Vol.2012-DPS-150 No.5
Vol.2012-CSEC-56 No.5
2012/2/29

未検知マルウェアへの対応に基づく アンチウイルスソフトウェアの評価

橋本遼太[†]　吉岡克成[†]　松本 勉[†]

マルウェアの出現数が増加を続けており，マルウェアの集合は常に変化を続けているのに対して，固定の検体セットに基づく従来のアンチウイルスソフトの評価は検知性能を正確に表しているとはいえない．実効性のあるマルウェア対策を行うためには，変化し続けるマルウェア群に対して適切に対応することが重要といえる．本稿では，未検知マルウェア情報を様々な方法でアンチウイルスベンダに提示し，当該マルウェアに対する対応が迅速に行われるか否かという観点でアンチウイルスソフトを評価する手法を提案する．また，提案手法を用いて 11 種類のアンチウイルスソフトの評価実験を行った結果を示す．評価実験で用いた未検知検体は，待受型のハニーポットで捕捉されたものであり，インターネットに接続していれば，誰でも遭遇しうる実マルウェアであるにも関わらず，アンチウイルスベンダの対応には大きな差が見られることがわかった．

Evaluation of Anti-Virus Software based on the Correspondence to Non-Detected Malware

Ryota Hashimoto[†]　Katsunari Yoshioka[†]
and Tsutomu Matsumoto[†]

Malware are evolving and the set of malware existing in the wild is constantly changing. Therefore, the traditional evaluation of malware detection capability of anti-virus software based on a fixed set of samples is not feasible to correctly estimating their ability to detect existing malware in the wild. It is important for anti-virus software to follow the rapid changes in order to maintain its effectiveness. In this study, we propose a new evaluation method of anti-virus software. In the method, we provide the information of non-detected malware to the anti-virus vendors using several means, and evaluate the quickness of their response against them. With the experiment using 11 anti-virus software products, we confirmed a notable difference in the way that anti-virus vendors respond to non-detected malware. The non-detected samples used in the experiment are “confirmed threats”, as they were collected in the wild by our honey pot and indeed have capability of remote exploitation. However some vendors never responded to them in our experiments.

1. はじめに

現在，インターネット上の脅威であるマルウェアに対して，エンドユーザはアンチウイルスソフトウェア（アンチウイルスソフト）を用いて対策を行うことが一般的となっている．従って，エンドユーザが用途に応じて適切なアンチウイルスソフトを選択する指標が必要である．

アンチウイルスソフトの評価は既存研究でいくつかなされている[1,3,4,5,6]．例えば文献[5,6]では事前に定めた検体セットに対するアンチウイルスソフトの検知率評価を行っているが，常に変化し続ける現実のマルウェア集合に対して十分に追随できるかが適切に評価されているとはいえない．先行研究[3,4]では，パッカー等により難読化したマルウェアに対する検知率を調べており，その結果はアンチウイルスソフト毎に大きく異なるという結果が出ている．文献[1]ではwebサーバ用のアンチウイルスソフトのマルウェア検知結果が時間経過とともに変動することが示されている．このようにアンチウイルスソフトの検知率は評価用の検体セットへの依存度が高く，さらにアンチウイルスソフト自体の更新も頻繁に行われることから，固定の検体セットによる特定の状態のアンチウイルスソフトの検知率を調べることでは，当該ソフトの実力を正しく測れない可能性がある．

そこで，本稿では未検知マルウェア情報を様々な方法でアンチウイルスベンダに提示し，当該マルウェアに対する対応の早さという観点でアンチウイルスソフトを評価する手法を提案する．提案手法はアンチウイルスベンダに対して未検知マルウェアの情報を提供する未検知検体情報提供フェーズ（情報提供フェーズ）とその後，検体情報のシグネチャへの反映を確認する検知実験フェーズの 2 つのフェーズからなる．提案手法を用いて 11 種類のアンチウイルスソフトの評価実験を行った．具体的には，情報提供を約 10 日ごとに，検知実験を 1 日ごとに行っていき，未検知検体の検査結果がどのように変化していくかを調査した．その結果，未検知検体に迅速に対応し，シグネチャの更新により当該検体が検知できるようになるアンチウイルスソフトと，実験期間ではどの未検知検体についても全く検知ができないものがあることが確認できた．評価実験で用いた未検知検体は，ハニーポットで捕捉された実マルウェアであり，インターネットに接続していれば誰でも遭遇しうる脅威であるため，この対応の差はアンチウイルスソフトを評価する上で重要といえる．

本稿の構成は次のとおりである．第 2 章では，まず我々が想定するアンチウイルスソフトのモデルを示す．第 3 章で提案手法である未検知マルウェアへの対応に基づくアンチウイルスソフト評価手法について述べ，第 4 章で評価実験について説明する．

