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

経営者向け 情報セキュリティ対策 実践手引き

西日本支部
富士通関西中部ネットテック㈱
嶋倉　文裕

支部のこれまで活動の関係

JNSA

気付き

- 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
- 略称：9to5
- URL:http://www.jnsa.org/result/2013/chusho_sec/index.html

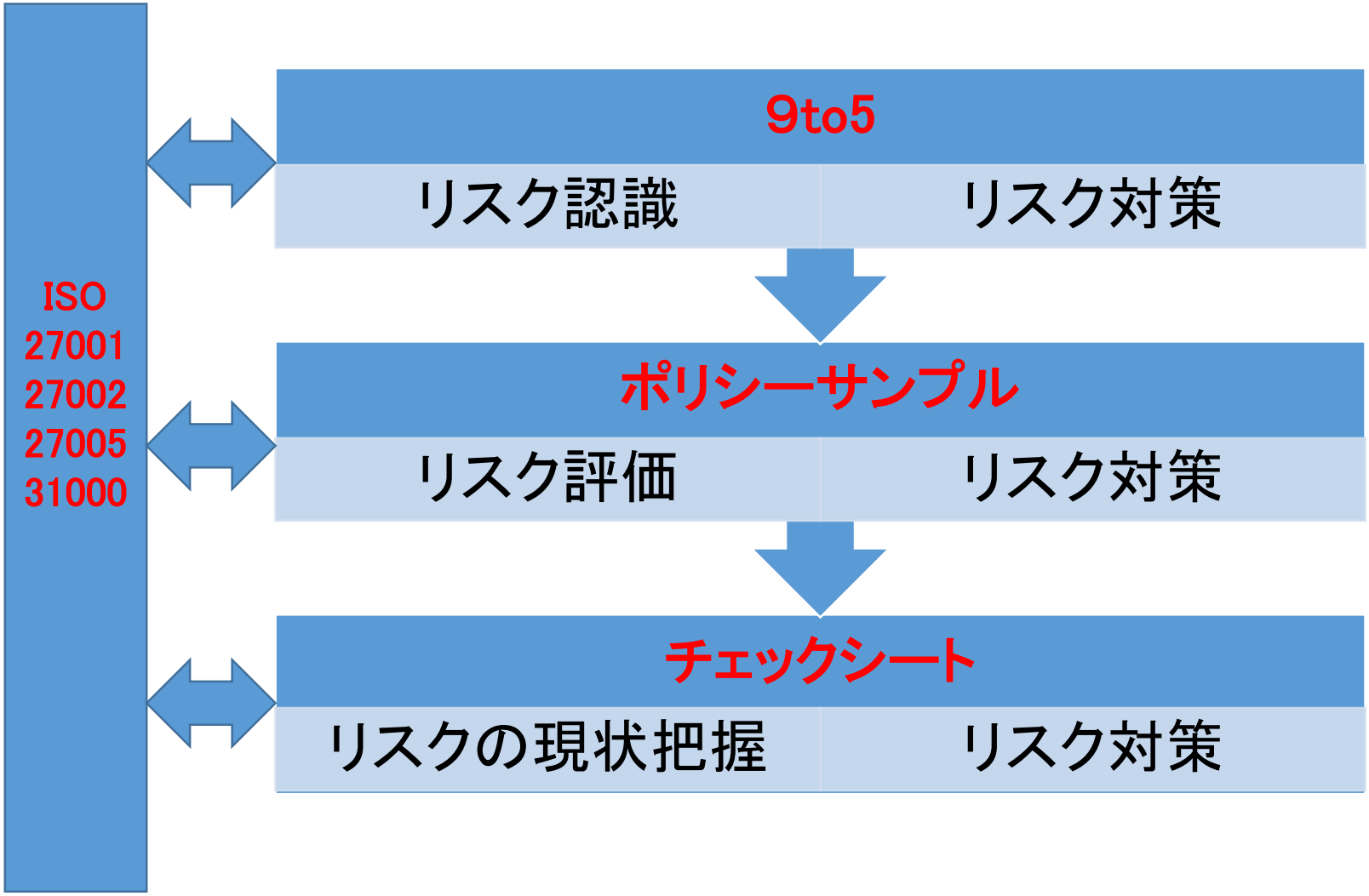
運用

- 中小企業向け情報セキュリティポリシー・サンプル
- 略称：ポリシーサンプル
- URL:http://www.jnsa.org/result/2016/policy/index.html

チェック

- 中小企業向け情報セキュリティチェックシート
- 略称：チェックシート
- URL:http://www.jnsa.org/seminar/nsf/2014kansai/

