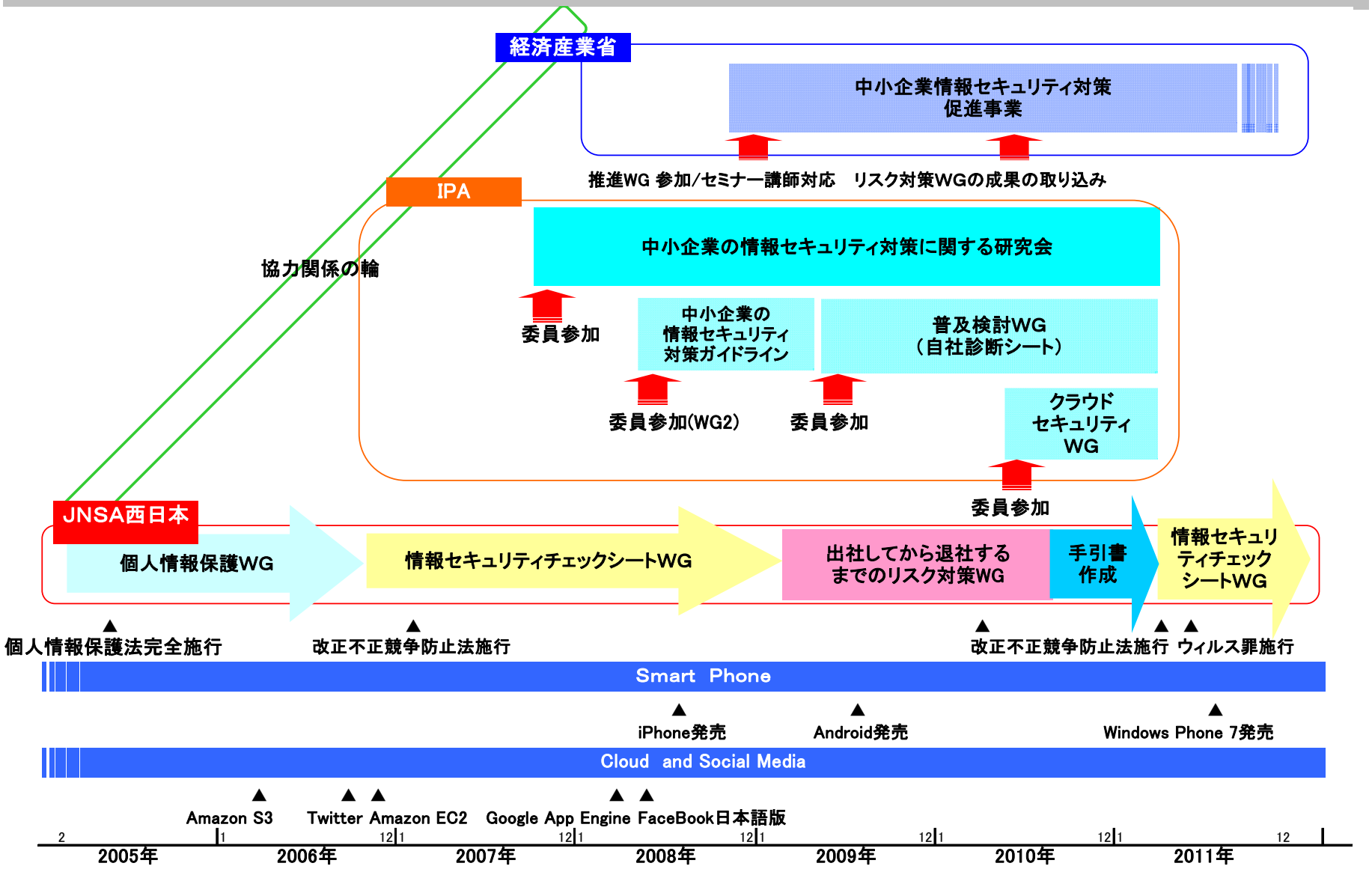
情報セキュリティチェックシートWGの現状と課題について

嶋倉　文裕
富士通関西中部ネットテック株式会社
2012年6月8日

JNSA西日本支部の中小企業セキュリティ活動



日常の危機管理

情報セキュリティチェックシート

２つの対象者向けから構成

・経営者、経営層向け

・情報セキュリティ責任者・担当者

ISO27001　管理策をベースに策定

（システム管理基準も一部、参照）

現状の情報セキュリティ対策状況を成熟度モデルで確認し、リスク認識を促す

→　実際の中小企業を対象にアンケート形式での実践調査、リスク認識の困難さが明らかに．．

リスクアプローチ手法

資産管理台帳からのアプローチ

企業の保有する情報資産を洗い出し、その資産に対するリスク分析・評価をおこなうアプローチ。

- システム管理者、資産の管理者だけで洗い出しが可能。
  ただし、ファイルサーバなどで集約的に管理されていなければ難しい。
- 資産の名称が同じでも業種、企業、部署、個人により内容は異なる。
- 資産の管理が不十分な場合、洗い出しが困難。
- 洗い出しの粒度が細かくなりがち。

リスクアプローチ手法

過去の「情報セキュリティチェックシートWG」

情報資産管理台帳の洗い出しのアプローチ
⇒固定資産台帳との区別がつかない
業界特有の資産名を例示しないと理解ができない

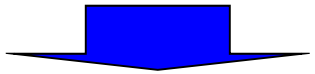
などの事実がわかりました

当時の活動の詳細とチェックシート
http://www.jnsa.org/result/2008/west/0812report.pdf
http://www.jnsa.org/seminar/2008/1217nsf2008/data/1217-C2-01checksheetA3.xls

以前の活動で認識した中小企業の限界

以前の活動から見えた中小企業のセキュリティ

- トラブル経験がなく、自社は大丈夫と考えている。
- 情報セキュリティを理解できる人がいない。
