

Azure AI Search のセキュリティの概要

[アーティクル] • 2024/04/11

この記事では、データと操作を保護する Azure AI Search のセキュリティ機能について説明します。

データ フロー (ネットワーク トラフィック パターン)

Azure AI Search サービスは Azure でホストされ、通常はパブリック ネットワーク接続を使用してクライアント アプリケーションからアクセスされます。このようなパターンとなることが多いですが、他のトラフィック パターンにも注意する必要があります。開発環境と運用環境をセキュリティ保護するには、すべてのエントリ ポイントと送信トラフィックについて理解しておく必要があります。

Azure AI Search には、3 つの基本的なネットワーク トラフィック パターンがあります。

- クライアントによって行われる、検索サービスへのインバウンド要求 (主要なパターン)
- 検索サービスによって発行される、Azure やそれ以外の場所の他のサービスへのアウトバウンド要求
- セキュリティ保護された Microsoft バックボーン ネットワークを介して行われる内部サービス間の要求

受信トラフィック

検索サービス エンドポイントを対象とする受信要求には、次が含まれます。

- 検索サービスでオブジェクトを作成、読み取り、更新、または削除する
- 検索ドキュメントのインデックスを読み込む
- インデックスのクエリ
- インデクサーまたはスキルセットの実行をトリガーする

[REST API](#) のページで、検索サービスによって処理される受信要求の全範囲が説明されています。

少なくとも、すべての受信要求は、次のいずれかのオプションを使用して認証される必要があります。

- キーベースの認証 (デフォルト)。受信要求が、有効な API キーを提供します。

- ロールベースのアクセス制御。認可は、検索サービスの Microsoft Entra ID とロールの割り当て経由で行われます。

さらに、[ネットワークセキュリティ機能](#)を追加して、エンドポイントへのアクセスをさらに制限できます。IP ファイアウォールでの受信の規則、またはパブリックインターネットから検索サービスを完全に遮断するプライベートエンドポイントのいずれかを作成することができます。

内部トラフィック

内部要求は、Microsoft によってセキュリティで保護され、管理されます。これらの接続を構成または制御することはできません。ネットワークアクセスをロックダウンしている場合、顧客が内部トラフィックを構成できないため、顧客からのアクションは必要ありません。

内部トラフィックは次で構成されます。

- タスク (Microsoft Entra ID 経由の認証と認可、Azure Monitor に送信されたリソースログ、Azure Private Link を使用した[プライベートエンドポイント接続](#)など) のサービス間呼び出し。
- [組み込みスキル](#)のための Azure AI サービス API への要求。
- [セマンティックランク付け](#)をサポートする機械学習モデルに対して行われた要求。

送信トラフィック

送信要求は、ユーザーがセキュリティで保護および管理できます。送信要求は、検索サービスから他のアプリケーションに向けて発生します。通常、これらの要求は、クエリ時にテキストベースのインデックス作成、スキルベースの AI エンリッチメント、ベクター化を行うために、インデクサーによって行われます。送信要求には、読み取りと書き込みの両方の操作が含まれます。

次の一覧は、セキュリティで保護された接続を構成できる送信要求の完全な列挙です。検索サービスは、検索自体のため、およびインデクサーまたはカスタム スキルのために要求を行います。

 [テーブルを展開する](#)

操作	シナリオ
インデクサー	外部データ ソースに接続してデータを取得します。 詳細については、「 Azure ネットワークセキュリティで保護されたコンテンツへのインデクサー アクセス 」を参照してください。

操作	シナリオ
インデクサー	Azure Storage に接続して、 ナレッジストア 、 キャッシュされたエンリッチメント 、 デバッグ セッション を持続させます。
カスタム スキル	サービス外でホストされている外部コードを実行している Azure Functions、Azure Web アプリ、またはその他のアプリに接続します。スキルセットの実行中に、外部処理に対する要求が送信されます。
インデクサーと垂直統合	Azure OpenAI とデプロイされた埋め込みモデルに接続するか、カスタム スキルを経由して、指定する埋め込みモデルに接続します。検索サービスは、インデックス作成中にベクター化のために埋め込みモデルにテキストを送信します。
ベクター化	クエリ時に Azure OpenAI またはその他の埋め込みモデルに接続して、ベクター検索化のために ユーザー テキスト文字列をベクターに変換 します。
検索サービス	機密データの暗号化および復号化に使用される カスタマー マネージド暗号化キー を取得するために、Azure Key Vault に接続します。

送信接続は、キーまたはデータベース ログインを含むリソースのフルアクセス接続文字列を使用して確立することも、Microsoft Entra ID とロールベースのアクセスを使用している場合は[マネージド ID](#)を使用して確立することもできます。

ファイアウォールの内側にある Azure リソースにアクセスするには、[他の Azure リソースに検索サービス要求を許可する受信規則を作成](#)します。

Azure Private Link によって保護された Azure リソースにアクセスするには、インデクサーが接続を確立するために使用的する[共有プライベート リンクを作成](#)します。

同じリージョンの検索サービスとストレージ サービスの例外

Azure Storage と Azure AI Search が同じリージョンにある場合、ネットワーク トラフィックはプライベート IP アドレス経由でルーティングされ、Microsoft バックボーン ネットワークで発生します。プライベート IP アドレスが使用されるため、ネットワークセキュリティ用に IP ファイアウォールまたはプライベート エンドポイントを構成することはできません。

次のいずれかの方法を使用して、同じリージョンの接続を構成します。

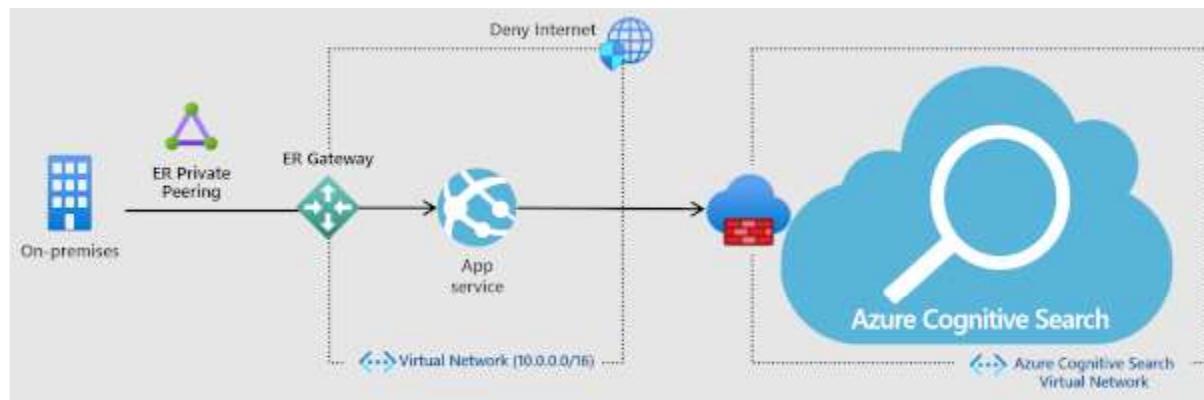
- [信頼されたサービスの例外](#)
- [リソース インスタンス ルール](#)

ネットワークのセキュリティ

ネットワークセキュリティは、ネットワークトラフィックに制御を適用することにより、未承認のアクセスや攻撃からリソースを保護します。 Azure AI Search は、未承認のアクセスに対する防御の前線になり得るネットワーク機能をサポートしています。

IP ファイアウォール経由の受信接続

検索サービスは、パブリック IP アドレスを使用して、アクセスを許可するパブリックエンドポイントによりプロビジョニングされます。パブリックエンドポイントを経由するトラフィックを制限するには、特定の IP アドレスまたは IP アドレスの特定の範囲から要求を許可する受信ファイアウォール規則を作成します。すべてのクライアント接続は、許可された IP アドレスを使用して行う必要があります。それ以外の場合、接続は拒否されます。



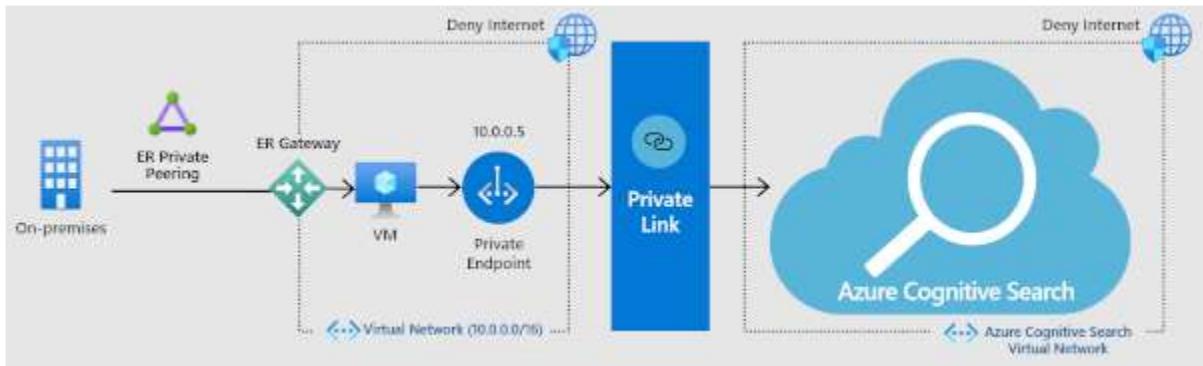
ファイアウォールアクセスを構成するには、ポータルを使用します。

または、管理 REST API を使用します。API バージョン 2020-03-13 以降では、[IpRule](#) パラメーターを指定することで、検索サービスへのアクセスを付与する IP アドレスを個別に、あるいは範囲で特定することで、サービスへのアクセスを制限できます。

プライベートエンドポイントへの受信接続 (ネットワーク分離、インターネットトラフィックなし)

より強力なセキュリティには、Azure AI Search の[プライベートエンドポイント](#)を確立して、[仮想ネットワーク](#)上のクライアントが [Private Link](#) を介して、検索インデックス内のデータに安全にアクセスできるようにします。

プライベートエンドポイントでは、検索サービスに接続するために仮想ネットワークのアドレス空間の IP アドレスが使用されます。クライアントと検索サービス間のネットワークトラフィックは、仮想ネットワークおよび Microsoft バックボーンネットワーク上のプライベートリンクを経由することで、パブリックインターネットでの露出を排除します。仮想ネットワークを使用すると、オンプレミスネットワークやインターネットで、リソース間の安全な通信が可能になります。



このソリューションは最も安全ですが、追加のサービスを使用すると、さらなるコストがかかります。そのため、使用の前に利点の詳細を明確に理解しておく必要があります。コストの詳細については、[価格ページ](#)を参照してください。これらのコンポーネントを連携させる方法の詳細については、[こちらのビデオ](#)をご覧ください。プライベート エンドポイント オプションの説明は、ビデオの 5:48 から始まります。エンドポイントを設定する方法については、[Azure AI Search でのプライベート エンドポイントの作成](#)に関するページを参照してください。

認証

検索サービス宛ての要求が承認された後も、要求が許可されているかどうかを判断する認証と認可を受ける必要があります。Azure AI Search は、2 つの方法をサポートします。

