情報処理学会論文誌 Vol.60 No.9 1466–1476 (Sep. 2019)

標的端末上でのみ動作するマルウェアに対するセキュリティアプライアンスの有効性評価

田辺 瑠偉[1,a)] 上野 航[2] 星澤 裕二[2] 齋藤 孝道[4] 笠間 貴弘[5]
井上 大介[5] 吉岡 克成[1,3] 松本 勉[1,3]

受付日 2018年11月26日, 採録日 2019年6月11日

概要：近年，ネットワーク内の通信を監視する機能を有するネットワークアプライアンスや未知のファイルをサンドボックス上で解析する機能を有するサンドボックスアプライアンスが人気を集めている．しかし，その一方で，攻撃者は標的端末上でのみ不正活動を行うマルウェアを作成することで，サンドボックスアプライアンスによる検知を回避する恐れがある．実際に，我々は先行研究において，攻撃者は標的端末に埋め込んだ情報を用いてサンドボックスアプライアンスによる検知の回避が可能であることを確認しており，セキュリティベンダに対して注意喚起を行った．本研究では，特に Browser Fingerprinting を用いて標的端末の情報を収集する偵察行為を想定し，これらの情報を用いて標的組織への侵入がどのように行われるか考察する．また，実組織において運用されているセキュリティアプライアンスによる検知が回避されうるか検証する．検証実験の結果，8 つのネットワークアプライアンスに検知されることなく標的端末から情報が収集可能であることを確認した．また，標的端末上でのみ動作する擬似マルウェア検体を作成し，3 つのサンドボックスアプライアンスに対して検知の回避が可能であることを確認した．Browser Fingerprinting は正規のサイトでも用いられているため，標的端末から情報を収集する偵察行為を検知することは難しく，マルウェア感染を未然に防ぐことを目的としたサンドボックスアプライアンスの性能向上が必要である．

キーワード：セキュリティアプライアンス，サンドボックス回避，標的型攻撃

Evaluation of Security Appliance against Customized Malware

Rui Tanabe[1,a)] Wataru Ueno[2] Yuji Hoshizawa[2] Takamichi Saito[4] Takahiro Kasama[5]
Daisuke Inoue[5] Katsunari Yoshioka[1,3] Tsutomu Matsumoto[1,3]

Received: November 26, 2018, Accepted: June 11, 2019

Abstract: In recent years, Network appliances that are designed to monitor network traffic and Sandbox appliances that are designed to detect unknown binaries which protect users from malware infection are becoming popular. However, adversaries can evade such Security appliances by implementing customized malware that only reveal its malicious behavior on targeted specific system. In our previous work, we have evaluated resilience of Sandbox appliances against customized malware that use marks, implanted in the reconnaissance phase, to identify target specific system. We disclosed our results to security vendors to insist the threat of customized malware. In this study, instead of implanting features, we use Browser Fingerprinting to gather information from the target system and show how adversaries can use Fingerprints to intrude target specific system. We evaluate Security appliances that are operated in a real organization to see if they can detect our test samples. From the experiment, none of the 8 Network appliances detected access to our web site that collected Fingerprints from the target specific system. We also examined that none of the 3 Sandbox appliances detected our test sample that search Fingerprints of the target specific system. Browser Fingerprinting is also used among many benign web sites that, it is difficult to detect Fingerprint-based reconnaissance attack. Therefore, it is important to improve resilience of Sandbox appliances against customized malware and prevent malware infection.

Keywords: security appliance, sandbox evasion, advanced persistent threat

1. はじめに

特定の企業や組織を執拗に狙った標的型攻撃による被害が深刻化している．標的型攻撃への対策を考えるうえで，攻撃の早い段階でマルウェアの侵入を防ぐことは重要である．アンチウイルスソフトをはじめとするマルウェア対策技術が広く普及しているが，このような対策技術を回避する高度なマルウェアが増加している．たとえば，悪意のあるコードを無害なプロセスの中に隠蔽するプロセスインジェクションやOS起動前に起動するブートキットを利用したマルウェア，実行ファイルをメモリ上に作成することでファイルの検査を回避するファイルレスマルウェアなどが存在する [27], [28]．そのため，標的組織のネットワークを監視するセキュリティアプライアンスや，標的端末の振舞いを監視する高度なエンドポイント対策技術が注目されている．エンドポイント対策技術については今後導入が進むことが予想され，その有効性についてはさらなる評価が必要である．一方，企業や官公庁といった多くの組織では，セキュリティアプライアンスの導入が進んでいる．また，セキュリティアプライアンスのみを導入している組織も存在する．このため，セキュリティアプライアンスによるマルウェアの検知が回避された場合には重大なセキュリティインシデントにつながる可能性があり，セキュリティアプライアンスは標的型攻撃に用いられる高度なマルウェアへの対策技術として重要な役割を果たしている．なお，セキュリティアプライアンスの種類はその機能によって様々であるが，本研究ではネットワーク通信を解析する機能を持つセキュリティアプライアンスをネットワークアプライアンスと呼び，サンドボックス解析機能を持つセキュリティアプライアンスをサンドボックスアプライアンスと呼ぶこととする．

セキュリティアプライアンスが人気を集めている一方で，攻撃者はサンドボックス解析を回避する機能をマルウェアに搭載するようになった．たとえば，仮想化技術やエミュレータなどのサンドボックスを構築する技術を検知するマルウェアが報告されている [2], [3]．これらのマルウェアは実行環境の情報を収集し，あらかじめ設定した条件と一致した場合に実行環境がサンドボックスであると判断する．このため，実マシンと区別がつきにくいサンドボックスを実現する研究が進んでいる [9], [10], [11], [25]．

しかし，近年，標的端末上でのみ動作するマルウェアが登場した．たとえば，標的端末のセキュリティ識別子（SID）やファイルシステムの情報を基に自身を復号して動作するマルウェアが報告されている [4], [5]．また，音声認証や顔認証などを利用してターゲットを絞り込めるマルウェアが開発されている [29]．これらのマルウェアは，実行環境から収集した情報が標的端末の情報と一致した場合にのみ，実行環境が標的端末であると判断して不正活動を行う．一方，サンドボックスなどで実行された場合には不正活動を行わない．そのため，サンドボックス固有の特徴を隠蔽することを目的とした従来の対策では，このようなマルウェアの本来の挙動を把握することは難しい．加えて，我々は先行研究 [1] において，攻撃者が標的端末に埋め込んだ情報を用いて標的端末上でのみ動作するマルウェアを作成した場合の攻撃シナリオを想定し，実組織で運用されているサンドボックスアプライアンスによる検知の回避が可能であることを確認した．セキュリティアプライアンスの検知範囲は多岐にわたるが，標的型攻撃の初期段階に対して有効に働くことが望ましい．このため，セキュリティアプライアンスの有効性を評価することは重要である．

