

YOU DESERVE THE BEST SECURITY

HARMONY CONNECT ID プロバイダ連携 簡易設定ガイド ~ AZURE AD 編~

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社 システム・エンジニアリング本部

- ・本ドキュメントは、検証、ハンズオン研修等での利用を目的としているため、
 一部の設定手順のみを記載しています。
- ・本番環境の設定は、Administration Guide 等に基づいて行ってください。
- 本手順書と、Administration Guide、SK等の記述内容が異なる場合は、原則、
 本手順書以外のドキュメントの内容が優先されます。
- ・本手順書は、2022年1月現在の設定内容、UIに基づいて作成されています。



- ユーザの作成 [Azure AD 連携]
- ConnectApp のマニュアルインストール
- AzureAD での認証連携設定

ユーザの作成 [Azure AD 連携] (1/6)

	Check Point Infinity Portal x +	int.com/dashhoard/connect#/settings/identity-n	rov Ø	a a a	<-	 ×
		📄 🏦 cp japan s 🗸 🌒 Under Attack?		cpjdemo000	<u>د</u>	HECK PC
GETING STARED STARED ASSETS DECY POLICY	10プロバイダ オンプレミス管理 レポート&ログ	IDプロバイダが定義されていません。 (1) 「カイバイダが定義されていません。 今すぐ接続				
Ö						

IDプロバイダ				×
1 IDプロバイダの選択	IDプロバイダの選択	ł		
		Microsoft Active Directory Federation Services		
 ドメインの検証 		Microsoft Azure AD		
 ③ メタデータの設定 	L	okta	_	'
(人) 培結の許可		onelogin		
		Pingldentity		
」 5 IDプロバイダの確認		1 Generic SAML Provider		
			キャンセル	次へ

「SETTINGS > ID プロバイダ」を選択する
 「今すぐ接続」を押す

3. 「Microsoft Azure AD」を選択して、「次へ」 を押す

ユーザの作成 [Azure AD 連携] (2/6)



- 4. 登録するドメインを管理する DNS サーバの TXTレコードに表示されている値を設定する
 5. Azure AD のドメイン名を入力して、「+」を 押す
 - 「+」は隠れ気味の時があるので注意

6. ドメイン認証に成功したことを確認して、
 「次へ」を押す

ユーザの作成「Azure AD 連携」(3/6)

IDプロバイダ	×
IDプロバイダの選択	Azureボータルで、以下の値を使ってパラメータを設定してください:
	エンティティID cloudinfra-saml.checkpoint.com
✓ ドメインの検証	応答URL https://cloudinfra-gw.portal.checkpoint.com/api/saml/sso
 3 接続の許可 	ユーザ属性& ケーパー クレームタイプ 値
Azure AD $> I$	ンタープライズアプリケーション
> Check Po	int Harmony Connect(Azure AD)
> シングル	・サインオン > 基本的な SAML 構成
に、設定する	
IDプロバイダ	х
✓ IDプロバイダの選択	フェデレーションメタデータXMLファイル
	SAML IDプロバイダ サーバには通常、メタデータXML設定ファイルが含まれています。この設定ファイルは、サービス URLや証明書パブリック キーなどのシングル サインオン プロパティで構成されます。
- ドメインの検証	Azureボータルで証明書を作成し、フェデレーション メタデータ ファイルをダウンロードして、以下にアップ

- Check Point Harmony Connect (Azure AD).xml ✓ 接続の許可
- Azure AD > エンタープライズアプリケーション
 - > Check Point Harmony Connect(Azure AD)

> シングルサインオン > SAML 署名証明書

の「フェデレーションメタデータ XML」をアップロード

- 7. 応答 URL を、Azure AD へ設定して、「次 へ」を押す
 - Azure AD のギャラリーアプリケーション を使用する場合、エンティティ ID は設定 済みのため入力不要

8. Azure AD からダウンロードした、「フェデ レーション メタデータ XML」ファイルをアッ プロードして、「次へ」を押す

ユーザの作成 [Azure AD 連携] (4/6)

10.「次へ」を押す

IDプロバイダ			x
🥑 10プロバイダの選択	ユーザ&グループ問題		
✓ ドメインの検証	次の権限は、Harmon 選択するために必要で	y ConnectポリシーでAzure Active Dir す:	rectoryからのユーザ グループを
	API增限 API/推获名 Group.ReadAll User.ReadAll	內容 Read all groups Read all user names	管理者承担 Yes Yes
A 115-2087	Azureボータルから次 ・アプリケーション (ク	のパラメータを指定してください: ライアント) ID	
3 ディレクトリ統合の	・ディレクトリ (テナン	⊦) ID	
RE	・クライアントシークレ	ev h	
⑥ IDプロバイダの確認			

