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

2002 年 11 月 13 日

1．情報セキュリティ被害調査WG活動目的

JNSA

- 国内におけるセキュリティインシデントに関する**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

- 被害の実態や対策の状況をつかむため、調査を実施。

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係る被害額･投資費用に関する調査」の実施

- 被害＆対策コストなどの算出モデル提案。

被害の範囲や金銭的な置き換えはどうする？

→「被害額算出モデル」の提案

3.3 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	121	50	41.32%	20	11	55.00%
非会員	5	4	80.00%	14	5	35.71%
合計	126	54	42.86%	34	16	47.06%

3.4 アンケート拒否の主な理由

･外資系企業で本社承認がとれなかった。
･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

3.4 調査結果の分析と特徴

3.4.1対象企業概要

①業種について

業種	回答数	割合
金融（銀行、保険、証券等）	3	6%
医療・製薬	0	0%
運輸	1	0%
エネルギー	1	2%
情報・通信	33	63%
教育・マスコミ	1	2%
建設	0	0%
飲食・小売	0	0%
その他サービス	7	13%
その他	6	12%
総合計	52 （未回答2件除く）	100%

②従業員数とコンピュータ(ＰＣ)の導入台数業種について

		a	b	c	d	e	
PC 保有台数 / 従業員数		1 台	2～10 台	11～100 台	101～1,000 台	1,000 台以上	合計
A	1 人						0
B	2～49 人			9			9
C	50～99 人			4	4		8
D	100～499 人				7		7
E	500～999 人				1	3	4
F	1,000～9,999 人					15	15
G	10,000 人以上			1		8	9
合計		0	0	14	12	26	52 （未回答2件を除く）

③インターネット接続状況

	接続形態	企業数	割合
a	接続なし	0	0%
b	ダイヤルアップ接続（モデム、ISDN）	0	0%
c	常時接続 ISDN	1	2%
d	常時接続 ADSL、CATV	6	12%
e	常時接続 専用線 ～1Mbps	2	4%
f	常時接続 専用線 1～5Mbps	27	51%
g	常時接続 専用線 5Mbps～	16	31%
h	その他	0	0%
	合計	52（未回答 2 件を除く）	100%

④情報セキュリティに関する規定の制定状況

少ない!

	情報セキュリティの規定状況	企業数	割合
1	ない	7	8%
2	情報セキュリティポリシーとして規定している	30	34%
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	15%
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	11%
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	13%
6	情報セキュリティ関連の作業手順を規定している	14	16%
7	分からない	1	1%
8	その他	2	2%
	該当項目数の合計	89	100%

⑤情報セキュリティの管理部門や管理者について

	情報セキュリティ管理部門の設置状況	企業数	割合
1	ない	7	13%
2	全社の情報セキュリティ業務を担当する専門部門がある	14	27%
3	全社の情報セキュリティ業務を兼任する部門がある	20	39%
4	全社の情報セキュリティ業務を担当する委員会がある	7	13%
5	各事業部や部単位で独自に情報セキュリティに対する取組をしている	2	4%
6	分からない	1	2%
7	その他	1	2%
	合計	52 (未回答2件有り)	100%

合計17%も!

	情報セキュリティ管理者	企業数	割合
1	責任者は決まっていない	8	15%
2	責任者が任命されている	35	65%
3	責任者は任命されていないが担当者はいる	7	13%
4	わからない	4	7%
	合計	54	100%

⑥情報セキュリティに関する教育の実施状況について

	セキュリティ教育の実施状況	企業数	割合
1	未実施	20	29%
2	経営者・役員クラスを対象とした情報セキュリティ管理教育	4	6%
3	全管理職を対象とした情報セキュリティ管理教育	11	15%
4	全管理職を対象とした情報セキュリティ関連技術教	2	3%
5	一部の管理職を対象とした情報セキュリティ管理教	2	3%
6	一部の管理職を対象とした情報セキュリティ関連技術教育	1	1%
7	情報セキュリティ管理者を対象とした情報セキュリティ関連技術教育	6	8%
8	希望者を対象とした情報セキュリティ関連教育	3	4%
9	全社員を対象とした情報セキュリティ関連教育	19	27%
10	分からない	3	4%
	合計	71	100%

⑦情報セキュリティ関連予算について

独立科目は13%のみ!

