

# ユニアデックス アプライアンスPKI認証ソリューション

高度なセキュリティー環境を低コストで構築  
多彩なネットワーク環境と幅広いシステム規模に対応



*Certificate  
Solution*

**UNIADEX**

# ネットワークセキュリティーが 後回しになっていませんか？

無線LANが急速に普及し、インターネットを介した社内システムへのアクセス機会が増加するなど、ビジネス・ユーザーにとっての使い勝手が向上すると、同時にセキュリティー面での不安も増えてきます。一方、セキュリティーを強化しようとしても、構築や運用が複雑でハードルが高いのも事実。ユニアテックスのアプライアンスPKI認証ソリューションは、そのような悩みをスマートに解決する、有効な処方箋を提供します。

# APPLIANCE PKI

企業のインフラとして無線LANを使うには  
セキュリティーが心配！

高いセキュリティーが必要なネットワークに  
PKIを導入したいが、構築・運用が大変！

無線LANとリモートアクセスVPN  
まとめて運用・管理できないだろうか？



## アプライアンスによるPKI認証で、 高度なセキュリティーをらくらく確保。

ユニアテックスのアプライアンスPKI認証ソリューションは、高度な認証機能をソリトンシステムズ社製のアプライアンスサーバーNet'Attestシリーズに集約、構築や運用の余分な手間を徹底的に排除し、コスト負担も大幅に軽減します。Net'Attestシリーズには認証サーバーとプライベートCA（認証局）の機能が統合されており、お客様は、高いセキュリティーレベルを持つPKI認証を、容易に実現することができます。

### システムごとに分散していた 認証システムの運用を一元化

無線LAN、クライアントVPN、拠点間VPN認証、ダイナミックVLANの認証を1台のアプライアンスでカバー。通常のネットワーク認証サーバーの機能に加え、サーバー証明書とクライアント証明書両方の発行、証明書失効リストの発行といった機能を一元管理できます。これにより、構築の短期化と簡単・安価な運用管理が可能になります。

### 課題が多かった無線LANの セキュリティーを強固に

無線LANのセキュリティー対策としてIEEE802.1xの認証方式を採用。IEEE802.1x対応の無線LANスイッチや無線LANアクセスポイントを介し、クライアントとの間で認証を行うことで不正アクセスを遮断し、安全な無線LAN環境を実現します。

## アプライアンスPKI認証ソリューション

### 3つのポイント

1 多彩なネットワーク環境に強固なセキュリティーを提供

2 階層構成で大規模ネットワークに対応

3 他の認証システムとの柔軟な連携



# 多彩なネットワーク環境に強固なセキュリティーを提供

無線LAN、クライアントVPN、拠点間VPN、ダイナミックVLAN。  
複数のネットワークの認証に1台で対応します。

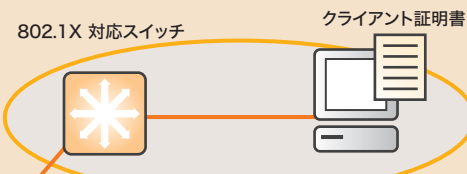
## 無線LAN認証

急速に普及する反面、セキュリティーには大きな課題がある無線LAN環境。アプライアンスPKI認証ソリューションは、無線LANにおいて「証明書を使用した相互認証」+「WEP鍵の自動更新による暗号化通信」を実現（EAP-TLSを使用）。高度で堅牢なセキュリティー環境を実現しながらも、証明書の運用を大幅に簡素化し、クライアントPCの快適な操作性を妨げません。



## ダイナミックVLAN

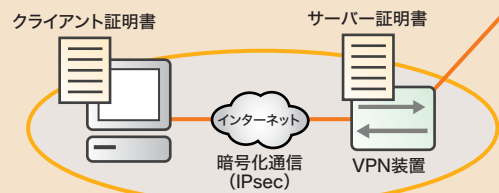
組織間で異なる運用ポリシー、セキュリティーポリシーを統合するために利用されるダイナミックVLAN。アプライアンスPKI認証ソリューションは、クライアント証明書と802.1xベースの認証を組み合わせたダイナミックVLANを実現。ユーザーごとに異なるVLAN割り当てを容易に実現し、柔軟でユーザビリティの高いネットワークインフラの構築を支援します。



