Japan Information Security Management Systems User Group

情報セキュリティマネジメント・セミナー2023

JISQ27001:2023の新規管理策の実装方法についての考察

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

2023年12月18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

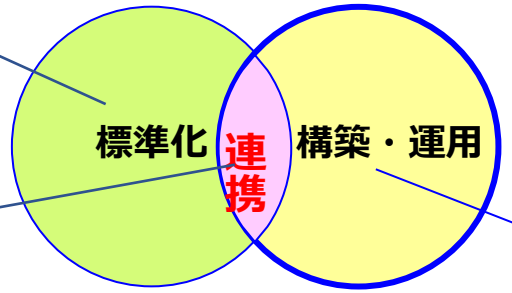
標準化の活用＆定着

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】

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

2023年

■ JISQ27001:2023の新規管理策の実装方法についての考察（講演3）

■ 「ISMS内部監査」どうやってますか?（講演4）

：本日の発表テーマ

インプリメンテーション研究会の2023年活動テーマ

	テーマ名	テーマの活動概要	備考
テーマ1	JISQ27001:2023の新規管理策の実装方法についての考察	規格改定された要求事項の中で今回追加された新規の管理策11個についてどのように実装すればよいか整理を行うことで各認証組織が新規格への移行検討において参考に出来るアウトプットとしてまとめる（下記の方向性で） ・新規格の要求事項の明確化 ・組織の成熟度に応じた対応方針（松竹梅） ・具体的な実装事例の提示 ・疑問点は残さない（・・・出来るだけ）	
テーマ2	「ISMS内部監査」どうやってますか?	マンネリ化や内部監査など過去のテーマについて取り巻く環境や研究会メンバーも代わっているので再整理することで新しい発見が生まれる可能性がある	

ISO/IEC 27001:2022, Annex Aの新規管理策（11個） 1/2

	新規管理策	概要	備考
1	**5.7 脅威インテリジェンス**	**既存や新規の脅威に関する情報を収集及び分析し、脅威に対する対策を講じることで、組織のISMSに影響を及ぼすリスクを低減するための活動**	**優先的に全体フレームワークの整理を実施（その1）**
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	クラウドサービスを利用する場合には、契約形態によるクラウドコンピューティング環境の責任分界（CSPとCSCの役割と責任の境界と範囲）を明確にし、組織が必要とする情報セキュリティが実現できるかどうかを評価する	
3	5.30 事業継続のための ICT の備え	ICT継続の準備では、経営資源の投入を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必要がある	
4	7.4 物理的セキュリティの監視	認可されていない活動を検知し、窃盗・盗難、破壊、干渉などを防ぐために、継続的に物理的アクセスを監視しなければならない（人的監視、システム監視など）	
5	**8.9 構成管理**	**組織が使用する情報システムについて、導入時及び運用中のハードウェア、ソフトウェア（ライセンス含む）、サービス（クラウド含む）、ネットワークの構成を管理し、情報セキュリティ方針及びトピック固有の方針に従ってセキュリティを設定し維持しなければならない**	**優先的に全体フレームワークの整理を実施（その2）**
6	8.10 情報の削除	個人情報などの機微な情報は、保有する期間が長いほど漏えいや流出のリスクが高くなり、漏えいすると組織に影響を与える可能性のある情報は、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、期限を過ぎたものは適時に削除する必要がある	
7	8.11 データマスキング	個人情報保護法における「匿名加工情報」対応を含め、個人情報及びその他の機微な情報を外部から解読できない状態にするために、特定の方針及びその他のデータ保護に関連する要求事項に従ってデータマスキングを実施する必要がある	

ISO/IEC 27001:2022, Annex Aの新規管理策（11個） 2/2

	新規管理策	概要	備考
8	8.12 データ漏えいの防止	外部からの不正アクセスや盗聴及びマルウェア感染や個人による内部不正やシステムの設定ミス又は運用ミスによっても生じる情報漏えいについて、個人又はシステムによる情報の認可されていない開示及び抽出を検出し防止する必要がある	
9	**8.16 監視活動**	**情報システムの運用状況やシステムの処理又は動作について異常がないかを監視し、インシデントに繋がるかもしれない兆候を検出し対応する必要がある（NWなどのトラフィック、システムログ、イベントログ、認証ログ、システム異常・障害など）**	**優先的に全体フレームワークの整理を実施（その3）**
10	8.23 ウェブフィルタリング	従業員が悪意のあるWebサイト にアクセスすることで、マルウェア感染、スパイウェアの侵入、情報及び認証情報の詐取などによる被害に遭わないように、悪意のあるWebサイトへのアクセスをブロック（フィルタリング）する必要がある	
11	8.28 セキュリティに配慮したコーディング	ソフトウェア開発においてセキュリティに配慮することでリスク源となるぜい弱性を減少させるためにはソフトウェアの開発時に適用するセキュリティに配慮したコーディングのための原則を確立し適用する必要がある	

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）

	新規管理策
1	**5.7 脅威インテリジェンス**
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**
6	8.10 情報の削除
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

元々あるもの（実施している管理策）をベースに新規管理策をどのように実装するか検討して頂く時の材料としてご利用ください

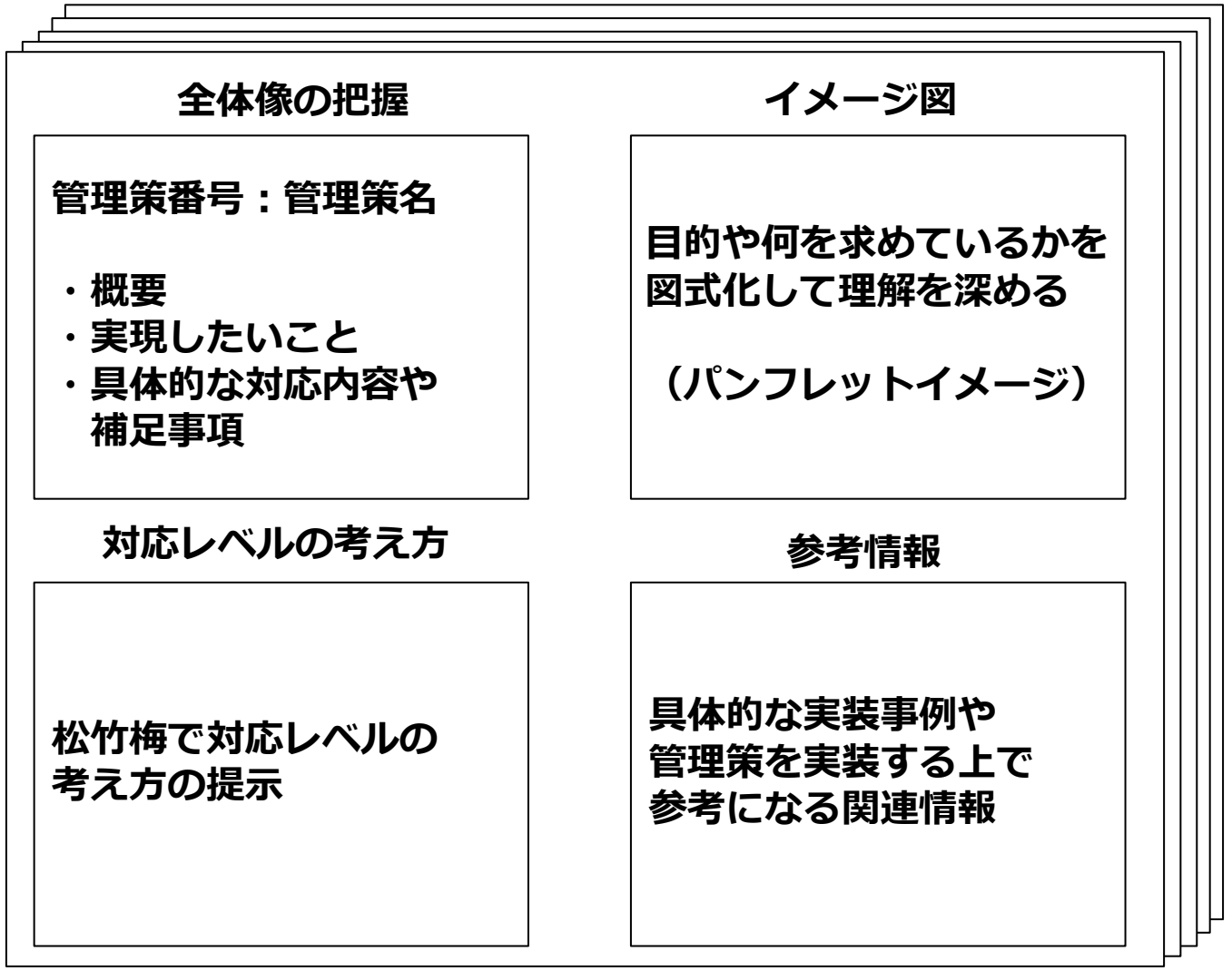
新規の管理策11個を中心にISMSの規格要求事項の実装要件を整理

新規管理策の実装における指針や考え方についての提案

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）

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

＜注意＞
本日は研究会の成果をすべて共有させて頂きますが、時間の関係で説明を割愛するスライドがあります

規格要求事項から見た整理

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

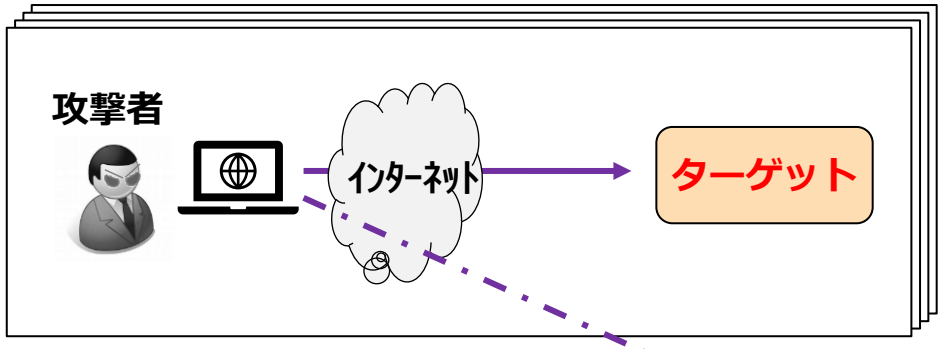
・脅威インテリジェンスは、攻撃者の動機、標的、攻撃手法を理解して対応するために収集・分析されたデータ

・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

「被害内容・対応情報」および「攻撃技術情報」・・・総務省の掲載事例

被害内容・対応情報（被害内容を示す情報）	被害組織名	—
	業種／規模	—
	被害内容	・感染台数、侵害範囲について ・漏えいした情報の種類や件数、内容について ・システム停止やデータ損失によるサービス停止など
被害内容・対応情報と攻撃技術情報が混在	タイムライン（対応状況）	被害組織がどのような対応を行ったのかという時系列
	タイムライン（技術情報）	攻撃者がどのように侵害したのかという時系列
	攻撃対象システム	攻撃対象となったシステムに関する情報
	（被害対象の）対策状況	攻撃対象となったシステムにおいて事前に取られていたセキュリティ対策／設定に関する情報
	攻撃主体に関する情報	攻撃グループ名や攻撃者が他にどのような攻撃活動を行っているのかという情報
攻撃技術情報（攻撃方法を示す情報）	脆弱性関連情報等	悪用された脆弱性の有無やその詳細について
	マルウェア	現場で見つかったマルウェアに関する情報（※マルウェア検体そのものは含まない場合もある）
	通信先	不正アクセスの通信元やマルウェアの通信先など
	その他 TTP 情報(攻撃の手口)	上記以外の攻撃者が用いた攻撃手法に関する情報

表 3

サイバー攻撃被害に係る情報の共有・公表 ガイダンス

https://www.soumu.go.jp/main_content/000867112.pdf

参考情報

JPCERT/CC インディケータ情報・・・総務省の掲載事例

****
情報の共有範囲 本情報は、取扱注意情報(AMBER)です。本情報は、機密性の高い非公開情報を含む ため情報の共有範囲が制限されます。共有範囲は自組織および関連組織内の必要最小限 としてください。(Web サイトや公開のメーリングリストなどを使用して一般へ公開する ことを禁止します。)
****
JPCERT/CC で国内の組織に対して行われた標的型攻撃に関する情報を入手いたしま したので、参考までに情報をお伝えします。 以下の標的型攻撃に関する情報を参考のうえ、自システムなどの確認をお勧めします。

1)攻撃が行われた期間
　202x 年 x 月以降

2)攻撃の特徴
標的型攻撃メールの本文に URL が記載されており、JPCERT/CC が確認時点 で URL へ接続すると ZIP ファイルがダウンロードされました。ZIP ファイル 内には、ショートカットファイル(.lnk)が格納されており、実行するとマルウェアに感染し、外部サイトへの接続に繋がります。

[メールの件名]
(※メールの件名を記載)

3)攻撃に使用された検体

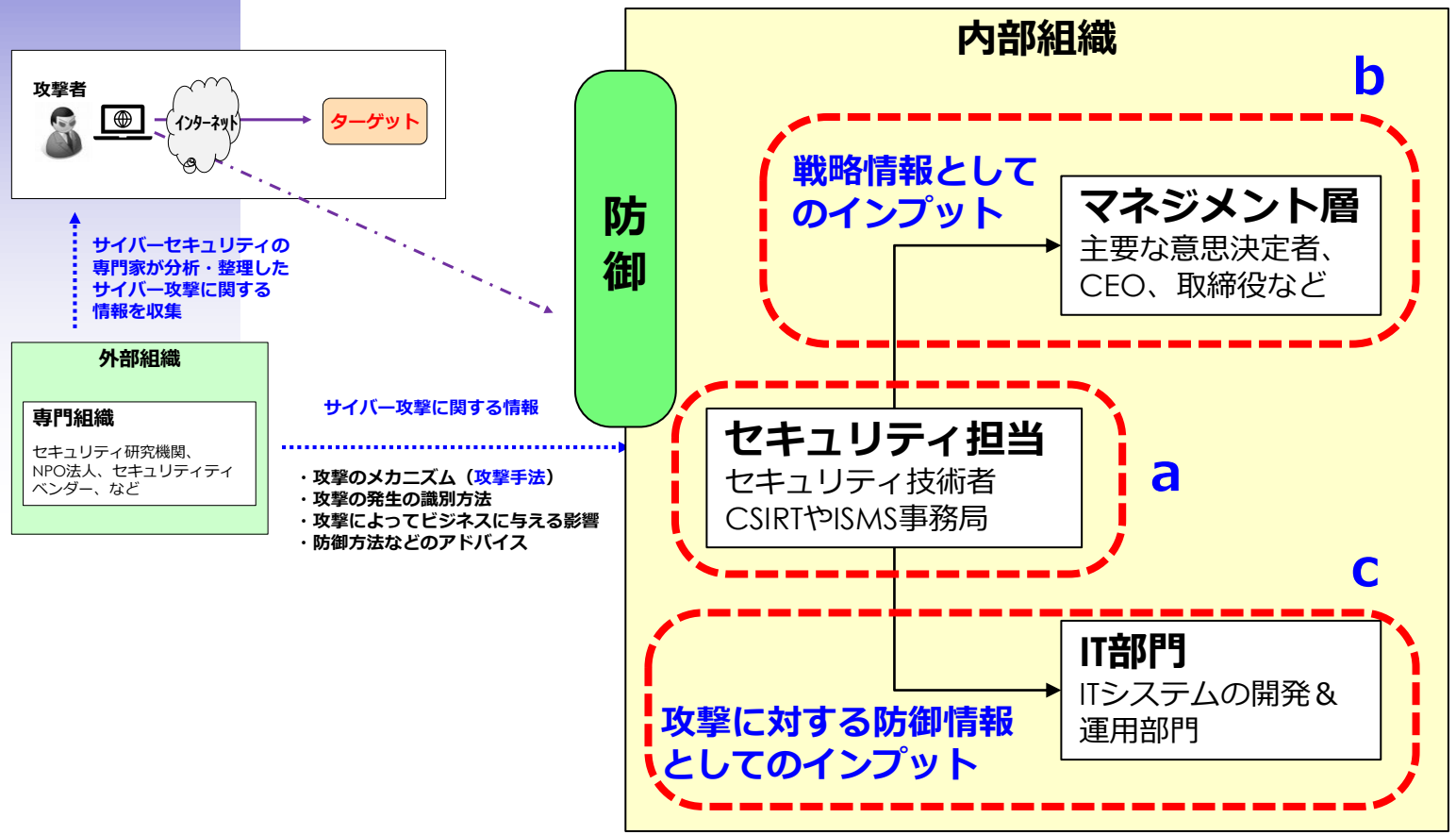
JPCERT/CC が確認しているファイルや検体のハッシュ値は次のとおりです。
ファイル名: (※実際のファイル名).zip
 File Type :

サイバー攻撃被害に係る情報の共有・公表 ガイダンス

https://www.soumu.go.jp/main_content/000867112.pdf

脅威インテリジェンスの活用ポイント・・・a、b、c

専門機関からの収集する情報を整理してサイバー攻撃に対する防御に有効活用するプロセスを確立する



活用ポイント

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

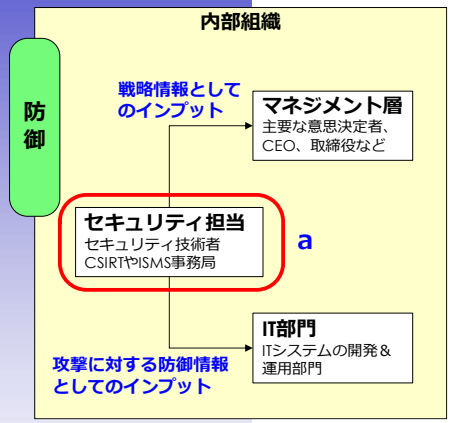
b.経営層へのインプットする条件やタイミングの判断基準を作成

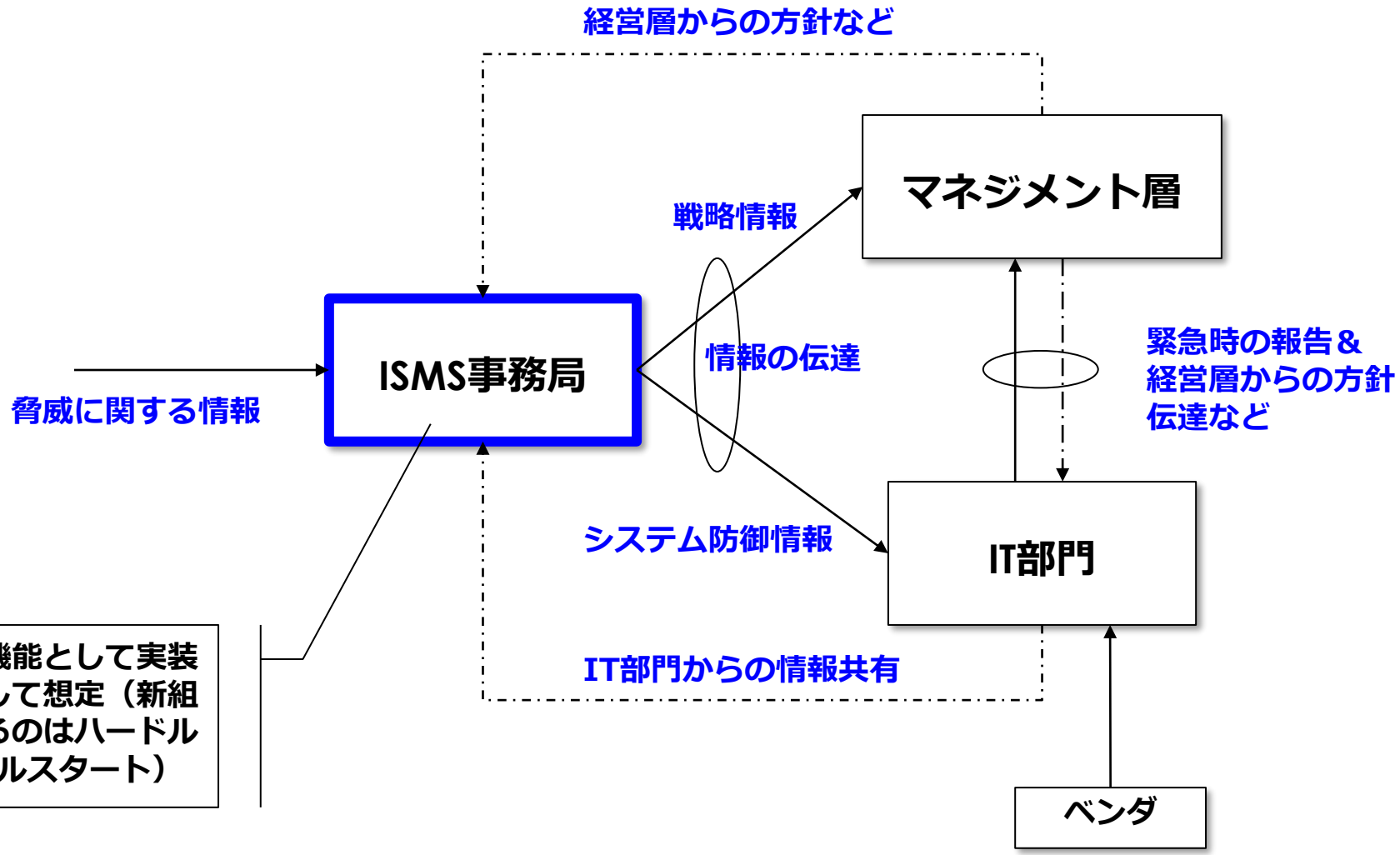
c.関係部署（社員、システム担当）に流す情報と期待する行動を定義する

参考情報

活用ポイント・・・a

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



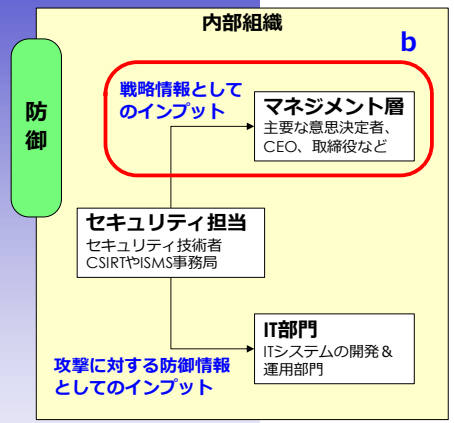


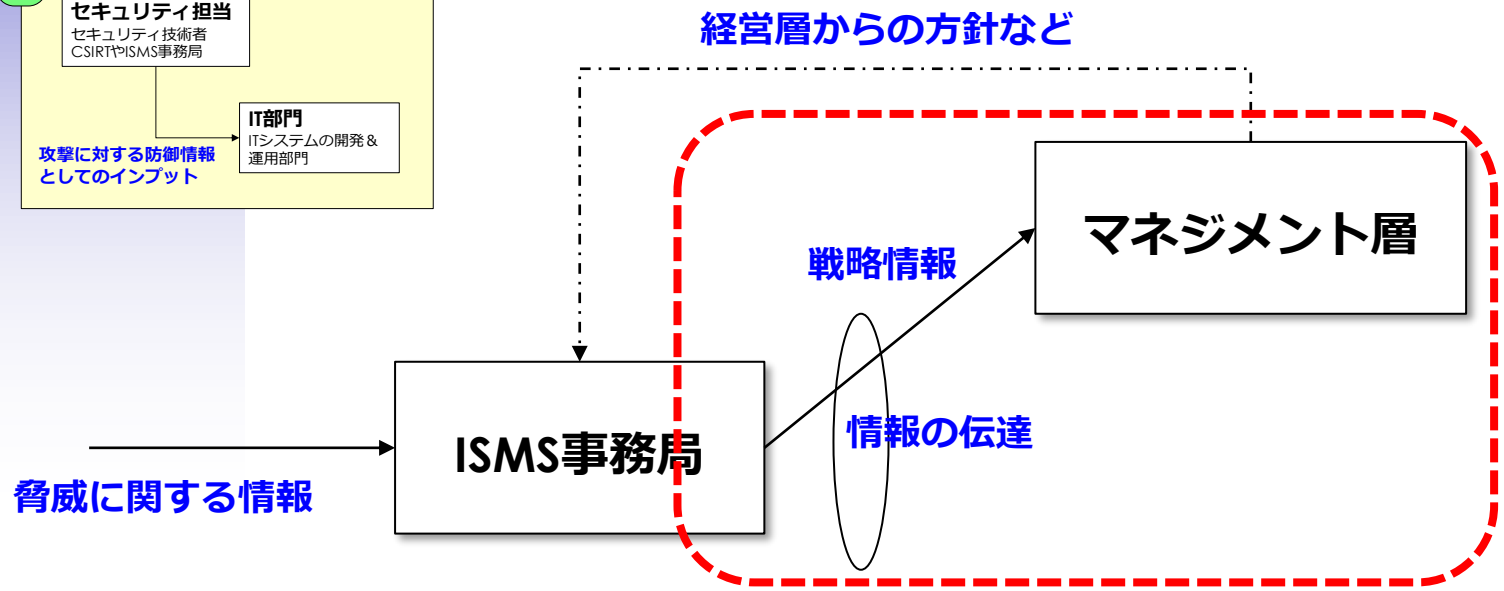
既存の組織の中に機能として実装することを前提として想定（新組織として独立させるのはハードルが高いのでスモールスタート）

