セキュリティ教育が必要な理由　①

2018 年 5 月 30 日作成

近年情報の管理が問題となり、「セキュリティ教育」の必要性が語られる事が多くなっています。各国の対応もあり、会社、学校、地域等にて問題が話題となり、恐怖さえも感じている方も居られるのではないでしょうか。

特に、５月２５日に開始となった「GDPR」に至っては個人情報管理に違反すると「２０００万ユーロ（日本円１９億円弱）又は前年度世界での売り上げの４％」が制裁金で請求される可能性があります。そして、違反は摘発する側が違反を証明する方法から、指摘された側が違反をしていない事を証明する方法へと変化しています。この欧州での考え方は世界各国での変化へと繋がっていく可能性があります。

その様な状況にも関わらず、「何が問題となっている」、「何を知る必要がある」、「何を考えて行動する必要がある」が明確では無いと感じています。貴方はどの様に感じて居られるでしょうか。

今現在、正解は在りません。河の流れに乗って動いている船の様に環境は変化しているので、対応や対策は柔軟に行う必要があります。従って、基本を定義する事は非常に難しく、確定した先から変更が必要になっている状況です。

その様な状況だからこそ、変化が激しく、早く、深刻であるからこそ「セキュリティ教育が必要な理由」を明確にして、「考え方の基本」を明らかにして行く必要があるではないかと思って居ります。

記載の流れとしては、基本的に３文書で記載させて頂きます。

・「現在の状況概要とセキュリティが必要になった軌跡」に関する記載
・「現在のリスクの概要と対策」に関する記載
・「情報セキュリティに関する思考と重要性」に関する記載

賛否両論や見解の相違が多い事は重々承知しております。その上で、記載させて頂きたいと思っております。ご意見等頂ければ幸いです。

ＳWM　（Support to Worlds Member）
《夢ある明日を貴方と共に》
情報作成／システム教育サポート
代表　石川光信

Tel/FAX: 042-422-0593
Mail：mishikawa@wswm.jp
https://www.wswm.jp

「現在の状況とセキュリティが必要になった軌跡」

先ず初めに、現状での規制等に関する事と、情報セキュリティの変化に関して記載させて頂きたいと思います。理由は、皆さんに「規制や法務」の頼りない状況と「何故騒がれている状況になっているのか」を理解して頂きたいと思うからです。

今に至る変化について知って頂いた後に、現状での「必要性」と「思考方法」へと話を移っていきたいと思います。

現在、私共が考えているセキュリティ対応で心がけて欲しい事は、下記の３点です。

・自ら状況判断が出来る、知識と思考力を持つ。
・想像力と思考力を活かした、状況判断力を持つ。
・自分の対応可能範囲を把握して、上級専門者と協力した対応力を持つ。

出来る範囲で結構ですので、上記の３要素の向上を目指して頂きたいと思います。

１）日本の法律から見た、情報セキュリティ

先ずは、皆様に関連する可能性がある日本における法律を見てみましょう。

情報管理で、最初に思いだす法律としては「**個人情報保護法**」として知られる、「個人情報の保護に関する法律」ではないでしょうか。「生存する個人を特定し得る情報」を保護し、特定される個人の権利や利益を保護する為に、本人の許可なしに提示及び利用が禁止されている法律になります。

情報漏洩で問題となる多くは、この個人情報の漏えいになります。従って、５月２５日に開始された「GDPR(Genera Data Protection Regulation)」でも個人データに関する管理の法律です。その理由は関係する人数が桁違いに多く、国や組織への影響も大きいからです。

一度の漏えいで数十万人規模以上の漏えいが多く、Facebook に至っては、５，０００万人分以上の情報が漏えいしていました。もし、情報漏洩により慰謝料として一人に１万円払う事になったとしたら、数十万人で数十億円以上、５，０００万人だと５、０００億円以上の損失になります。従って、GDPR の制裁金１９億円弱も理解出来る部分もあるわけです。

会社の信用損失に伴う売り上げ低下、顧客損失だけでなく、社員の給与、昇給、賞与にもひびき、最悪倒産する事もありえるのです。個人情報を大量に保持運用している企業が重点を置くのは理解頂けるかと思います。