本研究では，攻撃者が標的端末上でのみ動作するマルウェアを作成して標的組織へ侵入する攻撃シナリオを想定し，セキュリティアプライアンスの有効性を評価する．標的端末上でのみ動作するマルウェアを作成するには，攻撃者は標的端末の情報を事前に収集する必要がある．一般に，標的型攻撃の初期段階では，標的組織の情報システムやセキュリティ対策などに関する情報の収集が入念に行われる [22]．そこで，Browser Fingerprintingを用いて標的端末の情報を収集する偵察行為を想定し，これらの情報を用いて標的型攻撃の侵入行為がどのように行われるか検討する．また，実組織で運用されているネットワークアプライアンスやサンドボックスアプライアンスによる検知が回避されうるか検証する．そして，先行研究 [1] で指摘した，標的端末に埋め込んだ情報を用いて標的端末に侵入する攻撃シナリオを整理し，本攻撃シナリオへの対策について考察する．

検証実験では，Browser Fingerprintを取得するWebサイトを用いて，標的端末から25種類の情報を8つのネットワークアプライアンスに検知されることなく収集可能であることを確認した．また，9種類の情報を用いて標的端末上でのみ動作する擬似マルウェア検体を作成し，3つのサンドボックスアプライアンスに対して検知の回避が可能であることを確認した．本研究は標的端末上でのみ動作するマルウェアによるサンドボックス解析回避を困難にし，サ

[1] 横浜国立大学先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[2] 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
[3] 横浜国立大学大学院環境情報研究院
Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[4] 明治大学
Meiji University, Kawasaki, Kanagawa 214–8571, Japan
[5] 国立研究開発法人情報通信研究機構
National Institute of Information and Communications Technology, Koganei, Tokyo 184–8795, Japan
[a)] tanabe-rui-xj@ynu.ac.jp

イバー攻撃の標的となりうる組織のセキュリティ向上に資することを目的としている．このため，サンドボックスアプライアンスのセキュリティベンダ計 14 社に対して，標的端末上でのみ動作するマルウェアの脅威を指摘し，推奨される対策方法などの情報提供を行った．具体的には，マルウェア検体を動的解析した際に発生した不正活動の有無だけではなく，実行環境の情報を取得する挙動をとらえることで，標的端末上でのみ動作するマルウェアを検知できる可能性があることを伝えた．このうち，1 社からは提供情報に基づき，システムの改善を行った旨の連絡を受けている．また，このうち 1 社とは開発を行っている技術者と今後の対策について直接意見交換を行った．

以降では，2 章で関連研究を説明し，3 章で攻撃シナリオについて説明する．そして，4 章で Fingerprint ベースの攻撃に対するセキュリティアプライアンスの有効性を評価し，5 章で Implant ベースの攻撃に対するセキュリティアプライアンスの有効性を評価する．最後に，6 章で考察を行い，7 章でまとめと今後の課題を説明する．

2. 関連研究

前述のとおり，攻撃者はサンドボックス解析を回避する機能をマルウェアに搭載するようになった．このため，サンドボックス構築技術やサンドボックス解析技術に関する研究が活発に行われている．

サンドボックス構築技術：これまでに実マシンと区別がつきにくいサンドボックスを実現する研究が行われている．論文 [9] では，攻撃者がサンドボックスを検知するのに利用する情報を調べ，サンドボックスの情報を実マシンの情報に置き換える手法が提案されている．論文 [10] では，ハードウェアの仮想化支援技術を用いてサンドボックスを実現する方法が提案されている．論文 [11] では，サンドボックスを実ハードウェア上で実現する方法が提案されている．論文 [25] では，サンドボックス固有の特徴を少なくしたサンドボックスを実ハードウェア上で実現する方法が提案されている．一方，論文 [23] では，Android マルウェア向けのサンドボックスを実デバイス上で実現する方法が提案されている．論文 [24] では，Android マルウェアが解析環境の検知に用いる技術を分類することで，回避耐性を有するサンドボックスを実現する方法が提案されている．

また，解析環境の向上を目的に，サンドボックスに見られる特徴を明らかにする研究が行われている．論文 [6] では，Android サンドボックスの情報を収集し，Fingerprint を作成することで解析を回避する攻撃が指摘されている．論文 [7] では，サンドボックスとユーザマシンの利用履歴の差が明らかにされている．我々は論文 [8] において，サンドボックスの情報を収集するツールを提案し，サンドボックスに共通して見られる特徴を明らかにした．

サンドボックス解析技術：サンドボックス解析を回避するマルウェアは実行環境の差異によって挙動を変えるため，この特徴を検知する研究が行われている．論文 [12] では，マルウェアの挙動を観測する技術が組み込まれたサンドボックスとそうでないものを用意して挙動の差異を検知する手法が提案されている．論文 [13] では，マルウェアの挙動をモデル化する手法を提案し，実現技術の異なるサンドボックス上でマルウェアを実行したときの挙動の差異を検知する手法が提案されている．また，論文 [14] では，プログラム内の分岐を検出してマルウェア本来の挙動を明らかにする手法が提案されている．論文 [26] では，マルウェアが実行環境をサンドボックスであると判断するのに用いるシステムコールを検知する手法が提案されている．

このように，サンドボックス解析を回避するマルウェアに対抗する技術の研究開発が進んでいる．しかし，その多くはサンドボックス固有の特徴を隠蔽することや，実行環境から収集した情報があらかじめ設定した条件と一致した場合にサンドボックスであると判断するマルウェアの検知を目的としており，標的端末上でのみ動作するマルウェアの挙動を把握できるとは限らない．そこで，本研究では，攻撃者が標的端末上でのみ動作するマルウェアを用いて標的組織へ侵入する攻撃シナリオを検討する．また，本攻撃シナリオに対するネットワークアプライアンスとサンドボックスアプライアンスの有効性を評価する．

3. 攻撃シナリオ

標的型攻撃の手口は様々であるが，情報処理推進機構では攻撃のステップを①計画立案，②攻撃準備，③初期潜入，④基盤構築，⑤内部侵入・調査，⑥目的遂行，⑦再侵入，の 7 つに分類している [15]．このように標的型攻撃はいくつかのステップに分けられ，攻撃者が標的組織内のセキュリティ対策を回避して継続的かつ秘密裏に不正活動を行うことで，標的組織の情報漏えいや改ざんといった重大なインシデントにつながることが知られている．本研究では，標的型攻撃の初期段階に注目して，攻撃の流れを偵察フェーズと侵入フェーズに分類する．以降では，3.1 節で偵察フェーズを説明し，3.2 節で侵入フェーズを説明する．

