Microsoft Defender for Cloud
Microsoft Defender for servers
Microsoft Defender for Endpoint

Microsoft Defender for Cloudには
Microsoft Defender for serversが含まれる。
Microsoft Defender for serversには、
Microsoft Defender for Endpointが含まれる。

serversは小文字

Microsoft Defender for Cloud

CSPM
（クラウドセキュリティ態勢管理、「設定ミス」の発見）。無料。
元「Azure Security Center」

https://learn.microsoft.com/ja-jp/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1-2
https://learn.microsoft.com/ja-jp/azure/defender-for-cloud/defender-for-servers-introduction

Microsoft Defender for Cloud

強化されたセキュリティ機能(enhanced security features)

CSPM
（クラウドセキュリティ態勢管理、「設定ミス」の発見）。無料。
元「Azure Security Center」

CWPP
（クラウドワークロード保護プラットフォーム、VM等の保護）。有料。
CWP(クラウドワークロード保護)とも。
元「Azure Defender プラン」

https://learn.microsoft.com/ja-jp/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1-2
https://learn.microsoft.com/ja-jp/azure/defender-for-cloud/defender-for-servers-introduction

Microsoft Defender for Cloud

強化されたセキュリティ機能(enhanced security features)

Microsoft Defender for servers
（プラン1: $5/サーバー/月、プラン2: $15/サーバー/月）

オンプレ/クラウドの
Windows/Linux

Microsoft Defender for storage

Microsoft Defender for container

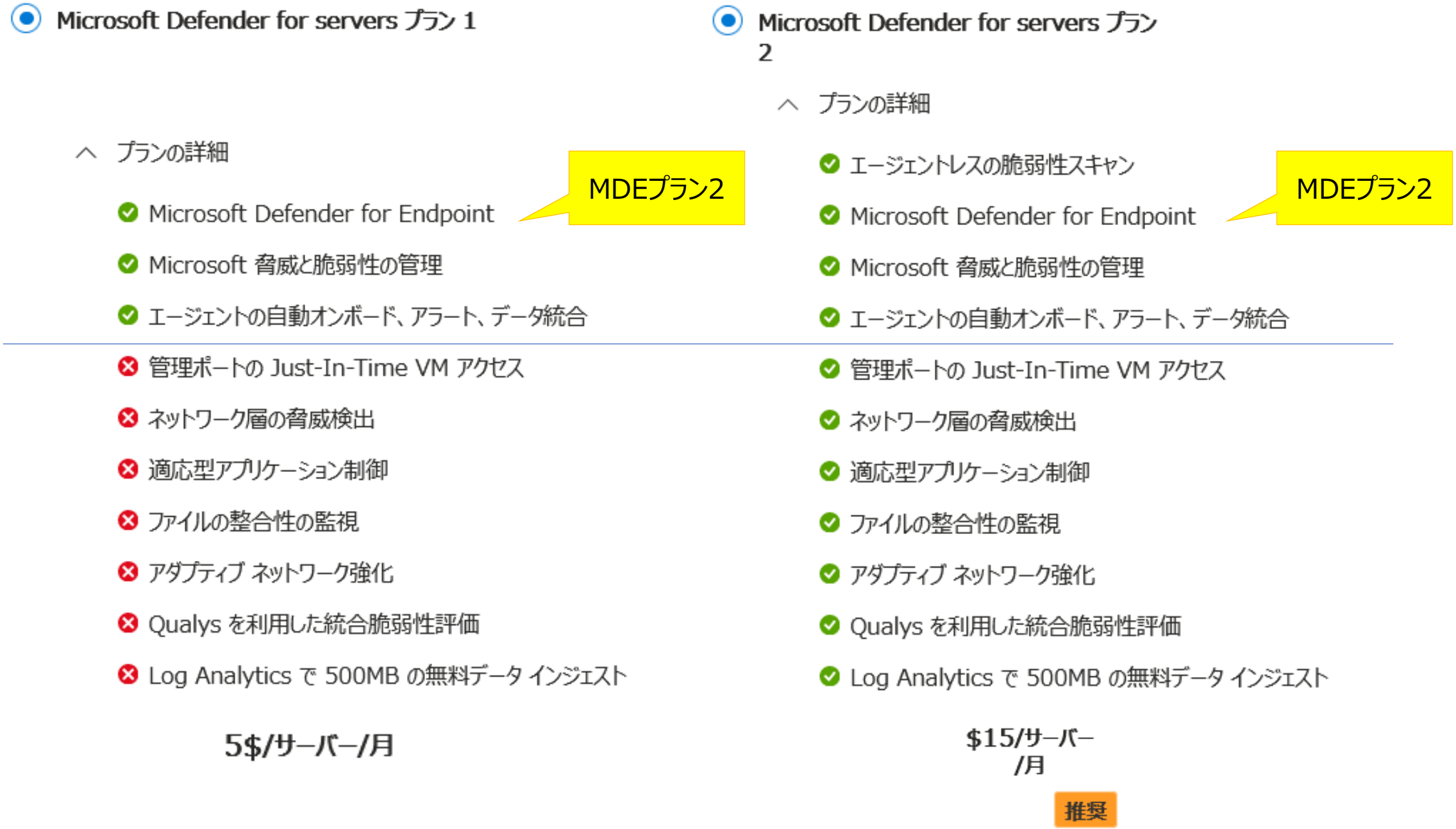
CSPM
（クラウドセキュリティ態勢管理、「設定ミス」の発見）。無料。
元「Azure Security Center」