次に業務で関連する法律としては、金融関連企業や経理担当が関係する事が多い「**電子機器使用詐欺罪**」に関係する可能性があります。電子情報を操作して詐欺をおこなう犯罪です。

多くの方は自分には関係ないと思われるでしょう。しかしながら、この犯罪と関係する事が多い「**不正アクセス禁止法**」に関連して犯罪者の一員となってしまう事があります。

何かの機会で知った、担当者のユーザ ID やパスワードを用いてシステムの操作実施、又は情報を伝達する事で、犯罪者の一員になる可能性があるのです。懲戒解雇だけに留まらず、刑法として罰則は１年以下の懲役または 50 万円以下の罰金を科される犯罪であり、その上民事で賠償請求や慰謝料請求が加わる事が殆どです。

その他としては、商品や自社を売り込みたいが為に「名刺交換した先」、「取引がある顧客先」、「宛先が公になっている先」以外の人達に許可なくメールを送ると「**特定電子メール法**」の違反者になってしまいます。特に営業関連の方は気を付けて下さい。

セキュリティ担当者や業界・業種によっては他にも存在します。個別業務以外で、一般的に気を付けないとならない法律は上記の４つが主です。但し、日々新たな法律や規則等が作成されていますので、気を付けて下さい。例えば、６月１日に施行される割賦販売法（割販法）改正版への対応などは大変だと思います。

従って、社内での個人的なセキュリティ保護の多くは、上記の様な法律違反が発生しない事を目的に実施されます。その他は、業務の停止、業務の継続困難、業務情報漏洩に対する対応になります。こちらの要因や対策は、次のレポートである「現在のリスクの概要と対策」で説明させて頂きたいと思います。

多くの法律は、事件が発生してから後追いで作られているのが現状です。将に犯罪者との知恵比べを行っている状況です。どうしてそうなってしまったのか？次に記載させて頂く現状までの軌跡を読んで頂ければ多少はご理解いただけるかと思います。

２）情報管理の経過から見た、情報セキュリティ

コンピュータが開発される前でも情報管理は必要でした。例えば、「富山の薬売り」で有名な方々は、前任者から受け継いだ顧客と自分で繋がりを持った顧客の情報を頼りに年間を通じて行商を行っていました。顧客の情報を守る事は、以前から重要な事だったのです。

江戸時代から現在まで顧客の情報、取引先の情報、業界の情報は常に必要な情報です。必要な事は変わっていないのに、なぜ今問題とされているのでしょうか。違いは二つあると思われます。ひとつ目は、以前は自分の情報を持っている人が判っていました。富山の薬売りの場合、顧客もどの薬売りが自分の情報を持っているか知っていたので、その方から購入をする事や追加の情報を提供する事に不安がなかったのです。残るひとつは、電子情報ではない事です。盗もうとしたら記載文書を盗むか書き写す必要がありました。情報入手の困難さ、要する時間、取得に必要な費用も全く異なると共に、拡散のスピードも遅かったのです。

従って、苦労して盗む事によって得る利益と、犯罪が露見するリスクの差が大きかったと思われます。

ところが、情報が電子化された途端変わりました。以下に現在までの経過と現状の要因と思われる事項について、私共なりの見解を記載させて頂きます。

２－１）パソコン、ミニコンの普及による状況変化

情報が電子化したとしても、汎用コンピュータ（メインフレーム）が主体の時代では、印刷物にするか、写真で撮らないと情報を盗み出す事が殆ど出来ませんでした。

理由は２つあります。一つ目は、電子情報として取り出し盗み出しても、読み込むには高価な同じ汎用コンピュータが必要だった事です。今の金額で億単位の価値があった電子計算機を用意するだけでも費用が掛かりますし、台数も限られていました。残る一つは、汎用コンピュータは、特別な冷暖房完備の部屋に設定され施錠され管理人が昼夜いる状態です。その状態で、電子情報のまま持ち出すとしたら数十センチもある大きなテープに書き込んで盗か、速度の遅いプリンター（今なら数分で打ち出せる量を一日がかりでした。）で A3 サイズを超える用紙に打ち出した大量の印刷物を持ち出す必要がありました。従って、隠れて持ち出すのは美術館から美術品を盗み出す程度に難しかったのです。

