標的型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－

鈴木 文仁[†1]　上原 哲太郎[†2]　名和 利夫[†1]　佳山 こうせつ[†1]　村上 弘和[†3]
堀添 裕太[†4]　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．本稿では，現状の LIFT システムの全体像を紹介する．すなわち本システムは，収集したログの分析を行い，攻撃の徴候を検知し，ベイジアンネットワークなどの人工知能技術を利用し、確信度を算出，攻撃事象が推定された場合は応急対策を指示し，攻撃事象が推定されなかった場合は追加調査の自動実行や管理者へのガイドを行うものであることを具体例とともに示す．

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，人工知能，ベイジアンネット

Development and enhancement of intellectual network forensic system LIFT against targeted attacks (Patr1)- Overview of LIFT -

Fumihito Suzuki[†1]　Tetsutarou Uehara[†2]　Toshio Nawa[†1]　Kousetsu Kayama[†1]
Hirokazu Murakami[†3]　Yuuta Horizoe[†4]　Ryoichi Sasaki[†1]

Abstract: In recent years, targeted mail attacks targeting specific companies and organizations are becoming a problem. In order to cope with such attacks appropriately, the authors are developing LIFT (Live and Intelligent Network Forensic Technologies) which is a system for guiding measures using log analysis and artificial intelligence. In this paper, we introduce the overview of the current LIFT system. In other words, this system analyzes collected logs, detects signs of attacks, uses artificial intelligence technologies such as Bayesian networks, calculates certainty factors, and when an attack event is estimated, emergency measures are taken And instructs automatic execution of additional surveys and guidance to administrators when an attack event is not estimated, along with concrete examples.

Keywords: Digital Forensics, Network Forensics, Targeted Attacks, Artificial Intelligence, Bayesian Network

1. はじめに

近年，サイバー攻撃が増加しており，特に特定の組織や個人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重要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]．標的型メール攻撃は攻撃対象に対してメールを用いて攻撃を行う標的型攻撃で，三菱重工や日本年金機構などが被害に遭っている[2][3].

このような攻撃に対応するため，SIEM（Security Information and Event Management）システムが注目を浴びている．SIEM は，ログ管理統合ツールにセキュリティ脅威に対するリアルタイムな検知機能を追加したシステムである[4]．SIEM は，標的型メール攻撃に総合的に対応することが可能である．また，SIEM はリアルタイムにネットワークフォレンジックができるので，ネットワークフォレンジックシステムと呼ぶことができる．ネットワークフォレンジックは，証拠性を確保しログの保存と収集と分析を行うことである．しかし，SIEM のパフォーマンスは，あまりにも管理者の能力に依存している．組織に高い能力の管理者が複数いるならば，SIEM を使いこなすことができるが，一般的な組織では SIEM を使いこなせていない場合が多い．さらに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（Live and Intelligent Network Forensic Technologies）プロジェクトを立ち上げ，プロジェクト内で LIFT システムの研究開発を行ってきた[5][6][7][8]．LIFT システムの目的は，ベイジアンネットなどの人工知能技術を用いて攻撃の段階を把握、対策をガイドすることである．本稿では現状の LIFT システムの全体像を紹介する．

†1 東京電機大学
Tokyo Denki University
†2 立命館大学
Ritsumeikan University
†3 株式会社 SIG
SIG Co., Ltd.
†4 株式会社テプコシステムズ
TEPCO SYSTEMS CORPORATION

2. 関連研究

標的型攻撃についての研究は，標的型攻撃の検知の研究[9][10][11]，標的型攻撃の予防的対策の研究 [12]などが行われている．人工知能についての研究は，SIEM と SVM（Support Vector Machine）を組み合わせた研究[13]，ネットワークの異常検知に SVM を用いた研究[14]，分類器のパフォーマンス評価[15]などが行われている．

