



NetIQ® Identity Manager 識別情報アプリケーションのユーザー ズガイド

2024 年 5 月

保証と著作権

Copyright 2009-2024 Open Text.

Open Text、関連会社、およびライセンサ（「Open Text」）の製品およびサービスに対する保証は、当該製品およびサービスに付属する保証書に明示的に規定されたものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。Open Text は、本書に技術的または編集上の誤りまたは不備があっても責任を負わないものとします。本書の内容は、将来予告なしに変更されることがあります。

証明書関連の通知および商標などの追加情報については、<http://www.microfocus.com/about/legal/> (<http://www.microfocus.com/about/legal/>) を参照してください。

目次

本書およびライブラリについて	7
ページのパート I Identity Manager の紹介	9
1 はじめに	11
役割とリソースの理解	11
Identity アプリケーションの理解	11
Identity Manager ダッシュボードの理解	11
ダッシュボードの機能	12
[アプリケーション] ページの理解	13
タスクを理解する	14
Identity アプリケーションを使用する一般的な方法	14
Identity セルフサービスの仕組み	14
役割とリソースの仕組み	15
プロセス要求の仕組み	16
ヘルプデスクの仕組み	16
2 Identity アプリケーションへのアクセス	19
Identity アプリケーションにアクセスする際の考慮事項	19
初めてログインする	20
優先するロケールのチェックに対応	22
ログインの問題のトラブルシューティング	22
パスワードを忘れた場合	22
ログイン処理で問題が発生した場合	22
追加情報の入力を求められた場合	23
ログアウト	23
ページのパート II ダッシュボードのカスタマイズ	25
3 ウィジェットとレイアウトの管理	27
グローバルダッシュボードの管理	28
ダッシュボードレイアウトの変更	28
ウィジェットの追加	29
全般ウィジェットの追加	30
Identity Manager のウィジェットの追加	31
Identity Governance のウィジェットの追加	32
ウィジェットのオプション	32
ウィジェットの設定	33

ページのパート III 許可および Identity プロファイルの管理	35
4 許可要求の管理	37
許可の表示	37
許可の要求	39
要求の表示	39
要求の追跡	40
要求のキャンセル	40
ヘルプデスクチケットの作成	41
許可の取り消し	41
要求へのディープリンク	42
5 アプリケーションの管理	45
おすすめ項目の作成	45
アプリケーションの追加	45
許可の追加	46
カテゴリの追加、変更、または削除	46
カテゴリの追加	46
カテゴリの変更	47
カテゴリの削除	47
6 自分のタスクの管理	49
自分のタスクの表示	49
承認または拒否の要求の管理	50
ヘルプデスクタスクの管理	52
7 他の人の代わりに実行する	53
自分の代理人割り当ての表示	53
代理ユーザとしての作業	53
代理人割り当ての管理	53
8 委任の管理	55
9 可用性の管理	57
10 プロファイルの管理	59
プロファイルの更新	59
11 組織図の管理	61
組織図の表示	61
組織チャートの理解	62
組織図での作業	63
組織チャートビューでのルートのリセット	64
組織チャートビューの切り替え	64
表示する関係の選択	65
関係階層の次のレベルに移動	66

組織チャートからユーザへの電子メールの送信	67
ユーザの詳細情報の表示	67
12 パスワードの管理	69
Identity Manager でのセルフサービスパスワード管理の使用	69
パスワード確認の回答の理解	70
パスワードを変更する	70
パスワードポリシーステータス	71
従来のパスワード管理の使用	71
パスワード確認の回答	72
パスワードヒントの変更	73
パスワード変更	73
パスワードポリシーステータス	75
パスワード同期ステータス	75
ページのパート IV ユーザ、グループ、およびチームの管理	77
13 ユーザの管理	79
ユーザの作成	79
ユーザ情報を編集する	79
ユーザの一覧表示	80
ユーザの検索	81
ユーザのソート	82
14 チームの管理	83
チームの表示	83
チームの作成	84
チームの変更	84
15 グループを管理する	85
グループの作成	85
ページのパート V 付録	87
A Identity Manager 承認アプリケーションの使用	89
製品の要件	89
承認アプリケーションのインストール	90
承認アプリケーションの設定	90
ユーザアプリケーションからのモバイルアクセスの要求	90
設定リンクまたは QR コードの使用	91
承認アプリケーションの手動設定	92
承認アプリケーションの概要	94
[タスク] ビュー	94
詳細ビュー	95
Bulk Mode (一括モード)	95
[Completed Tasks (完了したタスク)] ビュー	96
[ログイン設定] ビュー	96

[Advanced Settings (詳細設定)] ビュー	96
承認アプリケーションの表示言語の変更	97

本書およびライブラリについて

このガイドでは、エンドユーザと一部の管理者が、NetIQ Identity Manager Identity アプリケーション (特にダッシュボードとユーザアプリケーション) を使用する方法について説明します。

本書の読者

本書は、管理に関する概念を理解し、安全な分散管理モデルを実装する担当者を対象とします。

ライブラリのその他の情報

Identity Manager のライブラリの詳細については、[Identity Manager マニュアルの Web サイト \(https://www.netiq.com/documentation/identity-manager-49/\)](https://www.netiq.com/documentation/identity-manager-49/) を参照してください。

Identity Manager の紹介

NetIQ Identity Manager は、組織内のユーザコミュニティのアクセス権を安全な方法で管理するためのシステムソフトウェア製品です。ユーザコミュニティの所属メンバーは、Identity Manager の導入メリットをさまざまな形で享受できます。たとえば、Identity Manager を使って次のことを実行できます。

- 使い始めたその日から、情報 (グループ組織図、部署別電話帳、従業員検索) に加え、役割およびリソース (社内システムの機器とアカウント) に対するアクセス権をユーザに付与する
- 複数のパスワードを同期して、すべてのシステムに対してシングルログインできるようにする
- 必要に応じて (誰かが別のグループに異動するときや組織を離れる場合など)、すぐにアクセス権を変更したり、無効にしたりする
- 政府関連規制への準拠をサポートする

Identity Manager Identity アプリケーションとその基本的な使用方法を理解するために、このパートを最初にお読みください。このガイドは、組織の以下のタイプのオンラインアクティビティを支援することを目的としています。

- 組織のリソースに関連付けられたオンラインの Identity を管理する。
- 組織の役割とリソースへのアクセス権を表示または変更する。
- リソースと役割へのアクセス権の要求を承認する。
- 組織がそのメンバーに提供するソフトウェアアプリケーションおよびその他のリソースに関連付けられた許可を管理する。

1 はじめに

この項では、Identity アプリケーションの基本的な使用方法について説明します。主なトピックは次のとおりです。

- 11 ページの「役割とリソースの理解」
- 11 ページの「Identity アプリケーションの理解」
- 11 ページの「Identity Manager ダッシュボードの理解」
- 12 ページの「ダッシュボードの機能」
- 14 ページの「タスクを理解する」
- 14 ページの「Identity アプリケーションを使用する一般的な方法」

役割とリソースの理解

Identity アプリケーションでは、許可は、ユーザまたはユーザのグループに対して提供される、役割またはリソースに対するアクセス権を意味します。役割は、1 つ以上のターゲットシステムまたはアプリケーションに関連する一連の許可を定義します。たとえば、ユーザ管理者の役割には、ユーザのパスワードをリセットする権限が与えられますが、システム管理者の役割には、ユーザを特定のサーバに割り当てる権限があります。リソースは、任意のデジタルエンティティ (ユーザアカウントなど)、コンピュータ、またはビジネスユーザがアクセスできる必要のあるデータベースです。

Identity アプリケーションの理解

Identity Manager Identity アプリケーションは、ブラウザベースの複数の Web アプリケーションが相互接続されたセットです。これにより、組織では、ユーザが利用できるさまざまな役割とリソースに関連付けられたユーザアカウントおよび許可を管理することができます。役割の要求やパスワードの変更など、ユーザに対してセルフサービスサポートを提供するように Identity アプリケーションを設定することができます。役割とリソースの管理および割り当ての効率が向上するようにワークフローを設定することも可能です。

Identity Manager ダッシュボードの理解

NetIQ Identity Manager ダッシュボード (ダッシュボード) は、Identity アプリケーションへの主要な入口ポータルとして機能します。ダッシュボードには、特定のアクティビティに関するクイック情報の表示に役立つ 1 つ以上のウィジェットを設定することができます。ダッシュボードから、次のアクティビティを実行できます。

- プロファイルの設定とパスワードを管理する。
- 組織図の詳細を表示する。

- アクセスに対するユーザ要求の承認などのタスクをレビューして完了する。
- 役割、リソース、またはプロセスの許可を要求する。
- 許可に対する要求の状態と履歴をレビューする。
- 組織内のその他のユーザを見つける。
- ダッシュボードをパーソナライズし、ウィジェットを追加したり、自分の興味に基づいてウィジェットを再配置する。
- システムから代理人として任意のユーザを設定する。
- システムから他のユーザにタスクを委任する。

適切な許可を使用して、以下の操作を行うことができます。

- ユーザプロフィールを作成および編集する。
- 他のユーザの組織図の詳細を表示する。
- チームに関連付けられたプロビジョニング要求および承認タスクを実行できる、ユーザとグループのセットを表すチームを作成および変更する。
- 組織内の他のユーザの代わりに許可を要求するか、または許可を取り消す。

ダッシュボードの機能

ダッシュボードには、ウィジェットの形式で、タスク、許可、および要求に関するクイック情報が表示されます。1回のクリックで、特定のページまたはアプリケーションに移動することができます。また、ダッシュボード上でウィジェットを追加、削除、再配置、および設定することができます。ダッシュボードのパーソナライズの詳細については、[27 ページの第3章「ウィジェットとレイアウトの管理」](#)を参照してください。

ダッシュボードのデフォルトのウィジェットオプションを説明する例を以下に示します。

図1-1 パーソナルダッシュボードの例



Identity Manager ダッシュボードでは、Identity Manager のさまざまなアクティビティを管理できます。タスクとアクティビティを管理するのに役立つページを以下に示します。

アプリケーション

プロビジョニングされているすべてのアプリケーションを一覧表示します。このページには、Identity Manager で実行する必要がある基本的なタスクを効率化するために、複数の領域へのデフォルトのリンクが表示されます。詳細については、[13 ページの「\[アプリケーション\] ページの理解」](#)を参照してください。

タスク

アクションを保留中のすべてのタスクを表示します。適切な役割があれば、他のユーザのタスクを表示することができます。たとえば、「Team Manager」のタスクを表示できます。

アクセス

許可の表示または許可の要求を行うことができます。要求された許可のステータスを表示するには、[\[要求履歴\]](#)に移動します。このページには、すべての要求とそれらのステータスが表示されます。

ユーザ

システム内の他のユーザまたはグループ、および他のユーザの[\[組織図\]](#)を表示できます。これは、ユーザとグループの関係を視覚化するのに役立ちます。

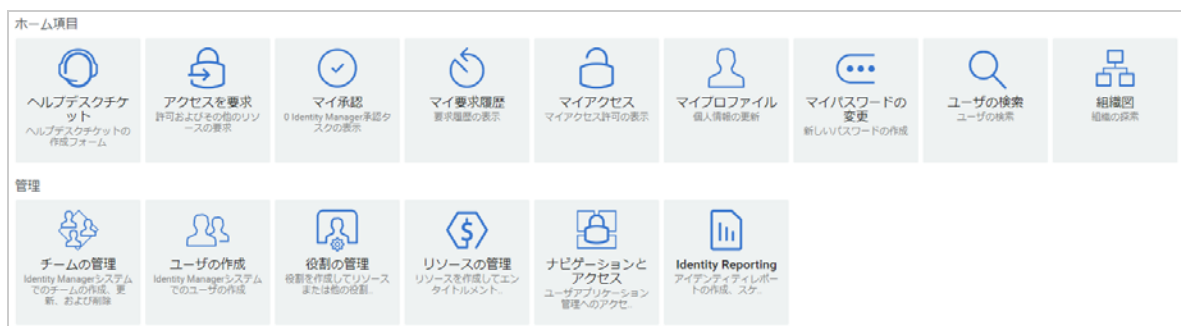
管理

役割、リソース、許可の更新、およびその設定を表示および管理できます。このオプションは管理者にのみ表示されます。管理タスクの詳細については、『[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)』の「[Identity Applications Administration](#)」を参照してください。

[アプリケーション] ページの理解

ダッシュボードの2つ目の重要なビューは、[\[アプリケーション\]](#)ページ ([図 1-2](#)) です。このページには、エンドユーザと管理者が Identity Manager で実行する必要がある基本的なタスクを効率化するための複数の領域へのデフォルトのリンクが表示されます。

図1-2 ダッシュボードの「アプリケーション」ページの例



デフォルトでは、[\[ヘルプデスクチケット\]](#)が[\[アプリケーション\]](#)ページに表示されます。このオプションを使用すると、ヘルプデスクにチケットを作成することができます。

