2023 年 7 月 10 日

サイバー攻撃を知る-その１

対策を検討するため、相手（コンピュータウイルス）を知る

技術士（情報工学部門）
きよし事務所　代表　清　孝雄（Takao Kiyoshi）　著

目次

１　コンピュータウイルスの種類と特徴

～ファイル感染型、マクロ感染型、ワーム型、トロイの木馬型など～

コンピュータウイルス、Emotet（エモテット）、ランサムウェアに対する対策は、まず、相手を知ることが重要です。攻撃者がどのような手法を使っているかを理解することで、それに対する対策を考えることができます。

例えば、ランサムウェアの場合、バックアップを定期的に取ることで、被害を最小限に抑えることができます。また、セキュリティソフトの導入やアップデートも重要です。

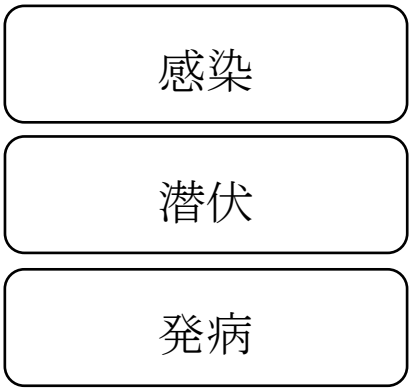
このような対策を行うことで、コンピュータウイルスやランサムウェアなどの被害を最小限に抑えることができます。

今話題の、ランサムウエアのお話の前に、コンピュータウイルスの種類と特徴についてお話します。

(1) コンピュータウイルスとは

コンピュータウイルスとは、プログラムやデータベースに対して被害を及ぼすよう、悪意のある第三者が作り上げたプログラムのことです。

経済産業省の「コンピュータ対策基準」によると、『



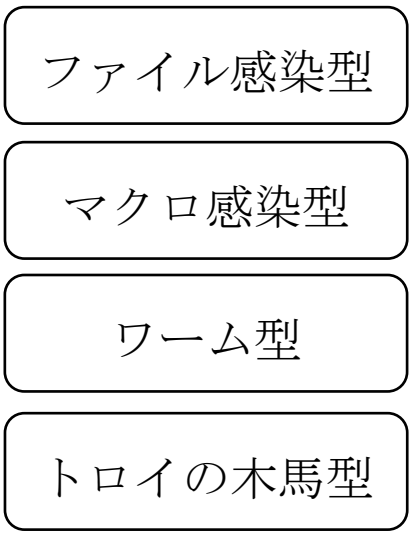
・「自ら増える（感染）」
・「特定の期間潜伏する（潜伏）」
・「ファイルを破壊したり意図しない動作をしたりする（発病）」

のうち、1つ以上の機能を持っているもの』と定義されています。

病気の新型コロナやインフルエンザウイルスのように拡散能力が強いため、第三者へ

の影響も考慮しなければならない非常にやっかいな存在です。

⑵ コンピュータウイルスには、



などがあります。

ア　ファイル感染型

ファイル感染型は、プログラムに付着して勝手に改ざんし感染・増殖する種類のウイルスで、上書き型・追記型といった複数のパターンがあります。

⑺ ファイル感染型ウイルス

ファイル感染型ウイルスは、実行形式のファイルに付着しているウイルスです。

ファイルサイズなどが変わることなどで発見しやすく、感染したことが判りやすいと言われています。

代表例の PE_EXPIRO（ピーイー・エクスピロ）は不正な Java アプレットを介して PC に侵入し、情報収集機能を備えたウイルスでした。

⑴ PE_EXPIRO は、2010 年に登場したファイル感染型のコンピュータウイルスで、感染すると、端末内の情報収集を行い、複数のサーバに送信することがあります。 このウイルスに感染すると、以下のような症状が現れることがあります。

