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

元持哲郎
アイネット・システムズ株式会社
JNSA西日本支部

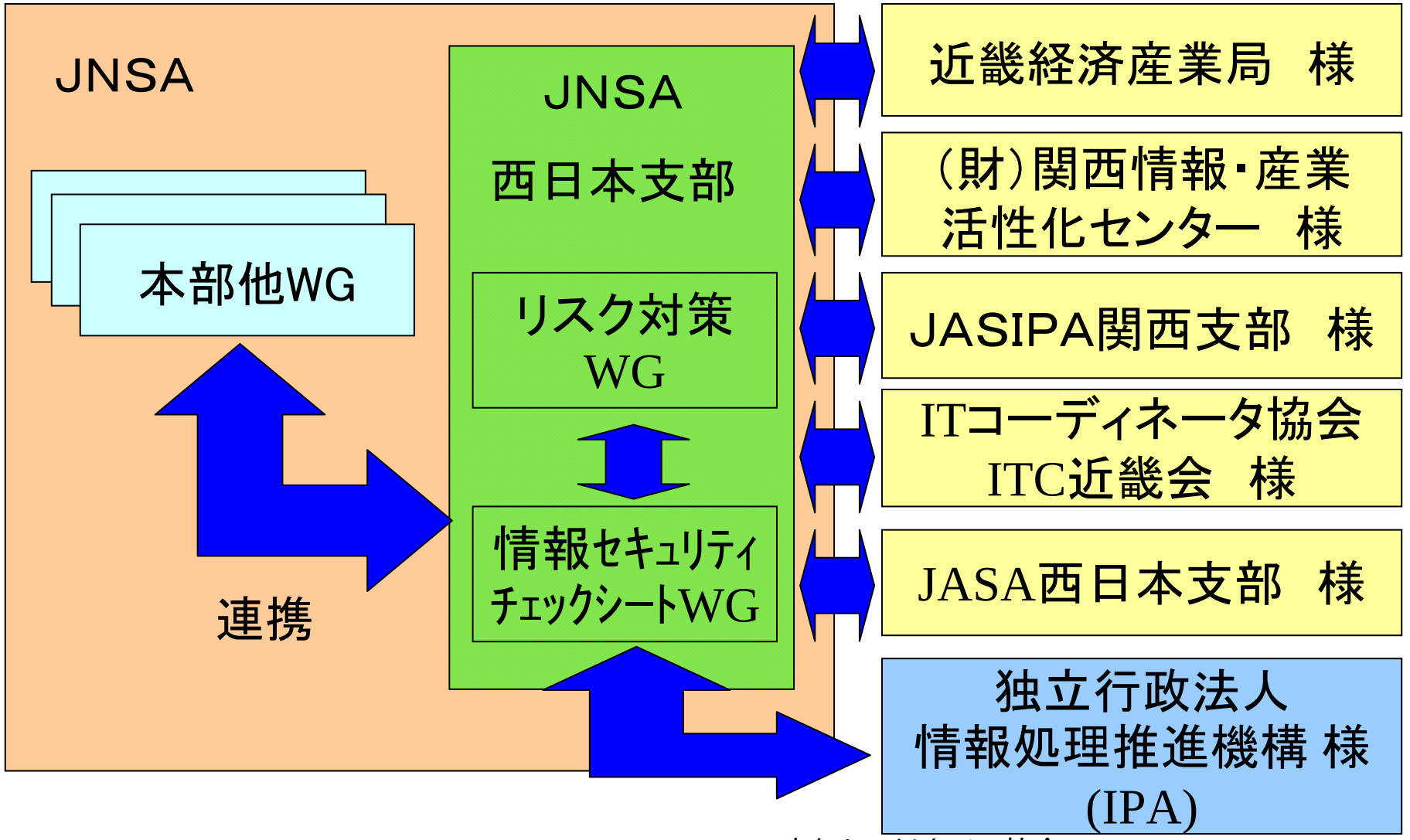
2010 年 1月27日

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											←	↔
リスク定量化方法等課題検討												
まとめ												

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	←	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	→

