ITセキュリティ推進から始める ITガバナンス

株式会社エクサ
コンサルティング推進部
中村一成
2013年7月10日

自己紹介

- 専門は情報セキュリティ・ITセキュリティ全般コンサル
  - 現状調査・分析、改善支援・指導、全体推進PDCA、各種ポリシー・推進文書整備など
- 主な経歴
  - グローバル企業の情報セキュリティ・ITセキュリティに関するマネジメントシステムの全体整備・推進
  - 重要業務・システムに対するリスクアセスメントと改善支援
  - システム監査の枠組み構築および試行
  - 製品セキュリティ・製造ラインセキュリティの枠組み整備
  - システムセキュリティ実装に関する要件定義・標準化
  - Webセキュリティの維持・改善の枠組み整備
  - ソーシャルメディアガイドラインの検討と策定
  - ITセキュリティ管理に関する監査対応システム導入支援

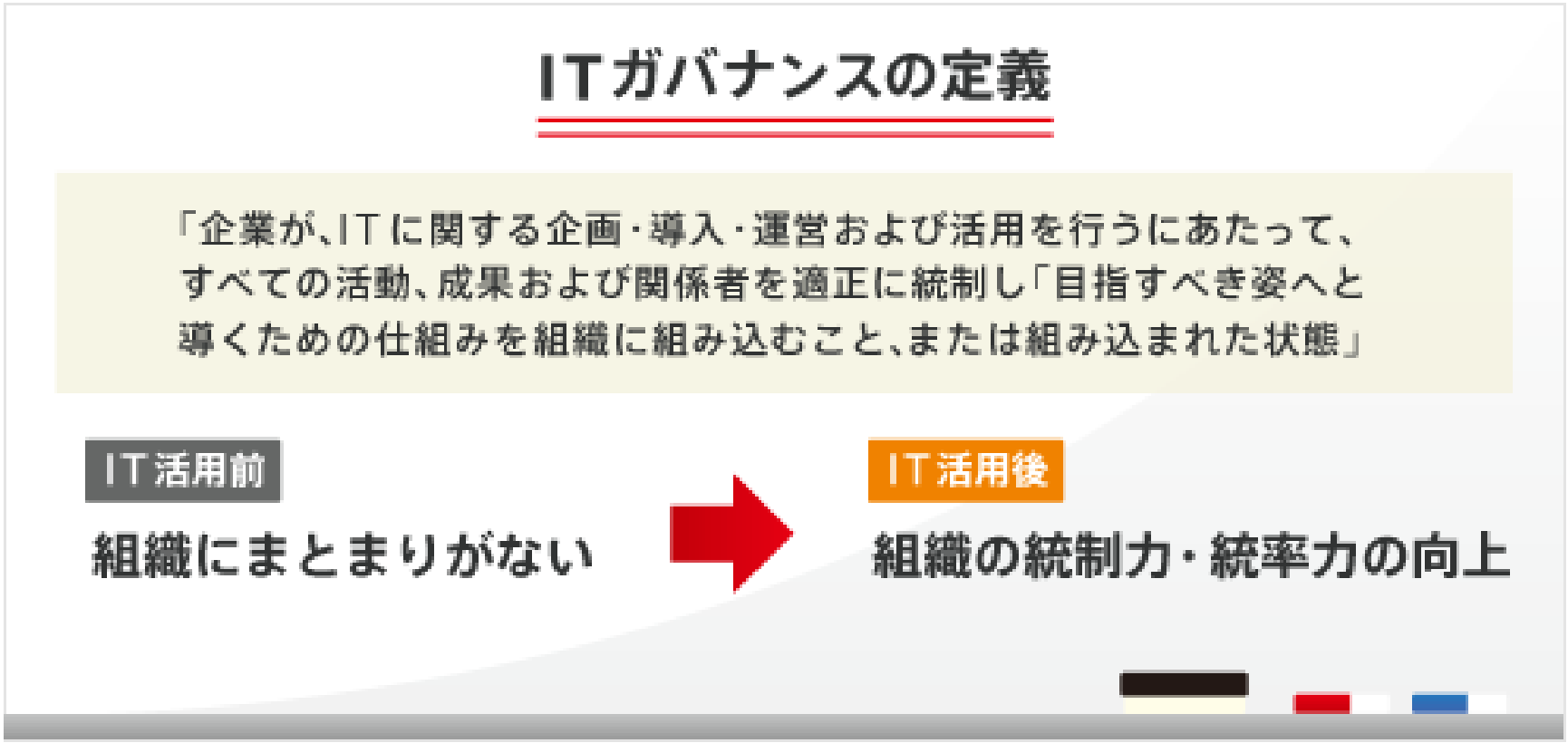
講演の概要

- 様々な情報システムでセキュリティ事故や問題が続出
- いつまで経っても改善が終わらない・進まない
  - どこから改善して良いのかわからない
  - 幾つかを改善しても、別のシステムや別の問題が出てくる
  - 改善が進まない・遅すぎる
  - 手間やコストがかかり過ぎる・予算が付かない

- ではどのように進めるのが良いのか？
- より踏み込んで、組織全体としてITをよりよく管理し、ITガバナンスを確立するにはどうしたら良いのか？

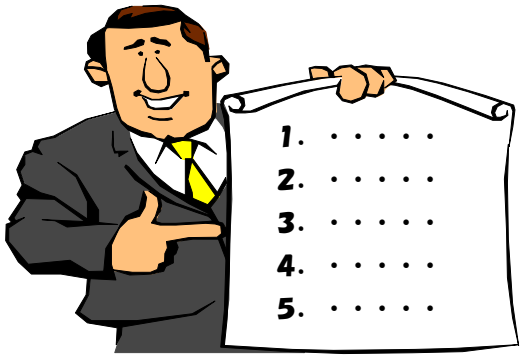
以上について、コンサルで得られた知見を纏めました

- **経済産業省 IT経営ポータルより**



http://www.meti.go.jp/policy/it_policy/it_keiei/action/keyword/governance/

情報セキュリティから
ITセキュリティへの流れ



一般的なITセキュリティ事故・事件とは

- ITセキュリティ事故は情報機器や情報システムが関係するもの
- 例えば
  - メモリーカード等記憶媒体の紛失
  - ノートPCの紛失や、デスクトップPCの盗難
  - ウィルス感染によるPCの利用不能
  - マルウェアによる情報漏洩、踏み台化による外部への攻撃
  - Webサイトの改ざん

  - 不正アクセスでの権限外システム操作・情報閲覧
  - 悪意の者によるシステムからの情報漏洩・改ざん・破壊
  - 設定不備・誤操作による情報漏洩・改ざん・破壊

- これらはITでの対策だけでは改善しない
- 人や物の管理など業務全体を含めた改善が必要

- ITだけではなく情報セキュリティ全般の推進活動へ

まずは情報セキュリティ推進から

- 情報漏洩事故・事件の多発により、組織的な情報セキュリティへの取り組みが始まる
- 法令面では不正競争防止法が拠り所
  - 悪意の者への責任追及が可能になった（刑事・民事）
  - 情報保有者・取扱者にも管理責任が負わされた

- 情報セキュリティ規格のISO27000に基づいて推進
  - Information Security Management System （ISMS）
  - ISO27000は管理項目・枠組みを示しているに過ぎない
  - 個別の管理策・レベルは組織事情を反映した設定が必要
- 個人情報保護やPCIDSSなどはISO27000が整備済みの前提

