

セキュリティ対策案選択問題に対するフォールトツリー解析の応用

山本 貴則[†] 石橋 勇人[†]
安倍 広多[†] 松浦 敏雄[†]

ネットワーク上の情報システムを安定して稼働させることへの需要が高まる中、体系的なセキュリティ対策にしたがった高品質の運用が求められている。情報システムを対象としたリスクの定量的分析手法は、セキュリティ対策を考える上で重要であるにもかかわらず、確立されたものは未だ存在しない。本研究では、フォールトツリー解析と離散最適化問題の解決により、情報システムにおいて想定されるリスクを体系的に管理し、かつ、セキュリティ対策案の選択を可能とする効果的な手法について提案する。本手法に沿ってシミュレーションをおこなった結果、特定の予算制約条件下において最善と考えられるセキュリティ対策の選択をおこなうことができることを確認した。

An Application of Fault Tree Analysis to Determine Optimal Security Measures

YAMAMOTO TAKANORI,[†] ISHIBASHI HAYATO,[†] ABE KOTA[†]
and MATSUURA TOSHIO[†]

As it is important to run network-based information systems securely and steadily, applying systematic security measures against such systems is required. While to establish quantitative analysis technique of risks against information systems is important for choosing proper security measures, such technique has not well-established so far. In this paper, we propose an effective method to systematically manage possible security risks against information systems by applying fault tree analysis. By solving combinatorial optimization problem on the resulting fault trees, it is also possible to choose proper security measures for the system. We have experimentally confirmed that our method can choose proper security measures on a sample information system under certain budget constraint.

1. はじめに

ISMS¹⁾ や ISO/IEC17799²⁾ では、情報システムを安定して稼働させるために PDCA(Plan-Do-Check-Act) サイクルに基づいたリスクマネジメントの実施が求められている。マネジメントサイクルにおいて、リスクの大きさを定量的に分析し把握することはセキュリティ上の対策を考える上で非常に重要である。

一般にそのようなリスク分析をおこなう際には、想定される脅威を挙げ、その脅威の程度と発生頻度とを元にリスクの大小を決定する必要がある。ネットワークで接続されたシステムの場合、ある脅威が他の脅威を喚起するといった脅威の依存関係が成立することが多々あり、リスクの大きさを正確に判断するには脅威の依存関係についての充分な理解がなされていなければならない。

しかしながら、情報システムを対象としたリスクの分析手法には幾つかあるが、脅威の依存関係まで考慮されているようなものは少なく、結果としてシステムの規模が大きくなるにつれ、想定される脅威を列挙し、被害の大きさを見積もるために多くの知識が必要とされることになり、誤りなく管理をおこなうことは困難なものとなりがちである。

脅威の依存関係をツリーとして表し、うまく管理しようとする手法としては、フォールトツリー解析(FTA - Fault Tree Analysis)がある。情報システムを対象にフォールトツリー解析を導入しようとする試みもなされており、織茂³⁾ や佐々木⁴⁾ による研究が挙げられる。文献 3) は情報システムのフォールトツリーを構築するための手法について論じられたものであるが、対策案を効率的に選択する手法については触れていない。文献 4) はある制約条件下において最善と考えられる対策をシミュレーションにより求めるものであるが、その対象は不正コピー問題への対策に限定されている。

[†] 大阪市立大学 大学院 創造都市研究科

Graduate School for Creative Cities, Osaka City University

2. 本研究の提案する手法

本研究では、ネットワークでつながった複数のサービスからなる情報システムを対象に、フォールトツリーおよび離散最適化問題を活用することにより、あたえられた制約条件下において効果的なセキュリティ対策を選択するための手法を提案する。

実際の手法としては、以下の手順によりおこなう。

2.1 フォールトツリーの構築

まず、分析対象となる情報システムのフォールトツリーを構築し、脅威の依存関係についてのモデル化をおこなう。本研究では、従来の類似の研究とは異なり、情報システムの構成要素とその上で稼働する各サービスに関して、それぞれの頂点出力をもつフォールトツリーを構築し、ツリー同士を互いに連絡させて用いることとした。

