Soliton White Paper 2015

MAC アドレス制限は “効果ゼロ”

～NetAttest EPS で見直す企業無線 LAN のセキュリティ～

株式会社 ソリトンシステムズ

SMKT1510-A

目次

第 1 章　MAC アドレス制限は “効果ゼロ”

スマートフォンやクラウドの進展により、企業の無線 LAN 環境のセキュリティ対策が急務になりつつある。特に、危惧されるのは、MAC アドレスフィルタリングや PSK 認証といった穴の多い技術を使い続けることのリスクだ。本当に必要とされる無線 LAN セキュリティ対策は何か。ソリトンシステムズが提供する認証サーバアプライアンス「NetAttest EPS」の機能を紹介しながら、求められる無線 LAN セキュリティの姿を提案したい。

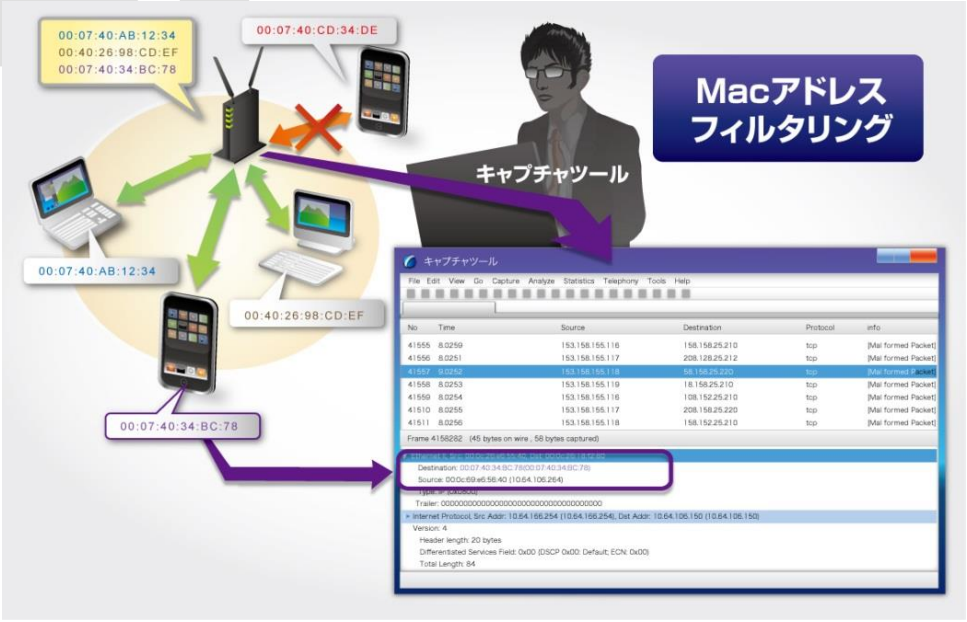
本当は怖い MAC アドレスフィルタリング

ネットワーク機器に割り当てられた MAC アドレスを使ってネットワークへのアクセス制限を行う MAC アドレスフィルタリング。家庭用ルーターなどでは無線 LAN セキュリティの 1 つの機能のように扱われ、ときには「MAC アドレス認証」といった認証方式の 1 つのような言い方をされることもある。このため、「完全ではないものの一定の効果は期待できるセキュリティ機能」などと理解している方も多いのではないだろうか。

しかし、MAC アドレスフィルタリングは、昨今の企業を対象にしたサイバー攻撃に対して、セキュリティ上、ほとんどなんの意味も持たないことがわかっている。「効果は限定的」「無いよりはまし」といったレベルではなく、場合によっては「MAC アドレスフィルタリングを設定して安心している」ことが、セキュリティ管理の甘いネットワークであることを攻撃者に対して通知する機会を与えることにもつながっている。

MAC アドレスフィルタリングが"危ない"理由の 1 つは、なりすましが容易いことだ。MAC アドレスはネットワーク上で暗号化されないため、無線 LAN のパケットをキャプチャすれば外部から丸見えだ。MAC アドレスを変更できるツールはインターネットで配布されており簡単に入手できる。つまり、悪意を持った攻撃者は、それらツールを使って MAC アドレスを偽装するだけで、あっさりと、かいくぐることができるのだ。