参考情報

活用ポイント・・・b

b.経営層へのインプットする条件やタイミングの判断基準を作成（※1）





※1：継続性、再現性を目的とした文書化で
1ページサーマリ的なものをイメージ

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

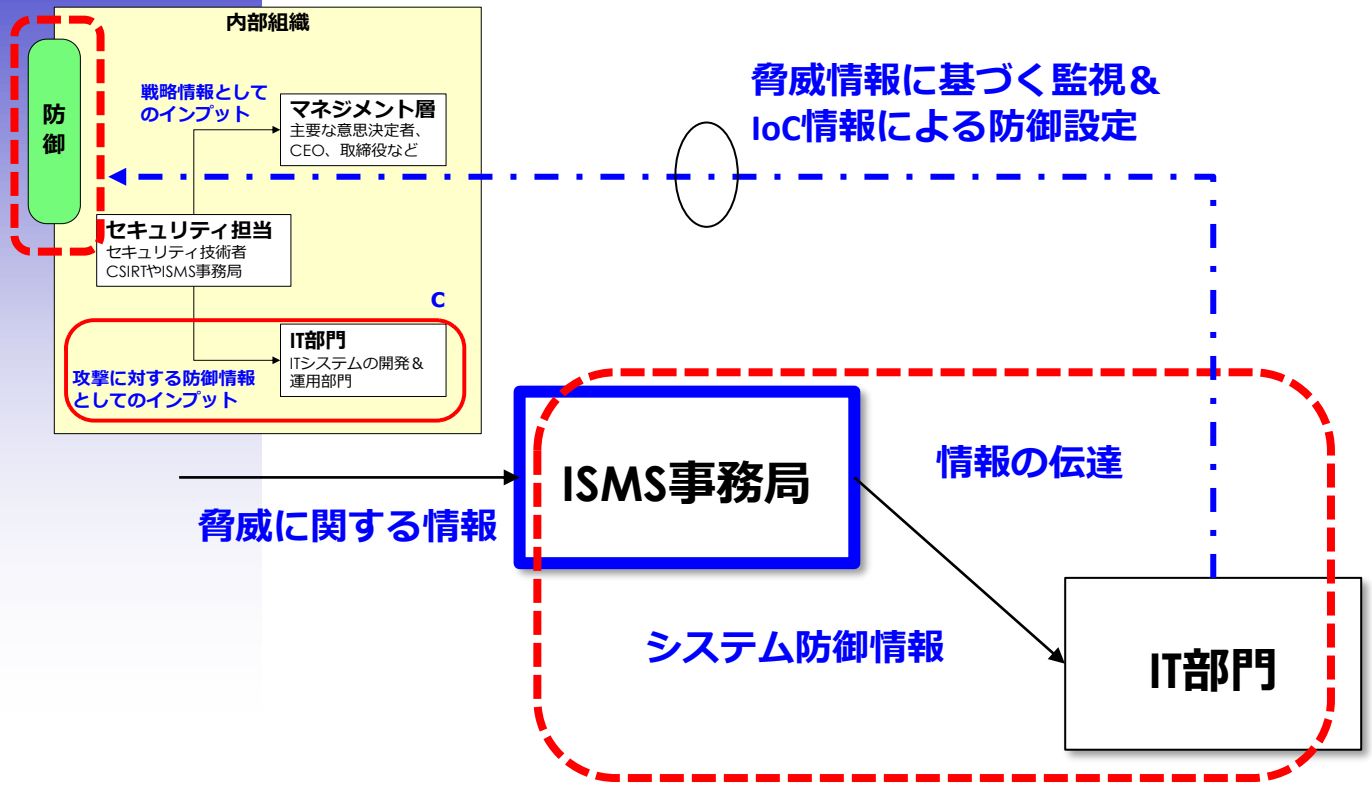
マネジメントレビューのフィードバックの記録

・経営層からの指示は記録し、リスク対応計画や課題管理する

参考情報

活用ポイント・・・c

c.関係部署（社員、システム担当）に流す情報と期待する行動を定義する



インプット情報

- サイバー犯罪で利用される攻撃手法の情報
- システムにおいて悪用される可能のある脆弱性情報
- **サイバー犯罪集団が攻撃した際の最新のIoC情報（※１）**
- 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）
- 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）
- 自組織への攻撃を目論むサイバー犯罪者情報

期待する行動

- インプット情報をもとに攻撃に対する防御設定

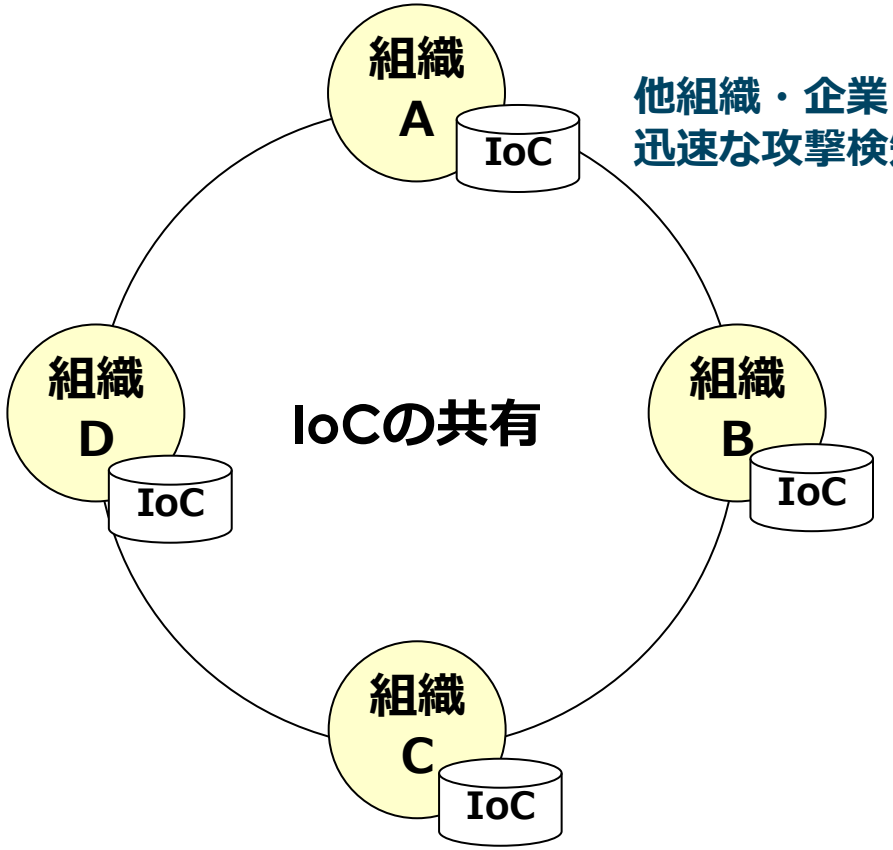
※1：「Indicator of Compromise」の略で侵害指標や痕跡情報などで攻撃者が使用したマルウェアのファイル名、攻撃によって変更されるレジストリ、通信先のURIやIPアドレスなど

「Indicator of Compromise」：侵害指標や痕跡情報

実際に発生した攻撃者が使用するマルウェアのファイル名、攻撃によって変更される
レジストリ、通信先のURLやIPアドレスなど

IoCの事例（次ページ参照）

- Network Indicator
  - ・IPアドレス
  - ・ドメイン名（通信先のURL）
- Host Indicator
  - ・ハッシュ値
  - ・ファイルのパス
  - ・レジストリ



他組織・企業と共有することで
迅速な攻撃検知が可能

さまざまなシステムから記録されたIoCを参照することで、流行しているマルウェアなどによる被害を速やかに検知が出来る可能性がある
IoC自体はあくまでも攻撃の痕跡を記録したデータのため、マルウェアの発見や隔離、駆除などの機能をもつセキュリティ対策ソフトと組み合わせることが推奨

IoCで取得できる主な情報

IoCのサンプル事例

攻撃時に通信先となったIPアドレス	関連する脅威	活動確認期間	遮断方向（内⇔外）
＜*.*.*.*＞	マルウェアの種別	2023.06.14～07.23	内 → 外

- **マルウェアのファイル名**

  攻撃を行ったマルウェアのファイル名を取得

- **不正に変更されたデータの情報**

  マルウェアは、システム内に保存されているデータに不正な変更を加えるケースがあり、その記録されたデータ情報

- **攻撃時に通信先となったIPアドレス**

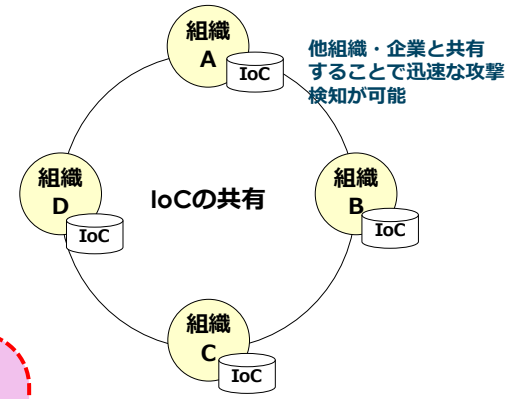
  情報漏えいなどを目的としたマルウェアは、不正に取得したデータを外部に送信する場合に通信先として使用されたIPアドレス

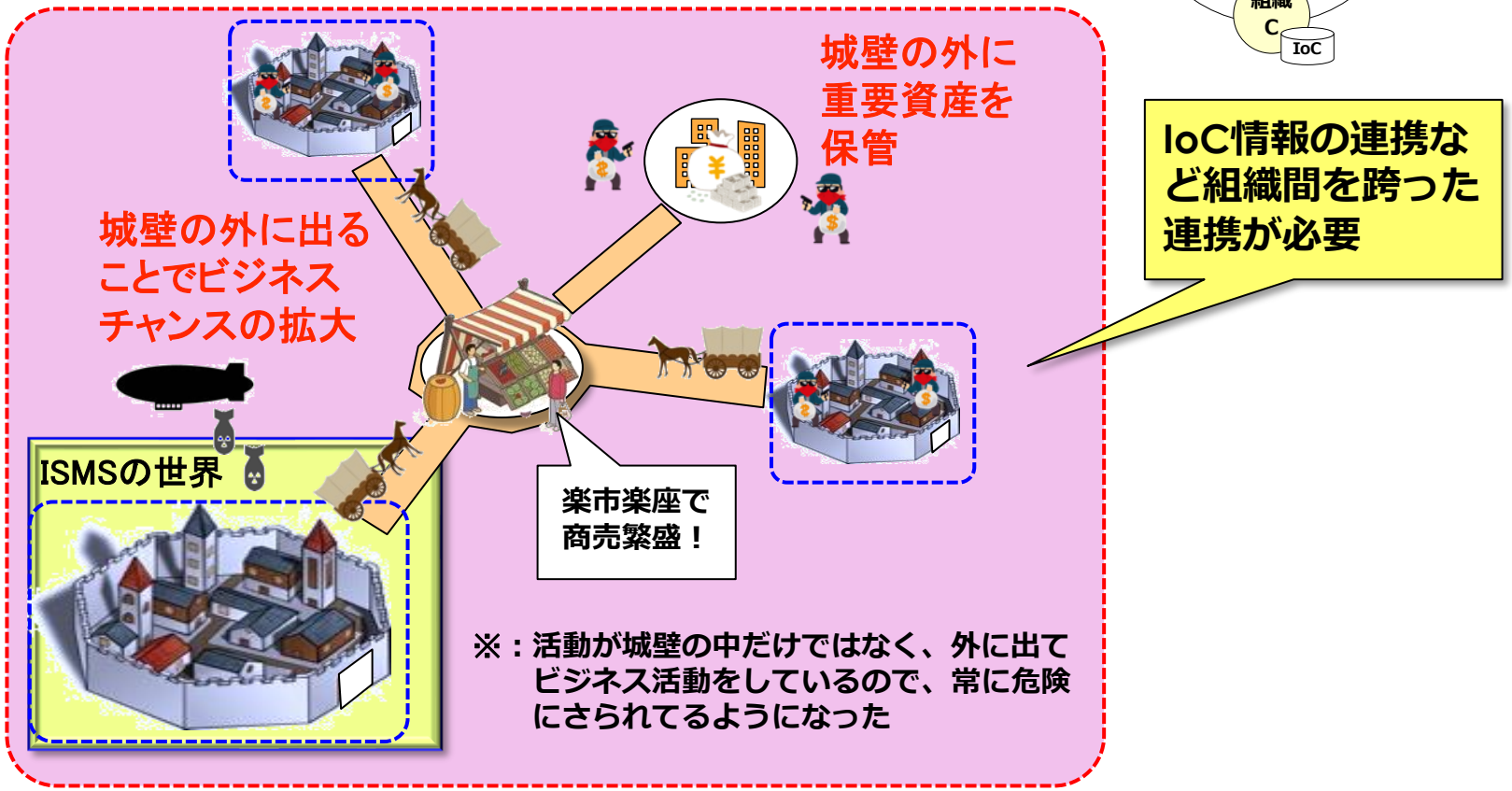
- **不審なログイン試行の痕跡**

  何度もログインを試行、ランダムなユーザーIDやパスワードが入力されているなどの痕跡

ISMSの活動範囲を超えた情報共有の必要性（IoC情報など）

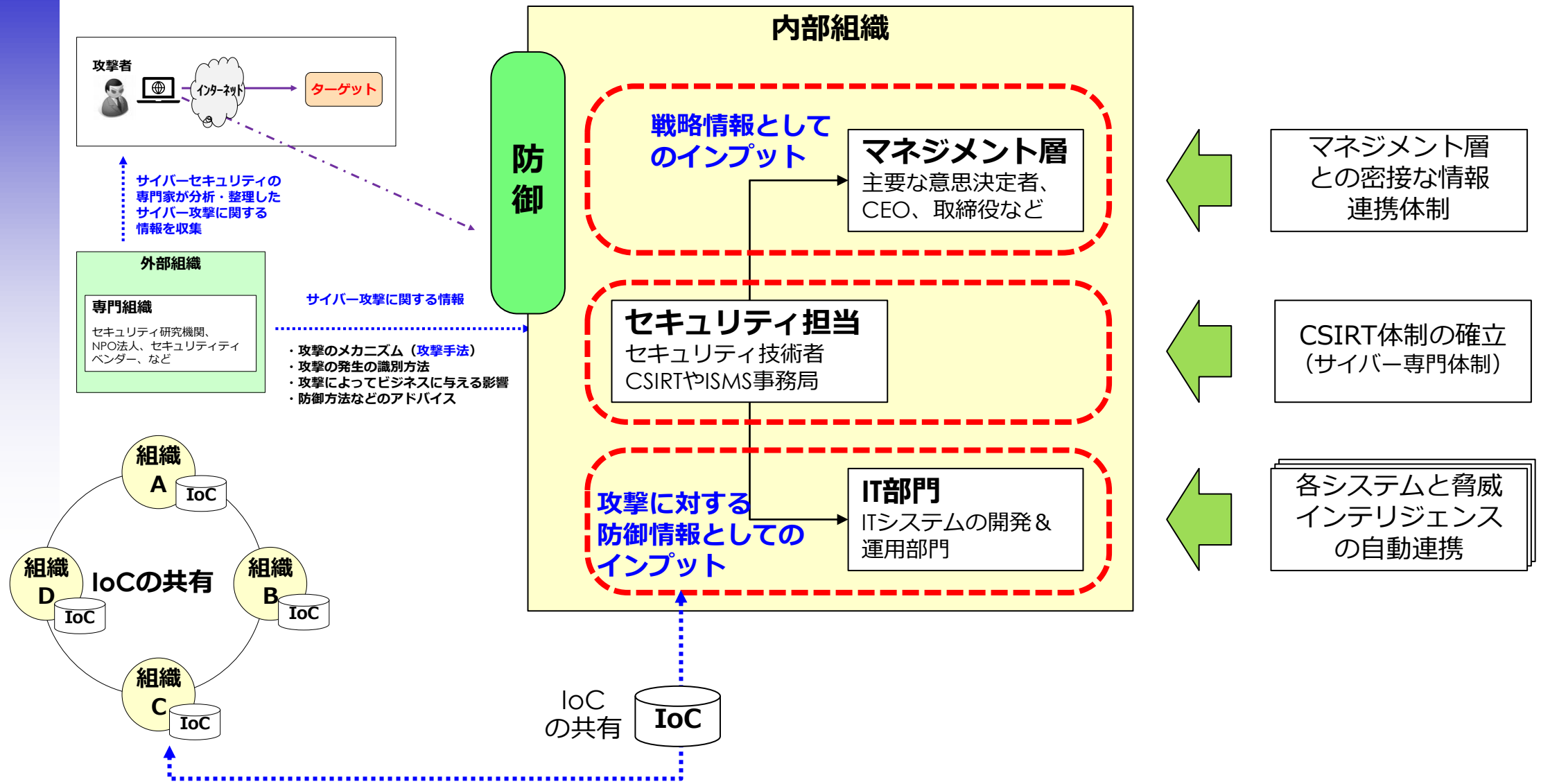
- サイバー攻撃は従来の組織の枠組みを超えたもの
- 様々な攻撃パターンで攻めてくるので相手を知る必要があり、その手段の一つとして脅威インテリジェンスがある
- 攻撃情報についてはみんなで共有することで安全が守られる（IoCの共有など）





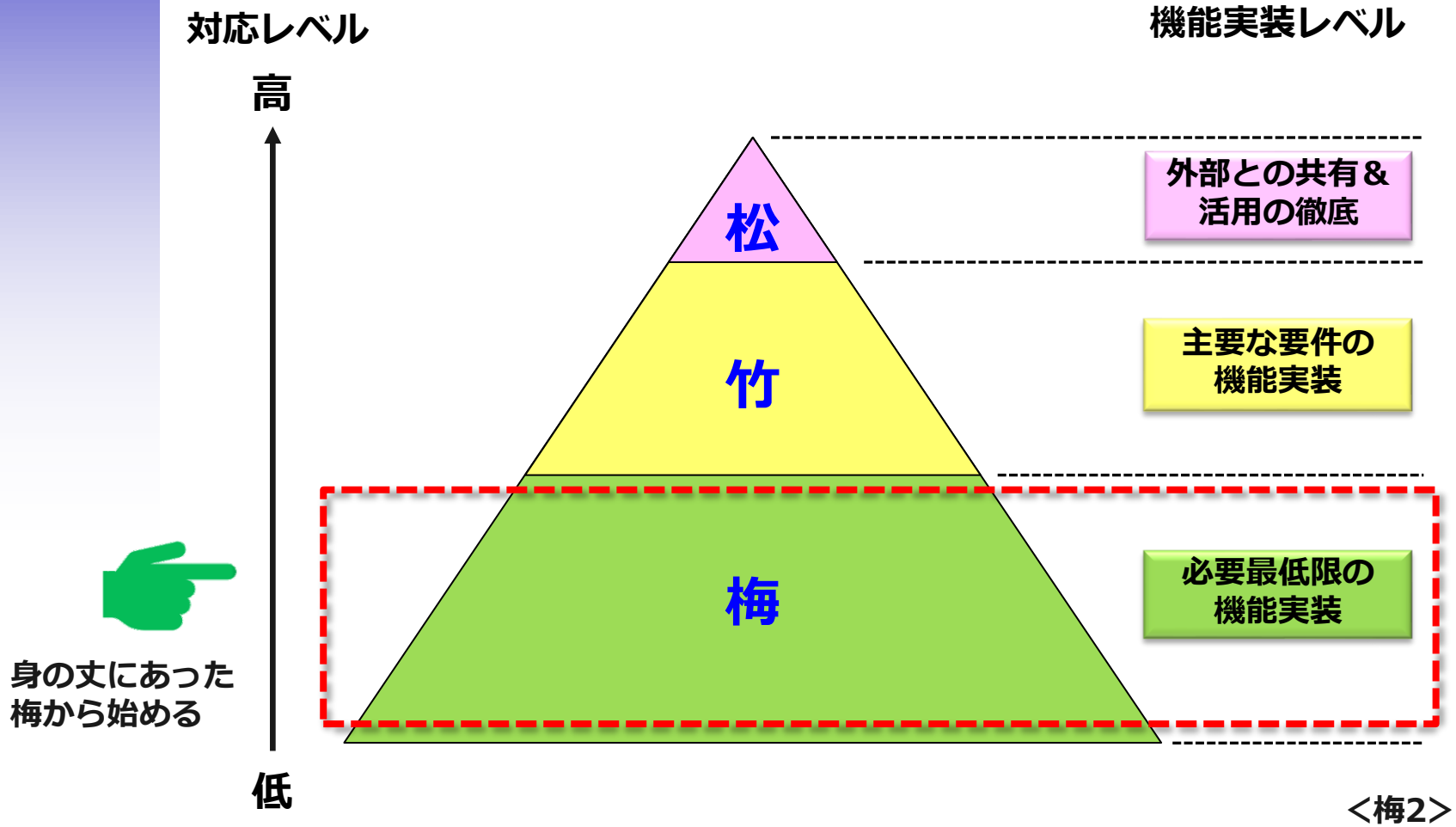
参考情報

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）



参考情報　IPA 情報セキュリティ10大脅威 2022を脅威インテリジェンスに利用

IPAから提供されている10大セキュリティ脅威を元に自組織にマッチした対策を実施

前年順位	個人	順位	組織	前年順位
2位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	2位	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	5位	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	6位	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	8位	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	10位	不注意による情報漏えい等の被害	9位

各脅威に対する具体的な対策を自組織にマッチしたものを選択

https://www.ipa.go.jp/security/10threats/10threats2022.html

規格要求事項から見た整理

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＞

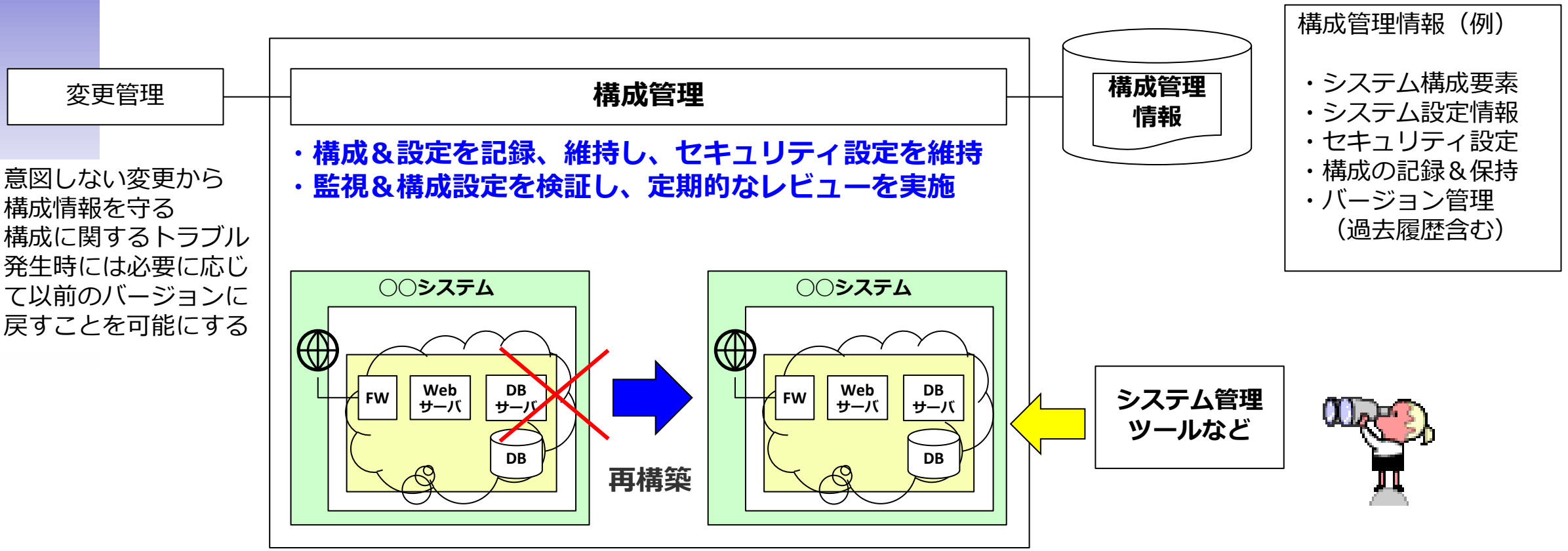
- システム（※1）の構成および設定情報
- セキュリティ設定情報

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

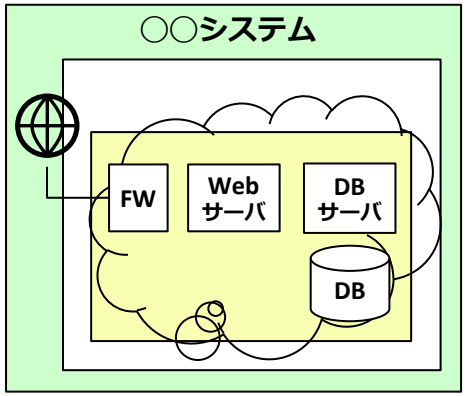


※1： HW、SW、サービス（クラウド含む）及びNW

構成管理のセキュリティ設定の考慮事項

構成管理

構成＆設定を記録、維持し、
セキュリティ設定を維持する
監視＆構成設定を検証し、
定期的なレビューを実施
（変更管理プロセスにて適正に管理を実施することで意図しない変更からシステムを保護する）

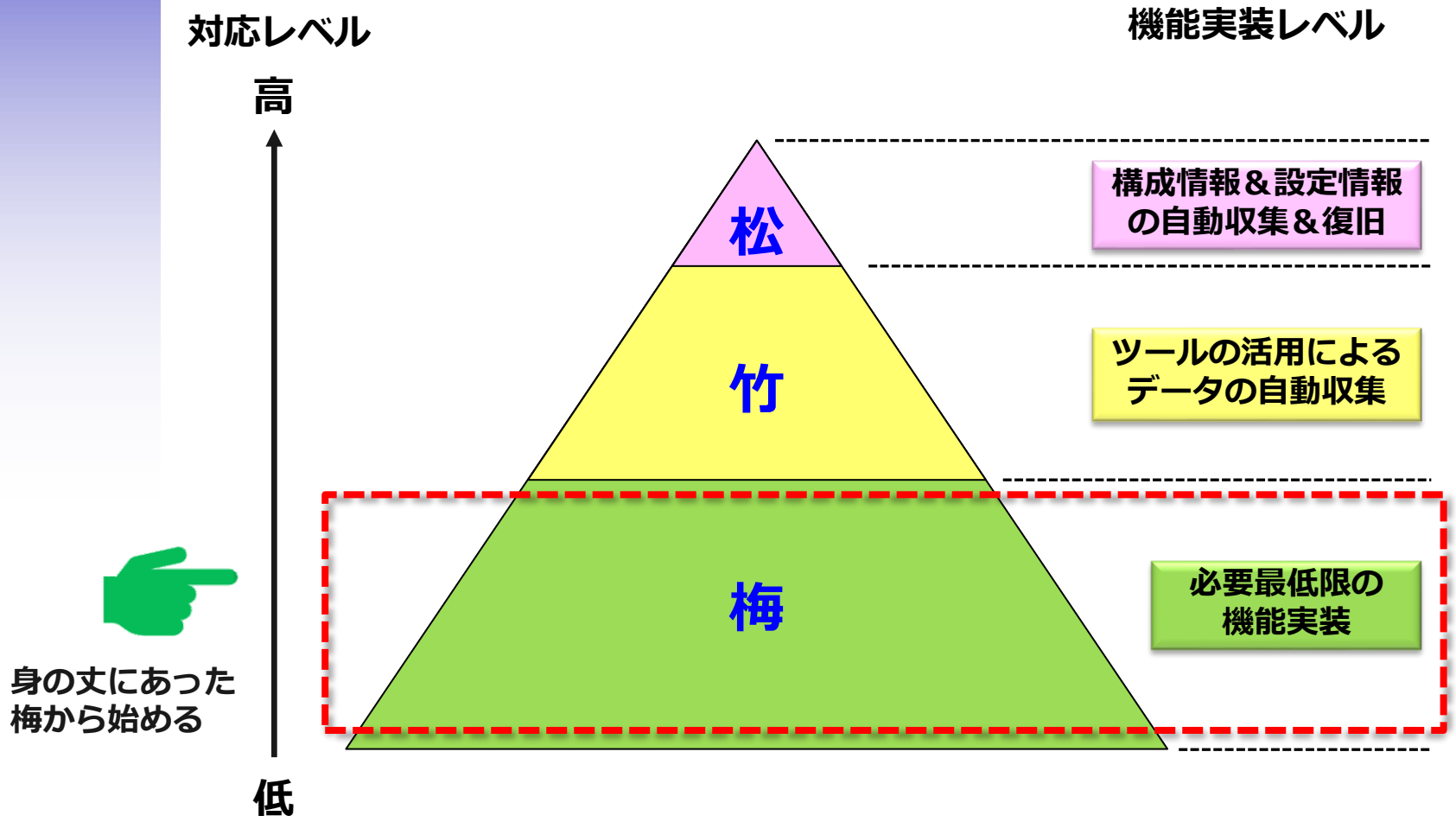


セキュリティ設定の考慮事項

- 特権的、実務管理レベルのアクセス権を持つ識別情報
- 使用されていない識別情報や不要なものを無効化
- **不必要なサービスを無効化、制限する**
  （インストール時にデフォルト設定で意図せず自動組込みされた不要モジュールなどの無効化）
- 強力なユーティリティプログラム
- ホストパラメータへのアクセスの制限
- クロックを同期させる
- **初期PWDの変更、セキュリティ関連パラメータの初期状態のレビュー**
- 自動ログオフタイムの設定