Identity 管理者は、ユーザが定期的にアクセスする一般的に要求されるリソースまたはアプリケーションにリンクされているタイルを含むように **[アプリケーション]** ページをカスタマイズします。適切な管理役割を使用して、これらのタイルのユーザアクセスを設定することができます。**[ユーザの ID] > [設定] > [アクセス]** に移動して、必要なナビゲーションアイテムのトラスティを追加します。プロビジョニングアクセスの詳細については、『[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)』の「[Managing User Access](#)」を参照してください。

このページ上のタイルの一部は、Identity アプリケーションの管理役割を持つユーザに対してのみ表示される場合があります。たとえば、役割を作成または変更できる人には、**[ユーザの作成]** および **[役割の管理]** に似ているタイルが表示されます。

ダッシュボードの使用の詳細については、ダッシュボードの②をクリックしてください。

タスクを理解する

[タスク] ページでは、一覧表示されたタスクのアクションを承認または拒否することができます。

Identity Manager ダッシュボードでは、**[タスク]** ページから Identity Manager および Identity Governance のタスクを管理できます。同じユーザインタフェースから Identity Manager のタスクと Identity Governance のタスクの両方を表示および承認できるようになりました。

Identity アプリケーションを使用する一般的な方法

組織内での Identity アプリケーションの一般的な使用例をいくつか示します。

- 14 ページの「[Identity セルフサービスの仕組み](#)」
- 15 ページの「[役割とリソースの仕組み](#)」
- 16 ページの「[プロセス要求の仕組み](#)」
- 16 ページの「[ヘルプデスクの仕組み](#)」

Identity セルフサービスの仕組み

- Ella (エンドユーザ) がログイン時に Identity セルフサービスを使用して、忘れたパスワードを回復する

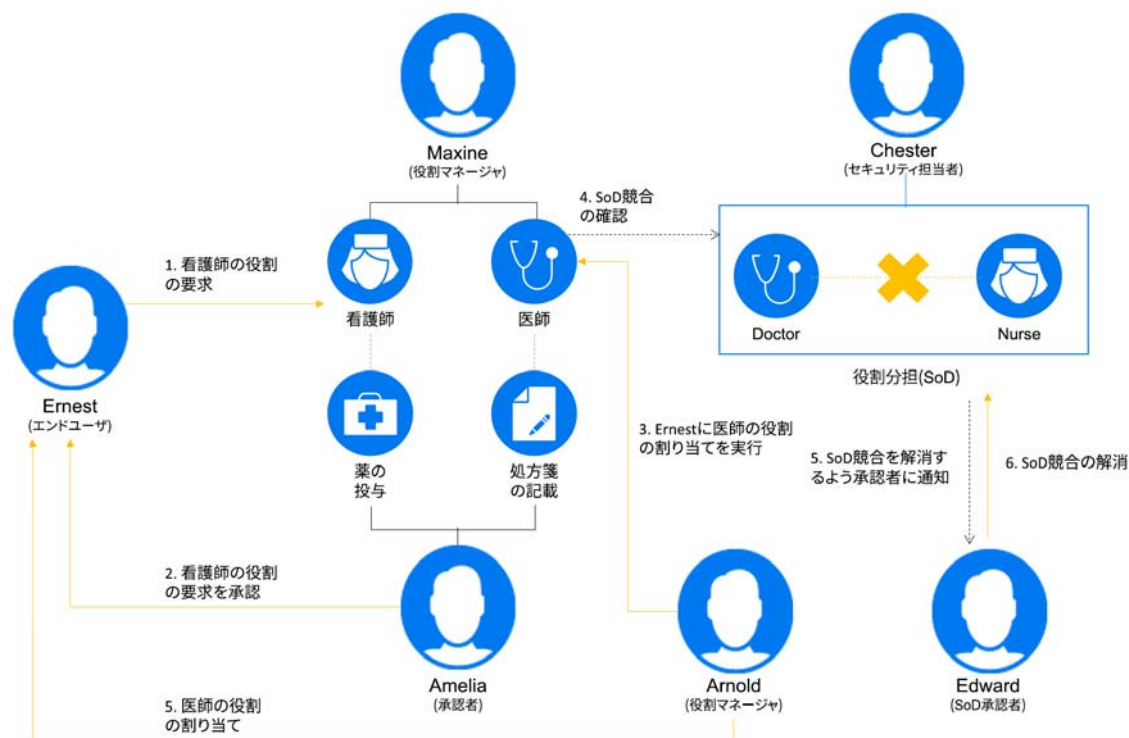
デフォルトでは、ユーザが自分のパスワードを変更できるように、Identity Manager で SSPR (Self Service Password Reset) が使用されます。ただし、パスワードを忘れた場合の対処方法として、他の方法を使用することもできます。

- Erik (エンドユーザ) が、彼の所在地にいてドイツ語を話す従業員すべてを検索する
- Eduardo (エンドユーザ) が組織図を参照して、Ella を検索し、電子メールアイコンをクリックして Ella にメッセージを送信する。

役割とリソースの仕組み

システムにおける役割とリソースの要求の流れを説明する例を以下に示します。

図1-3 役割割り当てのシナリオ例



- Maxine (役割マネージャ) が、「看護師」と「医師」というビジネス役割、および「薬の投与」および「処方箋の記述」という IT 役割を作成する。Maxine はこれらの役割に必要ないくつかのリソースを作成し、これらのリソースを役割に関連付ける。
- Maxine (役割マネージャ) が、看護師および「薬の投与」の役割間の関係を定義して、看護師の役割に「薬の投与」役割が含まれるように指定する。さらに Max が、医師の役割に「処方箋の記述」および医師の役割間の関係を定義して、「処方箋の記述」の役割が含まれるように指定する。
- Chester (セキュリティ責任者) が医師と看護師の役割が競合する可能性があることを示す義務の分離制約を定義する。これは、通常同じユーザに対して両方の役割を同時に割り当てておくべきではないことを意味します。状況によっては、役割割り当てを要求する個人がこの制約を上書きすることもできます。義務の分離の例外を定義するには、割り当てを要求する個人が正当な理由を提供する必要があります。
- Ernest (エンドユーザ) が使用できる役割のリストを参照し、看護師の役割への割り当てを要求する。
- Amelia (承認者) が電子メール (URL が記載されている) で承認要求の通知を受信する。Amy が URL のリンクをクリックすると承認フォームが表示され、Amy は要求を承認する。

- Arnold (役割マネージャ) が、Ernest に医師の役割を割り当てるように要求する。Ernest にすでに割り当てられている医師の役割と看護師の役割が競合する可能性があることが Arnold に通知されます。Arnold は、義務の分離制約の例外を許可してもらうための正当な理由を提供します。
- Edward (義務の分離の承認者) が電子メール経由で義務の分離の競合についての通知を受信する。Edward は、Arnold の義務の分離制約を上書きする要求を承認します。
- Amelia (承認者) が電子メール経由で医師の役割に対する承認要求の通知を受信する。Amelia は、Ernest を医師の役割に割り当てるという Arnold の要求を承認します。
- Bill (役割監査官) が SoD 違反および例外レポートをチェックし、Ernest が「医師」と「看護師」の両方の役割に割り当てられていることを確認する。さらに、彼は Ernest にこれらの役割に関連付けられたリソースが割り当てられていることを確認する。

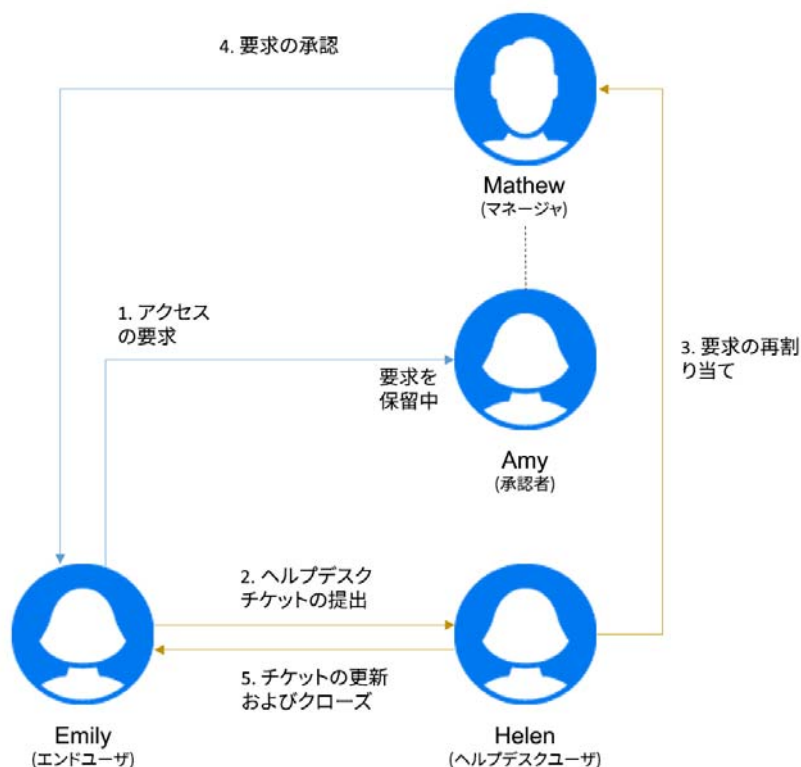
プロセス要求の仕組み

- Ernie (エンドユーザ) が、使用できるリソースの一覧を参照し、Siebel* システムにアクセスできるように要求する。
- Amy (承認者) が電子メール (URL が記載されている) で承認要求「通知」を受信する。Amy が URL のリンクをクリックすると承認フォームが表示され、Amy は要求を承認する。
- Ernie が、以前発行した Siebel システムへのアクセス要求の「ステータス」を確認する (このアクセス要求は、承認を受けるため 2 人目の承認者に転送されている)。その要求がまだ処理中であることがわかる。
- Amy はこれから休暇に入るので、休暇中は「稼働できなくなる」旨を設定する。彼女が不在の間、追加の承認タスクは割り当てられない。
- Amy が自分の承認タスクリストを開く。承認タスクの数が多すぎて、迅速に対応できないことがわかる。そのため Amy は、一部の承認タスクを同僚に再割り当てする。
- Pat (Amy の「代理」ユーザである管理アシスタント) が Amy のタスクリストを開き、Amy の代わりに承認タスクを実行する。
- Max (マネージャ) が「自部署の従業員のタスクリスト」を表示する。Amy が休暇中であることを知っているため、Max は Amy のタスクを部署の他の従業員に再割り当てする。
- Max が部署内の直属の部下に対するデータベースアカウントの要求を開始する。
- Max が Dan を Amy の正式な委任先として割り当てる。
- Dan (委任された承認者) は Amy の休暇中、Amy のタスクを受け持つ。
- Max が無給のインターンを雇う。このインターンは人事システムに登録すべきでない。システム管理者がこのインターンのユーザレコードを作成し、Notes、Active Directory、および Oracle へのアクセスをこのインターンに許可するよう要求する。

ヘルプデスクの仕組み

システムにおけるヘルプデスクチケットの流れを説明する例を以下に示します。

図1-4 ヘルプデスクの例



- Emily (エンドユーザ) が、オフィスプリンタへのアクセスを要求しました。この要求は長い間保留中になっていました。このため、彼女はヘルプデスクチケットを作成しました。
- Helen (ヘルプデスクユーザ) は、彼女のタスクリストでヘルプデスクチケットの通知を受け取ります。
- Helen は問題を分析し、要求が Amy (承認者) に割り当てられていることを知ります。
- この要求は、Amy が外出しているため、システムで保留中になっています。
- Helen はタスク要求を再割り当てする許可を持っています。彼女はこの要求を Mathew (Amy のマネージャ) に再割り当てします。
- Mathew は要求をレビューして承認します。Emily はオフィスプリンタにアクセスできます。
- Helen はヘルプデスクチケットを更新して閉じます。

2 Identity アプリケーションへのアクセス

ダッシュボードなどの Identity アプリケーションには、Web ブラウザでアクセスします。Identity Manager は代表的な Web ブラウザのほとんどをサポートしています。サポート対象 Web ブラウザの種類、および Web ブラウザのインストールについては、システム管理者にお問い合わせください。アプリケーションへのアクセスに必要な URL と資格情報は、組織から提供されます。

- [19 ページの「Identity アプリケーションにアクセスする際の考慮事項」](#)
- [20 ページの「初めてログインする」](#)
- [22 ページの「優先するロケールのチェックに対応」](#)
- [22 ページの「ログインの問題のトラブルシューティング」](#)
- [23 ページの「ログアウト」](#)

Identity アプリケーションにアクセスする際の考慮事項

ダッシュボードなどの Identity アプリケーションにアクセスする前に、以下の考慮事項を確認してください。

- Web ブラウザでクッキーと JavaScript* を有効にする必要があります。
- Internet Explorer を使用するとき、プライバシーレベルを少なくとも [中] に設定する必要があります。[ツール] > [インターネットオプション] > [全般]、[閲覧の履歴] > [設定] > [保存しているページの新しいバージョンの確認] の下の [Web サイトを表示するたびに確認する] オプションも選択する必要があります。このオプションを選択しておかないと、ボタンが正しく表示されない場合があります。
- Identity Manager ユーザアプリケーションにアクセスしたことがある場合は、同じユーザ名とパスワードを使用してダッシュボードにアクセスできる可能性があります。
- 次のいずれかの文字が名前に含まれているアカウントを使用して Identity アプリケーションにアクセスすることはできません。
\\ / , * ? . \$ # +
- ログインできない場合は、[パスワードを忘れた場合] をクリックしてください。詳細については、[22 ページの「パスワードを忘れた場合」](#)を参照してください。

