イベントツリーを用いたリスク評価ツールの実装と 標的型攻撃対策最適組み合わせ問題への適用

石井 亮平† 金子紀之† 佐々木 良一‡

†東京電機大学
120-8551 東京都足立区千住旭町 5 番
ishii@isl.im.dendai.ac.jp

あらまし 近年，標的型攻撃による被害が増加している．その為，企業や組織は標的型攻撃への危機意識を高め，セキュリティ技術や製品の導入を検討している．しかし、1 つの対策だけでは十分な効果を得ることができず、コストやリスク低減効果さらには使いやすさを考慮した対策案の最適な組み合わせを求めるツールが必要とされている．本稿では，イベントツリーを用いたリスク評価ツールの実装を行うとともに，対象となる組織を想定し標的型攻撃に適用することで対策の最適な組み合わせを求めることができたので，その適用結果を報告する．

Development of the risk evaluation tool based on the event tree analysis and application to the problem for obtaining optimal combination of measures against targeted cyber attacks

Ryohei Ishii† Noriyuki Kaneko† Ryoichi Sasaki†

†Tokyo Denki University
5, Senju-Asahi-cho, Adachi-ku, Tokyo, 120-8551 JAPAN
ishii@isl.im.dendai.ac.jp

Abstract Recently, the damage caused by targeted attacks has been increasing. Companies and organizations examine the introduction of security technologies and products caused by conscious of the danger of a targeted attack. However, only one measure cannot achieve a sufficient effect. Therefore, tools determining the optimal combination of measures considering of the cost, the effect of risk reduction, and ease to use are needed. In this paper, we report the implemented tool based on the event tree analysis method, and optimal combination of measures obtained by applying the tool for an assumed institute.

1. はじめに

情報社会の進展とともに，デジタルデータに対する攻撃は日々増している．特に脅威とされている攻撃が，標的型攻撃である．

標的型攻撃とは，特定の組織を狙ったサイバー攻撃である．様々攻撃な手法が存在するが，ソーシャルエンジニアリングを活用した攻撃が一般的である．ソーシャルエンジニアリングを活用するため，攻撃対象側は攻撃が発生

したことすら気づかない状況が多いと言われている. この標的型攻撃の被害件数は増加傾向にあり, 標的型攻撃への対策を検討する需要が高まっている.

しかし, 対策を1つ導入しただけでは標的型攻撃に対して十分な効果を得ることは期待出来ない. また闇雲に対策を増やしたところでそれらが生み出す効果が有効であるとは言い難い. それに加えて, セキュリティへのリスク対処が新たなリスクを生み出す派生リスクの問題が存在する. その為, コストやリスク低減効果や派生リスクを考慮しつつ対策を検討する必要があると考える.

筆者らは, イベントツリー分析法に基づく標的型攻撃の分析評価ツールの開発と適用に関する検討を行ってきた[1]. その後, 定式化の見直し等を行ったので, 本論ではアプローチ方法, 定式化結果, 求解結果, 今後の展開などに関し報告する.

2. 最適な対策案を求める手順

標的型攻撃に対して最適な対策案を求める手順を以下に示す.

(1) 対象の決定

標的型攻撃には様々な攻撃手法が存在するため, ここでは標的型攻撃を具体的に特定し, 分析の対象と分析の前提を決定する.

(2) イベントツリー分析によるリスク分析

(1)で決定した分析の対象, 分析の前提からイベントツリーを作成する.

(3) 最適化問題としての定式化

最適な対策案の組合せを求めるのに必要な目的関数と制約条件の定式化を行う. 各対策案を 0-1 変数で採択し, 組合せ最適化問題として定式化する.

(4) 最適解の求解

設定された制約条件の下で, 最適な対策案の組み合わせを算出する. また, パラメータを変更し, 最適解を算出する.

(5) 結果の分析

本稿ではフォレンジック対策の有効性と最小のコスト制約で最も効果的な対策案の組み合わせについて検証していく.

