特集
マルウェア

マルウェア観察日記（2）
―サービスとして提供される攻撃―

須藤年章（NTT コミュニケーションズ（株））

危険な毎日

攻撃や被害が発生してから発表される脆弱性情報，普段からよく閲覧している一般の Web サイトがある日突然改ざんされ，そのサイトを閲覧しただけでマルウェアに感染するような攻撃手法の流行により，どれだけ注意深く行動しても，どれだけのセキュリティ対策を講じても，安心してインターネットを利用することができない毎日が続く．専門家，素人，老若男女関係なく誰もがいつ被害者になるか分からない．これらの攻撃によって受ける被害はアカウント情報，パスワードや銀行口座番号などの個人情報収集だけではない．その情報の直接的な売買や，その情報を利用したさらなる攻撃の拡大につながるため将来的に直接的，間接的に受けるであろう被害は甚大なものになる．このようなさまざまな攻撃状況を毎日観察していると攻撃者たちが，得られる利益をより高めるために，どのようなシステムインテグレーションを行っているのか，どのような新しい試みを行っているかの最新状況が見えてくる．

サービス化する攻撃

マルウェア配布，ボットネット，フィッシング，スパムメールなどの攻撃に利用されるシステムは，時代の変化や世の中の流行にあわせ，さまざまなインターネットサービスを利用し，そこに紛れ込み，次々と姿と場所を変えていく．そして新たなコンセプト，機能の試行が繰り返され，一般のインターネットサービス（以降，一般サービス）☆1 よりもすぐれた機能や運用品質を目にすることがある．最近ではインターネット上のサービスというかたちで攻撃ツールやマルウェア，実際の攻撃コントロール環境の提供が行われ，俗称で CaaS（Crimeware as a Service）や MaaS（Malware as a Service）と呼ばれている．攻撃者は特別な開発スキルも特殊なシステムも必要なく，これらのサービスを利用するだけで簡単に高度な攻撃ができるようになっている．これは一般サービスとして提供されている SaaS（Software as a Service）やクラウドと呼ばれるサービスと同じようなコンセプトに基づき，コスト面や，技術面など，攻撃参加の敷居を下げ，被害の増大を助長することになる．そのサービスイメージは図 -1 のようになる．一般サービスだけではなく，ボットに感染した PC（以降，ボット感染 PC）もインフラの一要素として利用する「サーバインフラ層」と，その上に構築される「基本サービス層」，さらにそれらを利用してさまざまな「悪性サイト☆2 やシステム」が構築される．

図 -1　サービスイメージ

複雑化する悪性サイト

古典的なマルウェア配布は，専用に運用されているマルウェア配布サーバと感染 PC という単純な組合せで実行されていたが，最近の攻撃に関連するシステムは前述のようなサービスを利用して構築されるようになっている．当然，そのサービスに対しては，より高い効率性や安定性などが求められる．効率的なシステム構築や運用，新技術の開発というサービス提供面からの理由と，セキュリティ対策や障害によりサービス継続性が損なわれないようするための品質面の理由により，攻撃に関連する

☆1 ホスティング，ファイル共有，Web メール，ブログなどインターネットで利用することができるサービス全般のことを示す．
☆2 マルウェア配布サイト，フィッシングサイトや情報収集サイトなど，悪意ある第三者が攻撃活動に使用するサイトのことを悪性サイトと呼ぶこととする．

