Japan Information Security
Management Systems User Group

リスクアセスメントについて考える

～ リスクアセスメントについて振り返る ～

JNSA 標準化部会
日本ISMSユーザグループ　リーダー
インプリメンテーション研究会　主査

2024年12月 6日

魚脇　雅晴

（NTTコミュニケーションズ株式会社）

日本ISMSユーザグループの活動紹介

標準化動向

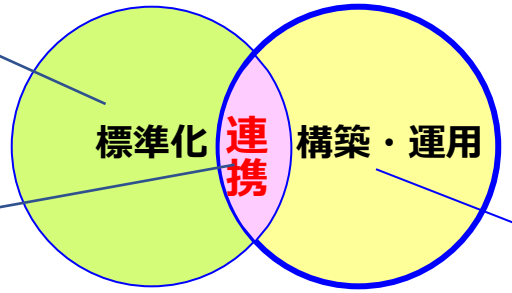
標準化の活用＆定着

ISMSの普及・促進

情報セキュリティセミナー

標準化動向の情報発信

貢献



リエゾン参加

SC 27/WG1 小委員会
アドホック会議

インプリメンテーション研究会

ISMSの構築・運用におけるベストプラクティクスを検討＆提供

標準化されたものをどのようにビジネスの世界に反映＆定着させるか・・・

インプリメンテーション研究会の活動紹介

2006年～　　現在

ISMSの構築・運用におけるベストプラクティスを検討＆提供

【過去のテーマ名】

2023年	■ JISQ27001:2023の新規管理策の実装方法についての考察 ■「ISMS内部監査」どうやってますか?
2022年	■最新の環境の変化に対応したISMSのスコープの再定義について ■続・効率的リスクアセスメント
2021年	■ISMSとゼロトラストセキュリティについての考察 ■ISMS要求事項の解釈と運用の実態（箇条4について）
2020年	■実践かつ効果的なセキュリティ教育 ■規格の解釈（ISO/IEC27002の改定）に伴う対応についての取り組み
2019年	■最新の環境変化に伴うISMSの実装検討 ■各社の事例から学ぶISMSの実装について
2018年	■ISMS規格要求事項から紐解く最新の　ビジネス環境リスク ■働き方改革における情報セキュリティ
2017年	■現場と連携したリスクアセスメント手法の実践活用 ■内部監査を有効に運用するための手法の考察
2016年	■サイバー攻撃を事例としたリスクマネジメントの実践 ■運用フェーズにおける有効性の評価

2015年以前は省略

2024年

■リスクアセスメントについて考える（講演4）

■委託先管理、どうやってますか?（講演5）

：本日の発表テーマ

LT（ライトニングトーク）形式勉強会

- 13個のISMS認証を一年で1個にした話
- NIST OSCALが切り開く、ISMSと情報セキュリティの未来

本テーマの狙い

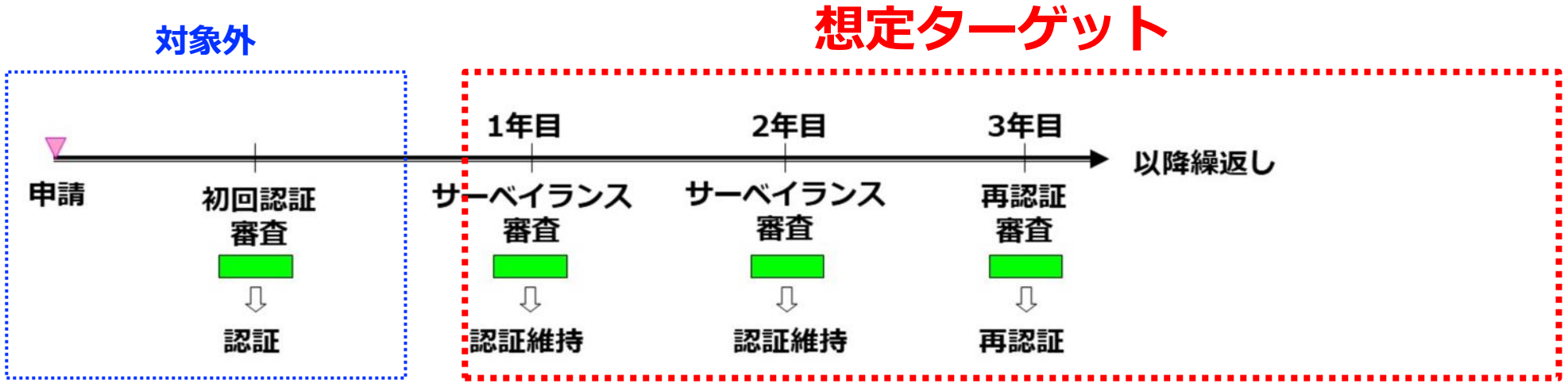
　これまでにいろんな方法によるアプローチが行われ、試行錯誤されてきたリスクアセスメントですが、こうすれば大丈夫という特効薬は残念ながらありません。
そこでリスクアセスメントに対して**どのように取り組めば良いか振り返ることで改善のための気づきに繋がる機会**になればと考えて下記のようなサブテーマを設定して深掘りしました。
取り組みの最終目標として**事務局だけが頑張る構図ではなくリスクオーナーと一緒に取り組む組織全体での取り組み**を夢見ています。

①誰でも理解出来るリスクアセスメントの一般事例

②サイバー攻撃や委託先管理における具体事例紹介

③リスクアセスメントのトリガーやリスクコミュニケーションなど

今回のテーマのターゲット層について



- ISMSの運用プロセス（リスクアセスメント）が自組織として確立していて、実践している
- 最善なやり方が無いか自問自答している

https://www.jipdec.or.jp/project/smpo/ninsyou.html

本日の説明の流れ

誰でも理解出来る

リスクについて知る（一般論）

管理策Ａ：柵による保護
管理策Ｂ：群から離れないよう制御

羊と狼の事例

具体的な事例から学ぶ

ユースケースからリスクアセスメントについて学ぶ

事例1：サイバー攻撃
事例2：委託先からの情報漏洩

実践事例の提案

その１：リスクアセスメント実施のトリガーの明確化

その２：マネージメント層とのリスクコミュニケーション

リスクアセスメントについて考える

誰でも理解出来る

リスクについて知る（一般論）

管理策Ａ：柵による保護
管理策Ｂ：群から離れないよう制御

羊と狼の事例

具体的な事例から学ぶ

ユースケースからリスクアセスメントについて学ぶ

事例1：サイバー攻撃
事例2：委託先からの情報漏洩

実践事例の提案

その１：リスクアセスメント実施のトリガーの明確化

その２：マネージメント層とのリスクコミュニケーション

リスクの概念

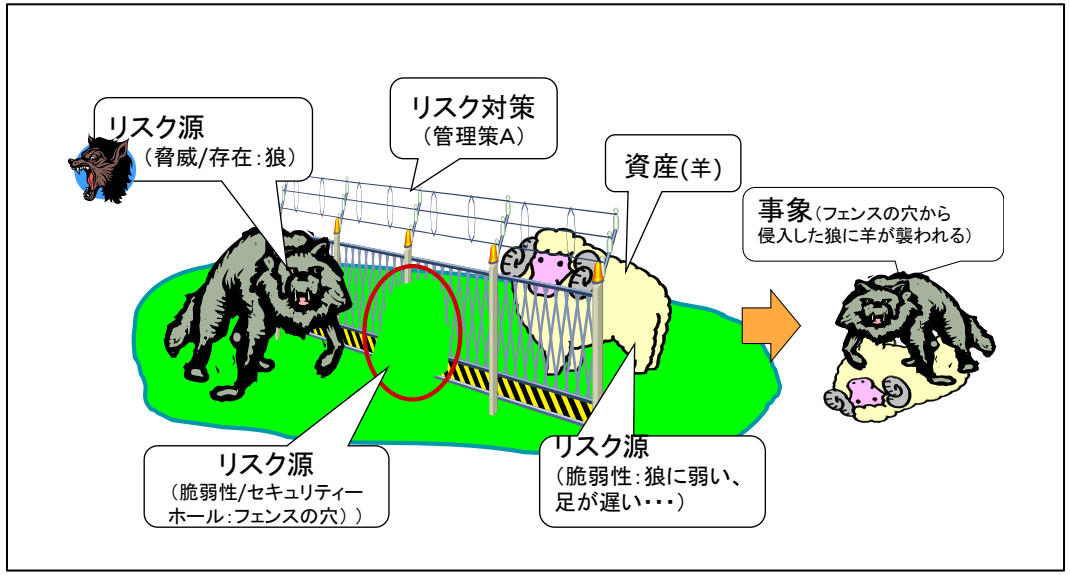
リスクについて考える

リスク(risk)の定義

目的に対する不確かさの影響
(effect of uncertainty on objectives)

ISO/IEC27000 用語・・・引用先

狼と羊を例にリスクについて考える



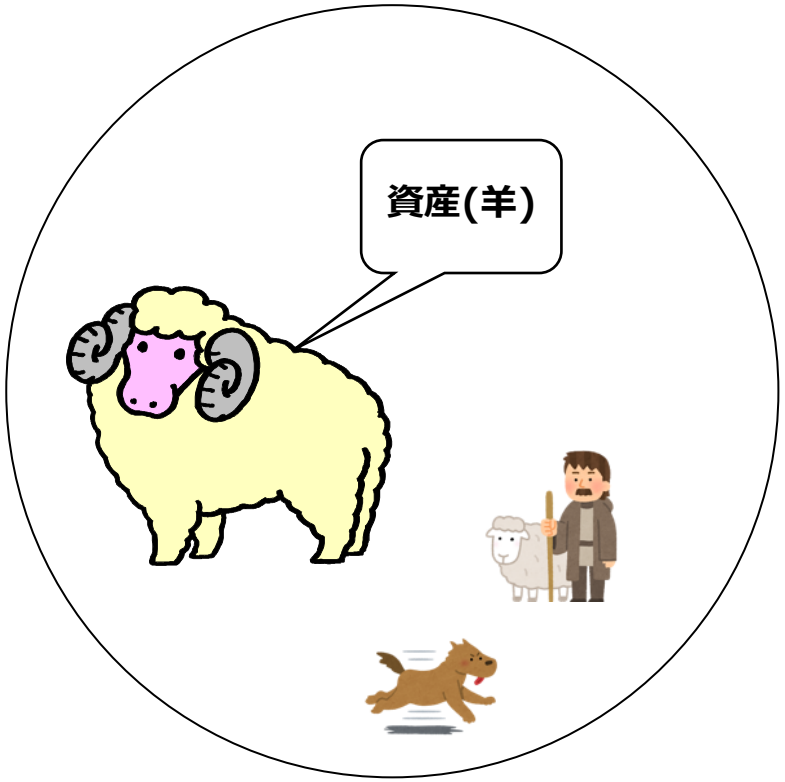
概念ではなく事例で紐解く

ユースケースに基づきリスクについて考える

牧場で羊を飼って羊毛等を販売しているビジネスを題材

攻める側

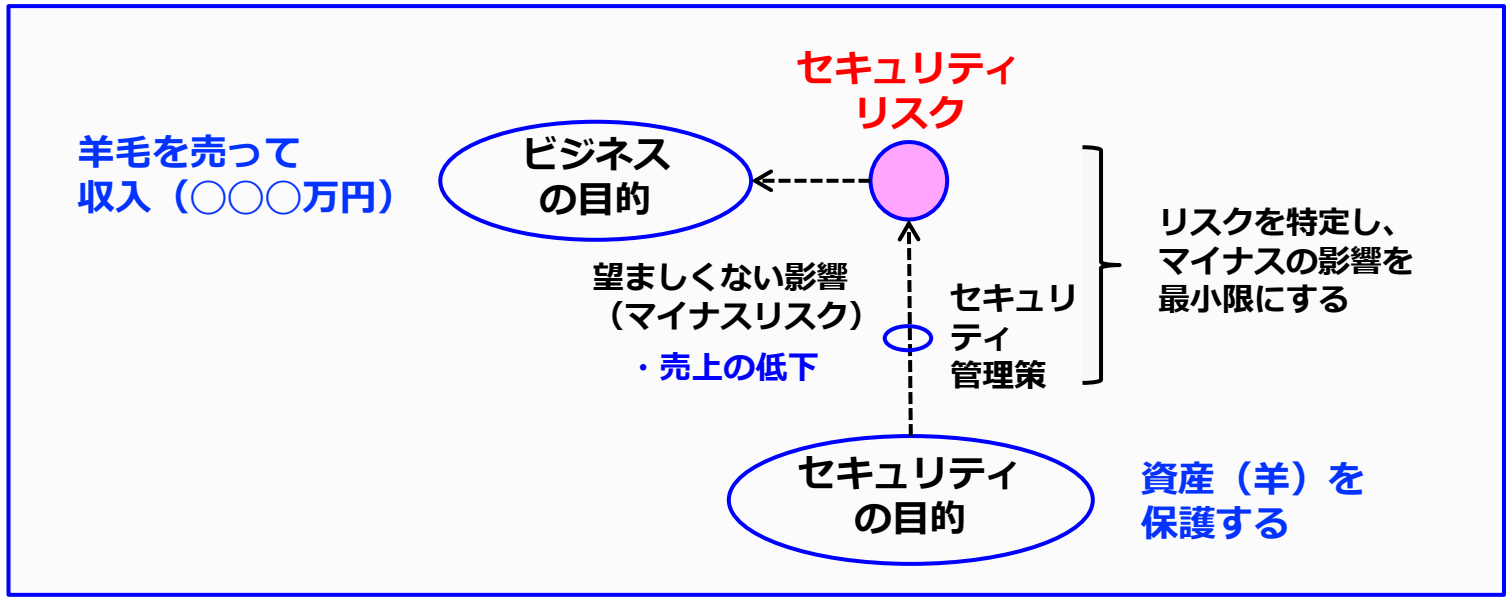
守る側



リスクを考える前提条件（ビジネスとセキュリティの目的）

ビジネスの目的	羊を飼育（投資）して羊毛を売って収入（○○○万円）を得る
組織を取り巻く環境	羊を狙う狼が出没している
ビジネスリスク	資産である羊が狼に襲われることで、ビジネス投資が無駄になる（子羊の購入代金、エサ代などの経費）
セキュリティの目的	資産（羊）を保護することでビジネスリスクを低減する

