中澤ゼミ

情報セキュリティ対策予算配分の意思決定～被害額算出とリスク分析～

a1200324　沼田雅巳

1 はじめに

インターネットの普及により，企業における情報セキュリティは今や必要不可欠なものとなっている[1]．これは企業の持つ顧客の個人情報など重要なものだからである．しかし，企業が所有する多様化し増え続ける企業情報は，きちんとした対応策をとらない限りリスクにさらされている．

このことから対応策をとり，リスクから情報を守るためにリスクが発生する原因･大きさを知らなければならない[2]．そのためにリスクを分析，被害額の算出を行い予想されるリスクを評価するのである．本研究ではこの方法に着目し，その結果から情報セキュリティ対策予算をどの情報セキュリティ事故被害に対し配分するべきかを提案する．

2 情報セキュリティ

2.1 情報セキュリティについて

情報セキュリティとは，情報資産[1]についての機密性[2]，完全性[3]，可用性[4]を維持･向上していくことである[3]．また，情報セキュリティの目的は情報資産を脅威から守り，障害･損害を最小限に抑えることである．

情報セキュリティを導入するにあたって，場当たり的な対応をとることは好ましくない[2]．場当たり的な対応では業務に支障をもたらすような不具合が生じる可能性もあり，信頼のおける基礎のできた情報セキュリティを確保するためには戦略として考える必要がある．そのためには，情報資産に対するリスクを分析し，適切な管理策を講じる必要がある[4]．

2.2 情報資産におけるリスク分析

情報セキュリティのリスク分析は，情報資産の洗い出しと評価，情報資産に対する脅威分析･評価，脆弱性分析･評価，リスク評価を行う[5][6]．これらは定量的測定[5]で評価することは難しいため，定性的測定[6]で行う[2]．

[1] 企業に関連する情報およびシステム全体の構成要素のこと
[2] 許可された者のみが情報にアクセスできること．
[3] 情報の正確性と完全性が保護されていること．
[4] 必要なとき確実に情報にアクセスできること．
[5] 金額そのもので表す測定方法
[6] 前もって用意した基準(大中小など)を用いて価値を測定する方法

2.3 情報資産の洗い出しと評価

情報資産の洗い出しでは，まず情報資産の分類から始める．一般的には狭義の情報資産[7]，ソフトウェア資産[8]，物理的資産[9]，サービス[10]の 4 項目に分類される[2]．4 項目に分類したものを，機密性，完全性，可用性の面から評価し，情報資産の価値を決定する[6] [10]．これらの評価値の合計を求め，表 1 に従って資産価値を決定する．

表 1:資産価値[2]

資産価値(合計)	概要
3(3-6)	組織の経営に大きな影響を及ぼす情報資産
2(7-12)	組織の経営に大きな影響は及ぼさないものの,業務を推進する上で大きな影響を及ぼす情報資産
1(13-15)	業務を推進する上での影響は少ないもが,組織にとって何らかの効果が期待できる情報資産

2.4 脅威分析･評価[2][6][10]

脅威とは情報システムに損害をもたらす潜在的な原因であり，脆弱性によって引き起こされる．脅威の分類として，人為的脅威と環境的脅威に分けられ，さらに人為的脅威は意図的脅威と故意的脅威に分けられる．脅威の例として，停電，ほこり，盗難，盗聴などがあり，それぞれを人為的脅威，環境的脅威に分類し脅威の大きさを表 2 のような基準に従って評価する．

表 2.脅威の評価基準の例[2]

大きさ	内容
1	発生する可能性は低い
2	中程度の可能性で発生する
3	発生する可能性が高い

2.5 脆弱性分析･評価[2][6]

脆弱性とは脅威の発生を引き起こす情報資産の弱点やセキュリティホールのことである．脆弱性そのものは障害とはならないが，脅威を浮き彫りにして損害の原因となる可能性がある．脆弱性の分類として，環境，

[7] データベース，ユーザマニュアルなど
[8] 業務用ソフトウェア，システムソフトウェア
[9] コンピュータ装置，通信装置など
[10] 通信サービス，一般ユーティリティ

ハードウェア，ソフトウェアなどに分けられる．一つの例として環境を挙げると，脆弱性は不安定な電源設備で，想定される脅威は停電である．このようにして脆弱性を分類し大きさを表3のように評価する．

表3.脆弱性評価の基準の例[2]

