

デジタル証明書認証を**簡単に**導入する クラウド管理型 Wi-Fi／VPN認証サービス

株式会社 ソリトンシステムズ
2021年 5月

Soliton[®]



Security White Paper

400 社アンケートから読み解く

無線 LAN を導入する企業が 攻略すべき「たった一つ」の課題

企業における新たな取り組みは「安心・安全の無線ネットワーク」を前提とします。
日々の業務に欠くことのできない無線 LAN は、その便利さの反面、ひとたび対応を
誤ると深刻なセキュリティ事故にも直結します。
企業が無線 LAN を導入・検討する際に絶対に外してはいけないポイントとは？
400 社の情報システム担当者へのアンケート結果を紐解きつつ、企業無線 LAN の
"あるべき姿"を解説します。

© Soliton Systems K.K., All rights reserved.

400 社アンケートから読み解く！ これから無線LANを導入する企業が攻略すべき 「たったひとつ」の課題

無線LANを導入できた企業と、できなかった企業では何が違うのか。

情報システム部門400名へのアンケート結果 から見えてきた課題と、
それを解決する方法について解説します。

無線LANの導入を検討中の方はもちろん、お客様に無線LANを
提案する方にもぜひ一読いただきたいホワイトペーパーです。

ホワイトペーパー

これから無線LANを導入する企業が攻略すべき「たったひとつ」の課題

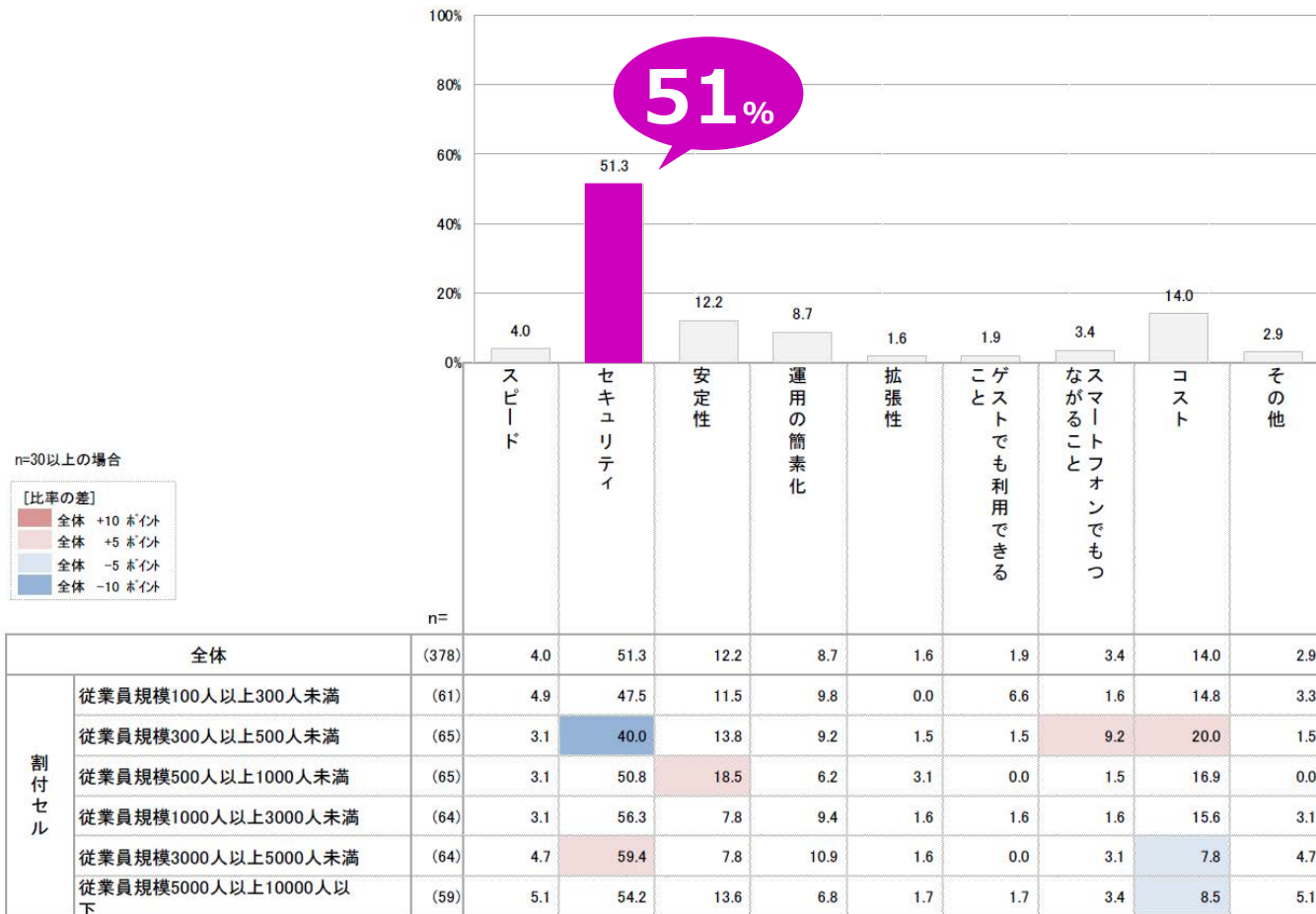
 <https://www.soliton.co.jp/special/WirelessSecurity.html>

