〇〇〇　様

情報セキュリティ
リスクマネジメントのご提案

株 式 会 社 Ｔ Ｎ Ｔ ソ リ ュ ー シ ョ ン

2025年〇月〇日

目次

目次

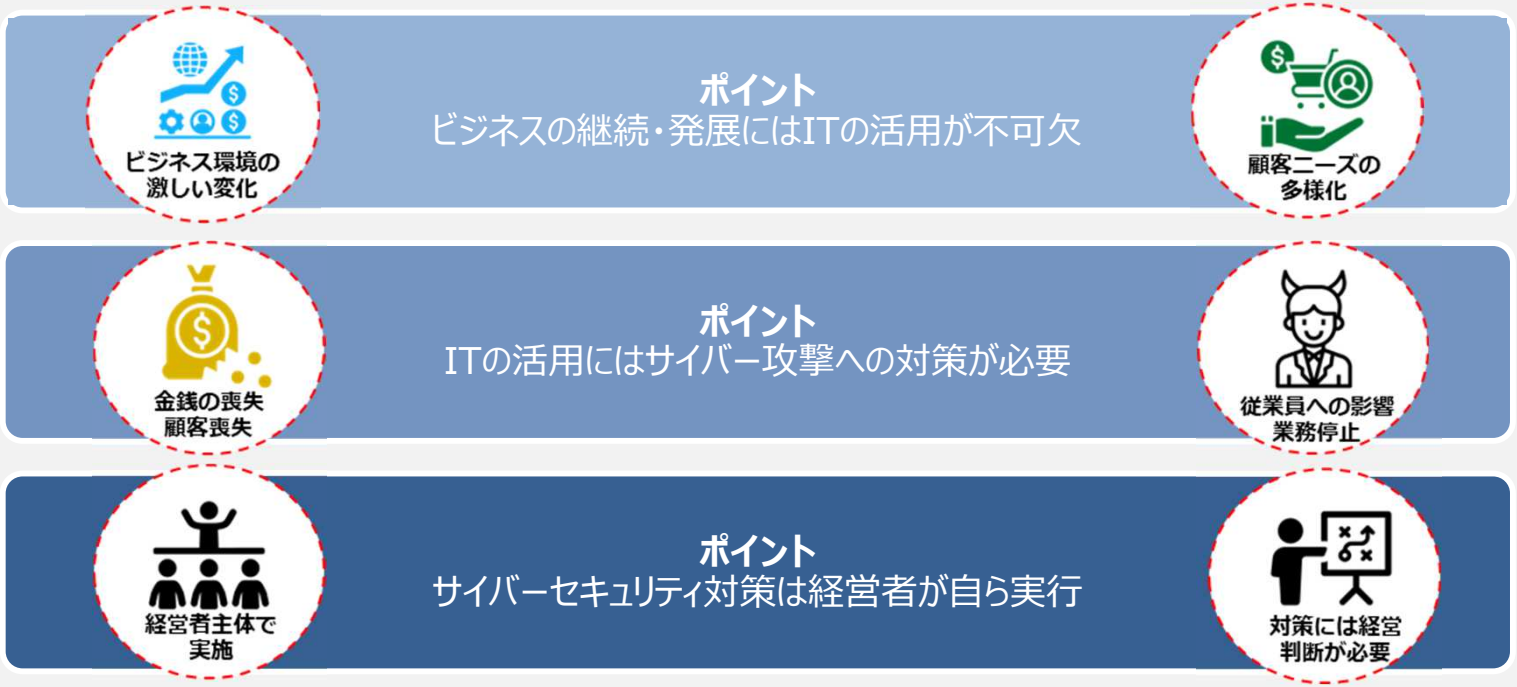
リスクマネジメントとは？

リスクマネジメントとは、組織が保有する情報を脅威から守るために体系的な管理や運用を行うことです。
組織全体で統一された基準に基づき、機密性・完全性・可用性をバランスよく保ちながら情報を管理・運用することがポイントです。
メリットとしましては
1. 情報漏洩などの情報セキュリティリスクを低減することができます。
2. 漏れなく組織全体のセキュリティを効率的に高めることで
   様々なリスクの防止やリスク発生時においても高い事業継続性を
   維持し、強い企業経営ができます。
3. 対外的に企業の信頼性を高めることができます。
4. 費用対効果を考慮した最適なIT投資をすることができ、無駄なIT投資
   を回避できます。

