情報セキュリティ

第1回： ガイダンス

◆テキスト

『情報セキュリティ読本 五訂版』, 実教出版株式会社
『ネットワークセキュリティ』, オーム社

◆参考書

『情報セキュリティの技術と対策がしっかりわかる教科書』, 技術評論社
『入門サイバーセキュリティ理論と実験』, コロナ社

◆履修条件

特になし

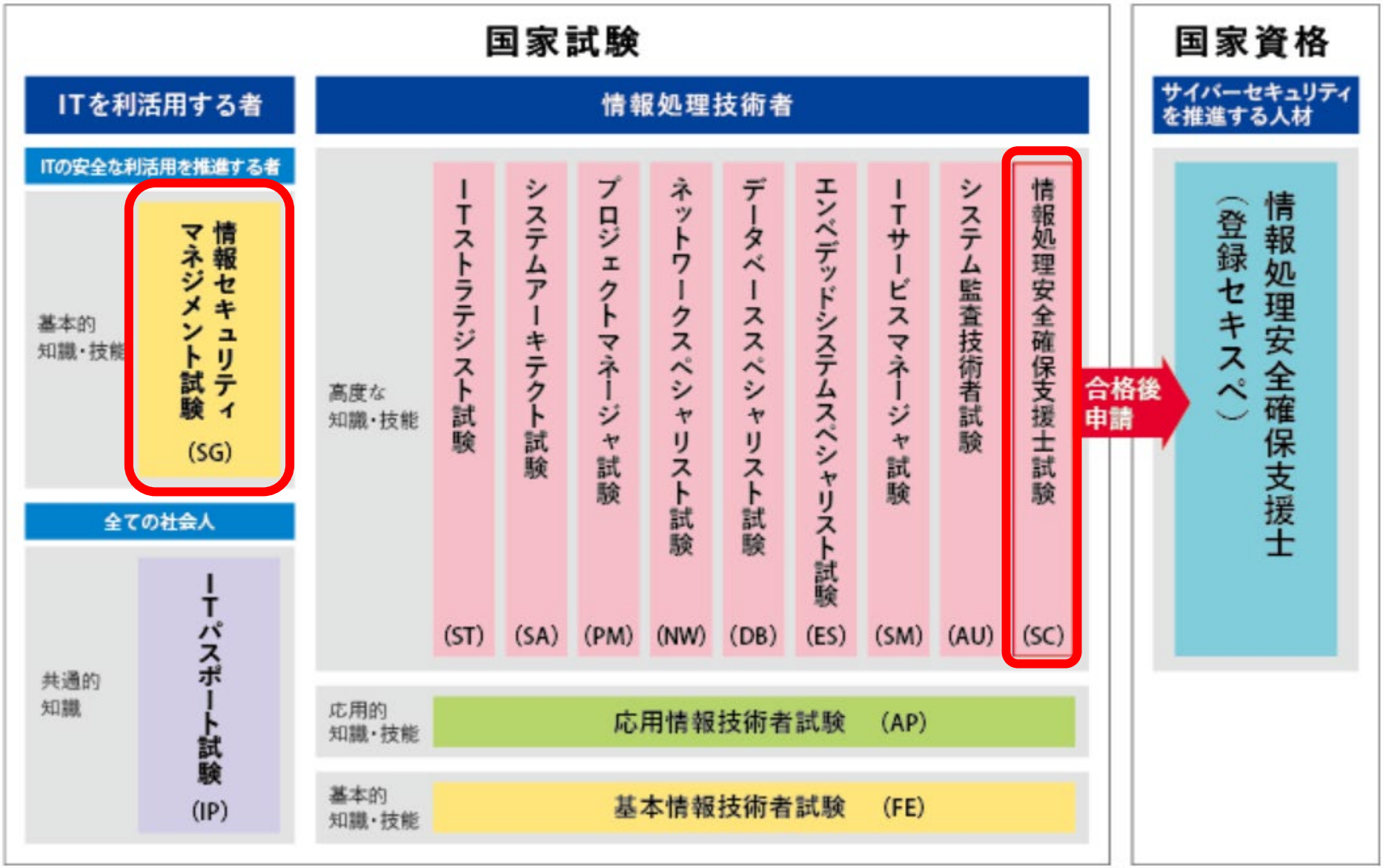
◆評価

- ✓ 認定条件：出席率80%以上
- ✓ 評価方法：小テスト（3回）：50%, 本試験：50%

◆授業の到達目標

- 事例を元に情報セキュリティ対策の必要性を理解する.
- コンピュータウイルス（マルウェア）侵入の可能性, コンピュータウイルス（マルウェア）の感染場所と感染後の動作による分類を理解する.
- アンチウイルス（マルウェア対処）ソフトウェアの基本的な仕組みを理解し説明できる.
- ネットワーク上の様々なサイバー攻撃手法および攻撃への対策を理解し, 説明できる.
- 暗号化・認証手法等セキュリティ技術および方法を修得する.

＜参考＞情報処理関係の国家試験と国家資格



授業計画

①ガイダンス
② インターネット上の脅威について
③ 攻撃について
④ コンピュータウイルス（マルウェア）について
⑤ 小テスト，ネットワーク上の各種攻撃の紹介
⑥ 攻撃の技術
⑦ 情報・ネットワーク技術の基礎
⑧ ネットワークセキュリティに関する技術と方法
⑨ 暗号の基礎
⑩ 小テスト，セキュリティ技術と方法に対する確認
⑪ 対処法１（システムリスク）
⑫ 対処法２（ソーシャルリスク：SNS）
⑬ 対処法３（ソーシャルリスク：インターネット・スマホゲーム）
⑭ 対処法に関する小テスト
⑮ 全体のまとめ

本日の講義内容

1. 情報システムの脅威
2. 情報セキュリティの定義
3. 情報セキュリティの構成要素
4. 情報資産
5. リスクとインシデント
6. 情報リテラシーと情報倫理

Ⅰ. 情報システムの脅威

ネットワークされた情報システムは，情報の共有やサービスの提供を迅速，便利（時間・場所の制限なく）とすることが可能となり，たくさんのメリットをもたらしている．

