情報処理学会論文誌 Vol.59 No.2 553–563 (Feb. 2018)

推薦論文

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

田辺 瑠偉[1,a)] 石井 攻[1] 横山 日明[1] 吉岡 克成[2,3] 松本 勉[2,3]

受付日 2017年5月1日, 採録日 2017年11月7日

概要：継続的かつ執拗に特定の組織などへの侵入を試みるサイバー攻撃に対して組織を完全に防御することが困難な状況になっている．これらの攻撃者は，偵察行為や標的組織への侵入の過去の成功経験から標的組織の情報システムやセキュリティ対策に関する内部情報を有している場合がある．さらなる侵入や継続的な情報漏えいを防ぐためには，このような強い前提の攻撃者に対しても対応が必要である．そこで本研究では，標的組織の内部情報を有する攻撃者に対するセキュリティ対策技術の有効性を評価する．特にシグネチャによる検知が困難な標的型攻撃に対して有効とされる，サンドボックス型のセキュリティアプライアンスを対象にし，内部情報を有する攻撃者によってセキュリティアプライアンスによる検知の回避がどのように行われうるかを考察する．また，実組織において運用されているあるセキュリティアプライアンスに対して内部情報を有する攻撃者による侵入が可能であるかを検証する．検証の結果，評価対象のアプライアンスに導入されたサンドボックスとユーザマシンとの間には環境に大きな差異が存在し，攻撃者はこれらの特徴を用いて検知を回避する可能性があることを確認した．

キーワード：セキュリティアプライアンス，サンドボックス解析，解析検知

Evaluation of Sandbox Appliance against Persistent Attackers Who Has Prior Knowledge of Target Organization

Rui Tanabe[1,a)] Kou Ishii[1] Akira Yokoyama[1] Katsunari Yoshioka[2,3] Tsutomu Matsumoto[2,3]

Received: May 1, 2017, Accepted: November 7, 2017

Abstract: It is becoming more difficult to defend against persistent cyber-attacks, which targets specific organizations. Some attackers have prior knowledge of target organization from the experience of successful intrusion in the past or by reconnaissance. To prevent further intrusion and information leakage, countermeasures against these persistent attackers who have the information of target systems including their defense mechanism are required. Therefore, we evaluate the capability of security appliances against attackers whom have prior knowledge of target organization. In this paper, we focus on evaluating sandbox appliances, which are expected to be effective against advanced attacks that evade signature-based detection. We consider how attackers evade sandbox appliances by abusing information of target system and sandboxes. Moreover, we evaluate an actual security appliance deployed in an existing organization to see if it is effective against an attacker who has the prior knowledge of the organization. From the experiment, we found that there is a critical gap between the environment of user machines and that of sandboxes inside the evaluated appliance, showing that the defense can be easily bypassed.

Keywords: security appliance, sandbox analysis, sandbox evasion

1. はじめに

近年，特定の企業や組織を狙ったサイバー攻撃による被害が深刻化している．たとえば，2015 年に発生した日本

[1] 横浜国立大学
Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[2] 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
[3] 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
[a)] tanabe-rui-nv@ynu.jp

本論文の内容は 2016 年 10 月のコンピュータセキュリティシンポジウム 2016/マルウェア対策研究人材育成ワークショップ 2016 にて報告され，同プログラム委員長により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

年金機構を狙った攻撃では，125 万件の年金情報が漏えいした．当該攻撃では，不正サイトのリンクが記されたメールや不正ファイルが添付されたメールが数週間にわたって送信された．侵入に成功した攻撃者はネットワーク内で感染を広げ，年金受給者に関する情報を外部に漏えいさせた [1]．このように，セキュリティ対策技術の導入が進んでいる一方で，継続的かつ執拗に侵入を試みる攻撃に対して組織を完全に防御することが困難な状況になっている．

継続的に標的組織に侵入し情報を収集する攻撃者は，様々な偵察行為や標的組織への侵入行為により，標的組織の情報システムやセキュリティ対策に関する内部情報を有していることが想定される．たとえば，標的マシンのセキュリティ識別子（SID）を基に復号鍵を生成し，自身を復号して動作するマルウェアが報告されている [35]．このため，標的型攻撃の対策技術は，このような強い前提の攻撃者に対しても有効に働くことが望ましい．本研究では，標的型攻撃の対策技術として注目され，広く導入が進んでいる，サンドボックスによるマルウェア検知を行うセキュリティアプライアンスの有効性を評価する．まず，サンドボックスアプライアンスが導入されている組織に対する攻撃を分類し，どのような情報がサンドボックスアプライアンス回避に有効であるかを検討する．そして，標的組織の内部情報を利用した攻撃の具体例として，サンドボックスと実ユーザ環境の差異に着目してマルウェアの挙動を変えることでアプライアンスによる検知回避を試みる攻撃者を想定し，実際に組織に導入されたサンドボックスアプライアンスが回避されうるかを検証する．

検証の結果，OS の言語設定や AV ソフトの有無，IP アドレスなど，サンドボックスとユーザマシンには大きな差異が存在し，これに着目したアプライアンスの回避が容易であることが確認された．すなわち，実際に製品として導入されたサンドボックスアプライアンスにおいても導入先の組織内の環境と整合性のあるようなカスタマイズは行われていない例が確認された．標的組織の内部情報を有する攻撃者に対してサンドボックスアプライアンスが有効に働くためには，組織内の環境と整合したサンドボックスを用意する必要があるといえる．

以降では，2 章でサンドボックスアプライアンスについて説明し，3 章でサンドボックス解析を回避するマルウェアについて説明する．そして，4 章で標的組織の内部情報を有する攻撃者がどのような情報を用いてサンドボックスアプライアンスを回避するか検討し，5 章で実際に組織に導入されたサンドボックスアプライアンスに対して内部情報を有する攻撃者による侵入が可能であるか検証する．最後に，6 章で考察，7 章で関連研究，8 章でまとめと今後の課題を説明する．

2. サンドボックスアプライアンス

セキュリティアプライアンスとは，ネットワーク内の機器を不正侵入やマルウェア感染から守ることを目的とした装置のことであり，ファイアウォールや IDS/IPS，AV ソフト，アンチスパム，コンテンツフィルタリングなど様々なセキュリティ機能を有する．本研究では，サンドボックスによるマルウェア検知を行う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．

サンドボックスアプライアンスは，ルータやスイッチなどといったネットワーク機器に接続されている場合や，他のセキュリティアプライアンスに接続されている場合が多い．このため，保護対象組織内のネットワークトラヒックを監視することで，メールに添付されたファイルやユーザがインターネット上からダウンロードしたファイルをサンドボックス上で解析する役割を持つ．なお，サンドボックスアプライアンスの中にはユーザからファイルの投稿を受け付け，解析レポートを作成する機能を持つものも存在する．サンドボックスアプライアンスには，クラウド上に存在するサンドボックスを用いてマルウェア動的解析を行うクラウド型と，導入先ネットワーク内でサンドボックスを作成してマルウェア動的解析を行うオンプレミス型の 2 種類が存在する．一般に，クラウド型はオンプレミス型に比べて安価であり，セキュリティベンダがサンドボックスの管理を行うため，シグネチャの更新やメンテナンスが容易である．一方，オンプレミス型の場合，検査対象ファイルを外部に送る必要がないため，セキュリティポリシの厳しい組織でも利用することができる．

