当社ITシステム構築の標準体系におけるセキュリティ

Security Features of Toshiba Standard IT System Solutions

山田　朝彦 YAMADA Asahiko
小林　智恵子 KOBAYASHI Chieko
原嶋　秀次 HARASHIMA Shuji

当社のIT（情報技術）システムビジネスの中心はWebtopベースのシステム（以下，Webtopシステムと略記）であり，現在はWebtopシステムのセキュリティ機能の研究・開発を進めている。Webtopシステムにおいて，ユーザーを正しく識別し，Webコンテンツ，Webアプリケーション，データベース（DB）などへのユーザー権限に応じたアクセスの実現を目指している。当社は，Webサーバへのログイン IDによる，Webアプリケーションからの DBまでのシングルサインオンを実現した。

We are conducting research on security functions for Webtop systems.　In Webtop systems, a user must be identified correctly and access to information resources, such as Web contents, Web applications, and databases, is permitted only if the user is authorized to use them.

Toshiba has realized the implementation of a system which performs delegation and single sign-on throughout the information resources.　Database systems authenticate the user with authentication information passed by the application, which is stored in the directory server (LDAP server) with confidentiality.　This enables us to build a highly secure system in which a user can have access to the information if and only if that user has the right to do so.

1 まえがき

当社では，ITシステム構築においてWebtopシステムを重視しており，その標準的なソリューション体系を提案している。そのセキュリティ機能として，ユーザー認証，アクセス制御，秘匿，監査などの研究・開発に取り組んでいる[(1)]。特に，Webtopシステムにおいて，ユーザーを正しく認識し，Webコンテンツ，Webアプリケーション，DBなどの情報資源へのアクセスをユーザー権限に応じて可能にし，これらの情報資源の不正利用や漏えいを防止するための研究・開発を行っている。

ユーザー権限などのセキュリティ情報の一元管理には，ディレクトリサーバの活用が有効である。TCP/IP（Transmission Control Protocol/Internet Protocol）上でディレクトリにアクセスするためのプロトコルLDAP（Lightweight Directory Access Protocol）[(2)]が標準化されてから，ディレクトリサーバの利用は急速に一般化した。ディレクトリサーバは，これまでのような単なる電話帳検索的な使い方から，情報を一元管理するリポジトリとして，情報システムの中核コンポーネントになりつつある。当社は，ディレクトリサーバ上のユーザー情報を駆使して，Webサーバ，Webアプリケーションサーバ，DB管理システム（DBMS）までのシングルサインオンを実現した。シングルサインオンとは，アプリケーションごと，サーバごとに複数回発生するユーザー認証をエンドユーザーが一度行った後はシステムが代行する機構である。

ここでは，Webアプリケーションサーバ上のアプリケーションからDBMSへのアクセスにおいて，ブラウザを利用するユーザーの権限でログインを実現するメカニズムについて述べる[(3)]。ディレクトリサーバで管理された認証情報を，今回作成したライブラリが利用してDBMSにログインする。

2 DBアクセスのセキュリティ

現在，一般的に行われているWebtopシステムの運用では，Webアプリケーション構築時に，あらかじめWebアプリケーションがDBMSにアクセスするためのログイン情報をDBMSに登録しておき，このログイン情報で，Webアプリケーションから DBMSにアクセスしている。この従来方式では，ブラウザを利用するユーザーの権限に応じたDBMSアクセスは行えないという問題があった。

当社は，Webアプリケーションにログインユーザーの認証情報をあらかじめ記述することなく，Web上でアクセスを許可されたユーザーの権限でDBMSへアクセスする方式を提案する[(3)]。

2.1 Webtopセキュリティ機能

Webtopセキュリティ機能は，当社の提供するソリューション体系において，Webtopコンピューティングを実現させる基盤環境“Webtopプラットフォーム”の一機能と位置づけられる。Webtopプラットフォームは，インターネット，イントラネット上で業務システムを開発／運用するための基盤技術であり，UNIX[(注1)]，Microsoft® Windows®[(注2)]が混在するオー

