日本のサイバーセキュリティを「連携」「学び」「創造」

JNSA 2025年度活動報告会

日本ISMSユーザグループ

「標準化動向やインプリメンテーション研究会の活動の情報発信など」

標準化部会　日本ISMSユーザグループ

WGリーダー　魚脇 雅晴

（NTTドコモビジネス株式会社）

2025年7月24日

本日の説明の流れ

1. ISMS-UGの紹介
   - 標準化部会とISMS-UG
   - ISMS-UGの活動（標準化と研究会との関係）
2. 2024年の活動報告
   - 標準化動向（気候変動）
   - インプリメンテーション研究会の活動（リスクアセスメント）
   - LT形式の勉強会
3. 2025年の活動計画案
   - インプリメンテーション研究会の活動（認識合わせ、マネジメントレビュー、DX/AI）
   - 情報セキュリティマネジメントセミナーのご案内（12/5）
   - LT形式の勉強会のご案内（9/2）
4. インプリメンテーション研究会へのお誘い

日本ISMSユーザグループのご紹介

標準化部会のWG　日本ISMSユーザグループ

業種・業界・分野等の標準化・ガイドライン化などを推進する。
特にJNSA目線のセキュリティベースラインの提供、情報セキュリティ対策ガイドラインの策定などを進める。また、国際標準/国際連携との親和性の高い案件については、国際標準への提案やコメント、国際連携案件も視野に入れて、議論を進める。さらに、近年のデジタル化促進にともなる技術要素についても積極的に取り上げ、標準化部会での技術共有や課題抽出を実施していく。

- デジタルアイデンティティWG
- 電子署名WG
- **日本ISMSユーザグループ**
- PKI相互運用技術WG

https://www.jnsa.org/active/std.html

日本ISMSユーザグループの活動目的＆予定

1．WGの活動目的

ISMS認証取得企業（ユーザ）とISMSの専門家が連携し、意見交換・議論を進めることで
ISMSの構築・運用に関わるユーザ視点でのベストプラクティスを提供し、日本における
健全かつ効果的なISMS普及・促進に貢献する活動を行う

2．WGの年間活動予定

・インプリメンテーション研究会におけるISMSの構築や運用における課題検討（毎月）
（メインテーマとして「新規格改定に伴う新規管理策の実装方法について」検討を行う）

・情報セキュリティマネジメントセミナーの開催と研究結果の発表（12月）
・LT（ライトニングトーク）形式勉強会の開催（9月）

日本ISMSユーザグループの活動紹介

標準化動向

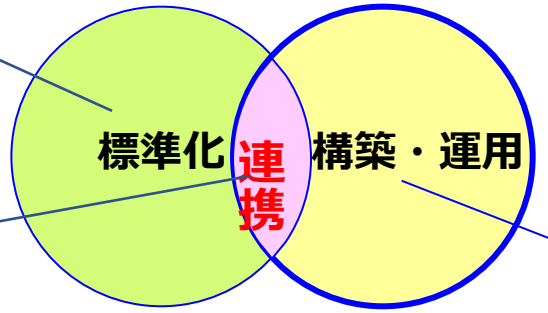
標準化の活用＆定着

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～　ISMSの構築・運用におけるベストプラクティスを検討＆提供　現在

【過去のテーマ名】（2015年以前は省略）

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

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

2024年　**2025年**

■リスクアセスメントについて考える
■委託先管理、どうやってますか?

■認識合わせ
■マネジメントレビュー
■DX/AI

＋

LT形式勉強会（2024年、2025年）

：本日の活動紹介テーマ（抜粋）

■ LT（ライトニングトーク）形式による勉強会

（27000シリーズの最新動向とベストプラクティスの提案）

2024年9月5日（木）13:00～14:00　ハイブリッド開催（ Share Working Studio35　&　zoom）

◆ LT（ライトニングトーク）形式による勉強会◆
ISMSの身近なテーマと未来を考えるテーマ　～気軽に参加してみませんか？～

日本ISMSユーザーグループでは誰でも参加出来る気軽な勉強会を開催します。
今回扱うテーマは2つのテーマを取り上げます。身近なテーマとしては13個の認証組織を1年で１個にした極意（Tips）やディスカッションを予定しています。
また、未来を考えるテーマとしてはNISTが開発したオープンセキュリティ制御評価言語(OSCAL)についてご紹介します。システムのセキュリティ情報をOSCAL で表現することで、セキュリティ評価、監査、および継続的な監視プロセスを自動化出来るかもしれないという最新動向について情報発信&ディスカッション出来ればと考えています。
皆さまとのディスカッションを楽しみしていますので、気軽に参加頂ければ幸いです。

テーマ1：「13個のISMS認証を一年で1個にした話 」

テーマ2：「NIST OSCALが切り開く、ISMSと情報セキュリティの未来」

https://www.jnsa.org/seminar/std/isms/20240905/index.html

■情報セキュリティマネジメントセミナー2024

（27000シリーズの最新動向とベストプラクティスの提案）　2024年12月6日（金）PM

JNSA

【標準化動向】ISO27001、ISO27002などの27000シリーズの標準化の最新動向など
- 「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」
- 「マネジメントシステム規格に追加された気候変動への対応」（本日ご紹介：抜粋版）
- 「OSCALのISMSにおける活用方法」

【研究会成果報告】インプリメンテーション研究会の活動成果
- テーマ1：リスクアセスメントについて考える（本日ご紹介：抜粋版）
- テーマ2：委託先管理、どうやっていますか？

【パネルディスカッション】最新のトピック（気候変動＆OSCAL）についてディスカッション
テーマ1：「気候変動に関わるマネジメントシステム規格の追補版への対応について」（抜粋版）
テーマ2：「NIST OSCALが切り開く、ISMSと情報セキュリティの未来」

