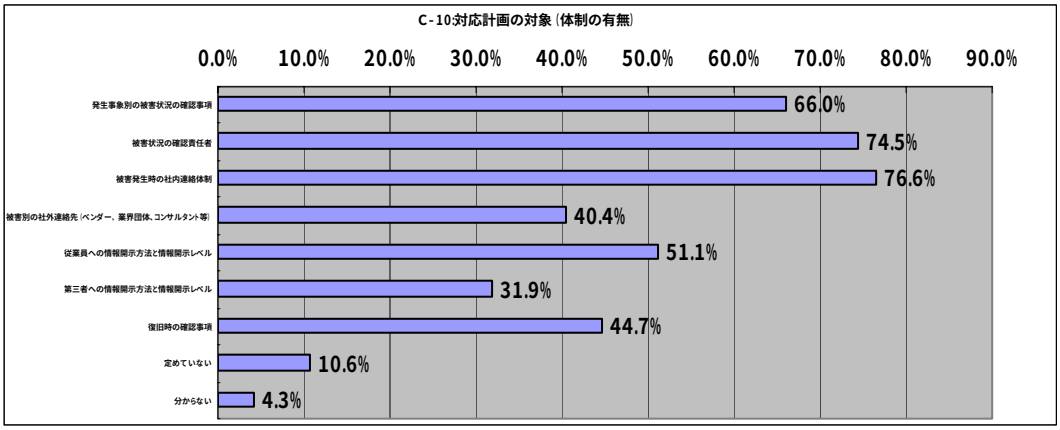



***Note***

正社員以外の情報セキュリティの対策については、取引先に対するのと同様に機密保持契約が74%と多くなっている。次が情報セキュリティの教育で51%と続き社員だけではなく、情報セキュリティに配慮しているのがわかる。

C-10　被害が発生した時の対応計画の対象をご回答下さい。（体制の有無）（該当全てに○をお付け下さい）

| | 対応計画 | 件数 | 割合 |
|---|---|---|---|
| 1 | 発生事象別の被害状況の確認事項 | 31 | 66.0% |
| 2 | 被害状況の確認責任者 | 35 | 74.5% |
| 3 | 被害発生時の社内連絡体制 | 36 | 76.6% |
| 4 | 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） | 19 | 40.4% |
| 5 | 従業員への情報開示方法と情報開示レベル | 24 | 51.1% |
| 6 | 第三者への情報開示方法と情報開示レベル | 15 | 31.9% |
| 7 | 復旧時の確認事項 | 21 | 44.7% |
| 8 | 定めていない | 5 | 10.6% |
| 9 | 分からない | 2 | 4.3% |




| | 対応計画（最近１年以内に設置） | 件数 | 割合 |
|---|---|---|---|
| 1 | 発生事象別の被害状況の確認事項 | 2 | 4.3% |
| 2 | 被害状況の確認責任者 | 3 | 6.4% |
| 3 | 被害発生時の社内連絡体制 | 4 | 8.5% |
| 4 | 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） | 2 | 4.3% |
| 5 | 従業員への情報開示方法と情報開示レベル | 2 | 4.3% |
| 6 | 第三者への情報開示方法と情報開示レベル | 3 | 6.4% |
| 7 | 復旧時の確認事項 | 2 | 4.3% |

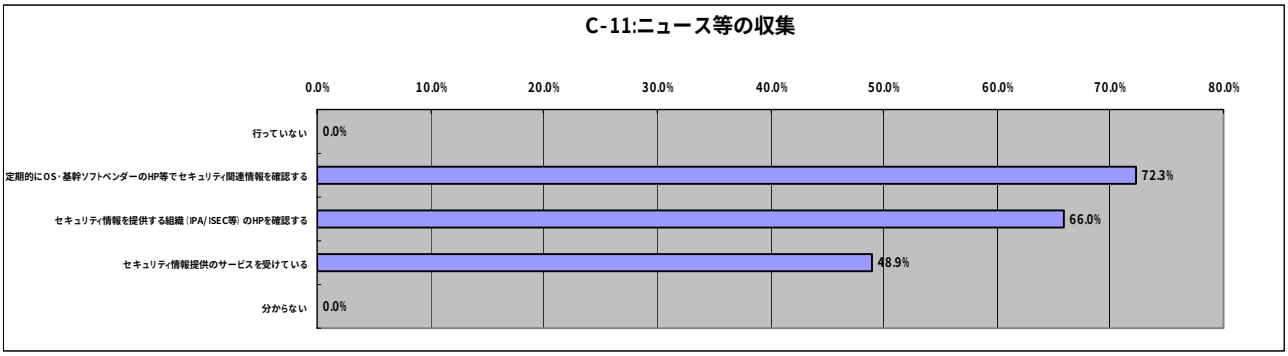
| | 対応計画（事故を契機に設置） | 件数 | 割合 |
|---|---|---|---|
| 1 | 発生事象別の被害状況の確認事項 | 2 | 4.3% |
| 2 | 被害状況の確認責任者 | 1 | 2.1% |
| 3 | 被害発生時の社内連絡体制 | 1 | 2.1% |
| 4 | 被害別の社外連絡先（ベンダー、業界団体、コンサルタント等） | 0 | 0.0% |
| 5 | 従業員への情報開示方法と情報開示レベル | 0 | 0.0% |
| 6 | 第三者への情報開示方法と情報開示レベル | 1 | 2.1% |
| 7 | 復旧時の確認事項 | 0 | 0.0% |

***Note***

被害が発生した時の対応計画に対するアンケートである。C-7 と似たアンケート結果になった。連絡体制、確認責任者、被害状況の確認事項が整備されている比率が高いのがわかる。第三者に対する情報開示方法と情報開示レベルが 31.9%であるのに比べ、従業員に対する同比率が 50%を越えているのは、第三者に開示してしまった場合に発生し得る、故意による事故の再発等のリスクを想定するとうなずける比率である。

C-11 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）

| | ニュース等の収集 | 件数 | 割合 |
|---|---|---|---|
| 1 | 行っていない | 0 | 0.0% |
| 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 | 34 | 72.3% |
| 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 | 31 | 66.0% |
| 4 | セキュリティ情報提供のサービスを受けている | 23 | 48.9% |
| 5 | 分からない | 0 | 0.0% |

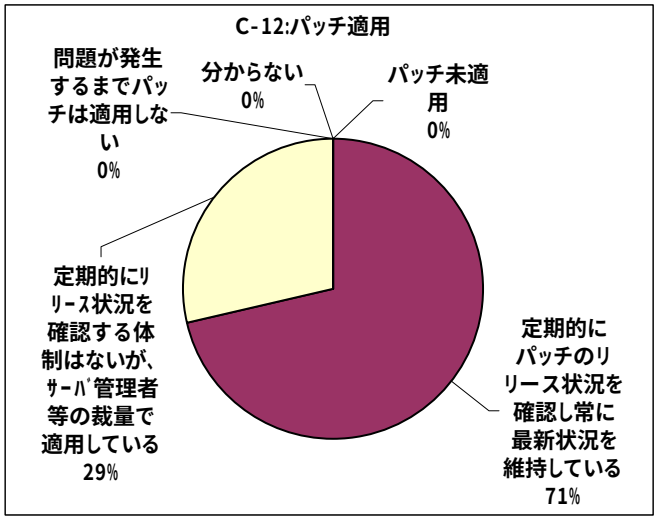



***Note***

情報セキュリティ関連ニュースの収集に関するアンケートでは、行っていない企業はなく Web を使って情報収集していることがわかる。また、情報提供のサービスを受けている企業も約半数近くに及ぶ。

C-12　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）

| | パッチの適用 | 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 | 30 | 71.4% |
| 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 | 12 | 28.6% |
| 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% |

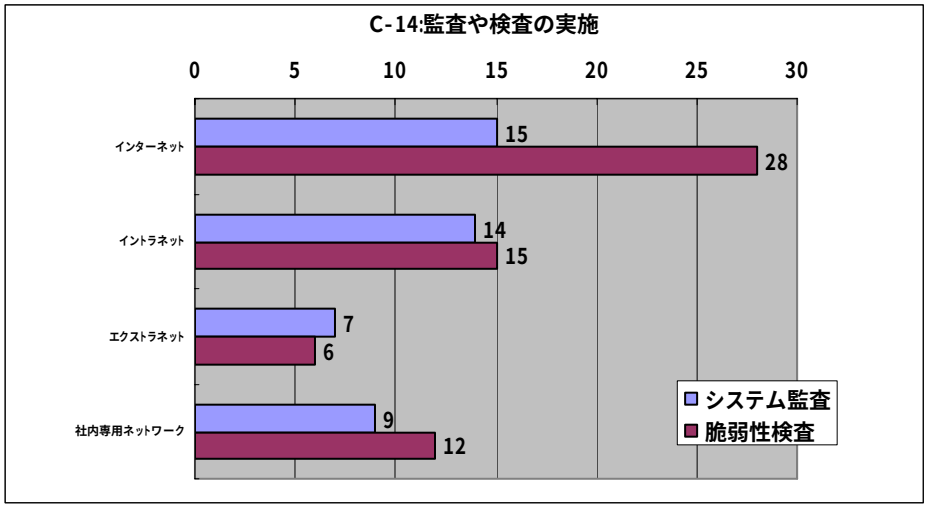



***Note***

パッチの適用に関しては、ヒアリング時にもかなり気を使っているのを感じる事が多い。パッチを当てることによるシステムの停止などの不具合が心配されるからである。それを踏まえても 71%の企業で最新状態を維持しているという回答は、パッチを当てないリスクの方が大きいと考える企業が多いのであろう。

C-13　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 | 脆弱性検査 |
|---|---|---|
| インターネット | 15 | 28 |
| イントラネット | 14 | 15 |
| エクストラネット | 7 | 6 |
| 社内専用ネットワーク | 9 | 12 |

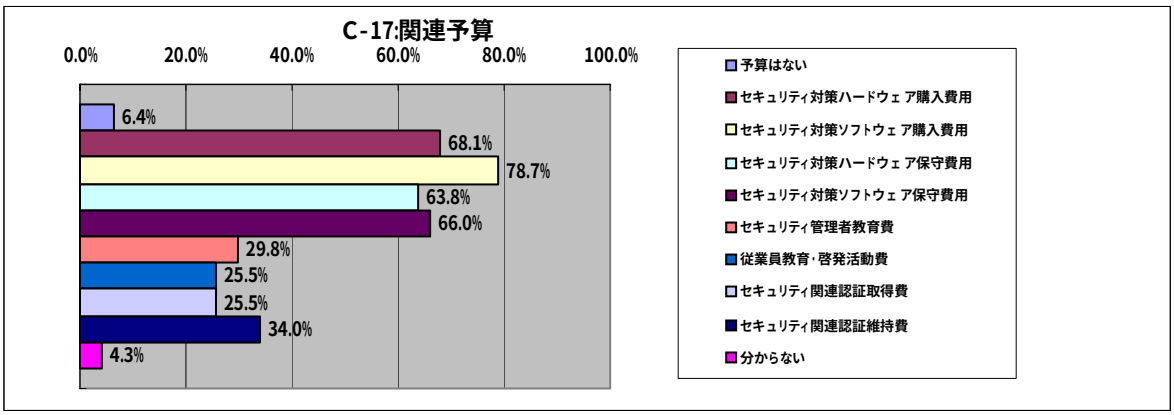



***Note***

インターネットゾーンでの脆弱性検査の件数が、他の約 2 倍になっており外部からの侵入に備える企業の姿勢が見える。

C-17　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）

| | 情報セキュリティ関連予算の対象 | 件数 | 割合 |
|---|---|---|---|
| 1 | 予算はない | 3 | 6.4% |
| 2 | セキュリティ対策ハードウェア購入費用 | 32 | 68.1% |
| 3 | セキュリティ対策ソフトウェア購入費用 | 37 | 78.7% |
| 4 | セキュリティ対策ハードウェア保守費用 | 30 | 63.8% |
| 5 | セキュリティ対策ソフトウェア保守費用 | 31 | 66.0% |
| 6 | セキュリティ管理者教育費 | 14 | 29.8% |
| 7 | 従業員教育･啓発活動費 | 12 | 25.5% |
| 8 | セキュリティ関連認証取得費 | 12 | 25.5% |
| 9 | セキュリティ関連認証維持費 | 16 | 34.0% |
| 10 | 分からない | 2 | 4.3% |

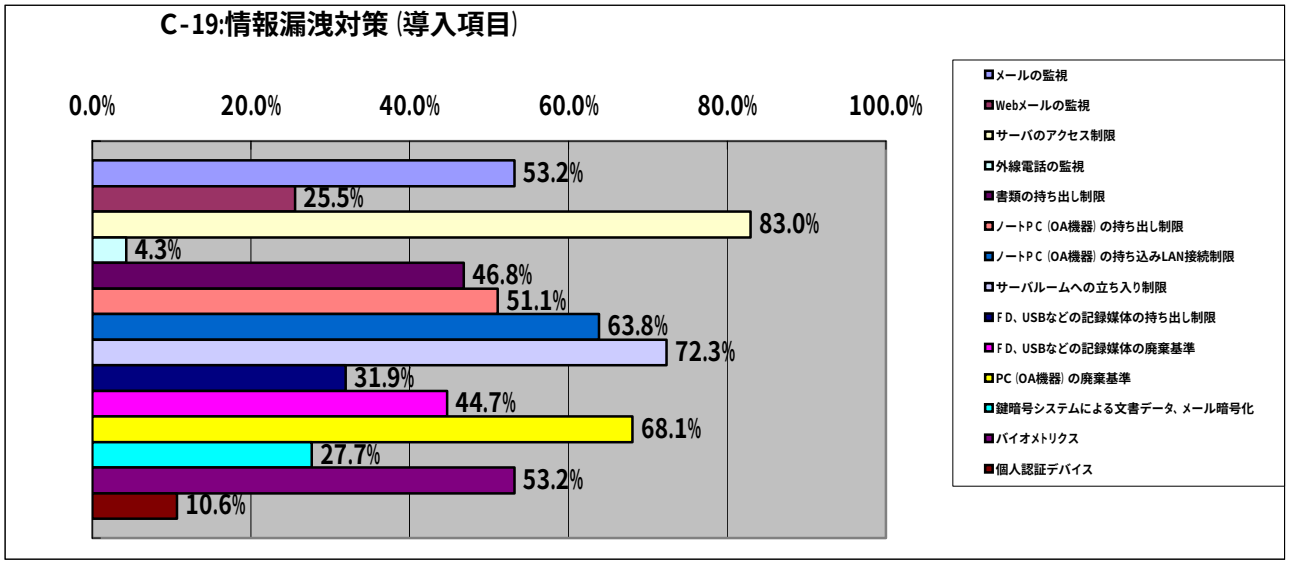



***Note***

情報セキュリティ関連予算が無いと回答のあった企業が 3 社あった。その他ではハードウェア、ソフトウェアとも購入、保守は同程度の割合になっている。

C-19　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。（導入項目）（該当全てに○をお付け下さい）

| | 情報漏洩防止対策 | 件数 | 割合 |
|---|---|---|---|
| 1 | メールの監視 | 25 | 53.2% |
| 2 | Web メールの監視 | 12 | 25.5% |
| 3 | サーバのアクセス制限 | 39 | 83.0% |
| 4 | 外線電話の監視 | 2 | 4.3% |
| 5 | 書類の持ち出し制限 | 22 | 46.8% |
| 6 | ノートＰＣ（OA 機器）の持ち出し制限 | 24 | 51.1% |
| 7 | ノートＰＣ（OA 機器）の持ち込み LAN 接続制限 | 30 | 63.8% |
| 8 | サーバルームへの立ち入り制限 | 34 | 72.3% |
| 9 | ＦＤ、USB などの記録媒体の持ち出し制限 | 15 | 31.9% |
| 10 | ＦＤ、USB などの記録媒体の廃棄基準 | 21 | 44.7% |
| 11 | PC（OA 機器）の廃棄基準 | 32 | 68.1% |
| 12 | 鍵暗号システムによる文書データ、メール暗号化 | 13 | 27.7% |
| 13 | バイオメトリクス | 25 | 53.2% |
| 14 | 個人認証デバイス | 5 | 10.6% |



| | 情報漏洩防止対策（最近1年以内に導入） | 件数 | 割合 |
|---|---|---|---|
| 1 | メールの監視 | 4 | 8.5% |
| 2 | Web メールの監視 | 2 | 4.3% |
| 3 | サーバのアクセス制限 | 2 | 4.3% |
| 4 | 外線電話の監視 | 0 | 0.0% |
| 5 | 書類の持ち出し制限 | 3 | 6.4% |
| 6 | ノートＰＣ（OA 機器）の持ち出し制限 | 3 | 6.4% |
| 7 | ノートＰＣ（OA 機器）の持ち込み LAN 接続制限 | 4 | 8.5% |
| 8 | サーバルームへの立ち入り制限 | 2 | 4.3% |
| 9 | ＦＤ、USB などの記録媒体の持ち出し制限 | 2 | 4.3% |
| 10 | ＦＤ、USB などの記録媒体の廃棄基準 | 2 | 4.3% |
| 11 | PC（OA 機器）の廃棄基準 | 3 | 6.4% |
| 12 | 鍵暗号システムによる文書データ、メール暗号化 | 3 | 6.4% |
| 13 | バイオメトリクス | 2 | 4.3% |
| 14 | 個人認証デバイス | 2 | 4.3% |

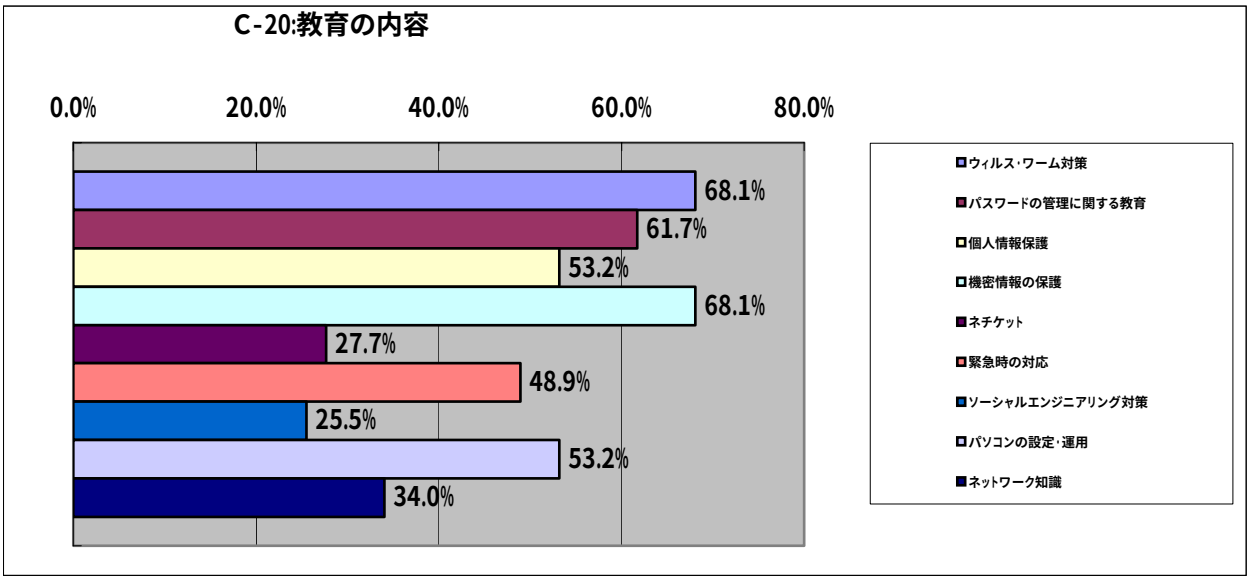
| | 情報漏洩防止対策（事故を契機に導入） | 件数 | 割合 |
|---|---|---|---|
| 1 | メールの監視 | 0 | 0.0% |
| 2 | Web メールの監視 | 0 | 0.0% |
| 3 | サーバのアクセス制限 | 0 | 0.0% |
| 4 | 外線電話の監視 | 0 | 0.0% |
| 5 | 書類の持ち出し制限 | 1 | 2.1% |
| 6 | ノートＰＣ（OA 機器）の持ち出し制限 | 1 | 2.1% |
| 7 | ノートＰＣ（OA 機器）の持ち込み LAN 接続制限 | 0 | 0.0% |
| 8 | サーバルームへの立ち入り制限 | 0 | 0.0% |
| 9 | ＦＤ、USB などの記録媒体の持ち出し制限 | 0 | 0.0% |
| 10 | ＦＤ、USB などの記録媒体の廃棄基準 | 0 | 0.0% |
| 11 | PC（OA 機器）の廃棄基準 | 0 | 0.0% |
| 12 | 鍵暗号システムによる文書データ、メール暗号化 | 0 | 0.0% |
| 13 | バイオメトリクス | 0 | 0.0% |
| 14 | 個人認証デバイス | 0 | 0.0% |

***Note***

情報漏洩防止対策としては、「サーバのアクセス制限」「サーバルームへの立ち入り制限」といったサーバのデータに対する保護が上位にきている。「ノート PC の持ち込み LAN 接続制限」が 4 番目に入っているのは、最近のウイルス感染ルートの変化に対する対応と見られる。

C-20　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)

| | 情報セキュリティ教育の内容 | 件数 | 割合 |
|---|---|---|---|
| 1 | ウイルス･ワーム対策 | 32 | 68.1% |
| 2 | パスワードの管理に関する教育 | 29 | 61.7% |
| 3 | 個人情報保護 | 25 | 53.2% |
| 4 | 機密情報の保護 | 32 | 68.1% |
| 5 | ネチケット | 13 | 27.7% |
| 6 | 緊急時の対応 | 23 | 48.9% |
| 7 | ソーシャルエンジニアリング対策 | 12 | 25.5% |
| 8 | パソコンの設定･運用 | 25 | 53.2% |
| 9 | ネットワーク知識 | 16 | 34.0% |




***Note***

「ネチケット」「ソーシャルエンジニアリング対策」は 20%台であるが、その他の項目は 50%を越えている項目もあり、企業が網羅的に教育に取り組んでいることがわかる。

C-21　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)

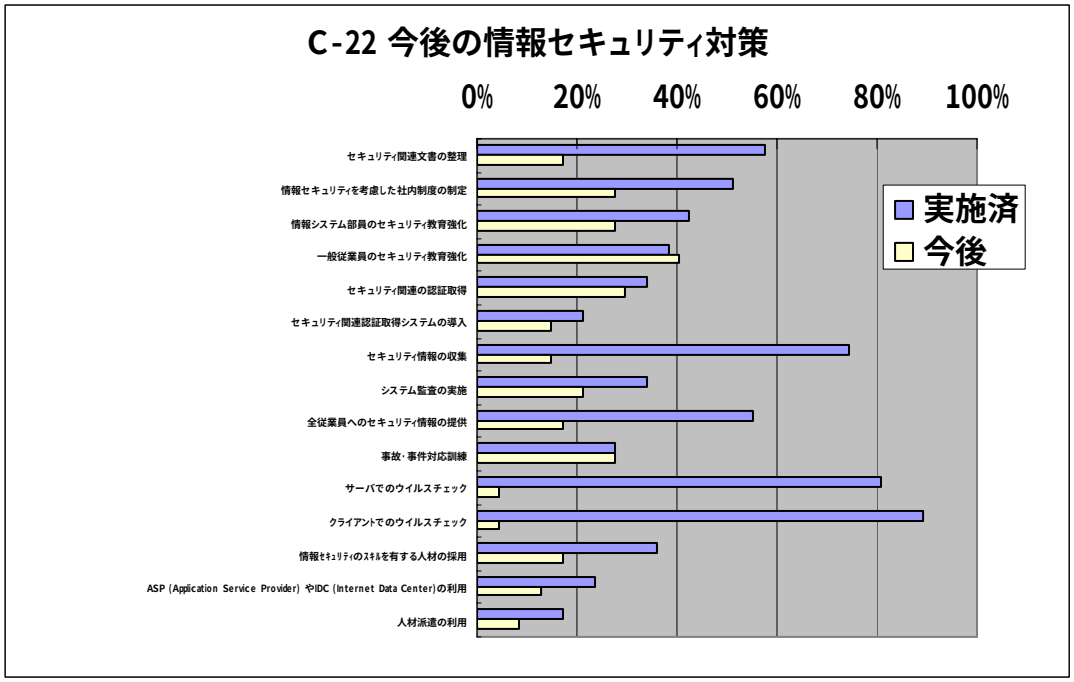
| | 教　育　内　容 | 平均人数 | 平均年回数 |
|---|---|---|---|
| 1 | 一般従業員 (ユーザー教育) 向け教育 | 1,659 | 2 |
| 2 | マネージャー向け教育 | 69 | 1 |
| 3 | 専門家向け教育 | 258 | 3 |