（注1）　UNIXは，商標。
（注2）　Microsoft，Windowsは，米国Microsoft Corporationの米国及びその他の国における登録商標。

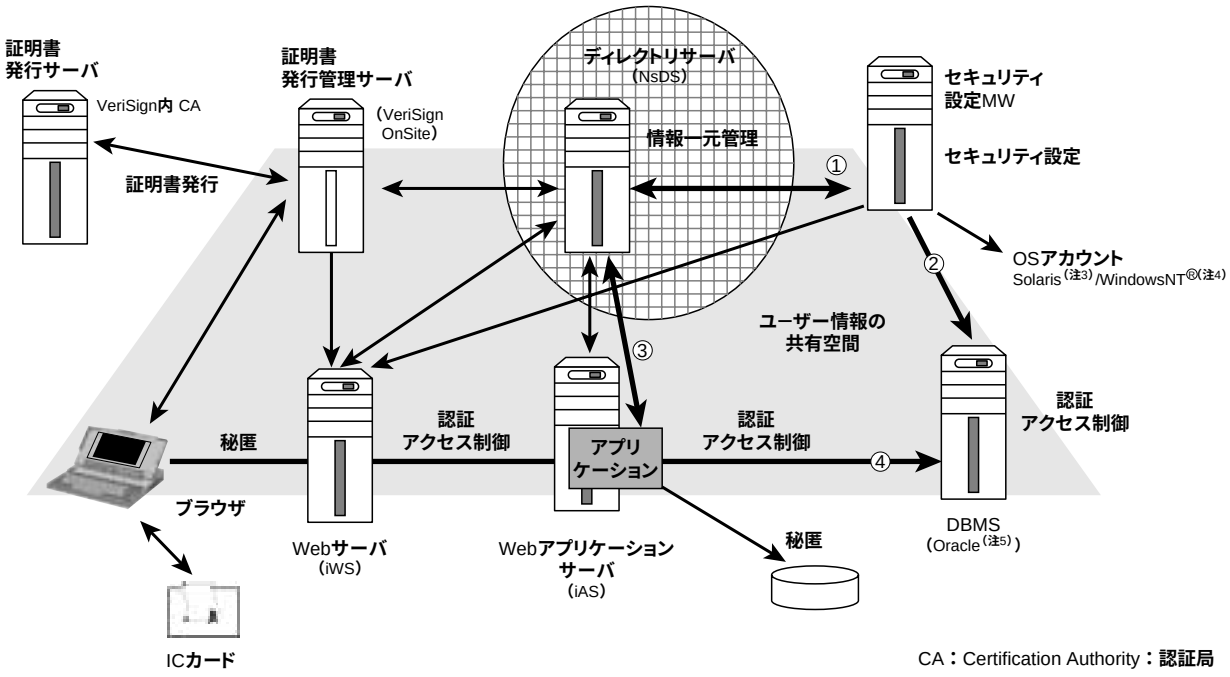


図1．当社の標準的Webtopシステムの構成　ユーザー情報はディレクトリサーバで一元管理する。
Configuration of Toshiba standard Webtop system

プンな環境下において，アプリケーション開発や運用に必要な標準機能を提供し，アプリケーションの信頼性や拡張性を強化する。Webtopセキュリティ機能は，ディレクトリサーバとセキュリティ設定ミドルウェア（以下，セキュリティ設定MWと略記）を軸にして統合的なセキュリティ管理を実現している。セキュリティ設定MWについては2.2節で述べる。

Webtopセキュリティ機能を**図1**に示す。独自に開発したセキュリティ設定MWを通して，ユーザー情報のディレクトリサーバへの格納をはじめとするセキュリティ情報の設定を行う。ICカードを利用することにより，Webtopシステムでのシングルサインオンを実現している。図中の①から④がこの論文で述べる機能である。図中の①，②は，DBMSへのシングルサインオンを行うための登録系処理であり，セキュリティ設定MWからディレクトリサーバとDBMSへ情報を登録する機能である。また，図中の③，④は，DBMSへのシングルサインオンを行うための実行系処理であり，Webアプリケーションサーバ上で動作するWebアプリケーションに組み込んで利用するライブラリの処理である。このライブラリは，DBMSに接続するために必要な認証情報をディレクトリサーバから取得し，DBMSへ接続する。この際，Webアプリケーションには DBMSへの接続情報だけが渡され，ユーザー情報はライブラリからWebアプリケーションに渡されることなく，安全なシステムとすることができる。