講演映像　講演映像をYouTube JNSAChannelで公開中＞＞ JNSA CHANNEL

https://www.youtube.com/playlist?list=PL1nvarmw8MRu8VJ62_6mxEURDH3f_Wwhl

講演資料　https://www.jnsa.org/seminar/std/isms/2024/index.html

標準化動向（気候変動）

標準化動向（気候変動）について

伝えたいこと

・全てのマネジメントシステム（EMS,QMS、ISMS・・・）に気候変動への取り組みが盛り込まれた

・昨年のセミナーの質問の大半（規格の解釈＆実装についての悩み）を占め、パネルでも話題

WHY？（審査機関も認証組織も事例がなく、どのように実装すればよいか悩んでいた）

本日は全体像および解釈と実装の方針（案）について簡単にご紹介します
（詳細はセミナーサイトの質疑応答の掲載情報を参照願います）

ISOのマネジメントシステム規格に気候変動への対応が追加

背景

国連における気候変動への対応を背景に、
2021年9月、ISOは気候変動への取組み方針を
ロンドン宣言として表明
https://www.iso.org/ClimateAction/LondonDeclaration.html

ロンドン宣言を実践する活動の一つとして、2024年2月に、ISOのマネジメントシステム規格に気候変動への対応を追加

1. マネジメントシステム規格に適用する共通の構造（共通の箇条構成、用語及び定義、テキストを含む）の規定（＊）に、気候変動への対応に関する規定を追加
   ＊ ISO/IEC Directives, Part 1, Annex SL

2. 2024年2月に、上述の規定を、ISO 9001、ISO 14001、**ISO/IEC 27001** を含むそれぞれの**マネジメントシステム規格に追補（Amendment）として反映**

気候変動に関する規格解釈の
前提条件＆対応方針について

・ISO/IEC 27001:2022, 4.1 追補の要求事項の解釈について

・ISMS-UGにおける規格の適用や運用についての対応方針

ISO/IEC 27001:2022, 4.1 追補の要求事項について

気候変動については、二つの取り組みがある

（1）「1. a.（気候変動を）人類の課題と認識し、原因に働きかける」取り組みについて

1. a.の課題への具体的な対応は、温室効果ガスの排出削減です。
→この取り組みで対応する課題は、追補に基づき、**ISMSにおいて課題ではないと決定**することになります。
→これは、**ISO/IEC 27001;2022, 4.1における「ISMSの意図した成果を達成する組織の能力に影響を与える」に該当しないため**です。

（2）「2.（気候変動の）結果が組織にもたらす影響に対処する」取り組みについて

- **気候変動をISO/IEC 27001:2022, 4.1における課題であると決定する場合**
  →インプットとして、気温上昇、海面上昇、異常気象などの中で、ISMSで対処が必要になりうる（情報セキュリティリスクアセスメント及び情報セキュリティリスク対応の変更が必要になりうる）状況を挙げることになります。
- **気候変動をISO/IEC 27001:2022, 4.1における課題としない場合**
  →気候変動の結果である気温上昇や海面上昇が、その組織のISMSで実施している情報セキュリティリスクアセスメント及び情報セキュリティリスク対応の変更を必要とする規模のものではないと判断した場合となります。

ISMS-UGにおける規格の適用や運用についての対応方針

選択肢として下記の2点が考えられます。
組織の状況に応じて選択することになりますが、
項番②の方向性が望ましいのではと日本ISMSユーザグループでは考えます。

①気候変動はISMSの課題ではないと判断

課題ではないと判断したことに対する理由を問われた時に説明することが必要となるケースがあります。

②組織として気候変動に対して取り組む（すでに取り組んでいるケースも含む）ことに対してISMSとして連携して気候変動に対して取り組みを行う

気候変動についてはマネジメントシステム全体に気候変動について付記された背景を考慮するとISMSにおいても気候変動の原因に働きかける活動に取り組むことが望ましいと考えます。

注）ただし、気候変動の原因に働きかける活動（温室効果ガス排出削減）の背景に「一般的な意味における気候変動の課題があること（組織として課題として設定）」を理解しておく必要があります。（「ISO/IEC 27001:2022, 4.1（追補を含む）で規定する限定された意味での課題には該当しないこと」）

標準化動向（気候変動）について（詳細についてはこちら）

講演資料

・講演2「マネジメントシステム規格に追加された気候変動への対応」

https://www.jnsa.org/result/isms/seminar/2024/2024-002.pdf

・質問および気候変動に関する規格解釈の前提条件について

https://www.jnsa.org/result/isms/2024/index.html

・パネルディスカッション
テーマ1：「ISO/IEC 27001:2022 における気候変動への対応について」

https://www.jnsa.org/result/isms/seminar/2024/2024-006.pdf

詳細については
こちらを参照

講演映像

講演映像をYouTube JNSAChannelで公開中＞＞ JNSA CHANNEL

https://www.youtube.com/playlist?list=PL1nvarmw8MRu8VJ62_6mxEURDH3f_Wwhl

2024年の活動紹介
インプリメンテーション研究会

■リスクアセスメントについて考える （抜粋版）

■委託先管理、どうやってますか?

2024年　インプリメンテーション研究会　活動2テーマ

テーマ1：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の実践方法に関する提案

今年のテーマは認証組織において永遠の課題であるリスクアセスメントについて取り上げました。こうすれば大丈夫という特効薬や残念ながらありませんが、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機会になればと考えて下記のような方法を提案。

①誰でも理解出来る一般論としてのリスクアセスメント事例紹介（羊と狼）
②実際のビジネスモデルから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

本日ご紹介
（抜粋版）

テーマ2：委託先管理、どうやってますか?