- Microsoft Entra 認証では、認証された ID として（要求ではなく）呼び出し元が確立されます。Azure ロールの割り当てが認可を決定します。
- キーベースの認証は、API キーにより（呼び出し元のアプリやユーザーではなく）要求に対して行われます。このキーは、要求が信頼できるソースからの要求であることを証明する、ランダムに生成された数字と文字で構成される文字列です。キーは要求ごとに必要です。有効なキーの送信は、要求が信頼されたエンティティのものであることの証明と見なされます。

両方の認証方法を使用することも、検索サービスで使用可能にしない[方法を無効にする](#)こともできます。

承認

Azure AI Search には、サービス管理とコンテンツ管理のためのさまざまな認可モデルが用意されています。

Azure サービス管理

リソース管理は、Microsoft Entra テナント内の[ロールベースのアクセス制御](#)によって認可されます。

Azure AI Search では、Resource Manager を使用して、サービスの作成または削除、API キーの管理、サービスのスケーリング、セキュリティの構成が行われます。そのため、[ポータル](#)、[PowerShell](#)、[Management REST API](#) のどれを使用しているかにかかわらず、Azure で割り当てられているロールによって、これらのタスクを実行できるユーザーが決定されます。

[3 つの基本ロール](#) (所有者、共同作成者、閲覧者) が検索サービスの管理に適用されます。ロールの割り当ては、サポートされている任意の方法 (ポータル、PowerShell など) を使用して行うことができ、サービス全体に適用されます。

① 注意

Azure 全体のメカニズムを使用して、サブスクリプションまたはリソースをロックし、管理者権限を持つユーザーが検索サービスを誤って、または許可なく削除しないようにすることができます。 詳細については、[リソースのロックによる予期せぬ削除の防止](#)に関するページを参照してください。

コンテンツへのアクセスを承認する

コンテンツ管理とは、検索サービスで作成およびホストされるオブジェクトを指します。

- ロールベースの認可の場合、[Azure のロールの割り当て](#)を使用して、操作に対する読み書きアクセスを確立します。
- キーベースの認可の場合、[API キー](#)と修飾されたエンドポイントによってアクセスが決定されます。エンドポイントはサービス自体、インデックスコレクション、特定のインデックス、ドキュメントコレクション、特定のドキュメントなどである場合があります。連結されている場合、エンドポイント、操作 (作成または更新要求など)、キーの種類 (管理者またはクエリ) によってコンテンツへのアクセスと操作が認可されます。

インデックスへのアクセスの制限

Azure ロールを使用している場合は、プログラムによって実行される限り、[個々のインデックスに対するアクセス許可を設定](#)できます。

キーを使用すると、サービスに対する[管理者キー](#)を持っている人は誰でも、そのサービスのインデックスの読み取り、変更、削除を行えます。インデックスが誤って削除さ

れたり、悪意によって削除されたりすることを防止するうえで、コード資産の社内ソース管理は、望ましくないインデックスの削除または変更を元に戻すための解決策になります。 Azure AI Search は可用性を確保するためにクラスター内のフェールオーバーを備えていますが、インデックスの作成または読み込みに使用される専用コードを格納したり実行したりしません。

インデックス レベルでセキュリティ境界を必要とするマルチテナント ソリューションの場合、通常、アプリケーション コードの中間層でインデックス分離を処理します。マルチテナントのユース ケースの詳細については、「[マルチテナント SaaS アプリケーションと Azure AI Search の設計パターン](#)」を参照してください。

ドキュメントへのアクセスの制限

"行レベル セキュリティ" とも呼ばれるドキュメント レベルのユーザー アクセス許可是、Azure AI Search でネイティブにはサポートされていません。 Azure Cosmos DB など、行レベル セキュリティを提供する外部システムからデータをインポートする場合、Azure AI Search によってインデックス付けされているため、そのようなアクセス許可はデータと共に転送されません。

検索結果のコンテンツに対するアクセス許可が必要な場合、ユーザー ID に基づいてドキュメントを含めるか、除外するフィルターを適用する手法があります。この回避策では、グループまたはユーザー ID を表す文字列フィールドをデータ ソースに追加します。このフィールドは、インデックスでフィルター可能にできます。次の表では、承認されていないコンテンツの検索結果をトリミングする 2 つのアプローチについて説明しています。

[+] テーブルを展開する

アプローチ	説明
ID フィルターに基づいたセキュリティによるトリミング	ユーザー ID アクセス制御を実装する基本的なワークフローについて記載しています。また、インデックスへのセキュリティ ID の追加について取り上げているほか、そのフィールドに対してフィルター処理を行い、禁止されているコンテンツの結果をトリミングする方法について説明しています。
Microsoft Entra ID に基づくセキュリティ トリミング	この記事は前の記事を拡張したものであり、Azure クラウド プラットフォームの 無料サービス の 1 つである Microsoft Entra ID から ID を取得する手順について説明しています。

データの保存場所

お客様は、検索サービスを設定するときに、顧客データがどこで格納および処理されるかを決定する場所またはリージョンを選択します。構成した機能が別の Azure リソースに依存し、そのリソースが別のリージョンにプロビジョニングされている場合を除き、Azure AI Search は、指定したリージョンの外部に顧客データを格納しません。

現在、検索サービスが書き込む唯一の外部リソースは Azure Storage です。ストレージアカウントは、お客様が指定したストレージアカウントであり、任意のリージョンに存在する可能性があります。[エンリッチメント キャッシュ](#)、[デバッグ セッション](#)、[ナレッジストア](#)のいずれかの機能を使用する場合、検索サービスは Azure Storage に書き込みます。

データ所在地のコミットメントに対する例外

オブジェクト名は、お客様が選んだリージョンまたは場所以外の場所に格納され、処理されます。お客様は、名前のフィールドに機密データを配置することや、これらのフィールドに機密データが格納されるように設計したアプリケーションを作成することはできません。このデータは、Microsoft がサービスのサポートを提供するために使うトレーメトリ ログに表示されます。オブジェクト名には、インデックス、インデクサー、データソース、スキルセット、リソース、コンテナー、キー コンテナーストアの名前が含まれます。

トレーメトリ ログは 1 年半保持されます。その間、Microsoft は次の条件下でオブジェクト名にアクセスして参照する場合があります。

- 問題の診断、機能の改善、バグの修正を行います。このシナリオでは、データ アクセスは内部のみであり、サードパーティがアクセスすることはありません。
- サポート中、問題への迅速な解決策を提供し、必要に応じて製品チームを昇格させるために、この情報が使用される場合があります

データ保護

ストレージ層には、インデックスやシノニム マップ、およびインデクサー、データソース、スキルセットの定義など、ディスクに保存されるすべてのサービス マネージドコンテンツに対するデータ暗号化が組み込まれています。サービス マネージド暗号化は、長期データストレージと一時データストレージの両方に適用されます。

必要に応じて、インデックス付きコンテンツの補足暗号化用にカスタマー マネージドキー (CMK) を追加し、保存データの二重暗号化を行うことができます。2020 年 8 月 1 日以降に作成されたサービスでは、CMK 暗号化は一時ディスクの短期データにも拡張されています。

転送中のデータ

Azure AI Search では、暗号化は接続時および転送時に開始されます。パブリックインターネット上の検索サービスでは、Azure AI Search によって HTTPS ポート 443 がリッスンされます。すべてのクライアントとサービスの間の接続では、TLS 1.2 暗号化が使用されます。より前のバージョン (1.0 または 1.1) はサポートされていません。

保存データ

検索サービスによって内部で処理されるデータについて、次の表で [データ暗号化モデル](#) を説明しています。ナレッジストア、インクリメンタルエンリッチメント、インデクサー ベースのインデックス作成などの一部の機能は、他の Azure サービスのデータ構造から読み書きされます。Azure Storage に依存するサービスでは、そのテクノロジの [暗号化機能](#) を使用できます。

[+] テーブルを展開する

モデル	キー	必要条件	制限	適用対象
サーバー側暗号化	Microsoft のマネージドキー	なし (組み込み)	なし。2018 年 1 月 24 日以降に作成されたコンテンツについては、すべてのリージョンのすべての階層で使用できます。	データディスクおよび一時ディスク上のコンテンツ (インデックスとシノニム マップ) と定義 (インデクサー、データソース、スキルセット)
サーバー側暗号化	カスタマー マネージドキー	Azure Key Vault	2020 年 8 月 1 日以降に作成されたコンテンツについては、特定のリージョンの請求対象階層で使用できます。	データディスク上のコンテンツ (インデックスとシノニム マップ)
サーバー側の完全暗号化	カスタマー マネージドキー	Azure Key Vault	2021 年 5 月 13 日以降の検索サービスについては、すべてのリージョンの請求対象階層で使用できます。	データディスクおよび一時ディスク上のコンテンツ (インデックスとシノニム マップ)

サービス マネージド キー

サービス マネージド暗号化とは、256 ビット [AES 暗号化](#) を使用する Microsoft 内部操作です。 (2018 年 1 月より前に作成された) 完全に暗号化されていないインデックスに対する増分更新を含む、すべてのインデックス作成で自動的に行われます。

サービス マネージド暗号化は、長期および短期ストレージ上のすべてのコンテンツに適用されます。

カスタマー マネージド キー (CMK)

カスタマー マネージド キーには、Azure Key Vault という別の請求対象のサービスが必要です。このリージョンは別であってもかまいませんが、Azure AI Search と同じサブスクリプションのものである必要があります。

CMK のサポートは、2 つのフェーズでロールアウトされました。最初のフェーズで検索サービスを作成した場合、CMK 暗号化は長期ストレージと特定のリージョンに制限されていました。2021 年 5 月以降の 2 番目のフェーズで作成されたサービスでは、任意のリージョンで CMK 暗号化を使用できます。2 番目のウェーブのロールアウトの一環として、コンテンツは長期ストレージと短期ストレージの両方で CMK 暗号化されます。CMK のサポートの詳細については、「[完全二重暗号化](#)」を参照してください。

CMK での暗号化を有効にすると、インデックスのサイズが増加し、クエリのパフォーマンスが低下します。これまでの観測に基づくと、実際のパフォーマンスはインデックスの定義やクエリの種類によって異なりますが、クエリ時間が 30 から 60 パーセント増加することが予想されます。パフォーマンスへの悪影響があるため、この機能を本当に必要とするインデックスでのみ有効にすることをお勧めします。 詳細については、[Azure AI Search でのカスタマー マネージド暗号化キーの構成に関するページ](#)を参照してください。

セキュリティと管理

API キーを管理する

API キーベースの認証に依存するということは、Azure のセキュリティのベストプラクティスに従って、定期的に管理者キーを再生成するための計画を立てる必要があることを意味します。Search サービスごとに最大 2 個の管理キーがあります。API キーのセキュリティと管理の詳細については、[API キーの作成と管理](#)に関する記事を参照してください。

アクティビティとリソースのログ

Azure AI Search では、ユーザー ID はログに記録されないため、特定のユーザーに関する情報のログを参照することはできません。ただし、このサービスでは、ログの作成、読み取り、更新、削除の各操作がログに記録されるため、これらのログを他のログと関連付けて、特定のアクションの機関を理解できる場合があります。

