Red Hat build of OpenJDK 11

Red Hat build of OpenJDK 11.0.21 のリリースノート

Last Updated: 2024-05-10

Red Hat build of OpenJDK 11 Red Hat build of OpenJDK 11.0.21 のリリースノート

法律上の通知

概要

Red Hat build of OpenJDK 11.0.21 のリリースノート では、Red Hat build of OpenJDK 11 の新機能の概要と、潜在的な既知の問題と考えられる回避策のリストを提供します。

目次

はじめに 3

RED HAT BUILD OF OPENJDK ドキュメントへのフィードバック 4

多様性を受け入れるオープンソースの強化 5

第1章 RED HAT BUILD OF OPENJDK のサポートポリシー 6

第2章 アップストリームの OPENJDK 11 との相違点 7

第3章 RED HAT BUILD OF OPENJDK の機能 8

3.1. RED HAT BUILD OF OPENJDK の新しい機能と機能拡張 8

3.2. RED HAT BUILD OF OPENJDK の非推奨機能 9

第4章 このリリースに関連するアドバイザリー 11

はじめに

Open Java Development Kit (OpenJDK) は、Java Platform Standard Edition (Java SE) のオープンソース実装です。Red Hat build of OpenJDK には、8u、11u、17u の 3 つのバージョンがあります。

Red Hat build of OpenJDK 向けパッケージは、Red Hat Enterprise Linux および Microsoft Windows で利用でき、Red Hat Ecosystem Catalog の JDK および JRE として同梱されています。

RED HAT BUILD OF OPENJDK ドキュメントへのフィードバック

エラーを報告したり、ドキュメントを改善したりするには、Red Hat Jira アカウントにログインし、課題を送信してください。Red Hat Jira アカウントをお持ちでない場合は、アカウントを作成するように求められます。

手順

1. 次のリンクをクリックして **チケットを作成します**。
2. **Summary** に課題の簡単な説明を入力します。
3. **Description** に課題や機能拡張の詳細な説明を入力します。問題があるドキュメントのセクションへの URL を含めてください。
4. **Submit** をクリックすると、課題が作成され、適切なドキュメントチームに転送されます。

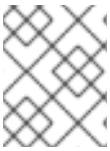
多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、Red Hat CTO である Chris Wright のメッセージ を参照してください。

第1章 RED HAT BUILD OF OPENJDK のサポートポリシー

Red Hat は、Red Hat build of OpenJDK の一部のメジャーバージョンを製品でサポートします。一貫性を保つために、これらのバージョンは、Oracle が Oracle JDK 向けに長期サポート (LTS) を指定しているバージョンと同じになります。

Red Hat build of OpenJDK のメジャーバージョンは、最初に導入された時点から少なくとも 6 年間サポートされます。詳細は、OpenJDK のライフサイクルおよびサポートポリシー を参照してください。



注記

RHEL 6 のライフサイクルは 2020 年 11 月に終了します。このため、Red Hat build of OpenJDK は、サポート対象の設定として RHEL 6 をサポートしていません。

第2章 アップストリームの OPENJDK 11 との相違点

Red Hat Enterprise Linux (RHEL) の Red Hat build of OpenJDK には、OpenJDK のアップストリームディストリビューションの構造上の変更が数多く含まれています。Red Hat build of OpenJDK の Microsoft Windows バージョンは、RHEL の更新にできる限り従います。

次のリストは、Red Hat build of OpenJDK 11 の最も注目すべき変更点を詳しく示しています。

- FIPS のサポート。Red Hat build of OpenJDK 11 は、RHEL が FIPS モードであるかどうかを自動的に検出し、Red Hat build of OpenJDK 11 がそのモードで動作するように自動的に設定します。この変更は、Microsoft Windows 向けの Red Hat build of OpenJDK ビルドには適用されません。

