Soliton Systems
Security White Paper 2017

MAC アドレス制限は“効果ゼロ”

今さら聞けない「無線 LAN 認証」の基本

Soliton

はじめに

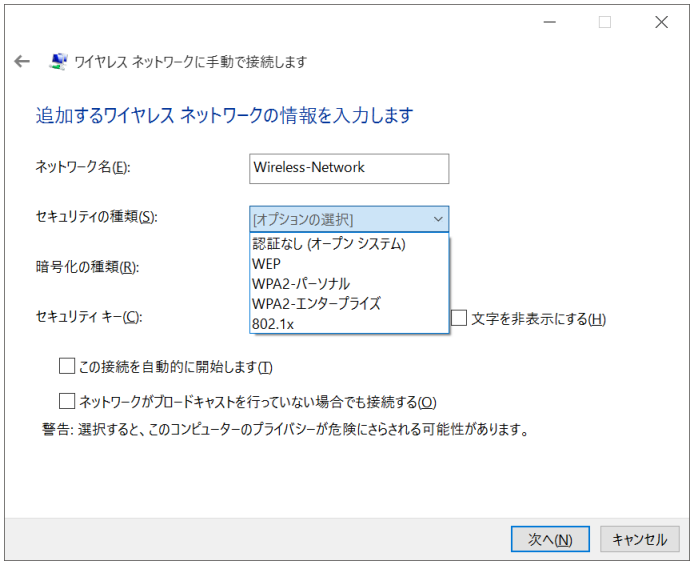
スマートフォンやタブレットの普及にも後押しされ、いまや不可欠な通信インフラとなった「無線 LAN」。家電量販店には安価で高性能な無線アクセスポイントが並び、企業のなかにも、一般家庭と同じような機器・セキュリティ設定で運用をされている場合があるでしょう。しかし、この無線 LAN の設定を間違えると、取り返しのつかない事態に陥ってしまいます。本書では、無線 LAN を安全に利用するための要となる「認証」の基本についてわかりやすく説明します。

1. パーソナルとエンタープライズのちがい

無線 LAN を安全に利用するには、用途にあった認証方式を選び運用していく必要があります。無線 LAN にアクセスしようとするユーザーやデバイスを確認することで、不正アクセスを防ぐためです。しかし、その設定や管理方法を誤ると、通信の盗聴や不正利用といった重大なリスクを招くことになってしまいます。そうならないよう、企業の担当者はどのような対策を施すべきでしょうか。

まず、無線 LAN 認証の種類を簡単に整理します。スマートフォンや PC を家庭用無線ルータに接続した経験があれば、端末の設定画面で「WPA/WPA2 パーソナル」「WPA/WPA2 エンタープライズ」などといった項目を目にしたはずです。WPA/WPA2 はセキュリティ規格のことで、暗号化方式と組みあわせて「WPA-TKIP」「WPA2-AES」などと表記される場合もあります。なお、認証の種類は「パーソナル」「エンタープライズ」などの部分からわかるようになっています。

たとえば、Windows における無線 LAN 認証の種類は以下のように表示されています。



Windows のワイヤレス ネットワークでは「セキュリティの種類」で認証を設定する

パーソナルとは、「PSK(Pre-Shared Key/事前共有鍵)」と呼ばれる共通のパスフレーズで認証する方式です。接続先となるネットワーク名を示す SSID と PSK を指定するだけで利用できる手軽さから、個人や家庭向けの小規模な無線 LAN で広く普及しています。

一方、エンタープライズは、ユーザーやデバイスを専用のサーバを使って認証する外部認証タイプであり、この方式では、個別の ID・パスワードや電子証明書が用いられます。

家庭用ルータや公衆無線 LAN を日常的に利用していると、企業利用であっても WPA/WPA2 パーソナル（WPA/WPA2 -PSK）を使えば十分なセキュリティが担保できると思ってしまいがちですが、これは極めて危険な誤解です。パーソナル（個人）とエンタープライズ（企業）とわけられるのには、しかるべき意味があります。

2. 企業での「PSK 認証」は危険!?

