



4984 El Camino Real, Ste 200
Los Altos, CA 94022
Phone: 650-969-7884
Fax: 650-969-2783
www.sutisoft.com

SECURED BioNet :

指紋による無線 LAN へのアクセス制御





目次

目次	2
概要：	3
<u>WiFi LAN での安全に関する懸念</u>	<u>3</u>
<u>WiFi の脆弱性について：</u>	<u>4</u>
<u>WiFi LAN s における安全性の解決策について：</u>	<u>4</u>
安全性におけるバイオメトリックスの利点について	5
<u>SECURED BioNet™：指紋ベースによる Wi-Fi LAN の安全保障</u>	<u>5</u>
強固なセキュリティー	7
Plug - and - Play デザイン	7
ハッカーフリーデバイス	7
<u>SECURED BioNet 設計仕様</u>	<u>7</u>
<u>SECURED BioNet:容易な導入</u>	<u>8</u>
<u>SECURED BioNet と他の方法との比較</u>	<u>8</u>
総 論	9



概要：

近年、WiFi ローカルエリアネットワーク（WLANs）の利用が急速に増えています。その理由として、WiFi によりもたらされた大きな利便性と、コスト削減があげられます。その一方で、安全性に関して深刻な懸念が生じています。その内の一つの懸念としては、企業資産の不正利用を目的とした、企業のネットワークへの侵入が、比較的容易であることがあげられます。多くの会社は、このような危険性を承知のうえで、無線ネットワークを使いつづけるか、もしくはその安全性が確保されるまで、その利用を断念しているかのどちらかです。

バイオメトリクスは、情報システムにおける安全性の問題の解決に役立つものとして、魅力あるものになってきています。バイオメトリック技術は、ユーザーの物理的あるいは生態上の特徴、すなわち指紋、顔の特徴、声のパターンによって、ユーザーの身元確認（ユーザー認定）を可能としました。幾つかのバイオメトリック技術の中で、指紋の利用は、最も一般的なものとなってきています。指紋技術は、利用者の識別及び確認用に使用するには、コストも安く、確実に便利な技術です。

SECURED BioNet™は、会社内の WLAN への最初のコンタクトポイント-WiFi アクセスポイントにおいて、指紋ベースのアクセス制御を可能としています。WiFi の最新の安全規格と生態認証技術を結び付けることにより、SECURED BioNet は企業内ネットワークに対し、大変に強固なアクセス制御をもたらしました。ユーザーが WLAN に接続しようとする場合は、そのユーザーの指紋が SECUREDBioNet により認証されなければなりません。

SECURED BioNet は、Wireless Protected Access (WPA) に準じた暗号化機能を持つアクセスポイントとの組み合わせで稼動する、DSP ベースのネットワーク認証デバイスです。全体の認証プロセスを高速に処理するために、データ保存用のストレージ、プロセッサ、そしてメモリーを備えています。全ての利用者の指紋データとアクセスログは、SECURED BioNet デバイス内に保管されています。SECURED BioNet は、クライアント(無線アクセスポイント)と通信を安全に行ないます。

WiFi LAN での安全に関する懸念

WiFi(あるいは Wi-Fi)は、Wireless Fidelity の略語ですが、IEEE802.11 ファミリー標準に準じた技術を採用しています。“WiFi”の用語は、無線機器や技術をテストして、“Wi-Fi Certified”として認定している Wi-Fi アライアンスによって提唱されたものです。Wi-Fi 認定製品は、例え異なるメーカーから発売されていても、互いに置き換え可能であることが期待されています。IEEE802.11 はローカルエリアネットワークでの無線接続の仕様であり、IEEE802.11a, 802.11b, および 802.11g を含めて一連の標準をカバーしています。

WLAN 技術の利点により、WiFi は企業、ホーム、軍隊、各種のモバイルユースを含めて、多くの異なる市場で一般的になってきています。

その成功の一方で、WLANs の安全性には深刻な問題があります。以下に WiFi の安全上の脆弱性について述べます。

WiFi の脆弱性について :

