Vol.2015-CSEC-69 No.1
Vol.2015-IOT-29 No.1
2015/5/21

マルチモーダルマルウェア解析システムを用いたプロキシアクセス型マルウェアの解析結果の考察

下間直樹† 鬼頭哲郎† 重本倫宏† 林直樹† 仲小路博史†

近年、標的型攻撃等のサイバー攻撃の高度化により、シグネチャ型のウィルス対策ゲートウェイなどの入口対策が突破されることが日常的になってきている。さらに最近では、出口対策の最終砦である認証付きプロキシをも突破するマルウェアの出現も確認されている。本研究では、多種のサンドボックスと複数のマルウェア解析エンジンを有する「マルチモーダルマルウェア解析システム（M3AS）」を用いてマルウェアを解析した結果、プロキシ認証突破型マルウェアを実際に 8 種類確認した。さらに、これらのマルウェアの傾向について分析した結果の考察を述べる。

Consideration of Proxy Access Malware Analysis Results by using Multimodal Malware Analysis System

NAOKI SHIMOTSUMA† TETSURO KITO† TOMOHIRO SHIGEMOTO†
NAOKI HAYASHI† HIROFUMI NAKAKOJI†

In recent years, due to the sophistication of cyber attacks such as targeted attacks, greater number of malware cannot be blocked by inbound measures such as anti virus gateway. Moreover, it is confirmed that malware which can perform external access through authentication proxy which is the last measure of outbound measures emerged. In this report, we analyzed malware using "Multimodal Malware Analysis System (M3AS)", which has a variety of sandboxes and multiple analysis engines, confirmed that eight of the malware have an ability to pass authentication proxy and discussed about the result.

1. はじめに

近年、特定の企業を狙った標的型攻撃が社会的な問題となっている。標的型攻撃の手口には不正アクセスや USB メモリからのウィルス感染など様々あるが、主要な手口の一つに、添付ファイルを開かせることでウィルスに感染させたり、特定のサイトに誘導することで気付かれないようにウィルスを送りつける「標的型攻撃メール」がある。企業における近年のセキュリティ事故原因の一位はマルウェア感染であり、マルウェア対策が企業のセキュリティにおいてますます重要となってきている[1]。

また、最近のマルウェアの半数以上は既存のマルウェア対策ソフトでは検知できない[2]。このため、組織へ侵入してしまうことを前提とした「事故前提型」「多層防御型」のセキュリティ対策が重要となっている。これに対し、IPA(情報処理推進機構)では多層防御の一環として出口対策に認証付きプロキシを設置することを推奨している[3]。

しかしながら、新型 PlugX をはじめ、認証付きプロキシをも突破するマルウェアの出現も報告されている。

上記に対して、著者らは多層防御を高度化するため、マルウェアが組織に侵入してしまった場合、すなわち感染後のマルウェアの挙動を自動的に解析する多種環境マルウェア動的解析システム(M3AS)の研究を進めている[4]。

本報告では、認証付きプロキシを導入した M3AS を構築し、2014 年 10 月の一ヶ月間に取得したマルウェアのうち 629 種類のマルウェアを解析し、プロキシ認証突破型マルウェアの数とその傾向を分析した結果について報告する。

† (株)日立製作所
Hitachi Ltd.

2. プロキシアクセス型マルウェア

本章ではプロキシアクセス型マルウェア出現までの歴史的背景と、プロキシ認証突破型マルウェアの認証情報窃取方法について述べる。

まず、プロキシアクセス型マルウェアをはじめとするネットワーク通信型マルウェアの攻撃手法の変遷について述べる。ネットワーク通信型マルウェアの出現当初、企業の外部にいる攻撃者が、攻撃対象の脆弱性を狙ってバックドアを仕掛け、ここから攻撃者との通信チャネルを開設し、攻撃対象の企業に対して直接的な攻撃を行っていた。これに対し、企業は、ファイアウォール（FW）を設置したり、ネットワークアドレス変換（NAT）を行うなどして、外部からの直接接続を不可能にして、企業からインターネットへの限られたサービス（メールやウェブ）のみ許可を与える対策を行った。そこで攻撃者はボットや遠隔操作型マルウェアをメールやウェブ経由で企業に送付し、組織内の端末への感染、および感染端末が組織内部からインターネットに接続して指令サーバとコミュニケーションをとるような仕組みを採用するようになった。さらに企業はこの対策としてプロキシを設置したり、プロキシの認証機能を設定することによって、マルウェアが容易に外部に出られないような対策を行ってきた。しかし、前述したように、プロキシでの認証機能による対策をも突破するマルウェアの出

