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

2003 年 6 月 3 日

1．情報セキュリティ被害調査WG活動目的

＜昨年に引き続き＞

- 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

- **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。
- 昨年との違いを把握。
  →「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」

金銭的な被害額を知りたい。

- **第2部**：情報漏洩の被害額算出。
- 着眼点→賠償＆株価下落。
  →「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)」

2次的な被害額の予想。

3．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」

3.1 アンケート回収率とヒアリング引受率

	アンケート			ヒアリング		
	送付	回答	回答率	打診	承諾	承諾率
会員	159 (121)	53 (53)	33.33% (41.32%)	17 (20)	9 (11)	52.94% (55.00%)
非会員	20 (5)	13 (4)	66.66% (80.00%)	20 (14)	7 (5)	35.00% (35.71%)
合計	179 (126)	66 (54)	36.87% (42.86%)	40 (34)	20 (16)	50.00% (47.06%)

( )内は昨年度の数値

3.2 アンケート拒否の主な理由

- アンケート回答＝セキュリティ情報→公開不可。
- 社内ポリシーは外部に公開しない。
- 対策の開示は、自らの守り方の開示となる。 など

3.3 調査対象の状況

A-1属する主要業種

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

JNSAﾒﾝﾊﾞｰ企業中心のため高率

昨年とほぼ同率

A-2年間売上および従業員数

■ 平均値

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

A-3拠点数

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

添付ファイル制限が少なくない

B-1保有PCの台数

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

PCは1人1台以上保有

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

添付ファイル制限が少なくない

B-3Web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	3	4.5%
3	利用可能だが閲覧先の制限あり	13	19.7%
4	特に制限無く利用可能	50	75.8%
		66	100.0%

閲覧制限が少なくない

B-4インターネット利用可能ＰＣの割合

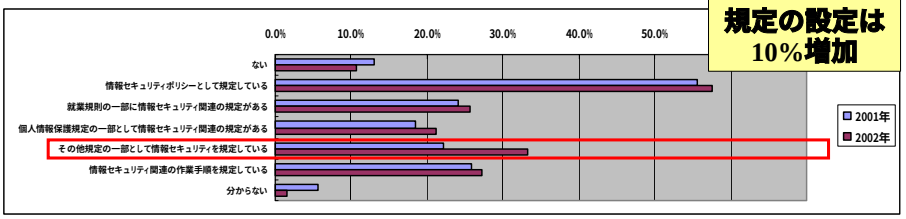
■ 平均値

1	インターネットメール (%)	90 %
2	Web閲覧 (%)	85 %

3．4情報セキュリティ状況の昨年比較
(詳細については報告書参照)

C-1情報セキュリティに関する規定について

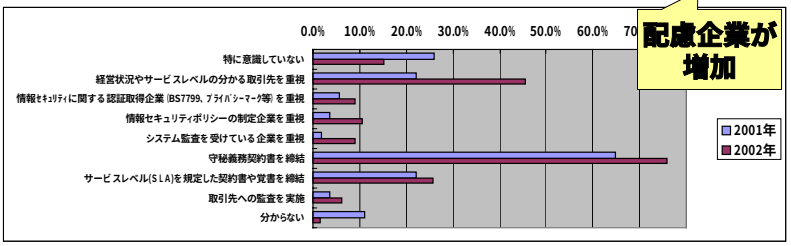
		2001年		2002年	
1	ない	7	13.0%	7	10.6%
2	情報セキュリティポリシーとして規定している	30	55.6%	38	57.6%
3	就業規則の一部に情報セキュリティ関連の規定がある	13	24.1%	17	25.8%
4	個人情報保護規定の一部として情報セキュリティ関連の規定がある	10	18.5%	14	21.2%
5	その他規定の一部として情報セキュリティを規定している	12	22.2%	22	33.3%
6	情報セキュリティ関連の作業手順を規定している	14	25.9%	18	27.3%
7	分からない	3	5.6%	1	1.5%



