

LSEG Workspace | Entra

よくある質問 (FAQ)



目次

本書の概要	2
対象範囲	2
参考資料	2
Workspace ドキュメント	2
Entra の基礎知識	3
Workspace の認証はどのように変わりますか？	3
Microsoft Entra とは何ですか？	3
SCIM とは何ですか？	3
自分の組織が Entra を使用しているかどうか確認するには？	3
自社が Entra を使用していない場合はどうなりますか？	3
社内 ID ポータル使用時に LSEG CIAM との連携は問題ありますか？	3
Workspace へのログインに Entra を使用するメリットは何ですか？	4
Entra 統合におけるオプション機能（アドオン）とは何ですか？	4
LSEG の Entra 認証戦略についてさらに詳しく知るには？	4
ユーザーエクスペリエンス	5
新しいログインページはどのようなものになりますか？	5
パスワードは引き続き変更できますか？	5
この変更は他の製品にも影響しますか？	5
Workspace と FX Trading を利用している場合、パスワードは同じままですか？	5
ライセンス 管理	6
Entra と LSEG 間の初回ユーザーマッピングはどのように行われますか？	6
Entra でユーザーのライセンスを削除するには？	6
Entra でユーザーを過剰にプロビジョニングした場合はどうなりますか？	6
Entra 連携は不正アクセスの防止に役立ちますか？	6
ネットワーク アクセス	7
インターネット経由でアクセスするには？	7
プライベート ネットワーク経由でアクセスするには？	7
Entra は専用線またはダイレクトファイバー接続経由で利用できますか？	8
コンプライアンス	9
Entra と LSEG 間の SCIM プロビジョニングは DORA に準拠していますか？	9
Azure または Entra の障害によって、LSEG サービスへのアクセスに影響が生じる可能性はありますか？	9
LSEG 製品との互換性	10
Entra のオンボーディングにより、リアルタイムデータへのアクセスはどのように変わりますか？	10
Entra を利用する際、社内の ID ポータルを使用していますが、LSEG との統合で問題は発生しますか？	10
DACS ID を別途使用している場合、それらは Entra または SCIM を介してフェデレーションされますか？	10
Entra でユーザーを無効化した場合、LSEG 側ではどのような処理が行われますか？	10

本書の概要

本書は、以下の場合にお客様からよく寄せられる質問への回答をまとめたものです:

- Microsoft Entra を初めて利用する場合
- LSEG Workspace の認証に Entra を使用するための設定を準備する場合

対象範囲

本書は、Entra 認証を必要とする LSEG Workspace for HERE Core の利用を予定している LSEG のお客様を対象としています。特に、以下の役割の方々にとって有用な内容となっています。

- ID 管理者
- IT 管理者
- Workspace 管理者

参考資料

- 本 FAQ で取り上げている内容についてさらにサポートが必要な場合は、[サポート](#)にお問合せください。
- Entra の構成に関するより詳細な技術情報については [Administrator Guide](#) をご参照ください。

Workspace ドキュメント

LSEG Workspace に関する一般的な技術情報については、[Workspace technical documentation site](#) をご覧ください。また、本書を含む Workspace の技術コンテンツに関するご意見・ご要望は DocFeedback@lseg.com までお寄せください。

Entra の基礎知識

Workspace の認証はどのように変わるのですか？

LSEG は 2025 年 3 月に、お客様の企業 ID 管理システムと LSEG の顧客 ID およびアクセス管理（CIAM）を統合するソリューションをリリースしました。具体的には LSEG とお客様の組織の Entra を連携できるようになります。この連携方式は SCIM と呼ばれ、認証時のシングルサインオン（SSO）にとどまらず、ID 管理全般を対象とする業界標準の連携方式です。また、お客様はユーザーおよびライセンスのプロビジョニングを自動化できるため、運用負荷を軽減できます。

現在、多くのお客様が以下のようなメリットを理由に、このソリューションを採用しています：

- セキュリティ
- コンプライアンス
- 運用負荷
- ユーザーエクスペリエンス

★ 従来の LSEG Workspace プラットフォーム（旧 Refinitiv Workspace）では引き続き認証に ForgeRock が使用されています。

Microsoft Entra とは何ですか？

簡単に言うと、Microsoft Entra はクラウド上の Microsoft Active Directory であると言えます。これは、Microsoft が提供する包括的な ID およびアクセス管理ソリューション群です。当社のお客様の多くは、Entra を次の目的で使用しています：

