

JDK 21 リリースノート (21.0.5→21.0.8) の差分調査

背景・調査方針

この調査では、非互換調査時点で使用されていた **OpenJDK 21.0.5** から、案件開始時点の **21.0.8** までの差分を確認しました。リリースノートにはテストやドキュメントのみの変更、性能改善、ガベージコレクション (GC) 関連の修正、新機能のバックポートが多数含まれますが、既存アプリケーションにクリティカルな影響が出るものを重点的に抽出するため、以下の変更は除外しました。

- **テストやドキュメントのみの変更** - issue サマリーに `open source`、`problemList`、`jtrg`、`doc` などのキーワードが含まれるもの
- **新機能／性能改善のバックポート** - issue タイプが Enhancement/New Feature で、サマリーに `Add`、`Support`、`Implement` を含むが `test` や `doc` を含まないもの
- **Windows 11 以外に限定された修正** - サマリーや説明に `Linux`、`macOS` 等の OS 名が明記されているもの
- **GC 関連の修正** - コンポーネントが `hotspot/gc`、ラベルが `gc-*`、サマリーに `Shenandoah`、`ZGC`、`G1` 等を含むもの
- **パフォーマンス改善／安定性向上のみの修正** - 既存機能の動作に影響しないもの

以下では各バージョンごとに、Windows 11 環境やアプリケーション動作に影響する可能性がある修正をまとめます。issue ID、概要、影響・備考の順に記載しています。

21.0.6 の主な変更点 (21.0.5 → 21.0.6)

ID	概要	影響・備考
JDK-8319640	<code>DateTimeFormatter</code> が内部で使用する <code>ClassicFormat</code> の <code>parseObject()</code> が仕様では「失敗時に <code>null</code> を返す」とされているのに、 <code>DateTimeException</code> を投げることがある問題を修正 ¹ ² 。	標準の <code>java.time.format.DateTimeFormatter</code> を独自ラッパーに注入しているコードで、例外処理の挙動が変わる。従来は例外がスローされましたが、修正後は <code>null</code> が返るため <code>null</code> チェックが必要です。
JDK-8320192	SHAKE256 アルゴリズムで出力サイズ <code>n</code> が 137 bit 以上の場合に正しいダイジェストを生成しないバグを修正 ³ ⁴ 。	セキュリティライブラリを利用して 256 bit SHAKE256 を使用している場合、以前のバージョンでは不正なハッシュ値を返す可能性がありました。修正により正しいハッシュが計算されます。
JDK-8320575	レコード型のコンパクトコンストラクタで宣言された必須パラメータのジェネリック型情報がリフレクションから取得できなくなるバグを修正 ⁵ 。	リフレクションやフレームワーク(例: DI/シリアライゼーション)が記録のジェネリック型を取得できず、警告や不正動作を引き起こす可能性がありました。修正により正しい型情報が返されます。

