NRA-PKIのご紹介

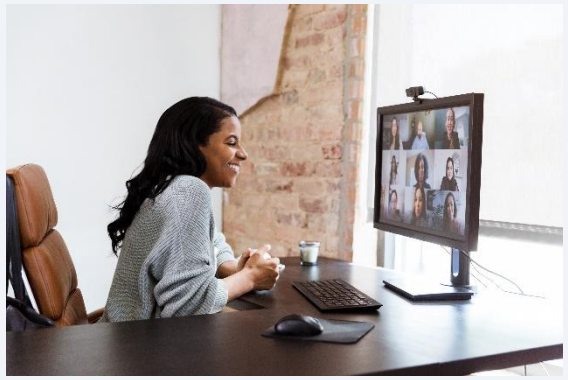
いつでもどこでもセキュアなアクセスを実現

日本RA株式会社

インターネットとスマートデバイスの普及による環境の変化

誰もが働きやすい環境・新しいワークスタイルの実現

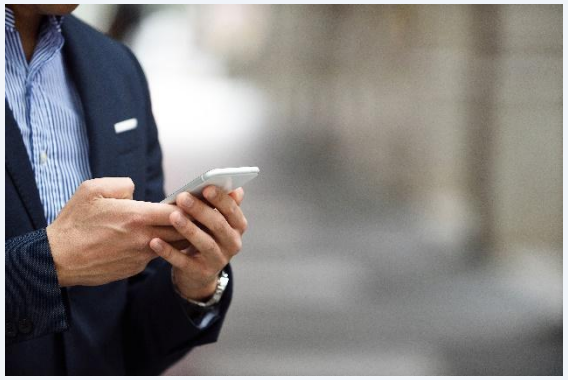
コミュニケーションの活性化



場所を選ばない働き方

ワークライフバランス

生産性の向上



NRA

情報セキュリティ10大脅威 2022

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	**1位**	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	**2位**	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**3位**	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	**4位**	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	**5位**	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	**6位**	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	**7位**	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	**8位**	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	**9位**	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	**10位**	不注意による情報漏えい等の被害	9位

出典：IPA「情報セキュリティ10大脅威 2022」

ランサムウェアによる被害、攻撃手口一例

ソフトウェアの脆弱性を未対策のままインターネットに接続されている機器に対して、その脆弱性を悪用してインターネット経由で感染させる

不正アクセスによる認証情報の窃取、正規の経路で組織内部に侵入

<情報セキュリティ対策の基本>

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する

NRA

ランサムウェア被害事例（徳島県半田病院）

2021年10月、徳島県の半田病院がランサムウェアの感染によって、
約8万5,000人分の電子カルテや会計システムにアクセスできなくなる被害を受けた。
同病院は**身代金を支払わずに２億円でシステムの再構築**を行い、復旧までの約2ヶ月間、
一部の診療科で新規患者の受け入れを中止する等の影響があったが、
2022年1月、通常診療を再開した。

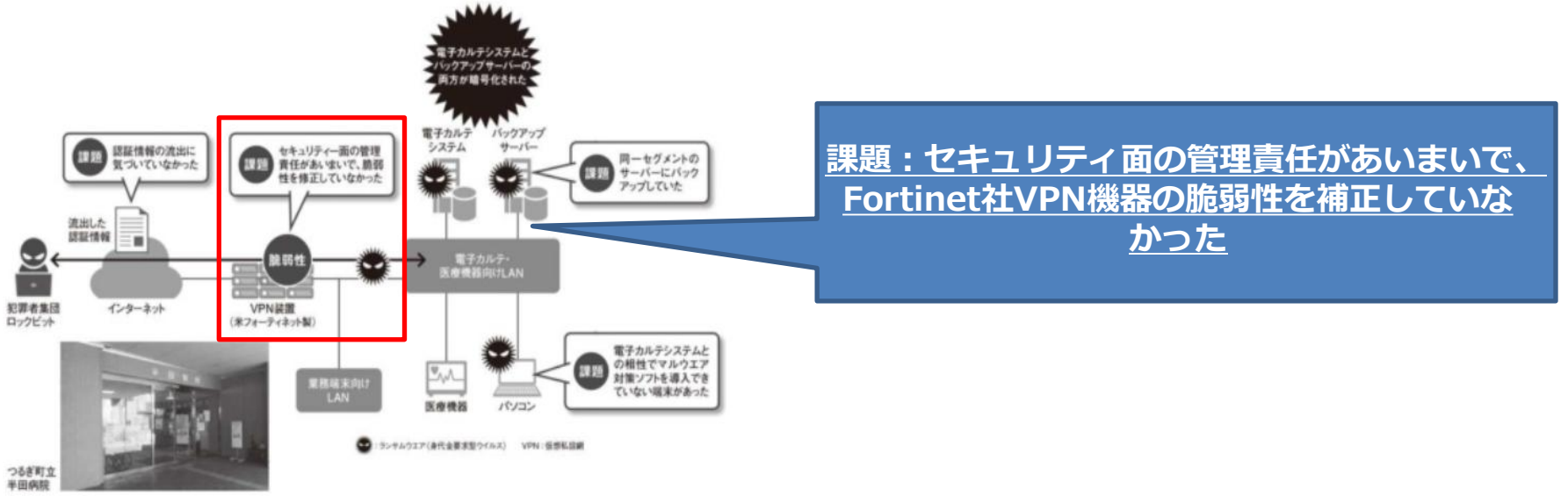


図 つるぎ町立半田病院のランサムウエア被害で表面化した課題
脆弱性に気づかず、管理責任も曖昧だった
[画像のクリックで拡大表示]

