中小企業向けシスコ製品の特徴について

Nov 14, 2008

【ワイヤレス編】

Cisco AP1131AG, AP521AG
vs
Buffalo

※本資料は、シスコ製品を販売する営業担当者向けの参考資料として作成したものです。
※本資料の内容は、公開されている情報および弊社が実施した検証テストの結果に基づく、弊社独自の見解を示しています。

合同会社ティー・エヌ・シー・ブレインズ

目次

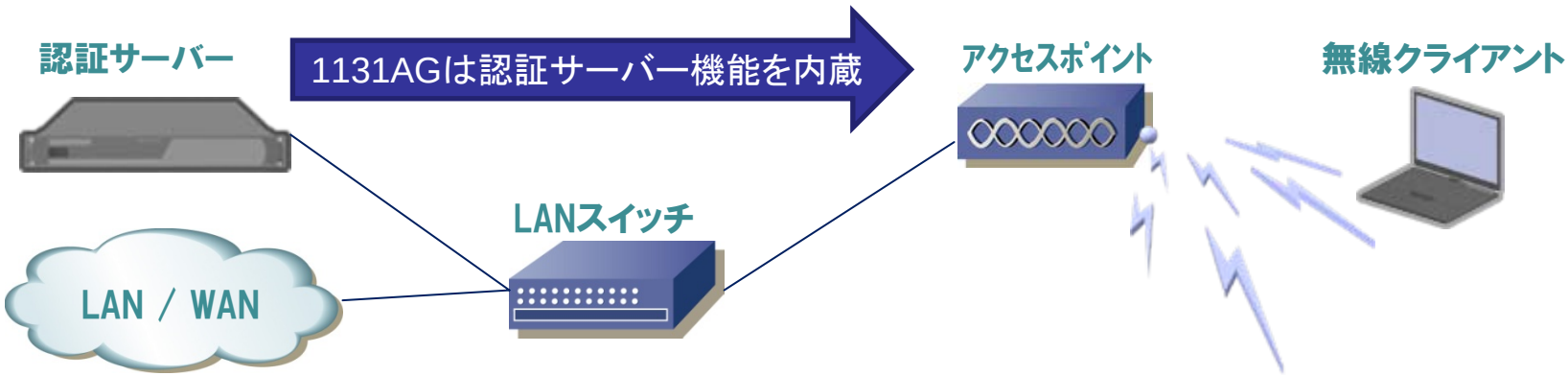
高セキュリティと低コストの両立！

予算が無尽蔵にあれば強固なセキュリティを構築することが可能です。しかし、小規模な拠点やIT管理者が不在の企業にまで、認証サーバーを使った本格的なシステム構築を求めるのは非現実的です。

また、WEPに脆弱性があることは周知の事実ですが、「WPAなら大丈夫」と思っていませんか？WPAでも、事前共有鍵を使用するWPA-PSKでは、キー解析および不正アクセスが可能です。

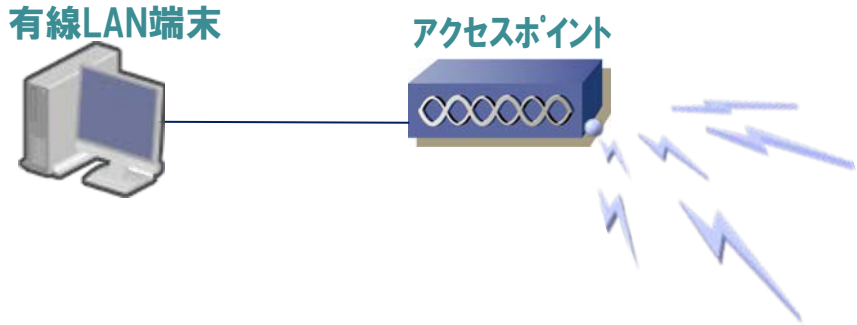
“外部の認証サーバーを使用しない”という条件で、インターネット上で容易に入手可能なハッキングツールを用いた不正侵入テストを行った結果、認証サーバー機能を搭載するCisco1131AGは不正アクセスを防止できることが確認されました。

