検疫結果を保証するセキュリティ保証基盤

磯原隆将[†] 石田千枝[†] 北田夕子[†]
竹森敬祐[††] 笹瀬巌[†]

通信相手の身元を認証する技術として，PKI（Public Key Infrastructure）などがあるが，通信自体の安全性を保証する技術ではなく，信頼すべき通信相手のサーバから，意図せず受け取ったウイルスや攻撃を防ぐことはできない．そこで本論文では，サーバのセキュリティ対策の状況を第三者機関であるセキュリティ保証局が確認して証明書を発行し，クライアント側でその署名を検証するセキュリティ保証基盤モデルを提案する．セキュリティ保証基盤を実現するにあたり，安全性，柔軟性，即時性に関する課題を整理して，通信プロトコルと各種処理モジュールについて提案・設計する．即時性については，本技術の普及のポイントとなるサーバ・クライアント間の証明書の提示処理について実装・評価を行い，十分な高速性を達成できていることを確認する．本基盤技術の達成により，セキュリティ対策機能を持たせ難い小型のユビキタスクライアント端末に対する通信制御などへの適用が期待される．

Security Key Infrastructure to Certificate Security Countermeasures

Takamasa Isohara,[†] Chie Ishida,[†] Yuko Kitada,[†]
Keisuke Takemori[††] and Iwao Sasase[†]

An authentication technology such as Public Key Infrastructure (PKI) is used for a server authentication. However, it does not certificate the security countermeasure of the server. When a client receives malicious packets from such a server, these packets can not be blocked. In this paper, we propose the Security Key Infrastructure (SKI), in which Security Certificate Authority checks a countermeasure of the server and issues a Security Certificate. The client can verify the certificate of the server. We consider the requirements for security, flexibility and feasibility, and we design processing modules and protocols. To consider feasibility, we evaluate the processing speed of certificate induction between the server and the client, and we show that this scheme can satisfy the need for quick response. Our proposed scheme can be applied to the access control in small client that has no security countermeasure in ubiquitous network.

1. はじめに

多くのクライアント端末がインターネットに容易に接続できる環境が整いつつある中，ネットワークを経由したウイルス感染や不正アクセス，なりすましなどの脅威が深刻な問題となっている．このための対策技術として，安全対策や相手認証に関する研究がさかんに行われている．安全対策の技術には，ウイルス感染を防止するためのウイルス検知システム（VDS: Virus Detection System），不正アクセスを防止および監視するためのファイアウォール（FW: FireWall），侵入検知システム（IDS: Intrusion Detection System），これらの安全対策システムの稼働状態やクライアント端末の OS の状態などを検証する検疫ネットワーク（QN: Quarantine Network）などがある．また，相手認証の代表的な技術として，公開鍵基盤（PKI: Public Key Infrastructure）がある[1)~6)]．

しかしながら，ユビキタス社会の発展にともない，こうした安全対策を組み込めない簡易なクライアント端末の普及が進むことが予想される．PKI は社会的に信頼されている認証局が，公開鍵に対応した秘密鍵の正規所有者を保証する技術であり，通信相手であるサーバの安全対策の状態を保証するものではない．もし，通信相手のサーバがセキュリティ対策を施さず，踏み台にされていた場合，その端末を信頼したクライアントが攻撃を受けることもあり，そのときの被害は甚大なものとなる．VDS の中には，検査済みのマーク

† 慶應義塾大学理工学部情報工学科
Department of Information and Computer Science, Keio University
†† 株式会社 KDDI 研究所
KDDI R&D Laboratories Inc.

をメールに付与して送信する製品もあるが，そのマークに対する担保はとられておらず詐称される可能性は否定できない．ネットワークの利用者によっては，安全対策の状態の不明な端末と通信することに抵抗を感じることもあり，自身の検疫結果を正しく通信相手に通知する技術が必要とされている．

そこで本論文では，通信相手であるサーバの安全対策の状態を保証するセキュリティ保証基盤を提案する．サーバがセキュリティ保証を受けることにより，携帯電話や PDA など，端末自身に十分なセキュリティ対策を組み込むことが困難なクライアントが，サーバの提示するセキュリティ証明書を参照することで安全性の判断を行うことができる．本基盤技術は，信頼できる第三者機関としてのセキュリティ保証局，サーバ側に導入される内部監査モジュール，サーバ側の安全対策の状態を保証するセキュリティ証明書，クライアント側でセキュリティ証明書を検証する検証モジュールから構成される．セキュリティ証明書を用いてサーバに対する監査や検疫結果を証明することで，サーバ側に安全対策のためのシステムを導入しており，それらが適切な設定のもとで確実に稼働している状態を通知することが可能となる．システムの設計にあたり，安全性，柔軟性，迅速性を考慮した処理モジュールおよび通信プロトコルの設計を行う．本基盤の通信の安全性を考慮して，処理モジュール間の通信に相互認証および暗号化を行うプロトコルを用いるシステムを設計する．また，内部監査モジュールの改ざんを防止するため，耐タンパハードウェアを用いる方式を提案する．タグを用いた通信データグラムを設計することで，証明書の発行にあたって多様なデータ形式を取り扱う方式を提案する．また，迅速性を考慮して，セキュリティ証明書の提示においてサーバの内部監査を証明書の提示とは非同期の周期で行う方式を設計する．

以降，2 章において安全対策の保証の必要性について述べ，3 章で関連技術について説明する．4 章においてセキュリティ保証基盤の基本モデルを提案し，5 章でその要件を整理する．6 章および 7 章においてそれぞれ，各処理モジュール，通信プロトコルの設計について説明し，8 章においてサーバとクライアントにおける即時性に関する評価を行う．最後に 9 章でまとめる．