[†] 横浜国立大学
Yokohama National University

Vol.2012-DPS-150 No.5
Vol.2012-CSEC-56 No.5
2012/2/29

最後に，第 5 章でまとめとする．

2. アンチウイルスソフト

2.1 アンチウイルスソフトによるマルウェア検知

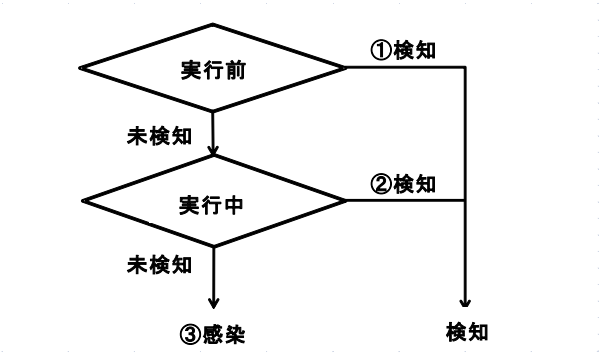

図 1　アンチウイルスソフトのマルウェア検知の流れ

図 1 にアンチウイルスソフトのマルウェア検知の流れを模式的に示す．マルウェア検知はその状況により，以下の 3 種類に分類される．アンチウイルスソフトはマルウェアを早い段階で検知，駆除を行う必要があるので，より数字の若い段階でマルウェアを検知できることが理想的だと考えられる．

① 実行前検査での検知

定期的なディスクスキャンや受信メールへの添付ファイル検査，オンデマンドのファイル検査など，検知対象のマルウェアが実行される以前にマルウェアを検知する．また，いくつかのアンチウイルスソフトでは実行ファイルがダブルクリック等で実行される直前に，仮想環境を用いた動的検査などの詳細な検査が行われる場合がある．この時点で検知した場合は，実行直前にその実行ファイルの実行を強制的に止めるので，マルウェアは実行されていない．

② 実行後検知

マルウェア実行後にマルウェア実行時の悪意のある挙動（レジストリの書き換え，バックドアの作成など）やマルウェアの通信を検知する．この時点での検知では保護対象システムがマルウェアに感染した後に検知している．

③ 感染

アンチウイルスソフトはマルウェアを検知できず，保護対象システムがマルウェアに感染する．

2.2 ベンダによるマルウェア情報収集とアンチウイルスソフトの更新

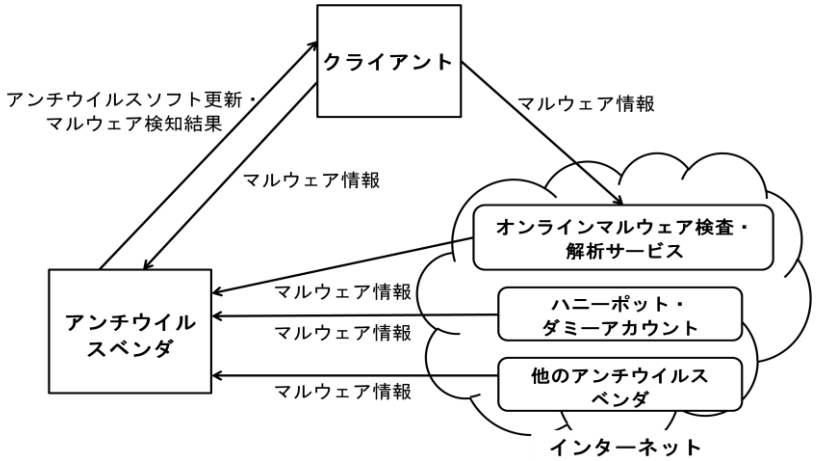

図 2　ベンダによるマルウェア情報収集の全体図

アンチウイルスソフトによる情報収集の全体図を図 2 に示す．アンチウイルスベンダは少なくとも 4 種類の方法でマルウェア情報を収集していると考えられる．一つ目はハニーポットやダミーメールアカウントを使用してインターネット上を流通するマルウェアを収集する方法である．2 つ目はアンチウイルスソフトのクライアントからの情報提供である．アンチウイルスソフトがインストールされたクライアント環境でマルウェアの疑いのあるファイルが検知された場合，そのインシデントに関する情報をベンダに送信する場合がある．特に近年はクラウド型のサービスも提供されており[15,16]，クライアントからの情報を集約し，対策に役立てている．また，多くのアンチウイルスベンダにはマルウェア情報投稿フォームが用意されており，誤検知や検知漏れに関する情報やマルウェア検体を投稿することが可能となっている．3 つ目の方法は，オンラインマルウェア検査やマルウェア解析サービスに投稿されたマルウェア情報の提供を受けることが考えられる．オンラインマルウェア検査，解析サービス[8,9,10,11,12]とは実行ファイルや URL 等をオンラインで受け付け，各種アンチウイルスソフトでの検査や解析を行い，検査結果を投稿者に提供するサービスである．例えば VirusTotal [8]では投稿されたファイルを 40 種類以上のアンチウイルスで検査した結果を投稿者に提供している．サービス提供側にはユーザから投稿された検体が蓄積され，これらの情報はアンチウイルスベンダに提供される場合がある．4 つ目の方法は，他のアンチウイルスベンダからの情報提供が考えられる．

