テーマ２
続・効率的リスクアセスメント

JNSA標準化部会
日本ISMSユーザグループ インプリメンテーション研究会
尾崎 幸彦 (株式会社Speee)

自己紹介

尾崎 幸彦 (おざきゆきひこ)

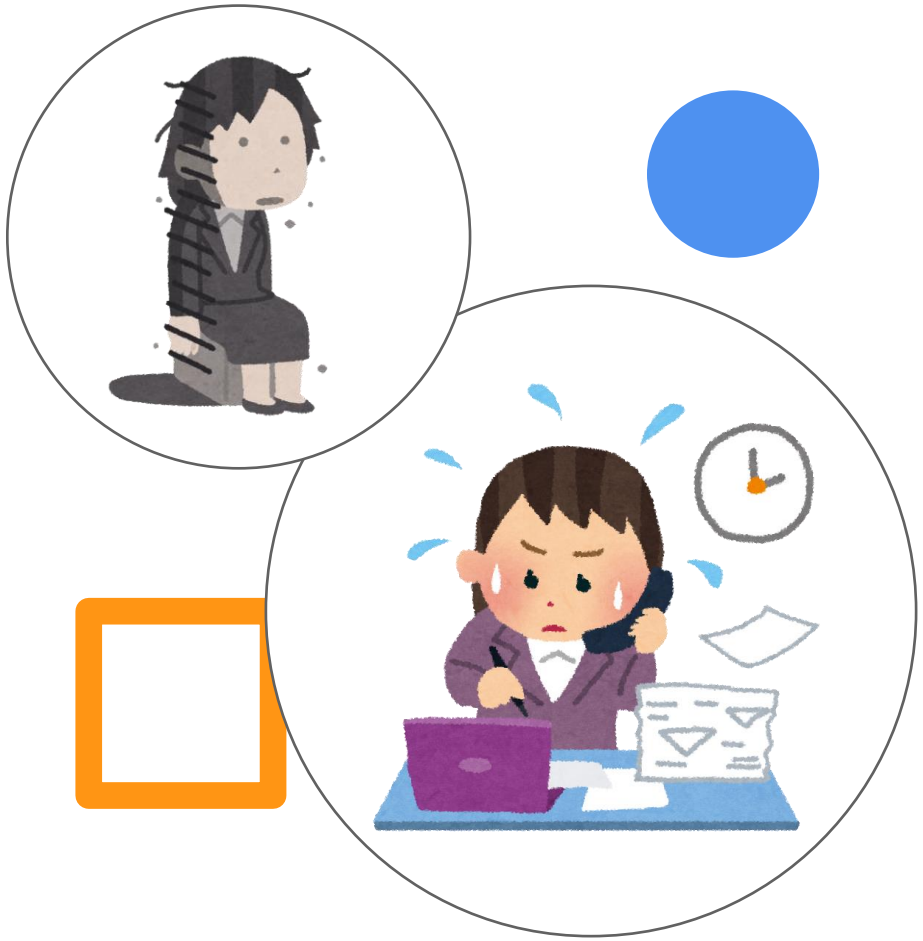
- 株式会社 Speee セキュリティ推進室
- ISMS/ISMS-CLS主任審査員

略歴	
2006年頃 ～2018年	NECソフトウェア中部 →[全国7社合併]→ NECソリューションイノベータ株式会社 • 情報セキュリティマネージャ • 7社合併(計1.5万人)時、既存13個のISMS認証を1年間で1個に統合
2019年4月 ～2021年10月	株式会社 日本環境認証機構 (JACO) • ISMS/BCMS 審査員
2021年11月～	株式会社 Speee • セキュリティ推進室 -情報セキュリティマネジメント担当

はじめに

グループ会社でのクロス監査や、審査員業務を通じて、ISMS事務局を担っている方々の「他組織ではどうやっているのだろう？」という思いや質問を数多く受けました。
私自身が事務局のときも、同様に感じていました。

それを思い出し、「ISMS-UGの方々の知見を集め、皆さんのお役に立てる情報をお届けできれば」、、、というのが、今回のテーマの発端でした。



目次

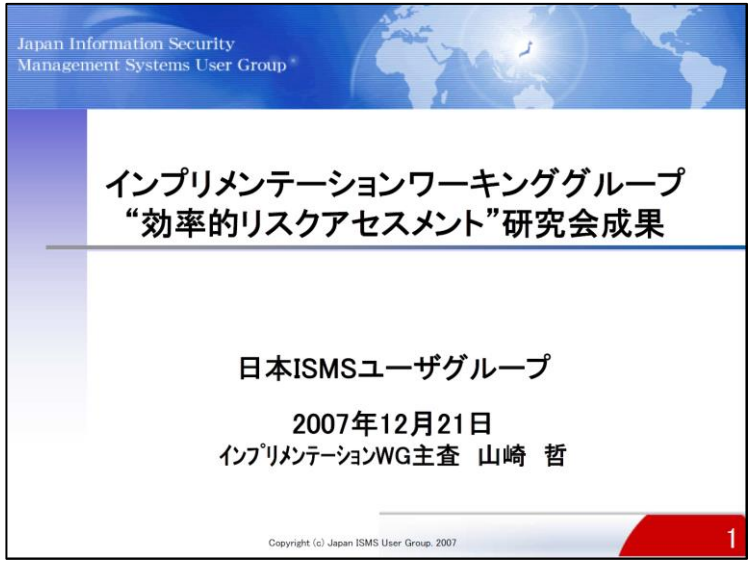
Part.1 過去の振り返り

2007年と2017年の本セミナーでリスクアセスメントを題材にしていたので
その内容を簡単にご紹介します。

リスクアセスメントを取り扱った、過去成果の振り返り

2007年

- 研究会各社対象にアンケートを実施し、リスクアセスメントでのベタープラクティスを抽出



2017年

- リスクアセスメントでの従来手法の課題5点を設定し、それぞれの解決方法を提案

2007年:各社の取り組みの特徴

各社発表において示されたセキュリティマネジメントの取り組みの特徴

- グループ全体のセキュリティマネジメントと併せて部門単位のセキュリティ体制も構築
- 合併した組織におけるセキュリティマネジメントの構築の難しさ
- 複数のデータセンター企業のセキュリティマネジメントの構築

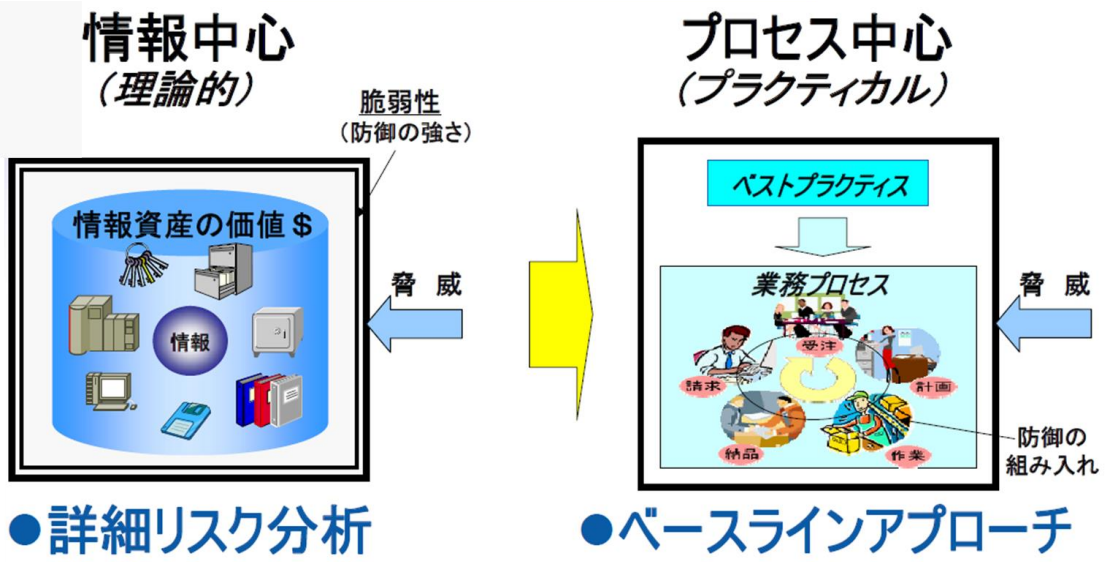
現在のリスクアセスメント手法

- 従来の情報資産リスト、リスクアセスメントは審査対応用、実際のリスク分析や改善は業務フローから実施
- 組み合わせアプローチが主流だが、ベースラインアプローチ及び詳細リスク分析の比率は企業によって異なっている

課題の認識と今後の方向性

- 環境の変化や事件・事故に対応できるリスクアセスメント
- グループに共通する標準の管理策を定める

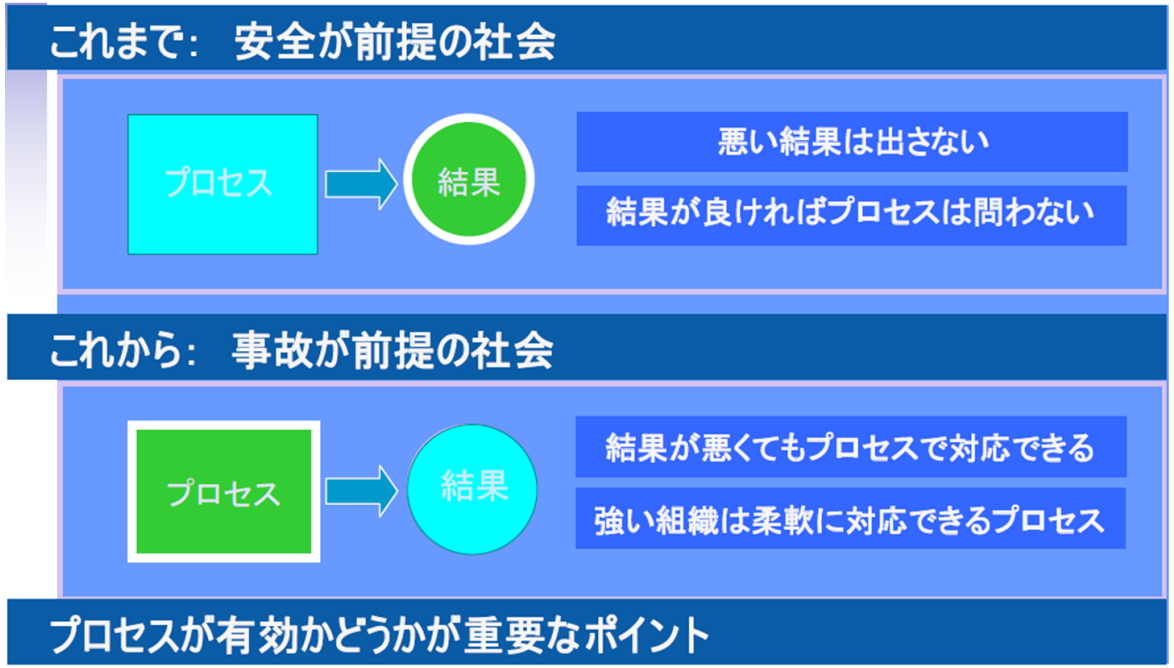
“情報中心”より“プロセス中心”