多くのセキュリティベンダがサンドボックスアプライアンスの研究開発を行っている．**表 1** にサンドボックスアプライアンスをまとめる．サンドボックスを構成する技術はアプライアンスごとに様々であり，VMware や VirtualBox などの仮想化技術を用いて実現される場合や，Bochs などのエミュレータを用いて実現される場合がある．また，サンドボックスにインストールされている OS やアプリケーションも様々である．このため，サンドボックスアプライアンスごとに exe ファイルや doc ファイル，PDF ファイルなど解析可能なファイルの種類は様々である．

3. サンドボックス解析を回避するマルウェア

政府機関や企業などでサンドボックスアプライアンスの導入が進んでいる一方で，サンドボックスによる解析を回避するマルウェアが報告されている [22], [23]．これらのマルウェアは，サンドボックス上で実行された場合には悪性挙動を示さず，ユーザマシン上で実行された場合にのみ悪性な活動を行うことで，サンドボックスアプライアンスを回避する．本研究ではサンドボックスによる検知を回避す

表 1 サンドボックスアプライアンス一覧
Table 1 List of Sandbox appliance.

製造社名	アプライアンス名 / サービス名	種類
Bluecoat	Malware Analysis System[2]	オンプレミス型
Check Point	Threat Emulation[3]	オンプレミス型 / クラウド型
Cisco	Advanced Malware Protection[4]	クラウド型
Dell	SonicWALL Capture[5]	クラウド型
FFRI	FFR Yarai Analyzer[6]	オンプレミス型
FireEye	Malware Analysis[7]	オンプレミス型
Fortinet	FortiCloud[8]	クラウド型
Fortinet	FortiSandbox[9]	オンプレミス型
Hitachi	MAAS[10]	オンプレミス型 / クラウド型
IIJ	SecureMX[11]	クラウド型
Lastline	Lastline Cloud[12]	クラウド型
Lastline	Lastline on-Premise[12]	オンプレミス型
McAfee	Advanced Threat Defence[13]	オンプレミス型
Paloalto	WildFire[14]	クラウド型
Proofpoint	Targeted Attack Protection[15]	クラウド型
Secure Brain	Zero-Hour Response[16]	オンプレミス型
Sophos	Sandstorm[17]	クラウド型
Symantec	Advanced Threat Protection[18]	クラウド型
TrendMicro	Cloud App Security[19]	クラウド型
TrendMicro	Deep Discovery Analyzer[19]	オンプレミス型
WatchGuard	APT Blocker[20]	クラウド型
Websense	Sandbox Modules[21]	オンプレミス型

る技術の中でも，サンドボックスが有する特徴をあらかじめ把握し，この特徴の有無を調べることでサンドボックスの検知を行い，サンドボックスとして判定された場合には悪性な活動を行わないことでアプライアンスによる検知を回避するサンドボックス検知型と，あらかじめ組み込んだ起動条件が実行環境内で発生するまで悪性な活動を行わず待機するトリガ型の 2 種類に着目する．図 1 にそれぞれの回避技術を用いたサンドボックス回避方法をまとめる．以降では，3.1 節でサンドボックス検知型の回避技術について説明し，3.2 節でトリガ型のサンドボックス回避技術について説明する．

3.1 サンドボックス検知型の回避技術

サンドボックスの多くは仮想化技術やエミュレータを用いて実現される場合が多い．また，サンドボックスの多くは OS インストール直後の状態に近い．このため，ユーザが利用しているマシンとは差異が存在する．そこで，サンドボックスを構成するハードウェアやシステム，アプリケーション，ネットワークなどの情報を用いてサンドボックスを回避する技術をサンドボックス検知型の回避技術と呼ぶこととする．当該技術を用いてサンドボックスを回避する場合，まず初めに実行環境をサンドボックスと判断するための条件を設定する．たとえば，プロセッサの数やメモリの大きさなどのハードウェアに関する情報，ホスト名やプロダクト ID などの OS に関する情報，Web 閲覧ソフトや文書作成ソフトなどのアプリケーションに関する情報，IP アドレスや MAC アドレスなどのネットワークに関する情報などが想定される．そして，実行環境の情報を取得し，取得した情報が設定した条件と一致した場合にサンドボックスと判断する．一方，取得した情報が条件と一致しない場合に悪性挙動を行う．実際に，特定の OS やアプリケーション上でのみ動作するマルウェアが報告されている [24]．また，VMware に関連するサービスの有無や VMware に固有のファイルの有無，VMware が仮想マシンとの通信に利用するバックドアポートの有無を条件にサンドボックスを回避するマルウェアが報告されている [24], [25]．加えて，デバッガや解析ツールの有無，インターネット接続の有無を条件にサンドボックスを回避するマルウェアが報告されている [25], [26]．

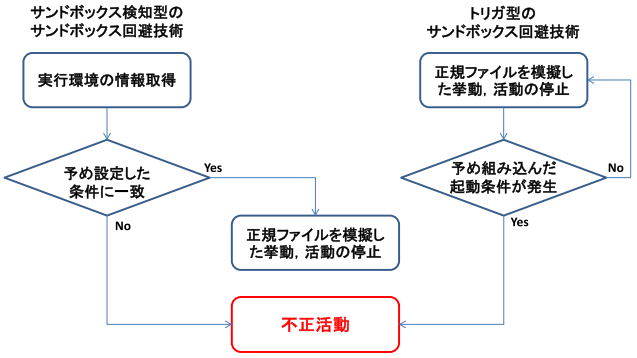

図 1 サンドボックス検知型・トリガ型のサンドボックス回避技術を用いたサンドボックス回避
Fig. 1 Sandbox evasion using Sandbox-detection based and Trigger based Sandbox evasion technique.

