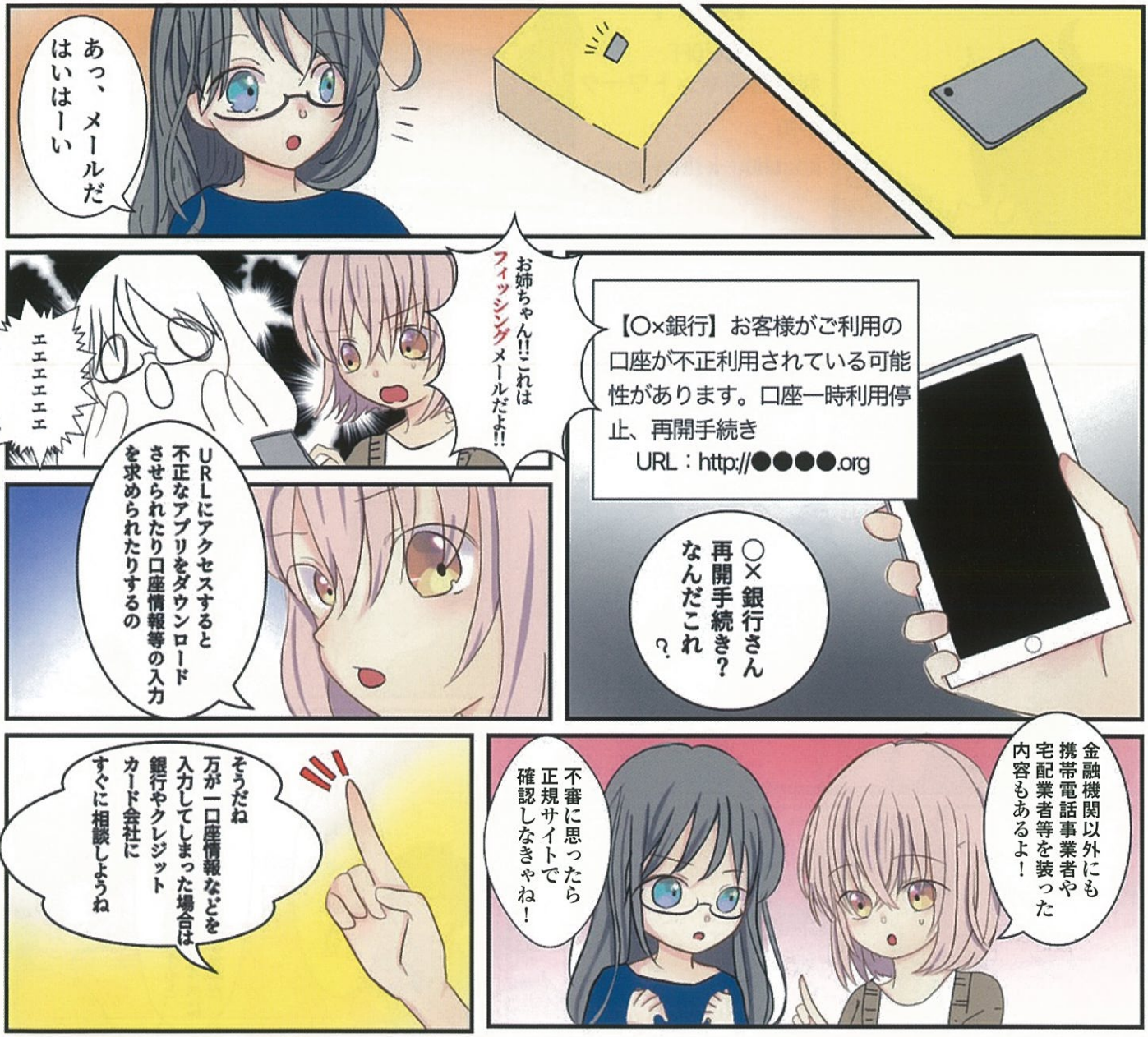
メール・SMSによるフィッシングに注意！



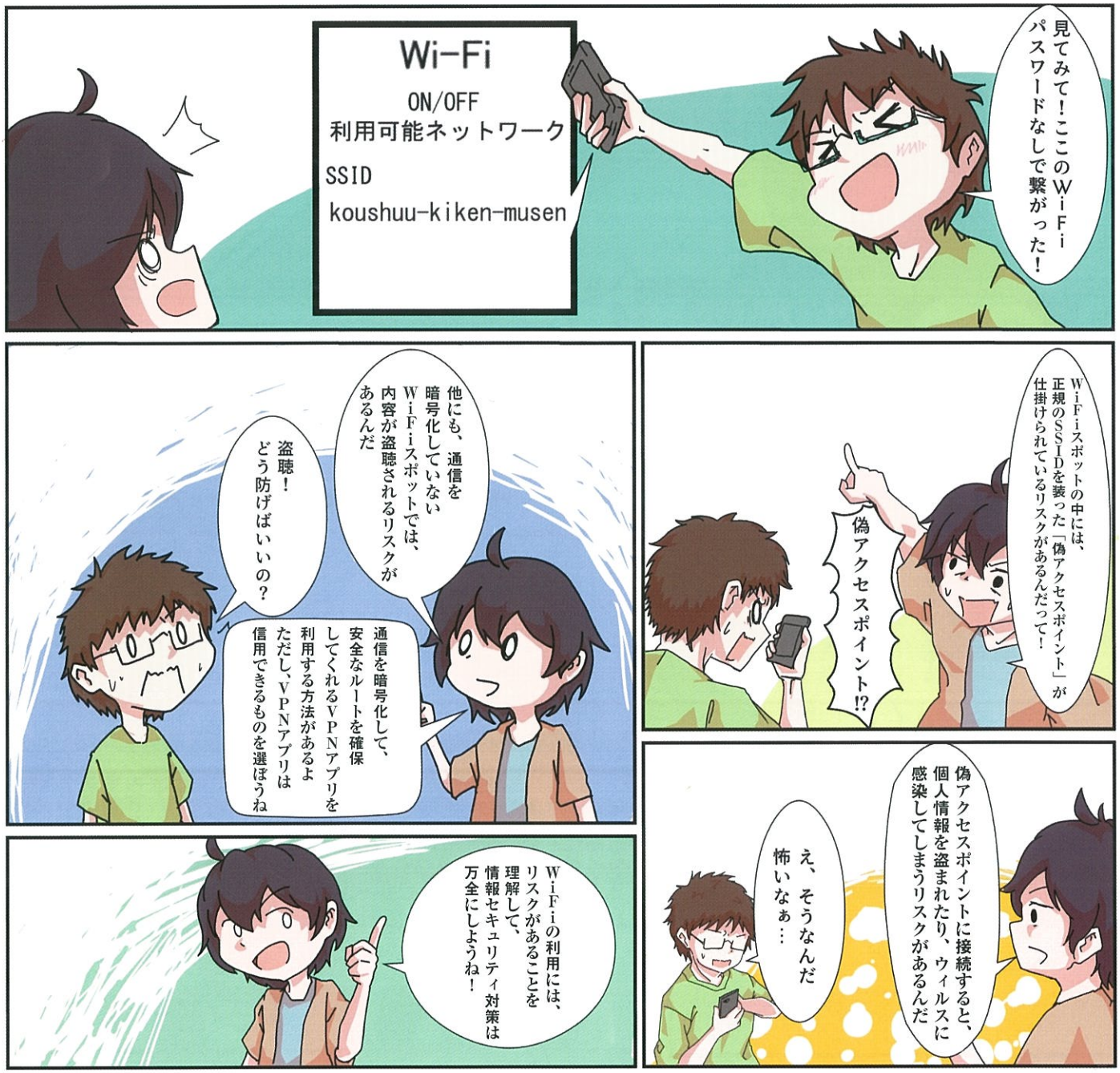
被害防止のポイント

- ○ 端末や機器は常に最新の状態にアップデートしておく
- ○ メール・SMSに記載のURLにはアクセスしない
- ○ アクセス先で口座情報や暗証番号等は入力しない
- ○ 記載内容の事実確認は正規サイトから行う
- ○ 何かあった時の連絡手順を確認しておく

