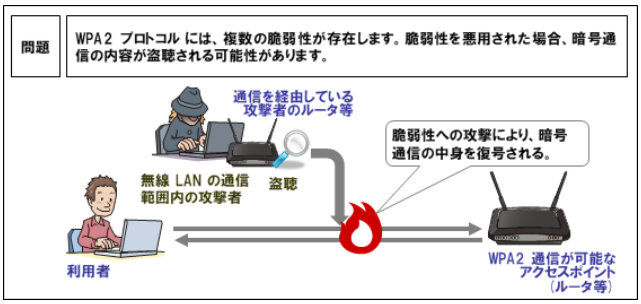
回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security News Letter Vol.29

あさまセキュリティニュースレター

安全性の高い無線LAN暗号化規格『WPA2』に複数の脆弱性が！！　(2017年10月19日)



現在最も安全性が高いとされ、ビジネスでも利用されている無線暗号化技術に複数の脆弱性が！
通信の盗聴が行われる可能性があり！！

ご利用の無線機器メーカーの情報をご確認、ソフトウェアのアップデートの適用を行うなどの対策を検討してください。

Windows （パソコン側）は、10月にMicrosoft 社より本脆弱性の修正プログラムを公開済み
無線機器側は、各メーカーファームウェアアップで対応するケースがほとんど。対象外のモデルもございますので、ご利用メーカーの最新の情報をご確認下さい！

暗号化規格の種類の比較

無線暗号化規格	なし	WEP	WPA / WPA2（今回の脆弱性）	
暗号化の種類	なし	WEP	TKIP	AES
暗号強度	×	×	△	◎
		容易に解読	危弱性あり	解読困難
特徴	盗聴されると誰でも通信内容がわかってしまう。鍵マークのないフリーWiFi、偽のフリーWifi等	無線LAN初期の暗号化規格で、現在は**数分で解読可能**。使用している場合、直ちに見直しを！	**脆弱性が発見されており**、時間をかければ解読される、**容易にシステムダウン可能**	**解読は困難**で、現在はこの方式が推奨されている

今回の脆弱性を悪用された場合のリスク

- パソコンの無線通信の傍受、盗み見
- 通信の乗っ取り、改ざん、不正利用
- 個人情報、企業情報、パスワードの漏えい等

※脆弱性の利用には、対象の無線に接続する必要があり。→　インターネット経由では今回の脆弱性を利用した攻撃はできない
通信の内容が暗号化されていれば傍受されていても内容を盗まれることはない　→　httpsサイトなど

被害

社内無線通信の盗聴・情報流出

盗んだ情報を元に不正アクセス、不正利用

対策

- ご利用中の無線機器の確認、メーカーホームページで最新の情報を確認
- 脆弱性の対象機種の場合、対策方法を確認し対策
- パソコン側の修正プログラムの適用
- SSIDが会社名、個人名の場合、どこの無線通信か特定されやすいため、見直す

情報源

IPA　https://www.ipa.go.jp/security/ciadr/vul/20171017_WPA2.html

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414