ホワイトペーパー

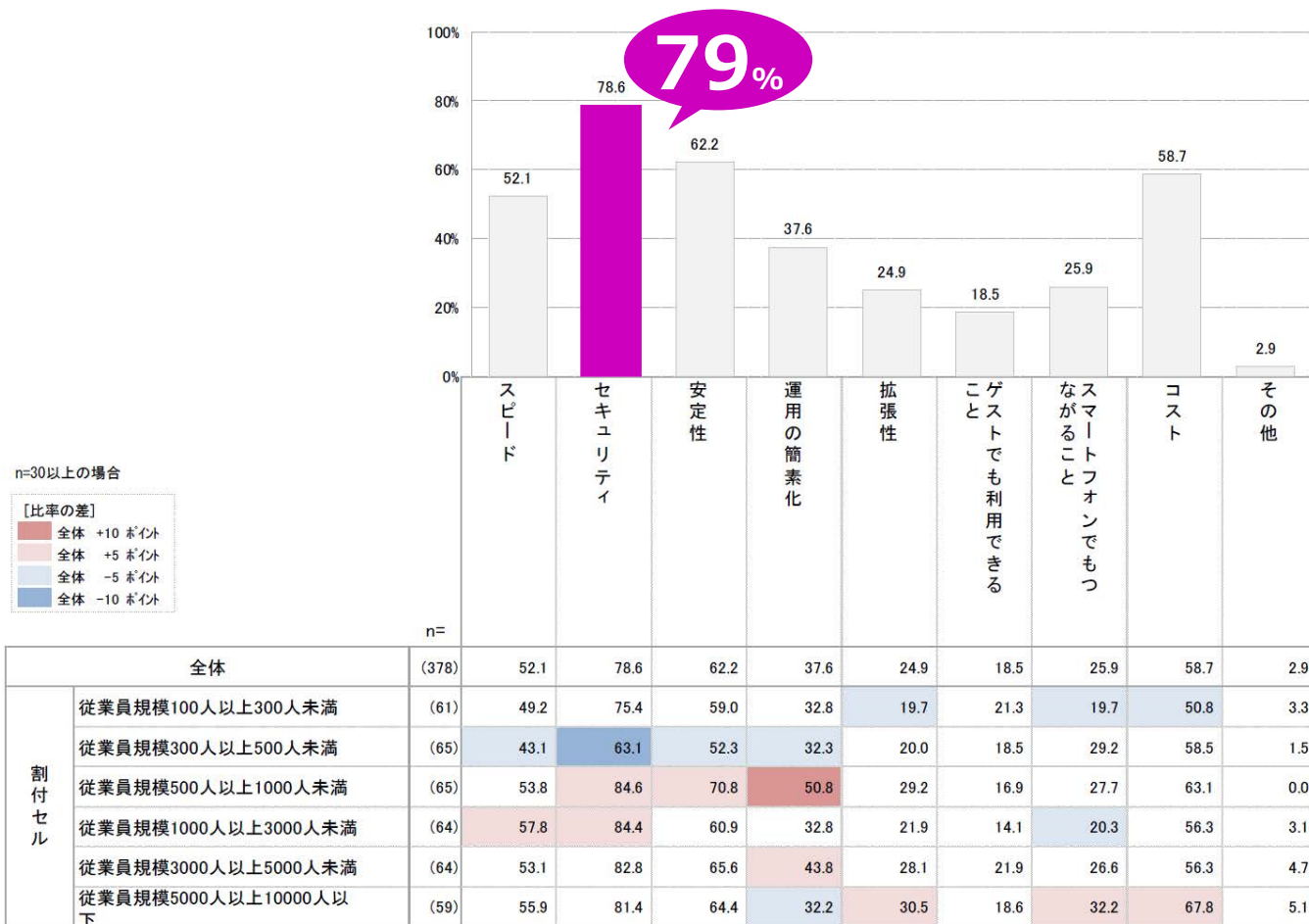
MACアドレス制限は"効果ゼロ" 今さら聞けない「無線LAN認証」の基本

 <https://www.soliton.co.jp/special/WirelessAuth.html>

【設問】無線LAN導入時に最も考慮した点は？（あてはまるものをひとつお選び下さい）

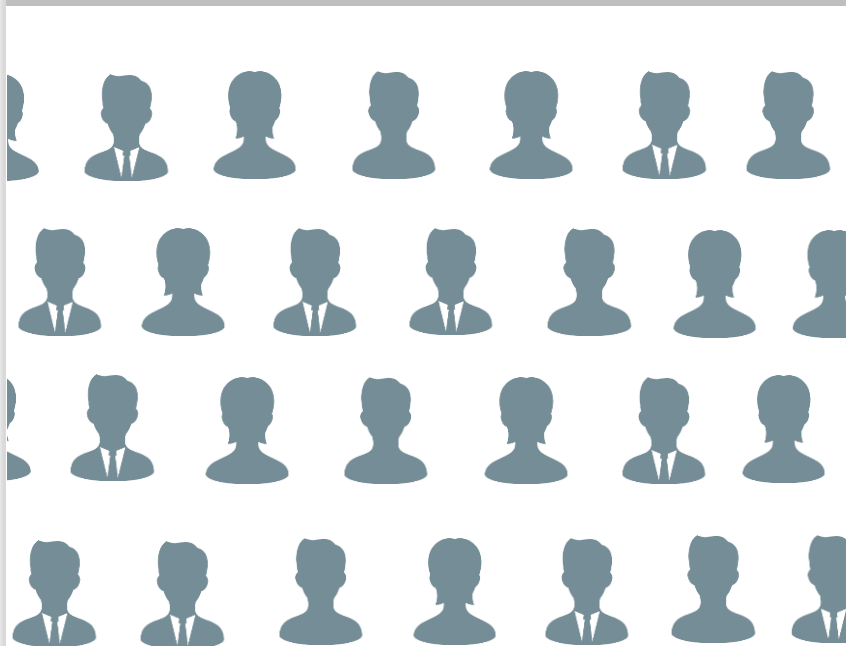


【設問】無線LAN導入時に考慮した点は？（あてはまるものをすべてお選び下さい）



(()) 不正接続に、気づけるか・・・？

隣接するオフィス、来訪者



執務室内

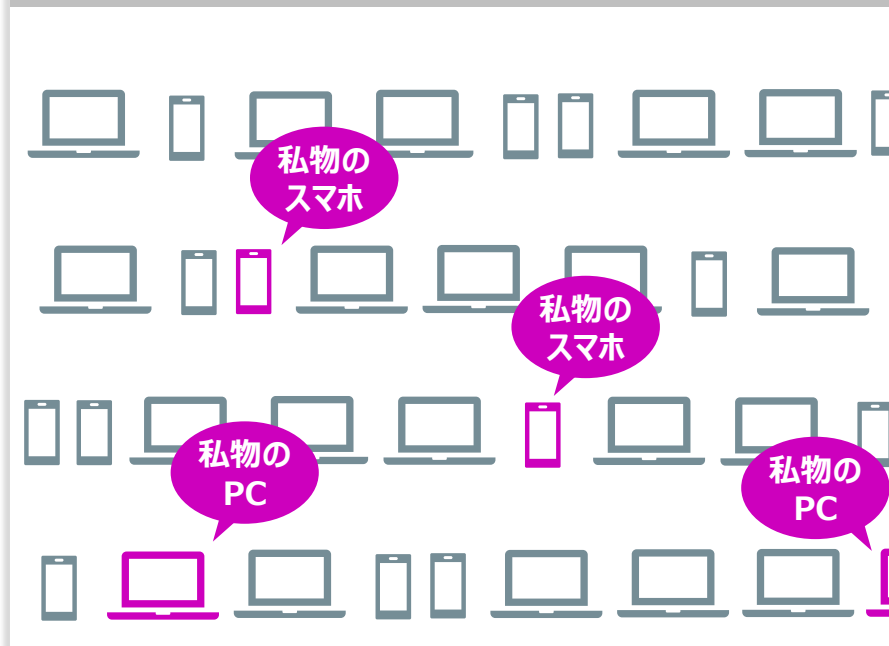


(()) 不正接続に、気づけるか・・・？

隣接するオフィス、来訪者



執務室内



見えないところでLAN利用・・・ 情報流出リスクが一気に増加

認証方式 ～パーソナルとエンタープライズの違い

新しいネットワークの追加

ネットワーク名

WIRELESS

セキュリティの種類

開く

WEP

WPA2-パーソナル AES

WPA2-エンタープライズ AES

802.11x WEP

保存 キャンセル

AP + 共通のパスフレーズ

- PSK（Pre-Shared Key）と呼ばれる、共通のパスフレーズで認証する方式
- SSIDとPSKを指定するだけで手軽に利用でき、家庭向けの無線で広く普及

AP + 認証サーバー

- ユーザーやデバイスを外部の認証サーバを使って認証する方式
- 利用者毎に異なる ID・パスワードや、デジタル証明書を用いる

企業でのPSK認証は危険 !?

PSK認証は

- **パスワードが外部に漏洩** する危険性がある
- 総当たり攻撃（Blute Force Attack）等により、**パスワードを窃取される危険性**もある
- そのため、**定期的なパスワードの更新が必須**となる
- 万が一、**パスワードが漏洩した場合**には、全利用端末のPSKを再設定

企業等が安心して
無線LANを導入・運用するために

総 務 省
平成25年1月30日

MACアドレス制限は効果ゼロ

来客スペースで、Wireshark を開けば・・・



No.	Time	Source	Destination	Protocol	Info
459	1.658598	30:75:12:...	ff:ff:ff:ff:ff:ff	IEEE 802.11	Unrecognized (Reserved frame)
460	1.658601	cc:e1:d5:...	cc:e1:d5:...	IEEE 802.11	Probe Request, SN=872, FN=...
461	1.658603	b0:c7:45:...	cc:e1:d5:...	IEEE 802.11	Clear-to-send, Flags=...
462	1.658819	b0:c7:45:...	cc:e1:d5:...	IEEE 802.11	802.11 Block Ack, Flags=...