- ♦ Identity Manager ユーザインタフェースにアクセスしたときに、この図と異なるページが表示された場合、それは、所属組織において Identity Manager がカスタマイズされているからです。また、作業を進めるにつれて、Identity アプリケーションの他の機能もカスタマイズされている場合があります。

この場合、システム管理者に連絡して、カスタマイズされたアイデンティティアプリケーションとこのマニュアルで説明されているデフォルトの設定がどのように異なっているかを確認してください。

初めてログインする

ダッシュボードなどの Identity アプリケーションにログインするには、認定されたユーザである必要があります。ログインに必要なユーザ名とパスワードを取得する必要がある場合は、システム管理者に連絡してください。

初めて Identity アプリケーションにログインするときに、Identity Manager で、将来パスワードのリセットに役立つ、アカウントのセキュリティパラメータを設定する必要があります。パスワードを忘れた場合、次のログイン時にパスワードをリセットしようとする、これらの設定済みの質問が Identity Manager によって表示され、正しい回答を指定するよう求められます。入力した回答がこのページで保存した回答と一致した場合、パスワードをリセットできます。

最初にログインするときにセキュリティの質問を設定するには：

- 1 ユーザ名とパスワードを入力し、[**ログイン**] をクリックします。
- 2 ログインページから [**本人確認の回答**] ページに自動的にリダイレクトされます。
- 3 セキュリティの質問に対する質問と答えを指定します。

セキュリティ質問のセットアップ

[ログアウト](#)

パスワードを忘れた場合は、セキュリティ質問に回答することによって、アカウントにアクセスできるようになります。

パスワードを忘れた場合の本人確認に使用する質問と回答を選択してください。これらの質問に対する回答はアカウントへのアクセスに使用できるため、他の人に簡単に推測されたり見つけられない回答を入力してください。

セキュリティ回答を入力してください

— リストから質問項目を選択してください —



— リストから質問項目を選択してください —



— リストから質問項目を選択してください —



— リストから質問項目を選択してください —



▶▶ 回答の保存

◀◀ キャンセル

- 4 [Save Answers (答えの保存)] をクリックすると、ダッシュボードにリダイレクトされます。

優先するロケールのチェックに対応

ログインしたときに独自の優先するロケールを選択するように求められた場合、管理者が Identity アプリケーションに対して行った設定に従って、ユーザのブラウザで言語チェックが実行されます。これは、参照する内容がサポートされている言語で表示されることを確認するために必要になる場合があります。

ロケールを追加するように求められた場合は、[\[Available Locales \(使用可能なロケール \)\]](#) リストを開き、ロケールを選択して、[\[追加 \]](#) をクリックします。詳細については、「[Identity アプリケーションへの新しい言語の追加](#)」を参照してください。

ログインの問題のトラブルシューティング

この項では、以下のタイプの共通のログインの問題に対するソリューションを示します。

- [22 ページの「パスワードを忘れた場合」](#)
- [22 ページの「ログイン処理で問題が発生した場合」](#)
- [23 ページの「追加情報の入力を求められた場合」](#)

パスワードを忘れた場合

パスワードを忘れてしまった場合は、[\[パスワードを忘れた場合 \]](#) リンクを使用できます。ログインページには、このリンクがデフォルトで表示されます。このリンクを使用できるのは、自分に関する「パスワードポリシー」がシステム管理者によって適切に設定されている場合です。

- 1 ログインページで [\[パスワードを忘れた場合 \]](#) リンクをクリックします。
- 2 ユーザ名を入力し、[\[送信 \]](#) をクリックします。

Identity Manager から、自分のパスワードポリシーが見つからないという応答があった場合は、システム管理者にサポートを依頼してください。

- 3 表示される本人確認の質問に回答します。Identity Manager により、設定した質問に回答するよう求められます。入力した回答が事前に保存した回答と一致した場合、パスワードをリセットできます。[\[送信 \]](#) をクリックします。次に例を示します。

本人確認の質問に回答して、パスワードのヘルプを利用します。システム管理者がパスワードポリシーをどのように設定しているかに応じて、次の処理が実行されます。

- パスワードが記載された電子メールを受信する
- パスワードをリセットするようプロンプトが表示される

ログイン処理で問題が発生した場合

ログインできない場合、ユーザ名とパスワードを正しく入力していることを確認してください (スペル、大文字または小文字など)。それでも問題が解決しない場合は、システム管理者にお問い合わせください。その際、発生している問題の詳細 (エラーメッセージなど) を報告すると、問題の解決に役立ちます。

追加情報の入力を求められた場合

ログインするとすぐに、その他の情報の入力を求められることがあります。追加情報の種類は、自分に関するパスワードポリシーがシステム管理者によってどのように設定されているかによって異なります。たとえば、次のような指定内容です。

- 初回ログインの場合、本人確認の質問と回答を定義するよう求められます
- パスワードの期限が切れている場合は、パスワードをリセットするよう求められます

ログアウト

ダッシュボードおよびその他の Identity アプリケーションでの作業を終了したら、ログアウトする必要があります。ダッシュボードの右上隅のユーザ名をクリックして、[サインアウト]を選択します。



ダッシュボードのカスタマイズ

Identity Applications には、「ダッシュボード」の表示を変更し、それをパーソナライズされたビューに保存するための多数のオプションが用意されています。たとえば、ウィジェットを追加して、自分の興味に基づいてそれらを再配置することができます。ウィジェットフィールドを設定して、それらをパーソナライズすることもできます。このドキュメントは、「ダッシュボード」をパーソナライズするためのさまざまなオプションを理解するのに役立ちます。

3 ウィジェットとレイアウトの管理

ウィジェットは、特定のアクティビティに対するユーザ固有の詳細を提供するために設計されたダッシュボードオブジェクトです。たとえば、[タスク] ウィジェットでは、新しいタスク、要求されたタスク、またはまもなく期限切れになる予定のタスクに関する詳細が提供されます。同様に、ダッシュボードで他の多数のウィジェットを設定することができます。

[設定] ページにアクセスできる管理者は、[ユーザの ID] > [設定] > [ダッシュボードウィジェット] で、ユーザ、グループ、コンテナ、または役割用のウィジェットをプロビジョニングすることができます。

ダッシュボードをパーソナライズするには、[ダッシュボード] に移動し、 をクリックします。

図3-1 ダッシュボードのパーソナライズ



ダッシュボードをパーソナライズするには、次のオプションを使用します。

図3-2 パーソナライズのオプション



ウィジェット

ダッシュボードにウィジェットを追加できます。詳細については、「[29 ページの「ウィジェットの追加」](#)」を参照してください。

レイアウト

ダッシュボードレイアウトを変更できます。詳細については、「[28 ページの「ダッシュボードレイアウトの変更」](#)」を参照してください。

キャンセル

ダッシュボードに行われたすべての変更をキャンセルします。

保存

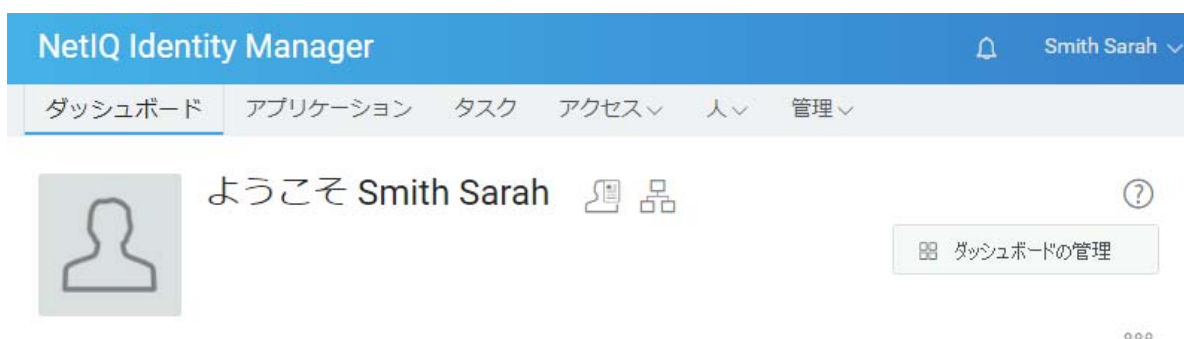
ダッシュボードに変更を保存して適用します。

グローバルダッシュボードの管理

グローバルダッシュボードには、システム内のすべてのユーザのダッシュボードに表示される一連のウィジェットが含まれています。ユーザは、管理者によってプロビジョニングされたアクセス権に基づいてこれらのウィジェットを表示できます。**[Manage Dashboard (ダッシュボードの管理)]** オプションを使用すると、グローバルダッシュボードのウィジェットを追加、変更、または削除できます。

注： **[Manage Dashboard (ダッシュボードの管理)]** オプションを使用するユーザは、トラスティとして追加されている必要があります。

図3-3 グローバルダッシュボードの例



管理者は、任意のユーザ、グループ、コンテナ、または役割を、グローバルダッシュボードを管理するトラスティとして追加できます。ダッシュボードを管理するトラスティを変更するには、**[YourID (自身の ID)] > [設定] > [アクセス]** に移動して、リストから **[Global Dashboard (グローバルダッシュボード)]** をクリックします。設定アクセスの変更に関する詳細については、『*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*』の「**Managing Dashboard Widgets**」を参照してください。

ダッシュボードレイアウトの変更

Identity Applications では、ダッシュボード上のウィジェットの外観レイアウトを変更できます。

- 1 **[ダッシュボード]** で **...** をクリックします。
- 2 **[レイアウト]** を選択します。
- 3 ダッシュボードに表示するレイアウトを選択します。

図3-4 レイアウトの変更

ダッシュボードの編集 ×

タイトル

ダッシュボード

構造

6-6

4-8

12/4-4-4

12/6-6

12/6-6/12

3-9 (12/6-6)

重要: 変更を適用するには、[保存] をクリックします。

ウィジェットの追加

ダッシュボードに新しいウィジェットを追加するには、[ダッシュボード] に移動し、**...** をクリックして、[**ウィジェット**] を選択します。

図3-5 ウィジェットの追加

新しいウィジェットの追加 ×

一般

IDM

IG

全般ウィジェットの追加

[一般] カテゴリでは、ダッシュボードに Identity Manager 標準ウィジェット以外のウィジェットを追加できます。必要なウィジェットの REST API URL を指定し、必要な情報を折れ線グラフ、円グラフ、またはテーブルチャートの形式で表示できます。

- 1 リストから次のいずれかのウィジェットタイプを選択します。
 - ◆ **線グラフ**: 選択した要素の要求された情報を折れ線グラフの形式で表示します。
 - ◆ **リンク**: 頻繁に使用されるリンクをブックマークして、迅速にアクセスできるようにします。
 - ◆ **円グラフ**: 選択した要素の要求された情報を円グラフの形式で表示します。
 - ◆ **テーブル**: 選択した要素の要求された情報をテーブル形式で一覧表示します。
- 2  をクリックして、ダッシュボードに追加されたウィジェットを設定します。
- 3 (条件付き) **[線グラフ]**、**[円グラフ]**、および **[テーブル]** ウィジェットについては、次の詳細を指定します。
 - ◆ **タイトル**: ダッシュボードに表示するウィジェット名を指定します。
 - ◆ **URL**: ダッシュボードに表示する必要なウィジェットの REST API URL を指定します。
 - ◆ **ルート要素**: チャートを表示する REST API コードの要素を指定します。このフィールドでは、大文字と小文字が区別されます。REST API コードで記述されているのとまったく同じ名前を入力する必要があります。
 - ◆ **列**: ウィジェットに表示するカラムを指定します。複数のカラムを追加できます。**[タイトル]** は、カラムの表示名を指定します。**[パス]** は、REST API で記述されているカラム名を指定します。**[パス]** フィールドでは、大文字と小文字が区別されます。REST API コードから、まったく同じ文字列を入力する必要があります。

