第一回 IT トレンド研究会　議事録

日時：　2011/10/18(火)14:00～17:00

会場：　丸紅ビル B1F A 会議室

テーマ：　**『スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン【 β 版】』の解説＆作成秘話～セキュリティを考慮した運用ガイドラインを徹底討論～**

講演者：　**アルプスシステムインテグレーション株式会社**
営業統括部　特販プロジェクト　グループマネージャー
松下　綾子　氏(JSSEC 利用ガイドライン　ワーキンググループ　リーダー)

司会・進行：　**IT トレンド研究会座長**
TIS 株式会社　IT 基盤サービス本部　IT 基盤サービス第 2 事業部
IT 基盤サービス第 2 部　主査
中村　和弘　氏

当研究会の運営方針により、個人/会社名を特定できる発言、および発表者から公開の許可を得られなかった内容は　議事録より削除されています。あらかじめご了承ください。

◆第1部

松下様のご講演

◆第二部

＜中村氏＞スマートフォン(※以下、スマホ)をどのように使用しているかを中心に進めたいので、スマホの使用目的を沿えて自己紹介をお願いします。

＜A 社＞私個人の利用状況ですが、携帯とスマホの 2 台持ち。スマホ側はプライバシーを探られたくないから利用時のみ電源を入れています。まだ、ビジネスにスマホを利用するのは早く、時期を見る必要があるとかんがえております。

＜A’社＞全てのシステム管理をしています。苦労話ならあります。

＜B 社＞業務でもプライベートでもスマホは使っていません。最近思うこととして、スマホも携帯も PC も OS が入っているのになぜ計算機と呼ばないのか。このようにバックグラウンド(背景にあるもの)をおざなりにしている状況で管理がうまくいくのか疑問に思っています。

＜C 社＞社内情シス部門からスマホなどの情報が追いついていないので法人営業部で検討して欲しいと依頼されている。今回は情報シス部門の一員として参加させてもらっている。

＜D 社＞
スマホは BYOD として使用している。情シス部門のお客様から相談を受ける立場である。
スマホ利用は運用ポリシが大切であり、どのような切り口でお客様に伝えるか苦労している。

＜E 社＞半導体を作る仕事をしており、外へ出て仕事をする社員が多いです。iPhone などを活用したいが、システムサイドの立場としてはセキュリティ維持が重要なので、導入検討はこれからです。JSSEC のガイドラインをみて、とてもまとめられた資料だと思いました。

＜F 社＞社内の状況として、社内業務にスマホなどを利用することに無関心な状態です。セキュリティの立場としては不用意に利用できないと思っているが、新しい業務デバイスとして利用を広げることを推進してきたいです。

＜G 社＞総務、情報システム担当。携帯を持っている人が 5 名、スマホは私だけ使用して様子を見ています。ノート PC が無くてもメールが見る事ができるといった利便性はあるが、紛失時の情報漏洩を危険視しています。

＜F 社＞製造業。スマホは総務の管轄で、社内利用禁止。個人的には PDA の時代からモバイル端末を使用していて現在は iPhone、iPad を使用しています。ようやく使えるモバイル端末が登場してきたと思っています。BYOD に興味があります。

＜G 社＞研究所システム管理者。上層部から総務にスマホ利用の話がきましたが、技術的な立場から協力をしています。海外の比率が多いので運用の難しさがあります。

＜H 社＞モバイル端末は 20 年前から使っています。携帯で個人の情報を登録できるようになり、スマホでは会社の情報も登録できるようになりました。スマホがより PC に近くなってくると感じています。

＜I 社＞データセンター管理を担当しています。ISMS 取得や検証機管理なども担当している。サーバ中心でしたが、PC、Android 端末などの管理も行ってくよていです。情報収集のため参加しました。

＜J 社＞昨年、社内で iPad、iPhone4 を導入しましたが、今回の講演資料は「脅威」のところわかりやすいと感じました。上層部への説明に使いやすいと思います。iPhone4S を 60 台追加予定でしたが、メール誤送信を危惧して上層部からストップがかかりました。普通のノートよりスマホの方が安全だと上層部に話をしていいます。私はスマホ推進派です。

＜K 社＞お客様の業務系システム構築を担当しています。今回、モバイルの業務システム構築において、お客様にセキュリティ面の説明をどのようにすれば良いかなどを得るために参加しました。便利なデバイスは増えてきますが、危険な面を含めた提案に生かしたいです。

