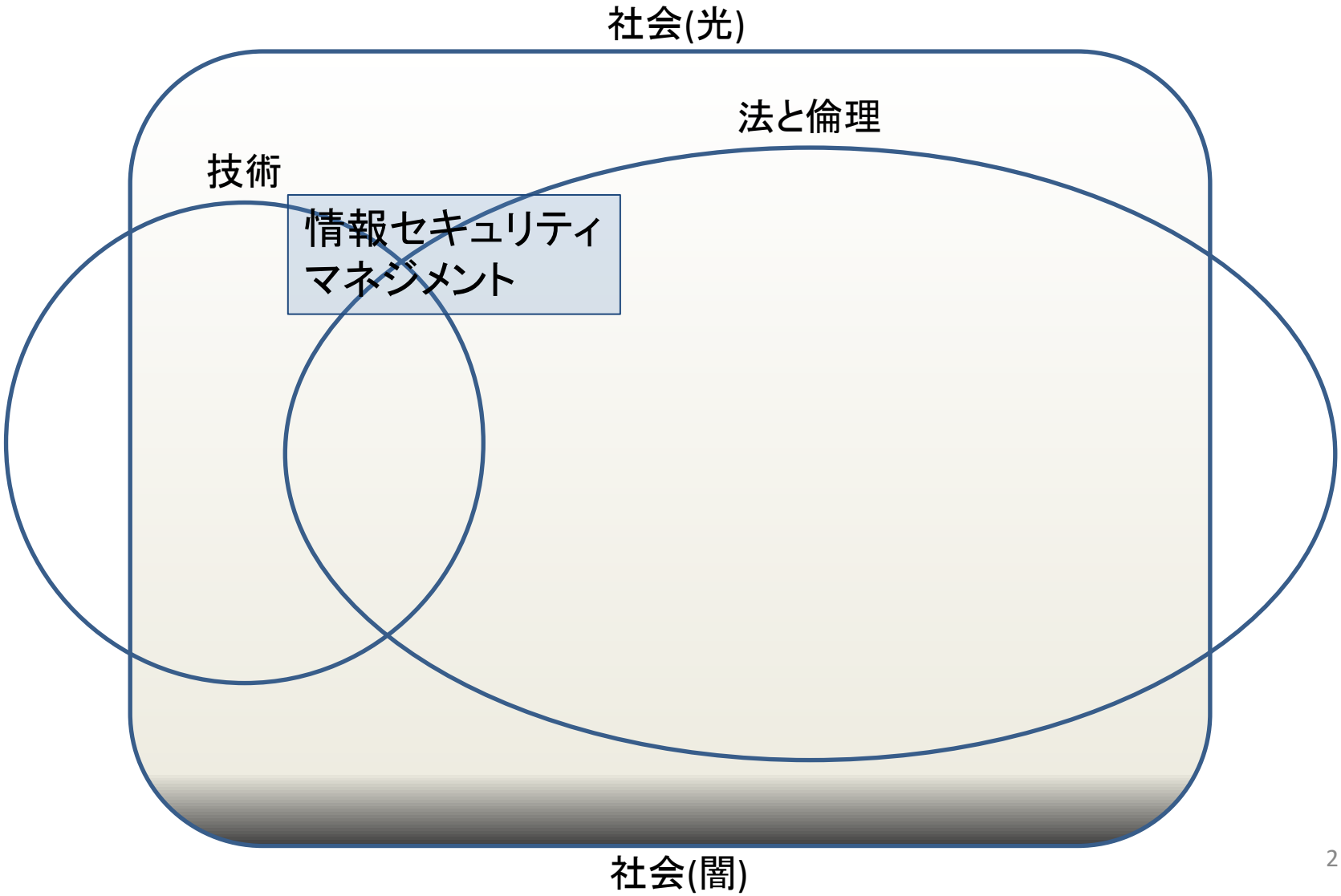
情報セキュリティと情報倫理

第12回　情報セキュリティマネジメント

2022/12/23

今日の内容



忘れないうちに

- 今回のミニレポート課題
  - 2023/1/06　16:10〆切
- 課題1
  - 2023/1/27　16:10〆切

セキュリティ上の脅威と向き合う仕組み

- 想定される脅威への対策を策定・実施・改善
  - リスクマネジメントの枠組みを利用
    - どこまでコストをかけてやるかは経営判断
    - 状況の変化に合わせて常に改善
- 情報セキュリティマネジメントシステム
  - ISMS(Information Security Management System)の略
  - PDCAサイクルによる組織的な体制を構築
    - cf. 環境マネジメントシステム(EMS)
    - JIS規格,ISO規格,政府統一基準などで標準化

一体何を守るのか？

- 守りたいのは「情報資産」
  - PCやハードウェア自体を守りたいのではない
  - 情報資産は電子データとは限らない
    - 紙の書類
    - メモ用紙
    - 記憶(操作手順、パスワード等)

どこまで守るのか？

- 電子文書だけ？
- PCごと盗まれたらどうする？
- 脅迫されたらどうする？
- 自社(自組織)の所有物だけ？
- 自社(自組織)の構成員だけ？

どのくらい守るのか？

- 高価なものだけ守れば良い？
- 常に誰かが見張っていないといけない？
- 書類は一切持持ち出し禁止？
- 全ての端末に指紋認証を義務づける？
- 全ての部屋をICカードで入退室管理？
- 電子メールを全て検閲？
- USBポートを全て封印？

トピック

- リスクマネジメント
  - リスクへの対処法
- リスク対応とモラル
- 情報セキュリティマネジメントシステム
  - 全体像
  - 情報セキュリティポリシー導入の流れ
  - 情報資産の格付け

想定される脅威の例

- 職場のデータをUSBで持ち帰り、自宅のPCで作業している間にファイル交換ソフトで流出
- 出張先から帰る途中、電車で寝ている間に鞄ごとノートPCを盗まれる
- 上のフロアで火事があり、消火作業のあおりで端末・サーバが浸水

情報資産

- 脅威から守る対象となる情報に加え
  - 情報の保持・利用に関わるあらゆる資産も含む

JIS Q 27002:2006「7.1.1 資産目録」より

情報資産	具体例
情報	データベース,ファイル,契約書,マニュアル,etc
ソフトウェア資産	業務用ソフトウェア,システムソフトウェア,ツール,etc
物理的資産	コンピュータ,ネットワーク機器,記録媒体,etc
サービス	計算処理,通信サービス,照明,電源,空調,etc
人,資格など	人,資格,技能,経験
無形資産	評判,イメージ

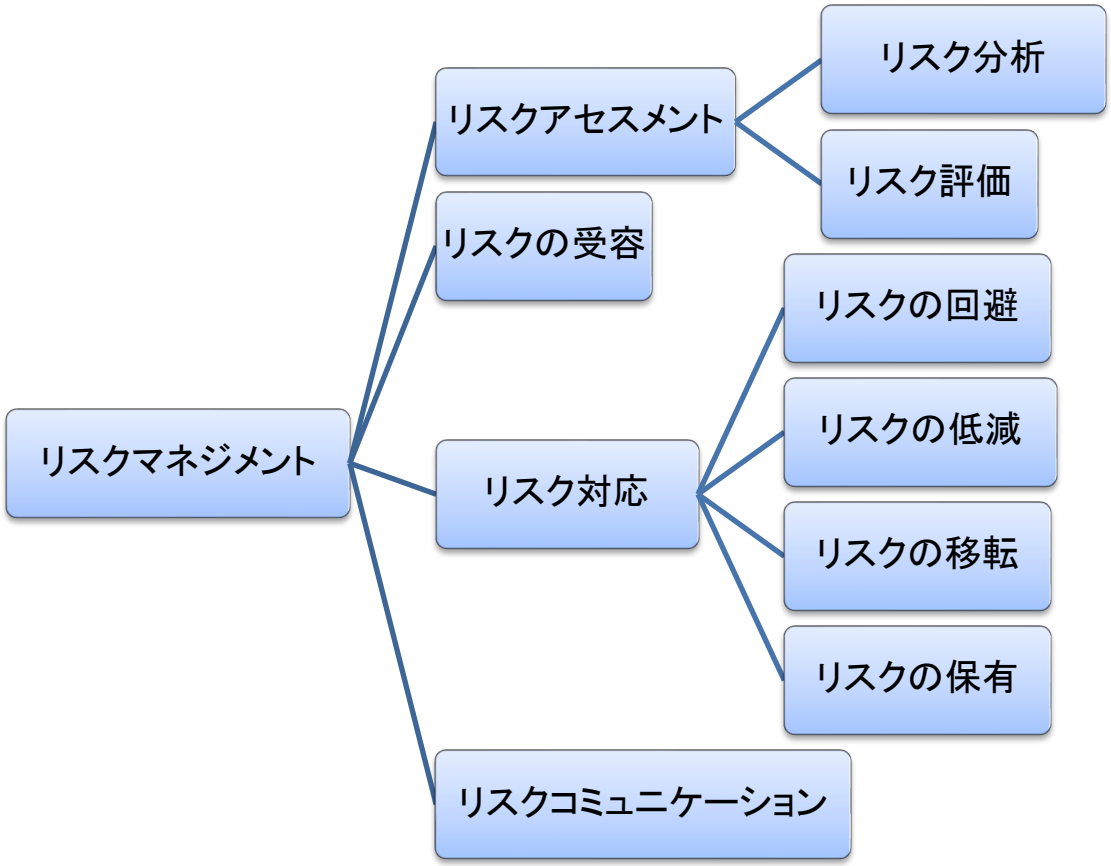
出典 http://www.irasutoya.com/2014/02/blog-post_4239.html