## Net'Attest EPS/EPS-DX

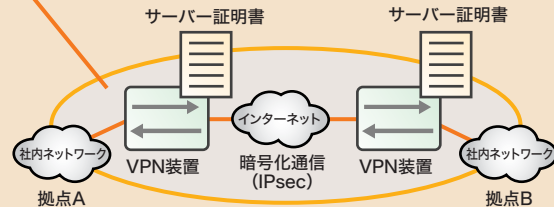
サーバー証明書

- Net'Attest EPS/EPS-DXの機能
- 認証局 (CA)
  - RADIUS認証サーバー
  - EAP認証サーバー



## クライアントVPN認証

ブロードバンド接続、ユビキタスな通信環境の普及により、モバイルオフィスを支えるクライアントVPN接続。このクライアントVPN接続において、CAが発行するサーバー証明書・クライアント証明書 (X.509) をIPsecと組み合わせて、安全で信頼性の高い接続環境を実現。ユーザーIDとパスワードによる旧来の認証に比べ、はるかに強固なセキュリティーを実現します。



## 拠点間VPN認証

広帯域回線の低廉化、企業をとりまく環境のグローバル化が進むにつれて、幅広く利用されているインターネットを利用した拠点間VPN接続。この拠点間VPN接続において、認証局が発行するサーバー証明書 (X.509) とIPsecを組み合わせ使用。複数企業間の接続のような強固なセキュリティーが必要とされる環境においても、セキュアな拠点間・企業間接続が可能になります。

# 階層構成で大規模ネットワークに対応

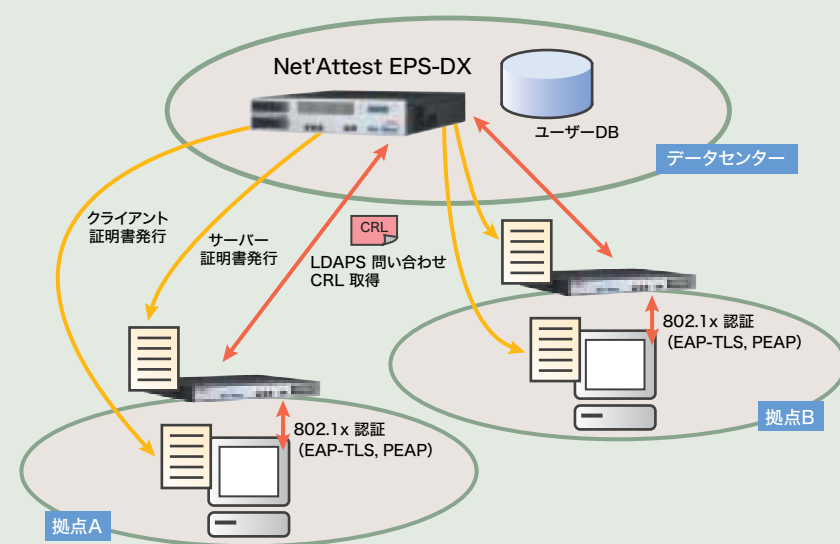
ユーザー情報・証明書の管理機能、ネットワーク認証機能の集中化と分散化  
スケーラブルに構成し、最大10万ユーザーまで収容できます。

## 集中モデル

全国のユーザーをセンターで集中管理するケース

全国のユーザーをデータセンターで集中管理し、認証する形態です。  
データセンターにNet'Attest EPS-DXを設置し、各拠点にはNet'Attest EPSを配置します。

- 認証は各拠点とデータセンターが連携して実施  
ユーザーの登録や、クライアントおよびサーバー証明書の発行などの管理業務はデータセンターで集中して行います。証明書を使用したネットワーク認証 (EAP-TLS, IPsecなど) やID/パスワードを使用した認証 (MS-PEAPなど) は、各拠点とデータセンターそれぞれに設置された認証サーバーが連携して実施します。
- 階層構成により障害の影響範囲を極小化  
Net'Attest EPS-DX単体でも10万ユーザーの収容は可能ですが、階層構成にすることで、障害が発生した場合の影響範囲を極小化できます。回線越えて認証しない、または認証を集中させないなどの対策をとることで、パフォーマンスを安定させることもできます。