構成管理の対応レベルについての考え方（案）

構成管理の管理レベル（案）



参考

事例：クラウドのセキュリティ設定（AWS)

セキュリティの柱

AWS Well-Architected フレームワーク

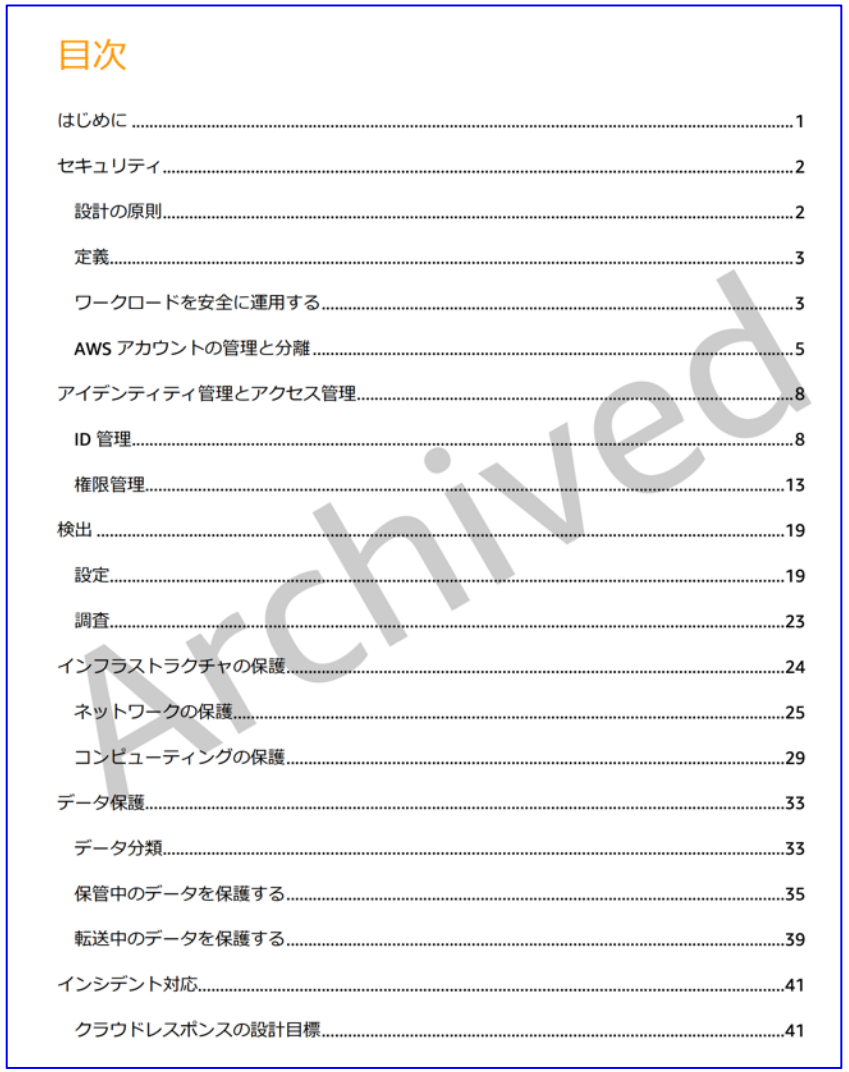
2020 年 7 月

This paper has been archived.

The latest version is now available at:

https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html

aws



目次

https://d1.awsstatic.com/whitepapers/ja_JP/architecture/AWS-Security-Pillar.pdf

参考

クラウドサービスにおけるセキュリティ設定項目（総務省）

クラウドサービス利用・提供における 適切な設定のためのガイドライン

図表Ⅱ．１．１－１　セキュリティ設定項目の類型と類型項目の意味

No.	セキュリティ設定項目の類型	類型項目の意味
1	ID とアクセス管理（IAM）	ID とアクセス管理とは、「誰が」「どのリソースに対し」「どのような操作ができるか」を定義し、アクセス制御を実現するために提供されているサービスである。ID には、大別してユーザー、管理者及び開発者等の人間に対するアカウントとアプリケーションなどが API 等で使用するサービスアカウントがある。これらに対するアカウントグループやアクセス権等の設定がある
2	ロギングとモニタリング	ロギングは、クラウドにおける挙動やアラート発報の基本となるものであり、ロギングを有効にするための設定、モニタリングを行うためのフィルタ設定及びログの保存期間設定などがある。
3	オブジェクトストレージ	クラウド利用におけるオブジェクトストレージのセキュリティでは、アクセス制御の設定、データの外部漏えいに備えた暗号化、ロギング及び一定期間経過後に削除するなどのライフサイクル設定等がある。
4	インフラ管理	
4.1	仮想マシン（VM,VPS）	物理サーバを論理的に分離する仮想マシンを利用する際、仮想マシンのディスク暗号化、エンドポイント保護などの設定がある。
4.2	ネットワーク	クラウド利用は、インターネット経由となるため、外部ネットワークとのアクセスに関する基本的なセキュリティ設定、仮想プライベートクラウドのセキュリティ設定、境界防護等に関する設定等がある。
5	セキュリティ等の集中管理	IaaS/PaaS が提供するセキュリティ集中管理機能、キーマネジメントサービス、運用管理コンソール、監査ツール、コスト管理サービスなど、構成管理を横断的に集中管理可能なツールやサービスが提供されている場合があり、使用するための各種設定がある。
6	IaaS／PaaS が提供する、その他のサービスや機能 ※短期間に新たなサービスや機能が追加されることがあるため、下記の項目以外にも追加された時点で、設定値についても確認を行う必要がある。	
6.1	鍵管理	鍵管理は安全に秘密鍵を管理・作成・制御する方法を提供するものであり、使用するクラウドに応じた適切な設定がある。
6.2	PaaS が提供するアプリケーション	クラウドで提供されるアプリケーションには様々なものがあるが、個々の事業者から提示されるアクセス許可などの設定やデフォルトの公開範囲等の設定を確実に行う必要がある。
6.3	データベース	クラウドで使用するデータベースの保護、監査、暗号化などの設定がある。
6.4	コンテナ	コンテナとは、ホスト OS 上で「コンテナエンジン」と呼ばれるシステムを動作させ、「コンテナ」と呼ばれる実行環境を複数構築する技術である。コンテナエンジンに係るセキュリティ関連の設定がある。
7	その他の設定項目	上記以外のクラウドサービス事業者が提供する統合資産管理、モバイルデバイス管理等のサービスについては、個々の事業者から提示されるセキュリティ設定がある。

https://www.soumu.go.jp/main_content/000843318.pdf

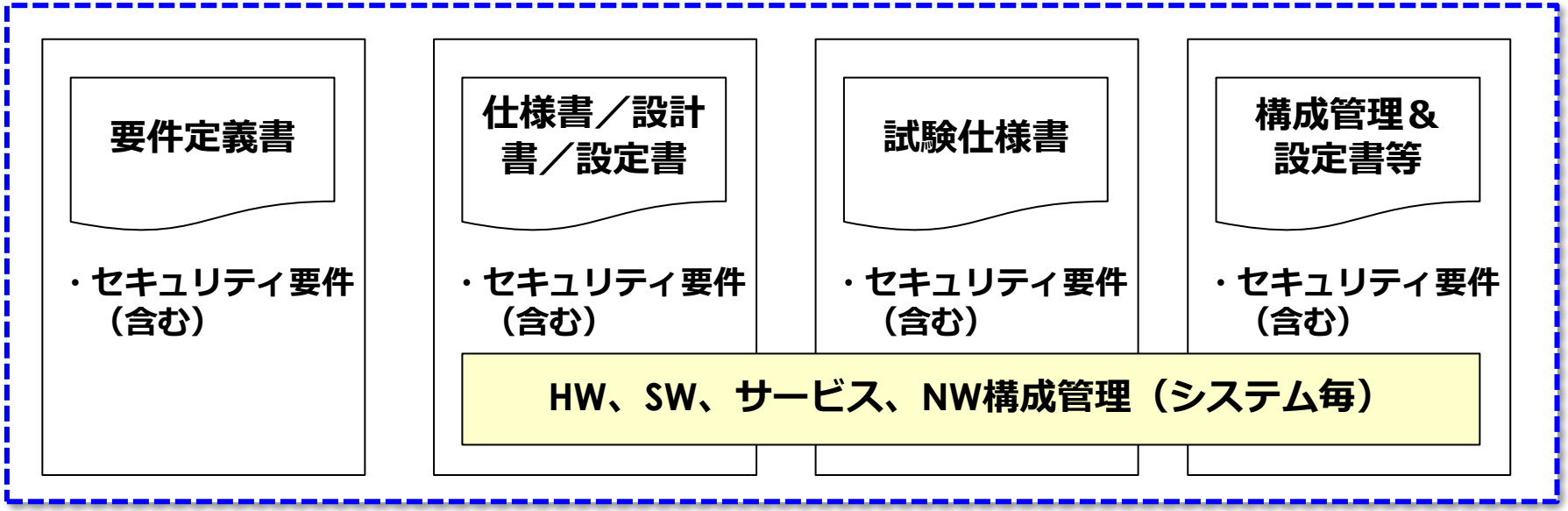
参考

システムのライフサイクルにおけるセキュリティ要件の組み込み

企画	開発・構築	試験	運用
RFP （セキュリティ要件）	仕様書／設計書／設定書 （セキュリティ要件の実装）	試験仕様書 （セキュリティ要件の実装＆充足性確認）	増設工事等のイベント （セキュリティ要件の充足性確認） セキュリティ設定の維持

テンプレート化することで品質保証（セキュリティ含む）を実現する

標準テンプレート



参考事例

構成管理ツールと Infrastructure as Code (IaC)

構成管理ツールと Infrastructure as Code (IaC)の機能概要

分　類	機　能　概　要	備　考
構成管理ツール	ハードウェアの保守情報や構成情報を管理するものや、ネットワーク構成情報・IPアドレスの割り当てを管理するもの、システムの設定を管理するものなど	
Infrastructure as Code (IaC)	ネットワーク・サーバー・クラウド基盤の設定から、ミドルウェアやアプリケーションの設定を管理することを目的としたツール（クラウドの普及により導入が加速） **IaCはインフラの構成をコードで記述するもので、下記のような要素を再現可能な形でコードとして定義するもの** ・クラウド基盤の設定 ・OSの設定 ・ミドルウェアのインストール・設定 ※：**一度定義してしまえば、コードを実行するだけで何度も同じ環境を作ることが可能** クラウド環境でインスタンスを追加・削除する場合など、設定漏れなどのミスなくリアルタイムに実現可能。コードとして管理しているので、バージョン管理の仕組との親和性も高い。 （代表的なツール：Chef, Ansible, Terraform など）	**メリット** 開発期間の短縮 運用フェーズにおける信頼性・保守性の向上 再現性（同じものを品質よくいくつでも作成可能） **デメリット** 導入までに多くの時間とコストがかかる

第10回：構成管理とは―目的と取り組み事例 | クラウド導入・システム運用ならアールワークスへ (rworks.jp)

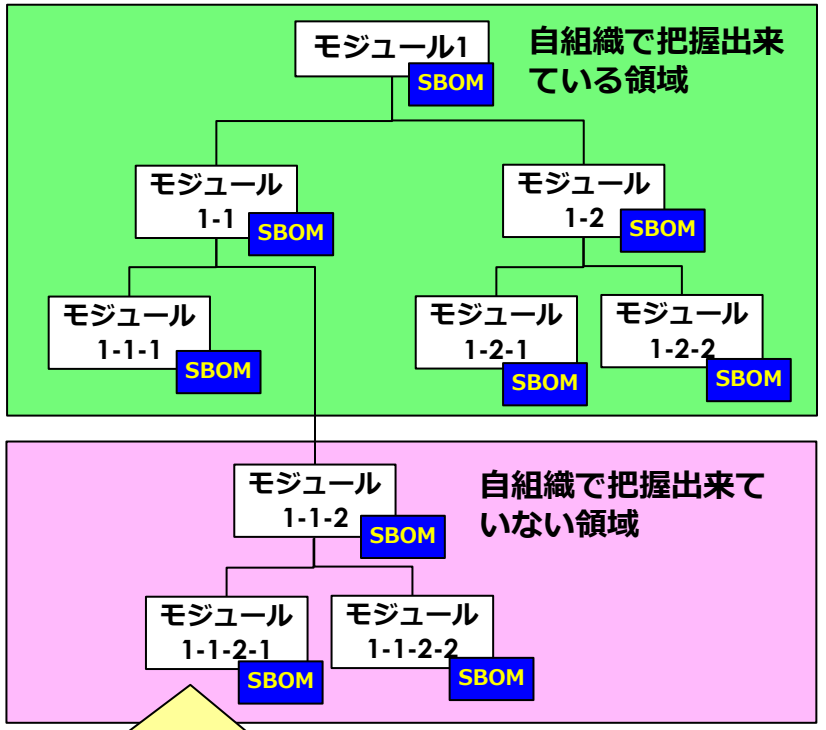
SBOM（Software Bill of Materials）*1ツールの活用

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

規格要求事項から見た整理

8.16 監視活動

8.16 監視活動（要約）

概要

情報システムの運用状況やシステムの処理、又は動作について異常な挙動がないかを監視し、インシデントに繋がるかもしれない兆候を検出し適切に対応する

実現したいこと

システムやネットワークに不正な挙動がないか監視を行うことでインシデントにつながる兆候や予兆を見つけ、速やかな対応に繋げる

具体的な対応内容や補足事項など

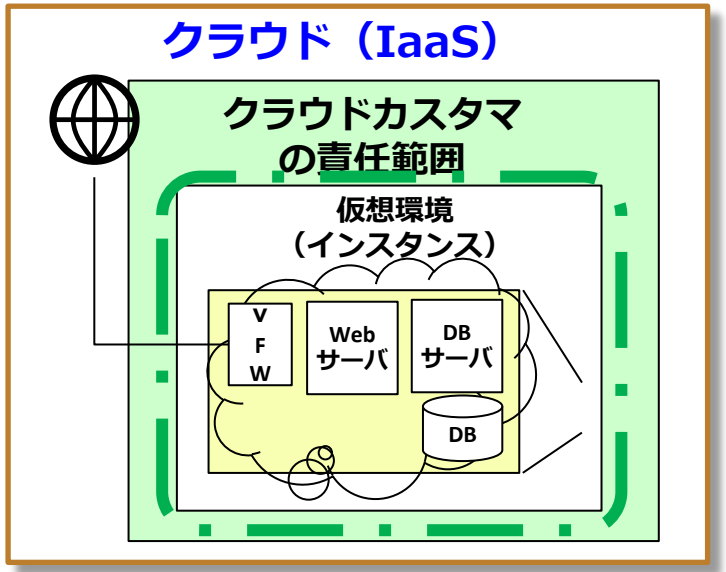
異常な行動・動作及び潜在する情報セキュリティインシデントを検出するために普段から情報システムの運用状況やシステムの処理又は動作について異常がないかを監視する
インシデントに繋がるかもしれない兆候を検出した場合は速やかに対応することで影響を最小限にする

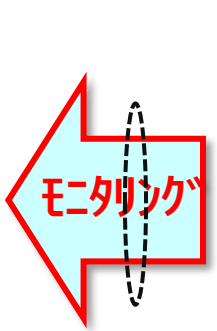
システム運用担当

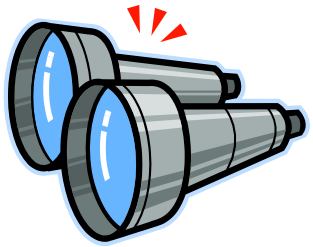
＜情報の例示＞

- **NW、システム、アプリケーションのトラフィック**
- **セキュリティツールからのログ（ウィルス対策ソフト、IDS/IPS、Webフィルタ、FW、DLPなど）**
- **システム、NWなどのイベントログ**
- **定常時と高負荷時のリソース使用率の分析**

8.16 監視活動（Monitoring activities）（イメージ図）







監視ソフトなどの
ツールによる常時監視

・情報システムの運用状況や処理異常などを監視
・インシデントに繋がる兆候を検出し対応

定常監視

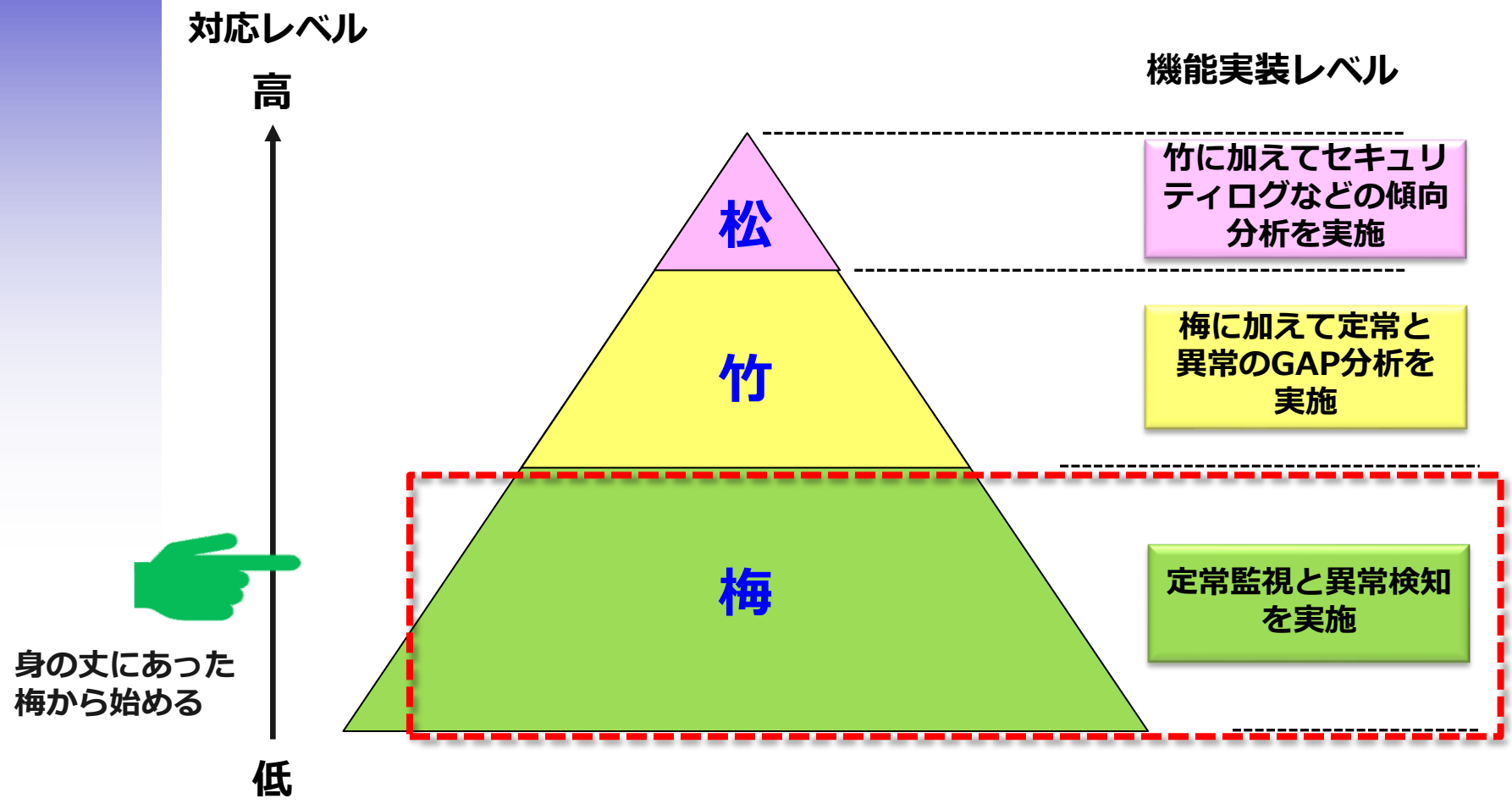
GAP分析

異常検知

兆候：すでに発生しているが未発見
予兆：発生前

監視活動の対応レベルについての考え方（案）

監視活動の管理レベル（案）



参考資料
（2019年）

イベントログのレビューの目的

イベントログのレビューの目的の3分類

- （事件・事故の）**原因調査**
- （いつの間にか発生してしまっているかもしれない）**問題発見**
- （起きるかもしれない事件事故の）**予防**

イベントログ取得	レビュー実施
イベントログに記録される事象	レビューの結果判明する事象
業務時間外にファイルサーバーにアクセスしている	不正アクセス
退職時に大量のファイルへアクセスしている者がいる	ファイルの持ち出し
複数の場所から同じアカウントを利用している	なりすまし
大量のアクセス失敗ログ	マルウェア感染

参考資料
（2019年）

目的によるログのレビューの視点の違い

ログのレビューの目的（3分類）

	原因調査	問題発見	予防
目的 の解説	インシデントの 解析に利用する	CIAの喪失につながる可能が 高い事象の発生を検知する （気づかない問題を発見）	CIAの喪失につながるかも しれない事象を検知する
レビュー のタイミング	事件・事故発生時	定期レビュー	定期レビュー
調査 の視点	・監視カメラのアーカイブ ・ハードウェアの 動作ログ ・ネットワーク トラフィックログ ・システム動作ログの アーカイブデータ ・バックアップ動作ログ	・監視カメラの映像 ・ハードウエアの動作ログ中の 障害イベント ・ネットワーク 異常検知 ・システムの 異常終了イベント ・バックアップの失敗	・監視カメラの映像 ・ハードウエアの動作ログ中の 機器内温度上昇イベント ・ネットワークの 恒常的な過負荷 ・CPUやメモリの 恒常的な高い使用率 ・バックアップ容量の低下

参考資料
（2019年）

「原因調査」のレビューの目的・視点

目的

システムに何か異常があることが分かった場合、「どのような異常なのか」、「どういう経緯で発生したのか」をたどる際、システムの動作記録(＝ログ)を確認(＝レビュー)し、異常の原因を調査することです(※)。

※多くの組織、運用者が認識しているログのレビューの目的はこれでしょう。

異常に対処する

視点

問題発生前および発生時に何が起こったか(必要な場合、問題発生後どのような影響があったか)を確認することです。

例１：ハードウエアの故障時

・故障直前の操作、故障直前の機器温度、故障直前の負荷状況

例２：データベースシステム異常停止時

・異常停止直前の操作、異常停止直前の接続数、異常停止直前のシステム負荷

参考資料
（2019年）

「問題発見」のレビューの目的・視点

目的

システムのC・I・Aが損なわれていても、「操作中の画面に異常が出る」とか「機械が異音を発している」などの明確に感知できる現象がないと利用者や運用者がすぐに認識できるとは限りません。認識が遅れると、長期に渡って誤った処理が行われたり、大量の情報が漏洩してしまったりなど被害・損害が大きくなってしまうことがあります。しかし、多くの場合、問題が発生している時にはその状況がログとして記録されています。定期的にログを確認することで「気が付かない間に起こっていた問題を発見」できることがあります。

気付かない問題を発見する

視点

問題になるようなイベントが発生していたかを確認することです。

例１：ハードウエアに異常がないかの確認

・想定外の時間での停止・再起動イベント、機器温度警告イベント、
動作指示に対する異常終了イベント、障害発生の警告イベント

例２:データベースシステムに異常がないか

・想定外の時間での停止・再起動イベント、システムの異常終了イベント、容量超過のイベント

参考資料
（2019年）

「予防」のレビューの目的・視点

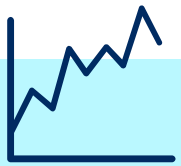
目的

定期的なレビューは、「起きているけれど気づいていない問題」の発見だけではなく、「まだ起きていない問題」の兆候の発見にも役立つ場合があります。システム上の問題の中には実際に被害・損害が発生する前に、なにかしらの兆候を伴うものがあります。こうした兆候を発見して問題(被害・損害)が発生する前に対処する(＝予防する)ことです。

これから起きるかもしれない問題を発見する

視点

問題発生の予兆はあるかを確認することです。



例１：ハードウエアの故障予兆

・処理時間の推移、システム負荷の推移、機器温度の推移、代替セクタの急増(HDDの場合)

例２：データベースシステム異常の予兆

・システム負荷の推移、容量(メモリ・HDD)残量の推移

残りの新規管理策（8項目）

	新規管理策
1	5.7 脅威インテリジェンス
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
6	**8.10 情報の削除**
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**

