

社内情報の管理とPKIの簡単応用

本年4月よりJ-SOXが施行され対象となる会社はその対応が一応完了したり、遅れながら対応に多忙な毎日を過ごしていると思います。その中でITの役割も大きなものとなっています。文書の不法改ざんや情報流出についての防止策は一番重要なポイントです。そこで今回はマイクロソフトのサーバーソフトウェアの機能であるPKI (Public Key Infrastructure) = 公開鍵基盤という難しそうな仕組みにつき出来るだけわかりやすく研究してみたいと思います。マイクロソフト社の宣伝のようですが実際には認証、データセキュリティの最高峰であるPKIの仕組みが手軽に使用できるようになったのはマイクロソフト社がWindows2000サーバーからCertificate Serverを組み込んだおかげです。ここではPKIについて簡単にお話ししようと思います。

PKIは何に使えるのか

| |
|-----------------------------|
| 無線 LAN アクセスの認証 |
| 暗号化メール |
| SSL/TLS で Webアプリケーションアクセス認証 |
| アプリケーション、データの署名 |
| LAN・WAN におけるログオン認証 |
| リモートアクセス、モバイルアクセス認証 |
| VPN (IPsec)認証 |
| 暗号化ファイルシステム (EFS) |
| SSO 認証 |
| 株券電子化セキュリティ |
| e-文書法対応セキュリティ等 |
| ネットショッピングの双方向確認 |
| フィッシング防止 |
| 電子政府等への申請書等の証明 |

Active Directory や LDAP などと連動し認証に必要な秘密鍵付き本人”証明書“を発行し、証明書にある情報で認証、や検証を行い、データの暗号化と復号化も行う非常に便利な仕組みです。

実はマイクロソフトサーバーソフトウェア (Windows2000 サーバー以降) には PKI ソフトウェアが備わっておりプライベート CA や鍵の発行機能まで備わっており、PKI - Ready となっています。また、マイクロソフトの各種アプリケーションにはこの機能に対応が可能であり設定が非常に簡単に出来るようになっています。現在では Active Directory でグループポリシーを利用して自動的に証明書の登録が可能でユーザーには殆ど負担が掛かなくなっています。

メール、ワード、Excel、アクセス等々の文書やデータの保護

暗号化を思い起こす方も多い筈です。暗号化には AES がいいと言われています。暗号化をするには AES のような暗号化方式 (アルゴリズム) と暗号化に必要な鍵が必要です。簡単な鍵もあれば非常に高品質で解読が難しい鍵もあります。その鍵を生成するのが CSP または HSM というソフトウェアかハードウェアがあり、PKI の基本機能となっています。また、鍵の持ち主を証明する証明書が付いていますとさらにセキュリティは高まります。データや文書を送る場合に、通信途上の盗難や、暗号解読、またはよからぬ意図を持った変更などの可能性は全く無いとは限りません。セキュリティの

お仕事はそのような“万が一”にそなえ、防止する機能を持っています。暗号化は機密文書の閲覧を防ぎます。証明書は文書の出所を証明できる情報を提供でき、証明書は暗号化/復号化の鍵が付いています。文書やデータの出所、経路を確認することで不法な変更や、盗み見が防げます。人は秘密を覗きたい願望があるようです。見えれば見るのが人情です。不用意な文書の扱いが思わぬ噂で社内のトラブル、社内情報の流出の可能性があります。人間の考えた仕組みは 100%とは行きませんが PKI は何とか到達できる可能性のある仕組みです。今そこにその仕組みが使用できる可能性があります。

マイクロソフト Windows サーバーには PKI 機能が付属

Windows2000 サーバーが出るまでは PKI といえば導入の際は企業規模で導入が必要な仕組みで大きな投資と専門知識が必要でしたが、この機能がサーバーに組み込まれてから非常にスケラブルな PKI 導入が可能となりました。Windows 2000 の暗号化ファイル システム (EFS) やインターネット プロトコル セキュリティ (IPSec) などの機能については、ネットワーク管理者の側で特別な準備作業を行わなくても独自の証明書を発行できるため導入が非常に迅速に行えます。