規定の設定は10%増加

C-5取引先の選定や契約時の注意点

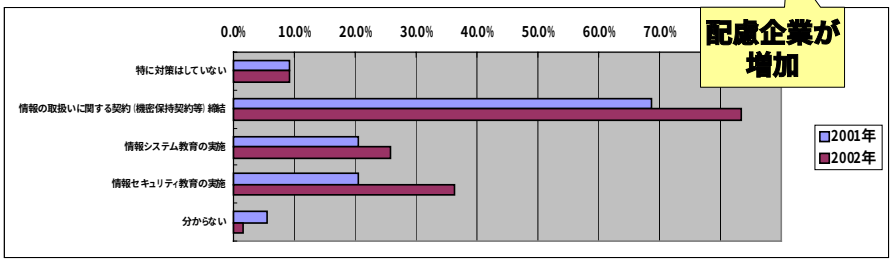
		2001年		2002年	
1	特に意識していない	14	25.9%	10	15.2%
2	経営状況やサービスレベルの分かる取引先を重視	12	22.2%	30	45.5%
3	情報セキュリティに関する認証取得企業（BS7799、プライバシーマーク等）を重視	3	5.6%	6	9.1%
4	情報セキュリティポリシーの制定企業を重視	2	3.7%	7	10.6%
5	システム監査を受けている企業を重視	1	1.9%	6	9.1%
6	守秘義務契約書を締結	35	64.8%	50	75.8%
7	サービスレベル(SLA)を規定した契約書や覚書を締結	12	22.2%	17	25.8%
8	取引先へ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



配慮企業が増加

C-6派遣社員や常駐作業員受け入れ時の配慮点

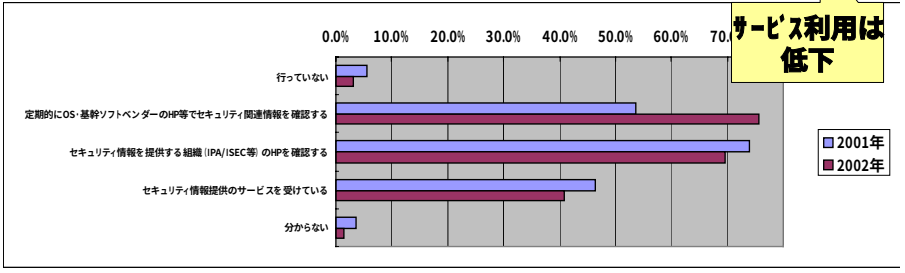
		2001年		2002年	
1	特に対策はしていない	5	9.3%	6	9.1%
2	情報の取扱いに関する契約（機密保持契約等）締結	37	68.5%	55	83.3%
3	情報システム教育の実施	11	20.4%	17	25.8%
4	情報セキュリティ教育の実施	11	20.4%	24	36.4%
5	分からない	3	5.6%	1	1.5%