コラム

- 日常業務にみる情報セキュリティ事故の実態
  - 携帯紛失、電子メール誤送信編「撲滅不可能？！ケータイの紛失、電子メール／FAXの誤送信」

情報セキュリティマネジメント

- 情報資産に関するリスクマネジメント



リスクアセスメント

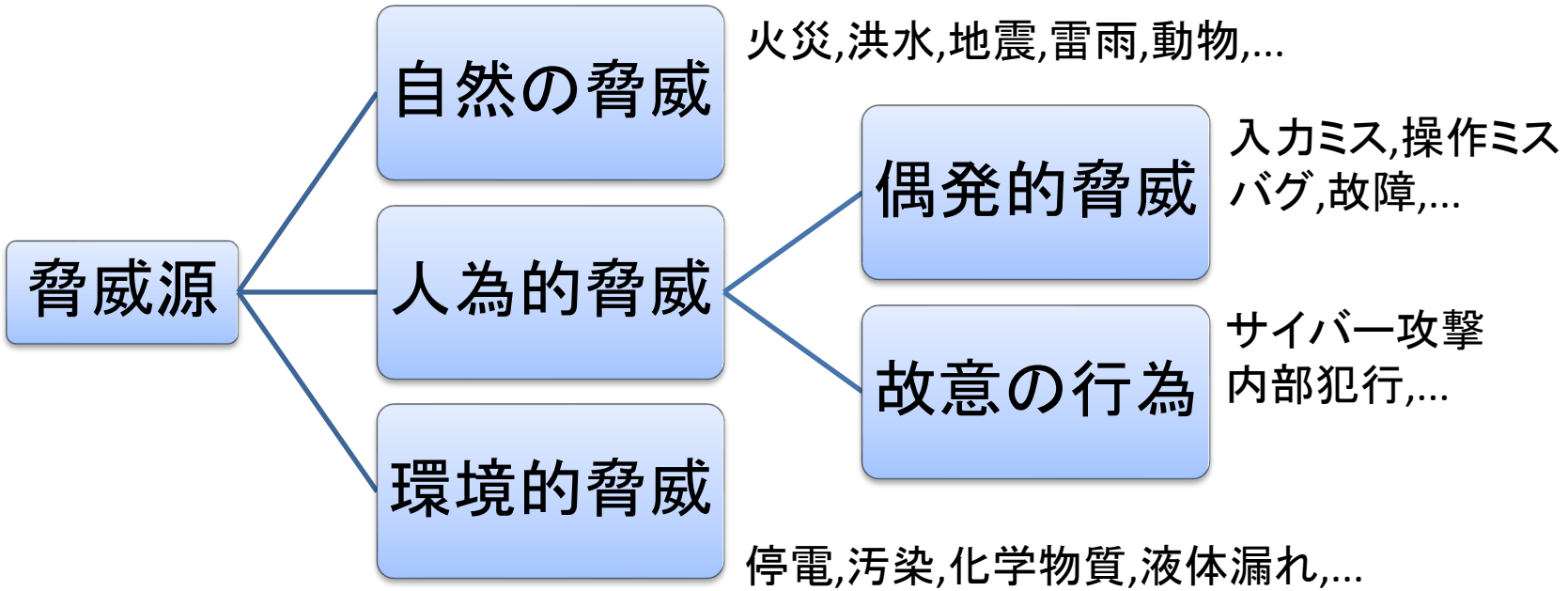
- 全てのリスクを同列に扱うのは非現実的
- 以下の3要素の組合わせでリスクを評価

