マルチメディア通信と分散処理　94－5
分散システム／インターネット運用技術　14－5
（1999．7．15）

電子流通実装基盤 SPAgent

梶浦 正浩† 後藤 哲也† 高橋 俊成‡ 秋山 浩一郎‡
† (株) 東芝 研究開発センター ヒューマンインターフェースラボラトリー
‡ (株) 東芝 研究開発センター コンピュータ・ネットワークラボラトリー

デジタルコンテンツやサービスの提供を透過に行う流通システム実装のための基盤モジュールSPAgentの設計・開発を行った。SPAgentは、ユーザ認証・クライアント情報開示・既存のサーバ／クライアントの機能拡張、などに伴う安全性などの問題点を回避し、ユーザやサービス提供者に対して、サービスプログラムのパッケージ化や統一的な入会／ログイン手段などを提供する。また、SPAgentはHTTPサーバやWWWブラウザから独立したモジュールによって構成されるため拡張性が高く、新規技術の導入や他の形態のサーバ・クライアントシステムへの移植、普及が予測される各種個人認証ハードウェアとの結合なども容易になる。

SPAgent— A Security Module Adaptable for EC Systems

M. Kajiura†, T. Goto†, T. Takahashi‡ and K. Akiyama‡
† Human Interface Laboratory, R & D Center, Toshiba Corp.
‡ Computer & Network Systems Laboratory, R & D Center, Toshiba Corp.

We have developed a basic module SPAgent which is suitable for implementation of digital contents/service distribution systems. SPAgent avoids many kinds of delicate problems derived from user authentication, controlling the client's privacy level, and adapting to ever-changing WWW server/client systems. And it provides common methods to execute service programs, unified ways of logging into access-controlled services, and other security features indispensable to EC systems. The module is highly extendable because its implementation is independent of HTTP servers and WWW browsers, and so it easily enables EC systems to make use of new technology, to adapt to other kinds of server/client systems, and to connect with new authentication hardware coming into wide use.

1　はじめに

昨今のインターネットの普及により、様々なデジタルコンテンツや情報サービスをユーザに提供するWWWサイトが増えている。また、HTMLに加えJavaなどブラウザが理解可能な記述言語や、CGIの他にASPなどサーバ上で動的にHTMLコンテンツを生成する環境など多彩になり、ユーザは高度で複雑なサービスを享受できるようになってきた。

しかし、このような発展した状況下においても、以下のようないくつかの問題点や改良点が考えられる。

(a) ユーザ認証面における問題点

WWWサイトの中には、有料無料を問わず、会員IDとパスワードによるユーザ管理をしているものが多い。これは、ユーザから使用料を徴収したり、ユーザ毎に異なるきめ細やかなサービスを提供したりするために利用される。

しかし、現状はユーザおよびサービス開発者に対して以下のデメリットを強いている状況である。

- ユーザは、サービス毎に異なるログインIDやパスワードを覚えなければならない。また、その取得方法、ログイン方法もサービス毎に異なっている。

- ユーザ認証と一口にいっても、サーバ毎に異なった作り込みをしており認証部の再利用が困難である。
- 同様にサーバ毎にユーザ認証部が異なるので、ユーザ認証後のサービス提供プログラムの再利用が困難である。

(b) ユーザ情報/クライアント PC 情報開示に関する改良点

ユーザ側（クライアント）の情報が適度に開示されることによって、サービスサイトはユーザに対してさらに決め細やかなサービスを提供することが可能となる。たとえば、クライアント PC 内部の状況に応じて提供するコンテンツを適切なものにカスタマイズして送り出したり、問題の生じている個所を修復するなど、従来の WWW ではなかったサービスを提供することができる。

このためには、セキュリティ上何等かの手段によってクライアントの情報開示に制限を設けなければならない。

(c) サーバ／クライアント機能拡張面における問題点

現在、HTTP サーバ／ WWW ブラウザの多くはそのソースが非公開であり、また、頻繁に更新されるそれらに追随して、HTTP サーバやブラウザの機能の独自の拡張を行っていくのは困難を伴う。

