JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

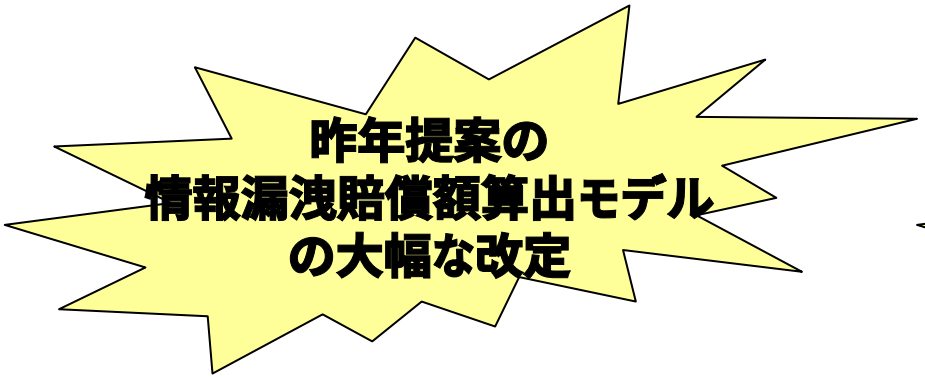
# 情報セキュリティ被害調査ワーキンググループ

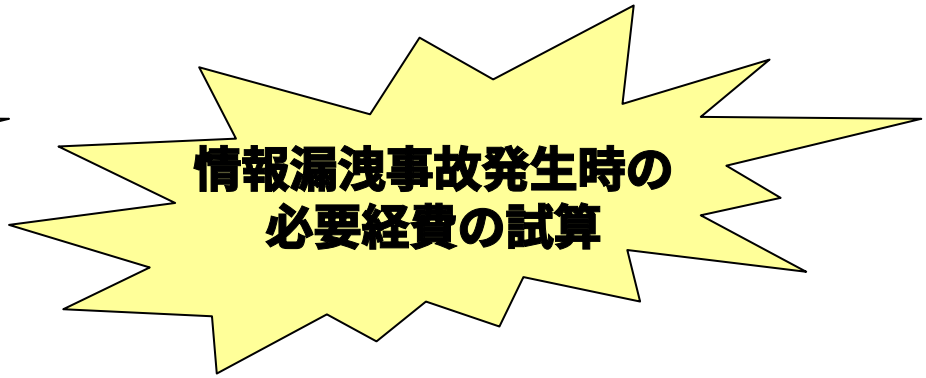
## 活動発表

2004 年 5 月 18 日

# 1．情報セキュリティ被害調査WG活動目的

- 国内におけるセキュリティインシデントに関する**幅広い現状把握**。
- 調査結果を基に、セキュリティインシデントの**被害額や対策額を推計するモデル提案**。
- 効率的な情報セキュリティマネジメントのツールとして、**モデルを精緻化**。



# 2．具体的な活動･成果

JNSA

- 第1部：被害の実態や対策の状況をつかむため、調査を実施し、傾向を把握。
- RISTEX協力による調査数の大幅増。

金銭的な被害額を知りたい。

→「情報セキュリティインシデントに関する調査および被害算出モデル」の実施

- 第2部：情報漏洩の被害額算出。
- 着眼点→賠償＆株価下落。

2次的な被害額の予想

→「情報漏洩による被害想定と考察(賠償額および株価影響額)」の提案

# 3．アンケート結果

## 1．アンケート回収率とヒアリング件数

| | 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% |

JNSA**のみ**　2002**年調査**　**送付**179　**回答**66　**回答率**36.8%

# A-1属する主要業種

| | 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% |

情報系への偏りが修正

## A-2年間売上および従業員数

■ 平均値

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

（昨年： 年間売上約1700億円、従業員1800名）

## A-3拠点数

| | 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% |

拠点数の多い企業への調査

# B-1保有PCの台数

| | 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% |

# B-2インターネットメールの利用状況

| | 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% |

基幹系との分離

添付ファイル制限

## B-3 WEB閲覧状況

| | 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% |

増えている

## B-4 インターネット利用可能ＰＣの割合

■ 平均値

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

(昨年： メール90%、Web閲覧85%)

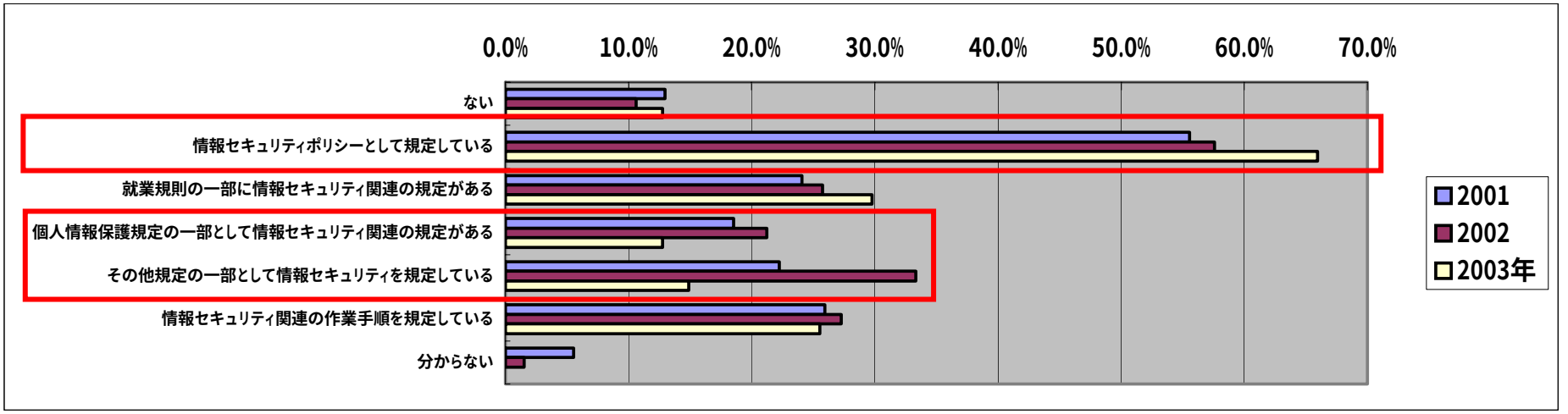
# 4．情報セキュリティ状況の変化

(JNSA調査分のみ)

## C-1 情報セキュリティに関する規定について

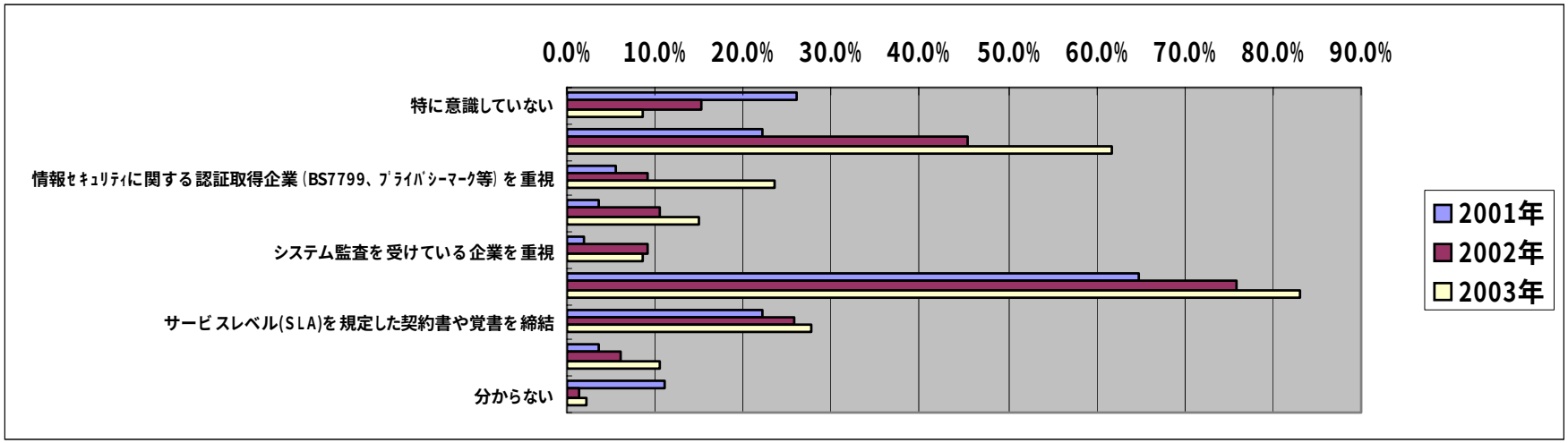
| | | 2001 | | 2002 | | 2003 | |
|---|---|---|---|---|---|---|---|
| 1 | ない | 7 | 13.0% | 7 | 10.6% | 6 | 12.8% |
| 2 | 情報セキュリティポリシーとして規定している | 30 | 55.6% | 38 | 57.6% | 31 | 66.0% |
| 3 | 就業規則の一部に情報セキュリティ関連の規定がある | 13 | 24.1% | 17 | 25.8% | 14 | 29.8% |
| 4 | 個人情報保護規定の一部として情報セキュリティ関連の規定がある | 10 | 18.5% | 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% |

