ＯＬＴＰ指向認証サービス

5Ｇ－2

村田　明文*　，　香川　弘一*　，　滝本　秀明*
貫井　春美**　，　佐波　公夫**

*（株）東芝　府中工場
**（株）東芝　システム・ソフトウェア生産技術研究所

1．はじめに

オンライントランザクション処理（ＯＬＴＰ）は企業の基幹業務、銀行、証券取引、生産管理などさまざまな分野で使用されその重要性がますます上がっている。そこで利用されるデータは非常に重要であり、データの不正アクセス（書き換え、覗き見）からの保護が望まれる。

現在、認証サービスを提供する製品は数種類あるが、ＯＬＴＰに組み込んだ形での提供は殆ど行われていない。そこで、今回ＵＮＩＸ*サーバー上の当社独自のＴＰモニターであるＴＸ／ＡＴＰＳに認証サービス機構を実現したので報告する。

2．設計方針

ＯＬＴＰシステムの特徴としてユーザや端末数が多く業務処理量が非常に多いことが上げられる。この様な大規模で性能が要求されるシステムの認証サービスとして、以下の点に設計上の注意を払った。

（1）性能の確保
　実用に耐えうるトランザクション実行性能。
（2）大規模拡張性
　大規模構成での検証及び、処理が集中した時の処理の分散
（3）運用の簡便性
　運用面としてＴＸ／ＡＴＰＳの運用となるべくリンクした運用コマンドのＩ／Ｆ。
（4）システム構築の容易性
　認証サービスを利用する時、従来よりあるクライアント用ＡＰＩの上位互換Ｉ／Ｆの提供。

3．システム構成

本システムは、認証システム用の認証／暗号化のライブラリである認証ライブラリ、鍵を配布する鍵サーバ、認証を行う認証サーバ、認証サービス用の運用管理コマンドを作成し、通信ドライバと、トランザクション投入のクライアントライブラリを改造することとにより実現される。

図１に本システムの構成を示す。

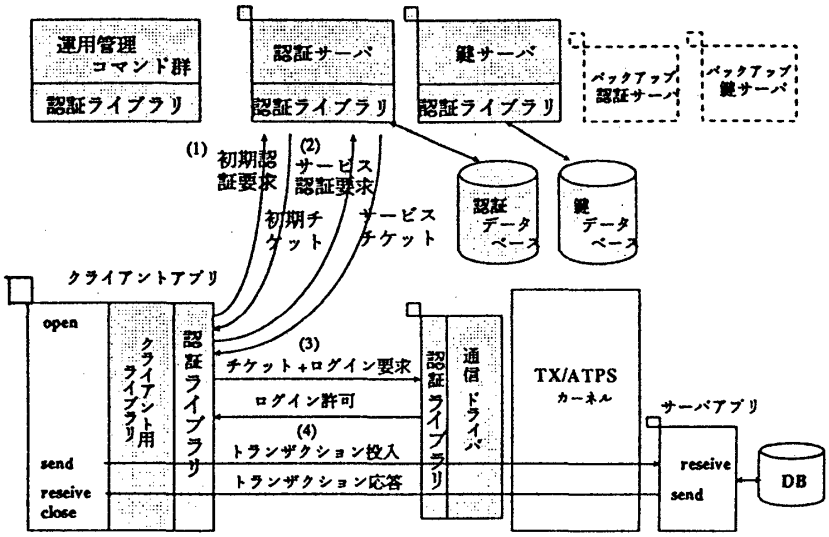


図 1: システム構成

上記構成でのトランザクション投入シーケンスを以下に示す。

（1）認証サーバにユーザの認証要求を送り、認証サーバがユーザ認証を行う。正しいユーザであれば、初期チケットをユーザへ返す。
（2）ＴＸ／ＡＴＰＳへのアクセス要求を初期チケットと共に認証サーバへ送り、正しいアクセス要求であればサービスチケットをユーザへ返す。
（3）チケットとログイン要求をＴＸ／ＡＴＰＳへ送付し、ＴＸ／ＡＴＰＳはチケットを確認する。確認できたら、ログイン許可をユーザへ返す。
（4）トランザクションを投入しその応答メッセージを受信する。

上記の全プロトコルをすべて暗号化する。暗号化に使用される暗号化方式は公開鍵暗号化方式によるディジタル署名を付けた相互認証暗号化と慣用鍵暗号化を組み合わせた独自の暗号化方式を採用している。

4．実現手法

２章で示した設計目標の内、トランザクション実行性能に関係する暗号化方式に付いて実現手法を述べる。

暗号化方式として、一般に公開鍵暗号化方式と慣用鍵暗号化方式がある。以下に、その特徴を述べる。

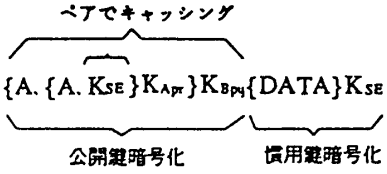
・慣用鍵暗号化方式：システム中の鍵の数が多く
　鍵管理に難点があるが暗号化性能が良い。
・公開鍵暗号化方式：システム中の鍵の数が少なく
　鍵管理が容易であるが暗号化性能が悪い。