規格要求事項から見た整理

5.23 クラウドサービス利用における情報セキュリティ

5.23 クラウドサービス利用における情報セキュリティ（要約）

概要

クラウドサービスを利用するケースにおいて組織としてのセキュリティ要求事項に従ったプロセスや手順（調達、利用、管理、及び利用終了）を定める

実現したいこと

直接コントロールが出来ないクラウドサービスにおいて間接コントロール範囲とインタフェースを明確にすることでセキュリティガバナンスを維持・向上させる

具体的な対応内容や補足事項など

・クラウドサービスを選定する上で組織が求めるセキュリティ要件を満たすサービスを選別する

・契約形態によるクラウド環境の責任分界（CSPとCSCの役割と責任の境界と範囲）を明確にし、組織が必要とする情報セキュリティが実現可能か評価する

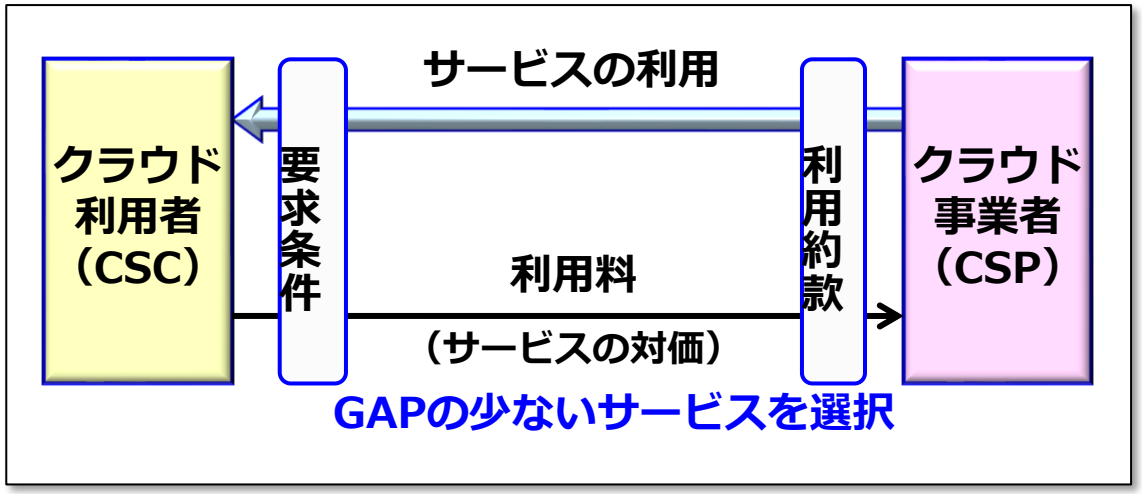
・クラウドの選定基準、利用ルール（申請、注意事項、終了時のデータ削除など）の可視化

<利用ガイドラインなどの例示>

・クラウド選定基準（チェックリストなど）
・利用手続き（利用開始～サービス利用時～終了時の手続き申請）

5.23 クラウドサービス利用における情報セキュリティ（イメージ図）

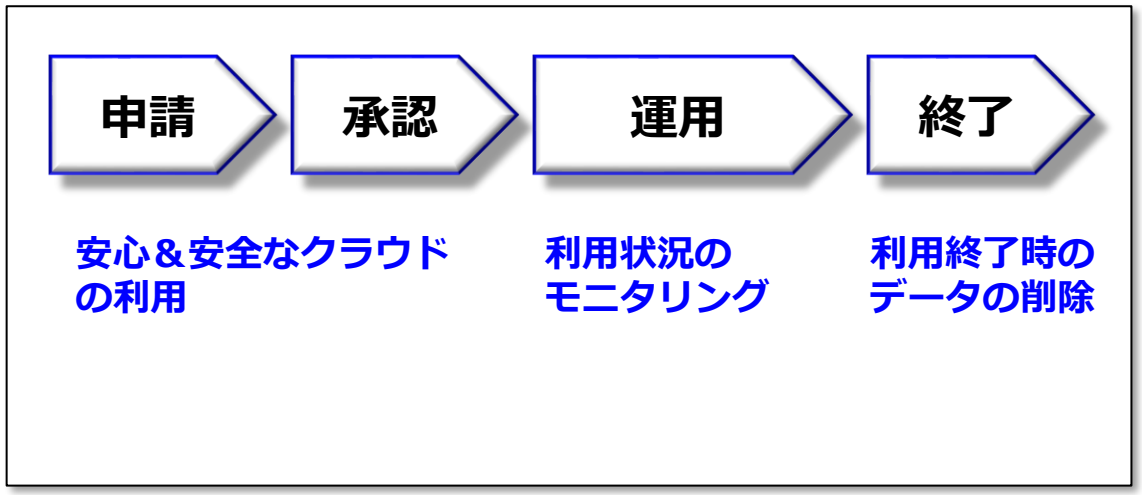
1. クラウド選定基準策定＆サービスの選定



クラウドサービスを選定する上で組織が求めるセキュリティ要件を満たすサービスを選別

クラウドの利用方針、責任共有モデルの理解、自組織が求める要件とのGAPへの対応（一部合致しないものに対し、リスクアセスメントを実施することで追加の管理策を実施）

2. 利用ルールの策定＆運用

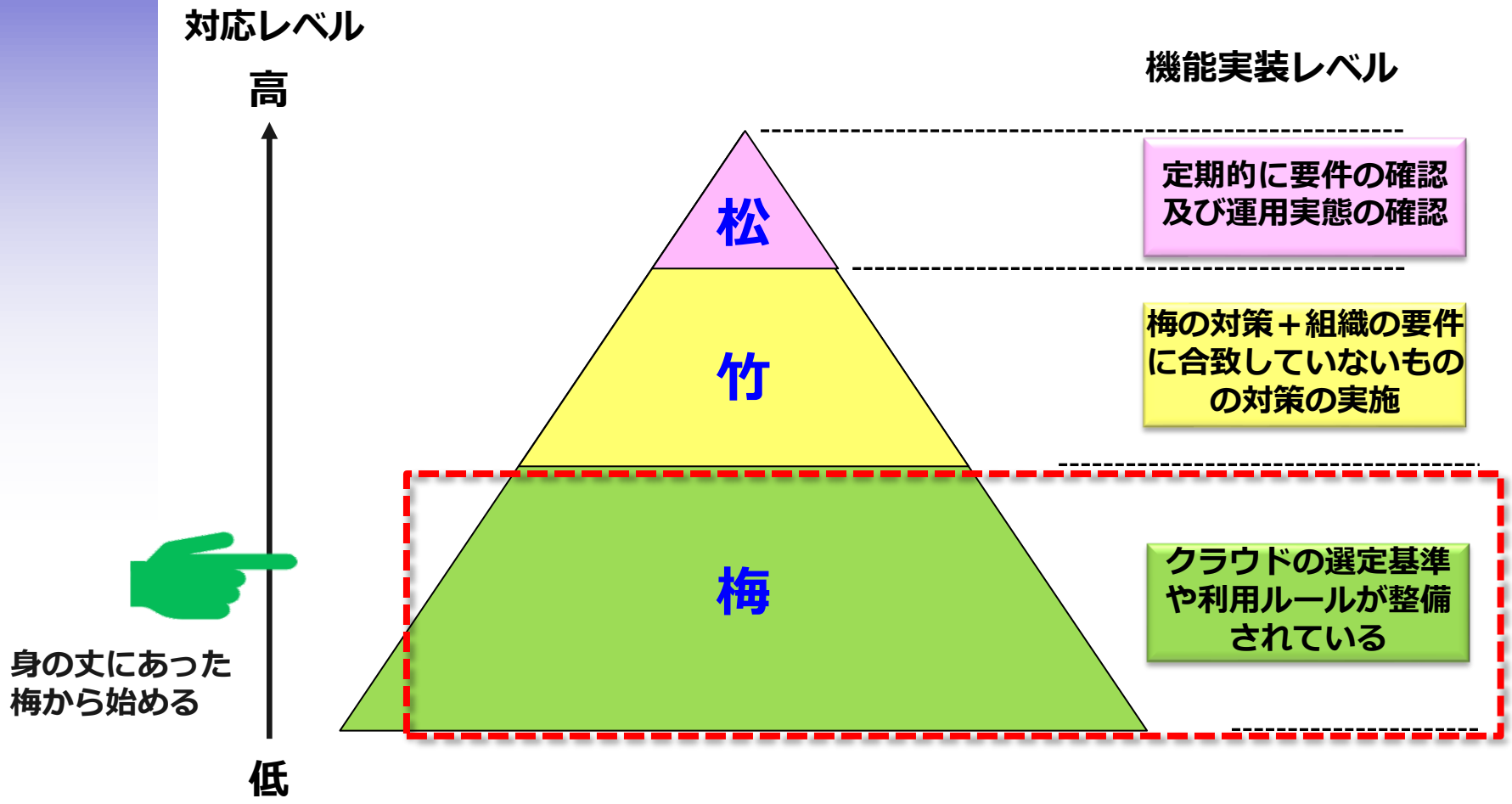


クラウドサービスを利用する上で安心＆安全なクラウドを利用出来るように組織として申請＆承認プロセスを構築する（野良クラウド撲滅）

- 申請＆承認、利用状況のモニタリング
- 利用時における注意事項（アクセス権などのセキュリティ設定など）
- 終了時の確実なデータ削除など

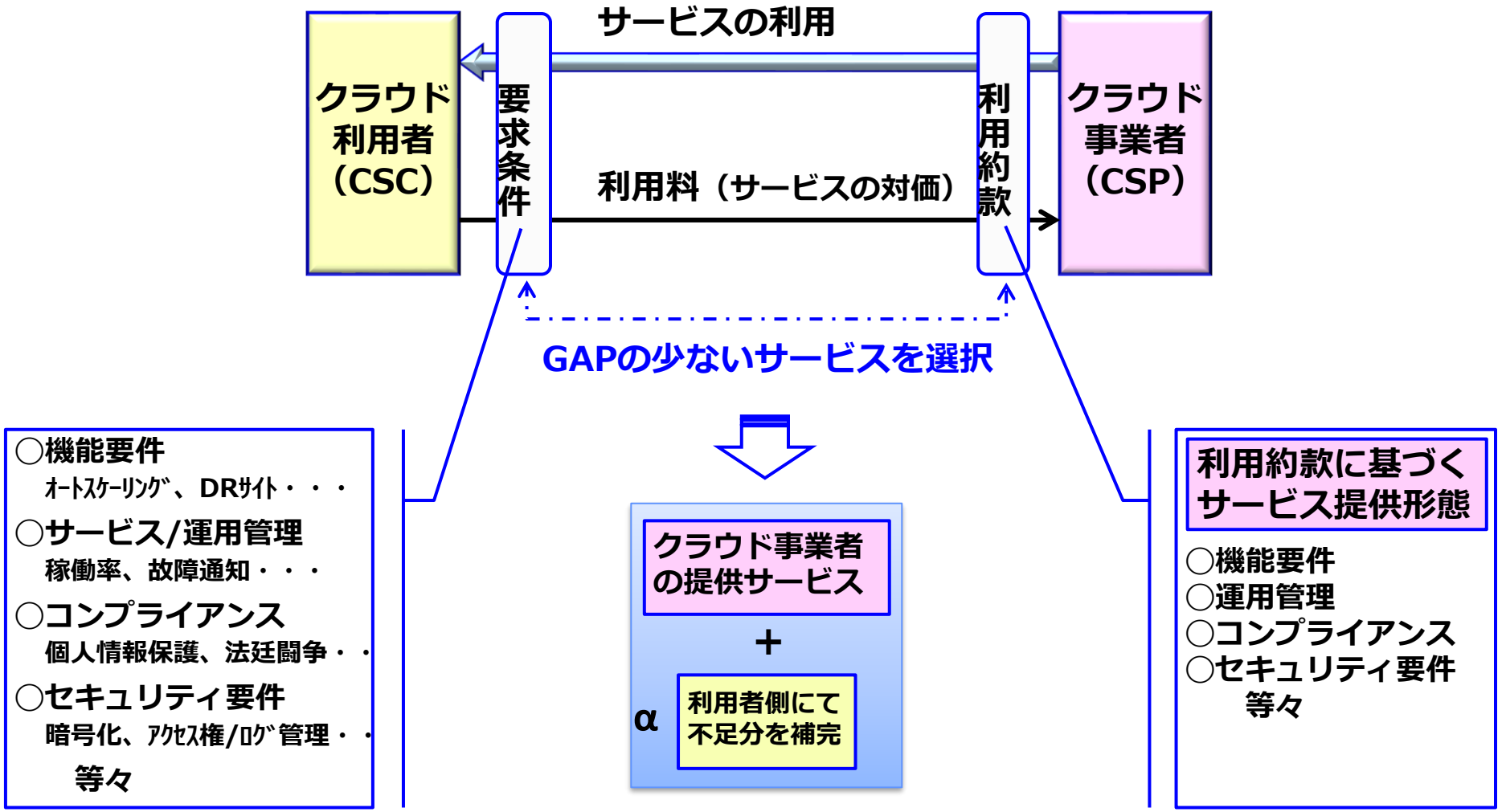
クラウドサービス利用における情報セキュリティの対応レベルについての考え方（案）

クラウドサービス利用における情報セキュリティの管理レベル（案）

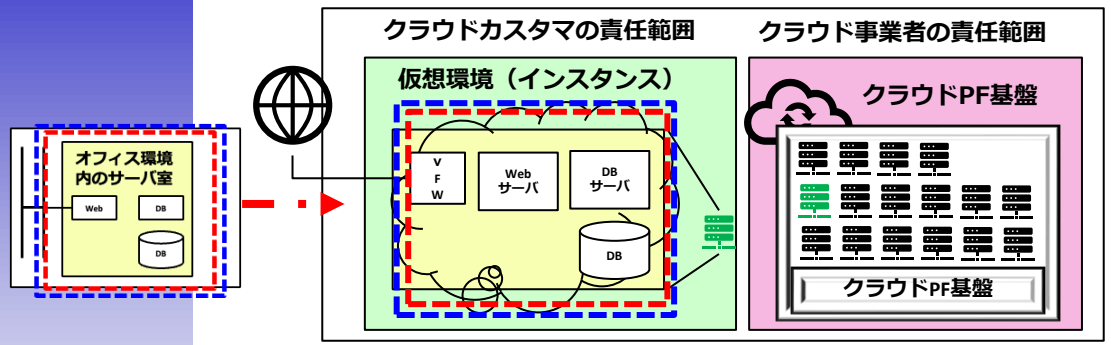


参考： クラウドサービス要件の確認事項（ISO/IEC27017）

サービス要件の確認＆GAPの可視化を実施（サービス利用の観点）



クラウドサービス利用における考慮事項



直接コントロール　間接コントロール

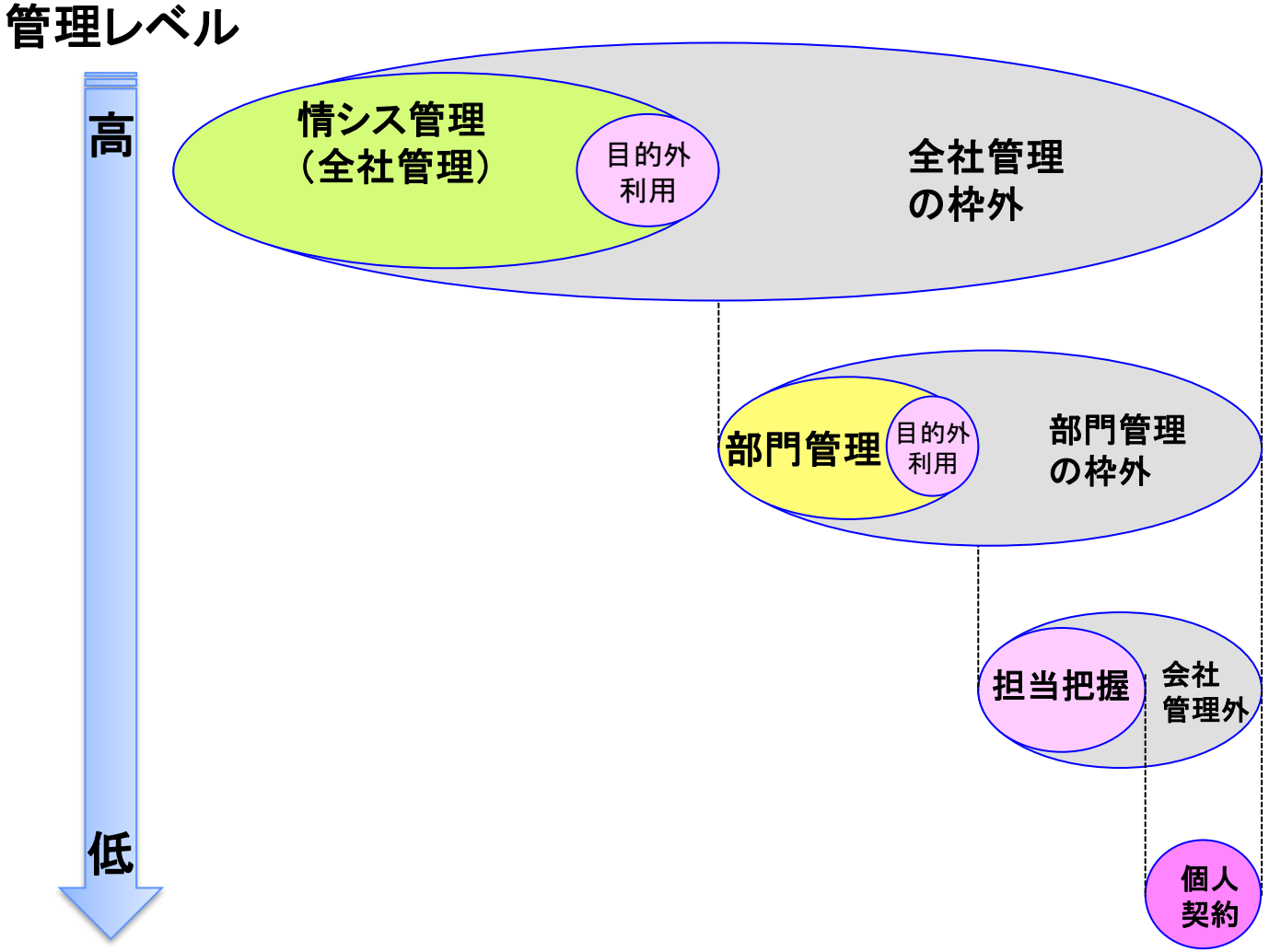
考慮ポイント
（箇条4.3の要求事項）

○外部の課題
　法令やガイドラインへの対応
　（約款の確認、国内リージョン指定など）
○内部の課題
　クラウド利用のガイドラインの制定＆教育
　従業員研修
○利害関係者のニーズ及び期待の理解
　インターネット上でシステムや機密情報が
　適切に管理運用されていること
○組織が実施する活動と他の組織が実施する活動
　との間のインフェース及び依存関係
　クラウド責任分界モデルやA15供給者との関係で整理
　コントロール内、コントロール外での管理策の考えに
　基づき整理を行い、必要に応じて追加の管理策の検討
　→ISMAPを利用した要件の確認など

参考資料
（2019年）

正規クラウド（承認済み）と野良クラウドの定義と管理レベル

管理内/外のクラウドの定義



全社管理のセキュリティルールのもとで運用管理

部門管理だが、セキュリティルールの設定＆運用管理は未徹底

・担当レベルでの把握のみ

・個人契約で管理外

参考資料
（2019年）

野良クラウドのリスクとカテゴリ分類

○野良クラウドのリスク（落とし穴）

- 組織の情報システム部門が導入や運用を把握していないクラウド
- 組織の情報セキュリティポリシーが遵守されないことによる機密情報の漏えいリスクの増大
- 利用状況が見えない（存在の有無がわからない・・・）

野良クラウドのカテゴリ分類

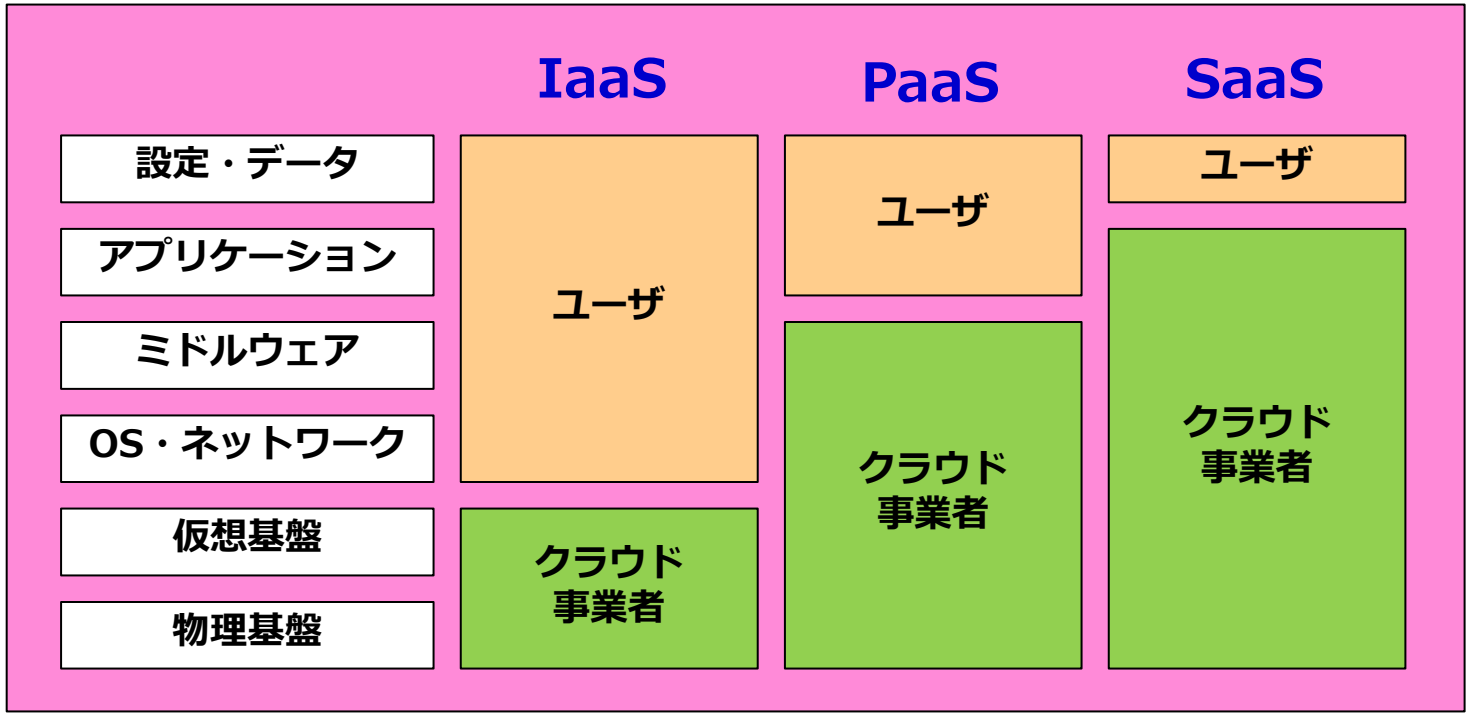
カテゴリ	1		2		3	4
管理主体	情シス管理（全社把握）		部門管理（情シス未把握）		担当（個人）把握（組織管理外）	個人契約分（会社管理外）
管理レベル	リスクアセスメント実施	リスクアセスメント未実施	リスクアセスメント不十分		リスクアセスメント未実施	リスクアセスメント未実施
利用目的範囲内外	利用目的内	利用目的外	利用目的内	利用目的外	未承認	未承認
費用管理	会社負担（無料枠での利用ケースも有）					個人
野良クラウド判定	正規	野良	野良	野良	野良	野良

大 ← 組織としてのコントロール → 小　組織管理外

参考資料
（2019年）

参考： クラウドの責任分界モデル

クラウドサービスの責任分界



責任分界でユーザとクラウド事業者の境界（直接コントロールが可能か否か）が決まる

規格要求事項から見た整理

5.30 事業継続のための ICTの備え

5.30 事業継続のための ICTの備え（要約）

概要

事業継続の中にICT継続の要件を盛り込む

どの程度の経営資源の投入が必要なのか事業影響度分析（BIA）を行うことで目標復旧時間（RTO）と目標復旧レベル（RLO)を設定しその目標達成を確実にするためのリソースを決定し準備＆試験する

実現したいこと

有事の際に
事業の要となるICTサービスについてサービスの全断からどのレベルまで、いつまでに、どのように復旧するかを予め検討＆計画することで事業の再開＆継続を目指す

具体的な対応内容や補足事項など

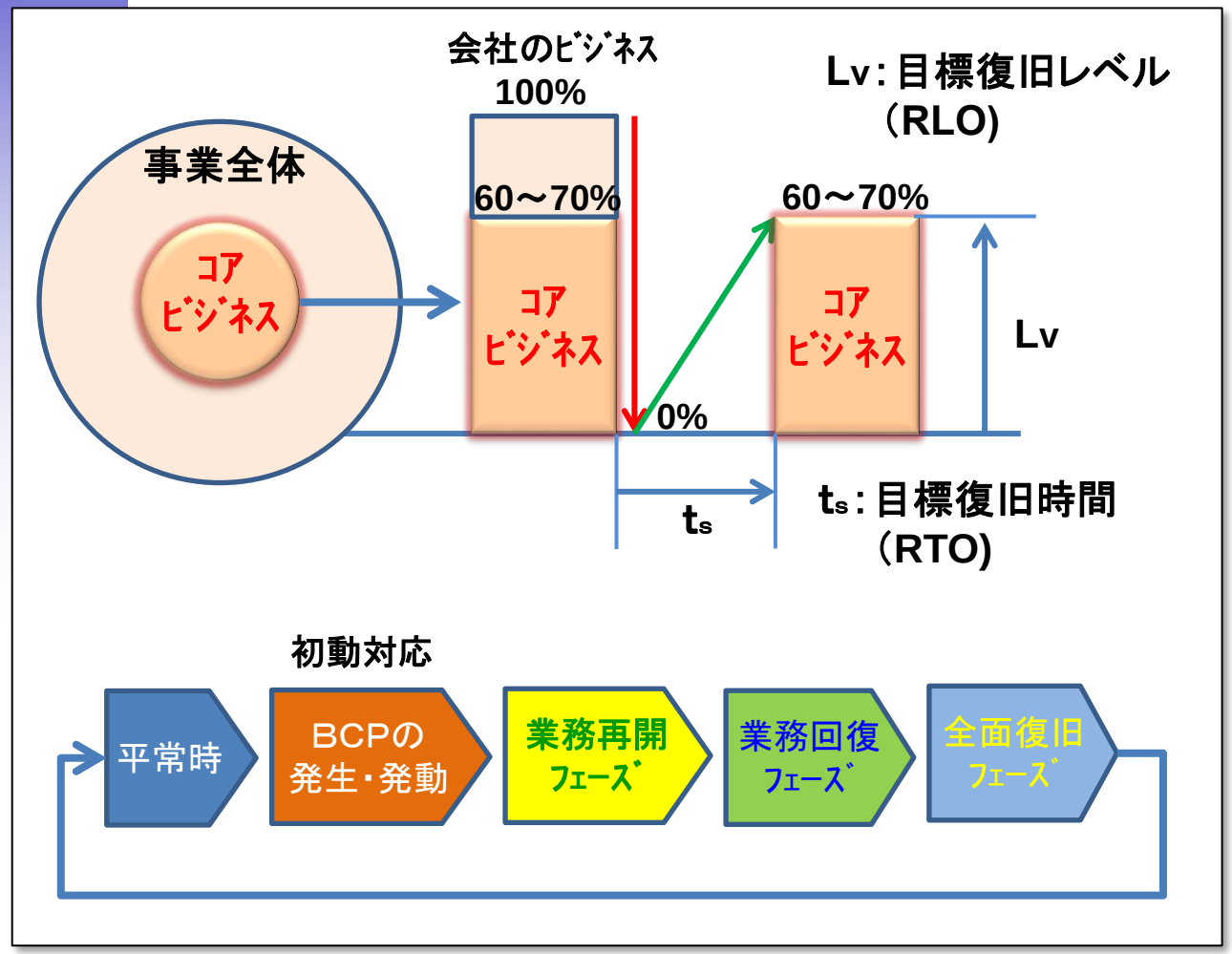
従来の事業継続の中に経営戦略として有事の際にICTサービスについてどのように組み込んでいくかを明確にする（すでにICTについて要件を組み込み済みの場合はそのまま継続）
ICTサービスの全断からいつまでにどのレベルまでどのように復旧するか決定し、リソースの投資＆手順を作成準備（訓練含む）することで実現可能な状態に維持する

