JNSA

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

情報セキュリティチェックシート WG報告

元持哲郎
アイネット・システムズ株式会社
JNSA西日本支部

2007 年 6 月6日

概　要

中小企業向け個人情報保護対策WGとして作成した「個人情報保護対策チェックシート」を情報セキュリティ全般を対象としたチェックシートに進化させ、中堅・中小企業の情報セキュリティ対策のガイドライン作成を目指します。

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。

目　標

大阪に集積する製造業の情報セキュリティ全般に焦点を当て、“おおさか”にフイットした中小企業向け情報セキュリティのガイドラインを作成し、情報セキュリティレベルの向上により、“おおさか”をより元気にすることを目指します

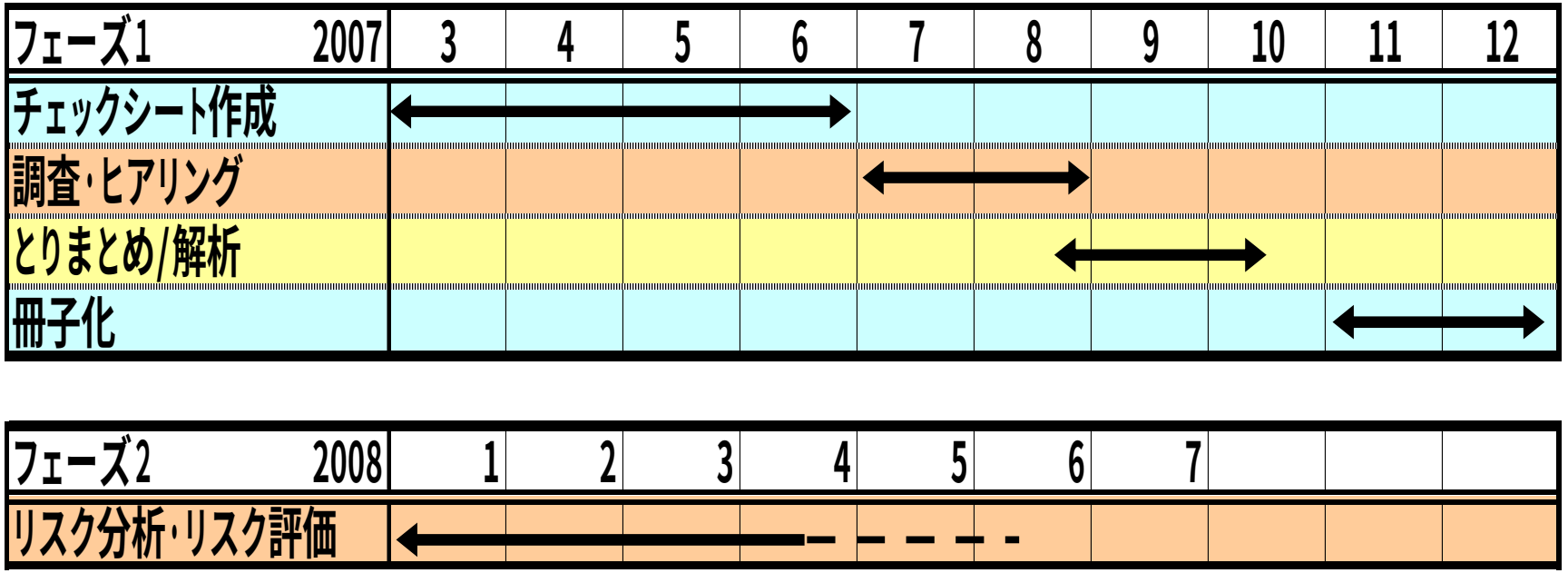
具体的には、

•ITの活用を前提として、機密性･完全性に偏重したチェックシートから可用性も意識したチェックシートの作成をします

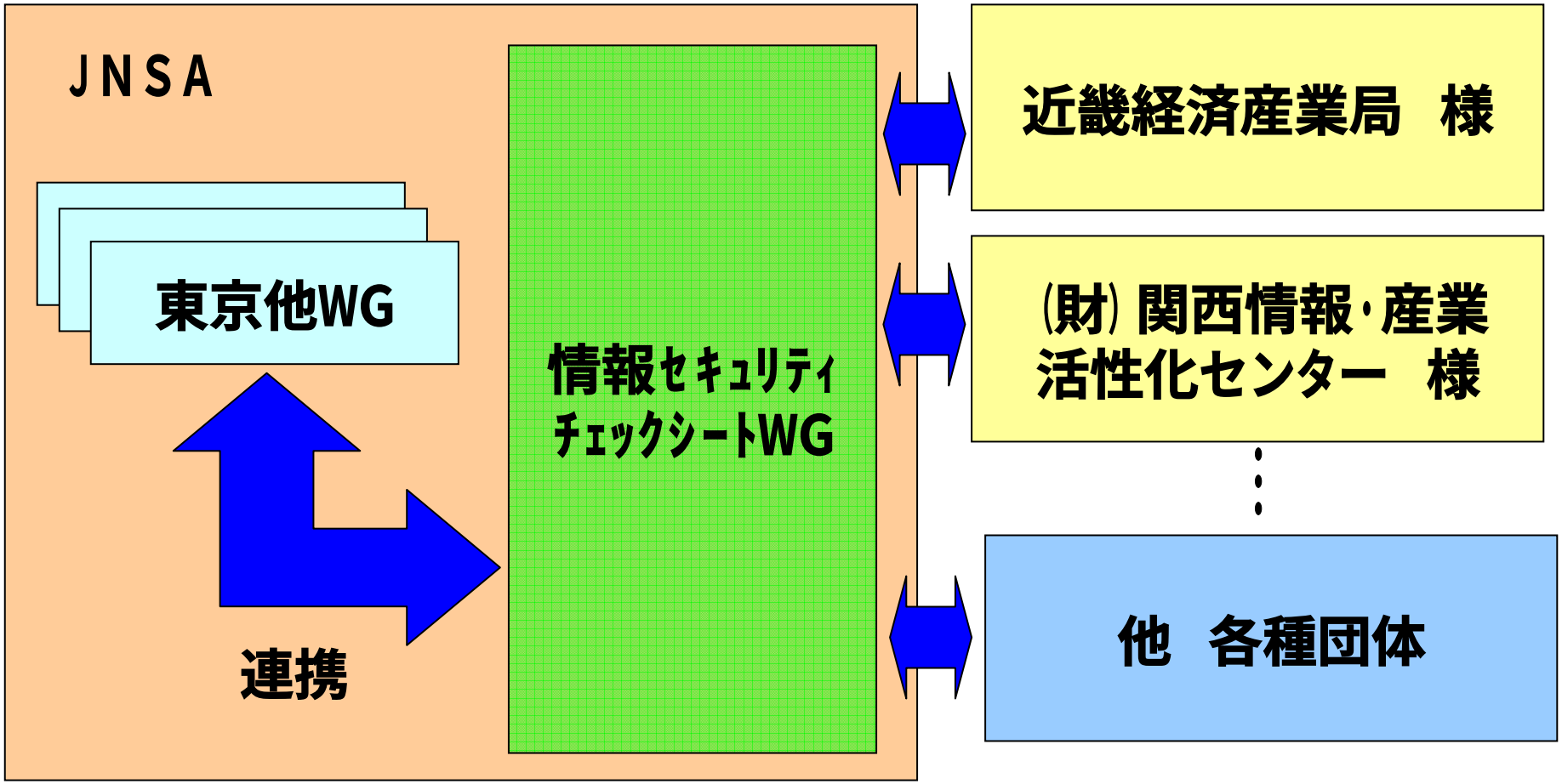
•セキュリティレベルを測定できる物差し(チェックシート)を作成し実際に測定(アンケート及びヒアリング)します