※：セキュリティリスクをコントロールして、ビジネスの目的を確実なものにする



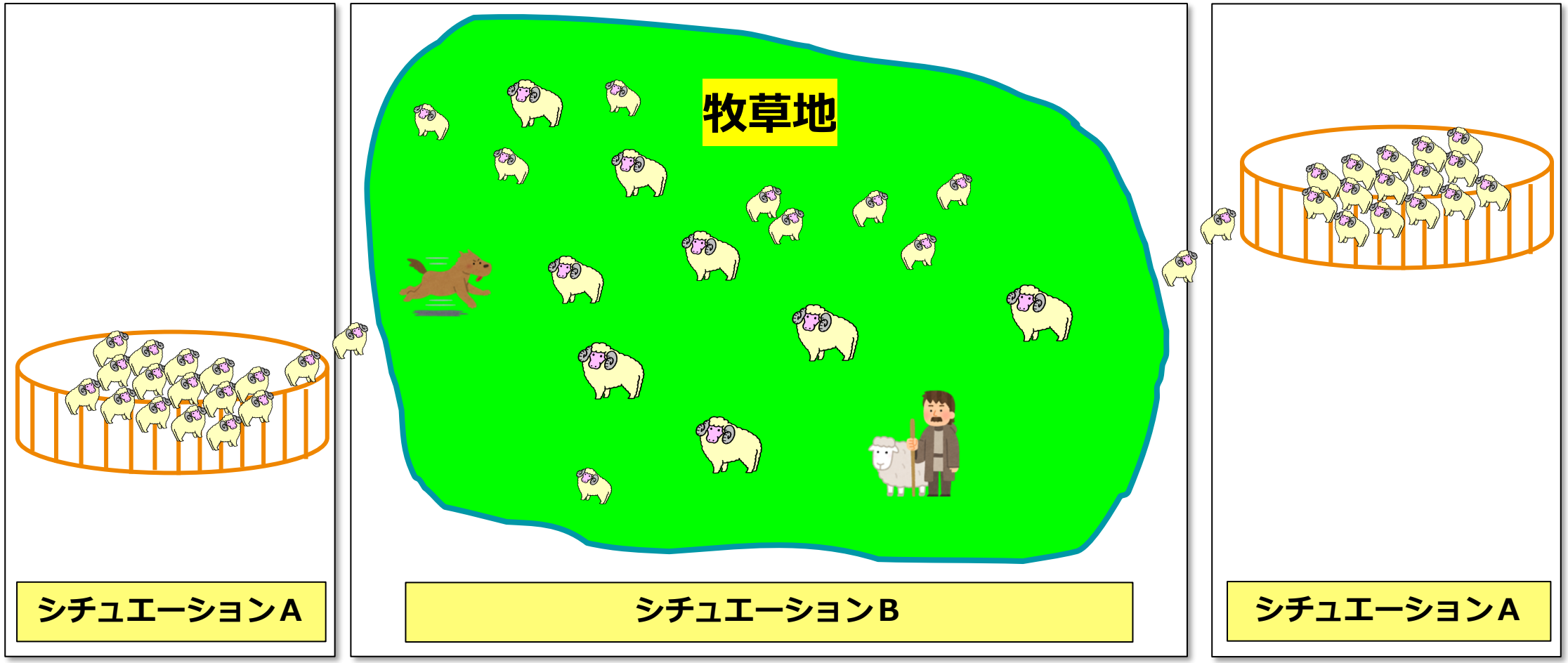
簡易業務フローと資産＆リスク源などの関係図

1日の業務の流れ

朝方 → 囲いから出す

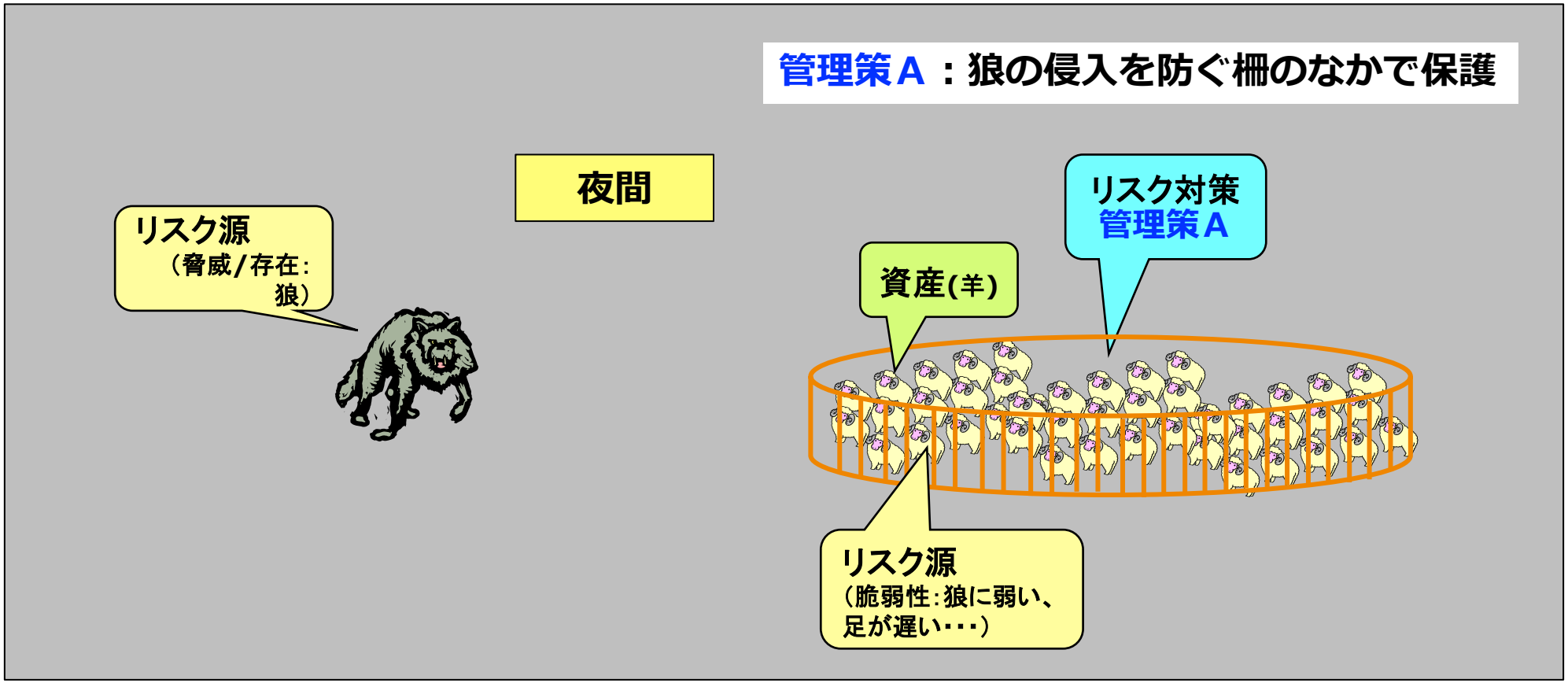
日中帯 → 広大な牧草地で食事＆運動、逸れないように監視

夕方 → 囲いに戻す



管理策Ａ：狼の侵入を防ぐ柵のなかで保護

シチュエーションＡ



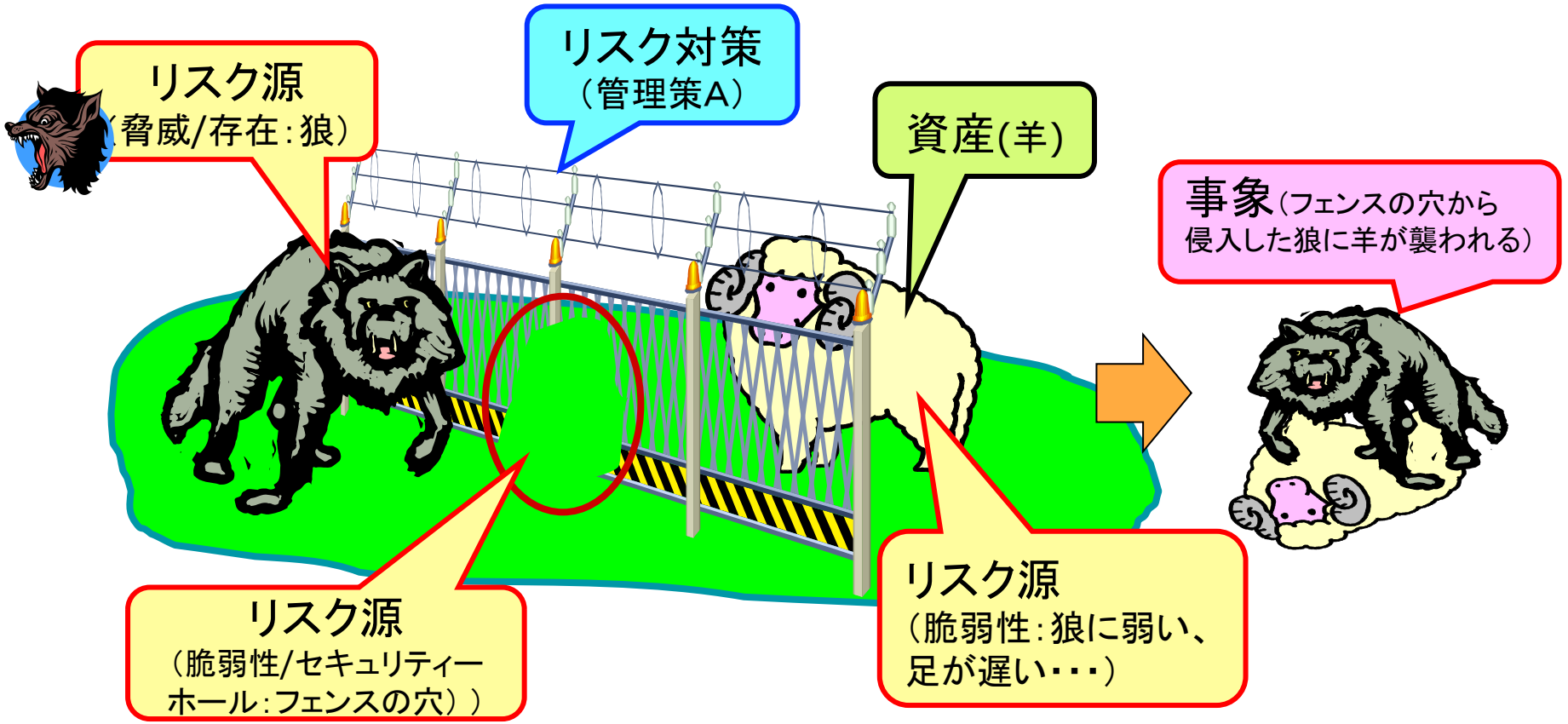
管理策Ａ：狼の侵入を防ぐ柵のなかで保護

シチュエーションA

リスク源と資産、リスク対策と事象の関係図

・資産（羊）がリスク源（狼）に襲われるとビジネスリスク（投資が無駄になる）が大きくなる

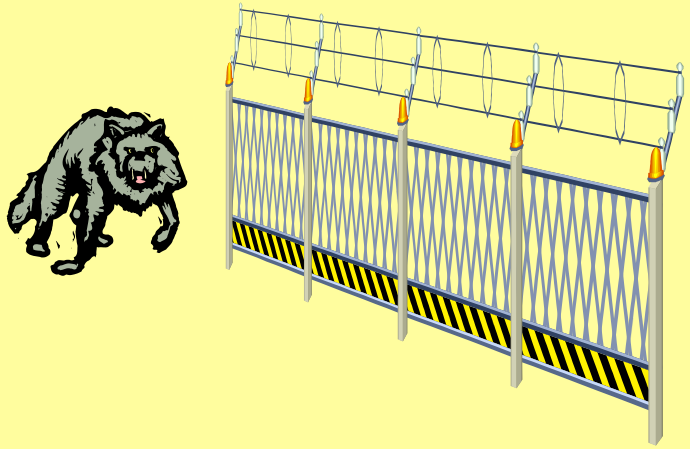
・対策としてフェンスを立てて資産（羊）を守るが、リスク源（フェンスの穴）があると
リスク源（狼）に襲われる確率が大きくなる



