Computer Security Symposium 2014
22 - 24 October 2014

文字列類似性を考慮した標的型攻撃のグループ化手法

北條　孝佳†　　松浦 幹太‡

† 警察庁情報通信局情報技術解析課
100-8974 東京都千代田区霞が関 2-1-2
hojo@post.cyberpolice.go.jp

‡ 東京大学生産技術研究所
153-8505 東京都目黒区駒場 4-6-1
kanta@iis.u-tokyo.ac.jp

あらまし　近年、特定の組織等を対象とした標的型攻撃が行われ、組織等が保有する機密情報等が窃取され被害が拡大している。標的型攻撃に対して個々の事案について分析がされているが、それだけでは横断的な分析による攻撃の実態解明が困難である。そこで、本研究は当該攻撃に対して単純なモデル化及び各段階において収集したデータに基づいてグループ化を行い、攻撃の実態解明の一助となることを目的としている。本稿では、標的型攻撃の一つである標的型メール攻撃に着目して横断的に分析を行うため、当該攻撃に関連する複数の要素から文字列の類似性をも考慮したグループ化する手法について提案し、実データに適用した結果について報告する。

The method of grouping targeted attacks by considering the similarity of strings

Takayoshi Hojo†　　Kanta Matsuura‡

†High-Tech Crime Technology Division, Info-Communications Bureau, National Police Agancy of Japan.
2-1-2, Kasumigaseki, Chiyoda-ku, Tokyo 100-8974, Japan
hojo@post.cyberpolice.go.jp

‡Institute of Industrial Science, the University of Tokyo
4-6-1, Komaba, Meguro-ku, Tokyo 153-8505, Japan
kanta@iis.u-tokyo.ac.jp

Abstract　Recently, organizations who are victims of targeted attacks and are damaged, for example, by the accompanying confidential or important data leakage have been increased. Each attack can be analyzed individually, but it is necessary to perform another analysis in order to link the series of cases likely organized by the same attacker. It is necessary to appropriately group the attacks for the latter analysis and the purpose of our research is to establish a method to automate the grouping. In this paper, we focus on targeted email attacks, and propose the method for grouping targeted email attacks by using various techniques to calculate data including similarity of string related to the attacks.

1　はじめに

近年、特定の企業や組織から情報を窃取する標的型攻撃が増加している。その代表的な手法は、拡張子を偽装した不正プログラムファイルや攻撃コードが埋め込まれたドキュメントファイル等を添付した標的型メールを送り付ける攻撃である。当該メールはその件名や本文を本物に似せたあるいは窃取した本物を使用しているため、メールを受信したユーザがこのような攻

撃に気付かず添付ファイルを開いてしまい感染する。そして、当該感染端末を遠隔操作できる状態にした上で機密情報等の様々な情報を窃取したり、破壊活動を行ったり、当該端末を経由して第三者を攻撃したりするなど、攻撃を受けた組織等だけではなく、第三者にまで被害を拡大するような事案が発生している。

標的型攻撃への対策として、入口対策、内部対策、出口対策などの事前及び事後対策や、同様の被害に遭わないための対策など、様々な対策を施し、複合的及び多層的に防御して自組織内を保護するといった取り組みがなされている。

標的型攻撃の攻撃者又は攻撃組織 (以下「攻撃者」という。) を推定し、対策を行うためには、様々な標的型攻撃を収集し、各攻撃を横断的に分析する必要がある。そして、このような分析によって、攻撃者の規模、攻撃手法、攻撃者の目的、攻撃者数などの実態を解明する手掛かりになり得る。また、実態解明によって得られた情報から攻撃者の推定・特定を行い、攻撃者に関する情報を各国と共有、連携をして攻撃の停止及び攻撃組織の解散などの対応が可能になる。