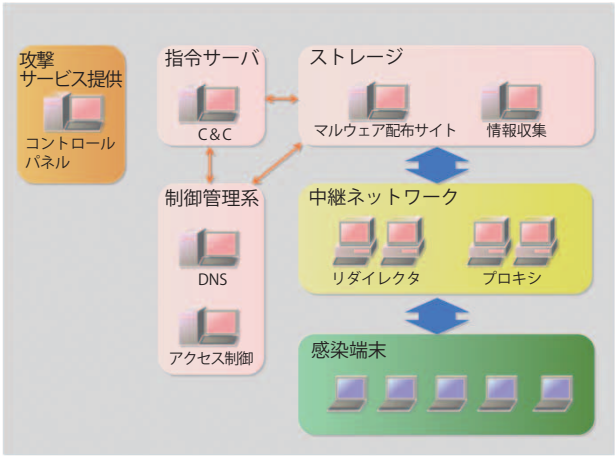

図 -2　システム分散

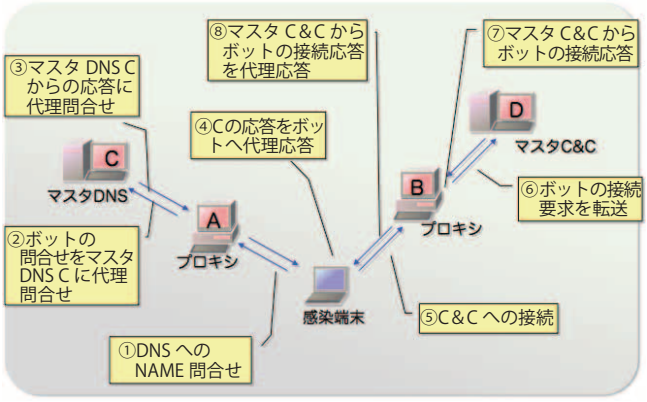

図 -3　プロキシ

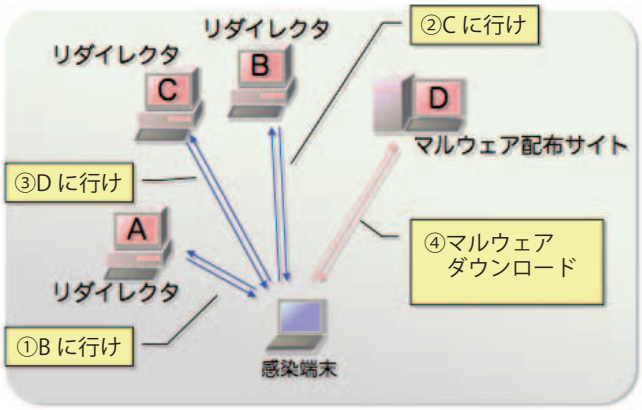

図 -4　リダイレクタ

システムの役割分担および機能分離，分散配置などが行われている．そして，図 -2 のように指令サーバ，制御管理系，ストレージなどの管理システム群と，これら管理システム群を守るための中継ネットワークなどが前述のサービスを利用して構築される．

制御管理系システム

個々のシステムを，機能分離することで，数日程度のサイクルで頻繁に行われるサーバの場所の変更や，新機能追加などのシステム変更，更改を容易にしている．また冗長構成，予備システム等も準備されており一部のシステムが何かしらの障害もしくは，防御側のセキュリティ対策により動作しなくなったとしても，予備で準備している同機能のシステムを部分的に組み替えることによりシステム全体としてのサービス継続性を確保する．

中継ネットワーク

中継ネットワークの多くは，図 -3 のようなプロキシや図 -4 のようなリダイレクタの仕組みを何段にも組み合わせた構成をとり，最終的な到達地点である管理システム群を隠蔽する役割を果たす．

このような仕組みを利用することで，マルウェア検体を解析して見つけたと思ったマルウェア配布サイトの URL が実は中継ネットワークの一部でしかなく，しかもその IP アドレスは一般ユーザの PC やサーバでしかないという状況を作りだす．これにより，本丸である管理システム群を保護する．さらに，中継ネットワークを破壊しようとしても，中継ネットワークを構成しているボット感染 PC やサービス上で稼働するボット自体も次々と入れ替わり，変化していくために，それを追跡したり，対策したりすること自体が非常に難しくなっている．

●利用される一般サービス

サーバインフラ層を構成するために無料のホスティングサービスや画像，ファイル共有サービスなどの一般サービスが利用され始めている．利用されるサービスは，ツールで無限にアカウント作成ができ，保存したファイルを公開 URL として利用できるサービスである．このようなサービスに対しては，必要に応じて自動アカウント作成機能のあるボット，あるいはボットネットを介して自動的に大量のアカウント作成を行っている．実際に利用されていることが観測されたサービスの例を表 -1 にまとめる．

これらのサービスを利用した場合，アカウントごとにサブドメインやディレクトリパスが割り当てられたとしても，ドメイン名や IP アドレスはサービス全体で共用することになる．つまり一般サービスを攻撃に利用することによって，マルウェアが使用する URL や IP アドレスを，同じサービスを利用する他の一般的な正規サイトと共用させたり，大量にユーザを抱える有名な正規サービスが絡んでくる状況を作り出す．防御側がセキュリティ対策で該当する URL や IP アドレスとの通信をブロックした場合には，正規サービス自体を利用できなくすることになる．ましてや TLD（Top Level Domain）単位のドメイン名で通信をブロックすることなど普通はあり

サービスの種類	実際に利用が観測されたサービス例
ホームページ，ブログ作成	GooglePages
画像ホスティング	ImageShark，BAYIMG
動画ホスティング	Youtube
ファイルホスティング オンラインストレージ	Rapidshare Windows Live SkyDrive
クラウド系	Amazon EC2
その他	Google Docs

