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—ユーザインタフェースの開発と評価—

杉原峻介[1] 橋本一紀[1] 比留間裕幸[1] 上原哲太郎[2] 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．この攻撃は現状対策するのが困難である．そこで著者らは高い技術力を持たない組織でもインシデント発生時に，人工知能を用いて適切な応急対応を支援するための LIFT (Live and Intelligent Network Forensic Technologies）システムの研究開発を行っている．本研究は，LIFT システムの管理者が適切な対処ができるようにするための分かりやすく使いやすいユーザインタフェースの検討を行い，実際に開発を行ったものである（JAVA で約 6000 ステップ）．適用実験とその評価により実用の見通しが得られたので報告する．

Development of intellectual network forensic system LIFT against targeted attacks - Development and evaluation of user interface for LIFT -

RYOSUKE SUGIHARA[1] KAZUKI HASHIMOTO[1] HIROYUKI HIRUMA[1]
TETSUTARO UEHARA[2] RYOICHI SASAKI[1]

1. はじめに

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，攻撃対象に攻撃対象にメールを用いて行う標的型メール攻撃が問題となっており，日本では年金機構や三菱重工が被害に遭っている．さらに，これらに対応する高い能力を持つセキュリティ技術者が全体を通して不足している現状もある．

これらの問題に対応する為に，著者らは2013年度後期に東京電機大学のサイバー･セキュリティ研究所内でLIFT プロジェクトを立ち上げ，プロジェクト内でLIFT (Live and Intelligent Network Forensic Technologies:以下LIFT) システムの研究開発を行ってきた[2]． 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に知的に対応できるようにするシステムである．

本研究ではLIFTシステムに初心者でも理解しやすいユーザインタフェースを追加し，管理者が攻撃者からの攻撃に対し，適切な対処ができるようにするための手法の提案を行う．

本稿では，２章でLIFTシステムについて述べ，３章で先行研究について述べる． ４章でLIFTシステムの機能と先行研究の問題点からLIFTシステムユーザインタフェースの要件を抽出する．５章で開発環境と開発した画面を示した後，６章で適用をし，７章で結果考察を行う．最後に８章で今後の展望を含めたまとめを述べる．

1 東京電機大学
Tokyo Denki University
2 立命館大学
Ritsumeikan University

2. LIFT について

2.1 標的型メール攻撃について

標的型メール攻撃とは，攻撃対象の組織にメールに添付したファイルを開かせたりメールに記述したURL踏ませたりして，マルウェアに感染させ標的組織へ侵入し，機密情報の窃取を行う攻撃である[1][6][7]．最近では，標的型メール攻撃は，社会の脅威と認識されており，日本では三菱重工や日本年金機構などの組織が攻撃を受け多大な被害を出している．

標的型メール攻撃の検知は，マルウェアの検知と標的型メールのブロックが最も効果的である．しかし，標的型メール攻撃で使用されるマルウェアは，ウィルス対策ソフトでは検知できないことが多い．また，標的型メールは，組織に関連する情報やメールの送信者を偽装し本物のメールと勘違いさせたり，何度かやり取りをしてメール送信者を安心だと信頼させたりする方法がある[8] [9]．そのため，標的型メールのブロックやメールを受け取った人がメールを開かないといった対策は困難である．そこで，組織に侵入された後や内部に侵入を拡大させている時にも検知できるようにすることが必要になってきていると考える．

2.2 LIFT プロジェクトについて

2013年度後期に東京電機大学サイバー・セキュリティ研究所内に設置されたプロジェクトである．LIFTプロジェク

トの概要図を図1に示す.本プロジェクトは巧妙化する攻撃から高い技術力を持たない組織を守ること，攻撃の影響を軽減することを目的としている.

