HPCI 認証基盤における Oracle Java SE サポート・ロードマップへの対策

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

Measures against Oracle Java SE Support Roadmap in HPCI authentication infrastructure

Koji Ishii, Eisaku Sakane, Kento Aida

National Institute of Informatics

概要

国立情報学研究所は，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担っている。HPCI 認証基盤の運用において発生した諸問題とその解決策，特に 2017 年 9 月に発表され，全面的な方針転換となる Oracle Java SE サポート・ロードマップへの対策を中心として報告する。

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，全国の大学や研究機関（HPCI システム構成機関）に設置・資源提供されているスーパーコンピュータやストレージを連携し，産業界を含めた幅広い利用者層の多様なニーズに応える共用計算環境基盤を実現するものである。2017 年 4 月からの第 2 期 HPCI においても，ネットワーク上に分散した計算資源や Web 上のサービス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）の提供を継続するため，国立情報学研究所 (NII) と 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 HPCI の供用開始当初から引き続き担当している。

HPCI 認証基盤は，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，課題参加者の認証情報を管理する Shibboleth Identity Provider (IdP) サーバ，スーパーコンピュータやストレージなどの計算資源へのログインノードとなる GSI-SSH サーバにより構成されている。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 上のサービス利用時には IdP のアカウント情報による Shibboleth 認証が，計算資源の利用時には HPCI 認証局が発行する電子証明書を用いた GSI 認証が，それぞれ行われる。[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) の一員として HPCI 認証局および関連システム等の運用を担当する他，HPCI 認証基盤に関連するソフトウェア開発や 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]

これまで HPCI 認証基盤を運用するなかで顕在化した大きな問題の 1 つに，2017 年 9 月に発表された Oracle Java SE サポート・ロードマップ [6] による Oracle の Java Platform, Standard Edition (Java SE) プロダクトの全面的な方針転換が挙げられる。Java 実行環境を必要とするソフトウェアを利用する HPCI 認証基盤への影響は小さなものではなく，現行を代替えする Java 実行環境への移行を迫られている。

本稿では HPCI 認証基盤の運用に関して，その諸問題と解決策などを交えつつ報告する。2 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等について述べる。3 節では HPCI 認証基盤における今後の Java 実行環境を含むソフトウェア環境を検討する。

2 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とソフトウェア開発に関わる近年のトピックを報告する。

