Computer Security Symposium 2017
23 - 25 October 2017

標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発と機能拡張（その 2）
- 対策案優先度評価法 -

島﨑 一樹[†1]　勅使河原 可海[†1]　柿崎 淑郎[†1]　佐々木 良一[†1]

概要：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．このような攻撃に適切に対処するため，著者らは，ログ分析と人工知能などを用いて対策をガイドするシステムである LIFT（Live and Intelligent Network Forensic Technologies）の開発並びに機能拡張を行っている．本システムは，収集したログの分析を行い，攻撃の徴候を検知し，人工知能技術を利用して，攻撃事象を推定し，攻撃事象に基づく応急対策の指示を行う．しかし，応急対策の候補はいろいろある．そこで本稿では，種々の対策案の効果推定値と対策コストをベースに対策優先度を推定する方式を提案する．併せて，本方式を用いて対策を決定した場合の長所を示す．

キーワード：デジタルフォレンジック，ネットワークフォレンジック，標的型攻撃，対策評価

Development and enhancement of intellectual network forensic system LIFT against targeted attacks (Part2)
- Proposed countermeasure priority evaluation method -

Kazuki Shimazaki[†1]　Yoshimi Teshigawara[†1]　Yoshio Kakizaki[†1]　Ryoichi Sasaki[†1]

Abstract: Recently, the number of targeted attacks to specific organizations, such as companies or governments, has been increasing. To solve such problem, the authors have developed and enhanced LIFT（Live and Intelligent Network Forensic System）which is a system to guide countermeasures using log analysis and artificial intelligence etc. The system analyzes collected logs, detects signs of attacks, estimates attack events using artificial intelligence techniques, and instructs emergency measures based on attack events. However, there are various candidates for emergency measures. Therefore, in this paper, we propose a method to estimate countermeasure priority based on effect estimation value of various countermeasures and countermeasure cost. In addition, we show the advantages when deciding countermeasures using this method.

Keywords: Digital Forensic, Network Forensics, Targeted attack, Countermeasure evaluation

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（以降，標的型攻撃と呼ぶ）が問題となっており，日本では国内の大手旅行会社や日本年金機構などが被害に遭っている[1].

標的型攻撃は，長期間にわたり段階的な攻撃が継続して行われるという特徴がある．また，事前準備段階での偵察により，標的の弱点を調べ上げた上で攻撃が実施されるため，侵入段階で防ぐことは困難である[2]. さらに，標的型攻撃を検知するためには複数のログやアラートの相関を見る必要があり，対応者には高度なセキュリティ技術が求められる．これに対して，著者らは対応者の能力に依存せず，適切な応急対応とログの保全が行えるよう支援するシステムとして LIFT（Live and Intelligent Network Forensic Technologies）システムの開発並びに機能拡張を行っている[3].

LIFT システムでは初めに，収集したログの分析を行い攻撃の徴候を検知する．次に，検知した攻撃の徴候を基に，人工知能技術を用いて攻撃事象を推定し，攻撃事象に基づく応急対策の指示を行う．そこで本稿では，LIFT システムが最適な応急対策案の提案を行うための手法を提案する．

標的型攻撃を受け，端末から不正な通信を検知した際には，「該当端末 IP の通信遮断」や「該当端末のネットワーク隔離」といった応急対策の実施が検討される．しかし，「該当端末のネットワーク隔離」や「該当端末の停止」といった応急対策は無闇に実施すると通常通りの業務が行えなくなる可能性や，証拠保全のための情報が減るといった問題がある．そのため，応急対策を実施する際には対策によって生じる悪影響を考慮する必要がある．

まず，第 2 章で用語説明と評価対象とする対策の定義，第 3 章で関連研究について述べる．第 4 章で対策案の効果推定値と対策コストを考慮した応急対策の優先度評価方式を提案し，第 5 章で提案手法に基づいた応急対策の優先度評価結果を示す．第 6 章で関連研究と比較した全体の考察

†1 東京電機大学
Tokyo Denki University

を述べ，最後に第 7 章で今後の展望を含めたまとめを述べる．

2. 用語の説明

表 1 に本稿で使用している用語の説明をまとめる．

表 1　用語の説明
Table 1　Explanation of terms.