表 -1　一般サービスの利用

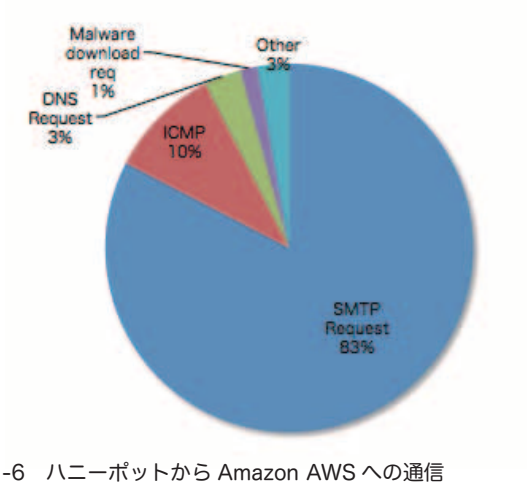

図 -6　ハニーポットから Amazon AWS への通信

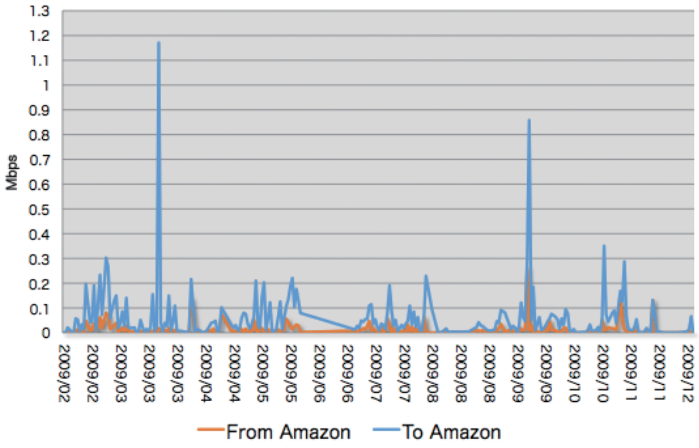

図 -5　ハニーポットと Amazon AWS 間のトラフィック量の推移

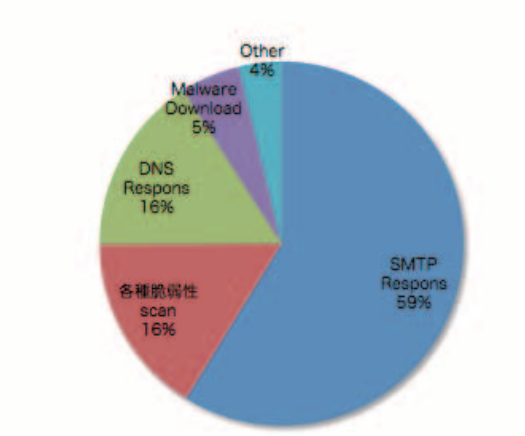

図 -7　Amazon AWS からハニーポットへの通信

得ない[☆3]．ただし，企業あるいは，個人利用において，通信相手を限定するという強制的なポリシーが適用できるならば，これらの一般サービスの利用を禁止するだけで攻撃を簡単にブロックできる．これらの一般サービスが制御管理系システムよりもリダイレクタ等の大量性があり代替手段が多く用意されているような中継ネットワークで使われることが多いのは，このような理由からかもしれない．

Amazon AWS の利用例

毎日の観察の中でみつけたタイムリーな情報の中から，一般サービスを利用した例として Amazon AWS を利用した攻撃の観測を紹介する．

図 -5 は 2009 年 2 月から 12 月までの期間に，ハニーポットで観測された Amazon AWS 関連のネットワークとの通信量の変化を示している．年間を通して継続的にトラフィックが観測されていることから，2009 年に入って突然使われ始めたわけではなく，すでに攻撃に利用可能なサービスの 1 つとして使われ続けていたようである．

図 -6，図 -7 はハニーポットと Amazon AWS 間で発生した通信内容であり，この内訳から，次のようなことを読み解くことができる．

- SMTP 通信が最も多く観測されているが，これは Amazon AWS を利用して提供されているメールサービスが多数あり，そのメールサービス利用者向けにボットがスパムメールを送信しようとしたために発生している．
- DNS 関連の通信についても同様に Amazon AWS を利用して DNS を運用しているサービスが存在しているため，その名前解決のために発生するトラフィックである．
- ハニーポットから Amazon 向けの ICMP 通信は，ボットの初期動作で行われる ICMP によるスキャン活動の対象に Amazon の IP アドレスブロックが含まれていたために観測された．
- Amazon AWS を利用してマルウェア配布サイトが構築されており，そのサイトを利用してマルウェア配布が継続的に行われている．

☆3　.jp や .com という単位で通信をブロックすること．

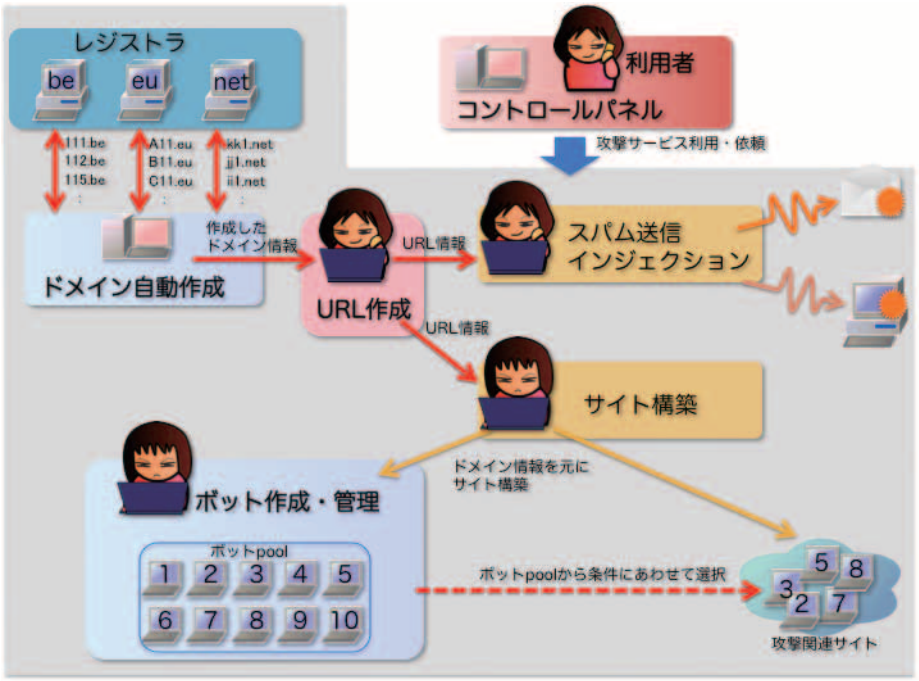

図 -8　悪性サイト構築の流れ

- Amazon AWS からハニーポット向けに脆弱性スキャン攻撃が多く観測されており，マルウェア配布サイトという利用方法だけではなく，ボット感染 PC と同等の攻撃システムとしても利用されている．

