JNSA

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

出社してから退社するまでのリスク対策WG
【中小企業対策編】

元持哲郎
アイネット・システムズ株式会社
JNSA西日本支部

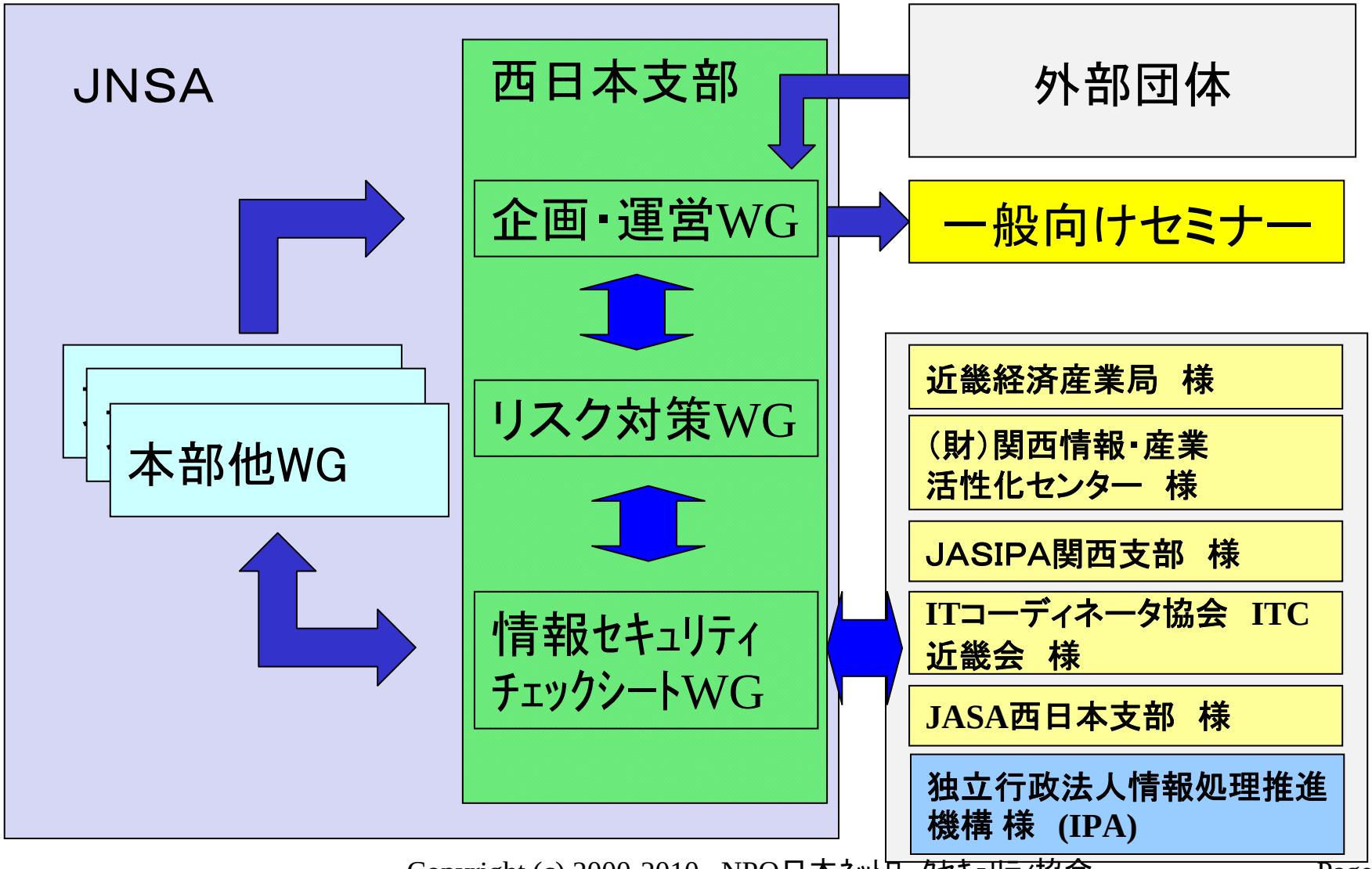
2010 年 6月11日

概　要

２００４年に開始した中小企業向け個人情報保護WG活動をステップアップし、中小企業向けにセキュリティ対策のガイドラインとして「情報セキュリティチェックシート」を作成しました。次のステップとして「情報セキュリティチェックシート」を活用したリスク分析・評価・対応・対策方法を検討します。