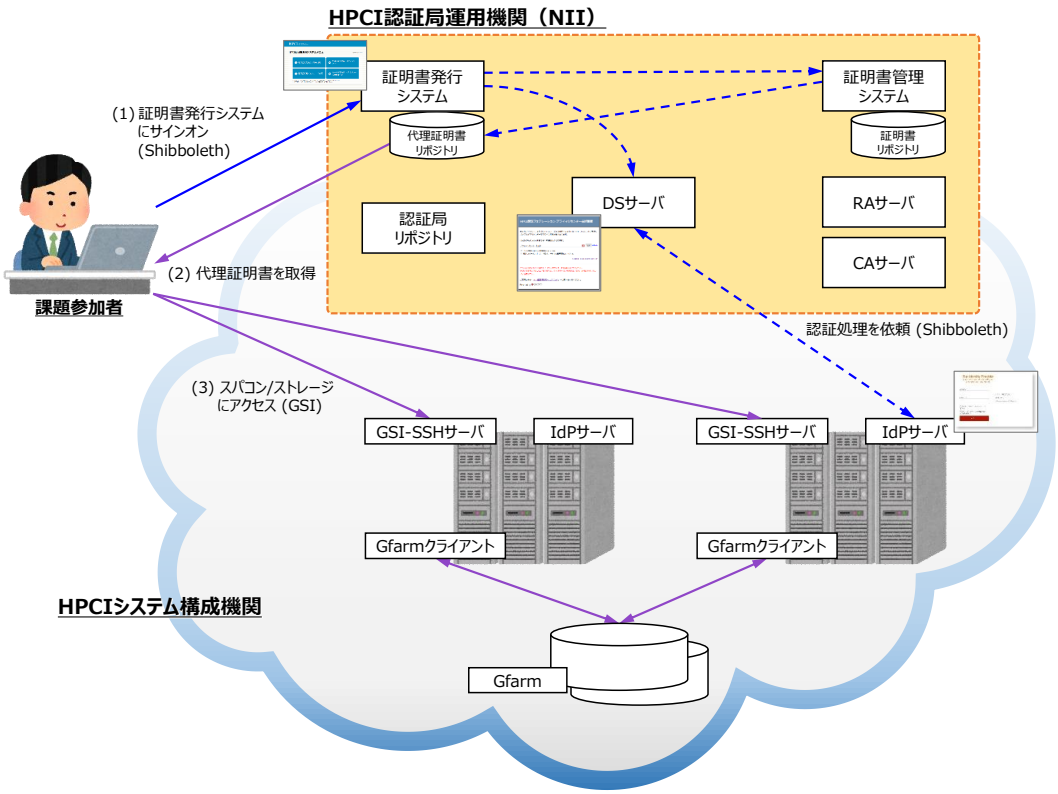

図 1　HPCI 認証基盤の構成とシングルサインオン手順

表 1　HPCI 認証基盤システム

システム名	主な役割
CA サーバ	電子証明書の発行および失効
RA サーバ	電子証明書発行および失効の処理受付
認証局リポジトリ	認証局に関する情報公開
証明書管理システム・証明書リポジトリ	発行済み電子証明書の管理， 電子証明書とローカルアカウントのマッピング情報管理
証明書発行システム・代理証明書リポジトリ	電子証明書発行のためのユーザインタフェース， 代理証明書の管理
DS サーバ	Shibboleth IdP 選択サービス

2.1　認証基盤システムの更新

HPCI 認証基盤システムは表 1 に掲げるサーバ群から構成されている。これらに冗長化のための待機システムを加えることでシステムの堅牢性を確保している。また，提供サービスの継続的かつ安定的な運用のための可用性向上システム，システムの設定変更や改修などに伴う更新等を試験するための HPCI システム構成機関向け公開試験環境，HPCI 認証基盤の利用するソフトウェアが更新された際に本運用システムへの適用以前に検証するための機能検証環境，HPCI 認証基盤システムのサーバログの改ざん防止およびバックアップのためのログ収集システムも用意している。

2017 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構成する機器およびソフトウェアの更新を行った。[7] システム更新作業は証明書発行業務の繁忙期となる年度末を避けたスケジュールで計画し，予定通り 2017 年 12 月までに全ての作業が完了している。

2.2　HPCI 認証局

2.2.1　発行状況

HPCI 認証局は HPCI 認証基盤の中核として，課題参加者の認証のために用いられるクライアント証明書の他，HPCI 上で運用されるサーバ向けにホスト証明書およびサービス証明書を発行している。それ

ぞれ具体的には，ホスト証明書は仮想端末を提供する GSI-SSH サーバの認証のため，サービス証明書は Gfarm によるストレージサービスの認証のために利用される。

2018 年 8 月 1 日現在，HPCI 認証局における電子証明書発行枚数は表 2 に示すとおりである。クライアント証明書，ホスト証明書については，年間に発行される枚数は過去 3 年間と比較して大きな増減はないが，2017 年度にストレージサービス用機器の更新が行われた結果，その更新以前と比べてサービス証明書の有効枚数は，ほぼ倍となっている。

2.2.2 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。[8] 本 CP/CPS は，グリッド計算資源の国際連携を支援するための共通ポリシや手引きの規定団体である Interoperable Global Trust Federation (IGTF) [9] が認証局に対して要求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 2014 年 8 月に IGTF の認定を受けている。

HPCI 認証局では MICS 運用要件を満たす CP/CPS に沿った運用が確実になされているかの監査を 1 年に 1 回行うことを定めている。この監査の対象となるのは HPCI 認証局を含む HPCI 認証基盤システムを運用する NII だけではなく，HPCI 認証基盤を構成もしくは連携する各システムを運用する大学および研究機関についても監査対象としている。

2018 年度は監査の実施を 6 月上旬に各機関へ依頼した。例年よりも 1 か月以上早い時期の依頼にもかかわらず，対象の全機関から速やかに回答をいただいた。この場をお借りして御礼申し上げる。

