ポリシーの比較（2020/6/22 時点）

Azure CIS 1.1.0 (New)（3.1.1）	Azure Security Benchmark（4.0.0-preview）
	非推奨のアカウントをサブスクリプションから削除する必要がある
読み取りアクセス許可を持つ外部アカウントをサブスクリプションから削除する必要がある	読み取りアクセス許可を持つ外部アカウントをサブスクリプションから削除する必要がある
特定の管理操作のアクティビティ ログ アラートが存在する必要がある	
特定の管理操作のアクティビティ ログ アラートが存在する必要がある	
特定の管理操作のアクティビティ ログ アラートが存在する必要がある	
特定の管理操作のアクティビティ ログ アラートが存在する必要がある	
特定の管理操作のアクティビティ ログ アラートが存在する必要がある	
特定の管理操作のアクティビティ ログ アラートが存在する必要がある	
特定のポリシー操作のアクティビティ ログ アラートが存在する必要がある	
特定のセキュリティ操作のアクティビティ ログ アラートが存在する必要がある	
特定のセキュリティ操作のアクティビティ ログ アラートが存在する必要がある	
特定のセキュリティ操作のアクティビティ ログ アラートが存在する必要がある	
脆弱性評価ソリューションによって脆弱性を修復する必要がある	脆弱性評価ソリューションによって脆弱性を修復する必要がある
	診断設定の監査
書き込みアクセス許可を持つ外部アカウントをサブスクリプションから削除する必要がある	書き込みアクセス許可を持つ外部アカウントをサブスクリプションから削除する必要がある
	所有者アクセス許可を持つ非推奨のアカウントをサブスクリプションから削除する必要がある
所有者アクセス許可を持つ外部アカウントをサブスクリプションから削除する必要がある	所有者アクセス許可を持つ外部アカウントをサブスクリプションから削除する必要がある
重要度 - 高のアラートの電子メール通知を有効にする必要がある	
重要なアクティビティをキャプチャするには、SQL 監査設定に Action-Groups を構成しなければならない	重要なアクティビティをキャプチャするには、SQL 監査設定に Action-Groups を構成しなければならない
	指定されたメンバーの一部が Administrators グループに含まれていない Windows VM を監査する前提条件をデプロイする
	指定されたメンバーの一部が Administrators グループに含まれていない Windows VM からの監査結果を表示する
	指定されたメンバーのいずれかが Administrators グループに含まれている Windows VM を監査する前提条件をデプロイする
	指定されたメンバーのいずれかが Administrators グループに含まれている Windows VM からの監査結果を表示する
	指定されたメンバーだけで Administrators グループが構成されているわけではない Windows VM を監査する前提条件をデプロイする
	指定されたメンバーだけで Administrators グループが構成されているわけではない Windows VM からの監査結果を表示する
関数アプリを実行するために使用する場合に、'HTTP バージョン' が最新であることを確認する	
関数アプリの一部として使用する場合に、'Python バージョン' が最新であることを確認する	関数アプリの一部として使用する場合に、'Python バージョン' が最新であることを確認する
関数アプリの一部として使用する場合に、'PHP バージョン' が最新であることを確認する	関数アプリの一部として使用する場合に、'PHP バージョン' が最新であることを確認する
関数アプリの一部として使用する場合に、'Java バージョン' が最新であることを確認する	関数アプリの一部として使用する場合に、'Java バージョン' が最新であることを確認する
関数アプリの一部として使用する場合に、'.NET Framework' バージョンが最新であることを確認する	関数アプリの一部として使用する場合に、'.NET Framework' バージョンが最新であることを確認する
関数アプリで認証を有効にする必要があります	
	関数アプリに HTTPS を介してのみアクセスできるようにする
	関数アプリでリモート デバッグを無効にする
関数アプリでは最新の TLS バージョンを使用する必要がある	関数アプリでは最新の TLS バージョンを使用する必要がある
関数アプリで 'クライアント証明書 (着信クライアント証明書)' が 'オン' に設定されていることを確認する	
	関数アプリではマネージド ID を使用する必要がある
	関数アプリでは FTPS のみを必須とする
	仮想マシン上の IP 転送を無効にする必要がある
	仮想マシンを新しい Azure Resource Manager リソースに移行する必要がある
	仮想マシンは、承認された仮想ネットワークに接続する必要がある
仮想マシンの管理ポートは、Just-In-Time のネットワーク アクセス制御で保護する必要があります	仮想マシンの管理ポートは、Just-In-Time のネットワーク アクセス制御で保護する必要があります
仮想マシンにディスク暗号化を適用する必要がある	仮想マシンにディスク暗号化を適用する必要がある