現が確認され、企業の最終砦を知らず知らずのうちに突破されている懸念が高まってきているのが現状である。

次に、プロキシ認証の仕組みについて述べる。企業の内部のネットワークと外部のネットワークとで通信する際、多くの企業ではプロキシサーバを介して企業内部の本人であるかどうかの本人認証を行う。このとき、あらかじめプロキシサーバでユーザ名とパスワードを設定したファイルを作成しておき、ブラウザではプロキシサーバにアクセスするように設定しておく。そして、ユーザ本人がブラウザ起動時に出現する認証確認画面で認証情報を入力することで、本人確認を行い、外部ネットワークとの通信を許可するという仕組みである。

バックドア通信型マルウェアの特徴として、あらかじめ設定していた攻撃チャネルの接続先サイト、または攻撃者自身のサイトと通信を行い、攻撃を行う。このとき、悪意のある外部サーバにアクセスする Connect 要求の 99.9%は SSL/TLS 通信である[5]。ここで、上記で設定した認証の手順を講じることで、マルウェアは外部サーバへアクセスする際に認証情報を要求され、単純に外部サーバへのアクセスだけをプログラミングされたマルウェアは外部サーバへのアクセスをできなくする。

しかし、上述の通り、最近のマルウェアにはこの認証情報を窃取して、プロキシ認証の際に窃取した認証情報をプロキシに認識させ、C&C サーバへとアクセスしてしまうものも確認されている。

また認証情報の窃取方法には以下の 5 つの方法が考えられる。以下の 5 つの方法はプロキシの認証情報の窃取方法として述べられているものではないが[5][6][7][8]、プロキシの認証情報の窃取方法にも用いられる可能性がある。

(1) 認証情報格納ファイル・レジストリから窃取
(2) キーロギング
(3) 画面取得による窃取
(4) Internet Explorer（IE）へのコードインジェクション
(5) ネットワーク盗聴

以下で、上記(1)〜(5)の認証情報の窃取方法の概要について述べる。

(1) 認証情報格納ファイル・レジストリから窃取

マルウェアが PC 中のプロキシ認証格納ファイル・レジストリにアクセスし、プロキシ認証情報を盗み見る方法が考えられる。具体例としてはマルウェアが FindFirstFile/FindNextFile API を用いて、指定したディレクトリ内のプロキシ認証格納ファイルを走査する方法である。

(2) キーロギング

ユーザのキーボード入力を盗み取って、プロキシ認証情報を窃取する方法が考えられる。キーボード入力を盗み取る方法としては以下の 2 種類がある。

a. システムフックを用いた方法

システムフックを用いたキーロギングでは、システム中の GUI プロセスに対して DLL を埋め込み、キーボード入力に伴うメッセージをフックする。フックされたメッセージは、マルウェアが用意した処理関数に入力される。

DLL の埋め込みには SetWindowsHookEx API を用いる。この API は様々なウィンドウメッセージに対するフック機構を提供する。キーロガーの多くがこの SetWindowsHookEx API を利用している。

b. システムフックを用いない方法

システムフックを用いないキーロギングでは、GetAsyncKeyState API や AttachThreadInput API が用いられる。

GetAsyncKeyState API は特定のキー入力がされているかどうかを判定する API で、一定時間ごとにこの API を呼び出して各キーに適用することでキーロギングを行う。

AttachThreadInput は他スレッドへのウィンドウメッセージを取得する API で、別ウィンドウへのキー入力を取得することでキーロギングを行う。

また、マルウェアはキーロギングを行う際に、GetForegroundWindow API を用いて、ユーザがどのアプリケーションに対してキー入力を行っているかを調べることがある。