目次

リスクマネジメントの重要性

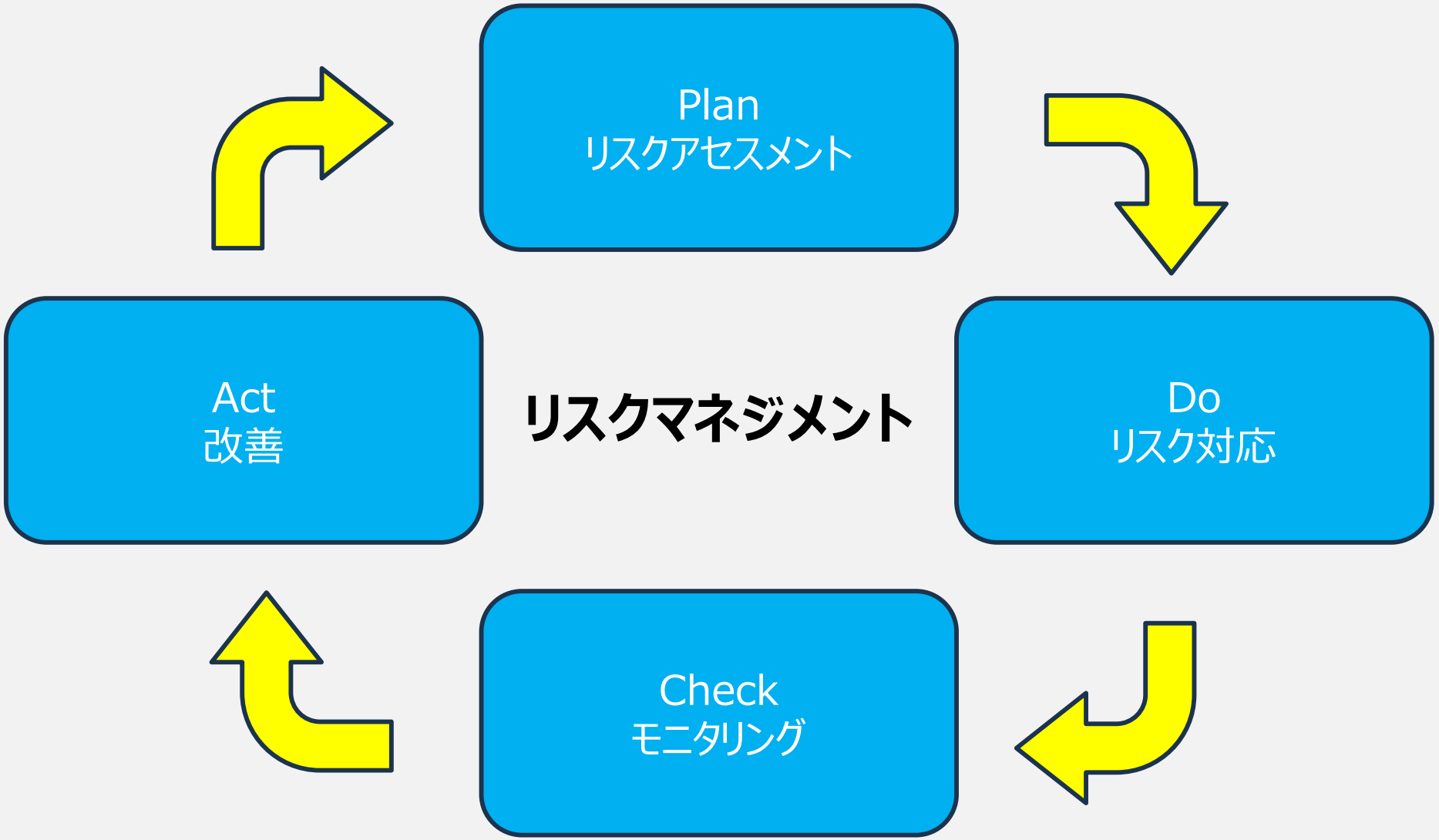
経営者が重要視すべき3つのポイント



