社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30（42）
2005／7／22

セキュアサービスプラットフォームにおけるセキュア通信の状態検知

高田 治　澤井 裕子　星野 和義　鍛 忠司　竹内 敬亮　藤城 孝宏　手塚 悟

（株）日立製作所 〒212-8567 川崎市幸区鹿島田 890
E-mail: takata@sdl.hitachi.co.jp

あらまし　セキュアサービスプラットフォーム（SSP）は、セキュア通信を仲介する基盤である。SSP を利用したセキュア通信においては、まず、通信をおこなう２つの通信端末は、通信のネゴシエーション処理を SSP を介して行う。次に、通信を行う２つの通信端末が SSP を介さずにアプリケーションデータの交換を行う。SSP がセキュア通信の開始や終了などの状態を検知するためには、SSP を介したネゴシエーション処理と、アプリケーションデータの交換の両方の情報から、状態を検知する必要がある。本研究では、通信端末が状態を検知し、通信記録を作成し、SSP に通知することにより、SSP がセキュア通信の状態を検知する手法について示す。

キーワード　セキュアサービスプラットフォーム，SSP，セキュア通信，状態検知

A Status Detection of Secure Communication in Secure Service Platform

Osamu TAKATA　Yuko SAWAI　Kazuyoshi HOSHINO　Tadashi KAJI　Keisuke TAKEUCHI
Takahiro FUJISHIRO　and　Satoru TEZUKA

Hitachi, Ltd.　890, Kashimada, Saiwai-ku, Kawasaki, 212-8567 Japan
E-mail: takata@sdl.hitachi.co.jp

Abstract　SSP (Secure Service Platform) is a platform that mediate secure communication. The secure communication using SSP needs two steps. First, the two entities negotiate through SSP. Second the entities exchange encrypted application data without SSP mediation. To detect status (e.g. start and end) of secure communication, SSP must watch both negotiation procedure and the application data exchange. This study shows the architecture of status detection in secure communication with SSP. The entities detect status of secure communication, and make communication log, and transmit the log to the SSP.

Keyword　Secure Service Platform, SSP, Secure Communication, Status Detection

1. はじめに

現在、日本におけるインターネット通信インフラは急速にその整備が進んでおり、また、そのユーザ数も DSL のサービス加入者数が 1300 万回線、FTTH が 240 万回線を越える（2005 年 1 月現在）など、急速に増加している。しかし、一方で、これらの通信インフラの整備とユーザの急増は、ネットショッピングやネットバンキングに絡んだ詐欺行為や不正アクセスなど、新たな社会問題を生み出している。

このような問題に対して、通信に対する安全性を高める技術が開発されている。例えば、通信の機密性・完全性を高めるための代表的なセキュア通信プロトコルとして、SSL や TLS[1]がインターネット上で一般的に広く利用されている。また、企業の拠点間を結ぶネットワークにおいて、IPsec[2]が多く利用されている。

我々の研究グループでは，安全な End-to-end 通信の確立をネットワーク側が代行するネットワーク基盤の研究を行っている[3]~[11]。（このネットワーク基盤を我々は，セキュアサービスプラットフォーム（SSP）と呼んでいる。）

本稿では、SSP におけるセキュア通信の通信状態の検知方式について検討を行う。まず２章で SSP の概要を説明する。次に、３章で今回検討した通信状態検知方式の概略を示し、４章でその詳細について説明する。

2. セキュアサービスプラットフォーム（SSP）

2.1. SSP の概要

SSP は、ユーザとサービス提供者との安全な通信のため、双方から信頼される第３者として、両者の認証や、両者間のセキュア通信の仲介・アクセスポリシーの管理・権限の管理、セキュア通信のためのネットワーク設定を行う。