- Windows ユーザー ID の管理
- アクセスの保護
- 機密データの保護

Entra には、Azure Active Directory や Microsoft Identity Manager などのサービスが含まれています。

SCIM とは何ですか？

SCIM（System for Cross-domain Identity Management）は、組織がユーザー ID を統合しユーザー管理や権限のプロビジョニングをリアルタイムで自動化するための確立された業界標準です。SCIM の詳細については [Microsoft FAQs on SCIM](#) を参照してください。

自分の組織が Entra を使用しているかどうか確認するには？

Microsoft Office 365 を利用している場合は、Entra を利用している可能性が高いです。貴社の IT 管理者、サービスデスク、または Microsoft サポートに問い合わせることで、企業 ID の管理に Entra を使用しているかどうかを確認できます。

自社が Entra を使用していない場合はどうなりますか？

LSEG では、お客様の企業 ID システムを通じてユーザーのログイン情報を LSEG 製品と連携させるための、その他のシングルサインオン（SSO）ソリューションの提供を予定しています。詳細については、LSEG Customer Implementation チームまでお問い合わせください。

社内 ID ポータル使用時に LSEG CIAM との連携は問題ありますか？

はい。独自のポータルを使用して企業 ID を Entra にマッピングしている場合、この統合は適していません。ただし、LSEG では、お客様のユーザーのログイン ID を企業 ID を通じて LSEG Workspace に連携できる別のソリューションも提供しています。詳細については、LSEG Customer Implementation チームまでお問い合わせください。

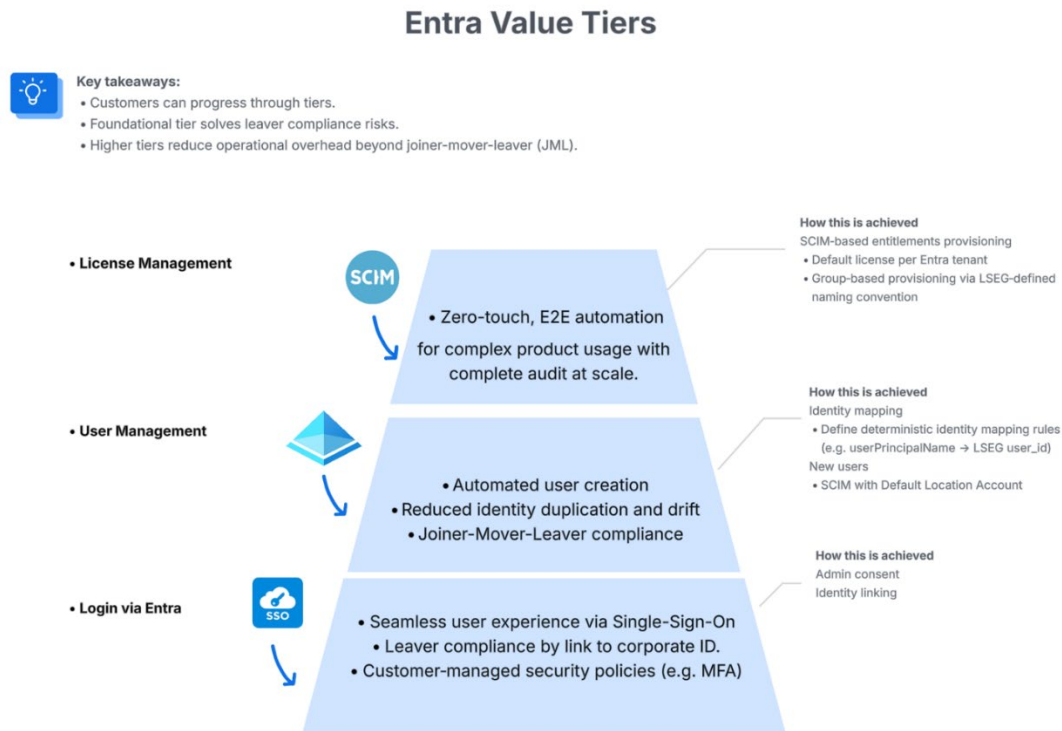
Workspace へのログインに Entra を使用するメリットは何ですか？

お客様の Entra テナントを通じて LSEG と連携することで、LSEG Workspace へのアクセスに使用される認証情報をお客様自身が完全に管理できます。また、運用負荷をさらに軽減するためのオプションのアドオン機能も用意されています（詳細は後述します）。主なメリットは次のとおりです：