地域性・企業規模への視点での活動が支部に与えられた命題とも考えており、関係する本部の他のWGにも、西日本支部代表として参加しながら、整合性にも配意して推進します。

WGの体制



目　標

中小企業で想定される一般的な業務を洗い出し、それぞれの業務に潜む情報セキュリティ上のリスクを特定し、各リスクに対する対応・対策を検討します。

具体的には、

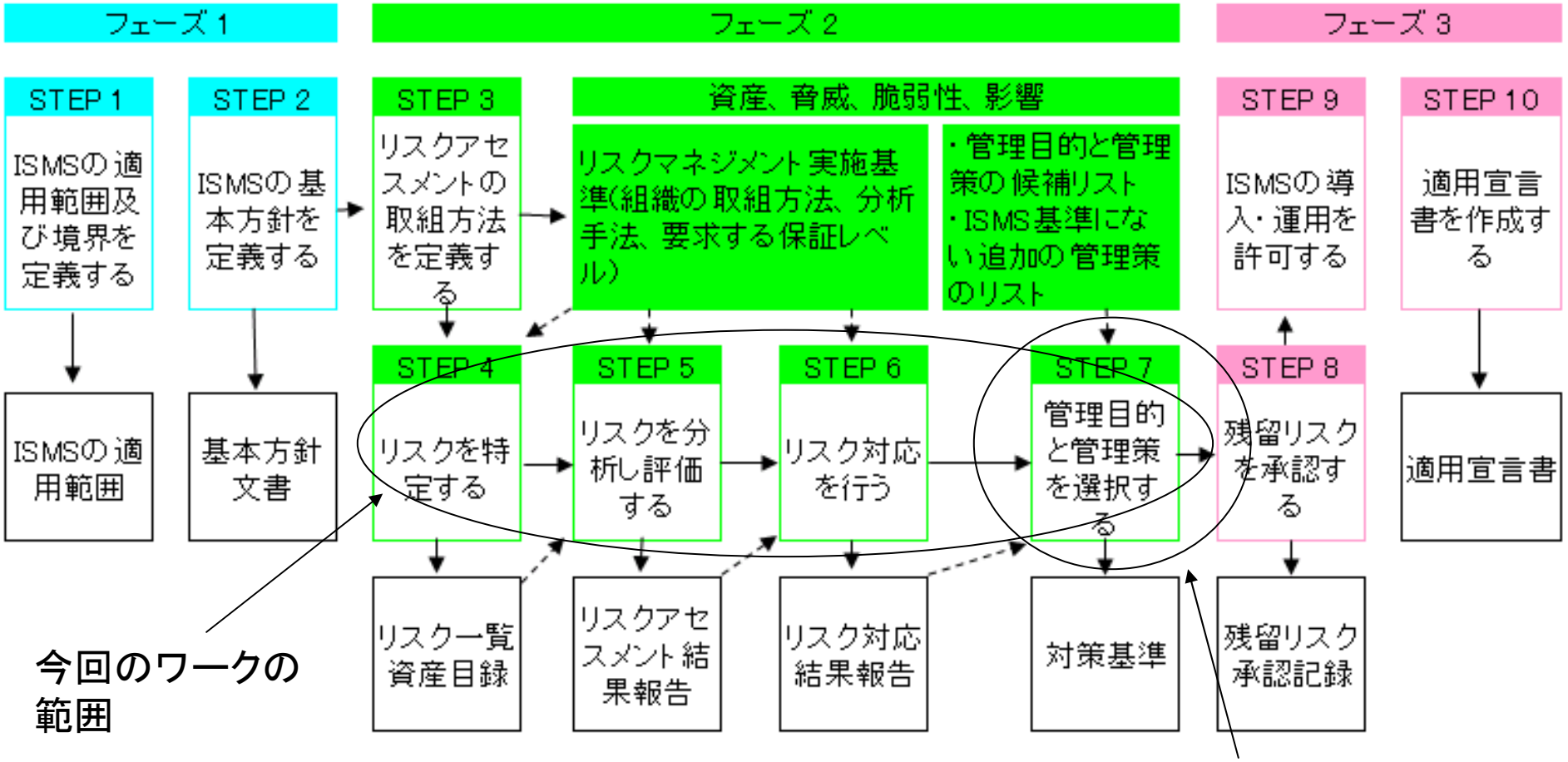
- 出社から退社までの業務の中で、発生するリスクの特定、分析、評価、対応すべき情報セキュリティ対策を行う
- 例示した業務を持つ中小企業がすぐにリスク対策を活用、参考できるようなDSS化の検討
- リスクの定量化の検討