NRA

なぜ認証なのか

ID/PWの基本認証には限界

ID/PWの盗まれ方は巧妙化

総当たり攻撃によるパスワード解析時間
（コンピューターによる自動攻撃）

パスワードの例	fjR8n	pYDbL6	fh0GH5h	F6&B is
桁数	5桁 大文字・小文字・数字	6桁 大文字・小文字・数字	7桁 大文字・小文字・数字	7桁 大文字・小文字・数字・特殊文字
総当たりでの解析時間	＞1秒	4秒	17.5秒	7時間

排除対策は「端末管理」と「証明書」で端末特定

NRA

マルチデバイス環境における最適な認証方式

「人の特定」（ユーザー認証）と「端末の特定」（端末認証）

認証方式	人の特定	端末の特定
ID/パスワード	○	×
ワンタイムパスワード	○	×
マトリックス認証	○	×
生体認証	○	×
MACアドレス認証	×	○
証明書認証	○	○

マルチデバイスでサポートされている「端末特定」の方式

端末の特定	Windows	iOS	Android
MACアドレス認証	○	×	△
証明書認証	○	○	○

NRA

クライアント証明書による2要素認証の実現

- ID/PWによる従来型のユーザー認証（知識）と許可された端末のみがアクセス可能な端末認証（所持）による安全で利便性の高い二要素認証を実現
- ID/PWが漏洩しても許可された端末がなければアクセスはできない
- 端末を紛失した場合は証明書の失効により不正利用を防止

アクセスできる
「人」と「端末」による
二要素認証

許可された人
「ユーザ認証」

ID
User
パスワード
●●●●●●●

許可された端末
「端末認証」

クライアント証明書

安全かつ利便性の高い認証

ID・パスワード漏えい

端末がなければアクセス不可

端末紛失

証明書を失効させブロック

NRA

NRA提供サービス

私たちは
ネットワーク社会を支える認証技術を極め、安価かつフレキシブル提供形態により、
世界の人々の安全で快適な情報利用に貢献します

NRA-PKI
クライアント証明書

- クライアント証明書の発行・管理を行うために必要な機能をSaaSで提供し、運用や発行単位、課金体系を小口ユーザー用にカスタマイズし、初期費用などを排除して導入コストを大幅に削減
- 1ライセンス分の料金で複数の機器に証明書をインストールして利用することができるマルチデバイス・ライセンス
- サイバートラスト電子認証センター」内で運用し安全に管理された認証局

サーバー証明書
SureServer

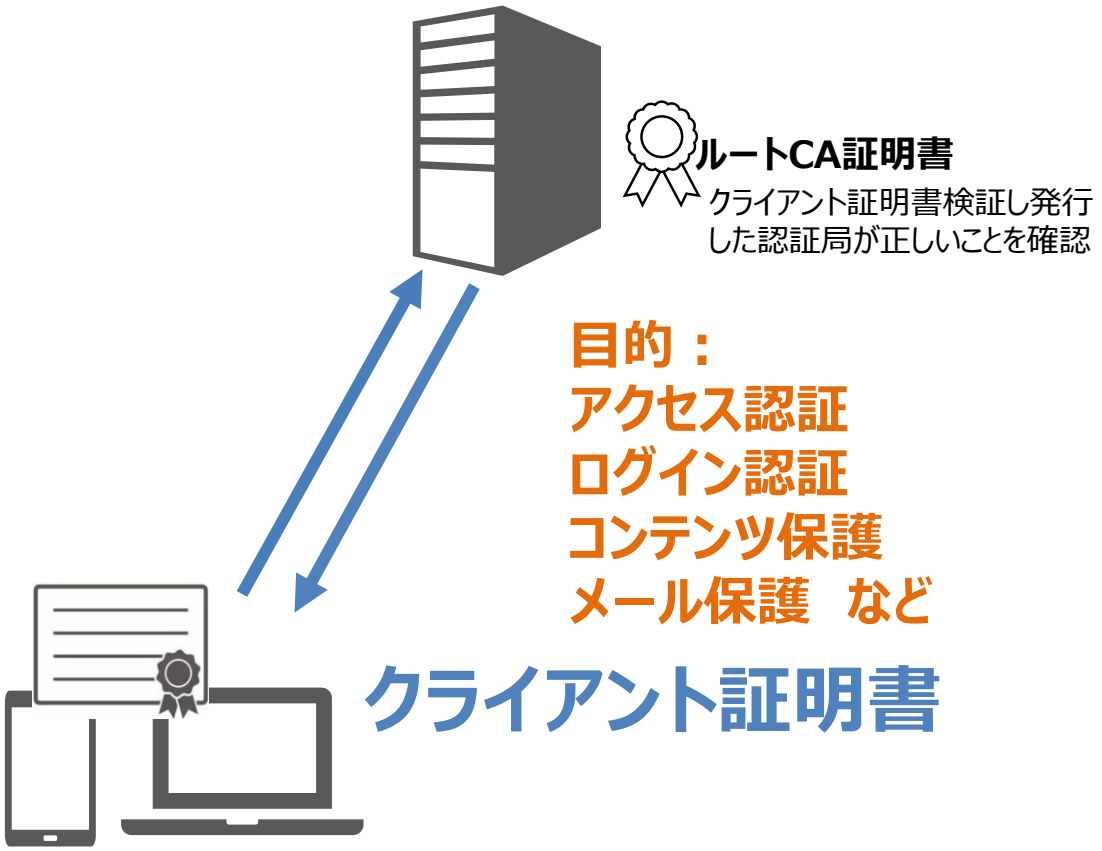
- 日本初の商用電子認証局として 20 年以上認証・セキュリティサービスを提供しているサイバートラスト社製の信頼性の高いサーバー証明書
- サーバートラスト社を株主とするSureServerセールスパートナーとして戦略的価格でご提供

