卒業論文

日本における情報セキュリティの現状

―現在の情報セキュリティ市場を覗いて―

東洋大学　経営学部　経営学科
1310160233 番
旭ゼミナール
鈴木秀嘉

目次

1.はじめに

現在の私たちの生活を形成している環境では様々な種類の情報が溢れかえっているのである。また、それらの情報の使用手段も様々であり、時代が進むにつれてそれは複雑化しているのである。我々はこれにより様々な場所で恩恵を受けていることは現代を生きている皆さんには理解しやすいのではないだろうか。そんな環境で生活している我々にとって見逃せない項目が存在するのである。それは現代の社会で恩恵を受けている我々にとって必然的に生まれたものといえるかもしれないもの、いつの時代にも存在するもの、それが犯罪者である。しかも、彼らは時代に沿って進化し、適合しており、我々の社会ではネット犯罪者、サイバーテロ、ハッカーなどの情報を悪用し、現代社会に大きな被害をもたらす存在となっているのである。にもかかわらず、我々の中には彼らの行動に気が付いていない者も数多く存在しているのである。その結果、そういった被害は年々増加しているので、そのことを知ってもらうため、また、それに対して私たちはどのように対応しているのかを確認するため、さらには、それらを知って我々はどのような行動をとるべきかといった現代社会特有の犯罪やその対処方法を調べ、考察するために今回は情報セキュリティという分野がどのように進化しているのかを検証していくのである。

故に、この論文における「情報セキュリティ」とは「企業や個人などが保有する機密情報などを外部の脅威から守る」という意義を含むものとして考えていくものであり、情報をより円滑に使用するといった情報処理分野の定義を今回は除外して考えているのでその点を踏まえた上でこの論文を読んでもらいたいのである。

ただし、情報セキュリティを検証するためにはその分野で使用される用語について理解してもらわなければならないので、ここからは頻繁に使用する語句についてはそれぞれの章の文頭に記述していくのでそれを理解したうえで論文を読み進んでもらいたいのである。そうすることで今回の論文をより一層深い次元で理解することができるからである。

以下、2章ではサイバー犯罪の現状を日本と世界規模で示し、3章はサイバー攻撃の表と裏を説明していき、サイバー攻撃を世間のために使えることを説明していくのである。4章は企業が実行しているサイバーセキュリティ対策について紹介していき、従来の技法と最新の技法を挙げ、比較していくのである。5章では情報セキュリティ市場の変化を記述していくのである。ここではサイバーセキュリティ市場がどのように変化してきたのかを資料などを使い説明していくのである。6章は日本にこれから求められるものを今までの記述や収集した情報をもとに考えていき、また、オリンピックに向けての日本のサイバーセキュリティ対策を考察していくのである。7章のおわりにではこの論文から見えたものを自分なりに解釈し、それを記載していくのである。以上が今回の論文の構成であるので、今回の論文のテーマ、サイバーセキュリティについて少しでも興味を持ってくれたら幸いである。

2.サイバー犯罪の現状

本章では現在の情報社会において発生している犯罪を日本規模と世界規模の２つの面から紹介し、その際に使用された犯罪の手口なども提示していく章である。また、この文章では以下の用語を特に理解してもらいたいのである。

サイバー犯罪

・コンピュータ技術及び電気通信技術を悪用した犯罪、ハイテク犯罪とも言われるもので、日本においてサイバー犯罪は主に次の３つに分類されているのである。

不正アクセス禁止法

・この法律は他人が不正に人のパスワードを入手し、アクセスする行為を防ぐものであり、これに違反したものは重い刑罰が科せられるのである。

コンピュータ・電磁的記録対象犯罪、不正指令電磁的記録に関する罪

・コンピュータの処理を間違えさせ、コンピュータやシステム上に記録されたデータを不正に改ざんする行為を罰するものであり、これに反したものは法に則った罰が与えられるのである。

ネットワーク利用犯罪

・ネットワークを利用した犯罪、又は犯罪の実行に必要不可欠な手段としてネットワークを利用した犯罪のことであり、これを実行したものは罰を科せられる。

マルウェア

・コンピュータの正常な利用を妨げたり、利用者やコンピュータに害を成したりする不正な動作を行うソフトウェアの総称であり、その種類としては、コンピューターウイルスやワーム、トロイの木馬、スパイウェア、ランサムウェア、キーロガー、バックドアなどがあるのである。

標的型攻撃

・特定の目標に対して経済的利益あるいは安全保障に悪影響を与えるなどの意図を持つ情報搾取、偵察などの活動のことで、主にウイルスを付与したメールの送信などのサイバー攻撃などがあるのである。

この論文ではサイバー犯罪をこの３つに分類して説明していくが、近年サイバー犯罪の手口が複雑化しているため、犯罪の種類によっては罰がいくつも課せられるものがあるので必ずしも犯罪に対する罪が一つでないことを理解してもらいたいのである。その種類について詳しく知りたい方はそのことについて詳細に述べている警察庁ホームページ「第１節　サイバー犯罪の現状」を読むべきである。

２－１　日本のネット犯罪の現状

我々の社会で発生しているサイバー犯罪は近年増加傾向にあるのである。対策側、警察などもその犯罪に対して様々な案を練り、対応している。例えば警察庁はサイバーテロ対策室を立ち上げ、進化するサイバー犯罪に対応したり、サイバー犯罪専門の窓口を作ったり、広告などの情報発信媒体を利用して外部に向け注意を促しているのである。にもかかわらず、被害は年々増加しているのである。

図 1 は警視庁が発表したサイバー犯罪者の検挙数である。これを見るに、2103 年は 8,113 件であったが 2107 年には 9,014 件まで増加しているのである。この結果を見るとサイバー犯罪者を警察が捕まえて被害が減っているように見えるかもしれないが実際はそうではないのが現実である。この増加は犯罪が増え、その結果、検挙数が増えているにすぎないのである。つまり、現状ではサイバー犯罪を完全には止めることは出来ていないということである。

犯罪者の手口も巧妙になっているため、対策側が対処しきれない場面が数多く存在しているのである。その中でも有名な事件をいくつか挙げるのでそれについて深く考えてほしいのである。

年次	H25	H26	H27	H28	H29
年次(西暦)	2013	2014	2015	2016	2017
不正アクセス禁止法違反(件)	980	364	373	502	648
コンピュータ・電磁的記録対象犯罪、不正指令電磁的記録に関する罪(件)	478	192	240	374	355
ネットワーク利用犯罪(件)	6,655	7,349	7,483	7,448	8,011
計	8,113	7,905	8,096	8,324	9,014

図表 1 サイバー犯罪の検挙件数の推移（引用元警察庁（2011）.「第 1 節 サイバー犯罪の現状 - 警察庁 Web サイト」）

犯罪者の手口も巧妙になっているため、対策側が対処しきれない場面が数多く存在しているのである。その中でも有名な事件をいくつか挙げるので日本のサイバー犯罪の現状について深く考えてほしいのである。

2.1.1 ケース 1～日本年金機構情報漏洩（2015 年 6 月）～

日本年金機構の年金情報管理システムサーバが外部の不正アクセスにより情報漏洩し、年金加入者の個人情報が約 125 万件流出したのである。

流出した個人情報項目内訳は

基礎年金番号、氏名（流出件数　約 3.1 万件）

基礎年金番号、氏名、生年月日（流出件数　約 116.7 万件）

基礎年金番号、氏名、生年月日、住所（流出件数　約 5.2 万件）

手口：日本年金機構の福岡市内オフィスで職員がメールに添付されているファイルを開封した際に PC がマルウェアに感染し、その PC から機構 LAN に接続され、細分化された複数のフォルダから情報を抜き取られたとされているのである。

この事件はかなり有名なものではないだろうか。手口としては上記で示したとおり標的型攻撃であり、それはまさにサイバー犯罪の典型例として考えられるものである。現代社会においてはこのような方法で我々の情報が他人に盗まれる危険性が含まれているのであ

る。この事件はいまだ解決しておらず、犯人特定に至っていないのである。それほどサイバー犯罪での検挙は難しく、一般犯罪と比べ検挙率がいいとは言えないのである。

この事件をもとにこの会社のセキュリティ対策において改善を行い、また、国、NISC（内閣サイバーセキュリティセンター）もこの事件を受けて以下の政策を打ち出したのである。

・インターネット接続がある府省庁情報システムで類似の攻撃を受けていないか点検、
・各府省庁における個人情報を含む重要情報の適正管理を職員へ徹底
・独法、特殊法人等、重要情報を取り扱いについて改めて指導を徹底
・これら全ての結果を迅速に NISC へ報告

この事件においては先ほどの分類のうちネットワーク利用犯罪があてはまると考えているのである。

2.1.2 ケース２～「東京都税クレジットカードお支払サイト」への不正アクセス発生（2017 年 3 月 10 日）～

当サイトの利用者のクレジットカード情報 67 万 6,290 件が外部へ流出した可能性があり、そのの可能性があるのは、2015 年 4 月～2017 年 3 月 9 日（午後 11 時 43 分）までにサイトを利用した都民の情報で、流出した個人情報の詳細は下記

