デジタルプラクティス　Vol.9 No.3 (July 2018)

特集招待論文

歴史を紐解くセキュリティ技術，その現在，そして未来

中尾 康二[1]

[1]情報通信研究機構

近年のセキュリティ技術を紐解くために，インターネットの歴史，マルウェアの歴史を概観する．また，侵入検知システム，マルウェア解析，攻撃モニタリング技術などのセキュリティ技術の過去，現在をまとめ，今後の課題について述べ，さらに今後の新しいインフラ環境における多様化，高度化，複雑化する脅威に鑑み，将来に向けたセキュリティ技術の在り方，方向性についても言及する．なお，本稿は，上記のような歴史的背景や現状のセキュリティ技術に基づき，本特集号を構成するほかの論文のガイド的な位置づけになるものである．

1. はじめに

セキュリティという言葉は，いろいろな側面で利用される．具体的には，非常に広義の意味の「サイバーセキュリティ」，情報に視点においた「情報セキュリティ」，インターネットのみを対象とした「インターネットセキュリティ」，物理的なリスクに対応する「物理セキュリティ」，暗号などで代表される「基盤的セキュリティ」などが主に挙げられるが，本稿では，インターネットを含めた広義のサイバー空間に必要となるセキュリティ技術に限定して議論をしたい．

セキュリティは，第3章で述べるマルウェアとの「イタチごっこ」の戦いの歴史により語られるといっても過言ではない．それは，第2章で述べるインターネットの歴史と深く関係する．さらに，インターネットが世界の情報通信インフラとして成熟した後においても，インターネットを活用するといった視点で，重要インフラやIoT活用など多種多様な環境が登場し，セキュリティにかかわる脅威を大きく増大させており，さらにネットバンキング，ネットショッピングなど，インターネットのインフラ上で利用されるアプリケーションやサービスにおいても，その脆弱性を狙った攻撃が後を絶たない状況になっている．

すなわち，情報通信インフラ，システムやサービス等に内在する脆弱性，弱点などをついた攻撃が発生し，それら攻撃に対抗するためのセキュリティ技術が（後追い的に）開発されてきたといえる．近年では，非常に高度なコンピュータシステムや通信技術の技能を保有している攻撃者（悪い意味のハッカー）がいる一方，既存のマルウェアを模倣し，既存の攻撃作成ツールを用いて，高いスキルがないものでも攻撃を行うことができる状況にあり，高度な攻撃から既存攻撃手法を模倣するレベルの攻撃まで広範囲の攻撃に対し，セキュリティ技術を用いた総合的な対策が

必要になってきている．いずれにしろ，人間が設計するインフラ，サービス，アプリケーション，さらに利用者が人間であることに鑑み，攻撃者が優位な立場で攻撃を行い，それを迎え撃つ防御側が「イタチごっこ」的に後追いでセキュリティ技術を用いた対応を行うといった構図は当分の間変わらないであろう．

本稿は，第2章でセキュリティを語る上で基盤となる「インターネット」の歴史に触れ，第3章で脅威の根源となっている「マルウェアの変遷」を概観する．第4章では，脅威に関連するセキュリティ対策技術を要約し，主に「侵入検知システム」「パッシブモニタリングシステム（ダークネットやハニーポット）」「マルウェア解析」「セキュリティマネジメント」，および「インシデント対応」などのセキュリティ技術について触れる．第5章ではこれまでのセキュリティ技術の全体像を概観し，今後の新しいインフラ環境における多様化，高度化，複雑化する脅威に鑑み，将来に向けたセキュリティ技術の在り方，その方向性についても言及する．

2. インターネットの歴史

1960年にインターネットの原型となる考え方が登場した後，今やその利用の拡大は想像以上に多様化，高度化し，世界中の人々がビジネスだけではなく，個人の余暇も含め，インターネットなくしては成り立たなくなっている．その反面，インターネットを用いた環境におけるセキュリティに関連する脅威（攻撃など）も年々増加し，また高度化，多様化しているのが現状である．本章では，セキュリティ上の脅威に深く起因するインターネットの歴史を概観する[1]．

1）「分散型コミュニケーションネットワーク」の提案（1960年）：計算機科学者ポール・バラン（Paul Baran）氏（米）は，大量の冗長リンクを持つ分散型コミュニケーションネットワークを考案．現代のインターネットの概念を提案．

2）「パケット交換理論」の考案（1968年）：計算機科学者しドナルド・デービス（Donald Davis）氏（英）は，これまでの「回線交換」とは異なる「パケット交換理論」を考案．パケット交換は，現代のインターネット技術の基本となる．

3）「インターネット」の起源（1969年）：米国防総省（ペンタゴン）の機関である国防高等研究計画局（DARPA）は，パケット交換理論に基づく分散コンピューティングネットワークの構築を行った．これは，パケット通信ネットワーク「ARPANET」と呼ばれ，世界で初めて運用され，1969年10月29日の22時30分に初めてパケットが送信された（**図1**）．