一方，それに伴い，ネットワーク（サイバー）空間での脅威が社会に及ぼす影響も深刻になってきた． 例えば，

- 不正アクセスによる社会インフラの停止や膨大な経済的な損失
- 標的型攻撃によるマルウェアの感染やデータベースから情報の漏えい
- ランサムウェアによる身代金請求　など

情報セキュリティ10大脅威 2024年版 [個人]（IPA）

「個人」向け脅威（五十音順）
インターネット上のサービスからの個人情報の窃取
インターネット上のサービスへの不正ログイン
クレジットカード情報の不正利用
スマホ決済の不正利用
偽警告によるインターネット詐欺
ネット上の誹謗・中傷・デマ
フィッシングによる個人情報等の詐取
不正アプリによるスマートフォン利用者への被害
メールやSMS等を使った脅迫・詐欺の手口による金銭要求
ワンクリック請求等の不当請求による金銭被害

情報セキュリティ10大脅威 2024年版 [組織]（IPA）

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロディ攻撃）
6	不注意による情報漏えい等の被害
7	脆弱性対策情報の公開に伴う悪用増加
8	ビジネスメール詐欺による金銭被害
9	テレワーク等のニューノーマルな働き方を狙った攻撃
10	犯罪のビジネス化（アンダーグラウンドサービス）

2. 情報セキュリティの定義

情報セキュリティとは，「正当な権利を持つ個人や組織が，情報や情報システムを意図通りに制御できることと，情報の機密性，完全性，および可用性を維持すること」である．

3. 情報セキュリティの構成要素

3.1　3大主要な要素

要素名	定義
機密性 (Confidentiality)	許可された者だけが情報にアクセスできるようにすることです．つまり，情報が漏洩しないことを指します．
完全性 (Integrity)	情報が正確であり，完全である状態を保持し，保護することです．つまり，情報が改ざんされたり，破損されたりしてしないことを指します．
可用性 (Availability)	許可された者が必要なときにいつでも情報にアクセスできるようにすることです．つまり，情報の保存・伝送媒体や処理機器が壊れたりすることがあっても，この可用性が損なわれないことを指します．