・クレジットカード番号
・有効期限
・利用者のメールアドレス

の３つである。

ただし、同サイトは、2017 年 3 月 11 日現在運用停止となっており、また、これまでに情報の不正使用等は確認されていないということである。

今回の不正アクセスは、2017 年 3 月 9 日に IPA（情報処理推進機構）からの情報提供で発覚し、その後、同サイトを運営する GMO ペイメントゲートウェイの調査により 3 月 10 日に不正アクセスが確認されたのである。

手口としては何らかの方法で当企業の個人情報を保護している箇所のアクセス権を何らかの方法で入手し、それを利用して今回のような事件を起こしたと考えているのである。

故にこの事件は不正アクセス禁止法に反しています。この事件で朗報なのがいまだ流通したクレジットカードの情報が使われていないことであろうが、もし、IPA が気付いていなければこの事件は発覚しなかったわけで、もしかしたら誰かのクレジットカード情報が気付かないうちに利用されていたかもしれない。このように、サイバー犯罪は気付かれないものが多く、気付いた時にはすでに悪用されていたという事件も存在する。

ケース３：インターネットバンキング不正送金

インターネットバンキングとは、各金融機関が設置しているインターネット上の銀行取引サービスのことで、それを利用したインターネットバンキング不正送金の被害額はなんと 30 億 7300 万円になっているのである。被害にあった銀行は、大手銀行だけでなく、地方銀行から信用金庫までさまざまであり、ターゲットは常に変更され、新しい手口であな

たの預金は狙われているのでる。その手口が以下のようなものである。

銀行からのメールを装い、「システム向上のため」という虚偽の事実を告げて偽のサイトにアクセスさせ、お客様情報の入力を促すのである。この場面ではログイン ID やパスワードだけでなく、送金するための暗証番号も入力することを促され、ここで入力して送信すると、犯人に口座情報全てが流通してしまい、預金をすぐに引き抜かれてしまうことがあるのである。このように実在する金融機関の名前を借り、メールをその企業の利用客に送りつけ、偽サイトに誘導してログイン ID やパスワード等を入力させる行為は、「フィッシング詐欺」と呼ばれる犯罪となるのである。

そのほかにも顧客情報を盗もうとする行為が存在するのである。それが不正送金ウイルス、マルウェアによる手法である。これは、本物の金融機関のウェブサイトにアクセスした際にログイン情報が盗まれるというもので、メールやウェブ閲覧中に顧客の使用デバイスをウイルス感染させ、必要のない情報を入力してしまう事例が数多く存在しているのである。このマルウェアによる不正送金手口は実に上手くできており、実際の金融機関のサイトにアクセスした際に、本物とは異なった別の入力画面に移り変わるように設定されているので、利用者はそのまま気づかずにログイン情報などを入力してしまうのである。

このように様々な手段を用いて顧客情報を入手しようと試みており、その手口は年々巧妙になっており、被害者が気付かないことが多いというのが現状である。そのため、その被害額が増加してしまっていると警察庁は公表しているのである。

２－２世界のサイバー犯罪の現状

2.2.1 ケース 1～ＰＥＴＹＡによる大規模なサイバー攻撃(2017 年 6 月 27 日発見)～

ウクライナを中心に欧州やロシアで 27 日、大規模なサイバー攻撃が起きたのである。

ウクライナでは政府機関や、中央銀行を含む金融機関、首都キエフの空港などのほか、チェルノブイリ原発も被害を受けていたことが明らかになったのである。また、このサイバー攻撃は欧州全域から米国にも拡大したとみられているのである。

この攻撃によりチェルノブイリ原発周辺の放射線の自動監視システムの一部が 27 日に使えなくなり、手動に切り替えられたのである。このような原発に対するサイバー攻撃で被害が出るのは極めて異例であったのである。この事件においては、施設の基幹システムは正常に動いており、新たな事故につながる恐れはないということが後の検査から確認されているのである。

ウクライナでは政府や金融機関のコンピューターネットワークの一部がダウンしており、また、攻撃の発信元は明らかになっていないのである。しかし、政府は「ウイルスを分析したところ、ロシアが関与した可能性がある」と発表したのである。

今回のサイバー攻撃では、５月に日本を含む世界規模の広がりをみせた身代金要求型ウイルス（ランサムウェア）の「ワナクライ」に似た「ＰＥＴＹＡ」が使われたといわれているのである。

ウクライナのほか、広告の英ＷＰＰグループや海運のデンマークのＡ・Ｐ・モラー・マースクなど国際展開する大手企業での被害が明らかになっており、また、ロシアでは鉄

鋼大手エブラズや国営石油ロスネフチが攻撃を受けたほか、インドでも被害があったと発表されている。

また、この攻撃の発覚によりイギリスの政府機関サイバーセキュリティセンターは声明を出し、「世界規模でランサムウェアによる攻撃が起きている。企業や公共機関はこうした攻撃から身を守るために対策を講じてほしい」と注意を呼びかけたのである。

ワナクライとは

あるハッカー集団がアメリカ国家安全保障局からエターナルブルーという脆弱性攻撃プログラムを盗み出したことにより作成されたものであり、このプログラムは世界中の多くの人が使う Windows の脆弱性を突くものであったのである。

また、従来のランサムウェアとは違い、このウイルスはワーム型であったのである。ワーム型のウイルスというのは文字通りワームのようにパソコンの中を勝手に動き回り、インターネットや LAN 経由でどんどん広がっていき、その結果、被害が加速度的に拡大していったのである。

ワナクライの主な感染経路はメールで、メールに添付してあるファイルを開くなどの行為によって感染し、知らないうちに自分のパソコンで複製、メールを送信といった形で広がっていったのである。

特徴は、感染したパソコンのユーザーから身代金を奪おうとする「身代金要求ウイルス」であることで、パソコンに侵入してデータを暗号化し、もとに戻したい場合はお金を払えと要求するのである。今まではこの金銭の受けとりの際に何らかの証拠が残り逮捕できるという可能性があったのですが、今回は支払いにビットコインが使われたのでその方法があまり使えず、困難を極めたのである。インターネットの発達によって匿名性も増していき、いまだに犯人の足取りさえつかめていない案件が数多く存在しているのである。

「PETYA」(ペトヤあるいはペチャ)とはこのワナクライの亜種とされているものである。しかも、これにおいては動作を完全に停止できる装置「キルスイッチ」が有効にされているワナクライと違い、PETYA はキルスイッチが有効になっておらず、動作を停止させる方法はまだ見つかっていないため、このウイルスによる被害は拡大すると考えられているのである。

2.2.2 ケース 2~国際的ハッカー集団によるサイバー攻撃~

国際的ハッカー集団である「Anonymous（アノニマス)」が北朝鮮の対外宣伝用の WEB サイトに対してサイバー攻撃を行い、登録利用者のデータを盗み出したとする犯行声明を発表したのでる。また、この攻撃の目的が

・北朝鮮政府は平和と自由への脅威になりつつあることの表明
・核開発の中止、金正恩第 1 書記の辞任、自由な直接民主制の導入
・全ての市民への検閲無しのインターネットアクセスの容認

を要求することであったのである。

しかし、攻撃を受けたと思われる北朝鮮は何の被害も受けていないと発表し、自国のセキュリティの高さを国外に示した。これが本当かどうかはいまだ確かめられていないので

ある。

今回の事件のように金銭的目的だけではなく、政治的・社会的主張に基づく、サイバー攻撃も世界中で行われているのである。

このように現代においてサイバー犯罪は国をも動かしえる影響力を持っているのである。なぜならば、冒頭でも述べたように現代社会は様々なものが情報化されているため、いったんその情報が盗まれた場合、それは様々なものに悪用されてしまうのである。今回でいうと氏名や住所などの個人を特定できる情報が漏洩、盗まれているのでそれをもとに個人に対して金銭を要求したり、本人が知らないうちに金銭を盗んだり、別の場所でその情報を使用したりする犯罪が行われる可能性もあるのであるのでサイバー犯罪において国は大きく動きうるのである。

2－3従来のサイバーセキュリティの常識は通用しない

近年、サイバー攻撃に使われるサイバーウイルスや技法が複雑化、巧妙化しているため、我々が今まで考えていたサイバーセキュリティの基本対策が全く通用しなくなっているのである。例えば次の5つが挙げられる。

コンピュータを最新の状態にするために、OSやアプリケーションにパッチを使用したり、アップデートしたりするのが今までの我々の常識であったが、高度なサイバー攻撃の前では攻撃者しか存在を知らない未知のウイルスや作成者本人などが気付いていない脆弱性箇所を悪用したものが発生しており、最新の状態にしていたとしてもサイバー攻撃の被害に遭うケースは数多く存在するのである。

ウイルス対策ソフトを最新の状態にしてコンピュータ内などを検査することは一般的サイバーセキュリティ対策になるが、1日に数十万の新種が発生している現在においてはウイルス対策ソフトの効果も限定的となってしまっているのである。そのため、ウイルス対策ソフトの検知率はせいぜい 40～50%程度になってしまっているのである。また、近年では標的型攻撃のような未知のマルウェアを使った攻撃も増加しており、従来のウイルス対策ソフトではもはや検知できないという状況に陥ってしまっているのである。

