標的組織の内部情報を有する攻撃者を前提とした セキュリティアプライアンス評価

田辺 瑠偉[†1] 石井 攻[†1] 横山 日明[†1]
吉岡 克成[†2] 松本 勉[†2]

概要：継続的かつ執拗に特定の組織等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．更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 Security Appliance against Persistent Attackers who has Prior Knowledge of Target Organization

Rui Tanabe[†1] Kou Ishii[†1] Akira Yokoyama[†1]
Katsunari Yoshioka[†2] Tsutomu Matsumoto[†2]

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, in this study, we evaluate the capability of security appliances against attackers who have prior knowledge of target organization. In this report, 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, implying that the defense could 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．例えば，2015 年に発生した日本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渡って送信された．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した[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事が想定される．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，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

†1 横浜国立大学
Yokohama National University
†2 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

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 章で考察を行い，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事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ー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無いため，セキュリティポリシーの厳しい組織でも利用することができる．

表 1. サンドボックスアプライアンス一覧

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

多くのセキュリティベンダー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毎に様々であり，vmware や vbox 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ー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毎に 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る技術の中でも，サンドボックスが有する特徴を予め把握し，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，予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ー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，ネットワーク等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．例えば，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して判断する．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]．

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，まず始めに悪性挙動を開始する条件を設定する．例えば，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時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

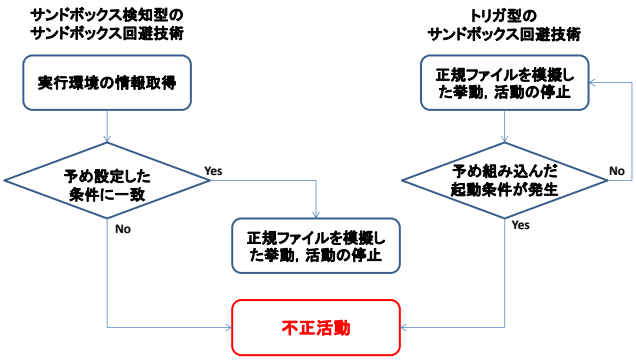

図 1. サンドボックス検知型・トリガ型のサンドボックス回避技術を用いたサンドボックス回避

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[24-26]．また，マスター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ものについて説明する．

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．標的組織に関する内部情報が多いほど，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．同様に，AV ソフトやスパムフィルタの有無，exe ファイルの送信可否といったセ

キュリティ対策やセキュリティポリシーに関する情報も重要である．そして，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，セキュリティ対策の迂回を試みる．サンドボックスアプライアンスの回避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 節で実験に用い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．

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 1 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ユーザマシンのトラヒックの一部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する．ツールの送信には，検体ダウンロード用 URL が記述されたメールをユーザに送る方法と，ツールをメールに添付してユーザに送る方法の 2 種類の方法を試した．どちらの方法でも，サンドボックスアプライアンスが検体の解析を行った．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と，全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．表 2 に収集した情報の一部をまとめる．クラウド型サンドボックスアプライアンスからは 2 種類のサンドボックスの情報を収集する事ができた（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）．サンドボックス 1，2 どちらもプロダクト ID とホスト名をランダムな文字列にしており，これらの情報を用いたサンドボックスの検知に