(3) 画面取得による窃取

マルウェアがデスクトップ画面を取得する際に用いる 2 つの API について述べる。一つ目は GetDC API で、これによりデスクトップのデバイスコンテキストを取得する。二つ目は BitBlt API で、GetDC API で取得したデバイスコンテキストの内容（画面データ）を別のデバイスコンテキストに出力する。その後出力先のコンテキストの内容をファイル等に出力することで、デスクトップ画面の取得が完了する。通常、プロキシの認証情報の入力内容はマスキングされており、入力画面のみの窃取は困難であると考えられるが、認証情報入力の際に利用者がパスワード管理ソフトウェアを利用している場合、認証情報確認時に認証情報を映し出した画面情報が窃取される可能性がある。

(4) Internet Explorer（IE）へのコードインジェクション

プロキシを突破するタイプのマルウェアが有する機能や動作の特性に関しては、様々なセキュリティベンダから調査レポートが公開されている[6][7]。新型 PlugX と呼ばれる RAT（Remote Administration Tool）では、プロキシ認証を突

破する方法として

Internet Explorer（IE）にインジェクションし、プロキシの認証情報を自動的に窃取する仕組みがある。これにより、IE を起動するたびに新型 PlugX が IE に対してコードインジェクションを仕掛け、4 つの API（HttpSendRequestA API、HttpSendRequestW API、HttpSendRequestExA API、HttpSendRequestExW API）にフックをかけることでプロキシの設定情報や認証情報を窃取する。

(5) ネットワーク盗聴

また新型 PlugX にはネットワーク盗聴機能によりプロキシの認証情報を窃取する仕組みもある。ネットワーク盗聴により、プロキシ認証突破型マルウェアはプロミスキャスモードになってネットワーク盗聴を行い、HTTP の通信内容からプロキシの設定情報や認証情報を窃取する。具体的には、“Authorization: basic”に続く文字列（ユーザ名とパスワードが base64 エンコードされている文字列）をデコードして、ユーザ名やパスワードを取得し、それを新型 PlugX の設定に追加することで、プロキシの Basic 認証を使用して C&C サーバと通信を行う。

ここまで、一般的な認証情報の窃取方法と実際に確認されたプロキシ認証突破型マルウェア 1 検体に対する調査結果を示した。

3 章では、上記調査結果を基に、プロキシ認証突破型マルウェアのプロキシ認証突破の有無を自動判定する手法について述べる。また、提案した手法を M3AS の拡張機能として実装し、これを用いて複数種類のマルウェアを多種環境で解析し、各種分析した結果について述べる。

3. マルチモーダル解析システム（M3AS）

3.1 M3AS の概要

本報告ではプロキシ認証突破型マルウェアを解析するにあたり、著者らが研究開発している M3AS を用いて、解析したマルウェアの中にプロキシ突破するマルウェアがあるか、環境依存するかなど分析した。このため、M3AS のコンセプトと機能構成の概要をまず説明する。

これまでは、疑わしいファイルを発見した場合、専門家が解析用の環境で実行して挙動を観測し、どのような活動をするかを手作業で明らかにしてきた。しかし近年のマルウェアには、検知や解析を逃れるため、自身が動作する環境を選ぶものが増えてきており、これまでのような手法では日々増え続けるマルウェアの解析が追いつかないという課題がある。そこで、M3AS ではマルウェアを解析用の環境で実際に動かして挙動を観測する動的解析手法を応用し、様々な OS やソフトウェアを組み合わせた複数の解析環境の上で同時に自動解析する（図 1）。また解析環境の構築にあたって、複数種類の解析エンジンや、世の中で公開されている脆弱性情報や、マルウェアの攻撃傾向を調査し、攻撃を受けやすい環境、すなわちマルウェアが動作しやすい環境を選定、構築した。

上記コンセプトで解析環境を構築し、マルウェアを自動解析することで、専門家が不在の組織においても、解析精度を高めたり、解析時間を大幅に縮めたりすることができ、安全性向上やコスト削減を実現できる。

