情報処理学会論文誌 Vol.59 No.3 1082–1094 (Mar. 2018)

イベントツリーとディフェンスツリーを併用した標的型攻撃に対するリスク分析手法の提案と適用

相原 遼[1,a)] 石井 亮平[1] 佐々木 良一[1]

受付日 2017年5月29日, 採録日 2017年12月8日

概要：近年，標的型攻撃による被害が増加傾向にある．標的型攻撃では，種々の攻撃を巧妙に組み合わせるためにそれを防ぐことが難しいといわれている．一方で標的型攻撃の研究や調査が進んだことで，リスクを低減できるいろいろな対策が提言されている．しかし，実際にはすべての対策を行うことはコストの面で不可能であり，残存リスクとコストを考慮した対策の選定が必要となる．このため標的型攻撃の特徴である種々の攻撃からなる多様な攻撃シーケンスの記述に適したイベントツリー分析法に加えて，各対策案の効果を記述しやすいディフェンスツリー分析法を考案した．そしてそれらを併用し対策案の最適な組合せを求められる EDC 手法を開発した．あわせて，どの程度のコストをかけて対策を実施すべきかを判断しやすくする可視化の方法を提案した．本論文では EDC 手法と可視化の方法を提案するとともに，それを大学の情報システムに対して実際に適用することによって得られた知見を記述する．

キーワード：標的型攻撃，イベントツリー，ディフェンスツリー，IT リスク

Proposal and Application of Event Tree and Defense Tree Combined Method for Risk Analysis against Targeted Attacks

Ryo Aihara[1,a)] Ryohei Ishii[1] Ryoichi Sasaki[1]

Received: May 29, 2017, Accepted: December 8, 2017

Abstract: In recent years, number of damages due to targeted attacks has been increasing. Based on evidences from many known incidents, establishing powerful protections against such attacks is difficult because of different techniques skillfully combined by the intruders. Despite the numerous leading studies which proposed measures aiming to decrease the risks, it is practically impossible to implement all measures due to the costs associated with their developments. Measures to be implemented must be selected for practical reasons, carefully considering costs and residential risks. In order to establish effective methods for making practical selections, this study adopted Event tree analysis for determining attack sequences, hence the characteristics, and the revised Defense tree analysis for evaluating the effectiveness of measures taken. This paper proposes the EDC method which in simple terms is the Event Tree analysis and Defense tree analysis combined. In addition, we developed a visualization method that makes it easier to decide how much cost to implement measures. In this paper, we propose EDC method and visualization method, and describe knowledge obtained by actually applying it to university information system.

Keywords: targeted attack, event tree, defense tree, IT risk

1. はじめに

サイバー空間のリスクの増大にともない，リスク評価を行い，対策案の最適な組合せを求めることの必要性が高まっている．このような問題に対処するため従来はフォルトツリー分析法 [1] やアタックツリー分析法 [2] に基づきリスクの評価を行ったうえで対策案の組合せを決定することが多かった．

近年，標的型攻撃による被害が増加傾向にある．このよ

[1] 東京電機大学
Tokyo Denki University, Adachi, Tokyo 120–8551, Japan
[a)] 16fumi01@ms.dendai.ac.jp

うな状況に対処しようとすると次のような 2 つの問題があった．

（問題 1） 標的型攻撃では各段階の攻撃の成功・失敗によって様々な攻撃シーケンスが存在する．これらのシーケンスをディフェンスツリーの最上位項目として表すと，アタックツリーは単一の事象に対して分析するものであるので 1 つ 1 つは非常に大きなツリーになるとともに，シーケンスの数だけこれらのツリーを作る必要が生じ，膨大な作業が必要となること．

（問題 2） 種々の対策の組合せを求める必要があり，多くのコストを要するがどこまで対策を実施すればよいかが分からず，経営者にとって大きな問題であった．

（問題 1）に対し，イベントツリー [3] を用いると，考えるべき攻撃シーケンスが右側に枝の形で分かりやすく表現でき，それらのシーケンスの発生確率と影響の大きさを与え，その積をとることで，シーケンスごとのリスクが容易に計算可能である．また，各段階の攻撃の成功失敗は，段階に限定したアタックツリーを記述すればよいので，比較的小さなアタックツリーの展開で済む．このためイベントツリーとアタックツリーを組み合わせる方法は，分析がアタックツリー単独で行う方法に比べ効率的なものになっているといえる．Bistarelli ら [4] は，アタックツリーの最下位項目に対策を結び付けたディフェンスツリーを提案している．本論文で提案するディフェンスツリーとイベントツリーを組み合わせる方法は，上記の特長以外に，対策ごとのリスクの変化を容易に推定できるという特長も持っている．

イベントツリーとディフェンスツリーを組み合わせることで標的型攻撃に対する対策案の最適な組合せを求める手法を EDC（Event tree and Defense tree combined method）手法と呼ぶ．

（問題 2）に対応するためコスト制約のもとに残存リスク含むトータルリスクを最小にする対策の組合せを求めるツールを開発するとともに，各コスト制約下における残存リスクと対策コストを足したものを可視化することにより投下すべきコストを判断できるようにした．

著者らが所属する東京電機大学では，TDU-CSIRT という名の CSIRT 組織が 2016 年 8 月に設立され，大学で初めて CSIRT 協議会に加盟しており，セキュリティ問題に対応していこうと種々の活動を行っている．その一環で標的型攻撃に対する具体的対策を決定するため，著者らが開発した EDC 方式を用いて検討を行うことになった．

本論文では，EDC 手法を示すとともに EDC 手法を用いて東京電機大学を対象にリスク評価を行った結果を報告する．本提案方式はいろいろな組織で使用可能なものであり，適用結果は大学等の組織においてどういう対策の導入が望ましいのか感触を得るのに有用であると考えている．

なお，ここで報告する分析結果は，セキュリティ製品名や購入価格の秘匿の必要性から，実際に使用した分析結果を簡易化または一部を変更したものである．

2. 関連研究

セキュリティ対策の評価にフォルトツリー分析法を用いるアプローチは広く行われてきた．たとえば，加藤らの研究 [1] や柴田らの研究 [2] は最適なセキュリティ対策を選定するにあたりフォルトツリーを用いてリスク分析を行っており，対策のコスト，対策の運用性や利便性における負担，または従業員の仕事量の負担を考慮した対策選定手法を提案している．

また，Bruce Schneier がセキュリティ評価に適するようにフォルトツリー分析法を改良したアタックツリー分析法もある．このアタックツリーに対策の適用を考慮した研究を Bistarelli ら [4] や Edge ら [5] が行っている．Bistarelli らは，アタックツリーに脆弱性への対策を適用したディフェンスツリーを定義し，対策を実施することで低減するリスクと対策コストを考慮して評価する ROI（Return on Investment）と，対策を実施することで攻撃者が得る利益をどのくらい邪魔できるかを評価する ROA（Return on Attack）の 2 つの指標を用いて最適な対策を選定する手法を提案している．