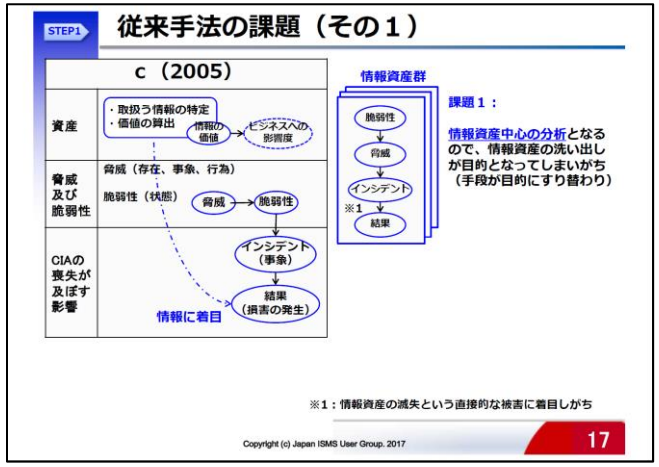
“情報中心”と“プロセス中心”の比較

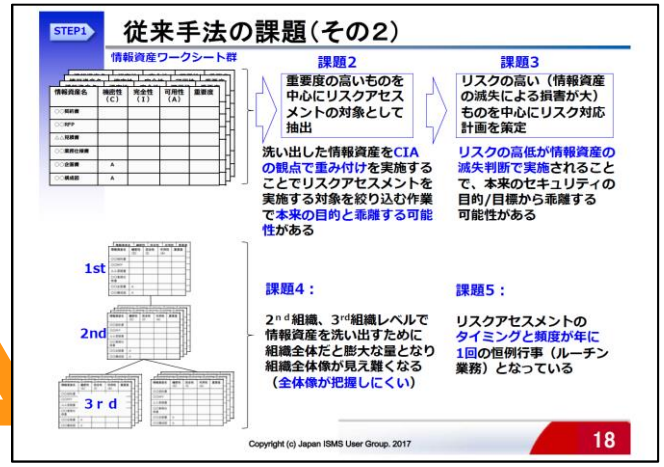
比較項目 ＼ 比較項目	情報中心	プロセス中心
▪手法	✓詳細に資産値、脅威、脆弱性よるリスク値を基に分析	✓実績のある対応策のフレームワークを基に分析を実施
▪日常業務の実態の反映	×実際のプロセスから情報資産への展開が難しい	○実際のプロセスに即して計画しインプリできる
▪変化への対応（法規程等）	×プロセスの変化に対応した情報資産の展開が困難	○プロセスの変化に素早く容易に対応できる
▪PDCAの回し易さ	×PDCAが回り始めた時、差分に対する評価が難しい	○PDCAの各プロセスに容易に導入し反映できる
▪ISMSの進展に応じた実践	×ISMS進展に応じて標準化・共通化が困難	○ISMSの進展に応じて標準化・共通化等効率化可能
▪ワーク負荷	×資産の要素の増加により複雑が増大し負荷大	○リスクアセスとプロセスが直結しているので評価し易い

“結果重視型”から“プロセス重視型”



2017年:従来手法の課題と解決方法



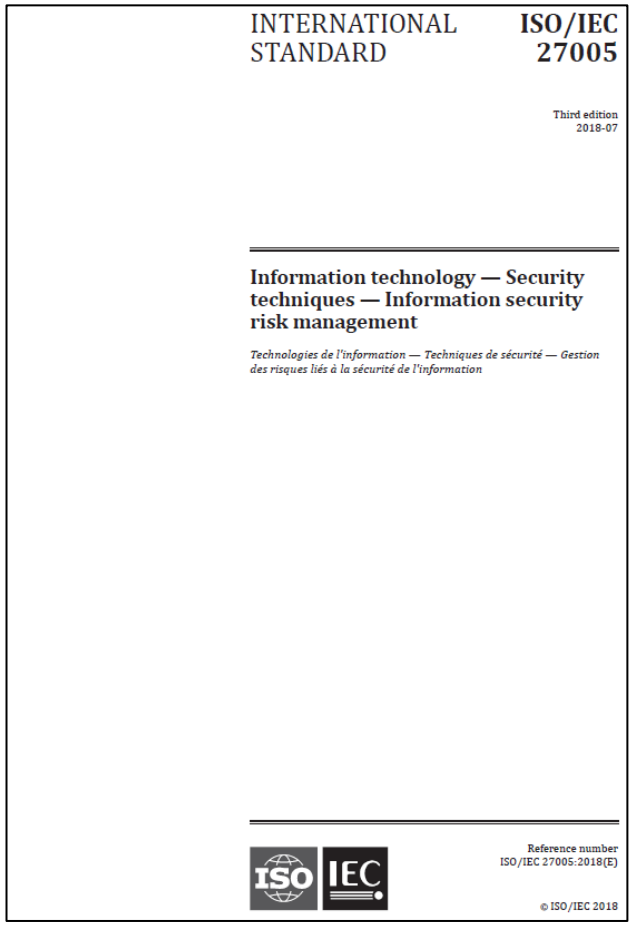


	従来手法の課題	解決方法
1	情報資産中心の分析となるので、情報資産の洗い出しが目的となってしまいがち(手段が目的にすり替わり)	リスクアセスメントの観点としてビジネスやセキュリティの目的/目標への影響度で判断 (情報資産を利用する業務プロセスも考慮)
2	洗い出した情報資産をCIAの観点で重み付けを実施することでリスクアセスメントを実施する対象を絞り込む作業で本来の目的と乖離する可能性がある	情報資産をCIAの滅失の影響の観点だけでなく、ビジネスやセキュリティの目的/目標への影響度も加味して判断する
3	リスクの高低が情報資産の滅失判断で実施されることで、本来のセキュリティの目的/目標から乖離する可能性がある	情報の滅失だけでなく、プロセスにも着目することでセキュリティの目的/目標を不確かにする要素を常に考慮する
4	2nd組織、3rd組織レベルで情報資産を洗い出すために組織全体だと膨大な量となり組織全体像が見え難くなる (全体像が把握しにくい)	組織全体や各部門等のセキュリティの目的/目標とを可視化することで対応すべきリスクを特定する →全体リスクと個別リスクとして整理
5	リスクアセスメントのタイミングと頻度が年に1回の恒例行事(ルーチン業務)となっている タイミングずれ(後手)	環境の変化に応じた適切なタイミングでの実施が必要 →環境に応じたタイムリーなリスクアセスメントを実施出来るように個別リスクの対応を現場サイドで実施出来るように整理する

Part.2 リスクアセスメントの規格

情報セキュリティリスクマネジメントの規格である27005での、
リスクアセスメントに関わる部分を少しご紹介します

ISO/IEC 27005

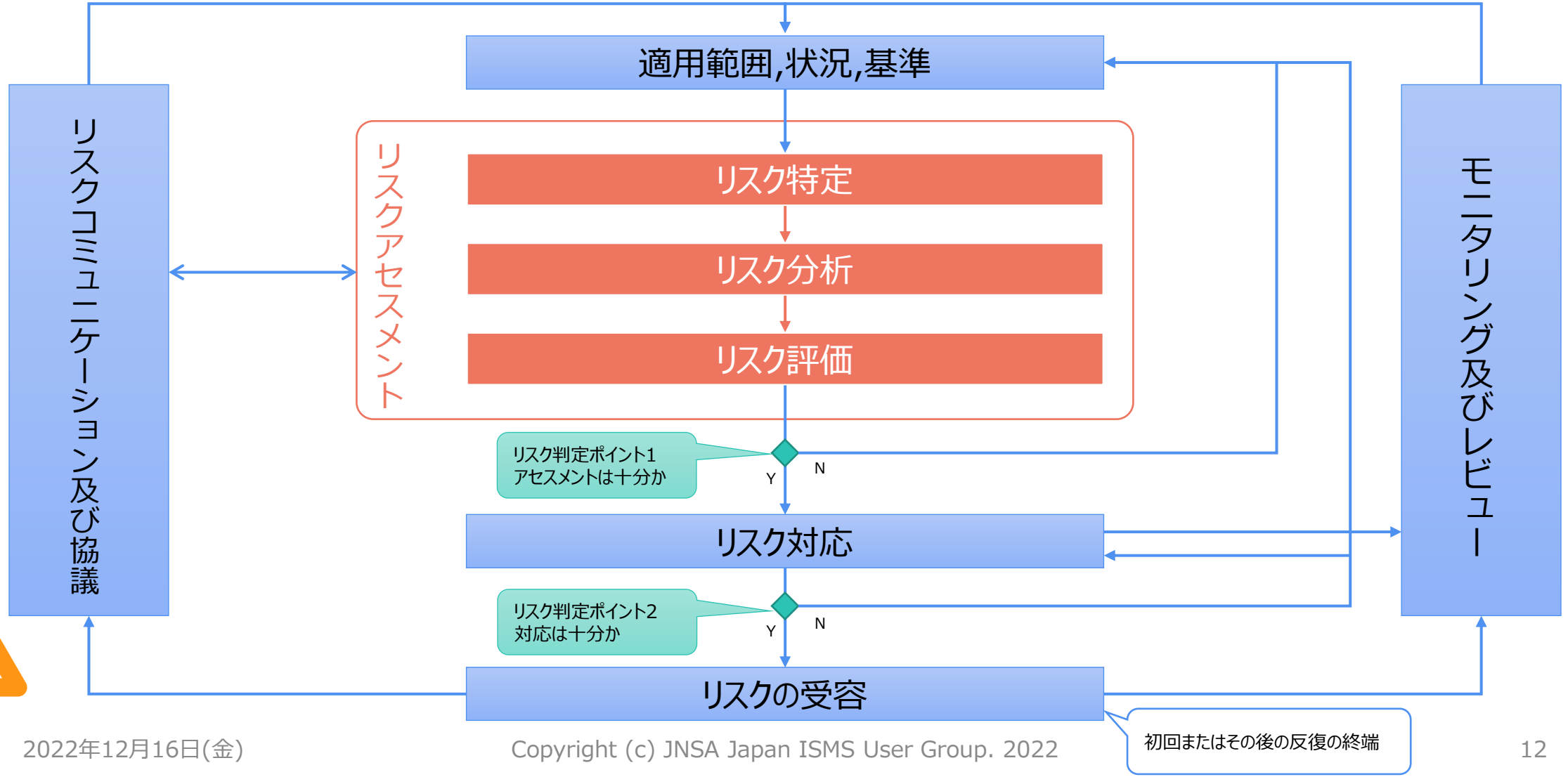


IEC/ISO 27005:2018

Information technology
- Security techniques
- Information security risk management