そして、汎用コンピュータ（メインフレーム）が主体の頃は、機械メーカによって書込みコードに不統一な部分がありました。データは、同じメーカの機械で処理する事が多かったのです。

この時期の情報セキュリティは、殆ど汎用コンピュータが設置してある電算室内の管理が中心でした。その室内で処理される記憶メディア、端末、印刷物、人員の管理が主です。

ところが、パーソナルコンピュータ（パソコン：Windows やアップル OS 搭載）やミニコン（Unix 又は独自の OS を搭載）が普及すると共に、標準の文字コード等が定義され出します。定義された同じコードで書き込まれる様になっただけでなく、電子情報の記憶媒体（テープメディア、フロッピーディスク、ハードディスク等）の性能も向上しました。

つまり、安い金額の高性能で小さなメディアに、他の計算機でも読める文字コードで書き込める様に成ったのです。担当者の端末で情報を抜き取り、書き込んだフロッピーディスクを、スーツのポケットに入れて持ち出す事も可能になりました。

電気計算機の値段も数億円する機械しかなかったのが、数百万で買える機械が売られようになりました。そして、直ぐに数十万で買えるようになっていったのです。

従って、盗んだ情報を自宅や事務所にあるパソコンやミニコン（今のサーバにあたります。）で読み込み、複製し、印刷する事も可能になったのがこの時代です。

また、この時代には現在も皆さんが使用している、コピー機や FAX 機器が一般化していきました。印刷物をコピーしたり、事務所の FAX 機器で送ったり出来る様になったのです。

この時代の情報管理は、対象が計算機室から電子計算機（パソコンやサーバ、ミニコン）の使用している場所全てへと変化しました。

その結果、この時期より社員教育の必要性が語られる様になります。しかしながら、未だ全員にパソコンが普及していません。社内一部のメンバーへ向けた運用規則、情報管理規則を厳守させるに留まっていた状況でした。

２－２）インターネット開始による状況変化

企業内にて複数の PC(パーソナルコンピュータ)、Unix やマイクロソフト OS 搭載のサーバ、汎用機の端末等が複数台使われる様になった事によって、コンピュータ同士を繋ぎ通信する必要が出てきました。今も使用している LAN（ローカルエリアネットワーク）にあたるものです。

まだこの時点では企業の外部へデータ通信は実施していなかった為、企業内での情報管理を厳密に行っていれば殆ど問題はありませんでした。ところが、電子メールが発達し、インターネットが普及すると共に事態は急転します。自分達の管理出来ないサーバやネットワークを介して情報が伝達されるからです。自分達とは関係のない人々が情報を操作出来るし、情報を送って来られる状況になりました。

その事によって、自分たちの環境に入り込める隙が生まれてしまったのです。各組織や企業での情報管理を考えただけでは済まなくなってしまいました。

例えて言うなら、草原に一軒家を建てて住んでいたつもりが、高層ビルの立ち並ぶ都市部のビル内に取り込まれてしまった状態へと変化してしまった感じです。入口も一緒、隣に住む人も知らない、水道、ガス、電気、電話線などが共同で使用する環境の中で暮らす様になったのと同じなのです。

この時点で法律や社会制度が情報化のスピードに追い付かなくなったと感じています。将に「**情報システムを使っていた時代から、情報システムに使われてしまう時代**」になってしまったのです。犯罪が横行し問題が多発し、事後ルールや法律で規制するしかない時代になってしまいました。それは現在まで続いていると感じています。

２－３）　現在の状況

現在は、インターネットが先進国を中心に広がり、一部の地域を除く世界各国へと広がっています。世界各国に広がった結果、情報処理の完成度が新たな世界の政治・国際問題と経済格差による問題を、生み出す様になりました。

先ずは政治・国際的な問題とし、情報戦略が第５軍の軍隊組織になってしまった事です。軍隊と言うと日本での自衛隊組織にあたる陸軍、海軍、空軍が有名ですが、現在はこれら３軍に加えて、**宇宙軍**と**情報軍**の５軍となっています。

ご存知の様に、コンピュータ自体が軍用向けに開発されたものなので、驚く事ではないと思われる方も多いのではないでしょうか。米国が弾道計算の為に開発、英国が暗号解読の為に開発したのが始まりです。