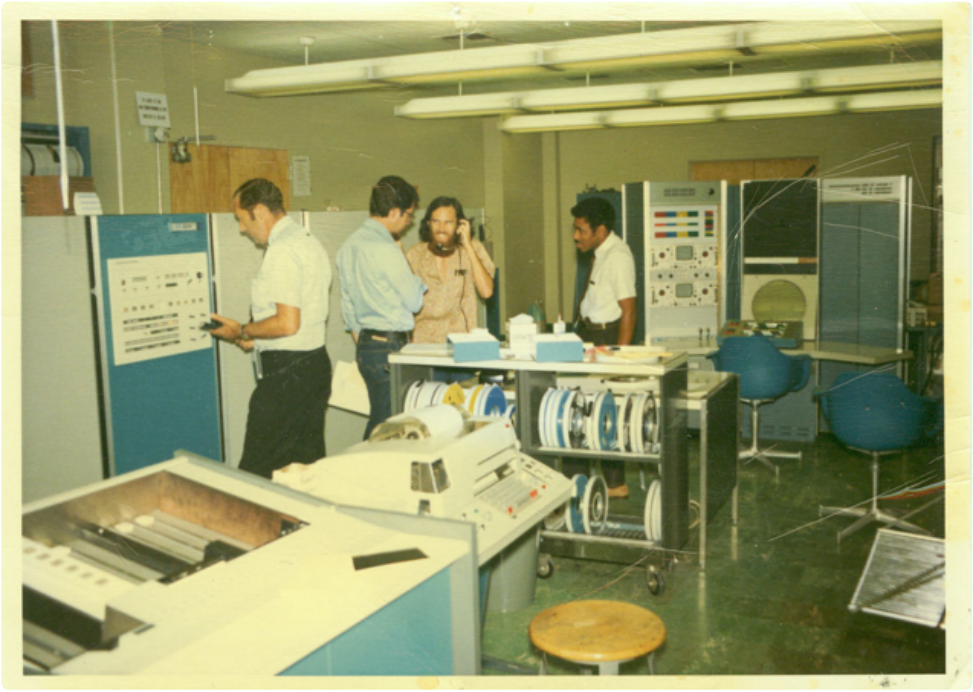

図1　ARPANETによる実験風景[1]

4）TCP/IPプロトコル（1978年）：「インターネットの父」の1人と呼ばれるヴィントン・サーフ（Vinton Cerf）氏とロバート・カーン（Robert Kahn）氏は，現在のインターネットの基礎となっている，TCP（トランスミッション・コントロール・プロトコル）とIP（インターネット・プロトコル）による「TCP/IP」の構築を行った．

5）インターネットの誕生（1983年）：ARPANETは，TCP/IPを介してユーザ同士が通信できるネットワークの世界標準を提案．ここで，パケット通信，および分散コンピューティングネットワークに基づく実用システムとなる「インターネット」が誕生．

6）米国議会での法令制定（1986年）：米国議会ではデータの盗難や不正なネットワークアクセスなどの不正行為を警戒し，これらのコンピュータ関連の犯罪行為に対して，法的制裁を与える法案「コンピュータ不正行為防止法」を1986年に制定．（なお，日本の「不正アクセス禁止法」の法制化は2000年）．

7）大規模ワーム（Morris Worm）の登場（1988年）：ロバート・T・モリス（Robert・T・Morris）氏（当時，コーネル大学在学）は，インターネットワーム（Morris wormと呼ばれる）を作成し，当時インターネットに接続されていた機器に感染し，その内10%にあたる数千台をクラッシュさせた．本ワームは，初めてバッファーオーバーフローを使用．モリス氏は米国のコンピュータ不正行為防止法により，初めて有罪判決を受けた．

8）WWWの登場（1991年）：欧州原子核研究機構 （CERN） のティム・バーナーズ＝リー（Tim Berners-Lee）氏は，1990年，世界初のWebブラウザと世界初のWWWサーバを構築．1991年，彼は WWW プロジェクトを公開し，WWWがインターネット上で利用可能なサービスとして初めて登場した．

9）革新的なブラウザ登場（1992年）：イリノイ大学の米国立スーパーコンピュータ応用研究所 （NCSA） によって，現在のように画像なども扱える革新的なブラウザ Mosaic が開発され，WWW は手軽に使うことのできるメディアとなる．一方で，本普及は，セキュリティ脅威が本格的なものとなるきっかけを与えた．

10）Webのアニメーション化（1996年）：Flashなどの新しい描画ツールやアニメーションツールやWeb拡張機能の登場し，Webブラウザは劇的に機能拡大．しかし，これらを悪用し，遠隔からのコンピュータ操作などを行う攻撃に繋がることとなる．

11）マルウェアの拡散の時代に（1996年以降）：世界的な利用が進むインターネットの環境は，犯罪を含めた悪事を働くもの（ハッカーなど）にとって，格好の場所となっていく．数千万人が感染したとされる2000年の「ラブレターウィルス」に代表されるように，インターネット利用者を攻撃対象として，多くのマルウェアが登場し，悪事に使われることとなる（第3章参照）．

12）インターネットの世界的定着（2003年から）：世界中にインターネットが浸透し，爆発的なインターネット利用が確認された時期．インターネットは金融，ネットショッピングなど多くのビジネスのインフラとなっただけでなく，多くの一般利用者の間でメール，Webを中心に利用され始めた．

