

# Oracle Cloud Infrastructureでの 緊急アクセス・アカウントの管理

2023年4月、バージョン1.0

Copyright © 2023, Oracle and/or its affiliates Public

## 免責事項

本文書には、ソフトウェアや印刷物など、いかなる形式のものも含め、オラクルの独占的な所有物である占有情報が含まれます。この機密文書へのアクセスと使用は、締結および遵守に同意したOracle Software License and Service Agreementの諸条件に従うものとし、本文書と本文書に含まれる情報は、オラクルの事前の書面による同意なしに、公開、複製、再作成、またはオラクルの外部に配布することはできません。本書は、ユーザーとのライセンス同意書の一部をなすものではなく、またオラクルやその子会社および関連会社とのいかなる契約上の合意事項にも含まれるものではありません。

本書は情報提供のみを目的としており、記載した製品機能の実装およびアップグレードの計画を支援することのみを意図しています。マテリアルやコード、機能の提供をコミットメント（確約）するものではなく、購買を決定する際の判断材料にするものでもありません。本書に記載されている機能の開発、リリースおよび時期については、オラクルの裁量により決定されます。製品アーキテクチャの性質上、コードが大幅に不安定化するリスクなしに、本書に記載されているすべての機能を安全に含めることができない場合があります。

## 改訂履歴

本書には下記の改訂が行われています。

日付	改訂
2023年4月	初版

# 目次

---

概要 .....	5
バックグラウンド .....	5
初期構成 .....	5
プロセスとポリシーの考慮事項 .....	6
緊急アクセス・アカウントの保護 .....	6
パスワード・ポリシーの構成 .....	6
多要素認証の構成 .....	8
緊急アクセス・アカウントの使用の監視 .....	10
アラートの構成 .....	10
アカウントに加えた変更に関するアラート .....	12
アカウント使用の監査 .....	12
結論 .....	13

## 概要

この技術資料では、OCI Identity and Access Management (IAM) を使用して、不必要なリスクを招いたり、セキュリティのベスト・プラクティスに反したりすることなく、Oracle Cloud Infrastructure (OCI) テナンスに緊急アクセスするメカニズムを実装する方法について説明します。

各OCIテナンスは、Administratorsグループと、テナンスへのフル・アクセスを許可する関連テナント管理ポリシーで作成されます。その結果、スーパーユーザー相当のロールが作成され、テナンス内のすべてのリソースを管理する権限が付与されます。OCIでは、お客様がテナンスを管理できなくなるのを防ぐため、少なくとも1つのユーザー・アカウントをAdministratorsグループに割り当てることが要求されます。リスクを軽減するため、テナンス所有者による、スーパーユーザー権限がある管理者アカウントの使用は必要な場合のみとするべきです。Administratorsグループのメンバーシップは、OCIクラウド管理者全員に付与するべきではありません。セキュリティのベスト・プラクティスでは、このグループは緊急アクセス（つまり「緊急時対応」）の目的のみに使用することを推奨しています。代わりに、他のクラウド管理者には、最小限の権限付与の原則に従い、それぞれのロールに適したアクセス権限のみを割り当てべきです。

Administratorsグループのユーザー・アカウントは、大きな権限があり、通常の使用を意図していないため、必要な場合には使用できるようにしながらも、そのようなアカウントに関連するリスクを低減するために、いくつかのコントロールを実装できます。この技術資料では、その目標を達成するために実装可能な、関連するいくつかの技術的コントロールについて詳しく説明します。

## バックグラウンド

OCIテナンスが作成されると、オラクルはテナンス用にデフォルトの管理者アカウントを設定します。テナンス所有者は、このアカウントを使用して追加の管理者を設定できます。このデフォルト・アカウントは、デフォルトのOCI IAM IDドメインにあるAdministratorsと呼ばれるグループのメンバーシップにより管理権限が付与されます。このグループは削除できず、常に少なくとも1人のメンバーがいなければなりません。

