# スマートデバイスに最適な認証ソリューション

池谷 亮平・岡田 英明
甲田 圭人・手塚 由起子

**要　旨**

近年、スマートフォンやタブレットなどのスマートデバイスを利用するユーザーが法人市場、個人市場ともに増加しています。法人市場ではスマートデバイスを利用した業務ワークスタイルの変革が始まっており、スマートデバイスを使って社外から業務を行うシーンが増えています。個人市場でも、各モバイルキャリアからスマートデバイスが発売されています。スマートデバイスの登場によって端末のOSやネットワークを限定しない利用が加速するなかで、ユーザーが安心・安全・簡単に利用できる認証ソリューションを、本稿では紹介します。

キーワード

●クラウド ●スマートフォン ●マルチデバイス ●3Aセキュアトークン
●ソフトウェア証明書 ●デバイス認証 ●ID統合 ●シングルサインオン ●一元管理 ●ユーザー識別

## 1. まえがき

法人市場におけるスマートデバイスの導入数は年々増加しており、今後も更に出荷台数は増えていくことが予想されます。

各企業では持ち運びやすさ、見た目の重視、ペーパーレスによるコスト削減を狙ってスマートデバイスの活用を進めています。個人市場においても、各モバイルキャリアにおけるスマートデバイス契約台数は年々増加傾向にあります。

ここ1、2年で各端末メーカの製品構成もスマートデバイスを中心としたものに変わっており、それに伴い、エンドユーザーに提供するサービスもスマートデバイス対応へと変化しています。

このような市場動向の背景には、スマートデバイスが高性能となったこと、タッチパネルなどのユーザーインタフェースによる操作性向上、価格の低下など幅広いユーザーが利用できる端末へと進化したことが挙げられます。

しかし、スマートデバイスの利用には課題が複数あり、解決策が求められています。本稿では、スマートデバイスを利用する際の主にセキュリティに関する課題と、それを解決するNECのソリューションを紹介します。

## 2. スマートデバイスを活用した業務

### 2.1 スマートデバイスの導入目的

法人企業における業務利用デバイスといえばPCが中心でしたが、スマートデバイスの進化とともに企業のワークスタイルもスマートデバイスを活用したものに変化しており、代表的な変化には下記のようなものが挙げられます。

1) 社外からのリモートアクセスによる業務の遂行
2) 会議における電子データ化によるペーパーレスの推進
3) タッチパネルを利用したお客様への説明や広報
4) PC、スマートデバイスなどのマルチデバイスの利用

上記に共通して言えることは「社外においてスマートデバイス1台で業務を処理できること」であり、各企業がスマートデバイスを導入する目的もまさにこれだと考えられます。

### 2.2 スマートデバイスの課題

社外で業務を遂行する際に課題となるのが、インターネット経由の場合のアクセス制御です。社内での業務では、PCなどの端末は閉域ネットワークに接続されているため、通常、

社員用のIDとパスワードでログインするだけでさまざまな業務システムにアクセスできます。社外にこのような業務システムをそのまま開放すると、IDとパスワードが不正入手されてしまった場合には、不正アクセスされてしまう可能性があります。

不正アクセスを防止する既存ソリューションとして、ハードウェアやソフトウェアのトークンによる2要素認証が考えられます。モバイルPCの場合、例えばワンタイムパスワード生成機器やUSBトークンなどのハードウェアのトークンを利用し、2要素認証を実現していました。しかし、スマートデバイスの場合、マイクロUSBなどの接続ポートが少ないため、ハードウェアの接続はPCに比べて手間が掛かります。更にスマートデバイスは手に持って操作するため、機器をつなげたままの利用では操作性が著しく悪くなります。

一方、ソフトウェアベースのトークンによる2要素認証では、アプリケーションによるワンタイムパスワード生成やソフトウェア証明書による方式があります。この場合は追加の機器や設備が必要なく、利便性高く利用できます。ただし、ソフトウェア証明書などはアプリケーションの仕組み上、セキュリティ自体がハードウェアトークンに比べて弱く、万が一証明書を盗まれてしまうと不正アクセスされてしまうといった問題があります。