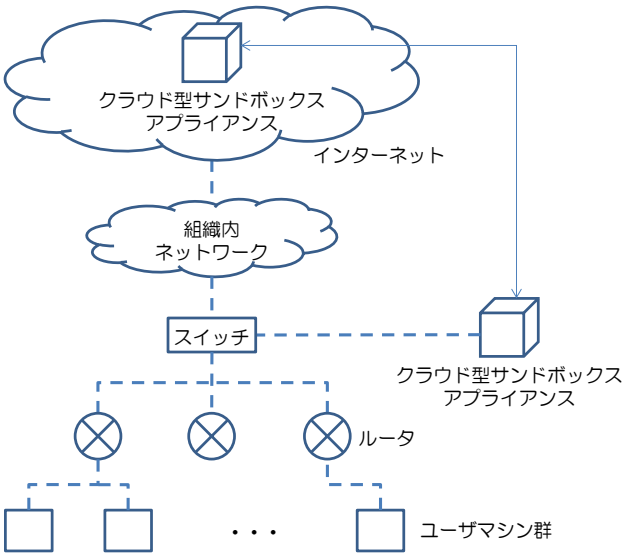

図 2. 実験環境のネットワーク構成

耐性がある事がわかった．一方，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．具体的には，ユーザマシンは ARP リストのホスト数が十以上であるのに対し，サンドボックスは数ホスト程度であった．また，ユーザマシンには多くの外部接続機器が接続されているのに対し，サンドボックスではあまり見られなかった．ユーザマシンの多くでファイルシステム上に AV ソフトの名前のディレクトリが存在するのに対し，サンドボックスには見られなかった．ユーザマシンではグローバル IP アドレスの国情報が日本であるのに対し，サンドボックスではアメリカであった．ユーザマシンの多くは組織内の DNS サーバを利用しているのに対し，サンドボックスでは独自の DNS サーバを利用していた．ユーザマシンの多くは最終ログイン日時が一ヶ月以内であるのに対し，サンドボックスは一カ月以上前であった．ユーザマシンの多くは検体をデスクトップ上で実行していたのに対し，サンドボックスでは Temp ファルダ上で実行していた．ユーザマシンはシステムロケールが日本であるのに対し，サンドボックスは英語であった．ユーザマシンではシステム稼働時間が数千秒であるのに対し，サンドボックでは数百秒程度であった．ユーザマシンはタイムゾーンが東京であるのに対し，サンドボックスは太平洋であった．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，実際には更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．

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

	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			[redacted]	[redacted]	[redacted]	[redacted]
bios manufactturer	Dell Inc	Dell Inc	Hewlett-Packard	Hewlett-Packard	Dell Inc	Dell Inc.
bios release date	2013/[redacted]	2013/[redacted]	2015/[redacted]	2015/[redacted]	2012/[redacted]	2013/[redacted]
Country code of IP address	USA	USA	JP	JP	JP	JP
hostname	….-..	….-..	[redacted]	[redacted]	[redacted]	[redacted]
IP address of DNS server	10.0.2.15	10.0.2.15	0.0.0.0	[redacted].143.221	[redacted].143.209	[redacted].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/[redacted]	2014/[redacted]	2014/[redacted]	2015/[redacted]	2013/[redacted]	2016/[redacted]
OS product ID	.*	.*	[redacted]	[redacted]	[redacted]	[redacted]
OS serial number	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
owner	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Admin
Registered user	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	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	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
bios manufactturer	Hewlett-Packard	Hewlett-Packard	Dell Inc.	Dell Inc.	Dell Inc.	Hewlett-Packard
bios release date	2014/[redacted]	2013/[redacted]	2011/[redacted]	2013/[redacted]	2012/[redacted]	2014/[redacted]
Country code of IP address	JP	JP	JP	JP	JP	JP
hostname	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
IP address of DNS server	[redacted].143.225	[redacted].143.203	[redacted].100.6	[redacted].143.235	[redacted].143.100	[redacted].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/[redacted]	2014/[redacted]	2011/[redacted]	2014/[redacted]	2015/[redacted]	2014/[redacted]
OS product ID	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
OS serial number	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
owner	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Registered user	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
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)

サンドボックス回避に有効な特徴	条件
ARPリスト内のホスト数	< 8
USBデバイスの数	< 2
AVソフトの有無	なし
IPアドレスの国情報	日本以外
DNSサーバのIPアドレス	10.0.2.15
最終ログイン日時	1ヶ月以上前
検体実行ディレクトリ	Temp
システムロケール	日本以外
システム稼働時間	< 700sec
タイムゾーン	東京以外