そこで、サーバやブラウザに手を加えることなく、(上記のユーザ認証や情報開示の問題点や改良点を含む) 機能拡張をするための何等かの手法が求まれる。

そこで、われわれは、上記の問題点や改良点をカバーしたシステムとして SPAgent(Service Providing Agent) を開発した。

SPAgent は、デジタルコンテンツやサービスをユーザにネットワークを経由して提供する HTTP サーバ — ブラウザシステムにおいて、

- 既存の HTTP サーバやブラウザ自体やブラウジングの操作性を変更することなく、それらが提供する機能の拡張が容易であり、また HTTP サーバやブラウザのバージョンの更新に左右されない汎用的なプラットフォーム
- サービスへの入会手続きとサービス提供プログラムを分離／モジュール化することによって、サービスのパッケージ化を可能にし、サービス提供プログラムの流通を促進する
- サーバ／クライアント認証／サービス単位の認証機能による一定の安全性の保証の下で、クライアント PC 上の情報の開示/非開示のきめ細かな制御を可能とし、ユーザに対してより高機能なサービスの提供を可能にする
- 既存の、もしくは将来出現するであろう様々な EC システム/本人認証システムとの連係・接続が可能な構造

などの特徴を持つ、デジタルコンテンツ・サービスの流通システムを実装するための基盤となるコアシステムである。

以下、本論文ではこの SPAgent についての詳細を述べる。

2 SPAgent の基本設計

2.1 問題解決方法の選択

ここでは、SPAgent の設計にあたって、前節で述べたいくつかの問題点の解決方法を考察する。

2.1.1 ユーザ認証

来訪するユーザを特定する手段とその長短としては主に以下が考えられる。

ユーザ ID +パスワード

比較的実装が容易で、おそらくこれが最も使用されている方法であろうと思われる。次の Cookie に比べ安全性が高いが、サーバ毎に実装や使用方法などが異なる点でユーザに負担をかけている。

Cookie

主なブラウザには HTTP サーバから送られてくる Cookie を保存する機能を持ち、再訪してきたユーザのブラウザに格納されている Cookie を取得することによって、ユーザの特定が可能となる。この実装は比較的容易である。

しかし、Cookie はブラウザの設定や種類によっては保存できないのでユーザの特定ができない場合が生じる、Cookie を不正にコピーする

ことによって悪意のユーザになりすましをされることがある、などの問題がある。

個人証明書

主なブラウザには、信頼のおける第三者機関が発行する公開鍵を含む個人証明書を登録する機能がある。この機能によりサーバ側／クライアント側（ユーザ側）が信頼する第三者機関がそのユーザ個人を保証することによって、サーバ側がアクセスしてきたユーザを特定することが可能となる。

この方法の欠点は、ユーザの情報が過剰にサーバ側に通知されてしまう可能性があるということであろう。通常物品の購入において自分の氏名やアドレスを告げないように、ネット上でのサービス利用においてもその匿名性を必要とすることは多い。

SPAgentでは、匿名性/安全性に優れるユーザID+パスワード方式を選択し、ユーザに負担のかからない統一的な使用方法を提供する形態とする。

2.1.2 ユーザ情報/クライアントPC情報の開示

ユーザの使用しているPC内部の状態に応じてさらにきめ細やかなサービスを提供したい、もしくは、信頼したサーバのサービスには自分のPC内部の情報を公開してより良いサービスを享受したい、という場合がある。しかし、PC内部の情報を公開する場合、内容が傍受されたり、サーバがなりすまされたりされると問題である。

また、サーバのなりすましや通信の傍受が解決されたとしても、1つのサーバが提供するサービスによって、クライアントPC内部の情報の公開／非公開をコントロールしたい場合がある。

これらを解決するため、

- サーバに対して信頼のおける第三者機関の証明書の発行し、公開鍵暗号系によるサーバ認証／通信秘匿の機構
- サーバが現在クライアントに対して提供しているサービス名の通知機構（1つのサーバには提供内容の異なる独立したサービスが複数存在して良い）