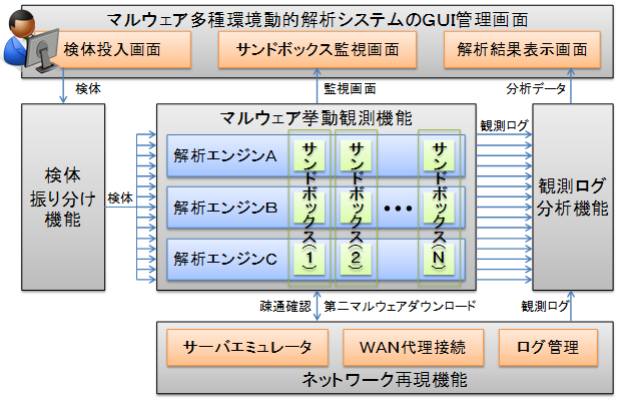

図 1 マルチモーダルマルウェア解析システム

3.2 M3AS の拡張

2 章で示したプロキシ認証情報窃取方法などによりプロキシ認証を突破するようなマルウェアが、実際にプロキシ認証を突破したか否かを判定する、プロキシ認証突破判定システムの概要を以下に示す。

本システムでは、下図の通りマルウェアを M3AS で解析し、マルウェアの挙動を解析する。解析環境はプロキシを介して擬似インターネットへ接続する構成とする。

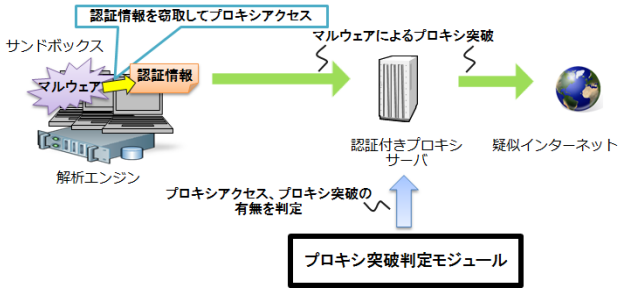

図 2 プロキシ認証突破判定システム

また、下図はプロキシのアクセスログの一部であり、ステータスコード“200”はプロキシ認証が成功し、要求した情報が返されたことを示しており、本実験ではプロキシを介して外部との接続確立が成功したことを示している。またステータスコード“407”はプロキシによる認証が必要であることを示しており、本実験ではプロキシを介した外部との接続確立が失敗したことを示している。

本システムでは、ある検体について、M3AS で解析した解析時間（解析開始時間と終了時間）のログを基に、プロ

キシアクセスのログを参照し、当該解析時間内にプロキシ認証が成功(ステータスが“200”)していれば、プロキシ認証突破型マルウェアであると判定する。

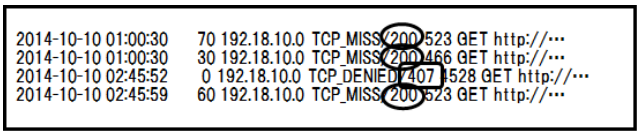

図 3　プロキシログ

また、プロキシ認証ではクライアント端末からプロキシサーバ間へ認証情報を送信し、プロキシがこれを処理したうえで、外部への Web アクセスを許可する。認証には下記 2 つの方式がある。

一つは BASIC 認証で、クライアント端末からプロキシ、ユーザ名とパスワードを“:”(コロン)でつなぎ、BASE64 でエンコードして送信する。プロキシはこれを認証し、認証情報が正しければステータス“200”を返す。

二つ目は Digest 認証で、ユーザ名とパスワードを MD5 でハッシュ化して送信する。本方式では、クライアント端末とプロキシ間でハッシュ化した認証情報をやり取りすることで、盗聴や改ざんを防ぐことを目的としている。

