秋号

京印季報

2019 秋季特別企画

教育研修セミナーより 富士ゼロックスにおける情報セキュリティマネジメント
～情報セキュリティ推進の実践事例～

京都府印刷工業組合

2019 Vol.648

目次

秋号表紙イラストレーション　コンセプト

赤や黄色、茶色など、秋を感じられる色をイメージして、秋山や、秋の木々をシンプルな絵になるよう描きました。

一本一本、微妙に違う色に染まり、日々色を変えていく木々や山の色はあたたかく、見ているだけでほっとします。夕暮れ時は少し寂しい気持ちにもなりますが、今年の秋は友達や家族と紅葉狩りをしに山登りをしよう！

京都造形芸術大学こども芸術学科３年次生　曽田みなみ

巻頭言

京都府印刷工業組合理事長

中西隆太郎

今年も８月御盆の頃、大型の台風10号が四国・中国地方を縦断して各地に雨による被害をもたらし、また９月に入ると、台風15号の影響により、千葉県内の随所で停電や断水が発生するなど市民生活に大きな影響を及ぼしました。10月に入り、ようやく台風シーズンも終盤を迎えますが、これ以上大きな台風被害が起きないことを願ってやみません。被災された皆様には心よりお見舞いを申し上げます。

なお、昨年も台風21号等により全国に甚大な被害をもたらしましたが、その風水害に対する保険大手４社の保険金支払額が１兆円台を超え、過去最大規模となりました。この10月より火災保険料の価格が上がりましたが、昨年の多額な保険金支払に伴う補てんは今回の値上げに織り込まれていないようです。

ところで、現在の中小零細企業の経営環境は、年初の原材料の値上げや雇用改善と人口減少による人手不足､そして後継者不在の問題等があり､存続が益々厳しい状況下にあります。このような中で、今年は働き方改革や10月からの消費税増税などにも対応していかなければなりません。

働き方改革による法改正により、いよいよ来年から中小企業においても改正された残業規制が適用されますが、経営者側が、残業時間の制約により売上が落ちるのではと危惧する一方、従業員は、残業時間の減少による収入減を心配しています。このように、法改正に対して労使双方に負のイメージが先行しているので、強い危機感を持っておられる方も多いのではないでしょうか。

しかし、以前から言われているように、日本の就業者１人当たりの労働生産性は相当低く、2017年の調査ではアメリカの66％に過ぎず、G7では最下位、経済協力開発機構（OECD）加盟の35か国中では21位です。その原因は“日本品質”の問題だと言われており、アメリカのように職務記述書を渡さず、仕事の範囲が曖昧であるためとの指摘もあります。過剰なサービスを大胆に見直すと共に、従来の発想を超える先端技術を活用した取り込みを図らなければ、人口減少が免れない日本では経済情勢も益々悪化の一途をたどるでしょう。法改正

を機に、過剰なまでの品質に対する考え方を改め、働き方改革に反映させていく必要があります

このような中、働き方改革を実行するにあたり、何からどのように行えばよいのかを分かりやすく解説するセミナーの開催が待たれておりました。

前号の盛夏号でも述べましたが､本部団体の全日本印刷工業組合連合会では、働き方改革に無理なく対応できる「幸せな働き方改革」を策定し、既に全国の各府県工組において説明会が実施されており、京都では、去る９月13日(金)に、「ステップ３」に該当する､「労務対策セミナー 幸せな働き方改革へ向けて‼ ～業務革新に取り組んで業績拡大に結び付ける～」を開催いたしました。

全印工連が提唱する「幸せな働き方改革」にはステップ１からステップ５まであり、ステップ１の「働き方改革の必要性を理解する」から始まり、ステップ２で「目標を設定し、計画をたてる」手法を研修。ステップ３では､「業務革新で生産性向上を図る」ことを目指し、到達点となるステップ４「就業規則の整備」とステップ５「人事考課・給与規定の整備」は、今年度中の完成と実行に向けて実施要領の策定が進められています。これらのプログラムは独立性もありますので、当組合では日本品質の弊害を考えるという趣旨からステップ３の「業務革新で生産性向上を図る」をテーマに取り上げました。

なお、本誌が発行される10月15日(火)には､「幸せな働き方改革」の５つのステップとは少し視点を変えた､「秋期研修会“働き方改革”を実現する、あしたの人事評価セミナー」を開催します。当セミナーでは､「社員の成長と会社の業績向上に繋がる人事評価の仕組み」が解説されるなど、労務対策セミナーのテーマであった「業務革新で生産性向上を図る」を補完する内容となっています。

京都府印刷工業組合では、今後も存在価値ある組合であり続けるため、組合員の皆さまに役立つ情報提供とともに、保険会社との連携による共済制度の運営、アドビ社との特別ライセンスプログラムの推進等、正しく“群れる”事によるスケールメリットを活かした各種事業のご周知とご提供等に向けて努力して参ります。引き続きのご協力・ご支援をお願い申し上げ、御挨拶とさせていただきます。