セキュリティの強化	Workspace の認証はお客様の IT システムを経由して実行されます。そのため、セキュリティポリシーおよびアクセス制御を組織全体で一貫して適用することができます。これにより、入社者および退職者に関するコンプライアンス要件にも、追加の対応を行うことなく対応できます。
コストの削減	複数のユーザー認証情報やアカウントの管理に伴う管理負荷を軽減します。
ユーザーエクスペリエンスの向上	シングル サインオンを有効にすることで、ユーザーは LSEG Workspace を含むさまざまなアプリケーションにシームレスにアクセスできるようになります。
パスワード管理負荷の軽減	ユーザーは、異なるアプリケーションごとに多数のパスワードを覚えることに苦勞することがよくあります。ID フェデレーションにより、ユーザーは一度ログインするだけで、Windows 環境と LSEG Workspace の両方にアクセスできます。
相互運用性の向上	認証および認可のための標準プロトコルを提供することで、相互運用性を促進します。これにより、異なるシステムやアプリケーションを連携して利用できるようになります。

Entra 統合におけるオプション機能（アドオン）とは何ですか？

オプションとして、SCIM（業界標準の技術）を使用して、お客様の Entra 構成からの更新情報を LSEG が自動的に受信できるようにすることができます。これらの更新情報を受信すると、LSEG は LSEG エコシステム内で、お客様の組織のユーザーおよびそのライセンスを管理できるようになります。その概要を以下の図に示します。



LSEG の Entra 認証戦略についてさらに詳しく知るには？

詳細については、LSEG アカウント チームまでお問い合わせください。

ユーザーエクスペリエンス

新しいログインページはどのようなものになりますか？

Entra による認証が設定されると、通常使用している企業アカウントの認証情報（例えば、電子メールアドレスとパスワード）の入力を求められます。このシングル サインオンにより、企業の Windows デスクトップ環境だけでなく、LSEG Workspace にもアクセスできるようになります。

ただし、すでに他のシステムで認証済みの場合は例外で、その場合は Workspace へシームレスにアクセスできます。

パスワードは引き続き変更できますか？

はい。企業アカウントのパスワードは引き続き変更できます。ただし、企業 ID を使用して Workspace にログインするよう設定された後は、LSEG は企業アカウントのパスワードの保管やリセットには関与しません。

Workspace は企業 ID に基づくシームレスなシングルサインオンを提供します。そのため、企業アカウントのパスワードのリセットは、既存の社内 IT プロセスに従って実施します。

この変更は他の製品にも影響しますか？

現在、Entra 認証により、Workspace および LSEG のサポートポータルやトレーニングポータルへのシームレスなログインが可能になります。また、LSEG では Entra に対応する製品を LSEG 製品群全体に拡大する取り組みを進めており、今後は企業 ID を使用して、より多くの製品をシームレスに利用できる予定です。

Workspace と FX Trading を利用している場合、パスワードは同じままですか？

現在のところ、FX Trading および FXall のスタンドアロン アプリケーションでは、既存のログイン方法が維持されており、LSEG が発行したログイン認証情報を引き続き使用します。

ライセンス 管理

Entra と LSEG 間の初回ユーザーマッピングはどのように行われますか？

初回のユーザーマッピングは、オンボーディング方法に応じて複数の方法で実施できます。

SCIM	SCIM プロビジョニングが有効になっている場合 ¹ 、マッピングはお客様の Entra テナントで設定された属性マッピングルールによって決まります（例：userPrincipalName を LSEG のユーザー識別子にマッピングする）。
セルフサービスマッピング	既存ユーザーは、セルフサービスによる ID リンク付けのフロー、または管理者が実施する ID リンク付けによって関連付けることができます。

Entra でユーザーのライセンスを削除するには？

ユーザーが SCIM によりプロビジョニングされている場合、Entra テナント内で該当ユーザーのプロビジョニングを解除したり、ユーザーをグループから削除したりすると、そのユーザーのライセンスは LSEG システムから自動的に削除されます。詳細については [Workspace | Entra - Administrator Guide](#) をご覧ください。

LSEG の Location Account レベルのライセンスプール管理は従来どおりであり、Entra のオンボーディングによって、契約に基づくライセンス総数の割り当てや削除の方法が変更されることはありません。SCIM を介して LSEG と連携している場合、ユーザーが Entra の設定から削除されると、SCIM イベントが LSEG のシステムに送信されます。その結果、当該ユーザーに割り当てられていたライセンスは、お客様が利用可能なライセンスプールに返却されます。