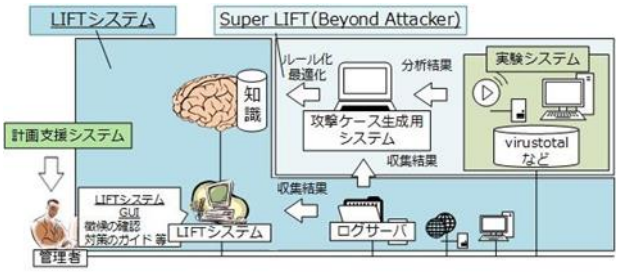


図1.　LIFTプロジェクトの概要図

2.3 LIFT システムについて

LIFT(Live and Intelligent Network Forensic Technologies：LIFT)システムとは，収集すべきログの管理や徴候から人工知能を用いて攻撃の推定，分析を自動で行い，高い技術力を持たない組織でもインシデント発生時に応急対応をできるようにすることを目的としたシステムである．図2にLIFTシステムの機能概略を示す．LIFTシステムでは，各ネットワーク機器や端末，検知ツールから攻撃事象における徴候を収集する．収集した徴候から徴候・事象関連テーブルを用いて攻撃事象を確定し，事象・対策関連テーブルを用いて有効な対策案の算出を行い，運用者へガイドラインを表示する．これにより，高い技術力を持たない組織であってもインシデント発生時に攻撃の影響を軽減するために適切な応急対応が行えるよう支援する.

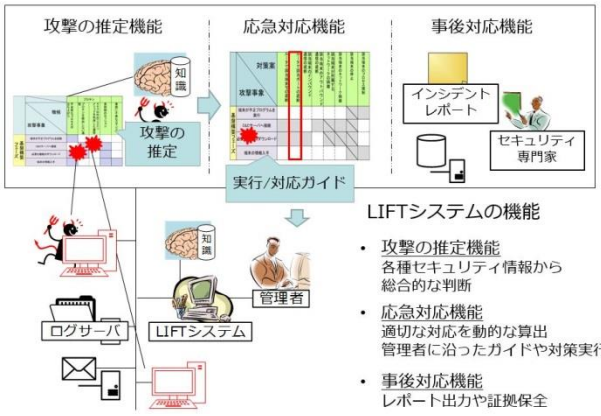


図２．　LIFTシステム機能概略図

2.4 LIFT システムの機能

LIFTシステムの機能を示す.

① 徴候から事象推定機能

LIFT システムは，検知した徴候から事象を推定する機能を持つ．事象を推定機能は，「徴候・事象関連テーブル」に書かれている事象毎の徴候の確信度と以下の数式を使用して推論を行っている.

$$\text{事象 P の確信度} = 1 - \prod_{i \in T} \left(1 - \text{徴候} P_i \text{の確信度}\right)$$

T=検知された徴候郡

事象Pの確信度が推定の閾値を超えた場合に，LIFTシステムは事象を推定したとする．しかし，先行研究の適用実験で複数事象を同時に推定する場合があることが判明した.そのため，プロジェクト内で「ベイジアンネットワーク」を使用した推定方法の検討が進んでいる[5].

② 自動証拠保全機能

LIFT システムは，事象の推定時にデータとログを自動的に証拠保全する機能を持つ．証拠保全を行うことで，セキュリティの専門家による本格的な原因究明を支援や，再発防止への本格的対策の検討の判断材料とすることができる.

③ 攻撃フェーズ推定機能

LIFTシステムは，推定された事象の前後に発生した関連する事象を調査する機能を持つ．関連する事象の徴候を調査し，新たに推論を行い関連する事象を推定する．また，関連する事象を推定することで組織への攻撃がどのぐらいの攻撃フェーズまで進んでいるかの判定を行う機能を持つ.

④ 対策選定機能

LIFTシステムは，推定された事象の応急対策を行う機能を持つ．対策の選択は，「事象・対策関連テーブル」に書かれている事象に有効な複数の対策から，検知された徴候の情報を基に行われる．対策の例として，事象「マルウェアがC2サーバとの通信を行う」への対策は，対策「感染端末の電源オフ」や対策「ルータによる感染端末の通信遮断」がある.