	情報セキュリティ関連予算	企業数	割合
1	ない	4	8%
2	情報セキュリティ対策費として計上される	7	13%
3	情報システム関連予算の一部として計上される	29	55%
4	その他予算の一部として計上される	5	9%
5	分からない	5	9%
6	その他	3	6%
	合計	53 (未回答1件有り)	100%

3.4.2被害状況の概要

①被害の状況 (回答30企業中の上位10企業分)

(インシデント毎の被害額、1企業最大3インシデントまで発生していた。)

	コスト／日	インシデント毎の被害額 ①事故	②事故	③事故	年間合計 (単位：円)
1	40,000	60,000,000			60,000,000
2	40,000	200,000	20,000,000	60,000	20,260,000
3	40,000	1,860,000	15,000,000		16,860,000
4	150,000	15,750,000			15,750,000
5	30,000	1,500,000	4,500,000		6,000,000
6	45,000	3,915,000	549,000	450,000	4,914,000
7	150,000	1,500,000	3,000,000	20,000	4,520,000
8	40,000	2,004,000	40,000	2,400,000	4,444,000
9	40,000	416,000	800,000	800,000	2,016,000
10	40,000	220,000	1,620,000	80,000	1,920,000

・金額は、報告ベース。
・不明な部分（下線）は、「復旧に要した作業量」 n名×m日×1日で算出。

②インシデント別被害の状況

アンケートコード No	被害項目	件数	件数比率	金額	金額比率
8	Nimda ニムダ	18	31%	73,730,000	52.1%
11	CodeRed コードレッド	13	22%	45,949,000	32.5%
10	Navidad ナビダッド	3	5%	15,778,800	11.2%
5	Magistr マジストラ	1	2%	1,620,000	1.1%
3	Sircam サーカム	3	5%	757,000	0.5%
7	Laroux ラルー	3	5%	516,000	0.4%
2	Badtrans バッドトランス	5	8%	345,000	0.2%
6	Aliz アリズ	1	2%	30,000	0.0%
12	風評被害	1	2%	80,000	0.1%
13	誤操作	2	3%	280,000	0.2%
17	ﾎｰﾑﾍﾟｰｼﾞ改ざん	1	2%	20,000	0.0%
19	その他	8	14%	2,374,000	1.7%
	合計	59	100%	141,479,800	100.0%

84%!

③被害のあった企業の特徴

＜検討項目＞
① 所属する主要業種
② 従業員数と保有しているパーソナルコンピュータの台数の関係
③ インターネットへの接続および、情報システムネットワークの有無
④ 情報セキュリティに関する規定の有無
⑤ 情報セキュリティに関する、管理部門、管理者の状況
⑥情報セキュリティに関する教育
⑦情報セキュリティ関連予算の状況

＜結論＞
被害のあった企業とない企業との間で大きな違いは見られない。

④インシデントが発生した最大の原因

No	最大の原因	回答数	割合
1	セキュリティ関連予算の不足	0	0%
2	セキュリティ管理体制が不十分	24	45%
3	セキュリティ対策技術が不十分	3	6%
4	セキュリティ関連情報の不足	11	21%
5	分からない	0	0%
6	その他	15	28%
	合計	53	100%

3.5調査総括

- HP改ざん、不正アクセス、情報漏洩などの被害報告件数はそれほど多くなかった。
- 重要インフラ、IT関連企業→基本的対策は一巡か？
- ウイスル、ワームによる局地的な被害を経験。
- 基幹システムや業務システムに大きな被害は無い。

(これらはインターネット未接続のため？)

