

au携帯電話用のモバイルトークンも自社開発 携帯性に優れた低価格の「KDDIワンタイム パスワード認証サービス」を提供

ユビキタス・ネットワーク社会の到来に向けた環境の整備と、高品質で利便性に富んだソリューションを提供する「ユビキタス・ソリューション・カンパニー」を目指すKDDI株式会社は、リモートアクセスユーザ向けの認証基盤を一新しワンタイムパスワード認証サービスを新たに低価格で提供する。また、本サービスでは自社内にインターネットVPNなどのリモートアクセス環境を持つユーザに対しても、認証機能の提供を行う。これによりSOHOから大企業に至るまで、ワンタイムパスワードの利用が可能となり、特に運用面、コスト面でワンタイムパスワードの導入に敷居の高かったリモートアクセスユーザには朗報である。



KDDI株式会社
ソリューション商品開発本部
ソリューション開発1部 開発1グループ



課長
水本 政宏氏



課長補佐
佐藤 優氏

KDDI株式会社
ソリューション商品開発本部
ソリューション企画部
ネットワークソリューショングループ



課長補佐
吉泉 浩平氏



課長補佐
川本 孝明氏



主任
吉川 元規氏

ユーザプロフィール

KDDI 株式会社

<http://www.kddi.com/>



携帯電話事業、ブロードバンド事業、ソリューション事業といったあらゆる情報通信サービスを一社で提供する唯一の通信事業者である。「ユビキタス・ソリューション・カンパニー」を目指し、いつでも、どこでも、より自由な情報へのアクセスが可能で、付加価値の高いソリューション・サービスを提供している。

- 資本金：141,851百万円
- 社員数：約9,000名(2003年4月1日現在)

リモートアクセス時の固定パスワードの利用は危険！ ニーズは低価格なワンタイムパスワード

KDDIでは既にリモートアクセスサービスのオプションとして固定パスワードによるRadius認証機能を提供しているが、最近ではワンタイムパスワード認証サービスへの要求が多く、新たに認証システムを構築した。その必要性に関して、担当されたKDDI株式会社 ソリューション商品開発本部の各氏に伺った。

「リモートアクセス時の固定パスワードによるベーシック認証では、パスワードの成りすましによる不正アクセスの危険性があります。固定パスワード使用時のセキュリティレベルを維持するためには、定期的なパスワードの更新が必要となりますが、運用面、管理面での負荷が非常に大きくなります。また、固定パスワードが漏洩した場合には長期間にわたって不正アクセスに気づかないことも考えられます。

その対策として、PINコード(暗証コード)とトークンの二要素認証により、使い捨てのパスワードを生成するワンタイムパスワードの利用は有効な手段となります。」(吉泉氏)

「実際にこれまでもリモートアクセスユーザからのワンタイムパスワード認証サービスの要求は多くありました。しかし、実際の導入には価格が問題視される場合が多いために、セキュリティレベルを下げずに低価格でのサービスの提供とモバイルトークンの開発による携帯性(利便性)の向上を目指

して、今回の認証システム構築の検討に入りました。」(水本氏)

低コストで半永久的に使用できる ActivCard au携帯電話用モバイルトークンも独自開発

KDDIでは各メーカーのワンタイムパスワード製品を比較検討した結果、米国ActivCard社のActivCardを選定した。ActivCardは世界で100万人以上のユーザが利用する実績あるワンタイムパスワード製品である。

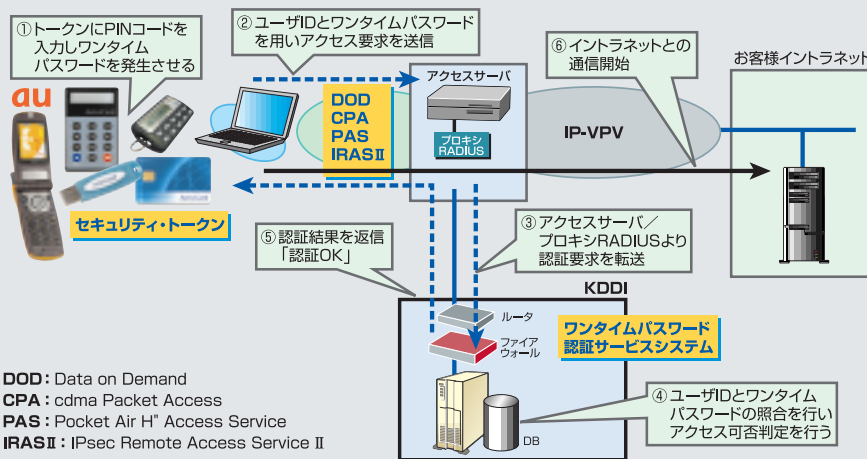
「ActivCardを選定するに至るまでには、それ程時間はかかりませんでした。第一の選理由は、ActivCardにはライセンスに有効期限がないために、低価格でサービスの提供が可能となることです。電池の交換も可能であり交換用のボタン電池もコンビニなどで購入できるために、半永久的な使用が可能となります。第二の選理由は、2変数でパスワードを生成するトークン製品が多いなかで、ActivCardは「クロック値」、「イベント値」、「シークレットキー」と言う3つの変数を基にパスワード生成すること、PINコードをネットワーク上に流さないという点で他社製品と比べセキュリティが強固であると判断しました。」(川本氏)