用語	説明
攻撃事象	標的型メール攻撃のシーケンスの一部で，被害者視点において攻撃者の攻撃行動を表したもの． 例：マルウェアが C&C サーバとの通信を行う
徴候	攻撃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．

2.1 評価対象とする対策

標的型攻撃に対する対策はその目的に応じて対策の種類が多岐にわたる．そのため，全ての対策を同一の指標で評価することは困難であると考える．本節では本稿で評価対象とする「応急対策」の定義を明確にする．

標的型攻撃から情報システムを防御するための対策に関する理解促進を目的として，総務省より文献[4]が公開されている．文献[4]では，標的型攻撃に対する技術的対策を以下の 3 パターンに分類している．（以下引用）

(1)　事前対策

被害を未然に防ぐ，又は攻撃者の攻撃コストを高め被害に遭いにくくするための対策を実施する．

(2)　検知

事前対策をすり抜けた攻撃を認知するためにシステムログに残される痕跡（IOC：Indicator of Compromise）を分析し，標的型攻撃を検知する．

(3)　事後対策

事後対策はさらに以下の 2 パターンに分類される．

A)　暫定対処

標的型攻撃の被害拡大の防止／抑制のための初動対処

B)　本格対処

標的型攻撃による被害の全貌分析／特定

本稿では，(3) 事後対策における暫定対処のための対策を「応急対策」と定義し，優先度評価を行う．例として，表 2 に特定の端末において攻撃事象「マルウェアが C&C サーバとの通信を行う」が発生した際の応急対策の候補を示す．

表 2　攻撃事象と応急対策の例
Table 2　Examples of attack events and emergency measures.

攻撃事象	マルウェアが C&C サーバとの通信を行う
応急対策 1	該当ドメイン・IP へのアクセス遮断
応急対策 2	該当端末のネットワーク隔離
応急対策 3	該当端末が所属するネットワークの隔離

3. 関連研究

本章ではまず，事前対策の選定に着目した関連研究について述べる．次に，応急対策に関する既存の対策選定手法とその問題点について述べる．

佐々木らは，主に事前対策の選定手法としてリスク，コストと業務への影響を考慮した対策選定手法を提案している[5]．本提案手法を用いることで対策による業務への影響を十分に評価することができると考える．しかし，対策による業務への影響を評価するためには対象とする組織で業務分析を行い，業務一つ一つのプロセス数や実行時間などを詳細に定義する必要がある．組織にとって詳細な業務分析は大きな手間となり，業務や情報システムが変化する度に再定義が必要となる．

標的型攻撃を受けた際に行う対策の選定手法として，佐藤らは攻撃者と防御者の戦略をゲーム理論的にモデル化し，動的に意思決定する手法を提案している[6]．また，橋本らはイベントツリーを用いて最適な対策案を選定する手法を提案している[7]．

しかし，[6]で提案されている手法では，攻撃策の実施コストを対策選定時に利用しているが，これは被害組織の環境や攻撃手法によって大きく変動することが想定される．また，応急対策の有効性や対策選定時に利用する評価指標の評価値を算出する手順が十分に示されていない．

また，[7]で提案されている手法では，応急対策実施のための組織の金銭的な負担額を主な評価指標として最適対策を算出しているが，金銭的な負担額は対象とする組織の環境により大きく変動することが想定される．また，[6]と同様に対策の有効性を算出する手順が十分に示されておらず，対策の有効性が対策選定時に考慮されていない．

応急対策一つ一つに対して評価を行った例として，文献[4]では暫定対処策を実施した場合の C（機密性），I（完全性），A（可用性）の影響を考慮し，暫定対処策を CIA の 3 項目を用いて 3 段階で評価している．本評価法によって，暫定対処策がもたらす情報資産の影響を推定することができる．

しかし，CIA を用いた文献[4]中の評価法では以下の 3 つ

の課題があると考える．

(1) 類似する対策や包含関係にある対策が存在すること

応急対策の中には，対策目的が類似している対策が含まれている．例えば，「端末のネットワーク隔離」と「端末の停止」の対策の主目的は端末の悪性活動を止めることであることが多い．そのため，一方の対策が実施されている場合にもう一方の対策を実施する意味は薄くなる．

また，応急対策には包含関係にある対策があり，対策 A を包含している対策 B が実施されている場合，対策 A を実施する意味は無いと言える．

(2) 評価結果が曖昧であること

対策対象に応じてユーザ，エンドポイント，セグメントと別々に CIA による評価を行っているため，対策対象間で評価を比較することができない．

また，評価が 3 段階であるため同一の評価となっている対策が多い．そのため，対策間の相違点が不明瞭になり，対策の意思決定者がどの対策を選択すればよいか分からなくなることが想定される．

