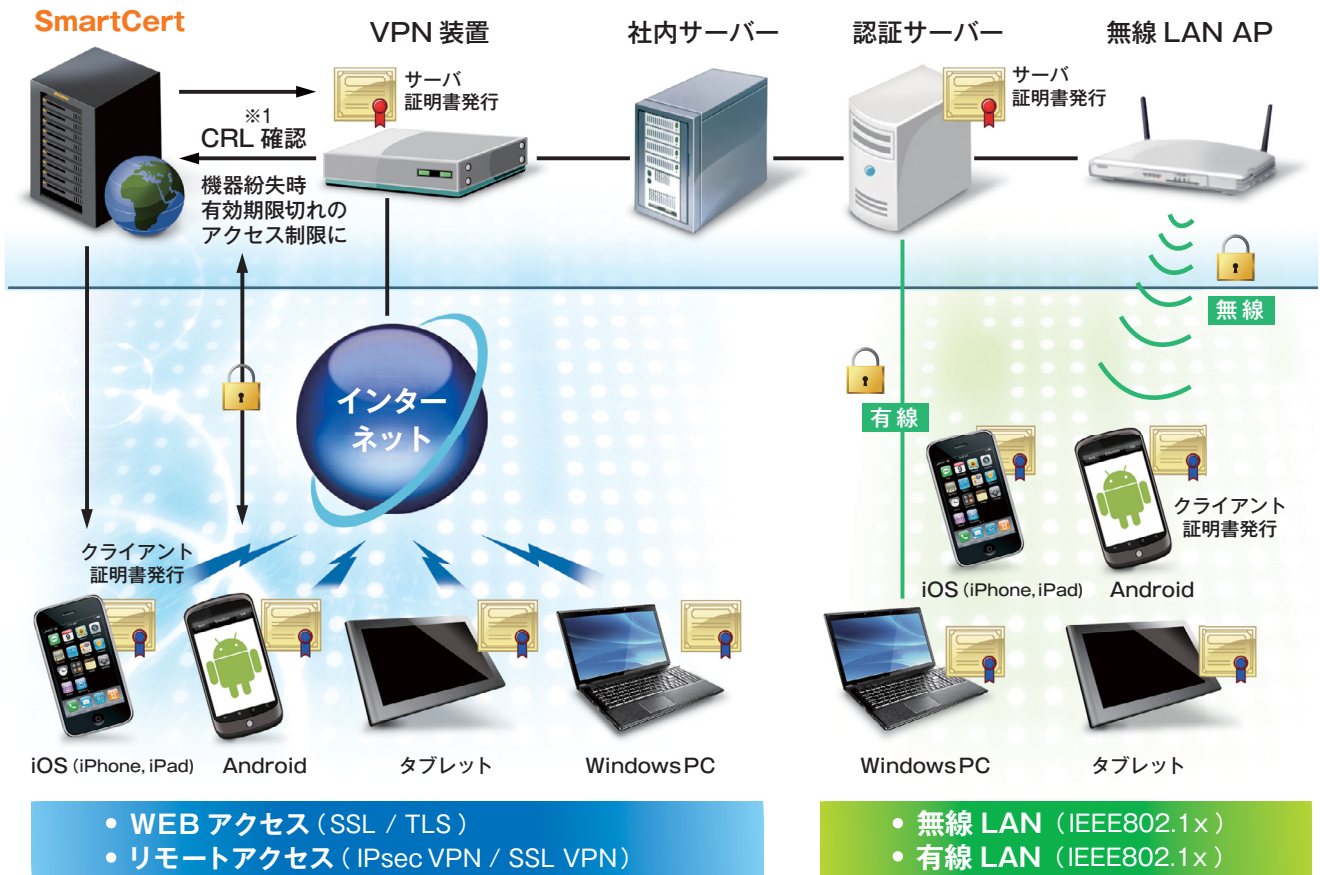


Smart Cert



SmartCert とは、お客様企業に対して、その企業のシステム管理者様が登録した情報に基づき、お客様企業ごとにプライベートな CA※2 を提供するサービスです。