新規の各テナンスには、テナンス内のすべてのOCI API操作とすべてのOCIリソースへのアクセス権をAdministratorsグループに付与するポリシーも自動的に作成されます。このポリシーは変更または削除できません。したがって、Administratorsグループに追加されたアカウントは、テナンス全体とその中のすべてのリソースにフル・アクセスできます。

Administratorsグループに少なくとも1人のメンバーを存在させるという要件を満たしており、関連する管理者ポリシーがあれば、すべてのテナンスは緊急アクセス・アカウントを確実に持つことができます。このグループまたはポリシーを削除できるか、またはグループからすべてのメンバーを削除できるのであれば、どのユーザーもアクセス権を割り当てることができず、すべてのユーザーがテナンスからロックアウトされるという状況が生まれる可能性があります。

## 初期構成

緊急アクセスを目的としてユーザー・アカウントを作成する場合、そのアカウントはデフォルトIDドメイン内に作成し、Administratorsグループに割り当てる必要があります。緊急アクセス用のアカウントには、EmergencyAccessといったユーザー名を割り当てるなどして、分かりやすいラベルを付けます。この名前は、アクセス権の再検討時に間違いが発生することを避けるためのものです。

外部のIDプロバイダからフェデレーション・サインインでOCIにアクセスする場合でも、緊急アクセス・アカウントはローカルに作成する必要があります。IDプロバイダの停止は、緊急アクセスが必要になる可能性のある主要なシナリオです。

デフォルトでは、OCI IAMにおいて、ユーザー・アカウントの作成時に電子メール・アドレスを割り当てる必要があります。電子メールは、初期アカウント・パスワードの配信に使用され、アカウントのリカバリにも使用できます。緊急アクセス・アカウントに使用される電子メールは適切に管理する必要があり、メールボックスへのアクセスは監視する必要があります。パスワード・リカバリ・プロセスによるアカウント乗っ取りのリスクを低減するため、この技術資料のガイダンスを使用して、緊急アクセス・アカウントの多要素認証（MFA）を有効にしてください。

オプションとして、電子メール通知を受け取る機能なしでアカウントを作成する場合、アカウントのアクティブ化と初期パスワードの配信は、IAM APIを使用して実現できます。電子メール・ベースのアカウント・リカバリを無効にするには、電子メール・アドレスなしでアカウントを作成する必要があります。「**Domain Settings**」ページでIDドメインの「**Primary email address required**」設定を無効にすると、電子メール・アドレスの要件を一時的に削除できます。その後、電子メール・アドレスなしでアカウントを作成し、それから電子メール・アドレスの要件を再度有効にすることができます。

このアカウントを作成し、セキュリティ・モデルに沿う特定の目的（ユーザーを管理するID管理者、ポリシーを管理するセキュリティ管理者、ストレージ・リソースへのアクセスを管理するストレージ管理者など）のためにクラウド管理者を作成するポリシーを構成したら、テナンシーの Administratorsグループから他のすべてのメンバーを削除する必要があります。

---

**注：** デフォルトIDドメインのユーザーとグループを変更する権限を持つユーザーは、緊急アクセス・ユーザーと Administratorsグループを変更できます。これらの権限を付与するポリシーには注意を払い、定期的にアクセス権を再検討してください。また、この技術資料で後述するように、これらのオブジェクトが変更されたときに生成されるアラートを構成することもできます。

---

## プロセスとポリシーの考慮事項

クラウド管理用の緊急アクセス・アカウントは、常に組織固有のセキュリティ・ポリシーに従って扱う必要がありますが、考慮すべきいくつかのベスト・プラクティスがあります。たとえば、緊急アクセス・アカウントには、そのアカウントの資格証明ライフサイクルの管理に責任を持つ、定義された管理人（または管理人のグループ）が必要です。管理人は、緊急時の承認されたアカウント使用の後に、資格証明をローテーションしてテストする責任を負います。この操作のメカニズムとタイミングは、緊急変更管理プロセスで定義しておく必要があります。緊急アクセス資格証明を設定またはローテーションしたら、それらを物理的または仮想的な「金庫」に保護できます。これはポリシーによって緊急手順時にしかアクセスできないものであるべきです。