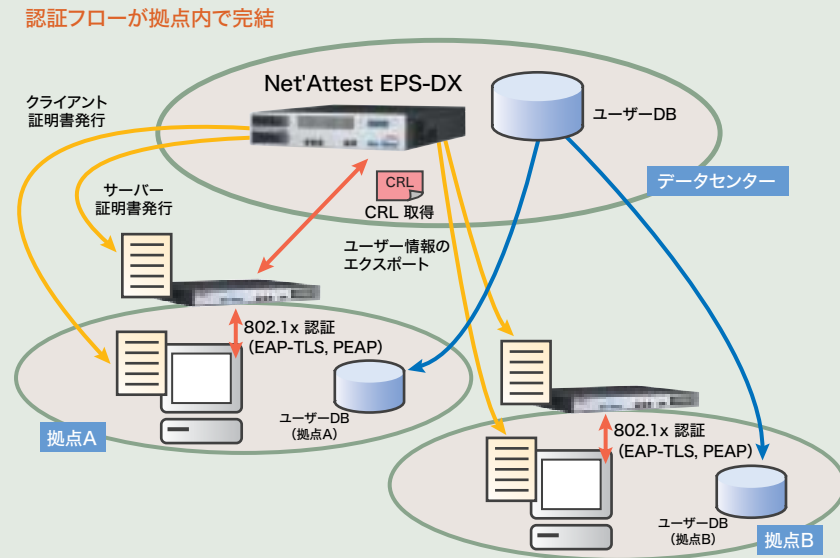


## 分散モデル

拠点で認証トラフィックを完結するケース

ユーザーDB を拠点の Net'Attest EPS に分散配置し、  
証明書、ID/パスワード両方式の認証処理を各拠点内で完結させる形態です。

- 回線に障害が発生しても認証可能  
集中モデル同様に、ユーザーの登録や、クライアントおよびサーバー証明書の発行などの管理業務はデータセンターで行いますが、証明書を使用した認証とID・パスワードの認証は、各拠点内で完結するため、認証トラフィックがセンター拠点間で発生しません。全国を接続するネットワークに障害が発生しても、それぞれの拠点で認証を受けることができ、通常どおりシステムにアクセスできます。
- 冗長構成にも対応  
また、データセンターのNet'Attest EPS-DX と拠点の Net'Attest EPS 間での冗長構成も可能です。これにより、拠点のNet'Attest EPSに障害が発生しても、認証フローに影響を与えない、高い信頼性を得ることができます。

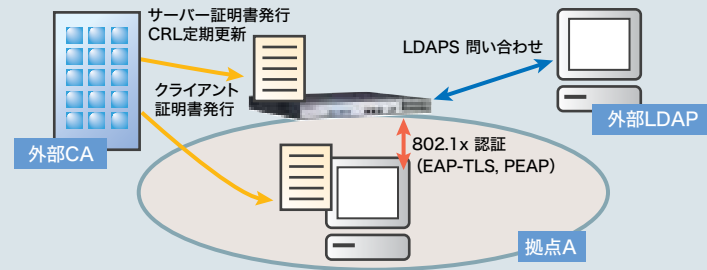


# 他の認証システムとの柔軟な連携

外部CAやLDAP、証明書格納デバイスに対応。  
柔軟でセキュアな連携機能を提供します。

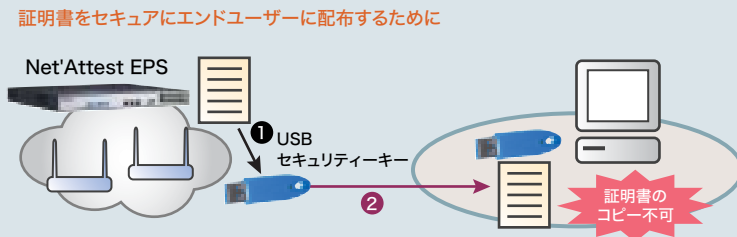
## 外部 CA, LDAP との連携

アプライアンスPKI認証ソリューションは、既存認証インフラと柔軟に融合。パブリックCAやLDAPサーバーが存在する場合、それらと連携し、セキュアな認証環境を構築できます。



## 証明書格納デバイスとの連携

クライアントPCに保存されている証明書は、コピーされる危険もあります。そこで、USBセキュリティキーなど携帯用デバイスに証明書を保管し、配布できます。証明書のコピーを防ぎ、セキュアに証明書を配布することで、より高いレベルのセキュリティを確保できます。



## アプライアンスPKI 認証ソリューションを支える技術

### PKIとは?

PKI (Public Key Infrastructure) とは、一般的には公開鍵暗号を用いた技術・製品全般を指す言葉。電子商取引サイトやe-Japanなどの電子政府における認証・暗号化の基盤技術として広く普及している。

### デジタル証明書とは?

CA (認証局) が発行する本人確認のためのデータ。信頼されたCAからデジタル署名用の公開鍵が発行され、その内容が未改ざんであることを確認することで本人確認が可能。デジタル証明書の仕様はITU-T X.509で既定されている。

### CAとは?

デジタル証明書を発行・管理する仕組み。Certificate Authorityの略で、認証局とも呼ばれる。CAには「パブリックCA」と「プライベートCA」があり、前者は電子商取引など不特定多数に対して第三者として認証サービスを提供する機関を指し、後者は企業内や特定の取引企業間など比較的閉じた環境内で使用される仕組みを指すことが多い。

