サイバーセキュリティ読本【完全版】

ネットで破滅しないためのサバイバルガイド

一田和樹

サイバーセキュリティ読本【完全版】

ネットで破滅しないためのサバイバルガイド

一田和樹

星海社

111

SEIKAISHA SHINSHO

次のうち、現実に起きたと思うものにマルをつけてください。

□ 海外からの攻撃で国中のネットワークが機能しなくなり、銀行も操業できなくなる事態が起きた。

□ ネットに接続できる家電機器（テレビ、掃除機、防犯カメラなど）の中にはセキュリティ対策が充分ではなく、簡単に乗っ取られて悪用されるものが少なくない。

□ インターネットに接続されている機器２００万台がroot、adminあるいはパスワードなしでアクセス可能だった。それらの中には設備制御に利用しているものも

あった。

□ 自動車の制御装置は無線で結ばれているので、外部からハッキングできる。

□ ツイッター、フェイスブックなどソーシャルネットワークを監視し、個人情報や位置情報を特定・収集するソフトを販売する会社が複数存在し、アメリカの警察や政府機関が購入している。

□ インターネット広告でマルウエア（ウイルスなど）が配信された。

□ グーグル、ヤフー、ツイッター、フェイスブックは、保有する個人のデータ（個人情報、メールの内容など）をアメリカの政府関係機関は盗聴していた。

□ 世界のどこからでもネットを介して匿名で送金できる仕組みが存在し、犯罪者が利用している。

□ ツイッターのパスワードを変えても、前のパスワードのままで利用できる。

□ 無償で配布されている攻撃ツールがあり、これを利用した犯罪も行われている。

□ アンドロイドをターゲットにした、見ただけで感染するマルウェアが登場した。

□ スマホやパソコンをマルウェアから完全に守る方法はない。感染する前提で対策を考える必要がある。

□ 多くのアンドロイドスマホではＯＳのセキュリティアップデートできる期間は明示されておらず、自己責任で守るしかない。

□ 位置情報（ＧＰＳ）は妨害や偽装できる。

□ 軍や警察といった政府機関のみに、専用のマルウェアなどを販売するサイバー軍

需企業が存在し、堂々とＷＥＢサイトでそのことを告知している。

□ 感染すると自分のパソコンのデータを暗号化し、さらにクラウドやネットワークで接続されたマシンのデータまで暗号化するマルウェアがある。

□ 海外のサイバー軍需企業の社内資料が盗まれ、ネット上にさらされる事件が起き、日本の政府機関と思われる組織との電子メールのやりとりも含まれていた。

□ アメリカはサイバー戦では遅れをとっており、日本はさらに遅れている。

□ 日本を狙ったサイバー攻撃作戦が行われた。

回答

全て本当のことです。

多くの方は知らないか、自分の身近なことと結びつけて考えていないと思います。

本書では私たちの日常生活をとりまくサイバーセキュリティの現在を、物語風にご紹介します。

舞台となるのは、篠山兄弟社（しのやまきょうだいしゃ）という架空の中堅書店です。東京郊外のN市に5店舗を持っています。5年前からネット書店も開いていますが、こちらは一般の本ではなく篠山兄弟社で発行した自費出版物のみを扱っています。一般書籍のネット通販ではアマゾンをはじめとする大手に敵（かな）わないと判断したためです。地元の名士やお年寄りの本を自費出版するサービスは、売上げこそ大きくないものの利益では篠山兄弟社を支える柱となっていました。

ある日、社長の篠山泰治（たいじ）はニュースを見ていて危機感を覚えました。なにかをしなけれ

ばならない！　そう感じた泰治は翌日出社すると、弟の泰山（たいざん）と相談して数名の社員に特命を与えました。彼らにサイバーセキュリティ対策マニュアルを作らせるのです。

特命社員たちがマニュアルを作っていく過程を通して、読者のみなさんにもサイバーセキュリティについて学んでいただければ幸いです。

プロローグ

篠山兄弟社の社内で秘密の会議が開かれようとしていた。

議長である河合牡蠣は、社長が行きつけの中華料理屋からもらった丸いテーブルに集まったメンバーふたり（男ひとり、女ひとり）の顔をぼんやりとながめていた。自分を含めて3人だ。

ぽっちゃりした顔に、セルフレームの眼鏡、おかっぱの黒髪。白いシャツに赤いベストとジーンズ。どうということのない服装だが、ぴったりと太腿に張り付いたジーンズの曲線がかわいらしさと、色気をかもしだしていると河合は自賛している。

「オレ、いつも会議室に来るとチャーハンを食べたくなるんだよな」

片山はそう言いながら、テーブルの上の回転する円板を軽く手で押した。円板はゆっくりと回り始める。太った身体にスキンヘッド。だが、どことなく愛らしい目つきが彼を好人物に見せている。以前は本店の文芸フロアを担当していたが、今は自費出版サービスの