委託先管理を題材に、研究会メンバーでの実態や知見を集め討議した内容をご紹介

ISMS運用で、以下のような思いや悩みを抱いている方、いませんか？

・前任者から引き継いだ仕組みを続けている、大きな問題はない(つもり)
・審査で指摘事項はないけれど、要改善点が無いとは思えない
・今の方法が自組織にとって良いやり方なのか、判断する知見・基準が無い
・他の組織がどのようなやり方をしているのか知る機会が欲しい

リスクアセスメントの成果物のご紹介（抜粋）

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

本日説明（抜粋版）

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

本日説明（抜粋版）

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

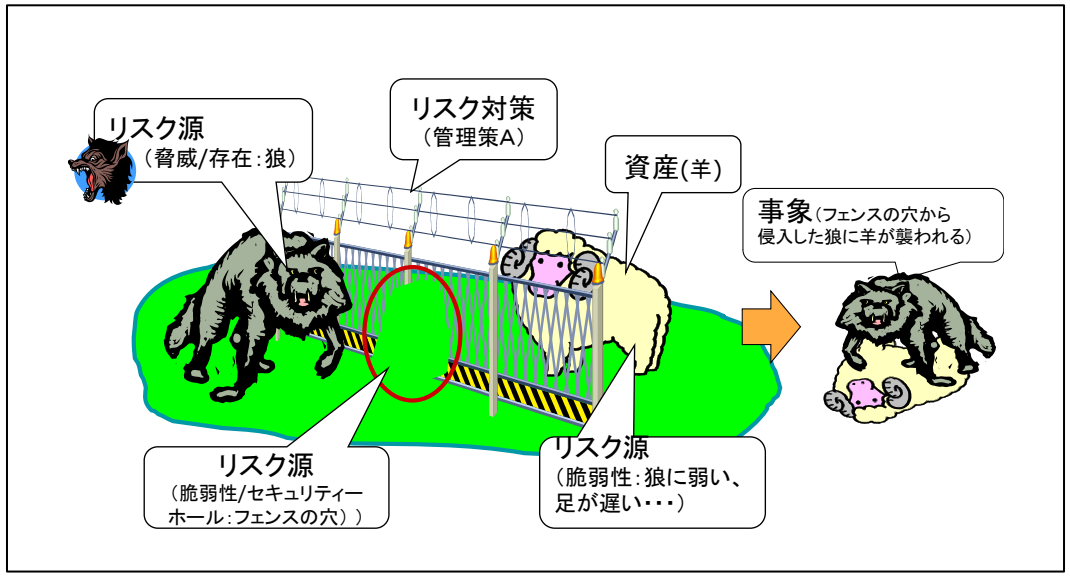
リスクについて考える

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



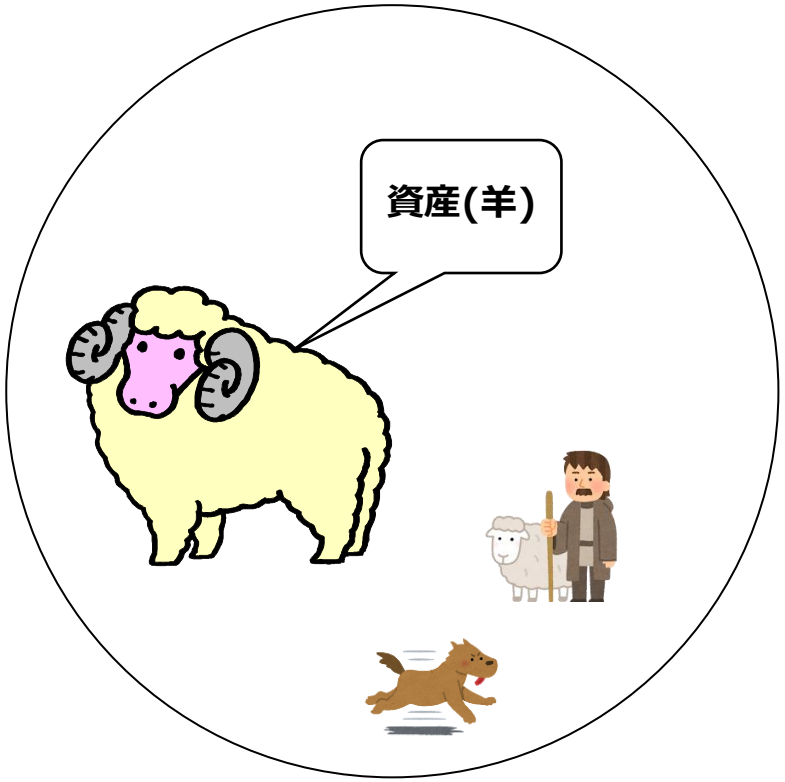
概念ではなく事例で紐解く

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にしてリスクについて考える

攻める側

守る側

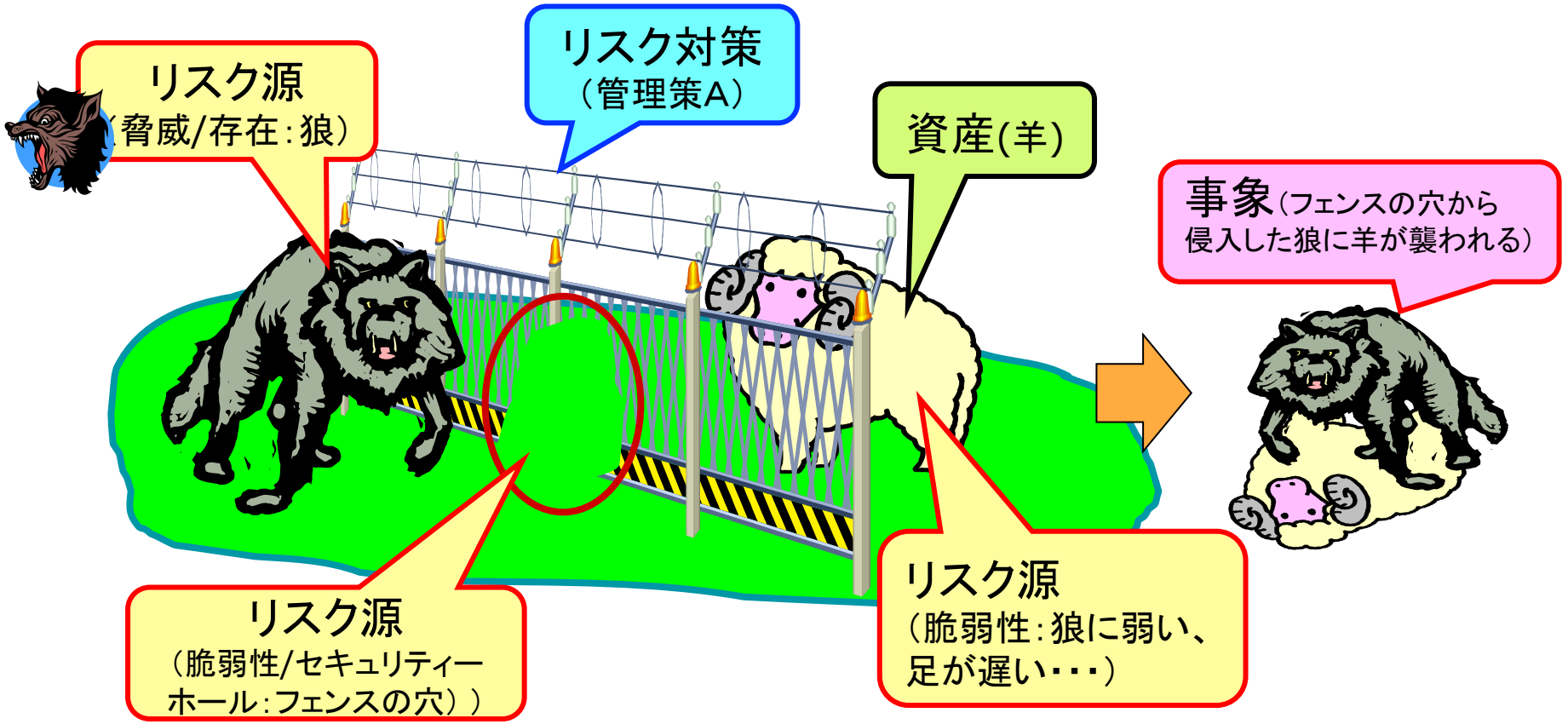


管理策Ａ：狼の侵入を防ぐ柵のなかで保護

リスク源と資産、リスク対策と事象の関係図

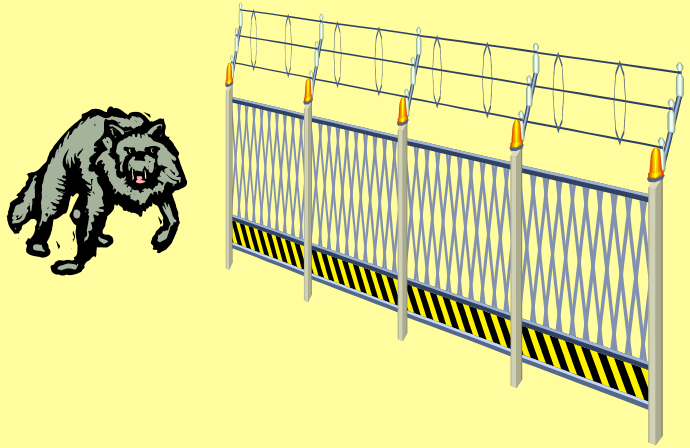
・資産（羊）がリスク源（狼）に襲われるとビジネスリスク（投資が無駄になる）が大きくなる