・ファイルの改変

・情報収集

PE_EXPIRO は、主にメールの添付ファイルや Web サイトからダウンロードされたファイルなどを通じて感染することがあります。

イ　マクロ感染型

マクロ感染型は、表計算ソフトなどに搭載されているマクロ機能を悪用したウイルスです。

(ｱ) マクロ型ウイルス

メールに添付されたファイルを開くことで感染します。

代表例の Melissa は、感染したパソコンからメールを大量に送信し、何人もの受信者が何の疑いもなく自ら添付ファイルを開くことで被害が拡散しました。

(ｲ) Melissa は、1999 年 3 月に初めて発見されたマクロウイルスで、感染すると、Microsoft Word で作成された文章ファイルで自己拡散によるサーバへの高負荷が目的で、Outlook の登録アドレス上位 50 件にウイルスを自動転送することがあります。

このマクロウイルスに感染すると、以下のような症状が現れることがあります。

・メールの送信
・ウイルスの自動転送
・ウイルスに感染したファイルの作成

Melissa は、マクロ型ウイルスに感染しているファイルを開いたり、Office 製品を使用している場合に感染することがあります。

他に有名なマクロ型ウイルスには、以下のようなものがあります：

・ILOVEYOU
・Nimda
・Code Red
・Sasser

これらのウイルスは、感染すると、コンピュータの動作を遅くしたり、データを消去したりすることがあります。感染経路は、メールの添付ファイルや Web サイトからダウンロードされたファイルなどがあります。

ｳ　ワーム型

(ｱ) ワーム型は、自己増殖をするウイルスで、感染したコンピュータから自動的に他のコンピュータに感染します。

ワーム型ウイルスは自己増殖しながら、他のデバイスへ感染を拡げるのが目的の不正プログラムを指します。メールやネットワークに接続されているだけで感染する場合もあり、感染力が強いのが特徴です。

感染するとパソコンが重くなるなどの症状が出ます。代表的なものとして、LOVELETTER（ラブレター）、Slammer（スラマー）、MyDoom（マイドゥーム）などが有名です。

(ｲ) LOVELETTER は、2000 年 5 月にフィリピンで発生したワーム型ウイルスです。

症状としては、メールの添付ファイルを開くと、自動的に送信者のアドレス帳にある人々に自分自身を送信するようになっています。また、感染したコンピュータ内のファイルを削除する機能も持っています。

侵入経路は、メールの添付ファイルを開くことで感染します。

(ｳ) Slammer は、2003 年 1 月に発生したワーム型ウイルスです。

Microsoft の SQL Server に存在する脆弱性を利用して、インターネット上で瞬

時に膨大な量の感染を招きました。症状としては、ネットワークの遅延やサーバのダウンなどが報告されています。

侵入経路は、ハッカーまたは感染されたホストからMicrosoftのSQL Serverに存在する脆弱性を利用して感染します。

(ｴ) MyDoomは、2004年に発生したワーム型ウイルスです。

感染したコンピュータから大量のメールを送信することで、インターネット上で瞬時に膨大な量の感染を招きました。症状としては、メールの添付ファイルを開くと、自動的に送信者のアドレス帳にある人々に自分自身を送信するようになっています。

侵入経路は、メールの添付ファイルを開くことで感染します。

エ　トロイの木馬型

(ｱ) トロイの木馬型は、偽装して侵入するウイルスで、一見正常なプログラムとして振る舞いますが、実際には不正な操作を行うようになっています。

トロイの木馬型ウイルスは、ほかのシステムやファイルに感染しないウイルスです。正規のアプリに偽装してユーザーがインストールすることで侵入します。

パスワードやファイルの削除や個人情報流出などが主な被害事例です。

代表的なものとしては、Emotet（エモテット）、Twitoor（トゥイトーアー）などがあります。

(ｲ) Emotetは、2014年に初めて発見されたマルウェアで、主に電子メールを介して感染する遠隔操作型のボットマルウェアです。

Emotetに感染すると、以下のような症状が現れることがあります。

・さまざまなマルウェアに感染する
・個人情報や機密情報の流出
・他のデバイスへの伝染
・サーバのデータを失う

Emotetは、悪意のあるサイトにアクセスしたり、悪意のあるマクロを含むファイルを開いたりすることで感染します。

(ｳ) Twitoorは、攻撃者のTwitterアカウントを介して攻撃指令を受け取るAndroid版トロイの木馬で、2016年に発見されました。

このトロイの木馬に感染すると、定期的に司令用の不正Twitterアカウントをチェックし、情報の送信やマルウェアのダウンロードを行うことがあります。

☕コーヒーブレイク　ちょっと一休み☕

【トロイの木馬とは】

　トロイの木馬という名前の由来は、ギリシャ神話のトロイア戦争だ。侵攻を続けるギリシャ軍は、難攻不落の都市であったトロイを攻略するため、自軍の一部を巨大な木馬に潜ませ偽装撤退する。