Web Doctor
脆弱性診断※

- SaaS型純国産自動診断ツールをにより低価格で利便性の高いサービスをご提供
- エンジニアによるサイト仕様を確認しながら行う手動診断サービスもご用意
- 経済産業省管轄の『情報セキュリティサービス基準』の認可サービス
- 診断事業者として10年以上の実績のあるビジネスパートナーより実施

※実際の診断は弊社協力会社により実施

サーバー証明書とクライアント証明書



※ルートCA証明書はサーバー/クライアント証明書の検証を行うために必要

NRA

クライアント証明書の利用用途

Windowsログオン認証

- 社員証
- スマートカード
- USBキー

リモートアクセス認証

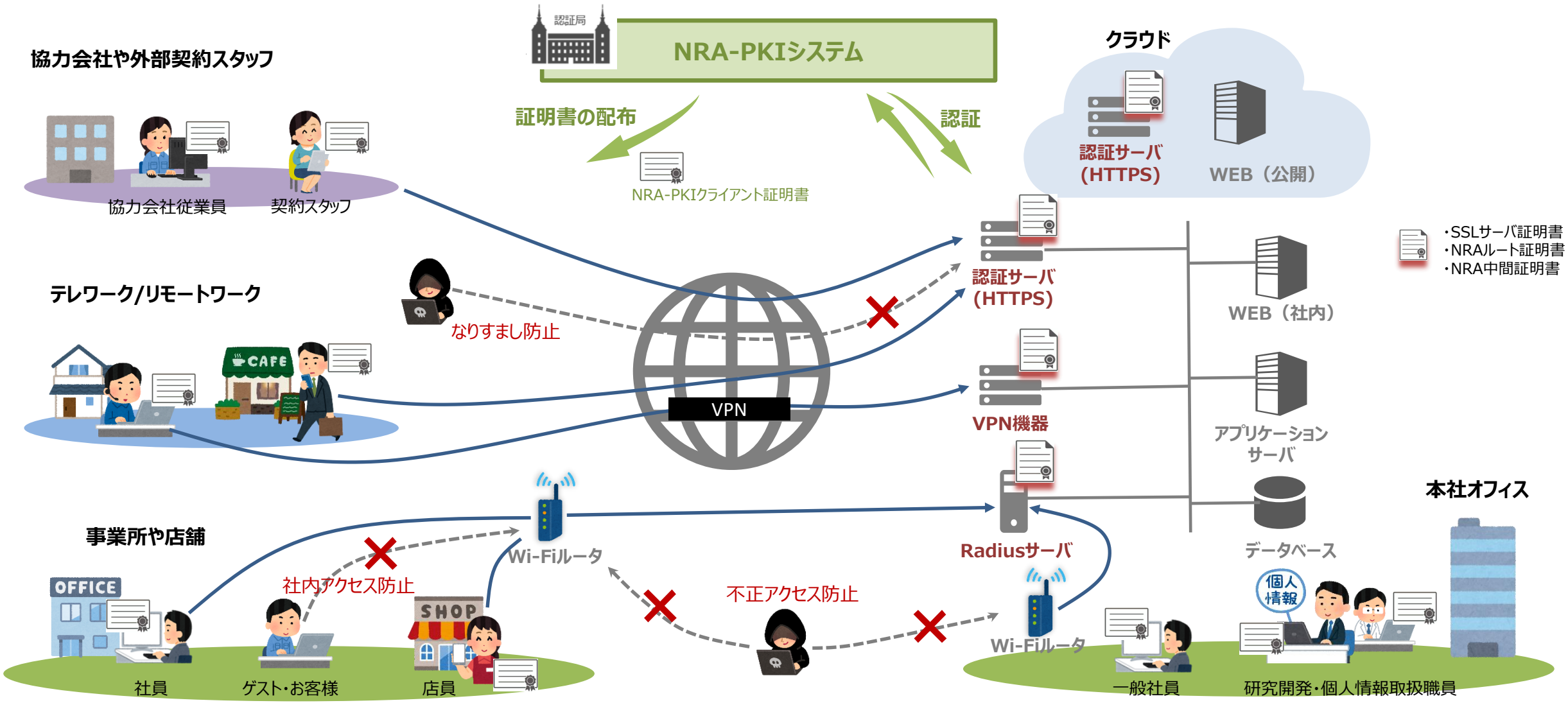
- SSL-VPN
- 有線・無線LAN認証

Webアクセス認証

- アクセス認証

NRA

NRA-PKIシステム～ID/パスワード認証から証明書認証へ～



※NRAPKIクライアント証明書をご利用いただくためには赤字機器を用意していただく必要がございます。
また赤字機器と周辺装置の設定についてもお客様にて対応いただく必要がございます。

NRA-PKIの特長

1

マルチデバイス対応（PC・iOS・Android）
1つのライセンスでマルチデバイスをサポート

2

マルチネットワークアクセス
SSL-VPN、無線LAN、Webアプリケーションに対応

3

SaaS向けWeb APIの提供
サービスと連携したシームレスな運用の実現

4

圧倒的なコストパフォーマンス
従来のPKIは高いイメージを払拭

安全に管理された認証局

高レベルのセキュリティで運用管理された「サイバートラスト電子認証センター」内に設置

耐震措置、電源設備、消火設備、空調、ネットワーク監視、脆弱性チェックをクリアした環境で運用。高い安全性と信頼性を維持しています

NRA

NRA-PKIの優位性

	日本RA NRA-PKI	A社	B社	C社	D社
種別	クライアント証明書	クライアント証明書	クライアント証明書	クライアント証明書	プライベート認証局
認証局	クラウド	クラウド	クラウド	クラウド	ラックマウント
初期費用	無償	￥300,000	オープン	無償	￥2,000,000～
運用費用	オープン （￥72,000）	オープン	オープン	￥90,000	オープン
ライセンス価格	オープン （年間：￥2,400） （1ヶ月あたり￥200）	年間：￥10,800 1ヶ月あたり￥900	年間：￥100,000 1ヶ月あたり￥8,330	年間：￥72,000 1ヶ月あたり￥600	オープン
初回購入	5～	100～	10～	20～	50～
ライセンス	マルチデバイス	端末ごとにライセンス発生	端末ごとにライセンス発生	端末ごとにライセンス発生	端末ごとにライセンス発生
