JNSA

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

中小企業と秩序あるBYOD

嶋倉　文裕
JNSA西日本支部
2012年10月24日

BYODの対象デバイスの確認

Bring Your Own Device

今日のお話！

- Smart Phone
  （iPhone、Android、Windows Phone）
- Tablet
  （iPad、Android、Windows）
- Note PC
  （Ultrabook、Mac etc....）
- External Media
  （USB、HD、SD.....）

使う場所は．．．

Where？　Anywhere．．．Mobility

事務所
　（自席、会議室、自社の他事業所）
社外
　（客先、電車、駅、ホテル、自宅．．．）

何に使うのか

事務所
- 自席 -> 日常業務
- 会議室 -> 打合せ
- 自社の他事業所 -> 打合せ、メール

社外
- 客先 -> 打合せ、現場作業
- 電車、駅、ホテル -> メール、事務処理
- 自宅 -> 日常業務

BYODのメリット

会社にも、個人にもメリットはありそう

項目		会社（経営者）	個人（従業員）
端末	好きな端末の選択 -> 生産性の向上？		○
	使い慣れ -> 生産性の向上？		○
	最新機種、OSの選択スピードup -> モチベーション向上？		○
	持ち歩き端末の集約、減少		○
	端末コストの削減	○	
	端末設定・サポートの負荷削減	○	
利用シーン・波及効果	働き方（どこでも、いつでも）	○	○..?
	優秀な人材の確保 - 育児・介護を伴う従業員の雇用継続（女性の力の活用）	○	○
	従業員のモチベーション向上（自分の時間の使い方）	○	○..?
	リモート作業による移動コスト（時間・費用）の削減	○	○
	意志決定の迅速化	○	○
	BCP（非常時における事業継続）	○	○

BYODのデメリット

会社にも、個人にもデメリットはありそう

項目		会社（経営者）	個人（従業員）
端末	端末の盗難・紛失 -> 保存データが第三者に情報漏洩	○	○
	Jailbreak/root化によるウイルス感染 -> 情報漏洩	○	○
	盗難・紛失の端末による社内システムへの成りすましアクセス	○	
	ウイルス対策不備によるウイルス感染 -> 情報漏洩	○	○
	多種多様な端末管理・セキュリティ対策の負担増	○	
	ウイルス感染した端末から社内にウイルス拡散	○	
	多種多様な端末にシステム基盤、アプリの対応、費用増	○	
	個人のコスト負担増		○
影響	働き方（どこでも、いつでも）	○	○
	勤務時間の長時間化、不規則化 -> モチベーション劣化	○	○

