JNSA
NPO 日本ネットワークセキュリティ協会
Japan Network Security Association
Network Security Forum 2009
【A2】

セキュリティ被害調査WGの定量化アプローチ
～試行錯誤から、わかったこと～

セキュリティ被害調査WG

大谷 尚通

(株)NTTデータ

2010 年 1月27日

セキュリティ被害調査WG

JNSA

目的

- **情報セキュリティインシデントにおける被害の定量化**
- **適切な情報セキュリティに対する投資判断、投資対効果の提示**
  - 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・投資額などの実態をアンケートやヒアリングによって調査した。この調査結果をもとに**「情報セキュリティインシデントに関する被害額算出モデル」**を策定した。
  - 一年間に報道された個人情報漏えいインシデント（事件・事故）を調査・分析し、「JOモデル（JNSA Damage Operation Model for Individual Information Leak）」を用いて想定損害賠償額などを推定し、結果を報告書にまとめた。

新型インフルエンザによる
関西地域の経済損失は744億円（試算）

- 一般家庭の消費減= 720億円
  （四府県の全720万世帯 一律一万円の出費減と仮定）
- 観光関連＝50億円
- イベント中止＝100～120億円
- 休校による周辺への影響＝10億円

情報セキュリティ分野において
被害の定量化や投資対効果の
考え方をもっと普及・発展させたい

1．情報セキュリティインシデントに関する被害額算出モデル（2002～2003年）

「情報セキュリティインシデント被害額算出モデル」を使って、ウィルス被害などのインシデントの被害額を算出し、被害額と対策コストの関係を検討していた。

【参考：最新の情報インシデント被害調査結果】
「IPA 2006 年 国内における情報セキュリティ事象被害状況調査報告書」
http://www.ipa.go.jp/security/awareness/johorouei/index2.html

インシデント被害額 ＝表面化被害額 ＋ 潜在化被害額

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

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

間接被害額 ＝補償、補填、損害賠償など、間接的に生じた被害額

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
＝（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）

式が少し複雑。データが集まらない。

1．情報セキュリティインシデントに関する被害額算出モデルを振り返って

JNSA

■ 汎用的な算出式、算出精度を追及した算定式

- ✓ ウィルス感染も、不正侵入も、情報漏えいも、被害額が計算できる。
- ✓ 直接被害額（逸失利益）も、間接被害額（損害賠償）も、潜在化被害額（業務影響）も計算できる。

⇒ **複雑な式**

被害額の算出が難しい。
（長い数式に対する拒否反応!?）

被害額の算出に必要な情報が集まらない。
（そんな統計は録っていない。測り方がわからない）

被害額の算出に使用されない。
（セキュリティ技術者も、使っているかどうか・・・）

2. JOモデル：個人情報漏えい（2003年～）

JNSA

インシデント被害額 ＝ 直接被害額 ＋ 間接被害額 ＋ 潜在化被害

- 逸失利益
- 復旧に要したコスト
- 営業継続費用
- 喪失情報資産額
- 機会損失額

- 補償、補填、損害賠償など、間接的に生じた被害額

補償・損害賠償
訴訟費用

- 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、顧客イメージ

システムの規模に応じた被害額

- 算出には多くの情報が必要
- 情報（資産）が失われない
- 個人情報が漏洩しても システムは停止しない

- 報道された情報で推定可能

- インシデントの報道は、株価に現れる可能性がある

株価への影響を調査してみる

簡単な定式化を試みる
「想定損害賠償額算定式」
（誰でも使える簡単な定式化！）

実被害額　　**想定額**　　**想定額**

2. JOモデルを振り返って

JNSA

■ 簡単な算出式、誰でも使える算定式
- ✓ 個人情報の価値と個人からの損害賠償請求額の算出に特化した式
- ✓ 式の項数を極力減らし、入手が容易な情報から算出可能。

精度が高い式でも、使われなければ、意味が無い。

最初から完璧な式を求めない。被害額算出の考えを広める きっかけにしたい。

⇒ 計算できる、理解しやすい式

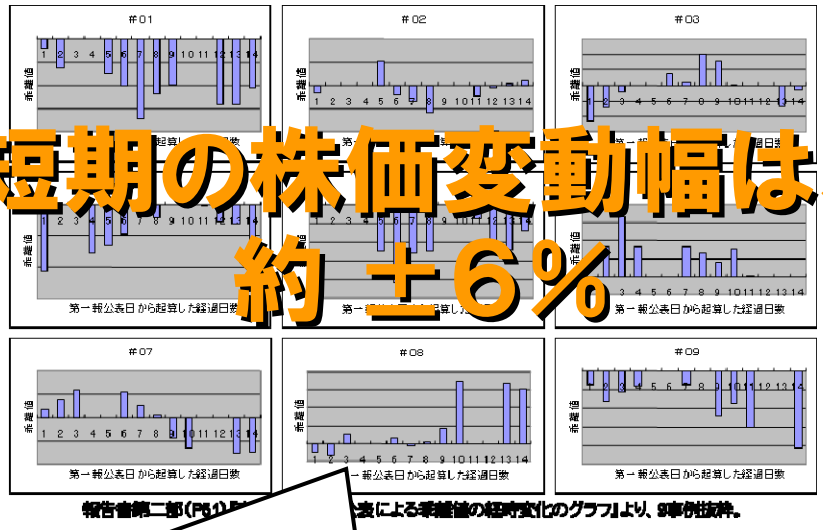
予想以上にセキュリティ非専門家も引用。
（情報セキュリティに関心のあるブロガーも、取り上げられている）