また，Edge らは，構築したアタックツリーとほぼ同様の構造を持つプロテクションツリーを提案した．攻撃を達成するためにトップダウンに要因を分析するアタックツリー分析に対して，プロテクションツリー分析は防御を達成するためにどのような対策が必要となるのかをトップダウンに分析を行い，対策の成功確率と対策コスト，攻撃のリスクから最適な対策を選定している．

しかし，このアタックツリー分析法は，標的型攻撃のような時間経過によって種々の攻撃事象が組み合わされる攻撃を扱うのには向いておらず，標的型攻撃等への適用例は報告されていない．

イベントツリー分析法とフォルトツリー分析法を組み合わせた研究は，原子力プラントの安全性評価に広く使われてきた．それらを改良するものとして，Bowles ら [6] や Andrews ら [7] の研究が行われている．

イベントツリー分析法をセキュリティ対策の評価に用いたものは少ない．著者らの研究室では，藤本らの研究 [8] において，公開鍵暗号の危殆化が生じた場合について，イベントツリーを用いて様々なケースを考慮してリスク分析を行い，危殆化への最適な対策の選定を行っている．しかし，これはイベントツリー単独で用いるものであり，このままでは標的型攻撃のように多様な対策案が考えられる問題には適用できない．

したがって，標的型攻撃の分析を行っている研究はいまだ少ないせいもあり，EDC 手法のように標的型攻撃に対する対策案の最適な組合せを求める方法は我々の調査した

範囲では存在しない．

また，サイバー攻撃の対策を決定するためコスト制約のもとに残存リスクを最小にする対策の組合せを求めるとともに，各コスト制約下における残存リスクと対策コストを足したものを可視化する方式の提案は従来なかった．

3. 適用事例の最適解演算のための事前準備

3.1 EDC 手法

EDC 手法とは，イベントツリー分析とディフェンスツリー分析を併用したリスク分析であり，職種や規模，分析の対象とする標的型攻撃を定めてイベントツリー分析とディフェンスツリー分析を行い，分析結果と制約条件から最適な対策を算出することのできる手法である．EDC 手法は**表 1** に示す 7 つのステップから構成されている．

3.2 ステップ 1：対象の決定

分析にあたり，まず攻撃を受ける組織の人数や，PC・サーバ台数等の前提条件を考慮する必要がある．そのため，どのような組織を対象とするのかを決定する．

適用対象を設定して，手法の具体的な適用を行った．例としては下記のものが考えられる．

- 組織の人数
- PC およびサーバの種類や数
- ネットワーク構成
- 守る対象の設定（攻撃者が狙う情報）

3.3 ステップ 2：標的型攻撃の分析

標的型攻撃は公開サーバへの不正アクセスや，メールを利用したなりすまし攻撃等の標的を絞った攻撃手法の総称であり，様々な攻撃シーケンスが存在するが，侵入後は共通性が高い．IPA の標的型攻撃のレポート [9] を見ても，攻撃の基本的な流れが同じであることが分かる．そこで，実際に起きた標的型攻撃の事例を基に分析をすることで，攻撃の流れを具体的に把握し，詳細な分析を行う．

標的型攻撃の事例の候補はいくつかあるが，本研究では，詳細な報告書が出ている日本年金機構への攻撃を参考としている．分析の際には，報告書から読み取れる攻撃者の行動以外にも，記載はないものの行ったと予想される行動や，この事例では選択されなかった攻撃手法を予想し，分析を行うことで，標的型攻撃としてより汎用的な攻撃シーケンスを導出した．

この報告書を見ると，IPA の標的型攻撃のレポートにある攻撃シーケンスとあまり違いがないことが分かる．したがって，この攻撃シーケンスは現時点における標的型攻撃として汎用性の高いものになっていると考える．

説明用に行う攻撃も同様な手順をとるものとする．大まかな事例の流れとして，まずメールによる感染が発端となる．次に感染した端末に対して C&C サーバとの通信を確立した後に，組織内部の他端末への感染を進める．当事例の場合には，年金に関する個人情報を処理する基幹系システムとそれ以外の処理をする情報系システムに論理的に分離された状態にあったものの，業務の必要を理由に条件付きでの情報系システムの共有フォルダへの個人情報の保存が許可されており，共有フォルダから情報流出が発生した．

表 1 EDC 手法のステップ
Table 1 Steps of the EDC method.

ステップ	内容
1	対象の決定
2	標的型攻撃の分析
3	イベントツリー分析
4	ディフェンスツリー分析
5	対策案の決定
6	目的関数・制約条件の決定
7	対策案の最適組み合わせの決定

3.4 ステップ 3：イベントツリー分析

ステップ 2 の分析結果にイベントツリー分析（ETA）を適用し，標的型攻撃によって被るリスクと大まかな攻撃の流れ，また攻撃が発生したときの影響を推定する．本節におけるイベントツリーの説明は簡易化した**図 1** を用いる．

本イベントツリーの適用手順は以下のとおりである．

（ア）イベントツリー分析法は，事件/事故の引き金となる事象を初期事象と呼び，これをリストアップする．本事件は，攻撃者の目線から考えると，図 1 の左上に示すように「メール送信」が初期事象であるといえる．

（イ）初期事象が決定すると，次にイベントツリーの構造を決定する．一般的なイベントツリーの適用方法は，たとえば火災が発生した事象を初期事象に置き，それを保証する安全対策を各事象とする．しかし，EDC 手法中のイベントツリー分析は攻撃者の目線から考える

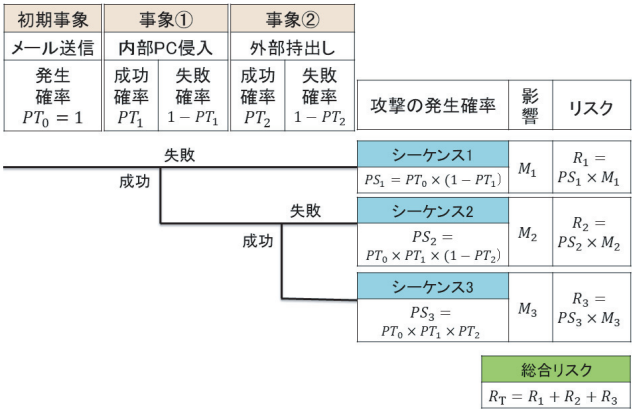

図 1 説明用イベントツリー
Fig. 1 Explanatory event tree.