このようにスマートデバイスの業務利用では「セキュリティと利便性の両立」という課題が存在します。

## 2.3 マルチデバイス認証

弊社の製品である「NC7000-3A」では、上記セキュリティと利便性の両立を実現する「3Aセキュアトークン」を実装しています。特長として下記があります。

1) 追加機器不要のソフトウェア証明書
2) 盗まれても利用されないカモフラージュ技術
3) Windows PC、iOS、AndroidとOSを限らず、マルチデバイス利用が可能

**(1) 追加機器不要のソフトウェア証明書**

3Aセキュアトークンは、ソフトウェアをベースとした独自拡張の証明書を利用しています。ソフトウェア証明書のため、ハードウェアトークンなどの特別な機器は不要であり、調達コストや運用コストも抑えることが可能です。

また、3Aセキュアトークンは2通りの使い方が可能です。1つ目はIDとパスワードを入力して認証する方法、2つ目はIDとパスワードを入力せずに認証する方法です。

上記それぞれの方式は、セキュリティと利便性がトレードオフとなるため、サービスやユーザーの利用形態によってどちらが最適なのかは決定する必要があります。

**(2) 盗まれても利用されないカモフラージュ技術**

通常のソフトウェア証明書では、盗まれた場合のオフラインでのブルートフォースアタック（総当たり攻撃）に対しては、仕組み上の脆弱性がありました。3Aセキュアトークンでは、上記の問題をカモフラージュ技術によって解決しました（**図1**）。

通常のソフトウェア証明書では、ブルートフォースアタックによって秘密鍵情報が特定されて抜かれてしまい、悪意のある攻撃者に不正利用されてしまいます。3Aセキュアトークンのカモフラージュ技術では、秘密鍵らしき情報が毎回出力されるため、どれが本当の秘密鍵かを攻撃者が確認するには、認証サーバに直接認証要求を送信する必要があります。何億通りものカモフラージュされた秘密鍵情報を全て確かめる前に、複数回NGとなった場合は認証サーバ側でロックを掛けることで不正アクセスを防止できます。

このようにソフトウェア証明書でありながら、ハードウェアトークンと同等のセキュリティ強度を実現しています。

**(3) マルチデバイス利用**

スマートデバイスやPCを1人で複数台利用するマルチデバイス利用も増加しています。このような複数台の端末

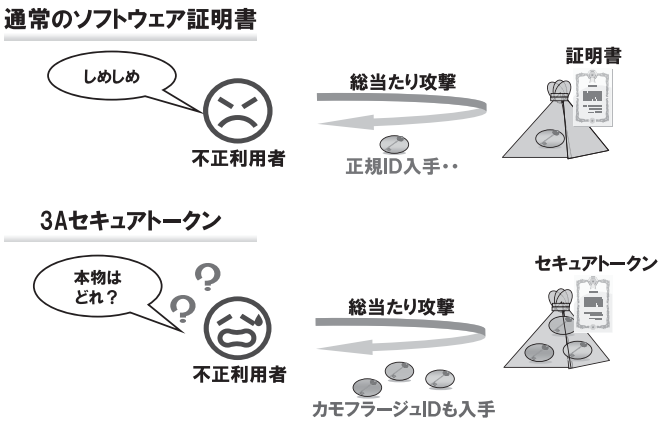


図1　3Aセキュアトークンのカモフラージュ技術

を利用している場合でも、同じIDとパスワードで3Aセキュアトークンの認証が可能です。
3AセキュアトークンはWindows PC、Android OS、iOSなどOSを限定することなく各種端末で利用可能です。更にネットワークを限定することなく、各端末がオンラインであれば認証は可能です。
更に、ソフトウェア証明書をインストールする場合も、オンラインであればどこでもダウンロードできるため、端末を集めて設定する必要はありません。

## 2.4 NEC Cloud Authentication

上記3Aセキュアトークンによるマルチデバイス認証を法人向けクラウド認証サービスとして提供しているのが「NEC Cloud Authentication」です。クラウドサービスとして提供することで、早期開始や設備運用などコストの削減が可能です（**図2**）。