結局，クラウドはバーチャルホスティングと同じような機能を提供するものなので，バーチャルホスティングと同じような目的で幅広い用途で利用されている．今後，クラウドが攻撃に利用されるかどうかは，他のサービスと比較して，利便性とコストがどの程度有利かなどの試行を通じて決まることになるのであろう．

●悪性サイト構築プラットフォーム

一般的にボット感染 PC や乗っ取られたサーバは，直接的な攻撃ツールの 1 つとして利用されるものだと思われがちである．しかし，最近では直接攻撃だけではなく，悪性サイトを構築するためのサーバインフラとして利用されることが多い．フィッシングサイトやマルウェア配布サイトが実は大量のボット感染 PC を用いたラウンドロビン構成☆4 という状況が日常的に観察できる．

このような状況は図 -1 で説明したサービスイメージ中のサーバインフラ部分の要素としてボット感染 PC が利用されているために発生する．このようなボット感染 PC などから構成されるサーバインフラの上に一般的なホスティングサービスと同様な Web サーバや DNS，オンラインストレージなどのサービスが構築される．さらに，このサーバインフラを利用してフィッシングサイトやマルウェア配布サイトなども構築される．このようなサイトを観察していると，ボット感染 PC がラウンドロビン構成で組まれた巨大なサーバに見えてくる．

専用プラットフォームの存在意義

このような専用プラットフォームが用意されつつある背景には，防御側のさまざまなセキュリティ対策をかいくぐりながら，攻撃の効率，品質の向上や，攻撃規模，種類，頻度の拡大を実現することへの一般サービスを利用したアプローチに限界がきたことがあるのではないかと想定される．実現されている機能を見ると，障害対策，防御側のセキュリティ対策を回避するためにサーバインフラの構成要素であるボット感染 PC を頻繁に入れ替えながら一定の形にとどめることなく変化させ続けている．さらに，その上位レイヤのサービスやシステムに影響をあたえることなく攻撃そのものの継続性と管理システム群の隠蔽をより強固にすることは，一般サービスを利用しているだけでは実現が難しいものが多い．コストを抑えながら，このようなより複雑で高機能な仕組みを実現するため，独自のインフラやサービス基盤が必要とされているのであろう．

悪性サイトの構築

専用の悪性サイト構築プラットフォームを利用した悪性サイトの構築の流れを図 -8 に示す．

悪性サイト構築において，ドメインの作成と運用が重要であり，まず攻撃に利用するドメインの作成が行われている．たとえば図 -9 は 2009 年を通じて猛威が続い

☆4 負荷分散や冗長性を確保するために，同様な構成を持つ系を複数用意して，処理要求を順番に割り振ること．

```
www.facebook.com.ujtqwaqo.co.uk
www.facebook.com.ujtqwaqo.eu
visa.com.umr1iep0.me.uk
visa.com.umr1iep0.org.uk
online.cdc.gov.yttt4l.org.im
online.cdc.gov.yttt4r.co.im
online.cdc.gov.yttt4r.com.im
online.cdc.gov.yttt4r.im
online.cdc.gov.yttt4r.net.im
chaseonline.chase.com.gerdcxd.be
chaseonline.chase.com.jerr1aa.be
chaseonline.chase.com.jerr1ah.be
```

図-9　ZeuS/zbot で利用されるドメイン

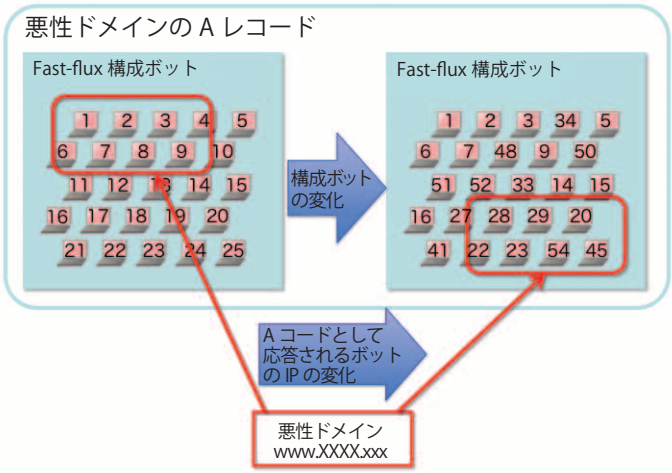

図-10　Fast-flux

た ZeuS/zbot や Bredolab などの攻撃に利用されるドメインの例である．年間を通して 1 日あたり数十から数百の新規ドメインが観測された．このようなドメインの自動的かつ大量作成には登録審査の甘い，あるいは意図的にビジネスとして悪性サイト用のドメイン作成に加担するレジストラ☆5 やリセラが利用作成されている．さらに，どのレジストラが利用しやすいか，目的とする攻撃に適しているかなど，将来に向けての試行も行われているようである．このため，あるレジストラが何かしらの防御対策を行ったとしても代替策が何重にも準備されている状態から抜けだすことはできない．

次に作成されたドメインを使って悪性サイトの URL を作成し，その URL を利用したサイトの構築と誘導のためのスパムメール送信やインジェクション等の攻撃が行われる．このスパムメール送信やインジェクションは別の専用のボットネットを利用して実行される．悪性サイト構築時に組み込まれるボット感染 PC は，前述の通り構築の都度，プールされている大量のボット感染 PC の中から条件にあった最適なものが選択される．このボットプール内のボット感染 PC の在庫が時期により特定の国や AS に偏ることがあるため，攻撃が特定の国や AS に関連して発生しているように見えることがある．

