JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

《スマートフォン活用セキュリティガイドライン正式版》
リリースに関するWG活動の概要

加藤 智巳

株式会社ラック

2013 年6月7日

2012年度WG活動概要

- 第6回　4月19日
  - この間、行き詰まり、、、。
- 第7回 11月30日
- 第8回 12月07日
- 第9回 12月20日

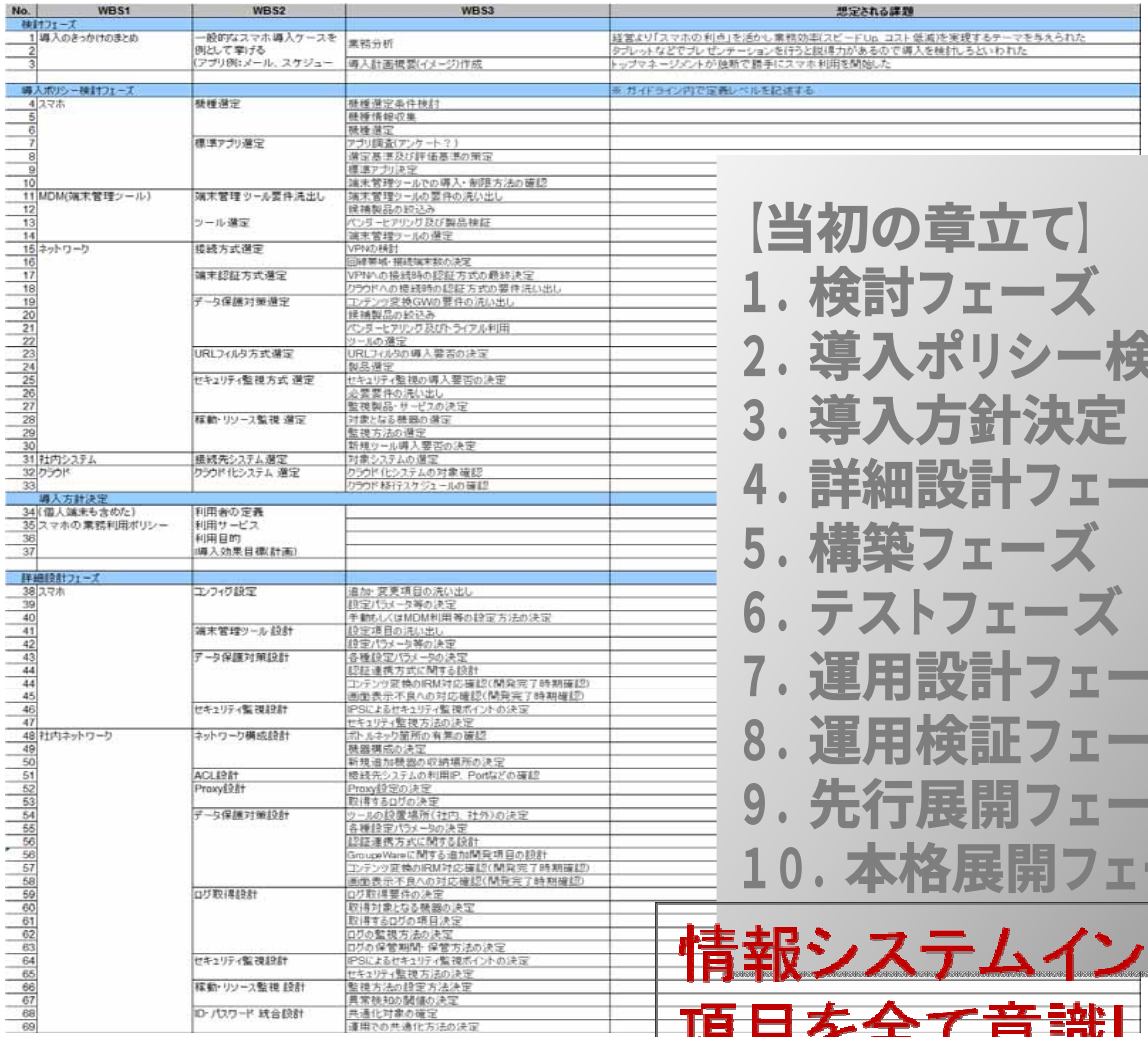
※正式版作成WG 第1回～5回は2012年度に実施

※負荷分散のためサブリーダミーティングは幾度となく実施

正式版リリースまでの歩み ①

- 2012年4月に正式版リリースに向けて、2011年10月7日にWGをスタート
  - β版の章立てから大きく変えて、スマートフォン導入部門の担当者の立場を想定して企業の情報インフラ全体をも視野に入れたガイドラインにしたい
  - インフラ関連の検討材料がどんどん追加されていき、スマートフォンガイドラインではなく、情報システムインフラガイドラインの方向に。
    - WGは破綻状態（というか私自身がボトルネック）