怪しいWebサイトを閲覧しないというのは一般常識であるが、一般の人が普段閲覧するような正規のWebサイトであったとしても改ざんされるなどといった悪意のある第三者からのサイバー攻撃により発生する事件が多発しており、何も知らない人がその改ざんされたWebサイトを閲覧した場合、そのサイトからマルウェアに感染することがあるのである。このようなサイトは本物のサイトとほとんど区別が付けづらく、素人には全く分からないのが現状なため、その被害はさらに拡大しているのである。

不審なメッセージは開かないという行為は前述の怪しいサイトを閲覧しないという行為と同じで周知のことではあるが、近年ではソーシャルエンジニアリングと呼ばれている騙しのテクニックが利用されており（個人のパスワードを何らかの方法で盗み取ったり、ネットワーク利用者や顧客になりすまし、新しいパスワードを聞き出したりするなどの手法)、普通にメールを読んだだけではそのメールが悪意のあるものなのかどうか不審に思わないようなメールを作成し、サイバー攻撃をおこなうため、ある程度の知識と余程の注意力を持っ

た人でない限り、見破るのは難しくなっているのである。

出所のよくわからないソフトウェアやアプリをインストールしないというのもごくごく一般的なものであるが、近ごろは著名ソフトウェア企業のアップデートサーバを改ざんし、悪意のあるプログラムを搭載した偽アプリが蔓延しているのである。これも中々本物と区別が付きにくいため、本人が知らないうちに自分の電子機器がウイルスに汚染されるという被害が拡大しているのである。

２－４なぜサイバー犯罪は起こるのか

サイバー犯罪が起こる理由は数多く存在しているのである。何故ならば、今の我々の生活環境がこの犯罪を促進させる要因を数多く含んでいるからである。現在の社会は前述で述べたように様々なものが情報化されており、その使用方法も多様である。しかしながら、それらには一つの共通点が存在していると考えているのである。それは様々なものを電子的情報化していることである。ここでいう電子的情報化とは様々な事象、知識、行動などをネットワーク世界に留めるあるいはその世界で活用するなどの行為を可能にするためにものを電子的存在に変化させることである。そうすることで私たちは様々な場面で過去よりも楽に行動ができるのであるが、その一方で、それらのもの、行動がある一定の世界において存在、あるいは行動しているため、その世界に侵入することができれば誰もがそこに存在するものを入手、利用できるのである。これは昔よりも我々の秘密や行動などがより危険にさらされていることを意味しているのである。その世界を利用すれば簡単にお金を手にしたり、欲しいものを簡単に奪ったりするなどの犯罪行為が可能になるのである。また、技術の発達によりこの世界への侵入は容易になってきているのである。極端に言うとやり方を教えれば小学生であろうと企業のネットワーク環境に侵入し、様々な情報を閲覧、盗むなどの犯罪活動を行えるのである。このことを踏まえ、我々は自分たちの情報、企業の秘密事項が危険な状態にさらされていることを自覚しなければならないのである。

その他にも要因は存在しており、情報化社会における匿名性の高さが裏目に出ていることである。この匿名性により、我々は以前よりも人目を気にせずに様々な行動を容易に行えるようになったが、その一方で、犯罪者たちの匿名性も高めてしまったのである。そのせいで、彼らは匿名性を武器に様々な角度から犯罪活動を行っているのである。匿名性は個人を特定することを困難にするものであるため、犯罪活動を行った人間を守ってしまい、だれがどのようにしてその行為を行ったのかなどの情報を隠してしまうのである。その結果、犯罪者を捕まえるまでに時間がかかってしまい被害が増大したり、犯罪行為への罪悪感を薄れさせてたりしてしまうのである。

情報を扱う媒体が数多く存在しているのも要因の一つになっているのである。何故ならば、利用する媒体が多ければ多いほど管理が難しくなり、その結果、被害にあったことに気付くのが遅れたり、知らぬ間に犯罪に使われたりするなどといったことが引き起こされるのである。

さらには、盗まれた情報場ブラックマーケットで売られているのである。また、そのマーケットではサイバー犯罪を行うためのソフトも売られており、専門知識がないものでも犯罪

行為を行えるようになってしまうのである。ちなみに盗まれた情報の値段としては以下が基本的相場である。

メールアドレス 1000 件　　⇒￥1,000
パスポートスキャン画像 1 枚⇒￥200
ゲームアカウント　　⇒￥1,500
カスタムマルウェア　　⇒￥350,000
クレジットカード情報　　⇒￥2,000

このほかにも様々な情報が売られており、そこでは一つの国だけではなく様々な国の情報が売られているのである。

また、現在の情報社会において情報を守る側の人材が攻める側と比べ圧倒的に不足しているため、攻撃に対しての防衛が間に合わなかったり、気付くことができなかったりといった事象が多くあり、犯罪者の危機感を和らげている状況にあるのである。

このような理由の他にも多くの理由が今の社会には数多く存在しているので我々は今一度自分たちの電子的情報化された物の扱い方について思考する必要があり、また、自分たちがどのような状況下で生活しているのかを再認識する必要があるのである。

3．サイバー攻撃の表と裏

この章ではサイバー攻撃を行う側、ハッカーについて語っていくのであるが、その際に 2 種類のハッカーを説明していくのである。そうすることでサイバー攻撃がすべて悪ではないということを理解してもらい、よりいっそうこの項目について理解を深めてもらいたいのである。

3.1 ホワイトハッカー

3.1. 1 ホワイトハッカーとは

ホワイトハッカーとは、優れたコンピュータ技術を持つハッカーであり、また、その技術を世の中のために活用しようとする人たちのことであり、善玉ハッカー、ホワイトハットハッカーとも呼ばれているのである。

ホワイトハッカーは基本的に政府や企業などにセキュリティ対策の人材として雇われ、サイバー攻撃を予防するため、システムへ許可をもらったり、事前に告知するなどして善意で侵入し、そのセキュリティプログラムが本当に情報を守れるかどうかをテストし、その結果を企業に報告したりするなどして、企業がサイバー攻撃を受ける前にセキュリティの不備を指摘するのが主な仕事である。

また、ホワイトハッカーはサイバー攻撃手法を熟知しており、前述で説明したサイバー攻撃、ユーザーのデータを人質に身代金を要求するランサムウェアなどの様々な悪意のあるサイバー攻撃から大切な情報を守るのも彼らの仕事である。

3.1.2 ホワイトハッカーに必要なもの

基本的にホワイトハッカーになるための資格は存在していませんが、獲得することでホワイトハッカーとしての知識、経験が身につくものがいくつか存在し、有名なものとしては

CEH、情報処理安全確保支援士（国家資格)、ホワイトハッカーの育成機関への入学などがあるのである。

CEH（Certified Ethical Hacker：認定ホワイトハッカー）は米国 EC-Council 社が提供する国際的な資格であり、アメリカで人気がある情報セキュリティの資格の一つである。

この資格の考えとして、ブラックハッカーに対抗するには、ブラックハッカーのように考える必要があるというもので、より実践的なカリキュラムが用意されているのである。そこではブラックハッカーの攻撃手法を学び、サイバー攻撃者の視点からその攻撃、ハッキングなどの様々なサイバー攻撃を理解することで、セキュリティ技術を高めていくのである。そこではマルウェア、スニッフィング、SQL インジェクション、暗号技術など 18 のモジュール、専門技術が用意されており、最新のセキュリティ技術を習得することができるようになっているのである。

情報処理安全確保支援士は、従来の「情報セキュリティスペシャリスト試験」の後継に当たる資格で、IPA（情報処理推進機構）が試験を実施しているもので、情報セキュリティに関する実践的な技能を自分は所有していることを証明してくれる資格であり、情報セキュリティに関する資格としては国内最難関と認定されているものである。

試験に合格して登録することで、情報処理安全確保支援士と名乗ることができるようになり、現在、様々な企業でセキュリティ対策は重要事項であり、それに携わる技術者を必要としているので、この資格を持っていると就職が有利になるのである。

サイバーセキュリティ人材、ホワイトハッカーなどを育成する機関として、平成 29 年に総務省の予算成立を受け「ナショナルサイバートレーニングセンター」が設置されたのである。

このナショナルサイバートレーニングセンターでは、国の行政機関などを対象としてサイバー防御演習を実施する「CYDER」、2020 年の東京オリンピックを想定してサイバー演習を行う「サイバーコロッセオ」、若年層を対象にセキュリティ技術を指導する「SecHack365」という 3 つの事業が存在し「SecHack365」では、25 歳以下の社会人や学生が公募で集められ、サイバーセキュリティに関する開発・研究・実験・発表が一年を通して行っているのである。これらの演習に参加している人たちは自ら開発したプログラムを発表したり、一流の研究者や技術者などの専門家たちと交流したりする中で、日々セキュリティに関する技術を磨いていき、一流のホワイトハッカーになれるように努めているのである。

このようにホワイトハッカーになるための資格はないものの、世間では様々な角度からホワイトハッカーに様々なものを提供したり、要求したりするようになっているのである。そこから察するに、ホワイトハッカーにはそれ相応の技術が求められていることが明らかである。

