1F-3 企業内システムにおける電子証明書を用いたセキュリティ管理

山本実香
日本アイ・ビー・エム システムズ・エンジニアリング(株)

1. はじめに

インターネット化が急速に高まる中、多くの企業がインターネットを使用した業務展開を始めてきている。インターネット・モールやインターネットバンキングなどを始めとする不特定多数の顧客を相手に個人情報や金銭をやり取りする業種においてインターネットセキュリティ対策を行なうことは言うまでも無い。現在では、SSL や SET などデータ暗号化およびクライアント認証を行なう標準プロトコルを使用することによりインターネットのさまざまな脅威を防御している。それでは、上記にあげた以外の企業に関してはどうだろうか？やはりどの企業も何らかの形で業務がインターネットと関係している。例えばそれがグループ会社間とのインターネットメールのやり取りであったり、Web サーバー上でのデータ公開であったりする。SSL クライアント認証を使用することにより企業内システムへのシングルサインオンが実現可能となることや、S/MIME インターネットメール暗号化によりインターネットを介した企業間取引が安全となることなど、電子証明書におけるセキュリティ管理は現在企業が抱えているさまざまな問題を解決してくれる。しかし、これらの企業が電子証明書を使用したセキュリティ管理をしているという話はあまり聞かない。本稿では、インターネットを主としたビジネスを行なっていない一般の企業をターゲットとし、電子証明書によるセキュリティ管理が普及していない問題点や今後の運用管理における方向性についてビジネスの観点から論じる。

2. 企業に立ちはだかるさまざまな壁

インターネットビジネスを主としていないからといって企業が何も考えていない訳ではない。多くの企業が盗聴やなりすましによる脅威からセキュリティを確保するために X.509 電子証明書の使用に向かいさまざまな検討を行っていると思われる。しかしそこにはさまざまな問題点が浮上し、企業側ニーズが急速に高くなっている現実とは裏腹に実現にはなかなか到っていない。以下にビジネス面から見た大きな問題点を 2 つあげる。

- コスト問題：SSL や S/MIME を行なうための電子証明書を発行するために「認証局(CertificateAuthorities)」を構築する必要があるが、現在のネット社会では公的に信頼されている認証機関に証明書の発行・管理を依頼するという形態が一般的である。しかし、そこには膨大なコストが必要とされる。
- 運用管理問題：第三者の CA を隔てると証明書の申請・更新の度に第三者との間で手続きを行なう必要があり、特にクライアント証明書を使用する場合にはユーザー個人が手続きを行なわなければ行けない。「ユーザー個人に委ねられてしまう作業」を企業側が管理するのは非常に難しく、管理する上での大きな問題となる。

3. 独自 CA の構築

上記 2 つの問題点を解決する方法に「独自 CA を構築する」という案があげられる。最近では企業が独自に CA を構築するためのソフトウェアが出てきていることや企業システム内にて使用しているグループウェア製品に CA 構築機能が追加されたことから、第三者の認証機関に膨大なコストをかけて委託しなくても電子証明書

Security Management of external system between related company with using X.509 certificate
Mika Yamamoto
IBM Japan Systems Engineering Co., Ltd.
1-1 Nakase Mihama-ku, Chiba-shi, Chiba 261-8522, Japan

を使用したセキュリティ管理が実現可能である。独自の CA を構築した場合の唯一の問題点は、「その CA が信頼できるものであるか誰も分からない」点である。しかし、不特定多数のユーザー相手に商売をする訳ではなく、決められた社内及び関連会社・グループ会社ユーザー間でのみ発生する業務に対してのセキュリティを確保する分には独自の CA でも何の問題もないはずである。独自の CA を構築するソフトにも公的な認証局からの署名をもらって実現できるものもあれば、最近では電子証明書を登録する「登録局」は企業独自に構築・管理可能とし、実際に発行する「発行局」は今まで通り公的な認証機関が管理するというオンサイトサービスを始めた認証機関もある。これも、前にあげた運用管理の問題点から発生した企業の強いニーズによるものと考えられる。しかし、結局のところコスト面からすれば証明書の数分だけ認証機関に料金を支払わなければいけなく、問題が全て解決したことにはならない。コスト面からして最も良いのはやはり独自の CA を構築することで、特に既にグループウェアを使用している企業で、その製品の機能を利用すれば、全くコストをかけずに電子証明書を用いた企業内セキュリティ管理を実現することが可能となる。

4. 電子証明書の運用管理

X.509 証明書管理での最も大きな問題点は、新規登録時と更新時の作業である。一般的に秘密鍵が改ざんされる可能性を押さえるという安全性から、認証局が発行する証明書の有効期限は 1 年というものが多く、毎年証明書の更新手続きを行なう必要が出てくる。サーバー証明書だけを用いた SSL 暗号化を行なうのであれば更新手続きは管理者が行なえば良く、忘れることも間違えることも無い。しかし、SSL クライアント認証や S/MIME を行なうためにはどうしてもユーザー個人による手続きが必須であり、さらにその証明書はユーザー自身がクライアント上で保管するため、管理者による一元管理ができないという問題が発生する。認証機関によって手続きはさまざまであるが、Web 上で指定した項目を入力するだけで良いところもあれば、メールや FAX、郵送などの手段で手続きを求められることもある。これらの問題も独自の CA を構築することによりある程度解決可能である。実際、あるグループウェア製品を使用している場合、その CA 機能により S/MIME 用の個人証明書をサーバー側で一括作成でき、しかもその証明書はサーバー上のアドレス帳で保管・管理可能なため、LDAP サーバーのような公開鍵を共有させるためのサーバーを別途構築する必要もなくなる。しかし、この機能は残念ながらそのグループウェア専用のクライアントを使用している場合に限るものである。ブラウザを使用した SSL 機能においては、どのソフトウェアにおいても一般的な認証機関と同様の手続きおよび管理を要することとなる。但し、閉じられた企業内での管理であれば、ユーザーの代わりに管理者が一括して証明書を発行することも可能であると考えられる。

5. 考察

本来、決められた企業内でのみのセキュリティ管理を行なううことを考えれば、自社の限られたユーザーに対して証明書を発行するのに「個人を証明するもの」など必要無く、管理者側でまとめて作成しユーザーへ配布する(もしくは取りに来てもらう)ことが標準機能で可能となっても良いはずである。すなわち、グループウェアにおけるユーザーID 管理と同様の作業で済んでも良いはずである。現状にて電子証明書を使用したセキュリティ管理を行なうためには、本稿であげた問題以外にも、サーバーのパフォーマンスや LDAP サーバーの構築管理などさまざまな問題を残している。電子証明書を用いたセキュリティ管理はインターネットを主なベースとして展開している企業においては必須の要件であっても、その他の一般企業ではやはりコスト・運用面とのトレードオフにより採用を躊躇するケースが少ないくないというのが現状である。しかし今後は、近年のインターネット化の急速な発展に伴いインターネットにおける脅威が騒がれる中、多くの企業が SSL や S/MIME の使用を検討し始めるのは間違いない事実である。今後のプロトコル技術、製品技術の発展に大きく期待したい。