本報告でのプロキシ認証突破判定システムでは、認証付きプロキシの認証方式としてよく用いられる BASIC 認証を設定に用いた。

4. 各種分析結果と考察

本章では 2014 年 10 月の一ヶ月間に取得した 629 検体のマルウェアについて、プロキシ認証突破判定システムの判定結果に基づき、プロキシアクセス型マルウェア（プロキシ認証突破型マルウェア、プロキシ利用マルウェア（プロキシ認証失敗）を含む）の各種分析結果とその考察を述べる。またプロキシ認証突破判定結果の分析と考察にあたり、プロキシ認証が成功したマルウェアであっても、プロキシ認証成功した後のアクセス先 URL が明らかに不正サイトでない通信先のみであった場合には（たとえば Office の更新機能によるアクセスなど)、プロキシ認証突破判定の結果は「プロキシ認証突破」でなく「プロキシ利用（プロキシ認証失敗)」として分類した。

4.1 プロキシアクセス型マルウェアの検体数

一ヶ月間に取得した全 629 種類の検体（マルウェア）においてプロキシアクセス型マルウェアがどの程度の割合で存在するのかを把握するため、下表の通り整理した（Table 1)。下表では、全 629 検体のうち、プロキシアクセスした検体（プロキシアクセス型マルウェア）の数と、プロキシアクセスしなかった検体（プロキシアクセスなしのマルウェア）の数を示している。

表 1　プロキシアクセス型マルウェアの検体数

	検体数（全 629 検体）
プロキシアクセス型	92
プロキシアクセスなし	537

次に、プロキシアクセス型マルウェア（92 検体）すべてについて、M3AS による動的解析中に各サンドボックス内でブラウザ（IE）を起動して、予めプロキシ認証情報が保存されている認証ダイアログが起動したタイミングで OK ボタンをクリックし、擬似インターネットにアクセスした後、ブラウザを終了する一連の処理を自動的に行う機能を実装した。これにより、プロキシ認証突破した検体（プロキシ認証突破型マルウェア）を 8 検体確認した。

上記処理により得た結果を表 2 に示す。

表 2　プロキシ認証突破型マルウェアの検体数

	検体数（全 629 検体）
プロキシ認証突破型	8
プロキシ利用型 (プロキシ認証失敗)	84
プロキシアクセスなし	537

ここで、本解析では解析環境が外部ネットワークから隔離された(攻撃者から画面情報を盗み見ることができない)環境で、解析の手順も、予めプロキシ認証情報が保存されている認証ダイアログの OK ボタンをクリックするのみ（キーボード入力なし）の処理を行っている。このため、上記で確認したプロキシ認証突破型マルウェアは全て、キーロガーや画面窃取以外の方法で認証情報を窃取するタイプのマルウェアであるといえる。

4.2 プロキシアクセス型マルウェアの検体数（拡張子別）

4.1 節で分類したプロキシ認証突破型マルウェア、プロキシ利用型マルウェア（プロキシ認証失敗)、プロキシアクセスなしマルウェアそれぞれについて、特にプロキシ認証突破型マルウェアがどの拡張子のファイルに多い傾向があるかを把握するため、下表（表 3）の通り拡張子別に分類した。

表 3　プロキシアクセス型マルウェアの検体数(拡張子別)

	拡張子							
	bat	dll	doc	exe	pdf	jar	rtf	scr
プロキシ認証突破型	0	0	1	7	0	0	0	0

プロキシ利用型 (プロキシ認証失敗)	1	0	4	65	0	0	14	0
プロキシアクセスなし	1	1	4	410	1	1	113	6
検体の総数	2	1	9	482	1	1	127	6

本分析の結果、プロキシ認証突破型のマルウェアには exe 形式や doc 形式のファイルが特に多い傾向があることが分かった。また、拡張子が doc や exe のマルウェアはプロキシ利用型（プロキシ認証失敗）の数に対してプロキシ認証突破型のマルウェアが一定の割合で（それぞれ 4:1、65:7）で存在したが、拡張子が rtf のマルウェアについてはプロキシ利用型（プロキシ認証失敗）14 検体に対してプロキシ認証突破型 0 検体という結果を得た。