	仮想マシンで管理ポートを閉じる必要がある
	仮想ネットワークでは、指定された仮想ネットワーク ゲートウェイを使用する必要がある
安全なアプリケーションのホワイトリスト登録のために適応型アプリケーション制御をマシンで有効にする必要がある	安全なアプリケーションのホワイトリスト登録のために適応型アプリケーション制御をマシンで有効にする必要がある
マシンのセキュリティ構成の脆弱性を修復する必要がある	マシンのセキュリティ構成の脆弱性を修復する必要がある
	ストレージ アカウントを新しい Azure Resource Manager リソースに移行する必要がある
ストレージ アカウントへの安全な転送を有効にする必要がある	ストレージ アカウントへの安全な転送を有効にする必要がある
ストレージ アカウントは、信頼された Microsoft サービスからのアクセスを許可する必要がある	
	ストレージ アカウントは仮想ネットワーク サービス エンドポイントを使用する必要がある
ストレージ アカウントではネットワーク アクセスを制限する必要があります	ストレージ アカウントではネットワーク アクセスを制限する必要があります
システムの更新プログラムをマシンにインストールする必要がある	システムの更新プログラムをマシンにインストールする必要がある
サブネットはネットワーク セキュリティ グループに関連付けられている必要がある	サブネットはネットワーク セキュリティ グループに関連付けられている必要がある
サブスクリプション所有者に対する重要度 - 高のアラートの電子メール通知を有効にする必要がある	
サブスクリプションのセキュリティ連絡先の電話番号を指定する必要がある	サブスクリプションのセキュリティ連絡先の電話番号を指定する必要がある
サブスクリプションのセキュリティ連絡先の電子メール アドレスを提供する必要がある	サブスクリプションのセキュリティ連絡先の電子メール アドレスを提供する必要がある
	サブスクリプションに複数の所有者が割り当てられている必要がある
サブスクリプションに対する読み取りアクセス許可を持つアカウントに対して MFA を有効にする必要がある	サブスクリプションに対する読み取りアクセス許可を持つアカウントに対して MFA を有効にする必要がある
サブスクリプションに対する書き込みアクセス許可を持つアカウントに対して MFA を有効にする必要がある	サブスクリプションに対する書き込みアクセス許可を持つアカウントに対して MFA を有効にする必要がある
	サブスクリプションには最大 3 人の所有者を指定する必要がある
サブスクリプションで所有者アクセス許可を持つアカウントに対して MFA を有効にする必要がある	サブスクリプションで所有者アクセス許可を持つアカウントに対して MFA を有効にする必要がある
サブスクリプションで Log Analytics 監視エージェントの自動プロビジョニングを有効にする必要がある	サブスクリプションで Log Analytics 監視エージェントの自動プロビジョニングを有効にする必要がある
	コンテナーのセキュリティ構成の脆弱性を修復する必要があります
キー コンテナー オブジェクトが回復可能でなければならない	キー コンテナー オブジェクトが回復可能でなければならない
	カスタム RBAC 規則の使用監査
カスタム サブスクリプションの所有者ロールは存在してはなりません	
インターネットに接続されている仮想マシンをネットワーク セキュリティ グループで保護する必要がある	インターネットに接続されている仮想マシンをネットワーク セキュリティ グループで保護する必要がある
	イベント ハブは仮想ネットワーク サービス エンドポイントを使用する必要がある
	イベント ハブにおける診断ログを有効にする必要がある
インターネットからの SSH アクセスをブロックする必要がある	
インターネットからの RDP アクセスをブロックする必要がある	
インストールする必要があるのは、許可されている VM 拡張機能のみ	
アダプティブ ネットワーク強化の推奨事項をインターネット接続仮想マシンに適用する必要がある	アダプティブ ネットワーク強化の推奨事項をインターネット接続仮想マシンに適用する必要がある
アタッチされていないディスクを暗号化する必要がある	アタッチされていないディスクを暗号化する必要がある
アクティビティ ログを 1 年以上保持する必要がある	
アクティビティ ログがあるコンテナーを含むストレージ アカウントは、BYOK を使用して暗号化する必要がある	
Web アプリを実行するために使用する場合に、'HTTP バージョン' が最新であることを確認する	
Web アプリの一部として使用する場合に、'Python バージョン' が最新であることを確認する	Web アプリの一部として使用する場合に、'Python バージョン' が最新であることを確認する
Web アプリの一部として使用する場合に、'PHP バージョン' が最新であることを確認する	Web アプリの一部として使用する場合に、'PHP バージョン' が最新であることを確認する
Web アプリの一部として使用する場合に、'Java バージョン' が最新であることを確認する	Web アプリの一部として使用する場合に、'Java バージョン' が最新であることを確認する
Web アプリの一部として使用する場合に、'.NET Framework' バージョンが最新であることを確認する	Web アプリの一部として使用する場合に、'.NET Framework' バージョンが最新であることを確認する