今回の開発では，WebサーバはiPlanet Web Server（iWS），ディレクトリサーバはNetscape Directory Server（NsDS），WebアプリケーションサーバはiPlanet Application Server（iAS），DBMSはOracle8i(注6)を対象とした。

2.2　セキュリティ設定MW

1章で述べたように，セキュリティ情報の一元管理にはディレクトリサーバの活用が有効である。しかし，ディレクトリサーバにおいて，シングルサインオンに向けてOS（Operating System）などのシステムコンポーネントとの連携・統合が必要なことなどの課題がある。

セキュリティ設定MWは，分散した複数サーバにおけるユーザー／グループ情報やアクセス制御情報など，セキュリティ情報を一元管理するための支援ツールであり，LDAP上のユーザー情報と連携してDBMSへのデータ登録／変更／削除を行う。そのほかに，WindowsNT®やNetwork Information Service（NIS）管理のOSアカウント情報やファイルアクセス制御情報，また，Webサーバ上のコンテンツに関するACL（Access Control List）情報を統合的に管理する。セキュリティ設定MWは，サーバ／エージェントモデルで実装しており，OSやWebサーバやDBMSを搭載するハードウェア上にエージェントを設置する。したがって，セキュリティに関する情報設定の対象となるコンポーネント用のエージェントを作成／追加することが可能であり，情報の一元管理を容易にしている。

2.2.1　ディレクトリサーバへの登録／変更／削除

DBMS と連携させるために必要な情報を**表1**のとおり定

（注3）　Solarisは，米国SunMicrosystems社の商標。
（注4）　WindowsNTは，米国Microsoft Corporationの米国及びその他の国における登録商標。
（注5），（注6）　Oracle，Oracle8iは，Oracle Corporationの商標。

表1．ディレクトリサーバに格納されるDBアクセス用ユーザー情報
User information for database access stored in directory server

属　性	型	備　考
ユーザー名	文字列	
パスワード	バイナリ	ディレクトリには暗号化して登録する
インスタンス名	文字列	
接続名	文字列	
オーナーテーブル	文字列	選択肢　－/R/W/RW
その他のテーブル	文字列	選択肢　－/R/W/RW
オーナープロシージャ	文字列	選択肢　－/EX
その他のプロシージャ	文字列	選択肢　－/EX
ロール	文字列	
ユーザー表領域	文字列	
一時的な表領域	文字列	
DBMSユーザー作成フラグ	文字列	選択肢　true/false
DBMSユーザー削除フラグ	文字列	選択肢　true/false

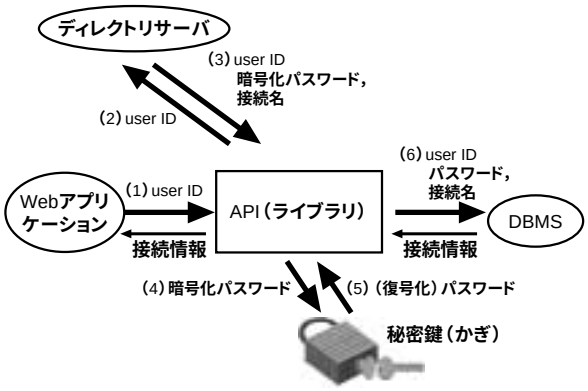


図2．DBセキュリティライブラリの動作　ディレクトリサーバからユーザー情報を獲得し，DBMSにログインする。
Function of database security library

義した。ディレクトリサーバには個々のDBのスキーマ情報を持ち込まず，セキュリティポリシーだけを管理する方式とした。ディレクトリサーバには，LDAP-API（Application Programming Interface）を用いて情報を登録／変更／削除する。

