

標的型メール攻撃に対する計画・運用問題解決のための イベントツリーを用いた最適な対策案の選定手法の提案

橋本一紀^{†1} 比留間裕幸^{†1} 上原哲太郎^{†2} 松本隆^{†3} 佳山こうせつ^{†1}
柿崎淑郎^{†1} 八槇博史^{†1} 佐々木良一^{†1}

近年、特定の企業や組織を攻撃対象とする標的型メール攻撃が問題となっている。企業や組織は攻撃への複数の対策を求められているが、多くの問題があり対策を選定することは困難である。このような問題に対処するため、著者らは標的型メール攻撃問題について、LIFT システムの開発を行っている。しかし、このような対応を適切に行おうとしても、情報が取れる仕組みやログをとる仕組みをシステム計画時に組み込んでいなければ、良い対策をとることはできない。著者らは、適切な対策の組み合わせを求める方式として MRC の開発を行い、個人情報漏洩対策などに適用し有効性を証明してきた。しかし、標的型メール攻撃のように攻撃のシーケンスが長く、計画問題と運用問題の両方を考慮しつつ、最適な対策案の組み合わせを求める方式については未検討であった。本研究は標的型メール攻撃問題についてイベントツリー分析法を用いコスト制約の中で LIFT システムが最適に動作する場合のセキュリティ機器とログや情報の収集方法の組み合わせを求める方式について提案ならびに、標的型メール攻撃への適用を行ったものである。

Proposal of optimal selecting method for control strategy using the event tree to solve the planning and operating problems against targeted email attacks

KAZUKI HASHIMOTO^{†1} HIROYUKI HIRUMA^{†1} TETSUTARO UEHARA^{†2}
TAKASHI MATSUMOTO^{†3} KOSETSU KAYAMA^{†1} YOSHIO KAKIZAKI^{†1}
HIROFUMI YAMAKI^{†1} RYOICHI SASAKI^{†1}

1. はじめに

近年、特定の企業や組織を攻撃対象とする標的型メール攻撃が問題となっている。標的型攻撃とは、金銭や知的財産等の秘密情報の不正な取得を目的として特定の標的に対して行われるサイバー攻撃である[1]。その中でも、攻撃対象にメールを用いて攻撃を行う標的型メール攻撃が問題となっている。また、日本では国内の大手重工メーカーや衆議院が標的型メール攻撃の被害に遭っている[2]。

このような問題に対処するため、著者らは標的型メール攻撃問題について、事故発生時にネットワークログ等を適切に利用し、運用者が適切な対策をとれるようにするためのガイドシステムとして LIFT (Live and Intelligent Network Forensic Technologies:以下 LIFT) システムの開発を行っている[3][4]。しかし、このような対応を適切に行おうとしても、情報が取れる仕組みやログをとる仕組みをシステム計画時に組み込んでいなければ、良い対策をとることはできない。そのため、運用時の対応も考慮しつつ適切な対策の組み合わせを求める方式の開発が必要である。著者らは、リスクコミュニケーションを行い、複数の対策の最適な組

み合わせを求める多重リスクコミュニケーター (Multiple Risk Communicator:以下 MRC)である MRC の開発を行い、個人情報漏洩対策などに適用し MRC の有効性を証明してきた[5][6][7]。しかし、標的型メール攻撃のように攻撃のシーケンスが長く、計画問題と運用問題の両方を考慮しつつ、最適な対策案の組み合わせを求める方式については未検討であった。本論文では標的型メール攻撃問題についてイベントツリー分析法を用いコスト制約の中で LIFT システムが最適に動作する場合のセキュリティ機器とログや情報の収集方法の組み合わせを求める方式について提案する。