企業における無線 LAN の認証方法に PSK を採用すると、どのような危険があるのでしょうか。

まず、パスフレーズが流出する場合を想定してみましょう。企業無線 LAN に接続している（＝共通のパスフレーズが設定されている）デバイスを紛失したり盗難にあったりすると、そのデバイスが企業オフィスに近づくだけで企業無線 LAN に接続されてしまいます。デバイスを悪意ある攻撃者に操作されれば、ネットワークパケットのキャプチャツールなどを使って、通信内容の傍受と情報の窃取もできてしまいます。

また、盗難や紛失のほかに近年の脅威として注視しなければならないのが、内部の人間による不正です。会社に不満を持ちながら退職した人間が、在職中に使っていた SSID とパスフレーズで企業無線 LAN にアクセスする可能性は十分にあり得ますし、内部の関係者やパートナーのなかにも、犯行をくわだてるケースを想定する必要もあるでしょう。

こうしたデバイスの盗難や紛失、退職・異動によるユーザーの入れ替わりなどが発生した際には、ただちにパスフレーズを変更する必要があります。PSK 認証では全員が同じフレーズを利用しているため、その対象は無線 LAN を継続利用する全てのデバイスとアクセスポイントです。また、変更作業中はネットワークに接続できなくなるため、業務に大きな影響が出ないよう速やかに作業を完了させなければなりません。一般的なパスワードの運用と同じく定期的に変更しておいた方がよいでしょう。

つまり、企業ネットワークにパーソナル(PSK)方式を選択するなら、セキュリティ強度とリスクの評価とは別に、頻繁に大規模な設定作業を行う覚悟と、不定期なネットワーク停止を前提にする必要があるのです。

3. 「MAC アドレス認証」は悪意を持った攻撃者の前では無意味

PSK 認証に加えて「MAC アドレス認証」という方式を採用する場合もあります。頻繁に使用される言葉なので、一度は耳にしたことがあるのではないでしょうか。MAC アドレス認証とは、ネットワーク機器に割り当てられた MAC アドレス（Media Access Control Address）を利用して、ネットワークへのアクセスを制限する手法です。

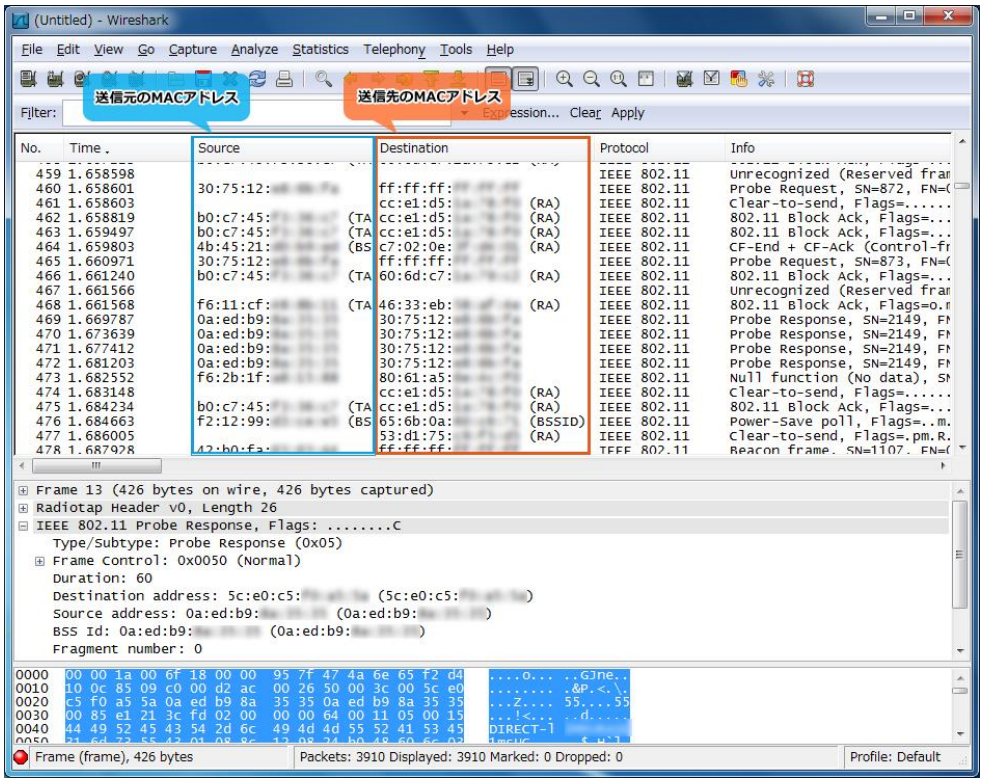
家庭用ルータなどでは、MAC アドレス認証をまるで無線 LAN セキュリティの機能のひとつとして扱われることがあります。そのため、「完全ではないものの一定の効果は期待できるセキュリティ機能」といったように理解し、たとえ共通パスフレーズが漏れても MAC アドレス認証を併用し、デバイス自体のアクセスを制御すればいいのではと考える人も多いのが実情です。