Azure でアラートとログ記録インフラストラクチャを使用すると、クエリ ボリュームの急増や、予想されるワークロードから逸脱したその他のアクションを検出できます。ログの設定の詳細については、[ログ データの収集と分析](#)および[クエリ要求の監視](#)に関する記事を参照してください。

認定資格とコンプライアンス

Azure AI Search は通常の監査に参加し、パブリック クラウドと Azure Government の両方について、グローバル、リージョン、および業界固有のさまざまな標準に対して認定を受けています。完全な一覧については、公式の監査レポート ページから [Microsoft Azure Compliance Offerings ホワイトペーパー](#) をダウンロードしてください。

コンプライアンスのために、[Microsoft クラウド セキュリティ ベンチマーク](#)の安全性の高いベストプラクティスを、[Azure Policy](#) を使用して実装できます。Microsoft クラウド セキュリティ ベンチマークは、サービスやデータに対する脅威を軽減するために実行する必要のある主要なアクションにマップされる、セキュリティ コントロールに体系化された、セキュリティに関する推奨事項を集めたものです。現在は、[ネットワークセキュリティ](#)、ログ記録および監視、[データ保護](#)などを含む 12 のセキュリティ コントロールがあります。

Azure Policy は、Microsoft クラウド セキュリティ ベンチマークの標準を含む複数の標準に対するコンプライアンスの管理に役立つ、Azure に組み込まれた機能です。広く知られたベンチマークについては、コンプライアンス非対応の場合に使用できる、基準と実施可能な対応の両方の組み込みの定義が、Azure Policy によって提供されています。

Azure AI Search には、現在 1 つの定義が組み込まれています。これはリソース ログ用です。リソース ログが欠落している検索サービスを識別するポリシーを割り当てて、有効にできます。 詳細については、「[Azure AI Search 用の Azure Policy 規制コンプライアンス コントロール](#)」を参照してください。

このビデオを観る

セキュリティ アーキテクチャと各機能カテゴリーの概要については、こちらのビデオをご覧ください。

<https://learn.microsoft.com/Shows/AI-Show/Azure-Cognitive-Search-Whats-new-in-security/player>

関連項目

- Azure セキュリティの基礎
- Azure Security ↗
- Microsoft Defender for Cloud

Azure ネットワーク セキュリティで保護されたコンテンツへのインデクサー アクセス

[アーティクル] • 2024/05/06

概念に関するこの記事では、Azure リソースが Azure 仮想ネットワークにデプロイされている場合に、検索インデクサーがネットワーク セキュリティによって保護されているコンテンツにアクセスする方法について説明します。送信トラフィック パターンとインデクサー実行環境について説明します。また、Azure AI Search でサポートされるネットワーク保護と、セキュリティ戦略に影響を与える可能性のある要因についても説明します。最後に、Azure Storage はデータ アクセスと永続ストレージの両方に使用されるため、この記事では、[検索とストレージの接続](#)に固有のネットワークの考慮事項についても説明します。

代わりに詳細な手順をお探しですか? [インデクサー アクセスを許可するようにファイアウォール規則を構成する方法](#)または[プライベート エンドポイントを介して送信接続を行う方法](#)に関する記事を参照してください。

インデクサーによってアクセスされるリソース

Azure AI 検索インデクサーは、次の 3 つの状況において、さまざまな Azure リソースへの送信呼び出しを行うことができます。

- インデックス作成中に外部のデータ ソースに接続する場合
- カスタム スキルを含むスキルセットを介して外部のカプセル化されたコードに接続する場合
- スキルセットの実行中に Azure Storage に接続してエンリッチメントをキャッシュしたり、デバッグ セッションの状態を保存したり、ナレッジストアに書き込んだりする場合

通常の実行でインデクサーがアクセスする可能性がある Azure リソースの種類を次の表に一覧表示します。

□ [テーブルを展開する](#)

リソース	インデクサー実行内の目的
Azure Storage (BLOB、ADLS Gen 2、ファイル、テーブル)	データ ソース

リソース	インデクサー実行内の目的
Azure Storage (BLOB、テーブル)	スキルセット (エンリッチメントのキャッシュ、セッションのデバッグ、ナレッジストアのプロジェクト)
Azure Cosmos DB (さまざまな API)	データ ソース
Azure SQL データベース	データ ソース
Azure 仮想マシン上の SQL Server	データ ソース
SQL Managed Instance	データ ソース
Azure Functions	スキルセットに接続され、カスタム Web API スキルのホスティングに使用される

① 注意

インデクサーは、組み込みのスキルのために Azure AI サービスにも接続します。ただし、その接続は内部ネットワーク経由で行われ、制御下のネットワークプロビジョニングの対象なりません。

インデクサーは、次の方法を使用してリソースに接続します。

- パブリック エンドポイントと資格情報
- Azure Private Link を使用したプライベート エンドポイント
- 信頼されたサービスとしての接続
- IP アドレス指定を通して接続する

Azure リソースが仮想ネットワーク上にある場合は、プライベート エンドポイントまたは IP アドレス指定を使用して、データへのインデクサー接続を許可する必要があります。

サポートされているネットワーク保護

Azure リソースは、Azure によって提供される任意の数のネットワーク分離メカニズムを使用して保護できます。リソースとリージョンに応じて Azure AI Search インデクサーは、次の表に示す制限付きで、IP ファイアウォールとプライベート エンドポイント経由で送信接続を行うことができます。

 [テーブルを展開する](#)

リソース	IP 制限	プライベート エンドポイント
Azure Storage のテキストベースのインデックス作成 (BLOB、ADLS Gen 2、ファイル、テーブル)	ストレージ アカウントと検索サービスが異なるリージョンにある場合にのみサポートされます。	サポートされています
Azure Storage の AI エンリッチメント (キャッシュ、デバッグ セッション、ナレッジ ストア)	ストレージ アカウントと検索サービスが異なるリージョンにある場合にのみサポートされます。	サポートされています
NoSQL 用 Azure Cosmos DB	サポートされています	サポートされています
Azure Cosmos DB for MongoDB	サポートされています	サポートされていない
Azure Cosmos DB for Apache Gremlin	サポートされています	サポートされていない
Azure SQL データベース	サポートされています	サポートされています
Azure 仮想マシン上の SQL Server	サポートされています	該当なし
SQL Managed Instance	サポートされています	該当なし
Azure Functions	サポートされています	Azure Functions の特定の層に対してのみサポートされます

インデクサー実行環境

Azure AI Search には、ジョブの特性に基づいて処理を最適化する "インデクサー実行環境" の概念があります。2つの環境があります。IP ファイアウォールを使用して Azure リソースへのアクセスを制御している場合は、実行環境について理解しておくと、両方の環境を含む IP 範囲を設定するのに役立ちます。

指定されたインデクサーの実行に対し、Azure AI Search で、そのインデクサーを実行するための最適な環境が決定されます。インデクサーは、割り当てられているタスクの数と種類に応じて、2つの環境のどちらかで実行されます。

 [テーブルを展開する](#)

実行環境 説明
プライベート 検索サービスの内部。プライベート環境で実行されているインデクサーは、コンピューティング リソースを、同じ検索サービス上の他のインデックス作成およびクエリのワー

実行 説明	
環境	
一ト	クロードと共有します。通常、この環境では、テキストベースのインデックス作成(スキルセットを使わない)を実行するインデクサーのみが実行されます。インデクサーとデータの間にプライベート接続を設定する場合は、これが使用できる唯一の実行環境です。
マルチテナント	追加料金なしで Microsoft によって管理およびセキュリティ保護されます。これは、ご自分の管理下にあるどのネットワーク プロビジョニングの対象にもなりません。この環境は、大量のコンピューティング処理を要する処理の負荷を軽減して、サービス固有のリソースをルーチン処理に残しておくために使います。リソースを大量に消費するインデクサー ジョブの例には、スキルセットのアタッチ、大規模なドキュメントの処理、大量のドキュメントの処理などがあります。

インデクサー実行の IP 範囲の設定

このセクションでは、どちらの実行環境からの要求でも許可する IP ファイアウォール構成について説明します。

Azure リソースがファイアウォールの内側に存在する場合は、インデクサー要求を発信できるすべての IP に対して **インデクサー接続を許可する受信規則** を設定します。これには、検索サービスで使用される IP アドレスと、マルチテナント環境で使用される IP アドレスが含まれます。

- 検索サービス(およびプライベート環境)の IP アドレスを取得するには、`nslookup`(または `ping`) で検索サービスの完全修飾ドメイン名(FQDN)を使用します。パブリック クラウドの検索サービスの FQDN は、`<service-name>.search.windows.net` です。
- インデクサーが実行される可能性のあるマルチテナント環境の IP アドレスを取得するには、`AzureCognitiveSearch` サービス タグを使用します。

[Azure サービス タグ](#)には、リージョンごとのマルチテナント環境の公開された IP アドレス範囲が含まれています。これらの IP は、[Discovery API](#) または[ダウンロード可能な JSON ファイル](#)を使用して調べることができます。IP 範囲はリージョン別に割り当てられるため、開始する前に検索サービスのリージョンを確認してください。

Azure SQL の IP 規則の設定

マルチテナント環境の IP 規則を設定する場合、特定の SQL データ ソースで IP アドレスの指定に対する単純なアプローチがサポートされます。規則内のすべての IP アドレスを列挙する代わりに、`AzureCognitiveSearch` サービス タグを指定する [ネットワークセキュリティ グループ規則](#)を作成できます。

データソースが次のいずれかである場合は、サービスタグを指定できます。

- Azure仮想マシン上のSQL Server
- SQLマネージドインスタンス

マルチテナント環境のIP規則にサービスタグを指定した場合でも、`nslookup`から取得した、プライベート実行環境(検索サービスそのものを意味する)の明示的な受信規則が必要であることに注意してください。

接続方法の選択

検索サービスは、仮想マシン上でネイティブに実行されている特定の仮想ネットワークにプロビジョニングすることはできません。一部のAzureリソースでは[仮想ネットワークサービスエンドポイント](#)が提供されますが、この機能はAzure AI検索では提供されません。次のいずれかの方法の実装を計画してください。

[+] テーブルを展開する

アプローチ	詳細
Azureリソースへの受信接続をセキュリティで保護する	インデクサーによるデータの要求を許可する受信ファイアウォール規則をAzureリソースに構成します。ファイアウォール構成には、マルチテナント実行のサービスタグと検索サービスのIPアドレスを含める必要があります。 インデクサーへのアクセスを許可するファイアウォール規則の構成 に関する記事を参照してください。
Azure AI検索とAzureリソースの間のプライベート接続	リソースへの接続のために検索サービスによって排他的に使用される共有プライベートリンクを構成します。接続は内部ネットワークを経由し、パブリックインターネットをバイパスします。リソースが完全にロックダウンされている場合(保護された仮想ネットワークで実行されている場合、またはパブリック接続で使用できない場合)、プライベートエンドポイントが唯一の選択肢となります。 プライベートエンドポイントを経由した送信接続の作成 に関するページを参照してください。