対面認証による本人確認手続きを行う最寄りセンター向けの内部監査では一部機関における本人確認書類の取扱いに関する課題，課題参加者の認証情報を管理するプライマリセンター向けではアカウント失効などに際して通知する方法に関しての問題が確認されたが，これらについては当該機関と協力し，改善の取り組みが進められている。

HPCI 認証局自身が実施する自己監査も例年通り実施し，2019 年 3 月開催予定の APGridPMA [10] Face-to-Face Meeting にて結果を報告する予定である。

表 2　電子証明書発行枚数（2018 年 8 月 1 日現在）

証明書種別	有効数	総数
クライアント証明書	206 枚	2,541 枚
ホスト証明書	66 枚	572 枚
サービス証明書	207 枚	981 枚

2.3 NAREGI-CA ソフトウェアの機能強化

NAREGI-CA ソフトウェア [11] 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するとともに，インターネット上のピア間のセキュアな通信を可能とする TLS (Transport Layer Security) プロトコル v1.2 を実装しており，認証局を構成するサーバ間において TLS 通信を利用することにより安全性の高い通信を担保している。しかしながら昨今のソフトウェアあるいはプロトコルに対する脆弱性情報が次々と公開される現状を鑑みれば，HPCI 認証基盤を構成する要素技術は活発に研究開発が続けられており，ことに，TLS もその機能改善・拡張が積極的に検討されており，これら最新の要素技術に追従することは認証基盤の安全性を維持する上で必要不可欠である。

TLS v1.2 仕様を更新する TLS v1.3 は，2017 年度の機能強化を計画した時点では標準規格として承認はされていなかったものの，基本的な仕様はほぼ固まりつつあった。仕様が確定する前ではあったが TLS v1.3 のプロトコルおよび独立に仕様が策定されている暗号アルゴリズムの両方をそれぞれ実装することを 1 件の開発案件とした場合，2016 年度までの NAREGI-CA における実装状況等を考慮すると単年度での開発完了は難しいボリュームとなることが想定された。

以上の状況をふまえ，2017 年度の機能強化では，TLS v1.3 で必須となる新しい暗号アルゴリズム，具体的にはストリーム暗号 CHACHA20 およびワンタイム認証子 POLY1305，RSA 公開鍵暗号を用いた署名アルゴリズム RSASSA-PSS，メッセージ認証コード HMAC に基づく鍵導出関数 HKDF をそれぞれ実装した。これにより，TLS v1.3 に関連する実装のうち 1 四半期分の開発を先取りしたことになる。

2.4 NII による独自の GSI 保守

GSI 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 Globus Toolkit [12] においてセキュリティ機能を提供するもので，HPCI 認証基盤システムを構成する主要な認証・認可技術の 1 つである。しかしながら，シカゴ大学から 2017 年 5 月 26 日（現地時間）に発表 [13] されたとおり，Globus Toolkit の機能のうち Globus cloud service が依存しない構成要素であるため，GSI のサポートは 2018 年 1 月に打ち切られている。また，2018 年末には Globus Toolkit の全てのサポートが終了となる。

Globus Toolkit のサポート終了，特に GSI に関する影響は，HPCI の構成要素において多岐にわたるうえ [7]，HPCI の基幹部分である認証・認可機構を半年程度で再構築することは事実上不可能であることから，オープンソースソフトウェアとして公開されている Globus Toolkit のソースコードに基づく脆弱性・障害対応，また必要に応じて仕様変更・機能拡張を行い，それらの成果の国際連携や Red Hat Enterprise Linux (RHEL) 6 および 7（それらの互換 OS を含む。）を対象としたバイナリパッケージの作成・配布を一貫して行える NII 独自の保守管理体制を構築，次期 HPCI システム更新までの HPCI 認証基盤の安全性を維持できる必要最低限の環境を整備した。