3.1 偵察フェーズ

偵察フェーズでは，攻撃者は標的端末上でのみ動作するマルウェアを作成するのに必要な情報を標的端末から収集，あるいは，標的端末に埋め込むことを目標とする．また，その際，ネットワークアプライアンスに検知されることなく秘密裏に攻撃を遂行することを目標とする．**図 1** に偵察フェーズの流れをまとめる．

標的に関する情報を収集する方法は多岐にわたるが，多くの組織がインターネットを利用しており，電子メールや Web ブラウジングは日常業務において必要不可欠となっている．そこで，攻撃者は自身の管理下に置かれた Web サ

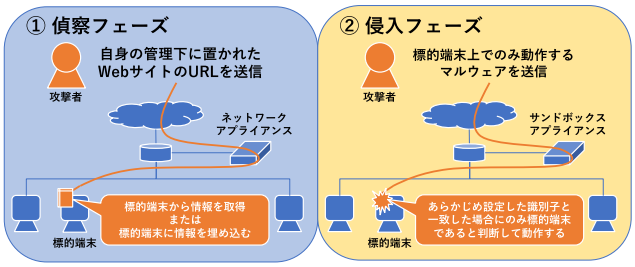

図 1 攻撃シナリオの概要
Fig. 1 Overview of the attack scenario.

イトの URL を標的にメールで送信し，URL をクリックさせる攻撃を想定する．標的に送信する URL には，標的端末から情報を収集することを目的とする (1) **Fingerprint ベース**の偵察行為と，標的に情報を埋め込むことを目的とする (2) **Implant ベース**の偵察行為が考えられる．以降では，それぞれの偵察行為について説明する．

Fingerprint ベースの偵察行為：本攻撃シナリオでは，攻撃者は標的端末から収集した特徴 (Fingerprint) を識別子として，標的をマルウェアに感染させる攻撃を想定する．標的の情報を収集する技術は多岐にわたるが，Web ブラウザの情報を収集することを目的とした Browser Fingerprinting の研究開発が進んでいる．このため，標的型攻撃においても Browser Fingerprint を取得する Web サイトの URL を標的に送信する偵察行為が考えられる．当該技術は多くの正規サイトで利用されているため [16]，ネットワークアプライアンスで検知することは難しく，攻撃者は標的端末から怪しまれずに情報を収集することができる．ユーザが端末を個別にカスタマイズしている環境では，標的端末に固有，かつ，時間による変化が少ない特徴を収集することができる Browser Fingerprinting が有効である．

Implant ベースの偵察行為：機器の管理やセキュリティを高めるためにすべての端末を同一のイメージで管理する環境下では，サンドボックスも同一のイメージを持つことが予想される．このため，標的端末から取得した Fingerprint が標的端末の特定に有効に働くとは限らない．そこで，本攻撃シナリオでは，攻撃者は標的端末に埋め込んだ情報を識別子として，標的をマルウェアに感染させる攻撃を想定する．標的に情報を埋め込む方法には，攻撃者が自身の管理下に置かれた Web サイトの URL を標的に送信して，ブラウザの閲覧履歴やキャッシュに URL 情報を埋め込む偵察行為が考えられる．攻撃者が用意する Web サイトは，アクセスしたクライアントに対して攻撃を行うサイトである必要はなく，正規の Web サイトと同じ構成のサイトを用いることができるため，攻撃者は標的に気付かれることなく情報を埋め込むことができる．ただし，埋め込んだ情報は削除，上書きされる可能性があるため，偵察フェーズと侵入フェーズの間の時間を適切に設定する必要がある．

3.2 侵入フェーズ

侵入フェーズでは，攻撃者は標的端末上でのみ動作するマルウェアを用いて標的に侵入することを目標とする．また，その際，サンドボックスアプライアンスに検知されることなく秘密裏に攻撃を遂行することを目標とする．図 1 に侵入フェーズの流れをまとめる．

実際に，標的端末上でのみ動作するよう設定されたマルウェアが攻撃キャンペーンに用いられたケースが報告されている [4]．しかし，標的端末を特定するのに用いられた情報は Web 経由での収集が困難であり，攻撃者は事前に標的端末に侵入する必要などがある．そこで，本攻撃シナリオでは，攻撃者は標的端末に事前に侵入することなく，偵察フェーズで収集した情報/埋め込んだ情報を識別子として標的端末上でのみ動作するマルウェアを作成する攻撃を想定する．攻撃者は作成したマルウェアはメールに添付するなどして標的に送信し，標的端末上で実行されたマルウェアは実行環境の情報を収集して，あらかじめ設定した識別子と一致した場合にのみ実行環境が標的であると判断する．その際，悪性ペイロードを復号する機能をマルウェアに搭載することで，サンドボックス解析だけでなく静的解析を難しくすることができる．

4. Fingerprint ベースの攻撃に対するセキュリティアプライアンスの有効性評価

本章では，Browser Fingerprinting を用いた偵察行為により作成した，標的端末上でのみ動作するマルウェアに対するセキュリティアプライアンスの有効性を評価する．以降では，Browser Fingerprinting を用いて 25 種類の情報を収集する Web サイトを 4.1 節で説明し，構築した Web サイトを用いてネットワークアプライアンスの有効性を評価した結果を 4.2 節で説明する．そして，収集した情報を用いて作成した擬似マルウェア検体を 4.3 節で説明し，作成した検体を用いてサンドボックスアプライアンスの有効性を評価した結果を 4.4 節で説明する．

4.1 Browser fingerprint を取得する Web サイトの構築

Browser Fingerprinting で収集できる情報は多岐にわたるが，本研究では 3 つに分類する．**表 1** に Browser Fingerprint を取得する Web サイトが収集する情報をまとめる．

(1) **Hardware**：システムの基本となっているハードウェアを変更するためには大きなコストがかかるため，標的端末から収集できる情報は一定していることが予想される．また，リソースが限られているサンドボックスには見られない特徴的な値が取得できる可能性がある．

(2) **Software**：標的端末に関する様々な情報を収集する

表 1 Browser Fingerprinting を用いて取得する情報
Table 1 Fingerprinting features.