●無線LANの認証システム



高セキュリティと低コストの両立！

●テスト構成



※有線LAN端末と正規の無線クライアント間の
通信データをキャプチャし、キー解析を行う

●テスト結果

	Buffalo	Cisco AP1131AG
セキュリティ手段	WPA2-PSK	WPA2-EAP-FAST
テスト結果	**容易に不正アクセスが可能** （ツールのマニュアル通りの操作で簡単にキー解析が可能だった）	**不正アクセス不可能** （現在のコンピュータ科学においてキーの解析が現実的に不可能）

コラム：WPA-PSKの脆弱性について

- WPA-PSKでは認証の際のハンドシェークを傍受して解析することにより、パスフレーズ（認証キー）を特定可能であることが知られています。
  http://wifinetnews.com/archives/002452.html
- この原理を利用したパスフレーズの解析ツールが出回っており、誰でもインターネットからダウンロードして使用することが可能です。
- 一旦ハンドシェークをキャプチャできれば、あとはオフラインで時間をかけて解析できるため、WEPの脆弱性以上にリスクが大きいとする意見もあります。
- 今回使用したツールではパスフレーズを21文字以上に設定すれば解析できませんでしたが、これはツールの仕様であり、原理的に不可能という事ではありません。
- WPA-PSKを安全に運用するためのガイドラインとしては、共有キーに可能な限り長くランダムな文字列を使用するとともに、定期的にキーを設定し直すことを推奨します。しかし、現実的に中小規模の企業でそのような運用をすることは難しいと思われます。

補足：1131AGのEAP-FAST認証

- 1台のAPで50ユーザーまで認証可能
- 5認証／秒の性能
- 想定する用途
  - ✓APが1台しか必要のない場合
  - ✓WAN超えでRadius serverにアクセスする構成でのバックアップ
- 認証手段
  - ✓ユーザー認証：Windowsへログインする際のID/Password
  - ✓マシン認証：端末のMACアドレス（IP/Passwordとの併用可能）
- パスワードを推測して何度もアクセスを試みるユーザーを拒否する設定も可能
- EAP-FASTに対応するサプリカント
  - ✓Cisco Secure Services Client（CSSC）
  - ✓DELL WLANユーティリティ
  - ✓Intel PROSet/Wireless
  - etc
- 設定方法（参考URL）
  - ✓EAP-FASTについて
  - http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/wr/airo1k/eapfast/chapter01/eapfast.shtml
  - ✓APを認証サーバーとして使用する方法
  - http://www.cisco.com/en/US/docs/wireless/access_point/12.3_4_JA/configuration/guide/s34local.html

発見されにくいAP

- 無線LANでは、APが定期的に発信するビーコン信号にSSIDと呼ばれる文字列を含めることにより、APを容易に識別できる仕組みがあります
- 公衆サービスや一般家庭で利用する場合、この仕組みによってユーザーは簡単に無線LANに接続できるようになります
- しかし、企業利用の場合には限られたメンバーのみが接続できればよいため、ビーコン信号にSSIDを含める必要はありません
- 不用意にSSIDを配信することはセキュリティの低下をまねき、不正アクセスによる情報漏えいや犯罪目的の踏み台にされる恐れがあります（このような意図で無防備なAPを探す行為は“ウォードライビング”と呼ばれています）
- シスコのAPはデフォルト設定でもSSIDを配信せず、ウォードライバーから発見されにくい状態になっています
- これは、シスコの無線LAN製品が企業利用を前提とした設計思想で開発されていることを示す一例です

集中管理型のメリット

※シスコのワイヤレスLAN製品は、分散型と集中管理型の2つの動作モードをサポートしています。
ここでは、集中管理型のメリットを整理します。

集中管理のメリット－１（サービスを止めない）

単一フロアに複数のAPを設置している企業において、APのうち１台が故障してしまった。

通常のWLAN	シスコ集中管理型WLAN
① 故障APの近辺ではWLANが利用できなくなる ② メーカーから代替用APが届くまで待つ ③ 代替APを設置し、再度設定を行う（専門知識が必要なので保守費を支払ってインテグレータのSEを呼ぶ） ④ 復旧	① コントローラが自動的に近隣APの電波出力を最大化し、故障APのエリアをカバーする ② メーカーから代替APが届く ③ APを交換し、LANケーブルを接続する（設定情報はコントローラから自動的にダウンロード） ④ 復旧
利用停止期間 １週間程度	利用停止なし