このような各攻撃の横断的な分析は、一般的には手動によって行われており、非常に時間がかかるため、効率が悪く、見逃しや間違い、分析者の主観に大きく左右されてしまう。また、標的型攻撃の分析手法を変更した場合や別の分析者が行う場合に、多数のデータを見直す必要が生じ、照合が困難になるおそれが生じる。

そこで、本研究は、収集した標的型攻撃を自動的にグループ化することによって、攻撃者を推定し、その実態を解明するための一助となることを目指している。攻撃のグループ化は、不正プログラムの解析結果、当該解析結果に関する付随的情報、不正プログラムの侵入手法、窃取される情報等を集約して行う。このようなデータに基づいてグループ化を行うことで、同一の攻撃者が複数の組織等に攻撃している可能性が浮かび上がり、重点的に対処を行う動機付けにもなり得る。

これまでの研究 [12] では、第 2 節の各段階で収集した全てのデータに対して、各不正プログラムから収集した各要素がそれぞれ合致するかどうかのみでグループ化を行っていた。しかし、攻撃者が任意に設定する項目については類似性があるものも存在するため、合致の有無だけでは手動によるグループ化と一部異なる結果となった。そこで、本稿では、文字列の類似度を計算し反映したデータに基づいてグループ化を行った結果について報告する。

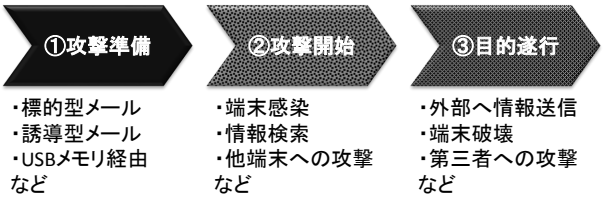

図 1: 標的型攻撃の流れ

2 標的型攻撃の概要とモデル化

標的型攻撃は、前述のように特定の組織等を攻撃し、情報の窃取等を行うサイバー攻撃の一種である。この攻撃の流れを図 1 に示す。

まず、不正プログラム等を添付した標的型メールの送信や不正プログラム等が埋め込まれた Web サイトに誘導する誘導型メールの送信、又は USB メモリ経由で不正プログラムを実行させるための USB メモリの配布など、攻撃の準備活動が開始される (攻撃準備)。次に不正プログラムに感染した端末を経由して重要な情報が存在するサーバを検索したり、同一組織内の他の端末への侵入を試みたりするなどの攻撃活動が開始される (攻撃開始)。最後に、重要な情報を外部に送信したり、破壊活動を行ったり、感染した端末を経由して第三者へ攻撃したりするなどの攻撃の目的を遂行する活動が開始される (目的遂行)。

この単純な 3 つの段階から構成されるモデル以外にも、攻撃準備より前段階の標的対象とする組織の調査、攻撃開始後の潜伏や内部ネットワークの調査を別の段階とすることも考えられるが、本研究では、各段階でデータを収集することが目的のモデル化であるため、この 3 つのモデルが適している。

3 関連研究

本研究における関連研究としては、不正プログラムか否かの判定や不正プログラムの亜種を

発見するための類似性の判定を行う研究などが挙げられる。例えば、バイナリコードから抽象化した関数を抽出する機構を用いて類似性を判定する手法 [7]、機械語命令列やバイナリ列から類似性を判定する手法 [13]、動的挙動から不正プログラムと判定する手法 [1, 2, 3, 4, 6, 8, 10, 11] などがある。

しかし、不正プログラムの類似性の判定だけでは、誤ったグループ化がされてしまうおそれがある。例えば、不正プログラム作成ツール (ビルダーやこれが含まれる制御コントローラ) はアンダーグラウンド等で販売されており、これを入手した別々の攻撃者が異なる設定を行い不正プログラムを作成した場合などである。また、攻撃者が同じであっても複数の不正プログラムを用いる場合も考えられるが、不正プログラムの判定や類似性のみを判定するだけでは別々の攻撃者と判定してしまうなどの問題が存在するため、本研究に採用することができない。