を用いる。

同様のWWWブラウザ上で動作するクライアント情報開示の機構としては、現在P3P (Platform for Privacy Preferences)[3]がW3Cにて検討されている。ただし、後述の機能拡張の節とも関係するが、P3Pの認証機構はユーザエージェントであるWWWブラウザと一体になっているのに対して、SPAgentは既存のブラウザやサーバと分離し、他のサーバクライアントシステムへの移植性を向上する形態とする。

2.1.3 機能拡張

HTTPサーバやWWWブラウザのソースは大半がそのソースプログラムが非公開であり、何等かの独自の機能拡張を行う場合の障害となる。また、頻繁にバージョンが変わった場合の対応もコストがかかる。

そこで、容易な（上記のユーザIDと情報の開示の2点も含む）機能拡張のための形態として、SPAgentはサーバやブラウザからは独立したモジュール構成とする。これにより、機能拡張性や他のサーバ／クライアントシステムへの移植性の向上を実現する。

2.2 運用形態

図1にSPAgentおよびその周辺を含んだ運用形態を示す。

通常のWWW利用形態は、図1の上部の破線で結合された三者から成る。サービス利用者はWWWブラウザによってHTTPサーバと接続し、HTTPサーバはサービス利用者の要求によって適宜CGIプログラムを実行し、その結果をHTTPサーバを通じて利用者のWWWブラウザに送り返す。

これに対し、SPAgentを用いた基本的な運用形態は図2の実線で示したものであり、

- サービス利用側のPCクライアントにはWWWブラウザの他にSPAproxyが動作し、適宜SPAfilterがSPAproxyにより起動される
- サービス提供側のHTTPサーバのCGIプログラムの一つとしてSPAserverが存在し、ユーザからの要求にしたがってサービスプログラム(SVP)を起動する

である。

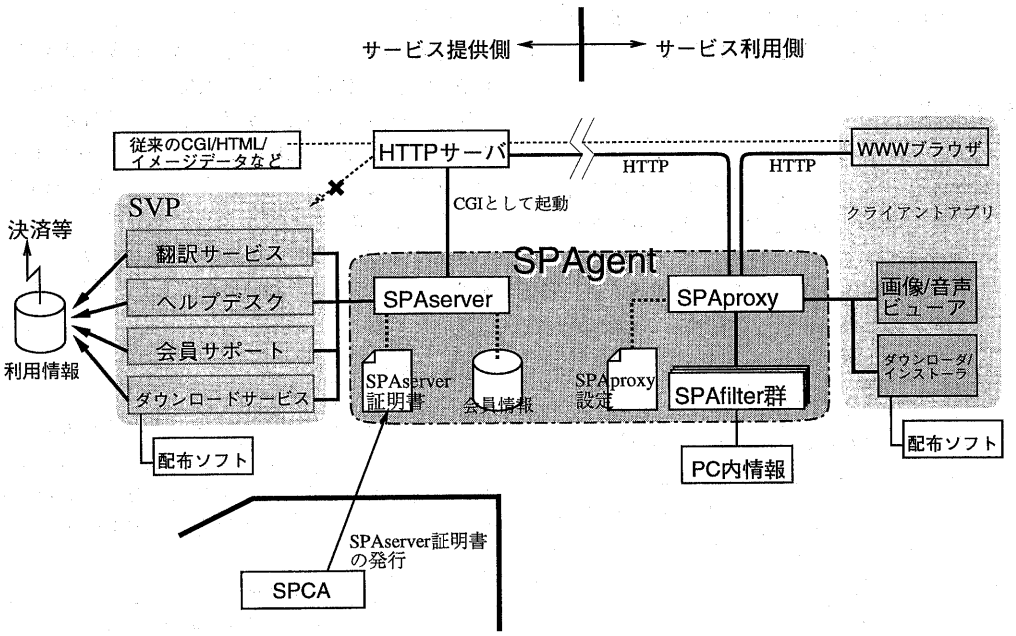

図 1: SPAgent の運用形態

以下に各部の動作や他部との関連について述べる。

2.2.1 SPAproxy

SPAproxy はブラウザ（もしくはダウンローダなどのプログラム）からの POST データを受けとり、（その内容に SPAfilter を起動する指示があれば適宜起動してから） POST データを圧縮・暗号化して HTTP サーバに送る。

