特集
マルウェア

マルウェアと戦う技術

「Web からの脅威」とマルウェア検出・防御技術

小松優介（トレンドマイクロ（株））

脅威の傾向変化と Web からの脅威

●攻撃者の目的の変化

攻撃者によるマルウェアの作成目的が変化して久しいといわれている．この変化とは，自身の技術力の誇示，いたずらから，換金性の高い個人情報等の詐取への切り替えである．

作成目的の変化に伴い，マルウェアの侵入方法，活動方法の傾向も変化してきている．過去（1998 年から 2004 年頃）のマルウェアは，アウトブレーク（大規模感染）型と呼ばれている．マスメーリング☆1 や OS の脆弱性を悪用して，マルウェアが自身のコピーをネットワーク経由で頒布する感染活動を行い，感染被害を拡大させるものが多かった．不特定多数のユーザを対象に攻撃が行われ，地域を問わず，世界中でアウトブレークを引き起こす傾向にあった．

これに対して，現在（2005 年以降）のマルウェアは，標的型，シーケンシャル型と呼ばれている．特定の地域，組織，コミュニティ等を攻撃対象とし（標的型），複数のマルウェアを順次送り込むことにより（シーケンシャル型），情報の詐取をはじめとした犯罪行為を行う．マルウェアを順次送り込む手段として使用されるのが，Web サイト（HTTP 通信）である．インターネットに接続された PC が，一度マルウェアに感染すると，そのマルウェアが新たなマルウェアを呼び込むため，攻撃活動も複雑となり，感染状態から抜け出すことが困難となる．また，マルウェア作成ツールをはじめとする各種攻撃ツールのインターネット上での流通に伴い，マルウェアの絶対数が大幅に増加してきている．

図 -1 は，ドイツのマルウェア調査機関「AV-Test.org[1)]」が集計したマルウェア種別数の推移である．1985 年にわずか 564 種類だったマルウェアが，2006 年には，972,606 種類．さらに，2007 年には，5,490,960 種類に増加している．2007 年のマルウェア種別数を 2006 年と比較すると，実に 5.65 倍に増加している．

☆1 マルウェアを添付した電子メールを大量頒布して，大規模感染につなげる手段．

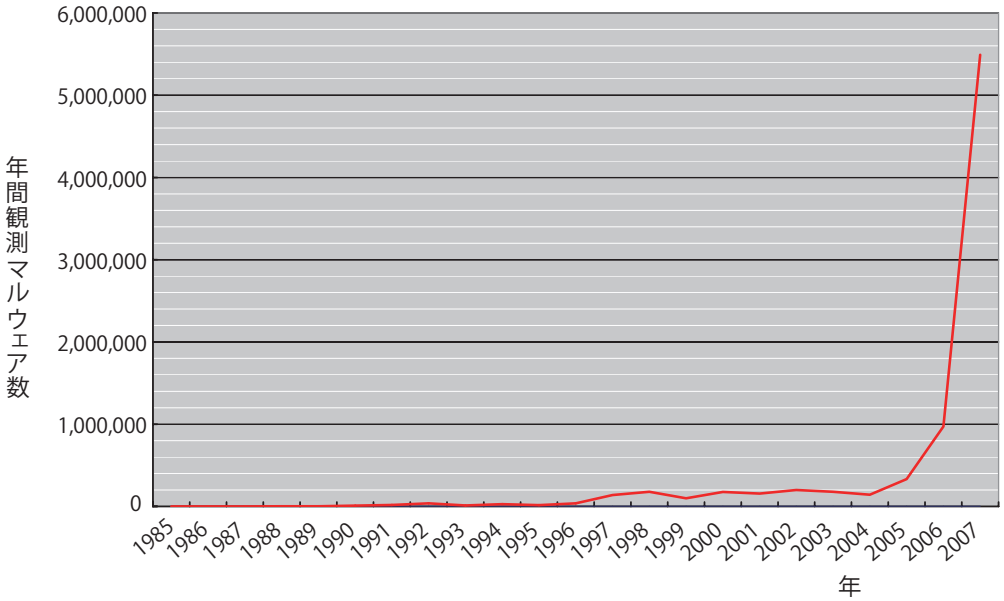

図 -1　マルウェア種別数の推移（AV-Test.org）

過去のマルウェアの特徴

図 -2 は，1999 年に流行したマルウェア WORM_SKA.A[2] に感染した際の，PC 上に表示される画面である．

WORM_SKA.A（別名 Happy99）は，電子メールの添付ファイルとしてユーザに届く．ユーザが添付ファイル Happy99.exe を実行すると，PC のデスクトップ上に，“Happy New Year 1999!” というメッセージと花火の打ち上げ画像が表示される．WORM_SKA.A は，Windows のシステムファイル WSOCK32.DLL を改変し，ユーザの電子メール送信とニュースグループへの投稿動作を監視する．これらの動作を確認すると，もう一通同じ宛先に同じ件名で電子メールやニュース記事に Happy99.exe ファイルを添付して送信する．

