「認証ネットワークソリューション forBusinessのご紹介」

～ビジネスデマンドを損なわない 情報セキュリティ基盤の確立～

アヴェイルテクノロジ株式会社

はじめに

◆当社は、ネットワーク業界において第一線で活躍してきた**経験豊かな技術者**を中心に、ネットワーク基盤のインテグレーションサービスを提供しております

◆こうした経験に基づく確かな技術力を強味とし、なおかつ**独立性を活かし**、お客様の既存環境と事業要求に最適な**柔軟なソリューションの提供**をします

◆企画から展開まで**一貫した支援体制**でお客様のサポートをします

認証ネットワーク導入の背景

①企業の情報セキュリティ強化の必要性

社会からの要求

情報セキュリティ対策が整っていないことは、顧客、取引先、関連会社を含む社会からの**信用失墜**に直結します

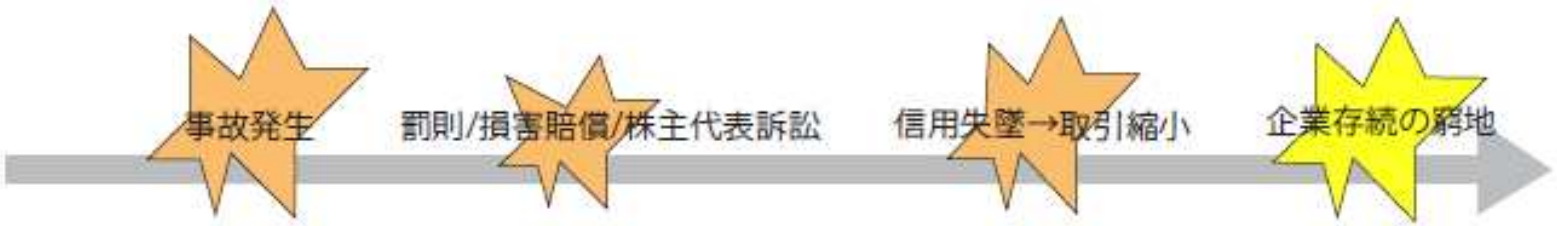
法令からの要求

個人情報保護法、大企業法、J-SOX 法等の法整備が整備されてきている昨今では IT 監査への対応も含め、企業と経営者にはより一層の**法令順守**が求められます

②情報セキュリティ強化を怠った場合の結果

情報セキュリティ対策を怠った結果としての代償は、**信用失墜と業績悪化**にまで波及し、企業を窮地に陥れる大きなリスクとなります。過去の情報事故とその影響の金額は、企業と経営者に事前の対策が必要であると認識させるに足る統計結果が出ております。

また、企業と社会に一番大きなインパクトを与えるのは**情報漏洩**であることは昨今の事例からも明らかです。



③情報漏洩を防ぐには

リスクの事前把握

情報漏洩リスクの把握は、まず情報資産の場所と漏洩を起こす要因を把握することが必要です。夫々サーバや端末に分散しているものの、**情報資産は利用の利便性のためにネットワーク上**に配置されていることは共通しています。この点から漏洩の最大リスクは、情報資産への**不正端末や不正ユーザによる不正アクセス**にあります。