PKI は公開鍵基盤と呼ばれていますが実際には一人のユーザーに特定のペアの鍵しか相互に暗号化、復号化が出来ない**公開鍵と秘密鍵のペア**が作られ提供されます。誰でも使用できる公開鍵 A で暗号化されたデータを秘密鍵の持ち主だけが解読できる仕組みと、自分のデータを自分のものである証明をするのに秘密鍵を使用して、受取る側が公開鍵（この場合検証鍵と呼ぶこともあります。）で検証する仕組みがあります。

また、マイクロソフトの Office にはこの仕組みに対応できる機能が同時に備わっています。この文書の後ろに例としてそれらアプリケーションの設定を簡単に説明していますので、それをご参考にご自分のアプリケーションでお試し下さい。

2004 年施行の電子文書法 (e-文書法) では企業が業務に使用した帳簿、注文書等が電子でできるくできるようになり商法が定める 10 年間という期間 (税法では企業は 7 年間) 倉庫に頼らずの保管が可能になりました。検索も早いので企業にとってもメリットがあります。これに PKI が使用されています。省スペースが実現できます。

e-文書法は、正式名称を「**民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律**」「**同法施行に伴う関係法律の整備等に関する法律**」という二つの法律を指します。

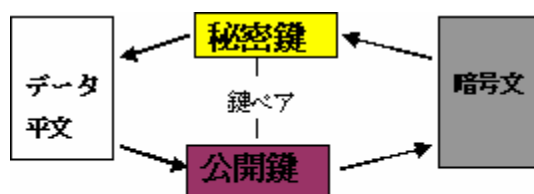
これからは電子政府や電子取引が本格的に個人も対応せざるをえない時代を迎えます。その先駆けが、住民台帳カードによる各種申請書の電子化です。具体的には税申告の電子化です。普通なら誰が書いて判を押しても受け取れましたが、本人証明の無い電子申告受けられないようになります。

PKI の基本技術

今までのお話は PKI の一般的用途と有効性、マイクロソフト社がサーバーソフトウェアに PKI サーバーを追加し、PKI の設定が非常に手軽になったことをまとめました。これからは PKI 技術の基本について “ なんとなく ” 理解していただくようお願いしたいと思います。

PKI は一人のユーザーに一つの公開鍵/秘密鍵と呼ばれる鍵ペアを用意し、データ暗号化に使用します。暗号解読にはこの特定鍵ペアのどちらか一方を持っていないと、暗号化、復号化が出来ない仕組みです。**あるペアの公開鍵で暗号化したデータは別なペアの秘密鍵では復号化出来ません。** どちらの鍵でも暗号化が可能ですが使用目的によって決まります。この基本的な鍵の使用方法は今後のお話を理解していただく基礎となります。