13）モバイルデバイスの登場（2007年）：2007年にAppleによる初代iPhoneが発売され，2008年にはGoogleによるAndroidスマートフォンが発売され，モバイルデバイスの需要が加速．インターネットに接続される機器を持ち歩く時代に突入した時期．

14）インターネットの活用の爆発（2010年以降）：産業制御系システム，クラウドコンピューティング，IoT，車など，多くの環境において何らかの形でインターネットが利用される．2010年以前は発見される脆弱性の数は多くはなく，それらを管理運用する（登録管理／パッチ対応後の脆弱性公開など）ことが可能であったが，2010年以降，インターネット上に運用されるサービス，アプリケーション，機器が爆発的に増大し，発見される脆弱性についても，管理できない状態になっているといわれている．

3. マルウェア（ウィルス）

3.1 マルウェアとは

最近，不正なプログラム（コード）を「マルウェア」と総称して呼ぶことが多いが，単に「（広義の）ウィルス」と呼ばれることも多い．歴史的には，「ウィルス」という言葉は，1983年11月，フレッド・コーエン（Fred Cohen）氏が自己複製するコンピュータ・プログラムを初めて「ウィルス」と呼び，1984年には，コンピュータ・ウィルスを「ほかのプログラムを書き換えて，自分自身をコピーするという手法で『感染』するプログラム」と定義した．コンピュータ・ウィルスの拡散を「感染」と初めて呼んだのもコーエン氏である．「ウィルス」の言葉の定義を正確に記載すること自身に意味はなく，総括的に不正なプログラムをウィルスやマルウェアと呼称しているのが現状である．しかしながら，マルウェアに関連する用語がいろいろと使われているため，それらの意味を以下に整理することとしたい．

ワーム：単体で動作し自己増殖を行い，感染能力を持ち，大規模感染を引き起こす潜在力を持つ．感染経路としては，電子メール，リムーバブルメディア（USBメモリ等）などがあり，OSやアプリケーションの脆弱性に対する攻撃コードを用いたり，Windowsのファイル共有やメッセージング機能を利用したりする．
トロイの木馬：有用なプログラムやファイルに偽装し，ユーザ自身によるシステムへのインストールや起動を誘発するが，感染機能をもたないものが多い．
スパイウェア：個人情報や個人の行動履歴などの情報を収集し，それらを特定のサーバなどに送

信する．ユーザのキーボード操作を記録・収集するキーロガーもこの種のマルウェア．
アドウェア：ユーザの画面に企業広告などを表示し，ユーザへの同意なしで広告をホップアップし，Webサイトに強制誘導する特徴がある．
ランサムウェア：ユーザのPCに保存されるデータを強制的に暗号化，またはパスワード付きZIP圧縮し，データ復号鍵や圧縮解凍コードの提供の見返りとして，ユーザから身代金（多くは仮想通貨を利用）を搾取する．
スケアウェア：ユーザに対し，マルウェア感染やPCの汚染などの虚偽情報を提示し，ユーザの不安（Scare）を煽り，無意味な感染駆除などのソフトウェアを販売する．
ボット：パソコンに感染し，指令サーバ（C2と呼ばれる）からの遠隔操作により，DDoS攻撃，情報搾取，感染活動などを行うマルウェアの総称．それがネットワーク化していることから，その全体をボットネットと呼ぶ．

3.2　マルウェアの歴史

3.2.1　メインフレームの時代のマルウェア

1971年，BBNテクノロジーズ社のボブ・トーマス（Bob Thomas）氏により，初期の自己複製型プログラムの1つ「クリーパー」が作成（DEC社／PDP-10上）された[2]．1974年，複数の自己複製を行う「ラビット」が作成され，世界初のトロイの木馬と見なされた．

3.2.2　パーソナルコンピュータ時代のウィルス

1981年，リチャード・スクレンタ（Richard Skrenta）氏が初のパーソナルコンピュータ（Apple II向け）のウィルス，「Elk Cloner」を作成． フロッピーディスクのブートセクタを利用．
1987年，MS-DOSの実行ファイルに感染するウィルス，Vienna virusが発見された．同年，初のウィルス対策（アンチウィルス）ソフトウェアが開発された[3]．
1987年以降，パーソナルコンピュータで動作するさまざまなコンピュータウィルスが作成・発見されており，以下は主なものの抜粋．
1987年，プログラムの主要部分が暗号化された初めてのウィルス，「Cascade」が発見された．
1987年10月，「13日の金曜日」にすべての実行ファイルを破壊する，「エルサレム・ウィルス」が発見された．
1987年12月，電子メール（と電話帳）を利用して広がるウィルス，「Christmas Tree EXEC」が発見された．
1988年11月，ロバート・T・モリス氏による，「Morris worm」が発生（第2章参照）．
1989年，マッキントッシュの「DESKTOP」という隠しファイルに感染する，「WDEF」が発見された．
1990年，コード機能は変えずに変化するポリモルフィックコードを用いたウィルス「1260」が発見された．
1995年，Microsoft Wordをターゲットとした，初のマクロウィルスである「Concept」が作成された．