2.2. SSP の構成

図１は、SSP の機能の中の一部である認証とセキュア通信の仲介、に着目したシステム構成を示している。

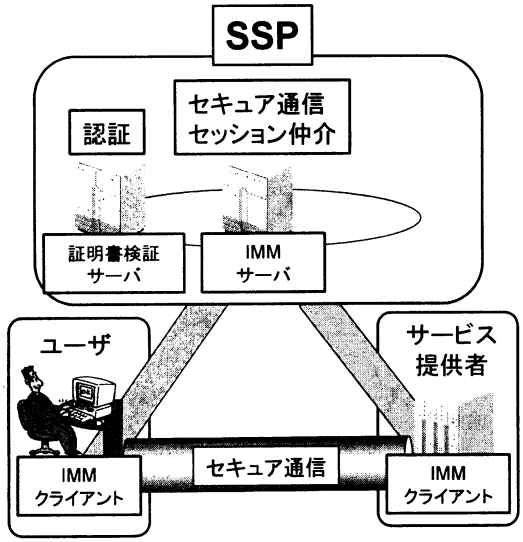

図1　システム構成図

SSP には、ユーザからサービス提供者へのセキュア通信の確立を仲介する IMM（IP address Management and authentication Mediator）サーバと、ユーザとサービス提供者を PKI を用いて厳密に認証するための証明書検証サーバとがあり、ユーザとサービス提供者には IMM クライアントが導入される。なお、ユーザとサービス提供者の IP アドレスを管理し、また、認証の仲介を証明書検証サーバと連携して行う（IP address Management and authentication Mediator）サーバを略し以下 IMM サーバと呼ぶ。

2.3. SSP のシステム動作概要

図 1 におけるユーザがサービス提供者との間で通信を開始・終了する手順を示す。

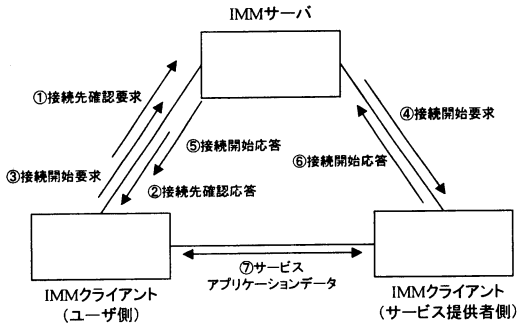

図2　通信開始処理手順

表1　通信開始処理の概要

メッセージ	概　要
①接続先確認要求	ユーザ側 IMM クライアントが、サービス提供者の IP アドレスを IMM サーバへ送信し、サービス提供者側 IMM クライアントの名前を問い合わせる。
②接続先確認応答	IMM サーバが IMM クライアントから問い合せを受けた IP アドレスに対応する名前を応答する。
③接続開始要求	ユーザ側 IMM クライアントとサービス提供者側 IMM クライアントとの間の通信開始要求を、①②で取得した名前を利用して、IMM サーバに送信する。
④接続開始要求	IMM サーバは、受信した接続開始要求を、サービス提供者側 IMM クライアントに転送する。
⑤接続開始応答	サービス提供者側 IMM クライアントは、接続開始要求を受信すると、その応答を IMM サーバに応答する。
⑥接続開始応答	IMM サーバは、受信した接続開始応答を、ユーザ側 IMM クライアントへ転送する。
⑦サービスアプリケーションデータ	HTTP リクエスト/レスポンスや、ストリーミングデータなど、サービス提供者がユーザに提供するアプリケーションデータを交換する。

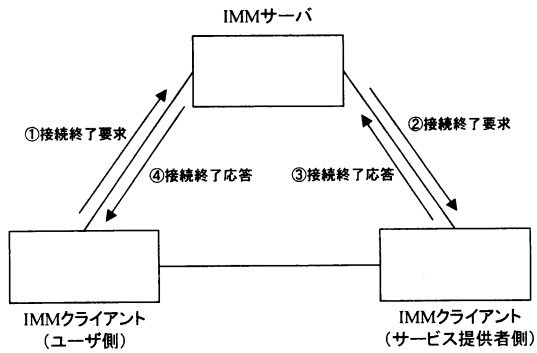

図3　通信終了処理手順

表2　通信終了処理の概要

メッセージ	概　要
①接続終了要求	ユーザ側 IMM クライアントとサービス提供者側 IMM クライアントのサービスアプリケーションデータの交換が終わると、ユーザ側 IMM クライアントは、接続終了要求を IMM サーバに送信する。
②接続終了要求	IMM サーバは、受信した接続終了要求をサービス提供者側 IMM クライアントへ転送する。

③接続終了応答	サービス提供者側 IMM クライアントは、接続終了要求を受信すると、IMM サーバへ接続終了応答を送信する。
④接続終了応答	IMM サーバは、受信した接続終了応答をユーザ側 IMM クライアントへ転送する。