また、標的型攻撃等、インシデント発生時の特徴をまとめる OpenIOC というツールが存在する [9]。これは、攻撃手法における様々な項目を定義しておき、新たに入力したインシデントの特徴と合致した部分を表示させるものである。しかし、このツールは、合致する部分を抽出するだけであり、把握した攻撃全体のグループ化を行うものではないため、横断的な分析を詳細に行うことができない。

本研究の目的は、標的型攻撃をグループ化するための情報を抽出し、自動的にグループ化することによって実態解明の一助とすることであり、不正プログラムの類似性を判定することや合致部分のみを抽出することとは目的を異にする。すなわち、標的型攻撃全体を通してグループ化を行うことで攻撃グループを推定及び特定するための補助的役割を目的とするものである。

4 標的型攻撃におけるグループ化手法

4.1 本研究全体の流れ

標的型攻撃は、前述のように「攻撃準備」、「攻撃開始」、「目的遂行」の各段階がある。そして、同一の攻撃者であれば、これらの行動が類似していると考えられる。そこで、攻撃手法の類似性に基づいてグループ化することで、攻撃の実態解明の手掛かりを得られると考えられることから、以下の流れに沿って行うこととする。本稿は 3. までを対象としている。

1. **標的型攻撃の解析・分析** 不正プログラムの解析だけではなく、不正プログラムに付随する情報や感染端末から情報を窃取する際の接続先サーバに関する情報を収集する。
2. **解析結果等に基づきデータを整理・整形** 攻撃者のグループ化を行うために、前述の「攻撃準備」、「攻撃開始」、「目的遂行」の各段階において特徴となる項目 (要素) を抽出し、計算処理を行うためにデータを整理・整形する。
3. **データを用いてクラスタリング等を行い各攻撃をグループ化** 前項で整理･整形を行ったデータを用いて、類似度計算やクラスタリング技術を用いて各攻撃をグループ化する。
4. **攻撃手法の分類** 前項でグループ化した攻撃のうち、単独型や第三者が攻撃を請け負う請負型等の攻撃手法に分類する。
5. **攻撃者の組織、規模等を推定** グループ化した攻撃、分類した攻撃手法等を基に組織的攻撃かどうか、組織規模等を推定する。
6. **実態解明の手掛かり** 攻撃者の所属組織や規模等から標的型攻撃の実態解明に結び付く手掛かりを抽出する。

4.2 グループ化手法の提案

4.2.1 グループ化のために用いるデータ

本稿では、昨今注目されている標的型攻撃の一種である、標的型メール攻撃に焦点を当てて解析を行った。

標的型メール攻撃において、グループ化を行うための特徴データとなる項目を前述した標的型攻撃の流れ (図 1) に基づいて抽出する必要がある。本稿では実データのグループ化時に用いた項目のみを次節に記述する (項目末尾のカッコ内の数字は重み付け値：4.2.4 参照)。

4.2.2 標的型攻撃の各段階で抽出したデータ

第 1 の「攻撃準備」については、標的型メールに付与されたメールヘッダの項目が対象とな

る (表 1 参照)。なお、メール本文については、攻撃対象となる組織等によって内容が異なるため類似性を判定することは困難と考え項目外とした。

表 1: 攻撃準備に関するデータ

(1)	送信元メールアドレス (10)
(2)	エラー時メールアドレス (10) (return path)
(3)	返信先メールアドレス (10) (reply-to,in-reply-to)
(4)	送信日時 (1)
(5)	送信日時を日本時間に変換 (1)
(6)	タイムゾーン (1)
(7)	メーラーの種類 (X-mailer)(5)
(8)	送信元 IP アドレス (10) (X-Originating-IP)
(9)	Mime-Version(1)
(10)	言語 (content-language)(1)
(11)	content-type(1)
(12)	message-id(1)
(13)	件名 (10)