脅威 x 脆弱性 x 影響度

発生可能性

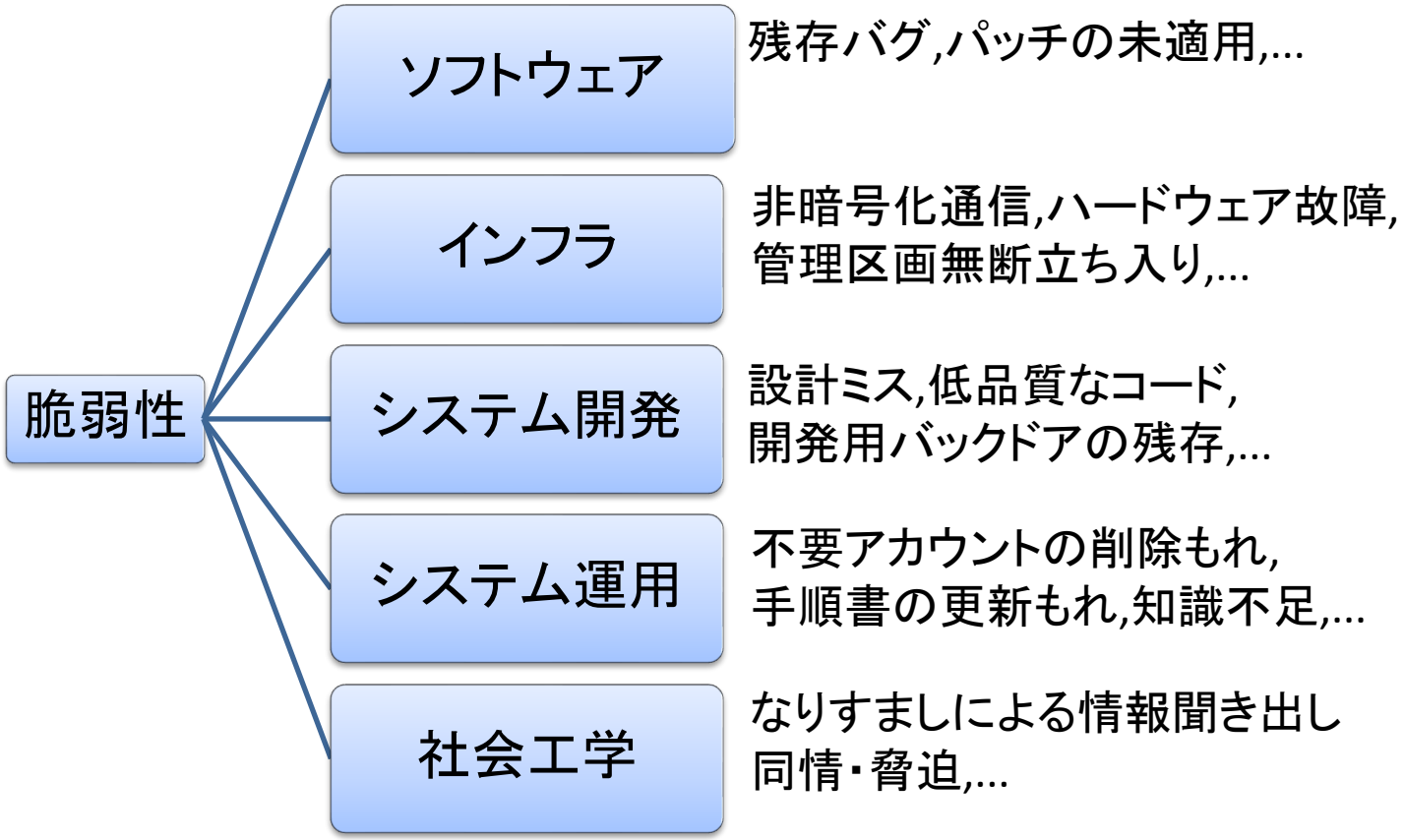
リスク分析:脅威

- 情報資産に好ましくない影響を及ぼす事象



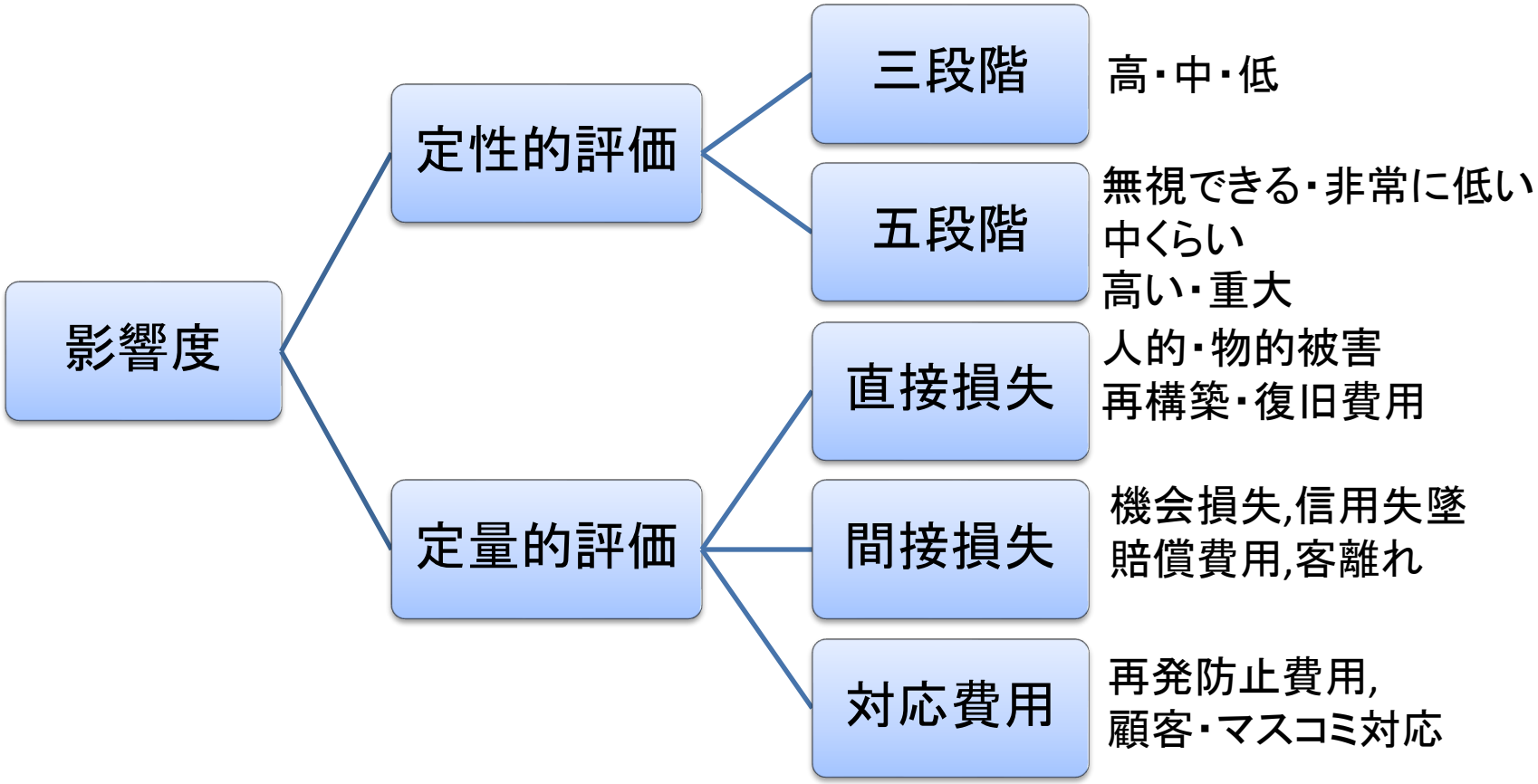
リスク分析:脆弱性

- 情報資産が持つ弱点.脅威によって顕在化



リスク分析:影響度

- 情報資産の価値(想定される損害)で評価



影響度の定量的評価

- 直接費用
  - まだ算出しやすい
- 間接費用
  - 確立された計算モデルはない
  - 損害賠償は過去の裁判事例が参考になる
- 対応費用
  - 確立された計算モデルはない

個人情報漏洩時の損害賠償額

- 1件あたりの賠償額試算式(JNSAによる)

  賠償額 = 漏洩個人情報の価値x社会的責任度x事後対応評価

項目	値
漏洩個人情報の価値	基礎情報価値x機微情報度x本人特定容易度
基礎情報価値	500(固定)
機微情報度	精神的苦痛と経済的損失より算出(後述)
本人特定容易度	特定困難=1,コストをかければ可能=3,容易=6

項目	値
社会的責任度	一般:1.0, 一般より高い: 2.0
事後対応評価	適切:1.0, 不適切:2.0

機微情報度の算出

- 機微情報度= $\max(10^{x-1}+5^{y-1})$
  - x:精神的苦痛レベル, y:経済的損失レベル

経済的損失レベルy				
3	口座番号&暗証番号,クレジットカード番号&有効期限,銀行のアカウント&パスワード,…	遺言書	前科前歴,犯罪歴,与信ブラックリスト
2	パスポート情報,口座番号・カード番号のみ,…	年収,資産,建物,年,所得,…	
1	氏名,住所,生年月日,性別,メールアドレス,会員番号,身長,体重,血液型,写真,…	健康診断,心理テスト,手術歴,看護記録,DNA,病歴,指紋,スリーサイズ,日記,職歴,学歴,成績,…	加盟政党,信条,思想,宗教,信仰,病状,…
	1	2	3

精神的苦痛レベル x

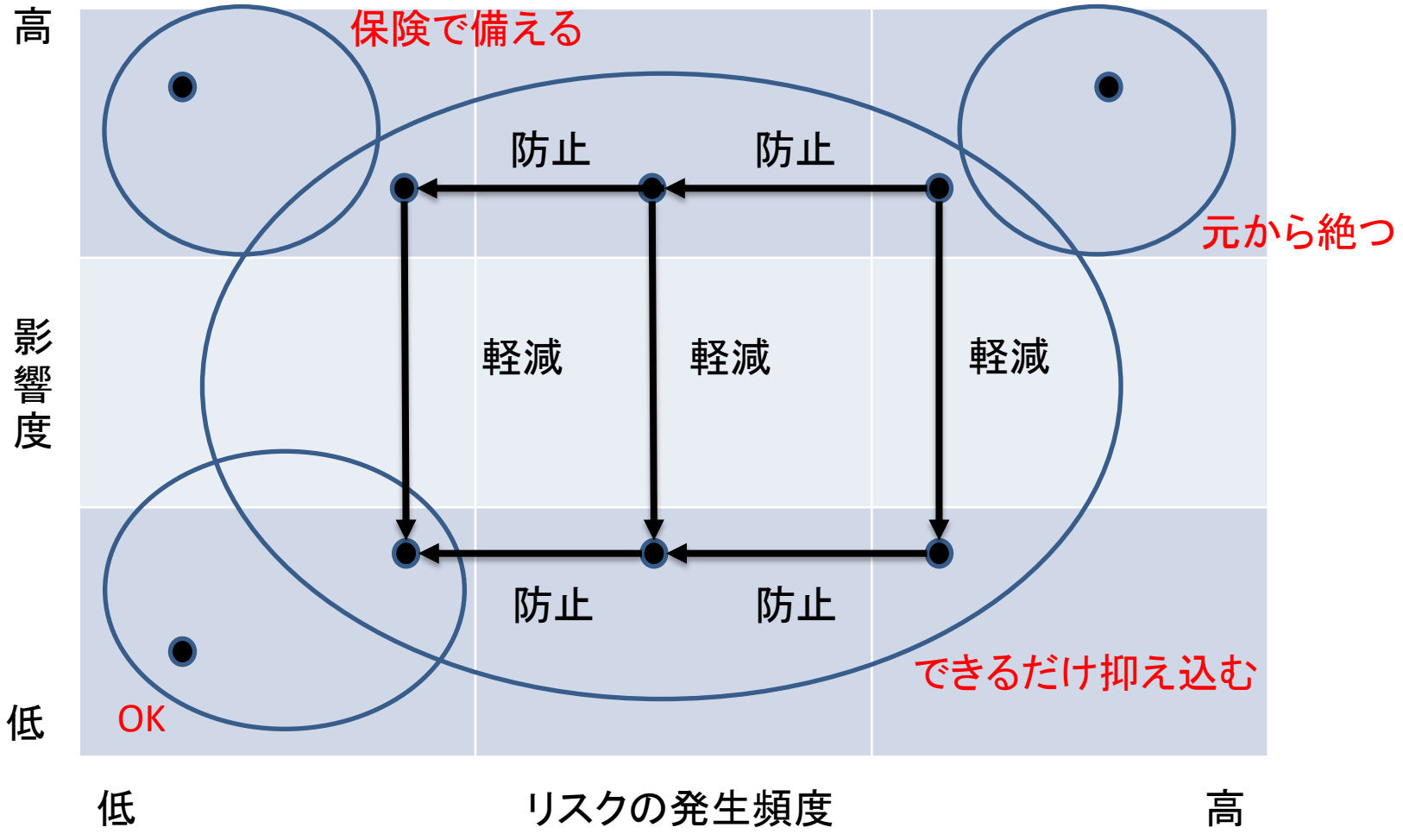
個人情報漏洩賠償額の算出例

- 例：会計事務所にて10000人の顧客情報が流出
  - 内容は住所・氏名・生年月日・年収
  - 当初、漏洩はないと報告し、後に大炎上

項目	値
漏洩個人情報の価値	基礎情報価値x機微情報度x本人特定容易度
基礎情報価値	500(固定)
機微情報度	このケースは(10+5) = 15
本人特定容易度	容易=6
社会的責任度	一般より高い: 2.0
事後対応評価	不適切:2.0