注：機密性は秘匿性とも呼ばれる．

- 機密性に対する脅威の例
  - ネットワークの盗聴
  - 不正コピー

- 完全性に対する脅威の例
  - データの改ざん
  - 偽造

- 可用性に対する脅威の例
  - サービス利用不能攻撃（DoS）
  - 破壊

3.2 4つ付加要素

要素名	定義
真正性 (Authenticity)	ユーザや情報そのものが本物であることを明確にすることです.
責任追跡性 (Accountability)	ある行為が誰によって行われたかを明確にすることです.
否認防止 (Non-Repudiation)	情報の作成者が作成した事実を後から否認できないようにすることです.
信頼性 (Reliability)	情報システムの処理が, 欠陥や不具合なく確実に行われることです.

4. 情報資産

4.1 情報資産とは

個人および組織に蓄えられている個人情報，技術情報，人事情報，顧客情報，戦略情報，財務情報などです．情報には価値があります．

4.2 情報資産の形態

- データ
- ノウハウ
- ハードウェア
- ソフトウェア
- ネットワーク
- システム　など

5. リスクとインシデント

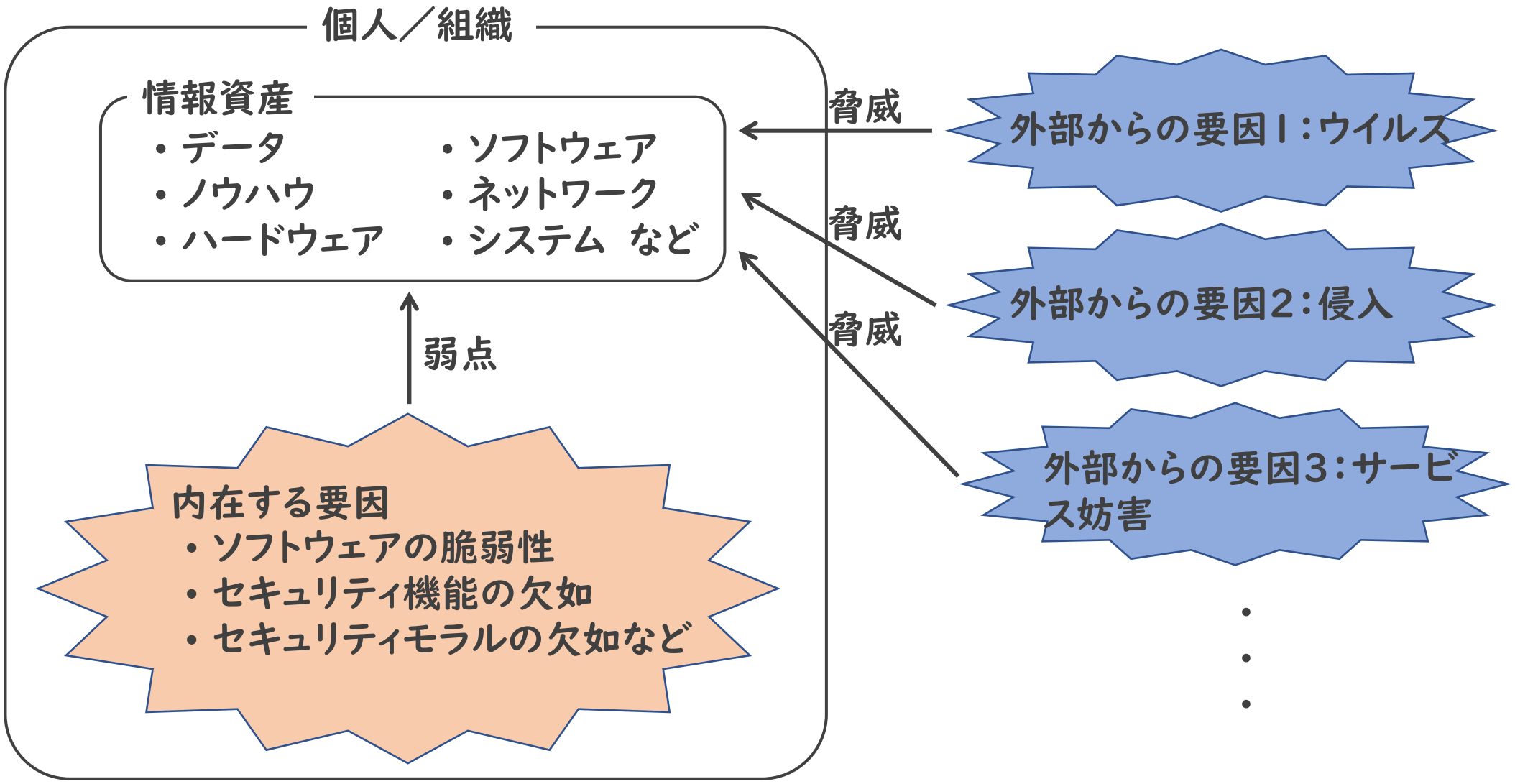
5. 1　定義

リスク（risk）とは，情報資産を脅かす内外の要因（脅威と脆弱性など）によって情報資産が損なわれる可能性をいいます．

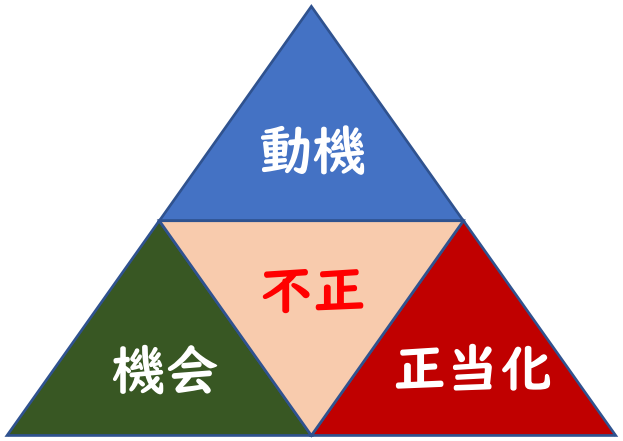
インシデント（incident）とは，実際に情報資産が損なわれるリスクが顕在化した事態をいいます．

ただし，脆弱性（vulnerability）とは，脅威の発生を招く内在の弱点のことです．また，脅威とは，情報資産に危害を与える原因となるものです．

5.2 リスク／インシデントの要因



5.3 不正行為のメカニズム



不正のトライアングル

動機