- SI‘er、ベンダーに丸投げ、情報資産の保管・格納場所さえ分からない。



このような状況で、リスク対策が企業にとって重要であるかを理解させることができるか？

リスクアプローチ手法

- **業務からのアプローチ**

  企業の持つ業務プロセスを洗い出し、その業務プロセスに対するリスク分析・評価をおこなうアプローチ。

  - それぞれの業務を行う担当者が、業務を洗い出す必要がある。
  - 業種、企業、部署、個人によって業務はそれほどに変わらない。

  例:「業務」の捉え方にもよるが、PCを利用した書類の作成、共用ファイルサーバへの情報格納、など仕事のやり方に着目すると変わらないと考える

リスクアプローチ手法

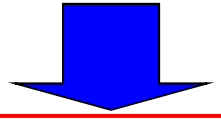
- 業務からのアプローチ
  - 資産の管理が不十分でも、業務の洗い出しは可能。
  - 洗い出しの粒度が大雑把になる可能性はある。

出社してから退社するまでのリスク対策WG

「出社してから退社するまでのリスク対策WG」で考えたこと

中小企業では、十分な資産の洗い出しをすることが難しい。

業務からアプローチする方が、リスクと紐付けし易い（資産価値の把握は困難になるが）、トラブル経験がなく、自社は大丈夫と考えている中小企業にとって、セキュリティ対策の契機となる可能性がある。



日常の業務のなかで、ヒューマンエラーを少なくする仕組みと、社員の意識の向上や、スキルアップ

業務からのアプローチ手法

大きく、５つの日常サイクルと２つの特別な業務に分類

日常サイクル	
出社	出社時の会社への入館方法
社内	社内の仕事の仕方
社外	社外の仕事の仕方
退館・退出	会社をでるときの振る舞い、退館方法
帰宅	自宅での仕事の仕方や家族との会話
特別な業務	
人事管理	入社、退職、人事評価
システム管理	システム管理者の仕事

業務からのアプローチ手法

業務の洗い出し方法

とにかく、まずは抽出し、それから整理
“業務“そのものではなく、共通的な業務のやり方にフォーカスし洗い出す

- IT系の業務
- 非IT系の業務

手引書へのまとめ

JNSA

この取り組みの結果を手引書に!