3. 組合せ最適化のための方式

3.1 対象の決定

3.1.1 衆議院への標的型攻撃

2011 年 7 月に行われた衆議院への標的型攻撃を対象とする[2]. この事件では, 3 台の議員端末に対しマルウェアが添付されたメールが送信され, そのうち1台がマルウェアを開封・実行したことにより, マルウェアに感染したことが発端となっている.

事件の流れとして, まず感染した議員端末の ID とパスワードが窃取された.

次に攻撃者は, サーバと運用管理端末の管理者 ID とパスワードを窃取し, 議員用アカウントサーバに不正なプログラムを埋め込んだ. また, 運用管理端末からは全議員の ID とパスワードが窃取され, サーバ上に保存していたメールは盗み見られた.

更に, 議員用アカウントサーバにログオンした他の議員端末に不正なプログラムがコピーされ, 25 台の議員端末に感染が広がることとなった.

この事件を対象にリスク分析を行うにあたり, サーバ数等のネットワーク情報を加味する必要がある. しかし, 確実な情報を得ることが出来ない為, 表 1 のように設定した.

従業員は, 議員 480 人と秘書 480 人と事務員 1650 人を合わせた人数になっているが, ホストは議員と秘書に 1 台ずつ与えられていると仮定している.

表 1. 衆議院ネットワーク情報

従業員数	2260
ホスト数	960
Web サーバ数	2
メールサーバ数	2
データベースサーバ数	1
AD サーバ数	4
運用管理端末数	2

3.2　イベントツリー分析

3.2.1　イベントツリー分析とは

イベントツリー分析（Event Tree Analyze : ETA）とは，ツリーの枝をたどるように分析を行うことにより，事故の進展状況が順を追って把握でき，事故の進展を防止するための対策を立てやすい分析手法である[3].

3.2.2. イベントツリー分析の適用

衆議院への標的型攻撃事件に対して，イベントツリー分析の適用を行った.

本事件では，初期事象から最終事象までの事象を 1 次感染，2 次感染，3 次感染に分けて分析することにより，状況をより分かりやすく把握できるようにしている.

まず1次感染では，初期事象から 3 台の議員用端末に対して標的型メールが届くところから，1 台の議員用端末がマルウェアに感染し，キーロガー攻撃によってキーボード入力情報が窃取されるまでとする.

次に 2 次感染では，前述の事象から議員用アカウントサーバにマルウェアが埋め込まれ，運用管理端末およびメールサーバから情報が窃取されるまでとする.

最後に 3 次感染では，前述の事象から 25 名の議員端末に感染が広がるまでとする.

これら各事象を細分化し，イベントツリー分析に適用した.

3.2.3. イベントツリー分析の事象の決定

衆議院への標的型攻撃を細分化したことにより，事象を以下の表のように設定した．表 2 の分析を基にイベントツリーを作成すると，図 1 のようになる．また，設定した事象は攻撃者の視点となっている.

表 2. 1 次感染の事象一覧

1 次感染		
No	事象	発生確率
①	衆議院議員のメールアドレス宛に標的型メールが届く	1 / 年
②	標的型メールの添付ファイルを開く	0.999
③	マルウェアがアンチウィルスソフトに検知されない	0.25
④	C&C サーバへの感染報告送信に成功する	0.999
⑤	C&C サーバから新たなベクターの受け取りに成功する	0.999
⑥	キーロガー攻撃が成功する	0.999

同様に表3，表4の分析を基にイベントツリーを作成する．ただし，本稿では省略する.

表 3. 2 次感染の事象一覧

2 次感染		
No	事象	発生確率
⑦	サーバ及び運用管理端末への不正アクセスに成功する	0.999
⑧	AD サーバ内のマルウェアがアンチウィルスソフトに検知されない	0.999
⑨	情報を外部へ送信することに成功する	0.999

