*C Solution*TM プラットフォームコンポーネント

*C Solution*TM Platform Components

山田　朝彦 YAMADA Asahiko
貫井　春美 NUKUI Harumi
小林　恵 KOBAYASHI Megumi

OSや通信のインタフェースが標準化され，オープンシステムの時代となり，顧客が製品を自由に選択してシステムを構築できるようになったが，複数のベンダーの製品を組み合わせてシステムを構築することは予想以上の困難を伴うことがわかってきた。

当社はシステム インテグレーション サービスを中核とした事業を展開するなかで，システムが本来備えていなければならない機能を洗い出し，実現するためのコンポーネントを全世界から選定し，入念な組合せ検証を行い，不足部分を補いながら*C Solution*TM プラットフォーム コンポーネントとして提供している。システム エンジニア集団によるサービスとの組合せで，高い顧客満足を得ている。

As a result of the trend toward open systems, users can build their own system with products freely selected from those available on the market. At the same time, however, users have become aware of the difficulties involved in building a system by combining multivendor products.

During the process of expanding its system integration business, Toshiba extracted the essential functionality of systems and selected the best components from around the world to provide this functionality. These components have been combined and tested carefully, then provided as *C Solution*TM platform components. With the services of our skilled system engineers, these *C Solution*TM platform components have achieved high customer satisfaction.

1 まえがき

従来から，メインフレームやオフィスコンピュータ(以下，オフコンと略記)が提供してきた基本サービス機能を，グローバル スタンダードと呼ばれる製品群で実現することが*C Solution*TM プラットフォーム コンポーネントの目的である。コンポーネントの選定に先立って，システムが本来備えていなければならない機能を洗い出し，仮想的なコンピュータを創出させた。

仮想的なコンピュータの基本機能としては，基幹業務の世界では必須(す)でありながら，オープンシステムの弱点となっている次の二つの機能がある。

(1) 画面／印刷のフォーム(帳票)の制御機能
(2) オンライン系およびバッチ系を統合するジョブフロー機能

さらに，UNIX(注1)，WindowsNT®(注2)などの複数基本ソフトウェア(OS)上のアプリケーション プロセス(以下，アプリケーションと略記)が分散化，広域化したネットワークを介して相互動作するために必要な機能として次の三つがある。

(3) マルチOS環境でのメッセージ連携機能
(4) ネットワークとシステムの統合管理機能
(5) 情報システムのセキュリティ機能

これらの機能を実現するためのコンポーネントを全世界から選定し，入念な組合せ検証を行い，不足している機能を開発した。

2 フォーム(帳票)制御機能

複数のフォントやグラフィックを多用した表現力豊かなドキュメントの作成はオープンシステムの得意分野である。

ところが，オフコンが提供してきた帳票処理はオープンシステムの弱点となっている。

2.1 オープンシステムでのフォーム制御機能

フォーム制御機能は，従来から基幹系業務には必須の機能であった。フォーム制御機能は以下の機能群から構成される。

(1) 帳票の書式定義
(2) フィールドに入力される文字種別、データ種別を制約するためのフィールド属性
(3) フィールドに入力されたデータを編集および表示するためのフィールド属性制御
(4) フィールドからフィールドへのカーソル移動の制御

(注1) UNIXは，The Open Groupの米国およびその他の国における登録商標。
(注2) WindowsNTは，Microsoft社の商標。

(5) あらかじめ準備した帳票書式を下敷きとして，印刷データの重ね合せを行うフォーム オーバレイ処理

オフコンでは，きめ細かな顧客ニーズに対応するため独自機能を提供してきた。しかし，オープン プラットフォーム上で，フィールド制御機能のようなきめ細かな機能を提供するソフトウェアは欠落してしまっている。

反面，オープン化されたことで，マルチ プラットフォームで印刷処理ができるとか，豊富なフォントが利用できるといったメリットも生まれている。

図1に，従来とオープン プラットフォームでの帳票処理機能の分布を示した。Webtopプラットフォーム(注3)のフォーム制御機能は，オフコンで提供されていたフォーム制御機能のきめ細かさを踏襲し，オープン プラットフォームがもつメリットを加え，図1に示すように全体に機能を拡張し提供する。

