無線 LAN ステルスモードの安全性

2010　　川島　哲也

1　はじめに

近年、技術の大幅な進歩に伴い、インターネット接続は有線 LAN 通信から無線 LAN 通信に変わり、パソコン端末も手のひらサイズまでに小型化し、どこでもインターネットが利用できる時代となっている。無線 LAN 通信は電波に情報を乗せてインターネットに接続しているため、有線 LAN 通信と比べてセキュリティ面では不安がある。今の段階で無線 LAN 通信のセキュリティ対策は複数あり、それらを組み合わせて安全なインターネット接続を実現している。無線 LAN セキュリティ対策にはデータの暗号化、ステルスモード、MAC アドレスのフィルタリング、IEEE802.1X 認証などがある [3]。

無線 LAN セキュリティ対策の一つであるステルスモードとは AP（基地局の役割をするアクセスポイント）が発信している識別子である SSID を隠蔽することである。ステルスモードの目的は意図していない他者からの不正接続をさせないことである。しかし、ステルスモードには通信中に SSID を発信してしまう問題点が知られている [3]。

このように意図した安全性が確保されていないので、ステルスモードは知られていること以外にも安全性に問題点があるかも知れない。そこで、本論文では無線 LAN ステルスモードの安全性を研究し、ステルスモードを行うことによって生じるセキュリティ上の問題点を議論する。

2　ステルスモード

本研究の対象となるステルスモードについて述べる。ステルスモードとは無線ＬＡＮ通信における、AP が発信している SSID を隠蔽するセキュリティ対策の一つである。

2.1　SSID

SSID とは AP に対して一連のビットを割り当てるものである。この一連のビットは人間が読むことのできる文字列として割り当てられているため、SSID を AP のネットワーク名として利用している。

2.2　ステルスモード

ステルスモードとは AP が発信している SSID を隠ぺいする無線ＬＡＮセキュリティ対策の一つである。後で説明するアクティブスキャンではステーションから AP の SSID を知る必要があるため、SSID を知らないステーションはアクティブスキャンで AP を探さなければいけない。ステルスモードの目的は任意の相手からの不正接続を防ぐことである。ステルスモードにも 2 種類存在し、ビーコンフレーム（SSID など無線通信に必要な情報が含まれている配達箱のようなもの) は発信するが SSID が含まれていない場合とビーコンンフレーム自体が発信されない場合の 2 種類が存在する。

3　AP の発見方法

無線 LAN ネットワークにおいて AP を探すことをスキャンという。スキャンにはパッシブスキャンとアクティブスキャンの 2 種類存在する。そこで本節ではこの 2 種類を説明する。また、ステルスモードではアクティブスキャンが行われるので、AP がステルスモードの場合のアクティブスキャンについて説明する。

3.1　パッシブスキャン

パッシブスキャンとは AP が一方的にビーコンフレーム発信し、ステーションが受信した複数のビーコンフレームの中から意図するものを選び AP を探す方法。箇条書きにてパッシブスキャンの流れを述べる。

1. AP はビーコンフレームを発信し続けている
2. ステーションは発信し続けているビーコンフレームを受信する。
3. ステーションは AP からプローブ応答が送られてきたら、認証（ステーションが正当であるか確認すること)、アソシエーション (ステーションがネットワークへ加入する手続き) など接続に必要な手順を踏む。
4. 上記の手順が全て終わって、ステーションはインターネット接続ができるようになる [2]。

3.2　アクティブスキャン

アクティブスキャンはパッシブスキャンと違いビーコンフレームを受信するのを待つのではなく、ステーション自身が積極的なふるまいを行い AP をスキャンをする。AP のふるまいはスキャン同様ビーコンフレームを発信し続けている。箇条書きにアクティブスキャン（ビーコンを発信している）の流れを述べる。

3.2.1　通常モード（AP が SSID を含むビーコンフレームを発信している場合）

1. AP はビーコンフレームを発信し続けている。
2. ステーションは AP にプローブ要求（ステーションが AP を探す場合に使われるもの。SSID などが含まれている。) をする。
3. AP は送られてきたプローブ要求の中に含まれている SSID が一致するなら、ステーションにプローブ

