



**HCL Domino**

# HCL Domino SAMLとOktaでの 統合ログイン



**HCL Software Academy**  
for HCL Digital Solutions

Creating a new generation of experts

Jan F. Zeuthen – [jfz@opusneo.com](mailto:jfz@opusneo.com)

## Table of Contents

Author .....	3
はじめに.....	4
前提条件 .....	4
Domino サーバーの構成.....	5
インターネットサイト文書の作成.....	5
IdP CatalogDatabase の構成Configure the IdP CatalogDatabase.....	5
SAMLデバッグ設定の有効化 (notes.iniを使用).....	5
Oktaの構成 .....	6
SAML 2.0 の新規チケットの作成.....	6
metadata.xml ファイルの取得 .....	8
IdPカタログ文書を完成させる .....	8
統合のテスト .....	10
Domino HTTP タスクの再起動.....	10
Oktaチケットを開く.....	10
任意: チケットの自動起動の有効化 .....	11
Domino セキュリティを構成する .....	11
アクセス制御リスト.....	11
アプリケーションYour Application .....	12
まとめ.....	12
法的記載事項.....	13
免責事項 .....	13

## 著者について

この文書は以下の専門家によって作成されました。



**Jan F. Zeuthen**  
**Company: Opus**  
**Neo**

### 経歴

Janは、Opus Neoの共同設立者でありCEOです。Dominoの管理者およびインテグレーターとして長年の経験を持ち、世界中の多くのクライアントと仕事をしてきました。現在は、コラボレーションと従業員エンゲージメントに注力しています。

### 連絡先:

[jfz@opusneo.com](mailto:jfz@opusneo.com)

---

## はじめに

このガイドでは、サービスプロバイダとして HCL Domino を使用し、ID プロバイダ (IdP) として OKTA を使用して、SAML 連携ログインを設定する方法を説明します。この設定は、オンプレミスまたはクラウドベースのディレクトリとアプリケーションの両方を持つクライアント/サーバー環境で、シングルサインオンソリューションを作成したい場合に用いるものです。

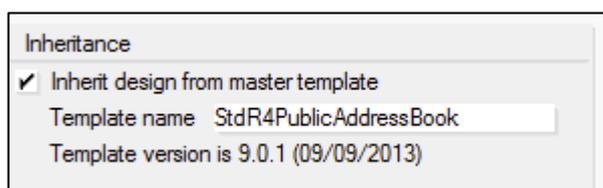
## 前提条件

このガイドでは、Domino の管理経験があり、Okta についてある程度の知識があることを前提にしています。参考になる HCL ドキュメントがある場合はそのリンクが提供されます。

このガイドの手順を完了するには、次のものがが必要です。

- ・ 9.0x 以降の Domino サーバーで http タスクが実行されていること。Domino の最新リリースを推奨します。
- ・ チケット (Chiclets) を作成するための管理者としての Okta アカウント
- ・ ログイン後にアクセスする Domino アプリケーション

開始する前に、Domino Directory データベース (names.nsf) の設計テンプレートが StdRxxxPublicAddressBook、バージョンが 9.0.1 以降に基づいていることを確認してください (最新リリースを推奨します)。それ以前のバージョンは、SAML をサポートしていません。データベースのプロパティ (下図) で確認できます。



## Domino サーバーの構成

インターネットサイト文書と IdP カタログデータベースを作成し、notes.ini で SAML デバッグ設定を有効にして、構成の準備をします。

### インターネットサイト文書の作成

Server 文書で Internet Site 文書を有効にします (まだ有効になっていない場合)。

既存のドキュメントを使用していない場合は、新しい Internet Site文書を作成します。詳しくは、以下を参照してください。

製品ドキュメント: [インターネットサイト文書を作成する](#)

[ホーム URL]には、Okta チケットから開くアプリケーションを指定します。インターネットサイト文書が正しく動作し、アプリケーションにログインが求められることを確認します (ACLで「匿名」アクセスを無効にしておく必要があります)。