(3) 攻撃段階に応じて応急対策が挙げられていない

応急対策の有効性は，攻撃段階に応じて変化すると考える．しかし，対策が攻撃段階と対応付けられていないため，現在の攻撃段階で該当の対策が有効であるかが不明確となっている．

本稿では以上の課題を緩和および解決する応急対策の優先度評価方式を提案する．

4. 提案方式

本章ではまず，応急対策の優先度評価の基本的考え方と前提条件について述べる．次に，4.1 節で優先度評価方法の概要を述べ，4.2 節および 4.3 節で評価指標の算出方法について述べる．また，4.4 節では応急対策間の包含関係に対する考え方を示す．

本稿では応急対策の優先度付けを，応急対策ごとに算出した評価値を用いて行う．また，評価値の算出は標的型攻撃が発生する前に行う．そして，標的型攻撃が発生した際は推定された攻撃事象に応じて評価値が高い順に応急対策を示し，それを応急対策の優先順位とする．

また，本稿では応急対策の評価値を，応急対策の内容や実施時の組織への影響を考慮して算出する．しかし，対策内容や組織への影響は，対象とする組織の規模や提供しているサービスの内容によって大きく変化するという問題がある．そのため，本稿で想定している組織の環境を以下と仮定する．

- ネットワーク及び端末数が小規模～中規模の組織
- 事務処理などで業務にインターネットを用いる
- 応急対策を行う対応者がネットワークや情報システムに対する基礎的な知識を有している
- サービスの中心がインターネットを用いたものではない（サービスとしてクラウドを提供する等）

4.1 優先度評価方法

提案する応急対策の優先度評価は特定の攻撃事象が発生した場合における，その攻撃事象に対する該当対策の評価値を算出することにより行う．評価値の算出には 2 項目の評価指標を用いる．以下に評価指標の定義を示す．

(1) 対策効果推定値

対策効果推定値は，応急対策が特定の攻撃事象に対してもたらす影響の規模を示す指標である．

(2) 対策コスト

対策コストは，応急対策を実施した際に発生が予想される業務への影響や損失の規模を示す指標である．本稿では，対策実施時に機材の導入費や運用費が十分に小さい応急対策を評価対象とし，前述の費用は対策コストに含まないものとする．

また，図 1 に優先度評価方法全体のフローを示す．

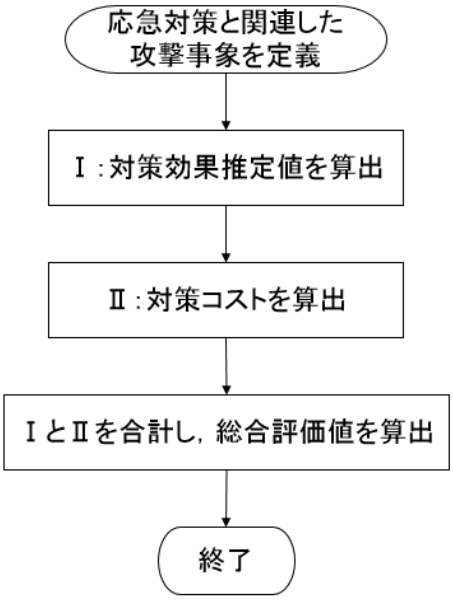

図 1　優先度評価方法フローチャート

Figure 1　Flowchart of priority evaluation method.

図 1 中のⅠとⅡの評価値算出方法の詳細については以下の節で述べる．

I.　対策効果推定値（4.2 節）

II.　対策コスト（4.3 節）

ここで，(1) と (2) 共に評価値が「高いほど」該当の評価指標の面から見て応急対策が優れていることになる．

また，本稿では総合評価値を算出する際，ⅠとⅡの比率を 2 パターン用意して検討を行っている．詳細については 5.3 節で述べる．

4.2 対策効果推定値の算出方法

対策効果推定値を算出する方法の一つとして，応急対策によって標的型攻撃全体に対してどの程度被害拡大の防止や抑制が行えるかを基準にする方法が考えられる．しかし，この方法で算出可能な対策効果推定値は，攻撃者視点における評価値であるため被害者側から算出することは困難であり，多くの推測に基づいて算出されることとなる．

そこで本稿では，応急対策を実施した際に現在発生している攻撃事象が抑制される可能性，すなわち攻撃事象に対する応急対策の成功確率を対策効果推定値として算出する．本手法では被害者側から見た攻撃者の攻撃行動である「攻撃事象」に対して評価を行うため，準定量的な評価を行うことができる．