- 情報セキュリティ推進の中にITセキュリティ推進を含める
  - 情報の扱いは紙でも電子データでも基本は同じ

ISO 27000の構造

- ISO 27000は、情報セキュリティのマネジメントシステムと管理策の集合体（ベストプラクティス）
  - 11領域に区分された133個の管理策（コントロール）
- ITに関する項目も多い
  - A.10～A.12の他、一般論としてITに関係する項目も多い
  - 綺麗に分離されていない

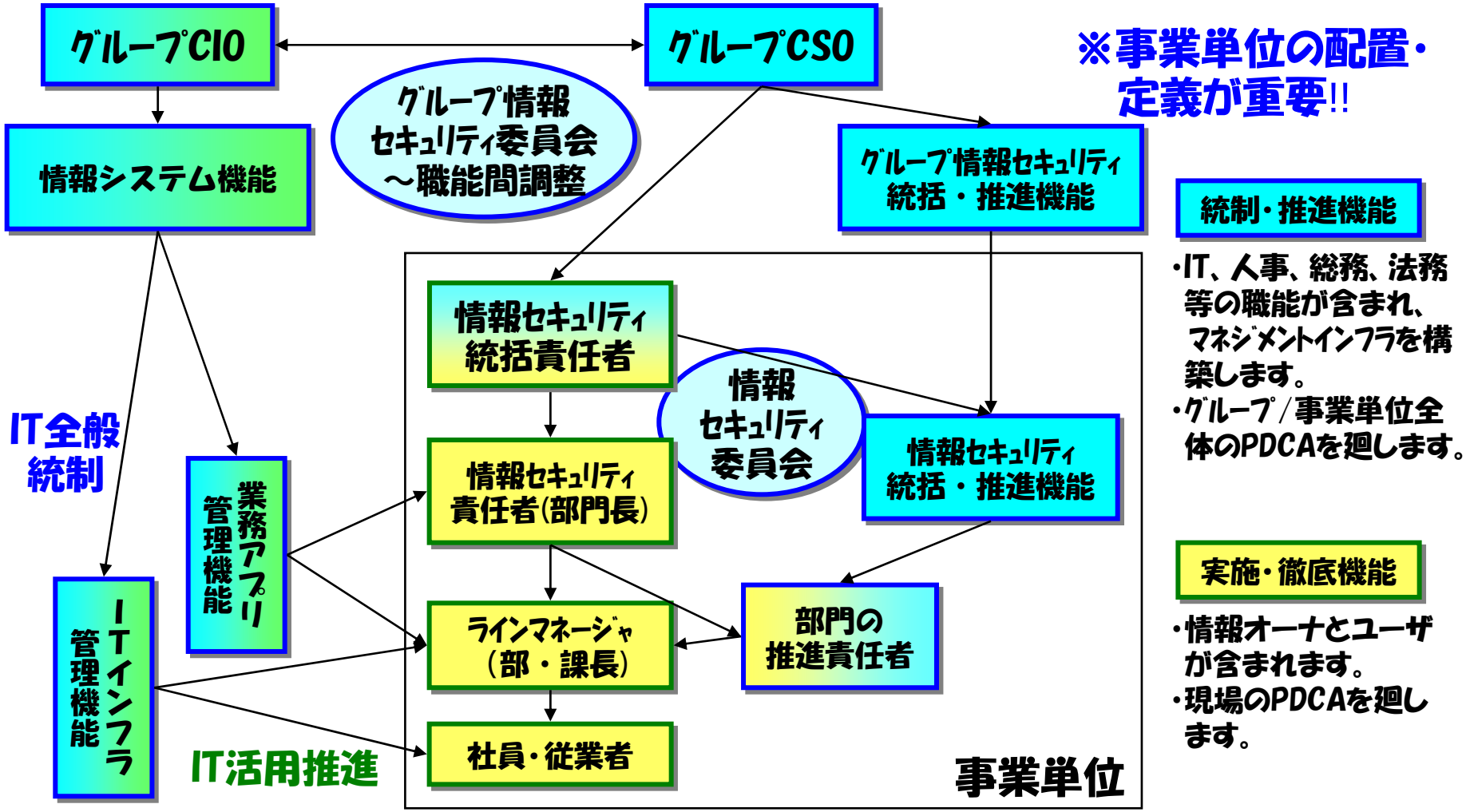
- **全社推進体制**
  - 全体推進の事務局は総務・法務・CSR等の部門が担当することが多い
  - 推進メンバーには本社部門・主要事業部門のセキュリティ担当の他、IT部門が加わる

IT部門主体では進まないことが多い

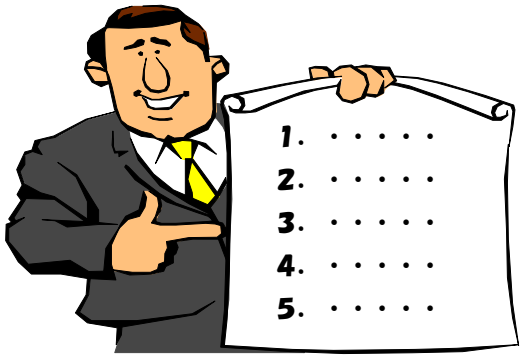
- **活動開始初期のテーマ**
  - 現状把握
    - どのような重要な情報（紙、データ）があり、どのように取り扱われているか
    - 早期に改善しなければならない重大リスクは何か
  - 社内規定・実施文書の整備
    - セキュリティ推進活動の裏付けとなるセキュリティポリシー
    - 情報洗い出しのための調査票・台帳
    - 改善のためのガイド文書、安全な情報取扱のための手順書等
  - 社内情報伝達系統の整備
    - 部門・支社・支店・工場等へのセキュリティ推進担当者設置
    - 担当者への教育