リスクへの対策

つまり、上記のリスク排除のための処置としては不正アクセスを経路で断つという手段が必要です。つまり

「不正端末と不正ユーザからのネットワーク利用の遮断」

が必要になります。

④必要なソリューション

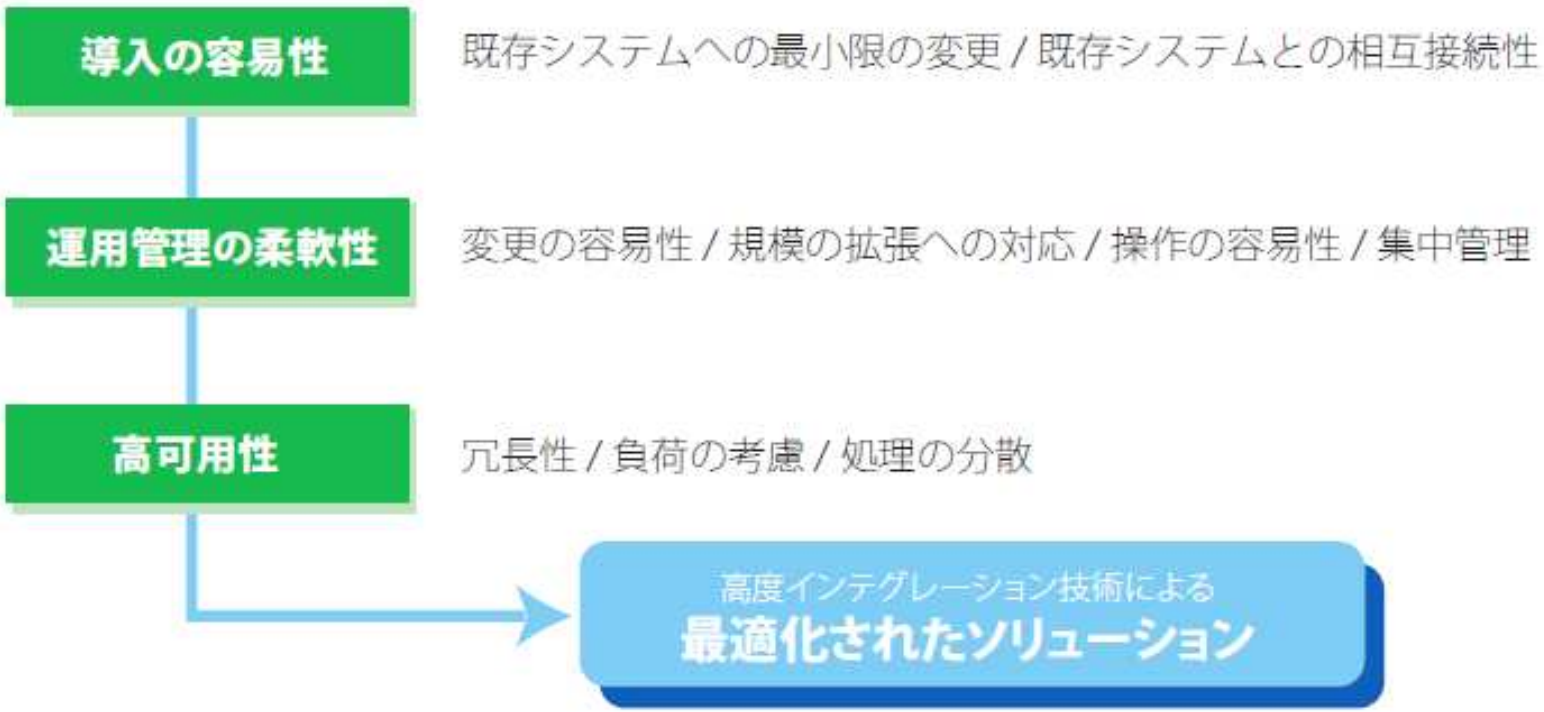
情報資産を不正端末と不正ユーザから守る

認証ネットワークの構築

AVAIL TECHNOLOGIES

ソリューションに必要な視点

お客様の既存環境とビジネスデマンド(事業要求)
を把握した上で最適化されたソリューションの提供



ネットワーク認証に用いられる認証方式の比較

以下の認証方式の組み合わせ、或いは既存認証システムとの組み合わせにより
最適化されたソリューションを提供します

①認証方式

MAC 認証 [端末認証]

「端末固有の MAC アドレスをスイッチが認証サーバと連携して
認証をおこなう方式」

- ユーザが認証を意識しない
- 端末環境に依存しない
- スイッチ毎の登録・管理が手間である
- MAC アドレスの詐称により違反が可能

→他の機構との組み合わせにより、セキュリティ強度が増強される

WEB 認証 [ユーザ認証]

