Vol.2013-DPS-154 No.20
Vol.2013-CSEC-60 No.20
2013/3/14

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

金子紀之[†1]　　佐々木良一[†2]

近年，国や企業を狙った標的攻撃が増加してきており，大きな脅威となっている．標的型攻撃とはコンピュータシステムやインターネットを利用し，標的のコンピュータやネットワークへ侵入，そこからデータの詐取や破壊，改ざんを行い，システムを機能不全に陥らせる行為である．それらについて対策を検討することの必要性が高まっているが，対策を無闇に講じたところで，それらが生み出す効果が有用であるとは言い難い．また，リスク対策が新たなリスクを生み出す派生リスクの問題などが存在してしまう．そのため，対策コストと効果を考慮した上で最適な対策の組み合わせを求めることのできるツールの確立が必要であると考える．本研究は，イベントツリー分析法に基づく手法ならびにツールの開発を行うとともに，2011年に起きた衆議院への標的型攻撃事件への適用を行ったものである．

Development of evaluation tool based on the event tree analysis and its application to the cyber attacks

NORIYUKI KANEKO[†1]　RYOICHI SASAKI[†2]

Recently, target attacks aiming at the countries and companies have become a major threat. The target attack has behaviors that invade the Internet or computer systems and bring fraud, corruption of data or system down. Although the necessity of the measures against such attack is increased, it is very difficult to determine optimal measures, because not only the effectiveness of the measures but the cost and the derivation risk. Therefore we developed the method and the related tool to obtain the optimal combination of measures considering the cost and the derivation risk are necessary. This paper deals with the support tool based on the Event Tree Analysis and the application to the target attack to the House of Representatives in 2011.

1. はじめに

近年，情報技術の発展・普及に伴い，様々な問題が発生している．そのような中で，国や企業を狙った標的型攻撃が増加してきており，大きな脅威となっている．

標的型攻撃とはコンピュータシステムやインターネットを利用し，標的のコンピュータやネットワークへ侵入，そこからデータの詐取や破壊，改ざんを行い，システムを機能不全に陥らせる行為である．不特定多数の人達が標的とされていることや，特定の組織や集団が標的とされることもある．その為，目的次第では誰もが標的となってしまう可能性がある．それらの行為が日本国内を含む世界中で，著しく増加してき，標的型攻撃が日常化してきている．その為，こういった標的型攻撃について対策を検討することの需要が高まっている．アメリカでは表１のように年々件数が増加している．

表１　標的型攻撃発生件数
Table 1

（セクター）	2009 年（9）	2010 年(41)	2011 年 (198)
水道	33%(3)	5%(2)	41%(81)
エネルギー	33%(3)	44%(18)	16%(31)
複合部門	22%(2)	15%(8)	25%(49)
ダム	11%(1)	2%(1)	NA
核・原子力	NA	12%(5)	5%(10)
科学	NA	7%(3)	5%(9)
政府機関	NA	5%(2)	6%(11)
重要インフラ	NA	5%(2)	1%(1)
その他	NA	NA	5%(5)

しかし，標的型攻撃の対策を考えることは難しく，無闇に講じたところで，それらが生み出す効果が有用であるとは言い難い．さらにリスク対策が新たなリスクを生み出す派生リスクの問題などが存在する．そのため，コストやリスク低減効果や派生リスクを考慮した上で対策を検討することが必要であると考える．

本研究はイベントツリー分析法に基づく手法ならびにツールの開発を行うとともに，2011 年に起きた衆議院への

†1 東京電機大学
Tokyo Denki University.