表 2: 攻撃開始に関するデータ

(1)	ZIP やドキュメントファイルのパスワード (10)
(2)	検体のファイル名 (5) 及びファイル種別 (1)
(3)	検体の設定ファイル等の標的ごとの特徴部分 (20)
(4)	検体が実行ファイルの場合のコンパイル日時 (5)
(5)	検体の Linker,OS 等の Minor,Major バージョン (1)
(6)	検体の主要言語 (1)
(7)	検体の Company 名 (1)
(8)	検体の Description 及び Internal(1)
(9)	検体の Copyright 及び Trademark(1)
(10)	検体の Original File Name(1)
(11)	検体の Build(1)、ファイルバージョン (1)、製品バージョン (1) 及び製品 Build(1)
(12)	検体の Product Name(1)
(13)	検体のアンチデバッグの有無及び手法 (5)
(14)	検体の Base64 の変形テーブル (10)
(15)	検体が使用する Mutex(20)

第 2 の「攻撃開始」については、不正プログラムから判明した事項が対象となる (表 2 参照)。なお、不正プログラム本体、不正プログラムが生成したファイル及び外部のサーバからダウンロードしたファイルを併せて「検体」という。

第 3 の「目的遂行」については、情報を窃取する場合、別途攻撃者が用意したサーバに接続することから、当該サーバに関する項目や接続時に行われる通信に関する項目が対象となる。

表 3: 目的遂行に関するデータ

(1)	接続先サーバのドメイン名 (10)
(2)	接続サーバの IP アドレス (10)
(3)	接続時のメソッド名、接続先 URL 及びクエリパラメータ (5)
(4)	接続時の UserAgent 及び Referer(5)
(5)	情報送信時に使用される暗号化鍵 (10)

4.2.3 文字列の類似性

4.2.2 で示したデータのうち、送信元メールアドレス、件名、又はファイル名等、文字列として使用しているデータがいくつか存在する。同一の攻撃者が行う全ての攻撃について、それぞれ全く異なるように各値を変更して攻撃を行うことは、異なる値を準備したり異なる文字列となるように管理したりする必要があり、攻撃の手間が大幅に増加し、攻撃コストが掛かる。そのため、同一の攻撃者であれば、付与した文字列に重なり合いが認められる場合があり得る。文字列が合致する場合は各項目の末尾に付与した数値が割り当てられるが、類似性がある場合にもこの類似性に適した数値が割り当てられるように類似度の計算を行うことでより適切なグループ化を行うことが可能になる。

そこで、これらの文字列のデータに対して類似度を計算し、この値を用いることで、類似した文字列を持つ攻撃についてもグループ化することが可能になる。

文字列の類似度を計算するには、文字列の意味をそれほど重視する必要がないために、代表的な方法である Levenshtein 距離又は LCS(Longest Common Subsequence) を用いることを検討した。これらによって計算される値を、完全に一致する場合は 1 を、全く一致しない場合は 0 とな

るように標準化する。Levenshtein 距離を標準化した NLD(Normlised Levenshtein Distance) を式 (1) に、LCS を標準化した NLCS(Normalised Longest Common Subsequence) を式 (2) に示す。

$$NLD = \left(1 - \frac{LevenshteinDistance}{max\left(len\left(x_1\right), len\left(x_2\right)\right)}\right) \quad (1)$$

$$NLCS = \frac{len\left(LCS\left(x_1, x_2\right)\right)^2}{len\left(x_1\right) \times len\left(x_2\right)} \quad (2)$$

ここで、送信元メールアドレスの場合に攻撃者が通常設定又は変更するのはメールアカウント名 (*test*@*example.com* の *test* のように @ より前の文字列) であると考えられるため、この文字列のみを比較する方が攻撃者の特徴が表れると考える。このことは、接続先サーバのドメイン名にも同様のことがいえるため、.jp や.ru のような TLD(Top Level Domain) を除外した部分のみを比較対象とする。

