

Azure Security Center (ASC) セキュリティセンター

セキュリティ体制を強化する統合インフラストラクチャ セキュリティ管理システム。Azure 内かどうにかかわらずクラウド内とオンプレミス上のハイブリッドワークロード全体を保護する高度な脅威防止機能があります。

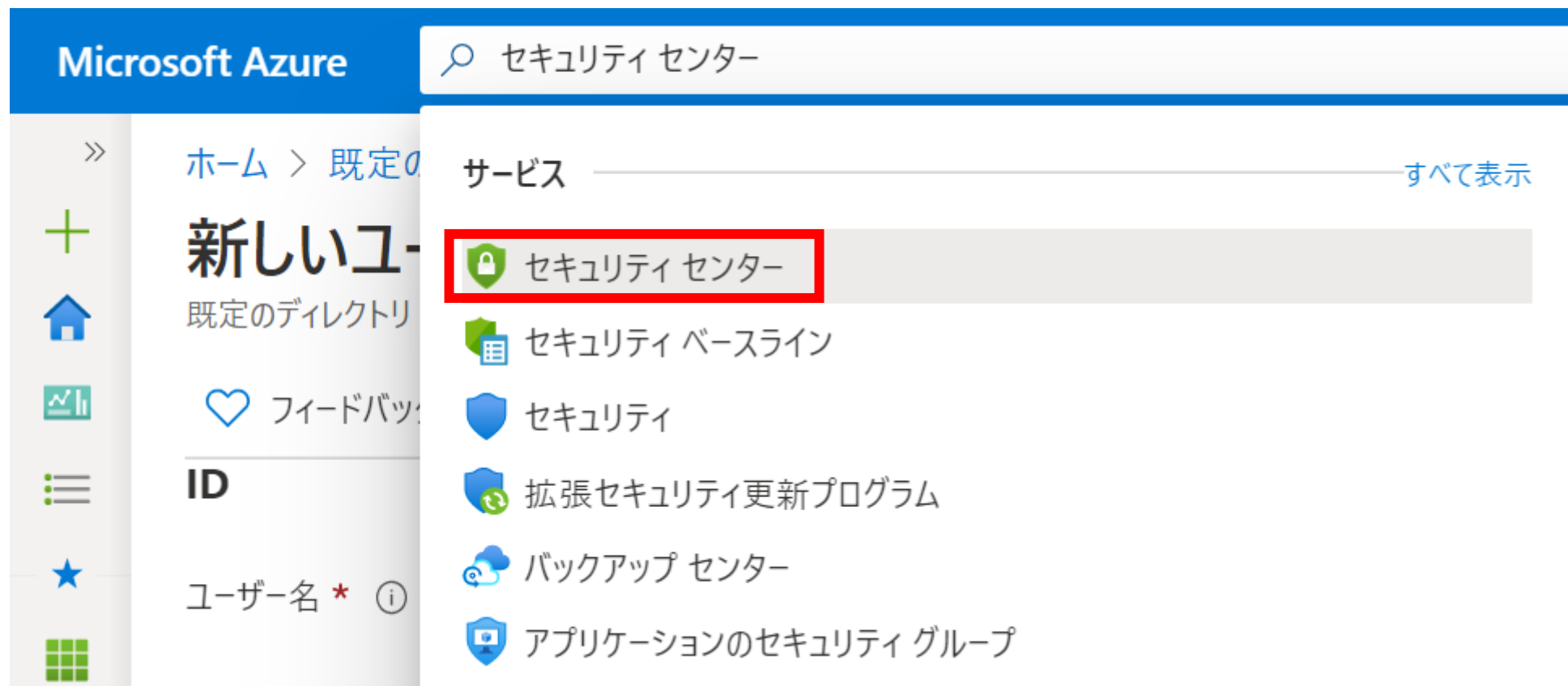
セキュリティセンターとは？

- データセンターのセキュリティ体制を強化する統合インフラストラクチャセキュリティ管理システムです。
- Azure 内かどこかにかかわらずクラウド内とオンプレミス上のハイブリッドワークロード全体を保護する高度な脅威防止機能があります。
 - たとえばAWS Config, AWS SecurityHubと連携して、AWS環境を監視することもできる
- ご自分の環境を評価することができ、リソースの状態や、それらがセキュリティで保護されているかどうかを把握できます。
- ワークロードが評価され、脅威防止の推奨事項とセキュリティアラートが生成されます。

セキュリティセンターの有効化

- ポータルのメニューから [セキュリティ センター] を選択します。
- セキュリティセンターの概要ページが表示されます。
- ご自身や他のサブスクリプション ユーザーによってまだ有効化されていない Azure サブスクリプションは、自動的に無料で有効になります。
- セキュリティセンターを初めて起動してから数分以内に、以下の項目が表示されます。
 - 接続されているリソースのセキュリティを向上させる方法についての 推奨事項。
 - Security Center によって現在評価されているリソースとそれぞれのセキュリティの状態の インベントリ (目録)。

セキュリティ センターの起動



セキュリティ センター

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

test2021-0518@outlook...

既定のディレクトリ

ホーム > セキュリティ センター

セキュリティ センター | はじめに
サブスクリプション 'Azure Pass - スポンサー プラン' を表示しています

検索 (Ctrl+/) << アップグレード

全般

概要

はじめに

推奨事項

セキュリティ警告

インベントリ

ブック

コミュニティ

クラウド セキュリティ

セキュア スコア

規制コンプライアンス

Azure Defender

Firewall Manager

管理


価格と設定

セキュリティ ポリシー

セキュリティ ソリューション

ワークフローの自動化


カバレッジ



お使いのサブスクリプションで Azure Defender を有効にします。


30 日間の無料試用版を使用開始

Security Center では、すべてのサブスクリプションのハイブリッド クラウド ワークロードで、脆弱性を発見し、脅威にさらされる機会を制限し、攻撃を検出して迅速に対応します。[詳細情報 >](#)




クラウドのセキュリティ体制の管理

Azure セキュア スコアを使用して継続的な評価と優先度付けされたセキュリティ推奨事項を取得し、規制基準へのコンプライアンスを確認します



マシンのクラウド ワークロード保護

Windows、Linux、オンプレミスのサーバーを保護します。保護には、構成と脆弱性の管理、ワークロードの強化、サーバーの EDR が含まれます



PaaS に対する高度な脅威保護

App Service プラン、ストレージ アカ운 ト、SQL Server などの PaaS ワークロードで脅威を防止し、通常と異なるアクティビティを検出します




Azure Defender を有効にする 1 個のサブスクリプション

☒ 名前

↑↓ リソースの合計

☒ Azure Pass - ... 3


合計: 3 個のリソース

 1 サーバー	\$15	サーバー/月
 0 App Service インスタンス	\$15	インスタンス/月
 0 Azure SQL データベース	\$15	サーバー/月

※下にスクロールしてください

アップグレード（Azure Defenderの有効化）を行います。

Azure Defender を有効にする 1 個のサブスクリプション

<input checked="" type="checkbox"/> 名前	↑↓	リソースの合計	Azure Defender プラン
<input checked="" type="checkbox"/>  Azure Pass - スポンサー プラン		3	オフ (試用期間は残り 30 日です)

最初の30日間、無料で「Azure Defender」を試用できます。

アップグレード

また [スキップ](#) ①
は

合計: 3 個のリソース

 1 サーバー	\$15	サーバー/月
 0 App Service インスタンス	\$15	インスタンス/月
 0 Azure SQL データベース	\$15	サーバー/月
 0 マシン上の SQL サーバー ①	\$15 \$0.015	サーバー/月 コア/時間
 0 オープンソース リレーショナル データベース (プレビュー)	\$15	サーバー/月
 1 ストレージ アカウント	0.02 ドル	10K トランザクション
 0 Kubernetes コア	2 ドル	月あたりの VM コア
 0 コンテナ レジストリ	\$0.29	画像
 1 キー コンテナ	0.02 ドル	10K トランザクション
 Resource Manager	8 月 1 日まで無料	①
 DNS	\$0.7/分の DNS クエリ	①

サポートされているリソースの種類に対して、Azure Defender の料金が自動的に課金されます。以前に使用したことがない場合は、30 日間の無料試用が適用されます。仮想マシン、SQL サーバー、App Service インスタンス、Kubernetes Service インスタンスプランは、時間単位で課金されます。Security Center の価格の詳細については、[価格ページ](#) > をご覧ください

Azure Defenderとは？

- セキュリティセンターには2つのモードがあります
 - **Azure Defender 無効** (無料モード) - Azure Defender を使用しない Security Center。セキュリティ ポリシー、継続的なセキュリティ評価、Azure リソースの保護に役立つ実践的なセキュリティの推奨事項が提供されます
 - **Azure Defender 有効** - 無料モードの機能を、プライベートおよび他のパブリック クラウドで実行されているワークロードまで拡張し、ハイブリッド クラウド ワークロード全体に統合されたセキュリティ管理と脅威防止機能を提供します。
- 脅威防止機能(threat protection)を含め、Security Center のすべての機能を有効にするには、適用可能なワークロードを含む**サブスクリプションで Azure Defender を有効にする**必要があります。