SAML認証方式はまだ有効にしないでください。

### IdP CatalogDatabase の構成Configure the IdP CatalogDatabase

idpcat テンプレートから新しい IdP Catalog データベースを作成し、その中に IdP 構成文書を作成します。詳しくは、HCL Domino の製品ドキュメントの「[SAML 認証を準備する](#)」を参照してください。

注: IdP 設定文書では、フェデレーションプロトコルとして「TFIM」 (または SAML 2.0) を選択します。Metadata.xml ファイルを取得する方法は本書の「[Okta の構成](#)」の章を参照してください。

### SAMLデバッグ設定の有効化 (notes.iniを使用)

デバッグのために、SAML 認証を設定する Domino サーバーの notes.ini に次の行を追加します。

```
DEBUG_SAML=31
```

DEBUG\_SAML 文の値は、次のオプションから計算できます。

0x0001 (1)	デバッグ出力に http 側の情報が含まれる。
0x0002 (2)	デバッグ出力にSAMLパース情報が含まれます。
0x0004 (4)	デバッグ出力はエラーのみを含む。
0x0008 (8)	デコードされたアサーションをダンプするためのデバッグ。
0x0010 (16)	IdPcatactivityをトレースするためのデバッグ
0x0020 (32)	リプレイ防止をトレースするためのデバッグ

0x0080 (128)	XMLツリー全体をダンプ
0x0100 (256)	正規化バッファをダンプ
0x0200 (512)	ライブラリソートのデバッグ
0x0800 (2048)	名前空間使用のデバッグ
0x2000 (8192)	証明書管理のデバッグ出力

その他の SAML 設定

SAML_NotOnOrAfterSkewInMinutes=[#]	SAML アサーションの 'not on or after' タイムスタンプのチェックで余分な分数を許可します。
SAML_NotBeforeSkewInMinutes=[#]	SAML アサーションにおける 'not before' タイムスタンプチェックで、追加の時間(分)を許可する。その他の DEBUG_SAML ステートメントは、欄外の URL先で参照ください。

サポート技術情報: Domino Web サーバーで SAML 認証を行なう際のデバッグの設定について  
[https://support.hcltechsw.com/csm?id=kb\\_article&sysparm\\_article=KB0086670](https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0086670)

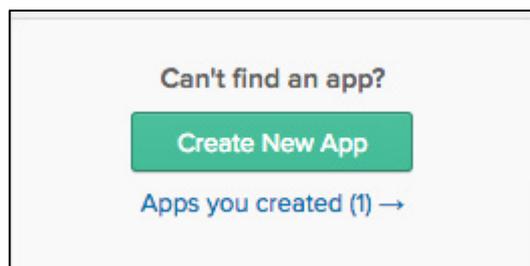
## Oktaの構成

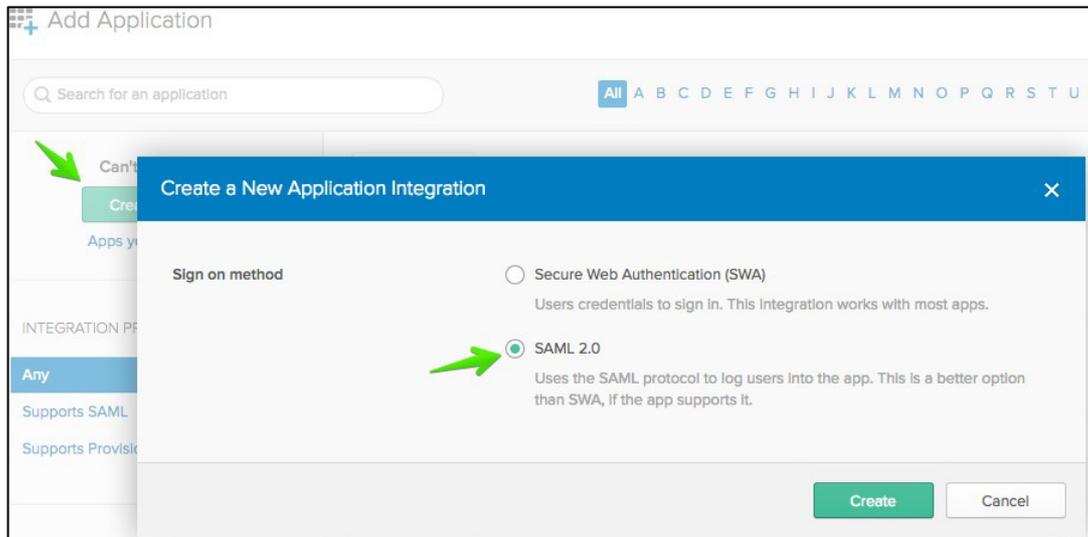
ウィザードを使用してOkta SAML 2.0シクレットを作成し、Dominoアプリケーションを起動する予定です。このスクリーンショットは、これを読む頃には古くなっているかもしれませんが、コンセプトは同じです。

