先進事例にみる統合的情報セキュリティのデザインと実現

情報セキュリティにおける昨今の潮流としては、個人情報保護法に加え、差し迫る日本版SOX法の施行を見据えた内部統制の観点からセキュリティ状況の可視化の必要性を挙げることができます。またユーザ企業様や官公庁様では、ITシステムの増加にともなうID/パスワード管理の限界や雇用環境の流動化により、セキュリティリスクへの認識が非常に高まってきています。本稿ではある先進的なお客様企業の事例をベースに、認証情報など様々なユーザ情報を一元管理し、かつICカードを社員証として共通利用することで利便性や運用性での様々な課題を解決して運用にいたるまでの進め方についてご紹介します。

はじめに

最近の大手企業におけるセキュリティ要件では、入退室(館)をはじめ、ネットワークアクセスやPCなどトータルでのセキュリティ強化とともに、ICカード化した1枚の社員証を使用した「認証」と「運用管理」の基盤作りを挙げられるケースが増えてきました。

これらのお客様では、それぞれ認証の仕組みの異なるシステムに対するICカードの共通利用実現に加え、ICカードのライフサイクルに従った運用管理や個々のセキュリティシステムへのデータ連携をいかに実現し、スムーズで容易な運用管理を行えるかがお客様に対する提案のポイントになります。弊社のセキュリティ関連事業においては、自社の各種セキュリティ製品が優れているというのみならずNECが自らが使い、運用している社員証ICカードやディレクトリ認証基盤での利用実績、およびそれらの実績で培ったノウハウを生かした総合的な提案力が評価され様々な業界のお客様に採用いただいております。

本稿でご紹介するシステムは、弊社が実際に先進的なお客様にご提案し、一緒に作り上げられた事例をベースに、いくらか一般的に記載したものです。

提案システムの概要

図1に示すシステム概略図に基づき、システム概要を説明します。

まず中核となるICカード運用管理システムでは、ユーザ情報の登録とともにICカードの発行申請、失効申請、再発行などをWEB上で一元的に行うことができ、これらの操作で更新された情報を必要とする各種システムへデータ配信することで、ICカード運用に関わる作業を軽減します。ICカード利用を行うシステムには、入退管理システム、PCセキュリティ、各種業務システム、リモートアクセスなどがあり、ユーザIDだけでなくPKI認証が必要なシステムも混在する場合には、接触/非接触の両インタフェースを1チップで実現するデュアルカード(例:FeliCaデュアル)を社員証として利用可能です。ICカード運用管理システムからはCAサーバ(CA:Certificate Authority/電子

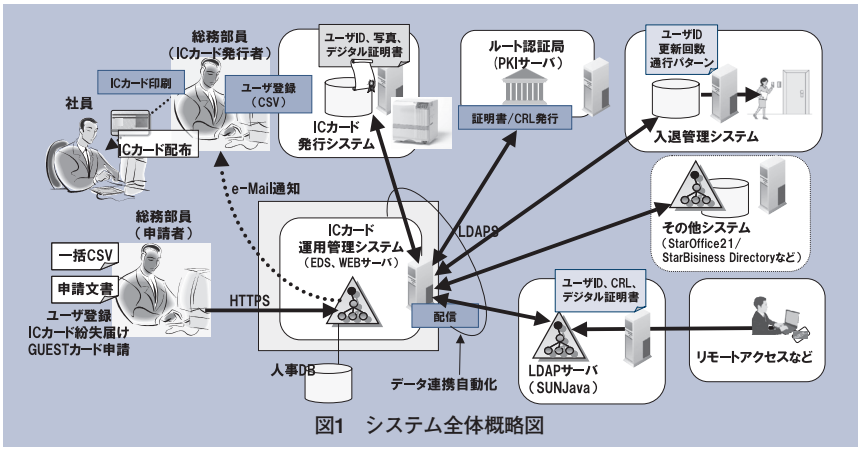

図1　システム全体概略図

証明書を発行する認証局)やカード発行機にもデータ連携が図られており、カードの失効や追加発行が容易に行えるシステムとなっています。

システム構成と機能

本システムの基本構成を**表**に示します。また主要システムの連携内容や機能を以下に示します。

(1)ICカード運用管理システム

本システムは、①カード情報や認証情報を格納するLDAP(LightWeight Directory Access Protocolの略。ディレクトリデータベースにアクセスするための標準プロトコル)サーバに加え、②各種情報の追加や諸申請などカード運用に必要なアプリケーションで構成されています。提供機能は以下のとおりです。

