5. 高度インターネットセキュリティ環境の構築実証実験

佐藤義男　(株) コムニック創研
對比地正樹　日本ディジタルイクイップメント（株）
松井健司　日本ディジタルイクイップメント（株）

■インターネットセキュリティ技術の必要性

ソフトウェアCALS環境によるソフトウェア開発に参加する企業は，インターネットを介して開発情報を交換する際に，外部からの侵入による各企業内情報の不正な閲覧，改ざん，または破壊などといった脅威から保護するためのセキュリティ確保がきわめて重要となる．セキュリティを確保するためには，各ビジネス形態やそこで発生する各プロセスに適したセキュリティを実装することが大切である．このため，防護すべき対象とセキュリティ対策のレベル（セキュリティ基準）を考慮する必要があるが，指針などを示す規約はいまだ整備されていない．

このため，次世代ソフトウェア開発ビジネスモデル（本特集「4．分散オブジェクト環境における部品組立型ソフトウェア開発の実証実験」図-1参照）における企業間機能統合の実現に焦点を当て，そこで必要なセキュリティ実装規約の作成とインターネットセキュリティ機能を開発し，これらを実際に複数企業間で利用して有効性，実用性を検証することにした．

■セキュリティ技術の実証

各種の職種に特化した企業群が，インターネットを利用して水平協業するための，必要な規約／ツール／環境を整備した．またそれを基に，人事情報システムを実際に開発することにより現実にそれが有効であることを，本特集「4．分散オブジェクト環境における部品組立型ソフトウェア開発の実証実験」の7社の仮想企業からなる実証実験で用いて実証した．

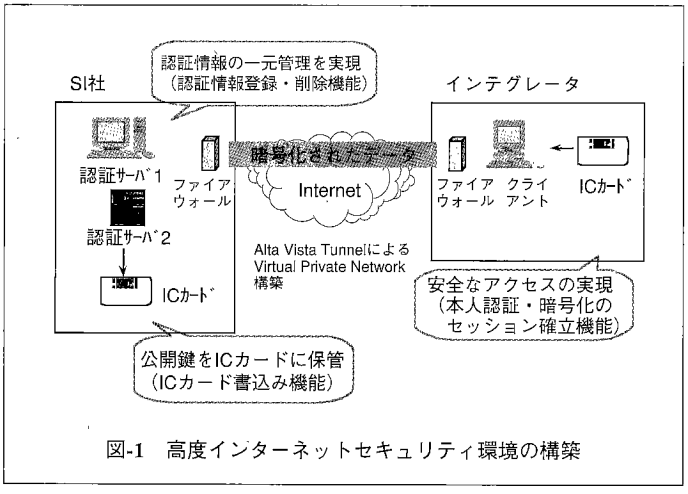

図-1　高度インターネットセキュリティ環境の構築

セキュリティ実装規約の内容としては，ネットワークセキュリティ構築・運用手順書，企業間情報伝達セキュリティ構築・運用手順書，認証情報管理・運用手順書がある．

次に，SI社とインテグレータ間にファイアウォールとVPN（Virtual Private Network）環境を構築し，セキュリティインタフェース機能（認証情報登録・削除機能，ICカード書込み機能，本人認証・暗号セッション確立機能，共有リポジトリセキュリティ機能）利用による以下の検証を行った．

- ファイアウォール構築の実証
- ICカード接続の実証
- 共有リポジトリアクセスの実証
- ワンタイムパスワードによる共有リポジトリアクセスの実証

企業間での高度セキュリティ確保のために，企業内ネットワークをインターネットに接続する際に，データを暗号化して漏出や盗難を防止し，外部PCなどの認証を行う．ここでは，盗聴に対してはAlta Vista Tunnel（DEC社）による通信データの暗号化（IP層の暗号化によるインターネット上の仮想的専用線の構築），成りすましに対してICカードを用いた本人認証というように，2つのセキュリティ技術を組み合わせることで信頼性の高い企業間での情報交換を実現している．通信データの暗号化には公開鍵（RSA方式），秘密鍵（RC4方式）による暗号化技術を組み合わせることで機密性を高めている．本人認証すなわち本人であることの証明には，改ざんがきわめて難しいICカードとパスワードによる保護によってセキュリティを高めている．

図-1にセキュリティインタフェース機能により，SI社とインテグレータ間において認証と暗号セッションの確立を行う例を示す．ここでは，本人認証をするための認証サーバを設置し，利用者から本人認証のための情報を受け取り，セキュリティパッケージが管理する認証情報リポジトリに登録・削除する機