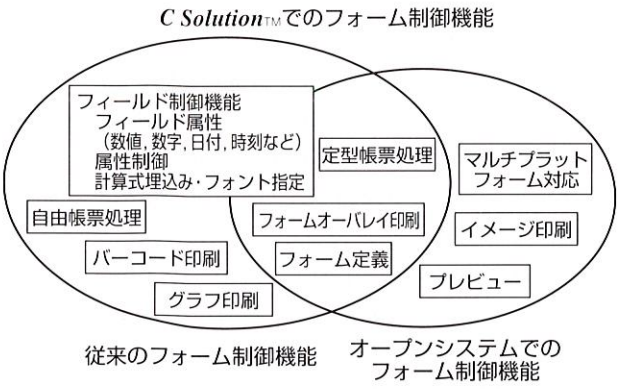

図1 フォーム制御機能　　*C Solution*™のフォーム制御機能では，従来のフォーム制御とオープンシステムのフォーム制御の利点を合わせもっている。

Form control facility

2.2 フォーム制御機能の構成

フォーム制御機能は，フォームについての印刷処理機能，Webベースシステムの画面であるブラウザ上での帳票処理機能，また，これらの処理に不可欠となる外字を含んだ漢字管理機能を提供する。これにより，従来の基幹系業務で必要不可欠であった帳票処理を，オープン プラットフォームのメリットを加えて実現する。

各機能は以下のとおりであり，図2にフォーム制御機能の構成を示す。

(1) 帳票印刷機能　　帳票のフォーマットを定義し，出力データをそのフォーマットに重ねるフォーム オーバレイ印刷を行う機能と，アプリケーションに対するインタフェースを提供する。

(注3) インターネット技術／WWW(World Wide Web) 技術に基づくアプリケーションシステム(Webベースシステム) のためのプラットフォーム。

(注4) Windowsは，Microsoft社の商標。

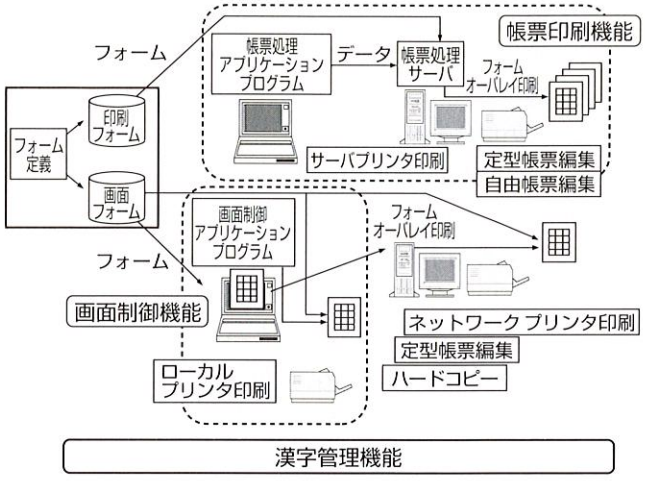

図2 フォーム制御機能の機能構成　　フォーム制御機能は帳票印刷，画面印刷，漢字管理の三つの機能から構成される。

Configuration of form control facility

(2) 画面制御機能　　Webtopシステムのクライアントであるブラウザでの帳票制御処理機能と，アプリケーションに対するインタフェースを提供する。

(3) 漢字管理機能　　UNIX，Windows®(注4)混在の環境において，外字処理を含んだ漢字処理機能を提供する。

3 ジョブフロー機能

オープンシステムでは，オンライン系アプリケーションのように会話型の処理を構築するためのソフトウェアが充実している。反面，従来のバッチ処理は苦手な分野となっている。

3.1 オープンシステムでのジョブフロー機能

Webtopプラットフォーム上では，アプリケーション システムの動作形態が2種類ある。一つはWebベースのオンライン系アプリケーション，もう一つが従来からあるバックエンドでのバッチ系アプリケーションである。

Webtop上での電子商取引(EC：Electronic Commerce)を例にとると，Webベースのオンライン系アプリケーションで購入した商品情報は，バックエンドでのバッチ系アプリケーションに渡され，発注・物流といった処理に連携される。

