利用者教育こそがセキュリティ強化への道

信越ポリマー株式会社

■ 執筆者Ｐｒｏｆｉｌｅ ■

明島　末依

2013年　信越ポリマー（株）入社
2016年　現在 管理本部情報システム部所属
　　テクニカル担当

■ 論文要旨 ■

巧妙さを増していくサイバー犯罪の被害から身を守るため、システム利用者はセキュリティに対していつまでも”他人ごと”であっては許されない。利用者の自己防衛ができて初めて、組織全体の強化を実現することができる。

私は業務対応を行う中で、管理者だけではなく、利用者自身もセキュリティに対して常にアンテナを張っていかなければならないことに気が付いた。そこで情報システム部門(以下、情シス部門)とのコミュニケーションの場を活用することで、システムに関心を持つきっかけをつくると同時に、全社的な啓蒙活動を行った。セキュリティ対策に終わりはない。利用者と情シス部門間の積極的なコミュニケーションを通じ、我々を取り巻く脅威に対して個人が自立的な判断で行動できる、強い組織を今後も目指していく。

■ 論文目次 ■

１．はじめに ……《 3》

２．組織を取り巻く脅威 ……《 5》
２．１　外部からのリスク
２．２　内部のリスク

３．管理者と利用者のセキュリティ対策……《 7》
３．１　管理者の対策
３．２　利用者の対策

４．利用者とのコミュニケーション……《 8》
４．１　データベースの活用
４．２　PCアドバイザー制度の導入

５．標的型攻撃メールの訓練実施……《 12》
５．１　訓練の主旨
５．２　利用者への効果
５．３　今後の対策

６．結論 ……《 14》
６．１　現在の課題
６．２　今後の課題

■ 図表

表１　2005年～2008年 情報セキュリティ10大脅威……《 3》
表２　2012年～2014年 情報セキュリティ10大脅威……《 4》
表３　2016年 個人・組織別の情報セキュリティ10大脅威……《 5》

図１　ランサムウェアによって暗号化されたファイル……《 6》
図２　メールの件名に[GRAYMAIL]と表記……《 6》
図３　システム作業依頼……《 9》
図４　システムQ&A……《 9》
図５　かわら版……《 10》
図６　PCアドバイザー制度告知のチラシ……《 11》

１． はじめに

企業を標的としたセキュリティ脅威は年々深刻になってきている。昨今、社会的に影響のあるインシデントが報道されたことにより、企業もセキュリティ対策で奔走しているのが現状だ。次の表1,2は独立行政法人 情報処理推進機構による、年ごとの情報セキュリティ10大脅威についてまとめた表である。約10年前と現在を比較して組織を取り巻く脅威の特徴について傾向を考察したい。

順位	2005年	2006年	2007年	2008年
1位	事件化するSQLインジェクション	漏えい情報のWinnyによる止らない流通	高まる「誘導型」攻撃の脅威	DNSキャッシュポイズニングの脅威
2位	Winnyを通じたウイルス感染による情報漏えいの多発	表面化しづらい標的型(スピア型)攻撃	ウェブサイトを狙った攻撃の広まり	正規ウェブサイトを経由した攻撃の猛威
3位	音楽CDに格納された「ルートキットに類似した機能」の事件化	悪質化・潜在化するボット	恒常化する情報漏えい	巧妙化する標的型攻撃
4位	悪質化するフィッシング詐欺	深刻化するゼロデイ攻撃	巧妙化する標的型攻撃	検知されにくいボット、潜在化するコンピュータウイルス
5位	巧妙化するスパイウェア	ますます多様化するフィッシング詐欺	信用できなくなった正規サイト	恒常化する情報漏えい
6位	流行が続くボット	増え続けるスパムメール	検知されにくいボット、潜在化するコンピュータウイルス	脆弱な無線LAN暗号方式における脅威
7位	ウェブサイトを狙うCSRFの流行	減らない情報漏えい	検索エンジンからマルウェア配信サイトに誘導	誘導型攻撃の顕在化
8位	情報家電、携帯機器などの組込みソフトウェアにひそむ脆弱性	狙われ続ける安易なパスワード	国内製品の脆弱性が頻発	減らないスパムメール
9位	セキュリティ製品の持つ脆弱性	攻撃が急増するSQLインジェクション	減らないスパムメール	組込み製品に潜む脆弱性
10位	ゼロデイ攻撃	不適切な設定のDNSサーバを狙う攻撃の発生	組み込み製品の脆弱性の増加	ユーザIDとパスワードの使いまわしによる危険性

凡例：

脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネット バンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン 関連

（出展：IPA情報セキュリティ10大脅威2016【資料1】）
表1 2005年～2008年情報セキュリティ10大脅威

表1の2005年から2008年にかけては、システムの脆弱性を狙うサイバー攻撃が目立つ。事象からも専門的な技術を持つ人間が企業や組織を対象にした犯行に及んでいることが読み取れる。さらにYouTubeやニコニコ動画などの利用者参加型動画サイト、iPhoneやAndroidといったスマートフォンの登場も相まって、この時期はインターネットへアクセスする敷居が下がった。このように企業から個人に至るまで利用環境が整ったことで、サイバー空間がどの利用者においても重要な基盤となった。インターネット利用人口増加に伴い、組織だけでなく、個人を狙った標的型攻撃の脅威もこの頃から顕在化してきたという特徴が見受けられる。

