実　践
サイバーセキュリティ
モニタリング

八木　　毅
青木　一史
秋山　満昭
幾世　知範
髙田　雄太
千葉　大紀

コ ロ ナ 社

ま　え　が　き

インターネットは，すでに生活に欠かせない水道や電気のようなサービスインフラになっている。パソコンやスマートフォンなどの端末を使えば，Web やメール等のさまざまなサービスを，Web サーバやメールサーバ等を経由して利用できる。しかし，このような利便性を重視した状況は，社会的に重要なサービスや個人情報がインターネット上で活用される文化を作り出した。この結果，インターネットに存在してきたサイバー攻撃の目的が，愉快犯やサービス妨害から，金銭目的や軍事目的へと変化してきた。

サイバー攻撃には，情報を収集する攻撃やサービスの提供を妨害する攻撃などが存在するが，多くの攻撃にはマルウェアが利用される。マルウェア（malware）とは，悪意ある（malicious）ソフトウェア（software）を意味する造語で，代表例としてコンピュータウィルスが挙げられる。攻撃者は，端末やサーバをマルウェアに感染させ，不正に操作することで，情報を収集するだけでなく，さまざまなサイバー攻撃の発信元として利用する。すなわち，マルウェア感染を防止することができれば，多くのサイバー攻撃を防ぐことができる。

本書では，マルウェア感染攻撃を中心に，攻撃を観測して解析する技術を，演習を交えて解説する。本書は，サイバーセキュリティ分野のみでなく，サイバー攻撃対策を必要とする多くの分野において将来活躍が期待できる学生や専門家を対象に，本質的な検討方法や実践的な解析技術を学べるよう，構成されている。1 章では，本書で扱う技術の全体像を解説する。2 章から 4 章にかけて，攻撃を観測するために用いられる “おとり” のシステムである “ハニーポット” について解説する。さらに，5 章では，マルウェアを解析する技術について解説し，6 章では，攻撃を検知するためのトラヒック解析技術を解説する。また，本書の章末問題の解答や，演習を実施する際に有効となる情報の一部は，コロ

ナ社の Web ページ http://www/coronasha.co.jp/np/isbn/9784339028539/ からダウンロードできる。ダウンロードファイルのパスワードは各章に記載する。章末問題は演習を中心に構成されている。非常に有効な演習となっているため，ぜひ取り組んでいただきたい。

なお，本書では，インターネット技術やサイバー攻撃の基礎知識を前提に解説する部分がある。これらの基礎知識は，コロナ社から出版されている「コンピュータネットワークセキュリティ」[1)†]で習得できるため，参考にしていただきたい。加えて，引用文献に記載する専門書も読み解いていただきたい。

また，本書では，サイバー攻撃への対策技術を解説する際に，攻撃方法についても解説するが，当然本書で学んだ方法で他者を攻撃してはならない。対策技術の検討には攻撃方法の知識が必須ではあるが，攻撃の実践は仮想環境や閉域環境で実施すべきであり，インターネット上で実践した場合は犯罪となるため，高い倫理観を持って本書を活用いただきたい。

本書の内容を理解することで，サイバー攻撃に対応するための実践力を身につけることができる。本書が，サイバー攻撃の被害を抑制するのみでなく，サイバー攻撃対策が必要となる多くの分野における先駆者の創出や発展に貢献できることを期待する。

本書を執筆する機会を提供して頂いた大阪大学の村田正幸教授や，本書作成においてご指導頂いた早稲田大学の後藤滋樹教授や森達哉准教授，本書作成にご協力頂いた日本電信電話株式会社の針生剛男氏，矢田健氏，芝原俊樹氏に感謝の意を述べたい。

2016 年 1 月

執筆者一同

† 肩付き数字は，巻末の文献番号です。

目　　次

1. サイバー攻撃におけるマルウェア感染

2. ハニーポットでのデータ収集

3. クライアントへの攻撃とデータ解析

4. サーバへの攻撃とデータ解析

5. マルウェア解析

6.　正常・攻撃トラヒックの収集と解析

1 サイバー攻撃におけるマルウェア感染

サイバー攻撃とは，標的のコンピュータやネットワークに侵入してデータの搾取や破壊を実施したり，標的のシステムを機能不全にしたりすることである。インターネットが生活に欠かせない社会となった今，サイバー攻撃は金銭や国家機密に直接的に関わる悪質な犯罪行為となっている。多くのサイバー攻撃では，マルウェアに感染した端末やサーバが悪用されている。このため，マルウェア感染攻撃がサイバー攻撃の根源といえる。本章では，マルウェア感染を中心としたサイバー攻撃の概要や観測の重要性を，本書の構成と併せて説明する。

