様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　　５　日現在

機関番号：　３２６５７
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０１６１

研究課題名（和文）標準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技術の開発

研究課題名（英文）Development of intellectual networks forensic technologies against targeted attacks

研究代表者

佐々木　良一（Sasaki, ryoichi）

東京電機大学・東京電機大学・教授

研究者番号：７０３３３５３１

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：標的型メール攻撃があった場合に、運用管理者に適切にガイドしたり半自動運転したりすることを可能とするLIFT（Live and　Intelligent Network Forensic Technologies）システムの基本方式を確立した。
この方式は、AI技術の1つであるルールベースシステムとベイジアンネットワークなどを利用し、徴候ー事象ー対策の関係を記述し、徴候群から事象と対策を明確にする。C#を用い約2000ステップのLIFTシステムのプロトプログラムを開発。
プロトプログラムによる評価実験を行い過去に起きたのと類似の事象について６件中６件正しく発見できることを示し、基本的有効性を確認した。

研究成果の概要（英文）：We established the basic method of the LIFT (Live and Intelligent Network Forensic Technologies) system in order to enable the proper guide to the operation manager and semi-automatic operation of the IT systems, when there is a target type mail attack.
This method uses the rule base system and Bayesian network which are classified as AI technology to describe the relationship between symptom - event - countermeasures and clarify the event and countermeasures from the symptom group. We have developed prototype program of LIFT system consisting of about 2000 steps using C #.
By conducting the evaluation experiment using this prototype program, we showed that 6 out of 6 cases can be correctly found for events similar to what happened in the past, and confirmed the basic effectiveness.

研究分野：　情報セキュリティ

キーワード：　セキュアネットワーク　デジタルフォレンジクス　ネットワークフォレンジクス　人工知能　ルールベース　イベントログ

１．研究開始当初の背景

サイバー攻撃が多様化し，ハッカーなどによる面白半分の攻撃だけでなく，スパイなどによる機密情報入手目的の高度な攻撃が増え大きな問題になっていた．個人情報や機密情報入手目的の高度な攻撃として標的型メール攻撃があり，三菱重工や衆議院など多くの組織に攻撃が行われてきた．その後，日本年金機構などに対しても同様な攻撃が行われており，その対策はますます重要性を増している．

２．研究の目的

標的型メール攻撃に対処するためには，パケットなどのネットワーク系のログをしっかり取得・管理することにより情報の漏えいなどを防止できるようにするためのネットワークフォレンジックシステムが非常に重要となる．しかし，従来のシステムは，対策の総合的判断が過度に運用者に依存しており，適切な対応がとれる人や組織は非常に限定されるという問題があった．

本研究ではこれらの問題に対し，人工知能技術を導入することにより，ネットワークフォレンジックシステムのインテリジェント化をすすめ，自動運転や運用管理者への適切なガイドを可能とするための基本技術の確立を図るとともに，プロトプログラムを開発し，適用実験を行うことにより，基本的有効性を確認するとともに，要改良項目を明確にする．

３．研究の方法

（１）標的型メール攻撃があった場合に，サーバログやパケットログ，人間行動のログなどを用いて，発生事象の推定を行い，対策を運用管理者に適切にガイドしたり，半自動運転したりすることを可能とするために，LIFT（Live and Intelligent Network Forensic Technologies）システム（知的ネットワークフォレンジックシステムともいう）の基本方式を確立した（図１参照）．

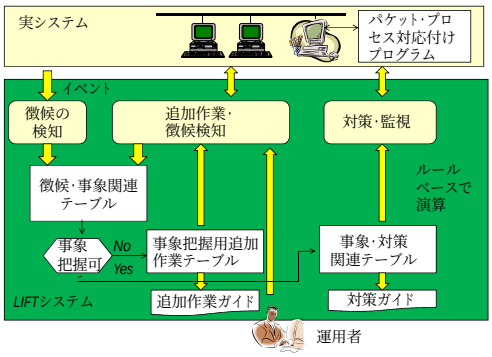

図　1*LIFT*システムの運用イメージ

この方式は，AI 技術の１つであるルールベースシステムとベイジアンネットワークなどを利用し，徴候ー事象ー対策の関係を記述し，観測された徴候群から事象並びに対策を明確にするものである．

（２）C#を用い約 2000 ステップの LIFT システムプロトプログラムを開発した．ここでは，（方式１）徴候ー事象ー対策をすべてツールベースで表現するものと，（方式２）徴候ー事象の関係をベイジアンネットで，その他をルールベースで表現するものの２つを用意した．

（３）表１に示すように６つの事象に対し評価実験を行うことにより過去に起きたのと類似の事象については，方式２を用いれば６件中６件正しく発見できることを示した．

表*1*　事象の推定実験結果

事象番号	観測対象の対象とした事象	方式1	方式2
1	社員がメールに添付された不正プログラムを起動する	事象５も同時に推定	推定
2	マルウェアがC2サーバとの通信を行う	推定	推定
3	攻撃基盤の端末の中の情報入手する	推定	推定
4	攻撃者が攻撃基盤から内部ネットワークを探索する	推定	推定
5	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	事象１も同時に推定	推定
6	攻撃者が攻撃基盤からサーバへ侵入する	推定	推定