Vol.2012-DPS-150 No.5
Vol.2012-CSEC-56 No.5
2012/2/29

上記のように様々な方法で収集されたマルウェア情報を元にアンチウイルスソフトの更新を行っていると考えられる．また，クラウド型のサービスの場合，ベンダ側でマルウェア検知処理を実施し，その結果をクライアントに提供する状況が考えられる．

2.3 アンチウイルスソフトの評価とその問題点

文献[5]では，20社のアンチウイルスソフトが対象となっており，ウイルス・ワーム・トロイの木馬・バックドア・ボットなどを含む合計1,562,092種の検体による検出テストを行っている．検体は，ハニーポット，各ウイルスベンダなどから収集している．結果は，検知率が一番低いもので約85%，一番高いものでは，ほぼ100%となっている．一方，文献[6]では92体のゼロデイマルウェアを用いた検知率の調査,検査日から2~3ヶ月以内に収集された216,640体のマルウェアを用いた検知率の調査，AV-TEST [13]の調査により広く拡散している思われる5,000体のマルウェア用いた検知率の調査の3種類の評価が21種類のアンチウイルスソフトに対して行われている．一部のアンチウイルスソフトを除いて多くのアンチウイルスソフトが上記の既存の評価において85%以上の検知率を示している。

上記のように固定の検体セットを用いたアンチウイルスソフトの評価では，多くのアンチウイルスソフトが高い検知率を示している．しかし，現在マルウェアの種類数は増加を続けており，実効性のあるマルウェア対策を行うためには，変化し続けるマルウェア群に対して適切に対応することが重要といえる．また， 先行研究[3,4]では、難読化したマルウェアに対する検知率は10%以下のものから80%以上のものまで幅広く，それ以前の評価とは異なる結果となっている．さらに，文献[1]では web サーバ用のアンチウイルスソフトのマルウェア検知性能のある時点での検知結果とその 1 月後の検知性能の比較が行われ，アンチウイルスソフト毎にマルウェアの検知結果の変化に差が生じるという結果も出ている．このようにアンチウイルスソフトの検知率は評価用の検体セットへの依存度が高く，さらにアンチウイルスソフト自体の更新も頻繁に行われることから，固定の検体セットによる特定の状態のアンチウイルスソフトの検知率を調べることでは，当該ソフトの実力を正しく測れない可能性がある．

3. 未検知マルウェアへの対応に基づくアンチウイルスソフトの評価手法

提案手法はアンチウイルスが評価対象検体を検知できるかどうかを確認するための検知実験フェーズと，アンチウイルスベンダに対して未検知マルウェアの情報を提供する情報提供フェーズからなる．まずハニーポット等により用意した検体セットに対して検知実験フェーズにより，未検知検体を特定後，後述のルールに従い評価に用いる検体を選択する．次に情報提供フェーズでアンチウイルスベンダに未検知検体の情報を提供する. なお, 評価実験では約 10 日ごとに情報提供を行った. 情報提供終了後，アンチウイルスベンダの対応を確認するために検知実験フェーズを再度実施する．評価実験では，1 日ごとに検知可否を確認した．以下，各フェーズの詳細について説明する．

3.1 検知実験フェーズ

検知実験フェーズでは評価用検体をアンチウイルスソフトで検査することにより検知の可否を確認する．なお，検知実験フェーズの目的は，未検知検体の検知可否の確認であり，検体の情報提供ではないため，評価対象のアンチウイルスソフトを検査時点での最新状態に更新した後，実験環境のインターネット接続を切断した上で，検知実験を行う．これによって，検知実験時に未検知検体情報がベンダに送信されることを防ぐ．また，評価実験では，マルウェア検体を扱うので安全面を考慮し，検査は仮想マシン上で行った．

3.2 未検知検体情報提供フェーズ

情報提供フェーズでは,未検知検体を 3 つに分け下記の 3 種類の方法でアンチウイルスベンダに対してマルウェア検体情報を送信する．

① クライアント環境からの情報送信

アンチウイルスソフトがインストールされたクライアント環境でマルウェアが検知された場合にその情報がベンダに送信されるようになっている場合がある．本稿では，仮想環境上で未検知マルウェア検体を実行し，実行時の挙動を情報として提供する．また，実際にマルウェアを動作させるので，感染ホストから外部に攻撃が行われる可能性を考慮し，専用の実行環境を用いることで外部への攻撃通信等は防ぎながら，アンチウイルスベンダに対して情報の提供を行う．専用の実行環境については 3.4 節で詳しく説明する．

② オンラインマルウェア検査サービスへの投稿

アンチウイルスベンダがオンラインマルウェア検査サービスからマルウェアの情報を取得している場合を想定し，オンラインマルウェア検査サービスにマルウェアを投稿することでアンチウイルスベンダに対して間接的にマルウェア情報を提供する．今回の評価実験では，VirusTotal に対して検体を投稿した．