このように似ている送信元メールアドレスや似ているドメイン名等が使用されている場合、同一の攻撃者が付与した可能性が高いと考えられる。そのため、このような類似性のある値について計算した類似度をグループ化する計算に用いることでより適切なグループ化が可能になる。

もっとも、類似度が低い値をグループ化に使用すると、類似性がほとんど無い攻撃同士をグループ化してしまうおそれがある。そこで、定数 C_s 以上の類似度を閾値とし、式 (3) の場合に類似度 ($Simi$) をグループ化する計算に使用することとする。

$$Simi = \begin{cases} NLD|NLCS & (\geq C_s) \\ 0 & (< C_s) \end{cases} \quad (3)$$

4.2.2 で示したデータのうち、本稿では、表 1(1)、(2)、(3)、(7)、(11)、(12)、(13)、表 2(1)、(2)、(3)、(7)〜(10)、(12)、(14)、(15)、表 3(1)、(3)、(4)、(5) について文字列の類似度を計算する。

4.2.4 重み付け

文字列の類似性だけではなく、ある攻撃と他の攻撃との特徴的な項目が似ている場合、同一の攻撃者である推定が働く。そこで、このような項目には重み付けを行い、同一のグループになり易くなるようにした。例えば、感染した端末の情報を窃取して送信するサーバのドメイン名が、他の攻撃と同一や類似の場合である。さらに、ZIP ファイルやドキュメントファイルを開く際のパスワードが同一である場合等、同一の攻撃者しか設定し得ないと考えられる項目も存在する。これらの項目に対してはより大きな値を用いて重み付けを行うこととした。

本稿では様々な値で試験を行った結果、4.2.2 で示した各表の項目の末尾に付与した数値を重み付けとした。例えば、末尾の数値が 1 の項目は、合致すれば 1、合致しなければ 0、類似度が閾値以上ならその値に、数値が 5 の項目は数値が 1 の各場合の 5 倍になる。

4.2.3 及び 4.2.4 から表 4 のようなマトリックス型のデータを作成する。

表 4: 抽出したデータを整理・整形した例

事案番号	xxx.serxxx	xxx.mxx	11x.xx.xx.xx	GET /xxxx.cgi	m_ID=Kxxxxx1	m_ID=Kxxxxx2	glexxx	jmaxxx	+0900 (JST)	-0400 (EDT)	件名 1 〜	…
1	10	0	0	0	0	0	1	0	0	1	1	⋯
2	0	10	0	0	0	1	0	0	0	1	0	⋯
3	0	10	0	0	0	0	0.85	0	0	1	0	⋯
4	0	8.1	0	0	0	0	0	1	1	1	0	⋯
⋯	0	0	10	0	0	0	0	0	1	0	0	⋯

4.2.5 データに基づくグループ化手法

各攻撃からデータを抽出して整理・整形した表 4 のデータに基づいてグループ化を行うが、その方法には様々なものが存在する。本研究では、手動で行う方法、コサイン類似度を用いる方法、クラスタリングを用いる方法のグループ化を提案している [12]。

なお、本研究は、複数のグループ化手法を用いて、手動によるグループ化を効率化すること、及び手動によるグループ化では発見できなかった類似性のある攻撃を浮かび上がらせることを主な目的としている。そのため、いずれの手法が最良かを決定するものではなく、分析者が攻撃のグループ化を行うために有効な情報を効率的に提供する補助的役割を主目的としている。

4.2.6 コサイン類似度を用いたグループ化

コサイン類似度は、検体 x と検体 y の類似度を測るものであり、式 (4) で表される。

$$0 \leq \cos\theta = \frac{\vec{x} \cdot \vec{y}}{|\vec{x}||\vec{y}|} \leq 1 \tag{4}$$