ISO規格を採用



経営者に訴求するには？

経営者に情報セキュリティ対策の必要性を訴求し、
対策に投資をしてもらうには？

リスク認識が重要

経営者にリスクを認識して頂くためには…

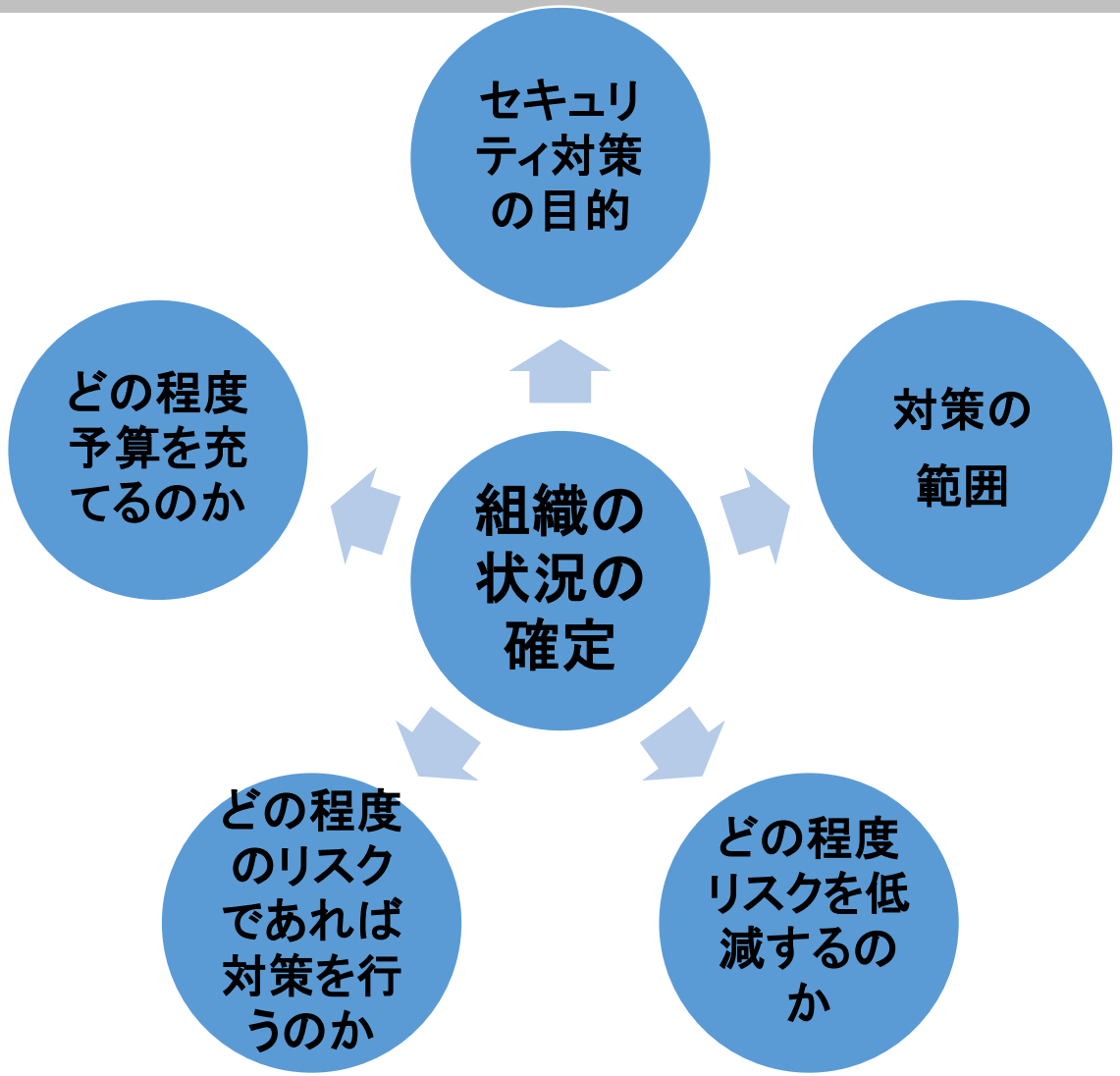
組織の状況から理解してもらうことが必要

組織の状況の確定

- ISO31000による外部状況と内部状況例

外部状況例	国際、国内、地方又は近隣地域を問わず、社会及び文化、政治、法律、規制、金融、技術、経済、自然並びに競争の環境
	組織の目的に影響を与える主要な原動力及び傾向
	外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観
内部状況例	統治、組織体制、役割及びアカウンタビリティ
	方針、目的及びこれらを達成するために策定された戦略
	資源及び知識として把握される能力（例えば、資本、時間、人員、プロセス、システム、技術）
	内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観
	組織の文化
	情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の両方を含む。）
	組織が採択した規格、指針及びモデル
	契約関係の形態及び範囲

