セキュリティ教育が必要な理由　③

2018 年 6 月 1 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、３文書目として、「情報セキュリティに関する思考と重要性」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

「情報セキュリティに関する思考と重要性」

今までの２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」と「現在のリスクの概要と対策」にて、情報セキュリティが必要な状況となった状況と、現在対応が必要となるリスクの主なるものに関して、多少ご理解頂けたのではないかと思います。

もちろん、上記の２文書にあたる内容を詳しく記載すれば何冊もの書籍又は数百ページ以上の文書となってしまいます。従って、概要的な内容に留まりイメージのみとなっている事に関しましては、ご容赦願います。

現在の脅威に関する詳細内容は、IPA 独立法人情報処理推進機構 様が多種多様な文書やビデオ、チェックシート等を作成して下さっています。皆様が必要と思われる内容から、参考される事をお勧めします。（IPA ホームページ：https://www.ipa.go.jp/index.html ）

私共と致しましては、IPA 独立法人情報処理推進機構 様のサイトでの記載や文書を理解頂く前に、流れや概要的な部分を理解して頂けたらと思っております。

皆様に判り易くお伝えさせて頂きたいとの思いから、視点を変えた例やイメージを含めた記載をさせて頂きます。技術的な部分は最低限にさせて頂いています。

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）情報セキュリティへの個人としての対応について

現在発生している、主なるリスク・脅威と対応に関して理解して頂いた上で、個人的にはどの様な対応が必要なのかを、考えてみたいと思います。

前文書である、「現在のリスクの概要と対策」にて記載させて頂きました様に、脅威としては下記の４つが多くを占めています。

・【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

「対応人員不足」に関しては、次の組織での対応で記載させて頂きますので、その他の３リスクに関して考えたいと思います。

１－１）情報漏洩に対する個人としての対応について

情報漏洩は、組織よりも個人的な対応が重要になります。理由としては、総ての個人に情報漏洩の可能性があり、総ての個人が理解した上で対応しないと防げない脅威だからです。

他の２脅威も同様ではないかと思われた方も多いと思います。しかし、他の２脅威は組織やシステムの強化で対応が出来る部分がありますが、この情報漏洩は困難なのです。その点を中心に記載したいと思います。

情報漏洩は、下記の様な方法で起こる可能性があります。他にもありますが、特に注意して頂きたい漏洩方法のみ記載させて頂きました。

・社外への情報持ち出し中に、紛失する事での漏洩
・社外での業務実施及び作業（営業活動、報告書作成等）中に漏洩
・個人的な環境上で、情報処理中に漏洩
・人為的な操作や活動中に漏洩
・個人的な情報伝達による漏洩
・社内業務中でのマルウェアによる漏洩

報告等での多くは、最後の「社内業務中でのマルウェアによる漏洩」の内容です。そして、社内教育での重要点も同様です。しかしながら、重要な情報漏洩の多くはその前の５つによる漏洩であるのが現状です。何故なのかは、下記を読んで頂けると多少ご理解いただけるかと思います。

下記に、事例と注意点について簡単ですが記載させて頂きます。

① 社外への情報持ち出し中に、紛失する事での漏洩

＜事例＞：会社から顧客や出張先への移動時、又はセミナー等への参加時、印刷文書やパソコン等モバイル機器、USB 等の記憶媒体を失くしてしまう。

＜注意＞：必要最低限のデータ以外は持ち歩かない事。記録媒体は暗号化を行い、最悪盗難や紛失しても漏洩に繋がらない様にする。が基本です。

② 社外での業務実施及び作業（営業活動、報告書作成等）中に漏洩

＜事例＞：客先又は公共ネットワーク（特に無線 LAN）使用等により、漏洩。外部ネットワーク上のルータ等通信機器又は、サーバ等にマルウェアが存在し漏洩。

＜注意＞：外部ネットワークの使用は最低限に抑える。使用環境のセキュリティレベル（暗号化通信、マルウェア対応等）を確認し、送受信時は暗号化通信を行う。

スマートフォンでの情報漏洩には特に注意する。（下記に難しい状況を理解頂く為に、技術的な部分も多少含めて説明させて頂きます。セキュリティ担当者以外の方は、技術的な記載は理解頂けなくても大丈夫です。）

