

第一回 ITトレンド研究会 議事録

日時: 2011/10/20(木)15:00~18:00

会場: クオリティ(株) 本社 6F 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【B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

HOYA 株式会社 オプティクス事業部 管理本部

情報システム管理課 IT グループ グループリーダー

柿崎 敦司 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

松下様の公演

■第2部

自己紹介、ディスカッション

<A社>社内でスマートフォン利用の要望が出ており情報収集中です。

<B社>インフラ系運用担当。スマートフォンの導入担当ではないが、導入されると運用することになります。基幹のネットワークとは繋げていけないルールになっています。部分導入はしていますが、裏口で繋がっていたりするので、そのセキュリティ対策を検討しています。インターネット接続を制御できるツールは何か知りたいです。

<C社>社長が iPad を入れたため、情シスでも使っています。しかし、ルールは何も決まっていないため、早急にルール化が必要だと思えます。目的と利用、どういうルールがあるか、また実際に起きている問題があれば教えて欲しいです。

<D社>ルート権限の制限について知りたいです。

<E社>コンプライアンス全般を担当。スマートフォンは未導入だが、自然増で利用している人が増えてきているので、最低限のルールを出す必要が出てきました。WiMAX から LAN になる場合の危険とは何か聞きたいです。

<F社>iPhone、iPad を配布しているが、アンドロイドよりは安全というのは本当でしょうか。また、普段のセキュリティ対策なしで使用しても、大丈夫なのか知りたいです。

<G 社> 営業の iPad 利用について検討中です。スマートフォンのアプリなどのルート権限を取られたときに大丈夫なのか知りたいです。

<H 社> 先行導入し仕組みを作る部門にいます。働き方の多様化の要望について、iPhone、iPad、MDM をユーザ評価期間としての環境で使っています。現状では、営業がカタログを見せるために使っています。本当に仕事で使えるのか？現状どう使っているか、使わせているか他社さんの話を聞きたい。

<I 社> つぶやきなど情報漏洩に繋がる危険もありますが、そのことについて上層部も理解しておくべきだろうと考えています。また、業務時間にスマートフォンをやることについて、会社から何か言われたいのか、PC は BYOD とは言われたいのに、スマートフォンはなぜそうなのか、など色々話していきたいです。

<J 社> スマートフォン、タブレット PC のテスト導入をしました。BYOD でやっている人はどうやっているのか聞きたいです。

<K 社> スマートフォンの理想の使い方を聞きたいです。

<L 社> 社長が「買ってきたら設定しておいて」、という会社もやはり多いそうです。真摯協定で私物を業務で使っているお客さんも多いそうです。カレログが話題ですが、出口の経路がたくさんできて脅威が増えました。自社では社員に誓約書を書かせている。

<M 社> スマートフォンの社内利用のセキュリティガイドラインを策定中です。目的を明らかに、どう使わせるかもっと活用させるための情報収集のため参加しました。気になっているところは、BYOD に対してどう考えるか？誓約書だけでなく、紛失した場合など実際どうしたらよいか。また、社外の回線に繋がってつぶやきされてしまうという危険などどう押さえるか、です。

スマートフォンはアクセス回線がいろいろあるが、なんでも使わせていいのか？もし、業務での使い方によって使用を認めるかを決める運用をしている企業があれば聞きたいです。

<N 社> 新しい物を入れる社風ではないため、他社の話を聞いて自社の状況を考えるために参加しています。個人的にはスマートフォンはあるのは当たり前というものになるだろうと思っています。無作為に飛び交う情報をどう制御していくべきか、聞きたいです。

<O 社> スマートフォンは全社で 20 台ほど導入しました。現場は利用したいのですが、経営層はまだ必要があるとは思っていないため、経営層への上手い説明方法が課題です。

<P 社> アンドロイド端末で外から仕事をしたいが、VPN を使ったサービスが社内がないのでまだ使えずにいます。外資は誓約書ベースで外の持ち出し OK とか聞いています。スマートフォン、タブレット PC ができることがメールとスケジュール管理だけなら入れる価値はあるのか、知りたいです

■セキュリティ関係について

・自宅からの情報漏洩が問題です。

Q:クラウドは接続の口が多く、VPN じゃなくても繋がります。

→会社の取り組みだけでなく、誓約書、罰則が必要になってくると思います。

Q:会社の考え方としてクラウド上に会社の情報をおくべきか。

→ガイドラインには SNS の件はのせていなかったが、SNS を使う時間が圧倒的に多いので載せざるを得ないです。ただ、社内向けの SNS がある企業もあります。

Q:ISMC について、Wi-Fi に繋がらなくするツールはありますか。

→(クオリティソフト)ある。社内は OK。公衆は NG。

Q:NG で接続したらログを送る機能はありますか。

→(クオリティソフト)Wi-Fi の接続先の制限はできます。ログの件は仕様を検討中です。

■私物解禁(Bring Your Own Device)について

そもそも私物 PC は NG なのに、スマートフォンは問題ないのでしょうか。

遠隔でワイプができることが利用の条件だとしたら、私物を業務に使いますか。

→紛失時のデータ消去について、個人と会社のデータの取り扱い、等ルール化しなければなりません。

■事前アンケートの話

Q:スマートフォンの業務での使用とはどこまでか知りたいです。

→VPN に個人 PC で入るのは OK(申請は必要)データが個人 PC に落ちないようにすることを検討しています。管理職用は社内から貸与する方向です。

→緊急時の連絡は何を使っても OK だが、仕事上では私物を利用する事は NG。

Q:緊急時会社のもを必ず携帯しているとは限らないのではないのでしょうか。

→簡単に社内システムに入れるようになっているため、教育が必要だと思う

・社内メールがスマートフォンに転送され、メールを見ている事が前提となるため、やらないわけにはいきません。

Q:個人的にストレスにならないのでしょうか。

→立場や会社によって違いがある。外資系は時差の関係で特に負担になることが多いです。

■本日の研究会まとめ

スマートフォンの企業利用の対応は迫られているが、まだ様子を見ている企業がほとんどのようです。

- ・スマートフォンの利用ルールを作成中、または作成を迫られている会社が多い。
- ・スマートフォンの業務利用に興味はあるが、セキュリティが心配。
- ・スマートフォンの企業利用は本当に流行るのか？
- ・スマートフォンはPCに成り代わるとは思っていない。情報の出入り口としての利用。
- ・パーソナライズができること自体は、情シスで押さえておくべき