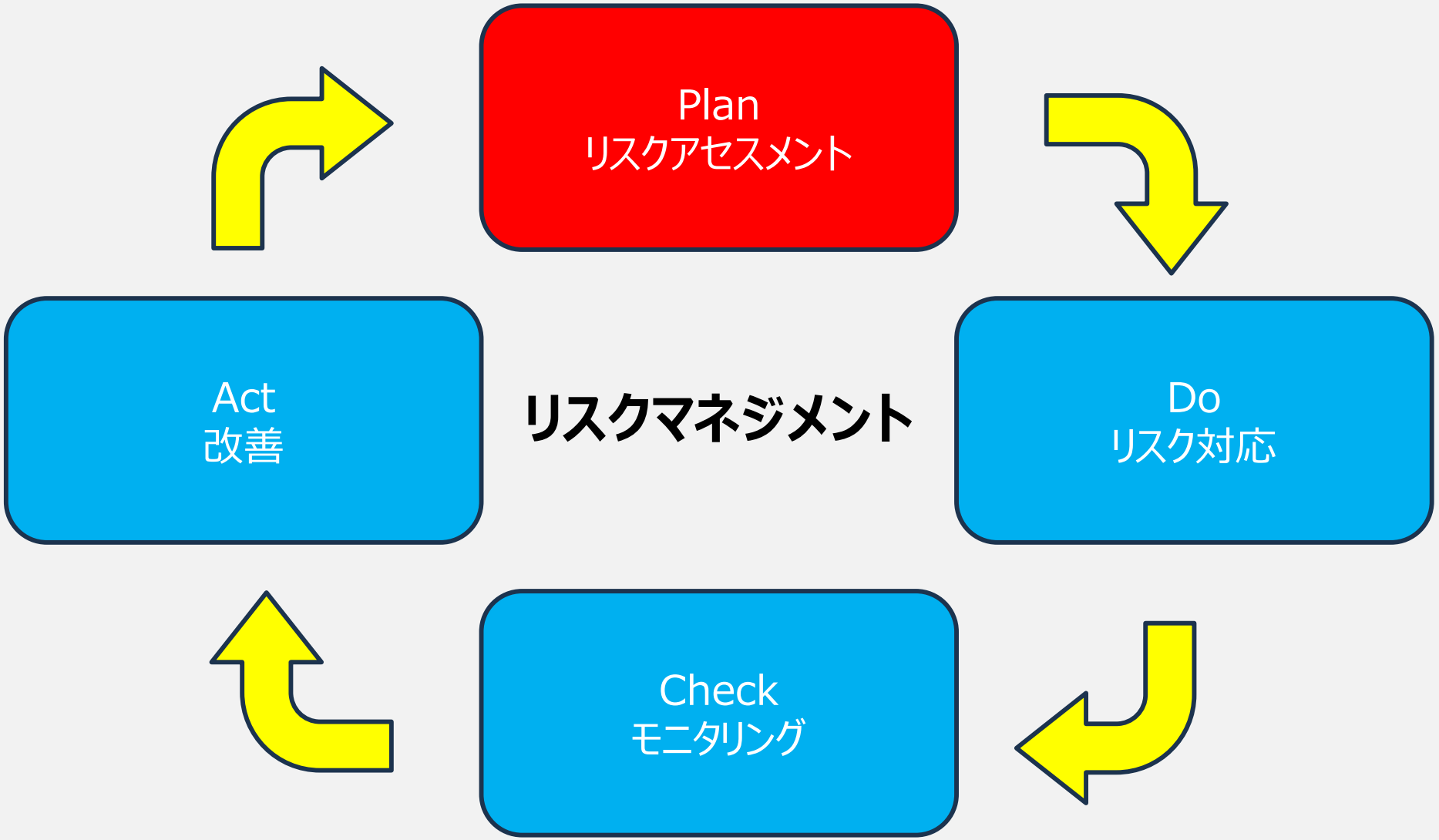
ITの活用とサイバーセキュリティ対策の関係性
（出典） 東京都産業労働局「MISSION 3-1 サイバーセキュリティ対策が経営に与える重大な影響」