なお，DBMSユーザー用パスワード情報は暗号化して登録する。後述するDBセキュリティライブラリがパスワード情報を取得する際，パスワード情報が漏えいすることを防ぐためである。暗号化については2.3節で述べる。

2.2.2　DBMSへの登録／変更／削除　表1に示すデータをDBMSに対して登録／変更／削除する。ただし，フラグ情報は，ディレクトリ上の情報とDBMS上の情報との整合性管理のために，ディレクトリで利用するものである。例えば，情報の管理として，ディレクトリサーバからDBMSに関する情報を削除するがDBMS側には残したい場合は，削除フラグをfalseにすることにより，DBMS側には情報をそのまま残し，ディレクトリからだけ削除できる。DBMSには，SQL＊Net（Net8）などのネットワークソフトウェアにより通信し，SQL（Structured Query Language）文を実行する。

2.3　DBセキュリティライブラリ

DBセキュリティライブラリは，APIを提供し，ディレクトリサーバで一元管理している認証情報を使って，DBMSへの接続を可能にする。DBセキュリティライブラリの処理を図2に示す。

2.3.1　ディレクトリサーバからの情報取得　図2の(1)，(2)，(3)の処理で実現される。ユーザー認証ID（IDentification）（以下，user IDと略記）は，WebサーバからWebアプリケーションサーバを経て，Webアプリケーションが取得する。その後，DBセキュリティライブラリは，以下の処理を実行する。

(1)　Webアプリケーションからuser IDを受け取る。
(2)　取得したuser IDをキーに，ディレクトリサーバを検索する。
(3)　ディレクトリサーバに一致するuser IDが存在すれば，暗号化されたパスワードと接続名を取得する。

2.3.2　DBMSへの接続　図2の(4)，(5)，(6)の処理で実現される。ディレクトリサーバから取得したDBMSへの接続情報を用いて，認証／接続を行う。なお，ディレクトリサーバから取得するパスワード情報は，機密性を保つために，トリプルDES（Data Encryption Standard）を用いて暗号化している。暗号化されたパスワードはDBセキュリティライブラリの中で復号化する。DBMS接続時は復号化されたパスワードを使ってアクセスする。以下に，APIの処理概要を示す。

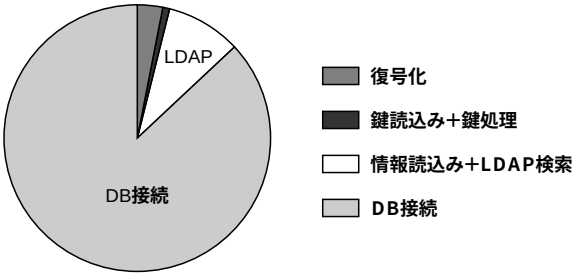
(4)　ディレクトリサーバから取得した暗号化されたパスワードを復号化する。
(5)　復号化されたパスワードを取得する。
(6)　user ID，復号化されたパスワード，接続名を使ってDBMSへ接続する。

3　DBアクセスのセキュリティへの考察

2章で述べたように，セキュリティ設定MW及びDBセキュリティライブラリにより，WebtopシステムにおけるDBアクセスまでを含めたシングルサインオンを実現できた。これにより，安全性の高い，しかも，よりきめ細かいユーザー権限を反映したDBアクセスを行うシステムの構築が可能となった。しかし，ユーザー情報以外のDBMSが扱う情報の設定をセキュリティ設定MWはサポートしていないなど，まだ課題は多い。

今回作成したDBセキュリティライブラリの性能を検証した。トリプルDESは対称暗号方式でもっとも利用されているものの一つである。暗号処理の欠点として，アルゴリズムの実行に時間が掛かる点が挙げられるが，実際に処理時間を測定して影響を調べた。

連続100回実行した各処理時間の平均値を図3に示す。この図に示すように，トリプルDESによる復号化の処理時間は全体の3％程度であり，ほとんど影響しないことがわかった。