教育研修セミナー
富士ゼロックスにおける情報セキュリティマネジメント
～情報セキュリティ推進の実践事例～

講師／神林　彰　氏　（富士ゼロックス㈱CP&RM部 情報セキュリティセンター センター長）

セミナー会場

京印季報10月秋号の特別企画では、去る６月19日（金）午後６時より京都印刷会館２階大ホールにおいて開催された、教育研修セミナー「富士ゼロックスにおける情報セキュリティマネジメント」～情報セキュリティ推進の実践事例～をご紹介します。

「情報セキュリティ」には、個人情報保護、サイバー攻撃、ヒューマンエラー、内部不正など様々なリスクが身近に存在していて、放置すると、問題が顕在化し、事業継続を脅かしかねない事態になることもあります。

セミナーでは、情報セキュリティの体制、リスクの特定、ルール、教育・啓発、インシデント対応など、中小印刷事業所にも対応可能な情報セキュリティマネジメントの実践事例について詳しく解説していただきました。是非ご一読ください。

はじめに


講師の神林　彰氏

富士ゼロックスの神林と申します。本日はよろしくお願いいたします。

私は富士ゼロックスに入社して35年以上経ちますが、入社当時はマウスも余り普及していませんでした。そのような時代、当社ではマウスを使ったコンピューターや、ネットワーク、イーサネット（Ethernet）、マルチウインドウといった仕組みのワークステーションをビジネスとして展開していて、私はSEや開発を担当していました。

その後は情報システム等の担当を経ながら、この20年間は本社で情報セキュリティを含むリスクマネジメント全般を担当してきました。情報セキュリティの事故が起きれば当然対応しますが、他にも地震の対応、パンデミックの対応、従業員の不祥事の対応など、様々な会社のリスクマネジメントに取り組んできました。

富士ゼロックスの概要

当社の創業は1962年。本社は六本木にあります。開発の拠点は横浜のみなとみらいや海老名市に、工場は中国やベトナムにあります。

当社の製品・サービスは、主に３つに分かれます。１つ目は「オフィスプロダクト&プリンター事業」で、複写機・複合機のビジネスです。２つ目は「プロダクションサービス」で、高速のプリンターを使った印刷に関わるビジネスです。３つ目の「ソリューション&サービス事業」は、マイナンバーなどのアウトソーシングの受託、クラウドなどITサービス等の新しい分野です。

今、当社では、「紙の情報を複写する」というビジネスからの事業構造転換を推進していて、お客様の情報をお預かりするビジネスに大きくシフトしているので、非常にセキュリティが重要になってきています。印刷業界におかれても、お客様の情報をお預かりするビジネスに取り組まれている会社が増えていると思うので、セキュリティは重要なテーマではないでしょうか。

情報セキュリティの脅威

～セキュリティ対策を怠ることで企業が被る不利益～

情報セキュリティ対策を怠ると会社の中で様々な不利益が生じます。

１つ目は「金銭の損失」です。当たり前かもしれませんが、事故を起こしてしまって、お客様の情報漏洩につながると、結果的に損害賠償やお詫びの支払いをしないといけなくなります。

また、幸い当社では起きていませんが、ビジネスメール詐欺の被害による金銭の損失もあります。国内での被害も発生しており、皆様も気をつけてください。

２つ目は「顧客の喪失」です。事故を発生させた企業という風評により、顧客離れが生じることもあります。また、結果的に情報漏洩に至らなくても、普段のやりとりの中で「ずさんな管理をしている」と思われた瞬間から、お客様は離れていってしまいます。

３つ目は「業務の停滞」です。実際に情報漏洩が起きると、お客様の対応に負われ、担当部署は数か月間、日常業務ができないこともあります。

４つ目は「従業員への影響」です。事故が起きると、部門長はつい当事者を責めたくなるものです。しかし、叱責が行き過ぎると、従業員が働く意欲を失ってしまうこともあります。また、会社全体が情報管理やセキュリティに関心がなくずさんだった場合、従業員の情報倫理や情報モラルが低下することに繋がります。

～標的型攻撃の事例～

次に、ある企業の事例を紹介します。サイバー攻撃を受け、数百万人のお客様の個人情報が流出ました。不審な通信があり、おかしいと気づいた社員もいたようですが、経営トップに報告されるまでに２か月かかりました。

当事例の問題は、インシデントが起きた後の対応が鈍いことです。その企業の社長は「情報伝達

が伝わらなかったことが最大の反省点」と述べています。もっと早くエスカレーションして手を打っていれば、被害をもっと極小化できたのではないかと思われます。

加えて、対応が遅くなると、「隠しているのではないか」という疑いを持たれてしまいます。そうなると、結果的に信頼を大きく失う。事故を防ぐことが一番大事ですが、事故後の対応をしっかりやらないと、もっと大変なことになってしまいます。