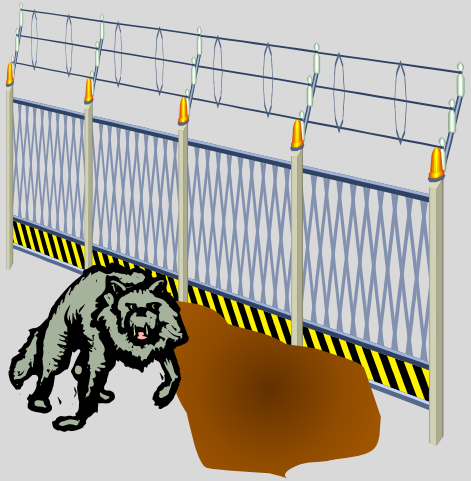
管理策Ａ：狼の侵入を防ぐ柵の比較評価（脆弱性）

シチュエーションA

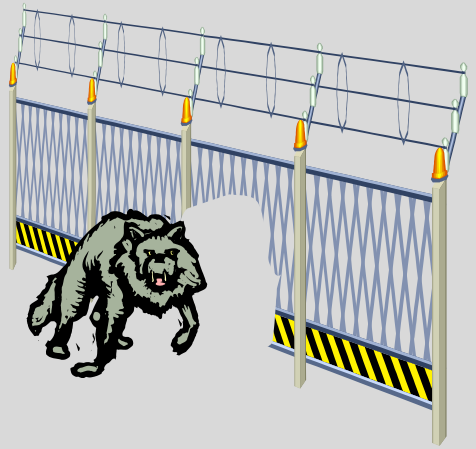
適切なリスク対策



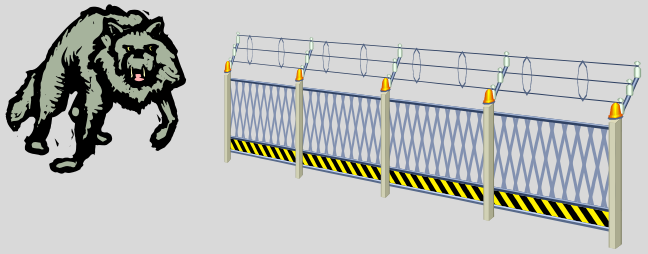
（脆弱性：柵の下の穴）



（脆弱性：金網破れの穴）

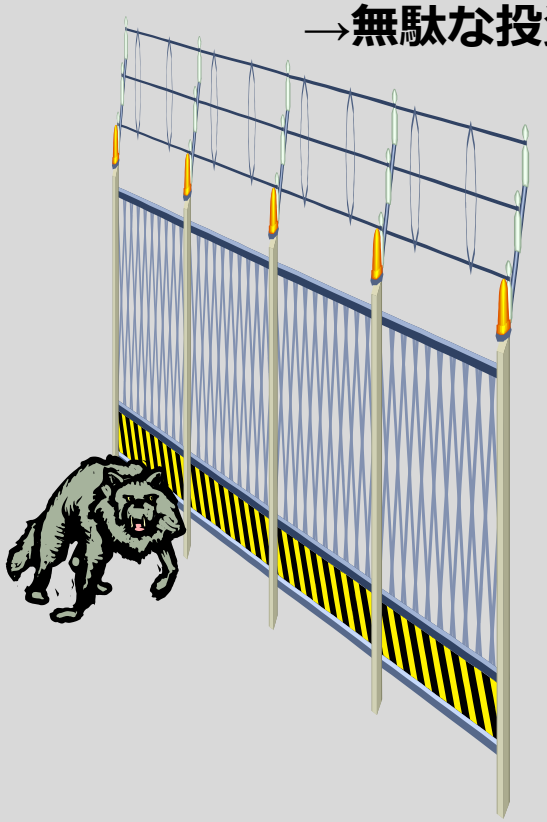


（過小対策：低すぎる柵）



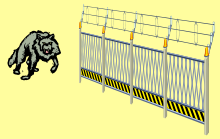
不適切なリスク対策

（過剰対策：高すぎる柵）
→無駄な投資



管理策Ａについてもう少し掘り下げると・・・

シチュエーションＡ

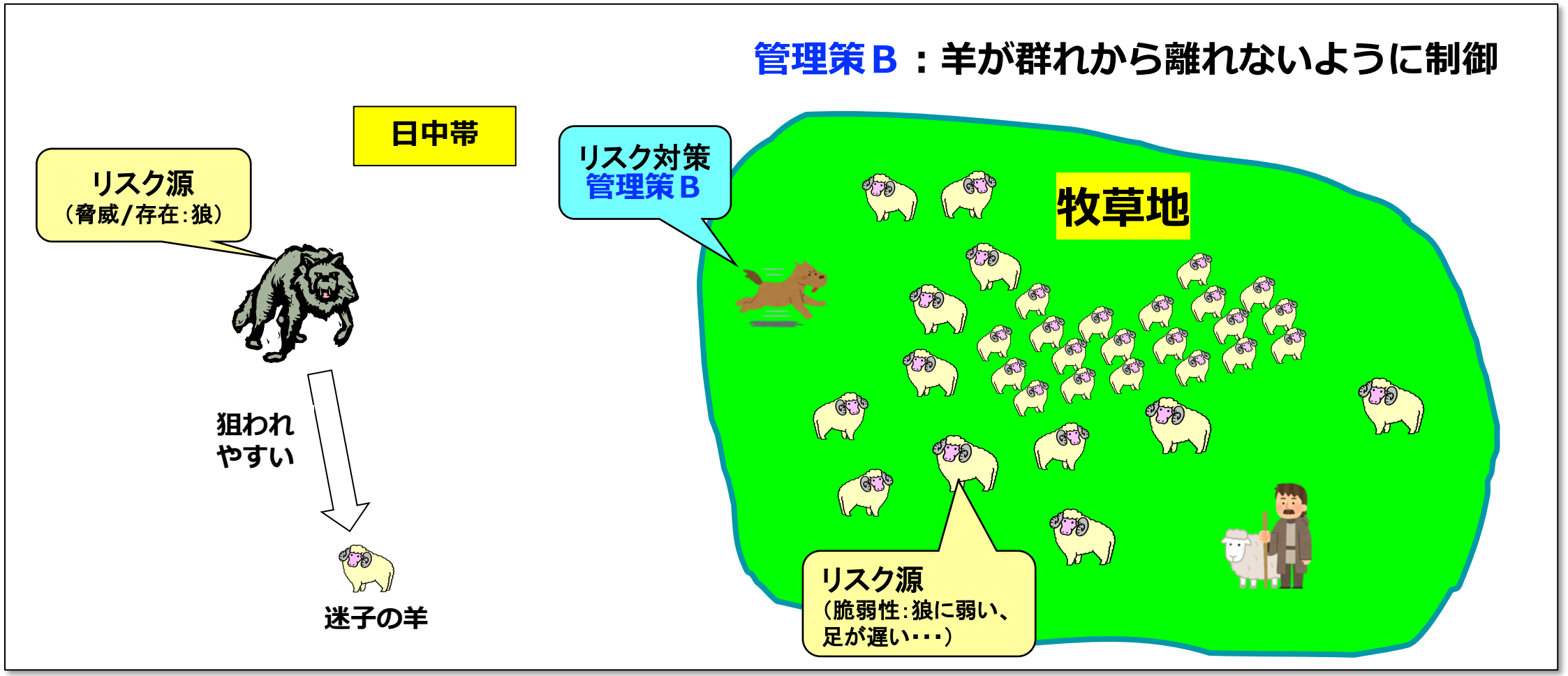
	イメージ図	適切／不適切	想定される脆弱性	備考
①		適切なリスク対策	（現時点での想定では）無し	想定した脅威（狼）対策としてはOK
②		不適切なリスク対策 （過小対策：低すぎる柵）	低すぎる柵を飛び越えて狼が侵入	リスクアセスメントが不十分で狼の身体能力についての分析がされていない（対策ありき？）
③		不適切なリスク対策 （脆弱性：柵の下の穴）	柵の下の土が掘られてトンネル状態のところから狼が侵入	対策レベルは項番①と同等だが、新たな脆弱性（柵の下の穴）が発生
④		不適切なリスク対策 （脆弱性：金網破れの穴）	金網の破れが拡大し、狼が侵入	対策レベルは項番①と同等だが、新たな脆弱性（金網の破れ）が発生
⑤		不適切なリスク対策 （過剰対策：高すぎる柵） →無駄な投資	（現時点での想定では）無し 高すぎると強風を受けて倒壊する可能性あり	必要以上に高い柵を設置 狼対策としてはOKだが、過剰投資でコストバランスが悪く、強風によって倒れるという脆弱性が生まれる可能性がある

管理策Ｂ：羊が群れから離れないように制御

シチュエーションＢ

・柵で囲われた安全エリアにいては餌の牧草が確保出来ないため、日中は牧草地にて放牧

・羊が迷子にならないように、牧羊犬が監視＆コントロールする　→迷子になると狼に狙われる



管理策Bについてもう少し掘り下げると・・・

シチュエーションB

	管理策	適切／不適切	想定される脆弱性	備考
①	牧羊犬1匹で羊の群れを監視＆制御 ＋ 羊飼いが全体をコントロール	突発的な事象が発生しなければ適切 牧羊犬のスキルに応じた対応の検討が必要	牧羊犬は1人前になると1頭で600頭の羊をコントロールできるので、能力以上の羊のコントロールや訓練中の牧羊犬の場合は迷子の羊が発生する可能性あり	日中帯ならば捜索、日没までに見つからなければその日の捜索は打ち切り 迷子の羊の耳などにタグを付けて第三者にて識別可能とすることで牧場間で連携
②	夕方までに羊を集めて柵の中に入れて、施錠する	適切 施錠の徹底等の運用状況のモニタリングが大事	牧羊犬が羊を柵の中に追い込んで羊飼いが施錠する流れだが、しっかりと施錠していないとぶつかった衝撃で開く可能性がある →施錠の確認 →施錠のかんぬきによる施錠に加えてロープで固定など	

管理策ＡをISMSの分類で整理してみると・・・

シチュエーションA

	管理策	分類	実施する管理策概要	備考
①	物理的保護（狼の侵入を防ぐ柵の設置）	7 物理的管理策 7.1 物理的セキュリティ境界	物理的な保護のために下記を実施する ・夜間に羊を保護する柵のエリアを決定する ・強度を定め、狼の侵入を防ぐ柵を設置する	防御
②	セキュリティエリアの監視	7 物理的管理策 7.4 物理的セキュリティの監視	保護柵のエリア内に侵入者がいないか定期的に監視する	検知
③	柵の管理状況の自主点検＆保全	6.人的管理策 6.8 セキュリティ事象の報告（弱点の報告を含む）	下記の状況で脆弱性が発生していないか点検 ・柵に使用している金網に破損が無いか？ ・柵の下に穴が空いて侵入可能な状態か？	検知
④	自主点検　＆ セキュリティ事象（弱点）の報告	5 組織的管理策 5.36 情報セキュリティのための方針群、規則及び標準の順守（セルフチェック） 6.8のセキュリティ事象の報告	定めたルール通りに運用されているか、柵の管理状況を定期的に確認する インシデントに繋がる弱点が見つかった場合は速やかに報告	検知
⑤	実施している管理策が有効か定期的に確認する	5 組織的管理策 5.35 情報セキュリティの独立したレビュー	定期的（半年）もしくは重大な環境の変化が生じた時に現在実施している管理策（保護柵）が有効かどうかについて関係者で検証を実施する 事例）脅威の変化： 狼→クマ（現在の保護柵の強度で十分か否か）	識別

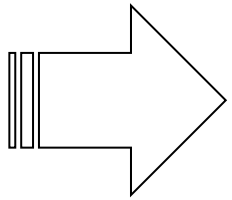
識別(Identify)、防御(Protect)、検知(Detect)、対応(Respond) 、復旧(Recover)

一般論としてのリスクについての小まとめ（1/2）

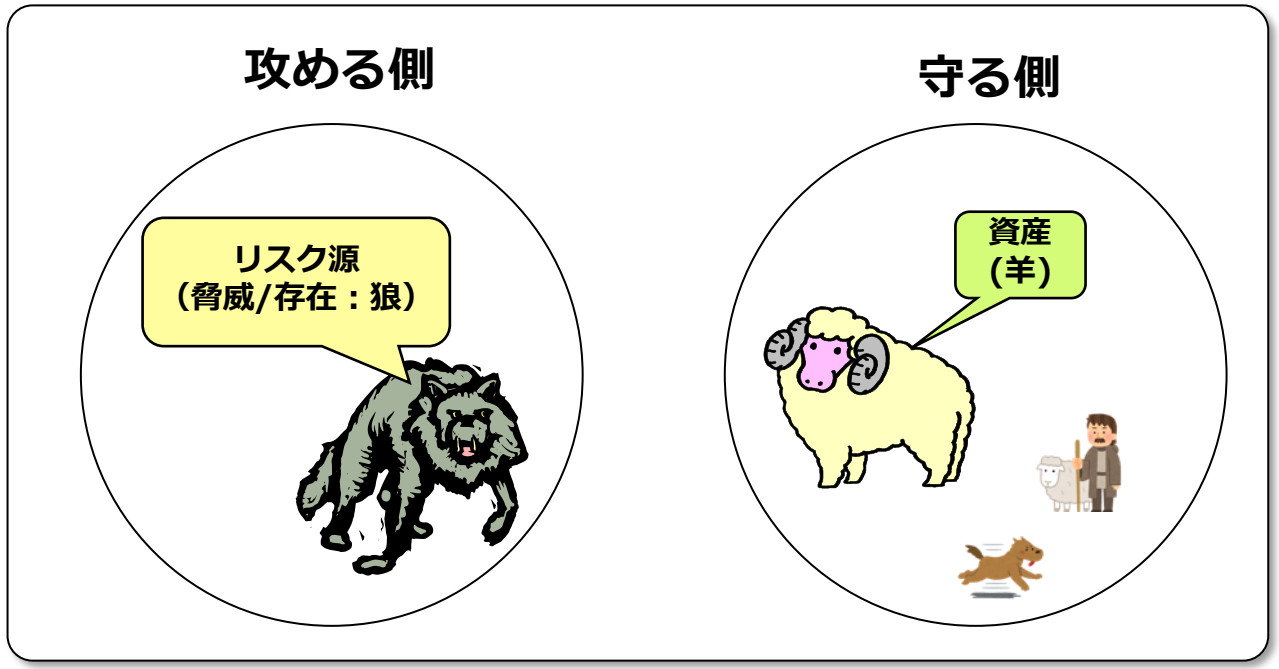
今回はリスクについての概念を理解しやすくするために、資産としての羊とリスク源（脅威/存在）としての狼をテーマに説明しました。
常にビジネスを取り巻く環境は変化しています。リスクアセスメントは一度実施すれば終わりではなく、定期的に見直しすることが必要です。

例えば、新たな脅威としてクマの存在が確認された場合には現行の対策では不十分となります・・・

新たな脅威の出現



今回の説明の範囲



一般論としてのリスクについての小まとめ（2/2）

羊と狼の一般モデルを見てきました、如何だったでしょうか？

留意点は下記となります

- 定期的に環境の変化をモニタリング
- 新たな**環境の変化**（狼から熊）に対応した**再リスクアセスメント**
- 狼や熊だけに脅威を限定せず**伝染病等の病気(*1)など多角的に検討が必要**