プライベートエンドポイント経由の接続は、検索サービスのプライベート実行環境から開始する必要があります。

IPファイアウォールの構成は無料です。Azure Private Linkに基づくプライベートエンドポイントは、課金に影響します。詳細については、「[Azure Private Linkの価格](#)」をご覧ください。

ネットワークセキュリティを構成したら、続いてロールの割り当てによって、どのユーザーとグループにデータと操作に対する読み取りと書き込みのアクセス権があるかを指定します。

プライベート エンドポイントの使用に関する考慮事項

このセクションでは、プライベート接続オプションに絞って説明します。

- 共有プライベート リンクには、課金対象の検索サービスが必要です。その最小レベルは、テキストベースのインデックス作成向けの Basic、またはスキルベースのインデックス作成向けの Standard 2 (S2) のいずれかです。 詳細については、[プライベート エンドポイントの数に対するレベルの制限](#)に関する記事を参照してください。
- 共有プライベート リンクが作成されると、それは検索サービスで常にその特定の Azure リソースへのすべてのインデクサー接続に使用されます。 プライベート接続はロックされ、内部的に強制されます。 パブリック接続のためにプライベート接続をバイパスすることはできません。
- 課金対象の Azure Private Link リソースが必要です。
- サブスクリプション所有者がプライベート エンドポイント接続を承認する必要があります。
- インデクサーのマルチテナント実行環境をオフにする必要があります。

これを行うには、インデクサーの `executionEnvironment` を `"Private"` に設定します。 この手順により、すべてのインデクサー実行が、検索サービス内でプロビジョニングされたプライベート環境に限定されます。 この設定のスコープは、検索サービスではなくインデクサーです。 すべてのインデクサーをプライベート エンドポイント経由で接続する場合は、それぞれに次の構成が必要です。

JSON

```
{  
    "name" : "myindexer",  
    ... other indexer properties  
    "parameters" : {  
        ... other parameters  
        "configuration" : {  
            ... other configuration properties  
            "executionEnvironment": "Private"  
        }  
    }  
}
```

リソースに対して承認されたプライベート エンドポイントができると、*private* に設定されているインデクサーは、Azure リソース用に作成および承認されたプライベート リンクを介してアクセスを取得しようとなります。

Azure AI 検索で、プライベート エンドポイントの呼び出し元に適切なロールの割り当てがなされていることが検証されます。たとえば、読み取り専用のアクセス許可があるストレージ アカウントへのプライベート エンドポイント接続を要求した場合、この呼び出しは拒否されます。

プライベート エンドポイントが承認されていない場合、またはインデクサーがプライベート エンドポイント接続を使用していない場合は、インデクサーの実行履歴に `TransientFailure` エラー メッセージが表示されます。

トークン認証を使用してネットワーク セキュリティを補完する

ファイアウォールとネットワーク セキュリティは、データと操作への未承認のアクセスを防ぐための最初の手順です。次の手順となるのが承認です。

ロールベースのアクセスをお勧めします。この場合、Microsoft Entra ID のユーザーとグループは、サービスへの読み取りと書き込みのアクセス権を決定するロールに割り当てられます。組み込みロールの説明とカスタム ロールを作成する手順については、[ロールベースのアクセス制御を使用した Azure AI 検索への接続](#)に関するページを参照してください。

キーベースの認証が必要ない場合は、API キーを無効にし、ロールの割り当てのみを使用することをお勧めします。

ネットワークで保護されたストレージ アカウントへのアクセス

検索サービスでは、インデックスとシノニム リストを格納します。ストレージを必要とするその他の機能の場合、Azure AI Search は Azure Storage に依存します。エンリッチメント キャッシュ、デバッグ セッション、ナレッジ ストアは、このカテゴリに分類されます。各サービスの場所と、ストレージ用のネットワーク保護によって、データ アクセス戦略が決まります。

同じリージョンのサービス

Azure Storage では、ファイアウォール経由でアクセスするには、要求が別のリージョンから送信されている必要があります。Azure Storage と Azure AI Search が同じリージョンにある場合は、検索サービスのシステム ID の下にあるデータにアクセスして、ストレージ アカウントの IP 制限を回避できます。

システム ID を使用してデータ アクセスをサポートするには、次の 2 つのオプションがあります。

- Azure Storage で[信頼済みサービス](#)として実行し、[信頼済みサービスの例外](#)を使用するように検索を構成します。
- Azure リソースからの受信要求を許可する[リソース インスタンス ルール](#)を Azure Storage で構成します。

上記のオプションは認証用の Microsoft Entra ID によって異なります。つまり、Microsoft Entra ログインで接続する必要があります。現在、ファイアウォール経由の同じリージョン接続では、[Azure AI Search システム割り当てマネージド ID](#) のみがサポートされています。

異なるリージョンのサービス

検索とストレージが異なるリージョンにある場合は、前述のオプションを使用するか、お使いのサービスからの要求を許可する IP ルールを設定できます。ワークフローによっては、次のセクションで説明するように、複数の実行環境のルールを設定する必要がある場合があります。

次のステップ

Azure 仮想ネットワークにデプロイされたソリューションのインデクサー データ アクセス オプションについて理解したら、次の手順として次のハウツー記事のいずれかを確認します。

- [プライベート エンドポイントへのインデクサー接続を確立する方法](#)
- [IP ファイアウォールを介してインデクサー接続を確立する方法](#)

Azure AI Search の Azure Policy 規制コンプライアンスコントロール

[アーティクル] • 2024/02/29

Azure Policy を使用して Microsoft クラウド セキュリティ ベンチマークのレコメンデーションを適用している場合は、準拠していないサービスを識別して修正するためにポリシーを作成できることは、既にご存じかもしれません。このようなポリシーは、カスタムの場合もあれば、よく知られたベストプラクティスのためのコンプライアンス条件と適切なソリューションを提供する組み込み定義に基づく場合もあります。

Azure AI Search の場合、現在、以下に示す 1 つの組み込み定義があり、ポリシー割り当てで使用できます。組み込みは、ログ記録と監視のためのものです。作成するポリシーでこの組み込み定義を使用すると、システムによってリソース ログのない検索サービスがスキャンされ、それに応じて有効にされます。

Azure Policy の規制コンプライアンスにより、さまざまなコンプライアンス基準に関連するコンプライアンス ドメインおよびセキュリティ コントロールに対して、"組み込み" と呼ばれる、Microsoft によって作成および管理されるイニシアチブ定義が提供されます。このページでは、Azure AI Search のコンプライアンス ドメインおよびセキュリティ コントロールの一覧を示します。セキュリティ コントロールの組み込みを個別に割り当てることで、Azure リソースを特定の基準に準拠させることができます。

各組み込みポリシー定義のタイトルは、Azure portal のポリシー定義にリンクしています。[ポリシーのバージョン] 列のリンクを使用すると、Azure Policy GitHub リポジトリのソースを表示できます。

① 重要

各コントロールは、1 つ以上の Azure Policy 定義に関連付けられています。これらのポリシーは、コントロールのコンプライアンスの評価に役立つ場合があります。ただし、多くの場合、コントロールと 1 つ以上のポリシーとの間には、一对一、または完全な一致はありません。そのため、Azure Policy での準拠は、ポリシー自体のみを指しています。これによって、コントロールのすべての要件に完全に準拠していることが保証されるわけではありません。また、コンプライアンス標準には、現時点でどの Azure Policy 定義でも対応されていないコントロールが含まれています。したがって、Azure Policy でのコンプライアンスは、全体のコンプライアンス状態の部分的ビューでしかありません。これらのコンプライアンス標準に対するコントロールと Azure Policy 規制コンプライアンス定義の間の関連付けは、時間の経過と共に変わることがあります。

CIS Microsoft Azure Foundations Benchmark

1.3.0

すべての Azure サービスに対して使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、[Azure Policy の規制コンプライアンス - CIS Microsoft Azure Foundations Benchmark 1.3.0](#) に関するページを参照してください。このコンプライアンス標準の詳細については、[CIS Microsoft Azure Foundations Benchmark](#) に関するページを参照してください。

[+] テーブルを展開する

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーの バージョン (GitHub)
5 ログと監視	5.3	診断ログがそれをサポートするすべてのサービスで有効になっていることを確認する	Search サービスのリソースログを有効にする必要がある	5.0.0

CIS Microsoft Azure Foundations Benchmark

1.4.0

すべての Azure サービスで使用可能な Azure Policy の組み込みがこのコンプライアンス標準にどのように対応しているのかを確認するには、[CIS v1.4.0 に関する Azure Policy の規制コンプライアンスの詳細](#)に関する記事を参照してください。このコンプライアンス標準の詳細については、[CIS Microsoft Azure Foundations Benchmark](#) に関するページを参照してください。

[+] テーブルを展開する

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーの バージョン (GitHub)
5 ログと監視	5.3	診断ログがサポートされているすべてのサービスに対して有効になっていることを確認する。	Search サービスのリソースログを有効にする必要がある	5.0.0

CIS Microsoft Azure Foundations Benchmark

2.0.0

すべての Azure サービスで使用可能な Azure Policy の組み込みがこのコンプライアンス標準にどのように対応しているのかを確認するには、[CIS v2.0.0 に関する Azure Policy の規制コンプライアンスの詳細](#)に関する記事を参照してください。このコンプライアンス標準の詳細については、[CIS Microsoft Azure Foundations Benchmark](#) に関するページを参照してください。

[+] テーブルを展開する

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
5	5.4	Azure Monitor リソース ログが、それをサポートするすべてのサービスで有効になっていることを確認します	Search サービスのリソース ログを有効にする必要があります	5.0.0 ↗

CMMC レベル 3

すべての Azure サービスで使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、[Azure Policy の規制コンプライアンス - CMMC レベル 3](#) に関する記事をご覧ください。このコンプライアンス標準の詳細については、[サイバーセキュリティ成熟度モデル認定 \(CMMC\)](#) に関するドキュメントをご覧ください。

[+] テーブルを展開する

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	AC.1.001	情報システムへのアクセスを、許可されているユーザー、許可されているユーザーの代わりに動作するプロセス、およびデバイス(他の情報システムを含む)に制限する。	Azure AI Services リソースでネットワーク アクセスを制限する必要があります	3.1.0 ↗
アクセス制御	AC.1.002	情報システムへのアクセスを、許可されているユーザーが実行を許可されているトランザクションおよび機能の種類に制限する。	Azure AI Services リソースでネットワーク アクセスを制限する必要があります	3.1.0 ↗
アクセス制御	AC.2.016	承認された認可に従って CUI のフローを制御する。	Azure AI Services リソースでネットワー	3.1.0 ↗

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
ク アクセスを制限する必要がある				
構成管理	CM.3.068	不要なプログラム、関数、ポート、プロトコル、およびサービスの使用を制限、無効化、または禁止する。	Azure AI Services リソースでネットワークアクセスを制限する必要がある	3.1.0 ↗
システムと通信の保護	SC.1.175	組織システムの外部境界と主要な内部境界で、通信 (つまり、組織システムによって送受信される情報) を監視、制御、および保護する。	Azure AI Services リソースでネットワークアクセスを制限する必要がある	3.1.0 ↗
システムと通信の保護	SC.3.183	ネットワーク通信トラフィックを既定で拒否し、ネットワーク通信トラフィックを例外的に許可する (つまり、すべて拒否し、例外的に許可する)。	Azure AI Services リソースでネットワークアクセスを制限する必要がある	3.1.0 ↗