Azure Defender オフとオンの比較

Azure Defender オフ

- ✓ 継続的な評価とセキュリティの推奨事項
- ✓ Azure Secure Score
- ✗ Just In Time VM アクセス
- ✗ 適応型アプリケーション制御とネットワーク強化
- ✗ 規制コンプライアンスのダッシュボードとレポート
- ✗ Azure VM と Azure 以外のサーバーの脅威保護 (サーバー EDR を含む)
- ✗ サポートされている PaaS サービスの脅威保護

Azure Defender オン

- ✓ 継続的な評価とセキュリティの推奨事項
- ✓ Azure Secure Score
- ✓ Just In Time VM アクセス
- ✓ 適応型アプリケーション制御とネットワーク強化
- ✓ 規制コンプライアンスのダッシュボードとレポート
- ✓ Azure VM と Azure 以外のサーバーの脅威保護 (サーバー EDR を含む)
- ✓ サポートされている PaaS サービスの脅威保護

継続的な評価と推奨事項の表示、セキュリティスコアの参照は、オフ（無料）でも利用できます。
その他の高度な保護機能は、オンの場合のみ利用できます。

Azure Defenderの価格

- Azure Defender は、最初の 30 日間は無料で利用できます。
- 30 日経過した時点で、サービスの利用を継続することを選択した場合、使用量に応じた課金が始まります。

Azure Defenderを有効化しました。次に「データ収集エージェント」をインストールします。

リソース、サービス、ドキュメントの検索 (G+)

test2021-0518@outlook...
既定のディレクトリ

はじめに ...
ラン' を表示しています

エージェントのインストール はじめに

試用版の開始
1 サブスクリプションで Azure Defender の試用版を正常に開始しました

17:18

データ収集エージェントを有効にして、Security Center を最大限に活用します

セキュリティ アラートと推奨事項を受信するには、データ収集用の仮想マシンにエージェントをインストールする必要があります。

[詳細情報 >](#)

エージェントを自動でインストールします

Log Analytics エージェントは、選択されたサブスクリプションのすべての仮想マシンに自動的にインストールされます。

へ エージェントのインストール先サブスクリプションを選択する 1 管理対象リソース

<input checked="" type="checkbox"/> 名前	保護されていない...
<input checked="" type="checkbox"/> Azure Pass - スポンサー プラン	1

エージェントのイン...

エージェントを手動でインストールします

既に別のワークスペースがある場合は、仮想マシンをそのワークスペースに接続して、以下から自分でエージェントをインストールできます:

[価格と設定のページ](#)

エージェントをインストールせずに続行します

エージェントをインストールしない場合、多くの重要なセキュリティ機能は機能しません。





[エージェントをインストールせずに続行します](#)

既に SCOM または OMS エージェントのいずれかがローカルにインストールされている VM の場合であっても、Log Analytics エージェント拡張機能がインストールされて、構成済みのワークスペースに接続されることには変わりありません。


データ収集エージェントとは？


- Security Center では、セキュリティの脆弱性と脅威を監視するために、**データ収集エージェント（Log Analytics エージェント）**を使用して、Azure 仮想マシン (VM)などからデータを収集します。
- 不足している更新プログラム、OS のセキュリティ設定ミス、エンドポイント保護のステータス、正常性と脅威の防止を可視化するためには、データ収集が必要です。
- 収集される構成とイベントログ：オペレーティングシステムの種類とバージョン、Windows イベント ログ、実行中のプロセス、マシン名、IP アドレス、ログインユーザーなど


「データ収集エージェント」のインストールが開始されました。



test2021-0518@outlook...
既定のディレクトリ




 エージェントのインストールが開始されました

19:43 

1 サブスクリプションでエージェントのインストールが正常に開始されました

「Azure Defender」有効化と、「データ収集エージェント」インストールの設定が終わりました。

ホーム >

 **セキュリティ センター | 概要** ...

サブスクリプション 'Azure Pass - スポンサー プラン' を表示しています

[サブスクリプション](#) [新機能](#)

全般

概要

はじめに

推奨事項

セキュリティ警告

インベントリ

ブック

コミュニティ

クラウド セキュリティ

セキュア スコア

規制コンプライアンス

Azure Defender

Firewall Manager

管理

価格と設定

セキュリティ ポリシー

セキュリティ ソリューション

ワークフローの自動化

カバレッジ

クラウド コネクタ

表示されている情報が限られている可能性があります。テナント全体にわたる可視性を取得するには、こちらをクリックします →

1

Azure サブスクリプション

6

評価済みリソース

5

アクティブな推奨事項

--

セキュリティ アラート

セキュア スコア

正常でないリソース

4

これらのリソースを強化してスコアを改善するには、セキュリティの推奨事項に従います

現在のセキュリティ スコア

11%

4 ポイント

完了
コントロール

3/11

完了
推奨事項

14/19

[セキュリティ スコアを改善する >](#)

Azure Defender

リソースの適用範囲

100%

完全に保護するには、1 個のリソース プランを有効にします

重大度別アラート

4

0

セキュリティ警告はありません

0

High
0

Medium
0

Low
0

分析情報

最も一般的な推奨事項 (リソースごと)

ストレージアカウントは、仮想ネットワ...

脆弱性評価ソリューションを仮想マシ...

Network Watcher を有効にする必...

キー コンテナーでは、消去保護を有効...

増加の可能性が最も高いコントロール


Secure management ports +21% (8pt)

Apply system updates +16% (6pt)

Remediate vulnerabilities +16% (6pt)

[コントロールの表示 >](#)

Azure Security Center コミュニティ



GitHub 上の Azure Defender コミュニティに参加して、他のお客様やエキスパートと対話して学び、フィードバックを提供し、Azure Defender に関する知識を共有します。

Azure Defenderの設定の確認

Azure Defenderの設定の確認

ホーム > セキュリティ センター

セキュリティ センター | 価格と設定

サブスクリプション 'Azure Pass - スポンサー プラン' を表示しています

検索 (Ctrl+/)

全般

概要

はじめに

推奨事項

セキュリティ警告

インベントリ

ブック

コミュニティ

クラウド セキュリティ

セキュア スコア

規制コンプライアンス

Azure Defender

Firewall Manager

管理

価格と設定

セキュリティ ポリシー

セキュリティ ソリューション

価格と設定

Azure サブスクリプションとワークスペースの価格、データ収集、追加設定を構成します。

1 サブスクリプション

名前前で検索

名前	Azure Defender プラン
<div><div>Azure Pass - スポンサー プラン</div></div>	オン

Azure Defenderの設定の確認

ホーム > セキュリティセンター >

設定 | Azure Defender プラン

Azure Pass - スポンサー プラン

検索 (Ctrl+/)

保存

設定

Azure Defender プラン

自動プロビジョニング

電子メールの通知

脅威検出

ワークフローの自動化

連続エクスポート

クラウド コネクタ

Azure Defender では、強化されたセキュリティが提供されます。詳細情報 >

Azure Defender オフ

✓ 継続的な評価とセキュリティの推奨事項

✓ Azure Secure Score

✗ Just In Time VM アクセス

✗ 適応型アプリケーション制御とネットワーク強化

✗ 規制コンプライアンスのダッシュボードとレポート

✗ Azure VM と Azure 以外のサーバーの脅威保護 (サーバー EDR を含む)

✗ サポートされている PaaS サービスの脅威保護

Azure Defender オン

✓ 継続的な評価とセキュリティの推奨事項

✓ Azure Secure Score

✓ Just In Time VM アクセス

✓ 適応型アプリケーション制御とネットワーク強化

✓ 規制コンプライアンスのダッシュボードとレポート

✓ Azure VM と Azure 以外のサーバーの脅威保護 (サーバー EDR を含む)

✓ サポートされている PaaS サービスの脅威保護

Azure Defender プランが適用されるのは、このサブスクリプションのうち 3 個のリソースです

リソースの種類別に Azure Defender プランを選択

すべて有効にする

Azure Defender のプラン	リソースの数	価格	プラン
サーバー	1 台のサーバー	\$15/サーバー/月	<div>オン</div> <div>オフ</div>
App Service	0 個のインスタンス	\$15/インスタンス/月	<div>オン</div> <div>オフ</div>
Azure SQL データベース	0 個のサーバー	\$15/サーバー/月	<div>オン</div> <div>オフ</div>
マシン上の SQL サーバー	0 個のサーバー	\$15/サーバー/月 \$0.015/コア/時間	<div>オン</div> <div>オフ</div>
オープンソース リレーショナル データベース...	0 サーバー	\$15/サーバー/月	<div>オン</div> <div>オフ</div>

Azure Defenderはオン
になっています。

たくさんの「Azure
Defenderプラン」があり、
デフォルトではすべてオン
になります。

Azure Defenderの「プラン」

- Azure Defender にはさまざまな「プラン」があります。
 - Azure Defender for App Service
 - Azure Defender for Storage
 - Azure Defender for SQL
 - など、10種類（2021/5現在）
- デフォルトではすべてのプランがオンになります。
- プランは個別に価格設定されています。個別に有効/無効に設定できます。
 - たとえば、App Service を使用していない場合、「Azure Defender for App Service」をオフにすることができます。

自動プロビジョニングの設定の確認

ホーム > セキュリティセンター > 設定

設定 | 自動プロビジョニング ...
Azure Pass - スポンサー プラン

検索 (Ctrl+/)

