音響信号を利用した個人認証システム

蛭子　隆彦

個人情報保護法の施行と相俟って企業の情報通信システムにおけるセキュリティ対策には，

「入れない」，「見せない」，「出さない」

という3つの基本原則に則ったさまざまなツールとソリューションが提案されている。「入れない」という対策の一つにワンタイムパスワード方式による個人認証があるが，近年このワンタイムパスワードを“音”に変換して伝達し，認証する技術が実用化されている。

この音響信号を用いた個人認証システムは「音響署名カードシステム」と呼ばれ，nCryptone社（フランス／パリ市，旧AudioSmartCard社）により開発され，音響署名株式会社（京都市）により国内向けに販売されている。

沖コンサルティングソリューションズ（株）は，音響署名（株）殿への技術コンサルティングと事業立ち上げコンサルティングを通じて本システムの市場展開支援を行っており，本稿ではその特徴，技術内容および導入事例を紹介する。

音響署名カードシステムとは

カード型の認証トークン「音響署名カード」から“音”になったワンタイムパスワードを発生し，ネットワークを経由して送られるこのワンタイムパスワードを認証サーバで検証する個人認証用のシステムである。**図1**に音響署名カードの外観と操作の様子を示す。

図1　音響署名カード外観図

(1) 適用分野

各種システム，ネットワーク，アプリケーションでの個人認証ステージに適用が可能であり，

- リモートアクセスユーザ認証
- ASPサービスユーザ認証
- 電子商取引本人確認
- コンタクトセンタ本人確認

等の不正侵入やなりすましの防止が強く求められる応用システムへの適用が効果的である。

(2) 特徴

■ マイクロフォン入力

PC，PDA，Thin Client，電話等のマイクロフォンにより“音”を入力できる端末が利用でき，ワンタイムパスワード表示器，ICカードリーダ等の特殊な認証機器が不要である。

■ 2要素認証

暗証番号（PIN Code，数字4桁）認証と組み合わせた2要素認証により，セキュアな本人確認が可能である。

(3) 導入メリット

■「入れない」対策の強化

既存のアプリケーションにアドオンする形でワンタイムパスワード認証の導入が可能であり，既存システムへの不正侵入／なりすましに対しより強固な対策が実現できる。

■ 利便性の向上

カード上のボタンを押して暗証番号（数字4桁）を入力するという単純操作で認証が実行されるため，従来型の認証トークンのように表示されたワンタイムパスワードを人手で再入力する必要がなく，操作性が大幅に向上する。特にモバイルユーザでは，ICカードリーダ等の認証機器を持ち歩く必要が無く使い勝手がさらに向上する。

■費用の削減

特殊な認証機器が不要であり，カードに添付されている小型マイクまたは安価な市販マイクが利用可能なため，従来型認証トークンに比べて1／2程度の費用で導入可能である。また従来型トークンでの人手入力ミスに伴なう

無効化からのヘルプデスクによる復旧対応等が減少し，維持管理負担についても削減可能である。

システム概要

本システムは，既存および新規の応用システムまたはアプリケーションにおいて個人認証が必要な箇所に組込み可能な認証サブシステムである。

図2に応用システム適用の概念図を示す。ユーザが音響署名カードのボタンを押すと“音”になったワンタイムパスワードが発生し，これをPC，PDA，Thin Client等データ端末上のクライアントソフトウェアがキャプチャした後，暗証番号の入力を要求する。利用者が暗証番号を入力するとワンタイムパスワードと暗証番号が認証サーバに送信される。認証サーバでは受信したワンタイムパスワードと暗証番号が検証され，正当性が確認されると応用システムまたはアプリケーションにその旨通知されて当該ユーザのアクセスが許可される。