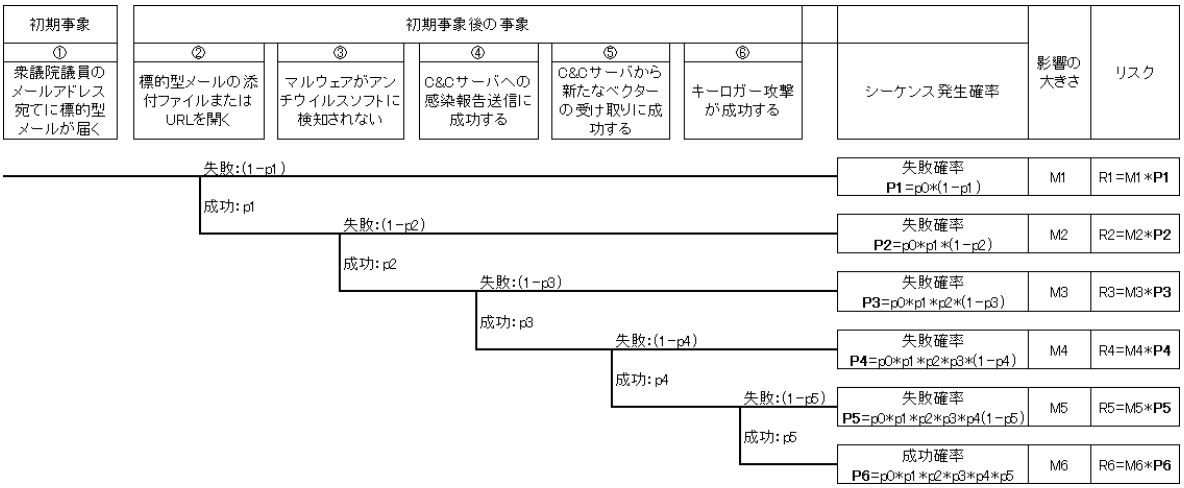

図 1. 1 次感染イベントツリー

表 4. 3 次感染の事象一覧

3 次感染		
No	事象	発生確率
⑩	AD サーバのログオンスクリプトによりダウンロードしたマルウェアがアンチウィルスソフトに検知されない	0.999

各事象の発生確率の設定根拠を以下に示す.

(1) No1 の事象

衆議院議員のメールアドレスはインターネットに公開されているため，メールは確実に届くと考えらえる.

(2) No2 の事象

開封確率 Q が一定と仮定したとき，n 人の内最低でも 1 人が標的型メールを開封してしまう確率は以下の式で表される.

$$P = 1 - (1 - Q)^n$$

この式を計算すると，Q の値を 0.01 にしたとしても，n の値が 500 を超えると P の値は 0.99 になる. このことから，人数が多いほど発生確率は 1 に近づくことが分かる.

(3) No3 の事象

アンチウィルスソフトの検知精度は，AV-Comparative が行ったアンチウィルスソフトのヒューリスティックスキャン結果の平均値から算出している[4].

(4) No4, 5, 6 の事象

公務用パソコンがウイルスに感染したと仮定すると，以後の事象である，C&C サーバへの感染報告，C&C サーバからベクターの受け取り，キーロガー攻撃はほぼ成功すると考えられる.

(5) No7 の事象

攻撃者の管理者権限を窃取した手法は不明とされている. その為，管理者権限を窃取した状態から事象を考察すると，サーバ及び運用管理端末への不正アクセスはほぼ成功すると考えられる.

(6) No8 の事象

ネットワーク内のアンチウィルスソフトは全て同様のものを使用していると仮定すると，初期感染に成功した攻撃者のマルウェアが検知される確率は低いと考えられる.

(7) No9 の事象

サーバにマルウェアが感染してしまった為，情報を外部に送信することはほぼ成功すると考えられる.

(8) No10 の事象

AD サーバにアクセスした議員端末も，No8 の事象と同様に考えられる.

3.2.4. リスクの計算方法

図 1 に示したイベントツリー分析のリスクの計算方法と 3.4 節で述べる対策案の対応付けについて述べる.