シクレットが作成されたら、metadata.xmlファイルを取得し、Domino上のIdPカタログ文書にインポートします。

### SAML 2.0 の新規シクレットの作成

SAML App integration Wizard を使用して、新しいアプリを作成します。Create New App" ボタンをクリックして開始します(下図参照)。





自分のドメインを使用して、設定に適したフィールドに入力します。設定は、metadata.xml ファイルのソースに含まれます。インターネットサイト文書の「Home URL」フィールドで定義されたアプリケーションが、チケットにリンクされていることを忘れないでください。

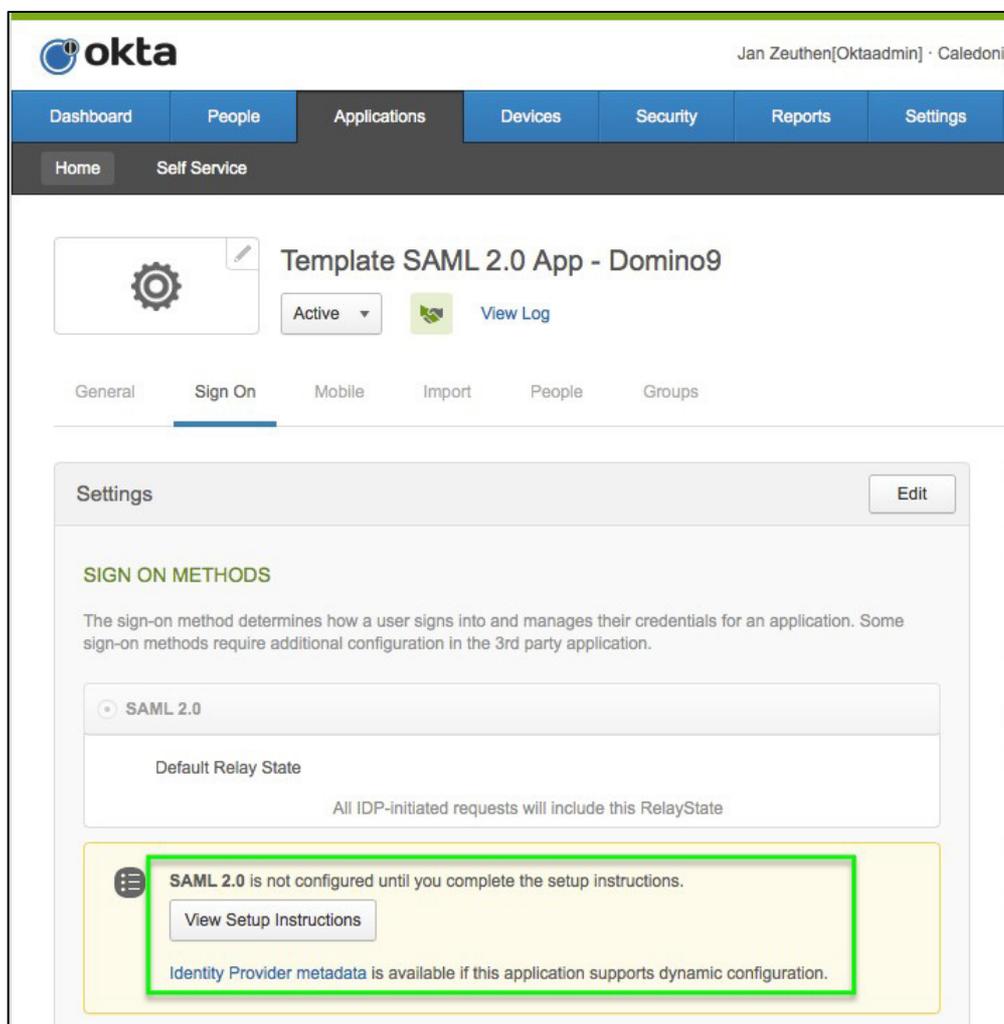
The image shows a screenshot of the 'SAML Settings' configuration page. The 'GENERAL' section is highlighted with a green border. It contains the following fields:

- Single sign on URL: . A checkbox 'Use this for Recipient URL and Destination URL' is checked.
- Audience URI (SP Entity ID):
- Default RelayState: . A note below says 'If no value is set, a blank RelayState is sent'.
- Name ID format:
- Application username:
- Authentication context class:

Other settings include Response (Signed), Assertion Signature (Signed), Signature Algorithm (RSA-SHA256), Digest Algorithm (SHA256), Assertion Encryption (Unencrypted), Enable Single Logout (unchecked), Honor Force Authentication (No), and SAML Issuer ID (http://www.okta.com/\${org.externalKey}). A 'Download Okta Certificate' button is visible on the right side.

## metadata.xml ファイルの取得

チクレットの保存後、チクレットを開いて設定を確認します。Sign-Onタブに、metadata.xml ファイルへのリンクが表示されます。右クリックでファイルをダウンロードします。これは Domino サーバー上の IdP カタログ文書に必要なものです。



Identity Provider metadata というテキストが Metadata.xml ファイルへのリンクです。

## IdPカタログ文書を完成させる

idP Catalog ドキュメントの構築を開始し、フォームのアクションボタンを使用して metadata.xml ファイルをインポートします。

**ヒント:** metadata.xml ファイルをインポートする前に、Domino IdP カタログ文書を明示的に保存します。これにより、バックエンドのフィールドが再計算されます。

<b>IdP Configuration : OKTA</b>			
<a href="#">Basics</a>   <a href="#">Client Settings</a>   <a href="#">Certificate Management</a>   <a href="#">Administration</a>			
<b>Basics</b>			
Host names or addresses mapped to this site:	http://rgf.eu.workplaceon.com		
IdP name:	OKTA		
Protocol version:	SAML 2.0		
State:	Disabled		
Federation product:	TFIM		
Service provider ID:	http://rgf.eu.workplaceon.com		
Artifact resolution service URL:			
Single sign-on service URL:	/ldplnitiatedSignOn.aspx		
Signing X.509 certificate:			
Encryption X.509 certificate:			
Protocol support enumeration:			
Comment:			

**ヒント:** metadata.xmlをインポートした後、ドキュメントのプロパティで「X.509証明書の署名」フィールドをチェックし、余分なキャリッジリターンがないことを確認します。見つかった場合は、X.509証明書の文字列をメモ帳などにコピーしてください。文字列がすべて1行のテキストであることを確認します（ワードラップを無効にします）。その文字列をIdPカタログ文書のX.509証明書フィールドに貼り戻し、再度保存します。

