JNSA 2024年度活動報告会

日本ISMSユーザグループ

インプリメンテーション研究会活動報告

「 JISQ27001:2023の新規管理策の実装方法についての考察など 」

標準化部会　日本ISMSユーザグループ
WGリーダー　魚脇 雅晴
（エヌ・ティ・ティ・コミュニケーションズ株式会社）

活動報告内容

1. 日本ISMSユーザグループのご紹介

2. 2023-2024の活動概要（インプリメンテーション研究会）

   -2023年： ISO/IEC 27001:2022の新規管理策の実装方法についての考察

   -2024年： リスクアセスメントについて考える（仮）

3. 2024年の開催イベントのお知らせ

   - 2024年情報セキュリティマネジメントセミナー開催（2024年12月6日開催予定）

   - 2024年： LT（ライトニングトーク）形式による勉強会（ 2024年9月5日開催予定）

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/2023/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）**

5

日本ISMSユーザグループの活動紹介

標準化動向

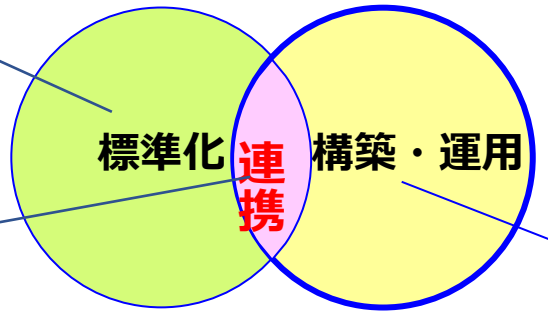
標準化の活用＆定着

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）

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

2023年

- **■ISO/IEC 27001:2022の新規管理策の実装方法についての考察**
- ■続・内部監査

2024年

- **■リスクアセスメントについて考える**
- ■委託先管理（仮）

：本日の活動紹介テーマ（抜粋）

2023年の活動紹介
インプリメンテーション研究会

ISO/IEC 27001:2022の新規管理策の実装方法についての考察

（抜粋版）

テーマとして選んだ背景

- ISO/IEC27001が2022年10月に改訂
- 認証組織ではJISQ27001：2015からJISQ27001：2023への移行が大きなイベント
- 新規の管理策が11個あるので要求事項を正しく理解した実装が必要

ISO/IEC 27001:2022の新規管理策の実装方法についての考察

ISO/IEC 27001:2022, Annex Aの新規管理策（11個）

新規: **11個**

統合: **24個**
更新: **58個**
削除: **0個**

	新規管理策
1	**5.7 脅威インテリジェンス（抜粋）**
2	5.23 クラウドサービス利用における情報セキュリティ
3	5.30 事業継続のための ICT の備え
4	7.4 物理的セキュリティの監視
5	**8.9 構成管理 （抜粋）**
6	**8.10 情報の削除 （抜粋）**
7	8.11 データマスキング
8	8.12 データ漏えいの防止
9	8.16 監視活動
10	8.23 ウェブフィルタリング
11	8.28 セキュリティに配慮したコーディング

新規管理策11個の実装要件を整理（指針＆考え方）

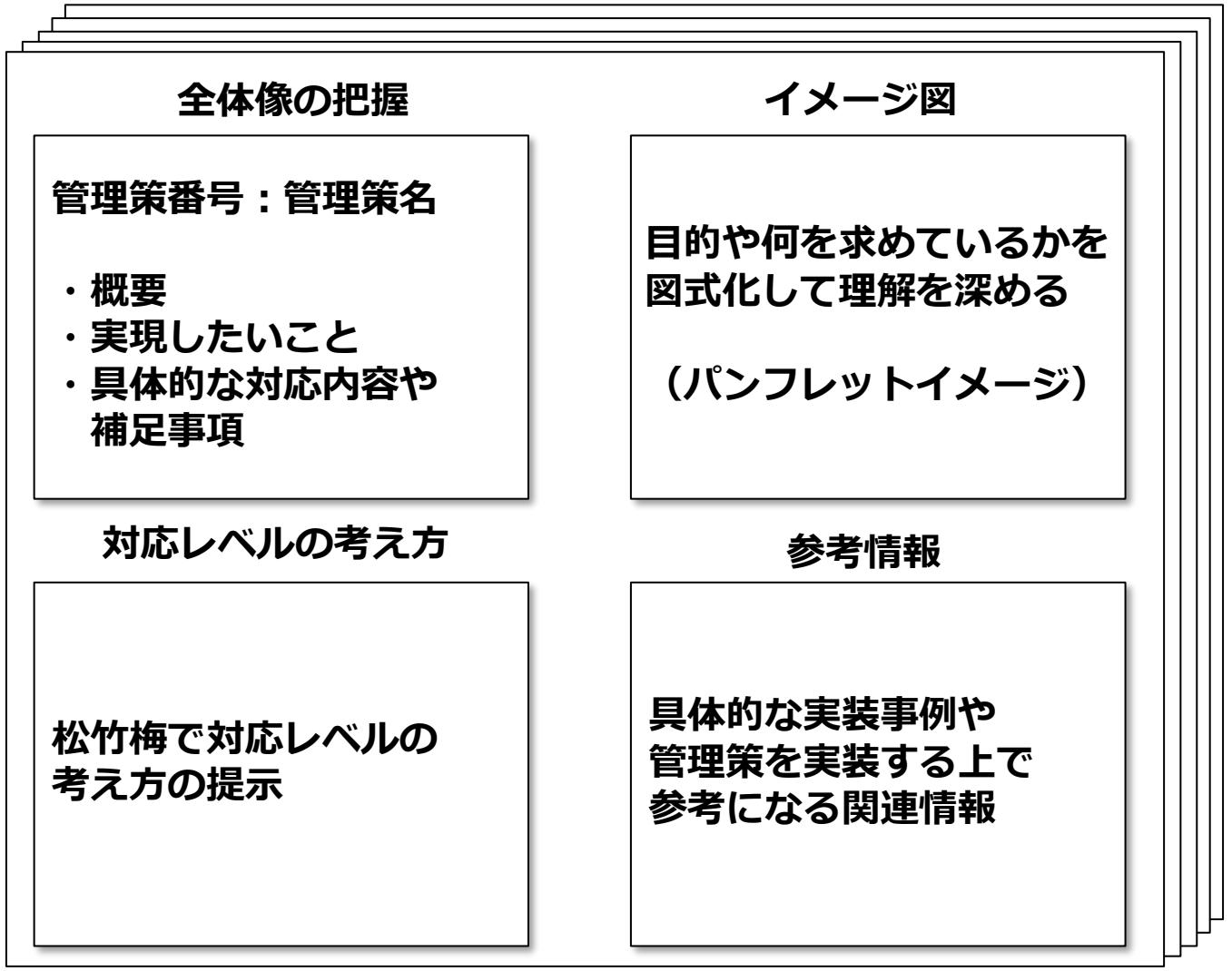
実装についてはベストプラクティスではなく松竹梅などのレベルに応じたものを提案（特に梅に注力）