⑤ 対策実行機能

LIFTシステムは，対策を自動で実行する機能を持つ．また，対策の実行の自動・手動の切り替え等の設定が可能である．なぜなら，対策「感染端末が所属するネットワークの隔離」のような対策を自動で実行することは，業務トラブルが発生する可能性があるからだ．対策の実行に関する設定内容は自動で実行を行う，実行する前に管理者の許可を求めるようにする，管理者が手動で実行する，対策を選択対象としないがある．管理者が手動で実行する場合，LIFTシステムは対策方法のガイドを表示することが可能である．また，LIFTシステムは，対策によって攻撃が停止したかどうかの対策結果を推論の材料とする.

⑥ 管理者へのガイド表示機能

LIFTシステムは，対策方法や徴候の調査方法などのガイドを表示する機能を持つ．LIFTシステムは，高い能力を持つセキュリティ技術者でなくても扱えるという目的がある.そのため，LIFTシステムのGUIやガイドの表示方法に関して検討が進んでいる．本稿３章以降で主に扱うのはこの部分である.

⑦　管理者へのレポート出力機能

LIFTシステムは，管理者向けのレポートを出力する機能を持つ．レポートには，検知された徴候と推定した事象の情報が書かれている．また，攻撃フェーズ推定や対策が実行された場合，レポートに追加でフェーズと類似の攻撃ケースや対策の結果が書かれる．

2.5　用語の説明

LIFTシステムにおける用語の説明を示す．

(1)攻撃ケース(Attack case)

攻撃ケースは，過去に発生した攻撃の流れを表す．

(2)攻撃フェーズ(Attack phase)

攻撃フェーズは,標的型メール攻撃の進捗度合いを表す．攻撃フェーズは，IPAの標的型メール攻撃のシナリオ[10]を基に我々が作成した．攻撃フェーズを表1 に示す．侵入フェーズは，標的型メールを使用してPCをマルウェアに感染させ，組織に入り込もうとする段階である．基盤構築フェーズは，マルウェアを感染させたPCの内部の情報を窃取する段階である．内部侵入・調査フェーズは，内部ネットワークを探索し，管理端末やサーバに侵入し，攻撃者が扱うことができるPCを増殖させている段階である．目的遂行フェーズが,攻撃者が機密情報を窃取している段階である．

表１．　攻撃フェーズ

Table 1　　Attack phase

フェーズ	攻撃フェーズ
I	侵入フェーズ
II	基盤構築フェーズ
III	内部侵入・調査フェーズ
IV	目的遂行フェーズ

(3)事象(Event)

事象は，攻撃者が行う攻撃を表したものである．LIFTシステムは，事象の推定を行うことを目的とする．LIFTシステムは，推定した事象から攻撃フェーズの推定や攻撃者の行動の予測，応急対応の立案を行う．

(4)徴候(Clue)

徴候は，攻撃者が攻撃(事象)を行うことによって表れる結果である．例えば、事象「マルウェアがC2サーバとの通信を行う」を行った時に，プロキシを経由せずに通信をすれば，徴候「プロキシを経由しない通信」が発生する．また,業務や作業で使用されていないポートでhttpsの通信を行った場合は，徴候「443以外のCONNECTメソッドを利用した通信」が発生する．このように，事象と徴候は１対多の関連を持つ．また，徴候はログやアラートとなって組織のシステムに表れる．

(5)確信度

事象の確信度は，事象が発生している確率である．事象の確信度が高いほど，攻撃されている可能性が高いとLIFTシステムは判断する．徴候の確信度は，事象に対しての情報量である．徴候の確信度は，事象毎に付加されている．事象の確信度は，検知された徴候の確信度を基に計算される．

(6)ソース(Source)

ソースは,機器が出力するログやアラートのことである．

(7)テーブル

テーブルには，専門家の知見や資料，過去の攻撃の分析を基にした情報が書かれている．「徴候・事象関連テーブル」には，事象と徴候の関係とそれぞれの確信度が書かれている．「事象・対策関連テーブル」には，事象に有効な複数の対策が書かれている．