皆さんが普段実施されている業務モデルを題材としてリスクアセスメントについてもう少し踏み込んで見ていきたいと思います

＊1：発生時のビジネスインパクト（出荷停止、全頭処分など）が大きい

リスクアセスメントについて考える

誰でも理解出来る

リスクについて知る（一般論）

管理策Ａ：柵による保護
管理策Ｂ：群から離れないよう制御

羊と狼の事例

具体的な事例から学ぶ

ユースケースからリスクアセスメントについて学ぶ

事例1：サイバー攻撃
事例2：委託先からの情報漏洩

実践事例の提案

その１：リスクアセスメント実施のトリガーの明確化

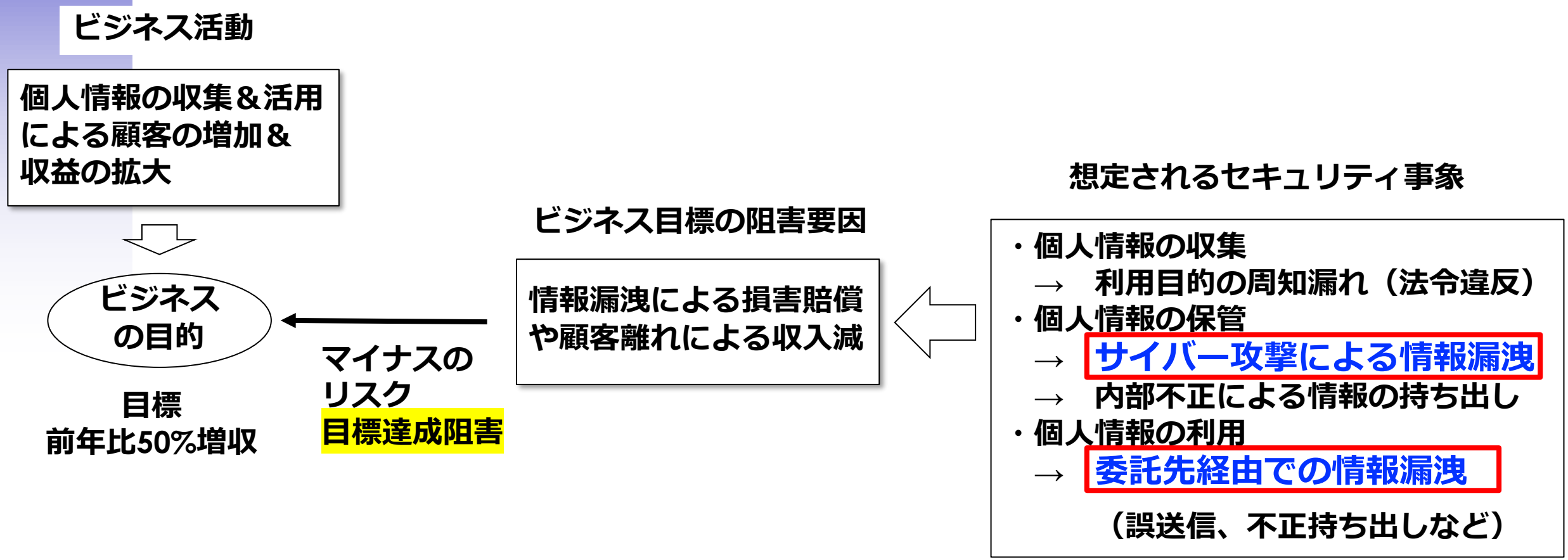
その２：マネージメント層とのリスクコミュニケーション

具体的な事例から考える

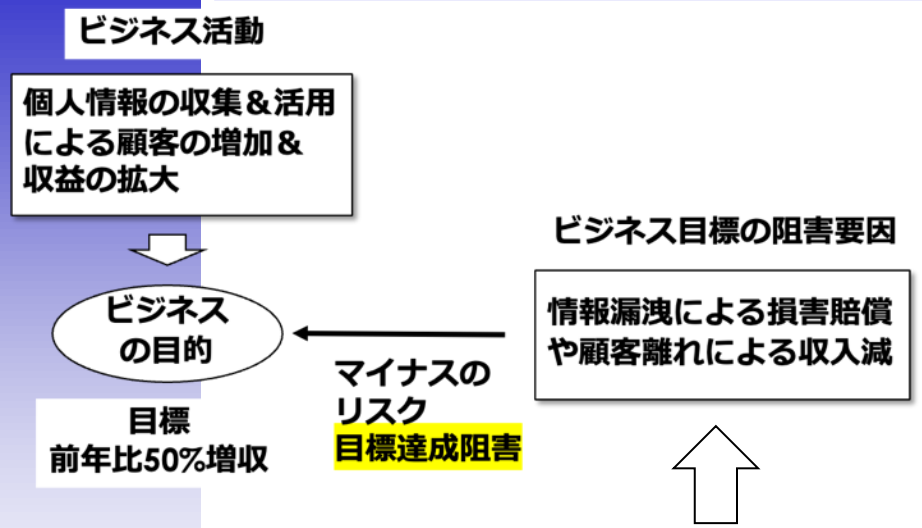
ユースケースを元にした
マイナスリスクの二つの事例

ユースケース（具体的な事例）からリスクアセスメントについて学ぶ

ネット販売を中心にビジネスを展開している組織におけるビジネスの目的に影響を与えるマイナスのリスクの事例（サイバー攻撃、委託先関連）



ユースケースを元にしたマイナスリスクの二つの事例



- 個人情報の収集
  →利用目的の周知漏れ（法令違反）
- 個人情報の保管
  →**サイバー攻撃による情報漏洩**
  →内部不正による情報の持ち出し
- 個人情報の利用
  →**委託先経由での情報漏洩**
  （誤送信、不正持ち出しなど）

事例 ①

- 標的型攻撃メールによるマルウェア感染
  感染端末→他端末感染→サーバ感染→情報漏洩
- **Webの脆弱性を突いたサイバー攻撃**
  例：SQLインジェクションなど

事例 ②

- 業務用端末からUSBメモリ経由で個人情報の
  持ち出し
- **保守/開発系端末からシステムのDBへ直接**
  アクセスして個人情報を丸ごと持ち出し

ユースケースを設定する上での前提条件

単純化したモデルケース

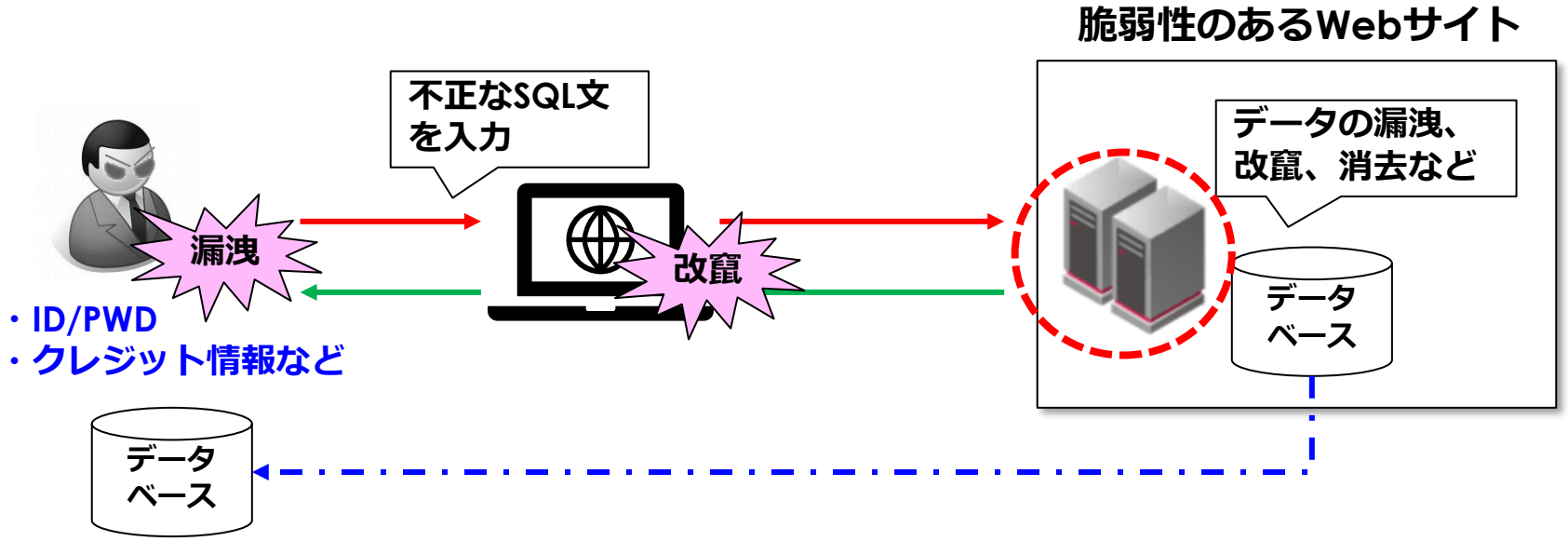
本編では正確性＆網羅性を追求するのではなく
リスクアセスメントを理解する上で解りやすさ
を追求

事例①

Webの脆弱性を突いたサイバー攻撃

事例①：Webの脆弱性を突いたサイバー攻撃

事例：セキュアなコーディングが出来ていない場合に発生するリスク（SQLインジェクション）



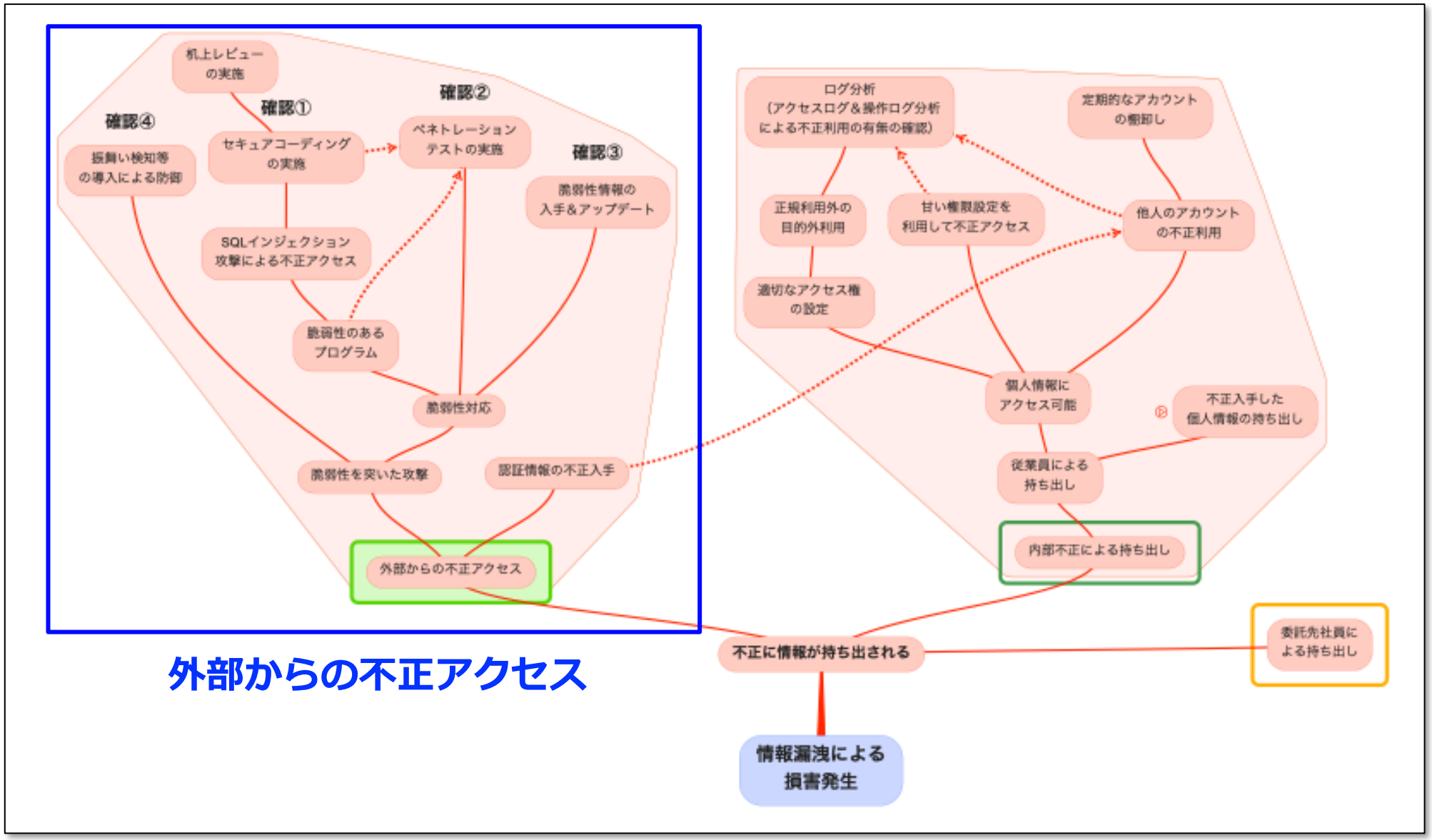
事例）

クレジットカード決済システム
　データベースから数十万件のクレジットカード番号や有効期限、セキュリティーコードなどの流出

学習塾のメールアドレス流出
　メールアドレスがフィッシング詐欺などに悪用、クレジットカード番号や個人情報の流出などの
　二次被害につながる可能性

会員サイト
　登録会員数十万人分の顧客情報が流出（住所や氏名、性別、生年月日、電話番号、メールアドレスなど）

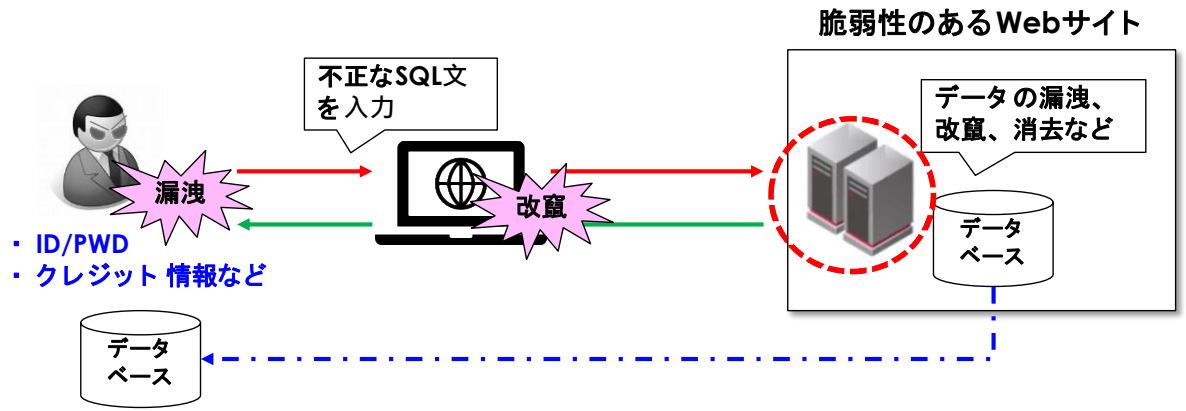
事例①：外部からの不正アクセスの情報漏洩についてのリスクの特定へのアプローチ



マインドマップによるリスクの特定

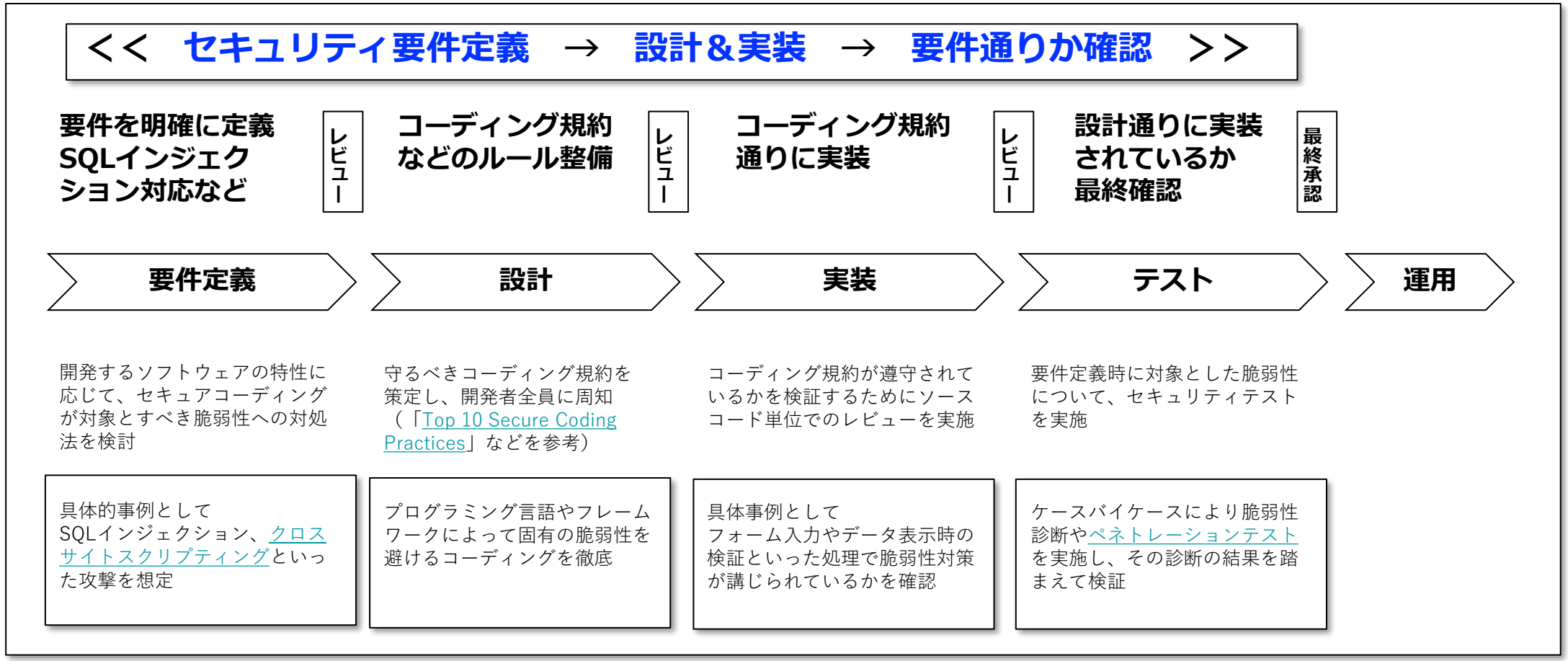
事例①：外部からの不正アクセスの情報漏洩についてのリスクの特定へのアプローチ

	セキュリティ要件	セキュリティ対策（例）	管理策の4つ分類			
			組織的	人的	物理的	技術的
確認①	セキュアコーディングの実施	セキュリティ要件を定義し、設計＆実装を行い受け入れテストを実施する プロセスとしてルール化して定着化を行う	○	ー	ー	○
確認②	ペネトレーションテストの実施	サイバー攻撃の侵入経路となり得る脆弱性から実際に侵入するテスト 出荷テストとして必須のプロセスとする	○	ー	ー	○
確認③	脆弱性情報の入手＆アップデート	システムを構成するソフト（OS、ミドルウェア、DB、PKG、AP等）の脆弱性情報を入手して、随時アップデートを行う リスクに応じて緊急度を定義し、実施する	○	ー	ー	○
確認④	振舞い検知ツール等の導入による防御	ゼロデイ攻撃等の対応として不正侵入時の異常を検知することで止血に努める	ー	ー	ー	○