4.3 VirusTotal での分析結果（ハッシュ値別）

近年、標的型攻撃が増加しているなか、これら標的型攻撃に用いられるマルウェアのウィルス対策ソフトによる検知率が低下している[9][10][11]。このことから、プロキシ認証突破型マルウェアのほうがより高度な機能を具備している分、プロキシ利用マルウェア（プロキシ認証失敗）やプロキシアクセスなしマルウェアよりもウィルス対策ソフトによる検知率が低い、という仮説を立て、検証を行った。具体的には VirusTotal[12]での判定結果の傾向を検体ハッシュ値（MD5 ハッシュ値）を用いて調査した。

上記分析の結果を下表（表 4）に示す。Table 4 では、上記各タイプのマルウェアについて、各タイプの全検体のうち VirusTotal で検知できなかった検体数の比率を表す。

表 4　VirusTotal での分析結果（ハッシュ値別）

	解析不可の検体数の割合
プロキシ認証突破型 (8 検体)	50%
プロキシ利用型 (プロキシ認証失敗) (84 検体)	39%
プロキシアクセスなし (537 検体)	36%

本分析の結果、プロキシ認証突破型マルウェアが VirusTotal でマルウェアと検知できなかった比率は 50%であり、プロキシ利用マルウェア（プロキシ認証失敗）が VirusTotal で解析できなかった比率は 39%、プロキシアクセスなしマルウェアが VirusTotal で解析できなかった比率は 36%であった。上記の分析結果から、仮説で示した傾向が見られたが、検体数が少数であるため今後も検体数をさらに増やして分析を重ねていく必要がある。

4.4 VirusTotal での分析結果（アクセス先 URL 別）

4.3 節と同様の仮説のもと、プロキシにアクセスのあったアクセス先 URL 別に VirusTotal で分析した。

表 5 では、プロキシ認証突破型マルウェアのアクセス先 URL と、プロキシ利用マルウェア（プロキシ認証失敗）のアクセス先 URL それぞれについて、全サイトのうち、VirusTotal での解析の結果、不正サイトであると判定された判定結果が「0」のアクセス先 URL と VirusTotal で解析できなかったアクセス先 URL との合計サイト数の比率を表す。

表 5　VirusTotal 解析結果（アクセス先 URL 別）

	解析不可のアクセス先 URL の割合
プロキシ認証突破型（17 サイト）	64.7%
プロキシ利用型 (プロキシ認証失敗)（90 サイト）	29.6%

本分析の結果、プロキシ認証突破型マルウェアのアクセス先 URL が VirusTotal で解析できなかった（もしくは不正サイトとして判定されなかった）比率は 64.7%であり、プロキシ利用マルウェア（プロキシ認証失敗）のアクセス先 URL が VirusTotal で解析できなかった（もしくは不正サイトとして判定されなかった）比率は 29.6%であり、仮説で示した傾向が見られることが確認できた。攻撃者も、プロキシ認証突破するタイプのマルウェアのアクセス先サイトについてはウィルスチェックサイトの検知から巧妙に隠ぺいしようとしている可能性がある。

4.5 国別のアクセス先サイトの数

NISC（内閣官房情報セキュリティセンター）では、平成 25 年度における標的型メール攻撃で使用された不正プログラム等の国別のアクセス先の調査結果を公開している[13]。

本報告でも、プロキシアクセス型のマルウェアのアクセス先サイトがどの国のネットワークセグメントに多い傾向があるかを把握し、これにより攻撃者がどの国から攻撃を仕掛けてきているかの紐付けや、対策につなげるための判断材料とするため、プロキシアクセス型マルウェアのアクセス先サイトを国別で分類した結果を表 5 と図 4 に示す。

表 6　国別のアクセス先サイトの数

	アメリカ	オランダ	カナダ	リトアニア	ベトナム	フランス	イタリア	日本	イギリス	その他
アクセス先 URL のサイト数	36	10	4	4	3	2	2	2	2	10