※ SmartCert は、NTT エレクトロニクス プライベート認証局サービスの登録商標です。

Smart Cert の5つの特長

Security

証明書を安全に発行する基盤をご提供します。機体認証機能により、企業が認める端末に対してのみ、証明書を発行・安全簡単に格納しますので、安全性が高まります。

Mobility

スマートデバイス※3 では移動性が重視されます。証明書を活用した相互認証により、スマートデバイス等の企業内、外でのシームレスなセキュア接続を実現します。

price Advantage

CA の構築運用は弊社で行いますので、お客様の CA 費用が削減できます。また、他の認証方式や証明書サービスよりも安価で簡便な仕組みでご提供します。

Rich Application

国際標準形式の証明書 (X.509 形式) ですので、証明書を利用した様々なアプリケーションに適用可能です。

Technical Support

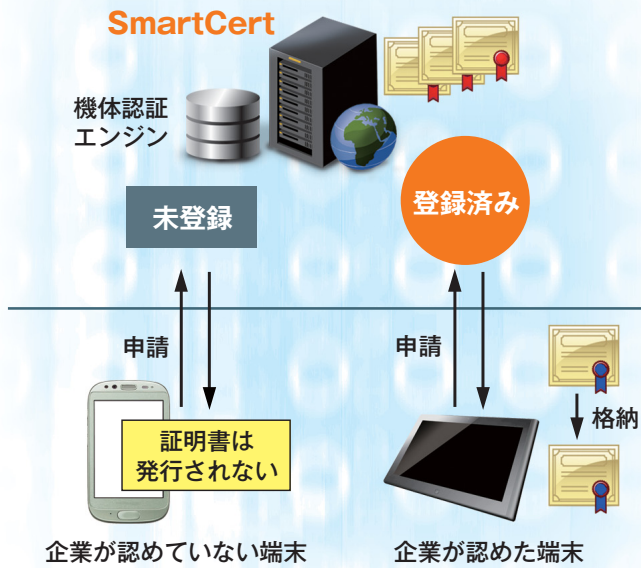
自社開発システムですので、新端末や新 OS への対応、及び暗号の追加のご要望にも迅速に対応します。ソリューション提案や技術サポートにも柔軟に対応します。

※1 : Certificate Revocation List. 失効した電子証明書のリスト。

※2 : Certificate Authority. 認証局。

※3 : 情報処理端末の中で、多岐にわたる用途に利用可能な端末。スマートフォンやタブレット端末を指す。

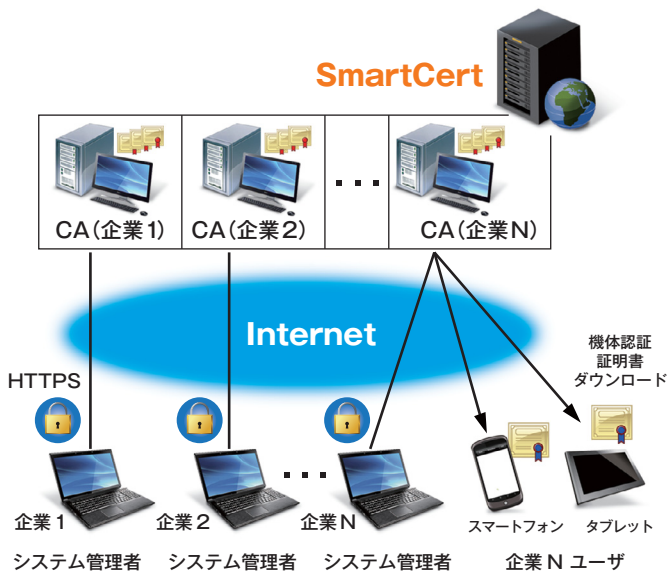
機体認証機能



- 企業等のお客様でリモートアクセスを許可された端末（スマートデバイス、ノートPC等）についてのみ、電子証明書を安全・簡単に且つ確実に配布する機能です。
- 電子証明書はOSにより保護されており、他の端末へ簡単にコピーすることができません。許可されている端末に限定した、成りすましてできない安全なリモートアクセスを実現します。
- 機体認証機能 ON/OFF どちらでも、簡単な操作で電子証明書を端末へ格納できますので、幅広いお客様にご利用いただけます。

SmartCert サービス基本仕様

御提供サービス	証明書発行機能（機体認証機能） CRL 発行機能 発行証明書管理機能（検索、失効等）
CA の Issuer	お客様
証明書形式	X.509 Ver.3
証明書鍵長	鍵長：1024bit / 2048bit（選択可能）
署名アルゴリズム	SHA256 with RSA（推奨） SHA1 with RSA
対象端末	PC、スマートフォン、タブレット など
システム管理端末	Windows 系 PC
利用用途	二要素認証用途、IPsec VPN、SSL VPN、IEEE802.1x（有線 LAN、無線 LAN）、SSL/TLS、リモートデスクトップ、シンクライアント等のアクセス時の端末認証、外部クラウド認証強化、文書への署名、暗号メール（S/MIME※5）等



- お客様のシステム管理者が、WEB アクセス（双方向の HTTPS※4）により証明書の発行に必要な情報を安全に登録することで、簡単に証明書の発行ができます。

※4：Hypertext Transfer Protocol over Secure Socket Layer。HTTP の安全性向上目的で利用されている。

※5：Secure / Multipurpose Internet Mail Extensions。署名と暗号化が施された安全なメールのやりとりをする規格。

ご注意

- 本パンフレットの記載内容は、2017年10月現在のものです。
- 本パンフレット中の弊社名または弊社商品名、他社商品名は、弊社並びに他社の商標登録または商標登録出願中のものです。
- 本資料に記載された内容につきましては、予告なしに変更することがあります。ご用命の際は、弊社営業担当者までご確認ください。
- 本サービスを海外でご利用の際には、「外国為替及び外国貿易法」を遵守してください。詳しくは、弊社営業担当者までご連絡ください。

195-P/P17-10-02



NTT エレクトロニクス株式会社

営業本部 映像コンポーネント営業部

〒221-0031 神奈川県横浜市神奈川区新浦島町1-1-32

TEL：050-9000-6003 FAX：045-453-9710