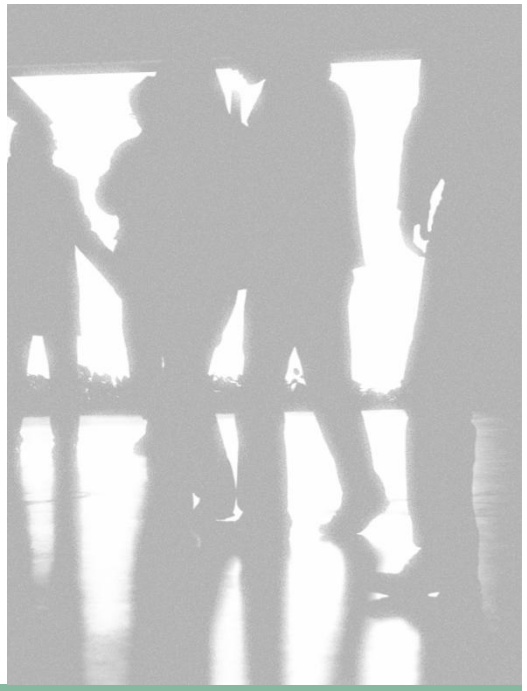
セキュリティ対策技術は
どこまで
導入すればいいのか？



2014
11/14

情報処理推進機構　CIO補佐官
葛西　重雄

IPA

セキュリティ対策の空白　－専門性の分断－

各種団体
コンサルタント

情報セキュリティマネジメント
ISMS　ISO27002

システム部門
運用会社

情報セキュリティ管理の実践
ISO27002

監査法人
コンサルタント

情報セキュリティ監査
情報セキュリティ監査基準

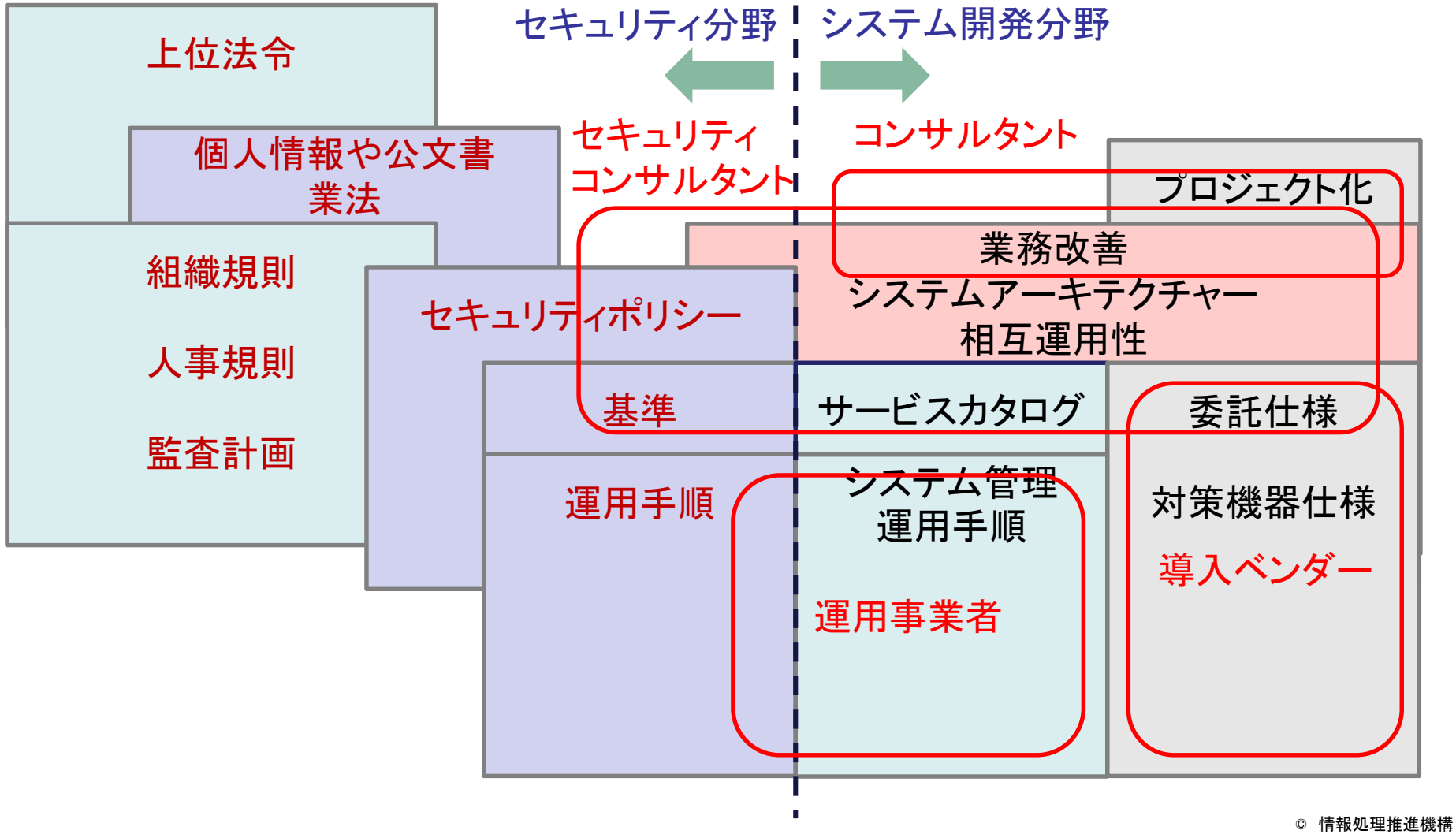
運用会社
SI・ベンダー

ITサービスマネジメント
ITIL

SI・ベンダー
メーカー

情報セキュリティ対策
ソリューションの導入