ため，ステップ 2 での調査結果を基に，事件の中で行われたと思われる攻撃方法を各事象とする．また，これらの事象をヘッディング項目と呼ぶ．今回の説明用のイベントツリーでは，初期事象から「メール送信」・「内部 PC 侵入」・「外部持出し」と設定した．

（ウ）ディフェンスツリーを利用して，各ヘッディング項目の成功確率を計算する．ディフェンスツリーを利用した計算方法については後述する．続いて各事象に示された攻撃方法の成否の組合せをシーケンスとして表現し，各事象の成功確率を用いてシーケンス別の攻撃の成否確率を計算する．図 1 での各ヘッディング項目の成功確率は．「メール送信」が PT_0，「内部 PC 侵入」が PT_1，「外部持出し」が PT_2 とし，各シーケンスの発生確率は，シーケンス 1 を PS_1，シーケンス 2 を PS_2，シーケンス 3 を PS_3 とした．このとき，シーケンスの発生確率は，下記の式 (1)〜(3) で表される．

$$PS_1 = PT_0 \cdot (1 - PT_1) \tag{1}$$

$$PS_2 = PT_0 \cdot PT_1 \cdot (1 - PT_2) \tag{2}$$

$$PS_3 = PT_0 \cdot PT_1 \cdot PT_2 \tag{3}$$

（エ）イベントツリーのシーケンスごとに影響の大きさの推定を行う．影響としては，ステップ 1 で考案した項目から金額で算出する．図 1 でのシーケンス 1〜3 に対応する影響はそれぞれ M_1，M_2，M_3 とした．
対象組織が攻撃を受けた際に発生する損害額を設定する．例としては下記のものが考えられる．

- 感染した PC の復旧費用
- 信頼の低下による損失額
- 情報流出による直接的な賠償金
- 応急・事後対応費

（オ）最後に（ウ），（エ）の結果より，シーケンスごとに両者の積をとりリスクを計算する．そして，各リスクを合計することで，全体のリスク（総合リスク）を算出する．シーケンス 1 に対応するリスク R_l は以下の式 (4) で表される．

$$R_l = PS_l \cdot M_l \tag{4}$$

図 1 ではシーケンス 1〜3 に対応するリスクはそれぞれ R_1，R_2，R_3 となる．また，シーケンスが L 個のとき，シーケンス 1 から L までのリスクの和が総合リスク R_T となる．

$$R_T = \sum_{l=1}^{L} R_l \tag{5}$$

3.5 ステップ 4：ディフェンスツリー分析

前節のイベントツリーの適用手順（ウ）において，ヘッディング項目の発生確率 PT_k を求めるにあたり，標的型攻撃は各ヘッディング項目が単一の原因で発生することは希であるため，それぞれの事象の発生原因を詳細に分析する必要があると考えた．そこでイベントツリーの各ヘッディング項目に対してディフェンスツリー分析法を適用した．ディフェンスツリー分析法は，各事象の発生に至る攻撃方法，その攻撃が発生する確率，その攻撃に対する対策案を分析する手法である．イベントツリーの事象①「内部 PC 侵入」を例にとると，それに対応するディフェンスツリー（これをディフェンスツリー①とする），は**図 2** となる．同様に事象②に対するディフェンスツリーは**図 3** となる．

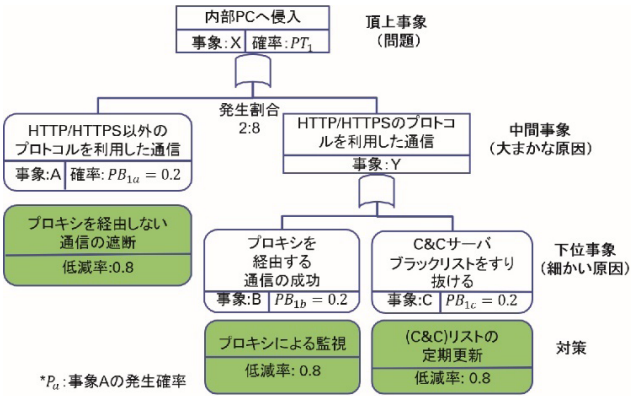

図 2 説明用ディフェンスツリー①
Fig. 2 Explanatory defense tree ①.

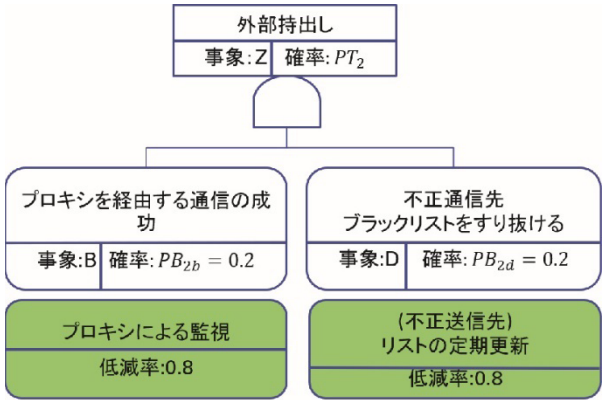

図 3 説明用ディフェンスツリー②
Fig. 3 Explanatory defense tree ②.

本ディフェンスツリーの適用手順を以下に示す．

A） まず，評価の対象者にとって望ましくない事象を頂上事象と呼び，これが起こる原因をリストアップする．これがイベントツリーの k 番目のヘッディング項目であり，発生確率 PT_k にあたる．図 2 においては「内部 PC 侵入」を頂上事象としている．

B） 頂上事象が決定したら，次にディフェンスツリー中のアタックツリーに相当する部分（頂上事象，中間事象，下位事象）の構造を決定する．頂上事象の発生原因である中間事象（図 2 では「HTTP/HTTPS のプロトコルを利用した通信」）を推定し，ゲートを設定する．ゲートは AND と OR があり，すべての原因事象が原

因ならばANDゲート，どれか1つの原因事象が原因ならばORゲートを用いる．また，原因事象の発生原因が複数あるならば，その事象から同じようにより細かい粒度の原因（下位事象）の推定（図2では「プロキシを経由する通信の成功」等）と，ゲートの設定を行う．これらを繰返して，ディフェンスツリーの構造を決定する．

以下，事象xと事象yについてx OR yを「x，y」，x AND yを「xy」と表す．また，事象xの発生確率をP_xとする．ANDおよびORの計算は次の式を用いる．

$$\text{AND}：P_{xy} = P_x \times P_y$$
$$\text{OR}：P_{x,y} = 1 - (1 - P_x) \times (1 - P_y)$$

対策を考慮しない場合の頂上事象の発生確率PT_kは以下の式で表される．

$$PT_k = AT(PB_{k1}, PB_{k2}, \cdots, PB_{km}, \cdots, PB_{kM}) \tag{6}$$

PT_kは頂上事象の発生確率

PB_{km}はk番目のヘッディング項目を構成するm番目の下位項目の発生確率．

ATはディフェンスツリー中のアタックツリー部でANDやORで表される，PB_{km}の組合せの関数

Mはk番目のヘッディング項目に含まれる下位項目の総数

C) 各下位事象の発生確率とその発生頻度の割合を推定する．発生確率等の数値に関しては，すべての人が納得する絶対的な算出根拠は存在しないが，統計データの値を用いたり，関係者が討議し合意した値を用いたりする．そのうえで，不安が残るものは感度解析でその数値を変え，結果にどのように影響するかを確認する．感度解析を行うことで，要素の個々の影響だけではなく全体に対しての影響を確認したうえでの議論を行うことができる．このように統計データや合意の下で決定した値を基に，頂上事象の発生確率を計算する．