情報システムに発生する障害には、その被害の範囲がある特定の枠内に閉じるものと、より広い範囲に波及するものとがある。たとえば、複数のサービスが単一のハードウェア上で提供される場合と、別個のハードウェアに分散して提供されている場合、ハードウェアに起因する問題の影響範囲は自ずと異なる。複数のフォールトツリーを組み合わせて用いると、このようない違いうまく表すことができる。

2.2 離散最適化問題の組み立て

情報システムに対するセキュリティ対策案として幾つかの候補を用意し、これら候補の中から、資産価値や投資に対する利益率を最大化するための組み合わせを選択するには、離散最適化問題を解決することでこれをおこなう。

以下、情報システムにおける効果的なセキュリティ対策案を選択するための、離散最適化問題の組み立てについて説明する。

まず、システムを構築する際の予算を C_T とする。システムを構成するための m 個のコンポーネント (DNS やファイアウォールといった要素で、これはセキュリティ対策案の選択により変動する) があるとする。それぞれのコンポーネントを構築するのに費用 $C_i (1 \leq i \leq m)$ が発生したとすると、予算に関する制約条件として、

$$\sum_{p=1}^m C_p \leq C_T \quad (1)$$

が与えられる。

商業的なシステムでは、システムを稼働しサービスを顧客に提供した結果、見返りとしてその代価が得ら

れるはずである。あるサービス j において、そのサービスが完全に機能した場合に想定される（つまり最大となる）期待収入を W_j 、障害が発生し、期待収入を得る機会が損なわれる可能性を P_j とすると、そのサービス単体での想定される収入は $W_j(1 - P_j)$ として考えることができる。システム全体として n 個のサービスが提供されている場合、この情報システムを稼働させることにより、最終的に受け取ることができると予想される収入（期待収入）の合計 I は、

$$I = \sum_{q=1}^n W_q(1 - P_q) \quad (2)$$

となる。ここで P_j の値は、情報システムの利用形態（サービス）に関するフォールトツリーを解析することにより求めることができる。

期待収入からコストを差し引いたものは期待利益 R となる。

$$R = \sum_{q=1}^n W_q(1 - P_q) - \sum_{p=1}^m C_p \quad (3)$$

投下資金に対する期待利益率 S については、

$$S = \frac{\sum_{q=1}^n W_q(1 - P_q) - \sum_{p=1}^m C_p}{\sum_{p=1}^m C_p} \quad (4)$$

としてこれを求めることができる。

また、手持ち資金を含めた期待残存資産の合計 T は、

$$T = C_T + \left(\sum_{q=1}^n W_q(1 - P_q) - \sum_{p=1}^m C_p \right) \quad (5)$$

である。

3. サンプルケース

3.1 想定するネットワーク・システム

本節では、図 1 のようなネットワーク・システムを対象に、本研究の提案する手法を用い、実際にセキュリティ対策案の選択をおこなった結果を示す。なお、情報セキュリティに関しては、人的側面、物理的側面からの視点もあるが、本サンプルケースにおいては技術的側面を主軸にリスクの分析をおこない、モデルを作成した。