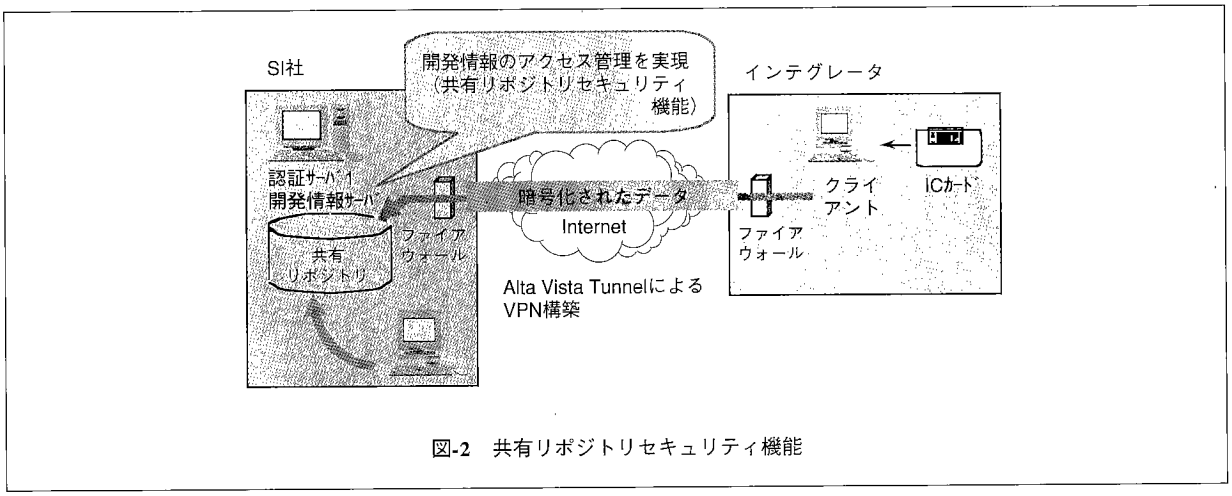

図-2　共有リポジトリセキュリティ機能

能，および認証情報と暗号化の鍵をICカードに書き込む機能を提供．さらにクライアント端末においてICカードから認証情報を読み込み，本人であることを確認後，セキュリティパッケージを通じて暗号化通信のセッションを確立する機能を提供している．

また，SI社とインテグレータ間での情報共有を実現する1つの手段として，SI社に共有リポジトリをおきインテグレータからアクセスを行うことを考慮している．実証実験では，その際のユーザ認証やアクセス制御といったセキュリティ確保の方式として，図-2に示す「共有リポジトリセキュリティ機能」（アクセス権限認証機能，アクセス権限認証ファイル作成機能，ワンタイムパスワード認証機能を含む）を適用した．この機能により，実際に使用された開発情報ファイル（機能仕様書，構造仕様書，結合試験仕様書，契約管理，進捗管理）に対してアクセスレベルを設定し，アクセス権限認証について機能面から検証した．さらに，SI社内での情報共有にグループウェアLinkWorks（DEC社）を利用し，企業間での情報共有に「共有リポジトリセキュリティ機能」を利用した場合の運用面での評価も行った．

■実証実験に対する評価

本実験では，インテグレータが分散環境において開発したサブシステムを，SI社がレガシーシステムへの移行するプロセスに適用して以下の実用性を確認できた．

- ファイアウォール構築では，機能をどのように設定するかは利用形態と企業の運用ポリシーに大きく依存するが，構築・運用手順書により設定作業が簡略化できる．
- ICカードを認証情報管理に利用した方が，通常方式（鍵情報と経路情報をフロッピーディスクに保持）よりも安全．しかし，ICカードリーダの設置が必要となる．
- Webサーバのユーザ認証とアクセス権限認証機能により，企業間でWeb経由による開発情報交換の安全性を確保できる．
- 固定パスワードがネットワークを流れる場合の危険性をツールで確認することにより，ワンタイムパスワード認証システムの有用性を確認できた．また，パスワード認証は，固定パスワードの危険性やユーザへのパスワードに対する危機意識を持たせることを教育することにより効果が上がることを認識した．

前述の技術実証により，各開発プロセスに共通なセキュリティ構築において以下の有効性を確認できた．

- インターネットトンネルとICカードにより，VPNの利便性を損なわずに安全性を高めることが可能．
- 共有リポジトリセキュリティ機能のアクセス制限のように，共有する情報によりアクセスのレベル設定が必須．

今後，ソフトウェアCALSを複数企業間でビジネスモデルとして採用するには，技術的な観点からみて少なくとも次の考慮が必要である．

- 共有リポジトリセキュリティ機能が管理する以外のリソースについても，アクセス制限の設定基準が必要．
- 複数企業間での実用的なインターネットセキュリティポリシーが存在すること．
- 運用面では，ICカードのユーザ登録，共有リポジトリのユーザ登録に手間がかかるため，運用ポリシーと合わせて検討が必要．

■高度インターネットセキュリティ環境の構築

複数企業間で水平分業を行うためには，セキュリティに関する規約／ツール／環境の整備が必須である．今回整備したものは実証実験にて，実際に人事情報システムの構築に使用され，その実用性が確認された．

参考文献
1）佐藤義男，青山幹雄，山下利夫，村山一美，高原　清，安竹由起夫：次世代ソフトウェアCALS基盤における部品組立型ソフトウェア開発，情報処理学会ソフトウェア工学研究会，No.118-8，pp.55-62（Mar. 1998）．

（平成10年8月7日受付）