HPCI 認証基盤の運用における課題とその解決策

石井 宏治, 坂根 栄作, 合田 憲人

国立情報学研究所

k_ishii@nii.ac.jp

Solutions to the issues in system operation of HPCI authentication infrastructure

Koji Ishii, Eisaku Sakane, Kento Aida

National Institute of Informatics

概要

国立情報学研究所では，革新的ハイパフォーマンス・コンピューティング・インフラ (HPCI) を構成する認証基盤の運用を行っている。本稿では，HPCI 認証基盤の運用において発生した課題とその解決策について報告する。

1　はじめに

革新的ハイパフォーマンス・コンピューティング・インフラ (High Performance Computing Infrastructure: HPCI) [1] は，ネットワーク上に分散した計算資源や Web アプリケーションに対して統一したアカウント情報で認証できる環境（シングルサインオン）を提供している。平成 29 年 4 月から開始となった第 2 期 HPCI においてもシングルサインオンの提供を継続するため，国立情報学研究所 (NII) と計算資源を提供する機関（HPCI システム構成機関）では，公開鍵認証基盤に基づく Grid Security Infrastructure (GSI) [2] および Shibboleth [3] を用いた認証基盤（HPCI 認証基盤）の運用を引き続き行っている。

HPCI 認証基盤は，HPCI 認証基盤の中核となる HPCI 認証局ならびに証明書発行システムなどの関連システム（HPCI 認証基盤システム）および HPCI システム構成機関の Identity Provider (IdP) サーバ，GSI-OpenSSH サーバで構成される。図 1 は，HPCI 認証基盤の構成と課題参加者が計算資源にシングルサインオンする際の手順を示している。Web アプリケーションの利用時は HPCI アカウントを用いた Shibboleth 認証，計算資源の利用時は HPCI 認証局が発行する電子証明書を用いた GSI 認証が行われる。[4]

NII は HPCI 連携サービス運営・作業部会 認証基盤サブワーキンググループ (Sub-WG) として HPCI 認証基盤システムを運用しており，これらに加えて HPCI 認証基盤に関連するソフトウェア開発，HPCI 運用事務局ヘルプデスクに対する運用支援業務なども行っている。[5]

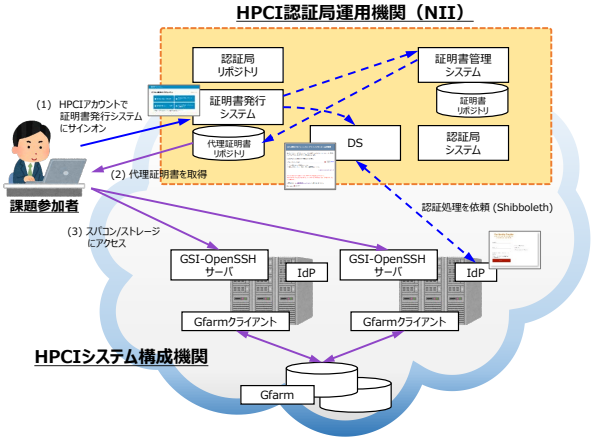

図 1　HPCI 認証基盤

本稿では HPCI 認証基盤の運用において，近年顕在化した課題とその解決策等を報告する。2 節では，平成 29 年度 B 期「京」利用研究課題の開始に係る認証基盤 Sub-WG の対応を述べる。3 節では，遠隔地在住者の本人確認方法の検討について述べる。4 節では，認証基盤 Sub-WG 内外との電子データ授受に関する取り組みについて述べる。5 節では，HPCI 認証基盤のシステム運用やソフトウェア開発状況などを報告する。最後に 6 節では，まとめを述べる。

2　B 期課題対応

HPCI の利用研究課題の募集は平成 29 年度から年 2 回となり，第 2 回目の募集による課題（B 期課題）

は，10 月から 1 年間が実施期間である。この B 期課題は，理化学研究所 計算科学研究機構が資源提供する「京」のみを利用する研究課題が対象であり，平成 29 年度時点では「京」以外の計算資源を利用する研究課題は募集対象外となっている。