スケジュール

フェーズⅠ　2009年	3	4	5	6	7	8	9	10	11	12	1	2
方法論の検討	◆→											
業務の洗い出し		◆→	→◆									
リスク分析・評価・対応・対策				◆→	→	→	→	→	→	→◆		
見直し及び整理											◆→	→◆

フェーズⅡ　2010年	3	4	5	6	7	8	9	10	11	12	1	2
見直し及び整理(2009より続き)	◆→	→	→	→◆								
DSS化の方法論検討					◆→	→◆						
DSS化作業							◆→	→	→	→◆		
リスクの定量化検討	◆→	→	→	→	→	→◆						
成果報告											◆	
まとめ											◆→	→◆

リスク対策はISMSをベース



※JIPDEC ISMSユーザーズガイドより

情報セキュリティチェックシートの範囲

WGでの対象の中小企業

従業員数が100名～300名で、下の表の意識が○、△の企業

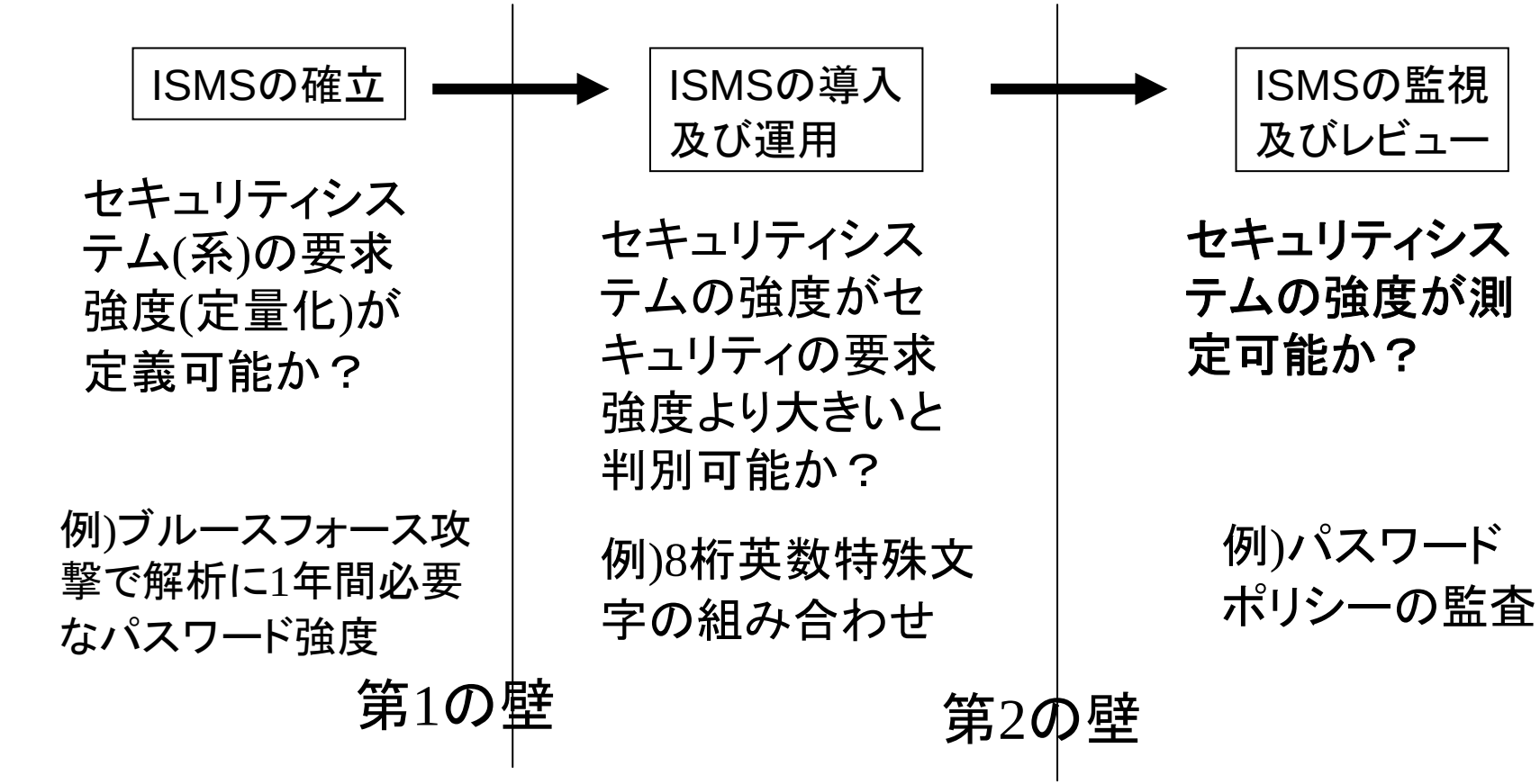
企業分類	意識	対策の要請
取引先からの要請に応える事が求められる企業 （大手企業との取引のウエイトが高い企業）	◎	企業規模に拘わらず委託元と同等の水準を求められている。