しかし、これは大変危険な状況です。MAC アドレス認証について誤った理解のまま運用すると、攻撃者に悪用されかねません。

そもそも、MAC アドレスは認証という用途には向いていません。ある要素を「認証」に用いるには、第三者に情報が知られず、また偽装もされにくいことが最低限の条件になりますが、MAC アドレスはこうした要件をまったく満たしていないのです。

MAC アドレスはネットワークデバイス固有の値だが、それは通信するために便宜的に割り当てられたものにすぎません。いうなれば住所のようなものです。通信相手に積極的に開示される情報であり、全く隠されていません。

無線 LAN では通信が暗号化されているので大丈夫では? と誤解されがちですが、むしろ有線 LAN よりも危険なのです。通信するために用いる MAC アドレスは暗号化の範囲に含まれておらず、空中を飛び交っているパケットを収集すれば、許可されているであろう MAC アドレスを、容易に知ることができてしまいます。



ネットワークパケットキャプチャソフト「Wireshark」を使えば、MAC アドレスを簡単に知ることができる

また、通信に用いる MAC アドレス情報を後から変更することは禁止されていません。書き換えるツールは、インターネット上で「MAC アドレス　書き換え」などのキーワードで検索すれば、すぐに見つけることができます。その気になりさえすれば、特別な技能や機材がなくても MAC アドレスを取得し、端末にその値を設定して、何の苦もなくアクセスできるのです。

実際に、MAC アドレス認証を突破してネットワークに侵入された事例も報告されています。例えば 2016 年 6 月に起きた佐賀県教育情報システムでの情報漏えい事件では、校内無線 LAN の一部に MAC アドレスによる制限が行われていましたが、犯人は MAC アドレス認証を突破し個人情報を窃取しています。

MAC アドレスは、一定の「フィルタリング」を行うことはできますが、デバイス認証の手段としては、まったく頼りになりません。「進入禁止」と書かれた規制テープのようなものであり、一定の抑止効果はあるものの悪意を持った攻撃者はそれを気にもとめず乗り越えてくることを理解した上で導入すべきでしょう。

4. 企業無線 LAN には「エンタープライズ認証」を

いまや無線 LAN は企業活動に欠かせないインフラ基盤です。利用される分野も広がっており、例えば総務省は、2020 年までに全国すべての小・中・高校に無線 LAN(Wi-Fi)を導入するよう進めています。今後、ますます無線 LAN がネットワークの標準として普及していくことは間違いありません。

だからこそ、企業無線 LAN を PSK や MAC アドレス認証で運用する危険性を知っておかなければなりませんし、PSK 認証における危険性を回避する WPA2 エンタープライズへの正しい理解も求められているのです。