3.2 ブラックハッカー

今までは犯罪の方法や事件を説明していたが、肝心な犯罪者については深くは説明していなかったので今回はサイバー犯罪者について説明していくのである。

3.2.1 ブラックハッカーとは

ブラックハッカーは前述のホワイトハッカーとは真逆の存在であり、様々なウイルスを使用し、ありとあらゆる場所へサイバー攻撃を行う者たちである。2 章で述べた様々な事件は彼らによる仕業であり、また、彼らの行動理由は様々であり、時にはお金目的であったり、世界に対しての何らかの声明であったりするのである。また、彼らによる被害は小さいものから莫大なものまで幅広く存在し、時には国を脅かす事件を引き起こすこともあるのである。最悪なことに、彼らの攻撃は発見しづらく、気付いた時にはすでに情報が盗まれていたり、お金を盗まれていたりするのである。

また、ブラックハッカーによる攻撃は日々行われており、その件数は発見できるものだけでも計り知れない数となっているのである。その方法は日々進化しており、使用されるウイルスなどは常に新しいものが使われるなど、企業などが対策しづらいように巧妙な手を使っているのである。

サイバー犯罪では個人で行う者もいれば集団で行う者も存在するのである。その中でも有名なサイバー犯罪集団、シャドーブローカーズと Anonymous について今回は紹介していくのである。

3.2.2 シャドーブローカーズ

前述で述べたワナクライの話題で「あるハッカー集団がアメリカ国家安全保障局からエターナルブルーという脆弱性攻撃プログラムを盗み出したことにより作成された」という文章を記載したがこの「あるハッカー集団」というのが彼ら、シャドーブローカーズである。彼らはアメリカが誇るエリートハッカー集団でもあるアメリカ国家安全保障局に対してハッキングを行ったのである。これは一般的に考えて非常事態である。何故ならば、多くの国は通常自国の情報を様々なセキュリティプログラムを用いて厳重に保管しており、そこにアクセスできるのもほとんどおらず、使用制限が自国民に対してでも設けているのである。しかし、シャドーブローカーズはその防壁を突破し、アメリカの機密情報などを盗み出したのである。その際に、ワナクライの元となるプログラムを同時に奪い取ったのである。そして、彼らはそれを利用し、様々なサイバーウイルスを作成し、全世界で悪用、流通させたのである。彼らのサイバー攻撃の対象は様々であり、時には不特定多数の人へサイバー攻撃を行ったり、またある時は一国のサーバーを全て停止させたり、原子力発電所の機能を停止、変更させたり、銀行を使えなくしたりするなどして世界各国にその技術の高さを誇示しているのである。また、1 年間に起こるサイバー攻撃の大半がシャドーブローカーズによるものであると言われているのである。これほど広範囲に活動していてもいまだその正体は掴めておらず、構成員や出身国、年齢などの詳細なことは何もわかっていないのである。

3.2.3　Anonymous

図表 2Anonymous のシンボル（引用元）アノニマスの仮面がドンキで買える！仮面の意味や由来はあの映画？

彼らは匿名のハッカー集団であり、Anonymous（アノニマス）は無名・匿名を意味するのである。この集団は主に国家や大企業に対する抗議活動をサイバー攻撃で行うのであり、その手段として，DDoS 攻撃(ネット上の特定サーバーに大量のデータを送りつけるなど)で，インターネット上の特定のサーバーをアクセス不能にしたり，サーバーに侵入し，データの改ざんや流出を行ったりする集団だが，現在までのところ特定されていないのである。

彼らが実際に起こした犯罪としては前述の北朝鮮を筆頭に、オーストラリア政府への攻撃、アラブの春、麻薬組織への対抗、違法ダウンロード刑事罰化への対抗、過激派組織 ISIL へ宣戦布告、ネットいじめの犯人探し、KKK 名簿の公表などが挙げられる。これらは犯罪活動ではあるが、中には世間から賞賛を浴びている事件も存在しており、彼らの行動から影響を受けてサイバー攻撃を行うような者たちも現れているのである。さらには Anonymous を題材とした映画やドラマなどが数多く作成されており、彼らの行動は良くも悪くも世間に様々な影響を与えるほどの影響力が携わっているのである。そのいい例として次のものが挙げられるのである。

3.2.3.1　Anonymous に憧れた少年ハッカー

2016 年に兵庫県警警備部が、同県内に住む高校２年の少年（１６）を書類送検した事件があり、その内容が自宅のパソコンにコンピューターウイルスを保管していたことによる不正指令電磁的記録保管容疑で書類送検されたというものである。不正指令電磁的記録保管とは不正指令電磁的記録に関する罪の一つであり、これはコンピューターウイルスの作成、提供、供用、取得、保管行為を罰せるものである。

少年は中学入学後、ネットでブログを書くようになってアノニマスの存在を知り、憧れを抱くようになり、プログラミングに使う「Ｃ言語」を独学で習得し、アノニマスのメンバーと名乗る国外のハッカーたちと英語で交信し、ハッキング技術を磨き、高校入学後、ハッキングに使うためのパソコン２台を自力で組み立てたのである。

しかし、少年には外部のサーバーを乗っ取る技術がなく、実際にインターネットバンキングの不正送金などに使用されるウイルス、Ｚｅｕｓを使った攻撃を仕掛けることはできなかったが、自身のパソコン内に作り出した仮想空間で攻撃の予行演習を繰り返していたと述べたのである。また、少年は警察の調べに対して「環境が整えば攻撃を試していたと思う」とも打ち明けたのである。後に県警が押収した少年のパソコン内にはＤｏｓ攻撃に使うツールが９６種類も保管されており、その中の１種類は自作のプログラムであったのである。

この少年の犯罪が公になった理由としては少年がツイッター上で、政府を標的にしたサイ

バー攻撃を示唆する不穏なやりとりを行い、また、自身のツイッターに「秘蔵フォルダ」、ウイルスと疑われる９種類の不正プログラムが入ったものを公開したことで、公開理由は「アノニマスのメンバーから技量をばかにされ、攻撃を受けたときに仕返しができることを知らせたかった」と述べていたのである。馬鹿にされた原因としては、ネット上でハッキングツールを搭載した「アノニマスＯＳ」というプログラムが流通した時に少年がアノニマスを自称するメンバーにプログラムの存在を通知したが、そのプログラムがウイルスだったことが後に判明し、少年はそのプログラムがウイルスだと見抜けなかったことで少年の保有する技術がそこまで高度のものではないと見なされ、そこから仲間内で無視されるようになったことがその原因となったということが分かっているのである。このようにかなり若い年齢層の者でもサイバー犯罪集団に影響を受け、犯罪活動をゲーム感覚で行ってしまうのである。

また、前述の犯罪集団このほかにもインターネット上には、「Lizard Squad」や「APT28」などのさまざまなシステムにダメージを与えようとする集団が多く存在しているのである。そんな彼らの目的は政治的メリットのためや単なる楽しみのため、お金を楽に手に入れるためなどの個人的理由から国家的理由などのさまざまな理由が存在しているのである。

このように現代においてサイバー犯罪は国をも動かしえる影響力を持っているのである。なぜならば、冒頭でも述べたように現代社会は様々なものが情報化されているため、いったんその情報が盗まれた場合、それは様々なものに悪用されてしまうのである。今回でいうと氏名や住所などの個人を特定できる情報が漏洩、盗まれているのでそれをもとに個人に対して金銭を要求したり、本人が知らないうちに金銭を盗んだり、別の場所でその情報を使用したりする犯罪が小規模から大規模な範囲で行われる可能性もあるのでサイバー犯罪において国は大きく動きうるのである。

4. 企業のサイバーセキュリティ対策

この章では今までの企業が今まで取っていたサイバーセキュリティ対策を紹介すると共に日本の最新セキュリティ対策システムを紹介していくのである。4.1 では従来のセキュリティ対策ではいくつかの企業が実際に使用していたサイバーセキュリティ技法を紹介し、4.2 では最新のセキュリティ対策 FFRI「yarai」について紹介していくのである。この FERI「yarai」は今までの日本のセキュリティ対策にはない機能が備わっており、これは世界のセキュリティ対策と比べてみても遜色ないものである。これは現在の日本のサイバーセキュリティ分野においては途轍もない商品である。このことを理解してもらうために従来のセキュリティ対策の機能を紹介し、「yarai」の機能についても詳しく紹介していくのでその機能の凄さを理解してもらいたいのである。

4.1 従来のサイバーセキュリティ対策

日本を含め、世界のサイバーセキュリティ市場で従来使われていた技法が「パターンマッチング」であり、従来のセキュリティ対策のすべてがこの技法を備えたセキュリティソフトであったのである。これにより多くの企業、個人情報などが悪意のあるサイバーウイルス、マルウェアから保護されたのである。