管理策の種類	管理策数
5 組織的管理策	37個
6 人的管理策	8個
7 物理的管理策	14個
8 技術的管理策	34個
合計	**93個**

114個（旧） → 93個（新）

新規管理策の説明の全体フレームワーク

新規管理策の説明をする上で下記のようなテンプレート構成で資料化しています



新規管理策11個の解説＆実装の考え方について提案

規格要求事項から見た整理

抜粋版

5.7 脅威インテリジェンス

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」の研究対象として取り上げます

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

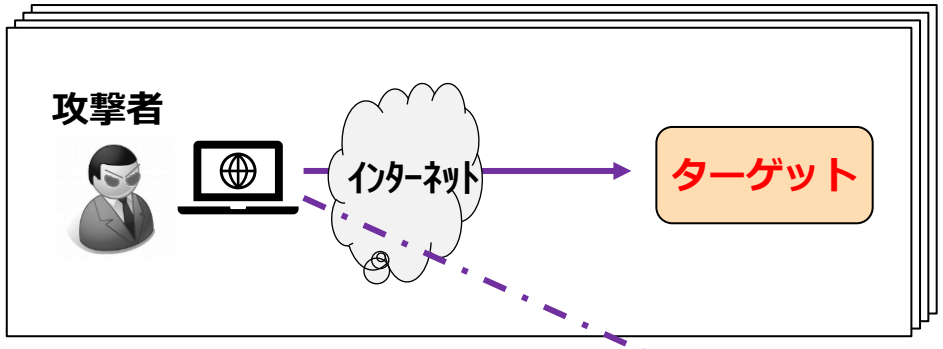
・脅威インテリジェンスは、攻撃者の動機、標的、攻撃手法を理解して対応するために収集・分析されたデータ