営業だ。
「いたずらしないでください。会議を始めますよ」
河合は円板を片手で押さえて止めると立ち上がった。それからおもむろに紙を配布する。
「出欠を取ります。呼ばれたら、はいと返事してください」
河合が言うと、
「見りゃわかるじゃん」
片山が苦笑した。
「気は心です。こういうのは形が大事なんです。片山くん」
「くん？　くんづけなの？　河合ちゃん、本気？」
ひと回り以上年下の女性に〝くん〟づけされた片山は、よほど驚いたらしく目を丸くしている。
「ここではあたしが議長です。あたしの決めたルールに従ってもらいます」
河合は、胸を張った。豊かな胸に片山の視線が注がれるのがわかる。
「卯城（うしろ）くん」
河合がそう言うと、もうひとりの女性は無言で手を上げた。河合がぽっちゃりしている

のに対して、卯城はやせている。転んだだけで折れそうな細い身体。黒いセーターに黒いスカートという組み合わせが余計にそう見せる。河合は、シャープペンの芯みたいだなと見るたびに思う。

「はい、と言ってください」

「……はい」

卯城は、ぼんやりした表情でそう言うと、すぐに手を下ろした。慢性貧血のような真っ白な顔。いつも無表情。この子はきっと身体か心の病気なのだ、と河合は思った。だが、偏った本の知識は社内随一で「困った時の卯城さん」と呼ばれている。

「えー、みなさん、**アメリカがサイバー空間を第五の戦場と宣言**したことはご存じだと思います。私どもは当たり前のようにインターネットを使っていますが、備えなしにネットを使うなんていうのは**戦場を全裸で散歩するようなもの**です」

河合は話しながら、ホワイトボードに「第五の戦場」と大きく書いた。

「いつなんどき、我が社も被害に遭うかわかりません。知らない間に感染してウイルスつきのメールを送ったり、アドレスを盗まれたりして取引先やおつきあいのある作家さんにもご迷惑をかけることになりかねません。そこで招集されたのがこの委員会です。データ

漏洩は謝って済む問題じゃないんです。信用を失うだけでなく、お金も失います。日本は世界的にもデータ漏洩コストが高い国です。そのうえ、うちみたいな規模の企業だって狙われる世の中になってるんです。２０１５年の企業規模別標的型攻撃の43％は従業員数２５０名以下なんです」

河合は、そこで言葉を止めると、大きく息を吸った。興奮で少し頬が赤い。

「**総務部安全対策委員会**！　その目的は正しく安全なネットの使い方を社内に啓蒙することです！」

そして板書した。残るふたりは、はりきっている河合を不思議そうにながめている。

「委員会の最終目的は、我が社のサイバー防衛態勢の確立です。ここに**オペレーション〝ザ・ブック〟を発動することを宣言します**」

河合は、ホワイトボードの真ん中に〝ザ・ブック〟と書いて、バンと叩いた。叩いたはずみでペンが落ちる。片山と卯城は、どのような反応をすればよいのかわからず、顔を見合わせた。

「これって笑うところでしょうか？」

卯城が小声で片山に尋ねた。河合は、卯城をにらんだ。目の前なんだから小声でも聞こ


卯城
河合
ザ・ブッ
片山

えているし、というかここは笑うとこじゃない。
「……拍手じゃないかな？」
「じゃあ、手を叩きましょう」
ふたりは、おそるおそる手を叩いた。やればできるじゃないか、河合は何度もひとりでうなずいた。
「で、その〝ザ・ブック〟ってなにをすんの？」
片山が質問した。
「いや、だから**サイバーセキュリティの社内マニュアルを作るんですよ**」
「それだけ？」
「大事なことです！」
と言いながらふたたびホワイトボードを叩いた。今度はイレーサーが落ちた。片山と卯城は、びくっとのけぞる。
このようにして篠山兄弟社の〝ザ・ブック〟プロジェクトは始まった。社内サイバーセキュリティ・マニュアル作りだったはずのこのプロジェクトが、あのような結末を迎えるとは、この時点では誰も予想できなかった。

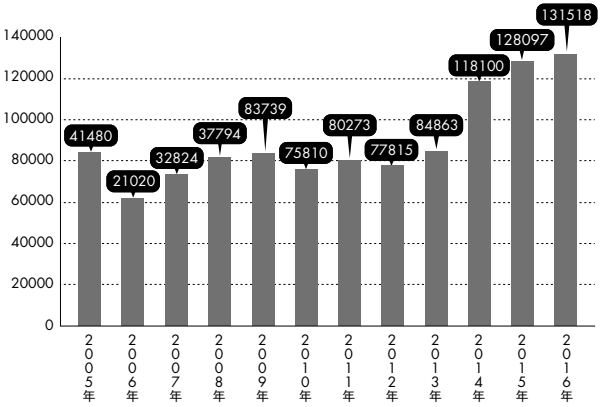
河合は豊かな胸をそらすと、ふたりに付け焼き刃で取得した知識を語り始めた。

「ニュースでサイバー攻撃やハッキング事件の報道を目にしたことがあるでしょう。あまり自分には関係ないと思ってませんか？　あんなことが自分や自分の勤務する会社に降りかかってくると思いませんよね。