3.2 トリガ型のサンドボックス回避技術

サンドボックスの多くは，短時間で大量のマルウェアを解析する必要があるため，マルウェア検体実行後一定時間が経過すると解析を終了する．また，検体の転送や実行は自動で行われる．このため，ユーザが利用しているマシンとは差異が存在する．そこで，プログラム内に組み込んだ起動条件が発生するまで不正な活動を行わない技術をトリガ型のサンドボックス回避技術と呼ぶこととする．当該技術を用いてサンドボックスを回避する場合，まず初めに悪性挙動を開始する条件を設定する．たとえば，一定時間経過後に不正活動を開始するといった条件や，特定の日付になったら不正活動を開始する，再起動後に不正活動を開始する，キーボード入力やマウス操作が観測されたときに不正活動を開始するといった条件が想定される．そして，実行環境内で起動条件が発生するまで不正活動を行わずに待機する．一方，条件が発生した場合に不正活動を行う．実際に，スリープ関数や実行環境の現在の時刻を取得する関数を用いてサンドボックス解析を回避するマルウェアが報告されている [24], [25], [26]．また，マスタブートレコー

ドに感染するなどしてシステム再起動時に不正活動を行うマルウェアが報告されている [22], [26]．加えて，マウスイベントやダイアログボックスのクリックを条件に，サンドボックス解析を回避するマルウェアが報告されている [24]．

4. 標的組織の内部情報を有する攻撃者によるサンドボックスアプライアンスの回避

標的組織を狙った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 [27]．標的型攻撃の多くは，標的組織内に存在する重要情報の漏えいや改ざんを目的としているが，より多くの情報を得るためには組織内のセキュリティ対策を回避し，継続的かつ秘密裏に不正活動を行う必要がある．そのため，標的組織のセキュリティ対策に関する情報も攻撃者にとって重要であり漏えいの対象と考えられる．以降では，4.1 節で標的組織からのセキュリティ対策情報の漏えいについて特にサンドボックスアプライアンスの回避に関係する情報やその特徴について説明する．

4.1 標的組織からのセキュリティ対策情報の漏えい

攻撃者は，事前に標的組織の情報システムやセキュリティ対策に関する情報を収集し，セキュリティ対策の迂回を試みる．標的組織に関する情報が多いほど，セキュリティ対策を迂回できる可能性が高くなる．収集対象の情報には，当該組織について一般に公開されているものから，当該組織内に侵入することで得られる情報，他の攻撃者や標的組織内部者からの情報など様々であるが，サンドボックスアプライアンスによる検知に有効な情報としては，標的組織内で運用されているサンドボックスアプライアンス製品の種類や具体的な環境などが考えられる．加えて，組織内のユーザマシンやそのマシンを利用しているユーザに関する情報，ネットワーク構成など，標的組織の情報システムに関する情報も重要である．攻撃者は，これらの情報を用いてサンドボックスアプライアンスを回避して，標的マシンでのみ不正活動を行うマルウェアを作成する．そして，次のステップとして作成したマルウェアを標的に送る．このとき，標的組織のセキュリティポリシやセキュリティ対策技術に関する情報が重要である．たとえば，標的組織におけるメールポリシに応じて，マルウェアをメールに直接添付して送信するのか，あるいは圧縮ファイルや Drive-By Download 攻撃を行う URL にして送信するのかといったマルウェアの送信方法を検討する必要がある．また，攻撃者は作成した標的メールやマルウェアが，スパムフィルタや AV ソフトなどのセキュリティ対策技術に検知されないようにする必要がある．攻撃者は，このように収集した情報の中から標的組織のセキュリティ対策を回避するのに有効な特徴を特定し，一連の攻撃を行う．サンドボックスアプライアンスを回避するマルウェアを作成するのに有効な特徴は様々考えられるが，本研究ではサンドボックスと実ユーザ環境の差異に着目してマルウェアの挙動を変えることでサンドボックスアプライアンスによる検知回避を試みる攻撃者を想定する．

5. 検証実験

検証実験では，標的組織の内部情報を利用した攻撃の具体例として，サンドボックスと実ユーザ環境の差異に着目してマルウェアの挙動を変えることでアプライアンスによる検知回避を試みる攻撃者を想定し，実際に組織に導入されたサンドボックスアプライアンスが回避されうるかを検証する．以降では，5.1 節でサンドボックス情報とユーザマシン情報の収集について説明し，5.2 節で実験に用いたサンドボックスとユーザマシンの環境の差異について説明する．そして，5.3 節でサンドボックスとユーザマシンの環境の差異に着目したサンドボックスアプライアンスの回避について説明する．

5.1 サンドボックス情報とユーザマシン情報の収集

標的組型攻撃を再現するため，ある組織で実際に運用されているクラウド型サンドボックスアプライアンスの監視下にある 20 台のユーザマシンに対して，実行環境の情報を取得するツールを送信し，標的組織に関する情報を収集した．**図 2** に実験環境をまとめる．ユーザマシンはそれぞれルータに接続しており，クラウド型サンドボックスアプライアンスはネットワーク内を流れるトラヒックのうち，HTTP(80/tcp) と SMTP(25/tcp) に関する通信をミラーリングすることでネットワークの監視を行っている．実行環境の情報を取得するツールは実行可能ファイルであり C 言

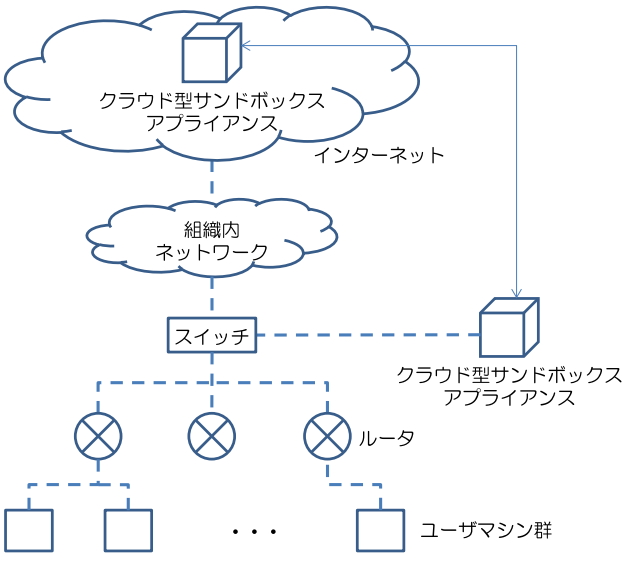

図 2 実験環境のネットワーク構成
Fig. 2 Network architecture of experiment environment.