図2においては，それぞれの下位事象の成功確率は比較を容易にするため発生確率を0.2と同じ値とする．

D) 既存のリスク分析と同様に，すべての事象の発生は独立であるという前提条件から，対策は発生原因が単一である下位事象にのみ効果があり，対策事象としてディフェンスツリーに記述する．複数の対策のうち，実施した対策の低減率を下位事象の確率にかけていくことで，対策を行った場合の発生確率を求めることができる．したがって，対策の個数が増えるほど，頂上事象の発生確率が減少し，リスク値の低下につながる．対策を考慮した場合の下位事象の発生確率の一般式は式(7)で表される．

$$PB_{km}{}' = PB_{km} \times \prod_{i=1}^{n} \{(1 - x_i) + PD_i \times x_i\} \tag{7}$$

$PB_{km}{}'$は対策を考慮した場合のk番目のヘッディング項目を構成するm番目の下位項目の発生確率．

PB_{km}は対策を考慮していない場合のk番目のヘッディング項目を構成するm番目の下位項目の発生確率．

nはPB_{km}に対する対策の総数

iは対策の番号

x_iは対策iの状態を表し，実施した場合に$x_i = 1$，実施しない場合に$x_i = 0$となる

PD_iは対策iによる低減率

ここで，図2で事象B「プロキシを経由する通信の成功」に対して，「プロキシによる監視」という対策を行った場合について例を示す．対策を考慮した下位事象の発生確率$PB_{1b}{}'$は式(8)のようになる．

$$PB_{1b} = 0.2, \quad PD_1 = 0.8, \quad n = 1, \quad i = 1$$
$$\begin{aligned} PB_{1b}{}' &= PB_{1b} \times \prod_{i=1}^{n} \{(1 - x_i) + PD_i \times x_i\} \\ &= 0.2 \times \{(1 - 1) + 0.8 \times 1\} \\ &= 0.16 \end{aligned} \tag{8}$$

E) 既存のディフェンスツリー[4]に新たに加えた要素として，攻撃者がとる攻撃手法の割合を追加した．攻撃の成功確率とは別に，特定の攻撃手法の流行やあまり使われることのない攻撃といったものを評価に考慮することを目的としている．割合はORゲートにのみ存在し，ある事象が占める割合をORゲート中で最も多く占める事象の割合で割った値を重みとしている．たとえば，図2における「HTTP/HTTPS以外のプロトコルを利用した通信」と「HTTP/HTTPSのプロトコルを利用した通信」は必ずしも同じ頻度で起こらない．トレンドマイクロの調査結果[10]よりマルウェアのおよそ80%がWeb系プロトコルを用いるというデータがあり，成功確率に発生頻度の重みづけを行う必要がある．「HTTP/HTTPS以外のプロトコルを利用した通信」と「HTTP/HTTPSのプロトコルを利用した通信」のそれぞれの発生する割合は2 : 8とした．発生頻度が大きい「HTTP/HTTPSのプロトコルを利用した通信」の発生確率の重みを8/8（= 1）とし，「HTTP/HTTPS以外のプロトコルを利用した通信」の発生確率に2/8をかける．割合を考慮した「HTTP/HTTPS以外のプロトコルを利用した通信」の発生確率を以下の式(10)で表す．

$$PB_{1a}{}' = PB_{1a} \times \frac{2}{8} = 0.2 \times \frac{2}{8} = 0.05 \tag{9}$$

以上がディフェンスツリー適用方法である．

3.6 ステップ 5：対策案の作成

標的型攻撃への対策は様々なものが存在するため，ステップ 4 までの分析結果を基に導入する対策案のリストを作成する．また，対策案の効果やコスト，ディフェンスツリーへの適用範囲の値付けを行う．

標的型攻撃の分析において用いられる対策は，IPA が推奨している対策 [9] や関係者の意見の中から判断し，分析結果に関係が深いと思われる対策を抜粋する．

今回の簡易な例の場合には表の 4 つの対策において検討を行う．**表 2** は対策の番号，対策の内容，対策のコスト（万円），対策の効果を表す低減率，対策の効果のある事象を表している．対策の実施による影響度を確認するため，対策のコストを 20 とし，低減率を 0.8 と同値を設定した．

3.7 ステップ 6：目的関数・制約条件の決定

様々な対策案の組合せが存在する中で，制約条件を満たしつつ，目的関数を最大・最小にするような対策の組合せが最適解となる．

EDC 手法では，総合リスク値の最小化を目的関数とした．また，制約条件として対策コストの上限を設定し，上限値を決め条件を満たす中で総合リスク値が最小となる対策の組合せを見つける．

Minimize:

$$R_T = \sum_{l=1}^{L} R_l(Xi\colon i = 1, 2, ---, I) \tag{10}$$

Subject to

$$\sum_{i=1}^{Ji} C_i \times X_i \leqq Ct \tag{11}$$

$$(X_i = 0, 1)$$

R_l は 3.4 節で説明したとおりイベントツリーとディフェンスツリーから求められる X_l の関数

L はイベントツリーのシーケンス数

I は対策案数

C_i は i 番目の対策コスト

C_t は対策コストの上限値

X_i は対策 i の状態を表し，実施した場合に $X_i = 1$，実施しない場合に $X_i = 0$ となる

ほかに考えられる制約条件としては，同時に入れられないような対策や同時に入れると効果が薄い対策の組合せを除外するような制約条件がある．

表 2 説明用対策の一覧
Table 2 List of Explanatory measures.

ID	対策の名称	コスト	低減率	対策対応個所
1	プロキシを経由する通信の遮断	20	0.8	事象 A
2	プロキシによる監視	20	0.8	事象 B
3	リストの定期更新	20	0.8	事象 C
4	設定の見直し	20	0.8	事象 D

3.8 ステップ 7：対策案の最適組み合わせの決定

ステップ 6 で決定した制約条件を満たす中で目的関数を最小とする対策の組合せを求める．

各組合せに対して総合リスク値と対策コスト値を算出する．すべての対策コスト値の合計が制約条件を満たしている中で，総合リスク値が最も小さい対策の組合せが最適解となる．求めた最適解を用いて議論を行い，必要によって事象の発生確率や影響等の値を変更し EDC 手法のステップを関係者全員が納得するまで繰り返し，最適解を求める．

4. 説明用 EDC 手法でのリスク評価

4.1 イベントツリーにおける対策の影響

EDC 手法を用いて図 1，図 2，図 3 の説明用のイベントツリーとディフェンスツリーに対してリスク値の計算を行う．ここでイベントツリーの影響は M_1 から順に 0，10^2，10^4 とする．導出した対策を何も実施しない場合の各事象の発生頻度は**表 3** となる．

ここで，図 1 のイベントツリーは事象①「内部 PC 侵入」と事象②「外部持出し」の 2 つで構成されている．仮にイベントツリーの事象①と事象②のそれぞれの発生確率を半分にするような対策がある場合について考える．その場合のリスク値を**表 4** に示す．

イベントツリーの事象①と事象②のそれぞれに効果がある対策を実施した場合の総合リスク値を算出した．結果として，事象①の発生確率を半減させる対策を行う方が事象②に対策を行うよりも小さい総合リスク値を示した．対策

表 3 説明用リスク値
Table 3 Explanatory risk value.