セキュリティに配慮したコーディング＆テスト

悪意のある攻撃者による脆弱性（ソフトウェアが抱える不備や不具合）を突いてデータの盗聴・改ざんやマルウェアに感染させたりといった攻撃に対応するため、セキュアコーディングではこうした攻撃を受けることを想定して、脆弱性を抱えないようにソフトウェアを開発する手法



事例②

委託先経由での情報漏洩

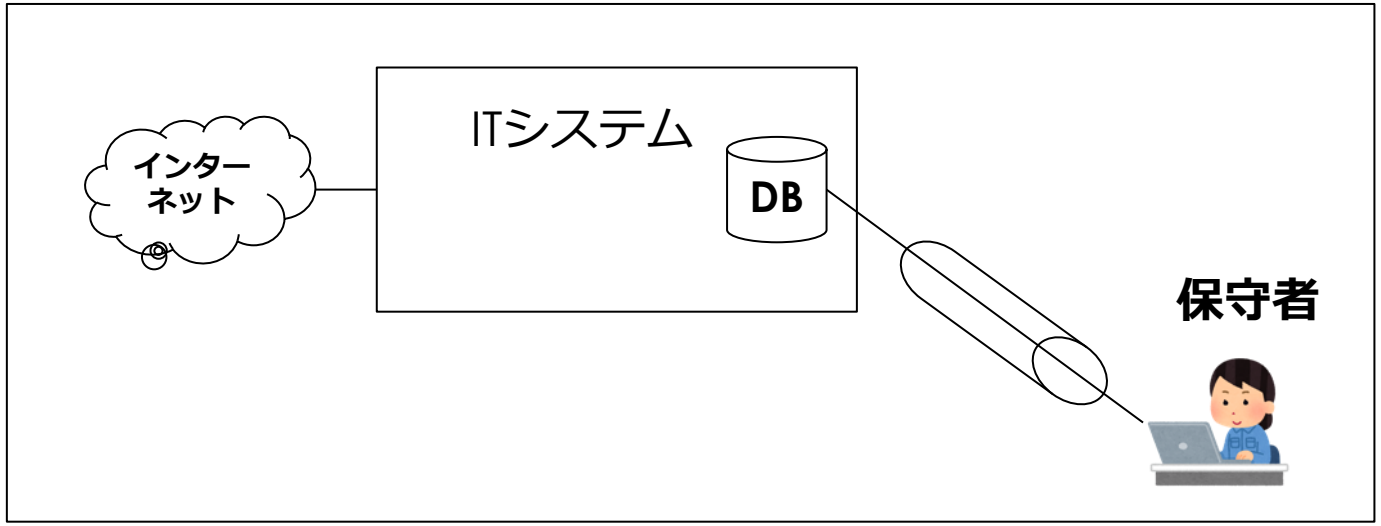
事例②：委託先経由での情報漏洩

様々なケースが想定されるが、いきなりリスクアセスメントを実施するのではなく想定されるインシデントが起こる要因について洗い出しを行い、ブレークダウンしながら、リスクの特定を行う

想定事例を絞るために下記のユースケースを想定：

保守/開発系端末からシステムのDBへ直接アクセスして個人情報を丸ごと持ち出し（持ち出しルート：USBメモリへの書き出しやSaaS経由での持ち出し）

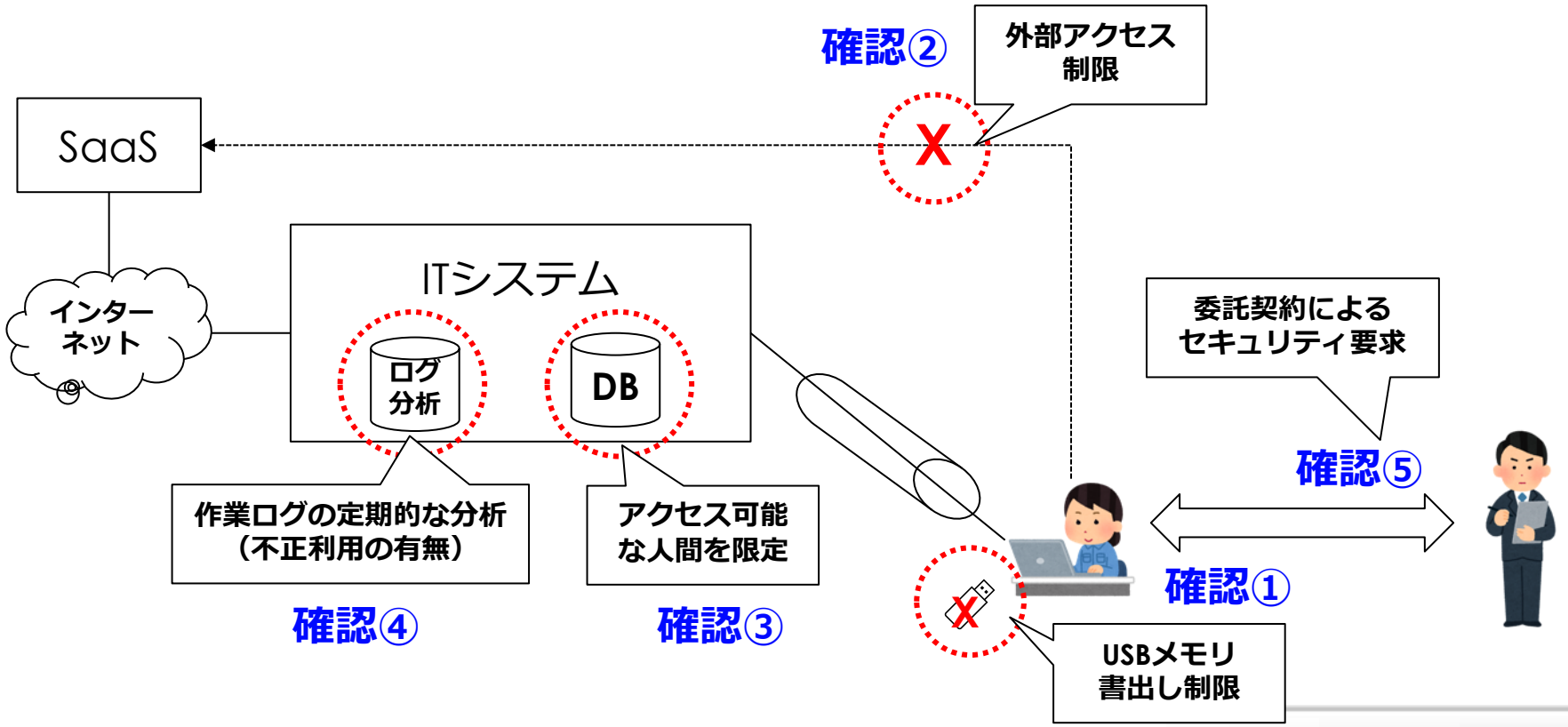
システム構成図（概略）



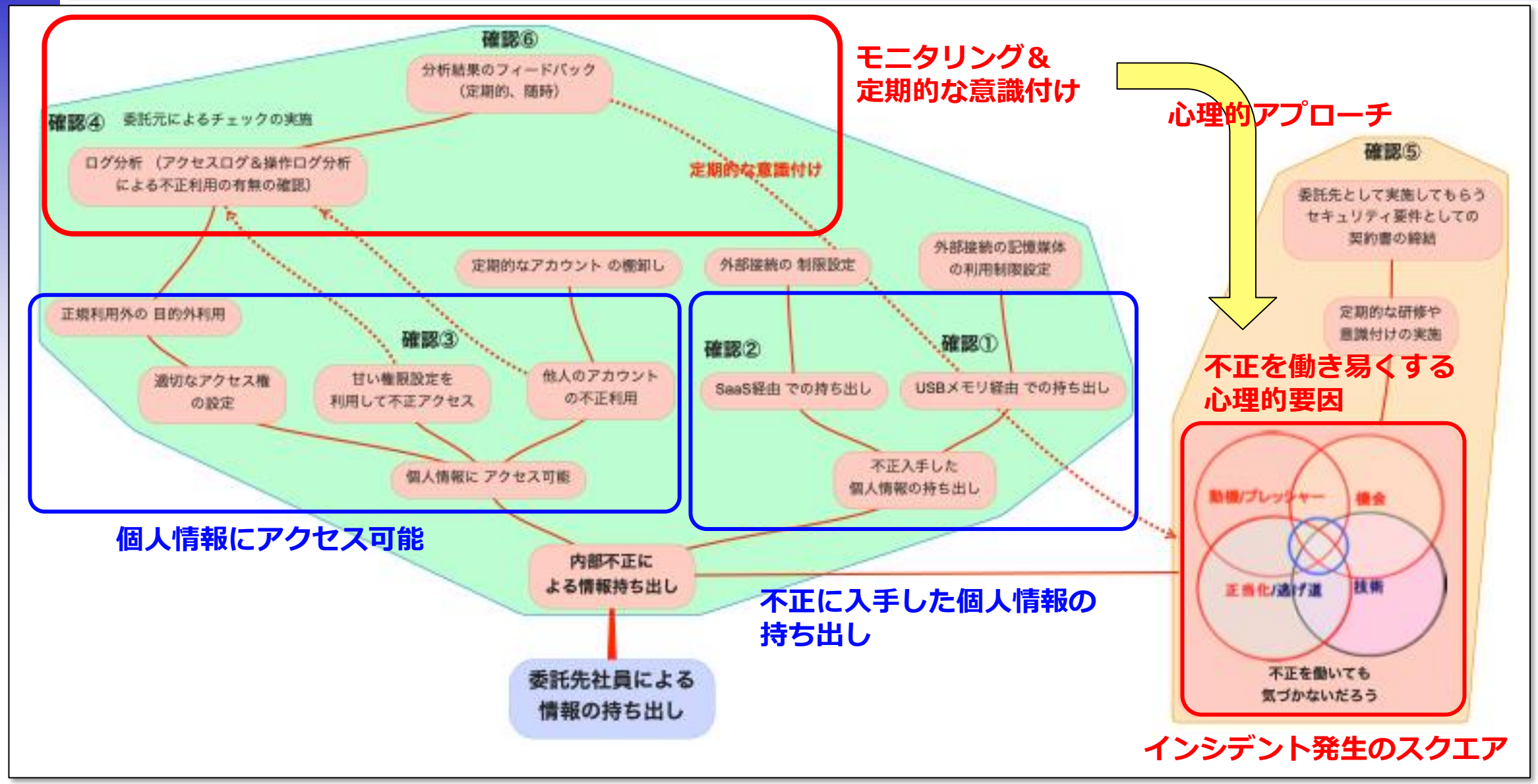
事例②：委託先経由での情報漏洩についてのリスクの特定へのアプローチ

保守/開発系端末からシステムのDBへ直接アクセスして個人情報を丸ごと持ち出し
（持ち出しルート：USBメモリへの書き出しやSaaS経由での持ち出し）

環境状況
自社ではIT環境の構築は実施しておらず、委託先に環境構築＆維持管理、運用を
業務委託している（DBへのアクセス権限等特権アカウントを委託先にて保持）



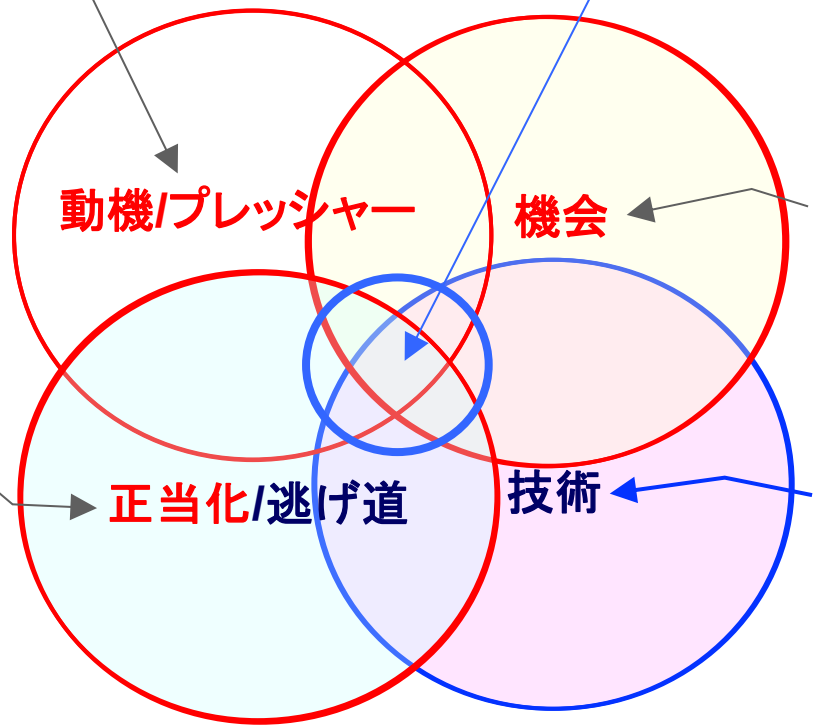
事例②：委託先経由での情報漏洩についてのリスクの特定へのアプローチ



マインドマップによるリスクの特定

参考： インシデント発生のスクエア

動機がなければ考えない（不満、不安、金銭的悩み、欲望、利益（見返り）、など、動機となる原因を調査し、観察する）

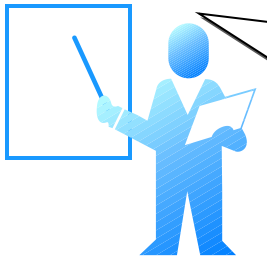


四要素が重なっている部分で問題が発生し易い。

機会がなければ実行できない（機会を与えない）

自己正当化と逃げ道がなければ実行し難い（監視、検知の仕組みと、記録、報告の徹底を行う）

技術がなければ実行できない（高度な技術で防御するか、管理者以外には変更できない仕組みとする）



不正のトライアングル（赤〇の項目）は、米国の犯罪学者であるD.R.クレッシーが、人間（犯罪者）の心理面を研究して導き出した理論ですが、情報セキュリティの面からみると、トライアングル理論に、「技術」や「逃げ道」などを追加することで、より効果的にインシデントを防止できる可能性があります。

