PKI 技術紹介と Xnet（社内電子認証局）における BS7799-2: 1999 ISMS 構築

宇田川 誠（富士ゼロックス（株）DPSC ／サービス開発部）
makoto.udagawa@fujixerox.co.jp
森　久三（富士ゼロックス（株）コンサルティングセンター 情報セキュリティグループ）
mori.hisazo@fujixerox.co.jp
神林　彰（富士ゼロックス（株）コーポレートインフォメーションマネージメント部 情報戦略グループ）
akira.kanbayashi@fujixerox.co.jp

電子情報は複製や改ざんが容易なため，インターネットの利用目的が拡大するに従い，いたずらや不正が無視できなくなってきた．EC（Electronic Commerce）の普及により，この課題への最有力な対応策として PKI（公開鍵認証基盤）が技術的にも法的にも整備されつつあり，本格利用段階が近づいてきている．本稿では，PKI 技術の紹介，社内電子認証局（Xnet）の構築事例と商品への展開について解説し，その後当社の Xnet において BS7799-2（ISMS）を構築した事例について述べる．

セキュリティ問題と PKI 技術

さまざまなセキュリティ問題をユーザからの見方で分類すると，セキュリティ問題，すなわち脅威には，「改ざん」，「盗聴」，「なりすまし」の 3 種類がある．改ざんは電子情報を不正に変更すること，盗聴は利用権利のない電子情報を不正に入手すること，なりすましは他人に成り代わってシステムを利用することである．インターネットの普及に伴い，情報システムは Web ベースに移行しつつある．Web ブラウザや Web サーバは，すでに PKI 技術に対応したものになっている．公開鍵証明書を発行する CA（Certificate Authority）を設置・運用することで，情報システムの安全性を高めることができる．また，PKI は本人確認を行う標準システムなので，本人確認のレベルがパスワードなどよりも高く，電子署名法などの法的認知を持っている．ユーザの利便性の面でも，個々の情報システムが PKI 対応していくことにより，PKI によるシングルサインオンが実現されるようになる可能性がある．

PKI 技術

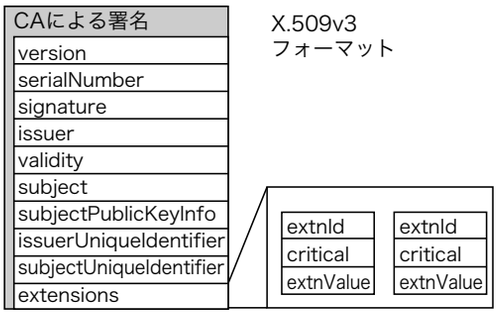
概要

PKI とは，Public Key Infrastructure の略で，公開鍵暗号技術（PK）を用いてセキュリティを提供する基盤（I）を指す．公開鍵暗号は，各自の鍵が公開鍵と秘密鍵のペアになっていて，秘密鍵は持ち主の責任で秘密に保持し，公開鍵は誰にでも公開可能な特徴を有する暗号体系である．一方の鍵での変換を，他方の鍵でのみ逆変換することができる．これにより，ある人が特定の秘密鍵を持っていることを他の誰でもが公開鍵で検証できる．そして，秘密鍵を認証根拠や署名の根拠とすることができる．公開鍵暗号を利用する際には，個人と公開鍵の対応が保証されねばならない．そのために，この対応を保証する公開鍵認証機関（CA）という第三者を設置する．ネットワーク上の各自が同一の CA を信頼する前提により，直接知らない他者であっても互いの公開鍵を信頼することができる．結果として，ネットワーク上の任意の 2 者が暗号・電子署名を行う基盤が提供される．PKI は，このように CA を用いて個人と公開鍵の対応を保証する枠組みである．**図 -1** に公開鍵証明書の記載内容を，**図 -2** に PKI の構成要素の例を示す．人やサーバなどが情報の発信者・受信者となる．CA は，人やサーバ各々に公開鍵，秘密鍵の鍵ペアを生成し，その名前や公開鍵を含む図 -1 に示される情報に署名することで公開鍵証明書とする．公開鍵証明書は公開情報として流通でき，秘密鍵は各自が秘密に管理する．

PKI でできること

PKI の基本機能は，暗号化，電子署名，ユーザ認証の 3 つである．PKI を利用した応用例を以下に示す．

① SSL：（Secure Socket Layer）により，1 対 1 の通信を暗号化することができる．SSL はトランスポート層の直上に挿入され，いろいろなプロトコルを容易に SSL 化できる．機能は 3 つあり，通信路の暗号化，クライアントから見てサーバが本物かを証明する機能，クライアントが本人であるかをサーバに対して証明する機能である．



・認証機関（CA）は，利用者と公開鍵の対を認証機関によるディジタル署名した「公開鍵証明書」を発行する．

version： X.509のバージョン
serialNumber： 認証機関がユニークに割り当てるシリアル番号
signature： 公開鍵証明書の署名方式
issuer： 公開鍵証明書の発行者である認証機関のX.500識別名
validity： 公開鍵の有効期限（開始日時と終了日時）
subject： 本証明書内に含まれる公開鍵に対応する秘密鍵の所有者のX.500識別名
subjectPublicKeyInfo： この証明書が証明する公開鍵
issuerUniqueIdentifierおよびsubjectUniqueIndentifier
： それぞれ認証機関の固有識別子，所有者の固有識別子
extensions： 拡張型（extnId），拡張値（exthValue）およびクリティカルビット（critical）の3つ組の集合
X.509で定められた拡張型には「公開鍵の利用目的」，「所有者の別名」，「認証機関かどうか」などがある．