でも、それは間違い。**誰でも被害者になる時代**なんです。2016年には、「Gooligan」と呼ばれるマルウェアが百万台以上のアンドロイドに感染してグーグルアカウントの情報を盗み出されたし、**他人の携帯電話を自分の支配下におくようなソフトも世界中に蔓延**しています。

中小企業も例外じゃないんです。アメリカのオバマ大統領は再選後の2度目の一般教書演説で、国家間のサイバー攻撃において一定規模以上の企業もターゲットにな

サイバー犯罪などに関する相談件数推移



警視庁「平成28年中におけるサイバー空間をめぐる脅威の情勢等について」を基に作成

ると言いました。サイバー攻撃はすぐには気づかないことも多いんで、やられていても気づかないんです。アメリカ国内の多数の企業から情報を盗み、企業活動を妨害し、経済を疲弊させることも狙いのひとつです。**ごく普通の企業もいやおうなく国際的なサイバー戦争に巻き込まれる**とオバマ大統領は指摘したわけです。

日本企業も狙われています。中小企業の持つ技術や情報を狙ったサイバー攻撃も考えられます。すでに始まっていて、それに気がついていない可能性だってあるんです。

世の中のいたるところにインターネットが使われており、そこからさまざまな脅威が迫ってきます。交通事故に気をつけるように、インフルエンザを予防するように、サイバー攻撃に注意を払う時代です。**誰でも明日は我が身**なんです」

目次

ACT. 1

特命書店員・河合牡蠣と二人の相棒

身近なサイバー兵器マルウェア

マルウェア防衛は、企業にとっても個人にとっても基本

河合が〝ザ・ブック〟の会議に向かうために廊下を歩いていると、自称ナンバーワン営業マンの高野(たかの)が近づいてきた。

「ハアイ」

高野のアメリカンな挨拶を河合はまじまじと見つめた。安易に調子を合わせて挨拶するのは危険だ。何度か目が合っただけで「あの人は僕を好きなんだ」と本気で思い込む危険分子。人生で互いの道が交わることはない、という事実を、大人の配慮でかもしださねばならない。

「なんでしょう?」

河合は意識して硬い声を出した。

「僕ね。最近、困ってるんですよ。女の子が積極的すぎて……」

にやけた高野の表情を観察しながら、河合はどのような思考回路でそんな発想が出てくるのか考えた。だが、話を聞いているうちに、美人局(つつもたせ)だとわかった。ネットで知り合い、言葉巧みにビデオチャットに誘導。そこに現れるのはセクシー美女。盛り上がってくると、服を脱ぎはじめ、あなたも脱ぎなさいと言い出す。誘いにのって裸になると、しばらくし

てから強面の脅迫メールが送られてくるという寸法だ。金を出さなければ、お前の裸の写真をばらまくと言われて、初めてからくりに気づく人も多い。

幸福そうにモテモテ話を語る高野を、河合は菩薩のような心境で見守った。菩薩でなければ肘打ちで顎を砕き、倒れてくるところを顔面に膝を合わせて総入れ歯にしている。

「でもね。僕、これからえらくなっちゃうから、あまり節操なく女性とおつきあいできないんですよね」

高野が、でれでれしながらさらに大きなホラを吹きだしたので、さすがに河合は離脱しなければと思った。高野はホラ吹きで有名だ。もっとも彼は、それが真実だと信じ込んでいる節があるので、否定するのは手榴弾のピンを抜くようなものだ。

「高野さんの幸福を祈ってます」

河合は、そう言うと高野の返事を待たずにそのまま立ち去った。20歩歩いてから振り向くと、高野はさきほどと同じ場所で瘴気に包まれてひとりでぶつぶつ言っていた。

河合が会議室に入ると、すでに他のふたりは部屋にいた。

「すみません。遅くなりました。廊下で高野くんにつかまってしまって……」

河合は、そう言いながら席についた。
「高野さんとおつきあいしてるという噂は本当だったんですね」
卯城が怪訝そうな声を上げた。
「違います。その噂は高野くんが自分で流しているものでしょ。彼は墓穴を掘るのが趣味ですから」
「私も噂になったことがあります。怒鳴られたこともあります。帰りにたまたま電車に乗り合わせたんです。さしさわりのない話をしていたら、急に独り言モードに入って、意味不明のつぶやきをはじめて、それから急に怒鳴ったんです」
「怖い……理由なく怒鳴ったの？」
「それが……〝なんで金利を下げたんだ〟って最初に怒鳴って、それから〝採点方法がおかしい〟とかわけのわからないことを言うんです。10分間くらい怒鳴りっぱなしでした。あんなに人に怒鳴られたのって、実家を出て以来です」
「高野くんは要注意ですね」
「あんまり、いじめるなよ。あいつはさびしい可哀想なヤツなんだよ」
見かねた片山がフォローのつもりでそう言うと、河合と卯城は顔を見合わせた。