Entra でユーザーを過剰にプロビジョニングした場合はどうなりますか？

自動ライセンス プロビジョニングが構成されており、ライセンスプールで利用可能なライセンス数に上限があるとして、ライセンスプールに利用可能なライセンスが残っている場合、新たに追加されたユーザーは LSEG システム内に作成されます。一方、ライセンスプールを使い切った後に SCIM を通じて新しいユーザー情報が受信された場合でも、ユーザーレコード自体は LSEG システム内に作成されますが、ライセンスは割り当てられません。

もちろん、既存の LSEG プロセス（ライセンス管理ツールや 営業担当者または運用担当者を通じて）を利用して、ライセンスを管理することもできます。ライセンス管理には、次のような作業が含まれます：

- ライセンスの追加
- ユーザーへのライセンスの割り当て
- ライセンス利用権（Entitlement）の確認

Entra 連携は不正アクセスの防止に役立ちますか？

はい。Entra を使用すると、次のような条件付きアクセス ポリシーを適用できます。

- 信頼済みデバイス
- ロケーションベースのアクセス制御
- 準拠デバイス要件
- 多要素認証（MFA）の適用

これらの制御はユーザーが LSEG のシステムにアクセスする前に適用されるため、コンプライアンスに準拠した利用を確保し、不正なデータアクセスのリスクを低減できます。多くのお客様が、安全なアクセス管理のための中核的な管理基盤として Entra を活用しています。

これらの機能の詳細については、[Microsoft Entra Conditional Access site](#) をご覧ください。

¹ ユーザーの自動プロビジョニング機能を利用するには、SCIM 連携を有効にしておく必要があります。

ネットワーク アクセス

新しい ID および認証サービスはクラウドでホストされており、固定 IP アドレスは使用しません。

△ お客様は、エンドユーザーを自社の Entra テナントで認証するために、各組織の要件に応じた適切な構成を採用することが想定されています。そのため、Entra 認証および関連ドメインについては、本書の対象範囲外です。

インターネット経由でアクセスするには？

パブリック インターネットへのアクセスをホワイトリスト方式で制御している場合は、以下の完全修飾ドメイン名 (FQDN) ² へのアクセスを許可する必要があります。

FQDN1	プロトコル / ポート	新しいドメイン	配信方法	説明
openfin.co	HTTPS, 443		WWW	HERE Core Runtime (RVM) およびアップグレードのダウンロード
lseg.com	HTTPS, 443	token.workspace.lseg.com login.workspace.lseg.com workspace.lseg.com api.workspace.lseg.com	WWW	認証用セキュリティトークンの発行および更新
既存のすべての WWW ドメイン ³	HTTPS, 443 WSS, 443 ⁴	*.Refinitiv.com *.refinitiv.net	WWW	アプリケーションへのアクセス

プライベート ネットワーク経由でアクセスするには？

新しい Azure サービス エンドポイントにアクセスするため、プライベート ネットワークを使用しているお客様は、これまでに案内された IP レンジに加えて、以下の新しい IP アドレスをホワイトリストに追加する必要があります。これは、Delivery Direct、FCN、および CMC のユーザーに影響します。

- 159.43.248.0/23 [AMERS]
- 159.43.240.0/23, 159.43.244.0/23 [EMEA]
- 159.43.227.0/24 [APAC]

これらの新しい IP アドレスは、過去のネットワーク関連文書で案内されているより大きな IP サブネット 159.43.192.0/18 に含まれています。LSEG では、このより広い IP サブネットへの接続を許可することを推奨しています。

LSEG Workspace は、新しいセキュリティ/認可トークンサービスへの接続および HERE Core Runtime のアップグレードにインターネットアクセスを利用します。そのため以下のドメインへのアクセスを許可するようネットワークを構成してください。

FQDN1	プロトコル/ポート	新しいドメイン	配信方法	説明
lseg.biz	HTTPS 443	login.workspace.lseg.biz	プライベート ネットワーク	アプリケーションへのアクセス
既存のすべてのプライベート ドメイン ³	HTTPS, 443 WSS, 443 ⁴	*.Refinitiv.biz *.refinitiv.net	プライベート ネットワーク	アプリケーションへのアクセス