設定

Azure Defender プラン

自動プロビジョニング

電子メールの通知

脅威検出

ワークフローの自動化

連続エクスポート

クラウド コネクタ

保存

自動プロビジョニング - 拡張機能

Security Center では、お使いのリソースとサービスからセキュリティデータとイベントを収集し、脅威を検出、対応を行います。セキュリティ ポリシーを割り当てると、拡張機能を有効にしたときに、それが新規または既存のリソースにインストールされます。[詳細情報](#)

すべての拡張機能を有効にする

拡張機能	状態	拡張機能がないリソース	説明	構成
Azure VM の Log Analytics エージェント	オン	1 個中 1 個の 仮想マシン インベントリに表示	分析のためにセキュリティ関連の構成とイベント ログをマシンから収集し、そのデータを Log Analytics ワークスペースに保存します。 詳細情報	選択したワークスペース: Azure Defender の既定のワークスペース 構成の編集
Microsoft Dependency Agent (プレビュー)	オフ	0 個中 0 個の 仮想マシン	VM Insights サービス にオンボードすると、ネットワークトラフィック データを収集して格納できます。 詳細情報	-
Kubernetes 用の Policy アドオン	オフ	0 個中 0 個の マネージド クラスター	Gatekeeper v3 が拡張され、一元的で整合性のある方法で、規模に応じた実施と保護がクラスターに適用されます。Kubernetes v1.14.0 以降が必要です。 詳細情報 。	-

データ収集エージェント
(Log Analyticsエージェント) の
自動プロビジョニングが
オンになっています。

仮想マシンの作成 ...

基本 ディスク ネットワーク **管理** 詳細 タグ 確認および作成

VM の監視と管理のオプションを構成します。

Azure Security Center

Azure Security Center では、統合されたセキュリティ管理と高度な脅威防止機能がハイブリッド クラウド ワークロードに提供されます。

[詳細情報](#) 

✔ ご利用のサブスクリプションは、Azure Security Center の Standard プランで保護されています。

自動プロビジョニングが有効なため、
データ収集エージェントが
自動でインストールされます。

VM作成後、拡張機能の確認（上：Linux VM、下：Windows VM）

test | 拡張機能 ...
仮想マシン

検索 (Ctrl+/)

概要
アクティビティ ログ
アクセス制御 (IAM)
タグ

+ 追加

項目の検索とフィルター...

名前	種類	バージョン	状態
OmsAgentForLinux	Microsoft.EnterpriseCloud.Monitoring...	1.*	Provisioning succeeded

Linux用のデータ収集エージェント（Log Analyticsエージェント）の拡張機能が導入されます。

ホーム > test2
test2 | 拡張機能 ...
仮想マシン

検索 (Ctrl+/)

概要
アクティビティ ログ
アクセス制御 (IAM)

+ 追加

項目の検索とフィルター...

名前	種類	バージョン
MicrosoftMonitoringAgent	Microsoft.EnterpriseCloud.Monitoring.MicrosoftMonitoringA...	1.*

Windows用のデータ収集エージェント（Log Analyticsエージェント）の拡張機能が導入されます。

セキュリティセンターの
アーキテクチャ

セキュリティセンターを有効化すると、自動的に「DefaultResourceGroup-EUS」といったリソースグループ、「DefaultWorkspace-~~~~-EUS」といったLog Analyticsワークスペースが作成されます。

DefaultResourceGroup-EUS

リソース グループ

検索 (Ctrl+/)

追加

列の編集

リソース グループの削除

更新

CSV にエクスポート

クエリを開く

フィードバック

モバイルで開く

...

概要

アクティビティ ログ

アクセス制御 (IAM)

タグ

イベント

設定

リソース コスト

デプロイ

セキュリティ

ポリシー

プロパティ

ロック

監視

分析情報 (プレビュー)

警告

基本

サブスクリプション (変更)
Azure Pass - スポンサー プラン

サブスクリプション ID
1f28afed-09e4-4089-98f0-b217bf3940dd

タグ (変更)
タグを追加するにはここをクリック

デプロイ
1 成功

場所
米国東部

任意のフィールドのフィルタ...

種類 == すべて

場所 == すべて

フィルターの追加

5 件中 1 ~ 5 件のレコードを表示しています。

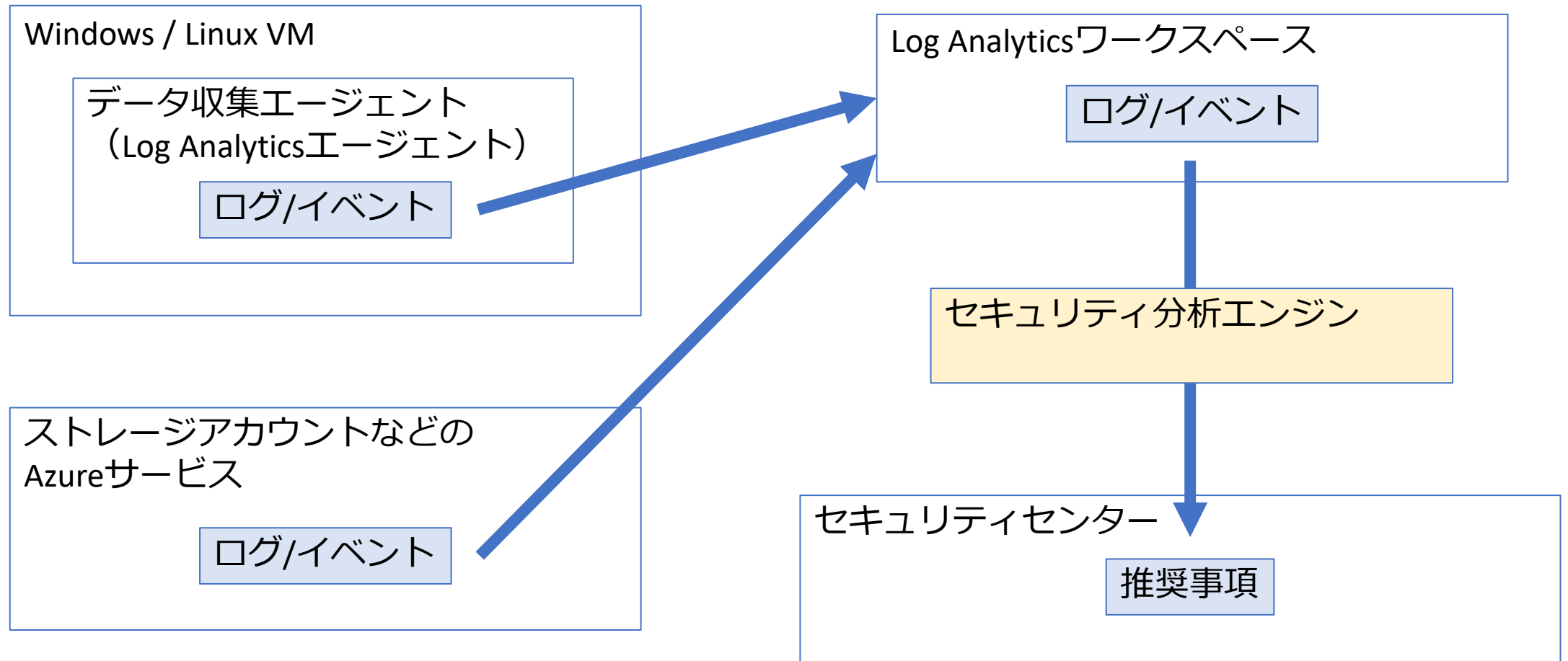
非表示の型の表示

グループ化なし

リストビュー

名前 ↑↓	種類 ↑↓	場所 ↑↓
<input type="checkbox"/> DefaultWorkspace-1f28afed-09e4-4089-98f0-b217bf3940dd-EUS	Log Analytics ワークスペース	米国東部
<input type="checkbox"/> Security(DefaultWorkspace-1f28afed-09e4-4089-98f0-b217bf3940dd-EUS)	ソリューション	米国東部
<input type="checkbox"/> SecurityCenterFree(DefaultWorkspace-1f28afed-09e4-4089-98f0-b217bf3940dd-EUS)	ソリューション	米国東部
<input type="checkbox"/> SQLAdvancedThreatProtection(DefaultWorkspace-1f28afed-09e4-4089-98f0-b217bf3940dd-EUS)	ソリューション	米国東部
<input type="checkbox"/> SQLVulnerabilityAssessment(DefaultWorkspace-1f28afed-09e4-4089-98f0-b217bf3940dd-EUS)	ソリューション	米国東部

データ収集エージェントと Azure から収集されたイベントは、セキュリティ分析エンジンで相互に関連付けられ、調整された**推奨事項** (強化タスク) が提供されます。これに従うことで、ワークロードをセキュリティで保護できます。



セキュリティポリシー

管理グループ、サブスクリプション全体、さらにはテナント全体に対して実行するように「セキュリティ ポリシー」を設定できます。ポリシーの評価結果は、推奨事項の生成に利用されます。

セキュリティセンターの「セキュリティ ポリシー」

ホーム > セキュリティ センター



セキュリティ センター | セキュリティ ポリシー ...