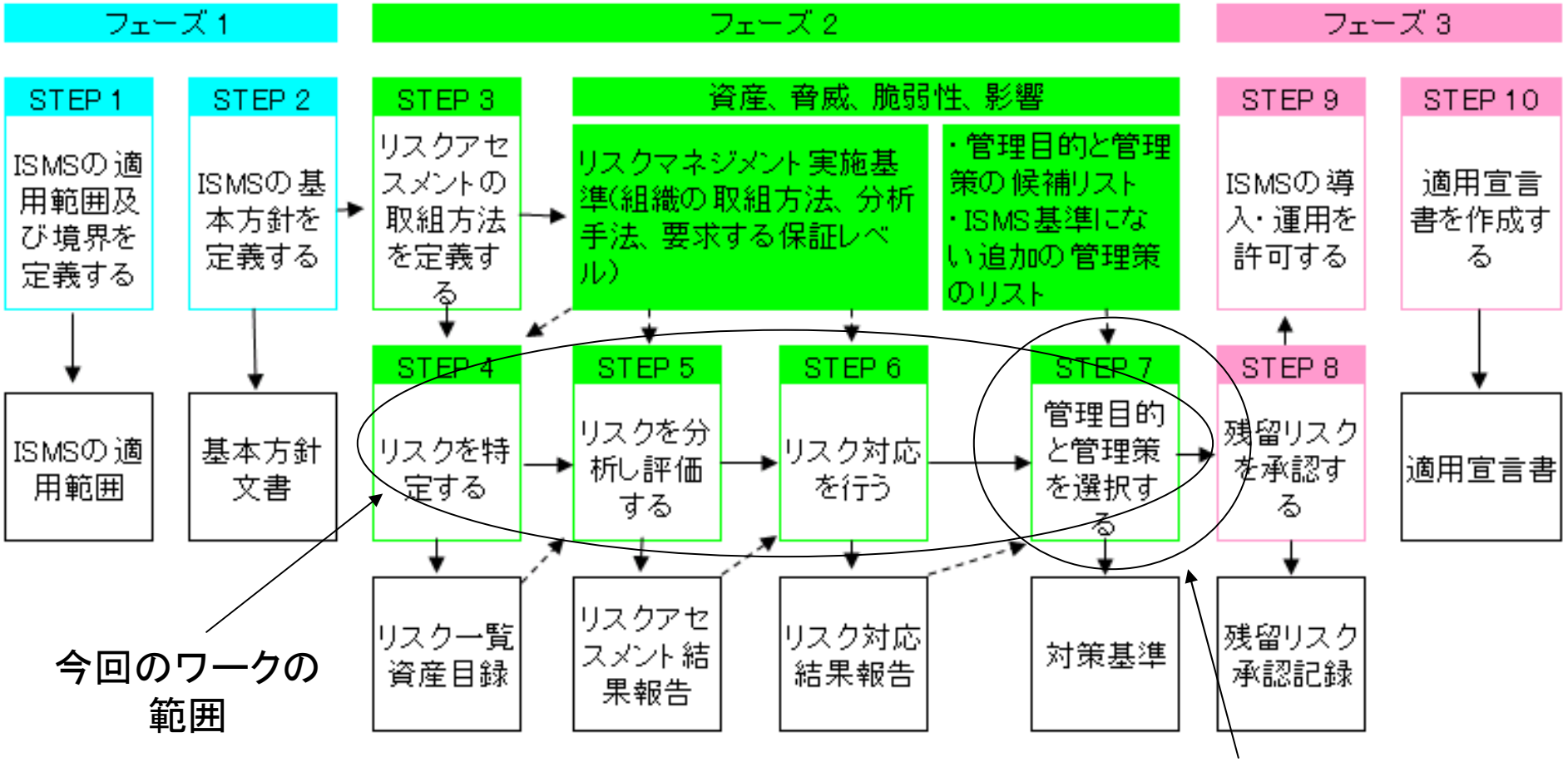
WGでの対象の中小企業

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

リスク対策はISMSをベース

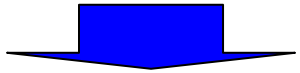


※JIPDEC ISMSユーザーズガイドより

情報セキュリティチェックシートの範囲

中小企業のリスク対策における制限

① トラブル経験がなく、自社は大丈夫と考えている。
② 情報セキュリティを理解できる人がいない。
③ 財政面、工数の制限
④ 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？