これまで HPCI 認証局では，HPCI の利用研究課題の募集は年 1 回，実施期間は 4 月から 1 年間（A 期課題）であることを前提として，課題参加者を対象に有効期間が「3 月 25 日から翌年 4 月 24 日」となる電子証明書を発行してきた。しかし B 期課題が新設されることで，前述の前提条件が変わるため，HPCI 認証基盤では対応策の検討を平成 28 年度から続けてきた。HPCI 認証局が発行する電子証明書のうち B 期課題が新設されることにより対応策が必要となるのは，課題参加者に対して 1 年に 1 回発行するクライアント証明書である。B 期課題開始の如何を問わずクライアント証明書の有効期間の設定をこれまで通りの有効期間満了日を日付固定で指定する方法のまま変更せずにクライアント証明書の発行を継続する場合，平成 29 年 10 月の B 期課題の開始から約半年後の平成 30 年 4 月 24 日にクライアント証明書の有効期間満了日を迎える。この時，A 期課題参加者視点では，前年度用として平成 30 年 3 月 24 日以前に発行したクライアント証明書は失効，平成 30 年度用として平成 30 年 3 月 25 日以降に発行のクライアント証明書は翌年 4 月 24 日まで利用できる。一方，B 期課題参加者視点では，使用しているクライアント証明書が研究課題の期間途中で有効期間満了日を迎えて失効となるため，平成 30 年 4 月 24 日以降も実施中の研究課題においてクライアント証明書を使用するためには，平成 30 年 3 月 25 日以降にクライアント証明書を発行し直して更新する必要がある。

以上のように，何らかの対応策を打たないままでは，B 期課題参加者にのみ実施期間の途中でクライアント証明書の更新を強いることになるため，平成 29 年 9 月 25 日以降に発行するクライアント証明書については，有効期間満了日を日付固定で指定するのではなく，有効期間を発行後 395 日間と日数指定するように証明書プロファイルを変更する。この変更の適用以後に発行されるクライアント証明書の有効期間満了日は課題参加者一律ではなく，課題参加者がクライアント証明書を発行した日を基準として有効期間満了日が起算される。したがって平成 29 年 9 月 25 日以降は，A 期課題参加者であっても有効期間の指定方法が日数指定となったクライアント証明書が発行される。例えば，研究課題の実施期間の途中で電子証明書の失効および再発行が必要になる場合（氏名等の HPCI-ID 登録情報を変更した場合，秘密鍵危殆化もしくは危殆化の疑いがある場合，有効期間内の電子証明書を保持していて，その証明書のパスフレーズを失念したためパスフレーズを初期化した場合）に再発行したクライアント証明書の有効期間は，参加する研究課題の実施期間に関わらずクライアント証明書の再発行日から起算して 395 日間となる点には注意が必要である。なお，発行したクライアント証明書の有効期間満了日が研究課題の実施期間終了以後の日付に設定される場合もあるが，有効期間満了日を迎える以前に参加するすべての研究課題が終了となった時点で発行済の電子証明書が失効となるのは従来通りである。

前述のとおり，これまでクライアント証明書の有効期間満了日は，すべての課題参加者で一律の日付（毎年 4 月 24 日）であったため，有効期間満了日の通知と今後も継続して使用する場合の電子証明書の再発行依頼を年度末に HPCI 運用事務局から HPCI アカウント所有者宛てに電子メールで一斉に連絡することで問題はなかったが，平成 29 年 9 月 25 日以降は有効期間満了日をクライアント証明書の発行日から起算する方法に変更となるため，課題参加者個別にクライアント証明書の有効期間満了日の通知と再発行の依頼を行うように変更する必要がある。しかし現在の HPCI には，このような通知を行う仕組みは存在しないため，課題参加者それぞれが発行したクライアント証明書が有効期限切れを迎える一定期間より前に電子メールで個別に有効期間満了日を通知する機能を HPCI 認証基盤システムに追加し，平成 30 年 9 月下旬までに運用を開始する予定である。