すなわち，Webベースのオンラインアプリケーションとバッチ系アプリケーションの連携を支援する機能は必須であり，Webtop上のジョブフロー機能の一つと考える。

Webtop環境では，ネットワーク上の任意のノード(接続中継点) のジョブと連携することも考えられる。すなわち，一つのノード内でのジョブフローだけでなく，ネットワークを介したジョブフロー制御も必要となる。

C Solution™プラットフォームコンポーネントでは，従来のバッチ環境の提供に加えて，オンライン系アプリケーションとの連携や，ネットワークワイドでジョブフローを構築するための環境を提供できる。

3.2 ジョブフロー機能の概要

Webtopプラットフォームのジョブフロー機能には，バッチジョブの処理効率向上と，オンライン処理系とバッチ系処理の連携といった課題を解決し，Webtopシステムにおけるオンライン系アプリケーションとバッチ系アプリケーションの連携を容易にし，かつ，高信頼なシステムを構築することを目的としている。さらに，ネットワークワイドなジョブフロー機能もサポートする。

そのため，ジョブフロー機能は以下の機能を提供する。

(1) ジョブフロー制御機能　　オンライン系アプリケーションとバッチ系アプリケーションの連携や，ネットワークワイドなジョブの連携を支援し，これらジョブの実行制御機能を提供する。

(2) シリアルバッチ機能　　逐次的処理の実行制御機能を提供する。

(3) パラレルバッチ機能　　ジョブネットワークによる並列処理機能に加えて，データを共有または最適に分割しバッチ処理に割り当て，複数のバッチジョブを並列に実行制御する機能を提供する。

4 メッセージ連携機能

4.1 オープンシステムでのメッセージ連携機能

オープンプラットフォーム，特にマルチプラットフォーム環境では，各アプリケーションがリアルタイムに密に連携するだけではなく，非同期に比較的疎な形で連携をする場合も多い。例えば，ホストコンピュータ上の既存アプリケーションシステムとの連携などはこの代表例である。

このような場合，メッセージを安全に転送することに加え，メッセージの到着により任意のアプリケーションを実行するといったメッセージベースのアプリケーション連携機能が必要になる。これをメッセージ連係機能と呼ぶ。

4.2 メッセージ連携機能の概要

メッセージ連携機能は，UNIX，Windows®，ホスト系OSといったマルチプラットフォーム上のアプリケーションに対して，信頼性の高い非同期型のメッセージ通信機能を提供し，さらに，このメッセージ通信における送受信をイベントとしたアプリケーション実行制御機能を提供する。

主な機能は以下のとおりであり，図3にメッセージ連携機能の構成を示す。

(1) メッセージ通信機能　　信頼性あるメッセージ通信機能を提供する。メッセージ通信は，非同期通信方式を基本とし，メッセージ送信先のコンピュータシステムやネットワークの障害をアプリケーションに意識させず，信頼性あるマルチプラットフォーム環境でのメッセージ通信ができる。

信頼性を高めるための機能としてメッセージの到着保証や障害発生時のリトライ機能を具備する。

(2) アプリケーション連携機能　　メッセージの送受信や時刻・時間といった各種イベントをトリガとしてアプリケーションを起動することでアプリケーション連携機能を提供する。

(3) 履歴管理機能　　上記のメッセージ通信，アプリケーション連携の履歴を収集し管理する。メッセージ通信はネットワーク上のコンピュータシステム間にまたがった履歴収集が必要となる。

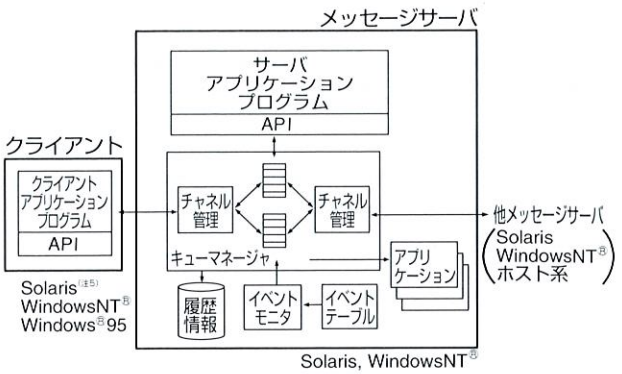

図3　メッセージ連携機能の構成　　メッセージを安全に転送し，メッセージによるアプリケーションの非同期的な連携ができる。
Configuration of message facility