スマートフォンやタブレットで無線 LAN に接続する場合にセキュリティを確保が非常に難しいという問題があります。パソコンでは、サーバが正しいかどうかをルート証明書で認証します。一方、スマートフォンなどでは、ルート証明書を持っていなくても接続できる仕様になっています。認証サーバが正規のものかどうかを確認しないため、例えば無線 LAN では、攻撃者が用意した偽のアクセスポイント（AP）に接

続させられるといった危険性があります。このような問題があるため、セキュリティを重視するなら EAP-TLS への移行が望ましいです。ただクライアント証明書の準備に時間がかかることもあります。そうした場合には、ハードウエアを認証する MAC アドレス認証を EAP-PEAP に組み合わせるという一時的な対処方法もあります。

③ 個人的な環境上で、情報処理中に漏洩

＜事例＞：自宅の環境又は友人等会社外の環境にて情報使用時に漏洩。スマートフォン等個人使用機器とリンクした使用時に情報漏洩。

＜注意＞：個人環境にて仕事関連及び自社関連の情報は取り扱わない。仕事上で使用する機器の私的用途での使用は控える。

④ 人為的な操作や活動中に漏洩

＜事例＞：社内作業中に、自分の PC 等又は机上より他のメンバーが情報を入手し漏洩。ビル内、喫茶、喫煙所、車内、路上での会話より情報漏洩。

＜注意＞：社内でも離席時は画面ロック、資料の保存を徹底する。一歩席を外したら、誰が聞いているか、見ているか判らない状況にあると考える。

⑤ 個人的な情報伝達による漏洩

＜事例＞：SNS 等にて限られたメンバーでの情報共有のつもりが、公共ネット上に漏洩。スマートフォン等個人使用機器やメールから情報漏洩。

＜注意＞：SNS のセキュリティ及びフリーメールのセキュリティは信用しない事。
自分の判断で情報の価値を決めることなく、顧客、会社、仕事に関しての話題はネット上に流さない。(その情報に価値がある人物、組織、会社が存在する場合があります。)

⑥ 社内業務中でのマルウェアによる漏洩

＜事例＞：自分を含む社内の機器がマルウェアに感染した事による情報漏洩。

＜注意＞：添付ファイルは送信者に送信を確認してから開く。受け取る必要が無い人からのメールは開封しない。「確認要請」に従った、URL のクリックは行わない。
フリーメールや送信メールと送信者のメールアドレスが不一致したメールは開封しない。

上記の内容から、不信感を持って行動する事が必要になってしまう事が、⑥を中心に報道や社内教育が行われる事が多い原因だと思われます。「友人、同僚、上司、部下、取引先、社会のあらゆる環境を信じてはいけない。」と言われている様な気分になります。私共としても、伝える内容に苦慮する部分ではあります。

１－２）金銭搾取に対する個人としての対応について

「ランサムウェア」の様なターゲット先から金銭搾取を実施する手法のリスクには、個人的な対応と組織的な対応の両方が必要になります。

現在問われている事項として、「暗号化又は情報ロックをかける主なる理由は金銭搾取なのか」があります。「証拠隠滅」を目的としている場合があると言われています。情報搾取の後に証拠隠滅を行う為、暗号化等を行い最後の利益を上げるのではないか、空き巣実施後に家に火を放って証拠隠滅する様な事なのではないかと言う事です。

金銭搾取のうち、「ランサムウェア」に関する個人的な対策は、「⑥ 社内業務中でのマルウェアによる漏洩」と同じです。何故ならば、個人が関係する場合にはメール又は URL のクリックによりマルウェアに感染する事から始まるからです。