責任の明確化・職務の分類が行われている企業 （自社の情報セキュリティ対策が必要な企業）	○	企業価値向上・内部統制等目的から対策する事の必要に迫られている。
永遠のビギナー （責任の明確化・職務分類が行われていない企業）	△	守るべき情報資産があり、守らねばならない必要意識が漠然とはあるが、費用対効果が見えず躊躇・逡巡し、対策の実践が伴わない。
	×	情報セキュリティ対策の必要を感じない。

WGの対象

リスク対策例 Phase1

業務	PCの起動･ログイン
現状のセキュリティレベル	①パスワードが簡単なため覗き見で判ってしまう ②パスワードをメモとして書き貼り付けている
リスクシナリオ	ログオン時の覗き見やパスワードをメモ書きし貼り付けていることによりパスワードが漏えいし、機密情報に不正アクセスされる
業務対象	その業務をする人
情報を保存･処理する場所	PC
影響	機密性、完全性、可用性
情報の形状	無形
脅威	訪問者、委託業者、従業員(本人外)
責任	従業員
対策の仕組み	①適当な強度(8文字以上、英数字記号の組み合わせ)を持つパスワードを設定できるIDを作成し、定期的に変更する ②パスワードを書いた紙を人目にさらさない
対策	①適当な強度(8文字以上、英数字記号の組み合わせ)を持つパスワードを設定できるIDを作成し、定期的に変更する ②パスワードを書いたメモの管理を行う(人目にさらさない)