	PS_1	PS_2	PS_3	合計
発生頻度	0.61	0.8	0.02	
リスク値	0.00	37.63	156.80	194.43

表 4 対策を行った場合のリスク値
Table 4 Risk value when measures are implemented.

		PS_1	PS_2	PS_3	合計
事象①に対策	発生頻度	0.80	0.19	0.01	
	リスク値	0.00	18.82	78.40	97.22
事象②に対策	発生頻度	0.61	0.38	0.01	
	リスク値	0.00	38.42	78.40	116.82

表 5 対策によるリスク値
Table 5 Risk value by measures.

実施対策		PS_1	PS_2	PS_3	合計
1	発生頻度	0.61	0.37	0.02	
	リスク値	0.00	37.02	154.24	191.26
2	発生頻度	0.64	0.35	0.01	
	リスク値	0.00	35.00	115.71	150.71
3	発生頻度	0.64	0.35	0.01	
	リスク値	0.00	34.71	144.64	179.35
4	発生頻度	0.61	0.38	0.01	
	リスク値	0.00	37.95	125.44	163.39

の効果が同じであり，対策費用について考慮しないという条件の場合には初期事象に近い事象での入口対策を行うことが有効であることがいえる．しかし，IPA の資料 [9] を見ても分かるように一般的に入口対策となりうるものはセキュリティ製品であり対策費用が高い傾向にある．一方で内部・出口対策は業務・運用機器に分類されておりシステム設計で対策をとるため，比較すると価格が安くなることがある．

4.2 ディフェンスツリーにおける対策の影響

対策箇所によるリスク値を比較する．説明用ディフェンスツリー①と②は 5 つの下位事象を持つが，ディフェンスツリー①とディフェンスツリー②の事象 B は同じ事象であり，対策の種類は 4 種である．**表 5** は 4 種のうち 1 種にのみ対策を行った場合のリスク値の比較である．

4 種類の事象のうち，2 の事象 B「プロキシを経由する通信の成功」に対して対策「プロキシによる監視」を実施した場合に最も小さい総合リスク値を得られた．これは対策「プロキシによる監視」が複数個所に対して効果があるためである．イベントツリーとディフェンスツリーを作成すると，いくつかの下位事象に対して 1 つの対策が効果を持つことがある．同じ低減率であれば，対策が効果のある個所が多い方が総合リスク値の低下につながる．したがって表 5 のような結果となったと考えられる．

4.3 総当たりでの対策の評価

今回の対策は 4 つなので，その組合せは 16 通りとなる．**図 4** と**表 6** は総合リスク値と対策コストを表した図と 16 通りの対策の組合せの対応表である．図 4 は総合リスクの小さい順に並べた場合である．対策をすべて行った場合に最も小さい総合リスク値を得られるが，対策 2・対策 3・対策 4 を実施した場合との総合リスク値に大きな差がないことが分かる．仮に対策コストの上限を 40 に設定すると，総合リスク値が 4 番目である対策 2 と対策 4 を実施したときが最も低い総合リスク値を得ることができる．

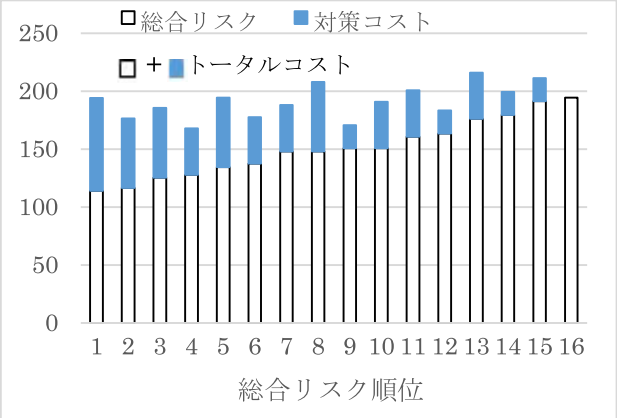

図 4 16 通りのリスクとコスト
Fig. 4 16 types of risks and costs.

表 6 対策の対応表
Table 6 Correspondence table of measures.

総合リスク順位	1	2	3	4	対策コスト	総合リスク	トータルコスト
1	○	○	○	○	80	114.03	194.03
2		○	○	○	60	116.52	176.52
3	○	○		○	60	125.43	185.43
4		○		○	40	127.80	167.80
5	○	○	○		60	134.47	194.47
6		○	○		40	137.41	177.41
7	○	○			40	147.91	187.91
8	○		○	○	60	147.91	207.91
9		○			20	150.71	170.71
10			○	○	40	150.71	190.71
11	○			○	40	160.72	200.72
12				○	20	163.39	183.39
13	○		○		40	176.02	216.02
14			○		20	179.35	199.35
15	○				20	191.26	211.26
16					0	194.43	194.43

4.4 リスクとコストの可視化

4.3 節の結果から，同じ対策コストをかけたときに総合リスクが最も低い組合せを抜き出すことで，各対策コストに上限を設けた場合の最適な対策の組合せを表す．**表 7** と**図 5** はそれらを抜き出したものである．図 5 より，対策コストを最もかけた場合に最小の総合リスクを得ることができるが，対策コストと総合リスクの和であるトータルコストを見ると，対策コストを 20 万円としたときが最も小

表 7 対策コスト上限内での最適解
Table 7 Optimal solution of measures for each upper limit.

対策コスト上限	実施対策				対策コスト	総合リスク	トータルコスト
	1	2	3	4			
80 万円	○	○	○	○	80	114.03	194.03
60 万円		○	○	○	60	116.52	176.52
40 万円		○		○	40	127.80	167.80
20 万円		○			20	143.00	163.00
0 万円					0	194.43	194.43

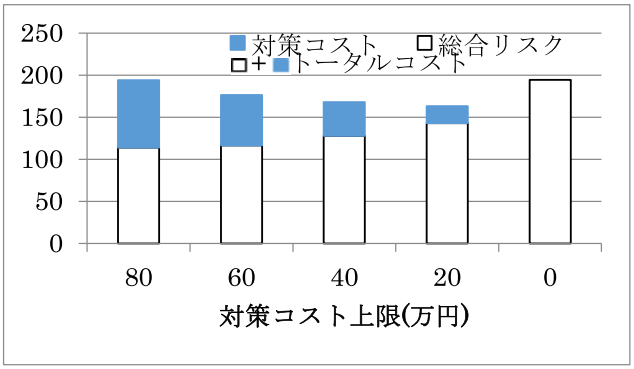

図 5 各対策上限でのリスクとコスト
Fig. 5 Risks and costs for each upper limit.