問題はもうひとつのタイプです。昨年日本航空が３億６千万程の被害を受けた詐欺による場合です。日経コンピュータが大手企業へアンケートした結果では、６割強の企業が詐欺メールを受け取り、４割強が連絡を行い、１割弱が実際に振り込んでいます。

「標的型攻撃」の詐欺は個人での対応は不可能と考えて下さい。相手は御社の人員構成、顧客の情報、取引履歴まで調査済の場合が多く、疑うべき事項が非常に少ないのです。但し、詐欺ですので必ず嘘の情報が含まれています。その嘘を見破る事が重要です。

個人としては、変更に関する報告内容があった場合には必ず他のメンバー、部署、専門家に確認を取る事が重要です。例えば以下の様なものです。

・システム不備により、メールアドレスが一時的に変更になりました。
・関係会社との取引上必要となり、振込先の口座が変更になりました。
・人事異動により、貴社担当が変更となりました。
・取引内容の変更をお願いします。

あまり有名な話ではありませんが、日本航空と同様の航空会社への詐欺は他にも発生し、未然に防げているものがあります。理由は、「振込先の口座」変更依頼を他の部署へ確認した結果、詐欺だと判明したからです。

社内での部署ごとによる機密主義は結構ですが、取引先の情報変更に関しては共有する事が重要だと思います。

その他の手法としては、最初は小規模の取引を実施し正常に完了します。次に大きな取引で詐欺を行うものが出ています。ネットワークを使う以前からある詐欺の方法です。取引詐欺に関しても考慮が必要です。

１－３）業務妨害に対する個人としての対応について

「業務妨害」に対する個人としての対応には３つあります。

・マルウェアを設定されない様にする対応
・妨害発生の予兆を発見する対応
・妨害発生時の対応

① 「マルウェアを設定されない様にする対応」

この対応は、情報漏洩の場合と同じです。基本的な攻撃方法は、メールか URL のクリックから開始されます。自分が受け取る理由のないメールや不信は添付ファイル、特に実行形式や圧縮ファイル、意味不明は拡張子のファイルは気を付けて下さい。

② 「妨害発生の予兆を発見する対応」

攻撃時の規模にもよりますが、意味不明なメールやアクセス、業務効率の低下が起きる事がある様です。時にエラー表示のポップアップメッセージが表示される、画面上に不穏な文字や色、画像が表示される場合もあるとの事です。

自分で理解出来ない又は不信に思える状況が発生したら、間違いでも良いのでセキュリティ担当者に一報を入れる様にしましょう。

③ 「妨害発生時の対応」

即座に、セキュリティ担当者へ連絡し指示に従って下さい。状況判断が必要ですので、作業及び操作は即時停止した上で、電源は落とさないで下さい。セキュリティ担当者が捕まらない場合、直属の上司から始めて上位の管理者へ順番に連絡が出来る方を捕まえて判断を願って下さい。役員や社長、会長でも遠慮はいりません。その場合は、メンバー全員の業務停止とネットワーク停止を勧めます。

この件に関して私共として疑っている事象が一つあります。正式な報告としては無いのですが、この業務妨害も証拠隠滅の為にやっている可能性です。

DDoS 攻撃と言う、複数個所から大量のアクセスが集中して業務停止が行われた場合、推奨の対応は業務を停止しネットワークを切り離して、ログの解析を実施する事になっています。

実際にこの状況を実現した場合、システムのサーバ、端末、通信機器のメモリーや CPU は一時的に使い放題になってしまいます。その時を狙えば一気に証拠隠滅の作業を起動出来ます。母屋から逃げ出す為に倉庫に火を放つ様なものでしょうか。状況発生からログの解析開始までの時間は以外とありますし、解析が開始されても直ぐには付加はそれほど高くなりません。