中小企業の制限を乗越えるために

① リスクが企業に存在することを理解させる

② セキュリティを理解させるのではなく原因-結果-対策の関係を理解させる

③ 人的より、技術的対策に比重を置く

④ SI‘er、ベンダーに丸投げし易いようにする

補足資料

- 日本、中国、インドでの人件費、PCの費用比較
  - 人件費（為替レート不明)

国名	都市名	平均月収（額面）	実質月収（手取り）
日本	東京	314,600円	240,000円
中国	北京	35,500円	30,000円
中国	上海	46,200円	40,000円
インド	ムンバイ	28,400円	25,000円

【プレジテント07年12月号より】

  - PCの購入費用

日本　　94,980円
中国　　103,802円(RMB7,599　1元=13.66円で計算)
インド　　97,524円(Ps.47900　1ルピー=2.036円で計算)
※インドのPCは性能的に若干劣る

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。

定量化-脆弱性、脅威、価値

LAWRENCE A. GORDON and MARTIN P. LOEB
"The Economics of Information Security Investment"
ACM Trans. on Information and System Security Vol. 5, No.4 pp. 438-457, Nov. 2002 より

1. The Expected Loss=vt λ =vL
2. EBIS(v)=[v-S(z,v)]L
3. ENBIS(v) =[v-S(z,v)]L-z

- v:脆弱性による脅威が成功する確率(0<v<1) 、t: 脅威の発生確率 (0<t<1)、λ :脅威が成功した場合の損失(資産価値?)
- L:損失の可能性(Loss or Potential Loss)
- EBIS(v):セキュリティ投資を行った場合の利益期待値
- ENBIS(v):セキュリティ投資を行った場合の正味の利益期待値
- v:脆弱性の確率(0<v<1)、z:セキュリティ投資額
- S(z,v):脆弱性vを持つ系にセキュリティ投資zを行った場合の脅威の成功確率（The Security Breach Probability Function）

定量化-最適投資

LAWRENCE A. GORDON and MARTIN P. LOEB
"The Economics of Information Security Investment"
ACM Trans. on Information and System Security Vol. 5, No.4 pp. 438-457, Nov. 2002 より

モデルⅠ. $S(z,v)=v/(\alpha z+1)^{\beta}$ ここで $\alpha>0, \beta \geqq 1$
モデルⅡ. $S(z,v)=v^{\alpha z+1}$ ここで $\alpha>0$
The Security Breach Probability Function S(z,v)が上の二つのモデルに属する場合、最適投資額 $Z^{*}(v)<(1/e)vL \fallingdotseq 37\%vL$

上のモデルは次の仮説(条件)を満たす。

- 仮説1. S(z,0)=0 脆弱性が0なら事故は発生しない。
- 仮説2. S(0,v)=v 投資をしなければ脆弱性を低減できない。
- 仮説3. 0<v<1の区間で $S_z(z,v)<0$かつ$S_{zz}(z,v)>0$
  ここで S_zはZに関する微分である。
  Lim S(z,v)→0 (z→∞) 無限の投資で脅威の成功確率を0に低減できる。

定量化-測定可能な例

- 地震の場合
  - 脅威
    - 大地震の発生頻度(確率)
    - 統計的に定量化可能
  - 脆弱性/強度
    - 鉄筋/木造、築年数、耐震・免震
    - 設計評価、耐震診断から定量化可能
  - 価値
    - 建物の資産価値
    - 定量化可能

※人的(住んでる人、住み方)なものから独立

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！

作業方針

- 動的なWEBサイト及びクレジット情報を扱うWEBサイトは対象外
- 機微・重要な個人情報は対象外
- 具体的な対策が無いものは削除する
  置き忘れ－＞暗号化　○
  置き忘れ－＞置き忘れないため注意　×
- 「悪意」「安易」など判断基準の無い言葉は極力使用しない
  「悪意」「安易」－＞ルール（具体的なルールは書かないが）外の
- 資産の持ち出し等禁止事項をできるだけ設けない
- 人的より技術的対策に比重を置く

