サイバー戦入門　その５

－標的型攻撃の仕組みとその対策－

三村　守（防大情報工学科）

１　はじめに

今日、数ある様々なサイバー攻撃の中でも、最も深刻な脅威となっているのは標的型攻撃であろう。標的型攻撃は特定の個人や組織を標的とし、利用者に気付かれずに秘密裏に実施されることが多い。そのため、標的型攻撃により情報を窃取されたことが数か月後に発覚する場合や、あるいは何年もの間、まったく気付かない場合すらある。このように、標的型攻撃には、サイバー空間におけるスパイ活動のような性質がある。標的型攻撃を用いたサイバースパイ活動は、必ずしも未知の脆弱性や高度なスキルを有する主体のみが実施しているわけではない。中には、脆弱性すら用いずにアイコンやファイル名を偽装して不正なプログラムを実行させたりする単純な攻撃や、攻撃元の素性を本気で隠そうとしない攻撃等、その手法は主体によって様々である。このような特定の個人や組織を狙った一連の標的型攻撃は、数か月から数年の長期間にわたって執拗に実施されることも珍しくなく、ＡＰＴ[1]あるいは新しいタイプの攻撃と呼ばれることもある。

標的型攻撃に用いられるマルウェア[2]は、主にメールを用いて対象の端末に送付される。このようにメールを用いてマルウェアを送付する手法は、かつては不特定多数を対象として用いられてきた。このような不特定多数を対象としたマルウェアは、ウイルス対策ソフトを導入し、その定義ファイル、ＯＳ、アプリケーション等を最新の状態に維持することで、ほとんど対策をとることができた。しかしながら、近年の標的型攻撃では、最新の定義ファイルを適用したウイルス対策ソフトでさえ、そのマルウェアを検知することは難しい。さらに、未知の脆弱性を用いたゼロデイ攻撃[3]を用いる場合もあり、ＯＳを最新の状態に維持していても制御が奪われてしまう場合すらある。２０１０年６月に発見されたＳｔｕｘｎｅｔ（スタックスネット）と呼ばれるマルウェアには、複数の未知の脆弱性が用いられていたことから国家の関与が疑われ、大きな話題となった。わが国においても、２０１１年には国会、政府関係機関、防衛関係企業等で、大規模な標的型攻撃による情報漏洩の被害が確認されている。そ

---

1 APT (Advanced Persistent Threat)

2 利用者の意図に反した動作を実施する不正なプログラム

3 修正プログラムが公開されていない未知の脆弱性を用いた攻撃であり、ＯＳやアプリケーションを最新の状態に更新していても防ぐことができない。

の後も日本年金機構にて標的型攻撃による大規模な情報漏洩の被害が確認される事案等が発生し、その被害はとどまるところを知らない。このような機密情報の流出は、個人や組織のみならず、場合によっては国家の安全保障に重大な影響を与える場合すらある。このように、標的型攻撃はサイバーセキュリティにおける最も深刻な脅威であり、今日の情報化社会においては誰もがその脅威を認識しておく必要がある。

「サイバー戦入門　－サイバー攻撃の技術的仕組みと対策－」では、サイバー攻撃とは何かを理解するために必要な基本的な仕組みを、技術的な観点から体系的に解説することを試み、「サイバー戦入門　その２　－サイバー戦の概念と作戦－」ではサイバー戦の概念とサイバー作戦の種類について平易に解説することを試みた。その３からは、サイバー戦に関する各トピックスをより掘り下げて平易に解説することを試みている。本稿では、標的型攻撃とその対策技術をとりあげる。以下、第２節ではＡＰＴの具体例を挙げて概要を説明する。第３節では標的型攻撃の定義と分類を示し、第４節では標的型攻撃の仕組みについて説明する。第５節では、その対策技術について説明し、最後にまとめと課題について述べる。

２　ＡＰＴの具体例

（１）初期のＡＰＴ

初期のＡＰＴとしてよく知られている事例は、Ｍｏｏｎｌｉｇｈｔ　Ｍａｚｅと呼ばれる１９９８年以降に開始された米国、英国、カナダ、ブラジル及びドイツの軍、政府、教育関係の情報システムに対する一連のサイバー攻撃である。このキャンペーンの期間は２年以上に及び、米国においてはＮＡＳＡ、エネルギー省、国及び軍の研究所、軍の基地等から、数千もの機微な軍事技術に関する文書が盗まれたとされている。これらのサイバー攻撃の一部は、モスクワからのダイヤルアップ接続[4]を起点とし、ロンドン及びシンシナティ大学等の米国の大学の情報システムを経由し、Ｔｅｌｎｅｔ[5]、ＦＴＰ[6]等の一般的なプロトコル[7]を用いて実施されていた。このような古典的なプロトコルでは、通信内容は暗号化されておらず、認証手段もパスワードのみであった。そのため、何らかの手法で攻撃者がパスワードを入手するか、あるいは推測することさえできれば、容易にどこからでも不正アクセスを実施することが可能であった。

---

4 電話回線を使用してインターネット等のネットワークにアクセスする仕組み
5 ネットワークを介してコンピュータを操作するための古典的なプロトコル
6 FTP (File Transfer Protocol) ネットワークを介してコンピュータ同士がファイルを転送するための古典的なプロトコル
7 通信規約

このように、２０００年以前においては軍や政府関係の情報システムですら（現在と比較すると）セキュリティが甘く、攻撃者はわざわざ脆弱性を使用しなくても、古典的な手法でその制御を奪うことが可能である場合があった。また、遠隔操作のためのマルウェアやＣ＆Ｃサーバ[8]を用いる必要もなく、一般的なプロトコルで不正アクセスを実施することができた。さらに、当時は遠隔で利用可能な脆弱性も多数存在しており、コンピュータが直接インターネットに接続する構成となっている組織も多かったため、不正アクセスの手法は能動的な攻撃が主流であったと考えられる。そのため、Ｍｏｏｎｌｉｇｈｔ　ＭａｚｅはＡＰＴと呼ばれることはあるが、一般に標的型攻撃には分類されない。その後、ＯＳやアプリケーションのセキュリティが強化され、遠隔で利用可能な脆弱性が減少するとともに、インターネットとＬＡＮ[9]を論理的に分離し、ファイアウォールでアクセス制御を実施する構成が一般的となってきた。また、Ｔｅｌｎｅｔ、ＦＴＰ等の古典的なプロトコルの代用となるＳＳＨ[10]と呼ばれるプロトコルも普及してきた。そのため、攻撃者は従来のように古典的な手法や遠隔で利用可能なリモートの脆弱性を利用して、能動的な攻撃を実施することが難しくなってきた。そこで、標的型攻撃のようなローカルの脆弱性を利用した受動的な攻撃が実施されるようになってきた。

（２）本格的な標的型攻撃

２０００年以降になると、本格的な標的型攻撃が実施されるようになった。標的型攻撃として知られる最初の有名な事例は、２００３年以降に米国、英国、カナダ、オーストラリア及びニュージーランド（いわゆるＦｉｖｅ　Ｅｙｅｓ）を狙ったＴｉｔａｎ　Ｒａｉｎと呼ばれるＡＰＴキャンペーンである。このキャンペーンの期間は少なくとも３年以上に及び、米国のロッキード・マーティン社、サンディア国立研究所、レッドストーン兵器廠、ＮＡＳＡ等の情報システムから、軍需産業に関する機微な文書が盗まれたとされている。この攻撃は迅速かつ正確であり、トロイの木馬として知られるマルウェアが攻撃に用いられ、国防省の多くのコンピュータが遠隔操作可能な状態に陥ったと言われている。盗まれた文書は、韓国、香港や台湾のサーバを経由し、最終的に中国のサーバに送信されていたようである。そのため、ＰＬＡ[11]の関与が指摘されているが、攻撃者の正体を示す決定的な証拠は示され

---

8 C&C or C2 (Command and Control) Server トロイの木馬に感染した端末を遠隔操作するために指令を中継するサーバ

9 LAN (Local Area Network)

10 SSH (Secure SHell) 認証や暗号の機能を付加した Telnet 及び FTP に代わるプロトコル

11 PLA (People's Liberation Army) 中国人民解放軍

ていない。

２０１０年には、米国のＩＴ技術、安全保障、軍需産業を狙ったＯｐｅｒａｔｉｏｎ　Ａｕｒｏｒａと呼ばれるＡＰＴキャンペーンが公表された。このキャンペーンは、２００９年6月から１２月の間にＧｏｏｇｌｅ、Ａｄｏｂｅ、Ｙａｈｏｏ、Ｓｙｍａｎｔｅｃ、ノースロップグラマン、モルガンスタンレー等少なくとも２０社を標的として実施された。これらの標的型攻撃では、ＩＥ[12]の未知の脆弱性が用いられ（いわゆるゼロデイ攻撃)、Ｃ＆Ｃサーバを介して複数種類のトロイの木馬による遠隔操作が実施されている。これらの標的型攻撃の犯人は、北京を拠点とするＥｌｄｅｒｗｏｏｄ（Ｓｎｅａｋｙ　Ｐａｎｄａとも呼ばれる。）と呼ばれるグループであるとされている。さらにこのグループは、Ｈｉｄｄｅｎ　Ｌｙｎｘ[13]と呼ばれるゼロデイ攻撃を用いる高度なスキルを有するハッカー集団との関係が指摘されている。中国を拠点とする攻撃者によるものとされるＡＰＴキャンペーンとしては、他にもＧｈｏｓｔ　Ｎｅｔ[14]、Ｎｉｇｈｔ　Ｄｒａｇｏｎ[15]、Ｓｈａｄｙ　ＲＡＴ[16]等が知られている。また、Ｓｈａｂｙ　ＲＡＴと関係が深いとされるＡＰＴ１は、Ｍａｎｄｉａｎｔ社が公表したレポート[17]において、上海を拠点とするＰＬＡの６１３９８部隊（Ｃｏｍｍｅｎｔ　Ｃｒｅｗとも呼ばれる。）の仕業であると暴露されたことで話題となった。