２）情報セキュリティへの組織としての対応について

次に、組織としての対応に関して考えてみたいと思います。前文書である、「現在のリスクの概要と対策」にて記載させて頂きました様に、脅威としては下記の４つが多くを占めています。

・【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

組織では特に「対応人員不足」が大きな問題となります。人員構成をどの様にして対応して行くかが問題になると考えています。

２－１）情報漏洩に対する組織としての対応について

個人の対応でも述べさせて頂きましたが、情報漏洩に関しては、組織よりも個人的な対応がより重要です。理由は、総ての個人に情報漏洩の可能性があり、総ての個人が理解した上で対応しないと防げない脅威だからです。

他の脅威である、「金銭搾取」及び「業務妨害」に関しては基本的に組織やシステムで対応する方法を考える必要があります。そして、組織で対応が必要な脅威です。

情報漏洩は、個人の対応なしでは防げない非常に対応が難しい脅威です。その上で、組織として出来る対応に関しても考えてみたいと思います。

情報漏洩は、下記の様な方法で起こる可能性があります。他にもありますが、特に注意して頂きたい漏洩方法のみ記載させて頂きました。

・社外への情報持ち出し中に、紛失する事での漏洩
・社外での業務実施及び作業（営業活動、報告書作成等）中に漏洩
・個人的な環境上で、情報処理中に漏洩
・人為的な操作や活動中に漏洩
・個人的な情報伝達による漏洩
・社内業務中でのマルウェアによる漏洩

最後の「社内業務中でのマルウェアによる漏洩」が話題となり、社内教育での重要点となる事が多いです。しかしながら、重要な情報漏洩の多くはその前の５つによるものです。簡単に事例と対応について記載させて頂きます。

① 社外への情報持ち出し中に、紛失する事での漏洩

＜事例＞：会社から顧客や出張先への移動時、又はセミナー等への参加時、印刷文書やパソコン等モバイル機器、USB 等の記憶媒体を失くしてしまう。

＜対応＞：情報を持出す記録媒体は、必ず暗号化を行います。持出す情報と使用機器は上司の承認が必要とする。業務中に使用している媒体での持ち出しは禁止する。

② 社外での業務実施及び作業（営業活動、報告書作成等）中に漏洩

＜事例＞：客先又は公共ネットワーク（特に無線 LAN）使用等により、漏洩。外部ネットワーク上のルータ等通信機器又は、サーバ等にマルウェアが存在し漏洩。

＜対応＞：外部記憶媒体による通信は、必ず暗号化通信を行う。外部から自社システムへの接続制限を設定する。サイト閲覧規制を設定する。客先及び公共ネットワークでの通信は最低限とし、通信ログ履歴の提出を義務とする。

③ 個人的な環境上で、情報処理中に漏洩

＜事例＞：自宅の環境又は友人等会社外の環境にて情報使用時に漏洩。スマートフォン等個人使用機器とリンクした使用時に情報漏洩。

＜対応＞：個人環境にて仕事関連及び自社関連の情報は取り扱い禁止とする。仕事上で使用する機器の私的用途での使用は禁止とする。

④ 人為的な操作や活動中に漏洩

＜事例＞：社内作業中に、自分の PC 等又は机上より他のメンバーが情報を入手し漏洩。ビル内、喫茶、喫煙所、車内、路上での会話より情報漏洩。

＜対応＞：操作機器の自動画面ロック時間を規定する。資料保存の施錠を義務とする。業務内容の会話可能範囲を規定する。組織及びグループでの監視・向上推進を規定する。

⑤ 個人的な情報伝達による漏洩

＜事例＞：SNS 等にて限られたメンバーでの情報共有のつもりが、公共ネット上に漏洩。スマートフォン等個人使用機器やメールから情報漏洩。。

＜対応＞：フリーメールでは、組織及び業務情報は一切記載禁止とする。SNS 等での情報発信内容は、社員個人に関連した情報に限る事を規定する。ウェーブ上、SNS 上での自社及び組織、顧客情報漏洩の状況を定期的に確認出来る様にする。