応答 (AP がステーションから送られてきた SSID が一致した場合に返事するもの) する。SSID が一致しなければ無視する。

4. ステーションは AP からプローブ応答が送られてきたら、認証、アソシエーションなど接続に必要な手順を踏む。
5. 上記の手順が全て終わって、ステーションはインターネット接続ができるようになる [2]。

3.2.2 ステルスモード 1（AP はビーコンを発信しているが SSID が含まれていない場合）

1. AP はビーコンフレームを発信し続けているが SSID が含まれていない。
2. 以降は通常モードと同じ。

3.2.3 ステルスモード 2（AP はビーコンを発信していない場合)

1. AP はビーコンフレームを発信していない。
2. 以降は通常モードと同じ。

4 実験

本実験の目的は机上で調査したスキャン方法はステーションと AP のやり取りが正しいことを確認することである。また、AP が存在しない場合にステーションがどのようにふるまうかを観察し、安全性を確認した。

本実験ではデータキャプチャソフト WireShark を使用しステーションと AP の接続フローを観察した。実験内容として机上で調査したパッシブスキャン、アクティブスキャン、ステルスモード 1、ステルスモード 2 の各々のステーションと AP のやり取りを確認した。また、本実験では机上で調査したスキャン方法以外に、AP が存在しない場合のアクティブスキャンでのステーションのふるまいも観察した。

4.1 実験器具

実験で使用した器具を以下に示す。

- 無線 LAN 接続可能な PC
- 無線 LAN アクセスポイント 2 台
- Wireshark
- Buck Truck(セキュリティ機能が詰まった Linux OS)
- airmon(無線 LAN デバイスをモニターモードにするソフト）

4.2 実験結果

パッシブスキャンの場合、AP がビーコンフレームを発信し続けていて、ステーションは受信したビーコンフレームから AP をスキャンしていた。ステーション自身ふるまいを起こして AP をスキャンすることはなかった。スキャン後、ステーションと AP のやり取りを行い無線 LAN 接続を可能にしていた。

アクティブスキャンはステーションが AP から発信しているビーコンフレームの受信を待つのではなく、ステーション自身がプローブ要求を発信し AP を探していた。AP は受信したプローブ要求の SSID が一致していたので、ステーションに SSID を含むプローブ応答を送信していた。ステーションが AP にプローブ要求する間隔は約 1 秒であった。その後、ステーションと AP のやり取りを行い無線 LAN 接続を可能にしていた。ステルスモード 1 は AP はビーコンフレームを発信していたが SSID は含まれていない為、ステーション自身がプローブ要求を発信し AP を探していた。以降はアクティブスキャンと同じであった。ステルスモード 2 は AP がビーコンフレームを発信していないので、ステーション自身がプローブ要求を発信し AP を探していた。以降はアクティブスキャンと同じであった。

AP が存在していない場合、アクティブスキャンのステーションはプローブ要求を発信し続けていた。

5 考察

ステルスモードに対して知られている通信中にステーションが SSID を発信してしまう問題点は実験を通じて確認することができた。

また、実験結果から、AP が無い場合においてステーションはプローブ要求を発信し続けていることが確認できた。したがって、ステルスモード設定の AP 情報を保有しているステーションは、無線スイッチを on にしていると保有している AP に接続を行こうとするため、その AP の SSID を発信してしまうことが明らかになった。攻撃者はこの情報をデータキャプチャすることによって、ステーションの保有するステルスモードの AP の SSID を手に入れることができるだけではなく、その SSID の AP になりすましてステーションとの接続を試みることが可能になる。以上のことからステルスモードには脆弱性が存在する。したがってステルスモードを使用する場合、IEEE802.1x 認証（無線 LAN におけるユーザー認証の規格）などのセキュリティ対策を併用する必要がある [3]。

参考文献

[1] IEEE Computer Society, IEEE Standard for Information technology— Telecommunications and information exchange between systems Local and metropolitan area networks— Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE (2012)

[2] Mattbew Gast , 渡辺　尚, 小野　良司, 林　秀幸, 802.11 無線ネットワーク管理, オライリー・ジャパン (2006)

[3] 手塚悟, 佐々木　良一, 情報セキュリティの基礎, 共立出版 (2011)