・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

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

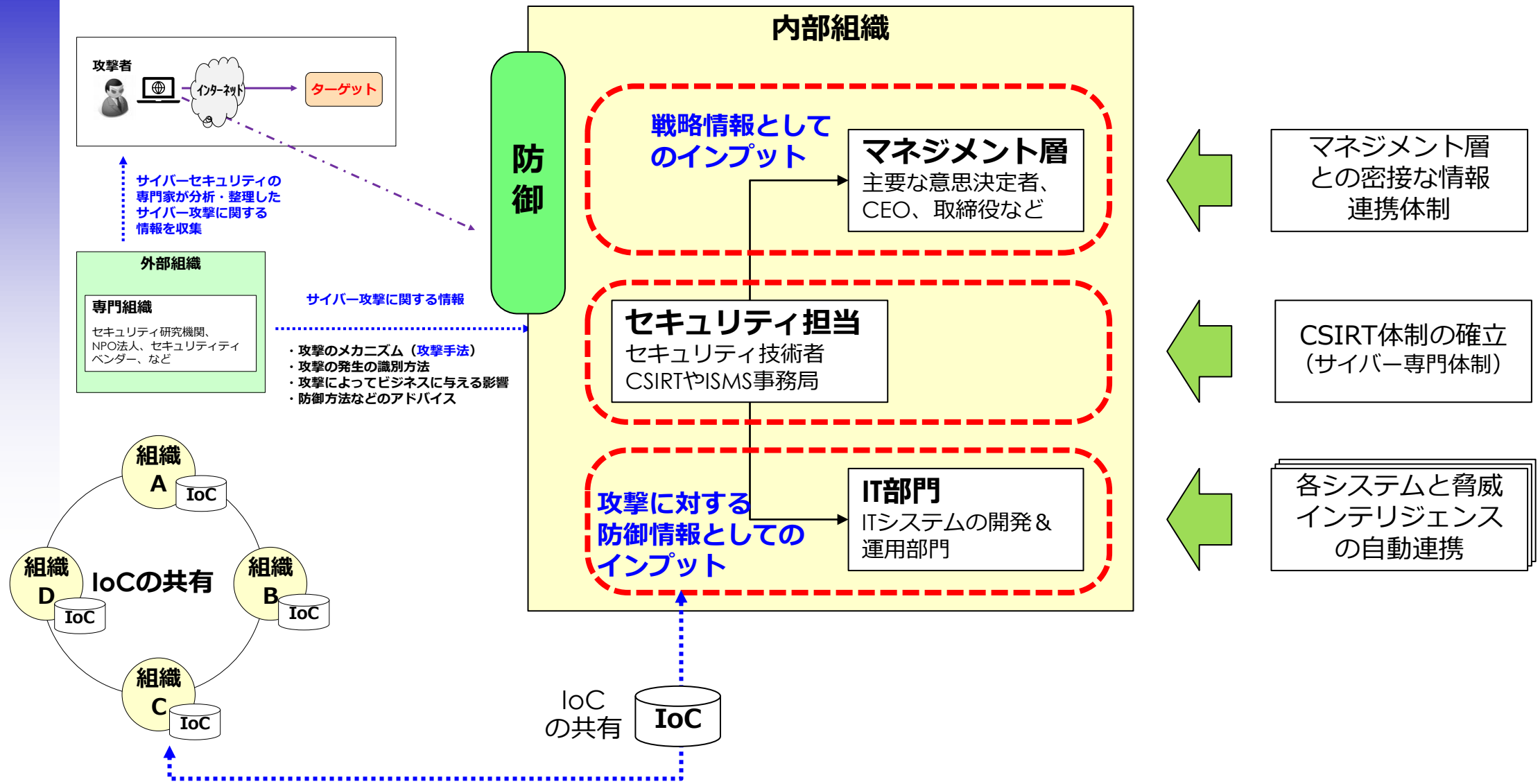
セキュリティ担当
セキュリティ技術者
CSIRTやISMS事務局

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

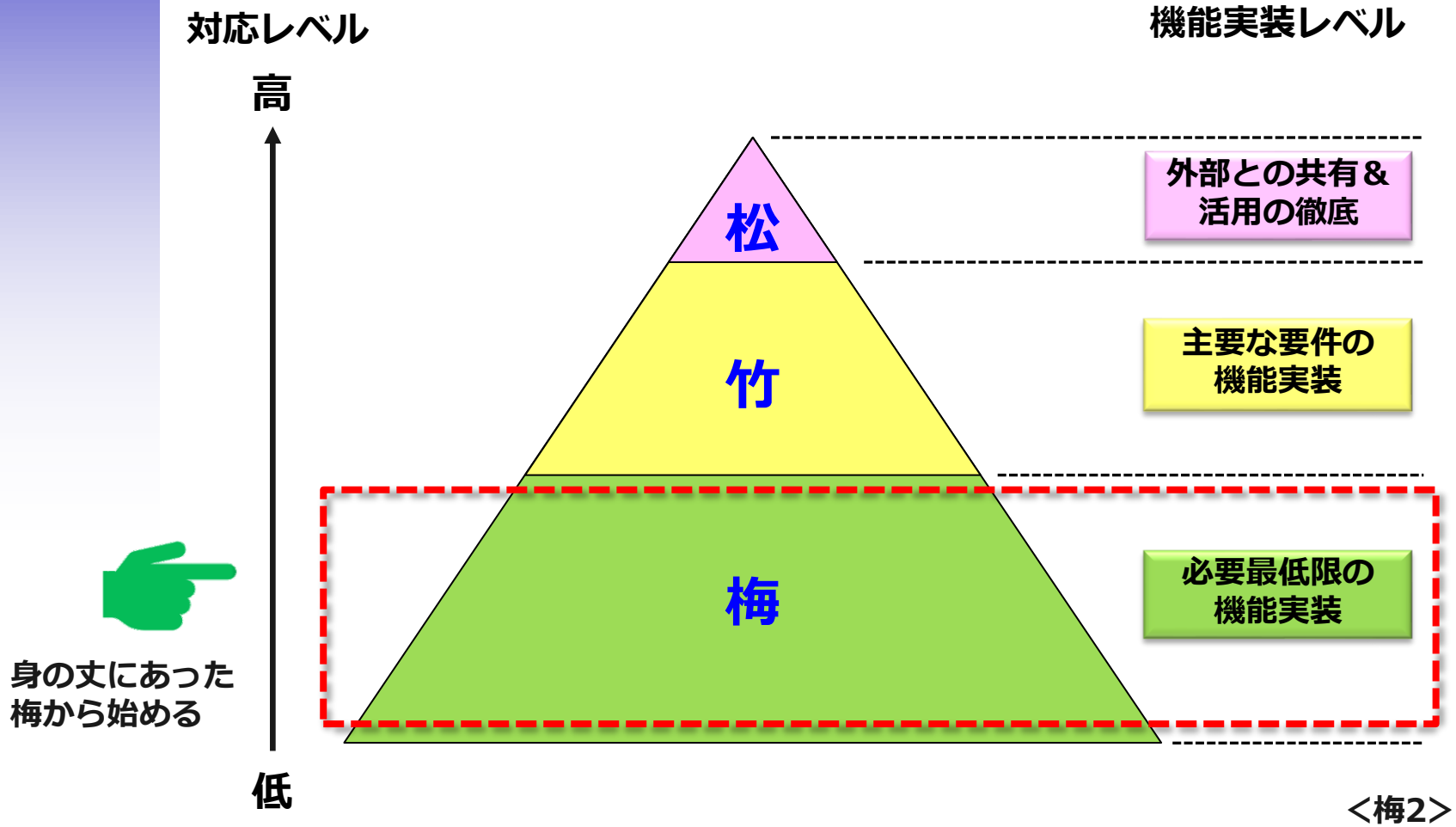
参考情報

脅威インテリジェンスの目指す姿（案）



脅威インテリジェンスの対応レベルについての考え方（案）

組織特性毎の脅威インテリジェンスの管理レベル（案）



規格要求事項から見た整理

抜粋版

8.9　構成管理

8.9 構成管理（要約）

概要

システム（※1）がどのような構成＆設定（セキュリティ設定含む）で動作しているかを再構築可能な形で情報として文書化し、実装し、監視＆レビューすること

※1： HW、SW、サービス（クラウド含む）及びNW

実現したいこと

構成情報を管理することで下記を実現する

- セキュリティ設定の抜け漏れを防ぐ
- ぜい弱性の影響の判定を迅速化する
- 不正な変更の検知を容易にする
- 不正な変更や機器故障などでシステムが損傷した場合の復旧を容易にする