セキュリティ強度



リスク対策例　Phase2

業務	PCの起動･ログイン
現状のセキュリティレベル	①パスワードが簡単なため覗き見で判ってしまう ②パスワードをメモとして書き貼り付けている
リスクシナリオ	ログオン時の覗き見やパスワードをメモ書きし貼り付けていることによりパスワードが漏えいし、機密情報に不正アクセスされる
業務対象	その業務をする人、業務を管理する人
情報を保存･処理する場所	PC
影響	機密性、完全性、可用性
情報の形状	無形
脅威	訪問者、委託業者、従業員（本人外）
責任	従業員、システム管理者
対策の仕組み	①適当な強度（8文字以上、英数字記号の組み合わせ）を持つパスワードを設定できるIDを作成し、定期的に変更する ②パスワードを書いた紙を人目にさらさない
技術的対策	複雑なパスワード、定期的パスワードの変更をさせるシステムを導入する
人的対策	①適当な強度（8文字以上、英数字記号の組み合わせ）を持つパスワードを設定できるIDを作成し、定期的に変更する ②パスワードを書いたメモの管理を行う（人目にさらさない）
対策のチェックポイント	パスワードポリシーを確認する

アルゴリズム化

定義

①フローとして記述可能

②分岐がある場合は明確な判断基準がある

範囲

プログラムではなく、人が行為を行う場合でも①②を満たす場合はアルゴリズム化と言う

メリット

1.チェックが可能

2.人が行う場合、工数計算が可能（費用化）

3.プログラム化が可能（費用化）

→JNSA企業でツール化商品化の検討が可能！

アルゴリズム化の例

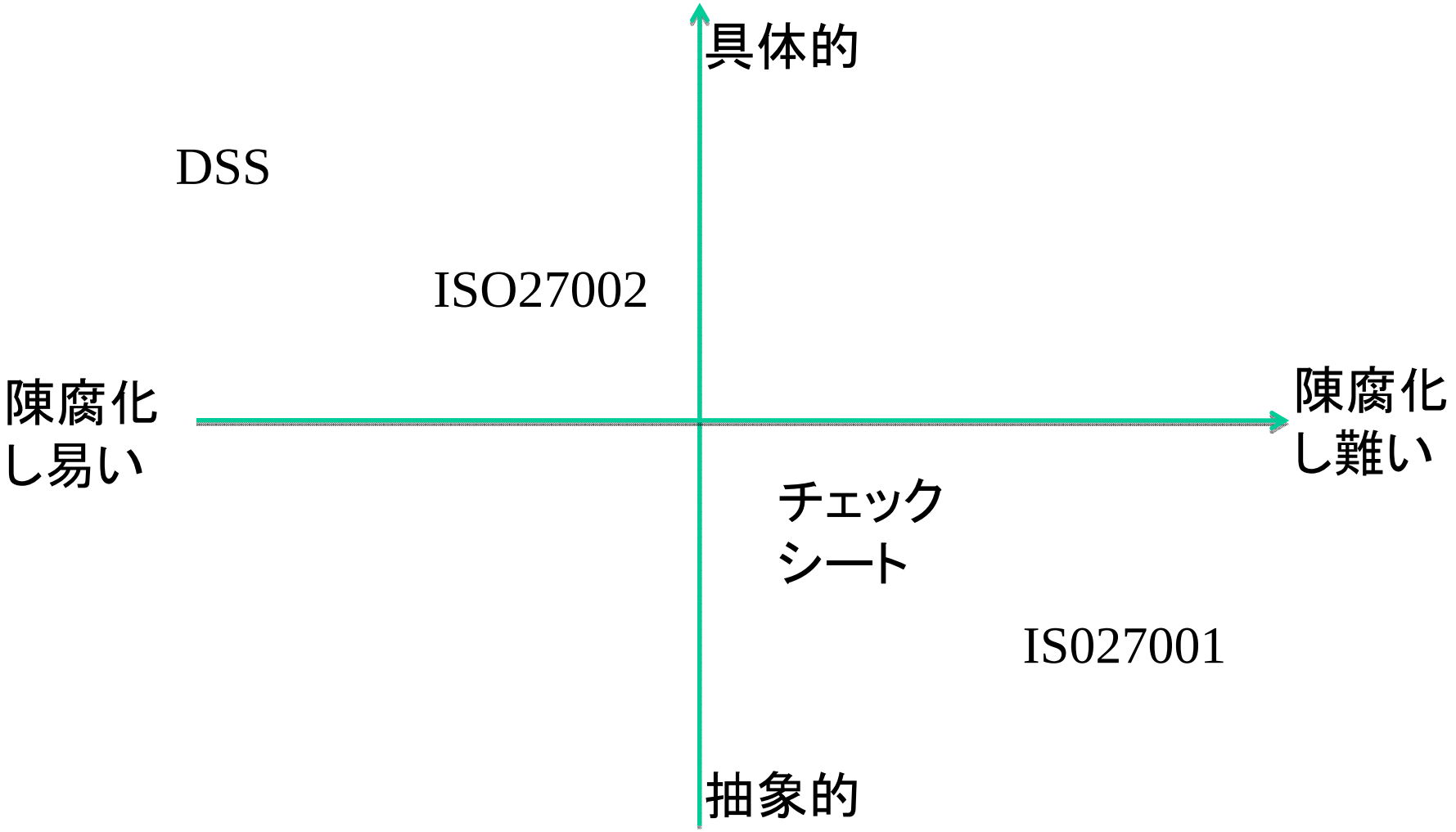
- リスク事象

  ヘッダー、フッター、ファイル属性から重要情報が漏えいする
- 人的アルゴリズム

  ヘッダー情報、フッター情報、ファイル属性の確認
- プログラム化

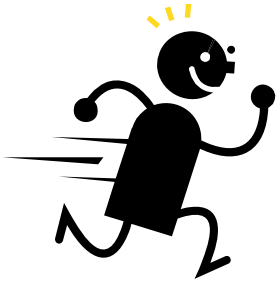