「片山さん、安易な同情は自分を貶めるだけですよ」
河合は、そう言うと立ち上がった。
「はい、雑談はここまで！　本日のテーマはマルウェア防衛です。**マルウェアは悪いことをするソフトの総称**です。昔はウイルスって呼んでいたんですけど、いろいろなタイプが現れて実態にそぐわなくなったので、最近はマルウェアと呼ぶことが多いです。片山くんはマルウェア対策をなにかやってますか？」
「アンチウイルスソフトをインストールしてるけど。それでじゅうぶんじゃないの？　今まで感染したことないしさ。ねえ」
片山はそう言いながら、隣の卯城に同意を求めた。
「……私、感染したことあります」
卯城はそれには答えず、窓の外に目を向けると独り言のようにつぶやいた。
「アンチウイルスソフト使ってなかったの？」
河合の言葉に、卯城は顔を横に振った。
「インストールしてたけどダメでした。感染したのも、すぐにはわからなかったんです。でも、いろんな人からメールや電話が来て……私から変なメールが来たって……私がウイ

ルスにかかったんだろうって言われた」
卯城の声が少し震えている。よほど怖い思いをしたのだろう。
「それで卯城くんは、どうしたの？」
「あわててＬＡＮケーブルを抜きました。勢いよく抜いたから、パソコンが机から落ちてディスプレイが割れてしまって……」
「そ……それは大変だったわね」
予想外の惨事に河合も言葉を失いそうになった。
「……壊れたディスプレイを片付けて掃除しようと思ったんです。でもたくさんケーブルがあって邪魔だったから抜いたんです。そしたらみんなのパソコンの電源が落ちてしまって……たくさんのデータが消えて……マルウェアって危険ですね」
「なんか違うような気もするけど、貴重な体験談をありがとう」
河合は、そう言うとホワイトボードに向かった。

マルウェアを防ぐことは原理的に無理！

大きく板書した。
「ウソだろ？　だってアンチウイルスソフトがあるじゃん」
片山が抗議の声を上げた。
「レッドオクトーバー作戦は知ってますか？」
「ショーン・コネリーが原潜でアメリカに亡命する話ですね」
すかさず卯城が答える。こういうどうでもいい知識は卯城の得意分野だ。
「それは『レッド・オクトーバーを追え！』。こちらは大規模サイバー作戦です。２０１３年1月にロシアのサイバーセキュリティ研究所カスペルスキーラボが、6年間におよぶ諜報作戦〝レッドオクトーバー〟の内容を暴露しました。ターゲットは東欧を中心とした全世界。世界中の重要人物のパソコンや携帯などから重要な情報を盗み出していました。日本もターゲットでした」
「へー、よく見つからなかったね」
「問題はそこなんです。この作戦がすごいのは、**6年間も気づかれなかった**ことです。理由は簡単です。全てのターゲットに合わせて、専用のマルウェアを使っていたんです。**その時点で検知、防御できない最新のゼロデイ攻撃**。しかも手強い相手には、いったんその相

手に近しくてガードの比較的甘い人物に感染させ、そこから狙いの相手を攻撃するといった手間のかけかたです。ここまでやられると防ぐことはかなり難しいです。親しい相手から添付ファイルが届いたら開けますよね。それで感染してしまうわけです」

「世の中は闇だわ。死のう。死にしか平穏はない」

「いや、まあ、あたしたちみたいな弱小民間企業にそこまで手間をかけることはないと思うけどね。そこまでされなくても、すでにじゅうぶん危険という現実もあります。卯城くんの例でもわかるように、**アンチウイルスソフトには限界がある**んです。世の中に出回っているマルウェアは国際間紛争の解決手段、つまり兵器になっているんです。そんな物騒なものが、1万円もしないアンチウイルスソフトで防げるわけがないでしょう。細菌兵器で攻撃されても花粉症のマスクしてるから大丈夫っていうようなものです。マイクロソフト社は、政府にまかせておけないと思ったのか、自前でサイバー犯罪対策チーム作って、FBIと共同作戦やってます。この10年間でマルウェアは劇的に変化したんです」

「ほんとか？　じゃあどうすればいいわけ？」

片山が驚いた様子で声を上げた。

「**死ぬのよ。みんな、マルウェアに脳髄まで侵されて心中することになるの**」

卯城がつぶやく。
「いや、卯城くん、それは行きすぎ。まずはちょっと基本的なことを整理しておきましょう」
河合は、セルフレームの眼鏡のつるを人差し指で、くいっと持ちあげて説明を始めた。

・ウイルス、マルウェア、スパイウェア

最初にまず言葉について整理しておきましょう。悪いことをするソフト全般をマルウェアと呼びます。この中で感染し、広がる力を持っているものがウイルスです。パソコンの中の情報を盗み出すものをスパイウェアと呼びます。ただし、ウイルスという言葉は昔から使われているので、マルウェア全体と同じ意味で使われることもあるので注意しましょう。

身を守るためには、危険なソフト全般から守ってもらわなきゃいけないので、アンチウイルスソフトはマルウェア、つまり悪いソフト全般を検知するように作られています。

・アンチウイルスソフトの弱点　未知の攻撃には対処できない

アンチウイルスソフトがマルウェア防御のためにしているのは、ひとことで言うと「既存のマルウェアに一致するものを検知し、対処する」こと。ふるまい検知などそれ以外の方法もありますが、主流ではありません。通信やファイルの内容をチェックして、すでにマルウェアとして知られているものと一致するものがあれば、警告を出して、隔離したり、駆除したりするわけ。やってることは単純です。