公開鍵で暗号化する場合

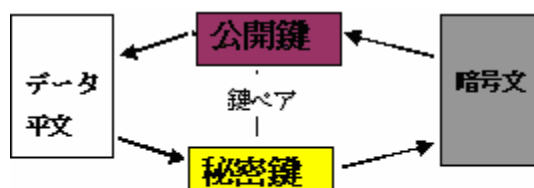


公開鍵暗号方式

公開鍵 = 暗号鍵
秘密鍵 = 復号鍵

秘密鍵で暗号化する場合

また、これと反対に秘密鍵で暗号化して公開鍵で復号化する方法があり。これを電子署名方式と呼びます。機能により呼び方を違える場合もあります。



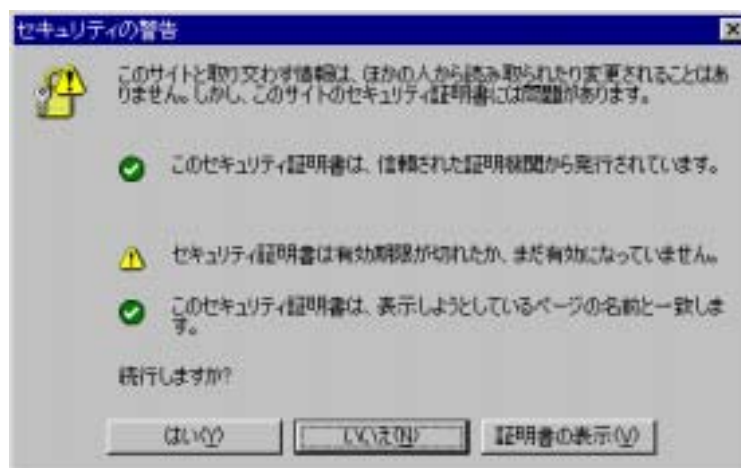
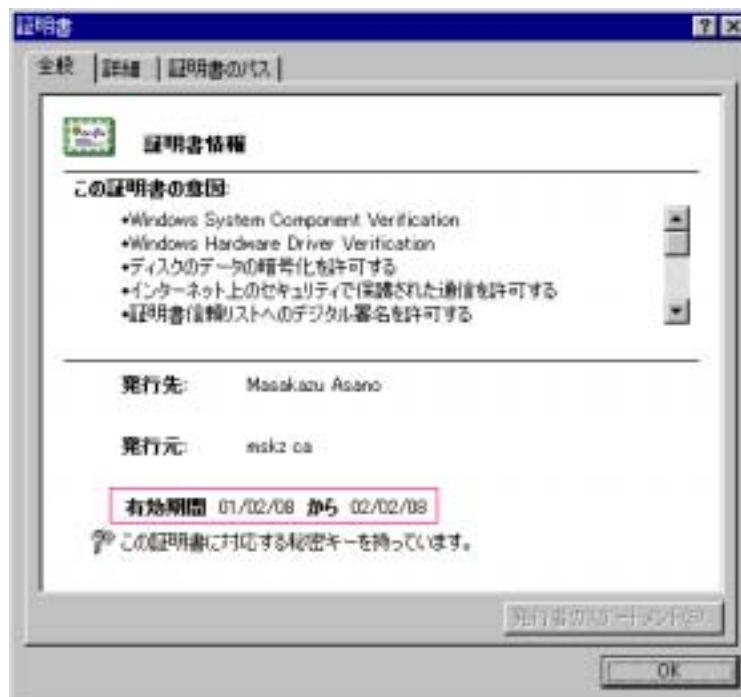
電子署名方式

秘密鍵 = 署名鍵
公開鍵 = 検証鍵

(電子)証明書

これらを都合よく利用して証明書を作りセキュリティを確保する仕組みが公開鍵基盤 = PKI と呼ばれるものです。証明書とはネット上でデータを送受信するのに暗号化、データの出どころを証明書安全性を確保するために使用したり、ネットアクセス権限などの確認に使用したりします。

証明書とは一人一人の本人であることの証明書で、本人情報と鍵が収納されています。記述される内容は管理者の方針で決められます。例としてこのような内容のものもあります。有効期間はとても大切です。



インターネットショッピングを利用する場合こんなダイアログの経験があると思いますがこれが証明書を交換している証拠です。また、ユーザーが本人である証明書を提示しているわけです。

PKIは何故安全性が高いのか

PKIは“Chain of Trust”または“Web of Trust”、信頼の連鎖という証明書が信頼ある証明書であることの証明を信頼ある第三者による証明書への署名という仕組みを使用して信頼性を確保するからです。大きくは2つあります。また、これら証明書や鍵の暗号化により本人以外は開けません。これにより暗号化されたファイルやデータは必要な人にしか復号化＝平文化できません。中間でのデータ改ざんは検知できるようになっています。この仕組みが Windows2000、2003 サーバーで簡単に使用できるようになっています。この仕組みで証明書を使用すると、シームレスにユーザーは安全にデータ交換、アクセスポリシーが得られ、全企業レベルでの信頼が確保されます。

通常行われている本人の検証方法



PKIの仕組み

1) プライベートPKI(プライベートCA)