†2 東京電機大学
Tokyo Denki University

ⓒ 2013 Information Processing Society of Japan

Vol.2013-DPS-154 No.20
Vol.2013-CSEC-60 No.20
2013/3/14

標的型攻撃事件[1][2][3][4]への適用を行ったものであり，種々のケースにおける最適な対策組み合わせを明らかにしている．

2. 多重リスクコミュニケータ(MRC)

2.1 MRC 概要

本研究の先行研究として，多重リスクコミュニケータ(MRC)が存在する．MRC は，ＩＴリスク上の多重リスク問題を解決するために開発された演算ツールである．フォルトツリー分析(FTA: Fault Tree Analysis)などを用いて，発生確率やリスクの分析を行なっている．複数の意思決定関与者の合意形成を支援するために，種々の評価指標を考慮しつつ，対策案の最適な組合せを求める機能をもつ[5][6].

2.2 MRC の問題点

MRC ではフォルトツリー分析(FTA: Fault Tree Analysis)を用いて分析をし，演算を行なっている．そのため，イベントツリー分析に適した問題への適応はそのままでは難しいと考えられる. MRC の適用方法を改良するアプローチも考えられたが，自由度を確保するため本研究では MRC を使用せずに研究を進めることとした．

3. 衆議院への標的型攻撃

3.1 事件の概要

2011 年 8 月，衆議院議員を標的とした，標的型メール攻撃が行われ，3 人の議員の公務用パソコンがウイルスに感染した．そのことが起点となり，衆議院の議員，秘書，職員が使っているサーバが標的型攻撃を受けた[2].
結果的に，2700 人の ID やパスワードが窃取されている．

本事件は，日本国内で注目度が高く，標的型メール攻撃という主流の手段が用いられているため，本研究の分析の対象とした[7].

3.2 事件の流れ

本事件は，標的型メールが 3 台の議員端末に送信され，うち 1 台の議員端末において，添付ファイルを開封，実行しウイルスに感染したことにより発生している．

その後，感染した議員端末から，この端末の ID，パスワード， キーボード入力情報が窃取された．

次に，窃取された情報を利用し，議員用アカウントサーバに管理者権限で不正ログオンされ，議員用アカウントサーバに不正なプログラムが埋め込まれた. このことにより，議員用アカウントサーバ，議員用運用管理端末，がウイルスに感染し，全議員の ID とパスワード情報が流出することとなった．

更に，議員用アカウントサーバに埋め込まれた不正プログラムにより，議員用アカウントサーバにログオンしたほかの議員端末に不正プログラムがコピーされ，25 台の議員端末がウイルスに感染することとなった．

上記が，本事件の一連の流れとなっている．

4. イベントツリー分析

4.1 イベントツリー分析とは

イベントツリー分析(ETA：Event Tree Analysis)とは，原子力産業で使われていた分析手法であり，現在では幅広い分野で使用されている[8].

利点として，ツリーの枝をたどるように分析を行うことにより，自己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ことが挙げられる．

4.2 イベントツリー分析の適応

イベントツリー分析に基づき，衆議院への標的型攻撃事件の分析を行った．

本事件の分析では，初期事象から最終事象までを 1 次感染，2 次感染，3 次感染に分け分析を行うことにより，より分かりやすく状況が順を追って把握できるようにしている．

まず，1 次感染では初期事象である，標的型メールが 3 人の衆議院議員の持つ議員端末に届くところから，1 台の議員端末がウイルスに感染し，キーボード入力情報が窃取されるところまでとする．

次に，2 次感染では，上記の事象から，議員用アカウントサーバ及び議員用運用管理端末への感染までとする．

同様に，3 次感染では，上記の事象から，25 名の議員の議員端末への感染までとする．

これらの各感染事象を細分化し，イベントツリー分析に適応した．

4.3 イベントツリー分析における事象一覧

衆議院への標的型攻撃事件を分析し，細分化したことにより，事象を以下の表のようすることとした．これらの事象を用いて，イベントツリーを作成した．各事象は攻撃者側から見たものとなっている[7][8][9].