ActivCardのトークンには、電卓タイプ、キーホルダータイプ、スマートカードタイプ、USBキータイプのラインナップがありユーザの利用形態に合わせた選択が可能とな



KDDIワンタイムパスワード認証サービス

サービスイメージ図



トークン設定費は1トークン当たり2000円で、利用料金はネットワークの規模により異なる。トークンのライセンス単価はライセンス数増加にしたがって割安となる。特にモバイルトークンでは4000円以下の低価格を実現している。*「今回のシステム構築により、他社サービスと比較して低価格でのワンタイムパスワード認証サービスの提供が可能となりました。9月からサービスを開始していますが、予想以上の反響を得ており、ワンタイムパスワード認証へのニーズの大きさを実感しています。」(吉川氏) 更に、KDDIではセキュリティトークンの紛失・盗難の際、該当のユーザIDを無効にする操作や、一時的に有効な固定パスワードを発行する操作をお客様システム管理者が実行できる「Webヘルプデスク機能」も無償で提供している。

*2003年9月時点の料金プラン

る。更に今回、KDDIは携帯電話を「ユビキタス時代の必需品」と考え、JAVAによるau携帯電話用モバイルトークンも独自開発した。

「このモバイルトークンにより、トークンの携行忘れや携帯する煩わしさからユーザを解放し、トークン紛失の危険性も低減すると思われま。また、自社開発により開発コストが抑えられ低価格での提供が可能となりました。」(佐藤氏)

「au携帯電話用のモバイルトークンの開発は、携帯電話サービスを提供するKDDIならではのメニューでもあり他社サービスとの差別化も意識しています。また、携帯電話の次期プラットフォームとして注目されるBREW™ (Binary Runtime Environment for Wireless)*上で動作するモバイルトークンもリリース予定となっています。」(水本氏)

*米国クアルコム社がCDMA携帯電話機用に開発したアプリケーションプラットフォーム

信頼性、安定性、継続性が要求されるユビキタス・ネットワークの認証システム

本認証システムの構築を担当した株式会社アクシオへの要求は、いつでも、どこでもアクセス可能な「ユビキタス・ネットワーク」の認証システムであるためにその信頼性、安定性、継続性についての要求は非常に厳しいものとなった。

最終的に認証サーバ、ディレクトリサーバ、データベースサーバはロードバランスによる負荷分散と冗長構成が必要となり、また、各サーバはサービスを停止することなくバックアップの取得が可能構成とした。これにより障害時にもユーザが意識することなく継続的なサービスの利用が可能となった。更にパフォーマンスに関してはカタログスペックだけでは実際の性能判断には不十分として、ユーザ数の需要予測からベンチマークテストを行いその性能を数値で証明した。

ここで将来的なサービス拡張の可能性に関して伺った。

「短期的には、サーバへのアクセスログなどの管理情報を報告する付加サービスなども検討しています。将来的には、今回のシステムを認証基盤としてSSO (シングルサインオン)、デジタル証明書によるPKI連携やアカウント連携なども考えています。また、公衆無線LANサービスであるネオモバイルからのアクセスへの利用も検討範囲となります。実際に今回の認証システムは、これら将来的なサービス拡張を考慮したシステム構成となっています。」(吉泉氏) また、同氏は今後のサービス拡張時もアクシオのソリューションに大いに期待されているとのことであった。

*記載された内容は予告なしに変更する場合があります。
 *掲載の社名、製品名は一般に各社の商標、登録商標です。