大きさ	内容
1	適切な管理策が講じられていて極めて安全である
2	適切な管理策が講じられていて安全だが，改善の余地についても考慮する
3	管理策の追加などにより改善の余地がある
4	想定される脅威に対して，まったく管理策が講じられていない

2.6 リスクの算出[2][10]

情報資産の洗い出し･評価，脅威分析･評価，脆弱性分析･評価の結果から情報資産の価値，脅威の大きさ，脆弱性の大きさからリスクを評価する．前出の情報資産価値，脅威評価の基準，脆弱性評価の基準の表より，それぞれの大きさを計算式に当てはめ算出する．

リスクの大きさを算出するに当たり，本研究では脆弱性がリスクの大きさに影響を及ぼすと考える．脆弱性は脅威を引き起こす原因となるため，脆弱性が存在しない場合の脆弱性評価は0であり，リスクの大きさは0になる．しかし，脆弱性が全くないということはありえないので脆弱性の評価は1からとなり，リスクの大きさに脆弱性が影響を及ぼすとしての算出式は，リスクの大きさ=(情報資産+脅威)×脆弱性，とする．

上記の算出式で求められた値を，表4の評価基準に当てはめてリスクを評価する．

表4. リスク評価の基準

リスクの分類		リスクの大きさ
許容可リスク	許容リスク	2, 3, 4
	要注意許容リスク	5, 6
許容不可リスク	優先度小リスク	8, 9, 10, 12, 15, 16
	優先度大リスク	18, 20, 24

3 被害額算出

リスク分析によって許容可リスクと許容不可リスクにわけることができた．ここでは，許容できないリスクについて実際に予想される被害額を算出する．

3.1 期待値(推定値)法[7][8]

期待値法は年間の平均的に予想される損失額を用いる方法である．一回あたりの損失をV(円)，年間の予想発生頻度をP(回)，1年当りの損失予想額をL(円/年)とすると

$$L=P\times V$$

となる．一回あたりの損失の予想される額は，直接的損失[11]，間接的損失[12]，対応費用[13]の合計である．年間の予想発生頻度を正確に算定するのは難しいが，一般的には統計や経験によるデータを参考にする．

3.2 ALE(Annual Loss Exposure)手法[7][8]

ALE手法は，ALE(円/年)=$10^{(f+i-3)}$/3 という式を用いて年間予想損出額を求めるものである．fおよびiの値は表5の通りである．

表5.ALE手法のパラメータ設定

年間発生頻度	fの値
300年に1回	1
30年に1回	2
3年に1回	3
100日に1回	4
10日に1回	5
1日に1回	6
1日に10回	7
1日に100回	8

※　コンピュータの稼働日数が3年間で1000日の時

1回当りの予想損失額	iの値
10円	1
100円	2
1,000円	3
10,000円	4
100,000円	5
100万円	6
1,000万円	7
1億円	8
10億円	9

期待値法，ALE手法ともに発生頻度に損失額を掛けて被害額を算出するという考え方は共通である．

3.3 インシデント被害額算出モデル[9]

インシデント被害額算出モデルでは，表面化被害額と潜在化被害額を求め，これらの総計でインシデント被害額を算出する．表面化被害額はインシデント被害[14]で発生する損失である．潜在化被害額はインシデント被害だが具体的な損失として表出しにくいものである．

3.3.1 表面化被害額

表面化被害額は，逸失利益とシステム復旧コストの合計である．逸失利益はシステム，ネットワークが停止しなければ得られたであろう利益額である．システム復旧コストはシステムの復旧に必要な費用[15]のことであ

[11] 事故で被った情報資産など
[12] 事故調査費用，損害賠償金など
[13] システム再構築費用など
[14] 不正アクセス，ウィルス被害など
[15] 人件費，ハードウェア･ソフトウェアの費用

る． 逸失利益は時間あたり利益にシステム停止時間を乗じたものである．時間あたり利益は，1時間あたりに換算した利益である．システム停止時間は，システムおよびネットワークの停止していた時間である．もう一方のシステム復旧コストは，システムの復旧に必要な人件費にハードウェア及びソフトウェアの費用を加算する.算出式は次の通りである.

システム復旧コスト
=システム管理部門の時間当たり人件費単価(円/人･時間)
×システム復旧所要時間(時間)
×システム復旧所要人数(人)
＋代替ハードウェア･ソフトウェア購入費(円)

ここで，システム管理部門の時間当たり人件費単価は，トラブル解消のために投入されるスタッフ一人の1時間当りの人件費単価である．システム復旧所要時間は，システム停止からシステム再開までの時間である．システム復旧所要人数は，トラブル解消のために投入されるスタッフの人数であり，ここまでで人件費を算出している．代替ハードウェア･ソフトウェア購入費は，システム復旧時に新たに購入しなければならなかったハードウェア･ソフトウェア購入費である.

