

## 正誤表

正誤箇所	誤	正
<p>「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)</p> <p>1.6.1. コンピュータ及びネットワークの管理</p> <p>(14) 無線 LAN 及びネットワークの盗聴対策</p> <p>修正前：P74 修正後：P74</p>	<p>(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。</p>	<p>(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。</p> <p>(<a href="https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/">https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/</a>)</p>
<p>「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</p> <p>4-1 情報資産の分類と管理方法</p> <p>修正前：P12 修正後：P12</p>	<p>(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」</p>	<p>(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」</p>

<p>「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</p> <p>5-3 物理的対策</p> <p>(1) 通信回線及び通信回線装置の管理</p> <p>修正前:P22 修正後:P22</p>	<p>コラム「SSID非表示設定はセキュリティ対策ではない?!」</p> <p>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もので十分な注意が必要です。</p> <p>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)</p>	<p>コラム「SSID非表示設定はセキュリティ対策ではない?!」</p> <p>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もので十分な注意が必要です。</p> <p>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。</p> <p>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。</p> <p><a href="https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/">https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/</a></p>
<p>「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</p> <p>用語集</p> <p>修正前:P46 修正後:P46</p>	<p>用語</p> <p>OAuth 2.0</p>	<p>用語</p> <p>OAuth 2.0</p>