独立して設定



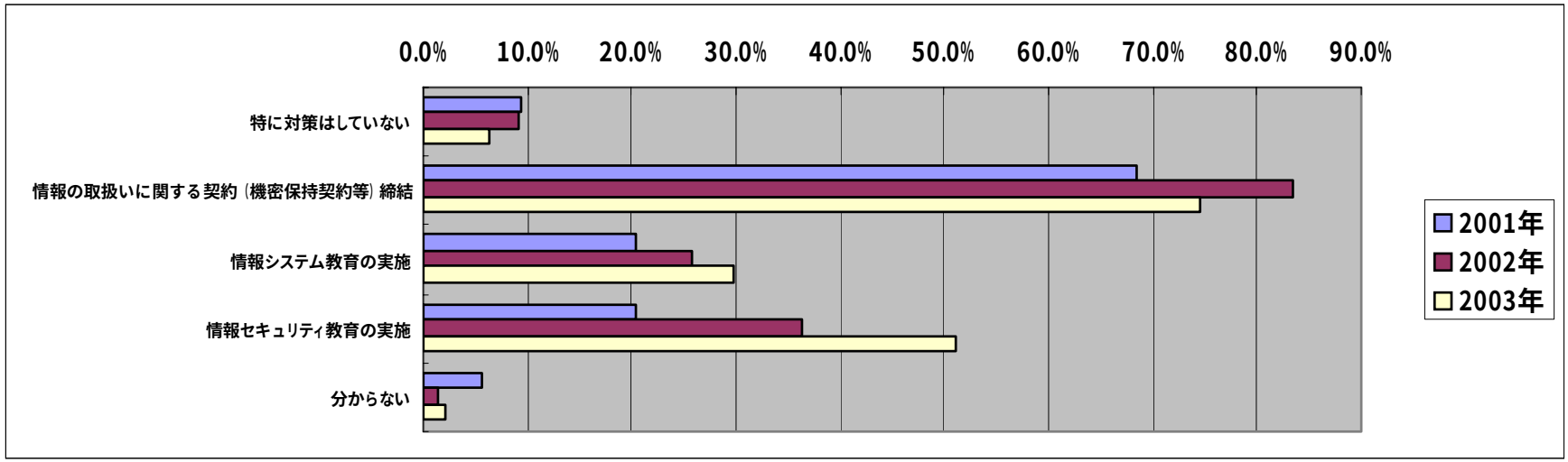
# C-8 取引先の選定や契約時の注意点

| | 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% |



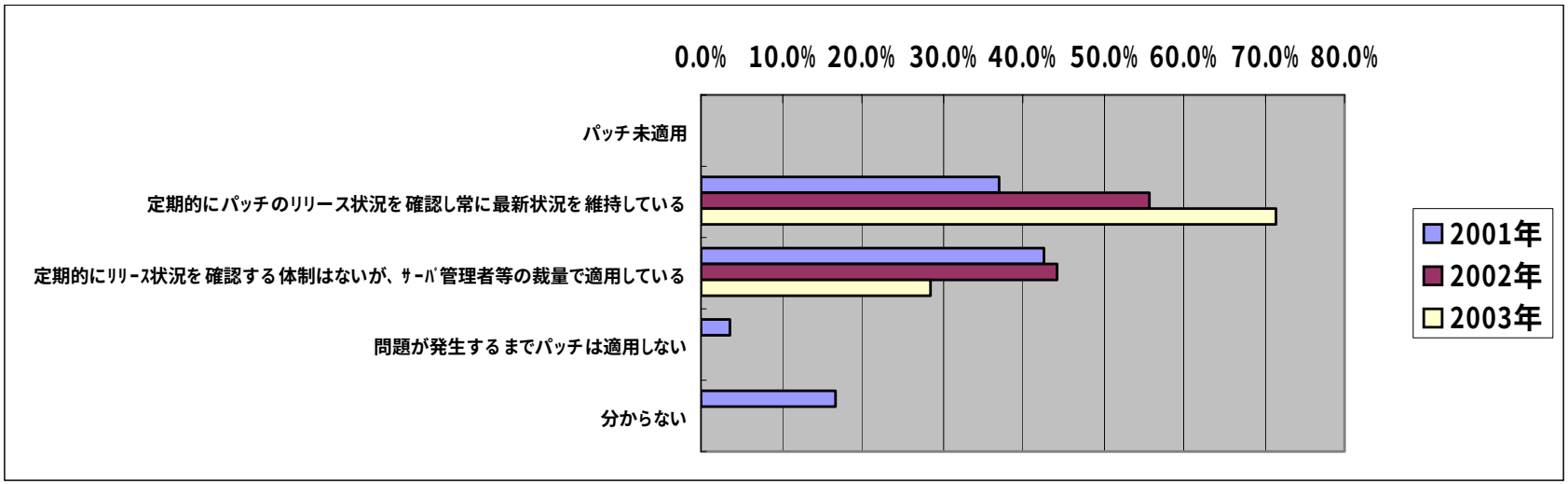
# C-9 派遣社員や常駐作業員受入れ時の配慮点

| | | 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% |



# C-12 パッチの適用

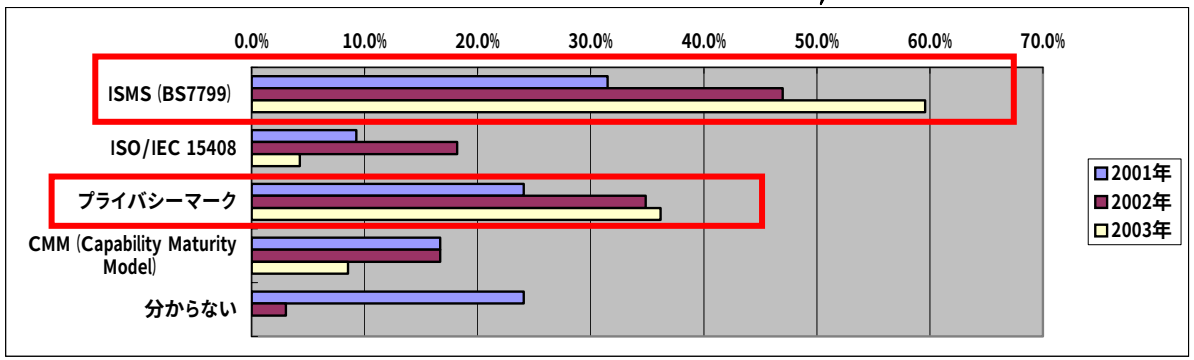
| | | 2001 | | 2002 | | 2003 年 | |
|---|---|---|---|---|---|---|---|
| 1 | パッチ未適用 | 0 | 0.0% | 0 | 0.0% | 0 | 0.0% |
| 2 | 定期的にパッチのリリース状況を確認し常に最新状況を維持している | 20 | 37.0% | 34 | 55.7% | 30 | 71.4% |
| 3 | 定期的にﾘﾘｰｽ状況を確認する体制はないが、ｻｰﾊﾞ管理者等の裁量で適用している | 23 | 42.6% | 27 | 44.3% | 12 | 28.6% |
| 4 | 問題が発生するまでパッチは適用しない | 2 | 3.7% | 0 | 0.0% | 0 | 0.0% |
| 5 | 分からない | 9 | 16.7% | 0 | 0.0% | 0 | 0.0% |



# C-13　認証等の取得計画や取得状況

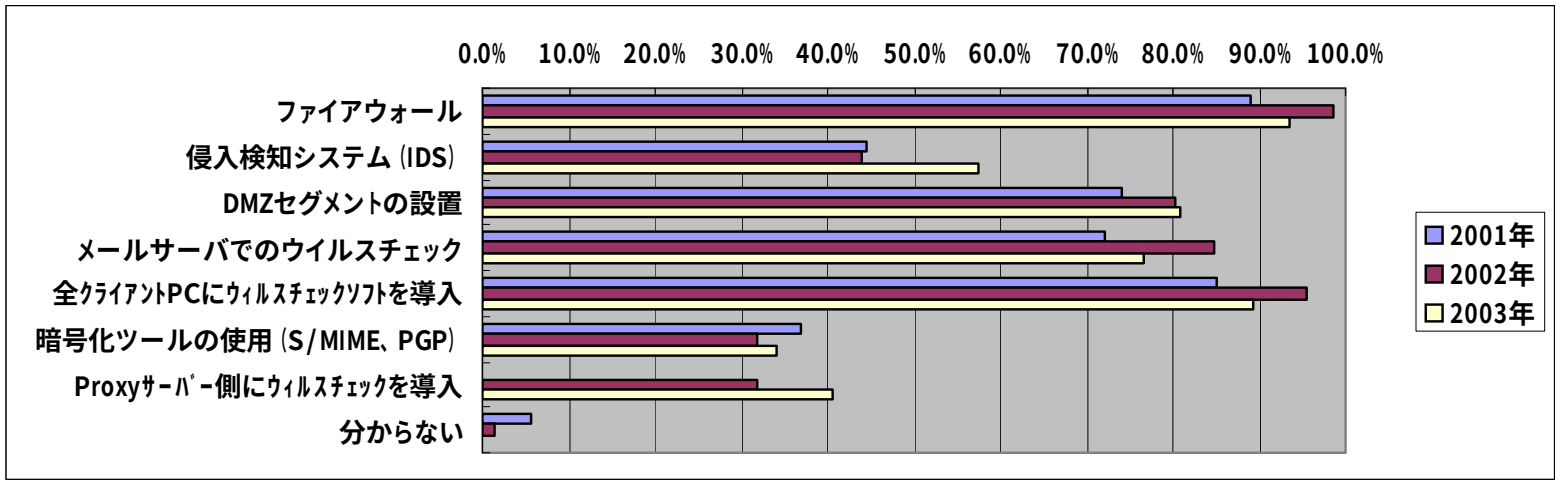
| 2001 | 名称 | 計画中 | 割合 | 取得済み | 割合 |
|---|---|---|---|---|---|
| 1 | ISMS (BS7799) | 14 | 25.90% | 3 | 5.60% |
| 2 | ISO/IEC 15408 | 5 | 9.30% | 0 | 0.00% |
| 3 | プライバシーマーク | 4 | 7.40% | 9 | 16.70% |
| 4 | CMM (Capability Maturity Model) | 8 | 14.80% | 1 | 1.90% |
| 5 | 分からない | 13 | 24.10% | 0 | 0.00% |
| 2002 | 名称 | 計画中 | 割合 | 取得済み | 割合 |
| 1 | ISMS (BS7799) | 21 | 31.80% | 10 | 15.20% |
| 2 | ISO/IEC 15408 | 7 | 10.60% | 5 | 7.60% |
| 3 | プライバシーマーク | 11 | 16.70% | 12 | 18.20% |
| 4 | CMM (Capability Maturity Model) | 9 | 13.60% | 2 | 3.00% |
| 5 | 分からない | 1 | 1.50% | 1 | 1.50% |
| 2003 | 名称 | 計画中 | 割合 | 取得済み | 割合 |
| 1 | ISMS (BS7799) | 12 | 25.50% | 16 | 34.00% |
| 2 | ISO/IEC 15408 | 1 | 2.10% | 1 | 2.10% |
| 3 | プライバシーマーク | 9 | 19.10% | 8 | 17.00% |
| 4 | CMM (Capability Maturity Model) | 1 | 2.10% | 3 | 6.40% |
| 5 | 分からない | 0 | 0.00% | 0 | 0.00% |

ISMS、Pマークへ関心大幅増



# C-18 情報セキュリティ確保のための導入システム

| | | 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 にｳｨ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 ｻｰﾊﾞｰ側にｳｨ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% |