このネットワーク・システムは、商用のウェブホスティングサービスを提供するために構築されるものであるとし、その詳細は以下の通りである。

- 提供されるサービスについては、「DNS ホスティングサービス」「ウェブホスティングサービス」の

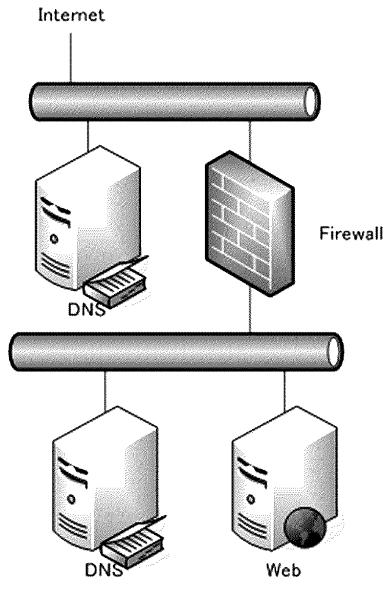


図 1 サンプルネットワークの模式図

2種類である。

- ・ウェブサーバ上ではOSとHTTPデーモンプロセスが稼働する。
- ・DNSサーバ上ではOSとDNSデーモンプロセスが稼働する。
- ・DNSのサービスを受け持つサーバ群については、権威DNSをうけもつものと、再帰問い合わせを解決するもの（再帰DNS）とに分離して設置する。また、複数のサーバによる冗長構成を取ることができる。
- ・権威DNSはファイアウォールの外側に設置する。
- ・再帰DNSはファイアウォールの内側に設置する。
- ・DNSのホスティングサービスについては、利用者のDNSメイン情報を、当該システム上の権威DNSサーバ内に格納し、ネットワーク上でのDNS問い合わせに対し、ドメインを提供できる。
- ・ウェブサーバ上のホスティングサービスについては、利用者のウェブコンテンツを、当該システム上のウェブサーバ内に格納し、ネットワーク上からのHTTP問い合わせに対し、コンテンツを提供できる。
- ・利用者がウェブサーバにウェブコンテンツを格納する際には、ファイル転送サービスを用い、ネットワーク経由でこれをおこなうことができる。
- ・「ファイアウォール」については、ハードウェアと一体となった、ターンキーシステムにより実現されるものとする。中身については完全なプラット

クボックスであり、初期設定以外に調整する余地はない。

- ・侵入行為を迅速に検知すること目的に、幾つかのサーバに対し、ホスト型侵入検知システムを設置することができる。

3.2 フォールトツリーの構築

3.2.1 全体構成のフォールトツリー

分析をおこなうにあたり、まずこのネットワーク・システムのフォールトツリーを書く。本システムは、大きく分けて「ファイアウォール」「DNS」「ウェブサービス」の要素から構成されると考えることができる。それぞれの構成要素に関し、その可用性に関する依存関係を大局的に分析した結果、図2に示すような内容のフォールトツリーを得た。

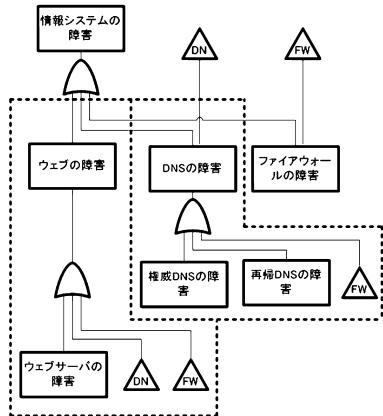


図 2 全体構成のフォールトツリー

3.2.2 障害発生までのモデル

情報システムは多くの場合、同種または異種の実装を組み合わせることにより構築される。

それら実装にセキュリティ上の理由から障害が発生するメカニズムをモデル化するにあたっては、いくつもの方法が考えられるが、本サンプルとしては、比較的簡素なものとして、

- (1) その実装にセキュリティホールが存在し、かつ、
- (2) その実装をターゲットとした不正侵入の試みがなされ、かつ、
- (3) 不正侵入の試みに気づかなかった場合

に障害が発生するものとした。もちろん、必要に応じて、より詳細なモデル化をおこなうことは自由であり、技術的に何らかの制約があるわけではない。

3.2.3 脆弱性のデータベース

実装それぞれごとに、脆弱性（その実装にセキュリティホールがどれだけ存在しているか）の度合いは異

なるものである。本研究において使用したシミュレーション・プログラムでは、実装それぞれごとの脆弱性について、事前に知識としてデータベースに貯めておいたものを、必要に応じて参照し、フォールトツリーにコピーして用いることができるような仕組みをとっている。

3.2.4 ファイアウォールのフォールトツリー

ファイアウォールによって、ウェブサーバや再帰DNSが設置されたネットワーク（内部ネットワークまたはサーバ・セグメント）をファイアウォールによって外部ネットワークから分離し、かつ、両ネットワーク間の通信をチェックすることで、外部ネットワークから内部ネットワーク上のサーバに対する侵入行為などを未然に防止することができる。