～情報セキュリティの課題～

そもそも情報セキュリティの全体像とは何で、どういうところに気をつけないといけないのかがわかりにくいものです。整理をしないと、経営者も何からどう手を付ければよいのかわからなくなります。情報セキュリティの課題は業界や企業により様々ですが、例えば、「個人情報保護法への遵法」、「パソコンのファイルが開かなくなってしまうランサムウエアによるサイバー攻撃」、「メール誤送信などのヒューマンエラー」、「不正な情報持出しなどの内部不正」というように、テーマを決めて取り組むことが必要ではないでしょうか。

経営者が認識すべき３原則

課題が明確になれば、次は「なにをすべきか」です。経産省とIPA（独立行政法人情報処理推進機構）では、「サイバーセキュリティ経営ガイドライン」の中で、経営者が情報セキュリティとして認識すべき三原則を公表しています。

１つ目は、「セキュリティの対策は経営者のリーダーシップで進める」です。例え現場の従業員がセキュリティに関心を持ち対応したいと考えても、従業員全員の賛同を得るのは難しい。経営者の意志によって対策を主導しなければなりません。

２つ目は、「委託先のセキュリティ対策まで考慮する」です。最近、サプライチェーンセキュリティが重要視されています。攻撃者は弱いところから攻撃をします。情報漏洩が委託先の不備であ

情報セキュリティ課題の例

- **コンプライアンス**
  - ✓ 個人情報保護(利用目的管理などの対応)
  - ✓ 各国・地域独自の法制定への対応
  - ✓ ソフトウエアの適切なライセンス管理(うっかりでは許されない)
- **サイバー攻撃**
  - ✓ 外部サイトへの攻撃(サイト改ざん/情報漏えい/踏み台)
  - ✓ ランサムウエア等マルウエア感染
  - ✓ ビジネスメール詐欺(自社の被害、取引先の被害)
- **ヒューマンエラー**
  - ✓ モバイルPCの紛失・盗難
  - ✓ 書類誤送付
  - ✓ メール誤送信
- **内部不正**
  - ✓ 退職予定者からの情報持出し

っても、委託元としての管理責任が問われるので、自社同様に十分な注意が必要です。

３つ目は、「関係者とは常に情報セキュリティに関するコミュニケーションをとる」です。日頃から様々な人とコミュニケーションをとって情報収集すると共に、お客様に対しては、「当社はこういうセキュリティの考え方で、このような対策を打っています」と伝えることが肝要です。そうすることで、日頃から業務上の関係者との間で、信頼関係が構築でき、万が一事故が起きた時には説明責任が果たせるのではないでしょうか。

なにをすべきか
①対応方針を定める

それでは、３原則に対して具体的に何を実行すればよいのでしょうか。「サイバーセキュリティ経営ガイドライン」の中では10項目が掲載されていますが、その中のいくつかを取りあげます。

１つ目は「対応方針を定める」です。情報セキュリティは幅が広いので、「当社はこういう考え方でセキュリティ対策に取り組んでいます」と説明できるよう整理します。それを従業員にも示せば、社内全体が同じベクトルに合わせることができます。また、情報セキュリティの担当組織、担当者を決めます。一番望ましいのは、情報セキュリティの専任者を設置することです。当社では、2005年の個人情報保護法の施行とともに専任体制をつくりました。

下の表は当社の情報セキュリティ基本方針です。

各々の会社で考え方が違うと思いますが、当社では、様々な情報の中で、お客様からお預かりしている情報がとても重要だと認識していることを明記しています。また、セキュリティ対策を執るに当たっては、リスクアセスメントによって、メリハリのある対応をするとともに、万一事故が起きてしまった際は、初動対応と迅速なエスカレーションに努めると明記しています。

～情報セキュリティ視点で情報を区分～

方針だけ立てても実態が伴わなければ効果は得

情報セキュリティ基本方針

富士ゼロックスおよび関連会社は、お客様をはじめとしたステークホルダーの皆さまにご安心頂ける企業を目指すため、情報セキュリティの維持・強化を図るとともに、継続的な改善に努めます。