⑥ 社内業務中でのマルウェアによる漏洩

＜事例＞：社内の機器がマルウェアに感染した事による情報漏洩。

＜対応＞：社員セキュリティ教育にて、感染方法及び対応を定期的に伝達すると共に、伝達対応状況を確認する。不穏な動き思われる状況が発生した場合の、対応体制と手順を確定する。感染に関する責任問題は、重要としない様にする。報告者への奨励体制を整える様にする。

２－２）金銭搾取に対する組織としての対応について

「ランサムウェア」の様なターゲット先から金銭搾取を実施する手法のリスクには、個人的な対応と組織的な対応の両方が必要になります。

現在問われている事項として、「暗号化又は情報ロックをかける主なる理由は金銭搾取なのか」があります。「証拠隠滅」を目的としている場合があると言われています。情報搾取の後に証拠隠滅を行う為、暗号化等を行い最後の利益を上げるのではないか、空き巣実施後に家に火を放って証拠隠滅する様な事なのではないかと言う事です。

金銭搾取のうち、「ランサムウェア」に関する組織的な対策は、「⑥ 社内業務中でのマルウェアによる漏洩」と同じです。個々人の操作によってマルウェアに感染する事から始まるからです。そして、報告及び対応体制の確立が重要になります。

問題はもうひとつのタイプです。個人の対応でも記載させて頂きました様に、昨年日本航空が３億６千万程の被害を受けた詐欺による場合の対応が組織として重要になります。

日経コンピュータが大手企業へアンケートした結果では、６割強の企業が詐欺メールを受け取り、４割強が連絡を行い、１割弱が実際に振り込んでいるのです。個人での対応は不可能との共通認識を整える事が先ず重要になります。

相手は御社の人員構成、顧客の情報、取引履歴まで調査済の場合が多く、疑うべき事項が非常に少ないのです。但し、詐欺ですので必ず嘘の情報が含まれています。その嘘を見破る事が重要です。組織として、変更に関する報告内容があった場合には必ず他のメンバー、部署、専門家に確認を取る事を義務付ける事です。例えば以下の様な依頼があります。

・システム不備により、メールアドレスが一時的に変更になりました。
・関係会社との取引上必要となり、振込先の口座が変更になりました。
・人事異動により、貴社担当が変更となりました。
・取引内容の変更をお願いします。

日本航空と同様の航空会社への詐欺が発生し、未然に防げているものがあります。理由は、「振込先の口座」変更依頼を他の部署へ確認した結果、詐欺だと判明したからです。

社内での部署ごとによる機密主義は結構ですが、取引先の情報変更に関しては共有する事が重要だと思います。

２－３）業務妨害に対する組織としての対応について

「業務妨害」に対する組織と対応には、個人と同様に３つあります。

・マルウェアを設定されない様にする対応
・妨害発生の予兆が発見された場合の対応
・妨害発生時の対応

① 「マルウェアを設定されない様にする対応」

この対応は、情報漏洩の場合と同じです。基本的な攻撃方法は、個人へのメール又はURL のクリックによって開始されます。従って、各個人が認識を高めると共に、組織として教育、報告、バックアップ体制を整える事が必要になります。

② 「妨害発生の予兆が発見された場合の対応」

組織構成人員又は顧客、取引先より予兆発見の報告を受けた場合に対する、報告受取り、報告体制、調査実施、対応実施の手順とバックアップ体制を整える事が必要になります。報告奨励の体制と取引会社、顧客を含めた協力に向けた、連絡及び対応体制の整備が必要になります。

③ 「妨害発生時の対応」

発生時の報告から調査、連絡、対応体制の確立と情報共有体制が必要になります。状況により、協力会社、顧客、公的機関への連絡の判断基準も含めた規定を整える必要があります。