463	1.659497	b0:c7:45:...	cc:e1:d5:...	IEEE 802.11	802.11 Block Ack, Flags=...
464	1.659803	4b:45:21:...	c7:02:0e:...	IEEE 802.11	CF-End + CF-Ack (Control frame)
465	1.660971	30:75:12:...	ff:ff:ff:ff:ff:ff	IEEE 802.11	Probe Request, SN=873, FN=...
466	1.661240	b0:c7:45:...	60:6d:c7:...	IEEE 802.11	802.11 Block Ack, Flags=...
467	1.661566	f6:11:cf:...	46:33:eb:...	IEEE 802.11	Unrecognized (Reserved frame)
468	1.661568	0a:ed:b9:...	30:75:12:...	IEEE 802.11	802.11 Block Ack, Flags=...
469	1.669787	0a:ed:b9:...	30:75:12:...	IEEE 802.11	Probe Response, SN=2149, FN=...
470	1.673639	0a:ed:b9:...	30:75:12:...	IEEE 802.11	Probe Response, SN=2149, FN=...
471	1.677412	0a:ed:b9:...	30:75:12:...	IEEE 802.11	Probe Response, SN=2149, FN=...
472	1.681203	0a:ed:b9:...	30:75:12:...	IEEE 802.11	Probe Response, SN=2149, FN=...
473	1.682552	f6:2b:1f:...	80:61:a5:...	IEEE 802.11	Null function (No data), SN=...
474	1.683148	cc:e1:d5:...	cc:e1:d5:...	IEEE 802.11	Clear-to-send, Flags=...
475	1.684234	b0:c7:45:...	cc:e1:d5:...	IEEE 802.11	802.11 Block Ack, Flags=...
476	1.684663	f2:12:99:...	65:6b:0a:...	IEEE 802.11	Power-Save poll, Flags=...
477	1.686005	53:d1:75:...	53:d1:75:...	IEEE 802.11	Clear-to-send, Flags=pm.R.
478	1.687928	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff	IEEE 802.11	Beacon frame, SN=1107, FN=...