サブスクリプション 'Azure Pass - スポンサー プラン' を表示しています

<<

全般

 概要

 はじめに

 推奨事項

 セキュリティ警告

 インベントリ

 ブック

 コミュニティ

クラウド セキュリティ

 セキュア スコア

 規制コンプライアンス

 Azure Defender

 Firewall Manager

管理

 価格と設定

 セキュリティ ポリシー

 セキュリティ ソリューション

 ワークフローの自動化

 カバレッジ

 クラウド コネクタ



ポリシー管理

次のタスクを実行するには、以下の一覧からサブスクリプションまたは管理グループを選択してください。

- 既定の ASC ポリシーを表示および編集する
- カスタム ポリシーを追加する
- コンプライアンス ダッシュボードに規制コンプライアンス標準を追加する

詳細については、[ここをクリックしてください](#) >

1 サブスクリプション

名前	既定のポリシー
 Azure Pass - スポンサー プラン	割り当て済み

セキュリティセンターの「セキュリティ ポリシー」

[ホーム](#) > [セキュリティ センター](#) >

セキュリティ ポリシー ...

Azure Pass - スポンサー プラン

以下に対するセキュリティ ポリシー: Azure Pass - スポンサー プラン

この subscription で有効になっているポリシー



Security Center の既定のポリシー

これは、お使いのサブスクリプションで既定で有効になっている Azure Security Center 推奨事項の既定のポリシーです。

割り当て	割り当て日	監査ポリシー	拒否ポリシー	無効化ポリシー	除外対象ポリシー	
ASC Default (subscription: 1f28afed-09e4-408...	サブスクリプション	185	0	7	0	...



業界および規制の基準



カスタム イニシアティブ

ASC Default という「規定のポリシー」がサブスクリプションに割り当てされている。

「セキュリティポリシー」の実体は、サブスクリプションに割り当てされた「Azure Policy」（正確にはイニシアティブ）。

ホーム > サブスクリプション > Azure Pass - スポンサー プラン > ポリシー

ポリシー | コンプライアンス

検索 (Ctrl+/)

ポリシーの割り当て | イニシアティブの割り当て | 最新の情報に更新

概要

はじめに

コンプライアンス

修復

イベント

作成

割り当て

定義

適用除外

関連サービス

ブループリント (プレビュー)

Resource Graph

ユーザー プライバシー

スコープ

Azure Pass - スポンサー プラン

種類

すべての定義の種類

コンプライアンスの状態

すべてのコンプライアンスの状態

検索

名前または ID でフィルター処理...

リソースの全体的なコンプライアンス

11%

9 からの 1

コンプライアンスの状態別のリソース

1 - 準拠している

0 - 適用外

8 - 準拠していない

9

準拠していないイニシアティブ

1

(3 個のうち)

準拠していないポリシー

47

(203 個のうち)

名前	スコープ	コンプライアンスの状態	リソースのコンプライア...	準拠していないリソース	準拠していないポ!
ASC Default (subscription: 1f28afed-...	Azure Pass - スポンサー プラン	準拠していない	11% (1/9)	8	47
ASC DataProtection (subscription: 1f...	Azure Pass - スポンサー プラン	準拠している	100% (0/0)	0	0
ASC OpenSourceRelationalDatabases...	Azure Pass - スポンサー プラン	準拠している	100% (0/0)	0	0

セキュリティセンターの「セキュリティ ポリシー」

Security Center を有効にすると、Security Center に組み込まれたセキュリティ ポリシーが、Security Center カテゴリの組み込みのイニシアティブとして Azure Policy に反映されます。

組み込みのイニシアティブは、Security Center のすべての登録済みサブスクリプションに対して (Azure Defender が有効になっているかどうかに関係なく) 自動的に割り当てられます。

セキュリティセンターの「セキュリティ ポリシー」

ホーム > セキュリティ センター >

セキュリティ ポリシー ...

Azure Pass - スポンサー プラン

以下に対するセキュリティ ポリシー: Azure Pass - スポンサー プラン

この subscription で有効になっているポリシー

Security Center の既定のポリシー

業界および規制の基準

コンプライアンス ダッシュボードに表示できるコンプライアンス ポリシー。より多くのコンプライアンス標準を追加するには、[標準をさらに追加] をクリックします。

Azure Security Benchmark	推奨されたポリシーと評価のセットに基づいて、コンプライアンス ダッシュボードで Azure セキュリティ ベンチマークのコントロールを追跡します。	既定
PCI DSS 3.2.1	推奨されたポリシーと評価のセットに基づいて、コンプライアンス ダッシュボードで PCI-DSS v3.2.1:2018 コントロールを追跡します。	既定
ISO 27001	推奨されたポリシーと評価のセットに基づいて、コンプライアンス ダッシュボードで ISO 27001:2013 コントロールを追跡します。	既定
SOC TSP	推奨されたポリシーと評価のセットに基づいて、コンプライアンス ダッシュボードで SOC TSP コントロールを追跡します。	既定

標準をさらに追加

無効化

有効化

有効化

有効化

カスタム イニシアティブ

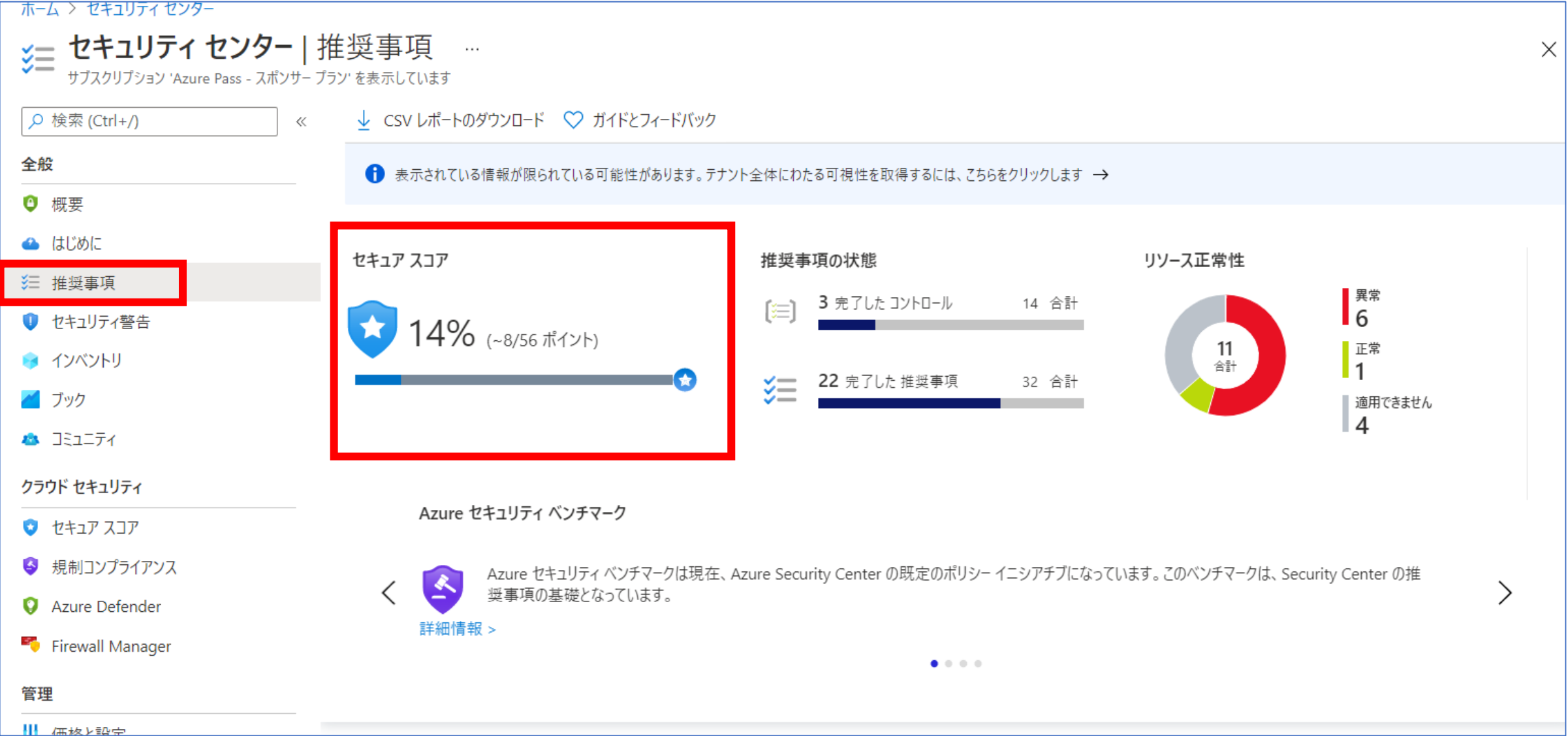
カスタムのイニシアティブも定義・有効化できる。

「Azure Security Benchmark」、
「PCI DSS」、
「ISO 27001」、
「SOC TSP」などのポリシーを
オプションで有効化することもできる。

推奨事項

推奨事項に従うことで、ワークロードをセキュリティで保護できます。

推奨事項の「セキュアスコア」で、現在のセキュリティの状況をすばやく確認できる



※下にスクロールしてください

推奨事項の一覧が、「セキユアスコア」の上昇の可能性が高い順に表示される

推奨設定の検索

コントロールの状態：2 件選択済み

推奨事項の状態：2 件選択済み

フィルターのリセット

コントロールでグループ化:
オン

最高スコアで...