情報セキュリティリスクマネジメント

6.情報セキュリティリスクマネジメントの概要 図2



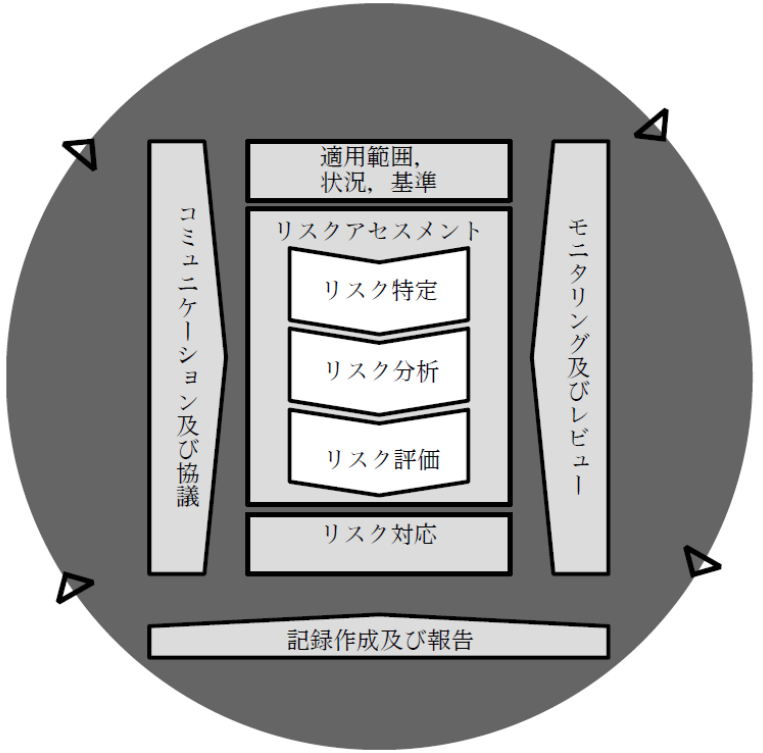
(補足)27001と27005と31000の関係

JIS Q 27001:2013

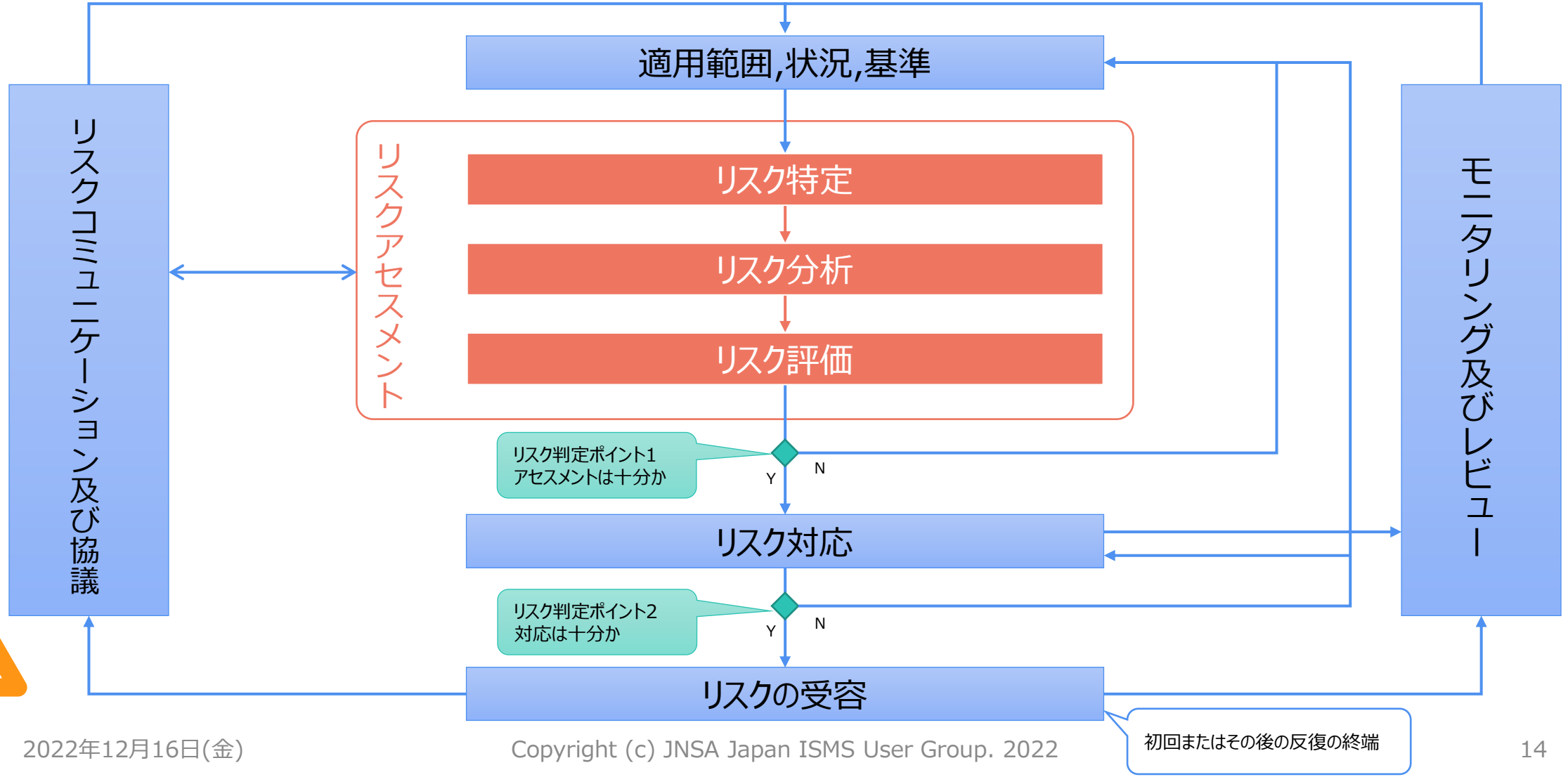
6.1 リスク及び機会に対処する活動

注記
この規格の情報セキュリティリスクアセスメント及びリスク対応のプロセスは，JIS Q 31000に規定する原則及び一般的な指針と整合している。

JIS Q 31000
6 プロセス 6.1 一般 図4



6.情報セキュリティリスクマネジメントの概要 図2



ISO/IEC 27005

8 情報セキュリティリスクアセスメント

8.1 リスク特定

8.2.2 資産の特定

8.2.3 脅威の特定

8.2.4 既存の管理策の特定

8.2.5 脆弱性の特定

8.2.6 影響の特定

8.3 リスク分析

8.3.1 リスク分析手法

8.3.2 影響の評価

8.3.3 インシデントの起こりやすさのアセスメント

8.3.4 リスクレベルの決定

8.4 リスク評価

8.2.2 資産の特定

インプット	• リスクアセスメントを行う適用範囲と境界 • その構成要素(資産のオーナー、所在地、機能等)のリスト
アクション	適用範囲内の資産を特定する
導入の手引	• 資産は組織にとり価値を有するものであり、従って保護を必要とする ➢ 情報システムは、ハードウェアやソフトウェア以外からも構成されていることを明記する • 資産の特定は適切な精細さのレベルで行う ➢ 詳細さのレベルは、リスクアセスメントのときに収集する情報量全体に影響する。レベルは、リスクアセスメントを繰り返す中で練り直すことができる • 各資産について資産のオーナーを特定する ➢ オーナーは資産の所有権を持つとは限らないが、その生産、開発、維持、使用及びセキュリティに関する責任を適宜、保有する (27001 6.1.3 f))のリスク所有者)
アウトプット	• リスクマネジメントの対象となる資産のリスト • 資産に関連する事業・業務プロセスとそれらの関連性のリスト
附属書B:資産の特定及び評価の詳細情報	

8.2.3 脅威の特定

インプット	インシデントレビュー、資産のオーナー、ユーザ及び、外部脅威のカタログを含むその他の情報源から入手した脅威に関する情報
アクション	脅威及びその発生源を特定する
導入の手引	• 偶発的な原因によるものと故意のものの、両方を特定する • 脅威は種類別に (例えば、認可されていない行為、物理的損傷、技術的障害)特定してから、その分類の中で個別の脅威を特定する • 脅威の特定及び起こりやすさの推定のインプット ➢ 資産のオーナー又はユーザ、人事スタッフ、施設管理及び情報セキュリティの専門家、物理的セキュリティの専門家、法務部並びに、法人、気象協会、保険会社及び政府機関を含めたその他の関係する組織など • インシデントで得られた内部経験及び過去の脅威のアセスメントを考慮する • 関連する脅威は絶えず変化していること(事業環境又は情報システムが変化していれば特に)認識する
アウトプット	脅威の種類及び原因を特定した脅威のリスト
附属書C:脅威の種類に関する詳細情報	

