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

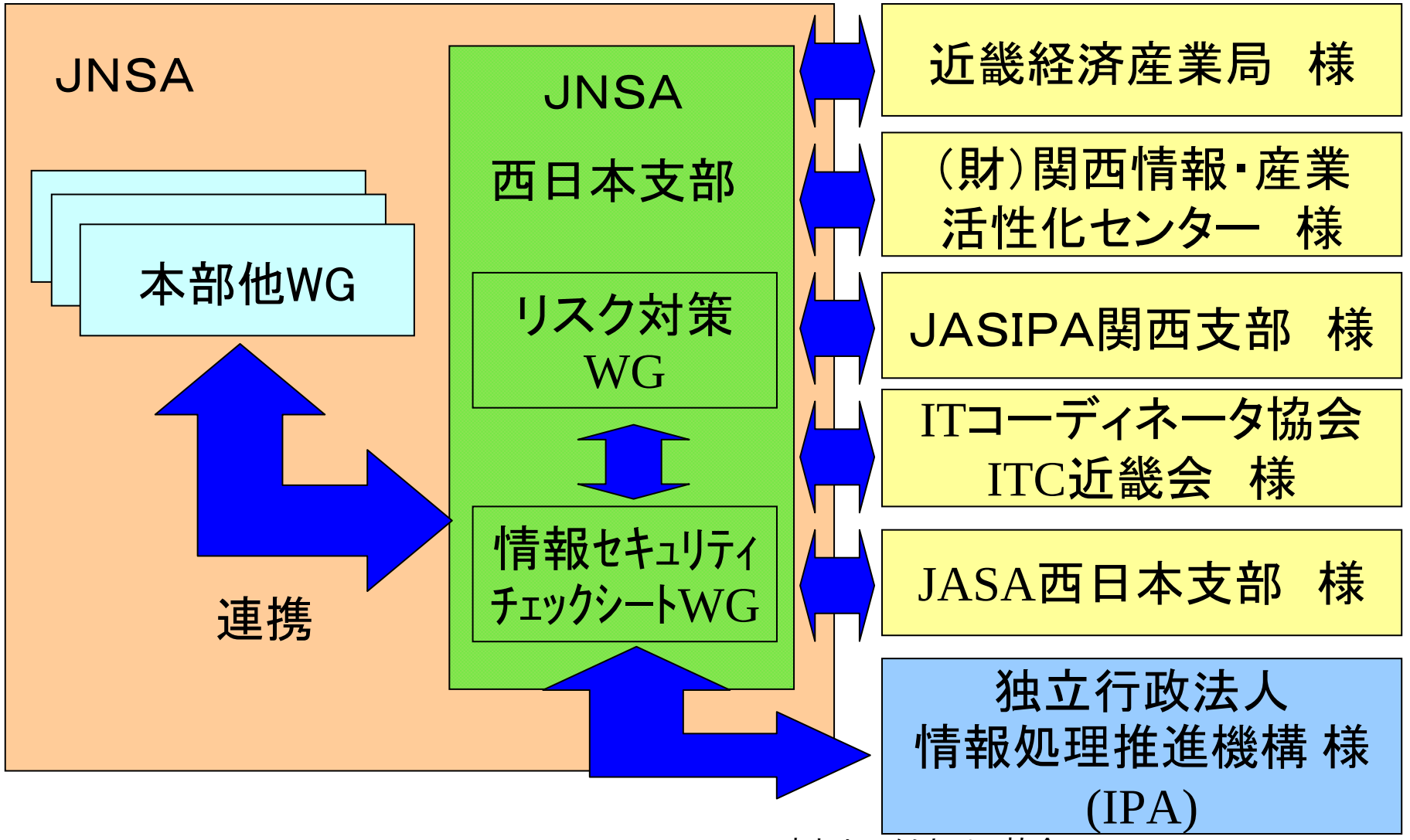
元持哲郎
アイネット・システムズ株式会社
JNSA西日本支部
2009 年 6月3日

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、

- 資産の洗い出しが不十分でもリスク対策が可能な手法の検討
- 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1　2009	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				↔	↔	↔						
結果の見直し							↔					
リスク定量化方法等課題検討								↔	↔			
セミナーでの成果発表									●			
まとめ										↔	↔	↔

フェーズ2　2010	3	4	5	6	7	8	9	10	11	12	1	2
リスクの定量化	←										→	?