2018 年度もソフトウェア保守管理体制を維持しており，随時の対応を行っている。GSI を利用できるようにした SSH の実装である GSI-OpenSSH において利用可能な Cipher（ブロック暗号および暗号利用モードの組み合わせ）のうち，aes192-ctr, aes256-ctr のどちらかを利用すると GSI-SSH サーバでの認証に失敗するという問題があった。GSI-OpenSSH の設定ファイル (/etc/gsissh/sshd_config) のディレクティブ DisableMTAES の項目値に yes を設定することで問題を一時的に回避することはできるが，Globus Toolkit における GSI-OpenSSH のパッケージ gsi-openssh-server が Globus Alliance による Version 7.3p1c-1 である場合，DisableMTAES ディレクティブ自体が存在しないため新規に追加する必要がある。ソースコードの精査により，GSI-OpenSSH に取込まれたパッチの不整合が，この問題の原因と判明している。当該パッチに対する修正と技術な裏付けを進め，GSI を利用するコミュニティへも共有していく予定である。

2.5 GSI-SSHTerm の機能強化

HPCI において課題参加者が計算資源にシングルサインオンする際の推奨仮想端末ソフトウェアの 1 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行っている。平成 29 年度は，HPCI において GSI-SSHTerm を利用する際の作業効率性を向上させる機能強化を実施した。

GSI-SSHTerm は，もともと欧米で開発されたソフトウェアであるためか日本語の表示は考慮されておらず，HPCI の課題参加者または管理者が日常的に利用するアプリケーションにおいて研究開発または管理業務の効率性を下げる GSI-SSHterm に起因する不具合がいくつか確認されていた。[7] これらの問題解決のため，GSI-SSHTerm の実装における不具合修正および使用上の制限緩和，日本語を含む取扱可能文字種拡充およびキー入力イベントの実装強化の改修を行い，GSI-SSHTerm 0.91i-nii7 として 2017 年 2 月に公開した。[14]

2.6 証明書発行システムの機能強化

証明書発行システムは，課題参加者向けのクライアント証明書の発行や利用および管理者向けのホスト証明書およびサービス証明書の発行申請をオンライン操作で行うための Web アプリケーションである。

2017 年度から HPCI の利用研究課題は年 2 回の募集となり，毎年 4 月に開始して年度末に終了となる従来の課題実施期間（A 期）の他に，10 月から翌年 9 月末までの課題実施期間（B 期）が追加された。[7]

これまでの証明書発行システムは，HPCI の利用研究課題の募集が年 1 回の A 期のみであることを前提として，課題参加者向けに有効期間が「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が，課題参加者を対象に 1 年に 1 回発行するクライアント証明書の有効期間が前述のままでは，B 期の開始から約半年後に有効期限切れとなり，B 期の課題参加者は実施期間の途中でクライアント証明書の更新を強いられることになる。

この問題への対応として，有効期間を発行後 395 日間と日数指定するクライアント証明書の発行が可能となるよう証明書発行システムを改修した。この改修の結果，クライアント証明書の有効期間満了日は，これまでの全課題参加者で一律の毎年 4 月 24 日から，それぞれのクライアント証明書の発行日から起算の日付となるため，クライアント証明書が有効期限切れを迎える以前に電子メールで課題参加者個別に有効期間満了日を通知と再発行の依頼をするための機能を追加した。これらの機能強化により，課題参加者の管理負担を軽減した。

3 Oracle Java SE サポート・ロードマップへの対策

本節では，HPCI 認証基盤における Java の利用状況ならびに Java に対する要件を再確認したうえで，2017 年 9 月に発表された Oracle Java SE サポート・ロードマップから受ける影響について述べる。続いて，代替えの選択肢となる Java 実行環境について評価を行った後，HPCI 認証基盤が採るべき対策について論じる。

3.1 HPCI 認証基盤と Java

2018 年 8 月現在，HPCI 認証基盤において Java 実行環境を必要とするソフトウェアは，HPCI システム構成機関が運用する IdP サーバのための Shibboleth IdP ならびに課題参加者が使用する GSI-SSHTerm の 2 つである。ここでの Java 実行環境とは，Java Platform, Standard Edition (Java SE) 仕様に準拠したソフトウェア実装および実行環境のことを指す。