有線 LAN に比べて、WLANs は固有の問題を含んでいます。WLAN の信号は無線なので、その無線有効エリアにおける全ての人が利用可能です。有線 LAN では、信号を受けるために、利用者は物理的にそのネットワークに接続する必要があります。WLAN の場合、WLAN 信号を受け取ることができる誰もが、その信号に干渉したり、傍受したりすることができます。すなわち、その利用者が送信もしくは受信しようとするデータには、潜在的には、誰にでも見られ、もしくは侵入者により改悪されるような、深刻な脆さが存在します。

有線 LANs では、物理的に LAN ケーブルを接続することが、そのネットワークに許可されていないアクセスを防ぎます。WLANs ではそのような制限（物理的な接続）が一切ありません。WLAN アクセスポイントは、信号を発信し、同時にその電波有効領域内の利用者からの信号を受け取ります。そのネットワークに接続するために必要な情報を持つ人は、誰もが接続可能です。

上記に加えて、WLANs はサービス拒否の攻撃（DoS—Denial of Service）にさらされます。WLANs は電波の到達域が隔離されていないために、悪意ある者が正常な通信を妨げるために攻撃することが可能です。

WiFi LAN s における安全性の解決策について :

WEP は Wired Equivalent Privacy(有線と同等のプライバシー)の略ですが、WLAN s において、有線 LANs と同等の安全性を得るために制定された規格です。WEP の基本的考えは、利用者が設定したキーと自動的に発生したキーの二つを用いて、データを暗号化することです。WEP は、伝送データの暗号化と受信後の解読処理に、同一のキーを用いるので、本質的には送受信が対照的なシステムといえます。WEP アルゴリズムとその使用にいくつかの欠点が指摘されていますが、それらはシステムの安全性を大きく損なうものです。WLAN のキーを自動的に見出すプログラムが、インターネットで容易に手に入るため、WEP は企業のネットワークを守るのには、十分な方法とは言えません。

WEP はデータを暗号化し、盗聴者に対しそれを不明瞭なものにしていますが、それは認可されていないコンピューターが WLAN に接続することを防ぐものではありません。MAC (Media Access Control) アドレス・フィルタリングは、この問題の解決を目指したものです。MAC はネットワークの各ノード特有のハードウェアアドレスです。システム管理者は、無線アクセスポイントに、認定されたコンピューターの MAC アドレスを登録します。そのアクセスポイントは、登録された MAC アドレス（もしくはより厳密である NICs）を持つコンピューターのみ、アクセスを許可します。フィルター上に明確に定義されていないアドレスは、アクセスを拒否されます。この MAC アドレス・フィルタリングは、ある程度の効果はありますが、残念ながら決して安全なものではありません。MAC アドレスの模倣は容易であり、したがって簡単に WLAN にアクセスすることができます。MAC アドレス・フィルタリングの問題点は、ユーザーの認証でなく、装置の認証をすることです。

IEEE 802.11i 標準は、WLAN s の安全上の脆弱性を解決するために制定されたも

のであり、WEPやWPAを包括しています。WPAはWi-Fiアライアンスによって制定されたWEPの危険性にたいしての中間的解決策です。802.11iは、認証方式にはIEEE802.1Xを、伝達経路の記録（トラッキング）にはRSN(Robust Security Network)を、そして秘密性、転送データの完全性、認証由来（origin authentication）には、AESによる暗号化を使用します。802.1Xはポイントとポイントの接続をサポートする、LANポートに付属したデバイスに対しての認証を行いません。802.11iは2004年6月に承認されたものであり、802.1Xと比較して、より広範囲をカバーしています。

安全性におけるバイオメトリックスの利点について

バイオメトリックスは、ユーザーの物理的特長と（もしくは）行為に基づく個人の認証を行います。通常のバイオメトリックスは、指紋、声紋、網膜、顔の特徴を含みます。さまざまなバイオメトリックスの中で、個人の識別、確認用としては、指紋の利用がマーケットで普及してきています。それには、低価格、高信頼性、指紋技術およびシステムの応答の速さ等の、多くの理由があります。