FedRAMP High

すべての Azure サービスに対して使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、[Azure Policy の規制コンプライアンス - FedRAMP High](#) に関するページを参照してください。このコンプライアンス標準の詳細については、[FedRAMP High](#) に関するページを参照してください。

[+] テーブルを展開する

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	AC-2	アカウント管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0 ↗
アクセス制御	AC-2 (1)	システム アカウント管理の自動化	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0 ↗
アクセス制御	AC-2 (7)	ロールベースのスキーム	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0 ↗

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	AC-3	アクセスの適用	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.1.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある	1.0.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure Cognitive Search サービスではパブリックネットワーク アクセスを無効にする必要がある	1.0.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0 ↗
アクセス制御	AC-17	リモート アクセス	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある	1.0.0 ↗
アクセス制御	AC-17	リモート アクセス	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0 ↗
アクセス制御	AC-17 (1)	自動監視/制御	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある	1.0.0 ↗
アクセス制御	AC-17 (1)	自動監視/制御	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0 ↗
監査とアカウントアビリティ	AU-6 (4)	一元的なレビューと分析	Search サービスのリソース ログを有効にする必要があります	5.0.0 ↗
監査とアカウントアビリティ	AU-6 (5)	統合またはスキヤンと監視機能	Search サービスのリソース ログを有効にする必要があります	5.0.0 ↗
監査とアカウントアビリティ	AU-12	監査の生成	Search サービスのリソース ログを有効にする必要があります	5.0.0 ↗
監査とアカウントアビリティ	AU-12 (1)	システム全体または時間相關の監査証跡	Search サービスのリソース ログを有効にする必要があります	5.0.0 ↗
識別と認証	IA-2	識別と認証 (組織のユーザ)	Azure AI Services リソースのキー アクセスが無効になっている必要があります	1.1.0 ↗

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
	一)		す (□一カル認証を無効にする) ↗	
識別と認証	IA-4	識別子の管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (□一カル認証を無効にする) ↗	1.1.0 ↗
システムと通信の保護	SC-7	境界保護	Azure AI Services リソースでネットワーク アクセスを制限する必要がある ↗	3.1.0 ↗
システムと通信の保護	SC-7	境界保護	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある ↗	1.0.0 ↗
システムと通信の保護	SC-7	境界保護	Azure Cognitive Search サービスではパブリックネットワーク アクセスを無効にする必要がある ↗	1.0.0 ↗
システムと通信の保護	SC-7	境界保護	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある ↗	1.0.0 ↗
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure AI Services リソースでネットワーク アクセスを制限する必要がある ↗	3.1.0 ↗
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある ↗	1.0.0 ↗
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure Cognitive Search サービスではパブリックネットワーク アクセスを無効にする必要がある ↗	1.0.0 ↗
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある ↗	1.0.0 ↗

FedRAMP Moderate

すべての Azure サービスに対して使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、[Azure Policy の規制コンプライアンス - FedRAMP Moderate](#) に関するページを参照してください。このコンプライアンス標準の詳細については、[FedRAMP Moderate](#) に関するページを参照してください。

[+] テーブルを展開する

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	AC-2	アカウント管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (□一から認証を無効にする) ↗	1.1.0 ↗
アクセス制御	AC-2 (1)	システムアカウント管理の自動化	Azure AI Services リソースのキー アクセスが無効になっている必要があります (□一から認証を無効にする) ↗	1.1.0 ↗
アクセス制御	AC-2 (7)	ロールベースのスキーム	Azure AI Services リソースのキー アクセスが無効になっている必要があります (□一から認証を無効にする) ↗	1.1.0 ↗
アクセス制御	AC-3	アクセスの適用	Azure AI Services リソースのキー アクセスが無効になっている必要があります (□一から認証を無効にする) ↗	1.1.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure AI Services リソースでネットワークアクセスを制限する必要がある ↗	3.1.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある ↗	1.0.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure Cognitive Search サービスではパブリックネットワークアクセスを無効にする必要がある ↗	1.0.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある ↗	1.0.0 ↗
アクセス制御	AC-17	リモートアクセス	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある ↗	1.0.0 ↗
アクセス制御	AC-17	リモートアクセス	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある ↗	1.0.0 ↗
アクセス制御	AC-17 (1)	自動監視/制御	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある ↗	1.0.0 ↗
アクセス制御	AC-17 (1)	自動監視/制御	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある ↗	1.0.0 ↗
監査とアカウントタビリティ	AU-12	監査の生成	Search サービスのリソースログを有効にする必要があります ↗	5.0.0 ↗

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
識別と認証	IA-2	識別と認証 (組織のユーザー)	Azure AI Services リソースのキー アクセスが無効になっている必要があります (□一カル認証を無効にする) ↗	1.1.0 ↗
識別と認証	IA-4	識別子の管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (□一カル認証を無効にする) ↗	1.1.0 ↗
システムと通信の保護	SC-7	境界保護	Azure AI Services リソースでネットワークアクセスを制限する必要がある ↗	3.1.0 ↗
システムと通信の保護	SC-7	境界保護	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある ↗	1.0.0 ↗
システムと通信の保護	SC-7	境界保護	Azure Cognitive Search サービスではパブリックネットワークアクセスを無効にする必要がある ↗	1.0.0 ↗
システムと通信の保護	SC-7	境界保護	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある ↗	1.0.0 ↗
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure AI Services リソースでネットワークアクセスを制限する必要がある ↗	3.1.0 ↗
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある ↗	1.0.0 ↗
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure Cognitive Search サービスではパブリックネットワークアクセスを無効にする必要がある ↗	1.0.0 ↗
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある ↗	1.0.0 ↗

HIPAA HITRUST 9.2

すべての Azure サービスに対して使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、[Azure Policy の規制コンプライアンス - HIPAA HITRUST 9.2](#) に関するページを参照してください。このコンプライアンス標準の詳細については、[HIPAA HITRUST 9.2](#) に関するページを参照してください。

[+] テーブルを展開する

Domain	コントロール ID	コントロールのタイプ	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
12 監査ログと監視	1208.09aa3System.1-09.aa	1208.09aa3System.1-09.aa 09.10 監視	Search サービスのリソース ログを有効にする必要があります	5.0.0 ↗

Microsoft クラウド セキュリティ ベンチマーク

Microsoft クラウド セキュリティ ベンチマークでは、Azure 上のクラウド ソリューションをセキュリティで保護する方法に関する推奨事項が提供されます。このサービスを完全に Microsoft クラウド セキュリティ ベンチマークにマップする方法については、「[Azure Security Benchmark mapping files ↗](#)」(Azure セキュリティ ベンチマークのマッピング ファイル) を参照してください。

すべての Azure サービスに対して使用可能な Azure Policy 組み込みを、このコンプライアンス 基準に対応させる方法については、[Azure Policy の規制コンプライアンス - Microsoft クラウド セキュリティ ベンチマーク](#)に関するページを参照してください。

[+] テーブルを展開する

Domain	コントロール ID	コントロールのタイプ	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
ネットワーク のセキュリティ	NS-2	ネットワーク制御を使用してクラウド サービスをセキュリティで保護します	Azure AI Services リソースでネットワーク アクセスを制限する必要があります	3.1.0 ↗
ID 管理	IM-1	一元的な ID および認証システムを使用する	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0 ↗
ログと脅威検出	LT-3	セキュリティ調査のためのログを有効にする	Search サービスのリソース ログを有効にする必要があります	5.0.0 ↗

すべての Azure サービスに対して使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、[Azure Policy の規制コンプライアンス - NIST SP 800-171 R2](#) に関するページを参照してください。このコンプライアンス標準の詳細については、[NIST SP 800-171 R2](#) に関するページを参照してください。

[\[+\] テーブルを展開する](#)

[ドメイン]	コントロール	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	3.1.1	承認されているユーザー、承認されているユーザーの代わりに動作するプロセス、およびデバイス (他のシステムを含む) へのシステムアクセスを制限する。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
アクセス制御	3.1.1	承認されているユーザー、承認されているユーザーの代わりに動作するプロセス、およびデバイス (他のシステムを含む) へのシステムアクセスを制限する。	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある	1.0.0
アクセス制御	3.1.1	承認されているユーザー、承認されているユーザーの代わりに動作するプロセス、およびデバイス (他のシステムを含む) へのシステムアクセスを制限する。	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0
アクセス制御	3.1.12	リモート アクセス セッションの監視および制御を行う。	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある	1.0.0
アクセス制御	3.1.12	リモート アクセス セッションの監視および制御を行う。	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0
アクセス制御	3.1.13	リモート アクセス セッションの機密性を保護するため暗号化メカニズムを採用する。	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある	1.0.0
アクセス制御	3.1.13	リモート アクセス セッションの機密性を保護するため暗号化メカニズムを採用する。	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0

[ドメイン]	コントロール ロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	3.1.14	管理対象のアクセス制御ポイントを介してリモート アクセスをルーティングする。	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある	1.0.0 ↗
アクセス制御	3.1.14	管理対象のアクセス制御ポイントを介してリモート アクセスをルーティングする。	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0 ↗
アクセス制御	3.1.2	システム アクセスを、許可されたユーザーが実行を許可されているトランザクションおよび機能の種類に限定する。	Azure AI Services リソース のキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0 ↗
アクセス制御	3.1.3	承認された認可に従って CUI のフローを制御する。	Azure AI Services リソース でネットワークアクセスを制限する必要がある	3.1.0 ↗
アクセス制御	3.1.3	承認された認可に従って CUI のフローを制御する。	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある	1.0.0 ↗
アクセス制御	3.1.3	承認された認可に従って CUI のフローを制御する。	Azure Cognitive Search サービスではパブリック ネットワーク アクセスを無効にする必要がある	1.0.0 ↗
アクセス制御	3.1.3	承認された認可に従って CUI のフローを制御する。	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0 ↗
システムと通信の保護	3.13.1	組織システムの外部境界と主要な内部境界で、通信 (つまり、組織システムによって送受信される情報) を監視、制御、および保護する。	Azure AI Services リソース でネットワークアクセスを制限する必要がある	3.1.0 ↗
システムと通信の保護	3.13.1	組織システムの外部境界と主要な内部境界で、通信 (つまり、組織システムによって送受信される情報) を監視、制御、および保護する。	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある	1.0.0 ↗
システムと通信	3.13.1	組織システムの外部境界と主要な内部境界で、通信 (つまり、組織シ	Azure Cognitive Search サービスではパブリック ネ	1.0.0 ↗