しかし，本論文で示すようなベイジアンネットワークを用いて標的型攻撃全体に対応する研究は我々の調査した範囲では見当たらない．

3. LIFT システム

3.1 概要

LIFT システムとは，収集するべきログの管理や，徴候から人工知能技術を用いて攻撃の推定，分析を行い，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応急対応を支援することを目的としたシステムである[10]. 図 1 に LIFT システムの概要図を示す．

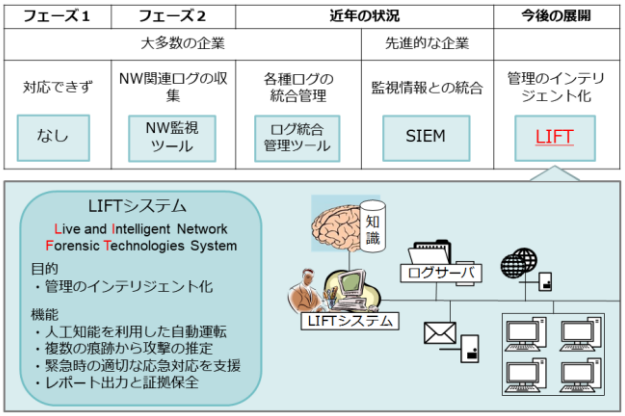

図 1　LIFT システムの概要図

Figure 1　Outline drawing of LIFT system.

3.2 LIFT システムにおける攻撃の構造と用語の説明

LIFT システムにおける攻撃の構造と用語の説明を図 2 に示す．

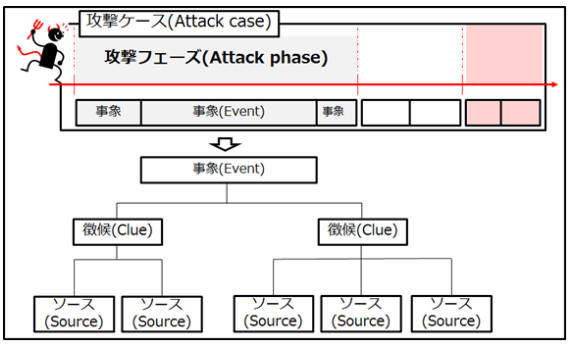

図 2　攻撃における各種名称の階層構造

Figure 2　Hierarchical structure of names in attack.

- 攻撃ケース

  攻撃ケースは過去に発生した攻撃の流れを表す．

- 攻撃フェーズ

  攻撃フェーズは攻撃の進捗を表す．攻撃フェーズは IPA の攻撃シナリオを基に作成した[16]．攻撃シナリオを攻撃者の目的ごとにフェーズ分けしたものを表 1 に示す．

表 1　攻撃のフェーズ分け

Table 1　Phase separation of attack.

フェーズ	攻撃フェーズの名称
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

- 事象

  事象は，攻撃を表したものである．推定された事象から攻撃フェーズの推定，攻撃者の行動の予測，応急対応の立案が可能となる．事象が表す粒度は「C&C サーバとの通信」や「内部のシステム情報の探索」といった形であらわす．

- 徴候

  兆候は，攻撃によって表れる結果である．事象と徴候は 1 対多の関連を持つ．徴候が表す粒度は「80，443 以外の CONNECT メソッド通信」や「外部機関からの不審な通信があるという連絡」といった形であらわす．

- ソース

  ソースは，ログやアラートである．

- 確信度

  確信度は，それぞれの事象が発生している確率である．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．

3.3 LIFT システムの機能

LIFT システムの機能の概要を図 2 に示す．

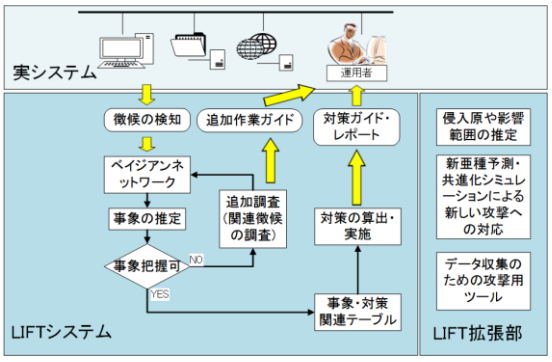

図 3　LIFT システム機能概要

Figure 3　Function of LIFT System.