Frame 13 (426 bytes on wire, 426 bytes captured)
Radiotap Header v0, Length 26
IEEE 802.11 Probe Response, Flags:C
Type/Subtype: Probe Response (0x05)
Frame control: 0x0050 (Normal)
Duration: 60
Destination address: 5c:e0:c5: (5c:e0:c5:)
Source address: 0a:ed:b9: (0a:ed:b9:)
BSS ID: 0a:ed:b9: (0a:ed:b9:)
Fragment number: 0

0000 00 00 1a 00 6f 18 00 00 95 7f 47 4a 6e 65 f2 d4 ... 0GJne.
0010 10 0c 85 09 c0 00 d2 ac 00 26 50 00 3c 00 5c e0&P.<.
0020 c5 f0 a5 5a 0a ed b9 8a 35 35 0a ed b9 8a 35 35 ... Z 55 ... 55
0030 00 85 e1 21 3c fd 02 00 00 64 00 11 05 00 15 ... !< ... d ...
0040 44 49 52 45 43 54 2d 6c 49 4d 4d 53 52 41 53 45 DIRECT-1 ...
0050 21 64 22 54 43 51 08 8e 13 08 14 b9 46 60 0c 02 ... 6 ... 02

Frame (frame), 426 bytes Packets: 3910 Displayed: 3910 Marked: 0 Dropped: 0 Profile: Default

MACアドレスは

- 通信相手に積極的に開示される情報であり、隠されていません
- 通信が暗号化されている無線LANでも、MACアドレスは暗号化の範囲に含まれません
- 電波が届くエリアであれば、キャプチャは簡単
- 突破され、LANに侵入されるケースは多数、報告されている

MACアドレス制限は効果ゼロ

a1:b1:c1:d1:e1:f1:11:22



ソフトウェアの
値が使われる

ソフトウェア (OS)

aa:bb:cc:dd:ee:ff:11:22

偽装

a1:b1:c1:d1:e1:f1:11:22

比較的
容易に
偽装できる

ハードウェア (NIC)

aa:bb:cc:dd:ee:ff:11:22

偽装は困難



認証方式 ～パーソナルとエンタープライズの違い

新しいネットワークの追加

ネットワーク名

WIRELESS

セキュリティの種類

開く

WEP

WPA2-パーソナル AES

WPA2-エンタープライズ AES

802.11x WEP

保存 キャンセル

AP + 共通のパスフレーズ

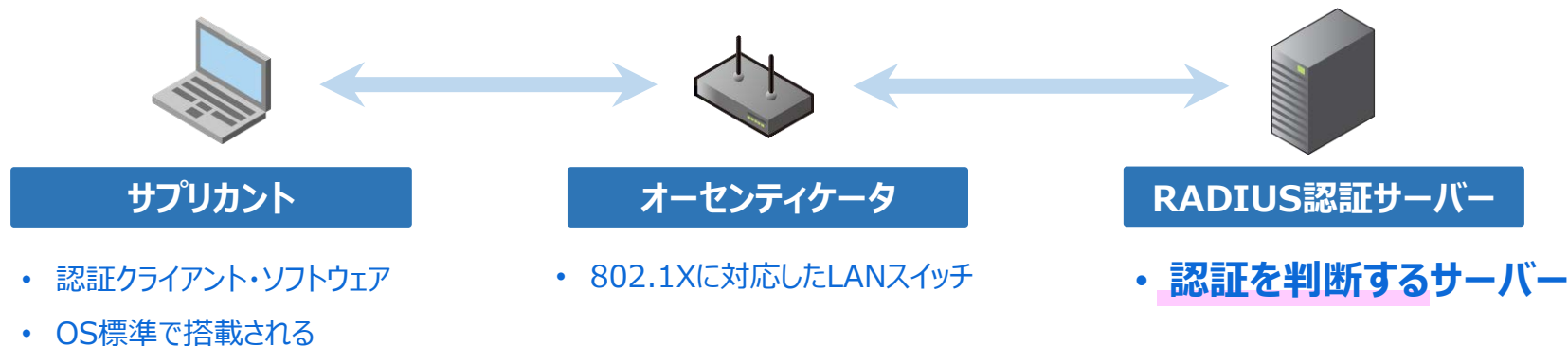
- PSK (Pre-Shared Key) と呼ばれる、共通のパスフレーズで認証する方式
- SSIDとPSKを指定するだけで手軽に利用でき、家庭向けの無線で広く普及