- 長時間停止した場合でも、代替え手段や復旧後の残業などで、被害を抑制している。

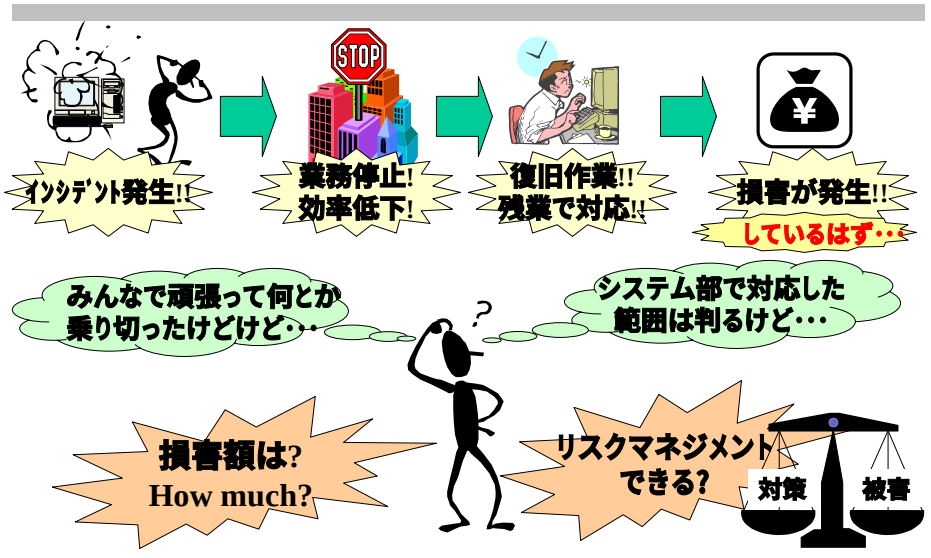
- **メール感染のウイルス発症時の企業の行動。**
  - ネットワークから切断して検疫。感染経路特定と他システムへの伝播を確認。
  - 他システムも一時的にネットワークから切断し、検疫。感染範囲を特定し、それぞれ検疫。
  - 感染システムが少ない場合、代替機で業務を継続。システム使わない業務フローに切り替える。
  - 感染システムが多数の場合でも、代替え手段で業務を継続しつつ、情報システムやパワーユーザーが復旧に尽力。

- 業務継続性→ダウン時の代替え手段の有無による影響は大きい。
- 業務スタート時点から、システム＆ネットワークで行う業務は、特に注意が必要。(新興のドットコム企業など)
- 被害の金額について質問
  →回答の範囲や形態は様々。

4．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

- 調査で情報セキュリティインシデントに関する被害の金額について質問を行うが、**回答の範囲や形態は様々**だった。
- 被害として認識する範囲や被害金額として算出する方法に**統一性が無ければ、被害の規模や規模の比較が行えない**。
- **「各人の認識のすりあわせ」＝「被害額算出モデル」が必要!!**　(対策額についても同様!)

算出モデルの必要性



4.1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。

4.1.1 1次的な被害額

1次的な被害額＝

逸失利益＋復旧に要したコスト

（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）

4.1.2 2次的な被害額

2次的な被害額＝

補償、補填、損害賠償利益など、2次的に生じた被害

4.2 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。

4.2.1 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

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

4.3 インシデント被害額算出モデル

インシデント被害額
＝潜在化被害＋表面化被害
＝業務にかかわる潜在化被害＋業務外の潜在化被害＋表面化被害
＝（（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）
＋復旧に要したコスト（ハードウエア、ソフトウエア、工数）
＋逸失利益（直接的な被害）
＋補償・補填・損害賠償（間接的な被害）

＜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。

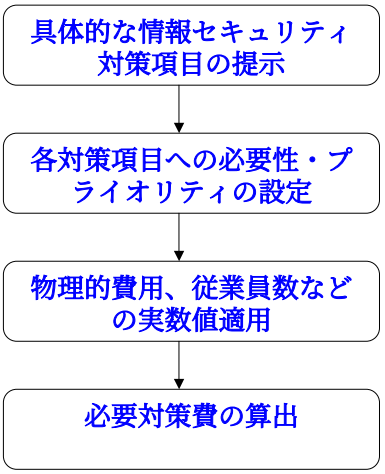
5. 情報セキュリティインシデント対策費用額の算出モデルについての検討

5.1 情報セキュリティ関連予算の実際と算出モデル

- 「情報セキュリティ対策費」予算化→約17%
- 理由は?(推測)
  ① 情報システム関連費用からの分離が困難
  ② 別予算化の必要性について認識が無い
  ③ リスク分析が不十分(場当たり的な対策?)
  ④ アウトソーシング多い→セキュリティ部分合算?業者任せ?
  ⑤対策費用の範囲が不明確→算出できない!