LIFT システムは，検知した徴候からベイジアンネットワークを利用した事象の推定機能，「事象・対策関連テーブル」を利用した対策の選択機能を持つ．ベイジアンネットワークと事象・対策関連テーブルは専門家の知見や資料，過去の攻撃の分析を基に作成されている．そして，事象推定の状況や対策案によって運用者に対してガイドを表示する．

また，LIFT システムの外部拡張として，マルウェアの侵入源や影響範囲の推定機能，新たな攻撃の予測機能，攻撃データ収集のための攻撃用ツールを持つ．

3.3.1 ベイジアンネットワーク

ベイジアンネットワークとは，「原因」と「結果」の関係を複数組み合わせることにより，「原因」「結果」がお互いに影響を及ぼしながら発生する現象をネットワーク図と確率という形で可視化したものである．ベイジアンネットワークは「原因」「結果」を表す「ノード」，各ノードの関連を表す「エッジ」，「原因」「結果」間の条件付確率表から構成される[17]．

例として LIFT システムで利用しているベイジアンネットワークの一部を図 4 に示す．

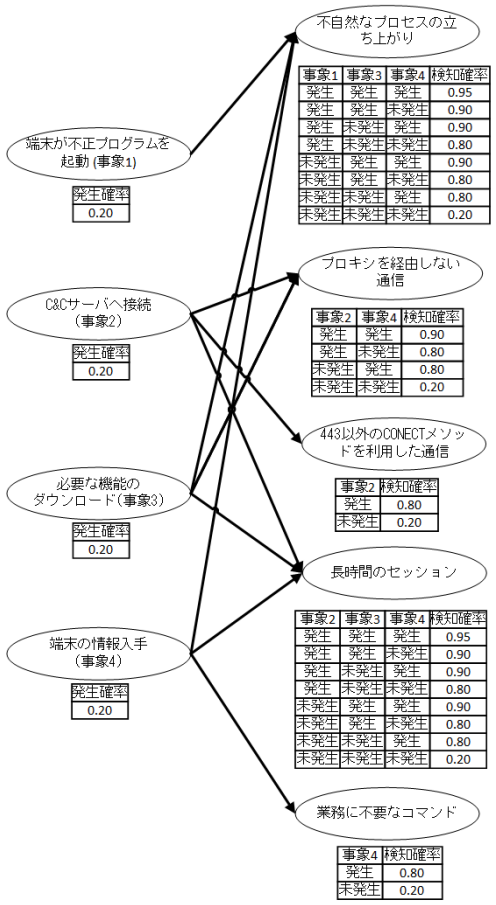

図 4　ベイジアンネットワーク例

Figure 4　Example of Bayesian Network.

図 4 では，右側の「結果」である「徴候」のノードが，左側の「原因」となる「事象」のノードを親に持つ構造となっており，各ノードの下にある表が条件付き確率の表で，表の中の確率は事前に入力する必要がある．

ベイジアンネットワークでは実際に発生した「原因」や「結果」の入力を行うことで，「原因」や「結果」の発生する確率の算出が可能となる． LIFT システムでは，徴候が検知された，または徴候が発見されなかったという「結果」を入力することで「原因」となる事象の確率が変化する．これを用いて事象の推定を行う．