1) お客様および関係会社の人事情報や委託関係者情報の追加
2) 人事情報には含まれない各種ユーザ情報(ICカードの更新回数、顔写真データ、デジタル証明書、通行パターン、有効期限、ID/パスワードなど)のデータ反映
3) ICカード発行システムやプライベートCA局、入退管理やPC/ネットワークアクセスといった各システムの認証DBへのデータ連携(LDAPS)
4) カードの有効期限や通行パターン、その他各種ユーザ情報の参照・検索

本システムでは総務部員の方が運用されることを想定し、分かりやすく操作性の良いインタフェースを実現しました(**図2**参照)。たとえばICカードを紛失した場合には、ブラウザから対象者の失効申請をするだけで、CA局への失効要求に加え、発行された失効リストを必要とする各システムに配信、入退管理システムに対しては紛失カードの更新フラグから対象カードのみ使用不可にするなど、個々のシステムでわざわざ失効処理しなくとも自動反映されます。またカード発行申請がなされた場合には、CA局へのデジタル証明書の発行要求に加え、入手したPKCS#12ファイル(PKCSはPublic Key Cryptography Standardsの略。公開鍵暗号技術をベースとした規格群で、#12ファイルは電子証明書と秘密鍵が一緒に格納されています)やカード発行に必要なデータ(その他カード内書き込みデータ、写真などの券面情報)がカード発行システムに自動送信(送信完了後メール通知)され、かつ新たな認証データが各システムに自動反映されます。各システムが管理

表　システム基本構成

No.	連携システム名（例）	使用ソフトウェア、OS	
1	ＩＣカード運用管理システム／顔検索システム	HW	Express5800
		OS	Red Hat Enterprise Linux
		DB	EnterpriseDirectoryServer（NEC製LDAPサーバ）
2	ICカード発行システム	HW	発行機：CX320、PC
		OS	WindowsXP、Internet Explore r
		DB	Cards3000
			LDAP Connector（NEC製）
3	CA局	OS	Windows2003
		CA	CertWorker（NEC製CAサーバ）
4	入退管理システム	HW	SAFEWARE-iX、Experss5800
		OS	Windows2003、Internet Explorer
		DB	Oracle9i
			LDAP Connector（NEC製）
5	LDAPサーバ	OS	Solaris9
		DB	Sun Java System Directory Server
6	業務系ポータルシステム	OS	Windows2003
		DB	StarOffice21/BussinessDirectory（NEC製）
			（LDAP Connector）

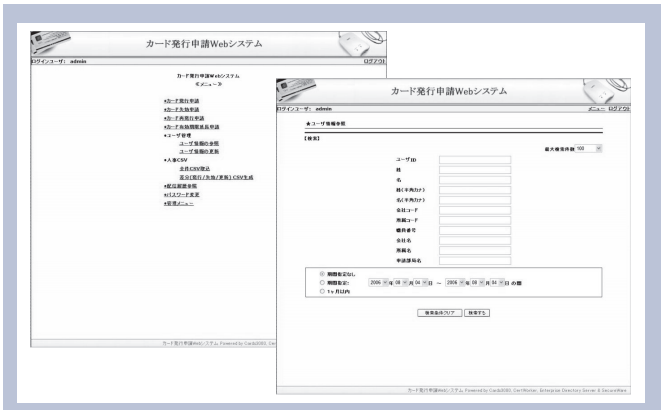

図2　WEB操作画面

するユーザ情報やDBシステムはそれぞれ異なりますが、本システムでは、その差異を自動的に変換し反映することが可能となっています。さらに本システムはICカード利用以外の認証情報も一元的に管理されており、必要に応じてID/パスワードの反映も可能です。ユーザ情報の参照機能では、たとえばICカードを持たない方(カード忘れなど)が入館しようとした場合、警備員がブラウザから顔写真検索による本人確認をも容易に行うことが可能となっています。

(2)ICカード発行システム

本システムは、①カード内データや写真などの券面データを格納するDBと発行ツール、および②カードプリンタで構成されます。FeliCaデュアルでは、FeliCa OS領域(非接触用。入退管理用データなど格納)、Java OS領域(接触用。デジタル証明書など格納)の各々へのデータ書き込み(**図3**参照)が必要ですが、本システムでは、券面印刷に加え、各領域へのデータ書き込みを1プロセスで実現しています。したがって、発行システム操作者はメール受信後に対象者のカード発行を簡単操作で行うことができます。