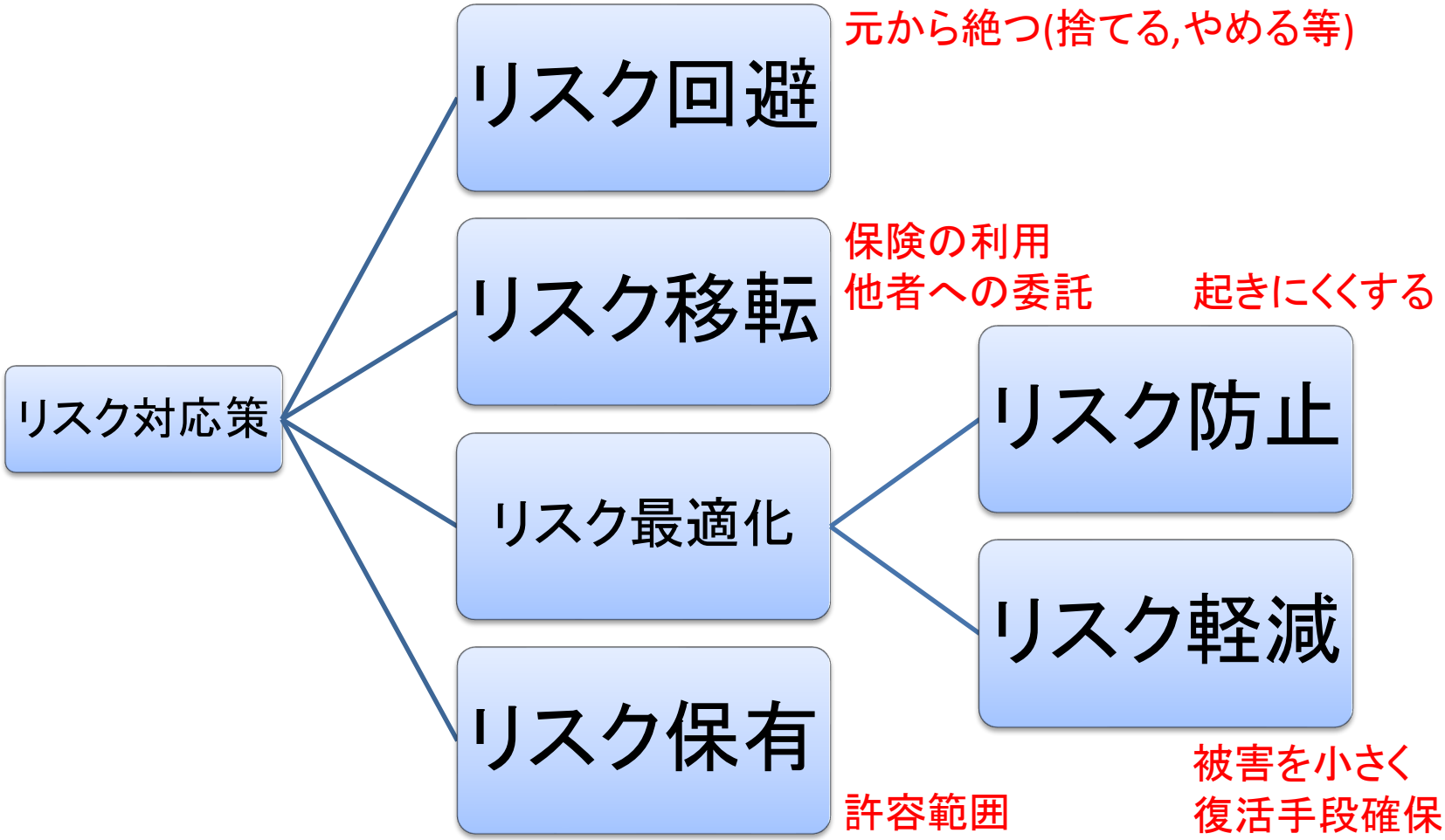
賠償額　= 500 x 15 X 6 x 2 x 2 x 10000 = 180,000 x 10000 = 18億円

リスク対応

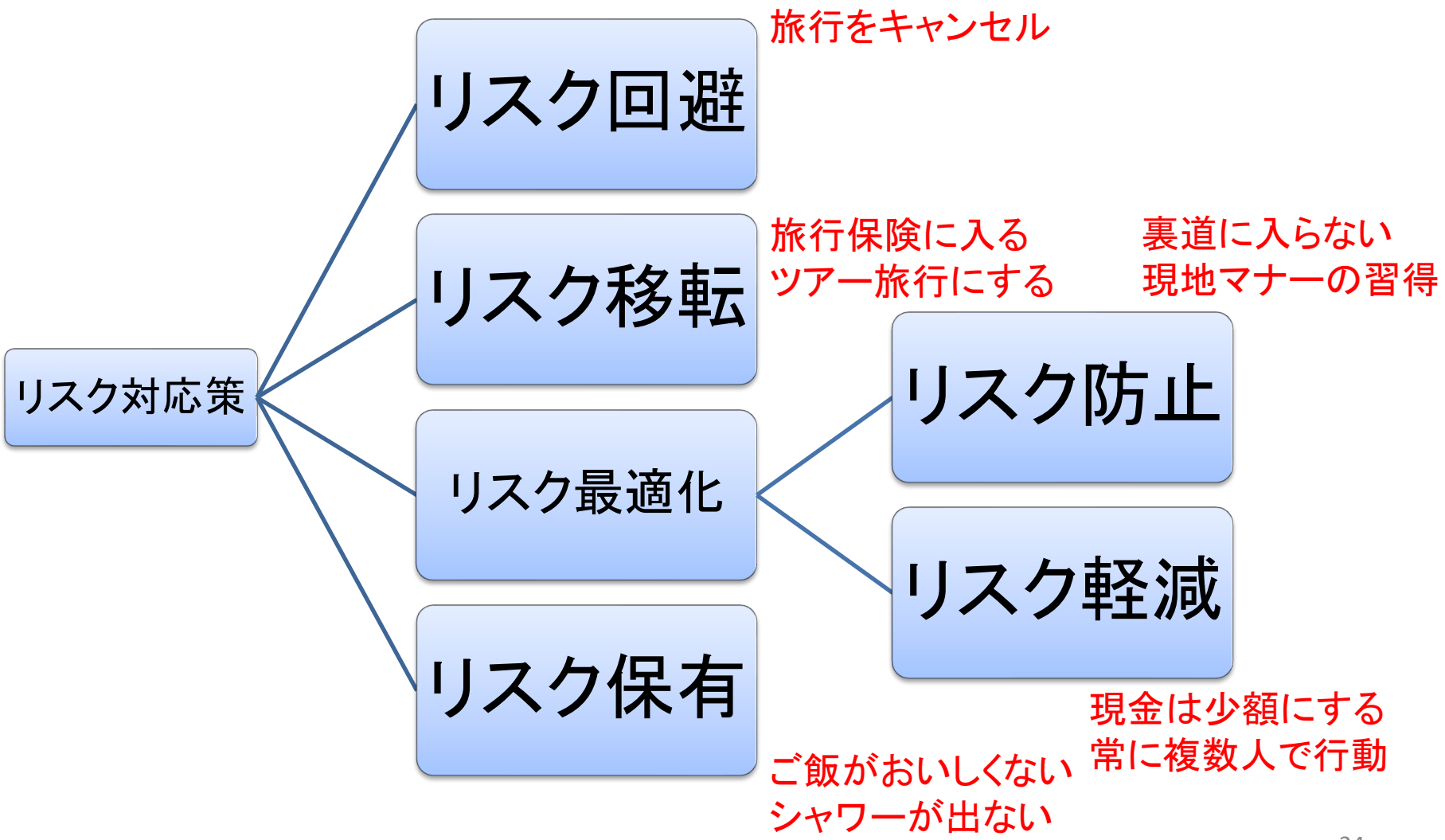


(発生可能性 = 脅威 x 脆弱性)

リスクへの対応策


リスク対応策
リスク回避
元から絶つ(捨てる,やめる等)
リスク移転
保険の利用
他者への委託
リスク最適化
起きにくくする
リスク防止
リスク軽減
被害を小さく
復活手段確保
リスク保有
許容範囲

例：外国旅行のリスクと対策



リスクコミュニケーション

- リスク管理方法についての合意形成活動

平常時

- 関係者との意見交換・情報共有
  - リスクの発見と特定
  - コミュニケーション手順の確立
- 緊急時活動計画の作成と訓練

緊急時

- 活動計画に基づいた連絡・発表
  - 利害関係者への情報提供
  - 国、地方自治体、関係機関への報告

リスク対応とモラル

- 「対策コスト >損害額」ならあえてリスク受容？
  - 合理的ではあるが、本当にそれでよいか
  - フォード社ピント事件
    - 燃料タンクの改善に必要なコスト > (社会的)損害額
    - タンクの改善費用は1台あたり11ドル
- 公衆優先原則
  - 公衆の安全、健康、および福利を最優先する
    - 「悪いことはするな」
  - 例 : Don’t be evil (Googleの社是)

技術者の責務

- 公益を最優先すること
- 正直であること、誠実であること
  - 「自分の領域について技術的判断」を行うこと
  - 経営的判断を行ってはならない
    - ex.設計不良だけど、これ売ったら儲かるし
- 業務遂行とのジレンマ
  - そうはいってもサラリーマンだと・・・
  - モラルとのせめぎ合い