図-1　公開鍵証明書のフォーマット

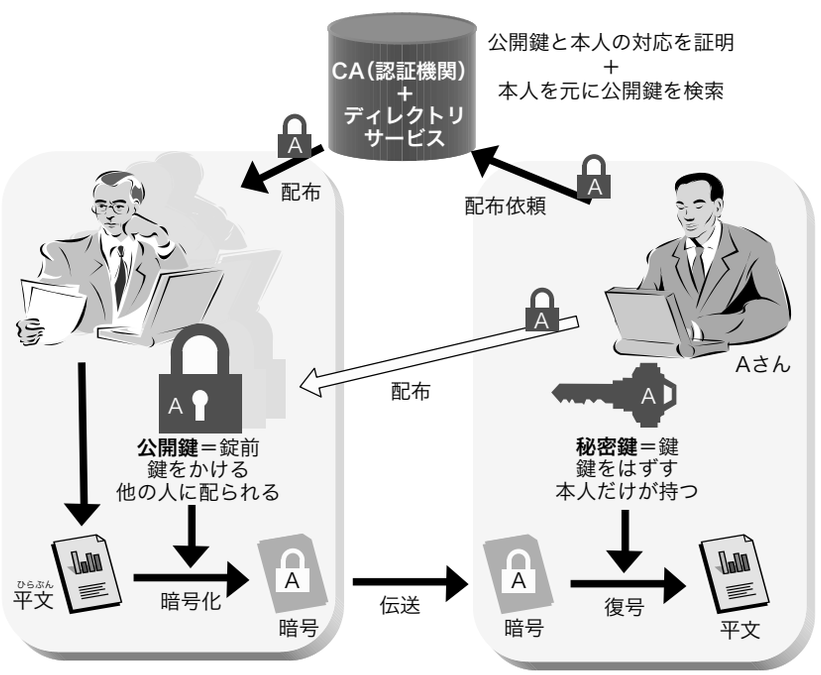


図-2　PKIの構成要素

② S/MIME：（Secure/Multipurpose Internet Mail Extensions）を使うことにより，電子メールの本文の暗号化と，送信者による電子署名を行うことができる．

③ VPN：（Virtual Private Network）は，インターネットを仮想的な専用線のように用い，暗号化をすることにより安全性を確保しているが，暗号の鍵交換を行う際にPKIを用いることができる．

④コードサイン：署名の検証により，プログラムが改変されていないかどうかを確認できる．また，プログラムが正規のベンダが提供しているものなのか，を確認することができる．

⑤権限の管理：PKIは本人確認のメカニズムであるので，人とシステムアクセス権限の対応を別途管理するシステムと連動すれば，権限を確実に管理することができる．

⑥文書の承認など：電子文書にはさまざまなフォーマットがあるが，文書にPKIによる電子署名をつけることにより，承認などの本人操作を保証する文書が作れる．

⑦否認防止：電子署名は本人以外できないので，電子情報上で署名確認を行えた場合，本人が承認したものと見なすというシステム対応が可能になる．

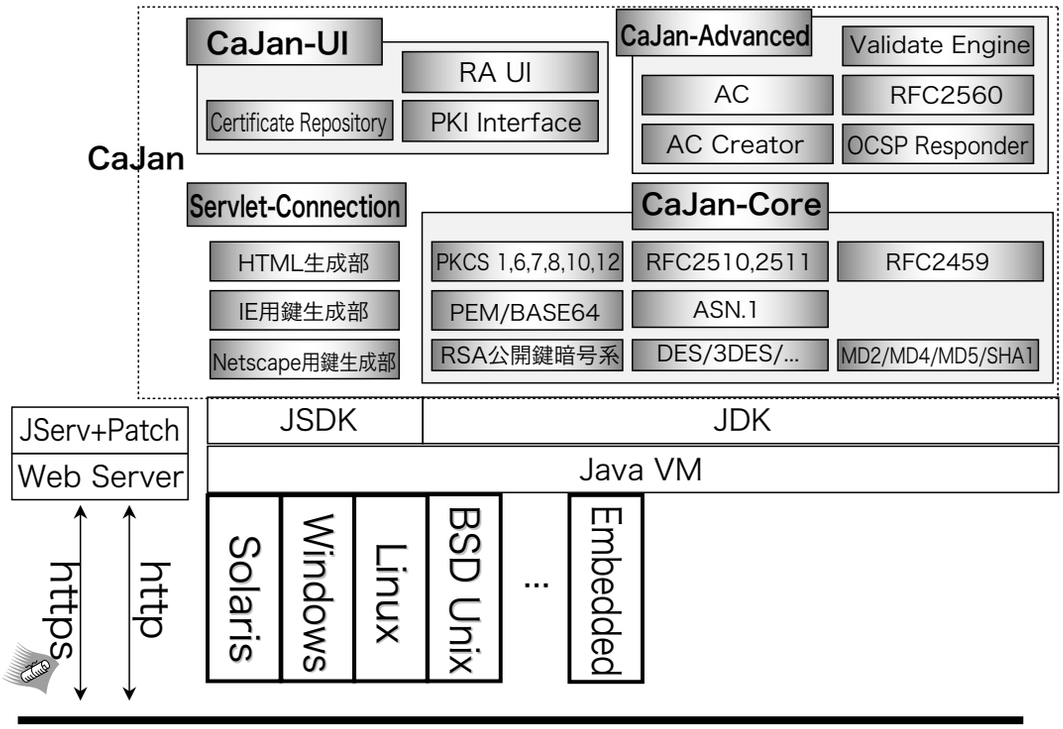


図 -3　CaJan 構成

PKI 技術の動向

1 つの CA サーバから発行される証明書群によって構成される認証範囲をドメインと呼ぶ．実用上多数の PKI ドメインが混在し，マルチドメイン環境を構成している．また，CA 製品や証明書と連動するアプリケーションは増加中で，マルチベンダ環境になっている．マルチドメイン，マルチベンダ環境による「相性」が問題になりやすい状況になってきた．そのため，各国ではマルチベンダ，マルチドメイン環境での相互接続実験を行い，標準文書の解釈のズレを補正しようとしている．マルチドメインの中でも，ルートが複数あるブリッジモデルと呼ばれる複雑なモデルが実用化されようとしている．GPKI（政府認証基盤），LGPKI（地方公共団体における組織認証基盤）など，電子政府・電子自治体の認証基盤はブリッジモデルを採用している．