順位	2012年	2013年	2014年
1位	クライアントソフトの脆弱性を突いた攻撃	標的型メールを用いた組織へのスパイ・諜報活動	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
2位	標的型諜報攻撃の脅威	不正ログイン・不正利用	内部不正による情報漏えい
3位	スマートデバイスを狙った悪意あるアプリの横行	ウェブサイトの改ざん	標的型攻撃による諜報活動
4位	ウイルスを使った遠隔操作	ウェブサービスからの利用者情報の漏えい	ウェブサービスへの不正ログイン
5位	金銭窃取を目的としたウイルスの横行	オンラインバンキングからの不正送金	ウェブサービスからの顧客情報の窃取
6位	予期せぬ業務停止	悪意あるスマートフォンアプリ	ハッカー集団によるサイバーテロ
7位	ウェブサイトを狙った攻撃	SNSへの不適切な情報公開	ウェブサイトの改ざん
8位	パスワード流出の脅威	紛失や設定不備による情報漏えい	インターネット基盤技術を悪用した攻撃
9位	内部犯行	ウイルスを使った詐欺・恐喝	脆弱性公表に伴う攻撃
10位	フィッシング詐欺	サービス妨害	悪意のあるスマートフォンアプリ

凡例：

脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネットバンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン関連

（出展：IPA情報セキュリティ10大脅威2016【資料1】）
表2 2012年～2014年情報セキュリティ10大脅威

これに対し2012年から2014年にかけては、金銭目的の個人情報窃取が目立つようになり、スマートフォンの利用者を狙う攻撃も顕在化してきたことが特徴である。スマートフォンが世の中に普及したために、現在ではどこでも誰とでも手軽にコミュニケーションができる環境が整った一方で利用者のITリテラシー欠如も伴い、誰でもサイバー犯罪の加害者あるいは被害者になりうる可能が生じてきたとも言える。加えて犯罪の背景には政治的な意思主張を目的で犯行に及ぶハクティビストも出現してきたという特徴がある。

このようにわずか10年で攻撃者と犯罪目的や規模に変化が生じており、現在、サイバー空間で利用者はセキュリティに関してリスクを考えながら行動する必要がより一層高まってきている。ITを取り巻く世界は変化が目覚ましく、便利になった分だけ利用者が背負うリスクも増加の一途を辿るであろう。自分の力で考え、問題を解決していこうとする姿勢―まさにセキュリティに関して自立的な思考ができる環境を整えることが私たち情シス部門の役目だと私は考える。

信越ポリマー株式会社は、塩化ビニル樹脂やシリコーンゴムの加工技術で、電子機器や半導体関連製品から建設関連製品に至るまで多岐に渡る製品を提供している。取り扱う製品もさることながらバックグラウンドに関しても豊かな人材が集う当社ではセキュリティに対してどのような対策を講じているか述べていきたい。

２．組織を取り巻く脅威

現在、実際にどのような対策が組織で施されているのであろうか。
個人を対象にした攻撃では直接的な金銭目的の脅威が特徴的であるが、組織における脅威は“機密情報”の窃取を目的としたものが多いことに着目してほしい。

■「情報セキュリティ 10 大脅威 2016」個人別・組織別　順位

（ ）内は総合順位、（－）は総合順位でのランク外です。

個人（カッコ内は総合順位）	順位	組織（カッコ内は総合順位）
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）	1 位	標的型攻撃による情報流出（2 位）
ランサムウェアを使った詐欺・恐喝（3 位）	2 位	内部不正による情報漏えい（8 位）
審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ（7 位）	3 位	ウェブサービスからの個人情報の窃取（4 位）
巧妙・悪質化するワンクリック請求（9 位）	4 位	サービス妨害攻撃によるサービス停止（－）
ウェブサービスへの不正ログイン（5 位）	5 位	ウェブサイトの改ざん（6 位）
匿名によるネット上の誹謗・中傷（－）	6 位	対策情報の公開に伴い公知となる脆弱性の悪用増加（10 位）
ウェブサービスからの個人情報の窃取（4 位）	7 位	ランサムウェアを使った詐欺・恐喝（3 位）
情報モラル不足によるサイバー犯罪の低年齢化（－）	8 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）
職業倫理欠如による不適切な情報公開（－）	9 位	ウェブサービスへの不正ログイン（5 位）
インターネットの広告機能を悪用した攻撃（－）	10 位	過失による情報漏えい（－）

（出展:IPA情報セキュリティ10大脅威2016【資料2】）
表3 2016年 個人・組織別の情報セキュリティ10大脅威

2014年7月には通信教育大手の内部犯行による機密情報窃取が発覚し、2015年6月には日本年金機構における標的型攻撃メールによる個人情報の流出が発覚した。今まで当たり前に”安全”と信用してきた組織からセキュリティ事故が生じたことで、情報資産を取り巻いている潜在的な脅威が世間に認知されるきっかけとなった。このような脅威を組織の外部と内部に分類して考察していきたい。