ユーザーの個人認証用として指紋の利用が普及してきたのは、パスワード、トークンベースのシステムに、いくつかの問題が見出されたためです。過去数年、個人が利用するオンライン口座の数が増えてきています。15以上のオンライン口座を持つ人は、決して珍しくありません。多くのパスワードを記憶しておくことは、たやすいことではありません。まれにしかアクセスしない人には、特にそれがいえます。この問題を解決するために、口座情報を紙に書き留める（メモ）する人もいます。こうした習慣は、メモの置き忘れや、紛失の可能性を考えると、とても危険です。多くのパスワードを管理する困難さは、結果的に、パスワード関連についての、IT部門への問い合わせの電話の増大を引き起こしています。同様な問題が、ハードウェア・トークンによる認証方式でも起きています。口座管理にトークンを利用している人々がいますが、持ち運びやその管理が難しくなっています。加えて、ハードウェア・トークンは容易に紛失します。

指紋ベースの個人認証は、パスワード及びハードウェア・トークンベースでの認証で顕著になった多くの問題に対して、洗練された解決策をもたらします。指紋技術が実現可能になり、信頼性があるものになって以来、個人認証用としての利用が普及してきています。SutiSoftの製品であるSECURED BioNetは、指紋による認証をとおして、アプリケーションや企業のネットワークへの正しいアクセス管理を実行しています。

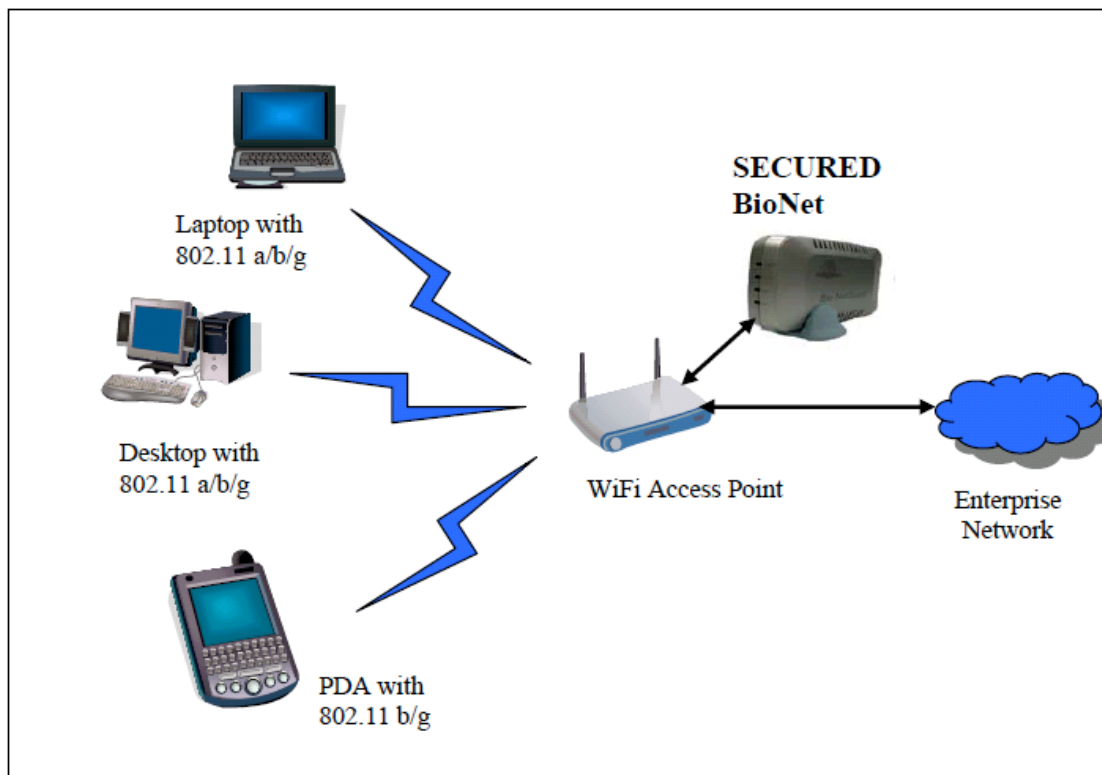
SECURED BioNet™：指紋ベースによるWi-Fi LANの安全保障

SECURED BioNetは、ネットワークの最初のコンタクト、すなわちWiFiアクセスポイントにおいて、指紋による企業内ネットワークへのアクセス管理を実行とします。最新のWiFi暗号化とバイオメトリックス個人認証技術を組み合わせて、SECURED BioNet™は御社のネットワークに、大変に頑丈なアクセス管理の仕組みを提供します。利用者がWiFi LANに接続する前に、SECURED BioNet™によってユーザーとして認証されなければなりません。