1.1 サイバー攻撃の仕組み

サイバー攻撃は，コンピュータネットワークを構成する端末[†1]を対象とする攻撃と，クライアントにサービスを提供するために設置されるサーバ[†2]を対象とする攻撃に大別できる。なお，通信事業者が運用しているネットワークインフラへの攻撃や，工場や発電所などの制御システムへの攻撃などが脅威となっているが，これらの攻撃に対しては，目的に応じて端末側の視点とサーバ側の視点から攻撃の影響を考慮して対策を講じることになる。

1.1.1 サイバー攻撃の対象と被害

端末への攻撃の代表例として，受信者の意図とは無関係にクライアントへ送付されるスパムメールがある。スパムメールは，不正広告の配信のみでなく，

†1 サーバの提供する機能やデータを利用する端末はクライアントと呼ばれる。本書でも，サーバとの通信を中心に解説する場面では端末をクライアントと呼ぶ。

†2 本書では，端末やサーバを区別せずにコンピュータを示す場合はホストと呼ぶ。

フィッシングサイトへユーザを誘導して銀行などのアカウント情報を不正に入手する攻撃にも利用される。さらに，スパムメールを用いて，3 章で解説する悪性な Web サイトへユーザを誘導したり，添付ファイルを実行させたりすることで，ユーザをマルウェアに感染させる場合もある。

端末への攻撃がサーバへの攻撃と連動する代表例として，Web サイトのコンテンツを書き換える Web サイト改ざんがある。この攻撃は，Web サイトが提供する情報や機能を変更してサービスを妨害する際のみでなく，閲覧ユーザを別サイトへ誘導してフィッシングやマルウェア感染を実施する際にも用いられる。なお，Web サイト改ざんは，辞書攻撃やパスワードリスト攻撃と呼ばれるような，多くのアカウント情報を用いて不正ログインを試行する攻撃が成功した際に実施される場合がある。この場合，不正ログインの脅威は不正ログインされたアカウントの権限に依存するが，管理者のアカウントで不正ログインが成功した場合，DB (DataBase) に記録されている重要な情報が漏えいする可能性や，Web サイトが他の攻撃に悪用される可能性が高くなる。なお，SQL インジェクションを利用すれば不正ログインをせずに DB の不正閲覧や不正制御が実施できる。

サーバへの攻撃の代表例として，標的に対して大量の負荷をかける DoS (Denial of Service) 攻撃がある。DoS 攻撃が発生すると，標的が提供するサービスが機能しなくなる。複数のホストから DoS 攻撃を実施する DDoS (Distributed Denial of Service) 攻撃や，DNS (Domain Name System) サーバを利用したアンプ攻撃など，DoS 攻撃はさまざまな形に進化している。

1.1.2　サイバー攻撃とマルウェア

近年，サイバー攻撃は犯罪として扱われるため，攻撃者は，他人のホストを経由して攻撃を実施することで，自身の存在を隠ぺいする。この際，オープンプロキシと呼ばれる第三者が用意した代理アクセス用サーバを経由する場合や，Tor[2)] と呼ばれるネットワークのような一般公開されているネットワークを経由する場合と，他人のホストを不正操作する場合がある。オープンプロキシや

Tor に関しては，情報が一部公開されており，攻撃を受ける側での対策が講じやすいため，近年では不正操作が攻撃の中心的な役割を担っている。

他人のホストを不正操作する多くの場面では，**マルウェア**が利用される。マルウェア (malware) とは，悪意ある (malicious) ソフトウェア (software) を意味する造語で，代表例としてコンピュータウィルスが挙げられる。攻撃者は，さまざまな手段でホストをマルウェアに感染させ，情報の漏えいや攻撃の発信に悪用する。代表的なマルウェアに**ボット** (Bot) と呼ばれるマルウェアがある。攻撃者は，ボットに感染したホストによって構築された**ボットネット**を用いて攻撃を実施する。ボットネットには，ボットマスター (botmaster) やハーダー (herder) と呼ばれる攻撃者†から指令を受けて他のボットを制御する**コマンドアンドコントロール (C&C) サーバ**と，C&C サーバから指令を受けてサイバー攻撃を実行するボットが存在する。このような複雑かつ大規模なボットネットを活用することで，攻撃者は，自身の存在を隠ぺいしつつサイバー攻撃を実施する。マルウェアに感染したホストは，情報を盗み取られるだけでなく，**図 1.1** に示すように，ボットネットに組み込まれ，攻撃元の隠ぺいのための踏み台として，別のホストに対するマルウェア感染攻撃に悪用されたり，別のサイバー攻撃に悪用されたりする。このため，サイバー攻撃においてホストをマルウェアに感染させるマルウェア感染攻撃は諸悪の根源だといえ，マルウェア対策がサイバー攻撃対策において非常に重要であるといえる。