5 ネットワークシステム管理機能概要

急速に普及したパソコン(PC)を収容するために拡大したネットワークは，インターネット時代を迎え，トラフィック量が爆発的に増加した。また，ネットワークへの依存度が高くなり，ネットワークの障害が広範な基幹業務の停止に直結する時代となった。こうのような状況のなかで，ネットワークの構成を把握し，障害に迅速に対応するために管理ツールを導入する顧客が増えてきた。

SNMP(Simple Network Management Protocol)によるネットワーク管理の標準化が定着したことにより，ネットワーク管理プラットフォーム製品が普及している。

その一方で，顧客を訪問すると高機能なツールを導入したが，本来の機能を使いこなせないでいる場合が多い。特に，スイッチネットワークやバーチャルLANの登場で，ネットワークが高度化したことにより，ツールを導入しただけでは適切な管理は実現できないという状況が生まれた。

(注5)　Solarisは，米国SunMicrosystems社の商標。

管理範囲が広く，標準化が遅れているシステム管理の分野ではこの傾向はさらに深刻であり，ソフトウェア配布，ファイル バックアップといった特定のシステム管理分野で著名なソフトウェアを買いそろえても，相互の連携がないために管理業務が煩雑になってしまっている。顧客はネットワークとシステムの管理を統一的にサポートする環境を必要としている。

当社は，ネットワーク システム管理の分野を本質的にサービスを指向する事業領域ととらえ，システム エンジニアを集結させたセンター組織を設置し，最新技術を活用したサポートサービスの開発・提供に注力してきた。全世界レベルで優れたツール群を活用した当社のネットワーク システム管理のシステム インテグレーション サービスが***C Solution***TMベースのシステムを強力にサポートする。

5.1 ネットワーク管理機能

ネットワーク管理の最初のステップは，自社のネットワークの構成を把握することである。ネットワークへの機器の接続状況やネットワーク機器のトポロジー(配置) の変更が日常化しているため，紙ベースでの管理には限界がある。ネットワークの最新構成を把握し，障害を迅速に切り分けるために，“OpenView(注6) ネットワークノードマネージャ”のオートディスカバリ機能を活用した構成管理機能を提供している。ネットワークに接続された機器の情報を収集し，ネットワークマップが自動作成される。ネットワークマップは論理的な接続関係で描画されるが，障害箇所の把握を容易にするために，フロアやビルの物理的なマップを背景としたネットワークマップへとカスタマイズする構築支援サービスも提供している。

ネットワーク機器から送り出された障害メッセージを顧客の環境に合わせて，わかりやすいメッセージに変換して表示することも構築支援サービスの一つである。さらに，遠隔に設置された警報装置への通報や，電子メールやポケベルを活用した管理者への障害通知を可能とすることで，TCO(Total Cost of Ownership) の削減を実現する。

最近ではネットワークのトラフィック(一定時間に流れるデータ量) について顧客の関心が高まっており，日常のトラフィックを記録し，ネットワークの状態を把握することで，障害を事前に回避したり，将来の設備計画を立案するためのデータとして活用が試みられている。運用支援サービスでは，このような日常のトラフィックの収集から解析・レポート作成を支援するサービスも提供している。

5.2 サーバ管理機能

Webtopコンピューティングでは，ネットワークの管理に加えて，ネットワーク上に分散配置されたサーバおよびサーバ上のプログラムの稼働状況の管理が重要となる。

WindowsNT®用のシステム管理ソフトウェアは次の2種類に大別される。

(1) UNIX用のシステム管理ソフトウェアをWindowsNT®へ移植したもの

(2) WindowsNT®にターゲットを絞って開発されたもの

当社は，WindowsNT®環境のきめ細かな管理を実現するために，後者に分類されるOpenView ManageXを採用し，図4に示すように顧客の全社レベルの管理を担当するOpenView IT/Operationsとの連携により，シームレスな管理を実現している。