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

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

サンドボックスとユーザマシンの環境の差異に着目して，実験に用いたサンドボックスアプライアンスが実際に回避できるか検討した．表 3 に当該アプライアンスの回避をして，ユーザマシン上で悪性挙動を行うマルウェアを作成するのに有効な条件をまとめる．本実験では，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，全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とも推測できる情報が存在する．例えば，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全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．一方，サンドボックスとユーザマシンにはログイン履歴やシステム稼働時間に差が見られた．これらの特徴はユーザマシン毎に様々であるが，攻撃者もサンドボックスの回避に有効な条件を推測できる事が予想される．

6. 考察

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サンドボックスアプライアンスを回避できる可能性があることを確認した．検証実験では標的組織の内部情報の収集に実行形式のツールを用いており，全ての組織で実行形式のファイルを実行させ情報を収集できるとは限らない．しかしながら，実行形式のファイ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 等を用意しておき，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も考えられる．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，例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].

一般に，組織毎にユーザマシンやサンドボックスアプライアンスの設定は異なる．このため，5.3 節で示したサンドボックスアプライアンスの回避に有効な特徴が他の組織に見られるとは限らない．しかし，標的組織の情報を収集してサンドボックスアプライアンスとユーザマシンの差異を特定することで，他の組織においてもサンドボックスアプライアンスを回避できる可能性がある．このようにサンドボックスアプライアンスを回避するマルウェアに対する対策が必要である．

本実験で使用したサンドボックスアプライアンスは，検体が実行される度にプロダクト ID やホスト名をランダマイズしており，サンドボックス検知を困難にしている．また，プロセッサの数やメモリの大きさなどは実マシンと同等の値になっており，検知耐性があることがわかる．しかし，OS の言語設定や使用しているアプリケーションなど，ユーザマシンに共通して見られる特徴がサンドボックスアプライアンスには見られなかった．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，ユーザマシンは日常の業務に用いられるため，カスタマイズされることが多い．例えば，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,office など）が含まれていることが多い[29]．このような特徴をサンドボックスに反映し，標的組織内の環境と整合したサンドボックスを用意することで，攻撃者にサンドボックスとユーザマシンの区別を難しくすることが重要である．

検証実験では，サンドボックスと実ユーザ環境の差異に着目して実際に組織で運用されている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したが，攻撃者はサンドボックスに固有な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事が可能であった．実際に，当該実験に使用したサンドボックスでは，OS インストール日時，プロダクト ID，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，システム所有者は常に同じ値になった．インターネットに接続されたサンドボックスアプライアンスを運用している組織に対しては，このような攻撃方法も有効である．

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ー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，実行環境毎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，更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する．

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を検証した．

今後の課題は，情報収集方法を改善するとともに，更に多くの環境下で実験を行う事である．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事である．

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．

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. http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf, last visited 2016/08/12.
[2] BlueCoat, Malware Analysis System. https://www.bluecoat.com/ja/products-and-solutions/malware-analysis, last visited 2016/08/09.
[3] CheckPoint, Threat Emulation. https://www.checkpoint.co.jp/products/threat-emulation-sandboxing/index.html, last visited 2016/08/09.
[4] Cisco, Advanced Malware Protection. http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html, last visited 2016/08/09.
[5] Dell, SonicWall Capture. https://www.sonicwall.com/jp-ja/products/sonicwall-capture-atp/, last visited 2016/08/09.
[6] FFRI, Yarai Analyzer. http://www.ffri.jp/products/yarai_analyzer/, last visited 2016/08/09.
[7] FireEye, Malware Analysis. https://www.fireeye.com/products/malware-analysis.html, last visited 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. http://www.fortinet.co.jp/press_releases/130311.html, last visited 2016/08/09.
[9] Fortinet, FortiSandbox. http://www.fortinet.co.jp/products/fortisandbox/, last visited 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. http://www.hitachi-as.co.jp/news/141225.html, last visited 2016/08/09.
[11] IIJ, IIJ セキュア MX サービス. http://www.iij.ad.jp/biz/smx/, last visited 2016/08/09.
[12] Lastline, Provide your forensics team with the tools they need. https://www.lastline.com/platform/analyst, last visited 2016/08/09.
[13] McAfee, Advanced Threat Defence. http://www.mcafee.com/jp/promos/atd/index.aspx, last visited 2016/08/09.
[14] Paloalto, WildFire. https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/wildfire, last visited 2016/08/09.
[15] Proofpoint, Targeted Attack Protection. https://www.proofpoint.com/jp/products/targeted-attack-protection, last visited 2016/08/09.
[16] SecureBrain, Zero-hour Response System. http://www.securebrain.co.jp/products/zhr/, last visited 2016/08/09.
[17] Sophos, Sandstorm. https://www.sophos.com/ja-jp/lp/sandstorm.aspx, last visited 2016/08/09.
[18] Symantec, Advanced Threat Protection. https://www.symantec.com/ja/jp/advanced-threat-protection/, last visited 2016/08/09.
[19] TrendMicro, Deep Discovery ファミリー. http://www.trendmicro.co.jp/jp/business/products/dd/, last visited 2016/08/09.
[20] WatchGurad,APT Blocker. https://www.watchguard.co.jp/apt-blocker, last visited 2016/08/09.
[21] Websence, Sandbox Modules. https://www.websense.com/assets/datasheets/datasheet-module-sandbox-en.pdf#search='Websence+Sandbox+Modules, last visited 2016/08/09.
[22] McAfee, McAfee Labs 2016 年の脅威予測.