9. Azure AD から以下の3つの値をコピーして、 入力する

• アプリケーション ID

- アプリの登録 > Check Point Harmony Connect (Azure AD) の 概要ページ
- ・ ディレクトリ(テナント) ID
 - アプリの登録 > Check Point Harmony Connect (Azure AD) の 概要ページ
- クライアントシークレット
 - アプリの登録 > 証明書とシークレットで、新しいクライアントシークレットを作成し、クライアントシークレットの「値」をコピー

ユーザの作成 [Azure AD 連携] (5/6)

● IDプロバイダの選択 IDプロバイダ Azure ● ドメインの検証 フェデレーシ ョンメタデー Check Point Harmony Connect (Azure AD).xml タ ● 接続の許可 ドメイン smb-se.checkpoint.sc ● メタデータの設定 アブリケーシ ョン(クライ アント)ID ● ディレクトリ	ĺ
 ・ ドメインの独臣 アエデレーションメタデー Check Point Harmony Connect (Azure AD),xml タ 	
 ◆ 接続の許可 ドメイン smb-se.checkpoint.sc アプリケーシ => (クライ アント)ID モッレクトリ 	H
▼ メタデータの設定 アプリケーション(クライ アント)ID モメレクトリ	
ディレクトリ	l
ディレクトリ統合の (テナント)ID 設定	l
 クライアント Dプロバイダの確認 詳細は雪雅ガイドを参照してください 	1
夏る 10プロバイダの追加	a l
Check Point Infinity Portal x + Check Point Infinity Portal x + → C	
III- HARMONY CONNECT I apjapan smb se 🗸	ų
は Harmony Connectアプリ IDプロバイダ IDプロバイダ	I
Application Access Application Access Application Access Application Access	
ASERS オフラレミス管理 ドメイン ロボート&ログ smb-se.checkpoint.sc	
POLICY	
LOGS & EVENTS	

11.ID プロバイダの設定内容を確認して、「ID プ ロバイダの追加」を押す

12. Harmony Connect への ID プロバイダの追加 が完了

ユーザの作成 [Azure AD 連携] (6/6)

Scarch	米 New ▼
Groups (4)	Any Identified User
Any Identified User	
HamonyConnect	Client, or at a site (using identity awareness).
Sales-G	
System-G	
	使用場所: 未使用

13.ID プロバイダと Harmony Connect との間 で、ユーザとグループの同期が完了すると、 「POLICY > アクセスコントロール > イン ターネットアクセス」のオブジェクトに、 ID プロバイダの「ユーザ」と「グループ」

が自動追加される

• 「ユーザ、「グループ」の同期が可能な ID プロ

バイダは、Azure AD、Okta、PingID のみ

14.「ユーザ」と「グループ」は、Access

Control のルール作成時に「ソース(送信

元)」として指定可能

ConnetApp のマニュアルインストール(1/4)



- 1. 「ASSETS > ユーザ&デバイス」を選択する
- 2. 「アプリのダウンロード」を押す
- ファイルタイプを選択して「ダウンロード」
 を押してダウンロードする

4. インストールファイルをダブルクリックする

ConnetApp のマニュアルインストール(2/4)



認証ダイアログボックスが表示されるので、
 「ユーザ名(メールアドレス形式)」を入力し、「次へ」を押す

サインインを求められるので、「サインイン ブラウザを開く」を押す

ConnetApp のマニュアルインストール (3/4)

דאלא 🚼 🖿	トにサインイン × +		-	D	×
$\leftarrow \rightarrow c$	https://login.mi 🏠 📮	3 ₫	Ē		
	Microsoft				
	サインイン				
	alice@smb-se.checkpoint.sc		_		
	アカウントにアクセスできない場合				
		次へ			
			_		
	-				
	♀ サインイン オブション				
		利用規約	^プ ライバシー	と Cookie	
_					
-					
 דאסטען 	-159472472 x +		_	0	×
الاولىر	トビザインイン × 十 合 https://login.mi 公 旦	3 ₫	Ð -	•	×
ת וינמלית ∎ לאלילית באלי באלילילי	-にサインイン x + 合 https://login.mi 介。 💻	3 ↓ 5 [±]	- -	•	×
الرونير ∎ ← → C	トビサインイン × 十 合 https://login.mi 🏠 💻	3 ☆	- -	•	×
וענמלע ו ל< → C	・Cザインイン x + https://login.mi 介。 Microsoft	3 €	- -	•	×
الرونير ■ ← → C	-にサインイン × + ♪ https://login.mi ☆ ■ Microsoft ← alice@smb-se.checkpoint.sc	G ¢=	- -	•	×
الاכמד ■ דאסטע ← → C	・Cザインイン x + ① https://login.mi 公 I Microsoft ← alice@smb-se.checkpoint.sc パスワードの入力	3 ₽	- -	•	×
 ■ 70000 ← → C 	 トビサインイン × + https://login.mi ☆ ■ Microsoft ← alice@smb-se.checkpoint.sc バスワードの入力 がスワード 	G ¢=	- -	•	×
الادرير ■ ک ← → C	-にサイソイン x + ① https://login.mi 公 Q Microsoft ← alice@smb-se.checkpoint.sc パスワードの入力 パスワード パスワード	3 €	- -		×
תנימד וו ← → C	・とサインイン × + ♪ https://login.mi ☆ ■ Microsoft ← alice@smb-se.checkpoint.sc パスワードの入力 /(スワード パスワードを忘れた場合	3 ↓ f=	-	•	×
 ■ 770004 ← → C 	-にサイソイン x + ① https://login.mi 公 Q Microsoft ← alice@smb-se.checkpoint.sc パスワードの入力 パスワード パスワード	3 €	- @	•	×
 ■ # γτιστη ← ⇒ C 	・とサインイン × + ♪ https://login.mi ☆ ■ Microsoft ← alice@smb-se.checkpoint.sc パスワードの入力 /(スワード ノスワードを忘れた場合	3 €= 9	- -	•	×

