サイバー戦入門

－サイバー攻撃の仕組みと技術的対策－

三村　守（防大情報工学科）

１　はじめに

陸・海・空・宇宙に続き、サイバースペースという第５のドメインが提唱され、サイバー戦という言葉ぐらいは誰もが耳にするようになった。近年ではサイバースペースの重要性は広く認知され、各国がサイバー戦能力の向上に積極的に取り組んでいる。国内では、従来の電子戦の概念がサイバースペースにも拡張され、包括的電子戦としての概念の整理及び、それに対応するための新体制の検討が実施されるようになってきた。しかしながら、その発端となったサイバースペースの特性については驚くほど理解されていない。これは、サイバースペースの重要性についてはある程度理解されつつあるものの、その変化に対応するための具体的な人材育成については、少数の専門家に重点が置かれているためであると考えられる。それにもかかわらず、全体の底上げを図るための組織的な取り組みは進んでいるとは言いがたい。

陸・海・空の従来のドメインは、各種戦に体系化されて整理されており、各々の規定が定められている。例えば、海のドメインでは、対潜戦、対空戦、対水上戦等に体系化されており、各戦闘の規定が明確に定められている。このような規定を策定するためには、各戦闘の特性が十分に理解されていなければならない。例えば、ミサイルが飛来したときにどのような対処をするべきかについては、各対抗手段の効果がどの程度か、あるいはそれらの対抗手段のコストはどの程度なのか等の特性が理解されていなければ策定のしようがない。陸・海・空の従来のドメインについては、将来の技術の進歩に伴って変化が生じる可能性はあるものの、このような特性は比較的に組織全般に理解されていると言える。

しかしながら、サイバースペースについては、サイバー戦に関する具体的な規定がなく、体系的な整理も不十分である。この原因の一端は、サイバー攻撃とは何かが組織全般に理解されていないためであると考えられる。これが組織全般に理解されていなければ、サイバースペースに関する組織的な取り組みを適切に進めることは困難である。また、サイバー作戦を立案して意思決定をする必要が生じた場合にも、そもそも作戦を立案することすら困難である。平時においても、新聞報道などでサイバー攻撃や情報流出の事件を目にする機会は増えてきている。それらの事件におけるサイバー攻撃が、自分たちの組織にどのようなインパクトを与えるのかを検討するためには、サイバー攻撃とは何か

を理解することが不可欠である。しかしながら、専門家以外にはサイバー攻撃はおろか、それを理解するためのサイバースペースに関する基本的な仕組みもほとんど教育されていないのが現状である。

そこで本稿では、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る。以下、第２節ではまずサイバー攻撃とは何かを理解するために不可欠な、脆弱性とは何かについて説明する。第３節では、その脆弱性を用いたサイバー攻撃の種類について説明し、第４節ではこれを攻撃者の視点から時系列で追っていく。第５節では、これらのサイバー攻撃に対抗するためのセキュリティ機材の役割について説明し、最後に全体をまとめる。

２　脆弱性とは何か？

サイバー攻撃とは何かを解説するにあたり、まずは「サイバー攻撃で何ができるのか？」という単純な問いについての検討からはじめたいと思う。サイバー攻撃では、対象となるシステムを錯乱、無力化、機能低下、破壊等様々なことが可能であるとされている。例えば、２００７年９月にイスラエルがシリアの施設を空爆した事件では、シリアの防空システムがサイバー攻撃を受けて無力化されたため、空爆を許してしまったと言われている[1]。２０１０年６月に発見されたスタックスネットと呼ばれるマルウェア[2]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いた[3]。さらに、２０１１年には米国の無人機が偽のＧＰＳ[4]信号により制御を奪われ、イラン領内に着陸させられて捕獲されたと言われる事件が発生した[5]。このように、サイバー攻撃では、その対象とするシステムの制御を奪うことができれば、その権限の範囲内で基本的にどのようなことでも実施できるポテンシャルを持っている。これらの事例からわかるように、サイバー戦の範囲はインターネットのみならず、制御システムやネットワーク化されたビークルにまで急速に拡大している。

このようなサイバー攻撃が引き起こされる主要な原因としては、対象となるシステムに脆弱性が存在することが挙げられる。脆弱性とは、システムの仕様、設計、実装等に起因する情報セキュリティ上の欠陥のことであり、正規の利用

---

[1]Fulghum, D.A. (2007). Why Syria's Air Defenses Failed to Detect Israelis, Aviation Week and Space Technology

[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]Kushner, D. (2014). The Real Story of Stuxnet, IEEE Spectrum

[4]GPS (Global Positioning System)

[5]Iran’s Alleged Drone Hack: Tough, but Possible, https://www.wired.com/2011/12/iran-drone-hack-gps/

者以外の第３者が悪用することが可能なものである。その脆弱性を突くコードは、エクスプロイト・コードと呼ばれ、人間には意味不明な機械語の文字列で記述される場合が多い。主な脆弱性の分類を表１に示す。脆弱性の種類は、大まかに「権限昇格」と「サービス拒否」に分類され、「権限昇格」はさらに「任意の命令実行」と「アクセス制限の突破」に分類される。これらの脆弱性にはまた、ネットワークを介して遠隔のコンピュータに適用可能なリモートの脆弱性と、ネットワークを介さずにコンピュータの内部に適用可能なローカルの脆弱性という分類がある。これらの脆弱性を突くコードは、それぞれリモート・エクスプロイト、あるいはローカル・エクスプロイトと呼ばれることもある。例示したような洗練されたサイバー攻撃は、単にこれらのエクスプロイトを利用するだけでなく、ソーシャル・エンジニアリング[6]等の様々な人的要素も組み合わせて入念に計画されていることが多い。

表１：脆弱性の分類

種類		説明
権限昇格	任意の命令実行	対象とするシステムの制御を奪い、任意の命令を実行することを可能とする脆弱性
	アクセス制限の突破	対象とするシステムのアクセス制限を突破し、保護されている情報の閲覧を可能とする脆弱性
サービス拒否		対象とするシステムのサービスの提供を妨害し、無力化あるいは機能を低下させることを可能とする脆弱性

（１）任意の命令実行

表１において一般的に最も深刻な脆弱性は、「任意の命令実行」の脆弱性である。この脆弱性は、対象とするシステムを制御下に置くことを可能とするものであり、攻撃者にとっては最も強力かつ使い勝手がよい。攻撃者が対象とするシステムを制御下に置いた後には、その権限の範囲内においてあらゆることが実行可能となる。

例えば、特定の人物にマルウェアを埋め込んだ不審なドキュメントファイルをメールで送りつける標的型攻撃[7]では、この種類の脆弱性が利用されることが多い。このタイプの攻撃では、当該ドキュメントファイルを閲覧するソフトウェア[8]の脆弱性を突き、任意の命令を実行してシステム利用者の端末を制御下において遠隔操作する。

---

[6]人間の行動や心理の特徴を悪用して機密情報等を入手する手法を指す。
[7]特定の組織の情報を狙って実施されるサイバー攻撃の一種
[8]ＭＳ　Ｗｏｒｄ、一太郎、Ａｄｏｂｅ　Ｒｅａｄｅｒ等