3.3.2 事象の推定

LIFT システムの事象推定のフローを図 4 に示す．

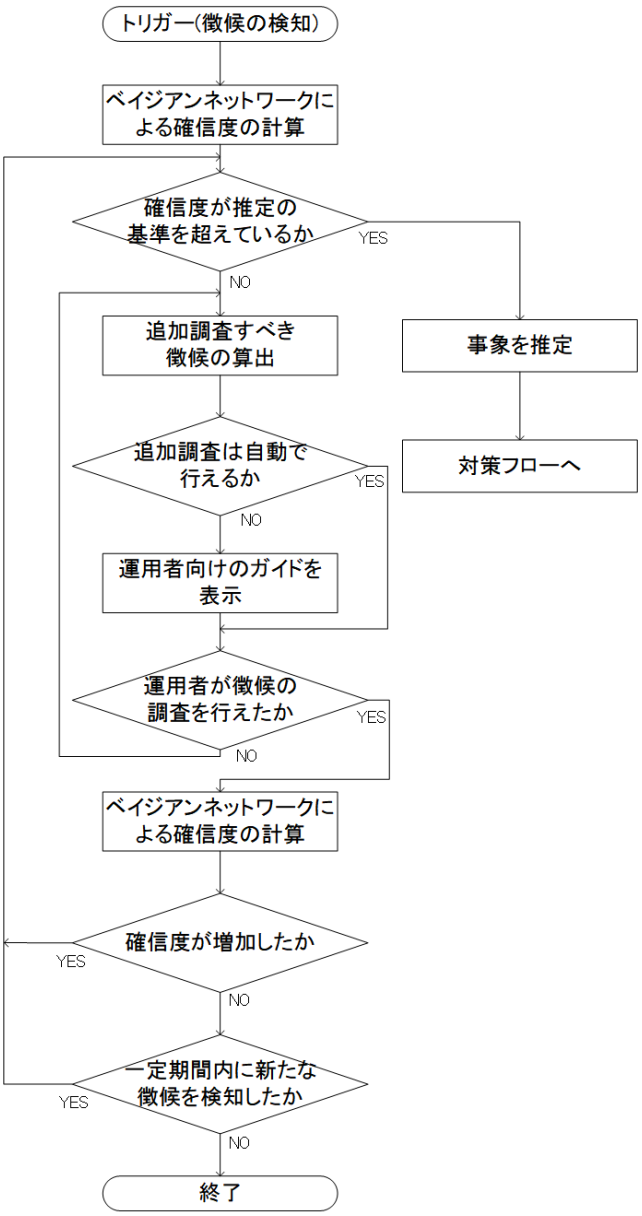

図 5　事象推定フローチャート

Figure 5　Flowcharts of event estimation.

LIFT システムは，攻撃によって各種機器にトリガーとなる徴候が現れると事象の推定を開始する．ベイジアンネットワークに検知された徴候を入力し，各事象の確信度を求

める．確信度が基準値を超えた事象を現在発生している事象と推定する．確信度を超える事象がなかった場合には徴候の追加調査を行う．

追加調査すべき徴候は，ベイジアンネットワークの徴候のノードの確率が最も大きい徴候から行う．追加調査は自動で行えるものと行えないものがあり，自動で行えないものは運用者へガイドを表示し，調査結果を入力させる．追加調査の結果，確信度の増加，または一定期間内に新たな徴候が検知された場合は，再び確信度と基準値の比較を行う．確信度が変化しない，もしくは減少かつ，一定期間内に徴候が検知されなかった場合は，誤検知とし，推定処理を終了する．