③ マルウェア検体情報投稿フォームを用いた投稿

2.2 節で述べたマルウェア検体情報投稿フォームを用いて，未検知検体を投稿することでアンチウイルスベンダに対して情報を提供する．

3.3 評価用検体収集方法及び未検知検体の選別方法

評価用検体の収集方法として，既存のマルウェアに対してパッカーなどを用いて暗号化，圧縮するなどして新しいマルウェアを作成する方法が考えられる．しかし，提

Vol.2012-DPS-150 No.5
Vol.2012-CSEC-56 No.5
2012/2/29

案手法で使用するマルウェアの情報は実際にアンチウイルスベンダに提供されるため，評価のためとはいえ，実インターネット上に存在しないマルウェア検体を生成することは，アンチウイルスベンダの業務に支障を与える可能性がある点で望ましくない．よって，我々の評価実験では，インターネット上を流通する実マルウェアを使用する．具体的にはハニーポットを用いて収集した検体を使用する．しかし，このようにして収集した実マルウェア検体の中には実行可能ファイルとして不完全なものなどが含まれる．特にハニーポットを検知した攻撃者は，無効なダミーファイル等を送信してくる場合があるため，注意が必要である．従って，実験に用いる検体が実際にマルウェアとしての機能をもっており，検知すべき対象であるかを事前に確認する必要がある．確認の方法としては，検体を詳細に解析し悪意のある動作を示すかを確認することが理想的であるが，今回の実験では簡単のため以下のように未検知検体の選定を行った．

① ハニーポットで取得した検体のうち，評価対象の 11 種類のアンチウイルスソフトで検査を行い，あるアンチウイルスソフト S で検知されないにも関わらず S 以外の 2 種類以上のアンチウイルスソフトに検知される検体を，S に対する評価用検体候補とする．
② ①の候補検体群の中から PE ファイルの構造をもつ検体を選定する
③ ②の検体を実験環境上で実行し，実行エラーが出ない検体を未検知検体とする

3.4 未検知検体情報提供用環境

未検知検体情報提供用環境とは，アンチウイルスソフトをインストールした仮想マシンであり，この上でマルウェアを実行することで，アンチウイルスソフトにその挙動を観測させ，アンチウイルスベンダへの情報提供を促すための環境である．

マルウェア検体情報提供用環境の概要図を図3に示す．実線の矢印はマルウェア及びアンチウイルスソフトの通信を示し，破線の矢印はシステム制御のための通信を示す．実装環境は以下の4つの構成要素からなる．

● 犠牲ホスト

犠牲ホストには評価対象のアンチウイルスソフトがインストールされており，未検知検体を実行し，アンチウイルスソフトにその挙動を観測させ，情報提供を促す．

● アクセスコントローラ

アクセスコントローラは犠牲ホストにおいて実行されたマルウェアからの通信を疑似インターネット内の疑似サーバに適切に転送する役割を持つ．なお転送設定は設定情報に基づき解析マネージャによって設定される．本稿では，DNS名前解決のための通信を実インターネットへと転送した．また，アンチウイルスソフトがマルウェア情報送信のために行う通信については実インターネットへの接続を許可する設定とした．

● 疑似インターネット

疑似インターネットは，HTTPやSMTPなどのサービスを提供するいくつかの疑似サーバから構成され，マルウェアに対してネットワークサービスを提供する．この際，マルウェアからの特定のアクセスについては設定情報に基づきサーバ応答が返される．またマルウェアの攻撃対象として，疑似インターネット内に脆弱なホストとしてハニーポットを用意することで，マルウェアの攻撃の実行を促す．