3.2.3　メールやファイル共有ソフトを使うウィルス

1999年，Microsoft Outlook ExpressとInternet Explorerを利用したワーム，「Happy99」が発見された．
1999年， Microsoft Outlookを利用したウィルス「Melissa」が発見され，多くの亜種が作成された．
2000年，数時間で世界中に拡散した，ウィルス「LOVELETTER」が発見された．
2001年，メール添付でOutlookのアドレス帳のユーザに拡散するウィルス，「Anna Kournikova」が発見された．
2001年7月，Microsoft IISの脆弱性を利用して感染する，「Code Red」が発見され，世界中へ拡散された．
2001年9月，Microsoft IISの脆弱性を利用し，数多くの感染手段を保有する，「Nimda」が発

見された．
2001年10月，Outlook Expressをプレビューしただけで感染する，「クレズ（Klez）」が発見された．
2003年1月，Microsoft SQL Serverのセキュリティホールを狙ったワーム，「SQL Slammer」が発見された [4]．
2003年8月，Windows XPとWindows 2000の脆弱性（TCPポート135）を狙うワーム，「Blaster」が発見された．脆弱性未対策PCでは接続するだけで感染した．
2003年8月，メールの添付ファイルを開くことで広範に感染するウィルス，「Sobig」が発見された．
2003年8月，ファイル共有ソフトWinnyなどをターゲットにしたウィルス，「Antinny」が発生した．パソコン内のファイルを勝手に共有フォルダに入れる機能を保有．
2003年11月，Windowsの脆弱性を利用し，IRC型のバックドアを仕込む，ボット型「Agobot」が発見された．
2004年1月，メールの添付ファイルやP2Pソフトを通じて感染する，「MyDoom」が発見された．感染は非常に速く，「Sobig.F」を越える過去最悪規模となった．
2004年5月，Microsoft Windowsの脆弱性を利用した「Sasser」が発見された．他ウィルスを除去する特徴あり．
2004年6月，携帯電話をターゲットとした初のワーム，「Cabir」が発見された．Symbian OSをターゲットとし，無線通信Bluetoothを通じて感染．
2005年3月，携帯電話のMMSを狙った初のウィルス，「Commwarrior-A」が発見された．
2006年2月，2001年にリリースされたMac OS Xをターゲットとした初のウィルス，「Leap」が発見された．
2006年9月，感染後，改良版ウィルスを自動ダウンロードする機能を保有する，「Stration」が発見された．このためウィルス定義ファイルで検出するのが困難化．
2007年7月，Microsoft Windowsをターゲットにしたトロイの木馬作成ツール，Zeusが出現．Zeusで作られたマルウェア「Zbot」は，銀行口座情報を詐取．2008年頃から感染が拡大．
2008年11月，Microsoft Windows 2000やWindows 7ベータの脆弱性を用いたワーム，「Conficker」が発見され，1,000万台以上のシステムに影響を与えた．

3.2.4　産業制御系システムなどをターゲットとするサイバーテロ

2009年7月4日，電子メールを利用して広まった，「W32.Dozer」により，アメリカ合衆国と韓国に対して大規模なサイバーテロ（DDoS攻撃）が発生．
2010年1月，感染したパソコンを スパムボットに変える，「Waledac」が発見され，数十万台に感染．Microsoftは，277個のボットドメイン遮断で，抑え込みに成功[5]．
2010年6月，産業制御システムSCADAをターゲットにした初のワーム，「Stuxnet」が発見された．制御系システムへのセキュリティ脅威が注目された．
2011年7月，Microsoft WindowsのRemote Desktop Protocolを利用するウィルス，「Morto」が発見された．
2012年5月，中東の政府機関・研究機関をターゲットにしたと思われるマルウェア，「Flame」が発見された．
2012年8月，中東のエネルギー関連施設（制御系）をターゲットにしたとみられるマルウェア，「Shamoon」が発見された．ワークステーション3万台が攻撃を受けた．

3.3　マルウェアの変遷

3.2節では，感染力が高く注目を集めたものや新しいマルウェア機能が作成されたものなどを中心に紹介したが，1971年から1980年前半あたりまでのマルウェアは，「可能性を探ること」が目的で，発見されたマルウェア数も多くない．その後1998年ごろまでマルウェアは次のステップに進み，マルウェアの実用性や機能性を確かめるために，「実験的な試行」を目的とする形に変遷している．その後，インターネットの発展と同期するように，多種多様なマルウェアが作

成され，徐々に「犯罪目的（主に金銭）」のマルウェアが増加した．また，2003年以降，多くのパーソナルコンピュータにボット型のマルウェアが感染し，多種多様な攻撃（DDoSや情報詐取など）に利用する手法（ボットネット）が主流となってきた．2009年以降は，金銭目的のマルウェアだけではなく，産業制御システムや政府を標的としたサイバー攻撃にマルウェアが利用されるようになった．本攻撃は「標的型攻撃」と呼ばれ，ボット型の攻撃とは異なり，攻撃先となるターゲットを決め，マルウェアを用いてターゲットに侵入し，実際の攻撃は攻撃者（人間）によって実行され，政府機関などの重要な情報詐取が主な目的となってきた．