***Note***

情報セキュリティ教育の回数は、専門家、一般従業員、マネージャーの順で回数が多い傾向にある。

C-22　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)

| | 今後の情報セキュリティ関連対策 | 実施済 | 割合 | 今後 | 割合 |
|---|---|---|---|---|---|
| 1 | セキュリティ関連文書の整理 | 27 | 57.4% | 8 | 17.0% |
| 2 | 情報セキュリティを考慮した社内制度の制定 | 24 | 51.1% | 13 | 27.7% |
| 3 | 情報システム部員のセキュリティ教育強化 | 20 | 42.6% | 13 | 27.7% |
| 4 | 一般従業員のセキュリティ教育強化 | 18 | 38.3% | 19 | 40.4% |
| 5 | セキュリティ関連の認証取得 | 16 | 34.0% | 14 | 29.8% |
| 6 | セキュリティ関連認証取得システムの導入 | 10 | 21.3% | 7 | 14.9% |
| 7 | セキュリティ情報の収集 | 35 | 74.5% | 7 | 14.9% |
| 8 | システム監査の実施 | 16 | 34.0% | 10 | 21.3% |
| 9 | 全従業員へのセキュリティ情報の提供 | 26 | 55.3% | 8 | 17.0% |
| 10 | 事故･事件対応訓練 | 13 | 27.7% | 13 | 27.7% |
| 11 | サーバでのウイルスチェック | 38 | 80.9% | 2 | 4.3% |
| 12 | クライアントでのウイルスチェック | 42 | 89.4% | 2 | 4.3% |
| 13 | 情報ｾｷｭﾘﾃｨのｽｷﾙを有する人材の採用 | 17 | 36.2% | 8 | 17.0% |
| 14 | ASP (Application Service Provider) や IDC (Internet Data Center)の利用 | 11 | 23.4% | 6 | 12.8% |
| 15 | 人材派遣の利用 | 8 | 17.0% | 4 | 8.5% |




***Note***

情報セキュリティ対策については、「今後実施したい」割合が「実施済み」を越えているのが「一般従業員のセキュリティ教育強化」だけである。次が「事件・事故対応訓練」となっており、一般的な情報セキュリティ対策については、ほぼ終えている JNSA 会員企業の特徴が出ている。

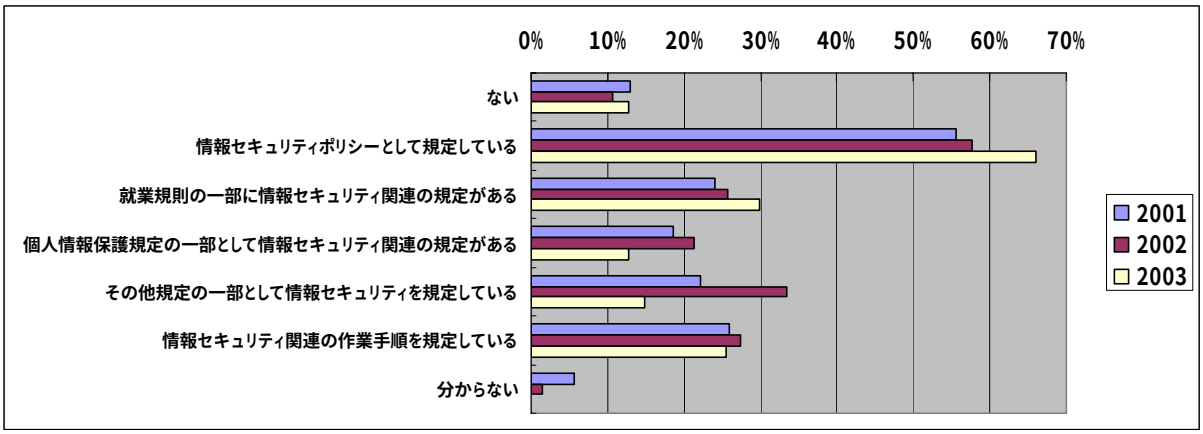
### 3.4.2　過去 2 年間の調査結果と今年度調査結果の比較

本調査も 3 年目になり、過去の調査結果と本年 2003 年度の調査結果を比較してみた。過去 2 年の調査対象が JNSA 会員企業を中心になっていたので、2003 年度も JNSA 会員企業（一部非会員を含む）を中心のデータを使用している。

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 | | 2002 | | 2003 | |
|---|---|---|---|---|---|---|---|
| 1 | ない | 7 | 13.0% | 7 | 10.6% | 6 | 12.8% |
| 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% | 31 | 66.0% |
| 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% | 14 | 29.8% |
| 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% | 6 | 12.8% |
| 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% | 7 | 14.9% |
| 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% | 12 | 25.5% |
| 7 | 分からない | 3 | 5.6% | 1 | 1.5% | 0 | 0.0% |

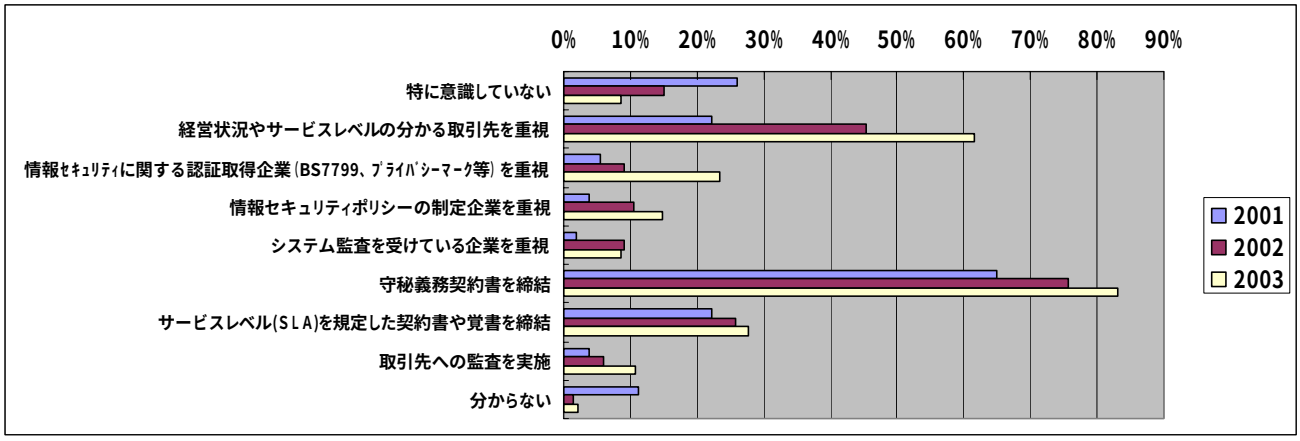



***Note***

傾向としては、情報セキュリティポリシーの伸びが目に付く。2002 年度は既存の規定に情報セキュリティ関連の規定を盛り込んでいる傾向が見られたが、2003 年には情報セキュリティポリシーに集約しているようにも見える。

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 | | 2002 | | 2003 | |
|---|---|---|---|---|---|---|---|
| 1 | 特に意識していない | 14 | 25.9% | 10 | 15.2% | 4 | 8.5% |
| 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% | 29 | 61.7% |
| 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% | 11 | 23.4% |
| 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% | 7 | 14.9% |
| 5 | システム監査を受けている企業を重視 | 1 | 1.9% | 6 | 9.1% | 4 | 8.5% |
| 6 | 守秘義務契約書を締結 | 35 | 64.8% | 50 | 75.8% | 39 | 83.0% |
| 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% | 13 | 27.7% |
| 8 | 取引先への監査を実施 | 2 | 3.7% | 4 | 6.1% | 5 | 10.6% |
| 9 | 分からない | 6 | 11.1% | 1 | 1.5% | 1 | 2.1% |

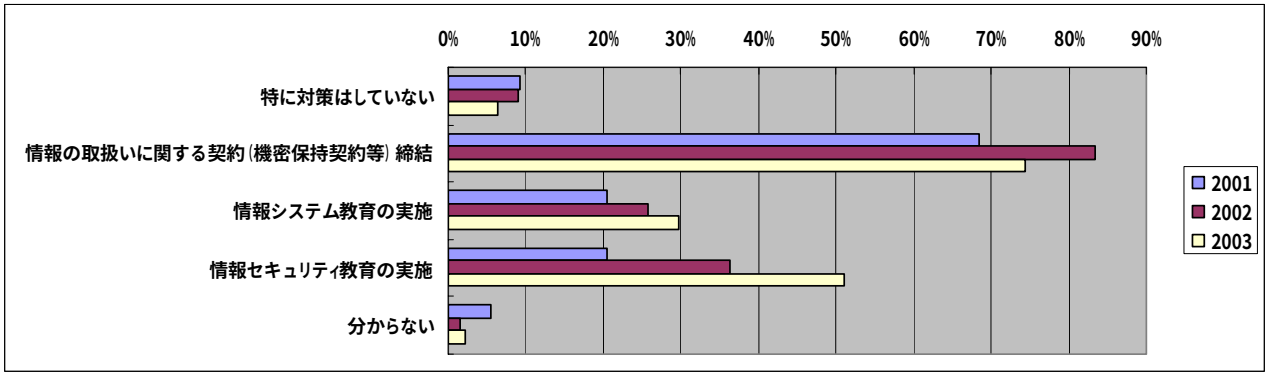



***Note***

「特に意識していない」が減少し、その他の項目は概ね増加傾向にある。全体のパーセンテージは 23%であるが、認証取得企業を重視するという項目が 2002 年度より 2 倍以上になっているのが注目される。

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）

| | | 2001 | | 2002 | | 2003 | |
|---|---|---|---|---|---|---|---|
| 1 | 特に対策はしていない | 5 | 9.3% | 6 | 9.1% | 3 | 6.4% |
| 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% | 35 | 74.5% |
| 3 | 情報システム教育の実施 | 11 | 20.4% | 17 | 25.8% | 14 | 29.8% |
| 4 | 情報セキュリティ教育の実施 | 11 | 20.4% | 24 | 36.4% | 24 | 51.1% |
| 5 | 分からない | 3 | 5.6% | 1 | 1.5% | 1 | 2.1% |

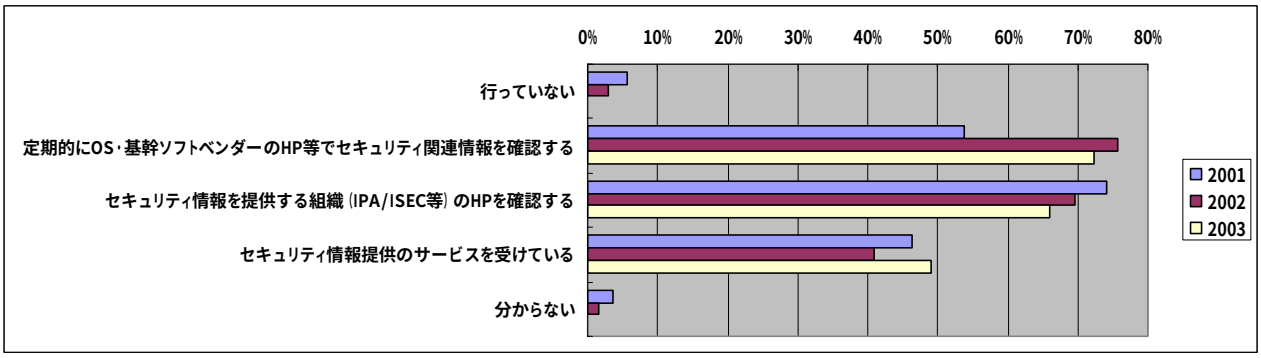



***Note***

情報システム教育・情報セキュリティ教育がこの 3 年間で増加している。特に情報セキュリティ教育は 2001 年の 20%から 2003 年は 51%まで増加している。企業が正社員以外の人員にも教育に注力しているのがわかる。

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 | | 2002 | | 2003 | |
|---|---|---|---|---|---|---|---|
| 1 | 行っていない | 3 | 5.6% | 2 | 3.0% | 0 | 0.0% |
| 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% | 34 | 72.3% |
| 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% | 31 | 66.0% |
| 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% | 23 | 48.9% |
| 5 | 分からない | 2 | 3.7% | 1 | 1.5% | 0 | 0.0% |

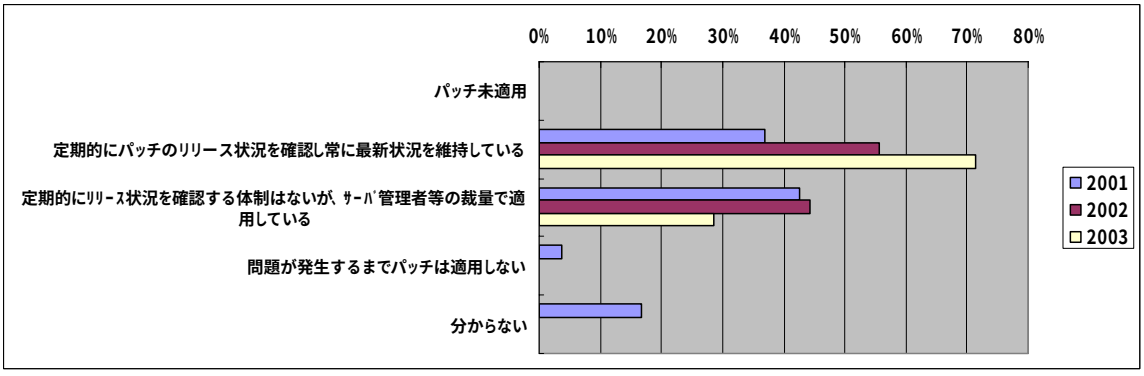



***Note***

2003 年度には、情報セキュリティ関連ニュースを収集していない企業はなくなったが、全体としては、大きな変化は見られない。

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 | | 2002 | | 2003 年 | |
|---|---|---|---|---|---|---|---|
| 1 | パッチ未適用 | 0 | 0.0% | 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% | 30 | 71.4% |
| 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% | 12 | 28.6% |
| 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% | 0 | 0.0% |
| 5 | 分からない | 9 | 16.7% | 0 | 0.0% | 0 | 0.0% |




***Note***

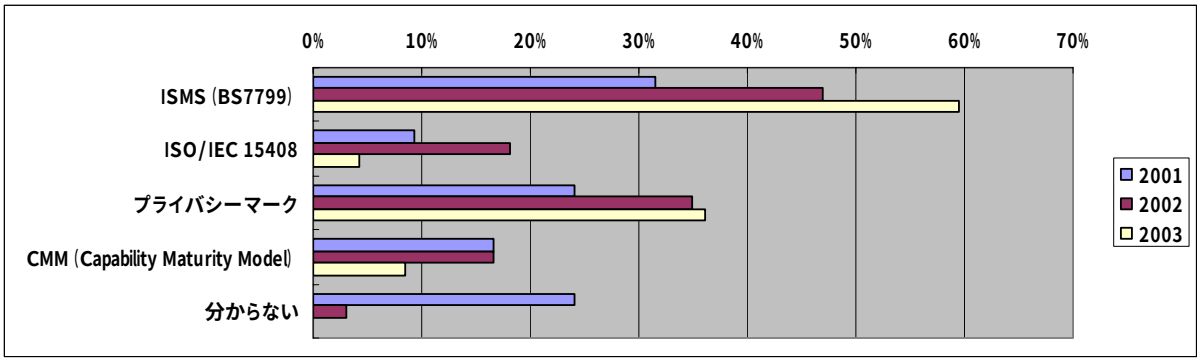
サーバに対するパッチ当てに関しては、大きく傾向が変化している。最新の状況に維持しているという回答が、2001 年度と比較すると 2 倍近く増加している。

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 | | | | | |
|---|---|---|---|---|---|
| | 名称 | 計画中 | 割合 | 取得済み | 割合 |
| 1 | ISMS (BS7799) | 14 | 25.9% | 3 | 5.6% |
| 2 | ISO/IEC 15408 | 5 | 9.3% | 0 | 0.0% |
| 3 | プライバシーマーク | 4 | 7.4% | 9 | 16.7% |
| 4 | CMM (Capability Maturity Model) | 8 | 14.8% | 1 | 1.9% |
| 5 | 分からない | 13 | 24.1% | 0 | 0.0% |

| 2002 | | | | | |
|---|---|---|---|---|---|
| | 名称 | 計画中 | 割合 | 取得済み | 割合 |
| 1 | ISMS (BS7799) | 21 | 31.8% | 10 | 15.2% |
| 2 | ISO/IEC 15408 | 7 | 10.6% | 5 | 7.6% |
| 3 | プライバシーマーク | 11 | 16.7% | 12 | 18.2% |
| 4 | CMM (Capability Maturity Model) | 9 | 13.6% | 2 | 3.0% |
| 5 | 分からない | 1 | 1.5% | 1 | 1.5% |

| 2003 | | | | | |
|---|---|---|---|---|---|
| | 名称 | 計画中 | 割合 | 取得済み | 割合 |
| 1 | ISMS (BS7799) | 12 | 25.5% | 16 | 34.0% |
| 2 | ISO/IEC 15408 | 1 | 2.1% | 1 | 2.1% |
| 3 | プライバシーマーク | 9 | 19.1% | 8 | 17.0% |
| 4 | CMM (Capability Maturity Model) | 1 | 2.1% | 3 | 6.4% |
| 5 | 分からない | 0 | 0.0% | 0 | 0.0% |

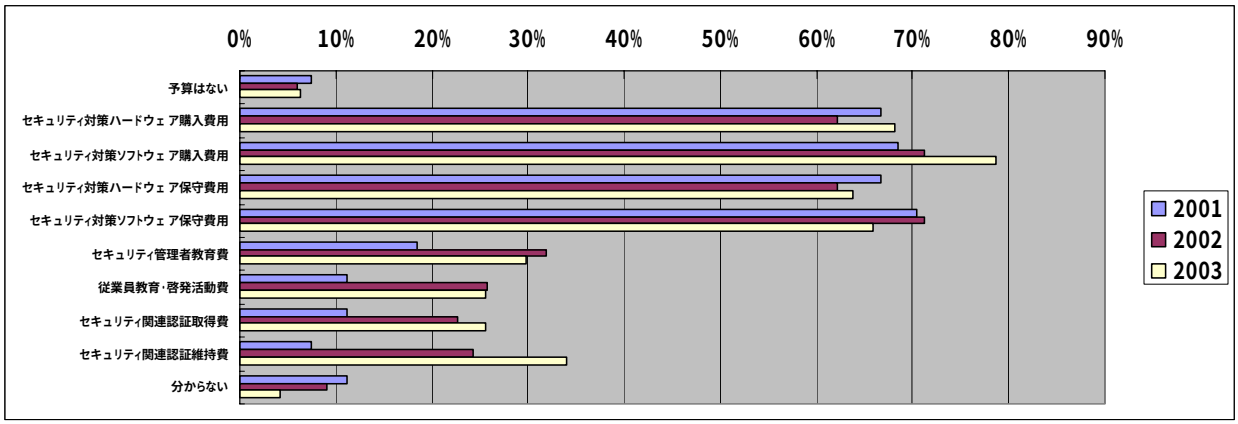



***Note***

上記グラフは、取得済みと計画中の合計で比較をおこなっている。傾向としては、ISMS とプライバシーマークが増加傾向にある。特に ISMS が 2003 年度に 60%近くまで伸びているのは、調査対象が JNSA 会員企業を中心になっているための特性と思われる。

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 | | 2002 | | 2003 | |
|---|---|---|---|---|---|---|---|
| 1 | 予算はない | 4 | 7.4% | 4 | 6.1% | 3 | 6.4% |
| 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% | 32 | 68.1% |
| 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% | 37 | 78.7% |
| 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% | 30 | 63.8% |
| 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% | 31 | 66.0% |
| 6 | セキュリティ管理者教育費 | 10 | 18.5% | 21 | 31.8% | 14 | 29.8% |
| 7 | 従業員教育･啓発活動費 | 6 | 11.1% | 17 | 25.8% | 12 | 25.5% |
| 8 | セキュリティ関連認証取得費 | 6 | 11.1% | 15 | 22.7% | 12 | 25.5% |
| 9 | セキュリティ関連認証維持費 | 4 | 7.4% | 16 | 24.2% | 16 | 34.0% |
| 10 | 分からない | 6 | 11.1% | 6 | 9.1% | 2 | 4.3% |

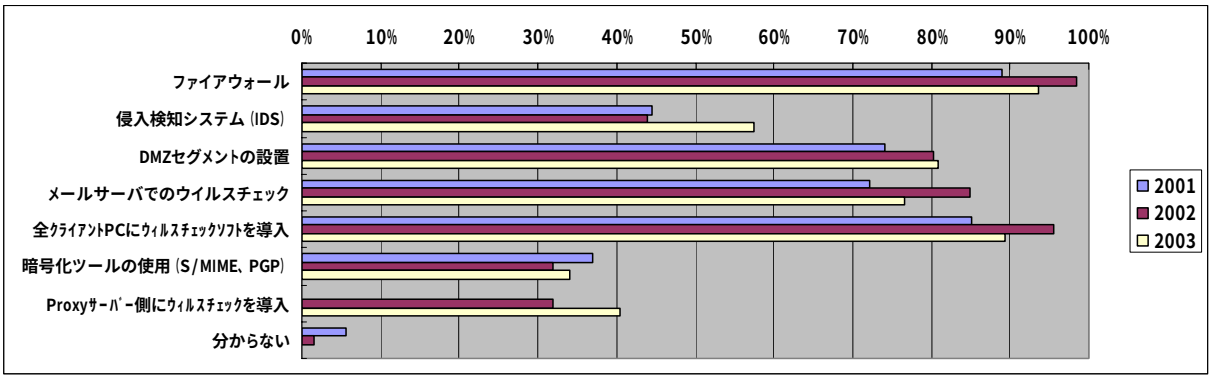



***Note***

この 3 年間では認証関連が増加傾向にあるが、その他の項目における大きな変化は見られない。

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 | | 2002 | | 2003 | |
|---|---|---|---|---|---|---|---|
| 1 | ファイアウォール | 48 | 88.9% | 65 | 98.5% | 44 | 93.6% |
| 2 | 侵入検知システム (IDS) | 24 | 44.4% | 29 | 43.9% | 27 | 57.4% |
| 3 | DMZ セグメントの設置 | 40 | 74.1% | 53 | 80.3% | 38 | 80.9% |
| 4 | メールサーバでのウイルスチェック | 39 | 72.2% | 56 | 84.8% | 36 | 76.6% |
| 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% | 42 | 89.4% |
| 6 | 暗号化ツールの使用 (S/MIME、PGP) | 20 | 37.0% | 21 | 31.8% | 16 | 34.0% |
| 7 | Proxy ｻｰﾊﾞ側にウイルスﾁｪｯｸを導入 | - | - | 21 | 31.8% | 19 | 40.4% |
| 8 | 分からない | 3 | 5.6% | 1 | 1.5% | 0 | 0.0% |