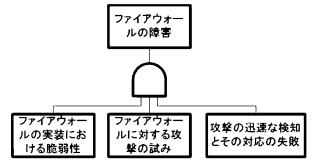


図 3 ファイアウォールのフォールトツリー

ファイアウォールを設置するにあたっては、その選択案として、

- (0) 「単なる L3 ルータ」
 - (1) 「簡単なアクセス制限とステートフルインスペクション機能を有するもの」
 - (2) 「上記に加え、セッション数制限とパケットのセーニング機能を有し、サーバへの DoS 攻撃などを抑制できる機能を備えるもの」
 - (3) 「上記に加え、アプリケーションレイヤの情報内容のチェック機能を有し、バッファオーバーフロー攻撃などを抑制できる機能を備えるもの」
- の 4 通りの選択をとりうることとする。

3.2.5 DNS のフォールトツリー

DNS のシステムはファイアウォールを跨いで、外側に権威 DNS、内側に再帰問い合わせに対応する DNS を用意することとする。

DNS は複数サーバによる冗長化が比較的容易なサービスである。ここではその選択案として、

- (0) 「権威 DNS、再帰 DNS ともに 1 台を設置」
 - (1) 「権威 DNS を 2 台、再帰 DNS を 1 台設置」
 - (2) 「権威 DNS を 1 台、再帰 DNS を 2 台設置」
 - (3) 「権威 DNS、再帰 DNS ともに 2 台を設置」
- の 4 通りの選択をとりうることとする。

DNS に関するフォールトツリーとしては、図 4 の

ようなものを想定し用いた。

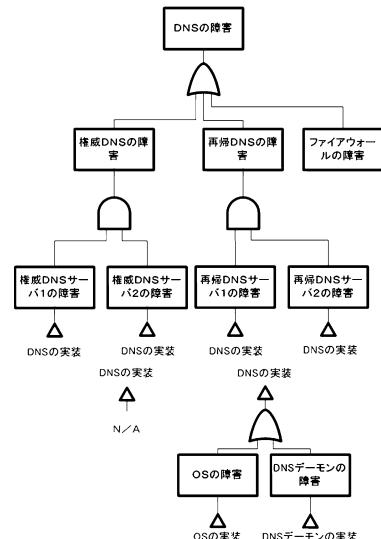


図 4 DNS のフォールトツリー

また、各 DNS サーバの実装において、それら実装が用いる OS と DNS デーモンそれぞれの障害に関しては、事前に用意したデータベースからそれら情報を参照し、フォールトツリーにサブツリーとして持ち込むことで、全体としてのツリーを生成する。ここで、データベースに格納されているサブツリーは図 5、図 6、図 7、図 8 のような構造を有する。

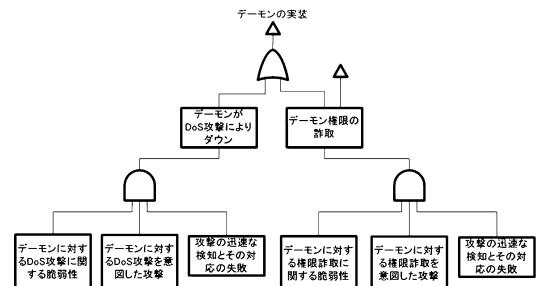


図 5 デーモンのフォールトツリー

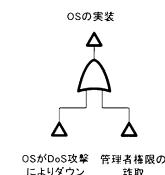


図 6 OS のフォールトツリー

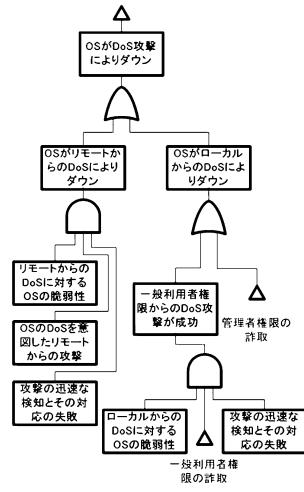


図 7 OS のフォールトツリー (DoS)