語を用いて作成した．Windows API や Windows コマンドを用いて情報を取得し，HTTP 通信を介して外部に情報を漏えいさせる．ツールの送信は実際の攻撃を想定し，3 種類の方法を試した．まず初めに，実行形式のファイルの送受信が許可されていない組織を想定し，ツールを圧縮ファイルにしてユーザに送信した．ユーザにはあらかじめ実験内容を伝え，受け取ったファイルを解凍し，ツールの実行を行うように指示した．この結果，すべてのユーザマシンから実行環境の情報を収集することができた．一方，サンドボックスアプライアンスは圧縮ファイルを解凍することができなかった．次に，実行形式のファイルの送受信を許可している組織を想定し，あるユーザに対して当該ツールをメールに直接添付して送信した．ユーザにはあらかじめ実験内容を伝え，メールに添付されたファイルの実行を行うように指示した．この結果，再度ユーザマシンから実行環境の情報を収集することができた．また，サンドボックスアプライアンスが当該ツールを実行し，情報を収集することができた．このように，マルウェアをメール経由で直接送信する攻撃者は標的組織のメールポリシを把握する必要がある．最後に，当該ツールをダウンロード可能な Web サーバを構築し，数人のユーザに URL を送信した．ユーザにはあらかじめ実験内容を伝え，受け取った URL からツールをダウンロードし，実行を行うように指示した．この結果，再度ユーザマシンから実行環境の情報を収集することができた．また，再度サンドボックスアプライアンスが当該ツールを実行し，情報を収集することができた．なお，実験は 2016 年 2 月から 2016 年 5 月の間に行った．

5.2 サンドボックスとユーザマシンの環境の差異

クラウド型サンドボックスアプライアンスでは，実行環境の情報を収集するツールが複数回実行され，2 種類のサンドボックスの情報を収集することができた（以降では，サンドボックス 1 とサンドボックス 2 と呼ぶこととする）．また，すべてのユーザマシンから 1 回以上実行環境の情報を収集することができた．**表 2** に収集した情報の一部をまとめる．どちらのサンドボックスも検体が実行されるたびにプロダクト ID とホスト名をランダム化していた．また，サンドボックス 1 についてはシステム製造元をランダム化していた．このように，サンドボックスの特徴の一部はランダム化されているが，サンドボックスとユーザマシンには大きな差異が見られた．サンドボックスとユーザマシンに差異が見られる原因は様々考えられるが，サンドボックスの多くは限られたリソースで実現されることや，デフォルト設定のまま利用されること，スナップショットを用いて復元されるなど，サンドボックスに共通して見られるが，ユーザマシンには見られない特徴が存在する [29]．一方，同一組織内のユーザマシンはネットワークの設定やシステムの設定が類似していることや，同じアプリケーションソフトを利用していることなど，標的組織のユーザマシンに共通して見られるが，サンドボックスアプライアンスには見られない特徴が存在する．以下に，検証実験において差異が見られた特徴をまとめる．

ネットワーク情報：標的組織のユーザマシンは ARP リスト内のホスト数，ネットワークコネクション数が複数存在した．一方，サンドボックスは一般に感染拡大を防止するため同一ネットワーク内のホストとの通信を制限している．また，ユーザマシンと利用目的が異なるため，ネットワークコネクション数や ARP リスト内のホスト数は限られていた．標的組織のユーザマシンはグローバル IP アドレスの国情報が同じであった．また，ローカル IP アドレスも同一ネットワーク内の IP アドレスであった．一方，サンドボックスにはこれらの特徴は見られなかった．これらの特徴は他の組織では異なる国情報や IP アドレスになる可能性があるが，同一組織内のユーザマシンは類似した特徴になることが予想される．

ハードウェア情報：標的組織のユーザマシンは複数の外部機器が接続されているとともに，比較的新しい外部機器が接続されていた．また，ディスプレイの大きさや C ドライブの容量，物理メモリの容量などのリソースが大きかった．サンドボックスはユーザマシンと異なりマルウェアの解析や検知を目的としているため，古いマウスやキーボードが接続されていた．また，外部接続機器の数も限られていた．メモリ容量やディスプレイなどもリソースが低かった．

システム情報：標的組織のユーザマシンは登録されている組織やタイムゾーン，システムロケールが共通しており，サンドボックスとは違う特徴になった．これらの特徴は他の組織では異なる可能性があるが，同一組織内のユーザマシンは類似したシステムになることが予想される．

ユーザ利用履歴：標的組織のユーザマシンは多数のプロセスが立ち上がっていた．また，デスクトップフォルダ内のファイル数，壁紙などが設定されていた．加えて，ファイルアクセス履歴の数やシステム稼働時間，最終ログイン日時など，ユーザ利用履歴が存在した．一方，サンドボックスはスナップショットを用いて復元されることからユーザ操作は限られていた．標的組織内のユーザマシンは同じ AV ソフトのプロセスが起動していた．また，MS Office ソフトがインストールされていた．しかし，サンドボックスにはインストールされていなかった．これらの特徴は他の組織では異なる可能性があるが，同一組織内のユーザマシンには共通したソフトウェアがインストールされている可能性がある．

検体実行方法：標的組織のユーザマシンはツールをデスクトップ上で実行するとともに，ツール実行時のファイル名に変更は見られなかった．一方，サンドボックスは解析を自動化しているため，検体を特定のフォルダ上で実行していた．また，検体実行時のファイル名を変更していた．

表 2 サンドボックスアプライアンスとユーザマシンの情報収集結果

Table 2 Feature fingerprinting result of Sandbox appliance and User machines.