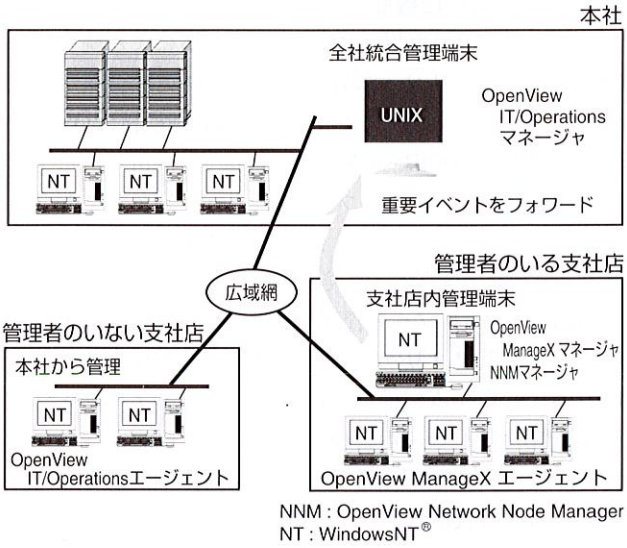

図4 サーバ管理のシステム構成　管理者がいる支社店では，下位マネージャで管理し，重要なイベントを本社の上位マネージャへ転送する。
Configuration of server management system

当社は，これらのサーバ管理ツールにより管理のための枠組みを提供するとともに，構築支援サービスとして，顧客の環境に合った管理ポリシーの設計をサポートしている。

管理ポリシーは，管理対象の管理方法を記述したスクリプトであり，障害の早期検出や自動修復のかなめとなる。管理ポリシーはノウハウの固まりであり，当社がもつORACLE(注7) データベースやLotus Notes(注8) などを利用した豊富なシステム構築経験に基づき，顧客の環境と条件をよく認識しながら開発している。

5.3 PCクライアント管理機能

急速に普及が進み，数万台規模のPCクライアントを抱え，日常的な管理業務に忙殺されるという状況が生まれている。PCクライアントを管理するために必要となる以下の機能を提供するツールとして，PCクライアント管理機能をもつ

(注6) OpenViewは，Hewlett Packard社の商標で，同社のネットワークシステム管理製品群の総称。
(注7) ORACLEは，Oracle社の商標。
(注8) Lotus Notesは，Lotus Development社の商標。

OpenView DTA(DeskTop Administrator)を選定した。

(1) ソフトウェア配布機能
(2) ソフトウェアおよびハードウェアの構成管理機能
(3) ライセンスの管理機能

全社レベルで導入するためには，ネットワークの構成やそのトラフィックを事前に分析し，企画・設計段階で分散化や階層化を検討しておく必要がある。個々の機能は単純でわかりやすいが，規模やネットワーク構成によっては十分な検討と事前検証を必要とする。

5.4 リソース管理機能

オープン化以前の専用システムでは，OSによる統一的な管理機構により，リソース管理や，ジョブ実行管理が実現されていた。オープン化によりこれらの管理機構はOSから欠落し，DBMS(DataBase Management System：データベース管理システム)やジョブスケジューリングソフトウェアといったミドルウェアや，個別のアプリケーションによる作り込みにより実装されてきた。

C SolutionTMのリソース管理機能は，オープンシステム上で動作する分散アプリケーション間で利用されるリソースを統一的に管理する機構で，標準化によるアプリケーションの生産性の向上と運用管理コスト低減を目的に，リソース共有，リソース制御機能，リソース監視機能を提供する。

リソース共有機能は，システム内で共有するリソースを集中して管理するディレクトリサービスで，ユーザー管理，セキュリティ管理，システム構成管理を実現する基盤となる機能である。リソース制御機能は，リソースの割付け，共有および排他といったアプリケーションやコンポーネント間の同期・排他制御機能を提供する。リソース監視機能は，アプリケーションレベルの統一されたログ記録(コンピュータの運用記録)機能によりリソース状況を収集・解析する機能で，システム開発時のデバッグ試験や性能チューニング，運用時の障害解析やリソース計画に利用する。

5.5 システム生成支援機能

システム生成支援機能は，***C Solution***TMプラットフォームの各機能のコンポーネントをシステム上に構築し，統一的な実行環境を提供する。パラメータ化した構成管理情報を基に以下の機能を提供する。