対策額の算出においても被害額算出と同様に算出モデルが必要!!

- **対策費用額の算出モデル検討手順**



5.2 具体的な情報セキュリティ対策項目の提示

対策対象によって、「ウイルス被害」、「不正アクセス・不正侵入」、「内部犯罪等による機密情報漏洩」の3つに大きく分類される。

インシデントの種類	対策例	対象資産	
		物的ﾘｿｰｽ	人的ﾘｿｰｽ
ウイルス	ウイルス対策ソフトの導入	○	◎
	最新のセキュリティパッチの適用		◎
不正アクセス	サーバーの要塞化	○	○
	サーバーへの最新セキュリティパッチの適用		○
	システムのセキュリティ監査（検査）	○	○
	24 時間監視	○	○
	データ／ソフトウエアのバックアップ	○	○
	ハードウエアの増長性確保	○	○
	ファイアウォール	○	○
	IDS 導入	○	○
	暗号化技術の適用	○	◎
	認証システムの導入	○	◎

＜つづき＞

インシデントの種類	対策例		対象資産	
			物的ﾘｿｰｽ	人的ﾘｿｰｽ
機密情報漏えい	ソーシャルエンジニアリング対策	廃棄物処理	○	◎
		建物（施設）のセキュリティ強化	○	
		ネットワーク管理ツール	○	
全般	セキュリティポリシーの徹底	ポリシーの策定		○
		ポリシーの運用と見直し		○
		従業員教育		◎
	コンティジェンシープランの策定	プランの策定		○
		物理的なリソースの確保	○	
		定期的な訓練		◎
		プランの見直し		○

＊人的リソースの“◎”は従業員全員が関与するもの、“○”は主にセキュリティ管理部門（者）が関与するもの

5.3 各対策項目への必要性・プライオリティの設定

5.3.1 経営サイドから見た必要性、プライオリティの設定

事業予算＞情報システム関連予算＞セキュリティ対策予算

5.3.2 システム（セキュリティ）管理者サイドから見た必要性、プライオリティの設定

資産の洗い出し、

① 対象となるコンピュータシステム

② 当該コンピュータシステムで提供される業務

重要度	サービスレベル
S	業務が停止することは許されない。
A	24時間以内に復旧する必要がある。
B	3日以内に復旧する必要がある。
C	緊急事態の際には停止してもよい。

加害者にならないためには、最低限のセキュリティ対策は必須!!

5.4 物理的費用、従業員数などの実数値の適用、必要対策費の算出

① 物的リソース

→実際に発生するハードウェア費用、ソフトウェア費用（初期導入費用、保守費用）の設定

② 人的リソース

→対象業務に関与する

人数×人件費×時間

により求められる金額を設定

5.5 情報セキュリティ対策費用把握の必要性について

- 情報システムは、戦略的な投資対象として扱われる傾向大。
- 重要インフラの保守側面として、情報セキュリティインシデント対策費用が急拡大。
- 「効果」と「安全」の2予算の正確な把握が効率的な投資に必要!

6. 想定企業および被害への情報セキュリティ被害算出モデルの適用と考察

- 「被害額算出モデル」を架空の会社、インシデントに当てはめて算出。
- 算出結果に基づき、モデルの実用性を検証。
- モデル利用において、ユーザが事前に知っておくべきパラメータ（人件費や売上規模、IT依存度など）を確認。

6.1 被害額算出モデルを使用したシミュレーション

6.1.1 会社のプロファイル

架空企業のセキュリティ対策は弱く設定し、被害が広範囲となるように設定した。

＜概要＞

中堅のシステムインテグレーターを想定!!