1. **情報セキュリティの目的**
   お客様・お取引先様からお預かりした情報や自社の技術情報をはじめ、重要な情報を、漏えい・改ざん・消失などにつながる様々な脅威から守り、適切に取り扱うことを、情報セキュリティの目的とします。特に、お客様の機密情報および個人情報を扱う場合は、より厳しい管理・運用をすることにより、情報漏えい防止に万全を期します。
2. **情報セキュリティの運用**
   全社統制のもと、法令、契約および社内規程を遵守し、情報セキュリティを適切に管理・運用します。具体的には、リスクアセスメントをもとに各種施策の実施、点検、改善を行うとともに、教育・啓発により、従業者の意識醸成を図ります。
3. **情報セキュリティ事故の管理**
   万一、事故が発生した場合には、被害拡大防止等の初動対応および経営層・関連組織へのエスカレーションを迅速に実施することで、影響を最小限に抑えるとともに再発防止に努めます。

られません。情報セキュリティ視点で管理すべき情報を区分することで、機密性の高い区分の情報は厳しい情報管理を実施し、そうでない区分の情報は情報活用に重きをおく対応をしています。IPAの「中小企業の情報セキュリティ対策ガイドライン」の中でサンプルとして掲載されている情報区分の例を次に示します。

区分がなぜ必要なのかというと、個人でなく組織で情報を扱うからです。情報を扱う従業員が重要な情報が何かを識別でき、適切な管理をするためには、情報を区分して取り扱い方を明確にしておくことが必要です。

もう一つ、皆様方も取り組まれておられるかもしれませんが、施設管理もセキュリティとして重要です。

施設管理においては、情報の取扱いレベルに応じて境界を設定する考え方(ゾーニング)を適用します。例えば、レベルが１・２・３と境界を設定し、３の境界内の領域が最も重要なところです。個人情報を扱うような重要なエリアはレベル３とします。そして監視カメラを出入口に設置する、スマホ、パソコンの持ち込みを禁止するなどのルールを決めます。

このように“メリハリ”をつけて取り組むことで、仮に個人情報をお預けになるお客様が、本当にきちんと管理しているのかと視察に訪問されたとしても、「当社はこのような考え方で、お客様からお預かりする情報はレベル３のゾーニングの中で扱って管理しています」と説明することができます。

～情報セキュリティ体制～

当社は情報セキュリティセンターがセキュリティを担当していて、機能としては、コンプライアンスとガバナンスのルールを作る、教育を行う、個人情報の保護に取り組む等を行うチームと、サイバーセキュリティ対応のチームに分かれています。もしかすると、富士ゼロックスのように、４万人もいる会社だから、こんな対応が行えるのだろうと思われるかもしれませんが、セキュリティ

情報の機密区分の例

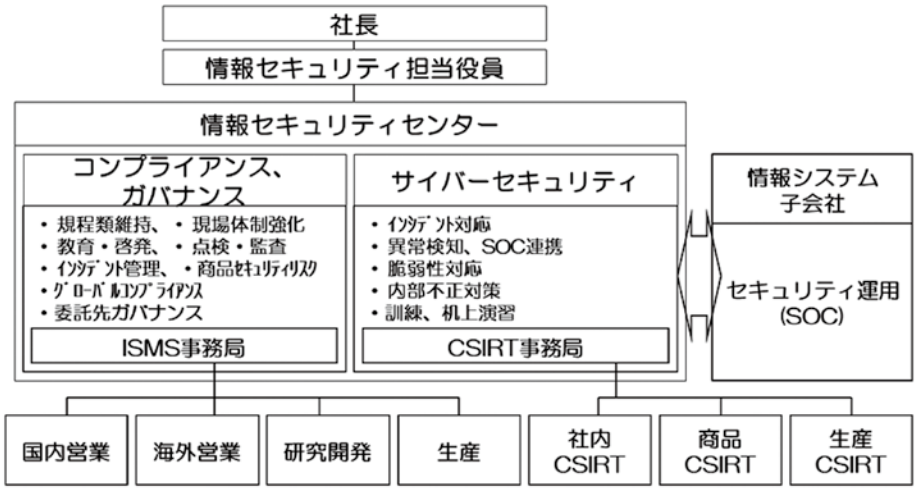
機密性2：極秘	● 法律で安全管理が義務付けられている ● 守秘義務の対象として指定されている ● 限定提供データ（一定の条件を満たす特定の外部者に提供すること を目的とする情報）として指定されている ● 営業秘密（秘密として管理されているもの）として指定されている ● 漏えいすると取引先や顧客に大きな影響がある
機密性1：社外秘	漏えいすると事業に大きな影響がある
機密性0：公開	漏えいしても事業にほとんど影響はない

出典：「中小企業の情報セキュリティ対策ガイドライン」
付録5： 情報セキュリティ関連規程（サンプル）
/IPA

ファシリティのゾーニングの例

レベル３： 高機密エリア	● 特に重要な資産を取扱い・管理・保管しているエリア ● 監視カメラの設置 ● 情報機器の持込み禁止　他
レベル２： オフィスエリア	● オフィスエリア、原則来訪者の入場禁止 ● 鍵。入場許可証による入退の管理 ● 来訪者は入場から退場まで、社員の同伴　他
レベル１： 来訪者エリア	● 来訪者に開放しているエリア ● 来訪者認識カードの着用 ● 入退場ゲートの設置　他