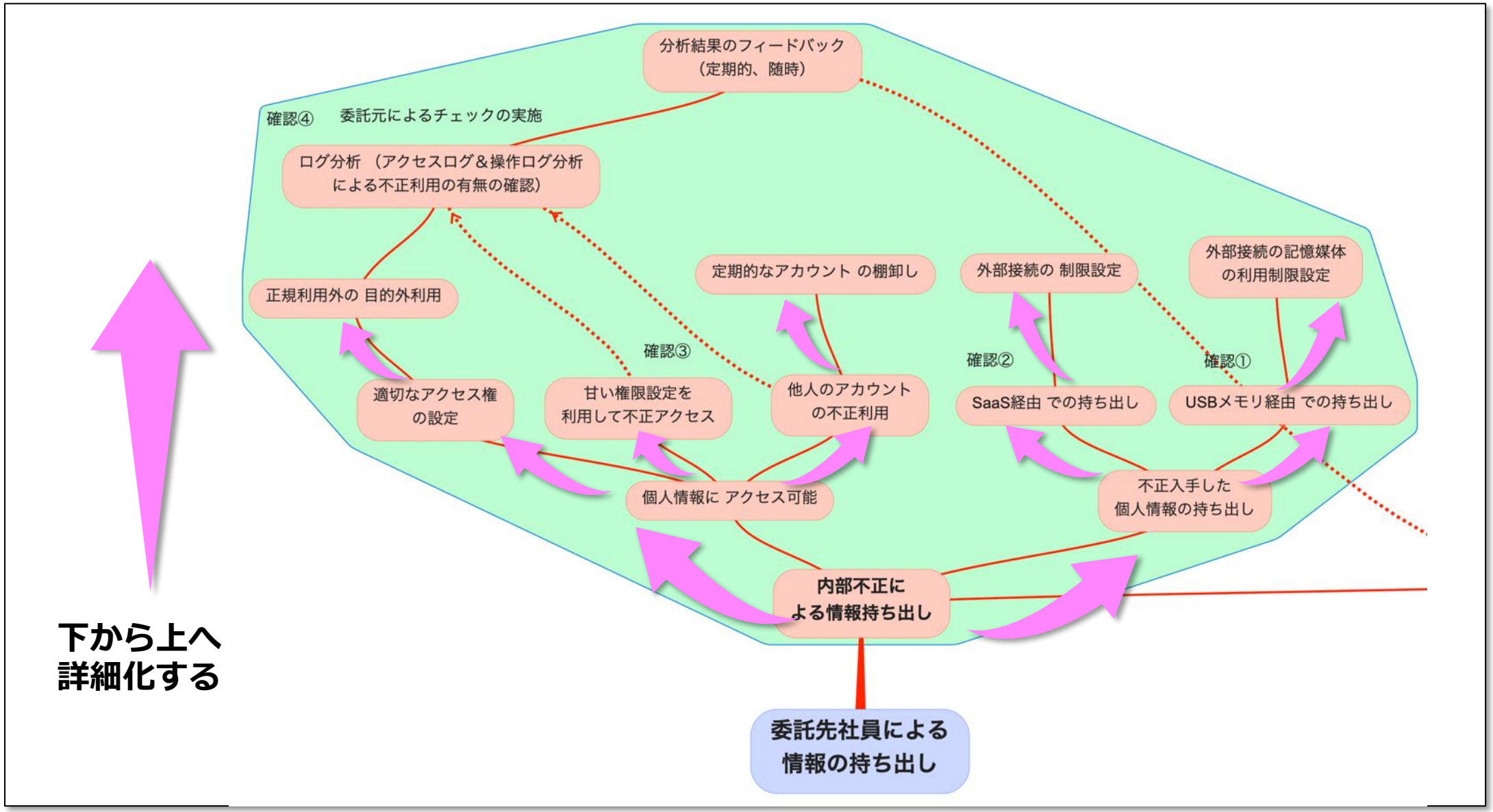
事例②：委託先経由での情報漏洩についてのリスクの特定へのアプローチ

	セキュリティ要件	セキュリティ対策（例）	管理策の4つ分類			
			組織的	人的	物理的	技術的
確認①	USBメモリ書出し制限	組織としてアクセスルール（書出し制限）を定める ツールによる書出し制限 「5.10　情報及びその他の資産の許容される利用」も関連	○	ー	ー	○
確認②	外部アクセス制限	組織としてアクセスルール（接続制限）を定める P-FWなどによる保守ルート以外のアクセスの制限	○	ー	ー	○
確認③	アクセス可能な人間を限定	組織としてアクセスルール（権限制限）を定める 重要な情報（DB）へのアクセス可能なアカウント権限の払い出し限定	○	ー	ー	○
確認④	作業ログの定期的な分析（不正利用の有無）	アクセスログ＆操作ログの取得＆ログ分析システムの導入	ー	ー	ー	○
確認⑤	委託先へ要求するセキュリティ要件の明記	委託先へ要求するセキュリティ要件を明記した契約書の締結 5.20　供給者との合意におけるセキュリティの取り扱い	○	ー	ー	ー
	セキュリティ要件の順守状況の確認	委託先におけるセキュリティ要件（ルール）に基づき実行（定期的な研修や意識付け）されていることを確認（モニタリング）する 5.22　供給者のサービス提供の監視及びレビュー	○	ー	ー	ー
確認⑥	定期的かつ明確な意識付け	アクセスログや操作ログに基づくモニタリング結果の通知やヒアリングによる見られているという明確な意識付けの実施 5.22　供給者のサービス提供の監視及びレビュー	ー	○	ー	ー

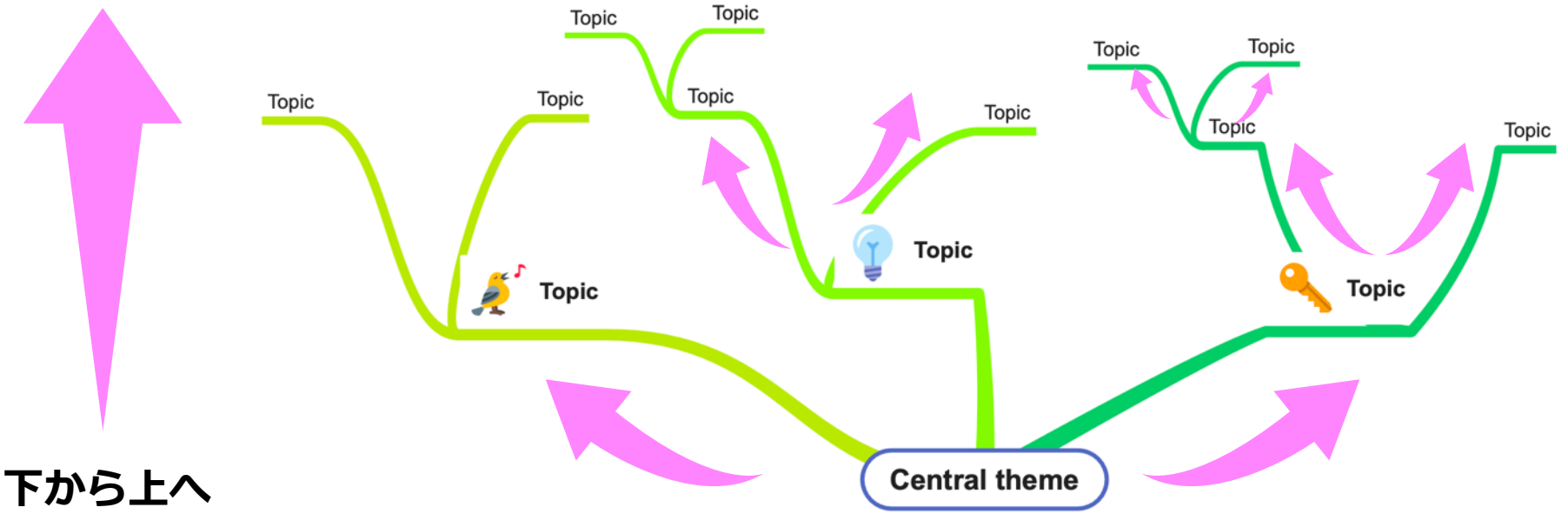
実データに基づく点検の実施

マインドマップを活用したリスクの特定のアプローチの提案

事例：マインドマップを活用したリスクの特定へのアプローチ（委託先経由の情報漏洩）



マインドマップを活用したリスクの特定へのアプローチ



下から上へ
詳細化する

マインドマップ
活用の利点

メリット1：大きな項目から関連性を持たせながら詳細化するので抜け漏れが少ない
（関連性から他の項目に広がりが出てくる）

メリット2：作業者の思考経路を図式化するので後からトレースしやすい
（グループウェアとしてノウハウが共有可能）

リスクアセスメントについて考える

誰でも理解出来る

リスクについて知る（一般論）

管理策Ａ：柵による保護
管理策Ｂ：群から離れないよう制御

羊と狼の事例

具体的な事例から学ぶ

ユースケースからリスクアセスメントについて学ぶ

事例1：サイバー攻撃
事例2：委託先からの情報漏洩

実践事例の提案

その１：リスクアセスメント実施のトリガーの明確化

その２：マネージメント層とのリスクコミュニケーション

内部/外部の環境の変化に伴うリスクへの対応について

課題①
組織を取り巻く環境は変化し、それに伴いリスクも変化

課題②
事務局を中心に個別＆詳細対応していくには稼働的に困難

？
組織全体として網羅的に実施するには？

！
リスクアセスメントのトリガーを明確にしてリスクオーナーと連携して組織として実施

リスクアセスメントのトリガーを明確にすることで網羅的に実施

・どのタイミングでどのように実施するか主要な項目について定義
・それに基づくプロセスを構築

組織として一定のベースラインでの実効性を担保

トリガーイベント	リスクアセスメントの観点＆概要	頻度	特徴＆補足事項
環境の変化	環境の変化に着目したリスクアセスメント ・人の意識の低下 ・物理環境の変化 ・ﾌﾟﾛｼﾞｪｸﾄ新設/廃止等 ・ｼｽﾃﾑ/ｻｰﾋﾞｽ新設/廃止等 ・ASP/ｸﾗｳﾄﾞｻｰﾋﾞｽ等の利用 ・ｻｲﾊﾞｰｾｷｭﾘﾃｨ対応 ・技術の変化 ・攻撃手法の変化 ・法令規制要求事項の変化 など	事象発生毎	・組織横断的なものについては事務局中心に実施 ・リスクオーナー中心に実施なものは必要に応じて支援

環境の変化に伴うリスク対応イベント（例）と個別リスクアセスメントの流れ

- 環境変化に対応したリスク対応イベント事例に従いリスクアセスメントを実施
- リスクを網羅的に特定することで抜け漏れ防止・・・最低限のベースライン

	リスク対応イベント（例）
1	オフィス新設/移転/廃止
2	PJルーム新設/移転/廃止
3	他ネットワークとの接続
4	新サービス･システムの導入/廃止
5	取扱う情報の変化
6	社内システム開発
7	外部サービスの利用 （ASP、クラウド等）
8	リモートアクセスポイントの接続
9	検証ネットワークのウイルス対策等のセキュリティ対応
10	サイバーセキュリティ攻撃対応
11	人の異動/担務変更
12	法令/ガイドライン等の改定
13	人の意識の低下 SNS、野良クラウド

参考事例： リスク対応イベントとリスク特定の観点

	リスク対応イベント	リスクアセスメントの背景＆リスク特定の観点（一例）	
7	**外部サービスの利用（ASP,クラウド）**	背景	外部サービス利用を行う場合には会社で守るべき機密情報を相手先に預けることになります。また、**契約としてはサービス利用約款に従う**ことになるため、自社で管理する場合や業務委託するケースと違い、個別でセキュリティ要求事項等の締結が出来ないため、オンプレミスでのサービス利用の場合と外部サービス利用のケースでのGAP分析を実施し、リスクの特定を行う必要があります。
		特定の観点	・利用者として求めるサービスレベルとサービス提供側のサービスレベルとのGAP分析し、可視化 ・預託する情報の機密レベルに応じたリスク分析 ・**サービス利用約款での記載事項についてCIAの滅失の観点で分析** （稼働率の観点や損害賠償等の法定対応時の裁判所の確認など）
10	**サイバーセキュリティ対応（随時）**	背景	OA環境や商用環境、開発＆検証環境等において、標的型攻撃メールや不正アクセスサイトへの誘導等によりマルウェアにPCが感染することで機密情報の漏洩リスクや外部のサイトへの攻撃の踏み台になったり（被害者から加害者）、外部記憶媒体経由（USB等）からマルウェアが社内やお客様環境へ拡散する可能性があることを認識し、**リスク対応（予防＆事後対応プロセスの確立）**する必要があります。
		特定の観点	・OA環境等において利用するメールサービスにおける不正メールのスクリーニングやSandbox機能等の導入による ～　省略　～ ・マネジメントプロセスだけでは守れないのでサイバー攻撃対応の防御システムの導入が必要 ・**脆弱性対応プロセスとして脆弱性情報の入手ルートの確立＆パッチ適用プロセスの確認** ・商用環境、開発＆検証環境の利用ガイドラインの作成による適正な運用の確認等
11	**人の異動/担務変更等（随時）**	背景	**人の異動/担務変更等時には貸与しているリソースはすべて返却や削除**が基本ルールだが、異動する本人の都合ではなく異動元の都合において必要になるかもしれないという理由等で一定期間、削除されずにそのまま放置されるケースが少なからずある。 また、一定期間と定めていても長期化する傾向があり、管理者の記憶が薄れたり、管理者自体の異動でやがて放置されるケースに繋がる。
		特定の観点	・**正規のルールから逸脱する時の手順を定める**（申請＆承認プロセス） ・必ず非正規の運用ルールを適用する期間（長くて3ヶ月）を定めておく →延長が必要な場合には延長申請を実施 ・管理対象の情報資産（アカウント、PC、ファイルなど）を一覧化して保管場所と管理者を明記 ・管理情報に基づき、3ヶ月毎に棚卸しを実施