数ある標的型攻撃の中でも特に世界に衝撃を与えたのは、２０１０年6月に発見されたＳｔｕｘｎｅｔ（スタックスネット）と呼ばれるマルウェアである。このマルウェアには、原子力関係の施設における遠心分離機の誤動作を目的とする機能が組み込まれており、物理的破壊を伴うサイバー攻撃であったとされている。また、ＵＳＢメモリを介して感染してエアギャップ[18]を突破する機能を有しており、複数の未知の脆弱性を用いていることから国家の関与が疑われた。後にスノーデン氏[19]の証言により、ＮＳＡ[20]とイスラエル軍の共同作戦であるＯｌｙｍｐｉｃ　Ｇａｍｅｓの一環であったことが判明している。その後も２０１１年にはＤｕｑｕ（ドゥークー)、２０１２年にはＦｌａｍｅ（フレーム）と呼ばれるＳｔｕｘｎｅｔの後継と考えられ

---

12 IE (Internet Explorer)
13 Symantec (2013). Hidden Lynx – Professional Hackers for Hire
14 Information Warfare Monitor (2009). Tracking GhostNet: Investigating a Cyber Espionage Network
15 McAfee (2011). Global Energy Cyberattacks: “Night Dragon”
16 McAfee (2011). Revealed: Operation Shady RAT
17 Mandiant (2013). APT1: Exposing One of China’s Cyber Espionage Units
18 セキュリティ対策としてインターネット等のネットワークから隔離された環境
19 2013 年に米国の個人情報収集の手口等を告発した NSA の元職員
20 NSA (National Security Agency) 米国の国家安全保障局

るマルウェアが発見されている。このように、もはや標的型攻撃は、国家のインテリジェンス活動の重要な要素となっている。

２０１６年５月には、米国の民主党全国委員会の情報システムに対し、ＡＰＴ２８[21][22]およびＡＰＴ２９[23]と呼ばれる集団によるものとされる、ＧＲＩＺＺＬＹ　ＳＴＥＰＰＥ[24]と呼ばれる一連のサイバー攻撃が確認された。その後の２０１６年７月、クリントン前国務長官が民主党大統領候補として指名される直前には、Ｗｉｋｉｌｅａｋｓが民主党全国委員会のメール１万９千通以上を暴露している。ここで暴露された情報は、ロシア政府の関与が疑われるＧＲＩＺＺＬＹ　ＳＴＥＰＰＥにおいて流出したものと考えられている。そのため、ロシア政府がより親密なトランプ共和党候補を優位にさせるために流出させたとの見方がある。ロシア政府はもちろんこれを否定しているが、この介入がもし事実であれば、インテリジェンスを武器化し、サイバー攻撃を実世界での影響力を行使するために利用した新しい事例であると言える。その後の２０１７年６月には、メディアが入手したＮＳＡの機密文書が暴露され、ロシア連邦軍参謀本部情報総局[25]が米国の電子投票用紙事業者の従業員のアカウントに不正アクセスを実施し、その情報を用いて政治関係者に標的型メール攻撃を実施していたことが判明した[26]。２０１８年３月には、その詳細な情報が公開されている[27]。この攻撃では、利用者に添付ファイルを開かせ、パスワードや２段階認証のための電話番号や認証コードを収集していた。なお、米国財務省はこれらのサイバー攻撃にかかわったとして、ロシアの政府機関を含む５つの組織及び１９人に制裁措置を実施することを発表している[28]。２０１８年５月には、２０１６年の米大統領選介入に関連する一連のハッキング等の罪で、ロシア連邦軍参謀本部情報総局の２６１６５部隊及び７４４５５に所属する１２名が起訴された[29]。

（３）わが国における標的型攻撃

---

[21] FireEye (2014). "APT28: A Window into Russia's Cyber Espionage Operations?"
[22] Fancy Bear とも呼ばれており、正体はロシア連邦軍参謀本部情報総局(GRU)とされている。
[23] Cozy Bear とも呼ばれており、正体はロシア連邦保安局(FSB)と考えられている。
[24] DHS and FBI (2016), "GRIZZLY STEPPE - Russian Malicious Cyber Activity"
[25] GRU (Glavnoye Razvedyvatelnoye Upravleniye)
[26] Matthew Cole et al. (2017). "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election"
[27] DHS and FBI (2018), " Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors"
[28] U.S. Department of the Treasury (2018). "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks"
[29] U.S. Department of Justice (2018). "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election"

わが国においては、２００５年頃から政府機関等に対する標的型攻撃が観測されるようになった。２００７年には、日本固有のアプリケーションである一太郎の未知の脆弱性を用いたゼロデイ攻撃が確認されている。この事実は、ある程度のスキルと組織力を有する集団が、明確に日本あるいは日本人を標的としていることを示唆している。その後、２０１１年７月には、標的型攻撃をきっかけとして衆議院のサーバの管理者権限が奪取され、国会議員、秘書、職員等のＩＤとパスワードが流出する事案が発生した。この事案は新聞にも大きく取り上げられ、サイバー攻撃の脅威が注目されるようになった。また、同時期には三菱重工、ＩＨＩ、川崎重工、三菱電機等の防衛産業に対するサイバー攻撃の被害も確認された。これらのわが国の国会、防衛産業等への一連の標的型攻撃は、Ｉｃｅｆｏｇ[30]と呼ばれるＡＰＴキャンペーンの一環であったと分析されている。

その後、２０１４年９月頃から、日本の政府、報道、防衛、金融、情報通信等の様々な分野の組織を狙ったＢｌｕｅ　Ｔｅｒｍｉｔｅ[31]あるいはＣｌｏｕｄｙ　Ｏｍｅｇａ[32]と呼ばれるＡＰＴキャンペーンが発生し、その脅威はますます顕在化している。２０１５年５月に発生した日本年金機構における個人情報流出事案[33]は、その氷山の一角にすぎない。さらに、２０１６年８月には、Ｓｎａｋｅ　Ｗｉｎｅ[34]呼ばれるグループによる日本の企業、政府、教育機関等を標的としたサイバー攻撃が確認されている。このようにわが国は、明確に日本だけを標的とする主体から、サイバー攻撃を常続的に受けている状況にある。繰り返しになるが、これらの事例はわが国を標的とするサイバー攻撃のほんの一部分にすぎない。サイバー攻撃を受けたという情報が公表されない場合や、被害者が攻撃に気づいていない場合も多いものと考えられる。

３　標的型攻撃の定義と分類

標的型攻撃は、特定の組織や個人を標的とし、メールやＷｅｂコンテンツを用いて不正なプログラムを利用者の端末に送付し、その制御を奪って遠隔操作により機密情報の窃取等を実施するサイバー攻撃の一種である。特定の組織や個人の機密情報の窃取を狙った一連の標的型攻撃は、数か月から数年の長期間にわたって執拗に実施されることもあり、ＡＰＴあるいは新しいタイプの攻撃

---

30 Kaspersky (2013). The 'Icefog' APT: A Tale of Cloak and Three Daggers
31 Kaspersky (2015). Blue Termite －日本を標的にする APT 攻撃－
32 Symantec 社の呼称
33 サイバーセキュリティ戦略本部(2015). 「日本年金機構における個人情報流出事案に関する原因究明調査結果」
34 Cylance (2017). The Deception Project: A New Japanese-Centric Threat

とも呼ばれる。このような情報窃取のための長期間にわたる一連の標的型攻撃は、サイバースパイ活動、サイバーエスピオネージあるいはＡＰＴキャンペーンと呼ばれることもある。標的型攻撃は、情報セキュリティの３要素である機密性、完全性、可用性のすべてを侵害する可能性があり、極めて大きな影響を与える可能性を秘めたサイバー攻撃である。