SECURED BioNet™は、WPA対応のどのアクセスポイントでも稼動する、DSPを用いた認証専用のハードウェア部品です。全体の認証プロセスを高速に処理するために、データ保存用のストレージ、プロセッサ、そしてメモリを備えています。すべての利用者の

指紋データとアクセスログが、SECURED BioNet デバイス内に保管されます。SECURED BioNet は、クライアント(無線アクセスポイント)と通信を安全に行ないます。

システム管理者は、SECURED BioNet の管理機能を用いて、SECURED BioNet デバイスに記憶されたユーザーID やユーザー情報を、サーバーもしくは記憶装置上にバックアップし、またそれを用いて、SECURED BioNet を再復帰することが可能です。システム管理用ユーティリティソフトでは、2つの SECURED BioNet デバイスに登録されたユーザー情報を、1 個のデバイスに移したり、あるいは別のデバイスに移したりすることができます。





強固なセキュリティ

SECURED BioNet は、WLAN s に強固で侵入不可能な安全性を提供します。指紋ベースのアクセス管理により、MAC フィルタリングやユーザーID、パスワードタイプのアクセス管理に伴う脆弱性を取り除きます。

Plug - and - Play デザイン

SECURED BioNet はプラグ&プレイに対応しており、その関連ソフトが付属されています。インストールとシステムの環境設定を行なうには、5分程で可能です。SECURED BioNet はすでに制定されている標準や、策定中の標準に完全に準拠しており、現在入手可能なアクセスポイント、アダプターカードに対応しております。

ハッカーフリーデバイス

SECURED BioNet はプロセッサ、記憶装置と RAM を持つ DSP ベースのデバイスです。特定のオペレーティング・システムを必要としないため、ほとんどハッカーフリー(不正侵入防止)です。

SECURED BioNet 設計仕様

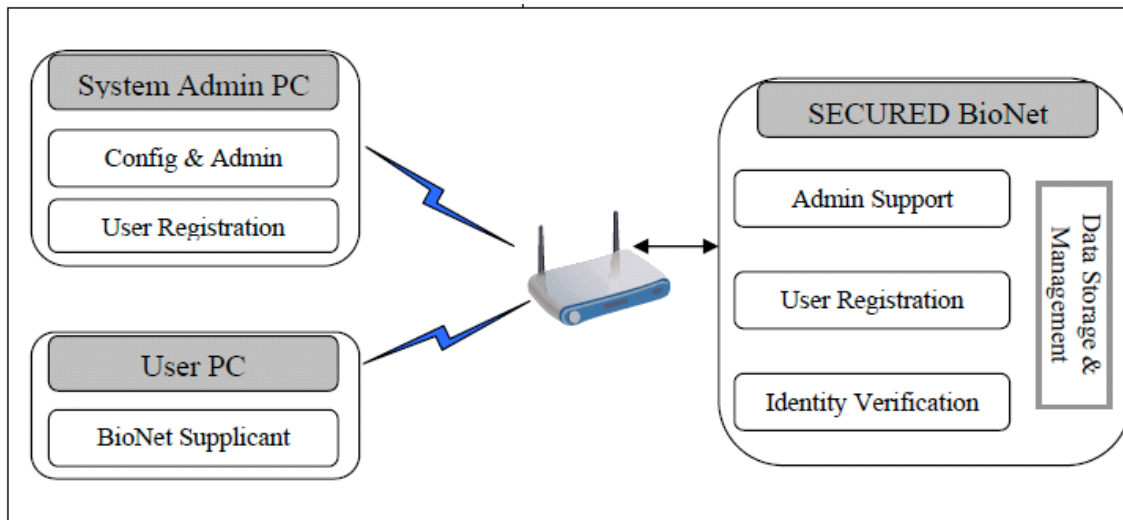
SECURED BioNet システムは、SECURED BioNet デバイスとその関連ソフトから成り立っています。ソフトウェアには 3 つの基幹部分があります。SECURED BioNet の環境設定とその管理、利用者登録、そして指紋ベースの認証を利用する WiFi クライアント・ソフトウェアの 3 つです。これら基幹部分はそれぞれ二つの部分に分けられます。片方は PC 上にて働き、他方は SECURED BioNet デバイスにて対応する部分です。