さくなる．対策コストが総合リスク値の低下に対して効果が見合っていないことが図から見て取ることができる．こういった図表を用いることで，組織がどの程度の対策コストをかけるべきかといった議論を管理者層に行うことができる．

5. 実適用と対策の選定

5.1 EDC 手法の実適用

EDC 手法を支援するツールを Excel を用いて開発し，そのツールを東京電機大学の標的型攻撃対策のための分析に適用した．ここで述べる分析内容および結果は，製品名や実際の購入価格を秘匿するため簡易化または一部を変更したものである．

5.2 実適用における対象組織

適用対象は，**表 8** のとおりである．個人情報として学生の成績を想定した．個人情報が流出した際の 1 人あたりに支払う賠償金は JNSA の JO モデルを基に算出した [11]．

5.3 実適用におけるイベントツリー

実適用における参考にする攻撃は 4.2 節と同様に日本年金機構への攻撃とする．日本年金機構への標的型攻撃事件に対して，イベントツリー分析法を適用した．作成したイベントツリーの全体像は**図 6** となり，4.2 節での調査結果を基に，事件の中で行われたと思われる**表 9** をイベントツリーの各事象とした．影響は**表 10** のとおりに設定した．

表 8 対象組織の概要
Table 8 Outline of target organization.

大学教職員数	500 人
全生徒数	10,000 人
攻撃者が狙う情報	生徒の成績
一人あたりの賠償金	5,500 円

表 9 イベントツリーの事象
Table 9 Events of the event tree.

事象番号	内容
1	攻撃者が標的型メールを送信する
2	だれか 1 人の PC をマルウェアに感染させる
3	バックドア開設・ネットワーク環境の調査・探索
4	他端末を乗っ取り，侵入範囲を拡大する
5	データの外部送信

表 10 イベントツリーの影響
Table 10 Impacts of the event tree.

	影響 (万円)	内訳 (万円)	内容
M_1	0	0	影響はない
M_2	100	100	PC1 台のフォレンジック調査
M_3	1500	1000	PC10 台のフォレンジック調査
		500	レピュテーション
M_4	2000	1000	インシデント対応費
		1000	レピュテーション
M_5	11500	5500	損害賠償
		3000	インシデント対応費
		3000	レピュテーション

5.4 実適用におけるディフェンスツリー

図 6 のイベントツリーに対して，ディフェンスツリー分析を行った．初期事象を除く 4 つの事象に対して分析を行ったが，ここでは事象②の「だれか 1 人の PC をマルウェアに感染させる」に対しての分析結果を**図 7** に示す．

5.5 実適用における対策案の決定

標的型攻撃の分析において用いられる対策は，IPA が推奨している対策 [9] や関係者の意見の中から判断し，前節までの分析結果において関係が深いと思われる対策を 13 個抜粋した（**表 11**）．

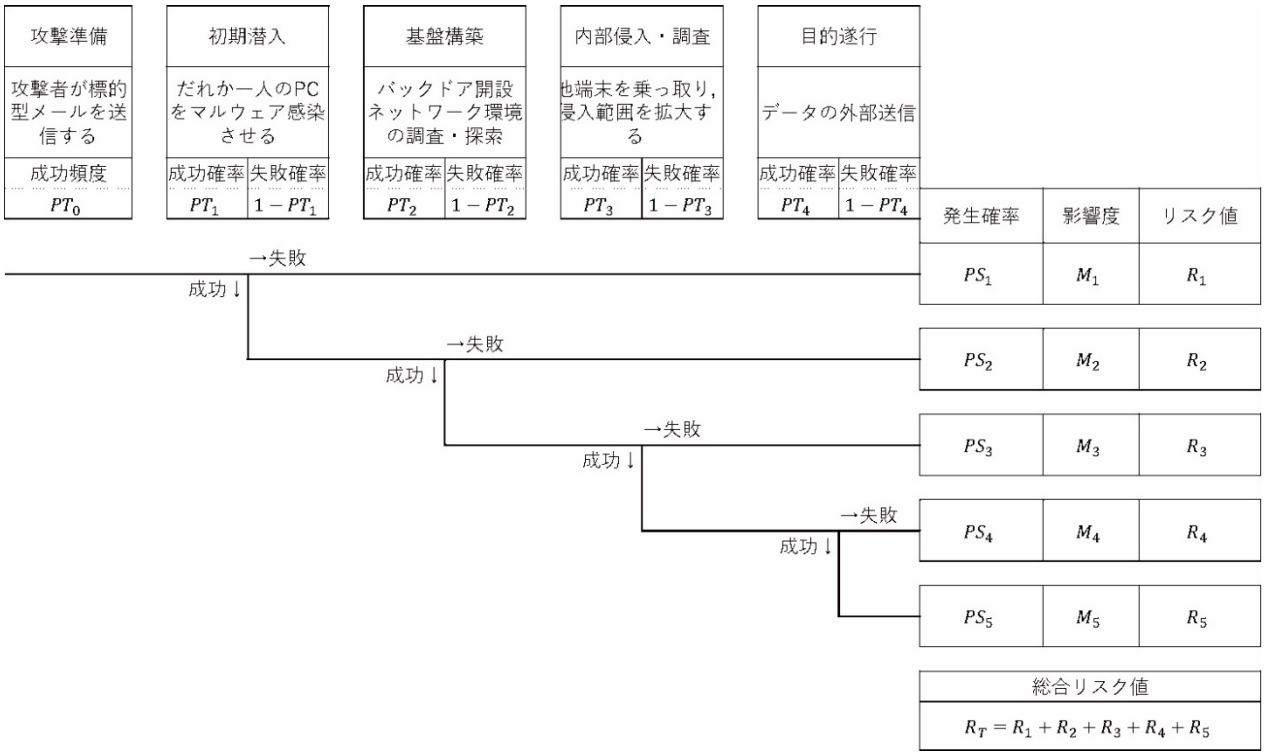

図 6 実適用イベントツリー
Fig. 6 Actual application event tree.

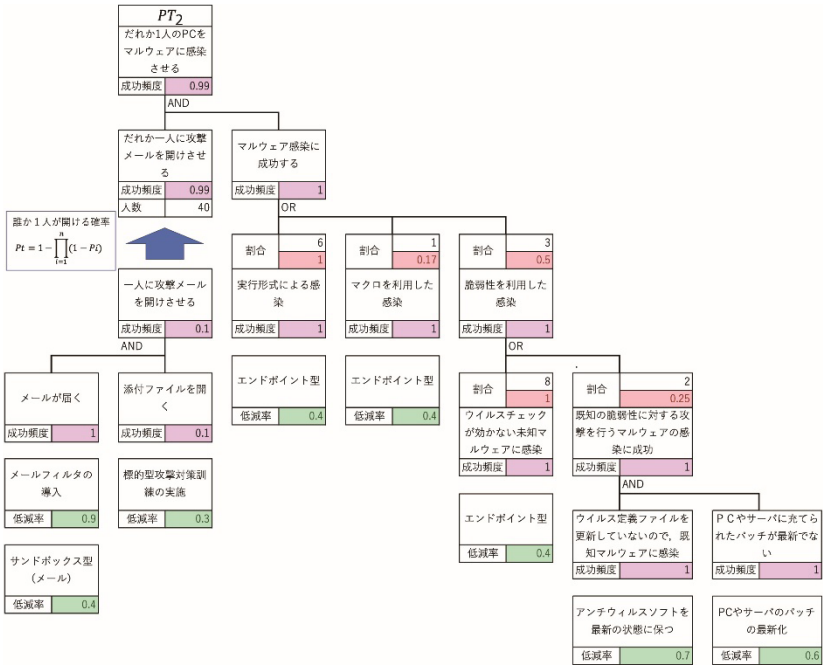

図 7 実適用ディフェンスツリー
Fig. 7 Actual application defense tree.