知り合いから届く電子メールにマルウェアが添付されていたことから，実行してしまうユーザが多く，感染被害が拡大した．

WORM_SKA.A の侵入方法，活動内容をまとめると次のようになる．

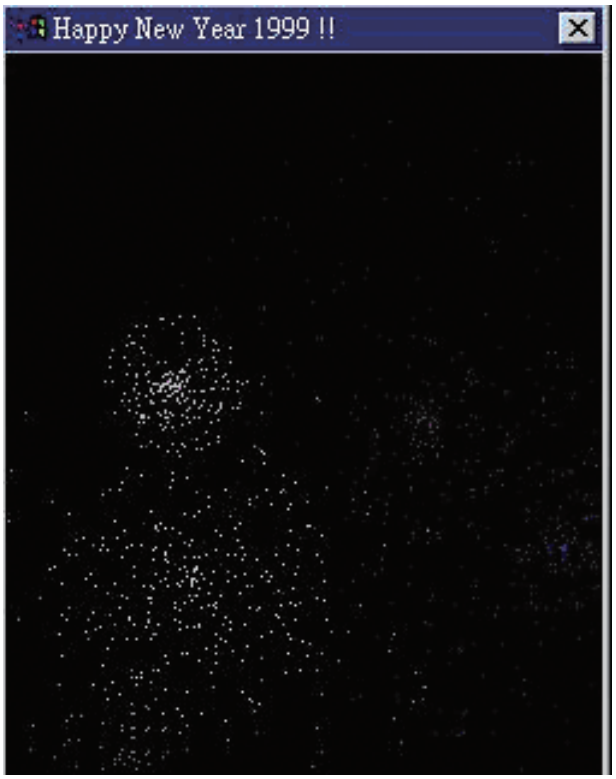

図 -2　WORM_SKA が表示する画面

侵入方法

- 電子メールの添付ファイル

活動内容

- デスクトップ上に画像およびメッセージを表示
- システム改変（WSOCK32.DLL を書き換え）
- ワーム活動（自身のコピーを頒布）

電子メールを介して侵入したマルウェアが，いたずらメッセージを表示し，自身のコピーを外部にばら撒く．PC が感染することにより，システムファイルの改変，知人へのマルウェア送信が発生するものの，いたずらメッセージの表示自体は，さほど大きな問題に入らないかもしれない．また，WORM_SKA.A は単体活動型☆2 のマルウェアであり，アンチウイルスソフトでの検出・削除が容易であった．

現在のマルウェアの特徴

現在（2005 年以降）のマルウェアによる攻撃はどのようなものであろうか．

図 -3 は，2009 年 5 月頃より，感染被害報告数が急増している，ホームページ誘導感染型マルウェア，通称 Gumblar 攻撃の流れである．

Gumblar 攻撃では，改ざんした正規 Web サイトを利用したマルウェア配布サイト（以降，攻撃サイト）への誘導，アプリケーションの脆弱性を悪用したマルウェア実行を通して，最終目的である FTP アカウント情報の詐取を行う．

攻撃の流れについて順を追って見ていきたい．

(1) 攻撃者：正規 Web サイトが提供するホームページに攻撃サイトへ誘導する Java スクリプトを埋め込む．
(2) ユーザ：改ざんされた正規 Web サイト（以降，誘導元サイト）にアクセスをする．Web サイトはいつも利用しているサイトであるため，ユーザは不正活動に巻き込まれていることを意識しにくい．
(3) ブラウザ：誘導元サイト内に埋め込まれた Java スクリプト（検出名：JS_AGENT）によって，攻撃サイトに誘導される．
(4) ブラウザ：アクセスした攻撃サイトからマルウェア（検出名：TROJ_PIDIEF）をダウンロードする．
(5) ブラウザ：PC に，Adobe Reader および Adobe Acrobat の脆弱性が存在する場合，この脆弱性を利用されダウンロードした TROJ_PIDIEF 自身を実行されてしまう．結果として PC は感染してしまうことになる．
(6) マルウェア（TROJ_PIDIEF）：新たなマルウェアを呼び込むため攻撃サイトにアクセスし，順次マルウェア（検出名：TROJ_SEEKWEL）をダウンロードし実行する．
(7) マルウェア（TROJ_SEEKWEL）：FTP アカウント情報を詐取する．

