# モノづくり通信

Vol.72　2023 年 1 月発行

## 1．ごあいさつ

**新年あけましておめでとうございます。**

株式会社アイリンク　照井清一です。年末、年始、お店は買い物客で賑わっていました。親におねだりする子供も見ていてほほえましいです。世界には、今も極寒の塹壕で銃を構える兵士や、灼熱の太陽の下、お腹を空かせた子供がいます。

いつか誰もが笑顔で買い物に行く日が来ることを心から願っています。

## 1．ハッキングから会社を守る　～情報セキュリティ・個人情報保護法の課題～

日々の仕事になくてはならないコンピューター、それはサイバー空間における自分のオフィスです。このオフィスの戸締りと言えるのが情報セキュリティです。以前はコンピューターへの不正侵入は大企業に限られ「わが社は狙われることはない」と多くの中小企業は考えていました。しかし今はどの会社も不正侵入や情報漏洩のリスクにさらされています。「そのリスクとは何か」、「誰が狙うのか」、「どう対処すればいいのか」情報セキュリティについて考えました。

### 1）マルウェア感染のためトヨタの 14 工場が停止！！

トヨタ自動車は 2022 年 3 月 1 日の国内 14 工場の生産停止を決定しました。理由は協力会社　小島プレス工業のサーバーがウイルスに感染し部品供給のめどが立たなかったからです。原因は小島プレス工業の子会社の通信機器にウイルス(ランサムウェア)が侵入し、小島プレス工業のサーバーが多数感染したためでした。感染発覚後、トヨタは１００人態勢で応援しましたが、その週末には復旧できず、週明け 3 月 1 日の生産を中止しました。たった 1 台の機器の脆弱性のため、トヨタの受けた損害は数億円にもなりました。

### 2）ティーンエージャーがボーイング、連邦地方裁判所へ不正侵入

ティーンエージャーのハッカー、マットとコスタは、コンピューターから手当たり次第に電話をかけていて、偶然連邦地方裁判所のモデム番号を見つけました。そこに「トロイの木馬」というウイルスを送って、モデムに接続されているコンピューターの情報を引き出しました。その中にボーイングの情報もあり、彼らはボーイングのコンピューターにまで侵入しました。ある日ボーイングの情報システム担当者は、パスワードがクラック(解除)された痕を発見、それをたどった結果マットとコスタが連邦地方裁判所のコンピューターにまで侵入していたことが判明しました。ボーイングから連絡を受けた FBI は、電話番号を逆探知してマットとコスタの居場所を突き止め 2 人を逮捕しました。

## 2、攻撃者のタイプ

コンピューターに不正侵入する攻撃者には 3 つのタイプがあります。

① 政治的、経済的な利益を求め、特定の国や企業へのサイバー攻撃や身代金目的に攻撃する。

② 個人の利益のためにデータを盗む者。これは内部の犯行が大半を占めます。企業が所有する顧客リストは高く売れるからです。ベネッセから流出した顧客リストは複数の名簿事業者が購入、犯人は数百万円の利益を得ました。

③ マットとコスタのように、好奇心から不正侵入する愉快犯です。侵入自体が目的なので侵入が困難なほど挑戦意欲を掻き立てます。防御が難しくやっかいなのは実はこのタイプです。

では攻撃者はどのような攻撃手段を取るのでしょうか？

## 3、攻撃手段

**①　ランサムウェア**

ネットワークなどを通じ感染するマルウェア（悪意を持ったソフトウェア）の一種です。「ランサム」とは英語で「身代金」を意味します。これに感染するとコンピューターのファイルが暗号化されて復元できなくなったり、端末が起動不能または操作不能になったりします。

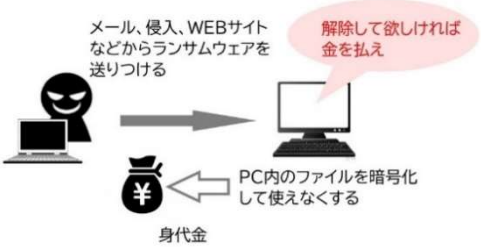


図 1　ランサムウェアの仕組み

**② 標的型攻撃メール**

一見顧客からのメールですが、添付ファイルにウイルスが仕込まれたり、URL をクリックすると問題のあるサイトに誘導されます。予め攻撃対象を特定して攻撃する方法です。