標的型攻撃については、標的型攻撃の検知の研究[8]、標的型攻撃自体を解明する研究[9]、標的型攻撃の予防的対策の研究[10]などがあるが、本論文で示すような研究は我々のグループ以外では行われていないと考える。また、同グループ内でイベントツリーを用いたリスク評価と標的型攻撃への適用が行われている。しかし、一般的な対策の検討であり、計画問題と運用問題を考慮していない部分と、フォレンジックの対応の部分が提案方式と差異がある[11]。

なお、本稿では、2章で用語の説明、3章で本研究室が開始した LIFT システムについて述べ、4章で提案方式を説明する。5章で提案方式の計画問題への適用を行い、6章で適用の結果と結果に基づいた考察について述べる。

^{†1} 東京電機大学
Tokyo Denki University

^{†2} 立命館大学
Ritsumeikan University

^{†3} ネットエージェント株式会社
Net Agent Company

2. 用語の説明

本稿で使用している用語の説明を表1にまとめる。

表1. 用語の説明

事象	標的型メール攻撃のシーケンスの一部で、被害者側で LIFT が検知できるもの。
兆候	LIFT が事象を推定するときに用いるもの。事象が発生した時に、人が気づけるものや機器のアラート、ログの異常となって現れるもの。
兆候 【大カテゴリ】	兆候を特定の種類で分類したもの。

3. LIFT

3.1 ネットワークフォレンジックとは

ネットワークフォレンジックとは、セキュリティ上の攻撃や問題を発生させるインシデントの発生源を発見するために、ネットワーク上のイベントをキャプチャ、記録、分析することである[12]。ネットワークフォレンジックに関連するツールとして SIEM (Security Information and Event Management : SEIM) が挙げられる。SIEM はセキュリティインシデントの予兆を発見・通知を行い、分析はセキュリティ技術者が行うことになっている[13]。そのため、優秀な運用者を持つ一部の企業でしか有用でないという問題がある。この問題を解決するため、ネットワークフォレンジックのインテリジェント化が重要となっている。

3.2 LIFT プロジェクトと LIFT システム

LIFTシステムとは、東京電機大学サイバー・セキュリティ研究所LIFTプロジェクト(図1参照)で開発を進めているシステムである。LIFTシステムは、ネットワークフォレンジック等を用いてインシデントを知的に対応できるようにするためのシステムである[3]。LIFTプロジェクトとは、LIFTシステム及び、関連するシステムを開発するためのプロジェクトである[4]。本研究はLIFTプロジェクトの計画支援システムに位置付けられるものである。

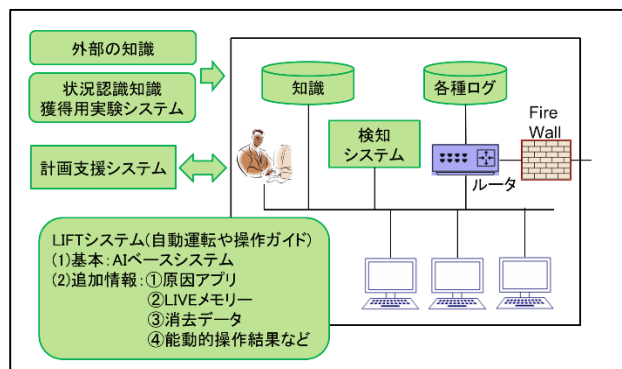


図1. LIFTプロジェクトの全体像

4. 提案方式

4.1 イベントツリー

4.1.1 イベントツリー分析とは

図2はヘディング項目が2つのイベントツリーのイメージ図である。イベントツリー分析(Event Tree Analysis: 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、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分析手法である[14]。