# C-22 現在実施もしくは今後実施の対策

| | | 2002 | | | | 2003 | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 実施済 | 割合 | 今後 | 割合 | 実施済 | 割合 | 今後 | 割合 |
| 1 | セキュリティ関連文書の整理 | 27 | 40.90% | 25 | 37.90% | 27 | 57.40% | 8 | 17.00% |
| 2 | 情報セキュリティを考慮した社内制度の制定 | 26 | 39.40% | 25 | 37.90% | 24 | 51.10% | 13 | 27.70% |
| 3 | 情報システム部員のセキュリティ教育強化 | 21 | 31.80% | 30 | 45.50% | 20 | 42.60% | 13 | 27.70% |
| 4 | 一般従業員のセキュリティ教育強化 | 21 | 31.80% | 38 | 57.60% | 18 | 38.30% | 19 | 40.40% |
| 5 | セキュリティ関連の認証取得 | 12 | 18.20% | 25 | 37.90% | 16 | 34.00% | 14 | 29.80% |
| 6 | セキュリティ関連認証取得システムの導入 | 5 | 7.60% | 18 | 27.30% | 10 | 21.30% | 7 | 14.90% |
| 7 | セキュリティ情報の収集 | 44 | 66.70% | 10 | 15.20% | 35 | 74.50% | 7 | 14.90% |
| 8 | システム監査の実施 | 20 | 30.30% | 21 | 31.80% | 16 | 34.00% | 10 | 21.30% |
| 9 | 全従業員へのセキュリティ情報の提供 | 38 | 57.60% | 14 | 21.20% | 26 | 55.30% | 8 | 17.00% |
| 10 | 事故･事件対応訓練 | 9 | 13.60% | 29 | 43.90% | 13 | 27.70% | 13 | 27.70% |
| 11 | サーバでのウイルスチェック | 56 | 84.80% | 4 | 6.10% | 38 | 80.90% | 2 | 4.30% |
| 12 | クライアントでのウイルスチェック | 60 | 90.90% | 2 | 3.00% | 42 | 89.40% | 2 | 4.30% |
| 13 | 情報ｾｷｭﾘﾃｨのｽｷﾙを有する人材の採用 | 20 | 30.30% | 13 | 19.70% | 17 | 36.20% | 8 | 17.00% |
| 14 | ASP(Application Service Provider)や IDC(Internet Data Center)の利用 | 14 | 21.20% | 15 | 22.70% | 11 | 23.40% | 6 | 12.80% |
| 15 | 人材派遣の利用 | 6 | 9.10% | 9 | 13.60% | 8 | 17.00% | 4 | 8.50% |

# 5．被害状況の概要

## ①被害の状況(被害額上位20件)

| 順位 | 業種 | 直接被害 | 間接被害 | 潜在化被害 | 被害合計 | 被害 |
|---|---|---|---|---|---|---|
| 1 | 製造 | 37,500,000 | 0 | 225,000,000 | 262,500,000 | MSBLASTER |
| 2 | 情報･通信 | 201,875,000 | 0 | 0 | 201,875,000 | KLEZ |
| 3 | 医療･製薬 | 0 | 0 | 81,000,000 | 81,000,000 | MSBLASTER |
| 4 | 情報･通信 | 72,000,000 | 0 | 0 | 72,000,000 | MSBLASTER |
| 5 | 製造 | 45,500,000 | 0 | 0 | 45,500,000 | MSBLASTER |
| 6 | エネルギー | 37,500,000 | 0 | 0 | 37,500,000 | MSBLASTER |
| 7 | 製造 | 1,350,000 | 0 | 36,000,000 | 37,350,000 | MSBLASTER |
| 8 | 製造 | 24,010,000 | 0 | 12,148,000 | 36,158,000 | MSBLASTER |
| 9 | 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 |
| 10 | 建設 | 2,350,000 | 0 | 30,000,000 | 32,350,000 | MSBLASTER |
| 11 | 医療･製薬 | 0 | 0 | 30,000,000 | 30,000,000 | MSBLASTER |
| 12 | 製造 | 15,500,000 | 0 | 14,000,000 | 29,500,000 | MSBLASTER |
| 13 | 情報･通信 | 28,800,000 | 0 | 0 | 28,800,000 | MSBLASTER |
| 14 | 運輸 | 3,899,363 | 0 | 18,900,000 | 22,799,363 | その他のウイルス被害 |
| 15 | 医療･製薬 | 0 | 0 | 20,000,000 | 20,000,000 | MSBLASTER |
| 16 | 製造 | 0 | 0 | 18,750,000 | 18,750,000 | MSBLASTER |
| 17 | 製造 | 10,000,000 | 0 | 7,500,000 | 17,500,000 | MSBLASTER |
| 18 | 金融(銀行、保険、証券等) | 13,500,000 | 0 | 3,780,000 | 17,280,000 | MSBLASTER |
| 19 | 製造 | 8,000,000 | 0 | 7,500,000 | 15,500,000 | MSBLASTER |
| 20 | 医療･製薬 | 13,200,000 | 0 | 0 | 13,200,000 | MSBLASTER |

**合計：約11億8千万円(件数113件、平均1,050万円)**

- 回答をベースにして、算出モデルに従い被害額を算出。

# 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 | 0 | 0.6% |

＜昨年＞
被害項目上位：クレズ、フレゼム
件数：１１件

# 6．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

## 6.1被害発生を抑止しているインシデント対策の状況

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

- 残念ながら、被害の発生と対策内容との相関を見出せず。(逆に対策率高い。被害後に対策実施か?)

| 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 にｳｨ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 ｻｰﾊﾞｰ側にｳｨﾙｽﾁｪｯｸ | 51 | 47.2% | 41 | 38.7% |
| 分からない | 0 | 0.0% | 0 | 0.0% |

## 6.2事故抑止モデルの情報セキュリティ予算の実際

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

・各グループの従業員数とセキュリティ予算の1あたり予算

「被害にあわなかったグループ一人あたり予算」　→5,647円

「被害にあったグループ一人あたり予算」　→13,910円

（突出した2企業を除くと、被害ありグループ　→7,100円）

＜昨年＞

・各グループの従業員数とセキュリティ予算を合計して

「被害にあわなかったグループ一人あたり予算」　→15,991円

「被害にあったグループ一人あたり予算」　→5,327円（3倍の差）

# 6.3望まれる対策レベルと予算規模

## ①望まれる対策レベル

| 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 | |

**教育啓蒙、監視が重要**

**「運用上の対策の実効性向上（セキュリティ教育・啓発活動の実施）レベル」までを推奨。**

# 7．調査総括

JNSA

- 被害件数、被害額は昨年に比べ大幅に増加。
  →ブラスターによる被害多い。
- 各社のセキュリティ対策は、さらに前進。

- 情報漏えいについては、人的要素でさらに取り組み強化。
- 被害のあった企業も各種対策は実施。(事故の覚知が敏感？)
- セキュリティ対策の「コスト」と「効果」を「定量的に把握」することが現時点では難しい。

# 8.情報セキュリティインシデント被害額算出モデル（変更なし）

## ・昨年検討したモデルを今年も継続利用。（被害額算出時に利用）

### ・ｅｘ）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

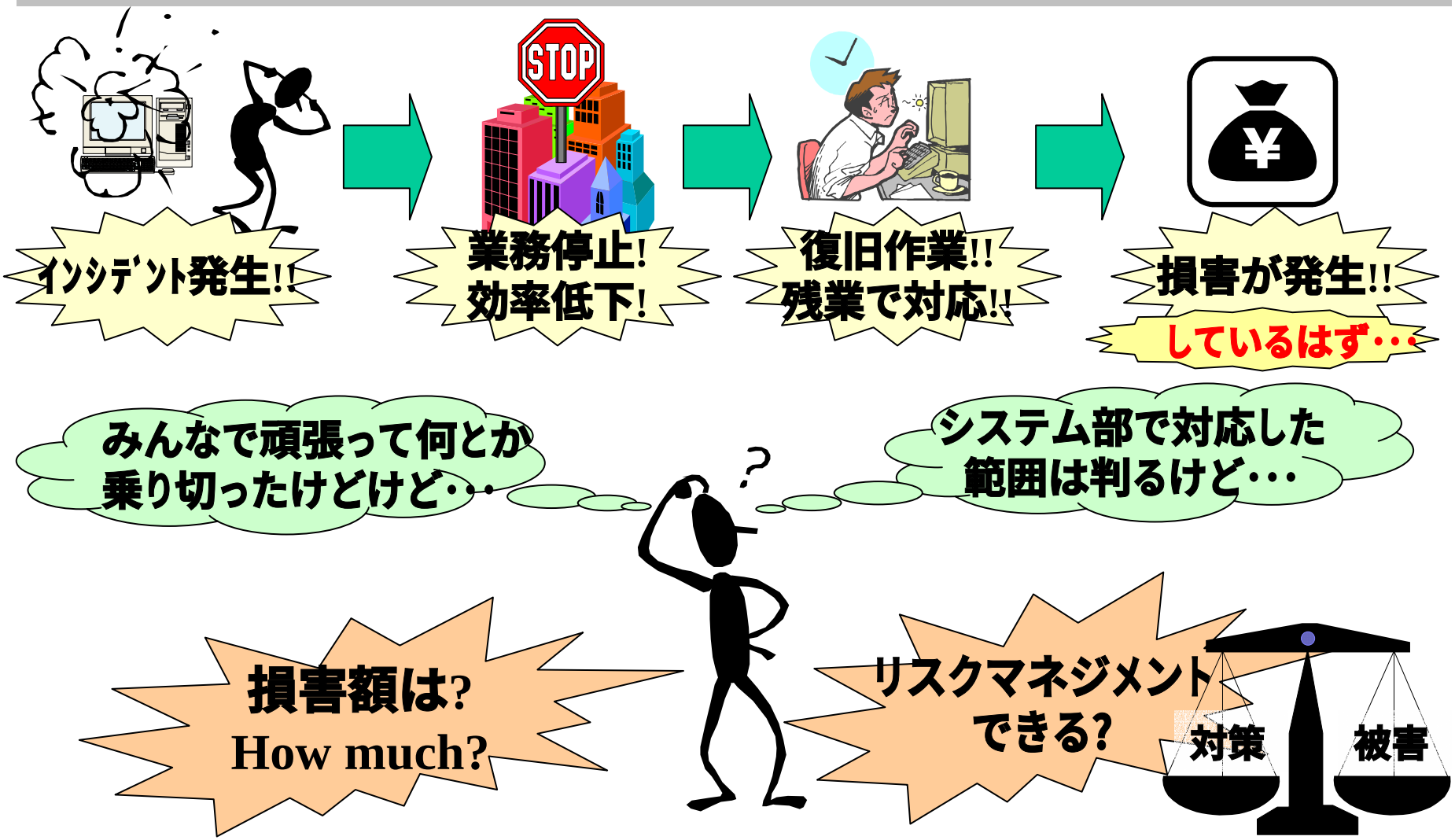
B.復旧完了まで27時間÷8時間×20人×一人当たりの人件費15,000円＝1,012,500円