次に，応急対策の成功確率を基に対策効果推定値を算出するための式を示す．応急対策 m の成功確率を PS_m とし，最高値を 100 とした場合の対策効果推定値 E_m は式(1)によって算出することができる．また，応急対策の成功確率は応急対策の失敗確率を用いて算出することができる．応急対策の失敗確率を PF_m と置き，攻撃パターン i における攻撃失敗パターンを F_i および失敗パターンの発生確率を PF_i と置くと，n 個の失敗パターンを持つ応急対策の成功確率は式(2)と表すことができる．

$$E_m = PS_m \times Max \quad \cdots(1)$$

ここで，$Max = 100$

$$PS_m = 1 - PF_m \quad \cdots(2)$$

$$= 1 - \sum_{i=1}^{n} PF_i$$

応急対策の失敗確率は該当の攻撃事象が発生する攻撃行動のパターンを可能な限り列挙し，全てのパターンにおいて評価対象とする応急対策が攻撃事象の抑制に繋がるか否かを検討して算出する．また，本稿では「対策失敗」および「失敗パターン」を以下のように定義する．

- 対策失敗の定義
  ある攻撃パターンによって攻撃事象が発生した場合，応急対策が攻撃事象の抑制に役立たない，あるいは攻撃者が応急対策を容易に回避可能と想定される場合

- 失敗パターンの定義
  対策失敗時において攻撃者がとった攻撃行動

ここで，成功確率算出の例として攻撃事象「攻撃者が攻撃基盤から他の端末へ侵入し，攻撃基盤を増やす」における応急対策「パスワードの変更」を検討する．

まず，攻撃事象に対して該当対策が有効であることを確認する．応急対策「パスワードの変更」を攻撃者が遠隔操作をしている端末に対して行った場合，攻撃者に対して該当端末の再認証が求められる．ここで，攻撃者が該当端末の初回認証をブルートフォース攻撃やパスワードリスト攻撃を用いて突破していたと仮定する．応急対策によって該当端末のパスワードを使い回していない強固なものに変更した場合，再認証を初回認証時と同一の攻撃手法で突破することは難しくなる．よって，仮定した場合において応急対策「パスワードの変更」は有効であると言える．

続いて，本攻撃事象が発生する別の攻撃行動のパターンとして，攻撃者が初回認証の際に上記の攻撃手段を用いない場合を検討する．例えば，以下の 2 パターンが考えられる．

I. 脆弱性を突き，認証を回避して攻撃基盤を操作した
II. パスワードダンプツールを用いた

ここで，上記のパターンにおいて応急対策「パスワードの変更」が有効であるかを検討する．

Ⅰの場合，認証そのものを回避しているのでパスワードを変更する意味はないと言える．同様にⅡの場合も検討する．

標的型攻撃時に攻撃ツールとして使用が報告されているパスワードダンプツールに mimikatz がある[8][9]．mimikatz を利用することで端末の管理者権限を所持していれば攻撃者は容易にパスワードハッシュを入手することができる．そのため，攻撃者が認証の際にパスワードハッシュを用いた場合，パスワードを変更する意味は殆どないと言える．

これにより，ⅠとⅡの攻撃パターンにおいて，応急対策「パスワードの変更」は失敗すると言える．また，本対策の成功確率は式(2)で述べた通り，1 から上記の攻撃パターンの発生確率を合計したものの差をとったものになる．

上記に述べた通り，対策効果推定値は 4.2 節の式(1)および式(2)を用いることで算出できる．しかし，失敗時の攻撃パターンの発生確率を定量化するために，攻撃事象が発生する攻撃パターンを可能な限り列挙することは容易ではないと考える．そこで本稿では，対策の成功確率を専門家による討議により設定した，表 3 の 5 段階の評価指標を用いて算出することとする．

表 3　応急対策の成功確率評価指標

Table 3　Success probability evaluation index of emergency measures.

点数	成功確率の評価指標
100 点	きわめて高い（失敗パターンがまずない）
80 点	高い（確実に何かしらの効果がある，攻撃者が応急対策を回避することは困難）
50 点	中程度（失敗パターンがある）
25 点	低い（失敗パターンが多い）
10 点	きわめて低い（失敗パターンが非常に多い）

4.3 対策コストの算出方法

対策コストの算出は後述する 5 つの評価項目を用いて行う．対策コストを算出するための評価項目は複数考えられるが，本稿では対策を実施する組織の環境による依存が比較的小さい 5 つの項目とした．また，評価項目による業務への影響や損失の変動量を考慮し，専門家による討議により直接評価法を用いて評価項目ごとに重要度を 10 段階で評価した．表 4 に評価項目と重要度を示す．

- 直接評価法

  直接評価法とは全評価項目の重みを同時に直接的に決定する方法であり，一対比較法と比べて煩雑な計算を伴わないというメリットがある[10].