配慮企業が増加

C-8情報セキュリティ関連のニュース収集

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

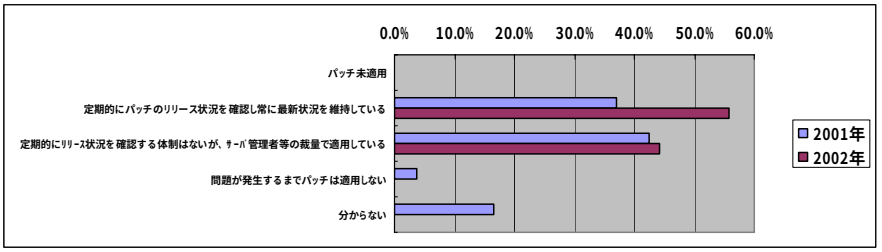


サービス利用は低下

C-9パッチの適用

配慮企業が増加

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

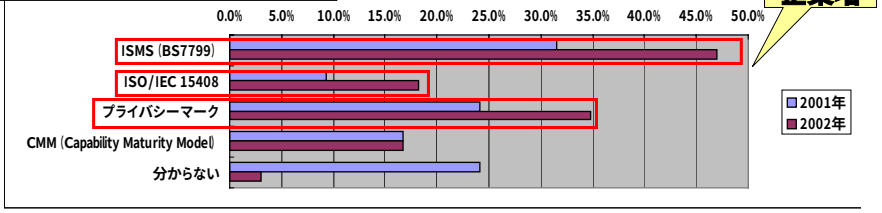


C-10各種認証の取得計画および取得状況

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

取得済＋検討中の合算

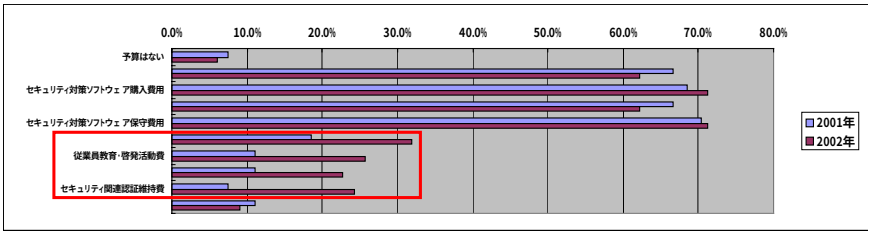
注目企業増



C-14情報セキュリティ関連予算

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

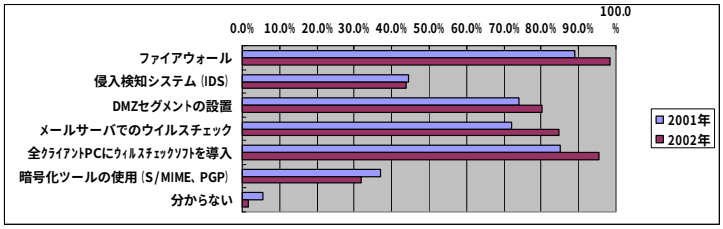
教育・啓蒙
認証が増加



C-15情報セキュリティ確保のための導入システム

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

F／W
ｳｨﾙｽﾁｪｯｸ
は当たり前



C-19現在実施もしくは今後実施の対策

★＝実施＋検討で75%以上

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

3.5被害状況の概要

①被害の状況 (インシデント毎の被害額)

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

＜昨年＞
合計額　約1億4千万円
平均　約32万円
件数　59件

被害額は激減

②インシデント別被害の状況(件数順)

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

＜昨年＞
被害項目上位：ﾆﾑﾀﾞ、ｺｰﾄﾞﾚｯﾄ
件数　59件

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。

- 「セキュリティ対策システムの導入比率との関係」
  →残念ながら特に相関を見出せず。(被害後、直ぐに対策実施か?)
- 「セキュリティ対策システムの導入率」は、かなり高い。
  →被害発生および拡大防止の大きな要因。
- システム以外の対策では、「情報セキュリティ教育」や「インシデント被害対策体制」が被害発生・拡大の抑止に貢献。

4.2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。

	従業員数（人）	セキュリティ予算（万円）	予算の割合（%）	一人あたりの予算（円）
被害有り平均	3,948	2,103	13.30%	12,977
被害無し平均	970	1,552	14.90%	67,051

・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）
・「情報セキュリティ予算」は、企業規模＝大で、一人あたりの金額＝少。

4.3望まれる対策レベルと予算規模

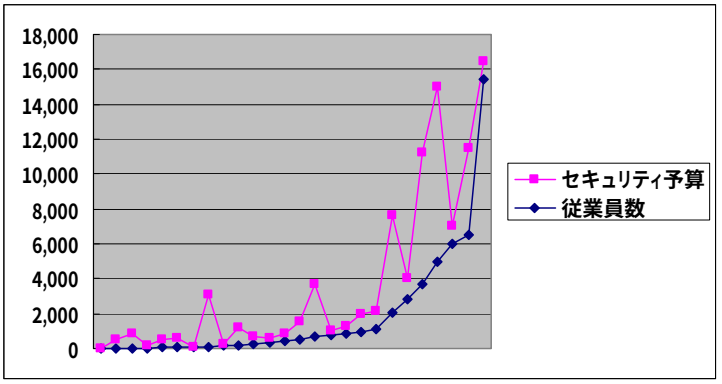
①現状で考えられる最低限の対策レベル

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

教育啓蒙が重要

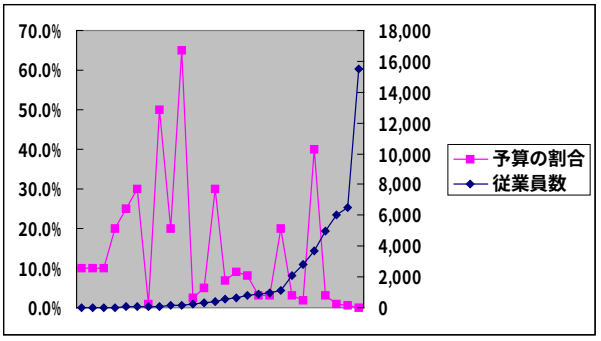
「運用上の対策をユーザに浸透させるセキュリティ教育・啓発活動の実施レベル」までを推奨。

