

NO.	ご質問	回答
1	社内で既にADDSを使用している認識です。	ご質問ありがとうございます。いただいたご質問の後半部分が消えてしまったように見えますが、内容としましては、「社内に既存ADDSがるが、追加でAzure ADも使えるか？連携することができるか？」というご質問と理解しました。可能です。いま丁度説明されていますが、Azure AD Connectというツールが、オンプレ側のADDS側からオブジェクト（ユーザーIDなど）を読み取ってAzure AD側に同期（コピー）してくれます。つまり、オンプレ側をこれまでどおり正として使っていく（ユーザ追加や削除など）を行うと、自動的にAzure ADにも反映されていきます。
2	同期サーバー(AD connect)は、Windowsサーバーを使用するのでしょうか？	ご質問ありがとうございます。 Azure AD Connect は、ドメインに参加している Windows Server 2016 以降にインストールする必要があります。 詳細は、こちらに記載がございます。 https://docs.microsoft.com/ja-jp/azure/active-directory/hybrid/how-to-connect-install-prerequisites
3	システム監査で、Azureに対する権限適用のチェックが行われた場合、ポリシー定義でレポート機能がありますか？	ご質問は「ご利用中のAzure環境において高い権限を持つユーザが適切に管理されているかどうか、などをレポートする機能があるか？」というご質問と理解しました。可能です。いくつか方法はございますが、最も簡単な方法はMicrosoft Defender for Cloud (旧Azure Security Center) 機能を使い、コンプライアンスに準拠していない（適切な権限設定がされていない）リソースが全体でどの程度あり、具体的にどのリソースか、まで確認できます。

規制コンプライアンス

×

↓ レポートのダウンロード 🛡️ コンプライアンス ポリシーの管理 🔗 クエリを開く 📄 監査レポート ✉️ 経時的なコンプライアンス フック

📘 ダッシュボードで追跡する標準を完全にカスタマイズできるようになりました。上の [コンプライアンス ポリシーの管理] を選択して、ダッシュボードを更新してください。 →

Azure Security Benchmark

11 件 (全 44 件中) の 合格したコントロール

最低のコンプライアンス規制標準

17 件すべてを表示する

CMMC Level 3	0/55
NIST SP 800 171 R2	1/45
ISO 27001	1/20
SOC TSP	1/13

監査レポート

Microsoft のクラウド サービスに関するプライバシー、セキュリティ、コンプライアンス関連の最新情報を常に把握します。


開く


Azure Security Benchmark V3 ISO 27001 PCI DSS 3.2.1 SOC TSP NIST SP 800 53 R4 NIST SP 800 171 R2 Azure CIS 1.1.0 GCP CIS 1.1.0 AWS CIS 1.2.0 AWS PCI DSS 3.2.1 ...


適用可能な各コンプライアンス コントロールの下に、Defender for Cloud で実行され、そのコントロールに関連付けられている評価のセットがあります。すべて緑の場合は、これらの評価が現在合格しつつあることを意味しますが、そのコントロールに完全に準拠していることを保証してはいません。さらに、特定の規制のすべてのコントロールが Defender for Cloud の評価対象になるわけではないため、このレポートはコンプライアンス状態全体の一部を示すに過ぎません。




Azure Security Benchmark は 3 個のサブスクリプションに適用されます

☐ すべてのコンプライアンス コントロールを展開する




▼  NS. ネットワーク セキュリティ

▼  IM. ID 管理




▲  PA. 特権アクセス

▲  PA-1. 高い権限を持つユーザーと管理ユーザーを分離して制限する [コントロールの詳細](#)  

お客様の責任	リソースの種類	失敗したリソース	リソース コンプライアンスの状態
A maximum of 3 owners should be designated for subscriptions	 サブスクリプション	2 of 3	<div><div></div></div>
External accounts with owner permissions should be removed from your subscription	 サブスクリプション	2 of 3	<div><div></div></div>
There should be more than one owner assigned to subscriptions	 サブスクリプション	0 of 3	<div><div></div></div>
Deprecated accounts with owner permissions should be removed from your subscription	 サブスクリプション	0 of 3	<div><div></div></div>


▼  PA-2. アカウントとアクセス許可の継続的なアクセスを避ける [コントロールの詳細](#)  

▼  PA-3. ID とアクセスのライフサイクルを管理する [コントロールの詳細](#)  

▼  PA-4. ユーザー アクセスを定期的を確認して調整する [コントロールの詳細](#)  

▼  PA-5. 緊急アクセスを設定する [コントロールの詳細](#)  

▼  PA-6. 特権アクセス ワークステーションを使用する [コントロールの詳細](#)  

▼  PA-7. Just Enough Administration (最小限の特権) の原則に従う [コントロールの詳細](#) 