•測定結果を解析することで、中小企業がSI’er,ベンダーへのRFPに活用して頂けるものにします

スケジュール



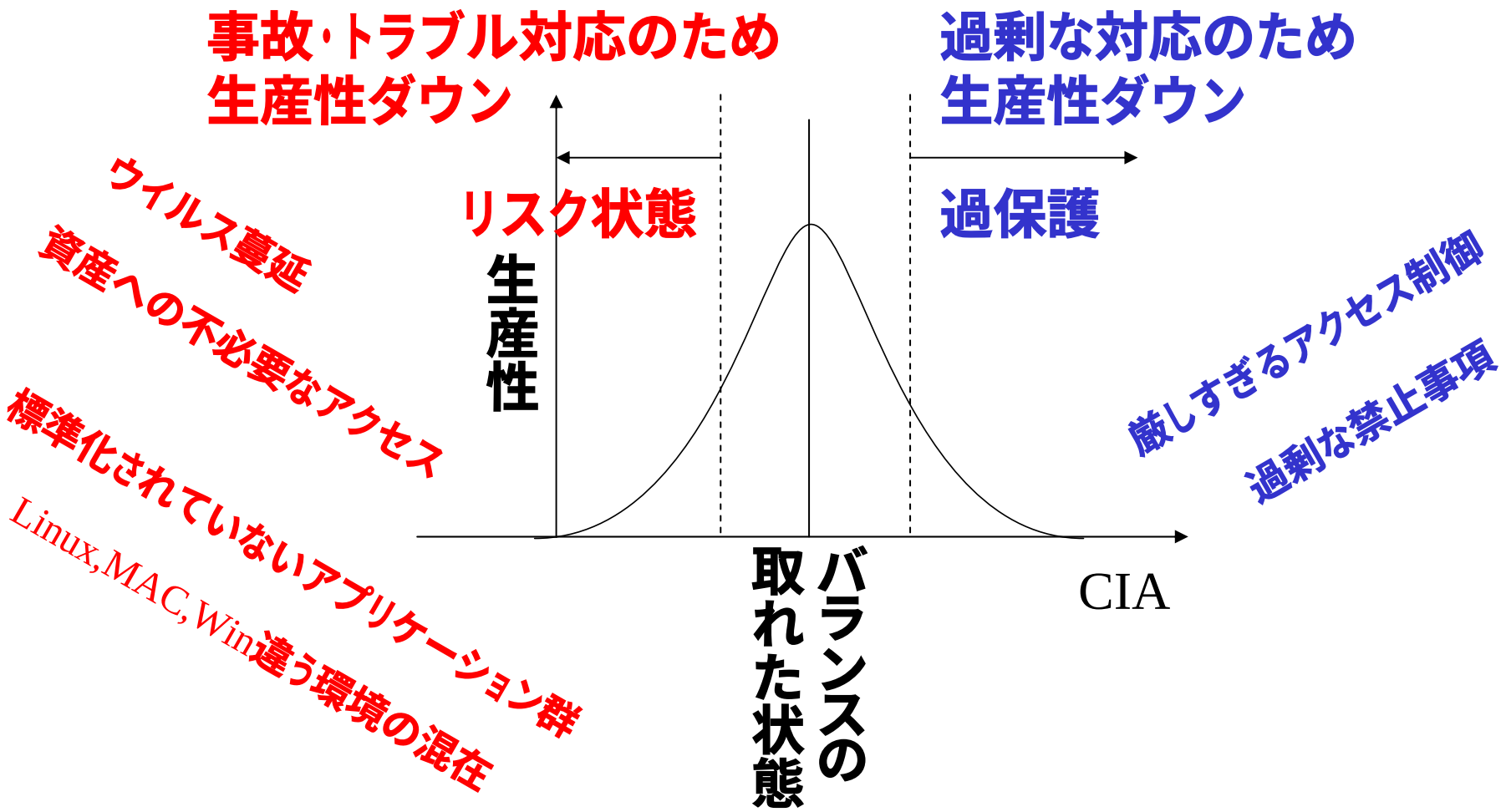
WGの体制



WG活動で使用する仮説

- セキュリティレベルの向上で生産性を向上できる
- セキュリティレベルはアンケートで測定可能である
- セキュリティレベルは企業規模に依存する