Single sign-on service URL:	https://rgf-workplaceon.okta-emea.com/app/opusneo_rgfwp0_1/exkzcf13fSakZSVsv0i6/isso/saml
Signing X.509 certificate:	MIIDljCCAn6gAwIBAgIGAV0ZR3y3MA0GCSqGSIb3DQEBBQUAMIGLMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcml5YUJTEWMBQGA1UEBwwNU2FulEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmkZlXDDAKBgNVBAMMA3JnZjEcmBoGCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTAeFw0xNzA3MDYxOTAwNDFAFw0yNzA3MDYxOTAwNDFAmIGLMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcml5YUJTEWMBQGA1UEBwwNU2FulEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmkZlXDDAKBgNVBAMMA3JnZjEcmBoGCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTCCASlwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAlchA iOd+52WlVe3fpayfIYg6AH8c4C0UMXMELL664u8Gdyv7basqe3l2GzW6X2BhVV he+ZnsvmOxV+KMJlulPKo19raWtGnlPYGeWWbXG7F8mqLS3/e8SuggSp2UO M2nN6Dy7cmN3pN96xJBGAR2QwrLYCXq/pw7uQfv6gHcr/cPmB5kP9ULX2wD+ PpdyPgdDnB41Cict8cOst99ue61Hx7x4dfS50FbOtTwmhBwn905vE2Xq8ZlnJ0 KQb0EvrLmTBLN28irVoSuRdl8eKWMY7Gkx87UhZQCG4FIZNcesG9YJ4PHe2E /cj5U+aQuujerSK4Tbjwpob6Tj1NAo0CAwEAATANBgkqhkiG9w0BAQUFAAOCAQ EACwE2RimKTU1X0FvbsMzvUuvb/okFUJlQDJMik2k3yXvHxpuflF9M7aUf2d0x Dd1aCjeCZ+6JGruoYigxsF3WdUJqCqct1+fs/Do+4FEDG0Uv0Zi+NuTGF1SVEBa ALEP0dW0sinSDfikAbNh1V70DmXAS0yic4rGJRb7FuyLqvxZug/zGA4YyKioM2Rl 3P4R1zEJJxpFunB61BOyfxPxe3punphk+PI1185Rfb8k2UEtYr77HX/y61rTJZnGEt fw7bwpU+02vuHbF8D0yM1pUO5x/OMfmkaxvOjl/MqgTbt3VX2e1g1Nb7pAXC6C mDStAQIRyrrmpPL9wWV/ypuirA==
Encryption X.509 certificate:	
Protocol support enumeration:	urn:oasis:names:tc:SAML:2.0:protocol
Comment:	

## 統合のテスト

これで、インターネットサイト文書で SAML を有効にして Domino http タスクを再起動し、Web ブラウザで Okta に移動して、作成した SAML シクレットをクリックして、設定をテストすることができるようになりました。



The screenshot shows the Domino Web Site Administration console for a site named 'Web Site samltest'. The 'Security' tab is selected. Under the 'HTTP Sessions' section, the following settings are visible:

- Session authentication: SAML (selected from a dropdown menu)
- Web SSO Configuration: LtpaToken (selected from a dropdown menu)
- Force login on SSL: No (selected from a dropdown menu)
- SAML single server session expiration: 120 (selected from a dropdown menu)
- When overriding session authentication, generate session cookie: Yes (selected from a dropdown menu)

An 'Open IdP Configuration' button is located to the right of the Session authentication dropdown.

## Domino の IdP 構成をテストする

Notes では、インターネットサイトドキュメントで "Open IdP Configuration" ボタンを押し、IdP 設定が Domino idpcat データベースにリンクされていることを確認します。作成した文書にリンクしているはずですが。

## Domino HTTP タスクの再起動

Domino コンソールの "restart task http" でタスクを再起動します。SAML デバッグを有効にすると、Domino コンソールでサイトが "SAML ready" と表示されるのがわかります。さらなるデバッグのために Domino コンソールを開いたままにします。

## Okta チクレットを開く

Okta にログインし、作成したチクレットを開きます。すぐに Domino アプリケーションにリダイレクトされ、ログインを必要とせずに開くことができるはずですが。Domino コンソールをチェックして、SAML トラフィックを監視します。すべてうまく動作しましたでしょうか。おめでとうございます。

