セキュリティ教育が必要な理由　②

2018 年 5 月 31 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

今回は、２文書目として、「現在のリスクの概要と対策」に関して記載させて頂きます。

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

「現在のリスクの概要と対策」

先の文書「現在の状況概要とセキュリティが必要になった軌跡」を一読頂けた方には、困った状態になっている事を理解頂けたのではないかと思います。

二文書目のこの文書では、現在の状況で特に問題となっているリスクの内容と対応に関して記載させて頂きたいと思って居ります。

記載の多くは、IPA 独立法人情報処理推進機構 様からの発表内容を使用させて頂いております。（IPA ホームページ：https://www.ipa.go.jp/index.html ）従いまして、IPA 独立法人情報処理推進機構 様のサイトもご参照頂ければと思います。

今回の記載では、皆様に判り易く伝えさせて頂きたいとの思いから、イメージを持って頂く事と概要を掴んで頂く事を目的としている為、技術的な部分は可能な範囲で省かせて頂きたいと思っています。

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）今年の１０大脅威に関する状況

IPA 情報処理推進機構様より、２０１８年の脅威となる１０リスクに関して今年初めに発表がありました。理解の助けとなる図も含めた内容が先月提示されたので、弊社のサイトにて確認出来る様にしています。ご参照下さい。
（https://www.wswm.jp/news/IPA_2018TenRiskV3.pdf）

２０１７年から比較して、下記の３点に関するリスクが増加しています。

・ビジネスメール詐欺による被害
・脆弱性対策情報の公開に伴う悪用増加
・脅威に対応する、セキュリティ人材の不足

上記３点は２０１７年まで１０大脅威にまでは含まれていませんでした。しかしながら、これらの脅威は欧米では決して低いリスクの項目ではありません。或る意味で「日本も狙われ出した！」と言えるのだと思います。日本語への対応や日本文化の研究が進むと共に、日本の企業でのセキュリティ環境が進んで来たのだと感じています。

私共の見解としては、日本国内での情報セキュリティ強化が進んでいる事もあり、２大脅威である「標的型攻撃による被害」と「ランサムウェアによる被害」に関係して上記の３リスクが増大したのだと思っています。

環境強化が進んだ結果、簡単には詐欺や脅しが出来なくなりました。そこで、脆弱性対策が未完な時点での攻撃や、手間が掛かるがターゲット企業への周到なる調査を実施した上で、

人的コミュニケーションを取り入れた攻撃が浮上して来たのだと思います。

次に、個人向けの 10 大脅威では「インターネットでの詐欺」や「ネット上の誹謗・中傷」が増加しています。こちらは、スマートフォンの普及もありネット上での記載情報が個人に影響する度合いが増加して来ている事が原因だと思われます。将に個人的にもネット上の情報に振り回される様になり、情報の精査や管理が行き届かない状態に成って来ています。

スマートフォンの便利さは宣伝されていますが、特に学生や主婦、退職者へのリスク、脅威、そしてセキュリティの低さは伝達されていません。組織での使用と同様に、知識と対応の伝達なしに使用させるのは危険極まりない状況と成って来ています。各メーカーも最大限の努力は行って居られるのでしょうが、機器の管理機能が PC 等とは異なるので、難しいのだと思います。

「個人」関する対応は、提供側の対応が重要である為、この文書では「組織」の１０大脅威を中心に記載させて頂きます。

■「情報セキュリティ 10 大脅威 2018」　　NEW：初めてランクインした脅威

昨年順位	「個人」の 10 大脅威	順位	「組織」の 10 大脅威	昨年順位
1 位	インターネットバンキングやクレジットカード情報の不正利用	1 位	標的型攻撃による情報流出	1 位
2 位	ランサムウェアによる被害	2 位	ランサムウェアによる被害	2 位
7 位	ネット上の誹謗・中傷	3 位	ビジネスメール詐欺 NEW	ランク外
3 位	スマートフォンやスマートフォンアプリを狙った攻撃の可能性	4 位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	ランク外
4 位	ウェブサービスへの不正ログイン	5 位	セキュリティ人材の不足 NEW	ランク外
6 位	ウェブサービスからの個人情報の窃取	6 位	ウェブサービスからの個人情報の窃取	3 位
5 位	情報モラル不足に伴う犯罪の低年齢化	7 位	IoT 機器の脆弱性の顕在化	8 位
8 位	ワンクリック請求等の不当請求	8 位	内部不正による情報漏えい	5 位
10 位	IoT 機器の不適切管理	9 位	サービス妨害攻撃によるサービスの停止	4 位
ランク外	偽警告 NEW	10 位	犯罪のビジネス化（アンダーグラウンドサービス）	9 位