2. 安全対策の保証の必要性

本章では，端末に対する安全対策の保証が要求される事例について検討する．

2.1 e コマース

e コマースなどの web サービスにおいては，サービス提供者に住所や氏名，クレジットカードの番号などの個人情報を送信する場合がある．このとき，サービス提供者は受信した個人情報に対して外部の侵入者による盗難を防止する安全対策を図っておく必要がある．第三者から安全対策の保証を受けることは，サービス利用者に対してのアピールに有効である．また，サーバに対して接続するクライアントの数が多いほど，サーバにウイルスを仕込まれるなどの侵害を受けた場合，その被害は深刻なものになる．そのため，「安全性のアピール」のほかに，本提案の目的とする「安全対策の保証」を通じて，安全対策を意識的に行い，セキュリティ上の侵害の発生とその被害を最小限に食い止めることは重要である．

2.2 ユビキタス端末

ユビキタス社会においては，様々な端末がネットワークに接続される．CPU やメモリ資源が限られた簡易端末の中には，安全対策のシステムを組み込むことが困難なものもある．したがって，これらの端末では通信相手の安全性を確認して，接続の継続や拒否を判断することが，安全な通信を行うための有効な手段となる．

2.3 暗号通信路

IPsec などの暗号通信路では，ネットワーク管理者が通信路のトラヒックの内容を監視することができず，暗号通信路を通じてウイルスなどの攻撃トラヒックが送受信され続ける場合もある．本提案によってサーバの安全対策を保証し，セキュリティ侵害に対するサーバの耐性を維持することで，暗号通信路に意図しない攻撃トラヒックを持ち込むことを防ぐことができる．

3. 関連技術とその問題点

本章では端末における安全対策および相手認証の技術とその問題点について述べる．

3.1 VDS/FW/IDS

通信の安全性を確保するための技術として，VDS/FW/IDS について説明する．

VDS は，端末上のファイルもしくはネットワーク上で送受信されるファイルの中に，ウイルスなどの特徴と一致するコードを検知する．VDS の中には送受信されるメールを検査して，ウイルスが含まれているメールを棄却したり，正常性が確認されたメールに検査済みマークを記入したりするものもある[1)]．

FW は，ネットワークや端末の接続点において，許可されていないアクセスを棄却する装置である．主に，外部ネットワークから内部ネットワークへのアクセス

制限によって攻撃を防いでいる[2]．

IDS はネットワーク上を流れるパケットや端末上のログファイルを監視して，攻撃パターンと一致するパケットやログファイルを検知する[3]．

3.2 検疫ネットワーク

OS やアプリケーションのバージョン，パッチの状態を確認して，最新の情報を確保するアップデートシステムがある[4]．この応用研究として，端末をネットワークに接続する際に検査を行い，最新の状態であることを確認できたら接続許可を与える検疫ネットワークが提案されている[5]．

3.3 認 証 技 術

通信相手の身元を証明する代表的な技術として X.509 の PKI がある[6]．これは，認証を受けたい端末の公開鍵に対して，社会的に信頼されている認証局がデジタル署名を施した公開鍵証明書を発行する技術であり，その証明書は「証明書に記載された公開鍵に対応した秘密鍵の正規所有者」を提示する．この処理は，認証局が端末から公開鍵を受け取り，端末の身元をオフラインで確認した後に，端末の公開鍵とその付随情報を含めた情報の全体に対して，認証局自身の秘密鍵でデジタル署名を施すものである．その端末と通信する利用者は，端末から送られてくる公開鍵証明書のデジタル署名を，認証局の公開鍵を用いて検証することで，その正当性を確認し認証している．

3.4 オンラインマークとセキュリティマーク制度

電子商取引において，なりすましや詐欺を行っていないことを証明し，利用者に信頼を与えることを目的としたオンラインマーク制度がある[7]．また，事業者の運営するサーバに対して不正アクセス対策が適切に行われていること，および SSL 証明書の正当性を保証するセキュリティマークがある[8]．なかでも，インターネットマークと呼ばれる，電子透かしと電子署名を用いてサイトの真正性を証明する認証情報を画像マークに埋め込む技術が注目されている[9]．画像マークが真正性を確認されているサイトとは異なるサイトに張り付けられた場合，不正が行われていることを示すメッセージが画像に現れ，利用者はサイトの真正性を簡単に確かめることができる．マークの発行にあたっては，オフラインによる事業者の実在証明と審査が行われる．

3.5 従来技術の問題点

VDS/FW/IDS は，システムを導入している端末を脅威から守る機能を実現している．また，検疫ネットワークはクライアントの安全対策の状態をネットワーク側に通知する機能を実現している．しかし，これらの技術は単体ではその役割を果たしているものの，それぞれの技術だけでは，通信相手のクライアントに，サーバ自身の安全対策の状態を通知できない．

認証技術およびオンラインマーク制度はそれぞれ，通信相手の身元や該当するサイトの真正性を保証する技術であり，通信相手の安全対策を保証するものではない．また，証明書を発行するサービスの中には，迅速に確認してほぼリアルタイムで発行しているものもあるが，オフラインでの確認作業が基本となっており，窓口業務の手間がかかる．オフラインであっても，目標を達成するモデルを構築することはできるが，VDS/IDS のパターンファイルの頻繁な更新頻度を考慮した場合，オンラインで提案方式を実現する以外，現実的ではない．

以上をふまえると，通信相手の安全対策を保証するための課題は「安全対策の確認作業をオンラインで行うこと」となる．

4. セキュリティ保証基盤の提案

4.1 システムの設計に対する要件

本節では，セキュリティ保証基盤の基本モデルを設計するにあたって考慮すべき要件を，安全性に関する要件，柔軟性に関する要件，即時性に関する要件に分類し，整理する．

4.1.1 安全性に関する要件

悪意のユーザがセキュリティ保証局になりすまして偽の証明書を発行する場合や，サーバのなりすましを行って偽の証明書を取得したり，クライアントに対して偽の証明書を提示したりする攻撃を想定して，通信にあたっては相手認証を行う必要がある．