●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

# 算出モデルの必要性(参考)



# 8.1表面化被害

逸失利益、被害の結果による支出など、被害が金額として認識できるもの。1次的なものと、2次的なものを考える。

## 8.1.1 直接被害額(昨年は1次的な被害額)

直接的な被害額＝

逸失利益＋復旧に要したコスト

＋営業継続＋喪失情報資産＋機会損失

（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）

## 8.1.2 間接被害額

間接的な被害額＝

補償、補填、損害賠償利益など、間接的に生じた被害

# 8.2 潜在化被害

対外的な業務やサービスレベルの低下など、影響はあるが、被害が潜在化し、金額として表出しにくいもの。

## 8.2.1 潜在化被害額

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

(ブランド価値の低下)

業務にかかわる潜在化被害

＝ 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

# 8.3 インシデント被害額算出モデル

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(風評被害など)

# ＜各項目補足＞

JNSA

・固定費（人件費）

影響を受けた従業員の時間あたり人件費単価を設定

・インシデントによる影響を受けた人数

クライアントPCであれば、その台数を設定
サーバであれば、サービス利用者数を設定

・停止時間

システムないしネットワークが停止していた時間
業務効率が通常レベルに戻るまでにかかった時間

# ＜各項目補足＞

JNSA

## ・IT感応度（業務依存度）

- 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
- システムやネットワークへの業務依存度が高い
  →感応度も高い
- 業務に全く影響無し→ゼロ

## ＜IT感応度の算出例＞

システムないしネットワークでの処理　→１００件／時
手作業や代替え手段での処理　→　８０件／時
２０％ダウン → IT感応度（業務依存度）＝０．２

***実施の調査・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」を推奨。***

# 被害調査シート(参考)

**モデルの項目を反映**

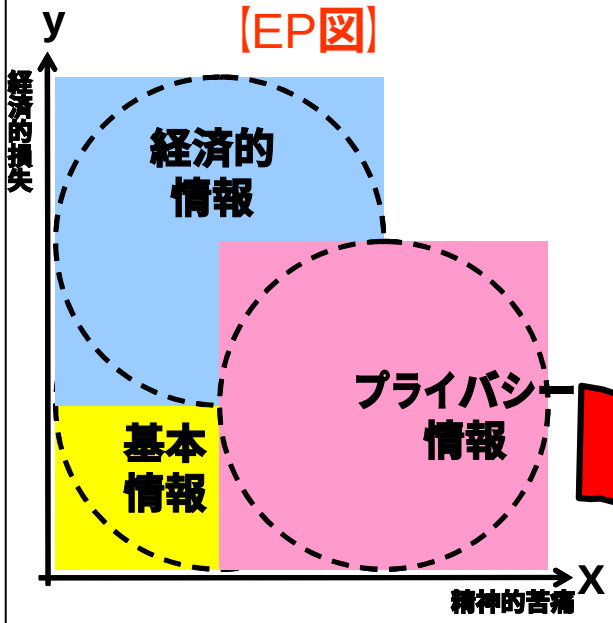
**自社における被害調査への活用**

| | | |
|---|---|---|
| **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。 | | |

# ９．第２部「情報漏洩による被害想定と考察(賠償額および株価影響額)」

## 賠償額算出モデル
## →２００３年「プライバシー面」「経済面」の２要素で損害賠償額を算定するモデルに進化。

【EP図】




【判定基準表】

| 判定基準 | | 社会的責任度 |
|---|---|---|
| 一般より高い | 適正な取扱いを確保すべき個別分野の業種（医療、金融・信用、情報通信等）および、知名度の高い大企業、公的機関。 | 2 |
| 一般的 | 上記以外の企業、組織。 | 1 |

| 判定基準 | 事後対応評価 |
|---|---|
| 適切な対応 | |
| 不適切な対応 | |
| 不明、その他 | |

| 判定基準 | 本人特定容易度 |
|---|---|
| 個人を簡単に特定可能。「氏名」「住所」が含まれること。 | 6 |
| コストを掛ければ個人が特定できる。「氏名」または「住所+電話番号」が含まれること。 | 3 |
| 特定困難。上記以外。 | 1 |

損害賠償額＝（基礎情報価値 × 機微情報度 × 本人特定容易度）
×情報漏洩元組織の社会的責任度
×事後対応評価

# 9.1国内の情報漏洩の分析

| No. | 業種名 | 漏洩原因区分 | 漏洩経路 | 被害人数 | 氏名 | 住所 | 生年月日 | 性別 | 電話番号 | 職業 | Emailアドレス | その他 | No. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 金融・保険業 | 情報持ち出し | 不明 | 1,000人 | ○ | | | | | | | 社内格付け等 | 1 |
| 2 | 教育、学習支援業 | 設定ミス | FD等可搬記録媒体 | 不明 | | | | | | | | 受験結果等 | 2 |
| 3 | 情報通信業 | 誤操作 | Email経由 | 202人 | ○ | | | | | | ○ | | 3 |
| 4 | その他 | 設定ミス | Web経由 | 不明 | ○ | | | | | | | 連絡先 | 4 |
| 5 | 運輸業 | 誤操作 | Email経由 | 190人 | | | | | | | ○ | | 5 |
| 6 | 教育、学習支援業 | 管理ミス | FD等可搬記録媒体 | 220人 | ○ | ○ | | | ○ | | | 成績表 | 6 |
| 7 | サービス業(他に分類されないもの) | 設定ミス | Web経由 | 443人 | | | | | | | ○ | | 7 |
| 8 | 教育、学習支援業 | 不明 | FD等可搬記録媒体 | 7,381人 | ○ | | | | | | | 成績、高校名 | 8 |
| 9 | 情報通信業 | 情報持ち出し | 紙媒体経由 | 1,500人 | ○ | ○ | | | | | | 年齢 | 9 |
| 10 | サービス業(他に分類されないもの) | 設定ミス | Web経由 | 450,000人 | ○ | ○ | ○ | | | | | 学校名、趣味等 | 10 |
| 11 | 公務(他に分類されないもの) | 不明 | 不明 | 92人 | | | | | | | ○ | | 11 |
| 12 | 公務(他に分類されないもの) | 管理ミス | 紙媒体経由 | 574人 | ○ | ○ | | | | | | 会社名、給与所得等 | 12 |
| 13 | 情報通信業 | 設定ミス | Email経由 | 不明 | ○ | | | | ○ | | ○ | メールの内容 | 13 |
| 14 | 金融・保険業 | 情報持ち出し | FD等可搬記録媒体 | 15,000人 | ○ | ○ | ○ | | ○ | | | カード番号、口座番号、年収等 | 14 |
| 15 | その他サービス | バグ・セキュリティホール | 不明 | 2人 | | | | | | | | | 15 |
| 16 | 医療、福祉 | 内部犯罪 | 不明 | 1,300人 | ○ | ○ | ○ | ○ | | | | 血液型、感染症検査結果等 | 16 |
| 17 | 教育、学習支援業 | 置き忘れ | 紙媒体経由 | 950人 | ○ | | ○ | ○ | | | | 学科名、受験番号 | 17 |
| 18 | 金融・保険業 | 誤操作 | Email経由 | 2,800人 | | | | | | | ○ | | 18 |
| 19 | 金融・保険業 | 誤操作 | Email経由 | 98人 | ○ | ○ | | | ○ | | | 障害の程度 | 19 |
| 20 | 公務(他に分類されないもの) | その他 | PC本体 | 100人 | ○ | | | | | | | 補償金額、交渉経緯 | 20 |
| 21 | 金融・保険業 | 内部犯罪 | 不明 | 800人 | ○ | ○ | ○ | ○ | ○ | ○ | | 信用情報 | 21 |
| 22 | サービス業(他に分類されないもの) | バグ・セキュリティホール | Email経由 | 170人 | | | | | | | ○ | | 22 |
| 23 | 教育、学習支援業 | 不正アクセス | Web経由 | 23,000人 | | | | | | | | | 23 |
| 24 | サービス業(他に分類されないもの) | バグ・セキュリティホール | Web経由 | 210人 | ○ | ○ | | | ○ | | ○ | | 24 |
| 25 | 卸売・小売業 | その他 | 不明 | 560,000人 | ○ | ○ | ○ | | ○ | | | | 25 |
| 26 | 公務(他に分類されないもの) | 盗難 | PC本体 | 1,300人 | ○ | ○ | ○ | | | | | 児童扶養手当、生活保護、結婚相談等 | 26 |
| 27 | 公務(他に分類されないもの) | 設定ミス | Web経由 | 761人 | ○ | ○ | ○ | ○ | ○ | ○ | | クレジットカード番号 | 27 |
| 28 | 金融・保険業 | 内部犯罪 | 不明 | 325人 | ○ | ○ | ○ | | | | | 取引内容 | 28 |
| 29 | 製造業 | 誤操作 | Email経由 | 573人 | | | | | | | ○ | | 29 |
| 30 | 製造業 | 管理ミス | FD等可搬記録媒体 | 不明 | ○ | ○ | | ○ | | | | 除籍・改製原戸籍 | 30 |
| 31 | 金融・保険業 | 不明 | 不明 | 74人 | ○ | ○ | ○ | | | | | 保険掛金額 | 31 |
| 32 | 公務(他に分類されないもの) | 誤操作 | Web経由 | 128人 | ○ | ○ | | | ○ | | | | 32 |
| 33 | 情報通信業 | 誤操作 | Email経由 | 480人 | | | | | | | ○ | | 33 |
| 34 | 金融・保険業 | 管理ミス | その他 | 126人 | ○ | ○ | | | ○ | | | カード番号 | 34 |
| 35 | 金融・保険業 | その他 | FD等可搬記録媒体 | 1,453人 | ○ | ○ | ○ | ○ | ○ | ○ | | カード番号、有効期限、口座情報等 | 35 |
| 36 | 卸売・小売業 | 情報持ち出し | 不明 | 182,780人 | ○ | ○ | ○ | ○ | ○ | | ○ | | 36 |
| 37 | 情報通信業 | 誤操作 | Web経由 | 不明 | ○ | ○ | | | | | | ユーザID、旧パスワード | 37 |
| 38 | 医療、福祉 | 管理ミス | Web経由 | 240人 | ○ | | ○ | | | | | 病名、がん告知等 | 38 |
| 39 | 情報通信業 | 誤操作 | Email経由 | 173人 | | | | | | | ○ | | 39 |
| 40 | 卸売・小売業 | 設定ミス | Web経由 | 6,000人 | ○ | ○ | | | ○ | | | 購入したビデオタイトル | 40 |
| 41 | 金融・保険業 | 不正アクセス | FTP経由 | 79,110人 | ○ | ○ | ○ | ○ | ○ | ○ | | 住居形態、年収区分 | 41 |
| 42 | 金融・保険業 | 情報持ち出し | 紙媒体経由 | 75人 | ○ | ○ | ○ | ○ | ○ | ○ | | 信用情報 | 42 |
| 43 | 情報・通信 | 誤操作 | その他 | 1,370人 | ○ | | | | ○ | | ○ | 会社名、役職 | 43 |
| 44 | 情報通信業 | 盗難 | PC本体 | 3,974人 | ○ | | | | ○ | | ○ | | 44 |
| 45 | 情報通信業 | その他 | FD等可搬記録媒体 | 58,515人 | ○ | ○ | | | | | | 氏名、生年月日、続柄等 | 45 |
| 46 | 公務(他に分類されないもの) | 管理ミス | 紙媒体経由 | 872人 | ○ | ○ | ○ | | | | | 選挙人名、投票情報 | 46 |
| 47 | 卸売・小売業 | 設定ミス | Web経由 | 1,912人 | ○ | ○ | | | ○ | | | | 47 |
| 48 | 運輸業 | その他 | 紙媒体経由 | 10人 | ○ | ○ | ○ | ○ | ○ | ○ | | 家族構成、年収等 | 48 |
| 49 | 教育、学習支援業 | 盗難 | PC本体 | 197人 | ○ | ○ | | | ○ | | | 保護者名、高校入試得点等 | 49 |
| 50 | サービス業(他に分類されないもの) | バグ・セキュリティホール | Web経由 | 1,200人 | ○ | ○ | | ○ | ○ | | ○ | 相談内容 | 50 |
| 51 | サービス業(他に分類されないもの) | 内部犯罪 | PC本体 | 不明 | ○ | ○ | ○ | ○ | ○ | | | 口座番号、請求履歴等 | 51 |
| 52 | 金融・保険業 | 管理ミス | 紙媒体経由 | 280人 | ○ | ○ | | | ○ | | | 請求年月、未納金、未納金残高等 | 52 |
| 53 | 情報通信業 | その他 | PC本体 | 4,312人 | ○ | ○ | | | ○ | | | 土地面積、建物面積、査定方法等 | 53 |
| 54 | 運輸業 | 内部犯罪 | 不明 | 131,742人 | ○ | ○ | | | | | | | 54 |
| 55 | 卸売・小売業 | 設定ミス | Email経由 | 9人 | | ○ | | | ○ | | ○ | | 55 |
| 56 | 情報通信業 | 誤操作 | 紙媒体経由 | 985人 | ○ | | | | | | | 利用金額、請求額等 | 56 |
| 57 | 公務(他に分類されないもの) | 盗難 | FD等可搬記録媒体 | 9,584人 | ○ | ○ | ○ | ○ | | | | 戸籍、選挙権、住民票コード等 | 57 |
| | 合計 | | | 1,554,592人 | 45 | 35 | 19 | 13 | 25 | 6 | 16 | | |
| | 1件あたりの平均(不明を除く) | | | 30,482.2人 | 79% | 61% | 33% | 23% | 44% | 11% | 28% | | |