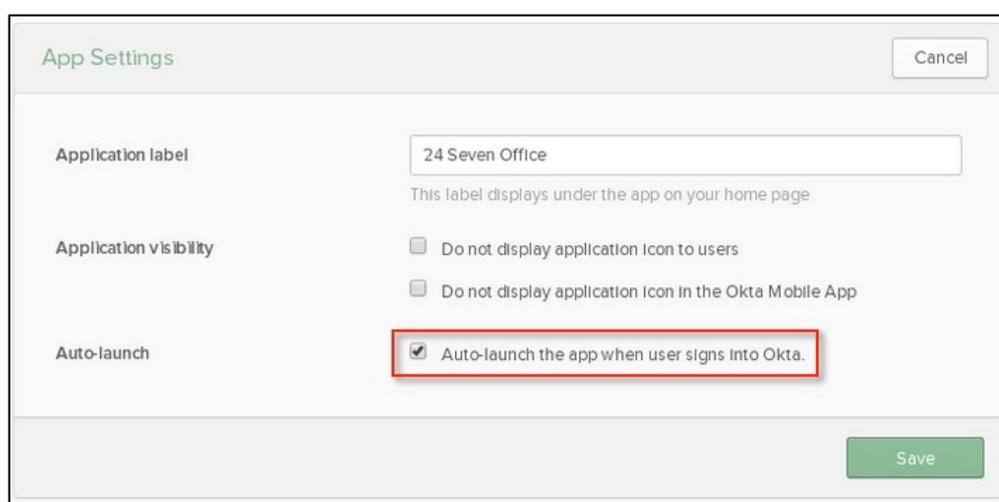
notes.ini にある SAML デバッグ行を削除することを忘れないように。

## 任意: チクレットの自動起動の有効化

SAMLアサーションのテストが成功したら、ユーザーがログインした後にアプリを「自動起動」できるようにすることができます。(Oktaのヘルプによると) 管理者は、サインイン時にすべてのエンドユーザーに対して特定のアプリを自動起動できるようになりました。以前は、このオプションはエンドユーザーのみが利用できました。現在、管理者は、「Oktaアプリケーションページの使用」で詳しく説明されているように、特定の<App>ページ > Generalタブ > App Settingsからこのオプションにアクセスできます。

<https://help.okta.com/en-us/Content/Topics/Apps/apps-access.htm>

注：このオプションのチェックは、アプリに新しく割り当てられたエンドユーザーのみに影響します。以前から割り当てられているユーザーは、アプリのチクレット<App>設定ボタンにアクセスし、手動で自動起動を選択する必要があります。



The screenshot shows the 'App Settings' dialog box in Okta. It has a title bar with 'App Settings' and a 'Cancel' button. The main content area has three sections: 'Application label' with a text input field containing '24 Seven Office' and a subtext 'This label displays under the app on your home page'; 'Application visibility' with two unchecked checkboxes: 'Do not display application icon to users' and 'Do not display application icon in the Okta Mobile App'; and 'Auto-launch' with a checked checkbox labeled 'Auto-launch the app when user signs into Okta.'. A red rectangular box highlights the 'Auto-launch' checkbox. At the bottom right, there is a green 'Save' button.

## Domino のセキュリティ設定

認証方法として SAML を使用するようになったので、アプリケーションはこの新しい目的のために準備される必要があります。良いニュースは、Domino セキュリティモデルが同じであることです。

### アクセス制御リスト

通常通りアクセス制御リストを使用してデータベースアクセスを制御しますが、SAML ユーザーに対応する特定の階層はありません。その代わりに、"- Default-" 設定を「読者」に設定し、ユーザーがデータベースを開けるようにする必要があります。

## アプリケーション

読者フィールドは、SAML では機能しません。代わりに、ユーザーアカウントを作成/管理し、適切なアクセス権を割り当てる必要があります。

SAML を使用する前にログイン名などを表示していた場合、SAML を使用する前は "Joe Block" と表示している場合、SAML を使用した後の名前は、設定によって異なって見えるはずですが、いくつかのコードを使用すると、SAML名を親しみやすい表示名に変換できます。