②従業員数とセキュリティ関連予算



・情報セキュリティ関連予算の割合：
　　最大６５％（従業員数140名）、最小０．１％（従業員数15,470名）、平均１４．５％
・「従業員数」と「セキュリティ予算額」は、「ほぼ比例」している。

③従業員数と情報システム予算割合の比較



・「情報セキュリティ関連の保守費、運用対策費、セキュリティ教育費」
　　→情報システム予算の５～１５％程度をセキュリティ関連費用として計上。
・教育に関わる「セキュリティ教育啓発活動」に関しては、年間スケジュールを立案し計画的なセキュリティ対策の運用が重要。

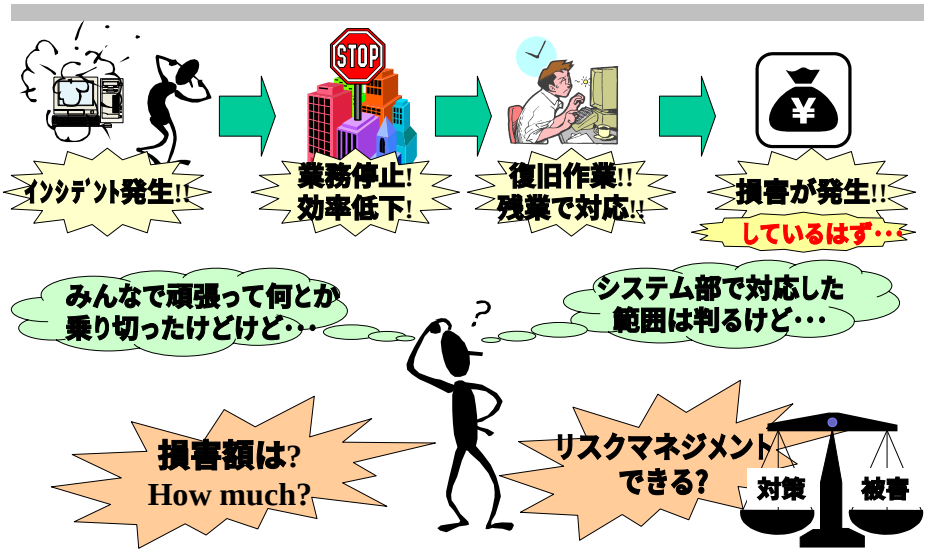
5.調査総括

・被害額は昨年に比べ大幅に減少。
　→ウイルス定義ファイルの更新の徹底が大きな要因。
・各社のセキュリティ対策は、かなり前進。
　→ファイアウォールやアンチウイルス対策＝ほぼ100％
　→侵入検知システム（IDS）＝43.9％
　→パッチ適用＝100％
・情報漏えいについては、人的要素大きい。
　→ポリシー等規定を設定＝約90％
　→体制整備・教育の実施も高い比率
　　→被害額が低く抑えられる結果につながった。
・被害のあった企業も各種対策は実施。（被害は小さい）
・情報セキュリティ予算は、65.2％が関連予算の一部で計上。
　（売上高対比は小さい。優先順位がまだ低い？）
・セキュリティ対策の「コスト」と「効果」を「定量的に把握」することが今後の課題である。

6.情報セキュリティインシデント被害額算出モデルに関する検討

- 昨年のモデルをベースに、今年度の調査項目を決定したが、調査項目に応じた回答はほとんど得られなかった。
- 今年度モデルについては、用語の整理、範囲拡張などを行った。

算出モデルの必要性(参考)



6.1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。

6.1.1 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）

6.1.2 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

6.2 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。

6.2.1 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

6.3 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＞

・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＞

・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

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

7. 今後の課題

JNSA

7.1 モデルの課題

7.1.1 情報セキュリティインシデント被害額算出モデルの課題

<昨年から継続の課題が多い>

- 実際の算出作業では、社内他部署へのヒヤリングなど「慣れ」が必要。
- 「IT感応度」は、導入状況や業種で大きく異なる。 (一般向け推奨値は0．2程度)
- 「IT感応度」の精緻化：被害発生時に調査し、システムダウンによる業務量低下の情報を収集。 (今年度は事故少なく、十分な収集できず)