目次

リスクマネジメントの流れ



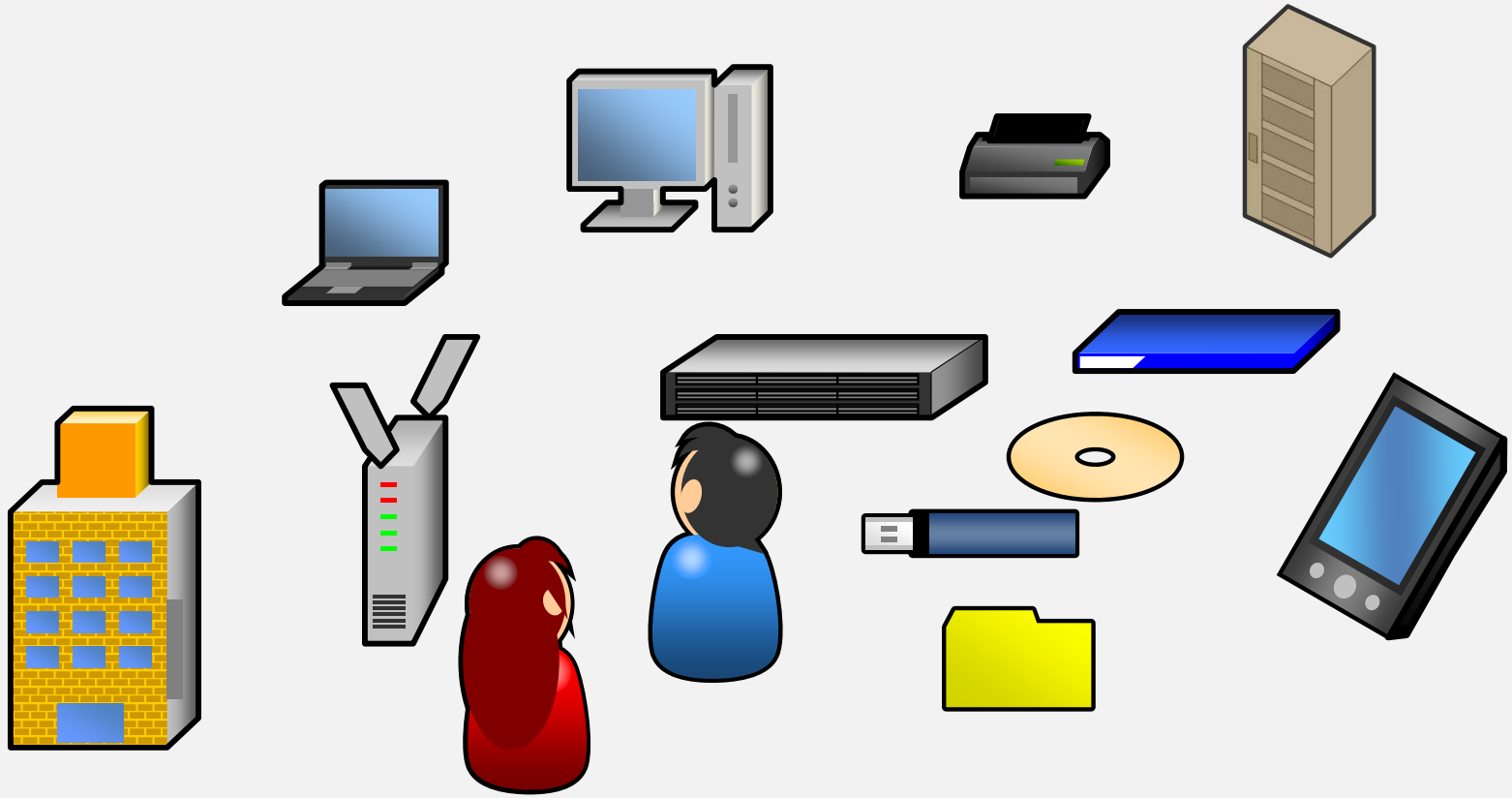
リスクマネジメントの流れ



目次

リスクアセスメントとは？

リスクアセスメントとは、企業や組織が保有する情報資産に潜むリスクを特定・分析・評価し、組織における情報セキュリティリスクの対応策を決めるプロセスです。
具体的には、特定されたリスクを分析して重大性を評価し、対処すべきかどうかを判断する作業のことです。



目次

リスクアセスメントの流れ

目次

情報資産の洗い出し

情報資産＝組織や企業が保有する情報やデータ、それに関連する資源。

情報資産の種類	内容
物理的資産	通信装置やコンピュータ、ハードディスクなどの記録媒体など
ソフトウエア資産	業務やシステムのソフトウエア、開発ツールなど
人的資産	経験や技能、資格など
無形資産	組織のイメージ、評判など
サービス資産	一般ユーティリティ(電源や空調、照明)、通信サービス、計算処理サービスなど
直接的情報資産	データベースやファイル、文書記録など

情報資産の洗い出し

どのような情報資産があるか洗い出して重要度を判断する

例えば、、、
仕訳帳
総勘定元帳
現金出納帳
売上帳

→ 情報資産名称「会計データ」
媒体・保存先「クラウド上のサーバ」

- 情報資産管理台帳の作成
- 情報資産ごとの機密性・完全性・可用性の評価
- 機密性・完全性・可用性の評価値から重要度を算定

情報資産管理台帳

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値			重要度	保存期限	登録日	現状から想定されるリスク（入力不要・自動表示）		
						個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性				脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性 ※「対策状況チェック」シートに入力すると表示	