セキュリティレベルの向上で生産性を向上できる？



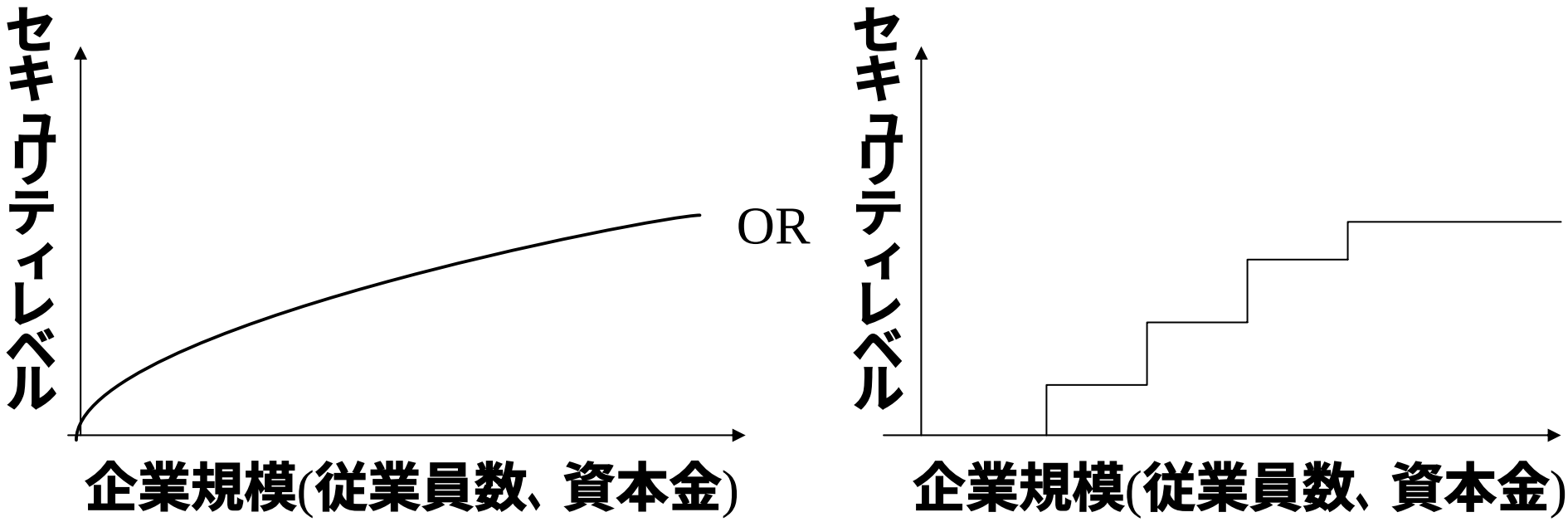
セキュリティレベルはアンケートで測定可能である？

- アンケート回答者による、解釈、評価等主観的要素をどうするか？
  ➡ アンケート対象者を経営層と実務層とに区分すると共に、回答戴く対象企業を企業規模別に予め分類、リクエストする事で、吸収できる様にしたい