2013年以降，マルウェアの数は激増の一途をたどっており，1つのマルウェアに多くの亜種が出現する．特に，2014年以降は，ランサムウェアが多く流行しており，「CryptoLocker（2014年）」，「TeslaCrypt（2015年）」，「Locky（2016年）」などが有名．当初のランサムウェアは言語的問題で日本をターゲットとすることは少なかったものの，徐々に多言語対応が進み，2017年には28カ国言語対応（日本語も含む）のWannaCryが世界中に猛威を振るった記憶は新しい．2018年に入り，世界全体で一日に発生するマルウェア数は，300,000を超えていると言われており，それらへの対策がますます難しくなっている現状にある．

4. セキュリティ技術

4.1 はじめに

上述したインターネット，およびマルウェア（ウィルス）の変遷に追随する形で，数多くのセキュリティシステムが開発され，発展してきた．本節では，マルウェア対策といった視点を中心に主なセキュリティ技術について外観する．具体的には，不正な侵入を検知する侵入検知システム（IDS），マルウェアの解析技術，マルウェア捕獲やその挙動を観測するためのモニタリングシステム，組織などのためにリスクを特定，認識した上で総合的なセキュリティ対策を実施するためのセキュリティマネジメントなどについて説明する．なお，現在多くの組織で利用されているファイアーウォール（FW）[6]は，登録されたルールにしたがって外部から内部へ（または内部から外部へ）のトラヒックを遮断したり，遮断した通信ログをとったりする基本的なセキュリティシステムではあるが，本稿では詳細の説明を割愛している．

4.2 侵入検知システム（IDS）

1）IDSとは

第3章で概説したマルウェアをまずはシステム等に侵入させることが攻撃者のモチベーションであるため，その侵入を検知するためのシステム（IDS）は重要な役割を担う．IDSは，侵入の検知を行い，その検知結果をシステム管理者に通知する機能を保有するが，侵入の防御は行わない． 以下に，IDSに関連する用語がいろいろと使われているため，それらの意味を整理する．

＜IDSの種別＞

Network-based IDS（NIDS）：ネットワーク上に検知装置を設置し，ネットワークへの侵入検知をする形態．
Host-based IDS（HIDS）：ソフトウェアベースのIDS．クライアントやサーバにインストールして利用し，個々のホストへの侵入を検知する形態．
IPS（Instruction Prevention System）：IDSに防御機能がついたもの．ネットワークにインラインで導入する．

＜IDSの検知手法＞

異常検知：侵入検知の手法の1つ．通常の利用方法を学習しておき，そこから逸脱した挙動がないかを検知する．未知の攻撃も検知可能．欠点は誤判定が多いことである．
誤用検知：侵入検知の手法の1つ．既知の攻撃を定義し検知する．既知攻撃の誤検知は少ないが，未知の攻撃の検知が難しい．

2）IDSの生い立ち[7].

- **1972年，** James P. Anderson氏（米国空軍）により，ホストログの監査を行って不審な通信や動作がないかを確認する自動化ツールを初めて提唱[8]．本ツールでは，ユーザの振る舞いの統計的分析で異常を検知．
- **80年代後半，** リアルタイムに侵入を検知するモデル（IDES）が開発．本モデルはルールベースの誤用検知．
- IDSの登場初期は異常検知が主流．90年には実ネットワーク上の異常を検知するシステムが構築[9]．結果，攻撃の前段で攻撃試行が検知できる可能性が広がる．
- **90年代半ば，** 商用の誤用検知用NIDSが多く出現．新攻撃に対する定義更新が必要となり運用面が課題．
- その後， HIDSにより，ログの監査，分析をリアルタイムおよび分散して行うことが見直され，NIDSとHIDSのハイブリット利用が促進．
- **1998年，** IDSツール（snort等）や製品が多く出現．
- 現在では，専用ハードウェアによる高速化や，出力フォーマットの共通化などがIETFで行われている．

3）IDSの課題

IDSについては，現在ではNIDSを中心に，多くの組織でその活用が実施されているが，新しい攻撃パターンに追随するための定義作成の自動化が課題．また，通信環境の高度化／高速化の現状において，10Gbps程度の通信速度に耐えられるような検知能力，定義との照合処理能力の具備も必須となる．さらに，ネットワーク上の通信内容が暗号化された場合，どのような検知を考えるべきかなどといった課題も存在する．

また，異常検知などのルールの更新には機械学習などを利用した自動化も多く研究されている[10].