8.2.5 脆弱性の特定

インプット	• 既知の脅威のリスト • 資産及び既存の管理策のリスト
アクション	脅威のつけ込む余地があり、資産又は組織に対して危害を及ぼす脆弱性を特定する
導入の手引	• 脆弱性は次の分野において特定することがある ➢ 組織/プロセスと手順/管理の定常業務/要員/物理的環境/情報システム構成/ハードウエア、ソフトウエアまたは通信機器/外部組織への依存度 • 脆弱性はそれにつけ込む脅威が必要であり、脆弱性それ自身では損害を引き起こさない。 • 対応する脅威の無い脆弱性は管理策を必要としないが、変化を監視すること。 • 資産を購入・作成したときに意図された以外の方法または目的で使用する場合に、資産の特性に関連する脆弱性がでてくる可能性がある。資産に内在あるいは外在する異なる源から発生する脆弱性を考慮する必要がある
アウトプット	• 資産、脅威及び管理策に関連する脆弱性のリスト • レビューのために特定された脅威に関係しない脆弱性のリスト
附属書D:脆弱性の例及び脆弱性のアセスメント方法	

ISO/IEC 27005

附属書A: 情報セキュリティリスクマネジメントプロセスの適用範囲及び境界の定義

附属書B: 資産の特定及び評価並びに影響アセスメント

附属書C: 典型的な脅威の例

附属書D: 脆弱性及び脆弱性アセスメントの方法

附属書E: 情報セキュリティリスクアセスメントアプローチ

附属書F: リスクの修正の制約

ISO/IEC 27005 **付属書B**
資産の特定及び評価並びに影響アセスメント

資産の種別

主要資産	• 事業プロセス及び事業活動 • 情報
支援資産	ハードウェア、ソフトウェア、ネットワーク、要員、拠点(サイト)、組織の構成

主要資産の特定

事業プロセス **(又はサブプロセス)**	• その損失又は低下によって、組織の使命達成が不可能となるプロセス • 機密プロセス又は専有技術を伴っているプロセス • 修正された場合、組織の使命の達成に大きく影響するプロセス • 組織が契約、法令又は規制の要求事項を順守するために必要となるプロセス
情報	• 組織の使命又は事業の遂行に不可欠の情報 • プライバシーに関する国内法の観点で、特別に定義するべき個人情報 • 戦略的方向性によって決定される目的の達成に必要となる戦略情報 • 収集、保管、処理及び送信に長時間を要する高コスト情報及び 又は高い取得費用を伴う高コスト情報

ISO/IEC 27005 **付属書B**
資産の特定及び評価並びに影響アセスメント

支援資産の特定

ハードウェア	データ処理装置、可搬形装置、固定装置、周辺装置、データ媒体、電子媒体、その他の媒体
ソフトウェア	オペレーティングシステム(OS)、サービス/保守又は管理用ソフトウェア、パッケージソフトウェア/標準ソフトウェア、ビジネスアプリケーション
ネットワーク	媒体とサポート、受動または能動リレー、通信インタフェース
要員	意思決定者、ユーザ、運用/保守スタッフ、開発者
拠点(サイト)	ロケーション(所在地) • 外部環境、構内、ゾーン、必須サービス、通信、ユーティリティ
組織	当局(Authorities)、組織の構成、プロジェクト又はシステム組織、下請負業者/供給者/製造業者

ISO/IEC 27005 **付属書C** 典型的な脅威の例

代表的な脅威の事例

偶発的…情報資産に偶発的な損害を与える人為的なもの、故意…情報資産を狙った故意によるもの、環境…人為的な行為に基づかない全てのインシデント

種類	脅威	発生源の分類
物理的損傷	火災、水害、汚染、重大事故、機器や媒体の破壊、塵埃・腐食、凍結	偶発的,故意,環境
自然現象	気候現象、地震現象、火山現象、気象現象、洪水	環境
重要なサービスの損失	空調設備・給水設備の故障	偶発的,故意
	電源の喪失	偶発的,故意,環境
	通信設備の故障	偶発的,故意
放射線による妨害	電磁波、熱放射、電磁波パルス	偶発的,故意,環境
情報の漏洩・流出	危険な干渉信号の傍受、遠隔地からのスパイ行為、盗聴、媒体や文書の盗難、機器の盗難、リサイクルまたは廃棄された媒体の回収、ハードウェアの改ざん位置検出	故意
	情報漏洩、信頼できないソースからのデータ、ソフトウェアの改ざん	偶発的,故意
	機器の故障、機器の誤動作、ソフトウェア誤動作	環境

以降略

ISO/IEC 27005 **付属書C** 典型的な脅威の例

人が原因となる脅威の例

脅威の発生源	動機	起きうる結果
ハッカー、クラッカー	チャレンジ、自尊心、反抗、ステータス、金銭	ハッキング、ソーシャルエンジニアリング、システムへの侵入、ブレークイン、システムへの不正アクセス
コンピュータ犯罪者	情報の破壊、違法な情報公開、金銭的な利益、不正なデータ改ざん	コンピュータ犯罪(サイバーストーカーなど)、詐欺行為(例:再生、なりすまし、傍受など)、情報収受、なりすまし、システム侵入
テロリスト	恐喝、破壊、搾取、恨み、政治的利益、メディアへの露出・掲載	爆弾/テロリズム、情報戦、システム攻撃(DoS攻撃など)、システム侵入、システム改ざん
産業スパイ(情報機関、企業、外国政府、その他政府関係者)	競争上の優位性、経済スパイ	防衛上の優位性、政治的な優位性、経済的搾取、情報窃取、個人情報の侵害、ソーシャルエンジニアリング、システム侵入、不正なシステムアクセス(機密情報、専有情報、技術関連情報へのアクセス)
内部者(訓練不足、不満、悪意、過失、不誠実、解雇	好奇心、自尊心、諜報、金銭的な利益、復讐、非意図的な失敗および見落とし(例:データ入力	従業員への暴行、恐喝、個人情報の閲覧、コンピュータの不正使用、詐欺・窃盗、情報の詐取、偽造・変造された日付の入力、傍受、悪質なコード(例:ウイルス、論理爆弾、トロイの木馬など)、人事情報の売買、システムバグ、システ

以降略

ISO/IEC 27005 **付属書D1**
脆弱性及び脆弱性アセスメントの方法

脆弱性と脅威の例示

種類	脆弱性の例	脅威の例
ハードウェア	記憶媒体に関する保守作業不足・設置不良	情報システムの保守に対する違反
	定期的な交換の仕組みの欠如	機器や媒体の破壊
	湿度、埃、汚れに対する感受性	塵埃、腐食、凍結
	電磁波の影響を受けやすい	電磁波
	効率的な設定変更管理の欠如	誤使用
	電圧変動に対する感受性	電源の喪失
	温度変化に対する感受性	気象現象
	保護されていない状態での保管、廃棄時における注意の欠如、廃棄時における注意の欠如、不適切なコピー	媒体や文書の盗難
ソフトウェア	ソフトウェアテストの未実施または不足、ソフトウェアの既知の脆弱性、ワークステーションを離れるときに「ログアウト」忘れ、適切な消去を行わずに記憶媒体の廃棄または再利用、監査証跡の欠如、アクセス権の不適切な割り当て	権利の濫用

ネットワーク
要員
サイト
組織

以降略

Part.3 ① 2022年の各社アンケートから

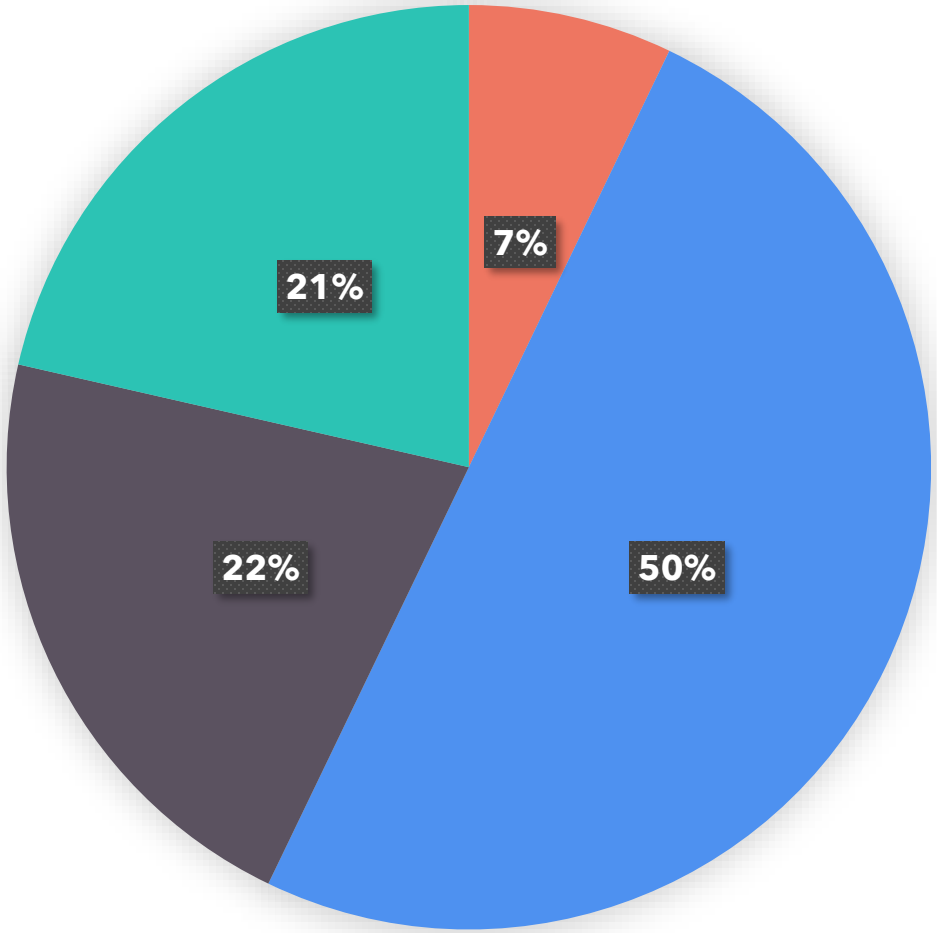
インプリメンテーション研究会参加社各位に、
自組織におけるリスクアセスメントの状況を調査した結果です。

回答組織プロフィール

	A	B	C	D	E	F	G	H	I	J	K	L	M
適用範囲人数	16～25人	876～1,175人	6,801～8,500人	10,701人以上	1,551～2,025人	3,451～4,350人	1,176～1,550人	86～125人	10,701人以上	66～85人	1,176～1,550人	1～10人	10,701人以上
適用範囲サイト数	1サイト	6～10サイト	201サイト以上	201サイト以上	6～10サイト	5サイト	6～10サイト	2サイト	20～50サイト	1サイト	6～10サイト	1サイト	51～100サイト
ISMS認証有無	認証取得	認証取得	認証取得	認証取得	認証取得	認証取得	認証取得	認証取得	認証取得	予定あり	未取得	認証取得	認証取得
認証とって何年目？	1～3年	16～20年	16～20年	16～20年	16～20年	21年以上	16～20年	11～15年	16～20年	-	-	1～3年	16～20年
事務局人数	2人	3人	5人	4人	5人	11～20人	5人	6～10人	5人	4人	11～20人	1人	2人