YOU DESERVE THE BEST SECURITY

CHECK POINT

8. サインインページで「ユーザ名(メールアド レス形式)」を入力し、「次へ」を押す

9. 「パスワード」を入力し、「サインイン」を 押す

ConnetApp のマニュアルインストール (4/4)



10.サインインが完了すると、ConnectApp のイ ンストールが完了する

11.インストールが完了すると、自動的にHarmony Connect がトラフィックの保護を開 始する

Azure AD での認証連携設定(1/10)



- 1. 基本的には Microsoft が公開しているチュートリアルに沿っ て設定すればよいが、一部設定が不足している
 - チュートリアル: Azure Active Directory シングル サインオン (SSO) と Check Point Harmony Connect の統合
 - https://docs.microsoft.com/ja-jp/azure/active-directory/saasapps/check-point-harmony-connect-tutorial
- 2. Azure AD SSO の構成の流れ
 - I. エンタープライズアプリケーションの作成
 - II. SSO 方式の選択
 - III. SAML 構成の設定
 - Ⅳ. 属性とクレームの確認
 - V. フェデレーション メタデータ XMLのダウンロード
 - ∨Ⅰ. クライアントシークレットの作成
 - VII. APIのアクセス許可設定

S^C CHECK POINT[™] YOU DESERVE THE BEST SECURITY^{VIII}. ユーザ、グループの割り当て

Azure AD での認証連携設定(2/10) エンタープライズアプリケーション> すべてのアプリケーション (プレビュー)

 ■ エンタープライズ アプリケーション - Mic ← → C ● https://poor 	× +
≡ Microsoft Azure	/ース、サービス、ドキュメントの検索(G+/) 🛛 🖸
ホーム > CPJ > エンタープライズア	^{プリヶーション} アプリケーション すべてのアプリケーション
CPJ - Azure Active Directory	
概要	 ② 新しいエンタープライズ アプリ検索のプレビューをお試しください。クリック
★ 問題の診断と解決	Azure AD テナントを ID プロバイダーとして使用するように設定されている、こ
管理	理、検索します。詳細については、こちらをご覧ください。
 リハ このアフリリーション アプリケーション プロキシ 	アノリケーションの値頭 アフリケーションの状態 アフ エンタープライズ アプリ すべて す
🐼 ユーザー設定	

Check Point Harmony Connect (/ 🗙 +	- • ×
🗧 🔶 C 🗈 https://portal.azure.com/#blade/Microsoft_AAD_IAM/AppGa	llery8ladeV2 🖉 🕼 🚇 🖉 🕼 🚇 🖤
■ Microsoft Azure P リソース、サービス、ドキュメントの検索 (G+/)	R 🖗 🕸 🧟 🐺 🧕
*ーム、販売のディレクトリンエンタープライズアプリケーションン Azure AD ギャラリーの参照 …	Check Point Harmony Connect (Azure AD) \times
	👰 フィードバックがある場合
+ 独自のアプリケーションの作成 (1) 新しいギャラリーアプリを要求する A ² ?	ロゴ () 名前*()
飲良された新しいアプリギャラリーエクスペリエンスをご利用いただいています。従来の	Check Point Harmony Connect (Azure AD)
uure AD アプリ ギャラリーは、シングル サインオン (SSO) と自動ユーザー プロビジョニン ドプロイするときに、事前に構築されたチンプレートを活用して、ユーザーをより安全に7 Sい。	発行売 0 プロビジョング 0 Check Point 自動プロビジョングはサポート されていません
 	シングル サインオン モード 〇 URL 〇 SAML ペース の テインオン http://checkpoint.com/ リンタ きれた サインオン
RFOARROS S E RERCI L'UIST Connect (Azure AD) Connect (Azure AD) Const Dent 응	Check Point Harmony Connect (Azure AD) 現金の手順に関するチュー トリフット 読む Check Point Harmony Connect protects (Jochaly distributed branch office or vitual networks to Instremt GSU202) connections with advanced threat prevention and can automatically secure Azure assets.
Check Point Identity Awareness Chack Point Chack Point Chack Point Chack Point Chack Point	