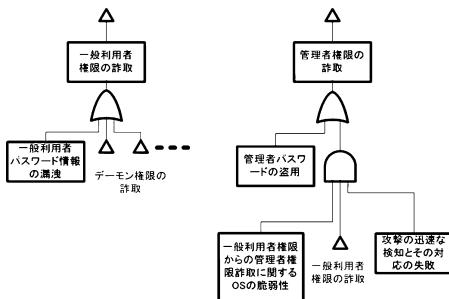


図 8 OS のフォールトツリー (権限詐取)

3.2.6 ウェブサービスのフォールトツリー

ウェブサーバ上ではファイル転送のためのデーモンが動作し、ウェブサーバ内に蓄積されたコンテンツを利用者が遠隔地から変更・設置・取得・削除できる。ここでは選択案として、

- (0) 「ウェブサーバ上でFTPデーモンを稼働させる」
- (1) 「ウェブサーバ上でSFTPデーモンを稼働させる」

の2通りの選択をとりうることとする。

ウェブサービス回りのフォールトツリーは、図9の内容とした。

3.2.7 ホスト型IDSについて

各サーバ上には、攻撃行為を検知し、管理者に通知するためのホスト型IDSを設置できるものとする。

ホスト型IDSの導入に関する選択案としては、

- (0) 「ウェブサーバ上に導入」
- (1) 「再帰DNSサーバ#1上に導入」
- (2) 「再帰DNSサーバ#2上に導入」
- (3) 「権威DNSサーバ#1上に導入」

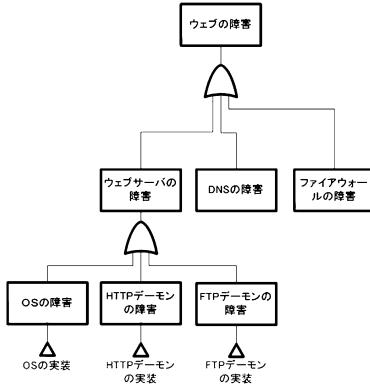


図 9 ウェブサービスのフォールトツリー

(4) 「権威 DNS サーバ#2 上に導入」

の選択をとりうることとする。選択肢の数は、最大 $2^5 = 32$ 通りである。

3.2.8 DNSホスティングサービスのフォールトツリー

顧客の所有するドメインのホスティングサービスを本システムの権威DNS上にておこなう。サービスの定性的リスク分析をおこなった結果、最終的に図10のようなフォールトツリーが作成された。

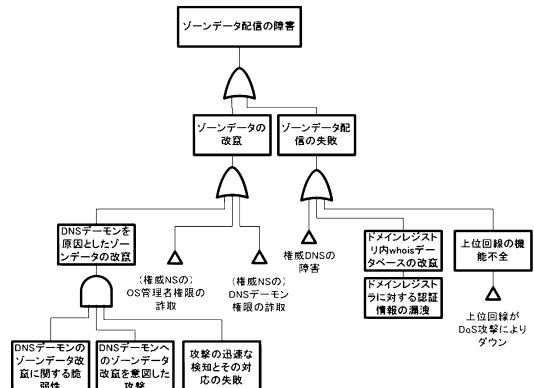


図 10 DNSホスティングサービスのフォールトツリー

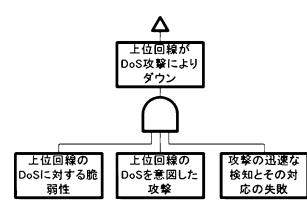


図 11 上位回線のフォールトツリー

3.2.9 ウェブホスティングサービスのフォールトツリー

本システムのウェブサーバ上において、顧客の所有するウェブコンテンツを格納し、閲覧者側の問い合わせに応じて送信する、いわゆるウェブホスティングのサービスをおこなう。サービスのフォールトツリーは図 12 の内容とする。