（４）推定された事象に対応して，対策効果や対策に要するマンパワーなどを考慮して，実施すべき対策のプライオリティ付けをする方式を開発した．

（５）また，プロトプログラムの表示画面について被験者によるアンケートを実施し，使い勝手については大きな問題がないことも確認した（図２参照）．今後，適用実験を繰り返し，さらに使いやすいものに改良を行う予定である．

図２　LIFT システムの出力の一例

（６）現状の LIFT システムは既に発生した攻撃と同様な攻撃が起きた場合には，正しいガイドや自動運転が可能であるが，新しい攻撃に対応するのは困難であるという問題があることを認識した．この問題を解決するため Proactive な対策を可能にするようシス

テムの改良を進めた．

（７）改良システムでは，ＰＣなどの各装置におけるパケットと，プロセスの対応付けをカーネルドライバで情報の収集を行い，ログとして管理するプログラム Onmitsu （C++ で約 1000 ステップ）を開発した．実験により，情報の収集漏れがないことを確認するとともに，処理速度の低下も１%以下であることを確認した．このプログラムを使うことにより新しい攻撃であっても，PC 内の感染の有無や挙動が推定できるようになった．

（８）また，複数端末内の Onmitsu のプロセスログを解析することで標的型メール攻撃における内部侵入・調査段階で感染経路を検知する手法について検討した．このとき，機器間の関係をオントロジで記述した．これにより各端末のログとネットワーク構造を統合でき，感染経路が検知可能となった．実験で感染経路検知手法の有効性を検証した．すなわち実験の結果，マルウェアを検知した 5 次感染端末から初期感染端末の感染源プロセスを発見することができた．また，開発プログラムでの処理時間は RDF 集約なしの手法を用いると高々5 秒程度だった．これにより，感染経路を検知する手法に対する解決の見通しを得た．

（９）また，同様の方法を用い，組織内の感染の広がりを推定する機能も開発中である．この機能を使うと，対策すべき PC が明確になり，システム停止後の運転再開までの時間を短縮することが可能となる．

（１０）今後どういう新しい攻撃が出てくるか推定するために，PoisonX や Emdevi などの類似マルエア間の亜種生成の類似性分析を行った．亜種の発生パターンが同じなら，先行するマルウエアの亜種の発生から，対象となるマルウエアの発生パターンが予測できるからである．しかし，多次元尺度法を用いた今回の分析では，マルウエア間で，それぞれの亜種の発生パターンは異なることが明らかになった．今回の分析は 3 カ月のデータに基づくものなので，もっと長い期間のデータをとることにより，分析を実施する予定である．

（１１）ＡＩの一手法であるマルチエージェント法を用い，マルウエアと防御対策が互いに最適の戦略をとった場合のマルウエアと防御対策の進化の過程を見ることにより，今後現れる攻撃を予測できるのではないかと考えた．そのため，マルウエア進化の過程をマルチエージェント法に基づく，共進化モデルを用いて推定するための基本方式を確立した．今後，プログラム開発を行い，実験を繰り返す予定である．

４．研究成果

標的型メール攻撃があった場合に，運用管理者に適切にガイドしたり，半自動運転したりすることを可能とするための方式を固めるとともに，プロトプログラムを開発し，方式の基本的有効性を確認した．この結果，既に発生した攻撃と類似の攻撃を推定できることを確認するとともに，今後生じうる攻撃にも対処できる見通しを得た．そのうえで，新しいタイプの攻撃にも対応できるようにする方法の検討も行った．

この過程で，７件の論文化，3 件の海外発表，10 件の国内発表を行った．また，Onmitsu については，特許出願を行うとともに，企業において製品化され実用化されている．

さらに改良を行った後，実用システムに適用実験を行いたいと考えている．

５．主な発表論文等

（研究代表者，研究分担者及び連携研究者には下線）

〔雑誌論文〕（計７件）

① 佐藤信，杉本暁彦，林直樹，磯部義明，佐々木良一，マルウエアによるネットワーク内の挙動を利用した標的型攻撃における感染経路検知ツールの開発と評価，情報処理学会論文誌，査読有，58 巻第 2 号,2016，1-9

② 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，査読有，57 巻第 9 号,2016，1944-1953

③ Naoki Kobayashi, Ryoichi Sasaki, Proposal and evaluation of an evidence preservation method for use in a common number system, International Journal of Electronic Commerce Studies，査読有,6 巻第 1 号,2015，５１－６８
doi:10.7903/ijecs.1394