**③ SQL インジェクション攻撃**

ホームページのお問い合わせフォームなどデータベースへの入力欄に不正な SQL コマンド(データベース操作コマンド)を入力して、情報の搾取、改ざんや削除を行う攻撃です。

**④ ゼロデイ攻撃**

OS やアプリケーションなどのバグ(脆弱性)はメーカーによって随時発見され修正パッチが提供されます。ゼロデイ攻撃は、メーカーが修正パッチを提供してからユーザーがインストールする間に、その脆弱性を衝く攻撃方法です。

**⑤ パスワードのハッキング**

攻撃者は最初ネットワーク経由でどれかの端末(PC)に侵入します。その PC に PC 操作を盗み見るソフトを入れて今度はサーバーに接続するパスワードを盗みます。あるいはパスワードクラッキングツールで総当たり攻撃を行ってパスワードを解除します。こういったツールは闇サイト(ダークウェブ)で容易に入手できます。

**⑥ ソーシャルエンジニアリング**

社員を装ってネットワーク管理者に電話をかけパスワードを聞き出す、逆に管理者になりすまし直接利用者からパスワードを聞き出すなど、私立探偵などが使う情報収集の方法がソーシャルエンジニアリングです。

優れたハッカーでも全くヒントがなければ侵入は容易ではありません。元ハッカー　ケビン・ミトニックはこの手法で多くの企業や政府のシステムに不正侵入しました。他にも肩越しに覗き見するショルダーハッキングやオフィスが出したごみを調べるトラッシングもあります。ごみには管理者が書いたサーバーの設定情報を書かいたメモがあったりするからです。

## 4、企業が行うべき対策

侵入者から攻撃されるポイントは図 2 に示す 4 点です。これに対しどのような防御策があるのでしょうか?

(1) システムの脆弱性

どのシステムも脆弱性(バグ)はあります。ゼロデイ攻撃のリスクを減らすには修正パッチはすぐにインストールし、サポートの切れた製品は使用を中止します。

(2) ゲートウェイ

インターネットの入り口のゲートウェイではファイアウォールが不正アクセス(通信)を防ぎます。しかし不正なメール、WEB サイト、アプリケーションはファイアウォールでは防げないので WEB フィルタリングなどを導入します。これらを統合した UTM という機器もあります。

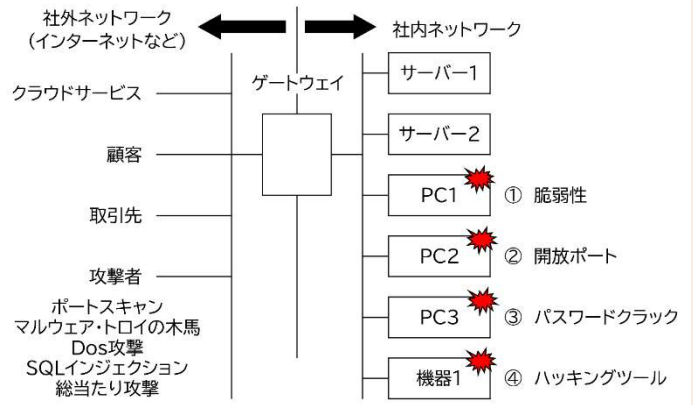


図 2　システムが攻撃を受けるポイント

(3) エンドポイント

使用していないネットワークのポートが開放されている、古いパソコンがネットワークに接続されている、これはハッカーから見ればオフィスの戸が開いているようなものです。ネットワークの開放ポート、古いパソコンや端末機器を点検し不要なものは撤去します。データのフォルダはアクセス権を設定し必要のない社員はアクセスできないようにします。

(4) クラウドサービスとテレワーク

使用するソフトウェアやクラウドサービスは会社が許可したものに限定し、クラウドサービスは https など暗号化通信のサービスを利用します。テレワークの場合、PC は支給し自宅の Wi-Fi は WPA や WPA2 など暗号化通信を使用します。