- 暗号化ポリシーのサポート。Red Hat build of OpenJDK 11 は、RHEL から有効な暗号化アルゴリズムとキーサイズの制約のリストを取得します。これらの設定コンポーネントは、トランスポート層セキュリティー (TLS) 暗号化プロトコル、証明書パス検証、および署名された JAR によって使用されます。さまざまなセキュリティープロファイルを設定して、安全性と互換性のバランスをとることができます。この変更は、Microsoft Windows 向けの Red Hat build of OpenJDK ビルドには適用されません。

- RHEL の Red Hat build of OpenJDK は、アーカイブ形式のサポート用の **zlib**、イメージのサポート用の **libjpeg-turbo**、**libpng**、**giflib** などのネイティブライブラリーと動的にリンクします。また、RHEL はフォントのレンダリングと管理のために、**Harfbuzz** および **Freetype** に対して動的にリンクします。

- **src.zip** ファイルには、Red Hat build of OpenJDK に同梱されるすべての JAR ライブラリーのソースが含まれています。

- RHEL の Red Hat build of OpenJDK は、タイムゾーン情報のソースとして、システム全体のタイムゾーンデータファイルを使用します。

- RHEL の Red Hat build of OpenJDK は、システム全体の CA 証明書を使用します。

- Microsoft Windows の Red Hat build of OpenJDK には、RHEL で利用可能な最新のタイムゾーンデータが含まれています。

- Microsoft Windows の Red Hat build of OpenJDK は、RHEL から入手可能な最新の CA 証明書を使用します。

関連情報

- システムが FIPS モードであるかどうかの検出の詳細は、Red Hat RHEL Planning Jira の システム FIPS 検出の改善 の例を参照してください。

- 暗号化ポリシーの詳細については、Using system-wide cryptographic policies を参照してください。

第3章 RED HAT BUILD OF OPENJDK の機能

最新の Red Hat build of OpenJDK 11 リリースには、新機能が含まれる可能性があります。さらに、最新リリースは、以前の Red Hat build of OpenJDK 11 リリースに由来する機能を強化、非推奨、または削除する可能性があります。

注記

その他の変更点やセキュリティー修正は、OpenJDK 11.0.21 Released を参照してください。

3.1. RED HAT BUILD OF OPENJDK の新しい機能と機能拡張

Red Hat build of OpenJDK 11.0.21 リリースが提供する新しい機能と機能拡張について理解するには、以下のリリースノートを参照してください。

TLS Diffie-Hellman のデフォルトのグループサイズが増加しました
Red Hat build of OpenJDK 11.0.21 では、Transport Layer Security (TLS) 1.2 の JDK 実装は、デフォルトの Diffie-Hellman キーサイズである 2048 ビットを使用します。これは、デフォルトの Diffie-Hellman キーサイズが 1024 ビットであった以前のリリースの動作を置き換えるものです。

これは、**TLS_DHE** 暗号スイートがネゴシエートされ、クライアントまたはサーバーのいずれかが Finite Field Diffie-Hellman Ephemeral (FFDHE) パラメーターをサポートしない場合にかかわってくる拡張機能です。JDK TLS 実装は FFDHE をサポートします。FFDHE、デフォルトで有効になっており、より強力なキーサイズをネゴシエートできます。

回避策として、**jdk.tls.ephemeralDHKeySize** システムプロパティーを **1024** に設定することで、以前のキーサイズに戻すことができます。リスクを軽減するためには、デフォルトのキーサイズである 2048 ビットを使用することを検討してください。

注記

TLS 1.3 はすでに 2048 ビットの最小 Diffie-Hellman キーサイズを使用しているため、この変更の影響は受けません。

JDK-8301700 (JDK Bug System) を参照してください。

サーバー側の暗号スイート設定がデフォルトで使用されるようになりました
Red Hat build of OpenJDK 11.0.21 では、SunJSSE プロバイダーがデフォルトでローカルのサーバー側の暗号スイート設定を使用します。これは、サーバーが接続クライアントが指定した設定を使用していた以前のリリースの動作に代わるものです。