セキュリティ証明書の発行においては，サーバの安全対策に関する情報がセキュリティ保証局に送信される．このとき，悪意のユーザに通信内容を傍受され，サーバの安全対策が漏洩することが想定される．同様にして，セキュリティ証明書に安全対策の詳細が記されることで，サーバの脆弱性を読み取られる攻撃も想定する．

また，悪意のサーバ管理者が設置されている内部監査モジュールを偽造し，偽の監査結果によってセキュリティ証明書を取得する場合や，VDS/IDS を停止させた状態でセキュリティ証明書を提示する攻撃を想定し，内部監査モジュールの真正性を確保する必要がある．

本技術では，セキュリティ証明書がサーバの安全対策を保証するための重要な要素となる．したがって，証明書に関する発行責任を明確にし，信頼できるものであることを満たす必要がある．

要件 1 相手認証をともなう通信プロトコルである

こと

要件 2 セキュリティ保証局とサーバ間との間の通信内容を第三者に秘匿にできること

要件 3 内部監査モジュールに対する真正性を担保すること

要件 4 セキュリティ証明書がサーバの脆弱性を公表しないこと

要件 5 セキュリティ証明書の発行主体が明確であること

4.1.2 柔軟性に関する要件

セキュリティ保証局とサーバ間は，監査結果の通信において多様なデータ形式を交換する．また，セキュリティ証明書には，署名や発行日時に関する文字や，日付を意味する数値やバージョン番号を表す数値など，多様な意味表現が混在する．したがって，通信プロトコルはこれらの情報を柔軟に取り扱うことを考慮する必要がある．

要件 6 様々なデータ形式の情報を交換できる通信プロトコルであること

4.1.3 即時性に関する要件

VDS/IDS のパターンファイルは，頻繁に更新されるため，セキュリティ証明書もそれにともなって頻繁に更新される．したがって，証明書の発行処理は迅速に行われる必要がある．また，サーバとクライアントの通信における証明書の提示処理は，所望する通信に対するオーバヘッドであることから，証明書の提示に要する時間が短いことが，本基盤技術の普及のポイントとなる．

要件 7 証明書の発行が迅速に行えること

要件 8 サーバから迅速に証明書を提示できること

4.2 セキュリティ保証基盤の運用

本節では，課題および 4.1 節で整理した要件を満たすセキュリティ保証基盤の運用の一例を示す．

課題を考慮して，証明書の発行は処理モジュールがオンラインで監査結果を検証することにより完結するシステムを設計する．

ここでオンラインとは，サーバにおける安全対策の状態を，セキュリティ保証局がネットワークを経由して内部監査結果の取得および外部監査を行い，監査結果が適切であった場合，サーバにネットワーク経由でセキュリティ証明書を送付する処理と定義する．

また，監査はセキュリティ証明書を発行するときに実施する「発行のための監査」と，クライアントからの要求に従って実施する「提示のための監査」がある．前者はネットワークを介した監査結果の収集および検証のため数分程度の処理時間を想定している．後者はサーバがクライアントからの証明書の提示要求にリアルタイムで応答する必要があるため，10 秒以内の処理時間を想定している．

図 1 に，サーバ・クライアントモデルにおけるセキュリティ保証基盤の基本モデルを示す．基本モデルでは，サーバにおける安全対策をセキュリティ保証局が確認してセキュリティ証明書を発行し，クライアントはサーバから受け取った証明書を検証する．

以下に，1) セキュリティ証明書の発行，2) クライアントへの証明書の提示，からなるセキュリティ証明書の運用に関するライフサイクルを示す．

ここで例として，1) についてはセキュリティ証明書をサーバが発行するモデル，2) についてはセキュリティ証明書をセキュリティ保証局が提示するモデルなど様々な処理の流れが想定される．したがって，以下に示すのは，本提案の処理の流れの一例となる．

基本モデルの運用の前提条件として，サーバおよびセキュリティ保証局の公開鍵証明書は，既存の PKI で用いられる認証局が発行し，その正当性が保証されている．

事前準備

(1) セキュリティ保証局とサーバはそれぞれ，自身の公開鍵と秘密鍵のペアを生成し，既存の認証局から公開鍵証明書の発行を受ける．また，クライアントは，事前にセキュリティ保証局とサーバの公開鍵証明書を検証可能なルート証明書を入手しておく．

セキュリティ証明書の発行

(2) サーバは，VDS/IDS や OS/アプリケーションのバージョンおよびパターンファイルの更新を行う．

(3) 更新により状態が変化したサーバは，セキュリティ保証局に対してセキュリティ証明書の発行を依頼する．

(4) 内部監査はセキュリティ証明書の発行を行うタイミングで実施し，OS やアプリケーション，VDS/IDS のバージョン状態を監査する．

(5) 外部監査は証明書を発行するタイミングとは別のタイミングで実施し，FW の設定と稼働状態を監査する．ただし，外部監査はシステムに大きな負荷とならない程度の短い間隔で実施する．