(1) ソフトウェア，データの配布
(2) インストールと環境設定
(3) ソフトウェア，データの変更管理

これらの機能により，システム構築時の環境構築作業と，運用時の変更管理作業の自動化を支援できる。

6 セキュリティ機能の概要

インターネットの普及とともに，情報システムのセキュリティが認識されるようになった。かつては各ベンダー固有の技術で築かれてきた情報システムが，オープン化の時代を迎えて共通の技術基盤の上に構築されるようになった。なかでもTCP/IP(Transmission Control Protocol/Internet Protocol)に代表される共通のネットワーク技術の意味は大きく，とりわけWebの出現により情報システムは転換期を迎えている。その反面，他社の情報資産をねらうハッカー達にとっても活動のしやすい環境が築かれたとも言える。公開Webには誰でもアクセスできるが，もしそこにセキュリティの不備があれば，ホームページが落書きされたりすることになりかねない。盗聴，改竄(ざん)，なりすましなどのネットワーク環境での脅威を防ぐためのセキュリティ技術は，情報システムに欠かすことができなくなっている。

セキュリティの重要性に反し，その実現は容易ではない。システム全体にわたる統一的な方針の徹底，システム管理者にとって管理のしやすさ，エンドユーザーにとっての使いやすさが必要だからである。また，現実のオープンシステムにおいては，セキュリティ機能はOSやミドルウェアにより個別に提供されているため，システム全体で統一的なセキュリティを実現することは困難である。ネットワークがボトムアップで形成されてきたことも，セキュリティ管理を困難にさせる原因となっている。また，セキュリティを徹底させた場合，エンドユーザーにとっては利便性が低下する場合が多い。サーバにアクセスするたびにパスワードが要求されるなどである。このような問題を解決するセキュリティ製品も提供されてはいたが，特別な環境が必要になったり，既存アプリケーションの改造が必要になったり，導入への障壁があった。

これら従来のシステムセキュリティの問題点をWebtopベースで総合的に解決することが，***C Solution***TMのセキュリティの主な目標である。すなわち，セキュリティを確保しつつ，TCO削減，ユーザーの利便性低下の抑制，システム全体を統合するセキュリティを実現することである。

以上の条件を満たしつつ，***C Solution***TMはセキュリティ機能を提供する。Webtopベースのシステムにおいて，各ユーザーを正しく認識し，Webコンテンツ，アプリケーション，データベースなどの情報資源へのユーザー権限に応じたアクセスができる。さらに，これらの情報資源の不正利用を防ぎ，情報の漏洩(えい)を防止し，万一問題が発生した場合は原因究明を補助する下記機能を提供する。

(1) ユーザー情報管理機能
(2) ユーザー認証機能
(3) アクセス制御機能
(4) 秘匿機能
(5) 監査機能

図5にセキュリティ機能を示す。

これらの機能群の基礎となるのが，ユーザー情報管理機能とユーザー認証機能である。この二つの機能のシステム

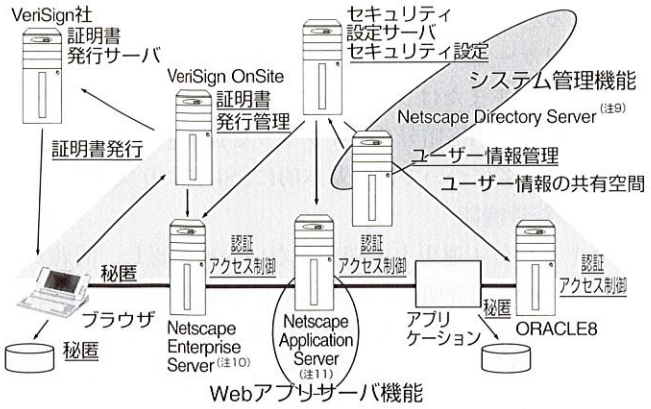

図5　*C Solution*™セキュリティ機能の構成　ディレクトリサーバが管理するユーザー情報の共有が*C Solution*™のセキュリティを支える。ユーザー認証情報は公開鍵証明書を使い，通信はSSLで保護する。