Fast-flux

インフラを構成するボット感染 PC が動的に組み替えられる運用の例としてマルウェア配布サイトやフィッシングサイトなどに広く利用されている Fast-flux の仕組みについて説明する．Fast-flux 活用は，2007 年の StormWorm，2008 年の Waledac などの悪性サイトでさまざまな実験が繰り返され，その有効性が確認されてきたようである．2009 年に入ってからは，ZeuS，Bredolab，cutwail 等のマルウェア配布サイト，関連するフィッシングサイトなどに幅広く用いられるようになっている．

Fast-flux を一言でいえば動的な構成変更機能を備えた DNS ラウンドロビンであり，一般サービスでも近いかたちの運用は広く行われている．図-10 の例は，最初に悪性ドメイン「www.XXX.xxx」にアクセスすると DNS の名前解決で 192.168.1.1 から 2，3，4，6，7，8，192.168.1.9 という A レコード☆7 が応答され，この中の 1 つにアクセスすることになる．これらの IP アドレスはすべてボット感染 PC の IP アドレスである．この場合，「www.XXX.xxx」というサイトの Fast-flux 構成には実際には 1 から 25 までのボット感染 PC が存在し，その中から 8 つのボット感染 PC が選択されているだけである．また，名前解決のタイミングによっては別の 8 つのボット感染 PC の IP アドレスが選択されることもある．さらに利用可能なボット感染 PC が減少した場合や意図的に構成を変えるときには，プールされていた 1 から 25 までのボット感染 PC の一部が別のボット感染 PC に入れ替えられるなど，ボット感染 PC の組合せは常に変化する．実際の例では，プールされるボット感染 PC 数は，数十という小規模なものから数千以上の大規模なものまで存在した．このため次々と現れる新規の IP アドレス 1 つ 1 つに対策を行うことの困難さを伴う非常に厄介なシステムである．

悪性サイトのドメイン運用

悪性サイトの構築運用で非常に重要な要素となっているドメインについての観察結果を述べる．

☆5　インターネット上の住所にあたるドメイン名の登録申請を受け付ける組織をレジストラと呼び，レジストラの下で登録受付業務を行う組織をリセラと呼ぶ．
☆6　Autonomous System の略．各組織が保有・運用する自律したネットワークのことを示す．
☆7　Address の略．A レコードは，ドメイン名に対応する IP アドレスを記載した DNS レコードのことを示す．

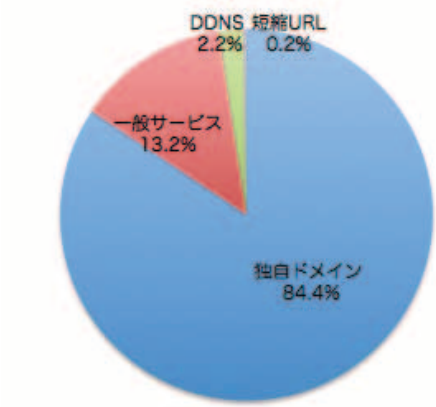

図-11　マルウェア配布ドメイン種別

●ドメイン種別

2008年4月から2009年4月の期間に，ハニーポット，スパムメール，SQLインジェクション等の解析環境で捕捉された悪性サイトのドメイン種別を分類すると図-11のようになる．

前述のように専用の悪性サイト構築プラットフォームを利用したZeuS/zbot等のボットネットやインジェクションなどの攻撃で利用されるドメインが大量に作成され続けていることもあり独自ドメイン比率が非常に高くなっている．スパムメールでの誘導URLも古典的に独自ドメインが利用される例が多いので，この傾向を強める要素になっている．ダイナミックDNS（DDNS）や短縮URLについては，利用する攻撃システムが限定的なのか，試行中なのか分からないが，継続的ではなく，ある月だけ，ある週だけと期間が限定されて大量に観測されるような状況であり，年間を通して集計するとこのような割合になる．

●独自ドメイン

コストや作成の簡易性のみを考えれば無料のホスティングやダイナミックDNSのドメインを利用するのが最も適しているが，前述のような高度で複雑なサーバインフラの構築や運用のためには独自ドメインを大量に利用することが必要になる．レジストラやリセラの中には比較的登録審査の緩い組織が存在したり，悪性サイト構築者やスパマなどを大量にドメインを契約してくれる上顧客として扱い，ビジネスを行っているBullet-Proofホスティングと呼ばれるホスティング事業者なども存在する．しかもこれらの事業者は独自ASやドメインを持ち，BGP，DNS，メール等のあらゆる要素を独自に運用できるため，有効であると信じられているさまざまな防御側のセキュリティ対策を無意味なものにできてしまう．そのため，このような事業者への対策として，AS単位でインターネットからの接続性が断たれたとか，レジストラの権限を剥奪したなどのニュースが聞かれることがある．しかし，世界中に同じような事業者が複数存在しているのでASという単位で接続性を断たれたとしても，別のASで同じことを始めることで攻撃が止まるようなことはない．