LIFTシステムにおける用語の構造を図2 に示す．

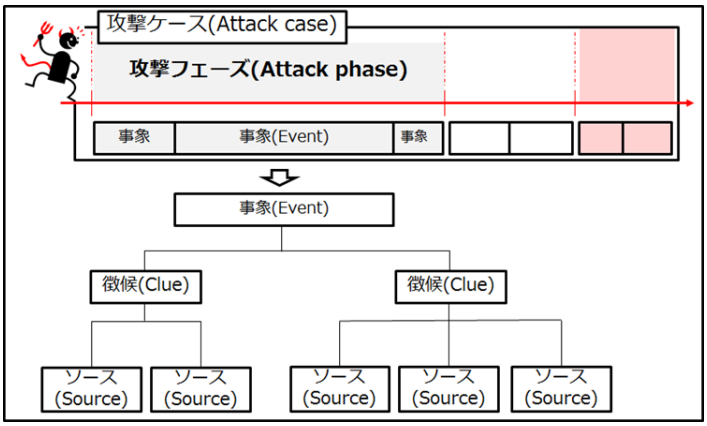


図3.　LIFTシステム用語の構造

3.　先行研究

同研究室の橋本・比留間による先行研究では，収集したログを基に徴候から事象を推定し，ガイドを管理者に表示し，管理者が適切な対処を行えるようなユーザインタフェースを開発した[3]．ユーザインタフェースの評価実験として，管理者として研究室の学生１０人にLIFTプログラムを利用してもらった．評価したものは表２である．

表2.　先行研究の評価実験の結果

項目名	評価
使いやすさ	3．4
見やすさ	2．9

各項目の評価指標は以下のようになっている．

・使いやすさ

5. 直感的に操作をしやすい

3. 説明を聞く，または，説明書を読めば操作を行うことができる，

1. 使い難いと感じる

・見やすさ

5. 直感的に情報を理解しやすい

3. 表示されている情報を理解しやすい

1. 表示されている情報が見難く，理解し難い

いずれも5が最大で1が最小である．

この研究の問題点として以下のようなものがあった．

(ア) 一度に表示されている情報量が多い

(イ) 出てきたウィンドウに対して管理者が適切に対処しにくい

4. 提案手法

4.1 LIFT システムユーザインタフェースの要件

2.3の⑥, ⑦からLIFTシステムユーザインタフェースの要件を抽出した.

A) 現在のシステムの状況を表示できる
B) LIFTシステムの動きが表示される
C) LIFTシステムからの指示を管理者に示すことができる

次に，先行研究の問題点アから要件Ⅰを問題点イから要件Ⅱを抽出した.

要件Ⅰ　LIFTシステムに表示する情報を選択できるようにする
要件Ⅱ　ウィンドウをユーザが能動的に開く様なものにする

4.2 デザインの参考

画面のGUIはintra-martのUIデザインガイドラインのUI基本方針を参考にデザインをしていく[4].

5. 開発

5.1 開発環境

開発環境を表３に示す.

表3.　開発環境

開発環境	NetBeans eclipse Javafx SceneBuilder
動作環境	Javaがインストールされている環境
開発言語	Java8

5.2 開発した画面

開発した画面を図４に示す．左上の丸は，実システムの状態を表している．通常状態では，緑色である．色は，事象の確信度が上がり基準値を超える毎に黄色，赤色へ変化する．これはLIFTシステムユーザインタフェースの要件Aを満たす．画面の上部には，LIFTシステムが緊急で管理者へ伝えたいメッセージが表示される．メッセージの例としては,「事象を推定した」や「徴候の追加調査」等がある．上部に表示されているメッセージは，左の方が新しいメッセージである．画面中央には，LIFTの状態等が表示される．上の方が新しい状態を示している．これはLIFTシステムユーザインタフェースの要件Bを満たす．また，ネットワーク図やログを表示させることも可能である.