- 機密性、完全性のみならず可用性も考慮に入れて測定可能か？
  ➡ SLAも加味した効率性・生産性視点でのシステム管理基準的な要素を加える

- 企業のリスクに見合ったセキュリティレベルを評価できるか？
  ➡ ユーザ視点でリスク分析・リスク評価を実践するフェイズ2で対応

セキュリティレベルは企業規模に依存する？



セキュリティレベルは従業員1人あたりの対策費用に関係すると考えられる事から、IT投資に負担感を感じている中小企業にとっては対策の形骸化の恐れあり？

製造業を対象とする理由

JNSA

•大阪には製造業が多く分布している

各事業者の比率	近畿	大阪	全国
製造業事業者	11.83%	12.56%	9.74%
農林漁業	0.11%	0.02%	0.31%
鉱業	0.02%	0.00%	0.06%
建設業	7.71%	5.79%	9.53%
電気・ガス・熱供給・水道業	0.04%	0.03%	0.05%
情報通信業	0.80%	1.08%	0.92%
運輸業	2.03%	2.26%	2.20%
卸売・小売業	27.69%	26.83%	27.47%
金融・保険業	1.25%	1.18%	1.45%
不動産業	5.82%	6.74%	5.35%
飲食店，宿泊業	13.80%	14.05%	13.56%
医療，福祉	4.75%	4.73%	4.65%
教育，学習支援業	2.72%	2.95%	2.78%
複合サービス事業	0.41%	0.23%	0.52%
ｻｰﾋﾞｽ業(他に分類されないもの)	16.97%	16.07%	18.19%

（出所）総務省　「平成１６年度事業所・企業統計調査」より

製造業を対象とする理由

- 西日本支部の活動目的「西日本における情報セキュリティレベルの維持向上を図る事により大阪をより元気にしたい！」にフイットする活気ある業種
- 重要な情報資産及び脅威が特定し易い
- JK(自主改善)活動、安全活動を通してPDCA、リスク管理を導入している
- 靴製造からハイテクまで多岐に分かれており製造業の中でも分類が可能

対象とする中小企業の規模

中小企業庁や商法の定義より対象を決定

- 中小企業者の定義
  ３００人以下　又は　３億円以下の資本金

- 小規模企業者の定義
  ２０人以下

企業規模ごとのアプローチ

	近畿内の製造業における従業員比率		大阪内の製造業における従業員比率	
	事業者数	比率	事業者数	比率
小規模企業	105,961	86.55%	50,128	87.54%
中規模企業	15,882	12.97%	6,923	12.09%
大規模企業	544	0.44%	195	0.34%