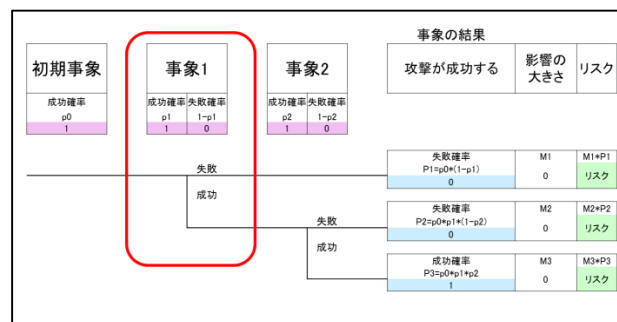


図2. イベントツリーのイメージ図

4.1.2 イベントツリーの事象

イベントツリーの事象は図3のようになるが、LIFTシステムの効果を分かりやすくするため、図4のように事象を発生事象と検知事象の2つに分割した。発生事象の成功確率は、事象が発生する確率や攻撃者が攻撃を試みる確率とする。検知事象の成功確率は、攻撃者側から見ての成功であり、LIFTシステムの検知部が適切な情報がないために事象を検知できない確率とする。

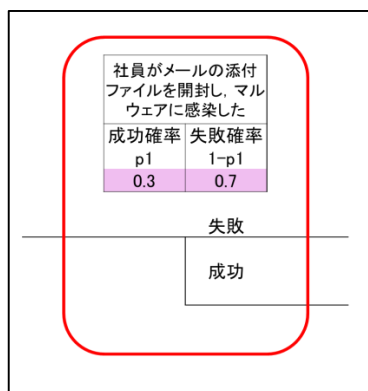


図 3. イベントツリーの事象

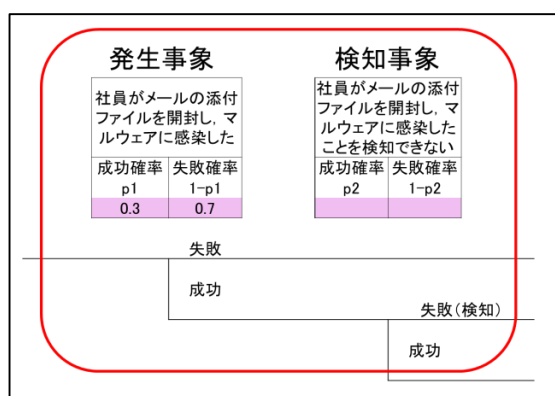


図 4. 提案方式でのイベントツリーの事象

4.1.3 発生事象の確率

発生事象の成功確率は、明らかである場合または、推定可能である場合ならばそのまま使用する。

例として、社員がメールの添付ファイルを開封し、マルウェアに感染したという事象をあげる。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。

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

なお、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 に近づくと推定できる[11]。

発生事象の成功確率が明らかでなく推定も難しい場合は、関係者の議論により確率を求める。

4.1.4 検出事象の確率

検出事象の成功確率は、採用する対策案によって変動する。

LIFT システムの検知部分は兆候から事象を推定する。事象と兆候【大カテゴリ】、兆候、対策の関係を図 5 に示す。対策を採用し、事象に対する兆候をどの程度捉えられるかを確率とする。具体的な確率は、表 2 を使用して求める。表 2 は事象に対する兆候の重要度をまとめた表である。兆候の重要度は、その兆候からの事象の推定のしやすさと対

策が兆候を捉えることができる確率の積である。事象の重要度の合計と対策の組み合わせが捉えられる兆候のみの事象の重要度の合計の割合を求める。これは検知が成功する確率である。成功確率は検知が失敗する確率なので、その割合を 1 から引いた値とする。