NEC Cloud Authenticationは下記シーンに利用できます。

- **屋外から社内システムへのアクセス**
  社外から業務用Webシステムにアクセスする際、マルチデバイス認証を利用してセキュアにアクセスが可能です。
- **ハードウェアトークンの代替**
  ハードウェアトークンは高セキュリティですが、コストが非常に高いという課題があります。同等のセキュリティレベルで安価なソフトウェアトークンへの置き換えに利用できます。
- **SSL-VPN認証**
  マルチデバイス認証ではRADIUS認証に対応しており、Juniperシリーズなどの SSL-VPN装置のVPN接続時にマルチデバイス認証で接続できます。
- **システムやクラウドサービス間のシングルサインオン**
  OpenID 2.0やSAML 2.0、OAuthといった標準プロトコルに対応しており、ドメインが異なるサービス間のシングルサインオンが可能です。各ユーザーは異なるサービスでも同じIDとパスワードで認証することができ、認証済みの場合は再度IDとパスワードを入力することなく利用が可能です。
- **LDAP連携**
  企業内のLDAPサーバとの連携が可能です。

## 3. コンシューマ向け認証サービス

コンシューマサービスにおいても、スマートデバイスとフィーチャーフォンの違いによるセキュリティ課題があります。

各モバイルキャリアが提供していた3GネットワークやLTEネットワークでは、利用者のSIMカードと端末をひも付けてネットワーク側で認証することが可能でした。ところが、スマートデバイスになるとモバイル網以外のWi-Fiなどのインターネットが並行して利用されることになります。各モバイルキャリアで提供しているネットワーク認証と同等の利用者セキュリティを、インターネットベースのオープン化された世界でも実現する必要が出てきています（**図3**）。

セキュリティを強固にする手段としては、ハードウェアトークンの利用やパスワードの桁数を増やすことが考えられますが、いずれもユーザーの利便性を損なう結果となります。

そこで考えられるのが3Aセキュアトークンによる認証です。

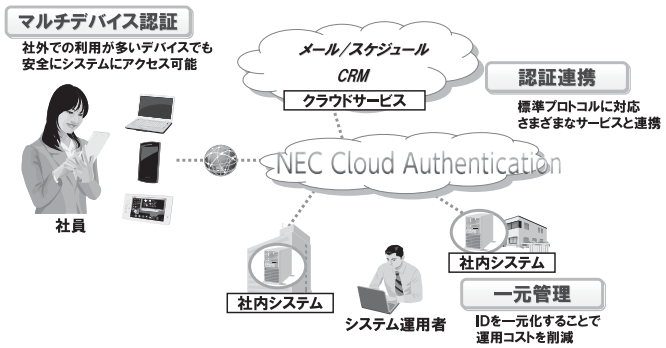


図2　NEC Cloud Authentication概要

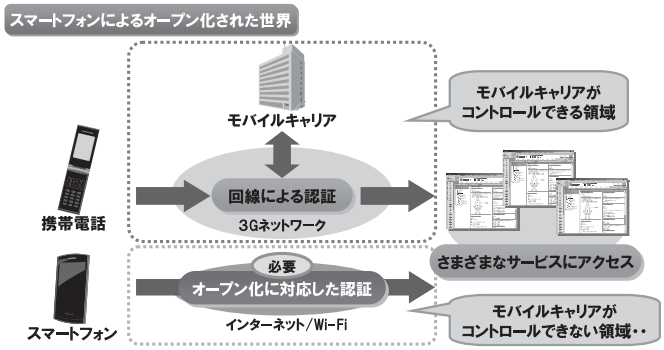


図3　オープン化された世界の認証方式

ソフトウェアでありながらセキュリティ強度が高く、また端末の種類や利用するネットワークを限らずに利用できます。3Aセキュアトークンであれば、インストールするだけで追加のハードウェア不要で利用でき、更にユーザビリティを考慮して4桁のPINコードだけで認証させることも可能です。セキュリティと利便性を両立させて、ITリテラシーが決して高くないコンシューマにも、安心して利用していただくことが可能です。

更にマルチデバイス認証によって、ユーザーがアクセスした際に個人に適したレコメンドやパーソナライズされた情報を配信するための識別子を付与できます。上記を実現するコンシューマ向けクラウド認証サービスが「Smart Cloud Sign」です。