[役割] ページのサンプル REST API コードを次に示します。

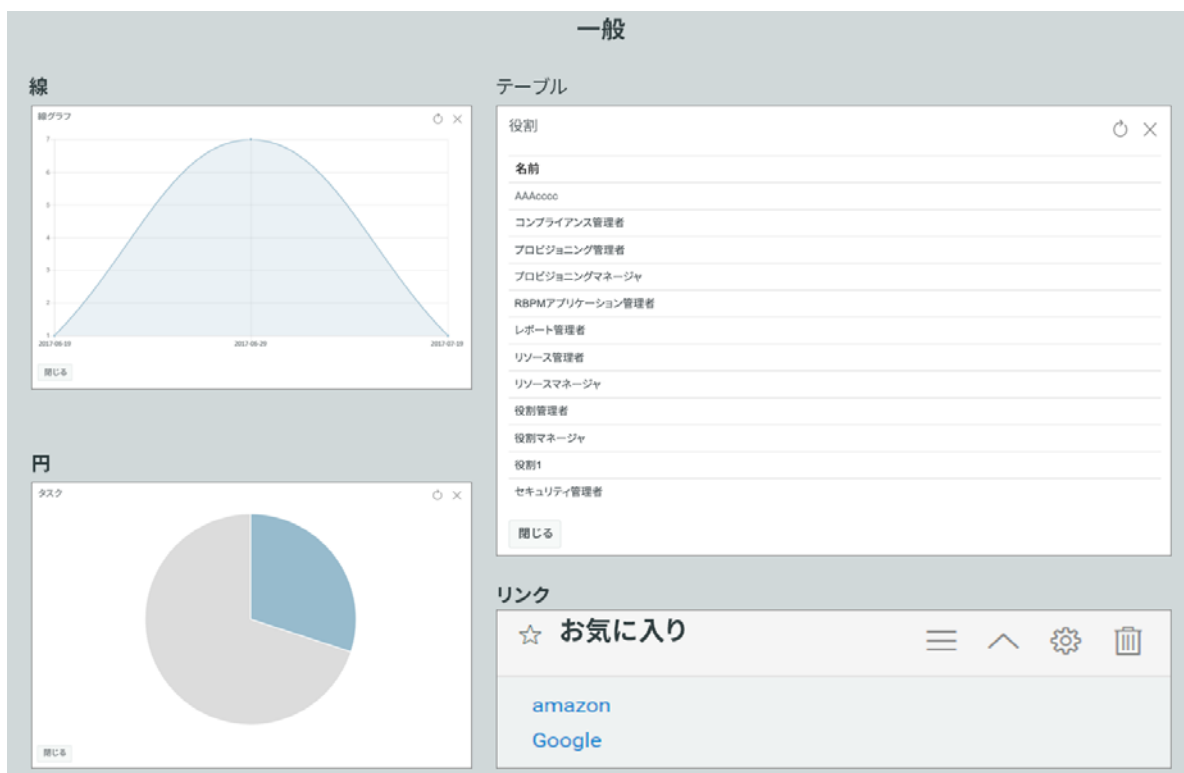
```
{
  "total": 12,
  "nextIndex": 0,
  "token": "60045d6be10f4419a2da9fa728683b06",
  "assignments": [
    {
      "id":
      "cn=aaacccc,cn=level30,cn=roledefs,cn=roleconfig,cn=appconfig,cn=user
      application driver,cn=driverset1,o=system",
      "name": "AAAcxxx",
      "description": "afasfdsf",
      "entityType": "role",
      "link": "/IDMProv/rest/access/assignments/item",
      "bulkRemovable": "true",
      "categories": [
        {
          "categoryId": "default",
          "categoryName": "Default"
        }
      ]
    }
  ]
}
```

このサンプルでは、割り当てはルート要素で、名前は表示用に選択されたカラムで、ウィジェットに表示されます。ダッシュボードからアクセスする URL をブックマークすることもできます。

- 4 (条件付き) [リンク] ウィジェットの場合は、リンクの [タイトル] を指定して、ダッシュボードからアクセスするリンクを追加します。
- 5 [保存] をクリックして、変更を適用します。

ダッシュボードに追加可能なサンプルチャートとリンクウィジェットを次に示します。

図3-6 全般ウィジェットの例



Identity Manager のウィジェットの追加

[IDM] カテゴリでは、標準の Identity Manager ウィジェットをダッシュボードに追加できます。

次に例を示します。

- **アクセス:** 役割とリソースの数、およびそれらに関するその他の情報を表示します。
- **その他の要求:** 他のユーザの保留中の要求と拒否された要求の数を表示し、これらのユーザの要求を作成することができます。
- **セルフ要求:** 保留中の要求と拒否された要求の数を表示し、新しい要求を作成することもできます。
- **タスク:** 新規または保留中のタスク、あるいは期限切れが近いタスクの数を表示します。

これらのウィジェットを設定するには、[33 ページの「ウィジェットの設定」](#)を参照してください。

重要: 変更を適用するには、[保存] をクリックします。

Identity Governance のウィジェットの追加

Identity Governance のウィジェットを使用するには、Identity Governance を Identity Manager ダッシュボードと組み合わせてインストールおよび設定する必要があります。

[IG カテゴリでは、標準の Identity Governance ウィジェットをダッシュボードに追加できます。] 次に例を示します。

フルフィルメントタスク

システム内のアクセス要求、ビジネス役割、および許可の割り当てエラーの数が表示されます。

レビュータスク

システム内の保留中レビューと完了済みレビューの数が表示されます。

SoD 違反

システム内の未レビュー、承認済み、または解決中の SoD 違反の数が表示されます。

ウィジェットのオプション

ウィジェットに対して次の操作を実行できます。



更新

ウィジェットのコンテンツを最新の情報で更新します。

再配置

ダッシュボード全体にウィジェットを移動することができます。

設定

ウィジェットのプロパティを設定できます。詳細については、「[33 ページの「ウィジェットの設定」](#)」を参照してください。

削除

ダッシュボードからウィジェットを削除します。

縮小

ウィジェットの情報を非表示にし、ウィジェットのタイトルのみを表示します。

ウィジェットを全画面で開く

全画面モードでウィジェット情報を表示します。

注

- [リフレッシュ]および[ウィジェットを全画面で開く]オプションは、[一般]カテゴリに属するウィジェットに対してのみ表示されます。
 - 変更を適用するには、[保存]をクリックします。
-

ウィジェットの設定

ダッシュボードに追加される各ウィジェットを設定できます。たとえば、ウィジェットのフィールドを有効または無効にしたり、フィールドの表示色を変更することができます。

- 1 設定するウィジェットで⚙️をクリックします。
- 2 ウィジェットのプロパティを変更します。
たとえば、ウィジェットのタイトルを変更したり、ウィジェットフィールドのラベルの色を変更することができます。プロパティページで、ウィジェットフィールドを有効または無効にすることもできます。
- 3 ダッシュボードで変更を表示するには、[適用]をクリックします。

たとえば、次のようにタスクウィジェットを変更できます。

図3-7 ウィジェット設定の例

タスク

×

タイトル

Tasks

新規タスク

☒

■

▼

間もなく期限切れ

☒

■

▼

引き受け済み

☒

■

▼

委任済みタスク

☐

■

▼

再割り当て済みタスク

☐

■

▼

適用

キャンセル

ダッシュボードで変更を表示するには、[適用] をクリックします。

タスク

▲

新規タスク

0

間もなく期限切れ

0

引き受け済み

0

合計タスク: 0

全般ウィジェットを設定するには、ウィジェットの追加中に表示されるオプションを変更します。詳細については、[30 ページの「全般ウィジェットの追加」](#)を参照してください。

重要: 変更を適用するには、[保存] をクリックします。



許可および Identity プロファイルの管理

Identity Manager ダッシュボードは、日常のタスクを完了させるために必要なリソースと役割へのアクセス権を要求するのに役立ちます。アクセス権に対する要求の承認など、Identity Manager 環境で割り当てられたタスクを実行することもできます。リソースと役割の所有者はプロセスを管理できます。

許可を要求すると、Identity Manager は、必要な役割またはリソースを保持できるように、要求を効率的にレビューするプロセスを開始します。マネージャは、電子メールまたはダッシュボードで通知を受け取り、要求をレビューします。場合によっては、要求を組織の他の個人が承認することもあります。

一部のユーザは、他のユーザの代わりに要求を行ったり、別のユーザの代理になることもできます。

- ◆ [37 ページの第 4 章「許可要求の管理」](#)
- ◆ [45 ページの第 5 章「アプリケーションの管理」](#)
- ◆ [49 ページの第 6 章「自分のタスクの管理」](#)
- ◆ [53 ページの第 7 章「他の人の代わりに実行する」](#)
- ◆ [55 ページの第 8 章「委任の管理」](#)
- ◆ [57 ページの第 9 章「可用性の管理」](#)
- ◆ [59 ページの第 10 章「プロファイルの管理」](#)
- ◆ [61 ページの第 11 章「組織図の管理」](#)
- ◆ [69 ページの第 12 章「パスワードの管理」](#)

4 許可要求の管理

このセクションでは、次の操作の方法について説明します。

- ◆ 37 ページの「許可の表示」
- ◆ 39 ページの「許可の要求」
- ◆ 39 ページの「要求の表示」
- ◆ 41 ページの「許可の取り消し」
- ◆ 42 ページの「要求へのディープリンク」

これらのアクティビティに関するダッシュボードの情報について①を確認できます。

許可の表示

許可とは、使用可能なアカウント、役割、またはリソースを表します。許可は、組織によって自動的に割り当てられる場合もあれば、特定の許可を要求することもできます。役割の関係を使用して一部の許可を間接的に継承することもできます。またはグループまたはコンテナのメンバーである場合にも継承できます。

アクセス権のある役割またはリソースを表示するには、ダッシュボードで以下を選択します。

[アクセス] > [許可]

次に、その役割またはリソースの詳細に対して特定の許可を選択することができます。この許可によって、許可の割り当てに関して示された理由を一覧表示することもできます。大きいリストで特定の許可を見つけるには、検索ボックスに許可の名前、CN、または説明を入力します。リストをフィルタ処理することもできます。

注：

- ◆ デフォルトでは、直接割り当て済みまたは承認済みの許可を一覧表示できます。ただし、管理者がページをどのように設定したかによって異なる場合があります。詳細については、『*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*』の「User Settings」を参照してください。
 - ◆ 割り当て済みまたは承認済みの許可にマップされた子許可を表示するには、🔍をクリックします。
-

許可の詳細の表示

詳細を表示する許可を選択します。個々の許可に対して表示されるフィールドを次の表に一覧表示します。

表 4-1 許可フィールドとその説明

フィールド	説明
説明	役割またはリソースの説明
有効開始日	許可割り当ての日時
有効期限日	許可がユーザに割り当てられる最終日。有効期限オプションが有効になっている許可の有効期限日のみが表示されます。
理由	許可をユーザに割り当てる理由を指定します。
許可の割り当て	許可をユーザに割り当てた人を指定します。 承認プロセスを使用して役割がユーザに直接割り当てられる場合、[役割承認情報を表示する] オプションの下で割り当て要求を承認した承認者を一覧表示できます。 メンバーシップを使用してユーザによって役割がグループまたはコンテナに継承される場合、[役割からグループへの割り当て情報を表示する] オプションの下に次の詳細が表示されます。 • 「要求者」：許可を要求した人を指定します。 • 「要求の説明」：許可を要求したときに記入した説明 • 「承認者の詳細」：リンクをクリックすると、役割の割り当て要求を承認した承認者のリストが表示されます。

Identity Applications 管理者は、[\[その他 \]](#) タブで他のチームメンバーの許可を表示することができます。[\[その他 \]](#) タブに移動して、ユーザ名または許可の詳細で検索します。

- ユーザで検索すると、そのユーザに割り当てられているすべての許可が一覧表示されます。次に、特定の許可を選択して、割り当てられた日付、許可を割り当てたユーザ、許可の割り当てに何らかの理由が提供されているかどうかなどの詳細を確認できます。詳細については、[38 ページの表 4-1](#) を参照してください。
- 許可で検索すると、その許可に割り当てられている、すべてのユーザ、個人、およびグループまたはコンテナに存在するユーザが一覧表示されます。

注：許可の詳細による検索は、チームマネージャまたはスーパーバイザユーザにはサポートされていません。ただし、チーム名または説明を検索することによってチームメンバーの許可を表示できます。また、このページにはユーザ名による検索も用意されていて、特定のチームメンバーの許可を検索および表示できます。

詳細については、ダッシュボードの①をクリックしてください。

許可の要求

役割とリソースを要求するには、[[アクセス](#)] > [[要求](#)] をクリックします。

許可を要求する前に、以下の考慮事項を確認してください。

- 別のユーザの代わりにアクセスを要求することも可能です。たとえば、チームマネージャは通常、チームメンバーの代わりに務めることができます。要求を [[自己](#)] ではなく [[その他](#)] に関して指定する必要があることを除き、プロセスは同じです。
- 要求する許可を指定するときに句読点を使用しないでください。要求する許可の名前に句読点が含まれる場合は、検索時に句読点を除外します。
- 管理者による許可フォームの設定に応じて、許可ごとに異なる情報が必要になります。許可に詳細情報が必要になる場合は、許可を選択するときにダッシュボードから別個のウィンドウにリダイレクトされます。
- 同時に複数の許可を要求することができます。

ただし、要求のいずれかに対する許可フォームで、特殊なタイプの情報が必要になる場合は、複数の許可要求にその許可を含めることができないことがあります。一度に複数の許可を要求する場合、さまざまな要求に対する要求フォームで、詳細情報を必須にすることはできません。

- リソースまたは役割を要求する際に終了日を指定できます。

Identity Governance の許可を要求するには：

次の 2 つの条件、すなわち、[[環境設定](#)] > [[Identity Governance](#)] ページで [[Show IG Catalog in request page](#) ([[要求](#)] ページに [IG カタログを表示する](#))] オプションを有効にしている場合、および [[自己](#)] に対して許可を要求する場合にのみ適用されます。