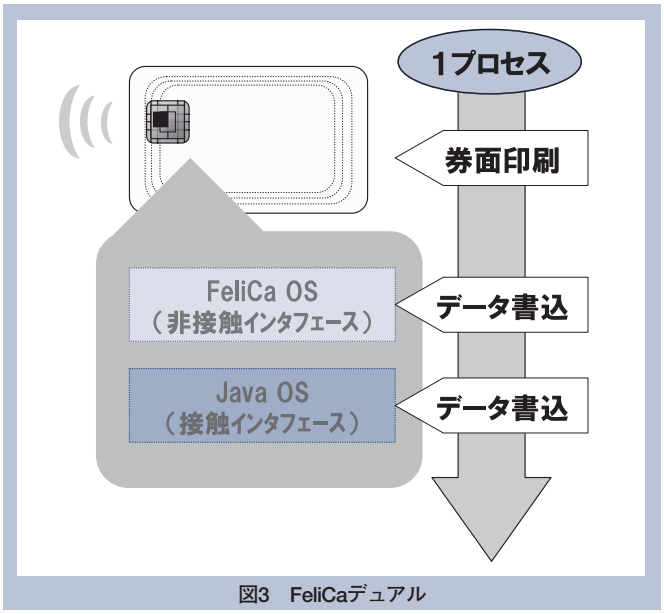

図3　FeliCaデュアル

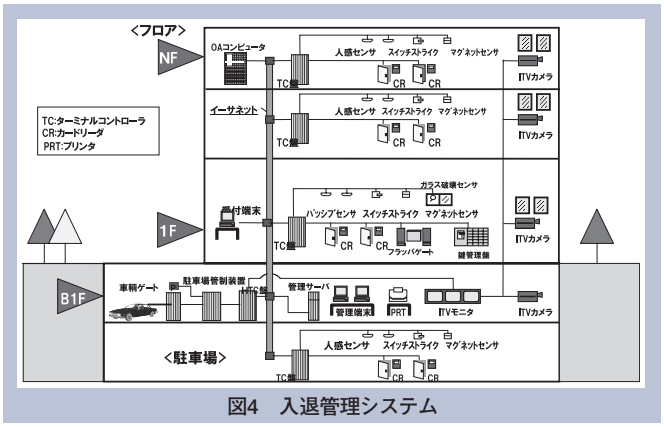

図4　入退管理システム

(3)入退管理システム

本システムは、①ユーザ/カード情報や通行パターン、入退履歴情報などを管理するサーバと、②ゲート通過時の認証用カードリーダ、および③サーバとカードリーダ間の通信を制御したり、センサ/カメラなどのビル管理設備との接点を有するターミナルコントローラなどで構成されます(**図4**参照)。それぞれはIP化されており、既存LAN配線の有効利用やフロアレイアウト変更時などの工費削減が図れるだけでなく、各種データ反映がスムーズに行え、大規模ユーザまで対応可能なシステムです。ユーザ認証に必要なデータはサーバから各カードリーダにあらかじめ配信され、認証はカードリーダ単体で行われるため、認証が高速でかつネットワークやサーバ障害の影響を受けず入退館(室)が可能です。カード紛失時などはカード発行申請WEBサーバから入退管理サーバ経由で速やかに各カードリーダにデータ反映がなされます。

導入ユーザにおける今後の展開

前述でご紹介したシステムの導入ユーザでは、今後入退管理システムの各拠点展開や、NW/ITセキュリティへの連携などICカードの利用範囲を拡大し、さらなるセキュリティ強化と運用性、利便性強化を計画中です。このため

には、ICカード運用管理システムにおけるユーザ認証情報の統合化にむけ機能強化と各システムとの連携強化を実施していく予定です。このように段階的に利用範囲を拡大していくためにも、認証情報の統合と運用管理の一元化は必須であり、今後ますますニーズが高まる領域であると考えます。

むすび

ICカードを共通の認証媒体としたシステムや、統合認証基盤の構築は、お客様の運用まで踏み込んだ付加価値を提供でき、弊社の強みを発揮できる領域です。前述でご紹介した導入システムを元に申請・承認ワークフローの機能も盛り込み、弊社ではSECUREMASTER/EnterpriseIdentityManagerとして汎用的な統合ID管理ツールのリリースを予定しています。しかし、統合ID管理ツールは魔法の箱ではありません。お客様ごとに連携させるシステムや管理情報は異なり、将来の拡張も考慮したうえでどのような情報をいかに管理するか、どのように各システムへのデータ連携(プロビジョニング)を図るかの要件定義が重要であり、IT/ネットワーク、セキュリティにおける各領域の総合的なSI力の発揮がいっそう求められると考えます。

執筆者プロフィール

宮原 博昭
エンタープライズソリューション事業本部
UNIVERGEソリューション推進本部
ブロードバンド推進部
マネージャー

問合せ先
日本電気株式会社
UNIVERGEソリューション推進本部
ブロードバンドセキュリティ推進部
住所：〒108-0075 東京都港区港南2-16-1
品川イーストワンタワー7F
TEL：03-6405-0730