### CRLとは?

Certificate Revoke Listの略で、証明書の紛失・誤発行などの理由により、有効期間内に無効となった証明書のリスト。証明書の受取人は証明書とCRLを照合することにより、証明書が現在も有効かどうかを確認できる。

### IEEE802.1xとは?

IEEE (米国電気電子技術者協会) において規格化されたLAN内でのユーザー認証方式。有線・無線を問わず利用可能な汎用的な技術であるが、セキュリティに課題が多い無線LANにおける認証の仕組みとして特に注目を集めている。

### EAP, EAP-TLS, PEAPとは?

EAPとはIEEE802.1xで規定された拡張性の高い認証プロトコル。EAPと組み合わせて使用する標準の認証方式としてTLS (Transport Layer Security)、シスコシステムズとマイクロソフト、RSAセキュリティが共同開発した認証方式としてPEAP (Protected EAP) がある。両者ともデジタル証明書を使用した強度の高い認証方式としてさまざまなソフトウェアベンダー、ネットワーク機器ベンダーによって支持されている。

### LDAPとは?

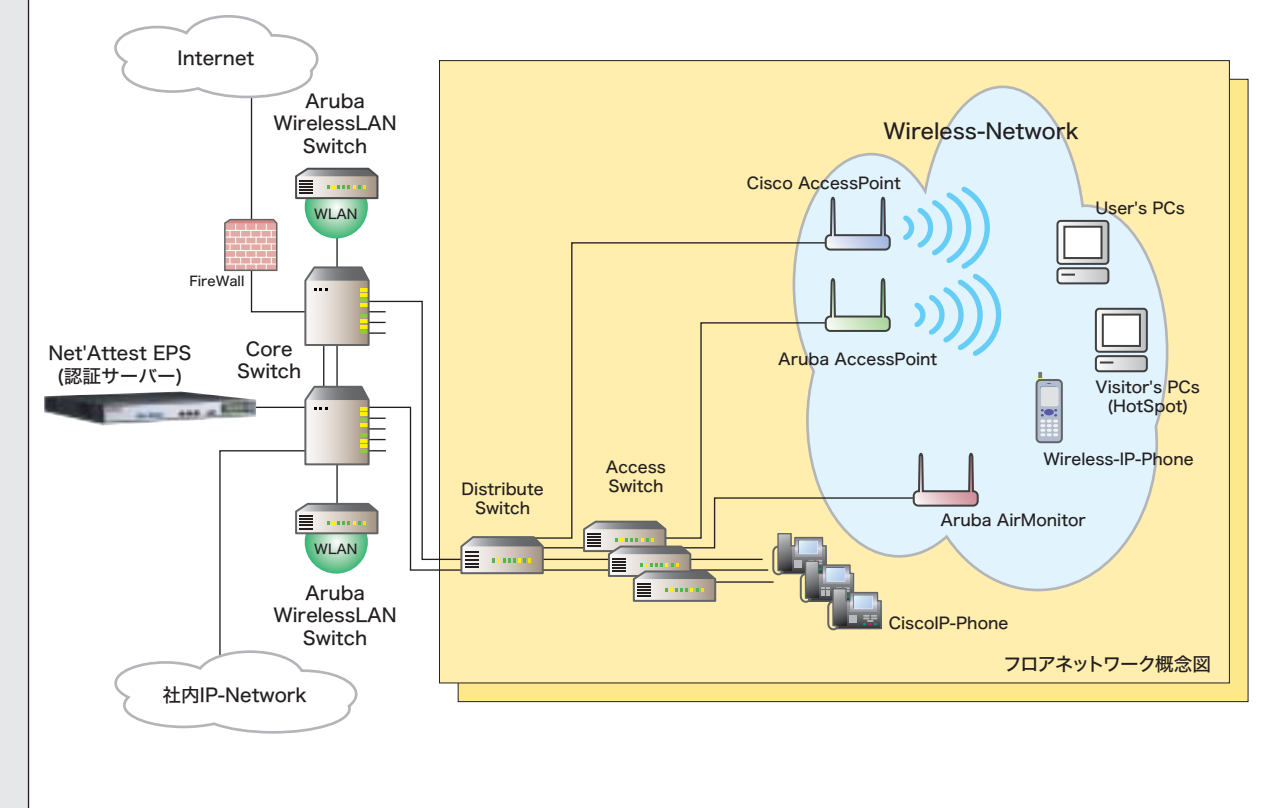
氏名・メールアドレス・証明書などの属性を登録したディレクトリサービスにアクセスするためのプロトコル。IETFによって標準化されている。取り扱いの簡単さから各種OSに導入されており、マイクロソフトのActive Directoryなどで採用されている。