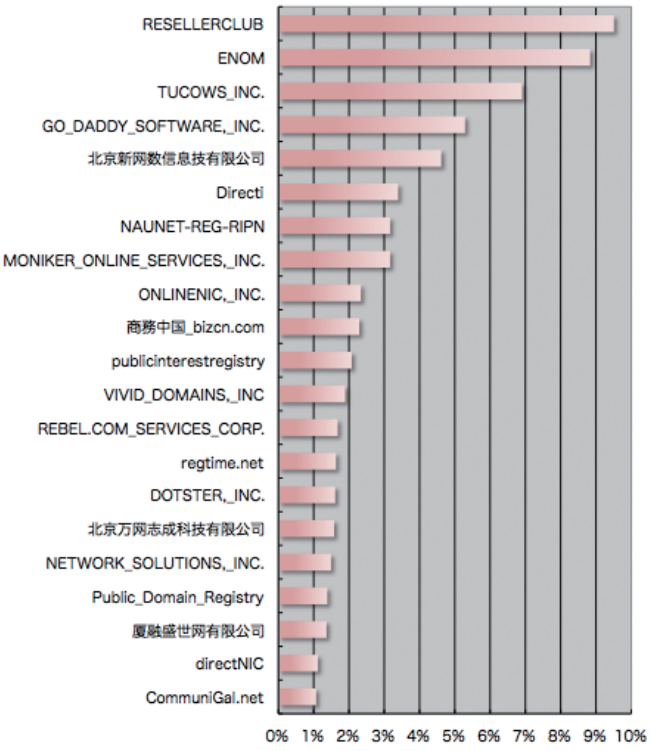

図-12　悪性ドメイン作成に利用されるレジストラ

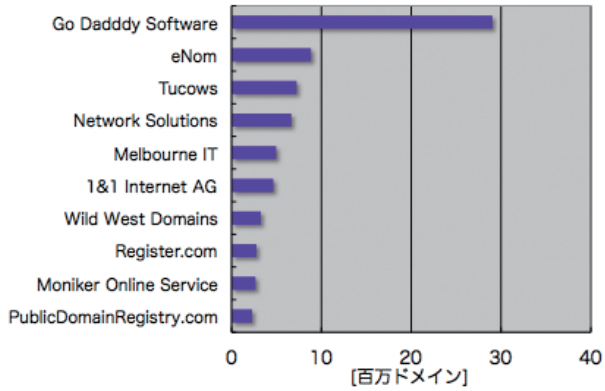

図-13　レジストラとドメイン登録数(2009/1/31)

攻撃に利用されるドメインのレジストラ

84.4%を占める独自ドメインについてそのレジストラを解析した結果を図-12に示す．

比較のために一般的なドメイン登録数の多いレジストラを図-13に示す．

6位のDirecti（インド）は，1位のRESELLERCLUB（アメリカ）や，22位のANSERABLE（インド）をはじめとする50社以上のレジストラやリセラを傘下に抱えてい

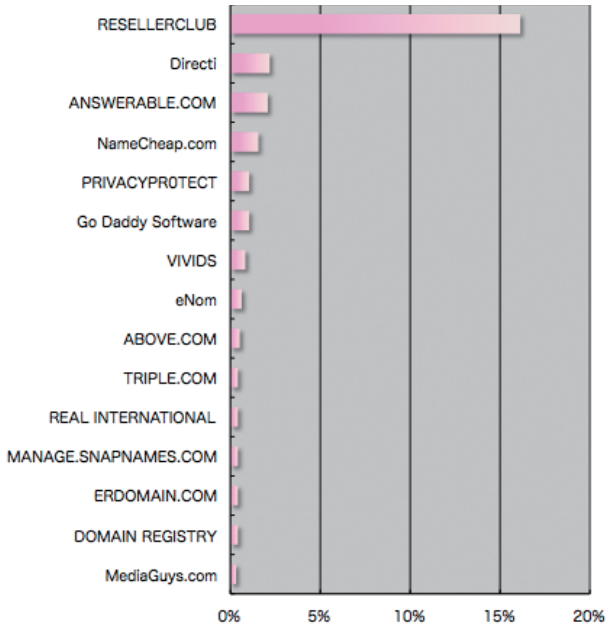

図 -14　偽アンチウイルスソフト関連のドメイン作成に利用されるレジストラ

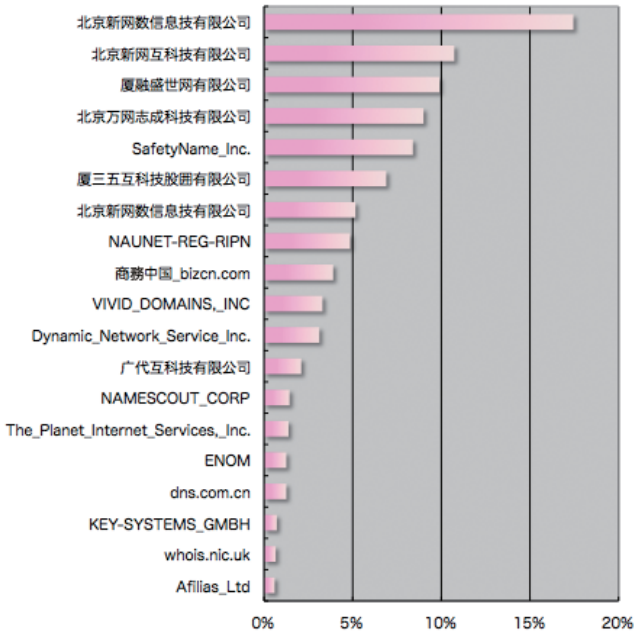

図 -15　SQL インジェクション関連のドメイン作成に利用されるレジストラ

て，悪性サイトに利用されるドメインの保有数が非常に多くなっている．同じような特性を持つ大小のレジストラやリセラも存在するが，これらの提携関係や関連会社の関係を調査すると面白い傾向が発見できる．また，一般的にドメイン登録数の多いドメインレジストラもその数にほぼ比例して登場する．