分類	特徴	説明
Hardware	Device Pixel Ratio	画像の1ピクセルを端末のディスプレイ上でレンダリングする際の比率
	Physical Cores	物理プロセッサの推定数
	Screen Size	スクリーンの横と縦の長さ
	Sorted Screen	スクリーンの向きを無視したスクリーンの大きさ
	SSE2	倍精度浮動小数点数(64ビット)演算のための拡張命令の実装の有無
	Touch Enable	タッチパネルでのタッチ操作の可否
Software	Canvas Fingerprint	Canvas要素を利用した文字や図の描画結果
	Do not Track	HTTPリクエストヘッダー内のDNT(Do No Track)設定の有無
	Font	端末にインストールされているフォント
	HTTP Accept	ブラウザが利用可能なデータ形式
	HTTP Accept Charset	ブラウザが利用可能な文字セット
	HTTP Accept Encoding	ブラウザが利用可能な圧縮方式
	HTTP Accept Language	ブラウザが利用可能な言語
	HTTP Connection	TCPコネクションの継続性
	HTTP Origin	フェッチの起点
	HTTP User Agent	HTTPヘッダーから取得したUser Agent
	Java Script User Agent	JavaScriptで取得したUser Agent
	Local Storage Enable	明示的に削除しない限り永続的にデータを保存する仕組みの可否
	Plug-in	ブラウザにインストールされているプラグイン
	Session Storage Enable	ブラウザのタブが閉じられるまでデータを保存する仕組みの可否
	Time Zone	端末の時刻設定
	Version-free User Agent	ブラウザのバージョン情報を除いたUser Agent
Network	External IP Address	インターネット接続するのに利用しているIPアドレス
	Internal IP Address	内部のネットワークで利用しているIPアドレス
	ISP	External IPアドレスから推測したネットワークの設定

ことができる．たとえば，Web ブラウザに関する情報やシステムに関する情報などである．特に，システムにインストールするソフトウェアはユーザに依存するところが大きいため，同じハードウェアを利用しているユーザでも異なるソフトウェア情報が収集される可能性がある．

(3) **Network**：インターネットを利用するためにはネットワークの設定が必要である．このため，標的端末が内部のネットワークで利用しているローカル IP アドレスのほかに，インターネットと通信を行うためのグローバル IP アドレスやその ISP の情報を取得できる可能性がある．

4.2 ネットワークアプライアンスの有効性評価

Browser Fingerprint を取得する Web サイトを構築した．当該 Web サイトは研究室の Web サイトの一部であり，検索エンジンからアクセスすることができる．また，ユーザの同意が得られた場合にのみ Fingerprint を取得するよう設定されている．このため，同意が得られた場合にのみ Web ブラウザが JavaScript をダウンロードし，Fingerprint を取得してサーバに送信する仕組みとなっている．

実組織で運用されているネットワークアプライアンスの監視下にある端末を用いて，2017 年 4 月 12 日に構築した Web サイトへのアクセスを行った．ネットワークアプライアンスとは，保護対象組織内のネットワークトラヒックを監視して攻撃を検出することを目的とした，Firewall，IDS，IPS，Web Application Firewall（WAF），コンテンツフィルタなど様々なセキュリティ機能を有した装置である．

構築した Web サイトへのアクセスは 3 種類の Web ブラウザ（IE，Chrome，Firefox）から行った．この結果，すべての Web ブラウザから Browser Fingerprint を取得することができた．また，実験に用いた 8 種類のネットワークアプライアンスのいずれからもセキュリティアラートは確認されなかった．このため，攻撃者は Browser Fingerprinting を用いて標的端末から怪しまれずに情報を収集することができる．

4.3 標的端末上でのみ動作する検体の作成

攻撃者は実行環境が標的端末であると判断するために，標的端末でのみ見受けられ，かつ，時間による変化が少ない特徴を用いることが考えられる．そこで，Browser Fingerprint を取得する Web サイトをインターネット上に公開し，収集した Browser Fingerprint を分析することで，標的端末上でのみ動作するマルウェア検体を作成するのに有効な特徴を特定した．

構築した Web サイトを 2014 年 9 月から 2017 年 6 月までの間にインターネット上で公開したところ，32 カ国，4,470 の IP アドレスからアクセスを観測することができた．また，10,010 の Browser Fingerprint を取得することができた．各アクセスに対して Cookie 情報（以降では，UID と呼ぶこととする）を取得しており，同じブラウザからのアクセスを 1 つにまとめたところ，3,370 種類の Browser Fingerprint を取得することができた．さらに，1,332 の Web ブラウザから 2 回以上のアクセスが，822 の Web ブラウザから 7 日以上経過した後に 2 度目のアクセスが行われていた．そこで，取得した Browser Fingerprint がどの程度ユニークであり，時間による変化をどの程度受けるか調査した．

Browser Fingerprint のエントロピー：取得した Browser Fingerprint がどの程度ユニークであるか次の式で定義される Shannon Entropy を用いて計算した．

$$H(P) = -\sum_{A \in \Omega} P(A) \log_2 P(A)$$

ここで，$P(A)$ は確率密度関数であり Ω が Fingerprint の集合である．ただし，サンプル数の異なる計算結果を比較することは難しいため，次の式で定義される Normalized Shannon Entropy（NE）を用いた．

$$NE = \frac{H(P)}{\log_2 N}$$

ここで，N はサンプル数の合計であり，NE は 0 から 1 の範囲で計算される．**図 2** に取得した Browser Fingerprint のエントロピーを計算した結果をまとめる．この結果から，UserAgent，IP Address，Plug-in が高いエントロピーを有しており，標的端末の特定に有効であると予想される．また，攻撃者は取得した Browser Fingerprint を組み合わせることで，標的端末に固有な Fingerprint を作成することができる．

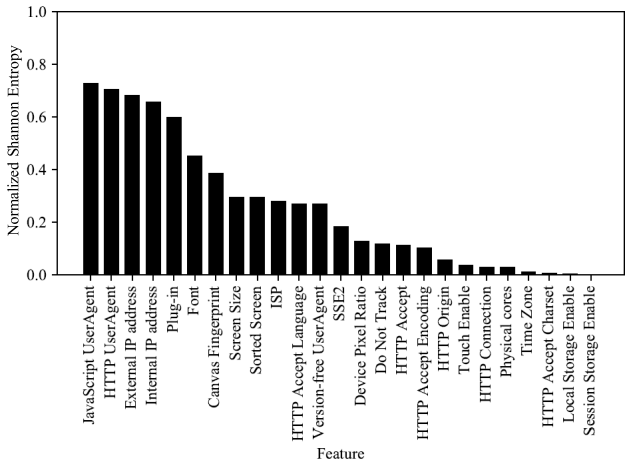

図 2 Browser Fingerprint のエントロピー（値が大きいほど情報量がある）

Fig. 2 Entropy of Browser Fingerprint (larger is better).