では、このマルウェアから情報を守っていたパターンマッチングとは何なのかを次で説明

していくので、どのように我々の大切な情報が守られてきたのかを理解してもらいたいのである。

4.1.1 パターンマッチング

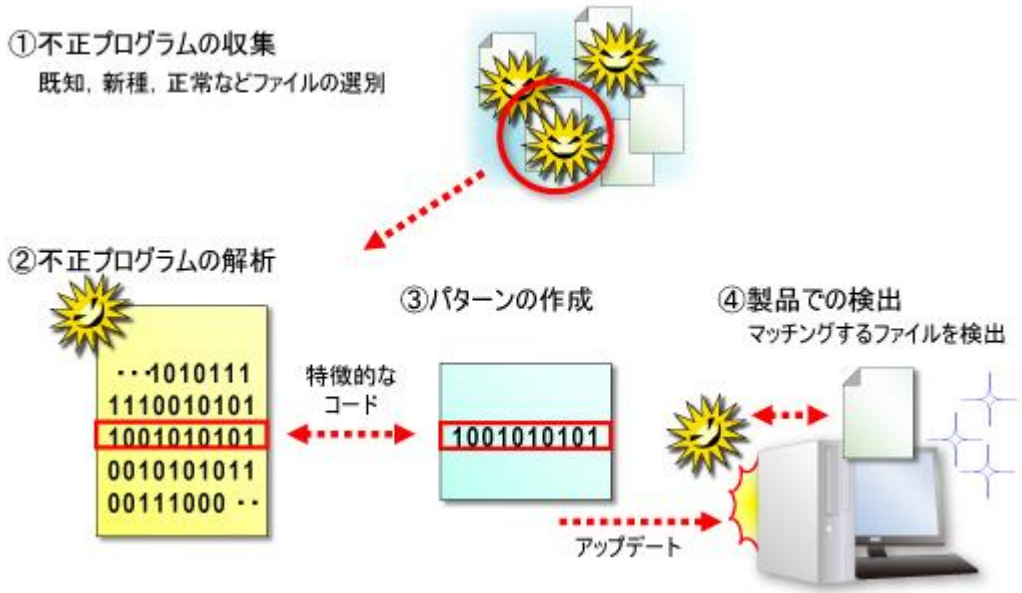
パターンマッチングとはサイバーウイルス対策ソフトが悪意のあるウイルス、マルウェアなどを発見するために使用されていた従来では最も基本的なものであったのである。

このウイルス対策ソフトはパターンファイルと呼ばれるウイルス一つ一つが持つ特徴（パターン）を記録したリストを持っており、そして、そのリストに載っているウイルスのパターンとパソコン内のファイルのパターンを比較して、そのファイルがリストと一致した場合、そのファイルにウイルスが存在していると判定し、ファイル内のウイルスを削除するのである。これが、パターンマッチングと呼ばれるサイバーセキュリティの技法である。

このパターンマッチングは、すでに存在が知られている既知のウイルスはほぼ100%検出できることが分かっており、当時のセキュリティ対策ソフトには必ず組み込まれていたものである。

つまり、パターンマッチングとは、所謂犯罪者リストを使って一般の人の中に悪人が混ざっていないか探すような機能のである。

しかし、このパターンマッチングには欠点が存在していたのである。それを次で説明していくので、なぜパターンマッチングが通用しなくなったのかを知ってほしいのである。



図表 3パターンマッチング（引用元日経 XTECH（2007）「第 5 回 パターン照合だけではダメ，力を合わせてディフェンスを固める」）

4.1.2 なぜパターンマッチングは通用しなくなったのか

パターンマッチングはその性質上、新しいウイルスが登場した際、そのウイルスの存在が世間に知られて、セキュリティ対策のパターンファイルに新しいサイバーウイルスとして情報が登録されるまではそのサイバーウイルスに対してパターンマッチングを採用しているサイバーセキュリティ対策ソフトはどれだけ優れていたとしても何の効果も示さないのでそのウイ

ルスは削除される事無く、他社の電子機器、パソコンなどを汚染し、情報を盗んだり、改ざんしたりするのである。このようなウイルスのことを亜種といって、既知のウイルスを少し改変しただけでこの技法は亜種のウイルスに対応できなくなってしまうのである。その結果、サイバーウイルスによる被害は年々増え続けているのである。何故ならば、現在でもこの技法、パターンマッチングが使われているからである。その例として、前述で述べた銀行への標的型攻撃や国へのサイバー攻撃などが挙げられるのである。さらには、日々サイバー攻撃に使われるウイルス、マルウェアなどは改良、新開発されているのである。このような状況下ではパターンマッチングは限りなく不利であることが今までの説明から理解できると思われるのである。

では、我々は第三者からのサイバー攻撃から自分たちの情報を守れないのかというと、そうではないのである。何故ならば、世界のセキュリティ市場ではこの問題を解決するべく様々なセキュリティプログラムを開発してきているのである。この活動は今もなお続いており、日々サイバーテロとの攻防が行われているのである。近年では日本にサイバー攻撃が集中するようになっているがその理由は後の章で述べるとして、ここでは世界のセキュリティプログラムにも負けていないセキュリティプログラム、「yarai」について説明していくのである。

4.2 最新のセキュリティ対策

先ほど述べたように従来の技法、パターンマッチングでは現在のサイバー攻撃、つまり、日々進化するサイバーウイルスを使った攻撃から重要な情報を保護することはほぼウ可能になってしまっていることは理解できたと考えているので、今回はその問題を解決するために作られた技法を紹介するのである。その際に、現在日本で作成されているサイバーセキュリティ対策ソフトでこの技法が使われているものを例として使って説明していくので、従来の技法、パターンマッチングとの違いを考えながら読み進めてほしいのである。なぜならば、そうすることでサイバーセキュリティプログラムがどのような進化を遂げているのか理解しやすいからである。

4.2.1 FFRI「yarai」

FFRI は先ほど述べた最先端の技法を使ったセキュリティプログラムソフトを作成しているのである。それはパターンマッチングの欠点を補ったものである。ここではその技法を説明していくのであるが、その際に FFRI についても少しばかり説明していくのである。何故ならば、日本の企業もまだまだ世界のサイバーセキュリティプログラム技術に引けを取っていないことを理解してもらいたいからである。

4.2.1.1 株式会社 FFRI

株式会社 FFRI は日本においてトップレベルのセキュリティリサーチチームを企業内部に作り、IT 社会の情報保護に貢献すべく 2007 年に設立されたのである。前述で説明した日々進化しているサイバー攻撃技術を FFRI 企業独自の視点で分析、解析し、日本国内で対策技術の研究開発に取り組んでいる会社である。

また、彼らが行う研究内容は国際的なセキュリティカンファレンス（サイバーセキュリティに関する研究結果の発表の場あるいは企業のセキュリティプログラムお披露目の場）で継

続的に発表し、海外からも高い評価を受けており、これらの研究の過程から得た知見やノウハウなどの様々なサイバーセキュリティに必要不可欠な情報をもとに作り上げた製品やサービスなどといったものを外部へ提供しているのである。その優れたサイバーセキュリティプログラム作成会社が作り上げた最新鋭のプログラムが「yarai」である。

4.2.1.2「yarai」とは

「yarai」とは FFRI によって作成された標的型攻撃に特化した「プログレッシブ・ヒューリスティック技術」による次世代セキュリティソフトであり、この『FFRI yarai』の製品コンセプトは、従来の技法であるパターンファイルを全く必要とせず、マルウェアや脆弱性攻撃を防御し、既知や未知の脅威から個人、企業などの大切な情報資産を守るというものと定義されており、また、『FFRI yarai』はプログレッシブ・ヒューリスティック技術を構成する次の 5 つの振る舞い検知エンジンを実装しており、これらのエンジンによって今まで対応できなった未知のサイバーウイルスから様々なデータを保護することができるのである。

4.3 プログレッシブ・ヒューリスティック

プログレッシブ・ヒューリスティック技術とは、従来のセキュリティプログラムで使われていたパターンマッチングに一切依存しない、サイバー攻撃の進化を先読みし、さらにセキュリティ対策ソフト自体が進化し続けることを促す先読み技術のことである。これは革新的技術であることは今までの文章を読んできたならば理解することができると思っているのである。なぜならば、従来の技法の欠点、未知のウイルスから情報を守ることを可能にしているからである。この技術は世界でも注目を集めており、世界と比べると遅れていた日本のサイバーセキュリティ市場に追い風をもたらす存在であることは言うまでもないのである。

この技術を支えている 5 つのエンジンとは「ZDP エンジン」、「Static 分析エンジン」、「Sandbox エンジン」、「HIPS エンジン」、「機械学習エンジン」である。これらそれぞれにプログレッシブ・ヒューリスティックを支える技術が備わっているので、それを一つ一つ詳しく説明していくのでパターンマッチングとの違いを考慮しながら読んでもらいたいのである。

4.3.1「ZDP エンジン」

「ZDP エンジン」では、既知、未知のマルウェアで行われる「任意コード実行型の脆弱性」を狙ったサイバー攻撃、つまり、セキュリティ上の欠陥を悪意のある第三者が利用して攻撃、侵入し、サイバー攻撃側が任意のプログラムを実行し他人のコンピュータなどを操るといったウイルス攻撃の 99%以上を検知して防御できるのである。

また、このエンジンで使われている任意コード実行型脆弱性の攻撃から情報を守る FFRI 独自の技術が備わっており、その技術とは「API-NX」(特許第 4572259 号)と呼ばれるものである。