- **IDM Catalogs (IDM カタログ)**: 使用可能な Identity Manager 役割、リソース、およびワークフローをすべて一覧表示します。
- **IG Applications (IG アプリケーション)**: Identity Governance で収集されたすべてのアプリケーションを一覧表示します。その後、選択したアプリケーションに関連付けられた許可を選択できます。
- **IG Technical Roles (IG テクニカルロール)**: Identity Governance のすべてのテクニカルロールを一覧表示します。要求したい IG 役割を選択し、役割を要求する理由を指定します。

詳細については、ダッシュボードの ① をクリックしてください。

要求の表示

進行中の要求および完了した要求のステータスを表示するには、ダッシュボードで以下を選択します。

[[アクセス](#)] > [[要求履歴](#)]

チームマネージャまたはスーパーバイザは、[[その他](#)] タブで他のチームメンバーの要求履歴を表示することができます。

保留中の要求については、ヘルプデスクチケットを作成することもできます。

- ◆ 40 ページの「要求の追跡」
- ◆ 40 ページの「要求のキャンセル」
- ◆ 41 ページの「ヘルプデスクチケットの作成」

詳細については、ダッシュボードの①をクリックしてください。

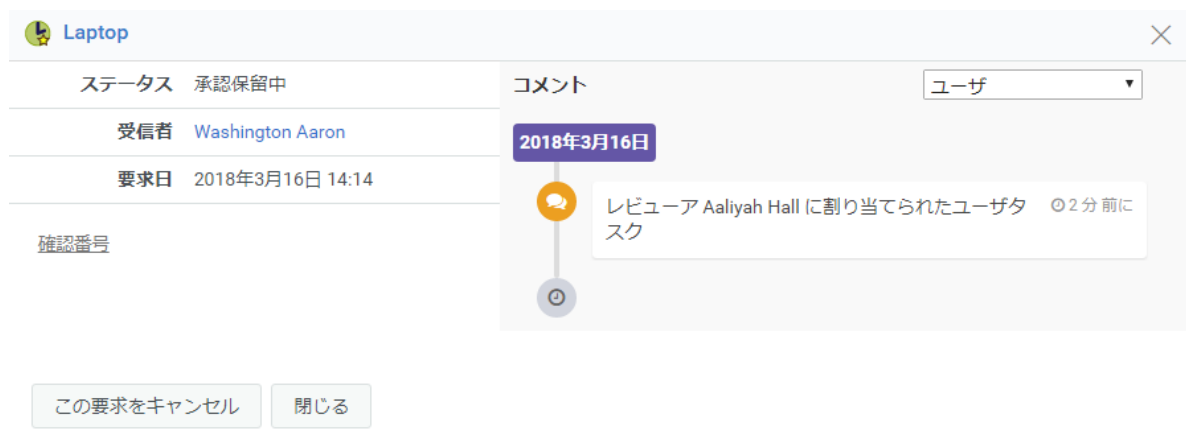
要求の追跡

要求ごとに、アクションだけでなく、要求の承認または拒否に関係するワークフローも表示することができます。プロセス内の各ステップにタイムスタンプがあります。

注：[IG アプリケーション] または [IG テクニカルロール] タブからアプリケーションまたはテクニカルロールを要求する場合、[要求履歴] ページから追跡することはできません。IG 要求を追跡するには、ダッシュボードの[アプリケーション] ページから IG 履歴の URL を追加できます。

保留中の要求を追跡するには、要求を選択して、右上のメニューを[ユーザおよびシステム]に変更します。ダッシュボードに、承認プロセスにある要求の現在の状態が表示されます。

図4-1 要求の追跡



要求のキャンセル

[要求履歴] から「保留中」の要求をキャンセルすることができます。リストで要求を選択し、続いて表示されるウィンドウで[この要求をキャンセル]を選択します。

ヘルプデスクチケットの作成

長期間放置されたままになっている要求に関するヘルプを希望している場合は、ヘルプデスクに問い合わせることができます。

次の場所でヘルプデスクチケットを作成することができます。

- [アクセス]>[要求]で、[ヘルプデスクチケット]をクリックします。
- [アプリケーション]で、[ヘルプデスクチケット]をクリックします。
- [アクセス]>[要求履歴]で、ヘルプデスクチケットを作成する要求の①をクリックします。

詳細については、ダッシュボードの②をクリックしてください。

ヘルプデスクメンバーは、ヘルプデスクチケットに関する通知を受け取ります。チケットが解決または閉じられると、チケットの通知が届きます。

許可の取り消し

役割またはリソースにアクセスする必要がなくなった場合は、その役割またはリソースへの許可を取り消すことができます。許可を取り消すには、[アクセス]>[許可]の順に移動し、必要な許可を選択して、許可を取り消す理由を指定します。

他のユーザの代わりに許可を取り消すこともできます。たとえば、チームメンバーが部署1から部署2に異動し、そのチームメンバーが特定のリソースにアクセスする必要がなくなった場合、Identity Managerはそのユーザの許可を取り消す機能を提供します。許可を取り消すには、[その他]を選択して許可を削除します。一度に複数の許可を取り消すことができます。取り消しを決定する前に、これらの許可をキューに追加してレビューすることができます。

他のユーザの許可を取り消すことができるのは、管理者とチームマネージャだけです。管理者は組織内の全ユーザの許可を取り消すことができますが、チームマネージャはチームメンバーの許可のみを取り消すことができます。

次の方法で他のユーザの許可を取り消すことができます。



- **ユーザで検索** : ユーザを検索し、そのユーザの許可を取り消すことができます。ユーザの許可を直接取り消したり、キューに許可を追加することができます。キューは、許可を一時的に格納することができる永続的な作業領域です。格納した許可は、必要

に応じてレビューしたり、取り消したりすることができます。その後、そのユーザから取り消す他の許可を検索し、キューに追加することができます。これにより、一度にすべての許可を取り消すことができます。

- ◆ **許可で検索** : 特定の許可を検索することができます。許可を選択すると、その許可を持つすべてのユーザが一覧表示されます。選択したユーザの許可を直接取り消したり、この許可をキューに追加して、複数のユーザからその許可を一度に取り消すことができます。

チームマネージャ : チームマネージャは、[**その他**] タブでチームメンバーの許可を取り消すことができます。チームマネージャは、他のメンバーの許可を取り消すための必要な許可を持っている必要があります。

管理者 : 管理者は、チームマネージャに取り消し許可を追加できます。たとえば、チームマネージャに、「ユーザから役割を取り消す」許可を追加するには、[**人**] > [**チーム**] に移動して、チームの許可を編集して、チームマネージャの取り消し許可を有効にします。

図 4-2 チームマネージャの取り消し許可を追加する例



このオプションを使用すると、チームマネージャは、選択した役割をチームメンバーから取り消すことができます。

注 : 許可を取り消した場合、許可リストにすぐに変更が反映されないことがあります。この理由として、その許可が、時間のかかる取り消しプロセスに関連付けられていることが考えられます。この場合は、リストを更新して変更を表示してください。

詳細については、ダッシュボードの②をクリックしてください。

要求へのディープリंक

Identity Applications では、特定のプロセス要求 (プロビジョニング要求とも呼ばれます) にディープリंकすることができます。この機能により、マネージャは特定のプロセス要求 URL を従業員に送信できるので、この従業員は Identity Manager ダッシュボードを使用することなくプロセスを迅速に要求できます。プロセス要求にディープリंकすると、Identity Applications のヘッダとともに、要求フォームがページの本文に表示されます。

許可が要求されると、要求はリクエストの [**アクセス**] > [**要求履歴**] ページに表示され、レビューアの [**タスク**] ページにも表示されます。

プロセス要求へのディープリंकに使用される URL は、次の形式を使用します。

- ◆ レガシフォームの場合 :

```
https://<server:port>/IDMProv/  
requestForm.do?uid=<PRD_ID>&aqua=true&idmdash=true&recipient=<recipient>&jsa=<operation_type>
```

プロビジョニング要求定義へのディープリンクに使用する URL の内容の例を次に示します。

```
https://testserver:8543/IDMProv/requestForm.do?uid=cn=request mobile approval app,cn=requestdefs,cn=appconfig,cn=user application driver,cn=driverset1,o=system&aqua=true&idmdash=true&recipient=&jsa=%7B%22submit%22%3A%22submitThenOpener%283000%29%22%2C%22cancel%22%3A%22window.close%28%29%22%7D
```

- ◆ 新しい JSON フォームの場合 :

```
https://<server:form_renderer_port>/forms/#/form/details?id=<formID>&recipient=<recipient>&pid=<workflowID>&sid=IDM&uri=<forms_uri>&formContainer=RequestForms&locale=<language>
```

プロビジョニング要求定義へのディープリンクに使用する URL の内容の例を次に示します。

```
https://testserver:18600/forms/#/form/details?id=cn%3DHelp-desk%20Request%20Form,cn%3DWorkflowForms,cn%3Dappconfig,cn%3DUser%20Application%20Driver,cn%3Ddriverset1,o%3Dsystem&recipient=&pid=cn%3Dhelpdeskticket,cn%3Drequestdefs,cn%3Dappconfig,cn%3Duser%20application%20driver,cn%3Ddriverset1,o%3Dsystem&sid=IDM&uri=%2Frest%2Faccess%2Fforms&formContainer=RequestForms&locale=en
```


5 アプリケーションの管理

Identity Applications の管理者として、[アプリケーション] ページを変更して、ユーザにアクセスさせるすべてのアプリケーション、アクティビティ、および許可を表示することができます。Identity Applications には、デフォルトで [ホーム項目] カテゴリが用意されており、これは削除できません。

変更した後に [アプリケーション] に戻るには、[編集完了] をクリックします。

おすすめ項目の作成

任意の数のアプリケーションと許可を作成して、[アプリケーション] ページに追加できます。これらの項目を [ホーム項目] または他の [アプリケーション] カテゴリに追加する必要はありません。

- 1 (条件付き) 新しい項目を作成するには、[アプリケーション] または [許可] タブの [+] をクリックします。
- 2 アプリケーションまたは許可のフォームに入力します。45 ページの「アプリケーションの追加」または 46 ページの「許可の追加」を参照してください。

注: アプリケーションの名前や説明など、アスタリスク (*) の付いたすべてのフィールドに値を指定する必要があります。

- 3 (オプション) 新しいアプリケーションまたは許可をカテゴリにドラッグアンドドロップします。
- 4 (条件付き) 既存の項目を変更するには、タイル内の編集アイコンを選択し、値を更新します。

アプリケーションの追加

アプリケーションを追加するには、次の詳細を指定します。

(条件付き) カテゴリに追加

このアプリケーションのカテゴリを指定します。

名前

アプリケーションの名前を指定します。

説明

アプリケーションの性質を指定します。

(オプション) イメージ

アプリケーションのロゴまたはイメージを指定します。

リンク

このアプリケーションのリンクを指定します。[42 ページの「要求へのディープリンク」](#)を参照してください。

(オプション) API URL

パラメータの値やバッジなどの追加の詳細を提供する JSON データを使用して、REST エンドポイントの URL を指定します。詳細については、マニュアルを参照してください。

許可の追加

許可を追加するには、次の詳細を指定します。

権限

許可を指定します。役割、リソース、または PRD を指定できます。

(条件付き) カテゴリに追加

このアプリケーションのカテゴリを指定します。

(オプション) イメージ

アプリケーションのロゴまたはイメージを指定します。

カテゴリの追加、変更、または削除

[アプリケーション] 項目を論理カテゴリに編成できます。組織で必要になると考えられるカテゴリをいくつでも作成できます。カテゴリ内のタイルを再配置したり、別のカテゴリにタイルを移動したりすることもできます。

カテゴリの追加

- 1 [新規カテゴリ] を選択します。

カテゴリがカテゴリグループの最後に追加されます。追加されたカテゴリを表示するには、下にスクロールする必要がある場合があります。

- 2 新しいカテゴリの名前を指定します。
- 3 [+] をクリックして、[アプリケーション] または [許可] を選択します。
- 4 アプリケーションまたは許可のフォームに入力します。

注: アプリケーションの名前や説明など、アスタリスク (*) の付いたすべてのフィールドに値を指定する必要があります。

- 5 [追加](+) を選択します。

カテゴリの変更

カテゴリは以下の方法で変更できます。

- ページ右側の **[新規項目]** および **[許可]** セクションからタイルをドラッグアンドドロップして、アプリケーションおよび許可のタイルを追加する
- 項目のタイル内にあるごみ箱アイコンを選択して、アプリケーションまたは許可を削除する
- 項目の設定を変更する
- カテゴリの名前を変更する
- カテゴリ内の項目を並べ替える

カテゴリの削除

カテゴリを削除するには、カテゴリ名の右側にあるごみ箱アイコンを選択します。

6 自分のタスクの管理

Identity Manager の要求された許可を承認または拒否する責任がある場合は、ユーザアプリケーションで以前実行した可能性があるタスクを、ダッシュボードを使用して管理することができます。要求を 1 つずつ承認または拒否したり、詳細情報を必要としない複数の単純な要求を一括して承認または拒否したりすることが可能です。