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			2	0	0	2		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2
人事	社員名簿	社員基本情報	人事部	人事部	書類	有			2	2	2	2		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	書類		有		2	2	1	2	5年	2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	事務所PC			有	2	2	1	2	7年	2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施して	2
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	総務部	書類				1	1	1	1		2016/7/1	2:特定の状況で脅		1
経理	発行済請求書控	当社発行の請求書の控え（過去3年分）	総務部	総務部	書類				1	1	1	1		2016/7/1	2:特定の状		
共通	電子メールデータ	重要度は混在のため最高値で評価	担当者	総務部	事務所PC	有			2	2	2	2		2016/7/1	3:通常の状態		2
共通	電子メールデータ	Gmailに転送	担当者	総務部	社外サーバー	有			2	2	2	2		2016/7/1	3:通常の状態で脅威	実施して	2

パソコンで見ているこのデータはどこに保存されているんだろう？

目次

リスク算定(リスク値)

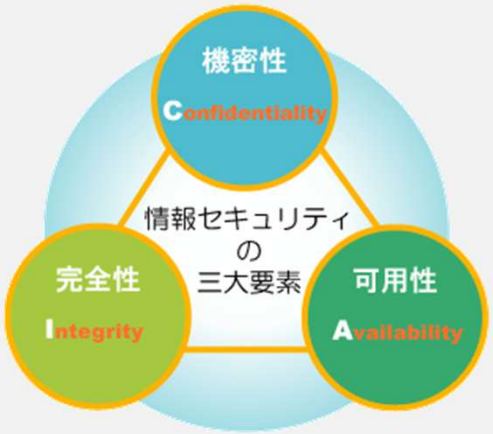
リスク値は重要度と被害発生可能性から算定する

リスク値＝重要度×被害発生可能性

リスク値の大きいものから対策を検討する

リスク算定(重要度)