Web アプリで認証を有効にする必要があります	
Web アプリでは最新の TLS バージョンを使用する必要がある	Web アプリでは最新の TLS バージョンを使用する必要がある
	Web アプリではマネージド ID を使用する必要がある
	Web アプリでは FTPS を必須とする
Web アプリで 'クライアント証明書 (着信クライアント証明書)' が 'オン' に設定されていることを確認する	Web アプリで 'クライアント証明書 (着信クライアント証明書)' が 'オン' に設定されていることを確認する
Web アプリケーションには HTTPS を介してのみアクセスできるようにする	Web アプリケーションには HTTPS を介してのみアクセスできるようにする
	Web アプリケーションでリモート デバッグを無効にする
	Virtual Machines に対して Azure Backup を有効にする必要がある
	Virtual Machine Scale Sets のセキュリティ構成の脆弱性を修復する必要がある
	Virtual Machine Scale Sets のシステム更新プログラムをインストールする必要がある
	Virtual Machine Scale Sets における診断ログを有効にする必要がある
	Virtual Machine Scale Sets に Endpoint Protection ソリューションをインストールする必要がある
	SQL データベースの脆弱性を修復する必要がある
SQL データベースで Transparent Data Encryption を有効にする必要がある	SQL データベースで Transparent Data Encryption を有効にする必要がある
	SQL Server は仮想ネットワーク サービス エンドポイントを使用する必要がある
SQL Server の監査期間は 90 日以上に構成する必要がある。	SQL Server の監査期間は 90 日以上に構成する必要がある。
SQL Server の監査を有効にする必要があります	SQL Server の監査を有効にする必要があります
SQL Server の Advanced Data Security 設定にはセキュリティ アラートを受け取る電子メール アドレスを含める必要がある	SQL Server の Advanced Data Security 設定にはセキュリティ アラートを受け取る電子メール アドレスを含める必要がある
SQL Server の Advanced Data Security 設定で管理者とサブスクリプションの所有者に対する電子メール通知を有効にする必要がある	SQL Server の Advanced Data Security 設定で管理者とサブスクリプションの所有者に対する電子メール通知を有効にする必要がある
SQL Server の Advanced Data Security 設定では、Advanced Threat Protection の種類を 'All' に設定する必要があります	SQL Server の Advanced Data Security 設定では、Advanced Threat Protection の種類を 'All' に設定する必要があります
SQL Server に対して Azure Active Directory 管理者をプロビジョニングする必要がある	SQL Server に対して Azure Active Directory 管理者をプロビジョニングする必要がある
	SQL Server で脆弱性評価を有効にする必要がある
SQL Server で Advanced Data Security を有効にする必要がある	SQL Server で Advanced Data Security を有効にする必要がある
SQL Server TDE 保護機能を自分のキーで暗号化する必要がある	SQL Server TDE 保護機能を自分のキーで暗号化する必要がある
SQL Managed Instance の TDE 保護機能を自分のキーで暗号化する必要がある	SQL Managed Instance の TDE 保護機能を自分のキーで暗号化する必要がある
SQL Managed Instance の Advanced Data Security 設定に、セキュリティ アラートを受け取るメール アドレスを含める必要がある	SQL Managed Instance の Advanced Data Security 設定に、セキュリティ アラートを受け取るメール アドレスを含める必要がある
SQL Managed Instance の Advanced Data Security 設定で管理者とサブスクリプションの所有者に対するメール通知を有効にする必要がある	SQL Managed Instance の Advanced Data Security 設定で管理者とサブスクリプションの所有者に対するメール通知を有効にする必要がある
SQL Managed Instance の Advanced Data Security 設定では、Advanced Threat Protection の種類を [すべて] に設定する必要がある	SQL Managed Instance の Advanced Data Security 設定では、Advanced Threat Protection の種類を [すべて] に設定する必要がある
