

# REPRODUCIBLE BUILDS (再現可能なビルド)

## 検証可能なリリースによりソフトウェアの完全性を保護

### 概要

脅威が拡大する中、企業はソフトウェア・サプライチェーン攻撃を防御し、ソフトウェア開発プロセスにおける脆弱性のポイントを排除するソリューションが求められています。ソフトウェアの完全性を守るアプローチのひとつに、ビルドプロセス中にリリースを検証するというものがあります。

「リリース」は、ソフトウェアサプライチェーンセキュリティフレームワークの一部として、Reproducible Builds (再現可能なビルド) または Deterministic Compilation (決定論的コンパイル) を活用することで、公開ソフトウェアにマルウェアやスパイウェアが混入するリスクを低減する DigiCert Software Trust Manager の機能です。「リリース」を使用することで、組織はコミット署名を実行し、異なるビルド環境で同じソースからコンパイルされたバイナリのハッシュを比較することで、ビルド成果物を検証できます。

「リリース」機能は、出力バイナリの不一致をキャプチャすることにより、公開ソフトウェアの完全性を保証します。さらに、「リリース」は鍵ペアと署名の割り当てを強力に制御し、ソフトウェアビルドに対する不正な署名活動を防止します。

### 主な特長

- ベースラインリリースに対してビルドアーティファクトを検証することで、ビルドプロセス中のマルウェア混入のリスクを低減
- リリース時の鍵ペアと署名を一元管理することで、計画外の署名とリリースを防止
- ソフトウェアビルドからのインサイトを利用して、プロセスを再構築し、悪意のあるアーティファクトを排除

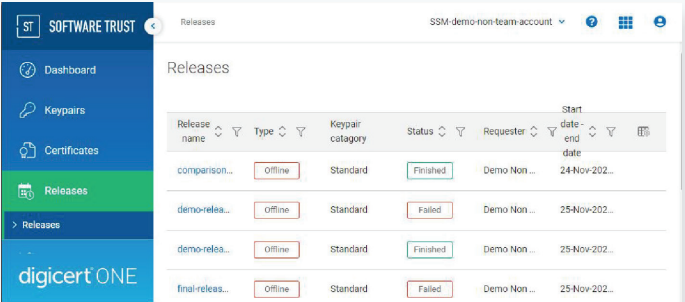
### 主な機能

ソフトウェア・サプライチェーン・セキュリティ・フレームワークのベストプラクティスに対応  
コミット署名を有効にしハッシュを使用してテスト・リリースを生成・比較し、ベースラインまたはプロダクション・リリースを作成

鍵ペアと署名に関するきめ細かな制御の実装  
事前に承認された日時(リリース・ウィンドウ)、承認された鍵ペア、承認された署名者などの鍵ペア使用制限をサポート  
リリースを許可された署名者の署名にのみ関連付け

不規則なビルドを制限  
問題が解決されるまで、一致しない成果物のビルド処理を自動的に中止。

ビルド成果物のレポートと分析  
すべてのリリースの比較分析を生成し、一致するアーティファクトと一致しないアーティファクトのビルド要因に関するインサイトを提供



Release name	Type	Keypair category	Status	Requester	Start date	End date
compenson...	Offline	Standard	Finished	Demo Non ...	24-Nov-202...	
demo-reles...	Offline	Standard	Failed	Demo Non ...	25-Nov-202...	
demo-reles...	Offline	Standard	Finished	Demo Non ...	25-Nov-202...	
final-reles...	Offline	Standard	Failed	Demo Non ...	25-Nov-202...	

DigiCert Software Trust Managerのリリース機能は、Reproducible Builds (再現可能なビルド) をサポートし、鍵ペアと署名の制御を実施することで、マルウェア混入のリスクを低減し、ソフトウェアの完全性を保護します。