＜ICT継続の要求事項の考え方＞

- 事業影響度分析（BIA)を行う
  （事業への影響の種類や基準を加味）
- 優先順位づけを行い、目標回復時間（RTO)と目標復旧レベル（RLO)を設定
- 上記をもとにICT継続計画の策定、演習、復旧手順等を盛り込む

5.30 事業継続のための ICTの備え（イメージ図）

事業継続計画（従来）



要素を加味

ICT-BCPの考慮事項

災害発生やサイバー攻撃などの緊急時において業務に必要なICTシステムを維持する

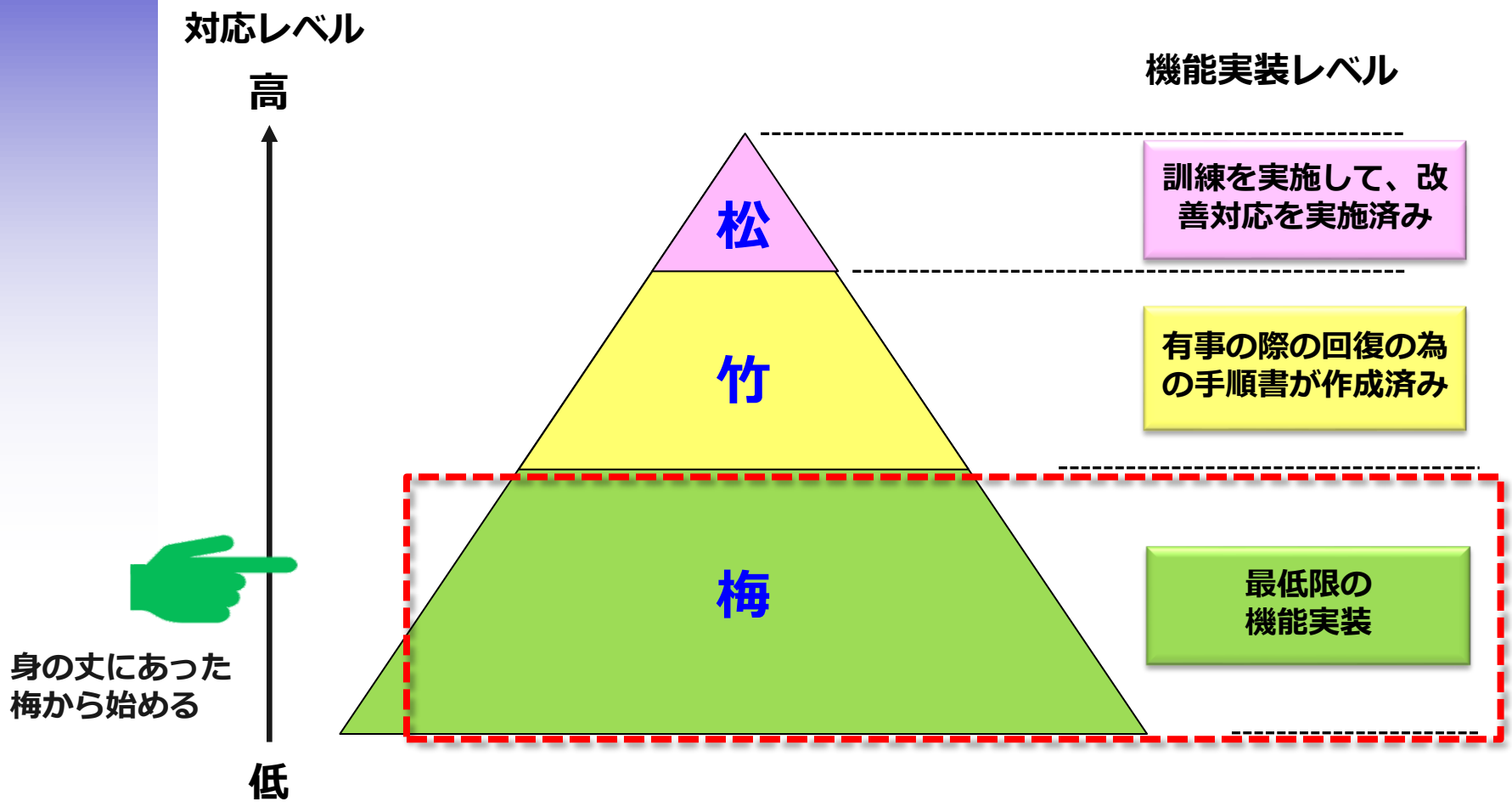
整理の観点

- ICTと業務との関係性
- ICTの管理責任者の明確化
- ICTの課題とその対応策
  （データ保管＆バックアップ、リモートワーク、コミュニケーション手段、セキュリティ対策など）
- BCP時のICT復旧の見込みや対策

など

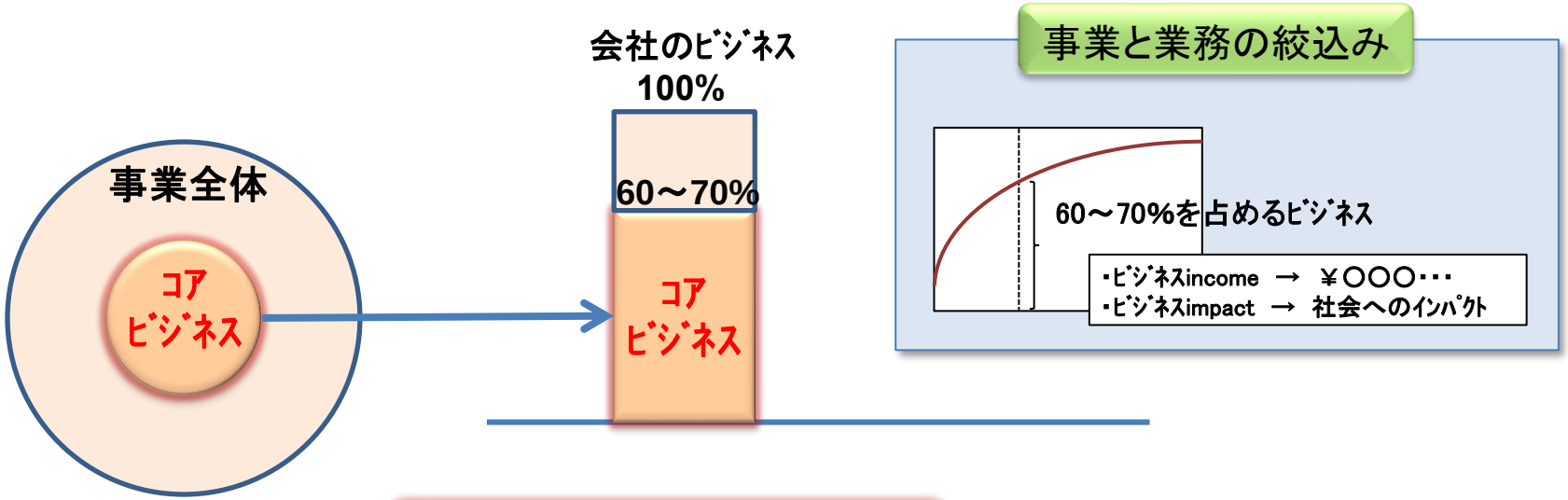
事業継続のための ICTの備えの対応レベルについての考え方（案）

事業継続のための ICTの備えの管理レベル（案）



参考資料
（2012年）

BCPモデル検討の考え方



経営戦略

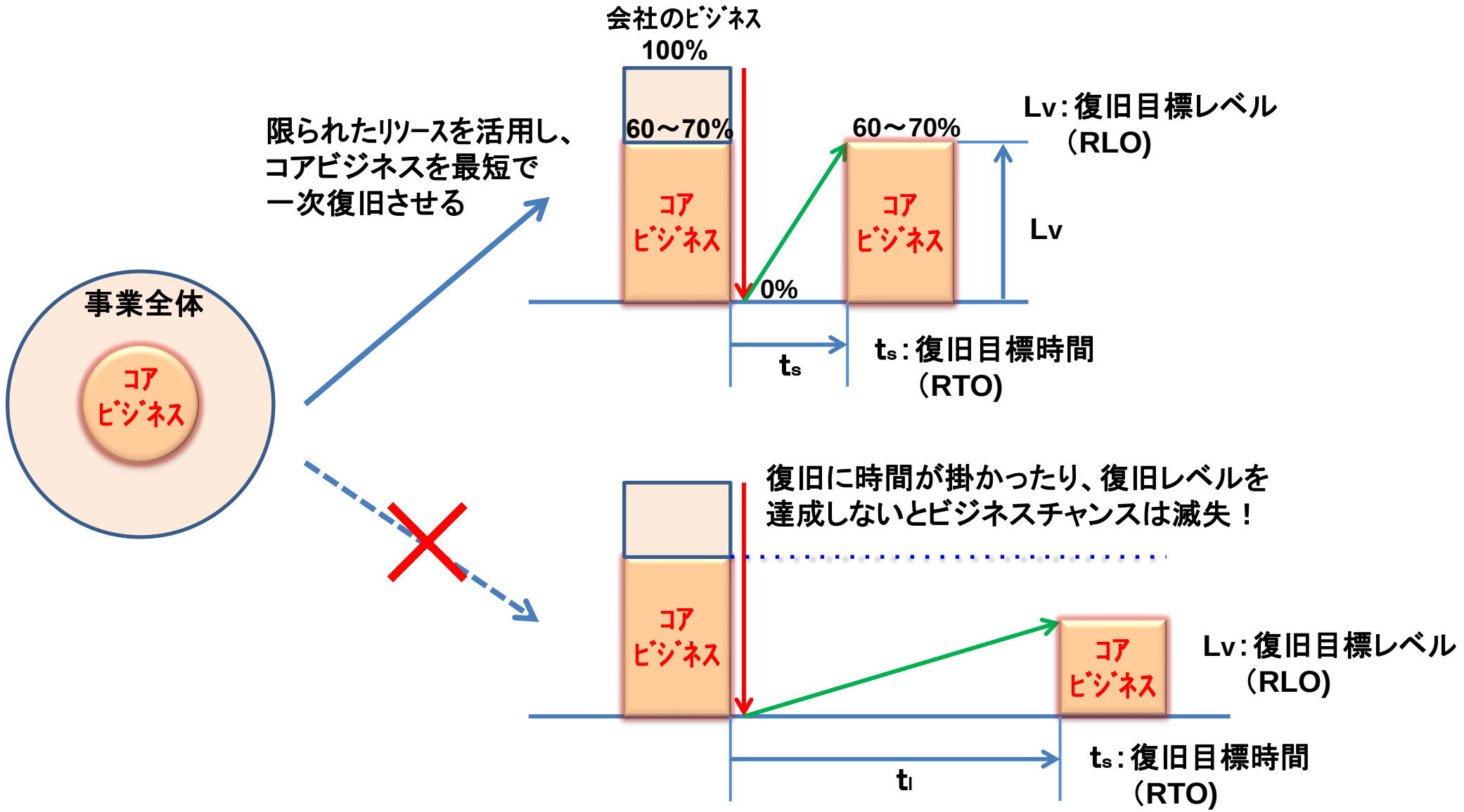
下記の8要素を多角的に判断

コアビジネスの考慮要素

- 収入割合
- 社会ｲﾝﾊﾟｸﾄ
- 市場占有率
- 競合製品
- 自己完結率
- 市場優位性
- 将来性（成長率）
- 相手調和

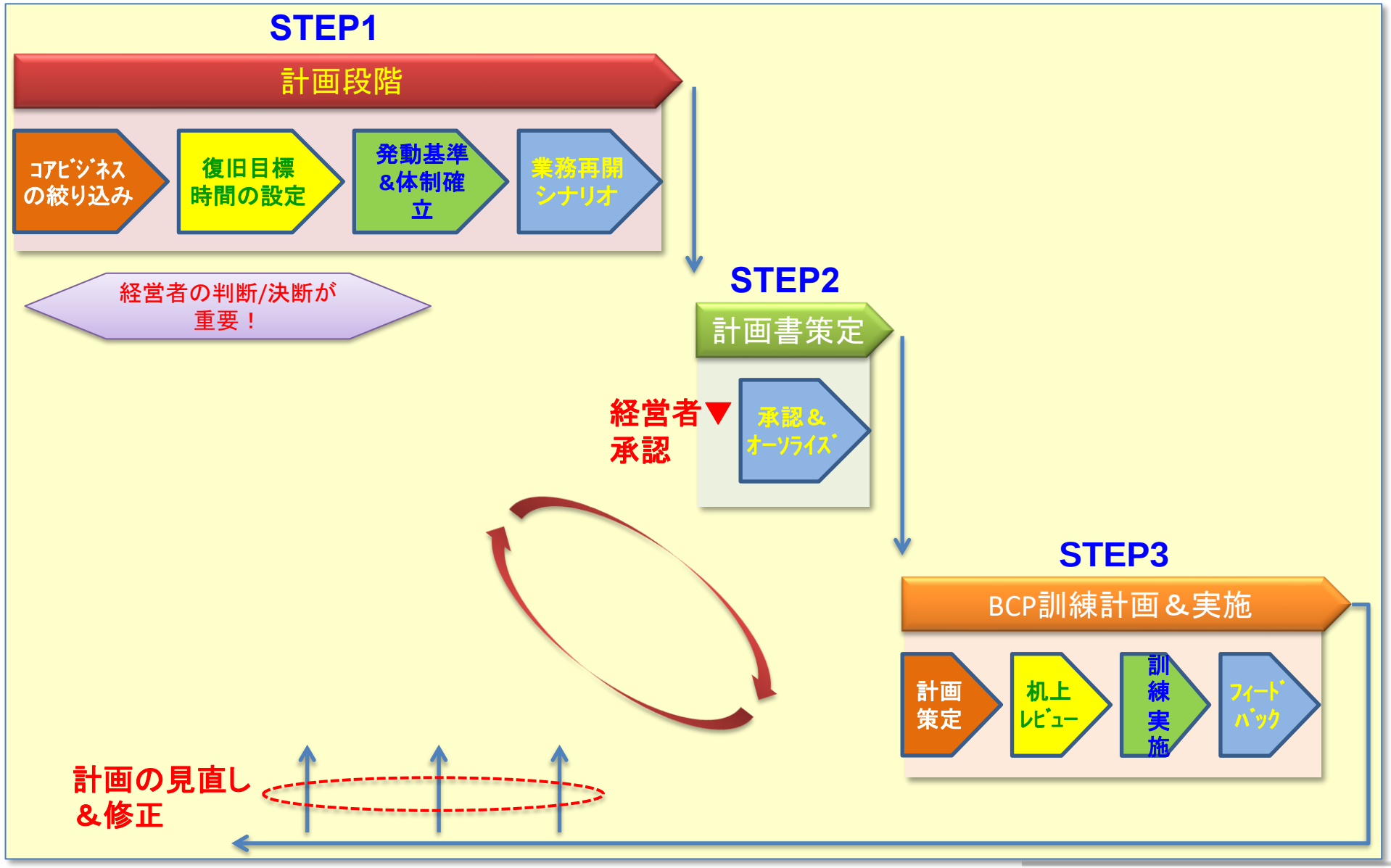
参考資料
（2012年）

BCPモデル検討の考え方



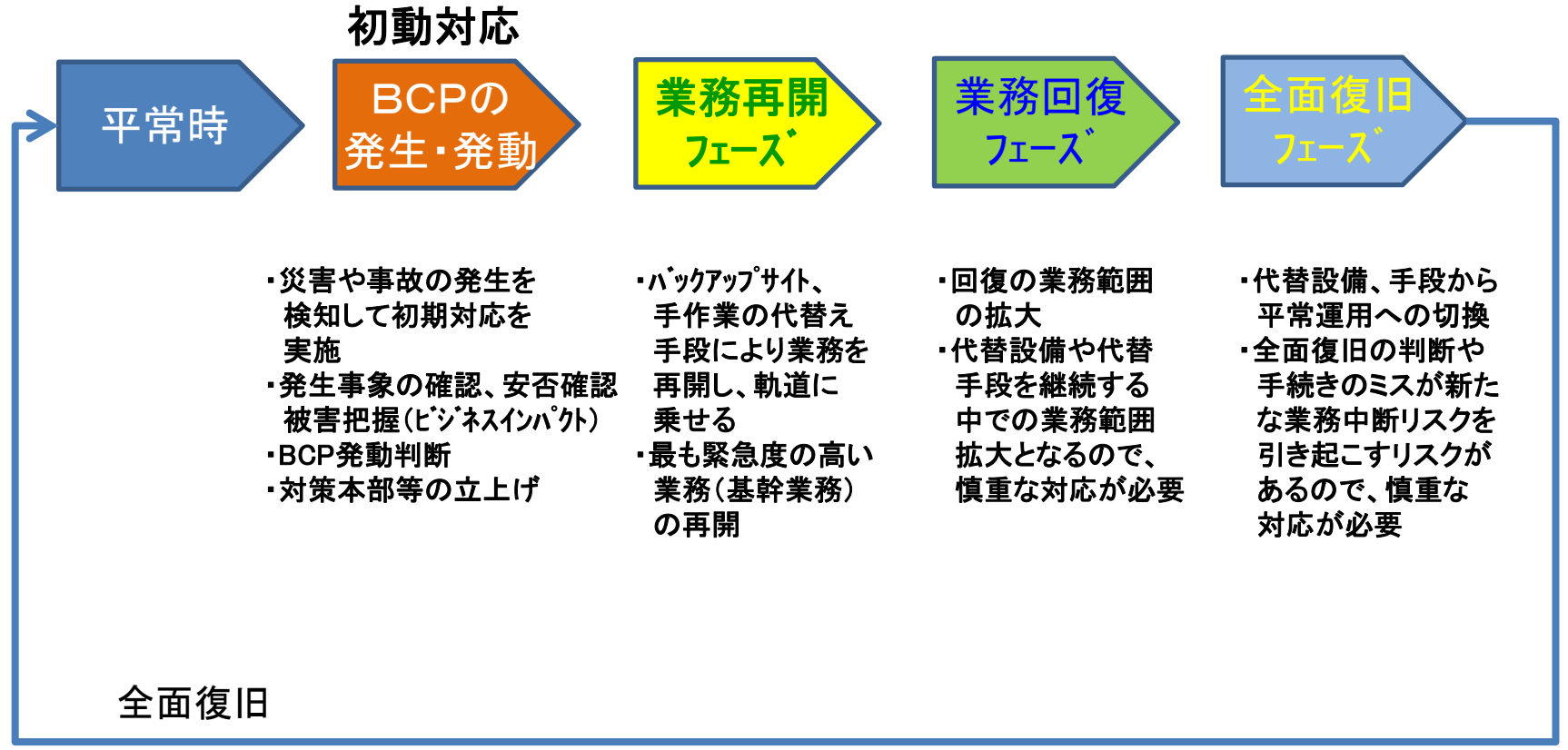
参考資料
（2012年）

BCP全体のフレームワーク



参考資料
（2012年）

BCP発動時のフェーズの流れ



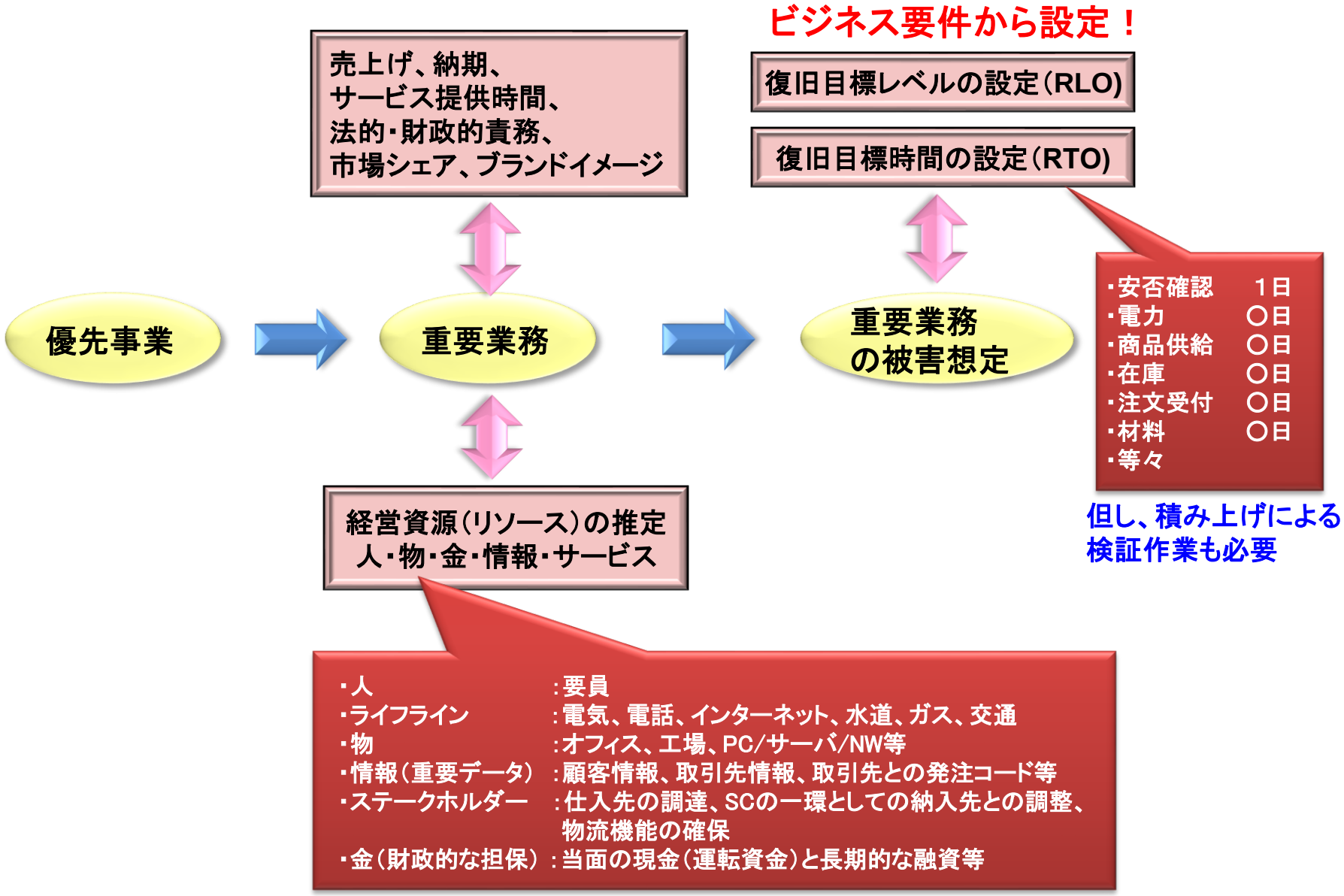
BCP訓練として実施される多くのパターン例 → 緊急連絡訓練

本来のBCP訓練のスコープ範囲

参考資料
（2012年）

BCP対象業務の絞り込みの考え方

STEP1



規格要求事項から見た整理

7.4 物理的セキュリティの監視

7.4 物理的セキュリティの監視（要約）

概要

保護すべき領域での作業において認可されていない活動を検知し、窃盗・盗難、破壊、干渉などを防止するために、セキュリティ対策を実施し、物理的アクセスを監視（人的監視、システム監視など）する