具体的な対応内容や補足事項など

- システムやサービスが必要なセキュリティ設定で正しく機能すること確実にするために構成管理情報を文書やツールなどにより適切に管理を行う

- 構成情報や設定が不適切に変更されたり、意図せず変更されないように変更管理を行うとともに監視、レビューを定義実施する

  主な実施者：システム管理者や運用管理者など

＜情報の例示＞

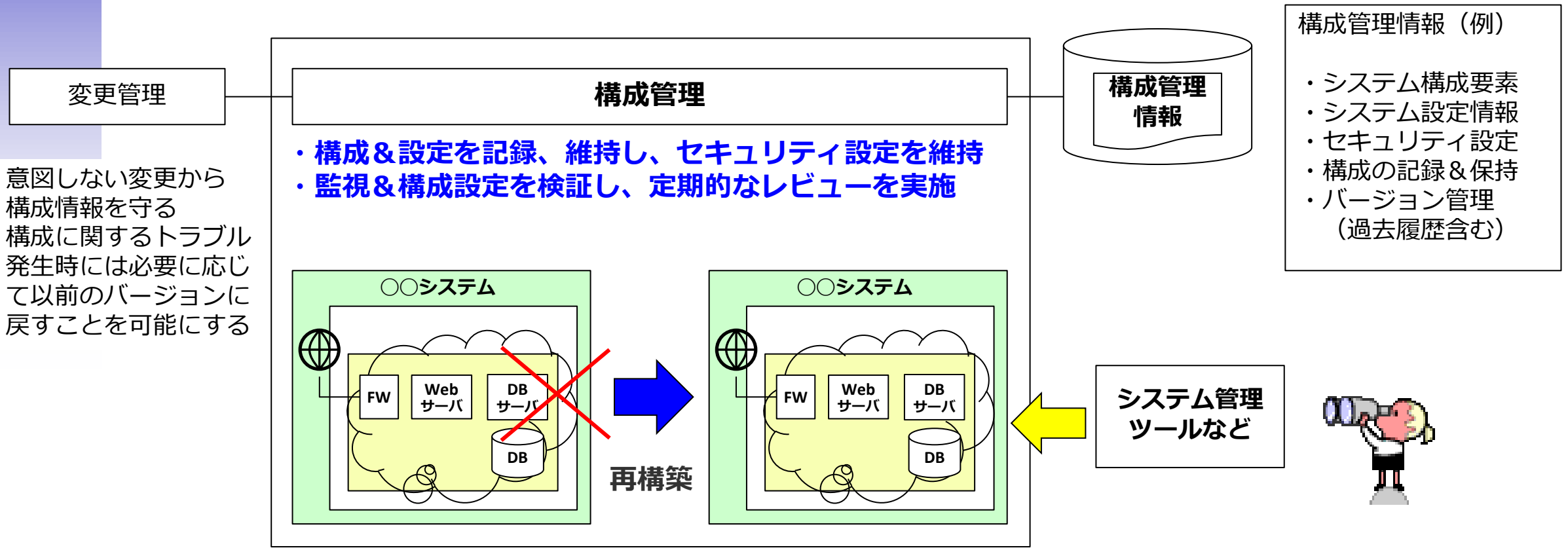
- システム（※1）の構成および設定情報
- セキュリティ設定情報

など

※1： HW、SW、サービス（クラウド含む）及びNW

8.9 構成管理（イメージ図）

システム（※1）がどのような構成＆設定（コンフィグレーション）で動作しているかを、再構築可能な形で情報として記録＆管理すると共にセキュリティ設定を維持すること
システム管理ツール等により監視する＆構成設定を検証し、定期的にレビューする



※1： HW、SW、サービス（クラウド含む）及びNW

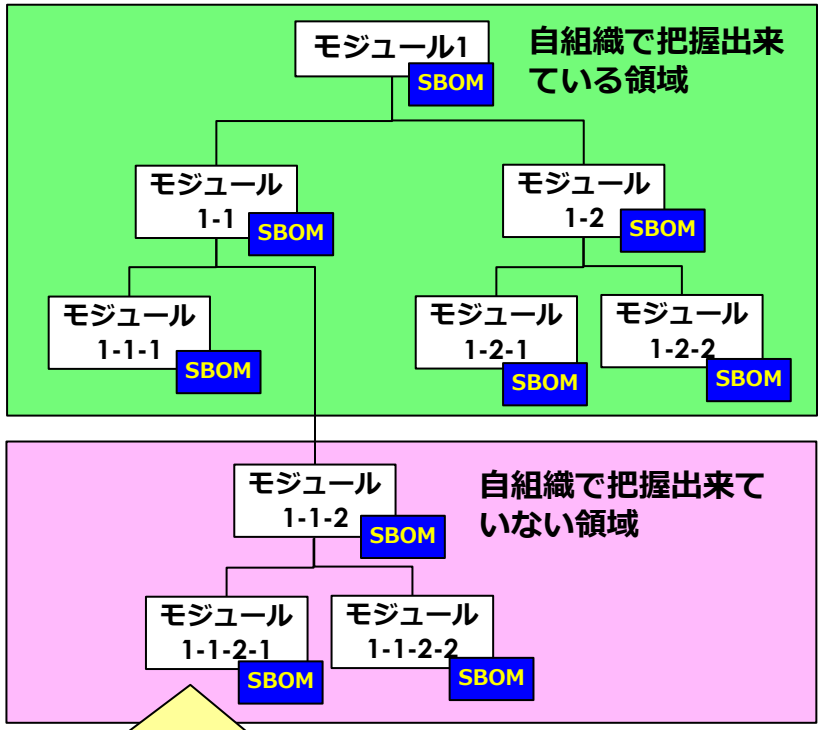
SBOM（Software Bill of Materials）*1ツールの活用

ソフトウェアを構成する部品の一覧情報を**ライセンスや脆弱性に係るリスクの把握に活用**する

ソフトウェアサプライチェーンに提供する価値

	既存の問題点（SBOM導入前）	解決の方向性（SBOM導入後）
透明性	含まれているソフトウェア部品の一覧情報がないため、脆弱性の影響有無や適用されるライセンスを正確に把握できない	ソフトウェアを構成する部品の一覧情報に基づいて**ライセンスや脆弱性に係るリスクを正確に評価**することが可能
完全性	不正コードやマルウェアの混入を検知することができない	ハッシュ値に基づいて**ソフトウェアの改ざん有無を検証**することが可能
識別性	共通脆弱性識別子（CVE）が作成され、影響を受けるソフトウェアの共通プラットフォーム一覧（CPE）が提供されるが、自身が利用するソフトウェアとの対応を特定しにくい	ソフトウェアIDを用いてより**正確にソフトウェアを特定**することが可能

ソフトウェアA



自組織で開発したモジュール

他組織で開発したモジュールを構成部品として利用（OSSなど）

「SBOMの提供が無ければモジュール1-1-2の利用までしか把握出来ないため、モジュール1-1-2-1や1-1-2-2に脆弱性が発見されたとしても自組織が影響を受けるかどうか把握出来ない」

＊1：製品に含まれるすべてのソフトウェアコンポーネント、ライセンス、依存関係を一覧化したもの

抜粋版

規格要求事項から見た整理

8.10 情報の削除

8.10 情報の削除（要約）

概要

個人情報などの機微な情報は長期間保有するほど管理主体が不明確になり情報漏洩や流出のリスクが高くなるため、保有期限が過ぎた時点で適時削除を実施しなければならない

実現したいこと

漏えいすると組織に影響を与える可能性のある情報について法令・規制要求事項と契約上の義務の順守及び業務上の必要性から保有期限（削除・廃棄期限）を定め、適時削除することで情報の保有リスクを低減する