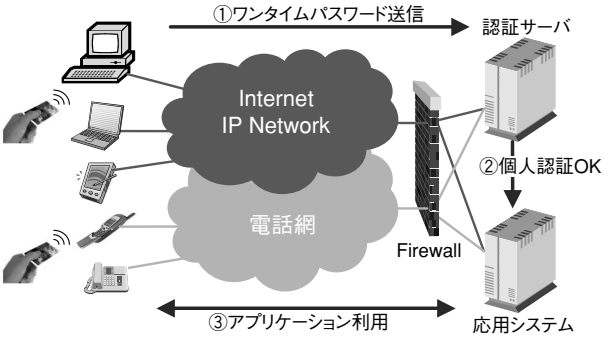

図2　システム概念図

認証の仕組み

本システムは，認証トークンである音響署名カード，端末で動作するクライアントソフトウェア，およびサーバ上の認証ソフトウェアにより構成される。**図3**に認証の仕組みと処理概要を示す。

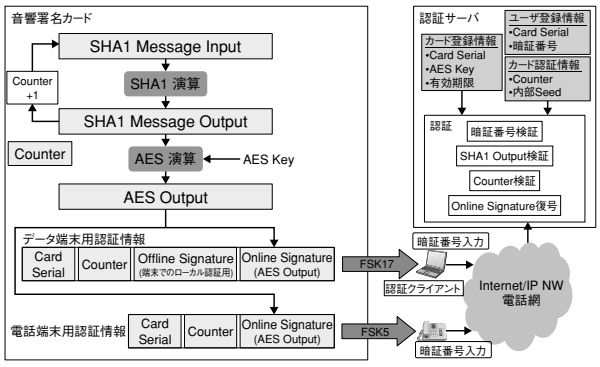

図3　認証方式構成

カード内部における認証情報の生成とサーバでの認証との間ではカウンタ方式により論理的に同期がとられている。

(1) 音響署名カードの構成

図4に示すように音響署名カードには，演算処理プロセッサ，スピーカ，押しボタン，およびバッテリが組込まれている。

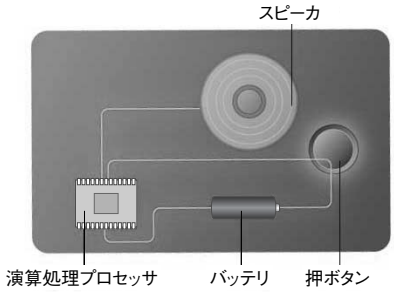

図4　音響署名カードの構造

ボタンを押して生成されたワンタイムパスワードは，周波数偏移変調方式（FSK）により変調されスピーカより音響信号として出力される。PC等データ端末用の信号と電話端末用の信号の両方が出力可能であり，短くボタンを押した場合にはデータ端末用の信号，長く押した場合にはデータ端末用の信号と電話端末用の信号の両方が連続して出力される（**表1**）。

また内蔵バッテリ容量の条件により，カード利用可能期間の目安は，1日あたり平均10～20回の認証操作にて3年間である。

表1　音響署名カード主要諸元

項　目		主要緒元
名称		V27CT音響署名カード
形状		53H×85W×2D ㎜
音響信号変調方式		周波数偏移変調方式
種類	データ端末用	FSK17
	電話端末用	FSK5
利用期間(寿命)		3年 条件:1日あたり平均10～20回のカード使用

(2) 認証情報生成方式

音響署名カード上のボタンが押されると，格納されている前回のハッシュ情報（SHA1 Message Output）が新しいシードとして入力されてハッシュ演算（SHA1アルゴリズム）が行われ新しいハッシュ情報が生成される。同時にカウンタが更新される。生成された新しいハッシュ情報は暗号化（AESアルゴリズム）され，カード番号

(Card Serial) および更新されたカウンタ値 (Counter) と共に音に変調されて送出される。また生成されたハッシュ情報はカード内部に保持され次回のハッシュ演算のシードとなる。

カード製造時にはカード番号 (Card Serial) ごとに異なる初期入力シードが使われるため，カードごとかつボタン操作する度に毎回異なる情報が生成されることになる。したがってこれを使い捨てのワンタイムパスワードとして利用することが可能となる。

データ端末用には，Offline SignatureとOnline Signatureの2種類の認証情報が生成される。この内，Online Signatureはネットワーク経由で送信されて認証サーバで検証される情報であり，Offline Signatureはデータ端末でのローカルな認証に使用される情報である。両情報ともに生成の方式は同じであるがカード製造時の初期入力シード情報が異なっている。