7.1.2 情報セキュリティインシデントの対策標準モデルの課題

- 「事故少ないの理由」→事故有無によるグルーピングで比較検討。

→事故発生とアンケート時期とのタイムラグがあり、効果比較は難。(今後は事故とその後の対策についても調査の必要有り)

- 対策予算については、以前よりも具体的な数字を入れる企業が増えている。
- 今後重要な人系の教育や啓蒙の内容についても、踏み込みたい。

7.2 調査の課題

7.2.1 アンケートの課題

- 被害発生が昨年と比べ非常に少ない。
- 被害を金額化して回答を頂くことは、まだまだ非常に難しい。
- アンケート項目は、モデルに近い形に充分絞り込めた。
- 同じ担当者の回答を得られ、定点観測の体制は充実してきた。

7.2.2 ヒアリングの課題

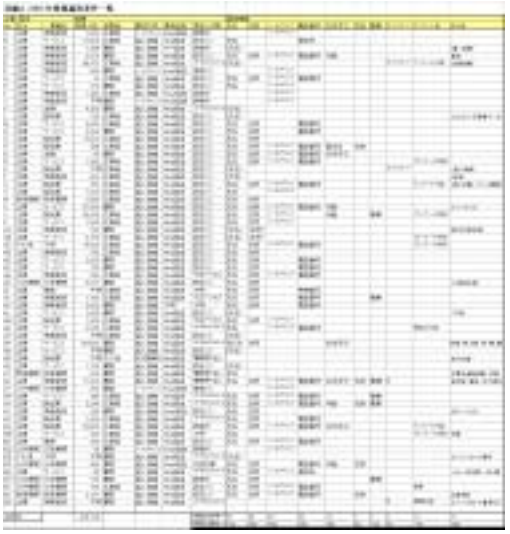
- ヒアリング調査に応じていただける先は、まだ少ない。
- 2回目の調査であり、調査はスムーズに行えた。
- 何分人手が少なく、ヒアリング業務がメンバーの負荷となる。

8. 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)」

＜目的＞

- 算出モデル
→波及的な被害として、損害賠償額などの被害についても言及。
- 情報漏洩を対象とした「損害賠償の可能性」についての検討や考察、企業価値の一端となる「株価への影響」について実例調査などを実施し、モデルへの適用も狙いたい。
- 当WGより、「損害賠償金額の算出」や「株価への影響額」の算出について、提案を行う。
- 未熟な提案でも、各方面の専門家に対する「共通の題材」としての意義は大きいと考える。
- 企業経営者が考えるべき情報資産に関わるリスク量の把握や行うべき投資判断基準の材料となることを期待。

8.1国内の情報漏洩の分析



＜漏洩事故の概要＞

個人情報漏洩　　：57件 (90%)

メールアドレス漏洩：5件 (8%)

非公開資料漏洩　：1件 (2%)

インターネット公表　：63件

被害者の合計人数　：41万8,716人

1件当たり人数　　：6,646人

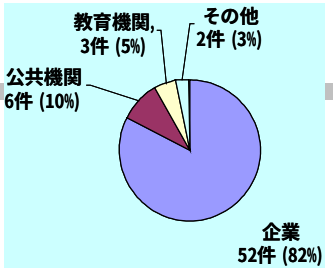
8.2漏洩情報の分析(項目)

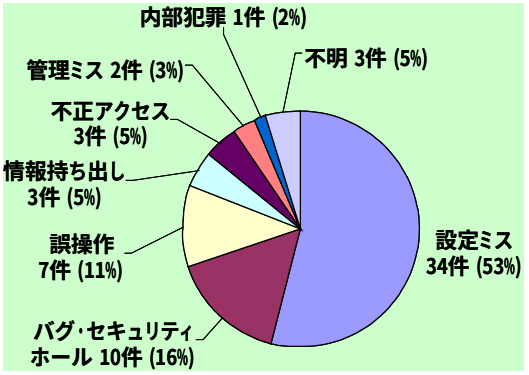
漏洩情報名称	件数 (出現%)
氏名	54 件 (86%)
住所	38 件 (60%)
メールアドレス	29 件 (46%)
電話番号	28 件 (44%)
生年月日	10 件 (16%)
職業	6 件 (10%)
性別	5 件 (8%)
ユーザ ID	4 件 (6%)
パスワード	2 件 (3%)
アンケート関連	11 件 (17%)
その他	21 件 (33%)