[ドメイン]	コントロール ロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
信の保護		システムによって送受信される情報を監視、制御、および保護する。	ネットワークアクセスを無効にする必要がある	
システムと通信の保護	3.13.1	組織システムの外部境界と主要な内部境界で、通信 (つまり、組織システムによって送受信される情報を監視、制御、および保護する。	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0
システムと通信の保護	3.13.2	組織のシステム内で効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発手法、システムエンジニアリングの原則を採用する。	Azure AI Services リソースでネットワークアクセスを制限する必要がある	3.1.0
システムと通信の保護	3.13.2	組織のシステム内で効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発手法、システムエンジニアリングの原則を採用する。	Azure Cognitive Search サービスでは、プライベートリンクをサポートするSKUを使用する必要がある	1.0.0
システムと通信の保護	3.13.2	組織のシステム内で効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発手法、システムエンジニアリングの原則を採用する。	Azure Cognitive Search サービスではパブリックネットワークアクセスを無効にする必要がある	1.0.0
システムと通信の保護	3.13.2	組織のシステム内で効果的な情報セキュリティを促進するアーキテクチャ設計、ソフトウェア開発手法、システムエンジニアリングの原則を採用する。	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0
システムと通信の保護	3.13.5	内部ネットワークから物理的または論理的に分離されている、公的にアクセス可能なシステムコンポーネントのサブネットワークを実装する。	Azure AI Services リソースでネットワークアクセスを制限する必要がある	3.1.0
システムと通信の保護	3.13.5	内部ネットワークから物理的または論理的に分離されている、公的にアクセス可能なシステムコンポーネントのサブネットワークを実装する。	Azure Cognitive Search サービスでは、プライベートリンクをサポートするSKUを使用する必要がある	1.0.0
システムと通信	3.13.5	内部ネットワークから物理的または論理的に分離されている、公的に	Azure Cognitive Search サービスではパブリックネ	1.0.0

[ドメイン]	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
コントロール ID			
信の保護	にアクセス可能なシステムコンポーネントのサブネットワークを実装する。	ネットワークアクセスを無効にする必要がある	
システムと通信の保護	3.13.5 内部ネットワークから物理的または論理的に分離されている、公的にアクセス可能なシステムコンポーネントのサブネットワークを実装する。	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0
システムと通信の保護	3.13.6 ネットワーク通信トラフィックを既定で拒否し、ネットワーク通信トラフィックを例外的に許可する(つまり、すべて拒否し、例外的に許可する)。	Azure AI Services リソースでネットワークアクセスを制限する必要がある	3.1.0
システムと通信の保護	3.13.6 ネットワーク通信トラフィックを既定で拒否し、ネットワーク通信トラフィックを例外的に許可する(つまり、すべて拒否し、例外的に許可する)。	Azure Cognitive Search サービスではパブリックネットワークアクセスを無効にする必要がある	1.0.0
監査とアカウントアビリティ	3.3.1 違法または承認されていないシステムアクティビティの監視、分析、調査、および報告を有効にするために必要な範囲までシステム監査ログとレコードを作成して保持する	Search サービスのリソースログを有効にする必要がある	5.0.0
監査とアカウントアビリティ	3.3.2 個々のシステムユーザーのアクションからそのユーザーまで一意に確実にたどれるようにし、彼らが自分のアクションの責任を負えるようにする。	Search サービスのリソースログを有効にする必要がある	5.0.0
識別と認証	3.5.1 システムユーザー、ユーザーの代わりに動作するプロセス、およびデバイスを特定する。	Azure AI Services リソースのキーアクセスが無効になっている必要があります(一回認証を無効にする)	1.1.0
識別と認証	3.5.2 組織システムへのアクセスを許可するための前提条件として、ユーザー、プロセス、またはデバイスのIDを認証(または検証)する。	Azure AI Services リソースのキーアクセスが無効になっている必要があります(一回認証を無効にする)	1.1.0

[ドメイン]	コントロール ロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
識別と認証	3.5.5	定義された期間、識別子の再利用を防止する。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (□一カル認証を無効にする) ↗	1.1.0 ↗
識別と認証	3.5.6	定義された非アクティブな期間の経過後に識別子を無効にする。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (□一カル認証を無効にする) ↗	1.1.0 ↗

NIST SP 800-53 Rev. 4

すべての Azure サービスに対して使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、[Azure Policy の規制コンプライアンス - NIST SP 800-53 Rev. 4](#) に関するページを参照してください。このコンプライアンス標準の詳細については、[NIST SP 800-53 Rev. 4](#) に関するページを参照してください。

[+] テーブルを展開する

[ドメイン]	コントロール ロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	AC-2	アカウント管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (□一カル認証を無効にする) ↗	1.1.0 ↗
アクセス制御	AC-2(1)	システム アカウント管理の自動化	Azure AI Services リソースのキー アクセスが無効になっている必要があります (□一カル認証を無効にする) ↗	1.1.0 ↗
アクセス制御	AC-2(7)	ロールベースのスキーム	Azure AI Services リソースのキー アクセスが無効になっている必要があります (□一カル認証を無効にする) ↗	1.1.0 ↗
アクセス制御	AC-3	アクセスの適用	Azure AI Services リソースのキー アクセスが無効になっている必要があります (□一カル認証を無効にする) ↗	1.1.0 ↗

[ドメイン]	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	AC-4	情報フローの適用	Azure AI Services リソースでネットワークアクセスを制限する必要がある	3.1.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure Cognitive Search サービスでは、プライベートリンクをサポートするSKUを使用する必要がある	1.0.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure Cognitive Search サービスではパブリックネットワークアクセスを無効にする必要がある	1.0.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0 ↗
アクセス制御	AC-17	リモートアクセス	Azure Cognitive Search サービスでは、プライベートリンクをサポートするSKUを使用する必要がある	1.0.0 ↗
アクセス制御	AC-17	リモートアクセス	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0 ↗
アクセス制御	AC-17 (1)	自動監視/制御	Azure Cognitive Search サービスでは、プライベートリンクをサポートするSKUを使用する必要がある	1.0.0 ↗
アクセス制御	AC-17 (1)	自動監視/制御	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0 ↗
監査とアカウンタビリティ	AU-6 (4)	一元的なレビューと分析	Search サービスのリソースログを有効にする必要がある	5.0.0 ↗
監査とアカウンタビリティ	AU-6 (5)	統合またはスキャンと監視機能	Search サービスのリソースログを有効にする必要がある	5.0.0 ↗
監査とアカウンタビリティ	AU-12	監査の生成	Search サービスのリソースログを有効にする必要がある	5.0.0 ↗
監査とアカウンタビリティ	AU-12 (1)	システム全体または時間相関の監査証跡	Search サービスのリソースログを有効にする必要がある	5.0.0 ↗
識別と認証	IA-2	識別と認証(組織のユーザー)	Azure AI Services リソースのキーアクセスが無効になっている必要があります(□一カル認証を無効にする)	1.1.0 ↗

[ドメイン]	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
識別と認証	IA-4	識別子の管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (一カ月認証を無効にする)	1.1.0 ↗
システムと通信の保護	SC-7	境界保護	Azure AI Services リソースでネットワークアクセスを制限する必要がある	3.1.0 ↗
システムと通信の保護	SC-7	境界保護	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある	1.0.0 ↗
システムと通信の保護	SC-7	境界保護	Azure Cognitive Search サービスではパブリックネットワークアクセスを無効にする必要がある	1.0.0 ↗
システムと通信の保護	SC-7	境界保護	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0 ↗
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure AI Services リソースでネットワークアクセスを制限する必要がある	3.1.0 ↗
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure Cognitive Search サービスでは、プライベートリンクをサポートする SKU を使用する必要がある	1.0.0 ↗
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure Cognitive Search サービスではパブリックネットワークアクセスを無効にする必要がある	1.0.0 ↗
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0 ↗

NIST SP 800-53 Rev. 5

すべての Azure サービスに対して使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、[Azure Policy の規制コンプライアンス - NIST SP 800-53 Rev. 5](#) に関するページを参照してください。このコンプライアンス標準の詳細については、[NIST SP 800-53 Rev. 5](#) に関するページを参照してください。

[+] テーブルを展開する

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
アクセス制御	AC-2	アカウント管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0 ↗
アクセス制御	AC-2 (1)	システム アカウント管理の自動化	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0 ↗
アクセス制御	AC-2 (7)	特権ユーザー アカウント	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0 ↗
アクセス制御	AC-3	アクセスの適用	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.1.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure Cognitive Search サービスでは、プライベート リンクをサポートする SKU を使用する必要がある	1.0.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure Cognitive Search サービスではパブリック ネットワーク アクセスを無効にする必要がある	1.0.0 ↗
アクセス制御	AC-4	情報フローの適用	Azure Cognitive Search サービスはプライベート リンクを使用する必要がある	1.0.0 ↗
アクセス制御	AC-17	リモート アクセス	Azure Cognitive Search サービスでは、プライベート リンクをサポートする SKU を使用する必要がある	1.0.0 ↗
アクセス制御	AC-17	リモート アクセス	Azure Cognitive Search サービスはプライベート リンクを使用する必要がある	1.0.0 ↗
アクセス制御	AC-17 (1)	監視および制御	Azure Cognitive Search サービスでは、プライベート リンクをサポートする SKU を使用する必要がある	1.0.0 ↗
アクセス制御	AC-17 (1)	監視および制御	Azure Cognitive Search サービスはプライベート リンクを使用する必要がある	1.0.0 ↗
監査とアカウ	AU-6	一元的なレビ	Search サービスのリソース ログを有効	5.0.0 ↗

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
ンタビリティ	(4)	ユーザーと分析	にする必要がある	
監査とアカウントナビゲーション	AU-6 (5)	監査レコードの統合分析	Search サービスのリソース ログを有効にする必要がある	5.0.0
監査とアカウントナビゲーション	AU-12	監査レコードの生成	Search サービスのリソース ログを有効にする必要がある	5.0.0
監査とアカウントナビゲーション	AU-12 (1)	システム全体および時間相関の監査証跡	Search サービスのリソース ログを有効にする必要がある	5.0.0
識別と認証	IA-2	識別と認証 (組織のユーザー)	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
識別と認証	IA-4	識別子の管理	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
システムと通信の保護	SC-7	境界保護	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.1.0
システムと通信の保護	SC-7	境界保護	Azure Cognitive Search サービスでは、プライベート リンクをサポートする SKU を使用する必要がある	1.0.0
システムと通信の保護	SC-7	境界保護	Azure Cognitive Search サービスではパブリック ネットワーク アクセスを無効にする必要がある	1.0.0
システムと通信の保護	SC-7	境界保護	Azure Cognitive Search サービスはプライベート リンクを使用する必要がある	1.0.0
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.1.0
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure Cognitive Search サービスでは、プライベート リンクをサポートする SKU を使用する必要がある	1.0.0
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure Cognitive Search サービスではパブリック ネットワーク アクセスを無効にする必要がある	1.0.0
システムと通信の保護	SC-7 (3)	アクセス ポイント	Azure Cognitive Search サービスはプライベート リンクを使用する必要がある	1.0.0