保留中の要求を確認するには、[タスク] をクリックします。

または、返信の電子メールでの要求の承認または拒否を可能にするリンクを含む電子メール通知を受け取ることもできます。

ユーザ要求に基づいて実行する前に、以下の考慮事項を確認してください。

- 複数のタスクを選択して、一括で承認 / 拒否することができます。
- 詳細情報が必要になる複雑な要求の場合は、ダッシュボードにチェックボックスが表示されません。各要求を選択してフォームに記入することによって、これらの要求を承認または拒否する必要があります。
- 承認または拒否する複雑な要求を選択した場合、ダッシュボードから別個のブラウザタブで要求フォームを開くことが必要になることがあります。
- 一般的に、選択したタスクを承認または拒否する理由を説明するコメントを提供する必要があります。

自分のタスクの表示

タスクを管理するには、[タスク] を選択します。その他のユーザに割り当てられたタスクを表示するには、[その他] をクリックします。

その他のタスクの代理人または委任先になっている場合、他のユーザに割り当てられているタスクを完了することができます。プロキシ割り当ておよび委任割り当ての詳細については、[代理ユーザとしての作業](#)を参照してください。

IDM Approvals (IDM 承認): [環境設定] > [Identity Governance] ページで、[Show IG Approvals in tasks page ([タスク] ページに IG 承認を表示する)] オプションが有効になっている場合にのみ適用されます。

このタブには、すべての Identity Manager タスクが一覧表示されます。デフォルトでは、すべての [自己] タスクが一覧表示されます。適切な役割とともに他のタスクを表示するには、[その他] をクリックします。

- [再割り当て済みタスク]、[返されたタスク]、または [委任済みタスク] フィルタを使用してタスクを検索できます。[自己] に対して [委任済みタスク] フィルタを使用すると、自分に委任されているタスクのみが表示されます。
- 管理者である場合、[自分に割り当て]、[受信者を自分にする] フィルタを使用してタスクをフィルタすることもできます。

- 他のユーザのタスクを検索する場合は、[返されたタスク]、[再割り当て済みタスク]、または [委任済みタスク] の各フィルタを使用できます。[その他] に対して [委任済みタスク] を使用すると、システム内の他のユーザに委任されるすべてのタスクが表示されます。
- システム内で発生しているタスクに基づいてタスクの検索を絞り込むこともできます。
 1.  を選択します。
 2. (条件付き) 特定の期間に作成したタスクを表示するには、[週]、[日]、または [時間] で期間を指定します。
 3. (条件付き) フィルタするタスクステータスを指定します。
 4. [フィルタ] をクリックします。
- ヘルプデスクユーザである場合、[ヘルプデスクタスク] フィルタを使用して絞り込まれたリストを表示できます。ヘルプデスクのタスクを管理するには、ダッシュボードのヘルプを参照してください。

アクセス要求ポリシーでユーザが要求の承認者として指定されている場合は、要求された項目を承認する必要がある可能性があります。これらの承認要求項目は、[承認] タブに一覧表示されます。

IG Approvals (IG 承認): [環境設定] > [Identity Governance] ページで、[Show IG Approvals in tasks page ([タスク] ページに IG 承認を表示する)] オプションが有効になっている場合にのみ適用されます。

このタブには、Identity Governance の保留中の承認タスクのすべてが一覧表示されます。[Reassign (再割り当て)] オプションを使用して、その他のユーザにタスクを再割り当てすることができます。

承認または拒否の要求の管理

一部の組織では、アクセスの要求の確認、承認、および拒否をグループで担当している場合があります。このような場合、グループの各メンバーが同じ要求を受け取ります。たとえば、IT サービスチームが通信機器およびコンピューティング機器に対する要求をすべて担当しているとします。新しい従業員から携帯電話の要求があった場合、その要求は IT サービスチームのすべてのメンバーに割り当てられます。チームの誰でもその要求を完了できます。

要求に対して次のいずれかのタスクを実行できます。

要求の引き受け

要求に対する「責任を引き受け」、要求されたタスクにすぐに対応するか、後で対応することができます。この場合、自分がいつタスクに対応するかには関係なく、その要求はグループの他のメンバーの [タスク] に表示されなくなります。

要求の解放

引き受けた要求に対応したくない場合は、その要求を解放することができます。

要求の再割り当て

自分に割り当てられたタスクは、組織内の他のユーザに再割り当てすることができます。タスクの再割り当てには、次の考慮事項が適用されます。

- タスクを完了できない場合は、マネージャに再割り当てすることができます。**[自己]**タブで要求を選択し、**[再割り当て]**を選択します。タスクはマネージャに自動的に再割り当てされます。
- チームマネージャは、自分のタスクを自分のマネージャにのみ再割り当てすることができます。ただし、チームのメンバーに割り当てられているタスクを再割り当てする場合は、**[その他]**タブを使用して行えます。**[その他]**タブに移動し、必要なタスクのチェックボックスをオンにして、**[再割り当て]**をクリックします。**[割り当て先]**ドロップダウンメニューで、タスクを再割り当てするチームメンバーを選択し、再割り当てのコメントを入力して、**[再割り当て]**をクリックします。タスクは選択したチームメンバーに再割り当てされます。
- 指定した時間枠内にタスクに対応しなかった場合は、次のアクションを行うことができます。
 - 管理者は、タスクを別のユーザに再割り当てできます。管理者は、組織内の任意のユーザにタスクを再割り当てする許可を持っています。
 - チームマネージャは、別のチームメンバーにタスクを再割り当てできます。チーム作成時にチームマネージャの「宛先タスクの管理」許可が有効化されていることを確認します。

これは、チーム作成時に**[メンバー]**オプションを使用してメンバーをチームに追加する場合にのみ適用されます。詳細については、[84 ページの「チームの作成」](#)を参照してください。

注: **[すべてのユーザ]** または **[関係]** オプションを使用してチームを作成する場合、チームマネージャはチーム内の別のメンバーにタスクを再割り当てできません。

- ヘルプデスクユーザは、**[設定]** ページで定義した階層レベルまで、タスクをマネージャに再割り当てできます。管理者は、マネージャ階層を設定します。

タスクが再割り当てされても、それを引き受けることができない場合は、タスクを割り当てたユーザにタスクを返すことができます。

要求を返す

再割り当てされた要求に対応したくない場合は、その要求を返すことができます。Identity Applications は、返されたタスクを実際の承認者に自動的に割り当て直します。

注: 返すことができるのは、再割り当てされた要求のみです。

詳細については、ダッシュボードの①をクリックしてください。

ヘルプデスクタスクの管理

ヘルプデスクタスクは、システムで提出されたヘルプデスクチケットごとに生成されます。16 ページの「ヘルプデスクの仕組み」の例によると、Emily のチケットにより、Helen の[タスク] ページにヘルプデスクタスクが作成されます。Helen は、このヘルプデスクタスクに対して適切なアクションを取ることができます。

ヘルプデスクユーザである場合、アクションが必要なヘルプデスクチケットを選択します。選択したヘルプデスクチケットに対して、次のいずれかのアクションを実行します。

アップデート

適切なコメントを付けてヘルプデスクチケットをアップデートします。

完了

解決策のコメントを含むヘルプデスクチケットを完了します。

キャンセル

適切なコメントを付けてヘルプデスクチケットを閉じます。

注: ヘルプデスクタスクの[引き受け]または[解放]を行うことができます。タスクのリストからヘルプデスクチケットを引き受けると、ヘルプデスクチケットが[自己]タスクに表示されます。

詳細については、ダッシュボードの①をクリックしてください。

7 他の人の代わりに実行する

組織によっては、他の人のために、代理、または委任としてタスクを完了できる場合があります。たとえば、個人秘書が、上司の代理アクションを実行する場合です。また、同僚が産休の間、一時的に彼女の代わりに作業を割り当てられる場合もあります。

- 53 ページの「自分の代理人割り当ての表示」
- 53 ページの「代理ユーザとしての作業」
- 53 ページの「代理人割り当ての管理」

詳細については、ダッシュボードの①をクリックしてください。

自分の代理人割り当ての表示

代理人割り当てを表示するには、ダッシュボードで以下を選択します。:

[アクセス]>[代理人割り当て]

代理ユーザとしての作業

管理者から、別のユーザの代理人に指名されることがあります。この場合、右上隅のアカウントメニューに代理オプションが追加されます。

[ユーザの ID]>[代理人対象]

たとえば、Sarah Smith が顧客関係を管理している場合を考えます。Identity アプリケーションには、Sarah Smith をチームマネージャとする顧客関係チームが含まれています。彼女は、彼女のチームのメンバーである Maria Belafonte の代わりに務めることができます。この場合、Dashboard で、彼女は [ssmith]>[代理人対象] を選択し、次に [mbelafonte] を選択します。

代理人割り当ての管理

管理者またはチームマネージャは、割り当てを作成、変更、および削除することができます。チームのために代理人割り当てを管理するチームマネージャは、チームを適切に設定する必要があります。チームマネージャは、チームメンバーのみの割り当てを作成することができます。

8 委任の管理

組織によっては、別のユーザにタスクを委任することもできます。他のタスクの委任先になった場合、またはタスクを組織内の他のユーザに委任した場合、その委任情報を [管理] > [委任] で確認することができます。

委任されたタスクは [タスク] ページに表示されます。 アイコン付きのタスクは、そのタスクが委任されていることを示します。

重要: 委任割り当てを作成するには、可用性の詳細を指定する必要もあります。委任割り当ての作成中に可用性の詳細を指定するか、委任を作成してから別のアクションで可用性の詳細を指定できます。これは、管理者が必要な設定を有効にしているかどうかによって異なります。有効にしている場合は、[委任割り当ての作成] ページに [稼働不可開始日] オプションが表示されます。ただし、[稼働不可開始日] オプションが表示できない場合は、委任割り当ての作成後に、[可用性設定] ページから可用性の詳細を指定する必要があります。これにより、委任が期待どおりに機能するようになります。詳細については、ダッシュボードの  をクリックしてください。

9 可用性の管理

特定の期間中に作業できない委任割り当てを持つリソース要求を指定できます。自分が特定のリソース要求を処理できない期間、そのリソース要求の処理を委任されたユーザは、そのリソース要求を処理できます。

可用性を表示するには、ダッシュボードで以下を選択します。

[人] > [可用性]

[稼働不可開始日] アクションを使用する前に、作業を行うには少なくとも 1 つの委任割り当てが必要です。チームマネージャ (またはプロビジョニングアプリケーション管理者) に委任割り当てを作成してもらう必要があります。

可用性ベースの委任に関連するグローバル設定は、[設定] > [カスタマイズ] > [ナビゲーション項目] > [一般] で [委任割り当ての作成中に可用性を設定する] で指定します。要求定義ごとに可用性を個別に指定しない場合は、[変更ステータス] アクションから [すべての要求で稼働不可] を使用できます。

詳細については、ダッシュボードの①をクリックしてください。

10 プロファイルの管理

Identity アプリケーションは、Identity 情報を表示および操作する便利な方法を提供します。また、他のユーザに関する情報が必要になったときにその情報へのアクセス権を与えることによって、組織が迅速に対応できるようにすることもできます。たとえば、以下のような場合が考えられます。

- 自分自身のユーザアカウントを直接管理する
- 必要に応じて組織内の他のユーザやグループを検索する
- ユーザやグループの関係を図でわかりやすく表示する
- 関連付けられているアプリケーションを表示する

システム管理者は、組織内のユーザのために Identity アプリケーションの内容を設定する責任があります。一般に、各ユーザが表示できる情報および実行できる操作は、ユーザのジョブ要件と権限レベルによって決まります。

プロファイルの更新

Identity プロファイルを表示または更新するには、ダッシュボードで以下を選択します。

[ユーザの ID] > [マイプロフィール]

または

ダッシュボードの  をクリックします。

このページには、自身のレポーティングマネージャ、役割、リソース、およびグループが一覧表示されます。自身の情報を編集したり、自身の組織図を表示したりするには、管理者アクセス権が必要です。

プロフィールには、名前、電子メールアドレス、電話番号などの設定が含まれています。このページには、[検索] と [読み取り] のアクセスが有効化されたユーザ属性が表示されます。これらのアクセスプロパティは、ディレクトリ抽象化レイヤ (DAL) で設定できます。詳細については、『[NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications](#)』の「[Attribute Properties](#)」を参照してください。変更できる設定を決定するのは、所属する組織です。たとえば、電話番号は変更できますが、名字は変えられないようになっています。

11 組織図の管理

Identity Manager ダッシュボードは、組織内のエンティティを検索し、その組織図を表示する便利な方法を提供します (エンティティは管理者によって定義されたユーザ、グループ、またはカスタムエンティティのいずれかです)。組織図には、組織内のエンティティ間のマネージャ - 従業員、グループのメンバーシップ、ユーザグループなど、関係の階層が表示されます。

デフォルトでは、ダッシュボードの [組織チャート] ページには、管理者によって設定された組織チャート関係に基づいて、組織内のユーザエンティティの配置、およびその他のユーザエンティティとの関係階層が表示されます。組織チャートのデフォルト設定の詳細については、「[Customizing the Views](#)」を参照してください。ユーザエンティティ以外のエンティティの組織チャートを表示する方法の詳細については、『[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)』の「[Viewing the Organization Chart of an Object](#)」を参照してください。