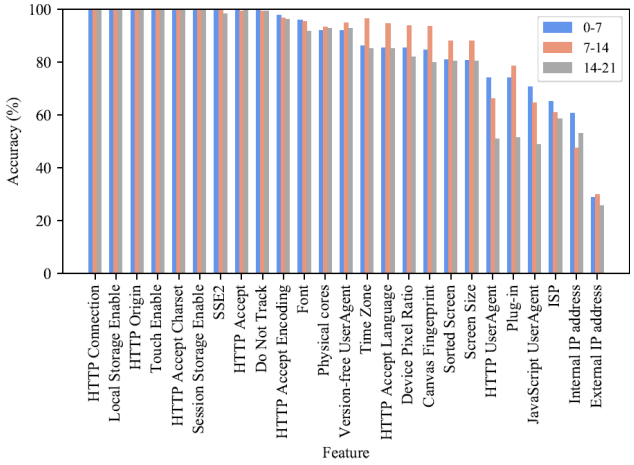

図 3 Browser Fingerprint の時間による変化（値が大きいほど変化が少ないことを表す）

Fig. 3 Time stability of Browser Fingerprint (larger is better).

Browser Fingerprint の時間による変化：続いて，Browser Fingerprint が時間とともにどのように変化するか調査した．Browser Fingerprint を 2 回以上取得することができた Web ブラウザに対して，1 度目のアクセスと 2 度目のアクセスで取得された情報が一致するかを次の期間ごとに計算した．**図 3** に Browser Fingerprint の時間ごとの変化を計算した結果をまとめる．また，以下に計算方法をまとめる．

(1) 最初のアクセスと次のアクセスまでの期間が，0 日以上 7 日以下の場合（青色で表記）
(2) 最初のアクセスと次のアクセスまでの期間が，8 日以上 14 日以下の場合（オレンジ色で表記）
(3) 最初のアクセスと次のアクセスまでの期間が，15 日以上 21 日以下の場合（灰色で表記）

この結果から，ハードウェア情報は時間が経過しても変化が少なく，ソフトウェア情報やネットワーク情報は時間とともに大きく変化する場合があることが分かった．実験で取得した特徴の多くは 1 週間以内であれば変化が少ないため，攻撃者は偵察フェーズと侵入フェーズの間を短くすることで，時間による変化を受けにくい Fingerprint を作成することができる．

表 2 標的端末上でのみ動作する疑似マルウェア検体の作成に用いる情報

Table 2 Features used to implement test samples that can identify target system.

	Feature	Normalized Shannon Entropy	Time stability
Hardware	Screen size	0.296	80.8%
	Physical cores	0.030	91.9%
	CPU architecture	0.072	99.5%
Software	OS version	0.385	94.1%
	HTTP Accept Language	0.271	85.5%
	Time zone	0.011	86.3%
	Browser version	0.479	79.9%
	Plug-in	0.598	74.0%
Network	Internal IP address	0.656	60.7%

表 3 実験に用いた標的端末の Fingerprint

Table 3 Fingerprint of target system used in the experiment.

	Feature	Observation	Anonymity set size
Hardware	Screen size	2560x1440	42/10010
	Physical cores	4	1330/6585
	CPU architecture	amd64	3699/10010
Software	OS version	Windows 7	1140/10010
	HTTP Accept Language	ja-JP	1729/10010
	Time zone	9	9720/10010
	Browser version	Chrome 57.0	68/10010
		Firefox 52.0	15/10010
		Internet Explorer 11.0	496/10010
	Plug-in	Shockwave Flash 25.0	151/10010
		Silverlight Plug-In 5.1	1315/10010
Network	Internal IP address	*.*.*.204	1/10010
Combined	Combination of Hardware	3 feature	13/10010
	Combination of Software	5 feature	4/10010
	Combination of all	9 feature	1/10010

標的端末上でのみ動作する検体：エントロピーが高く，かつ，時間による変化が少ない 9 種類の特徴を手動で選定した．**表 2** にその結果をまとめる．なお，CPU Architecture や OS Version，Browser Version は User Agent から抽出した．

続いて，選定した特徴を用いて標的端末上でのみ動作する検体を作成した．作成した検体は C#によって実装された実行形式のファイルであり，実行されると Windows API や Windows 関数を用いて 9 種類，合計 12 個の特徴を収集する．そして，収集した情報が 4.2 節で取得した Fingerprint と一致した場合にのみ，実行環境が標的であると判断する．

作成した検体を標的端末で実行したところ，Browser（Chrome と Firefox）と Shockwave Flash のバージョン情報が一致しなかった．これは，標的端末の情報を取得した 2017 年 4 月 12 日から 3 カ月以上経過した 2017 年 7 月 11 日に作成した検体を実行したためである．実際の攻撃では，偵察フェーズと侵入フェーズの間は短く，すべての特徴が一致することが予想されるため，作成した検体はすべての特徴が一致した場合にのみ標的端末であると判断するようにした．**表 3** に標的端末の Fingerprint をまとめる．

本研究で想定する標的端末上でのみ動作するマルウェアは，サンドボックスや標的でないユーザの端末上では

不正活動を行わない．そこで，実際に標的でないユーザの端末を標的であると判断する可能性を調査するため，論文 [17] で使われている Anonymity Set Size を計算した．これにより，データセットの中から評価対象の特徴がどの程度存在するのかを確認でき，評価対象の特徴を持つデータ数/データセットのデータ数で計算される．分母のデータセットには，上記の実験で収集した 10,010 の Browser Fingerprinting を用いた．表 3 に計算結果をまとめる．ただし，Software 情報の組合せには Browser Version として “Firefox 52.0” を，Plug-in として “Shockwave Flash 25.0” を用いている．この結果から，9 種類の特徴を組み合わせることで実験に用いたデータセットの中から標的端末を一意に特定することができるといえる．このため，作成した検体が他の環境を標的端末と判断する可能性は低いと予想される．なお，標的端末には組織の固定 IP アドレスが割り当てられていたため，実際の値を匿名化して表記している．

4.4 サンドボックスアプライアンスの有効性評価

作成した検体を用いてサンドボックスアプライアンスの有効性を評価した．サンドボックスアプライアンスとは，未知のファイルをサンドボックス上で解析することで保護対象組織内のユーザをマルウェア感染から守ることを目的とした装置である．実験に用いた標的端末は日々の業務に使われており，3 種類のサンドボックスアプライアンスの監視下にある．ただし，これらのアプライアンスはネットワーク接続を許可していないため，作成した検体をアプライアンスに投稿し，解析レポートを分析することでサンドボックスアプライアンスが回避されうるか調査した．実験の結果，作成した検体は 10 個のサンドボックス上で実行された（Windows 10，Windows 7，Windows XP，32/64 bit）．サンドボックスの中には OS Version，Browser Version，Plug-in，HTTP Accept Language，Physical Cores，CPU Architecture の一部が一致するものが存在した．しかし，4 つ以上の特徴が一致するサンドボックスは存在しなかった．また，2 個のサンドボックスではすべての特徴が不一致であった．このため，攻撃者は特徴を組み合わせることで実験に用いたサンドボックス群を回避することができる．