Web API連携	公開	無し	無し	無し	無し
請求方法	月額、一括請求	一括請求	一括請求	一括請求	一括請求

※弊社調べ。各社公開資料によるもの。必ずしも記載内容を保証するものではありません。（ ）内は推定小売価格となります。

様々なビジネスモデルに対応

社内ITライフサイクルに合わせた導入プランのご提供

自社Webサービスへ認証組込み事業者プランのご提供

年額/月額プランや時間制限による利用により
適用業務範囲が拡大※

※基本的なご提供方法は年額のみになります。月額および時間制限によるご提供は、お客様の利用計画、ご契約ボリュームをお伺いしご提案させていただきます。時間制限についてはお客様のアプリケーション連携または管理者様による運用を想定しております。

NRA

NRA-PKI基本仕様

認証対象	各ご利用デバイス (PC,スマートフォン,タブレットなど)
申請情報	法人基本情報、管理者情報など
証明書記載情報	会社名、発行先（姓名、メールアドレス）など
CAブランド	Nippon RA Root Certification Authority
登録業務	証明書発行サービス利用企業にて実施
配付方法	・利用者操作による端末への個別インポート ※メール通知、Window/iOS/Android/Mac ・管理者操作によるPKCS#12の一括ダウンロード
最低ライセンス数	5ライセンス～
鍵長	SHA-2
有効期間	5年　（ご請求は1年毎でも可能）
初期費用	OPEN
必要ライセンス	クライアント証明書ライセンス CA基本利用料 ※オプションでSSLサーバー証明書（プライベート or パブリック）も提供可能
導入までの期間	お申し込み後、3営業日以内

サポートプラットフォーム

Windows 10

macOS
iOS
iPadOS

Windows 11

ANDROID

SSL-VPN/IPSec-VPN/無線LAN/Wifi

FORTINET
CISCO
Pulse Secure
JUNIPER NETWORKS
aruba NETWORKS

Webサーバー

Apache 2 （Tomcat）
Microsoft Internet Information Server
nginx

SSO/その他

Gluegent Gate
Akamai Enterprise Application Access

NRA

NRA統合認証基盤システム管理者画面

わかりやすいUIにより容易に証明書の運用管理が可能

メールアドレス…
利用者に割り当てられる代表メールアドレスです。こちらのメールアドレス数をライセンス数としてカウントします。赤枠の**「利用者情報 現在使用中のユーザー数」**で登録したライセンス数を確認することができます。