まず，各リスクについての計算式だが，初期事象から標的型攻撃の成否が決定するまでの流れをシーケンス，各事象をヘッディング項目として表現すると，以下のような式になる.

$$R_l = P_l * M_l \cdots (1)$$

l は l 番目のシーケンスを表す

$$P_l = P_0 * \prod_{i=1}^{H} P_i \cdots (2)$$

i は i 番目のヘッディング項目を表す

H はヘッディング項目数

Pi は i 番目のヘッディング項目の分岐確率

$$P_i = ((1 - p_i)(1 - y_i) + p_i * y_i) \cdots (3)$$

$$y_i = \begin{cases} 1: \text{ヘッディング項目が下に展開} \\ 0: \text{ヘッディング項目が横に展開} \end{cases}$$

R_lは，式(1)に示すように，シーケンスごとのリスクであり，ここでは発生確率P_lと影響の大きさM_lの積で表している.

P_lは，式(2)に示すように，初期事象P_0と各ヘッディング項目の発生確率の積で表すことができる.

P_iは，式(3)に示すように，各ヘッディング項目が下に展開する場合と横に展開する場合を式で表したものである.

M_lは，情報が摂取されない場合$M_l = 0$をとり，情報が窃取された場合，下記の表を参考に計算を行う.

表 5. 盗まれた情報

議員端末の ID･パスワード	5000 円 / 件
議員のメール情報	30000 円 / 人

表 6. 国の信頼の低下

影響度	値
小	10 億
中	100 億
大	1000 億

表 5 は本事件で盗まれた情報とその損害額である. また，表 6 は攻撃が成功した深さに応じて損害額は増えていくと想定した.

下記の式(4)はヘッディング項目 i に設定した対策案が 1 つのとき，その効果をa_{i1} （i は各ヘッディング項目を示し，1 はその 1 番目の対策案を示す）とし，対策案適用前の攻撃成功確率を$\overline{p_i}$とした際の ETA の攻撃成功確率p_iとの関係を表現するものである.

$$p_i = \overline{p_i} * (1 - X_{i1}) + \overline{p_i} * ((1 - a_{i1}) * X_{i1}) \cdots (4)$$

(X_{i1}=0, 1)

ここでX_{i1}は，ヘッディング項目 i の 1 番目具体的対策案を表す 0-1 変数である. また，ヘッディング項目 i に設定した対策案が 2 つのとき，3 つのときも式を算出し，計算を行う.

式(5)は，フォレンジック対策の効果をa_fとし，対策案適用前のシーケンスごとのリスクを$\overline{R_l}$とした際の ETA のシーケンスごとのリスクR_lとの関係を表している. ただし，本事件のフォレンジック対策はシーケンス 3 以降で効果を発揮するものとしている.

$$R_{l\geq 3} = \overline{R_{l\geq 3}} * \prod_{f=1}^{F}\left((1 - a_f) * X_f + (1 - X_f)\right) \cdots (5)$$

$$(X_f = 0, 1)$$

F はフォレンジック対策数

前述と同様にX_fはフォレンジック対策の f 番

目具体的対策案を示す 0-1 変数である.

3.3 組合せ最適化問題の定式化

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，トータルコストに関する目的関数を最小にする最適解を導出する.

目的関数は，シーケンスごとのリスクの和と対策コストを加算したものをトータルコストとし，トータルコストが最小になるものを目的関数とする. これを定式化したものが式(6)となる.

また，制約条件は対策コストを設定し，定式化すると(7)になる.

Minimize:

$$\sum_{l=1}^{L} R_l + \sum_{i=0}^{H} \sum_{j=1}^{Ji} C_{ij} * X_{ij} + \sum_{f=1}^{F} C_f * X_f \cdots (6)$$
$$(X_{ij} = 0,1 \ X_f = 0,1)$$

Subject to:

$$\sum_{i=0}^{H} \sum_{j=1}^{Ji} C_{ij} * X_{ij} + \sum_{f=1}^{F} C_f * X_f \leq C_t \cdots (7)$$
$$(X_{ij} = 0,1 \ X_f = 0,1)$$

ここで，$X_{ij,\,f}$は 0-1 変数である. また，$C_{ij,\,f}$は対策案のコストの値を用いて求められる.

3.4 対策案の決定

3.4.1 対策の前提条件

衆議院ネットワークで既に行われている対策を調べることはできないため，表 5 のように想定した. アンチウィルスソフトは自動で定義ファイルを更新していると仮定する.