WPA2 エンタープライズは「IEEE 802.1X EAP 認証」を採用しており、大きく分けて下記の 2 つがあります。

（1）ID とパスワードを用いて認証するタイプ
（2）電子証明書を用いて認証するタイプ

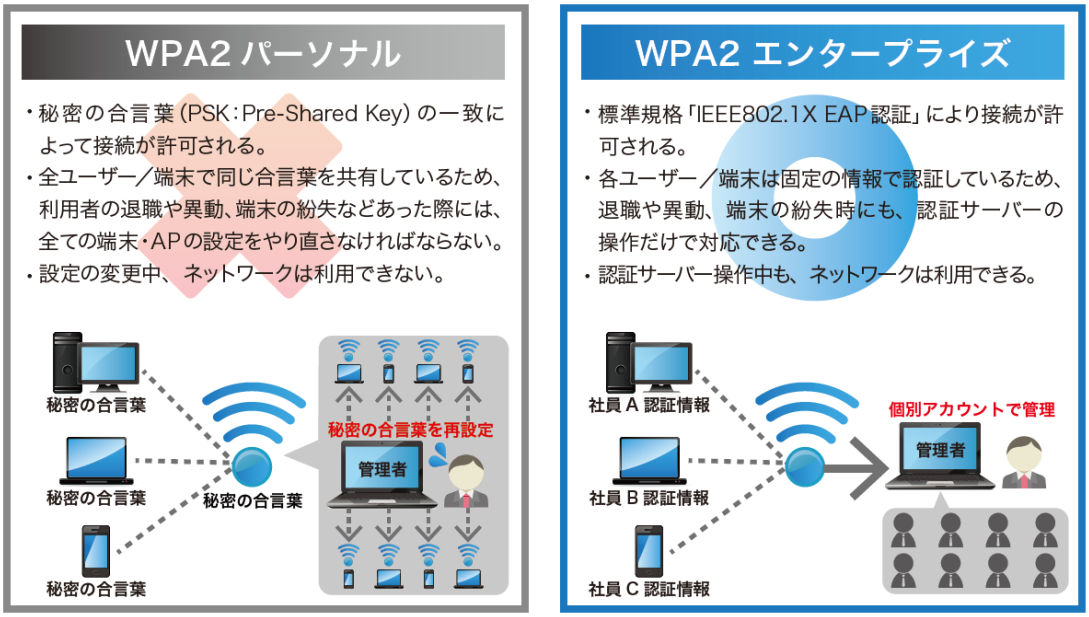
特に近年では、クライアント PC を有線 LAN で接続する機会が急速に減る一方、無線 LAN の普及が急速に進み、社員が利用するデバイスもモバイル PC やタブレット、スマートフォンが主流になってきました。こうした流れもあり、WPA2 エンタープライズの環境を整備し、社内の無線 LAN 環境を強固なセキュリティで保護する必要性もさらに高まっています。

5. ID とパスワードによるセキュリティと"限界"

まず WPA2 エンタープライズのうち、EAP-PEAP に代表される「ID とパスワードを用いて認証するタイプ」が WPA2 パーソナルとどう違うのかを整理します。

WPA2 パーソナルでは、共通のパスフレーズ(PSK)で認証を行います。PSK を知っているユーザーのみがアクセスを許可される仕組みはパスワード認証と同様ですが、共通のフレーズを使用するため認証情報が外部に漏えいした場合の影響は大きくなります。一方、WPA2 エンタープライズでは、ユーザーごとに異なる ID とパスワードを用います。認証情報を秘密として管理しやすく、いつ、どのユーザーがアクセスしたのかを把握することも可能です。

運用面でのメリットも大きく、ID とパスワードが漏えいした場合でも、該当ユーザーのアカウントを停止するだけで済むため、WPA2 パーソナル環境で見られた全ての端末・アクセスポイントを対象とした再設定作業は必要ないですし、その間のネットワーク停止も発生しません。



WPA パーソナルと WPA2 エンタープライズの違い

一見、WPA2 エンタープライズにしさえすれば手軽に安全を確保できるように思えますが、セキュリティ要件によっては適さない場合があります。それは、「ID とパスワードを用いて認証するタイプ」はユーザーごとの認証であり、デバイスごとの認証はない点です。

6. 「シャドーIT」を野放しにしておくのは危険!