情報セキュリティ体制



対策を行うには、これらのリスクがあるならば、会社の大小に関係なく同じことをしなければならないと思います。但し、１人で全部取り組むことは難しいかもしれません。

例えば、会社の中で様々なルールを定めて統制する活動は自社で行い、技術的な対応は社外の専門会社に任せるというやり方もあると思います。

なにをすべきか ②リスクを把握し対策を実行する

対応方針が定まれば、次はリスクを把握して対策を実行することです。自社にとって、優先度の高いセキュリティのテーマを整理します。IPAの「中小企業情報セキュリティ対策ガイドライン」の中で自社診断があり、何ができている、できていないをチェックすることで、およそ自社がどのような状況にあるのかがわかります。

さらに詳細リスクアセスメントという方法に取り組むと、よりきめ細かい、自社の弱いところがわかるようになります。課題を把握した上で、優先度の高いテーマから順に取り組んでいくのが良いと思います。

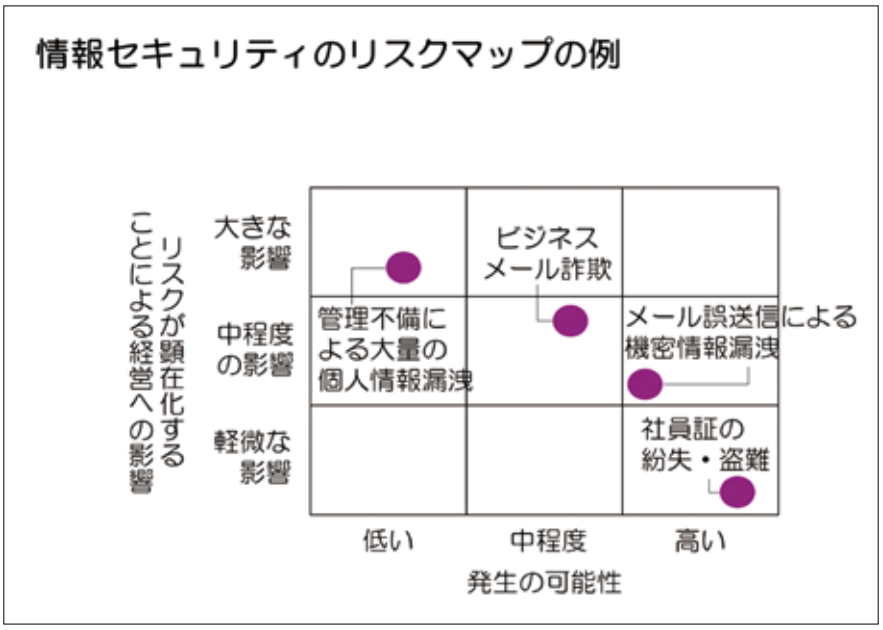
当社の場合は、情報セキュリティリスクの抽出を行い、重要なリスクを優先して対応しています。

例えば、下の図のようにリスクマップに、どのリスクがどこにあるのかをプロットしながら、何から手を付けるかを議論します。

縦軸に、その問題が起きるとどのぐらい影響があるのかというレベルを、上(最大)から下(最小)に向けて区分しています。横軸は、それがどの程度の可能性で起きるのかを、右(最高)から左(最低)に向けて区分しています。例えば、先ほど述べたビジネスメール詐欺の場合、送金してしまう可能性は極めて高く、かつ非常に損害が大きいと考えられるならば、リスクマップの右上にプロットします。このようにして複数のリスクをプロットして比較することで、優先すべき課題を抽出します。

～全部門長による取り組み～

当社では昨年度より、現場の部門長に情報セキュリティを主体的に考えてもらうための施策に取り組んでいます。全部門長に、「あなたの組織の中で、懸念されるリスクは何ですか」と問い、リストアップしてもらいます。本社サイドはそれを見て、各部門長をサポートしています。従業員を管理する部門長がリスクとして懸念していることを全て抽出し、それに対して一生懸命対策を講じていけば、重大な問題を撲滅することができるに違いないと考えています。



～身近なリスクへの取り組み～

次に、情報セキュリティ課題の中で、ヒューマンエラーとサイバー攻撃に対する取り組みの事例をご紹介します。

働き方改革の推進で、モバイルパソコンを持ち帰ったり、出張先で使用する機会も増えるので、モバイルパソコンからの情報漏洩対策も重要になっています。

当社では、モバイルパソコンのセキュリティ対策を人的・組織的対策と技術的・物理的対策の両者で取り組んでいます。

人的・組織的対策では、持出し不可のパソコンと持出し可能のパソコンとを容易に識別できるように、持ち出し可能なパソコンには「持ち出しパソコン」というシールを張って、自分も周囲も一目でわかるようにしています。