ISO15408 ISO27033

セキュリティ分野とシステム開発分野の分断



主観的な評価から合理的な解決へ

セキュリティ統一基準などのガイドラインによると

ISMSの準拠を前提とすると
セキュリティ監査によると

標的型攻撃が増加している
運用システムでアラートが出ている

このレベルのセキュリティ対策でいいのか？
そのようにいつ誰が決めたのか？

脅威や脆弱性

セキュリティ問題から発生する可能性のある事業損害に対してバランスがとれている必要がある。
（ISO27002:2014）

制約条件

プロジェクト化の能力　－定量化の必要性－

セキュリティコンサルタントはプロジェクトマネジメントのコンサルタントとはかぎらない

COCOMOに共通する式（バリーベーム）

$$E = a(L)_b (a > 0, b > 0)$$

E = 開発工数
L = 開発規模（KLOC）
a、b= 定数

$$D = c(E)_d (c > 0, d > 0)$$

D = 開発期間
c 、d = 定数

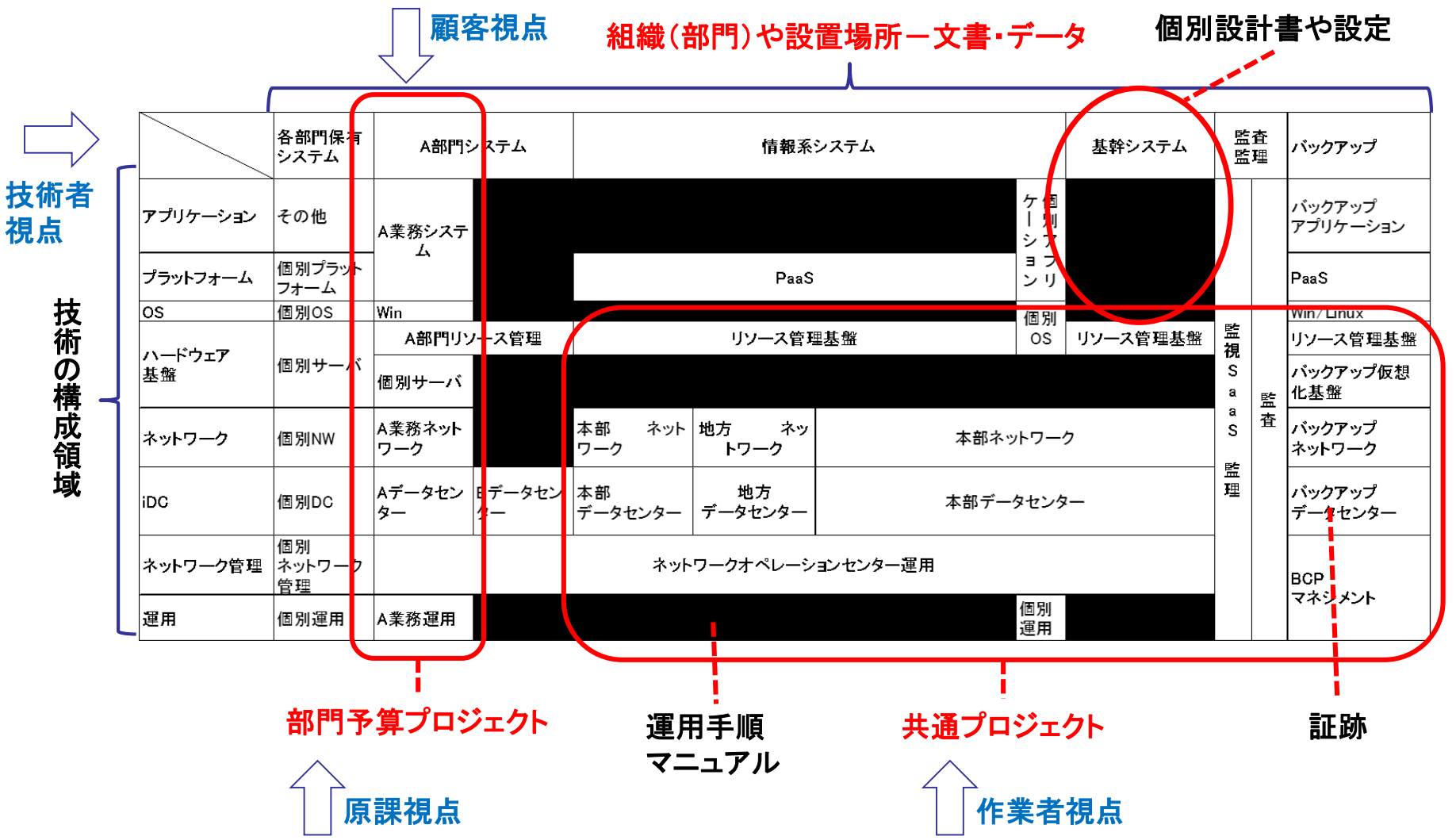
COCOMOはスクラッチ開発の
見積もり技法ですよね？

どんなにベンダーに無理を言っても、
対策実施の範囲や、導入機器のボリュームによってセキュリティ対策は
期間内に完遂できない。
※期間的制約には抗えない

「保有する情報資産」
「対象となる業務種別」
「サービスの価値」

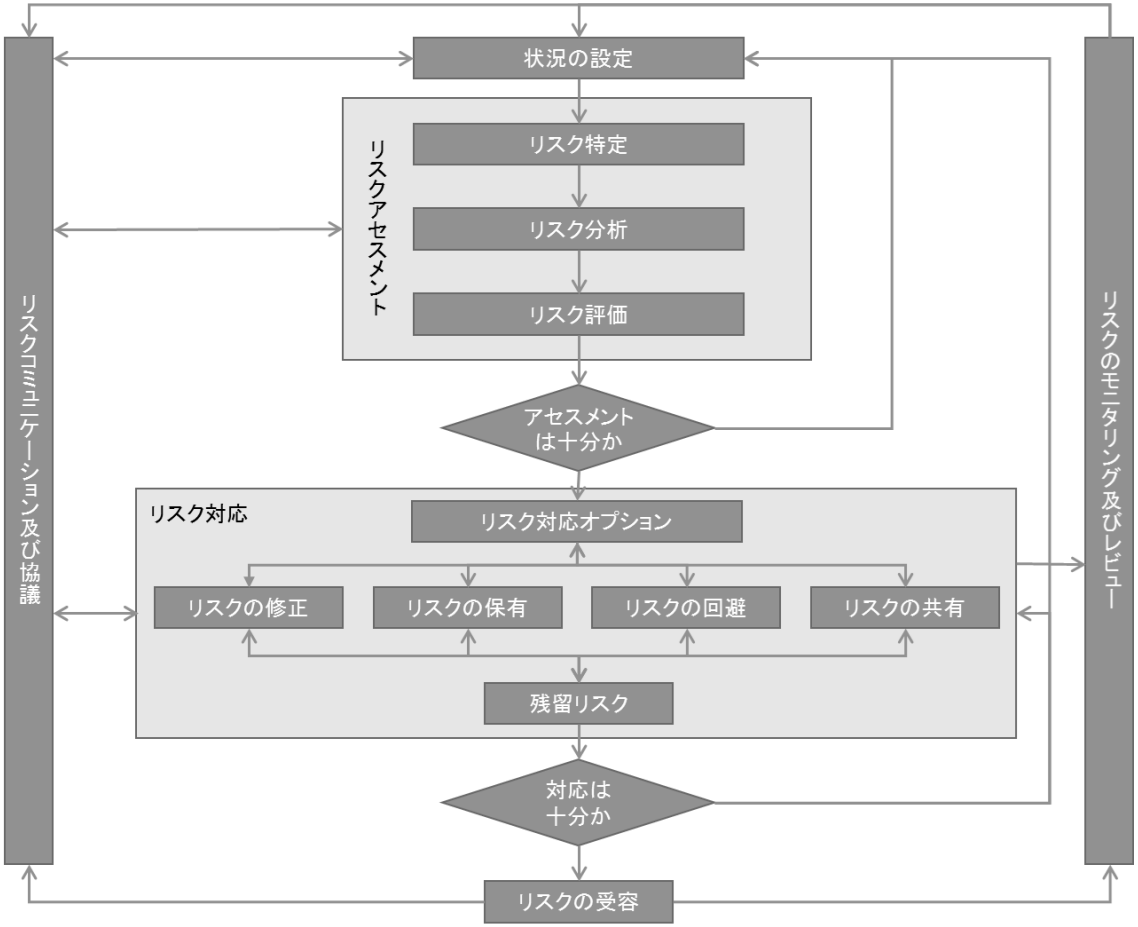
WBSの作成やプロジェクトを実施した際の期間を類推する
ファンクションポイント概算の見積もりの誤差は20～40%