正式版リリースまでの歩み ②



No.	WBS1	WBS2	WBS3	想定される課題
	検討フェーズ			
1	導入のきっかけのまとめ	一般的なスマホ導入ケースを例として挙げる（アプリ例：メール、スケジュー	業務分析	経営より「スマホの利点」を活かし、業務効率/スピードUp、コスト低減/を実現するテーマを与えられた
2				タブレットなどでプレゼンテーションを行うと説得力があるので導入を検討しろといわれた
3			導入計画概要(イメージ)作成	トップマネージメントが独断で勝手にスマホ利用を開始した
	導入ポリシー検討フェーズ			※ガイドライン内で定義レベルを記述する
4	スマホ	機種選定	機種選定条件検討	
5			機種情報収集	
6			機種選定	
7		標準アプリ選定	アプリ調査(アンケート？)	
8			選定基準及び評価基準の策定	
9			標準アプリ決定	
10			端末管理ツールでの導入・削除方法の確認	
11	MDM(端末管理ツール)	端末管理ツール要件洗出し	端末管理ツールの要件の洗い出し	
12			候補製品の絞込み	
13		ツール選定	ベンダーヒアリング及び製品検証	
14			端末管理ツールの選定	
15	ネットワーク	接続方式選定	VPNの検討	
16			回線帯域・接続端末数の決定	
17		端末認証方式選定	VPNへの接続時の認証方式の最終決定	
18			クラウドへの接続時の認証方式の要件洗い出し	
19		データ保護対策選定	コンテンツ変換GWの要件の洗い出し	
20			候補製品の絞込み	
21			ベンダーヒアリング及び5ライアル利用	
22			ツールの選定	
23		URLフィルタ方式選定	URLフィルタの導入要否の決定	
24			製品選定	
25		セキュリティ監視方式 選定	セキュリティ監視の導入要否の決定	
26			必要要件の洗い出し	
27			監視製品・サービスの決定	
28		稼動・リソース監視 選定	対象となる機器の選定	
29			監視方法の選定	
30			新規ツール導入要否の決定	
31	社内システム	接続先システム選定	対象システムの選定	
32	クラウド	クラウド化システム 選定	クラウド化システムの対象確認	
33			クラウド移行スケジュールの確認	
	導入方針決定			
34	(個人端末も含めた)	利用者の定義		
35	スマホの業務利用ポリシー	利用サービス		
36		利用目的		
37		導入効果目標(計画)		
	詳細設計フェーズ			
38	スマホ	コンフィグ設定	追加・変更項目の洗い出し	
39			設定パラメータ等の決定	
40			手動もしくはMDM利用等の設定方法の決定	
41		端末管理ツール設計	設定項目の洗い出し	
42			設定パラメータ等の決定	
43		データ保護対策設計	各種設定パラメータの決定	
44			認証連携方式に関する設計	
45			コンテンツ変換のIRM対応確認(開発完了時期確認)	
46			画面表示不具合への対応確認(開発完了時期確認)	
47		セキュリティ監視設計	IPSによるセキュリティ監視ポイントの決定	
48	社内ネットワーク	ネットワーク構成設計	セキュリティ監視方法の決定	
49			ボトルネック箇所の有無の確認	
50			機器構成の決定	
51		ACL設計	新規追加機器の収納場所の決定	
52		Proxy設計	接続先システムの利用IP、Portなどの確認	
53			Proxy設定の決定	
54		データ保護対策設計	取得するログの決定	
55			ツールの設置場所(社内、社外)の決定	
56			各種設定パラメータの決定	
56			認証連携方式に関する設計	
57			GroupWareに関する追加開発項目の設計	
58			コンテンツ変換のIRM対応確認(開発完了時期確認)	
59		ログ取得設計	画面表示不具合への対応確認(開発完了時期確認)	
60			ログ取得要件の決定	
61			取得対象となる機器の決定	
62			取得するログの項目決定	
63			ログの監視方法の決定	
64		セキュリティ監視設計	ログの保管期間・保管方法の決定	
65			IPSによるセキュリティ監視ポイントの決定	
66		稼動・リソース監視 設計	セキュリティ監視方法の決定	
67			監視方法の設定方法決定	
68		ID・パスワード 統合設計	異常検知の閾値の決定	
69			共通化対象の確定	
			運用での共通化方法の決定	

【当初の章立て】

1. 検討フェーズ
2. 導入ポリシー検討
3. 導入方針決定
4. 詳細設計フェーズ
5. 構築フェーズ
6. テストフェーズ
7. 運用設計フェーズ
8. 運用検証フェーズ
9. 先行展開フェーズ
10. 本格展開フェーズ

破綻

情報システムインフラ担当者が関連する項目を全て意識したため

正式版リリースまでの歩み ③

- β版は、「とにかく早くリリースする」が世の役に立つと信じて出した、、、
  - セキュリティ課題を書き連ねただけ？
    でもβ版だからと、ある種のエクスキューズ的な感覚

- β版の立付けに戻し、丁寧にブラッシュアップするという方針に切り替え
  - 「2年の大きな変化」があったにもかかわらず
    β版ガイドラインの内容としてはほぼ想定内だった

β版との違い(意識した点)

- 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した
- 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
- 重要なポイントはより明確な要件として表現

正式版のメッセージ

- 「スマートフォンのセキュリティとはどう考えるべきなのか」
  - スマートフォンは脆弱なデバイスであると認識し、それを踏まえてネットワークの設計･管理･運用を検討するべきである
    - 事実上のBYOD運用
    - 対策された最新OSへ更新できない機器の存在
    - 利用者のリテラシーに依存せざるを得ない状況の認識
  - スマートフォン収容ネットワークは独立させる
  - 既存の組織内サービスネットワークを保護する対策

※結局、スマホを導入するから云々、、、ではない。

主な追記事項

- スマートフォンとID
- 社内ネットワークへの接続の課題
- 認証方式の検討
- 端末管理ツール要件とツール選定
- 無線LANの検討
- ネットワークの運用設計
- アプリケーションのインストール
- キッティング

2013年度の活動予定

- 正式版のブラッシュアップ
  - スマートフォンに関連する最新情報に基づき、より利用しやすい内容に修正
- OSを絞り込み、見識を高めてより充実させる。
  - 今年度はアンドロイド？iOS？
- 今年度はコンスタントに地道に
  - WGのみなさんよろしくお願いします。