でも、実際にはひどく大変です。なぜかというと、マルウェアは毎日新種が大量に生まれてくるから、それにいちいち対応しなければいけない。自動的に新しいマルウェアを発見して、それに対処できるようになるわけではないのです。基本は手動。アンチウイルスソフト大手のトレンドマイクロ社は毎月2万件の新種ウイルスを発見しているらしいから、その労力は相当なものでしょう。

アンチウイルスソフトによって呼び方は違うけど、パターンファイルとか差分とかワクチンとかそういうものを毎日ネットからダウンロードして更新しているのは、新しいマルウェアに対応するためです。

だからアンチウイルスソフトの会社は、新しいマルウェアの検体を入手して、迅

速に対処する態勢になっています。検体というのは、マルウェアそのもの、ソフトそのもののことです。

ここでカンのいい人ならわかると思いますが、新種のマルウェアが活動を開始してから、アンチウイルスソフトが対応するまでには少しタイムラグがあります。誰かが新しいマルウェアを作ってもすぐに見つかるわけではないので、作られてそれが発見され、さらに対処できるようになるまでの間は守る方法がないことになります。

「へー、そうなんだ。知らんかった。勉強になる」

素直に感心する片山に河合は、えへんと胸を張る。片山の視線が、その胸に向けられる。

「片山さんの目にマルウェアが侵入した模様です」

卯城はそう言うと、片山の目に人差し指を突っ込もうとした。

「うわ！　やめろって」

「ふたりとも、遊ばないでください。これは業務なんですよ」

「オレのせいじゃない。卯城が暴れるから」

「片山さんがいやらしい目つきで河合さんを見るからです」
「ああ、もうやめてください！　続けますよ。ゼロデイ攻撃って聞いたことあります？」
「オレ、聞いたことある。でもなんだっけ？」
「世の中に存在するシステムやソフトに絶対安全ということはありません。一時的に安全でも、時間が経てば弱点が見つかります。サイバーセキュリティ業界では、脆弱性と呼ぶことが多いですけど。**脆弱性が見つかってから、その対策ができるまでの間は守る方法がない**わけです。この空白期間に攻撃することをゼロデイ攻撃と呼びます。新しいマルウェアが出てきてから、アンチウイルスソフトが対応するまでの空白期間に似てます」
「えー、その間ってアンチウイルスソフトは全然役に立たないのかよ」
「正確に言うと、ふるまい検知みたいな方法はあることはあります。ふるまい検知というのは、外部から来たものの活動の内容を観察して確認する方法です。でもこれも限界があるんですよ。誤検知、マルウェアでないものをマルウェアと勘違いすることが多いし、観察している間は怪しいことをしないでやりすごすものも出てきたし、検知結果をいちいち人が確認する必要があるし、いろいろ面倒なんですね。インストールして終わりというほど簡単ではないわけ。というわけでゼロデイ攻撃を使われると、かなりヤバイわけです」

「人類が作る道具は、常にその利益を上回る不幸を与えます」

卯城が暗い顔でつぶやいた。

「文明史はスルーします。じゃあ、次にどんなルートで感染するか見てみましょう」

感染ルートはまずメール、次にサイト

「マルウェアの感染元はメールからというのが多いですね。メールに添付されていたファイルを開いて感染するパターンです。あとマルウェアの置いてあるサイトへ誘導するのも多いです。なにしろ、電子メールのおよそ5通に1通はマルウェアのあるサイトへ誘導するものなんです」

「私の時もそうだったみたい。メールに添付されていたファイルを開いたら……あんなことになってしまって」

「そういう被害者はたくさんいますね。毎日大量に送られてくる迷惑メールの中にもマルウェア付きのものもあるし、マルウェアを配布するサイトに誘導するものもあるんです。添付ファイルを開くと感染するタイプが一般的。添付ファイルの種類は、マイクロソフト

オフィスの文書ファイル、PDF、画像ファイルなどいろいろなものがあります。最近のメーラー、メールソフトの多くは添付ファイルを開こうとすると警告が出るようになっていますね。これはここからの感染が多いためです」

「あの手、この手で襲ってくるんだな。しつこい勧誘みたいだ」

片山がため息をつくと、河合はうなずいた。

「しかも巧妙なんです。最近増えている標的型攻撃は、特定の相手に合わせたメールを送ってくるんですよ。こんなメールが来たらつい開いてしまいそうでしょう？　ぼかしてあるところは、実在の知り合いの名前なんですよ」

「こりゃ、すごい。本物にしか見えないだろ」

「次によくあるのが、サイト。メールやブログに貼ってあるサイトに行くと、ソフトをダ

電子メールの悪質な添付ファイル

ランク	ファイル拡張子	メールでブロックされた割合
1	.doc	55.8%
2	.xls	15.0%
3	.zip	8.7%
4	.htm	7.9%
5	.docm	2.4%
6	.js	2.2%
7	.mso	1.9%
8	.html	1.6%
9	.exe	0.9%
10	.png	0.8%