ユーザー認証を厳格に実施していたにも関わらず、不正なアクセスを見逃してしまうケースは、決して特異な例ではなく、企業無線 LAN でも十分に起こりうる問題です。

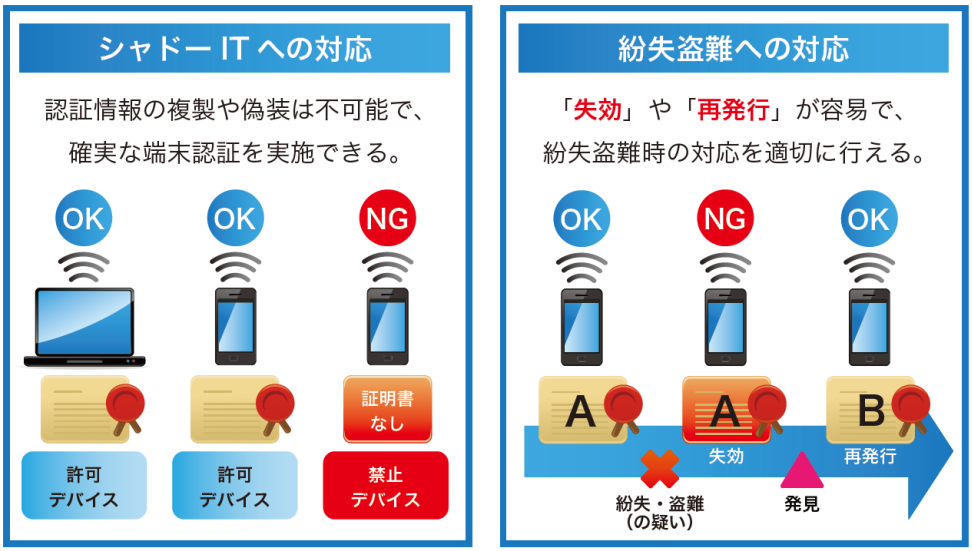
その原因のひとつとして「シャドーIT」があります。シャドーIT とは、社員が会社の許可を得ずに持ち込んだ私物のデバイスや、それらが業務で利用されている状態を指します。管理外のデバイスが無秩序に社内 LAN に接続され、インターネットなどの外部ネットワークにアクセスすることで、ウイルス感染や情報漏えいなど、思わぬトラブルにつながりかねません。

有線 LAN が主役であった時代、「持ち込み PC 対策」としてネットワーク接続できるクライアントを制限する目的で、不正な PC が接続された際には、すみやかに検知できる仕組みを導入した企業は多くありました。小型で高性能、オフィスに持ち込まれる頻度が桁違いのスマートフォンを対象とする無線 LAN では、より一層の注意が必要です。

上記を踏まえて、ID とパスワードによる認証環境を考えてみましょう。社員は自身の ID とパスワード知っています。この状況で社内イントラ上の業務情報を今すぐ確認したくなった場合、手元には使い慣れた私物のスマートフォンやタブレットがあり、パスワードを入力すれば簡単に接続できるとすればどうでしょう。社員本人の悪意の有無とは別にして、社内データを私物のスマートフォンやモバイル PC にコピーし、自宅に持ち帰って作業したり、個人端末からインターネット上のファイル共有サービスにデータをアップロードしたりするといった事態が起こることが、容易に想像できてしまいます。

7. 電子証明書を用いてセキュアな無線 LAN 環境を実現

無線 LAN 認証という観点から、こうしたシャドーIT の問題に対応するのが、EAP-TLS と呼ばれる「電子証明書を用いて認証するタイプ」です。電子証明書は現実の世界における運転免許証やパスポートのようなもので、対象を正しく認証・特定するインターネット上の身分証明書です。電子証明書を導入した端末のみがアクセスできるようにすることで、シャドーIT への対応はもちろん、デバイスの紛失や盗難時においても、デバイスを社内 LAN にアクセスさせないという対策を迅速にとることが可能です。



シャドーIT・紛失盗難への対応法

すでに WPA2 パーソナルで運用している場合でも、法人向けアクセスポイントを導入しているのであれば、WPA2 エンタープライズにも対応している可能性が高いので、この機会に確認いただくのが良いでしょう。