3.3.2 潜在化被害額

潜在化被害額は，システム停止中の業務効率低下コストと復旧に係わる一般業務コストの合計である．システム停止中の業務効率低下コストはシステム停止中の人件費であり，算出式は次の通りである.

システム停止中の業務効率低下コスト
＝業務部門の時間当たり人件費単価(円/人･時間)
×システム停止時間(時間)
×インシデントによる影響を受けた人数(人)
×業務効率低下割合

業務部門の時間当たり人件費単価は，トラブルが起きた業務部門(現場)のスタッフ一人の1時間当りの人件費単価である．インシデントによる影響を受けた人数は，通常業務が困難，不可能となった業務部門(現場)スタッフ人数である．業務効率低下割合は業務をIT依存業務と非依存業務に分けたとき，依存業務は業務を継続するが効率は低下する（通常時効率を A とし，効率が低下しているときを B とすると B<A となる）．非 IT 依存業務はシステムと無関係であり，業務効率は変わらない(C とする).

業務全体の IT 依存割合をαとすれば，

通常時業務効率＝A×α＋C×(1-α)　(1)

インシデント発生時効率＝B×α＋C×(1-α)　(2)

となる.

業務効率低下比率は，通常時業務効率に対するインシデント発生時業務効率低下分である.

業務効率の低下比率

$$= \frac{\text{通常業務効率} - \text{インシデント発生時業務効率}}{\text{通常業務効率}}$$

と表せる．先ほどの(1)と(2)の式より，

業務効率低下比率

$$= \frac{A\times\alpha - B\times\alpha}{\{A\times\alpha + C\times(1-\alpha)\}} \qquad (3)$$

ここで求めたいものは，通常時業務効率がインシデント発生時にどの程度低下するかの割合である．通常時業務効率を 1(=100%)とおくと，(3)式より

業務効率低下比率＝α×(A－B)

となる.

復旧に係わる一般業務コスト
＝業務部門の時間当たり人件費単価(円/人･時間)
×業務復旧所要時間(時間)
×インシデントによる影響を受けた人数(人)

業務復旧所要時間は，システム停止に係わる復旧作業開始からシステムの完全正常化までの時間である.

特に 4.3 のモデルは事前に用意する項目が多いが，算出されたものは部門別に具体的な被害額を知ることが可能である.

4 予算配分の決定[11][12]

これまでリスク分析，被害額算出によって予想される被害を見積もった．ここでは，その結果から投資対効果と被害の種類により，予算を配分する方法を提案する.

4.1 投資対効果を利用する[13][14]

投資対効果を算出しそれをもとにして予算の配分を決定する方法である．表 6 のような例を挙げて説明する.

表 6：被害と対策の例

被害	被害額	頻度	期待値	対策費	頻度減少率
A	100 万円	30%	30 万円	20 万円	70%
B	100 万円	40%	40 万円	10 万円	20%
C	1，000 万円	3%	30 万円	20 万円	70%

まず，対策をとったときに頻度が減少したときの値を求める．被害Aの場合，30%の頻度で起こっている被害が 70%減少するという意味であり，計算すると 30%×(100%-70%)=9%となる[16]．同様に被害B，Cについてもそ

[16] 0.3×0.3=0.09，0.4×0.8=0.32，0.03×0.3=0.009

れぞれ 32%, 0.9%となる. 次に被害額に減少した頻度を乗じて期待値を求める. 被害Aは 100 万円×9%=90,000 円となり, B, Cはそれぞれ 320,000 円, 90,000 円となる. 次にもともとの期待値から先ほどの期待値を引く. 被害Aは 30 万円-9 万円=21 万円, 同様にしてBは8万円, Cは21万円となる. 最後に効果を算出するために先ほどの差額から対策費を引く. 被害Aの差額は 21 万円, そこから被害Aに対する対策は 20 万円を引いて 1 万円となる. Bは-2 万円, Cは 1 万円となる. また, 比でみた場合は次の通りになりA, B, Cそれぞれ, 21/20=1.05, 8/10=0.8, 21/20=1.05 となる. これらの値が, 情報セキュリティに対する投資の効果である.