２．１　外部からのリスク

組織外部からのリスクとして想定されるのは、ウィルス感染である。
メールの添付ファイル開封をきっかけに、パソコンへウィルスを感染させるサイバー攻撃を例に挙げると、被害は一時点だけの事象に留まらない。その上、攻撃の方法としても被害が顕在化しているものと潜在化しているものがある。前者がランサムウェアで、後者は標的型攻撃メールだ。ランサムウェアとは、本人の意思とは関係なく、利用者のパソコンにプログラムをインストールし、攻撃者からの遠隔操作によってパソコン内のファイルを暗号化してしまうマルウェアである。データを復元するためには金銭を支払わなければならないといった警告がなされることから、ransom(身代金)+software(ソフトウェア)の造語で呼ばれている手口である。データが暗号化されたという明確な事実があるため、利用者

自身でサイバー攻撃の被害者になったことを判断することができる。

当社でも中国圏の利用者がメールに添付されたランサムウェアのプログラムを実行してしまい、2016年8月,9月で合計2件、ローカル上のデータが暗号化された事象を確認している。1回目の事故においては、不審なメールの添付ファイルを5名が開封したことで、合計で106,465件のExcelファイルが暗号化された。図１は、実際にファイルが暗号化され、拡張子が.zeptoになってしまったファイルの一部である。

名称	修改日期	类型	大小
4CDB4C0A-F3A2-35B9-2EDC-4B952956C5A2.zepto	2016/8/2 9:34	ZEPTO 文件	316 KB
4CDB4C0A-F3A2-35B9-3AFC-840C09F03FDA.zepto	2016/8/2 9:37	ZEPTO 文件	549 KB
4CDB4C0A-F3A2-35B9-3F83-7B3D2C49327F.zepto	2016/8/2 9:33	ZEPTO 文件	21 KB
4CDB4C0A-F3A2-35B9-05E5-2ECBFF3A3BFC.zepto	2016/8/2 9:34	ZEPTO 文件	32 KB
4CDB4C0A-F3A2-35B9-5A9B-3F9200539DBD.zepto	2016/8/2 9:33	ZEPTO 文件	399 KB
4CDB4C0A-F3A2-35B9-6DA1-1E29EC1FD736.zepto	2016/8/2 9:34	ZEPTO 文件	15 KB
4CDB4C0A-F3A2-35B9-8D34-1956DA8392DE.zepto	2016/8/2 9:37	ZEPTO 文件	85 KB

図1 ランサムウェアによって暗号化されたファイル

2回目の事故においては、200,000を超えるExcel、Word、Powerpoint、PDFのファイルが無作為に暗号化された。データの復旧に関しては、メールを開封した同一ネットワークのパソコン全件をウィルス対策ソフトでスキャンし、別箇所に保存していた前日までのバックアップから復旧している。利用者へは不審なメールを絶対に開封しないよう教育した他、迷惑メールフィルターに加えて正規のメールかどうか判断が難しい受信メールに関しては図２のように件名に[GRAY MAIL]と追加表示するようにして、視覚的な注意を促した。

Roxie Hardin	[GRAYMAIL] Corrected report	昨日 20:56	15K
Marcos Briggs	[GRAYMAIL] Corrected report	昨日 20:58	15K
Mariano Rose	[GRAYMAIL] Corrected report	昨日 21:00	15K
Forest Barron	[GRAYMAIL] Corrected report	昨日 21:26	15K

図2 メールの件名に[GRAYMAIL]と表記

これに対し、何が攻撃対象とされているかを把握することが難しい脅威が標的型攻撃メールだ。攻撃者がウィルスに感染させたパソコンを踏み台として組織のネットワークへ侵入する部分まではランサムウェアと共通するが、長期間に渡って潜伏して機密情報を窃取していく場合もあるため、被害自体を把握しにくい。当社では、現在までに標的型攻撃メールを開封した事実を確認していないが、こうした脅威に対して注意喚起を促すための訓練を行っている。当然のことながら外部ネットワークとの接続についてはファイアーウォールやウィルス対策ソフトの導入によりアクセス先を制限しているが、これに加えてパソコンやサーバを踏み台として外部へ接続しようとするC&C(コマンドアンドコントロール)攻撃など、自社では検知しづらい脅威の監視を外部機関へ依頼し、サイバー攻撃に対して多層化した防御体制を構築している。