AP + 認証サーバー

- ユーザーやデバイスを外部の認証サーバを使って認証する方式
- 利用者毎に異なる ID・パスワードや、デジタル証明書を用いる

IEEE802.1X

- ☑ LAN接続時に使用する認証規格。
- ☑ 接続を認めた端末機器以外がコンピュータネットワークに参加しないように、認証によって接続を規制する。



どのように「認証を判断」するか？

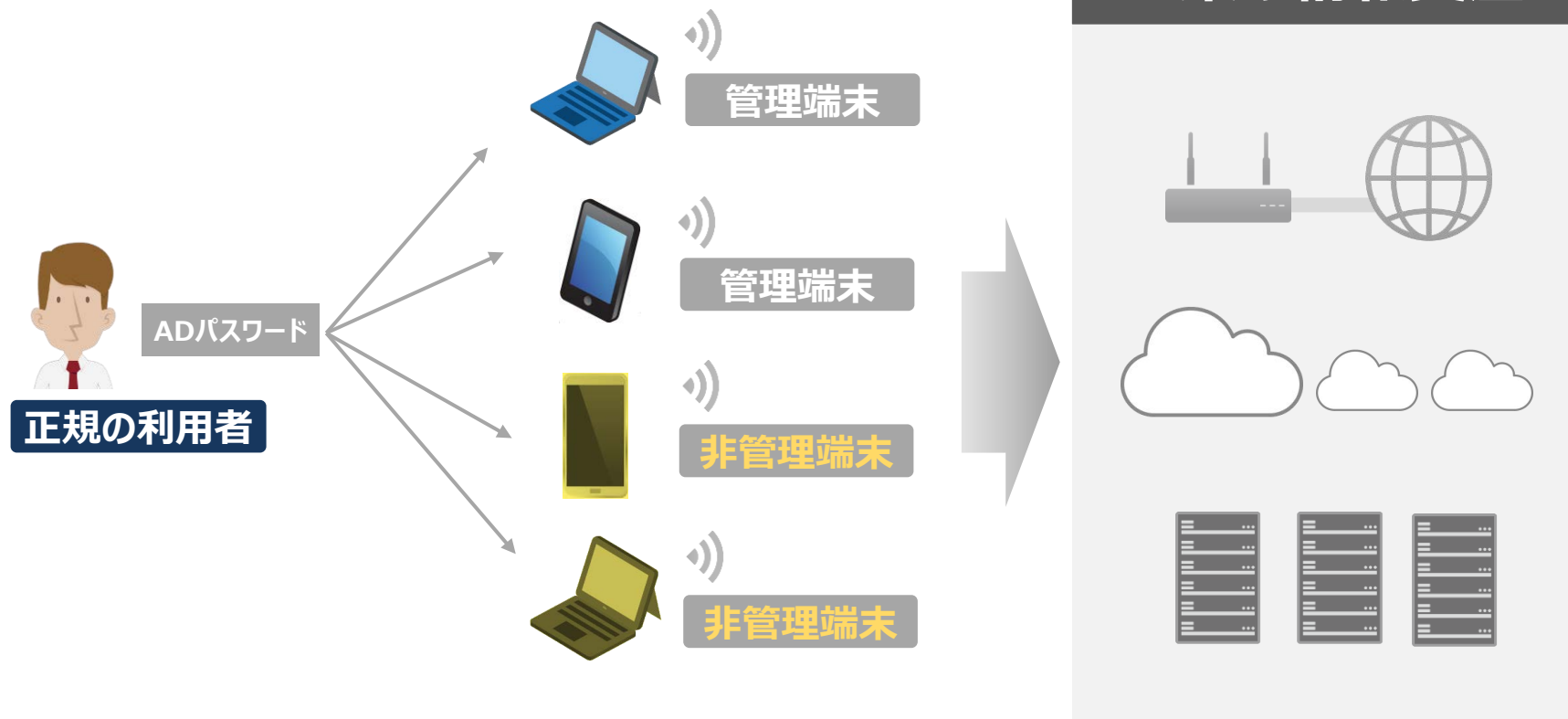
利用者が記憶するパスワードで判断

ユーザーIDとパスワードで認証する、EAP-PEAP認証方式。
サブリカントでADアカウントを使ったSSO設定も可能であるが...