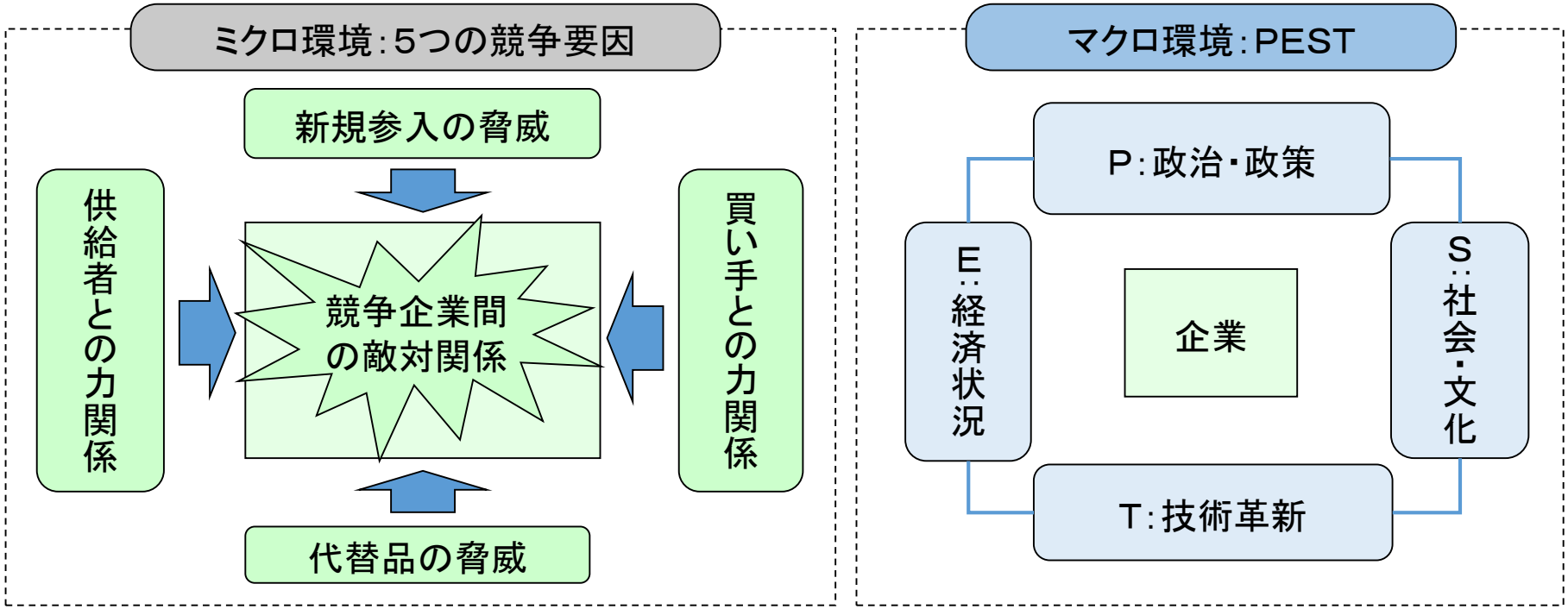
状況から導けること



外部環境分析手法

- ミクロ環境　　Five　Force
- マクロ環境　　PEST

こういうもので表現できないか



リスクの落とし込み　外部状況

ISO3100の項目

PESTやFiveForce視点の取込み

		分類	セキュリティとの関係	再分類	
外部状況	国際、国内、地方又は近隣地域を問わず、社会及び文化、政治、法律、規制金融、技術、経済、自然並びに競争の環境	政治	P:政策により、セキュリティ攻撃等セキュリティ脅威が増大	マクロ環境	要求要件
		経済	E:セキュリティ投資に影響		
		金融	セキュリティ投資に影響		
		社会及び文化	S:脅威、セキュリティ対策に影響（要リスク評価）		
		技術	T:脅威、セキュリティ対策に影響（要リスク評価）		
		法律/規制	脅威、セキュリティ対策に影響（要リスク評価）		
		自然	脅威、セキュリティ対策に影響（要リスク評価、事業継続）		
		競争環境	ミクロ環境:脅威、セキュリティ対策に影響（要リスク評価）	ミクロ環境	
	組織の目的に影響を与える主要な原動力及び傾向	N/A	組織の目的に影響を与えるセキュリティレベル （最低のセキュリティレベルより大） セキュリティ対策の目的、セキュリティ対策の範囲、セキュリティレベル	セキュリティ対策の目的 セキュリティ対策の範囲 セキュリティレベル	
	外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観	株主	業種により外部から要求されるセキュリティレベル （最低のセキュリティレベル） セキュリティレベル、範囲		
		顧客			
		取引先他			