推奨事項の成熟度：すべて

重要度：すべて

リソースの種類：すべて

応答アクション：すべて

適用除外を含む：すべて

環境：すべて

制御	最大スコア	現在のスコア	スコア上昇の可能性	正常でないリソース	リソース正常性	操作
▼ MFA を有効にす	10	0	+ 18% (10 ポイント)	1 個中 1 個のリソース		
ご..				🔑 1 個中 1 個のサ...		
ご..				🔑 なし		
> 管理ポートをセキ	8	0	+ 14% (8 ポイント)	2 個中 2 個のリソース		
> システムの更新フ	6	0	+ 11% (6 ポイント)	2 個中 2 個のリソース		
> 脆弱性を修復す	6	0	+ 11% (6 ポイント)	2 個中 2 個のリソース		
> セキュリティ構成	4	0	+ 7% (4 ポイント)	2 個中 2 個のリソース		
> 承認されていない	4	0	+ 7% (4 ポイント)	2 個中 2 個のリソース		
> 保存時の暗号化	4	0	+ 7% (4 ポイント)	2 個中 1 個のリソース		
> アクセスとアクセ	4	4	+ 0% (0 ポイント)	なし		
> 転送中のデータを	4	4	+ 0% (0 ポイント)	なし		
> 適応型アプリケー	3	0	+ 5% (3 ポイント)	2 個中 2 個のリソース		
> Endpoint Protec	2	0	+ 4% (2 ポイント)	2 個中 2 個のリソース		
> 監査とログを有効	1	0	+ 2% (1 ポイント)	3 個中 3 個のリソース		
> Azure Defende	スコアなし	スコアなし	+ 0% (0 ポイント)	なし		
> セキュリティのペ	スコアなし	スコアなし	+ 0% (0 ポイント)	6 個中 1 個のリソース		

推奨事項をクリックすると、説明、修復手順、影響を受けるリソースが表示される。

ホーム > セキュリティセンター >

ご利用のサブスクリプションに対して所有者アクセス許可があるアカウントでは、MFA を有効にする必要があります



適用除外 ポリシー定義の表示 クエリを開く

説明

アカウントまたはリソースの侵害を防止するため、所有者アクセス許可を持つすべてのサブスクリプション アカウントで多要素認証 (MFA) を有効にする必要があります。

修復の手順

手動修復:

条件付きアクセスを使用した MFA を有効にするには、Azure AD Premium ライセンスと、AD テナント管理者のアクセス許可が必要です。

- 関連するサブスクリプションを選択するか、使用可能な場合は [アクションの実行] をクリックします。MFA を使用していないユーザー アカウントの一覧が表示されます。
- [続行] をクリックします。[Azure AD 条件付きアクセス] ページが表示されます。
- [条件付きアクセス] ページで、ユーザーの一覧をポリシーに追加します (ポリシーが存在しない場合は作成します)。
- ご使用の条件付きアクセス ポリシーについて、以下を確認します。
 - [アクセス制御] セクションで、多要素認証が許可されている。
 - [クラウド アプリまたは操作] セクションの [対象] タブで、Microsoft Azure の管理 (アプリ ID: 797f4846-ba00-4fd7-ba43-dac1f8f63013) または [すべてのアプリ] が選択されていることを確認する。[対象外] タブで、これが除外されていないことを確認する。

Azure Active Directory で MFA セキュリティの既定値群 (Azure AD Free に含まれる) を有効にするには、次の手順を実行します。

- セキュリティ管理者、条件付きアクセス管理者、グローバル管理者のいずれかとしてサインインし、[Azure AD] の [プロパティ] ページに移動します。
- ページ下部の [セキュリティの既定値群の管理] を選択します。
- [セキュリティの既定値群の有効化] を [はい] に設定します。
- [保存] を選択します。

注意: 変更が Security Center に反映されるまで最大 12 時間かかる場合があります。

影響を受けるリソース

異常なリソース (1) 正常なリソース (0) 適用できないリソース (0)

サブスクリプション を検索

<input type="checkbox"/> 名前	↑↓ サブスクリプション	リソース グループ	理由
<input type="checkbox"/> 1f28afed-09e4-4089-98f0-b217bf3940dd	Azure Pass - スポンサー プラン		Azure AD Conditional Access isn't con

セキュリティ警告（アラート）

ワークロードを継続的に分析し、クラウドリソースでの潜在的な悪意のあるアクティビティに関するアラートを受け取ることができます。

セキュリティ警告（アラート）とは？

- リソースでの潜在的な悪意のあるアクティビティに関するアラートを受け取ることができます。
- すべてのセキュリティ アラートを統合された 1 つのビューで確認できます。
- セキュリティ アラートは、検出されたアクティビティの重要度に基づいて優先度が付けられます。重要度が高いアラートから先に対応します。
- サンプルのアラートを生成して、機能を検証することができます。

セキュリティセンターの「セキュリティ警告」

[ホーム](#) > [セキュリティセンター](#)

**セキュリティセンター | セキュリティ警告** ...

サブスクリプション 'Azure Pass - スポンサー プラン' を表示しています

[最新の情報に更新](#) | [状態の変更](#) | [クエリを開く](#) | [抑制ルール](#) | [セキュリティ アラートのマップ](#) | **[サンプルのアラート](#)** | [CSV レポートのダウンロード](#) | ...

全般

[概要](#)

[はじめに](#)

[推奨事項](#)

[セキュリティ警告](#)

[インベントリ](#)

[ブック](#)

[コミュニティ](#)

クラウド セキュリティ

[セキュア スコア](#)

[規制コンプライアンス](#)

[Azure Defender](#)

[Firewall Manager](#)

管理

[価格と設定](#)

[セキュリティ ポリシー](#)

[セキュリティ ソリューション](#)

[ワークフローの自動化](#)

[カバレッジ](#)

[クラウド コネクタ](#)

 新しいセキュリティ アラート ページに関するご意見をお聞かせください。こちらをクリックしてフィードバックをお送りください →

**0**
アクティブなアラート

**0**
影響を受けたリソース

[サブスクリプション == すべて](#) | [状態 == アクティブ](#) × | [重要度 == 低, 中, 高](#) × | [フィルターを追加](#)

グループ化なし

重要度 ↑↓

アラート タイトル ↑↓

影響を受けるリソース ↑↓

アクティビティの開始時刻 (UTC+9) ↑↓

MITRE ATT&CK® 戦術

状態 ↑↓



アラートが見つかりません

サンプル アラートの作成 (プレビュー)



様々な Azure Defender プランからサンプル アラートを作成して、Azure Defender アラートをお試しください。
[詳細情報 >>](#)

サブスクリプション

Azure Pass - スポンサー プラン




Azure Defender プラン

6 項目が選択されました




サンプル アラートの作成

サンプルのアラートが生成されました。

 27

アクティブなアラート

 7

影響を受けたリソース

アクティブなアラート (重要度別)

■ 高 (11) ■ 中 (14) ■ 低 (2)

ID、タイトル、影響を受けるリソースで検索し...


























サブスクリプション == すべて

状態 == アクティブ ×

重要度 == 低, 中, 高 ×

+ フィルターの追加

グループ化なし

<input type="checkbox"/>	重要度 ↑↓	アラート タイトル ↑↓	影響を受けるリソース ↑↓	アクティビティの開始時刻 (UTC... ↑↓	MITRE ATT&CK® ...	状態 ↑↓
<input type="checkbox"/>	高	 Suspicio... サンプル アラート	 Sample-App	21/05/20 午後11:36		アクティブ
<input type="checkbox"/>	高	 Phishing ... サンプル アラート	 Sample-App	21/05/20 午後11:36	 コレクション	アクティブ
<input type="checkbox"/>	高	 Attempte... サンプル アラート	 Sample-DB	21/05/20 午後11:35	 攻撃前	アクティブ
<input type="checkbox"/>	高	 Potential ... サンプル アラート	 Sample-DB	21/05/20 午後11:35		アクティブ
<input type="checkbox"/>	高	 Unusual ... サンプル アラート	 Sample-DB	21/05/20 午後11:35	 流出	アクティブ
<input type="checkbox"/>	高	 Access fr... サンプル アラート	 Sample-Storage	21/05/20 午後11:35	 攻撃前	アクティブ
<input type="checkbox"/>	高	 Unusual ... サンプル アラート	 Sample-Storage	21/05/20 午後11:35	 流出	アクティブ
<input type="checkbox"/>	高	 Digital cu... サンプル アラート	 Sample-VM	21/05/20 午後11:35	 実行	アクティブ
<input type="checkbox"/>	中	 Suspicio... サンプル アラート	 Sample-App	21/05/20 午後11:36	 コレクション	アクティブ

< 前へ

ページ 1 / 1


次へ >

サンプルのアラートの例

ホーム > セキュリティセンター >

セキュリティ アラート ☆ ...

2517807794372709520_61472cc6-bfcf-43ff-943a-58f87e9b7d50

 Suspicious WordPress theme invocation detected サンプル アラート

高
重要度


⚙️ アクティブ
状態


🕒 21/05/20 ...
アクティビティの時刻

アラートの説明

THIS IS A SAMPLE ALERT: The Azure App Service activity log indicates a possible code injection activity on your App Service resource. The suspicious activity detected resembles that of a manipulation of WordPress theme to support server side execution of code, followed by a direct web request to invoke the manipulated theme file. This type of activity was seen in the past as part of an attack campaign over WordPress.