サイバー攻撃は、攻撃者が主体的に任意のタイミングで実施できる「能動的攻撃」と、被攻撃者による何らかの動作を必要とする「受動的攻撃」に分類できる。この分類によると、標的型攻撃は「受動的攻撃」であり、その攻撃の対象は図１に示すように、主に内部の情報システムの端末である。まず、攻撃者は利用者に不審なコンテンツをメールで送付する（図１①)。利用者が受信したメールに対して何らかの動作を実施すると、攻撃者が遠隔操作を実施するための不正通信が発生する（図１②)。この時、利用者が受信したメールに対して何らの動作を実施しなければ、攻撃者は当該端末を遠隔操作することはできない。つまり、攻撃者は攻撃のタイミングを能動的に制御することができず、そのタイミングは利用者の動作のタイミングに依存する。利用者の端末からＣ＆Ｃサーバへの不正通信（図１②）が確立すると、攻撃者はＣ＆Ｃサーバを介して利用者の端末を遠隔操作することが可能となる（図１③)。

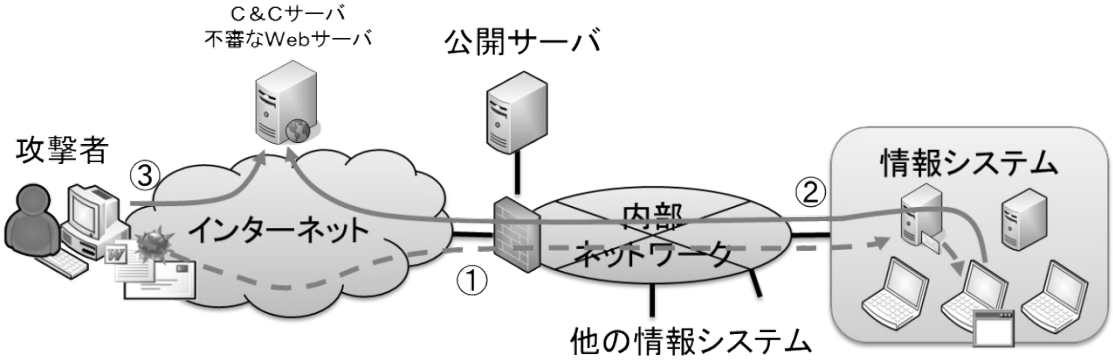

図１：情報システムの端末に対する標的型攻撃

（１）標的型攻撃の特徴

特定の組織や個人を標的とする標的型攻撃は、不特定多数を標的とする一般的な攻撃[35]と比較すると様々な特徴がある。主な標的型攻撃の特徴を表１に示す。なお、表１に示す特徴はあくまでも一般的な傾向を示すものであり、すべての標的型攻撃が必ずしもこの特徴に合致するわけではない。

表１：標的型攻撃の特徴

[35] 標的型攻撃以外の受動的攻撃であり、いわゆる「バラマキ型攻撃」を含む。

	標的型攻撃	一般的な攻撃
攻撃者の標的	特定の組織や個人	不特定多数
攻撃者の目的	機密情報の窃取、破壊	金銭、愉快犯
攻撃の期間	長い	短い
マルウェアの入手	困難	容易
ウイルス対策ソフトで検知できる可能性	低い	高い
ゼロデイ攻撃の可能性	あり	低い
メールの件名や本文	特定の者や組織にのみ関係する内容	一般的な興味を引く内容
感染に気付く可能性	低い	高い

これまでの主要なＡＰＴキャンペーンの分析レポートによると、標的型攻撃における攻撃者の目的は、機密情報の窃取である場合がほとんどである。また、場合によってはＳｔｕｘｎｅｔのように破壊等を目的とする場合もある。攻撃者は、一度攻撃に失敗したとしても、その目的を達成するために、数か月から数年以上の長期間にわたって執拗に攻撃を継続する傾向がある。これに対し、一般的な攻撃における攻撃者の目的は、愉快犯や金銭目的であるとされている。そのため、その標的は特定の組織や個人である必要はなく、攻撃が失敗した場合には標的に固執せず、成功率が高い他の組織や個人に標的を変えるのが攻撃者にとって合理的である。

標的型攻撃に用いられるマルウェアは、あらかじめウイルス対策ソフトに検知されないことを確認している可能性があると言われている。さらに、標的型攻撃では特定の組織や個人が標的となるため、攻撃に用いられるマルウェアは拡散しにくく、検体を入手することが困難な場合もある。一般に、ウイルス対策ソフトにおいて新たなマルウェアを検知するためには、パターンファイルを作成するためにそのマルウェア（検体）を必要とする。そのため、標的型攻撃に用いられるマルウェアは、ウイルス対策ソフトで検知できる可能性が低い傾向がある。また、未知の脆弱性を用いたゼロデイ攻撃の場合すらある。これに対し、一般の攻撃の場合には不特定多数が標的となり、マルウェアは拡散しやすく、検体の入手も容易なため、ウイルス対策ソフトにおいて検知できる可能性は高い。また、ゼロデイ攻撃が用いられる可能性も低い傾向がある。

標的型攻撃に用いられるメールの件名や本文は、特定の者や組織にのみ関係する内容であることが多く、メールの送信者が関係者に詐称されることも珍しくない。また、何らかの方法で窃取された本物の業務用のメールの複製

を用いる場合や、すでに乗っ取った関係者の端末を踏み台にし、実際にその関係者の端末からメールを送付する場合もある。さらに、当初は通常のやり取りを装い、相手を信用させた後にマルウェア等を送付する「やり取り型」攻撃と呼ばれる手法もある。この通常のやり取りには、メールだけでなくＳＮＳで架空のプロファイルを用いて実施される場合も増えてきている[36]。このように巧妙に偽装された場合、もはや利用者がメールの件名、本文等から標的型攻撃に気付くのは不可能に近い。また、広報や問い合わせ窓口では、その業務の性質から不特定多数の相手からのメールを開封せざるを得ない。他方、機械翻訳を用いて作成したような明らかに、あるいは若干の違和感のある日本語が使用される場合もあり、そのクオリティは様々である。さらに、標的型攻撃に用いられるマルウェアは、積極的に感染を広げるような動作はせず、通常の通信に見せかけて攻撃者からの指令を受け取る傾向があるため、感染後の検知も困難であるという特徴がある。これに対し、一般の攻撃の場合には、メールの件名や本文は、特定の者や組織に限定されない一般的な興味を引く内容であることが多い。また、金銭目的のランサムウェアの場合には、ファイルが暗号化され、金銭を要求する画面が表示されるため、マルウェアに感染したことは利用者にも明確となる。

（２）標的型攻撃の分類

適切なセキュリティ対策を実施している組織では、利用者の端末が接続する内部ネットワークと公開サーバが接続するインターネットは論理的に分離されており、端末からインターネットへのアクセスは必要最小限のプロトコルに制限しているのが一般的である。例えば、一般的な利用者の端末からインターネットへのアクセスは、プロキシサーバ経由のＷｅｂサイトの閲覧及びメールの送受信に限定し、それ以外のプロトコルはファイアウォールで遮断するという構成のＬＡＮがある。この構成のＬＡＮの場合、利用者の端末からインターネットへのアクセス手段は、メール及びＷｅｂに絞り込まれる。したがって、利用者の端末への初期のネットワーク経由の不正アクセスも、このどちらかの手段で実施されることになる。ネットワーク経由の標的型攻撃を、感染経路を基にして分類すると、標的型メール攻撃及びドライブ・バイ・ダウンロード攻撃（以下ＤｂＤ攻撃）[37]に分類することができる。標的型メール攻撃及びＤｂＤ攻撃の概要を図２に示す。

---

[36] Secure Works (2017). The Curious Case of Mia Ash: Fake Persona Lures Middle Eastern Targets

[37] DbD (Drive by Download)攻撃

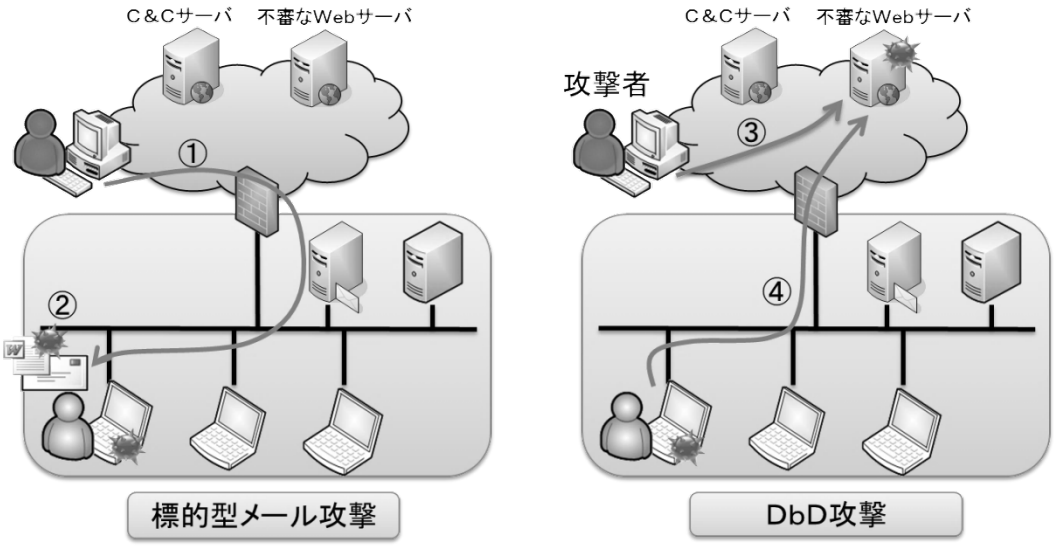

図２：標的型メール攻撃及びＤｂＤ攻撃の概要

標的型メール攻撃は、メールにマルウェアを添付して標的となる組織や個人に送付し（図２①）、利用者がその添付ファイルを開封する（図２②）とその端末の制御が奪われ、攻撃者に遠隔操作されるサイバー攻撃の一種である。標的型メール攻撃では、マルウェアの感染経路はメールの添付ファイルとなる。