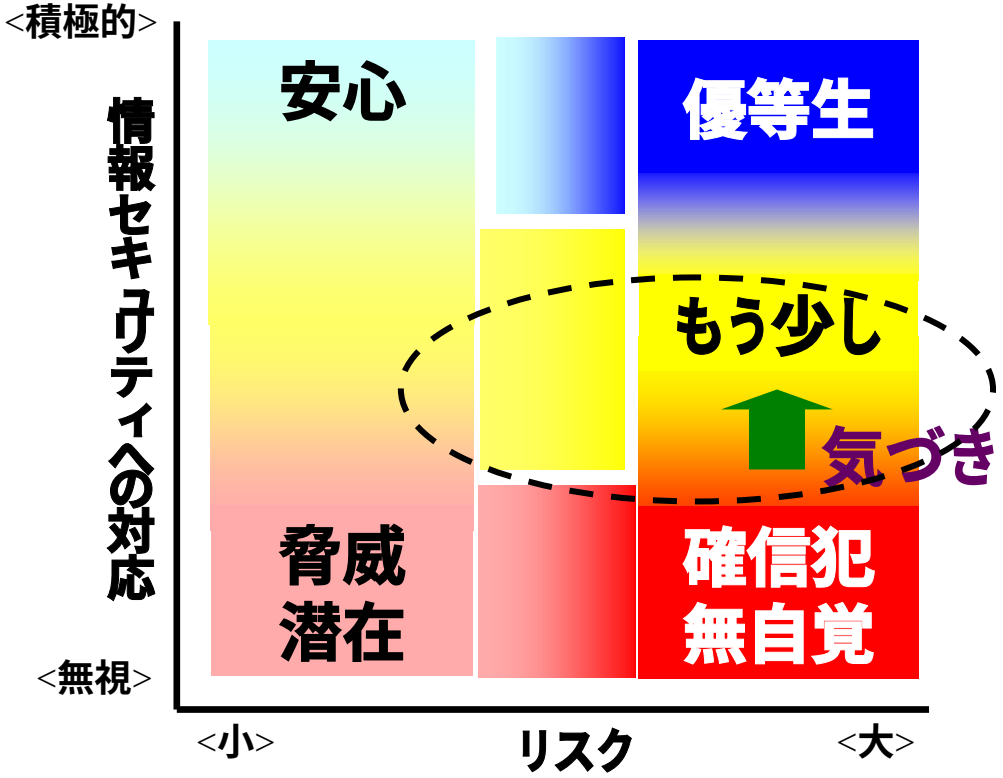
（出所）総務省　「平成１６年度事業所・企業統計調査」より

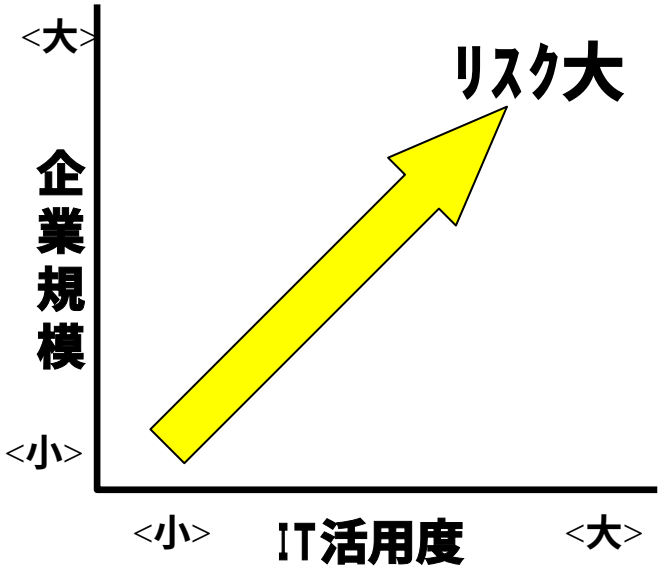
小規模企業 → 簡易版チェックシートを提供

中規模企業 → チェックシートによるアンケートを実施

大規模企業 → 独自で対策する体力あるという理由から対象外

対象とする中小企業





チェックシートの比較

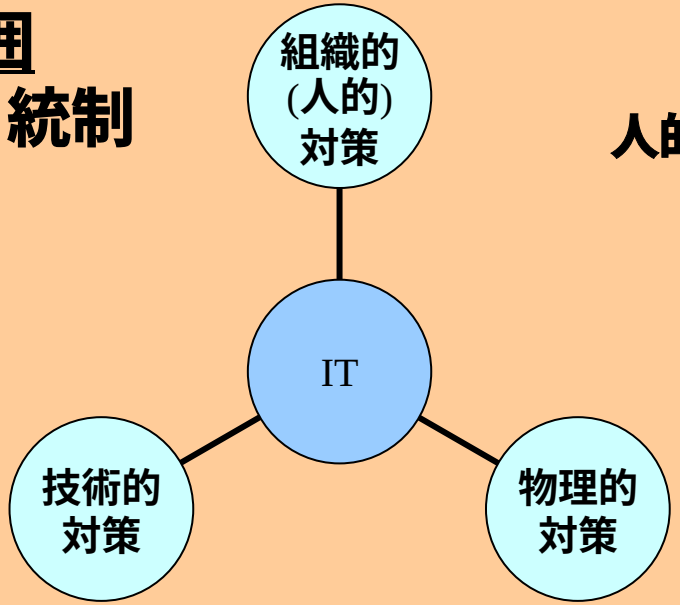
比較項目	ISO27001 付属書A	個人情報保護対策チェックシート	システム管理基準
セキュリティ(C,I)	◎	○	×
	セキュリティ全般(特にネットワーク?)に重点	ISO27001 とほぼ同じであるが、電子データの漏えい対策に重点をおいている	システム管理全般にわたる。開発・運用に重点
セキュリティ(A)	○	△	◎
	・バックアップ ・事業継続	・バックアップ	・バックアップ ・運用における障害対策 ・災害対策 ・事業継続
ITの活用	IT活用が前提?	IT活用が前提	戦略的に全体最適を考慮して利用
表現	やや抽象的	具体的	抽象的