この方式は企業が認証局となり社内証明書の検証を行う方法で、費用は初期投資と管理費ということになります。

2) 第三者認証局(CA)証明書によるPKI

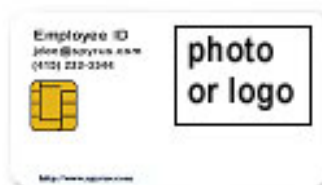
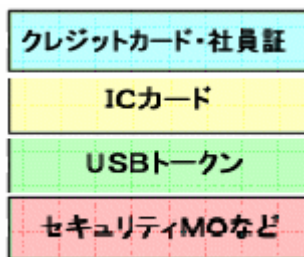
一般的にPKIと呼ばれる方法で、外部信頼ある認証局からの元証明書を使用して内部の証明書の検証を行うものです。この方法には色々な組合せがあり、非常に緻密な設計が必要です。元証明書の費用は一般的に1台のサーバーに対しては15-20万円/年、ユーザー一人は2500-5000円/年ほどの費用を認証局に支払うようになっています。

3) 1)と2)に組合せて2)の範疇に入るPKI

この仕組みを利用している企業は非常に高いセキュリティ意識と、大きな投資を行っていることが理解できます。

マイクロソフト社のWindows2000サーバーが出る前まではこの2)が一般的方法でしたので費用の点、設計の煩わしさ、管理の煩雑さによりPKIは残念ながら一般的ではありませんでした。また、この仕組みは歴史的なイメージがあり簡単には一般的に導入は進んでいないのが現状です。まずはプライベートCA方式で運用し、3)の仕組みに移行してゆくことも可能です。

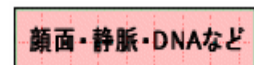
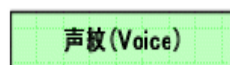
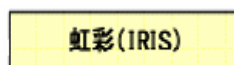
また生体認証等と組合せて3ファクター認証も可能です。



スマートカード



USB トークン



PKIの応用

KK ICH 3-5-17-408 Nishigotanda, Shinagawa, Tokyo 141-0031 Japan

Phone +81-3-3432-3336

<https://www.ich-one.com>

証明書のみによる検証

Web サーバー証明書などは典型です。これは Web サーバーが本当にアクセスする予定のサーバーなのかを証明するためにサーバーから送る証明書の確認をクライアントが行います。クライアントは自分を証明するクライアント証明書を送ります。確認が出来て初めて通信が開始されます。ネットショップなどのこの方法を使っています。これは証明書を PC に保存し使用する方法です。ネットショッピングに活用されています。ネットショッピングを行っている方々は証明書の何通かはご自分の PC に入っているはずで

USB トークン、スマートカードによる検証

ネットワークアクセス、アプリケーションを使用する場合に、証明書を USB トークンやスマートカードに入れておきそれをアクセス時の証明書を使用する方法です。これにより、高い本人証明が可能になります。カードや USB トークンの持ち主が本人ということになります。これは入室管理にも利用することが可能です。スマートカードにはカードリーダーが必要となります。

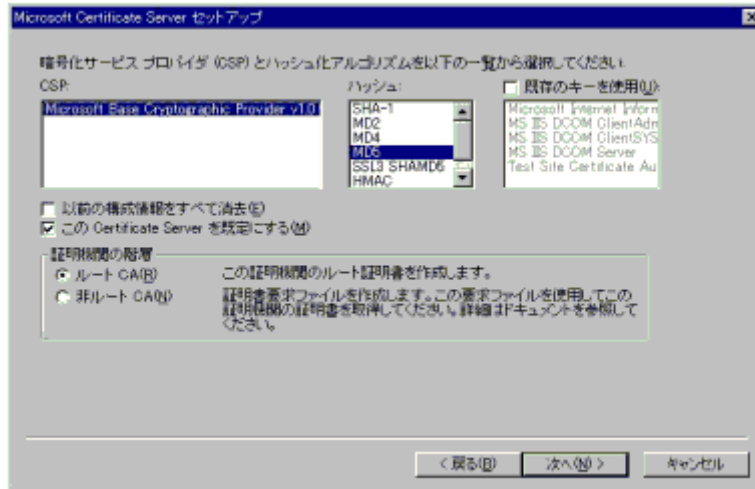
サーバー上にあるアプリケーション、ファイル、データにアクセスの認証、暗号ファイルの復号化等にも利用され、セキュリティ管理上、とても便利なものです。