このタイプの脆弱性の影響を評価する際に注目するポイントは、任意の命令実行が成功する可能性と、当該システムが動作する権限の範囲である。脆弱性を突くことによる任意の命令実行は、必ずしも実行が成功するとは限らない。なぜならば、成功が攻撃者の制御不能な何らかの外部の環境に依存する場合や、純粋に確率に依存する場合もあるためである。当然のことながら、成功する可能性は高ければ高いほど使い勝手は良い。当該システムが動作する権限の範囲は、任意の命令実行が可能となる範囲を意味する。例えば、先のドキュメントファイルを閲覧するソフトウェアの脆弱性を突く場合には、当該ソフトウェアが動作する権限[9]の範囲内で任意の命令が実行可能となる。当該端末で管理者権限を必要とする命令を実行するためには、管理者権限で動作するシステム[10]の脆弱性を突く等の方法で、さらに権限昇格を実施する必要がある。

（２）アクセス制限の突破

「アクセス制限の突破」については、第３者がアクセス制限を突破して保護されている情報の閲覧を可能とする脆弱性である。攻撃者はこの脆弱性を利用し、保護されている機密情報を盗み出すだけでなく、その盗み出した情報がパスワードのようなものであった場合には、さらにその情報を用いて不正アクセスを継続することができる。

例えば、インターネットにおいてデータベースの検索結果などを提供するＷｅｂサーバにＳＱＬ[11]インジェクションの脆弱性がある場合には、攻撃者は検索文字列に不正な文字列を入力してＷｅｂサーバの脆弱性[12]を突き、一般には公開されていないデータベースの中身すべてを入手することができてしまう。この場合、保護されるべきデータベースの中身が流出してしまうことになる。また、そのデータベースにパスワード、あるいはそれに相当する情報が含まれていた場合には、攻撃者はその情報を用いてさらに不正アクセスを試みることができる。

このタイプの脆弱性の影響を評価する際のポイントは、流出する可能性がある情報の価値である。換言すると、その情報が流出することにより何が起こる可能性があるのかを検討すればよいことになる。

（３）サービス拒否

「サービス拒否」の脆弱性については、サービスを無力化あるいは機能を低下させることを可能とする脆弱性であり、一般に「権限昇格」の脆弱性よ

---

[9]一般ユーザの権限で動作していることが多い。
[10]ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）が提供するサービス等
[11]データベースを操作する際に用いるプログラム言語の一種
[12]正確にはそのＷｅｂサイトで動作するプログラムの脆弱性

りも影響は小さいことが多い。

このタイプの脆弱性の影響を評価する際のポイントは、影響を受けるサービスの価値とその影響の程度である。例えば、自分たちの組織のＷｅｂサーバに「サービス拒否」の脆弱性があった場合について検討してみる。当該Ｗｅｂサーバにおいて単に情報提供を実施している場合の影響は、その情報の閲覧に支障が生じるだけである。したがって、その情報を当該Ｗｅｂサーバで提供することがクリティカルでないのであれば、その影響は軽微であると言える。しかしながら、当該Ｗｅｂサーバにおいてオンライン・ショッピングのサービスを提供しているような場合には、当該サービスの提供に支障が生じてしまうと、売上に直接影響を与えてしまう可能性がある。したがって、このような場合には、その脆弱性の影響は重大であると言える。

なお、「サービス拒否攻撃[13]」は、必ずしも「サービス拒否」の脆弱性を利用したものであるとは限らない。例えば、Ｗｅｂサーバに通常のアクセスを大量に実施することで、当該Ｗｅｂサーバのサービスの提供を妨害することが可能である。このような脆弱性を用いない攻撃は、通常のアクセスと区別することが難しく、一般に対策は困難である。しかしながら、前述のとおり単に情報提供を実施するＷｅｂサーバであれば、その影響は軽微であることが多いことから、冷静に検討して過剰に反応しないことが重要である。

３　能動的攻撃と受動的攻撃の違い

以前にあまりこの分野に精通していない方から「ハッキングは防げるのに標的型攻撃はなぜ防げないのか？」という質問を受けたことがある。この質問にきちんと答えるためには、サイバー攻撃の手法の分類とその違いを理解する必要がある。サイバー攻撃の手法はいくつもあり、その分類の視点も様々である。その中でも筆者が特に重要と考える視点は、攻撃のタイミングである。攻撃のタイミングは、主導権の所在を意味するだけでなく、その影響範囲や対策にも大きく関係してくるからである。この視点に基づくと、サイバー攻撃は表２に示すように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、最初の質問にあったハッキングは能動的攻撃、標的型攻撃は受動的攻撃となる。

---

[13]コンピュータや回線に負荷をかけてサービスの提供を妨害する攻撃であり、DoS (Denial of Service)攻撃や DDoS (Distributed Denial of Service)攻撃とも呼ばれる。

表２：能動的攻撃と受動的攻撃の違い

攻撃の種類	タイミング	脆弱性	攻撃対象	例
能動的攻撃	攻撃者が主体的に任意のタイミングで実施可能	主にリモートの脆弱性を利用	主にインターネットに公開されたサーバ	・Ｗｅｂサーバに対するＤｏＳ攻撃 ・ホームページの改ざん
受動的攻撃	被攻撃者による何らかの動作を必要とし、その動作のタイミングでのみ実施可能	主にローカルの脆弱性を利用	主に利用者の端末（クライアント）	・標的型メール攻撃 ・ドライブ・バイ・ダウンロード攻撃 ・水飲み場攻撃

（１）能動的攻撃

能動的攻撃は、主にリモートの脆弱性を利用し、攻撃者が主体的に任意のタイミングで実施できる攻撃である。リモートの脆弱性とは、ネットワークを介して他のコンピュータに対して適用することができる脆弱性のことである。

例えば、図１に示すようなＷｅｂサーバに対するＤｏＳ攻撃は、攻撃者が自分の任意のタイミングで攻撃ツールを実行する（図１①）か、あるいは踏み台となるコンピュータに指示を与えることで実施する（図１②）ことが可能である。なお、ＤｏＳ攻撃には、対象とするシステムのメモリ等のサーバのリソースを圧迫するリソース枯渇型の攻撃と、ネットワークの帯域を飽和させる帯域枯渇型の攻撃があり、攻撃の種類によって対策も異なるので注意が必要である。