## 4. むすび

本稿では、スマートデバイスを利用する際のセキュリティ課題と、解決策として弊社の認証基盤製品とクラウド認証サービスを紹介しました。今後は、社内の機密システムの業務にもスマートデバイスを活用することが予想されます。その場合には、よりセキュリティを考慮した方式を検討する必要があります。弊社では今後もサービスを拡大するとともに、法人企業やコンシューマサービス事業者の課題を解決するソリューションを提供してまいります。

**関連URL**

NC7000-3A:
http://www.nec.co.jp/netsoft/nc7000-3a/
NEC Cloud Authentication:
http://jpn.nec.com/solution/vas/nec_cloud_authentication/
Smart Mobile Cloud:
http://www.smartmobilecloud.com/

*Androidは、Google Inc.の商標または登録商標です。
*iOSの商標は、Ciscoの米国及びその他の国のライセンスに基づき使用されています。
*LTEは、欧州電気通信標準協会（ETSI）の登録商標です。
*OpenIDは、OpenID Foundationの登録商標です。
*Wi-Fiは、Wi-Fi Allianceの登録商標です。
* Windowsは、米国Microsoft Corporationの米国及びその他の国における登録商標です。

## 執筆者プロフィール

**池谷 亮平**
キャリアサービス事業本部
第三キャリアサービス事業部

**岡田 英明**
キャリアサービス事業本部
第三キャリアサービス事業部
マネージャー

**甲田 圭人**
NECソフト
UNシステム事業部

**手塚 由起子**
キャリアサービス事業本部
第三キャリアサービス事業部

# NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

## NEC技報WEBサイトはこちら

NEC技報(日本語)　　NEC Technical Journal(英語)

## Vol.65 No.3　スマートデバイス活用ソリューション特集

スマートデバイス活用ソリューション特集によせて
スマートデバイス活用に向けたNECグループの取り組み

### ◇ 特集論文

**サービス基盤**
OSやキャリア不問のスマートデバイスの管理・セキュリティソリューション
スマートデバイスの活用を支えるソリューションと導入事例
スマートデバイスに最適な認証ソリューション
スマートデバイスの利活用に貢献する「Smart Mobile Cloud」
高品質なサービスの構築を支える「BIGLOBEクラウドホスティング」
スマートデバイス向けコンテンツ配信サービス「Contents Director」
BYODに最適なスマートデバイス活用基盤「UNIVERGEモバイルポータルサービス」
スマートデバイスの利用を促進するリモートデスクトップ・ソフトウェア
スマートデバイス対応アプリケーション開発を効率化する業務システム構築基盤「SystemDirector Enterprise」
BIGLOBEホスティングを活用したスマートフォン向けコンテンツ配信基盤サービス

**スマートデバイス**
Android搭載タブレット「LifeTouch」シリーズの概要
Windows 8搭載 大画面タブレットPC「VersaPro タイプVZ」
Android搭載タブレット型パネルコンピュータの開発

**ソリューション**
スマートデバイス対応のペーパーレス会議システム「ConforMeeting」
スマートフォンを活用したBusinessView保守業務ソリューション
UNIVERGE遠隔相談ソリューションの見守りサービスへの適用
画像認識サービス「GAZIRU」の紹介
インストア・コンシェルジュ～究極の接客ソリューション～
スマートデバイスを活用した業務システム向けテンプレートの開発
マルチデバイス対応のビデオコミュニケーションクラウドの紹介

**先端技術研究**
ユーザーフレンドリーなセキュリティ強化BYODソリューションに向けて
OpenFlowを活用した業務用スマートデバイスのセキュアな通信の実現
映像投影とジェスチャー入力によるインタラクション技術
雑音下でも頑健に動作する音声UI技術とその応用

### ◇ 普通論文

大規模災害における移動通信サービスの輻輳解決に向けた取り組み

### ◇ NEC Information

**C&Cユーザーフォーラム&iEXPO2012**
**人と地球にやさしい情報社会へ ～あらゆる情報を社会の力に～**
NEC講演
展示会報告

**NEWS**
2012年度C&C賞表彰式典開催


Vol.65 No.3
(2013年2月)

特集TOP