ここで、$\vec{x}$ は、検体 x の要素の配列であり、$\vec{y}$ は、検体 y の要素の配列を持ち、この要素に基づいて式 (4) を計算する。

この式から計算されたコサイン類似度のうち、値が定数 C_c 以上の検体同士をグループ化する。

4.2.7 クラスタリングを用いたグループ化

非階層的クラスタリングは、データ間の類似性 (距離) を尺度に、あらかじめ定めたクラスタ数にデータの集合を分類する手法である [14]。また、階層的クラスタリングは、クラスタリングされていないデータから、類似度の高い順に融合して次第に大きなクラスタを作成し、最終的に一つのクラスタに統合する手法をいう [14]。

本稿では非階層的クラスタリングには、代表的な K-means 法を、階層的クラスタリングには、Ward 法を用いた。

非階層的クラスタリングはクラスタ数を指定しなければならない。クラスタ数の算定基準には様々な方法が存在するが、本稿では計算量が比較的少ない、群内平方和の変化が少ないクラスタ数を用いることとした。

群内平方和は群内の分散であり、個々の値と群 (クラスタ) 平均値との偏差の平方を総和し、さらに各クラスタの総和を計算したものである。計算式を式 (5) に示す。

$$\sum_{j}\sum_{i}(x_{ij} - \overline{A_j})^2 \tag{5}$$

ここで、i はクラスタ内の i 番目の値、j は j 番目のクラスタ、x_{ij} はクラスタ内の個々の値、$\overline{A_j}$ は j 番目のクラスタの平均値を表す。

クラスタ数を変化させてそれぞれの場合について式 (5) を用いて計算を行い、クラスタ数が増加しても群内平方和の差が小さい又は負の値を取るクラスタ数を攻撃者数として指定した。またこの指定したクラスタ数を使用して、階層的クラスタリングにおいてもグループ化することとした。

5 実データへの適用

5.1 共通の不正プログラムを用いた標的型メール攻撃

前述したグループ化を行うための手法を実際の標的型メール攻撃に対して適用を行う。そのために、攻撃者のグループ化を行うためには前述したようにデータを整理・整形する必要がある。

標的型メール攻撃では、攻撃者が不正プログラムを独自に作成するよりも第三者が作成したものを入手して攻撃を行う方法が攻撃者にとって比較的容易であると考えられる。そのため、同一又は類似する不正プログラムを使用して標的型メール攻撃を行うことが多い。そこで、本稿ではまず解析結果によって判明した不正プログラム 1〜5 に焦点を当てることとした。そして、当該不正プログラムが用いられた標的型メール攻撃ごとに表 4 の項目を抽出し、これらのデータに基づいてグループ化を行った。

ここで、4.2.3 では、文字列の類似性判定に NLD 及び NLCS のそれぞれを使用することを検討したが、実データへの適用は、閾値 (C_s) が 0.75 の場合に各項目に当てはめると、常に NLCS よりも NLD の値の方が大きくなった。そこで、本稿では、類似性を高く判定する NLD のみを用いることとした。

5.2 各不正プログラムの特徴

各不正プログラムの特徴を表 5 に示す (不正プログラム 1〜4 の詳細については [12] を参照)。不正プログラム 5 は、特定のファイルを生成し、外部と通信を行い、暗号化のための鍵のシードを受信して鍵を生成し、この鍵を共通鍵として暗号化通信を行う。ファイルのアップロード、ダウンロード及び任意のコマンド実行が可能であり簡易な RAT になる機能を有している。また、2 種類の接続先が用いられていた。全体の特徴から 1〜4 の攻撃者グループが存在すると考えられるものであった。

不正プログラム 1〜5 を用いた標的型メール攻撃は全部で 108 件であり、接続先や IP アドレス、パスワードなどの特徴項目は 49 項目、特徴項目内の小項目の合計は 1,216 項目であった。