☆2 感染などの攻撃活動にかかわるマルウェアは 1 つの実行ファイル Happy99.exe のみである．

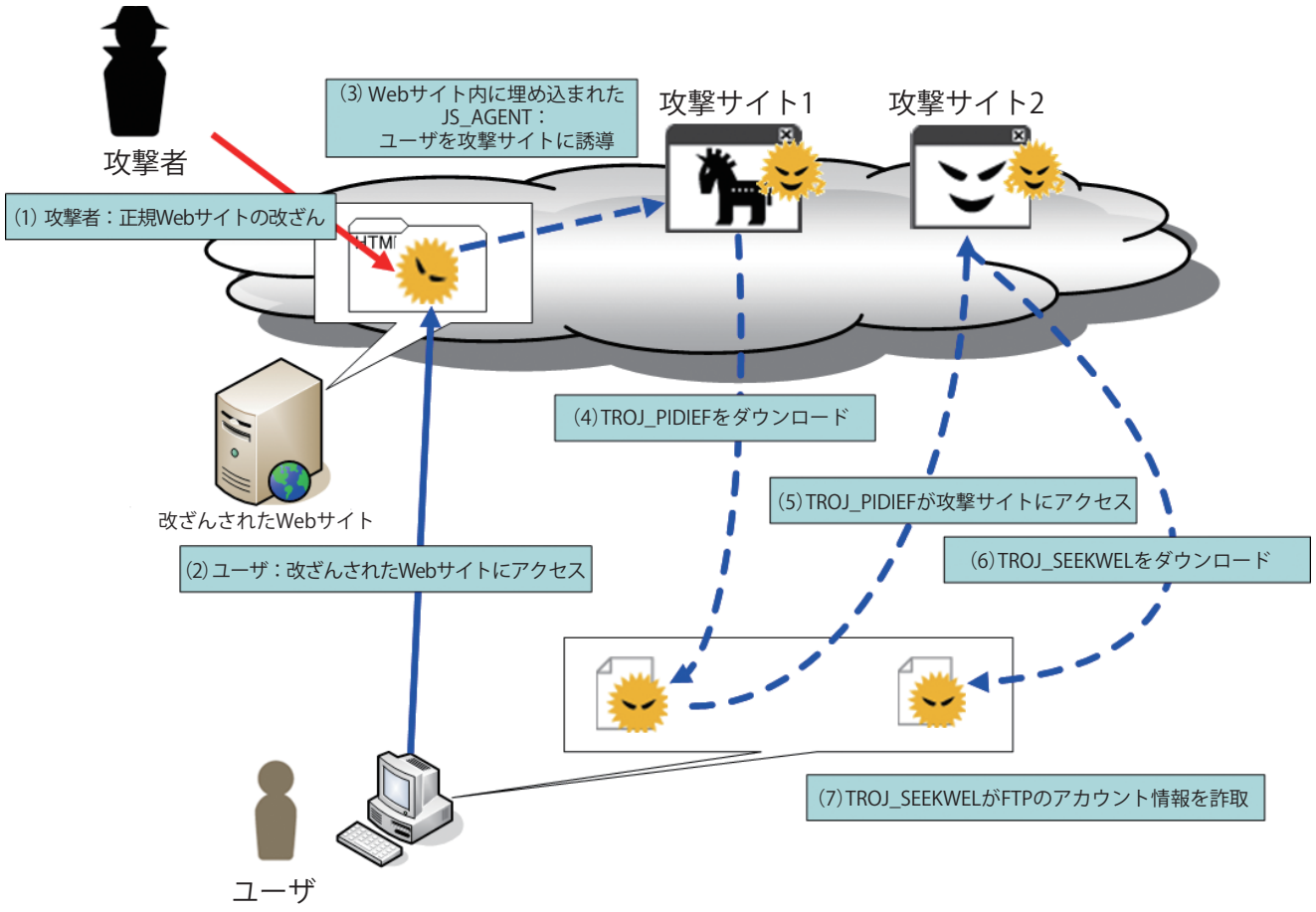

図 -3　Gumblar 攻撃の流れ

Gumblar 攻撃の侵入方法，活動内容をまとめると次のようになる．

侵入方法

- Web サイト経由

活動内容

- JS_AGENT を用いた攻撃サイトへの誘導
- アプリケーションの脆弱性を悪用した TROJ_PIDIEF 自身の自動実行と，新たなマルウェアを順次ダウンロードするための攻撃サイトへのアクセス
- TROJ_SEEKWEL による FTP アカウント情報の搾取

単体活動型の過去のマルウェア WORM_SKA.A と比較すると，複数のマルウェアが攻撃に介在し，最終的な目的である情報の詐取（FTP アカウント情報の搾取）が実施されていることが大きく異なる．また，これら一連の攻撃活動に Web サイトが介在していることと，複数の攻撃がつながり（連続性）をもって行われていることに注目したい．

Web からの脅威

現在の攻撃の主流となっている Web サイトを悪用する手法は「Web からの脅威」と呼ぶことができる．「Web からの脅威」では，起点となるマルウェアが PC に侵入した後，順次新たなマルウェアを呼び込むため，連続的なマルウェアのダウンロードを開始する．図 -4 は「Web からの脅威」の攻撃手法である．攻撃手法の特徴をまとめると次のようになる．

- 起点となるマルウェアの侵入方法は，電子メールに記載された攻撃サイトへの URL，USB メモリの自動実行，脆弱性を悪用する攻撃コードの埋め込まれた文書ファイル，攻撃サイトへ誘導するサイトなど，さまざまである．
- 起点となるマルウェアに PC が感染すると，攻撃サイト経由で複数の新たなマルウェアを順次ダウンロードし，連続的な感染被害が複数発生することになる．このため，駆除およびシステムの復旧が困難になる傾向が高い．
- 攻撃に使用されるマルウェア群は，アウトブレーク型のような表面的に活動が見え，派手な動作を行わない