	サンドボックス1	サンドボックス2	ユーザ1	ユーザ2	ユーザ3	ユーザ4
# ARP list	2	7	15	50	113	71
# Desktop icons	14	14	0	9	141	20
# Processors	4	4	4	4	4	4
# usb devices	1	1	6	10	24	32
AV soft			■■■■■■	■■■■■■	■■■■■■	■■■■■■
bios manufactturer	Dell Inc	Dell Inc	Hewlett-Packard	Hewlett-Packard	Dell Inc	Dell Inc.
bios release date	2013/■■/■■ ■■:■■:■■	2013/■■/■■ ■■:■■:■■	2015/■■/■■ ■■:■■:■■	2015/■■/■■ ■■:■■:■■	2012/■■/■■ ■■:■■:■■	2013/■■/■■ ■■:■■:■■
Country code of IP address	USA	USA	JP	JP	JP	JP
hostname	….-..	….-..	■■■■■■■	■■■■■■■	■■■■■■■■■■■■	■■■■■■■
Local IP address	10.0.2.15	10.0.2.15	■.■.11.37	■.■.143.221	■.■.143.209	■.■.143.211
last login	2016 4/7	2016 2/3	2016 1/13	2015 4/7	2016 1/25	2016 1/8
OS install date	2013/■■/■■ ■■:■■:■■■■	2014/■■/■■ ■■:■■:■■■■	2014/■■/■■ ■■:■■:■■■■	2015/■■/■■ ■■:■■:■■■■	2013/■■/■■ ■■:■■:■■■■	2016/■■/■■ ■■:■■:■■■■
OS product ID	.*	.*	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■
OS serial number	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■
owner	■■■■ ■■■■■	■■■■■■■	■■■■■■■■■■■■■■■■■■■■■	■■■■■■■■	■■■■■■■-■■	Admin
Registered user	■■■■ ■■■■■	■■■■■■■	■■■■■■■■■■■■■■■■■■■■■	■■■■■■■■	■■■■■■■-■■	Admin
Sample path	Temp	Temp		Desktop	Desktop	Desktop
System locale	English	English	日本語 (日本)	日本語 (日本)	日本語 (日本)	日本語 (日本)
System manufacturer	.*	Dell Inc	Hewlett-Packard	Hewlett-Packard	Dell Inc.	Dell Inc.
System up time (sec)	700	250	2656	1946106	786301	524221
Time zone	Pacific	Pacific	東京 (標準時)	東京 (標準時)	東京 (標準時)	東京 (標準時)
	ユーザ5	ユーザ6	ユーザ7	ユーザ8	ユーザ9	ユーザ10
# ARP list	28	39	20	12	87	20
# Desktop icons	0	16	7	45	138	14
# Processors	8	4	4	8	4	8
# usb devices	20	10	32	14	12	12
AV soft	■■■■■■	■■■■■■	■■■■■■	■■■■■■	■■■■■■	■■■■■■
bios manufactturer	Hewlett-Packard	Hewlett-Packard	Dell Inc.	Dell Inc.	Dell Inc.	Hewlett-Packard
bios release date	2014/■■/■■ ■■:■■:■■	2013/■■/■■ ■■:■■:■■	2011/■■/■■ ■■:■■:■■	2013/■■/■■ ■■:■■:■■	2012/■■/■■ ■■:■■:■■	2014/■■/■■ ■■:■■:■■
Country code of IP address	JP	JP	JP	JP	JP	JP
hostname	■■■■■■■■■-■■	■■■■■■■■	■■■■■■■■	■■■■■■■■■	■■■■■■■■■■■	■■■■■■■■
Local IP address	■.■.143.225	■.■.143.203	■.■.100.6	■.■.143.235	■.■.143.100	■.■.143.230
last login	2016 1/15	2016 1/13	2016 2/2	2016 1/13	2015 12/16	2016 1/13
OS install date	2015/■■/■■ ■■:■■:■■■■	2014/■■/■■ ■■:■■:■■■■	2011/■■/■■ ■■:■■:■■■■	2014/■■/■■ ■■:■■:■■■■	2015/■■/■■ ■■:■■:■■■■	2014/■■/■■ ■■:■■:■■■■
OS product ID	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■
OS serial number	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■	■■■■■-■■■■■-■■■■■-■■■■■
owner	■■■■■■■■■-■■	■■■■■■■■■■■■■■■■■	■■■■■■■■■■■■	■■■■■■■	■■■■■■■■■	■■■■■■■
Registered user	■■■■■■■■■	■■■■■■■■■■■■■■■■■	■■■■■■■■■■■■	■■■■■■■	■■■■■■■■■	■■■■■■■
Sample path	Desktop	Desktop	Desktop	Desktop	Desktop	Desktop
System locale	日本語 (日本)	日本語 (日本)	日本語 (日本)	日本語 (日本)	日本語 (日本)	日本語 (日本)
System manufacturer	Hewlett-Packard	Hewlett-Packard	Dell Inc.	Dell Inc.	Dell Inc.	Hewlett-Packard
System up time (sec)	7994	15595	61863	21787	2508769	242
Time zone	東京 (標準時)	東京 (標準時)	東京 (標準時)	東京 (標準時)	東京 (標準時)	東京 (標準時)

表 3 サンドボックスアプライアンスの回避に有効な特徴とその条件
Table 3 Feature and observation result exfiltrated for evading target sandbox appliance.

カテゴリー	サンドボックス回避に有効な特徴	サンドボックスと判断する条件
ネットワーク情報	ARPリスト内のホスト数	少ない
	現在のネットワークコネクション数	少ない
	グローバルIPアドレスの国情報	日本以外
	ローカルIPアドレス	ユーザと一致しない
ハードウェア情報	外部接続機器の数	少ない
	キーボードデバイスの種類	古い
	マウスデバイスの種類	古い
	ディスプレイの大きさ	小さい
	Cドライブの容量	小さい
	物理メモリの容量	小さい
システム情報	登録されている組織の有無	無
	タイムゾーン	日本以外
	システムロケール	日本以外
ユーザ利用履歴	起動中のプロセス数	少ない
	デスクトップフォルダ内のファイル数	少ない
	ファイルアクセス履歴の数	少ない
	システムの稼働時間	小さい
	AVソフトの有無	無
	MS Officeソフトの有無	無
	壁紙の設定	デフォルト
	最終ログイン日時	古い
検体実行方法	検体実行時のフォルダ名	ユーザと一致しない
	検体実行時のファイル名	ユーザと一致しない

なお，サンドボックス 1，2 それぞれ情報の取得に 11 回成功しており，取得したサンドボックス情報のうち，OS インストール日時，登録されているユーザ，シリアル番号が一致するものは同一のサンドボックスであると判断している．このため，実際にはさらに多くのサンドボックスが運用されている可能性がある．

5.3 サンドボックスとユーザマシンの環境の差異に着目したサンドボックスアプライアンスの回避

実験に用いたサンドボックスとユーザマシンの環境には大きな差異が存在したため，攻撃者はこの差異を用いてサンドボックスアプライアンスを回避する可能性がある．**表 3** に当該アプライアンスを回避して，ユーザマシン上で不正活動を行うマルウェアを作成するのに有効な 23 種類の特徴とその条件をまとめる．表 3 における条件とは，作成したマルウェアが条件を満たす場合に実行環境はサンドボックスであると判断し，そうでない場合にユーザマシンであると判断するための指標である．ARP リスト内のホスト数，現在のネットワークコネクション数，起動中のプロセス数，デスクトップフォルダ内のファイル数，ファイルアクセス履歴の数，システム稼働時間は定常的に変わる特徴であり，表 3 における条件も小さい，あるいは少ないとしている．ただし，サンドボックスよりも小さい，あるいは少ない特徴になるユーザマシンも存在したため，特徴を個別に用いた場合にはユーザマシンをサンドボックスと判断する可能性がある．キーボードデバイスの種類，マウスデバイスの種類，ディスプレイの大きさ，C ドライブの容量，登録されている組織は 1 度設定したら頻繁には変わらない特徴であり，表 3 における条件も古い，小さい，あるいは設定の有無としている．これらの特徴についても，サンドボックスと同じ特徴や，サンドボックスよりも小さい値になるユーザマシンが存在した．表 3 における AV ソフト，MS Office ソフトについてはインストールの有無，壁紙については設定状況，最終ログイン日時については古さを条件としている．これらの特徴についても，サンドボックスと同じ特徴を持つユーザマシンが存在した．上記の特徴については，複数の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とユーザマシンを正しく区別できる可能性がある．一方，グローバル IP アドレスの国情報，ローカル IP アドレス，タイムゾーン，システムロケール，検体実行時のフォルダ名，検体実行時のファイル名はすべてのユーザマシンで同じ特徴になった．また，これらの特徴はいずれのサンドボックスにおいても見られなかった．外部接続機器の数，物理メモリの大きさについてもユーザマシンとサンドボックスに大きな差異が見られた．このような特徴については，個別に用いた場合でも実験に用いたサンドボックスとユーザマシンを正しく区別できる可能性がある．検証実験では，これらの特徴の選定や条件の設定は手動で行ったが，機械学習などを用いて自動化することも可能であり今後の課題とする．