内部告発

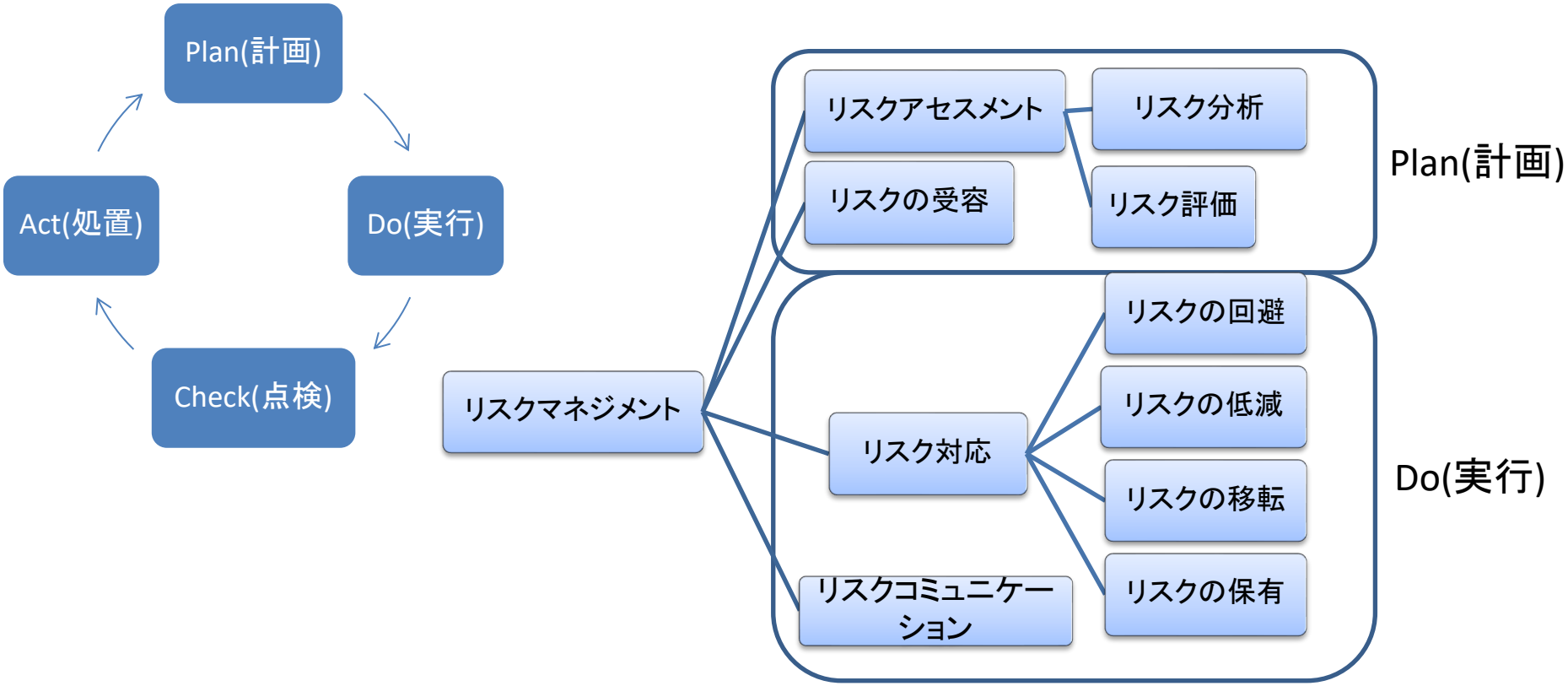
- はやまるな。本当に最後の手段
  - 前提条件が揃わないと法的正当性がない
  - 訴えが正当でも、倒産・失業など暗い結末も

本日のミニレポート

- 課題：自宅の情報資産を3つ挙げ，情報セキュリティの観点から情報資産管理台帳の各項目欄を埋めよ.
  - 情報資産の例
    - 住所録,郵便物,写真データ,録画ビデオ,音楽データ,成績簿（通信簿）,プライバシー関連(答案用紙,日記,etc)
  - 提出先：Moodle
    - https://moodle.cis.kit.ac.jp/mod/data/view.php?id=121521
      - 「エントリを追加する」をクリックして回答を登録