パソコンを持ち出しする際のルールとして、重要な情報が入ってる場合には上司の許可が必要としています。情報セキュリティには、need-to-knowの原則（知る必要性のある最小限にとどめる）という考え方があり、お客様への説明責任を果たすうえでも、持ち出しの必要性のある情報のみ持ち出しするという考え方が重要です。

また、帰宅時や離席時のパソコン管理においては、盗難対策のため施錠されたキャビネットにしまう、ワイヤーロックする等の対策を指導しています。

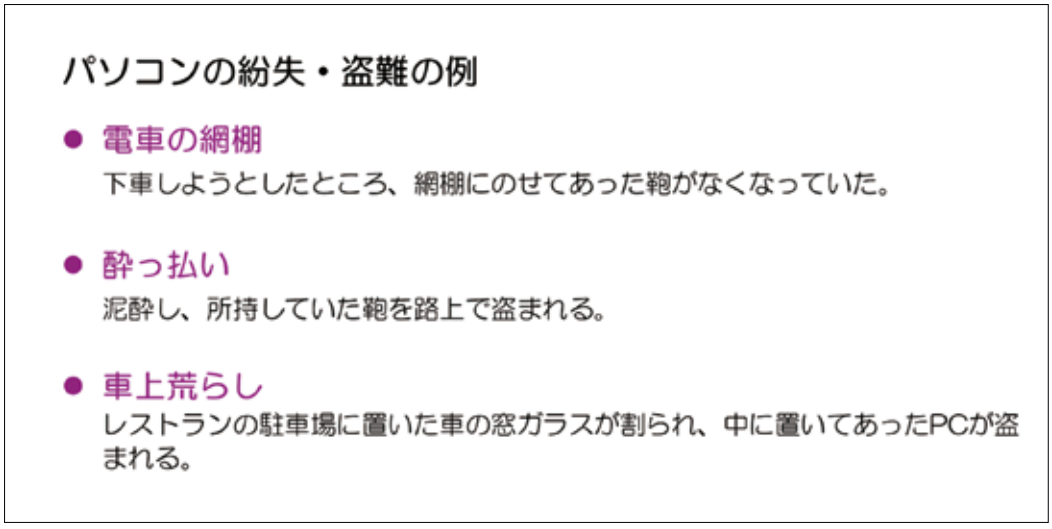
外部記憶媒体、USBメモリーの管理も重要です。当社では、以前はとてもたくさんのUSBメモリーが存在していました。しかし、個人の管理に委ねていたため、鞄に入れたまま持ち歩いたり、机の引き出しにしまっていたりして、いつの間にかなくなるケースがあったので、多くのUSBメモリーを回収しました。代わりにファイル転送サービスを使うよう指導し、どうしてもUSBメモリーが必要な場合は個人管理でなく部門管理として、貸し出し管理をしています。

次に技術的・物理的対策です。当社では、持ち出し用パソコンに自動消去機能を入れています。一定時間の経過など特定の条件でデータが自動的に消える機能です。これにより、パソコンの紛失・盗難による情報漏えいリスクを低減しています。

～モバイルパソコンの紛失・盗難～

モバイルパソコンの紛失・盗難事例を見ると、「酔っぱらい」、電車の「網棚」や「足元」等への置き忘れ、そして「車上荒らし」が目立ちます。

当社の基本的なルールでは、「飲み会にはパソコンを持ち出すな」です。しかし、現実には酒宴の席にパソコンを持っていかなければならないケ



ースもあります。このようなときのために、ボタン一つでパソコンのデータを消去する機能をパソコンにつけています。飲み会の前にパソコンのデータを消せるので、安心してパソコンを持ち運ぶことができます。

～電子メールの誤送信～

ヒューマンエラーで多いのが電子メールの誤送信です。セキュリティベンダの調査では、従業員の６割以上が誤送信を経験しているという結果もあるようです。メールの誤送信は、ちょっとした操作ミスで大量の個人情報が漏洩してしまうおそれがあることです。

メールの誤送信を場合わけすると、主に３つに類型されます。１つ目は「宛先誤り」です。原因のひとつは、オートコンプリートという入力を補完する機能の確認ミスです。例えば「杉森」さんに送ろうとして「杉」と入力したところ、「杉田」さんが表示され、気づかずそのまま送ってしまうケースです。

また、社内の複数の人が同時にやり取りしているメールが自分宛に届き、社内の人にしか送られていないと思い込み一斉返信したところ、実は１人だけお客様が入っていて、社内情報が漏洩してしまうというケースもあります。