BYODメリット、デメリットをまとめると

メリット

- 端末視点のメリット
  - ・企業はコストメリット大、個人は自由度up
- 利用シーン・波及効果メリット
  - ・企業と個人はwin-winの関係

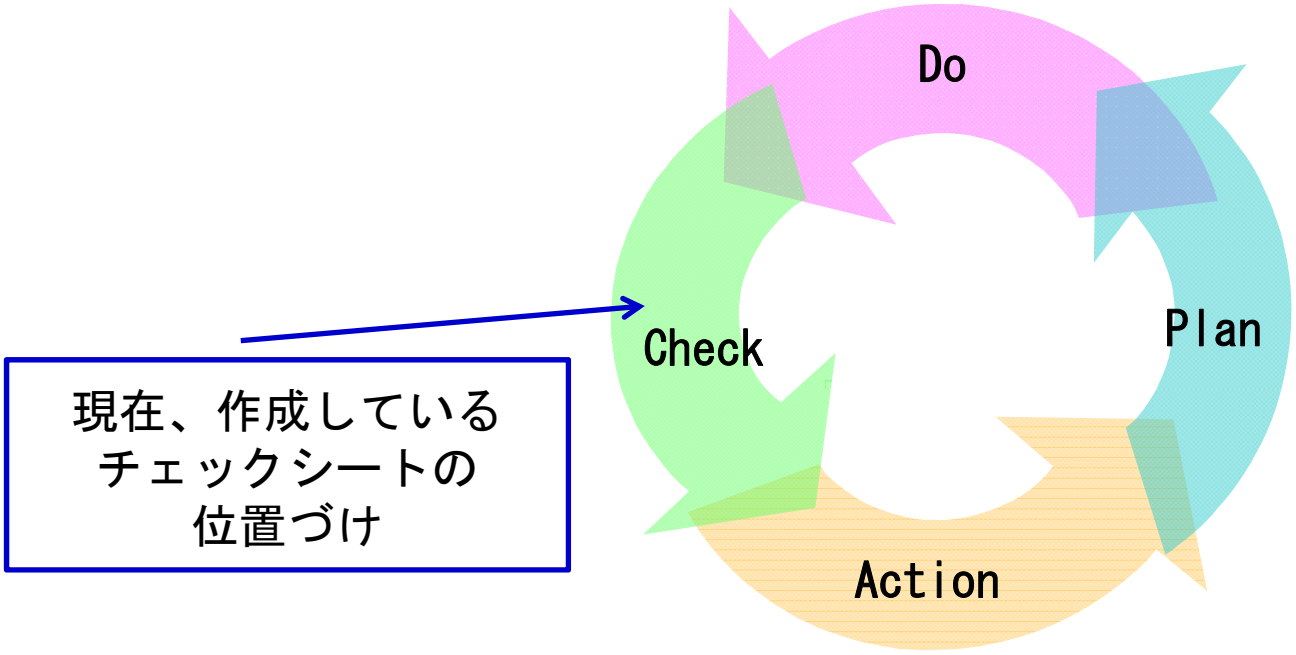
デメリット

- 端末視点のデメリット
  - ・企業は情報セキュリティ対策のコスト増
    個人はデバイス、通信費コストの負担
- 利用シーン・波及効果デメリット
  - ・就業時間があいまい

情報セキュリティチェックシート

JNSA西日本支部　情報セキュリティチェックシートWG

ＰＤＣＡサイクルを自主的にまわしていくことを支援可能なツール



情報セキュリティチェックシートから見て

情報セキュリティチェックシートから見たBYOD

No.	キーワード	対象					影響			付属書A他	脅威					脆弱性
		クライアント	ネットワーク	サーバ	アプリ	データ	機密性	完全性	可用性	ISMS管理策	外部悪意	内部悪意	内部過失	障害・災害	脅威例	(ﾄﾗﾌﾞﾙ事象例と対策の間からこの位置に順番入れ替え)
1	情報セキュリティ基本方針	○	○	○	○	○	○	○	○	システム管理基準 Ⅰ.情報戦略 1.全体最適化(1),(6)					・会社を取りまく環境の変化(技術、社会、会社規模・ﾋﾞｼﾞﾈｽ..etc)	・変化への不適合
										A.5.1.1 情報セキュリティ基本方針文書		○	○			
										A.5.1.2 情報セキュリティ基本方針のレビュー						
2	責任の明確化	○	○	○	○	○	○	○	○	システム管理基準 Ⅰ.情報戦略 2.組織体制 2.1(1),2.2(1)					役割の不明確	・障害、問題発生時の連絡体制がない 〈別階層〉 ・従業員かどうかを識別、認証する仕組みが無い ・取り扱う情報の重要度に応じたエリア分けをしていない
										A.6.1.1 情報セキュリティに対する経営陣の責任						
										A.6.1.2 情報セキュリティの調整						
										A.6.1.3 情報セキュリティ責任の割当て						
										A.6.1.4 情報処理設備の認可プロセス						
										A.6.1.6 関係当局との連絡						
										A.6.1.7 専門組織との連絡				○		
										A.6.1.8 情報セキュリティの独立したレビュー						
										A.8.1.2 選考						
										A.8.1.3 雇用条件						
										A.8.2.1 経営陣の責任						
										A.8.2.3 懲戒手続き						
										A.8.3.1 雇用の終了又は変更に関する責任						
										A.8.3.2 資産の返却						

脅威と脆弱性

BYOD固有の脅威と脆弱性の明確化が重要

新しいデバイスも既存のISMS管理策をベースにしたチェックシートに取り込みが可能

BoF
テーマ

モデレーター:

富士通関西中部ネットテック株式会社　嶋倉 文裕

パネリスト:

KDDI研究所　竹森 敬祐氏

日本マイクロソフト株式会社　香山　哲司氏

株式会社神戸デジタル・ラボ　近藤　伸明氏

１．　BYODの事例

- BYODって、新しいことですか？
  - 中小企業は個人PCや個人携帯を仕事で使っている
  - 大企業も個人PCの利用禁止は、１０年ぐらいの話
- 今のBYODは、スマホの登場で加速されているのは間違いない
- BYODはデバイスの話？仕事のやり方の話?
- 近藤さんから導入事例と、香山さんからグローバル企業であるマイクロソフトの事例をお聞きします
- ご来場の皆様のところはどうでしょうか

2. BYODの課題？思い込みもある？

- 私物はセキュリティが担保できない、会社支給は大丈夫、本当か？
- 守る対象はデバイス？ データ？
- 私物手帳は使っている、手帳は良いのか？
- 管理する側からの懸念事項は、具体的に何？

- 近藤さんから自社でのBYOD実践するためのセキュリティの考え方をお聞きします
- 香山さんから管理者視点での懸念事項をお聞きします
- 竹森さんから技術的視点からBYOD固有の考慮すべき事項をお聞きします

３．　具体的な対策に向けて

JNSA

- リスクと向き合いバランスのとれた対策のポイントって何？
- 私物と社給で対策の違いは？
- 仕事に使うには、私物でも責任を負うよね？利用者の意識は変わる？
- データセキュリティのためにどうすべきか？
- PublicとPrivateのせめぎあいはどこまで？

- 竹森さんから技術的な対策についてお聞きします
- パネラー、および来場の皆さんの意見交換をお願いします

ご清聴ありがとうございました。