3. セッションの状態検知の概要

3.1. 状態検知の目的とシステム要件

SSP では、通信の開始と終了時に、接続開始要求、や接続終了要求の処理が行われる。これらの処理に対応して、セキュア通信チャネル（図1参照）で通信が行われていることを保証するためには、セッション状態を管理するシステムが、ユーザとサービス提供者の間の通信セッションの開始、終了を正確に検知する必要がある。

3.2. セッション状態検知のモデル

本システムでは、ユーザやサービス提供者が作成した、ユーザとサービス提供者間の通信の記録を、通信記録管理システムで管理するモデルを採用する。

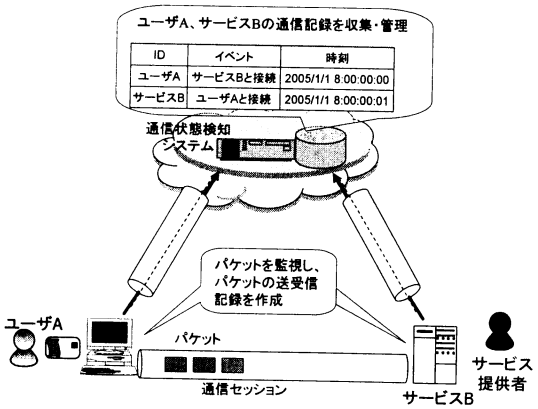

図4　セッション状態検知のモデル

IMM サーバは、図2、図3に示すように、IMM クライアント間の通信の開始と終了処理を仲介するため、開始と終了のイベントを検知することができる。しかしながら、IMM サーバは、通信の開始処理に伴って、ユーザとサービス提供者間の通信セッションのパケット交換が開始されることや、通信の終了処理が行われると、パケット交換が終了することを検知できない。また、IMM クライアント間で交換される通信量の情報を取得できない。そこで、図4に示す状態検知モデルでは、ユーザとサービス提供者が、通信セッションを確立している間、通信セッションの状態を検知することで、通信セッションの開始・終了時刻の情報を取得する。また、通信の開始から終了までに送受信したパケット量の情報を取得する。ユーザとサービスは、それぞれ取得した開始・終了時刻、通信量の情報を、通信状態検知システムに送り、通信状態検知システムは、それらの通信記録をデータベースに保管する。

3.3. 通信セッション状態の種類

まず、対象となる通信セッションの状態、すなわちユーザ側 IMM クライアントと、サービス提供者側 IMM クライアント間の通信セッションの状態を挙げ、それぞれ以下のように呼ぶこととする。

表3　通信セッションの状態（通信開始時）

通信セッションの状態	処理状態
接続処理中	以下の一連の処理の途中 1. 接続先確認要求 2. 接続先確認応答 3. 接続開始要求 4. 接続開始応答
接続中	上記の接続処理 1～4 の処理が正常に終了 かつ ユーザ側 IMM クライアントと、サービス提供者側 IMM クライアント間でパケットの交換中

表4　通信セッションの状態（通信終了時）

通信セッションの状態	処理状態
接続終了処理中	以下の処理の途中 1. 接続終了要求 2. 接続終了応答
接続終了－1	上記　1．接続終了要求と2．接続終了応答の処理が正常に終了し かつ ユーザ側 IMM クライアントとサービス提供者側 IMM クライアントのパケット交換なし
接続終了－2	上記　1．接続終了要求と2．接続終了応答の処理は行われていない、かつ、 ユーザ側 IMM クライアントとサービス提供者側 IMM クライアントのパケット交換がなくなり、一定時間が経過。

また、表3、表4の状態に該当しない状態として以下がある。

表5　通信セッションの状態（異常状態）

通信セッションの状態	処理状態
異常接続中	表1に示す通信開始処理が行われていないにもかかわらず、 ユーザ側 IMM クライアントと、サービス提供者側 IMM クライアント間でパケットを交換