(6) 証明書は，内部監査の結果と，証明書を発行する時点で最新の外部監査の結果が妥当であれば発行することで，即時的なオンラインの発行を実現する．

セキュリティ証明書の提示

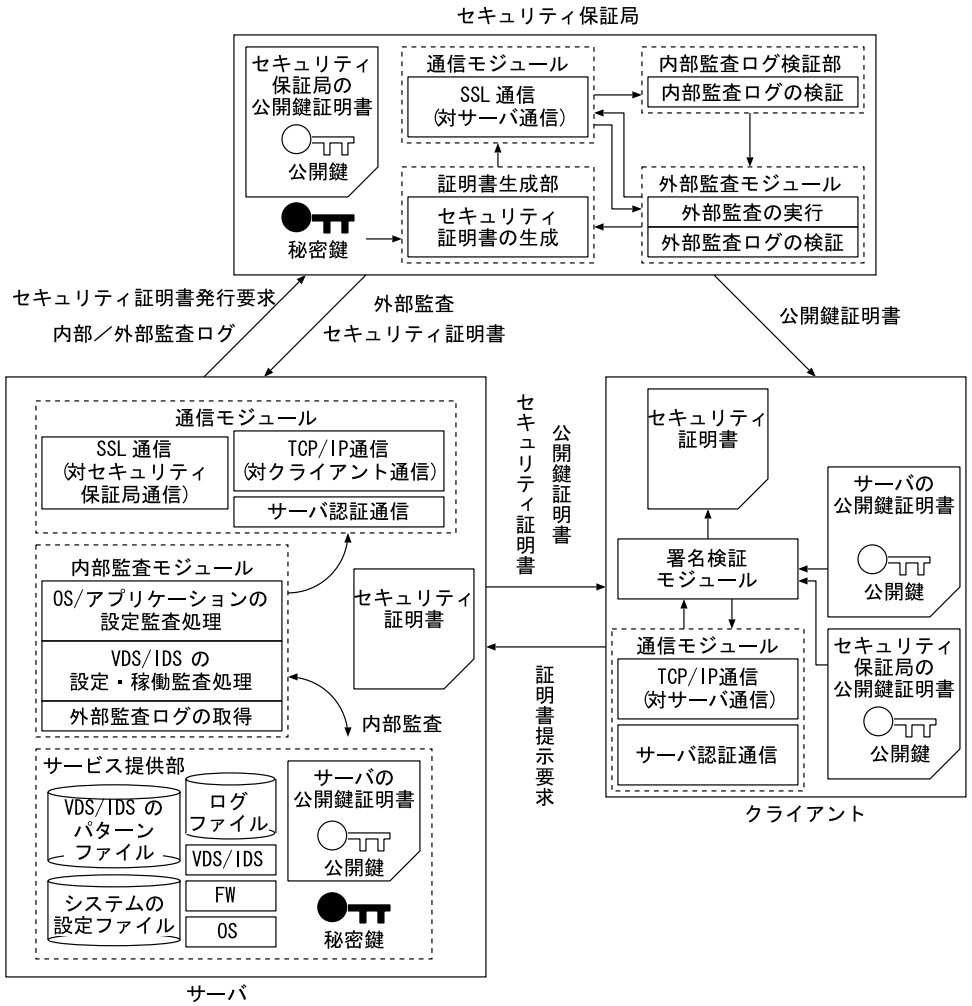

図 1 セキュリティ保証基盤の基本モデル
Fig. 1 Basic model of security key infrastructure.

(7) 通信の開始時点において，クライアントはサーバに対してセキュリティ証明書の提示を要求する．また，サーバの相手認証を行うため，乱数を送付する．

(8) サーバは自身のセキュリティ証明書をクライアントに返信するとともに，自身の秘密鍵を用いてクライアントが送付した乱数に対する署名を生成し返信する．

(9) クライアントは，サーバ認証のためにサーバの公開鍵を用いて送付した乱数に対する署名検証を行い，セキュリティ証明書の正当性を確認するためにセキュリティ保証局の公開鍵を用いて署名検証する．

4.3 セキュリティ証明書の発行

本節では，セキュリティ証明書の発行について述べる．

証明書は，OS とアプリケーションのパッチ状態が適切なときに発行され，VDS，FW，IDS のいずれか 1 つが正しく稼働していた場合には，安全指数が 1 となり，すべての状態が正しい場合には安全指数が 3 として，加算される形式で発行される．

この根拠として，サーバに対する既存の検疫手法として，Windows で用いられている Windows セキュリティセンター[10] を参考にする．この技術は，OS やアプリケーションに対するパッチの自動更新機能が稼働しているか，VDS が稼働しており最新のパターンファイルが適用されているか，FW が稼働しているか，を監査対象とし，いずれかの条件が満たされない場合，警告を表示する．本提案では，IDS の稼働状態も監査項目に加え安全指数の加算対象に用いる．

ただし，VDS，FW，IDS のいずれも正しく稼働していない場合には，侵入者に弱点を公開することになるため，証明書は発行されない．

証明書の発行は，証明書が有効期限を迎えた場合の定期的な間隔と，サーバの状態変化が発生した場合のいずれかで行う．特に，サーバの状態が変化した場合にただちに証明書の発行を依頼することで，基本的には保証の隙間は発生しない．

5. 処理モジュールの設計および実装

本章では，セキュリティ保証基盤を構成する各種処理モジュールの設計および実装について説明する．それぞれの処理モジュールの構成は，図 1 に示している．

5.1 セキュリティ保証局の設計

4.1 節の要件 1，2 を考慮して，セキュリティ保証局とサーバ間の通信において相互認証と暗号通信路を実現するための暗号通信モジュールを実装する．

暗号通信モジュールの実装方式には，IPsec および SSL が考えられる．IPsec は OS のカーネルに対する実装が必要となる一方で，SSL は OS レベルに対する改良を加えずに通信アプリケーションごとに柔軟に対応できることから，基本モデルでは SSL による実装を行った．

また，外部監査の実行および内部/外部監査の検証を行うため，外部監査の実行部，外部監査ログ検証部，内部監査ログ検証部を実装する．

基本モデルにおいて，内部監査の検証は，サーバの内部監査モジュールが実行した内部監査のログから，サーバで稼働している OS/アプリケーションの名称，バージョン情報などを取得し，正当性を検証する実装を行った．また，外部監査の実行部は FW 稼働状態および，その設定について検証を行う実装を行った．FW の設定の検証は，サーバとして提供しているサービスポート以外を閉じていることを確認し，具体的には，サービスを提供しているポート，および UDP 53 番ポートのみが開かれていることを確認する．

内部監査や外部監査の結果の検証処理は，既存の検疫システムに置き換えることも可能である．

また，監査結果に応じたセキュリティ証明書を生成，送付するため，証明書生成部を実装する．

5.2 サーバの設計

サーバはセキュリティ保証局およびクライアントと通信するための通信モジュール，内部監査を実施する内部監査モジュール，そしてサーバとしてのサービスを提供するサービス提供部より構成される．

サーバのサービス提供部に対する内部監査を行うため，OS/アプリケーションの設定監査処理および VDS/IDS の稼働監査処理部を実装する．

外部監査ログの取得部は，外部監査により監査対象のアプリケーションが生成したログをシステムから取得する．

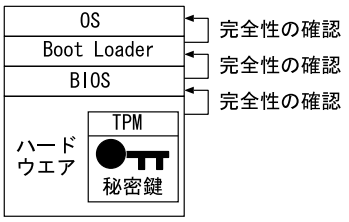

図 2 TPM による信頼性の確保
Fig. 2 Chain of integrity based on TPM.