以上のようにLIFTシステムは事象の推定を行う．

3.3.3 対策案の選定

LIFTシステムの対策フローを図に示す．

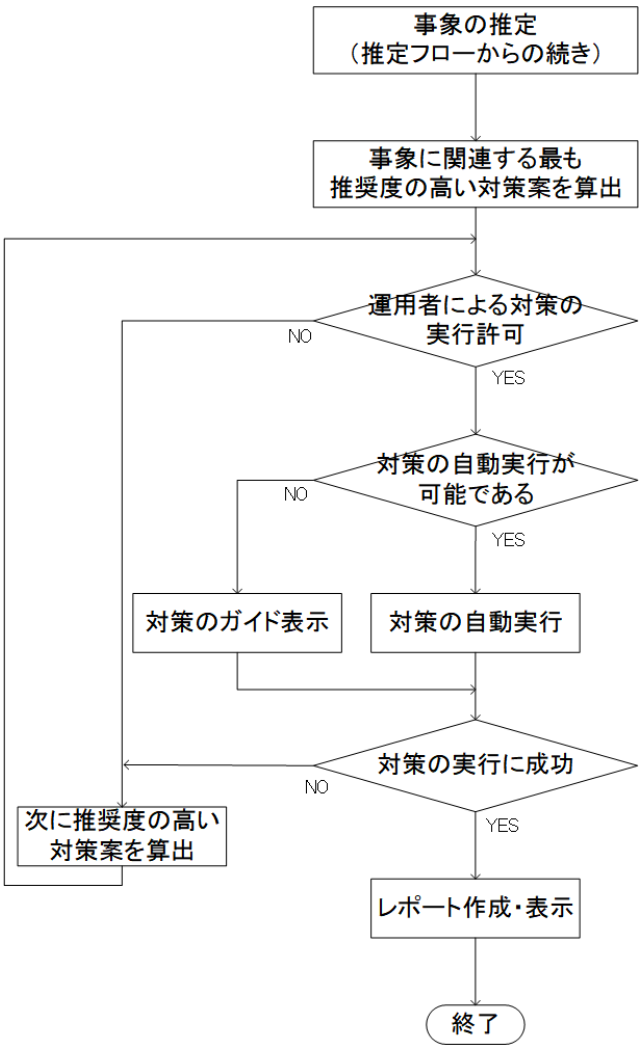

図 6　対策フローチャート

Figure 6　Flowchart of measures.

LIFTシステムは事象推定後，対策の選定を行う．対策の選定は，事象・対策関連テーブルを用いて行われる．図 7 に事象・対策関連テーブルを示す．対策はそれぞれの事象に対し推奨度が設定されている．推奨度は，対策に要する時間や複雑さ，影響範囲などの対策の実施コストと自動実行の可否によって計算される．詳しくは文献[18]を参照されたい．対策は推定された事象と対策の推奨度によって選択される．

対策の選定後，LIFTシステムは選定された対策を実行してよいか確認を取る．これは，対策の実行により，業務に影響が発生する可能性があるためである．実行許可された場合，自動で行えるものは実行し，自動で行えないものは運用者へガイドを表示し，結果を入力させる．対策の実行許可が出なかった場合や，何らかの原因で対策の実行がうまくいかなかった場合は次に推奨度の高い対策案を提示する．

対策の実行に成功した場合，検知された徴候と推定した事象，フェーズと類似の攻撃ケース等が書かれたレポートを表示する．

フェーズ	対策	全端末でウイルススキャン	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	該当端末IPのイン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	該当端末のネットワーク隔離	該当端末のプロセス規制	該当端末の停止	該当端末が所属するネットワークの隔離	組織のネットワーク停止
侵入	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							◎	◎	△	▲	▲
基盤構築	マルウェアC&Cサーバとの通信を行う			○		◎	○	◎		△	▲	▲
	必要な機能のダウンロード				○	△	△	◎		△	▲	▲
	攻撃基盤の端末の中の情報を入手する								○	△		
内部侵入・調査	攻撃者が攻撃基盤から内部ネットワークを探索する			○	○			◎		△	○	▲
	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	△									◎	▲
	攻撃者が攻撃基盤からサーバへ侵入する	△									◎	▲
目的遂行	端末の破壊								○			
	機密情報の送信			△		○	○	△		△	◎	○

優先度評価
◎　殆どの場合，一定の効果が見込まれる（90%以上）
○　概ね効果が見込まれる（70%～89%）
△　効果が無い場合がある（40%～69%）or 効果が不明瞭
▲　効果が見られないことが多い（1%～39%）or コストが割に合わない

図 7　事象・対策テーブル

Figure 7　Event/countermeasure table.