実現したいこと

認可していない物理的アクセスについて継続的に監視することで外部や内部からの不正なアクセスによる窃盗・盗難、破壊、干渉などを防止するため

具体的な対応内容や補足事項など

・組織全体としてのルール整備として保有する情報資産のレベルに応じた対策を共通ルール化することで不正アクセスなどのリスクを低減する

・運用管理において共通ルール化された対策に従った監視＆防御を実施する（必要に応じてリスクアセスメントを実施）

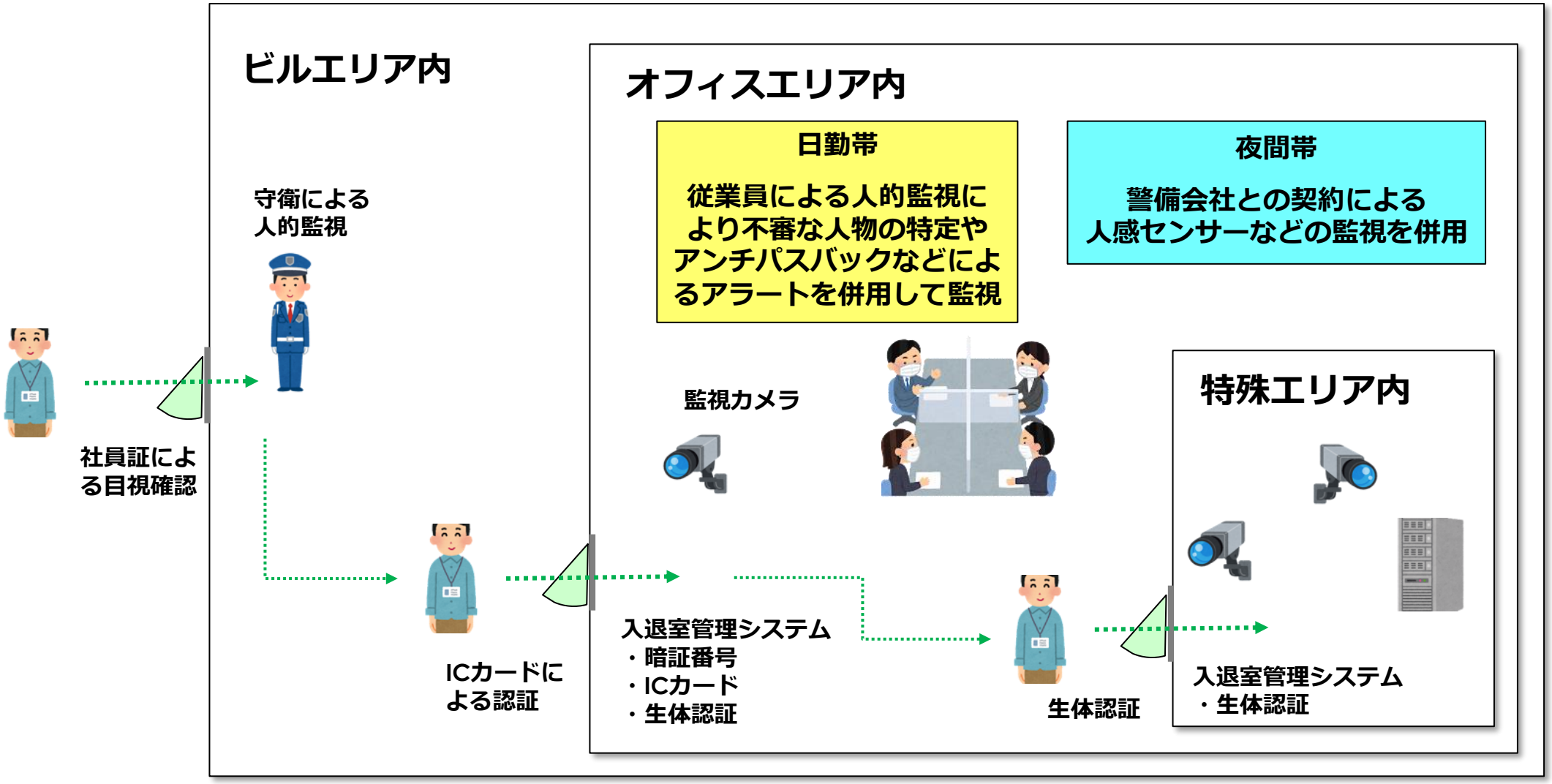
＜情報の例示＞

・入退室ログやアラート
・監視カメラ映像
・各種監視ツールによるログ

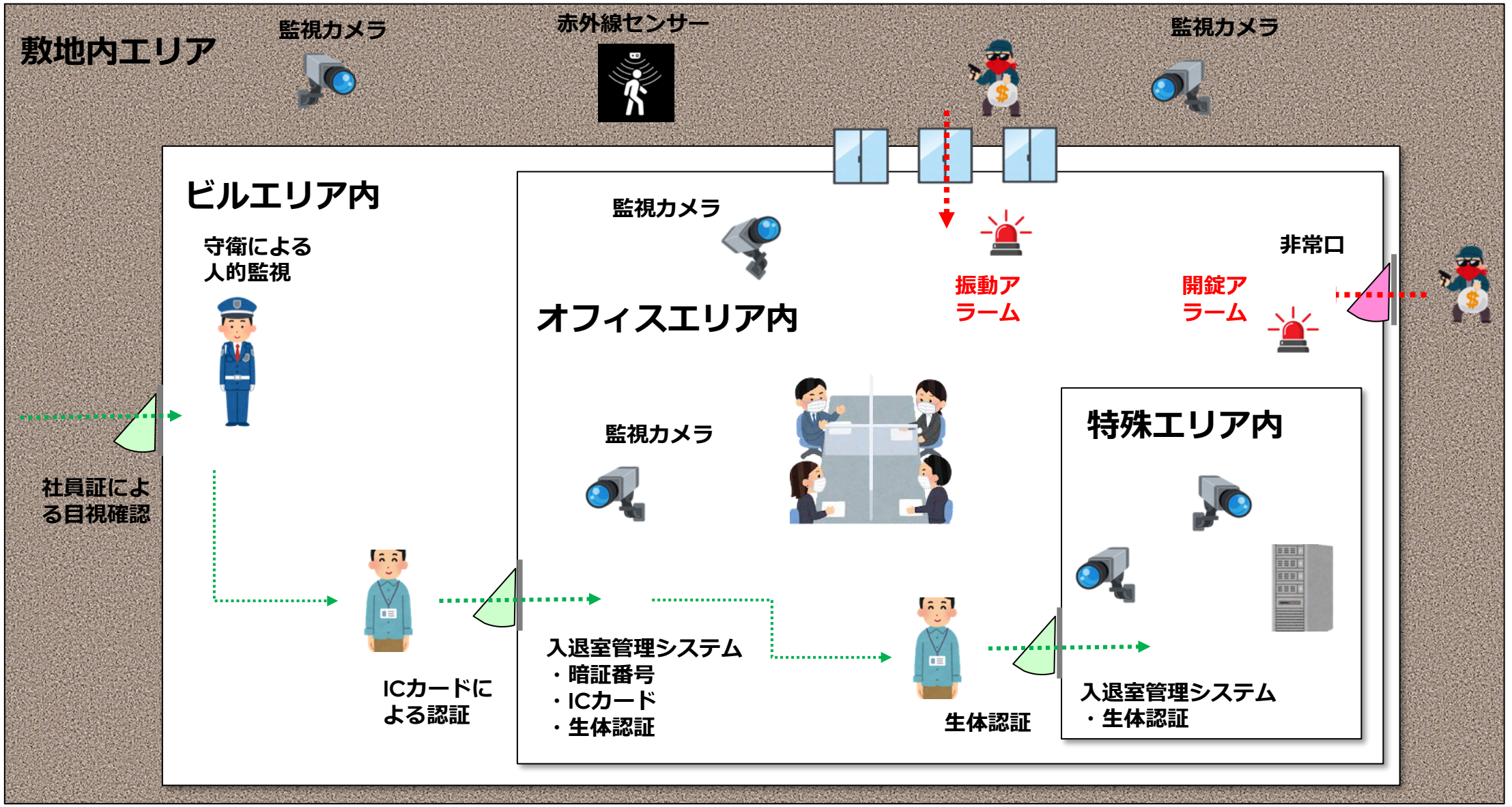
など

7.4 物理的セキュリティの監視（イメージ図）

下記はイメージ図（物理的セキュリティの監視の全体像）・・・正規の出入り口



非正規の出入り口からの侵入のリスク事例

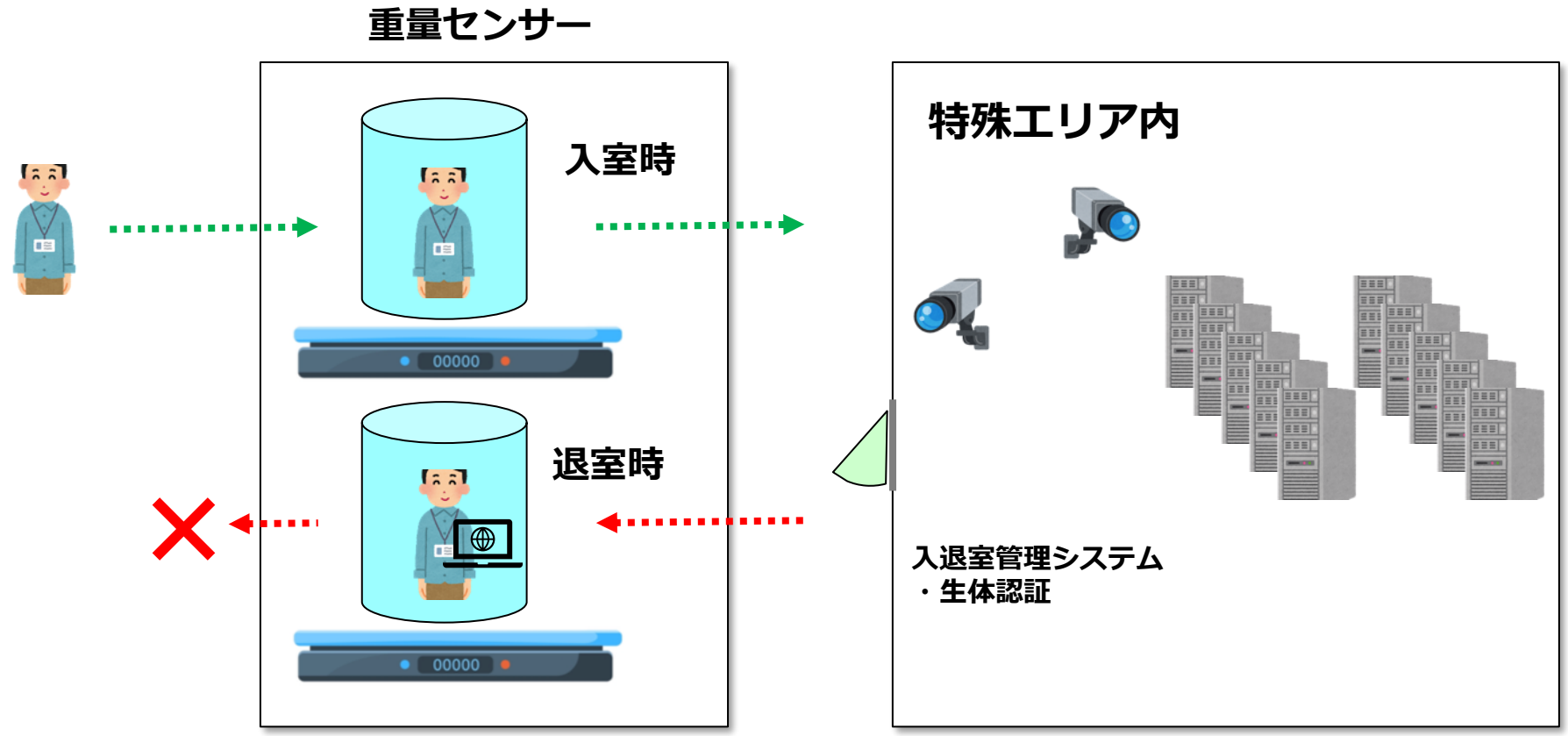


事例

入退室時の重量センサーの事例（松の特殊事例）

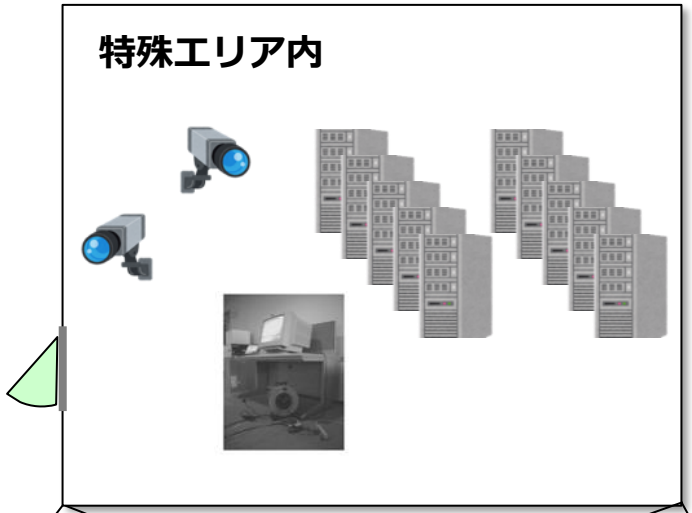
特別に重要なエリアの入退室管理で厳密性を求める場合は下記のような対策を選択する場合がある

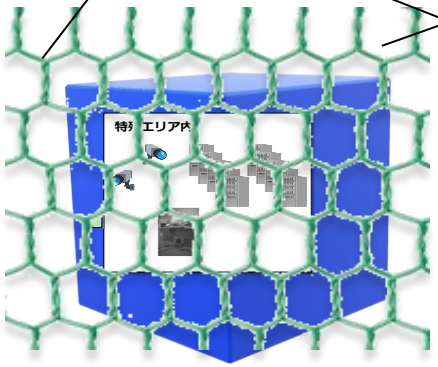
入退室時の重量を計測することで機器の持ち込み、持ち出し等を検知
＆アラートを発報することで情報漏洩などのリスクを軽減する



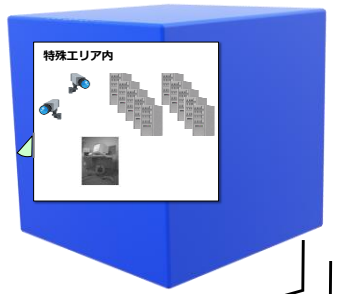
事例

ディスプレイの微弱電波を受信して画像化の事例（松の特殊事例）





データセンタ自体を金網で囲いアースを実施（実際の導入事例有り）



対策未実施

資料：端末からの漏洩電磁波の傍受による表示画面の再現実験

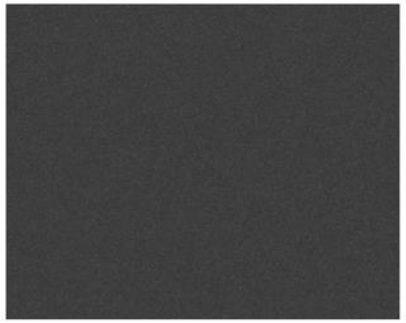


図 7　同調前のノイズ画面
Fig. 7　Noise image before tunings

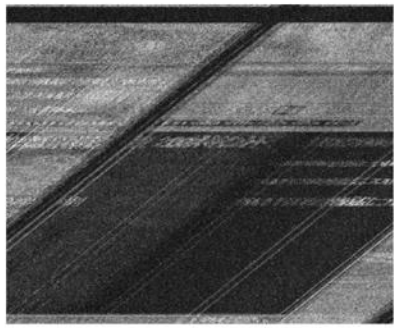


図 8　同調後の傍受画面(未処理)
Fig. 8　TEMPEST image under processing

図 9　実験 A における最も鮮明な傍受画面
(32 枚の画面を平均化した結果)
Fig. 9　Completed TEMPEST image of desktop PC with LCD (32 frames averaging image)

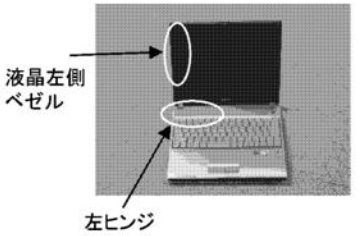


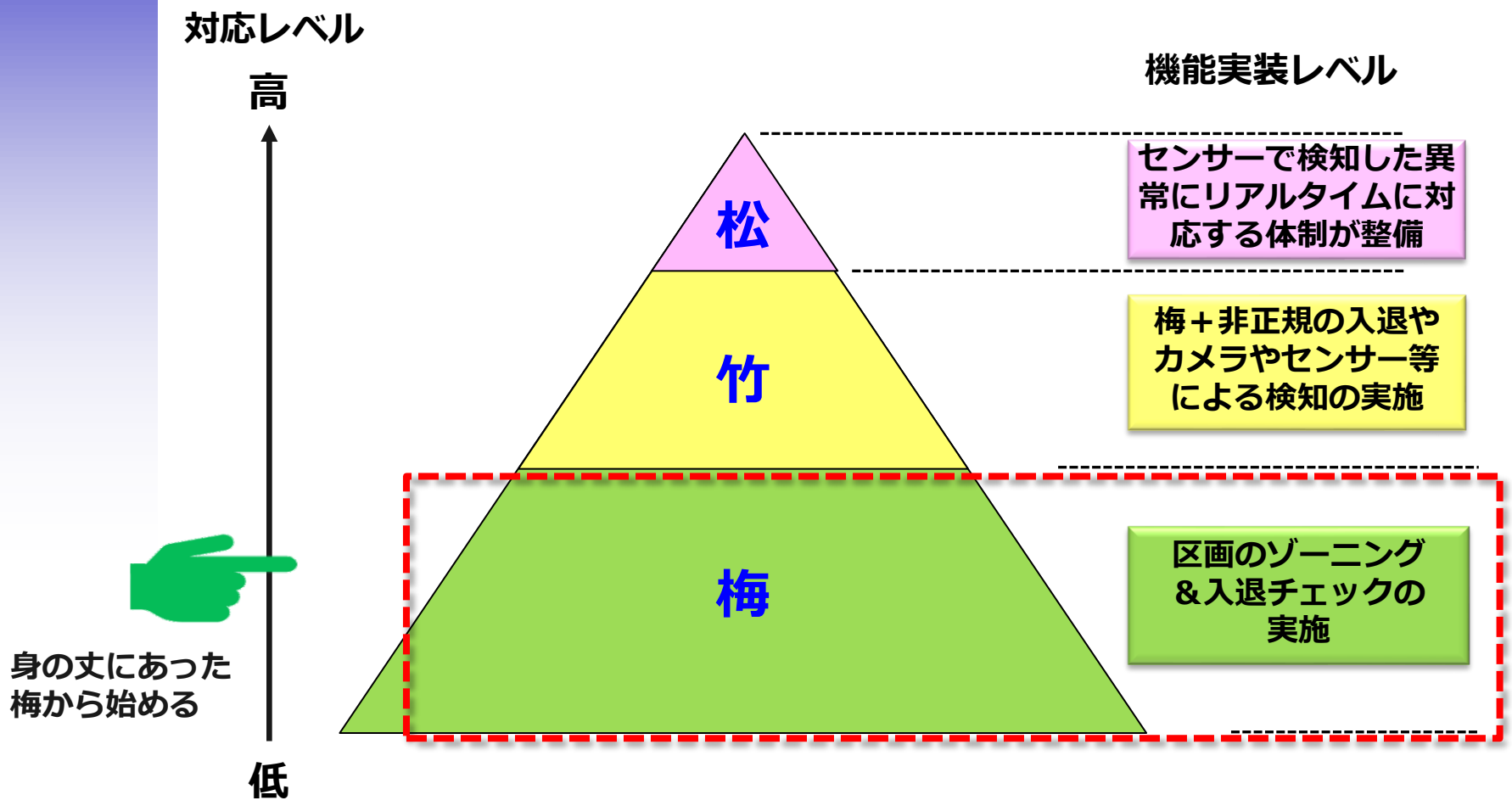
図 10　ノート PC において顕著に電磁波の漏洩が観測された箇所(白円の内側)
Fig. 10　The place (inside of white circle of the figure) of Note PC where the electromagnetic wave is emanated most.

微弱電波を受信して画像化する（数十m以上離れてもOK)

https://www.jstage.jst.go.jp/article/iieej/34/2/34_2_147/_pdf
https://www.ieice.org/~cs-edit/magazine/ieice/spsec/Bplus10_sp.pdf

物理的セキュリティの監視の対応レベルについての考え方（案）

物理的セキュリティの監視の管理レベル（案）



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

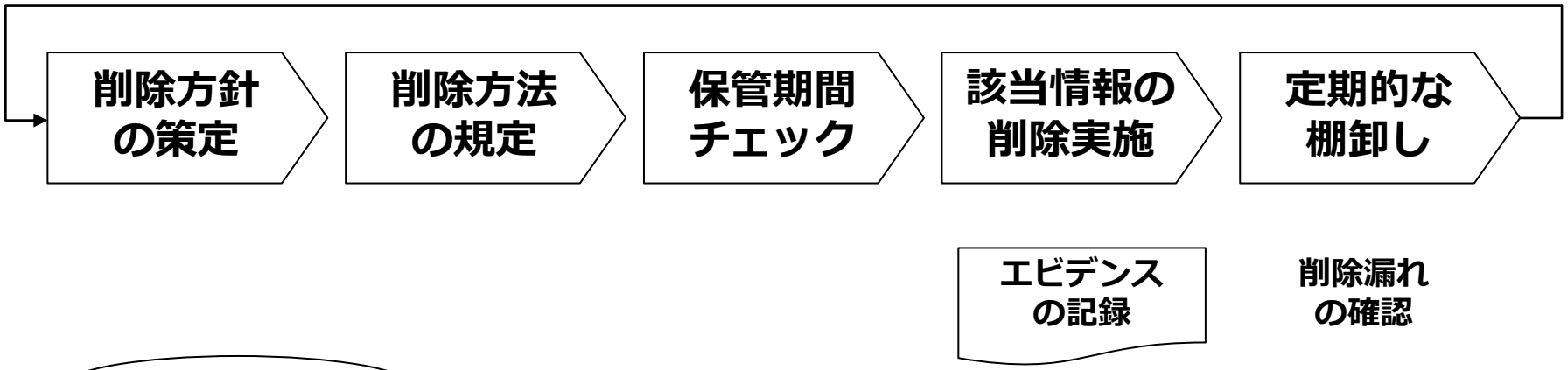
・ビジネスの現場において情報資産台帳に保有期限を掲載し、定期的に削除プロセスを実施することによる漏洩リスクの低減を図る

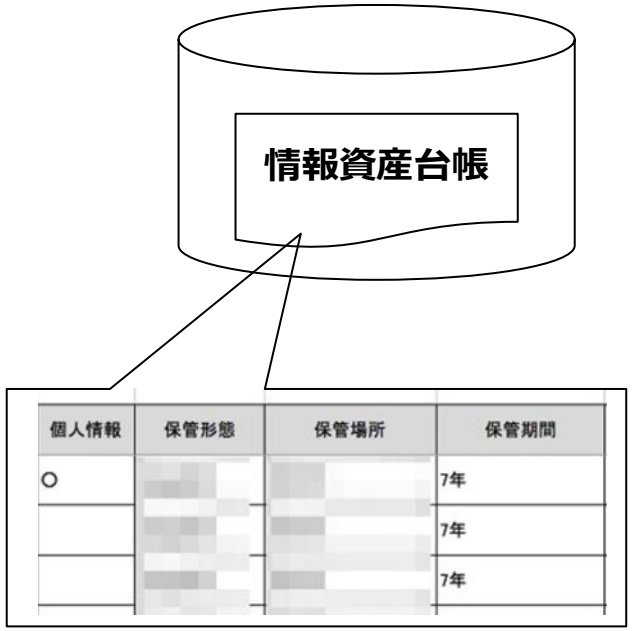
＜削除における考慮事項＞

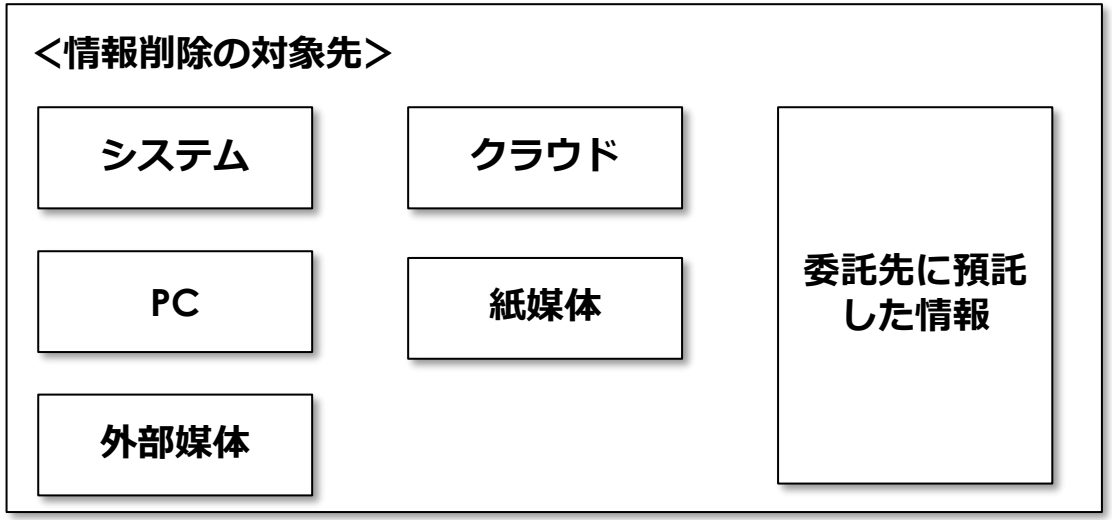
・情報の削除方針の明確化（情報の種類、機密レベル、業務上＆法律要件を加味）
・削除方法の規定
・エビデンスの記録
・システムや委託先の保管情報も加味
・定期的な棚卸しによる削除漏れ防止

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1）

◯復元不可能な方法で消去

分類	情報削除方法例	備考
紙	焼却、溶解、シュレッダーなど	
電子データ（クラウド内の保有データ含む）	データ削除ソフト（完全消去ツールなど）による消去など クラウド（サービス毎に事前に確認）	事前に暗号化対応も有効な手段
記録媒体	専用ソフトウェアによる消去処理など	