＜L 社＞会社は、スマホアプリの開発も行っていますが、管理面では MDM も導入されていません。会社で運用することが走り出したところです。MDM ツールを探しています。今回はセキュリティガイドラインを策定するためにお話を聞きに来ました。

＜M 社＞クライアント管理勉強会も参加しました。会社の携帯端末 1000 台を管理しています。iPad25 台いれたが、管理する仕組みがなく、MDM を導入するため Apple と交渉しています。少しでも前に進めたいため参加しました。

＜I 社＞社内のセキュリティはガチガチで、社外からまったく入れない環境です。個人的には様々なデバイスを使っています。スマホが広まっている状況で、危険な面を知らない人にも広まっている状況が怖いと思います。写真を撮ると GPS 情報を付与され知らないままアップロードすると自宅も知られてしまうという危険があります。教育がないまま広まっている状況だと思います。しかし、便利に利用できるものは使用していくべきだと思います。

社内でモバイルを利用するのであればシンクライアントが良いと思います。

＜J 社＞基幹システム運用しており、Web コンテンツ開発を担当しています。社内でスマホに関するラボチームができました。何をやっていくかから始まり、商業施設でのモバイル利用を想定するなど、情報収集していますので、成果につなげたいです。

＜K 社＞社内システム開発を担当しています。日報系システムをスマホで動かないかと上層部から指示がきました。CIO から 6 台スマホ購入したからテストをするように指示がきたので、MDM、シンクライアント等どのようにすべきか、勉強して帰りたいと思っています。

◆ディスカッション
＜中村氏＞使用目的が明確になってない印象がありますが、どうしたらいいかなど聞いておきたいことはありませんか。

Q＜B 社＞何に使うか興味がある。iPad は何に使用するのでしょうか？
→＜M 社＞動画なども含めて、チラシを PDF でお見せするために使用する予定です。導入目的は、ペーパーレスから始まりますが、それ以外に色々できることを知っている人もいるので、阻止する手段が必要だと思います。
→＜A 社＞プレゼン利用のために 5 台導入しました。iPhone と iPad ではぜんぜん目的が違います。iPad は導入したいが iPhone は必要ではないと思います。
→＜A´社＞基本的に何かをインストールすることは禁止しており、決められたもの意外はダウンロードも禁止という前提で端末を渡しています。リモートメールサービスは、外から Exchange のメールを見るために導入しているので、デバイスにデータが残らないことが良いです。管理はデータ持ち出しに関することからはじめていくのが良いと思います。
→＜中村氏＞シンクライアント端末として利用しています。紛失時にデータを消せることが重要です。自分の端末は、パスワード 8 桁以上、5 回の失敗でデータ削除設定を行うなどちゃんと管理することで、社内利用を認めてもらっています。

＜D 社＞紛失時にロックするようにお願いしていますが、個人のデバイスを管理することは難しいです。
ファイル暗号化システムを導入していますが、社外で個人デバイスから利用したいため平文で添付メールを送っているなど問題があります。管理のやり方としては、シンクラしかないかと思います。

＜H 社＞情報は重要度でレベル管理が必要だとおもいます。

＜C 社＞添付を画像化するサービスを利用できますが、社内ではそれも利用禁止されています。

＜B 社＞情報は画面を覗かれても漏洩します。情報は漏洩するものとして、ランク付けと責任の所在を明確にする教育が必要です。役員、社長は最大のセキュリティホール。役員が情報の見せ合いをするなどの対策が必要だと思います。

＜H 社＞携帯は急激に進化をはじめてスマホなど高性能化が顕著です。

＜松下氏＞「スマートフォン」の定義は少しづず変わっていくのかなと考えています。5 月のころには 3G が搭載されていない端末も登場してきました。これも管理に含めるのか議論が必要ですので、ガイドラインで伝えていきたいと思っております。また、用語の一覧なども追加していく予定です。端末の進化が顕著で、マルチタスクが実装されたことで一気に広まりました。今は 3G 搭載かどうかではなく、常時接続しているかどうかに重点を置いています。

＜H 社＞今はスマホなどで何ができるかを解説する本がでていて一般に広まっています。いつ裏の部分が悪意をもって現れるかわからないと思います。

＜松下氏＞一般の人にスマホ利用の恐怖、危険を、必要以上には煽る必要はないと思います。企業で利用する場合は、端末 ID や位置情報を取る点では、配慮が必要です。また、個人端末のワイプ実行などやりすぎるとプライバシー侵害の恐れもあるので気をつける必要があります。」