● マネージャ

マネージャは，犠牲ホストのOSイメージ管理，マルウェア管理，アクセスコントローラの設定，疑似インターネットの設定などシステムの中核として働く．

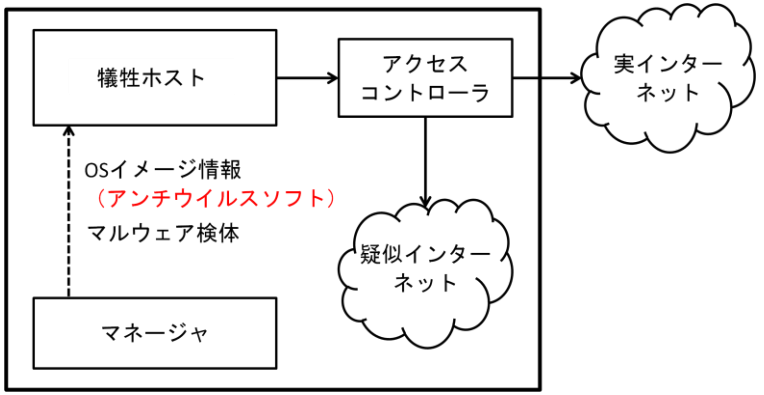

図 3 未検知検体情報投稿用環境の概要

4. 評価実験

4.1 実験方法

ある観測地点に設置した低対話型ハニーポット（Nepenthes[2]）で 2010 年 7 月までに収集されたマルウェア検体及び別の観測地点に設置した低対話型ハニーポット（Nepenthes 及び Dionaea[7]）で 2011 年 4 月~10 月の間に収集されたハッシュ値の異なるマルウェア検体計 9753 検体に対して 3.3 節の方法で未検知検体の選別を行い，提案手法を用いて 11 種のアンチウイルスソフト（AV1~AV11）の評価を行った． AV1~AV9 の実験期間は 2011/12/26～2011/1/26 の間となっており，情報提供フェーズは 2011/12/26, 2012/1/06，2012/1/16 に行った．また，AV10，AV11 の実験期間は 2012/1/06~2012/1/26 の間となっており，情報提供フェーズは 2012/1/06，2012/1/16 に行った．なお，AV4，AV6，AV11 に関してはマルウェア情報投稿フォームが存在しなかったので，マルウェア情報投稿フォームを用いた情報提供は行っていない．

Vol.2012-DPS-150 No.5
Vol.2012-CSEC-56 No.5
2012/2/29

4.2 実験結果

● 未検知検体選別

3.3 節のルールに従い検体を選別した結果を表 1 に示す．まず，収集した評価用検体のうち 3.3 節の①の条件を満たす評価用検体候補は 1791 体だった．その中で，②の条件である PE ファイルの構造をもつ検体は 1743 体だった．そして，この 1743 体のうち,③の条件を満たす,エラーを起こさずに実行可能な検体は 1468 体だった.次に、選別後の各アンチウイルスソフト用の検体数及び各情報提供方法別に使用した検体数を表 2 に示す．例えば、AV1 については，評価用検体は全部で 85 体あり，そのうち，25 体をクライアント環境からの情報提供に, 30 体を VirusTotal に, 残りの 30 検体を，投稿フォームを通じて提供した．なお，情報提供は，毎回全ての検体群に対して行うこととし，これを 2 回から 3 回繰り返した．

参考として選別後の検体を Symantec[14]で検査した際の科名を表 3 に示す.

表 1　未検知検体選別結果

総検体数	9,753
AV ソフトに検知されない検体数	1,791
PE フォーマットの検体数	1,743
実行可能な検体数	1,468

表 2　各アンチウイルスソフトの選別後の検体数及び情報提供に使用した検体数

	総検体数	クライアント環境	VirusTotal	フォーム投稿
AV1	85	25	30	30
AV2	118	38	40	40
AV3	247	80	87	80
AV4	816	100	716	フォーム存在せず
AV5	180	60	60	60
AV6	513	100	413	フォーム存在せず
AV7	155	50	53	50
AV8	359	100	125	124
AV9	333	100	118	115
AV10	30	10	10	10
AV11	18	9	9	フォーム存在せず

表 3 Symantec での科名

検体名	検体数	検体名	検体数
Adware.CPush	3	W32.Gobot.A	2
Adware.Istbar	2	W32.HLLW.Deadhat	2
Adware.Purityscan	21	W32.HLLW.Gaobot	1
Backdoor.Graybird	23	W32.Ifbo.A	5
Backdoor.IRC.Bot	3	W32.IRCBot	37
Backdoor.Pcclient	28	W32.IRCBot.Gen	22
Backdoor.Sdbot	4	W32.Korgo.G	2
Backdoor.Trojan	30	W32.Korgo.P	5
Bloodhound.W32.1	1	W32.Korgo.Q	7
Downloader	3	W32.Korgo.R	3
Hacktool	184	W32.Korgo.S	61
IRC.Backdoor.Trojan	1	W32.Korgo.V	17
IRCTrojan	1	W32.Korgo.W	5
Linux.Backdoor.Kaiten	5	W32.Korgo.X	20
Packed.Generic.333	1	W32.Korgo.Z	8
Packed.Generic.335	1	W32.Mixor.Q@mm	2
Packed.Generic.342	6	W32.Poxdar	1
Packed.Generic.52	3	W32.Protoride.Worm	1
Packed.Mystic!gen4	1	W32.Rinbot.V	1
Suspicious.Bifrose	1	W32.Sasser.D	4
Suspicious.Cloud.2	12	W32.Spybot.Worm	67
Suspicious.Cloud.7.F	2	W32.Virut!gen	1
Suspicious.IRCBot	68	W32.Virut.B	4
Suspicious.MH690.A	29	W32.Virut.CF	1
Trojan.Adclicker	1	W32.Virut.U	4
Trojan.Dropper	2	W32.Virut.W	2
Trojan.Gen	43	WS.Trojan.G	2
Trojan.Gen.2	11	WS.Trojan.H	195
TrojanHorse	114		