リスクマネジメントとISMS

- 情報資産に関するリスクマネジメント継続体制



セキュリティの原則

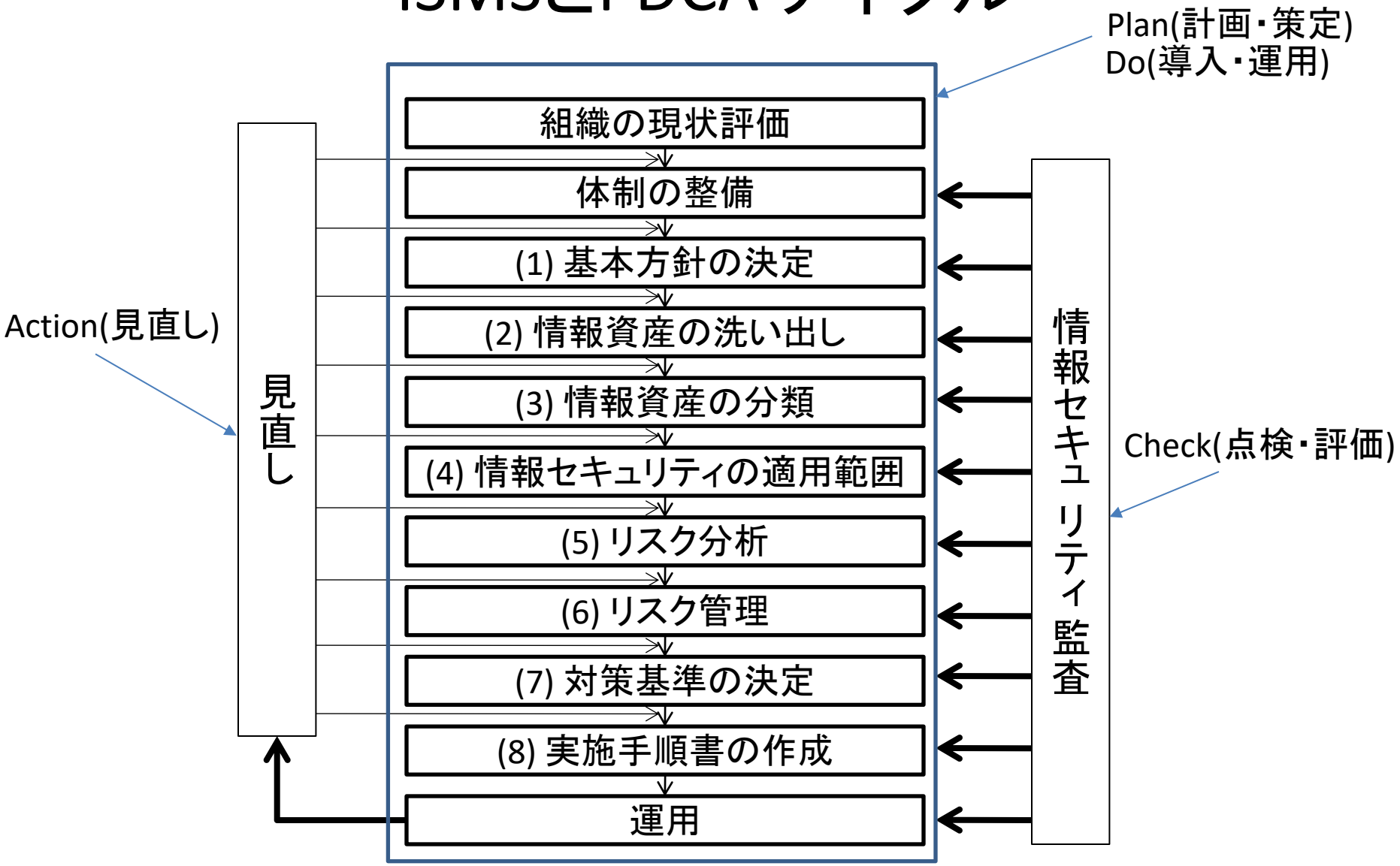
- 桶の理論
  - 最も弱い部分がセキュリティ水準を決める

出典 http://www.irasutoya.com/2014/02/blog-post_4239.html

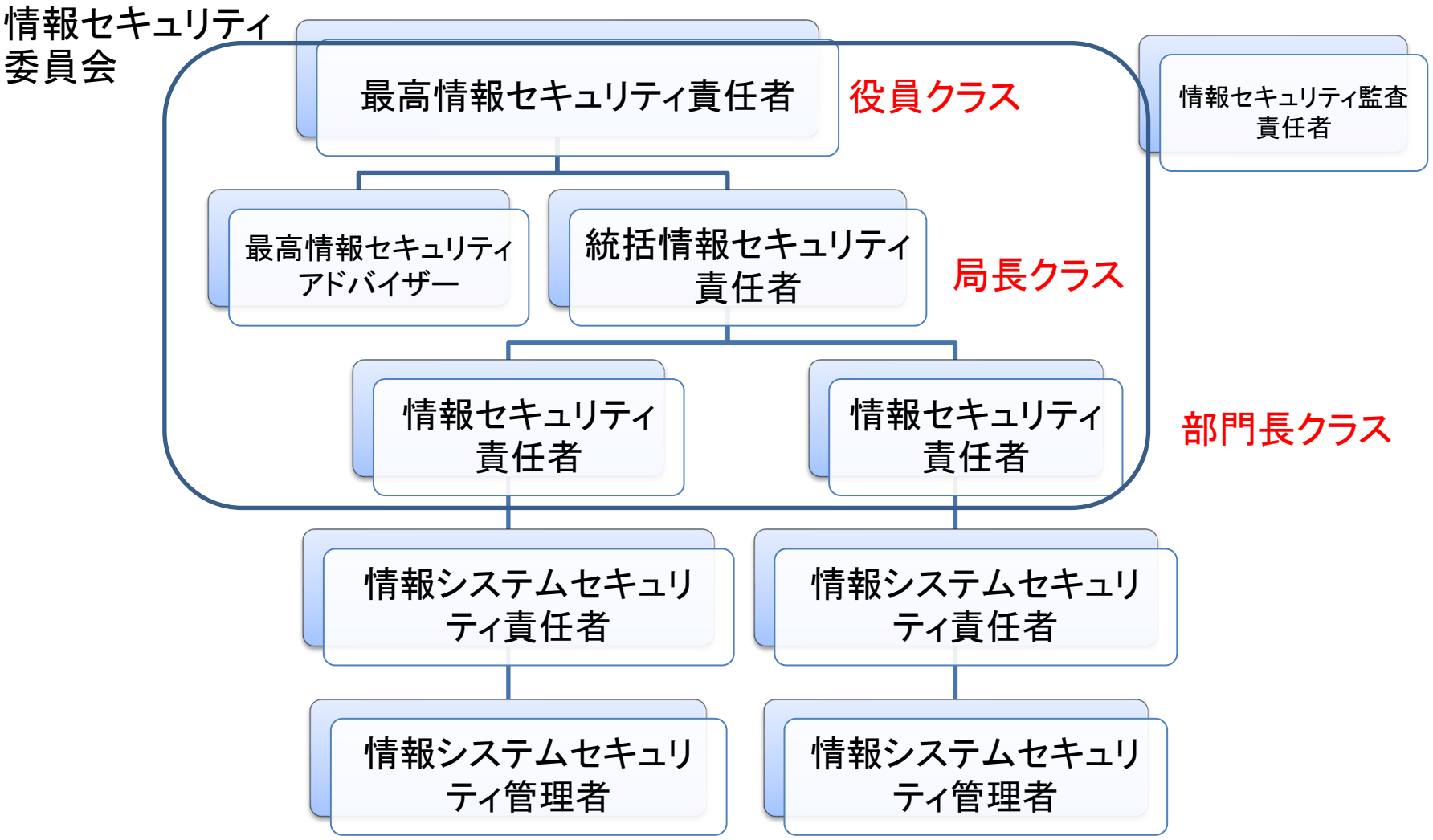
情報セキュリティの確保

- 組織全体の協力が必要
  - 組織のセキュリティレベルは最も脆弱な部分で決定
  - 1箇所でも脆弱性が存在すれば，そこを踏み台として組織全体が被害を受ける
- 各自の率先した情報セキュリティ活動は期待できない
  - 生産・販売活動に直結しないから
- 何らかの基準を参照しながら自組織の実態に照らして意思決定するというプロセスが必要

ISMSとPDCAサイクル

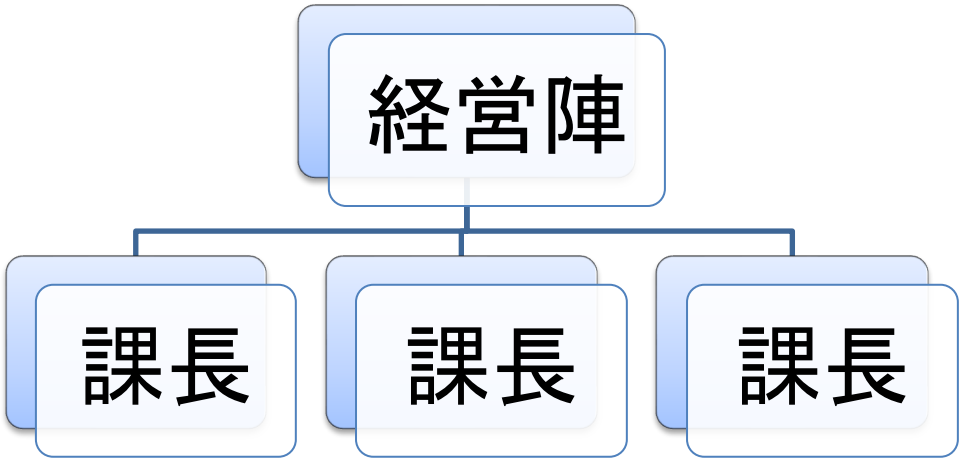


組織体制

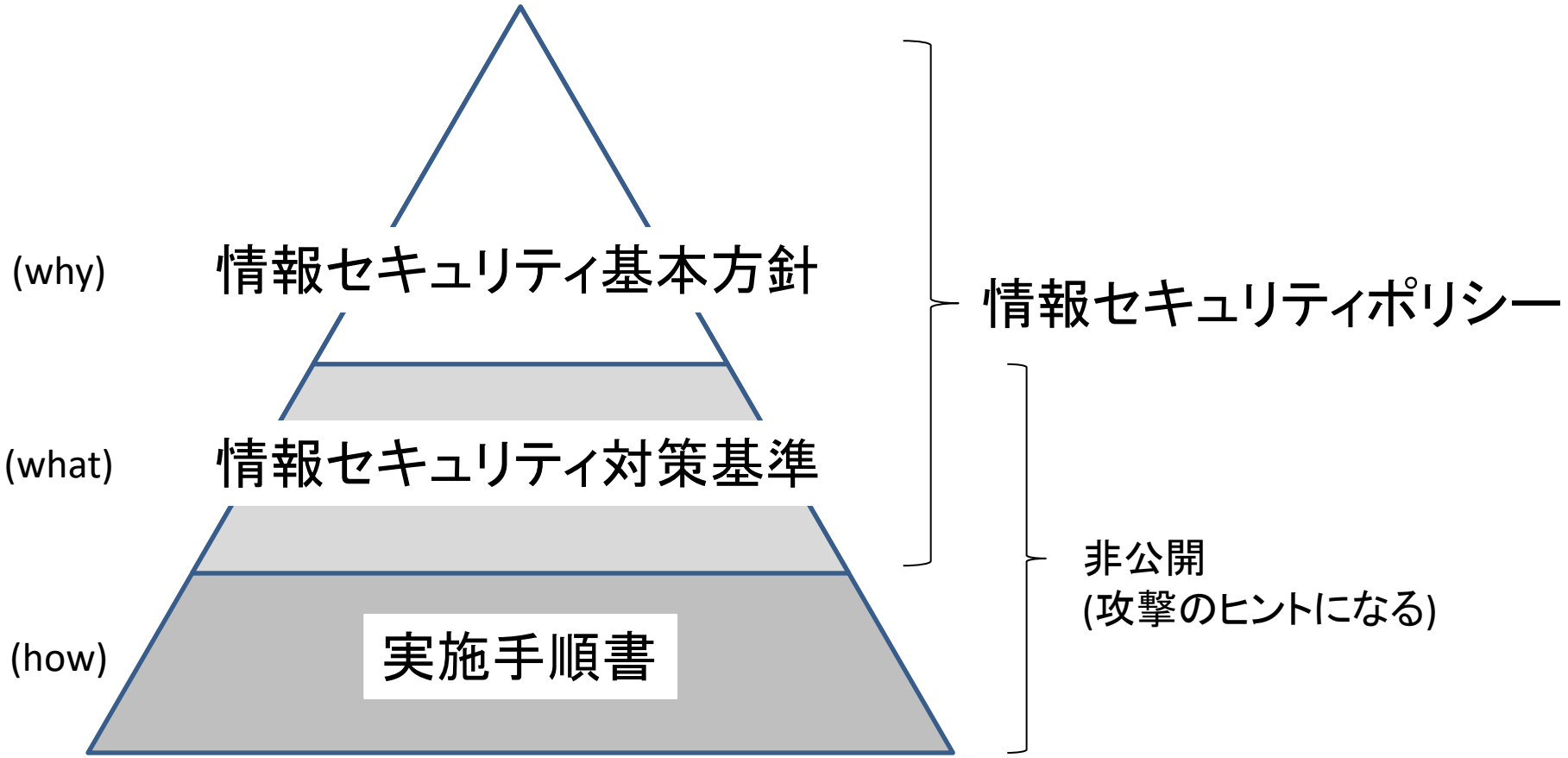

情報セキュリティ委員会
最高情報セキュリティ責任者
役員クラス
情報セキュリティ監査責任者
最高情報セキュリティアドバイザー
統括情報セキュリティ責任者
局長クラス
情報セキュリティ責任者
情報セキュリティ責任者
部門長クラス
情報システムセキュリティ責任者
情報システムセキュリティ責任者
情報システムセキュリティ管理者
情報システムセキュリティ管理者