情報セキュリティチェックシートWG からの経緯

チェックシートの紹介　1

各情報セキュイリティ対策の項目

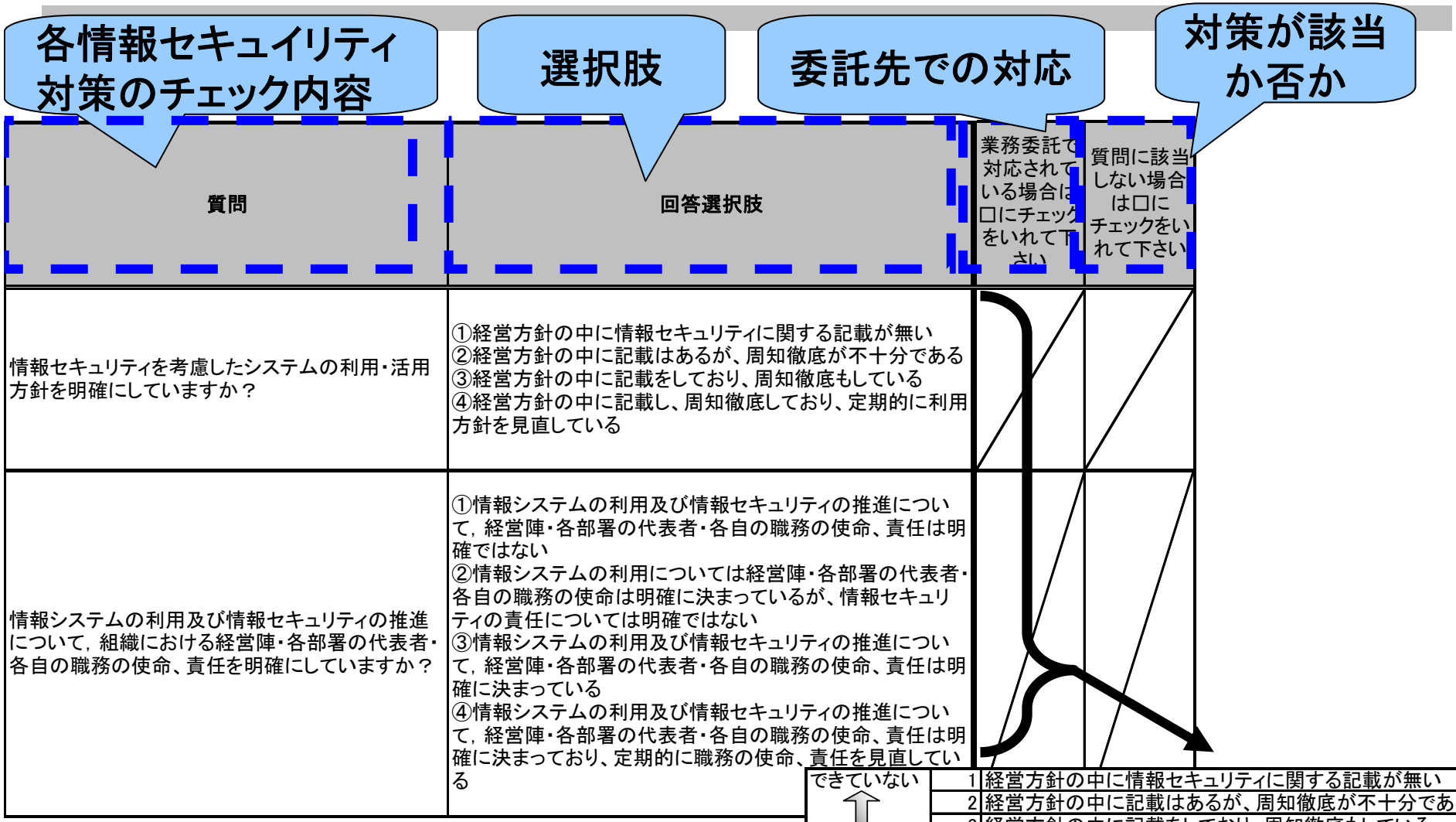
各情報セキュイリティ対策が対象とするもの

各情報セキュイリティ対策のカバー対象

リスクが想定できるようにトラブル事象例を表示

No.	キーワード	対象					影響			トラブル事象例
		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	
1	情報セキュリティ方針	○	○	○	○	○	○	○	○	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