シマンテック社「2016年インターネットセキュリティ脅威レポート」を基に作成

2015年には、Officeドキュメントが最もよく利用される添付ファイルとなり、実行可能ファイルの利用は減少しています。添付ファイル全体の1.3%が、.exe、.com、.pif、.batなどの実行可能ファイルでした。

標的型攻撃メールの例

●●●

リスクベース評価手法を用いた船舶設計に関する
国際ワークショップ開催のご案内.zip

関係各位
独立行政法人******(理事長*****)
及び一般財団法人*****(会長*****)は、
国際海事機関(IMO)で導入が進む
リスクベース評価手法の最先端の研究動向について
海外からリスク評価研究に関する
専門家を招き、国際ワークショップを
平成23年10月11日・12日に開催します。

※添付書類:
リスクベース評価手法を用いた船舶設計に関する
国際ワークショップ開催のご案内(10/07)
以上

●●●

6月4日、5日会議出席報告

各位
いつもお世話になっております。
6月4日、5日の会議録を送付いたします。

ご査収下さいますようお願い申し上げます。

ウンロードするように言われるとかね。**最近注意が必要なのが、ソーシャルネットワーク経由かな。ツイッターやフェイスブックから感染するパターン。**これもやっぱりリンクが貼ってあってクリックすると、勝手にファイルをダウンロードし始めるような罠があるのね」

「**世界は悪意に満ちている**」

卯城もため息をつく。

「まあね。メール以外にもたくさん感染ルートがあります」

河合はプリントを配った。

㉓WEBサイト

WEBサイトの多くはスクリプトやJavaアプレットなどを用いています。これらを悪用して感染させようとすることもあります。手の込んだものでは、「あなたのパソコンがマルウェアに感染しているかどうか検査します」と言って検査するふりをして、マルウェアをインストールさせるものもあります。

❸ソーシャルネットワーク

最近急激に増えています。ソーシャルネットワーク経由でメッセージを送って、危険なアプリをインストールさせたり、危険なサイトに誘導したりするものです。ツイッターやフェイスブックのアプリは、しつこく友達を誘えと言ってくるので、健全なアプリも誘いのメッセージを送ってくるものがあります。それに慣れていると、危険なアプリとの区別がつかなくなってしまいます。

❹USBメモリを差し込む

直接USBメモリを挿して感染させることもできます。この方法は相手が特定されている場合にしか使えません。

他の会社や官公庁に行った時に、こっそりとUSBメモリを挿す悪い人もいます。また、出入りの業者、宅配便、清掃の人なども犯行におよぶことが可能。

一番やりやすいのは内部犯行。誰にも見られないように、他の人のパソコンにUSBを挿すくらいならさほどむずかしくありません。

⑥その他

ベンダが配布しているＣＤ－ＲＯＭやＤＶＤの中にマルウェアが混入していることもありますし、社内ＬＡＮ経由で感染することもあります。さまざまな方法で感染を広げてくるんです。

「マルウェアに感染するとどうなるかも説明しておきますね」

河合は、そう言うとホワイトボードに書きだしていった。

他の人に感染を広げる踏み台になる

「アドレス帳や過去のメールを参照してメールを送りまくり感染を拡大させるんです。自分の名前で勝手にメールを出したり、ツイッターやフェイスブックでメッセージを送ったりして感染を広げようとします」

情報を奪われてさらされる

「情報を盗み出してどこかに送られてしまうことも多いです。パソコンに保存しているアドレス帳やメールの記録など大事な情報が盗まれます。業務用の顧客情報を奪われるようなことがあると悲劇です」

個人情報を盗まれて、なりすまし詐欺の被害に遭う

「銀行口座などの情報と認証情報（ＩＤやパスワード）を盗まれて、お金を奪われてしまいます」

パソコンの操作を監視して、その内容をどこかに送る

「利用しているサイトのＩＤやパスワードを盗まれてしまうわけです」

なりすまされていたずらされる

「ＩＤとパスワードを盗まれると、犯人は自分になりすますことができますから、いたずらや悪いことをやり放題です」

新しいマルウェアをダウンロードする

「マルウェアが勝手にバージョンアップ、機能強化してしまうんです」

パソコンを利用して、他のパソコンやサーバを攻撃する

「自分のパソコンが誰かに勝手に遠隔操作されてしまうんです。なにをされるかわかりません。**知らない間に犯罪に加担してしまうことだってあります。**

こんな感じです。いやでしょう？　昔のマルウェアは、感染するとすぐにわかりました。他の人にメールを送りまくるとか、画面に変なものが表示されるとか、わかりやすくおか

しなことが起こりました。今でも、そういうマルウェアはありますが、**危険なのは深く静かに隠れていて、大事なものを盗んでいくもの**です」
「いやな世の中になったなあ」
「それだけじゃないんです。**発見されないマルウェアもある**んです。いいですか？　マルウェアは、目に見える悪さをするから、感染したってことがわかるわけで、静かに情報だけ盗みとっていたらわからないでしょう？　これっていやじゃありませんか？」
「なるほどね。さっきのレッドオクトーバーとかもそうだよな」
「そうです。特定の相手を狙ったマルウェアで標的型攻撃と呼ばれるものです。主に政府関係機関や大企業が狙われています」
「オレたちには関係なさそうだな。そんな狙われるような会社じゃないもんな」
「いえ、標的型攻撃の対象の43％は２５０名以下の会社なんです。これからはそうとも言えないんです」
「やっぱり、みんな死ぬのね」
「だから違うってば！　なぜうちみたいな会社も狙われる可能性があるか説明しますよ」