連続100回実行の平均値（単位：ms）

復号化	鍵読込み＋鍵処理	情報読込み＋LDAP検索	DB接続	全体処理
4.62	0.7	14.83	130.67	150.82

図3．DBセキュリティライブラリの処理時間測定結果　暗号処理時間の占める割合は小さい。
Results of database security library processing time measurement

4 その他の取組み

Webアプリケーションの開発においても，セキュリティを重視すると，暗号化の要求が出てくる。しかし，例えば，トリプルDESライブラリなどのセキュリティ関係のライブラリは，その呼出し手順が複雑なため，一般のアプリケーション開発者が利用するのは容易ではない。当社では，アプリケーション開発者が容易にセキュリティライブラリを利用できるようにするため，APIの開発を進めている。すなわち，セキュリティライブラリのインタフェースを単純化し，ファイルからファイルへの暗号化／復号化などを一度の呼出しだけで実現するようなAPIを開発している。これらは，現在，デファクトスタンダードのセキュリティライブラリを対象としているが，今後は当社独自の暗号ライブラリも対象に加えていく。

Webtopシステムでは，J2EE(注7)（Java2 Enterprise Edition）アーキテクチャが標準的なものになり，またEJB(注8)（Enterprise Java Beans）などのコンポーネントベースの開発が開発効率／再利用性の良さから盛んになっており，これに加えて当社の標準的ソリューション体系では，アプリケーションフレームワーク(4)という独自のアプリケーション開発体系も持っている。また，CORBA(注9)（Common Object Request Broker Architecture）連携も重要性を増してきている。当社では，これらの動きに合わせて，標準的ソリューション体系を強化している。これに合わせて，上記セキュリティライブラリのコンポーネント化，システム全体としての統一感を持ったWebtopシステムのセキュリティ機能がより重要性を増しており，これらの開発を進めていく。

（注7），（注8）　J2EE，EJBは，SunMicrosystems社の商標。
（注9）　CORBAは，Object Management Groupの商標。

5 あとがき

ここで提案したDBアクセスのセキュリティ実現方式により，ブラウザを利用するユーザーの権限でのDBMSへのログインが可能となり，Webアプリケーションサーバ内でのユーザーデータの安全性を高めることが可能となった。また，この方式では，セキュリティ設定MWがDBMSにユーザー情報を設定するので，複数の種類の異なるDBMSが存在する場合への対応が容易である。更に，DBへのアクセス結果に応じて処理を変える仕組みを組み込むことによって，ユーザーごとの処理を，DBの登録内容で変更するといった利用方法も考えることができる。今後，WebtopシステムにおけるDBのセキュリティについてより深く研究・開発を進め，また，Webtopシステム全般のセキュリティ機能も強化していきたい。

文　献

(1) 山田朝彦，ほか．C Solutionプラットフォームコンポーネント．東芝レビュー．**54**，1，1999，p.38−44.
(2) Lightweight Directory Access Protocol（V3）RFC2251，1997−12.
(3) 小林智恵子，ほか．Webtopシステムにおけるデータベースアクセスのセキュリティ実現．データベース工学研究会「夏のワークショップ」，電子情報通信学会／情報処理学会．2000−7，p.109−114.
(4) 斉藤悦生，ほか．コンポーネントベース・フレームワーク技術（C Solution APF）全体構想とアーキテクチャ．情報処理学会第60回（平成12年度前期）全国大会．2000−3，p.1-241−1-242.

山田　朝彦　YAMADA Asahiko，D.Sc.
e-ソリューション社 SI技術開発センター SI技術担当主査，理博。運用を中心とした，システムセキュリティの研究・開発に従事。情報処理学会会員。
Systems Integration Technology Center

小林　智恵子　KOBAYASHI Chieko
e-ソリューション社 SI技術開発センター SI技術担当主務。LDAPを利用したセキュリティ情報管理，ユーザー認証，アクセス制御など Webtopシステムの研究・開発に従事。
Systems Integration Technology Center

原嶋　秀次　HARASHIMA Shuji
e-ソリューション社 SI技術開発センター SI技術担当主務。データベースシステムの研究・開発に従事。情報処理学会，電子情報通信学会，ACM会員。
Systems Integration Technology Center