２．２　内部のリスク

組織内部のリスクとして想定されるのは、情報資産の取り扱いに対するヒューマンエラーである。近年、社員が企業の機密情報を窃取し、売買した問題が大きく報道されたことをきっかけに、内部犯行が組織の信頼を損なう恐れのある大きなリスクとして認識されたことは記憶に新しい。言うまでもなく、会社で扱う情報はすべて会社の資産だ。システム利用者にとって身近な情報資産のパソコンを例に挙げると、当社ではセキュリティ対策として以下の対応を施している。紛失した際の情報流出防止を目的として、全モバイル用のパソコンのハードディスクを専用ソフトで暗号化している。この仕組みにより、パソコンの盗難もしくは紛失によるデータ流出事故は現在に至るまで発生していない。加えて日常的に使用するツールから社外への情報流出も避けたい。当社では、送信メールをサーバ上に5分間滞留してから外部へ送信する、メール誤送信防止を目的としたサービスを情シス部門内で試験的に運用している。これは組織外の宛先に向けたメールを即時に送信しないことで、メールの内容や宛先に誤りがあった場合、滞留時間内であれば送信を中止することができる内容となっている。私がこれまでこのサービスを利用した感覚では、宛先を間違えたなど余程のことがない限り日常的にメリットを感じたとはない。しかし情報流出の予防策として送信メールについて誤りがないか再度確認する時間を設けたと捉えると有効的な機能と考えられる。現在部内において利便性と効果を検証中だ。

このように組織内外のリスクは、利用者によるシステムの誤操作が起因して生じる共通性がある。

３．管理者と利用者のセキュリティ対策

組織における対策はシステム管理者向けと利用者向けで行うべきものは異なる。それぞれがセキュリティに対して受け身ではなく、積極的に必要なアクションをとる姿勢が脅威へ対抗する最大の防御であると私は考える。

３．１　管理者の対策

先の章では利用者側のシステム対策を紹介した。ここでは管理者側の対策を講じたい。管理者のセキュリティ対策としても各自が役割に応じた業務を着実に積み重ねていくことが有効である。

当社の情シス部門は企画、ヘルプデスク、開発、テクニカルの4チームで構成しており、それぞれが役割を分担している。例えばセキュリティ事故が起きたことを想定すると、ヘルプデスクチームが利用者からの問い合わせを受け、テクニカルチームが事故の起きた原因を追究し、対策を講じる。事故対応が終了したところで開発チームが作成したグループウェア上の共有データベースへ企画チームが再発防止策を社内に対して発信する。このように業務内容を分担しておくことで、緊急時にも各自が連携して対応をスムーズに遂行することが可能だ。業務分担だけでなく、パソコン以外の機器に対して管理をきちんと行うことも情シス部門の重要な役目である。平易なことではあるが、プリンターやアクセスポイント、サーバなど機器を更新する期間の長いものに関してはIDとパスワードを初期設定のままにして運用しない、パソコンやスマートフォンの運用については管理者と利用者の権限で利用できるサービスを分ける、インターネットへ接続されている機器へ修正プログ

ラムを随時適用するなど、身近ではあるが見落とされがちな機器の管理からしっかりと対策を講じていくことが、結果として組織全体の脆弱性対策へつながると私は考える。

３．２　利用者の対策

サイバー空間における脅威を”自分のこと”と当たり前に捉えることができる習慣を目指し、システム利用者は情報資産に対する理解と扱い方を正しく解釈することが重要だ。利用者に対しても管理者と同じく、身近な事象から始めることが求められているのではないだろうか。配属時に教育を受けているにも拘らず、利用者の大半は使用するソフトウェアの業務上の位置づけや効率的な操作方法を知らない。そのため、システムに関する問い合わせを受けた際、私はマニュアルを渡すだけでなく利用者のもとへ足を運び、利用しようとしている仕組みの”意味”と”目的”から理解できるよう説明を工夫している。これは、システムへ関心をもつことを目的としただけでなく、情シス部門担当者の顔を覚えてもらい、日常的に相談しやすい環境をつくることを意識しているためだ。「明島さん、これ教えてくれる？」「この間教えてくれたことを試してみたいのだけれど、もう一回教えて」などといった問い合わせが来たときは、やりがいを感じるひとときだ。信頼関係が構築され始めたことを実感するとともに、利用者が課題に対して”自分”でどうにか対応しようと踏み出した瞬間と感じるためである。普段からコミュニケーションをとることは、利用者がどこへシステムに関して連絡や相談をしたらよいかを確認できるため、私は大変重要なことであると考える。例えばウィルスが添付されたメールを受信し、開封してしまった場合、利用者や情シス部門の知らない間に外部からの攻撃が内部へ拡散してしまう可能性がある。利用者が日常的に相談窓口を認識していれば、有事の際の初動対応を迅速に行うことができ、サイバー攻撃による被害を最小限に食い止めることが可能だ。

加えてシステムだけでなく、会社で扱う情報資産についても理解を促したい。当社では入社した社員全員へ向けてセキュリティ教育を行っている。昨今のサイバー犯罪のトレンドから始まり、会社で想定される脅威への対策や事故発生時の対応手順、身近な情報資産の取り扱いなどを2時間程度で解説するといった内容だ。会社の入り口に立っている社員への教育をしっかり行うことこそが組織全体の意識改革へ波及していくきかっけとなると私は考えるため、社員一人一人に合わせたアプローチを今後も工夫していきたい。