上記に示す各種処理モジュールやサーバ OS への攻撃対策となる要件 3 を考慮して，サーバには Trusted Platform Module（TPM）に代表される耐タンパモジュールを設置して，信頼の基点を設ける．**図 2** に，TPM による信頼性の確保の仕組みを示す．ここで TPM とは，信頼できるコンピュータプラットフォームを構築するための業界標準仕様の開発，普及を目的とした団体である Trusted Computing Group（TCG）が提唱する耐タンパモジュールであり[11),12)]，BIOS，OS，ソフトウエアの改ざんを発見するためのハッシュ値を管理する機能，公開鍵と秘密鍵を生成して秘密鍵を管理する機能などを持つ．TPM には，改ざん検知の対象となる情報のハッシュ値を生成し，耐タンパモジュールの情報を保護するメモリ領域に記録する．内部監査を行う場合，監査を行う時点で守るべき情報のハッシュ値を生成し，耐タンパモジュールに記録されているハッシュ値と比較を行い，改ざんされていないことを確認する．また，完全性の確認の連鎖により通常の記憶領域にインストールされ，稼働するアプリケーションの信頼性を確保する．これにより，内部監査モジュールの真正性を確保できる．TPM の代わりに，スマートカードなどの技術も適用できる．TPM による信頼の基点によって守るべき情報と守られる情報を**表 1** にまとめる．

5.3 クライアントの設計

クライアントには，サーバ認証を行う通信モジュールおよびサーバが提示するセキュリティ証明書の安全指数などを検証する署名検証モジュールを実装する．

5.4 セキュリティ証明書の設計

図 3 にセキュリティ証明書の構成を示す．

セキュリティ証明書の構成は，PKI で用いられる X.509 を参考に，セキュリティ保証基盤で必要となる

表 1 TPM による信頼の基点によって守るべき情報と守られる情報
Table 1 Information that should defend by TPM and defended information.

守るべき情報	守られる情報
・BIOS，Boot Loader OS のハッシュ値 ・公開鍵と秘密鍵を生成する機能 ・秘密鍵 ・内部監査モジュールのハッシュ値	・BIOS，Boot Loader OS ・通常の記憶領域の内部監査モジュール ・パッチファイル

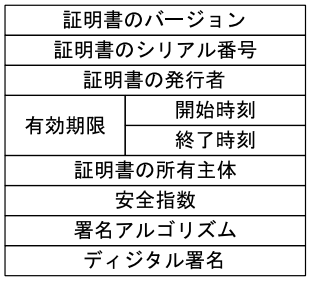

図 3 セキュリティ証明書の構造
Fig. 3 Structure of security certificate.

情報を持っている[6]．ここで，要件 4 を考慮してセキュリティ証明書にはサーバのセキュリティ対策に関する詳細な情報を隠蔽するために，対策の度合を示す指数として安全指数を導入する．なお，安全指数が低い場合でも，クライアントはサーバに接続できる．その場合，クライアントがサーバへの接続を続行するときは，たとえば，クライアント自身の安全対策の状態が最新であることを確認した後に接続することや，該当するサーバから受信したメールの添付ファイルの取扱いには留意することになる．また，要件 5 を考慮して証明書には発行主体に関する情報を記載する．

セキュリティ保証基盤モデルでは，既存の PKI モデルに比べて頻繁に証明書の更新・失効処理が繰り返されるため，証明書の有効期限は短くなる．失効証明書リストを用いた管理では，セキュリティ保証局における負荷が高くなり，迅速な署名検証を行えない．したがって，要件 7 を考慮して，本論文ではセキュリティ証明書の失効処理は行わないこととし，証明書に記載されている有効期限を失効状態の指標と見なす．

6. 通信プロトコルの設計

本章では，セキュリティ保証基盤における処理モジュール間で用いられるデータグラムの設計と通信プロトコルの設計について説明する．

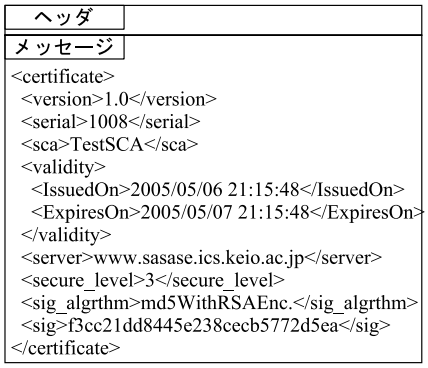

図 4 データグラムの構造
Fig. 4 Datagram structure.