中小企業の場合

- 全社的な意思決定ができる体制ならOK

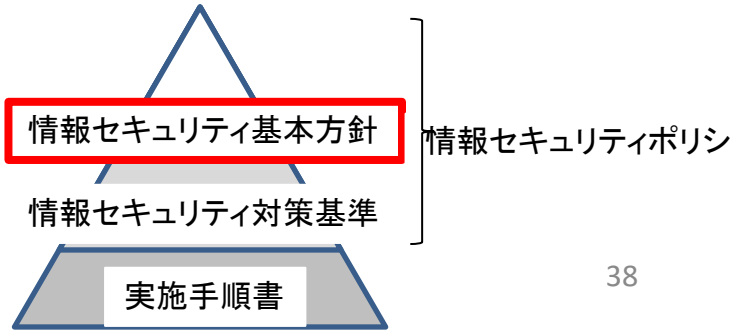


情報セキュリティ関連文書



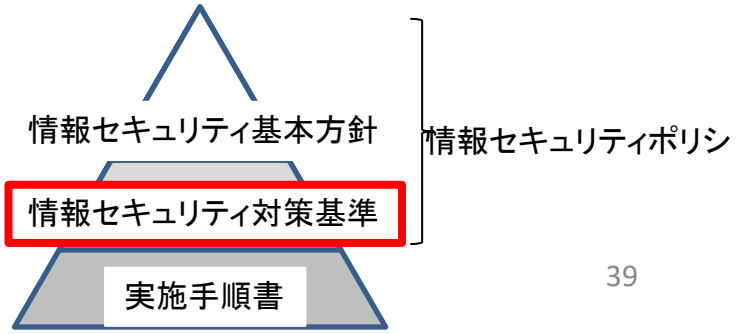
情報セキュリティ基本方針（policy）

- なぜ（why）情報セキュリティが重要であるかということを示す文章
- 組織の情報資産を適切に保護，管理することを経営者が意思表明
- 経営者の名において，組織の情報セキュリティ活動における行動規範，必要な組織体制を記述



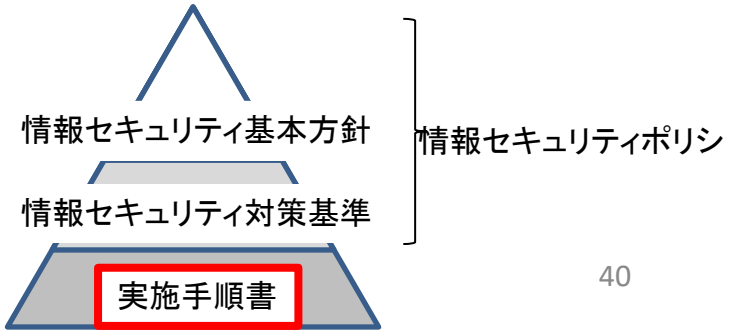
情報セキュリティ対策基準（standards）

- 適用範囲，対象者を明確にし，項目毎に遵守（じゅんしゅ）すべき具体的な項目（what）を網羅的に記述
- 基本方針の宣言を受けて作成



実施手順書（procedures）

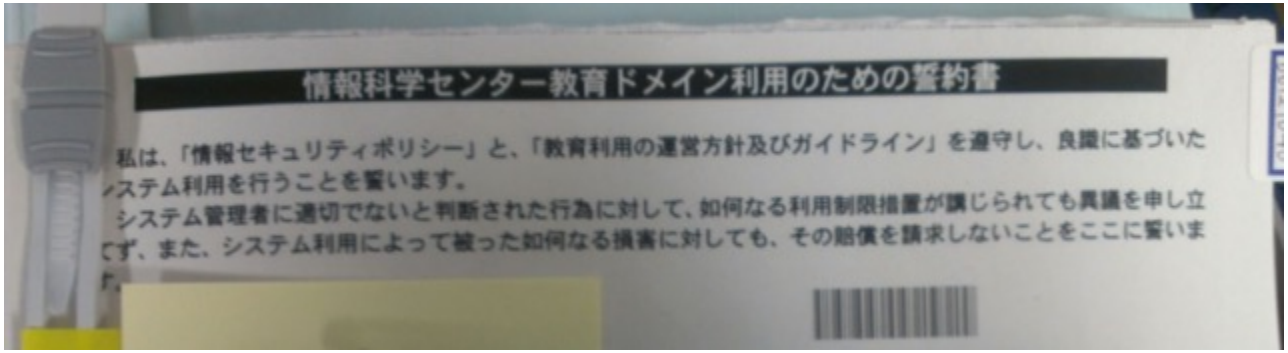
- いかに（how）実施するかを具体的に記述した文書
- 対象者が実際に参照することを前提
- 対策基準に記述された事項から必要に応じて選択
  - ex. Webサーバーの設定
  - ex. 電子メールソフトの使い方
  - ex. 持ち出しPCの取り扱い



京都工芸繊維大学の場合

- 情報セキュリティ基本方針
  - https://www.kit.ac.jp/national_university_corporation/information-security-policy/

- Q:内容を読んだことのある人は？
- Q:内容を覚えている人は？



サンプル規程集

- 政府機関等の情報セキュリティ対策のための統一基準
  - 内閣サイバーセキュリティセンター(NISC)により策定
  - 国立大学は独立行政法人なのでこの基準が適用される
- 高等教育機関の情報セキュリティ対策のためのサンプル規程集
  - 政府統一基準を大学に当てはめたもの
    - 「国立情報学研究所学術情報ネットワーク運営・連携本部　高等教育機関における情報セキュリティポリシー推進部会」にて維持管理
      - 情報工学課程の稲葉先生の名前があります

情報資産の格付け

- どの資産をどの脅威からどのように守るか？
  - 3つのセキュリティ要件から格付け
  1. 機密性：漏洩した場合の影響
  2. 完全性：無許可で変更・削除された場合の影響
  3. 可用性：必要な情報を利用できない場合の影響
  - 脅威,リスク,対策は要件毎に異なる
- 格付けの高いものについて詳細分析
  - 脅威の発生確率、被害の大きさの分析
  - 対象の線引きは経営判断

被害の大きさの定性的な格付け

格付け	内容
1	影響なし
2	一部の業務で軽微な被害が発生
3	事業全体で軽微な被害が発生
4	一部の業務で重大な被害が発生
5	事業の継続に関わる被害が発生

機密性、完全性、可用性のそれぞれについて格付け

機密性（confidentiality）

- 正当と認められるときに，正当と認められる方法で，正当と認められる個人，組織およびプロセスにのみに，データが開放されること
- 確保する方法例
  - アクセス制御，認証，暗号化
  - プログラムやコマンドにも属性を付与
    - データにアクセスするのは人とは限らない

完全性（integrity）

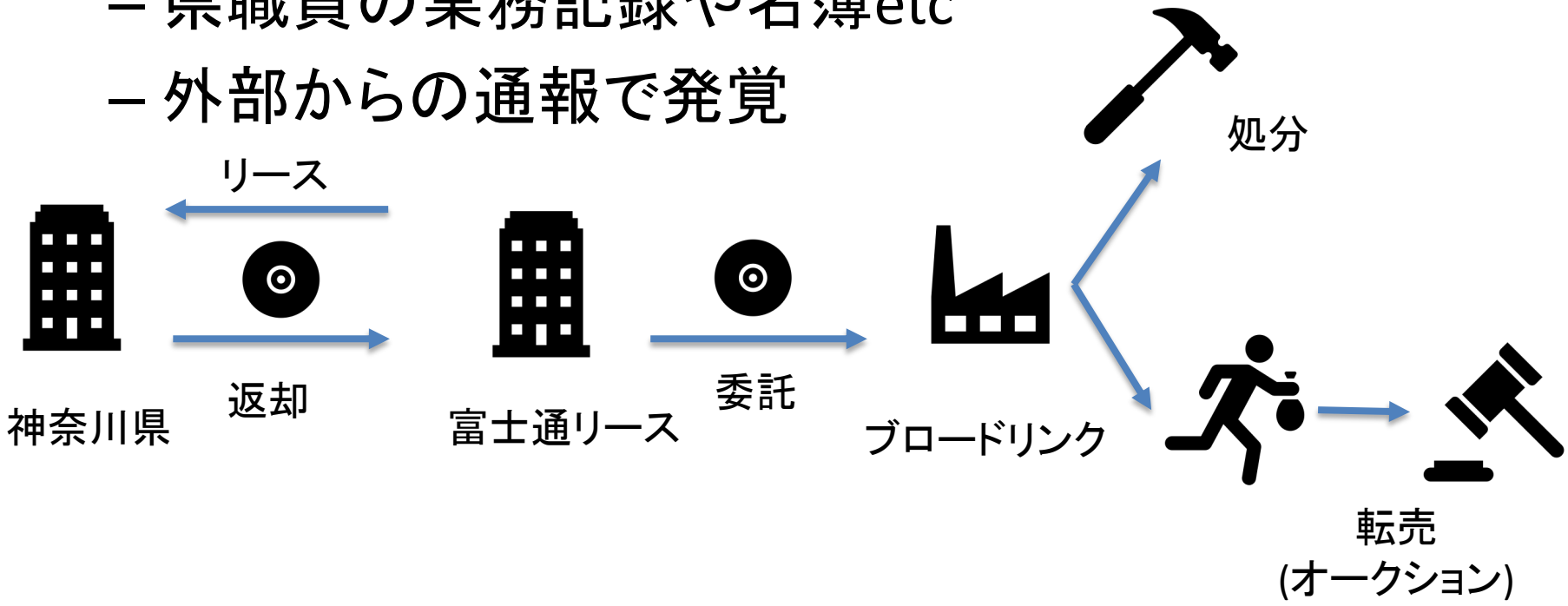
- データにアクセスしたときに，データが常に正確で完全であること.
- 完全性が確保されないシステムは成り立たない
  - 処理結果に矛盾や異常が発生
- 確保する方法例
  - ハッシュ関数やデジタル署名の利用