IT関係の推進は負荷の面で後回しも多い

- 情報セキュリティの管理構造は、統制・推進機能（職能系）と実施・徹底機能（ビジネスライン）の配置が重要

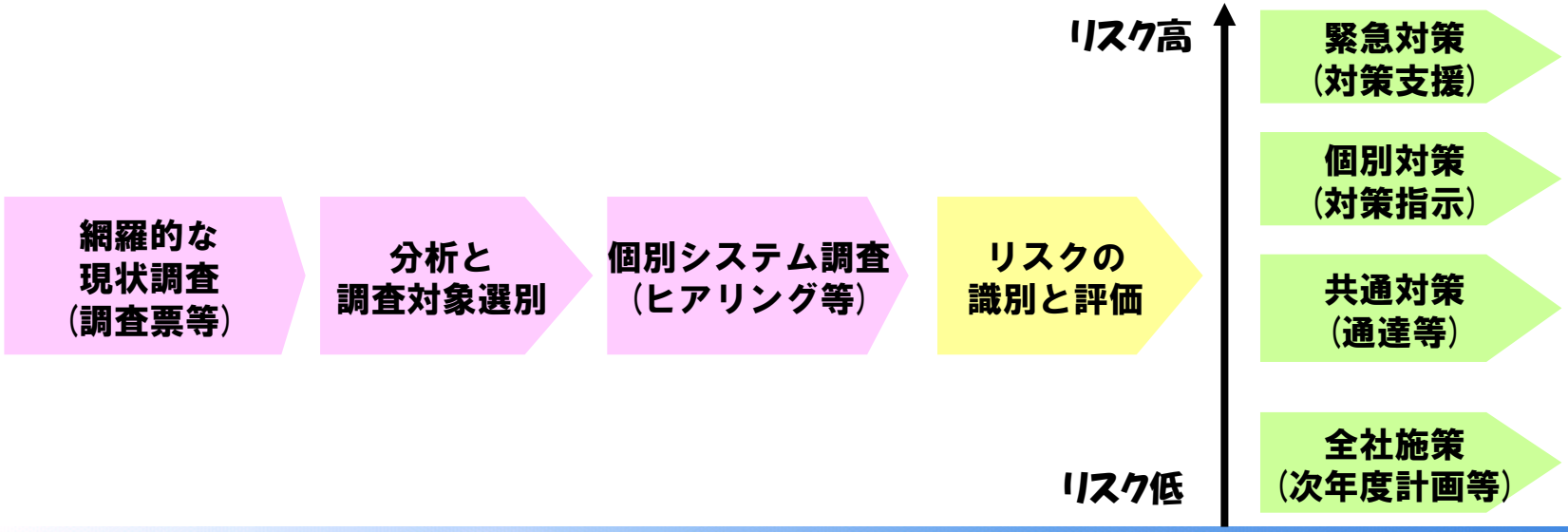


ITセキュリティ推進
～リスクの識別から改善へ～



組織内ITセキュリティリスクの識別と評価

- ITセキュリティ推進は個別対策から始めると失敗する
  - AシステムとBシステムどちらの対策を優先すべきなのか？
  - セキュリティ対策aとbどちらが効果が高いのか？費用対効果は??
  - 他のシステムは大丈夫なのか？
  - システム外の外に出してしまったデータの扱いは大丈夫なのか?
  - など、発散してしまい方向性を失ってしまうことが多い
- 組織内のリスクを網羅的に洗い出し、高リスクから対応が基本
  - 網羅的なリスクの把握の後に、組織の事情や現状を反映しリスク評価基準を定める



リスクの識別と評価：現状調査

- 部門別の現状把握では「情報資産」の棚卸から
  - 「情報資産」とは情報が紙文書、電子データ、機械・物品等（化体物）の形態になったもの
- 「IT資産」も棚卸
  - 上記の電子データに加え、これを保管・処理する物
  - 保管する物
    - メモリーカード・DVD・磁気テープ等の電子媒体
    - ファイルサーバーのフォルダー
    - データベース
  - 処理する物
    - サーバー本体、ソフトウェア
    - 外部サービス（通信回線、ASP・SaaS・クラウド等）

ITでも
見えるものを
優先

- 全社状況を広く・浅く・早く把握するため、調査票の配布・回収で行う
  - 取扱状況は可能な範囲で把握
  - 情報資産棚卸の他、物理管理（入退室管理・文書施錠保管など）や人的管理（教育実施、誓約書取得等）
- IT資産はIT部門管轄のシステムか否かを問わず、出来るだけ広い範囲で
  - 回答者はITに詳しくない前提で、調査項目を設定する
  - サーバーの有無、外部サービスの利用程度
  - 最低限、ヒアリング調査を行うためのシステム管理担当者が判れば良い

リスクの識別と評価：個別調査対象の選別

- 調査結果から高リスクの可能性があるシステムをピックアップ
  - インターネット系システム
    - Web、ソーシャルメディア
  - 機密情報取扱システム
    - 新製品企画、販売戦略・計画
    - 技術開発情報、設計図面、組みたて手順書、品質管理基準
    - システム設計書・プログラムソースコード、暗号鍵
  - 個人情報取扱システム
    - 会員情報取扱、通信販売実施等
    - コールセンター対応記録
  - J-SOX関連システム
    - 経理情報・財務情報を扱うもの
    - 適時開示リスクがあるもの（プレスリリースの発表等）
- さらに管理状況が危うそうなものを個別調査対象に
  - 本社IT部門管理下ではない
  - 特に担当者が一人でメンテナンスしているようなものは危ない

- 個別調査はシステム管理担当者へのヒアリングで行うことが多い
  - インターネット系システムでは脆弱性検査を併用する場合も

リスクの識別と評価: 詳細調査

- 詳細調査はヒアリングが中心
  - 情報セキュリティ推進の一環で行うことが多い
  - リスクはシステム本体だけではなく業務面にもあり分け隔てなく調査
  - 業務面では重要な情報資産と、それにかかわる業務や人の種別
    - 顧客からの預かり情報、契約書等
    - 社員、派遣社員、業務委託先がどのような業務に関わっているか
  - 執務環境調査
    - 入退室管理、開錠・施錠管理、来訪者の扱い
    - 媒体保管用の引き出し・ロッカーの設置場所・施錠状況
    - 休日・深夜作業の有無なども聴く

- ITに関する質問項目の例
  - システムの主管部門、実務担当者
  - システムの用途と利用状況
    - ユーザー数、ユーザー種別（正社員、派遣社員、パートナーなど）
  - 主な取り扱い情報とそれにかかわる業務フロー
  - システムの設置場所
  - システム構成
    - ハード、OS、ミドルウェア、ネットワーク環境等
  - システムの管理状況
    - 体制、ID改廃、パスワード変更、パッチ適用、バックアップ等
    - 未実施、不明が多い前提で、細かく聞きすぎない

リスクの識別と評価: 発見されがちなリスク-1

- セキュリティ事故には至っていないが事故発生が懸念されるリスクが多い

- パスワード管理がずさん
  - 初期パスワードがIDと同じで、変更せずに放置
  - 定期的な変更を掛けていない
  - ゲストアクセス可のところに重要な情報を置いている
- ID改廃が出来ていない
  - 日常的に共通IDを利用
  - 離任者のIDが存在
  - これらIDのパスワードは全く変更されていない
  - 棚卸できていないので、上記状況もつかめていない
- 脆弱性のあるバージョンを放置
  - パッチや新バージョンが出ているにも関わらず未適用
  - 既にサポートが切れているソフトを活用
- 事業継続性・サービス継続性に難あり
  - ハードウェア保守契約が切れている、メーカーが保守を打ち切っている
  - データのバックアップが採られていない、あっても回復手順が無い
- システム上の情報資産が不明
  - 当初意図していなかった機密情報や個人情報が置かれている
  - その可能性が高いが、ファイル数が多く棚卸が困難

リスクの識別と評価: 発見されがちなリスク-2

- 部門管理のシステム
  - 研究開発部門に置かれたファイルサーバーに図面やソースコード
  - ファイルサーバー上での顧客情報(個人情報)のやりとり
  - レンタルWebサーバー上での個人情報の収集・蓄積
    - 業務全体を外部委託しており、IT資産を所有しているという意識が無い場合も
  - 製造設備を制御しているWindows/Linuxサーバー
    - セキュリティパッチが適用不能
- ユーザー部門のITに詳しい人が属人的に管理していることも多い

- 外部サービス(特にクラウドサービス)
  - ファイル転送・同期サービス
  - 電子メール・スケジュール共有
  - blog,ソーシャルメディアによる情報発信
  - メールマガジン配信、およびそのためのメールアドレス取得
  - これらを組織的な合意なしに利用している
- 個人的な利用も多く、管理対象になることが意識されていない
  - 有償サービスでは契約や支払があるので、突き止めることができる
  - これらが無い無償サービスの把握は難しい

- 改善はリスクの高いシステム・業務から着手
  - 大量の消費者個人情報を扱うシステム
    - プライバシー情報（健康情報、家族構成、世帯収入等）を扱う場合にはより高いリスク
  - 通信販売等の電子決済システム
    - クレジットカード情報を扱う場合は、さらに高リスク
  - 取引先の業務に関わる情報
    - 設計開発情報
    - 商品企画情報
    - 受発注・売上情報
    - 情報オーナーは取引先で情報の取り扱いに関する指示があり、管理責任を負わされているもの
  - 財務報告・適時開示に関わるシステム
    - 金融商品取引法（J-SOX）に関わるシステム
  - インターネットシステム
  - 上記が組み合わさるほど高リスクとなる