WGでは「紙」媒体のリスクについても検討しましたが、手引書では、“対象がIT”、または“対策がITで可能”なものとし、それ以外は省いています。

http://www.jnsa.org/result/2010/chusho_security_tebiki.html

手引書とWGの違い

手引書で省いたもの

（１） 対象が紙・物に関するもの　※

（２） 電源、空調等の設備管理に関するもの

（３） 対策できないもの、対策が中小企業レベルでは難しいもの

- 経営者、システム管理者等の権限者の不正
- DoS攻撃

（４） 個人情報保護に特化したもの

（５） 委託管理に関するもの

（６） 対策が教育・啓蒙になるもの

手引書では参考資料を提示

※ 手引書では記憶媒体、PCの持ち出し、廃棄などを盛り込んでおり、紙についても同様なシーンのリスクの把握は可能

情報セキュリティチェックシートWG
2011年度までの活動

情報セキュリティチェックシートWG活動

「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」と情報セキュリティチェックシートとの対応付け

⇒ ・現状の情報セキュリティチェックシートの不足内容や構成、整理の仕方を再検討

・中小企業が実際にチェック・アクションに活用できる情報セキュリティシートチェックシートへの改訂

クラウド、スマートフォンなど新しいサービスやデバイスのセキュリティの取り込み方も検討

情報セキュリティチェックシートとの紐付け

情報セキュリティチェックシートと手引書の業務との紐付け

管理策

手引書　業務No.

No.	キーワード	付属書A他	9-5紐付け	トラブル事象例
1	情報セキュリティ方針	システム管理基準　Ⅰ.情報戦略　1.全体最適化(1),(6) 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	無し	機密性、完全性、可用性のバランスを取ったシステムの利用方針がないと全てのトラブルに発展する可能性がある
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) 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	1,2,21	責任の明確化ができていないとトラブル時の対処が遅れたり、事後の対処が的確に出来ない等の可能性がある

情報セキュリティチェックシートとの紐付け

情報セキュリティチェックシートと手引書との紐付けができると、何が良いのか．．．．

- ISMS管理策ベースの情報セキュリティチェックシートの網羅性を活かす。
- 情報セキュリティチェックシートのトラブル事象が、業務ベースのリスクシナリオと結びつくことで、リスクについて、理解しやすい。

紐付け作業での課題

業務ベースで整理したリスクの対策と情報セキュリティチェックシートの対策の紐付の課題

・紐付は、「直接的な対策」のみとするか？
「補完的な対策や前提となるもの（例：手続き）」は？
手続きは全てと紐づく？

☞「直接的な対策」を基本とする
対策の前提となる手続き、コンプライアンス等については別階層で整理を加える

手順書、チェックシートの今後

現在の作業

情報セキュリティチェックシート

情報セキュリティチェックの各項目と手引書の“業務にもとづくセキュリティ対策項目“との紐付けは完了。

“業務にもとづくセキュリティ対策項目”の以下の項目を対応するチェックシートの項目に取り込む

（ ）内は情報セキュリティチェックシートの項目名

- リスクシナリオ（トラブル事象例）
- 現状のレベル（脆弱性）
- 対策（対策）

他に必要なものはないか。

（脅威がチェックシートにない。。。。）

再確認とこれからの活動

- チェックリストはPDCAサイクルいずれの視点か？
  -> 現状は現状確認(PDCAのCから)から着手という視点、まずはここからスタート。
  P、Dにおけるチェックシートって？
- 現状の確認の次に、どうすべきか「A」につながるものの示し方は？ 「判断基準」の見せ方、軽い対策から理想の対策への展開などの対策レベルの見せ方．．．
- 前提となる手続き等を別扱いとしたチェックシート項目を、どう整理するか、見せるか、の検討が必要
- キーワードの利用者視点での表現の改善、また階層別(業務フロー、システム、物理的、組織的・人的)に整理しなおすことによるわかりやすさの追求

クラウド、スマホの取り込み

次のステップ..

- クラウド利用のリスク
  中小企業のクラウド利用シーン
    - Public Cloud SaaS利用
    - ASP利用

  自社でシステムをもつリスク、持たないリスクどっち？
- スマートフォン利用のリスク
  中小企業のスマート利用シーン
    - 社外でのPublic Cloudにアクセスする端末
    - 会社支給　or 個人所有
    - Android vs iPhone

  スマートフォンのリスク、PCのリスク　違いは？

メンバー

浅野　二郎
礒元　芳昭（株式会社OSK）
井上　陽一（JNSA西日本支部長）
宇佐川　道信（パナソニックESファシリティマネジメント（株））
大財　健治（株式会社ケーケーシー情報システム）
久保　寧（富士通関西中部ネットテック株式会社）
小柴　宏記（株式会社ケーケーシー情報システム）
小山　正人（キャノンITソリューションズ株式会社）
齋藤　聖悟（株式会社インターネットイニシアチブ）
塩田　廣美
嶋倉　文裕（富士通関西中部ネットテック株式会社）
元持　哲郎（アイネット・システムズ株式会社）