ＤｂＤ攻撃は、Ｗｅｂサイトに不正なコンテンツを設置し（図２③）、利用者がそのＷｅｂサイトを閲覧する（図２④）と様々なＷｅｂサイトを経由してその端末の制御が奪われ、攻撃者に遠隔操作されるサイバー攻撃の一種である。ＤｂＤ攻撃では、マルウェアの感染経路はＷｅｂサイトとなる。攻撃者が利用者を不正なコンテンツを埋め込んだＷｅｂサイトに誘導する手段としては、リンクをメールで送付してクリックさせる手法や、あらかじめ利用者がよく閲覧するＷｅｂサイトを改ざんして待ち受ける手法[38]、人気があるサイトの偽のサイトを作成する手法等が考えられる。さらに、ＤｂＤ攻撃の中には閲覧者のアクセス制御を実施し、特定の組織の利用者がアクセスした場合のみマルウェアに感染させる水飲み場攻撃もある。水飲み場攻撃の場合には、特定の組織以外の利用者やサイバー攻撃の分析者がアクセスした場合にはマルウェアに感染しないため、発見が難しく、対策が遅れてしまう可能性がある。

ネットワークを経由しないローカルの標的型攻撃としては、ＵＳＢメモリ等を経由した攻撃が代表的である。かつて、ＵＳＢメモリを利用した攻撃で

38 広義で水飲み場攻撃と呼ばれる場合もある。

は、Ａｕｔｏｒｕｎ[39]と呼ばれる自動実行のための機能や、脆弱性を利用して不正なプログラムの実行を試みる場合が多かった。例えば、Ｃｏｎｆｉｃｋｅｒと呼ばれる２００８年頃に発見されたマルウェアの亜種は、感染を広げるためにＡｕｔｏｒｕｎの機能を悪用していた。Ａｕｔｏｒｕｎの機能が有効な端末では、Ｃｏｎｆｉｃｋｅｒに感染したＵＳＢメモリを挿入するだけでその端末はマルウェアに感染してしまう。そのため、セキュリティ対策として端末のＡｕｔｏｒｕｎの機能を無効化することが提唱されるようになった。また、２０１０年６月に発見されたＳｔｕｘｎｅｔには、当時は未知であったショートカットの脆弱性[40]を利用し、ＵＳＢメモリを経由して感染する機能が組み込まれていた。そのため、端末のＡｕｔｏｒｕｎの機能を無効化していたとしても、そのＵＳＢメモリの中身を確認するだけで感染してしまう状況であった。さらに、２０１４年８月には、ＵＳＢの規格の脆弱性を悪用したＢａｄＵＳＢと呼ばれる攻撃手法が発表された。ＢａｄＵＳＢではファームウェア[41]を書き換えることにより、マルウェアのインストール、ＵＳＢメモリの改ざん、ＵＳＢキーボードの操作等が可能とされている。この脆弱性を修正するためには、現在のＵＳＢの代替となる新しい規格をつくる必要がある。そのため、この脆弱性は、短期的には実質的に修正することが不可能である。このように、もはやインターネットに接続していないクローズな環境の情報システムがサイバー攻撃を受けることは珍しくない。ゆえに、今日ではエアギャップはもはや万全の対策とは言い難い。

その他の感染経路としては、あらかじめ不正な機能を埋め込んだ情報システム、プログラム、電子機器等を、標的とする組織に出荷する手法が考えられる。例えば、中国から出荷されるコンピュータやスマートフォンの一部からは、不正な機能が埋め込まれた製品が確認されている。また、米国の大手企業から出荷されたネットワーク機器の一部についても、不正な機能が埋め込まれていることがスノーデン氏に暴露されて話題となった。このようなサプライチェーンを用いたサイバー攻撃は、出荷するハードウェアを用いたローカルに分類される手法が中心であるが、ネットワーク経由で不正なプログラムを配信する手法もある。例えば、２０１３年３月に韓国の放送局や銀行がサイバー攻撃を受けた事件[42]で使用されたマルウェアは、オンラインのアップデート機能を用いて配信されたと言われている。わが国では、２０１４

---

39 CD, DVD, USB メモリ等を挿入した際にプログラムを自動実行するための機能

40 細工をしたショートカットファイルを表示するだけで感染してしまう脆弱性であり、当時最新の修正プログラムを適用していても防ぐことは困難であったとされている。

41 電子機器に組み込まれたハードウェアを制御するためのソフトウェア

42 韓国においては「３・２０電算大乱」と呼ばれている。

年８月に、ＥｍＥｄｉｔｏｒ[43]というソフトウェアの更新機能を悪用し、マルウェアを配信しようとする攻撃が確認されている。この攻撃では、特定のＩＰアドレスから接続があった場合のみマルウェアが配信され、明確に標的が絞られていた。サプライチェーンを用いたサイバー攻撃は、特にハードウェアの場合には技術的に発見が非常に困難であり、サプライチェーンリスクの問題として議論されている。

このような主な標的型攻撃を、感染経路ごとに整理して分類すると表２の通りとなる。ＩＰＡ[44]が実施した調査[45]によると、マルウェアの侵入経路はＷｅｂサイトの閲覧によるものが６５．４％、メールによるもの６０．４％であり、次いでＵＳＢメモリ等の外部記憶媒体によるものが３４．５％となっている。

表２：感染経路に基づく標的型攻撃の分類

感染経路		攻撃の種類
ネットワーク経由	メールの添付ファイル	標的型メール攻撃
	Ｗｅｂサイト	ドライブ・バイ・ダウンロード攻撃（水飲み場攻撃）
ローカル	ＵＳＢメモリ等	Ｓｔｕｘｎｅｔ等
	サプライチェーン	サプライチェーンリスク

４　標的型攻撃の仕組み

（１）標的型攻撃の段階

標的型攻撃の手順を時系列で整理すると、いくつかの段階に区分することができる。例えば、ＩＰＡは標的型攻撃を表３に示す段階に区分している[46]。

表３：標的型攻撃の段階

段階		説明	サイバーキルチェーンの対応
1	計画立案	攻撃目標の選定 攻撃に必要な情報の収集 計画の立案	偵察

43 国産の高機能なテキストエディタ
44 IPA (Information-technology Promotion Agency) 情報処理推進機構
45 情報処理推進機構(2014). 「「2014 年度情報セキュリティ事象被害状況調査」報告書」
46 情報処理推進機構(2014). 「「高度標的型攻撃」対策に向けたシステム設計ガイド」

2	攻撃準備	攻撃に必要なインフラの準備 不正なコンテンツの作成	武器化
3	初期潜入	不正なコンテンツの送付あるいは誘導により端末の制御を奪取	配送～攻撃
4	攻撃基盤構築	ＲＡＴ[47]のインストール 必要なツールのダウンロード等	インストール ～遠隔操作
5	内部調査侵入	情報システム内部の調査 アクセス権の拡大等	侵入拡大
6	目的遂行	機密情報の窃取 情報システムの破壊等	目的遂行
7	再侵入	必要に応じて再度侵入して調査	―

まず「計画立案」の段階では、攻撃目標を選定して必要な情報を収集し、計画を立案する。「攻撃準備」の段階では、Ｃ＆Ｃサーバ等の攻撃に必要なインフラを準備するとともに、マルウェア等の不正なコンテンツを準備する。「初期潜入」の段階では、不正なコンテンツを作成し、標的に送付あるいは誘導してその端末の制御を奪う。「攻撃基盤構築」の段階では、端末を恒久的に遠隔操作するためにＲＡＴと呼ばれるマルウェアをインストールし、その後の「内部調査侵入」に必要なツール等をダウンロードする。「内部調査侵入」の段階では、情報システムの内部を調査してアクセス権を徐々に拡大し、「目的遂行」の段階では目標とする機密情報の窃取や情報システムの破壊等を実施する。「攻撃基盤構築」～「再侵入」の段階には厳密な区分はなく、必要に応じて適宜の順序で実施される。他の良く知られた標的型攻撃を段階的に区分したモデルとしては、ロッキード・マーティン社が提唱した[48]サイバーキルチェーン[49]が知られている。表３の右側は、ＩＰＡの各段階に対応するサイバーキルチェーンのプロセスを示している。

これまでの多くの主要なＡＰＴキャンペーンの分析レポートによると、標的型攻撃における感染経路のほとんどはネットワーク経由である。ネットワーク経由の標的型攻撃において、「計画立案」及び「攻撃準備」の段階ではまだ対策を講じることができない。次の「初期潜入」の段階は、ネットワーク経由の標的型メール攻撃とＤｂＤ攻撃でその手法は異なるが、それ以降の「攻撃基盤構築」～「再侵入」の段階における手法はほぼ共通である。そこ