・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

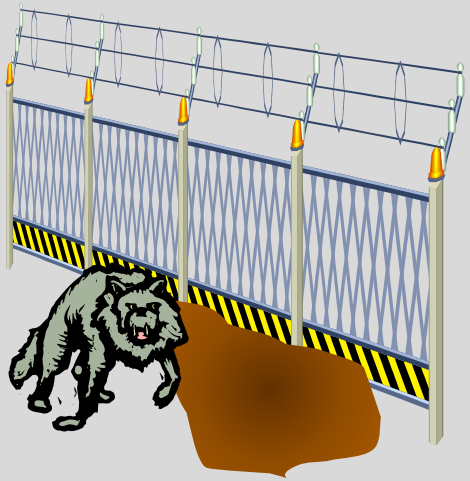


管理策Ａ：狼の侵入を防ぐ柵の比較評価（脆弱性）

適切なリスク対策

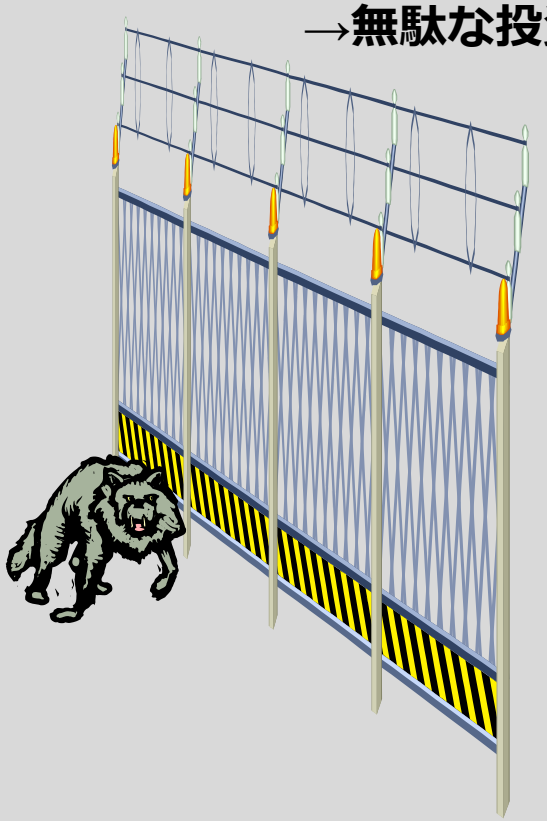


（脆弱性：柵の下の穴）

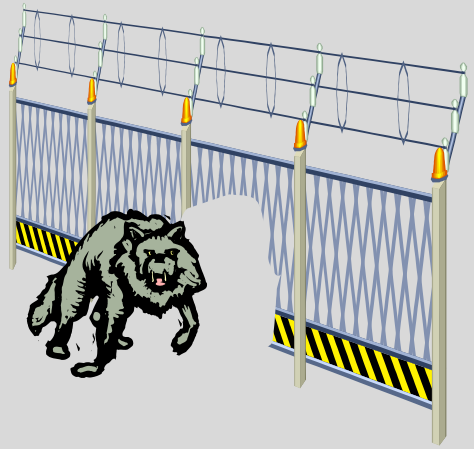


不適切なリスク対策

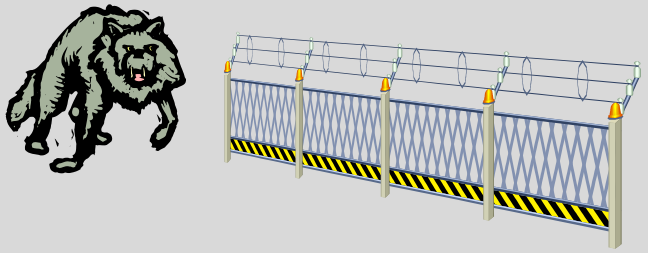
（過剰対策：高すぎる柵）
→無駄な投資



（脆弱性：金網破れの穴）



（過小対策：低すぎる柵）



管理策ＡをISMSの分類で整理してみると・・・

	管理策	分類（ISMS）	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)