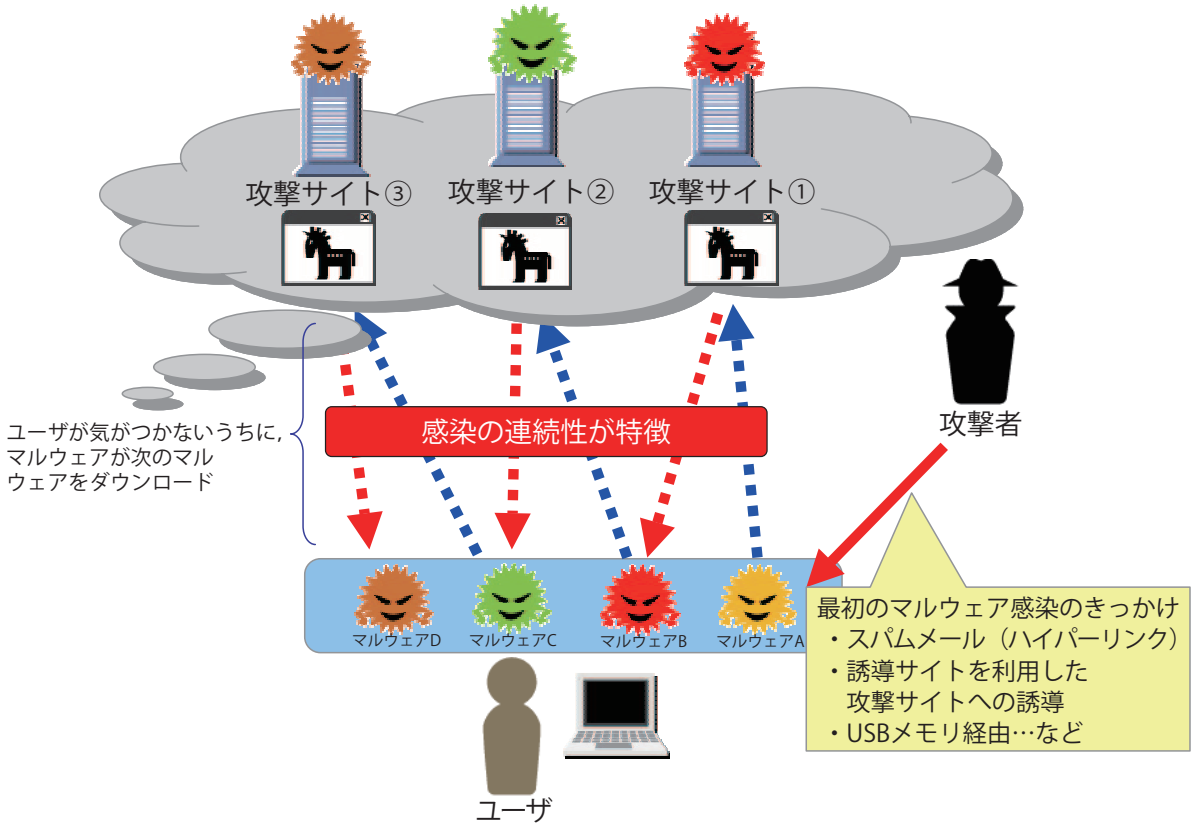

図 -4　「Web からの脅威」の攻撃手法

ので，ユーザは感染に気がつきにくい．

- 攻撃サイト上のマルウェアは，アンチウイルスソフトに検知されないよう，常に更新され続けている．このため，あるタイミングでシグネチャを用いた検出ができたとしても，次のタイミングでダウンロードされるファイルは，未知のマルウェアとなっている可能性がある．これは，常に新たな未知のマルウェアに感染している状態を作り出すことができることを意味する．

一度「Web からの脅威」によるマルウェア感染の連鎖の輪に巻き込まれて，感染状態に陥ってしまうと，その連鎖の輪から抜け出すのが困難となる．マルウェア作成の目的が変化したことに伴い，このように攻撃の手法も大きく変化してきた．

次に，攻撃からユーザ環境を保護するための既存の技術および，現在の脅威である「Web からの脅威」に対抗するための新たな対策技術について見ていきたい．

マルウェアを検出するための技術

●パターンマッチング方式

アンチウイルスソフトが持つ，マルウェアを検出するための仕組みとして，パターンマッチング方式がある．

パターンマッチング方式とは，マルウェア内の特徴的なコードをパターン(シグネチャ)としてデータベース化し，検査対象となるファイルと比較して検出する仕組みである．アンチウイルスベンダは，マルウェアの検体ファイルを解析し，シグネチャを作成する．作成したシグネチャは，アンチウイルスソフトの最新シグネチャとして提供され，PC にファイルとして侵入したマルウェアの検出に使用される．

マルウェア検出を，実世界の犯罪捜査にたとえると，このシグネチャは，いわば犯人の指名手配写真である．あらかじめ，犯人の顔写真を指名手配書として登録しておき，指名手配書と一致する人を逮捕する方法である．

パターンマッチング方式のメリットとして，検出精度の良さが挙げられる．マルウェアから抽出したコードを元に検出を行うため，正常なファイルを誤ってマルウェアとして検出する誤警告は少なくなる．また，パターンマッチング方式で使用するシグネチャは，一定のルールに従って，マルウェア内の特徴的なコードを抽出し，機械的にパターン化している．マルウェアの検体ファイルさえ入手できれば，シグネチャ作成は容易であり，検出対応コストも低く抑えることができる．検出精度の良さ，検出対応コストの点から，パターンマッチング方式は，マルウェアを確実に検出するための仕組みとして，ほぼすべてのアンチウイルスソフトが採用している方式である．

このパターンマッチング方式にもデメリットが存在す

る．マルウェアの特徴的なコードをデータベース化したシグネチャを用いて検出を行うため，データベースに登録されていないマルウェア☆3を検出できない．アンチウイルスベンダは，ハニーポットをはじめとした，未知のマルウェアの収集に力を入れ，シグネチャの拡充を図っている．しかし，流通するマルウェア数の爆発的な増加に伴って，シグネチャで検出できない未知のマルウェアが増加してきている．また，シグネチャの拡充によって，データベース化したファイルサイズの肥大化も無視できない．特に，法人ユーザにとって，数千，数万のPCに対して，巨大なシグネチャのファイル配信を行う場合，ネットワーク帯域の圧迫が問題となる．

●ヒューリスティック方式

ヒューリスティック（heuristic）とは，発見的問題解決法，経験則という意味である．アンチウイルスソフトのヒューリスティック方式とは，既存のマルウェアの動作ルールを抽出し，検査対象ファイルの動作と比較し，活動内容の不正を検出する方法である．パターンマッチング方式が，ファイルのコードの特徴をもとに検出するのに対し，ヒューリスティック方式では，ファイル実行時の動作の特徴をもとに検出する．

たとえば，ファイル感染型のマルウェアの動作をルール化すると次のようになる．

1. PC内の実行可能形式ファイルの検索
2. 発見した実行可能形式ファイルへの書き込み処理の準備
3. 実行可能形式ファイルへの不正コード追記
4. 追記した不正コード実行のための，実行可能形式ファイルの一部改変
5. 実行可能形式ファイルへの書き込み処理の終了

これらの動作を，ファイル感染型マルウェアの特徴的な動作としてルール化しておく．次に検査対象ファイルの動作をエミュレートし，このルールと比較する．一致する場合，検査対象ファイルは，ファイル感染型マルウェアの可能性が高い不審なファイルであると判定する．ヒューリスティック方式のメリットは，パターマッチング方式とは異なり，マルウェアの検体ファイルをあらかじめ入手していなくてもよく，ファイルの不審な動作から判定できる点にある．つまり，未知のマルウェアを検出できる点が特徴となる．

ただし，ヒューリスティック方式では，ファイルの動作をもとに不審なファイルか否かを判定できるが，本当にマルウェアであるかどうかを判定するには，ファイルの解析が必要である．マルウェアの検出精度という面では，パターンマッチング方式には及ばない．さらに，ファイルの動作をエミュレートするために，PCに多少の負荷をかける．ファイル検査スピードなどのパフォーマンス面でパターンマッチング方式に劣る．