重要度は機密性、完全性、可用性いずれかの最大値で算定する



重要性の評価値	内容
機密性	アクセスを許可された者だけが情報にアクセスできる。 **漏洩すると事業にどれくらい影響があるか？を評価**
完全性	情報や情報の処理方法が正確で完全である。 **改ざんされると事業にどれくらい影響があるか？を評価**
可用性	許可された者が必要な時に情報資産にアクセスできる。 **利用できなくなると事業にどれくらい影響があるか？を評価**

リスク算定(被害発生可能性)

被害発生可能性は脅威と脆弱性から算定する

被害発生可能性の評価値	内容
脅威	媒体や保存先に対する想定される典型的な脅威の発生頻度を把握して、**起こりやすさを評価**
脆弱性	様々な情報セキュリティ対策に対する実施状況を把握して、**つけこみやすさを評価**

目次

情報セキュリティ対策の検討

リスク対応の考え方

リスク対応の考え方	内容
物理的対策	入退室管理や物理区画の適切化、情報資産の適切な保護といった**物理的なセキュリティを確保する対策**。
人的対策	権限の適切な分配、従業員教育や規程、手順書によるルール化などにより、**人的リスクを低減することでセキュリティを確保する対策**。 管理的セキュリティと呼ばれることもある。 不正行為は内部関係者によって行われることが多い為、それを防ぐ対策が必要。
技術的対策	暗号化、認証、アクセス制御などの**技術的な手段でセキュリティを確保する対策**。 攻撃を防いで内部に侵入させない為の入口対策と侵入された後にその被害を拡大や外部に広げない為の出口対策がある。また、複数の対策を組み合わせる多層防御もある。