3.3.4 外部拡張機能

- 侵入源・影響範囲推定機能

  複数の端末のプロセスとその通信試行のログを解析・突合することで侵入源や波及範囲を推定する．これにより，被害範囲の想定や優先して調査すべき端末の特定が可能となると考える．詳細は文献[19]を参照されたい．

- 新たな攻撃の予測機能

  LIFTシステムは，既知の攻撃には対応可能であるが，新しい攻撃に対応するのは困難である．そこで，共振化モデルに基づく新たなマルウェアの予測や，過去のマルウェアの亜種の発生パターンから新機能を持つ類似マルウェアの予測を行う．詳細は文献[20]を参照されたい．

  予測した結果はデータ収集用攻撃ツールで利用される．

- データ収集用攻撃ツール

  データ収集用攻撃ツールは，様々な攻撃ケースによ

って，実験用のシステムに攻撃する．それにより発生するログ分析し，ベイジアンネットワーク更新する．また，予測したマルウェアの機能を用いた攻撃ケースを利用することで，新たな攻撃への対応が可能になると考えられる．

3.4 LIFT システムの構成

図 8 に LIFT システムの構成図を示す．

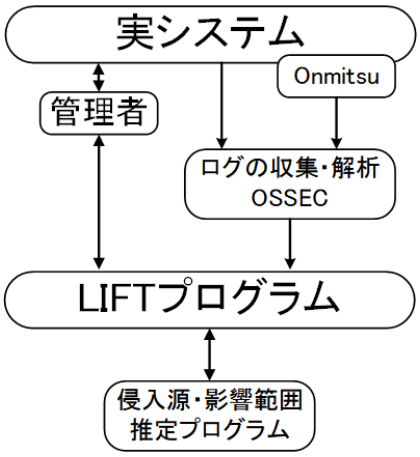

図 8　LIFT システム構成図

Figure 8　Configuration diagram of LIFT system.

- 実システム

  実システムは企業や組織内で利用されている PC やサーバ，ネットワーク機器等である．

- Onmitsu

  Onmitsu とは，不審な通信の原因特定に有用な情報源である揮発性情報を記録するために三村らが開発したプロセスログ記録ツールである[21]．Onmitsu は，メインメモリー上のプロセス状態と実行されたプロセス情報を関連付けて逐次記録する．Onmitsu のログは攻撃に使用されたマルウェアとソフトウェアを識別する時間を減らすことが可能である．

- OSSEC

  OSSEC とは，オープンソースのホスト型 IDS である[22]．ログ収集やログ解析，ファイルの変更監視等の機能があり，LIFT システムでは OSSEC を用いてログの収集，分析を行い，徴候を検知する．

- LIFT プログラム

  LIFT プログラムは，事象の推定，対策案の算出，運用者向けの UI，ガイド，対策の自動実行機能を持つ．OSSEC の徴候を検知したというアラートを受け取り，各種機能を実行する．

- 侵入源・影響範囲推定プログラム

  侵入源・影響範囲推定プログラムは Onmitsu のログを利用する．複数の端末のプロセスとその通信試行のログを解析・突合することで侵入源や波及範囲を推定し，被害範囲の想定や優先して調査すべき端末の特定を可能とする．

4. 実験

4.1 実験概要

仮想環境上に構築した実験環境に攻撃を行い，徴候の検知，事象の推定，対策の提案という一連の流れが行えるかを確認する目的で実験を行った．実験環境を図 9 に示す．

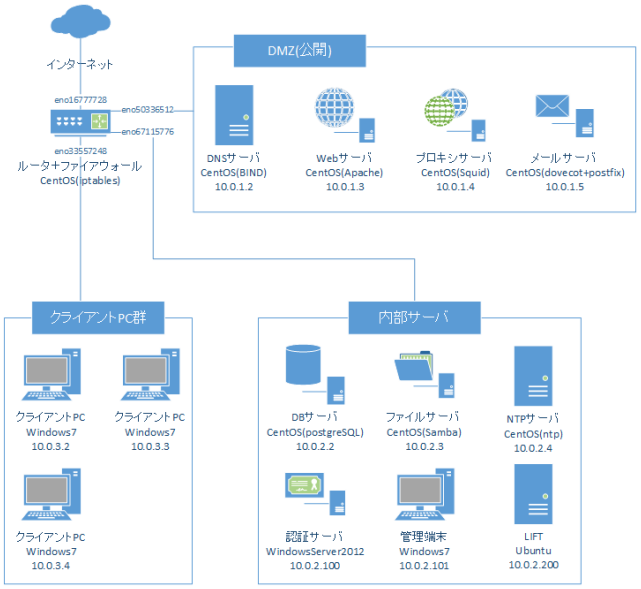

図 9　実験環境

Figure 9　Experiment environment.