当社での PKI アプローチ

数年前からの技術開発活動の 1 つとして PKI 技術に着目したことを機に，コア部分の試作，社内業務への適用，商品化といくつかのステップを経て成長してきた．

プロトモデル CaJan

図 -3 に当社での，CA 部分のプロトタイプ（開発名 CaJan）の構成図を示す．CaJan は主に 5 つのコンポーネントから成り立っている．Core には，公開鍵証明書を生成・確認するために必要な基本的な暗号エンジンのライブラリ群と，RFC（IETF が発行する Request for Comments）に基づくエンコード・デコード関係のライブラリ群，そして証明書生成要求（CSR）から証明書を生成するプログラムが含まれる．Advanced は，まだ標準が明確でない部分の暫定実装を集めた部分で OCSP（Online Certification Status Protocol）のデーモン，属性証明書生成部，証明書有効性確認部分などからなる．Connection は，Web クライアントからの証明書生成要求を受け付ける部分で，ブラウザごとの鍵ペア生成を起動する機能を持つ．UI（ユーザインタフェース）は，CA サービス全体の Web UI である．最後は，Java 環境で Servlet を用いてクライアント認証 SSL による Web サービスを実現する動作環境である．Java で記しているため，組み込み環境からさまざまな OS まで，動作環境への依存度が低いこと，必要な暗号エンジンの実装を CaJan 自身が持っていることが特徴である．

社内電子認証局（XnetCA）の構築事例

インターネット経由で電子情報を取引先と共有することは，企業活動の中で日常的になってきた．そのため，当社のお客様や取引先との情報交換にかかわる工数や時間の削減，インターネットを用いて安全に情報交換する共通のインフラとして，社内標準サービス（Xnet）を提供することにした．Xnet は，インターネットを介して安全にドキュメントを交換するためのサービスである Xnet DDS（ドキュメント配付サービス）と，そのアクセス管理を行う証明書を発行する XnetCA とからなる．本人確認，情報漏洩への安全性を向上させる目的に PKI

を利用し，業務システムへの柔軟性を確保するために社内技術を用いた．当社から部品の調達先に設計図面を送ったり，物品の発注を取引先に行う際には，データをインターネットを介して受け渡している．そのサービスをアクセスするための本人確認と通信経路の暗号化を，Xnet の電子証明書により行っている．現在は，開発部門と親密取引先との間の設計図面の共有，生産段階での定期的な部品発注や納品，および現品管理業務，ソフト・ライセンス購入などで，この仕組みを使っており，徐々に対象業務を拡大している．

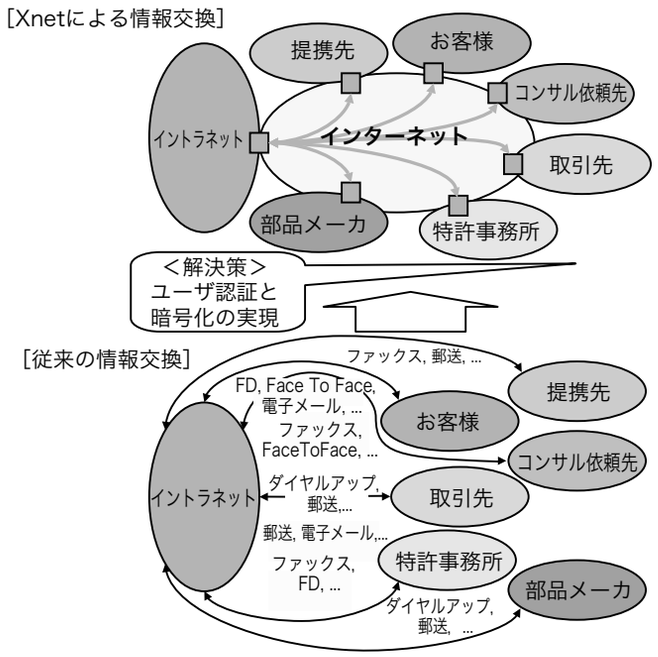


図 -4　Xnet の利用目的

■ Xnet と XnetCA 概要

図 -4 に Xnet の利用目的を示す．XnetCA は，Xnet ユーザに公開鍵証明書を発行するプライベート CA システムである．Xnet 証明書は当社社員だけでなく，アルバイトなどの社員以外の従業員，当社取引先の勤務者が含まれる．また，各グループ企業に証明書発行権限を委譲し，当社と同様に，各グループ企業の社員，従業員，取引先勤務者に証明書を発行する．証明書発行対象には，実在する人，Web サイトのほかに業務プログラム，人の集合である役割なども含まれる．**図 -5** に XnetCA の概念図を示す．

■ XnetCA の特徴

全社員に社員証を配ることと異なり，業務上必要な人に証明書を発行するため，多彩な利用者に個別の目的で証明書を発行できるよう，認証モデルを発行対象ごとに設計した．工場の部品発注伝票などの基幹業務システムに用いることを想定し，担当者の不在・交替などにも対応する必要がある．夜間に大量の伝票情報をアップロード・ダウンロードできるよう，業務プログラムが証明書を持つことも想定した．