  「ドキュメントの検査」機能の利用（Office2007以降）

DSSとチェックシートの比較



現状の問題点

- アルゴリズム化の限界
- 業務のプロセスとアルゴリズム化と相性が悪い？
  - システム管理 ❤ アルゴリズム化
  - 通常業務 ❤ チェックシート or教育
- 陳腐化の速度が速い



Speed Up!

出社してから退社するまでのリスク対策WGの歩みと今後！

業務の洗い出し
- 通常業務で発生する業務パターンを網羅的に洗い出し
- パターンを共通化し一般的業務として抽出

リスク事象の特定
- 業務とその対象となる情報資産と脆弱性を紐付け
- 業務に潜むリスク事象を特定

リスク対策
- リスクに対応するリスク対策を網羅的に洗い出し
- 対策が可能であるもの＋中小企業規模で可能なもののみを選択

編集
- 対象がITか対策がITであること
- 対策を技術的対策と人的対策に編集＋チェックポイントの追加
- 重複する対策の併合
- 現状のセキュリティレベルとリスク対策の整合性

DSS
- リスク対策の目的
- セキュリティ事象
- 技術的対策、人的対策（管理責任者と業務担当者に分け対策を検討）←PCI DSSの要件に相当
- チェックポイント←PCI DSSのテスト手順に相当

WGメンバ

50音順、敬称略

- 浅野　二郎
- 礒元　芳昭
  株式会社OSK
- 宇佐川　道信
  パナソニック電工株式会社
- 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
- 斎藤 聖悟
  株式会社インターネットイニシアティブ
- 嶋倉　文裕
  富士通関西中部ネットテック株式会社
- 田口　智子
  株式会社 ラック
- 宮下 勝彦
  ヒューベルサービス株式会社
- 元持　哲郎　WGリーダ
  アイネット・システムズ株式会社
- 近畿経済産業局地域経済部　情報政策課
- 井上　陽一
  JNSA顧問・西日本支部長

ご清聴ありがとうございました。