情報セキュリティ基礎

第１回　イントロダクション

藤本 章宏

自己紹介

- 和歌山大学学術情報センター
  システム工学部NIメジャー
- 講師　藤本 章宏（ふじもと あきひろ）
- 専門
  - ✓ 情報ネットワーク
- 業務
  - ✓ セキュリティ教育、インシデント対応、脆弱性検査など

質問等は fujimoto@wakayama-u.ac.jp まで

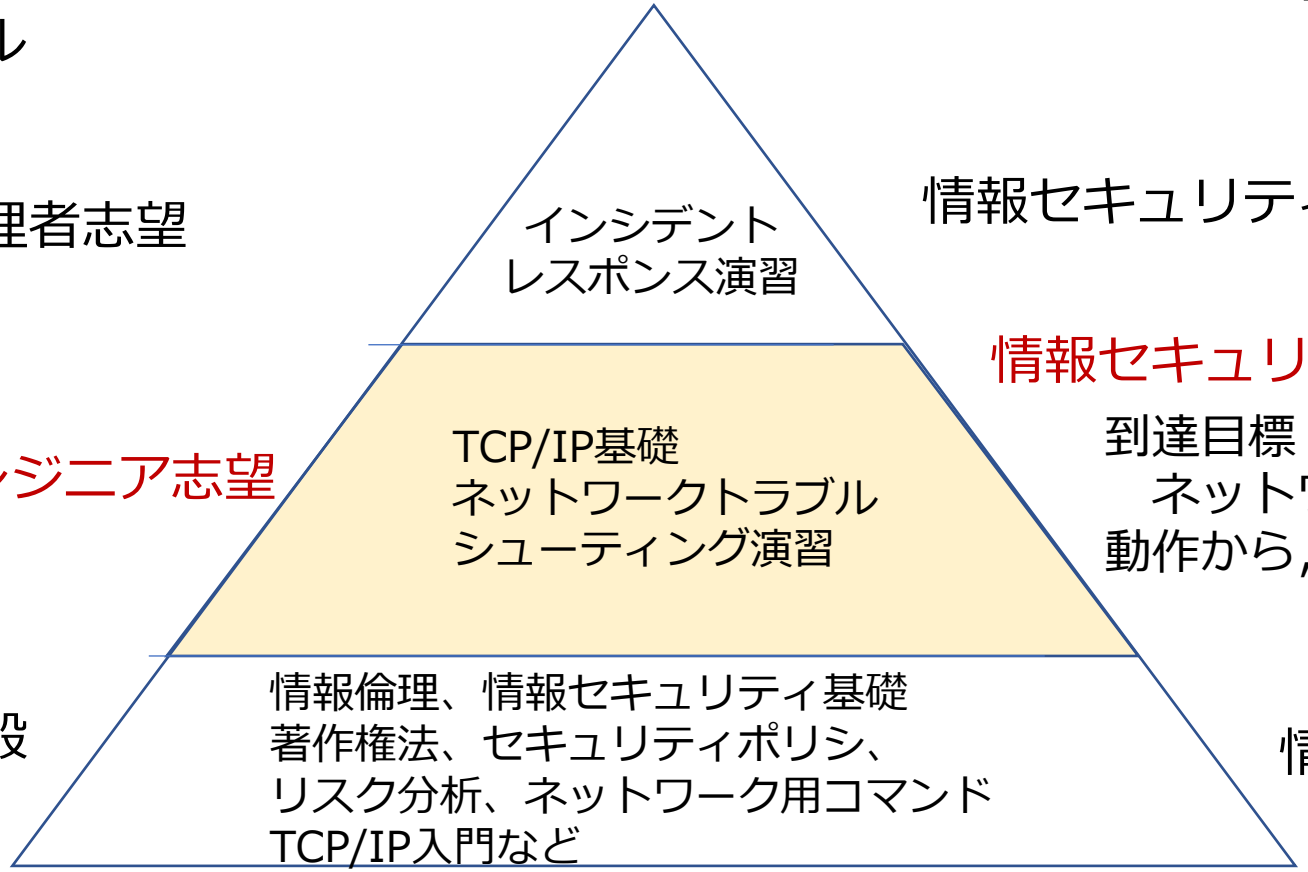
情報セキュリティ関連リカレントコース

対象、レベル

コース名

ネットワーク管理者志望
（大学院以上）

情報セキュリティエキスパート（仮）



情報セキュリティ基礎

到達目標：
　ネットワーク/アプリケーションの