リスクアセスメントの成果物のご紹介（抜粋）

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

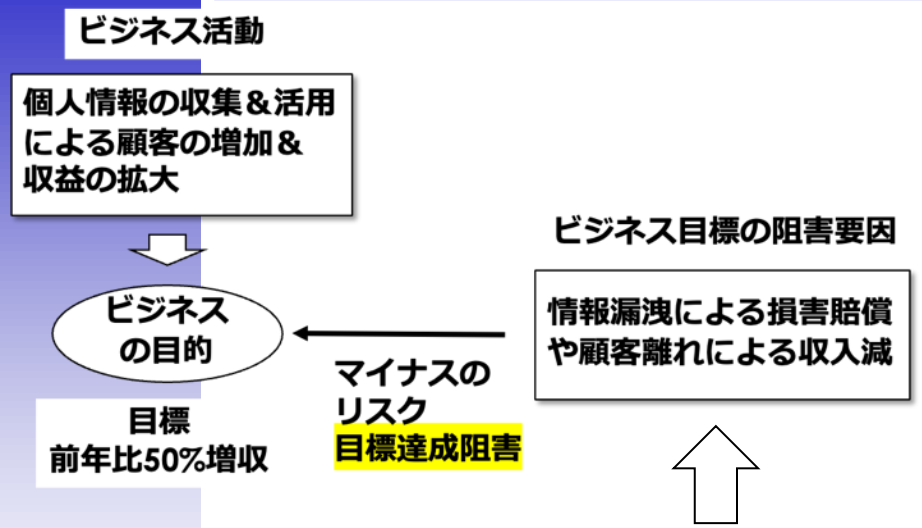
本日説明（抜粋版）

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

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

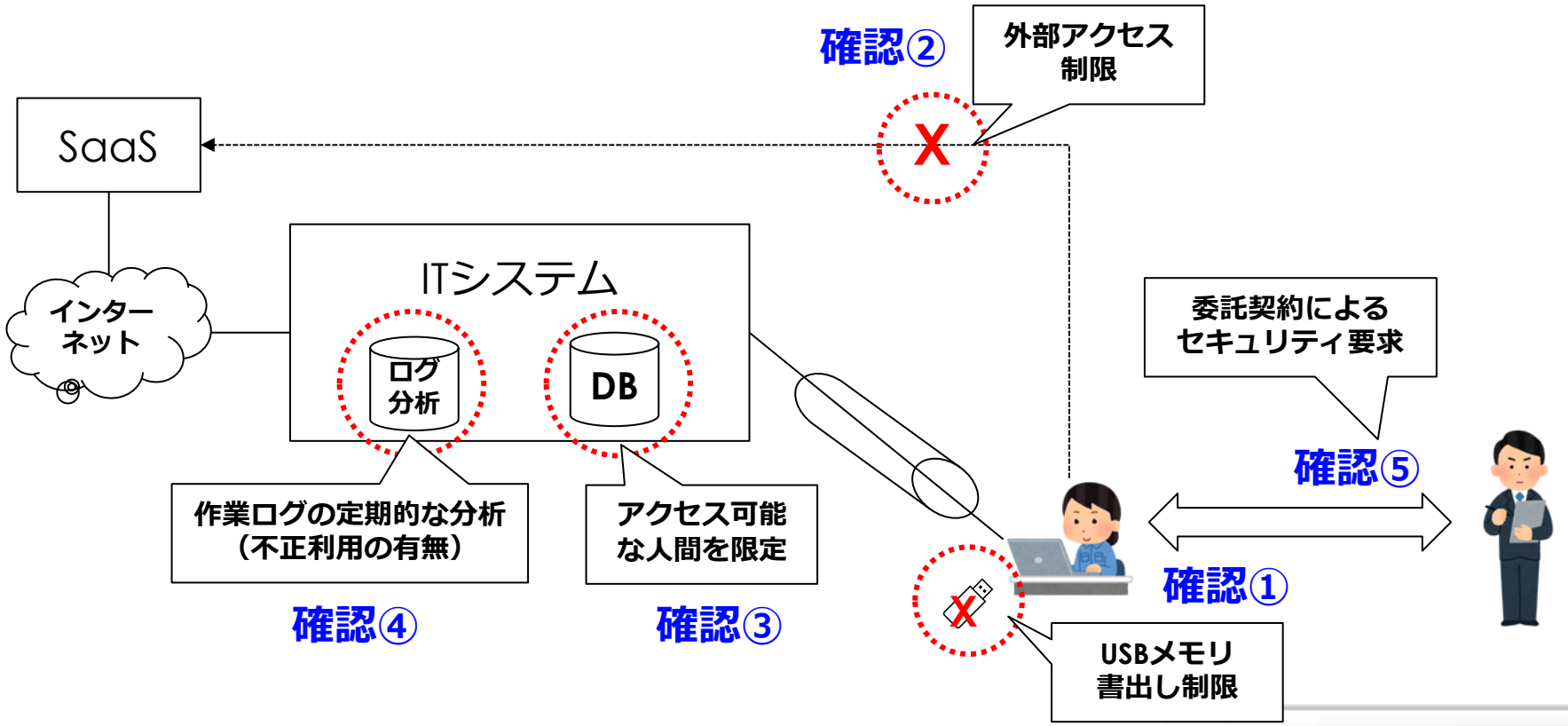
事例 ②

- 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

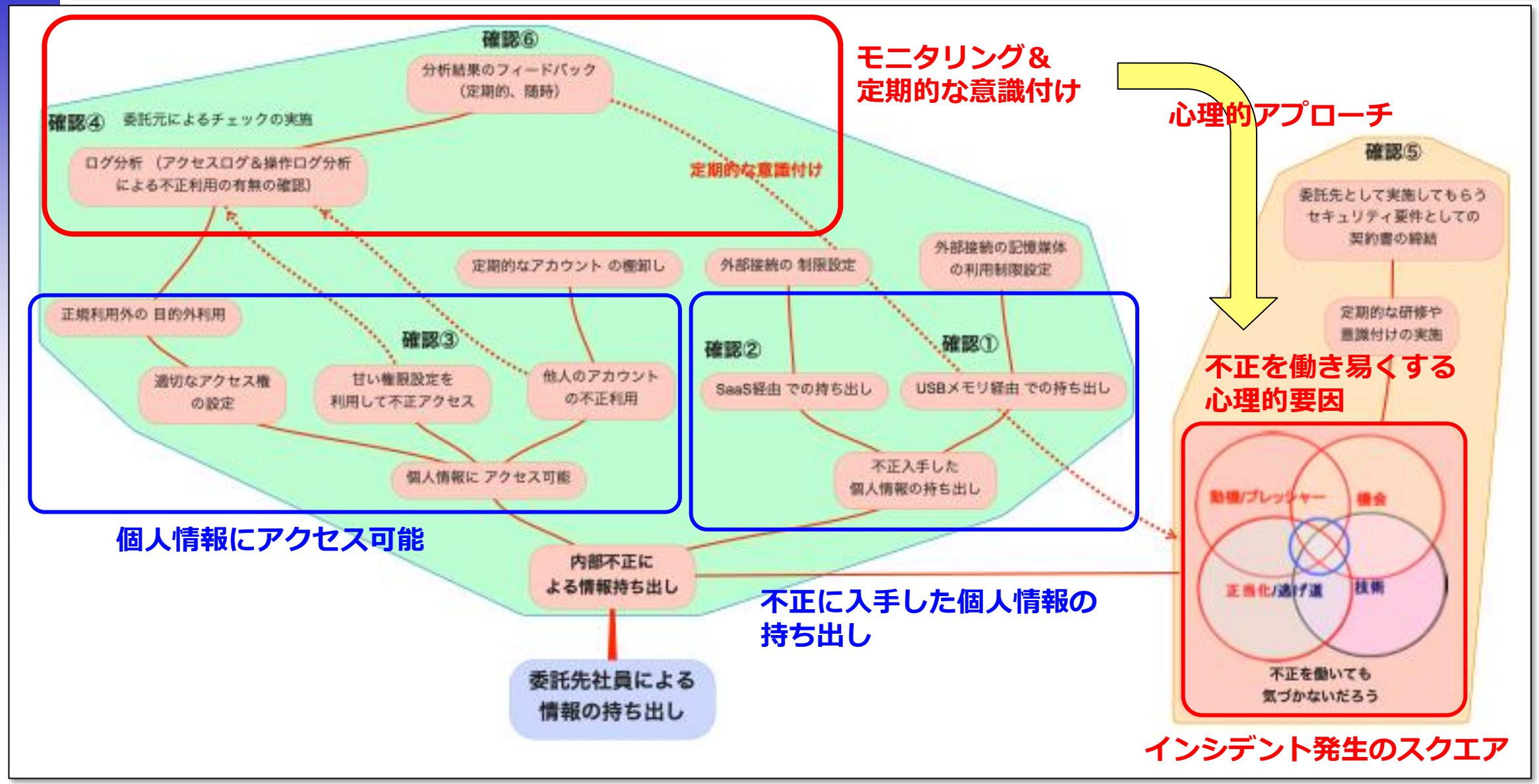
事例②：委託先経由での情報漏洩についてのリスクの特定へのアプローチ

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）

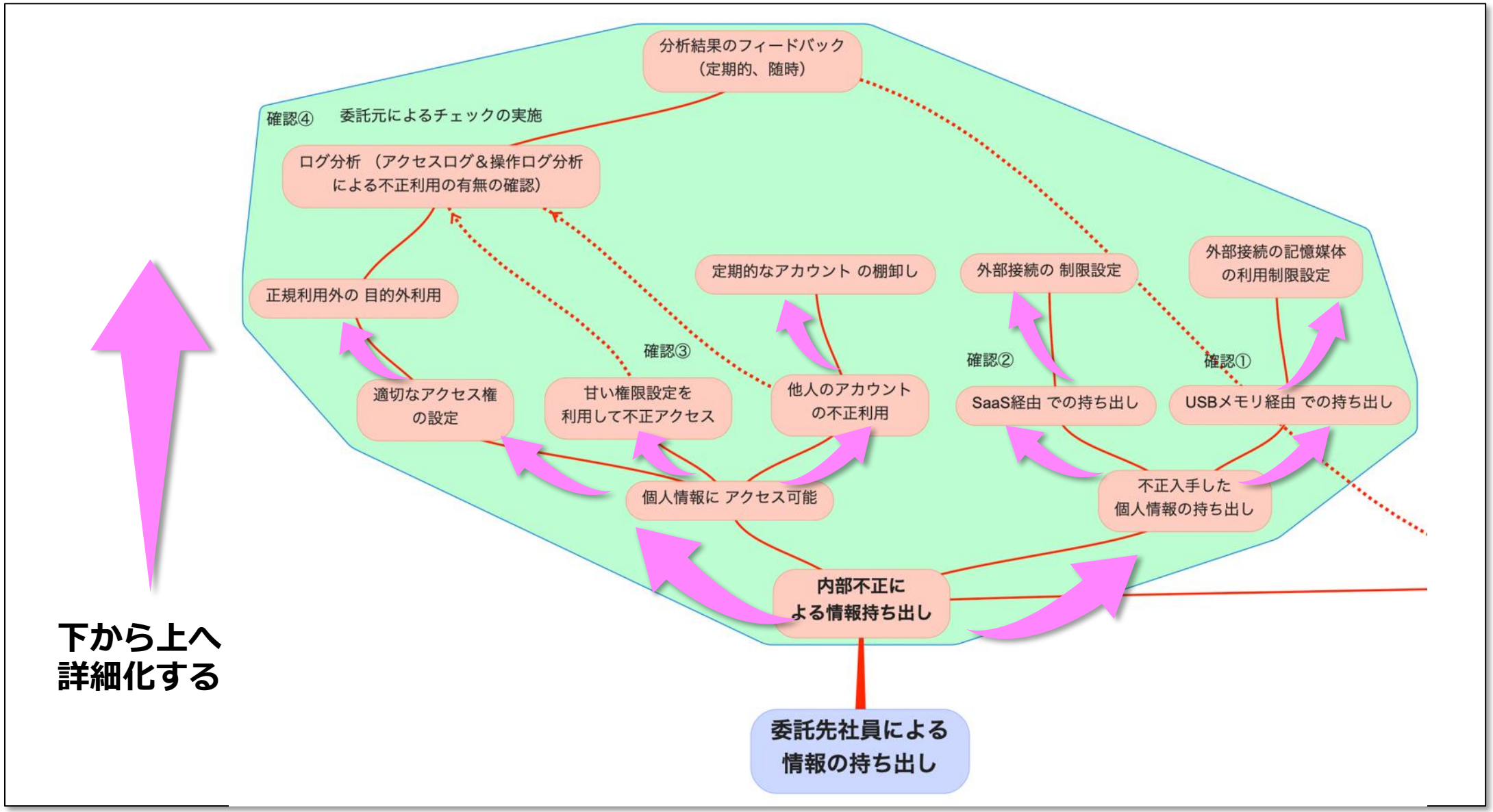


事例②：委託先経由での情報漏洩についてのリスクの特定へのアプローチ

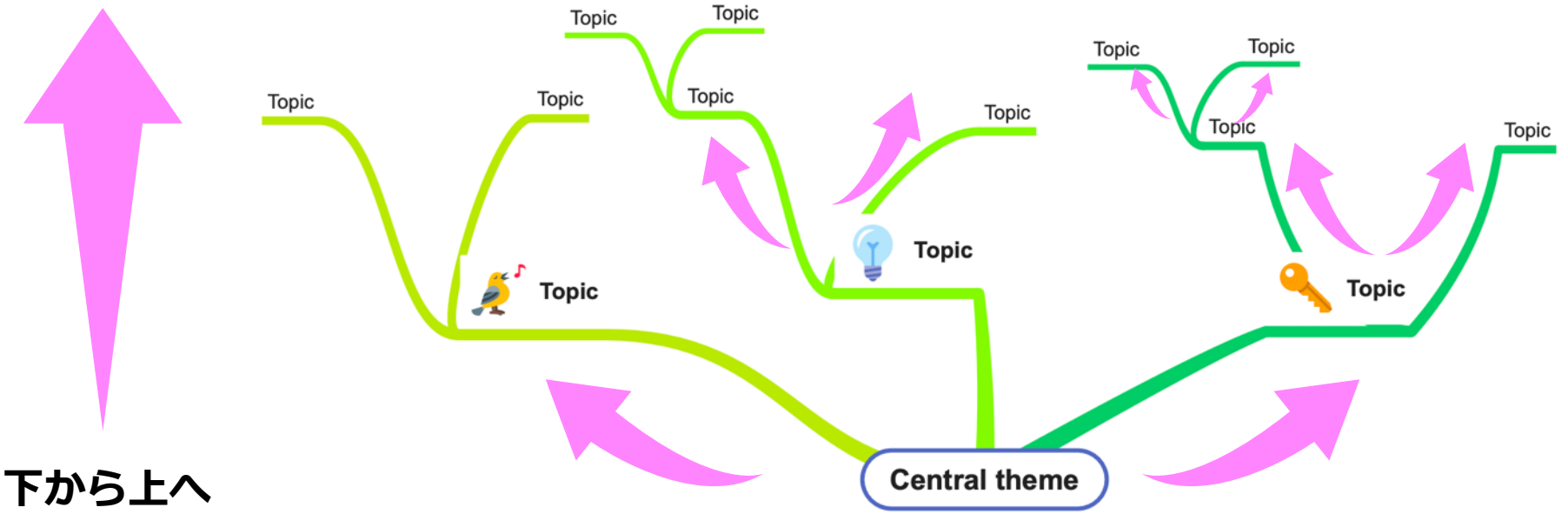


マインドマップによるリスクの特定

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の成果物の狙い

事務局中心に実施されてきたリスクアセスメントを組織全体の活動として取り組めるように誰でも理解出来るような説明資料を作成する

・誰でも理解出来る

・事務局中心から現場と連携したリスクアセスメント

本日ご紹介した範囲（抜粋版）

・リスクアセスメントのトリガーの明確化

・規格要求事項から見た全体像

などなど

■情報セキュリティマネジメントセミナー2024

（27000シリーズの最新動向とベストプラクティスの提案）　2024年12月6日（金）PM

JNSA

【標準化動向】ISO27001、ISO27002などの27000シリーズの標準化の最新動向など

- 「ISO/IEC 27000 関連規格の動向 及び ISO/IEC 27002 ポイント解説」