(3) データ端末機能

音響署名カードより送出された音響信号はデータ端末のマイクロフォンを通じてキャプチャされ，認証クライアントにより復調されて元の認証情報に戻される。認証クライアントは，この認証情報とユーザが入力した暗証番号を連携するアプリケーションを経由してサーバに送信し認証を要求する。

(4) サーバでの認証機能

認証サーバではあらかじめ登録されているユーザ情報，カード情報および内部認証情報により，端末より受信した認証情報 (Counter，Online Signature，暗証番号) の正当性が検証される。

受信Counter値は保存されている過去の認証成功時の値と比較され，差分が規定値以下の場合だけ有効となり，内部シード値を用いて当該Counter値に対応するハッシュ値が計算される。受信Online Signature (AES Output) はAES Keyによる復号化によりSHA1 Message Outputに復元され，この復元されたSHA1 Message Output は受信Counter値から求められた上記ハッシュ値とのチェックにより正当性が検証される。

(5) 認証クライアント

本システムではユーザが日常的に出会う認証要求ステージに対応して次の基本的な認証機能が提供されている。

■ アクセス認証

VPN，RAS等ネットワーク資源およびグループウェア等クライアント／サーバ型アプリケーション利用時のユーザ認証に使用され，固定ID/Password認証をよりセキュアなワンタイムパスワード認証に高度化できる。

■ Webログイン認証

Webページ上から認証情報，暗証番号を直接キャプチャしユーザを認証する。ID/Password不要の仕組みを構築可能である。

■ Webログイン用ID/Passwordの代入

Webページ上から認証情報，暗証番号をキャプチャしてユーザを認証後，認証サーバに登録済のID/Passwordを当該ページに代入してログインする。ID/Passwordをより安全に管理できる。

■ SSL VPNログイン認証

SSL VPNログイン時のユーザ認証が可能である。端末用のソフトウェアは必要時ダウンロードされるため，個別のインストール作業は不要となる。

■ PCログイン認証

Windows PC起動時のローカルユーザ認証が可能である。

端末では上記の認証機能に対応するクライアントソフトウェアが走行し，音響署名カードからの認証情報のキャプチャと復調，暗証番号の受信，および認証サーバとの情報交換により認証動作が実行される。**表2**に認証クライアントの種類を示す。

表2　認証クライアント

クライアント名称(形式)	認証機能 (用途)	概要
MemoKEY (Application)	アクセス認証	VPN,RAS等各種ネットワークおよびアプリケーション利用時のユーザ認証。
WinLogon (Application)	Windows PC ログイン認証	Windows PC起動時のローカルユーザ認証。
WebPass (IE Plug In)	Webページ ログイン認証	IE Plug Inがキャプチャした認証情報を認証サーバで検証しユーザを認証。
MemoPass (IE Plug In)	Webページログイン用ユーザID,Passwordの代入	IE Plug Inがキャプチャした認証情報を認証サーバで検証しユーザを認証後，あらかじめユーザが登録した固定ID, Passwordを当該ページに代入しログイン。
SSL VPN用クライアント (Active X)	SSL VPNログイン認証	ActiveXがキャプチャした認証情報を認証サーバで検証しユーザを認証，ログインを許可。

(6) 主要アプリケーションへの対応

本システムで提供される認証機能により，広く普及しているアプリケーションにおいてワンタイムパスワード認証が可能となる。**表3**に対応可能な主要アプリケーションを示す。

導　入　事　例

社内ネットワークへの不正侵入およびなりすましの防

表3　主要な対応アプリケーション

分　類	対応アプリケーション
MS Windows Network Access	MSWindows 2000/XP Network Access MS Windows 2000/XP RAS MS Windows 2000/XP Remote Desktop
MS Windows Application	MS Outlook 2000/XP MS Outlook Express MS .NET Messenger Service MS Money
VPN	Nortel VPN Client Cisco VPN Client Checkpoint VPN1 SecuRemote Netscreen VPN Client
その他	Lotus Notes R5/R6 Citrix ICA Client VNC Client Biz/Browser 4.0