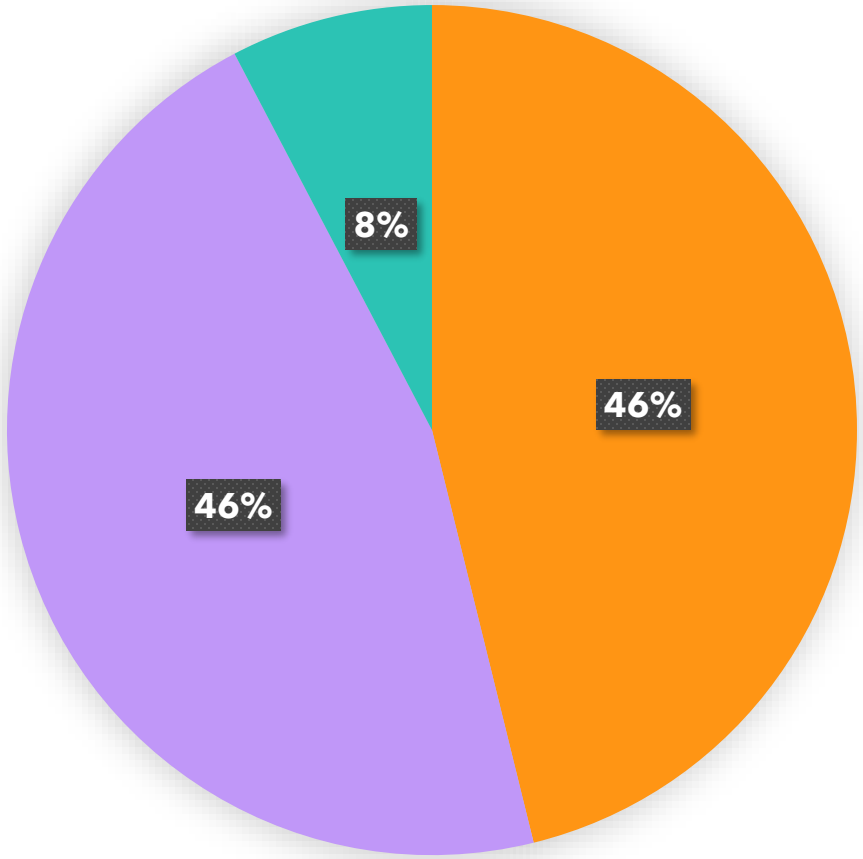
- 回答内容には、2022年現在ではない過去の状況(情報)も含みます。
- 受審組織ではない、コンサルティング業務の方の意見も採用しています。
- 上表「適用範囲人数」の単位は、JISQ27006 付属書B 審査工数 表B.1のテーブルを利用しています。

リスクアセスメントでは、どんな手法を用いているか



「その他の手法」には以下がありました
- 商用サービスツールを利用しており、種別が判然としない
- 部門により手法がバラバラである

ベースラインアプローチ(ギャップ分析)では、どんな基準を用いているか



- JIS Q 27001の付属書A(管理策)
- 自社の情報セキュリティポリシー(規程、ガイドライン等)
- 上記以外、または上記に加えて上記以外の何か

ベースラインアプローチ(ギャップ分析)の例①

注:とある組織の実物を引用しているため、記述内容は必ずしも正解ではありません

ｾｷｭﾘﾃｨ管理策	要求項目	要求事項	確 認	現　状					脆弱性ランク	詳細対策	関連する規程	項番	対策後脆弱性ランク
				関連する社内規程等	該当箇所	分析結果	脆弱性	管理策					
A.6.2.1	モバイル機器の方針	モバイル機器を用いることによって生じるリスクを管理するために，方針及びその方針を支援するセキュリティ対策を採用しなければならない。	端末(ノートPC、タブレット、スマートフォン等)の社外への持ち出す場合の注意事項について定められているか？	アクセス管理規程	8.1	Y	端末の持ち出しルールが定められていない。	規程に定めており、申請はワークフローで行っている。	1				
A.8.1.4	資産の返却	全ての従業員及び外部の利用者は，雇用，契約又は合意の終了時に，自らが所持する組織の資産の全てを返却しなければならない。	すべての従業員及び関係者が退職、配属替え、退会した人に関する資産の返却について定められているか？	人的セキュリティ管理規程	6	Y	資産の返却手順が不明確である。	規程に定めており、退職時の返却物チェックリストにのっとり運用されている。	1				
A.15.1.3	ICT サプライチェーン	供給者との合意には，情報通信技術（ICT）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めなければならない。	第三者と契約を締結にあたって、契約書に盛り込まなければならない事項を明確に定めているか？	情報セキュリティ運営管理規程	8.1	Y	第三者に対するセキュリティ対策が不十分である。	規程に定めており、契約書を交わしている。	1				

管理策に該当する施策が存在するか否かをY/Nで表記

管理策に該当する施策が無かった場合の想定

現状

スライド37参照

ベースラインアプローチ(ギャップ分析)の例②

ISO27001/27017の管理策			設問①(あるべき姿)		設問②(事象発生時の影響と頻度)		
A.6.1.3 (CLS)	関係当局との連絡	クラウドサービスカスタマは、クラウドサービスカスタマ及びクラウドサービスプロバイダが併せて行う操作に関連する関係当局を特定すること。	部門内で利用するクラウドサービスでは、データが物理的に保存されている国が特定されている。	選択	プライバシーポリシー未記載の国に個人情報データを保管し、法令違反となる。	選択	選択
A.11.1.3	オフィス，部屋及び施設のセキュリティ	オフィス，部屋及び施設に対する物理的セキュリティを設計し，適用しなければならない。	執務スペース内では常時、セキュリティカードをロゴマークが見えるよう着用している。		従業員との見分けがつかないため、不審者の入室を許し不正不法行為が発生する。		

a.未実施かつルール未周知
b.周知・認識されているがほぼ未実施
c.未実施が大半であるが、実施して者もいる
d.一部未実施があるが、実施している方が大半である
e.ルールが確実に実施されているはずだが確認までは出来ていない
f.ルールが確実に実施されている事が確認できている
g.該当しない

現状を選択

a.お客様に損害が発生する
b.Speee全体にビジネス面の悪影響が発生する
c.事業部内にビジネス面の悪影響が発生する
d.Speee全体に対応工数が発生するが、ビジネス面の悪影響はない
e.事業部内に対応工数が発生するが、ビジネス面の悪影響はない
f.発生しても対応に工数は全く要しない、影響ゼロ

発生したらどうなる？

a.原因さえあれば何時でも発生する可能性がある
b.毎日1回程度発生する可能性がある
c.週1回程度発生する可能性がある
d.月1回程度発生する可能性がある
e.年1回程度発生する可能性がある
f.数年に1回程度発生する可能性がある
g.該当しない

起こりうる頻度

ベースラインアプローチ(ギャップ分析)の例②

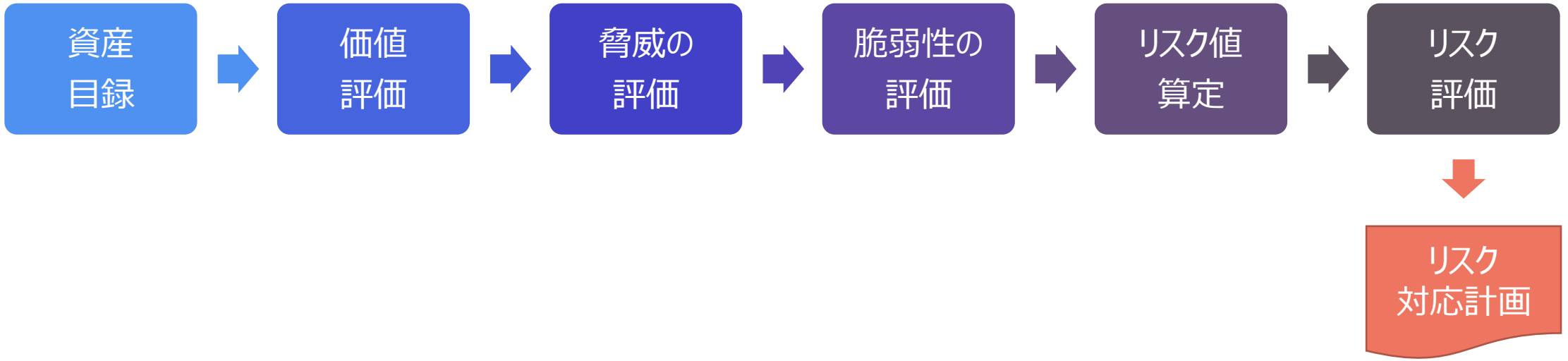
ISO27001/27017の管理策			設問①(あるべき姿)		設問②(事象発生時の影響と頻度)			脆弱性	重要性	発生確率	リスク値
A.6.1.3 (CLS)	関係当局との連絡	クラウドサービスカスタマは、クラウドサービスカスタマ及びクラウドサービスプロバイダが併せて行う操作に関連する関係当局を特定すること。	部門内で利用するクラウドサービスでは、データが物理的に保存されている国が特定されている。	脆弱性	プライバシーポリシー未記載の国に個人情報データを保管し、法令違反となる。	重要性	発生確率	0～3	0～3	0～3	**0～27**
A.11.1.3	オフィス，部屋及び施設のセキュリティ	オフィス，部屋及び施設に対する物理的セキュリティを設計し，適用しなければならない。	執務スペース内では常時、セキュリティカードをロゴマークが見えるよう着用している。		従業員との見分けがつかないため、不審者の入室を許し不正不法行為が発生する。			0～3	0～3	0～3	**0～27**