Something you know



PEAP認証方式の課題



非管理端末でも、業務情報にアクセスできダウンロードできてしまう。

利用者が記憶するパスワードで判断

ユーザーIDとパスワードで認証する、EAP-PEAP認証方式。

端末の特定ができず、シャドーITからの情報漏洩リスクが・・・

Something you know



クライアントのデジタル証明書で判断

クライアント証明書で認証する、EAP-TLS認証方式。

利用端末を特定でき、スマートデバイスの接続制御にも最適。

Something you have



デジタル証明書が入った **許可端末だけ** がつながる

許可端末



許可端末



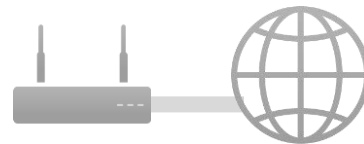
非管理端末



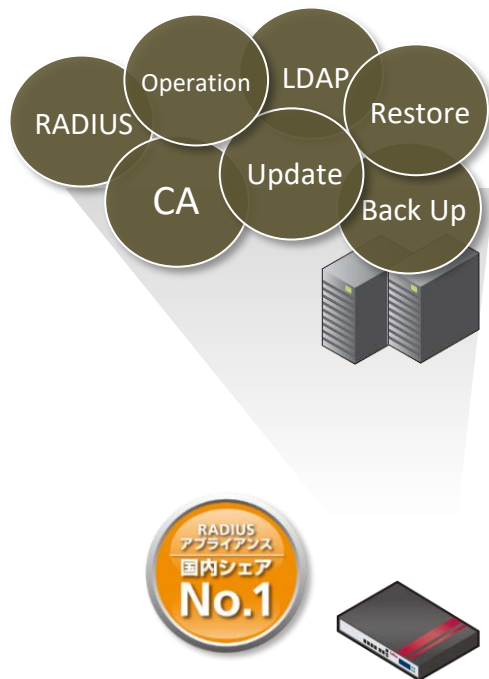
非管理端末



企業の情報資産



認証サーバーの導入は大変？



社内でRADIUSサーバーを構築



NetAttest EPS



導入工数は
1/2 以下に！



NetAttest EPS



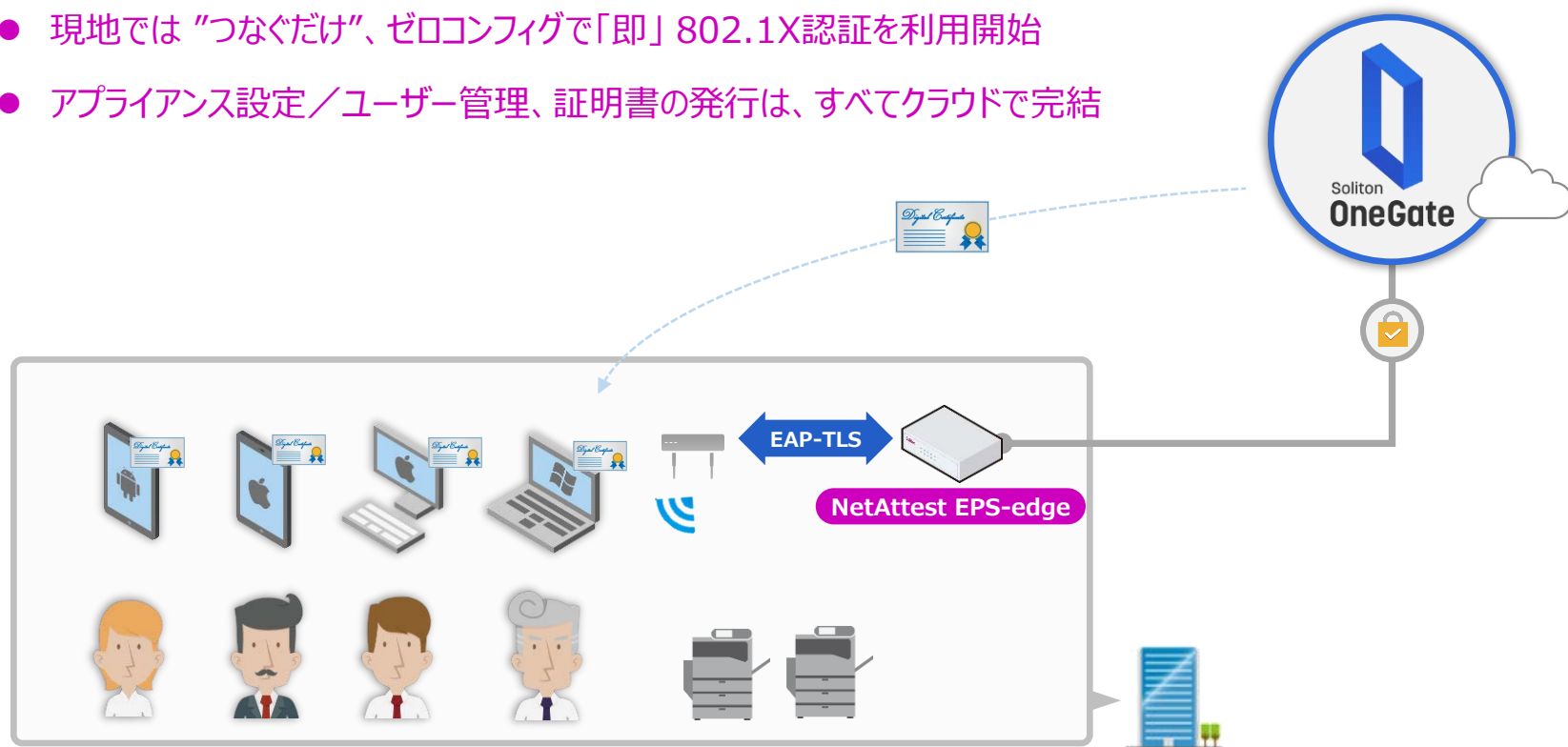
- 高度なネットワーク認証環境を短期間で構築
- 国内シェアNo.1、16年間の販売実績
- 壊れにくく、安定稼働、サポートも安心
- 万一の時も短時間で復旧・稼働
- 多くのVPN機器、有線・無線LAN機器との連携実績
- クラウド管理型 & ゼロコンフィグで運用負荷も抑えたい

➡ “EPS-edge” をラインナップ



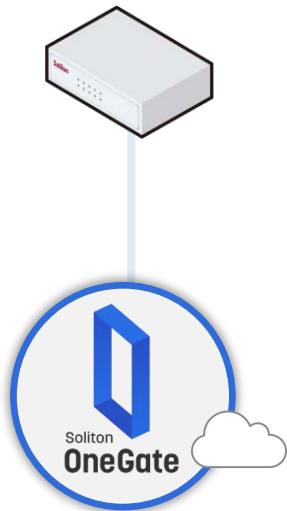
無線LANやVPNを不正侵入から守る Wi-Fi／VPN認証サービス

- 現地では “つなぐだけ”、ゼロコンフィグで「即」802.1X認証を利用開始
- アプライアンス設定／ユーザー管理、証明書の発行は、すべてクラウドで完結



ゼロコンフィグだから、これだけ

NetAttest EPS-edge



● ネットワークケーブルを接続

電源を入れるとクラウドに接続（DHCPでIPアドレスを取得して、自動接続）



● クラウド管理画面で、アプライアンス登録

本体シールの登録コードを入力、あとは自動でアクティベート

新しいアプライアンスの追加

登録コード *

例 : aB0123456789

※ 本体のシールに記載の12桁の登録コード(REG)を入力してください。

自動承認

☐ 管理者による承認を省略する

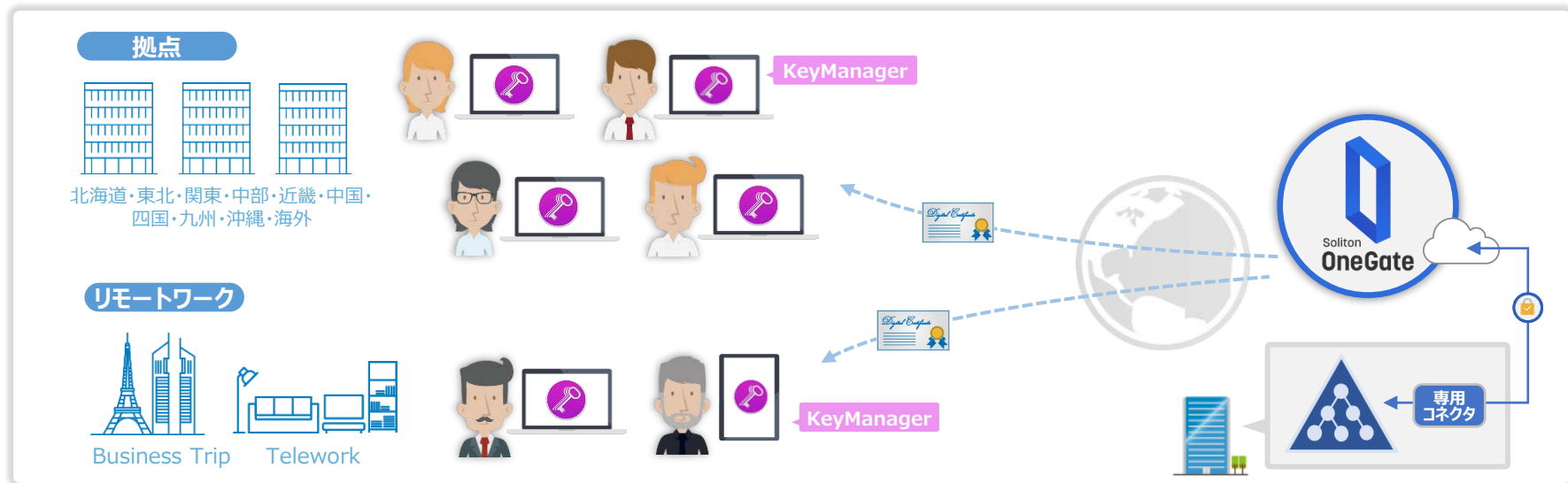
※ アプライアンスの接続後、承認なしで登録処理を完了させる場合はチェックしてください。