接続終了異常	表２に示す通信終了処理が完了したが、ユーザ側 IMM クライアントとサービス提供者側 IMM クライアントのパケット交換が継続

4. 状態検知システム

4.1. 通信セッション状態検知システムの構成

3.3 で示した通信セッションの状態を検知し、ログ管理サーバで検知した状態のログを管理するために、図５に示すシステムの構成をとる。

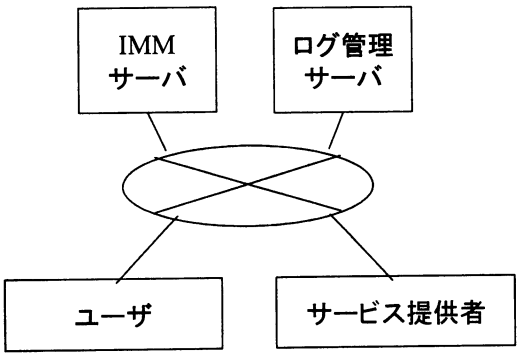

図５　セッション状態検知システムの構成

図５では、セッション状態の検知システムの構成を示している。このシステムでは、ユーザとサービス提供者が暗号化通信を行う場合に、その通信記録を、ログ管理サーバが管理する。

4.2. 状態検知の処理フロー

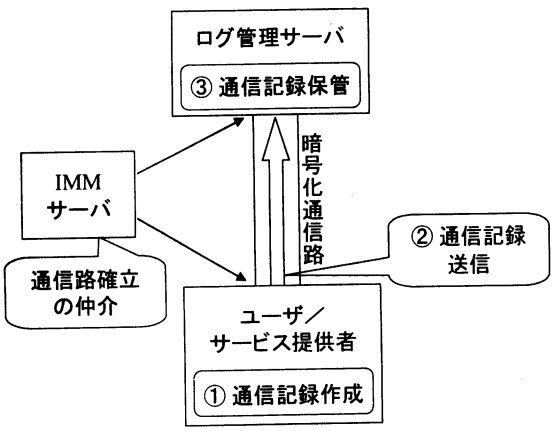

図６　通信記録通知の手順

通信記録の通知は、図６に示される手順で行われる。

①　通信記録作成

ユーザやサービス提供者は、通信状態検知機能により通信状態を検知し、ユーザーサービス提供者間の通信記録を作成する。

②　通信記録送信

ユーザやサービス提供者は、通信記録のログ管理サーバ通知機能により、作成した通信記録をログ管理サーバに送信する。その際、IMM サーバを仲介して確立された暗号化通信路を使う。

③　通信記録保管

ログ管理サーバは、ユーザあるいはサービス提供者から受信した通信記録をログ管理サーバ内の通信対応表と、通信記録表に保管する。

これらのステップのシーケンスを図７に示す。

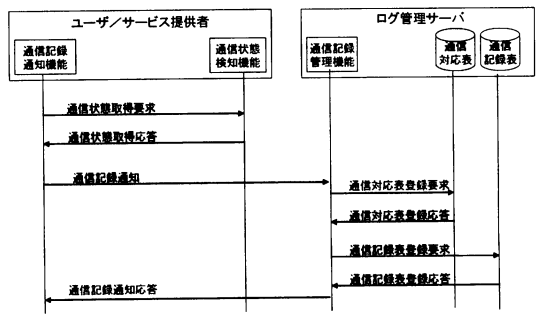

図７　通信記録通知シーケンス

次に、①通信記録作成、②通信記録送信、③通信記録保管について、その詳細を示す。

4.3. 通信記録作成

ユーザ／サービス提供者は、以下の２つの処理の結果をもとに、通信セッションの状態を検知する。

・通信開始・終了要求メッセージの送受信

ユーザは、ユーザーサービス提供者間の通信開始時に IMM サーバを介してサービス提供者に通信開始要求を送り、その応答を受け取る。

また、ユーザは、ユーザーサービス提供者間の通信が終了すると、IMM サーバを介して通信終了要求をサービス提供者に送り、その応答を受け取る。

・パケット監視

ユーザ側 IMM クライアントとサービス提供者側 IMM クライアントは、それぞれ交換するパケットを監視する。

これらの検知結果を元に、通信記録を作成する。通信記録には、通信状態の変化を記録するイベント記録（表６）と、通信量を記録する通信量記録（表７）がある。

表６　イベント記録の例

イベント名	通信開始
時刻	2005/02/01 10:10:30.130

通信元 IP アドレス	10.202,142.10
通信元 ポート番号	1234
通信先 IP アドレス	10.202,142.20
通信先 ポート番号	1234