アンチウイルスソフトでは防ぎきれない標的型攻撃
重要なのは基本の心がけ

「中学生がウイルスを自作する時代なんです。万引きでつかまった子供が腹いせに攻撃することだってありえます。本屋のお姉さんに恋をして、個人情報を知りたくなって本屋の監視カメラをハッキングすることだってあるでしょう。

ごていねいに開発キットまであります。２０１２年には**13歳の中学生がウイルスを作成して補導**されています。ウイルスを作るのは、そんなに特別なことではなくなっています。犯罪組織が特定の企業を狙ってオリジナルのマルウェアを作ったり、個人的な復讐のためにウイルスを作ったりする時代なんです。我が社も中小企業だからといって安心はできません。競合相手や怨みをもって退職した社員から攻撃されるかもしれません。警察庁によれば２０１６年に不正アクセス禁止法で摘発されたのは10代が全年代もっとも多かったそうです」

「信じられない……！」

「子供は怖い。子供はほんとうに怖いんです」

「卯城くん、ちょっと黙ってて。世の中、どんどん便利になってきてるんです。それで攻撃のためのツールもどんどん増えてきて、その結果**誰でもお手軽にネット犯罪者になれる**ようになりました」
「でもさ、そういう情報って子供が手に入れられるようになる頃には、もう古くて使えないんじゃないの？　知れ渡って、アンチウイルスソフトとかが対応してて さ」
「ブー！　甘いですね。**世の中には、ぬるい人がたくさんいるんです**」
　河合は、そう言うと天井に向かって指を突き上げた。卯城がその指先の示す先に目をやったが、ベージュに塗られた天井にはくすんだ染みがあるだけだった。
「“SERT Quarterly Threat Intelligence Report”というサイバーセキュリティ専門会社が発表したレポートで、よく利用されている26のサイバー攻撃用ツールキットを調べた結果、58％は2年以上前の脆弱性を利用していたそうです。古いものには２００４年のものも含まれていたというから驚きですね。世の中、サイバーセキュリティにうとい人が多いんです」
「ほんと？」
「アンチウイルスソフトも使わず、ＯＳやアプリの更新もしない人がたくさんいるんです。だからそこをちゃんとするだけでも、かなりましです」

「なるほどね。でもさ、特定の相手向けに作られたマルウェアは検知できないんだろ？」
「基本的にはそうですね」
「じゃあ、防ぎようがないんじゃないの？」
片山が肩をすくめ、
「やっぱり……死ぬのね」
卯城が床を見つめてつぶやいた。
「いや、死なないから！　ええとですね。こう考えるといいと思います。交通事故を防ぐために信号やガードレールがありますよね？　でも、赤信号で渡ったり、ガードレールを乗り越えたりすれば意味がない。信号を守っていても車が突っ込んで来ることもあるし、ガードレールを破ってくることもある。信号やガードレールでの防御には限界があります。でも、ないよりはあった方がはるかに安全でしょう。アンチウイルスソフトも同じです」
「えーっ、その程度なの？　なにか決め手はないの？」
「道具はしょせん道具です。最大の防御は、心がけです。不審なファイルは開かないこと、危ないサイトには行かないこと、送り主のわからないメールやソーシャルネットワークのメッセージにはじゅうぶん注意することです」

「それってすごく基本的なことだよね？」
「基本ですけど、これが守られていればかなり安全ですよ」
「誰も助けてくれないのね」
「卯城くん、リアル世界だって誰も助けてくれませんよ」
「リアルではカレが助けてくれますよ」
「お前、男いるの？　脳内彼氏ってヤツじゃないの？」
「失礼なことを言わないでください。**私のカレはいつでも私のそばにいます、バッテリーの続く限り**」
卯城はそう言って携帯電話を取り出すと、待ち受け画面に見入った。片山と河合はしばし言葉を失った。
「……ここは笑うところです。信じないでください。失礼ですよ」
卯城がそう言ったので、ふたりはほっとした。だが、笑う気にはなれない。

マルウェア防御5箇条

「ええとですね。話を続けます。敵も警戒している相手にも感染させたいから、いろいろ

工夫をしてくるんです。特に覚えておきたいのはこのへんです」

河合は、ふたりに背中を見せると、ホワイトボードに注意事項を書き始めた。

知人や信頼できる発信者を装う

（取引先、知人、公的機関、利用しているサイト、金融機関など）

興味あるいは身近にありそうな目をひくタイトルと内容

「東日本大震災や原発事故に関連したメールのマルウェアも多く出回りました。ターゲットを決めて狙ってくる時は、業務内容に関したメールを送ってくることもあるので見極めるのが難しいです。