http://www.mcafee.com/jp/resources/reports/rp-threats-predictions-2016.pdf, last visited 2016/08/12.
[23] Lastline blog, Three interesting changes in malware activity over the past year. http://labs.lastline.com/three-interesting-changes-in-malware-activity-over-the-past-year, last visited 2016/08/12.
[24] FireEye, ファイルベースのサンドボックス回避. https://www.fireeye.jp/content/dam/fireeye-www/regional/ja_JP/current%20threats/pdfs/fireeye-hot-knives-through-butter.pdf#search='hot+knives+fireeye, last visited 2016/08/12.
[25] G.N.Barbosa, R.R.Branco. (2014) Prevalent characteristics in modern malware. https://www.blackhat.com/docs/us-14/materials/us-14-Branco-Prevalent-Characteristics-In-Modern-Malware.pdf#search='Prevalent+characteristics+in+modern+malware', last visited 2016/08/12.
[26] 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. http://japan.zdnet.com/article/35047336/2/, last visited 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. “http://www.ipa.go.jp/files/000046236.pdf”, last visited 2016/08/12.
[28] Panopticlick. https://panopticlick.eff.org/, last visited 2016/08/12.
[29] A.Yokoyama, K.Ishii, R.Tanabe, Y.Papa, K.Yoshioka, T.Matsumoto, T.Kasama, D.Inoue, M.Brengel, M.Backes, and C.Rossow. "Sandprint: Fingerprinting Malware Sandboxes to Provide Intelligence for Sandbox Evasion". 19th International Symposium on Research in Attacks, Intrusions and Defenses, RAID 2016, Paris, France.
[30] A.Vasudevan, and R.Yerraballi, Cobra: Fine-grained Malware Analysis using Stealth Localized-executions”, IEEE Symposium on Security and Privacy, 2006.
[31] A.Dinaburg, P.Royal, M.Sharif, and W.Lee, Ether, “Malware Analysis via Hardware Virtualization Extensions”, ACM Conference on Computer and Communications Security (CCS) , 2008.
[32] D. Kirat, G. Vigna, and C. Kruegel, “Barebox: Efficient malware analysis on bare-metal”, Annual Computer Security Applications Conference (ACSAC), 2011, 403-412.
[33] D.Kirat, G.Vigna, and C.Kruegel, “Barecloud: bare-metal analysis-based evasive malware detection”, 23rd USENIXconference on Security Symposium (SEC'14). USENIX Association, Berkeley, CA, USA, 287-301.
[34] M.Lindorfer, C.Kolbitsch, and P.Milani, “Detecting Environment-Sensitive Malware”, 14th international conference on Recent Advances in Intrusion Detection(RAID’11), 338-357, 2011.