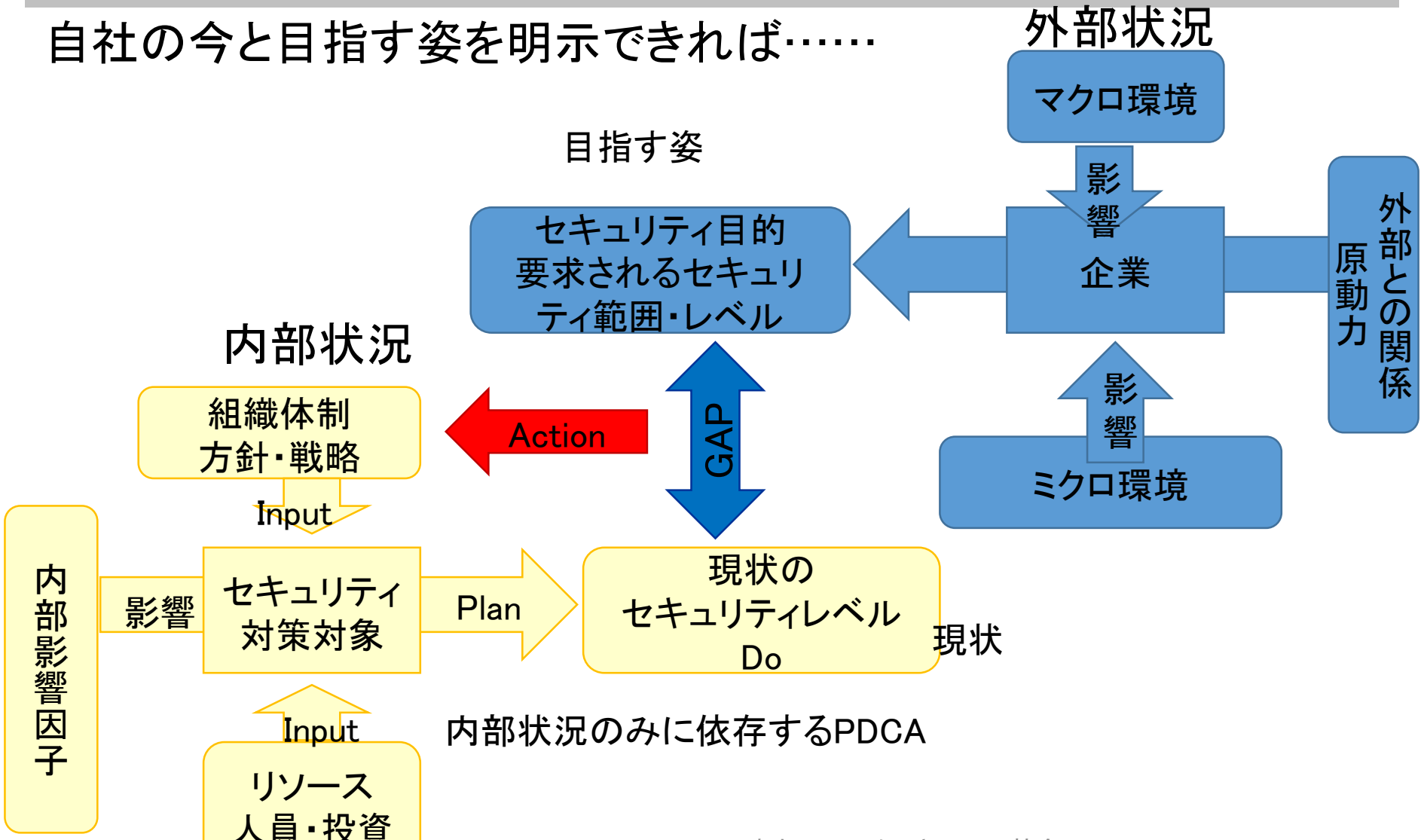
リスクの落とし込み　内部状況

ISO3100の項目

		分類	セキュリティとの関係	再分類	
内部状況	統治、組織体制、役割及びアカウンタビリティ	統治	脆弱性：組織的対策	組織体制・方針・戦略	現状
		体制			
		役割			
	方針、目的及びこれらを達成するために策定された戦略	経営方針	脆弱性：組織的対策		
		情報セキュリティポリシー群			
	資源及び知識として把握される能力（例えば、資本、時間、人員、プロセス、システム、技術）	資本	セキュリティ投資	リソース（人、金、プロセス）	
		人員/時間	リスク評価分析、セキュリティ対策・管理を行う人材		
		プロセス/システム	リスク評価分析、セキュリティ対策・管理方法		
		技術	リスク評価分析、セキュリティ対策・管理を行う技術力		
	内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観	経営者	脆弱性：組織的対策 ※内部組織の関係、認知及び価値観に基づき組織を構成する	内部影響因子	
		セキュリティ管理部門			
		情報システム部門			
		従業者			
	組織の文化	組織の行動原理 ※ITリテラシー	脆弱性：人的対策、技術的対策 ※組織の文化を考慮して人的対策、技術的対策を検討する		
		組織の思考様式 ※ITリテラシー			
	情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の両方を含む）	情報資産	脆弱性：組織的対策、人的対策、技術的対策、物理的対策	セキュリティ対策の対象＝現状のセキュリティレベル	
		情報処理			