●ジェネリック検出

パターンマッチング方式，ヒューリスティック方式ともに，メリット・デメリットが存在するが，これらを巧みに組み合わせることで，効果的な検出を実現するのがジェネリック検出である．

ジェネリック検出は，特定のマルウェアの亜種☆4を検出するための方法である．通常，新たなマルウェアが出現すると，そのマルウェアを元に複数の亜種が作成される．これらは，不正動作などの特徴が類似しているため，同一のマルウェアファミリとして分類する．たとえば，2006年から2007年にかけて，世界的に流行したWORM_STRATIONファミリ[3]では，アンチウイルスソフトのパターンマッチング方式により検出されるのを避けるために，大量の亜種が次々に作成された．

ジェネリック検出では，パターンマッチング方式の課題を解決するために，WORM_STRATIONが共通して使用していた不正な圧縮方式に着目する．マルウェアのコードに含まれるこの共通部分をパターン化することで，新たに出現するWORM_STRATION亜種の検出が可能となる．ヒューリスティック方式との違いは，エミュレーションの有無である．ジェネリック検出では，エミュレーションを実施するのではなく，マルウェアのコードの共通的な特徴に着目した検出を行うことにより，PCに必要以上の負荷をかけることなく，精度の高い検出を実現できる．このように，ジェネリック検出は，WORM_STRATIONファミリのような大量に亜種が流通するマルウェアに対して効果的である．

●振舞い検知

PC上でのマルウェアの動作を，ヒューリスティック方式のようにエミュレートすることなく，検出する方法に振舞い検知がある．

振舞い検知は，ブラックボックス手法と呼ばれる手法の1つである．不正な動作を検出するために，PC上で実行されたプログラムの動作を監視し，実際に行われた動作から，マルウェアの可能性が高い不審なファイルか否かを判定する．

☆3 通常，このようなマルウェアのことを，未知のマルウェアと呼んでいる．

☆4 最初に発見されたマルウェアを元に作成され，感染形態や機能が変化した新たなマルウェアのこと．マルウェアを分類するために特徴が似ているものを，亜種と呼んでいる．

たとえば，PC 内で IP アドレスとホスト名との対応を記載している HOSTS ファイルを書き換える操作を監視する．また，Windows のシステムファイルを書き換える操作，レジストリエントリを追記し，ファイルの自動起動設定を有効にする操作等，マルウェアによる不正な動作と思われる各種操作が監視の対象となる．ただし，これらの操作は，正規のユーザによる正規な操作や，正規のプログラムによる正規な操作が含まれている可能性もある．そのため，正規のプログラムを監視対象のホワイトリストに登録しておくことにより，正規のプログラムの正規な動作に対する誤警告を防いでいる．

3 つのレピュテーション技術と相関分析による防御

ここまでに紹介した 4 つの検出技術は，いずれも単体活動型マルウェアをベースとした検出技術である．「Web からの脅威」では，一度マルウェアに感染すると，そのマルウェアが，異なる新たなマルウェアを連続的に呼び込む傾向が顕著である．さらに，新たなマルウェアの出現間隔も短くなっている．トレンドマイクロのマルウェア解析センタであるトレンドラボに寄せられた，新種のマルウェア種別数は，2007 年で 1 時間あたり平均 205 個であったが，2009 年には平均 1,484 個となる見込みである．2.5 秒に 1 個の割合で新種のマルウェアが出現していることになる．

このように，加速度的に増え続けるマルウェアをシグネチャによるパターンマッチング方式で 1 つずつ検出するのではなく，そのマルウェア配布にかかわる発信元，すなわち攻撃サイト自体をブロックするためのアプローチがレピュテーション（Reputation）である．レピュテーションとは，評判・世評という意味である．マルウェア配布にかかわる Web サイトや，攻撃サイトへの誘導を促す電子メールの発信元サイトの評判をデータベースに蓄積し，インターネットのサービスにアクセスする際に，サイトの危険度判定情報として利用する．なお，レピュテーションで使用されるデータベースは，大容量かつ，頻繁にデータ更新する必要があるため，インターネット上のクラウド型システム（以降，クラウド型レピュテーションシステム）で保持するのが一般的である．

Web レピュテーション

Web レピュテーションは，マルウェア配布にかかわる Web サイトへのアクセスをブロックすることで，ユーザを危険なサイトに近づけないようにする仕組みである．

Web サイトへのアクセス制御技術として，URL フィルタリングが普及している．URL フィルタリングは，Web サイトへのアクセス可否を URL 単位で設定することで，Web サイトのコンテンツ（内容）へのアクセスを制御する．たとえば，業務時間中には，ビジネスカテゴリに属する URL 群にはアクセスを許可するが，ショッピングカテゴリに属する URL 群にはアクセスを禁止することで，Web サイトの適正利用を実現する．

Web レピュテーションは，Web サイトの危険度判定結果をもとに，ユーザを危険なサイトに近づけないようにする URL フィルタリング技術と言える．マルウェア配布にかかわる攻撃サイトなど危険度の高い Web サイトへのアクセスを遮断することによって，マルウェア感染の危険を回避する．一般的に，攻撃サイトで使用される Web サーバの運用期間は短く，Web サーバの所在地も短期間で変更されるなど，運用面での安定性が低い傾向にある．Web サイトの危険度判定には，このような Web サイトの運用状況をチェックしている．また，マルウェアを配布している攻撃サイトは，配布行為自体が危険な行為であることから，危険なサイトであると判定する．また，既知の攻撃サイトへのリンクを保持している Web サイトは，マルウェア配布にかかわるサイトである可能性が高いことから，同様に危険なサイトと判定できる．

迅速な判定結果をユーザに提供するために，これらの項目を用いて Web サイトの危険度を判定する機能および，その危険度判定情報を格納するデータベースをインターネット上のクラウド型レピュテーションシステムとして構築することが多い．