可用性（availability）

- データおよび情報システムが，要求された方法で適時にアクセス可能かつ利用可能であること
  - 使いたい時に使えなければ意味がない
    - ×頻繁にシステムダウン
    - ×レスポンスが遅い
- 確保する方法例
  - システムやネットワークなどの設備の二重化
  - システムリソース（メモリ，CPU，ディスクスペース）の十分な確保

神奈川県HDD転売・情報流出事件(2019)

- 廃棄したはずのHDDから個人情報流出
  - 個人名・住所が記載された自動車税の納税記録
  - 県職員の業務記録や名簿etc
  - 外部からの通報で発覚



成績表改ざん(2019)

- 成績表改ざん疑いの中学生「3教科で評価“3”を“4”に」
  - 中学校3年生の学生
    - 教員用サーバのID・パスワードを入手
    - スマートフォンで教員用端末を遠隔操作
    - 「ためらいはあったものの、好奇心がまさってしまった」
  - 参考:教員用PC貸与が発端となった中学生による校内不正アクセス事案についてまとめてみた

自治体クラウド障害(2019)

- 自治体クラウドJip-Base(70団体が利用)
  - 記憶装置に障害発生。サービス停止(12/4)
  - バックアップデータから復旧を試みるも…
  - 53自治体でシステム障害、7割復旧も全面復旧の見通し立たず(12/16時点)
    - 一部自治体でバックアップがエラーになっていた
- システム障害の練馬区、通知表の学期末配布できず…年明けに延期(12/17)

情報資産の価値評価

- 機密性，完全性，可用性を段階に分類
  - 例：高/中/低（＝3/2/1）
- 各情報資産管理責任部門で評価

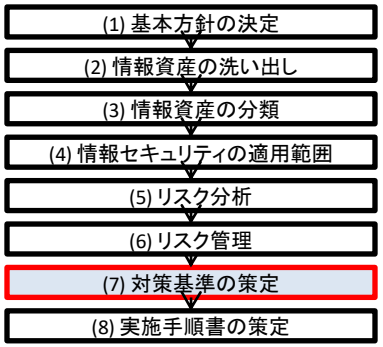
No.	情報資産	管理責任者	情報資産の価値		
			機密性	完全性	可用性
1	顧客情報	△△△△	3	2	1
2	取引先情報	○○○○	2	3	1
3	…	…	…	…	…

機密性，完全性，可用性の優先度

- いずれも不可欠な特性
- システムの特徴や性質により求められるレベルや優先順位は異なる
  - 機密情報を取り扱うシステム
    - 機密性最優先
  - 災害情報の収集・提供システム
    - 高い可用性
  - 公共的なシステム
    - 高い完全性と可用性

情報セキュリティ対策基準の策定

- 組織のもつ情報資産に対してどのような管理策（保護対策）をとらねばならないかを決定
- 情報セキュリティ対策の分類
  - 物理的セキュリティ対策
  - 技術的セキュリティ対策
  - 人的セキュリティ対策



物理的セキュリティ対策

- 情報システム機器（コンピュータ設備，ネットワーク設備など）および付帯設備（電源設備，空調設備など）の損壊および設置場所への不法侵入などにより，情報システムの正常運用が阻害されることを防止するための対策

物理的セキュリティ対策例

- セキュリティを確保するための障壁を設置し，入退出管理を施す
- 災害対策を施す
  - 火災，水害，地震などにより想定される最悪の事態から，いかに迅速に情報システムを元の状態に復旧させるかが重要
- 防犯対策を施す
- 電源設備，通信ケーブルなどのセキュリティ確保
- オフィスの机の上を整理整頓する

技術的セキュリティ対策

- アクセス制御
  - 職位，権限に応じて利用者に加えられる情報システムの利用範囲の制限をシステム技術的に実現する機構
  - 例：ユーザIDとパスワード
- データ秘匿のための暗号化など

人的セキュリティ対策

- 組織の編成
- 組織毎の責任分担
- 教育訓練
- 採用時の身元確認
- 運用手続き
- システム開発管理
- 事故発生時の連絡体制
- 復旧手続き

教育，罰則

- 情報セキュリティ対策は，組織全員の情報セキュリティ意識の喚起，規定遵守，未規定の事態に対する判断能力が必要
- 組織の構成員に情報セキュリティに対する責務を自覚させるため教育・啓蒙活動実施
  - 情報セキュリティポリシの周知など
- 罰則規定
  - 規定遵守のため
    - 情報セキュリティポリシの形骸化を防ぐ
  - 就業規則との整合性必要

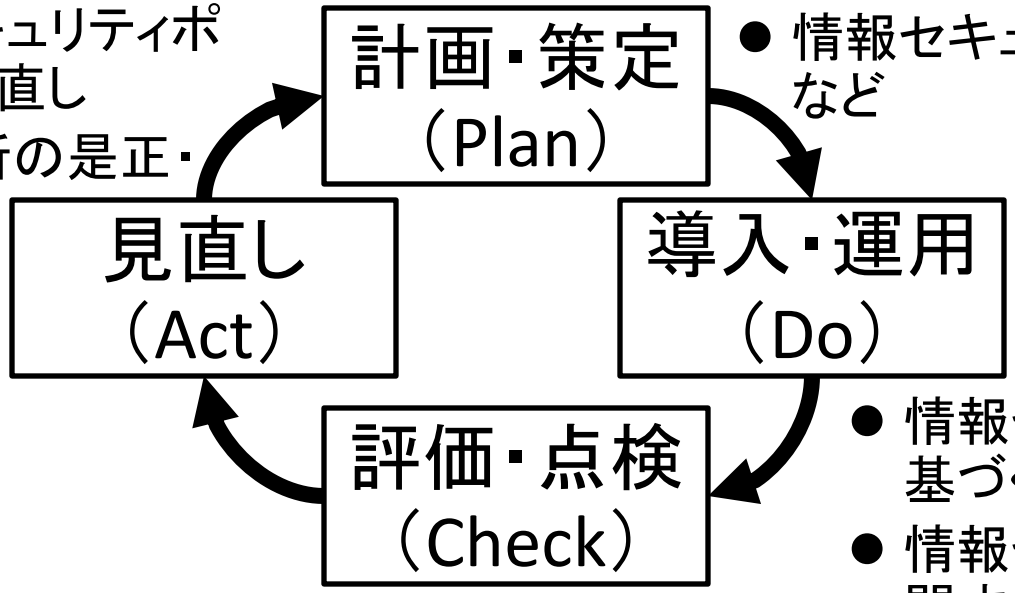
規則は守られるか？

- 具体的･合理的であること
- 悪い例
  - 判断基準のない規則
    - 「重要な情報は適切に暗号化してください」
  - 時代遅れになった規則
    - 「データはフロッピーディスクで受け渡すこと」

評価・見直し

- 情報セキュリティポリシの定期的評価必要
  - 過剰なコントロールになっていないか
  - 経営目標の達成に役立っているか
  - 技術革新による情報システムの進化
  - 組織活動活発化による情報資産の増加
- 問題があれば情報セキュリティポリシを見直し
  - 更新したポリシを組織構成員に周知
- 評価方法例
  - セキュリティ強度テスト
  - 第三者による情報セキュリティ監査

ISMSのPDCAサイクル



- 情報セキュリティマネジメント推進計画の立案
- リスクアセスメントの実施
- 情報セキュリティポリシの策定など

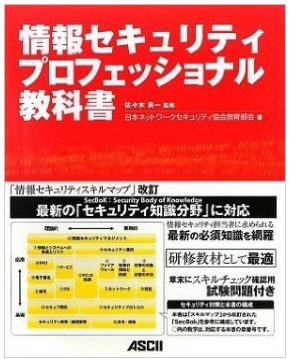
- 情報セキュリティポリシに基づく対策の実施・運用
- 情報セキュリティポリシに関する教育の実施
- システムの正常稼働，不正アクセスの監視など

- 情報セキュリティポリシ遵守状況の評価
- 情報セキュリティポリシの適切性の監査

- 情報セキュリティポリシの見直し
- 問題箇所の是正・改善など

参考資料

- 情報セキュリティプロフェッショナル教科書
  - アスキー・メディアワークス
  - ISBN: 978-4048677820
- 情報セキュリティ教本
  - 実教出版
  - ISBN: 978-4407316964
- 情報セキュリティ教科書
  - 東京電機大学出版局
  - ISBN: 978-4501544300



参考資料

- ヒューマンエラー
  - 丸善
  - ISBN: 978-4621080573

- 技術者倫理とリスクマネジメント
  - オーム社
  - ISBN:978-4274068720