http://www.uquest.co.jp/embedded/columns/lan2.html
http://blogs.yahoo.co.jp/bunomajikana/26579448.html

WEP

もともと IEEE802.11 で定義されているセキュリティとは、 以下の三つでした。

（1） ESSID
（2） MAC フィルタリング
（3） WEP64/128

（1）は単なる AP 接続とグルーピングが目的であり、（2）はステーションの MAC アドレスで AP への接続規制を行うわけですが、ステーションの MAC アドレスは偽造することも不可能ではありません。よってこれら（1）（2）は、厳密な意味でのセキュリティとは言えません。

（1）、（2）とは違い、（3）は実際に流れるデータを隠すという目的のために用意されており、AP とステーションで事前に共有鍵を設定しておく、という形をとります。しかしながら、WEP アルゴリズムは暗号学的には弱い部類に入る暗号なので、電波が届き、かつそのデータを傍受できる PC があれば、クラッキングツールを用いて容易に鍵の類推をすることができ、生データを見ることが可能になってしまいます。

WPA

IEEE802.11 という規格に対して、この普及を促進する業界団体 Wi-Fi アライアンス（発足当時の名称は WECA）は、無線 LAN 同士の相互接続の認証を行い、Wi-Fi というブランドを構築していました。IEEE802.11 だけのセキュリティの弱さを危惧した Wi-Fi は、WPA (Wi-Fi Protected Access) を 2002 年 10 月に発表しました。WPA は、認証を事前秘密鍵で行うか、RADIUS サーバーを使用するかで二つに別れ、前者は WPA-PSK、後者は WPA-1X(あるいは単に WPA) と呼ばれています。

WPA-PSK

WPA-PSK では、AP とステーションで共有するパスフレーズから、決められたアルゴリズムに従って 512bit のマスターキー（PMK と呼ばれる）を事前に生成しておきます。そして、AP- ステーション間の LINK 確立後、4Way-Handshake と呼ばれるプロトコルで乱数とお互いの MAC アドレスを交換し、それらとマスターキーを組み合わせて 512bit（但し、AES を使用する場合は 384 ビット）のテンポラリキー（PTK と呼ばれる）を生成します。このうち最初の 128bit は、PTK として両者が同じ物を持ったことを確認するために使用されます。次の 128bit は、この後行われる GroupKey-Handshake において、ブロードキャスト／マルチキャストの暗号鍵（GTK と呼ばれる）の暗号化に使われ、GTK は定期的に AP から配布されます。残りの 256bit（AES を使用する場合は 128bit）は、ユニキャストの暗号鍵として使用されます（図４）。

このように 4Way-Handshake、GroupKey-Handshake を使うことで、キーの変わらない WEP64/128 と違い、接続あるいは AP からの更新の度に鍵が変わるようにしてセキュリティの強度を上げています。

WPA 1X

共有マスターキーを認証の一部とする WPA-PSK とは違い、WPA-1X は認証として IEEE802.1X を使用します（図５）。IEEE802.1X とは RADIUS サーバーを使用して、いわゆる Credential（証明書）で認証を行う方式であり、このために、ステーションと AP 間で EAPoL（EAP over LAN）、AP と RADIUS サーバー間で RADIUS プロトコル（EAP が RADIUS プロトコルで Wrap される）が使用されます。

IEEE802.1X で決められている認証方式は EAP であれば、特に既定されていませんが、WPA での使用にあたっては、EAP-TLS、PEAP、EAP-TTLS など TLS をベースとしたものに限定されます。これは、IEEE802.1X が認証だけを規定しているのに対し、WPA はそれに加え、PTK 生成に必要なマスターキー（PMK）の生成を要求するためです。上記の方式では、その認証の過程において PMK が生成され、RADIUS サーバーは AP にその PMK を MPPE（Microsoft Point-to-Point Encryption）を使って転送します。そして、認証成功後、WPA-PSK と同様、4Way-Handshake、GroupKey-Handshake が行われます。

EAP-TLS、PEAP、EAP-TTLS はセキュアなトンネルを生成するところは共通しますが、細かいところで違いがあるため、以下にその違いを要約します。

方式	内容	ステーションへの負荷
EAP-TLS	お互いの認証を X.509 証明書で行う	大
PEAP	X.509 証明書による認証はサーバーのみ。ステーションの認証はセキュアトンネル内でさらに EAP による認証を行う	中
EAP-TTLS	X.509 証明書による認証はサーバーのみ。セキュアトンネル内で AVP(Attribute-Value Pair) 形式による認証を行う	小

上記以外にも、Cisco が提唱する EAP-FAST や携帯電話での認証を応用した EAP-SIM などが次世代の認証方式として期待されていますが、まだ一般的には使用されておらず、WPA-1X はもっぱらビジネスユースで PEAP、EAP-TTLS で使用されているのが実情のようです。

WPA2

そもそも IEEE802.11 のセキュリティは、IEEE802.11i での標準化作業が進んでいたものの、無線 LAN が世の中に急速に広まったおかげで、セキュリティ対策が必要になったために Wi-Fi アライアンスから急遽出されたという背景が WPA にはあり、セキュリティ的に十分ではないと考えられていました。そんな中、2004 年 6 月にようやく IEEE802.11i の標準化作業がおわり、これを反映した WPA2 が制定されました。WPA 自身は Wi-Fi アライアンス内でしか開示されていませんが、以下に述べる部分を含む基本的な部分は IEEE802.11i として公開されているものと同じですので、以下については、IEEE802.11i の規格として説明します。

WPA2（IEEE802.11i）は、プロトコルで使用されるフレームフォーマットが細かいところで違うものの基本的には WPA と同じです。WPA との大きな違いを挙げれば以下のようになります。

（1）AES を標準とする。（TKIP はオプション）
（2）事前認証が行える。
（3）PMK キャッシュが行える。

このうちの（2）と（3)、接続する AP が変わる毎に認証が必要になり利便性が悪くなるという、WPA-1X が本来持っていた問題を解決する機能です。「事前認証」とは、現在接続中以外の AP に対して、今接続中の AP を経由して IEEE802.1X 認証を行うものです（図６）。これにより、ローミングなどで接続する AP が変わっても、事前認証が済んでいる AP に接続することで認証処理を省略することが可能になり、通信の回復がすばやく行えるようになります。

「PMK キャッシュ」とは、一度認証に成功し接続可能となった AP との間で共有している PMK を AP がキャッシュしておくことにより、先の「事前認証」と同様、ローミングなどで接続する AP が変わっても認証処理を省略することが可能になり、同様の効果が得られます（図７）。