**＜漏洩事故の概要＞**

**個人情報漏洩　　：54件 (95%)**

**メールアドレス漏洩：16件 (28%)**

**非公開資料漏洩　：5件 (5%)**

**インターネット公表　：57件**

**被害者の合計人数　：1,554,592人**

**1件当たり人数　　：30,482人**

**＜昨年＞**

**インターネット公表　：63件**

**被害者の合計人数　：418,716人**

**1件当たり人数　　：6,646人**

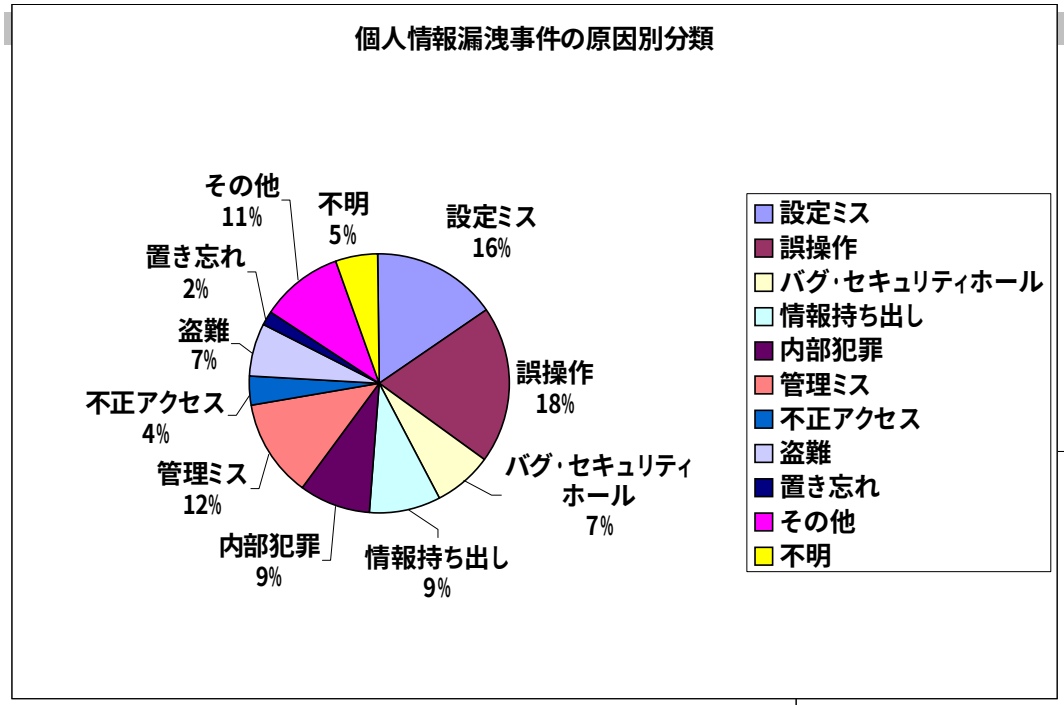
# 9.2漏洩情報の分析(項目)

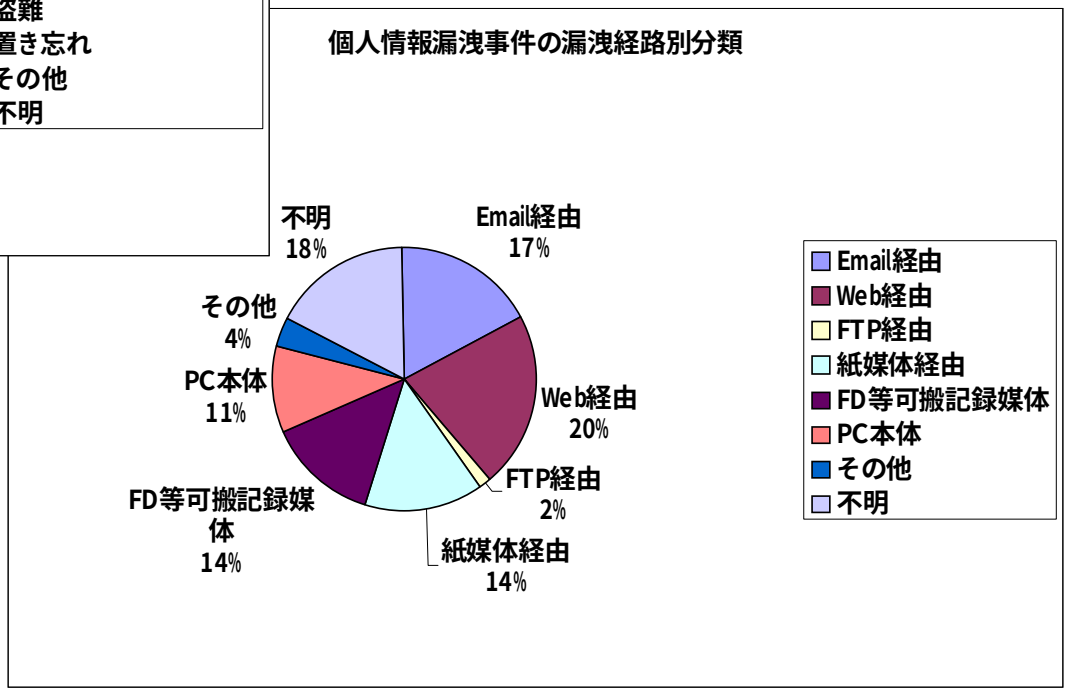
| 漏洩情報分類 | 件数 | 漏洩率 |
|---|---|---|
| 氏名 | 45 | 79% |
| 住所 | 35 | 61% |
| 生年月日 | 19 | 33% |
| 性別 | 13 | 23% |
| 電話番号 | 25 | 44% |
| 職業 | 6 | 11% |
| Email アドレス | 16 | 28% |

**「氏名」→79%**
**上位**
**→「氏名」、「住所」、「メールアドレス」、「電話番号」、「生年月日」**

**<u>その他</u>**
**ユーザID、クレジットカード番号、信用情報、カードの利用状況、年収、銀行名、口座番号、年齢、会社名、学校名、成績、趣味、職業、血液型、病名、感染症検査の結果、障害の程度、保険掛金額、戸籍　など。**

# 9.3情報漏洩元の分析



# 9.4情報漏洩経路の分析

## 昨年度

・漏洩情報は、個人情報が大半(90%)であった。
・漏洩元は、企業が大半(82%)であった。
・原因は、技術的な人為的ミスと対策不足が大半(88%)であった。
・経路は、インターネット経由が大半(98%)であった。