Vol.2012-DPS-150 No.5
Vol.2012-CSEC-56 No.5
2012/2/29

● 評価実験結果

評価実験の結果を図 4~図 7 に示す．図 4~図 7 は情報提供フェーズを行った日から 10 日，20 日，30 日の間に検知されるようになった検体の割合(検知可能検体数/提供検体総数)を情報提供方法別に表している．以降ではこの割合を単に検知率と呼ぶ．1 回目の情報提供後，AV1, AV2, AV3, AV6, AV7, AV8, AV11 において検知率が増加した．そのうち，AV3, AV6, AV7 に関しては 2 回目の情報提供後にも検知率が増加した．特に AV3 は 2 回目の情報提供フェーズ後に大きく検知率が増加した．3 回目の情報提供後は，全ての AV について検知率に変化は見られなかった．また，AV8 はマルウェア検体情報投稿フォームに投稿を行った検体のみ検知可能となり，AV11 はクライアント環境からの情報提供を行った検体のみ検知可能となった．このように，情報提供された未検知検体に対する対応は各ベンダによって大きく異なることが分かった．また，どのベンダも提供された未検知検体全てに対応するわけではないことが分かった．さらに，ベンダによっては，特定の情報提供方法にのみ対応することが確認できた．

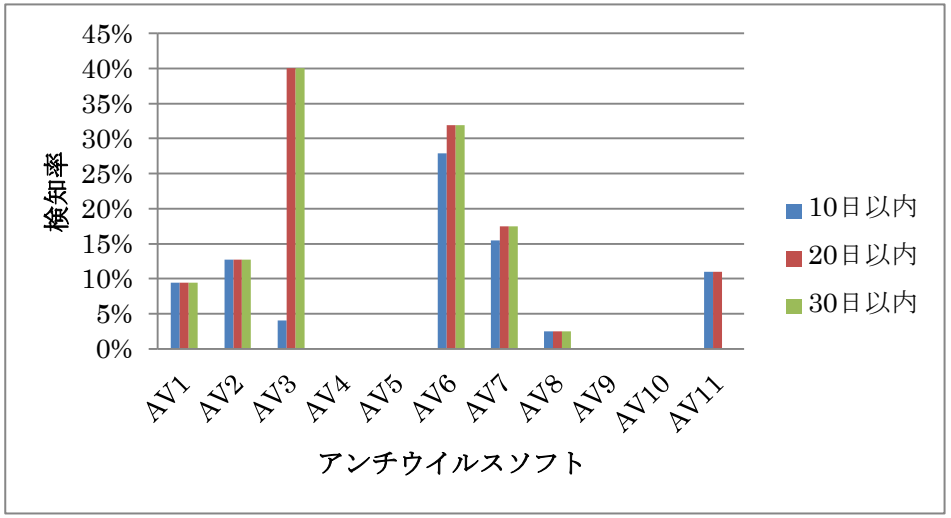

図 4　未検知検体全体の情報提供後の検知率

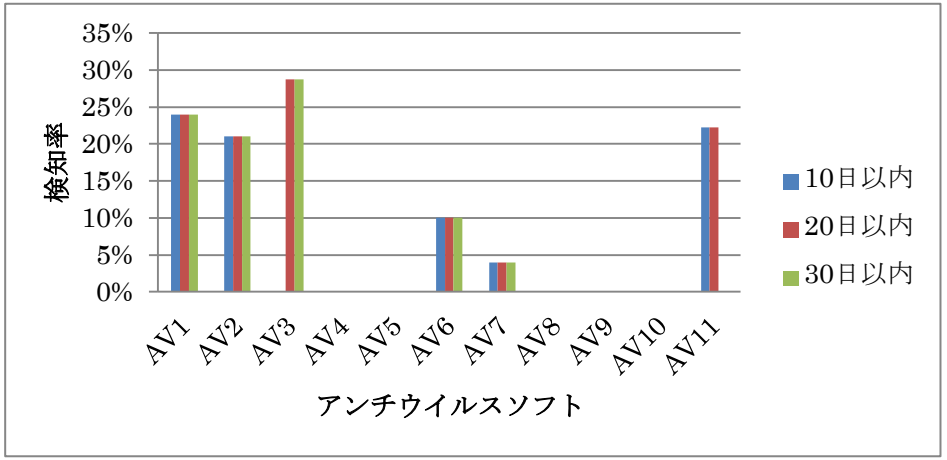

図 5　クライアント環境からの情報送信を行った未検知検体の情報提供後の検知率

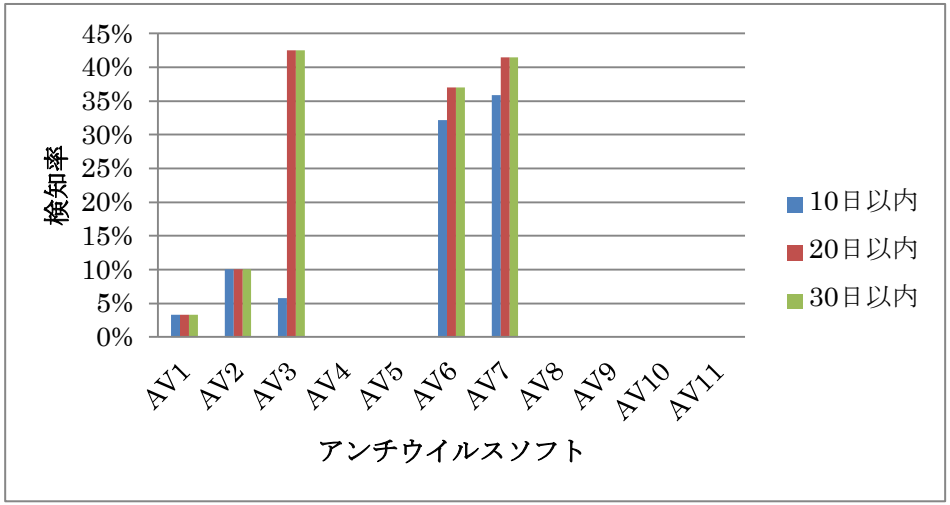