実際の攻撃では，攻撃者は標的組織から収集したユーザマシンとサンドボックスの情報を比較し，差異が見られる特徴やその条件を特定する．そして，その特徴を用いてサンドボックスアプライアンスを回避する機能を有するマルウェアを実装する．マルウェアの実装には，特定した特徴を個別に利用する場合や，複数の特徴を組み合わせる場合が考えられる．一般に，特徴を組み合わせることでユーザマシンとサンドボックスを区別できる可能性は高くなるが，サンドボックスアプライアンスの中にはサンドボックスの情報を収集する挙動を検知するものが存在する．このため，特徴の選び方は攻撃者の目的によって様々である．同様に，サンドボックスがユーザマシンと判断される可能性を低くしたいのか，ユーザマシンがサンドボックスと判断される可能性を低くしたいのかなど攻撃者の目的によって特徴の組合せやその条件の設定方法も様々である．そのため，検証実験で特定した特徴や条件を攻撃者が利用するとは限らない．しかし，検証実験の結果から実際に製品として導入されたサンドボックスアプライアンスにおいても，導入先の組織内の環境と整合性のあるようなカスタマイズは行われていない例が確認された．また，攻撃者は同様の方法を用いて標的組織のサンドボックスアプライアンスを回避するマルウェアを作成することが可能である．標的組織の内部情報を有する攻撃者に対してサンドボックスアプライアンスが有効に働くためには，組織内の環境と整合したサンドボックスを用意する必要がある．具体的な対策については 6 章で考察する．

一方，攻撃者はユーザマシンとサンドボックスに差異が見られる特徴以外にも，サンドボックスに固有な特徴をブラックリストとして用いることで，サンドボックスアプライアンスを回避することができる．たとえば，検証実験に使用したサンドボックスは，OS インストール日時，bios 情報，キーボードデバイス ID，マウスデバイス ID，登録されているユーザ，シリアル番号，システム所有者がつねに同じ値/文字列になった．攻撃者はこれらの特徴を用いてサンドボックスを回避するマルウェアを作成することができる．同様に，過去の侵入成功経験などからすでに標的のマシン情報を有する攻撃者は，標的マシンに固有な情報をホワイトリストとして用いることで，特定のマシン上でのみ動作するマルウェアを作成することができる [35]．

6. 考察

6.1 検証実験結果の一般性

検証実験では，あらかじめユーザに実験内容を伝え，意図的に情報収集ツールを実行するように指示した．このため，すべての攻撃者が我々と同様の情報を収集できるとは限らない．しかし，情報収集ツールを用いて収集した情報の中には，ユーザから情報を収集しなくても推測できる情報が存在する．たとえば，実験環境のユーザの多くが日本人であることから，使用しているマシンの言語設定は日本語設定であることが推測できる．実際に，実験に使用したユーザマシンはすべて日本語環境であるのに対し，サンドボックスはいずれも英語環境であった．同様に，IP アドレスの国情報やタイムゾーンの情報も容易に推測することができる．また，情報収集ツールを実行させる以外にも，標的組織の構成員がアクセスする可能性のある Web サイトに情報収集用の JavaScript などを用意しておき，これを介して情報収集する方法，いわゆる水飲み場型攻撃や，これらの Web サイトへのアクセスを誘引するメールを送付する方法が考えられる．JavaScript で取得できる情報は実行形式のファイルに比べて限られているが，たとえばブラウザの種類やバージョン，利用可能なフォント，プラグイン，言語などの情報を収集することができる [28]．

検証実験を行ったユーザは研究を行う組織に所属しており，論文の調査や資料の作成を業務としている．また，多くのマシンが組織内の DNS サーバを用いてインターネットと通信を行うとともに，DHCP サーバからローカル IP アドレスを取得しており，典型的なネットワーク構成をしている．実験に用いたマシンは，比較的新しいものから数年前に購入されたデスクトップマシン，ノート PC が含まれている．このため，マシンの性能には差異が見受けられ，5.3 節で説明したようにサンドボックスと同じ特徴を持つマシンが存在した．一般に，組織の種類や規模，部署ごとにユーザ環境は異なるため，表 3 に示す結果が他の組織で有効とは限らない．しかし，検証実験の結果から標的組織の内部情報を有する攻撃者はこれらの特徴以外にも，攻撃対象組織のサンドボックスとユーザマシンの間で差異が存在する特徴を特定することで，サンドボックスアプライアンスを回避するマルウェアを作成する可能性がある．このため，複数の組織に対して実験を行うことが望ましく，今後の課題とする．

サンドボックスアプライアンスは標的型攻撃や未知の脅威に対抗する手段として人気を集めており，研究開発が進んでいる．セキュリティベンダのもとには世界中に設置したセンサから日々脅威情報が届き，アプライアンスにフィードバックすることでより多くのマルウェアの検知が可能となっている．一方，マルウェア解析サービスや研究者が管理しているサンドボックスはマルウェア検体の解析を目的としている．このため，サンドボックスアプライアンスはこれらのサンドボックスに比べ回避耐性を有することが予想される．検証実験では，ある特定の組織に導入されているクラウド型サンドボックスアプライアンスの回避可否を検証した．しかし，サンドボックスが導入先の組織内に設置されているオンプレミス型サンドボックスアプライアンスに比べ，回避耐性が低い可能性がある．また，導入先の組織内の環境と整合性のあるサンドボックスを運用している組織も存在するため，複数の組織に対して実験を行うことが望ましい．セキュリティアプライアンスを導入している組織に対して検証実験を行うのは難しい場合が多いため，今後はより多くのアプライアンスで実験を行うことを目標とする．

6.2 サンドボックスアプライアンス回避攻撃への対策

一般に，組織ごとにサンドボックスアプライアンスの種類やユーザ環境は異なるため，表 3 に示す結果が他の組織で有効とは限らない．しかし，標的組織のサンドボックスとユーザマシンの間で差異が存在する特徴を特定することで，攻撃者はサンドボックスアプライアンスを回避することが可能である．このため，サンドボックス運用者は組織内の環境と整合したサンドボックスを用意する必要がある．組織内の環境と整合したサンドボックスを用意するためには，5.2 節で特定した標的組織のユーザマシンに共通して見られるがサンドボックスアプライアンスには見られない特徴を改善することや，その一方でサンドボックスに共通して見られるがユーザマシンに見られない特徴を改善する必要がある．

検証実験では，グローバル IP アドレスの国情報やローカル IP アドレス，タイムゾーン，システムロケールはすべてのユーザマシンで同じ特徴になり，サンドボックスには見られなかった．オンプレミス型サンドボックスを運用している組織では，サンドボックスの設定を変更することで容易に改善することができる．一方，クラウド型サンドボックスアプライアンスの場合，セキュリティベンダがサンド