3　電子データ授受

HPCI 認証基盤において HPCI の機関が行う各種申請の手続きは，HPCI 認証基盤各担当者一覧（担当者一覧）に記載されている各機関の担当者本人のみ行うことができる。この申請手続きには各機関の担当者と認証基盤 Sub-WG との間で各種電子データ（サーバ証明書の CSR や電子証明書失効・パスフレーズ初期化申請書など）の授受を伴う場合がある。認証基盤 Sub-WG において，機関担当者との間で行う電子データ授受は電子メールへの添付を基本としているが，機関のポリシー等により電子メールへのファイル添付が禁止されている機関もあるため，メール本文への直接記載やオンラインストレージを介して電子データを送

受信する方法も併用している。

HPCI 認証基盤において HPCI の機関が各種申請を行う際，電子データを電子メールに添付して認証基盤 Sub-WG に受け渡す場合，機関担当者は必要事項を記載したメールに受け渡すファイルを添付して認証基盤 Sub-WG 宛てに送信する。この時，サーバ証明書の CSR などのテキストデータである場合はファイルの内容をメール本文に直接記載しても良い。添付ファイルにパスワードを設定する場合，申請の電子メールとは別便のメールにて送信する。また申請に使用するデータが大量であるなど，申請時のメール本文に直接記載できない電子データをオンラインストレージを介して受け渡す場合，機関担当者は受け渡すファイルをオンラインストレージに配置し，そのファイルに対して適切なアクセス制限（パスワードによるアクセス制限，ユーザ認証など）を設定して認証基盤 Sub-WG がダウンロードできるようにする。この際，HPCI 共通セキュリティ要件を満たしているオンラインストレージを使用することが望ましい。機関担当者は必要事項を記載した電子メールにオンラインストレージからファイルをダウンロードするための URL（ダウンロード URL）も記載して認証基盤 Sub-WG 宛てに送信する。パスワード等のアクセス制限の情報はダウンロード URL を記載したメールとは別途のメールで送信する。

認証基盤 Sub-WG にて機関担当者からの電子メールを受信した際は担当者一覧をもとに差出人に不備がないか確認，担当者一覧に記載の機関担当者の電話番号宛てに架電する。受信した電子メールは機関担当者本人からの申請であることを確認した後，メールで送られてきたファイルもしくはメールに記載されたダウンロード URL から電子データを入手し，申請に対する処理を開始する。

認証基盤 Sub-WG から機関担当者へ電子データを受け渡す場合は電子メールにファイル添付しての送信を基本とする。添付ファイルにパスワードを設定する際は別便のメールにて連絡する。機関のポリシー等により機関担当者が添付ファイルを受信できない場合，機関担当者はその旨を認証基盤 Sub-WG へ返信する。その際，代替えとなる電子データ授受の方法としてメール本文へ直接記載または機関担当者が指定するオンラインストレージへのアップロードのどちらかを選択する。オンラインストレージへ電子データの配置を依頼する場合はアクセス先 URL，ユーザ名，パスワードなど指定のオンラインストレージへ認証基盤 Sub-WG がファイルを配置するための情報が必要である。認証基盤 Sub-WG にて機関担当者からの電子メールを受信した際は，前述と同様にメールの差出人確認を行い，代替え手段による電子データの再送依頼であることを機関担当者に電話で確認した後，指定された方法で電子データを受け渡す。指定のオンラインストレージを介して受け渡す場合は配置するファイル自体にもパスワードを設定し，電子データの再送を連絡するメールとは別途のメールにてファイルのパスワードを通知する。

以上が機関担当者と認証基盤 Sub-WG との間における電子データ授受の手順である。また，電子データ授受の範囲が認証基盤 Sub-WG 内部に限定される場合のファイルの受け渡しは，電子メールへのファイル添付，NII 内のファイル共有サーバへの配置のいずれかまたは併用で行う。認証基盤 Sub-WG では，平成 29 年度から S/MIME を試験的に導入している。S/MIME を利用することでメール配送経路途中での盗聴，メールの送信者なりすまし，メール内容の改ざんのリスクに対応できるため，機関担当者との電子データ授受において実施しているメールの差出人が本人であることの確認手順やメールの内容確認および別途のメールにてパスワードなどを通知する手法を S/MIME によるメールへの電子署名の付与とその確認およびメールの暗号化によって置き換え，より強固なものとしている。