また、SPAproxy は、HTTP サーバから送り返されてきた SPAserver によって暗号化・圧縮された SVP の出力を復号・伸長し、（その内容に SPAfilter を起動する指示があれば適宜起動してから）ブラウザ（もしくはダウンローダなどのプログラム）に送る。なお、ブラウザ等にデータを送らずに、再度 HTTP サーバにデータを送り、複数回連続して SPAserver とセッションを結ぶことができ、SPAfilter の実行結果をブラウザを介すことなく SPAserver に送ることが可能である。

2.2.2 SPAfilter

SPAfilter は、WWW ブラウザなどの クライアントアプリから、もしくは SPAserver から送られてきたデータ中に含まれている特定の命令によって起動され、SPAproxy を通過する HTTP データを加工する一種のフィルタコマンドである。

SPAfilter は、それぞれの機能に応じて受けとったデータを加工するだけでなく、PC 内の情報の取得やファイルへの読み書きなどを行う。このため、ユーザのデータの漏洩や改竄を防ぐため、SPAserver 証明書によってサーバを認証し、さらに SVP ごとに SPAfilter の動作を制御するユーザの設定（制御ファイル）にしたがって、SPAfilter を起動する（もしくは起動しない）ようになっており、図 2 はその設定画面を示している。

2.2.3 SPAserver

SPAserver は主に以下の動作を行う。

1. SPAproxy から送られてきた要求データを認証し、会員 SPAproxy からのデータであれば、復号・伸長後、内容に応じて SVP を起動し、結果を（圧縮・暗号化した後）HTTP サーバを経由して SPAproxy に送り返す。
2. SPAproxy から送られてきた要求データが非会員 SPAproxy からのデータであれば、入会モードに移り、その SPAproxy に対して、 SPAproxyID

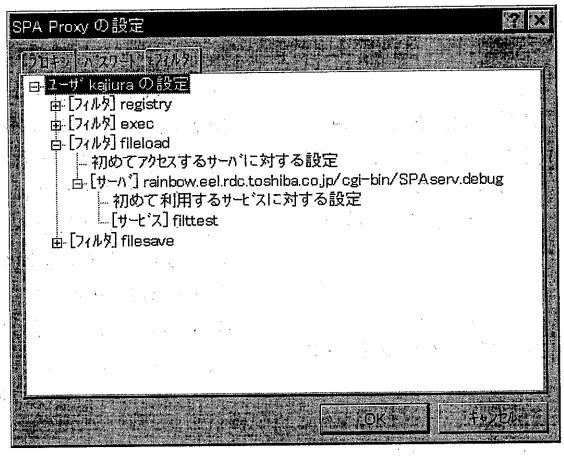

図 2: SPAfilter のアクセス制御

の発番・共有鍵乱数[1]の交換を行う。

2.2.4 SVP（サービスプログラム）

SVP はユーザに提供するサービスのための、プログラムおよび固定のデータ（HTML/イメージなど）の集合体である。SVP のプログラムの構造は基本的に一般的な CGI と同じであるが、SVP は SPAserver が正しい SPAproxy からのアクセスか否かの認証を既に行った後に起動されるので、従来の CGI プログラムが行っているような認証を行わなずに、サービスに特化した機能のみを実装すれば良いようになっている。

2.2.5 クライアントアプリ

SPAproxy にデータを POST し、また、SVP の実行結果を SPAproxy から受けとるクライアントマシン上でのソフトウェア全てを、クライアントアプリと呼ぶ。WWW ブラウザを含む。

2.2.6 SPCA, SPAserver 証明書

SPCA（SPAgent Certificate Authority）は SPAserver 証明書の発行局である。

SPAserver 証明書は、SPAserver の URL, 名称, 連絡先など、SPAserver を特定するに必要な情報およびセッション鍵の暗号化に用いられる公開鍵が含まれており、SPCA は自らの秘密鍵を用いて SPAserver 証明書に署名を行い、各 SPAserver に発行する。この SPCA の署名用の公開鍵は SPAproxy に埋め込まれており、SPAserver が送ってきた SPAserver 証明書が SPCA に正しく署名されたものかを判別することができる。