最後に，サンドボックスアプライアンスのセキュリティアラートを調べた．作成した検体を実行した 10 個のサンドボックスのうち，9 個のサンドボックスからはアラートが観測されなかった．一方，1 個のサンドボックス（Windows XP）からハードウェアに関するアラートが観測された．作成した検体は Windows XP より新しい OS で実行可能である．しかし，実験に用いた標的端末は Windows 7 であることから，Windows 7 以降で有効なライブラリを用いて検体を再実装してサンドボックスアプライアンスに投稿した．この結果，いずれのサンドボックスからもセキュリティアラートは観測されなかった．そのため，攻撃者は実験に用いたサンドボックスアプライアンスをステルスに回避することができる．

5. Implant ベースの攻撃に対するセキュリティアプライアンスの有効性評価

我々は先行研究 [1] において，攻撃者は標的端末に Implant した情報を用いて標的端末上でのみ動作するマルウェアを作成し，実組織で運用されているサンドボックスアプライアンスによる検知の回避が可能であることを確認した．本章では，標的端末に埋め込む情報を整理し，本攻撃シナリオに対するセキュリティアプライアンスの有効性を検討する．以降では，5.1 節でネットワークアプライアンスの有効性を検討し，5.2 節でサンドボックスアプライアンスの有効性を検討する．

5.1 ネットワークアプライアンスの有効性評価

標的端末に埋め込むことができる情報は多岐にわたるが，本研究では 3 つに分類する．

(1) **Software**：多くの組織で Web ブラウジングや電子メールでのやりとりは日常業務において必要不可欠となっている．そこで，標的端末で利用されている Web ブラウザやメールクライアントなどのソフトウェアに情報を埋め込む偵察行為が考えられる．たとえば，Web ブラウザの中には閲覧履歴や Cookie などの情報を保存するものが存在する．これらの情報の多くは端末内のファイルに保存されるため，攻撃者は自身の管理下にある URL を標的に送信して，標的端末の Web ブラウザに情報を埋め込むことができる．また，メールクライアントの中には，メールヘッダ内に記述されている URL やイメージファイルをインターネットからダウンロードするものが存在する．読み込んだ画像は端末内のキャッシュに保存されるため，攻撃者は自身の管理下にある URL をメールヘッダ内に記述して標的に送信して，標的端末のメールクライアントに情報を埋め込むことができる．

(2) **System**：Windows 環境ではデフォルト設定で，システム上で起きたエラーはイベントログに記録される．また，Windows OS の様々な動作がログとして保存される場合が多い．そこで，標的端末のシステムに情報を埋め込む偵察行為が考えられる．たとえば，Domain Name System（DNS）を利用してドメインを名前解決する際，どの DNS サーバからも応答がなく要求がタイムアウトした場合にイベントログに情報が記録される．このため，攻撃者は自身の管理下にある URL を標的に送信して，標的端末のイベントログに情報を埋め込むことができる．

(3) **Network**：一般的に，Web サイトを閲覧する際に DNS サーバを利用してドメインを名前解決する．また，名

前解決したドメインの情報はDNSキャッシュとして一時的に保存される場合が多い．そこで，標的端末のネットワークに情報を埋め込む偵察行為が考えられる．たとえば，Windows環境ではDNS Stub Resolverがデフォルトインストールされており，DNSサーバにドメインを問い合わせて取得した情報を端末内のキャッシュに保存する．このため，攻撃者は自身の管理下にあるURLを標的に送信して，標的端末のDNSキャッシュに情報を埋め込むことができる．

このように，攻撃者は自身の管理下にあるURLを標的に送信して，URLをクリックさせることで標的端末に情報を埋め込むことができる．攻撃者が用意するWebサイトは，正規サイトと同じ構成のWebサイトを利用することができるため，標的端末に埋め込む偵察行為は日常業務において発生するWebアクセスと差異がなく，ネットワークアプライアンスでの検知は困難であると予想される．

5.2 サンドボックスアプライアンスの有効性評価

我々は先行研究[1]において，Webブラウザ（Browser History，Browser Cache）とDNS Stub Resolverのキャッシュに情報を埋め込む攻撃シナリオを想定し，実際の攻撃キャンペーンに用いられたマルウェアを暗号化し，標的端末に埋め込んだ情報を復号鍵として自身を復号する擬似マルウェア検体を作成した．そして，実組織で運用されている3種類のサンドボックスアプライアンスにおいて，作成した擬似マルウェア検体が復号されずに解析が終了することを確認した（Windows 10，Windows 7，32/64 Bitからなる5個のサンドボックス）．また，セキュリティアラートは観測されなかったため，攻撃者は実験に用いたサンドボックスアプライアンスをステルスに回避できることを確認した．

このように，攻撃者は標的端末にあらかじめ埋め込んだ情報を用いて，標的端末上でのみ動作するマルウェアを作成することができる．標的端末に埋め込んだ情報はサンドボックスには見られない特徴であるため，サンドボックスアプライアンスでマルウェア本来の挙動を把握することは困難であると予想される．しかし，作成したマルウェアは実行環境の情報を取得して，あらかじめ設定した条件と一致した場合にのみ実行環境が標的端末であると判断する．このため，サンドボックスアプライアンスでマルウェアの情報を取得する挙動をとらえることで，標的端末上でのみ動作するマルウェアを検知できる可能性がある．実際に，4.4節の評価実験においてもサンドボックスアプライアンスからセキュリティアラートが観測されているが，さらなる性能向上が必要である．

6. 考察

6.1 攻撃対策

本攻撃シナリオへの対策として，標的端末で行う対策とセキュリティアプライアンスの性能向上が考えられる．

Browser Fingerprinting対策：本攻撃シナリオへの対策の1つとして，Browser Fingerprintの取得を難しくする方法が考えられる．たとえば，Webブラウザの特徴を難読化するPlug-inが存在する[18], [19], [20]．特に，エントロピーが高くなる特徴の取得を難しくすることで攻撃者のコストを高められる．また，JavaScript，CSS，Flashなどを無効化することでBrowser Fingerprintの取得を防ぐことができる．ただし，これらを無効化することでユーザの利便性が損なわれる可能性がある．

Implant対策：本攻撃シナリオへの対策の1つとして，Implantした情報の有効期間を短くする方法が考えられる．たとえば，Webブラウザの閲覧履歴やキャッシュを定期的に除去することで，攻撃者のコストを高められる．また，キャッシュの無効化を行うことで情報の埋め込みを難しくする方法が考えられる．ただし，ユーザの利便性を損なう可能性があるため，設定を行う際は注意が必要である．