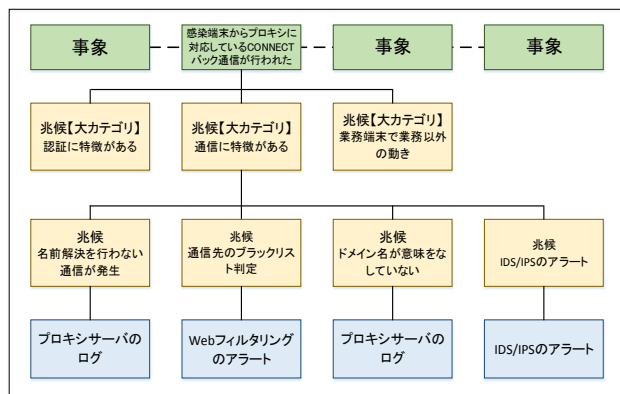


図 5. 事象と兆候と対策の関係

表 2. 事象徴候関連テーブル

事 象 \ 徴 候	名前解決を行わない通信が発生	通信先のブラックリスト判定	ドメイン名が意味をなしていない	IDS/IPSのアラート
感染端末から、プロキシに対応しているコネクトバック通信が行われた	3.0	0.4	1.0	0.3
新たなマルウェアを追加でダウンロードされ、感染端末にインストールされた	0	0	0	0
感染端末からネットワーク情報の収集が行われた	0	0	0	3.0

4.2 イベントツリーでのリスクの計算方法

イベントツリーでのリスクの計算方法を以下に示す[15]。

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

l は l 番目のシーケンスを表す。

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

i は i 番目のヘディング項目を表す。

H はヘディング項目数を表す。

P_i は i 番目のヘディング項目の分岐確率を表す。

$$P_i = ((1 - \bar{p}_i)(1 - y_i) + \bar{p}_i \cdot y_i) \cdots (3)$$

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

$$R = \sum_{i=1}^H R_i \cdots (4)$$

R_i は、式(1)に示すように、シーケンスごとのリスクであり、ここでは危殆化確率 P_i と影響 M_i の積で表している。

P_i は、式(2)に示すように、初期事象 P_0 と各ヘディング項目の発生確率の積で表すことができる。式(3)に示すとおり、 P_i は、各ヘディング項目が、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。

R はシーケンスごとのリスクを全て合計した値である。この値を標的型メール攻撃のリスクとする。

4.3 最適な対策案を求める手順

標的型メール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) 最適化問題としての定式化
- (2) イベントツリーの作成
- (3) 対策案のリストアップ
- (4) 最適化問題のパラメータや制約条件値の入力
- (5) 最適解の求解

5. 評価ツールの適用

5.1 評価ツール

前項の内容を定式化し、対策案の組み合わせの評価を行うツールを作成した。開発環境は表3に示す。

表3. 開発環境

開発OS	Microsoft Windows 7 Professional
動作環境	Microsoft Office Excel 2010
開発言語	VBA

5.2 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

Min{標的型メール攻撃のリスク} (円)

Subject To $\sum_{i=1}^K C_i X_i \leq C_t$ (イニシャルコスト)

$\sum_{i=1}^K D_i X_i \leq D_t$ (ランニングコスト)

標的型メール攻撃のリスクは、標的型メール攻撃の事象の成功確率とその事象のもたらす被害の大きさにより設定している。 X_i は0-1変数で $X_i=1$ の時に対策案*i*を採用、 $X_i=0$ の時に不採用とする。

5.3 最適化問題としての定式化

ここでは基本的な標的型メール攻撃を想定し、適用を行うための定式化を行う。攻撃対象として想定した組織を表4に示す。想定した組織で稼働しているサーバはWEBサーバ、メールサーバ、プロキシサーバ、DNSサーバ、DHCPサーバ、DBサーバ、ファイルサーバとした。

表4. 想定した組織情報

組織情報	
組織カテゴリ	EC会社 (B to Cモデル)
社員数	180人
PC数	200台
顧客数	30,000人
平均支払額	10,000円
取り扱っている個人情報	クレジットカード情報 携帯電話番号、住所、氏名

5.4 イベントツリーの作成

イベントツリーの事象は標的型メール攻撃で行われているシーケンスを議論し、初期事象含め10個採用した。採用した事象を以下に示す。この採用した事象を発生事象と検知事象に分けイベントツリーを作成した。