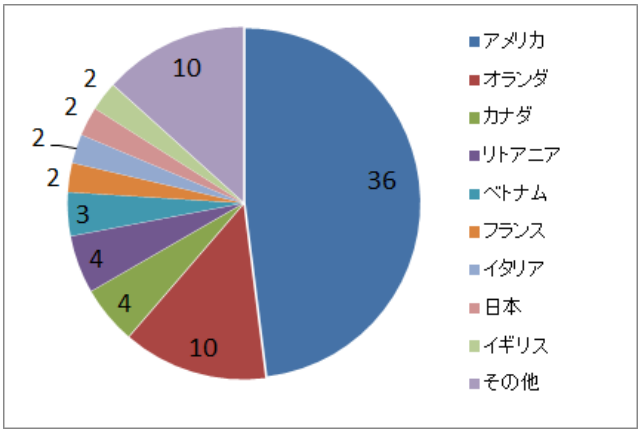

図 4　国別のアクセス先サイトの割合

文献[12]の調査結果では、標的型メール攻撃に使用されたアクセス先は 1 位パレスチナ、2 位ウクライナ、3 位米国であった。本分析結果では文献[13]の通りの国別順位ではなかったが、標的型メール攻撃のアクセス先として大半が国外であるという傾向は NISC の公開情報と同じく確認できた。

4.6　プロキシ認証突破型マルウェアの動作依存環境の分析結果

プロキシ認証突破型マルウェア（8 検体）について、動作環境の傾向を把握し、対策につなげていくことを考え、M3AS での多種環境解析結果を用いて環境依存の傾向を分析した（表 7）。

表 7 では、M3AS の各サンドボックスの構成要素（物理・仮想や OS、インストールアプリなど）別の各サンドボックスと、上記の各サンドボックス別でと、プロキシ認証突破したか否か（プロキシアクセスの有無）とをパラメータとして、相関係数を算出した。

表 7　プロキシ認証突破型マルウェアの相関係数算出結果

Malware ID	Physical PC	Virtual PC	Japanese	English	Office 2007	Office 2010	…
1	-0.35	0.48	0.11	-0.11	-0.12	0.24	…
2	0.14	-0.07	-0.44	0.44	0.15	-0.06	…
3	0.36	-0.17	-0.12	0.12	0.17	-0.15	…
4	0.12	0.02	-0.10	0.10	0.71	-0.28	…
5	-0.38	0.08	0.16	-0.16	-0.28	0.12	…
6	0.29	-0.14	-0.89	0.89	0.30	-0.12	…
7	0.15	-0.07	0.03	-0.03	-0.09	-0.06	…
8	0.32	-0.30	-0.15	0.15	-0.01	-0.03	…

本分析の結果、プロキシ認証突破した 8 検体のマルウェアのうち、2 検体のマルウェアで強い相関があるパラメータがあることを確認した。

たとえば、検体 ID が「4」のマルウェアにおいて、Office2007 がインストールされているサンドボックスで動作する傾向が強いことが確認できた。また、検体 ID が「6」のマルウェアにおいて、言語が English のサンドボックスで動作する傾向が強いことが確認できた。ただし、他の 6 種類のプロキシ認証突破型のマルウェアでは特には環境依存の傾向が見られなかったことから、プロキシ認証突破型マルウェアであることと環境依存性を有することとが同値ではないと考えられる。マルウェアの動作と環境との相関関係をより厳密に算出する際には文献[4]の評価手法の適用も考えられる。

4.7　プロキシ認証突破型マルウェアの解析ログ分析結果

プロキシ認証突破したマルウェアがどのようにして認証情報を窃取し、プロキシ認証突破したかを特定するために、M3AS の解析エンジンによる解析ログ情報を分析した。下図（図 5）はプロキシ認証突破したマルウェアのうち 1 検体の、解析ログの Strings（マルウェアのバイナリファイル中に含まれている文字列抽出部分）の一部抜粋である。

```
…
“eueyuey7832783unquestion”,
“Label3”,
“Label8”,
“Label1”,
“fulltime”,
“user32”,
“GetAsyncKeyState”,
“GetKeyState”,
“GetForegroundWindow”,
“GetWindowTextA”,
“advapi32.dll”,
“RegCloseKey”,
…
```