ID	概要	影響・備考
JDK-8323562	<code>SaslInputStream.read()</code> が <code>InputStream</code> の仕様では 0-255 の範囲の値を返すべきところ、負の値を返すことがある不具合を修正 ⁶ 。	SASL 認証で <code>SaslInputStream</code> を直接使用している場合、読み取り値が符号付きとして扱われ誤動作する恐れがありました。修正により正しい値が返されます。
JDK-8328723	サーバーソケット側で HTTPS エンドポイントチェックを有効にすると、ソケット接続時にクライアント証明書のサーバー名検査が実行され例外が発生する問題を修正 ⁷ 。	<code>javax.net.ssl.SSLServerSocket</code> を使用し、HTTPS エンドポイントチェックを有効にした場合にクライアント認証エラーが発生していた。修正によりサーバー側ではエンドポイント検査が行われないため正常に通信できます。
JDK-8331391	<code>keytool</code> コマンドで信頼証明書を読み込む処理 (<code>buildTrustedCerts</code>) を、 <code>-trustcacerts</code> オプション指定時にのみ行うよう変更 ⁸ 。	標準の <code>keytool -genkeypair</code> 等では従来不要な信頼証明書の読み込みが常に行われていたが、修正によりオプション指定時のみ読み込むようになりました。動作自体は既定値を変えないが、独自ツールで <code>keytool</code> をラップしている場合に挙動が変わる可能性があります。
JDK-8333317	サーバー側 ECDH ハンドシェイク中に不正な署名が送出され、TLS ハンドシェイクが失敗する問題を修正 ⁹ 。	ECDH 鍵交換を使用する TLS 接続で <code>invalid signature</code> エラーが発生する場合があります。修正によりハンドシェイクが正常に完了し、通信が可能になります。
JDK-8333427	日本語 Windows での改行コード判定テストが失敗する問題を修正 ¹⁰ 。	問題は主にテストに関連していますが、OS のデフォルトエンコーディングと改行コードの処理に関する不具合が原因であり、ファイル I/O で改行コードを扱う独自ロジックを持つ場合に影響があるかもしれません。
JDK-8337066	2 バイト文字を含む文字列に対して <code>StringBuffer.reverse()</code> を繰り返し呼び出すと逆順結果が誤ってしまう不具合を修正 ¹¹ 。	文字列操作で <code>StringBuffer.reverse()</code> を多用するアプリケーションでは、逆順処理が正しく行われない可能性があります。修正によりマルチバイト文字を含む場合でも正しい逆順が得られます。
JDK-8337331	仮想スレッドがピン留めされ、かつ <code>javaagent</code> を使用していると JVM がクラッシュする問題を修正 ¹² 。	Project Loom の仮想スレッドとエージェントを併用する場合に JVM がクラッシュすることがありました。修正により安定性が向上します。
JDK-8340812	<code>MethodHandle::updateForm</code> を介してラムダフォームを更新する処理がスレッドセーフではなく、 <code>NullPointerException</code> が発生する不具合を修正 ¹³ 。	メソッドハンドル API を動的に生成／更新するようなフレームワークで、稀に <code>NullPointerException</code> が発生する問題を修正します。
JDK-8340923	ロギング API の <code>LogSelection</code> クラスが未初期化のメモリをコピーするバグを修正 ¹⁴ 。	ログ関連の不具合で、ログ出力の初期化時に不定値が扱われる可能性があります。修正により安全に初期化されます。

ID	概要	影響・備考
JDK-8342905	<code>ForkJoinPool</code> 共通プール内のスレッドから <code>Thread.setContextClassLoader()</code> を呼び出してもクラスローダが設定されない問題を修正 ¹⁵ 。	<code>ForkJoinPool.commonPool()</code> を使用し、その内部でコンテキストクラスローダを設定しているアプリケーションでは、設定が無視されていた可能性があります。修正により意図したクラスローダがセットされます。

上記以外にも多数のテスト修正や GC・パフォーマンス改善がありますが、アプリケーションの挙動に影響する項目に絞り込みました。

21.0.7 の主な変更点 (21.0.6 → 21.0.7)

ID	概要	影響・備考
JDK-8293345	PKCS#11 プロバイダが一部のトークンでメカニズムチェックを過度に厳格に行っていたため、医療用スマートカードなどが動作しない問題を修正 ¹⁶ 。	PKCS#11 トークンを利用しているアプリケーションで、特定カードが使用できなかった現象が解消されます。セキュリティ上の機能向上ではなく、互換性向上と考えられます。
JDK-8302111	オブジェクトの直列化時に、コンストラクタで行われる検証と同じバリデーションをデシリアライズ時にも強制するように変更 ¹⁷ 。	直列化対象クラスのコンストラクタで入力値検証を行っている場合、従来はデシリアライズ時にその検証が実施されず不正な状態のオブジェクトが生成されることがありました。修正によりコンストラクタと同じチェックが行われるため、不正なストリームを読み込むと例外が発生します。バージョンアップ後に古いシリアライズデータを読み込む場合は注意が必要です。
JDK-8304701	<code>HttpClient</code> を使用し HTTP/1.1 の持続的接続で複数のリクエストを送信し、長いタイムアウトを設定した場合、タイマーが切れた際に接続を強制的に閉じてしまい、他の要求が <code>java.io.IOException: connection closed</code> となる問題を修正 ¹⁸ ¹⁹ 。	<code>java.net.http.HttpClient</code> でタイムアウトを使用しているアプリケーションでは、一つのリクエストがタイムアウトした際に次のリクエストまで影響を受けていた可能性があります。修正により、タイムアウトが発生しても他のリクエストへの接続を閉じないようにになりました。
JDK-8309841	<code>jarsigner -verify</code> で署名付き JAR にエントリを削除してもエラーが出ない問題を修正し、適切に警告を表示するように変更 ²⁰ 。	JAR を署名後に内容を変更しても検証が成功することがありました。修正により不正な JAR には警告が表示されるため、CI やビルドパイプラインでの検証結果が変わる可能性があります。
JDK-8311546	証明書の名前制約(name constraints)がドットで始まる場合(例: <code>.example.com</code>)、正しく検証できず <code>CertPathValidatorException</code> が発生するバグを修正 ²¹ 。	TLS/HTTPS の証明書検証で、特定の名称制約付き証明書を使用している場合に接続エラーとなっていたものが解消されます。