- 「マネジメントシステム規格に追加された気候変動への対応」
- 「OSCALのISMSにおける活用方法」

【研究会成果報告】インプリメンテーション研究会の活動成果

- 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、どうやっていますか？

本日ご紹介：抜粋版

【パネルディスカッション】最新のトピック（気候変動＆OSCAL）についてディスカッション

テーマ1：「気候変動に関わるマネジメントシステム規格の追補版への対応について」

テーマ2：「NIST OSCALが切り開く、ISMSと情報セキュリティの未来」

詳細についてはこちらを参照

講演映像　講演映像をYouTube JNSAChannelで公開中＞＞ JNSA CHANNEL

https://www.youtube.com/playlist?list=PL1nvarmw8MRu8VJ62_6mxEURDH3f_Wwhl

講演資料　https://www.jnsa.org/seminar/std/isms/2024/index.html

2025年の活動紹介
インプリメンテーション研究会

認識合わせ
マネジメントレビュー
DX/AI

（概要紹介）

■2025年インプリメンテーション研究会の活動　3テーマ

テーマA：認識合わせ

認識の齟齬によるコミュニケーションエラーの事例＆対策に関する提案

各ステークホルダー間の認識違いなどによって発生するISMS関連の無駄稼働の削減＆効率化事例を例示することで認証組織に対する悩み解決の情報提供

テーマB：マネジメントレビュー

マネジメントレビューに関する具体的な事例紹介＆効果的な運用に関する提案

各組織で実施しているマネジメントレビューの実態（議題や付議タイミング）について具体的な運用実態の紹介＆多忙なマネジメント層との効果的なコミュニケーションを模索する

テーマC：DX/AI

「ISMSにおける課題」を解決するためのDX/AI活用に関する提案

「ISMSにおける課題」を解決するためのひとつの模索としてDX/AI活用事例の列挙と深堀りを行うとともに、DX/AIを推進する上での課題を可視化する

■情報セキュリティマネジメントセミナー2025

（27000シリーズの最新動向とベストプラクティスの提案）

開催予告

JNSA

2025年12月5日（金）午後　・・・　詳細は別途、案内予定