運用面として鍵管理方式が容易でなおかつ性能の良い暗号化方式とするため、新しい暗号化方式を採用した。この暗号化方式について以下に述べる。

基本方針として、簡易な運用とするため、鍵管理としては公開鍵管理方式を採用し、実際のデータ暗号化としては慣用鍵暗号化方式を採用することとした。

この暗号化方式を以下図２を用いて説明する。

この例では、ユーザAがユーザBにDATAを送る場合のユーザAの暗号方法を示している。



慣用鍵暗号化用鍵
K_{SE}：慣用鍵(ランダム作成)
公開鍵暗号化用鍵
K_{Apr}：ユーザAの秘密鍵
K_{Apu}：ユーザAの公開鍵
K_{Bpr}：ユーザBの秘密鍵
K_{Bpu}：ユーザBの公開鍵

図2：暗号化方式

（１）ユーザデータの暗号化の為、K_{SE}（慣用鍵）をランダム作成する。DATA（ユーザデータ）をK_{SE}で慣用鍵暗号化方式で暗号化する。次に、K_{SE}をディジタル署名を付けて公開鍵暗号化方式で暗号化する。最後に２つの暗号化データを一緒にし送信データとする。

この方式は以下の２つの利点を持つ。

・サイズが不明なユーザデータを性能の良い慣用鍵暗号化方式で暗号化できる。
・鍵管理方式として管理が容易な公開鍵管理方式を採用出来る。

この暗号化方式でトランザクション実行性能を測定した結果未だ満足のいくものでは無かったためさらに以下の工夫を加えた。

（２）OLTPシステムでの使用を考えた場合、ｸﾗｲｱﾝﾄは

①ログイン
②数回のトランザクション実行
③ログアウト

を繰り返すのが一般的である。暗号を解読する為の慣用鍵の解析に必要とされる時間に対して、上記ｾｯｼｮﾝは十分短い時間であり上記ｾｯｼｮﾝ中で同一の慣用鍵を使用しても安全性・機密性を損なうことはないと考えられる。そこで、ユーザデータを暗号化する慣用鍵は上記の１ｾｯｼｮﾝ内で同一のものを使用し、送信相手（受信の場合は送信者）をキーとして慣用鍵と公開鍵暗号化の部分のデータをｷｬｯｼｭし再利用できるようにした。

この暗号化方式ではログインまでの間に公開鍵暗号化部分はｷｬｯｼｭ上にのるので、トランザクション実行時には慣用鍵暗号化による暗号化時間のみが暗号化に掛かる時間となる。

上記２点の工夫により、OLTP指向の認証サービスとして満足のいく暗号化性能を実現した。

図３に、この暗号化方式でのトランザクション実行性能を示す。暗号化をしない場合に比べ、２割程度の性能劣化に押さえた。

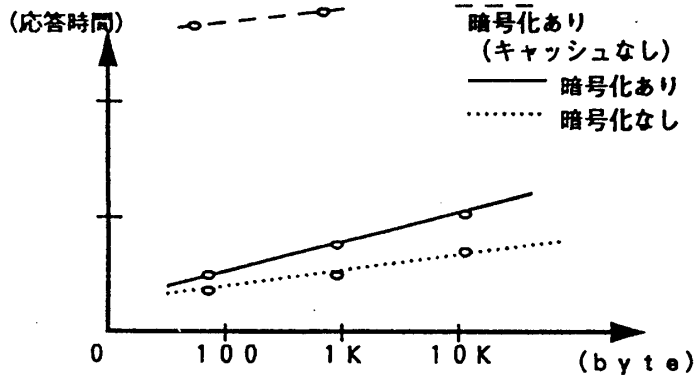


図３　トランザクション実行性能

５．まとめ

分散システムでの認証サービスとしてDCEのｋｅｒｂｅｒｏｓが上げられるが、米国国防省の輸出規制の為アプリケーションデータの暗号化が出来ない等の問題がある。また、OLTPシステムに組み込んだ形での認証システムの提供は殆ど行われておらず、OLTPシステムから認証サービスを使用するのは難しい。

この点に着目し、OLTPシステムへ組み込んだ形での認証サービスを開発した。OLTPシステムと連動した運用、アプリケーション構築性の良さ（上位互換Ｉ／Ｆ）、実用に耐えうるトランザクション性能を実現した。

参考文献
[1]佐波　他：分散環境におけるユーザ認証システム
　情報処理学会第４３回全国大会(1991)

＊ UNIXは、X/Openｶﾝﾊﾟﾆｰﾘﾐﾃｯﾄﾞがﾗｲｾﾝｽしている米国ならびに他の国における登録商標です。