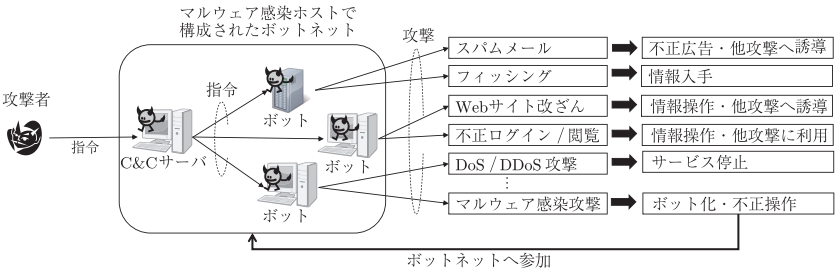

図 1.1　サイバー攻撃とマルウェア感染

† 本書では，サイバー攻撃を行う人物を一律に攻撃者と呼ぶ。

1.2　マルウェア感染攻撃の観測

マルウェア対策は，攻撃やマルウェア[†1]の特徴情報[†2]を把握し，この特徴情報と一致する動作をホスト上やネットワーク上で検知することによって実現できる。マルウェア対策には，対策を実施する目的と環境において，複数の側面が存在する。

対策を実施する目的は，マルウェア感染を未然に防止するという目的と，マルウェアに感染したホストを発見して被害を最小限に抑制するという目的に大別できる。感染を未然に防止する対策では，マルウェア感染攻撃を検知し，被害を未然に防ぐことが目的となる。マルウェアの感染経路には，USB メモリ経由や，製品出荷時における混在など，さまざまな経路が存在するが，インターネット上のホストとの通信による感染が主流である。一方，被害を最小限に抑制する対策では，感染ホストを特定し，被害の拡大を防ぐことが目的となる。多くのマルウェアは，C&C サーバに代表されるインターネット上のホストと通信し，攻撃命令の受信や収集情報の送付および追加プログラムの受信などを実施することで被害を拡大させる。なお，マルウェア感染時や感染後には，通常では発生しない処理がホスト上で実行されることが多い。このため，マルウェア対策において，ホスト上で発生する処理の観測と，他のホストとの通信の観測は，大きな役割を担う。

対策を実施する環境は，ホスト上とネットワーク上に大別できる。ホスト上での対策は，アンチウィルスソフトの適用が中心となる。端末用やサーバ用が用意されているアンチウィルスソフトは，インストールされたホスト上で，受信ファイルと既知のマルウェアとの類似性や異常処理などを監視し，監視結果に基づいてマルウェア感染を検知して制御する。一方，ネットワーク上での対

[†1] 解析対象として扱うマルウェアをマルウェア検体，または単に検体と呼ぶことがある。
[†2] 攻撃時に用いられる IP アドレスや URL，攻撃時の通信やマルウェアに用いられるバイナリ列，攻撃時にホスト上でみられるファイルアクセスやレジストリアクセスなど，幅広い情報を示す。

策は，インターネット上に存在するさまざまな機器において講じることができる。ローカル IP アドレスをグローバル IP アドレスに変換する NAT (Network Address Translator) や NAPT (Network Address Port Translator) は，ローカル IP アドレスが割り当てられた収容ホストに対するインターネットからのアクセスを制限する一方，収容ホストはインターネットからの攻撃に対して保護される。ホストに対してインターネットアクセスの代理応答機能を提供するプロキシサーバも同様の効果が期待できる。内部ネットワークと外部ネットワークの境界に設置されるエッジルータや，**ファイアウォール**や **IDS (Intrusion Detection System)** および **IPS (Intrusion Prevention System)** に代表される**セキュリティアプライアンス**では，収容ホストの通信を監視して対策を講じることができる。また，DNS サーバでは，DNS クエリやレスポンスの内容から攻撃に関わる悪性な宛先へのアクセスを制限することができる。