４．利用者とのコミュニケーション

ここでは利用者とのコミュニケーションの手段を具体的に述べたいと思う。

４．１　データベースの活用

当社ではグループウェアとしてIBMのNotesを利用しており、その中のデータベースをカスタマイズして運用している。テーマの進捗情報を可視化したことで、関係者がリアルタイムで業務の状況を確認可能な条件を整えた。利用者・情シス部門・全社で使用するデータベースを例題にして以下に紹介していきたい。

① 利用者が情シス部門に対して使用するデータベース

以下の図３に示したシステム作業依頼を例とする。このデータベースの利点はテーマの進捗状況を利用者がリアルタイムで確認でき、情シス部門では依頼内容に応じて人員を効率よく割り振ることができる点である。さらに、利用者は過去事例を参照することができるため、類似案件に関して申請手続きの煩雑さも和らげることが可能となっている。

No.572D0125

システム作業依頼

申請部門記入欄

依頼日	2016/10/27	ｼｽﾃﾑ ｶﾃｺﾞﾘ	『その他』	状況 （承認中）	受付
依頼者	[redacted]	会社	『SJ』	部門	『営業本部長室』
ITリーダ	[redacted]	責任者（部門長）	[redacted]	稼動希望日	『2016/10/28』
業務名称	『モバイルコネクトインストール依頼』				
依頼内容	『 iPhoneへのインストールをお願いします。 対象者：営業本部長室 [redacted] 端末は到着済、作業は10/28午前中の希望です。※メールアドレスですが、別途、明島さんにご連絡致します。 』				
定性効果	『 』				
定量効果	金額削減（円）：『 』　期間短縮（日）：『 』　工数削減（人/月）：『 』				
計算根拠	『 』				

添付ファイル　『 モバイルアクセス申請書.pdf 』

図3 システム作業依頼

② システム部門から利用者に対して情報を発信していくデータベース

以下の図４に示したシステムQ&Aを例とする。これは利用者からヘルプデスクが受け付けた質問や課題へ対する回答をまとめたもので、作業依頼のデータベースと同様に全てのNotes利用者が参照可能だ。緊急時以外は同様の質問があるかどうかこのデータベースをまず確認してから情シス部門へ連絡するように全社的に呼びかけており、ヘルプデスクの負担軽減を目指している。

16日	No. 521Q0122	対応中	GPS	RC- Ribbon Report show repeated data	調査中
5日	No. 521Q0109	対応中	SMaRT	目標と実績原価差異の見方を教えてください	調査中
10日	No. 521Q0064	対応中	Notes	受信エラー	ユーザーで受信拒否リストを確認する方法はありません。
26日 ▶	No. 521Q0052	対応中	GPS	Separate the WIP status within OA1 and OA2 at Local Info System	もう少し詳しく記入お願い致します。
21日	No. 512Q0199	対応中	GPS	Error when creating operation logsheet	もう一度試した結果を教えて下さい。
1日	No. 502Q0004	対応中	SMaRT	PO not showing User ID	Bugs in the program
26日	No. 572Q0040	対応済	仮想デスクトップ	仮想デスクトップの問題	サーバーを再起動します。
26日	No. 572Q0039	対応済	Notes	NOTESの問題	Kドライブ上のノーツフォルダが一部消されているようです。
26日	No. 572Q0038	対応済	SMaRT2	SCASとSMaRTに登録されている経費支払先で重複しているコード、一定期間取引の無いコードを調べ	有効な手立てはありません・・・
26日	No. 572Q0037	対応済	SMaRT2	インボイス発行ができない	こちらの設定が不十分でした、申し訳ありません。
24日	No. 572Q0035	対応済	その他	安否確認システム	社長室にお問い合わせください。
20日	No. 572Q0034	対応済	Notes	Notes-Folder missing	別途、電話でご連絡ください。
19日	No. 572Q0033	対応済	GPS	製造指図書の内容異常	指図書の見出しがずれていました。
18日	No. 572Q0032	対応済	SMaRT2	Packing List出力　Excelファイルが	GUIの設定が適切ではなかったようです。
18日	No. 572Q0031	対応済	SMaRT2	SAからのPO、顧客添付用のInvoiceが出力出来ません	572Q0032と同様。
18日	No. 572Q0030	対応済	Notes	ノーツ　ブックマークカレンダーを利用したい	Bookmark.nsfを作り直してみてください。
18日	No. 572Q0029	対応済	Notes	RC/TOEF/2005 でInput Approval ボタンが表示されない	Judgement欄に値を設定してください。

図4 システムQ&A

③ 全社的に使用するデータベース

以下の図5に示したかわら版を例とする。これはすべての利用者が参照し、編集できるデータベースである。管理部門の更新頻度が高く、人事発令からシステムメンテナンスの予定に至るまで全社的なメッセージの発信が主な用途だ。情シス部門ではシステムメンテナンスに加え、流行しているサイバー攻撃に対して注意喚起を促すメッセージ発信を以前から行っている。

SMaRTメンテナンスのお知らせ(SMaRT is out of service)

各位

日頃、情報システムの運用にご理解とご協力をいただき、ありがとうございます。
下記の日程で、SMaRTのサーバーメンテナンスを予定しております。
期間中は、システムのご利用ができませんので、あらかじめご了承ください。

日時: 11/12(土) 12:00 ～ 11/13(日) 20:00
　　 11/19(土) 12:00 ～ 11/20(日) 20:00
対象: SMaRT本番機(CL100)

ご協力お願いいたします。

情報システムG
ヘルプデスク

Dear all members,

We would like to inform you that we had scheduled maintenance of SMaRT as below.
During the maintenance, CL100 will be unavailable.