図 -5 は，Web レピュテーションによる，Web アクセス制御の流れである．

ユーザが Web サイト 1 にアクセスを行う際に，Web レピュテーションデータベースに Web サイトの危険度判定を問い合わせる（①）．Web レピュテーションデータベースから回答「Web サイト 1 ＝安全なサイト」を得た場合には（②），Web サイト 1 へのアクセスを許可する（③）．

ユーザが危険なサイトにアクセスを試みた場合には，Web レピュテーションデータベースから回答「Web サイト 2 ＝危険なサイト」を得ることになるため，危険な Web サイトへのアクセスをブロックする（④，⑤，⑥）．

Web サイトが未評価の場合，Web レピュテーションデータベースから回答「Web サイト 3 ＝不明なサイト」を得る．この場合，Web レピュテーションの判定システムが Web サイト 3 からコンテンツをダウンロードし，危険性を判定する（⑩）．その判定結果は Web レピュテーションデータベースに登録され，次回以降のアクセスに，Web サイトの判定結果として利用される．

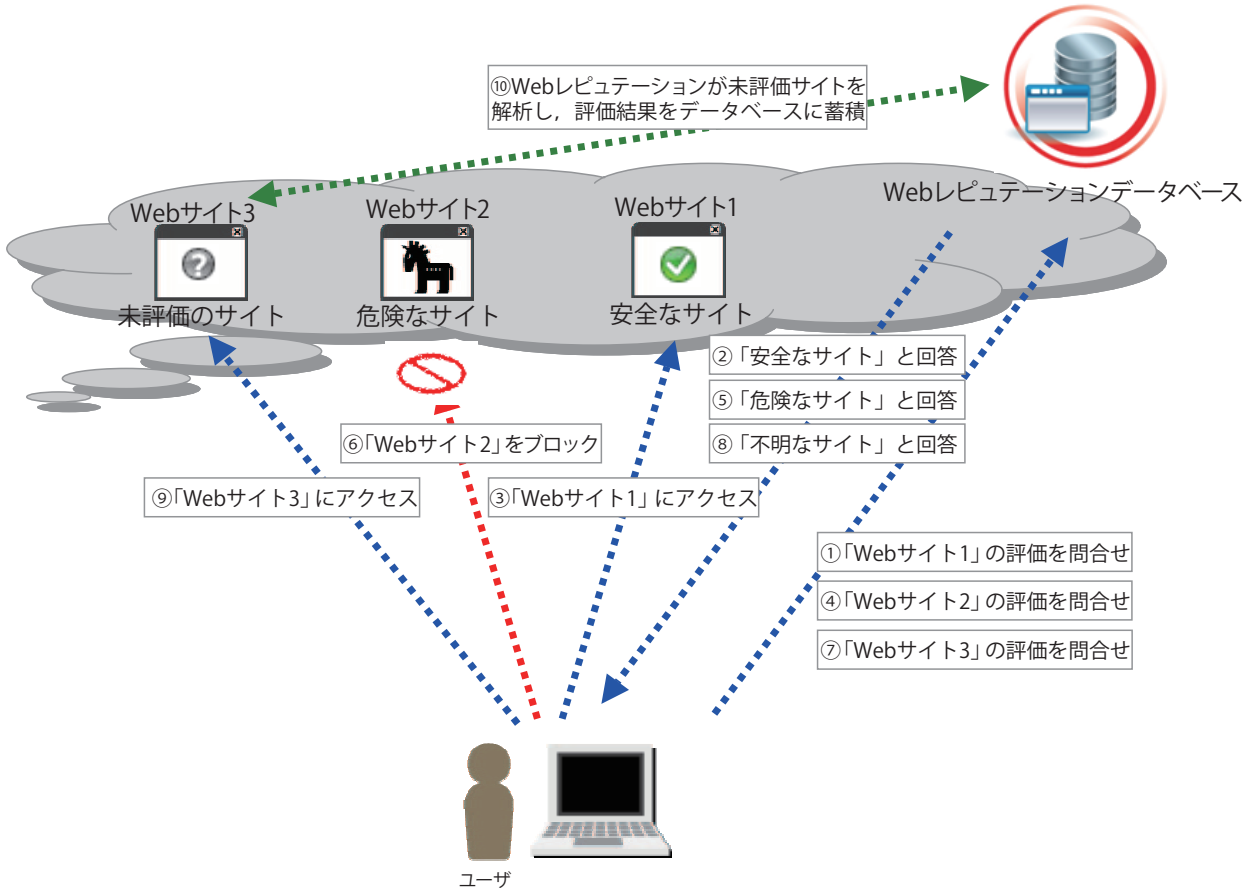

図 -5　Web レピュテーションの動作

E-mail レピュテーション

受信者にとって不要・迷惑なメール，すなわちスパムメールは，サーバ資源，ネットワーク資源を圧迫するだけではなく，ユーザの生産性低下を招く．また，昨今，スパムメールに記載した URL から攻撃サイトに誘導して，偽セキュリティソフトウェアのダウンロードにつなげるなど，マルウェアの侵入口としても活用されている．

スパムメール対策として，送信者情報または電子メールの内容から，スパムメールか否かを判定するスパムフィルタリング技術がある．しかし，攻撃者は，スパムフィルタリングにより電子メールが破棄されるのを避けるために，電子メールの送信者情報の偽装，単語分割等による電子メール本文の内容偽装☆5，画像スパム☆6，電子メール本文に URL を記載した Web サイトへ誘導など，その手口を進化させている．

また，ボットネットによるスパムメール送信に見られるように，スパムメールとマルウェアとの関係がより密接になってきている．たとえば，スパムメールに記載した URL から攻撃サイトに誘導して，新たなマルウェアのダウンロードにつなげる．あるいは，スパムメールに添付したマルウェアを起点として，攻撃サイトから新たなマルウェアのダウンロードにつなげるなど Web サイトと連携した攻撃手法が確立している．