表 5. 導入済みの対策

No	対策案
1	ファイアウォールの設置
2	アンチウィルスソフトの導入
3	セキュリティポリシーの作成

3.4.2 対策案一覧

本稿では，分析した攻撃手法に関係が深いと思われる対策として，IPA が推奨している対策案の中から 14 個の対策案を抜粋した（表 6）[5].

表 6. 対策案の一覧

No	対策案	対策対象事象
1	スパムフィルターの導入	①
2	セキュリティポリシーを定期的に共有し，確認する	②
3	標的型メール攻撃に対する予防訓練	②
4	アンチウィルスソフトを最新の状態に保つ	③, ⑩
5	IDS・IPS の導入	④
6	ファイアウォールの適切な通信制御	④
7	プロキシサーバを利用した経路制御	④
8	適切なユーザ認証を行っている	⑦
9	アクセスログの監視	⑦
10	重要サーバに対するルート制御/ネット隔離	⑨
11	ファイル暗号化	⑨
12	ネットワークログの取得・分析	Ⓕ
13	サーバログの取得・監視	Ⓕ
14	危機対応体制の整備	Ⓕ

対策対象事象の値は，表 2, 3, 4 の値に対応している. ただし，値がⒻの対策はフォレンジック対策になるので，式(5)に対応する.

対策案のパラメータを表 7 のように設定した. 対策効果は値が 0.1 のとき対象となる数値を 1

割下げることを意味している.

表 7. 対策案のパラメータ

No	対策効果	コスト
1	0.5	1,783,000
2	0.1	500,000
3	0.2	3,000,000
4	0.1	1,152,000
5	0.5	7,400,000
6	0.3	0
7	0.5	1,528,000
8	0.3	0
9	0.3	1,500,000
10	0.7	15,000,000
11	0.3	4,608,000
12	0.3	4,700,000
13	0.3	3,450,000
14	0.1	500000

4. 評価ツール適用実験

以上のリスク分析によって得られたデータを評価ツールに適用し，最適解の算出を行った.

表 9. 制約条件無しの最適解の算出

	フォレンジック対策有り	フォレンジック対策無し
目的関数	138,806,002	248,908,648
発生確率	0.001302	0.001302
対策コスト	45,121,000	36,471,000
対策案	全て	全て

表 9 は制約条件を設定せずに行った最適解である. 全ての対策案が採用されたことから，IPA の対策は全て行っておく必要があることが言える. また，フォレンジック対策を採用することによって，対策コストの値は増加するが目的関数の値は減少することが分かった.

更に，制約条件として対策コストの値を全体総数値の半分の値に設定して最適解の計算を行うと，表 10 の結果が得られた.

表 10. 制約条件有りの最適解の算出

	フォレンジック対策有り	フォレンジック対策無し
目的関数	421,755,524	551,361,555
発生確率	0.007751	0.004341
対策コスト	22,513,000	21,471,000
対策案	1,2,4,5,6,7,8,9,12,13,14	1,2,3,4,5,6,7,8,9,11

表 10 から，対策コストを同程度の値に止めたとしても，フォレンジック対策を行うことで目的関数の値は減少することが分かる.

以上 2 つの実験結果から，IPA の対策の必要性とフォレンジック対策の有効性が証明できたと言える.

続いて，最小コストで最も効果的な最適解を算出し，算出結果の分析を行った.

制約条件として対策コストを 50 万 ~ 4000 万までの値に設定し最適解を算出すると，図 2 のようなグラフになる.

このグラフから対策コストとして 500 万円程度掛ければ，費用対効果が高い対策案の組み合わせを得ることができると言える. 具体的に 250 万円と 500 万円の対策案の組み合わせを見てみると，表 11 のようになった.

表 11. 対策コスト別対策案の組み合わせ

	250 万円	500 万円
対策案	6, 7, 8, 14	1, 6, 7, 8, 9

250 万円の対策案は機器の設定や組織の体制を導入しているのに対し，500 万円の対策案ではそれに加えて具体的なツールを導入していることが分かる. このことから，トータルコストを一定以上抑えるためにはセキュリティツールを導入する必要があると言える.

