スマートフォン活用
セキュリティガイドライン策定WG　活動報告

スマートデバイスのガイドラインって難しい？
～より広く活用頂くために～

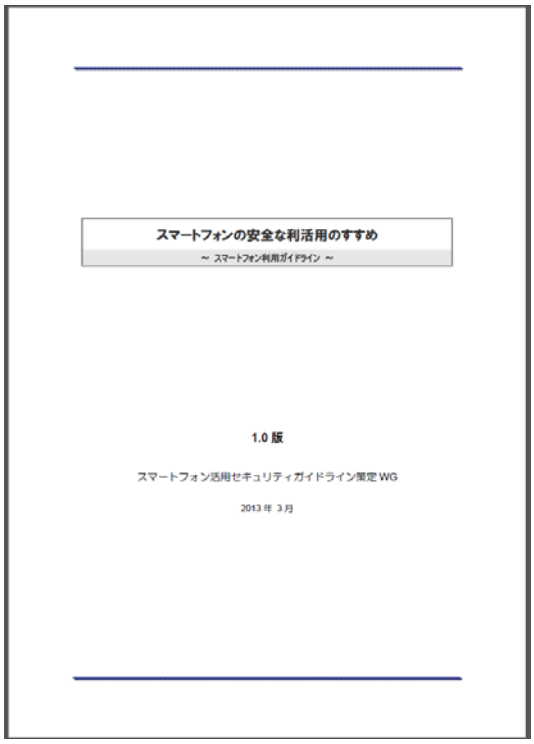
栃沢 直樹
トレンドマイクロ株式会社

2015年6月9日

これまでのWGの沿革

2010年	WG発足
2011年4月	「スマートフォンの安全な利活用のすすめ ～ スマートフォン利用ガイドライン ～ 」 β版リリース
2013年4月	「スマートフォンの安全な利活用のすすめ ～ スマートフォン利用ガイドライン ～ 」 正式版リリース
2014年	WGリーダー交代 （LAC加藤さんより。理由は「言えない。。。」）

β版から正式版（1.0版）へ



正式版リリースに向けて意識したこと

- セキュリティ課題の提示だけではなく、より情報システム部門担当者の目線で検討するべき項目を整理
- 情報システムインフラを管理する担当として新しいデバイスの導入をどう考えるのかが重要
- 利用者のリテラシー向上と組織内のネットワークにスマートデバイスを接続する際に留意するべき特有の課題の解決策を提示

β版から正式版リリースまでの2年間で、環境変化はあったが、β版で考えていた基本的な考え方は変える必要はなかった。

2014年度の活動

正式版から次の一歩へ

はじめは、、、

●企業におけるスマートフォン利活用度調査。

企業におけるスマートデバイス利活用度調査（ベストプラクティス/活用できていない事例）をまとめることにより、企業の利用の実態を把握し、第2版のガイドラインにフィードバックして現実的な利活用のためのガイドラインを策定する。
（第2版とするか、別ドキュメントとするかは未定）