このような，攻撃サイトへの誘導型スパムメールの増加を踏まえ，危険なメールサーバからの電子メールをユーザに届けないようにする新たな仕組みが E-mail レピュテーションである．

E-mail レピュテーションでは，メールサーバの危険度判定をもとに，電子メールをブロックする．一般的に，長期間にわたって安定して運用されているメールサーバは信頼できる発信元とみなすことができる．一方，運用面での安定性が低いメールサーバは，不審な発信元となる．メールサーバの危険度判定には，このような電子メールサーバの運用状況に加えて，実際にそのメールサーバ（IP アドレス）からスパムメールが送信された実績もチェックすることで危険度判定の精度をあげている．

迅速な判定結果に基づき，電子メールをブロックするために，Web レピュテーションと同様，メールサーバの危険度を判定する機能および，その危険度判定情報を格納するデータベースをインターネット上のクラウド型レピュテーションシステムとして構築するのが一般的である．これは，システムを集約化することにより，危険

☆5 故意に違う綴りを用いる（例：V1AGRA），空白で単語を分割する（例：ＳＰＡＭ）などの方法がある．
☆6 電子メールのメッセージをテキストではなく，メッセージを書き込んだ画像として送付する方法である．

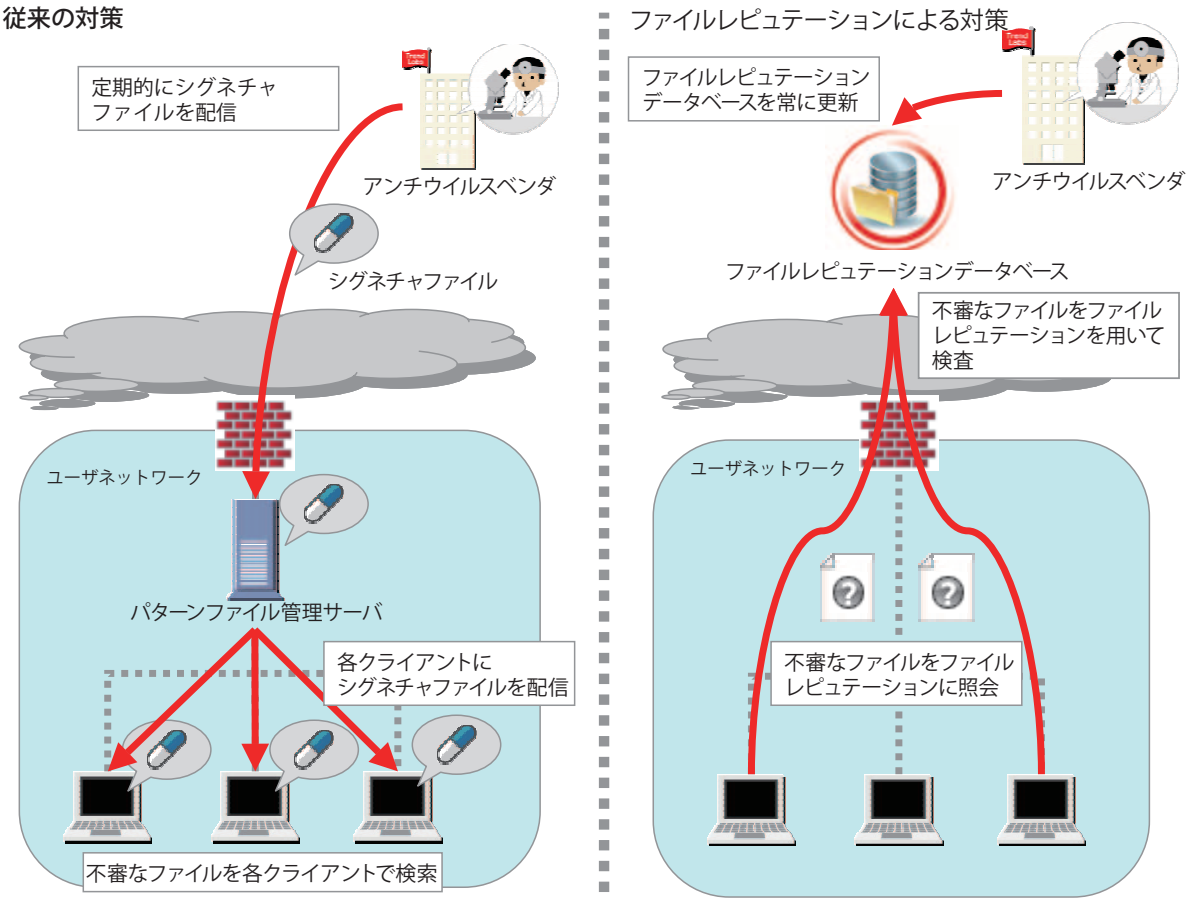

図 -6　従来の対策とファイルレピュテーションによる対策の比較

度判定の対象となるメールサーバも広がり，ボットネットを用いて動的に IP アドレスを変えながら発信されるスパムメールのブロックなどにも対応できるというメリットがある．

E-mail レピュテーションによるスパムメールのブロックは，Web レピュテーション同様に高い効果をあげている．

●ファイルレピュテーション

上記で説明した Web レピュテーションおよび E-mail レピュテーションは，マルウェアの侵入口を危険度という指標を用いて判定し，攻撃サイトへのアクセスをブロックしたり，スパムメール受信をブロックしたりする仕組みである．あくまでも，ユーザを危険から遠ざける技術であり，従来からの直接的な対策の補完技術である．このため，従来からの直接的な対策技術である，パターンマッチング方式，ヒューリスティック方式，ジェネリック検出，振舞い検知の重要性は以前と変わりはない．