業種　：SIベンダー
従業員数　：社員　95名　　派遣　8名
年商　：30億円（8千万円がオンラインショップ売上）

6.1.2 社内システムの構成

端末　：全 120台
サーバ　：全10台(内部GW、業務系、開発用、公開用、F/W)

6.1.3 現在のセキュリティ施策(想定)

- インターネットアクセス（メール、Web閲覧）、ユーザ端末間のファイル共有に規制無し。
- ゲートウェイ型ウイルスチェックサーバなし。
- ウイルス対策は各ユーザ端末で実施。ただしウイルスパターン更新はユーザまかせ。
- 障害発生時の手順は未整備（セキュリティポリシーなし）。
- セキュリティ管理者不在（情報システム担当が兼務）
- 公開サーバは情報システム部門が管理(最新パッチはあてている)。
- 派遣社員の端末も情報システム部門が管理。
- 社内サーバや各端末のパッチなどメンテナンスは各部署および各ユーザまかせ。

6.1.4 事前に判明しているパラメータ

＜項目抜粋＞

・平均人件費：　時間単価6,000円

・1日の平均売上：通常売上、オンラインショップ

　・各部署別の1名あたりの時間被害額（固定費×IT感応度）

　　・営業部　　：　2,700円/1h

　　・技術部　　：　4,500円/1h　　など

・各サーバの停止が及ぼす被害の範囲

　・公開サーバ：全社員のメールなど、オンライショップ

　・内部ゲートウェイ：　全社員のメールなど

　・営業サーバ：　営業部員の資料作成など

　・業務サーバ：　受発注業務など、オンライショップ　　など

6.1.5 被害のシナリオ

・メール添付のウイルスで感染
・サーバ、端末を社内ＬＡＮから切り離す。
・最新のウィルスパターンをメディアで配布。
・各サーバ数百～数千のファイルが感染のため、
　駆除を断念しフォーマット、バックアップ。　など

6.1.6 シナリオに沿った被害額の算出 (被害額算出モデルの利用)

・各サーバの停止時間
　・内向けGW　：　23時間30分
　・営業サーバ　：　23時間30分
　・技術サーバ　：　23時間30分
　・業務サーバ　：　11時間
　・経理サーバ　：　11時間

a. 業務に関わる潜在化被害＝

固定費×影響を受けた人数×IT感応度×停止時間

・各部署毎に算出。
・サーバの停止時間のみを考慮。(端末は先に復旧)
・サーバの停止時間＝業務時間。(20:00～翌9:00を引く) など

＜各部署の被害額の算出＞

・営業部：　2,700円×22人×12時間＝712,800円
・技術部：　4,500円×24人×12時間＝1,296,000円
・マーケティング部：　3,200円×11人×12時間＝422,400円　など

業務に関わる潜在化被害：約３６０万円

b. 業務外の潜在化被害

本シナリオでは被害なし：　0円

c. 復旧に要したコスト

- 社員がウイルスチェックに関わった時間：10分/1人
- 端末のウイルス駆除、再構築所要時間：4時間/台
- 管理・経理サーバのウイルス駆除、再構築所要時間：11時間/台
- その他サーバのウイルス駆除、再構築所要時間：24時間/台
- ウイルスパターン更新用CD-ROM作成および支店配布費用
- FAXによる詫び状送付

復旧に要したコスト：　約１３０万円

d. 逸失利益（直接的な被害）

- 通常の営業利益は残業や代替手段で業務を継続することで損失なし。
- 業務サーバ11時間停止＝オンラインショップ停止

360,000円×11時間/24時間＝165,000円

e. 補償・補填・損害賠償（間接的な被害）→　0円

f. 総合計　a.～e.の合計：約５１０万円

6.2シミュレーションの評価・考察

6.2.1経験的に想定される被害額と算出された被害額の差異

- 調査で「復旧金額を60,000,000円」の回答者
- クライアント数4300台規模のユーザ
- クライアント数→本想定企業の約40倍

- ヒアリング調査のユーザ事例：　60,000,000円
- 6.1.6　c.の復旧費用の40倍：1,316,900円×40＝　53,036,000円

6.2.2パラメータに関する検証

a. 人件費

基本的には全社員の平均人件費の使用で充分と考える。

b. IT感応度

コンピュータやネットワークに依存する割合で考慮すべき項目

- 職種： 営業、技術、業務・・・。
- 役職： 社長、部長、課長、一般社員・・・。
- 作業内容： Web閲覧、メール、各種文書作成、開発、受発注、伝票処理・・・。
- 代替手段： 紙ベースの受発注処理、手書きの見積、FAXによる提案書送付・・・。
- 季節係数： 決算期、年末年始・・・。