具体的な対応内容や補足事項など

・組織全体として機密情報の保有期限を定めることにより、統一的なマネジメントプロセスを構築する

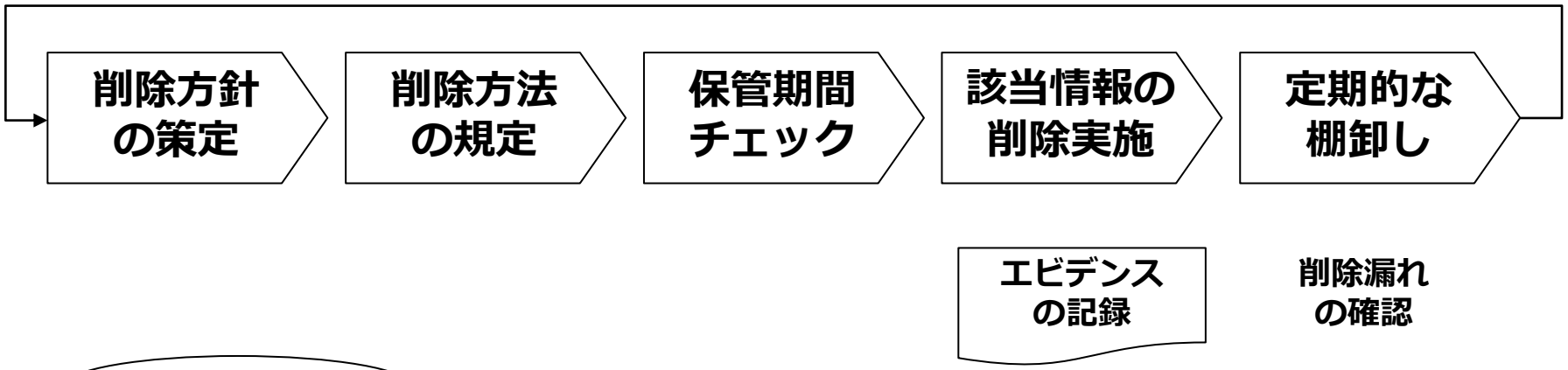
・ビジネスの現場において情報資産台帳に保有期限を掲載し、定期的に削除プロセスを実施することによる漏洩リスクの低減を図る

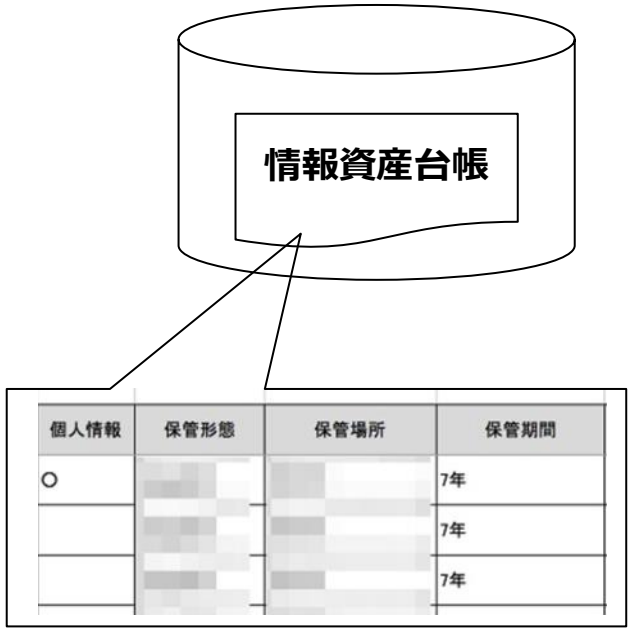
＜削除における考慮事項＞

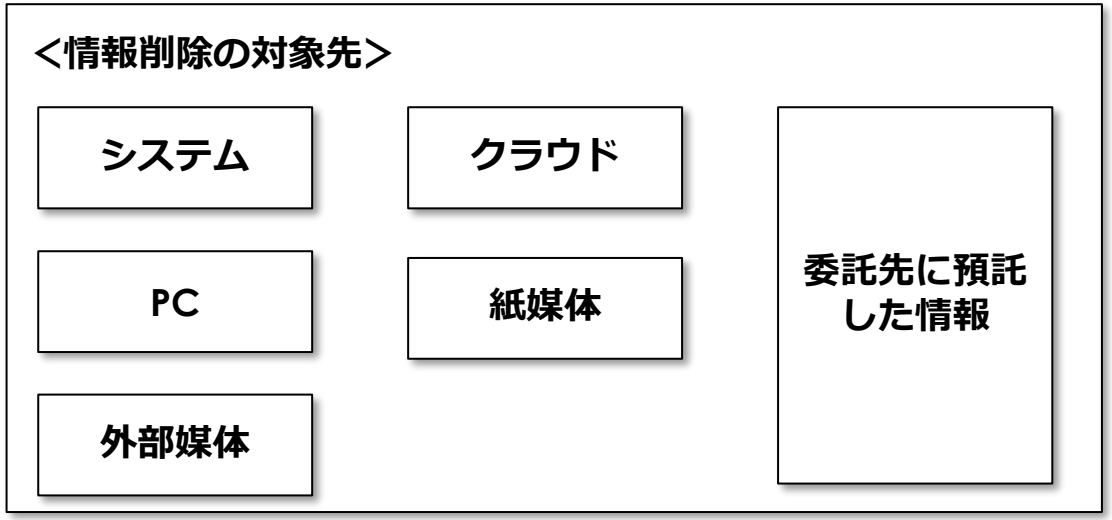
・情報の削除方針の明確化（情報の種類、機密レベル、業務上＆法律要件を加味）
・削除方法の規定
・エビデンスの記録
・システムや委託先の保管情報も加味
・定期的な棚卸しによる削除漏れ防止

8.10 情報の削除（イメージ図）

情報削除のプロセス

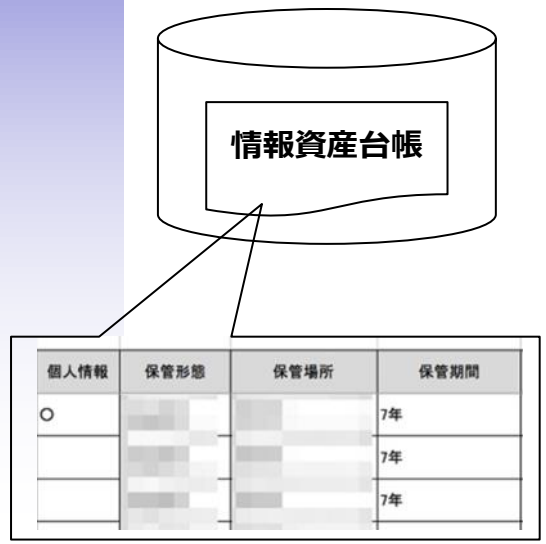






情報の削除における留意事項（その2）

情報の保管期間についてはそれぞれの情報の特性に応じた対応が求められると共に削除対象の情報を特定するためには業務プロセスへの組み込みが必要
（情報作成時から○年間というように単純化出来ない）