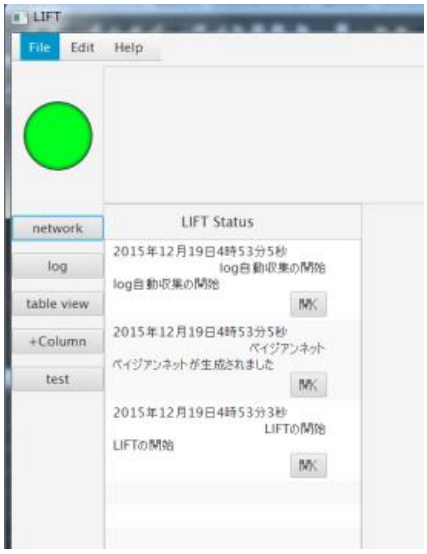


図4.　通常時のユーザインタフェース

次にユーザインタフェース上の動作を説明する．図５は，収集したログから徴候「プロキシを経由しない通信」を検知し，徴候「機密情報を含んだ通信の発生」の追加調査メッセージを表示している．徴候が検知され事象の確信度が上昇したため，丸の色が黄色に変化している．徴候「機密情報を含んだ通信の発生」は，自動収集が開始されたログから検知されるが，管理者がガイドを表示し，徴候を調査することも可能である．ガイドはHelpボタンを押すとPDFファイルで表示される.



図5.　徴候検知時のユーザインタフェース

図６は,「機密情報を含んだ通信の発生」が検知され，事象「マルウェアが添付されたメールが届く」を推定した状態を表示している．これはLIFTシステムユーザインタフェースの要件Cと先行研究からの要件Ⅱを満たす.



図6.　事象推定時のユーザインタフェース

図７は，管理者が特に注視して見たい情報がある時に使う機能である．まず+Columnというボタンを押し，図の右側のようなウィンドウを開く，次に，見たい情報を左から右へドラッグ＆ドロップで移動させる．図では「レポート出力」と「徴候検知」を選択している．そして，addColumnボタンを押すと，user定義というカラムが追加され，見たい情報が抽出されて表示されるようになる．これは先行研究からの要件Ｉを満たす．

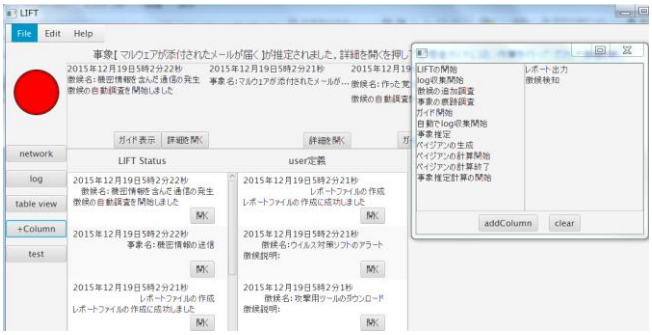


図7.　User定義カラムの追加

図８から図１０は，ネットワーク図である．青いバーはサーバーの状態を表しており，正常時では青色，徴候が検知された場合には黄色，事象推定時には赤色に変わる．これはLIFTシステムユーザインタフェースの要件Aを満たす．

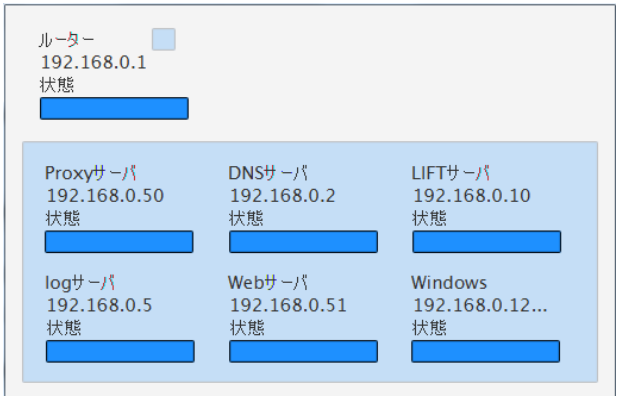


図8.　ネットワーク図(正常時)

