



## Q&A

### WPA2™

**1. Q: WPA2 は IEEE 規格に準拠していますか？**

A: はい、WPA2 は IEEE 802.11i 規格に準拠しています。

**2. Q: IEEE 802.11i と WPA2 はどのような関係にあるのですか？**

A: WPA2 について Wi-Fi 認定を受けている製品はすべて IEEE 802.11i 規格に準拠しており、本規格の必須要件をすべて満足しています。WPA2 は 802.11i の相互接続性を Wi-Fi アライアンスが具体化し、認定するものです。

**3. Q: Wi-Fi アライアンスが WPA2 に関する相互接続性認定試験の実施を開始するのはいつになりますか？**

A: 認定試験は 9 月 1 日開始されました。

**4. Q: WPA2 の Wi-Fi 認定製品はいつごろ入手可能になりますか？**

A: 2004 年 9 月になります。Wi-Fi アライアンスでは WPA2 の Wi-Fi 初回認定製品の発売を 9 月 1 日に発表いたしました。さらにその後数週間・数ヶ月中に多数の製品が WPA2 に対する Wi-Fi 認定を受けることになるでしょう。

**5. Q: WPA™ と WPA2 との類似点は何でしょうか？**

A: WPA ならびに WPA2 双方ともエンドユーザやネットワーク管理者にそのデータの守秘と認定ユーザのみのアクセスに対する高度な保障を提供するものです。

これら双方とも 802.1X を採用、また認証手続については拡張認証プロトコル ( EAP ) を採用しています。さらに両規格とも個人市場と企業市場における個別のニーズに対応するためにパーソナルモードとエンタープライズモードを装備しています。

**6. Q: WPA と WPA2 との相違点は何でしょうか？**

A: WPA2 では Advanced Encryption Standard ( AES ) によるさらに強力な暗号化機能を提供しており、この規格は企業や政府機関ユーザの一部では必須項目となっています。

**7. Q: WPA2 は WPA に対して下位互換性を維持していますか？**

A: はい、WPA2 について Wi-Fi 認定を受けた製品はすべて WPA について Wi-Fi 認定を受けた全製品と相互接続可能です。

**8. Q: WPA 製品を WPA2 にアップグレードすることは可能ですか？その場合何が必要になりますか？**

A: WPA 製品にはソフトウェアで WPA2 へのアップグレードが可能になるものもあります。しかしその他の製品では WPA2 に不可欠な AES 暗号化機能が膨大な演算作業を要求するため、ハードウェアに変更を加える必要が生じる可能性があります。

**9. Q: WPA2 は WEP との下位互換性を維持していますか？**

A: Wi-Fi アライアンスでは WEP をセキュリティの高いソリューションであると判断しておりません。セキュリティ上の理由から、WPA と同様に、WPA2 モードで動作中の製品が WEP デバイスを同時にサポートすることは出来ません。

しかし既存デバイスへの対応を考慮して、WEP は Wi-Fi 認定製品すべてについて基本的な相互接続試験の一部として維持されています。また将来的には Wi-Fi アライアンスが WEP を Wi-Fi 認定の要求事項から削除する可能性があります。

**10. Q: WPA2 では個人仕様と企業仕様を提供していますか？**

A: WPA と同様に WPA2 でも個人モードならびに企業モード双方で動作可能です。個人モードでは認証手続に Pre-shared Key ( 事前共有キー ) が使用されますが、企業モードにおける認証は 802.1X および EAP によって行われます。個人モードではアクセスポイントとクライアントデバイスがあれば良いのですが、企業モードではほとんどの場合ネットワーク上に RADIUS あるいはその他の認証用サーバが必要になります。

**11. Q: WPA2 の認証方法はどのようなものでしょうか？**

A: 企業モード WPA2 では IEEE 802.1X および EAP を利用して認証を行います。個人モードでは Pre-shared Key ( 事前共有キー ) またはパスワードで認証を行います。

**12. Q: WPA2 のデータ暗号化はどのように実行されますか？**

A: WPA2 のデータ暗号化は AES によるものです。しかし WPA では TKIP を利用しています。

**13. Q: WPA2 にはセッションキーはありますか？**

A: WPA と同様に WPA2 は通信を確立するたびに新規セッションキーを生成します。その利点はネットワーク上の各クライアントで使用される暗号化キーがその個人に対して固有で、特定されたものとなることです。要するに空中波で送られる各パケットはすべて固有キーによって暗号化されます。キーの再利用を避け、固有の新規暗号化キーを発行する機能は良質なセキュリティ処理の常套手段であり、これにより WPA ならびに WPA2 双方でこのような良質なセキュリティが提供できるのです。

**14. Q: WPA2 が登場したことで企業における Wi-Fi<sup>®</sup> ネットワークの採用は増加するのでしょうか？**

A: 政府機関や商用分野における Wi-Fi ネットワークの運用増加は WPA2 対応の Wi-Fi 認定製品の発売に連動していくであろうと期待しています。

**15. Q: WPA は今でも安全ですか？**

A: はい、WPA は今までどおり安全です。WPA は Wi-Fi セキュリティに対する重要なアップグレードであり、企業や一般ユーザ双方に対応できるものです。WPA は WEP における既知のあらゆる弱点を克服するものであることが公式に証明されています。WPA2 は WPA における弱点を是正するために導入されたものではないのです。

**16. Q: Wi-Fi アライアンスが WPA2 を導入する理由は何ですか？**

A: 企業ユーザには 802.11i に完全準拠した Wi-Fi 認定製品を必要とする企業もあります。また特定の政府機関では FIPS 140-2 の要求事項に対応可能なセキュリティソリューションを必要としており、WPA2 の AES がこれに対応できるからなのです。