ITセキュリティ改善: 個別システムでの対策

- システム改善責任はシステムオーナーに
  - 改善に必要な費用の負担を求める
- リスクの認識
  - 漏洩リスク
  - コンプライアンス違反
- 運用の重要さの認識
  - 実施すべき運用が出来ていないことを認識させる

- 部門管理のシステム
- 情報の重要さに応じた管理を求める
  - 技術的な対策だけではなく、運用面の対策も
- 改善の見込みがないものは更新・廃止を求める

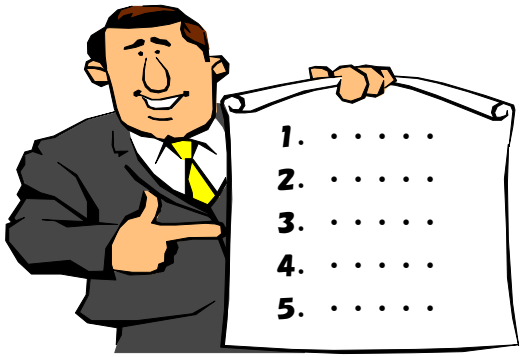
- 組織的な管理を求める
  - ITに詳しい人がいるだけでは運用出来ない状態に追い込む
  - 継続的な実施を求める
  - 属人的な管理の排除

ITセキュリティ改善： 推進上の課題

- リスクを理解してもらうことが困難
  - 部門管理や個人利用の場合は、相手にIT知識が期待できない
- 見つかった問題点だけを修正
  - 抜本的な対策は後回し、手を付けない
  - 似たような違う問題が発生し続ける
- 利用者への管理強化は期待できない
  - 厳重な管理は徹底が困難で効果が上がらない
    - 定期的なパスワード更新の徹底は困難
  - 管理強化と引き換えに、利便性が低下
    - ユーザー側に不満が募る、従わなくなる
- 組織的な取り組みが出来ていない
  - ITに詳しい担当者が属人的に対応
  - 事前のセキュリティ対策費用を見込んでいない
  - 都度、最小限の対応のみ

組織的なセキュリティ管理が出来るシステムのみ存続へ

ITセキュリティPDCAの確立



ITセキュリティ推進体制の確立

- 組織全体での情報伝達経路の確立
- IT資産の把握
- セキュリティ状況およびリスクの把握
- 高リスクシステムに対して改善実施

- 全社IT部門の統制下に
- 未達システムへは更新・集約・廃止へ
- セキュリティレベルの維持と定期的な報告

- これらをPDCAサイクルで回し、レベルアップにつなげる

個別対策から包括対策へ

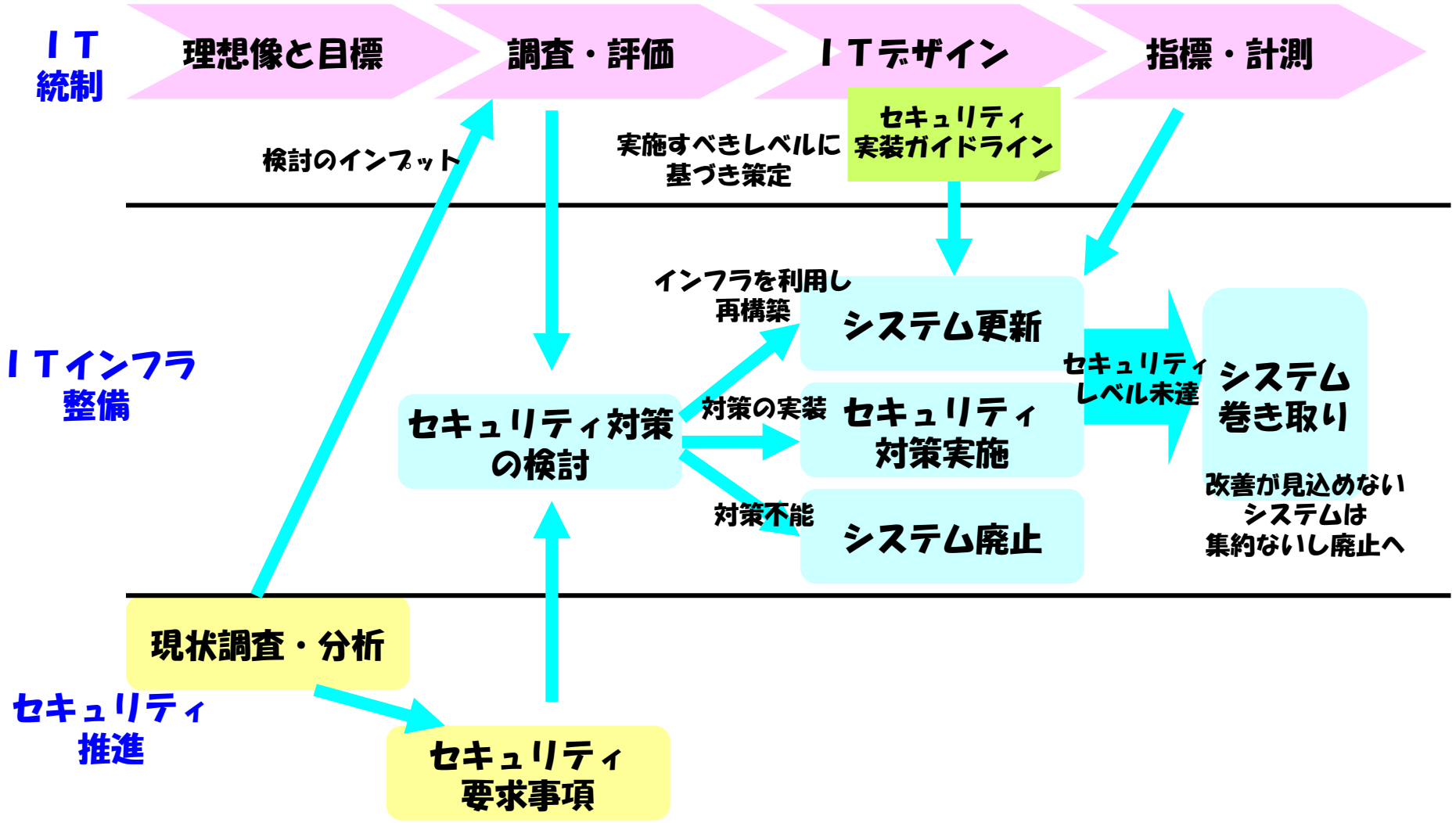
- 高いリスクが発見されたシステムでは改善を実施
- 次の点検・監査では、改善が進んで無い・新たなリスクが発生して、リスクが下がらない
  - 特に部門管理のシステムが多い

- このような、改善が進まないシステムの扱いが課題

- 本質的には組織としてセキュリティ維持を含むシステム保守体制を組めていないのが問題
- 体制を含めた改善の見込が無いシステムは、部門任せにしない行政力を行使

ITインフラ整備の例

- セキュリティ推進とIT統制を連動し、包括に改善する



システム集約の考え方

- 業務上必要だが部門管理ではリスクが高すぎるシステムは全社集約
  - データのみ移行（ファイルサーバー、グループウェア）
  - 全社提供環境（Iaas/PaaS等）に再構築
  - 現行サーバーを移行（移設、P2V）

- 集約効果
  - セキュリティ運用を全社IT側で行う
  - インフラ共通化で効率化し、費用対効果を向上させる
- 似たような違うものは作らせない
  - カスタマイズし過ぎると、バージョンアップ等に追従できなくなる
  - カスタマイズコストの経済合理性を認識させる
  - 80点主義で