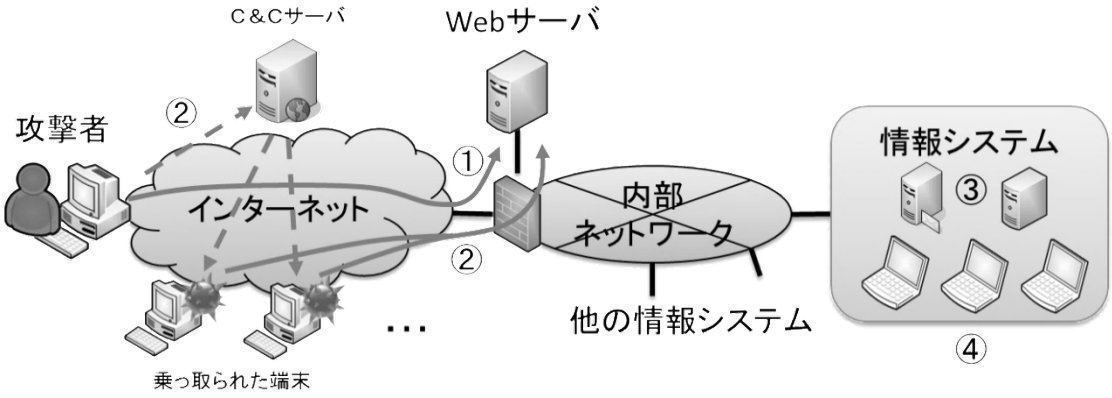

図１：Ｗｅｂサーバに対するＤｏＳ攻撃

ホームページの改ざんについても同様に、攻撃者が自分の任意のタイミングで、Ｗｅｂサーバでサービスを提供するソフトウェアの脆弱性を利用して実施することが可能である。なお、この脆弱性は、攻撃者がネットワークを介して細工を施した通信内容をＷｅｂサーバに送信し、当該Ｗｅｂサーバでサービスを提供するソフトウェアがその通信内容を処理する過程において発生する不具合のことである。

このような不特定多数からの能動的攻撃が可能となるのは、対象となるコンピュータ（この場合はＷｅｂサーバ）がインターネットに公開[14]されているためである。サーバがインターネットに公開されていれば、インターネットに接続する世界中のあらゆる端末（不特定多数）からアクセスすることが可能となる。したがって、組織の内部ネットワーク[15]でのみ公開されているサーバ（図１③）は、インターネットに接続されている端末からの能動的攻撃（図１①②）の対象とはならない。なぜならば、インターネットに接続されている端末からは、特別な設定[16]がされていない限り、内部ネットワークにアクセスすることはできないからである。しかしながら、同じ内部ネットワークに接続している端末（図１④）からはこのサーバにアクセスすることは可能であるため、内部ネットワークからの能動的攻撃の可能性は考えられる。

このように、能動的攻撃は攻撃者が任意のタイミングで実施することが可能であるが、その対象となるのは主にインターネットに公開されたサーバであり、内部ネットワークの利用者の端末を直接的に攻撃することは基本的にはできない。また、仮にインターネットに公開されているサーバの制御を奪ったとしても、サーバと内部ネットワークはセキュリティ機材により分離されていることが多いため、そのサーバを踏み台にして内部ネットワークに侵入することは困難である場合が多い。さらに、近年ではＯＳやミドルウェア等の基本ソフトウェアのセキュリティは強化されており、リモートの脆弱性は減少しているため、能動的攻撃によるリスクは相対的に減少していると考えられる。

（２）受動的攻撃

受動的攻撃は、主にローカルの脆弱性を利用し、被攻撃者による何らかの動作（トリガー）を必要とする攻撃である。ローカルの脆弱性とは、ネット

---

[14]正確にはインターネットで使用されるグローバルＩＰアドレスを保持している。
[15]インターネットとは異なる体系のＩＰアドレスを付与している。
[16]インターネットから特定のポートへの通信をあらかじめ指定した内部の機器に転送する設定

ワークを介さずにそのコンピュータの内部に適用することができる脆弱性のことである。

例えば、図２に示すような利用者にマルウェアを埋め込んだ不審なドキュメントファイルをメールで送りつける（図２①）標的型メール攻撃[17]では、利用者が受信したメールの添付ファイルを開いた際に、当該ドキュメントファイルを閲覧するソフトウェアの脆弱性が突かれ、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２②）。この場合、利用者が受信したメールの添付ファイルを開くことがトリガーになっており、受信者がメールの添付ファイルを開かなければ、攻撃者は当該端末を遠隔操作する（図２②③）ことはできない。なお、当該ドキュメントファイルを閲覧するソフトウェアの脆弱性とは、攻撃者が細工を施したドキュメントファイルを読み込む過程における不具合であり、ネットワークを介さずにそのコンピュータの内部で動作するものである。

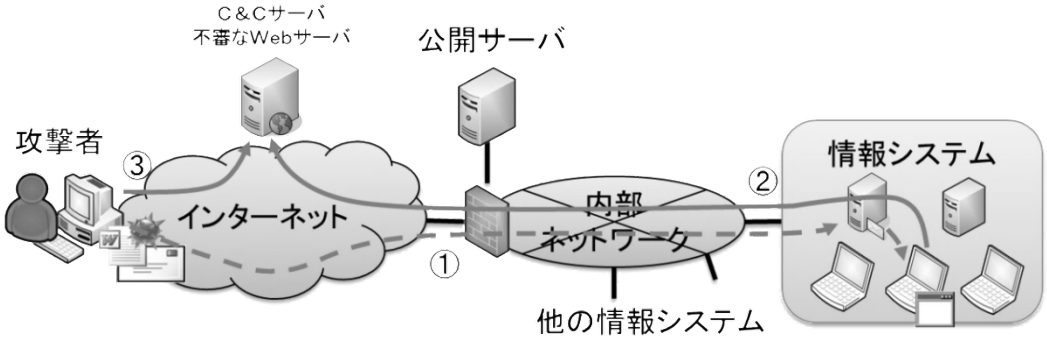

図２：標的型攻撃

また、利用者を不審なＷｅｂサーバに誘導してマルウェアに感染させるドライブ・バイ・ダウンロード攻撃[18]や、さらにその攻撃対象を特定の者に限定する水飲み場攻撃[19]では、利用者が当該不審なＷｅｂサーバにアクセス（図２②）した際に、そのコンテンツを読み込むソフトウェア[20]の脆弱性が

[17]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、利用者がその添付ファイルを開封する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

[18]Ｗｅｂサイトに不正なコンテンツを設置し、利用者がそのＷｅｂサイトを閲覧すると様々な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

[19]ドライブ・バイ・ダウンロード攻撃の一種であり、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（広義の水飲み場攻撃）と、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手法（狭義の水飲み場攻撃）がある。

[20]IE (Internet Explorer), Firefox 等のブラウザやそのプラグイン等

突かれ、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２②）。この場合には、利用者が当該不審なＷｅｂサーバにアクセスすることが脆弱性のトリガーになっており、利用者がリンクをクリックするなどして当該不審なＷｅｂサーバにアクセスしなければ、攻撃者は当該端末を遠隔操作することはできない。なお、コンテンツを読み込むソフトウェアの脆弱性とは、攻撃者が細工を施したコンテンツを読み込む過程における不具合であり、ネットワークを介さずにそのコンピュータの内部で動作するものである。

