(2030~2040)

第２部　情報セキュリティ（必須）

＊出題のポイント

２０点

1. 情報セキュリティの技術要素

基礎知識：**暗号化**と**認証技術**

ハイブリッド暗号方式（共通鍵＋公開鍵）

**公開鍵暗号基盤**（PKI: Public Key Infrastructure）

＝印鑑と印鑑証明

**認証局**（CA: Certification Authority）

1. 進化を続ける攻撃手法

**ランサムウェア、標的型攻撃、水飲み場型攻撃**

身代ウェア, Targeted attack, Watering hole attack

1. 情報セキュリティ問題を解く心構え

**通信プロトコルに関する知識やネットワーク構成図を読み解いたうえで整理する力**