表 2　1 次感染事象一覧
Table 2　List of first infection events

1 次感染		
No.	事象	発生確率
1	議員に標的型メールが届き添付ファイルを開封する	３／年（0.0000000856／人・件・年）
2	マルウェアがアンチウイルスソフトに検知されない	0.567
3	Ｃ＆Ｃサーバへの感染報告送信に成功する	0.999
4	Ｃ＆Ｃサーバからベクターの受け取りに成功する	0.999
5	キーロガー攻撃に成功する	0.999

ⓒ 2013 Information Processing Society of Japan

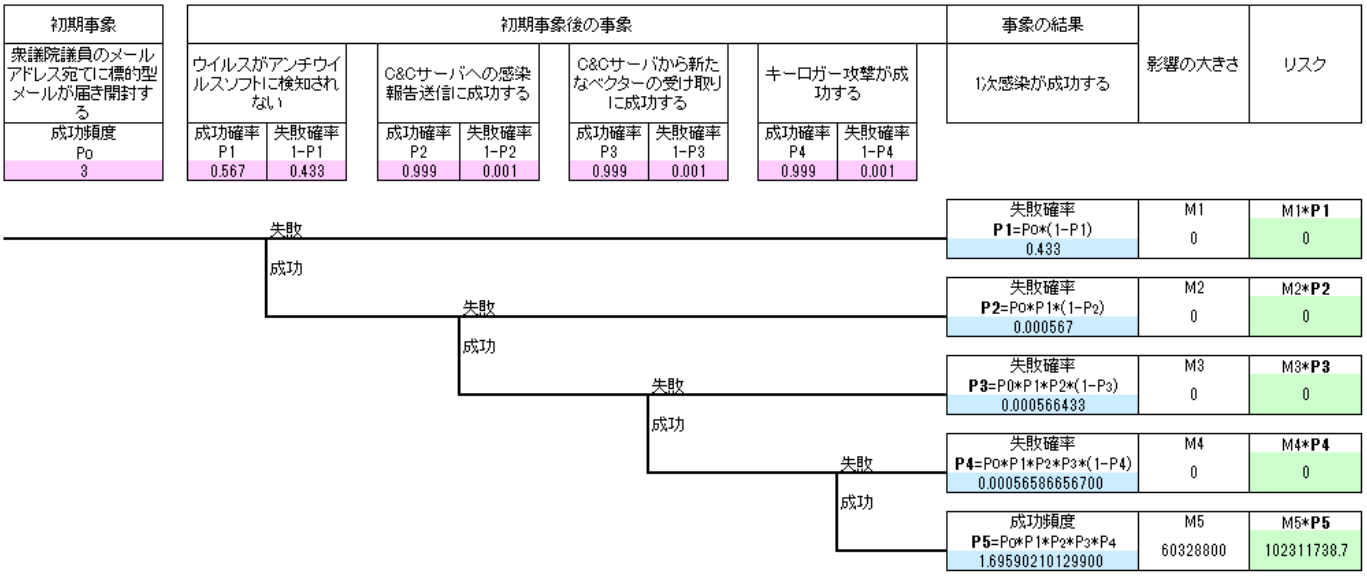


図 1　1 次感染イベントツリー
Figure 1　Event tree of first infection

1 次感染の事象をイベントツリーにまとめると，図 1 のような形となる．事象は初期事象，初期事象後の事象に分けられる．図 1 は 1 次感染が成功することが目的となるため，事象の結果は図 1 の通りとなる．影響の大きさは 1 次感染が成功した時点での，予想される影響値である．最終事象である 3 次感染への影響も考慮して決定した値である．

なお，２次感染と３次感染に関するエベントツリー分析結果は付録に示すとおりである．

表 3　2 次感染事象一覧
Table 3　List of second infection events

2 次感染		
No.	事象	発生確率
6	不正アクセスに成功する．	0.999
7	サーバ内を探査するマルウェアがアンチウイルスソフトに検知されない．	0.567
8	情報を外部に送信することに成功する．	0.999