追加

キャンセル



インターネット経由でデジタル証明書を安全配布



マルチOS対応

全OS同じ手順で
デジタル証明書を取得

利用者も管理者も低負担

ブラウザの設定やActiveXは不要
ヘルプデスク工数ほぼゼロ

不正コピーが一切できない※

不正接続を許さない仕組みで
リモートワークを促進



- 証明書管理画面

[利用者管理](#)
[クラウド設定](#)
[AD設定](#)
[証明書管理](#)
[アプライアンス管理](#)
[同期スケジュール設定](#)
[システム設定](#)
[ログ管理](#)
[admin](#)

証明書管理 > 招待コード管理

[発行](#)
[失効](#)
[CA情報](#)
[招待コード管理](#)
[証明書一覧](#)
[証明書ログ](#)
[すべて](#)

☐ すべて選択

[表示順序](#)
[発行日時\(降順\)](#)
[前へ](#) | [1 - 7 / 7](#) | [25](#), [50](#), [100](#) | [次へ](#)

☐	発行済み	堀江 麻子	招待コード: h5mtHJ 発行者: admin 発行日時: 2020/07/07 12:07:19
☐	発行済み	Nico Leon	招待コード: 2aeJE9 発行者: admin 発行日時: 2020/07/06 17:54:13
☐	使用済み	鷗木 彩	招待コード: FIFKa 発行者: admin 発行日時: 2020/07/03 12:05:29
☐	発行済み	植田 淳平	招待コード: QN9ifo 発行者: admin 発行日時: 2020/07/03 12:02:36
☐	失効済み	竹吉 健	招待コード: ie5nXL 発行者: admin 発行日時: 2020/07/03 11:39:34 失効日時: 2020/07/03 11:39:41
☐	発行済み	岩田 宗次	招待コード: 90OeSL 発行者: admin 発行日時: 2020/07/03 11:39:28
☐	使用済み	中村 知倫	招待コード: gZPXkp 発行者: admin 発行日時: 2020/07/03 11:39:21

発行された招待コード
「h5mtHJ」

[最初](#) [前へ](#) [1](#) [次へ](#) [最後](#)

デバイス紛失時は、ADユーザー名と
デバイスOS種別を素早く確認

証明書管理 > 証明書一覧

失効

紛失したデバイスだけ「失効」

すべて ▾

検索キーワードを入力して下さい。

☐ すべて選択 | 表示順序 開始日時(降順) ▾

前へ | 1 - 8 / 8 | 25, 50, 100 | 次へ

☐	アプライアンス	500SL50050 CN=500SL50050	シリアル番号: 8 (0x8) 開始日時: 2020/07/07 17:45:32 終了日時: 2021/07/07 17:45:32 発行元: release-1-2-0 発行先: SOGRO-SX15-A
☐	アプライアンス	500SL50050 CN=500SL50050	シリアル番号: 7 (0x7) 開始日時: 2020/07/07 17:45:29 終了日時: 2021/07/07 17:45:29 発行元: release-1-2-0 発行先: SOGRO-SX15-A
☐	利用者	堀江 麻子 CN=ahorie	シリアル番号: 6 (0x6) 開始日時: 2020/07/06 10:24:23 終了日時: 2021/07/06 10:24:23 発行元: release-1-2-0 発行先: Windows SKM
☐	利用者	堀江 麻子 CN=ahorie	シリアル番号: 5 (0x5) 開始日時: 2020/07/06 10:23:55 終了日時: 2021/07/06 10:23:55 発行元: release-1-2-0 発行先: Android SKM
☐	利用者	中村 知倫 CN=tnakamura	シリアル番号: 4 (0x4) 開始日時: 2020/07/03 18:24:59 終了日時: 2021/07/03 18:24:59 発行元: release-1-2-0 発行先: Windows SKM
☐	利用者	鷺木 彩 CN=aunoki	シリアル番号: 3 (0x3) 開始日時: 2020/07/03 16:30:12 終了日時: 2021/07/03 16:30:12 発行元: release-1-2-0 発行先: iPad OS Safari
☐	利用者 失効済み	岩田 宗次 CN=siwata	シリアル番号: 2 (0x2) 開始日時: 2020/07/03 12:05:57 終了日時: 2021/07/03 12:05:57 発行元: release-1-2-0 発行先: Mac SKM
☐	利用者	Nico Leon CN=nleon	シリアル番号: 1 (0x1) 開始日時: 2020/07/03 12:02:02 終了日時: 2021/07/03 12:02:02 発行元: release-1-2-0 発行先: iPad OS Safari

証明書発行時に
OS種別を自動記録

発行はもちろん、失効も素早く、円滑

Wi-Fi／VPN認証サービス (NetAttest EPS-edge) の機能について

● RADIUSサーバー機能

- クラウド上で管理されたアカウント情報を使って、無線LAN認証（EAP-TLS）、VPN認証（PAP）
- RADIUSサーバーは、複数台設置する事で負荷分散、障害対策などに柔軟に対応
（RADIUSクライアント側で複数のRADIUSサーバーを指定）
- RADIUSクライアント数の制限はありません

モデル	SOGRO-SX15-A
アプライアンス名	NetAttest EPS-edge
アプライアンス利用料	初期費用：8万円／台 月額費用：5,000円／台
外形寸法 (W×H×D)	165mm × 43mm × 106mm
重量	0.65kg
電源	90～264Vac、47～63Hz（90～135Vacのみサポート）
最大消費電力	22VA
発熱量	75BTU/h、18.9lcal、22W
動作環境	温度0～40℃、湿度20～90%RH結露なきこと