4.3　マルウェア解析技術

マルウェア解析は，新しく観測検知したマルウェアの挙動を解析・把握することにより，インシデント対応（4.6節）でのマルウェアによる被害状況の特定／推定などに役立てることができる．マルウェアの解析手法は，動的解析と静的解析の2つに大別できる．両手法にはメリットとデメリットがあり，実際のマルウェア解析作業では，双方のやり方を組み合わせて行うのが効果的であると考えられる．

4.3.1　動的解析（ブラックボックス解析）

ほかのシステムに影響を与えない隔離環境で，実際にマルウェアを実行して，その挙動を調べる手法．さまざまなシステムモニタリングツールが利用される．短時間で容易にマルウェア動作を把握することができるといった利点はあるものの，たとえば，日付や確率などで発症するマルウェアについては，条件が一致するような環境整備が必要となり，煩雑となる．本手法では，期待通りにマルウェアが動く環境を構築できるか否かが鍵．

4.3.2　静的解析（ホワイトボックス解析）

バイナリコードを逆アセンブルして分析する．作業の中心を担うのは逆アセンブラツールで，逆アセンブルしたコードをすべてチェックすることによりマルウェアの完全な挙動を把握することができる．ただし，それらの挙動解析にはそれ相応の時間と手間がかかるといった難点がある．静的解析は気軽にできる作業ではなく，それを実施するためにはあるレベルのスキル（OSやネットワーク，プログラミング言語など幅広い知識）が要求される．

4.3.3　マルウェア解析の課題と今後

動的解析，静的解析のいずれの方法でも，時間さえかければマルウェアの動作を細部にわたって詳細に解析できるが，1つの解析に十分な時間をかけられない．解析が長引けば，マルウェア感染が拡大し，甚大な被害をもたらす危険性がある．したがって，いかに解析時間を短縮させるかが最重要課題である．

最近では，大抵のマルウェアが難読化（静的解析を困難化）やアンチデバッギング（デバックを困難化）といった機能を持っており，さらにマルウェア解析を困難にしている．攻撃者は「パッカー」と呼ばれるツールを利用することで，容易に難読化などが施されたマルウェアの作成が可能となっている．また，マルウェアによっては，解析環境検知（アンチサンドボックス／アンチVM機能）を保有しており，これらの機能への対策も課題となる．

すべてのマルウェアの手動解析では，迅速に解析結果の提供ができないため，マルウェア挙動の自動解析が必要となる．自動化を提供するサービスも近年では多く提供されており，短時間で解析結果が入手し，マルウェアに対する初動対応に役立てている．

4.4　ダークネットやハニーポットを用いたモニタリングシステム

4.4.1　ダークネット観測

「ダークネット観測」とは，未使用のIPアドレス空間を用いて，攻撃者による不正な挙動（マルウェアによるスキャン，DDoS攻撃の跳ね返りなど）を観測し，それをセキュリティに資することを目的としており，インターネット上の大規模攻撃活動の観測に適している．特に，ネットワーク経由で感染を拡げるワーム系マルウェアの大量感染などについては，ダークネット観測ではその特徴や傾向を早い段階で把握することが可能となる．

1）ダークネット観測の現状

2000年初期から，米国ミシガン大学のプロジェクトが発端となったArbor Networksプロジェクトでは，複数の/16のIPアドレス空間をダークネット観測に活用し，主に研究活動を実施していた．

2005年から，情報通信研究機構（NICT）ではダークネットに基づくインターネット上のトラヒック観測を行っており，観測した情報に基づき，スキャン手法，スキャン元アドレス，利用するポート番号などの情報から，該スキャンに関連するマルウェアを導出する相関分析などの研究を行っている．現在，NICTでは30万アドレスのダークネット空間で観測を進めており，ダークネットで観測したトラヒック量は年々倍増している．2016年の年間観測パケットは1,280億個を超えており，2017年はさらに大きく増加している．

2）IoT機器へのスキャンやDDoS攻撃の観測

2013年まではMicrosoft Windowsの脆弱性を狙ったスキャンが主流であったが，2014年以降は，徐々にIoT機器に関連するスキャンが増加する[11]．2016年のダークネット観測データによると，全スキャンの60％以上はIoT機器（IoT機器使用のポート）を狙ったものであった．本

現象は，マルウェア感染した多数のIoT機器が脆弱なIoT機器探索を実施している推測される．

一方，ダークネット観測を用いると，送信元IPアドレス偽装されたSYN-Flood 攻撃（DDoS）の跳ね返り（DDoS攻撃の標的からの応答（SYN-ACK））を実時間で観測できるため，これらの検知情報をDDoS攻撃早期対応などに活用することが可能となる．

4.4.2　ハニーポット技術

ハニーポットは，攻撃者の標的となるシステムを模倣した「おとり」を用いることで，第3章で述べたマルウェアを捕獲し，マルウェア本体やその侵入方法を解析することを主な目的とする．また，不正アクセスなどを行う攻撃者をおびき寄せ重要なシステムから攻撃をそらしたり，リフレクション型DDoSのリフレクタを模倣したハニーポットでは，実際のDDoS攻撃を受けることで，早期のタイミングでDDoS攻撃を把握できる．さらに，広域にハニーポットを設置することにより，それらに記録された操作ログ・通信ログなどの情報から，世の中で広く蔓延しているマルウェア侵入方法やそれらの傾向分析を行うことも目的となる．以下に，ハニーポット技術を概観する．

1）ハニーポットの基本技術

一般的なハニーポットシステムは，オペレーティングシステム （OS） やアプリケーションに脆弱性を残して攻撃を受ける機能（おとり機能），受けた攻撃によって外部への踏み台とならないための通信制御機能，および攻撃者の不正アクセスなどを適切に記録する機能（通信ログも含む）によって構成される．