チェックシートの紹介　2



チェックシートの紹介　３

経営者向け大項目

１．情報セキュリティ方針
２．責任の明確化
３．職務の分離
４．委託先の管理
５．情報資産管理台帳
６．文書化された手続き
７．ルール
８．秘密保持
９．ゾーン管理
１０．入退管理
１１．サービスレベルの確保（２つのチェック項目）
１２．ソフトウエアの選別と開発
１３．業務データの管理
１４．障害報告
１５．障害対策
１６．情報システム監査

チェックシートの紹介　４

情報システム部門向け大項目

１．ID
２．パスワード
３．アクセス権限
４．ネットワークアクセス制御（４つのチェック項目）
５．ウィルス（２つのチェック項目）
６．PC・電子媒体・紙の管理
７．電子メール
８．オンライン取引
９．　インターネット販売
１０．ホームページ
１１．監査ログ
１２．障害ログ
１３．バックアップ
１４．性能管理
１５．リリース管理
１６．変更管理
１７．構成管理

アンケートの方法

情報セキュリティチェックシートによるアンケートと一部、ヒアリングを行い、中小企業の情報セキュリティ対策の状況調査と情報セキュリティチェックシートの有効性を調査

Step１　近畿経済産業局様のご支援により
１５社先行調査
Step２　近畿中小企業３３７社に郵送し、
調査（回答　１６社）

調査からの事実　1

全体的な特徴

①組織的な対策は二極化

②取引先から情報セキュリティ対策を求めれている企業は、要求事項に沿いバランスよく対策されている

③品質ISO、環境ISOの監査と情報セキュリティ監査を誤解しているケースあり

④情報資産管理台帳と固定資産との区別がない

⑤ID管理、パスワード管理は企業によりばらつき大

⑥二極化とは関係なく、ウィルス対策や障害対策は実施済み

調査からの事実 2

情報セキュリティが組織化されていない企業

①トラブル経験がなく、自社は大丈夫と考えている。
（差し迫った問題ではない）（他人事）

②他社（外部）に迷惑をかける事は無いと思いこんでいる。

③性善説尊重（フアミリー的）、信用・信頼がビジネスの原点。

④チェックシートの内容を理解できる人がいない。
総務部門等が兼務しており業務に忙殺されている。

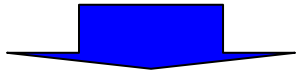
⑤SI‘er、ベンダーに丸投げ、情報資産の保管・格納場所さえ分からない。

情報セキュリティチェックシートの課題

情報セキュリティチェックシートの課題

・情報セキュリティチェックシートによる「気づき」を期待するが企業側がそれを理解できたか疑問

・情報セキュリティチェックシート回答企業の多くは情報資産管理台帳を作成していない
平均レベル　２以下）



情報資産管理台帳が情報セキュリティ対策の入り口のはず！

調査の方法

JNSA

情報資産管理台帳の雛形を提示し、実際に作成して頂くことで、情報資産の把握、リスク認識、および情報セキュリティ対策への展開につながることを期待

実際の作成とアンケート調査を実施

対象を金型業界、および鞄業界に絞り郵送調査（約200社に郵送、5社回答）

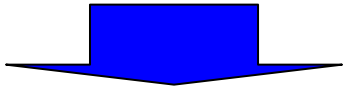
各業界特有の情報資産名を考慮した記入例、および影響度の説明を添付

情報資産管理台帳

管理No	情報資産名	対象（媒体）	保管・格納場所	利用範囲	管理部門情報			台帳登録日	廃棄日	保存期間	最終棚卸し日	影響度			備考
					管理責任部門名	管理責任者	連絡先					機密性	完全性	可用性	
記入要綱	別紙「情報資産分類」を参考に記入 情報資産例より細かくても、それらを組み合わせたものでも良い、管理する単位で洗い出すこと	情報資産が情報の場合、情報が保存された状態あるいは保存されている媒体を記入 例） ・紙 ・設計製造システム ・CD－R ・ファイルサーバ 等	情報資産が保管・格納される場所を記入 例） 情報の保管場所がサーバ、PCの場合 ・ホスト名 を記入、 紙の場合 ・ロッカー ・キャビネット 等	情報資産の利用範囲を記入 ・全社 ・部内 ・課内 ・グループ内 ・××プロジェクト内 ・幹部社員内 等		情報資産の実際の管理責任部門名、管理責任者、連絡先（内線、外線、ﾒｰﾙｱﾄﾞﾚｽ）を記入		情報資産の本台帳への登録日を記入	情報資産を廃棄する場合、廃棄した日を記入（初回記入時は空白）	登録日に情報資産の保存期間を記入 特に情報の場合、法令や契約を考慮して記入すること	情報資産の棚卸しを最後にした日を記入（初回記入時は現在の日にち）		別紙「CIA影響度」を参考に情報資産が情報か情報以外かに注意して影響度を記入		
記入例															
1	要求仕様書	ファイルサーバ	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
2	構想図面	ファイルサーバ	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		5年	2008/8/26	2	3	3	
3	承認図	ファイルサーバ	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
4	設計図面データ	設計製造システム	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
5	設計図面	紙	鍵つきキャビネット	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
6	部品図	紙	鍵つきキャビネット	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
7	加工データ	設計製造システム	サーバルーム	製造部門	製造部門	製造部長	内線:4444	2008/8/26		永久	2008/8/26	2	3	3	