- セキュリティポリシー等ルールを整備し、改善の見込みがないシステムは集約ないし廃止させる

集約環境の整備

- 全体最適の観点で構築
- SaaS環境
  - ファイルサーバー
  - グループウェア(掲示板、スケジュール管理など)
  - ワークフロー〈一般的な申請・承認・記録〉など
- IaaS/PaaS環境
  - x86でWindowsもしくはLinuxの特定の種類に絞る
  - OS,Webサーバー、ミドルウェア(Java, DB等)まで用意
  - インターネット提供と必要なセキュリティ機器(ファイヤウォール、ロードバランサー、アクセラレータなど)
- その他インフラ
  - 統合ID管理システム(LDAP, ActiveDirectory等)
    - ユーザーID改廃等の管理業務は全社側
  - ログ管理システム
    - アクセスログ、セキュリティログ、特権操作ログ、
- これらインフラのセキュリティ管理は全社IT側で実施
  - パッチ適用・バージョンアップ
  - バックアップ、キャパシティプランニングと必要な増強
  - コストは必要経費として部門に請求

ライフサイクル管理の徹底

- 新規システムのセキュリティ確保はどうするか？
  - 特にセキュリティ機能は企画段で意識しないと、後付は困難

- システム企画時からセキュリティを検討させる
  - システム・業務に関わるリスクの認識
  - 必要な対策とその費用の見積もり
    - 運用時コストも
  - システム化可否の再検討
- これにはIT部門の支援が必要

- さらに運用中のセキュリティ維持も必要
  - 脆弱性管理
  - ID改廃
  - システムバックアップ
  - これら運用を担う人的資源の確保
- システム寿命の意識
  - サポートが切れるとセキュリティパッチ等が出なくなる
  - セキュリティ維持が困難→原則システムの再構築または廃止
  - 全てのシステムコンポーネントのサポートに留意する
  - 再構築・移行・廃止などを計画させる

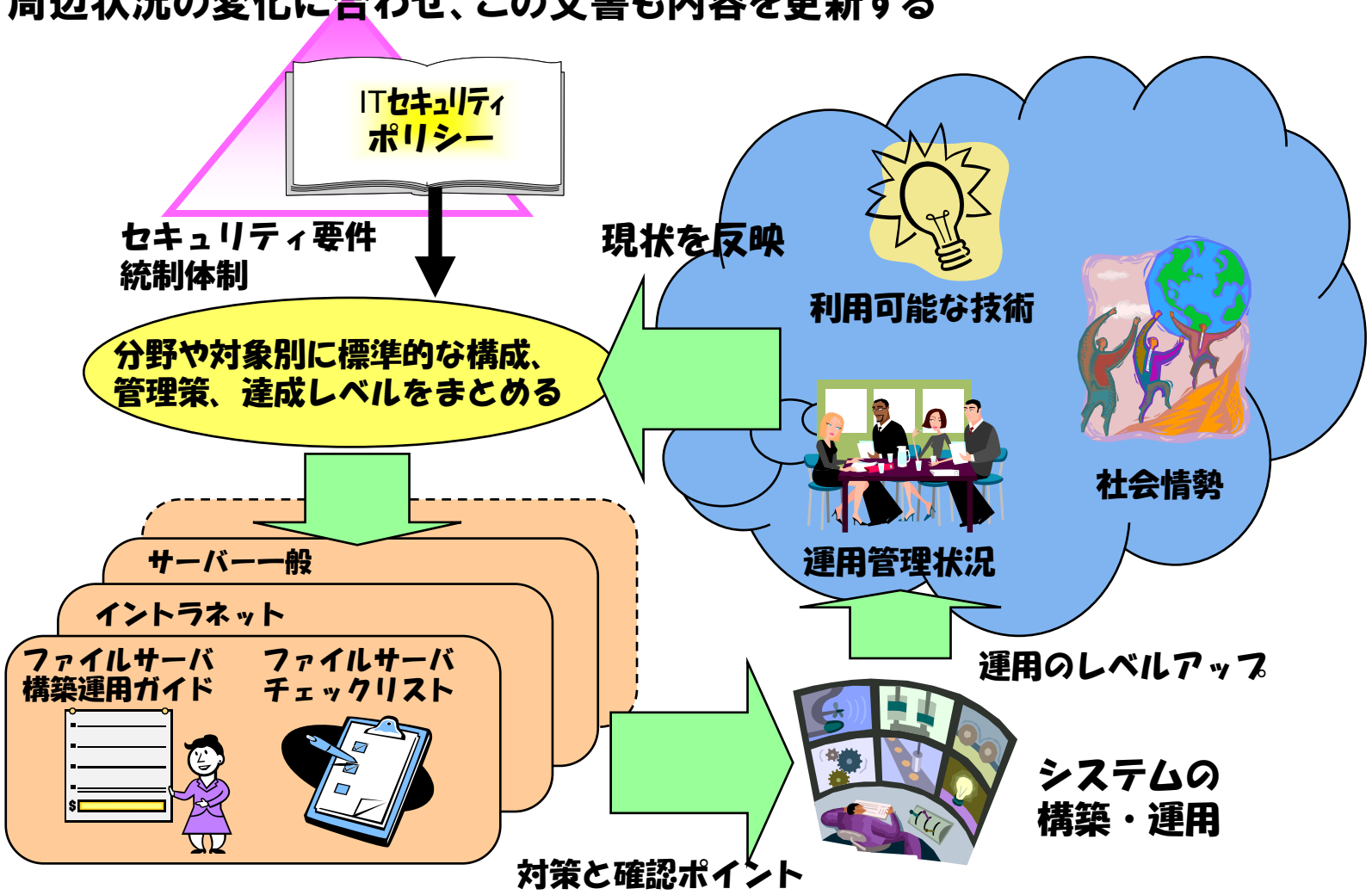
標準化の推進

- 多くのシステムが共通に利用する機能は標準化
  - システム構成
  - 運用手順
- 代表的な標準化項目
  - ハードウェア、OS, ミドルウェア (Web、アプリケーションサーバー、DB等)
  - ネットワーク機能 (Internet接続、FW/SSL/LB、VPN等全社が提供するものを利用)
  - ID管理機能、認証機能
  - ログ管理機能、特権管理機能
  - などから
- 運用も共通化
  - ログインIDは社員は社員ID、非社員は全社が発行したユニークID
  - パスワードは3ヶ月ごとに強制変更
  - システム管理作業は申請に基づき実施し、作業内容は全て記録・確認
  - など
- これらに従わない場合は、合理的な理由を示させる

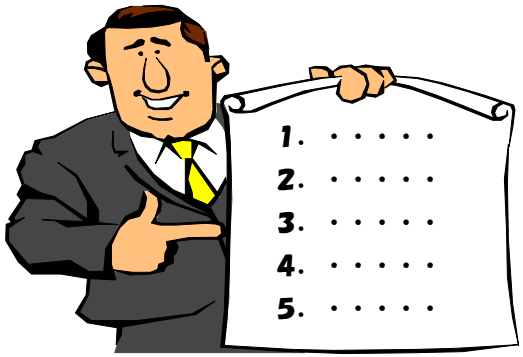
監査・点検ではセキュリティ機能が有効に機能しているか？
＝運用が出来ているか？
を問われる