情報（例）	保管期間	起算日	備考
契約書	10年	契約の満期日や解約日から起算	会社法により10年間保管（各事業年度の確定申告時に青色申告書を提出している法人）
	7年		法人税法施行規則により7年間保管（帳簿書類や取引で作成・受領した各種書類も7年間保管）
人事情報（履歴書）	5年	退職の日から起算	労働基準法 法改正の経過措置として「当分の間は３年間」
雇用保険の被保険者に関する書類	4年	被保険者がその事業所に在籍しなくなった日	雇用保険法施行規則

起算日の考え方に考慮した
削除タイミングの設定が必要

2023年活動の情報発信　（講演資料＆動画配信）

1. 情報セキュリティマネジメントセミナー2023資料（JNSAサイト掲載情報）

・標準化動向

「ISO/IEC 27000 ファミリー規格の動向及びISO/IEC 27002管理策について」
「ISO/IEC 27001及びISO/IEC 27002の活用」　– 情報セキュリティ管理策を軸に –

・インプリメンテーション研究会

「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?」

2. セミナー＆パネルディスカッション動画配信（Youtube）

講演映像をYouTube JNSAChannelで公開中＞＞ 

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

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（仮）

（抜粋版）

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下記の観点で再整理＆ディスカッション中
（シンプルに下記のよう方向性で模索）