²LSEG がこれまでに通知した既存のホワイトリスト登録済みドメインは、削除しないでください。

³ 詳細については [Workspace technical guides](#) サイト内の Configuration and Administration guide をご覧ください。

⁴ マーケットデータのストリーミング配信用

Entra は専用線またはダイレクトファイバー接続経由で利用できますか？

いいえ。Entra はパブリックインターネット経由で提供されるクラウドベースの ID サービスであり、専用線やプライベートピアリングなどの直接的なプライベート接続には対応していません。これは仕様によるもので、Entra はすべての管理対象デバイスおよびアプリケーションからグローバルにアクセス可能である必要があります。お客様は、Entra が公開しているエンドポイントへのアウトバウンド接続を許可するよう、セキュリティポリシーを設定してください。

コンプライアンス

Entra と LSEG 間の SCIM プロビジョニングは DORA に準拠していますか？

LSEG の SCIM 実装は、以下のような DORA に準拠した原則に従っています：

- ID ガバナンス
- 最小権限の原則
- セキュアな API 通信

ただし、最終的な DORA への準拠は、お客様による Entra の設定およびアクセスガバナンスの実装方法に依存します。影響する要素には次のようなものがあります：

- 条件付きアクセス
- 多要素認証 (MFA)
- デバイス準拠

また、SCIM 自体は Microsoft のプロビジョニング標準に準拠しており、現在の規制要件で求められる水準に対応しています。

Azure または Entra の障害によって、LSEG サービスへのアクセスに影響が生じる可能性はありますか？

お客様の認証ワークフローは、企業の ID プロバイダーとして機能する Microsoft Entra テナントに依存します。Entra は、Microsoft が提供するグローバル冗長性と高可用性を備えたサービスです。しかし、Entra でグローバル規模の障害が発生した場合、Entra により保護されているお客様の社内 IT システムへのアクセスに問題が生じる可能性があります。その結果、LSEG Workspace for HERE Core をはじめとする LSEG 製品へのサインインが一時的にできなくなる場合があります。

Entra の稼働状況およびサービス履歴は、Microsoft の公開ステータスページで確認できます。製品のドロップダウンメニューから「Microsoft Entra ID (旧 Azure AD)」を選択してください。

<https://azure.status.microsoft/en-us/status/history/>.

LSEG 製品との互換性

Entra のオンボーディングにより、リアルタイムデータへのアクセスはどのように変わりますか？

Entra のオンボーディングにより、Workspace は Entra のデバイス ID を認識できるようになります。これにより、認証されたユーザー について、リアルタイムのマーケットデータへのアクセスを一度に 1 台のデバイスに限定できます。デバイス ID の制御は、Entra の条件付きアクセス フレームワークの一部として提供されます。

Entra を利用する際、社内の ID ポータルを使用していますが、LSEG との統合で問題は発生しますか？

いいえ。社内の ID システムから最終的に Entra にフェデレーションされる構成であれば、LSEG は Entra によって検証されたユーザー オブジェクトを認識し、それを信頼できる情報源として扱います。

SCIM プロビジョニングおよび認証は、ID がどのような経路で Entra に登録されたかに関係なく、Entra テナント内に存在する情報のみに依存します。そのため、お客様の ID ポータルが引き続き正しく ID 情報を Entra と同期している限り、LSEG との統合は通常どおり機能します。詳細については [Microsoft Entra federated identity documentation](#) を参照してください。

DACS ID を別途使用している場合、それらは Entra または SCIM を介してフェデレーションされますか？

いいえ。DACS ID は、Entra と LSEG 間の ID フェデレーションの対象ではなく、SCIM によるプロビジョニングもサポートされていません。DACS ユーザーモデルの統合や変更についてご質問がある場合は、製品によって影響が異なるため、LSEG の製品チームにご相談いただくことをお勧めします。

Entra でユーザーを無効化した場合、LSEG 側ではどのような処理が行われますか？

ユーザーが Entra で無効化されると、そのユーザーは直ちに LSEG Workspace へのアクセス権を失います。さらに、SCIM 連携が構成されている場合、ユーザーが Entra で無効化または削除されると、SCIM は LSEG に対してプロビジョニング解除イベント⁵を送信します。自動ライセンス管理を構成している場合、そのユーザーに割り当てられていたライセンスは削除され、お客様のライセンスプールに返却されます。

⁵ 自動プロビジョニング解除は、SCIM 連携が構成されている場合にのみ利用できます。