表 4　対策コスト算出時の評価項目と重要度

Table 4　Items and significance for estimating countermeasure cost.

評価項目名	重要度
対策の影響範囲	**7**
対策による影響の大きさ	**5**
対策実施に要する時間	3
対策の複雑さ	2
消滅の可能性がある攻撃の痕跡	3

以下に表 4 中の各評価項目の詳細を示す．

A)　対策の影響範囲

応急対策を実施することによって何らかの影響が生じる端末やネットワークの範囲を表す．

B)　対策による影響の大きさ

応急対策による対策対象への影響の大きさを表す．例として，対策対象がネットワーク機能の一部または全部である場合，失われる情報量や可用性を考慮して「通信の遮断（小規模）」「通信の遮断（中規模）」「通信の遮断（大規模）」の 3 パターンに分けられる．

C)　対策実施に要する時間

応急対策の「作業開始～作業完了」までの時間を表す．「作業完了～効果発現」までの時間は含めないものとする．

D)　対策の複雑さ

応急対策の目的のわかりやすさ（一般性）と対応者への対策手順の説明の必要性を表す．

E)　消滅の可能性がある攻撃の痕跡

応急対策を実施することによって消滅する可能性がある攻撃の痕跡を表す．

4.3.1 対策コストの算出手順

以下に対策コストの算出手順を記す．

①　応急対策を表 4 の評価項目に基づいて詳細化

応急対策の実施手順や手間などを具体化し，表 4 の評価項目により評価可能な段階まで詳細化する．

②　評価項目ごとの評価値を算出

表 4 の 5 項目の評価値算出には，項目ごとに用意した評価基準を用いる．本稿では，専門家による討議により表 6～表 12 の通りに各評価項目における評価基準を設定した．

③　表 4 の評価項目間の重要度を割合に変換

表 4 の評価項目間の相対的な重要度を基に，全体における各評価項目の割合を算出する．4.3.2 節に算出方法を述べる．

④　評価項目ごとの評価値を総計し，総合評価値を算出

②より算出した評価項目ごとの評価値に表 5 の割合を乗じ，和をとることで対策コストの総合評価値を算出する．

4.3.2 評価項目の割合の算出

表 4 における各評価項目の割合は，該当評価項目の重要度を全体の重要度で除することで算出できる．算出結果を表 5 に示す．また，例として図 2 に評価項目「対策の影響範囲」の割合を求める過程を示す．

表 5　対策コスト算出時の評価項目の割合

Table 5　Items and rate for estimating countermeasure cost.

評価項目名	割合
対策の影響範囲	**35 %**
対策による影響の大きさ	**25 %**
対策実施に要する時間	15 %
対策の複雑さ	10 %
消滅の可能性がある攻撃の痕跡	15 %

例:「対策の影響範囲」の割合

$$= \frac{7}{7+5+3+2+3} \times 100$$

$$= 35(\%)$$

図 2　評価項目の割合の算出例

Figure 2　Containment relationship among emergency measures.

表 6　対策の影響範囲の評価基準

Table 6　Standard for evaluating influence range of countermeasures.

	単独の端末	ネットワークの一部	ネットワーク全体
点数	25 点	70 点	100 点

表 7　対策による影響の大きさの評価基準_1

Table 7　Standard for evaluating scale of impact by countermeasures 1.

	パスワード変更	プロセス停止	対象の隔離	対象の停止
点数	10 点	10 点	80 点	100 点

表 8　対策による影響の大きさの評価基準_2

Table 8　Standard for evaluating scale of impact by countermeasures 2.

	通信の遮断（小規模）	通信の遮断（中規模）	通信の遮断（大規模）
点数	10 点	30 点	60 点

表 9　対策実施に要する時間の評価基準

Table 9　Standard for evaluating time required for implementing countermeasures.

	極短（自動実行可能）	短	普通	長	極長
点数	10 点	25 点	50 点	75 点	100 点

表 10　対策の複雑さの評価基準（一般性）

Table 10　Standard for evaluating the complexity of countermeasures (Generality).

	一般的	非一般的	深い専門知識を有する
点数	10 点	30 点	50 点

表 11　対策の複雑さの評価基準（対策手順の説明）

Table 11　Standard for evaluating the complexity of countermeasures (Explanation of countermeasure procedure).