## 緊急アクセス・アカウントの保護

緊急アクセス・アカウントは、大きな権限があり、管理された状況のみでの使用を意図しているため、ベスト・プラクティスは、それに関連して強力なセキュリティ管理を実装することです。OCI IAM IDドメインは、個々のセキュリティ・グループに特定の制御を付与するように構成できます。

## パスワード・ポリシーの構成

デフォルトIDドメイン内でグループ・ベースのパスワード・ポリシーを使用することで、特定のパスワード・ポリシーを Administratorsグループに適用できます。これを行うには、次のスクリーンショットに示すように、[パスワード・ポリシーを作成し](#)、それをOCI IAM IDドメイン内の最高優先順位である優先順位1で Administratorsグループに割り当てます。この設定の組み合わせにより、Administratorsグループのアカウントは、デフォルト・パスワード・ポリシーの代わりに、これらの新しいパスワード管理の対象になります。

## Add password policy

Name  
BreakGlassPasswordPolicy

Description  
Password Policy for Emergency Access User

Priority  
1

Groups *Optional*

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Administrators	Administrators group in the OCI account

0 selected Showing 1 group < Page 1 >

Password policy strength  
 Simple  Standard  Custom

The following criteria apply to passwords:

Password length (minimum)  
50

Password length (maximum) *Optional*  
100  
No limit if left blank

Expires after (days) *Optional*  
0

Account lock threshold *Optional*  
12

Enable automatic account unlock ⓘ

図1 : 緊急アクセス・アカウントのパスワード・ポリシー

このパスワード・ポリシーは、カスタムのパスワード強度を使用するように構成でき、パスワード長を50文字以上とすることやアカウントの有効期限の削除など、適切な値を設定できます。

パスワード・ルールに選択する具体的な値は、組織のセキュリティ・ポリシーに従うものとする必要があります。ただし、パスワード長を50文字以上とするというのは、正確に入力するための妥当な長さを維持しながら、推測したりブルート・フォース攻撃で発見したりするのは事実上不可能な長さであるため、現実的な選択です。

## 多要素認証の構成

このアカウントには大きな権限があるので、ユーザー名とパスワード以外の追加の認証要素を構成するのがベスト・プラクティスです。ただし、アカウント・ログインが、緊急アクセスが必要ときに利用できない可能性のあるデバイスや個々のユーザーに拘束されないようにする必要もあります。パスワードと同じ物理的な金庫に保管されているFast ID Online (FIDO) セキュリティ・キーを使用することは、緊急アクセス・アカウントのための適切な多要素認証 (MFA) オプションとなる場合があります。

デフォルトのサインオン・ポリシーでサインオン・ルールを作成することで、MFA設定をAdministratorsグループのみに適用するように構成できます。このルールを使用して、緊急アクセス・アカウントに対して特定の要素を要求したり、緊急アクセス・アカウントでのMFAの使用を免除したりすることができます。

---

**重要：** デフォルトでは、すべてのOCIテナンシーに対してデフォルトのサインオン・ポリシーが構成されています。これはつまり、誤った構成を行うと、テナンシーへのアクセスを回復できなくなる可能性があるということです。このポリシーを変更するときは、別のブラウザまたはプライベート・ブラウザ・セッションで環境に引き続きアクセスできることを確認するまで、ポリシーを変更するために使用しているセッションからログアウトしないでください。

---

次のスクリーンショットに示すように、デフォルトのサインオン・ポリシー内で、Administratorsグループのメンバーシップを持っていることを唯一の条件とする新しいルールを作成します。

The screenshot shows the 'Add sign-on rule' interface. At the top, there is a 'Rule name' field containing 'Force Break Glass Users to use MFA'. Below this is an information box with an 'i' icon and the text: 'Specify all the conditions required by this rule and the actions performed when conditions are met.' The 'Conditions' section contains two dropdown menus. The first is 'Authenticating identity provider' with the value 'Optional' and a 'Select...' dropdown menu. Below it is the text: 'The identity providers to use to authenticate the user accounts evaluated by this rule.' The second dropdown is 'Group membership' with the value 'Administrators' and a dropdown menu. Below it is the text: 'Groups that the user must be member of to meet the criteria of this rule.'