## 本年度

・昨年と同様に漏洩情報は、個人情報が大半(95%)であった。
・昨年と同様に漏洩元は、企業が大半(86%)であった。
・昨年と異なり原因は、技術的な人為的ミスと対策不足が過半数(57%)にとどまり、新たに、非技術的な要素が27%であった。
・昨年と異なり経路は、２分されインターネット経由と媒体経由が、それぞれ39%であった。

# 9.5国内の情報漏洩事故による損害賠償被害額想定

## 各事例への算出モデルの適用と一覧表

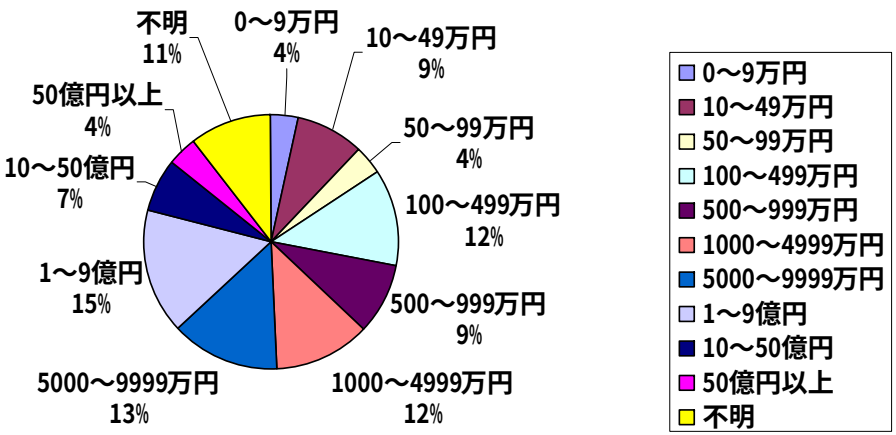
＜昨年：昨年モデル版＞
損害賠償：151億4,270万円 (合計人数 418,716人)
平均賠償額： 2億4,036万円 (平均人数 6,646人)

**損害賠償総額(想定) ：280億6,936万円** (合計人数 155万4,592人)

**平均損害賠償額(想定)： 5億5,038万円** (平均人数 30,482人)

**各事例にモデル適用**

一件当たりの損害賠償額




| No. | 業種名 | 被害人数 | 精神的苦痛レベル(x) | 経済的損失レベル(y) | 機微情報度 | 社会的責任度 | 事後対応評価 | 本人特定容易度 | 一人当たり損害賠償額 | 損害賠償総額(千円) | No. |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 金融・保険業 | 1,000人 | 2 | 1 | 11 | 2 | 2 | 3 | 66千円 | 66,000千円 | 1 |
| 2 | 教育, 学習支援業 | 不明 | 2 | 1 | 11 | 1 | 1 | 1 | 6千円 | 不明 | 2 |
| 3 | 情報通信業 | 202人 | 1 | 1 | 2 | 2 | 1 | 3 | 6千円 | 1,212千円 | 3 |
| 4 | その他 | 不明 | 1 | 1 | 2 | 1 | 1 | 3 | 3千円 | 不明 | 4 |
| 5 | 運輸業 | 190人 | 1 | 1 | 2 | 1 | 1 | 1 | 1千円 | 190千円 | 5 |
| 6 | 教育, 学習支援業 | 220人 | 2 | 1 | 11 | 1 | 1 | 6 | 33千円 | 7,260千円 | 6 |
| 7 | サービス業(他に分類されないもの) | 443人 | 1 | 1 | 2 | 1 | 1 | 1 | 1千円 | 443千円 | 7 |
| 8 | 教育, 学習支援業 | 7,381人 | 2 | 1 | 11 | 1 | 1 | 3 | 17千円 | 121,787千円 | 8 |
| 9 | 情報通信業 | 1,500人 | 1 | 1 | 2 | 2 | 1 | 6 | 12千円 | 18,000千円 | 9 |
| 10 | サービス業(他に分類されないもの) | 450,000人 | 1 | 1 | 2 | 1 | 1 | 6 | 6千円 | 2,700,000千円 | 10 |
| 11 | 公務(他に分類されないもの) | 92人 | 1 | 1 | 2 | 2 | 1 | 1 | 2千円 | 184千円 | 11 |
| 12 | 公務(他に分類されないもの) | 574人 | 1 | 2 | 6 | 2 | 1 | 6 | 36千円 | 20,664千円 | 12 |
| 13 | 情報通信業 | 不明 | 2 | 1 | 11 | 2 | 1 | 3 | 33千円 | 不明 | 13 |
| 14 | 金融・保険業 | 15,000人 | 2 | 3 | 35 | 2 | 1 | 6 | 210千円 | 3,150,000千円 | 14 |
| 15 | その他サービス | 2人 | 1 | 1 | 2 | 2 | 1 | 1 | 2千円 | 4千円 | 15 |
| 16 | 医療, 福祉 | 1,300人 | 3 | 1 | 101 | 2 | 1 | 6 | 606千円 | 787,800千円 | 16 |
| 17 | 教育, 学習支援業 | 950人 | 1 | 1 | 2 | 1 | 1 | 3 | 3千円 | 2,850千円 | 17 |
| 18 | 金融・保険業 | 2,800人 | 1 | 1 | 2 | 2 | 1 | 1 | 2千円 | 5,600千円 | 18 |
| 19 | 金融・保険業 | 98人 | 3 | 1 | 101 | 2 | 1 | 6 | 606千円 | 59,388千円 | 19 |
| 20 | 公務(他に分類されないもの) | 100人 | 2 | 2 | 15 | 2 | 1 | 3 | 45千円 | 4,500千円 | 20 |
| 21 | 金融・保険業 | 800人 | 2 | 2 | 15 | 2 | 1 | 6 | 90千円 | 72,000千円 | 21 |
| 22 | サービス業(他に分類されないもの) | 170人 | 1 | 1 | 2 | 1 | 1 | 1 | 1千円 | 170千円 | 22 |
| 23 | 教育, 学習支援業 | 23,000人 | 1 | 1 | 2 | 1 | 1 | 1 | 1千円 | 23,000千円 | 23 |
| 24 | サービス業(他に分類されないもの) | 210人 | 1 | 1 | 2 | 2 | 1 | 6 | 12千円 | 2,520千円 | 24 |
| 25 | 卸売・小売業 | 560,000人 | 1 | 1 | 2 | 1 | 1 | 6 | 6千円 | 3,360,000千円 | 25 |
| 26 | 公務(他に分類されないもの) | 1,300人 | 3 | 1 | 101 | 2 | 1 | 6 | 606千円 | 787,800千円 | 26 |
| 27 | 公務(他に分類されないもの) | 761人 | 1 | 3 | 26 | 2 | 1 | 6 | 156千円 | 118,716千円 | 27 |
| 28 | 金融・保険業 | 325人 | 1 | 2 | 6 | 2 | 1 | 6 | 36千円 | 11,700千円 | 28 |
| 29 | 製造業 | 573人 | 1 | 1 | 2 | 2 | 1 | 1 | 2千円 | 1,146千円 | 29 |
| 30 | 製造業 | 不明 | 3 | 1 | 101 | 1 | 1 | 6 | 303千円 | 不明 | 30 |
| 31 | 金融・保険業 | 74人 | 1 | 2 | 6 | 2 | 1 | 6 | 36千円 | 2,664千円 | 31 |
| 32 | 公務(他に分類されないもの) | 128人 | 1 | 1 | 2 | 2 | 1 | 6 | 12千円 | 1,536千円 | 32 |
| 33 | 情報通信業 | 480人 | 1 | 1 | 2 | 2 | 1 | 1 | 2千円 | 960千円 | 33 |
| 34 | 金融・保険業 | 126人 | 1 | 3 | 26 | 2 | 1 | 6 | 156千円 | 19,656千円 | 34 |
| 35 | 金融・保険業 | 1,453人 | 1 | 3 | 26 | 2 | 1 | 6 | 156千円 | 226,668千円 | 35 |
| 36 | 卸売・小売業 | 182,780人 | 1 | 1 | 2 | 1 | 1 | 6 | 6千円 | 1,096,680千円 | 36 |
| 37 | 情報通信業 | 不明 | 1 | 1 | 2 | 2 | 1 | 6 | 12千円 | 不明 | 37 |
| 38 | 医療, 福祉 | 240人 | 3 | 1 | 101 | 2 | 1 | 3 | 303千円 | 72,720千円 | 38 |
| 39 | 情報通信業 | 173人 | 1 | 1 | 2 | 2 | 1 | 1 | 2千円 | 346千円 | 39 |
| 40 | 卸売・小売業 | 6,000人 | 2 | 1 | 11 | 1 | 1 | 6 | 33千円 | 198,000千円 | 40 |
| 41 | 金融・保険業 | 79,110人 | 2 | 2 | 15 | 2 | 1 | 6 | 90千円 | 7,119,900千円 | 41 |
| 42 | 金融・保険業 | 75人 | 2 | 2 | 15 | 2 | 1 | 6 | 90千円 | 6,750千円 | 42 |
| 43 | 情報・通信 | 1,370人 | 1 | 1 | 2 | 2 | 1 | 3 | 6千円 | 8,220千円 | 43 |
| 44 | 情報通信業 | 3,974人 | 1 | 2 | 6 | 2 | 1 | 3 | 18千円 | 71,532千円 | 44 |
| 45 | 情報通信業 | 58,515人 | 1 | 1 | 2 | 2 | 1 | 6 | 12千円 | 702,180千円 | 45 |
| 46 | 公務(他に分類されないもの) | 872人 | 2 | 1 | 11 | 2 | 1 | 6 | 66千円 | 57,552千円 | 46 |
| 47 | 卸売・小売業 | 1,912人 | 1 | 1 | 2 | 1 | 1 | 6 | 6千円 | 11,472千円 | 47 |
| 48 | 運輸業 | 10人 | 2 | 2 | 15 | 2 | 1 | 6 | 90千円 | 900千円 | 48 |
| 49 | 教育, 学習支援業 | 197人 | 2 | 1 | 11 | 1 | 1 | 6 | 33千円 | 6,501千円 | 49 |
| 50 | サービス業(他に分類されないもの) | 1,200人 | 2 | 1 | 11 | 2 | 1 | 6 | 66千円 | 79,200千円 | 50 |
| 51 | サービス業(他に分類されないもの) | 不明 | 2 | 2 | 15 | 1 | 1 | 6 | 45千円 | 不明 | 51 |
| 52 | 金融・保険業 | 280人 | 2 | 3 | 35 | 2 | 1 | 6 | 210千円 | 58,800千円 | 52 |
| 53 | 情報通信業 | 4,312人 | 2 | 2 | 15 | 2 | 1 | 6 | 90千円 | 388,080千円 | 53 |
| 54 | 運輸業 | 131,742人 | 1 | 1 | 2 | 1 | 1 | 6 | 6千円 | 790,452千円 | 54 |
| 55 | 卸売・小売業 | 9人 | 1 | 1 | 2 | 1 | 1 | 3 | 3千円 | 27千円 | 55 |
| 56 | 情報通信業 | 985人 | 1 | 2 | 6 | 2 | 1 | 3 | 18千円 | 17,730千円 | 56 |
| 57 | 公務(他に分類されないもの) | 9,584人 | 3 | 1 | 101 | 2 | 1 | 6 | 606千円 | 5,807,904千円 | 57 |
| | 合計 | 1,554,592人 | | | | | | | | 28,069,364千円 | |
| | 1件あたりの平均 (不明を除く) | 30,482.2人 | | | | | | | | 550,380千円 | |