外部状況と内部状況の関係整理

自社の今と目指す姿を明示できれば……



一般論の限界

一般論で整理するには限界

・企業によって影響する外部環境は異なる

・企業によって内部環境は異なる

異なるものをいきなり一般論化には無理が..

仮想のモデル企業を作成

それを元に組織の状況を確定し、経営への見せ方を考える

→　共通的な要素を引き出し一般化

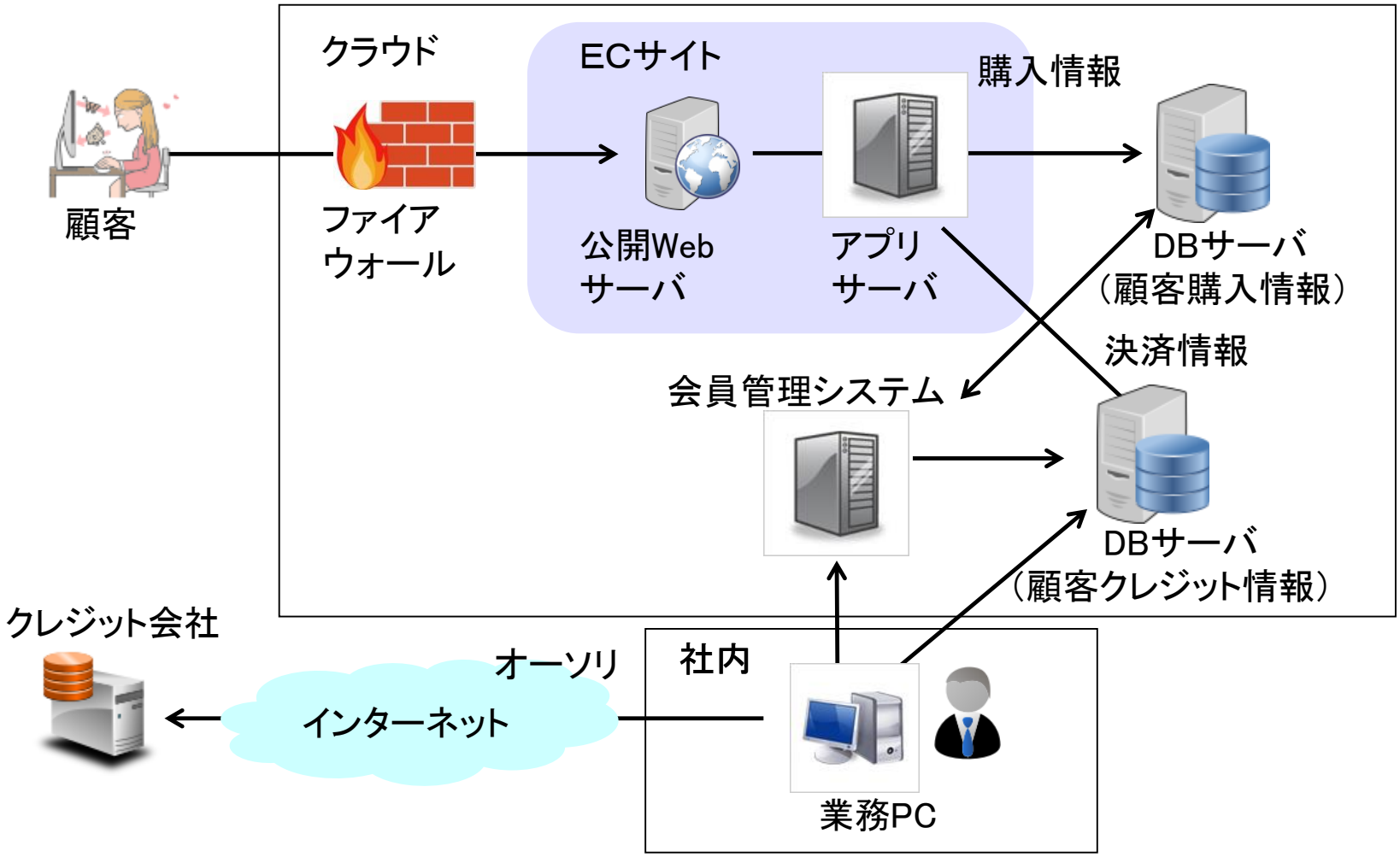
モデル企業　ECサイト

【会社のビジネス概要】
・健康食品の開発・製造、販売まで行う。
・店舗は持たず、Webでネット販売を行っている。

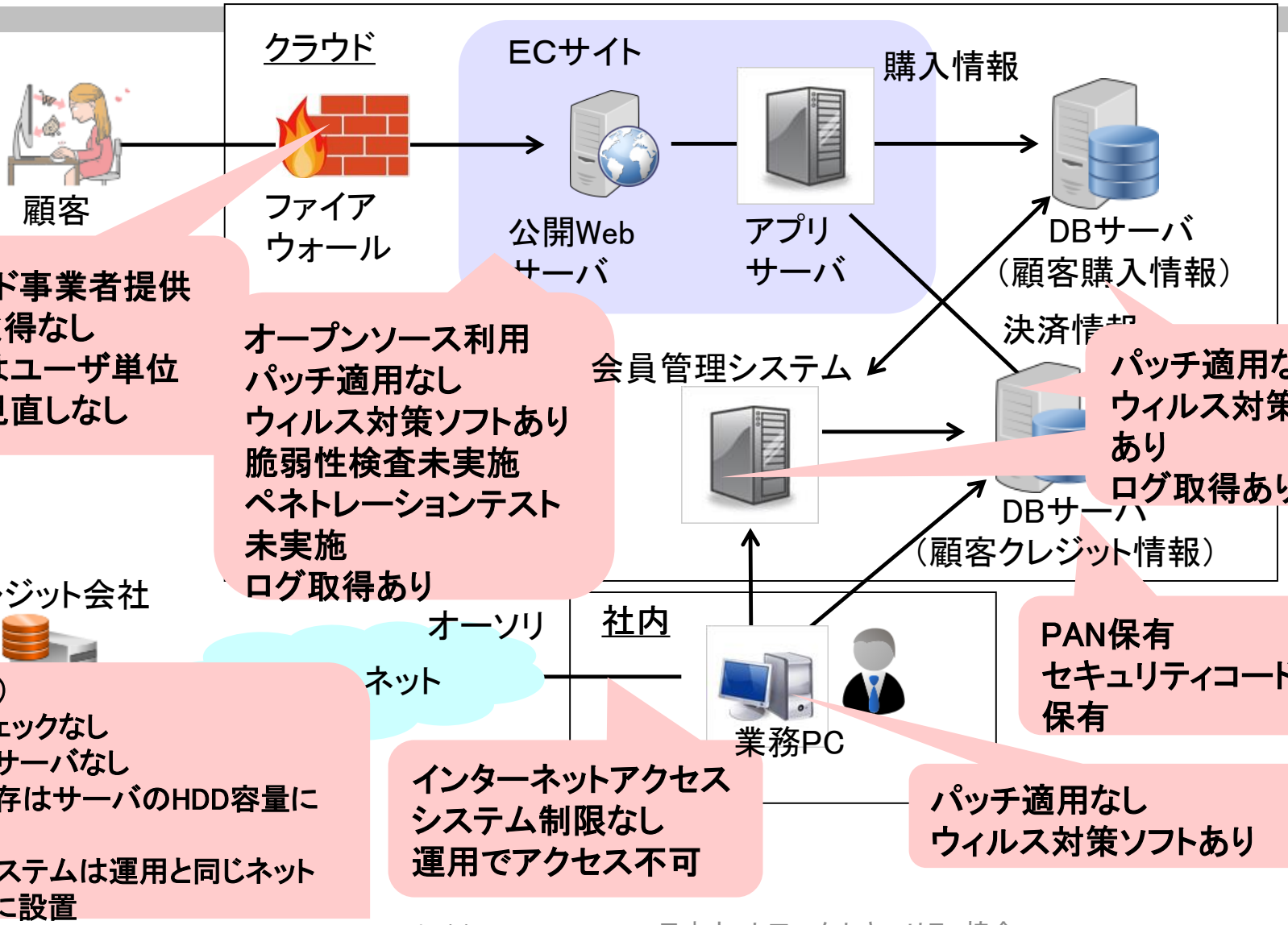
従業員	300名
売上	100億

企業IT活用方針	・IT活用に積極的でクラウド利用
情報セキュリティポリシー	・Pマークを取得しているが、PCIDSSには手が回っていない
体制	・情報システム部は存在する ・組織横通しの情報セキュリティ委員会、SOC、CERT機能はない ・個人情報管理委員会はある ・危機管理体制あり、製品問題、特許、従業員の就労問題、災害対策が主
役割	・CIO、CISOが不在、個人情報管理責任者は情報システム部長
経営者	・IT投資は行う ・情報セキュリティ対策の必要性は理解、現状および何から、どこまで着手すべきか把握できていない ・他社の対策状況を気にする
情報システム部門	・主業務はアプリ開発、それに伴うサーバ、DB構築も行うが、主に委託者が実施 ・担当社員は5名 ・ネットワーク技術者はいない（知識が少ない）