HPCI 認証基盤において指定する IdP サーバの動作環境は表 3 に示すとおりである。IdP サーバには，Shibboleth Consortium が提供する Shibboleth IdP Version 3 を採用しており，この Java 実行環境に Oracle Java SE Development Kit (Oracle JDK) 8 を指定する理由は，Shibboleth IdP Version 3 が Java 7 または 8 プラットフォーム向けに開発され，システム要件として，JRE (Java Runtime Environment) ではなく JDK (Java Development Kit) のみが正式にサポートされること，Oracle の標準 JVM を使用することが強く推奨されてきた [15] ためである。しかしながら 2018 年 8 月現在では，Shibboleth IdP Version 3 がサポートする Java 実行環境に OpenJDK [16] も含まれることを確認している。

GSI-SSHTerm 0.91i-nii7 の動作確認済環境は表 4 に示すとおりである。GSI-SSHTerm は，課題参加者が様々な環境下において利用することを想定しており，複数の OS 上で動作するように実装されている。課題参加者の負担を考慮すると，導入の容易さはもとより極力少ない費用で入手および利用できることが望ましく，長期的なサポートの提供が不可欠であることは言うまでもない。Java 実行環境については，Windows 版ではインストーラが付属し，macOS および RHEL のパッケージ管理ツールに対応する Oracle の Java SE プロダクト (Oracle Java) の他，RHEL のパッケージ管理ツールから導入可能な OpenJDK を動作確認対象としている。

表 3　HPCI 認証基盤における IdP サーバの動作環境

OS	RHEL 6 (x86_64, i386), RHEL 7 (x86_64), もしくは上記の互換 OS
IdP サーバ	Shibboleth IdP Version 3
Java 実行環境	Oracle JDK 8
Servlet コンテナ	Apache Tomcat 9.0

表 4　GSI-SSHTerm 0.91i-nii7 の動作確認済環境

OS	Java 実行環境
Windows 10 (64bit)	Oracle Java 8
macOS Sierra	Oracle Java 8
CentOS 7 (x86_64)	Oracle Java 8, OpenJDK 8 (Red Hat)

3.2 ロードマップ変更の影響

2017 年 9 月に Oracle が発表した Oracle Java SE サポート・ロードマップが及ぼす HPCI 認証基盤への最も大きな影響として挙げられるのは，HPCI の基幹部分である認証・認可機構を構成する IdP サーバおよび課題参加者が利用する GSI-SSHTerm が Java 実行環境として利用してきた Oracle Java 8（Oracle JDK 8 および Oracle JRE 8）は，2019 年 1 月に無償でのサポートが終了（例外として，非営利目的かつ非商用の個人利用に限り 2020 年 12 月までアップデートが提供される。）という点である。また，有償でのサポートは 2025 年 3 月まで継続される。

このロードマップでは，サポートポリシーが全面変更され，2017 年 9 月にリリースの Oracle Java 9 以降は，新機能を順次取込んだバージョンアップとして 1 年に 2 回（毎年 3 月と 9 月）のフィーチャー・リリース（非 LTS 版）の提供，バージョン別ライフサイクルは原則半年と短期間化，Oracle Java 11 を初回として長期サポート用バージョン（LTS 版）を 3 年ごとに 1 回のリリース，LTS 版では最低でも 8 年の長期に渡ってアップデートを提供，セキュリティパッチの配布は非 LTS 版と LTS 版のどちらもサポート期間中の各バージョンを対象に 1 年に 4 回（毎年 1 月，4 月，7 月，10 月）提供，という方針となっている。

各種 OS・プラットフォームへの対応については，Oracle Java 9 以降では Windows (32bit) および Solaris (x86_64) 向けは廃止となったが，Windows 版でのインストーラの付属，macOS および RHEL のパッケージ管理ツールへの対応は継続されている。