## まとめ

これで、Dominoをサービスプロバイダとして、Okta を IdP として使用する Federated Login が構成されました。

このセットアップでは、いくつか注意すべき点があります。この設定は、インターネットサイト文書で指定したDNSホスト名に関連付けられています。つまり、

- ・ フォームベース認証（domcfg.nsf経由）やIPアドレスを使用してログインすることはできません。
- ・ SAMLを使った認証のみ可能です
- ・ ログイン画面はOktasとなり、カスタマイズは制限されます。
- ・ name.nsfには、ユーザー用の人物ドキュメントは必要ありません。その場合は、ユーザー文書を作成し、アプリケーションへの適切なアクセスを提供する必要があります。  
「[Domino のセキュリティ設定](#)」のセクションを参照してください。
- ・ Domino サーバーの現在の時刻が正しくない、同期していないなど不正な状態な場合、SAML 経由の認証は失敗します。OS のメカニズムを使用して、サーバー上の正しい時刻と日付の設定を常時確認します。

## 法的記載事項

このエディションは HCL Domino バージョン 9 以降に適用され、新しいエディションで別途指示されるまでは、それ以降のすべてのリリースと修正に適用されます。

あなたが HCL Technologies Ltd. に情報を送るとき、あなたは HCL Technologies Ltd. に、あなたに対していかなる義務も負わずに、適切と考える方法で情報を使用または配布する非排他的な権利を付与します。

**©2022 Copyright HCL Technologies Ltd and others. All rights reserved.**

米国政府ユーザーへの注意事項 - 制限付き権利に関する文書 - 使用、複製、または開示は、HCL Technologies Ltd. との GSA ADP スケジュール契約に定められた制限に従います。

## 免責事項

本レポートは、HCL 利用規約(<https://www.hcl.com/terms-of-use>)および以下の免責事項の適用を受けるものとします。

本レポートに含まれる情報は、情報提供のみを目的として提供されています。本書に含まれる情報の完全性と正確性を確認するために努力しましたが、商品性、非侵害、特定目的への適合性の黙示保証を含むがこれに限定されない、明示または黙示のいかなる保証もなく、現状のまま提供されるものとします。さらに、この情報は、HCL の現在の製品計画と戦略に基づいており、HCL は予告なしに変更することがあります。HCL は、本レポートやその他の資料の使用、またはそれらに関連して発生した直接的、間接的、偶発的、結果的、特別またはその他の損害について、一切の責任を負うものではありません。本書に含まれるいかなる内容も、HCL、その供給者、ライセンサーからのいかなる保証や表明を意図するものではなく、またその効果をもたらすものでもなく、HCL ソフトウェアの使用に適用されるライセンス契約の諸条件を変更するものではありません。

本レポートで言及されている HCL の製品、プログラム、またはサービスは、HCL が事業を展開しているすべての国において利用可能であることを意味するものではありません。このプレゼンテーションで言及された製品のリリース日や機能は、市場機会やその他の要因に基づいて HCL の独自の裁量でいつでも変更することができ、将来の製品または機能の利用可能性を約束するものではありません。これらのレポートをサポートするために使用される基礎となるデータベースは、週単位で更新されます。このウェブツールを使用して生成されたレポートと他の HCL ドキュメント・ソースとの間に見られる相違は、このツールと他のソースの公開および更新サイクルが異なることに起因する場合がありますし、起因しない場合もあります。本レポートに含まれるいかなる内容も、記述することを意図しておらず、またそのような効果を持つものではありません。

また、本レポートに記載されている内容は、利用者が行った活動が特定の売上、収益の増加、節約、またはその他の結果につながることを意図したものではなく、そのような効果を持つものでもありません。本レポートの結果、あなたが得た結果またはあなたが下した決断に対する責任は、あなたが単独で負うものとします。HCL 利用規約(<https://www.hcl.com/terms-of-use>)にかかわらず、このサイトのユーザーは、このツールから生成されたレポートを、そのユーザー自身の内部ビジネス目的のためにコピーし保存することが許可されています。それ以外の使用は許可されません。