証明書メールアドレス…
→デバイス（端末）にインストールされる各クライアント証明書に割り当てられるメールアドレスになります。

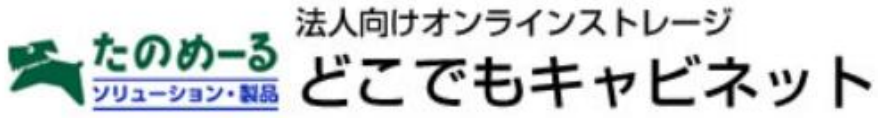
ご採用事例

導入事例 大規模からBYODまで

NRA-PKI　証明書累計発行数：　約750,000枚　　※2022年1月時点

OBCマイナンバーサービス

OMSS+OBCマイナンバーサービスに標準搭載
マイナンバー収集・管理・廃棄など、アクセス時の証明書認証



どこでもキャビネット

「ファイル共有」、「ファイル送受信」、「名刺管理」の３つの機能を
マルチデバイス対応で提供

WaWaOffice

グループウェアを中心に、SFA、ワークフロー、データベース、
WEB社内報などのサービスを提供

FortiGate SSL-VPN

社内配布の全てのスマートフォンに導入
SSL-VPNによるアクセス時の証明書認証

※その他、大手鉄道会社様、大手コンビニ様、家電メーカー様、証券会社様、自動車会社様、外資人材派遣会社様、保険会社様、運送会社様、
　食品会社様、精密機器メーカー様といった様々な業種の企業様で導入いただいております。
※導入事例：導入事例 – 日本RA株式会社 (nrapki.jp)

NRA

OMSS＋OBCマイナンバーサービス標準搭載でご提供

クラウドサービス

提供元：株式会社オービックビジネスコンサルタント

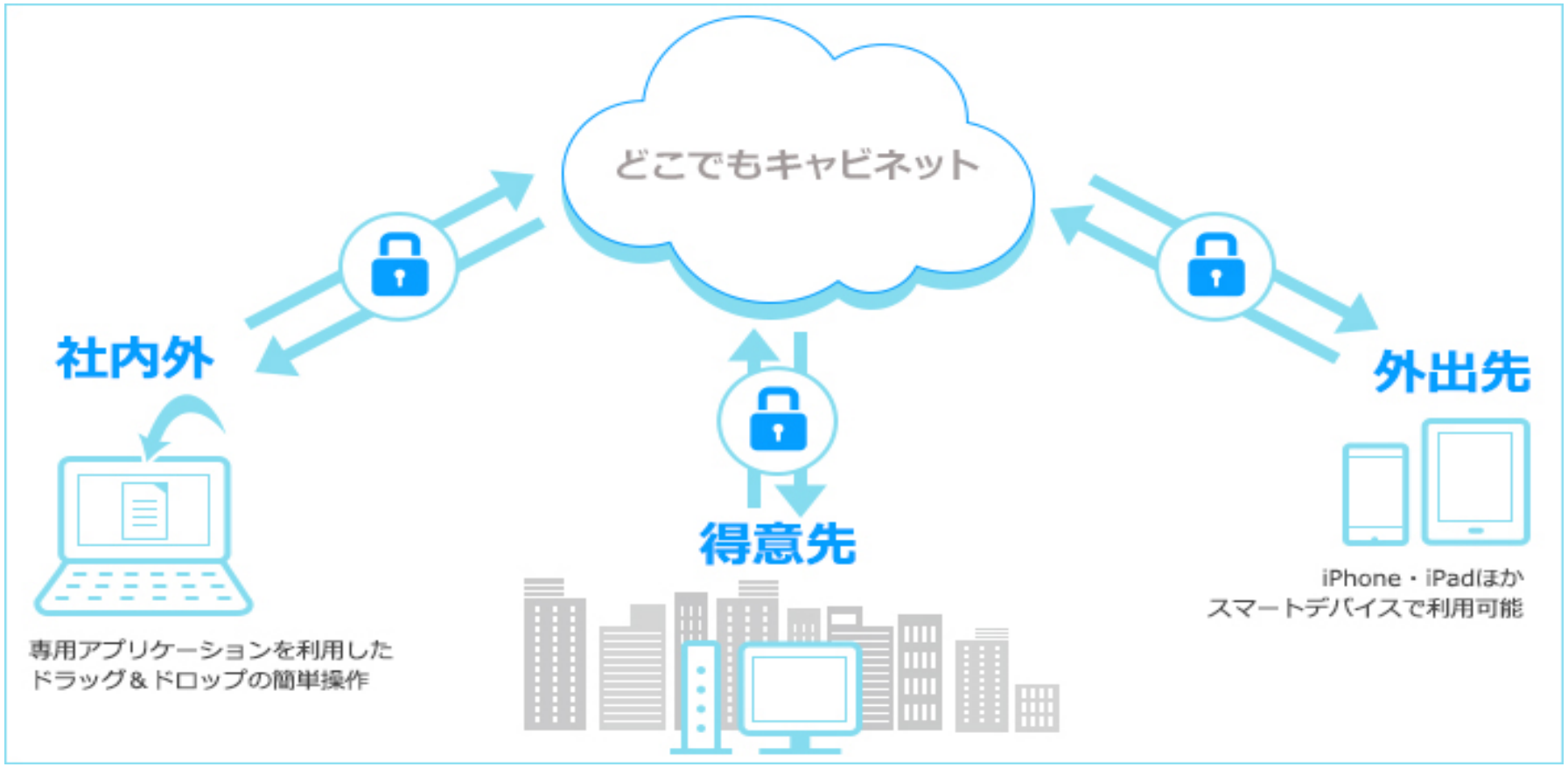
個人番号を自社内で保管することは、漏えい等のリスクを抱えることとなり、厳重な安全管理が必要です。このサービスでは、自社内ではなくクラウド上に保管することで、漏えい等のリスクを低減します。堅牢な日本のデータセンターへの保管、NRA-PKIクライアント証明書認証とSSL暗号化によるデータ通信などの高度なセキュリティ環境で、安全な番号保管・運用が可能になります。