参考情報

事例 環境の変化に伴う リスク対応イベントと リスク特定の観点

事例 環境の変化に伴うリスク対応イベントとリスク特定の観点

- 下記のような環境変化が発生することで、当初想定していたリスクが変化します。
- 発生するリスクに的確に対応することでビジネスに与えるインパクトを最小限にコントロールします。

	リスク対応イベント	リスクアセスメントの背景＆リスク特定の観点（一例）	
1	オフィス新設/移転/廃止	背景	オフィスエリアとして確保する居室のセキュリティレベルの確保のためにリスクアセスメントを実施します。観点として下記のような項目を意識する必要があります。
		特定の観点	・物理環境の観点でビル環境（電力、空調等含むファシリティ）状況 ・エリア管理の観点で要求されるセキュリティレベル（REDゾーン、特殊エリア等）の状況、監視カメラの設置状況 ・移転は新設＆廃止の組み合わせとなり、移転に伴うサービスの継続性や書類＆PC等の情報機器の移動に伴う情報の紛失や誤廃棄、重要情報のバックアップの確保などの確認が必要。 ・廃止では情報の廃棄漏れなどによる情報漏洩の防止が必要。
2	PJルーム新設/移転/廃止	背景	基本的にオフィス移転と同様な観点となりますが、プロジェクトとして要求される情報セキュリティ要件（A.6.1.5）に従ったリスクアセスメントが必要となります。そのためにはプロジェクトの特性の把握、PJルームに要求されるセキュリティ要件の洗い出しが重要となります。
		特定の観点	・エリア管理として入室者の限定 ・複数の業務用回線の混在利用（CSOL-NW、統合網、業務用個別回線（UNO等）） ・情報資産の持込み、持ち出し等の管理 ・共有ファイルサーバ等へのアクセス管理 ・移転についてはオフィスと同等の確認が必要。PJ特有としては複数の案件のPJで混在利用するケースも多いので、他PJの物品の不正持ち出し、誤廃棄等の対応が必要。
3	他ネットワークとの接続	背景	既存のネットワークに他のネットワークを接続することにより、許可していない利用者やシステムからの不正なアクセスが発生し、想定外の情報漏洩等が発生する可能性があります。接続元、接続先それぞれのアクセスポリシーを確認すると共にネットワーク領域の分離が必要となります
		特定の観点	・相互接続の必要性＆相互のアクセスの可否の設定状況 ・相互接続するネットワークそれぞれのアクセスポリシーの確認と相違点 ・目的外利用の可否 ・ネットワーク構成図（概念図、論理/物理構成図）に基づきアクセス許可/拒否ルールの確認

事例 環境の変化に伴うリスク対応イベントとリスク特定の観点

	リスク対応イベント	リスクアセスメントの背景＆リスク特定の観点（一例）	
4	新サービス･システムの導入/廃止	背景	新サービスの導入やシステムの新規導入において、どのような情報を取扱い、どのように保管するのか含めてリスクアセスメントを実施する必要があります。サービス要件、システム要件について可視化することでセキュリティ要件を明示し、リスクの特定を行います。
		特定の観点	・取り扱う情報の機密レベルの確認＆個人情報の有無 ・アカウント管理とアクセス権限設定 ・システムの場合は脆弱性管理（サーバの要塞化、脆弱性診断、サイバーセキュリティ対策等）
5	取扱う情報の変化	背景	業務の変化や新規業務に伴い取り扱う情報が変化します。お客様の要件が変更になり新たに重要な情報資産（機密区分：SA、A）の取扱いが発生するなどリスクが増大する可能性があります。個人情報だと取扱いについて法律要件が発生しますので取扱いについて厳密な管理が要求されます。 取り扱う情報資産の変化については情報資産ＷＳにてリスクアセスメントを実施しますが、機密区分がSA/Aのものや法律要件が変化した場合は情報資産WSを使ったリスクアセスメントに加えて業務プロセスから実施する詳細リスクアセスメントの実施が必要となります。
		特定の観点	・情報資産についてCIAの滅失の観点でどのようにビジネスに影響を与えるかを確認 ・個人情報については法律で厳格に管理することが要求されているので、ライフサイクルに応じた脅威に対するリスクアセスメントとリスク対応が適切に実施されていることを確認 ・機密区分SA、Aに対しては厳密な配布管理の確認、暗号化対応等
6	社内システム開発	背景	システム開発に際して提供するシステムが脆弱性対応が一定のレベルで実施出来ていることを保証するために、想定される脅威に対応したリスクアセスメントの実施が必要となります。
		特定の観点	・セキュアコーディング（クロスサイトスクリプティング、SQLインジェクション対応等） ・構成するOS、DB等のミドルウェア、開発AP等の脆弱性情報の把握＆リスク対応 ・脆弱性診断による脆弱性対応状況の把握＆製品に最新化等の対応プロセスの確認 ・暗号化対応（必要に応じて） ・FWのアクセスポリシーの設定、NWのセグメンテーション設計等 （特にクラウド利用の場合にはNWのアクセス制限の設定をしない状態でアクセス開放すると不正侵入され、他システムへの不正アクセスの踏み台にされるリスクが増大する）

事例 環境の変化に伴うリスク対応イベントとリスク特定の観点

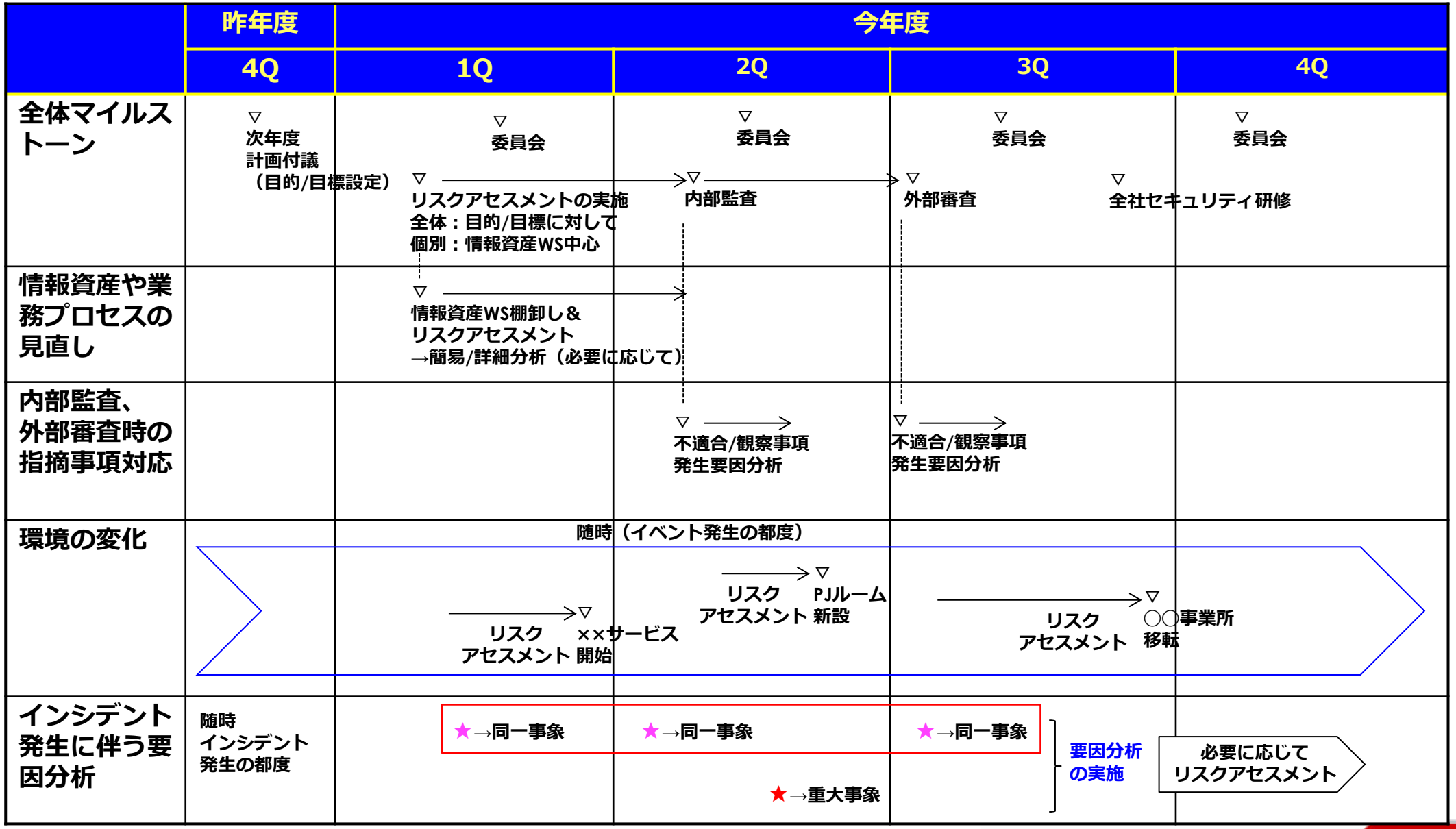
	リスク対応イベント	リスクアセスメントの背景＆リスク特定の観点（一例）	
7	外部サービスの利用 （ASP、クラウド等）	背景	外部サービス利用を行う場合には会社で守るべき機密情報を相手先に預けることになります。また、契約としてはサービス利用約款に従うことになるため、自社で管理する場合や業務委託するケースと違い、個別でセキュリティ要求事項等の締結が出来ないため、オンプレミスでのサービス利用の場合と外部サービス利用のケースでのGAP分析を実施し、リスクの特定を行う必要があります。
		特定の観点	・利用者として求めるサービスレベルとサービス提供側のサービスレベルとのGAP分析し、可視化 ・預託する情報の機密レベルに応じたリスク分析 ・サービス利用約款での記載事項についてCIAの滅失の観点で分析 （稼働率の観点や損害賠償等の法定対応時の裁判所の確認など）
8	リモートアクセス ポイントの接続	背景	リモートアクセスのポイントを作成することで、外部から侵入されるリスクが発生します。リモートアクセスの必要性、対象者の限定等についてリスクアセスメントが必要となります。
		特定の観点	・リモートアクセスポイントの認証方式とその運用方法 ・外部から不正アクセスに対する対応策 ・不正アクセスの有無＆正規利用者の目的外利用の有無の確認（アクセスログの取得＆分析） ・認証後のアクセス範囲の設定の正当性
9	検証ネットワークの ウイルス対策等の セキュリティ対応	背景	検証ネットワークにおいて重要な情報資産が無いという判断で接続PC等へのウィルス対策ソフトの導入がなされないケースがありますが、想定外の経路で情報資産が持ち込まれたり、マルウェアにPCが感染することで外部のサイトへの攻撃の踏み台になったり（被害者から加害者）、外部記憶媒体経由（USB等）からマルウェアが社内やお客様環境へ拡散する可能性があることを認識する必要があります。
		特定の観点	・検証環境における最低限実施すべきセキュリティ管理策の実施（ウィルス対策ソフトの導入、セキュリティパッチの施行、システムアップデートの最新化等） ・検証環境の利用ガイドラインの作成による適正な運用

事例 環境の変化に伴うリスク対応イベントとリスク特定の観点

	リスク対応イベント	リスクアセスメントの背景＆リスク特定の観点（一例）	
10	サイバーセキュリティ攻撃対応（随時）	背景	OA環境や商用環境、開発＆検証環境等において、標的型攻撃メールや不正アクセスサイトへの誘導等によりマルウェアにPCが感染することで機密情報の漏洩リスクや外部のサイトへの攻撃の踏み台になったり（被害者から加害者）、外部記憶媒体経由（USB等）からマルウェアが社内やお客様環境へ拡散する可能性があることを認識し、リスク対応（予防＆事後対応プロセスの確立）する必要があります。
		特定の観点	・OA環境等において利用するメールサービスにおける不正メールのスクリーニングやSandbox機能等の導入による振る舞い検知やマルウェア感染時に発生する不正アクセスの振る舞い検知によるモニタリング＆NWの遮断対応等 ・標的型攻撃メール等への対応として不正なメールについての認識や万が一添付ファイルを開封等を実施することで感染時の拡散予防対応プロセスの確立について（研修による理解＆標的型攻撃メールの対応訓練による理解度や実効性の確認） ・マネジメントプロセスだけでは守れないのでサイバー攻撃対応の防御システムの導入が必要 ・完全に防御することは不可能なのでインシデント発生後の事後対応として、被害拡散防止や攻撃の分析のためのマルウェアの検体の採取＆分析、NW遮断対応プロセスの構築の有無 ・脆弱性対応プロセスとして脆弱性情報の入手ルートの確立＆パッチ適用プロセスの確認 ・商用環境、開発＆検証環境の利用ガイドラインの作成による適正な運用の確認等
11	人の異動/担務変更等に伴う情報資産（引き継ぎ情報）の扱い（随時）	背景	人の異動/担務変更等時には貸与しているリソースはすべて返却や削除が基本ルールだが、異動する本人の都合ではなく異動元の都合において必要になるかもしれないという理由等で一定期間、削除されずにそのまま放置されるケースが少なからずある。 また、一定期間と定めていても長期化する傾向があり、管理者の記憶が薄れたり、管理者自体の異動でやがて放置されるケースに繋がる。
		特定の観点	・正規のルールから逸脱する時の手順を定める（申請＆承認プロセス） ・必ず非正規の運用ルールを適用する期間（長くて3ヶ月）を定めておく →延長が必要な場合には延長申請を実施 ・管理対象の情報資産（アカウント、PC、ファイルなど）を一覧化して保管場所と管理者を明記 ・管理情報に基づき、3ヶ月毎に棚卸しを実施