47 RAT (Remote Access Trojan or Remote Administration Tool)
48 Hutchins, E.M. et al. (2009). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains
49 標的型攻撃の段階を連鎖的に偵察、武器化、配送、攻撃、インストール、遠隔操作、目的実行に区分したモデル

で本稿では、標的型攻撃の仕組みを、「初期潜入」の段階とそれ以降の「攻撃基盤構築」～「再侵入」の段階に区分して解説する。

（２）標的型メール攻撃

標的型メール攻撃においてメールに添付されるマルウェアを大まかに分類すると、実行ファイルと文書ファイルに分類される。実行ファイルと文書ファイルの違いを表４に示す。

表４：標的型メール攻撃の添付ファイルの分類

添付ファイルの種類	他のアプリケーションの起動	脆弱性の使用	拡張子の例
実行ファイル	なし。	不要	exe, scr 等
文書ファイル	あり。	必要	doc, jtd, xls, pdf 等
文書ファイル（マクロ付）		不要	doc, xls 等

ここで言う実行ファイルとは、単独で動作可能なファイルや、ショートカットファイルのようにリンク先のファイルが実行され、実質的に実行ファイルと同様の結果をもたらすファイルの総称である。これらの実行ファイルに相当するファイルでは、他のアプリケーションは起動せず、その制御を奪うための脆弱性を必要としない。攻撃者は脆弱性を使用しなくとも、その実行ファイルに相当するファイルに直接不正な命令を記述することで、容易に利用者の端末の制御を奪うことが可能である。したがって、出所が不明なファイル、あるいは信頼できないソースから入手した実行ファイルに相当するファイルをダブルクリックするのは非常に危険な行為である。このようなリスクを回避するためには、添付ファイルの種類が実行形式に相当するファイルか否かを認識する必要がある。攻撃者はこれを困難にするために、添付ファイルのアイコンをその他のファイルのアイコンに偽装したり、長いファイル名やＲＬＯ[50]と呼ばれるテクニックを用いて拡張子を偽装したりする。利用者は、「右クリック」で表示されるメニューからファイルの「プロパティ」を選択し、「ファイルの種類」の欄を確認すれば、このような場合にもファイルの種類を確認することができる。しかしながら、業務が多忙な場合や知人からのメールの場合には、このような確認を怠ってしまう場合も珍しくな

[50] RLO (Right-to-Left Overwrite) 文字の向きを反転させる制御コードを用いて拡張子を偽装するテクニックである。例えば、ファイル名に「cod」という文字を利用し、これを反転させて「doc」という文字列をファイル名の最後になるように長さを調整することで、ＭＳ　Ｗｏｒｄの拡張子を偽装することができる。

い。ゆえに、このような実行ファイルに相当するファイルを添付したメールを、自動的に遮断するアプローチをとっている組織もある。しかしながら、ファイルが圧縮されてパスワードで保護されている場合などは、内包されているファイルの種類を確認することは難しい。したがって、パスワードで保護された圧縮ファイルの取扱についても、実行ファイルに相当するファイルと同様に十分に注意する必要がある。

表３の文書ファイルとは、実行形式に相当するファイル以外のあらゆる文書ファイル等のことであり、そのファイルを開くために他のアプリケーションの起動を必要とする。文書ファイルを用いて端末の制御を奪うためには、そのアプリケーションの脆弱性をつくか、あるいはマクロ[51]を実行させるのが一般的である。脆弱性をつく場合には、攻撃者はエクスプロイトコードと呼ばれる脆弱性を突く命令群と、シェルコードと呼ばれるマルウェア本体の実行ファイルを展開する命令群をその文書ファイルに埋め込む。利用者がその文書ファイルをダブルクリックすると、関連づけられたアプリケーションが起動し、その脆弱性がつかれて実行ファイルが呼び出される。マクロの場合には、利用者がマクロの実行を許可した場合、マクロに記述された命令によって実行ファイルが呼び出される。実行ファイルは、その文書ファイルから取り出される場合[52]と、インターネットからダウンロードされる場合[53]がある。このように実行ファイルが隠された場合、添付ファイルを確認したとしてもマルウェアか否かを判断することは難しい。しかしながら、文書ファイルの場合には脆弱性をつく必要があるため、その脆弱性の修正プログラムを適用していればマルウェア本体は実行されない。したがって、可能な限り速やかに修正プログラムを適用していれば、ゼロデイ攻撃の場合を除き、ほとんどの文書ファイルによる攻撃を防ぐことが可能である。

（３）ＤｂＤ攻撃（水飲み場攻撃）

ＤｂＤ攻撃（水飲み場攻撃を含む。）では、多くの場合に複数のＷｅｂサイトを経由して端末の制御が奪われる。端末の制御が奪われた後のプロセスは、標的型メール攻撃と同様となる。ＤｂＤ攻撃のプロセスの概要を図３に示す。

---

51 コンピュータの操作を自動化するためにアプリケーションに組み込まれた機能
52 ドロッパーと呼ばれる。
53 ダウンローダと呼ばれる。

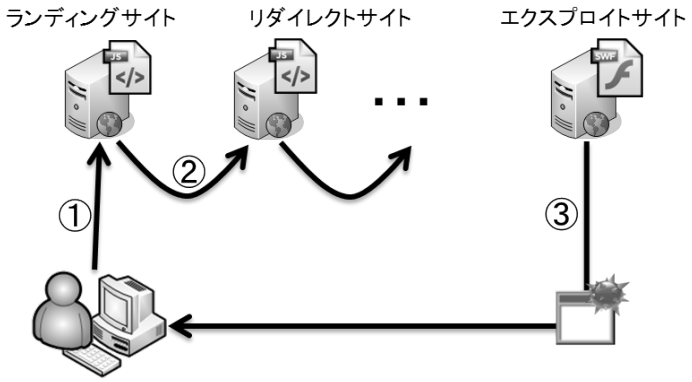

図３：ＤｂＤ攻撃のプロセスの概要

まず、標的となる端末がランディングサイト（あるいは入口サイト）と呼ばれる攻撃の起点となるＷｅｂサイトにアクセスする（図３①）。ランディングサイトの役割は、標的となる利用者をおびき寄せることである。したがって、正規のサイトを改ざんしたり、アクセス数の多いサイトを複製した偽のサイトを用いたりすることもある。

次に、リダイレクトサイト（あるいは転送サイト）と呼ばれる転送用のサイトをしばしば複数回にわたって経由する（図３②）。このリダイレクト（転送）は、ｉｆｒａｍｅタグ[54]、Ｏｂｊｅｃｔタグ[55]、Ｅｍｂｅｄタグ[56]等を用いて利用者に気付かれないように巧妙に実施されることが多い。例えば、ｉｆｒａｍｅタグを用いてＷｅｂサイトの表示を複数のフレームに分割し、片方のフレームに不正なコンテンツを埋め込んだページを読み込ませる。この時に、不正なコンテンツの読み込む側のフレームの表示サイズを０に設定すれば、利用者の目には見えないため、リダイレクトに気付くことは難しい。他にも、微小サイズのコンテンツを用いる手法、閲覧可能な領域の外に不正なコンテンツを配置する手法、コンテンツに透過属性を付与して不可視にする手法等がある。リダイレクトサイトの役割は、攻撃の標的を絞り込んだり、攻撃の追跡を困難にしたりすることである。例えば、ＷｅｂサイトでＦｉｎｇｅｒｐｒｉｎｔｉｎｇ[57]と呼ばれる手法を用いて端末の情報を収集し、標的であればエクスプロイトサイトに転送し、そうでない場合は「指定のページが存在しません。」等の偽のページを表示させたりする。

リダイレクトサイトを経由した後、最終的に利用者はエクスプロイト（あ

54 インラインフレームの略であり、Web サイトを分割して異なるコンテンツを同時に表示するための仕組み
55 外部のコンテンツを読み込むための仕組み
56 コンテンツに音声や動画などを埋め込むための仕組み
57 ブラウザ等から得られる情報から端末を一意に識別・追跡（トラッキング）するための技術であり、ユーザごとに効果的な広告を表示する用途等に用いられる。

るいはダウンロード・攻撃サイトとも呼ばれる。）に転送される。エクスプロイトサイトでは、ローカルの脆弱性がつかれ、端末にマルウェアがダウンロードされて実行される（図３③）。ここで用いられる脆弱性は、ブラウザ、Ｆｌａｓｈ　Ｐｌａｙｅｒ[58]、Ｊａｖａ[59]等のＷｅｂサイトの閲覧に関係するアプリケーション等の脆弱性である。したがって、Ｗｅｂサイトを閲覧する端末に不要なアプリケーションをインストールしなければ、攻撃を受けるリスクは減少する。特に、Ｊａｖａの実行環境であるＪＲＥ[60]については、非常に多数の脆弱性がＤｂＤ攻撃に利用された実績があるため、インターネットに接続する端末においては、やむを得ない理由がない限りはインストールすべきではない。また、ブラウザにおいて未知のＷｅｂサイトのＪａｖａアプレット[61]の実行を許可するのは、インターネットから未知のプログラムをダウンロードしてインストールするようなものである点を認識すべきである。