NRA

大塚商会「どこでもキャビネット」とWebAPI連携

WebAPI実装

提供元：株式会社大塚商会



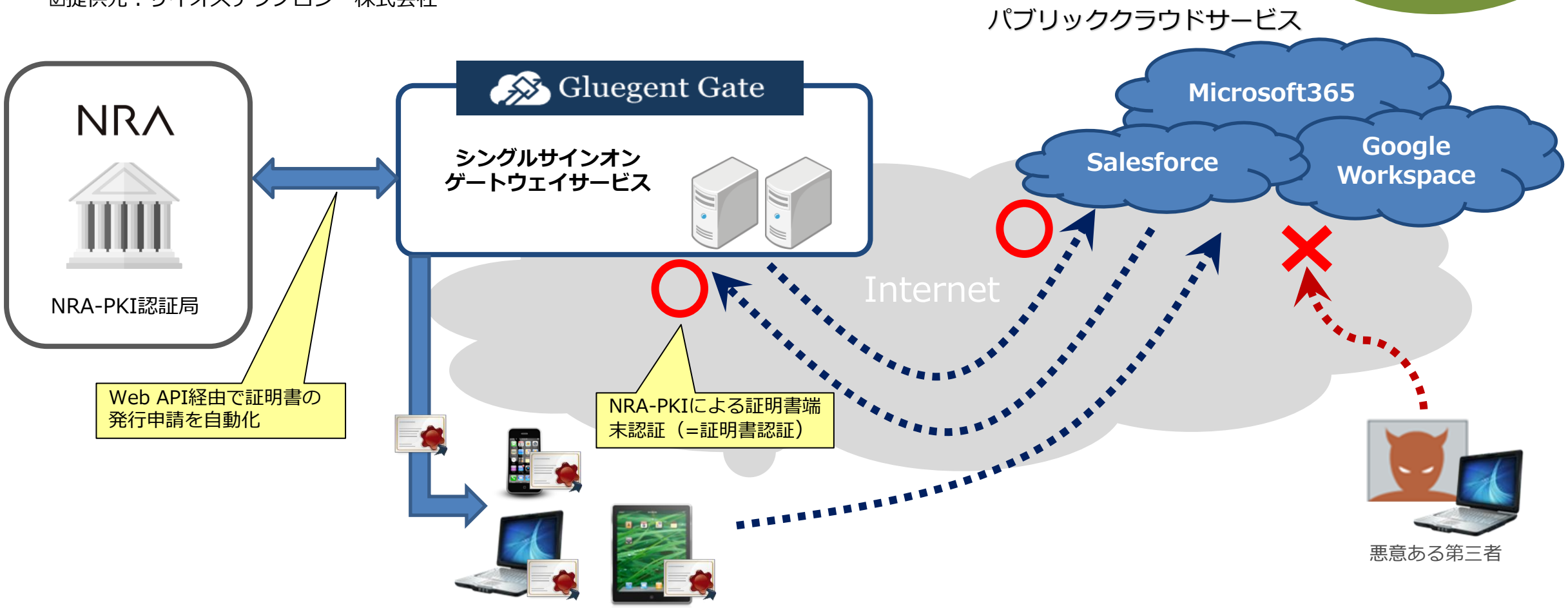
どこでもキャビネットは法人向けのオンラインストレージサービスですが、その性質上お客様からのセキュリティに対するニーズは高い傾向にありました。NRA-PKIクライアント証明書による端末認証により利用端末が限定することで、”なりすまし”を完全に排除することができ、セキュリティに敏感な企業でも安心してご利用いただけるようになりました。

NRA

IDaaS「Gluegent Gate」とWeb API連携

WebAPI実装

☑提供元：サイオステクノロジー株式会社



IDaaS「Gluegent Gate」は、Google WorkspaceやMicrosoft365等の様々なクラウドサービスのシングルサインオンを実現するゲートウェイサービスです。
1度の認証で複数のクラウドサービスにログインできるため利便性が向上します。また、NRA-PKI（端末認証）を導入することにより、悪意ある第三者の不正アクセスを防止し、安心安全なクラウドサービスの利用を実現します。