図 5　プロキシ認証突破型マルウェアの解析ログ

本分析から、マルウェアのバイナリファイル中に 2 章で述べたキーロギングに用いられる API（たとえば“GetAsyncKeyState API”，“GetForegroundWindow API”）が含まれていることが分かった。実際にマルウェアを動的解析したログからは上記 API の呼び出しは確認できなかっ

た。今回の実験ではキーボード入力をせずに解析したため、本マルウェアがキーロギングによる認証情報窃取以外の方法でプロキシ認証突破したことは明らかであるが、認証情報窃取方法の一つとして上記 API も利用するタイプのマルウェアである可能性がある。

5. おわりに

本報告では, マルチモーダルマルウェア解析環境（M3AS）を用いて 2014 年 10 月からの一ヶ月間で取得したマルウェアについてのプロキシアクセス型マルウェアの各種分析結果を示した。

上記分析を行うにあたり，まずプロキシ認証情報の窃取方法を調査し、その結果を踏まえて M3AS の拡張機能としてプロキシ認証突破判定手法のプロトタイプを開発した。

開発したプロトタイプを用いてマルウェアの解析を行い、プロキシアクセス型マルウェアに関する各種分析結果を示した。具体的には、解析した全 629 検体のマルウェアのうち 84 検体がプロキシ利用するマルウェアで、8 検体がプロキシ認証突破するマルウェアであることを確認した。4 章で示した分析結果は今後、プロキシアクセス型マルウェアに対する迅速な検知手法の考案に活用することができると考える。

今後の課題の一つとして，プロキシ認証突破判定機能においてサンドボックスのブラウザの種類を変えてプロキシアクセスの挙動が変わるかどうかの追加分析が挙げられる。また、プロキシ認証情報の窃取方法の特定手法を確立し、プロキシ認証突破型マルウェアの対策手法につなげていくことも今後の課題として挙げられる。

謝辞 本研究の評価にあたりご協力頂いた皆様に，謹んで感謝の意を表する．

参考文献

1) 日本情報経済社会推進協会（JIPDEC）, IT Report 2014 Spring, http://www.jipdec.or.jp/WSR/itreport_spring.pdf
2) IPA,「2013 年版 10 大脅威」～セキュリティ専門家が選んだセキュリティ脅威～, http://www.ipa.go.jp/security/event/2013/isec-semi/documents/2013ten_threats_v1.pdf
3) IPA, 「高度標的型攻撃」対策に向けたシステム設計ガイド, http://www.ipa.go.jp/files/000042039.pdf
4)仲小路博史, 重本倫宏, 鬼頭哲郎, 林直樹, 寺田真敏, 菊池浩明, “多種環境マルウェア動的解析システムの提案”, コンピュータセキュリティシンポジウム 2014 論文集 pp984-pp991
5) IPA, 「標的型サイバー攻撃対策」, 2014 年 2 月. http://www.ipa.go.jp/security/event/2013/isec-semi/documents/2013videosemi_targeted_cyber_attacks_v1a.pdf
6) IIJ, 新型 PlugX の出現, 2013 年 11 月, https://sect.iij.ad.jp/d/2013/11/197093.html
7) トレンドマイクロ, 標的型攻撃に利用される PlugX の脅威とは, http://about-threats.trendmicro.com/relatedthreats.aspx?language=jp&name=Pulling%20the%20Plug%20on%20PlugX
8) Michael Sikorski , Andrew Honig, “Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software”, No Starch Press, 2012 年 2 月
9) マクニカネットワークス, 既存セキュリティ対策をすり抜ける標的型攻撃を検知し適切な防御策を支援, http://diamond.jp/articles/-/19410?page=2
10) すべてわかるセキュリティ大全―基礎知識から最新の攻撃手法や対策まで, 日経 BP 社, 2014 年 9 月
11) 三井物産セキュアディレクション, サイバーセキュリティ事件簿, http://www.mbsd.jp/casebook/20130212.html
12) VirusTotal, https://www.virustotal.com/ja/
13) NISC, 「標的型攻撃等の脅威について」, 2014 年 9 月, http://www.nisc.go.jp/conference/suishin/ciso/dai18/pdf/2.pdf