3. エンタープライズアプリケーション画面で、「新しい

アプリケーション」をクリックする

- Azure AD ギャラリーで、「Check Point Harmony Connect」のキーワードで検索する
- 5. 「Check Point Harmony Connect (Azure AD)」を選択 する
- 6. 「作成」を押す

Azure AD での認証連携設定(3/10)

エンタープライズアプリケーション > Check Point Harmony Connect (Azure AD) > 概要

7. 「シングルサインオンの設定」をクリックする

← → C Ô https://porta	n L ' al.azure.com/?l=ja.ja-jp#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/ 8a 🎲 📮 🕃 🇯 🔂 🧟	
Microsoft Azure タリソ-	ース、サービス、ドキュメントの検索 (G+/) 🛛 💀 🖉 🛞 🕜 🔗	0
ホーム > CPJ > エンタープライズ アフ	プリケーション 〉 Azure AD ギャラリーの参照 〉	
Check Point Harmo	ony Connect (Azure AD) 概要 …	×
«		1
4 概要	プロパティ	
🛄 デプロイ計画	▲前 ①	
管理	Check Point Harmony Conn	
プロパティ	アプリケーション ID ①	
🔺 所有者	0	
。 ロールと管理者 (プレビュー)		
▶ ユーザーとグループ	Getting Started	
シングルサインオン		
⊅ プロビジョニング		
⊙ セルフサービス	 2。シングルサインオンの設定 1。ユーザーとグループの割り当て ジーボーが自分の Azura AD 資格停留を使 	
💁 カスタム セキュリティ属性 (プレ	特定のユーザーおよびグループにアプリ コーリーが自力の general 気 (目前) (Control (ローン) (ロー) (ロー) (ロー) (ロー) (ロー) (ロー) (ロー) (ロー	
ピュー)	シージョン にんこう きるようにする ユーザーとグループの割り当て たまっませい	
セキュリティ	TEREVORIA	
🎍 条件付きアクセス		
🖁 アクセス許可		

Check Point Harmony Connect (/		×					
$\leftarrow \rightarrow \mathbb{C} \textcircled{a} \texttt{https://portal.azure.com/?l=ja.ja-jp#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/S} \texttt{as} \textcircled{a} \end{array}{a} \textcircled{a} \end{array}{a} \textcircled{a} \textcircled{a} \textcircled{a} \textcircled{a} \end{array}{a} \textcircled{a} \textcircled{a} \textcircled{a} \end{array}{a} \end{array}{a} \textcircled{a} \textcircled{a} \end{array}{a} }a \end{array}{a} }a \end{array}{a} }a \\a \\a \\a \\a \\a \\a $							
😑 Microsoft Azure 🔎 リソー	ス、サービス、ドキュメントの検索(G+/) 🛛 🕞 🖓 🛞 🕐 🔗	0					
ホーム > CPJ > エンタープライズ アプ	リケーション > Azure AD ギャラリーの参照 > Check Point Harmony Connect (Azure AD)						
Check Point Harmo TVタープライズアプリケーション	ny Connect (Azure AD) シングル サインオン …	×					
×		1					
116	シングルサインオン (SSO) により、組織内のユーザーが、自分が使用しているすべてのアプリケーションに、1 つのアカウントで サインインできるようになるため、ユーザーが Azure Active Directory のアプリケーションにサインオンするときのセキュリティと	- 1					
山 デプロイ計画	利便性を向上します。一度ユーザーがアプリケーションにログインすると、その資格情報は、そのユーザーがアクセスする必要が	- 1					
管理	ある他のすべてのアプリケーションに使用されます。詳細については、こちらをご覧ください。	- 1					
プロパティ		- 1					
🎥 所有者	シングル サインオン方式の選択 判断に役立つヘルプの表示	- 1					
👃 ロールと管理者 (プレビュー)		- 1					
🎄 ユーザーとグループ	★Abb ★A	. 1					
∋ シングル サインオン	シングルサインオンが有効になってい SAML (Security Assertion Markup SAML (Security	- 1					
Φ プロビジョニング	ません。ユーザーは、[マイ アプリ]か Language) プロトコルを使用した、ア らアプリを起動できません。 プリケーションに対する多機能かつセ						
⊖ セルフサービス	キュリティで保護された認証。						
■ カスタム セキュリティ属性 (プレ ビュー)							