ECサイト　システム



ECサイト　特徴



ECサイト企業の外部状況

影響元	状況		セキュリティ目的・範囲・レベル
マクロ環境	社会・文化	・実店舗に出向かない買い物の要望の拡大 ・働き方の変化により時間を気にしない買物の要望の拡大	・顧客が安心して製品の購入が可能なWebサイトの提供 ・サイバー攻撃や内部犯行によるクレジット情報、個人情報の流出は顧客離れ、損害賠償や、Webサイトの停止につながり、売上/利益が減るため、Webサイト、DBの保護が最優先 ・クレジット情報漏洩リスクを軽減する非保持化などのPCIDSS準拠が必須
	政治	・キャッシュレスの推進	
	技術	・クラウド活用によるECサイト構築のハードル低下	
	法律・規制	・割賦販売法の改正（カード会社の加盟店での取り合扱い状況確認義務）	
ミクロ環境	競争環境	・店舗を必要としないため多くの同業他社の参入（製造とインターネット販売の一体化）	
	市場	・健康志向により地域に関係なく市場の拡大	
外部との関係	クレジット業界	・PCIDSS準拠への要求	
	顧客	・インターネットでのカード決済への不安 ・個人情報漏洩時は損害賠償訴訟	

ECサイト企業の内部状況

影響元	状況	
組織体制 方針・戦略	方針	・IT活用に積極的でクラウド利用
	情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ	・Pマークを取得
	体制	・情報システム部は存在する ・組織横通しの情報ｾｷｭﾘﾃｨ委員会はない ・SOC、CERT機能はない ・個人情報管理委員会はある ・危機管理体制あり、製品問題、特許、従業員の就労問題、災害対策が主
	役割	・CIO、CISOが不在、個人情報管理責任者は情報システム部長
内部影響 因子	経営者	・IT投資は行う ・情報ｾｷｭﾘﾃｨ対策の必要性は理解、現状および何から、どこまで着手すべきか把握できていない ・他社の対策状況を気にする
	情報ｼｽﾃﾑ部門	・主業務はアプリ開発、それに伴うサーバ、DB構築も行うが、主に委託者が実施 ・ﾈｯﾄﾜｰｸ技術者はいない（知識が少ない）
リソース	人員	・明確化な情報セキュリティ担当者はいない ・情報システム部門の人材のみではECサイトの構築、運用人員が不足するため、外部委託している
	技術	・リスク評価、必要な対策を決定、運用する技術力はない

当初考えた　AsIsと ToBe

AsIs

・ECサイトでクレジット決済を提供
・Pマークは取得済
・顧客が入力した**クレジット情報、セキュリティコードを保存**
・電話注文でもクレジット決済に対応
・保有する会員情報、クレジット情報へのアクセス、インターネット経由でクレジット会社へのオーソリのため接続は業務PCに限定、**該PCはオーソリ以外のインターネット接続はしないが、システム的な接続制限はなし**
・**脆弱性検査、ペネトレを実施したことはない**
・保有するサーバ、業務PCにパッチは適用しないが、ウィルス対策ソフトは導入
・**アクセスログは取得しているがチェックはしていない**

ToBe

顧客情報を安全に活用したビジネス
・顧客が安心して製品を購入するWebサイトの提供
・サイバー攻撃や内部犯行によるクレジット情報、個人情報の流出は顧客離れや、Webサイトの停止により売上が減るため、Webサイト、DBの保護が最優先
・クレジット情報漏洩リスクを軽減する**セキュリティコード以外のクレジット情報も非保持化**
・**定期的な脆弱性検査、ペネトレによる安全性の確認**
・**アクセス制限やパッチ適用による安全性の確保**
・改正割賦販売法の順守

Gap

・セキュリティコード以外も含むクレジット情報の安全な取扱いを行っていない
・安全性の確保、定期的な安全性の確認など、セキュリティ維持が行われていない

当初考えた　AsIsと ToBe

Gap

・セキュリティコード以外も含むクレジット情報の安全な取扱いを行っていない
・安全性の確保、定期的な安全性の確認など、セキュリティ維持が行われていない

Target

セキュリティコード以外も含むクレジット情報の安全な取扱いや、システムの安全性の確保、定期的な安全性の確認など、PCIDSSへの対応により、セキュリティを維持したWebサイトの提供と顧客に安心感を与え、ビジネスの拡大を目指す