ITセキュリティポリシー・実施ガイドライン・実装標準の整備

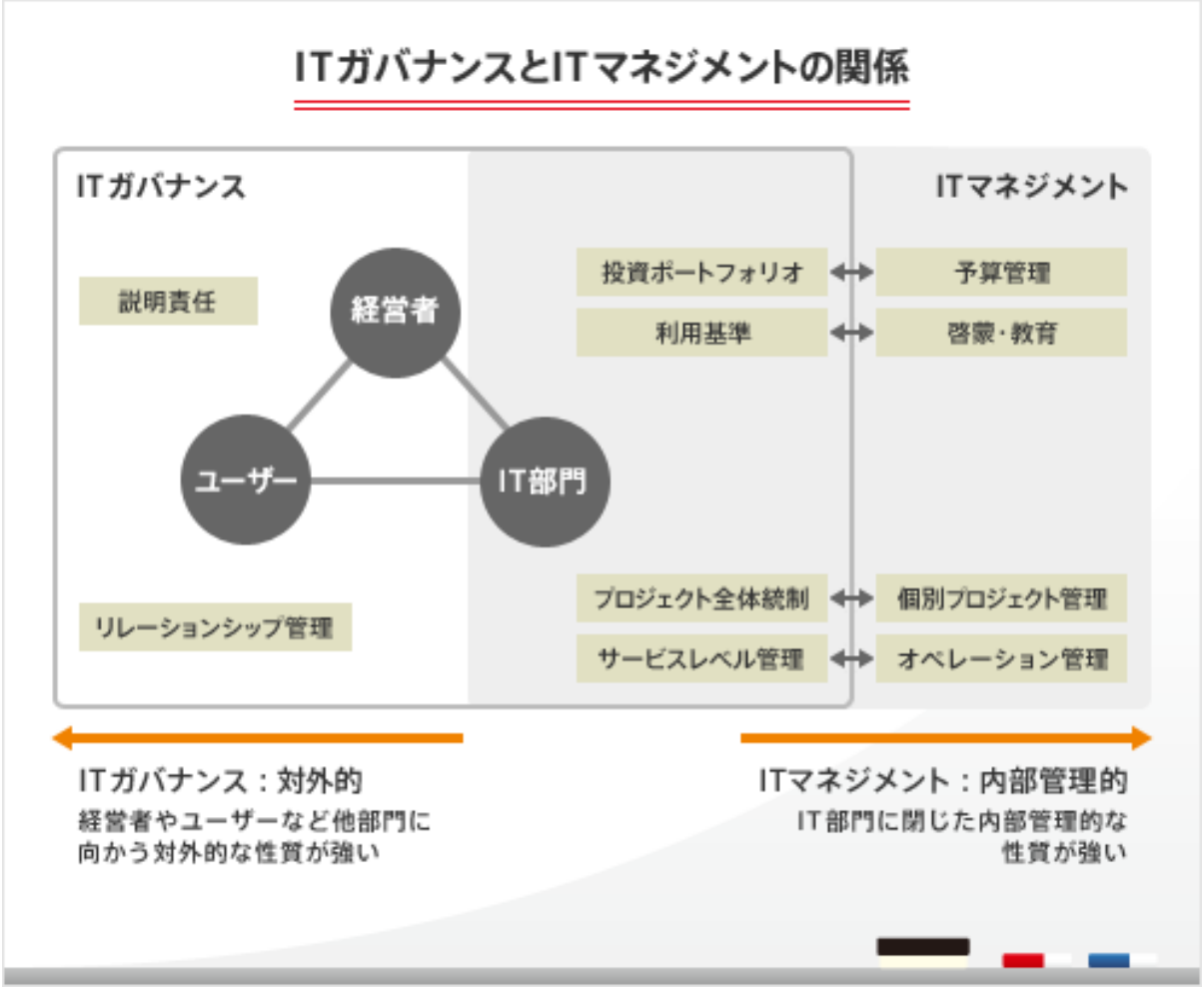
- 管理要件を実現するために、より具体的な文書を作る
  - 分野別に対策とチェック項目をまとめ、実施の徹底と管理
  - 周辺状況の変化に合わせ、この文書も内容を更新する



ITセキュリティから
ITガバナンスへ



- セキュリティはITガバナンス全領域に渡るため、初期段階の取り組みテーマになりやすい



http://www.meti.go.jp/policy/it_policy/it_keiei/action/keyword/governance/index03.html

- グループ全体のIT戦略に基づいた、IT施策を行えること

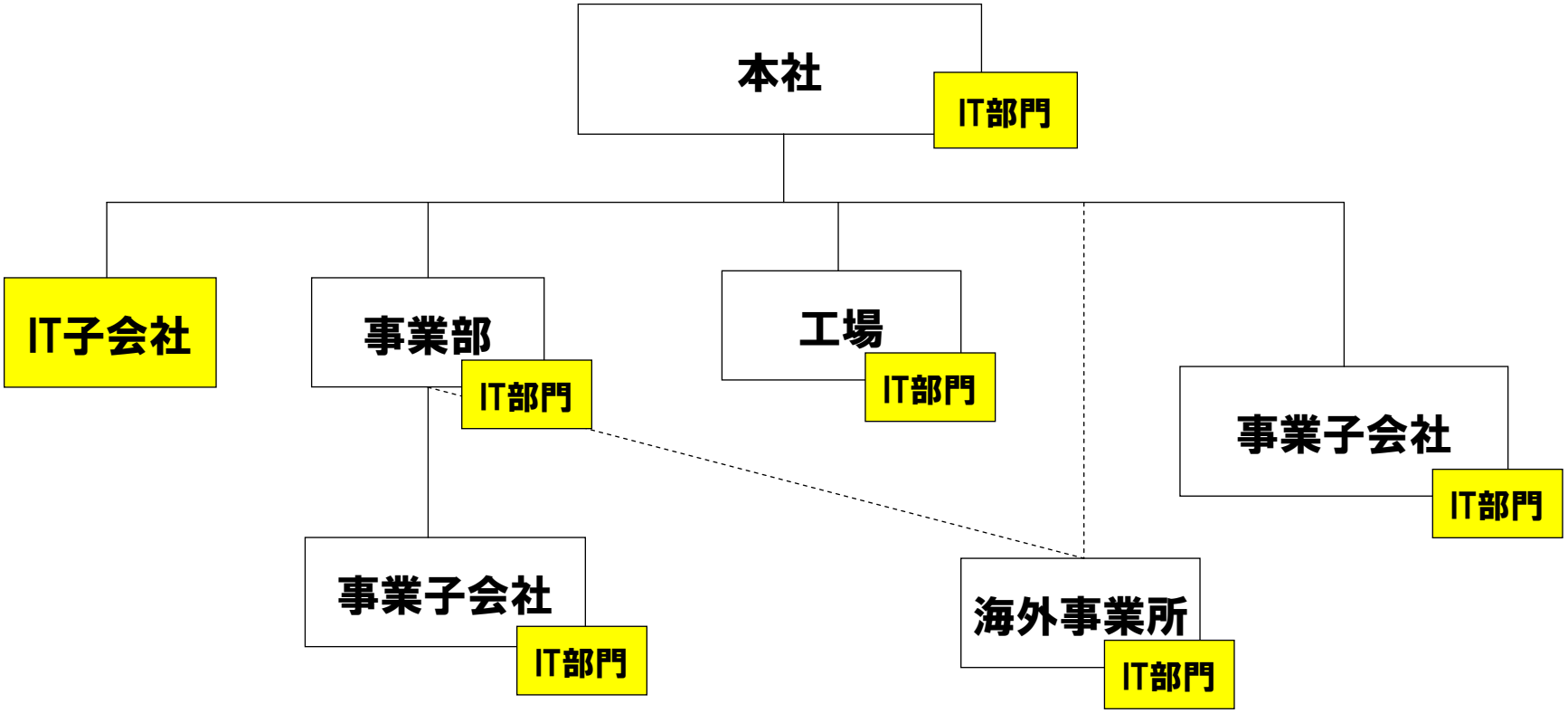
- IT戦略の例
  1. ITガバナンスの方針を明確にすること。
  2. 情報化投資及び情報化構想の決定における原則を定めること。
  3. 情報システム全体の最適化目標を経営戦略に基づいて設定すること。
  4. 組織体全体の情報システムのあるべき姿を明確にすること。
  5. システム化によって生ずる組織及び業務の変更の方針を明確にすること。
  6. 情報セキュリティ基本方針を明確にすること。