CWPP
（クラウドワークロード保護プラットフォーム、VM等の保護）。有料。
CWP(クラウドワークロード保護)とも。
元「Azure Defender プラン」

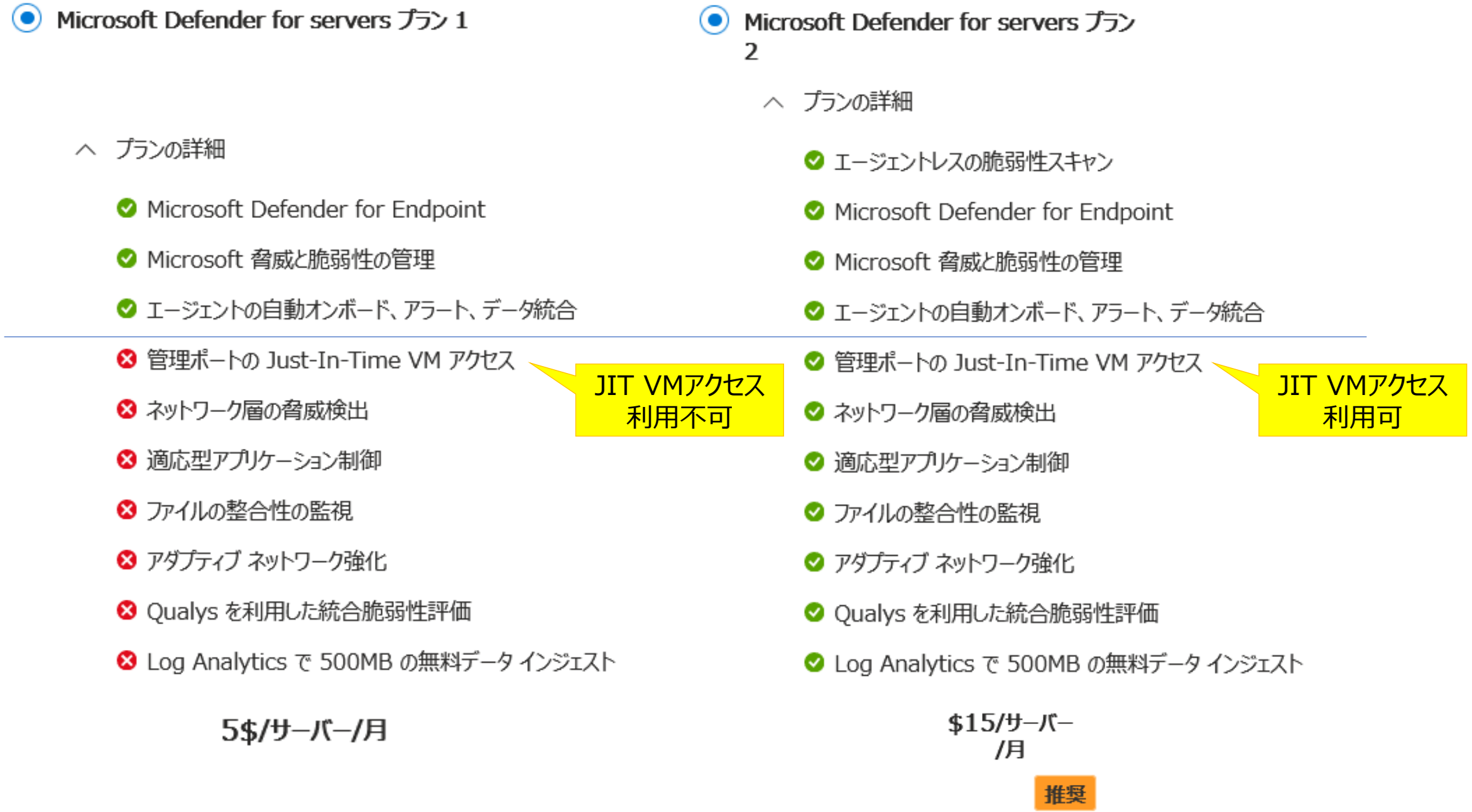
「強化されたセキュリティ機能」に含まれるプランの1つ。マルチクラウドとオンプレのWindows/Linuxマシンを保護。