（2018 年 1 月 30 日、IPA　情報処理機構発表内容より）

２）組織における情報リスクと対策について

組織でのリスクに対する対策を、上記の１０大脅威中心に考えてみたいと思います。

組織に対するリスクは、ほぼ下記４つに分類出来ます。そこで、其々のリスクに関して考えてみたいと思います。

- **【情報漏洩】　　組織が保有している情報を抜き取る事が目的**
- **【金銭取得】　　組織から金銭を搾取する事が目的**
- **【業務妨害】　　業務妨害により、他組織が利益を得ることが目的**
- **【対応人員不足】　　対応準備が困難な事によるリスクの拡大**

２－１）「情報漏洩」に関する対策について

「情報漏洩」に対するリスクは、１０大脅威の下記３つに関連すると思われます。

第１位　　標的型攻撃による情報流出
第６位　　ウェーブサービスからの個人情報の搾取
第８位　　内部不正による情報漏えい

上記の脅威に対する対策は２つに分かれます。１つ目は、コミュニケーションと情報共有を向上させる事です。そしてもう１つが、情報の管理方法の向上です。

「標的型攻撃による情報流出」に関しては、両方が必要になります。情報流出は、人為的なコミュケーション、電話やメール等で発生する場合が意外と多いのです。この場合、相手先や他の社員、部署との情報共有で回避出来る場合が多いです。

しかしながら、標的型攻撃の場合には、数カ月以上もかけ、取引先や顧客に開放したユーザ ID やパスワード等の取得から行う場合があります。実際、取引先へ開放していたシステムへのログイン ID を使って情報流失された例もあります。取引先でのシステム管理、情報管理も確認が必要です。

「ウェーブサービスからの個人情報の搾取」に関しては、情報の管理方法の向上による対策が必要になります。主には二つの対策が必要になります。１つ目は個人情報をデータベースから抜き出す時に、不要な情報が抜き出せない様にする事です。データベースから抜き出す事が困難であれば、搾取される可能性は低くなります。

もう１つが、情報の提供及び情報の変更を行う時の、実施方法や手順へのセキュリティ強化を行う事です。例えば、一定以上の情報量の提供には許可が必要とする。管理者の情報変更は別手順で定期的に提供（PC とスマートフォンの情報を合わせないと不可等）する。などにする事で、搾取される可能性や情報量を低く出来る場合があります。

「内部不正による情報漏えい」に関しては、多くの管理者が対策を悩む事が多いと思います。ご存知かも知れませんが、「不正のトライアングル」３つの要因が揃うと犯罪が行われると言われています。「動機」「機会」「正当化」です。例えば、個人的な金銭問題の「動機」、チェックが出来ていない状況による「機会」、上司も不正を行っている等の「正当化」です。

「不正のトライアングル」が揃わない様にするには、組織内でのコミュニケーションの向

上と、お互いの友好関係による情報共有が主になると思われます。米国等の様な監視体制ではなく、「不正のトライアングル」が揃わない様に、友好と情報システムの向上に努めていく事が、日本的で良いのだと思っています。

２－２）「金銭搾取」に関する対策について

「金銭搾取」に対する脅威は、１０大脅威の内で下記３つに関連すると思われます。

第２位　　ランサムウェアによる被害
第３位　　ビジネスメール詐欺
第１０位　　犯罪のビジネス化（アンダーグラウンドサービス）

上記の脅威に対する対策は、２つに分かれます。１つ目は、コミュニケーションと情報共有を向上させる事です。そして、もう１つが、発生した障害の拡大をさせない環境の構築です。

「ランサムウェアによる被害」に関しては、主に発生した障害の拡大をさせない環境の構築を実施する対応になります。発生する事を抑える対策は明確にはなっていないのが現状です。発生の抑制に関しては、「情報漏洩」に対する対策とほぼ同じ対策を行う事が基本になると思います。発生したら戻せる環境まで戻す事が基本の対策です。従って、戻せる環境を保持する様にすることが重要になります。

この脅威は、２０１７年に「WannaCry（ワナクライ）」が猛威を振るったので浮上したのだと思います。バックアップ用のディスクをネットワークに接続した状態に保ってしまい、バックアップ用ディスクも暗号化された組織もありました。注意が必要です。

しかしながら、「ランサムウェア」に対する対策は、システムの再構築が出来る為のバックアップやシステム切り替えが出来る環境を整える事です。最近では、証拠隠滅の為に実行された可能性が、問われています。