　トロイ軍はつかの間の勝利に沸き、この木馬を戦利品として城砦内に運び宴を開催した。トロイ軍が酒肴に酔いしれ寝静まったころ、木馬に潜んでいたギリシャ兵が抜け出し城門を開ける。

　ギリシャ軍は難なく城門を突破し、不意を打たれたトロイは陥落してしまう。

この故事のように、トロイの木馬は無害なプログラムを装ってターゲットの端末に侵入し不正を働く。

　侵入に成功したトロイの木馬は ID やパスワードなどの情報窃取、他のマルウェアのダウンロードを行う。秘密裏に潜伏し、一定期間の経過後に行動するため感染してしまうため発見しづらいのが特徴です。

２　コンピュータウイルスによる被害事例

具体的な被害について見ていきましょう。

(1)動作しない	(5)システム・ ネットワーク停止
(2)ファイル削除	(6)個人情報漏えい
(3)ウイルスメール 大量自動送信	(7)暗号化・身代金
(4)踏み台	(8)HP 改ざん・信用失墜

(1) パソコン本体やソフトウェアが動作しなくなる
(2) 保存しているファイルが削除される
(3) ウイルス付きのメールが大量に自動送信される
(4) データ大量送信による加害者（踏み台）となる
(5)　〃　受信被害者（システム・ネットワーク停止）になる
(6)保存している個人情報（パスワードやクレジットカード情報含む）が盗まれる
(7)パソコンが暗号化され、業務停止を余儀なくされ身代金を要求される　など
(8)恐ろしいのは実害だけではありません。もしホームページ改ざんやウイルス被害が出たと世間に広まれば、「あそこはセキリュティ意識が低いから仕事を任せられない」と、社会的信頼や取引先からの信用は失墜します。

以上のことから、コンピュータウイルスのセキュリティ対策は万全にしておくべきといえるでしょう。

☕コーヒーブレイク　ちょっと一休み☕

Emotet

Emotet は、もともとバンキングマルウェアだったが、数年で強力な感染力をもつ「モジュール型マルウェア」へ進化している。感染後に Outlook からメールの送信者名などを窃取し、その情報をもとにさらなる標的型攻撃を行う。
さらにはランサムウェアに感染させて金銭を要求します。

(1) 国内でのランサムウェアの被害事例

ア　ランサムウェアの感染によるシステムの停止

企業のシステムがランサムウェアに感染し、サーバ内のファイルが暗号化されたことが原因でシステムが起動しなくなった事例です。外部からのアクセス制限が適切に作動しなかったことから、攻撃者の侵入を許したことが原因と推測されています。

イ　種類

ランサムウェアには、「WannaCry（ワナクライ）、TeslaCrypt（テトラクリプト）、CryptoWall（クリプトウォール）、Bad Rabbit（バッドラビット）、Oni（オニ）、Locky（ロッキー）、SNAKE（スネーク）、Maze（メイズ）」などがあります。

ウ　特徴

これらのランサムウェアは、感染した端末やそこに保存されているファイルを使用不能にし、その解除と引き換えに身代金を要求するマルウェアです。

エ　感染経路

ランサムウェアは、不正なメール（攻撃メール）から感染が拡大しているマルウェアです。

VPN やリモートデスクトップの脆弱性を悪用したランサムウェアによる攻撃も確認されています。ランサムウェアの感染経路について、NISC（独立行政法人情報処理推進機構）によると、社外から社内の業務システムに接続する際に使われる VPN（仮想私設網）機器が最多で、次にパソコンを遠隔から操作する「リモートデスクトップ」が多くなっています。