※：ここで示したものはあくまでもサンプルで考え方や整理の方向性を示したものとなりますので、自組織にあったものを検討してみてください

参考：　年間活動計画から見たリスク洗い出しイベント（例）



リスクアセスメントについて考える

誰でも理解出来る

リスクについて知る（一般論）

管理策Ａ：柵による保護
管理策Ｂ：群から離れないよう制御

羊と狼の事例

具体的な事例から学ぶ

ユースケースからリスクアセスメントについて学ぶ

事例1：サイバー攻撃
事例2：委託先からの情報漏洩

実践事例の提案

その１：リスクアセスメント実施のトリガーの明確化

その２：マネージメント層とのリスクコミュニケーション

事例1：マネージメント層との リスクコミュニケーション

・様々なステークホルダーとのリスクコミュニケーションが必要

ステークホルダー（stakeholder）

意思決定若しくは活動に影響を与え、影響されることがある又は影響されると認知している、あらゆる人又は組織

株主や投資家
役員、従業員
関連会社
行政機関
顧客や取引先
地域社会
など

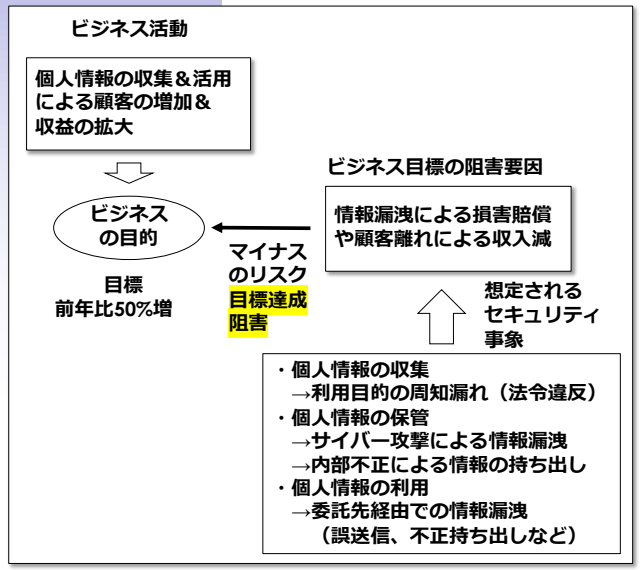
・今回はイメージしやすいマネージメント層との リスクコミュニケーションを題材として設定

・マネージメントレビューへのインプットの観点で考察

リスクコミュニケーションの観点からの考察

内部/外部の課題の可視化とマネージメント層へのインプット情報

内部/外部の課題や利害関係者のニーズ及び期待の可視化



内部/外部の課題

内部の課題	変化：委託先への依存度増加傾向 → 委託先管理の徹底
外部の課題	変化：無差別なサイバー攻撃の増加 → 振舞い検知ツールの導入 → セキュリティ体制の強化

＋

利害関係者のニーズ及び期待の可視化

株主	株価の安定 → 増収＋社会的信用の維持＆向上
お客さま	安心・安全なサービスの提供 → 預託した個人情報等の管理の徹底

マネージメントレビューへのインプット情報（事例）

サイバー攻撃の状況の共有
- 脅威インテリジェンスの活用

サイバー攻撃への**対応プラン＆リスクアセスメント実施結果**など
- 未対応時のビジネスリスク
- 費用対効果

振舞い検知ツール（EDR/NDR）の導入
- 初期費用
- ランニング費用等

サイバー攻撃に対応する体制強化
- 分析対応（内製／外注）リソース
- 人材育成費用等

昨年の脅威インテリジェンスについての振り返りを実施しながら、経営層とのリスクコミュニケーションを考える

詳細は2023年度情報セキュリティマネジメントセミナー資料を参照

https://www.jnsa.org/seminar/std/isms/2023/index.html

抜粋

5.7 脅威インテリジェンス（要約）

概要

情報セキュリティの脅威に関する情報を収集及び分析し、脅威インテリジェンスを構築すること。

実現したいこと

サイバーセキュリティの脅威（※1）から組織の活動を守るため、脅威インテリジェンスを活用する

※1：このテーマの中では、人的、組織的、物理的、技術的の4つの分野の脅威の中から、変化が激しく組織に重大な影響を与える可能性の高いサイバーセキュリティの脅威を「脅威インテリジェンス」の研究対象とする

具体的な対応内容や補足事項など

・脅威インテリジェンスは、攻撃者の動機、標的、攻撃手法を理解して対応するために収集・分析されたデータ

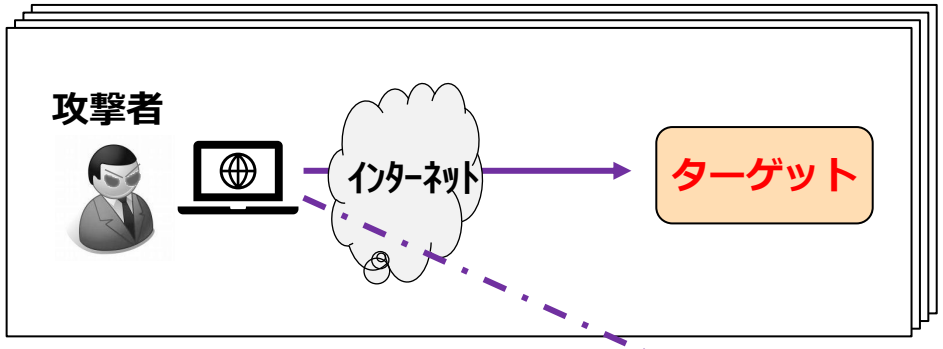
・経営戦略的な判断をするための入力情報として活用（経営層）したり、予想される攻撃や実際の攻撃から防御する　ための入力情報として活用（セキュリティの専門家、システム担当など）

＜情報の例示＞
サイバーセキュリティの専門家が分析・整理したサイバー攻撃に関する情報

・攻撃のメカニズム（攻撃手法）
・攻撃の発生の識別方法
・攻撃によってビジネスに与える影響
・防御方法などのアドバイス
・攻撃を実現させる環境・条件があるか

抜粋

5.7 脅威インテリジェンス（イメージ図）



サイバーセキュリティの
専門家が分析・整理した
サイバー攻撃に関する
情報を収集

外部組織

専門組織

セキュリティ研究機関、
NPO法人、セキュリティ
ベンダー、など

サイバー攻撃に関する情報

- 攻撃のメカニズム（攻撃手法）
- 攻撃の発生の識別方法
- 攻撃によってビジネスに与える影響
- 防御方法などのアドバイス

内部組織

防御

戦略情報として
のインプット

マネジメント層
主要な意思決定者、
CEO、取締役など

セキュリティ担当
セキュリティ技術者
CSIRTやISMS事務局

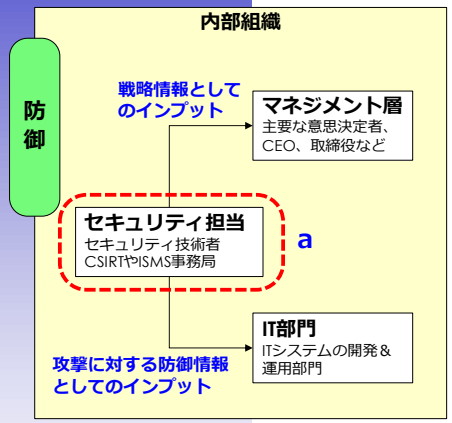
IT部門
ITシステムの開発＆
運用部門

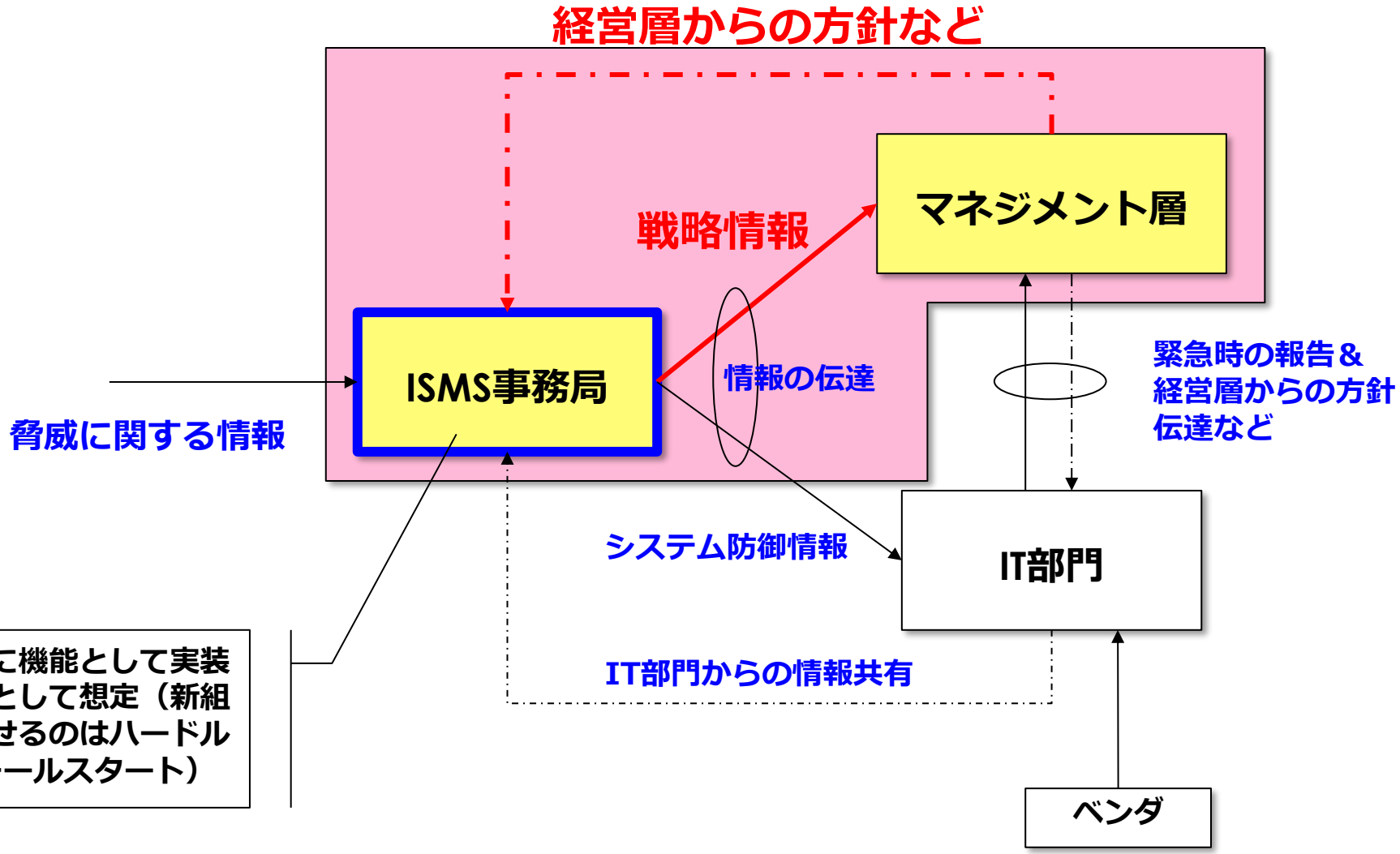
攻撃に対する防御情報
としてのインプット

参考情報

a.脅威情報を簡易分析（判断）する機能を実装し、情報を伝達する

脅威情報を基にサイバー攻撃の脅威に対して対応方針を相談する





既存の組織の中に機能として実装することを前提として想定（新組織として独立させるのはハードルが高いのでスモールスタート）

事例1：マネージメント層とのリスクコミュニケーション

マネージメントレビューへの
インプット情報（事例）

サイバー攻撃の状況の共有
・脅威インテリジェンスの活用

サイバー攻撃への対応プラン＆リスク
アセスメント実施結果など
・未対応時のビジネスリスク
・費用対効果

振舞い検知ツール（EDR/NDR）の導入
・初期費用
・ランニング費用等

サイバー攻撃に対応する体制強化
・分析対応（内製／外注）リソース
・人材育成費用等

経営層とのコミュニケーション情報（例）

インプットする条件

- **経営戦略上意識すべき脅威（中長期）**
- **ビジネスリスクに直面する脅威（短期）**

例）
- 自組織に関連する業界や組織を取り巻く脅威情報（アクティブなサイバー犯罪者情報など）
- サイバー犯罪で利用される攻撃手法の情報
- 自組織のブランドに悪影響をおよぼす情報（偽サイト情報など）

タイミング

- **中長期はマネジメントレビューのタイミング、短期は随時**

マネジメントレビューのフィードバック

- **経営層からの指示は記録し、リスク対応計画や課題管理**
- **投資判断が必要なものは事業計画に計上**

事例1：マネージメント層とのリスクコミュニケーション　（具体的なアクション事例）

マネージメントレビューへの
インプット情報（事例）

サイバー攻撃への対応プラン＆リスクアセスメント実施結果など
・未対応時のビジネスリスク
・費用対効果

振舞い検知ツール（EDR/NDR）の導入
・初期費用
・ランニング費用等

サイバー攻撃に対応する体制強化
・分析対応（内製／外注）リソース
・人材育成費用等

具体的なアクション事例（案）

サイバー攻撃への対応プラン＆リスクアセスメント実施結果など

事業継続（5.30 事業継続のための ICTの備え）の観点から一般的な災害対策に加えてサイバー攻撃についても下記を実施する

経営資源の投入が必要なので費用対効果を見極めるために事業影響度分析（BIA）によって、復旧時間目標（RTO）を設定しその目標達成を確実にするためのリソース決定し準備する

・未対応時のビジネスリスク
・費用対効果

事例1：マネージメント層とのリスクコミュニケーション

	昨年度	今年度			
	4Q	1Q	2Q	3Q	4Q
全体マイルストーン	▽次年度計画付議（目的/目標設定）	▽委員会 ▽リスクアセスメントの実施 全体：目的/目標に対して 個別：情報資産WS中心	▽委員会 ▽内部監査	▽委員会 ▽外部審査	▽委員会 ▽全社セキュリティ研修

ポイント2

計画的に実施（中長期）

昨年度			
1Q	2Q	3Q	4Q
▽委員会	▽委員会	▽委員会	▽委員会
脅威インテリジェンスの共有と組織の対応方針の検討をマネージメントレビューを計画的に実施しておく			

ポイント1

組織を取り巻く状況の変化についてマネジメントレビューを通じてのインプットが重要！

- 脅威インテリジェンスとして情報共有
- 組織としての取り組み方針について継続的にディスカッション
- 組織としての対応の判断材料を集める

まとめ

本日のテーマで取り上げた内容

ホップ

羊と狼の事例

一般論

リスクアセスメントについての**理解の底上げ**

組織全体の底上げ

ステップ

ユースケースによる事例解説

マインドマップ利用による
リスクの特定など

効率化＆品質

リスクトリガーの明確化＆
ベースラインの確保

ステークホルダーとの関係

リスクコミュニケーションの
事例紹介

リスクオーナーとの連携

ジャンプ！

目指すゴール

リスクオーナーが中心となって
実施するリスクアセスメント

**組織全体としてセキュリティ
ガバナンスの維持＆向上**

変化に強い組織づくり

リスクオーナー　　**事務局**

■インプリメンテーション研究会へのお誘い

・毎年、**組織を取り巻く環境の変化に対応したテーマに挑戦！**

テーマ１：　リスクアセスメントについて考える

テーマ２：　委託先管理、どうやってますか?

・気楽に参加可能（情報収集目的の参加でもOK）

一緒にディスカッションに参加しませんか？（組織特有の悩み相談もOK）

冷やかしも大歓迎ですので、気軽にJNSA事務局へご連絡を！

開催形式：ハイブリッド
（リアル会場＋Web会議）

毎月最終木曜日18:00～21:00開催

＋