このように、受動的攻撃では原則として攻撃者は自分の任意のタイミングで攻撃を実施することはできない[21]が、添付ファイルの開封やリンクのクリック等の端末の利用者の動作を伴うことで、内部ネットワークの利用者の端末を攻撃することが可能となる。また、重要なシステムを物理的あるいは論理的に分離する対策[22]をとっていたとしても、スタックスネットのようにＵＳＢメモリ等の外部デバイスを経由して侵入する場合もある。攻撃者は利用者の端末を制御下に置いた後、その端末を踏み台にしてさらに内部ネットワークの奥に侵入を試みることが多い。近年ではＯＳやミドルウェア等の基本ソフトウェアのセキュリティは強化されてきているが、端末で動作するソフトウェアのローカルの脆弱性は未だに多く発見されている。また、利用者の端末や内部ネットワークの奥が攻撃対象となるため、機密情報の流出等、組織に深刻な影響をもたらす被害が発生する可能性が考えられる。したがって、今日では受動的攻撃によるリスクは相対的に増大していると考えられる。

４　攻撃の手順

ここまで、脆弱性のメカニズムと攻撃の種類について、技術的な観点を中心に説明した。次に、攻撃者の視点でサイバー攻撃の手順について説明する。

（１）能動的攻撃

能動的攻撃の場合、攻撃者は任意のタイミングでツール等を活用し、対象とするサーバを攻撃する。例えば、Ｗｅｂサーバに対するＤｏＳ攻撃を実施する場合には、ＬＯＩＣ（ロイック）[23]やＨＯＩＣ（ホイック）[24]等のツールを活用することができる。これらのツールは、アノニマス[25]がサイバー攻撃に使用したとされることで知られている。単純なＤｏＳ攻撃であれば、攻撃者はツールに標的とするＷｅｂサーバのＵＲＬやＩＰアドレスを直接入

---

[21]トリガーとなる動作が自動実行されるシステムでは任意のタイミングで実施できる場合がある。
[22]エア・ギャップと呼ばれる。
[23]LOIC (Low Orbit Ion Canon)ネットワークの負荷をテストするためのツール
[24]HOIC (High Orbit Ion Canon) LOIC の後継として開発されたツール
[25]インターネット上の活動家が緩やかにつながりを持った国際的なネットワーク

力するだけで実行することができる。また、もう少し洗練されたホームページの改ざん等の不正アクセスを実施するためには、Ｍｅｔａｓｐｌｏｉｔ[26]等の対話形式で命令を入力するツールを活用することができる。この場合にも、攻撃者は標的を入力し、攻撃手法や脆弱性の種類等を選択するだけで、容易に攻撃を実施することができる。利用する脆弱性の種類が権限昇格の場合には、ツールにその結果が出力される。攻撃者はその結果を確認し、攻撃が成功した場合にはその権限において対象とするコンピュータを遠隔操作することが可能となる。攻撃者はその得られた権限において任意の命令を実行し、さらに権限を拡大するための攻撃を実施して不正アクセスを継続する。

（２）受動的攻撃

受動的攻撃の場合には、攻撃者はいくつかの下準備を実施する必要がある。例えば、メールを用いた標的型攻撃を実施する場合には、攻撃者は対象とする人物や組織のメールアドレスを入手する必要がある。また、対象に実行させるための細工を施したファイルやコンテンツ、遠隔操作をするための踏み台となるサーバも準備する必要がある。

対象とする人物や組織のメールアドレスを収集する最も手軽な方法は、インターネットにおいて情報収集を実施することである。多くの企業や組織は、広報用のメールアドレス等をそのホームページに公開している。担当者は、このような広報用のアドレスに送信されたメールを開封せざるを得ない。攻撃者はこれらのアドレスに顧客や取引先を装ってメールを送り、そのやり取りでさらに別のメールアドレス等の攻撃に有益な情報を収集することが可能である。このように、攻撃者は攻撃に有益な情報を収集するために、あらゆる社会工学的な手法を活用することが可能である。

対象に実行させるための細工を施したファイルやコンテンツは、一般にマルウェアあるいはコンピュータ・ウイルスと呼ばれている。このマルウェアも、Ｍｅｔａｓｐｌｏｉｔ等の専用のツールを用いて作成することが可能である。メールを用いた標的型攻撃で使用するマルウェアは、主として実行ファイルとそれ以外のドキュメントファイル等に分類される。実行ファイルの場合には、そのファイルがそのまま利用者の端末で実行されることになるため、攻撃者は脆弱性を利用する必要はない。攻撃者は攻撃の成功率を高めるため、実行ファイルのアイコンを文書ファイルのアイコンに偽装したり、拡張子を偽装したりする。そのため、利用者はそのファイルを注意して観察すれば、マルウェアかどうかをある程度は判断することができる。一般に、メールに添付された未知の実行ファイルをクリックすることは非常に危険で

[26]エクスプロイト・コードの作成や実行を行うためのフレームワークであり、脆弱性の検査や検証のための事実上標準のツールとなっている。

ある。また、ショートカット形式のファイルやマクロ[27]のように、実質的に実行ファイルに相当するファイルも非常に危険である。そのため、メールへの実行ファイル、あるいは実行ファイルに相当するファイルの添付を禁止している組織もある。ドキュメントファイル等の場合には、攻撃者は利用者の端末の脆弱性を突くコード、あるいはマクロをドキュメントファイル内に埋め込む。利用者がこのドキュメントファイルを開封して脆弱性を突くコードが実行されるか、あるいはマクロを有効にすると、その制御が一時的に奪われる。そして、本体となる実行ファイルを文書ファイルから取り出し、あるいはインターネットからダウンロードして実行する。この本体となる遠隔操作をするための実行ファイルはＲＡＴ[28]と呼ばれる。標的型攻撃に用いられる著名なＲＡＴとしては、ＰｏｉｓｏｎＩＶＹ[29]（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[30]。その後、そのＲＡＴはあらかじめ準備した遠隔操作をするための踏み台となるサーバに接続を試みる。このように、受動的攻撃の場合には、内部ネットワークにある端末からインターネット側にあるサーバの向きに接続を試みさせている点が、能動的攻撃と受動的攻撃の違いを理解するための重要なポイントである。能動的攻撃と受動的攻撃の通信の違いを図３に示す。インターネットと内部ネットワークは異なるＩＰアドレスの体系を利用していることが多いため、基本的にインターネット側から利用者の端末に能動的にアクセスを試みることはできない。しかしながら、内部ネットワークの利用者の端末からインターネットに公開されたサーバには、途中の経路でＩＰアドレスが変換され、能動的にアクセスできるようになっている場合がほとんどである。受動的攻撃では、この内部ネットワークからインターネットへアクセスする一方向性をうまく利用していると言える。

[27]複数の手順を自動的に実行させる機能
[28]Remote Administration Tool あるいは Remote Access Trojan
[29]FireEye (2014). "POISON IVY: Assessing Damage and Extracting Intelligence"
[30]Kaspersky Lab (2015). BLUE TERMITE －日本を標的にする APT 攻撃－