6.1 データグラムの設計

図 4 に，セキュリティ保証局がサーバにセキュリティ証明書を送付するときのデータグラムを示す．データグラムは，ヘッダ部とデータ部から構成される．

ヘッダ部には，あらかじめ規定されたメッセージが格納される．セキュリティ保証基盤の各モジュールは，受信したデータグラムのヘッダのメッセージを解読し，監査や証明書の生成などの処理を行う．

データ部では，処理に応じた様々なデータが格納される．ここで要件 6 を考慮して，データの記述方式は，あらかじめ規定したタグを用いてデータを囲む，マークアップ言語の形式を採用する．マークアップ言語を用いることで，様々なデータ形式をテキストで表現することが可能となり，また，それぞれのデータの意味表現をタグで示すことができる．

6.2 サーバとセキュリティ保証局間の通信プロトコル

図 5 に，SSL 通信を適用した場合のサーバとセキュリティ保証局間の通信手順を示す．セキュリティ証明書発行の通信は，相互認証や暗号化と独立した設計とする．したがって，相互認証および暗号通信路については IPsec，SSL などを柔軟に適用することができる．

サーバとセキュリティ保証局間の通信においては，TCP と UDP の選択肢があり，TCP では通信の信頼性が保証され，UDP では迅速な処理が可能となる．ここではモジュール間で確実にデータグラムが送受信されることを重視して，TCP を採用する．TCP の 3 ウェイハンドシェイクに続き，SSL による相互認証，通信路の暗号化が行われ，セキュリティ証明書の発行処理が行われる．

6.3 サーバとクライアント間の通信プロトコル

サーバとクライアント間の通信では，目的とする通信に先立ってセキュリティ証明書の提示処理が行われ

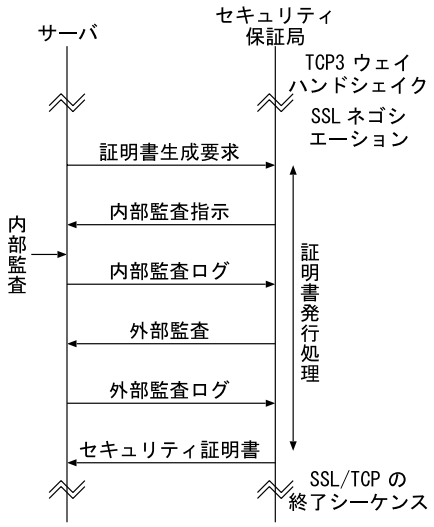

図 5 SSL 通信を適用した場合のサーバとセキュリティ保証局間の通信手順
Fig. 5 Protocol between the server and the security authority.

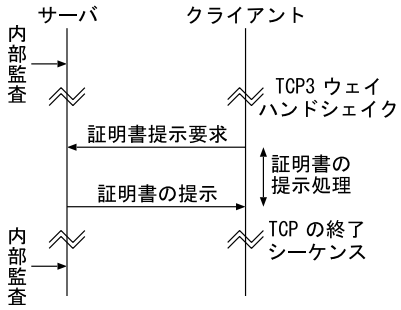

図 6 サーバとクライアント間の通信手順
Fig. 6 Protocol between the server and the client.

る．**図 6** に，サーバとクライアント間の通信手順を示す．

なお，セキュリティ証明書は TCP を用いて入手する．また，UDP 通信を行う場合においても，サーバ認証を行うため，TCP によって証明書を取得した後に，UDP による通信を行う．

要件 2 を考慮したサーバ認証を終えた後に，サーバから証明書を送付する．クライアントで証明書の検証に成功した場合，サーバとクライアント間で所望の通信が開始される．

要件 8 を考慮して，内部監査はクライアントからの証明書の提示要求に対して非同期に実施することとし，クライアントからの要求を受け次第，上記の署名処理を実施してセキュリティ証明書を提示する．

ここで**図 7** にクライアントにおけるセキュリティ証明書の検証画面を示す．

図 7 セキュリティ証明書の検証画面
Fig. 7 Screenshot of certification viewer.

7. 本提案と従来研究の比較

本章では，本提案とインターネット・マークおよびセキュリティマーク[7)~9)] の比較を行い，本提案の新規性および有効性を明確にする．

(1) 保証する内容

インターネット・マークは，マークを提示する Web ページのコンテンツ，URL，IP アドレスなどを検証し，Web サイトの真正性を保証する．

セキュリティマークは，マークを提示する Web サイトに対して，独自の監査ツールを用いてセキュリティホールのチェックとポート接続チェックを行う．また，SSL 通信に必要な SSL 証明書の監査を行い，基準を満たしていることを保証する．さらに，書類審査を通じてセキュリティ管理体制の確立状況を監査する．

本提案は，セキュリティ証明書の発行を受けるサーバにおいて，OS に最新のパッチが適用されていること，FW が適切に設定され稼働していること，VDS/IDS が最新のパターンファイルを用いて稼働していることを保証する．

(2) 適用されるサービス

インターネット・マークは Web サーバを利用したサービスの真正性と安全性を保証する．

セキュリティマークはセキュリティ管理体制の確立状況および Web サーバを利用したサービスの真正性と安全性を保証する．本提案は Web サーバ，メールサーバ，その他のアプリケーションサーバなど，サーバとして提供する機能全般に対する安全性を保証する．

(3) 証明書を発行するにあたっての監査内容

インターネット・マークは，マークを申請する

表 2 提案方式と従来方式の比較
Table 2 Comparison between conventional scheme and proposed scheme.

比較項目	セキュリティ保証基盤（提案方式）	インターネット・マーク	セキュリティマーク
保証内容	・サーバにおける安全対策の状態	・Web サイトの真正性	・セキュリティ管理体制の確立状況 ・不正アクセス対策と SSL 証明書の内容
適用されるサービス	・サーバが提供するサービス全般	・Web サーバを利用したサービス	
監査内容	・OS のパッチ適用状態 ・FW の設定と稼働状況 ・VDS/IDS の設定と稼働状況	・コンテンツ情報 ・URL ・IP アドレス	・不正アクセス対策 ・SSL 証明書の形式と署名
監査方式	・内部監査と外部監査	・書類監査	・書類監査と外部監査
耐タンパハードウエアの利用	・あり	・なし	
データ形式	・属性証明書に準拠	・画像データ	
保証のレベル分け監査	・複数段階	・一段階	
有効期限	・1 日から 1 週間程度	・1 年間程度	
失効管理	・なし	・有効期限を設定し，失効管理機能をオプションとして提供	
証明書を提示するときの監査	・あり	・なし	