サンドボックスアプライアンスの性能向上：動的解析した際に標的端末上でのみ動作するマルウェア本来の挙動を把握することは難しいが，実行環境の情報を取得する挙動をとらえることでこれらのマルウェアを検知できる可能性がある．また，これまでにサンドボックスをユーザ環境に近づける研究[21]が行われてきたが，サンドボックスを標的端末に近づけることで攻撃を防ぐことができる可能がある[22]．一方，サンドボックスがユーザに送られたURLをクリックするように設定することで，攻撃者のコストを高くする方法が考えられる．しかし，攻撃者は標的端末がサンドボックスアプライアンスに守られていることを把握することができる．また，サンドボックスの情報が漏えいすることになるため，インターネット接続されたサンドボックスがユーザに送られたURLをクリックするように設定することは望ましくない．

このように様々な対策が考えられるが，攻撃者は複数の攻撃シナリオを組み合わせる可能性があるため，防御側も単一の対策ではなく，複数の対策を組み合わせた多層防壁を実現することが望ましい．

6.2 攻撃シナリオの限界

本攻撃シナリオでは，偵察する端末と侵入する端末は同じ端末である必要がある．しかし，偵察フェーズと侵入フェーズはメール経由で行われるため，それぞれのフェーズに用いられる端末は日常業務に利用される同一端末であると予想される．偵察フェーズでは，攻撃者は送信したURLをユーザにクリックさせる必要がある．同様に，侵

入フェーズでは送信したファイルを実行させる必要がある．このため，ユーザ操作を促すソーシャルエンジニアリング攻撃などを用いる必要がある．一方，偵察フェーズにHTML メールを用いることで URL をクリックすることなく標的端末内に情報を埋め込める可能性がある．本攻撃シナリオについては今後の課題とする．

6.3 研究倫理的対応

本研究は，標的端末上でのみ動作するマルウェアによるサンドボックス解析回避を困難にし，サイバー攻撃の標的となりうる組織のセキュリティ向上に資することを目的とする．そのため，本研究成果をサンドボックスオペレータやセキュリティベンダに正確かつ詳細に伝えるとともに，攻撃者に悪用されるデメリットを減らすために，以下のような方策をとった．まず，本研究成果による直接的な影響があると予想される実験に用いたサンドボックスアプライアンスのセキュリティベンダ計 3 社に対して，標的端末上でのみ動作するマルウェアが解析を回避する恐れがある点の指摘や実験に用いた検体の提供，推奨される対策方法などの情報提供を行った．このうち，1 社からは提供情報に基づき，システムの改善を行った旨の連絡を受けている．次に，サンドボックスアプライアンスを研究開発しているセキュリティベンダ計 11 社に対して情報提供を行った．このうち，1 社とは開発を行っている技術者と今後の対策について直接意見交換を行った．最後に，実験に用いたセキュリティアプライアンスの名称や機器の特定につながる情報を記述することは避けた．このように，本研究はセキュリティアプライアンスの性能向上に貢献していると考えられる．

7. まとめと今後の課題

実行環境から収集した情報があらかじめ設定した条件と一致した場合にのみ，実行環境が標的端末であると判断して不正活動を行うマルウェアを用いて攻撃者が標的組織へ侵入する攻撃シナリオを想定し，セキュリティアプライアンスの有効性を評価した．評価実験の結果，実組織で運用されているネットワークアプライアンスに検知されることなく標的端末の Browser Fingerprint の取得が可能であることを確認した．また，実組織で運用されているサンドボックスプライアンスに対して解析の回避が可能であることを確認した．我々は，先行研究 [1] において，標的端末に Implant した情報を用いてサンドボックスアプライアンスによる検知の回避が可能であることを確認している．そこで，本攻撃シナリオへの対策について考察するとともに，研究成果をセキュリティベンダに提供して標的端末上でのみ動作するマルウェアへの注意喚起を行った．

今後の課題は，情報の収集方法や埋め込み方法を改善するとともに，さらに多くの環境で実験を行うことである．また，標的端末上でのみ動作するマルウェアを検知する方法について検討することである．

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．加えて，本研究の一部は，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」により得られた．

参考文献

[1] Tanabe, R., Ueno, W., Ishii, K., Yoshioka, K., Matsumoto, T., Kasama, T., Inoue, D. and Rossow, C.: Evasive Malware via Identifier Implanting, *Proc. 15th Conference on Detection of Intrusions and Malware & Vulnerability Assessment* (*DIMVA 2018*) (2018).

[2] Barbosa, G.N. and Branco, R.R.: Prevalent characteristics in modern malware (2014), available from ⟨https://www.blackhat.com/docs/us-14/materials/us-14-Branco-Prevalent-Characteristics-In-Modern-Malware.pdf⟩.

[3] Lastline blog: Three interesting changes in malware activity over the past year (2016), available from ⟨http://labs.lastline.com/three-interesting-changes-in-malware-activity-over-the-past-year⟩.

[4] The mystery of the encrypted gauss payload, available from ⟨https://securelist.com/the-mysteryof-the-encrypted-gauss-payload-5/33561/⟩.

[5] Ishimaru, S.: Why corrupted (?) samples in recent APT? case of Japan and Taiwan, available from ⟨https://hitcon.org/2016/pacific/0composition/pdf/1201/1201%20R1%201500%20why%20corrupted%20samples%20in%20recent%20apt.pdf⟩.

[6] Maier, D., Müller, T. and Protsenko, M.: Divide-and-conquer: why android malware cannot be stopped, *Proc. 9th International Conference on Availability, Reliability and Security* (*ARES 2014*) (2014).

[7] Najmeh, M., Mahathi, P.A., Nick, N. and Michalis, P.: Spotless sandboxes: evading malware analysis systems using wear-and-tear artifacts, *Proc. 38th IEEE Symposium on Security and Privacy* (*S&P 2017*) (2017).

[8] Yokoyama, A., Ishii, K., Tanabe, R., Papa, Y., Yoshioka, K., Matsumoto, T., Kasama, T., Inoue, D., Brengel, M., Backes, M. and Rossow, C.: Sandprint: Fingerprinting Malware Sandboxes to Provide Intelligence for Sandbox Evasion, *Proc. 19th International Symposium on Research in Attacks, Intrusions and Defenses* (*RAID 2016*) (2016).

[9] Vasudevan, A. and Yerraballi, R.: Cobra: Fine-grained Malware Analysis using Stealth Localized-executions, *Proc. 27th IEEE Symposium on Security and Privacy* (*S&P 2006*) (2006).

[10] Dinaburg, A., Royal, P., Sharif, M. and Lee, W.: Ether, Malware Analysis via Hardware Virtualization Extensions, *Proc. 15th ACM Conference on Computer and Communications Security* (*CCS 2008*) (2008).

[11] Kirat, D., Vigna, G. and Kruegel, C.: BareBox: Efficient malware analysis on bare-metal, *Proc. 27th Annual Computer Security Applications Conference* (*ACSAC 2011*) (2011).