イラスト：佛教大学漫画研究会

京都府警察本部サイバー犯罪対策課・Ksisnet

公衆無線LAN（Wi-Fi）の安全な利用について



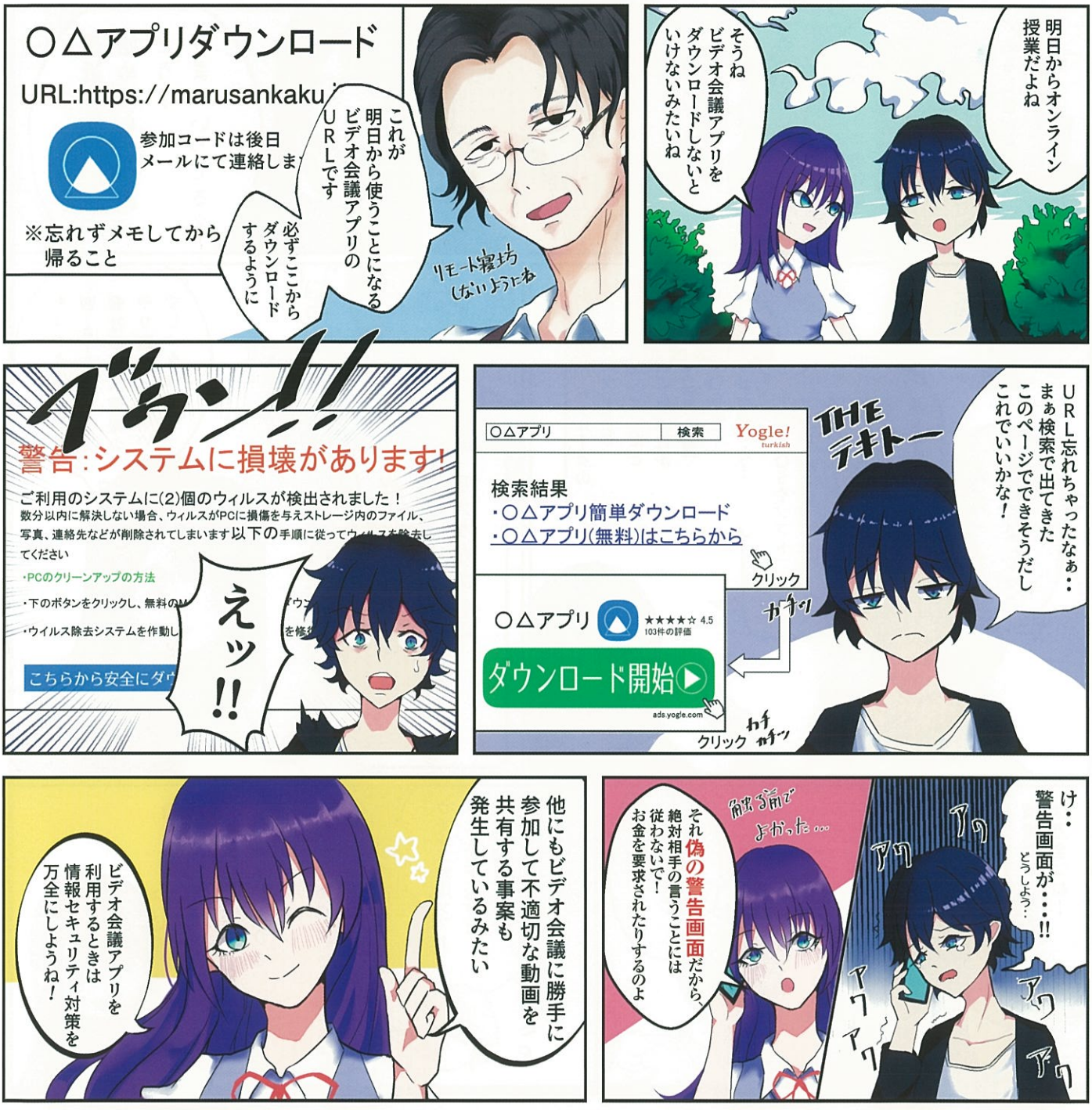
被害防止のポイント

- ○ 個人情報を含むアプリを使用したり、個人情報等の入力が必要なサイトにアクセスしない
- ○ ブラウザを使用する際は、HTTPS化されていないサイトの利用は避ける
- ○ 「偽アクセスポイント」に勝手に接続しないよう、Wi-Fiに自動接続する設定にはしない