組織図はしばしば「組織チャート」と呼ばれます。ダッシュボードではこれらの両方の用語が使用されている場合があります。

組織図の表示

デフォルトでは、セキュリティ管理者とプロビジョニング管理者は、システム内のすべてのエンティティの組織図を表示できます。

ユーザエンティティの組織図にアクセスするには、次のいずれかの方法を使用します。

- [人] > [組織チャート] に移動すると、このページには、[設定] ページで設定されたデフォルトの組織図の関係に基づいて、ログインしているユーザの組織図が表示されます。[マイプロフィール]、[ダッシュボード]、および [アプリケーション] ページで提供される  アイコンを使用して、組織図を表示することもできます。

システムの他のユーザの組織図を見つけるには、[組織チャート] ページで提供される検索バーで他のユーザの名前を入力します。

- [人] > [ユーザ] に移動して、リストから任意のユーザを選択して、そのユーザ名の横にある  をクリックします。詳細については、79 ページの第 13 章「ユーザの管理」を参照してください。

注: [組織図] を表示するには、[組織図] アクセス権が必要です。このアクセス権を割り当てるには、管理者に連絡してください。詳細については、『[NetIQ Identity Manager - Administrator's Guide to Identity Applications](#)』の「[User Settings](#)」を参照してください。

組織チャートの理解

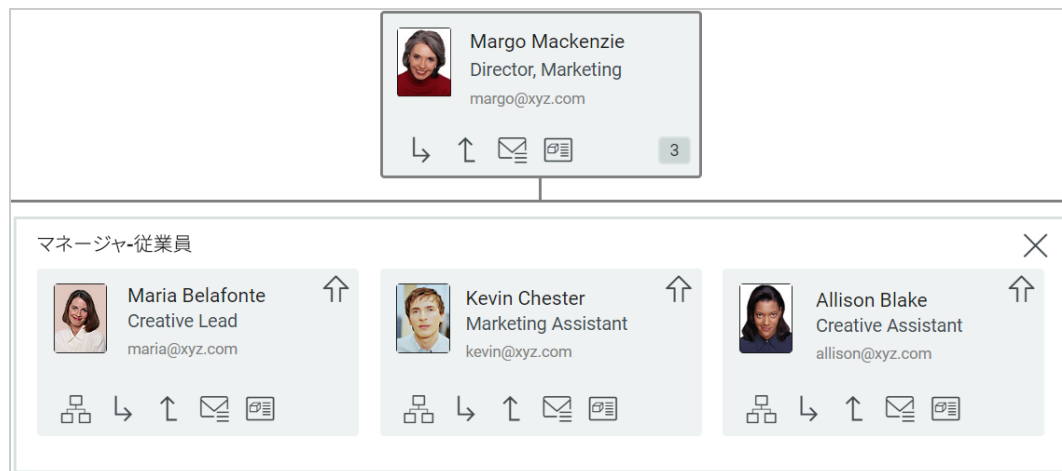
組織チャートにはカード形式でエンティティ情報が表示されます。これらのカードは、管理者が設定したデフォルトの組織チャート関係に基づいて階層順に配置されます。上部に表示されるルートまたは選択したエンティティは、組織図の開始点または方向点で、ルートエンティティ直下の子エンティティはデフォルトの関係に基づいて下部に表示されます。

各カードには管理者が定義したプライマリ属性とセカンダリ属性に基づいた情報が表示されます。これらの属性のカスタマイズ方法の詳細については、『[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)』の「[Customizing the Organization Chart View](#)」を参照してください。具体的には、ユーザエンティティの場合、管理者によって定義されたプライマリ属性とセカンダリ属性に加えて、ユーザのフルネームを表示するようにカードが設定されます。その結果、管理者が名と姓をプライマリ属性として設定すると、ユーザのフルネームが[ユーザ]ページの[カードビュー]と組織図に2回表示される場合があります。

注: 組織図ビューでは、エンティティのプライマリ属性とセカンダリ属性が管理者によって定義されていない場合、Identity Applications はそのエンティティの CN 属性を[組織チャート]ページに表示します。

図 11-1 は、デフォルトの組織図関係が「マネージャ - 従業員」に設定されているユーザ「Margo Mackenzie」の組織図の例を示しています。

図 11-1 ダッシュボードでの組織図の例



この例では、「Margo Mackenzie」がマネージャであり、「Maria Belafonte」、「Kevin Chester」、「Allison Blake」は彼女の直属の従業員です。各カードの上部には、ユーザのフルネームが表示されます。Margo の場合は、「Margo Mackenzie」が表示されます。その後、管理者がプライマリ属性とセカンダリ属性として設定した組織内の役割と電子メールアドレスが表示されます。「Margo Mackenzie」のカードの右下隅に表示されるカウントは、彼女の直属の従業員の数を示しています。

組織図での作業

【組織チャート】ページに入力された検索入力に基づいて、ダッシュボードにはエンティティの組織図が表示されます。このページでは、エンティティの他の関係の表示、ルートエンティティの変更とその組織図の表示、または関係階層の次のレベルのエンティティの組織図表示など、他のタスクを実行できます。

【組織チャート】ページで実行可能なタスクに関する詳細を理解するために、XYZ 社、マーケティングチームの次の例を考えてみましょう。

「Margo Mackenzie」はマーケティングチームのディレクターで、「Allison Blake」、「Kevin Chester」、および「Maria Belafonte」が彼女の直属の従業員です。「Margo Mackenzie」は、マーケティングチームの副社長「Timothy Swan」の直属の部下です。

ダッシュボードの【人】>【組織チャート】に移動し、「Timothy Swan」を検索して、彼の組織図を表示します。同様に、「Margo Mackenzie」の検索を実行します。図 11-2 と図 11-3 は、マネージャ - 従業員関係に基づく個々の組織図を示しています。

図 11-2 マネージャ役割の Timothy Swan の組織図

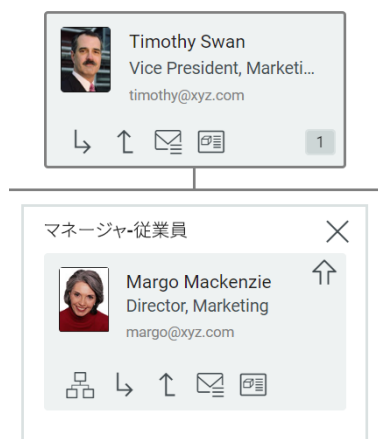
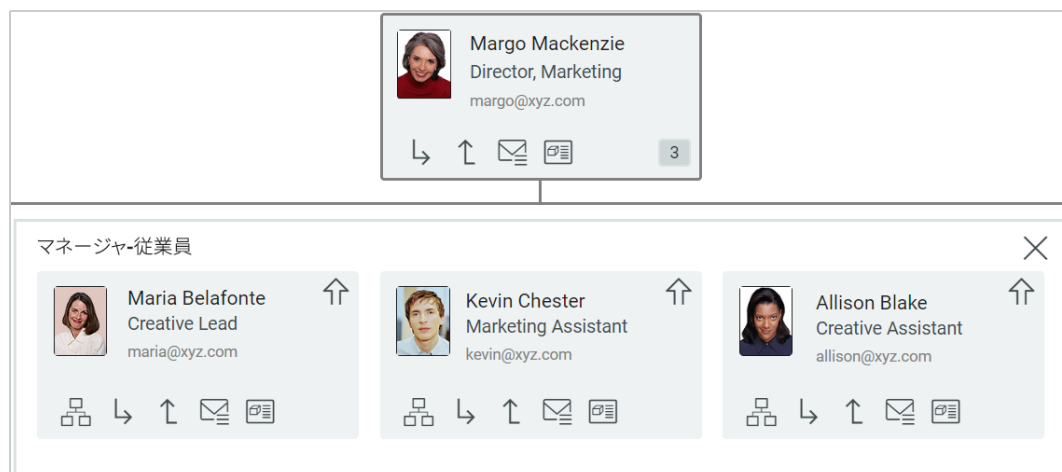


図 11-3 マネージャ役割の Margo Mackenzie の組織図



上記の例に基づく「組織チャート」ページで実行可能なタスクを見てみましょう。

- ◆ 64 ページの「組織チャートビューでのルートのリセット」
- ◆ 64 ページの「組織チャートビューの切り替え」
- ◆ 65 ページの「表示する関係の選択」
- ◆ 66 ページの「関係階層の次のレベルに移動」
- ◆ 67 ページの「組織チャートからユーザへの電子メールの送信」
- ◆ 67 ページの「ユーザの詳細情報の表示」

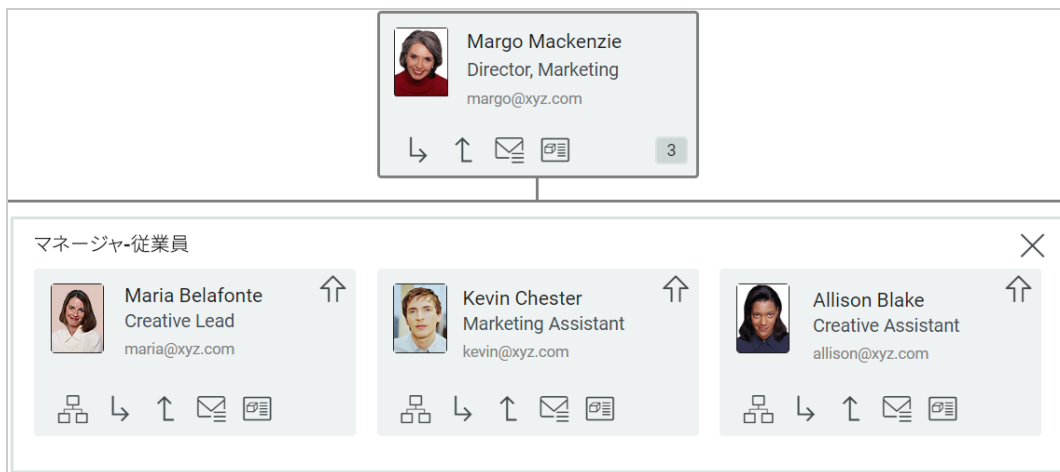
注：上記のタスクは、ユーザエンティティとカスタムエンティティの両方に適用できます。

組織チャートビューでのルートのリセット

組織チャートビューでルートユーザをリセットするには、

- 1 新しいルートとして作成するユーザを特定します。
「Timothy Swan」がマネージャの役割になっている組織図を表示していて、「Margo Mackenzie」を新しいルートにしたいとします。
- 2 「Margo Mackenzie の」カードに移動し、 アイコンをクリックします。彼女は新しいルートになり、マネージャ - 従業員の組織図のトップになっています。「Margo Mackenzie」の直属の従業員、すなわち、「Maria Belafonte」、「Kevin Chester」、および「Allison Blake」が彼女の下に表示されています。

図 11-4 組織チャートビューの新しいルートとしての Margo Mackenzie



組織チャートビューの切り替え

組織チャートビューのルートユーザとデフォルトの関係をリセットするには、次のアクションを実行します。

- 1 組織チャートを表示するユーザを特定します。

「Margo Mackenzie」がマネージャの役割になっている組織図を表示しているとします。「Maria Belafonte」は「Margo Mackenzie」の下で働く従業員で、「Kevin Chester」と「Allison Blake」のメンターでもあります。「Maria Belafonte」のメンター - 従業員関係を表示したいとします。

- 2 「Maria Belafonte の」カードに移動し、をクリックします。
- 3 ドロップダウンメニューから、関係として **[Mentor-Employee (メンター - 従業員)]** を選択します。「Maria Belafonte」がメンター - 従業員組織図のルートとなり、「Kevin Chester」と「Allison Blake」は彼女の下で働く従業員として表示されます。

図 11-5 メンター役割の Maria Belfonte の組織図



表示する関係の選択

デフォルト以外のユーザの関係を表示するには、次のアクションを実行します。

- 1 関係を表示するユーザを特定します。
「Margo Mackenzie」がマネージャの役割になっている組織図を表示しているとします。マーケティンググループの一員である「Maria Belafonte」のユーザグループ関係を表示したいとします。
- 2 「Maria Belafonte の」カードに移動し、をクリックします。
- 3 ドロップダウンメニューから、関係として **[ユーザグループ]** を選択します。「Maria Belafonte の」グループメンバーシップチャートが既存の組織チャートビューにインラインで追加されます。

注: ユーザの組織図を展開し、関係をインラインで表示できる最大レベルは、管理者によって定義されます。デフォルトでは、レベル 3 まで展開できます。レベル 1 は常にルートユーザに割り当てられます。