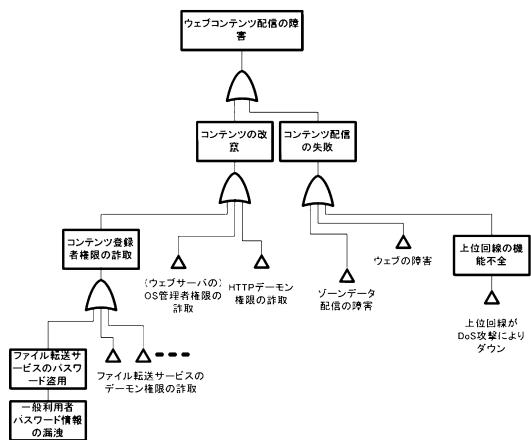


図 12 ウェブホスティングサービスのフォールトツリー

3.3 パラメータの決定

次に、必要となる各パラメータについて、具体的な数値を決定する。

3.3.1 サンプルネットワークのフォールトツリーにおける基本事象の生起確率

サンプルネットワークのフォールトツリーにおける基本事象の生起確率を定める。具体的な数値は表 1 のとおりとした。

次に、これら数値の決定理由について簡単に述べる。

- 情報システムの構成要素に対する各種攻撃の試みについては幾つかあるが、それらは全て解析対象となる期間内に必ず発生するものとし、生起確率は 1.00 とした。また、それら攻撃の検知とその対応については、一般的・日常的な管理の枠内で気づくことのできるものは少ないであろうという判断から、検知できない可能性として 0.90 を設定した。
- ファイアウォールの脆弱性については、その機能の高低により、実装自体に含まれる潜在的な脆弱性を 0.01~0.06 の幅で増減させることとした。
- 各種デーモンの DoS 攻撃に対する脆弱性については、発生する可能性は充分にあると考え、0.35 とした。DNS デーモンについては、プロトコルが

表 1 基本事象の生起確率

事象	生起確率
攻撃の試み	1.00
攻撃の迅速な検知とその対応の失敗	0.90
ファイアウォール	
タイプ 0 の脆弱性	0.01
タイプ 1 の脆弱性	0.02
タイプ 2 の脆弱性	0.05
タイプ 3 の脆弱性	0.06
DNS デーモン	
DoS に対する脆弱性	0.30
権限詐取に対する脆弱性	0.10
ゾーンデータ改竄に対する脆弱性	0.05
HTTP デーモン	
DoS に対する脆弱性	0.35
権限詐取に対する脆弱性	0.10
FTP デーモン	
DoS に対する脆弱性	0.35
権限詐取に対する脆弱性	0.10
SFTP デーモン	
DoS に対する脆弱性	0.35
権限詐取に対する脆弱性	0.05
OS	
リモートからの DoS に対する脆弱性	0.20
ローカルからの DoS に対する脆弱性	0.30
一般利用者権限からの管理者権限詐取に関する OS の脆弱性	0.10
上位回線	
上位回線の DoS に対する脆弱性	0.05
管理者パスワードの盗用	0.01
一般利用者パスワード情報の漏洩	0.90
ドメインレジストラに対する認証情報の漏洩	0.01

コネクションレス型である点などを考慮し、0.30 とした。デーモンの権限詐取に対する脆弱性については、まれに起こるものと考え、0.10 とした。SFTP デーモンについては、特段の対策がなされていると判断し、0.05 とした。DNS ゾーンデータが、権限詐取されることなく改竄される可能性については、再帰 DNS と権威 DNS を分離し、また、権威 DNS 間でのゾーン転送にも特段の注意を払うようにすることで、ほぼ起りえないと考え、0.05 とした。

- OS 自体がリモートから DoS を受け得る可能性については、ブルートフォース的に発生しうるものであると考え、0.20 とした。ローカルから DoS 攻撃を受けた場合については、より影響を受けやすいと考え、0.30 とした。一般利用者権限からの管理者権限詐取については、有り得ないことではないので、0.10 とした。
- 上位回線は充分なものが用意できるとし、DoS にたいする脆弱性は 0.05 とした。
- 管理者パスワードは厳重に管理されることとし、

盗用の可能性は 0.01 とした。一般利用者のパスワード情報については、ファイル転送サービスにおいて平文で電送される可能性のあることから、漏洩の可能性は極めて高いものとし、0.90 とした。ドメインレジストラに対する認証情報については、管理を徹底することとし、盗用の可能性は 0.01 とした。