表 5: 各不正プログラムの特徴の比較

番号	1	2	3	4	5
外部接続確認	○	○	×	×	×
設定ファイル又は設定値の有無	○	×	×	×	○
変形 Base64 テーブルの使用	×	×	○	×	×
外部接続	○	○	○	○	○
通信内容	平文	平文	難読化	暗号化	暗号化
遠隔操作	簡易	簡易	簡易	高度	簡易
ダミーファイル	なし	なし	なし	なし	一部あり

5.3 手動及び計算によるグループ化の結果

クラスタ数は、108 件の攻撃に対して同一の攻撃者が複数回攻撃したと仮定し、また、不正プログラム 5 の攻撃は最大 4 グループに分類されると考え、群内平方和を用いて 36 とした。手動でグループ化を行った結果と計算を用いて行った結果との比較を表 6 に示す。表内の Cos はコサイン類似度、K は K-means 法、W は Ward 法を表す。また、「なし」は、文字列の類似性を考慮しない ($C_s = 1$) 場合、「あり」は文字列の類似性を考慮し、実験により効果が高かった $C_s = 0.75$ とした。表の○は手動結果と合致、◎は手動結果では見逃したものをグループ化、△は手動結果と一部合致したものを示す。

表 6: 各方法を用いたグループ化の結果の比較

手動	Cos		K		W	
	なし	あり	なし	あり	なし	あり
A1	○	○	○	△	○	○
A2	○	○	○	○	○	○
A3	△	◎	◎	△	△	◎
A4	△	△	△	△	△	△
A5	△	△	○	○	○	○
A6	○	○	○	○	○	○

5.4 考察

文字列の類似性を考慮した場合に、K-means 法のみ異なる結果となり、それ以外は手動による A4 グループ以外は概ね考慮しない場合よりも良い結果が得られた。K-means 法は初期値にいずれを選択するかによって値が変わるため、さらに発展させた X-means 法の適用等、今後の検討の余地がある。

表 7: 不正プログラム 5 を用いた標的型メール攻撃の一部の比較

事案番号	5-1	5-2	5-3	5-4
メールの宛先	X、Y	X	X	X
送信元メールアドレス	A1	A2	A1	A3
件名	同じ			
タイムゾーン	B1			B2
メーラー	C1	C2	C1	
添付ファイル	ZIP			RAR
MD5	全て異なる			
検体ファイル名	同じ			
検体のアイコン	D1	D2	D2	D1
コンパイル日時	E1		E2	
アンチデバッグ方法	F1		F2	
接続先	同じ			
接続クエリ	同じ			

一方、A4 グループはほとんどの方式で手動とは異なる結果を示している。このグループは不正プログラム 5 を用いた攻撃であり、表 7 のような特徴を有する。ここで、表内の同じ記号は同じ内容であることを表している。手動による判定では類似している部分が多々存在したため、これらを全て同一の攻撃と判断したが、計算による場合には表 8 に示すように一部異なると判断されているものも存在する。

このように手動でグループ化した場合と計算によってグループ化した場合とで異なることもあり得、その上、どちらが正しいとはいえない結果になっている。しかし、本研究の目的は、自動的にグループ化することによって効率化を図ること及び分析者の能力に左右されないグループ化を提示することにあるため、今回のような結果を示すこともその目的に沿うものといえる。

6 まとめ及び今後

本稿では、標的型メール攻撃が有する要素の有無だけではなく、文字列の類似性を考慮したグループ化を提案し実データに適用した。その結果、一部の方法において効果が見られた。

表 8: 不正プログラム 5 を用いた攻撃をグループ化した結果の比較

	手動	Cos		K		W	
		なし	あり	なし	あり	なし	あり
5-1	同一	H1	I1	J1	K1	L1	M1
5-2			I2			L2	M2
5-3		H2	I1		K2		M3
5-4		H3	I3	J2			

より複数の攻撃を同一グループにするには、コサイン類似度では閾値を小さくし、クラスタリングではグループに含める距離を大きくすることやグループ数を小さくすることによって緩やかにグループ化される。しかし、意図していない攻撃もグループ化されるため、影響の少ない値を求める手法を検討する必要がある。また、分析者がこれらの値を自由に設定でき、グループ化の確認が可能なインターフェースを提供することによって、この課題を解決できる可能性があり、これについても検討する必要がある。

参考文献

[1] Irfan Ahmed and Kyung-suk Lhee. Classification of packet contents for malware detection. *Journal in Computer Virology*, Vol. 7, pp. 279–295, 2011.