ランサムウェアに感染すると、マルウェアがダウンロードされ、主に以下のような被害をもたらします。

・パスワードやクレジットカード情報などの個人情報を盗まれる
・感染したコンピュータを制御・暗号化される
・他のマルウェアをダウンロードされる

オ　手順１（メール）

ランサムウェアは、主に以下のような手順で発症します。

(ｱ) メールに添付されたファイルを開く
(ｲ) ファイルを開くと、ランサムウェアがダウンロードされる
(ｳ) ダウンロードされたランサムウェアが、ファイルを盗難・暗号化する
(ｴ) ランサムウェアは、身代金を要求する

カ　手順２（VPN やリモートデスクトップ）

(ｱ) 攻撃者は、VPNやリモートデスクトップのサービスを提供するサーバに対して、脆弱性を探索するスキャンを行います。
(ｲ) 脆弱性が見つかった場合、攻撃者はその脆弱性を利用して、サーバに侵入します。
(ｳ) サーバに侵入した攻撃者は、ランサムウェアをインストールし、サーバ上のファイルやデータを暗号化します。

(ｴ) ランサムウェアは、身代金を要求する

ランサムウェアは、2013 年に初めて検出され、2020 年代に入ってからは、特定の個人や企業を狙い撃ちして、セキュリティ対策が甘い部分を狙い、執拗に攻撃する事例が増えています。

(2) 国内での Emotet の被害事例

ア　Emotet の感染による遠隔操作・情報漏えいやマルウェア送信などの攻撃

(ｱ) Emotet は、主に電子メールを介して感染する遠隔操作型のボットマルウェアであり、感染後は、情報漏えいやマルウェア・スパム送信などのさらなる攻撃に利用されたり、ランサムウェアなど他のマルウェアに感染したりすることが確認されています。

(ｲ) 従業員のなりすましメールによってコンピュータウイルスに感染

なりすましメールによって、コンピュータウイルス Emotet に感染した事例です。従業員がなりすましメールの添付ファイルを開いた結果、取引先に着信したことで感染が発覚しました。

イ　種類

コンピュータウイルス Emotet には、Trickster（別名「TrickLoader」および「TrickBot」）や Ryuk（別名「Cryptotrojan」またはランサムウェアとも呼ばれる暗号化トロイの木馬）などがあります。

ウ　特徴

(ｱ) Emotet 自体はランサムウエアではありませんが、Emotet によってランサムウエアがダウンロードされることがあるということです。

(ｲ) Emotet に感染すると、以下のような傾向が見られます 。

・メールに添付されたファイルの容量が増加する
・メールに添付されたファイル名がランダムな文字列に変更される
・メール本文に不自然な文章が含まれる

以上のような症状や特徴がある場合は、Emotet に感染している可能性があります。

(ｳ) Emotet は、2014 年に初めて検出され、2019 年には最も流行している脅威の 1 つとみなされたマルウェアです。

2021 年 1 月に一旦、下火になっていたが、2021 年 11 月から活動を再開したマルウェア「EMOTET」が、日本国内でも被害が拡大する状況となっています。

エ　感染経路

Emotet が不用意な添付ファイルの操作や不審な URL のクリックにより感染、悪意のある攻撃者によって送られる不正なメール（攻撃メール）から感染が拡大しているマルウェアです。

感染するとランサムウェアへの感染や重要な情報の窃取などの被害を受ける可能

性があることがわかっています。

Emotet に感染すると、感染端末から連絡先、氏名などの個人情報や ID、パスワードといった認証情報などが盗み出されることがあります。

また、Emotet のマルウェア媒介機能でランサムウェアに感染すると、端末の重要なファイルが暗号化され、攻撃者から復号化（元の状態に戻す）のための費用を請求されることがあります。