2）ハニーポットの種別

A） 高対話型ハニーポット

実際に脆弱性を残した「被害ホストと同等」のOSやアプリケーションなどをハニーポットとして利用する．このため，情報収集能力は高い反面，侵入されたときのリスクが高い．

B）低対話型ハニーポット

特定のOSやアプリケーションをエミュレートし監視を行う．エミュレートした範囲に機能が制限されるため，情報収集能力は低い反面，高対話型に比べ比較的安全に（感染しないで）運用ができる．

3）ハニーポットの運用方法

- **ハニーネット**：ハニーポットを複数台設置し，それらをネットワークとして管理・解析する手法．ネットワークに流れるパケットや複数台のハニーポットの挙動を総合的に解析し，攻撃者の手口を明らかにすることが目的．
- **仮想ハニーポット**：仮想マシン（VMwareやXenなど）で構成されたハニーポット．仮想マシンを用いることで，ハニーポットを侵入前の状態を戻すなど，管理が容易である利点あり．動作環境が仮想マシンかを検証するマルウェアは分析できないのが欠点．
- **ハニーポットファーム**：ハニーポット用の管理ネットワークを用いて，遠隔地の監視を行う．侵入に伴うリスクを集中することができ，複数個所（物理的に遠隔地）にハニーポットを設置することをせずに監視が可能．

4）近年のハニーポット技術

攻撃者が用いる侵入挙動を解析する方法として，実際のシステムに侵入される前に，ハニーポット技術を用いた解析を行うことで，マルウェア挙動などを事前に把握でき，早期の対策を打てるようになってきている．しかしながら，高度な攻撃者はハニーポット検知機能をマルウェアに搭載し，ハニーポットでの解析を回避する等，ある意味攻撃者と解析者のイタチごっことなっている．

さらに，近年では，リフレクション型DDoS検知用，IoT機器への感染解析用など，攻撃種別や応用に特化した目的のハニーポットが多く開発されており，攻撃早期警戒などに一定の効果を上げている．

4.5　セキュリティマネジメント

組織やサプライチェーンにおいて，内在するセキュリティ上のリスクを特定し，それらのリスクを低減するためのセキュリティ対策を策定・決定し，その対策の有効性を評価し，さらに組織の目標にあった効果的なセキュリティ対策に向けて改善するために管理・運用することを「セキュリティマネジメントを実施する」という．セキュリティ対策には人的な対策（人材育成を含む），物理的な対策，管理上の対策，技術的な対策があるが，近年では，変化の激しい脅威（攻撃）の環境などに鑑み，組織におけるリスクを把握することが重要となり，把握されたリスク低減のため，環境の変化に合わせて適切なセキュリティ対策を動的に配備することが重要になっている．

4.6　インシデント対応

1）インシデント対応とは

情報漏えいやシステム停止などの攻撃に起因するインシデントが発生した際の対応を迅速かつ適切に行えるよう，平時からその準備や対策を配備すること．あらかじめ侵入や被害を受けることを前提として，その検知と初動対策に注力することで被害を最小化することを狙っている．なお，上記のセキュリティマネジメント（4.5節）においても，インシデント対応は重要な対策となっている．以下に，本節に関連する用語を以下に整理する．

SOC（セキュリティ・オペレーション・センター）：組織に設置するファイアウォールや侵入検知システム， ネットワーク機器や端末のログなどを常時監視し，インシデントの発見や特定，連絡を行う役割の専門組織．

CSIRT（Computer Security Incident Response Team，シーサート）：主にインシデントレスポンスを実施する組織．すなわち，ウィルス感染，不正アクセス，情報漏えいなどのセキュリティを脅かしている事象およびインシデントに対して，原因の調査，対応策の検討，サービス復旧などを適切に行うことが主務．たとえば，内閣官房内にある緊急対応支援チーム（NIRT：National Incident Response Team）は，CSIRTとして位置づけられる．

なお，インシデント対応を行う組織名称に，しばしば「**CERT（Computer Emergency Response Team）**」を用いるが，CERTはCMU商標で認可が必要であり，一般名称としては，「CSIRT」が使用される．ただし，日本には認可を受けているJPCERT/CCやNTT-CERTが存在する．

2）インシデント対応における課題

近年，インシデント対応の重要性が増加し，多くの組織にSOCやCSIRTの機能が実装されている．しかしながら，多くの組織でインシデントを監視し，発見する手法は，既存のセキュリティ機器であったり，監視機器であるため，高度な（新種の）攻撃によるインシデントの対応が遅れ，組織への実被害がでてしまう例も多い．したがって，最新の脅威情報，攻撃手法などを十分に調査・把握し，インシデント対応をより効果的に実施することが鍵となり，そのためには高いスキルと経験も必要となる．

4.7　電子認証技術

本稿の目的の1つとして，本特集号を構成するほかの論文のガイド的な位置づけになることがあるため，これまで解説していない「電子認証技術」について，以下に簡単に解説する．**電子認証技術**とは，通信相手の正当性を確認するために，電子認証局から発行される「電子証明書」を用いて，なりすましの防止や情報の改ざんを防止する技術．本技術により，現実世界で物理的に実施されている署名，捺印などの業務を安全に電子化することができ，近年では，電子契約書，電子請求書，電子議事録，電子稟議書などの多くの応用において，電子認証技術が活用されており，さらに，電子的に保存する文書や電子申込書などにおいても，文書の作成者の真正性を保証するための技術として利用されている．