表 11 は対策の番号，対策の名称，導入コスト，年間運用コスト，対策の効果を表す低減率を表している．図 6 のイベントツリーと図 7 等のディフェンスツリー，対策案として表 11 を用いる．

対策の導入コスト，運用コストの算出方法は以下のとおりである．

導入コスト：

- ハードウェア購入
- 設置費用
- ソフトウェア購入費用
- 社内人件費用
- 外部委託費用

表 11 対策案一覧
Table 11 List of measures.

ID	対策の名称	導入コスト(万円)	年間運用コスト(万円)	低減率
1	メールフィルタの導入	77	20	0.9
2	サンドボックス型メールセキュリティ対策	1000	0	0.4
3	標的型攻撃対策訓練の実施	0	240	0.3
4	エンドポイント型セキュリティ対策	180	270	0.4
5	アンチウィルスソフトを最新の状態に保つ	140	65	0.7
6	ＰＣやサーバのパッチの最新化	0	140	0.6
7	プロキシによる監視	567	150	0.3
8	FW でのポート制御	0	150	0.6
9	サンドボックス型セキュリティ対策	600	650	0.3
10	外部 SOC	333	1000	0.2
11	セグメント間の通信の制限	0	100	0.4
12	個人情報の速やかな削除	0	100	0.5
13	統合ログ監視ツールの導入	100	650	0.4

運用コスト：
- 社内人件費用
- 保守・サポート費用
- ライセンス費用

対策の導入は 1 回分の費用となり，また対策の運用は年間の費用となるため統一する必要がある．情報機器やセキュリティの見直しはどの程度の期間で行われるかを議論したところ，3 年程度との結論が出たため，導入コストを 3 で割ることで 1 年分のコストとした．

5.6 目的関数と制約条件の決定

様々な対策案の組合せが存在する中で，対策の選定を行う必要がある．3.7 節での目的関数・制約条件を用いて，条件を満たす対策の組合せの導出を行う．対策コストは，3 年分の導入コストを 3 で除算し，年間の運用コストを加算した値とした．こうすることで，導入コストと運用コストが年間でどれくらいかかるのかを容易に表すことができる．制約条件である対策コストの上限に変化を加え，対策の選定を行った．上限には，1,000 万円から 7,000 万円まで 1,000 万円ごとに上限を定めた場合と上限を無制限とした場合の 8 種において総合リスク値が最も小さくなる対策の組合せを導出した．

6. 対策の選定

6.1 実適用における最適解

5 章での分析結果を用いて，対象組織にとって最適な対策の選定を行う．**図 8** が各条件での総合リスク値が最も低くなるような対策を実施したときのトータルコストを示している．各条件で選ばれた対策の組合せとそのときの総合リスク値と対策コストおよびトータルコストは**表 12** のようになる．

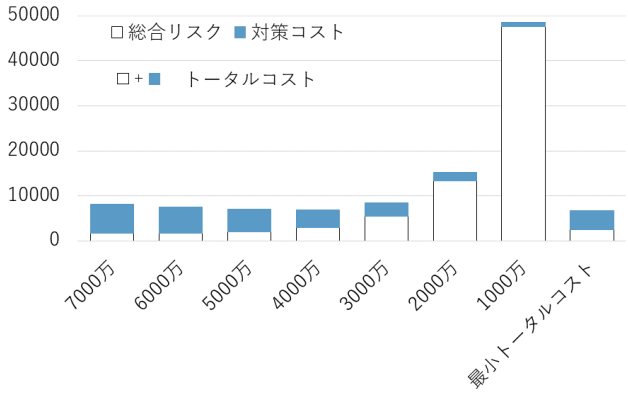

図 8 各対策コスト上限の最適解のリスクとコスト
Fig. 8 Risk and cost of optimal solutions for each upper limit.

1,000 万円から 7,000 万円の中で，トータルコストが小さくなるのは 4,000 万円付近であることが分かる．さらに分析を行うとトータルコストが最も小さくなるのは図 8 の右にある対策コストが 4,260 万円の場合で，その最小トータルコストは 6,734 万円の場合である．それ以上の対策コストをかけることで，総合リスクは小さくはなるが，それらの和であるトータルコストはより大きくなることが分かる．このような可視化を行うことにより，どのあたりまで対策をとればよいかが分かるようになったとの意見を評価参加者から得ることができた．

表 12 より，対策 ID3「標的型攻撃対策訓練の実施」，対策 ID4「エンドポイント型セキュリティ対策」，対策 ID11「セグメント間の通信の制限」の対策はいずれの条件でも選ばれているため，より有効な対策案の候補となる．それぞれの対策が算出された理由を考察すると，対策 ID3「標的型攻撃対策訓練の実施」は入口における教育対策であり，

表 12 各上限の場合での対策の組合せ
Table 12 Combination of measures for each upper limit.

対策 ID	7000 万	6000 万	5000 万	4000 万	3000 万	2000 万	1000 万	最小トータルコスト
1	○	○	○	○	○			○
2	○	○	○	○				○
3	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○
5	○	○						
6	○	○	○			○		○
7	○		○					
8	○	○	○			○	○	○
9	○	○						
10	○	○	○	○	○			○
11	○	○	○	○	○	○	○	○
12	○	○				○		
13	○	○	○	○	○	○		○
対策コスト(万円)	6532	5815	4977	3970	2970	1930	940	4260
総合リスク(万円)	1677	1766	2118	2918	5511	13281	47524	2474
トータルコスト(万円)	8209	7581	7095	6888	8481	15211	48464	6734

表 13 各対策の分類
Table 13 Classification of measures.

	1	2	3	4	5	6	7	8	9	10	11	12	13
入口	○	○	○	○	○	○			○				
内部							○	○	○	○	○		○
出口							○		○	○		○	

表 14 各対策コスト上限に含まれる対策種別の個数
Table 14 Number of measure types for each upper limit.