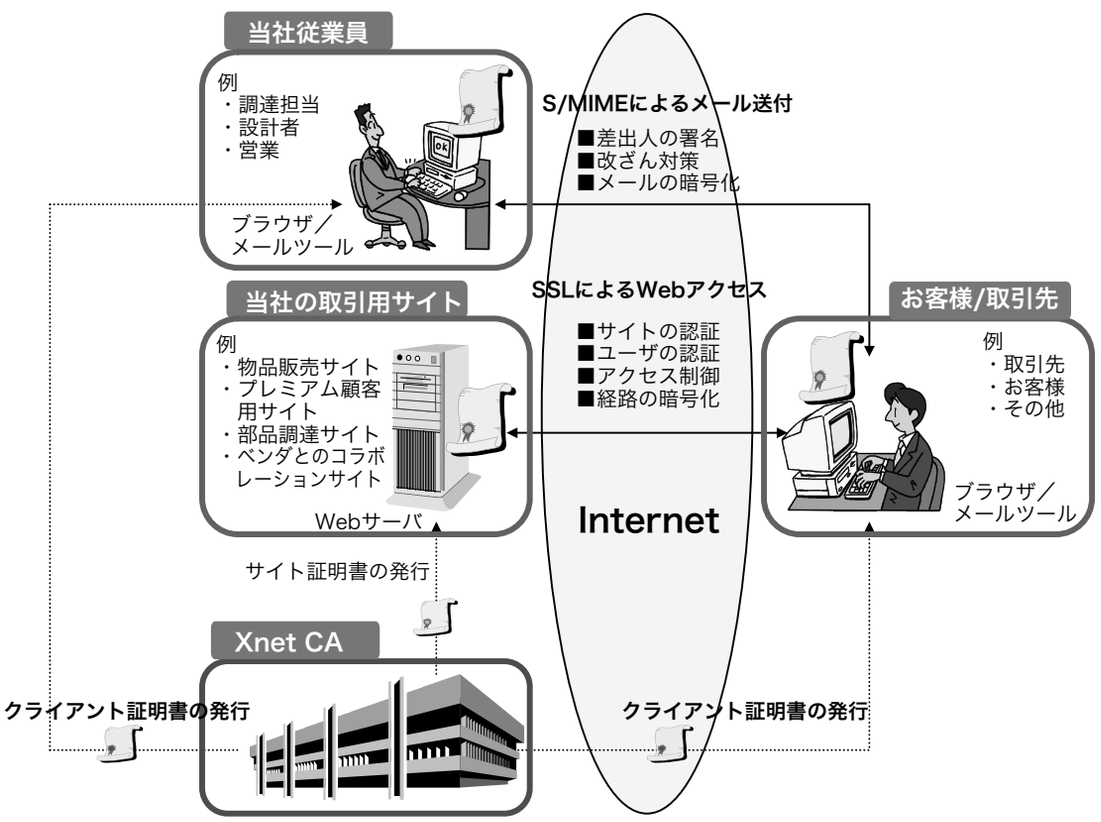


図 -5　XnetCA 概念図

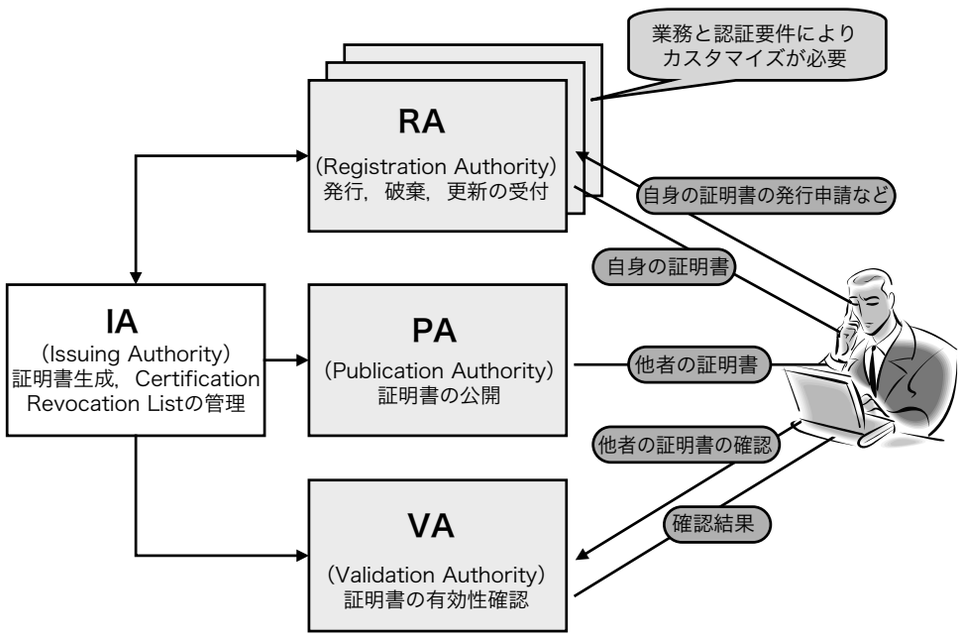


図 -6　CA の構成要素

■ XnetCA の実装技術

CA の構成要素を**図 -6** に示す．XnetCA は，CaJan を IA のベースに用い，RA 部分は認証フローに合わせて新規開発した．証明書の種類が複数あるため，RA が複数ある構成とした．ユーザ規模が拡大する場合に備え，EJB☆1 や EJB 用ミドルウェアを使用し，Web サーバとアプリケーションサーバを分割した 3 層構成をとった．実業務で使うため，PC のクラッシュなどによる秘密鍵の紛失によって生じる業務停止などのリスクを回避するために，当社グループ企業の社員および社員外従業員の秘密鍵は XnetCA 側でバックアップする．