「Web 認証は，Web ブラウザを使い，ユーザーにユーザー名と
パスワードの入力を求める認証方式」

- ブラウザさえあれば認証可能
- クライアントに特に設定は必要無い
- ユーザ ID の登録・管理のみで良い
- Windows 以外の OS(Machintosh や Linux など) にも対応可能

→ユーザ環境に依存せず、既存環境への変更も少ない為
Web サーバと制御する機構次第で非常に柔軟な認証
が可能

DHCP 認証 [端末認証]

「DHCP サーバとスイッチの連携で DHCP 要求の際の MAC アドレス
を中心とした情報を基に認証する方式」

- ユーザが認証を意識しない
- 端末環境に依存しない
- 認証前 VLAN を作成する必要がない
- DHCP サーバによる MAC アドレスの集中管理と認証が可能
- MAC アドレスの詐称が可能だが、DHCP サーバ上のログにより
スイッチ単独の認証と比較して発生源の究明が容易

→既存環境やスイッチへの手間がスイッチ単独の認証より軽減
される為、集中管理と非常に柔軟な認証が可能

802.1x 認証 [端末認証]

「サプリカントと呼ばれるクライアントソフトとスイッチ、
認証サーバが連携して認証を行う方式」

- 証明書による強固な認証が可能
- クライアントやスイッチに設定変更や管理が必要
- 証明書の管理の手間がある
- サプリカント対応のクライアントやスイッチが必要
- 末端の NW 機器まで 802.1X に対応している必要がある
- EAP-MD5/ EAP-TLS/ / EAP-TTLS /PEAP の方式の中から目的、
連携システムや機器によっての選定と統一が必要

→導入への障壁が多いが、既存環境が整っていて大規模なコスト
をかけられる前提では有効

②認証機構

認証 VLAN

上記認証方式の結果に応じて、認証前 VLAN と認証後 VLAN を割り当てる方式最も一般的な方式。1 つの VLAN 毎に予め同数の認証前 VLAN をスイッチ毎に設定 / 管理する必要がある

IP source guard

予め作成されたテーブル、また DHCPsnooping 機能により作成されたテーブルを基に、スイッチを経由する通信の通過と遮断を制御する機構

FW ポリシー制御

コントローラにより認証前ユーザと認証後ユーザの通信を様々な形態の外部認証サーバとの連携で通過、遮断制御をする機構。予め設定された FW ポリシーに基づいて制御する為、認証前 VLAN を作成する必要がなく、導入と運用の容易性に優れる

DHCPsnooping

スイッチと DHCP サーバ間でやりとりされるパケットをのぞき見 (snooping) することにより、スイッチ内部にテーブルを作成し、その後の通信制御に役立てる機能