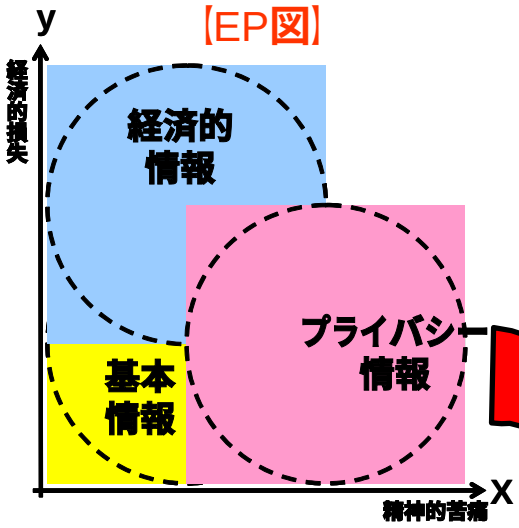
# 9.6情報の種類と賠償額

## 9.6.1 予想計算式の改良

「経済的損失」と「精神的苦痛」の２つのリスクを分析し、個人情報の価値を定量化する。他にも、判定基準表を用いて算出式の各項の数値を求めやすくする改良を実施。

＜算出イメージ＞

【EP図】




【判定基準表】

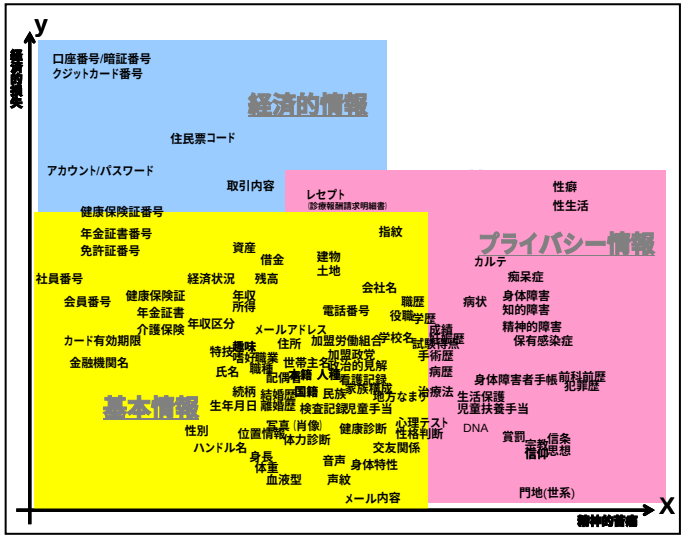
| 判定基準 | | 社会的責任度 |
|---|---|---|
| 一般より高い | 適正な取扱いを確保すべき個別分野の業種（医療、金融・信用、情報通信等）および、知名度の高い大企業、公的機関 | 2 |
| 一般的 | 組織。 | 1 |

| 判定基準 | 事後対応評価 |
|---|---|
| 適切な対応 | |
| 不適切な対応 | |
| 不明、その他 | |

| 判定基準 | 本人特定容易度 |
|---|---|
| 個人を簡単に特定可能。「氏名」「住所」が含まれること。 | 6 |
| コストを掛ければ個人が特定できる。「氏名」または「住所+電話番号」が含まれること。 | 3 |
| 特定困難。上記以外。 | 1 |

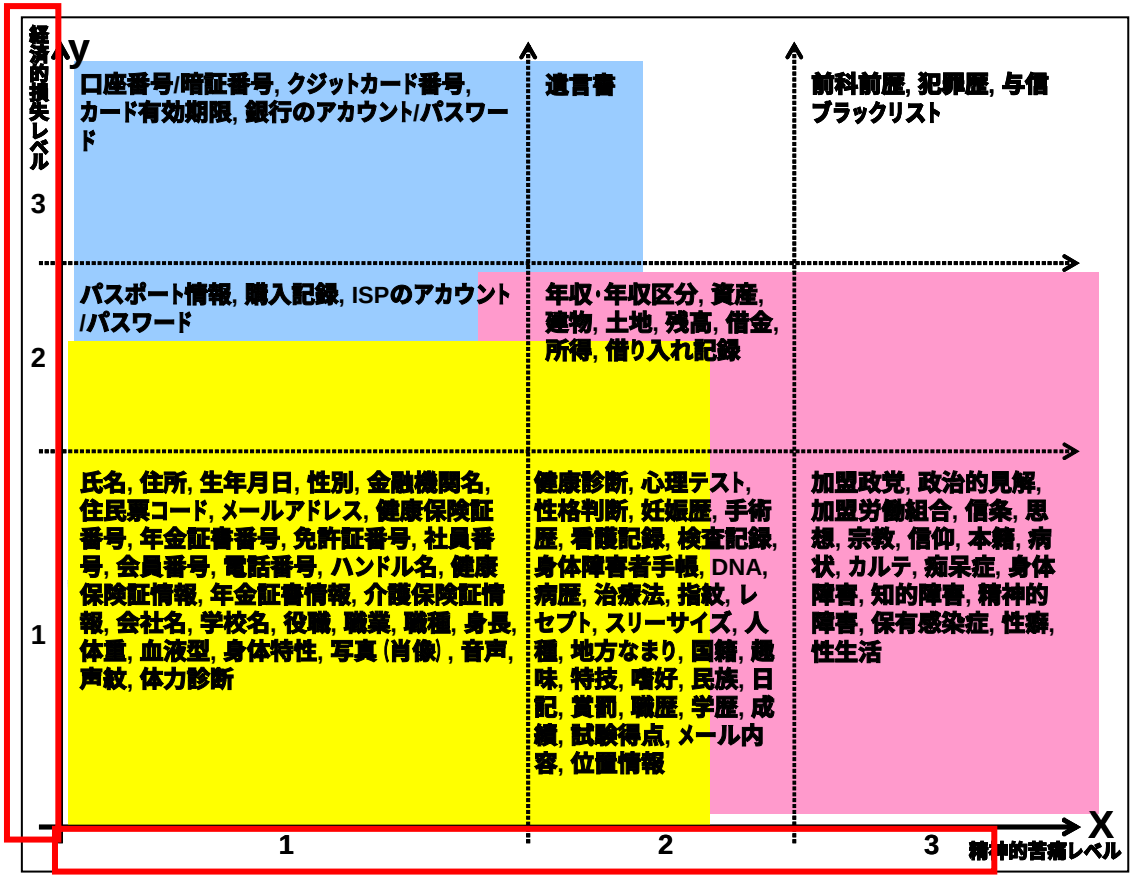
損害賠償額＝（基礎情報価値 × 機微情報度 × 本人特定容易度）
×情報漏洩元組織の社会的責任度
×事後対応評価

# 9.6.2情報の価値基準の検討




個人情報の配置例（EP図）

## Simple-EP図



# 9.6.3 2003年損害賠償額の予想計算式

**損害賠償額 ＝ 漏洩個人情報価値**
**×社会的責任度**
**×事後対応評価**

**＝ (基礎情報価値×機微情報度×本人特定容易度)**
**×情報漏洩元組織の社会的責任度**
**×事後対応評価**

**＝ 基礎情報価値　[500]**
**×機微情報度　[Max $(10^{x-1}+5^{y-1})$ ]**
**×本人特定容易度　[6, 3, 1]**
**×社会的責任度　[2, 1]**
**×事後対応評価　[2, 1]**

**機微情報度＝ $(10^{x-1}+5^{y-1})$**

x = 漏洩した情報の精神的苦痛レベルの最大値
y = 〃　経済的損失レベルの最大値

| 判定基準 | 本人特定容易度 |
|---|---|
| 個人を簡単に特定可能。「氏名」「住所」が含まれること。 | 6 |
| コストを掛ければ個人が特定できる。「氏名」または「住所+電話番号」が含まれること。 | 3 |
| 特定困難。上記以外。 | 1 |

| 判定基準 | | 社会的責任度 |
|---|---|---|
| 一般より高い | 適正な取扱いを確保すべき個別分野の業種（医療、金融・信用、情報通信等）および、知名度の高い大企業、公的機関。 | 2 |
| 一般的 | その他一般的な企業および団体、組織。 | 1 |

| 判定基準 | 事後対応評価 |
|---|---|
| 適切な対応 | 1 |
| 不適切な対応 | 2 |
| 不明、その他 | 1 |

# 10. 個人情報漏洩事件での緊急対応費用の推定

## 企業プロファイル (想定)

| 企業規模 | |
|---|---|
| 売上高 | 約1000億円 |
| 従業員 | 約1000名 |
| **カタログ販売部門** | |
| 会員数 | 約600万人 |
| 売上げ | 約900億円 |
| **インターネットショップ部門** | |
| 会員数 | 約100万人 |
| 売上げ | 約100億円 |
| 従業員 | 約30名 |