21.0.7 では主にセキュリティライブラリや HTTP クライアント、直列化処理の不具合が修正されました。GC 関連やビルド専用の修正は省略しています。

21.0.8 の主な変更点 (21.0.7 → 21.0.8)

ID	概要	影響・備考
JDK-6956385	<code>URLConnection.getLastModified()</code> が JAR ファイルの場合に内部で開いたファイルハンドルを閉じないためハンドルリークが発生する問題を修正 ²² 。	クラスパス内の JAR を <code>URLConnection</code> 経由で参照して最終更新日時を取得するようなユーティリティで、ハンドルが解放されずファイルがロックされる問題がありました。修正によりファイルハンドルが自動的に閉じられます。
JDK-8200566	CRL(証明書失効リスト) を取得する際に、複数の Distribution Point が指定されていると最初の取得に失敗した時点で終了してしまう問題を修正し、次のエンドポイントにフォールバックするように変更 ²³ 。	証明書検証で CRL の取得に失敗していたケースが改善され、複数の CRL エンドポイントが指定されている場合でも正しく検証できます。
JDK-8210471	<code>GZIPInputStream</code> のコンストラクタで例外が発生した場合に <code>Inflater</code> オブジェクトが解放されずリソースリークとなる不具合を修正 ²⁴ 。	GZIP 入力ストリームの初期化中に例外が投げられるケース（例えば不正なヘッダー）があると、ネイティブリソースが解放されませんでした。修正により例外時でも確実にクリーンアップされます。
JDK-8270269	<code>Desktop.browse()</code> を呼び出す前に同スレッドで COM が <code>COINIT_MULTITHREADED</code> 方式で初期化されていると、ブラウザを起動できない問題を修正 ²⁵ 。	Windows 環境でリンクをブラウザで開く API を使用するアプリケーションで、他のライブラリが COM をマルチスレッドモードで初期化していると <code>browse()</code> が失敗していました。修正により初期化状態に関係なくブラウザ起動が成功します。
JDK-8359170	セキュリティライブラリに Sectigo の TLS ルート証明書 2 件およびコード署名(CS)ルート証明書 2 件を追加 ²⁶ 。	新しいルート証明書の追加により Sectigo 発行の証明書が検証可能になりました。既存証明書への影響はありませんが、信頼ストアに含まれる証明書が増えます。
JDK-8356096 / JDK-8357548	ISO 4217 通貨コード改訂 (Amendment 179) に対応し、アラブ会計ディナールなど新しい通貨コード <code>XAD</code> を追加 ²⁷ 。	<code>java.util.Currency</code> で取得できる通貨コードが更新され、 <code>XAD</code> が含まれるようになりました。通貨コードをリストアップしているアプリケーションで新しいコードが表示される可能性があります。

ID	概要	影響・備考
JDK-8354893	コンストラクタの戻り値へ型注釈を付加する際に javac がクラッシュする問題を再修正 (redo backport) し、 <code>AssertionError</code> を解消 ²⁸ 。	javac の内部エラーが原因でコンパイルが失敗する状況がありました。特にアノテーション処理を行うビルドで影響があり、修正によりコンパイラが安定します。
JDK-8356104 など	VS2019/VS2022 のビルド警告対応や Linux 固有のビルドオプション修正などが含まれています。Windows 11 アプリケーションの実行には影響しないため省略しました。	

21.0.8 では Windows 向けの不具合修正として `Desktop.browse()` の問題が大きく、他にリソースリークの修正や信頼証明書の追加が含まれています。