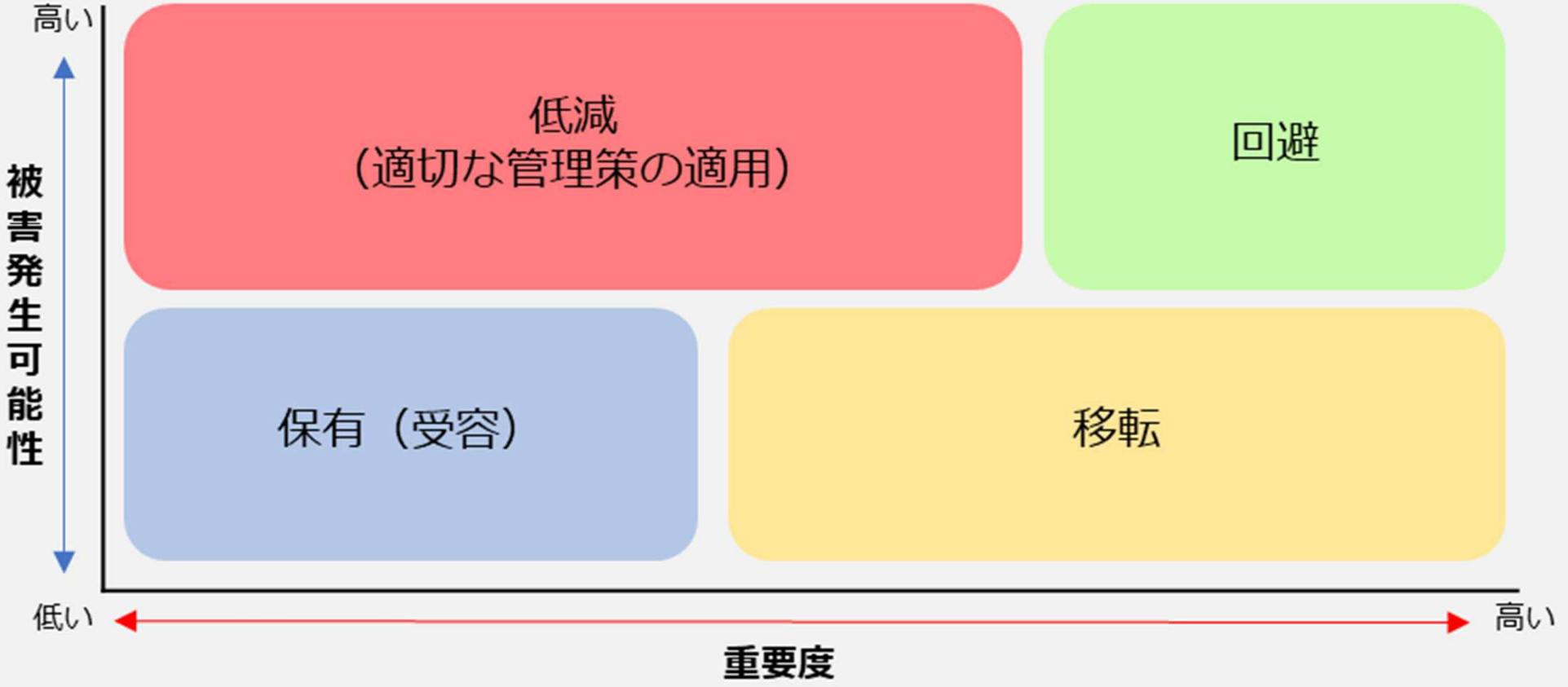
情報セキュリティ対策の検討

リスク対応方法の種類

リスク対応方法の種類	内容	対応例
低減する	脆弱性に対して情報セキュリティ対策を講じることにより、**脅威の発生可能性を下げる**	マルウエア対策ソフトを導入する、外部記憶媒体の接続を制限する等
保有する	リスクが事業に与える影響が小さい、あるいは対策にかかる費用が損害額を上回る場合などは**対策を講じず、許容範囲内として現状を維持**する	対策を講じない(残留リスク)
回避する	脅威発生の要因を停止、あるいは全く別の方法に変更することで**リスクが発生する可能性を取り去る**	外部からの不正アクセスという脅威に対し、機密情報が保存されているサーバは外部接続を行わない等
移転する	自社よりも有効な対策を行っている、あるいは補償能力がある他社のサービスを利用することで**自社の負担を下げる**	社内サーバをセキュリティ対策の充実した外部クラウドサービスに移行する、情報セキュリティに関連した保険商品に加入する等