Certificate Server の設定

IIS と Certificate Sever の追加コンポーネントをインストールします。CA の種類を決定します。(エンタープライズ証明機関、スタンドアロン証明機関 - 詳細はマニュアルをご覧ください。ドメインレベルの証明書か、個人レベルの証明書を発行するかにより決定します。)

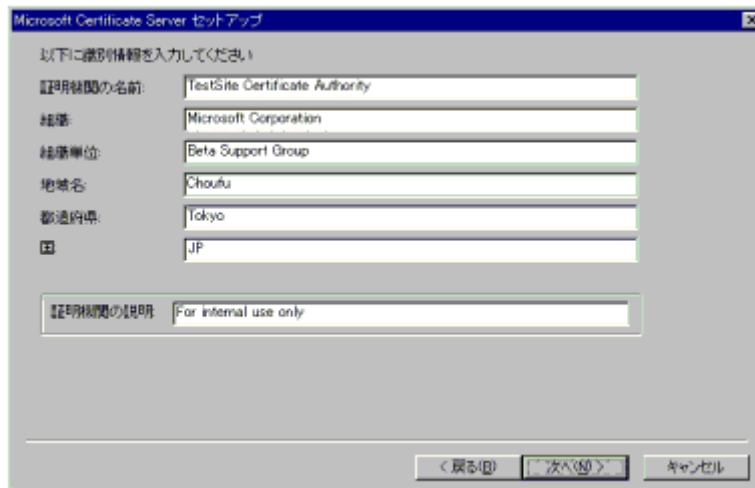
エンタープライズ証明書の場合は発行元として自動的にそのドメインに属するクライアント PC に登録されますので証明書の発行元の信頼性は自動的に確認されます。この証明機関の有効期間設定は重要項目です。エンタープライズ証明機関(エンタープライズのルート CA)に使用する証明書のデータベース(Repository)、やログのファイル名を指定します。デフォルトでは CertLog となります。





CSP とハッシュ化設定

CSP の設定で使用する CSP を選択します。CSP とは鍵ペアの作成するソフトウェアのことです。マイクロソフト CSP か外部 CSP (= HSM) を選択します。選択することで CSP に鍵生成のリクエストなどが行われるようになります。デフォルトではマイクロソフト CSP が選択されます。



証明書構成

大規模ドメインに対する証明機関の設定には慎重で緻密な設計、設定が重要です。この仕組みは一度動き出すと証明書の再発行手続きなど必要になります。

また、証明書の失効情報は重要で CRL (Certificate Revocation List) を CA に定期的に出させるように設定し、退社や協力会社の従業員などの変更に対応しなければなりません。

マイクロソフトサーバーPKI の弱点

PKI では秘密鍵/公開鍵のペアを生成しそれを基本として全てが始まります。また、秘密鍵は個人が所有するのと、保管を行い不測の事態に備えています。その保管は PKI において基本です。PKI の根幹である証明書、暗号化の基本情報としての鍵が流出してしまうということになります。

KK ICH 3-5-17-408 Nishigotanda, Shinagawa, Tokyo 141-0031 Japan

Phone +81-3-3432-3336

<https://www.ich-one.com>

外部 CSP=HSM のススメ

マイクロソフト社によると“キー管理。秘密キーは証明プロセスの信頼性の根幹を成すものなので、CA のキーは最も重要なリソースです。暗号化ハードウェア モジュールを使って、改ざんから保護されたキーの保管場所を用意し、サーバーで実行されている他のソフトウェアから暗号化の操作を分離することができます。これにより、CA キーに危害が加えられる危険性が小さくなります。証明書サービスでは他の提供元からの暗号化サービス プロバイダ (CSP) を使用できます。”となっています。より安全な運用は HSM が推奨されています。