選択結果に応じた値

リスク値が受容基準を超えた項目に対し、
事務局にてリスク評価及びリスク対応を策定する

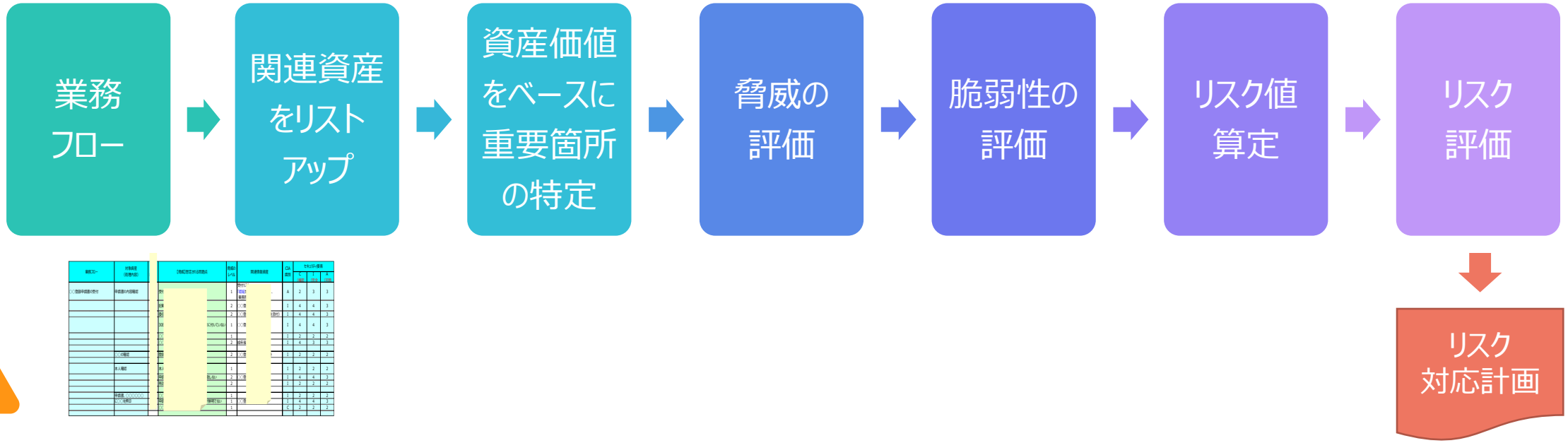
詳細アプローチの手法 例①

JIPDECユーザーズガイドに準じた、資産ベースで詳細リスク分析をするパターンが、アンケート回答では最多でした。



詳細アプローチの手法 例②

業務プロセス分析を起点に、重要箇所で取り扱う資産を対象に詳細分析を行うパターンもありました。



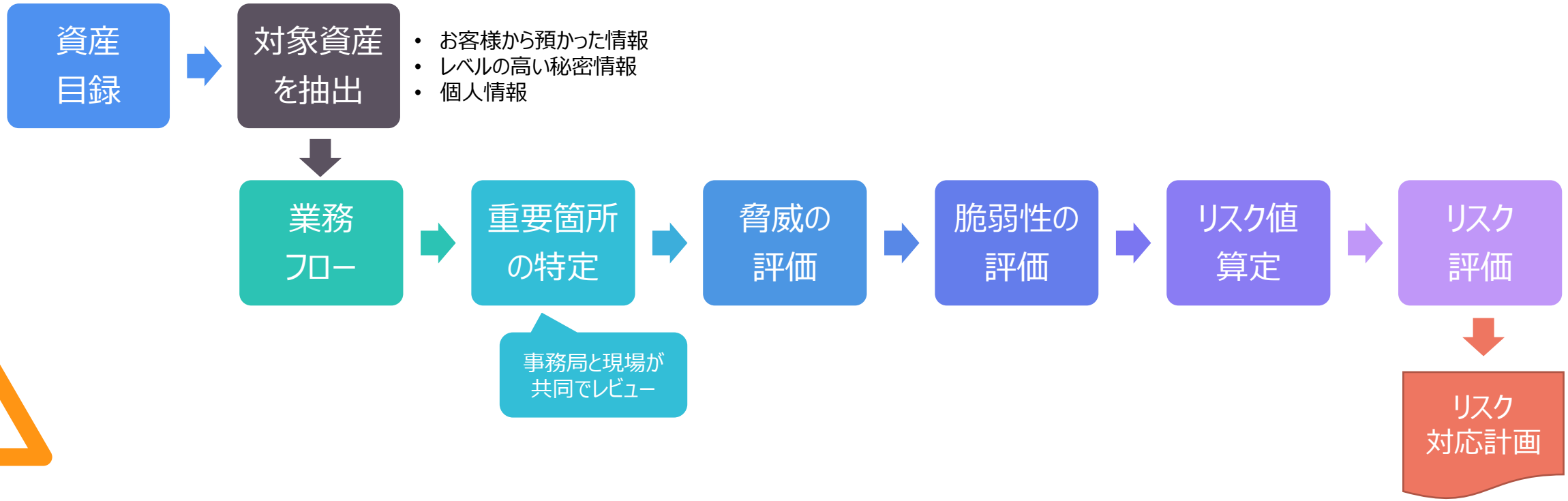
詳細アプローチの手法 例②

業務フローの例

業務フロー	対象資産 （処理内容）		【脅威】想定される問題点	脅威のレベル	関連情報資産	CIA識別	セキュリティ要素		
							C （機密	I （完全	A （可用
○○登録申請書の受付	申請書の内容確認		受付	1	受付リア 「認証 業務用	A	2	3	3
			記載	2	○○登	I	4	4	3
			委任	2	○○登 を添付）	I	4	4	3
			30日 に付いていない	1	○○登	I	4	4	3
			○○	1		I	2	2	2
			○○	2	成年後	I	4	3	3
	○○の確認		登録	2	○○登	I	2	2	2
	本人確認		本人	1		I	2	2	2
			申請 致しない	2	○○登	I	4	4	3
			有効	2		I	2	2	2
	申請書、○○○○○○		○○	1		I	2	2	2
	に○○を押印		申請 が鮮明でない	1	○○登	I	4	4	3
			○○	1		C	2	2	2

詳細アプローチの手法 例③

特定の資産を対象とし、その業務フローをもとに、事務局と現場の合同で詳細分析を行うパターンもありました。



資産価値の計算方法例

(a) 機密性

ランク	レベル	機密性の分類区分
4	極秘	所定の関係者や部署等のみ開示・提供が可能な資産。漏洩した場合、ビジネスに深刻かつ重大な影響がでる。
3	秘密（秘）	特定の関係者や部署等のみ開示・提供が可能な資産。漏洩した場合、ビジネスに影響がでる。
2	社外秘	組織内に開示・提供が可能な資産（社員、及び許可された従業員等のみ使用できる）。
	グループ外秘	組織内およびグループ会社に開示・提供が可能な資産（社員、及び許可された従業員等のみ使用できる）。
1	公開	社外一般にアクセス可能な資産。漏洩した場合に、ほとんどビジネスに影響がないもの。

(b) 完全性

ランク	レベル	完全性の分類区分
3	高	情報の内容を変更された場合、ビジネスに深刻かつ重大な影響がでる。(通常の手段では復旧が不可能で、その間は継続して機会損失が生じる)
2	中	情報の内容を変更された場合、ビジネスに影響がでる。(復旧に6時間以上を要する)
1	低	情報の内容を変更された場合、ビジネスに影響はほとんどない。(バックアップ等から容易に復旧が可能)

(c) 可用性

ランク	レベル	可用性の分類区分
3	高	利用不可能の場合、ビジネスに深刻かつ重大な影響がでるもの。目安として原則24時間365日のシステム稼働を保障する。
2	中	利用不可能の場合、ビジネスに影響がでるもの。目安として1時間程度のシステム停止が許容される。
1	低	利用不可能でもほとんどビジネスに影響がでない。目安として1日程度のシステム停止が許容される。

ISMSユーザーズガイド(JIPDEC)に準じた、このようなパターンでCIAを数値化する方法が多勢でしたが、

- レピュテーション
- 保険の補償範囲
- 遵法

といった観点(評価)を加えている組織もありました。

リスク値の計算方法 例①

ISMSユーザーズガイド(JIPDEC)に準じた、下記のパターンが多勢でした。

脅威の評価基準

ランク	レベル	脅威の分類区分
4	最大	目安として１回/週程度発生する可能性がある。
3	大	目安として１回/月程度発生する可能性がある。
2	中	目安として１回/半年程度発生する可能性がある。
1	小	目安として１回/年程度発生する可能性がある。