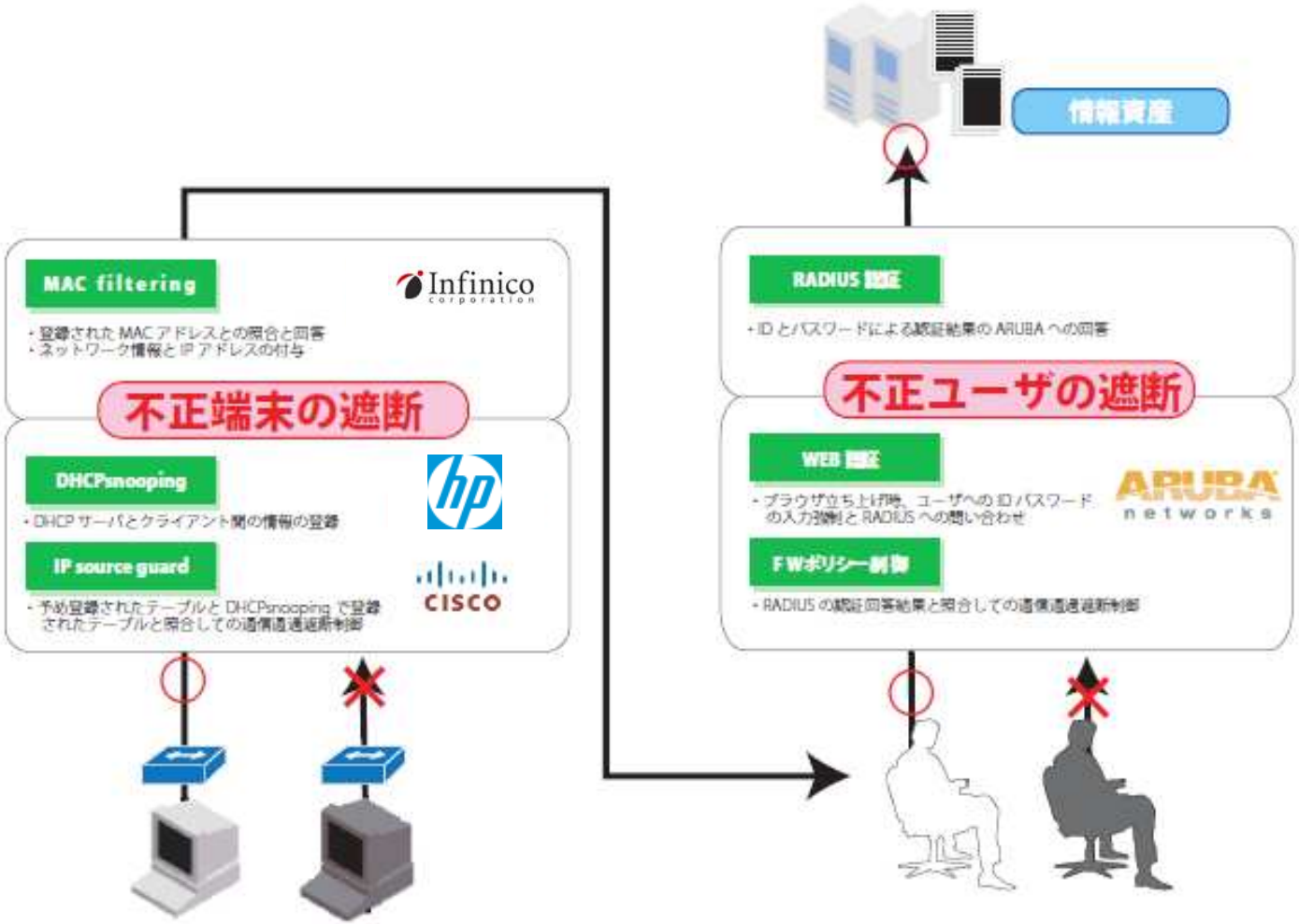
ソリューション例 ①

認証DHCPとWEBによるユーザ認証による
認証ネットワークソリューション
with ARUBA＆専用DHCP

中規模ユーザへの移行の容易性を重視した
ARUBAとInfinico社DHCPサーバの2製品を核とする
認証DHCP/WEB認証による機器(端末)と人の不正排除

AVAIL TECHNOLOGIES

認証の流れ



AVAIL TECHNOLOGIES

構成概要

ARUBA networks

・既存 RADIUS サーバを活かすために人の認証は WEB 認証をおこなうが、
　ARUBA は WEB 認証機能がある為、別途 WEB サーバを構築する必要がない
・FW ポリシーにより認証結果を受けての柔軟な通信制御が可能である
・既存 L3 への設定変更の軽減と負荷の分担ができる
・ARUBA は無線の速度とセキュリティ、管理に優れている
・大規模ユーザである為、コントローラでの制御により L2 スイッチと負荷分担できる

Infinico corporation

・柔軟な DHCP 割当てにより既存の固定 IP アドレスを使用機器のアドレスを継続利用できる
・L2 での MAC 認証と比較して固有機能の MACFilter 機能は集中管理に優れる
・冗長化構成を組むことができる稀有な DHCP アプライアンスである
・アプライアンス製品の為、機能に特化しておりスペックが高い