図2：Administratorsグループのメンバーのサインオン・ルールの作成

必ず「**Allow access**」を選択します。すべての管理者へのアクセスを拒否すると、テナンシーへのアクセスを回復できなくなる可能性があります。このルールに関連する操作を構成して、適切な認証メカニズム（特定の認証要素を指定するか、または追加要素を必要とせずアクセスを許可する）を適用します。次のスクリーンショットは、FIDO認証機能が必要な構成を示します。



## Add sign-on rule [Help](#)

**Actions**

Allow access     Deny access

Let users that meet the specified conditions of this rule sign in to this identity domain.

Prompt for reauthentication  
Require users to provide credentials the next time they sign in to this identity domain.

Prompt for an additional factor  
Require users to perform multifactor authentication.

Any factor     Specified factors only

Mobile app passcode

Fast ID Online (FIDO) authenticator

Frequency ⓘ

Once per session or trusted device

Every time

Custom interval

Enrollment ⓘ

Required

Optional

[Add sign-on rule](#)    [Cancel](#)

図3：緊急アクセス・アカウントに常にFIDO認証機能を使用した認証を要求するサインオン・ルール・アクションの構成

MFAの使用を構成する場合、「**Frequency**」を「**Every time**」に変更し、信頼するデバイスの作成を許可しないようにすることができます。こうすることで、デバイスが前のセッションから認識されたときにMFA要件はバイパスされます。さらに、「**Enrollment**」を「**Required**」に設定すると、すべてのグループ・メンバーをMFAに登録するように強制できます。OCI IAMは、ユーザーがMFAに登録していれば、毎回ユーザーに対してチャレンジを行います。緊急アクセス・アカウントが別のチャレンジ・メカニズムを使用して認証される場合、「**Specified factors only**」オプションを使用してその要素を指定できます。

ポリシーのサインオン・ルールは、条件に一致するものが見つかるまで順番に評価されるので、この新しいルールが緊急アクセス・アカウントに常に適用されるようにするためには、評価順序で最初のものとなるようにしておく必要があります。次のスクリーンショットに示すように、ルールの優先順位を編集し、新しいルールをリストの最上位に移動させることでそうすることができます。



## Default Sign-On Policy

Edit sign-on policy Deactivate sign-on policy

Sign-on policy information

**Description:** Default Sign on Policy for Tenant  
**Created:** Wed, Aug 24, 2022, 02:32:09 UTC

### Sign-on rules

Add sign-on rule Edit priority Remove sign-on rule

<input type="checkbox"/>	Priority	Name	
<input type="checkbox"/>	1	Force Break Glass Users to use MFA	⋮
<input type="checkbox"/>	2	Default Sign-On Rule	⋮

0 Selected Showing 2 Items

図4 : サインオン・ルールの優先順位によって適切なルールが緊急アクセス・アカウントに適用される

新しいサインオン・ルールが適用された後に、MFAが有効になっている場合、緊急アクセス・アカウント管理者はOCIにサインインして、初期MFA登録をトリガーする必要があります。MFA登録が構成され、認証フローがテストされた後、MFAに必要な資格証明および関連するマテリアルは、緊急アクセス・ポリシーに従ってローテーションされ、保管される必要があります。