実験は以下の手順で行った．

① クライアント PC にマルウェア添付メールを送信する．
② クライアント PC でマルウェア実行させる．
③ マルウェアは C&C サーバと通信し，攻撃用ツールのダウンロードを行う．
④ 攻撃用ツールを実行させる．

なお，マルウェアは RAT/ボットマルウェアシミュレータである ShinoBOT[23]，攻撃用ツールは，パスワード，ハッシュの入手などに利用される Mimikatz[24]を利用した．また，今回は動作確認が主な目的のため，ベイジアンネットワークの条件付確率票の値は確信度が大きく変動するように設定した．

4.2 結果

実験を行った結果，手順②で C&C サーバとの通信時に，徴候「通常とは異なる User-Agent による通信」を検知，攻撃用ツールのダウンロード時に，徴候「ブラックリストに含まれる URL へのアクセス」が検知され，事象「必要な機能のダウンロード」が推定された．そして，対策案として「該当端末のネットワーク隔離」が提案された．該当端末のイーサネットアダプタを無効にすることで C&C サーバとの通信が遮断された．

4.3 考察

実験結果より, LIFT システムの基本的な動作には問題がないことを確認した．しかし，今回行った攻撃は，非常に単純かつ簡単に検知できるものだったため，今後はより巧妙な攻撃を検知できるよう，徴候の検知ルールや，ベイジアンネットワークを調整していく必要があると考える．そのために，データ収集用攻撃ツールを利用し，繰り返し実験を行っていく必要がある．

また，今回は小規模のネットワークだったため，ログ収集によるトラフィックや，ログ分析のパフォーマンスは問題なかったが，ネットワークの規模が大きくなると問題になる可能性がある. ログ分析のパフォーマンスに関しては，分析用のサーバを物理的に増やすことで解消できると考えられる．

5. おわりに

本稿では，現状の LIFT システムの全体像と各種機能の説明をした．その後，動作確認実験を行い，徴候の検知から対策案の算出まで，問題なく動作することを確認した．今後は，徴候の検知のためのルール追加とベイジアンネットワークのチューニング，また運用者向けのガイド等，ユーザビリティにも考慮し，より高度な攻撃に対応できるよう改善していく予定である．

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.

参考文献

[1] “「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 | シマンテック”. http://www.symantec.com/ja/jp/theme.jsp?themeid=apt_insight, (参照 2015-12-21).

[2] “三菱重工を含む防衛産業 8 社が標的型攻撃の被害に、Trend Micro が分析 -INTERNET Watch Watch”. http://internet.watch.impress.co.jp/docs/news/20110920_478766.html, (参照 2015-2-23).

[3] “年金機構流出：３度の判断ミスで流出拡大 ： ＩＴ＆メディア ： 読売新聞（YOMIURI ONLINE）”. http://www.yomiuri.co.jp/it/security/goshinjyutsu/20150605-OYT8T50305.html, (参照 2015-2-23).

[4] “SIEM とは”. http://securityblog.jp/words/714.html, (参照 2016-2-22).

[5] 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, p. 155-162.

[6] 比留間裕幸, 橋本一紀, 柿崎淑郎, 八槇博史, 上原哲太郎, 佳山こうせつ, 松本隆, 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(その１）ー予兆検知と対策方法の提案ー. マルチメディア，分散，協調とモバイルシンポジウム 2015(DICOMO2015). 2015, p. 29-37.