影響を受けるリソース

 Sample-App
Web アプリケーション IaaS

 Azure Pass - スポンサー プラン
サブスクリプション


✓ お役に立ちましたか? ☐ Yes ☐ No ✕

アラートの詳細 アクションの実行

Sample Source IP Addresses
00.00.00.00

Sample URIs
/login.php


Sample User Agents
Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:48...
[さらに表示](#)

検出元
 Microsoft

Last Event Time
12/11/2019 12:34:27 AM

Sample Referer
-

関連エンティティ

▼  ホスト (1)

Next: Take Action >>

アラートに対するアクションの実行例（対応方法の表示）

アラートの詳細 アクションの実行


^  脅威の軽減

1. If WordPress is installed, make sure that the application is up to date and automatic updates are enabled.
2. If only specific IP addresses should be allowed to access the web app, set IP restrictions (<https://docs.microsoft.com/azure/app-service/app-service-ip-restrictions>) for it.

影響を受けるリソースについて、さらに 3 個のアラートがあります。 [すべて表示 >>](#)

^  将来の攻撃の防止

Solving security recommendations can prevent future attacks by reducing attack surface.

v  自動応答のトリガー

v  類似のアラートを抑制

セキュリティ警告（アラート）の「MITRE ATT&CK 戦術」列：アラートの状況を理解するのに役立つ

<input type="checkbox"/> 重要度 ↑↓	アラート タイトル ↑↓	影響を受けるリソース ↑↓	アクティビティの開始時刻 (... ↑↓	MITRE ATT&CK...	状態 ↑↓
<input type="checkbox"/> 高	 Phis... サンプル アラート	 Sample-App	21/05/20 午後11:36	 コレクション	アクティブ
<input type="checkbox"/> 高	 Atte... サンプル アラート	 Sample-DB	21/05/20 午後11:35	 攻撃前	アクティブ
<input type="checkbox"/> 高	 Pote... サンプル アラート	 Sample-DB	21/05/20 午後11:35		アクティブ
<input type="checkbox"/> 高	 Unu... サンプル アラート	 Sample-DB	21/05/20 午後11:35	 流出	アクティブ
<input type="checkbox"/> 高	 Acce... サンプル アラート	 Sample-Storage	21/05/20 午後11:35	 攻撃前	アクティブ
<input type="checkbox"/> 高	 Unu... サンプル アラート	 Sample-Storage	21/05/20 午後11:35	 流出	アクティブ
<input type="checkbox"/> 高	 Digit... サンプル アラート	 Sample-VM	21/05/20 午後11:35	 実行	アクティブ

MITRE（マイター）とは？

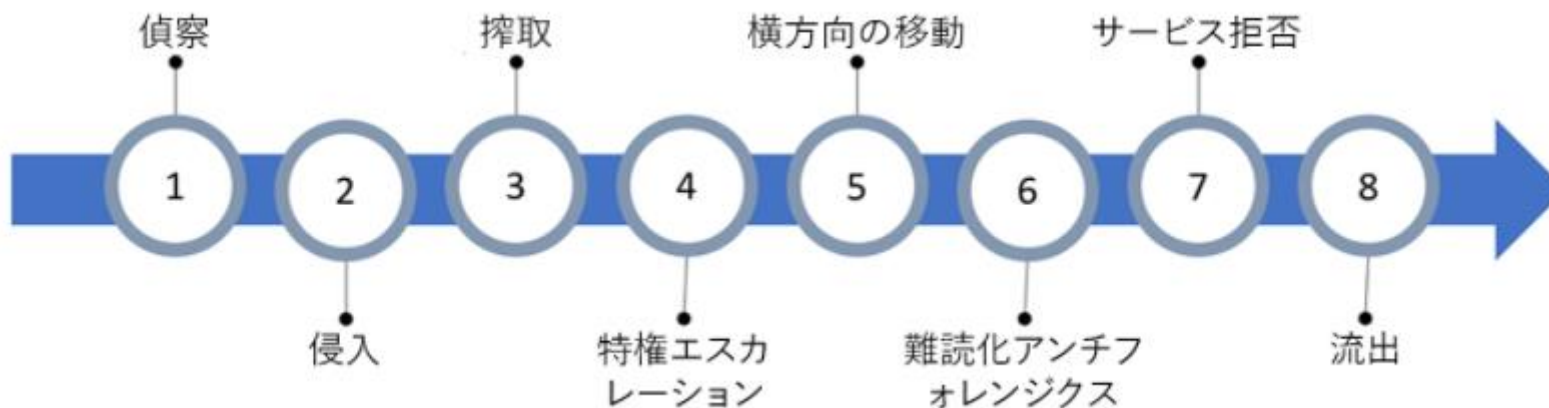
- MITREは、米国の連邦政府が資金を提供する非営利組織であり、R&Dセンターと官民のパートナーシップを通じて、国の安全性、安定性、福祉に関する事項に取り組んでいる。
- MITREは連邦政府、州政府、地方自治体だけではなく、産業界や学界の公共の利益のために活動している。
- 対象分野は、人工知能、直感的なデータサイエンス、量子情報科学、医療情報学、宇宙安全保障、政策と経済、信頼できる自律性、サイバー脅威の共有、サイバー回復力などであり、さまざまな分野で革新的なアイデアを生み出している。

MITRE ATT&CK（マイターアタック）とは？

- ATT&CKはAdversarial Tactics, Techniques, and Common Knowledgeの略で、直訳すると「敵対的な戦術とテクニック、共通知識」となる。
- ATT&CKはCVEをもとに、脆弱性を悪用した実際の攻撃を**戦術**と技術または手法の観点で分類したナレッジベースである。
- この**戦術**とは、初期侵入、悪意あるプログラムの実行、永続性、特権昇格、防御回避、認証情報アクセス、探索、水平展開、情報収集、C&C、情報送信、影響(Impact)に分類されている。
- そして、戦術ごとの個別の攻撃の技術・手法に対して、実際の実例、緩和策、検知方法、セキュリティベンダーやホワイต์ハッカーのレポートのリンクなどが記載されている。
- つまり、**サイバー攻撃の流れと手法を体系化したフレームワーク**とすることができる。
- ATT&CKは不定期もしくは4半期に一度、最新の脅威情報の追加が行われ、**多くのセキュリティ製品が戦術と攻撃手法の参照情報としてATT&CKが利用されている。**

セキュリティアラートでの MITRE ATT&CK戦術の活用

- それぞれのセキュリティアラートには、その攻撃の段階を表す、MITRE ATT&CK戦術 (tactic) が分析され、表示される。
- セキュリティ管理者は、この列の表示を見て、アラートがどのような段階なのか（攻撃者がどの段階の攻撃を行っているのか）を知ることができる。



ワークフローの自動化

ワークフローの自動化で「追加」をクリック

[ホーム](#) > [セキュリティセンター](#)



セキュリティセンター | ワークフローの自動化 ...

サブスクリプション 'Azure Pass - スポンサー プラン' を表示しています

<<

[+ ワークフロー-自動化の追加](#)

[最新の情報に更新](#)

[有効化](#)

[無効化](#)

[削除](#)

[?](#)

全般

[概要](#)

[はじめに](#)

[推奨事項](#)

[セキュリティ警告](#)

[インベントリ](#)

[ブック](#)

[コミュニティ](#)

クラウド セキュリティ

[セキュア スコア](#)

[規制コンプライアンス](#)

[Azure Defender](#)

[Firewall Manager](#)

管理

[価格と設定](#)

[セキュリティ ポリシー](#)

[セキュリティ ソリューション](#)

[ワークフローの自動化](#)

[ガバレッジ](#)

[クラウド コネクタ](#)

[選択さ... 有...](#)

[ト. Security](#)

名前

↑↓

状態

↑↓

スコープ



test

有効

Azure Pass - スポ

ワークフローの自動化の追加

ワークフロー自動化の追加

×

全般

名前 *

test2

✓

説明

this is a test

サブスクリプション ⓘ

Azure Pass - スポンサー プラン

▼

リソース グループ * ⓘ

test

▼

トリガーするロジックアプリを指定

トリガー条件を指定

トリガーの条件 ⓘ

構成されたアクションを自動的にトリガーするトリガー条件を選択します。

Security Center のデータ型の選択 *

Security Center の推奨事項

▼

推奨事項の名前 *

すべての推奨事項が選択されています

▼

推奨事項の重要度 *

すべての重要度が選択されています

▼

推奨事項の状態 * ⓘ

選択されたすべての状態

▼

操作

トリガーされるロジック アプリを構成します。
既存のロジック アプリを選択するか、または [Logic Apps ページにアクセスします](#) 新しいものを作成するには