CHECK POINT

8. 「SAML」をクリックする

Azure AD での エンタープライズアプリケー Microsoft Azure アリイス、ナーマス、ドキュメントの検索 (G+) かーム > CP) > エンターブライズアプリケーション > Azure AD ギャラリーの参照 > Check Point Harmony Connect (Azure AD) SAML ペースのサインオ エンターブライズアプリケーション)認証連携設 ション > Check Point Harr 9.	定(4/10) nony Connect (Azure AD) > シングルサインオン 「基本的な SAML 構成」欄の「編集」をクリックする
基本的な SAML 構成 識別子 (エンティティ ID) 応答 URL (Assertion Consumer Service URL) サインオン URL リレー状態 ログアウト URL	 ✓ 編集 必須 必須 必須 省略可能 省略可能 	
C まやりに SAML 観点 - Microsof × +	- □ × ★ ⊕ ⊕ • ··· × 10.	「応答URL」、「サインオンURL」欄に、以下のURL を入力する • https://cloudinfra-

gw.portal.checkpoint.com/api/saml/sso

既定

1

① プロビジョニング

💿 カスタム セキュリティ属性 (フ

サインオン URL* 💿

https://cloudinfra-gw.portal.checkpoint.com/api/saml/sso

😔 セルフサービス

セキュリティ

👃 アクセス許可

🟮 トークンの暗号化

 https://portal.azure.com/?l=ja.ja-jp#blade/Microsoft.AA crosoft Azure タリソース、サービス、ドキュメントの検索(G+/) 	ND_IAM/ManagedAppMenuBlade/S 려あ 12급 🔛 13 12 11 🕀 🐷	
$P_{1} > \pm 2 = 2 = 2 = 2 = 2 = 2 = 2 = 2 = 2 = 2$	区 碌 ♀ ◎ ァ 短 > Check Point Harmony Connect (Azure AD) > ML ペースのサインオン …	「接続の許可」の画面の「ユーザ属性とクレー
ススアプリケーション 属性とクレーム		が同じであることを確認する
givenname	user.givenname	
surname	user.surname	
emailaddress	user.mail	
name	user.userprincipalname	
groups	user.groups	
一意のユーザー ID	user.userprincipalname	
	- 0	
C C C Attps://portal.azure.com/?l=jaja-jp#blade/Microsoft_AA Cocoft Anuco C UV_Z C C C C C C C C C C C C C C C C C C C	D_IAM/ManagedAppMenuBlade/S 88 රු 🗳 🔇 රූ 🛱	12 「SAMI 署名証明書」欄の「フェデレーション
heck Point Harmony Connet () X 十 C 合 https://portal.azure.com/?l=ja.ja-jp#blade/Microsoft_AA rosoft Azure タリソース、サービス、ドキュメントの検索(G+/)	DJAM/ManagedAppMenuBlade/S ab G 里 G ☆ ● ®	12. 「SAML 署名証明書」欄の「フェデレーション
neck Roint Harmony Connet U × 十 C 合 https://portal.azure.com/?l=ja.ja-jp#blade/Microsoft.AA rosoft Azure クリソース、サービス、ドキュメントの検索 (G+/) ML 著名証明書	D_IAM/ManagedAppMenuBlade/S 88 分 厘 ③ ☆ @	12. 「SAML 署名証明書」欄の「フェデレーション データ XML」をダウンロードし、Harmony Cor
hetek Point Harmony Connet () × 十 C 合 https://portal.azure.com/?l=ja.ja-jp#blade/Microsoft,AA rosoft Azure タリソース、サービス、ドキュメントの検索(G+/) ML著名証明書	DJAM/ManagedAppMenuBlade/5 ab fg 単 ③ f= fg ●	12. 「SAML 署名証明書」欄の「フェデレーション データ XML」をダウンロードし、Harmony Cor
heck Point Harmony Connet (* X 中 C 合 https://portal.azure.com/?l=ja.ja-jp#blade/Microsoft.AA rosoft Azure クリソース、サービス、ドキュメントの検索 (G+) ML 著名臣明書	D.JAM/ManagedAppMenuBlade/5 88 73 単 3 12 6 6 2 日 日 夕 ② ③ ⑦ 尺 アクティブ	12. 「SAML 署名証明書」欄の「フェデレーション データ XML」をダウンロードし、Harmony Cor の「メタデータの設定」の画面でアップロード
eee Point Harmony Connect () × + C ① https://portal.azure.com/?l=jaja-jp#blade/Microsoft.AA rosoft Azure アリソース、サービス、ドキュメントの技術 (G+/) ML書名証明書 C ② 前期限 2	ND_JAM/ManagedAppMenuBlade/S さあ 分 国 ③ 介 優 ● 区 日 学 ※ ③ ア アクティブ 024/11/17 11:04:41	12. 「SAML 署名証明書」欄の「フェデレーション データ XML」をダウンロードし、Harmony Co の「メタデータの設定」の画面でアップロード

Azure AD での認証連携設定(6/10)

アプリの登録 > Check Point Harmony Connect (Azure AD)