[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）ープロトプログラムの開発と評価ー. マルチメディア，分散，協調とモバイルシンポジウム 2015(DICOMO2015). 2015, p. 38-43.

[8] 佐々木良一, 八槇博史. 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 3）ー今後の研究構想ー. マルチメディア，分散，協調とモバイルシンポジウム 2015(DICOMO2015). 2015, p. 44-50.

[9] 加藤雅彦, 小出洋, 金岡晃, 松川博英, 前田典彦, 岡本栄司. HTTP プロキシサーバでの Cookie 挿入によるバックドア通信の検出. 情報処理学会論文誌, 2014, vol. 55, no. 9, p. 2008-2020.

[10] Bo-Chao Cheng, Guo-Tan Liao, Chu-Chun Huang and Ming-Tse Yu. A novel probabilistic matching algorithm for multi-stage attack forecasts. IEEE Journal on selected areas in communications. 2011, Vol. 29, no. 7, p. 1438-1448.

[11] Natasha Arjumand Shoaib Mirza1, Haider Abbas, Farrukh Aslam Khan and Jalal Al Muhtadi. Anticipating Advanced Persistent Threat (APT) countermeasures using collaborative security mechanisms. 2014 International Symposium on Biometrics and Security Technologies (ISBAST). 2014, p. 129-132.

[12] 伊藤史人, 高見澤秀幸, 佐藤郁哉. 標的型攻撃メールの予防対策. 学術情報処理研究. 2012, no. 16, p. 100-110.

[13] MeeraGandhi, G.. Machine learning approach for attack prediction and classification using supervised learning algorithms. International Journal of Computer Science & Communication. 2010, vol. 1, no. 2, p. 247-250.

[14] Anumol, E. T.. Use of Machine Learning Algorithms with SIEM for Attack Prediction. Intelligent Computing, Communication and Devices. 2015, p. 231-235.

[15] Battista Biggio, Giorgio Fumera, and Fabio Roli. Security Evaluation of PatternClassifiers under Attack. IEEE transactions on knowledge and data engineering. 2014, vol. 26, no. 4, p. 984-996.

[16] “「高度標的型攻撃」対策 に向けたシステム設計ガイド”. https://www.ipa.go.jp/files/000046236.pdf, (参照 2014-9-21).

[17] 須鎗弘樹. ベイジアンネットワーク入門 (1). Medical imaging technology. 2003, vol. 21, no. 4, p. 315-318.

[18] 島崎一樹, 勅使河原可海, 柿崎淑郎, 佐々木良一. 標的型に対する知的ネットワークフォレンジックシステム LIFT の機能拡張（その 2）ー対策案優先度評価法ー. 情報処理学会コンピュータセキュリティシンポジウム 2017(CSS2017)(公演予定).

[19] 島川貴裕, 佐藤信, 佐々木良一. 標的型に対する知的ネットワークフォレンジックシステム LIFT の機能拡張（その 3）ー侵入源と波及範囲の推定ー. 情報処理学会コンピュータセキュリティシンポジウム 2017(CSS2017) (公演予定).

[20] 渋谷健太, 久山真宏, 松本隆, 八槇博史, 佐々木良一. 標的型に対する知的ネットワークフォレンジックシステム LIFT の機能拡張（その 4）ー将来起こりうる攻撃方法の推定ー. 情報処理学会コンピュータセキュリティシンポジウム 2017(CSS2017) (公演予定).

[21] 三村聡志, 佐々木良一. プロセス情報と関連づけた通信情報保全手法の提案. 情報処理学会論文誌. 2016, vol. 57, no. 9, p. 1944-1953.

[22] “About — OSSEC”. https://ossec.github.io/about.html, (参照 2017-08-24).

[23] “ShinoBOT -the rat/bot malware simulator, ShinoBOT Can you detect an APT like me? ”. http://shinobot.com/top.php, (参照 2016-07-23).

[24] “GitHub - gentilkiwi/mimikatz: A little tool to play with Windows security”. https://github.com/gentilkiwi/mimikatz, (参照 2017-08-24).