NL BIO Cloud Theme

すべての Azure サービスで使用可能な Azure Policy の組み込みがこのコンプライアンス標準にどのように対応しているのかを確認するには、「[NL BIO Cloud Theme に関する Azure Policy の規制コンプライアンスの詳細](#)」を参照してください。このコンプライアンス標準の詳細については、「[ベースライン情報セキュリティ政府サイバーセキュリティ - デジタル政府 \(digitaleoverheid.nl\)](#)」を参照してください。

[+] テーブルを展開する

[ドメイン]	コントロール	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
U.07.1 データ分離 - 分離	U.07.1	データの永続的な分離は、マルチテナントアーキテクチャの 1 つです。パッチは制御された方法で実現されます。	Azure AI Services リソースでネットワークアクセスを制限する必要がある	3.1.0 ↗
U.07.1 データの分離 - 分離	U.07.1	データの永続的な分離は、マルチテナントアーキテクチャの 1 つです。パッチは制御された方法で実現されます。	Azure Cognitive Search サービスでは、プライベートリンクをサポートするSKUを使用する必要がある	1.0.0 ↗
U.07.1 データの分離 - 分離	U.07.1	データの永続的な分離は、マルチテナントアーキテクチャの 1 つです。パッチは制御された方法で実現されます。	Azure Cognitive Search サービスではパブリックネットワークアクセスを無効にする必要がある	1.0.0 ↗
U.07.1 データの分離 - 分離	U.07.1	データの永続的な分離は、マルチテナントアーキテクチャの 1 つです。パッチは制御された方法で実現されます。	Azure Cognitive Search サービスはプライベートリンクを使用する必要がある	1.0.0 ↗
U.07.3 データの分離 - 管理機能	U.07.3	U.07.3 - CSC データおよび/または暗号化キーを表示あるいは変更する権限は、制御された方法で付与され、使用状況がログに記録されます。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0 ↗
U.10.2 IT サービスとデータ	U.10.2	CSP の責任の下、アクセス権が管理者に付与されます。	Azure AI Services リソースのキー アクセスが無効になっている必要があります	1.1.0 ↗

ドメイン	コントロール ロール	コントロールのタイトル	ポリシー	ポリシーのバージョン
ID			(Azure portal)	(GitHub)
U.10.3 IT サービスとデータへのアクセス - ユーザー	U.10.3	IT サービスとデータにアクセスできるのは、認証された機器を持つユーザーだけです。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0 (GitHub)
U.10.5 IT サービスとデータへのアクセス - 適格性	U.10.5	IT サービスとデータへのアクセスは技術的な手段によって制限され、実装されています。	Azure AI Services リソースのキー アクセスが無効になっている必要があります (ローカル認証を無効にする)	1.1.0
U.15.1 ログ記録と監視 - イベントの記録	U.15.1	ポリシー規則の違反は、CSP と CSC によって記録されます。	Search サービスのリソース ログを有効にする必要がある	5.0.0

インド準備銀行の銀行向けの IT フレームワーク v2016

すべての Azure サービスで使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、[Azure Policy 規制コンプライアンス - RBI ITF Banks v2016](#) に関する記事を参照してください。このコンプライアンス標準の詳細については、[RBI ITF Banks v2016 \(PDF\)](#) を参照してください。

[+] テーブルを展開する

Domain	コントロール ロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
フィッシング詐欺対策		フィッシング詐欺対策-14.1	Azure AI Services リソースでネットワーク アクセスを制限する必要がある	3.1.0

RMIT マレーシア

すべての Azure サービスで使用可能な Azure Policy 組み込みがこのコンプライアンス標準にどのように対応するのかを確認するには、[Azure Policy 規制コンプライアンス - RMIT マレーシア](#)に関する記事をご覧ください。このコンプライアンス標準の詳細については、[RMIT マレーシア](#)に関するドキュメントをご覧ください。

[+] テーブルを展開する

Domain	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
デジタルサービスのセキュリティ	10.66	デジタルサービスのセキュリティ - 10.66	Search サービスの診断設定をイベントハブにデプロイする	2.0.0 ↗
デジタルサービスのセキュリティ	10.66	デジタルサービスのセキュリティ - 10.66	Search サービスの診断設定を Log Analytics ワークスペースにデプロイする	1.0.0 ↗

SWIFT CSP-CSCF v2021

すべての Azure サービスで使用できる Azure Policy の組み込みが、このコンプライアンス標準にどのように対応するかを確認するには、「[SWIFT CSP-CSCF v2021 についての Azure Policy の規制コンプライアンスの詳細](#)」を参照してください。このコンプライアンス標準の詳細については、「[SWIFT CSP CSCF v2021 ↗](#)」を参照してください。

[+] テーブルを展開する

[ドメイン]	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
システムまたはトランザクション レコードに対する異常なアクティビティの検出	6.4	ログ記録と監視	Search サービスのリソース ログを有効にする必要がある	5.0.0 ↗

SWIFT CSP-CSCF v2022

すべての Azure サービスで使用できる Azure Policy の組み込みが、このコンプライアンス標準にどのように対応するかを確認するには、「[SWIFT CSP-CSCF v2022 についての Azure Policy の規制コンプライアンスの詳細](#)」を参照してください。このコンプライアンス標準の詳細については、「[SWIFT CSP CSCF v2022 ↗](#)」を参照してください。

[+] テーブルを展開する

ドメイン	コントロール ID	コントロールのタイトル	ポリシー (Azure portal)	ポリシーのバージョン (GitHub)
6.システムまたはトランザクションコードに対する異常なアクティビティの検出	6.4	セキュリティ イベントを記録し、ローカルの SWIFT 環境内の異常なアクションと操作を検出する。	Search サービスのリソース ログを有効にする必要があります	5.0.0 ↗

次のステップ[°]

- Azure Policy の規制コンプライアンスの詳細を確認します。
- Azure Policy GitHub リポジトリ [↗](#) のビルトインを参照します。

Azure Cognitive Search の Azure セキュリティ ベースライン

[アーティクル] • 2023/09/22

このセキュリティ ベースラインは、[Microsoft クラウド セキュリティ ベンチマーク バージョン 1.0](#) のガイダンスをAzure Cognitive Searchに適用します。 Microsoft クラウド セキュリティ ベンチマークでは、Azure 上のクラウド ソリューションをセキュリティで保護する方法に関する推奨事項が提供されます。 コンテンツは、Microsoft クラウド セキュリティ ベンチマークと、Azure Cognitive Searchに適用できる関連ガイダンスによって定義されたセキュリティ制御によってグループ化されます。

このセキュリティ ベースラインとその推奨事項は、Microsoft Defender for Cloud を使用して監視できます。 Azure Policy 定義は、[クラウド ポータルの Microsoft Defender] ページの [規制コンプライアンス] セクションに一覧表示されます。

機能に関連するAzure Policy定義がある場合は、Microsoft クラウド セキュリティ ベンチマークの制御と推奨事項への準拠を測定するのに役立つ、このベースラインに一覧表示されます。一部の推奨事項では、特定のセキュリティ シナリオを有効にするために有料Microsoft Defenderプランが必要になる場合があります。

① 注意

Azure Cognitive Searchに適用されない機能は除外されています。 Microsoft クラウド セキュリティ ベンチマークに完全にマップ Azure Cognitive Search 方法については、[完全な Azure Cognitive Search セキュリティ ベースライン マッピング ファイル](#) を参照してください。

セキュリティ プロファイル

セキュリティ プロファイルは、Azure Cognitive Search の影響の大きい動作をまとめたものです。これにより、セキュリティに関する考慮事項が高まる可能性があります。

≡ テーブルを展開する

サービス動作属性	値
製品カテゴリ	AI+ML、モバイル、Web
お客様は HOST/OS にアクセスできます	アクセス権なし

サービス動作属性	値
サービスは顧客の仮想ネットワークにデプロイできます	False
顧客のコンテンツを保存する	○

ネットワークのセキュリティ

詳細については、「[Microsoft クラウド セキュリティ ベンチマーク: ネットワーク セキュリティ](#)」を参照してください。

NS-1: ネットワーク セグメント化の境界を確立する

機能

Virtual Network 統合

説明: サービスは、顧客のプライベート Virtual Network (VNet) へのデプロイをサポートします。 詳細については、[こちらを参照してください](#)。

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

ネットワーク セキュリティ グループのサポート

説明: サービス ネットワーク トラフィックは、サブネット上のネットワーク セキュリティ グループルールの割り当てを尊重します。 詳細については、[こちらを参照してください](#)。

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

NS-2: ネットワーク制御を使用してクラウド サービスをセキュリティで保護する

機能

Azure Private Link

説明: ネットワーク トラフィックをフィルター処理するためのサービス ネイティブ IP フィルタリング機能 (NSG や Azure Firewall と混同しないように)。 詳細については、[こちらを参照してください。](#)

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

機能に関する注意事項: プライベート エンドポイント経由の送信接続については、「[プライベート エンドポイント経由で送信接続を行う](#)」を参照してください。

構成ガイダンス: プライベート エンドポイントをデプロイして、リソースのプライベート アクセス ポイントを確立します。 検索サービス向けのパブリック エンドポイント上のすべての接続をブロックします。 仮想ネットワークからのデータの流出をブロックし、仮想ネットワークのセキュリティを強化します。

リファレンス: [Azure Cognitive Searchへのセキュリティで保護された接続用のプライベート エンドポイントを作成する](#)

パブリック ネットワーク アクセスの無効化

説明: サービスでは、サービス レベルの IP ACL フィルター規則 (NSG または Azure Firewall ではなく) または [パブリック ネットワーク アクセスの無効化] トグル スイッチを使用して、パブリック ネットワーク アクセスを無効にできます。 詳細については、[こちらを参照してください。](#)

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: Azure Cognitive Searchでは、Azure 仮想ネットワーク セキュリティ グループで見つかる IP 規則と同様に、ファイアウォール経由の受信アクセスの IP 規則がサポートされています。IP 規則を利用することで、検索サービスのアクセスを、承認された一連のマシンとクラウド サービスに制限できます。これらの承認された一連のマシンやサービスから検索サービスに格納されているデータにアクセスするには、引き続き呼び出し側で有効な認可トークンを提示する必要があります。

リファレンス: [Azure Cognitive Search用に IP ファイアウォールを構成する](#)

ID 管理

詳細については、「[Microsoft クラウド セキュリティ ベンチマーク: ID 管理](#)」を参照してください。

IM-1: 一元的な ID および認証システムを使用する

機能

データ プレーン アクセスに必要な Azure AD Authentication

説明: サービスでは、データ プレーン アクセスに Azure AD 認証を使用できます。 詳細については、[こちらを参照してください](#)。

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
True	True	Microsoft

構成ガイダンス: 既定のデプロイでこれが有効になっているので、追加の構成は必要ありません。

データ プレーン アクセスのローカル認証方法

説明: ローカルユーザー名やパスワードなど、データ プレーン アクセスでサポートされるローカル認証方法。 詳細については、[こちらを参照してください](#)。

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

機能に関するメモ: ローカル認証方法またはアカウントの使用は避けてください。これらは可能な限り無効にする必要があります。代わりに、可能な場合は Azure AD を使用して認証します。