電子証明書を使った無線 LAN 認証では、外部の認証サーバなどが必要になるため、構築や運用が面倒だと思う人も多いかもしれません。しかし、無線 LAN 環境の普及と企業ニーズの高まりを受け、現在では、簡単に環境構築できるようになってきています。

8. 電子証明書は「使いやすさ」と「セキュリティ」を両立できる

電子証明書という言葉を聞いて、まず何を思い浮かべるでしょうか。「ID/パスワードと比べてなんだか難しそう」、「ユーザーに説明するのが面倒そう」、「運用が大変になりそう」といった感想を持つかもしれません。しかし、これは大きな誤解で、近年では電子証明書による無線 LAN 認証環境の導入や運用は想像以上に簡単なものとなっています。

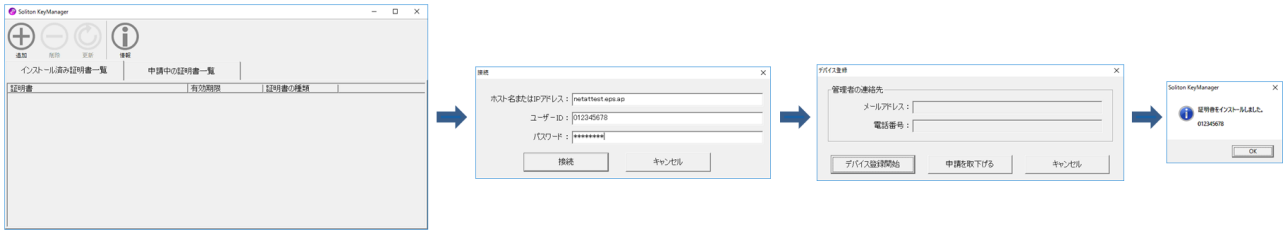
認証環境に必要な機器は、RADIUS サーバーと認証局(CA)の 2 つですが、かつては各サーバーを立てたうえで、データベース（Active Directory/LDAP）の連携を行う必要があるなど、管理に手間がかかっていました。しかし現在では、これらの機能がアプライアンスとして提供されています。つまり、既存環境に専用アプライアンス機を追加導入するだけで、電子証明書を使った無線 LAN 認証環境がすぐに構築できるのです。

9. 安全で簡単な証明書配布を実現する「Soliton KeyManager」

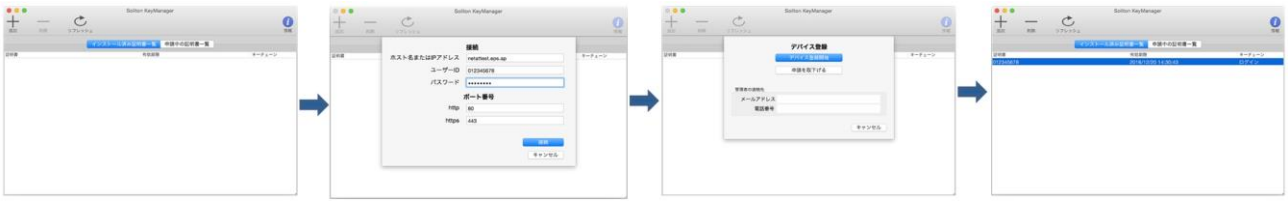
一般的に、電子証明書のインストールは p12 ファイル（PKCS#12 標準に準拠する、秘密鍵と公開鍵証明書をともに保存するファイルフォーマット）を安全な手段でユーザーの端末に受け渡し、端末上でウィザードを使って端末の証明書ストアにインストールする方法をとります。電子証明書をインストールした経験のある人はわかると思いますが、クリックしてインストールを進めるだけとはいえ、「p12 ファイルとは何か」「どこにどうインストールするのか」など、聞いただけではよくわからないことも多いです。逆に、IT に興味がある人であれば、p12 ファイルを複製して私物のスマートフォンなどにインストールし、スマートフォンからも無線 LAN にアクセスできるようにするといった不正行為を行ってしまう可能性もあります。

このほかにも、本当にイントールしてよい端末なのか、配布した p12 ファイルが途中で誰かに盗まれていないか、不正にコピーされていないかなど、電子証明書の配布においてチェックしなければならない項目は多数あります。たとえば、セキュリティを考慮すると、メールのような暗号化されない環境で、不特定多数に拡散するリスクが高い配布手段はとることができません。