	SQL Managed Instance で脆弱性評価を有効にする必要がある
SQL Managed Instance で Advanced Data Security を有効にする必要がある	SQL Managed Instance で Advanced Data Security を有効にする必要がある
	Service Fabric クラスターでは、クライアント認証に Azure Active Directory のみを使用する必要がある
	Service Fabric クラスターでは、ClusterProtectionLevel プロパティを EncryptAndSign に設定する必要がある
	Service Bus は仮想ネットワーク サービス エンドポイントを使用する必要がある
	Service Bus における診断ログを有効にする必要がある
Security Center の Standard 価格レベルを選択する必要がある	
	Search サービスにおける診断ログを有効にする必要がある
PostgreSQL データベース サーバーの切断はログに記録する必要がある。	
PostgreSQL データベース サーバーでは接続の調整が有効でなければならない	
PostgreSQL データベース サーバーではログ接続が有効でなければならない	
PostgreSQL データベース サーバーではログ期間が有効でなければならない	
PostgreSQL データベース サーバーではログ チェックポイントが有効でなければならない	
PostgreSQL データベース サーバーでは [SSL 接続を強制する] が有効でなければならない	PostgreSQL データベース サーバーでは [SSL 接続を強制する] が有効でなければならない
	PostgreSQL サーバーではプライベート エンドポイントを有効にする必要がある
Network Watcher を有効にする必要がある	Network Watcher を有効にする必要がある
MySQL データベース サーバーでは [SSL 接続を強制する] が有効でなければならない	MySQL データベース サーバーでは [SSL 接続を強制する] が有効でなければならない
	MySQL サーバーではプライベート エンドポイントを有効にする必要がある
	MariaDB サーバーではプライベート エンドポイントを有効にする必要がある
	Logic Apps における診断ログを有効にする必要がある
	Log Analytics エージェントは仮想マシンにインストールする必要がある
	Log Analytics エージェントは Virtual Machine Scale Sets にインストールする必要がある
	Log Analytics エージェントが適切に接続されていない Windows VM を監査するための前提条件をデプロイする
	Log Analytics エージェントが適切に接続されていない Windows VM からの監査結果を表示する
	Key Vault は仮想ネットワーク サービス エンドポイントを使用する必要がある
Key Vault における診断ログを有効にする必要がある	Key Vault における診断ログを有効にする必要がある
	IoT Hub における診断ログを有効にする必要がある
Endpoint Protection の不足を Azure Security Center で監視する	Endpoint Protection の不足を Azure Security Center で監視する
Azure サブスクリプションにはアクティビティ ログのログ プロファイルが必要	

	Data Lake Analytics における診断ログを有効にする必要がある
	Cosmos DB は仮想ネットワーク サービス エンドポイントを使用する必要がある
	CORS で関数アプリへのアクセスをすべてのリソースには許可しない
	CORS で Web アプリケーションへのアクセスをすべてのリソースには許可しない
	CORS で API アプリへのアクセスをすべてのリソースには許可しない
	Batch アカウントにおける診断ログを有効にする必要がある
	Azure 向け Microsoft Antimalware は保護定義を自動的に更新するように構成する必要がある
	Azure Stream Analytics における診断ログを有効にする必要がある
	Azure SQL データベースの長期的な geo 冗長バックアップを有効にする必要があります
Azure Monitor ログ プロファイルでは、'書き込み'、'削除'、'アクション' の各カテゴリのログが収集される	Azure Monitor ログ プロファイルでは、'書き込み'、'削除'、'アクション' の各カテゴリのログが収集される
Azure Monitor はすべてのリージョンからアクティビティ ログを収集する必要がある	Azure Monitor はすべてのリージョンからアクティビティ ログを収集する必要がある
	Azure DDoS Protection Standard を有効にする必要がある
	Azure Database for PostgreSQL の geo 冗長バックアップを有効にする必要があります