[2] Michael Bailey, Jon Oberheide, Jon Andersen, Z.Morley Mao, Farnam Jahanian, and Jose Nazario. Automated classification and analysis of internet malware. In Christopher Kruegel, Richard Lippmann, and Andrew Clark, editors, *Recent Advances in Intrusion Detection*, Vol. 4637 of *Lecture Notes in Computer Science*, pp. 178–197. Springer Berlin Heidelberg, 2007.

[3] Damiano Bolzoni, Christiaan Schade, and Sandro Etalle. A cuckoo's egg in the malware nest: On-the-fly signature-less malware analysis, detection, and containment for large networks. In *LISA '11: 25th Large Installation System Administration Conference*, pp. 201–216, Berkeley, CA, USA, December 2011. The USENIX Association.

[4] Julien Desfossez, Justine Dieppedale, and Gabriel Girard. Stealth malware analysis from kernel space with kolumbo. *Journal in Computer Virology*, Vol. 7, pp. 83–93, 2011.

[5] Mojtaba Eskandari, Zeinab Khorshidpour, and Sattar Hashemi. Hdm-analyser: a hybrid analysis approach based on data mining techniques for malware detection. *Journal of Computer Virology and Hacking Techniques*, pp. 1–17, 2013.

[6] I. Firdausi, C. Lim, A. Erwin, and A.S. Nugroho. Analysis of machine learning techniques used in behavior-based malware detection. In *Advances in Computing, Control and Telecommunication Technologies (ACT), 2010 Second International Conference on*, pp. 201–203, 2010.

[7] Charles LeDoux, Arun Lakhotia, Craig Miles, and Vivek Notani. Functracker: Discovering shared code to aid malware forensics. In *LEET '13*, 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats. University of Louisiana at Lafayette, 2013.

[8] Weiqin Ma, Pu Duan, Sanmin Liu, Guofei Gu, and Jyh-Charn Liu. Shadow attacks: automatically evading system-call-behavior based malware detection. *Journal in Computer Virology*, Vol. 8, No. 1-2, pp. 1–13, 2012.

[9] Mandiant(FireEye) Corp., OpenIOC. `http://www.openioc.org/`.

[10] Sandeep Romana, Swapnil Phadnis, Himanshu Pareek, and P.R.L. Eswari. Behavioral malware detection expert system - tarantula. In DavidC. Wyld, Michal Wozniak, Nabendu Chaki, Natarajan Meghanathan, and Dhinaharan Nagamalai, editors, *Advances in Network Security and Applications*, Vol. 196 of *Communications in Computer and Information Science*, pp. 65–77. Springer Berlin Heidelberg, 2011.

[11] Philipp Trinius, Carsten Willems, Thorsten Holz, and Konrad Rieck. A malware instruction set for behavior-based analysis. In *Conference or Workshop Item*, 2011.

[12] 北條孝佳, 松浦幹太. 標的型攻撃における攻撃者のグルーピング手法. 暗号と情報セキュリティシンポジウム (SCIS), 2014.

[13] 岩村誠, 伊藤光恭, 村岡洋一. 機械語命令列の類似性に基づく自動マルウェア分類システム. 情報処理学会論文誌, Vol. 51, No. 9, pp. 1622–1632, sep 2010.

[14] 平井有三. はじめてのパターン認識. 森北出版株式会社, 2012.