[12] Kirat, D., Vigna, G. and Kruegel, C.: BareCloud: bare-metal analysis-based evasive malware detection, *Proc. 23rd USENIX Conference on Security Symposium* (*USENIX 2014*) (2014).

[13] Lindorfer, M., Kolbitsch, C. and Milani, P.: Detecting Environment-Sensitive Malware, *Proc. 14th International Conference on Recent Advances in Intrusion Detection* (*RAID 2011*) (2011).
[14] Moser, A., Kruegel, C. and Kirda, E.: Exploring multiple execution paths for malware analysis, *Proc. 28th IEEE Symposium on Security and Privacy* (*S&P 2007*) (2007).
[15] IPA：「高度標的型攻撃」対策に向けたシステム設計ガイド (2016)，入手先 ⟨http://www.ipa.go.jp/files/000046236.pdf⟩.
[16] Englehardt, S. and Narayanan, A.: Online tracking: A 1-million-site measurement and analysis, *Proc. 23rd ACM Conference on Computer and Communications Security* (*CCS 2016*) (2016).
[17] Eckersley, P.: How unique is your web browser?, *Proc. Privacy Enhancing Technologies Symposium* (2010).
[18] Firegloves; cross-browser fingerprinting test 2.0, available from ⟨https://fingerprint.pet-portal.eu/?menu=6⟩.
[19] Github - ghostwords/chameleon: Browser fingerprinting protection for everybody, available from ⟨https://github.com/ghostwords/chameleon⟩.
[20] Noscript security suite: Add-ons for firefox, available from ⟨https://addons.mozilla.org/ja/firefox/addon/noscript/⟩.
[21] Nikiforakis, N., Joosen, W. and Livshits, B.: Privaricator: Deceiving fingerprinters with little white lies, *Proc. 24th International Conference on World Wide Web* (*WWW 2015*) (2015).
[22] 田辺瑠偉，石井 攻，横山日明，吉岡克成，松本 勉：標的組織の内部情報を有する攻撃者を前提としたサンドボックス型セキュリティアプライアンスの評価，情報処理学会論文誌，Vol.59, No.2 (2018).
[23] Mutti, S., Fratantonio, Y., Bianchi, A., Invernizzi, L., Corbetta, J., Kirat, D., Kruegel, G. and Vigna, G.: BareDroid: Large-Scale Analysis of Android Apps on Real Devices, *Proc. 31st Annual Computer Security Applications Conference* (*ACSAC 2015*) (2015).
[24] Gajrani, J., Sarswat, J., Tripathi, M. and Laxmi, V.: A robust dynamic analysis system preventing SandBox detection by Android malware, *Proc. 8th International Conference on Security of Information and Networks* (*SIN 2015*) (2015).
[25] Spensky, C., Hu, H. and Leach, K.: LO-PHI: Low-Observable Physical Host Instrumentation for Malware Analysis, *Proc. Network and Distributed System Security Symposium* (*NDSS 2016*) (2016).
[26] Kirat, D. and Vigna, G.: MalGene: Automatic Extraction of Malware Analysis Evasion Signature, *Proc. 22nd ACM SIGSAC Conference on Computer and Communications Security* (*CCS 2015*) (2015).
[27] FireEye：検出が困難で危険なブートキットによりカード決済情報を狙う脅威グループを確認，入手先 ⟨https://www.fireeye.jp/company/press-releases/2015/thriving-beyond-the-operating-system-financial-threat-group-targets-volume-boot-record.html⟩.
[28] McAfee Labs：2019 年脅威予測レポート，入手先 ⟨https://blogs.mcafee.jp/mcafee-labs-2019-threats-predictions⟩.
[29] Security Intelligence: DeepLocker: How AI Can Power a Stealthy New Breed of Malware, available from ⟨https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/⟩.

田辺 瑠偉 （正会員）

2017 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（情報学）．同年 4 月より横浜国立大学大学院環境情報研究院で産学官連携研究員として勤務．2018 年 4 月より横浜国立大学先端科学高等研究院特任教員（助教）．情報セキュリティ，特にネットワークセキュリティの研究に従事．2017 年情報処理学会山下記念研究賞受賞．

上野 航

2019 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前期修了．修士（工学）．同年 4 月 NTT コミュニケーションズ株式会社入社．在学中，情報セキュリティに関する研究に従事．

星澤 裕二 （正会員）

2015 年 4 月より PwC コンサルティング合同会社（旧プライスウォーターハウスクーパース株式会社）パートナー．同年 10 月より PwC サイバーサービス合同会社最高執行責任者．マルウェア解析や脆弱性収集・分析等のサイバーセキュリティの研究開発に従事．2007 年経済産業省商務情報政局長表彰（情報セキュリティ促進部門）．

齋藤 孝道 （正会員）

1997 年 3 月東京理科大学大学院理工学研究科情報科学専攻博士課程修了．博士（工学）．同年 4 月同大学助手．2005 年 4 月より明治大学理工学部情報科学科助教授．2016 年 4 月より同大学教授．プライバシーやネットワークセキュリティの研究に従事．

笠間 貴弘 （正会員）

2014 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）．2011 年 4 月より情報通信研究機構に研究員として入所．マルウェア解析やネットワーク攻撃観測・分析等のサイバーセキュリティの研究開発に従事．2011 年情報処理学会山下記念研究賞受賞．

井上 大介 （正会員）

2003 年横浜国立大学大学院工学研究科博士課程後期修了．博士（工学）．2003 年通信総合研究所（現，情報通信研究機構）に入所．2006 年よりインシデント分析センター NICTER の研究開発に従事．現在，情報通信研究機構サイバーセキュリティ研究所サイバーセキュリティ研究室室長．2002 年暗号と情報セキュリティシンポジウム論文賞，2009 年科学技術分野の文部科学大臣表彰（科学技術賞），2013 年グッドデザイン賞，2014 年 Asia-Pacific Information Security Leadership Achievements 等を受賞．

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 （正会員）

1986 年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．同年より横浜国立大学勤務．現在，同大学・環境情報研究院教授および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主任研究者および産業技術総合研究所サイバーフィジカルセキュリティ研究センター長．CRYPTREC 暗号技術検討会座長，日本学術会議連携会員を兼任．情報・物理セキュリティの研究教育に 1981 年より従事．この間，日本銀行金融研究所客員研究員，独カールスルーエ大学客員教授，日本学術振興会学術システム研究センター専門研究員，国際暗号学会 IACR 理事等を歴任．暗号学国際会議 ASIACRYPT，電子情報通信学会暗号と情報セキュリティシンポジウム SCIS，バイオメトリクス研究専門委員会，ハードウェアセキュリティ研究専門委員会等の創設に貢献．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・科学技術賞等受賞．