これまでの調査や他の調査を踏まえて　1

①機密性、完全性、可用性の理解あるいは資産管理台帳の例示が適当であれば、中小企業でも作成が可能（実際に従業員２１人規模の企業で記入例にない資産も挙げることができた）



・企業規模が小さく、経営者(あるいは少数の管理者)が情報資産の責任者になっている場合は比較的容易に洗い出しができると思われる

・詳細かつ網羅性を求めなければ、たとえ中小企業であっても情報資産の洗い出しができると思われる
例えば、ある一定以上の重要な情報資産をまずは洗い出すなど

チェックシートからリスク対策へ

WGでの対象の中小企業

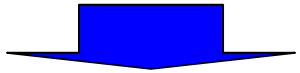
従業員数が100名～300名で、下の表の意識が〇、△の企業

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）	〇	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

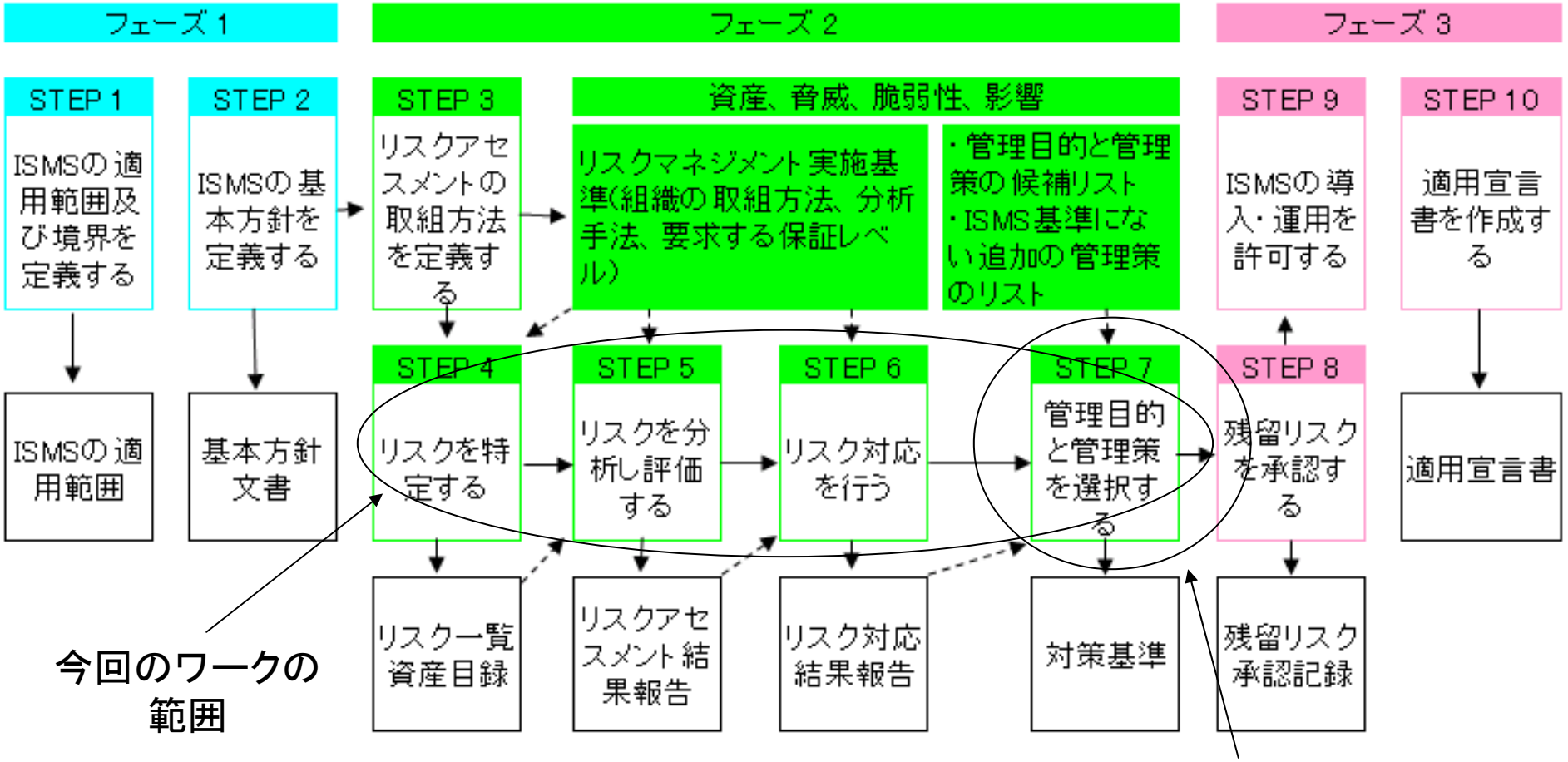
中小企業のリスク対策における制限

- 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。



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

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、その業務プロセスを構成する各業務に対するリスク分析・評価をおこなうアプローチ。

- 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。

各アプローチの特徴

- 業務からのアプローチ
  - それぞれの業務を行う、担当者で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んなに変わらない？
  - 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りがち？

- 資産管理台帳からのアプローチ
  - システム管理者、資産の管理者だけで洗い出しが可能。
    (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)
  - 資産名の名称が同じものであっても業種、企業、部署、個人により異なる。
  - 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。

業務からのアプローチを採用理由