イベントの種類の一覧を表７に示す。ユーザ／サービス提供者は、通信セッションの状態（表３、表４、表５）の変化を検出し、表７に示すようなイベントに対して、表６に示すような通信記録を作成する。

表７　イベントの種類

イベント名	通信セッション状態の変化
通信開始	接続処理中→接続
通信終了１	接続中→接続終了処理中→接続終了－１
通信終了２	接続中→接続終了－２
異常接続	任意の状態→異常接続
通信異常終了	接続中→接続終了処理中→接続終了異常

また、ユーザ／サービス提供者は、ユーザとサービス提供者間で交換されるパケットを監視することで、セッションの通信量を検出する。

表８では、あるセッション（通信元 IP アドレス・ポート番号と通信先 IP アドレス・ポート番号の対で特定）において、指定した期間に交換したパケット数とバイト数の情報が記載された通信記録の例を示している。

表８　通信量記録の例

記録開始時刻	2005/02/01 10:10:34.130
記録終了時刻	2005/02/01 10:11:34.130
通信元 IP アドレス	10.202,142.10
通信元 ポート番号	1234
通信先 IP アドレス	10.202,142.20
通信先 ポート番号	1234
パケット数	1000
バイト数	600K

このように、ユーザ、サービス提供者それぞれは、イベント記録と、通信量の記録の、２種類の通信記録を作成する。

4.4. 通信記録送信

ユーザ／サービス提供者は、表７に示したイベントが発生したことを検知すると、イベント記録を管理サーバに送信する。また、通信量記録を一定の間隔で、定期的にログ管理サーバに送信する。したがって、ログ管理サーバでは、ユーザとサービス提供者の間の通信セッションの開始、終了をリアルタイムに検知できる。ユーザ／サービス提供者は通信記録を送信した後、送信済みの通信記録をユーザのデータ保管領域から削除する。

通信記録は、ユーザあるいはサービス提供者の通信履歴情報であり、第三者による盗聴、改ざんから保護する必要がある。本通信状態検知システムでは、ユーザ／サービス提供者は、図６に示すように、ログ管理サーバとの間で、IMM サーバを介した暗号化通信セッションを確立することにより、通信記録を保護する。

4.5. 通信記録保管

ログ管理サーバは、ユーザやサービス提供者から受信した通信記録を、通信対応表と通信記録表で管理する。なお、ログ管理サーバは、ユーザとサービス提供者間の一つのセッションに対して、ユーザとサービス提供者双方から通信記録を受信し、記録する。

表９　通信対応表の例

通信番号	通信元		通信先	
	IP アドレス	ポート番号	IP アドレス	ポート番号
1	10.202.142.10	1234	10.202.142.20	1234
2	10.202.142.20	1234	10.202.142.10	1234
3	10.202.142.10	1234	10.22.0.10	1235
:	:	:	:	:

表１０　通信記録表（イベント）の例

通信番号	時刻	イベント
1	2005/02/01 10:10:34.130	通信開始
:	:	:

表１１　通信記録表（通信量）の例

通信番号	記録開始時刻	記録終了時刻	パケット数	バイト数
1	2005/02/01 10:10:34.130	2005/02/01 10:11:34.130	1,000	600K
2	2005/02/01 10:10:30.240	2005/02/01 10:11:30.240	1,005	610K
2	2005/02/01 10:11:30.240	2005/02/01 10:12:30.240	1,500	500K
1	2005/02/01 10:11:34.130	2005/02/01 10:12:34.130	1,495	497K
3	2005/02/01 11:00:04.130	2005/02/01 11:01:04.130	5	3K
:	:	:	:	:

表９と表１０と表１１は、通信対応表と通信記録表の例を示している。これらの表は、データに対するアクセス権限等を適切に設定することにより安全に管理する。通信記録管理機能は、ユーザあるいはサービス提供者から、通信記録を受信すると、通信対応表と通信記録表に情報を追加する。

通信対応表は、表９に示すような、通信元の IP アドレスとポート番号、通信先の IP アドレスとポート番号の組を管理しており、それぞれのエントリ（通信対応表の行）には、一意な番号を割り当てる。