  経済産業省　システム管理基準 より

- この実現に必要な、実施体制をグループ全体に展開すること

大規模企業における典型的なIT部門配置

- IT管理を行う部門・機能は組織に散らばっている
  - 小さい部門・部署（支社・支店・子会社等）では「システム担当者」等の場合や、担当が居ない場合もある
- 組織全体のITガバナンスはIT部門間の連携を高める必要がある
  - 組織によって現状は全く異なる



ITガバナンスが進まない原因

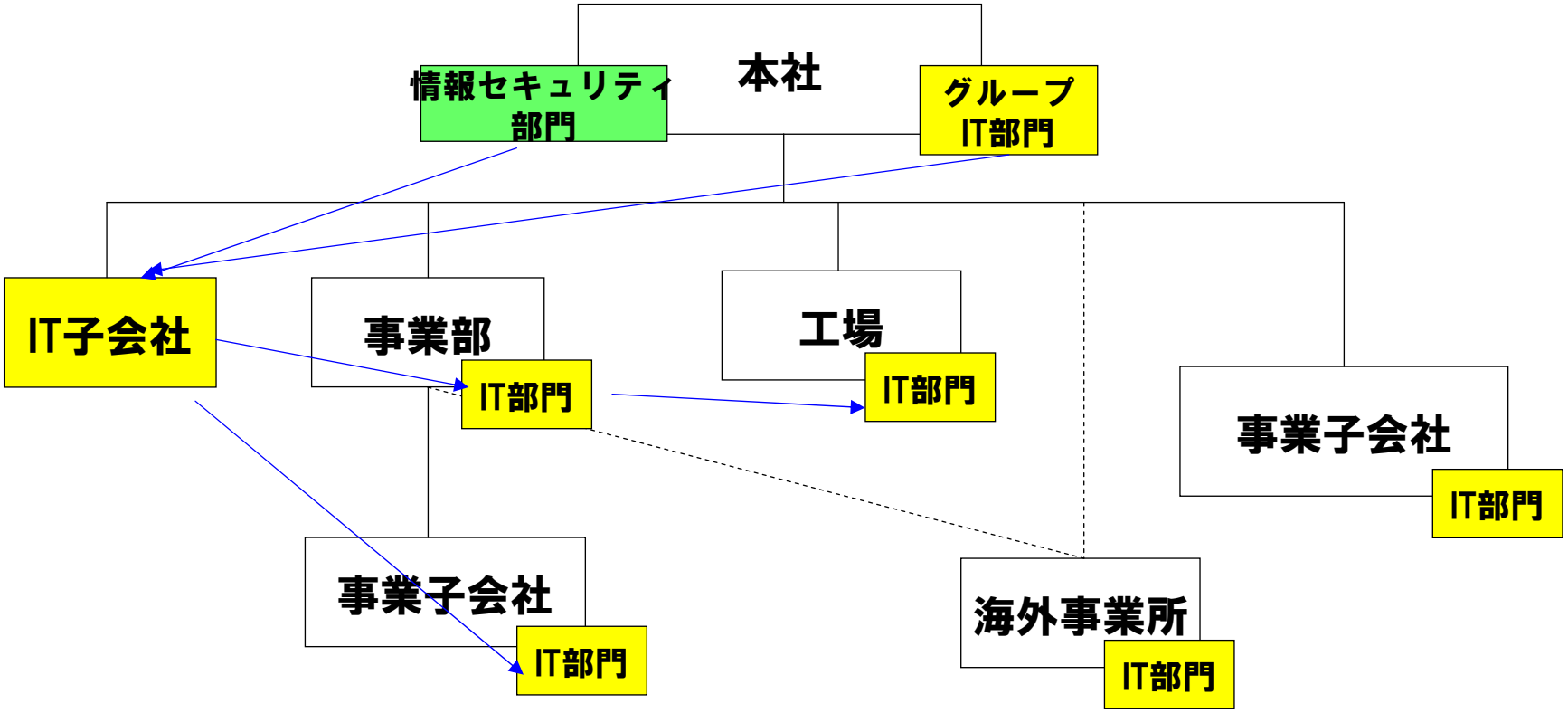
- 事業部のIT部門　＞　全社IT部門
  - 事業部投資を背景にIT化実務を担当
  - 業務ニーズを知り抜いている

- ユーザーが直接ITサービスを入手
  - パッケージ化、サービス化（クラウド）、低価格化、無償化の流れ
  - システム開発では直接SIerと要求仕様などを調整
    - PC，スマホ、タブレットなどの利用
    - ECサイト等高度なITシステムでのユーザー体験
    - 全社IT部門はサーバー設置等しか関与していない場合も

- 全社IT部門が期待されなくなる
  - 高コスト、低クオリティ、長納期など
  - 情報子会社化すると、次第に事業部側観点が欠けてくる

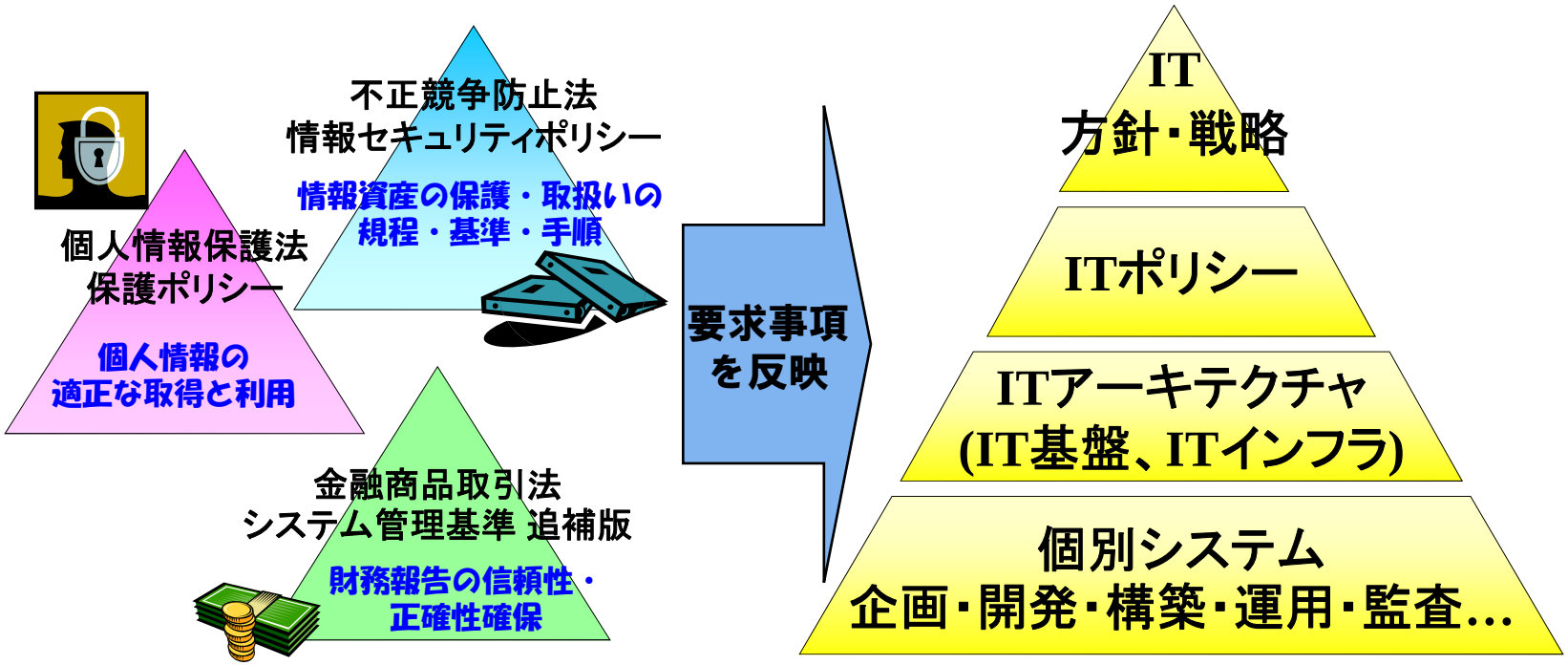
機能するIT部門連係

- グループ本社ではITや情報セキュリティに関する企画・施策を具体化する
- その実施はIT子会社を活用
  - 本社の裏付けがあるため、強いガバナンスが可能
- これら部門間の人的交流も重要
  - 検討への参加、各種施策の先行適用・試行
  - 研修会実施、人事ローテーション