https://learn.microsoft.com/ja-jp/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1-2
https://learn.microsoft.com/ja-jp/azure/defender-for-cloud/defender-for-servers-introduction

■Microsoft Defender for serversの「プラン1」と「プラン2」の違い



■Microsoft Defender for serversの「プラン1」と「プラン2」の違い



■Microsoft Defender for servers プラン2で使用できる「Just-In-Time (JIT) VMアクセス」とは？

Just-In-Time VM アクセスを有効にすることで、ポート22(SSH)・3389（RDP）・5985（WinRM）・5986（WinRM）ポートでの受信トラフィックをブロックできる。

※ポート番号はカスタマイズ可能

Defender for Cloud により、ネットワーク セキュリティ グループ (NSG) と Azure Firewall 規則で、選択したポートに対して "すべての受信トラフィックを拒否" 規則が存在することが保証される。これらの規則により、Azure VM の管理ポートへのアクセスが制限され、攻撃から保護される。

ユーザーが VM へのアクセス権を要求すると、Defender for Cloud によってそのユーザーが VM に対する Azure ロール ベースのアクセス制御 (Azure RBAC) アクセス許可を持っているかどうかがチェックされる。要求が承認されると、Defender for Cloud によって、関連する IP アドレス (または範囲) から選択したポートへの受信トラフィックを指定された時間だけ許可するように、NSG および Azure Firewall が構成される。

https://learn.microsoft.com/ja-jp/azure/defender-for-cloud/just-in-time-access-overview?wt.mc_id=defenderforcloud_inproduct_portal_recoremediation&tabs=defender-for-container-arch-aks