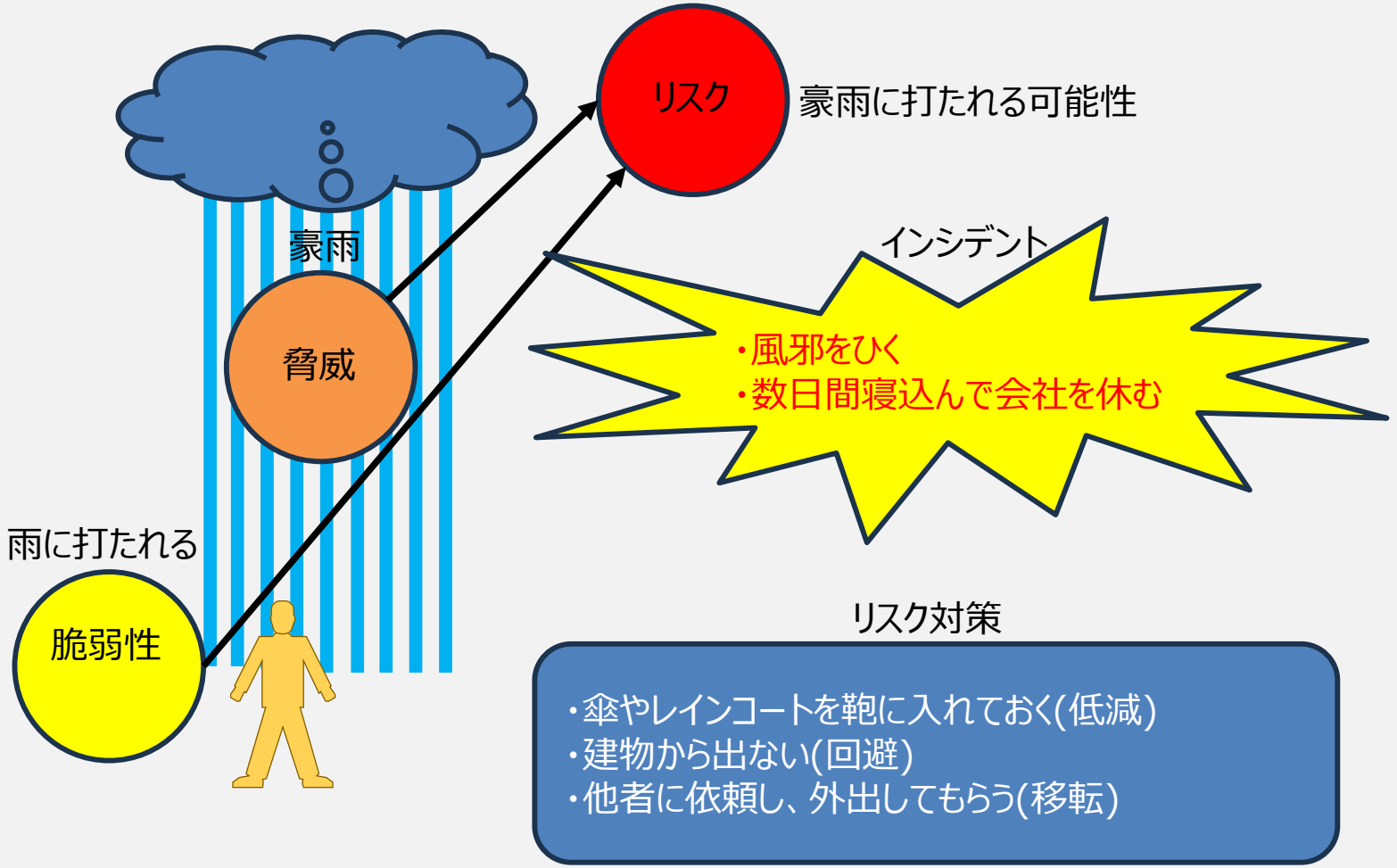
情報セキュリティ対策の検討

リスク対応方法の考え方



情報セキュリティ対策の検討

リスク対応の例(生活)



情報セキュリティ対策の検討

リスク対応の例(情報セキュリティ)

項目	内容
リスクの内容	公開Webサーバが不正アクセスで改ざんされたり、ウイルスを仕掛けられると顧客や閲覧者に被害が発生し、信用を失う。
リスク対応	リスクを低減する。
対策	・アクセス権限の最小化 ・パスワードの複雑化と定期的に変更する運用 ・多要素認証の導入 ・WAF(Web Application Firewall)の導入
対策基準の策定	技術的対策 ・公開サーバへの不正アクセス対策 ・公開サーバへのアクセス権の最小化と管理の強化

情報セキュリティ対策の検討

情報セキュリティ関連規程の例

名称	概要
組織的対策	情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定めます。
人的対策	取締役及び従業員の責務や教育、人材育成などのルールを定めます。
情報資産管理	情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。
アクセス制御及び認証	情報資産に対するアクセス制御方針や認証のルールを定めます。
物理的対策	セキュリティを保つべきオフィス、部屋及び施設などの領域設定や領域内での注意事項などのルールを定めます。
IT機器利用	IT機器やソフトウェアの利用などのルールを定めます。
IT基盤運用管理	サーバーやネットワーク等のITインフラに関するルールを定めます。
システム開発及び保守	独自に開発及び保守を行う情報システムに関するルールを定めます。
委託管理	業務委託にあたっての選定や契約、評価のルールを定めます。委託先チェックリストのサンプルが付属します。
情報セキュリティインシデント対応及び事業継続管理	情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。
テレワークにおける対策	テレワークのセキュリティ対策についてルールを定めます。

目次

マススケジュール


2025/〇
2025/〇
2025/〇
2025/〇
2025/〇
2023/〇
情報資産の洗い出し
リスク算定
情報セキュリティ対策
の検討
セキュリティ対策の実施