「ビジネスメール詐欺」に関しては、対策としてコミュニケーションと情報共有を向上させる事となります。２０１７年１２月に日本でも JAL が３億８千万円だましとられて話題になりました。日経の調査結果では、大企業の６割で詐欺メールを受け取り、１割弱が振り込んでいるとの結果が出ています。攻撃側は、送信元のメールアドレスを偽装したり、もっともらしい理由をつけてフリーメールで送ってきたりして詐欺メールを信用させます。

回避出来た企業では、振込先変更が一部の部署にしか来ていない事が判明しました。そこで、客先に確認する事によって詐欺が判明しています。情報を社内でも守ろうとした事が逆に攻撃者には都合が良かった様です。将に、コミュニケーションと情報共有に伴う協力体制の強化が良い対策なのだと思われます。

「犯罪のビジネス化（アンダーグラウンドサービス）」に関しては、なぜ「金銭搾取」に含まれるのか不思議に思われる方も居られるかも知れません。理由は、金銭を得ることが目的で行われる事が主だからです。他の分野で言えば闇社会、裏社会のマーケットです。時として大掛かりな組織もありますが、基本的には少人数の組織で構成されたグループ又は開発された製品です。ただし、天才的な奇抜な手法で攻めて来る場合がある事を忘れないで下さ

い。軍隊で言えば、小隊組織、ゲリラ部隊で常識破りの部隊です。基本的には正攻法で守れば良いと思われます。セキュリティ環境を強化して、セキュリティバッチを最新にし、脆弱性の対応を早急に行う事だと思います。森の中で戦わず、見晴らしの良い平原や草原で戦うイメージでしょうか。大量の金銭搾取、情報漏洩、複雑な業務妨害は珍しい脅威なので、早急なる対応と復旧が出来る環境の構築が必要となります。

アンダーグランドサービスでの取引は判明していませんが、奇抜は方法の発生が先日発表されました。「CSV 形式ファイル」を使用するリスクです。この脅威はウィルスソフトでも対応不可、脆弱性対策でも対応不可と言うやっかいなものです。脅威としては２００４年頃からあった脅威です。作業者の習慣や心の隙を狙っている様に思えます。基本操作時の注意点も確認が必要です。

２－３）「業務妨害」に関する対策について

「業務妨害」に対する脅威は、１０大脅威の内で下記の３つに関連すると思われます。

第４位　　脆弱性対策情報の公開に伴う悪用増加
第７位　　IoT 機器の脆弱性の顕在化
第９位　　サービス妨害攻撃によるサービスの停止

上記の脅威に対する対策は、３つあります。皆さんに中には、「脆弱性対策情報の公開に伴う悪用増加」と「IoT 機器の脆弱性の顕在化」が、「業務妨害」に含めている事を不思議に思われる方も居られるでしょう。理由は、業務に影響する脅威に関連する場合が多い為です。対策の１つ目は、セキュリティ情報の取得強化です。２つ目は、情報システムの耐久性の強化です。そして最後が、セキュリティ改善への早急なる対応強化です。「最新の情報を入手してシステムに反映する。」、「脆弱性に対応完了までの対応を実施する。」、「対応が完了したら早急に対応する環境を構築する。」事が重要になります。

これらの脅威に関しては、個別に対策は記載致しません。常にセキュリティの脆弱性や不備、他のシステムでの障害発生状況を入手する事が基本となります。その上で、自分達のシステムへの影響を考えて対策を練ります。時には対応までサービスの変更も必要になります。対応や対策が確定したら、早急に疑似システム上で確認してから対応します。ここで注意が必要な事は、特に脆弱性の対応結果に関しては、疑似環境又は一部に適用して問題が無いことを確認しないと新たな障害を招く場合がある事です。ご注意下さい。

２－４）「対応人員不足」に関する対策について

「対応人員不足」に対する脅威は、１０大脅威の中で、最後に残った下記です。

第５位　　セキュリティ人材の不足

実は、この対策が一番難しいと思います。理由は、必要とされる「セキュリティ人材」が明確でなく、国や管理機関、各組織のトップマネージャ、現場マネージャ、現場のメンバーで要求が異なる場合が多いからです。従って、この脅威に対する最初の対策は、組織にとって必要な「対応人材」とはどの様なスキルや知識、管理能力等を持ち合わせている人なのかを、明確にする事だと思います。理解頂きたいことは、現在の状況はメンバー全員がある程度の知識とスキルを持たない限り守れない状況です。セキュリティの専任者や担当者の対応で防げる状況ではなく、組織メンバー全員で防がないと防げない状況です。

上記の様に個々の対策を診ていくと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、減らした上で「最悪を想定し最善を尽くす。」と考えて頂きたいと思います。

以上で、「現在のリスクの概要と対策」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