**キックオフにて、
「JNSA以外で実施しているデータがあり、JNSAでやる必要があるのだろうか？」
ということでボツ案となる。**

正式版から次の一歩へ

ということで目指したいことを再確認することに、、、

●ガイドラインをより多くの人、必要な人に読んでもらいたい

●一方で、必要な人たちにガイドライン自体を知られていないし、知っていてもそれをすべて理解して、実装していくことは難しい。

●実際に課題を持っている人が、ゼロのままよりも一歩でも対策に踏み込める、または、考えるきっかけになるものを提供したい

万人受け、100%を目指すのではなく、本当に読んでもらえるガイドラインにする。

正式版から次の一歩へ

2014年度は！

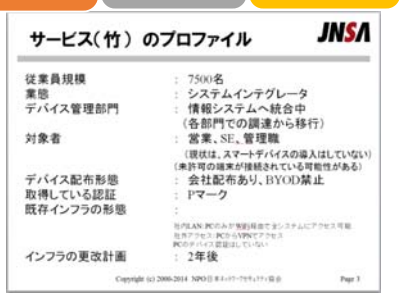
- **エンタープライズ領域でのスマートデバイスのユースケースから適切な対応策を検討しリリースする**
  - エンタープライズでのユーザの利用シナリオをいくつか作成する
    - 組織として管理者が提供するITサービスはどのような内容か？
    - 管理者がどの程度スマートデバイスの利用を管理・制御するか？
    - 利用者のリテラシー
  - 簡単なケースをベースに起こり得る脅威、環境・利用デバイス毎の違い、実施するべき対策を提示し、一部の対策だけでも実施できるようピックアップできるようにマトリックス化する

完璧に対処できないにしても、できることから少しずつでも考えてもらえるきっかけにしたい。

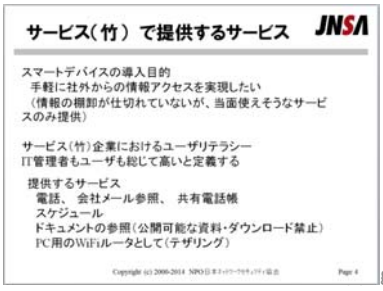
議論の展開

モデルユーザ企業の
イメージを3パターンに分類

松　竹　梅


サービス（竹）のプロファイル

従業員規模	：7500名
業態	：システムインテグレータ
デバイス管理部門	：情報システム統合中 （各部門での調達から移行）
対象者	：営業、SE、管理職 （現状は、スマートデバイスの導入はしていない） （未許可の端末が接続されている可能性がある）
デバイス配布形態	：会社配布あり、BYOD禁止
取得している認証	：Pマーク
既存インフラの形態	：
インフラの更改計画	：2年後


サービス（竹）で提供するサービス

スマートデバイスの導入目的
手軽に社外からの情報アクセスを実現したい
（情報の棚卸が仕切れていないが、当面使えそうなサービスのみ提供）

サービス（竹）企業におけるユーザリテラシー
IT管理者もユーザも総じて高いと定義する

提供するサービス
電話、会社メール参照、共有電話帳
スケジュール
ドキュメントの参照（公開可能な資料・ダウンロード禁止）
PC用のWiFiルータとして（テザリング）

提供するITサービスに対応した想定
されるリスクと対策をマトリクス化

<IT部門が提供する（予定の）サービス>	<対策として考慮すべきポイント>	リスク	対策	対策するべき項目		
				梅	竹	松
スマートデバイスの配布（基本機能：テザリング）	・テザリングの管理	会社PCからスマートデバイス経由のテザリングで社外へ持ち出す	MDM or キャリアサービスによる制御		注意喚起	
スマートデバイスの配布（基本機能：電話帳）	・電話帳の手動登録のルール化		（梅）→ クラウドサービスの利用リスクについて、認知をした上で利用することを喚起する。	注意喚起	注意喚起	MDM
社内ITリソースへのリモートアクセス	・社内ネットワークへのアクセス制御					
	BYOD端末：社内LANへ接続	未許可なデバイスによる不正アクセスとそれに伴うマルウェアなどの拡散	リモートアクセス時のデバイス認証		BYOD不許可	
	BYOD端末：社内LANへの接続不可		リモートアクセス時のデバイス認証		BYOD不許可	
	会社端末：社内LANへの接続		リモートアクセス時のデバイス認証			
	会社端末：社内LANへの接続不可		リモートアクセス時のデバイス認証			
	・社内アクセス時のデバイス制御（デバイス認証、ユーザ認証は前提として考える）					
	・野良WiFiへの接続	野良WiFiによる社内へのセキュリティレベルの低いAPからの不正アクセスなど	（梅）→ クラウドサービスの利用リスクについて、認知をした上で利用することを喚起する。			
社内無線LANによるスマートデバイスの社内アクセス許可	・野良WiFiへの接続	野良WiFiによる社内へのセキュリティレベルの低いAPからの不正アクセスなど	無線LANシステムの統合管理 ルールによる統制			
スマートデバイスの配布（基本機能：OSアップデート）	・OS/アプリケーションのバージョンアップ	脆弱性を突く攻撃	MDM or キャリアサービスによる制御			
スマートデバイスの配布（基本機能：ロック）	・ロックをかける	第三者による不正アクセス	MDM or キャリアサービスによる制御 ルールによる統制	ルール	ルール	MDM
スマートデバイスの配布（基本機能：ワイプ）	・ローカルワイプ/リモートワイプ	紛失時の情報漏洩	MDM or キャリアサービスによる制御			
アプリストアからのアプリダウンロードの許可	・アプリの利用制限	不正なアプリの利用	MDM or キャリアサービスによる制御	ルール	ルール	MDM
スマートデバイスの配布（基本機能：カメラ）	・写真データの管理	ファイルデータの情報漏洩	ルールによる統制	ルール	ルール	MDM
アプリアカウント情報の管理	・アプリ/Webアクセス時のアカウント情報の管理	デバイス紛失時のアカウント情報の抹取	ルールによる統制	ルール	ルール	ルール
クラウドサービスの利用	・データを無意識にクラウドへアップロード	管理外のクラウドサービスへの業務データのアップロー	（梅）→ クラウドサービスの利用リスクについて、認知をした上で利用するこ	注意喚起	注意喚起	MDM