4.3.2「Static 分析エンジン」

「Static 分析エンジン」ではファイルなどに埋め込まれているプログラムを実行させずに、静的にプログラムの構造を分析、数値化し、その数値が一定の閾値を超えた場合において、そのプログラムをマルウェアが存在するものと判定するというロジックになっているのである。また、「Static 分析エンジン」でマルウェアであるかの白黒の判別がつかなかったグレーなものについては 3 つ目の「Sandbox エンジン」に引き渡されるのである。

このエンジンに組み込まれている分析手法は「N-Static 分析」というもので、その中には「PE 構造分析」「リンカー分析」「パッカー分析」「想定オペレーション分析」など多数の分析手段が存在しているのである。

4.3.3「Sandbox エンジン」

「Sandbox エンジン」では、仮想的な CPU やメモリ、Windows サブシステムなどで構成される仮想環境の空間で検査対象となったファイルなどのプログラムなどを実行し、独自の検知ロジックで実行される命令の組み合わせを分析し、それがマルウェアなどのウイルスであれば検知するのである。また、ここで利用される仮想環境は VMware のような大きな仮想環境ではなく、端末のパフォーマンスを考慮した小さな仮想環境である。近年のマルウェアにおいて、Anti-VM や Anti-Sandbox の機能を実装したものもあり、仮想環境の存在を検知すると悪意のある挙動を行わなかったり、無駄な動作を大量に行うことで Sandbox での検知を諦めさせるよう行動したりするようなものもあるのである。しかし、FFRI の「Sandbox エンジン」はそれらのプログラムの挙動を逆手にとって、Anti-VM や Anti-Sandbox の技術を検知し、対象となったものを悪意のあるものとして判断します。

4.3.4「HIPS エンジン」

これらの 3 つのエンジンを使用して検索してもマルウェアとして扱われなかったものに対しては、「HIPS エンジン」で実際に動かしている際のそのプログラムが行う動作を監視するのである。仮にブラウザのような他のプロセスに何かしらの悪意のあるプログラム、キーロギングなどのような不正な振る舞いをした場合、それをすぐさま検知し、実害が出る前に防御することで所有者のコンピュータなどに被害がないようにするのである。

4.3.5「機械学習エンジン」

機械学習エンジンも「HIPS エンジン」と同様に実行中のプログラムを監視しするのである。

また、機械学習エンジンは、FFRI が独自に収集している膨大なマルウェアや正常系ソフトウェアをビッグデータとしてまとめ、それを機械学習によって分析、解析し、それによって導き出した検出ロジックを搭載しているので、既知のウイルスはもちろん、未知のウイルスも検出できるようになっているのである。

一般的に、マルウェアの分析には時間がかかるので、今までは質的にも量的にも限界があると考えられていたのですが、その問題を解決するために機械学習を利用した結果、従来よ

りも分析スピード劇的に向上し、網羅的な分析が可能となり、今まで人間が見い出すことができなかったマルウェアなどのサイバーウイルスの検出ロジックを発見できるようになったのである。

このように５つのエンジンが持つ様々な機能により既知、未知のサイバーウイルスが検出され削除されるのである。以下はその構成図とこの製品の実績である。

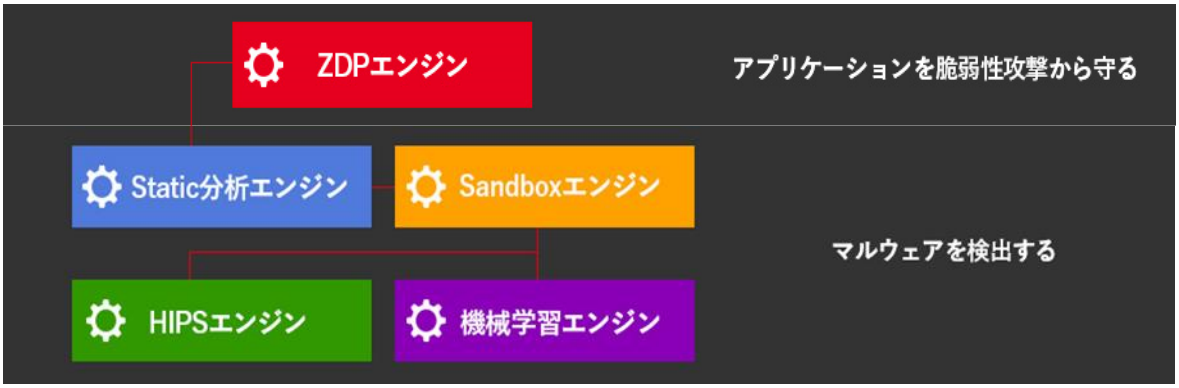


図 4　yarai 構成図　引用元（FFRI　(2018). 「[CODE:F]未知の脅威の"先読み防御"技術」）


FFRI yaraiの主な防御実績(未知マルウェア)

発生・報道時期	防御エンジンリリース時期	当時の未知脅威及び標的型攻撃	FFRI yarai 検知&防御エンジン
2016年5月	2015年7月	不正送金マルウェア「Gozi」	HIPSエンジン
2016年3月	2015年7月	ランサムウェア「PETYA」	Static分析エンジン
2016年2月	2015年7月	ランサムウェア「Locky」	HIPSエンジン
2015年12月	2015年7月	不正送金マルウェア「URLZone」	Sandboxエンジン
2015年12月	2015年6月	ランサムウェア「TeslaCrypt（vvvウイルス）」	Static分析エンジン
2015年10月	2015年6月	バンキングマルウェア「SHIFU」	HIPSエンジン
2015年6月	2014年8月	日本年金機構を狙うマルウェア「Emdivi」	（非公開）
2014年12月	2014年8月	FBIが警告「システム破壊型マルウェア」	Static分析エンジン
2014年11月	2014年8月	医療費通知偽装 マルウェア「Emdivi」	Static分析エンジン
2013年3月	2013年1月	韓国へのサイバー攻撃マルウェア	Sandboxエンジン

※FFRI yaraiの防御エンジンリリース時期は、当時の未知脅威及び標的型攻撃の発生時期より、およそ1ヶ月から1年程前のものであり、脅威が発生する以前の防御エンジンにより防御が可能であったことを示しています。
※防御実績は社内で入手、検証を行った検体に関する結果であり、全ての亜種の検知を保証するものではございません。

図 5　yarai の実績　引用元（FFRI　(2018). 「[CODE:F]未知の脅威の"先読み防御"技術」）

4 .4 サイバー保険

サイバー保険（情報セキュリティ保険）とは企業のサイバーセキュリティ被害を総合的に補償する損害保険である。もし企業がサイバー攻撃を受けてしまい、情報流出したときの備えとして役立ってくれるものである。このサイバー保険のメリットととしては以下のものが挙げられます。

1. 事故が起きたとき、保険金が支払われる

- ただし、受け取れる補償金は保険会社によって違ってくるのですが、一般的に次のような種類のお金が支払われるのである。
- 損害賠償金

- 争訴・訴訟費用
- 原因調査費用
- 見舞金（金券）購入費用
- お詫び状作成・郵送費用
- 謝罪広告費用
- コールセンター費用
- データ復元費用
- コンサルティング費用
- フォレンジック費用
- 喪失利益
- 営業継続費用
- サイバーセキュリティ被害以外によって起きたネットワークの停止や、第三者に提供するソフトウェアなどの欠陥による損害

2. 被害を最小限に食いとめるための効果的な初期対応コンサルティングサービスを受けられる

3. 付帯サービスによるサポート機能

お金の補償以外にも、対応のサポートをしてもらえるメリットがあるのである。もし、サイバー事故が起きたとき、企業は混乱してしまい、いったいどこへ対策や調査をお願いするかといったサポートセンターなどといったものを探す必要もある中、企業は一刻も早く原因究明をして情報流出を止めなければならないのである。そこで、保険会社が迅速な対応の手助けをしてくれるのである。空らには過去のケースから得たスキルが多く存在しているので、それらを活用し、適切なアドバイスなどをしてくれるのである。それらは主に原因究明、被害拡大防止措置、緊急時の広報対応、コールセンターの設置や運営などといった事故対応に関するサポートである。ただし、注意としては保険料や細かいサービス内容が保険会社によって異なるので、ウェブサイトや資料取り寄せるなどして自社や自分に合ったものを見つけなければなりません。また、この保険では補償されないものもあるのである。それは、天災や労働争議が原因で個人情報が流出した場合、海外サーバーに保存されている個人情報が漏えいした場合などといったものである。これらの場合は、補償の対象外であることがあるのである。これらのような補償対象外の案件の種類は保険会社により異なるので、これも事前にチェックしてから検討しなければならないのである。また、保険会社には絶対に保証できないものも存在するのである。それがブランドである。どれだけその保険会社が優秀であろうとブランドイメージは守れないのである。なぜならば、これは金銭的理由などといったものではなく顧客の心理的問題だからである。さらには、サイバー攻撃による損失は、範囲や種類が通常のサイバー犯罪などといったものよりも広いため、お金では補償しきれない部分もあるのである。以下に過去に起きた事件を挙げるので参考にしてほしいのである。