・標的型メール攻撃のイベントツリー

初期事象.社員がマルウェアの添付されたメールを受信した

1. 社員がメールの添付ファイルを開封し、マルウェアに感染した
2. 感染端末から、プロキシに対応しているコネクタバック通信が行われた
3. 新たなマルウェアを追加でダウンロードされ、感染端末にインストールされた
4. 感染端末内のシステム情報を収集された
5. 感染端末からネットワーク情報の収集が行われた
6. マルウェアの配布を行い、侵入を拡大された
7. 新たに感染した端末からサーバへの侵入をされた
8. サーバ内の重要な情報を収集された
9. 感染端末から機密情報を暗号化せずに外部へ送信された

5.5 対策案

採用した対策案は表5に示す。また、それぞれの対策にイニシャルコスト (万円) とランニングコスト (万円/月)、効果を設定する。

表 5. 採用した対策案

対策 No	名称	イニシャルコスト (万円)	ランニングコスト (万円/月)
1	web サーバのログを取得する	1	5
2	メールサーバのログを取得する	1	2
3	プロキシサーバのログを取得する	1	5
4	DNS サーバのログを取得する	1	1
5	DHCP サーバのログを取得する	1	1
6	DB サーバのログを取得する	1	2
7	ファイルサーバのログを取得する	1	1
8	業務端末のログを取得する	36	45
9	運用端末のログを取得する	4	10
10	ネットワーク機器のログを取得する	1	5
11	インターネットファイアウォールを導入する	90	3
12	IPS/IDS を導入する	256	5
13	Web フィルタリングを導入する	228	10
14	ウイルス対策ソフトを導入する	246	8
15	ゼロデイ対策ソフトを導入する	160	14

5.6 最適化問題のパラメータや制約条件値

制約条件を表 6 に示す。イニシャルコストの制約条件を 400 (万円) から 100 (万円) 刻みに 3 つ設定した。また、ランニングコストの制約条件を 90 (万円/月) から 10 (万円/月) 刻みに 3 つ設定した。イニシャルコストの制約条件 500 (万円)、ランニングコストの制約条件 100 (万円/月) を基準点とする。

表 6. 制約条件まとめ

制約条件 No	イニシャルコスト (万円)	ランニングコスト (万円/月)
1	600	110
2	600	100
3	600	90
4	500	110
5	500	100
6	500	90
7	400	110
8	400	100
9	400	90

5.7 被害の大きさの算出

被害の大きさは復旧費用や売上の損失、会社の信頼低下による損失、顧客へのお詫びを想定した組織情報を基に、関係者で議論し算出した。標的型メール攻撃が全て成功した時の被害の大きさは、392,328,767円である。

6. 適用結果と考察

6.1 適用結果

表 7 は評価ツールを使用した結果である。基準点における目的関数の値は 5,412,062 円で、採用された対策案はプロキシサーバのログを取得する、ファイルサーバのログを取得する、業務端末のログを取得する、運用端末のログを取得する、ウイルス対策ソフトを導入する、ゼロデイ対策ソフトを導入するであった。また、ランニングコストの制約条件による対策案の差異はなかった。

表 7. 適用結果

制約条件 No	対策案	目的関数 (円)
1	3,7,8,9,11,14,15	5,412,061
2	3,7,8,9,11,14,15	5,412,061
3	3,7,8,9,11,14,15	5,412,061
4	3,7,8,9,14,15	5,412,062
5	3,7,8,9,14,15	5,412,062
6	3,7,8,9,14,15	5,412,062
7	3,7,8,9,15	7,734,616
8	3,7,8,9,15	7,734,616
9	3,7,8,9,15	7,734,616

6.2 考察

採用された対策案から、セキュリティ機器による入り口対策だけではなく、ログを取得し攻撃者の攻撃を検知することが重要だと分かった。標的型メール攻撃のリスクを軽減するためには、LIFTシステムを導入し端末や攻撃対象になりやすいサーバのログの取得を行い、早期の攻撃検知を行うことが重要だと言える。