***Note***

技術的な対策に関しては、各項目とも大きな変化は見られない。2002 年度と比較すると侵入検知システム（IDS）が増加している。

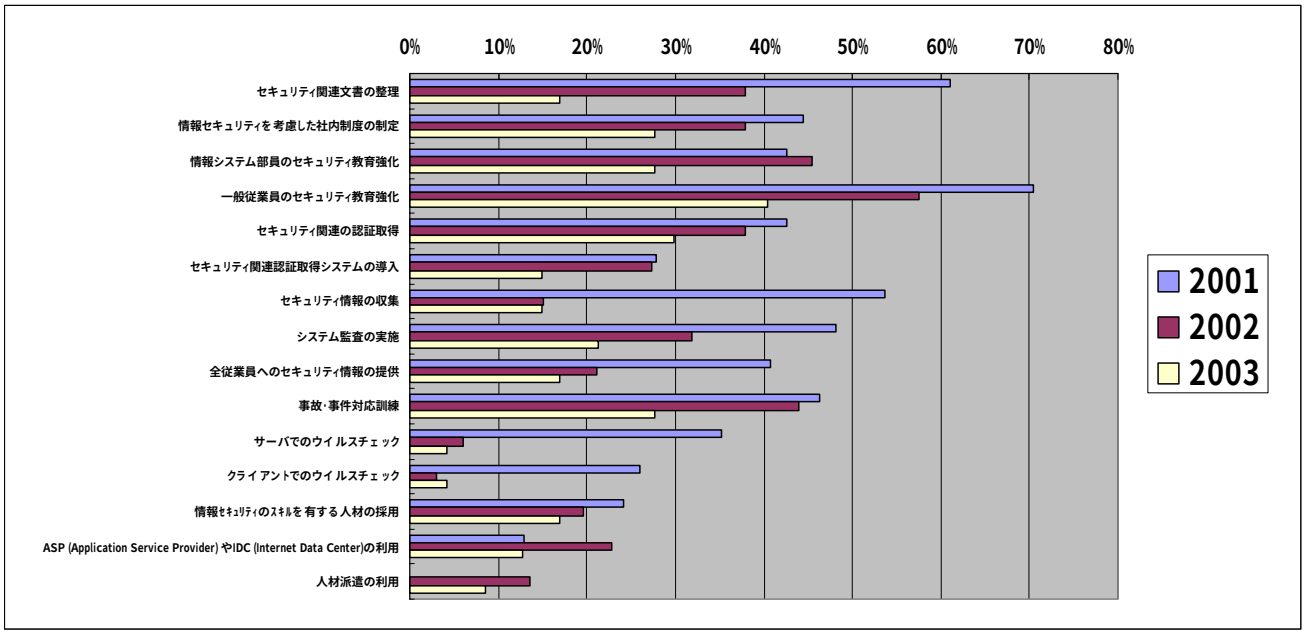
C-19 現在実施、また今後実施していきたいと考えている情報セキュリティ関連対策(該当全て)

| 2001 | | | |
|---|---|---|---|
| | | 今後 | 割合 |
| 1 | セキュリティ関連文書の整理 | 33 | 61.1% |
| 2 | 情報セキュリティを考慮した社内制度の制定 | 24 | 44.4% |
| 3 | 情報システム部員のセキュリティ教育強化 | 23 | 42.6% |
| 4 | 一般従業員のセキュリティ教育強化 | 38 | 70.4% |
| 5 | セキュリティ関連の認証取得 | 23 | 42.6% |
| 6 | セキュリティ関連認証取得システムの導入 | 15 | 27.8% |
| 7 | セキュリティ情報の収集 | 29 | 53.7% |
| 8 | システム監査の実施 | 26 | 48.1% |
| 9 | 全従業員へのセキュリティ情報の提供 | 22 | 40.7% |
| 10 | 事故･事件対応訓練 | 25 | 46.3% |
| 11 | サーバでのウイルスチェック | 19 | 35.2% |
| 12 | クライアントでのウイルスチェック | 14 | 25.9% |
| 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% |
| 14 | ASP(Application Service Provider)や IDC(Internet Data Center)の利用 | 7 | 13.0% |
| 15 | 人材派遣の利用 | 0 | 0.0% |

| 2002 | | | | | |
|---|---|---|---|---|---|
| | | 実施済 | 割合 | 今後 | 割合 |
| 1 | セキュリティ関連文書の整理 | 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 | 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 | 21 | 31.8% | 30 | 45.5% |
| 4 | 一般従業員のセキュリティ教育強化 | 21 | 31.8% | 38 | 57.6% |
| 5 | セキュリティ関連の認証取得 | 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 | 5 | 7.6% | 18 | 27.3% |
| 7 | セキュリティ情報の収集 | 44 | 66.7% | 10 | 15.2% |
| 8 | システム監査の実施 | 20 | 30.3% | 21 | 31.8% |
| 9 | 全従業員へのセキュリティ情報の提供 | 38 | 57.6% | 14 | 21.2% |
| 10 | 事故･事件対応訓練 | 9 | 13.6% | 29 | 43.9% |
| 11 | サーバでのウイルスチェック | 56 | 84.8% | 4 | 6.1% |
| 12 | クライアントでのウイルスチェック | 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 | 20 | 30.3% | 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% |

| 2003 | | | | | |
|---|---|---|---|---|---|
| | | 実施済 | 割合 | 今後 | 割合 |
| 1 | セキュリティ関連文書の整理 | 27 | 57.4% | 8 | 17.0% |
| 2 | 情報セキュリティを考慮した社内制度の制定 | 24 | 51.1% | 13 | 27.7% |
| 3 | 情報システム部員のセキュリティ教育強化 | 20 | 42.6% | 13 | 27.7% |
| 4 | 一般従業員のセキュリティ教育強化 | 18 | 38.3% | 19 | 40.4% |
| 5 | セキュリティ関連の認証取得 | 16 | 34.0% | 14 | 29.8% |
| 6 | セキュリティ関連認証取得システムの導入 | 10 | 21.3% | 7 | 14.9% |

| | | | | | |
|---|---|---|---|---|---|
| 7 | セキュリティ情報の収集 | 35 | 74.5% | 7 | 14.9% |
| 8 | システム監査の実施 | 16 | 34.0% | 10 | 21.3% |
| 9 | 全従業員へのセキュリティ情報の提供 | 26 | 55.3% | 8 | 17.0% |
| 10 | 事故･事件対応訓練 | 13 | 27.7% | 13 | 27.7% |
| 11 | サーバでのウイルスチェック | 38 | 80.9% | 2 | 4.3% |
| 12 | クライアントでのウイルスチェック | 42 | 89.4% | 2 | 4.3% |
| 13 | 情報ｾｷｭﾘﾃｨのｽｷﾙを有する人材の採用 | 17 | 36.2% | 8 | 17.0% |
| 14 | ASP(Application Service Provider)や IDC(Internet Data Center)の利用 | 11 | 23.4% | 6 | 12.8% |
| 15 | 人材派遣の利用 | 8 | 17.0% | 4 | 8.5% |




***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。2001 年には 50%を越える項目が 3 項目あったが、2003 年度の調査では一番多い項目でも 40%になっている。情報セキュリティ対策が整備されつつあるのが、このグラフから読み取れる。

### 3.4.3 被害状況の概要

2003 年度の被害調査アンケートでは、113 件のインシデントが集まった。業種別では、製造業が一番多く 59 件と 50%を越えている。被害の種類別では、MSBlaster が 69 件で 60%を占めている。

下記の被害状況の表では、直接被害・間接被害・潜在化被害の合計金額だけを表示しているが、被害額の算出方法の例を示す。(注：被害額を計算する要素は、第 6 章で説明しているように他にもあるが、今回のアンケートでは充分な情報を収集していないため割愛している。)

**例１）No.14 の直接被害額と潜在化被害額の計算例**

●直接被害額は、A+B で 1.160.445 円となる。

システムの時間当たりの売上額×想定利益率×復旧時間 ＝ 逸失利益

A.年間売上 240,000,000 円÷365 日÷24 時間×想定利益率 20%×復旧時間 27 時間＝147,945 円

復旧完了までの日数×復旧に携わった人数×従業員一人当たりの人件費 ＝ 復旧に要したコスト

B.復旧完了まで 27 時間÷8 時間×20 人×一人当たりの人件費 15,000 円＝1,012,500 円

●潜在化被害額は、6,075,000 円となる。

従業員一人当たりの人件費×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）×停止日数 ＝ 潜在化被害額

一人当たりの人件費 15,000 円×影響を受けた人数 600 人

×IT 感応度 0.2×停止時間 27 時間÷8 時間＝6,075,000 円

**例２）No.34 の直接被害額と間接被害額の計算例**

●直接被害額は、2,250,000 円となる。

復旧完了までの日数×復旧に携わった人数×従業員一人当たりの人件費 ＝ 復旧に要したコスト

復旧完了まで 24 時間÷8 時間×25 人×一人当たりの人件費 30,000 円＝2,250,000 円

●間接被害額は、3,000,000 円となる。

賠償・補償額やお詫び広告など ＝ 間接被害額

賠償・補償額として 3,000,000 円＝3,000,000 円

**① 被害状況（インシデント毎の被害額）**

| No. | 業種 | 直接被害 | 間接被害 | 潜在化被害 | 被害合計 | 被害 | 備考 |
|---|---|---|---|---|---|---|---|
| 1 | 製造 | 450,000 | 0 | 54,000 | 504,000 | MSBlaster | *1 |
| 2 | 製造 | 0 | 0 | 0 | 0 | MSBlaster | *3 |
| 3 | 製造 | 1,300,000 | 0 | 3,200,000 | 4,500,000 | MSBlaster | |
| 4 | 製造 | 1,350,000 | 0 | 3,150,000 | 4,500,000 | MSBlaster | *1 |
| 5 | 製造 | 4,500,000 | 0 | 0 | 4,500,000 | MSBlaster | *1 |

| No. | 業種 | 直接被害 | 間接被害 | 潜在化被害 | 被害合計 | 被害 | 備考 |
|---|---|---|---|---|---|---|---|
| 6 | 製造 | 4,500,000 | 0 | 0 | 4,500,000 | MSBlaster | *1 |
| 7 | 製造 | 140,000 | 0 | 1,400,000 | 1,540,000 | MSBlaster | |
| 8 | 製造 | 3,600,000 | 0 | 600,000 | 4,200,000 | MSBlasterR | |
| 9 | 製造 | 1,800,000 | 0 | 1,800,000 | 3,600,000 | MSBlaster | |
| 10 | その他サービス | 1,575,000 | 0 | 31,500,000 | 33,075,000 | その他のウイルス被害 | Nachi*4 |
| 11 | その他サービス | 0 | 0 | 0 | 0 | MSBlaster | *3 |
| 12 | 金融（銀行、保険、証券等） | 13,500,000 | 0 | 3,780,000 | 17,280,000 | MSBlaster | *1 |
| 13 | 建設 | 2,350,000 | 0 | 30,000,000 | 32,350,000 | MSBlaster | |
| 14 | 製造 | 1,160,445 | 0 | 6,075,000 | 7,235,445 | MSBlaster | |
| 15 | 金融（銀行、保険、証券等） | 0 | 0 | 0 | 0 | KLEZ | *3 |
| 16 | 金融（銀行、保険、証券等） | 0 | 0 | 0 | 0 | SOBIG | *3 |
| 17 | 金融（銀行、保険、証券等） | 0 | 0 | 0 | 0 | BUGBEAR | *3 |
| 18 | 医療・製薬 | 0 | 0 | 30,000,000 | 30,000,000 | MSBlaster | *1 |
| 19 | 建設 | 37,500 | 0 | 0 | 37,500 | Sircam | |
| 20 | 製造 | 8,000,000 | 0 | 7,500,000 | 15,500,000 | MSBlaster | |
| 21 | 製造 | 0 | 0 | 0 | 0 | MSBlaster | *3 |
| 22 | 製造 | 3,750 | 0 | 0 | 3,750 | MSBlaster | |
| 23 | 製造 | 112,500 | 0 | 225,000 | 337,500 | MSBlaster | *1 |
| 24 | 製造 | 3,750 | 0 | 0 | 3,750 | DoS 攻撃等でｻｰﾋﾞｽ停止 | |
| 25 | 製造 | 600,000 | 0 | 0 | 600,000 | MSBlaster | |
| 26 | 製造 | 56,250 | 0 | 0 | 56,250 | MSBlaster | *1 |
| 27 | 製造 | 951,000 | 0 | 0 | 951,000 | MSBlaster | |
| 28 | 製造 | 0 | 0 | 0 | 0 | BUGBEAR | *2 |
| 29 | 製造 | 15,000 | 0 | 6,750,000 | 6,765,000 | MSBlaster | *1 |
| 30 | 建設 | 112,500 | 0 | 225,000 | 337,500 | KLEZ | *1 |
| 31 | 製造 | 900,000 | 0 | 75,000 | 975,000 | その他のウイルス被害 | *1 |
| 32 | 製造 | 3,000,000 | 0 | 0 | 3,000,000 | MSBlaster | |
| 33 | その他サービス | 200,000 | 0 | 0 | 200,000 | DoS 攻撃等でｻｰﾋﾞｽ停止 | |
| 34 | 製造 | 2,250,000 | 3,000,000 | 0 | 5,250,000 | KLEZ | |
| 35 | 製造 | 75,000 | 0 | 0 | 75,000 | その他のウイルス被害 | |
| 36 | 金融（銀行、保険、証券等） | 45,000 | 0 | 0 | 45,000 | その他のウイルス被害 | |
| 37 | 金融（銀行、保険、証券等） | 0 | 0 | 0 | 0 | PC/PDA の盗難・紛失 | *2 |
| 38 | 製造 | 93,750 | 0 | 62,500 | 156,250 | MSBlaster | |
| 39 | 製造 | 1,125,000 | 0 | 2,700,000 | 3,825,000 | MSBlaster | |
| 40 | 製造 | 15,500,000 | 0 | 14,000,000 | 29,500,000 | MSBlaster | |
| 41 | 製造 | 0 | 0 | 0 | 0 | SOBIG | *2 |
| 42 | 医療・製薬 | 0 | 0 | 20,000,000 | 20,000,000 | MSBlaster | |
| 43 | 製造 | 90,000 | 0 | 0 | 90,000 | MSBlaster | *1 |
| 44 | その他 | 3,600,000 | 0 | 0 | 3,600,000 | MSBlaster | *1 |
| 45 | 製造 | 20,000 | 0 | 0 | 20,000 | MSBlaster | |
| 46 | 製造 | 0 | 0 | 0 | 0 | BUGBEAR | *2 |
| 47 | 製造 | 0 | 0 | 0 | 0 | KLEZ | *2 |
| 48 | 製造 | 0 | 0 | 0 | 0 | MSBlaster | *3 |
| 49 | 製造 | 156,250 | 0 | 3,125,000 | 3,281,250 | MSBlaster | |

| No. | 業種 | 直接被害 | 間接被害 | 潜在化被害 | 被害合計 | 被害 | 備考 | |
|---|---|---|---|---|---|---|---|---|
| 50 | 製造 | 37,500 | 0 | 125,000 | 162,500 | その他のウイルス被害 | | Nachi*4 |
| 51 | 建設 | 2,940,000 | 0 | 0 | 2,940,000 | MSBlaster | | |
| 52 | 製造 | 361,250 | 0 | 2,250,000 | 2,611,250 | MSBlaster | | |
| 53 | 製造 | 0 | 0 | 0 | 0 | MSBlaster | *2 | |
| 54 | 製造 | 18,750 | 0 | 75,000 | 93,750 | MSBlaster | *1 | |
| 55 | 製造 | 45,000 | 0 | 6,000 | 51,000 | その他のウイルス被害 | *1 | |
| 56 | その他サービス | 1,350,000 | 0 | 218,750 | 1,568,750 | MSBlaster | | |
| 57 | 製造 | 7,600,000 | 0 | 0 | 7,600,000 | SOBIG | | |
| 58 | 製造 | 1,080,000 | 0 | 0 | 1,080,000 | その他のウイルス被害 | *1 | Nachi*4 |
| 59 | 製造 | 4,500,000 | 0 | 600,000 | 5,100,000 | MSBlaster | *1 | |
| 60 | その他 | 0 | 0 | 0 | 0 | BUGBEAR | *2 | |
| 61 | 製造 | 1,500,000 | 0 | 0 | 1,500,000 | MSBlaster | | |
| 62 | 製造 | 10,000,000 | 0 | 7,500,000 | 17,500,000 | MSBlaster | *1 | |
| 63 | 建設 | 0 | 0 | 37,500 | 37,500 | KLEZ | *1 | |
| 64 | 製造 | 37,500,000 | 0 | 225,000,000 | 262,500,000 | MSBlaster | | |
| 65 | 建設 | 0 | 0 | 0 | 0 | KLEZ | *3 | |
| 66 | 建設 | 0 | 0 | 0 | 0 | MSBlaster | | |
| 67 | 製造 | 26,250 | 0 | 0 | 26,250 | MSBlaster | | |
| 68 | 情報･通信 | 180,000 | 0 | 0 | 180,000 | MSBlaster | | |
| 69 | 製造 | 1,350,000 | 0 | 36,000,000 | 37,350,000 | MSBlaster | *1 | |
| 70 | 金融（銀行、保険、証券等） | 28,125 | 0 | 0 | 28,125 | 社外公開ﾎｰﾑﾍﾟｰｼﾞ改竄 | | |
| 71 | 製造 | 0 | 0 | 0 | 0 | MSBlaster | *3 | |
| 72 | 医療･製薬 | 13,200,000 | 0 | 0 | 13,200,000 | MSBlaster | | |
| 73 | エネルギー | 37,500,000 | 0 | 0 | 37,500,000 | MSBlaster | | |
| 74 | 製造 | 0 | 0 | 18,750,000 | 18,750,000 | MSBlaster | *2 | |
| 75 | 情報･通信 | 72,000,000 | 0 | 0 | 72,000,000 | MSBlaster | | |
| 76 | 建設 | 0 | 0 | 0 | 0 | MSBlasterR | *2 | |
| 77 | 製造 | 11,600,000 | 0 | 0 | 11,600,000 | その他のウイルス被害 | *1 | Slammer*4 |
| 78 | 製造 | 45,500,000 | 0 | 0 | 45,500,000 | MSBlaster | *1 | |
| 79 | 運輸 | 3,899,363 | 0 | 18,900,000 | 22,799,363 | その他のウイルス被害 | | Welchia*4 |
| 80 | 医療･製薬 | 0 | 0 | 81,000,000 | 81,000,000 | MSBlaster | *1 | |
| 81 | 製造 | 0 | 0 | 0 | 0 | MSBlaster | *3 | |
| 82 | 建設 | 7,800,000 | 0 | 5,250,000 | 13,050,000 | MSBlaster | | |
| 83 | 金融（銀行、保険、証券等） | 30,000 | 0 | 6,000 | 36,000 | MSBlaster | *1 | |
| 84 | 金融（銀行、保険、証券等） | 30,000 | 0 | 6,000 | 36,000 | その他のウイルス被害 | *1 | |
| 85 | 金融（銀行、保険、証券等） | 15,000 | 0 | 3,000 | 18,000 | その他のウイルス被害 | *1 | |
| 86 | 金融（銀行、保険、証券等） | 30,000 | 0 | 6,000 | 36,000 | その他のウイルス被害 | *1 | |
| 87 | 製造 | 24,010,000 | 0 | 12,148,000 | 36,158,000 | MSBlaster | | |
| 88 | 製造 | 30,000 | 0 | 150,000 | 180,000 | その他のウイルス被害 | *1 | Opaserv*4 |
| 89 | 製造 | 15,000 | 0 | 0 | 15,000 | MSBlaster | *1 | |
| 90 | 飲食･小売 | 0 | 0 | 1,125,000 | 1,125,000 | MSBlaster | *1 | |
| 91 | 製造 | 900,000 | 0 | 1,800,000 | 2,700,000 | MSBlaster | | |
| 92 | 情報･通信 | 1,350,000 | 0 | 2,160,000 | 3,510,000 | MSBlaster | | |
| 93 | 金融（銀行、保険、証券等） | 41,250 | 0 | 0 | 41,250 | その他のウイルス被害 | *1 | |
| 94 | 製造 | 900,000 | 0 | 3,000,000 | 3,900,000 | MSBlaster | | |

| No. | 業種 | 直接被害 | 間接被害 | 潜在化被害 | 被害合計 | 被害 | 備考 | |
|---|---|---|---|---|---|---|---|---|
| 95 | 情報･通信 | 5,625 | 0 | 187,500 | 193,125 | MSBlaster | | |
| 96 | その他サービス | 0 | 0 | 0 | 0 | MSBlaster | *2 | |
| 97 | その他サービス | 0 | 0 | 150,000 | 150,000 | その他のウイルス被害 | *1 | |
| 98 | その他 | 0 | 0 | 0 | 0 | その他のウイルス被害 | *2 | |
| 99 | 情報･通信 | 37,500 | 0 | 0 | 37,500 | その他のウイルス被害 | *1 | Welchia*4 |
| 100 | 情報･通信 | 3,750 | 0 | 0 | 3,750 | 情報の漏洩 | | |
| 101 | 情報･通信 | 0 | 0 | 0 | 0 | PC/PDA の盗難･紛失 | *2 | |
| 102 | 製造 | 0 | 0 | 0 | 0 | BUGBEAR | *2 | |
| 103 | 製造 | 0 | 0 | 0 | 0 | PC/PDA の盗難･紛失 | *3 | |
| 104 | 情報･通信 | 28,800,000 | 0 | 0 | 28,800,000 | MSBlaster | | |
| 105 | 情報･通信 | 225,000 | 0 | 22,500 | 247,500 | その他のウイルス被害 | | Nachi,Welchia *4 |
| 106 | 情報･通信 | 201,875,000 | 0 | 0 | 201,875,000 | KLEZ | | |
| 107 | 金融（銀行、保険、証券等） | 30,000 | 0 | 0 | 30,000 | BUGBEAR | *1 | |
| 108 | その他サービス | 1,200,000 | 0 | 0 | 1,200,000 | 情報の漏洩 | | |
| 109 | 情報･通信 | 5,400,000 | 0 | 0 | 5,400,000 | 情報の漏洩 | | |
| 110 | 情報･通信 | 1,350,000 | 0 | 0 | 1,350,000 | MSBlaster | | |
| 111 | 教育･マスコミ | 45,000 | 0 | 157,500 | 202,500 | MSBlaster | *1 | |
| 112 | 情報･通信 | 1,350,000 | 0 | 0 | 1,350,000 | MSBlaster | *1 | |
| 113 | その他サービス | 22,500 | 0 | 0 | 22,500 | MSBlaster | *4 | |
| | 合計 | 600,884,558 | 3,000,000 | 582,855,250 | 1,186,739,808 | | | |

■ 算出条件

・直接被害額（人件費）の算出には、（復旧完了までの時間／8 時間）×（復旧に携わった人数）×（従業員の 1 日当たりの人件費）で試算した。

・間接被害額（人件費）の算出には、（システム停止時間／8 時間）×（影響を受けた従業員数）×（従業員の 1 日当たりの人件費）×（IT 感応度）で試算した。

・IT 感応度（システムの停止における業務への影響度）は、一律 0.2 で試算した。

・一般的な企業の 1 日の業務時間を 8 時間であることから、復旧完了までのシステム実停止時間を 8 時間で割って、システムが停止していた日数を算出した。

■ 注釈

*1 人件費の入力が無かったので、30,000 円／日で試算している。

*2 被害に対して対応人数（被害人数）の入力があったので被害はあったと想定されるが、対応時間（被害時間）の入力がないので被害額は未算出。

*3 被害に対して対応人数（被害人数）及び対応時間（被害時間）の入力がなく、実質的な被害はなかったと想定される。

*4 被害に対するコメントより、判明したウイルス名。

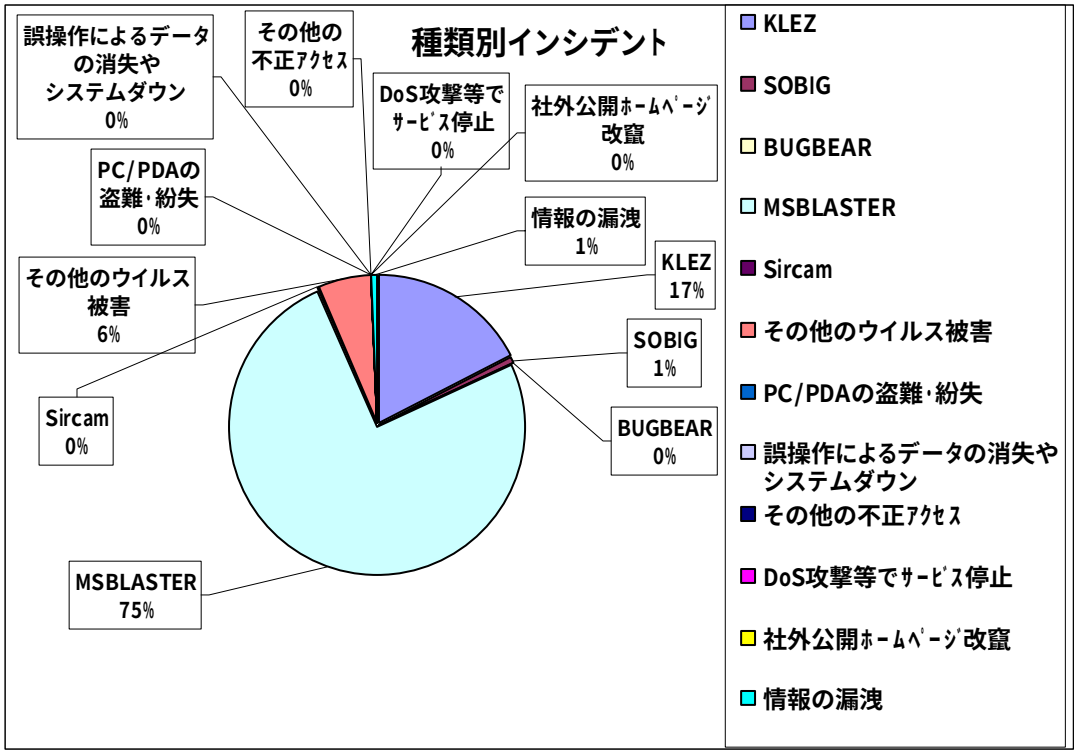
*Note*

試算した結果 2 億円を超える被害額となったインシデントが 2 件あった。また、この表には記載

していないが影響を受けた従業員数が 1 万人を超えた事例も 2 件あった。2003 年度のウイルス被害が拡大したことがこの表からもうかがえる。

② インシデント別被害の状況

| | 種類別 | 被害額 | 件数 | 平均被害額 | 割合 |
|---|---|---|---|---|---|
| 1 | KLEZ | 207,500,000 | 7 | 29,642,857 | 17.5% |
| 2 | SOBIG | 7,600,000 | 3 | 2,533,333 | 0.6% |
| 3 | BUGBEAR | 30,000 | 6 | 5,000 | 0.0% |
| 4 | MSBlaster | 894,127,570 | 69 | 12,958,371 | 75.3% |
| 5 | Sircam | 37,500 | 1 | 37,500 | 0.0% |
| 6 | その他のウイルス被害 | 70,609,113 | 18 | 3,922,729 | 5.9% |
| 7 | PC/PDA の盗難･紛失 | 0 | 3 | 0 | 0.0% |
| 8 | 誤操作によるデータの消失やシステムダウン | 0 | 0 | 0 | 0.0% |
| 9 | その他の不正ｱｸｾｽ | 0 | 0 | 0 | 0.0% |
| 10 | DoS 攻撃等でｻｰﾋﾞｽ停止 | 203,750 | 2 | 101,875 | 0.0% |
| 11 | 社外公開ﾎｰﾑﾍﾟｰｼﾞ改竄 | 28,125 | 1 | 28,125 | 0.0% |
| 12 | 情報の漏洩 | 6,603,750 | 3 | 2,201,250 | 0.6% |