◯廃棄・削除したことを記録しておく

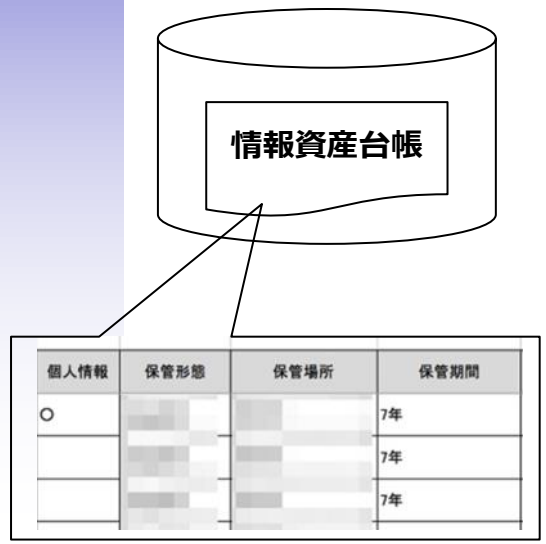
「廃棄した日」「内容」「廃棄責任者」などを記録、この廃棄記録も厳重に保管

◯委託先/再委託先に預託した情報の場合

自組織で削除するケースと同様に上記の対応を意識する必要があるので留意する
また、契約に基づく依頼を実施する必要があるので、契約時から意識する必要あり

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）

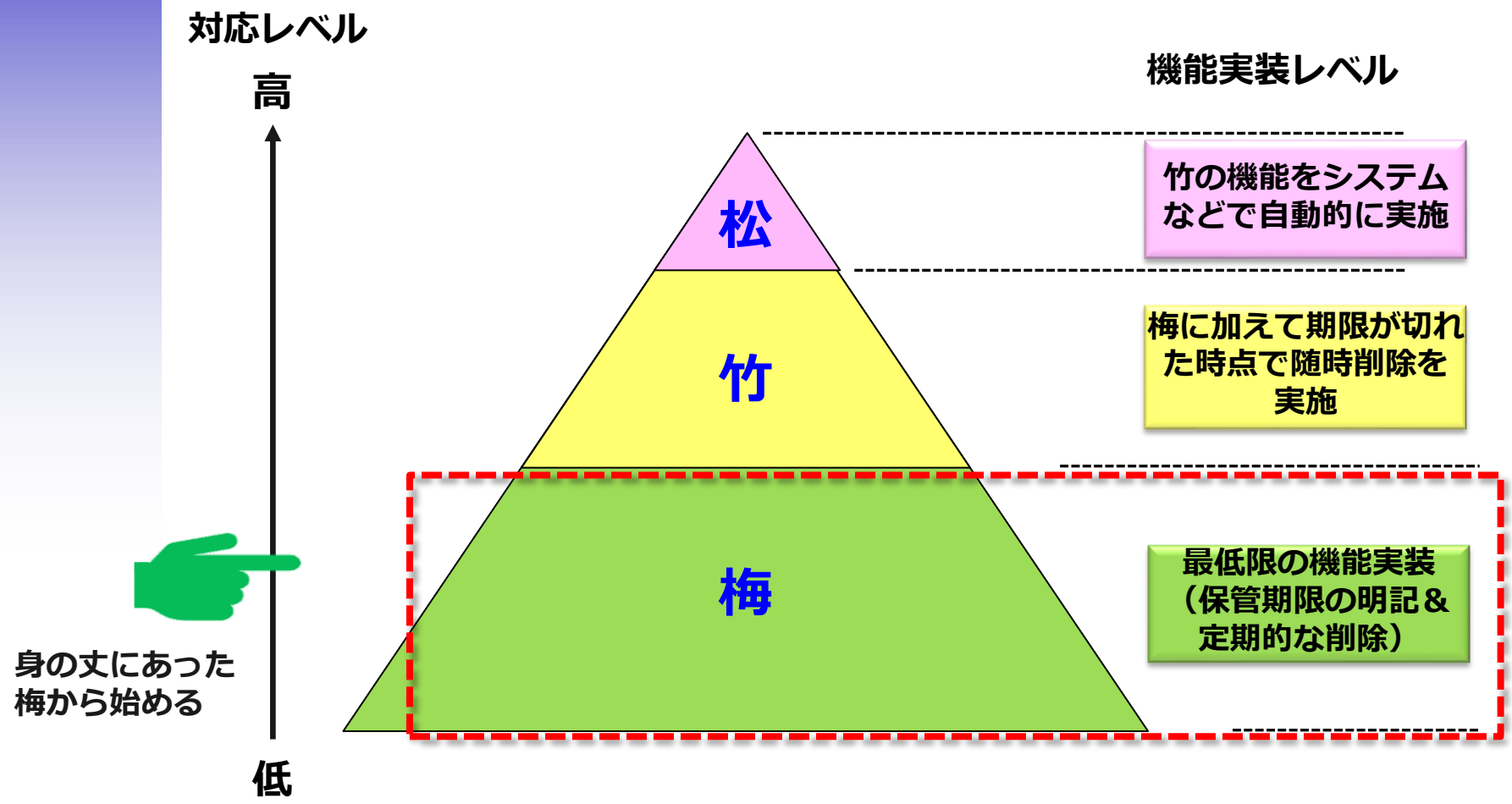


情報（例）	保管期間	起算日	備考
契約書	10年	契約の満期日や解約日から起算	会社法により10年間保管（各事業年度の確定申告時に青色申告書を提出している法人）
	7年		法人税法施行規則により7年間保管（帳簿書類や取引で作成・受領した各種書類も7年間保管）
人事情報（履歴書）	5年	退職の日から起算	労働基準法 法改正の経過措置として「当分の間は３年間」
雇用保険の被保険者に関する書類	4年	被保険者がその事業所に在籍しなくなった日	雇用保険法施行規則

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

情報の削除の対応レベルについての考え方（案）

情報の削除の管理レベル（案）



規格要求事項から見た整理

8.11 データマスキング

8.11 データマスキング（要約）

概要

個人情報保護法における「匿名加工情報」対応などの適用される法令を考慮し、個人情報及びその他の機微な情報を外部から解読できない状態にするための方針や要求事項に従ったデータのマスキングを実施し、利用する

実現したいこと

データの活用場面のリスクに応じて、データの一部を隠す（マスキングする）ことで不必要なメンバーに開示させない、個人情報などの機微な情報を暗号化や仮名化で解読出来ないようにすることでリスクを低減する

具体的な対応内容や補足事項など

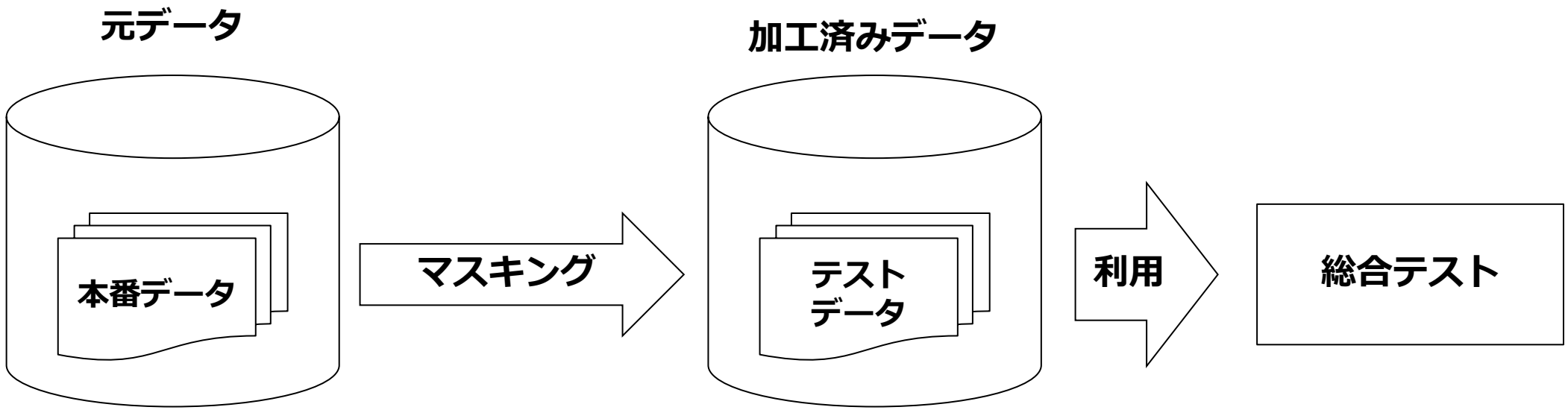
- アプリケーション表示・入力項目において特定の役割のメンバーのみ限定するなど
- テストにおける品質向上を目的とした本番データの活用時のデータ加工の方針の決定および対応方法の明確化
- 個人データの分析時に機微情報等を無効化することで不必要な情報の開示を行わない

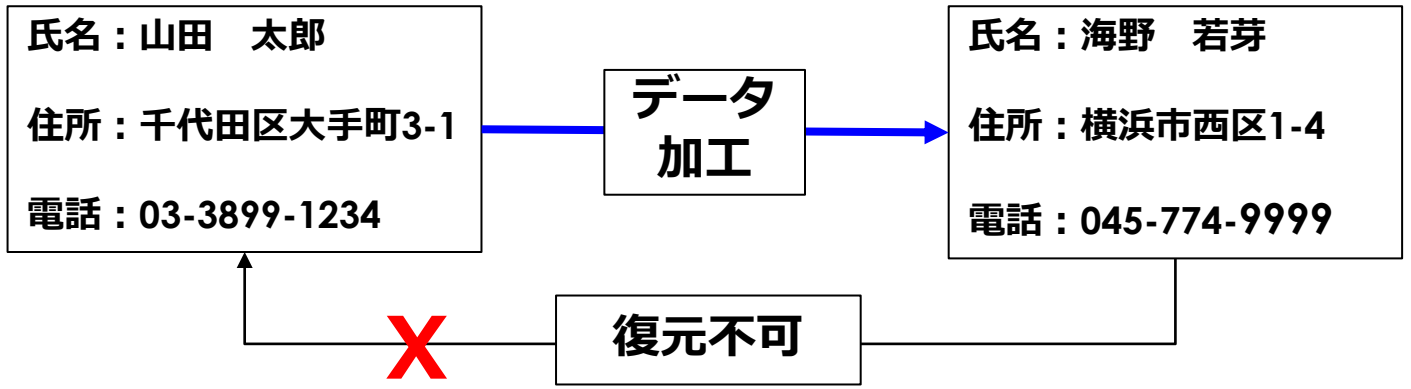
＜マスキング事例＞

- アプリケーション表示において特定の役割のメンバー以外には表示しない
- 暗号化
- 文字の無効化、削除、置換（全置き換え、クレジット番号などのように下3桁以外＊表示など）

8.11 データマスキング（イメージ図）

テストデータの加工の事例





＜加工方法の注意点＞

・不可逆な状態にする
・他の情報と突合すること
　で復元出来ないこと
・専用のツール等の利用推奨
　（抜け漏れの防止）

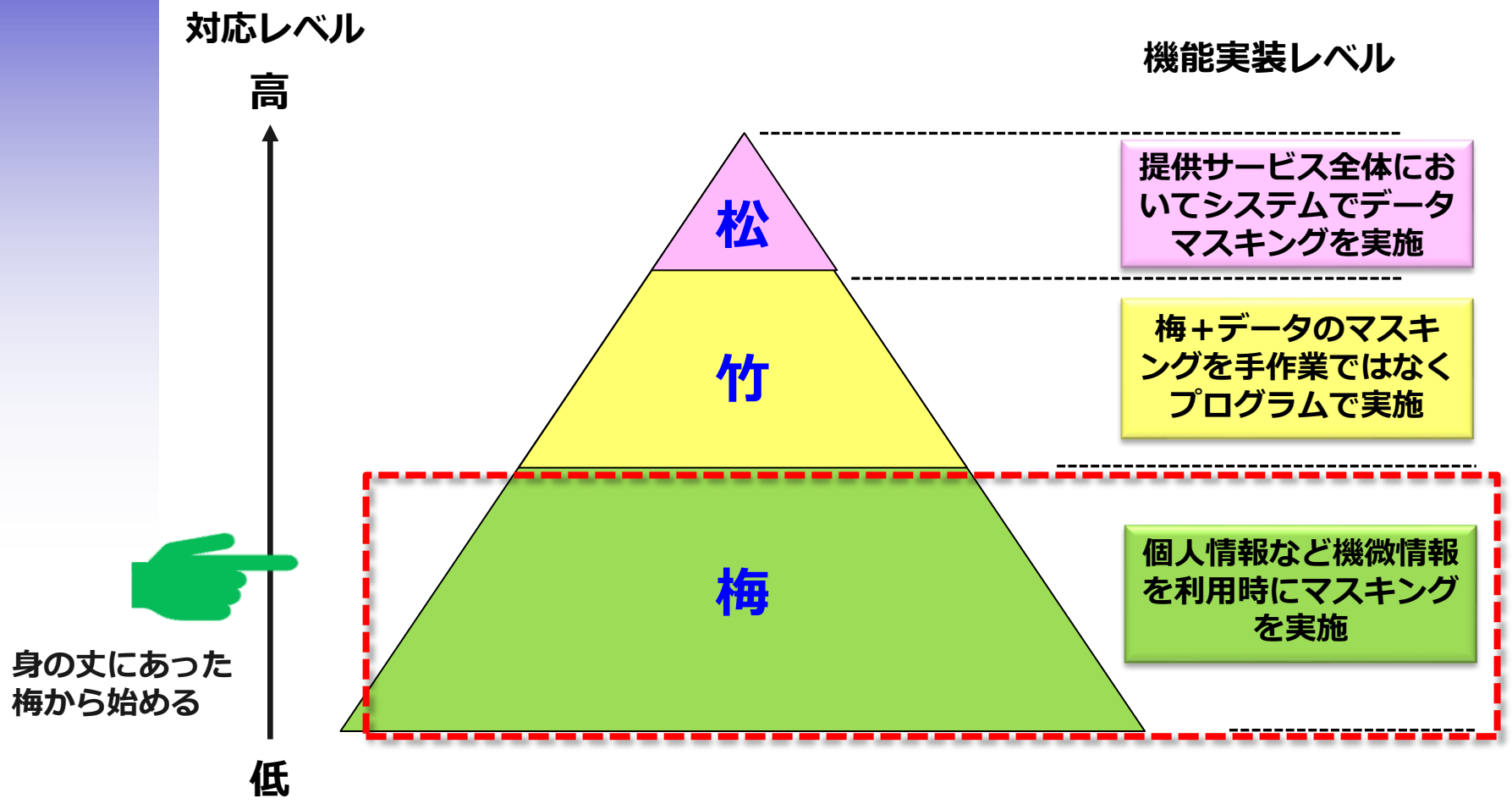
データマスキングの事例（主な用途と匿名化方法）

データマスキングとは、おもにシステムやアプリケーション開発において、機密情報を保護するために実施する工程として使われます。
具体的には、テストのために本番環境から非本番環境へデータをコピーする際に、その**一部を書き換えることでデータを匿名化する**ことで機密情報を保護します。

主な用途	匿名化方法
・テスト環境へのデータ移行 ・社内でのデータ共有 ・外部とのデータ共有（委託先へ渡してテストデータとして利用、統計分析の元データなど）	・文字列の一部を置換する方法 ・データの組み合わせをシャッフルする方法 ・暗号化する方法

データマスキングの対応レベルについての考え方（案）

データマスキングの管理レベル（案）



規格要求事項から見た整理

8.12 データ漏えいの防止

8.12 データ漏えいの防止（要約）

概要

組織が保護すべき情報において外部からの攻撃（不正アクセスや盗聴及びマルウェア感染）や内部不正やシステムの設定ミス、運用ミスによっても生じる情報漏えいについて、個人又はシステムによる情報の認可されていない開示及び抽出を検出し防止する

実現したいこと

様々なデータ漏えいのリスク（外部攻撃や内部不正や運用ミスや故障による場合など）に応じて認可されていない開示の可能性を網羅的に発見し防止する

具体的な対応内容や補足事項など

- 漏洩から守る情報（個人情報、機密情報など）の特定を行う
- 特定した情報に対してシステム運用監視において不正アクセスなどの外部攻撃や内部不正による情報漏洩に関する検知＆防御を行う
- 業務運用における内部不正防止のためのプロセス作りを行う

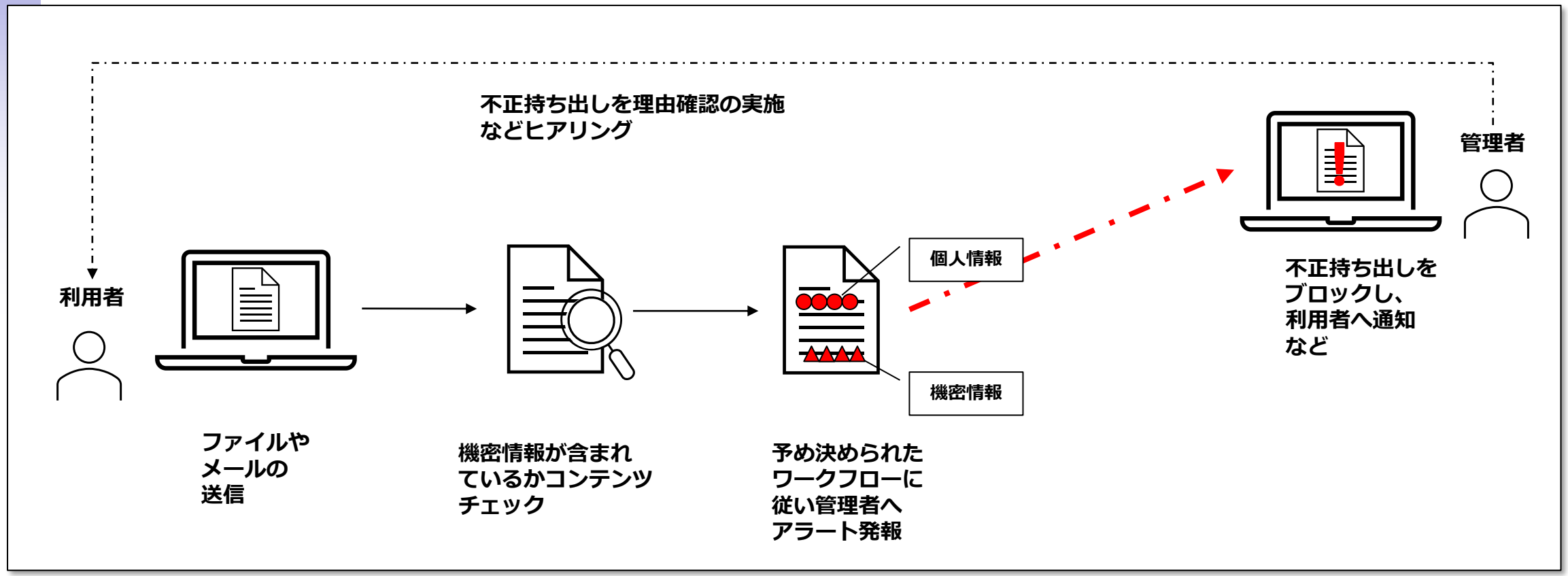
＜データ漏洩防止ツールや運用対策の例示＞

- Webフィルタリング
  →特定URL/単語の検出と制限
- EndPoint DLP
- NetWork DLP
- 利用者のアクセスログの監視
- 業務用のPCのスクリーンショットや写真撮影の禁止などの意識づけ

8.12 データ漏えいの防止（イメージ図）　・・・　ツール利用事例

事例：DLP（Data Loss Prevention）

機密情報と判別したデータやファイルを不正アクセスや持ち出しから保護する。
重要データ持ち出しや書き出しなどのアクションを検知して、管理者へアラート通知を行い、被害を最小限に食い止めるセキュリティ対策ツール



8.12 データ漏えいの防止　・・・　運用対処事例

事例：人為的ミスによるデータ漏洩防止

○メール誤送信（宛先誤り、添付ファイルミス）が発生しにくいプロセスの構築
- 宛先、添付ファイルの送信前チェックの確認リストの作成＆運用
- 誤送信に気づいた時に取り消せるようメールの送信を一定時間保留や外部送信時に上長の承認が必要となるメールシステムの導入

○ノートパソコン、スマホの不要な持ち出し・持ち込みを禁止
- ノートパソコンやスマートフォンの持ち出し原則禁止や持ち出す場合の上長承認
- リモートワイプ機能の導入（遠隔操作でモバイル機器のロックや情報の消去ソリューションの導入

○個人情報を安易に放置しない、定期的な棚卸し
- 顧客ファイルなどの情報を放置しない意図しない
- 定期的に保管している情報を確認することで漏洩の発見遅れを防止

○不用意な会話からの機密情報漏洩の注意喚起
- 日常会話（エレベータや居酒屋など）の中で潜んでいる個人情報漏洩の危険性の認識など

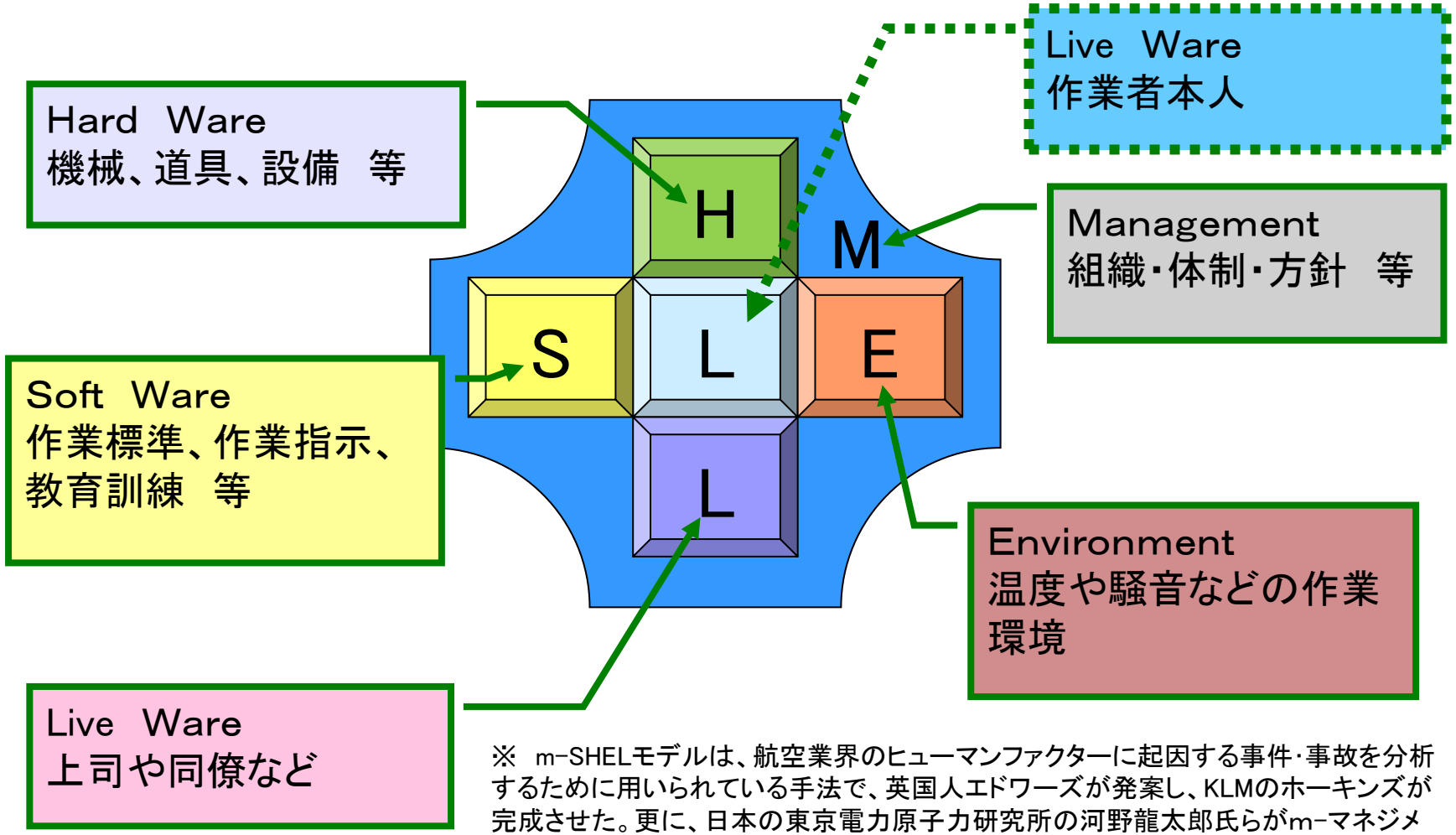
○従業員への定期的なセキュリティ教育＆意識づけ
- 定期的にデータ漏洩防止に向けたセキュリティ教育の実施

○運用対処の実施状況を自己点検する
- 定期的に上記の運用対処状況について自己点検を実施

参考資料
（2015年）

m-SHELLモデル

ヒューマンファクターの概念図

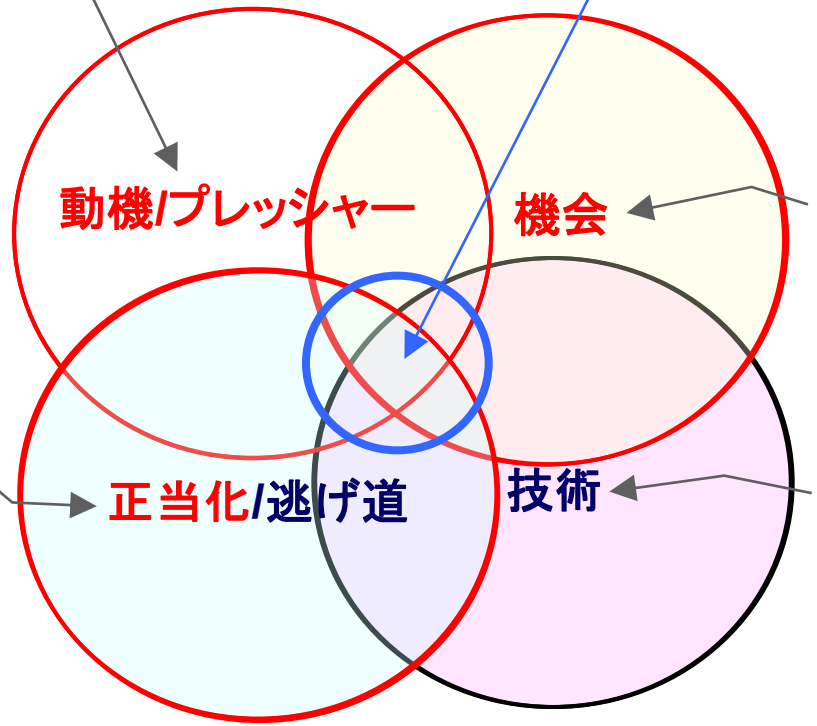


※ m-SHELモデルは、航空業界のヒューマンファクターに起因する事件・事故を分析するために用いられている手法で、英国人エドワーズが発案し、KLMのホーキンズが完成させた。更に、日本の東京電力原子力研究所の河野龍太郎氏らがm-マネジメントを追加したものである。