①～③を1年で対応、④をその次年に対応

①保存非許可データの保持の停止、消去
②Webサイト、会員システム、DB、ネットワーク等、PCIDSSに準拠したシステム移行
③PCIDSSの推進、監視、事故時の体制、役割の構築
④PCIDSSに準拠する定期的な試験、見直しの実施

経営者がこれを見て、どう思うか。。。。
情報システム部は、あれもこれもやらないとあかん！
経営者は？？？

経営者が思うことは何か？

結局、放置しておくと、何がおきる？
それで、どうなる？

どうしたら良いの？
なんぼ、必要？

何が起こるのか

現状

・店舗を持たないECサイトでの販売による、店舗費や人件費を抑えたビジネスの展開
・顧客情報の流出のリスクが残る現在のECサイト、業務 システム
（業界標準を達成せず、改正割賦販売法に対応不十分）
・ECサイト、業務システムの維持、運用に対し脆弱な体制

目指す姿

顧客情報を安全に活用したビジネス、売上/ 利益の拡大
・店舗費や人件費を抑えたECサイト活用のビジネスの展開
・顧客が安心して製品を購入可能なECサイトの提供
・顧客情報を保護するECサイトや業務システムの維持（業界標準に準拠）
・改正割賦販売法の順守
・上記を支えるための社内、協力会社との体制の維持とその運用

差異

・業界標準、改正割賦販売法に対応不十分なECサイト、業務 システム
・ECサイト、業務 システムの維持、運用に支障をきたす脆弱な体制

起こりうる被害

顧客情報（個人情報、クレジット情報）の漏洩に伴う企業価値の毀損、機会損失による売上/利益の減少

損金の発生	顧客の損害賠償請求（裁判対応、損害賠償の支払い）、クレジット不正利用の補償 クレジット再発行費用の補償、臨時コールセンターの設置　など 裁判費用 aaaa万円　　損害賠償 bbb円/人　会員数 ccc万人　max dddd万円　他 eee万円
売上/利益の減少	信頼喪失による顧客離れ、購入の減少、ECサイト停止（営業停止）により機会損失

改善の目的は

企業価値毀損、機会損失を招かないECサイト、業務 システムと運用体制強化

現状売上　mmm万/年　　現状利益　nnn万/年
改修費用回収予想　q年後
増加ランニング費用　ooo万/年
現状利益確保に必要な売上　　ppp万/年(+rrr%増)

改善策

ECサイト、業務システムの安全性の確保
①～②を1年で対応、③をその次年に対応

① 業界標準、改正割賦販売法への初期対応　　<今年度　xxx万の改修 >
② 業界標準、改正割賦販売法への完全移行　　<今年度　yyy万の改修 >
③ 安全性の定期的な確認、見直しの実施　　<来年度以降　zzz万/年>
①、②に伴う保守費、委託費　　<来年度以降　sss万/年>

通常時と事故などの異常時における、自社と協力会社との役割分担の見直し、責任の明確化、及び自社ビジネスを支えるECサイト、業務システムの運用体制の再構築

① 業界標準、改正割賦販売対応、事故発生時における社内、協力会社の役割の見直し
　<今年度　aaa万で検討>
② 社内、協力会社の推進体制の構築・運用
　<今年度　bbb万、来年度以降 ccc万/年>

情シスが欲しいもの

ECサイト、業務システムの安全性の確保

具体策

ECサイト、業務システムについては、セキュリティコード以外も含むクレジット情報の安全な取扱いやシステムの安全性の確保、定期的な安全性の確認など、PCIDSSに対応する。

①～②を1年で対応、③をその次年に対応

① 保存非許可データの保持の停止、消去
クレジット情報の非通過化（非保持）

② Webサイト、会員システム、DB、ネットワーク等、PCIDSSに準拠したシステム移行
開発システムと運用システムの分離
ログ管理システムの構築
WAFの導入　など

③ PCIDSSに準拠する定期的な試験、見直しの実施
脆弱性検査の実施(1Q単位、4回/年)
ペネトレーションテストの実施(1回/年)
脆弱性の把握、評価とパッチ適用
ログの確認　など

今後の予定

JNSA

今年度の作業予定

1. 仮想モデル企業を作成中
   ものづくり、そして運ぶ、売る　企業
   - 製造業（BtoB）
   - 物流
   - 流通業
     ＋メンバーの得意業種（医療）

2. 作成した仮想モデル企業から再整理
   - まとめ

ご清聴
ありがとうございました