漏れがないように　ーリファレンスの活用ー

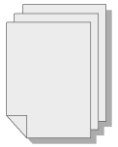


リスクアセスメントと対策の基準

リスクアセスメントのプロセス（ISO27005より引用）



業務一覧　文書管理簿 DB等技術の配置



基本法令
業務関連法令
秘密文書の取扱い

人命に関わる等倫理的事項

情報評価

直接収入に影響
緊急情報や重要情報
影響が大きい手続き

高いサービスレベル

影響が低い業務や情報
中程度以下のサービスレベル

復旧を急がない情報や業務
価値の低い情報や業務

リスクシナリオの推測

ーシナリオは定期的に確認し、更新するー

起因・原因

促進要因と対象

被害結果

マルウェアメール
不正サイト閲覧

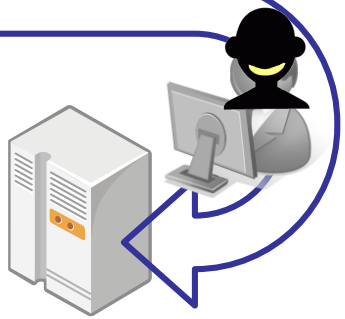
特権の取得

ウィルス拡散

運用作業のミス

悪意がある人への
情報漏えい

サービスの停止
情報の喪失



バックドアの
組み込み

技術的なセキュリティホール

災害による建造物破壊
電源喪失

秘密情報の売却
秘密情報の拡散

許可を得ない秘密情報
の持ち出し

人命に関わる事項や倫理的事項～被害額の算定

治療の停止、治療の躊躇、避難への影響、犯罪の誘発　等

大規模な産業被害、重要インフラへの影響、巨大投資の回収不能　等

必須

通常期損失収入＝サービス停止予測期間×通常期の一日の収入（損失額）

繁忙期損失収入＝サービス停止予測期間×繁忙期の一日の収入（損失額）

対応・対策費用＝外部CERTやSOCの緊急時稼働費用＋フォレンジクス費用
対策運用費用（システムの縮退等運転変更等）＋対策機器導入・入替費用

説明機会関連費用
会場費用＋告知費用＋広告費用＋調査費用＋法的対応費用