集中管理型のメリット

集中管理のメリット－2（無駄な電波を出さない）

新規に無線LANを構築することになり、単一フロアに複数のAPを設置した。

通常のWLAN	シスコ集中管理型WLAN
APの電波強度は調整せず、工場出荷時の設定（最強）をそのまま使用する **電波の飛ばしすぎ** **✓セキュリティリスク増大** **✓電波干渉の可能性大**	RRM (Radio Resource Management) 機能により、各APの電波強度やチャネルを自動的に調整。 オフィスレイアウトの変更や近隣企業の無線LAN導入などにより電波環境が変化しても、動的な調整が行われる。
または、 専門業者に依頼して、無線アナライザを利用した電波強度の調整を行った **電波環境が変化するたびに調整が必要**	

集中管理型のメリット

集中管理のメリット－3（APの負荷分散）

従業員の生産性向上のためオフィスレイアウトを見直し、複数のミーティングルームを同じエリアに集約した。

通常のWLAN	シスコ集中管理型WLAN
ミーティングルームにノートPCを持った多数の社員が集中すると、無線LANのアクセス速度が著しく低下する。何人かは無線LANに接続できない。 **特定の無線APに多数のクライアントが接続しようとするため、過度な負荷がかかっている**	ロードバランシング機能によって、特定のAPに負荷が集中しないよう、自動的に調整される。 無線LAN端末がAPに接続する際に、複数のAPから応答するよう、コントローラによって管理される。

集中管理型のメリット

集中管理のメリット－4（ゲストアクセス）

社内で不定期にセミナーを開催しており、来客者へのサービス向上のため、無線LANによるインターネットアクセスを提供したい。

通常のWLAN	シスコ集中管理型WLAN
SSIDとVLANのマッピング機能を利用して、ゲスト用のSSIDで無線LANに接続すると、インターネットのみへアクセス可能なVLANに収容されるよう、無線APの設定を行った。 **SSIDが解れば誰でもアクセス可能** **✓犯罪に悪用される恐れ** **✓不正利用によるトラフィック増加**	コントローラに内蔵されたWEBポータル機能で、ゲスト用の一時アカウントを簡単に発行できる。 ゲストは、ポータル画面からID、パスワードを入力することで、ネットワークにアクセスできる。 ゲストアカウントは決められた期限が過ぎれば、使用できなくなる。

集中管理型のメリット

集中管理のメリット－5（不正なAPへの対策）

ある地方拠点において、同じビルのフロアを利用している他の企業がセキュリティ設定をせずに無線LANを使用しており、自社の従業員が間違って他社の無線LANに接続してしまうトラブルが発生した。今回は先方の企業がセキュリティ設定を行ったことで解決したが、社長から、これを機に定期的に全拠点で無線環境をチェックして同様のトラブルが再発しないよう対策を指示された。

通常のWLAN	シスコ集中管理型WLAN
無線アナライザを使用して全ての無線機器を把握する。 自社の設備以外でセキュリティ設定のなされていないAPを発見した場合には、近隣のオフィスに連絡して所有者を探し、セキュリティ設定を依頼する。 ✓膨大な手間がかかる ✓所有者が判明するとは限らない ✓企業スパイによって故意に設置される不正APを即時に発見できない	無線LAN管理システム（WCS）によって、自社の管理外の無線機器の存在を常にチェックできる。 無線の信号強度から機器の位置を特定し、自社オフィススペースの内部に存在するものかどうかを判断できる。 発見された無線機器のMACアドレスとIPアドレスにより、自社のLANに接続されている機器かどうかを判断できる。 不正APに自社のクライアントが接続しないよう、妨害信号を送信できる。

無線LANのトラフィック制御

- 電波は目に見えないものであり、オフィスの壁を突き抜けて外部へ漏洩します。従って、どのようなセキュリティ技術を利用した場合でも、有線LANと比較して相対的にリスクの高い通信方法であると言わざるを得ません。
- 機密性の高い情報を扱う企業においては、無線LANを通じてアクセスするクライアントと有線LANのクライアントとを識別し、アクセス可能なサーバーやデータベースを制限することも有効な対策と考えられます。
- 無線LANのアクセスポイント（AP）は、OSIの7レイヤーモデルに当てはめるとレイヤ2に相当しますが、**シスコの無線APはレイヤ3以上の情報（下記）に基づいたアクセスリストを設定し、トラフィックを制御することが可能**です。
  - 宛先／送信元のIPアドレス
  - プロトコル種別
  - TCP/UDPのポート番号
- これによって、同じパソコンでも無線LAN経由でアクセスする場合には接続できるサーバーなどを制限する、といったことが出来ます。