算出結果の精度アップ→すべてを検討。
運用の簡便さを優先→「職種」と「作業内容」、「代替手段」

c. 停止時間

30分単位で充分

d. その他パラメータ

- 復旧に要したコスト→被害発生の記録が重要。特に人件費、ハード・ソフト費用以外に通信費や運送費など
- 逸失利益→間接的な利益の損失は難しい。(日本の企業は残業などでカバー) 業種によっては、季節的な変動も考慮。
- 補償などは事後に発生するもので、実際の金額はその時判明する。

6.2.3 算出モデルを利用するためのポイント

利用上のポイント

- 目的
- 事前に用意するパラメータ
- 精度

- **目　的**

→対策費を計上？事後の被害額調査？

- **精　度**

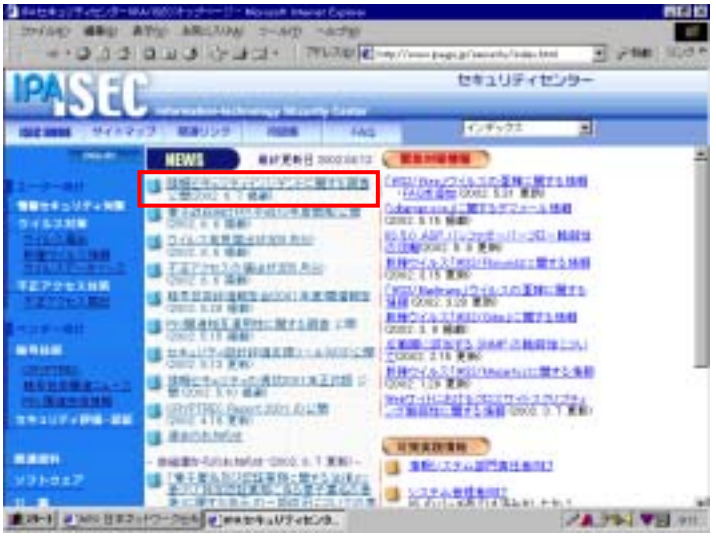
→事前調査する項目・パラメータも多くなる。運用上の簡便さとのバランス!!

6.2.4実例とモデル式の結果の比較

	A	B	C	D
企業規模（社員数）		30000	30000	
01 インシデント被害額(=11+12)	\77,434,000	\2,220,000	\18,600,000	\2,816,000
11 潜在化被害(=21+22)	\74,304,000	\360,000	\3,600,000	\2,400,000
21 業務に関わる潜在化被害(=31*32*33*34)	\74,304,000	\360,000	\3,600,000	\2,400,000
31 人件費（/時間）	6,000	6,000	6,000	6,000
32 影響を受けた人数	2,580	150	1,500	500
33 IT感応度（1～0）	0.2	0.2	0.2	0.2
34 停止時間（時間）	24	2	2	4
22 業務外の潜在化被害(=41)	\0	\0	\0	\0
41 業務外の潜在化被害	\0	\0	\0	\0
12 表面化被害(=51+52+53)	\3,130,000	\1,860,000	\15,000,000	\416,000
51 復旧に要したコスト（ハードウェア、ソフトウェア、工数）	\3,130,000	\1,860,000	\15,000,000	\416,000
52 遺失利益（直接的な被害）	\0	\0	\0	\0
53 補償・補填・損害賠償（間接的な被害）	\0	\0	\0	\0
01 インシデント被害額	\77,434,000	\2,220,000	\18,600,000	\2,816,000
実被害額	\60,000,000	\2,310,000	\19,500,000	\3,116,000
潜在化被害	\56,870,000	\450,000	\4,500,000	\2,700,000
表面化被害	\3,130,000	\1,860,000	\15,000,000	\416,000
モデルと実申請被害額との差	\17,434,000	\-90,000	\-900,000	\-300,000
率	1.29	0.96	0.95	0.90