マイクロソフト社の Certificate Server はデフォルトで鍵の生成と保管をソフトウェアで行っています。

| | |
|---------------------|--|
| 暗号化サービス プロバイダ (CSP) | Microsoft Base Cryptographic Provider v1.0 Microsoft Enhanced Cryptographic Provider v1.0 |
|---------------------|--|

これら **CSP (Cryptographic Service Provider)** は Microsoft Certificate Server の指令を受け鍵の生成を行い Microsoft Certificate Server に返し、証明書の生成を行います。(CA 機能)これらは全て Windows サーバーに付属しています。

このサーバーでは鍵の保管においてそれほど強度が高いわけではなく、そのために外部の **CSP** として **HSM (Hardware Security Module)** を必要に応じて使えるようにしてあります。HSM はマイクロソフト CSP に代わり高品質な鍵ペアを生成する専用ハードウェア CSP で、生成した鍵の保管を厳重に行えるようになってきています。例えばある HSM は不法に鍵を取り出そうとすると、HSM 自身がロックをかけ内部の情報の持ち出しが不可能になります。(高品質とは簡単に“解読されない”と言う意味になります。)

このような機能を耐タンパー機能といい PKI では FIPS という米国政府が定めた安全基準があります。最強がレベル4、マイクロソフト CSP はレベル1を提供しています。一般的にはレベル2 - 3のものが使用されていますが、政府、企業レベルの最高峰ではレベル4が要求されることがあります。

つまり、高度なセキュリティを確保するにはサーバーに外部の CSP である HSM を使用することにあります。HSM のベンダーは Windows サーバーに対応する自社 HSM 用のドライバーやソフトウェアを其々作成していますので導入にはそれほど問題はありせん。

HSM(Hardware Security Module)の基本機能

IETF の RFC5280 で定めのある X.509 証明書システムに供する機能を有していますが HSM の認定制度があり各ベンダーは米国政府とカナダ政府の認定制度にあわせて HSM を設計製造しています。機能におけるセキュリティレベルがあり米国 NIST 規格 FIPS-140-2 の中でレベル1から最高峰の4まであります。マイクロソフト Certificate Service における CSP はレベル1です。

鍵ペアの生成
保管
暗号化
証明書への署名

CSP (Cryptographic Service Provider) とは以上の機能を提供するソフトウェアまたはハードウェアのことで、ハードウェアでこれらを行うものを HSM と呼びます。

レベル4を取得しているのは世界で唯一、米国/英国の AEP Networks, Inc.の Keyperのみです。日本政府は現在レベル3を基本要件としていますが、いずれレベル4への要求が高まるといわれています。レベル3は耐タンパー性能で Tamper Resistant がレベル3、Tamper Reactive がレベル4となります。Tamperとは“改ざん“となりますが、この場合は暗号化領域に入り込み解読情報を盗んだり、見たりする行為と理解したほうが判り易いと思われます。

米国規格 FIPS-140-2 規格の基準概要

- レベル 1: 一番低いレベルであり、甚だしくセキュリティの欠如がないこと。
- レベル 2: レベル 1 に加え鍵へのアクセスを管理者権限が必要。
- レベル 3: レベル 2 に加え; 物理的な改竄への耐性、攻撃者のアクセスを困難にすること、管理者の ID ベースでの認証を行うこと、内部データの取扱機能の分離独立。
- レベル 4: 今までの全てに加え物理的攻撃、こじ開け、熱による密閉筐体への攻撃等に反応し内部データの流出を防ぐためにデータの破壊、または消去を行うこと。

* レベル4は世界で唯一米国/英国の AEP Networks, Inc.の Keyper が取得しています。

PKI を使用する環境

先にお話しましたがこの技術はインターネットショッピングや株取引等では使用されています。同じ仕組みを日常行われる WORD や Excel などの文書、データの交換に使用できます。また、ネットワークにアクセスしてどのような作業行なえるのかという権限をユーザーに毎に設定可能になります。そのためには以下の項目が必要です。