NRA

SWJDC（ソフトウェア共同開発協議会）とWebAPI連携
～全国展開するグループウェアのセキュアなアクセスを実装

WebAPI実装

提供元：株式会社アイアットOEC（SWJDC：全28社）

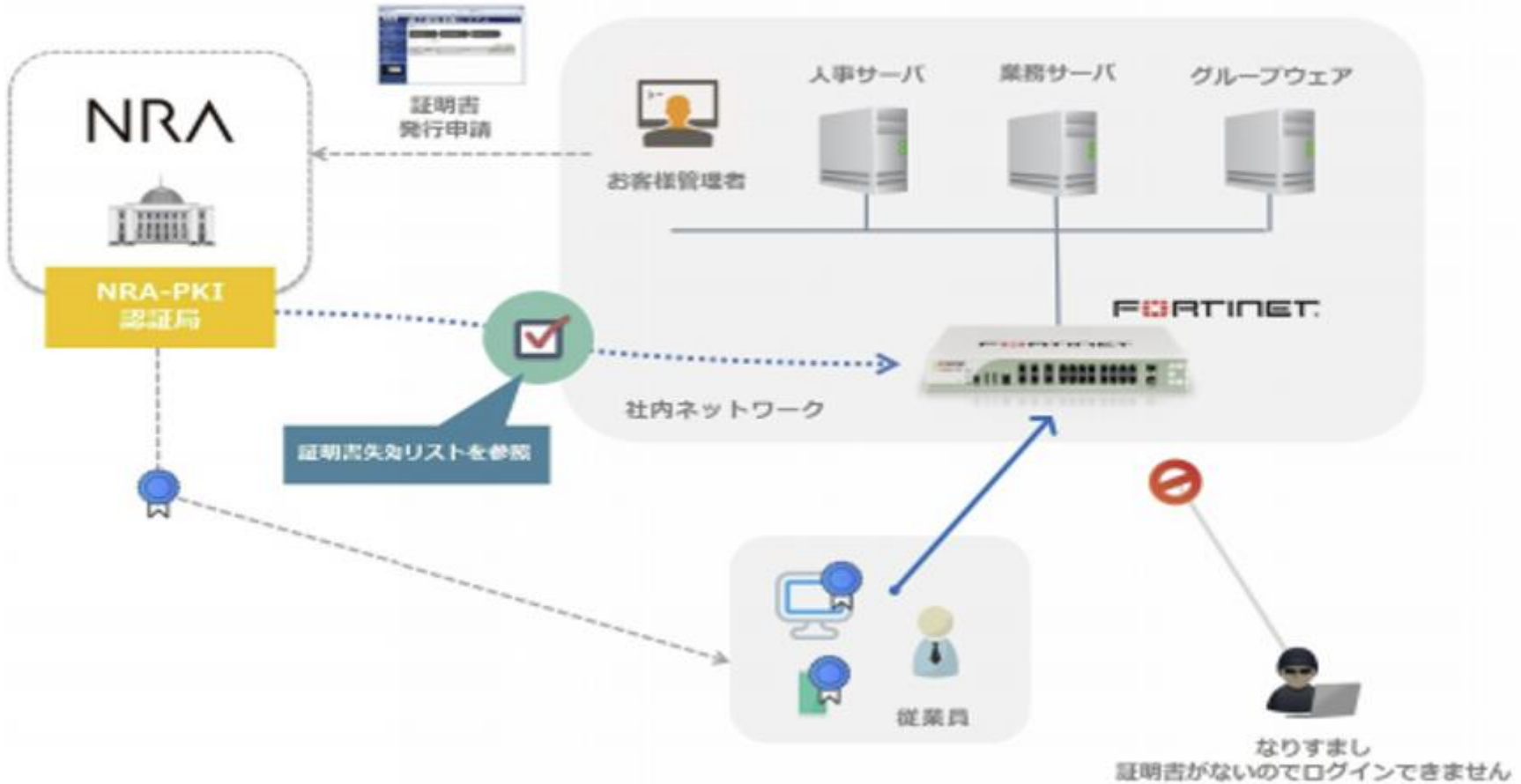
「WaWaOffice」は、営業マンの日々の活動を管理し、戦略的営業を行うためのSFA、ワークフロー等、様々な業務の利便性を考慮した純国産のクラウドサービスです。純国産のグループウェアの強みである、日本企業向けにカスタマイズしたインターフェースをはじめとする利用しやすいシステムで多くのお客様にご利用頂いておりますが、ID/パスワードの脆弱な部分に頭を悩ませておりました。NRA-PKIクライアント証明書を採用することで、従来懸念していたセキュリティ面のリスクや、パスワードやシステム部門の運用の煩雑さを軽減し、バリューアップした「WaWaOffice」をお客様へご提供致します。