動作から，攻撃の仕組みをイメージできる

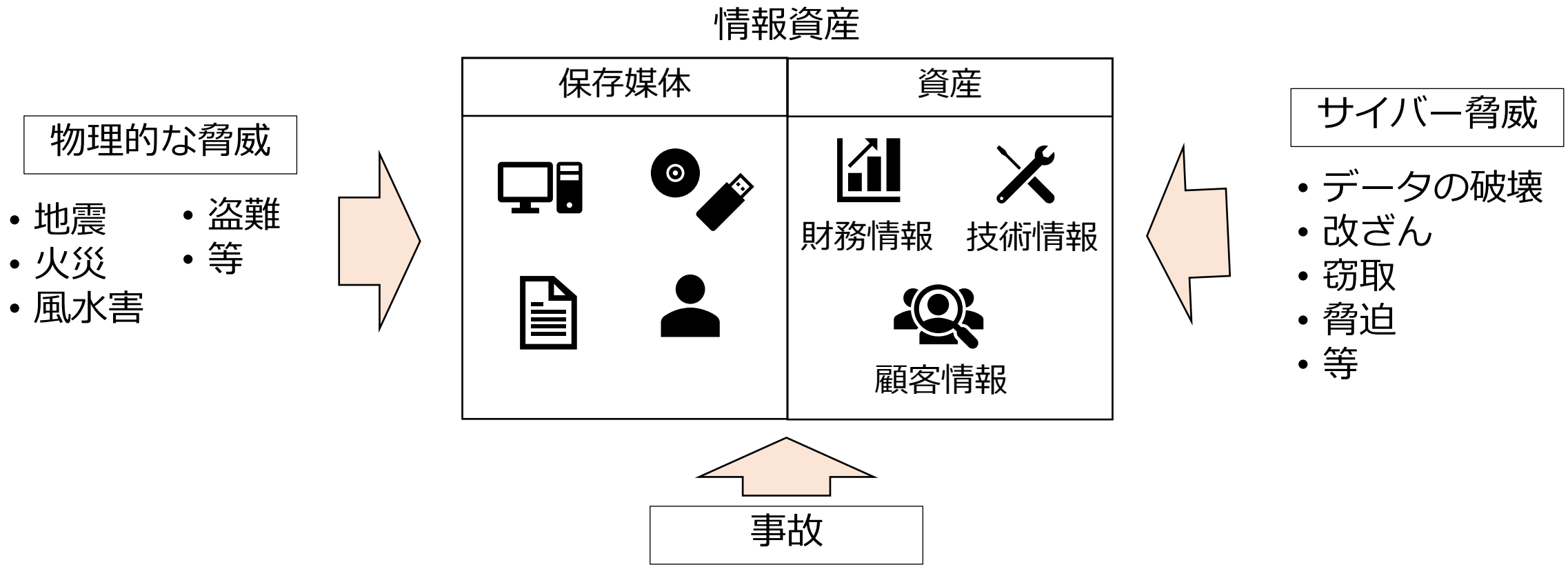
ネットワークエンジニア志望
（学部相当）

市民、社会人一般
（市民講座）

情報セキュリティ入門

情報セキュリティとは？

情報資産を様々な**脅威から守り、維持**すること



情報セキュリティの３要素

C onfidentiality (機密性)

権限を持った正規の利用者だけが情報にアクセスできること

対策例　アクセス制御や認証，暗号化

I ntegrity (完全性)

情報が**正確であり、欠落や改ざんの無い**状態を維持できること

対策例　ハッシュ関数やデジタル署名による検証

A vailability (可用性)