アメリカの小売店「Target」で 2013 年に 7000 万件の顧客情報が流出したが、複数のサイバー保険に入っていたため約 1 億ドルもの補償金をもらったとされていたのである。
しかし、事件後に利益が 46%下がり、その損失は約 4 億ドルにもなってしまったのである。

このように、「企業のイメージ低下による顧客離れ」までは、保険で補償することはできないので注意が必要である。

5．情報セキュリティ市場の変化

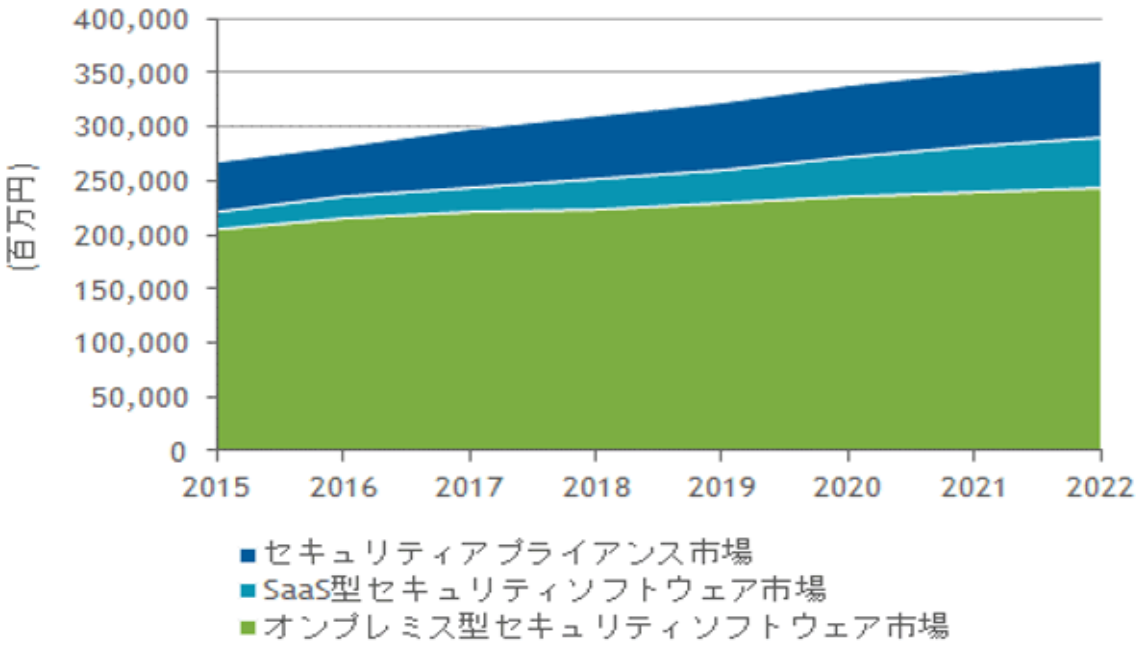
この章では題名の通り情報セキュリティ市場の変化について掲載していくのである。セキュリティ市場に対して現在どれほどの期待が抱かれているのか、将来的にどれほどの向上、あるいは降下するのかを研究し、この市場に対しての期待度などを述べていくのである。

市場の変化に伴ってどのようなサイバーセキュリティ対策関係の新商品が発売されているのかをここでは述べていくのである。何故ならば、新商品の開発はその市場の変化に合わせて作成されると私は考えているので、それらを調べればこの市場に対して顧客がどのようなものを欲しているのかといった顧客側からの要求などを把握出来、また、これからの市場には何が求められるようになるのかっといった推測も可能になってくるのである。

つまり、この章では市場の変化を資料と共に示すと共に、変化によって生まれたものなどを紹介していくのである。

5.1 市場の現状

まずは市場の変化である。前述で述べたように近年様々な種類のサイバー犯罪が増加しているのである。それに伴ってサイバーセキュリティ市場の需要、期待などはますます増加しているのである。そのいい例として前章の新技術、プログレッシブ・ヒューリスティックが挙げられる。これは従来のサイバーセキュリティ対策で使われていたパターンマッチングでは最新のサイバーウイルスを防ぎきることはほぼ不可能になってしまったのでこの市場に対して更なる技術が求められるようになったのである。そこで登場したのが前述で述べた先読み技術であったのである。このように日々新たなサイバーウイルスが作成されている状況下においてこの市場への需要はますますの増加が見込まれているのである。それは以下の図表から考えられるのである。



図表 6 サイバーセキュリティ市場の推移（引用元 IDC Japan 株式会社（2018).「国内情報セキ

ュリティ市場規模予測を発表」）

ここではサイバーセキュリティ市場を 3 つに分けて考えていくのである。それがセキュリティアプライアンス市場、SaaS 型セキュリティソフトウェア市場、オンプレミス型セキュリティソフトウェア市場である。

5.1.1 セキュリティアプライアンス

セキュリティアプライアンスとはセキュリティ機能に特化したコンピュータであり、導入や管理などの簡便性、コスト面、信頼性が優位というアプライアンス（ある特定の機能に特化したコンピュータ）の特徴をそのまま備えているのである。このセキュリティアプライアンス製品の代表的な機能にはファイアウォール、VPN ゲートウェイ、IDS/IPS 、アンチウイルスなどが挙げられるのである。また、このような様々なセキュリティアプライアンス機能を集結させたものが統合型セキュリティアプライアンスである。近年、この統合型セキュリティアプライアンスが急速に普及しているのである。その理由としては、サイバーウイルスや不正アクセスなどによるサイバー攻撃の脅威が高度化、多様化しながら増加する様子が見られるため、これまでは個別に導入してきた各種セキュリティ対策機能を止め、それらの機能を一度に導入、設置できるようにし、それらの運用管理が一元的に行えるようにしたことが大きいが、その他にも初期にかかる費用やランニングコストなどが低価格だという特徴をこの総合型は持っており、その特徴を多くの企業が気に入って購入し、また、その評価が技行間などで広まり多くの顧客を生んだこともこの製品が売れた要因である。先ほども述べたようにこの商品は急速に発展しているのである。それは図表 6 からも読み取れることである。

5.1.2 SaaS 型セキュリティソフトウェア

SaaS とは Software as a Service の略であり、日本語に訳すと「サービスとしてのソフトウェア」という意味である。これはユーザーが必要な機能を、必要なときに、必要な分だけサービスとして利用できるようにしたソフトウェア、もしくはその提供形態の略である。つまり今回の SaaS 型セキュリティソフトウェアとは顧客側がソフトウェア作成会社のサービスを必要だと思ったときに、必要な期間利用できるサービスである。

5.1.3 オンプレミス型セキュリティソフトウェア

このオンプレミス型セキュリティソフトウェアにはいくつかの特徴があるのである。それがセキュリティの強固さ、カスタマイズ性の高さ、他ソフトウェアとの統合性の高さ、オフライン環境での利用可能が挙げられるのである。

このオンプレミス型では社内ネットワークを利用するため、外部への情報漏洩やインターネットを介して侵入する脅威へのリスクが軽減し、また、自社のセキュリティポリシーに合わせて環境を構築できるので強固なセキュリティプログラムになるのである。

また、システム環境は全て自社で構築するので、このシステムを顧客側は自由にカスタマイズできるのである。そんため、顧客が実際に使用する場の声をすぐにこのシステムへと反映させることが出来るため顧客側にとってより最適な環境を構築できるのである。

既存のシステムが顧客の仕事場などにあるならば、自分たちで独自にこのソフトウェアの

構造を改良してドックすることが可能である。そうすることでその企業のオリジナルの統合システムを構築ことが可能になるのである。

万が一インターネットに何らかの障害が発生した場合であっても、このソフトウェアは社内ネットワークを利用しているのでシステム自体が止まることはないのである。

このようにこのソフトウェアには顧客側にとって有益となる機能が数多く存在しているため当初から現在に至るまで様々な企業から関心を得ているのである。

このほかにもセキュリティ市場は様々な分野に分けることができるのであるが、今回はこの３つの分野をだけを紹介したいのである。なぜならば、これらは我々の生活の中で最も身近なものであると考えているからである。これらはサイバー犯罪が変化するに伴って、その犯罪に適したものを作成してほしいという需要から生まれたものであることは明白である。つまり、セキュリティ市場は今もなお変化し続けていることが予想されるのである。それを裏付けるように、図から読み取れるようにサイバーセキュリティ市場は年々増加傾向にあることが分かるのである。その理由は今まで述べてきたようにサイバー犯罪の進化からきていることは周知の事実であるが、その他にも人々のサイバー犯罪への意識の改善も含まれているように思われるのである。なぜならば、前述で述べたように日本は世界と比べるとまだまだこの分野に関しては低いレベルであるが、周囲にサイバー犯罪がどれほど危険であるかといった注意勧告などの行動が近年ようやく行われるようになってきたのである。これは世間がサイバー犯罪を脅威になる存在であると認めたに他ならないのである。その結果、さらにサイバーセキュリティ市場により注目が言ったと考えられるのである。これらを踏まえてこの市場の将来の推移を予測すると次のように考えられるのである。