情報を盗み、改変、削除、拡散し、システムを崩壊させる事によって敵国の動きを停止させ壊滅する事も出来るのが現状となっています。将に、平和利用でダイナマイトを作ったら、その応用で戦争が激化してしまった様なものですね。

もう一つの問題は、経済格差に関連した問題です。ここには２つの側面あると思われます。一つ目は、情報格差またはデジタル・ディバイド（ digital divide）などから、経済格差が

広がっている状況です。ＩＴ技術の不足により、教育や生産、商業、金融の格差の広がりが進み、その影響が収入の格差拡大へと繋がっています。将に、戦時中において最新兵器開発や使用技術のない国が、高価な戦闘兵器と技術者を多大なる負債を抱えて用意しないと自国を守れない状態と同じなのです。ＩＴ化を推進する必要から個人の収入も問題ですが、地域や国の負担も多大になっているのが現状です。

そしてもう一つが、経済格差によってＩＴ技術の価値が一定にならない事です。有名な話として、マルウエアの一つとしてＤＤｏＳ攻撃（ターゲットのサイトに大量のアクセスを行い、業務で必要な送受信や処理が出来なくしてしまう攻撃です。）を行うソフトがブラックマーケット（情報処理関連では、「アンダーグラウンドサービス」と明記する場合が多いです。）にて数百円で売られています。

ＤＤｏＳ攻撃を受けてしまい回避できなければ、業務が停止して顧客や取引先を失う場合もあります。そして、売上の損失に留まらず企業の信用も失う事も多いのです。

攻撃を受けた先での損失は、数百万から数千万になる可能性もあるのですが、実行するためのソフトは数百円で買えてしまう場合があるのが現状です。

経済格差の問題で、作る側からすれば数百円でも開発する価値があるのです。自分たちの知恵と知識を集めて生活をかけて命がけで開発して来ます。リスクがあり犯罪と知っていても、今日生きる為に必死で行います。

この状況を知った時、中南米にて中学生ぐらいの少女が生活の為に避妊なしに日々売春をしていて、インタビューを受けている画像を思い出しました。エイズになる危険性に対して、彼女は次の様に答えていたのです。「エイズは確かに怖いです。でもエイズになっても今日死ぬことはありません。しかし、私がお金を持って帰らなければ家族は今日食べるものが無いのです。」格差が追い込む現状を表していると思いませんか。

この様な状況ですから、守る側も攻める側との知恵比べ、想像力比べになっているのが現状なのです。ある国のＩＴ攻撃部隊は数万人以上いると言われています。一人一人が戦士の気持ちで対応が必要になってしまった事に対して、個人的には悲しく思っています。

悲しんでばかりも居られませんので、では現在の状況の中でどの様な知識や対応が必要になっているのでしょうか。私共としては、下記の事項を心がけて頂きたいと思っております。

・電子情報のみではなく、二次的な情報で確認する様にする。
・外部からの情報を信用して、早急な行動を行わないようにする。
・自分の感性を敏感にし、想像力を働かせ、少しでも疑問があったら確認を実施する。
・人的な直接のコミュニケーションを重視して、自分一人で総てを判断しない様にする。
・セキュリティ管理は、前例が必ずしも正しく無いと考える様にする。
・最善を尽くし、最新の情報を把握している人・組織の知恵を活かす様にする。
・初期判断を行う為、基本知識を磨く様にする。

難しい様に思われるかも知れませんが、基本的な考え方を身に着ける様にして頂ければ、或る程度のリスクを減らす事は可能です。０％にする事は不可能としても、少なくした上で「最悪を想定し最善を尽くす」のが基本だと考えて頂きたいと思います。

以上で、「現在の状況概要とセキュリティが必要になった軌跡」編は終了したいと思います。賛否両論や見解の相違が多い事は重々承知で、記載させて頂いております。
ご意見等頂ければ幸いです。

ＳWM　（Support to Worlds Member）
《夢ある明日を貴方と共に》
情報作成／システム教育サポート
代表　石川光信

Tel/FAX: 042-422-0593
Mail：mishikawa@wswm.jp
https://www.wswm.jp