必要なときに、情報に**いつでもアクセス**できること

対策例　システムの二重化，バックアップ

情報セキュリティの７要素

3要素（CIA）に加えて以下の４要素

真正性

利用者やシステム，情報などが
主張どおりであることを確実にすること

「なりすまし」でないことを証明できること

対策例　多要素認証

責任追跡性

利用者やシステムの**振る舞いを**
遡って追跡することができること

対策例　アクセスログの取得

否認防止

利用者の行動を，本人が後から
否認できないように証明できること

対策例　操作ログの保存，デジタル署名

信頼性

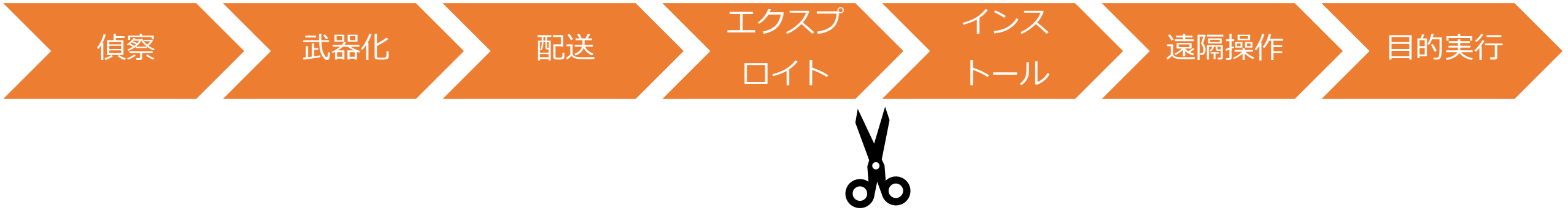
情報システムが**意図したとおりに動作し**，
結果を出力できること

欠陥やバグ等が無く，正常に動作すること

サイバーキルチェーン

サイバーキルチェーン

- 2009年に米「ロッキード・マーティン社」が考案したモデル
- 軍事分野で用いられていた概念を、サイバー攻撃（主に標的型攻撃）に応用したもの



いずれかのフェーズで止めることができれば，被害を食い止めることが可能

情報セキュリティにおけるリスク管理

限られたリソースで全てを守り切るのは不可能

- 検知だけでも様々なパターンを考える必要がある
- 漠然とした対策ではなく，**リスクに応じた優先度付**けが重要

リスクを評価するために

✓ 守るべきものは何か？

✓ それを脅かす脅威はどのようなものか？

を把握しておく必要がある

情報資産の把握と重要度の特定

手順

1. 情報資産管理台帳の作成

   事業において必要な情報資産を整理し，管理者や管理方法を明確化

2. 機密性・完全性・可用性の評価

   それぞれの特性が損なわれた場合の事業への影響や，法律遵守の観点から評価

3. 重要度の算出

   機密性・完全性・可用性の評価に基づき，その情報資産の重要度を決定

   算出例：機密性・完全性・可用性の最大値

参考: IPA 中小企業の情報セキュリティ対策ガイドライン 第3.1版

https://www.ipa.go.jp/security/guide/sme/about.html

洗い出し対象となる情報資産

情報資産は様々な場所に保管されていることに留意

保管媒体

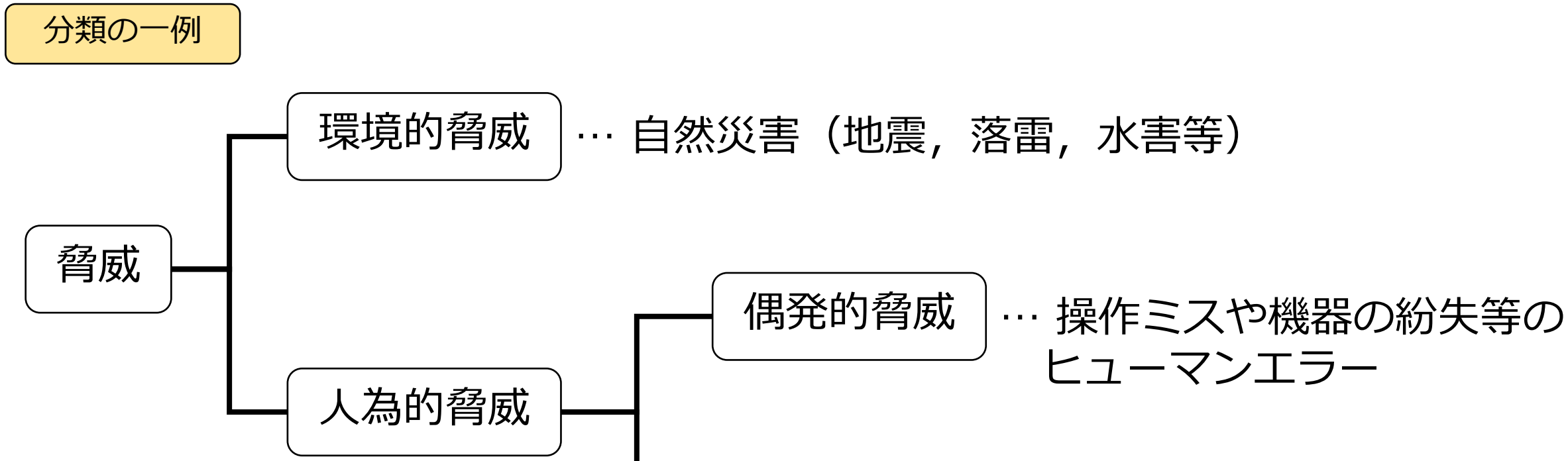
- ✓ HDD
- ✓ USBメモリ
- ✓ CD/DVD
- ✓ 紙

保管場所

- ✓ データベース
- ✓ クラウドストレージ
- ✓ 各部署のファイルサーバ
- ✓ 各ユーザのPC
- ✓ 委託先のストレージ
- ✓ 金庫や倉庫
- ✓ 机の引き出し

情報資産を脅かす脅威

脅威 = 情報セキュリティを脅かし，損失を発生させる直接的な原因



攻撃手法を知り，対策を立てる

サイバーキルチェーン

スキャン

- フィッシングサイト
- Webサイト改ざん
- マルウェアサイト

(メール等で誘導)

DoS/DDoS

いずれかのフェーズで止めることが
できれば，被害を食い止めることが可能

次回から

- ネットワークの仕組み
- なぜ攻撃が成立するか