損害賠償額－過去の事例や判例より
（個人情報漏えいの賠償額－一人あたり20000円～40000円、委託された業務の履行）

優先度や対応オプション設定

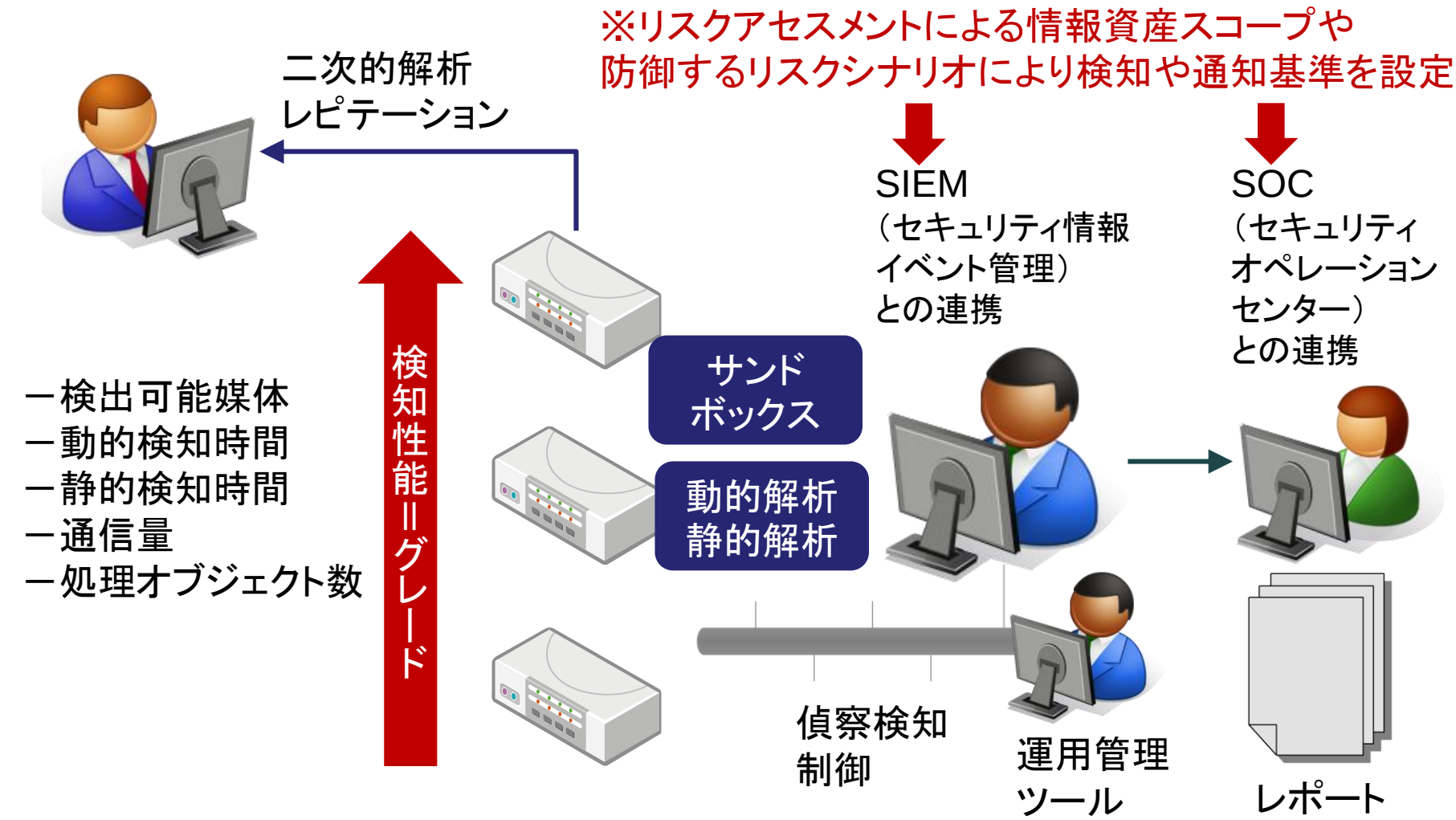
必須対策以外の対策優先度を決めるために
必須対策⇒被害額×影響範囲⇒対策可能性

業務・システム分類	インシデント	対象の情報資産	想定被害（額）	対応策と費用	分掌事務	組織等		
						係等の名称	課等の名称	部の名称

領域ー	関連システムー	対策種別ー	プロジェクト名ー	主管部門ー	予算種別ー	制約条件ー
XXネットワーク	XX業務システム	検知導入	XXLAN改修	情報システム	原資	（見積もり額） Xx月～xx月

検討仕様（テスト基準）ー標的型攻撃対策（侵入検知）
検知
検知後動作
カスタマイズ
解析
運用

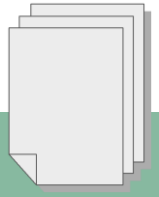
仕様の確定　－対策機器導入の盲点（APTを例に）－



セキュリティ対策と説明責任

対策できていないシナリオ（残留リスク＝被害額）を説明できるようにする必要がある

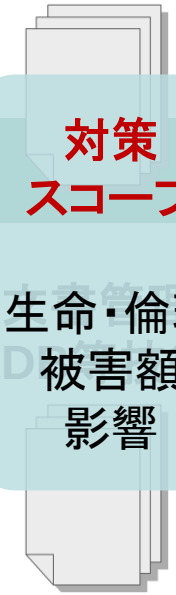
業務一覧



リスクシナリオ

被害予想額

業務一覧

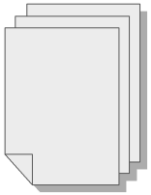


対策
スコープ

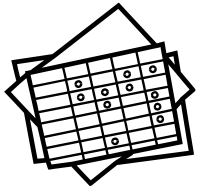
生命・倫理
被害額
影響

残留リスクシナリオ

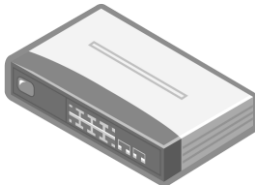
文書管理簿
DB等技術の配置



プロジェクト工数



対策費用概算



対策プロジェクト
実施