グループ・ベースのパスワード・ポリシーを構成し、グループ・ベースの条件をサインオン・ルールで構成することにより、緊急アクセス・アカウントのアクセス制御を他のアカウントから独立して構成できます。この分離により、管理者は、テナンシー内の他のすべてのアカウントに影響を与えることなく、ユーザーのグループのアクセス制御を管理できます。

## 緊急アクセス・アカウントの使用の監視

緊急アクセス・アカウントには大きな権限があり、通常の使用は意図していません。これらのアカウントの使用はいずれも、セキュリティ・ポリシーへの違反が生じる可能性があるものとして扱い、それに沿って各使用を評価することをお勧めします。

## アラートの構成

OCIは、緊急アクセス・アカウントにアクセスがあったときに、環境内の他の管理者にアラートを出せるように構成できるいくつかのサービスを提供しています。[OCI Events Service](#)は、OCI IAMを含む多くのOCIサービスにおいて、関心の対象となるイベントへの自動レスポンスを構成するための柔軟なメカニズムを提供します。Eventsを使用し、[OCI Notifications Service](#)によってアラートを送信できます。

まずOCIで、管理者アラートの送信に使用する[通知トピック](#)を構成します。

## Create Topic [Help](#)

To create a topic in a different compartment, [click here](#).

Name

Topic name must contain fewer than 256 characters. Only alphanumeric characters plus hyphens (-) and underscores (\_) are allowed.

Description *Optional*

Description must contain fewer than 256 characters.


 [Show advanced options](#)

図5：緊急アクセス・アカウントの使用について管理者にアラートを出すために使用する通知トピックの作成

トピックを作成した後に、1つ以上のサブスクリプションを追加できます。これはイベントによってトリガーされると通知を受け取ります。これらの通知は、電子メールとして送信したり、SlackやPagerDutyに送信したり、OCI Functionsや、webhookのサブスクライブによって別の通知ワークフローをトリガーしたりすることができます。管理者の好みの操作方法に適したメカニズムを選択します。

緊急アクセス・アカウント使用時の管理者への通知の送信を自動化するには、Events Serviceでイベント・ルールを作成し、サービスとして「**Identity SignOn**」、イベント・タイプとして「**Interactive Login**」を指定します。次に、**actorName**属性に、一致する条件を追加できます。以下のスクリーンショットは、イベント定義の例を示しています。

**注：** デフォルトIDドメインとの相互作用はルート・コンパートメントで発生するため、このルールはそのトップレベル・コンパートメントで作成する必要があります。

### Rule Conditions

Limit the events that trigger actions by defining conditions based on event types, attributes, and filter tags. [Learn more](#)

Condition	Service Name	Event Type
Event Type	Identity SignOn	Interactive Login

Condition	Attribute Name	Attribute Values
Attribute	actorName	breakglass@company.com

[+ Another Condition](#)

図6：緊急アクセス・アカウントによる認証イベントをキャプチャするためのイベント・ルールの構成

この構成を適用すると、緊急アクセス・アカウントが使用されたときに、他の管理者に通知され、適切なレスポンスがランブックにキャプチャされることになります。適切なレスポンスとしては、既存の未解決の問題やオペレーション・センターの対応に照らしたアクセスの検証や、緊急アクセス・アカウントの使用が不適切または悪意があると判断された場合のアカウント・リカバリ・ワークフローなどがあります。

## アカウントに加えた変更に関するアラート

類似の構成を使用して、APIキーを作成する機能の追加や、その他の潜在的に問題のある動作など、緊急アクセス・アカウントへの変更に関するアラートを出すことができます。このような変更により、**Identity**サービスは**Update**イベントを出力します。これは、次のスクリーンショットに示す構成を使用してトリガーできます。この構成では、この変更がアカウント管理人やIAM管理者などの別のユーザーによって行われる可能性があるため、アクターではなく、変更されたユーザー・リソースの**resourceName**が条件によりチェックされます。

**Rule Conditions**

Limit the events that trigger actions by defining conditions based on event types, attributes, and filter tags. [Learn more](#)