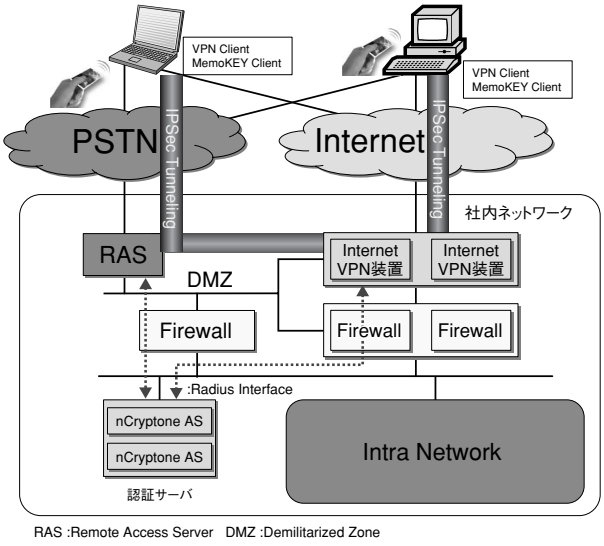

図5　リモートアクセスログイン認証導入例

止を目的に本システムを導入している事例を示す。この事例では図5のようにInternet VPN方式およびRAS接続方式によりリモートアクセスが可能であり，VPNログイン時の認証およびRAS接続時の認証に本システムが使われている。

Internet経由リモートアクセスでは，ユーザの端末にてVPNクライアントが起動されると認証クライアント（MemoKEY）が連動して図6のウインドウが表示される。ここでカードを鳴らすと認証情報がキャプチャされ，同時に暗証番号入力ウインドウがポップアップする。

認証クライアント（MemoKEY）により取り込まれた認証情報と暗証番号はVPNクライアントに渡されVPN装置との間でチャレンジシーケンスが起動される。

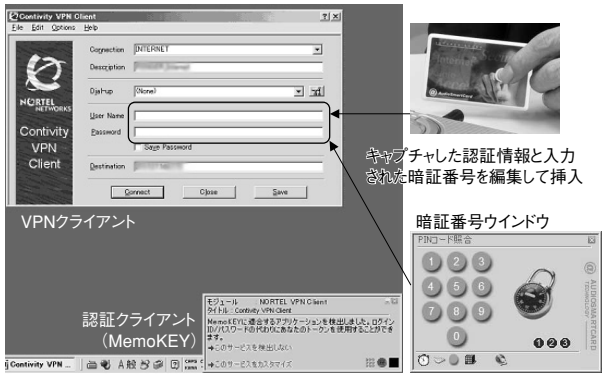

図6　リモートアクセスログイン操作画面

VPN装置が受信した認証情報はRADIUSインタフェースを通じて認証サーバに送られて検証される。認証結果はレスポンスシーケンスを通じて端末に通知され，成功の場合はIPSecトンネルが形成されてVPNコネクションが確立し，社内ネットワークへのアクセスが可能となる。この事例では社内ネットワークへのログイン操作が

① VPNクライアント起動操作
② 音響署名カードボタン操作
③ 暗証番号（数字4桁）入力

という3回のアクションで完了するため，ユーザからは従来の認証トークンに比べ操作が簡単で非常に使い易いとの評価を得ている。

お　わ　り　に

音響信号を利用した個人認証システム「音響署名カードシステム」の特徴，技術内容，導入事例について述べ，既存の固定ID/Password型個人認証をより安全なワンタイムパスワード型認証に移行可能であることを示し，併せて操作性の向上についても紹介した。

個人認証機会の増加と厳密性の要求に伴いワンタイムパスワード型認証の導入は着実に増加する傾向にあり，顧客への導入コンサルティングを通じて本システムとアプリケーションが融合したセキュリティソリューションの提供を行っていく。特に電話網を利用できる点が本技術の大きな特徴であり，これを活用したソリューションの開発にも取り組んでいきたい。 ◆◆

●筆者紹介

蛭子隆彦：Takahiko Ebisu. 沖コンサルティングソリューションズ株式会社