- 中小企業では、リスク対策ができる程、十分に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、リスクと紐付け安く(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。
- 業務ごとにDSS化の検討も可能！

業務からのリスクの洗い出し方法

- WGメンバによるKJ法を利用した洗い出し
- ISMSの管理策を考慮しての補足
- さらに情報を保存、処理する場所よりリスクを洗い出し

	脆弱性に起因する要素（人が何処何処で何々する）																				
	業務（人が何々する）	情報を保存・処理する場所																			
		建物（入り口）	部屋・ゾーン他	キャビネット	PC	サーバ	ネットワーク	USB他（媒体）	表示モニタ	紙	プリンタ	FAX	コピー機	ゴミ箱	会話	電話	携帯電話	ホワイトボード	ファイル交換（外サ）	廃棄業（外サ）	宅配・郵送（外サ）
出社	入館	○																			
		○																			
	入室・セキュリティゾーンへのアクセス		○																		
			○																		
	PCの起動・ログイン				○																
					○																

洗い出し(作業中)

	性に起因する要素(人が何処何処で何々	
	業務(人が何々する)	(人が何処何処で何々するために発生する)リスク
社外	公共の乗り物での業務	近隣の乗客による盗み見
		近隣の乗客による盗聴
	顧客訪問	PCからログアウトせずに放置
		PCの机上放置
		顧客先で携帯電話にかかってくる他社の案件に関する会話を顧客に聞かれる
		顧客先に他社向け資料の置忘れ
		顧客先で携帯電話カメラで無断撮影をした
	顧客ネットワークへの接続	ウイルスを感染させるあるいはウイルスに感染する
	PCを持って出張	紛失・盗難
		破損
		公共のネットワークでの接続
	記録媒体を持って出張	紛失・盗難
		インタネット・カフェ等公共の場所での使用
	書類を持って出張	紛失・盗難
	記録媒体の授受	授受記録が無い
		媒体からのウイルス感染
		顧客に無断で情報の持ち帰り
	書類の授受	授受記録が無い
	公共の場所での電話使用	会話の盗聴(立ち聞き)
		携帯電話の紛失・盗難
	公共の場所での会話	会話の盗聴(立ち聞き)
	無線LANを利用しての業務	無線LANの傍受
	プレゼンテーション	誤ったオペレーションによる重要情報の表示
	社内ネットワークへの接続	接続認証が無い
		クライアント−接続ポイント間が暗号化されていない
	社用車の利用	車上荒しによる盗難
	接待	重要書類・媒体・PCの置き忘れ
		重要な情報をつい漏らす