Condition	Service Name	Event Type
Event Type	Identity	User - Update × User Capabilities - Update × ×

---

Condition	Attribute Name	Attribute Values
Attribute	resourceName	breakglass@company.com ×

+ Another Condition

図7：緊急アクセス・アカウントへの変更をキャプチャするためのイベント・ルールの構成

追加の予防措置として、別のユーザーがAdministratorsグループに追加された場合のアラートを構成できます。このグループは緊急アクセス・アカウントにのみ使用されるため、このグループにユーザーを追加することは、そのテナンシーのセキュリティ・ポリシーに違反することになります。このイベント定義も、**Identity**サービスを使用し、イベント・タイプは**Group - Add User To**で、条件としてグループ名を使用します。

**Rule Conditions**

Limit the events that trigger actions by defining conditions based on event types, attributes, and filter tags. [Learn more](#)

Condition	Service Name	Event Type
Event Type	Identity	Group - Add User To ×

---

Condition	Attribute Name	Attribute Values
Attribute	resourceName	Administrators ×

+ Another Condition

図8：Administratorsグループへの変更をキャプチャするためのイベント・ルールの構成

## アカウント使用の監査

すべてのOCI管理アクティビティは、[OCI Audit Service](#)によって記録されます。その結果、緊急アクセス・アカウントの使用がログに記録され、そのログが悪意ある変更から保護されるようにするための追加の構成は必要ありません。組織の固有のセキュリティ・ポリシーに応じて、OCIの[Service Connector Hub](#)と[Object Storage Services](#)の組み合わせを使用して、監査ログのアーカイブと保存ポリシーを構成することをお勧めします。さらに、Service Connector Hubを使用して、監査ログをSecurity Incident and Event Management (SIEM) ツールに転送することもできます。

## 結論

この技術資料では、不必要なリスクを招いたり、一般的なセキュリティのベスト・プラクティスに反したりすることなく、OCIテナンシーに緊急アクセスするメカニズムを実装する方法について説明します。この構成では、組込みのAdministratorsグループとそれに関連するセキュリティ・ポリシーを使用します。これはテナンシーへのフル・アクセスを許可します。この技術資料では、緊急アクセス・アカウントに対する厳密認証を有効にする方法、および大きな権限があるそれらのアカウントの使用に関するアラートと監査について説明します。提供される詳細は、情報のみです。これらは一般的なセキュリティのベスト・プラクティスに従うことを意図していますが、テナンシー管理者は組織固有のセキュリティ・ポリシーに従う必要があります。

詳しくは、[OCIのセキュリティのベスト・プラクティスに関するドキュメント](#)および[IDドメインがあるOCI IAMのドキュメント](#)を参照してください。

---

### Connect with us

+1.800.ORACLE1までご連絡いただくか、[oracle.com](#)をご覧ください。北米以外の地域では、[oracle.com/contact](#)で最寄りの営業所をご確認いただけます。

 [blogs.oracle.com](#)

 [facebook.com/oracle](#)

 [twitter.com/oracle](#)

---

Copyright © 2023, Oracle and/or its affiliates. All rights reserved. 本文書は情報提供のみを目的として提供されており、ここに記載されている内容は予告なく変更されることがあります。本文書は、その内容に誤りがないことを保証するものではなく、また、口頭による明示的保証や法律による黙示的保証を含め、商品性ないし特定目的適合性に関する黙示的保証および条件などのいかなる保証および条件も提供するものではありません。オラクルは本文書に関するいかなる法的責任も明確に否認し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクルの書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

OracleおよびJavaはOracleおよびその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標です。

IntelおよびIntel XeonはIntel Corporationの商標または登録商標です。すべてのSPARC商標はライセンスに基づいて使用されるSPARC International, Inc.の商標または登録商標です。AMD、Opteron、AMDロゴおよびAMD Opteronロゴは、Advanced Micro Devicesの商標または登録商標です。UNIXは、The Open Groupの登録商標です。0120