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)	業務対象		情報を保存・処理する場所																							
		その業務をする人	業務を管理する人	建物（入り口）	部屋・ゾーン他	キャビネット	机上	PC	サーバ	ネットワーク	アプリケーション	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	ファイル交換等（外サ）	廃棄業（外サ）	委託業者（外サ）	宅配・郵送（外サ）
社外	公共の乗り物での業務	○						○					○														
		○																	○								
	取引先訪問	○						○					○														

リスクの洗い出し業務項目

	業務(人が何々する)
出社	入館
社内	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
	コピー機使用
	PCを使用した業務
	PCによる文書の保存
	PCによる文書の作成
	PCによるプリンタの使用
	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ファイル交換(宅ファイル便など)
	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
	社外者との打ち合わせ
	社内会議
	PC・媒体の廃棄・処分
社外	公共の乗り物での業務
	取引先訪問
	取引先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(NetCafeなど社外でのサービス利用)業務
	プレゼンテーション(取引先訪問に入れる)
	社内ネットワークへの接続
	社用車の利用
	社外の人間とのコミュニケーション
	接待
退館・退出	業務終了
	退館・退出
帰宅	業務用PCを持ち帰っての作業
	自宅PCを使用した作業
	社内LANへの接続
	PC、媒体、書類を持ち帰っての作業
	社用車・自家用車での帰宅
	PC、媒体、書類の保存
	家族とのコミュニケーション
人事管理	入社手続き
	人事評価・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(システムの定義、他の項
	サーバーの管理業務
	ネットワークの管理業務
	社内ネットワークへの接続(リモート接続)
	設備の管理業務
	レガシーシステム(アプリケーションが古いため最新のOSに対応できないシステム)の管理
	連絡体制
	WEB(ホームページを含む)サイトの設定

リスクの洗い出しシート の項目①

管理者観点か、
業務実行者観点か

	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)	業務対象		情報を保存・処理する場所																									
		その業務をする人	業務を管理する人	建物（入り口）	部屋・ゾーン他	キャビネット	机上	PC	サーバ	ネットワーク	アプリケーション	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	ファイル交換等（外サ）	廃棄業（外サ）	委託業者（外サ）	宅配・郵送（外サ）
社外	公共の乗り物での業務	○						○					○															
		○																	○									
	取引先訪問	○						○					○															
		○						○																				

リスクの洗い出しシート の項目②

適法性をCIAから独立（ライセンス違反などCIAに当てはまらない）

有形＝模型、サンプル品など無形＝狭義の情報

セキュリティ対策をしていない現状レベルを仮説

管理策を列挙

影響				情報の形状		現状のセキュリティレベル	対策の仕組み
機密性	完全性	可用性	適法性	有形	無形		
○					○	情報の内容を意識せず、PCを公共の乗り物で使っている	覗き見防止フィルタ（液晶フィルム）、公共の場所での重要な情報の利用を制限する、公共の乗り物ではPCを手元から放さない
○					○	~~会話における情報漏えいの危険性について周知していない~~	~~会話に際しての注意事項の明確化~~
○					○	取引先訪問時におけるPCの取り扱いを決めていない	パスワード付スクリーンセーバの自動起動設定、USBキー、離席時のログアウト若しくはコンピュータロックの徹底
○					○	取引先訪問時におけるPCの取り扱いを周知していない	PCの常時携行、ハードディスクの暗号化、BIOS認証の設定

リスクの洗い出しシート の項目③

中小企業でも行えれる管理策を記述

リスクが発生するシナリオ

対策	リスク事象(リスクシナリオ)
重要な情報は公共の場所では開かない	盗み見した近隣の乗客から重要な情報が漏洩する
~~機密情報に係る会話を控える 会話の内容を必要最小限にする 機密情報についてイニシャルトークなど文言を言い換える~~	~~会話を立ち聞した第三者から情報が漏洩する(IR情報→インサイダー、社内外の開発情報や戦略などの情報→メディアや競合先へのリーク等)~~
離席する際は、PCをログアウトする	離席した際に取引先に関係の無い情報を閲覧(PCを操作)される
関係者が不在となる場合は、PCを携行する	机上に放置することによりPCが盗まれる