CISCO

・固定 IP による通信を予め登録された IP 以外は遮断する機能がある
・DHCP とクライアントでやりとりされた情報をもとに通信制御できる機能がある
・末端のスイッチは既存機器を利用する前提とする為その上位 L2 として上記機能が必要である

hp

AVAIL TECHNOLOGIES

ソリューション例 ②

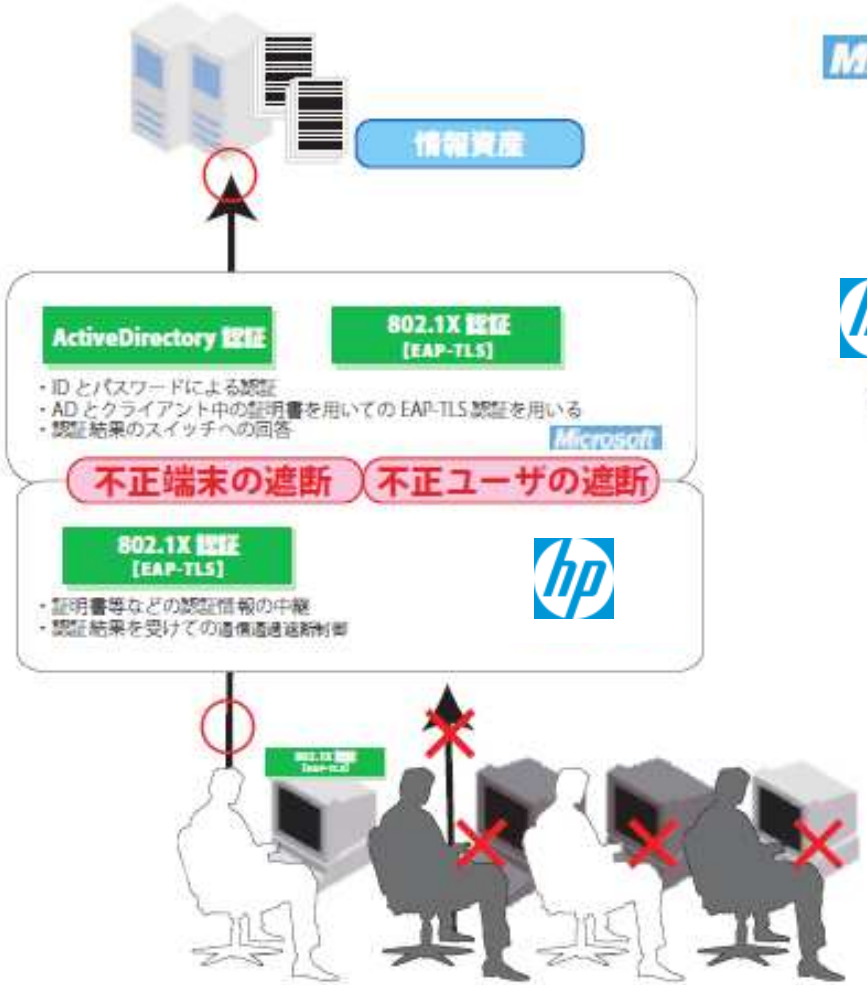
ActiveDirectory認証と802.1X認証による認証ネットワークソリューション

小規模ユーザへの集中管理と検疫システムの導入を見据えた
ActiveDirectory認証と802.1X認証の実現

既存環境と前提

◆従業員規模	50 名
◆物理編成	1 フロアに 50 名
◆既存認証システム	なし
◆端末環境	WindowsXP/Vista の混在環境
◆その他の要望	・情報システム部門不在の為、機器の数を最小限にしたい ・将来的には検疫システムを導入する予定