	7000	6000	5000	4000	3000	2000	1000	トータルコスト
入口	7	7	5	4	3	3	2	5
内部	6	5	5	3	3	3	2	4
出口	4	3	2	1	1	1	0	1

日々のメールに対し標的型攻撃の意識を持つことで，攻撃の発生確率を抑えることができるためだと思われる．対策 ID4「エンドポイント型セキュリティ対策」は，効果のある範囲が広い対策のなかでも設定したコストが比較的安いために算出されたと考えられる．対策 ID11「セグメント間の通信の制限」は，EDC 手法のツリー上で表された標的型攻撃の流れのうち，必ず行う事象に対して効果的であるためだと考えられる．

6.2 対策の分類

対策は一般的に入口対策，内部対策，出口対策の 3 種に分類される．表 11 の対策案一覧と 3 種の対応を**表 13** に示す．表 12 の最適解を表 13 の分類表を基に分類を行い，それぞれの条件の最適解で入口・内部・出口の選択数の集計結果を**表 14** に示す．

最近は，入口対策よりも内部・出口対策の方が重要であるというような論調が多いが，表 14 より，対策コストの上限に制限を加えていっても，入口・内部・出口のいずれか 1 種類が対策として選ばれないという形にはならないことが分かる．これより，入口対策・内部対策・出口対策をもれなく実施することが望ましいと考えられる．

この分析をより詳細化したものが，TDU-CSIRT メンバの協力を得ながら行われ，その結果は，東京電機大学で標的型攻撃対策を検討するのに使われた．

7. おわりに

本研究では，イベントツリー分析法とディフェンスツリー分析法を組み合わせた EDC 手法を提案した．対策は

初期事象に近い事象で発生確率を抑えるほうがより効果が高く，効果の適用範囲が広い対策の方が効果が高いことを確認した．また，EDC 手法を用いて実適用を行い，具体的な数値を入れ結果の検討を行った．その結果，対策コストを増やしても，総合リスクはあまり下がらず，対策コストが多くかかってしまい，トータルコストが大きくなってしまうことが分かった．これより，EDC 手法では対策コストと総合リスクのバランスを考えながら対策を選定できる手法であるといえる．対策コストの上限を定めたうえで，対策コストと総合リスク値を重ねて表示させることで，組織がどの程度対策をかけるべきかを管理者層を含めた関係者間での議論が可能となる．また，EDC 手法で分析結果から対策コストの上限に変更を加えても入口対策・内部対策・出口対策をもれなく実施することが有効であることが分かった．

提案手法を既存手法と比較した際の優位点として，イベントツリー分析を用いることで標的型攻撃が持つ攻撃の段階に即した分析を行うことができること，また段階ごとに分析することによって 1 つ 1 つの比較的小さいツリーの構築で済むため作業がしやすいこと，対策の選定までを行い，リスク値とコスト値を合わせて示すことで対策費用の目安となる結果を示せることがあげられる．

実適用においては，具体的な対策製品を用いて分析を行った．同じカテゴリに属する対策でも，ディフェンスツリーを細かく分析することで対策製品ごとの違いを記述することができ，対策製品の選定までを行うことが可能となった．具体的な製品になったために対策数が増え，計算量が大きくなったが，同種の対策を 1 つしか選ばないような制約条件を加えたり，議論の過程で採用・不採用が確定した対策を固定したりすることで計算量を減らす工夫を行った．また分析結果を対策コストと総合リスク値を示したグラフを見せることで，説明がしやすくかつ納得のしやすい形で示すことができ，それに沿った形で対策の実施が検討されており，本方式の有用性が具体的適用の中で確認することができた．一方で，2 つの製品をまとめて購入した場合に割引率を増やす等の提案があった場合には，それに沿った分析をやり直したり，対策によって予算枠が異なりそれぞれの制約に沿って分析をやり直す必要がある等，関係者全員の合意を得るまで会議を繰り返えし，分析を行った．

今後は EDC 手法での分析結果を基に，対策の選定を進めていく．また，対策が n 個の場合の対策の組合せは 2^n 通りとなるため，対策数が 20 個や 30 個を超えるとその計算時間が大幅に伸びてしまうことが課題となっており，短時間での，可能であれば議論中に再計算を行うことができるレベルの高速近似解法の確立を行いたいと考えている．

謝辞 方式の検討にあたり，貴重なご意見をいただいた FFRI の松木隆宏氏に深謝申し上げる．また，実適用においてご協力いただいた TDU-CSIRT メンバの皆様に，謹んで感謝の意を表する．

参考文献

[1] 加藤弘一，勅使河原可海：ネットワーク特別利用時におけるセキュリティと利便性を考慮した最適対策決定手法の提案，情報処理学会論文誌，Vol.49, pp.3209–3222 (2008).
[2] 柴田理洋，大久保隆夫：Attack Tree を用いたクリティカルパス検出による効果的対策の提案，コンピュータセキュリティシンポジウム 2016 論文集，No.2, pp.243–248 (2016).
[3] 石井亮平，佐々木良一，金子紀之：イベントツリーを用いたリスク評価ツールの実装と標的型攻撃最適組み合わせ問題への適用，コンピュータセキュリティシンポジウム 2013 論文集，No.4, pp.147–154 (2013).
[4] Bistarelli, S., Fioravanti, F. and Peretti, P.: Defense trees for economic evaluation of security investments, *The 1st International Conference on Availability, Reliability and Security, ARES 2006*, p.8 (2006).
[5] Edge, K.S., Dalton, G., Raines, R.A. and Mills, R.F.: Using attack and protection trees to analyze threats and defenses to homeland security, *Military Communications Conference, MILCOM 2006*, pp.1–7 (2006).
[6] Bowles, J.B. and Pelaez, C.E.: Application of fuzzy logic to reliability engineering, *Proc. IEEE*, Vol.83, pp.435–449 (1995).
[7] Andrews, J.D. and Dunnett, S.J.: Event-tree analysis using binary decision diagrams, *IEEE Trans. Reliability*, Vol.49, pp.230–238 (2000).
[8] 藤本，上田，佐々木：デジタル署名付き文書への公開鍵暗号危殆化対策の組合せ最適化法の提案と一適用（セキュリティ/危機管理，〈特集〉新しいパラダイムの中での分散システム/インターネット運用・管理），情報処理学会論文誌，Vol.49, pp.1105–1118 (2008).
[9] 「高度標的型攻撃」対策に向けたシステム設計ガイド，入手先 ⟨https://www.ipa.go.jp/files/000046236.pdf⟩（参照 2017-05-07）.
[10] 国内標的型サイバー攻撃分析レポート 2016 年版—状況と目的に応じて攻撃を変化させる攻撃者，入手先 ⟨https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=194⟩（参照 2017-05-07）.
[11] 2014 年情報セキュリティインシデントに関する調査報告書—個人情報漏えい編，入手先 ⟨http://www.jnsa.org/result/incident/2014.html⟩（参照 2017-05-07）.

相原 遼

平成 28 年東京電機大学未来科学部情報メディア学科卒業．同年 4 月より東京電機大学大学院未来科学研究科情報メディア学修士課程．IT リスクの研究に従事．

石井 亮平

平成 28 年東京電機大学未来科学部情報メディア学科卒業．同年 4 月より東京電機大学大学院未来科学研究科情報メディア学修士課程．平成 27 年 3 月同大学院修了．

佐々木 良一 （正会員）

1971 年 3 月東京大学卒業．同年 4 月日立製作所入社．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．2001 年 4 月より東京電機大学教授，工学博士（東京大学）．2002 年情報処理学会論文賞受賞．2007 年および 2017 年に総務大臣表彰等．著書に，『IT リスクの考え方』岩波新書（2008 年）等．日本セキュリティ・マネジメント学会会長，内閣官房サイバーセキュリティ補佐官等を歴任．本学会フェロー．