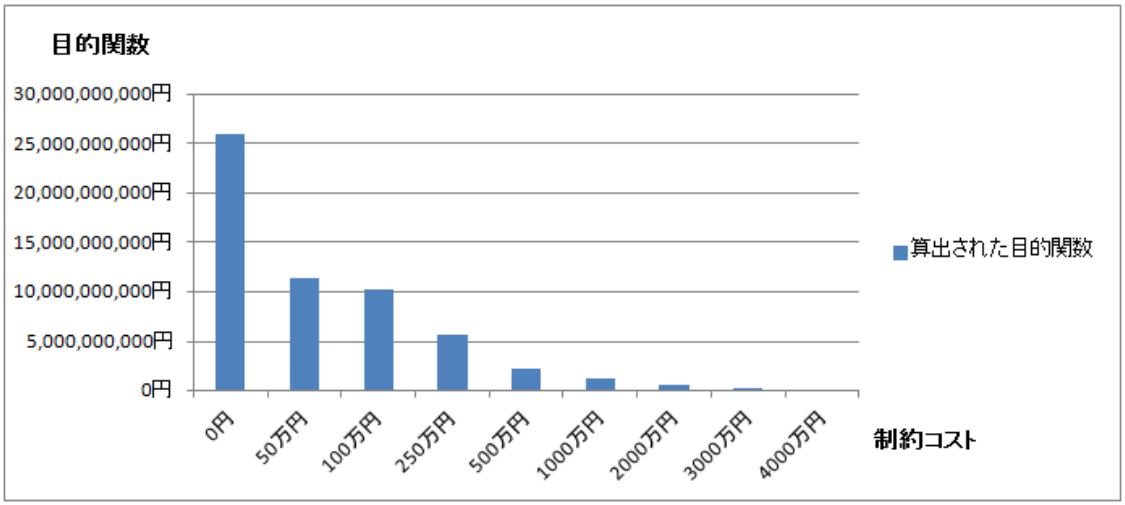

図 2. 対策コスト別目的関数の推移

250 万円の対策にはフォレンジック対策が導入されているが，500 万円の対策には導入されていない．これは制約コストの中でトータルの対策を考えた際に，フォレンジック対策よりも先に行う対策があることを示している．

また，表 11 の中に対策 No3 が導入されていないことから，3.2.3 節の(2)で示した式の通り人数が多くなるほどメールを開封する確率は高くなるため，予防対策の優先度は低くなると思われる．

5. おわりに

本稿では，標的型攻撃に対する最適な対策案の算出を行うにあたり，2011 年に起きた衆議院への標的型攻撃を対象にイベントツリー分析を行い，算出された対策案の考察・分析結果について報告した．

フォレンジック対策は，被害に遭った際の原因究明やデータの法的な証拠性を明らかにする為に必要な対策である．その為，どのデータを残すのか，どの程度の期間残すのかが重要になってくる．本稿では上記の分析が不十分であるため，今後はその点を意識した標的型攻撃の分析を行っていく予定である．

参考文献

[1] イベントツリー分析法に基づく標的型攻撃の分析評価ツールの開発と適用
https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=91111&item_no=1&page_id=13&block_id=8

[2] 議員運営委員会庶務小委員会 衆議院へのサイバー攻撃報道に関する件
http://www.shugiin.go.jp/itdb_kaigiroku.nsf/html/kaigiroku/009017920111114005.htm

[3] 中小企業総合事業団: リスク原因の究明，
http://www.smrj.go.jp/keiei2/kankyo/h11/book/3rab/html/kagaku1l.htm/

[4] AV-Comparative Proactive test
http://www.av-comparatives.org/wp-content/uploads/2012/07/avc_beh_201207_en.pdf

[5] IPA: 標的型攻撃 / 新しいタイプの攻撃の実態と対策
http://www.ipa.go.jp/security/J-CSIP/documents/presentation2.pdf