さらに、Emotet に感染したパソコンからメールの連絡先などの情報を窃取し、正規のやり取りを装って第三者へと攻撃メールを仕掛けることがあります。

Emotet に感染すると、マルウェアがダウンロードされ、主に以下のような被害をもたらします。

・パスワードやクレジットカード情報などの個人情報を盗まれる
・感染したコンピュータを制御・暗号化される
・他のマルウェアをダウンロードされる

オ　手順

ランサムウェアは、主に以下のような手順で発症します。

・メールに添付された Word 文書を開く。
・Word 文書内にあるマクロを有効化する。
・Emotet がダウンロードされ、感染が開始される。
・Emotet は、感染した端末から収集した情報を C&C サーバに送信し、その後、ランサムウェアやトロイの木馬などのマルウェアをダウンロードして感染を拡大することができます。

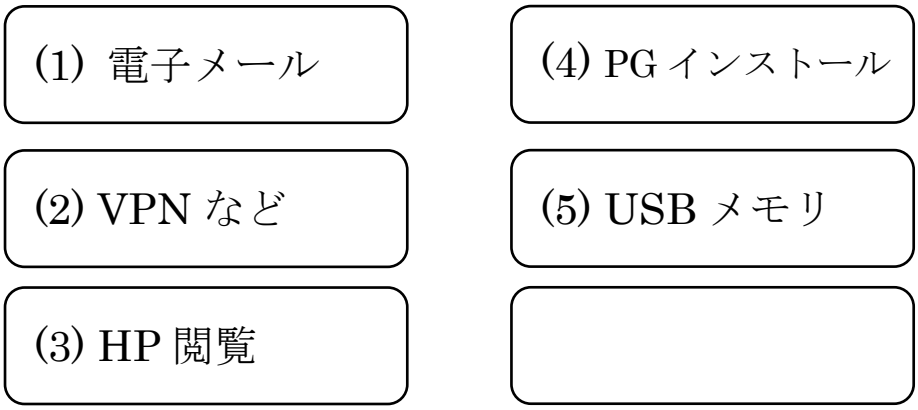
(3) 自社のホームページの不正な改ざん

コンピュータウイルスによってホームページのデザインが崩されたり、ウイルスを仕込まれたりした事例です。

2014 年には閲覧した人のコンピュータにウイルスが侵入したことで、大規模なネットバンキングの不正送金事件が発生したケースもありました。

３　コンピュータウイルスの感染経路について

コンピュータウイルスがどこから感染するのかを知っておくと、予防策を立てやすいです。ここではコンピュータウイルスの感染経路について解説します。



(1) 電子メールを開く

電子メールに添付されているウイルスファイルが原因で感染する経路は多いです。メッセージの URL をクリックすることによって、ウイルスが入り込むケースも増えてきました。

とくにメッセージが HTML 形式で書かれているタイプは、開くだけでウイルスに感染する可能性があるため注意が必要です。送り主に心当たりがない場合は、不用意に電子メールを開かないようにしましょう。

(2) VPN やリモートデスクトップのサービスの、脆弱性を利用し侵入を行います。

セキュリティパッチは可及的速やかに適用しなければなりません。

最新化できない場合は、接続しないことを至急検討する必要があります。情報漏えい・暗号化されてからでは遅いのです。

(3) ウイルスが仕込まれているホームページを閲覧する

動作・処理プログラムにウイルスが埋め込まれているホームページは、閲覧しただけで感染するリスクがあります。出会い系やアダルト系など、「人の興味引きやすいサイト」には注意しましょう。

また正規サイトが不法侵入を許し、そのままウイルスに仕込まれているケースも増えています。運営元の信頼性やセキュリティ意識もチェックしておくべきです。

(4) 怪しいプログラムをインストールする

開発元や配布元が曖昧なプログラムをインストールし、仕込まれていたコンピュータウイルスに汚染されるケースも増えています。

無料ダウンロードできるプログラムを安易にインストールしたり、突然表示される

「ウイルスに感染しています」という偽メッセージから偽のウイルスソフトへ誘導されたりなどの手口に気をつけましょう。

(5) 外部記憶媒体を PC とつなげる

外部記憶媒体にコンピュータウイルスが入っていた結果、PC が汚染される感染経路も存在します。USB メモリや CD-R、外付けハードディスクなどです。パソコンと接続しただけで感染する可能性があります。