２つ目は「添付誤り」です。特にオフィス文書に注意しなければならない要素が多々あります。例えばパワーポイントの場合、過去のファイルを流用して作成すると、ノート欄にあった流用元の情報を消し忘れてしまう可能性があります。また、ワードで過去に作成した議事録を流用すると、これまでの変更履歴が残っていて、過去の議事録の情報が流出してしまう恐れがあります。またエクセルで、表示されていないタブに気づかず、内部情報が入ったワークシートを送ってしまうことにも注意しなければいけません。

最後は「アドレス漏洩」です。宛先を伏せてBCCで送らないといけないところを、TOやCCで送ってしまうケースです。

以上のような誤送信に対してひとつで簡単に解決できる対策はなく、複数の対策を多層的に打っています。

例えば、「宛先誤り」を防ぐためには、宛先に社外のドメインが入っていた場合、「本当に送ってよいのか」という警告をポップアップしたり、社外の宛先を含むメールを一定時間保留したりする機能を導入しています。

また、暗号技術を利用することで、閲覧すべきでない者にはファイルを開かないようにすることができます。例えば、パワーポイント等の文書を特定の人にのみアクセス権を設定する機能です。

「添付誤り」の対策としては、原則オフィス文書をそのまま添付するのではなく、PDF化して送るよう指導しています。ファイル転送サービス（SECURE DELIVER）を利用しています。メールではなく、Webでダウンロードする方式ですが、これでファイルを送り届ければ、自動的に暗号化してくれます。また、誤ったファイルを送った場合も、相手がダウンロードする前に送信者が気づけば削除することができます。

「アドレス漏洩」の対策としては、メール配信ツールを利用しています。一斉に自動配信でき、かつ相手に宛先を見せないツールです。

今ご紹介した以外にも、誤送信抑止につながるツールが多数あると思います。従業員の意識向上は重要ですが、安心のためにはこうしたツールを利用してみてはどうでしょうか。

定型的な業務の中で誤送信が発生する場合は、ファイルの送信手段をメール以外の方法に切り替えるなどの業務プロセスの見直しが必要な場合もあると思います。

～ビジネスメール詐欺～

ビジネスメール詐欺とは、例えば取引先との間で取り決めている送金先口座を、「従来の口座が使用できないので変更してくれ」と、相手に成り済まして送信されるメールによる詐欺です。

ビジネスメール詐欺では、メールアドレスをなりすますケースがあり、例えば本物のメールアドレスの文字列を１文字置き換える、追加するなどをして送ってきます。

このように似せたものではなく本物のメールアドレスで送ってくる場合もあります。この場合は、メールを見て見破ることは困難です。なぜ本物のメールアドレスが使えるのかというと、攻撃者がメールシステムにアクセスするIDとパスワード

を知っていて、本物のメールアドレスから送信しているということが考えられます。

攻撃者は脆弱なシステムから入手したIDとパスワードのリストを保有している可能性があります。IDとパスワードを様々なシステムで流用していると、このように不正にシステムを利用される被害に遭う可能性があります。

詐欺被害を防ぐには、メールアドレスをよく確認する他、メールで入金口座の変更依頼が送られてきた場合は、メール以外の手段で本人確認しなければ口座を変更してはいけないとすることが必要です。

なにをすべきか
③緊急時の対応に備える

～インシデント報告をすることを周知～

緊急時の対応に備えるには、迅速に報告が上がってくるようにしなければなりません。ハインリッヒの法則では、１件の重大事件の背後には、ちょっと危なかったというヒヤリハットが300件ぐらいあると言われています。軽微な問題も報告することを習慣付け、日頃から再発防止に取り組むことで、重大事故に発展することを防ぐことが必要と考えています。

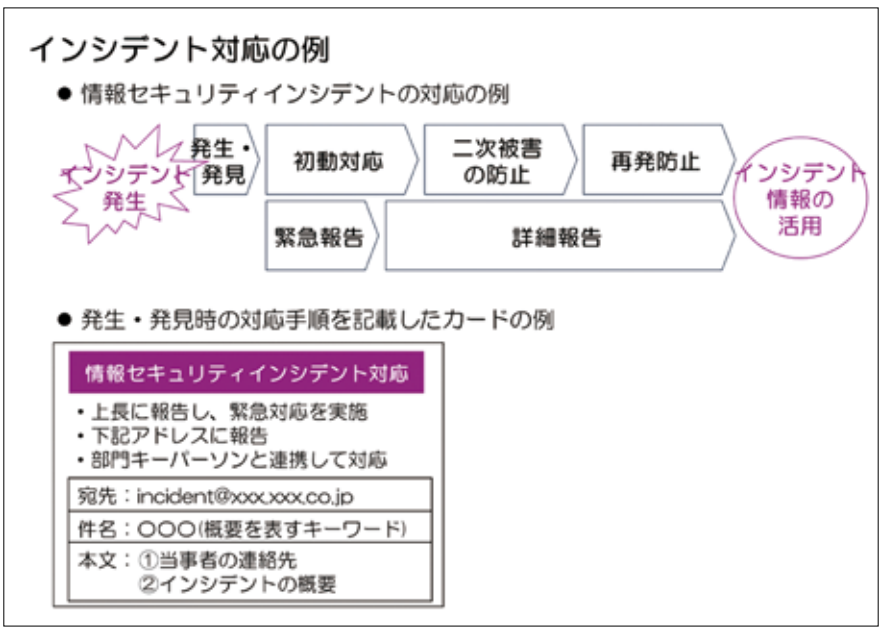
従業員は報告手順が記載された、所定のカードを所持しています。「何かあれば報告するように」と伝えています。人には正常性バイアスがあり、大変なことに遭遇しても不安感を拭い平静の状態でいようとするのだそうです。従って、重大事が否かを当事者は冷静に判断できないおそれがあるので、迷ったら報告することが必要です。