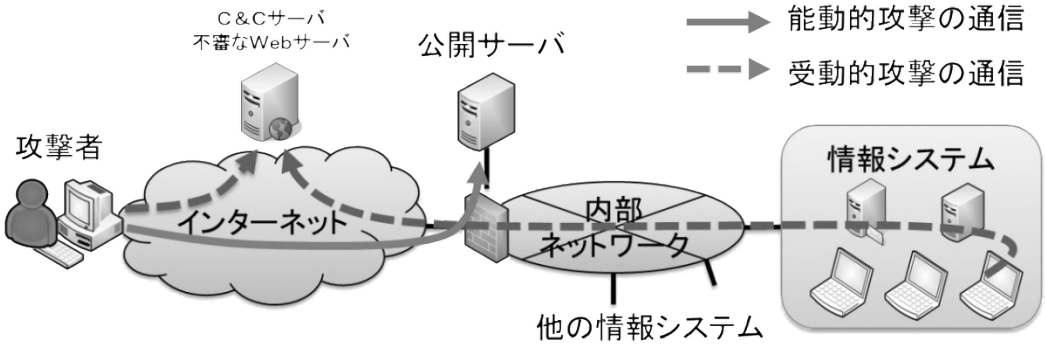

図３：能動的攻撃と受動的攻撃の通信

遠隔操作を実施するための踏み台となるサーバは、自分で用意したサーバをインターネットに接続して準備することもできるが、一般には能動的攻撃によって乗っ取るか改ざんしたサーバを用いることが多い。攻撃者は踏み台とするサーバを乗っ取った後、標的となる利用者の端末からの接続を待ち受けるプログラムを設置する。このプログラムは標的となる端末からの接続を受け付けた後、攻撃者はその端末を恒久的に遠隔操作することが可能となる。この場合、攻撃者の命令と制御に関する通信は、踏み台となったサーバを介して送受信されるため、このサーバはＣ＆Ｃ（Ｃ２）[31]サーバと呼ばれる。

５　対策とその効果

次に、サイバー攻撃の対策とその効果について、セキュリティ機材の機能と役割を中心に説明する。主なセキュリティ機材とその機能は表３に示すとおりである。以下、各機材の機能とその役割について解説する。

表３：主なセキュリティ機材とその機能

セキュリティ機材	機　能
ウイルス対策ソフト	主として端末の内部を監視し、既知の不正なファイルを検知する。
ファイアウォール、ＷＡＦ[32]、ルータ	ネットワーク上の通信を監視し、あらかじめ設定したルールに基づいてアクセス制御を実施する。
プロキシサーバ	端末の代理でインターネットにアクセスする。

[31]C&C or C2 (Command and Control)
[32]WAF (Web Application Firewall)

ネットワーク型侵入検知装置[33]	ネットワーク上の通信を監視し、不正な通信を検知あるいは遮断する。
ホスト型侵入検知装置[34]	主としてサーバの内部を監視し、不正な振る舞いを検知する。
ゲートウェイ型ウイルス対策製品	ネットワーク上の通信を監視し、不正なファイルを検知する。

（1）ウイルス対策ソフト

最も一般的なセキュリティ対策製品は、ウイルス対策ソフトである。今日では、よく管理されたネットワークであれば、ウイルス対策ソフトがインストールされていない端末はほとんど存在しない。ウイルス対策ソフトは、主として端末の内部を監視し、不正なファイルを検知するソフトウェアのことである。

ウイルス対策ソフトはパターンファイルというウイルスの定義ファイルを持っており、このパターンファイルに合致するファイルやデータを発見した場合には、それをマルウェアあるいは脅威として検知し、可能であればそれを除去する。このパターンファイルは、発見されたマルウェアを分析してその結果をもとにして作成される。近年では、最新のパターンファイルでも検知できない未知のマルウェアは、毎日当たり前のように発見されている。したがって、パターンファイルを常にアップデートして最新の状態に維持しておいたとしても、マルウェアを検知できるという保証はない。特に洗練された標的型攻撃は、ＡＰＴ[35]や新しいタイプの攻撃と呼ばれており、あらかじめ最新のパターンファイルを用いたウイルス対策ソフトで検知されないことを確認したマルウェア（未知のマルウェア）が用いられることが多い。

この未知のマルウェアは、ゼロデイ攻撃と呼ばれる未知の脆弱性を用いた攻撃と混同しないように注意が必要である。今日では、未知のマルウェアは毎日大量に発見されているが、脆弱性はそれほど多く発見されているわけではない。また、発見された未知の脆弱性の中でも、標的型攻撃に利用できる攻撃者にとって使い勝手の良い脆弱性は非常に限られている。未知のマルウェアは、基本的にウイルス対策ソフトでは検知することはできないが、既知の脆弱性を突くエクスプロイト・コードを用いていることが多い。したがって、脆弱性を修正するプログラム（パッチ）を適用さえしていれば、攻撃を

[33]NIDS (Network based Intrusion Detection System)
[34]HIDS (Host based Intrusion Detection System)
[35]APT (Advanced Persistent Threat)

防げる場合がほとんどである。これに対し、未知の脆弱性を用いたゼロデイ攻撃は、そもそもその修正プログラムが存在しないため防ぐことは困難である。攻撃者にとって使い勝手の良い未知の脆弱性は限られており、アンダー・グラウンドのマーケットでは高値で取引されていると言われている。したがって、スタックスネットのように複数の未知の脆弱性を用いたマルウェアを作成する能力がある組織は、非常に限られていると言える。

（２）ファイアウォール

代表的なセキュリティ機材として知られるファイアウォールは、ネットワーク上の通信を監視し、あらかじめ設定したルールに基づいて単純にアクセス制御を実施する機材である。このアクセス制御を実施するためのルールはＡＣＬ[36]と呼ばれる。ファイアウォールの設置場所は、インターネットと公開サーバの境界や、公開サーバと内部ネットワークの境界等の通信の要所に設置される場合がほとんどである。最近では、ファイアウォールは多くの端末にもソフトウェアとしてインストールされている。ファイアウォールは自動的にサイバー攻撃を防いでくれる魔法の箱ではない。単なるアクセス制御のための機材であり、適切にルールが設定されていなければただの箱である。したがって、ファイアウォールの役割を理解するためには、どのようなルールを設定できるかを理解する必要がある。

伝統的なファイアウォールでは、通信内容の論理的な最小の単位であるパケットの送信元、あて先及びそれらのプロトコル[37]に基づいてアクセス制御を実施する。パケットの送信元とあて先はＩＰアドレスで、それらのプロトコルはポート番号で指定する。アクセス制御とは、そのパケットの通過を許可するか拒否するかを設定することである。送信元とあて先については、単一のＩＰアドレスで設定することもできるし、複数のＩＰアドレスをまとめて設定することも可能である。実際のファイアウォールのルールは、複数のルールに優先順位をつけて複雑に組み合わされている。近年では、分割されたパケットを再構築して、通信内容に対してより高度なアクセス制御を実施する[38]ＷＡＦと呼ばれるファイアウォールも登場している。ＷＡＦはその名が示すとおり、ＳＱＬインジェクション等のＷｅｂサーバに対する複雑化した攻撃に対応するために開発されたセキュリティ機材である。各セキュリティ機材等のアクセス制御機能の違いを表４にまとめる。