検討の道のり

計9回のWGを実施

2014年6月30日	キックオフ
2014年7月30日	第2回WG
2014年8月26日	第3回WG
2014年9月16日	第4回WG
2014年10月21日	第5回WG
2014年11月18日	第6回WG
2014年12月9日	第7回WG
2015年1月22日	第8回WG
2015年2月24日	第9回WG

ここでテーマ確定！

ユースケースにおける『現時点での状況』と『対策後の状況』をどのように定義するかでスタックして年度をまたいでしまいました（リーダーとしての反省）

2015年度の活動計画

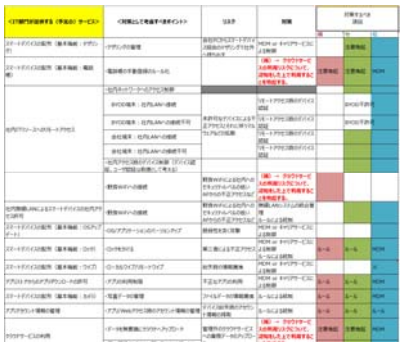
今年の活動計画

アウトプットを出します！

普段ガイドラインを意識して読まれない方でも簡単にやるべきセキュリティ対策の第一歩を踏み出せる『スタートアップガイド（仮）』

スタートアップガイド（仮）位置付け

何から始めたらよいか
分からないIT管理者様へ



スタートアップガイド（仮）

より深くセキュリティ対策を
理解し、実装されたい方へ

ガイドライン正式版

目次案

①はじめに　～本書の目的、想定読書

②作成の背景

ガイドライン読んでもらえないのよ（課題認識）

とはいえ、導入してしまった場合のセキュリティ対策を分かりやすく説明したい（目的）

③モデルケースの説明

松、竹、梅各プロファイルの会社属性、提供するITサービス、

（会社としてのセキュリティポリシー）、会社の体質・社員のリテラシー・　IT管理者の体制）

④モデルケースごとの想定されるリスク

梅⇒竹⇒松

※許容しても良いリスクと、許容できないリスク（契約で縛るなど）

↓

対策のコスト・運用（できれば）

※最低これだけはやっておくことを明記

⑤リスク毎の対策要件・対策方法

梅⇒竹⇒松

許容するべきリスク

⑥まとめ

最後に

2015年7月にWG再開を予定しております。
別途、今年度のメンバー募集をさせて頂きます。