ボックスの管理を行っているため，セキュリティベンダがアプライアンスを導入している組織ごとに整合性のあるサンドボックスを用意するか，マルウェア検体を実行する前にサンドボックスの特徴を変更する必要がある [37]．また，検証実験に用いたユーザマシンの多くは特定のソフトウェアをインストールしていたが，サンドボックスには見られなかった．サンドボックスにこれらのソフトウェアをインストールするにはコストがかかるが，ファイル名やプロセス名，ディレクトリ構造が同じダミーのプログラムを用意することでサンドボックスを改善できる可能性がある．

サンドボックスに共通して見られるがユーザマシンに見られない特徴を改善する方法については，研究開発が進んでいる．論文 [36] において，プロダクト ID などを用いて特定のサンドボックスを検知する手法が明らかにされており，実運用されているサンドボックスの中にも一部の値をランダム化することで，サンドボックス検知を困難にするものが存在する．同様に，サンドボックスの中には，サンドボックスの値を実マシンと同等の値にすることで，サンドボックス検知を困難にするものが存在する．検証実験で観測したサンドボックスにおいても，検体が実行されるたびにプロダクト ID やホスト名，システム製造元がランダム化されていた．また，プロセッサの数などは実マシンと同等の値になっていた．このため，検証実験に用いたサンドボックスアプライアンスも検知耐性があることが分かる．しかし，サンドボックスはマルウェア検体を実行するために作成されるため，インストール直後の状態で運用されることが多い．一方で，ユーザマシンは日常の業務に用いられるため，デスクトップやツールバーに，デフォルトではインストールされていないソフトウェアのアイコン（ブラウザ，プラグイン，クライアントソフトなど）などのユーザ利用履歴が存在することが多い [29]．また，サンドボックスの多くは解析を自動化しているため，検体実行時のフォルダ名や検体実行時のファイル名がユーザマシンと大きく異なる．このため，サンドボックス開発者はこれらの特徴を改善することで，サンドボックスの検知を難しくすることが重要である．

6.3 研究倫理的対応

本研究は，標的組織内の環境と整合したサンドボックスを実装することで攻撃者によるサンドボックス検知を困難にし，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サンドボックスオペレータとセキュリティベンダ計 23 者に対して，サンドボックスの特徴が検知回避に利用される恐れがある点の指摘や実験に用いた情報収集ツールの提供，推奨される対策方法などの情報提供を行った．このうち，2 者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，表 3 におけるサンドボックス回避有効な 23 種類の特徴については，判定のための明確な基準を示すことを避け，論文の情報が攻撃者に直接的に悪用されないようにしている．このように，本研究はサンドボックスの性能向上に貢献していると考える．

7. 関連研究

サンドボックス解析を回避するマルウェアが増加しており，対策が求められている．サンドボックス解析を回避するマルウェアに関する研究は様々存在するが，サンドボックスの多くは仮想化技術やエミュレータを用いて実現されため，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行われている．論文 [30] では，マルウェアが解析環境を検知するのに使う情報を調べ，サンドボックスの情報を実マシンのものに置き換える手法が提案されている．また，論文 [31] ではハードウェアに Intel VT のような仮想化支援技術を用いることによって実マシンと区別のつきにくいサンドボックスを実現する方法が提案されている．論文 [32] 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．

サンドボックスの実現方法に関する研究が行われている一方で，複数の実行環境でマルウェア検体を実行し，実行環境ごとに見られる挙動の違いを利用してサンドボックス解析を回避するマルウェアを発見する研究が行われている．論文 [33] では，サンドボックス内にマルウェアの挙動を観測する技術が組み込まれたものとそうでないものを用意し，解析結果を比較することでサンドボックスを回避するマルウェアを発見する手法が提案されている．また，論文 [34] ではマルウェアの挙動をモデル化する手法を提案し，サンドボックス実現技術の異なるサンドボックス上でマルウェア検体を実行したときの解析結果を比較することで，サンドボックスを回避するマルウェアを発見する手法が提案されている．

我々は，論文 [29] において標的組織の内部情報を持たない攻撃者でも，サンドボックスに共通して見られる特徴を用いてサンドボックスアプライアンスを回避できることを示した．本研究では，さらなる侵入や継続的な情報漏えいを防ぐために，標的組織の情報システムやセキュリティ対策に関する内部情報を有している攻撃者に対する，サンドボックスアプライアンスの回避耐性を調査した．

8. まとめと今後の課題

標的組織の内部情報を有する攻撃者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ため，サンドボックスアプライアンスが導入されている組織に対する攻撃を分類し，どのような情報がサンドボックスアプライアンス

回避に有効であるかを検討した．また，内部情報を利用した攻撃の具体例として，サンドボックスと実ユーザ環境の差異に着目してマルウェアの挙動を変えることでアプライアンスによる検知回避を試みる攻撃者を想定し，実際に組織に導入されたサンドボックスアプライアンスが回避されうるか検証した．

今後の課題は，情報収集方法を改善するとともに，さらに多くの環境下で実験を行うことである．また，サンドボックスアプライアンスを回避するマルウェアへの対策方法について検討することである．

謝辞 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」により得られた．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．