不正を行うしかないと考えるに至ってしまった事情，または不正を行うことを駆使する心理です．例えば，金銭や人間関係上の問題（トラブル），心理的プレッシャー，自己主張，自己満足など

機会

不正を行う環境があることを指します．例えば，親友や同僚などが関連業務を行っている，ネットワークに手軽にアクセスできる，電子機器やソフトウェアが簡単に入手できるなど

正当化

不正を行うために，自身を納得させる理由付けのことを指します．例えば，何かを守るために仕方なくやる，個人のノルマ達成や保身のために仕方なくやる，何となく役に立つからやるなど

不正は，「動機」「機会」「正当化」という要素が相関するときに起こる可能性の高い事象です

6. 情報リテラシーと情報倫理

6.1 情報リテラシー

情報リテラシーとは，情報機器やネットワークを活用する基本的な能力のことで，コンピュータの操作，データの作成や整理，情報検索能力のような，情報やデータを取り扱う上で必要となる基本的な知識や能力のことを指します．

その中に，情報セキュリティに関する基本的な知識も情報リテラシーに含まれると考えられている．

6.2 情報倫理

情報通信社会で必要とされる道徳やモラルであり，情報モラル，情報マナーともいいます．

インターネット上では，現実の人の顔が見えないため，過度に攻撃的な書き込みをしたり，いわれのない誹謗中傷などが行われることがあります．

SNSの利用においても，情報倫理やコンプライアンス違反の問題が起きています．例えば，自身が働くお店に来店したお客さんの情報を投稿したり，組織内の情報を外部に投稿したりすることが見受けられ，問題になっています．

誰もが守るべき基本的なこと：

- 他人の誹謗・中傷をしない
- 他人のプライバシーを侵害しない
- 著作権侵害をしない
- 組織内の情報を外部に漏洩しない

練習問題

1. 情報セキュリティの3大主要な要素はどんなものかを述べなさい.

2. インシデントが発生する仕組みについて簡単に述べなさい.