R定のディレクトリ - Microsoft Azur × +					-	o ×
\leftarrow \rightarrow G $\stackrel{\wedge}{\doteq}$ https://portal.azure.com/#blade/Microsoft_A	AD_IAM/ActiveDirectoryMe	nuBlade/Registered 🖉	ි 🚨 ර	£∕≡	@	
三 Microsoft Azure 👂 リソース、サービス、ドキュメントの被	索 (G+/)	📃 🛛 🖓 🖉 🖉				8
ホーム > 既定のディレクトリ						
<mark>₩</mark> 既定のディレクトリ│アプリの登録 . _{Azure Active Directory}	¢					×
● 概要	(ント 🤌 トラブルシュー	ティング 🖒 最新の情報に更新	新 🛓 ダウンロー	F		
 □ ブレビュー機能 ② 2020 年 6 月 30 日以降、 ニカル サポートとせき Microsoft 認証ライブラ! 	Azure Active Directory 認証ライ リティ更新プログラムは今後も (MSAL) および Microsoft Grap	ブラリ (ADAL) および Azure AD Gra 提供されますが、機能更新プログラ h にアップグレードする必要があり	aph に新しい機能は1 ラムは提供されません ます。 詳細情報	っう追加され .。アプリケ	ません。テ ーションを	÷ ×
管理 ▲ ユーザー 本 エー ガー	所有しているアプリケ	ーション 削除されたアプリ	ケーション			
	これらの結 つかりました	「ケーション (クライアント) ID 次	₹の値で始まる ╳	™ ₽ 7	ィルターの	1追加
 管理単位 Check Point Harmor エンタープライズ アプリケー 	y Connect (Azure AD)	アプリケーション (クライ 5072642f-70e1-4ace-9232-f.	作成日 ↑↓	証明書と -	:シークレ	୬ ト
ý≡>		bdc1ac05-5871-4942-a9a6-0	5 2021/12/7	-		
戦 アプリの登録						
 Identity Governance 						

 クライアント シークレットの追加 - Mic 	× +					-	0	×
\leftarrow \rightarrow C $https://portal$	al.azure.com/?l=ja.ja-jp#blade/Microsoft_AAD	_RegisteredApps/Appli	icationMe að	ය 🚨	3 ☆	œ		
≡ Microsoft Azure 🔎 リソー	ース、サービス、ドキュメントの検索 (G+/)	Þ	o 🗣 🖉 «	3 O R				0
$\pi - L > CPJ > Check Point Harmony$	Connect (Azure AD)	クライアン	トシークレ	ットの追	追加			×
 → 快悪 (Ctrl+r) ≪ 様		說明 有効期限		24 か月				~
管理 ■ ブランド ● 町田舎とシークレット Ⅲ トークン漠成	 Application registration certificates, secr Certificates (0) Lient secrets (0) トークンの要求時にアプリケーションが自 こともあります。 							
 ◆ APIのアクセス許可 ▲ APIの公開 	+ 新しいクライアントシークレット **** ********************************	۴						
СНЕСК	説明 demo	有効期限 2023/11/17	値		Q	シ-	-クレ	ÿ⊦ID

13. 「アプリの登録」画面で、「すべてのアプリケーショ ン」をクリックする

14. 「Check Point Harmony Connect (Azure AD)」が表示されるのでクリックする

15.「証明書とシークレット」をクリックする
16.「新しいクライアントシークレット」をクリックして、 クライアントシークレットを追加する

「説明」、「有効期限」は、任意

17. 作成されたクライアントシークレットの「値」をコピー して、Harmony Connect の「ディレクトリ統合の設

定 画面に入力する

Azure AD での認証連携設定(7/10)

アプリの登録 > Check Point Harmony Connect (Azure AD)

Check Point Harmony Connect (/ ×	+ - • ×
\leftarrow \rightarrow C $https://portal.azu$	re.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationM 🖉 🏠 🞴 🔇 🗲 🔂 😩 …
😑 Microsoft Azure 🔎 リソース、	サービス、ドキュメントの検索 (G+) 🛛 💀 🖓 🛞 🕐 🔗
ホーム > 既定のディレクトリ > Check Poi	nt Harmony Connect (Azure AD)
× 🕘 Check Point Harm	ony Connect (Azure AD) API のアクセス許可 🖌 …
▶ 検索 (Ctrl+/) ≪	○ 最新の情報に更新 🔗 フィードバックがある場合
賜 根憂	
📣 クイックスタート 🚀 統合アシスタント	⑦ "管理者の現在が必要"引には、追集の規定性が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリ どとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の確が反映されていない場合があ ります。 詳細情報
管理 ゴランド化とプロパティ	構成されたアクセス許可
	アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が行与されている場合、APA を呼び出 ことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要す ります。アクセス許可と同意に関する範疇情報
 ・ 証明管とソークレット ・ ・ ・	+ アクセス許可の追加 / 原定のディレクトリ に管理者の同意を与えます
→ APIのアクセス許可	API/アクセス許可 種類 説明 管理者の同意が必要 状態
··· API の公開	アクセス許可は温加されませんでした
🌇 アプリロール	
🎒 所有者	アクセス許可とユーザーの同意を表示および管理するために、エンタープライズ アプリケーションをお試しください。
•	·