CA 自社構築のメリット

市販の PKI 製品やサービスはすでにあるが，それぞれ固有のセキュリティポリシーを持ち，さらにそのセキュリティポリシーを維持する専用クライアントが必要であるなど，自由度に制約がある．B to B 用途では，利用企業の状況に応じたセキュリティポリシーを具体化する，より柔軟な PKI 製品が必要と考えた．特に，すでに管理体系のできてしまっている運用中の業務システムに，後から PKI を適用するには，既存の Data Base と関連を持たせる情報を証明書に入れるなどの柔軟性が必要である．また，業務にかかわるのは特定多数であるが，構成員に最初からさまざまな人々が含まれることも分かった．認証者を社員以外が行う場合が多いなど，現場の都合を再認識できた．

社内サービスノウハウの商品化

Xnet で得られたさまざまなノウハウを商品化することとした．商品化のため，多数の契約を管理する機能，利用料金を計算する課金機能を追加し，多数のルートを 1 システムでサポートする構造とした．商用システムの稼働後は，Xnet は商品の 1 契約へと移行した．第 1 弾として，「証明書発行」と「ドキュメント配付サービス」を，第 2 弾として「EDMICS データ共有サービス」，第 3 弾としてドキュメントハンドリングソフトウェア「DocuWorks 5.0」での電子署名・セキュリティ機能，をそれぞれ商品化した．また，電子政府向けにも，「セキュア･メーングリスト･サーバ」[5] の技術開発を行った．

情報セキュリティマネジメントシステム構築の概要

情報セキュリティマネジメントシステム構築の背景

Xnet は，BS7799-2 に準拠した ISMS（インフォメーションセキュリティマネジメントシステム）を構築し，外部機関より BS7799 の審査を受け，認証を取得することができた．当社が BS7799-2 に準拠した ISMS 構築を行ったのは次のような背景がある．

①社内の情報セキュリティ問題への関心の高まり

コンピュータウィルスの社外流出問題，インターネット上の有害サイトのアクセス，退職従業員アカウントの抹消問題など，主に社内に原因があるセキュリティ問題への取り組みが重要となってきた．これらへの対応には，技術面からのセキュリティ対応だけでなく，インターネットや電子メールの利用方法といった情報倫理的なアプ

☆1　EJB (Enterprise JavaBeans) は米国 Sun Microsystems, Inc. の商標です．

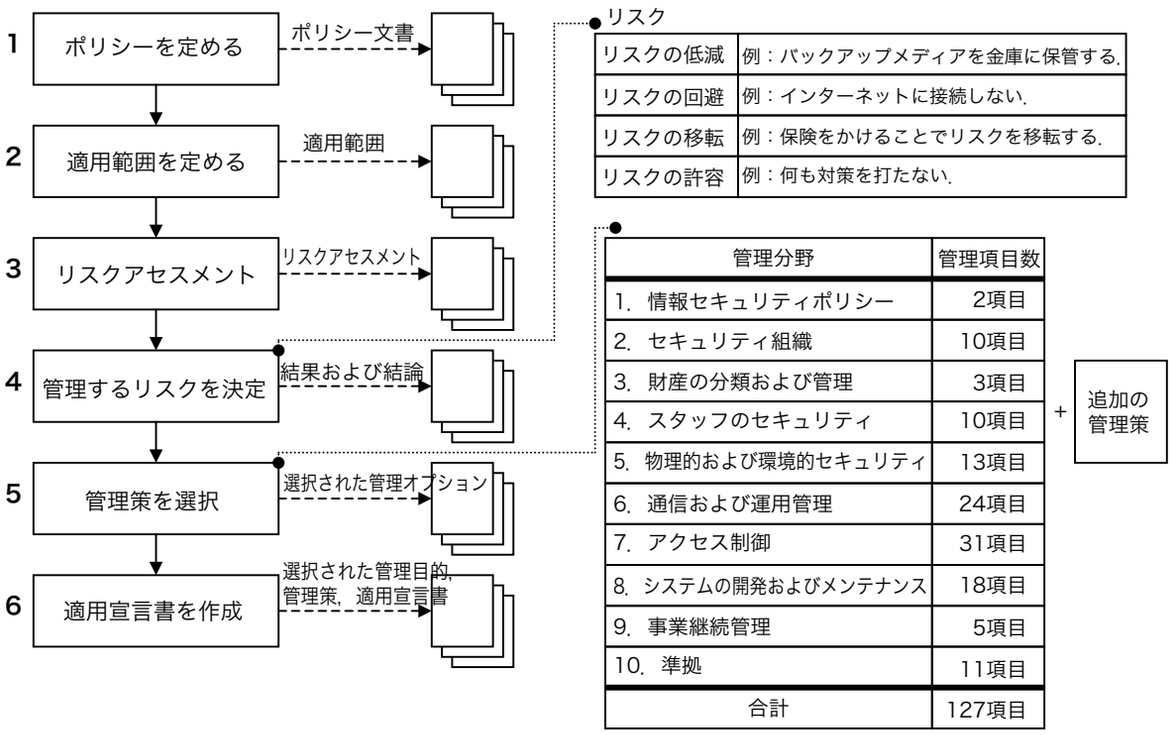


図 -7　ISMS 構築のステップ

ローチも必要となってきている．

②資本に関係しない企業間連携の高まり

従来，社員という家族にしか情報アクセスの鍵を渡していなかったが，資本関係のない取引先などパートナーにも鍵を預け，かつセキュリティを守らなければならない状況になってきた．