表 4　3 次感染事象一覧
Table 4　List of third infection events

3 次感染		
No.	事象	発生確率
9	ログオンスクリプトの書き換えに必要なウイルスを埋め込むことに成功する．	0. 999

4.4 事象の発生確率

1. No.1 の事象

年間，480 人の衆議院議員の元に 1 日 200 件のメールが届くと仮定する．それらのメールを開き添付ファイルを開封する確率を考える．その際，本事件において，全議員の中から届いた標的型メールを開封し，添付ファイルを開封したのは 3 人であった．そのため，1 日 1 人当たり 200 件のメールが届き，480 人の衆議院議員のうち，3 人の議員が添付ファイルを開封する確率は表 2 の数値になる．

2. No.2 の事象

本研究において，全議員のパソコンにはアンチウイルスソフトが入っており，ウイルスチェックを自動で行うと仮定する．そのため，既知のウイルスはアンチウイルスソフトによって検出されると仮定するため，本研究では添付ファイルには未知のウイルスが仕組まれていたという流れで研究を行う．その際，未知のウイルスがアンチウイルスソフトに検出されない確率は表 2 の数値とする．

3. No.3，No.4，No.5 の事象

その後，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ため，表 2 の数値とする．

4. No.6 の事象

同様に，キーロガー攻撃が成功し，ID，パスワードが窃取されたとなると，不正アクセスはほぼ成功

ⓒ 2013 Information Processing Society of Japan

すると考えられるため，表 3 の数値とする．

5. No.7 の事象

その後，サーバ内を探査するためのマルウェアが用いられるのだが，ここでも，既知のマルウェアがアンチウイルスソフトによって検出されると仮定するため，未知のマルェアが使用されると仮定する．このときの確率は表 3 の数値とする

6. No.8 の事象

探査するマルウェアに感染してしまった場合，情報を外部に送信することはほぼ成功すると考える．よって，このときの確率は表 3 の数値とする．

7. No.9 の事象

最後に，ログオンスクリプトを書き換えるために必要なウイルスを埋め込むのに必要なマルウェアが用いられるのだが，ここでも，既知のマルウェアがアンチウイルスソフトによって検出されると仮定するため，未知のマルェアが使用されると仮定する．このときの確率は表 4 の数値とする．

5. 対策案の検討

5.1 対策案一覧

表5.　対策案の一覧
Table 5　List of proposed measures

No.	対策案	対策効果	プライバシー負担度	利便性負担度	対策対象事象
1	臨時セキュリティ研修の実施	0.1	0	2	1
2	定期的なセキュリティ研修の実施	0.4	0	4	1
3	イントラ等に不審メール情報について告知する	0.2	0	0	1
4	標的型不審メール訓練の実施	0.27	5	5	1
5	マルウェア対策支援サービスの導入	0.5	0	0	2,7,9
6	IDS･IPSの導入	0.5	5	0	3,4,6,8
7	パッチ適用による脆弱性対策	0.2			3,4,8
8	既知のスパイウェアの通信サイトとの通信をブロック	0.5	0	0	3,4
9	AppLockerの適用	0.5	0	0	3,4,8
10	ネットワーク監視	0.6	0	0	3,4,6
11	キーロガー検出ツールの適用	0.2	0	0	5
12	ウイルス対策ソフトの適用	0.57	0	0	5
13	スクリーンキーボードの使用	0.2	0	6	5
14	システムアップデート	0.6	0	0	6

対策案と対策案効果,派生リスク値は表 5 のように決定した．対策効果に関しては,値が 0.1 のときは,イベントツリーの対応する事象の発生確率を 1 割下げることができることを意味している．プライバシー,利便性とは,対策をとることにより発生する派生リスクであるプライバシー負担度,利便性負担度のことである．対象の数値は表 2,表 3,表 4 の項目に対応している．