API アクセス許可の要求

API を選択します

Microsoft API 所属する組織で使用している API 自分の API

よく使用される Microsoft API

Microsoft Graph

Office 365、Enterprise Mobility + Security、Windows 10 の大量のデータを活用しましょう。Azure AD、Excel、 Intune、Outlook/Exchange、OneDrive、OneNote、SharePoint、Planner などに単一エンドポイント経由でアクセス できます。 18. 「API のアクセス許可」をクリックする

19. 「アクセス許可の追加」をクリックする

20. 「API アクセス許可の要求」画面で、「Microsoft Graph」を選択する

CHECK POINT YOU DESERVE THE BEST SECURIT

Azure AD での認証連携設定(8/10)

アプリの登録 > Check Point Harmony Connect (Azure AD)

API アクセス許可の要求			×		21. I	AP	1 5 2
く すべての API					•	ጠ	िंग्ना
Microsoft Graph							ℹϮ╹IJ⅃
https://graph.microsoft.com/ ドキュメント 🗗							
アプリケーションに必要なアクセス許可の種類			_)2 □		$\mathbb{L}\mathcal{D}^{-}$
委任されたアクセス許可	アプリケーションの許可			_	- <u></u>		
アプリケーションは、サインインしたユーザーとして API にアク・ スする必要があります。	アプリケーションは、サインインし ウンド サービスまたはデーモンとし	たユーザーなしで、バック して実行されます。	> グラ		右	까니	- + ;
アクセス許可を選択する		ुन् ,	べて展開		.H		
₽ アクセス許可を入力し始めると、これらの結果がフィルタ-	-処理されます				•		Grou
アクセス許可	管理者の	の同意が必要					
✓ Group (1)					•		User.
Group.Create () Create groups	はい						
Group.Read.All () Read all groups	はい						
Group.ReadWrite.All ① Read and write all groups		ony Connect (Az	zure A	D) API のアク セ	2ス許可 ♪		
	▶ 検索 (Ctrl+/) ≪	◇ 最新の情報に更新	R 2	ィードバックがある場合			
V User (1)	- 概要	アプリケーションはす。	こ対するアク	セス許可を編集しています。ユ	ーザーは、既に同意したこ	とがある場合で	でも同意が必要になりま
User.Export.All ① Export user's data	 						
User.Invite.All ① Invite guest users to the organization	管理 ■ ブランド化とプロパティ	● "管理者の同意が必 プリごとにカスター 合があります。 算	要" 列には、 マイズできま :細情報	組織の既定値が表示されます。 す。この列には、ご自分の組織	ただし、ユーザーの同意に や、このアプリが使用され	t、アクセス許™ いる組織の値が別	可、ユーザー、ア × 反映されていない場
User.ManageIdentities.All () Manage all users' identities	Э 認証	構成されたアクセス	許可				
- User.Read.All ①	↑ 証明書とシークレット	アプリケーションは、同	意 のプロセ	スの一環としてユーザーか管	理者からアクセス許可カ	付与されてい	る場合、API を呼び出
Read all users' full profiles	₩ トークン構成	すことが承認されます。 があります。 アクセス製	構成された F可と同意に	_ アクセス許可の一覧には、ア 関する詳細情報	プリケーションに必要な	すべてのアク	セス許可を含める必要
User.ReadWrite.All ① Read and write all users' full profiles	 APIのアクセス許可 						
	 API の公開 	+ アクセス許可の追加 ADI/アクセス許可の追加	u V 晄河	Eのディレクトリ に管理者の 諸朋	□思を与えます 管理表の同音ポぶ覀	计能	
アクセス許可の追加 破棄	アプリロール	API / デンセム計刊 Microsoft Graph (3)	住主状机	a.t. 17]	6 注省の1月息70 必安	1八悲	
		Group.Read.All	委任済み	Read all groups	はい	▲ 既定のテ	ディレクトリに… ・・・
		User,Read	委任済み	Sign in and read user pr	いいえ		
	- マニフェスト		200 Tale // 1 /	3			

アクセス許可の要求」画面で、「アプリケーショ 可」を選択する の一覧が表示されるので、以下のアクセス許可を

する

- Group.Read.All
- Jser.Read.All

Azure AD での認証連携設定(9/10)

る。

アプリの登録 > Check Point Harmony Connect (Azure AD)