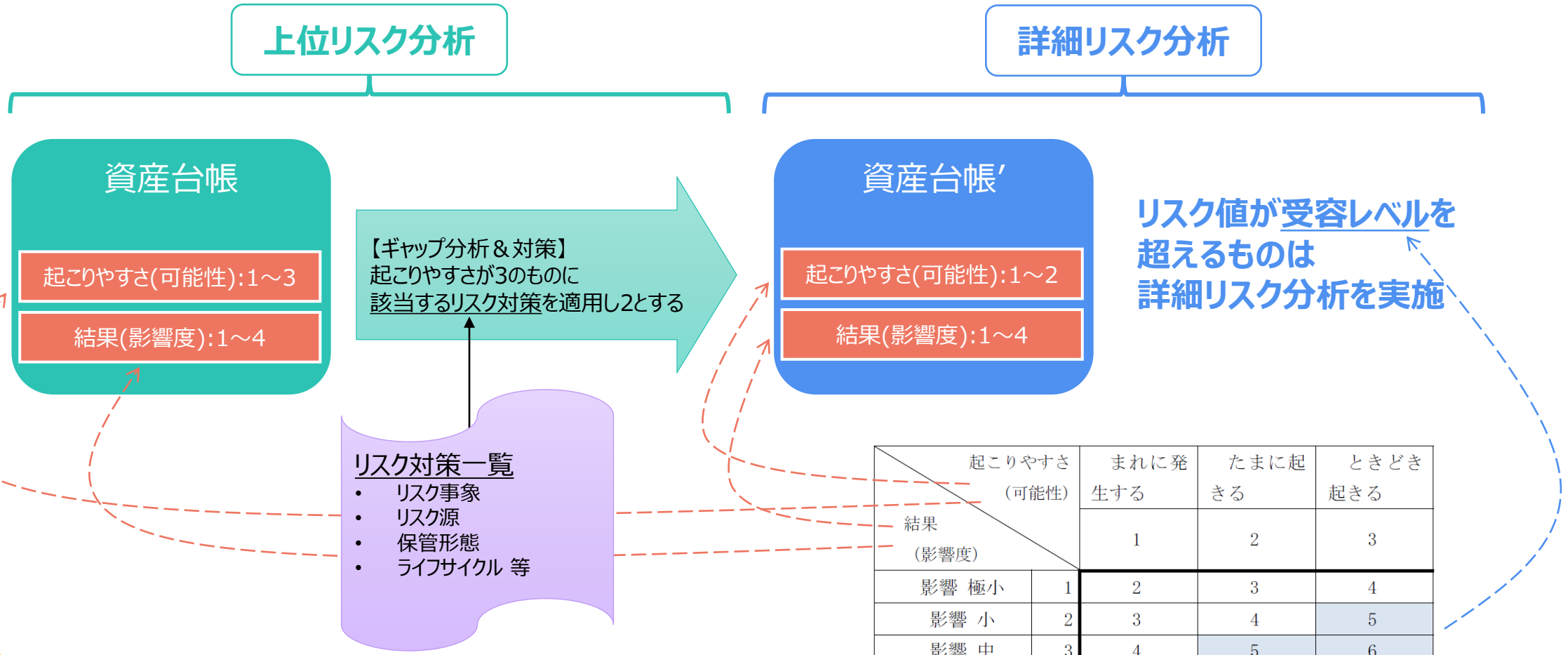
脆弱性の評価基準

ランク	レベル	脆弱性の分類区分
3	高	全く管理策が講じられておらず脆弱である。
2	中	管理策は講じられているものの周知徹底がなされていない又は管理策の追加等により改善の余地がある。
1	低	適切な管理策が講じられており、周知徹底がなされている。
0	なし	**技術的に**適切な管理策が講じられおり、悪用は不可能と考えられる。

表1　リスク値マトリックス

脅威		1				2				3				4			
脆弱性		0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
資産価値	1	0	1	2	3	0	2	4	6	0	3	6	9	0	4	8	12
	2	0	2	4	6	0	4	8	12	0	6	12	18	0	8	12	16
	3	0	3	6	9	0	6	12	18	0	9	18	27	0	12	16	32
	4	0	4	8	12	0	8	16	24	0	12	24	36	0	16	32	48

リスク値の計算方法 例②



結果（影響度） ＼ 起こりやすさ（可能性）		まれに発生する	たまに起きる	ときどき起きる
		1	2	3
影響 極小	1	2	3	4
影響 小	2	3	4	5
影響 中	3	4	5	6
影響 大	4	5	6	7

Part.3 ② 2022年の各社アンケートから

各組織の悩みや思い等をざっくばらんに

自慢・特徴や優れたところ

1	「情報のライフサイクル管理と一体化した資産目録」をExcelからWebで構築し、棚卸にかかる工数が25%軽減された。内部監査対象部門選定時にも活用。組織での「情報を扱う部門と、その内容の特定」が容易になった。
2	個人情報台帳とISMSの資産目録を共通化したツールを導入した。
3	事務局主導から現場サイドにアセスメントの実行主体を移行し、現場サイドのリスク認識向上と事務局コストの低減を実現した。
4	業務フローを元にInput/Outputでのリスクからアセスメントする手法により、業務に密着した判り易い手法を実現出来た。
5	「情報」「システム」に別けて資産の洗い出し・リスクアセスメントを行うように改善し解り易くなったことで、現場側のみでリスクアセスメントが完結できるようになり、事務局の負担が減少した。

改善したいところ、困っているところ、悩んでいるところ、やめたい事など

1	リスクアセスメントの品質を高めるためには実施する担当者の力量のアップや経験値が必要となるため、それを補う形で回答フォーマットを内容ごとにパターン化したり、事例化したりしているが限界はある。
2	経営サイドで「乱暴な判断によるリスク受容が決定」されるため、現場サイトが丁寧なリスクアセスメントを行ってもリスク対応に生かされない。
3	購入したテンプレートのツールを用い、相当工数をかけてリスクアセスメントを行っているが、「それが良いやり方・当社に合ったやり方」なのか判断出来ない。
4	ISMS活動、情報セキュリティ対策自体が、『審査のため、対外的な評価を得るため』に実施されており、現場で直接的な対応者となるISMS委員が「それ以外の仕事が出来ない人」が就く閑職扱いされていること。
5	改善したい・変えたい部分は多々あるが、「手順の変更に伴う工数」が現場・事務局ともに大きい事が想定され、そのデメリットがメリットを凌駕してしまう。

審査のためだけに行っている事
(リスクアセスメントに絡む部分で)

1	リスクアセスメントを含めて「次工程で使われない不要なもの」はすべて排除し、審査のためだけのプロセスを廃止した。
2	資産目録は「審査のために作成・更新する」以外では用途が無い。(リスクアセスメントには用いないため)

今後やりたいこと、やってみたいこと

1	情報資産台帳やプロセス含めた自動化。
2	ローコード開発や、RPAを用いるなど、紙を極力使わない運用管理の実現。
3	EXCELで個人情報台帳や情報資産目録を作成しているが、システム化して情報の見える化、一元管理を実施したい。

Part.4 Before/After事例

インプリメンテーション研究会参加社各位での、
Before/After事例をご紹介します。

得た効果①

a.情報資産計上数が減って、所要工数が激減した
b.情報資産計上漏れが無くなった
c.計上される資産粒度が均質化した
d.事務局問い合わせが激減した

Before

- ✓ 全ての情報資産を棚卸対象としていた
- ✓ 等しくグループ(課)単位で、それぞれが洗い出し作業を実施

After

a. 「共通棚卸資産台帳」を作成して、事務局で一括リスクアセスメントを実施

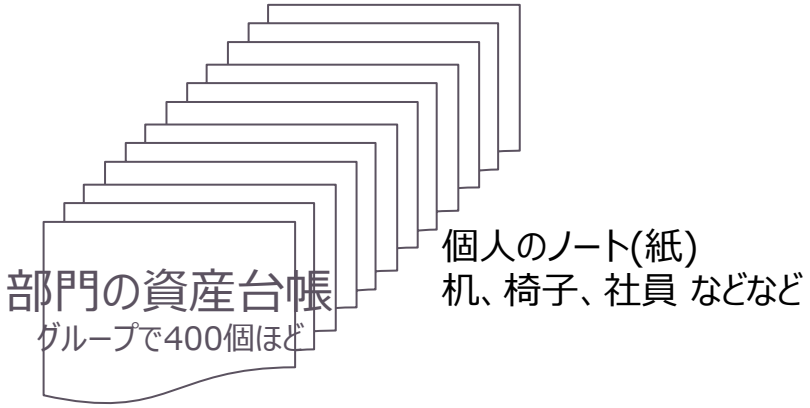
b. 詳細な情報資産計上分類表を作成して、資産計上漏れ防止、資産計上粒度の均質化を図った

c. 除外する情報資産項目の明確化(机・椅子・ファシリティ類)。情報保存が不可能な物は、明確に情報資産の定義から除外した

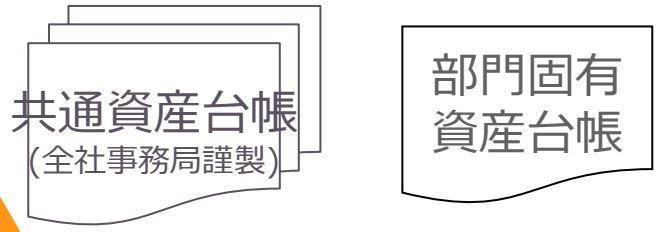
d. いつでも閲覧可能な情報資産台帳作成方法ビデオを作成して全社公開した

得た効果①

a.情報資産計上数が減って、所要工数が激減した
b.情報資産計上漏れが無くなった
c.計上される資産粒度が均質化した
d.事務局問い合わせが激減した



7～8割削減！



- 物理的な情報資産については、共通資産台帳だけでカバーできるかも
- 現場担当者しか認識できないような情報資産は、業務プロセス図を作成し、そこからリストアップするのが望ましい姿なのでは

課題

- 部門特有の特性に依る情報資産のリストアップが、以前より損なわれている部分がある

得た効果②

a.情報資産目録並びにリスクアセスメント策定レビュー工数の削減
b.業務に密着させることで、部門全体での活動となった

Before

- ✓ 部門ごとに情報資産を洗い出し、それらをグルーピングしてリスクアセスメント
- ✓ 資産のバラつき、ダブり、リスクアセスメント工数の増大があった

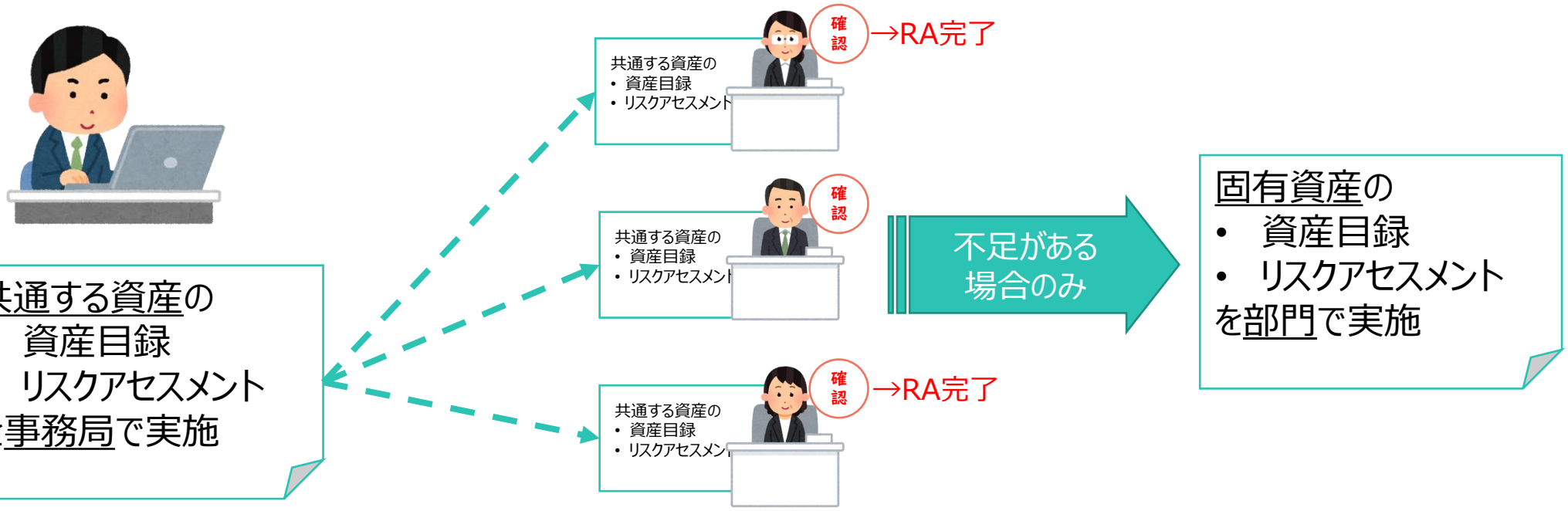
After

a. 共通的な資産は予め事務局で抽出しリスクアセスメントを実施。
各部門でその結果を確認した上で、(不足分の)部門固有の資産目録を作成しリスクアセスメントを実施した

b. 業務フローに基づくリスクアセスメントを併用して、より業務に近づけることを行ない、全員参加を目指した

得た効果②

a.情報資産目録並びにリスクアセスメント策定レビュー工数の削減
b.業務に密着させることで、部門全体での活動となった



ほとんどの部門が共通資産については確認で終わるため、工数が削減

得た効果③

a.組織としてリスクアセスメントを実施したことで組織内でリスク認識が共有され、
　リスク対策に主体的な取り組むようになった
b.部課長それぞれでリスクアセスメントが不要となり、負担が軽減された