例えば、ユーザが、表６や表８に示すような通信記録をログ管理サーバに送信した場合、ログ管理サーバ

の通信記録管理機能は、表９に示す一番上のエントリを作成し、通信番号を割り当てる。なお、通信管理機能は、エントリを作成する前に作成しようとしているエントリがすでに通信対応表に登録されているかどうかを確認し、登録済みの場合はエントリを作成しない。

例えば、ユーザが、表６や表８に示すような通信記録をログ管理サーバに送信した場合、ログ管理サーバの通信記録管理機能は、通信対応表の通信番号に対応したエントリを通信記録表に追加する。

通信記録表（表１０、表１１）では、一つの通信番号に対して、複数のエントリ（行）が存在しうる。表１１の例では、ユーザ(10.202.142.10)が、1234 番ポートで、サービス提供者(10.202.142.20)の 1234 番ポートと通信を行った場合を示している。この例では、１分間隔で通信記録（通信量）を作成しており、表１１には、通信番号１に対する複数のエントリが記録されている。

5. おわりに

SSP における通信状態の検知、検知結果の保管方法について検討を行った。

通信状態を検知するために、ユーザとサービス提供者が、それぞれユーザーサービス提供者間のセッション状態を検知し、リアルタイムにログ管理サーバに通知することにより、ログ管理サーバが、通信セッションの開始、終了をリアルタイムに検知する方式について検討した。

通信記録を管理する方法として、ユーザやサービス提供自身による分散管理と、ログ管理サーバによる集中管理の２つが考えられるが、ログ管理サーバで一元的に管理すれば、ユーザやサービス提供者自身が通信記録を管理するよりも、より安全に管理できると考えたため、本稿では後者を検討した。

具体的には、SSP で検知結果を管理するために、ユーザやサービス提供者が検知結果から通信記録をそれぞれ作成し、ログ管理サーバに送信し、ログ管理サーバが通信記録を管理する方式について検討した。

なお、本方式では、一つの通信セッションに対して、二つの通信記録が作成される。これらの通信記録の整合性を検証することにより、通信記録の正当性を評価することができるのではないかと考えている。その方式については、今後検討したい。

参考文献

[1] IETF, "The TLS Protocol Version 1.0", RFC2246, January 1999

[2] IETF, "Security Architecture for the Internet Protocol", RFC2401, November 1998

[3] 高田 他, "セキュアサービスプラットフォームにおける認証モデルの一検討", 2005年電子情報通信学会総合大会講演論文集, p170 (2005)

[4] 細木 他, "セキュアサービスプラットフォームでのセキュリティ状態を用いたアクセス制御に関する一検討", 2005年電子情報通信学会総合大会講演論文集, p171 (2005)

[5] 永岡 他, "セキュアサービスプラットフォームにおけるプライバシー保護アクセス制御手法の検討", 2005年電子情報通信学会総合大会講演論文集, p172 (2005)

[6] 近藤 他, "セキュアサービスプラットフォームにおけるサービス利用権限管理の一検討", 2005年電子情報通信学会総合大会講演論文集, p173 (2005)

[7] 渡辺 他, "セキュアサービスプラットフォームにおけるプライバシー保護のためのID管理方式", 2005年電子情報通信学会総合大会講演論文集, p174 (2005)

[8] 新 他, "セキュアサービスプラットフォームのためのクライアントの安全性管理", 2005年電子情報通信学会総合大会講演論文集, p175 (2005)

[9] 鍛 他, "セキュアサービスプラットフォームにおけるセキュア通信確立モデル", 情報処理学会研究報告, 2005-CSEC-28, pp.151-156 (2005)

[10] 小倉 他, "セキュリティ・ネットワーク経路選択方式の提案", 電子情報通信学会技術研究報告, 2005-TM-33, (2005)

[11] 渡辺 他, "セキュアサービスプラットフォームにおけるプライバシー保護を考慮したID生成管理方式の実装", 電子情報通信学会技術研究報告, NS2005-28, pp. 17-20, (2005)

謝辞

本稿は，総務省から委託を受けた「高度ネットワーク認証基盤技術の研究開発　－認証機能を具備するサービスプラットフォーム技術－」に関するものである。関係各位のご協力に感謝する。