5.2 対策案コスト

表6.　対策コストの一覧
Table 6　List of cost measures

No.	対策案	コスト（円）
1	臨時セキュリティ研修の実施	14,112,000
2	定期的なセキュリティ研修の実施	169,344,000
3	イントラ等に不審メール情報について告知する	500,000
4	標的型不審メール訓練の実施	1,580,000
5	マルウェア対策支援サービスの導入	4,560,000
6	IDS･IPSの導入	1,800,000
7	パッチ適用による脆弱性対策	4,560,000
8	既知のスパイウェアの通信サイトとの通信をブロック	1,854,720
9	AppLockerの適用	2,784,000
10	ネットワーク監視	5,205,000
11	キーロガー検出ツールの適用	500,000
12	ウイルス対策ソフトの適用	1,854,720
13	スクリーンキーボードの使用	500,000
14	システムアップデート	278,400

メール受信に関する対策として，SPF の導入などが考えられるが，衆議院では既に SPF がほぼ導入済みであるが，この方式の効果は他の組織や人がこの方式を採用するかどうかにかかっており，コントロールできないので対策から外した．

対策コストは衆議院議員 480 人を対象として計算をしている．基本的には，企業が提供しているサービスのデータ

ⓒ 2013 Information Processing Society of Japan

を利用してコストを決定している．

AppLocker の適用に関しては，Windows7 Enteprise, Ultimate, Windows8 Enterprise において利用可能となるため，それらの OS への新調コストとなっている[10][11][12][13][14][15][16].

6. 評価ツールの作成

6.1 評価ツールの概要

表 7　開発環境
Table 7　Development environment

開発 OS	Microsoft Windows 7 Professional
動作環境	Microsoft Office Excel 2007
開発言語	VBA

イベントツリー分析を使用し，分析した事象と，それらの事象に関する対策案の中から最も有効と考えられる最適解を算出するために評価ツールを作成した．

6.2 目的関数

最適解を算出する際の指標の数値として目的関数を設定する．目的関数値が低ければ低いほど良い結果であると考える．

本問題では下記のような式になる．

$$\mathrm{Min}\{\text{サイバー攻撃のリスク}+\text{対策コスト}\}(\text{円})$$

標的型攻撃のリスクは，標的型攻撃事象の発生頻度，その事象のもたらす影響の大きさにより設定している．

6.3 制約条件

最適解結果に制約を与えるために，制約条件を設定している．本問題の制約条件として，事象の発生頻度，対策コストの合計，対策案がもたらすプライバシー負担度，利便性負担度の合計を考慮している．

6.4 派生リスク

プライバシー負担とは，対策をとることによって発生する派生リスクであり，衆議院議員へのプライバシー侵害問題の影響値となる．

同様に，利便性負担度とは，衆議院議員への利便性の低下の影響値となる．

これらの値は 7 段階の段階的評価で値を決定している．

表 8　派生リスク値
Table 8　The value of the derived risk

数値	プライバシー負担度	利便性負担度
0	一切無い	一切無い
1	ほぼ無い	ほぼ無い
2	どちらかというと無い	どちらかというと無い
3	どちらでもない	どちらでもない
4	どちらかというと有る	どちらかというと低下する
5	プライバシーに影響がある	利便性が低下する
6	プライバシー負担に深く関わる	利便性が著しく低下する

6.5 演算方法

イベントツリー分析で分析した各事象の発生頻度，検討した対策案効果，対策案コスト，プライバシー負担度，利便性負担度の値を用いて，演算を行う．

各事象に関する対策案を採用しない，または 1 つ採用するという形式で全通りの演算を行い，制約条件値を考慮した上で，目的関数値を基に最適解を算出する．

7. 評価ツールの適応結果と考察

表 9　3 次感染最適解
Table 9　Optimal solution of third infection

3 次感染最適解		
	対策後	対策前
対策案	イントラ等に不審メール情報について告知する	-
	IDS･IPS の導入	-
	キーロガー検出ツールの適用	-
	システムアップデート	-
目的関数	5,553,402 円	57,894,792 円
発生確率	0.02（回/年）	0.544（回/年）
コスト	4,698,400 円	0
プライバシー負担度	7	0
利便性負担度	7	0

