

# セキュリティ経営の 近未来予測

NTTデータのセキュリティビジネスユニットは、国内初のBS7799認証を取得するなど積極的にセキュリティ事業を推し進めている。同社では多くの経験を踏まえ、セキュリティ投資について、企業の経営者の立場として考慮しなければならない視点やポイントと、ROSI (Return On Security Investment) というキーワードで投資効果の把握が重要だという。同社が啓蒙するセキュリティ施策のポイントを伺った。



株式会社NTTデータ ビジネス開発事業本部  
セキュリティビジネスユニット長  
遠藤 宏氏

## バランスのとれた セキュリティ対策の実施と指針

昨今の企業における情報セキュリティ投資は、個人情報保護対策を含み膨らむ一方である。しかしセキュリティ投資は、青天井ではいけない。組織的、システムの、物理的の3つの観点でバランスのとれたセキュリティ対策の実施が重要だ。

## 人技一体の セキュリティ対策の重要性

技術を使いこなせる運用技術とその技術者が重要である。セキュリティ人材は不足気味であり、セキュリティに手厚く人手をかけたサービスは他社との差異化要素になる。

人技一体となった手厚いサービスによって、お客様の信頼を得ることができる。

## 効果的なセキュリティ投資

セキュリティは企業にとって必要な別枠投資という考え方もあったが、最近の経営層はセキュリティ投資に関する懐疑心が生まれ、特に箱物セキュリティ投資を厳しい目で見始めた。どれ

だけの投資を行うべきか、またそれでバランスが取れているか、説明がされない、なかなか投資判断がしにくい。そこでセキュリティ投資についての判断の尺度が必要となってきた。

## セキュリティ投資効果の把握

目標達成度評価レベルを設定し、  
定量化された監査結果を導出

NTTデータでは、セキュリティ自己診断やセキュリティ・ポリシーアセスメントなどの施策を行う際に、目標達成度についてできるだけ定量的な要素を入れようとしている。

ROSI (Return On Security Investment) による効果の把握

CRMやERPなどエンタープライズアプリケーションでは、必然的に、ROI (投資対効果) の説明を定量的に求められる。この場合の投資効果は、業務効率化や売上拡大といったものになる。セキュリティ投資は、リスク削減のために行うので、その投資効果 (ROSI) は、次の式で表される。

$$ROSI = \frac{\text{情報セキュリティリスク削減額}}{\text{情報セキュリティ対策投資額}} \times 100\%$$

ROSIの式を定量化するには、セキュリティリスクそのものの定量化が必要となる。リスクの定量化は、ある事象が起こった場合の金銭的な損害に、その発生確率を掛けたものとして求めることができる。

## リスク定量化

(ある脅威による損害額 × その  
損害の発生確率)

損害の発生確率は、それを引き起こす原因となる脅威の発生確率と、その脅威に対する備えとも言うべき、管理策のレベルとの掛けあわせで決まる。

## 損害の発生確率

脅威の発生確率とそれに対する  
管理レベルによって決まる

万一、個人情報漏洩してしまった場合に、「いち早く原因を突き止め、被害者を特定し、誠意を以って謝罪し、被害者への賠償案の提示と再発の防止のために、根本的な是正計画を提示した」という合格点の事件対応の場合は、その後、二次的に発生するリスクは低く抑えられる傾向にある。

しかし、十分な対応が実施できない場合では、二次的に発生するリス

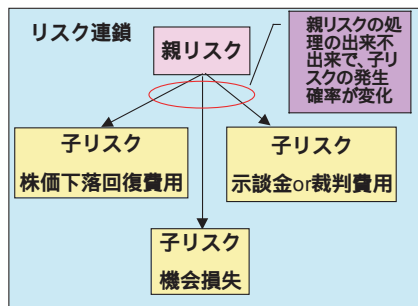


図1 リスク連鎖

クが増加してしまう。「リスク」は連鎖しており、リスクへの対処の仕方いかんでは、その後に発生するリスクは大きくなる（図1参照）。

図2は、個人情報漏洩が発生した場合に、直接的に被害の構成をイメージ化したものである。事件発生の検知が遅れると、その分影響範囲が拡大し、連動して、影響調査費用もアップする。一方、損害額にその発生確率を掛けると「リスク」となる。発生確率（一定期間の発生頻度）の求め方は、複雑だが、インターネットからの脅威の場合では、低い確率で起こる事象が、非常に大きい試行回数が互いに独立して起きるため、発生頻度の分布はポアソン分布として考えることができる。

例えば、「セキュリティ対策前のリスク額」が2.4億円、「セキュリティ対策後のリスク額」が0.3億円と求まったとしよう。仮に「セキュリティ対策投資」が3000万円とすると、ROSIは次式のように求まる。この場合700%であるので、投資は有効であると評価できる。

$$ROSI = \frac{2.4\text{億円} - 0.3\text{億円}}{3000\text{万円}} \times 100\% = 700\%$$

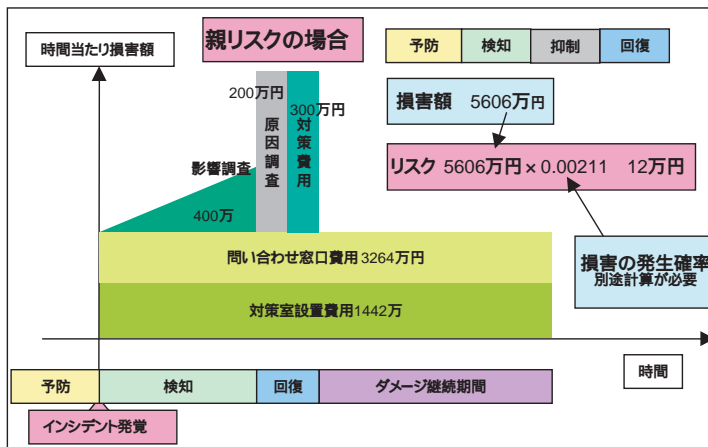


図2 損害額構成イメージ

### 今後求められる セキュリティ技術・サービス

NTTデータでは、今後次のような技術・サービスに期待が高まると考えている。

**DRM ( Digital Rights Management )**  
一般にはデジタル著作権管理技術だが、情報保護技術という意味でも使われるようになった。情報漏洩対策の中でもキーになる技術である。

**Forensic**  
キャプチャしたデータから不正アクセスや情報漏洩の痕跡を探す概念で、悪意を持った不正行為に対して係争する場合に備えるもの。タイムスタンプ技術との組み合わせにより証拠性を担保できる。

**セキュリティ保険**  
情報漏洩した場合の賠償被害リスク、費用被害リスクなどをカバーする損害保険商品。

**Open Sourceセキュリティ**  
オープンソースソフトウェアを利用する場合のセキュリティについて

は、まだ検討が始まった段階であるが、今後の期待度は高い。

#### DBセキュリティ

ネットワークセキュリティ対策が済み、内部者犯行対策が進むと最後は本丸のデータベースが残る。

メインフレームシステムのデータベース、またはクライアント・サーバシステムの基幹系データベースへのアクセスを分析し、不審な行為を探し出して対策を打つという技術が必要となる。

#### 戦略的なIT投資のために

自社の価値を高める戦略的なIT投資の実現のため、TCO削減とROSIのバランスを取り、万全なシステム構築をしていただきたい。

#### お問い合わせ先

(株)NTTデータ  
ビジネス開発事業本部  
セキュリティビジネスユニット  
TEL:03-3524-2851  
Mail:grsecure@kits.nttdata.co.jp