次のサブスクリプションからロジック アプリのインスタンスを表示します *

Azure Pass - スポンサー プラン

▼

ロジック アプリ名 ⓘ

ロジック アプリを選択します

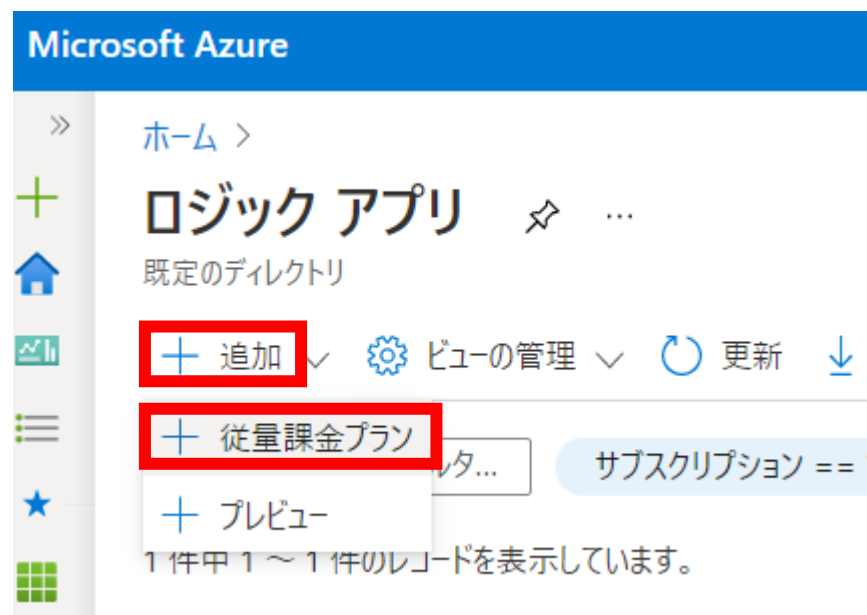
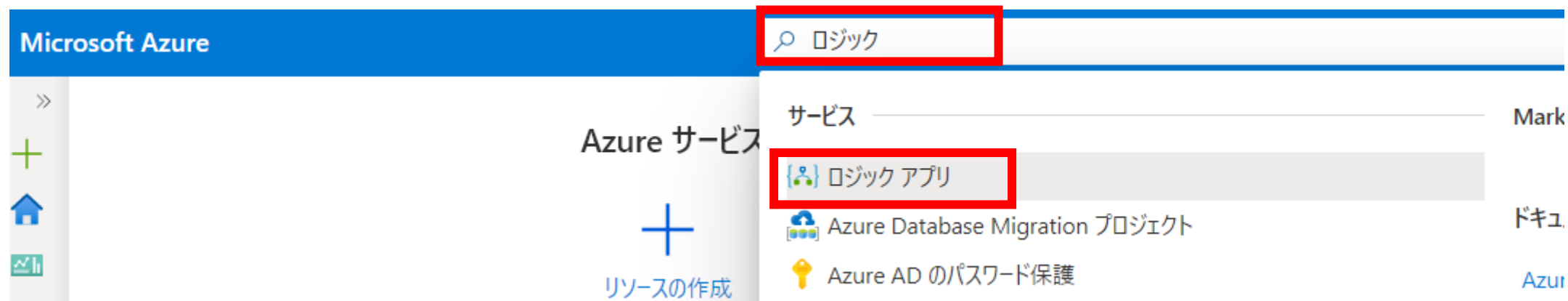
▼

[最新の情報に更新](#)

作成

キャンセル

ロジックアプリを作成



ロジックアプリを作成

ロジック アプリの作成 ...

基本 タグ 確認および作成

数百ものコネクタとビジュアル デザイナーを利用してワークフローを作成します。 [詳細情報](#) 

プロジェクトの詳細

デPLOYされているリソースとコストを管理するサブスクリプションを選択します。フォルダーのようなリソース グループを使用して、すべてのリソースを整理し、管理します。

サブスクリプション *

Azure Pass - スポンサー プラン

リソース グループ *

testrg

[新規作成](#)

インスタンスの詳細

ロジック アプリ名 *

test2

リージョン *

米国東部

統合サービス環境との関連付け ①

☐

統合サービス環境

ログ分析の有効化 ①

☐

Log Analytics ワークスペース

確認および作成

< 前へ : 基本

次: タグ >

[Automation のテンプレートをダウンロードする](#) ①

Logic Appデザイナーが表示されます

ホーム > Microsoft.EmptyWorkflow > test2 >

Logic Apps デザイナー ...

Introducing Azure Logic Apps

見る

後で見る

共有

統合ソリューションの構築がこれまで以上に簡単になりました

Logic Apps を利用することで、エンタープライズ統合の領域に速度とスケールビリティが加わります。使いやすいデザイナー、利用できる豊富なトリガーとアクション、強力な管理ツールにより、API の一元管理がこれまで以上に簡単になります。ビジネスのデジタル化が進む中、Logic Apps を利用すれば、従来型のシステムと最先端のシステムを結び付けることが可能です。

- ビジネス プロセスとワークフローを視覚的に作成する
- SaaS アプリケーションやエンタープライズ アプリケーションと統合する
- オンプレミス アプリケーションやクラウド アプリケーションから価値を引き出す

一般的なトリガーで開始する

最もよく使用するトリガーの 1 つを選択してから、コネクタの豊富なコレクションを使用して多くのアクションを調整します

メッセージが Service Bus キューで受信されたとき

HTTP 要求の受信時

新しいツイートが投稿されたら

Event Grid のリソース イベントが発生するとき

繰り返し

新しい電子メールが Outlook.com で受信されたとき

新しいファイルが OneDrive に作成されたとき

ファイルが FTP サーバーに追加されたとき

テンプレート

ロジック アプリを作成するには、下にあるテンプレートを選択します。

カテゴリ:

すべて

並べ替え:

人気

空のロジック アプリ

HTTP 要求と応答

ピークロックで Service Bus メッセージを受信して完了する

AS2 を介して X12 EDI ドキュメントを受信して XML に変換する

Logic Appデザイナーのテンプレートで、カテゴリ「セキュリティ」を選ぶと、セキュリティセンターと連携するアプリのテンプレートが表示されます。

テンプレート

ロジック アプリを作成するには、下にあるテンプレートを選択します。

カテゴリ:

セキュリティ

並べ替え:

人気

空のロジック アプリ



Get a notification email when Security Center creates a recommendation



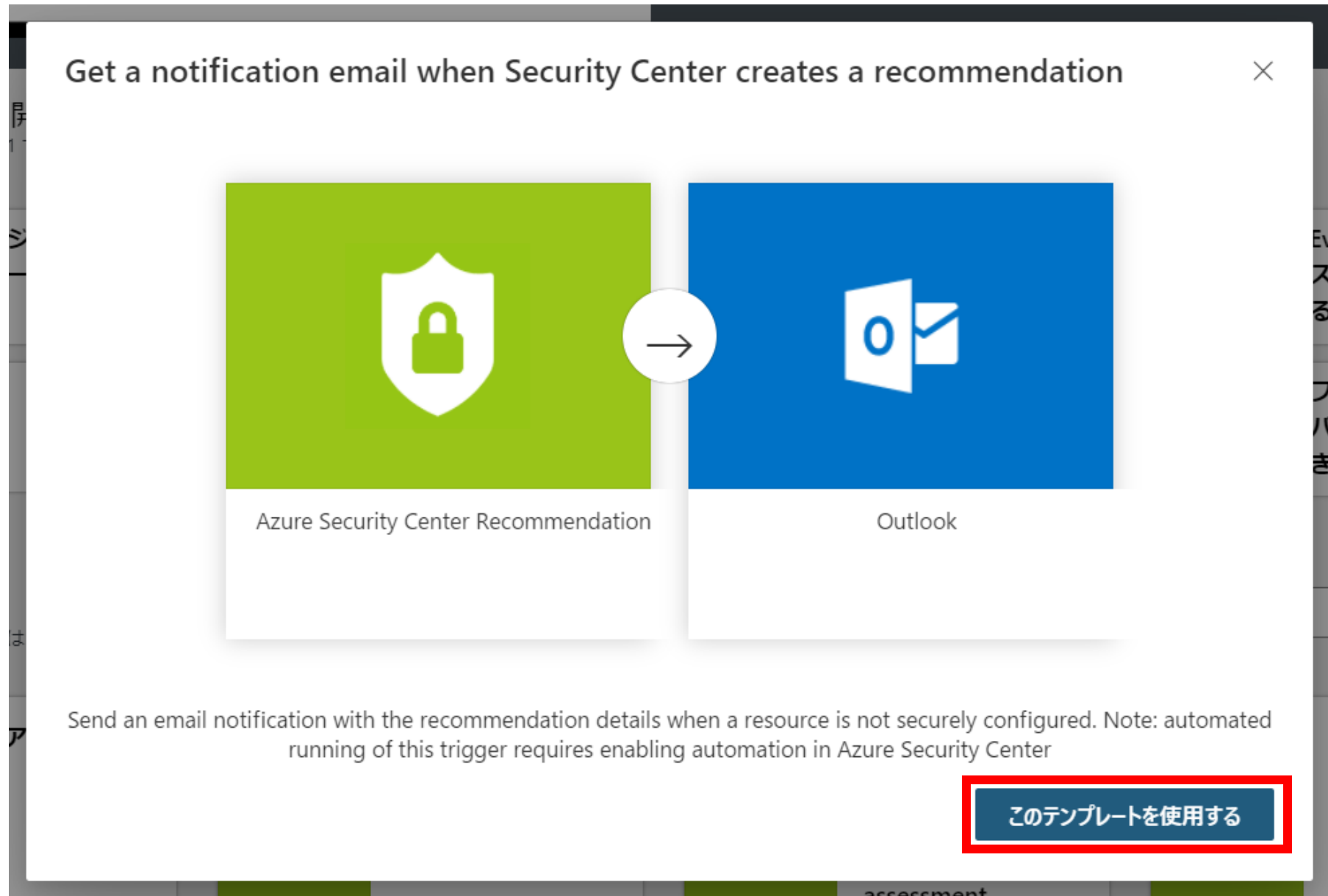
Get a notification email when Security Center creates a regulatory compliance assessment (Preview)



Get a notification email when Security Center detects a threat



「セキュリティセンターで推奨事項が作成されたらOutlookでメールを送信する」というテンプレートが利用できます。このテンプレートの場合、次の画面でMicrosoft 365のアカウントを選択する必要があります。



今回は Microsoft 365 の Outlook ではなく Outlook.jp を使用したいので、テンプレートを使わずに、「空のロジックアプリ」から作成します。

テンプレート

ロジック アプリを作成するには、下にあるテンプレートを選択します。

カテゴリ:

セキュリティ

並べ替え:

人気

空のロジック アプリ



Get a notification email when Security Center creates a recommendation



Get a notification email when Security Center creates a regulatory compliance assessment (Preview)



Get a notification email when Security Center detects a threat



Logic Appデザイナーが表示されます。まずトリガーを選択します。

ホーム > Microsoft.EmptyWorkflow > test2 >

Logic Apps デザイナー ...