図 6　VirusTotal に投稿を行った未検知検体の情報提供後の検知率

Vol.2012-DPS-150 No.5
Vol.2012-CSEC-56 No.5
2012/2/29

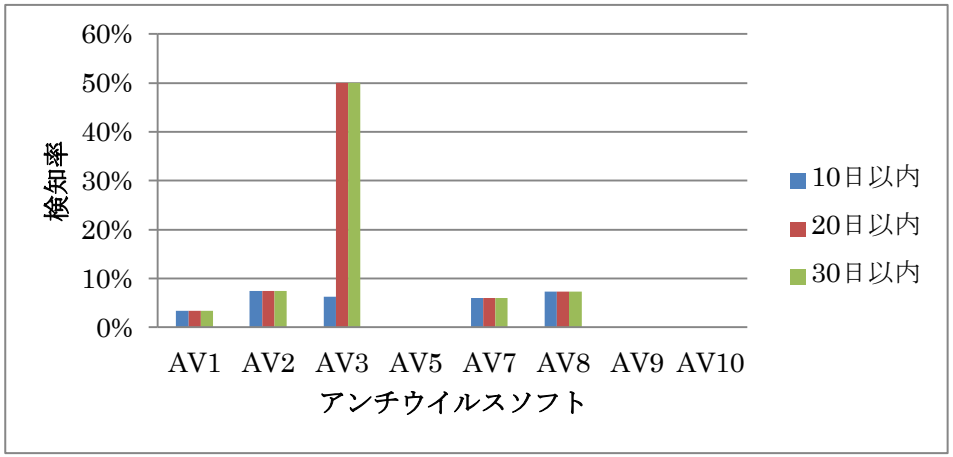

図 7　情報投稿フォームにより情報提供を行った未検知検体の情報提供後の検知率

5. 考察

5.1 マルウェア検体の取得時期について

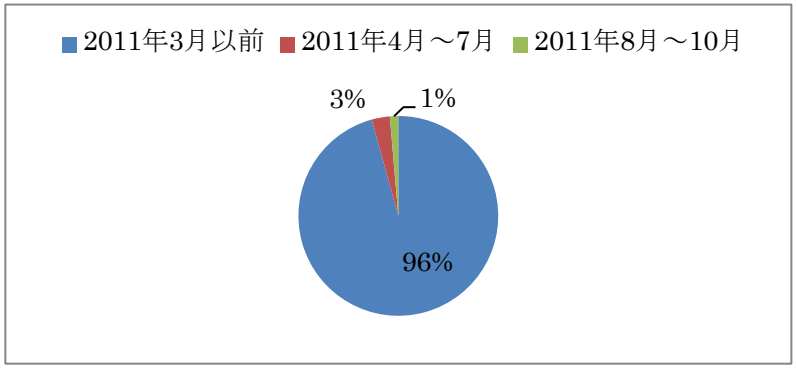

図 8　未検知検体のハニーポットでの取得時期

図 8 に 4 章の評価実験で用いた 1,468 体の未検知検体の，ハニーポットでの入手時期を示す. 図 8 より未検知検体の多くは 2011 年 4 月以前にハニーポットで収集された検体であることが分かる．これより，未検知検体は 10 か月以上も未検知のまま対応がなされていない実マルウェアであり，今回の情報提供にベンダが対応をしたことにより検知が可能となった可能性が高いことを示す.

5.2 情報提供により検知できるようになった検体の傾向

情報提供により検知が可能となった検体のハニーポットでの入手時期を図 9 にまとめる．5.1 節で述べたとおり，未検知検体の 96%が 2011 年 3 月以前に収集された検体だったため，ベンダが対応した検体もほとんどが 2011 年 3 月以前に収集された検体だったが，AV2 に関してはほとんどが 2011 年 4 月以降に収集された比較的新しい検体となっており，傾向が大きく異なっている．このことから，AV2 は何らかの方法で検体の新旧を判断し，新しい検体に優先的に対応している可能性があるが，その具体的な方法は不明であり，さらなる調査が必要である.