# アプライアンスPKI認証ソリューション活用例

## 多様なLAN環境とリモートアクセスのPKI認証を1台のアプライアンスで集中管理

社内システムのIPネットワーク、さらには、複数メーカーのアクセスポイントを含む無線LAN環境がフロアごとにくつも構築されている状態で、Net'Attest EPSをコアスイッチに接続し、PKI認証機能を1台に集約しました。外部からのリモートアクセス、社員のPCや無線IPフォンからのアクセス、ホットスポットでのビジターからのアクセスすべてに認証がかかるため、ネットワーク全体から不正アクセスを排除できます。また、CA (認証局) の構築、デジタル証明書の発行などセキュリティに関する運用管理の一元化を実現、PKI の導入・運用コストを大幅に削減しました。

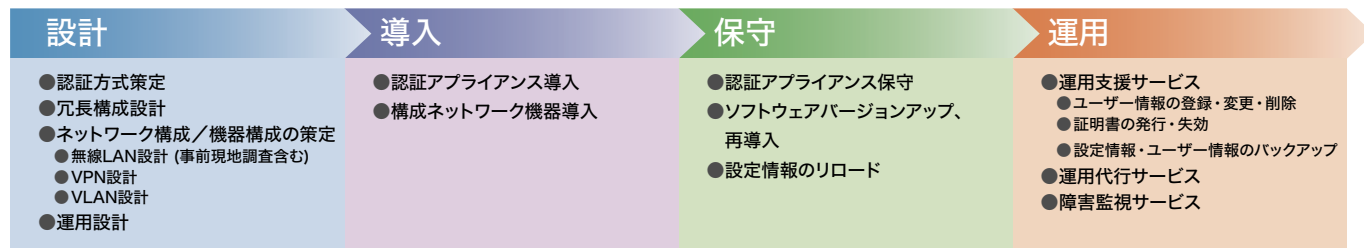
### WirelessNetwork概念図



## ■ 提案から保守まで一連のサービスを提供

長年にわたる豊富な構築実績と高い顧客満足度で定評のあるユニアデックス。

そのきめ細かなサービスで、設計や導入だけでなく、提案から保守までトータルに提供します。



## ■ 提供する機能

### EPS-DX03



### EPS-ST03



### EPS-SX03



- ユーザー認証方式で、EAP-MD5、EAP-TLS、Cisco-LEAP、MS-PEAP、EAP-TTLS、PAP、CHAPをサポート
- プライベートCA機能
  - サーバー証明書発行\*
  - クライアント証明書発行
  - CRL機能
  - 証明書更新機能
- 外部LDAPサーバー参照機能
- ユーザーアカウントグループ化機能
- UPS対応
- 外部認証システムとの連携
  - パブリックCA
  - Microsoft® Windows®ドメイン認証
- 10万ユーザーまで対応 (EPS-DX)
- IEEE802.1X/EAP対応スイッチのVLAN制御
- DHCPサーバー機能
- ディレクトリサーバーによるユーザー管理機能
- Webブラウザによる設定・管理
- 冗長化機能
- ログ管理機能
- SNMPエージェント機能
- NTPによる時刻同期

(\*) EPS-SX03では提供しておりません

# UNIADDEX

## ユニアデックス株式会社

東京都江東区豊洲1-1-1 135-8560  
TEL 03-5546-4900 (大代表)  
URL <http://www.uniadex.co.jp/>

## UNIADDEX, Ltd.

Headquarters: 111 Toyosu, Koto-ku, Tokyo 135-8560, Japan  
Telephone: +81(3)5546-4900  
URL: <http://www.uniadex.co.jp/>

関西支店 TEL06-6343-5188 中部支店 TEL052-204-6850 九州支店 TEL092-473-3003  
北海道営業所 TEL011-242-2350 東北営業所 TEL022-261-9217 新潟営業所 TEL025-247-7600  
首都圏第一営業所 TEL045-681-8861 首都圏第二営業所 TEL048-642-5881 北陸営業所 TEL076-233-9850  
静岡営業所 TEL054-272-4722 中国営業所 TEL082-242-5088

※Microsoftは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。  
※Windows、Windows Serverは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。  
※NetAttestは、ソリトンシステムズの商標です。  
※その他の記載の会社名・商品名は、各社の商標または登録商標です。  
※記載の仕様は、予告なく変更することがあります。