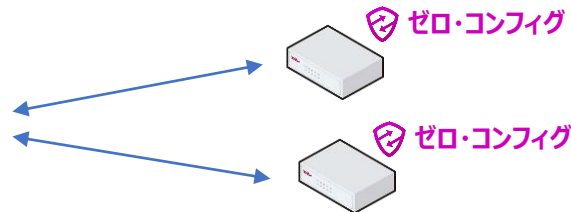
NetAttest EPS-edge

● クラウド上の管理機能

- ユーザー情報の一元管理（社内AD同期）
- EPS-edgeアプライアンスの管理
 - オンライン・アクティベーション
 - ログ管理
 - ステータス確認
 - ファームウェアアップデート



ユーザーとアプライアンスの管理



RADIUS認証サービス

認証局を簡単運用
安全なデジタル
証明書発行



強固なEAP-TLS認証
不正利用を防止



MIST Wi-Fi

802.1X



NetAttest EPS-edge



AIで自動運用
遅い・繋がらない
を解消

Mist
A Juniper Company



Soliton
OneGate

Cloud



食品加工メーカー、設備工事会社など
オフィスレイアウトの見直しにも最適



1 ID・認証管理の自動化を支援



クラウドID管理を自動化
デジタル証明書の運用支援

2 クラウドをまとめて 多要素認証



M365など業務サービスに
デジタル証明書 + FIDO2認証

3 オフィスWi-Fi／VPNを堅牢にする

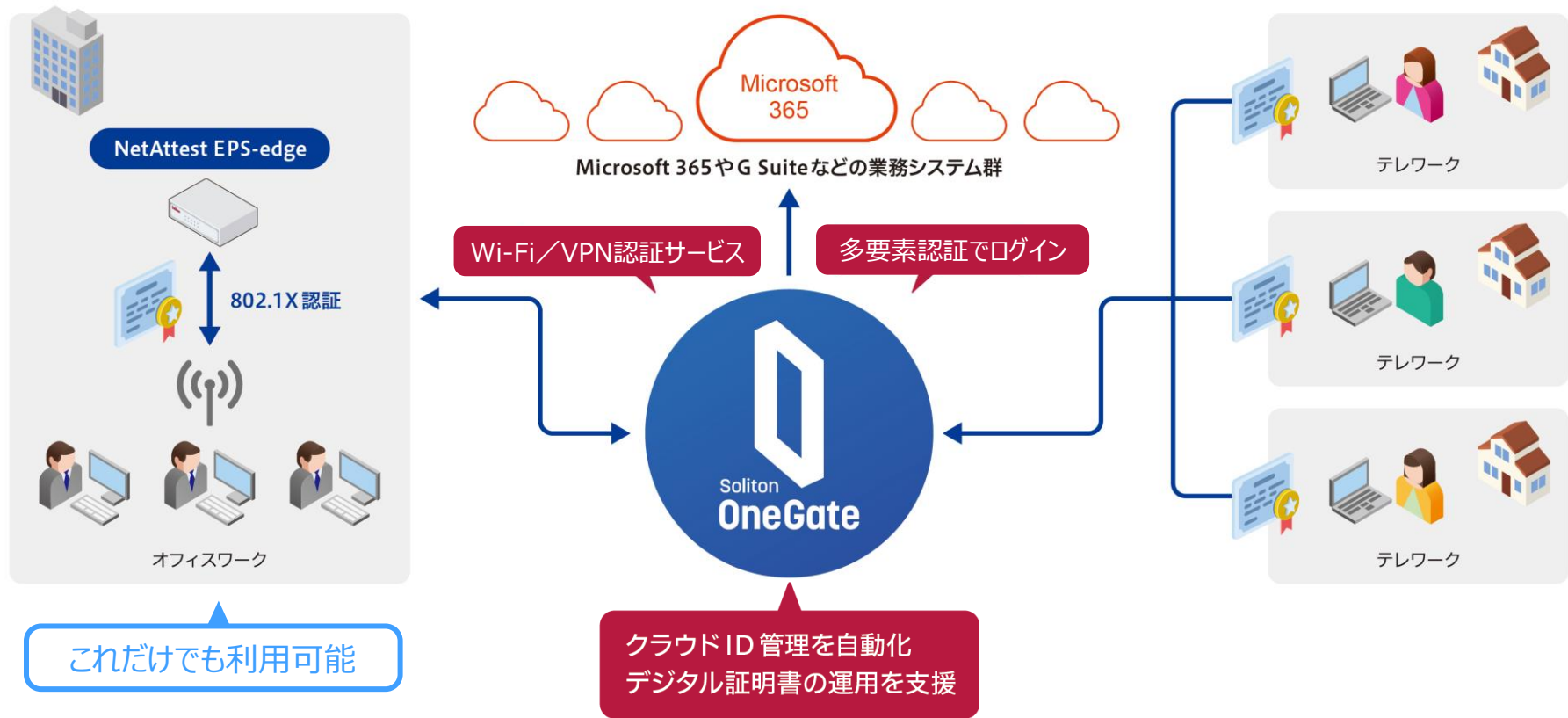


ゼロコンフィグのEPS-edgeで
802.1X認証を手早く導入

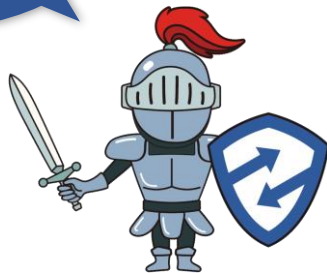
4 社内システムも パスワードレス



デジタル証明書対応
PC・スマホで動く代理認証アプリ



EPS-edgeの
無料トライアル
も可能



資料のダウンロード、トライアル申込は

ソリトンワンゲート

検索

株式会社 ソリトンシステムズ

〒 160-0022 東京都新宿区新宿 2-4-3

TEL 03-5360-3811 netsales@soliton.co.jp

大阪営業所	06-7167-8881	福岡営業所	092-263-0400
名古屋営業所	052-217-9091	東北営業所	022-716-0766
札幌営業所	011-242-6111		