次に観察していた中で特に活発だった 2008 年以降被害が拡大している偽アンチウイルスソフト配布に関連するドメインのレジストラを解析した結果を図 -14 に示す．ここでは前述の Directi 関連が主要なレジストラとなっている．

もう 1 つの例としてこちらも近年被害が拡大している SQL インジェクションに関連するドメインのレジストラ解析を図 -15 に示す．

こちらは，中国系のレジストラが非常に多く利用されている．解析した期間は，中国系のドメインが多く利用されていたためこのような結果になっている．最近はその他の国のドメインが多く利用されていることから，他の国のレジストラも多く利用されるようになってきている．このように攻撃の種類や時期によって利用されるドメインやそのレジストラの特性が顕著にあらわれる．根本的にはこれらの特定のレジストラによるドメイン作成の段階での対策が最も効果的で重要な役割を果たすことになるはずだが，前述の通り Bullet-Proof と呼ばれる事業者の存在によりその対策も難しい状況にある．

悪性ドメインの生存時間

最近の悪性サイトで利用されるドメインの多くは，その作成から攻撃開始，そして攻撃終了までの期間が非常に短いのが特徴である．悪性ドメインのドメイン作成から攻撃開始そして攻撃終了までの期間が数日で終わってしまうような状況では，捕捉すること自体が難しい．たとえ捕捉，解析してブラックリストやセキュリティ対策ソフト，サービスに反映させたとしても，その頃にはそのドメインの実質の攻撃利用が終わっており，別のドメインに切り替えられているということになる．

ドメイン作成から攻撃開始までの時間

ドメイン作成から攻撃開始までの期間を解析した結果を図 -16 に示す．ドメイン作成から 1 日以内で攻撃開始に利用されるドメインが 30% 程度，7 日以内では 85% になる．この割合は最近非常に多く観測されるインジェクションやボットネット関連のドメインに関してはより顕著な特徴が現れる．

次に ZeuS/zbot 系の攻撃に利用されるドメインに限定して攻撃開始までの時間を解析した結果を図 -17 に示す．

全体の結果に比べて攻撃開始までの期間が非常に短くなっていることが分かる．すべてのドメインが作成から 3 日以内には利用開始されている．

また図中で「-1 日」となっているものは，スパムメールでの誘導 URL 等として利用開始はされているが，実際にはドメインの A レコードの登録はおろか，ドメイン作成すらされずに攻撃が終了したものを示している．

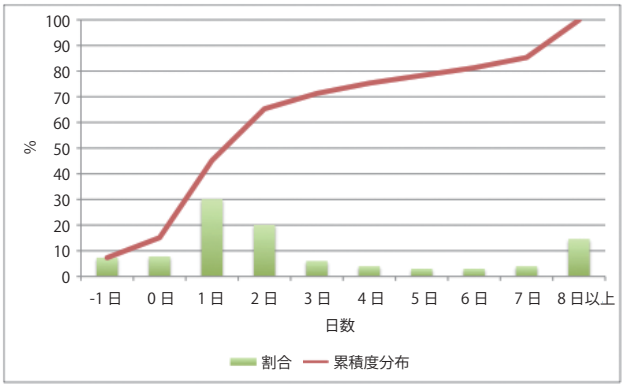

図-16　ドメイン作成から攻撃利用されるまでの日数(全体)

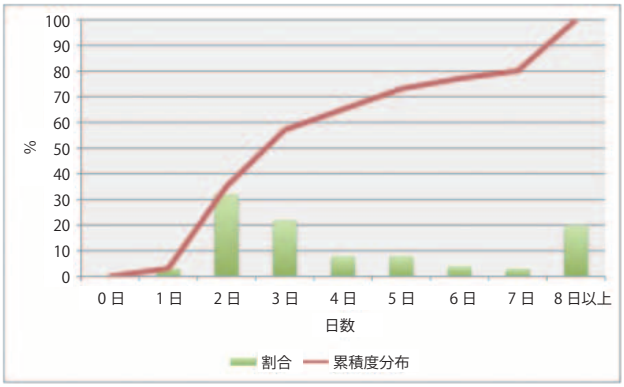

図-18　ドメイン作成から攻撃終了までの日数(全体)

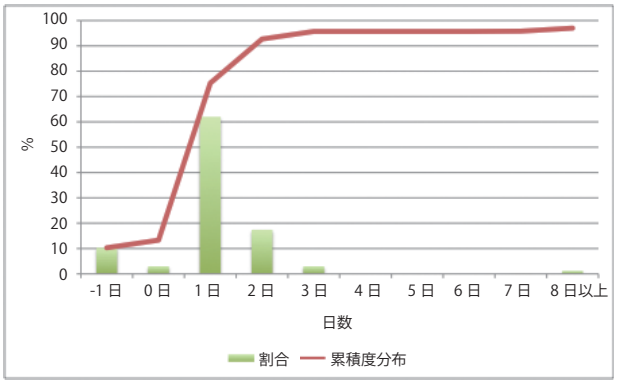

図-17　ドメイン作成から攻撃利用されるまでの日数(Zeus/zbot)