Security architecture of *C Solution*™

全体での共有が，*C Solution*™セキュリティの目標達成の基盤となる。以下，各機能について述べる。

6.1　ユーザー情報管理機能

ディレクトリサーバがシステム全体のユーザー情報を一括集中管理する。これにより，システム内のどのサーバからもシステムを利用する全ユーザーを識別することができ，システム全体を統合するセキュリティの基礎が築かれる。一括集中管理の結果，管理コストが低減する。なお，ディレクトリサーバはNetscape Directory Serverを利用する。

管理するユーザー情報は，個々のユーザーごとの，名前，ID(Identification Data)，認証情報(公開鍵証明書またはパスワード)，メールアドレス，所属組織，役職，電話番号，ファクシミリ(FAX)番号などである。これらの情報を，登録，変更，削除，検索することができる。

さらに，上記ユーザーからなるグループを定義して，ディレクトリサーバで管理する。グループ情報についても，ユーザー情報と同様の操作ができる。例えば，グループ検索機能で，あるユーザーuがグループGに属しているか否かを問い合わせることができる。同一の権限をもつユーザーをグループ化し管理することも，管理容易化の要因の一つである。ユーザーの組織異動があった場合もグループ情報の変更だけで対応することもできる。

6.2　ユーザー認証機能

ユーザー認証では，VeriSign社の公開鍵証明書(以下，VeriSign公開鍵証明書と略記)を*C Solution*™標準の認証情報として利用する。公開鍵証明書はディレクトリサーバに登録し管理する。各サーバはユーザーから提示された証明書をディレクトリサーバに問い合わせ，認証する。

VeriSign公開鍵証明書は，ユーザーの公開鍵を公開鍵認証局が電子署名した電子データであり，その形式は公開鍵証明書に関する世界標準のX.509に準拠している。これは，信頼できる第三者による身分証明による認証情報である。VeriSign公開鍵証明書を*C Solution*™の認証情報とした理由は，Netscape Enterprise Serverをはじめとする多数の製品でVeriSign公開鍵証明書が利用でき，一組織内に留まらず，インターネット上で通用する認証情報だからである。その結果，イントラネットだけでなくエクストラネット(注12)の実現に適している。

VeriSign公開鍵証明書とディレクトリサーバの協調により，統一的かつ各サーバ間での強い連携をもつセキュリティの実現ができる。例えば，Webサーバがユーザーから受け取った公開鍵証明書を，Webサーバと連携動作しWebから起動されるアプリケーションに関する管理機能を提供するWebアプリサーバに渡すことにより，背後のアプリケーションをユーザーの権限で実行させることができるなどである。

VeriSign公開鍵証明書は一般に個人単位でVeriSign社から発行を受けるが，VeriSign社製品OnSiteの利用により，当該組織内のユーザー証明書とその発行についての諸手続きを管理することができる(この場合も，証明書はVeriSign公開鍵証明書であることに変りはない)。

公開鍵証明書をICカードに格納すれば，セキュリティはより堅固になる。証明書をディスクに保持した場合は，PCの一時利用，複数ユーザーのPC共有の場合に問題がある。ICカードを携帯し利用すれば，ICカード以外の環境に左右されずユーザーごとの権限でシステム内資源が利用できる。その結果，エンドユーザーの利便性が向上する。

ブラウザとWebサーバ間は，公開鍵証明書によるSSL(Secure Sockets Layer)の相互認証を行なう。サーバがユーザー(またはクライアント)を認証するだけでなく，ユーザーがアクセス先のサーバを認証して信頼できるサーバか否かを判定することができる。

6.3　アクセス制御機能

アクセス制御機能は，システム内のWebサーバ，Webアプリサーバ，データベースサーバ上の個々のデータやプログラムなどの資源をユーザーの権限に応じて利用可否を決定する機能で，制御情報(ユーザーやグループごとの権限)を設定する機能と制御する機能自体に分けられる。

アクセス権限設定機能では，データやプログラムなどの資源ごとに，どのユーザー，または，どのグループに属するユーザーに対して，どのような処理を許可／禁止するかをあらかじめ設定する。ユーザー情報管理機能の場合と同

(注9)，(注10)，(注11)　Netscape Directory Server, Netscape Enterprise Server, Netscape Application Serverは，Netscape Communications社の商標。