③予防しきれない事態への備え

情報セキュリティ問題に対して，予防ができるようにしておくことが望ましい．しかし，自然災害やサイバーテロなど，予防しきれない事態の発生に対する備えの必要性が高まってきている．

ISMS 構築の対象範囲

ISMS 構築の対象範囲は，PKI 技術を用いた当社の社内認証局「Xnet」を対象とした．ISMS 構築に当たっては，全社を対象範囲としたり，情報システム部門の入っている事業所全体を対象とすることも可能だが，今回は Xnet というサービスを対象範囲とした．対象事業所は，設備運用，システム運用，業務運用，開発部門が入居する 3 拠点である．ISMS の構築に当たっては，社内の ISO コンサルティング部門などの支援部隊が参加している．この中で 4 名のコアメンバは業務の半分以上の工数をシステム構築のために費やした．

ISMS の構築，認証取得の目的

Xnet での ISMS の構築，認証取得の目的は主に 3 つあった．第 1 は，何か問題が起きてから場当たり的にセキュリティ対応をするのでなく，抜け漏れのないセキュリティマネジメントの仕組みや，継続的な改善の仕組みを組織に埋め込むことであった．第 2 は，緊急事態が発生した場合を想定し，事業継続計画の強化を図ることであった．2 年前に BS7799-2 で提供される管理策リストと現状とのギャップを分析した際，事業継続計画に関する評価点が最も悪かった．今回事業継続計画のノウハウを習得し，レベルアップを目指した．第 3 は，認証取得の対象範囲が取引先との安全なコミュニケーションのインフラであり，取引先に対する安全性のアピールを目的とした．

情報セキュリティマネジメントシステム（ISMS）構築の実際

ISMS 構築対象

商品化システムの 1 契約となった段階の Xnet が対象である．

ISMS 構築のステップ

図 -7 に示す 6 つのステップが，BS7799-2 ISMS 構築に当たって必要となる．適用範囲の決定と情報セキュリティポリシーの策定を行い，リスクアセスメントの結果から管理すべきリスクを決定し，そのリスクを低減するために 127 項目の管理策から導入策を選択した．導入管理策を適用宣言書にまとめるまでが構築の一連のステップである．適用範囲の検討においては，どこまでの組織，どこの拠点を入れるかなどの，境界を引く議論が必要となる．今回，開発組織に関しては，BS7799-2 取得

・情報システム部門，開発部門，運用部門，ISOコンサルティング部門から構成される部門横断プロジェクト体制

・Xnetセキュリティ委員会（毎週）の中で，ISMS構築検討会を開催

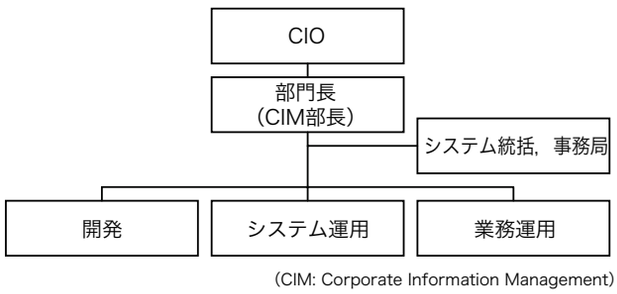


図 -8　ISMS 構築の体制

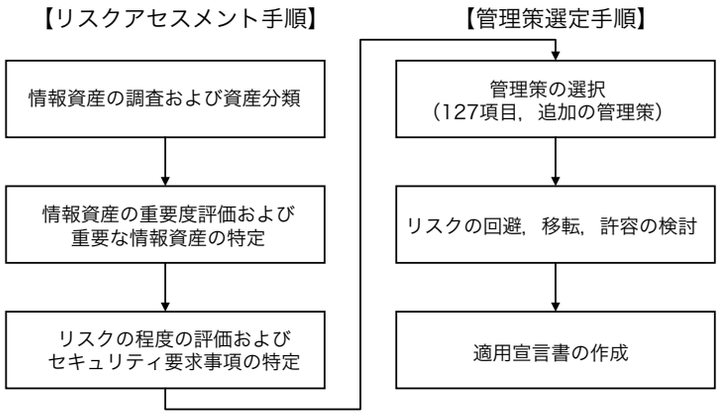


図 -9　リスクアセスメント，管理策選定

とその維持に関する業務開発工数がオーバーヘッドになると懸念されたが，網羅的にセキュリティマネジメントを行うべきとの観点から，適用対象とした．情報セキュリティポリシーは，人によってイメージするものが異なった．トップの声明文をイメージする人，より詳細な規則が入ったものまで含めてイメージする人，またファイヤウォールの設定仕様をイメージする人もいた．今回のポリシーは，BS7799-2 の規格要求に準拠させて作成したトップの声明を含めた，A4 サイズ 1 枚程度のものである．ISMS 構築の期間は規模や範囲，人数によってかなりバラツキが出ると思われる．当社では，2 年以上前から BS7799 の学習をしてきたが，最終的に認証取得を決定したのは 2001 年の夏で，情報担当役員の承認を得て決定し，直ちに認証取得に向けたプロジェクトを発足させた．BS7799-2 では経営層の関与が要求されている．ISMS 構築を行うには当然，たくさんの工数を必要とするが，経営層の決断をもらうのに多大な労力を使うケースも少なくはないであろう．