3.3.2 対策による生起確率の低減

システムを構成する際にとりうる選択の中には、セキュリティ対策となるものが含まれており、基本事象の生起確率を低減する働きをするものがある。表 2 に、セキュリティ対策とその対象となる事象、およびその事象の生起確率を低減できる率について示す。

表 2 対策とそれによる基本事象の生起確率低減率

対策と対象	低減率
ファイアウォール（タイプ 1）の導入	
再帰 DNS への攻撃抑制	0.90
ファイアウォール（タイプ 2）の導入（タイプ 1 に加え）	
再帰 DNS への DoS 攻撃抑制	0.80
ウェブサーバへの DoS 攻撃抑制	0.80
ファイアウォール（タイプ 3）の導入（タイプ 2 に加え）	
再帰 DNS への権限詐取攻撃抑制	0.80
ウェブサーバへの権限詐取攻撃抑制	0.80
SFTP デーモンの導入	
利用者のパスワード情報漏洩	0.99
ホスト型 IDS の導入	
検知失敗の抑制	0.80

3.3.3 コスト

情報システムを構成するための各構成要素について、それぞれを導入する場合に要するコストを表 3 のように定めた。このパラメータは、物品の購入にかかるインシャルコストと、維持管理・保守に要するランニングコストとの合算からなるものとする。

表 3 構成要素の導入コスト

構成要素	単価
ファイアウォール（タイプ 0）	400,000
ファイアウォール（タイプ 1）	500,000
ファイアウォール（タイプ 2）	1,100,000
ファイアウォール（タイプ 3）	2,000,000
DNS サーバ	800,000
ウェブサーバ	1,500,000
SFTP（全顧客へ配布する クライアントソフト一式）	7,800,000
ホスト型 IDS	1,500,000

3.3.4 予算額

予算額については、いくつかの予算制約下でシミュ

レーションをおこなうこととした。

3.3.5 最大期待収益

各サービスを提供することによる最大期待収益については、サービスの提供期間と顧客数、および客単価の見込みから、表 4 のように想定した。

表 4 最大期待収益

提供するサービス	最大期待収益
DNS ホスティングサービス	60,000,000
ウェブホスティングサービス	200,000,000

3.4 結 果

予算制約条件を 400 万～2200 万までとし、200 万づつ間隔をあけながら、とりうるセキュリティ対策案の全ての組み合わせの中から、残存資産ならびに投資効率のそれぞれについて、各予算制約の下で最大となる値が得られるものをシミュレーションにより求めた。なお、シミュレーションのためには専用のプログラムを開発し用いた。

その結果、残存資産を最大化する解は表 5 のとおりであった。同様に、投資効率を最大化する解は表 6 に示すものとなった。なお、表中、ファイアウォール/DNS/FTP の各選択については、3.2.4 節、3.2.5 節、3.2.6 節の選択番号と一致している。IDS の選択における記号は、「A1 = 権威 DNS サーバの 1 台目」「A2 = 権威 DNS サーバの 2 台目」「W = ウェブサーバ」をあらわし、ホスト型 IDS を該当サーバに導入することを意味する。

3.4.1 残存資産を最大化する場合

設備投資額は 1810 万で上限となり、たとえ予算が潤沢にあつた場合でもファイアウォールタイプ 3 の導入はおこなわれていない。これは、その対策の効果と、必要となる経費とが釣り合わないと判断されたためである。

予算が 1200 万を超えると、FTP が SFTP へと切り替わり、その際に DNS の冗長性が逆行している。これは、DNS の冗長性よりも SFTP 導入のほうがメリットがあると判断され、顧客へ配布する SFTP クライアントの費用を負担できるだけの予算があれば、そちらを優先しようと判断されたためと考えられる。

設備投資額が大きくなるにつれ、期待収入も大きなものとなる傾向にあるが、期待利益率については必ずしも追従するものではなく、1600 万付近で（実際には 1500 万の時点で）最大となり、あとは下降する。収入の最大化と利益率の最大化とは、必ずしも一致するものではないことがわかる。