1. リスクとは？

2. ISMSの活動の中での営み

3. リスクコミュニケーションについて考える

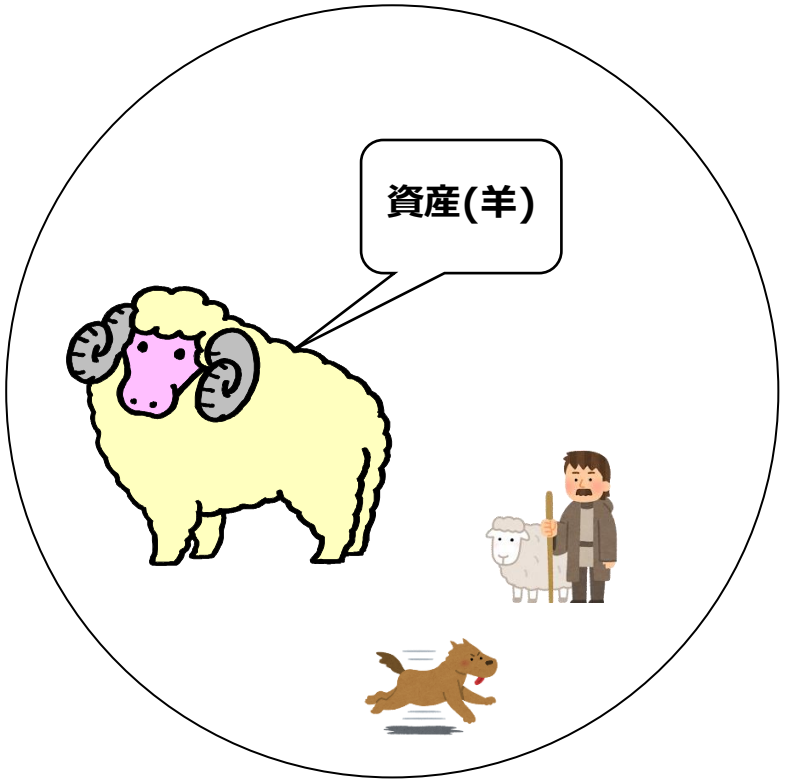
など・・・

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

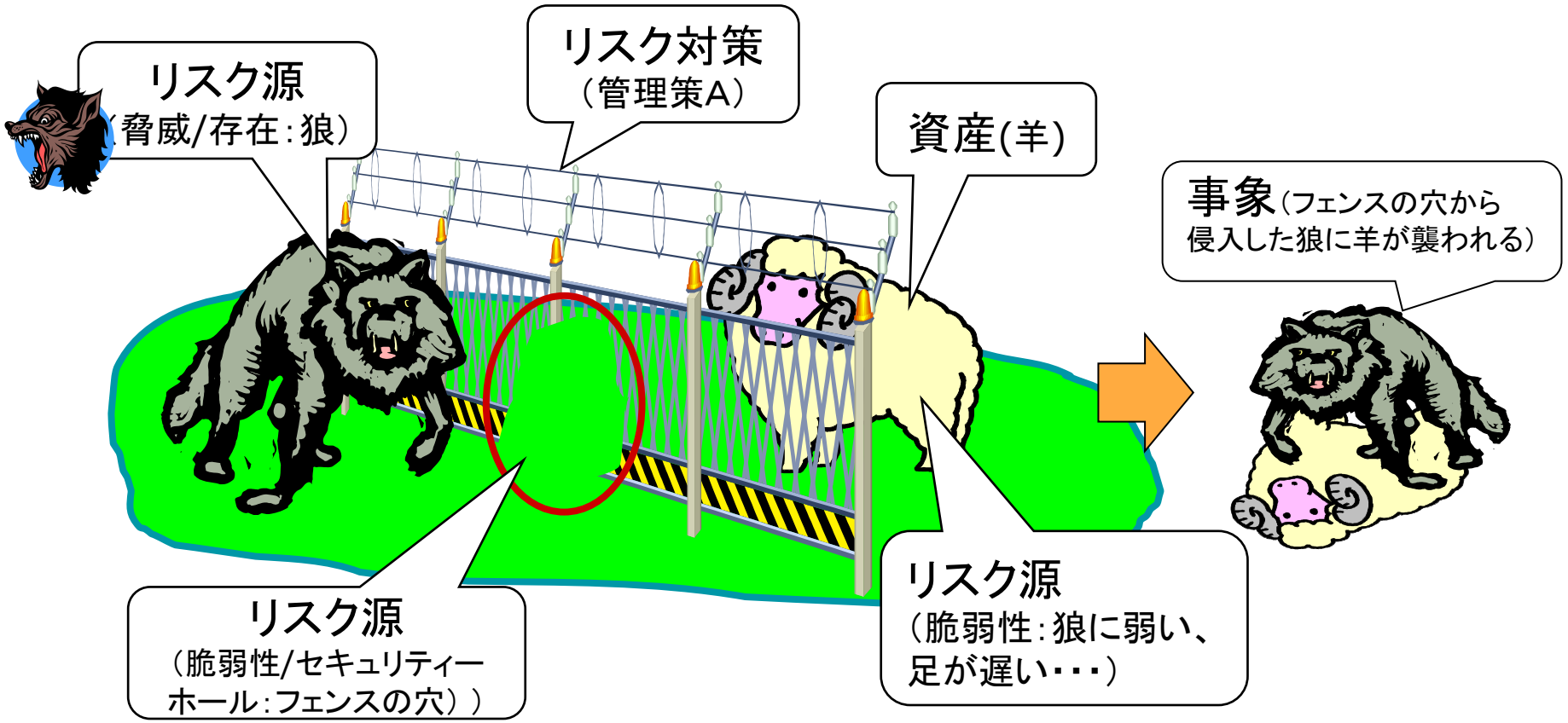
守る側



管理策A：狼の侵入を防ぐ柵のなかで保護

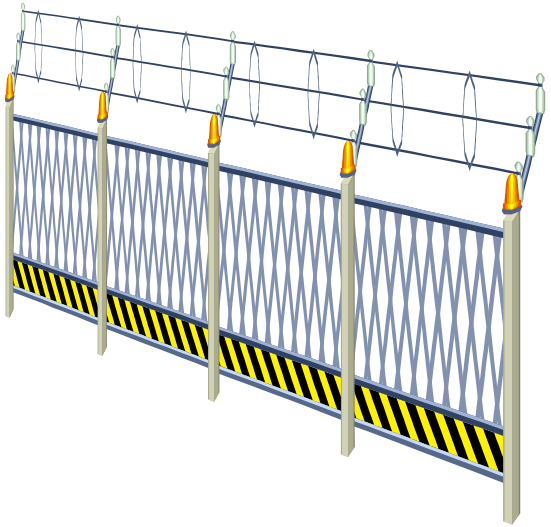
リスク源と資産、リスク対策と事象の関係図

・資産（羊）がリスク源（狼）に襲われるとビジネスリスク（収益が減る）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