管理ソフトの主な機能は、システム管理者が的確な IP とポートナンバー、そして必要な機密情報を、SECURED BioNet デバイスに設定することです。加えて、システム管理者は、利用者の登録の状況と、SECURED BioNet デバイス上の全ての動きを監視できます。

SECURED BioNet が環境設定され、会社のネットワークに接続された場合、次のステップは、ユーザーの指紋の登録です。これは、SECURED BioNet のユーザー登録プログラムで行います。システム管理者は、このプログラムを用いて、ユーザー ID、指紋、アクセスレベル (通常ユーザーなのか管理者なのか)、そして有効期限を登録します。一度、ユーザー登録を行うと、ユーザーは、WiFi アクセスポイントをとおして、ネットワークに接続することを許可されます。

ユーザーが SECURED BioNet アクセスポイントに接続しようとする時に、そのユーザーは、認証を得るために、ユーザーID と指紋を要求されます。このステップは SECURED BioNet のクライアントソフトウェアで行います。このソフトウェアは、ユーザーPC 上で稼動しており、ユーザーに要求された指紋とパスワードデータを収集し、認証のために、

SECURED BioNet と通信している WiFi アクセスポイントにそのデータを送ります。



SECURED BioNet:容易な導入

SECURED BioNet は、企業にとって容易に導入でき、その後の段階的な増設が可能なように設計されています。処理能力の要求が増えるにつれ、既存の無線アクセスポイントにさらに SECURED BioNet デバイスを追加することが可能です。環境設定が容易なプラグ&プレイのアーキテクチャーは、ユーザが高度な知識を必要せずに簡単にインストールすることが可能です。

SECURED BioNet と他の方法との比較

WLANの安全確保は、企業において非常に重要です。WEPとかMACフィルタリングのような安全確保の手段は、企業用途には十分ではありません。企業はネットワークをより安全なものとするため、他の手段を導入してきました。その中では、バーチャル・プライベート・ネットワーク（VPN s）とユーザー名パスワード認証用サーバーの利用が、一般的です。

VPNのセットアップにおいて、企業内のWLANの安全性（もしくは危険性）は、外部ネットワークからアクセスした場合と同レベルになります—すなわち、ユーザーは社内ネットワークに接続する場合でも、外部ネットワークから接続する場合と同様の接続手順を実行しないといけません。この方法には、設定のためのコストアップ、企業 VPN の管理、そしてユーザーがその会社に在籍している時でさえ、VPN プロセスを通して接続しなければならない不便さなどの多くの問題があります。

第二のオプションとしては、一般的なアクセス制御として利用される、ユーザーID/パスワード認証を使用することです。この（WLAN用のアクセスコントロールの）方法は、導入、維持、そして運用を考えると、むしろ高価なものになります。こうしたシステムを管理することは、非常に煩雑なものとなることは周知の事実です。加えてこの方法は、認証用のユーザーID/パスワードを使用する際に伴う、多くの問題を抱え、安全なものとは言えません。

SECURED BioNet は、上述の 2 例の方法よりは、十分なコストと作業上の利点を持つ



ています。フル装備、プラグ&プレイ、強固なシステムを提供することで、これは (SECURED BioNet は)、VPNシステムの煩雑な管理も含めて、高価なハードウェア、ソフトウェアの必要性を排除できます。SECURED BioNet は、導入コストと管理費用を低減するだけでなく、他の方法で提供されるものよりはるかに高い安全性を提供します。

総 論

SECURED BioNet は、WiFi LAN への接続許可を、ユーザーの指紋により行うことで、WiFi LAN での強固な安全性を確保しています。SECURED BioNet は、現存する WiFi 安全対策製品のどれよりも優れています。SECURED BioNet は DSP ベース、固有のプロセッサ、メモリー付きのフル装備のユニットです。全ユーザーのデータとアクセスログが保存され、SECURED BioNet 内ですべての処理が行なわれます。SECURED BioNet は、特定のオペレーティング・システムに依存せず、設置、構成の設定、管理が容易なデバイスであり、事実上、ハッカーフリーなものです。SECURED BioNet は、企業内の WiFi LAN 用としてこのレベルの安全性を提供できる、市場で唯一のデバイスです。