S/MIME を使用して電子署名もしくは暗号化したメールを送信するためには，電子メールの送信元となるメールアドレスにひもづく S/MIME 証明書が必要であるため，認証基盤 Sub-WG では NII が運営する UPKI 電子証明書発行サービス [6] にて S/MIME 証明書を発行し，これを利用している。

S/MIME を利用することで電子メールにおけるセキュリティのうち，メッセージの秘匿性，認証，メッセージの完全性は確保されるが，電子メールを取り巻く課題のすべてが解決する訳ではない。例えば，S/MIME によって電子署名もしくは暗号化されたメールにマルウェアが添付されるといった可能性は完全に否定をできず，別途の対策を講じる必要がある。また，機関のポリシー等により電子メールへのファイル添付が禁止されている場合，電子データ授受には前述のようなメール添付を代替する手段を引き続き採ることになるであろう。しかしながら，このような場合に利用するオンラインストレージのアクセス制限情報等の通知など，関係者以外には秘匿したい情報のやり

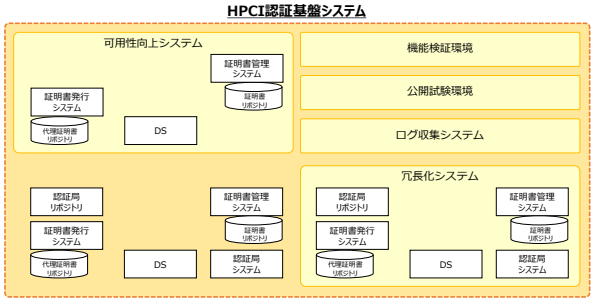

図 2　HPCI 認証基盤のシステム構成

取りに暗号化したメールを使用するといった目的において，S/MIME の導入は検討に値すると言える。

4　システム運用・ソフトウェア開発

この節では，NII が担当する HPCI 認証基盤のシステム運用，ソフトウェア開発ならびに HPCI 認証基盤全体に関わる近年のトピックを報告する。

4.1　HPCI 認証基盤システムの機器更新

HPCI 認証基盤では，平成 23 年度に HPCI 認証基盤システムを構築，平成 24 年度には冗長化のため待機システム (冗長化システム) を用意し，運用の堅牢性を確保したうえで本運用を開始している。また，システムの設定変更やシステム改修に伴う更新等を HPCI 認証基盤のサービスに影響を与えることなく実施可能とするための HPCI システム構成機関向けの試験環境（公開試験環境），NII で使用する検証環境（機能検証環境）を用意している。さらに，システムの可用性を向上させるためのサーバ（可用性向上システム）の構築を行い運用の安定性を高めている。これらに加えて，セキュリティの向上のため，HPCI 認証基盤におけるログの改ざん防止およびバックアップを行うために必要となるシステム（ログ収集システム）も導入するなど，副次的なシステムも順次整備してきた。平成 29 年 9 月現在の HPCI 認証基盤は，図 2 に示すシステム構成となっている。

当初に整備した各ハードウェアは導入から 5 年を経過する平成 28 年度以降，保守期限が順次到来するため，平成 28 年度および平成 29 年度の 2 回に分けて HPCI 認証基盤システムの機器を更新する。平成 28 年度は，HPCI 認証局システムおよび関連システムと冗長化システムについて機器を更新し，平成 29 年 2 月に運用を移行した。平成 29 年度は，可用性向上システム，公開試験環境，機能検証環境およびログ収集システムを対象に機器更新を行う。可用性向上システム，公開試験環境および機能検証環境の各サーバは，提供するサービス特性を考慮して，すべて仮想化基盤上に仮想マシンとして導入し，システム全体の運用効率の向上を図る。可用性向上システム，ログ収集システムについては平成 29 年 11 月中旬，公開試験環境は 12 月下旬までに運用を切り替える予定である。NII のみで使用する機能検証環境については，現在運用中の仮想マシン上の各サーバからの切り替えは，今回導入する仮想化基盤の構築が完了次第，順次実施する。