表 5 残存資産を最大化する解

予算制約	選択				設備投資額	期待収入	期待利益率
	FW	DNS	FTP	IDS			
4,000,000	1	0	0	-	3,600,000	21,266,032.2	4.9
6,000,000	2	0	0	A1	5,700,000	48,829,038.0	7.6
8,000,000	2	2	0	A1/W	8,000,000	54,564,382.0	5.8
10,000,000	1	3	0	A1/A2/W	9,700,000	59,357,277.1	5.1
12,000,000	2	0	1	-	12,000,000	83,009,258.5	5.9
14,000,000	2	0	1	A1	13,500,000	136,821,752.4	9.1
16,000,000	2	2	1	A1/W	15,800,000	179,076,350.9	10.3
18,000,000	2	1	1	A1/A2/W	17,300,000	184,995,229.4	9.7
20,000,000	2	3	1	A1/A2/W	18,100,000	190,990,233.7	9.6
22,000,000	2	3	1	A1/A2/W	18,100,000	190,990,233.7	9.6

表 6 投資効率を最大化する解

予算制約	選択				設備投資額	期待収入	期待利益率
	FW	DNS	FTP	IDS			
4,000,000	0	0	0	-	3,500,000	20,871,070.8	5.0
6,000,000	0	0	0	A1	5,000,000	46,164,151.5	8.2
8,000,000	0	0	0	A1	5,000,000	46,164,151.5	8.2
10,000,000	0	0	0	A1	5,000,000	46,164,151.5	8.2
12,000,000	0	0	0	A1	5,000,000	46,164,151.5	8.2
14,000,000	2	0	1	A1	13,500,000	136,821,752.4	9.1
16,000,000	2	0	1	A1/W	15,000,000	173,455,312.2	10.6
18,000,000	2	0	1	A1/W	15,000,000	173,455,312.2	10.6
20,000,000	2	0	1	A1/W	15,000,000	173,455,312.2	10.6
22,000,000	2	0	1	A1/W	15,000,000	173,455,312.2	10.6

3.4.2 投資効率を最大化する場合

設備投資額は 1500 万を超えると、それ以上投資されなくなる。効果的な対策案が残っていないと判断されたためであろう。

予算 400 万の際には、投資効率を最大化するために「何もしない」という対策が採られ得ることが判る。

残存資産を最大化する場合と比較して、選択肢の変動が少ない。これは、極力少ない出費で最大の効率を得られる対策を実施しようと、効率的な選択に集中したためであろう。

4. おわりに

以上のことから、本手法によって情報システムに対するセキュリティ対策の選択を、フォールトツリーに記述された内容を元として、データ駆動的におこなうことができることを確認した。

しかしながら、本手法には依然以下のようない課題が残っており、これらについては今後改善していくねばならないと考える。

まず、基本事象の生起確率の決定根拠が不十分であり、より正確な値を算定・入力できるようにする必要がある。これについては、実際の運用からのデータを収集し、そのフィードバックによって、経験的により確からしい数値へと近づけていくのではないかと考

える。

また、取りうる選択肢が増えるにつれ、最適な結果が得られる解を厳密に算出するための計算コストが跳ね上がってしまう問題が認められる。現在のプログラムでは総当たり法によって厳密解を見つけるようにしているが、より大規模な問題を対象にする場合には、近似解を求めるようにして、処理の高速化について考慮すべきであろう。

参考文献

- 1) "情報セキュリティマネジメントシステム適合性評価制度 ISMS 認証基準 (Ver.2.0)", 財団法人日本情報処理開発協会, 2003.
- 2) "TR X 5080 (ISO/IEC 17799) 情報技術 - 情報セキュリティマネジメントの実践のための規範", 財団法人日本規格協会, 2002.
- 3) 織茂昌之 津原進 山本倫子 佐々木良一, "情報システムにおけるセキュリティ対策立案のための計画手法", 情報処理学会論文誌 Vol.41, No.1, 2000.
- 4) 佐々木良一 吉浦裕 伊藤信治, "不正コピー対策の最適組み合わせに関する考察", 情報処理学会論文誌 Vol.43, No.8, 2002.