IT感応度

＝（IT化による業務効率化係数:α）×（IT化の危険度対策係数:β）



7. 今後の課題

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

- 実際の算出業務を行う場合、現実に数値を算出しにくいもの有り。
- 「IT感応度」は、今回提案した新しい概念であり、システムの導入状況や業種によって企業毎に大きく異なる。
- メールやデータ作成などの一般事務処理を行う社内LANなどでは、減少した業務量の把握は非常に難しいと考える。
- 「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。
- 業種や業態、システム導入状況別に、「IT感応度」を評価する仕組みが必要。
- 代替え手段の効果についての評価も同様に必要。

7.2 調査の課題

7.2.1 アンケートの課題

- システム担当者周囲で発生した対応や被害の回答がほとんど。
- 被害を金額化して回答を頂くことは非常に難しい。(→モデル化を提案)
- 既存アンケートの修正利用→項目数が多過ぎた。
- アンケートは、担当の知識範囲によって回答が異なる可能性が大きい。毎年同じ担当者に定点観測できるアンケート実施も好ましい。

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が非常に少ない。
- 初調査であり、調査者のレベル合わせが十分に行えなかった。
- ヒアリング対応者も、被害の状況を十分に把握していないことが多かった。
- 事前依頼が重要であり、調査前に質問ポイントのリクエストが必要だった。
- 何分人手と時間が少なく、十分なヒアリング数をこなすことが難しかった。

8．2002年度の活動

2001年度の被害調査では与えられた時間が少なく、被害や対策費用の算出モデルを提案する段階にとどまった。今年の活動では、前年同様にアンケートやヒヤリングによる被害調査を行い、この算出モデルの精緻化を行うと共に、対策と被害発生の相関についても何らかの手がかりを掴みたい。

8.1活動内容

- 2001年度調査の課題への対応と再調査実施　実施中
- 「IT感応度」などの簡易算出方法、各種指標の整理　実施中
- 被害発生時の緊急ヒヤリング体制整備、事故情報の収集

8.2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を提案。
- リスクマネジメントの現実的な解として、このモデルの精緻化、算出ツールの開発と普及を行う。

日本国内全体の被害推計への挑戦

8.3 2002モデル

- **項目名の修正**
- **項目の追加(営業継続費用、喪失情報資産、機会損失、ブランド価値の低下)**

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)

8.4アンケート ＆ヒヤリング実施

- **アンケート：12月**
- **ヒヤリング： 1月**

ご協力 お願いいたします。

ご協力謝礼として、JNSA作成CD-ROM を差し上げます。

D-1事故状況

	被害コード →		
1	<事故状況>		
2	発生日時	年 月 日 時間（ : ）	
3	被害システムについて		
4	被害システムの種類について(該当システムの右欄に○をお付け下さい。)		
	(1)インタネット	(4)社内専用ネットワーク	
	(2)イントラネット	(5)ＥＣ（BtoB）	
	(3)エクストラネット	(6)ＥＣ（BtoC）	
5	停止時間		時間
6	影響を受けた従業員の人数		人
7	システム停止時の業務処理量の低下割合		%
8	システムの年間売り上げ（EC関連の場合）		円
9	システムの年間収益（EC関連の場合）		円
10	被害を受けたサーバーの数		台
11	被害を受けたクライアントの数		台
12	営業継続費		円
	代替手段	<対応方法をご記入下さい>	
13	逸失利益(X%売上×停止時間、粗利を利益の逸失分等)		円
14	喪失した情報資産		円
15	機会損失(見込み利益で逸失分、売上増分の逸失など)		円
16	賠償・補償金額		円
17	その他調査出費（ブランド価値の維持費用）について