3 応用例

以下に、SPAgent を用いた応用例についていくつか述べる。

PC 診断・修復ヘルプデスク

PC 診断・修復ヘルプデスクは、何等かの障害が生じた PC の内部状態を調べ、必要ならば修復を行うサービスである。

このサービスでは PC の内部状態の開示が必要なので、SPAproxy のアクセス制御機能によってユーザが信頼したサーバ上のヘルプデスクサービスに対してのみアクセス許可を出すことにより、サービスを受けることができる。

[1]SPAproxy との通信内容を暗号化する鍵に利用されるデータで SPAproxy と SPAserver で同じ内容が保存される。通信内容を復号することが可能か否かで正規の SPAserver, SPAproxy かの判断を行う。

ソフトウェア/コンテンツのコピープロテクト

SPAproxy は PC 固有の情報を元に SPAserver から送られてきたデータに変更を加えることが可能である。この機能を用いて、ソフトウェアのコピープロテクト（他のクライアントＰＣで動作させない）をかけることができる。

ソフトウェアのダウンロード／インストール

SPAgent は PC 内部の情報を（ユーザが開示するよう設定すれば）参照することが可能なので、PC の現在の状況に応じて必要なファイルだけをダウンロード／インストールするようなサービスを提供することが可能となる。

同様に、イントラネット内の全ての PC を同じ環境に設定するなど、PC 管理システムを構築することが可能である。

4 今後の課題

SPAgent は、デジタルコンテンツ・サービスの流通システムを実装するための基盤となるコアシステムであるので、SPAgent の有効性を示し得るだけのアプリケーションの開発も必要であるが、コアシステムとしての SPAgent 自体の拡張も必要であると考える。

今後の SPAgent の発展の方向としては、以下が考えられる。

1. 本論文での SPAgent は HTTP サーバ- WWW ブラウザシステムをターゲットとしているが、SPAgent は既存の HTTP サーバや WWW ブラウザを全く変更せずに運用可能な独立性の高いシステムである。よって HTTP サーバ- WWW ブラウザではないサーバクライアントシステムにも応用可能である。PHS や PDA などのモバイルシステムなどを利用したサービスシステムにも僅かな修正で適用できる。
2. SPAgent のクライアント側の重要な情報は SPAproxyID と共有乱数の組合せであり、これが他人に洩れるのは避けなければならない。現在の SPAgent では、この SPAproxy 設定ファイルをパスワードによって保護しているが、このファイルを、既存もしくは将来出現するであろう個人認証ハードウェアなどによって保護することによって、より安全性が増すであろう。これは、様々な HTTP サーバや WWW ブラウザに何等手を加えることなく、個人認証ハードウェアを使ったサービスシステムを構築することが可能であることを示している。
3. 1 台の PC 上に搭載されている SPAproxy の SPAproxyID は、アクセスする SPAserver 毎に異なっている。これは、Pentium III のシリアル番号とは異なり、プライバシー保護の面からいっても有利であろうと思われる。つまり、ある SPAserver 上の利用状況が公にされてしまっても、他の SPAserver では公開された SPAproxyID は意味がないからである。この特徴（一種の匿名性）とクライアントの固有 ID（SPAproxyID）を利用すれば、ソフトウェアや画像などのデジタルコンテンツの個人向けライセンスの流通が促進されるのではないかと思われる。

今後は、SPAgent の有効性を示す良いアプリケーションとして PC 障害復旧 SVP の開発 [2]、SPAgent 自体の拡張として個人認証ハードウェアや決済システムとの融合を進めていく必要があるだろう。

参考文献

[1] 高橋,「ソフトウエアの電子流通システム ソフトパーク」金融情報システム, No. 189, 平成 9 年 7 月号.

[2] 半田他,「PC の障害の診断・修復機能を持つヘルプデスクシステム」インタラクション'99, pp. 137–138, 1999.

[3] http://www.w3.org/P3P