---

[36]ACL (Access Control List)

[37]通信を実施する上でのお互いの取り決めごと（通信規約）のことであり、この場合にはポート番号を示す。

[38]例えば通信内容の本文に特定の文字列を含むものを遮断する。

表４：各セキュリティ機材等のアクセス制御機能の違い

	ＩＰアドレス	ポート番号	通信内容
ファイアウォール	○	○	×
ＷＡＦ	○	○	○
ルータ	○	×	×

表４に示すとおり、単純にＩＰアドレスに基づくアクセス制御だけを実施したいのであれば、ファイアウォールだけでなく、パケットの経路をあて先に基づいて決定するルータでも実施可能である。他方、インターネットに公開されるＷｅｂサーバにおいて、データベースと連係した検索サービス等を提供している場合には、ＷＡＦの導入も検討に値するであろう。表４の分類は、あくまでも基本的な機能に基づいている。実際には、最近のファイアウォールにはＷＡＦと同等の機能や、後述するネットワーク型侵入検知装置の機能を付加した複合的な製品も存在している。また、多くのルータではポート番号によるアクセス制御が実施可能である。したがって、セキュリティ機材の選定にあたっては、その製品の機能をよく確認し、重複する無駄な機能がないように留意すべきである。

ファイアウォールのＡＣＬの設定のポリシーは、大まかに２とおりに分類される。

１つは、通過を拒否する設定を列挙して組み合わせるブラックリスト方式である。ブラックリスト方式のＡＣＬの例を表５に示す。この例では、表５中の「192.168.0.0/24」[39]は内部ネットワークのＩＰアドレス全体を示している。ポート２５はメールの送信、ポート１１０はメールの受信に使用されるプロトコルである。したがってこの例では、内部ネットワークからのメールの送受信が拒否され、それ以外の通信は許可される。このように、ブラックリスト方式では、あらかじめ不正な通信をすべて列挙して完全に網羅する必要がある。したがって、網羅できなかった言わば想定外の不正な通信については通過してしまう可能性があるため、あまり推奨されない。

表５：ブラックリスト方式のＡＣＬの例

送信元		あて先		動作
IP アドレス	ポート	IP アドレス	ポート	
Any	Any	Any	Any	許可
192.168.0.0/24	Any	Any	25	拒否

[39]192.168.0.1～192.168.0.254 の範囲

192.168.0.0/24	Any	Any	110	拒否

もう１つの方式は、通信を許可する設定を列挙し、それ以外の通信はすべて遮断するホワイトリスト方式である。ホワイトリスト方式のＡＣＬの例を表６に示す。表６中の「192.168.0.0/24」は同様に内部ネットワークのＩＰアドレス全体を示している。ポート８０及び４４３はインターネットへのＷｅｂアクセスの際に使用されるプロトコルである。したがってこの例では、内部ネットワークからのＷｅｂアクセスが許可され、それ以外の通信は拒否される。実際のネットワークでは、許可すべき正常な通信はこれよりもかなり多いことがほとんどである。このように、ホワイトリスト方式では、あらかじめ許可する正常な通信をすべて列挙する必要があるが、想定できなかった不正な通信を通過させてしまう可能性を局限できる。したがって、可能であればファイアウォールのルールはホワイトリスト方式で設定すべきである。なお、ここでいう不正な通信とは、送信元、あて先及びプロトコルの組み合わせが不適切なパケットを意味しており、必ずしも不正アクセスを意味するわけではない点には注意が必要である。

表６：ホワイトリスト方式のＡＣＬの例

送信元		あて先		動作
IP アドレス	ポート	IP アドレス	ポート	
192.168.0.0/24	Any	Any	80	許可
192.168.0.0/24	Any	Any	443	許可
Any	Any	Any	Any	拒否

次に、ファイアウォールが能動的攻撃及び受動的攻撃に対してどのような役割を果たすかについて考察する。

主としてインターネットに公開されているサーバに対して実施される能動的攻撃に対しては、ファイアウォールは主に不適切なプロトコルを遮断するという役割を果たす。例えばＷｅｂサーバであれば、そのプロトコルはあて先ポート８０番を利用するパケット及びその応答のパケットに制限することができる。基本的にはそれ以外のパケットの通過は許可する必要はない。送信元及びあて先に関しては、Ｗｅｂサーバは一般に不特定多数の送信元を想定しているため、アクセス制御を実施することは困難である。しかしながら、実際にＤｏＳ攻撃等のサイバー攻撃が発生した場合には、その送信元を遮断するルールを一時的に追加することは対策としてありえる。

主として内部ネットワークの端末に対して実施される受動的攻撃に関し

ては、能動的攻撃のように直接的な対策となるわけではないが、内部ネットワークにおいて端末に侵入された後の不正アクセスの拡大を妨げるという役割を果たす。例えば、内部ネットワークのファイアウォールにおいて、あらかじめ一般の端末同士の通信を遮断するルールを設定していれば、攻撃者による端末から端末への不正アクセスの拡大を防げる可能性がある。このように、ネットワークの構成やセキュリティポリシーに応じて、普段から多層防御の考え方でセキュリティ対策を実施しておくことは非常に重要である。

（３）プロキシサーバ

プロキシサーバは、内部ネットワークの中に配置され、端末の代理でインターネットにアクセスする（図４①）。ここで、ファイアウォールにおいてプロキシサーバ以外の端末からインターネットへのアクセスを遮断（図４②）すれば、すべて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を経由することになる。このように、従来のプロキシサーバの役割は、主にインターネットへのアクセスログ[40]を集中管理することや、アクセスが多いサイトのキャッシュ[41]を保存し、通信量を緩和することであった。また、プロキシサーバを経由した通信は、通信先のサーバからはプロキシサーバからの通信に見えるため、内部ネットワークの構成を保護するという役割を果たしている場合もあった。

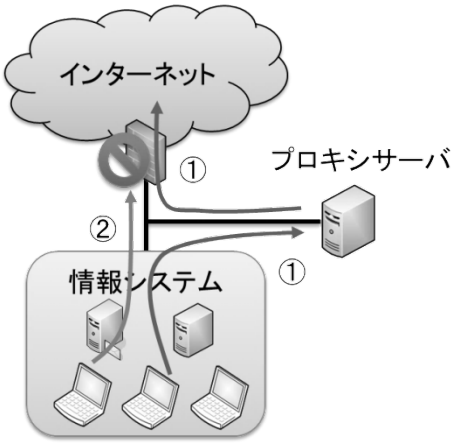

図４：プロキシサーバの仕組み

しかしながら、Ｗｅｂアクセスを模擬したＲＡＴの通信やドライブ・バイ・ダウンロード攻撃の発生に伴い、Ｃ＆Ｃサーバとの通信や不審なＷｅｂ

[40]アクセスの日付、時間、アクセス先、アクセス元等を記録した証跡
[41]一度アクセスしたサイトのデータを一時的に保存し、次回同一のサイトにアクセスがあった際の表示を速くするためのデータ