■Just-In-Time (JIT) VMアクセスでVMに接続するユーザーに必要なロールは？

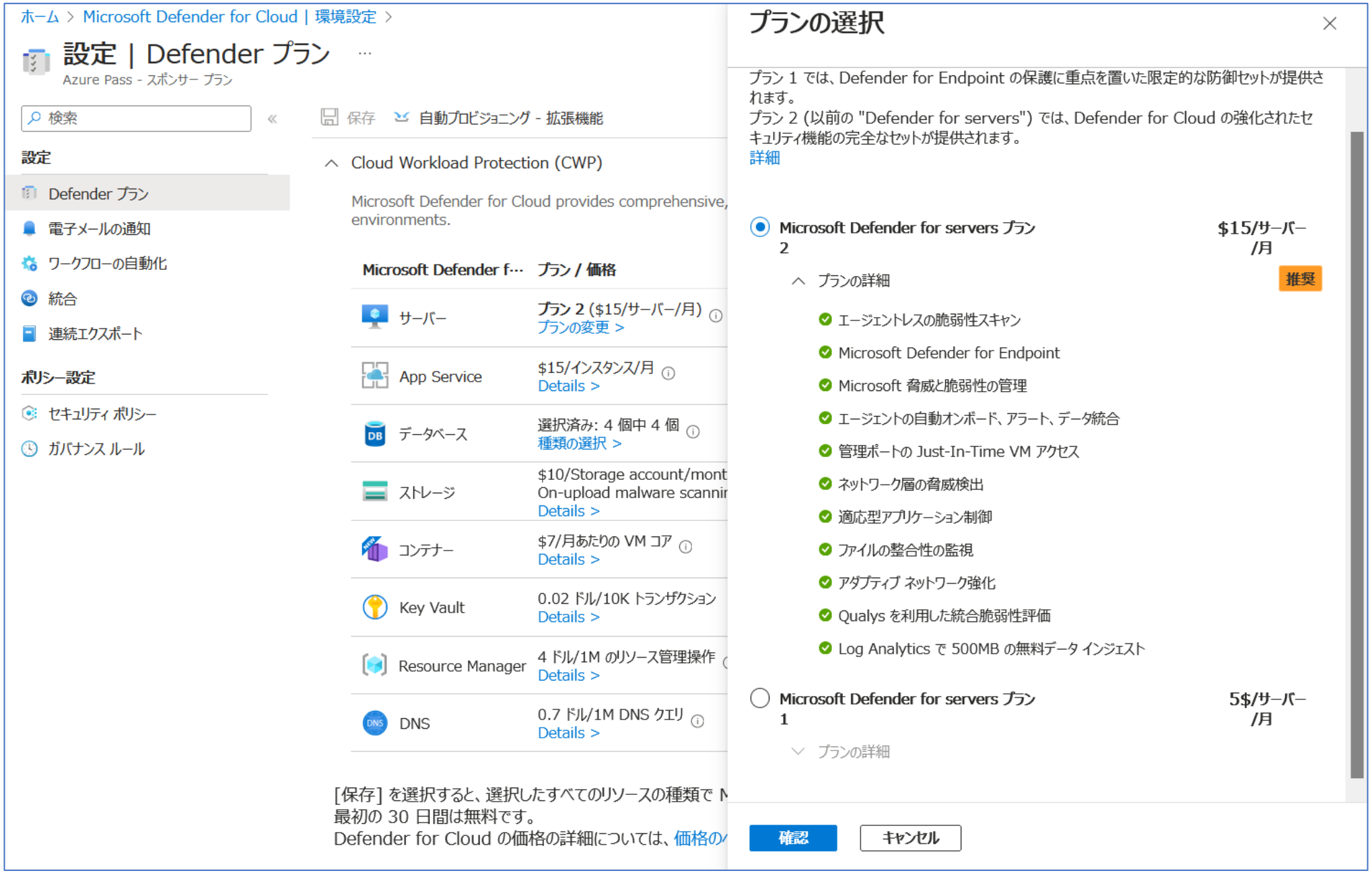
組み込みロールとしては存在しない。
カスタムロールを作成し、以下のアクションを含める。
そのカスタムロールをユーザーやグループに割り当てる。

VM への JIT アクセスを要求する　*これらのアクションをユーザーに割り当てます。*

- `Microsoft.Security/locations/jitNetworkAccessPolicies/initiate/action`
- `Microsoft.Security/locations/jitNetworkAccessPolicies/*/read`
- `Microsoft.Compute/virtualMachines/read`
- `Microsoft.Network/networkInterfaces/*/read`
- `Microsoft.Network/publicIPAddresses/read`

https://learn.microsoft.com/ja-jp/azure/defender-for-cloud/just-in-time-access-overview?tabs=defender-for-container-arch-aks

■プランの選択方法: Microsoft Defender for Cloudの「Defenderプラン」＞
サーバー（Microsoft Defender for Servers）＞プランの選択



Microsoft Defender for Cloud

強化されたセキュリティ機能(enhanced security features)

Microsoft Defender for Servers
（プラン1: $5/サーバー/月、プラン2: $15/サーバー/月）

オンプレ/クラウドの
Windows/Linux

Microsoft Defender
for Endpoint (MDE)
プラン 2

Microsoft Defender for ...