4.2　HPCI 認証局

4.2.1　発行状況

平成 29 年 9 月 27 日現在の HPCI 認証局における電子証明書発行枚数は，表 1 に示すとおりである。

表 1　電子証明書発行枚数（平成 29 年 9 月 27 日現在）

証明書種別	有効数	総数
クライアント証明書	276 枚	2,289 枚
ホスト証明書	87 枚	502 枚
サービス証明書	185 枚	710 枚

4.2.2　監査

HPCI 認証局は電子証明書の発行を行うにあたり，HPCI 認証局ポリシー管理委員会が定める HPCI 認証局運用規程 (CP/CPS) に従って運用されている。[7] HPCI 認証局の CP/CPS は，Interoperable Global Trust Federation (IGTF) [8] が規定する認証局に対する最低限の運用要件（認証プロファイル）の 1 つである MICS (Member Integrated Credential Services) プロファイルに準拠しており，HPCI 認証局は MICS 運用要件を満たす認証局として，平成 26 年 8 月に IGTF の認定を受けている。

HPCI 認証局では，CP/CPS に準拠すなわち MICS 運用要件を満たす運用がなされているか，年 1 回の内部監査を行う。平成 29 年度は，7 月下旬に内部監査の実施を各機関へ依頼し，対象の全機関から回答をいただいた。最寄りセンター向けの内部監査において本人確認書類の取扱いに関する問題，課題参加者の HPCI アカウントを管理するプライマリセンター向けではアカウントのライフサイクルに関する問題が確認され，現在は当該機関と協力しつつ改善に向けて検討を進めている。

HPCI 認証局自身の自己監査において，HPCI 認証局で独自に用意して IGTF にも共有したチェックリストをこれまで使用してきたが，今回からは IGTF で検討が始まった MICS CA 向けチェックリストを利用して自己監査を実施した。平成 29 年 10 月に開催される

APGridPMA Face-to-Face Meeting において監査結果を報告する予定である。

4.3 NAREGI-CA

NAREGI-CA ソフトウェア [9] は，認証局において電子証明書を発行するためのソフトウェアである。NAREGI-CA は，認証局の構築に必要な暗号ライブラリを包含し，現時点の推奨ハッシュ関数である SHA-2 族を実装しており，SHA-2 を利用する電子証明書の発行を可能とし，HPCI のような国家規模の高性能分散計算環境での利用をいち早く推進してきた。米国国立技術標準研究所 (NIST) は，次世代ハッシュ関数 SHA-3 のアルゴリズムを選定した後，3 年をかけて SHA-3 の標準技術仕様書を平成 27 年 8 月に公開した。また，平成 28 年 3 月には我が国の電子政府推奨暗号の安全性を評価・監視し，暗号技術を調査・検討するプロジェクトである CRYPTREC の策定する「推奨候補暗号リスト」に SHA-3 関数族が加わった。SHA-1 の危殆化（違う文書が同一のハッシュ値を出力してしまう衝突など）が現実的な問題となった昨今，SHA-3 ハッシュ関数族を利用するアプリケーションの実装ならびに動作検証を実施すべき段階に入ったと言える。

以上の状況を踏まえ，平成 28 年度の機能強化では，SHA-3 関数族を利用した電子署名が行えるように NAREGI-CA ソフトウェアを拡張するとともに，関連する暗号アルゴリズムの SHA-3 対応も同時に行った。本機能強化により，仮に SHA-2 の危殆化が現時的な脅威となったとしても迅速に SHA-3 への移行を検証・評価できるソフトウェア基盤が整備されたことになる。

4.4 NII による GSI 保守

Globus Toolkit[10] は，米国アルゴンヌ国立研究所およびシカゴ大学を中心とする Globus Alliance によってオープンソースソフトウェアとして開発および保守されてきたグリッドコンピューティング環境を構築するためのミドルウェアであるが，平成 30 年 1 月に Globus cloud service が依存しない機能のサポートを打ち切り，平成 30 年末までに Globus Toolkit のすべてのサポートを終了することが 2017 年 5 月 26 日（現地時間）付けでシカゴ大学から発表された。[11]