リスクの洗い出しシート の項目④

セキュリティを理解しない、セキュリティ投資をしない経営者は脅威か？

経営陣、取締役ではなく、代表取締役社長を示し、情報セキュリティの全ての最終的な責任を持つ者

正社員、契約社員、パート、委託社員（委託業者はその会社で行っている業務とは別の業務として考える）全てを含める

脅威									責任		
経営者↑有り得ない？	システム管理者（本人）	システム管理者（本人外）	従業員（本人）	従業員（本人外）	委託業者	訪問者	外部	偶発的要因	経営者	システム管理者	従業員
							○				○
			○								○
							○				○
							○				○

リスク対策例

業務	公共の乗り物での業務
現状のセキュリティレベル	情報の内容を意識せず、PCを公共の乗り物で使っている
リスクシナリオ	盗み見した近隣の乗客から重要な情報が漏洩する
業務対象	その業務をする人
情報を保存・処理する場所	PC・表示モニタ
影響	機密性
情報の形状	無形
脅威	外部
責任	従業員
対策の仕組み	覗き見防止フィルタ(液晶フィルム)、公共の場所での重要な情報の利用を制限する、公共の乗り物ではPCを手元から放さない
対策	重要な情報は公共の場所では開かない

作業で議論された内容

- 経営者の意識改革をどうするか？
- 脅威が同じでも各企業によってリスクが変わるのでは？
- 業種による違いをどのように包括するか？
- 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？
- パスワードポリシー等具体例が必要
- 人のミスによるものをどうするか？
- 対策の出来ないものをどうするか？

具体例の必要な項目

- パスワードポリシー
- 暗号
- 業務委託契約
- 教育(ポカミス、ヒューマンエラー対策)

教育に含める項目

- 社内の人間とのコミュニケーション-間違った情報を伝達するリスク
- 公共の乗り物での業務-会話を立ち聞した第三者から情報が漏洩する
- 社外の人間とのコミュニケーション-不要な情報を知り得た人が、他の人に情報を伝播させてしまい、結果情報漏えいとなる
- 家族とのコミュニケーション-機密情報を喋ってしまう
- 家族とのコミュニケーション-間違った情報を伝達するリスク
- 朝令・MTG-秘密事項（部内秘・社内秘・社外秘・極秘）が開示（誤っても含む）

対策ができないため削除

- 記録媒体の発送-決済手順を無視した独断での発送による情報漏洩
- 電話での会話-機密情報開示基準の不徹底により機密情報が漏れる
- 業務の委託-ルールを逸脱した情報の持ち出しにより情報が第三者に漏れる
- 社内会議-関係者秘情報をつい漏らす
- 社内会議-重要情報の無作為配布
- ネットワークの管理業務-DoS攻撃を受けサービスが利用できなくなってしまう

DSS化の対象業務

- 事件時の被害が算出可能
- 守るべき情報資産が明確
- 業務の対価が明確
- 業務の自由度が少ない（マニュアル業務）
- 対策が比較的簡単かつ低コストで行え、効果が大きい