(5) 社員の教育

標的型攻撃メールを防ぐため不正なメールと正常なメールの違いや、不正なメールを開いてしまったときの対処方法を教育します。

(6) パスワード

総当たり時間は英字 4 桁なら 3 秒、英数字+記号　8 桁なら 1,000 年です。しかし英数字+記号の 8 桁は記憶できません。今やパスワードはログインするための「電子鍵」なのです。パスワードを書いたメモを壁に貼っておくのは誰でもカギを持ち出せるようなものです。パスワードの決め方や記憶以外の管理方法を決めます。

クラッキングされにくいパスワード

- 8 桁以上
- 英数字、特殊文字を混ぜる
- 容易に推測されない

参考　総当たり時間

英字 26 文字　4 桁　3 秒

英数字+記号　8 桁　1,000 年　(2015 年)

(7) シャドーIT・BYOD の問題

無料の IT ツールが豊富な今日、社員が独自に IT ツールを使用するのがシャドー IT です。会社のメールを個人の Gmail に転送すれば自分のスマートフォンで見られます。また外出先で個人のノート PC から会社のサーバーにアクセスすれば外出先でも仕事ができます。テレワークの普及もあり、こうした BYOD(Bring Your Own Device)は広まっています。しかし無料ツールはセキュリティのリスクがあります。実はゲームソフトはハッカーの格好の標的なのです。またスマートフォンや PC が外出先で紛失・盗難に遭えば情報漏洩のリスクがあります。

できれば業務で使用するパソコンやスマートフォンは会社が支給します。私的利用は禁止し、使用するソフトウェアやクラウドサービスは安全性を確認したものに限定します。

図 3　IT ツールは便利だが、危険性も知っておく必要がある

情報セキュリティの詳細は IPA(独立行政法人情報処理推進機構)のホームページにあります。テレワークやウェブ会議を使用する際のセキュリティについても書かれていますので、ぜひ活用してください。

## 5. 何を守らなければならないのか？　知っておくべき法規制

情報セキュリティで守らなければならない情報にはどのようなものがあるのでしょうか？個人情報と営業秘密について取り上げました。

### 個人情報保護法　管理が必要なのは個人データ

個人情報とは氏名、生年月日、住所、顔写真など特定の個人を識別できる情報のことです。

生年月日や電話番号だけでは特定の個人を識別できませんが、氏名と組み合わせると特定の個人を識別できるので個人情報になります。**個人情報は安全管理の義務はありません。**

個人データとは、個人情報を分類、整理して検索できるようにしたものです。顧客が記入したアンケートは個人情報で、アンケートを表にしたりエクセルに入力したものは個人データです。**個人データは保管や漏洩防止などの安全管理が必要です。**

具体的な方法は「個人情報保護法ガイドライン」「8（別添）講ずべき安全管理措置の内容」にあります。ただし中小事業者(従業員 100 人以下)には、上記の要求は困難なので必要な最低限の措置が別に示されています。

### 不正競争防止法

企業が持つ情報の中で「不正競争防止法」で保護の対象となるのは「営業秘密」です。社員が営業秘密を持ち出せば、刑事罰や損害賠償の請求があります。営業秘密は以下の 3 つを満たす必要があります。

1. 秘密管理性
   その情報が秘密として適切に管理されている。
2. 有用性
   製品やサービスの生産・販売・研究開発に役立つ、事業者にとって有用な情報である。
3. 非公知性
   一般的に入手が困難で、公然とは知られていない。

営業秘密漏洩の多くは社員の故意によるものです。まずは、どれが営業秘密に当たるのか決めて、取扱いに注意することや故意に持ち出せばどうなるのかということを、社員に教育します。

## 6. 絶対安全はない　～攻撃を前提として考える時代～

今や完全なセキュリティは存在しません。情報漏洩や不正侵入はいつ起きてもおかしくありません。いつか起きるという前提で様々な対策を行います。さらに「情報セキュリティ事故」が起きた時にどうするかも事前に決めておきます。

情報漏洩やマルウェア感染など情報セキュリティ事故が起きた場合、社内の報告や対処、時には顧客へ報告も必要です。あるいはマルウェア感染の疑いがあるけど確証がない場合、どうするかを決めておかないと何もせずに危険な状態が放置されてしまいます。これからは「起きる」ことを前提に取り組む時代なのです。