＜柳原氏＞ワイプとバックアップは同時に検討すべきだと思います。

Q:＜E 社＞誓約書などのお話もありましたが、BYOD では、自分の持ち物であるが、会社の情報も含まれるので、会社のものであるなどの内容も必要でしょうか。JSSEC では、現在どのような誓約書をイメージしていますか。
→＜松下氏＞先回りをして、告知しておくべき情報を洗い出して、誓約書に盛り込みました。法律的に効果があるとは限りませんが、相手に知っておいてもらうことも重要です。また、モバイル端末を考慮してセキュリティポリシを替えたのであれば、こちらも周知することが重要だとおもいます。利用目的と利用ポリシがあることを誓約書で確認させる事ができます。利用目的を明確にして利用範囲を絞ることも目的に含まれます。
→＜E 社＞個人持ちのものを社内で利用する手段を講じるという方法もありますが、最近の機器は安価になっているので、企業で必要なものを全てそろえることも方法かもしれないです。

Q:＜A 社＞個人持ち端末をワイプする必要がでると難しいです。
→＜D 社＞無くしたら消されてもしょうがないことをコミットしておくのはいかがでしょうか。

＜L 社＞基本的に海外の方は自分の端末を持ち込みたい人が多いので、誓約書を作る必要があります。私物の端末を使っても良いのですが、何かあったら消すことをコミットしておかなければなりません。

＜F 社＞携帯は一人一台渡していますが、ロックを義務付けており、ロック中は誰からの電話かわからないため、私用の携帯番号をお客様に伝える人もいます。個人持ち、付与している端末の使い分けは期待できません。個人持ちを社内で利用することも考えていかなければなりません。
また、デバイスを選ばずに同じ情報にアクセスできる点からもクラウド利用も良いと思います。
従来のブロックするセキュリティ対策は限界かもしれないですし、情報が漏洩することは防げないので、困らないように情報の価値を利用者、マネージャが理解し、管理しているかを組織として整備する必要があると思う。

＜柳原氏＞大別すると皆さんは 2 つのグループになります。
・ソリューションを販売する立場
・純粋なユーザ
ユーザの方は更に
・上層部から利用を指示されている人
・個人的に推進したい人
となります。

＜松下氏＞ガイドラインは推進していただくために作っています。知っておいていただくために将来的にありえる脅威も乗せています。だから利用目的をはっきりさせることが重要です。
例えば、スマホを内線にも使いたいとなると考慮すべきことが多くなるなどといったことです。
スマホ導入は、システム全体を変更するきっかけにできると思います。検討はステップバイステップで進めるべきです。重要性、危険性を説明し、伝えることが大切で、一度にやろうとしても無理があります。
セキュリティは日進月歩です。費用をかければよいというわけでもありませんので、情報収集を行って下さい。
セキュリティをガチガチにして利便性をなくしてしまうと導入の意味がありません。スマホは使わせるツールではなく、使いたいと思うツールです。

＜中村氏＞ガイドラインを使って、必要な情報、必要ない情報の選別をしてください。

＜松下氏＞セキュリティ面、個人情報に関する不安があるため、少し前に周囲のメンバーに聞いたところでは、BYOD を要望する社員は少なかったです。

＜C 社＞アンケートを営業担当者に BYOD を聞きましたが、数名だけで大多数は反対でした。

＜B 社＞個人持ちなのに監査が入るということがわかっているからでしょう。

＜D 社＞本当の個人持ち端末は、別に持っているので抵抗無く差し出せます。

＜A 社＞個人安否システム等は、個人持ち端末でないと機能しないのではと思います。

Q：＜松下様＞ガイドラインに追加して欲しい項目や要望はありますか。

→＜D 社＞セキュリティ啓蒙のため、端末を無くしたら、どのようなことが起こるかを説明した資料が欲しいです。
→＜松下様＞別で活動している団体があり、有償だが世にでると思います。
→＜D 社＞有償だと 2 次利用できないです。

＜久保＞要望は事務局に投げてもらえばよいです。お役に立てたか挙手をお願いします。
※皆さん満場一致で役に立ったとの感想。
スマホの流れは、昔のインターネットと同じで、可用性、安全性のせめぎあいです。今後、クラウドも取り上げていきたいので、引き続きご参加お願いします。7 月に大会もあります。