7. おわりに

本稿では、標的型メール攻撃問題についてイベントツリー分析法を用いコスト制約の中でLIFTシステムが最適に動作する場合のセキュリティ機器とログや情報の収集方法の組み合わせを求める方式について提案と標的型メール攻撃への適用を行った。

今後の展開として、実際のシステムを対象にLIFTシステムに組み込んだ場合の運用実験と評価を行う。また、ネットワークの構造やログの保存方法、コストの算出方法を考慮しつつ評価を行っていくことが挙げられる。

謝辞

本研究に際して、様々なご指導を頂きました LIFT プロジェクトの関係者に深謝いたします。また、日常の議論を通じて多くの知識や示唆を頂いた情報セキュリティ研究室の皆様に感謝します。

参考文献

- 1) Symantec, 「標的型攻撃」に備えるーサイバー攻撃：標的型攻撃とは、APTとは、
<http://www.symantec.com/ja/jp/theme.jsp?themeid=apt_insight>
- 2) IPA独立行政法人情報処理推進機構, 標的型サイバー攻撃の事例分析と対策レポート,
<<http://www.ipa.go.jp/files/000024536.pdf>>
- 3) 佐々木 良一, 上原 哲太郎, 松本 隆, 標的型攻撃に対するネットワークフォレンジック対策の現状と今後の展望, 情報処理学会コンピュータセキュリティシンポジウム2013(CSS2013), (2013)
- 4) 比留間 裕幸, 橋本 一紀, 柿崎 淑郎, 八槨 博史, 上原 哲太郎, 佳山 こうせつ, 松本 隆, 佐々木 良一, 標的型メール攻撃に対する知的ネットワークフォレンジックのための予兆検知と対策方法の提案, マルチメディア、分散、協調とモバイルシンポジウム2014(DICOMO2014), (2014)
- 5) 谷山 充洋, 佐々木 良一, 多重リスクコミュニケーターの教育方法の提案と分析, 日本セキュリティ・マネジメント学会学会誌, Vol.22, No.3, pp.3-14 (2008)

- 6) 谷山 充洋, 日高 悠, 荒井 正人, 甲斐 賢, 伊川 宏美, 矢島 敬士, 佐々木 良一, 多重リスクコミュニケーターの企業向け個人情報漏洩問題への適用, 日本セキュリティマネジメント学会誌VOL.23, No.2, pp34-51
- 7) 守谷 隆史, 千葉 寛之, 佐々木 良一, 内部統制のための多リスク・多関与者を考慮した費用対効果の評価法の提案と適用, 日本セキュリティマネジメント学会誌Vol.22, No.3, pp3-14
- 8) 榊原 裕之, 河内 清人, 桜井 鍾治, ログ分析によるサイバー攻撃の検知について, 暗号と情報セキュリティシンポジウム(SCIS2014), (2014)
- 9) 松川 博英, 標的型攻撃の解析から見える攻撃全体動作と通信シーケンス, 電子情報通信学会技術研究報告(ICSS), 情報通信システムセキュリティ 112(91), 49, (2012-06-14)
- 10) 木村 壮太, メール攻撃危険予知訓練システムの開発, 情報処理学会研究報告(CSEC), 2013-CSEC-63(4), 1-6, (2013-12-02)
- 11) 石井 亮平, 金子 紀之, 佐々木 良一, 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, 情報処理学会コンピュータセキュリティシンポジウム 2013 (CSS2013), (2013)
- 12) デジタル・フォレンジック研究会, 証拠保全ガイドライン第3版の解説 - デジタル・フォレンジック研究会 ,
<<http://www.digitalforensic.jp/eximgs/20131114gijutsu.pdf>>
- 13) 日立ソリューションズ, SIEMとは ,
<<http://securityblog.jp/words/714.html>>
- 14) 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>>
- 15) 藤本 肇, 上田 祐輔, 佐々木 良一, 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, 情報処理学会論文誌 VOL.49, No.3, pp1105-1118, (2008-03-15)