Check Point Harmony Connect (/ 🗙	+					— C) ×
\leftarrow \rightarrow C $ riangle$ https://portal.a	zure.com/#blade/Microsof	t_AAD_Reg	isteredApps/ApplicationM.	- P to 🚨	(3 ≦	œ 🌘)
☰ Microsoft Azure ルリソース	ス、サービス、ドキュメント	の検索 (G+/		l 🕫 🔅 🧳	₹		0
ホーム > CPJ > Check Point Harmony C	onnect (Azure AD) ny Connect (Az	ure AD)) API のアクセ	【ス許可 ♪			×
	🕐 最新の情報に更新	🔊 🖓 ७४	ードバックがある場合				
概要	▲ アプリケーションに	対するアクセ	?ス許可を編集しています。ユー	-ザーは、既に同意したこ	ことがある場合でも	同意が必要に	なりま
🗳 クイックスタート	9 o						
🚀 統合アシスタント							
管理 ̄ ̄ ブランド化とプロパティ	● "管理者の同意が必要 プリごとにカスタマ 合があります。 詳録	見"列には、総 イズできます 田情報	1織の既定値が表示されます。; 。この列には、ご自分の組織が	ただし、ユーザーの同意! や、このアプリが使用され	t、アクセス許可、 いる組織の値が反映	ユーザー、ア されていない	× 場
● 認証	構成されたアクセス	忤可					
▼ 証明書とシークレット	アプリケーションは、同調	意のプロセス	の一環としてユーザーか管理	里者からアクセス許可か	「付与されている場	合、API を	手び出
 トークン構成 APIのアクセス許可 	すことが承認されます。《 があります。 アクセス許	^{実成されたり} 可と同意に開	・クセス許可の一覧には、ア: 創する詳細情報	フリケーションに必要る	いかべてのアクセン	(計刊公告の	る必要
🙆 API の公開	┿ アクセス許可の追加	🗸 СРЈ	に管理者の同意を与えます				
🔣 アプリロール	API / アクセス許可	種類	説明	管理者の同意が必要	状態		
🎎 所有者	✓ Microsoft Graph (3)						•••
♣ ロールと管理者 プレビュー	Group.Read.All	委任済み	Read all groups	はい	🛕 既定のディ	レクトリ に	
□ マニフェスト	User.Read	委任済み	Sign in and read user pr	いいえ			
サポート + トラブルシューティン 🗸	User.Read.All	委任済み	Read all users' full profil	はい 	▲ 既定のディ	レクトリに	

API / アクセス許可	種類	説明	管理者の同意が必要	状態	
∽ Microsoft Graph (3)			_		•••
Group.Read.All	委任済み	Read all groups	はい	🔮 既定のディレクトリ に	
User.Read	委任済み	Sign in and read user pr	いいえ	🔮 既定のディレクトリ に	
User.Read.All	委任済み	Read all users' full profil	はい	❷ 既定のディレクトリ に	•••

22. 「[ディレクトリ名] に管理者の同意を与えます」をク

リックして、API アクセス許可に管理者の同意を与え

©2022 Check Point Software Technologies Ltd. 21

Azure AD での認証連携設定(10/10)

エンタープライズアプリケーション > Check Point Harmony Connect (Azure AD)

	× +		- • ×
\leftarrow \rightarrow C $\textcircled{https://port}$	tal.azure.com/#blade/Microsoft_AAD.	_IAM/ManagedAppMenuBlade/ 🖉 🖞	3 🖪 4 14 🖷 🔵 …
≡ Microsoft Azure ዾリソ	ース、サービス、ドキュメントの検索・	(G+/) 🗵 🕞 🗳	୦ ନ 🙆
ホーム > CPJ > エンタープライズ:	アプリケーション > Check Point Har	mony Connect (Azure AD)	
👷 Check Point Harm	ony Connect (Azure A	\D) ユーザーとグループ	X
エンタープライズ アプリケーション (()			
1 极要	┼ ユーサーまたはクループの追	加 パ 編 属 回	π ≡≡ 91] ···
🛄 デプロイ計画	アプリケーションは、割り当 ィの中で [ユーザーに表示しま	てられたユーザーのマイ アプリ内に表示されます。 !すか?]を [いいえ] に設定します。	これを表示しないようにするには、プロパテ →
管理		す。すべてのユーザーとグループを検索するに	は、表示名を入力してください。
プロパティ	表示名	オブジェクトの種類	割り当てられたロール
🎥 所有者	AL alice	ユーザー	Default Access
🔓 ロールと管理者 (プレビュー)	BO bob	ユーザー	Default Access
🍱 ユーザーとグループ	CH char	ユーザー	Default Access
Э シングル サインオン	DO dozle	ユーザー	Default Access
⊅ プロビジョニング	EM emma	2-#-	Default Access
& ァクセス許可 ● トークンの暗: 選択され ロールを過	にいません 選択してください	ーザーとグループ	
User	٦) 検索	
		AL alice alice@smb-se.checkpoint.sc	
		BO bob bob@smb-se.checkpoint.sc	
	選	BO bob bob@smb-se.checkpoint.sc Rしたアイテム	
	躍; 耳	BO bob@smb-se.checkpoint.sc 駅したアイテム 頁目が選択されていません	

- 23. 「ユーザーまたはグループの追加」をクリックする
- 24. 「割り当ての追加」画面で、「ユーザーとグループ」を クリックする
- 25. 「ユーザーとグループ」画面に、Azure AD のユーザー
 - とグループが表示されるので、Harmony Connect を利
 - 用するユーザー、グループを選択する
 - Harmony Connect に「グループ」を割り当てるためには、Azure AD Premium P1、P2 等のライセンスが必要です



YOU DESERVE THE BEST SECURITY

THANK YOU