こうした課題を解決するのが、ソリトンシステムズが提供する電子証明書配布ソリューション「Soliton KeyManager」です。Soliton KeyManager を使えば、電子証明書のインストールをユーザー自身で簡単・安全に行うことが可能となります。たとえば、Windows や macOS の PC 版では以下のような手順を踏むだけで、**電子証明書を安全・簡単にインストールすることが可能となります。**



Windows での「Soliton KeyManager」画面



macOS での「Soliton KeyManager」画面

Soliton KeyManager は、スマートデバイス版のアプリケーションも提供しています。なお、iOS で無線 LAN 認証用に電子証明書を取得する場合は、Safari から電子証明書配布ページにアクセスします。

ここで大きなポイントになるのが、電子証明書の窃取や不正コピーの防止についてです。**Soliton KeyManager では、電子証明書の秘密鍵は発行要求時に端末内で自動生成し、電子証明書のインストール中、一切端末外に出さない方式をとっています。**また組織が許可する端末の識別コードを、予めサーバーに登録しておくことで、不許可端末からの発行要求を受け付けない運用も可能となります。そのため、**電子証明書が盗まれたり、不正に取得されたりする危険がありません。**

Soliton KeyManager による電子証明書配布は、NetAttest EPS と NetAttest EPS-ap を組み合わせることで利用可能となります。

10. 電子証明書の「失効」も簡単

NetAttest EPS と Soliton KeyManager は、運用面でも大きな効果を発揮します。

端末を紛失したり有効期限が切れたりした場合、電子証明書を失効したり、再発行する必要があります。PSK の再設定ほどではないにしろ、ユーザーや管理者にとっては大きな負担になりかねません。

ユーザーは端末を紛失したことを IT 部門に伝え、連絡を受けた IT 部門は、当該端末に発行されている電子証明書を発行履歴から特定し、速やかに失効しなければなりません。近年では、一人が複数台の端末を業務利用することも珍しくないため、IT 部門では、利用者と端末の組合せ毎にどの電子証明書を発行したのか、履歴を管理しておくことも必要となります。端末紛失してしまったユーザーが新たに端末を購入した場合も、電子証明書再交付の履歴を管理していかなければなりません。

NetAttest EPS と Soliton KeyManager を使えば、こうした運用管理も極めて簡単です。**一人が複数台の端末を業務利用している場合でも、サーバー側で発行済み端末の情報を自動収集し、ユーザーと紐づけて管理**しています。端末紛失時には、ユーザー名を検索するだけで、発行済み端末の情報を即座に確認し、当該端末の特定と失効を速やかに行うことが可能です。

電子証明書の失効運用イメージ

また、電子証明書の有効期限切れが近づいていることをユーザーへ自動通知することもできます。通知を受けたユーザーは、Soliton KeyManager を利用し、IT 部門に問合せることなく、自身で電子証明書を再取得します。サーバー側では、ユーザーが再取得した時点で、以前に発行された電子証明書の自動失効と端末情報の再収集が自動実行されます。このように、電子証明書を利用するための環境構築と運用は、多くの管理者やユーザーが想像する以上に簡単なものとなっています。

11. さいごに

クラウドやモバイルの普及とあわせ、無線 LAN は企業ネットワークの標準的な環境となっており、電子証明書を使って、安全性と利便性を両立した無線 LAN 認証を整備することは必須の状況です。企業における無線 LAN セキュリティに悩んでいる方や不安がある方は、本書で紹介したソリトンシステムズの NetAttest EPS のような製品を使い、簡単かつ安全に無線 LAN の環境整備に取り組んで頂ければ幸いです。

Soliton Systems Security White Paper 2017
MAC アドレス制限は “効果ゼロ” 今さら聞けない「無線 LAN 認証」の基本

SMKT1705-A
発行　2017 年 5 月 24 日
発行所　株式会社ソリトンシステムズ
お問合せ先　netsales@soliton.co.jp