サーバへのアクセスをブラックリスト方式でブロックする用途でも用いられるようになった。端末の利用者の意図に反したＣ＆Ｃサーバとの通信をブロックするため、ＩＤとパスワードによる認証機能を持つものもある。そのため、近年ではプロキシサーバはセキュリティ機材の１つと考えることもできる。

プロキシサーバと従来のファイアウォールで実施するアクセス制御機能の違いは、ファイアウォールでは主にＩＰアドレスやポート番号でアクセス制御を実施するのに対し、プロキシサーバではＵＲＬ、ドメイン名等でアクセス制御が実施できることである。ＷｅｂアクセスやＲＡＴの通信先は、多くの場合にＵＲＬ等で指定される。さらに、標的型攻撃ではこのＵＲＬ等に対応する最終的な通信先であるＣ＆ＣサーバのＩＰアドレスはしばしば変化する。そのため、プロキシサーバでは、ファイアウォールよりも効率的にアクセス制御を実施することが可能である。

また、プロキシサーバに蓄積されるアクセスログには、Ｗｅｂアクセスによる不正な通信が記録されていることが多い。そのため、何らかの手段でＣ＆Ｃサーバや不審なＷｅｂサーバのＵＲＬを入手した場合には、プロキシサーバのログにアクセスした痕跡があるかどうかを確認することで、不正アクセスの有無を確認することが可能である。アクセスログは、大規模な組織では膨大な量であり、一定の期間ごとにバックアップをとってから過去のログを消去して運用している場合が多い。過去のアクセスログを調査する場合には、バックアップデータからの復元に時間を要するため注意が必要である。したがって、運用者としてはこのバックアップの期間や容量を知っておくことは有益である。

なお、国内でＰＣの遠隔操作による誤認逮捕で話題となったＴＯＲ[42]は、このプロキシサーバの一種と言える。ＴＯＲは、図５に示すように複数のノードを経由し、通信を多重に暗号化することで、アクセス元の特定を極めて困難にする機能を提供している。まず、アクセス元はノード１（入口ノード）にアクセスする（図５①）。その後、この例では計６つのボランティア・ノード[43]を経由してアクセス先に到達するため、アクセス先からはノード６（出口ノード）からのアクセスにみえる（図５②）。この時、出入口ノードを除く各ノードは、暗号化により中継する通信内容を知ることはできない。ＴＯＲのように不特定多数の通信先を経由して通信の匿名性を向上させるサービスが有効に機能するためには、インターネット上で動作する多数のボランティア・ノードの存在が不可欠である。したがって、このようなサービ

[42]TOR (The Onion Router)
[43]自主的にサービスを提供するサーバ

スの質を評価するためには、その機能だけでなくサービスの実態も調査する必要がある。

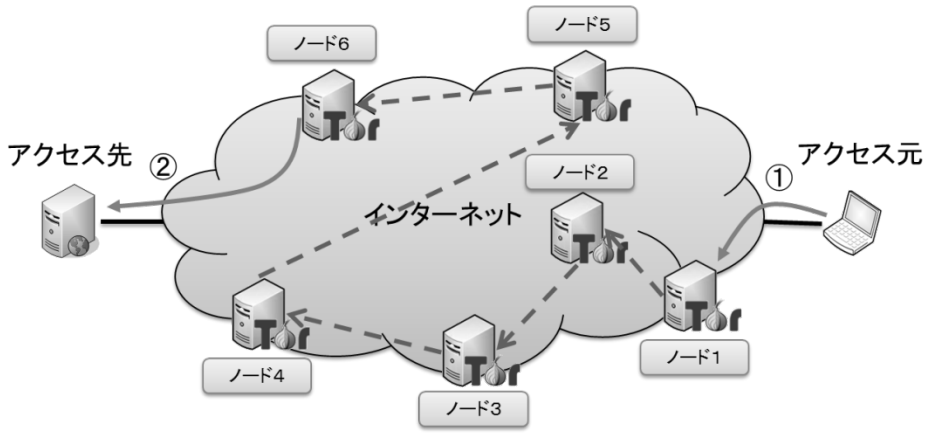

図５：ＴＯＲの動作の仕組み

（４）ネットワーク型侵入検知装置

ネットワーク型侵入検知装置は、ネットワーク上の通信を監視し、不正な通信を検知あるいは遮断する。不正な通信を検知する機能を持った機材を侵入検知装置、遮断する機能を持った機材を侵入防止装置（ＩＰＳ[44]）として区別する場合もある。ネットワーク型侵入検知装置もファイアウォールと同様に、インターネットと公開サーバの境界や、公開サーバと内部ネットワークの境界等の通信の要所に設置される場合が多い。その設置方式は図４に示すとおり、アウトライン方式とインライン方式がある。

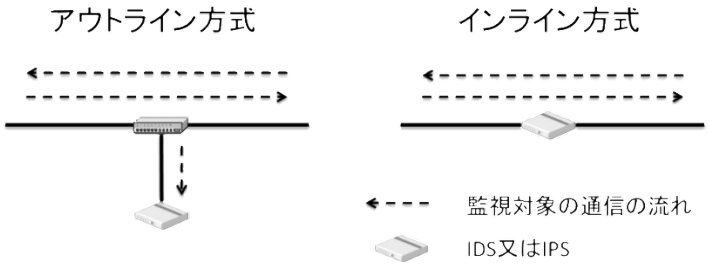

図４：ネットワーク型侵入検知装置の設置方式

アウトライン方式では、装置は監視対象の通信が流れる回線の外側に設置される。具体的には、監視対象とする通信を傍受できる機材から、通信内容のコピーを装置に転送する。したがって、アウトライン方式の場合には、

[44]IPS (Intrusion Prevention System)

一般に通信を遮断することはできない。インライン方式では、装置は監視対象とする通信が流れる回線の内側に設置される。侵入防止装置は不正な通信を遮断する必要があるため、一般にこの方式で設置されることが多い。

次に、装置がどのように不正な通信を検知するかについて説明する。ネットワーク型侵入検知装置は、傍受したパケットを再構築してその通信内容を検査する。ここで言う通信内容とは、主にブラウザやＷｅｂサーバ等のソフトウェアで自動的に処理される内容であり、暗号化された通信内容や電子メールの内容のように利用者のプライバシーを侵害するようなものではない。ネットワーク型侵入検知装置は、傍受したパケット及び再構築した通信内容に対し、あらかじめ登録された不正通信のパターンに合致するか否かを判定し、合致した場合にはアラートと呼ばれる警告を発する。この不正通信のパターンはシグネチャと呼ばれ、一般的に文字列やそれにやや柔軟性を持たせた正規表現で定義される。したがって、ネットワーク型侵入検知装置は、あらかじめシグネチャで定義された既知の攻撃は検知することができるが、未知の攻撃を検知することは困難である。シグネチャで検知できない新しい攻撃を検知するためには、その攻撃のパターンを定義して新たなシグネチャを作成する必要がある。このように、ネットワーク型侵入検知装置のシグネチャは、ウイルス対策ソフトのウイルス定義ファイルのようなものであり、定期的に更新する必要がある。更新の頻度についてはウイルス対策ソフトのように毎日必要なわけではないが、一般に１か月から数か月の単位で実施されている。