洗い出し(作業中)

	業務
出社	入館
社内	入室・セキュリティゾーンへのアクセス
	PCの起動・ログイン
	PCを使用した業務
	メールの受信確認
	メールの送信(本文)
	メールの送信(添付)
	FAXの送信
	プリンター・コピー使用
	PCによる文書の閲覧
	PCによる文書の作成
	PCによる文書の保存
	PCによる文書の印刷
	共有サーバの利用
	書類の受け渡し・発送(見積書等)
	記録媒体の発送
	外部サービスを利用したデータ交換
	書類、記録媒体の保管
	書類、記録媒体の廃棄
	電話での会話
	WEBサイトへのアクセス
	インターネットで収集した情報の利用
	業務の委託
	離席
	社外者の来訪
	社内会議
	PC・媒体の廃棄・処分
	書類の保管・廃棄
社外	公共の乗り物での業務
	顧客訪問
	顧客ネットワークへの接続
	PCを持って出張
	記録媒体を持って出張
	書類を持って出張
	記録媒体の授受
	書類の授受
	公共の場所での電話使用
	公共の場所での会話
	無線LANを利用しての業務
	プレゼンテーション
	社内ネットワークへの接続
	社用車の利用
	接待
業務終了	業務終了
帰宅	USB(電子媒体)を持ち帰っての作業
	PCを持ち帰っての作業
	自家用車での帰宅
	自宅PCを使用した作業
	書類を持ち帰っての作業
	PC、媒体、書類の保存
人事管理	入社手続き
	人事異動
	退職手続き
	朝令・MTG
システム管理	システムの設定変更作業
	アプリケーション・サーバーの管理業務
	ネットワークの管理業務
	設備の管理業務
	レガシーシステムの管理
	障害管理
	WEBサイトにおける設定

業務ごとの対策例

業務: 公共の乗り物での業務
リスク: 新幹線の中での作業中、周りの乗客（ライバル企業の社員）から情報を覗き見られる、あるいは重要な会話を聞かれる
脅威: 周りの乗客他
脆弱性: 作業方法
情報資産: Note PC、携帯電話、重要な情報
対策例1: 社員教育
対策例2: 公共の場所での、重要な情報を使用した作業を禁止する
対策例3: 覗き見防止シート、声を落とした会話
対策の有効性: ？

業務・リスク洗い出し作業での課題

- どうしても保護に視点が行ってしまう！
- 中小企業のレベル感が分からない？
- 脅威が同じでも各企業によってリスクが変わるのでは？
- 企業の中の人事、経理などの職種による違いをどのように包括するか？
- 業種による違いをどのように包括するか？
- リスクの粒度をどの程度にするか？
- リスクの網羅性をどのようにするか？