（４）「初期潜入」以降の段階

脆弱性等がつかれて制御が一時的に奪われた「初期潜入」の後、利用者の端末には恒久的に遠隔操作を実施するためのＲＡＴと呼ばれるマルウェアがインストールされる。標的型攻撃に用いられる著名なＲＡＴとしては、ＰｏｉｓｏｎＩＶＹ[62]（ポイズンアイビー）、ＰｌｕｇＸ（プラグエックス）、年金機構等へのサイバー攻撃で話題となったＥｍｄｉｖｉ（エムディビ）等が知られている。以後のプロセスは、標的型メール攻撃の場合もＤｂＤ攻撃の場合も同様となる。

端末にＲＡＴがインストールされると、攻撃者はＣ＆Ｃサーバを通じて能動的に端末を遠隔操作することが可能となる。遠隔操作が可能な状態になると、攻撃者はその端末に必要なツール等をダウンロードし、攻撃基盤を構築しようとする。図４に「初期潜入」～「攻撃基盤構築」の概要を示す。

---

58 Ｗｅｂサイトにおいて配信される動画の一方式を再生するためのソフトウェア

59 互換性を重視したオブジェクト指向のプログラム言語の一種

60 JRE (Java Runtime Environment) Java で開発されたプログラムを実行するために必要なソフトウェアのパッケージ

61 Web ブラウザに読み込まれて実行される Java のアプリケーションの一種

62 FireEye (2014). "POISON IVY: Assessing Damage and Extracting Intelligence"

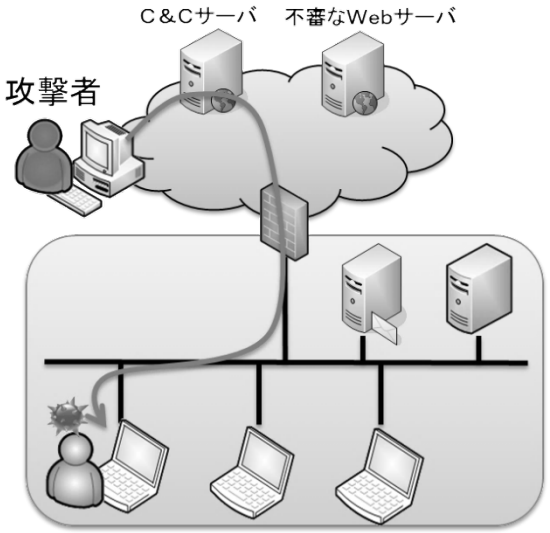

図４：「初期潜入」～「攻撃基盤構築」の概要

この際にダウンロードされるツールは攻撃者によって様々であるが、命令の実行、パスワード等の認証情報の窃取、通信の中継、遠隔操作、権限昇格、他の端末やサーバの権限奪取、情報収集、痕跡の削除等に用いられるツールが挙げられる[63]。

その後、攻撃者は内部の情報を調査し、アクセスできる範囲の拡大を試みる。「内部調査侵入」の概要を図５に示す。

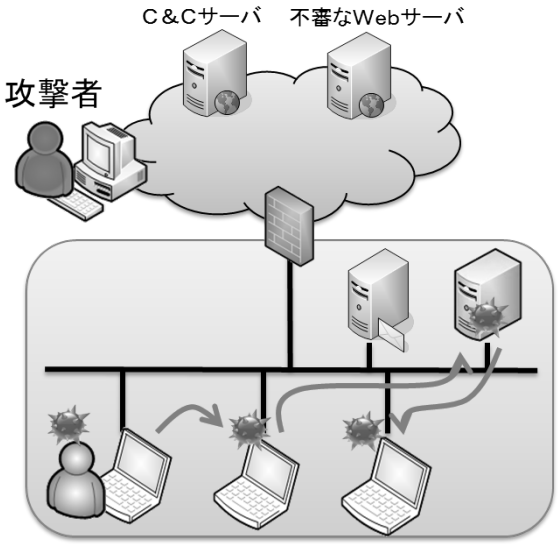

図５：「内部調査侵入」の概要

[63] JPCERT/CC (2016). 「インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書」

「内部調査侵入」における攻撃者の活動は大まかに表５に示すとおりである。

表５：内部調査侵入における攻撃者の活動

攻撃者の活動	説明
情報収集	アカウントやネットワーク情報の取得
認証情報の窃取	パスワードやそのハッシュ[64]の取得
権限昇格	権限の強いアカウントの取得
遠隔命令の実行	他の遠隔の端末やサーバでの命令の実行
通信の中継	他の遠隔の端末やサーバへの通信の中継
遠隔操作	他の遠隔の端末やサーバへのアクセス
権限取得	管理者権限の取得
痕跡の削除	インベントログの削除や時刻情報の改ざん

まず、攻撃者はアクセスした端末において、ｎｅｔコマンド等を使用してそのアカウントやネットワークに関する情報を取得する。これにより、攻撃者は現在のアカウントの権限、情報システムの構成、Ａｃｔｉｖｅ　Ｄｉｒｅｃｔｏｒｙ[65]を導入している場合にはその情報等を把握し、その状況に応じて次に実施する活動を検討する。

その端末で認証情報の取得を試みる場合には、攻撃者は主にパスワードやそのハッシュを記憶領域から入手するためのツール[66]を実行する。これにより、パスワードやそのハッシュが入手できた場合には、その認証情報を利用して他の遠隔の端末やサーバにログインすることが可能となる。あるいは、得られたハッシュから総当たり攻撃[67]や辞書攻撃[68]により、パスワードの復元を試みることが可能である。得られたパスワードが管理者のものであった場合には、攻撃者はその権限の範囲内であらゆるコマンドを実行することが

64 ここでは一方向性の演算処理により変換された文字列のことである。この演算処理では、同じパスワードは同じハッシュに変換され、通常はハッシュからパスワードを復元することはできない。この性質を利用し、パスワードがそのままの状態でコンピュータの内部に残らないようにするために利用される。

65 Ｍｉｃｒｏｓｏｆｔ社が開発したネットワーク上のコンピュータ、利用者、認証情報等を管理するための仕組み

66 Ｍｉｍｉｋａｔｚ、ＷＣＥ等が有名である。

67 取り得る組み合わせをすべて試してパスワードを奪取する攻撃であり、ブルート・フォース・アタックとも呼ばれる。

68 よく使用される単語や人名等が登録された辞書を順に試してパスワードを奪取する攻撃

可能となる。したがって、端末には管理者のパスワードやそのハッシュが残らないように留意することが重要である

権限昇格を試みる場合には、攻撃者は主にローカルの脆弱性をつくツールを実行することにより、本来は管理者権限を必要とするコマンドを実行する。

他の遠隔の端末やサーバでの命令の実行を試みる場合には、ＰｓＥｘｅｃ[69]やＰｏｗｅｒＳｈｅｌｌ[70]等の、本来は正当な管理のためのツールが悪用されることが多い。特に、ＰｏｗｅｒＳｈｅｌｌはＷｉｎｄｏｗｓ７以降では標準で利用が可能となっており、その高い機能性と利便性の反面、攻撃者に悪用されることが懸念されている。

他の端末やサーバへの通信の中継を試みる場合には、専用のツールが用いられる。これらのツールは、複数の端末やサーバを経由し、その経路を複雑にして解明を困難にする用途などに用いられていると考えられる。標的型攻撃において用いられる専用のツールとしては、ＨＴｒａｎ[71]が知られている。

他の遠隔の端末やサーバへのアクセスを試みる場合には、正規のサービスであるＲＤＰ[72]や、Ｐａｔｈ－ｔｈｅ－ｈａｓｈ（パスザハッシュ）と呼ばれる攻撃手法が用いられることが多い。Ｐａｔｈ－ｔｈｅ－ｈａｓｈとは、取得したパスワードのハッシュを使用し、その利用者の権限で他の遠隔の端末やサーバにアクセスする手法であり、専用のツール[73]を用いて実施される。

管理者権限の奪取については、多くの攻撃者の共通の目標である。Ａｃｔｉｖｅ　Ｄｉｒｅｃｔｏｒｙを導入している場合には、情報システムのアカウントやパスワード等のアクセス権に関する情報は、ドメイン・コントローラと呼ばれる特別なサーバで一元管理されている。端末のローカルの管理者権限と、ドメインの管理者権限の有効範囲は異なる。端末のローカルの管理者権限は、その端末でのみ有効である。これに対しドメインの管理者権限は、その管理下にあるすべてコンピュータで有効である。したがって、ドメインの管理者権限が奪取された場合には、その管理下にあるすべての端末やサーバが不正アクセスを受けた可能性があると考えるべきである。ドメイン管理者権限やアカウントを奪取する手法としては、ＭＳ１４－０６８[74]と呼ばれる脆弱性を利用する手法と、Ｇｏｌｄｅｎ　Ｔｉｃｋｅ