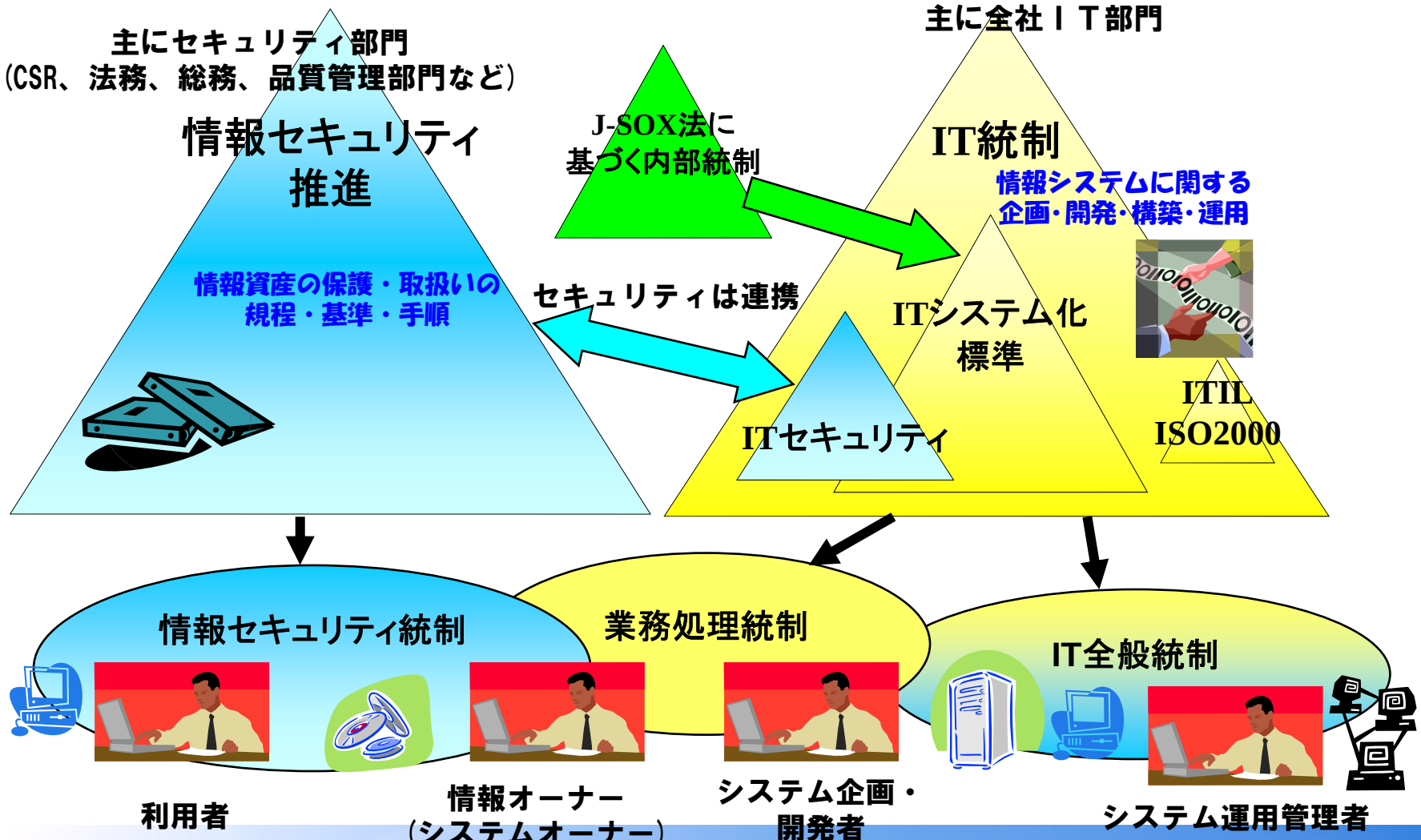
ITガバナンスの考え方：基本

- 法的・社会的な要求事項・コンプライアンスに、一つの体系で対応
  - 不正競争防止法、個人情報保護法、金融商品取引法、会社法なども含む
  - 各種規格（9000,14000,15000,20000,27000,…）、業界標準（PCIDSS等）
- ガバナンスはトップダウンが基本
  - IT方針・戦略 → ITポリシー → ITアーキテクチャ → 個別システム
  - この中にITセキュリティも含める
- 業務効率化・投資効率化・セキュリティ確保がテーマ
  - 標準化とアーキテクチャ選定がコスト効率化・セキュリティ確保を両立させる



情報セキュリテとITガバナンスの関係

- 全社のITセキュリティ整備から始める
- セキュリティのレベルアップとともにITガバナンスを確立していく



初期段階のITセキュリティガバナンス

- ITガバナンスはグループのIT資産の把握から
  - グループ全体でのIT資産の把握
  - 前述のITセキュリティに関するテーマが適している

- セキュリティ以外のシステム課題も把握
  - 事業継続性・災害対策の面のリスクが高い
  - 業務効率が向上していない
  - 投資効率が不明確など

- これらから全社課題と解決に向けた方向性を見出す

目指すべき方向

- IT部門が経営に貢献していることを明確にする
  - IT活用による業務効率化を積極的に提案
  - ITインフラ・運用の整理・統合により費用削減と運用レベルアップ
  - 安心・安全なサービス提供（セキュリティ、BCPなど）

- これらをPDCAに基づき実施
  - KPI/KGIに基づく計画と成果管理
  - システム監査・自己点検
  - これら結果からの個別システムおよびマネジメントシステムの改善

より良いサービスを提供するIT部門へ！

- 今回の講演は次の法令・規格等を参照にしています

- 情報セキュリティ
  - 不正競争防止法、営業秘密管理指針、ISO27000
- 個人情報・プライバシー
  - 個人情報保護法、経済産業分野ガイドライン、JIS Q.15001
- リスク管理
  - ISO31000、ISO 27005, ISO TR13335 (GMITS)
- BCP
  - ISO22301
- J-SOX,SOX
  - 金融商品取引法
  - システム監査基準追補版(財務報告に係るIT統制ガイダンス)
  - COSO/COBIT
- IT運用
  - システム管理基準、システム監査基準
  - ITIL/ISO20000

登録商標

1. windows、Active Directoryは、米国 Microsoft Corporationの米国及びその他の国における登録商標または商標です。
2. Javaは、米国およびその他の国における日本オラクルインフォメーションシステムズ社の商標または登録商標です。
3. Linuxは、Linus Torvalds氏の日本およびその他の国における登録商標または商標です。
4. その他会社名、製品名、またはサービス名も、他社の商標またはサービスマークである場合があります。

End of file