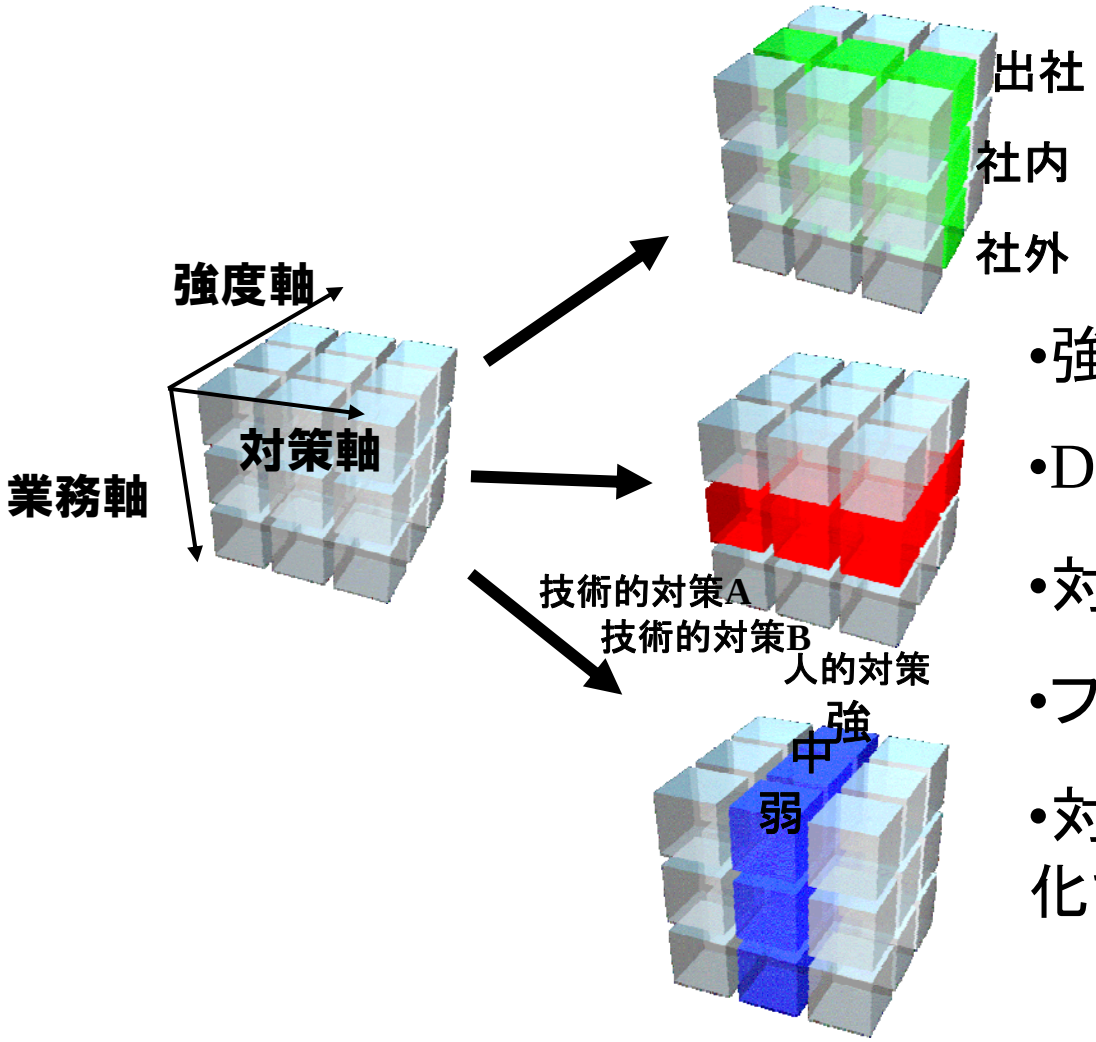
DSS化が理想？

- 個人情報の取り扱い
- 業務データをExcel マクロで処理
- 業務の委託

DSS化の検討

DSS化	企業分類	意識	対策の要請
PCIDSS、センシティブな個人情報DSSなど	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。
業務単位DSS（情報持ち出しDSSなど）	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。
基本DSS（認証、ウイルス対策等比較的簡単で効果が高いもの）	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。

DSS化の検討



- 強度（相対的）は？
- DSS化の業務の単位は？
- 対策の分け方は？
- フォーマット？
- 対象組織を明確にモデル化すべき？

今後の作業方針

- 全体としての整合性及び業務の整理
- 技術的対策、人的対策を分ける
- 対策の仕組みも、技術的、人的を分ける
- 対策のチェック方法を入れる
- 対策と対策の仕組みを分ける必要？
  - 進めながら検討する
- 対策できないものは教育、ルールで補完する
- 管理者の対策と、業務実行者の対策を作るべきか？
- 業務ごとにDSS化を目指す

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。