裁判事例と比較検証による精度向上(!?)
（実被害額とモデルの検証ができた）

$$500 \times (10^{x-1}+5^{y-1}) \times (6 \text{ or } 3 \text{ or } 1)$$

個人情報の価値算出の考え方を普及させた！

3. 株価影響モデル：個人情報漏えい（2003～2004年）



短期の株価変動幅は、約 ±6%

報告書第二部(P6,7)より、9事例抜粋。

- 情報漏洩インシデントの公表よりも、新製品発表などの他の報道が注目され、株価に影響する。（株価調査において、個人情報漏洩インシデント以外の影響を取り除くことができなかった。）
- 投資家は、個人情報漏洩インシデントによる一時的な影響には、反応していないかもしれない。
- 電力、ガスなど、乗り換えられない独占的な業種については、業績に対する影響が少ない。
- 銀行やクレジットカード会社など、手続きが面倒な業種についても、急激な業績の悪化は発生しない。

株価影響モデルを振り返って・・・

調査結果から、情報漏えいインシデント報道と株価変動の間に、相関する顕著な変化を見出すことができなかった。

ブランド価値、顧客イメージへの被害算出は難しかった。

一旦、終了。

4. 逸失利益・機会損失の大きさとは

インシデント被害額 ＝ 直接被害額 ＋ 間接被害額 ＋ 潜在化被害

- 逸失利益
- 復旧に要したコスト
- 営業継続費用
- 喪失情報資産額
- 機会損失額

システムの規模に応じた被害額

- 補償、補填、損害賠償など、間接的に生じた被害額

補償・損害賠償
訴訟費用

- 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、顧客イメージ

↓

被害のおよぶ範囲は、組織やシステムによってさまざま。

例）新製品情報が漏えいした場合の被害額は？
- 新製品の開発費用？
- 開発費用＋予想売上額？

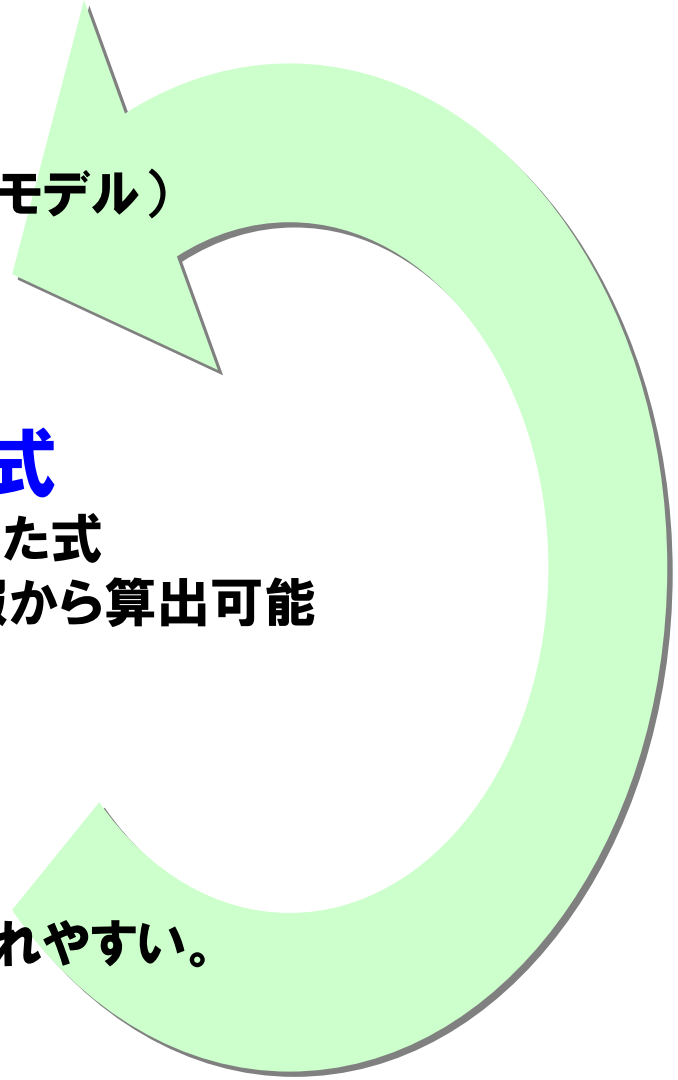
被害額が青天井になるかもしれない。

定式化は難しい。算出の考え方/方法論なら示せそう・・・。

5. セキュリティ被害調査WGの定量化アプローチ

■調査活動からのアプローチ

- ✓ 現実の現象もモデルに取り込む（経験的なモデル）
- ✓ モデル、算定式の検証・フィードバック



■簡単なモデル、誰でも使える算定式

- ✓ インシデント別・被害別などの状況に特化した式
- ✓ 式の項数を極力減らし、入手が容易な情報から算出可能

■わかりやすい定量化

- ✓ 一般的な値、検証しやすい値
- ✓ 被害額（金額）への換算が、もっとも認識されやすい。