ISMS 構築の体制

今回の構築体制は，情報システム部門，開発部門，運用部門に加えて，ISO14001 のマネジメントコンサルティングを行っているメンバで編成された（**図 -8**）．ISMS 構築に当たっては，情報セキュリティの技術的知識があるだけでは，認証取得まで行き着くことは難しいと思われる．情報セキュリティの技術的知識と，ISO のマネジメントシステム構築知識との両方が必要とされる．今回は，ISO14001 のスキルを持ったメンバがプロジェクトに参加したため，ISMS 構築の推進が円滑に行えた．また，ISMS 構築体制と運用体制が同じメンバから構成されていなかったが，実際に情報セキュリティを維持・改善するのは，運用メンバであるため，できるだけ構築の時点から実際の運用部隊が深く入り込む方が，マニュアルや手順書を早い時点で深く理解することができると思われる．

リスクアセスメントから管理策の選定まで（図 -9）

これまでにも簡易的なリスクアセスメントの経験はあったが，BS7799 であらかじめ提供されている 127 の管理策に落とす作業は初めてで，ここに多くの工数を費やした．工数の 30% 程度は，リスクアセスメントから管理策選定の作業に費やした．リスクアセスメントは決まったやり方しか許されていないわけではないが，今回実施した方法の概要を説明する．リスクアセスメントで最初に行うことは，情報資産の棚卸しである．各担当分野ごとに，調査シートを作成し，情報資産の一覧表を作成する．このとき，事前に情報資産の定義を行っておく必要がある．コンピュータに入っているデータだけをリストする人がいるし，紙のドキュメントを含める人もいるかもしれない．またマウスやキーボードなどハードウェアの部品までをリストする人が現れるかもしれない．Xnet では，250 以上に及ぶ情報資産をリストアップした．次に情報資産リストを持ち寄り，各情報資産の重要度評価を行った．評価に当たっては，その情報資産の機密性，完全性，可用性が脅かされたときのビジネス上の影響の大きさで，評価を行った．次に情報資産に対して，どのような脅威および脆弱性があるのか，その程度を定量的に評価を行い数値化した．最終的には，情報資産ごとに重要度の値と脅威，脆弱性の値とを掛け合わせて，その情報資産のリスク値とし，それをある閾値を超えたものに関して，管理すべきリスクとした．この作業は，一度では終わらず，アセスメントロジックや評価基準を更するなどを行いながら，何度か手順を繰り返し，担当者が不安を感じるようなリスクがしっかり抽出されていることを確認するまで，何度か作業を行った．

ドキュメンテーション，文書管理（図 -10）

BS7799-2 では，ISMS の管理および運用について定めた手順を文書化することが要求されている．我々は，情報セキュリティポリシー，リスクアセスメント，遵守すべき法規制，管理策などの手順を文書化した．また，選択したセキュリティ管理策の実施手順は，ISMS 構築以前からあった手順書をベースに BS7799-2 規格に準拠するよう手直しを実施したり，新たに必要な手順を追加した．選択した管理策が手順書に含まれていることを把握するために，選択した管理策がどの事業所ではどの手順書に記述されているかのマトリクスを作成し，管理を行った．このような，小さなノウハウが実際に ISMS 構築を行う上で，有効である（**図 -11**）．文書管理については，文書を容易に利用できる状態を維持し，バージョンを管理し，実情からかけ離れた文書は速やかに廃止されなければならないことが要求されている．Xnet は，拠点数が 3 つに跨ることから，紙でなく電子による文書管理を行っている．具体的には，電子文書管理システム（DocuShare）を導入し，関係者が常に最新の文書を閲覧できるようにした．手順書の版が更新された場合には，関係者に電子メールでそのことが自動通知されるようになっている．

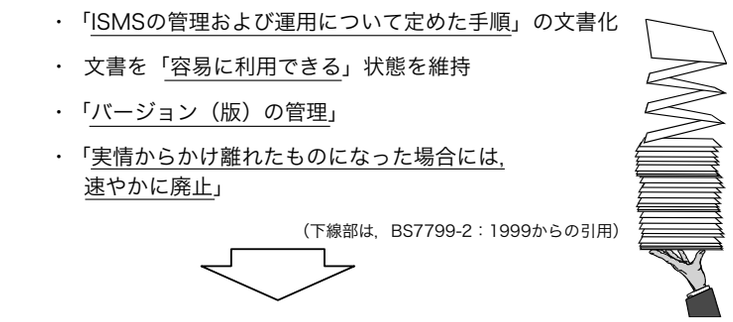


図 -10　文書管理

教育，訓練，内部監査（図 -12）

ISMS の運用に当たっては，関係者に対しての ISMS 集合教育を実施した．また，このときアンケートを実施し，受講者の理解度の確認を行った．情報セキュリティ教育全般ということでは，集合教育では限界があるため，グループ会社も含めた全従業員への情報セキュリティおよび情報倫理教育を WBT（ウェブベースドトレーニング）を用いて展開を行った．訓練は，万が一運用管理者のコンピュータにウィルスが蔓延してしまった場合を想定し，事前に作成した事業継続計画に沿って，復旧手順を実際に行った．火災，大規模地震・障害を想定して事業継続計画をあらかじめ作成しておき，実際に訓練を行うことは，事業継続計画の手順の適切性を確認することもでき有効であった．ISMS の運用内容が規格要求通り実施されていることを，社内の客観的な立場の者から，チェックを受けるため，内部監査を実施した．内部監査は，当社の業務監査部門とプロジェクトメンバの混合体制で実施した．自分たち自身で，情報セキュリティマネジメントの運用状態を確認し，改善に結び付けられると同時に，認証取得やサーベイランス時の事前準備や心構えを事前確認できるという効果があった．