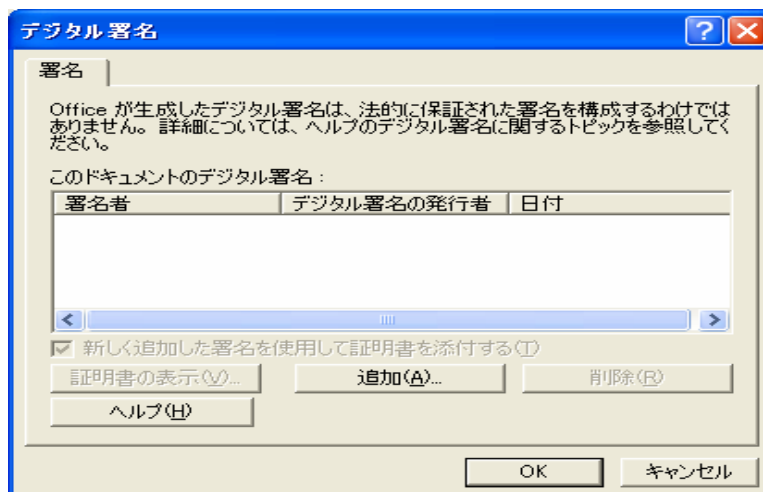
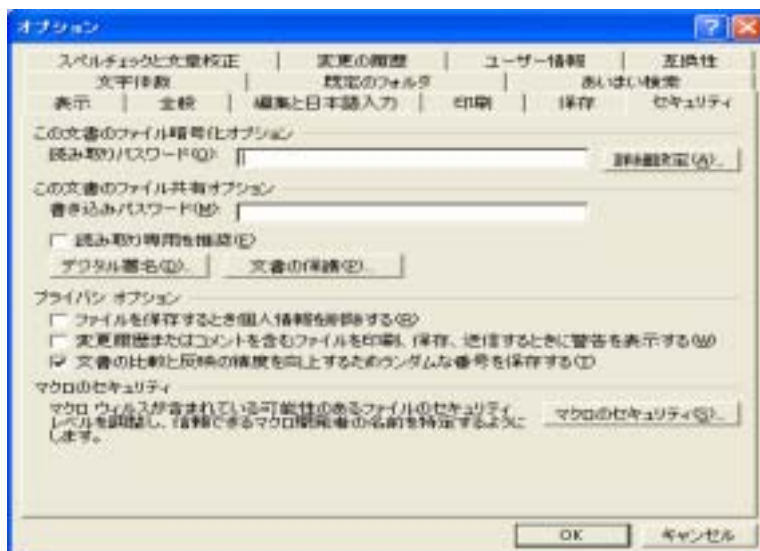
- 1) HSM
- 2) 証明書収納用 USB トークンまたはスマートカード
- 3) カードリーダー (USB の場合は不要)

以上で PKI 環境が構築できます。使用するアプリケーションの設定は必要です。

マイクロソフト Office の WORD の場合

例えばマイクロソフト WORD の場合以下のような設定が必要です。

ツール > > オプション > > セキュリティタブ > > デジタル署名



ここに証明書のインストールを行います。セキュリティまたはネットワーク管理者に証明書の発行をしてもらいインストールします。また必要に応じてマクロの作成も可能です。マクロにより作業の自動化を行い洩れの無い手続きが可能です。

PKI を導入することの有益性

インターネットには誰でもアクセス出来る利点がありますが、公道を歩くと同じようによからぬ意図を持って利用している方々もおります。つまり、インターネットは繁華街を歩くようなもの。社内のネットワークは機密情報のかたまりです。

“必要な人だけに必要な情報”を提供するのは業務を円滑に進めるための必須事項です。時々新聞や、インターネットのニュースサイトで大きく報道されるのは、外部侵入よりもむしろ最近はかなり多くが内部からの個人情報流出です。これらを防止するには PKI のチカラを使う必要があります。

