正誤表（令和３年６月 30 日）

正誤箇所	誤	正
「教育情報セキュリティポリシーに関するガイドライン」（令和３年５月版） 1.6.1. コンピュータ及びネットワークの管理 （１４）無線 LAN 及びネットワークの盗聴対策 修正前：P74 修正後：P74	（注１０）暗号化方式の１つである WEP（Wired Equivalent Privacy）については、既に脆弱性が公知となっているため、暗号強度が確認されている暗号方式を採用しなければならない。	（注１０）暗号化方式の１つである WEP（Wired Equivalent Privacy）及び WPA（WPA（Wi-Fi Protected Access）については、既に脆弱性が公知となっているため、暗号強度が確認されている WPA2 以降の暗号方式を採用しなければならない。暗号化を含めた無線 LAN 全般に関するセキュリティ対策は「Wi-Fi 提供者向け セキュリティ対策の手引き」を参照されたい。 （https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/）
「教育情報セキュリティポリシーに関するガイドライン」（令和３年５月版）ハンドブック ４－１　情報資産の分類と管理方法 修正前：P12 修正後：P12	（出典）教育情報セキュリティポリシーに関するガイドライン「図表６　情報資産の例示」	（出典）教育情報セキュリティポリシーに関するガイドライン「図表５　情報資産の例示」

「教育情報セキュリティポリシーに関するガイドライン」（令和３年５月版）ハンドブック ５－３　物理的対策 （１）通信回線及び通信回線装置の管理 修正前：P22 修正後：P22	コラム「SSID 非表示設定はセキュリティ対策ではない？！」 SSID の非表示設定（ステルス SSID)は一見してネットワークが見つからないため、安心感があります。しかし、実際には非表示ネットワークは簡単に見破ることができてしまい、セキュリティ対策とは見なされないので十分な注意が必要です。 SSID の非表示設定がされているネットワークを優先的に攻撃するツールもありますので、SSID を隠蔽するのではなく、ネットワークの暗号化や、WPA（Wi-Fi Protected Access）または WPA2 を使用しましょう。（WPA2 以降を推奨）	コラム「SSID 非表示設定はセキュリティ対策ではない？！」 SSID の非表示設定（ステルス SSID)は一見してネットワークが見つからないため、安心感があります。しかし、実際には非表示ネットワークは簡単に見破ることができてしまい、セキュリティ対策とは見なされないので十分な注意が必要です。 SSID の非表示設定がされているネットワークを優先的に攻撃するツールもありますので、SSID を隠蔽するのではなく、WPA2 以降による暗号化を利用しましょう。 暗号化を含めた無線 LAN のセキュリティ対策全般については「Wi-Fi 提供者向け セキュリティ対策の手引き」も参照しましょう。 https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/
「教育情報セキュリティポリシーに関するガイドライン」（令和３年５月版）ハンドブック 用語集 修正前：P46 修正後：P46	用語 QAuth 2.0	用語 OAuth 2.0