---

69 遠隔のコンピュータで簡易に命令を実行するためのツール

70 Ｍｉｃｒｏｓｏｆｔ社がシステム管理のために開発した命令実行のためのツールあるいはプログラム言語

71 中国紅客連名により開発されたパケットを転送するためのツール

72 RDP (Remote Desktop Protocol) Ｍｉｃｒｏｓｏｆｔが開発した端末やサーバの画面を転送して遠隔で操作するための仕組み

73 Ｍｉｍｉｋａｔｚ、ＷＣＥ等が有名である。

74 Ｍｉｃｒｏｓｏｆｔ社の製品に関する脆弱性の一連番号であり、ＭＳの後の２桁の数字は西暦年の下２桁、続く３桁の番号はその年の一連番号を示す。

ｔあるいはＳｉｌｖｅｒ　Ｔｉｃｋｅｔと呼ばれる攻撃手法[75]がある。

痕跡の削除については、単純にファイルやイベントログが削除される場合もあれば、専用のツールを用いて削除あるいは改ざんされる場合もある。専用のツールには、複数回の上書きによりファイルの復元ができないように削除するものや、時刻情報を復元してファイルにアクセスした痕跡を削除するものもある。

攻撃の最終目標が機密情報の窃取であった場合、攻撃者は収集した情報を一箇所に集積し、パスワードをかけて圧縮した後に外部のサーバに送信することが多い。「目的遂行」の概要を図６に示す。

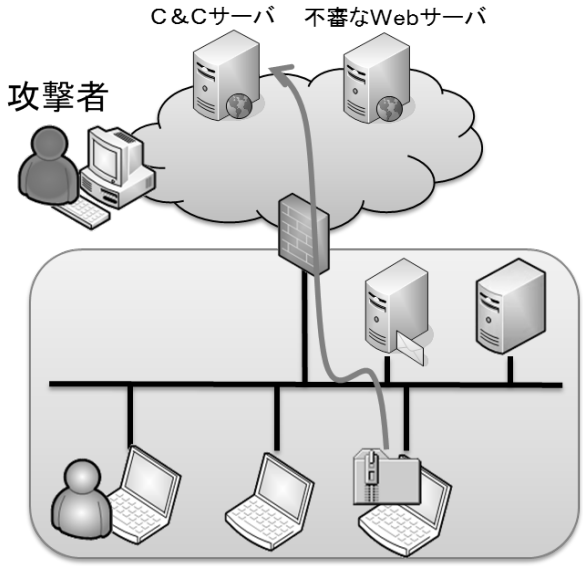

図６：「目的遂行」の概要

一般に、サイバー攻撃による情報漏洩が発生した場合、漏洩した情報を特定することは困難である場合が多い。しかしながら、このような圧縮されたファイルを発見できた場合、その内容を推定することが可能である。ただし、圧縮されたファイルを発見できたとしても、攻撃者が設定したパスワードを解除できず、内容を確認できない場合もある。

「目的遂行」の後、必要に応じて「再侵入」が実施される場合もある。再侵入の際には、「攻撃基盤構築」においてインストールしたＲＡＴが検知されていなければ、そのまま使用することが可能である。以後、「攻撃基盤構築」～「再侵入」の段階が適宜の順序で実施される。

５　標的型攻撃の対策技術

[75] Ｍｉｍｉｋａｔｚというツールを用いる。

（１）入口対策

標的型攻撃の入口対策とは、主な感染経路であるメール、Ｗｅｂ、ＵＳＢメモリ等において、マルウェアや不審な挙動を検知したりアクセス制御を実施したりすることにより、感染を未然に防ぐ対策のことである。入口対策は、時系列では「初期潜入」～「攻撃基盤構築」の段階における対策となる。感染経路及び対策位置毎の入口対策の例を表６に示す。

表６：感染経路及び対策位置毎の入口対策の例

<table>
<tr><th></th><th>メール</th><th>Ｗｅｂ</th><th>ＵＳＢメモリ等</th></tr>
<tr><td>インターネットの出入口</td><td>スパムフィルタ
ゲートウェイ型のウイルス対策製品
サンドボックス</td><td>アクセス制御
ＩＤＳ／ＩＰＳ
サンドボックス</td><td>－</td></tr>
<tr><td rowspan="2">端末やサーバ</td><td colspan="3">ウイルス対策ソフト
ＯＳやアプリケーションの修正プログラム</td></tr>
<tr><td>－</td><td>－</td><td>自動実行の無効化
不要なポートの無効化</td></tr>
</table>

表６の各行は対策を実施する位置を示しており、各列は感染経路を示している。

インターネットの出入口における対策としては、メール及びＷｅｂにおける不正な通信の監視やアクセス制御が挙げられる。

メールに関しては、スパムフィルタ及びゲートウェイ型のウイルス対策製品が基本的なセキュリティ対策となる。スパムフィルタは、メールサーバに中継されるメールを事前に検査し、不特定多数を対象とした広告等のスパムメールをあらかじめ除去する。スパムフィルタでは、不特定多数を標的にした一般的な攻撃を排除できる可能性がある。ゲートウェイ型のウイルス対策製品はスパムフィルタと同様に、メールサーバに中継されるメールを事前に検査し、マルウェア等を検知した場合には排除する。この仕組みは、基本的にはウイルス対策ソフトと同様である。したがって、既知の一般的なマルウェアであれば検知できる可能性は高いが、標的型メール攻撃を検知できる可能性は低い。このように、従来のスパムフィルタやゲートウェイ型のウイルス対策製品では、一般的な攻撃を検知することは可能であるが、標的型メール攻撃を検知することは難しい。しかしながら、スパムフィルタやゲートウ

ェイ型のウイルス対策製品において、実行ファイルに相当するファイルや、マクロ付の文書ファイルを遮断することができれば、標的型攻撃のリスクを大幅に減少させることができる。これらのファイルを一律で遮断すれば、脆弱性を用いない攻撃の手段はかなり限定される。脆弱性を用いた攻撃については、ゼロデイ攻撃でない限りは、修正プログラムを適用することで防ぐことができる。したがって、業務の遂行に特段の支障がないのであれば、実行ファイルに相当するファイルやマクロ付の文書ファイルについては遮断すべきである。さらに本格的な入口対策としては、サンドボックス[76]と呼ばれる動的解析[77]を実施する製品の導入が望ましい。

Ｗｅｂに関しては、アクセス制御及びＩＤＳ／ＩＰＳ[78]が基本的なセキュリティ対策となる。アクセス制御は、あらかじめＤｂＤ攻撃で使用されるランディングサイト、リダイレクトサイト、エクスプロイトサイト等をブラックリストに登録し、当該サイトへのアクセスをあらかじめ遮断することである。ブラックリストがＵＲＬ、ドメイン名等の場合には、アクセス制御はプロキシサーバ等で実施するのが一般的である。ＩＰアドレスの場合には、ファイアウォールで実施する場合もある。ＩＤＳ／ＩＰＳでは、ＤｂＤ攻撃における共通の通信挙動をシグネチャとして登録し、不正な通信を検知／遮断する。しかしながら、近年の標的型攻撃の通信は正常通信に類似しており、シグネチャの作成が困難である場合も多い。より本格的な対策であるサンドボックスは、メールを分析対象とする製品が多いが、Ｗｅｂを対象とした製品もいくつか存在する。これらの製品では、ＵＲＬを分析対象としてそのサイトに実際にアクセスし、ダウンロードされるファイル等の動的解析を実施する。動的解析の内容は、メールを分析対象とする製品と同様であることが多い。サンドボックスには、メールとＷｅｂの両方に対応した製品もある。

端末やサーバ（いわゆるエンドポイント[79]）における基本的な対策としては、ウイルス対策ソフト及び修正プログラムが挙げられる。ウイルス対策ソフトについては、自動アップデートを有効にし、常に最新の定義ファイルを適用した状態を維持することは最低限必要である。しかしながら、繰り返し述べているとおり、ウイルス対策ソフトでは標的型攻撃を検知できる可能性は低い。したがって、より本格的な対策としては、不審な挙動を検知するＨＩＤＳ[80]のような機能を有するエンドポイント対策製品の導入を検討すべき

---

76 仮想環境でそのファイルを実行し、その振る舞いを総合的に分析してマルウェアか否かを判定する製品

77 実際にマルウェアを動作させて分析する手法

78 IDS (Intrusion Detection System) / IPS (Intrusion Prevention System)

79 ネットワークの末端に接続された端末、サーバ等

80 HIDS (Host based Intrusion Detection System) 主に端末やサーバの内部を監視して不

である。挙動に基づくエンドポイント対策製品には、ウイルス対策ソフトと一体化した製品もある。ＯＳやアプリケーションの修正プログラムについては、速やかに最新の修正プログラムを適用することが望ましい。これにより、ゼロデイ攻撃を除いたほとんどの脆弱性を用いた攻撃の影響を緩和することが可能となる。修正プログラムの適用にあたっては、業務の妨げとならないようにＧＯＴＳ[81]品及び専用のソフトウェアの動作や、アップデート後の互換性を事前に検証する必要がある。ＧＯＴＳ品及び専用のソフトウェアが動作するサーバや、エアギャップを介したクローズな環境の情報システムについては、検証に要する環境やコストの不足により、修正プログラムの適用が見送られる場合もある。しかしながら、Ｓｔｕｘｎｅｔの事例を教訓とすると、クローズな環境の情報システムにおいてさえも、修正プログラムの不適用は重大なリスクとなり得る。したがって、ＧＯＴＳ品及び専用のソフトウェアが動作するサーバや、エアギャップを介したクローズな環境の情報システムについても、可能な限り修正プログラムを適用すべきである。特に、ドメイン・コントローラにおける修正プログラムの適用は必須である。