ハッカーの座右の銘「我々に見つけられないセキュリティの穴はない」

## 7、温故知新「徳川十六神将　鬼の作左の「正しきこと」に貫いた信念」

「一筆啓上、火の用心、お仙泣かすな、馬肥やせ」

日本一短い手紙と言われた文を書いたのが、徳川家康の家臣　本多作左衛門(重次)、通称「鬼の作左」です。

家康の家臣団も二つ割れ家康が窮地に陥った三河一向一揆では、作左衛門は迷わず改宗し家康の側につきました。そして歯向かう者は容赦なく切り捨てました。三方ヶ原の戦いでは敗走する家康のしんがりを務め、数十人の敵に囲まれた時は敵の騎馬武者の槍を握って落馬させ、その馬を奪って逃走しました。体は傷だらけ、片目、片足、指が欠けところから、人は「鬼の作左」と呼びました。その一方三河三奉行に登用された時は、情実によらず理路正しく沙汰を告げたため人々は驚きました。

家康が武田を破り、信州から駿河まで手にした頃です。安倍川で家康の目にとまったのは赤錆びた鉄の大釜。信玄の置き土産の罪人を焼き殺す煎人釜、直径 152cm、深さ 140cm もありました。吝嗇家の家康は「浜松へ運べ」とその場にいた奉行に命じました。

翌朝、釜が川原から運び出される時、本多作左衛門が通りがかりました。彼は「家康の命令であろうとかまわん、その釜を砕け」と奉行に命じました。


図 4　本多作左衛門誕生の石碑

彼は作左衛門の勢いにのまれ、釜を粉々に砕きました。作左衛門は奉行に「家康の前でこう申せ」と耳打ちしました。

翌日、作左衛門は家康の前に呼ばれます。彼はこう答えました。

「釜で煎り殺すような罪人が出来るようでは、天下国家を治めることは成り申さず。」

天下を治める理念とはそういうものとは違うと、作左衛門は家康に重いテーマをつきつけたのです。結果、作左衛門は「お咎めなし」。

しかし晩年は秀吉の怒りを買い、上総国（千葉県）に蟄居（一定の場所から出ない謹慎）を家康に命じられます。原因は、家康が秀吉の元へ上洛した際、代わりに送られた秀吉の母「大政所」の屋敷の周りに薪を積み上げたことで、秀吉の怒りをかったからです。作左衛門は家康にもしものことがあれば即座に「大政所」を焼き殺す腹でした。

寂しい晩年を送ったと言われますが、本当は「自分が正しいと思うことを貫き通したこと」に満足していたのではないでしょうか。

1 月から始まる「どうする家康」にもそんな一刻者が出てくるかもしれません。


図 5　碑のある犬頭神社

## 8. 未来戦略ワークショップ「なぜ社員は不正をするのか？自動車メーカーの不祥事を考える」

技術の進歩や経営事例を学び未来の戦略のヒントにする勉強会「未来戦略ワークショップ」次回は 1 月 22 日に「なぜ社員は不正をするのか？自動車メーカーの不祥事を考える」です。どなたでも参加できます。
（お申し込みはこちらから　https://ilink-corp.co.jp/1669.html）

## 9. 「中小製造業の値上げと価格交渉のポイント」

「値上げに対し取引先は何を心配しているのか」「値上げを受け入れてもらうにはどうすればいいのか」、かつて設計で買う立場だった経験が役立てばと思い値上げと価格交渉のポイントをまとめました。以下から誰でもダウンロードできます。
https://ilink-corp.co.jp/8192.html

## 10. 編集後記

作左衛門の石碑は、私の住む愛知県岡崎市宮地町にあるものです。この石碑は子供のころから見ていましたが、本多作左衛門を知ったのは最近です。それもあって町内には本多さんがとても多いです。

感想がありましたらぜひお聞かせください。また本ニュースレターが不要な方はお手数ですが、下記通信欄に、お名前又は社名と「不要」とご記入の上、FAX して頂くか、メールにて不要とお知らせください。

株式会社アイリンク　代表取締役　照井清一
〒444-0835　愛知県岡崎市城南町２丁目１３－４
TEL 0564-55-5661 / 0564-77-6810　FAX 0564-77-8203
URL http://ilink-corp.co.jp　メルマガ http://ilink-orp.co.jp/malmag.html
E-mail terui@ilink-corp.co.jp　https://www.facebook.com/se.terui
【通信欄】