参考文献

[1] NISC：日本年金機構における個人情報流出事案に関する原因究明調査結果, 入手先 ⟨http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf⟩ （参照 2016-08-12）.
[2] BlueCoat: Malware Analysis System, available from ⟨https://www.bluecoat.com/ja/products-and-solutions/malware-analysis⟩ (accessed 2016-08-09).
[3] CheckPoint: Threat Emulation, available from ⟨https://www.checkpoint.co.jp/products/threat-emulation-sandboxing/index.html⟩ (accessed 2016-08-09).
[4] Cisco: Advanced Malware Protection, available from ⟨http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html⟩ (accessed 2016-08-09).
[5] Dell: SonicWall Capture, available from ⟨https://www.sonicwall.com/jp-ja/products/sonicwall-capture-atp/⟩ (accessed 2016-08-09).
[6] FFRI: Yarai Analyzer, available from ⟨http://www.ffri.jp/products/yarai_analyzer/⟩ (accessed 2016-08-09).
[7] FireEye: Malware Analysis, available from ⟨https://www.fireeye.com/products/malware-analysis.html⟩ (accessed 2016-08-09).
[8] Fortinet：フォーティネット、持続的標的型攻撃（APT）を防止するためのクラウド型サンドボックスおよび IP レピュテーションサービスを開始，入手先 ⟨http://www.fortinet.co.jp/press_releases/130311.html⟩ （参照 2016-08-09）.
[9] Fortinet: FortiSandbox, available from ⟨http://www.fortinet.co.jp/products/fortisandbox/⟩ (accessed 2016-08-09).
[10] Hitachi：マッシュアップ型マルウェア解析支援システム，入手先 ⟨http://www.hitachi-as.co.jp/news/141225.html⟩ （参照 2016-08-09）.
[11] IIJ：IIJ セキュア MX サービス，入手先 ⟨http://www.iij.ad.jp/biz/smx/⟩ （参照 2016-08-09）.
[12] Lastline: Provide your forensics team with the tools they need, available from ⟨https://www.lastline.com/platform/analyst⟩ (accessed 2016-08-09).
[13] McAfee: Advanced Threat Defence, available from ⟨http://www.mcafee.com/jp/promos/atd/index.aspx⟩ (accessed 2016-08-09).
[14] Paloalto: WildFire, available from ⟨https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/wildfire⟩ (accessed 2016-08-09).
[15] Proofpoint: Targeted Attack Protection, available from ⟨https://www.proofpoint.com/jp/products/targeted-attack-protection⟩ (accessed 2016-08-09).
[16] SecureBrain: Zero-hour Response System, available from ⟨http://www.securebrain.co.jp/products/zhr/⟩ (accessed 2016-08-09).
[17] Sophos: Sandstorm, available from ⟨https://www.sophos.com/ja-jp/lp/sandstorm.aspx⟩ (accessed 2016-08-09).
[18] Symantec: Advanced Threat Protection, available from ⟨https://www.symantec.com/ja/jp/advanced-threat-protection/⟩ (accessed 2016-08-09).
[19] TrendMicro：Deep Discovery ファミリー, 入手先 ⟨http://www.trendmicro.co.jp/jp/business/products/dd/⟩（参照 2016-08-09）.
[20] WatchGurad: APT Blocker, available from ⟨https://www.watchguard.co.jp/apt-blocker⟩ (accessed 2016-08-09).
[21] Websence: Sandbox Modules, available from ⟨https://www.websense.com/assets/datasheets/datasheet-module-sandbox-en.pdf#search='Websence+Sandbox+Modules⟩ (accessed 2016-08-09).
[22] McAfee：McAfee Labs 2016 年の脅威予測，入手先 ⟨http://www.mcafee.com/jp/resources/reports/rp-threats-predictions-2016.pdf⟩ （参照 2016-08-12）.
[23] Lastline blog: Three interesting changes in malware activity over the past year, available from ⟨http://labs.lastline.com/three-interesting-changes-in-malware-activity-over-the-past-year⟩ (accessed 2016-08-12).
[24] FireEye：ファイルベースのサンドボックス回避，入手先 ⟨https://www.fireeye.jp/content/dam/fireeye-www/regional/ja_JP/current%20threats/pdfs/fireeye-hot-knives-through-butter.pdf#search='hot+knives+fireeye⟩ （参照 2016-08-12）.
[25] 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#search='Prevalent+characteristics+in+modern+malware'⟩ (accessed 2016-08-12).
[26] ZDNet：長期潜伏，自らを削除—サンドボックスを回避する未知のマルウェア，入手先 ⟨http://japan.zdnet.com/article/35047336/2/⟩ （参照 2016-08-12）.
[27] IPA：「高度標的型攻撃」対策に向けたシステム設計ガイド，入手先 ⟨http://www.ipa.go.jp/files/000046236.pdf⟩ （参照 2016-08-12）.
[28] Electronic Frontier Foundation: Panopticlick, available from ⟨https://panopticlick.eff.org/⟩ (accessed 2016-08-12).
[29] 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, *19th International Symposium on Research in Attacks, Intrusions and Defenses, RAID 2016*, Paris, France (2016).
[30] Vasudevan, A. and Yerraballi, R.: Cobra: Fine-grained Malware Analysis using Stealth Localized-executions, *IEEE Symposium on Security and Privacy* (2006).
[31] Dinaburg, A., Royal, P., Sharif, M. and Lee, W.: Ether, Malware Analysis via Hardware Virtualization Extensions, *ACM Conference on Computer and Communications Security* (*CCS*) (2008).
[32] Kirat, D., Vigna, G. and Kruegel, C.: Barebox: Efficient malware analysis on bare-metal, *Annual Computer*

Security Applications Conference (*ACSAC*), *2011*, 403-412.
[33] Kirat, D., Vigna, G. and Kruegel, C.: Barecloud: bare-metal analysis-based evasive malware detection, *23rd USENIX Conference on Security Symposium* (*SEC'14*), pp.287–301, USENIX Association (2014).
[34] Lindorfer, M., Kolbitsch, C. and Milani, P.: Detecting Environment-Sensitive Malware, *14th international conference on Recent Advances in Intrusion Detection* (*RAID' 11*), pp.338–357 (2011).
[35] Kaspersky：特定環境下でしか動かないマルウェアを報告，入手先 ⟨http://itpro.nikkeibp.co.jp/atcl/news/16/120703664/?rt=nocnt⟩（参照 2017-04-25）.
[36] 笠間貴弘，織井達憲，吉岡克成，松本 勉：公開型マルウェア動的解析システムに対するデコイ挿入攻撃の脅威，*Journal of Information Processing*, Vol.52, No.9, pp.2761–2774 (2011).
[37] 田辺瑠偉，八幡篤司，石井 攻，横山日明，吉岡克成，松本 勉：サンドボックス解析回避への耐性を高めるツール SandVeil の提案, 電子情報通信学会技術報告, ISEC2017-8, pp.43–49 (2017).

推薦文

本研究は攻撃者の視点でセキュリティアプライアンスをみた際に，攻撃者がいかにサンドボックスを検知できるかを明らかにしている．このような知見は今後さらに進化するマルウェア対策の方向性に示唆を与えるものである．本研究で明らかになったサンドボックスと実ユーザ環境の差異は，サンドボックスを活用する研究者および実務家の両者が前提知識として知っておくべき事実であり，実用性が高い．よって推薦論文として推薦する．

（マルウェア対策研究人材育成ワークショップ 2016
プログラム委員長 森 達哉）

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 月より国立大学法人横浜国立大学産学官連携研究員．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．

石井 攻

2016 年 3 月横浜国立大学理工学部数物・電子情報系学科卒業．同年 4 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に進学．マルウェア解析等のネットワークセキュリティに関する研究に従事．

横山 日明

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前期修了．修士（工学）．同年 4 月株式会社 NTT ドコモ入社．在学中，情報セキュリティに関する研究に従事．

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にて研究員として勤務．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 月より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・検知等の情報システム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）受賞．

松本 勉 （正会員）

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．2014 年 12 月より同大学先端科学高等研究院（IAS-YNU）情報物理セキュリティ研究ユニットリーダーを兼務．ネットワーク・ソフトウェア・ハードウェアセキュリティ，暗号，耐タンパ技術，生体認証，人工物メトリクス等の「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．1994 年第 32 回電子情報通信学会業績賞，2006 年第 5 回ドコモ・モバイル・サイエンス賞，2008 年第 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）各受賞．