Microsoft Defender for ...

エンドポイント（PC、サーバー等）の保護。ウイルス対策、攻撃の検出等。
プラン2はプラン1の全機能を含む。

CSPM
（クラウドセキュリティ態勢管理、「設定ミス」の発見）。無料。
元「Azure Security Center」

CWPP
（クラウドワークロード保護プラットフォーム、VM等の保護）。有料。
CWP(クラウドワークロード保護)とも。
元「Azure Defender プラン」

「強化されたセキュリティ機能」に含まれるプランの1つ。マルチクラウドとオンプレのWindows/Linuxマシンを保護。

MDEの自動プロビジョニング。
プラン1は「MDEプラン2」を含む。
プラン2は、プラン1の全機能を含む。

https://learn.microsoft.com/ja-jp/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1-2
https://learn.microsoft.com/ja-jp/azure/defender-for-cloud/defender-for-servers-introduction

■Microsoft Defender for Endpointの「プラン1」と「プラン2」の違い

Defender for Endpoint プラン 1	- 次世代保護 (マルウェア対策とウイルス対策を含む) - 攻撃面の縮小 - 手動応答アクション - 一元管理 - セキュリティ レポート - Api - Windows 10、iOS、Android OS、macOS デバイスのサポート
Defender for Endpoint プラン 2	Defender for Endpoint プラン 1 のすべての機能に加えて、次の機能も含まれます: - デバイス検出 - デバイス インベントリ - コア Defender 脆弱性管理機能 - Threat Analytics - 自動調査および対応 - 高度なハンティング - エンドポイントの検出と応答 - エンドポイント攻撃通知 - Windows (クライアントのみ) と Windows 以外のプラットフォーム (macOS、iOS、Android、Linux) のサポート

プラン1は、
基本的なウイルス・マルウェア対策機能などを含む。

Microsoft Defender for serversでは、MDEプラン2がサーバーにプロビジョニングされる

脅威分析

脅威ハンティング

攻撃通知

プラン2では、プラン1のすべての機能に加え、脅威分析、脅威ハンティング（捜索）、攻撃通知などの高度な機能を利用できる。

https://learn.microsoft.com/ja-jp/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1-2?view=o365-worldwide

まとめ

■Microsoft Defender for Cloud

CSPM（クラウドセキュリティ態勢管理、「設定ミス」の発見）。無料。元「Azure Security Center」

■Microsoft Defender for Cloudの「強化されたセキュリティ機能」(enhanced security features)

CWPP（クラウドワークロード保護プラットフォーム、VM等の保護）。有料。
CWP（クラウドワークロード保護）とも。元「Azure Defender プラン」

■Microsoft Defender for servers

Microsoft Defender for Cloudの「強化されたセキュリティ機能」に含まれる有料プランの一つ。
オンプレミス/マルチクラウドのWindows/Linuxサーバーの保護機能。
プラン1: $5/サーバー/月、プラン2: $15/サーバー/月。
どちらのプランにも「MDEプラン2」が含まれる。

■Microsoft Defender for Endpoint (MDE)

エンドポイント（PC、サーバー等）の保護。ウイルス対策、攻撃の検出等。
「プラン1」と「プラン2」がある。
プラン1は、基本的なウイルス・マルウェア対策機能などを提供。
プラン2は、プラン1のすべての機能に加え、
脅威分析、脅威ハンティング（捜索）、攻撃通知などの高度な機能を提供。