構成ガイダンス: Cognitive Search では、主要な認証方法としてキーベースの認証が使用されます。インデックスの作成やクエリを実行する要求など、検索サービス エンド ポイントへの受信要求の場合、一般に使用可能な認証オプションは API キーだけです。

リファレンス: [Azure Cognitive Search 認証に API キーを使用する](#)

IM-3: アプリケーション ID を安全かつ自動的に管理する

機能

マネージド ID

説明: データプレーンアクションでは、マネージド ID を使用した認証がサポートされます。 詳細については、[こちらを参照してください](#)。

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: 可能な場合は、サービスプリンシパルの代わりに Azure マネージド ID を使用します。これにより、Azure Active Directory (Azure AD) 認証をサポートする Azure サービスとリソースに対して認証できます。マネージド ID の資格情報は、プラットフォームによって完全に管理、ローテーション、保護されており、ソースコードまたは構成ファイル内でハードコーディングされた資格情報を使用せずに済みます。

リファレンス: [Azure Active Directory を使用して検索アプリへのアクセスを承認する](#)

サービス プリンシパル

説明: データプレーンでは、サービスプリンシパルを使用した認証がサポートされています。 詳細については、[こちらを参照してください](#)。

[+] [テーブルを展開する](#)

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: この機能の構成に関する現在の Microsoft ガイダンスはありません。 organizationがこのセキュリティ機能を構成するかどうかを確認して確認してください。

IM-7: 条件に基づいてリソースへのアクセスを制限する

機能

データ プレーンへの条件付きアクセス

説明: データプレーンアクセスは、Azure AD 条件付きアクセス ポリシーを使用して制御できます。 詳細については、[こちらを参照してください](#)。

[+] [テーブルを展開する](#)

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: ワークロード内の Azure Active Directory (Azure AD) 条件付きアクセスに適用できる条件と条件を定義します。 特定の場所からのアクセスのブロックや許可、危険なサインイン動作のブロック、特定のアプリケーションに対するorganizationマネージド デバイスの要求など、一般的なユース ケースを検討してください。

IM-8: 資格情報とシークレットの公開を制限する

機能

Azure Key Vault での、サービス資格情報とシークレットの統合とストレージのサポート

説明: データプレーンでは、資格情報とシークレットストアに対する Azure Key Vault のネイティブな使用がサポートされています。 詳細については、[こちらを参照してください。](#)

[+] [テーブルを展開する](#)

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

特権アクセス

詳細については、「[Microsoft クラウド セキュリティ ベンチマーク: 特権アクセス](#)」を参照してください。

PA-1: 高い特権を持つ/管理者ユーザーを分離して制限する

機能

ローカル 管理 アカウント

説明: サービスには、ローカル管理アカウントの概念があります。 詳細については、[こちらを参照してください。](#)

[+] [テーブルを展開する](#)

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

PA-7: Just Enough Administration (最小限の特権の原則) に従う

機能

Azure RBAC for Data Plane

説明: Azure Role-Based Access Control (Azure RBAC) を使用して、サービスのデータ プレーン アクションへのアクセスを管理できます。 詳細については、[こちらを参照してください。](#)

[+] [テーブルを展開する](#)

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: Azure は、プラットフォーム上で実行されているすべてのサービスに対してグローバル ロールベースのアクセス制御 (RBAC) 承認システムを提供します。 Cognitive Search では、次の目的で Azure ロールを使用できます。

- コントロール プレーン操作 (Azure Resource Managerを介したサービス管理タスク)。
- インデックスの作成、読み込み、クエリなどのデータ プレーン操作。

リファレンス: [Azure Cognitive Searchで Azure ロールベースのアクセス制御 \(Azure RBAC\) を使用する](#)

PA-8: クラウド プロバイダー サポートのアクセス プロセスを決定する

機能

カスタマー ロックボックス

説明: カスタマー ロックボックスは、Microsoft サポートへのアクセスに使用できます。 詳細については、[こちらを参照してください。](#)

[+] [テーブルを展開する](#)

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: Microsoft がデータにアクセスする必要があるサポート シナリオでは、カスタマー ロックボックスを使用して確認し、Microsoft の各データ アクセス要求を承認または拒否します。

データの保護

詳細については、「[Microsoft クラウドセキュリティベンチマーク: データ保護](#)」を参照してください。

DP-1: 機密データを検出、分類、ラベル付けする

機能

機密データの検出と分類

説明: ツール (Azure Purview や Azure Information Protection など) は、サービスでのデータの検出と分類に使用できます。 詳細については、[こちらを参照してください](#)。

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

DP-2: 機密データをターゲットにした異常と脅威を監視する

機能

データ漏えい/損失防止

説明: サービスでは、機密データの移動 (顧客のコンテンツ内) を監視するための DLP ソリューションがサポートされています。 詳細については、[こちらを参照してください](#)。

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

DP-3: 転送中の機密データの暗号化

機能

転送中データの暗号化

説明: サービスでは、データプレーンの転送中のデータ暗号化がサポートされています。 詳細については、[こちらを参照してください](#)。

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
True	True	Microsoft

構成ガイダンス: 既定のデプロイでこれが有効になっているので、追加の構成は必要ありません。

リファレンス: [転送中の暗号化中のデータをAzure Cognitive Searchする](#)

DP-4: 保存データ暗号化を既定で有効にする

機能

プラットフォーム キーを使用した保存データの暗号化

説明: プラットフォーム キーを使用した保存データの暗号化がサポートされています。 保存中の顧客コンテンツは、これらの Microsoft マネージド キーで暗号化されます。 詳細については、[こちらを参照してください](#)。

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
True	True	Microsoft

構成ガイダンス: 既定のデプロイでこれが有効になっているので、追加の構成は必要ありません。

リファレンス: [サービスマネージド キーを使用した既定のデータ暗号化の Azure Cognitive Search](#)

DP-5: 必要に応じて保存データ暗号化でカスタマー マネージド キー オプションを使用する

機能

CMK を使用した保存データの暗号化

説明: カスタマー マネージド キーを使用した保存データの暗号化は、サービスによって格納される顧客コンテンツでサポートされています。 詳細については、[こちらを参照してください。](#)

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: 規制コンプライアンスに必要な場合は、カスタマー マネージド キーを使用した暗号化が必要なユースケースとサービススコープを定義します。 それらのサービスでカスタマー マネージド キーを使って、保存データ暗号化を有効にして実装します。

リファレンス: [Azure Cognitive Searchでデータ暗号化用にカスタマー マネージド キーを構成する](#)

DP-6: セキュア キー管理プロセスの使用

機能

Azure Key Vault でのキー管理

説明: このサービスでは、カスタマー キー、シークレット、または証明書に対する Azure Key Vault 統合がサポートされています。 詳細については、[こちらを参照してください。](#)

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: Azure Key Vaultを使用して、キーの生成、配布、ストレージなど、暗号化キーのライフサイクルを作成および制御します。定義されたスケジュールに基づいて、またはキーの廃止や侵害が発生した場合に、Azure Key Vaultとサービスのキーをローテーションして取り消します。ワークロード、サービス、またはアプリケーションレベルでカスタマー マネージド キー (CMK) を使用する必要がある場合は、キー管理のベストプラクティスに従ってください。キー階層を使用して、キー コンテナーにキー暗号化キー (KEK) を使用して別のデータ暗号化キー (DEK) を生成します。キーが Azure Key Vaultに登録され、サービスまたはアプリケーションのキー ID を介して参照されていることを確認します。独自のキー (BYOK) をサービスに持ち込む必要がある場合 (オンプレミスの HSM から Azure Key Vault に HSM で保護されたキーをインポートする場合など)、初期キーの生成とキー転送を実行するための推奨ガイドラインに従ってください。

リファレンス: [Azure Cognitive Search でデータ暗号化用にカスタマー マネージド キーを構成する](#)

DP-7: セキュリティで保護された証明書管理プロセスを使用する

機能

Azure Key Vault での証明書管理

説明: このサービスでは、顧客証明書に対する Azure Key Vault 統合がサポートされます。 詳細については、[こちらを参照してください。](#)

[+] [テーブルを展開する](#)

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

アセット管理

詳細については、「[Microsoft クラウド セキュリティ ベンチマーク: 資産管理](#)」を参照してください。

AM-2: 承認済みのサービスのみを使用する

機能

Azure Policy のサポート

説明: サービス構成は、Azure Policy経由で監視および適用できます。 詳細については、[こちらを参照してください](#)。

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: Microsoft Defender for Cloud を使用して、Azure リソースの構成を監査および適用するAzure Policyを構成します。 Azure Monitor を使用し、リソースで構成の逸脱が検出されたときにアラートを作成します。 [deny] と [deploy if not exists] 効果Azure Policy使用して、Azure リソース全体でセキュリティで保護された構成を適用します。

リファレンス: [Azure Cognitive Search ポリシー](#)

ログと脅威検出

詳細については、「[Microsoft クラウド セキュリティ ベンチマーク: ログ記録と脅威検出](#)」を参照してください。

LT-1: 脅威検出機能を有効にする

機能

サービス/製品のオファリングのための Microsoft Defender

説明: サービスには、セキュリティの問題を監視およびアラートするためのオファリング固有のMicrosoft Defender ソリューションがあります。 詳細については、[こちらを参照してください](#)。

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

LT-4: セキュリティ調査のためのログを有効にする

特徴

Azure リソース ログ

説明: サービスは、サービス固有のメトリックとログ記録を強化できるリソース ログを生成します。お客様はこれらのリソース ログを構成し、ストレージ アカウントやログ分析ワークスペースなどの独自のデータ シンクに送信できます。 詳細については、[こちらを参照してください。](#)

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
True	False	Customer

構成ガイダンス: サービスのリソース ログを有効にして、Azure Cognitive Search操作ログ、検索メトリックなどを表示します。

リファレンス: [リソース ログ Azure Cognitive Search](#)

バックアップと回復

詳細については、「[Microsoft クラウド セキュリティ ベンチマーク: バックアップと回復](#)」を参照してください。

BR-1:定期的な自動バックアップを保証する

機能

Azure Backup

説明: サービスは、Azure Backup サービスによってバックアップできます。 詳細については、[こちらを参照してください。](#)

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

サービス ネイティブ バックアップ機能

説明: サービスでは、独自のネイティブ バックアップ機能がサポートされます (Azure Backupを使用していない場合)。 詳細については、[こちらを参照してください。](#)

[+] テーブルを展開する

サポートされています	既定で有効	構成の責任
False	適用しない	適用しない

機能に関するメモ: Azure Cognitive Searchはプライマリ データストレージソリューションではないので、Microsoft はセルフサービスのバックアップと復元のための正式なメカニズムを提供していません。 ただし、独自のコードを使用してインデックスをバックアップおよび復元できます。 「[バックアップと復元の代替手段](#)」を参照してください。

構成ガイダンス: この機能は、このサービスをセキュリティで保護するためにサポートされていません。

次のステップ[°]

- Microsoft クラウド セキュリティ ベンチマークの概要を参照してください
- Azure セキュリティ ベースラインの詳細について学習する