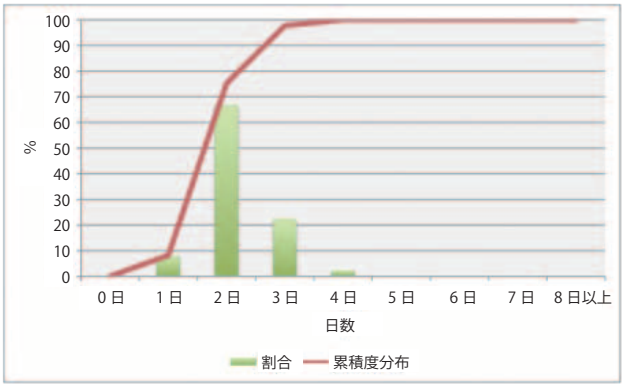

図-19　ドメイン作成から攻撃終了までの日数(ZeuS/zbot)

これは，前述した悪性サイト構築の分業化により，ドメイン作成，ボットネット構築，スパムメール送信間の連携が失敗したのかもしれない．あるいは，短期間で大量のドメイン作成とスパムメール送信を行えるため，不良率10%，歩留まり率90%程度のシステム運用で十分な成果が得られたために，ドメイン作成しなかっただけなのかもしれない．

ドメイン作成から攻撃終了までの時間

ドメイン作成から攻撃利用が終了しドメインが使い捨てられるまでの期間を解析する．ここでの攻撃の終了とは，DNSの有効な応答がなくなるまでの期間とする．したがって実際にはそれよりも短い期間でサイトとしての機能が停止してしまっている場合や，防御側としてのレジストラによる対策の影響が含まれている可能性もある．

図-18はドメイン作成から攻撃終了までの日数の割合を表す．ドメイン作成から攻撃終了までの期間は2日から7日以内のものが全体の80%程度を占めている．つまりドメイン作成から1週間以内に攻撃終了するドメインが非常に多い結果になっている．

次にZeuS/zbotに限定した場合には図-19のようになる．ドメイン作成から攻撃終了まで期間が短くなる傾向がさらに強まり，2日から3日でほとんどの攻撃が終了している．

このような特性から，効果的な対策を実施するには，攻撃検出から1日以内に対策を実施する必要があるということになる．また，これらの結果は1つのドメインを利用した攻撃がこの期間で終了するという意味であり，攻撃活動全体としては，毎日数百の新しいドメインが作成され並行して攻撃が行われている．攻撃自体は常に継続しているため，次々に作成される関連ドメインすべてに同様の短期間での対策を実施する必要がある．また，前述のように防御側としてのレジストラが，不正な利用の情報をもとに該当のドメインを利用不可能な状態にする対策が行われていることがある．レジストラによる短期間での利用停止は非常に効果的な対策であるが，中途半端な運用が行われた場合には，逆に攻撃者はとってはドメイン作成から数日で自動的に削除される期間限定利用ドメインとして利用できることになってしまう恐れがある．したがってドメインが簡単に大量に作成できる状況を改善しない限りはこれらの攻撃への対策に実質的な効果をあげることはできないのではないかと思われる．

Aレコードの変化

図-9で例に挙げたZeuS/zbotで利用されるドメインに登録されていたAレコードの特徴を観察した結果，1つのドメインに登録されているAレコードは15個，攻撃を検出してから24時間程度でこれらのドメインは利用されなくなる．その間登録されていたAレコードは次々に変化し1つのドメインで利用されたIPアドレスは合計で65個観測された．さらに同一の期間に309個のドメインが同じ攻撃に利用されており，全体で利用されたIPアドレスの総数は165個であった．大量のAレコードを持つドメインを，複数並行して運用することで，IPアドレスベースでのフィルタリング，ドメイン名ベースでのフィルタリングという2つの対策の効果を弱めるための手法である．IPアドレスの総数が数百を超えて全体像を把握することができないほど大量な場合もあり，また，攻撃に利用されているドメインすべてを補足することもほぼ不可能である．

結論

このように最近流行している攻撃に関連するシステムは，同時並行で大量に現れては，短期間で消滅したり，構成要素を次々と入れ替えたりしながら変化し続けていく．したがってハニーポットやマルウェア解析により得られた情報が，その時点でのインターネット全体の傾向を示しているのか，それとも特定の国，特定のAS，特定の組織，企業だけでしか観測されない特異な事象なのか判断が難しい．そして，その事象が最新のものなのか，それともすでに効力を失った残骸なのか，あるいは，実は解析を混乱させるためのおとりであるのかなど得られた情報の理解とその扱いが非常に難しい場面が増えている．このように判断を複雑にし，迷わせること自体が攻撃の一部でもあるので，それらに惑わされず，適切な解析，判断をもとにした対策および情報発信をタイムリーに行うためには，より多角的な視点で物事を見る個の力とそのような異なる視点を持つさまざまな人，組織との連携が必要となるであろう．マルウェアの観察は日々発見の毎日である．

(平成21年12月31日受付)

須藤年章
sudo@mfeed.ad.jp
OCN立ち上げ時よりネットワーク設計，構築に携わり，その後サービス開発，ISP運用を通してセキュリティ関連の業務を行うとともにTelecom-ISAC Japan等の活動に参加しISP運用者の立場でさまざまなインターネットセキュリティ問題の分析，対策を行う．