ＵＳＢメモリ等への対策としては、自動実行及び不要なポートの無効化が挙げられる。自動実行及び不要なポートの無効化については、Ｗｉｎｄｏｗｓの標準の機能のセキュリティポリシーで設定することが可能である。なお、Ｗｉｎｄｏｗｓ７以降では自動実行はＣＤ／ＤＶＤドライブのみで有効となっている。また、専用の端末やサーバ等を一元的に管理するソフトウェアや物理的にポートを閉塞することによって無効化することも可能である。

（２）出口対策

標的型攻撃の出口対策とは、主として不正アクセスを受けた後、外部との不審な通信や内部での不審な活動を検知する対策のことである。時系列では「攻撃基盤構築」～「目的遂行」の段階における対策となる。対策位置毎の出口対策の例を表７に示す。

表７：対策位置毎の出口対策の例

対策位置	対策手段
インターネットの出入口	アクセス制御 ＩＤＳ／ＩＰＳ
端末やサーバ	ウイルス対策ソフト

審な挙動を検知するシステム

[81] GOTS (Government Off-The-Shelf) 専ら政府が利用するために開発されたソフトウェアやハードウェアのことである。これに対応して民間の製品を COTS (Commercial Off-The-Shelf)と呼ぶ。

	ＯＳやアプリケーションの修正プログラム セキュリティポリシーの設定 ＨＩＤＳ
内部ネットワーク	アクセス制御 ＩＤＳ／ＩＰＳ ＳＩＥＭ

インターネットの出入口における基本的な対策としては、アクセス制御及びＩＤＳ／ＩＰＳが挙げられる。出口対策としてのアクセス制御は、あらかじめＣ＆Ｃサーバとして使用されるサイトをブラックリストに登録し、当該サイトへのアクセスをあらかじめ遮断することである。ただし、攻撃者はＣ＆ＣサーバのドメインやｉＰアドレスを頻繁に変更する等、攻撃インフラを再構築したりするため、ブラックリストへの登録はどうしても後追いとなってしまう。したがって、同一の攻撃者による被害の拡大を防ぐためには、Ｃ＆Ｃサーバのブラックリスト等を速やかに共有することが重要である。実際にアクセス制御を実施する機材は、入口対策の場合と同様にプロキシサーバやファイアウォールとなるが、その趣旨は入口対策とは異なるため、リストの管理は別々に実施すべきである。また、認証プロキシによるアクセス制御も標的型攻撃の対策として有効である。認証プロキシには、利用者がインターネットにアクセスする際に、パスワード等を用いた認証を実施することにより、ＲＡＴ等による不正なインターネットへのアクセスを制限する役割もある。しかしながら、ＲＡＴの中には、端末に保存された認証情報を窃取し、これを用いて認証プロキシを突破する機能を有するものもある。ＩＤＳ／ＩＰＳでは、Ｃ＆Ｃサーバとの通信における共通の通信挙動をシグネチャとして登録し、不正な通信を検知／遮断する。しかしながらＤｂＤ攻撃の場合と同様に、近年の標的型攻撃の通信は正常通信に類似しており、シグネチャの作成が困難である場合も多い。

端末やサーバにおける基本的な対策としては、ウイルス対策ソフト及び修正プログラムに加え、セキュリティポリシーの設定及びＨＩＤＳが挙げられる。ウイルス対策ソフト及び修正プログラムは、出口対策としても必要である。Ｗｉｎｄｏｗｓの標準の機能であるセキュリティポリシーについては、管理者権限の局限、端末及びサーバにおける証跡取得の設定が特に重要である。ユーザに不必要な権限が付与されていると、攻撃者に悪用される可能性がある。端末やサーバの証跡については、情報システムの内部に不正アクセスを受けた場合に、攻撃者の内部調査侵入の手口を明らかにするために有益となる。端末やサーバにおける証跡取得の設定がなされていない場合には、

不正アクセスを受けた際の攻撃者の行動を解明することは極めて困難となる。また、管理者権限のパスワードのキャッシュについては、端末に保存されることがないように運用にも留意する必要がある。特に重要なサーバについては、ＨＩＤＳを導入することにより、内部の不正な挙動や改ざんを検知することも重要である。

内部ネットワークにおける基本的な対策としては、アクセス制御及びＩＤＳ／ＩＰＳが挙げられる。内部ネットワークにおけるアクセス制御は、内部のネットワークを各領域に区分し、領域間のアクセスを必要最小限度にファイアウォールやルータで制御したりすることである。各領域に区分する際には、サーバ等が配置される重要な領域は分離し、特にＩＤＳ／ＩＰＳ等で監視を強化することが重要である。ＩＤＳ／ＩＰＳでは、シグネチャによる不正な通信の検知のほか、正常通信に合致しないパターンを検知するアノマリ検知のアプローチも有効である。さらに、各セキュリティ機材やネットワーク機材のログをＳＩＥＭ[82]に集約すれば、各ログの相関関係から不正な挙動を抽出したり、不正アクセスが発生した場合にも速やかに各ログを確認したりすることが可能となる。

６　おわりに

本稿では、標的型攻撃とその対策技術について説明した。第２節では、初期のＡＰＴ、本格的な標的型攻撃及びわが国における標的型攻撃について、具体例を挙げて説明した。第３節では標的型攻撃の定義と分類を示し、主に標的型メール攻撃とＤｂＤ攻撃の概要について説明した。第４節では、標的型攻撃の段階を示し、段階毎にその仕組みを説明した。第５節では、標的型攻撃の対策技術を入口対策と出口対策に区分して説明した。

本稿で解説した標的型攻撃は、数あるサイバー攻撃の中でも最も深刻な脅威である。標的型攻撃の問題は、情報システムの世界だけの単なるマルウェアの問題ではない。標的型攻撃の背景には、特定の個人や組織を狙い、数か月から数年の長期間にわたって執拗に攻撃を継続する主体が存在する。標的型攻撃の主体は、一個人、プロのハッカー集団、あるいは軍の専門部隊であるかもしれない。標的型攻撃は、もはや国家のインテリジェンス活動の手段ともなっている。したがって、国家の安全保障を考慮するにあたり、サイバー攻撃、とりわけ標的型攻撃の問題は、もはや切り離して議論することはできない。

本稿で示したのは、あくまでも基本的な対策技術である。標的型攻撃の手法

---

[82] SIEM (Security Information and Event Management) セキュリティ機器、ネットワーク機器、サーバ、アプリケーション等からログやイベント情報を集約し、統合的に管理する仕組みあるいはそのための機材

は日々刻々と進化しており、対策を回避する手法も次々と考案されている。また、標的型攻撃に利用される脆弱性も発見されている。したがって、本稿で示した対策を実施していたとしても、今後も継続して標的型攻撃を防ぐことができる保証はない。最新の技術動向や脆弱性に関する情報に注視し、セキュリティ対策を継続してアップデートしていくことが重要である。

本稿では、標的型攻撃と対策について、技術的な側面を取り上げた。当然のことであるが、標的型攻撃は技術だけでは防ぐことはできない。技術的な対策のみならず、情報システムの利用者の教育も重要である。今日では、情報システムをまったく使用しない職場はかなり減ってきている。また、情報システムと同じ仕組みで動作するスマートフォン、スマート機器等の普及もあり、誰もが何らかの形で情報システムの利用者となっている。そのため、情報システムやサイバーセキュリティに関する知識は、もはや全員に必須の素養となっている。情報システムやサイバーセキュリティに関する素養は、一般に年長者、高位者になるほど低い傾向がある。したがって、攻撃者にとっては、無知な年長者や高位者は絶好の脆弱なターゲットである。ある組織の情報システムおいてセキュリティ対策を万全に実施したとしても、そのＯＢや関係者、あるいは従業員の私用のパソコンが狙われ、そのような弱い所を足がかりとして不正アクセスが連鎖的に拡大してしまう場合も珍しくない。標的型攻撃では、情報システムの端末が一台でもやられると、その端末を踏み台として内部への不正アクセスが拡大してしまう。たった１名の情報システムの利用者の不注意がきっかけとなり、機密情報が窃取され、組織存亡の危機を招いてしまうポテンシャルを秘めている。したがって、専門家に任せきりではなく、全員が当事者であるという自覚を持たせ、必須の素養としてしっかりと体系的に教育を実施する必要がある。