これまで HPCI 認証基盤では，サポート終了以前に後継バージョンへ Java 実行環境を移行することで

対応してきたが，Oracle Java 8 の場合，次バージョンは非 LTS 版の Oracle Java 9 であることが問題となる。非 LTS 版は，次バージョンがリリースされた時点で直前バージョンのサポートは即時終了，つまり Oracle Java 9 は 2018 年 3 月にサポート終了済であるため，Oracle Java 8 から移行する対象には成り得えない。次々バージョンの Oracle Java 10 も非 LTS 版で，2018 年 9 月予定の Oracle Java 11 のリリースをもってサポート終了となるため同様の問題がある。また，Oracle Java 11 は，2026 年 9 月までサポートされる LTS 版が提供されるものの，Oracle Java 11 および以降のバージョンは，有償サポート契約を結んだ利用者にのみ提供するとしており，新たな費用負担が必要となる点は無視できない。

3.3 Java 実行環境の選択肢

次期 HPCI システム更新までの HPCI 認証基盤の安全性を維持するためには，Oracle Java 8 の代替えとなる Java 実行環境の導入は不可避であるが，幸いにして Oracle Java 8 のサポート終了以後に現行を置換可能な Java 実行環境の選択肢がいくつか存在する。新たな Java 実行環境を導入する計画を検討するため，第 2 期 HPCI の運用期間（2022 年 3 月末まで予定）と 2018 年 8 月時点で判明している Java 等のロードマップの関係を整理したものが図 2 である。

Java SE 仕様に基づいたプロダクトは，Oracle Java の他に，オープンソースプロジェクトによる OpenJDK がある。OpenJDK は，GNU General Public License (GNU GPL) バージョン 2（GPL リンク例外つき）でライセンスされており，OpenJDK のソースコードをビルドしたバイナリの提供元は複数存在する。

本小節では，一般向けに無償で提供されている OpenJDK バイナリとして，Oracle によるビルド，Red Had によるビルドおよび AdoptOpenJDK プロジェクトによるビルドのそれぞれを，提供形態やサポートの内容，OS・プラットフォームへの対応状況などの観点から比較する。

3.3.1 OpenJDK (Oracle)

OpenJDK プロジェクトが一般向けに公開しているのは，OpenJDK 8 以前ではソースコードのみであったが，OpenJDK 9 以降は Windows, macOS, Linux 向け（いずれも x86_64）のバイナリを無償にて提供している。これらのバイナリは Oracle がビルドしてテストを行ったもので，2018 年 8 月現在では，OpenJDK 10 が一般向けに提供されている。いずれのプラットフォーム向けも tar.gz 形式での配布であるため，Windows 環境ではアーカイブの展開にサードパーティのソフトウェアが必要となるうえ，インストーラ等も付属しない。macOS 版，Linux 版においてもパッケージ管理ツールに非対応となっている。[17]

これまで Oracle が有償で提供してきた Oracle JDK の機能（Java Flight Recorder など）の OpenJDK への統合が進められており，OpenJDK 11 以降では，Oracle JDK と Oracle がビルドする OpenJDK の機能的な差異は無くなる。

OpenJDK 9 以降のリリースタイミングは，Oracle Java と同様の毎年 3 月と 9 月に固定され，セキュリティパッチの開発は Oracle が担当しており，Oracle Java と同じく 1 年に 4 回（1 月，4 月，7 月，10 月）提供される。Oracle がビルドする OpenJDK は，半年ごとのリリースの度に直前バージョンのサポートが即時終了かつ Oracle Java のような長期サポートは提供されないため，バージョン間の移行期間が無い点には注意が必要である。

3.3.2 OpenJDK (Red Hat)

Red Hat による独自の実装を含む OpenJDK として，2018 年 8 月現在ではバージョン 8 および 10 のソースコードと Windows 用バイナリ (x86_64, i586) が Red Hat の開発者プログラム登録者を対象に提供されている。[18] これらのうち，サポート対象となるのは OpenJDK 8 の Windows 用バイナリ (x86_64) のみである。

RHEL のパッケージリポジトリから入手可能な OpenJDK の RPM パッケージには Red Hat 独自の長期サポート期間が設定されており，OpenJDK 8 に関しては 2020 年 10 月までサポートされる。[19] Red Hat は Oracle Java 8 の後継として OpenJDK 11 の利用を推奨しており，Red Hat からの具体的なリリース時期は公表されてはいないものの，RHEL 7 を対象プラットフォームとして長期間サポートの提供が予告されている。