ユーザが申告した Web ページのコンテンツ情報，URL，IP アドレスなどを監査する．

セキュリティマークは，マークを申請するサーバに対して不正アクセス対策に関する外部監査を行い，その結果を監査する．また，サーバが所有する SSL 証明書について，その形式と署名を監査する．

本提案は，セキュリティ証明書を申請するサーバに対して FW，VDS/IDS の稼働状態を確認する外部監査を行う．また，サーバに耐タンパハードウェアを実装して内部監査を行い，OS のパッチ適用状態，FW の設定と稼働状態，VDS/IDS の設定と稼働状態を監査する．

(4) マークもしくは証明書の形式

インターネット・マークおよびセキュリティマークは，JPEG などの画像データを用いる．

本提案で用いるセキュリティ証明書は，X.509 属性証明書に準拠した形式を用いる．

(5) 監査結果の分類

インターネット・マークおよびセキュリティマークは，マークの発行対象が一定の監査基準を満たしていることを提示するものであり，複数の基準は設定されていない．

本提案では，サーバの安全対策の状態に応じて「安全指数」を導入し，証明書ごとに異なる保証のレベルを提示できる．これによりクライアントは，安全指数を判断基準として，サービス内容に応じて柔軟な対応が可能となる．

(6) 証明書の有効期限と失効管理

インターネット・マークおよびセキュリティマークの有効期限は 1 年間に設定されている．失効管理はオプションとして考慮されている．

本提案では，セキュリティ証明書の有効期限は 1 日や 1 週間程度の短期間に設定されている．また，失効管理の機能は設けず，失効については短い有効期限と証明書の頻繁な発行により対応することを提案している．

(7) 証明書を提示するときの監査

インターネット・マークおよびセキュリティマークは，マークを提示する時点において，監査対象の項目に対する監査を行わない．本提案では，セキュリティ証明書を提示するタイミングと同期または非同期のタイミングで定期的にサーバの安全対策の状態を監査する．

以上の検討内容を，**表 2** にまとめた．

8. 通信に関する速度評価

ここでは要件 8 を確認するために，サーバとクライアント間における証明書の提示処理の通信速度を評価する．

8.1 評価環境

評価のために，サーバ・クライアント間のサーバ認証とセキュリティ証明書の提示処理に関する通信モジュールを実装した．実装に用いたサーバの諸元は，CPU

が Pentium4 3.4 GHz，メモリ容量が 2 GBytes，OS は FreeBSD-5.3，NIC は 100 Base-TX である．また，クライアントの諸元は，CPU が PentiumM 1.5 GHz，メモリ容量が 768 MBytes，OS は FreeBSD-5.3，NIC は 100 Base-TX である．

8.2 サーバ・クライアント間の通信速度の評価

ここでは，証明書の提示において内部監査を非同期に行う方式の即時性を確認するために，クライアントがサーバからセキュリティ証明書を受け取る際に，同じタイミングでサーバの内部監査を実施する「同期監査方式」と，別のタイミングで内部監査を行う「非同期監査方式」におけるサーバの応答時間を評価する．

内部監査については，1) OS の名称およびバージョン情報，2) FW の稼働状況と設定，3) VDS/IDS の稼働状態の監査を行う．

1) については，システムコール `uname` を実行し，返り値より OS の名称およびバージョン情報を取得する．

2) については，システムコール `netstat` を実行し，tcp および udp のリスンポートの一覧を取得する．

3) については，システムコール `whereis` を実行し，バイナリの存在を確認する．さらに，`md5` コマンドを用いてチェックサムを計算し，その正当性を確認する．また，`ps` コマンドを実行して該当するアプリケーションの実行中のプロセスを確認する．

なお，サーバに対する内部監査については，OS やアプリケーションのバージョンチェックやパッチの状態，VDS/IDS の稼働状態やパターンファイルのバージョン番号を確認する処理であり，数秒以内に完了できる．したがって，要求が重ならない限り同期と非同期のいずれでも処理しきれるため，監査項目に差異はない．

また，評価の前提条件として内部監査モジュールと同等の処理を行うプログラムを作成して監査にかかる時間を計測し，所要時間をおよそ 0.04 秒との結果を得た．

非同期監査方式ではサーバ認証とセキュリティ証明書の提示処理の時間が含まれ，同期監査方式はさらに内部監査の処理時間が含まれる．このとき，同期監査方式において新たな証明書の発行は発生しない．クライアントからの要求を増加させながら，証明書提示要求を発してから証明書を取得するまでの時間について，ネットワーク上でパケットをキャプチャすることで計測した．評価結果を**図 8** に示す．

図 8 より，いずれの監査方式においても同時接続数が増加するにともない，処理時間も増加していることが分かる．応答時間について，ローカルアプリケーションを例にとると，10 秒以上の処理を行う場合，時間のかかる処理としてタイトルバーに「応答なし」などの表示が行われる．結果より，クライアントからの同時接続要求が 100 件の場合に着目すると，非同期監査方式の応答時間は 10 秒未満となっている．一方，同期監査方式の応答時間は 10 秒を超えている．したがって，非同期監査方式はクライアントからの接続要求が多い場合にもローカルアプリケーションと同等の応答時間を得られており，即時性を達成できたと見なすことができる．

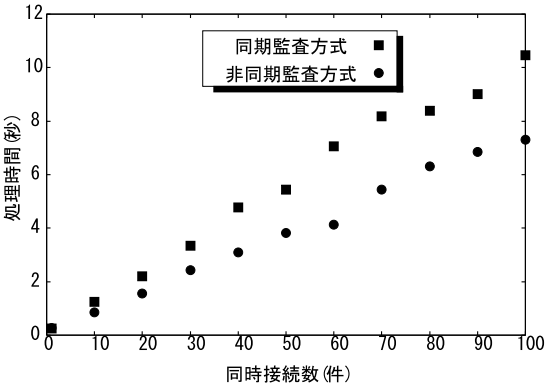

図 8 サーバとクライアント間の応答時間評価
Fig. 8 Response time between the server and the client.