ファイルレピュテーションは，従来からの直接的な対策技術を利用して，検査対象ファイルが不審なファイルか否かを判定するための分散型の大規模な検査システムである．ファイルレピュテーションでは，マルウェアの増加とともに，肥大化したシグネチャの配信ファイルサイズを縮小するために，Web レピュテーション，E-mail レピュテーションと同様，パターンマッチング方式で使用するシグネチャを格納するデータベースをインターネット上のクラウド型レピュテーションシステムとして構築する．

図 -6 は従来の対策とファイルレピュテーションによる対策の比較を示したものである．ファイルレピュテーションでは，シグネチャの一部を PC 上に保持し，検査処理も PC 側で実施する．PC は保持しているシグネチャで認識できない検査対象ファイルの情報をファイルレピュテーションデータベースに送信する．ファイルレピュテーションデータベースでは受信した情報から検査に必要となるシグネチャを判定して送り返す．すなわち，ファイル検査時に必要となるシグネチャをファイルレピュテーションデータベースから必要に応じてダウンロードして検査するという仕組みである．

ファイルレピュテーションと従来型のパターンマッチング方式の違いは，シグネチャを保持する場所だけの違いと言える．しかし，ファイルレピュテーションデータベースのシグネチャを利用するという仕組みは，次のような多くのメリットを持つ．

- PCへのシグネチャ定期配信が必要なくなり，PCは常に最新のシグネチャを利用できる．これは，新規マルウェアへの検出対応時間の短縮にもつながる．
- シグネチャをファイルレピュテーションデータベースとして保持する仕組みのため，各PCに配信するシグネチャのファイルサイズを縮小できる．あわせて，PCで保持するシグネチャは必要最低限となるため，PCのリソース消費を抑えることができる．

スマートフィードバックと相関分析

これら3種類のレピュテーション情報を効果的に使用し，PCをマルウェア感染から防御するための技術として，スマートフィードバックと相関分析がある．

スマートフィードバックは，アンチウイルスソフトとクラウド型レピュテーションシステムとが情報交換するための仕組みである．レピュテーションシステムは，アンチウイルスソフトに対して，レピュテーション情報（Webサイト，メールサーバ，ファイルの危険度判定情報など）およびシグネチャのアップデート情報等を送信する．アンチウイルスソフトでは，受信した情報を用いて検知したマルウェアなどの脅威情報をレピュテーションシステムに送信する．

双方向で情報交換を適宜行うことにより，PC側ではいち早くレピュテーション情報を活用でき，レピュテーションシステム側では効率的にレピュテーション情報を収集ならびに更新できる．たとえば，アンチウイルスソフトが，未知のURLからダウンロードしたファイルを既知のマルウェアとして検出した場合，検出したマルウェア情報とともに，ダウンロード元のURL情報，シグネチャのバージョン情報等をレピュテーションシステムに送信する．Webレピュテーションは，受信したURL情報を用いてWebサイトの危険度判定をし，その結果をレピュテーションデータベースに登録する．このように，スマートフィードバックには，1つのイベントをきっかけとして，そのイベントに関連する他のイベントについても危険度判定などの解析作業を起動できるというメリットがある．

さらに，各レピュテーション情報を相互に交換し，相関分析により関係性を明らかにしていくことで，危険と判定されるサイト，メールサーバやファイルなどの情報を先回りして各レピュテーションに登録できることになる．たとえば，スパムメールに記載されたURLにアクセスした結果，マルウェア感染が発生した場合には，スマートフィードバックを組み合わせることにより，次のような相乗効果を期待できる．

アンチウイルスソフトが既知のマルウェアを検出した場合，アンチウイルスソフトは，そのマルウェアをダウンロードしたURL情報をWebレピュテーションの判定システムに送信する．判定システムでは，Webサイトの危険度判定のため，URLからダウンロードしたファイル群を解析し，その結果をファイルレピュテーションに登録する．これによりファイルレピュテーションによって検出可能なファイルが増加する．

同時に，アンチウイルスソフトでは，該当するスパムメールの発信元となるメールサーバのIPアドレスを抽出し，スマートフィードバックによりE-mailレピュテーションの判定システムに送信する．次回以降，E-mailレピュテーションを用いたスパムメール受信のブロック，Webレピュテーションを用いた攻撃サイトへのアクセス回避が可能になる．

それぞれ独立して収集し，個別の対策で個々に利用されていた，マルウェア情報，危険なWebサイトのURL情報，スパムメールの発信元サーバ情報などが，スマートフィードバックを使用することにより，より早く，効率的に収集可能となる．さらに，収集した情報を相関分析により相互に結びつけていくことで，未知の脅威への柔軟な対応が可能となる．

まとめ

「Webからの脅威」に代表される現在の脅威においては，マルウェア種別数および出現スピードの増加が大きな問題となっている．これに伴い，ファイルに対するマルウェア検出のみに頼った既存の対策から，マルウェアの侵入回避（Prevention）も含めた対策が必要となっている．

脅威の複雑化，複合化が進む中，その対策についても，さまざまな視点から実施する必要がある．レピュテーションと相関分析の仕組みを，従来からの直接的な対策技術である，パターンマッチング方式，ヒューリスティック方式，ジェネリック検出，振舞い検知とともに使用することにより，連続的かつ複合的な「Webからの脅威」による攻撃に対して，大きな対策効果を期待できる．

参考文献

1）http://av-test.org/
2）WORM_SKA.A
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_SKA.A
3）WORM_STRATION
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_STRATION

（平成22年1月19日受付）

小松優介
Yusuke_komatsu@trendmicro.co.jp
トレンドマイクロ（株）サポートサービス本部セキュリティエンハンスメントグループThreat Monitoring Center担当課長代理．国内の脅威動向の監視・調査業務に携わり，顧客向け脅威分析レポートの作成に携わる．