図 1　ネットワーク上で暗号化されていない MAC アドレス



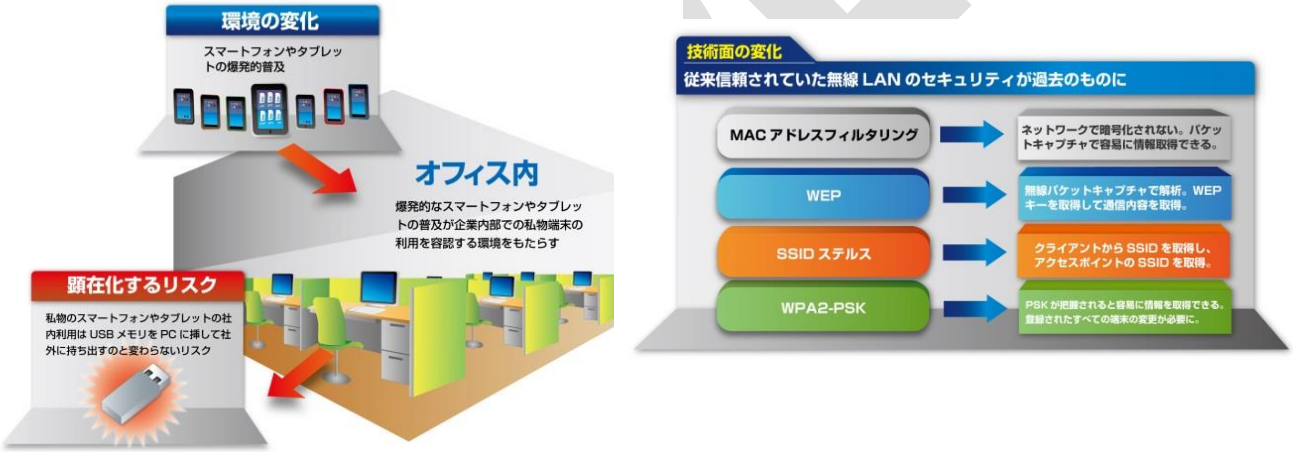
もちろん、かいくぐった後は暗号化通信の解読などが必要だ。ただ、MAC アドレスフィルタリングを「セキュリティ対策の一環」として実施し安心している企業であるなら、その他のセキュリティ対策も不十分であることが予想できる。攻撃者はその隙をついて、WEP などの簡単に解読できる暗号方式を使っていないか、簡単なパスワードを使いまわしていないかを調べていくわけだ。

昨今の標的型サイバー攻撃を見ればわかるように、攻撃者の手法は巧妙化の一途をたどるばかりだ。いまこそ、攻撃者を利する対策ではなく、企業無線 LAN について、本当に効果のあるセキュリティ対策を実施すべきだ。

遅れが目立つ無線 LAN セキュリティ対策

本来望まれる企業無線 LAN のセキュリティ対策とはどのようなものだろうか。現在の企業無線 LAN について、取り巻く環境の変化、リスク、必要な対策などの点から振り返ってみよう。

図 2　現在の企業無線 LAN における、環境と技術面の変化



環境の変化としては、スマートフォンやタブレットの急速な普及が大きい。私物 PC の持ち込みや USB メモリへのコピーなども長らく危険性は指摘されながらも、ようやく禁止する企業が増えてきた。しかし、私物スマートフォンを社内で使うことに対してはまったく配慮されていない現状がある。USB メモリを会社 PC に挿すことを諫める人は居ても、私物スマートフォンの利用に注意を払う人はほとんどいない。情報漏洩のリスクという点では同じであるにも関わらず社内制度やポリシーが追いついていないのだ。

同様に技術面でのリスクも大きく変化している。MAC アドレスフィルタリングや WEP 暗号化や、SSID ステルス化（SSID Broadcast OFF、ANY 接続拒否）、WPA2-PSK による通信。従来は代表的な無線 LAN のセキュリティ対策に挙げられていたものだが、現在では十分なセキュリティが確保できない。WEP はもはや論外として SSID ステルス化も、無線クライアントからは SSID 情報を誰でも取得することができる。

一般に、より強固だと思われている WPA2-PSK にも"罠"がある。PSK（プレシェアード