NRA

SSL-VPNをNRA-PKIクライアント証明書認証で強化

SSL-VPN

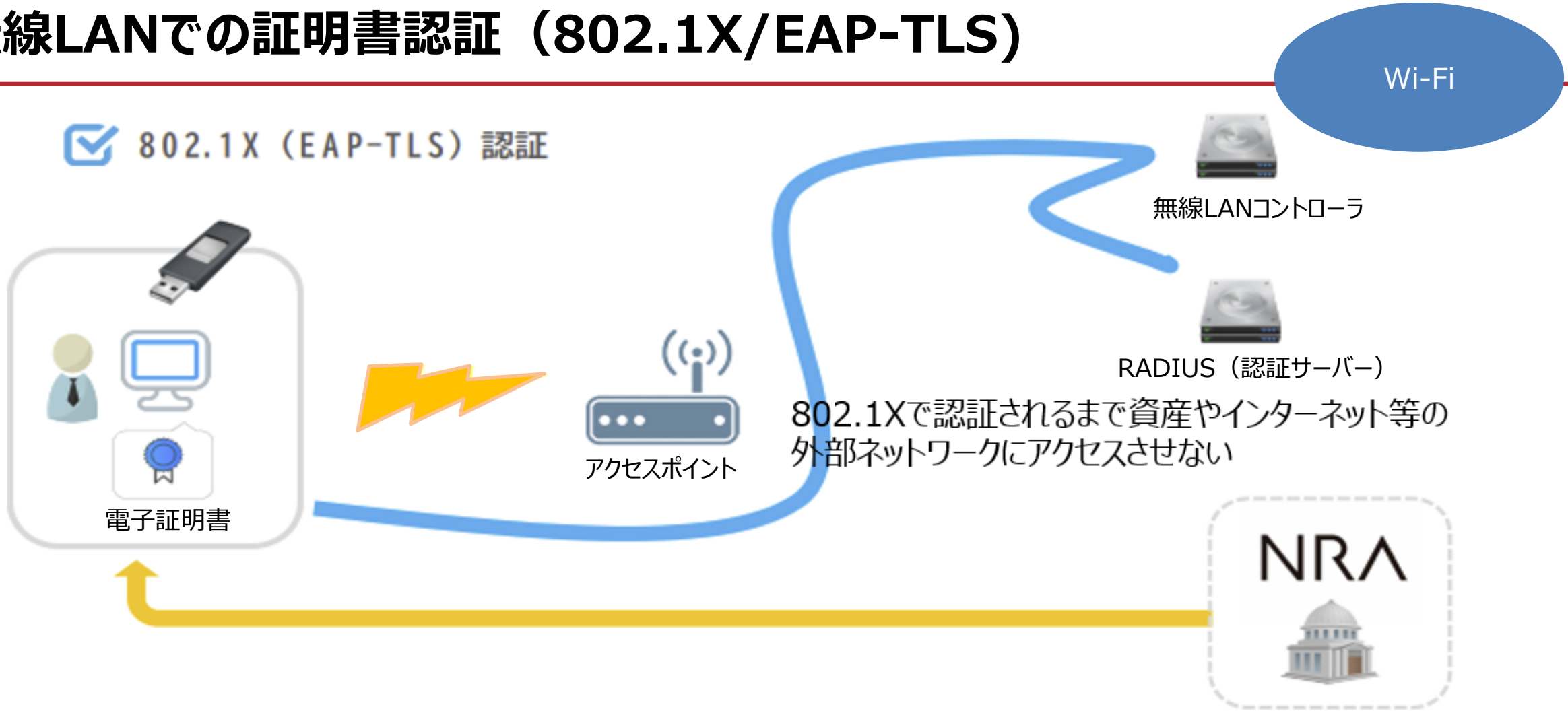
提供元：株式会社静岡朝日テレビ



SSLを利用したVPNによる暗号化通信は高度なセキュリティを実現していますが、暗号化通信を確立するための認証手段として、パスワード認証が多く利用されているのが現状です。パスワードによる認証は、安易なパスワードの設定を行われたり、またパスワードポリシーを厳しくすると利用者のパスワード忘れが発生したり、パスワード自体を利用者が付箋紙やテキストファイルに記載したりとなかなか安全な運用が難しいのが実情です。これでは十分な認証を行っているとは言えず、強力な暗号化通信を行う意味がなくなります。
これに対して、日本RAが発行するクライアント証明書（NRA-PKI）を使うことにより安全な認証を実現することが可能になります。

NRA

無線LANでの証明書認証（802.1X/EAP-TLS）



企業・組織における無線LANが広がりを見せておりますが、未だ認証に事前共有鍵（プリシェアードキー）を利用している例が多くみられます。
事前共有鍵方式はアクセスポイントと全端末が同じ鍵を持つため、どうしても十分なセキュリティを確保できているとは言い難く、またMACアドレスによるアクセス制限は詐称が容易に可能という弱点があります。
こういったセキュリティリスクを抱えながらも、「便利だから」という理由でセキュリティリスクを軽視して無線LANを利用している例は枚挙に暇がありません。企業・組織での無線LAN利用では、事前鍵共有方式を利用するのではなく、各ユーザ（或いは端末）毎に認証をかける802.1X方式が推奨されます。

NRA

ご参考：NRA-PKIサポート情報

■ NRA-PKIサポート情報サイト（https://www.nrapki.jp/support/）では、クライアント認証設定等に関する各種マニュアルを公開しています。ぜひご活用ください。