④ 天野貴通，上原哲太郎，佐々木良一，デジタル･フォレンジックのためのガイドライン総合支援システムの提案と開発，情報処理学会論文誌,査読有， 56 巻，9 号,2015，１８８９－１８９９

⑤ Ichiro Matsunaga, Ryoichi Sasaki, Development and Evaluation of a Continuity Operation Plan Support System for an Information Technology System, International Journal of Cyber-Security and Digital Forensics (IJCSDF)，査読有，4 巻第 2 号,2015，327-338

⑥ 小林直樹,佐々木良一，証拠性保全のための安全で効率的なログ署名方式の提案と評価，日本セキュリティマネジメント学会誌，査読有，28 巻第 2 号,2014，11-21

⑦ Takashi Shitamichi,Ryoichi Sasaki, Technology of Federated Identity and Secure Loggings in Cloud Computing Environment, International Journal of Electronic Commerce Studies,査読有，Vol.5，No.1,2014， 39-62
doi:10.7903/ijecs.1157

〔学会発表〕（計１３件）

① 島川 貴裕，標的型攻撃における侵害範囲特定ツールの開発と評価，第 76 回コンピュータセキュリティ合同研究発表会 2017 年３月２日～３月３日，厚木市神奈川工科大学
② 渋谷 健太，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 －標的型攻撃マルウェアの解析と亜種の予測－，情報処理学会ＤＩＣＯＭＯ2016， 2016 年７月６日～７月８日 三重県鳥羽シーサイドホテル
③ 鈴木 文仁，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－，情報処理学会ＤＩＣＯＭＯ 2016，2016 年 7 月 6 日～7 月 8 日，三重県鳥羽シーサイドホテル
④ 杉原 崚介，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－,情報処理学会ＤＩＣＯＭＯ 2016，2016 年 7 月 6 日～7 月 8 日，三重県鳥羽シーサイドホテル
⑤ 比留間裕幸，標的型攻撃に対する知的ネットワークフォレンジックスシステム LIFT の開発 (その 1) －予兆検知と対策方法の提案－，DICOMO2015,2015 年 7 月 8 日～7 月 10 日 ホテル安比グランド(岩手県八幡平市)
⑥ 橋本一紀，標的型攻撃に対する知的ネットワークフォレンジックスシステム LIFT の開発 (その 2)－プロトプログラムの開発と評価－，DICOMO2015,2015 年 7 月 8 日～7 月 10 日 ホテル安比グランド(岩手県八幡平市)
⑦ 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スシステム LIFT の開発 (その 3) －今後の研究構想 －DICOMO2015,2015 年 7 月 8 日～7 月 10 日ホテル安比グランド(岩手県八幡平市)
⑧ Makoto Sato，Proposal of a Method for Identififying the Infection Route for Targeted Attacks Based on Malware Behavior in a Network, CyberSec 2015,2015 年 10 月 29 日～10 月 31 日，Sampoerna University，Jakarta，Indonesia
⑨ Kazuki Hashimoto，Development of intellectual networks forensic system LIFT against targeted attacks，CyberSec 2015，2015 年 10 月 29 日～10 月 31 日，Sampoerna University，Jakarta，Indonesia
⑩ 八槇博史，知的ネットワークフォレンジックにおける事象推定のためのプロダクションシステムの適用,合同エージェントワークショップ＆シンポジウム 2014 （JAWS2014）,2014 年 10 月 27 日～ 10 月 29 日 ANA ホリデイインリゾート宮崎（宮崎）
⑪ 三村聡志，プロセス情報と関連づけたパケットを利用した不正通信原因推定手法の提案，情報処理学会 DICOMO2014,2014 年 7 月 9 日～7 月 11 日月岡温泉ホテル(新潟県新発田)
⑫ 比留間裕幸，標的型メール攻撃に対する知的ネットワクフォレンジのための予兆検知と対策方法提案，情報処理学会 DICOMO2014,2014 年 7 月 9 日～7 月 11 日月岡温泉ホテル（新潟県新発田）
⑬ Satoshi Mimura，Method for Estimating Unjust Communication Causes Using Network Packets Associated with ProcessInformation，The International Conference on Information Security and CyberForensics (InfoSec2014) 2014 年 10 月 8 日～10 月 10 日 Kuala Terenggaru，Malaysia

〔図書〕（計２件）

① 佐々木良一（監修），日科技連出版，改訂版 デジタル･フォレンジック事典，2014,300
② 佐々木良一編著，東京電機大学出版局，デジタル・フォレンジックの基礎と実践 ２０１７，２９０

〔産業財産権〕

○出願状況（計１件）

名称：ログ取得装置及び取得プログラム
発明者：佐々木良一,三村 聡志
権利者：同上
種類：特許,
番号：2014-127849
出願年月日：2014 年 06 月 23 日
国内外の別：国内

○取得状況（計０件）
名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
佐々木良一（RYOICHI,Sasaki）
東京電機大学・未来科学部情報メディア学科・教授
研究者番号：70333531