	不要（自動実行可能）	ほぼ必要なし	必要
点数	0 点	15 点	50 点

表 12　消滅の可能性がある攻撃の痕跡の評価基準

Table 12　Standard for evaluating traces of attacks that could potentially disappear.

	なし	マルウェア	揮発性情報	殆どの情報
点数	0 点	25 点	80 点	100 点

4.4　応急対策間の包含関係

応急対策間には包含関係が存在するため, 対策選定時には既に実施されている対策に応じて対策候補を減らす必要がある．これは，あらかじめ応急対策の包含関係を定義しておき, 対策 A を包含している対策 B が実施されている場合，対策の候補から対策 A を外すことで LIFT システムへの実装が可能であると考える．また，類似した応急対策に関してもあらかじめ対策の目的を定義しておくことで候補から外すことができると考える．

図 3 に応急対策間の包含関係を示す.

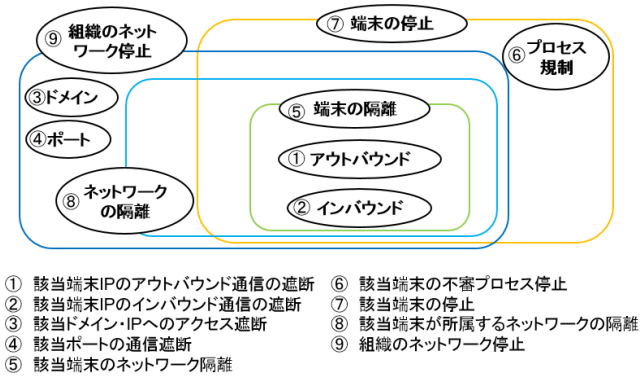

図 3　応急対策間の包含関係

Figure 3　Containment relationship among emergency measures.

5.　適用結果

4 章の提案方式に基づいて攻撃事象における応急対策の総合評価値をそれぞれ算出する．ここで，算出した総合評価値を比較することにより，攻撃事象における応急対策の優先順位付けを行うことができる．

5.1　対策効果推定値の算出

対策効果推定値は，4.2 節の式(1)および式(2)を用いて算

出することが望ましいが，4.2 節末尾で述べた通り本稿では表 3 を用いて対策効果推定値を算出する．図 4 に対策効果推定値を算出した結果を示す．

事象＼対策	パスワードの変更	該当端末IPのアウトバウンド通信の遮断	該当ドメイン・IPへのアクセス遮断	該当ポートの通信遮断（ハイポート）	該当端末のネットワーク隔離	該当端末の不審プロセス停止	該当端末の停止	該当端末がネットワークの隔離	組織のネットワーク停止
マルウェアが添付されたメールが届く									
社員がメールに添付された不正プログラムを起動する					100	25	100	100	100
マルウェアがC&Cサーバとの通信を行う		50	100	50	100		100	100	100
必要な機能のダウンロード			80	50	100		100	100	100
攻撃基盤の端末の中の情報を入手する						25	100		
攻撃者が攻撃基盤から内部ネットワークを探索する		25			80		80	100	100
攻撃者が攻撃基盤から他の端末へ侵入し、攻撃基盤を増やす	10							100	100
攻撃者が攻撃基盤からサーバへ侵入する	10							100	100
端末の破壊						25			
機密情報の送信		50	80	50	80		80	100	100

図 4　対策効果推定値の算出結果（一部抜粋）

Figure 4　Calculation result of countermeasure effect estimation value (Excerpt).

5.2 対策コストの算出

対策コストは 4.3.1 節の算出手順に基づいて算出した．図 5 に対策コストの算出結果を示す．

	割合	0.35	0.25	0.15	0.10	0.15	1.00	
自動実行	対策名	範囲	影響の大きさ	時間	複雑さ	痕跡消滅	合計	評価値
不可	パスワードの変更	25	10	25	25	0	17.5	82.5
可	該当端末IPのアウトバウンド通信の遮断	25	30	10	30	25	24.5	75.5
可	該当ドメイン・IPへのアクセス遮断	70	10	10	10	25	33.3	66.8
可	該当ポートの通信遮断（ハイポート）	70	30	10	10	25	38.3	61.8
可	該当端末のネットワーク隔離	25	80	10	10	25	35.0	65.0
可	該当端末の不審プロセス停止	25	10	10	30	25	19.5	80.5
可	該当端末の停止	25	100	10	10	80	48.3	51.8
不可	該当端末が所属するネットワークの隔離	70	80	50	25	25	58.3	41.8
不可	組織のネットワーク停止	100	100	75	25	25	77.5	22.5

図 5　対策コストの算出結果（一部抜粋）

Figure 5　Calculation result of countermeasures cost (Excerpt).