認証の流れ



構成概要

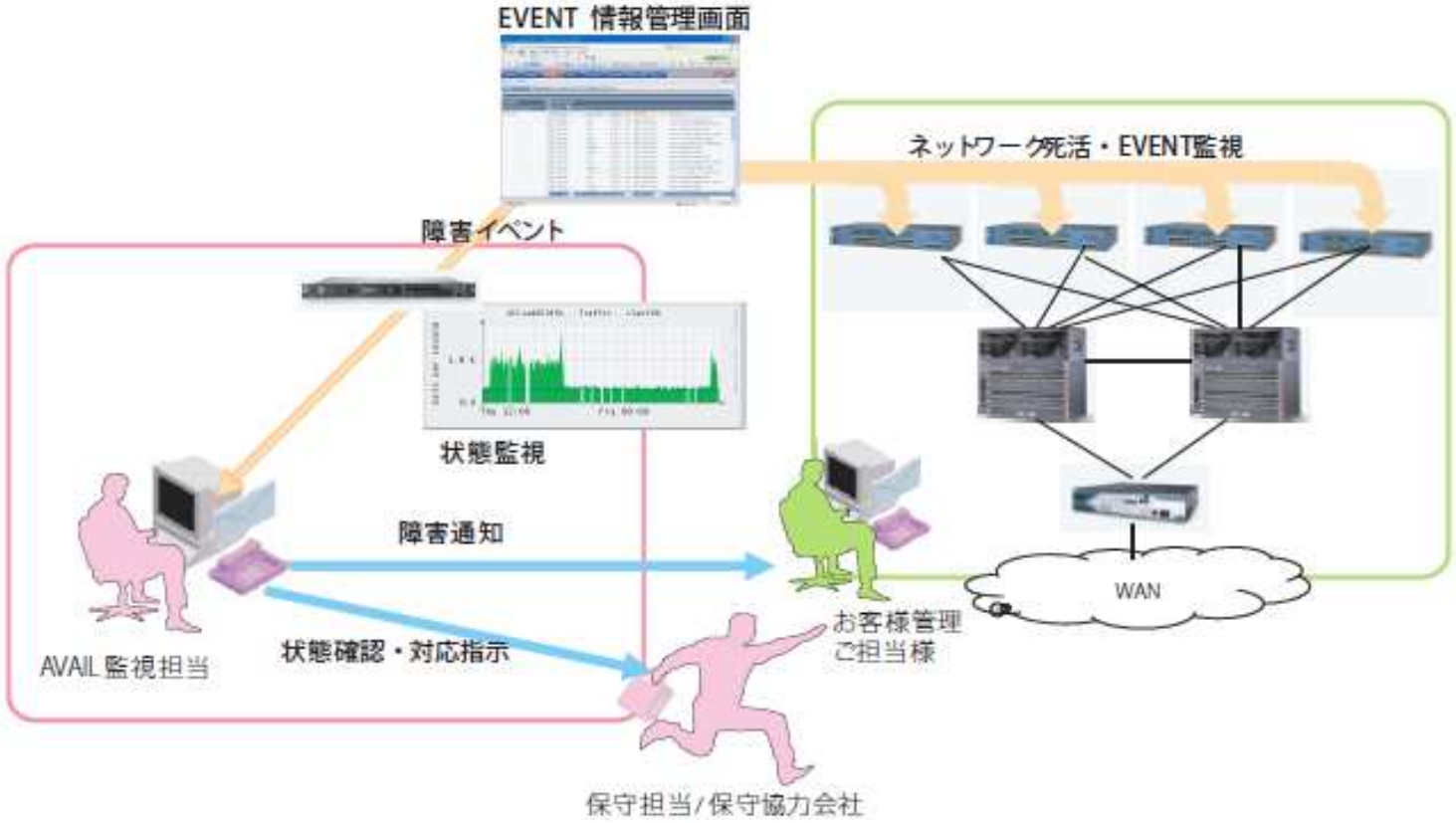
Microsoft

- 端末とユーザ認証の集中管理が可能
- 管理者に馴染みのある Window インタフェースが必要
- 証明書ベースの強固なセキュリティが可能
- AD とクライアント間の通信を考慮して認証方式は 802.1X の EAP-TLS を採用
- マイクロソフト社の NAP(検疫機構) との連携を視野に入れ Windows2008Server を用いる