5.2 これからの市場

IT 専門調査会社 IDC Japan の調査によるとソフトウェア製品とアプライアンス製品を合わせたセキュリティ製品の市場では 2017 年～2022 年の年間平均成長率が 3.9%まで上がり、市場規模において、2017 年は 2,973 億円で 2022 年には 3,602 億円にまで拡大すると予測されているのである。また、コンサルティングやシステム構築、運用管理、教育、トレーニングなどのサービスを含むセキュリティサービスの市場は、2017 年～2022 年の年間平均成長率が 5.4%で、市場規模においては、2017 年の 7,581 億円から 2022 年には 9,870 億円に拡大すると考えられているのである。今回の提示している調査資料は少数であるが、多くの調査会社などでのサイバーセキュリティ市場への研究結果において、多くが長期間の市場の拡大という答えを出していたのである。また、その市場の分類も様々であるので今回示した資料が絶対ではないことに注意してもらいたいのである。何故ならば、答えは最終的に同じであったのだが、その研究から導き出されたであろう数値や市場の変化などにはばらつきがあったのである。これを言い換えると、サイバーセキュリティ市場はこれからも成長していく市場であるが、その成長度合いが未知数であるという証明に他ならないと考えているのである。何故ならば、サイバーテロなどの脅威は日々増しており、それが将来どこまで進化するかは誰にもわからないため人々の不安は少なからず存在し、その不安からセキュリティ市場への需要が高まっていき、将来的には新たなセキュリティ分野が作られるのではないかと考えて

いるので、サイバーテロが無くならない限り、このセキュリティ市場は永遠と成長していく思われるのである。

つまり、この市場は他の市場と比べいまだ停滞する傾向が見られない成長性豊かな市場であることが分かるのである。

6．日本に求められるもの

ここでは従来の日本とこれからの日本を比較し、意識的面などといった側面からどのような変化が起きたのかを資料等を使って解説していくと共に、オリンピックとのつながりも紹介していくのである。また、人材面の方でも解決策を練っていく。

7．おわりに

ここでは今までの記述を踏まえて自分がどのように感じたかを記載するのである。

参考文献

Wikipedia (2005). 「アノニマス（集団)」
https://ja.wikipedia.org/wiki/アノニマス_(集団)
(2018-7-8 参照)
栢木 厚（2017).『平成 30 年度 イメージ&クレバー方式でよくわかる 栢木先生の IT パスポート教室（情報処理技術者試験)』技術評論社
警察庁（2018）.「統計｜警察庁 Web サイト」
https://www.npa.go.jp/publications/statistics/index.html
（2018-6-24 参照）
警察庁（2011）.「第 1 節 サイバー犯罪の現状 - 警察庁 Web サイト」
www.npa.go.jp/hakusyo/h23/honbun/html/1-toku2_1_1.html
（2018-6-24 参照）
株式会社シーズ・クリエイト(2018).「サイバー攻撃とは？その種類・事例・対策を把握しよう」
https://cybersecurity-jp.com/cybersecurity-guide/14651
(2018-7-4)
ライフハッカー［日本版］(2015). 世界的に有名なハッカー集団 4 組を徹底解説：それぞれの成立経緯と活動目標
https://www.lifehacker.jp/2015/04/150405hacker_motivation.html
(2018-7-4)
日本経済新聞(2018 年).「大規模サイバー攻撃、チェルノブイリ原発も被害」
https://www.nikkei.com/article/DGXLASGM28H2W_Y7A620C1MM0000/

(2108- 7 - 4 参照)
マルウェア情報局(2017).「「ワナクライ」に似た身代金要求マルウェア「ペトヤ」(PETYA)が世界中で大量拡散 」
https://eset-info.canon-its.jp/malware_info/special/detail/170706.html
(2108- 7 - 4 参照)
東北起業・イノベーション塾(2017).「身近に迫る危機！世界を揺るがすサイバー攻撃 3 選まとめ」
http://3media.biz/wadai/cyberterrorism.html
(2108- 7 - 4 参照)
TECH::NOTE(2018).「ホワイトハッカーとは？ブラックハッカーとの違いを解説」
https://tech-camp.in/note/technology/42671/
(2018-7-8 参照)
カラパイア(2015).「ハッカー集団「アノニマス」が暴いた最も衝撃的な 10 の秘密」
http://karapaia.com/archives/52205379.html
(2018-7-8 参照)
産経新聞(2016.2.17).「アノニマス」
https://www.sankei.com/west/news/160217/wst1602170006-n1.html
(2018-7-8 参照)
総務省(2003).「組織幹部のための情報セキュリティ対策」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security_previous/download/taisaku_kanbu.pdf#search=%27http%3A%2F%2Fwww.soumu.go.jp%2Fmain_sosiki%2Fjoho_tsusin%2Fsecurity_previous%2Fdownload%2Ftaisaku_kanbu.pdfsearch%3D%2527%25E3%2581%2593%25E3%2581%25AE%25E6%2583%2585%25E5%25A0%25B1%25E7%25A4%25BE%25E4%25BC%259A%25E3%2581%25AB%25E5%25BF%2585%25E8%25A6%2581%25E3%2581%25AA%25E3%2582%25BB%25E3%2582%25AD%25E3%2583%25A5%25E3%2583%25AA%25E3%2583%2586%25E3%2582%25A3%25E3%2583%25BC%2527%27
(2018-6-25 参照)
マルウェア情報局 – Eset(2017).「セキュリティ教育と社会的責任」
https://eset-info.canon-its.jp/malware_info/special/detail/170721.html
(2018-6-24 参照)
日経ビジネス（2018-7-2）『2025 年稼げる新職業親子で考える仕事選び』No.1948.22-39
FFRI （2018).「[CODE:F]未知の脅威の"先読み防御"技術」
https://www.ffri.jp/special/code_f.htm
（2018-7-13 参照）
IDC Japan 株式会社（2018).「国内情報セキュリティ市場規模予測を発表」
https://www.idcjapan.co.jp/Press/Current/20180528Apr.html
（2018-7-15 参照）

文末脚注

（1）Canon System & Support Inc. 「サイバー犯罪の現状と対策｜知っておきたいセキュリティの基本｜」
https://www.canon-sas.co.jp/portal/security/securityinformation/actualstatus.html
（2018-7- 6 参照）
（2） BUSINESS LAWYERS. 「リーガル・サイバーセキュリティの最新事情」
https://business.bengo4.com/category3/article298
（2018-7- 7 参照）
（3）株式会社 FFRI. 「［CODE:F]未知の脅威の"先読み防御"技術｜セキュリティ・リサーチの FFRI（エフエフアールアイ）」
https://www.ffri.jp/special/code_f.htm
（2018-7- 7 参照）
（4）富士通マーケティング. 「近年求められるサイバーセキュリティとサイバー攻撃の脅威～日本年金機構や JTB が被害を受けたサイバー攻撃とは～」
http://www.fujitsu.com/jp/group/fjm/mikata/special/forum2017/ffri/001.html
（2018-7- 9 参照）
（5）JNSA.「日本国内最大のセキュリティコンテスト」
http://www.jnsa.org/seccon/
（2018-7-11 参照）
（6）総務省.「総務省におけるサイバーセキュリティ政策の 最新動向」
http://www.soumu.go.jp/main_content/000469744.pdf#search=%27%E6%83%85%E5%A0%B1%E7%A4%BE%E4%BC%9A%E3%81%AB%E3%81%8A%E3%81%91%E3%82%8B%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E3%83%86%E3%83%AD%E5%A4%A7%E4%BC%9A%27
（2018-7-2 参照）
（7）サイバーセキュリティ.com. 「サイバー攻撃が増え続ける 5 つの原因」
https://cybersecurity-jp.com/cybersecurity-guide/14643
（2018-7-10 参照）
（8）【公式】NTTPC.「パターンマッチング - 用語解説辞典」
https://www.nttpc.co.jp/yougo/パターンマッチング.html
（2018-7-13 参照）
（9）日経 XTECH（2007）.「第 5 回 パターン照合だけではダメ，力を合わせてディフェンスを固める」
https://tech.nikkeibp.co.jp/it/article/COLUMN/20071005/283934/
（2018-7-13 参照）
（10）「アノニマスの仮面がドンキで買える！仮面の意味や由来はあの映画？ ｜ponta の一期

一会」
http://ponta23.com/1293.html
（2018-7-13 参照）
（11）サイバーセキュリティガイド（2016）.「サイバー攻撃の件数など統計情報」
https://cybersecurity-jp.com/cybersecurity-guide/14641
（2018-7-13 参照）
（12）ログミー.「FFRI 代表が最新のセキュリティ対策技術を解説」
https://logmi.jp/101347
（2018-7-13 参照）
（13）ITmedia エンタープライズ（2010）.「セキュリティはこれ 1 台で OK――統合セキュリティアプライアンスとは？ 」
http://www.itmedia.co.jp/enterprise/articles/0608/01/news030.html
（2018-8-16 参照）
（14）無料クラウド型グループウェア iQube（2010）.「サーバ不要のクラウド型とオンプレミス型を徹底比較」
http://www.iqube.net/cloud_on-premises-_groupware.html
（2018-7-16）
（15）セキュリティ対策のラック（2018）.「サイバー保険」
https://www.lac.co.jp/service/product/insurance.html
（2018-7-16）