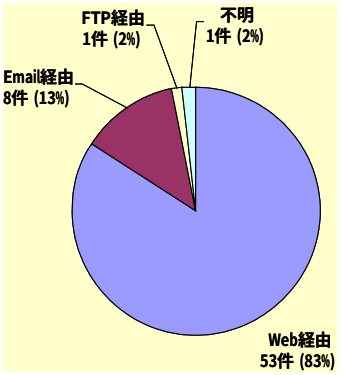
「氏名」→86%
上位4つの情報
→「氏名」、「住所」、「メールアドレス」、「電話番号」

その他
フリガナ、スリーサイズ、顔写真、身長、血液型、星座、趣味、年収、学歴、出身高校、進路情報、成績、企業名、部署名、セミナー応募情報、社内文書、社内資料、グローバルIP、クレジットカード番号、プリペイドカード番号など。

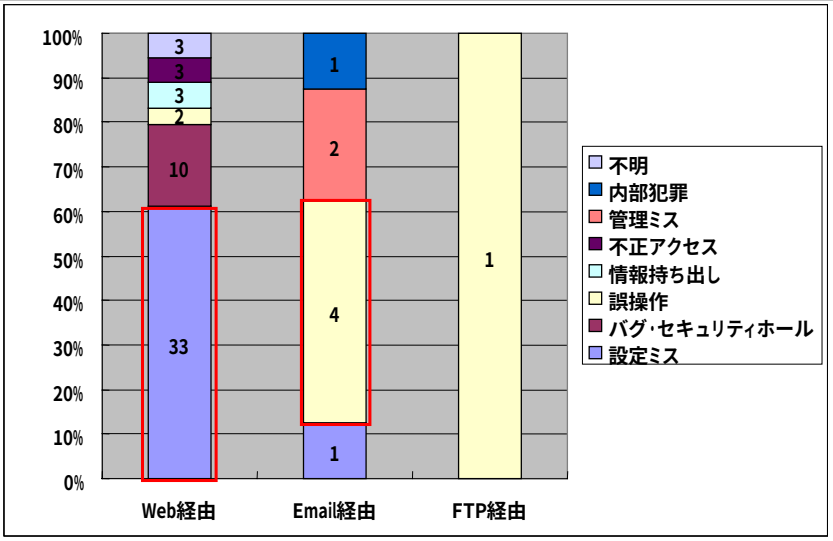
8.3情報漏洩元の分析



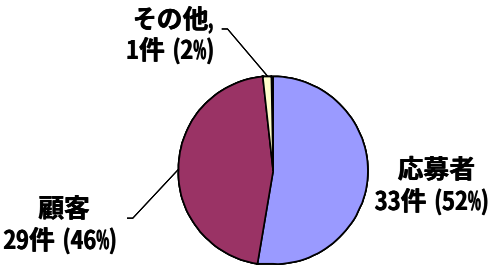




8.4情報漏洩経路の分析



8.5情報漏洩被害者の分析



応募者	444,276人	(54%)
顧客	379,868人	(46%)
その他	0人	(0%)

Web間での「情報漏洩事故」のため、被害者は2つに大別。
→アンケート、プレゼント応募
→商品などを購入した顧客
(被害者実数は、アクセス回数などのログが残っていない限り、正確な算出は困難なため、現状では、可能性のあるものは被害者数にカウント。)

8.6情報の種類と賠償額

8.6.1宇治市住民基本台帳データ大量漏洩事件控訴審判決より
・漏洩情報＝住民基本台帳の情報
個人連番の住民番号，住所，氏名，性別，生年月日，転入日，
転出先，世帯主名，世帯主との続柄等の個人情報の記録
・漏洩件数
住民記録 18万5800件
外国人登録関係 3297件
法人関係 2万8520件
合計 21万7617件
・賠償額
被控訴人らに対し、慰謝料として1人当たり1万円
弁護士費用は，被控訴人ら1人当たり5000円
よって、1人当たりの賠償額は、1万5000円