そして対策で大事なのは、なんといってもこの5つです」

河合はそう言うと板書した。

・OSやソフトを常に最新の状態にしておく

・アンチウイルスソフトをインストールしておく
・よほど信頼できる場合以外は、添付ファイルを開かない
・怪しいサイトにアクセスしない
・怪しいソフトをインストールしない

「特に後半の3つには注意が必要です」

よほど信頼できる場合以外は、添付ファイルを開かない

「メールの内容を確認して、本当に必要があって知り合いから送ってきたものかどうかを確認するのは基本です。

法人から送られてきた添付ファイルは要注意です。銀行、会員サイト、ECサイトから添付ファイルが送られてきたら、必ずチェックしましょう。ヤフーで個人情報漏洩が起きた時には、ヤフーのアドレスで怪しいメールが送られてきました。誰でも簡単に入手できる無料のヤフーメールのアドレスと、ヤフーの会社自身が使っているアドレスの区別がつ

きにくいことを狙った罠です。

送信者のアドレスがいつもと同じか確認する。似たようなまぎらわしいアドレスを使うことがあるので、一文字一文字きっちり確認しましょう。

メールの文章がおかしくないか確認する。

過去にも同じように送られてきたことがあるか確認する。もしも初めてであれば、その旨くわしい説明がなければなりません。

サイトを確認し、メールの内容の裏付けになるようなお知らせがあることを確認する。

それでも不安な時は、直接電話で確認しましょう」

怪しいサイトにアクセスしない

「最近は見ただけで悪さするサイトや、巧妙な文言で騙(だま)そうとするサイトがたくさんあります。怪しいサイトとは内容じゃなくて、運営している会社や個人が大丈夫かってことです。例えば、**あなたのパスワードの強度をチェックしますといってパスワードを入力させて盗む**とか、ウイルスに感染しているかどうかチェックしますといって、感染していないの

に感染しているからといって急いでこのソフトで駆除しましょうとか、あの手この手で騙してきます。一見もっともらしいことを言うので、うっかり騙されてしまう人もいます。だから、運営会社のチェックが必要なわけです。第一に、運営会社の名前や住所がわからなかったら、そこでアウトです。

守りを固めることも大事ですが、危ないところに行かないことも大事です。

リアルと同じですね。**怪しいところに完全武装で行くよりは、最初から危ない場所には行かないのが一番**ってことです。相手が自分よりも重装備だったらどうにもなりませんから」

怪しいソフトをインストールしない

「ネットにあるソフトは、よほど安心、信頼できるところでなければインストールしてはいけません。基本は、ネットのソフトはインストールしない！　これにつきます。この7つを守っていればたいていは防げます」

「なんか当たり前の話だなあ」

「でも、現実にはなかなかできないんです。だって業務で送られてきた添付ファイルは開

かざるを得ません。でも、それが罠だったりするわけです。全ての関係者が万全のセキュリティというわけではないですから、送られてきた書類には罠が仕込まれている可能性が常にあります」

「しょせん、人情紙風船」

「参考に付け加えると、ＩＰＡ（独立行政法人情報処理推進機構）ではウイルス対策を７箇条にまとめています」

1 最新のウイルス定義ファイルに更新しワクチンソフトを活用すること

2 メールの添付ファイルは、開く前にウイルス検査を行うこと

3 ダウンロードしたファイルは、使用する前にウイルス検査を行うこと

4 アプリケーションのセキュリティ機能を活用すること

5 セキュリティパッチをあてること

6 ウイルス感染の兆候を見逃さないこと

7 ウイルス感染被害からの復旧のためデータのバックアップを行うこと

「では、ひととおり説明しましたから、次回の会議までに片山くんにまとめておいてもらいましょうね」
河合は、そう言うと席に腰掛けてお茶をすすった。
「ええっ!?　オレなの？」
片山は、甲高い声をあげ、河合を見る。
「お茶おいしい」
河合は無視した。卯城はいつの間にか、そそくさと席を立ってどこかに隠れてしまった。
翌週、疲れた顔で会議にやってきた片山はまとめの紙を河合に手渡した。
「片山くん、よくできました」
河合は、そういうとにっこり笑った。

前提として知っておくべきこと

- マルウェアを完全に防御することはできないことを前提に備えを考える。
- マルウェアに感染しても気づかないことがある。だから危険な兆候には注意を払うようにする。

対策

- 感染ルートはメールとサイトが多いので、この2つの利用にあたっては、安易にファイルを開かない、インストールしないようにする。

- 知り合いあるいは関係している企業、機関からのメール以外は、じゅうぶん注意すること。表示される名前だけでなく、アドレスやドメインも確認すること。
- 危険な兆候があったらすぐにネットワークを切断して、状況を整理、確認する。
- アンチウイルスソフトをインストールしておく。
- OSやソフトを常に最新版にしておく。