以上より，証明書の提示処理を迅速に行うには非同期監査方式が適しており，要件 8 に示す即時性を達成できていることが分かる．

9. おわりに

本論文では，通信相手のセキュリティ対策を保証するセキュリティ保証基盤を提案し，各種処理モジュール，および通信プロトコルに関して，安全性，柔軟性，即時性に関する要件を整理して，設計，実装を行った．本基盤の通信の安全性を確保するために，モジュール間の相互認証および暗号化を行うシステムを設計した．また，耐タンパハードウェアを用いることでサーバの内部監査モジュールの安全性を確保する設計を行った．セキュリティ証明書に関しては，悪意のユーザがセキュリティ証明書から脆弱性を得る攻撃を想定し，証明書に具体的なセキュリティ対策を記載しない証明書の設計を行った．また，通信データグラムはヘッダ部とデータ部から構成されるデータグラムを設計し，データ部に格納するデータはマークアップ言語の形式を用いることで，複数のデータ構造を統合的に取り扱うことができ，同時にそれぞれのデータの意味情報を容易に定義できることを示した．サーバとクライアント間にお

けるサーバ認証とセキュリティ証明書の提示処理について実装を行い，通信速度を評価した結果，内部監査を非同期に行う場合であれば，迅速に証明書を提示できることを示した．本基盤技術は，サーバの監査や検疫結果を第三者機関が保証する技術であり，セキュリティ対策機能を持たせにくい小型端末に対する通信制御などへの利用が考えられ，今後の安心安全なユビキタス通信社会への寄与が期待される．

なお，今後の研究課題として，VDS/IDS のパターンファイルの内容およびバージョンの真正性を検証する手法について検討を進める予定である．

謝辞 本研究は KDDI 研究所のご支援によって行われた．関係者各位に深謝する．

参 考 文 献

1) 一瀬小夜，星澤裕二：インターネットセキュリティウイルスの原理と対策，ソフトバンクパブリッシング株式会社 (2002).
2) Feed, N.: Behavior of and Requirements for Internet Firewalls, IETF RFC2979 (2000).
3) 武田圭史，磯崎 宏：ネットワーク侵入検知，ソフトバンクパブリッシング株式会社 (2000).
4) Microsoft Windows Update. http://www.windowsupdate.com/
5) 三輪信介：持ち込み PC 検疫機構の提案，コンピュータセキュリティシンポジウム 2003 (*CSS2003*)，pp.265–270 (2003).
6) ITU-T Recommendation X.509 (2000): Information technology — Open systems interconnection — The Directory: Public Key and attribute certificate frameworks (2000).
7) オンラインマーク制度について. http://www.ecom.or.jp/onlinemark/
8) セキュリティマークの制定. http://www.ecom.jp/qecom/seika/rink3/hyousi.htm
9) 吉浦 裕：正当性の検証が可能な図形マークとその WEB サイト認証への応用，画像電子学会，Vol.30, No.3, pp.306–312 (2001).
10) Windows XP Service Pack 2 のセキュリティセンターでのセキュリティ設定の一元管理. http://www.microsoft.com/japan/windowsxp/using/security/internet/sp2_wscintro.mspx
11) Trusted Computing Group: Home. https://www.trustedcomputinggroup.org/home
12) TCG: TPM Main Part1 Design Principles, TCG PUBLISHED (2003).

(平成 17 年 5 月 12 日受付)
(平成 17 年 11 月 1 日採録)

磯原 隆将（学生会員）
平成 17 年慶應義塾大学理工学部情報工学科卒業．現在，同大学大学院修士課程在学中．主として，インターネットセキュリティに関する研究に従事．

石田 千枝（学生会員）
平成 16 年慶應義塾大学理工学部情報工学科卒業．現在，同大学大学院修士課程在学中．主として，インターネットセキュリティに関する研究に従事．本学会会員．

北田 夕子
平成 16 年慶應義塾大学理工学部情報工学科卒業．現在，同大学大学院修士課程在学中．主として，インターネットセキュリティに関する研究に従事．電子情報通信学会会員．

竹森 敬祐（正会員）
平成 6 年慶應義塾大学理工学部電気工学科卒業．平成 8 年同大学大学院修士課程修了．同年 KDD（株）入社．平成 16 年慶應義塾大学大学院博士課程修了．現在，(株）KDDI 研究所．主として，通信ネットワークおよびインターネットセキュリティに関する研究に従事．平成 14 年度電子情報通信学会学術奨励賞受賞．電子情報通信学会会員．

笹瀬　巌（正会員）

昭和 54 年慶應義塾大学工学部電気工学科卒業．昭和 59 年同大学大学院博士課程修了．同年オタワ大学理工学部電気工学科ポストドクトラルフェロー，昭和 60 年同大学講師．昭和 61 年慶應義塾大学理工学部電気工学科助手，昭和 63 年同大学専任講師，平成 4 年同助教授，平成 11 年同大学理工学部情報工学科教授，現在に至る．主として，ディジタル通信，通信ネットワーク，光通信理論，マイクロ波通信，非線形通信システム，通信理論，符号理論，インターネットセキュリティに関する研究に従事．工学博士．昭和 59 年度 IEEE COM．SOC．学生論文賞．昭和 62 年第 3 回井上研究奨励賞受賞，昭和 63 年第 1 回安藤博記学術奨励賞，昭和 63 年篠原記念学術奨励賞，平成 8 年度電子情報通信学会交換システム研究会優秀論文賞受賞．IEEE Senior Member，電子情報通信学会，情報理論とその応用学会各会員．