イラスト：佛教大学漫画研究会

京都府警察本部サイバー犯罪対策課・Ksisnet

ビデオ会議アプリの安全な利用について！



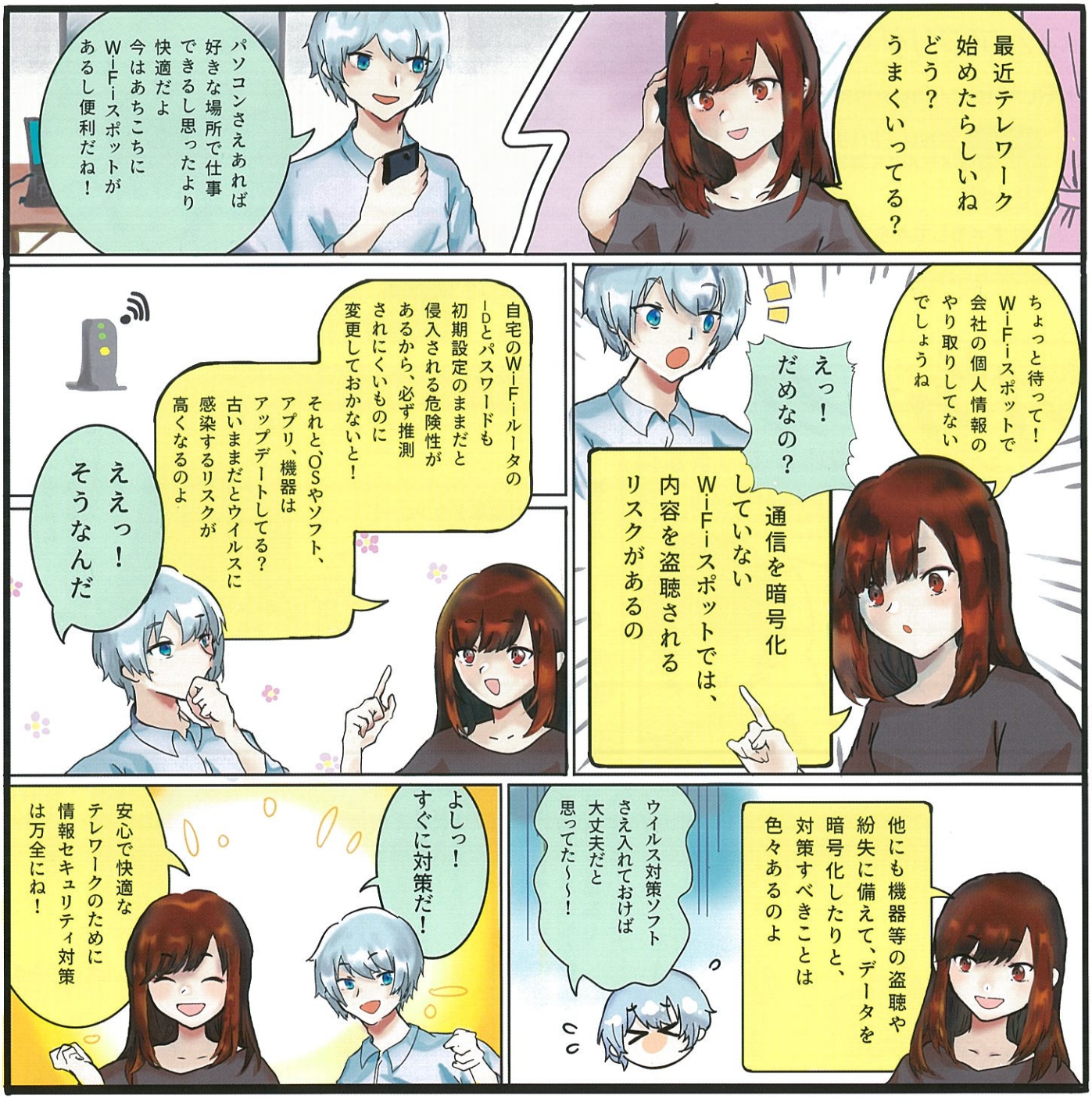
被害防止のポイント

- ○ 端末や機器は常に最新の状態にアップデートしておく
- ○ アプリは信頼できるサイトからダウンロードする
- ○ ダウンロードする際は、同名や類似名の偽アプリではないかを確認する
- ○ URLやパスワードはビデオ会議の参加者以外に教えない
- ○ 各アプリで提供されるセキュリティ設定を活用する

京都府警察本部サイバー犯罪対策課・Ksisnet

イラスト：佛教大学漫画研究会

テレワークのセキュリティ対策できていますか?



被害防止のポイント

- ○ Wi-Fiスポットは盗聴のリスクが高まることから、VPNを活用した通信の暗号化等を行う
- ○ 機器を乗っ取られる等のリスクが高まることから、自宅のWi-Fiルータの管理用ID・パスワードは初期設定のままにしておかない
- ○ 情報漏えい等のリスクに備えて、データの暗号化や複雑なパスワードの設定、多要素認証の利用等を行う

イラスト:佛教大学漫画研究会

京都府警察本部サイバー犯罪対策課・Ksisnet