ここで問題となるのが被害 A と被害 C の投資対効果が同じになってしまうことである. そこで, 被害 A をウィルス被害, 被害 B をユーザの操作ミス, 被害 C を災害事故であるとする. 先ほど被害 A と C が同じ投資対効果になっていたが, 被害の種類が違うものであることを考慮に入れる.

ウィルス被害と災害事故を比較して検討すると, ウィルス被害は一回の被害額は少ないが, 頻度としては比較的高いことが分かる. それに対し災害事故は一回あたりの額は大きいが頻度としてはかなり低いと言える. ウィルス被害はウィルスに感染してしまった場合, 被害者にも加害者にもなってしまう恐れがある. これは, 感染することでデータが破壊されてしまったり, ウィルスを誰かに感染させてしまう可能性があるからである. それに対し災害事故は, 主に被害者であることが多い. 地震や水害など防ぎようのない場合がある. これらを比較し, 被害の種類を考慮すれば対策を施しても防ぎようのないことがあるものよりも, 対策を施すことである程度の効果がみられるものの違いがわかる. ここでは, ウィルス被害は防ぐことができるもので, 災害事故を防ぎようのないものと考えれば, 投資対効果は同じであってもウィルス被害に対し予算を優先的にとればよいと言える.

5 おわりに

コストを削減し, 利潤を追求する企業にとって情報セキュリティ対策に予算を割くことは, マイナスなイメージを抱くのではないだろうか. それは目に見えた効果が得られるわけではなく, 保険的な意味合いで捉えているからである. また予算配分の決定において, 予想される被害に対し対策をとれば対策をとっただけの効果を得ることができるのかが分からないことも原因の一つであるといえる.

しかし, 期待値や被害額だけで判断するのではなく本研究で提案したように被害の種類を十分に把握し, どの種類の被害が対策をとったときに投資対効果を得られるかを判断することが可能となるであろう. 信頼のおけるセキュリティ対策をとることで顧客の信頼を得ることができるのであれば, それこそが利潤になるのではないだろうか.

参考文献･参考資料

[1]佐藤義孝, 内山亮二, 岸井智, 沼本尚明, 木暮淳一, 太田稔, “どのくらいかかる？情報セキュリティ投資”, COMPUTER&NETWORK LAN, 第21号, 11号, pp.13-37, 2003

[2]中野明 (株)コミュニケーションデザインネットワークス,『図解入門よくわかる最新ISMSVer.2の基本と仕組み』, 秀和システム, 2003

[3]http://www.gfocus.co.jp/information/column/column05.html , ［コラム］情報セキュリティはなぜ必要か, グローバルフォーカス株式会社

[4]http://www.isms.jipdec.jp/doc/JIP-ISMS113-10.pdf, 情報セキュリティマネジメントシステム(ISMS)適合性評価制度, 財団法人日本情報処理開発協会 ISMS 制度推進室

[5]http://www.atmarkit.co.jp/fsecurity/rensai/isms_sbs03/isms_sbs01.html, @IT:【実録】ISMS 構築･運用ステップ･バイ･ステップ(3), @IT-アットマーク･アイティ

[6]千葉昌幸, 松本正雄, “情報資産分布を活用したセキュリティ対策実施計画モデルの提案”, 電子情報通信学会, 信学技報, SWIM 2001-5

[7]http://melma.com/mag/96/m00049296/a00000010.html , ISO 塾！情報セキュリティ･コースーISO 塾！NO. 8「リスク分析4」, 日本最大級メルマガポータルサイト melma!［メルマ！］

[8]宇佐美博, “リスク分析とセキュリティ対策について”, 日本オペレーションズ･リサーチ学会

[9]http://www.ipa.go.jp/security/fy14/reports/current/2002-calc-model.pdf , 2002-calc-model.pdf, 独立行政法人情報処理推進機構

[10]相戸浩志,『図解入門よくわかる最新情報セキュリティ技術の基本と仕組み情報セキュリティエンジニアリングの基礎』, 秀和システム, 2003

[11]大村平,『戦略ゲームのはなし』, 株式会社 日科技連出版社,1990

[12]多田洋介,『行動経済学入門』, 日本経済新聞社, 2003

[13]http://www.ciojp.com/contents/?id=00001329;t=24, セキュリティ対策の ROI を測る, セキュリティ管理(CSO)-CIO Online

[14] http://www.ciojp.com/contents/?id=00001593;t=24,「数字」がセキュリティ投資を正当化する, セキュリティ管理(CSO)-CIO Online