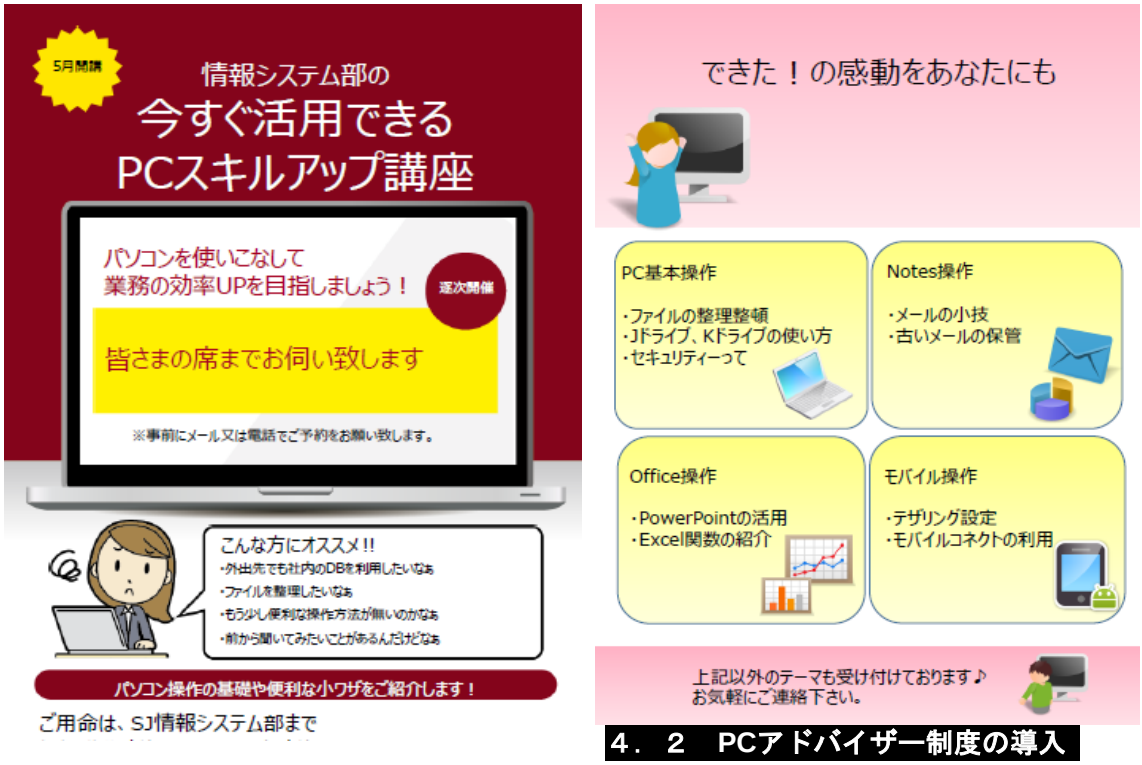
Date:　　Nov. 12(Sat.) 12:00 - 13(Sun.) 20:00 (JST)
　　Nov. 19(Sat.) 12:00 - 20(Sun.) 20:00 (JST)
Subjects:　SMaRT Production Server(CL100)

Thank you for your understanding and co-operation.

Information System Group
Helpdesk

図5 かわら版

その他にも会議室予約や業績目標など、種類は多岐に渡るが、このNotesのデータベースにおいて文書でコミュニケーションを行う点は共通している。どこにどのような内容が掲示されているか、困ったときや依頼事項がある時はどのように申請を行えばいいかといった利用者の疑問に対して、適切な情報源の”ありか”と”手順”、”窓口”を周知させることも我々情シス部門の役目である。既存のシステムの利用を強制するのではなく、利用者に寄り添った対応を今後も努めていきたい。



4．2　PCアドバイザー制度の導入

図6 PCアドバイザー制度告知のチラシ 左:表紙　右:裏面

PCアドバイザー制度は利用者のITスキル向上を目的に、情シス部門の広報活動の一環として2015年5月より開始した取り組みである。利用者とコミュニケーションをとることで個々の事業部におけるITの課題や取り組みを把握でき、結果として全社的なセキュリティの担保へ貢献できる点でも重要な活動であると私は考えている。現在、デバイスやセキュリティの管理を情シス部門が一貫して行っているが、一方的な運用方法になってしまっては利用者のITに対する潜在的な要望を把握することが出来ない。ITに関する質問を突破口に接点を持ち、利用者の元へ足を運ぶことで、現場ではどのようなことをITで実現したいのかを垣間見ることができる。例えば新しいソフトウェアの導入をしたい場合を想定すると利用者の要望実現に向けて事前に全社的なセキュリティへの影響が確認できていれば、安全で効率的な導入が可能となる。この取り組みを通じて、利用者と情シス部門両者がWin-Winな関係を構築できることを目指している。