～情報セキュリティ訓練～

また、サイバー攻撃に備えた訓練も有効です。皆様も、会社等で防災訓練を行われたりしていないでしょうか。サイバー攻撃に対しても、日頃から攻撃に備えた訓練を行っていることで、いざというときに効果を発揮します。

当社では、サイバー攻撃のシナリオをあらかじめ作り、どのように対応すれば良いかを考える机上演習を行っています。

机上演習することで、「直ちにお客様にお詫びしなければいけない」、「乗っ取られた原因を突き止めないと、個人情報の漏えいが継続するおそれがある」、「システムを止めないといけない」、「システムは誰の権限で止めることができるのか？」、「システムを停止するならアナウンスが必要だ」等、課題が抽出されます。机上演習によって、課題への対応を事前に考えておくことができます。



サイバー攻撃訓練の実施について

- 防災訓練や大規模地震対応訓練と同じように、サイバーセキュリティも訓練を実施
- サイバー攻撃のシナリオによるCSIRT訓練により、初動対応の課題発見・改善に結び付ける
- 全従業員が不審メール訓練を実施し、不審メールの見破りポイントの習得、開封時の初動対応を実践

	<参考> 大規模地震 を想定した訓練	サイバー攻撃 を想定した訓練
司令塔機能の訓練	本部訓練	攻撃発見時の CSIRT訓練
現場・従業員の訓練	安否確認訓練	不審メール 対応訓練

サイバー攻撃訓練の例

- CSIRTのインシデント対応力向上のため、様々なリスクシナリオによる訓練

月度机上訓練の実施状況

訓練シナリオ
公式サイトからの個人情報漏洩
フィッシング攻撃
内部不正による個人情報漏洩
大規模ランサムウエア感染
内部不正による個人情報漏洩
公式サイトの改ざん
DDoS攻撃
受託業務における情報流出

訓練からの学習

なにをすべきか ④委託に関する責任を明確にする

委託に関する責任を明確にするためには、委託先の情報セキュリティがどうなっているかを確認しておくことが必要です。安いからといって委託した業者のサービスが、じつはセキュリティの脆弱性対応がずさんで、攻撃をうけ被害が生じる可能性もあります。業者に委託する際は、実績や契約内容をきちんと確認した上で契約しなければいけません。

なにをすべきか ⑤最新動向を収集する

最新情報を収集するためには、情報セキュリティのコミュニティーに参加することも必要です。

印刷組合等の同業者のコミュニティーも有益です。同業他社のセキュリティスタッフとの交流の機会を定期的に設け、セキュリティに関しての情報交換を行っています。

さいごに

これまでリスクマネジメント全般に取り組んできた私が最も重要だと思うのは、万が一事故が起きてしまった場合、「空振りは許されるが、見逃しは許されない」という考え方です。疑わしきときは行動する、最悪の事態を想定して行動することが大事だと思っています。

本日のような金曜日の夜、同僚と飲んでいる最中に電話かかかってくることもあります。せっかくの週末、月曜日に対応したいと思ってしまいがちですが、後回しにすることで、後で大変な事故に繋がる可能性もあるのです。会社に戻って状況を把握した結果、問題なく空振りだったことの方が圧倒的に多いですが、それはそれで「よかった」で許される、そういうことです。

長時間おつき合いいただき、ありがとうございました。

（文責・編集委員会）

秋になると、外で遊んでいるこどもたちが、木ノ実や様々な色に染まった葉っぱ、小枝や虫が食べた後の枯葉を、嬉しそうに見つけ、手に取り、家族や友達に色んな発見を伝える姿が見られます。枯葉や木ノ実を求めて、たくさんの虫も鳴き始めます。日が暮れてしまうのは早いから、明るいうちにいろんな発見をしに外へ出かけよう！

京都造形芸術大学こども芸術学科3年次生　曽田みなみ