*Note*

MSBlaster が全体の 75%を占め、2003 年度最大の脅威であったことがわかる。平均の被害額では KLEZ が 2,964 万円とトップであったが、これは一件で 2 億円を越える事例があったため平均被害額を引き上げたようだ。

③ 業種別被害額

| | 業種別 | 被害額 | 件数 | 平均被害額 |
|---|---|---|---|---|
| 1 | 金融（銀行、保険、証券等） | 17,550,375 | 13 | 1,350,029 |
| 2 | 医療・製薬 | 144,200,000 | 4 | 36,050,000 |
| 3 | 運輸 | 22,799,363 | 1 | 22,799,363 |
| 4 | エネルギー | 37,500,000 | 1 | 37,500,000 |
| 5 | 情報・通信 | 314,946,875 | 13 | 24,226,683 |
| 6 | 製造 | 559,846,945 | 59 | 9,488,931 |
| 7 | 教育・マスコミ | 202,500 | 1 | 202,500 |
| 8 | 建設 | 48,752,500 | 9 | 5,416,944 |
| 9 | 飲食・小売 | 1,125,000 | 1 | 1,125,000 |
| 10 | その他サービス | 36,216,250 | 8 | 4,527,031 |
| 11 | その他 | 3,600,000 | 3 | 1,200,000 |

*Note*

業種別の被害額では、製造業がトップになった。アンケートの回答件数も多く、この結果から短絡的に被害に会いやすいとは、結論できない。逆に、すべての業種において被害が発生している点に注目したい。

## 3.5 日本全体におけるウイルス総被害額の推計

2003 年度の本調査では RISTEX 様の協力を得られたことで、調査範囲を一般の企業まで拡大でき、その結果をもって、日本全体における被害額を推し量ることが可能となったものと考える。よって、本調査結果をもとに、2003 年における日本全体でのウィスル被害額を推計する。

### 3.5.1 参考とした基礎数値

今回のアンケート結果から、日本全体のウイルスによる被害額を推し量るための基礎数値として、「財務省　統計局　H13 年版」の統計資料を利用させていただく。

http://www.stat.go.jp/data/jigyou/kakuhou/01.htm

| No. | 統計項目 | 数値 | 備考 |
|---|---|---|---|
| 1 | 会社企業数 | 161 万 8 千 | 株式会社，有限会社，合名・合資会社及び相互会社 |
| 2 | 総事業所数 | 635 万 | 事業内容等が不詳の事業所を除く |
| 3 | 従業員数 | 6015 万 8 千人 | 事業内容等が不詳の事業所を除く |

これは、平成 8 年の統計値と比べ、数%の減少となっているため、本推計値の基礎数値としては、十分な精度を持つものと考える。

企業における、ウイルスへの感染状況は、警察庁：平成 16 年「不正アクセス行為対策の実態調査」の値を利用させていただく

http://www.npa.go.jp/cyber/chousa/H16countermeasures.pdf

| No. | 統計項目 | 数値 | 備考 |
|---|---|---|---|
| 1 | 企業におけるウイルス等の感染割合 | ６１．４% | 上場企業を対象 |

### 3.5.2 被害額の推計

パターン１　「**会社企業数**」からの推計

| 1 企業あたりの被害額 | ＝ | 被害額の合計 | ÷ | 被害のあった企業数 |
|---|---|---|---|---|
| **1，１２０万円** | | 11 億 8674 万 | | １０６社 |

| 日本全体のウイルス被害額 | ＝ | 会社企業数 | × | 企業におけるウイルス等の感染の割合 | × | 1 企業あたりの被害額 |
|---|---|---|---|---|---|---|
| ４兆３千７百億 | | 161 万 8 千社 | | ６１．４％ | | 1，１２０万円 |

*Note*

日本全体の企業数（財務省値）には、中小企業が含まれており、今回の調査対象の主体が上場企業を対象としていることから、この数値は正当性に欠ける。

よって、日本の証券取引所に上場している企業を対象として考えることとする。ここでは複数の取引所に登録している企業もあることから、企業数を 5,000 として計算する。

| | |
|---|---|
| 札幌証券取引所 | 102 社 |
| 東京証券取引所 | 2,255 社 |
| 名古屋証券取引所 | 414 社 |
| 大阪証券取引所 | 1,114 社 |
| 福岡証券取引所 | 164 社 |
| ジャスダック | 924 社 |
| ヘラクレス | 103 社 |
| 計 | 5,076 社 |

| 上場企業のウイルス被害額 | ＝ | 上場企業数 | × | 企業におけるウイルス等の感染の割合 | × | 1 企業あたりの被害額 |
|---|---|---|---|---|---|---|
| **３４３億円** | | 5 千社 | | ６１．４％ | | 1 千１２０万円 |

パターン２　**「総事業所数」**からの推計

被害にあった事業所数は調査していないため、総数を元に推計する。

| 1 事業所あたりの被害額 | ＝ | 被害額の合計 | ÷ | 有効回答の事業所総数　※ |
|---|---|---|---|---|
| **６１，６７４円** | | 11 億 8674 万 | | 19,242 拠点 |

※　事象所の総数は、アンケートの回答が範囲による選択方式のため、平均値より合算し算出

| 日本全体のウイルス被害額 | ＝ | 国内総事業所数 | × | 1 事業所あたりの被害額 |
|---|---|---|---|---|
| **３９２億円** | | ６３５万拠点 | | ６１，６７４円 |

***Note***

パターン１で算出した、上場企業の被害額と殆ど差異のない値である。よって当計算方式に何らかの欠陥があることは否めない。今回のアンケートについては、事業所という単位での被害発生状況を集計していないため、このような結果になっていると考えられる。

実際、財務省　統計局の資料によると、従業員が 30 名未満の事業所数が 94．7%であるのに、従業員数の割合は、51．5%となっている。これは、日本における殆どの事業所は 30 名未満であるが、その事業所に所属する従業員の総数は、約半分ということである。

| 人数区分 | 事業所数 | 割合 | 従業員数 | 割合 |
|---|---|---|---|---|
| 1 ～　4人 | 3,867,570 | 61.1% | 8,422,537 | 14.0% |
| 5 ～　9 | 1,214,145 | 19.2% | 7,896,374 | 13.1% |
| 10 ～　19 | 678,174 | 10.7% | 9,107,494 | 15.1% |
| 20 ～　29 | 232,827 | 3.7% | 5,534,761 | 9.2% |
| **小計** | **5,992,716** | **94.7%** | **30,961,166** | **51.5%** |
| 30 ～　49 | 171,322 | 2.7% | 6,434,035 | 10.7% |
| 50 ～　99 | 102,975 | 1.6% | 6,999,666 | 11.6% |
| 100 ～ 199 | 39,803 | 0.6% | 5,411,499 | 9.0% |
| 200 ～ 299 | 10,614 | 0.2% | 2,562,194 | 4.3% |
| 300人以上 | 11,898 | 0.2% | 7,789,484 | 12.9% |
| **小計** | **336,612** | **5.3%** | **29,196,878** | **48.5%** |
| 合計 | **6,329,328** | | **60,158,044** | |

今回のアンケート結果から事業所数をもととした日本全体のウイルス被害額を推計することは無理がある。次年度以降における課題として検討していきたい。

パターン３　**「総従業員数」**からの推計

被害にあった従業員数は調査していないため、総数を元に推計する。

| 従業員１人あたりの被害額 | ＝ | 被害額の合計 | ÷ | 有効回答の従業員総数　※ |
|---|---|---|---|---|
| **１，４３２円** | | 11 億 8674 万 | | 829,007 人 |

※　従業員の総数は、アンケートの回答が範囲による選択方式のため、平均値より合算し算出

| 日本全体のウイルス被害額 | ＝ | 総従業員数 | × | 1 人あたりの被害額 |
|---|---|---|---|---|
| **８６１億円** | | 6，015 万人 | | １，４３２円 |

***Note***

3 パターンの推計方式の中で、もっとも妥当性のある結果と考えられる。ただし、アンケート対象が大企業を主体としたものであることから、次年度の調査にあたっては、中小企業を対象に含めることを検討課題としたい。

### 3.5.3　ウイルス総被害額の推計における考察

今回のアンケート結果の特徴として、以下の点があげられる。

・調査対象として、東証 1 部上場企業と JNSA 所属企業を対象としている。
・全クライアントへのウイルスチェックソフトの導入が９２%以上である。
・メールサーバでのウイルスチェックを実施しているのが８０%以上である。
・セキュリティ関連の規定がある企業が、８０%を超えている。
・セキュリティパッチの適用は、常に最新状態を維持しているのが７１%である。

ここから、今回の調査結果は、一般的よりも情報セキュリティに対する意識が高い企業であることがわかる。

これだけウイルスに対する対策を実施し、関連規定を整備し、セキュリティパッチの適用を行っていても、ウイルスによる被害を完全に防ぐことはできないということであり、それらの対策を実施している企業においても、従業員 1 人あたり、１，４３２円の平均被害額が発生しているということになる。

仮に日本全体における情報セキュリティ対策の実施状況が、今回の調査結果と同程度のレベルに達した場合の、日本全体におけるウイルス総被害額が、今回の推計値（８６１億円）と考えられるかもしれない。

つまり、現時点での日本全体におけるウイルス総被害額は、今回の推計値（８６１億円）よりもかなり大きいと考えられるということである。

ここでご注意いただきたいのは、「どんな対策を行っても、コンピュータウイルスは防ぐことはできない」ということではない。

個別企業へのヒアリングにおいて、過去に Nimda や CodeRed により全社的に業務停止に追い込まれたことがあるという企業では、上述のウイルス対策を実施することで、以降の被害を極小化できたとのお話を伺っている。

逆に、過去において全社的な被害がなかった企業においては、昨年度の MSBlaster によって、全社的な業務停止に追い込まれたというお話も伺っている。

かつて、人類の歴史にける大航海時代に、人々が世界中を大型船に乗って行き交うようになり、今まで存在しなかった病原菌（ウイルス）が広まることで、ウイルスに耐性のない原住民たちが次々と病に倒れていったと聞く。

現在、新たなインターネットという革命的な情報通信手段の出現とともに、我々はコンピュータウイルスという脅威にさらされているが、いつまでもウイルスに耐性のない原住民であるのではなく、正しい知識と情報を持つことで、コンピュータウイルスに対抗できるものと考えている。

## 3.6　調査結果の分析まとめ

昨年度の調査では、情報セキュリティ対策も前年と比較すると整備されてきて実際に大きなインシデントもなく、情報セキュリティ面では落ち着いてきたように見えた。

しかし、2003 年度の本調査ではそれが一時的な現象であったことを物語っている。今回の調査では、情報セキュリティ対策も 2002 年度と比較すると全般的により進んでいる傾向にある。ところが 2003 年度は MSBlaster を中心に被害が拡大した。

感染の原因は、今までのようにメールに添付されたファイルを開いて感染するというパターンよりも、外部から持ち込まれたノート PC を社内 LAN に接続したために感染するパターンと、ダイアルアップで接続して感染するパターン、またその感染したパソコンを社内 LAN に接続して被害を広げるパターンが目立った。また、トラフィックの増大も今回の特徴で社内 LAN が停止することも珍しいことではなかった。

現状わかっている脅威に対する対策をしていても、新しい脅威が発生した場合には有効ではないということが実証された結果になった。もう一点は、技術的な対策だけでなく、従業員への情報セキュリティ教育などを実施して、セキュリティに対する意識の向上の必要性も認識されてきた。これは、ウイルス対策というよりも、昨今の個人情報流出のリスクに対する対策という面が強いと思われる。

# 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

被害の有無と具体的対策状況の相関関係を分析するために、本年度のアンケート結果を『情報セキュリティインシデントにより被害にあった企業のグループ』と『被害にあわなかった企業のグループ』に分け、以下の項目で対比を行った。

**【比較した項目】**

① 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
② 情報セキュリティ被害が発生した時の対応計画の対象
③ 情報セキュリティ事件・事故発生時の連絡体制
④ 情報セキュリティ教育の内容
⑤ 派遣社員・常駐作業員受け入れ時の配慮
⑥ 情報セキュリティ規定の整備
⑦ 従業員 1 人あたりの情報セキュリティ予算

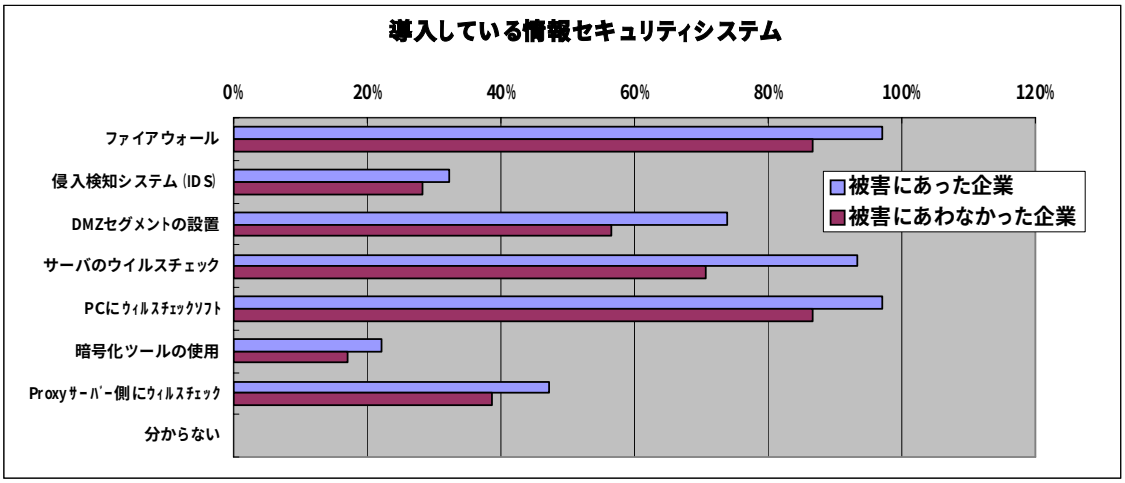
前年度も同様の分析を行ったが、対策が被害発生前に取られていたのか、あるいは被害発生後に導入されたものかが曖昧であったため、本年度は確認できる範囲で対策実施が被害発生前なのか後なのかを分類した。

本年度アンケートは RISTEX にも協力をもとめたため、RISTEX と JNSA で共通の調査項目である「① 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」「⑥ 情報セキュリティ規定の整備」「⑦ 従業員 1 人あたりの情報セキュリティ予算」については両協会のアンケート結果を統合した。したがって、これらの項目については他の項目と母数が異なることに注意していただきたい。

被害にあった企業とは、アンケートで被害を受けたと回答した内、被害発生年が 2003 年と回答があったものと、被害発生年は未記入であるが被害種別が MSBlaster と回答があったものをカウントした。

## ① 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

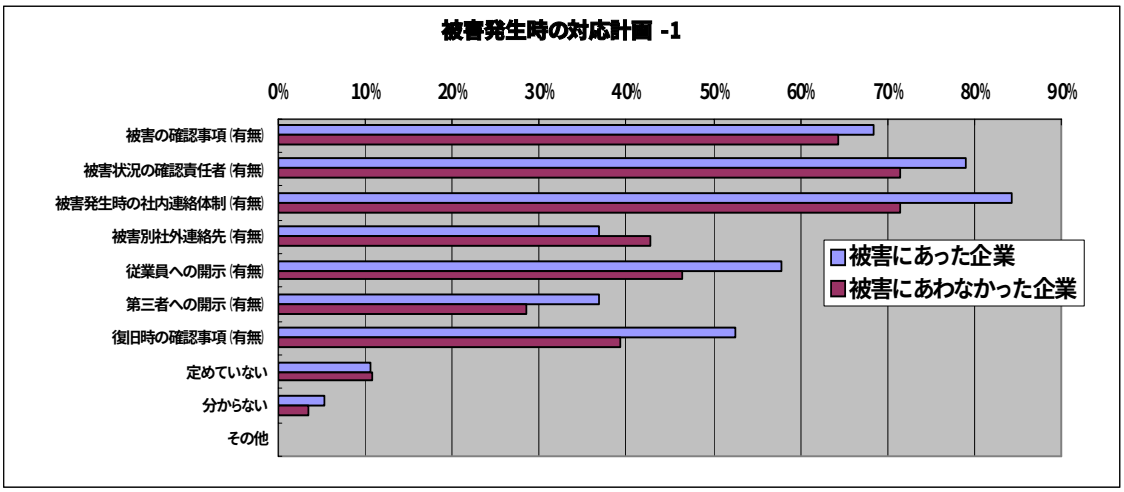
| 情報セキュリティを確保するために導入しているシステム | 被害にあった企業 (108 件) | | 被害にあわなかった企業 (106 件) | |
|---|---|---|---|---|
| ファイアウォール | 105 | 97.2% | 92 | 86.8% |
| 侵入検知システム (IDS) | 35 | 32.4% | 30 | 28.3% |
| DMZ セグメントの設置 | 80 | 74.1% | 60 | 56.6% |
| サーバのウイルスチェック | 101 | 93.5% | 75 | 70.8% |
| PC にウイルスﾁｪｯｸｿﾌﾄ | 105 | 97.2% | 92 | 86.8% |
| 暗号化ツールの使用 | 24 | 22.2% | 18 | 17.0% |
| Proxy ｻｰﾊﾞ側にウイルスﾁｪｯｸ | 51 | 47.2% | 41 | 38.7% |
| 分からない | 0 | 0.0% | 0 | 0.0% |

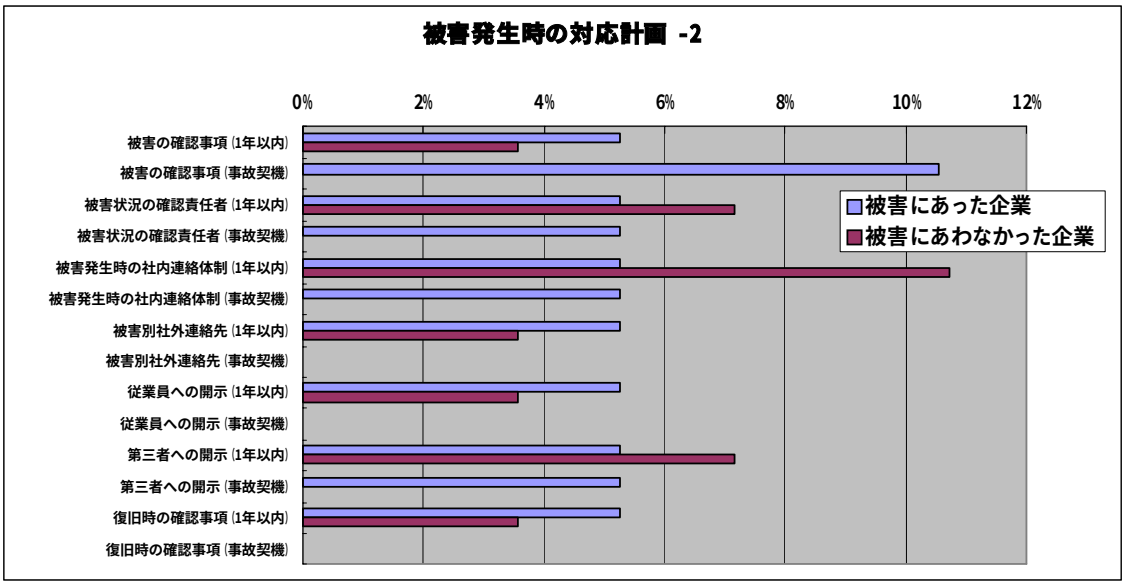



結果を見る限りでは両グループに差異はみられない、むしろ、被害にあったグループの方が導入は進んでいるという結果になった。前年度も同様の結果が得られていたため予測はしていたが、導入システムに差がないとすると、運用や体制など他の項目の実施状況が被害の有無を左右している可能性を示唆する。

② 情報セキュリティ被害が発生した時の対応計画の対象

被害にあった企業＝19 件　被害にあわなかった企業＝28 件



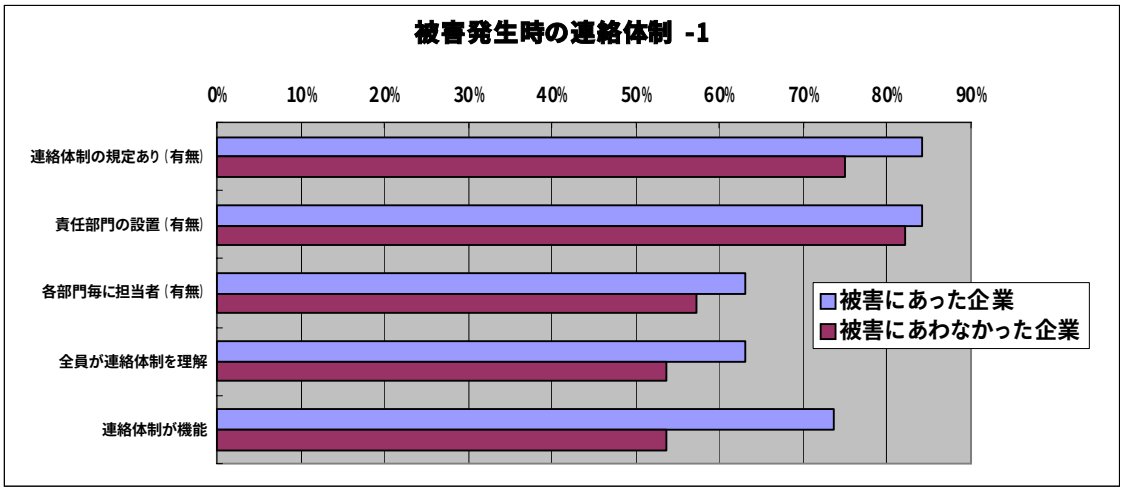



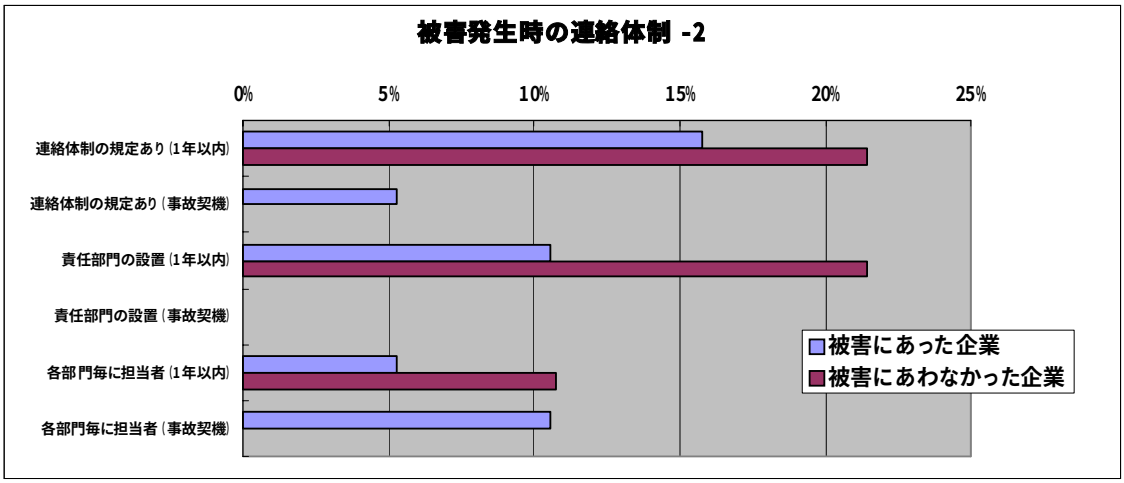

被害発生時の＜対応計画－1＞の結果を見ると、被害の有無に相関関係は見られないが、実施時期を調査した結果である＜対応計画－2＞のグラフを見たところ、被害時の「確認事項」「確認責任者」「社内連絡体制」については、被害発生後に実施した率が高くなっている。