比較によりISO27001を基礎にシステム管理基準も採用、個人情報保護対策チェックシートの表現・編集方法も組み込む

チェックシートの範囲

対象範囲

IT統制



人的対策は組織的対策に含める

アンケートの対象を経営者並びに実務層としている事から、回答者も組織を意識した回答となる事が想定されるため

対象者

- 経営者
- 実務者

＜対象外＞
事業継続

チェックシートの作成-進行中

No.	項目	管理策	システム管理基準 項目 No	システム管理基準	対策分類	チェックシート案
A.5	セキュリティ基本方針		I	情報戦略		
A.5.1	情報セキュリティ基本方針		1	全体最適化		
目的	情報セキュリティのための経営陣の方向性及び支持を、業務上の要求事項、関連する法令及び規則に従って規定するため。					
			(1)	ITガバナンスの方針を明確にすること。	組織的	セキュリティを考慮した情報システムの利用・活用方針を明確にしていますか?(機密性、完全性、可用性のバランスを取った情報システムの利用方針)
A.5.1.1	情報セキュリティ基本方針文書	情報セキュリティ基本方針文書は，経営陣によって承認され，全従業員及び関連する外部関係者に公表し，通知すること。	(6)	情報セキュリティ基本方針を明確にすること。	組織的	
A.6	情報セキュリティのための組織		I	情報戦略		
A.6.1	情報セキュリティ基盤		2	組織体制		
目的	組織内の情報セキュリティを管理するため。					
			2.1 (1)	全体最適化計画に基づき、(情報システム化)委員会の使命を明確にし、適切な権限及び責任を与えること。	組織的	経営陣は，情報システムの使用及び情報セキュリティの責任に関する明りょうな方向付け，組織のなかのそれぞれの職務の使命、責任を明確にしていますか？
			2.2 (1)	情報システム部門の使命を明確にし、適切な権限及び責任を与えること。		
A.6.1.1	情報セキュリティに対する経営陣の責任	経営陣は，情報セキュリティの責任に関する明りょうな方向付け，自らの関与の明示，責任の明確な割当て及び承認を通して，組織内におけるセキュリティを積極的に支持すること。				
A.6.1.2	情報セキュリティの調整	情報セキュリティ活動は，組織のなかの，関連する役割及び職務機能をもつさまざまな部署の代表が，調整すること。				
A.6.1.3	情報セキュリティ責任の割当て	すべての情報セキュリティ責任を，明確に定めること。				

現状の課題

- アンケートの設問を40問程度に抑える
- 設問で求める内容が複数の対応となっている場合の整理の仕方をどうするか？

  (アンケートでの回答時に迷いのないシンプルなものが望ましい)
- インフラ整備の側面と、運用の側面をどのように区別して設問するか？
- システム管理基準でのIT活用方針をどう表現するか？どう包含させて表現するか？
- 危機意識を啓発するためにトラブル対策を前提に設問を構成するが、保守的要素のあるものはどうするか？

WGメンバ

５０音順、敬称略

- 浅野　二郎
- 市川　順之
  伊藤忠テクノソリューションズ株式会社
- 臼井　義美
  株式会社ウェブエージェント
- 近畿経済産業局地域経済部　情報政策課
- 久保　寧
  富士通関西中部ネットテック株式会社
- JNSA西日本支部のメンバ　　アドバイザリ
- 嶋倉　文裕　WGリーダ
  富士通関西中部ネットテック株式会社
- 西村　祥
  伊藤忠テクノソリューションズ株式会社
- 元持　哲郎
  アイネット･システムズ株式会社
- 井上　陽一　　特別顧問
  ＪＮＳＡ西日本支部長

ご清聴ありがとうございました。