同様に，制約条件として，プライバシー負担度，利便性負担度の値を全体総数値の 48 の 3 分の 1 の値である，16 以下と設定して計算を行なっている．よって，これらの対策をとった際のプライバシー負担度，利便性負担度は比較的低い値であるといえる．

対策前の 3 次感染の発生頻度は 0.544（回/年）であるが，対策として，表 10 のような対策をとると，0.02（回/年）に抑えることが可能であると考える．

目的関数値は対策前の数値の約 8 分の 1 の値で抑えられることが可能であると考える．

表 10 のような対策案がとられたことから，意識向上のために日頃からイントラを利用した通知を行うことも必要であると考える．しかし，IDS・IPS を導入しつつ，システム

ⓒ 2013 Information Processing Society of Japan

のアップデートをすることが採用されたため，出口対策をとることも重要であると考える．

8. おわりに

本稿では，2011 年に起きた衆議院への標的型攻撃事件についてイベントツリー分析を行い，この事例に対する対策案の検討をし，作成した演算ツールを用いた対策案の考察結果について報告した．

今後は，色々な人にパラメータの値や制約条件に関するするデータを入れてもらい対策案の最適な組み合わせを求め対応に関する合意形成を図っていく．

また他の標的型攻撃事例の分析を行い，本研究の有用性を確かめつつ，評価ツールの更なる改良を目指していきたい．

謝辞

リスク分析に当たり東京電機大学の研究生だった木本裕司氏に種々の有益な意見をいただいたことに感謝申し上げる．

参考文献

1)佐藤直：通信ネットワークと情報セキュリティ，日本信頼性学会誌， http://ci.nii.ac.jp/naid/110008712162
2)木本裕司，佐々木良一：内閣官房情報セキュリティセンターが進める政府機関の情報セキュリティ施策，情報の科学と技術，http://ci.nii.ac.jp/naid/110009480282
3)内閣官房情報セキュリティセンター：政府機関等をかたる「なりすましメール」対策について，
http://www.nisc.go.jp/press/pdf/spf_press.pdf (2012).)
4)情報処理推進機構：標的型標的型攻撃の事例分析と対策レポート，
http://www.ipa.go.jp/security/fy23/reports/measures/，2013.1.24
5)佐々木良一，石井真之，日高悠，矢島敬士，古浦裕，杉村優子:『多重リスクコミュニケータの開発構想と試適用』情報処理学会論文誌，Vol.46，No8 (2005).
6)佐々木良一，日高悠，守谷隆史，谷山充洋，矢島敬士，八重樫清美，川島泰正，古浦裕：『多重リスクコミュニケータの開発と適用』情報処理学会論文誌 Vol49 No9 (2008)
7)衆議院サーバ等ウイルス感染事象について：衆議院サーバ等ウイルス感染防止対策本部，2011
8) 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/kagaku11.htm，(2013.1.24)
9)坊農豊彦， 長井壽満，橋本信彦：コンピュータ不正アクセスの脅威，情報処理学会研究報告，
http://ci.nii.ac.jp/naid/110002952317
10)株式会社ラック：IT セキュリティ予防接種，
http://www.lac.co.jp/service/campaign20120510_02.html，
(2013.2.16)
11)株式会社富士通ラーニングメディア：情報セキュリティ研修，
http://www.knowledgewing.com/kw/recommend/security.html?banner_id=g0010(2013.2.16)
12)Symantec：他社製品との比較
http://www.symantec-smb-solutions.com/jp/security_guide/compare(2013.2.16)
13)キャノン IT ソリューションズ株式会社：SniperIPS
http://canon-its.jp/product/ips/index.html，(2013.2.16)
14)ITmedia：標的型攻撃の“インテリジェンスを提供”、EMC がマルウェア支援サービス
http://www.itmedia.co.jp/enterprise/articles/1206/12/news073.html，(2013.2.16)
15)Vector：ノーロガー
http://www.vector.co.jp/soft/winnt/util/se337673.html，
(2013.2.16)
16)株式会社日立システムズ：総合セキュリティログ管理ソリューション SecureEagle／SIM，
http://www.hitachi-systems.com/solution/a0008/secure_eagle/index.html，(2013.2.16)