対応計画は予防・防御策では無いので、被害の有無に直接的な影響は無いと考えられるが、実被害にあった企業がその経験から上記対策を強化したという点は参考にすべきだろう。

### ③ 情報セキュリティ事件・事故発生時の社内連絡体制

被害にあった企業＝19 件　被害にあわなかった企業＝28 件

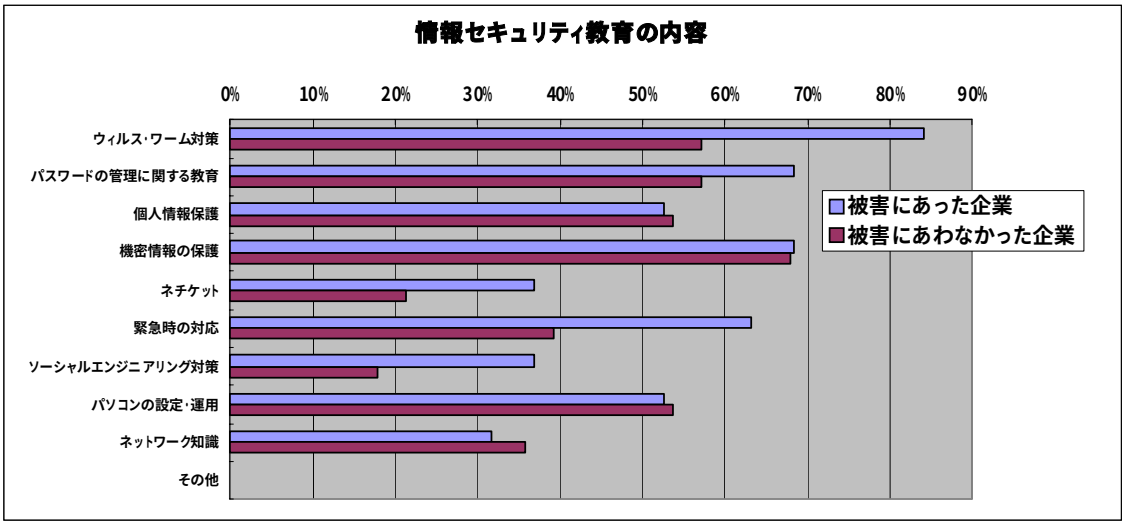



連絡体制についても、両グループに大きな差異は見られなかった。連絡体制が機能しているか否かについては被害にあったグループの方が良い結果が出ている。しかし、実施時期を見ると、「連絡体制の規定あり」「各部門に担当者」は被害を契機に実施しており、②でも述べた通り、実被害にあった企業がその経験からこれら対策を強化したという点は参考にする必要がある。

## ④ 情報セキュリティ教育の内容

被害にあった企業＝19 件　被害にあわなかった企業＝28 件

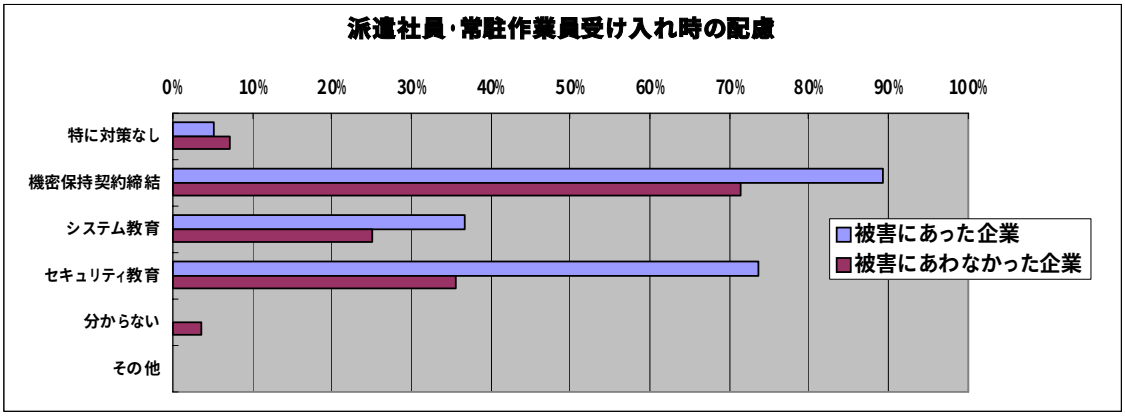



アンケート結果から見ると、情報セキュリティ教育は被害にあった企業の方が概ね実施状況が良いという結果が得られた。残念ながらこの項目については実施開始時期まで調査していないため、被害発生を契機に始めたかどうかは不明である。

したがって、この結果をもって教育の実施が被害の有無を左右したかどうかを判断することは難しい。

## ⑤ 派遣社員・常駐作業員受け入れ時の配慮点

被害にあった企業＝19 件　被害にあわなかった企業＝28 件

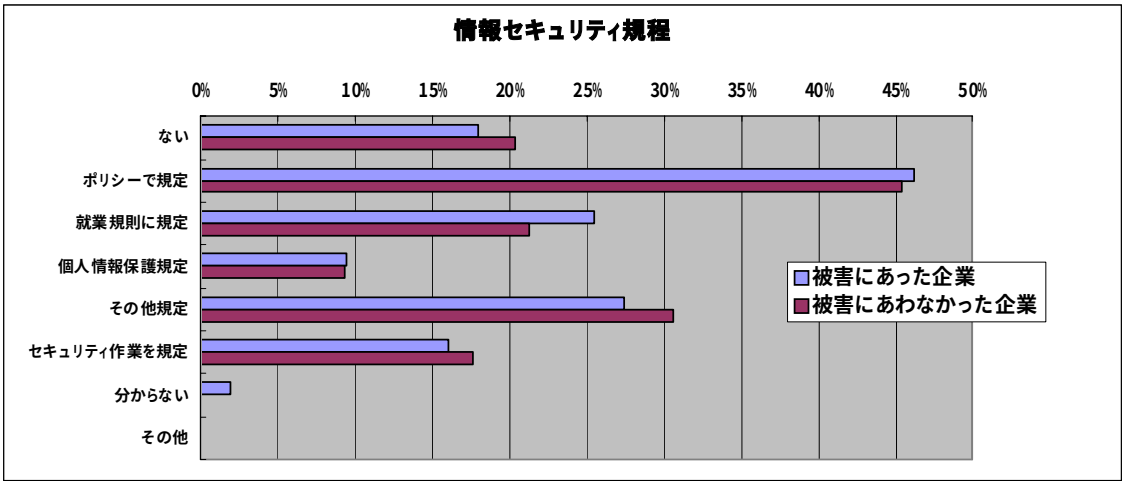



④と同様に被害にあった企業の方が概ね実施状況が良いという結果が得られた。残念ながらこの項目についても実施開始時期まで調査していないため、被害発生を契機に始めたかどうかは不明である。

したがって、この結果をもってこの項目が被害の有無を左右したかどうかを判断すろことは難しい。

## ⑥ 情報セキュリティ規定の整備

被害にあった企業＝106 件　被害にあわなかった企業＝108 件




規定の有無に関しても、被害にあった企業とあわなかった企業で大きな差は見られなかった。この結果もまた、実施開始時期の調査までいたっておらず、次年度の課題として残すことになった。

## ⑦ 従業員１人あたりの情報セキュリティ予算

**被害にあった企業（５１件）の情報セキュリティ予算**

| No. | 従業員数（人） | 情報セキュリティ予算（万円） | No. | 従業員数（人） | 情報セキュリティ予算（万円） |
|---|---|---|---|---|---|
| 1 | 1,349 | 600 | 27 | 513 | 500 |
| 2 | 1,000 | 1,000 | 28 | 1,499 | 300 |
| 3 | 9,284 | 125 | 29 | 600 | 500 |
| 4 | 158 | 200 | 30 | 4,819 | 15,000 |
| 5 | 700 | 1,000 | 31 | 836 | 500 |
| 6 | 4,754 | 2,000 | 32 | 2,822 | 1,000 |
| 7 | 1,025 | 2,000 | 33 | 140,000 | 150,000 |
| 8 | 3,800 | 2,400 | 34 | 7,155 | 1,650 |
| 9 | 1,476 | 500 | 35 | 630 | 23,000 |
| 10 | 5,000 | 300 | 36 | 2,125 | 500 |
| 11 | 490 | 240 | 37 | 4,489 | 4,000 |
| 12 | 5,000 | 1,500 | 38 | 2,679 | 500 |
| 13 | 2,100 | 5,000 | 39 | 1,244 | 1,000 |
| 14 | 850 | 300 | 40 | 10,000 | 3,000 |
| 15 | 713 | 300 | 41 | 3,500 | 2,000 |
| 16 | 600 | 150 | 42 | 1,222 | 3,000 |
| 17 | 1,000 | 50 | 43 | 2,600 | 600 |
| 18 | 8,000 | 2,500 | 44 | 14,700 | 500 |
| 19 | 12,500 | 5,000 | 45 | 15 | 1,000 |
| 20 | 800 | 2,000 | 46 | 44,300 | 200,000 |
| 21 | 4,310 | 4,000 | 47 | 1,160 | 1,000 |
| 22 | 2,000 | 1,100 | 48 | 3,515 | 2,970 |
| 23 | 847 | 500 | 49 | 45 | 86 |
| 24 | 2,179 | 3,500 | 50 | 105 | 200 |
| 25 | 2,330 | 300 | 51 | 100 | 300 |
| 26 | 700 | 500 | **合計** | **323,638** | **450,171** |

## 被害にあわなかった企業（４１件）の情報セキュリティ予算

| No. | 従業員数（人） | 情報セキュリティ予算（万円） |
|---|---|---|
| 1 | 1,200 | 250 |
| 2 | 300 | 200 |
| 3 | 4,000 | 2,000 |
| 4 | 243 | 200 |
| 5 | 3,786 | 200 |
| 6 | 750 | 500 |
| 7 | 292 | 175 |
| 8 | 1,300 | 5,000 |
| 9 | 270 | 1,000 |
| 10 | 10,000 | 100 |
| 11 | 1,673 | 160 |
| 12 | 2,445 | 2,000 |
| 13 | 2,745 | 1,850 |
| 14 | 1,628 | 1,000 |
| 15 | 2,414 | 21,000 |
| 16 | 2,847 | 333 |
| 17 | 3,196 | 3,000 |
| 18 | 1,415 | 120 |
| 19 | 3,191 | 2,000 |
| 20 | 1,892 | 110 |
| 21 | 4,000 | 1,000 |

| No. | 従業員数（人） | 情報セキュリティ予算（万円） |
|---|---|---|
| 22 | 14,000 | 600 |
| 23 | 500 | 1,000 |
| 24 | 800 | 200 |
| 25 | 1,555 | 3,700 |
| 26 | 2,700 | 300 |
| 27 | 1,057 | 500 |
| 28 | 626 | 200 |
| 29 | 1,488 | 500 |
| 30 | 2,200 | 100 |
| 31 | 7,000 | 4,000 |
| 32 | 8,316 | 5,000 |
| 33 | 24,000 | 5,000 |
| 34 | 2,300 | 4,000 |
| 35 | 3 | 50 |
| 36 | 116 | 500 |
| 37 | 18 | 100 |
| 38 | 113 | 2,500 |
| 39 | 12,053 | 10,000 |
| 40 | 15,815 | 1,000 |
| 41 | 70 | 50 |
| **合計** | **144,317** | **81,498** |

アンケートの中で従業員数と情報セキュリティ予算の両項目に回答があった企業のみを対象として集計した。

被害にあったグループとあわなかったグループで投資する予算の違いをはかるため、それぞれの 1 人あたりの情報セキュリティ予算を算定した。結果は以下の通り。

被害にあった企業＝450,171 万円÷323,638 人＝13,910 円

被害にあわなかった企業＝81,498 万円÷144,317 人＝5,647 円

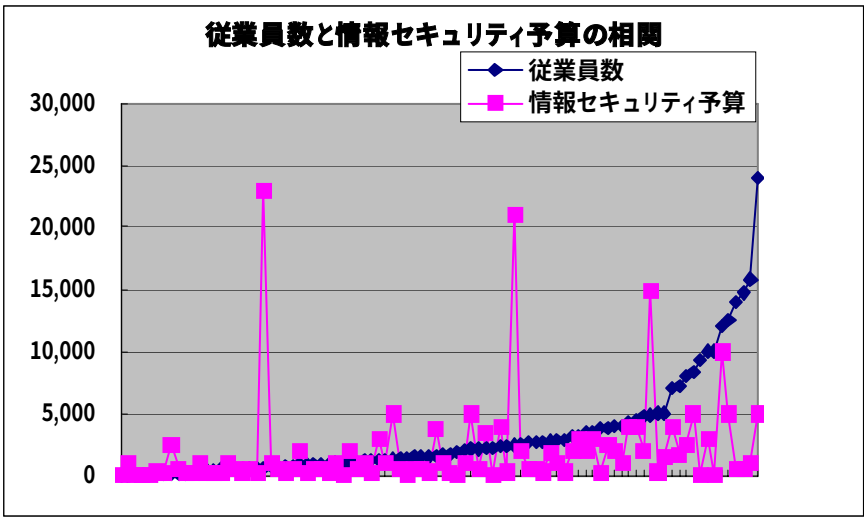
前年度の調査では、被害にあわなかった企業は被害にあった企業に比較して 1 人あたりに約 3 倍の予算をかけている結果が得られたが、本年度は逆転し「被害にあった企業の方」が「被害にあわなかった企業」よりも約 2.5 倍の予算をかけている結果となった。

被害にあったグループの内 No.33 と 46 の予算が突出しており、それが全体の予算を引き上げている可能性があるため、その 2 例を差し引いて再計算した。

No.33 と 46 を差し引いた後の被害にあった企業＝100,171 万円÷139,338 人＝7,100 円

結果、被害にあわなかった企業の 5,647 円に近づいたものの、やはり上回った。

なお、従業員数と１人あたりの情報セキュリティ予算の相関関係を見たのが次のグラフである。被害にあったグループの内 No.33 と 46 は他に比べ値が大きくグラフの詳細が見えなくなるためその２件を除いた。




グラフでは数件の予算が突出しているので、それは例外として分析すると 5,000 人弱の規模までは従業員数に比例しているが、それを超えると一定量以上予算は上がっていないことが分かる。

## 4.2　被害にあった企業とあわなかった企業の比較に関する考察

全体的に被害にあった企業の方があわなかった企業よりも対策が充実している結果が出た。しかし、4.1 の比較は数値そのものを評価するのではなく傾向を分析することを目的としたため、両グループの母数が異なることなどを考慮しなかった。したがって、結果をそのまま鵜呑みにせず以下のことを考慮して補正して考える必要がある。

a. ②③④⑤は、被害にあった企業の母数が 18 件で、あわなかった企業の母数が 28 件と異なるため、1 件あたりの影響度は 28 件に比較して 18 件の方は 1.7 倍弱となることを加味して考える必要がある。
b. 情報セキュリティシステムの導入や各種規定の策定などに差異がなく、それにもかかわらず被害の有無という差が生じたとすると、「何を持っているか」ではなくそれが有効かどうかに影響されている可能性がある。この点についてはヒアリングによる実態調査が参考になるだろう。
c. アンケート上では「被害にあわなかった」という回答をしている企業でも、回答者が実態を把握できていないだけで実際には被害にあっていることもありえる。このことが両グループの件数に影響をあたえている可能性が考えられる。
d. 回答者が立場上などの問題で情報セキュリティ予算を把握していない、あるいはシステム予算など他の予算の一部として計上しているため情報セキュリティ予算の範囲が明確でないなどの理由で、回答者の捉え方により予算にばらつきが出ている可能性がある。
e. 前年度の反省から、各対策の実施開始時期をアンケートに反映させたが、必要なすべての質問で徹底しなかったため分析結果が曖昧になった。

これらのことを踏まえて改めて考察をすると、集計結果に数値として現れないことにも重要な点が隠されていることがわかる。例えば上記c.d.で指摘したように担当者が実態を把握しきれていないがために集計の精度が下がったと思われる点だが、担当者が実態を把握できていないこと自体がセキュリティ上の不備と言えるだろう。さらに深読みすると、4.1 ②③の結果では、被害にあわなかったグループの中でも一年以内に対策をはじめたと答えた企業が多くあり、必要もなしに企業がそのような動きをする可能性は低いと想定すると、やはり実態を把握しきれていないか、被害があったものの何らかの理由で回答していない可能性も考えられる。把握できていないことを調査するのは困難であるが、誤差としてどこまで考えるかは課題のひとつである。

このように、分析自体の信頼性に疑問が残る結果となった。次年度は 4 章のような比較分析の必要性も含め再考する必要がある。

今回アンケートの結果からは、定量的な評価において「被害にあう・あわない」の明確な線引きはできなかった。回答を見る限り、大半の企業ではファイアウォールやインターネット接続点でのウイルスチェックは導入されていて、組織を外部から守る対策は十分に実施されている。

しかし、2003 年度は被害種別として MSBlaster によるものが多く、感染した数台の PC から社内 LAN 経由で被害が拡大したケースが多く見られたことから、組織レベルのセキュリティシステムから PC１台毎のセキュリティレベルにまで対策を広げる必要性が感じられた。アンケート結果では各 PC のウイルスチェック実装や適時パッチ適用を実施している比率は高かったものの、ヒアリングによる実態調査では実際に実施するか否かはユーザの運用に委ねていて、数人のユーザがパッチ対応を遅れたがために MSBlaster の被害を受けたケースがいくつかあった。その経験を踏まえ、各 PC に監査ツールを実装し、管理者が一元的かつ自動的にパッチ適用の有無を監視するシステムの導入を進めているという組織もみられた。

また、アンケートの結果から、被害にあった企業が被害を契機に「確認事項」「確認責任者」「社内連絡体制」「連絡体制の規定」「各部門に担当者を設置」を強化したという回答は大いに参考にすべきだろう。

## 4.3　望まれる対策レベルと予算規模の提案

前年度と同様にアンケートおよびヒアリングの結果から導き出される対策レベルと予算規模を検証する。

### ① 望まれる対策レベル

アンケートとヒアリングの結果から、対策レベルについて以下の要点が挙げられる。

a. ファイアウォールやウイルスチェックならびに IDS など基本的な情報セキュリティシステムの導入は最低限実施されている。

b. 情報セキュリティ規定や事故対応マニュアルなどドキュメント類の整備や情報セキュリティ管理者の設置など、セキュリティ対策の運用をささえる体制は整い始めている。

c. ISMS を実践している企業も、決めたことが実現できているか、それらが有効かといったユーザ（PC）単位での実施度の監査については必要性を感じている。

d. MSBlaster のように強力な脅威は今後も発生すると考えられる。現時点で出来る限りのセキュリティ対策を施していても、ある程度の範囲で被害が発生することは覚悟しなくてはならない。すなわち、事故前提でセキュリティを考え、事故が発生した後の対応を速やかに実施するための「確認事項」、「確認責任者」、「社内連絡体制」、「連絡体制の規定」、「各部門の担当者」の整備が望まれる。

これらの要件をまとめたのが下表である。

| 対応レベル | 対策 | 具体例 | 対応レベル |
|---|---|---|---|
| 対応レベル 1 | 技術的対策 | ファイアウォール | レベル 1 / レベル 2 / レベル 3（推奨レベル） / レベル 3 |
| | | ウイルス対策 | |
| | | IDS | |
| | | メール監視ソフト | |
| | | 認証デバイス | |
| | | PCセキュリティ(ウイルスチェック、パッチ適用、データ暗号化等) | |
| 対応レベル 2 | 運用的対策 | 入退出管理 | |
| | | セキュリティ責任者の設置 | |
| | | 情報セキュリティ規定の策定 | |
| | | セキュリティ事故対応マニュアルの策定 | |
| 対応レベル 3（推奨レベル） | 実施度の向上 | 情報セキュリティ教育・啓発 | |
| | | 罰則規定の整備 | |
| | | 監査機能の強化 | |
| | | 事故発生時の連絡体制の整備 | |
| | | 事故発生を想定した訓練 | |
| 対応レベル 4 | 第三者認証の向上 | ISMS・BS7799認証 | |
| | | プライバシーマーク取得 | |
| | | 情報セキュリティ監査の実施 | |

ここでは、対応レベル３を推奨レベルとした。末端の個人あるいはPC単体にいたるまで、対策が有効に働いているのか、決められたルールが守られているのかといった実施度を上げる施策を取っているかどうか。また、事故前提の組織を確立しているかどうかを基準としている。

4.2 の b.で挙げた「何を持っているか」ではなくそれが有効に機能しているかどうかが重要であると言うことを改めて述べているのだが、間違ってはならないのは、ファイアウォールなどを導入しても結果的に被害が防げないということを言っているわけではない。もし、ファイアウォールやインターネット接続点でのウイルスチェックが無ければさらに被害件数は増え被害規模も拡大したであろう。

「何をもっているか」とはここで言うレベル１・２であり、最低限必要な対策としていることをみていただきたい。

**② 被害規模と情報セキュリティ予算の関連**

4.1 ⑦で検証したとおり、被害にあったグループとあわなかったグループでは、従業員 1 人あたりの情報セキュリティ予算は被害にあったグループの方が若干大きく出る結果となった。しかし、本年度の被害種別は MSBlaster が最も多く、セキュリティ対策を講じていた企業でも被害にあっていることが多くみられたため、被害にあったか否かだけで比較するのではなく、改めて被害の規模（影響範囲）と予算の関係の検証を試みた。