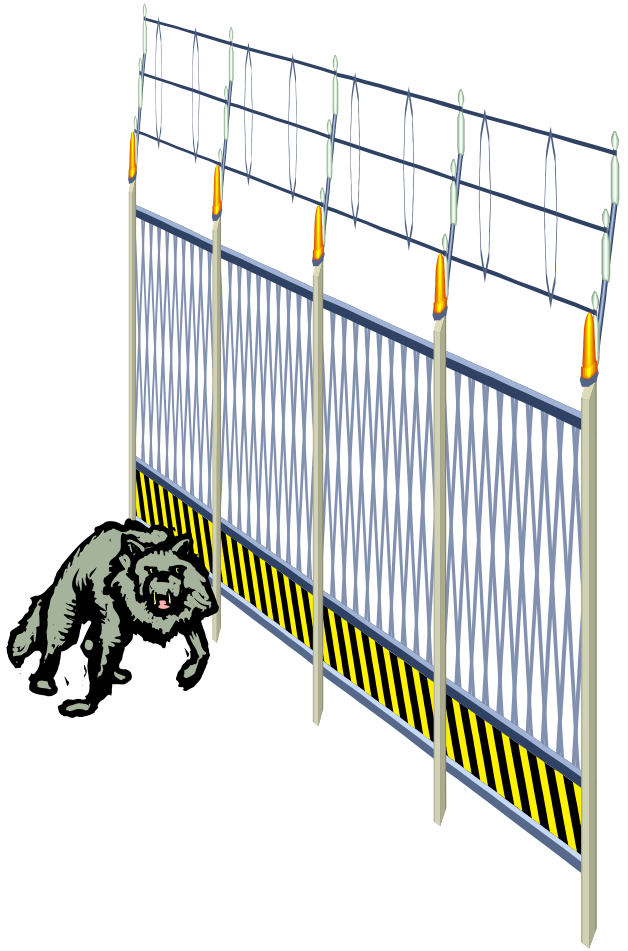
管理策Ａ：狼の侵入を防ぐ柵の比較評価（脆弱性）

適切なリスク対策

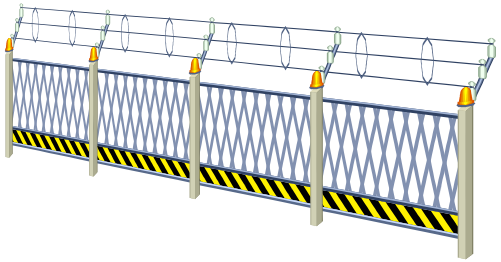


不適切なリスク対策
（脆弱性：塀の下の穴）

不適切なリスク対策
（過剰対策：高すぎる塀）
→無駄な投資



不適切なリスク対策
（過小対策：低すぎる塀）



不適切なリスク対策
（脆弱性：金網破れの穴）

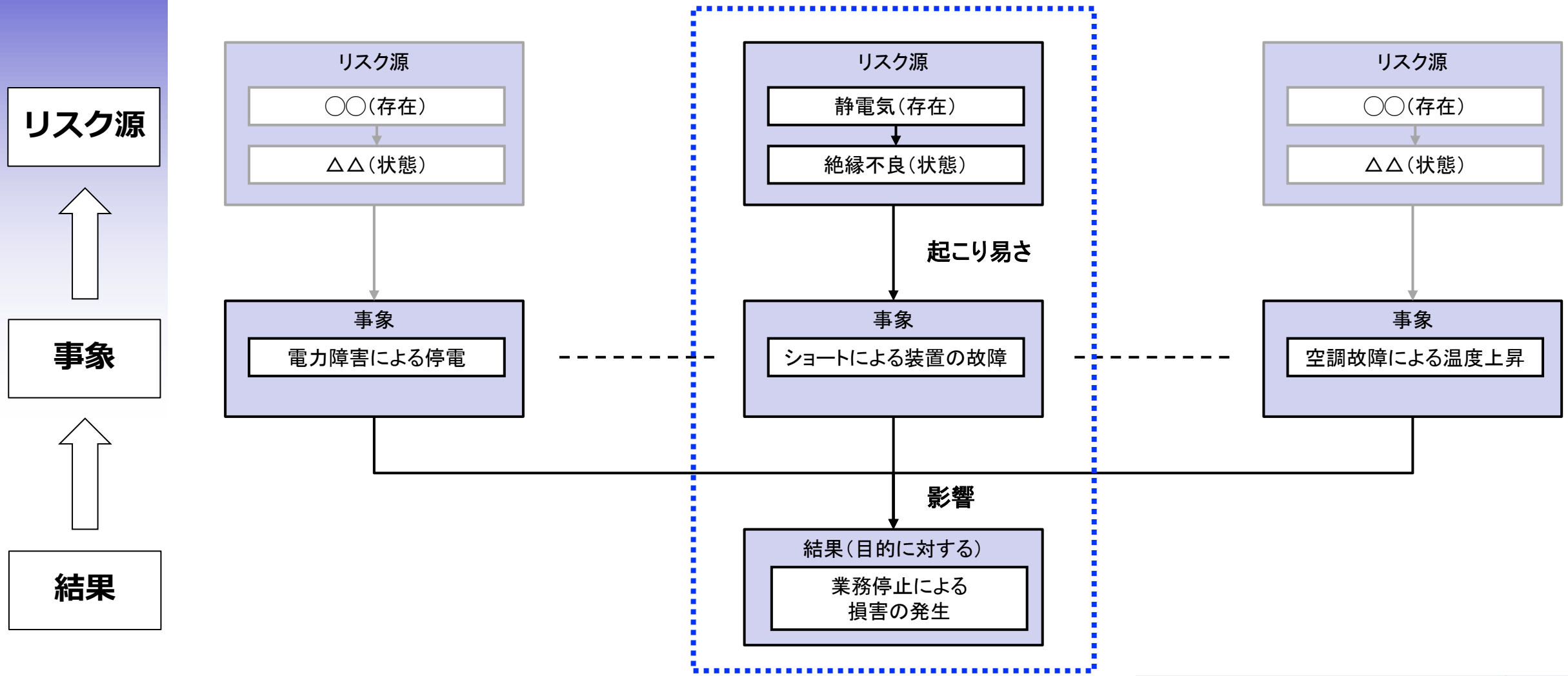
リスク対策ＡをISMSの分類で整理してみると・・・

	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 ・強度を定める ・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	6.8 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？	
④	自主点検　＆ セキュリティ事象（弱点）の報告	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	
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）	

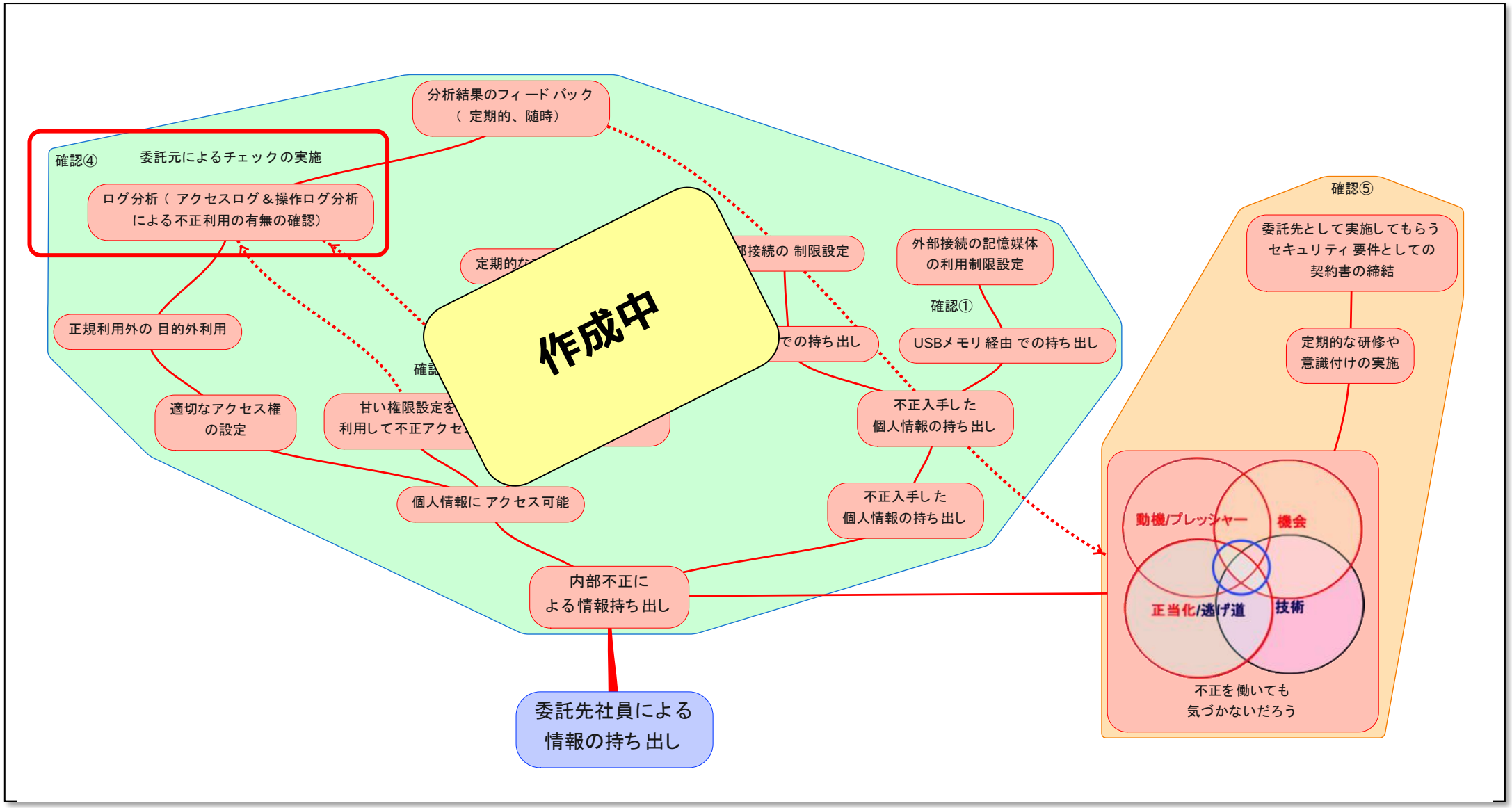
ISMSの分類で整理

リスクの要素：影響の可能性に関する認識（静電気の事例）

結果（目的に対する）　→　事象　→　リスク源　の順で考える



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



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

・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）

開催予告

JNSA

2024年12月6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1：リスクアセスメントについて考える（仮）
・テーマ2：委託先管理（仮）

【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（仮）

■ 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）

開催予告

JNSA

2024年9月5日（木）13:00～14:00（予定）

◆ 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」

■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1： リスクアセスメントについて考える（仮）

テーマ2： 委託先管理（仮）

＋

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