1.3　マルウェア対策に向けた攻撃の観測と解析

マルウェア対策を実施するためには，1.2 節で解説した目的と環境を意識しつつ，攻撃やマルウェアの特徴情報を把握する必要がある。特徴情報を把握する方法には，攻撃やマルウェアを収集して解析することで特徴情報を抽出する方法と，実際にユーザが利用しているホスト上の動作やトラヒックを解析することで攻撃を特定して特徴情報を抽出する方法がある。前者は攻撃の詳細を知ることができる反面，ユーザが利用している環境で発生している攻撃を観測できない場合がある。一方，後者はユーザが利用している環境で発生している攻撃の特徴情報を抽出できるが，巧妙化が進む攻撃トラヒックの識別が困難で攻撃の特徴情報を正確に抽出できない場合がある。マルウェア対策の実現に向けては，目的や環境に応じて両者を使い分ける必要がある。

攻撃やマルウェアを収集して解析する方法として，下記が検討されている。

- **ダークネット監視　ダークネット (darknet)**[3] は，特定のホストが割り当てられていない IP アドレス空間を意味する。ダークネット上には

索　　引

—著 者 略 歴—

八木　毅（やぎ　たけし）

2000年　千葉大学工学部電気電子工学科卒業
2002年　千葉大学大学院自然科学研究科修士課程修了
2002年　日本電信電話株式会社情報流通プラットフォーム研究所勤務
2012年　日本電信電話株式会社 NTT セキュアプラットフォーム研究所勤務
2013年　大阪大学大学院情報科学研究科博士課程修了
博士（情報科学）
2014年　日本電信電話株式会社 NTT セキュアプラットフォーム研究所主任研究員
現在に至る
〔2015 年より大阪大学招へい准教授（非常勤），早稲田大学非常勤講師，横浜国立大学 IAS（Institute of Advanced Sciences）客員研究員 (非常勤) を併任〕

青木　一史（あおき　かずふみ）

2004年　東北大学工学部情報工学科卒業
2006年　東北大学大学院情報科学研究科修士課程修了
2006年　日本電信電話株式会社情報流通プラットフォーム研究所勤務
2012年　日本電信電話株式会社 NTT セキュアプラットフォーム研究所勤務
2014年　日本電信電話株式会社 NTT セキュアプラットフォーム研究所研究主任
現在に至る

秋山　満昭（あきやま　みつあき）

2005年　立命館大学理工学部情報学科卒業
2007年　奈良先端科学技術大学院大学情報科学研究科修士課程修了
2007年　日本電信電話株式会社情報流通プラットフォーム研究所勤務
2012年　日本電信電話株式会社 NTT セキュアプラットフォーム研究所勤務
2013年　奈良先端科学技術大学院大学情報科学研究科博士課程修了
博士（工学）
2015年　日本電信電話株式会社 NTT セキュアプラットフォーム研究所研究主任
現在に至る
〔2015 年より大阪大学招へい准教授（非常勤），早稲田大学非常勤講師，横浜国立大学 IAS（Institute of Advanced Sciences）客員研究員 (非常勤) を併任〕

幾世　知範（いくせ　とものり）

2010年　豊田工業高等専門学校専攻科修了
2012年　奈良先端科学技術大学院大学情報科学研究科修士課程修了
2012年　日本電信電話株式会社 NTT セキュアプラットフォーム研究所勤務
現在に至る

髙田　雄太（たかた　ゆうた）

2011年　早稲田大学基幹理工学部情報理工学科卒業
2013年　早稲田大学基幹理工学研究科情報理工学専攻修士課程修了
2013年　日本電信電話株式会社 NTT セキュアプラットフォーム研究所勤務
現在に至る

千葉　大紀（ちば　だいき）

2011年　早稲田大学基幹理工学部情報理工学科卒業
2013年　早稲田大学基幹理工学研究科情報理工学専攻修士課程修了
2013年　日本電信電話株式会社 NTT セキュアプラットフォーム研究所勤務
現在に至る

実践サイバーセキュリティモニタリング

Practical Cybersecurity Monitoring

2016 年 4 月 18 日　初版第 1 刷発行　★

検印省略

著　者　八木　毅
青木一史
秋山満昭
幾世知範
髙田雄太
千葉大紀

発行者　株式会社　コロナ社
代表者　牛来真也

印刷所　三美印刷株式会社

112–0011　東京都文京区千石 4–46–10

発行所　株式会社　コロナ社

CORONA PUBLISHING CO., LTD.

Tokyo Japan

振替 00140–8–14844・電話(03)3941–3131(代)

ホームページ http://www.coronasha.co.jp

ISBN 978–4–339–02853–9　（森岡）　（製本：愛千製本所）

Printed in Japan