図 3 は，Globus Toolkit のサポート終了が HPCI へ及ぼす影響を示しており，赤色で示すシステムおよびプロトコルは Globus Toolkit の構成要素を利用している範囲である。GSI は，Globus Toolkit のセキュリティ機能として安全な通信と認証の仕組みを実現するものであり，HPCI 認証基盤を構成する主要技術として採用している。スーパーコンピュータへのアクセスには GSI を利用できるようにした SSH の実装である GSI-OpenSSH を利用している。共用ストレージへのアクセスは Gfarm が GSI ライブラリを利用して代理証明書による認証を実現している。証明書を集中管理する証明書リポジトリおよび代理証明書リポジトリは MyProxy で構築している。以上のとおり，Globus Toolkit のサポート終了による影響は多岐にわたる。また，代替となるソフトウェアは平成 29 年 9 月時点では提供されておらず，半年程度の短期間で HPCI の基幹を構成する技術を再構築することは非現実的と言える。オープンソースソフトウェアである Globus Toolkit のソースコードは公開されており，Globus Alliance から提供されるバイナリパッケージについても，RPM Package Manager (RPM) 形式で作成するための Source RPM (SRPM) が入手可能である。

以上の状況を踏まえ，今後の HPCI の信頼性および安定性の維持を目的として，平成 29 年 12 月から NII において必要最小限の保守を開始する。GSI，GSI-OpenSSH，MyProxy および関連する GSI ライブラリに対する脆弱性や障害への対応やセキュリティ動向を踏まえた仕様変更や機能拡張などを行うソースコード保守ならびに Red Hat Enterprise Linux，CentOS を対象としたバイナリパッケージの作成および配布を予定している。

NII での GSI の保守をいつまで継続するか，言い換えれば HPCI において GSI の利用をいつまで続けるかの検討および GSI に替わる認証技術の導入の検討は，HPCI 同様に GSI の利用を継続する欧州原子核研究機構 (CERN) の動向も確認しつつ進める必要があり，今後の継続的な課題である。

4.5 GSI-SSHTerm

HPCI において計算資源にアクセスするための推奨仮想端末ソフトウェアのひとつとして GSI-SSHTerm（NII 改修版）があり，NII では必要に応じて独自の改修を実施している。

平成 28 年 4 月に実施された「京」へのログイン用 GSI-OpenSSH サーバにおいて利用可能なメッセージ認証コードおよび Cipher（ブロック暗号および暗号利用モードの組み合わせ，ストリーム暗号）を高度化する設定変更および平成 28 年 9 月の Globus Toolkit 6.0 のアップデートにより，GSI-SSHTerm を使用して標準的な設定の GSI-OpenSSH サーバにサインオン

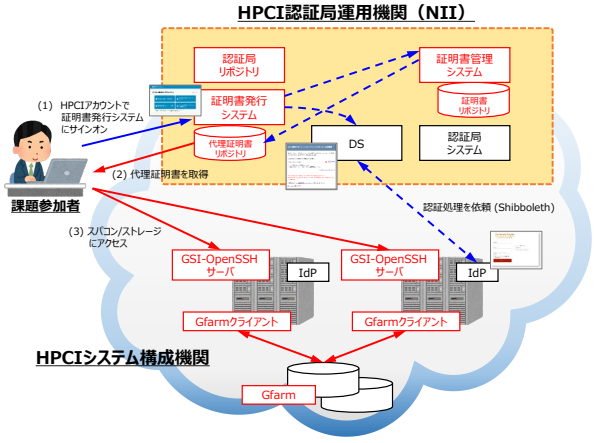

図 3　Globus Toolkit サポート終了の影響範囲

できない事象への対応ならびに HPCI へのアクセス環境の安全性強化を図る目的として，メッセージ認証コードは HMAC-SHA2-256，Cipher については，ブロック暗号は鍵長 128 ビット，192 ビットおよび 256 ビットの AES，暗号利用モードは CTR と CBC が利用できるよう，他の GSI-SSHTerm 実装に先行して改修を行い，GSI-SSHTerm 0.91i-nii6 として平成 29 年 2 月に公開した。[12]