まとめと移行時の注意点

- 21.0.6 での主な影響** – 文字列操作 (`StringBuffer.reverse()`)、日付フォーマッタのエラー処理、SASL 入力ストリーム、仮想スレッドと `javaagent` の組み合わせなど、既存アプリケーションの挙動を直接変える修正が含まれます。また、TLS ハンドシェイクやキー管理ツールで挙動が変わる可能性があります。これらの部分を使用している場合は、アップグレード後に動作確認が必要です。
- 21.0.7 での主な影響** – PKCS#11 プロバイダの制限緩和により、従来使えなかったトークンが利用可能となる一方、直列化時のバリデーション強化により古い不正データを読み込むと例外が発生する可能性があります。また、`HttpClient` のタイムアウト処理が改善され、JAR 署名検証の警告が出るようになっています。
- 21.0.8 での主な影響** – Windows 11 環境で `Desktop.browse()` が正しく動作するようになり、`URLConnection` や `GZIPInputStream` のリソースリークが解消されています。証明書検証関連では CRL 取得処理やルート証明書の追加があり、証明書チェーンの検証結果が変わる場合があります。また、通貨コード `XAD` の追加など国際化対応が含まれます。

総じて、21.0.5 → 21.0.8 への更新では新機能の追加は少なく、主にバグ修正とセキュリティ／互換性改善が中心です。ただし例外処理やリソース管理の挙動が変わる部分があるため、上記の修正箇所該当する API を使用しているアプリケーションでは動作確認と検証が推奨されます。

¹ ² [JDK-8319640] ClassicFormat::parseObject (from DateTimeFormatter) does not conform to the javadoc and may leak DateTimeException - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8319640>

³ ⁴ [JDK-8320192] SHAKE256 does not work correctly if n >= 137 - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8320192>

⁵ [JDK-8320575] generic type information lost on mandated parameters of record's compact constructors - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8320575>

⁶ [JDK-8323562] SaslInputStream.read() may return wrong value - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8323562>

- 7 [JDK-8328723] IP Address error when client enables HTTPS endpoint check on server socket - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8328723>
- 8 [JDK-8331391] Enhance the keytool code by invoking the buildTrustedCerts method for essential options - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8331391>
- 9 [JDK-8333317] Test sun/security/pkcs11/sslecc/ClientJSSEServerJSSE.java failed with: Invalid ECDH ServerKeyExchange signature - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8333317>
- 10 [JDK-8333427] langtools/tools/javac/newlines/NewLineTest.java is failing on Japanese Windows - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8333427>
- 11 [JDK-8337066] Repeated call of StringBuffer.reverse with double byte string returns wrong result - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8337066>
- 12 [JDK-8337331] crash: pinned virtual thread will lead to jvm crash when running with the javaagent option - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8337331>
- 13 [JDK-8340812] LambdaForm customization via MethodHandle::updateForm is not thread safe - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8340812>
- 14 [JDK-8340923] The class LogSelection copies uninitialized memory - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8340923>
- 15 [JDK-8342905] Thread.setContextClassLoader from thread in FJP commonPool task no longer works after JDK-8327501 redux - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8342905>
- 16 [JDK-8293345] SunPKCS11 provider checks on PKCS11 Mechanism are problematic - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8293345>
- 17 [JDK-8302111] Serialization considerations - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8302111>
- 18 19 [JDK-8304701] Request with timeout aborts later in-flight request on HTTP/1.1 cxn - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8304701>
- 20 [JDK-8309841] Jarsigner should print a warning if an entry is removed - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8309841>
- 21 [JDK-8311546] Certificate name constraints improperly validated with leading period - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8311546>
- 22 [JDK-6956385] URLConnection.getLastModified() leaks file handles for jar:file and file: URLs - Java Bug System
<https://bugs.openjdk.org/browse/JDK-6956385>

- 23 [JDK-8200566] DistributionPointFetcher fails to fetch CRLs if the DistributionPoints field contains more than one DistributionPoint and the first one fails - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8200566>
- 24 [JDK-8210471] GZIPInputStream constructor could leak an un-end()ed Inflater - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8210471>
- 25 [JDK-8270269] Desktop.browse method fails if earlier Colnitalize call as COINIT_MULTITHREADED - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8270269>
- 26 [JDK-8359170] Add 2 TLS and 2 CS Sectigo roots - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8359170>
- 27 [JDK-8356096] ISO 4217 Amendment 179 Update - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8356096>
- 28 [JDK-8354893] [REDO BACKPORT] javac crashes while adding type annotations to the return type of a constructor (JDK-8320001) - Java Bug System
<https://bugs.openjdk.org/browse/JDK-8354893>