GSI-SSHTerm の動作環境の 1 つである macOS に対応するバイナリは提供されていない。

3.3.3 AdoptOpenJDK

AdoptOpenJDK [20] は，OpenJDK バイナリを各種プラットフォーム向けに提供するプロジェクトである。2018 年 8 月現在，OpenJDK 8 については，Windows (x86_64), macOS (x86_64), Linux (x86_64, s390x, ppc64le, aarch64)，AIX (ppc64) 向けのビルドが用意されている。配布のバイナリには，いずれの

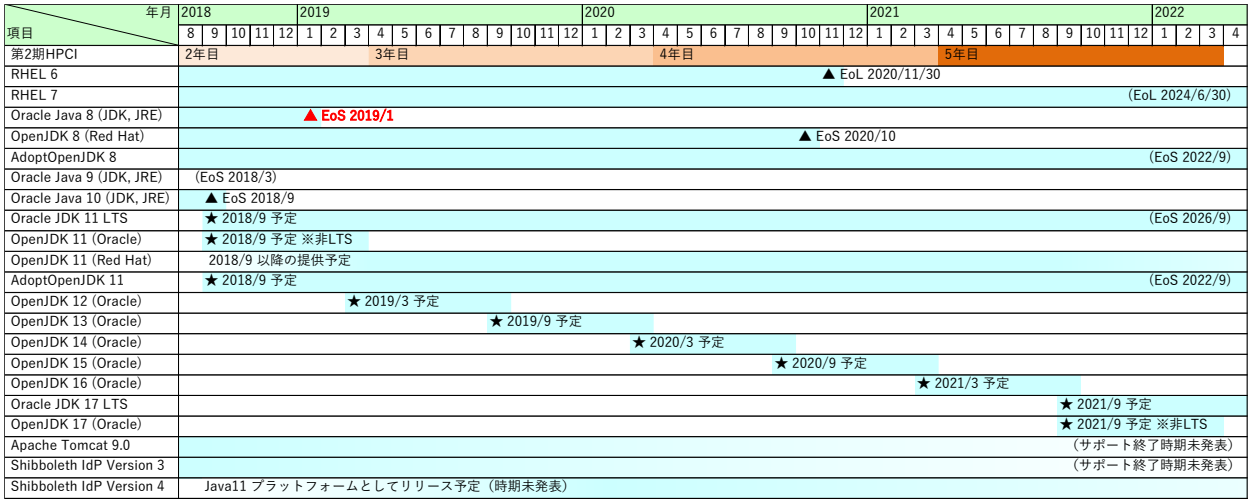

図 2　第 2 期 HPCI の運用期間と Java 等のロードマップ

プラットフォーム向けにもインストーラ等は付属せず，パッケージ管理ツールにも非対応となっている。

AdoptOpenJDK では，プロジェクト独自に無償の長期サポート用バージョン（LTS 版）をリリースしており，OpenJDK 8 に関しては，OpenJDK 11 またはそれ以降のバージョンへの移行を目的として 2022 年 9 月までサポートが提供される。[21] OpenJDK 11 についても LTS 版として，2018 年 9 月の提供開始，2022 年 9 月までのアップデートが予告されている。

3.4　今後のソフトウェア環境の検討

前小節で比較した各提供元による OpenJDK バイナリおよび Oracle Java のうち，長期間かつバージョン間の移行を考慮したサポートが無償で提供されるのは，Red Hat による OpenJDK と AdoptOpenJDK である。また，Windows，macOS および Linux の全てに対応するのは Oracle Java と AdoptOpenJDK である。

これらの状況を前提として，本小節では，HPCI 認証基盤において Java 実行環境を必要とする IdP サーバと GSI-SSHTerm のそれぞれにおける，Oracle Java 8 のサポート終了以後に採用すべきソフトウェア環境を検討する。

3.4.1　IdP サーバ

IdP サーバである Shibboleth IdP Version 3 は，Java 7 または 8 プラットフォーム向けに開発されており，Oracle JDK および OpenJDK の両方に対応している。2018 年 8 月時点では，Shibboleth IdP Version 3 のサポート終了期日および Java 11 を推奨プラットフォームとするとされる次期バージョン (Shibboleth IdP Version 4) のリリース時期は発表されていない。