Before

- ✓ 事務局が制定したリスク項目について、そのリスク項目に関係する部課長個人にリスクアセスメントを依頼
- ✓ １つのリスク項目に対して、多様な視点のリスクアセスメント結果が得られ、事務局は、それらを集計して総合的にリスクアセスメントを実施

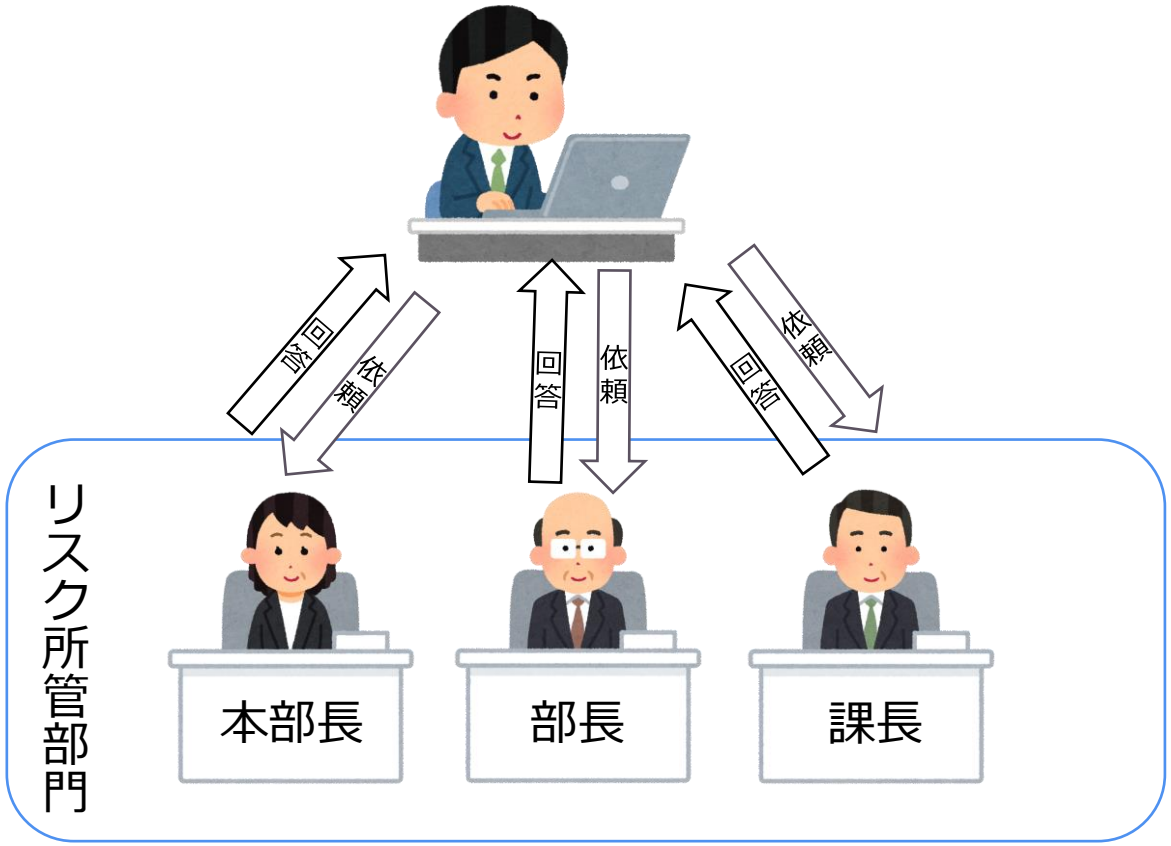
After

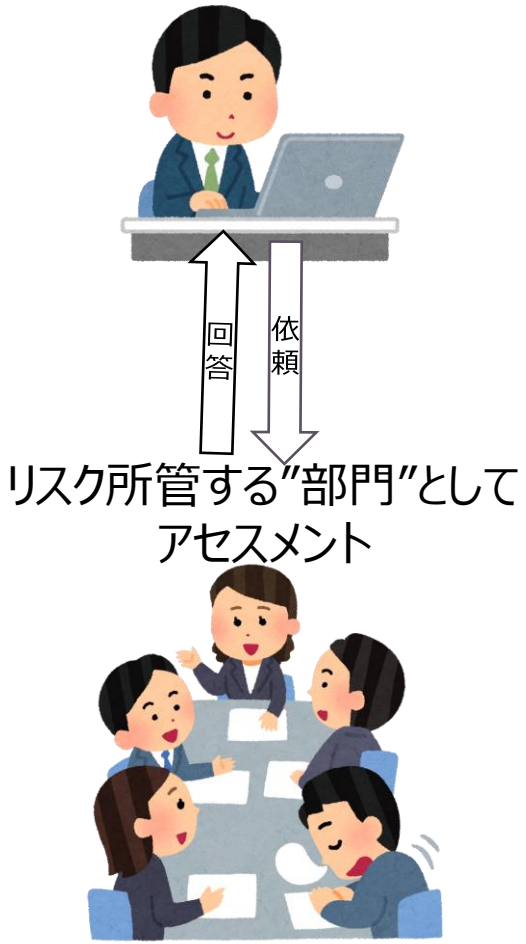
a. 事務局が制定したリスク項目について、そのリスク項目に関係する部門が主体となってリスクアセスメントを実施するように変更した

b. 「部門」としてリスクアセスメントを実施し、個人の見解ではなく部門の意思決定事項として実施

得た効果③

a.組織としてリスクアセスメントを実施したことで組織内でリスク認識が共有され、
　リスク対策に主体的な取り組むようになった
b.部課長それぞれでリスクアセスメントが不要となり、負担が軽減された





得た効果④

これまで固定化されやすかった重点リスク項目が年度毎の状況に応じて変わり、会社の運営方針と適合しやすくなった

Before

- ✓ リスク値の計算結果の高いリスク項目の上位を機械的に重点リスク項目として管理していた
- ✓ 毎年基本的に同じ項目が高リスク値となり、上位が固定化
  新たなリスク項目が生じてもリスク値が相対的に低いため、要対策リスクに選出されない

After

- リスク値の計算結果の高いリスク項目の上位の中から、定性的な観点も加味して選定して管理するように変更した

得た効果④

これまで固定化されやすかった重点リスク項目が年度毎の状況に応じて変わり、会社の運営方針と適合しやすくなった

「定性的な観点も加味して選定して管理する」とは

1. 先ずいったん、定量的にリスクを評点(例:スライド37)する
2. 協議にて、リスクオーナーのリスク認識と評点とをチューニング
3. 以下を特殊事項として特定
   - 例外的な条件により評点が高いもの
   - 対策や目標設定に馴染まないもの
4. 以上を踏まえた上で、経営層の意向や既存の取り組みを加味し、重点リスクを選定

得た効果⑤

a.部門間で授受している情報の不一致が解消された
b.各部門で情報資産の取り扱い方法に応じたリスクアセスメントの実施ができた
c.同一の情報資産でも部門ごとに適切な管理が実施できるようになった

Before

- ✓ 部門ごとに資産台帳を作成しリスク分析を実施しており、同じ情報資産でも資産価値にばらつきが発生
- ✓ 情報媒体の移動についてのリスク分析が甘かった
  (移動方法:通信、郵便等の配達、担当者による持参、車、公共交通機関、データ記憶媒体:紙、CD等の媒体、USB等可搬メモリ、PC)
- ✓ 「原本、複写、配布の管理」の意識が薄く、部門ごとに管理方法がまちまちで管理が不十分
- ✓ 顧客ごとの要求事項を考慮した資産価値分析ができていなかった

After

a. 部門間を跨る業務フロー図を作成し、情報資産、形態、移動手段を記述関連付けして記載

b. 資産台帳の記載精度が向上、保管部門での取り扱い状況に応じたリスク分析が実施できた

c. 情報資産としての管理が、自社規定 or 顧客要求かを明記することで、部門ごとの管理策の基準が明確化した

得た効果⑥

情報資産のライフサイクルに応じた、CIAおよびリスクが特定できるようになった

Before

- ✓ 部門ごとに台帳に資産名を書かせ、それぞれに資産価値(CIA)を判定していた
- ✓ CIAに対応した管理策の選択肢がないこと、資産価値の判定者と管理策の実施者が異なること等からCIAの結果と管理策に因果関係はなかった
- ✓ 情報資産台帳は、情報セキュリティマネジメントのためには利用されず、専ら監査資料として作成されていた。

After

- 部門ごと＆業務名ごとに、情報の作成・取得から削除・廃棄までの情報のライフサイクルに渡るワークフロー図を作成した
  その結果、情報資産のCIAが、取扱う業務や情報のライフサイクルによって異なることが認識出来るようになった

さいごに

今回は、研究会各社でのリスクアセスメントの状況を紹介いたしました。

それぞれの組織で置かれた条件や状況のもと、創意工夫で効率化を目指したり実現している姿を知る事が出来ました。

ここでお伝えした情報が皆さんのISMS活動の助けになれば、本テーマの目的を達成でき本望です。

ご覧いただき
ありがとう
ございました