一方で、情シス部門への問いあわせの大半はシステムの基本的な使い方に関するものである。アドバイザーは私を含む2名で構成しており、パソコンやソフトウェアの使い方などの質問に対し、テーマを決めて一つ一つ丁寧回答していく座学形式の取り組みを行っている。これまで行った8回開催した講習では、Windows標準の機能でもあるリモートデスクトップの使用方法や過去メールをローカルに保存する方法などのテーマを扱った。簡単なことからではあるが、身近なソフトウェアの操作方法の理解を通じ、業務効率化の体感する喜びを利用者に体感してもらうことでITリテラシーの向上も目指している。ITリテラシーが向上することで利用者自身のセキュリティに関する自己防衛力も高めることができる。

講習後は利用者からの評判も上々であり、口コミや紹介で次の講座開催に至っている。昨今流行しているセキュリティの脅威や対策、スマートフォンやタブレットなど新たなデバイスの操作方法についても啓蒙し、少しでも利用者がITに対して”自分のこと”に感じてもらうよう心掛けている。このPCアドバイザーをきっかけに、システムのことを知らないから”恥ずかしい”のではなく、知らないから”覚えよう”という意識の変化がもたらされることを期待している。まだ始めたばかりの試みであるが、今後もこの活動を通じて教育を行うだけでなく利用者からシステムへの要望も伺い、より良いコミュニケーションの場の構築を目指したい。

しかしながら、海外や国内の遠隔拠点においてはこのようなきめ細かい対応ができていない現状がある。当社では、情シス部門への依頼事項のとりまとめや利用者支援などの日常業務の補助を目的として、各事業部ごとに“ITリーダー”を１名ずつ配置している。国内拠点は情シス部門がデバイスからシステムに至るまで一貫して運用を行っているが、海外拠点ではパソコンの手配からセットアップ、サーバーの管理までをこのITリーダーが担当している拠点も存在し、セキュリティポリシーにバラツキが生じてしまっている現状がある。我々情シス部門が普段顔を出すことができない遠隔拠点に至っては、利用者との日常的な対面コミュニケーションは難しい。今後の課題は場所にかかわらず同一のケアができる体制の構築であり、実現のためには各拠点のITリーダーの教育と共通の指針の普及から始めたいと考えている。

５．標的型攻撃メールの訓練実施

口頭や文章でセキュリティの説明を受けても、実感をもって理解することは難しい。したがって近年注目度の高い”標的型攻撃メール”の訓練を国内グループ会社10社を対象として2015年8月～9月に2度実施した。尚、部内で事前にヘルプデスクを筆頭にメール配信から試験後の利用者の対応まで流れを確認し、部内のみで内容を共有する運用方針を徹底した。下記に実施手順を記す。

1)事前準備

本物の標的型攻撃メールの傾向に合わせた道具を以下の通り用意した。

① 配信元

フリーメールアドレスを用意し、情シス部門を装った送信元の表示をさせる。

② 文面

受信者の大半が興味を示すような内容で、3つのテーマを用意する。

③ 添付ファイル

パスワードなしで圧縮したプログラムファイルを用意し、実行された瞬間に情シス部門へ通知が送信され、利用者へは訓練メールであるというメッセージを表示するように設定する。

2)訓練の周知

多くの問い合わせが殺到しないように、事前に訓練を行う旨を全社的にアナウンスする。問い合わせが来た際に、訓練実施期間中は他の人へ口外しないことを伝えるなど情シス部

門内で対応マニュアルを作成する。
3)訓練メールの配信とフィージビリティ(実行可能性)の確認
メール配信後に指定した宛先への到達可否・添付ファイルの開封検知可否を確認する。

4)種明かしメールの配信
訓練終了後に今回のメールは訓練であり、添付ファイルについては無害であることや不審なメールに関する注意ポイント、開封してしまった時の対応手順を指導する。

５．１　訓練の主旨

今回は訓練であったが、同様のメールを実際に受信することを想定し、どのようなメールで何をしてはいけないかに関して利用者へ理解を促す。その上で添付ファイルを実行してしまった際は速やかに情シス部門へ報告し、セキュリティ事故が起こった時の対応手順の確認を目的とした。