5.3 総合評価値の算出

5.1 節と 5.2 節で算出した対策効果推定値と対策コストを総計し，応急対策の総合評価値を算出する．ここで，総計の際には「対策効果推定値」と「対策コスト」の比率を検討する必要がある．比率が不適切であると，総合評価値が一方の評価指標による評価値に大きく依存することとなり，もう一方の評価指標が適切に考慮されなくなる．そのため本節では，表 13 に示す 2 パターンにおいて総合評価値を算出すると共に，2 パターンを比較した考察を述べる．

表 13　対策効果推定値と対策コストの比率

Table 13　Ratio of countermeasures effect estimate value to countermeasures cost.

	比率 対策効果推定値：対策コスト	満点
パターン A	1：1	200 点
パターン B	1：**2**	300 点

5.3.1 算出結果

図 4 の対策効果推定値の算出結果に対し，図 5 の対策コストの算出結果の最終列を表 13 の比率を用いて総計した．図 6 にパターン A における総合評価値の算出結果，図 7 にパターン B における総合評価値の算出結果をそれぞれ示す．

算出結果より，パターン A およびパターン B において「社員がメールに添付された不正プログラムを起動」した場合，点数が最も高い「該当端末のネットワーク隔離」が最も推奨される応急対策であり，点数が最も低い「該当端末の不審プロセス停止」は非推奨であることが示されている．

事象＼対策	パスワードの変更	該当端末IPのアウトバウンド通信の遮断	該当ドメイン・IPへのアクセス遮断	該当ポートの通信遮断（ハイポート）	該当端末のネットワーク隔離	該当端末の不審プロセス停止	該当端末の停止	該当端末がネットワークの隔離	組織のネットワーク停止
マルウェアが添付されたメールが届く									
社員がメールに添付された不正プログラムを起動する					165	106	152	142	123
マルウェアがC&Cサーバとの通信を行う		126	167	112	165		152	142	123
必要な機能のダウンロード			147	112	165		152	142	123
攻撃基盤の端末の中の情報を入手する						106	152		
攻撃者が攻撃基盤から内部ネットワークを探索する		101			145		132	142	123
攻撃者が攻撃基盤から他の端末へ侵入し、攻撃基盤を増やす	93							142	123
攻撃者が攻撃基盤からサーバへ侵入する	93							142	123
端末の破壊						106			
機密情報の送信		126	147	112	145		132	142	123

図 6　総合評価値算出結果_パターン A（一部抜粋）

Figure 6　Comprehensive evaluation value calculation result _ pattern A (Excerpt).

事象＼対策	パスワードの変更	該当端末IPのアウトバウンド通信の遮断	該当ドメイン・IPへのアクセス遮断	該当ポートの通信遮断（ハイポート）	該当端末のネットワーク隔離	該当端末の不審プロセス停止	該当端末の停止	該当端末がネットワークの隔離	組織のネットワーク停止
マルウェアが添付されたメールが届く									
社員がメールに添付された不正プログラムを起動する					230	186	204	184	145
マルウェアがC&Cサーバとの通信を行う		201	234	174	230		204	184	145
必要な機能のダウンロード			214	174	230		204	184	145
攻撃基盤の端末の中の情報を入手する						186	204		
攻撃者が攻撃基盤から内部ネットワークを探索する		176			210		184	184	145
攻撃者が攻撃基盤から他の端末へ侵入し、攻撃基盤を増やす	175							184	145
攻撃者が攻撃基盤からサーバへ侵入する	175							184	145
端末の破壊						186			
機密情報の送信		201	214	174	210		184	184	145

図 7　総合評価値算出結果_パターン B（一部抜粋）

Figure 7　Comprehensive evaluation value calculation result _ pattern B (Excerpt).