15,000円 × 217,617件 = 32億6425万5,000円

8.6.2情報の価値基準の検討

・基本的な個人情報に対する慰謝料

「氏名」「住所」「電話番号」「生年月日」「性別」「メールアドレス」など、

・特徴的な個人情報に対する慰謝料

漏洩した情報が、個人の家族関係や身体的特徴に関するものなど私生活上の事柄を含むものならば、大きな精神的苦痛を感じるため、慰謝料が高額。

例）

- 身長、体重、スリーサイズ、顔写真、
- 年収、学歴、企業名、部署名
- 趣味、購入商品
- 家族構成、既婚/未婚　など

・情報漏洩元組織の社会的信頼度と慰謝料の関係：

情報漏洩元組織の社会的信頼度が高い＝漏洩情報の信憑性も高い。

8.6.3 被害者と情報漏洩元組織の対応姿勢

①情報漏洩元組織における事件に対する対応姿勢

- 事件の公表
- 被害者に対する事実周知と謝罪
- 漏洩情報の回収努力
- 事件再発防止の努力　など

②被害者における個人情報の取り扱い姿勢(提供の同意)

ベンダー・組織に対して顧客として個人情報を提供→非自発的

アンケートやプレゼント応募において個人情報を提供→自発的

8.6.4情報漏洩事件における損害賠償額の算出式

情報漏洩元組織の損害賠償額（評価ポイント）
= 漏洩情報の内容に基づく慰謝料→①
× 個人情報提供の同意の有無→②
× 情報提供者との関係→③
× 情報漏洩元組織の社会的信頼度→④
× 事件後の対応姿勢→⑤

算式項目	状況別ポイント
①被害者に対する慰謝料	基本的な個人情報 = 100
	特徴的な個人情報(3 種類以下) = 500
	特徴的な個人情報(それ以上) = 1000
	メールアドレスのみ = 10
	個人を特定する ID,パスワード関係 = 300
②個人情報提供の同意の有無	同意有り = 2.0
	同意無し = 1.0
③情報提供者との関係	顧客 = 2.0
	アンケート、プレゼント応募者 = 1.0
④情報漏洩元組織の社会的信頼度	一般より高い = 1.5
	一般的 = 1.0
事件後の対応姿勢	良い = 1.0
	普通 = 2.0
	悪い = 4.0

8.7想定慰謝料の評価ポイント

評価ポイントと想定慰謝料の対応表

1 件当たりの評価ポイント	想定慰謝料 (算出用基準)
1000 ポイント未満	0～ 5,000 円 (5,000 円)
1000～2000 ポイント未満	～10,000 円 (10,000 円)
2000～5000 ポイント未満	～50,000 円 (50,000 円)
5000 ポイント以上	50,000 円以上 (100,000 円)

評価ポイントの適用例(宇治市事例への適用)

宇治市事故への評価ポイント適用
= 漏洩情報の内容に基づく慰謝料 [基本情報+特徴情報：600]
× 個人情報提供の同意の有無 [同意有りと仮定：2]
× 情報提供者との関係 [顧客に相当：2]
× 情報漏洩元組織の社会的信頼度 [一般より高い：1.5]
× 事件後の対応姿勢 [良い：1]
= 3600ポイント→1～5万円範囲に相当(実際の慰謝料部分は1万円)

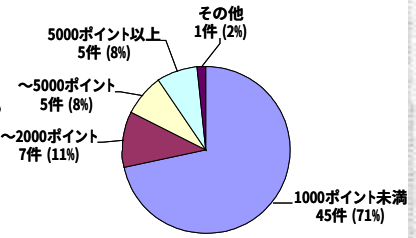
8.8国内の情報漏洩事故による損害賠償被害額想定

各事例への評価ポイントの適用と一覧表

損害賠償総額(想定) ：151億4,270万円 (合計人数 418,716人)

平均損害賠償額(想定)： 2億4,036万円 (平均人数 6,646人)

各事例に評価ポイント適用



9.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。

9.1情報漏洩事故発生後の株価変動の把握方法について

＜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＝（基準レシオー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＞

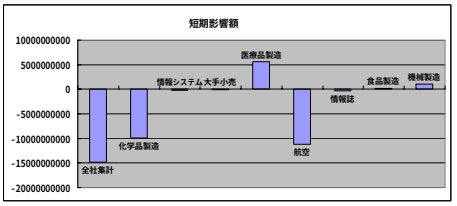
基準レシオ　＝　事故発生の前月末の（当該企業株価／日経平均）
nヶ月末レシオ　＝　事故発生のnヶ月末の（当該企業株価／日経平均）
nヶ月値＝（基準レシオーnヶ月末レシオ）×nヶ月末の日経平均値×発行株数
事故発生4ヶ月間を評価