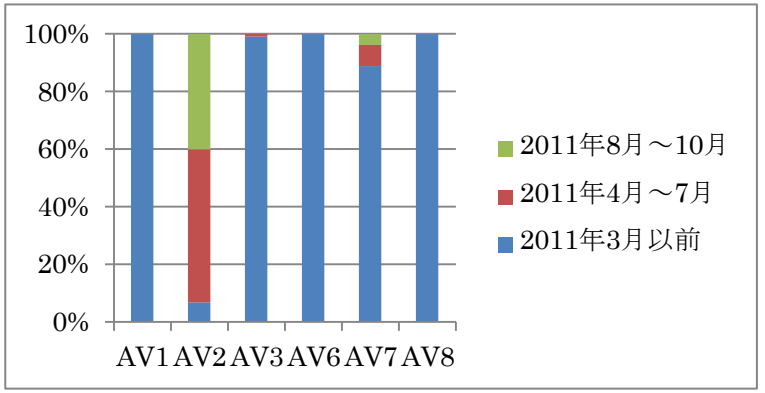

図 9　情報提供により検知されるようになった検体のハニーポットでの取得時期

6. まとめと今後の課題

本稿では，固定の検体セットに基づく従来のアンチウイルスソフトの検知率評価の問題点について述べ，日々変化を続けるマルウェアへの対応を評価するために，未検知マルウェア情報を様々な方法でアンチウイルスベンダに提示し，当該マルウェアに対する対応が迅速に行われるか否かという観点でアンチウイルスソフトを評価する手法を提案した. 提案手法を用いて 11 種類のアンチウイルスソフトの評価実験を行ったところ，その対応には各社で大きな差が見られることがわかった．評価実験で用いた未検知検体は，ハニーポットで捕捉された実マルウェアであり，インターネットに接続していれば誰でも遭遇しうる脅威であるため，この対応の差はアンチウイルスソフ

トを評価する上で重要といえる．

本研究の課題としてはまず検体取得方法が挙げられる．実験時はサーバ型の低対話型ハニーポットのみを用いて検体収集を行ったが，ハニーポットにはクライアント型や高対話型があるので，それらのハニーポットも併用した方がより多くの検体を収集可能である．また，今回の評価実験では，ハニーポットで収集した検体のうち，実行可能な検体を未検知検体とすることで選別を行ったが，このルールでは選別後の検体が確実にマルウェアであるとは言えない．検体選別の際は，各検体を詳細に解析し悪意のある動作を示すかを確認することが理想的である．

また，今回はアンチウイルスベンダ間の情報共有については評価対象にしていないが，あるベンダに提供した未検知検体の情報が他のベンダの検知結果にどのように影響するかを調べることも可能であるが，その具体的な方法や評価基準については今後の課題としたい．

謝辞 本研究の一部は，平成 23 年度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／サイバー攻撃情報とマルウェア実体の突合分析技術／類似判定に関する研究開発により行われた．

参考文献

1) 谷本直人,八木毅,針生剛男,伊藤光恭,“Web サイトへのマルウェア感染攻撃に関する実態調査”，コンピュータセキュリティシンポジウム 2010 Web セキュリティ(2) (CSS2010), 2010.
2) P. Baecher, M. Koetter, T. Holz, M. Dornseif, and F. C. Freiling, “The Nepenthes Platform: An Efficient Approach to Collect Malware,” 9th International Symposium on Recent Advances in Intrusion Detection (RAID 2006), pp.165-184, 2006.
3) Jon Oberheide, Michael Bailey, Farnam Jahanian,” PolyPack: An Automated Online Packing Service for Optimal Antivirus Evasion” Proceedings of the 3rd USENIX conference on Offensive technologies (USENIX WOOT2009), 2009.
4) Maik Morgenstern, Tom Brosch, “Runtime Packers : The Hidden Problem?,” Black Hat USA 2006, 2006.
https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Morgenstern.pdf,
Last Visit: 2012/01/30
5) AV-Comparatives On-Demand Comparative,
http://www.av-comparatives.org/images/stories/test/ondret/avc_retro_nov2011.pdf, Last Visit: 2012/01/30
6) AV-Test Nov/Dec 2011 - 23 home user and 8 corporate products – Windows 7,
http://www.av-test.org/en/tests/test-reports/novdec-2011/, Last Visit: 2012/01/30
7) Dionaea, http://dionaea.carnivore.it/, Last Visit: 2012/01/30
8) Virustotal, http://www.virustotal.com/flash/index_en.html, Last Visit: 2012/01/30
9) VirSCAN.org, http://www.virscan.org/, Last Visit: 2012/01/30
10) JOTTI, http://virusscan.jotti.org/de/, Last Visit: 2012/01/30
11) No Virus Thanks, http://scanner.novirusthanks.org/index.php Last Visit: 2012/01/30
12) FilterBit beta, http://filterbit.com/index.cgi, Last Visit: 2012/01/30
13) AV-Test, http://www.av-test.org/, Last Visit: 2012/01/30
14) Symantec, http://www.symantec.com/ja/jp/, Last Visit: 2012/01/30
15) gred アンチウイルス アクセラレータ, http://www.gredavx.jp/,
Last Visit: 2012/01/30
16) Panda Cloud Antivirus,
http://www.cloudantivirus.com/en/, Last Visit: 2012/01/30