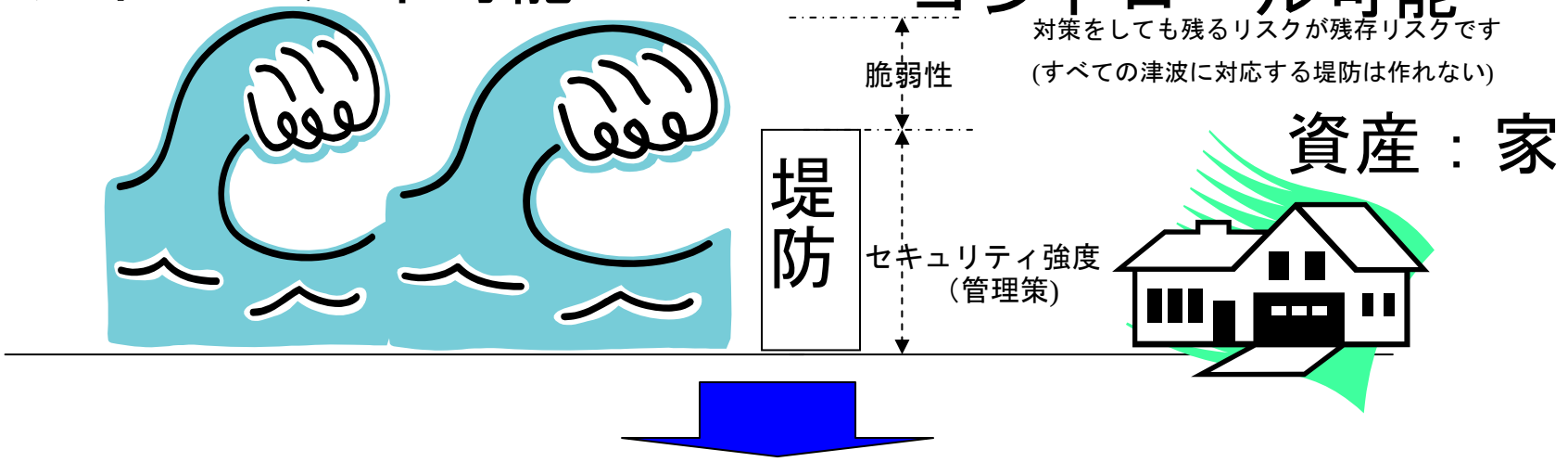
DSS化の課題ー対策の強度は？

脅威：津波の高さ

コントロール不可能

脆弱性：堤防の低さ

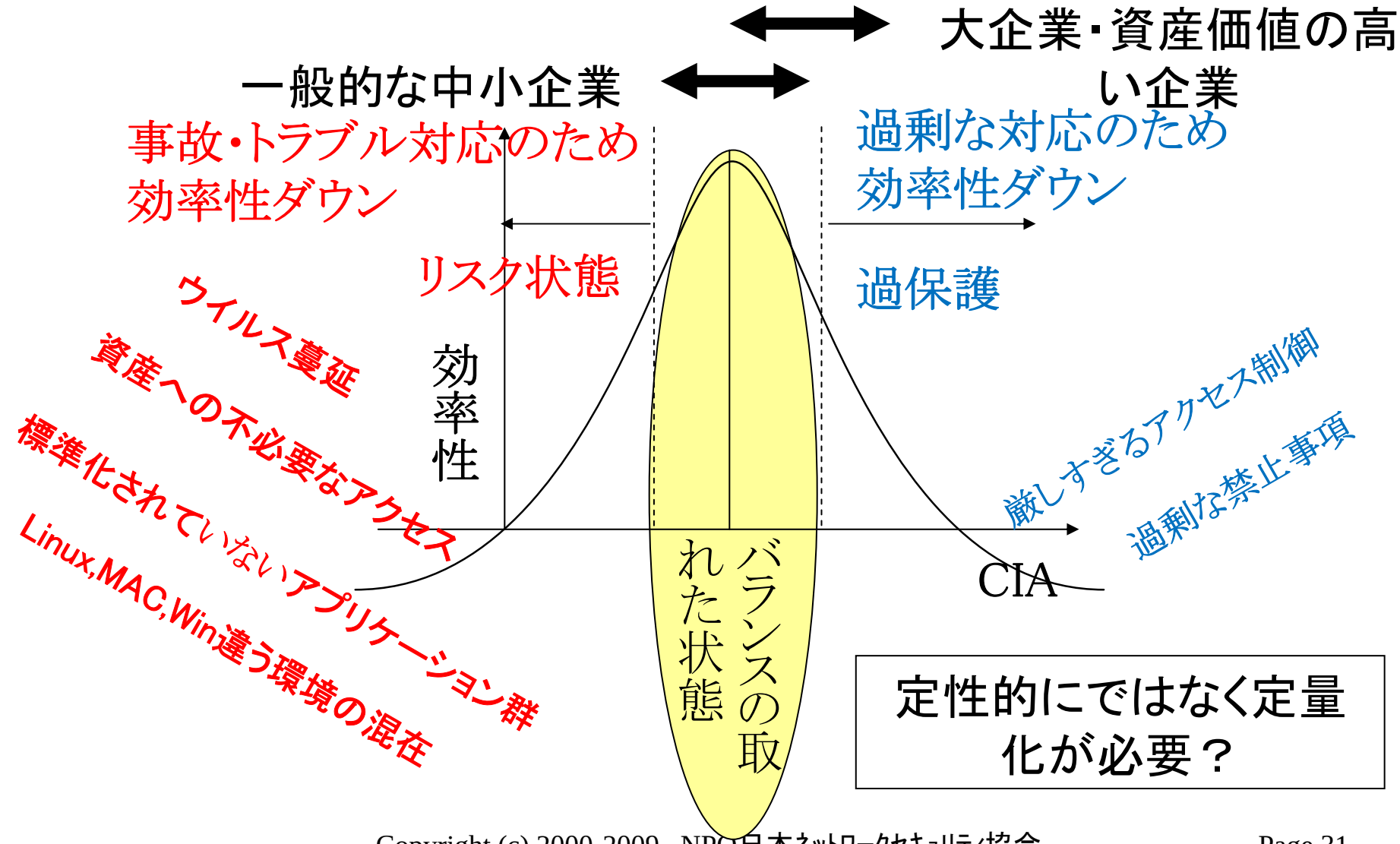
コントロール可能



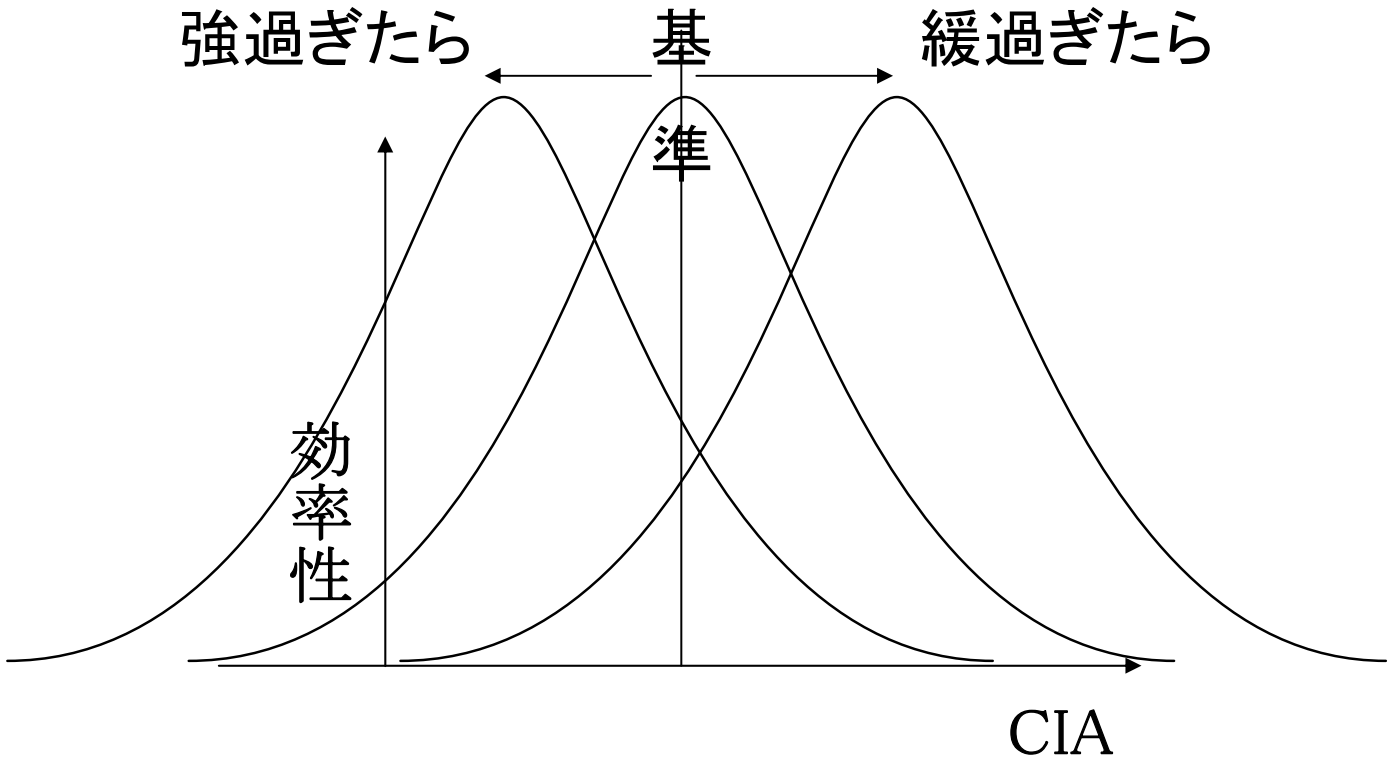
どんな規模・業種の企業でも脅威自体は変わらない

中小企業はリスクを自覚することが重要で、運用で逃げるしかない？

DSS化の課題―対策の強度は？



中小企業向けDSS化を検討！



定量化が難しいなら情報（Data）に対する何らかのセキュリティ(Security)に関する基準(Standard)を設けることは意味がある！

WGメンバ

50音順、敬称略

- 浅野　二郎
- 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
- 堀内 敦
  株式会社OSK
- 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。