GSI-SSHTerm の仮想端末上において，Emacs を利用する際のメタキーとして ESC キーが利用できないという事象が平成 27 年 2 月に報告されている。具体的な事例として「ESC キー＋ W キー」の操作を行うと入力内容とは異なる意図しない振る舞いをすることが確認されている。ESC キーによるメタキーの代替として「Ctrl キー＋ [キー」の操作もしくは ESC キーと組み合わせたコンビネーションキー入力時は ESC キーを 2 回押下することを回避策として案内している。平成 27 年 4 月には，GSI-SSHTerm の仮想端末上において，サーバから UTF-8 の文字符号化方式で日本語文字が送られて来た際に正しく表示ができないことが報告されている。GSI-SSHTerm は，日本語非対応の文字符号化方式 (Latin-1) を使用しており，UTF-8 などで日本語文字が送られてきても正しく扱えないこと，さらに Microsoft Windows プラットフォームにおいては日本語文字に対応していないフォントの使用が指定されていることなどが NII での調査により判明している。

平成 29 年 9 月現在，これらの問題解決を目的とする改修を行っており，GSI-SSHTerm の仮想端末上におけるキー入力イベントの実装を強化するとことで慣れない操作による不便を強いている状態の解消，日本語文字を正しく扱えるようにすることで管理者からのメッセージに日本語を使用できるなどの利便性向上も期待される。

5　おわりに

本稿では，HPCI 認証基盤の運用において発生した課題とその解決策等の報告を行った。今後もシステムの安定運用を継続し，安全な認証基盤の提供ができるよう，日々取り組んでいく所存である。

謝辞

HPCI 認証基盤の活動に対する HPCI 連携サービス運営・作業部会メンバーの方々のご理解，ご協力に感謝申し上げます。

参考文献

[1] 革新的ハイパフォーマンス・コンピューティング・インフラ (HPCI) の構築について, http://www.mext.go.jp/a_menu/kaihatu/jouhou/hpci/1307375.htm

[2] Von Welch, Frank Siebenlist, Ian Foster, John Bresnahan, Karl Czajkowski, Jarek Gawor, Carl Kesselman, Sam Meder, Laura Pearlman, Steven Tuecke, “Security for Grid Services”, in Proc. of the 12th IEEE International Symposium on High Performance Distributed Computing, 2003.

[3] R.L. Morgan, Scott Cantor, Steven Carmody, Walter Hoehn, Kenneth Klingenstein, “Federated Security: The Shibboleth Approach”, EDUCAUSE Quarterly, Vol.27, No.4, 2004.

[4] 合田 憲人, 坂根 栄作, 本山 一隆, 青木 道宏, 漆谷 重雄, “HPCI のためのネットワーク・認証基盤”, 大学 ICT 推進協議会 2013 年度年次大会論文集, 2013.

[5] 石井 宏治, 坂根 栄作, 合田 憲人, “HPCI 認証基盤の活動報告”, 大学 ICT 推進協議会平成 28 年度年次大会論文集, 2016.

[6] UPKI 電子証明書発行サービス, https://certs.nii.ac.jp/

[7] 坂根 栄作, 合田 憲人, 本山 一隆, “HPCI 認証局の現在とこれから”, 大学 ICT 推進協議会 2014 年度年次大会論文集, 2014.

[8] IGTF: Interoperable Global Trust Federation, http://www.igtf.net/

[9] NAREGI-CA development, http://ca-dev.

naregi.org/

[10] Globus Toolkit, http://toolkit.globus.org/toolkit/

[11] Vas Vasiliadis, "Support for Open Source Globus Toolkit Ends January 2018", https://www.globus.org/blog/support-open-source-globus-toolkit-ends-january-2018

[12] GSI-SSHTerm, https://www.hpci.nii.ac.jp/software/GSI-SSHTerm_0.91i_nii6.html