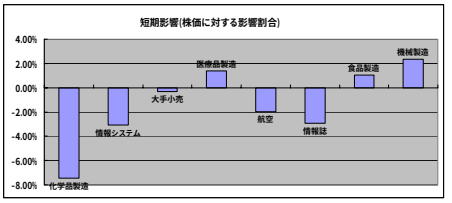
中期株式影響額＝1～4ヶ月値の合計／4ヶ月

9.2実例による株価変動の調査

9.2.1短期影響額

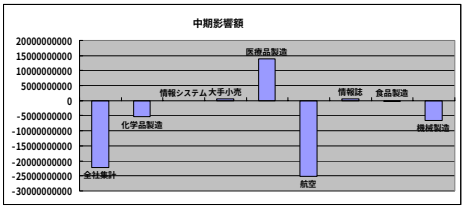
8社の短期影響額の合計　＝　150億円

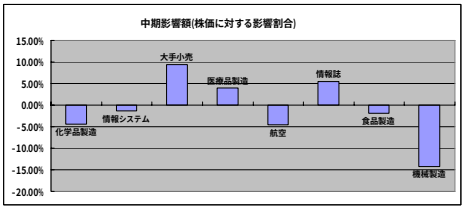




9.2.2中期影響額

8社の中期影響額の合計 ＝ 220億円





9.3 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。

9.4 算出基準値の課題

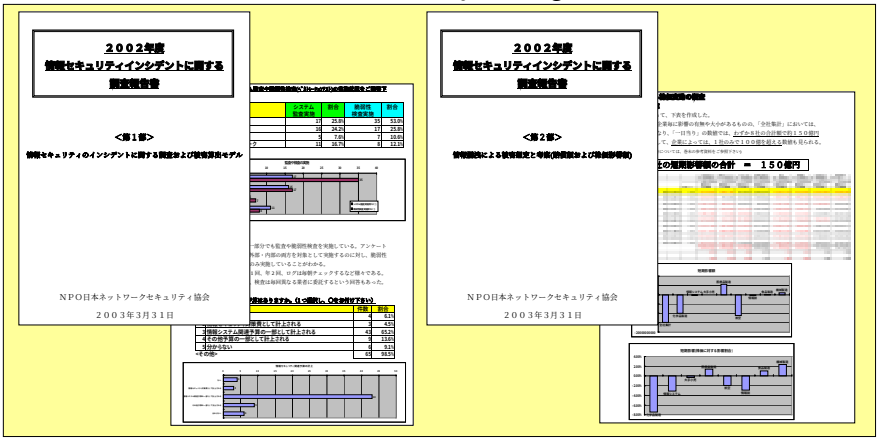
今回は、算出の基準値として「日経平均」を利用した。しかしながら、株価の動きには業種毎のトレンドがあり、「日経平均」と「業種平均」が乖離する事は日常的。

企業経営者の立場としては、**同業他社との優劣**も重要。今後は影響の把握をより精緻にするため、算出の基準値に**「業種平均」**を取り入れることを今後検討する。

10．２００２年度のWG報告書

6月中旬以降、ＪＮＳＡホームページに公開予定。
URL:　http://www.jnsa.org/

ヒヤリング でも
コメントも掲載



11．2003年度の活動

2002年度は、モデルの検討を十分に行ったが、被害そのものが少なく、調査結果からモデルの精緻化の作業を行うことは難しい状況であった。

対策レベルの向上に伴い、今後は、被害の有無だけでなく、**被害拡大の有無やその理由**までを検討していきたい。

また、今年度スポットをあてた**「情報漏洩の賠償や株価への影響」**の様に、企業経営者にとっての損害について検討を行いたい。

10.1活動内容

- 2002年度調査の課題への対応と**再調査実施**
- **モデルの精緻化**
- 被害発生時の**緊急ヒヤリング体制**整備、事故情報の収集
- 各種被害項目における被害額算出方法の検討

10.2成果目標

- 情報セキュリティーにおける「対策費用」対「効果」の把握を容易にするため、被害額や対策額の算出モデルの継続提案。
- リスクマネジメントの現実的な解として、各種項目における被害額算出方法の提案。

被害推計への挑戦

JNSA