5.3.2 考察

パターンAとパターンB共に全ての応急対策で総合評価値を算出し，応急対策の優先度付けを行うことができた．しかし,パターンAとパターンBの算出結果を比較すると，パターンAにおいて「該当端末が所属するネットワークの隔離」と「組織のネットワークの停止」の応急対策が他の応急対策と同程度の評価値となっていることが確認できる．通常，上記の応急対策は組織の業務に甚大な影響をもたらすため，他対策の実施後に最終手段として実施が検討されるものである．そのため，パターンAでは対策効果推定値と対策コストの比率が不適切であると考えられる．

一方,パターンBはパターンAと比較して前述の応急対策の評価値が他対策より概ね低くなっており．パターンAにおける問題点が解消されている．また，対策コストの比率を高めたことにより，対策コストが総合評価値に大きく依存し，対策効果推定値が考慮されない問題の発生について検討する．ここで，図7を見ると関連する攻撃事象に対して応急対策の失敗パターンが多い応急対策である,「パスワードの変更」や「該当端末の不審プロセス停止」に対し，対策コストが高めであるが失敗パターンが少ない応急対策である,「該当端末のネットワーク隔離」や「該当端末が所属するネットワークの隔離」が評価値を上回っている．これにより，対策コストだけではなく対策効果推定値も総合評価値の算出時に考慮されていると考える．

6. 全体の考察

本提案方式によって，関連研究で述べた課題の緩和および解決を果たすことができたと考える．提案方式では応急対策による業務への影響を，対策コストの一部として端末やネットワーク機能の可用性を考慮して評価した．これにより，本稿で想定する組織の環境を満たしている場合，業務分析を行わずとも業務への影響を部分的ではあるが考慮することができると考える．また，本稿では関連研究で算出手法が明記されていなかった，応急対策の有効性を算出するための一手法を提案し，対策選定時に考慮することに成功している．さらに，本評価手法は単純であるかつ標的型攻撃を受ける前段階で,評価値を算出することができる．そのため，本評価手法を実装するLIFTシステムは関連する事象の推定時に評価値の高い順に対策を表示するだけの,早急な応急対策選定を行うことができる．

また，文献[4]での課題点であった3項目に関しても提案方式で概ね解決できたと考える．しかし，さらに良いものにしていくには，実システムを対象とし，LIFTを実際に動かす実験結果を反映していく必要がある．

7. おわりに

本稿では，標的型攻撃の攻撃事象を抑制するために行う応急対策の対策効果推定値と対策コストに焦点をあて，応急対策の優先度評価方式を提案した．また，関連研究における複数の課題の緩和および解決を果たすことできた．

今後は，実システムを対象とし，本方式を組み込んだLIFTシステムを実際に動かすことで評価･改良を行っていきたい．

謝辞 本稿に際して，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．

参考文献

[1] 日本経済新聞：「標的型メール」対策急務 JTBで顧客情報流出，日本経済新聞（オンライン），入手先.〈http://www.nikkei.com/article/DGXZZO03723210X10C16A6000000/〉（参照 2017-2-25）.

[2] トレンドマイクロ：標的型サイバー攻撃とは - 脅威と対策，トレンドマイクロ（オンライン），入手先.〈http://www.trendmicro.co.jp/jp/security-intelligence/threat-solution/apt/index.html〉（参照 2017-2-25）.

[3] 鈴木文仁，上原哲太郎，名和利夫，佳山こうせつ，村上弘和，堀添裕太，佐々木良一：標的型攻撃に対する知的ネットワークフォレンジックシステムLIFTの開発と機能拡張（その1）-LIFTの全体像-，CSS2017.

[4] 総務省：サイバー攻撃（標的型攻撃）対策防御モデルの解説（詳細版）（別紙3），総務省（オンライン），入手先.〈http://www.soumu.go.jp/main_content/000495298.pdf〉（参照 2017-8-15）.

[5] 佐々木剛史，西村啓渡，加藤弘一，勅使河原可海：セキュリティ，コスト，業務への影響を考慮した対策選定手法の検討，CSS2010，pp.381-386（2010）.

[6] 佐藤直，渡邉均：サイバー攻撃・防御戦略の動的意思決定モデルの提案，ICSS2011，pp.49-54（2011）.

[7] 橋本一紀，比留間裕幸，上原哲太郎，松本隆，佳山こうせつ，柿崎淑郎，八槇博史，佐々木良一：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，DICOMO2014，pp.991-996（2014）.

[8] JPCERT/CC：インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書，JPCERT/CC（オンライン），入手先〈https://www.jpcert.or.jp/research/ir_research.html〉（参照 2017-08-15）.

[9] GitHub - gentilkiwi/mimikatz: A little tool to play with Windows security（online），available from〈https://github.com/gentilkiwi/mimikatz〉(accessed 2017-08-25).

[10] 国土交通省：Taro10-評価の方法に関する解説，国土交通省（オンライン），入手先.〈http://www.mlit.go.jp/kisha/kisha02/13/130830/130830_4.pdf〉（参照 2017-8-27）.