## 個人情報漏洩事件による被害額 (試算)

| 項目 | | | 費用 |
|---|---|---|---|
| 直接被害 | 逸失利益 | インターネットショッピングサイト利益額 (1ヶ月分) | 約8,330万円 |
| | 機会損失 | インターネットショッピングサイトの成長率分 (1ヶ月相当) | 約830万円 |
| 間接被害 | 業務継続費用 | 対策組織業務に係る人件費 (1ヶ月分) | 約2,000万円 |
| | | セキュリティコンサルタントの依頼費用 (1ヶ月分) | 約500万円 |
| | 損害賠償費用 | 損害賠償費用 | 約108万円 |
| | | 弁護士費用、裁判費用 | 約9万円 |
| | 見舞品費用 | 見舞品代＋送料他 (30万人分) | 約2億1,000万円 |
| | 謝罪訪問費 | 謝罪訪問に掛かる費用 (15人分) | 約165万円 |
| | 広報費用 | 謝罪広告費 (新聞5紙) | 約1,000万円 |
| | | 情報公開ページ作成費用 (5回) | 約25万円 |
| | 臨時的な対策費用 | コールセンター設置費用 (1ヶ月分) | 約1,000万円 |
| | | 問い合わせ窓口常駐人員 (1ヶ月分) | 約300万円 |
| 潜在化被害 | 影響業務 | 影響を受けた業務の人件費 (1ヶ月分) | 約3,000万円 |
| | 業務外の潜在化被害 | ブランド価値の低下 | ＋α |
| | | 合計 | 約3億8,237万円 |

# 11.情報漏洩による企業価値への影響 (株価面での考察)

＜目的＞

- 株価の動きには、様々な要因があり、単純に情報漏洩事故との連動を語ることは難しい。

- しかし、情報漏洩により企業の信頼失墜が生じることは間違いない。

- 現時点ではサンプル数が少ないが、一定の方法によって繰り返し調査し対象件数を重ねることで、将来的には事故と株価との相関についても傾向把握することを狙う。

**→２００２年に続き、継続実施**

# 11.1情報漏洩事故発生後の株価変動の把握方法について

JNSA

## ＜短期＞

基準レシオ　＝　事故発生の前日の（当該企業株価／日経平均）
n日レシオ　＝　事故発生のn日の（当該企業株価／日経平均）
n日値＝（基準レシオ－n日レシオ）×n日の日経平均値×発行株数
事故発生１０日間を評価

**短期株式影響額＝１～１０日値の合計／１０日**

## ＜中期＞

基準レシオ　＝　事故発生の前月末の（当該企業株価／日経平均）
nヶ月末レシオ　＝　事故発生のnヶ月末の（当該企業株価／日経平均）
nヶ月値＝（基準レシオ－nヶ月末レシオ）×nヶ月末の日経平均値×発行株数
事故発生４ヶ月間を評価

**中期株式影響額＝１～４ヶ月値の合計／４ヶ月**

# 11.2株価への影響

**今年は、情報漏洩発生と株価との影響に相関があまり見出せなかった。**

| 事故ケース | | #01 | #02 | #03 | #04 | #05 | #06 |
|---|---|---|---|---|---|---|---|
| 発行済み株式数 | | 107,600,000 | 97,683,133 | 858,672,607 | 63,859,251 | 2,955,000 | 147,295,200 |
| 第n日目の期待株価から起算して乖離値（公表日前日を基準とする） | 1 | ▲ 38.25 | ▲ 16.56 | ▲ 11.41 | ▲ 10.87 | ▲ 22.69 | ▲ 121.53 |
| | 2 | ▲ 126.84 | | ▲ 7.22 | | | 332.03 |
| | 3 | | | ▲ 2.14 | | | 666.15 |
| | 4 | | | | ▲ 7.74 | | 333.70 |
| | 5 | ▲ 148.88 | 52.71 | | ▲ 6.64 | ▲ 122.78 | |
| | 6 | ▲ 203.07 | ▲ 19.91 | 3.92 | ▲ 4.83 | ▲ 209.88 | |
| | 7 | ▲ 342.20 | ▲ 34.90 | 1.01 | ▲ 0.71 | ▲ 130.66 | 332.53 |
| | 8 | ▲ 234.56 | ▲ 57.38 | 9.87 | ▲ 2.12 | ▲ 121.96 | 269.58 |
| | 9 | ▲ 195.30 | | 7.82 | | | 161.77 |
| | 10 | | | 0.35 | | | 310.74 |
| | 11 | | ▲ 24.02 | | ▲ 0.10 | ▲ 37.40 | 3.88 |
| | 12 | ▲ 279.25 | ▲ 6.22 | | ▲ 2.75 | ▲ 114.77 | |
| | 13 | ▲ 278.57 | 4.41 | ▲ 6.45 | ▲ 3.13 | ▲ 120.10 | |
| | 14 | ▲ 213.59 | 9.01 | ▲ 1.40 | ▲ 5.95 | ▲ 71.05 | |
| | 合計 | ▲ 2,060.52 | ▲ 92.84 | ▲ 5.65 | ▲ 44.84 | ▲ 951.28 | 2,288.85 |
| | 1日平均 | ▲ 206.05 | ▲ 10.32 | ▲ 0.57 | ▲ 4.48 | ▲ 105.70 | 254.32 |
| 企業価値影響額（1日あたりの平均） | | ▲ 22,171,217,598 | ▲ 1,007,631,228 | ▲ 485,311,206 | ▲ 286,353,796 | ▲ 312,337,011 | 37,459,703,613 |

| 事故ケース | | #07 | #08 | #09 | #10 | #11 | #12 |
|---|---|---|---|---|---|---|---|
| 発行済み株式数 | | 211,317,082 | 661,639,986 | 77,648,751 | 2,240,000 | 1,482,973,799 | 11,375,069,845 |
| 第n日目の期待株価から起算して乖離値（公表日前日を基準とする） | 1 | 3.16 | ▲ 0.98 | ▲ 3.84 | 18,297.41 | 11.20 | 7.40 |
| | 2 | 7.85 | ▲ 1.35 | ▲ 8.19 | 10,541.94 | | |
| | 3 | 11.50 | 1.00 | ▲ 5.80 | | | |
| | 4 | | | ▲ 3.94 | | 3.54 | 9.05 |
| | 5 | | | | 25,516.66 | 7.63 | 7.07 |
| | 6 | 10.91 | 0.61 | | 11,668.16 | ▲ 5.07 | 6.19 |
| | 7 | 5.25 | ▲ 0.31 | ▲ 3.84 | 24,905.94 | ▲ 1.86 | 4.53 |
| | 8 | 1.36 | 0.21 | | ▲ 5,530.62 | ▲ 7.44 | 4.56 |
| | 9 | ▲ 8.97 | 1.66 | ▲ 12.09 | 5,619.35 | | |
| | 10 | ▲ 13.28 | 6.85 | ▲ 8.76 | | | |
| | 11 | | | ▲ 15.04 | | ▲ 3.16 | 4.42 |
| | 12 | | | | | ▲ 0.54 | 6.47 |
| | 13 | ▲ 15.13 | 6.64 | | 25.51 | ▲ 3.77 | 5.61 |
| | 14 | ▲ 14.98 | 6.14 | ▲ 20.65 | ▲ 17,471.74 | ▲ 0.01 | 2.86 |
| | 合計 | ▲ 12.31 | 20.47 | ▲ 82.13 | 73,572.61 | 0.52 | 58.15 |
| | 1日平均 | ▲ 1.23 | 2.05 | ▲ 9.13 | 8,174.73 | 0.05 | 5.81 |
| 企業価値影響額（1日あたりの平均） | | ▲ 260,100,870 | 1,354,500,428 | ▲ 708,575,857 | 18,311,404,791 | 77,055,394 | 66,143,283,185 |

| 事故ケース | | #13 | #14 | #15 | #16 | #17 | #18 |
|---|---|---|---|---|---|---|---|
| 発行済み株式数 | | 92,501,883 | 1,929,268,717 | 744,912,078 | 421,254 | 2,805,000 | 3,772,082 |
| 第n日目の期待株価から起算して乖離値（公表日前日を基準とする） | 1 | ▲ 4.29 | ▲ 30.80 | ▲ 34.26 | ▲ 897.75 | ▲ 15,733.01 | ▲ 16,685.28 |
| | 2 | ▲ 6.92 | ▲ 33.09 | | ▲ 1,759.73 | ▲ 15,171.91 | ▲ 47,506.16 |
| | 3 | ▲ 7.66 | | | ▲ 403.98 | ▲ 16,869.83 | ▲ 13,680.38 |
| | 4 | ▲ 6.27 | | ▲ 45.02 | | | ▲ 25,192.78 |
| | 5 | | | ▲ 3.83 | | | ▲ 59,228.92 |
| | 6 | | 1.22 | 14.01 | 232.83 | ▲ 5,432.69 | |
| | 7 | ▲ 1.61 | 1.98 | 133.76 | | ▲ 11,858.05 | |
| | 8 | ▲ 8.63 | 25.58 | 113.46 | ▲ 1,369.10 | ▲ 17,856.56 | ▲ 60,940.78 |
| | 9 | ▲ 8.19 | 19.39 | | ▲ 3,448.42 | ▲ 17,301.00 | |
| | 10 | ▲ 8.64 | | | 1,220.09 | ▲ 13,364.31 | ▲ 30,775.69 |
| | 11 | ▲ 4.90 | | 87.21 | | | 12.47 |
| | 12 | | 12.21 | 57.12 | | | 23,081.48 |
| | 13 | | ▲ 1.35 | 119.58 | ▲ 646.77 | ▲ 18,805.98 | |
| | 14 | 24.66 | ▲ 12.39 | 156.98 | 992.66 | | |
| | 合計 | ▲ 32.46 | ▲ 17.25 | 599.02 | ▲ 6,080.17 | ▲ 132,393.35 | ▲ 230,916.05 |
| | 1日平均 | ▲ 3.25 | ▲ 1.92 | 59.90 | ▲ 675.57 | ▲ 14,710.37 | ▲ 25,657.34 |
| 企業価値影響額（1日あたりの平均） | | ▲ 300,260,009 | ▲ 3,697,318,776 | 44,621,905,127 | ▲ 284,588,230 | ▲ 41,262,593,460 | ▲ 96,781,584,542 |

# ＜昨年参考＞ 企業における情報漏洩事故の株価への影響想定とその利用

## ＜影響額の試算＞

① 各社の「前日株価に対する差額割合」である「0～9%程度」の利用

**影響額　＝　自社株価×（0～9%）×発行株数**

② 全社集計の「一株当たり差額」である「6～9円程度」の利用

**影響額　＝　6～9円×発行株数**

## ＜利用法＞

- 情報漏洩事故の株価への影響額を事前想定することは、経営者における予防的なリスク管理として重要。
- 影響の大きさを考えると、「情報セキュリティ対策費用」を単なる「システムコスト」ではなく、「企業価値の低下を防ぐためのIR費用の一つ」として捉え直すことも必要。

# ２００３年度のWG報告書

６月初旬までに、ＪＮＳＡホームページに公開予定。
URL:　http://www.jnsa.org/