2018 年 7 月にプライマリセンター向けのアンケートを行ったところ，2018 年 12 月時点で IdP サーバに RHEL 6 または 7（およびそれらの互換 OS）以外の OS を使用する機関は無い見込みとの結果が得られた。

以上の状況をふまえ，Oracle JDK 8 がサポート終了となる 2019 年 1 月までに 表 3 の IdP サーバの動作環境から Java 実行環境を Red Hat が提供する OpenJDK 8 へ移行するための計画を立案中である。

OpenJDK 8 に対する Red Hat のサポートが終了する 2020 年 10 月は，第 2 期 HPCI の運用期間の途中であるため，以後の対応は今後の検討課題である。Oracle Java 8 の後継として Red Hat が推奨する OpenJDK 11 に関して，2018 年 8 月時点では RHEL 6 向けの提供予定に関して言及が無いことから，IdP サーバとして Shibboleth IdP Version 3 を RHEL 6 上で運用している場合，2020 年 10 月よりも早い時期に Shibboleth IdP Version 3 のサポート終了期日を迎えることとなった際には，Shibboleth IdP Version 4 への移行と同時に OS および Java 実行環境の移行も必要となる可能性がある点には注意が必要である。

3.4.2　GSI-SSHTerm

OpenJDK 11 のリリースが予定されている 2018 年 9 月から Oracle Java 8 のサポートが終了する 2019 年 1 月までの短期間で GSI-SSHTerm を OpenJDK 11 に対応させるための改修を終えることは現実的ではないことに加えて，次期 HPCI システムにおける認証・認可技術として GSI を採用するかは不透明であることから Java の新機能に追従していくことは難しい状況であるため，2018 年 8 月時点では，GSI-SSHTerm の OpenJDK 11 または以降のバージョンへの対応は

行わない方針とし，現在の OpenJDK 8 への対応を拡大して，マルチプラットフォーム対応かつ第 2 期 HPCI の運用期間以後も無償でのサポートが継続される AdoptOpenJDK 8 を GSI-SSHTerm の動作確認済リストに加える予定である。また，RHEL 6 および 7（それらの互換 OS を含む。）では，OS または Red Hat が提供する OpenJDK 8 のそれぞれがサポートされる期間において動作環境として扱う。

4 おわりに

本稿では，HPCI 認証基盤の運用において発生した諸問題とその解決策等の報告を行った。特に独立したトピックとして取り上げた，Oracle Java のロードマップ変更に対する HPCI 認証基盤の対策の内容が皆様のお役に立てば幸いである。今後もシステムの安定運用を維持し，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 認証基盤の安定的なサービス提供に対する 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] “Oracle Java SE サポート・ロードマップ”, https://www.oracle.com/technetwork/jp/java/eol-135779-ja.html

[7] 石井 宏治, 坂根 栄作, 合田 憲人, “HPCI 認証基盤の運用における課題とその解決策”, 大学 ICT 推進協議会平成 29 年度年次大会論文集, 2017.

[8] 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.

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

[10] Asia Pacific Grid Policy Management Authority, http://www.apgridpma.org/

[11] NAREGI-CA development, https://ca-dev.naregi.org/

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

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

[14] “HPCI 向けソフトウェア”, https://www.hpci.nii.ac.jp/software/index.html

[15] “SystemRequirements - Identity Provider 3 - Shibboleth Wiki”, https://wiki.shibboleth.net/confluence/display/IDP30/SystemRequirements

[16] OpenJDK, http://openjdk.java.net/

[17] “JDK 10 General-Availability Release”, http://jdk.java.net/10/

[18] “Red Hat Developer — OpenJDK Overview”, https://developers.redhat.com/products/openjdk/overview/

[19] “OpenJDK ライフサイクルおよびサポートポリシー”, https://access.redhat.com/ja/articles/1457743

[20] AdoptOpenJDK, https://adoptopenjdk.net/

[21] “Support — AdoptOpenJDK”, https://adoptopenjdk.net/support.html