データの暗号化

インターネットを使用する場合特に設定しない限り、ID、パスワード、データなどは誰でも読める平文で色々な経路を経由して相手に届きます。クレジットカード・データも同様です。その経路上でデータをすくい取り、悪用する輩もいます。防ぐためにはデータの暗号化が必要です。本人に“ナリスマシ”勝手に買い物をされたり、データの変更の可能性を防ぐためであります。

データへの署名

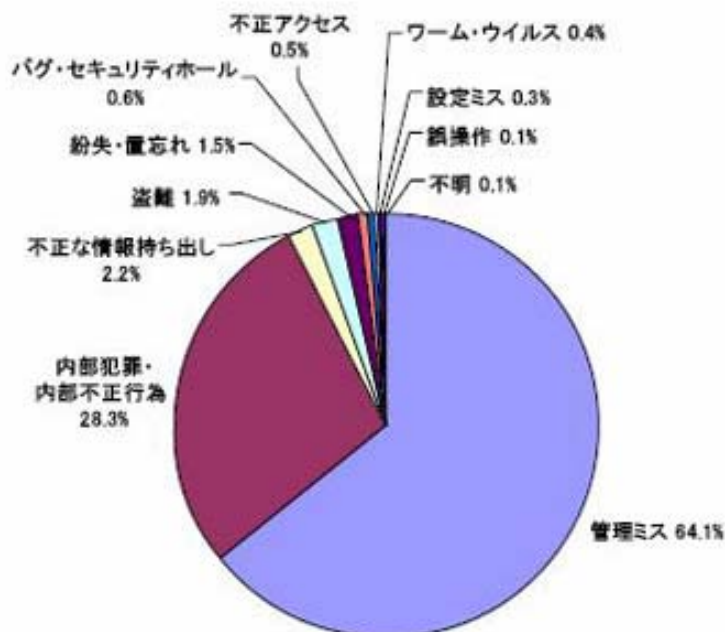
インターネット経由の商取引も非常に大きくなってきています。不正ユーザーと正規ユーザーの注文について見分けるには電子注文書に電子署名を付け検証させることが必要です。

改ざん人の特定否認防止

上記のような PKI 機能を使用しますと誰がどのような変更を行ったのか直ちに判明することになります。これにより文書に関する信頼性を更に高めることが出来ます。例えば電子による入札や商取引、税金申告などで有効です。

データ暗号化による内部情報の流出防止

日本ネットワークセキュリティ協会の 2007 年についての「情報セキュリティインシデントに関する調査報告書」によれば実に 1,200 万人のデータはデジタル記録媒体を経由して流失し、流失した個人情報の 39%を占めている。紙媒体による流出も 40%となっている。USB メモリーが廉価大容量になっているため更にこの数字は増加すると見られている。PKI により暗号化、アクセス管理を行うことで内部情報の持ち出しを管理できます。これらの原因は 64%が管理ミスによるものであるようです。流出の 28%が内部の犯罪から流出したものです。USB メモリーの使用を全面禁止している会社もあります。



日本ネットワークセキュリティ協会 2007 年

このようなデータ管理をコンピュータが管理するポリシー（簡単に申し上げますと、ネットワークで誰がどのような権限で何を行うかを決めておくこと）が自動的に管理します。PKI はそのようなシステムに寄与します。データの流出はアクセスポリシーと暗号化で防げます。PKI はその両方に使用できる機能を提供しています。PKI はまた、情報の変更について敏感であり、データ内容の変更について管理できる仕組みを提供しています。

差迫った PKI の利用範囲

日本では本年 4 月より一般に金融商品取引法または J-SOX 法が施行され、文書やデータの取扱内部統制について規定し遵守しなければならなくなりました。また、2005 年 4 月 1 日より電子文書法が施行され、法で定められた保管文書の一部を除くものの電子保存が出来るようになりました。条件は文書の完全性の確保です。ここでも PKI が必要です。暗号化と変更防止です。

PKI は非常に取組みにくい仕組みですが流れが判ると以外に簡単に採用が可能です。Windows サーバーを運用している方々にとってはもう直ぐそこに PKI があります。企業のコンプライアンスを維持する方法の一つとして是非ご検討をお勧めします。

以上

株式会社アイシーエイチ