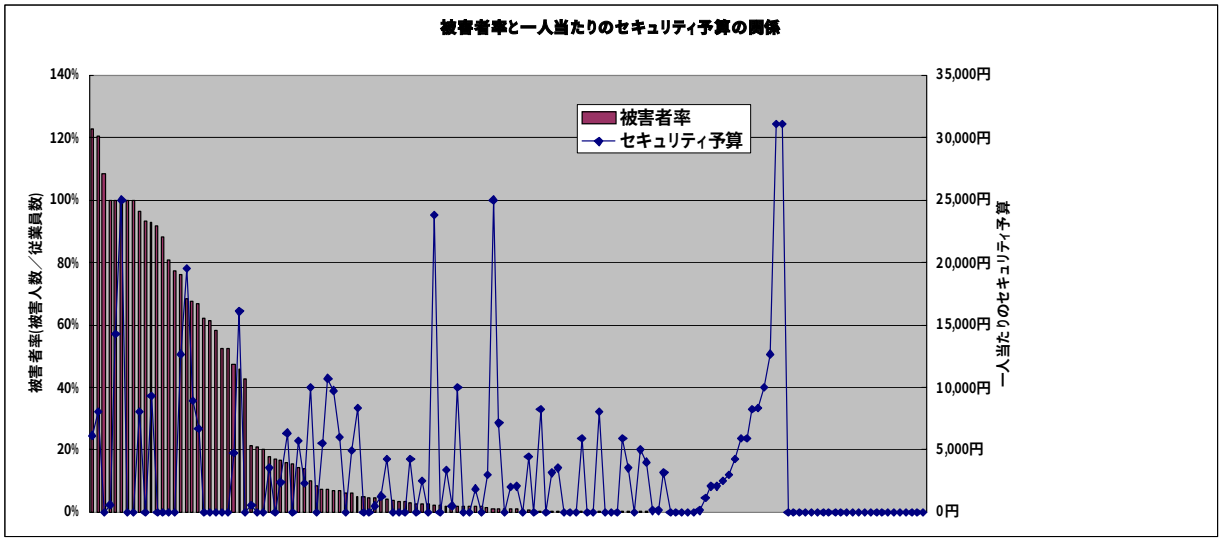
4.1 ⑦では予算不明と回答した企業は除外したが、ここでは予算不明の企業も含め分析を行った。

検証したのは以下の通り。

a. 被害者率と一人当たりのセキュリティ予算の関係
b. 影響人数と一人当たりのセキュリティ予算の関係
c. 被害台数と一人当たりのセキュリティ予算の関係

### a．被害者率と一人当たりのセキュリティ予算の関係

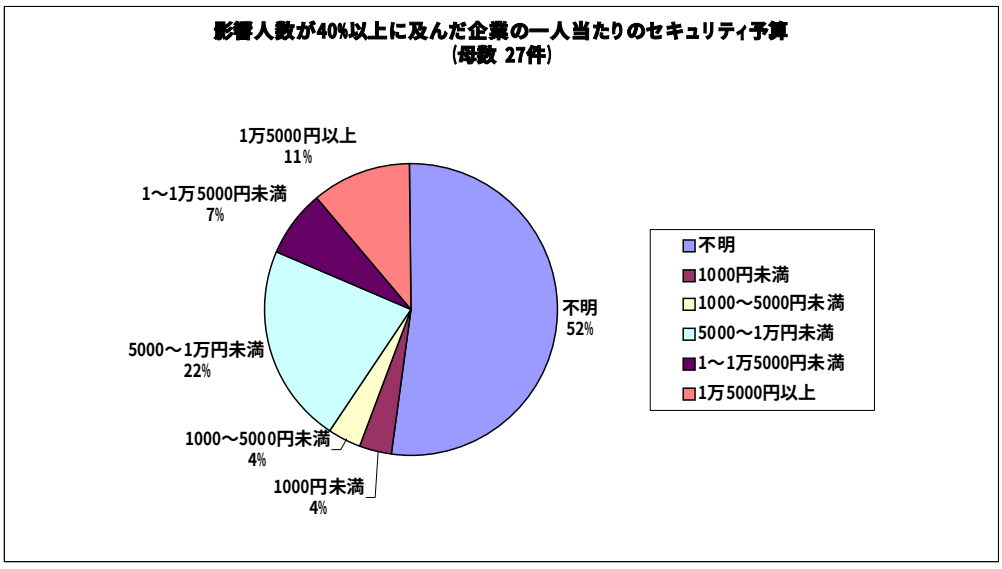
被害にあったと回答した企業 142 社を対象に、各社の被害者率と一人当たりのセキュリティ予算の対比を行った。対象の中には予算が不明という回答も有り、不明の場合は 0 円としたため、数値の信頼性は低いと考えられるが、おおよその傾向はつかめると考えてここに示した。なお、被害者率とは全従業員数の内影響を受けた人数の割合をいう。

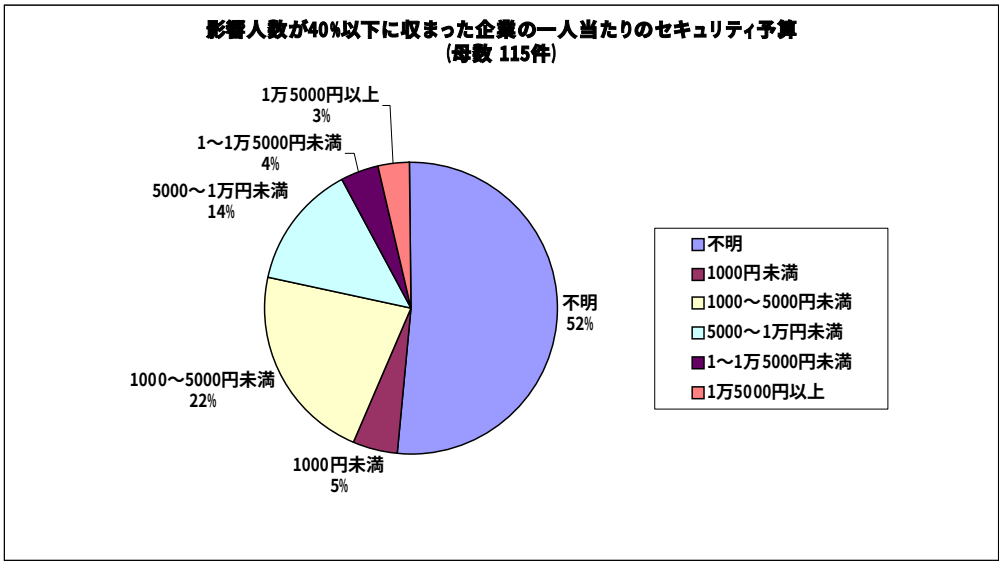



このグラフでは、被害規模と予算に明確な関係は見出せなかった。そのため、被害規模の基準を設けそれより大きいグループの予算、基準より小さいグループの予算の比較を試みたのが、以下の b.と c.である。

### b．影響人数と一人当たりのセキュリティ予算の関係

被害による影響人数が全従業員数の内 40%以上に及んだか、あるいは下回ったかで企業を 2 グループに分割し、両グループにおける従業員 1 人あたりのセキュリティ予算を分析した。



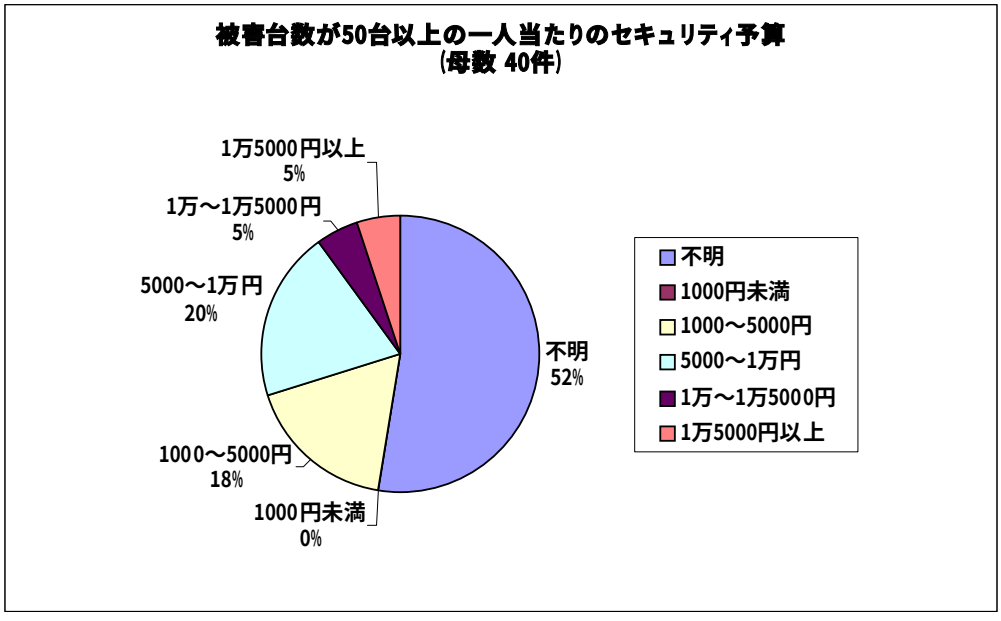


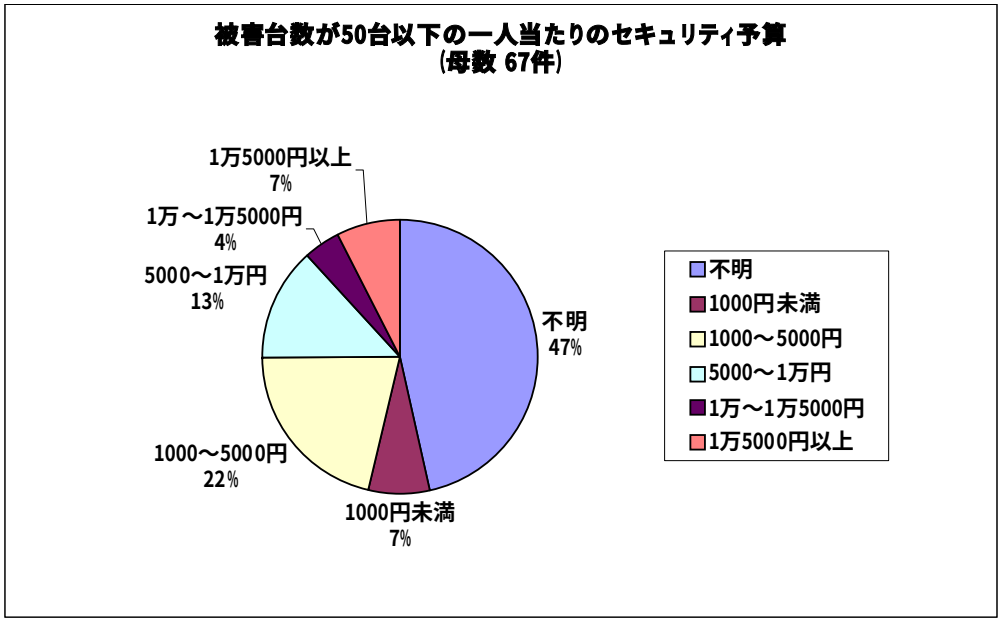

グラフによると、不明を除き最も比率の高い予算範囲は、影響人数が 40%以上に及んだグループは 5,000～1 万円未満（22%）で、影響人数が 40%以下に納まったグループが 1,000～5,000 円未満（22%）となった。

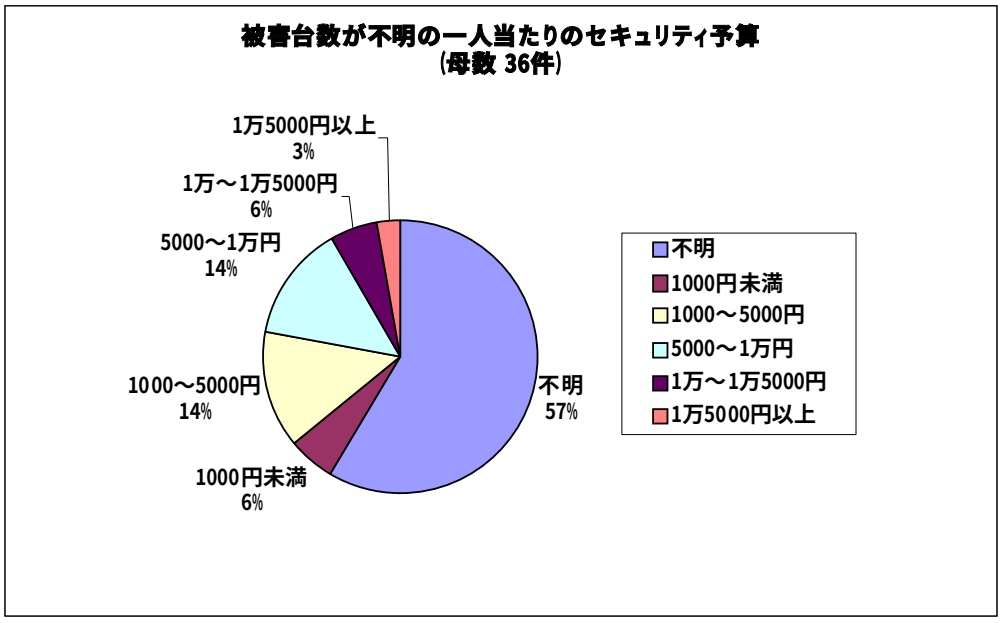
影響人数が少ないグループの方が 1 人あたりの予算が大きいのではないかという予想に反し、影響人数の大きい方が予算は大きいという結果となった。

### c. 被害台数と一人当たりのセキュリティ予算の関係

被害規模が保有コンピュータの内「50 台以上に及んだ」「50 台を下回った」「被害台数不明」の 3 グループに分割し、各グループにおける従業員 1 人あたりのセキュリティ予算を分析した。






グラフによると、不明を除き最も比率の高い予算範囲は、影響台数が 50 台以上に及んだグループは 5,000～1 万円未満（20%）で、影響台数が 50 台以下に納まったグループが 1,000～5,000 円未満（22%）となった。

また、影響台数が不明としたグループでは、5,000～1 万円未満と 1,000～5,000 円未満（共に 14%）が同率になった。なお、このグループは予算も不明と回答している率が高くなる（57%）傾向がみられた。

この分析においても b.と同様に、影響台数の大きい方が予算は大きいという結果となった。

**②の考察**

b.c.の結果をそのまま受け取ると、被害規模と 1 人あたりのセキュリティ予算には強い関連は見られないという結論にいたる。しかし、観点を変えて見ると、どのグループにおいてもセキュリティ予算が不明という回答の比率が高いということから、被害規模との関連以前の問題として予算を把握していないことの重大性がはからずも明らかになった。

予算の正確性を向上するための施策をどう行っていくかが来年度の課題となる。これは各企業の問題であり、直接的に当ワーキンググループで改善を働きかけることは難しいが、何をセキュリティ予算としてカウントするのか基準を示し、予算を把握することの重要性を説いていくことは、ワーキンググループの役割として考えなくてはならない。

# 5. 被害調査ヒアリングレポート

## 5.1　ヒアリングの意義について

紙ベースのアンケートからは、統計的な分析と判断が可能であるが、実際の被害状況を把握するためには、ヒアリングによる実態調査が欠かせない。そこで、当ワーキンググループでは過去３年に渡り、直接企業と面談して、情報セキュリティインシデントに関するヒアリングを実施してきた。

紙によるアンケートにお答えいただいた企業の内、ヒアリングにも対応いただけるとお答えいただいた企業に直接お伺いしているが、意外にも、かなり具体的な被害状況について、回答をいただくことができている。

ここで、「意外」といっているのは、情報セキュリティ自体が、「情報を不用意に外部に漏らさないこと」であり、かつ、「自社の被害状況は、身内の恥」であるため、JNSA のような中立的な機関であっても、なかなか回答は得づらいだろう、と考えていたからである。
しかし、実際には、ヒアリングに応じていただいた全ての方々に快くご対応いたき、生の声として、困っていること、上手くいっていることなどを具体的にお教えいただくことができている。

## 5.2　ヒアリング結果のまとめ方について

ヒアリング結果は定性的な部分が多く、かつ、ヒアリング対象企業が特定できてしまうような記載方法は、避けなければならないことから、昨年までは、被害額算出の基礎資料として利用する以外には、質問毎の回答を文章として羅列することで集約する形で提供してきた。

一方、ヒアリングに際して、ご対応いただいた担当の方々から「同業他社のセキュリティ対策状況は、どの程度なのか？」、「情報セキュリティが必要なことは理解できるが、どこまでやればいいのか？」などの本音に近い質問が調査者に行われていた。
貴重なお時間を使って、快くご対応いただいた方々への感謝の意味を込め、今年度のヒアリング結果のまとめとして、実際の現場対応で困っている点や、上手く対応している点を特定企業の判別できないように工夫しながら、情報セキュリティの実例集としてご報告する。

## 5.3　情報セキュリティの実例集

### 事例１ セキュリティ対策の理論と実際

A 社は金融業に分類される会社であり、その情報システム部は首都圏郊外のビルに入っている。その業態柄、監督官庁からの指示もあり、数年前から、会社全体として情報セキュリティ対策の取り組みを行っている。

A 社の情報システム担当の方は、数年前から各種のセキュリティセミナー等に参加したり、セキュリティ業者や、SI 会社から、様々な提案を受けたりしてきたが、どれも自社の環境にそのまま適用できるようなものではないと考えている。

実際、ウイルス・ワーム対策についても、全ての PC にアンチウイルスソフトを導入しているとともに、ウイルス・ゲートウエイ・サーバを導入しているが、ワームの発生を１００％食い止めることは出来ていない。

セキュリティポリシーの策定にあたっても、セキュリティ・コンサルタント等の外部への委託はせずに、情報システム部門が主体となって、各部門から情報セキュリティ担当者を選出し、自分たちでセキュリティポリシーの策定・運用を行っている。

最近の「個人情報漏えい関連の事件」への対応のために、FD、CD-R などの記録媒体を使った、情報の持ち出しが出来ないシステムの導入を行ったが、１００％のコントロールは不可能であり、やはり運用上の対策が重要であると考えている。

結局、セキュリティに関する様々な製品を導入する場合や、サービスの提供を受けるにあたっても、情報システムの導入と同様に、提供されたものをそのまま使うのではなく、自分たちで経験しながら適用していくことが必要と考えている。

### 事例２ システム開発の外注と、セキュリティの確保

B 社は製造業に分類される会社である。情報システムは基本的に自社で運営・管理している。昨今の情報セキュリティに関する流れから、昨年、JNSA のサイトにある、サンプルポリシーを参考に、セキュリティポリシーを策定したところである。

一方、昨年、勘定系のシステムの刷新に伴い、情報システムの全面更新を行ったが、自社の情報システム要員だけでは手不足なため、システム開発のための要員を外部から調達して開発を行った。

外注したシステム開発会社から派遣されてきた要員は、各々、ノート PC を持参してきており、それを使って開発することとなったが、アンチウイルスソフトの導入や、最新の定義ファイルの適用など、B 社のセキュリティポリシーに完全に統一することは不可能であった。

そのため、自社のセキュリティを確保するため、外部から派遣された開発要員には専用のネットワークを構築し、社内システムとは隔離した形で開発を行う事とした。

結果として、外部から持ち込まれたノート PC からのワームの感染が確認されたが、社内システムには影響を及ぼさず、隔離されたネットワーク環境内のみの感染に押さえることができた。

**事例３ 資産管理の重要性**

C 社は情報通信業に分類される会社である。主要な業務として、通信環境等のネットワーク構築等を行うことから、かなり以前より、セキュリティポリシーを策定し、情報セキュリティ対策には万全を期している。

全国各地に事業所は点在しているが、インターネットとの接続は、本社に一元化して外部とのアクセスの監視も行っている。

しかし、昨年の、MSBlaster 関連のワームについては、１００%防御することができず、外部から持ち込まれたノート PC により、ワームが感染してしまった。

感染は、複数の事業所で発見されたが、外部とのアクセスを本社にて一元管理し、ネットワークの監視をおこなっていることから、感染が検知された直後に、該当の PC の IP アドレスを特定し、対象の事業所に連絡することができた。

ところが、連絡された事業所では、ネットワーク接続（IP アドレスの振り方）を DHCP で行っていることから､本社から連絡された IP アドレスのみからでは、直接、感染している PC を特定することができず、あちこちと探し回ることとなってしまった。

ここで、幸いなことに、同事業所では、昨年 PC の総入れ替えを実施していたことから、配布した PC のマシン名（ホスト名）および、MAC アドレスを資産一覧として保存しており、マシン名、MAC アドレスから該当する PC の使用者を､帳簿上から調べることができた｡結果として感染している PC を特定し、ネットワークから切り離した上で、対策を行うことができた。

同社では、以前から資産管理ソフト（インベントリー収集ソフト）を導入しているが、あくまでソフトエアの資産管理にしか利用していなかったため､今後は､もっと有効に利用していこうと考えている。

**事例４ セキュリティ･マネジメント組織のあり方**

D 社は、製造業に分類される会社である。ISO9000, ISO14000 の認定は、業務上の必要性により以前から取得している。昨今の情報セキュリティの話題から、情報セキュリティのマネジメント体制構築にも取り組んでいる。

ISO9000, ISO14000 については、入札等の資格要件となっていることから認証の取得は必須であり、各々マネジメント体制の構築のため専任の担当者を設け、各部門にも担当者を設置している。

しかし、情報セキュリティについては、業務上の必要性がそれほど要求されないことから、ISMS 認証制度の取得は考えていない。

同社は、認証の取得までは考えてはいないが、情報セキュリティを確保するためには、システム的なセキュリティ対策と、情報システム担当者によるインシデント対応だけではなく、セキュリティポリシーの策定とその運用のための全社的なマネジメント体制を構築することが重要であると考えている。

実際に、情報セキュリティのマネジメント体制を構築するにあたり、ISO9000, ISO14000 と同様に専任者を設置し、各部署に担当者を設けることは現実的には不可能と考えた。

そして、会社組織のマネジメント体制、つまり、業務運営のための組織をそのまま、情報セキュリティ管理体制とすることとした。

具体的には、最高責任者を会社のトップとし、情報管理責任者を各部門の部門長として、セキュリティ委員会を設置し、事務局として情報システムの担当者が活動する体制とした。この体制は、情報セキュリティに関する規定を決定する、または、インシデント（セキュリティ事件・事故）の発生時においても効率的に機能する体制となっている。また、情報セキュリティ以外の危機管理体制としても、有効に機能するものと考えている。

**事例 5　事業継続計画 (BCP) 訓練実施の効果**

E 社は、情報サービス業に分類される会社である。システム開発や、ネットワーク関連機器の販売等を行っていることから、情報セキュリティに関しては積極的に取り組んでいる。そのため、ISMS 認証取得についても、認証制度が制定されると直に取得している。

E 社は、セキュリティポリシーの一部として、事業継続計画（BCP）を制定しており、ISMS 認証取得以降、定期的に、事業継続計画（BCP）の実施訓練を行っている。

事業継続計画（BCP）の実施訓練の内容は、「情報システムが何らかの障害により利用できなくなってしまった場合に、紙媒体による代替処理や、電話、FAX 等の通信手段の代替により、業務の継続を行う」というものである。

今時の企業であれば、電子メールによる顧客との連絡や、勘定系システムを使った受発注処理など、殆どコンピュータ化されていると思われるが、実際、それらが使えなくなった（停止した）場合に、はたして業務の継続が可能かどうかを真剣に検討している企業は、まだまだ少ないと思われる。

E 社の従業員の方々も、訓練を実施するまでは本当にそんなことが可能なのか？とかなり不安であったとのことである。

しかし、実際に、事業継続計画（BCP）に従った訓練を行ってみると、当初思っていたほどの混乱はなく、業務が継続できることが確認できたと言うことである。考えてみれば、つい、数年（3～4 年）前までは、殆どの業務が、紙ベースであり、顧客との連絡は電話、FAX が主体であったことから、不可能なものではないということがわかったということである。

コンピュータがなければ、事業が継続できないわけではなく、障害時の対応計画を事前に検討しておかないことから事業継続がストップするのだということが、身をもって実感できたということである。

**事例 6　事業部制からくる、セキュリティ対策の限界**

F 社は、建設業に分類される会社であり、日本各地に支社を持っている。各地の支社は、基本的に独立採算の事業部制をとっている。

F 社の情報システムは、基盤となる勘定系システムは本社で一元管理されているが、PC やソフトウエア等の購入については、各事業所単位で行っているため、本社ではその全体像は把握していない。

また、F 社の事業特性として、建設工事が始まると、その作業現場自体が、都度新たに事業所として設置され、PC の設置や、ネットワーク回線が敷設されるため、本社での全体像の把握は、殆ど不可能な状態である。

そのような中、F 社でワーム感染による大規模なネットワーク障害が発生し、各事業所間での通信が

不通になる被害が発生した。F 社では、Web を使った電子商取引を実施している部門もあり、全社的な問題としてクローズアップされることになった。

この事件の後、F 社の経営層から、全社の情報システム担当の方に対し、「F 社の情報セキュリティ対策の実情調査と、今後のリスク管理の実施」が指示され、以下のような対策を順次行ってきている。

- インターネットとの接続を本社に一本化
- メールについては、アンチウイルスサーバにて、全てウイルスチェックを実施
- 各事業所に対し、全ての PC にアンチウイルスソフトの導入と、最新のウイルス定義ファイルの適用を通達。
- 各事業所に対し、最新のセキュリティパッチの適用を通達