(注12)　エクストラネットは，インターネットの技術をベースに，特定の企業間または地域間に限定し利用できるように構築したネットワーク。

様に，グループ化がアクセス制御設定の管理コストを低下させる。しかし，実際はこのような設定は煩雑であり，セキュリティ管理の問題の一つである。この問題を，***C Solution***$_{TM}$の提供するセキュリティ設定サーバが軽減する。複数サーバにわたる設定内容から抽象化した“設定パターン”とそれに“直交”する情報を登録し，実際にアクセス権限情報を設定する際に，“設定パターン”と“直交”情報の組からアクセス権限情報を生成する。

以下，具体例で説明する。

経理部権限情報：

経理部部長→読取り可，経理部課長→読取り可

人事部権限情報：

人事部長→読取り可，人事部課長→読取り可

この二つの情報から，下記パターンを抽出することができる。

“設定パターン” α ：

部長→読取り可，課長→読取り可

“設定パターン” α に“直交”する情報は，それぞれ“経理部”と“人事部”である。“経理部”と α から経理部権限情報が，“人事部”と α から人事部権限情報が生成される。

利用頻度の高い“設定パターン”と“直交”情報をGUI (Graphical User Interface) ベースでセキュリティ設定サーバに登録し，同じくGUIベースでこれらの情報を組み合わせることで，アクセス権限設定の負荷が軽減される。

実行時にユーザーがサーバの資源にアクセスすると，アクセス権限設定機能で定めた権限と照合して，ユーザーの資源利用の可否を決定する。

以上はサーバがもつ機能としてのアクセス制御を述べたが，さらに細かいアクセス制御が必要な場合は，アプリケーションで作り込みを行えるよう，アクセス制御API (Application Program Interface) を***C Solution***$_{TM}$は提供する。

6.4 秘匿機能

秘匿機能では，ディスク上のデータとネットワーク上を流れるデータに対する暗号化および復号化の機能を提供する。ディスク上のデータの秘匿は，さらに，エンドユーザーが利用するマシンのローカル情報の秘匿とアプリケーションが利用するデータの秘匿に分けられる。

エンドユーザー向けローカル情報の秘匿は，ノートPCなどの盗難対策である。これに対してはDES (Data Encryption Standard) アルゴリズムによるファイル暗号化ツールを提供する。

アプリケーションによるデータ秘匿は，アプリケーションがファイルまたはファイルの一部を暗号化および復号化するための，DES暗号化ライブラリを提供する。

通信の秘匿については，基本的にSSLにより実現する。

6.5 監査機能

セキュリティ運用上の問題がないかを確認し，問題があった場合の原因究明に，ログの解析が重要な役割を果たす。また，内部犯罪の牽(けん) 制の意味でもログ解析は重要である。しかし，OSやミドルウェアごとに形式が異なったり，解析に熟練を要するため，ログが十分に活用されているとはいえない。***C Solution***$_{TM}$は，形式の異なるログを統一した形式に整形したり，あらかじめ定めたエラーに対してはシステム管理者に通知するなどの機能を提供して，システム管理者のログ解析コストの低減を図る。

7 あとがき

優れたコンポーネントを選定し，入念な組合せ検証を行い，オープン製品では不足している機能を補うことで，メインフレームやオフコンの基本機能をオープンシステムで実現した。***C Solution***$_{TM}$プラットフォーム コンポーネントを当社のシステム インテグレーション サービスとともに提供し，顧客が安心して使えるシステムを迅速に構築していく所存である。

山田　朝彦　YAMADA Asahiko, D. Sc.

SI技術開発センター セキュリティ技術支援担当参事，理博。情報セキュリティによるSIソリューションの開発に従事。情報処理学会会員。

System Integration Technology Center

貫井　春美　NUKUI Harumi

SI技術開発センター SIコア技術担当参事。
オープンシステムによるSIソリューションの開発に従事。情報処理学会会員。

System Integration Technology Center

小林　　恵　KOBAYASHI Megumi

SI技術開発センター ネットワーク管理技術支援担当グループ長。ネットワークシステム管理のSIサービスの開発に従事。情報処理学会会員。

System Integration Technology Center