図９の状態はProxyサーバから徴候が検知されたことを示している．図８では青色であったバーが黄色に変わり異常があったことを知らせている．

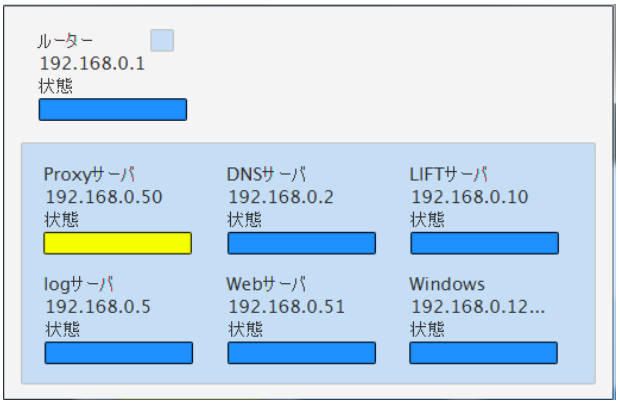


図9.　ネットワーク図(徴候検知時)

図１０の状態はProxyサーバで事象が起きたことを示している．図８では黄色であったバーが赤色に変わり異常の状態の変化を表している．

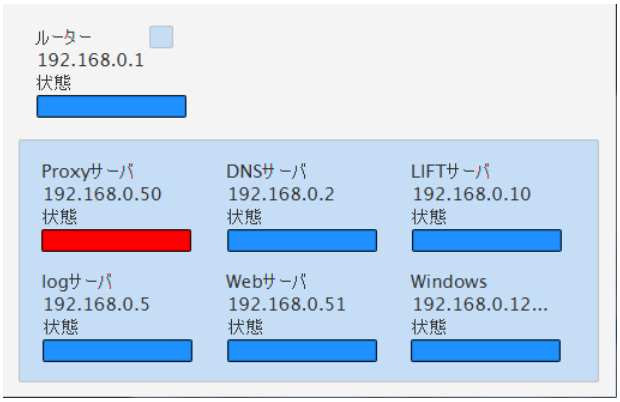


図10.　ネットワーク図(事象推定時)

図１１は推定された事象に対して有効な対策案を選定し，管理者に提示している画面です．この場合，事象「マルウェアが添付されたメールが届く」が推定され，他端末への感染を防ぐために「該当PCを社内ネットワークから隔離」が対策案として選定されている．

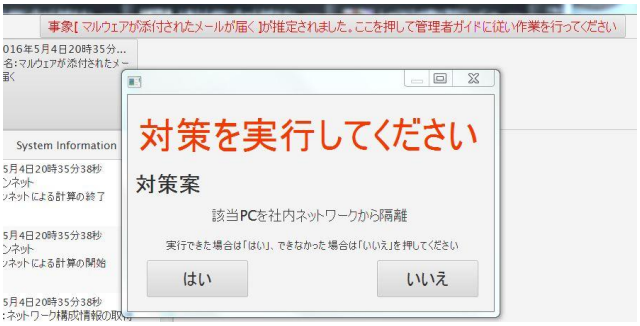


図11.　対策案選定

開発プログラムの合計ステップ数は約6000であった．

6. 適用実験の方法

上記のプログラムを用い，下記の 2 つの適用実験を行った．

＜適用実験A＞初心者にも理解しやすいユーザインタフェースを評価するために，被験者が先行研究のLIFTシステムと開発したLIFTシステムを使用してもらい，ユーザインタフェースを比較する実験を行う．実験を行う際，それぞれのシステム起動後に画面の説明をする時間を設けることとする．実験後，被験者にユーザインタフェースの使いやすと情報の見やすさのアンケートをとる．アンケートは５段階評価で，数字が大きいほど良いものである．

＜適用実験B＞対策案の選定をして管理者に表示させ，どの対策案を行ったか入力してもらうユーザインタフェースを評価するために，被験者が今回開発したLIFTシステムを使用してもらう．実験の前提条件として，提示された対策案の実行方法とそれを行った際に生じるリスクを理解しているとする．実験後，被験者にユーザインタフェースの使いやすと情報の見やすさのアンケートをとる．アンケートは５段階評価で，数字が大きいほど良いものである．