5. 今後のセキュリティ

インターネット，マルウェア，セキュリティ技術につき，上記に概観した．近年，脅威環境（攻撃の多様化など）は非常に複雑になっており，誰一人，脅威の全体像を把握できていない現状がある．さらに，攻撃と防御が「イタチごっこ」であることに加え，攻撃者の保有能力と防御側の能力には乖離があり，常に攻撃側が優位に立っているといえる．近年の高度な攻撃をしかける攻撃者集団では，セキュリティ機器の解析・調査だけではなく，攻撃モジュールの自動化開発を遂行するための十分な資金力もあり，防御側との技術的な差がさらにひらく．

これに対抗するためには，個別に活動している防御側は連携することが必須となり，脆弱性情報の迅速な連携共有，フレッシュな不正ドメイン／IPアドレスの共有化，国際的に連携したハニーポット配備などによる，攻撃挙動の連携観測などの実施が鍵となる対策となろう．一例として，セキュリティベンダ，OSベンダ，大学，警察組織などの組織が連携して，悪性サーバ（ボットネットC2等）のテイクダウンを行った事例があり，Operation B49（Waledac対策（3.2.4項），Operation B71（Zeus対策）などが有名である．また，セクタ（エネルギー，通信，金融など）においては，ISAC（Information Sharing and Analysis Center）の活動強化，および異なるISAC間の連携が重要となろう．さらに，個々の組織においては，上述の人材育成の強化等のセキュリティマネジメントの適正実施が必須となるが，組織のインシデント対応能力をさらに向上にするために，インシデント発生後の耐久力（レジリアンス）の強化，たとえば攻撃の影響を最小化などの実施も肝要となろう．

最後に，本特集号を構成する他論文の主テーマである，SOC構築，標的型攻撃，インシデント対応，CSIRT，人材育成，および電子認証技術については，第3章～第4章において概説した．

謝辞　本稿作成にご協力いただいた，星澤裕二氏（PwC），中里純二氏（NICT），吉岡克則氏（横浜国立大学），秋山満昭氏（NTT研究所）に深謝いたします．

参考文献

1）A history of Internet security - Washington Post,
http://www.washingtonpost.com/graphics/national/security-of-the-internet/history/
2） The Evolution of Viruses and Worms (2004),
https://www.researchgate.net/publication/228869267_The_Evolution_of_Viruses_and_Worms
3) SECURE LIST : History of malicious programs 1987,
http://www.securelist.com/en/threats/detect?chapter=108
4）The Spread of the Sapphire/Slammer Worm,
http://www.caida.org/publications/papers/2003/sapphire/sapphire.html
5） IT Pro : Microsoft，ボットネット「Waledac」の通信遮断で「大きな成果」(2010年2月26日),
http://itpro.nikkeibp.co.jp/article/NEWS/20100226/345119/
6）総務省：国民のための情報セキュリティサイト,
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security_previous/kiso/k01_firewall.htm
7）Bruneau, G. : The History and Evolution of Intrusion Detection, SANS Institute InfoSec Reading Room (2001),
https://www.sans.org/reading-room/whitepapers/detection/history-evolution-intrusion-detection-344
8）Anderson, J. P. : Computer Security Threat Monitoring and Surveillance,
http://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf
9）Heberlein, L. T., Dias, G. V., Levitt, K. N., Mukherjee, B., Wood, J. and Wolber, D. : A Network Security Monitor, in Proc. IEEE Computer Society Symposium on Research in Security and Privacy, pp.296-304 (1990),
10) Axelsson, S. : Intrusion Detection Systems : A Survey and Taxonomy, Technical Report 99-15, Department of Computer Engineering, Chalmers University of Technology (Mar. 2000).
http://neuro.bstu.by/ai/To-dom/My_research/Paper-0-again/For-research/D-mining/Anomaly-D/Intrusion-detection/taxonomy.pdf
11) 笠間貴弘，井上大介：大規模ダークネット観測と能動スキャンによるマルウェア感染IoT機器の分類，情報処理学会論文誌，Vol.58, No.9, pp.1388-1396 (Sep. 2017).

中尾 康二（正会員）ko-nakao@nict.go.jp
1979年早稲田大学卒業後，国際電信電話（株）に入社．KDD研究所を経て，現在KDDI（株）顧問，および研国立研究開発法人情報通信研究機構（NICT）サイバーセキュリティ研究所　主管研究員，横浜国立大学　客員教授を兼務．ネットワークおよびシステムを中心とした情報セキュリティ技術／サイバーセキュリティ技術の研究開発に従事．電子情報通信学会会員．経済産業省大臣表彰賞，KPMG情報セキュリティアワード，文部科学省大臣表彰賞，情報セキュリティ文化賞，総務大臣表彰等を受賞．

投稿受付：2018年3月6日
採録決定：2018年4月18日
編集担当：今原修一郎（（株）東芝）