マクロプログラムが実行される

ワード（Word）やエクセル（Excel）などの Office アプリケーションに登録できる「マクロ」を利用し、コンピュータウイルスを感染させるプログラムも存在します。コンピュータウイルスに感染している文書ファイルを開くだけで実行されるため、不用意な Office データのダウンロードは危険です。

職員の USB が感染経路になることもあるため、資料を扱わせる際はセキュリティがしっかりしている箇所で扱うことや､無料 Wi-Fi を利用しないなどの教育が必要です。

また他の対策として、「事前に決めておいた外部記憶媒体しか接続できないようルール化する」という方法も効果的です。仕事とプライベートの兼用 USB メモリや正体不明の CD-R などについては、そもそもパソコンへの接続を禁止することで、外部からのウイルス侵入を防げます。

４　コンピュータウイルスの感染予防

コンピュータウイルスのセキュリティ対策・予防策はどうすればいいでしょうか?

コンピュータウイルス侵入を防ぐには、まず「ウイルスを侵入させない」という基本的な部分が重要です。

(1)ルールの規定・改定	(5) 教育・研修
(2)不用意に電子メールを見たり、ダウンロードしない	(6) 定期的なホームページなどの脆弱性診断
(3) ウイルス対策機器・ソフト・認証を導入	(7) ログ管理
(4) OS やソフトウェアは常に最新の状態を維持	(8) 監査

(1) 情報セキュリティに係るルールを規定・改定する。

まずは、情報セキュリティポリシーを策定し、定期的に見直す。

(2) 不用意に電子メールを見たりソフトをダウンロードしたりしない

Emotet やトロイの木馬などのマルウェアの感染経路の多くは、電子メールや不審なホームページなどを経由してのルートが多数を占めます。

取引先や見知った人以外からのメールや、個人ブログの閲覧はむやみに行わないようにしましょう。ただし、なりすましメールの可能性もあるため、少しでも不審に感じたときは、送り主にメールを送ったかどうかの確認を行ってください。

(3) ウイルス対策機器・ソフト・電子証明書認証を導入する

ウイルス対策機器・ソフトを導入は必須です。

住民の個人情報、企業秘密などを守るためにも必ずインストールしてください。

ウイルス対策ソフトを選ぶときは、以下の要素を事前に検討しましょう。

・自社機器や OS に対応しているのか
・信頼性や実績がある機器・ソフトか
・メンテナンスやその他サポートを行ってくれる体制が整っているか　など

具体的な、対策については、入口、内部動作、出口のそれぞれに対して、以下のようなものをバランス良く組み合わせてください。

・FW
・UTM
・VPN
・EPP
・EDR、MDR
・ネットワーク監視（IDS、IPS）
・サンドボックス
・メール無害化（ぼてぃーろ）
・SASE（パブリッククラウド）

定期的にウイルス対策ソフトによるウイルススキャンを行ったり、月次レポートをチェックしたりなどの定期的な保守作業も重要です。

さらにウイルス対策ソフト自体も、定期的に最新バージョンへアップロードしておきます。古いバージョンのままでは、新ウイルスを始めとする進化した脅威から自社データを守れないかもしれません。

総務省が公表しているウイルスの被害事例にも、「ソフトはインストールしていたが、1 年前のバージョンだったため新ウイルスに対応できなかった」というケースが紹介されています。

導入しただけで安心するのは危険といえるでしょう。

新バージョンへの更新期間が来たら更新する、もしくは新しいセキュリティソフトに変更するなどの対応が必要です。

(4) OS やソフトウェアは常に最新の状態を維持しておく

Windows や Mac などの OS や、外部ソフトウェア・アプリなども、ウイルス対策ソフトと同じく常に最新の状態を維持しておきましょう。古いバージョンでは日々進化するウイルスに対して脆弱性が出るため、簡単に侵入を許してしまいます。最新アップデートはすぐに実行する意識が大切です。

(5) 従業員のセキュリティ教育・研修を進めておく

いくらウイルス対策ソフトや最新の OS・ソフトウェアをインストールしても、従業員のセキュリティ意識が低ければ簡単に侵入を許したり、外部から持ち込まれたりします。社内 OJT の実施やマニュアル作成などを通じて、従業員のセキュリティ教育・研修を進めるべきです。