サーバー側で **SSLParameters.setUseCipherSuitesOrder(false)** を使用すると、以前の動作に戻すことができます。

JDK-8168261 (JDK Bug System) を参照してください。

PKCS#1 形式の RSA 鍵がサポートされるようになりました
JDK プロバイダーが、SunRsaSign プロバイダーの RSA **KeyFactory.impl** など、PKCS#1 形式の RSA (Rivest-Shamir-Adleman) 秘密鍵および公開鍵を受け入れることができるようになりました。この機能を使用するには、RSA 秘密鍵または公開鍵オブジェクトが PKCS#1 形式であり、PKCS#1 RSA 秘密鍵および公開鍵の ASN.1 構文に一致するエンコーディングである必要があります。

JDK-8023980 (JDK Bug System) を参照してください。

-XshowSettings:locale 出力に tzdata バージョンが含まれました
Red Hat build of OpenJDK 11.0.21 では、**-XshowSettings** ランチャーオプションにより JDK が使用する **tzdata** バージョンも出力されます。**tzdata** のバージョンは、**-XshowSettings:locale** オプションの出力の一部として表示されます。

以下に例を示します。

```
Locale settings:
    default locale = English
    default display locale = English
    default format locale = English
    tzdata version = 2023c
```

JDK-8305950 (JDK Bug System) を参照してください。

Certigna ルート CA 証明書の追加
Red Hat build of OpenJDK 11.0.21 では、**cacerts** トラストストアに Certigna ルート証明書が含まれています。

- 名前: Certigna (Dhimyotis)
- エイリアス名: certignarootca
- 識別名: CN=Certigna Root CA、OU=0002 48146308100036、O=Dhimyotis、C=FR

JDK-8314960 (JDK Bug System) を参照してください。

デフォルトの java.security ファイルのロードに失敗した場合にエラーが出力されるようになりました
以前のリリースでは、**java.security** ファイルが正常にロードできなかった場合、Red Hat build of OpenJDK はハードコードされたセキュリティープロパティーのセットを使用していました。しかし、このプロパティーのセットは十分に維持管理されておらず、JDK がこれらのユーティリティーを使用していることがユーザーにはわかりませんでした。

この問題に対処するために、**java.security** ファイルが正常にロードできない場合、Red Hat build of OpenJDK 11.0.21 は代わりに **InternalError** を出力します。

JDK-8155246 (JDK バグシステム) を参照してください。

いくつかの JAAS コールバッククラスで配列が複製されるようになりました
以前のリリースでは、**ChoiceCallback** および **ConfirmationCallback** JAAS クラスで、配列がコンストラクターに渡されるとき、または返されるときに、配列が複製されませんでした。この動作により、外部プログラムがこれらのクラスの内部フィールドにアクセスできるようになっていました。

Red Hat build of OpenJDK 11.0.21 では、JAAS クラスは複製された配列を返します。

JDK-8242330 (JDK Bug System) を参照してください。

3.2. RED HAT BUILD OF OPENJDK の非推奨機能

次のリリースノートで、Red Hat build of OpenJDK 11.0.21 リリースで非推奨または削除された既存の機能を確認してください。

SECOM Trust Systems のルート CA1 証明書が削除されました

Red Hat build of OpenJDK 11.0.21 以降、**cacerts** トラストストアに SECOM Trust Systems のルート証明書が含まれなくなりました。

- エイリアス名: secomscrootca1 [jdk]
- 識別名: OU=Security Communication RootCA1、O=SECOM Trust.net、C=JP

JDK-8295894 (JDK Bug System) を参照してください。

第4章 このリリースに関連するアドバイザリー

このリリースに含まれるバグ修正と CVE 修正を文書化するために、次のアドバイザリーが発行されます。

- RHSA-2023:5734
- RHSA-2023:5735
- RHSA-2023:5736
- RHSA-2023:5737
- RHSA-2023:5739
- RHSA-2023:5740
- RHSA-2023:5741
- RHSA-2023:5742
- RHSA-2023:5743
- RHSA-2023:5744

改訂日時: 2024-05-10