

## 第8章 章末問題 解答

1. a: 暗号化鍵, b: 復号化鍵, c: 共有鍵暗号方式, d: 公開鍵暗号方式, e: 公開鍵暗号方式, f: 共通鍵暗号方式
2. (1)SSID 隠ぺい, MAC アドレスフィルタリング, (2)暗号化, 改ざん検知 (WPA など), (3)802.1X 認証, WEB 認証
3. Bluetooth, ZigBee などの近距離通信システム, 電子レンジからの漏洩電磁波などがある.
4. 暗号のためのシード長が短く (64 ビット), 現在の PC の能力では容易に解読できる. また, 改ざんを有効に検知する仕組みもなかった. 現在はシード長を長く, かつパケットごとに変化させることで解読を困難にしている. ハッシュを用いた改ざん検出も実装している.
5. 略