また意図的にウイルスを持ち込む悪質な従業員がいる可能性もあります。不正をすぐ発見できたり、怪しい動きを察知したりするための能力も伸ばしておきましょう。

(6) 定期的なホームページなどの脆弱性診断を行う

ホームページやウェブアプリケーションは、インターネット上に公開されているため、様々な攻撃にさらされます。例えば、SQL インジェクションやクロスサイトスクリプティングなどの手法で、データベースやサーバに不正アクセスされたり、ユーザーの情報を盗まれたりする可能性があります。これらの攻撃を防ぐためには、定期的にホームページなどの脆弱性診断を行う必要があります。脆弱性診断とは、専門のツールやサービスを使って、ホームページなどに存在するセキュリティ上の問題点を発見し、改善することです。脆弱性診断を行うことで、攻撃者に先手を打ち、情報漏洩やサービス停止などの被害を防ぐことができます。

ツールを利用し、侵入テスト（ペネトレーションテスト）を行い、セキュリティホールを早期に発見し、速やかに改善しましょう。

(7) PC アクセスログ管理を行う

PC アクセスログとは、PC にログインしたり、ファイルやメールを操作したりした際に残る履歴のことです。PC アクセスログ管理とは、これらの履歴を適切に収集し、保存し、分析し、監査することです。PC アクセスログ管理を行うことで、PC の利用状況や異常な行動を把握し、不正利用や内部犯行などのリスクを低減することができます。また、万が一の事故や事件が発生した場合には、PC アクセスログを証拠として利用することもできます。PC アクセスログ管理を行うためには、PC に専用のソフトウェアをインストールしたり、ログファイルを定期的にバックアップしたりする必要があります。アクセスログは１年保持することが推奨されています。

(8) 情報セキュリティ監査を行う

情報セキュリティ監査とは、組織内の情報セキュリティに関する方針や規定、実施状況などを第三者的な視点から検証し、評価し、改善することです。

情報セキュリティ監査を行うことで、組織内の情報セキュリティレベルや問題点を客観的に把握し、適切な対策や改善策を提案することができます。また、情報セキュリティ監査を行うことで、組織外からの信頼性や信用性も高めることができます。

情報セキュリティ監査を行うためには、専門的な知識や技術を持った監査人員や外部機関に依頼したり、定期的に監査計画や監査報告書を作成したりする必要があります。

☕コーヒーブレイク　ちょっと一休み☕

法務省「通信履歴の電磁的記録の保全要請に関するQ＆A」

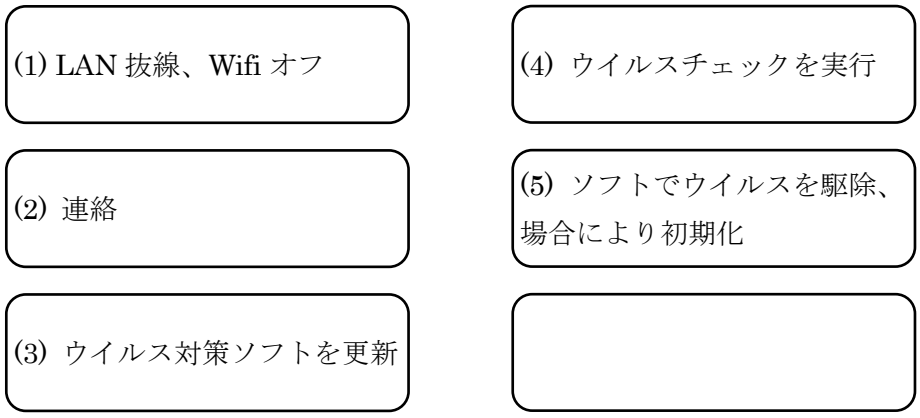
Q6 保全要請の期間として，90日も必要なのですか。

保全の期間の上限を90日間としたのは，サイバー犯罪に関する条約の規定に従ったものですが，実務的にもその程度の期間とする必要があります。現在においても，捜査機関は，通信履歴の電磁的記録に係る差押えを行うに際し，事前に通信プロバイダ等に連絡し，必要な通信履歴の電磁的記録について，差押え実施のための日程調整等を行うことがありますが，中には差押えの実施まで2か月程度かかることもあると承知しています。したがって，保全要請の期間の上限は90日間程度とする必要があるのです。