【標準化動向】

ISO27001、ISO27002などの27000シリーズの標準化の最新動向など

【研究会成果報告】

インプリメンテーション研究会の活動成果

テーマA：　認識合わせ
テーマB：　マネジメントレビュー
テーマC：　DX/AI

【パネルディスカッション】

最新のトピックについてディスカッション予定

■ LT（ライトニングトーク）形式による勉強会

（27000シリーズの最新動向とベストプラクティスの提案）

2025年9月2日（火）
13:00～14:00　リモート形式

JNSA

開催予告

◆ LT（ライトニングトーク）形式による勉強会◆
ISMSの身近なテーマを題材としたディスカッション　～気軽に参加してみませんか？～

日本ISMSユーザーグループでは誰でも参加出来る気軽な勉強会を開催します。
今回扱うテーマは下記の2つのテーマを取り上げます。
テーマ1はインシデント対応にISMS管理策は役立つか？という問いかけに対して実際にサイバーセキュリティインシデントが発生したとき、インシデントに対応する人と、普段、情報セキュリティマネジメントを運営している人はどのように連携できるのかについて紐解きます。
テーマ2は調達要件等で業界のガイドライン対応が求められている組織に向けて、ISMSが重要である事をガイドラインの比較を交えて解説します。
ひとつの考え方を情報発信し、テーマ毎にディスカッション出来ればと考えています。
皆さまとのディスカッションを楽しみしていますので、気軽に参加頂ければ幸いです。

テーマ1：「サイバーセキュリティ　インシデント発生時の対応とISMS管理策（仮）」

テーマ2：「ISO/IEC27001と国内ガイドラインの違いと融合点の考察（仮）」

■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**して ISMSの構築・運用に
おけるベストプラクティクスを検討しています。
ご興味のある方は一緒に検討に参加頂ければ幸いです。
冷やかしも大歓迎ですので、気軽にJNSA事務局へご連絡ください。

テーマA: 認識合わせ
テーマB: マネジメントレビュー
テーマC: DX/AI

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

＋