- 末端まで 802.1X 認証に対応が必要である為、高性能かつ経済的な機器が必要である

保守/ 監視サービス

導入後もLinuxベースによる独自の遠隔監視システムとオンサイト保守サービス
で認証ネットワークシステムの安定稼働に寄与します

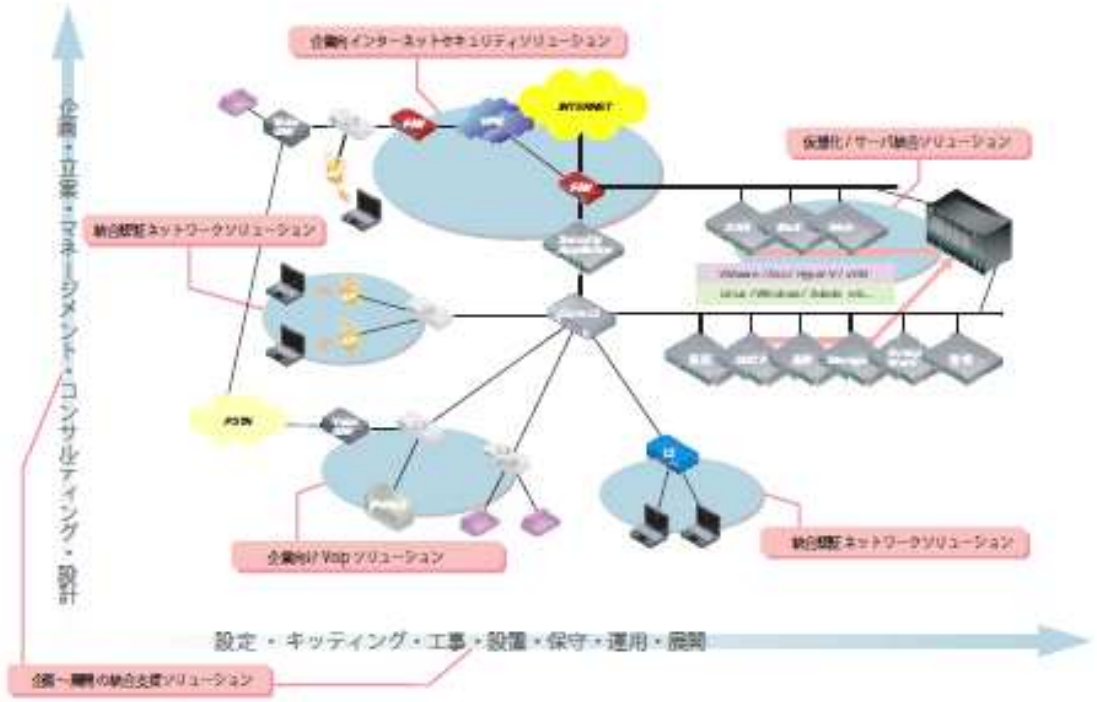


導入後の展開

◆当社の事業領域は認証ネットワークソリューションに限らず、企業の情報基盤全体にまたがった先進のテクノロジーを提供しています。

認証ネットワークを基盤とした展開

- ARUBAによる無線LAN統合認証ネットワーク構築
- MicrosoftのNAPによる検疫ネットワーク構築
- 仮想化技術によるサーバ統合システム構築
- Voipによる音声統合システム構築



サービス内容に関するご質問やご依頼は
お気軽にご相談ください。

アヴェイルテクノロジ株式会社
営業部
〒105-0004
東京都港区新橋5-7-9 東信ビル2F
TEL:03-6430-3310　FAX:03-6430-3318