もっとも，この90日間というのは，あくまでも保全期間の上限であり，個々の保全要請の実施に当たっては，具体的事案に応じて，犯罪捜査に必要な適切な期間が定められるものと考えています。また，捜査機関は，保全期間内であっても，保全対象の電磁的記録に係る差押えが可能となれば，速やかに差押えを実施することになります。

５　コンピュータウイルスに感染したときの対処方法

コンピュータウイルスに感染したときの対処法として、以下の手順を行います。



(1) ネットワークを切断

コンピュータウイルスによる二次被害や新しいウイルスの流入を防ぐために、ただちにコンピュータをネットワークから切り離しましょう。物理的に LAN ケーブルを抜く、Wifi をオフにするなどです。また、USB や外付けハードディスクなどの外部記憶媒体を PC から取り外すことも忘れてはなりません。

(2) セキュリティ担当者へ報告

上司や、情報セキュリティ担当者へ速やかに連絡してください。

(3) ウイルス対策ソフトを更新

ウイルスパターンファイルは最新のものを利用してください。

(4)ウイルスチェックを実行

セキュリティソフトをインストールし、ウイルスの特定と駆除を行います。まずはウイルススキャンによって「どのウイルスに感染しているか」をチェックし、その後ウイルスに駆除プログラムを実行します。外部記憶媒体にもウイルスが感染していないか確認が必要です。

(5) ソフトでウイルスを駆除、場合により初期化

ウイルス駆除が終わった後は、「今後感染しないためにはどうすればよいのか」を庁内で検討し、セキュリティ対策の強化を図ることが大切になります。

どうしても駆除がうまくいかなかったときは、コンピュータの初期化（リカバリー）を行ってください。こうした事態に備え、常に日頃からバックアップを取っておくことをおすすめします。

コンピュータウイルスのセキュリティ対策は万全にしておこう！

コンピュータウイルスのセキュリティ対策は、自社情報だけでなく取引先・顧客の情報を守るためにも必ず講じるべきです。怠れば各方面からの信用失墜につながるでしょう。

６　まとめ

重要なポイントを以下にまとめました。

(1) 感染経路は電子メールやインターネットを介したものが多い
(2) ウイルス対策ソフト導入や社員教育の徹底がセキュリティ対策につながる
(3) VPN、外部デバイスの接続制限や OS・ウイルス対策ソフトの最新バージョンへの更新も予防効果がある
(4) 感染した場合はネットワークを切断し、ウイルス駆除を行う
(5) ウイルス対策ソフトの稼働状態・バージョン情報などを収集し、集中管理できる
(6) 定期的な PC 利用チェックや違反者への警告、不正 PC の隔離を行える
(7) PC 操作ログ管理によって「いつ」「どこで」「誰が」「何を」という情報を正確に把握できる、ふるまい検知を AI を活用して行う
(8) 指定したデバイス以外からの使用や書き込みの制限等ができる「外部デバイス制御」機能がある

☕コーヒーブレイク　ちょっと一休み☕

「P2P(ピアツーピア)ソフトウェア

Winny(ウイニー)は、P2P(ピアツーピア)ソフトウェアであり、ファイル共有ソフトウェアです。ウイルスではありませんが、情報セキュリティを考える上で重要な脅威です。。

通常は、ファイルサーバなどのファイル共有のサービスを利用し、ファイルのやり取りが行われますが、P2P ソフトウェアとは、不特定多数の端末がサーバを介さずに、端末同士で直接データファイルを共有することができるソフトウェアのことです。

作成者は、日本の大学教授です。 裁判については、教授が著作権法違反容疑で逮捕されたことがあります。また、Winnyの使用者に対しても、著作権法違反容疑で摘発された事例があります。

Winnyに類似するソフトウェアとしては、Share(シェア)、Perfect Dark(パーフェクトダーク)などがあります。