参考資料
（2015年）

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）

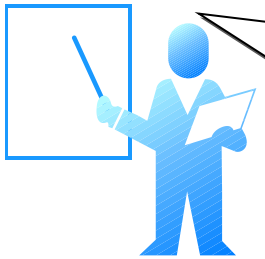


四要素が重なっている部分で問題が発生し易い。

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。

参考資料
（2015年）

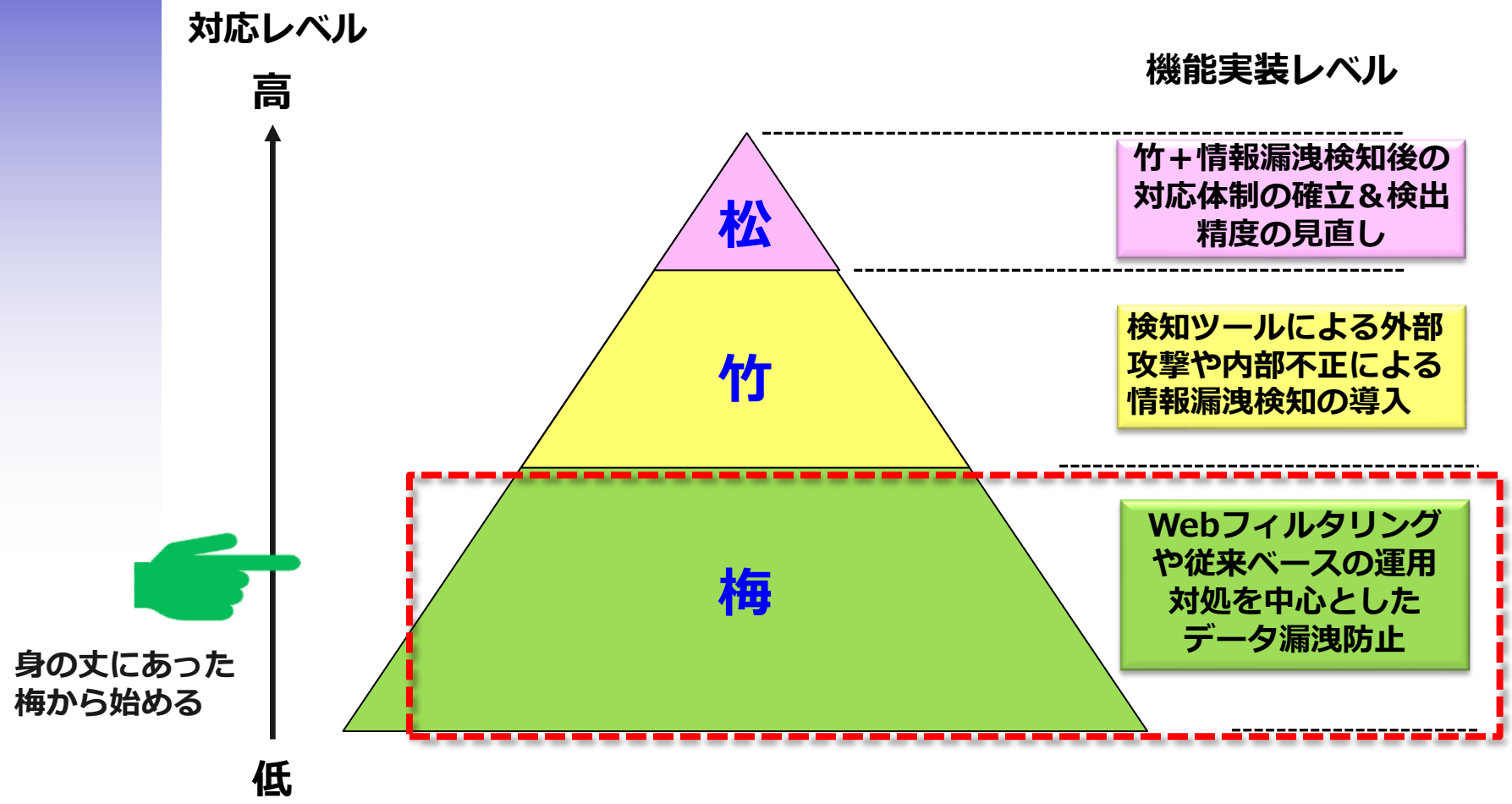
m-SHELLモデルによる分析の観点

（メール誤送信：宛先選択ミス）

Management 組織・体制・方針等	・機密情報等の取り扱いについての方針決定＆周知 ・ルール逸脱時の罰則規定の制定		
Soft Ware 作業標準、作業指示、教育訓練等	・メール送信時のチェック手続き ・管理方法（宛先の管理、新規追加の宛先管理、MLの管理方法） ・インシデント事例の共有	Live Ware 作業者本人	①本人の状態 ・体調不良による注意散漫（風邪、寝不足） ・業務繁忙時のチェック機能の弛み **※：本人の意識レベルの低下によるチェック機能の低下** **②本人の行動** **・宛先の単純選択ミス** **・宛先の手打ちによる誤設定** **・宛先の選択ミス（同姓同名）** **・all返信時の送信対象外の宛先削除漏れ** **・送信前の最終チェック漏れ（チェックの形骸化：しない、表面的、チェック内容の理解不足、勘違い等）** **※：宛先選択ミス（一次要因）とチェック機能不全（二次要因）**
Hard Ware 機械、道具、設備等	①メール誤送信防止ツールの導入 ②メール以外のツールの導入（ＳＮＳ、ファイル共有サーバ） ③メールクライアントツール（宛先選択時の関連情報の表示機能の有無）		
Environment 温度や騒音などの作業環境	・高温多湿 ・寒さ ・業務の繁忙期（時間帯、曜日変動、締め日等・・・） ・MLの宛先の維持管理状況		
Live Ware 上司や同僚等	・注意喚起 ・業務繁忙時の注意喚起の声掛け		

データ漏えいの防止の対応レベルについての考え方（案）

データ漏えいの防止の管理レベル（案）



規格要求事項から見た整理

8.23 ウェブフィルタリング

8.23 ウェブフィルタリング（要約）

概要

従業員が悪意のあるWebサイト にアクセスすることで、マルウェア感染、スパイウェアの侵入、情報及び認証情報の詐取などによる被害防止するために悪意のあるWebサイトへのアクセスをブロック（フィルタリング）する

実現したいこと

従業員が悪意のあるサイトにアクセスして、情報セキュリティ侵害を受けないようにシステム的にブロックする

具体的な対応内容や補足事項など

・社内OAシステムを担当する情シスにてプロキシ等で機械的にアクセス不能にするなどシステム的に制限を実施する

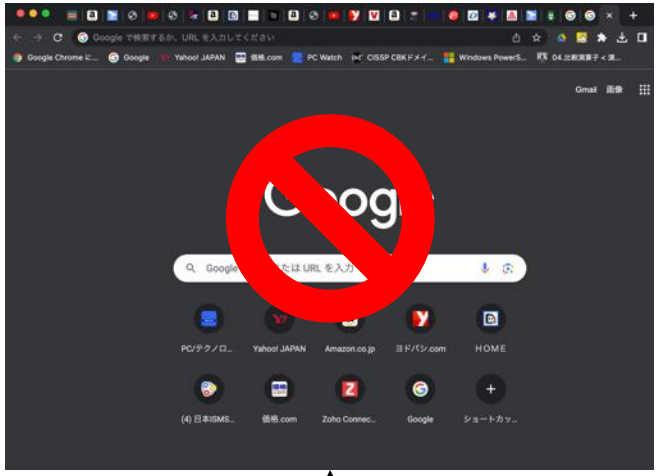
・セキュア Web ゲートウェイ（SWG）などを利用してWeb経由の攻撃を防御する

＜Webフィルタリングの例示＞
下記のようなフィルタリング方式があり、長短があるので組織の状況に応じて選択

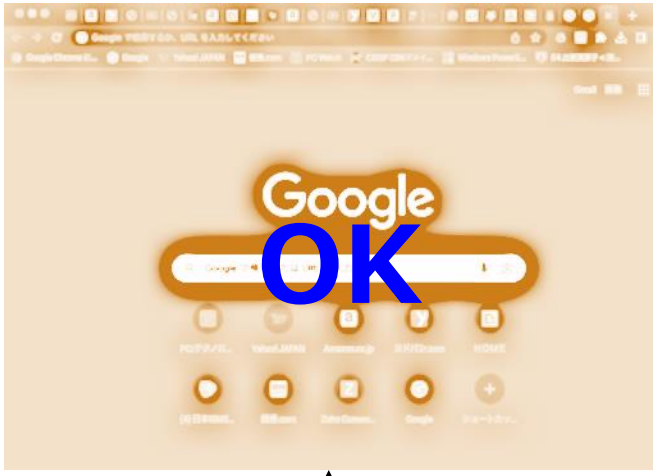
・許可リスト式
・拒否リスト式
・レイティング式
・カテゴリフィルタリング式
など

8.23 ウェブフィルタリング（イメージ図）

悪性サイトやアクセス禁止サイト



アクセス許可サイト



Webフィルタリング

事例：　閲覧限定方式の概要とメリット／デメリット

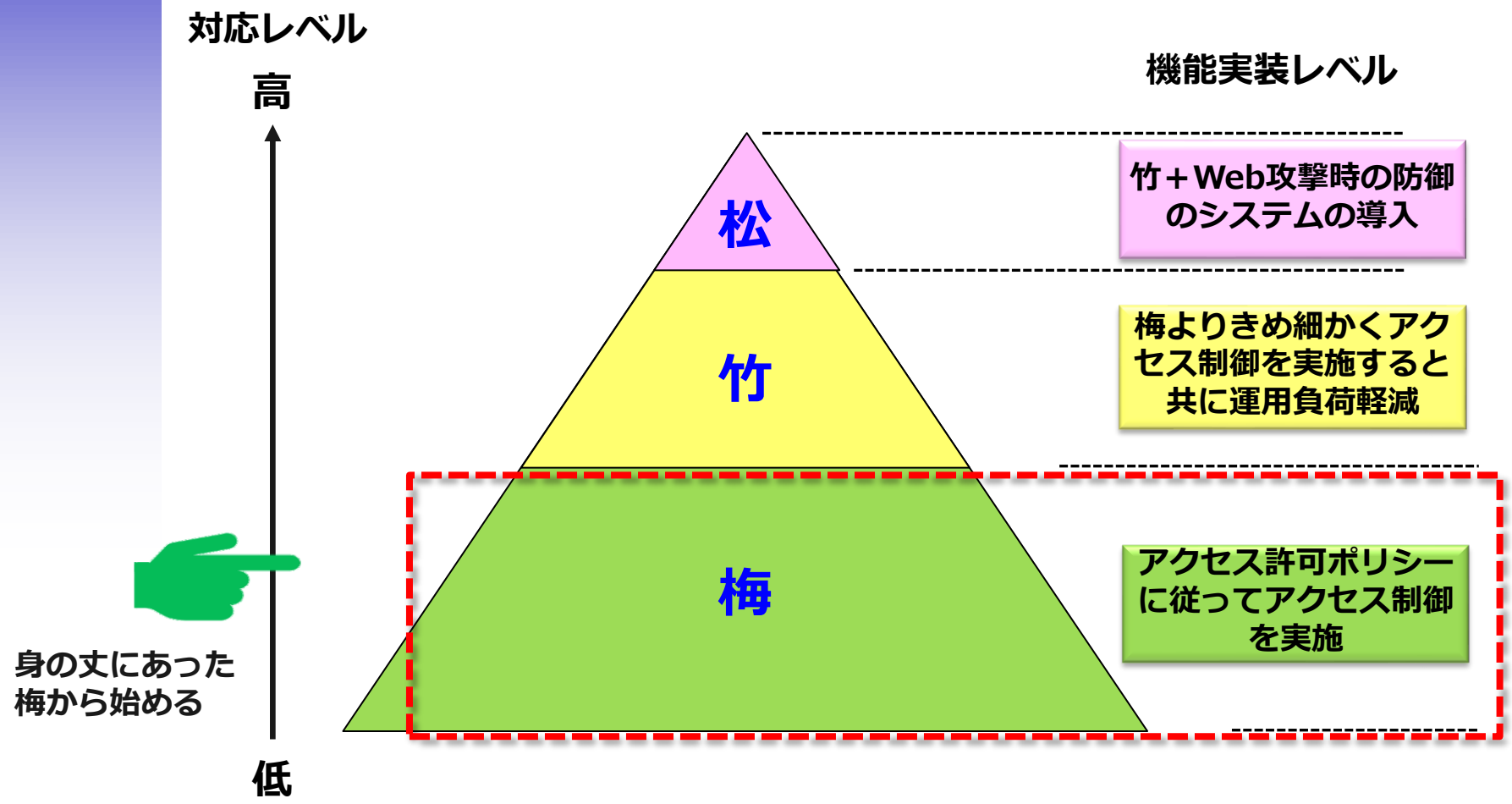
方式	概要	メリット	デメリット
許可リスト式	アクセスを許可するリストを作成して、該当しないURLへのアクセスをすべて遮断	未知の有害サイトも確実に遮断できる	有益なサイトの情報まで遮断するため様々な情報収集が必要な業務との相性は悪い
拒否リスト式	有害なサイトのリストを作成して、該当するURLへのアクセスを遮断する	許可リスト式より自由度が高い	有害サイトの情報の登録・更新に手間が掛かる
レイティング式	URLフィルタリングのリストに保存された各サイトの格付け結果をもとに自社の基準に合わないサイトを排除する	第三者機関が作成した格付け結果に基づくため、効果的なフィルタリングが可能	新しいサイトの情報の格付けが反映されるまでに時間を要するため遮断できない可能性がある
カテゴリフィルタリング式	Webサイトを特定のカテゴリに分類して閲覧拒否設定したカテゴリを遮断する（情報漏洩防止のためにSNSや掲示板のアクセスを禁止するなど）	拒否リスト式に似ているが、カテゴリのデータベースを提供するセキュリティベンダの情報を利用することで効率的に有害サイトブロックできる	

ウェブフィルタリングのソリューション事例

RBI（Remote Browser Isolation）	**ウェブ分離**とも呼ばれ、**すべての閲覧行為をクラウドベースのリモートコンテナでホストし実行**することで、ユーザーのデバイスをインターネット閲覧行為から分離するセキュリティ対策 **インターネット閲覧をサンドボックス化**することで感染したウェブサイトのコードに起因する次のようなあらゆる種類の脅威から、データ、デバイス、ネットワークを保護 •ウェブ経由でのマルウェアとランサムウェア •ゼロデイ攻撃 •プラグインなどブラウザの脆弱性 •感染したファイルのダウンロード •フィッシングメールに含まれる悪質なウェブリンクなど
SWG（セキュアWeb ゲートウイ）	**URLフィルタやアプリケーションフィルタ、アンチウイルス、サンドボックスなどの機能をクラウド型で提供するサービス**のこと アクセス先のURLやIPアドレスからその安全性を評価し、安全でないと評価された場合にはアクセスを遮断

ウェブフィルタリングの対応レベルについての考え方（案）

ウェブフィルタリングの管理レベル（案）



規格要求事項から見た整理

8.28 セキュリティに配慮したコーディング

8.28 セキュリティに配慮したコーディング（要約）

概要

ソフトウェア開発においてリスク源となるぜい弱性を減少させるために予めソフトウェアの開発時に適用するセキュリティに配慮したコーディングのための原則を確立し適用を行う

実現したいこと

セキュリティに配慮したコーディングのルールを制定＆周知徹底することでリスク源となる脆弱性を減らす

具体的な対応内容や補足事項など

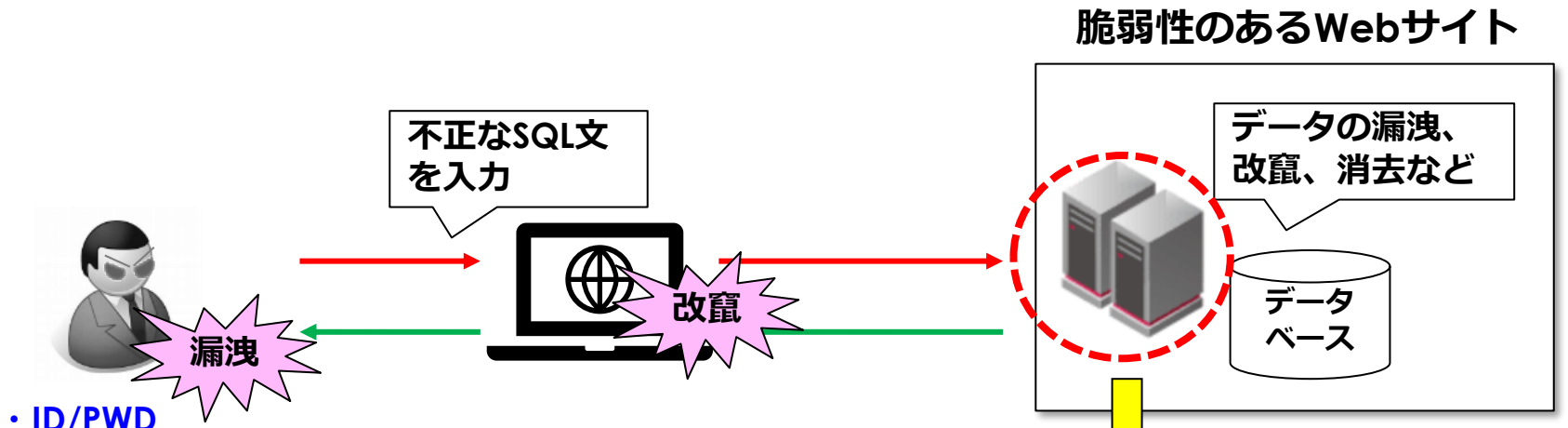
- 組織全体としてのセキュリティに配慮したソフトウェア開発の共通ルールとして整備する
- 開発のプロジェクトマネージャが社内＆委託先に適用するルールとして活用する（コーディング時やレビュー時）
- オープンソースも対象とする

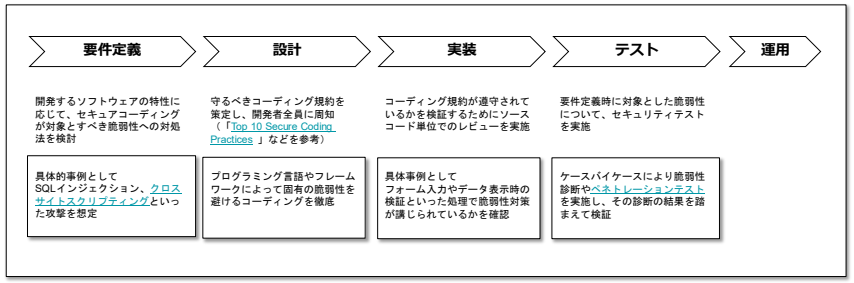
＜考慮事項の例示＞

- 設計＆開発段階でのセキュリティを意識した設計や機能の盛り込み
- セキュアな基準を盛り込んだ開発標準の策定
- SQLインジェクションやクロスサイトスクリプティングなどの脆弱性をなくすコーディング

8.28 セキュリティに配慮したコーディング（イメージ図）

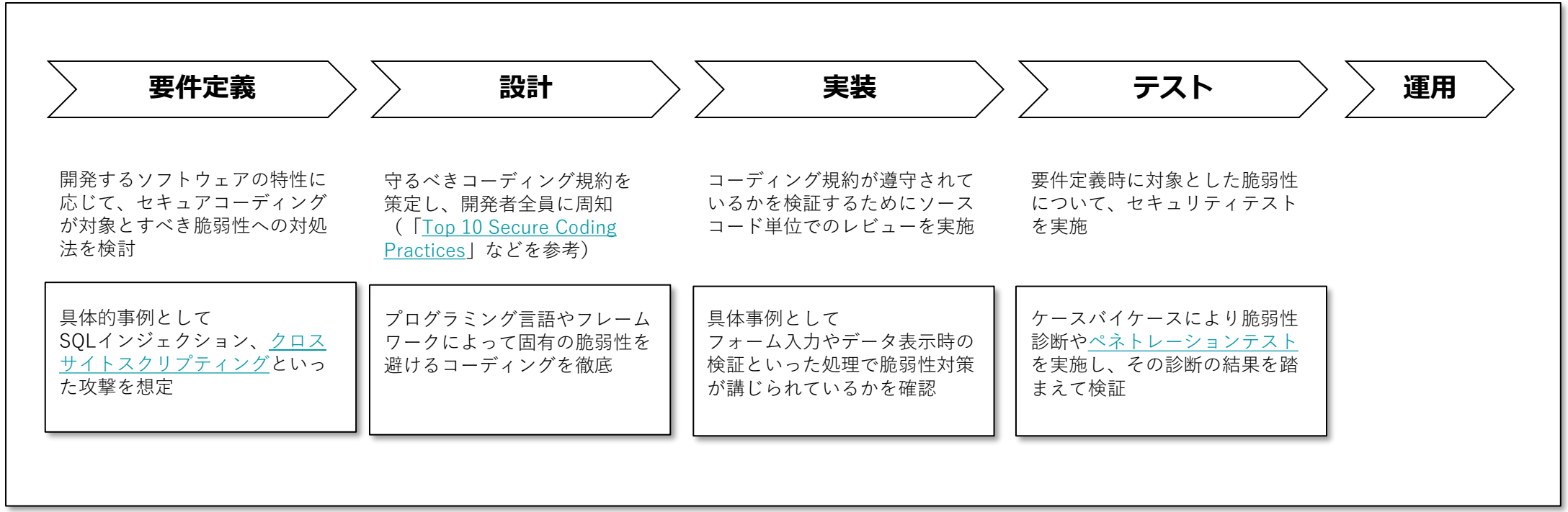
事例：セキュアなコーディングが出来ていない場合に発生するリスク（ SQLインジェクション）





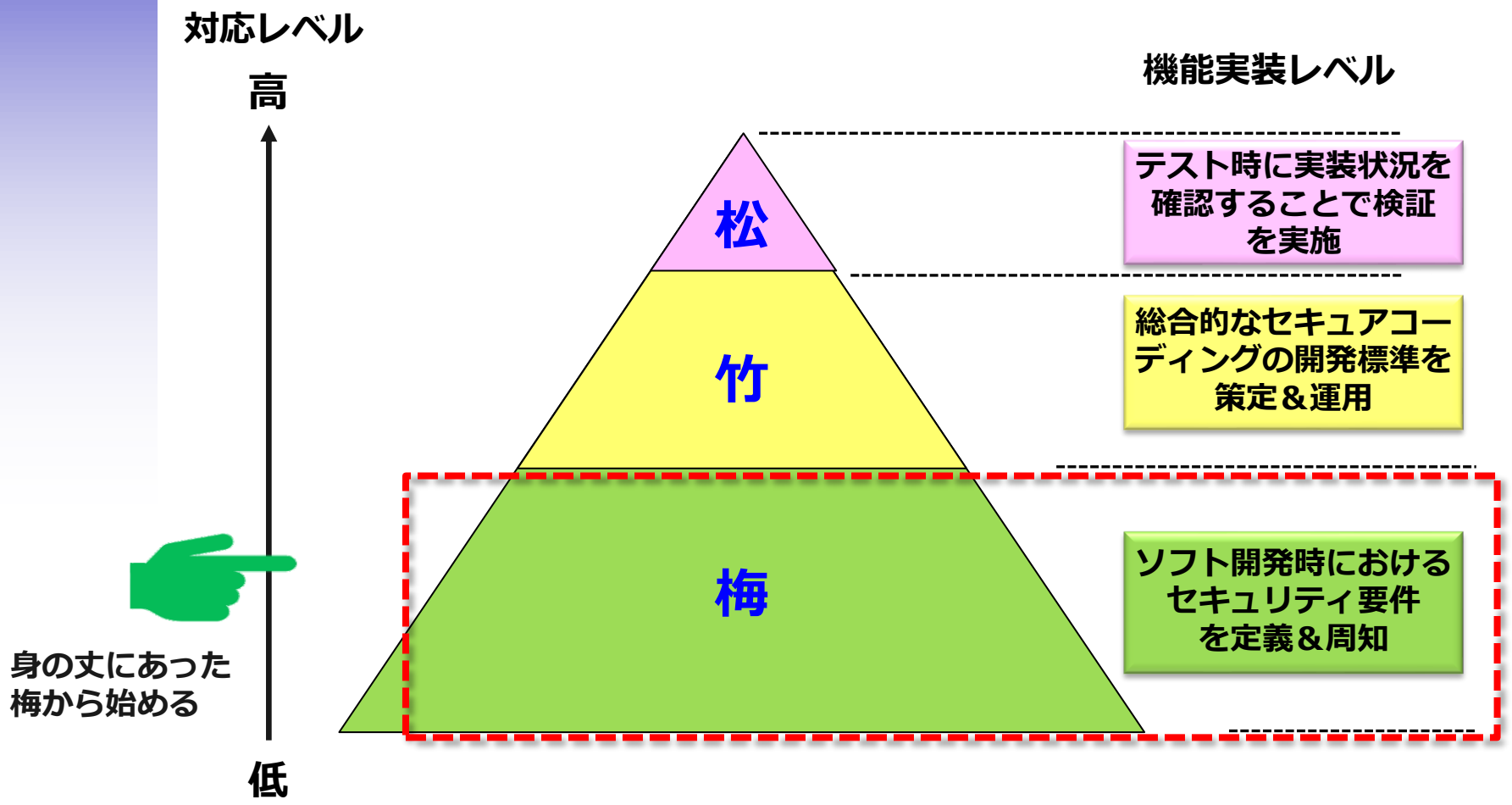
8.28 セキュリティに配慮したコーディング

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



セキュリティに配慮したコーディングの対応レベルについての考え方（案）

セキュリティに配慮したコーディングの管理レベル（案）



セキュアコーディングの対応事例

Webサービスからの情報漏洩対策として下記の対応を考慮する必要がある
（IPA：安全なウェブサイトの作り方）

1） SQL インジェクション
2） OS コマンド・インジェクション
3） パス名パラメータの未チェック／ディレクトリ・トラバーサル
4） セッション管理の不備
5） クロスサイト・スクリプティング
6） CSRF（クロスサイト・リクエスト・フォージェリ）
7） HTTP ヘッダ・インジェクション
8） メールヘッダ・インジェクション
9） クリックジャッキング
10） バッファオーバーフロー
11） アクセス制御や認可制御の欠落

https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000017316.pdf

まとめ

＜移行審査対応について＞

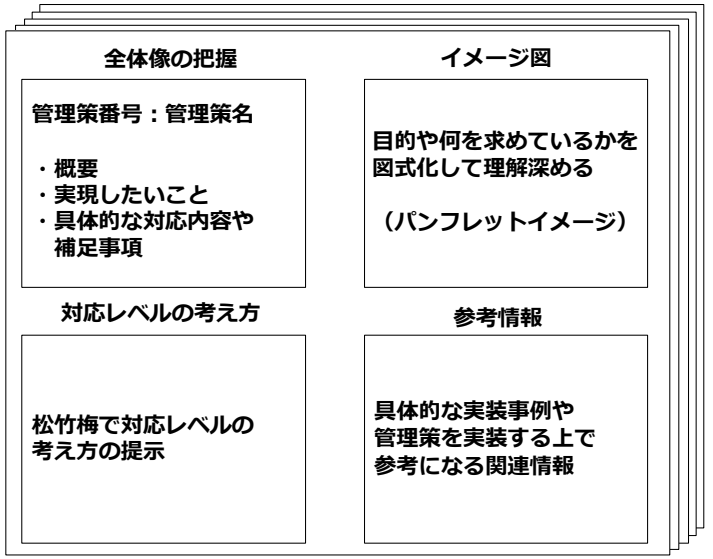
今回は管理策の改正が中心（本文は「箇条6.3 変更の計画」の新設）なので、実施すべきは、**「箇条6.1.3 c)の「6.1.3 b)で決定した管理策を附属書Aと比較し、必要な管理策が見落とされていないことを検証する」**ということになります。

本テーマで説明した新設の11の管理策ですが、ギャップ分析によってすでに実施済みのものと未実施のものに大別されます。

未実施のものは「箇条6.1.2　情報セキュリティリスクアセスメント」によって組織としての対応策を決定することになります。

具体的には、6.1.2で新規の管理策に関連する脅威とリスク源を洗い出し、6.1.3でリスク対応を決めるというプロセスを実施することとなりますので、インプリメンテーション研究会の成果が皆さまの移行検討に役立てば幸いです。

本テーマで実施した新規管理策についての考察



参考情報：JNSAメールマガジン　第273号【連載リレーコラム】　ISO／IEC27001：2022の移行対応について

https://www.jnsa.org/aboutus/jnsaml/ml_bk273.html

■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：　JISQ27001:2023の新規管理策の実装方法についての考察

テーマ2：　「ISMS内部監査」どうやってますか?

＋

現在、ハイブリッド（リアル会場＋Web会議）で討議しています！

毎月最終木曜日18:00～21:00開催