	Azure Database for MySQL の geo 冗長バックアップを有効にする必要があります
	Azure Database for MariaDB の geo 冗長バックアップを有効にする必要があります
	Azure Data Lake Store における診断ログを有効にする必要がある
	Azure Cache for Redis へのセキュリティで保護された接続のみを有効にする必要がある
Azure Active Directory への登録が関数アプリで有効になっていることを確認する	Azure Active Directory への登録が関数アプリで有効になっていることを確認する
Azure Active Directory への登録が Web アプリで有効になっていることを確認する	Azure Active Directory への登録が Web アプリで有効になっていることを確認する
Azure Active Directory への登録が API アプリで有効になっていることを確認する	Azure Active Directory への登録が API アプリで有効になっていることを確認する
	Automation アカウントの変数は暗号化する必要があります
	App Services における診断ログを有効にする必要がある
	App Service は仮想ネットワーク サービス エンドポイントを使用する必要がある
API アプリを実行するために使用する場合に、'HTTP バージョン' が最新であることを確認する	
API アプリの一部として使用する場合に、'Python バージョン' が最新であることを確認する	API アプリの一部として使用する場合に、'Python バージョン' が最新であることを確認する
API アプリの一部として使用する場合に、'PHP バージョン' が最新であることを確認する	API アプリの一部として使用する場合に、'PHP バージョン' が最新であることを確認する
API アプリの一部として使用する場合に、'Java バージョン' が最新であることを確認する	API アプリの一部として使用する場合に、'Java バージョン' が最新であることを確認する
API アプリの一部として使用する場合に、'.NET Framework' バージョンが最新であることを確認する	API アプリの一部として使用する場合に、'.NET Framework' バージョンが最新であることを確認する
	API アプリには HTTPS を介してのみアクセスできるようにする
	API アプリでリモート デバッグを無効にする
API アプリで認証を有効にする必要があります	
API アプリでは最新の TLS バージョンを使用する必要がある	API アプリでは最新の TLS バージョンを使用する必要がある
	API アプリではマネージド ID を使用する必要がある
	API アプリでは FTPS のみを必須とする
API アプリで 'クライアント証明書 (着信クライアント証明書)' が 'オン' に設定されていることを確認する	
	[プレビュー]: すべてのインターネット トラフィックはデプロイされた Azure Firewall を介してルーティングする
	[プレビュー]: SQL データベースの機密データを分類する必要がある
	[プレビュー]: Kubernetes Services では許可された IP 範囲を定義する必要がある
[プレビュー]: Kubernetes Services ではロールベースのアクセス制御 (RBAC) を使用する必要がある	[プレビュー]: Kubernetes Services ではロールベースのアクセス制御 (RBAC) を使用する必要がある
	[プレビュー]: Kubernetes Services ではポッドのセキュリティ ポリシーを定義する必要がある
	[プレビュー]: Kubernetes Service を脆弱性のない Kubernetes バージョンにアップグレードする必要があります
	[プレビュー]: Container Registry は仮想ネットワーク サービス エンドポイントを使用する必要がある
	[プレビュー] Virtual Machines で脆弱性評価を有効にする必要がある
	'管理用テンプレート - ネットワーク' の Windows VM 構成を監査するための前提条件をデプロイする
	'管理用テンプレート - ネットワーク' の Windows VM 構成の監査結果を表示する
	'セキュリティ オプション - ネットワーク セキュリティ' の Windows VM 構成を監査するための前提条件をデプロイする
	'セキュリティ オプション - ネットワーク セキュリティ' の Windows VM 構成の監査結果を表示する
	'セキュリティ オプション - ネットワーク アクセス' の Windows VM 構成を監査するための前提条件をデプロイする
	'セキュリティ オプション - Microsoft ネットワーク サーバー' の Windows VM 構成を監査するための前提条件をデプロイする
	'セキュリティ オプション - Microsoft ネットワーク サーバー' の Windows VM 構成の監査結果を表示する
	'セキュリティ オプション - Microsoft ネットワーク クライアント' の Windows VM 構成の監査結果を表示する