５．２　利用者への効果

訓練は同一の従業員を対象に全2回行った。1回目の添付ファイル開封率は全被験者の26.5%であった。開封者が多かったメールの文面は、”ウィルス感染の恐れあり”や”社員研修”などといった受信者の多くが関心を示す内容が目立ち、興味本位で開封してしまった利用者も多く見受けられた。訓練後、不用意に添付ファイルを実行しないために、送信者・メール本文・事故発生時の連絡手順の確認を中心とした内容の講習を全体に対して数回開催し啓蒙活動を行った。続く2回目の訓練では、情シス部門への問い合わせ数も1回目の訓練時と比較して46%減少し、ファイル開封率も全被験者の16.5%へと減少した。尚、2回の訓練とも連続してファイルを開封してしまった者は全2回に渡る被験者のうち6.2%であった。2回目の開封率が1回目より低いことから、利用者がセキュリティに対する危機意識を”自分のこと”として理解し、対応することが出来た割合が増えたと考えられる。

５．３　今後の対策

利用者にとって日常的に使用するコミュニケーションツールはやはりメールである。社外の機関とも連携した研究を通じ、より実践的な内容に基づいた訓練を今後も定期的に実施することで、引き続き利用者の当事者意識を高めていきたい。2015年は関連会社を含めた国内の社員のみを対象にしていたが、今後は海外関連会社、特にアジア圏へも対象を拡大していく予定である。情シス部門では、グループ全体で常に開封者を5%以下にすることを目標に一連の啓蒙活動を行っている。今回の訓練をきっかけに、セキュリティ事故へつながる可能性の高い事象が生じてしまった際は個人を特定するのではなく、事態を素早く報告できる風土や信頼関係を情シス部門筆頭に組織全体として築いていかなければならない。被害拡大を防止するためにも、部内だけでなく積極的に全社的なコミュニケーションの機会を増やしていくことが求められている。

６．結論

６．１　現在の課題

サイバー攻撃も日々変化してきている。その上、セキュリティ対策で絶対的なものは存在しないため、”何を守るか”を定義し、情報資産へ適切な対策を重ね合わせていくべきだ。例えば、データをどう守るかということに着目すると、複数拠点に渡ってバックアップを確保することやスタンドアローンの利用、非常用電源の確保などの対策を一つ一つ組み合わせて事業継続を支えたい。しかし、攻撃対象の拡大や手法の変化に伴い、管理者だけでは対策が追いつかなくなってきているのではないだろうか。だからこそ外部と接点のあるシステム利用者を根気強く教育していくことが現在の課題なのだ。度々報道されるニュースでは、どのようなサイバー犯罪が流行しているかを理解できるが、実際に自分の身に体験してみなければ実感が伴わない。ではどのようなことが今できるであろうか。標的型メールの訓練実施も利用者がサイバー犯罪による被害を自分事と考えるきっかけとなれば効果的な手法と言えよう。日常的にセキュリティ脅威という”敵”を認識し、対策を心がけることが大切だ。

６．２　今後の課題

さらに昨今、技術の進歩は目まぐるしく、スマートデバイスをはじめ、IoTや人工知能など新しいツールが次々と登場してきている。このような技術に対し、どのような脅威が想定されるか予想していくことも求められているではないだろうか。時間の経過とともに世の中に技術が普及していく一方で、使い方やセキュリティ対策を自力で行うことができない者たちがサイバー犯罪の恰好の餌食となる。クラウドサービスのハッキングや不正なアプリのインストールによって個人情報が流出している事件が既に報道されているように、現在はスマートフォンに関するサイバー犯罪が目立つ。今後はIoTで収集したビックデータや人工知能による新たなコミュニケーションプラットフォームの誕生など、これから世の中に普及していく技術に対しても既存の情報端末より高度なセキュリティ対策が必要となってくることが予測される。さらに、2016年の今年はマイナンバー利用開始に伴い、個人や組織で扱う機密情報の増加が想定されるため、更なる情報漏えい対策が求められるであろう。したがって組織だけでなく、個人が主体となって守るべき情報資産は今後増加していくことは必然である。

一方で当社のグループ会社へ目を向けてみると、全社的なITガバナンスの対応が追い付いていない現状がある。IT機器を海外拠点で一部委託運用している現状やアジア圏におけるサイバー攻撃の被害状況からも、ITに関する確固たるルールが未だに普及しきれていない事実や利用者へのセキュリティ教育不足が読み取れるため、国内外で統一した水準の導入と普及が早急に望まれる。全体のセキュリティー最適化には個別のITリテラシーの向上が必須だ。PCアドバイザーやe-Learningの活用で利用者個人に適した教育方法の工夫が求められている。そしてガバナンスを行うということは、思想や文化が異なる地域を束ねるためのリーダーとして“本社”の強い役割が求められていることを意味する。今こそ情報資産を死守する必要性をグループ全体で改めて認識し、本社組織を筆頭に行動するよう改

革を図らなければならない。

引用図表

[１]独立行政法人情報処理推進機構セキュリティセンター ：“情報セキュリティ10大脅威2016～個人と組織で異なる脅威、立場ごとに適切な対策を～”，(2016)
http://www.ipa.go.jp/files/000051691.pdf

[２] 独立行政法人情報処理推進機構セキュリティセンター ：“「情報セキュリティ10大脅威2016」を発表～新たに個人別・組織別のランキングを選出、影響を受ける脅威の違いが顕著に～” ，(2016)
http://www.ipa.go.jp/files/000050724.pdf