Cisco WLANの優位点（まとめ）

- **AP1131AG: セキュリティとコストを高い次元でバランス**
  - ✓ セキュリティはネットワークの規模や予算の大小に関係なく必須。認証サーバーを使用しなくても鉄壁の守りが出来るのはシスコだけです！
  - ✓ 例えば、デフォルト設定でもSSIDをブロードキャストしないなど、Ciscoの無線LAN製品は企業利用を前提として設計されており、一般ユーザー向け市場に軸足を置いたBuffalo製品とは設計思想が違います
  - ✓ レイヤ3以上の情報に基づくトラフィック制御が可能
- **AP521G（LAP521G）: この価格帯で集中管理型のアーキテクチャが利用できるのはシスコだけ！**

- **その他の優位点**
  - **オフィスの美観を高めるスマートなデザイン**（アンテナ内蔵）
  - 無線のESSIDと有線のVLANをマッピング
    - ✓ 例えば、ゲスト用のSSIDで接続すると社員用とは別のVLANに収容する、といったことが可能です
    - ✓ WLAH-G54には、この機能がありません

Cisco 1131AG vs Buffalo WAPM-HP-AM54G54（スペック比較）

機能	Cisco **AIR-AP1131AG-P-K-9**	Buffalo **WAPM-HP-AM54G54**
ネットワーク規格	IEEE802.11 a/b/g	IEEE802.11 a/b/g
アップリンク	10/100 Base-T イーサネット	10/100 Base-T イーサネット
セキュリティ	802.1X/各種のEAP をサポート(EAP-FAST, EAP-TLS, TTLS, PEAP-MSCHAPv2) MAC アドレス登録	802.1X/各種のEAP をサポート(EAP-TLS, TTLS, MS-CHAP) MAC アドレス登録
暗号化	128/40 bit WEP, TKIP, AES	128/64bit WEP, TKIP, AES
重量	0.67kg	1,33kg
環境仕様	温度 0~40℃	温度 0~45℃
	湿度 10-99%	湿度 10-99%
消費電力	12.2W	9.5W
電源	100-240VAC, 50/60hz	AC100V 50/60hz
寸法(高x幅 x 奥行) cm	19.1 x 19.1 x 3.3	4.3 x 20 x 4.1
価格	80,000（市場想定価格*）	88,000（定価）

*市場想定価格 : シスコ製品には定価の設定がないため、シスコパートナーが提示している定価の一例を示します。

Cisco 521G vs Buffalo WLAH-G54（スペック比較）

機能	Cisco **AIR-AP521G-P-K9**	Buffalo **WLAH-G54**
ネットワーク規格	IEEE802.11 b/g	IEEE802.11 b/g
アップリンク	10/100 Base-T イーサネット	10/100 Base-T イーサネット
セキュリティ	802.1X/各種のEAP をサポート(EAP-FAST, EAP-TLS, TTLS, PEAP-MSCHAPv2) MAC アドレス登録	802.1X/各種のEAP をサポート(EAP-TLS, TTLS, MS-CHAP) MAC アドレス登録
暗号化	128/40 bit WEP, TKIP, AES	128/64bit WEP, TKIP, AES
重量	0.67kg	748g
環境仕様	温度 0~40℃	温度 0~40℃
	湿度 10-99%	湿度 10-85%
消費電力	12.2W	6W
電源	100-240VAC, 50/60hz	AC100V 50/60hz
寸法(高x幅 x 奥行) cm	19.1 x 19.1 x 3.3	13.5 x 18 x 3
価格	60,000（市場想定価格*）	36,800（定価）

*市場想定価格 : シスコ製品には定価の設定がないため、シスコパートナーが提示している定価の一例を示します。


tnc
T.N.C.Brains
TRAINING & CONSULTING