ネットワーク型侵入検知装置はネットワーク上の通信を監視する機材であるため、ネットワークを経由して適用されるリモートのエクスプロイト・コードを検知するのに適している。よってその主な役割は、能動的攻撃を検知、あるいは遮断することである。その運用にあたっては、シグネチャの深刻度と普段の傾向を十分に把握しておく必要がある。ネットワーク型侵入検知装置では、誤検知[45]のアラートが発生することは珍しくなく、設定によってはしばしば発生することもある。したがってアラートが発生した場合には、その深刻度と普段の傾向を考慮した上でその内容を評価し、誤検知か否かを判断する必要がある。

このように、従来のネットワーク型侵入検知装置の役割は、主に能動的攻撃を検知することであった。しかしながら、近年では受動的攻撃の脅威の増大に伴い、端末の遠隔操作のためのＣ＆Ｃサーバとの不正な通信を検知する用途にも用いられるようになってきた。この遠隔操作のための通信にはリモ

[45]この場合は偽陽性（False Positive)のこと。なお、不正アクセスを正常な通信として見逃すことを偽陰性（False Negative）と呼ぶ。

ートの脆弱性を突くコードが含まれているわけではなく、正常な通信と区別することが困難である場合が多い。したがって、シグネチャを作成する場合にはその通信に含まれる文字列や正規表現だけでなく、その接続先であるＣ＆Ｃサーバのアドレスを用いる場合もある。このように、受動的攻撃を防ぐためには、攻撃者が利用するＣ＆Ｃサーバのアドレスを把握することが非常に重要である。したがって、受動的攻撃において利用されるＣ＆Ｃサーバのアドレスをブラックリストとして登録し、その情報を共有することは有益である。

（５）ホスト型侵入検知装置

ホスト型侵入検知装置は、主としてサーバの内部を監視し、不正な振る舞いを検知するための装置であり、通常はソフトウェアで提供される。ホスト型侵入検知装置は、コンピュータ内部での不正なコマンドの実行や、ローカルのエクスプロイト等の不正な挙動を検知する役割を果たす。それらの不正な挙動を検知するための仕組みは、基本的にネットワーク型侵入検知装置と類似しており、あらかじめ定義したシグネチャに合致する不正な挙動に対してアラートを発生させる。ただし、このシグネチャの内容は、ネットワーク上の通信内容ではなく、主にコンピュータ内部での挙動によって定義される。もちろん、最新の攻撃手法等に対応するためには、シグネチャは定期的に更新する必要がある。

もうひとつの重要なホスト型侵入検知装置の役割としては、サーバの内部のコンテンツの改ざんを検知することが挙げられる。この機能は、あらかじめ更新が発生しない正常なファイルの状態を記録しておき、定期的にそのファイルの状態に変化がないかを確認することによって、改ざんがあったかどうかを検査する。

不正アクセスや改ざんによってアラートが発生した場合には、その深刻度と普段の傾向を考慮した上でその内容を評価し、誤検知か否かを判断する必要がある。

（６）ゲートウェイ型ウイルス対策製品

ゲートウェイ型ウイルス対策製品は、ネットワーク上の通信を監視し、不正なファイルを検知あるいは遮断するセキュリティ機材のことである。ゲートウェイ型ウイルス対策製品はその名称が示すとおり、ネットワークの経路上にインラインで設置される。従来のゲートウェイ型ウイルス対策製品の動作は、すでに説明したウイルス対策ソフトの動作原理とほぼ同様である。したがって、その効果を発揮するためには、パターンファイルを常にアップデートして最新の状態に維持する必要がある。しかしながら、近年のＡＰＴや新しいタイプの攻撃と呼ばれる洗練された標的型攻撃では、あらかじめ最新

のパターンファイルを用いたウイルス対策ソフトで検知できないことを確認したマルウェアが用いられることが多いため、その効果は疑問である。

そのため、近年ではサンドボックスと呼ばれる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サンドボックス型の製品が登場している。このようなマルウェアを実際に動作させて分析する手法は、動的解析と呼ばれている。これに対し、実際にマルウェアを動作させずに分析する手法は静的解析と呼ばれる。サンドボックス型の製品は、主に外部から受信するメールの添付ファイルや、内部ネットワークの端末からインターネットへのアクセスを重点的に監視する。サンドボックス型の製品は、ネットワーク型侵入監視装置と同様に、ネットワークの経路上にアウトラインで設置する場合とインラインで設置する場合がある。検知したマルウェアを即座に遮断したい場合には、インラインで設置する必要がある。しかしながら、サンドボックス型の製品では実際にマルウェアを動作させるため、従来のゲートウェイ型ウイルス対策製品よりも負荷が大きい。そのため、インラインで設置した場合には通信速度が低下する可能性がある点には注意する必要がある。

６　おわりに

本稿では、サイバースペースの特性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た。第２節ではサイバー攻撃とは何かを理解するために不可欠な、脆弱性とは何かについて体系的に整理して説明するとともに、その影響を評価するためのポイントについて述べた。第３節では、サイバー戦のルールを理解するために、能動的攻撃と受動的攻撃の違いについて説明し、第４節ではこれを攻撃者の視点から時系列で整理した。第５節では、これらのサイバー攻撃に対抗するための代表的なセキュリティ対策であるウイルス対策ソフト、ファイアウォール、プロキシサーバ、侵入検知装置等の仕組みと役割について説明した。

本稿は、専門家以外の方々のサイバー・セキュリティに関する素養の底上げを図り、サイバー・セキュリティに関する理解を促進することを目的として執筆した。冒頭で述べたとおり、陸・海・空の従来のドメインは、各種戦に体系化されて整理されており、各々の規定が定められている。オペレータはこれらの規定や各ドメインの特性を考慮して作戦を立案し、意思決定をすればよい。しかしながら、サイバー・ドメインには具体的な規定がないばかりか、体系的な整理も不十分である。そのため、組織内で認識を共有することは極めて困難であると言わざるを得ない。このような状況では、適切な意思決定はおろか、作戦の立案も容易ではない。サイバー作戦を立案するためには、少なくともそ

のドメインの特性に関する理解は不可欠である。今日、サイバー戦の範囲はインターネットのみならず、制御システムやネットワーク化されたビークルにまで急速に拡大しており、ＳＦ小説や映画で描かれたサイバー攻撃の脅威が現実のものとなりつつある。また、シリアの防空システム、スタックスネット、米国の無人機等の事例を考慮すると、サイバー・ドメインは単独で考慮すべき対象ではなく、すでに各種戦や平時の活動とも密接に関係していると言える。

したがって、サイバースペースの特性は少数の専門家だけが理解していれば良い問題ではなく、組織全体で素養として理解していなければならない基本的な事項であると考えられる。本稿により、サイバースペースの特性を理解するために必要なサイバー攻撃の基本的な仕組みとその対策について、専門家以外の方々に少しでもご理解いただければ幸いである。