この対応に関しては、現在の対応が変わる可能性があると思っています。現在の最善といわれている対応は、機器を停止せずにネットワークを停止して分析する事になっています。しかしながら、この件に関して私共として疑っている事象が一つあります。正式な報告としては無いのですが、この業務妨害も証拠隠滅の為にやっている可能性です。

DDoS 攻撃と言う、複数個所から大量のアクセスが集中して業務停止が行われた場合、推奨の対応は業務を停止しネットワークを切り離して、ログの解析を実施する事になっています。

実際にこの状況を実現した場合、システムのサーバ、端末、通信機器のメモリーや CPU は一時的に使い放題になってしまいます。その時を狙えば一気に証拠隠滅の作業を起動出来ます。母屋から逃げ出す為に倉庫に火を放つ様なものでしょうか。状況発生からログの解析開始までの時間は以外とありますし、解析が開始されても直ぐには付加はそれほど高くなりません。

２－４）対応人員不足に対する組織としての対応について

組織での対応の中心は、教育、連絡体制、対応体制が中心になります。従って、一番問題となるのは、「**対応出来る人員がいない**」事です。

多くの経営者、組織管理者の悩みの多くは、この人員を如何に整えるかとなっています。セキュリティ対応では金銭は生み出せませんので、費用負担もあり悩みは尽きないのではないでしょうか。そこで、下記の事を考えて対応する必要があると思います。

・自組織での対応範囲を確定する。
・障害発生時の協力関係会社との契約等を整える。
・組織メンバーへの教育の向上を推進する。

① 自組織での対応範囲を確定する。

障害の発生抑制から調査、解決までの全てを組織内で整えるのは非常に難しいです。

数万人規模の組織であっても、組織内で総て行うのは難しいのではないか思われます。従って、自組織ではどこまで行うのかを決める必要があります。予兆を発見したら全て契約先の会社に任すのも一方法です。その場合には契約先に機密事項も閲覧される可能性があるので、注意が必要です。最低でも数名のセキュリティ担当者が契約先のセキュリティ会社と協力して対応する必要があります。

② 障害発生時の協力関係会社との契約等を整える。

自組織内での対応する範囲以外は、協力関係会社とチームを組んで調査、対応する必要があります。問題は扱うデータが機密情報も含む事が多く、早急なる対応を行わないと信用を喪失してしまう可能性がある事です。

従って、会社としての信頼が出来、技術的にも信用できる先との契約が必要となります。組織内のセキュリティ担当者のレベルによっては、信用出来る会社の協力を得た上で、技術的に優秀な会社のサポート受ける方法もあると思われます。

③ 組織メンバーへの教育の向上を推進する。

個人の対応にて述べさせて頂いた様に、組織メンバーの認識や対応がある程度のレベルに達していないと、セキュリティ脅威を防ぐ事は困難な状況です。

従って、組織が望むレベルまでの教育が必要になります。その教育では専門的な内容まで含む事はあまりなく、自らの対応する内容と連絡先、サポート体制先との協力内容が明確になる意識が中心になります。逆に専門的な知識があると、自分で対応を試みてしまい障害発生時の対応が遅れる場合がありますので、ご注意下さい。

上記の事項を踏まえて、組織での対応と教育体制を整える事が、人員不足への対応となります。

３　まとめ

上記の様に、個人的及び組織的な対応を整えるにはセキュリティ脅威に対する教育が不可欠になります。そして、その教育の内容は貴方の業務、貴方の組織、貴方の環境により異なります。営業主体、製品主体、サービス主体など、組織が実施する内容によりメンバーが把握する必要がある内容は異なり、体制も異なります。どこかの教育と同じとは行かないのが現状です。その様な教育を思考し、作り上げ、実施して行く事をお手伝い出来たらと考えております。宜しくお願い致します。

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