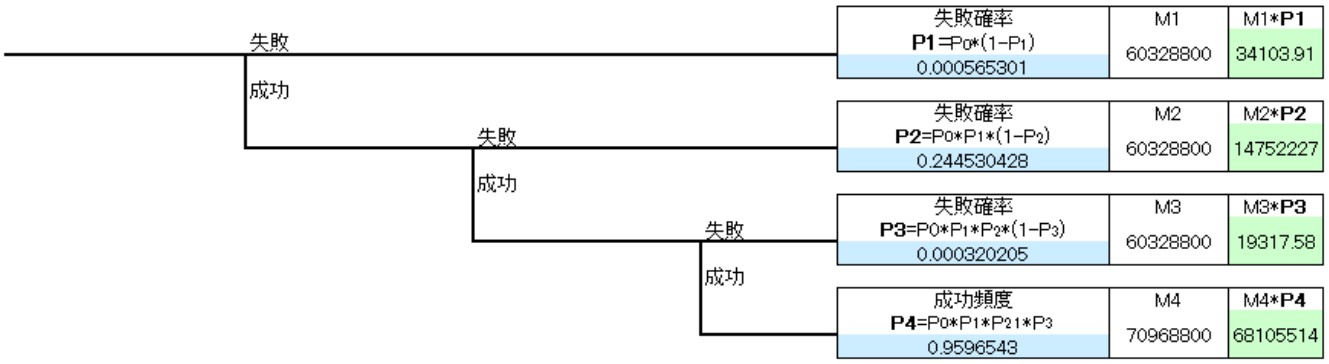
ⓒ 2013 Information Processing Society of Japan

Vol.2013-DPS-154 No.20
Vol.2013-CSEC-60 No.20
2013/3/14

付録

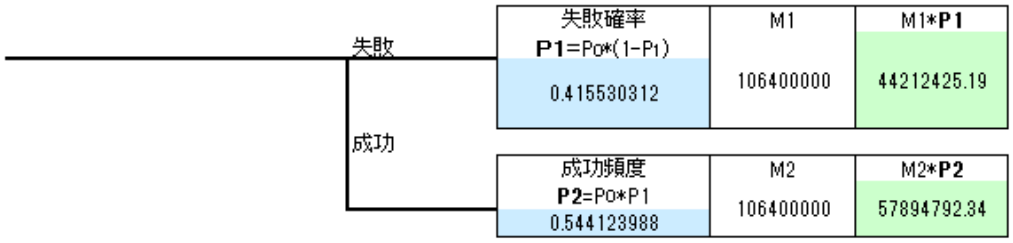
付録 A.1 2 次感染イベントツリー

初期事象	初期事象後の事象						事象の結果	影響の大きさ	リスク
1次感染が成功する	不正アクセスに成功する		サーバ内を探査するマルウェアがアンチウイルスソフトに検知されない		情報を外部へ送信することに成功		2次感染が成功する		
発生確率 P_0	成功確率 P_1	失敗確率 $1-P_1$	成功確率 P_2	失敗確率 $1-P_2$	成功確率 P_3	失敗確率 $1-P_3$			
1.6959021	0.999	0.001	0.567	0.433	0.999	0.001			



付録 A.2 3 次感染イベントツリー

初期事象	初期事象後の事象		事象の結果	影響の大きさ	リスク
2次感染が成功する	ログオンスクリプトの書き換えに必要なウイルスを埋め込むことに成功		3次感染が成功する		
発生確率 P_0	成功確率 P_2	失敗確率 $1-P_2$			
0.9596543	0.567	0.433			



ⓒ 2013 Information Processing Society of Japan