審査

審査の方法は認証機関ごとに多少の違いはあるようであるが，当社の場合は 3 段階の審査が行われた．まず初めの審査は，書類審査であった．この段階ではポリシー，リスクアセスメント，管理策の選定，準拠する法律，適用宣言書などから，ISMS の基本的なフレームワークができているかどうかの確認が中心だった．その 1 カ月後，初動審査を 2 日間受けた．マニュアル，手順書の確認が主だったが，加えて現場の確認もあった．初動審査の目的は，対象組織が本審査の受審レベルに至って

選択した管理策	拠点A（業務運用）	拠点B（システム運用，開発）	拠点C（設備運用）
4.5.1.2 物理的出入り管理策	施設入退室管理手順	オペレータ室セキュリティ手順	居室入退室手順
4.5.1.3 オフィス，ルームおよび施設のセキュリティ	施設入退室管理手順	オペレータ室セキュリティ手順	居室入退室手順
4.8.5.1 変更管理手順		システム更新管理手順	
4.8.5.2 オペレーティングシステムの変更の技術的レビュー		システム更新管理手順	
…… ……	……	……	……

図 -11　＜参考＞管理策と手順書の関連

・関係者に対するISMS集合教育を実施

・重要な障害や災害を想定しての事業継続計画を策定．この事業継続計画に従っての訓練を実施

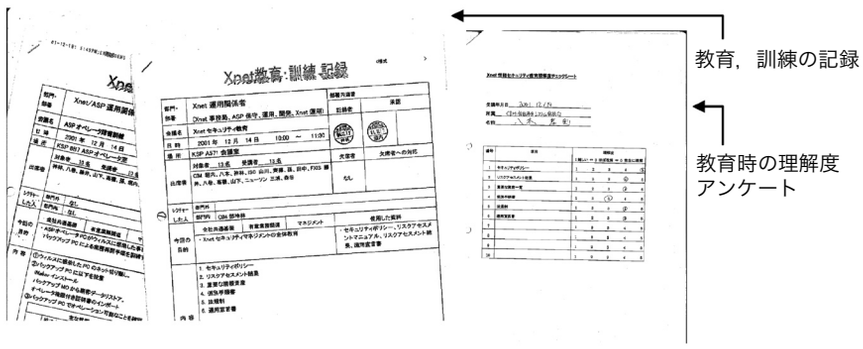


図 -12　教育，訓練

いるかどうかの確認である．本審査はさらに 1 カ月の期間を置き，3 日間行われた．経営者インタビューを行い，構築した ISMS 通りに現場が運用されているかどうかの審査があり，エビデンスの提出が求められた．その後，判定会議が開かれて，無事，合格の連絡を受け取った．

ISMS 導入による効果

この一連のプロセスで良かったと思う点は，当初の目的達成ができたこと．そして，Xnet の重要な守るべき資産とは何か，なぜそれだけのお金をかけるのか，もし破られた場合，問題が起きた場合はどうするか．このような一連の諸問題に対して，セキュリティ担当者が，第三者に対して説明できるようになったことである．今後見直すべき点は，文書体系の改善や ISMS 構築ツールの整備である．より広い分野に ISMS 構築の範囲を広げようとしたとき，既存のセキュリティ関連の規程類と ISMS 文書の整合をどうとるかについて検討を行う必要があると考えている．また，より容易にリスクアセスメントなどができるようにして ISMS 構築そのものの展開を容易にするための道具立てを用意していきたいと考えている．今回は Xnet という限られた分野での ISMS 構築だったが，BS7799 のフレームワークはきわめて有効な方法だと改めて実感した．これを活用して，認証取得は別にしても，他の組織や分野に展開していきたいと考えている．

まとめ

数年間の活動の結果，技術開発から社内利用，商品化，商品への社内システムの移行，BS7799 認証と，幅広い経験を積むことができた．現在，当社グループ企業と取引先向けの認証基盤としてだけでなく，Xnet は全社標準インフラに採用されている．セキュリティ技術といった安全性のためにある種の使いにくさを伴うものは，実際に使われてみないと設計の良し悪しが決められない．社内業務でユーザの声を聞きやすかったことが，技術の導入順序や商品のスペックを決めるのに役立った．今後は，コア技術を確実にするための相互運用実験 [6] などによる PKI 商品間の相性問題への取り組み，文書処理環境を構成する商品への適用拡大を考えていく．また，BS7799 ISMS 構築で蓄積したセキュリティマネジメントのノウハウを手法化して，セキュリティコンサルティングの事業に活かしていきたい．

謝辞　技術開発から社内利用，商品化，BS7799 認証と，社内外の数多くの方々の努力と支援とご協力をいただいた．当社技術者の PKI 技術を育てるためにお世話になった，IPA セキュリティセンター宮川寧夫氏，慶應義塾大学看護医療学部宮川祥子氏，にこの場を借りて感謝いたします．また，BS7799-2 の ISMS 構築および認証取得に当たって，BS7799-2 の国内認証機関である JACO-IS（（株）日本情報セキュリティ認証機構）の岡田社長を始め IS 認証部の皆様に大変お世話になったことを感謝いたします．

参考文献

1）青木隆一，稲田龍著，村井　純（監修）：PKI と電子社会のセキュリティ，共立出版 (2001).
2）稲田　龍，黒崎雅人，宇田川誠：PKI 技術紹介と Xnet －エクストラネット認証基盤－，富士ゼロックス　テクニカルレポート No.13, pp.29-37 (2000).
3）BS7799 Information Security Management Part1: 1999 Code of Practice for Information Security Management, BSI.
4）BS7799 Information Security Management Part2: 1999 Specification for Information Security Management Systems, BSI.
5）http://www.ipa.go.jp/security/fy13/tech/secure_ml/secure_ml.html
6）http://www.ipa.go.jp/security/fy13/report/pki_interop/pki_interop.html

（平成 14 年 10 月 3 日受付）