しかし、F 社の予算管理方法が、独立採算の事業部制であることから、各事業所に通達した内容を実施するにあたってのソフトの購入や、実施体制の足並みが揃わず、いまだにウイルスへの感染が発生し、苦慮している。

**事例 7 子会社のセキュリティ対策**

G 社は、製造業に分類される会社であり、日本各地に事業所を持っている。また製造業という業種柄、多数の子会社や、関連会社等のグループ会社を抱えている。

情報システムについては、全社としては ERP を導入し専任の情報システム担当が管理しており、各事業所や研究所では、各々兼務ではあるがかなり詳しい方々が情報システムの面倒をみており、情報セキュリティ対策についても全社として前向きに取り組んでいる。

特に、ウイルス・ワーム対策については、過去に、Nimda に感染し全社的に業務停止に陥った経験から、アンチウイルスサーバ（ゲートウエイ）の導入、全 PC へのアンチウイルスソフトの導入と、最新の定義ファイル更新、および、最新のセキュリティパッチの適用などを実施している。

そのような体制であっても、昨年の MSBlaster により、一部、業務が停止に追い込まれる事態が発生した。

具体的には、通常業務で使用している PC には、十分なウイルス対策を実施していたが、製造業務で使用するマシン(OS が Widows で動作するもの)が、ウイルス対策の対象から漏れていたためであった。これらは、そこで稼動しているソフトウエアの機能を使うためにハードウエアごとアプライアンスとして購入しており、セキュリティパッチの適用については、稼動しているソフトウエアのメーカーから動作保証されないという理由から実施していなかったのと、同じ理由から、アンチウイルスソフトウエアの導入も行っていなかったためであった。

この被害の発生を契機に、ソフトウエアメーカーに至急連絡をとり、ウイルスの駆除および、最新のセキュリティパッチの適用等を実施することとなった。

ここで、なぜ G 社のネットワークに MSBlaster が侵入したかについて、詳しい原因究明ができていないという事実を伺った。それは、G 社の管理している PC は、ほぼ全てウイルス対策が施されており、MSBlaster の発生した事業所では、外部からの PC の持ち込みが殆どない事業所であったからである。

G 社の情報システム管理担当の方のご意見を伺うと、「たぶん、グループ会社が感染し、そこから G 社のシステムに侵入したと思われる。」とのことであった。

G 社のセキュリティ対策は、自社内にはかなり浸透しているが、子会社を含む全てのグループ会社にまで、同様の対策を実施させることはできない。しかし、業務を遂行するうえで、子会社を含むグループ会社と専用線と同様のネットワーク接続をしていることから、そこからワームに感染したと想定されるとのことである。

今後は、グループ会社にもセキュリティ対策を要請していきたいと考えているが、子会社とはいえ資本の関係は様々であり一律の実施は困難であると考えている。

# 6. 2003 年度情報セキュリティインシデント被害額算出モデル(昨年から変更無し)

初年度(2001 年度)に作成した被害額の算出モデルを、昨年度(2002 年度)変更した。今年度については、特に変更していないが全体の理解のため、本章にて再度提示する。以下の内容は、昨年モデルと同じのため、本モデルを既知の方については、７章から読むことをお勧めする。

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。

## 6.1 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。

### 6.1.1 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

### 6.1.2 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

## 6.2 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。

### 6.2.1 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＝b ブ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)

## 6.3 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。

# 7. 被害状況及び対策・対応についての集約

本章では、アンケートで得られた被害の種類と被害状況や原因、事故対策・対応をまとめている。被害の発生状況や、対策等の参考としてご活用いただきたい。

| No | 被害種類 | 被害および原因の概要 | 事故対策･対応等 |
|---|---|---|---|
| 1 | DoS攻撃等でｻｰﾋﾞｽ停止 | ファイアウォールで遮断できているが、Dos攻撃に近いインターネット輻輳はしばしば観測される。 | - |
| 2 | DoS攻撃等でｻｰﾋﾞｽ停止 | 公開wwwサーバのＦＴＰサービスに対しての攻撃 | サーバ監視強化 |
| 3 | PC/PDAの盗難･紛失 | 電車内にてノートPCを盗難 | BIOSパスワード及びWindowsパスワードを設定してあり、情報は漏洩していないと思われる。 |
| 4 | PC/PDAの盗難･紛失 | 顧客データが保存されたPCが盗難にあった | モバイルPC管理対策の強化 |
| 5 | PC/PDAの盗難･紛失 | - | 退社時にはノートＰＣを机の中に収納し、鍵をかける様にした。 |
| 6 | PC/PDAの盗難･紛失 | 海外駐在員のＰＣ盗難。１人は電車内、もう１人はホテル内。 | 出張者のＰＣへの保険を強化。使用時のパスワード等の強化。出張者への呼び掛け。 |
| 7 | PC/PDAの盗難･紛失 | モバイルＰＣを駐車中の車内より盗難にあった（車上狙い） | ①ＰＣ内の情報（個人情報など）の管理の注意喚起。②全モバイルＰＣにＵＳＢセキュリティー･キーを導入（キーがなければ起動しない。ファイルは全て暗号化） |
| 8 | 社外公開ﾎｰﾑﾍﾟｰｼﾞ改竄 | ＴＯＰページの改ざん。 | プロバイダの変更。 |
| 9 | 情報の漏洩 | 顧客アドレスをBCCにする規程であるが、パート作業員が宛先に入れて送信してしまった | お詫びのメールを送付して完了 |
| 10 | 情報の漏洩 | セミナー案内で宛先をCCに入れ、送信先クレームが入った。 | 顧客からクレームが入り、担当者からお詫びメール。関係部署と取締役に報告。役員より再度お詫びメールし、その後全員へお詫びメール。 |
| 11 | 情報の漏洩 | 移動中の地下鉄内にてPCと顧客資料の入ったカバンを網棚に置いていたところ、カバンが盗まれた。後日カバンと資料は戻った。戻るまでの間、カバンの拾得者と思われる人物から、資料に記されていた顧客に対し不審な連絡が入った。 | - |
| 12 | 情報の漏洩 | 発信元詐称メールへのアドレス利用、リターンメール、SPAM | - |
| 13 | 不正ｱｸｾｽ | Linuxサーバ運用不可 | - |
| 14 | ウイルス被害 | - | 持ち出しパソコンの社内LAN制限を行った |

| No | 被害種類 | 被害および原因の概要 | 事故対策･対応等 |
|---|---|---|---|
| 15 | ウイルス被害 | 営業マンがインターネット経由で客先デモを行い、ウイルスに感染したと思われる。帰社後、社内LANに接続し、パッチを当てていないPCに感染 | 最新のパッチを当てていないPCは社内LANから切り離す。再度、最新定義ファイルの更新状況を確認 |
| 16 | ウイルス被害 | Virus対策ソフトのパターンファイル更新の隙間に入り込まれた。ただし、感染しても発症しない。(環境上の理由) | なし。既にVirusソフトは2社分入れており、これ以上の対応は困難。 |
| 17 | ウイルス被害 | メールによる第三者より感染。通常ウイルスチェックが働くと過信し、メール付ファイルを開き、2100通以上のメールを社外へ送付。 | ログの調査。ウイルス注意･喚起の連絡 |
| 18 | ウイルス被害 | リモートアクセス評価時にPC感染。このPCを社内LANに接続したことでウイルス対策ソフトをインスールしていないサーバに感染。NWの負荷が高まりダウン。各サーバをNWから切り離しウイルス削除。 | - |
| 19 | ウイルス被害 | ネットワーク停止 | 感染元端末にセキュリティパッチを対処 |
| 20 | ウイルス被害 | ID,パスワードをつくり、社内のPCにウイルスを広めた | - |
| 21 | ウイルス被害 | 社外に大量のPingを送るのでインターネットアクセスを停止した | - |
| 22 | ウイルス被害 | 送信元不特定から大量にウイルスメール。社員1名に50から100件ものメールを受信した。他社への被害はなし。 | - |
| 23 | ウイルス被害 | 顧客先ネットワークに当社のPCを接続し、ウイルス (Welchia.Worm)に感染。感染したPCを社内ネットワークに接続後、他のPCにウイルス検知のメッセージを表示し、感染していることが発覚した。 | 最新定義ファイル更新、リアルタイムスキャンを常時有効にしておく事を周知･徹底した |
| 24 | ウイルス被害 | MSBlasterに感染したPCの社内LAN接続によるパッチ未適用PCの感染 | パッチ適用の徹底強化 |
| 25 | ウイルス被害 | 最近のWindows Updateの適用及び最新のウイルスパターンファイルの適用がされていなかったPCに感染 | 社外とのポートフィルタリング実施。現在もそのままにしてある。ポートフィルタリングの体制を整備し、緊急対応できるようになった。 |
| 26 | ウイルス被害 | メールサーバによるウイルスチェックがパターンファイルの提供が遅かったため間に合わず、個人のPCに配信されてしまった。メールを受け取った本人がうっかり添付ファイルを実行してしまった。3台のPCが感染した。 | 事故の状況と対策を社内に周知し、再発防止を指示した。 |
| 27 | ウイルス被害 | Nachi,Welchia 感染。社内LANでWindows2000PCでセキュリティパッチMS03-026を適用していなかったものに感染した。 | - |
| 28 | ウイルス被害 | ①インターネットを経由してウイルスが侵入 ②Windowsの最新パッチがあたっていなかったので拡大した | Windowsに最新のパッチ付与を義務付けている。 |

| No | 被害種類 | 被害および原因の概要 | 事故対策･対応等 |
|---|---|---|---|
| 29 | ウイルス被害 | 外部より大量のウイルスメール受信によりメールサーバレスポンス低下 | - |
| 30 | ウイルス被害 | ①OSのインストール後、パッチ適用の前に感染　②管理者が不明なノートPCで、パッチ未適用のマシンを外につなぎ感染 | - |
| 31 | ウイルス被害 | ウイルス感染した私物のノートPCを社員が持ち込み、社内LANに接続したため、Windows Updateが行われていなかったPCに感染が広がった。 | - |
| 32 | ウイルス被害 | 検出しているため被害なし | - |
| 33 | ウイルス被害 | 社内LAN輻輳 | - |
| 34 | ウイルス被害 | プレゼン用ＰＣにＰＨＳ接続を行っていたノートＰＣが感染。 | - |
| 35 | ウイルス被害 | ウイルス感染したＰＣを社内ＬＡＮ接続したため。 | パッチ適応、パターン更新自動化、強化。 |
| 36 | ウイルス被害 | ①セキュリティホールへの対応が不備だったパソコンがあった為。②感染が早く、ウイルス検知･駆除プログラムの対応が間に合わなかった。 | - |
| 37 | ウイルス被害 | ウイルス感染した社外のＰＣを社内ネットワークに接続し、セキュリティ対策のなされていない社内ＰＣに感染した。 | - |
| 38 | ウイルス被害 | ＨＰ閲覧時に感染 | ウイルス対策ソフトで駆除、WindowsUpdate及びウイルスソフトの定義ファイルを最新のものに更新。 |
| 39 | ウイルス被害 | - | ウイルス対策ソフトで駆除、ＰＣ内のソフトのスキャン実施。 |
| 40 | ウイルス被害 | 電子メールの添付ファイルから感染 | ウイルス対策ソフトで駆除。 |
| 41 | ウイルス被害 | 外部から持ち込んだＦＤから感染 | 当該ＰＣにウイルス対策ソフトの最新版を再インストール。当該ＦＤ（2枚）を廃棄処分。 |
| 42 | ウイルス被害 | ＭＳのセキュリティパッチ適用を全社に指示をしてあったが、社外持込ＰＣからパッチ未適用ＰＣおよび新規導入ＰＣが感染した。 | セキュリティパッチ適用、ウイルス対策ソフトインストールの徹底。ＰＣ管理ツール、FWの監視強化。 |
| 43 | ウイルス被害 | 特に被害なし。メールＢＯＸに大量のメールが送信されたのみ。 | - |
| 44 | ウイルス被害 | メールサーバに大量のメールが滞留。転送が大幅に遅延した。 | - |
| 45 | ウイルス被害 | 長期出張から戻った社員のパソコンが感染。他のＰＣに感染し、ＤｏＳ攻撃が発生し、VoIP内線電話が利用できなくなった。 | パターンファイルは常に最新を保つよう指示。外部からのパソコンについてはウイルスチェックを行うよう指示。 |
| 46 | ウイルス被害 | 第3者にウイルス付きメールを送信した。 | パターンファイルのアップデート間隔の見直し |
| 47 | ウイルス被害 | メールサーバのレスポンス低下 | メールサーバのリプレースを予定 |
| 48 | ウイルス被害 | 2台のＰＣがウイルス感染したが、実害はなかった。 | 会社が貸与しているＰＣで、ダイヤルアップのインターネット接続の禁止を徹底した。 |

| No | 被害種類 | 被害および原因の概要 | 事故対策･対応等 |
|---|---|---|---|
| 49 | ウイルス被害 | 社内基幹サーバへの感染により、半日間のシステム停止。本社事業所ＰＣの感染による社内ネットワークの負荷増大。ネットワーク機器の一部機能停止等。（数分～数時間で復旧） | - |
| 50 | ウイルス被害 | 添付ファイルとして送信された事のみ | 特に被害なし |
| 51 | ウイルス被害 | 長期休暇中に感染し、社内LANに持ち込む。全PCの確認をする。 | 情報セキュリティの管理者の教育を徹底した。ウイルスソフトを自動更新に変更した |
| 52 | ウイルス被害 | 他社と同じ | - |
| 53 | ウイルス被害 | 社内ネットワークに接続しているパソコンのうちWin2000とWinXPのものがほとんど全てブラスタに感染し、ネットワークがほとんど使えなくなった。社内ネットワークに外部で感染したパソコンが持ちこまれ接続したためと推定。 | クライアントパソコンのウイルスパターンファイルの更新頻度を上げた。Windowsの最新バージョンへアップデートした。 |
| 54 | ウイルス被害 | 直接の被害はない。感染元の特定に時間がかかったこと。万全を機してOSを再インストールした等の手間のみ。 | - |
| 55 | ウイルス被害 | - | 外部監査の実施を行う。 |
| 56 | ウイルス被害 | ４０台のPCからウイルス発見 | - |
| 57 | ウイルス被害 | 社外から受信した添付メールを開いて感染 | 身に覚えのない相手からのメール、特に添付メール付、開かない事の全社掲示（電子掲示） |
| 58 | ウイルス被害 | ネットワーク監視システムによる異常トラフィクによる検知 | 出張先から持ち帰ったパソコンは社内LAN接続前にウイルスクリーニングする様指導。 |
| 59 | ウイルス被害 | MSブラスターに感染。社内の相当数のPCに被害が及んだ。動作不安定、ソフト起動異常、シャットダウン等が一部に発生。 | - |
| 60 | ウイルス被害 | - | 外部アクセス利用者の社内ネットワークへの接続禁止 |
| 61 | ウイルス被害 | - | ウイルス対策ソフトをメールサーバ、PCにインストール |
| 62 | ウイルス被害 | MSパッチを適用していなかった、あるいは適用が遅れ、約３０％のクライアントPCが感染し、ないし感染前（ウイルスが発見されたものの駆除できない旨のメッセージ表示）の状態となった。（サーバは早い段階で適用したため問題なかった） | - |
| 63 | ウイルス被害 | ウイルス対策ソフト（パターンファイル）対応前での感染。ランダムにＴＣＰパケット送信で社内ネットワークが不通となる。 | - |
| 64 | ウイルス被害 | プロキシサーバを経由せずにインターネット接続しているＰＣより、社内に侵入、社内にて増殖。 | - |
| 65 | ウイルス被害 | Ｎｏｄａｒｇに感染した、ウイルス定義ファイルのダウンロード前に感染したが、他のＰＣは無事だった。 | 英語メール（添付ファイル）は削除する様、通知した。（当社は国内企業のみ取引している。） |

| No | 被害種類 | 被害および原因の概要 | 事故対策･対応等 |
|---|---|---|---|
| 66 | ウイルス被害 | 社内センターサーバのＬＡＮのトラヒックが異常に高くなり、他サイトからもアクセスが殆ど出来なくなった。関連会社のサーバが、ＭＳＢlastに感染し、当社ネットワークを攻撃していた。 | 関連会社で当社ネットワークに接続している企業は、当社同等それ以上のウイルス対策を4月までに実施。 |
| 67 | ウイルス被害 | ＭＳのセキュリティパッチ未適用のクライアントＰＣで発生（発生源は特定できず）、ＬＡＮに接続されていたクライアントＰＣ数百台に感染、多量のＩＣＭＰパケット等により、社内ネットワークが停止状態となる。 | セキュリティパッチ適用、イベント管理の強化検討。 |
| 68 | ウイルス被害 | メールサーバ（レンタル）及び各社内クライアントに、ウイルスチェックソフトを導入していたが、ウイルス発生時には、まだパターンファイルの配付がメーカーからされていなかった。この状態で社員の１人が、ウイルスメールの添付資料を開いてしまった。 | 感染クライアントを、直ちにＬＡＮから外し、ウイルス駆除が確認出来るまで隔離した。 |
| 69 | ウイルス被害 | 社員の持ち込み個人ＰＣをネットワークに接続。そこからウイルスが蔓延した。社内ネットワークが遅くなり、通常利用不能の状態になった。パターンファイルの更新が出来ていないＰＣが感染した。感染数は数十台程度。 | パターンファイル更新の徹底と確認。必要なセキュリティパッチの適用を行った。 |
| 70 | ウイルス被害 | ウイルス対策ソフトのパターンファイルＮｏが、未最新のパソコンに侵入、被害が拡大した。 | パターンファイルの更新等検索ソフトの導入、サーバのＵｐＧｒａｄｅ。 |
| 71 | ウイルス被害 | MSBlasterが、社内ＬＡＮ（特に持込みＰＣ、ダイヤルアップＰＣより感染あり。） | - |
| 72 | ウイルス被害 | 工場現場事務所で、使用のパソコンを（感染）、社内に持ち込みＬＡＮ接続したことで、社内感染･増殖。 | - |
| 73 | ウイルス被害 | 最新ウイルスがメールチェックをすり抜け感染。その後メールを発信し、被害拡大→メールサーバ停止。 | 定義ファイルの更新を、1日1回から2回とした。 |
| 74 | ウイルス被害 | ＶＰＮ接続された個人パソコンによりウイルス感染したものと思われる。感染した理由はＭＳ０３－０２６の脆弱性に対するセキュリティ修正を全体規模で行ってなかった。 | ＭＳＵＳ（ＭｉｃｒｏｓｏｆｔＳｏｆｔｗａｒｅＵｐｄａｔｅＳｅｒｖｉｃｅ）の導入（セキュリティ修正の徹底）。ウイルス対策ソフトの変更による集中監視体制の強化（一斉スキャンの開始）。 |
| 75 | ウイルス被害 | 社外よりのメール、ウイルスソフトにより発見、実害無し。 | - |
| 76 | ウイルス被害 | ネットワークの負荷が増大した。 | Ｗｉｎｄｏｗｓのアップデートの実施とウイルスチェック |

| No | 被害種類 | 被害および原因の概要 | 事故対策･対応等 |
|---|---|---|---|
| 77 | ウイルス被害 | 夏季休暇中、社外に持ち出していたＰＣが感染。休み明けに社内ネットワークに接続したことにより、社内ＰＣに感染。社内感染したＰＣのウイルス対策ソフトは最新パターンに更新されていなかった。感染数：１３３台。また、感染ＰＣから発信される大量のパケットにより、Ｌ３スイッチがダウン（3回／日）したため、本社内ネットワーク利用不可となった。 | 全クライアントのウイルス対策ソフトのパターンを最新にした。社外利用ＰＣのウイルス発生防止ガイドラインを作成、配布した。 |
| 78 | ウイルス被害 | 外部サーバ経由で感染。モバイル利用ＰＣ経由で感染。 | ルール教育の徹底。現場監査の実施。 |
| 79 | ウイルス被害 | ウイルス感染したＥ－Ｍａｉｌの添付文書を開き感染した。パターンファイルはパソコンの電源をＯＮした時に自動取込みするようになっているが、パターンファイルがまだできていなかった。メールソフトはマイナーなソフトな為、実害は無し。 | - |
| 80 | ウイルス被害 | 取引先とのＥＤｉ用の回線から感染。最新のパターンファイルの適用されているパソコンで発見。実害なし。 | パターンファイル適用をパソコン電源ＯＮ時に自動に変更。 |
| 81 | ウイルス被害 | ダイヤルアップ接続でインターネットに接続し、ウイルスに感染したパソコンを社内ＬＡＮに接続したため。 | ＯＳのアップデート、クライアントファイアウォールソフトの導入 |
| 82 | ウイルス被害 | ウイルスチェックソフトが導入されていないＰＣがあり、感染。その後、ウイルス対策を行っていないクライアント数台にネットワーク感染した。 | ウイルスチェックソフトが導入されていないＰＣをリストアップし、全クライアントにウイルスチェックソフトを導入。 |
| 83 | ウイルス被害 | ＬＡＮを利用してパターンファイルを更新するシステムになっているが、モバイルＰＣでパターンファイルの更新されていない端末があり感染した。 | モバイルＰＣはＬＡＮ接続をして、パターンファイルを更新するようにアナウンスした。 モバイルＰＣを優先してＷｉｎｄｏｗｓＵｐＤａｔｅを行った。 |
| 84 | ウイルス被害 | 社内数事業所でウイルス感染の報告があった。 | - |
| 85 | ウイルス被害 | メール以外からの持込。 | 社内でパッチ当ての案内を公開 |
| 86 | ウイルス被害 | スパムメールの発信を社外より指摘された。 | - |
| 87 | ウイルス被害 | 感染したＰＣが持ち込まれ、一部のパッチ未適用のサーバが停止して発覚 | パッチ適用、ＩＤＳ導入。 |
| 88 | ウイルス被害 | Ｗｅｂメールを閲覧して感染。メールサーバ上ではチェックしていたが、Ｗｅｂメール（ＨＴＴＰ）の為、チェックされなかった。その後社内に広がり感染がわかった。対策ソフトのパターンファイルが最新でなかったのも原因の一つである。 | - |
| 89 | ウイルス被害 | ウイルス感染したＰＣが、共有ファイルに感染したため。 | ウイルス対策ソフトをサーバにも導入。 |

| No | 被害種類 | 被害および原因の概要 | 事故対策･対応等 |
|---|---|---|---|
| 90 | ウイルス被害 | 会社のＰＣを外部に持ち出し、そこで感染した。そのまま社内に接続。社内のＰＣには、ウイルスバスターがインストールされている為、大きな被害はなかった。 | - |
| 91 | ウイルス被害 | - | 不正ＰＣアクセス防止のためのインフラ対策等 |
| 92 | ウイルス被害 | ＭＹＤＯＯＭによるウイルスメールの送受信。ウイルスソフトのパターンファイル更新前にウイルス感染。 | ウイルス対策ソフトによる隔離 |
| 93 | ウイルス被害 | 社内ネットワークに外部ＰＣを接続 | ウイルス対策ソフトの全機導入 |
| 94 | ウイルス被害 | 自宅からＭＯの持ち込み | ウイルスパターン更新徹底。 社外からのメディア持込禁止。 |
| 95 | ウイルス被害 | 特定業務用ＰＣ（サーバ、クライアント）にウイルス対策されておらず、外部からのＦＤで感染→業務ストップに至りそうになった。 | 業務ＰＣもＯＡと同じくウイルス対策する。 |
| 96 | ウイルス被害 | ＰＣ誤動作 | ワクチンソフトにて駆除、全社通知 |
| 97 | ウイルス被害 | 感染経路は不明だが、ウイルスによるネットワークトラフィック増加が確認された。翌日、各オフィスへＰＣの起動停止、およびワクチンソフトを配布した。しかしウイルスの感染は収まらず、3日間の休日中に対策を再検討し、休み明けに再度全社的にウイルス対策を実施し、翌月に収束した。 | 各端末のウイルス感染情報、アンチウイルスソフト導入状況を把握できるアンチウイルスソフトに更新した。 利用者に対しＷｉｎｄｏｗｓフォルダ共有についての説明、またＩＩＳ利用者へはセキュリティパッチの適用をお願いした。 Ｐｒｏｘｙサーバに「．ｅｍｌ」ファイルを要求しないようにフィルタを設定した。 |
| 98 | ウイルス被害 | 被害を受けたと思われるパソコン及びそのＬＡＮセグメントを全社ネットワークより切離し、駆除ツールによるウイルス駆除と、周辺パソコンのウイルス検出を実施し、対策。原因はウイルスパターンファイル適用前に感染したと思われる。 | ウイルスパターンファイルの即時適用 |
| 99 | ウイルス被害 | 異常終了するＰＣが続発。ある事務所から本社との通信が遅くなり、インターネットやメール参照に支障が出始める。 | パッチ適用の早期化。 パターンファイル更新の早期化。 |
| 100 | ウイルス被害 | 持出用パソコンが社外で感染し、社内ネットワークに接続した時に広がった。 | 持出パソコンは社内ネット接続前に必ず最新パターンによるウイルスチェックを行うように規定 |
| 101 | ウイルス被害 | メール転送先が感染した結果、アドレス帳にあるアドレスに大量発信した。 | メール転送先のセキュリティ対策を義務化した。 |
| 102 | ウイルス被害 | 感染ＰＣの不注意による接続 | 自動配布ツール導入検討、ＩＴリスク管理体制整備 |
| 103 | ウイルス被害 | 低速回線で接続される拠点により、ＷＡＮ負荷増大に伴い本社サーバへの接続ができなくなった。 | 全社ＰＣ、ＷｉｎｄｏｗｓサーバへのＷｉｎｄｏｗｓ Ｕｐｄａｔｅの徹底 |
| 104 | ウイルス被害 | 社外持ち出しパソコンの社内ＬＡＮ再接続。 外注会社のパソコン持込み。 | パソコンの持ち出し、持ち込みに対するルール強化。社内通達。 パソコン利用状況一斉点検。 |