7. 実験結果と考察

7.1 実験結果

適用実験 A と B の結果を以下に示す．

A)　被験者として研究室の学生１１人がLIFTシステムを使用したアンケート結果を，表４に示す．

表4.　評価実験Aの結果

項目名	評価
使いやすさ	4．09
見やすさ	4．09

各項目の評価指標は以下のようになっている．

・使いやすさ

5. 前と比べて直感的にやることがわかる
3. 前と同じ
1. 前と比べて非常に使いにくい

・見やすさ

5. 前と比べて非常に見やすく与えられた情報にすぐ気づける
3. 前と同じ
1. 前と比べて非常に見にくい

B)　被験者として研究室の学生10人が今回開発したLIFTシステムを使用したアンケート結果を表５に示す．

表5.　評価実験Bの結果

項目名	評価
使いやすさ	4．4
見やすさ	4．0

各項目の評価指標は以下のようになっている．

・使いやすさ

5. 直感的に操作の仕方がわかる
3. よく見れば操作の仕方がわかる
1. わかりにくい

・見やすさ

5. 提示された情報を見てやることをすぐに把握できる
3. よく見れば提示された情報が把握できる
1. 見にくい

7.2 考察

適用実験 A と B の結果に関する考察を以下に示す．

A)　結果から先行研究からの問題点を解決できたと考えられる．また，情報の見せ方については，さらなる改善を行う必要がある．今回の実験で，多くの要望や意見を得られたので，それらを参考に修正を行っていく．

B)　画面自体の使いやすさと見やすさは改善点はあるものの概ね問題ないと考えられる．また，被験者からのアンケートよりイラスト等があると何を行ったら良いかのイメージが付きやすいというものがあった，これは改善点として挙げられるだろう．その他要望や意見が多く得られたのでそれらを参考に修正を行っていく．

8. 終わりに

本稿では，LIFTシステムユーザインタフェースの要件を述べたあと，その開発と仮想環境での適用と評価を行った．

今後の展開として，ユーザからの評価と意見を反映したユーザインタフェースの改善と対策案を行うことに伴うリスクを選定基準に組み込むことが挙げられる．

参考文献

[1]　Symantec:「標的型攻撃」に備える－サイバー攻撃 ：標的型攻撃とは、APTとは，入手先 <http://www.symantec.com/ja/jp/theme.jsp?themeid=apt_insight>

[2]佐々木，上原，松本: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 CSS2013(2013)

[3]橋本，比留間，上原，松本，佳山，柿崎，八槇，　佐々木: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（その２）－プロトプログラムの開発と評価－:，DICOMO2015

[4]intra-mart:UIデザインガイドライン，入手先 <http://www.intra-mart.jp/document/library/iap/public/im_ui/im_design_guideline_pc/index.html>

[5]鈴木文仁，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　―ベイジアンネットワークの適用―，東京電機大学学士論文(2016)

[6] 増井敏克:なぜ、「標的型攻撃」で情報が漏れるの？，@IT ，@IT，入手先 <http://www.atmarkit.co.jp/ait/articles/1510/27/news005.html>

[7] JNSA:増加する標的型攻撃メール，中小企業情報セキュリティ対策促進事業，中小企業情報セキュリティ対策促進事業，入手先 <https://www.jnsa.org/ikusei/spam/07_01.html>

[8]IPA独立行政法人情報処理推進機構:IPA テクニカルウォッチ「標的型攻撃メールの例と見分け方」，IPA，独立行政法人情報処理推進機構，入手先

<https://www.ipa.go.jp/files/000043331.pdf>
[9]IT用語辞典バイナリ:標的型メール，BINARY ，BINARY ，入手先
<http://www.sophia-it.com/content/%E6%A8%99%E7%9A%84%E5%9E%8B%E3%83%A1%E3%83%BC%E3%83%AB>
[10]IPA 独立行政法人情報処理推進機構:標的型メール攻撃対策に向けたシステム設計ガイド，IPA独立行政法人情報処理推進機構，入手先
<http://www.ipa.go.jp/security/vuln/newattack.html>