保存 破棄 実行 デザイナー コードビュー パラメーター テンプレート コネクタ ヘルプ 情報

security center で検索

security center

おすすめ

すべて

ビルトイン

標準

エンタープライズ

カスタム

要求

Security Center Alert

Security Center...

Security Center...

トリガー

アクション

When an Azure Security Center Alert is created or triggered

Security Center Alert

When an Azure Security Center Recommendation is created or triggered

Security Center Recommendation

When a Security Center Regulatory Compliance Assessment is created or triggered (プレビュー)

Security Center Regulatory Compliance

Azure Security Center アラートが手動でトリガーされた場合 (古い - 説明を参照)

要求

When an Azure Security Center Recommendation is created or triggered

必要な情報が表示されませんか?
次に追加するコネクタやトリガーについて、要望をお寄せください [UserVoice](#)



When an Azure Security Center Recommendation is created or triggered



この手順では、追加情報が必要ありません。後続の手順で出力を使用できるようになります。

Security Center Recommendation に接続しました。 [接続を変更してください。](#)

ステップを追加

+ 新しいステップ



When an Azure Security Center Recommendation is created or triggered



操作を選択してください

🔍 outlook

おすすめ すべて ビルトイン 標準 エンタープライズ カスタム

Office 365 Outlook

Outlook タスク

Outlook.com

Public 360

▼

トリガー	アクション
	Outlook.com
	メールの移動 Outlook.com
	メールの削除 Outlook.com
	メールの取得 Outlook.com
	メールの取得 (V2) Outlook.com
	メールの送信 (V2) Outlook.com
	メールの転送 Outlook.com

outlook で検索

「メールの送信」
を選択

When an Azure Security Center Recommendation is created or triggered

メールの送信 (V2) 2

*宛先
someone@contoso.com のようなメール アドレスをセミコロンで区切って指

*件名
メールの件名を指定します

*本文
フォント 12 B I U 動的なコンテンツの追加

メールの本文を指定します

Add new parameter

Outlook.com に接続しました。接続を変更してください。

宛先メールアドレス、件名、本文
などを入力。

件名、本文などに、セキュリティ
センターで生成された推奨事項の
データを挿入できます。

このフローで使用されるアプリやコネクタから動的 非表示
なコンテンツを追加します。

動的なコンテンツ 式

動的なコンテンツの検索

When an Azure Security Center Recomm... 表示を減らす

- 本文
- Properties Resource Details
Details to identify the resource on which the recommen...
- Properties Status
The recommendation health status (indicating whether t...
- Properties Additional Data
Additional data that changes from one recommendation...
- Properties Metadata
Recommendation metadata (description, type, etc.).
- Properties Links
Contains multiple associated links that can be used to fu...
- Properties
The recommendation details and metadata.
- Type

Logic Appデザイナーで、作成したアプリを保存します。

[ホーム](#) > [Microsoft.EmptyWorkflow](#) > [test2](#) >

Logic Apps デザイナー ...

 保存  破棄  実行  デザイナー  コードビュー  パラメータ

セキュリティセンターの推奨事項がOutlookに送信されてきます！

The screenshot shows the Outlook interface. The left sidebar lists folders like 'お気に入り' (Favorites), '受信トレイ' (Inbox) with 33 items, '送信済みアイテム' (Sent Items), '下書き' (Drafts), and 'フォルダー' (Folders). The main pane shows the '受信トレイ' (Inbox) with a list of emails. The selected email is from 'test2021-0518@outlook.jp' with the subject '> test' and a timestamp of 21:15. The email body contains a JSON object with the following structure:

```
{
  "name": "83f577bd-a1b6-b7e1-0891-12ca19d1e6df",
  "properties": {
    "resourceDetails": {
      "source": "Azure",
      "id": "/subscriptions/1f28afed-09e4-4089-98f0-b217bf3940dd/resourceGroups/TEST2_GROUP/providers/Microsoft.Compute/virtualMachines/test2",
      "displayName": "Install endpoint protection solution on virtual machines",
      "status": {
        "code": "Unhealthy",
        "statusChangeDate": "2021-05-20T12:13:59.0038419Z",
        "firstEvaluationDate": "2021-05-20T12:13:59.0038419Z",
        "additionalData": {
          "os Type": "Windows",
          "reporting workspace customer id": "e4c6ca88-40f5-40d4-bb81-5c6b6076574f",
          "reporting workspace azure id": "/subscriptions/1f28afed-09e4-4089-98f0-b217bf3940dd/resourcegroups/defaultresourcegroup-eus/providers/microsoft.operationalinsights/workspaces/defaultworkspace-1f28afed-09e4-4089-98f0-b217bf3940dd-eus",
          "metadata": {
            "displayName": "Install endpoint protection solution on virtual machines",
            "assessmentType": "BuiltIn",
            "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/af6cd1bd-1635-48cb-bde7-5b15693900b9",
            "description": "Install an endpoint protection solution on your virtual machines, to protect them from threats and vulnerabilities.",
            "remediationDescription": "1. Select one or more virtual machines, or use the filter to set criteria for which machines to select. 2. Select Install on [x] VMs.",
            "categories": {}
          }
        }
      }
    }
  }
}
```

Install an endpoint protection solution on your virtual machines, to protect them from threats and vulnerabilities. (仮想マシンにエンドポイント保護ソリューションをインストールして、仮想マシンを脅威や脆弱性から保護します。)

参考：Logic Appで利用できる主な「コネクタ」。これらを使用して、各サービスと連携した自動化処理を行うことができます。

種類	コネクタの例
Azure のサービス	VM, App Service, Container Instance, Cosmos DB, DevOps, Blob, Files, Event Grid, Event Hub, Service Bus, Resource Manager, Automation, Communication Services SMS, IoT Central, Data Factory, Sentinel
Azureの AI系のサービス	Text Analytics, Computer Vision, Face API, LUIS, Content Moderator, QnA Maker, Bing Search, Video Indexer
Microsoftのサービス	Excel、Word、Outlook、OneDrive、OneNote、SharePoint、Teams、Project、Yammer、Power BI、Forms, Planner
ソーシャル	Twitter, Youtube, LinkedIn, Pinterest, RSS
業務システム	GitHub, Slack, SAP, ServiceNow, Zendesk, Adobe Creative Cloud, Amazon Web Services, SMTP
ファイル/データベース連携	SFTP, FTP, File System, Microsoft SQL Server、MySQL, PostgreSQL, Oracle Database, DB2

Azure Security Center (ASC) まとめ

- 有効化
 - 「セキュリティセンター」にアクセスするとASCは自動で有効化される。
 - 「Azure Defender」(ASCの追加機能)を有効化することでより高度な脅威保護を利用できる。有償。30日無料で試用可能。
 - 「Azure Defender」を有効にしない場合、無料で、推奨事項とセキュアスコアのみ利用できる。
 - 「Azure Defender」は複数の「Azure Defenderプラン」で構成され、個別にオン・オフできる。それぞれ別料金。
- アーキテクチャ
 - VM等には「データ収集エージェント」がインストールされ、VMのデータが収集される。
 - ストレージアカウントなどのAzureサービスからもデータが収集される。
 - データはLog Analyticsワークスペースに蓄積され、推奨事項やセキュリティアラートの生成に利用される。
 - セキュリティセンター有効化により「セキュリティポリシー」(実体はAzure Policyイニシアティブ)が設定され、推奨事項やセキュリティアラートの生成に利用される。
- 推奨事項
 - 正常でないと判断されたリソース設定とその修復手順が、推奨事項としてリストアップされる
 - 「セキュアスコア」で点数化される
- セキュリティアラート
 - 潜在的な悪意のあるアクティビティに対し「セキュリティアラート」が生成され、優先度順で表示される。
 - MITRE ATT&CK (マイターアタック) の「戦略」情報が付与され、攻撃の段階を知るのに役立つ。
 - アクション (対処方法) も表示される。
- ワークフローによる自動化
 - 推奨事項やセキュリティアラートに対応する「ワークフロー」(Logic Appsのロジックアプリ)を定義し、トリガーすることで、通知や対処を自動化することができる。