| No | 被害種類 | 被害および原因の概要 | 事故対策･対応等 |
|---|---|---|---|
| 105 | ウイルス被害 | 海外子会社から大量のメールが届き、ネットワーク速度が著しく遅くなった。 | - |
| 106 | ウイルス被害 | 社内ネットワークに接続してＯＳのセキュリティパッチの自動更新がされて居なかった。海外へ出張した者が帰国後、故障として持参した。 | - |
| 107 | ウイルス被害 | プリンタに文字化けした文章が多数出力。 | - |
| 108 | ウイルス被害 | 禁止している個人ＰＣの社内ネット接続にて感染拡大。 | - |
| 109 | ウイルス被害 | ウイルス監視ソフトによる検知（ワクチン最新版を適用のため感染なし） | ＯＳのパッチ当て作業 |
| 110 | ウイルス被害 | 社外に持出したＰＣがインターネットアクセス実行によりウイルス感染。気づかずに社内ネットワークに接続し、社内ＰＣに感染活動を行った。 | ウイルスソフトのインストールの徹底、再教育。 |
| 111 | ウイルス被害 | 感染した個人用ＰＣの社内ＬＡＮへの接続。 | - |
| 112 | ウイルス被害 | １人の従業員が会社のファイア･ウォールを経由せずに、別のプロバイダに接続したためと思われる。 | パッチの実施、社内広報。 |
| 113 | ウイルス被害 | モバイルＰＣがウイルス感染し、動作が不安定になった。 | ウイルス対策ソフト管理サーバのパターンファイルの更新を１回／日から１０回／日とした。 |
| 114 | ウイルス被害 | - | WindowsUpdataの実施、ワクチン |
| 115 | ウイルス被害 | インターネットブラウザ検索よりウイルスダウンロード（侵入）、マイクロソフトネットワークを設定していた一部ネットワークより感染が拡大。 | 社内システム関係のみのウイルス対策費用 |
| 116 | ウイルス被害 | 会社として接続している以外のダイヤルアップ接続ＰＣより感染。他事業所のウイルス対策は済んでいたが、当該事業所は未済の状況であった為、複数ＰＣに感染、即ちにウイルスソフトをインストールし、解消した。外部への感染はなし。 | ダイアルアップ接続していた当人に接続しない旨通達。 |
| 117 | ウイルス被害 | 社外持出しＰＣにより、社内ＬＡＮ内に侵入。 | - |
| 118 | ウイルス被害 | ウイルス対策ソフト会社のパターンファイル提供前に感染（取引先からのＥメール）した。 | - |
| 119 | ウイルス被害 | 社外から持ち込まれたウイルス感染パソコンが、無許可でＬＡＮに接続され、各部門が独自に購入したウイルスソフト対策ソフトがインストールされていないパソコンにも感染が広がり、ブロードキャストアドレスへのPINGにより、工場のプロコンサーバ（WinNT）がネットワーク負荷に耐えられずダウンした。 | ウイルス対策ソフト未導入パソコンへの対策ソフトインストールの徹底（会社説明会、個別確認） |

| No | 被害種類 | 被害および原因の概要 | 事故対策･対応等 |
|---|---|---|---|
| 120 | ウイルス被害 | ゲートウェイサーバへのワクチン自動更新よりも、感染拡大が早かった。 | - |
| 121 | ウイルス被害 | 夏休み明けに持ち出しＰＣを社内ネットワークに接続して感染。 | - |
| 122 | ウイルス被害 | 最近のウイルス定義ファイルの更新前であった。幸いにも広がりもなく早期に対策できた。 | サーバより最近のウイルス駆除ツールを自動配信 |
| 123 | ウイルス被害 | - | ウイルス駆除ファイルを強制配布にする。パッチ当ての仕組み構築中。 |
| 124 | ウイルス被害 | パソコン内の資料が消滅 | - |
| 125 | ウイルス被害 | ウイルス感染したＰＣが内部でＬＡＮに接続され、社内ではWindows系のセキュリティホール対応が充分でなかったこと、アンチウイルスソフトのパターン更新が一部行われていない（本来は自動）ことから、ＬＡＮ内で異常な通信が発生し、全ＬＡＮ（3拠点）がダウンした。海外でも1拠点で影響があった。 | Windows系セキュリティホール対応用のサーバ構築。リモートＰＣのウイルス対策強化。 |
| 126 | ウイルス被害 | ウイルスメールの送信元が偽造されているので分からない。社内で感染しているのか、第三者なのか？ | - |
| 127 | ウイルス被害 | 本部－支店間のＷＡＮ不調。社外への拡散を防ぐためインターネットサービスを一時停止。 | セキュリティパッチ適用の自動化検討 |
| 128 | ウイルス被害 | 社外でのインターネット接続（海外、中国と思われる）時に感染。その後、社内ＬＡＮに接続時発生。 | パソコン持ち出しの手順書を作成。（アンチウイルスの徹底） |
| 129 | ウイルス被害 | クライアントのウイルスチェックソフトでの検知後、サーバへのパッチ当てを実施。実害は無し。 | - |
| 130 | ウイルス被害 | インターネットにダイヤルアップ接続で利用していたＰＣの社内ＬＡＮ接続による感染。 | 最新定義ファイルの自動更新の仕組みを全社展開した。ＭＳのセキュリティパッチの”緊急”分については、必ず適用する運用とした。 |
| 131 | ウイルス被害 | 営業員が誤ってウイルス付メールの添付ファイルを実行。使用しているパソコンは、ウイルス対策ソフトがインストールされていたが、ＯＦＦにされていた。 | ウイルスが実行されたパソコンの登録してあった連絡先へＴＥＬにて謝罪。メールアドレス5ヶ所に送信された。 |
| 132 | ウイルス被害 | モバイルＰＣを自宅のＬＡＮに接続し、ウイルスチェックソフトを終了したため感染したと推定。その後、感染ＰＣを社内ＬＡＮに接続し、計57台のＰＣに感染した。 | - |
| 133 | ウイルス被害 | 社外のネットワークを社内に接続し、そのネットワーク経由でウイルスが侵入。ほぼ全社的に感染。 | WindowsUpdateの徹底。 外部ネットワークと社内ネットとの接続厳禁の徹底。 |

| No | 被害種類 | 被害および原因の概要 | 事故対策･対応等 |
|---|---|---|---|
| 134 | ウイルス被害 | 会社のＰＣを自宅に持ち帰り、このＰＣを自宅のインターネットに接続した際に感染した。この感染したＰＣを会社のネットワークに接続した事により、MS社のセキュリティパッチが適用されていないＰＣに次々と感染が広がり、社内ネットワークが使用不可となった。1ヶ月前にイントラでセキュリティパッチを適用するように注意を促していたが、半数以上のＰＣが適用されていなかった。 | セキュリティパッチの自動化ツールの導入。 |
| 135 | ウイルス被害 | ＭＳブラスタ感染によりＮＷが遅くなる。 | 対策システム強化 |
| 136 | ウイルス被害 | ＳＱＬSlammerによるUDP１４３４へのアタック。 | ネットワーク設定の見直し |
| 137 | ウイルス被害 | MSBlasterWarmの社内蔓延、システム感染。 | 修正モジュールの適用プロセス整備 |
| 138 | ウイルス被害 | 感染したウイルス（Welchia）が感染前日に発見されたばかりのものだったため、感染防止対策が間に合わなかった。侵入経路としては、ファイアウォールで遮断できないインターネット接続サーバ（Webサーバ等）が感染し、社内ネットワークに広がったものと推測される。 | ①ウイルスパターンファイルの自動更新運用。②社内ＬＡＮ接続パソコンの管理強化。③障害復旧手順の整備。④危機管理体制の確立。 |

# 8. 最後に

近年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にも「被害額」の項目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。

当ワーキンググループにおいては、アンケートの被害項目の細分化を行いながら、JNSA 会員および RISTEX の協力を得て昨年を大きく上回る企業数のインシデントに関する調査や検討を行うことができた。

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の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、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。

一方、今回の調査では、第２部(別冊)において、昨年に続き、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新しい推定モデルを示すとともに、企業価値の一端を示す株価への影響についても検証した。

今年度は、漏洩した情報の賠償金額の推定モデルでは、「プライバシー面」と「経済面」を大きな２軸として考えて、金額を算出する方法を提案した。

被害の数値算出および算出課程を明示したことで、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の推進や安全な情報化社会の形成に役立つことを期待したい。

毎年のこととなってきたが、今回の調査および報告書作成については、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、貴重な時間を頂戴しており、この場でお礼を申し上げたい。

これに加え今年度は、「警察庁生活安全企画課セキュリティシステム対策室」より、多大なるご助言を頂いたことについても、重ねて謝意を表したい。

ワーキンググループの活動と本報告書が、企業の情報セキュリティ活動上の参考となり、今後の情報セキュリティレベル向上の一助になることを願う。

# 9. 参考資料

## 9.1 アンケート用紙(JNSA 実施分)

# 情報セキュリティ被害調査アンケート(JNSA 実施分)

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（%） | | % |

**B-5 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>

## 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 *C-1で「1 ない」以外を回答した方のみご回答下さい。*

**情報セキュリティの制定時期についてご回答下さい。**

| | |
|---|---|
| **制定年** | **年** |

**C-4 *C-1で「1 ない」以外を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の見直し状況についてご回答下さい。(該当全てに○をお付け下さい)**

| | | |
|---|---|---|
| 1 | 見直しルールがない | |
| 2 | 見直しルールがある(不定期) | |
| 3 | 見直しルールがある(1年以下の頻度) | |
| 4 | 見直しルールがある(2年以上の頻度) | |
| 5 | 分からない | |

<その他>

**C-5 前回の見直し時期(見直していない場合には制定時期)についてご回答下さい。(該当全てに○をお付け下さい)**

| | | |
|---|---|---|
| 1 | 1年以内 | |
| 2 | 2年未満 | |
| 3 | 2年以上 | |
| 4 | 分からない | |

<その他>

**C-6 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-7 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○）**

| | | 体制の有無 | 最近1年以内に設置 | 事故を契機に設置 |
|---|---|---|---|---|
| 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が設置されている | | | |
| 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-8 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-9　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-10 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）**

| | | 計画・体制の有無 | 最近1年以内に設置 | 事故を契機に設置 |
|---|---|---|---|---|
| 1 | 発生事象別の被害状況の確認事項 | | | |
| 2 | 被害状況の確認責任者 | | | |
| 3 | 被害発生時の社内連絡体制 | | | |
| 4 | 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） | | | |
| 5 | 従業員への情報開示方法と情報開示レベル | | | |
| 6 | 第三者への情報開示方法と情報開示レベル | | | |
| 7 | 復旧時の確認事項 | | | |
| 8 | 定めていない | | | |
| 9 | 分からない | | | |

<その他>

**C-11 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-12 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-13 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 | 取得年 |
|---|---|---|---|---|---|
| 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-14 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-15　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-16 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(%)** | | **%** |
| **前年のｾｷｭﾘﾃｨ予算に対する増減金額(万円)** | ＋, － | **万円** |

**C-17 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-18　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サーバ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-19 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)**

| | | 導入項目 | 最近1年以内に導入 | 事故を契機に導入 |
|---|---|---|---|---|
| 1 | メールの監視 | | | |
| 2 | Webメールの監視 | | | |
| 3 | サーバのアクセス制限 | | | |
| 4 | 外線電話の監視 | | | |
| 5 | 書類の持ち出し制限 | | | |
| 6 | ノートPC(OA機器)の持ち出し制限 | | | |
| 7 | ノートPC(OA機器)の持ち込みLAN接続制限 | | | |
| 8 | サーバルームへの立ち入り制限 | | | |
| 9 | FD、USBメモリなどの記録媒体の持ち出し制限 | | | |
| 10 | FD、USBメモリなどの記録媒体の廃棄基準 | | | |
| 11 | PC(OA機器)の廃棄基準 | | | |
| 12 | 鍵暗号システムによる文書データ、メール暗号化 | | | |
| 13 | 個人認証デバイスによる認証システム(ｱｸｾｽ、入退室) | | | |
| 14 | バイオメトリクスを用いた認証システム(ｱｸｾｽ、入退室) | | | |

**<その他>**

**C-20 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-21 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-22 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>

## 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４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＞

| | | |
|---|---|---|
| **A-1 被害コード一覧表から選択してください。** | | 被害コード【　1　】 |
| **B-1 発生日時** | 2003年　2月　10日　12時　00分 頃 | |
| **C-1 どのように被害を知りましたか、該当する項目に○をお付けください。(複数選択可)** | | |
| 1) 社内の当事者本人(※1)からの報告 | | (※1) 感染者・被害者・誤操作した本人など<br>(※2) 各種ログ、監視カメラ、など具体的に記述ください |
| 2) 取引先からの報告 | ○ | |
| 3) 取引先以外の第三者から報告 | | |
| 4) メールの監視で検知 | | |
| 5) ファイアウォールやIDSで検知 | | |
| 6) その他(※2) | 顧客連絡で送信先として指摘され、社内調査を行いマシンを特定した | |
| **D-1 インシデント被害の原因など概要を簡単にお書きください。(書式自由)** | | |
| ウイルス感染したE-Mailを職員が開封し感染。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。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。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。 | | |
| **E-1 被害を及ぼした範囲をご回答ください。該当する項目に○を付け、お答えいただける範囲で被害を受けた箇所の数もご記入ください。(複数選択可)** | | |
| 1) 本社内LANに被害を受けた | ○ | |
| 2) 支店や営業所などにも被害を及ぼした | ○ | 【　5　】箇所 |
| 3) 取引先にも被害を及ぼした | ○ | 【　3　】箇所 |
| 4) 取引先以外の外部に被害を及ぼした | | 【　　】箇所 |
| 5) その他 | 【　　】 | |
| **E-2 社内でご使用のコンピュータの内被害を受けたおおよその台数をご回答ください。** | | |
| 1) 外部公開サーバ | 【　1　】台 | |
| 2) 社内サーバ | 【　4　】台 | |
| 3) クライアントPC | 【　50　】台 | |
| **E-3 影響を受けたおおよその従業員数をご回答ください** | 【　80　】人 | |
| **E-4 おおよそのシステム停止時間をご回答ください。** | 【　12　】時間 | |
| **E-5 システムのおおよその年間売上をご回答ください(※3)。** | 【　2000万　】円 | |
| *↑(※3) ホームページで物販など有償サービスを行っており、そのシステムで直接的に得ている年間売上金額をご記入ください* | | |
| **E-6 システム停止により発生したおおよその機会損失をご回答ください。(見込み利益で逸失分、売上増分の逸失など)** | 【　20万　】円 | |
| **F-1 対応を開始してから復旧完了までのおおよその時間をご回答ください。** | 【　24　】時間 | |
| **F-2 復旧に携わったおおよその人数をご回答ください。** | 【　20　】人 | |
| **F-3 従業員の一日あたりのおおよその人件費をご回答ください。** | 【 25000 】円 | |
| **F-4 代替手段によるおおよその営業継続費をご回答ください。** | 【　10万　】円 | |
| **代替手段の内訳をご回答ください。(例: 代替設備設置、手作業による処理など)** | | |
| 電話、FAXなどによる対応を行い。作業時間が多く掛かり、かつ行えない作業が多く発生した。 | | |
| **F-5 データの復元に要したおおよその費用をご回答ください。** | 【 10万 】円 | |
| **F-6 その他復旧に要したおおよその費用をご回答ください。** | 【　不明　】円 | |
| **その内訳をご回答ください。** | | |
| 電話やFAXで受け付けたデータのデータ化作業 | | |
| **G-1 賠償・補償が発生した場合はそのおおよその金額をご回答ください。** | 【　不明　】円 | |
| **G-2 その他関連する出費があればご回答ください。** | | |
| 1) お詫び広告 | 【　500万　】円 | 3) お詫び行脚　【　10　】日人工 |
| 2) 謝罪出状 | 【　50000　】円 | 4) その他　[臨時の深夜残業代30万円] |
| **H　事故後の対策について、ご回答ください。** | | |
| ・最新定義ファイルの更新状況を確認できる体制とした。<br>・発見時の緊急対応として、LANケーブルの引き抜きと共に、無線LANアクセスポイントの電源オフを行う事とした。 | | |

## ＜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、同時に、実行可能形式ファイルへの感染活動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」も有り。メールのタイトルや本文に「CodeRed対策パッチ」などと記載し、ファイルを開くように促すタイプもある。 |
| 2 | ワーム型ウイルス | SOBIG (ソービッグ) | ワームに分類されるトロイの木馬型不正プログラム。特定の拡張子を持つファイルからメールアドレスを検索し、それらの宛先に自身のコピーを自らのSMTPエンジン機能を用いて送信する。亜種には、読み書き可能なWindows共有ネットワークを通じて感染するものもある。 |
| 3 | 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。ワームとして自身のコピーをメールに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。 |
| 4 | ワーム型ウイルス | MSBlaster (エムエスブラスター) | WindowsのRPCサービスのセキュリティホールを突いて感染するトロイの木馬型不正プログラム。Webアクセスなどのユーザによる能動的な操作を必要とせず、ネットワークに接続されているだけで感染する感染力の強さが大きな特徴。感染すると、Windowsが突然再起動したりするなど不安定な挙動を示すことが知られている。また、システム日付が特定の期間になると、windowsupdates.comへのDOS攻撃を行うことも知られている。 |
| 5 | ワーム型ウイルス | Sircam (サーカム) | Sobigとよく似た動きでメールアドレスを検索し、自身のコピーをメールに添付して送信するが、添付ファイルが「自身のコピー＋感染したPCからランダムに選んだファイル」の形式で、一見、問題の無い添付ファイルのように見えるのが特徴。メール以外には、Windowsの共有ドライブを通じても感染する。 |
| 6 | その他のウイルス被害 | | 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。 |
| 7 | PC/PDAの盗難・紛失 | | PCやPDAの紛失に起因する情報漏洩などの被害 |
| 8 | 誤操作によるデータの消失やシステムダウン | | 手順誤りなどヒューマンエラーなどによるトラブル |
| 9 | その他の不正ｱｸｾｽ | | 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 |
| 10 | 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 |
| 11 | 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 |
| 12 | 情報の漏洩 | | 媒体による情報の不正な持ち出しを含む |
| 13 | 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

| | | | |
|---|---|---|---|
| **A-1 被害コード一覧表から選択してください。** | | 被害コード 【　　】 | |
| **B-1 発生日時** | 年　　月　　日　　時　　分 頃 | | |
| **C-1 どのように被害を知りましたか、該当する項目に○をお付けください。(複数選択可)** | | | |
| 1) 社内の当事者本人 (※1) からの報告 | | (※1) 感染者・被害者・誤操作した本人など<br>(※2) 各種ログ、監視カメラ、など具体的に記述ください | |
| 2) 取引先からの報告 | | | |
| 3) 取引先以外の第三者から報告 | | | |
| 4) メールの監視で検知 | | | |
| 5) ファイアウォールやIDSで検知 | | | |
| 6) その他 (※2) | | | |
| **D-1 インシデント被害の原因など概要を簡単にお書きください。(書式自由)** | | | |
| | | | |
| **E-1 被害を及ぼした範囲をご回答ください。該当する項目に○を付け、お答えいただける範囲で<br>被害を受けた箇所の数もご記入ください。(複数選択可)** | | | |
| 1) 本社内LANに被害を受けた | | | |
| 2) 支店や営業所などにも被害を及ぼした | | 【　　】箇所 | |
| 3) 取引先にも被害を及ぼした | | 【　　】箇所 | |
| 4) 取引先以外の外部に被害を及ぼした | | 【　　】箇所 | |
| 5) その他 | 【　　】 | | |
| **E-2 社内でご使用のコンピュータの内被害を受けたおおよその台数をご回答ください。** | | | |
| 1) 外部公開サーバ | 【　　】台 | | |
| 2) 社内サーバ | 【　　】台 | | |
| 3) クライアントPC | 【　　】台 | | |
| **E-3 影響を受けたおおよその従業員数をご回答ください** | 【　　】人 | | |
| **E-4 おおよそのシステム停止時間をご回答ください。** | 【　　】時間 | | |
| **E-5 システムのおおよその年間売上をご回答ください (※3)。** | 【　　】円 | | |
| *↑ (※3) ホームページで物販など有償サービスを行っており、そのシステムで直接的に得ている年間売上金額をご記入ください* | | | |
| **E-6 システム停止により発生したおおよその機会損失をご回答ください。<br>(見込み利益で逸失分、売上増分の逸失など)** | 【　　】円 | | |
| **F-1 対応を開始してから復旧完了までのおおよその時間をご回答ください。** | 【　　】時間 | | |
| **F-2 復旧に携わったおおよその人数をご回答ください。** | 【　　】人 | | |
| **F-3 従業員の一日あたりのおおよその人件費をご回答ください。** | 【　　】円 | | |
| **F-4 代替手段によるおおよその営業継続費をご回答ください。** | 【　　】円 | | |
| **代替手段の内訳をご回答ください。(例: 代替設備設置、手作業による処理など)** | | | |
| | | | |
| **F-5 データの復元に要したおおよその費用をご回答ください。** | 【　　】円 | | |
| **F-6 その他復旧に要したおおよその費用をご回答ください。** | 【　　】円 | | |
| **その内訳をご回答ください。** | | | |
| | | | |
| **G-1 賠償・補償が発生した場合はそのおおよその金額をご回答ください。** | 【　　】円 | | |
| **G-2 その他関連する出費があればご回答ください。** | | | |
| 1) お詫び広告 | 【　　】円 | 3) お詫び行脚 | 【　　】日人工 |
| 2) 謝罪出状 | 【　　】円 | 4) その他 | 【　　】 |
| **H　事故後の対策について、ご回答ください。** | | | |
| | | | |

## 9.2　アンケート用紙(RISTEX 実施分)

# 情報セキュリティ被害調査アンケート(RISTEX 実施分)

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（%） | | % |

**B-5 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>

**B-6 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) | | |

**B-7　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>

**B-8　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(%) | | % |
| 前年のｾｷｭﾘﾃｨ予算に対する増減金額(万円) | ＋, － | 万円 |

**B-9　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＞

**B-10　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>

**B-11　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 | 取得年 |
|---|---|---|---|---|---|
| 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)＞

***B-12　情報セキュリティに関する監査、教育についてご回答ください。(該当全てに○をお付け下さい)***

| | | |
|---|---|---|
| *1* | *外部監査機関の情報セキュリティ監査を実施している。* | |
| *2* | *社内の部署が情報セキュリティについて内部監査を実施している。* | |
| *3* | *情報セキュリティについて全従業員を対象に教育している。* | |
| *4* | *上記の取り組みは個人情報保護の一環として行っている。。* | |

**C 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。**

## ＜以下、ＪＮＳＡ実施分に同じ＞