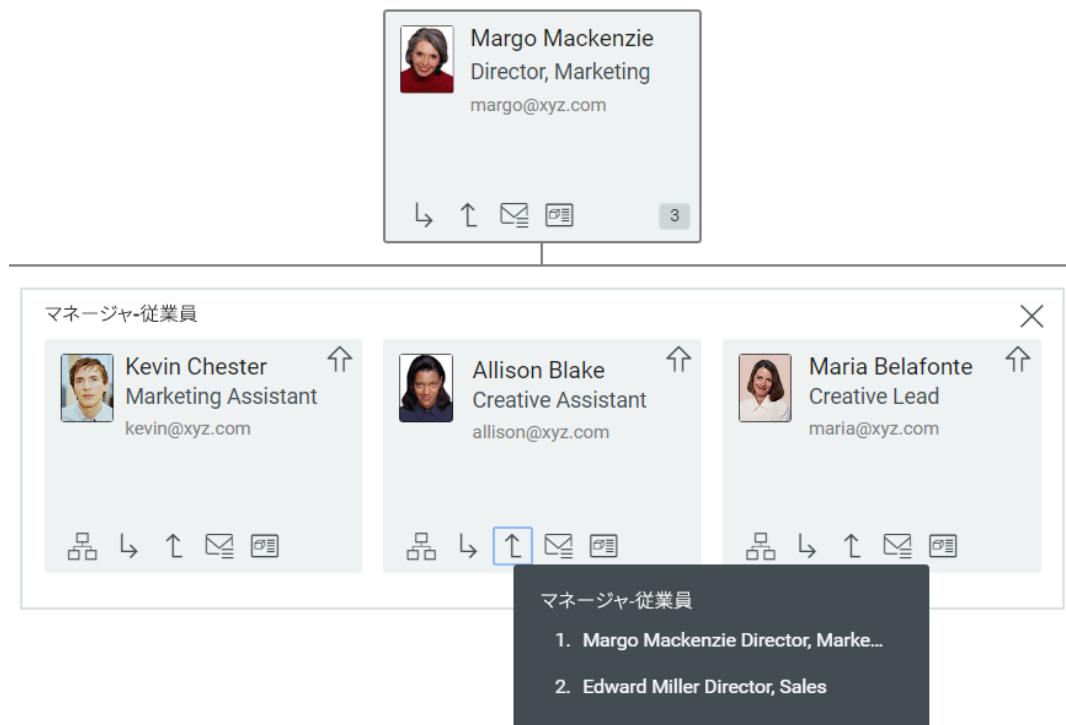
関係階層の次のレベルに移動

このタスクを理解するために、セールスチームのディレクターである「Edward Miller」の2番目の例を考えてみましょう。「Allison Blake」と「Filla Martell」は「Edward Miller」の直属の部下です。ご覧のように、「Allison Blake」はセールスチームとマーケティングチームの共通のメンバーであり、2人のマネージャ、すなわち「Edward Miller」と「Margo Mackenzie」の直属の部下です。

関係ツリー内の次のレベルに移動して展開するには、次のアクションを実行します。

- 1 表示するユーザを特定し、階層の次のレベルに移動します。
「Margo Mackenzie」がマネージャの役割である組織図を表示していて、「Allison Blake」の組織図を表示したいとします。
- 2 「Allison Blake の」カードに移動して、をクリックし、リストから再帰的なマネージャ - 従業員関係を選択します。
- 3 をクリックします。
[マネージャ - 従業員] ドロップダウンメニューで、従業員「Allison Blake」には直属の上司である2人のマネージャ、すなわち「Margo Mackenzie」と「Edward Miller」が表示されます。

図 11-6 Allison Blake の再帰的なマネージャ - 従業員関係



- 4 マネージャの「Edward Miller」を選択します。「Allison Blake」の組織図が表示されます。

図 11-7 Allison Blake の組織図



組織チャートからユーザへの電子メールの送信

✉ オプションを使用すると、次の操作を実行できます。

- 選択したユーザへの電子メールの送信
- 電子メール経由のエンティティのプロファイルリンクの共有
- (オプション、マネージャ-従業員関係にのみ適用可能) 選択したユーザ下にある全チームメンバーへの電子メールの送信

詳細については、ダッシュボードの①をクリックしてください。

重要：

- 組織チャートビューから電子メールを送信する前に、デフォルトの電子メールクライアントがシステムで設定されていることを確認する必要があります。
 - [新しい電子メール] および [電子メールチーム] オプションが機能するようにするには、[設定] ページで電子メール属性をプライマリ属性またはセカンダリ属性として設定します。詳細については、『[NetIQ Identity Manager - Administrator's Guide to Identity Applications](#)』の「[User Settings](#)」を参照してください。
-

ユーザの詳細情報の表示

- 1 情報を表示するユーザを特定します。
「Margo Mackenzie」がマネージャの役割である組織図を表示していて、「Kevin Chester」に割り当てられた役割やリソースなどの追加の詳細を表示したいとします。
- 2 「Kevin Chester」のカードに移動して、 アイコンをクリックします。プロファイルページに、彼に割り当てられた役割とリソースを含む詳細情報が表示されます。

ユーザのカード、たとえば、XYZ 組織の社長である、「Jack Miller の」カードで  アイコンが表示できない場合は、ユーザのカタログへの適切な許可がないため、彼のプロフィールを表示できないことを示しています。プロフィールを表示するために必要なアクセス権が必要な場合は管理者に連絡してください。

詳細については、ダッシュボードの  をクリックしてください。

12 パスワードの管理

Identity Manager には SSPR (Self Service Password Reset) が組み込まれており、パスワードの変更プロセスやパスワードを忘れた場合のリセットプロセスを簡単に管理できます。パスワードリセットの際には、本人確認の回答による認証方法を使用してユーザが認証されます。

- 69 ページの「Identity Manager でのセルフサービスパスワード管理の使用」
- 71 ページの「従来のパスワード管理の使用」

注: この項では、パスワード管理のデフォルトの機能について説明します。ジョブの役割、権限レベル、および組織内でのカスタマイズのために、ご使用の Identity Manager ユーザアプリケーションと異なっている可能性があります。詳細については、システム管理者に相談してください。

Identity Manager でのセルフサービスパスワード管理の使用

SSPR は、アイデンティティアプリケーションおよび Identity Reporting のシングルサインオンプロセスと自動的に統合されます。SSPR は、Identity Manager のデフォルトのパスワード管理プログラムです。ユーザがパスワードのリセットを要求すると、本人確認の質問に回答するよう求められます。回答が正しければ、SSPR は次のいずれかの方法で応答します。

- ユーザに新しいパスワードの作成を許可する
- 新しいパスワードを作成してユーザに送信する
- 新しいパスワードを作成してユーザに送信し、古いパスワードを期限切れとしてマークする

SSPR Configuration Editor でこの回答を設定します。新しいバージョンの Identity Manager にアップグレードした後は、Identity Manager がパスワード管理に従来使用していた NMAS を使用するように SSPR を設定することができます。ただし、SSPR は、パスワードを忘れた場合のプロセスを管理する際に既存のパスワードポリシーを認識しません。NMAS の代わりに、独自のプロトコルを使用するように SSPR を設定することもできます。このように変更した場合、パスワードポリシーをリセットせずに NMAS を使用する設定に戻すことはできません。

SSPR を使用して、72 ページの表 12-2 「パスワード管理機能」に記載されている機能を実行できます。

表12-1 パスワード管理機能

ページ名	実行できる作業
パスワード確認の回答	次の情報を設定または修正する - システム管理者によって定義された本人確認の質問に対する、有効な回答 - ユーザ定義の本人確認の質問とその回答
パスワード変更	システム管理者によって定められたルールに従って、自分のパスワードを変更 (リセット) する
パスワードポリシーステータス	パスワードポリシーの要件を確認する

パスワード確認の回答の理解

本人確認の質問は、ログイン時に自分のパスワードを忘れてしまったときに、自分が正規ユーザであることを証明する目的で使われます。システム管理者によって設定されたパスワードポリシーにおいて、この機能が自分に対して有効になっている場合、[パスワード確認の回答] ページで次の作業を実行できます。

- システム管理者によって定義された質問に対して有効であると考えられる、回答を指定する
- 自分専用の質問、およびその質問に対する有効な回答を指定する (この作業は、自分に関するパスワードポリシーでこの機能が有効になっている場合にのみ、実行できる)

ログインプロセス中に、ログインページから [本人確認の回答] ページに自動的にリダイレクトされます。このページで本人確認の質問に対する回答を設定します。詳細については、[22 ページの「パスワードを忘れた場合」](#)を参照してください。再度ログインし、忘れたパスワードをリセットしようとする、設定した質問が表示され、正しい回答を指定するよう求められます。入力した回答が事前に保存した回答と一致した場合、パスワードをリセットできます。

パスワードを変更する

パスワードは変更可能です (システム管理者の許可が必要になります)。

- ダッシュボードで、[アプリケーション] > [マイパスワードの変更] をクリックします。
- 現在のパスワードを入力します。[パスワードの変更] ページが開きます。

- 3 **[New Password (新しいパスワード)]** テキストボックスに新しいパスワードを入力します。
- 4 **[パスワードの確認]** テキストボックスに新しいパスワードをもう一度入力します。
- 5 **[パスワードの変更]** をクリックします。

新しいパスワードが、管理者がパスワードポリシーで定義したパスワードルールのいずれかに違反した場合、**[パスワードの変更]** ページにエラーメッセージが表示されます。

このページには通常、管理者が定義したポリシーの要件に合ったパスワードを指定する方法についての説明が表示されます。パスワードルールを確認し、もう一度やり直してください。

- 6 **[続行]** をクリックします。処理状況が表示されます。成功すると、OSP ログインページに戻ります。

パスワードポリシーステータス

注: この機能は、管理者ユーザのみが使用できます。

管理者によって、パスワードポリシーが割り当てられています。このポリシーは、パスワードに関連するセキュリティ対策を決定します。ユーザアプリケーション管理者から権限を与えられている場合を除き、ユーザはパスワードポリシーの要件を確認することはできません。ユーザアプリケーション管理者は、Identity Manager ホームページでパスワードポリシーのステータスを確認できます。デフォルトでは、このリンクは存在しません。このリンクを表示するには、ホームページをカスタマイズする必要があります。デフォルトの Identity Manager のホームアイテムのカスタマイズについては、[45 ページの第 5 章「アプリケーションの管理」](#)を参照してください。

ランディングページで、**[パスワードステータスとポリシー]** リンクをクリックします。

[Password Policy Status and Policy (パスワードポリシーステータスとポリシー)] ページが表示されます。Identity Manager のパスワードを変更するには、Identity Manager ホームに移動し、**[マイパスワードの変更]** を選択します。SSPR の **[パスワードの変更]** 領域にリダイレクトされます。

従来のパスワード管理の使用

この項では、Identity Manager ユーザアプリケーションの **[Identity セルフサービス]** タブに表示される、パスワード管理関連ページの使用方法について説明します。この節の内容は次のとおりです。

- [72 ページの「パスワード確認の回答」](#)
- [73 ページの「パスワードヒントの変更」](#)
- [73 ページの「パスワード変更」](#)
- [75 ページの「パスワードポリシーステータス」](#)
- [75 ページの「パスワード同期ステータス」](#)

注: この項では、パスワード管理関連ページのデフォルトの機能について説明します。ジョブの役割、権限レベル、および組織内でのカスタマイズのために、ご使用の Identity Manager ユーザアプリケーションと異なっている可能性があります。詳細については、システム管理者に相談してください。

[Identity セルフサービス] タブの使用に関する全般的な説明については、59 ページの第 10 章「プロファイルの管理」を参照してください。

パスワード管理関連ページを使用すると、72 ページの表 12-2 「パスワード管理機能」に一覧されているすべての機能を実行できます。

表 12-2 パスワード管理機能

ページ名	実行できる作業
パスワード確認の回答	次の情報を設定または修正する - システム管理者によって定義された本人確認の質問に対する、有効な回答 - ユーザ定義の本人確認の質問とその回答
パスワードヒントの変更	自分のパスワードヒントを設定または修正する
パスワード変更	システム管理者によって定められたルールに従って、自分のパスワードを変更 (リセット) する
パスワードポリシーステータス	パスワードポリシーの要件を確認する
パスワード同期ステータス	アプリケーションパスワードと識別ボールドとの同期の状態を表示する 注: 同期が完了する前にアプリケーションにアクセスすると、アプリケーションアクセスの問題が発生します。

パスワード確認の回答

本人確認の質問は、ログイン時に自分のパスワードを忘れてしまったときに、自分が正規ユーザであることを証明する目的で使われます。システム管理者によって設定されたパスワードポリシーにおいて、この機能が自分に対して有効になっている場合、[パスワード確認の回答] ページで次の作業を実行できます。

- システム管理者によって定義された質問に対して有効であると考えられる、回答を指定する
- 自分専用の質問、およびその質問に対する有効な回答を指定する (この作業は、自分に関するパスワードポリシーでこの機能が有効になっている場合にのみ、実行できる)

[パスワード確認の回答] ページを使用するには

- [Identity セルフサービス] タブのメニューで、[パスワードの管理] カテゴリにある [パスワード確認の回答] をクリックします。

[パスワード確認の回答] ページが開きます。

- 2 それぞれの **[回答]** テキストボックス (すべて必須) に適切な回答を入力するか、以前に保存した回答を使用します。**[保存した回答を使用する]** を選択した場合、ラベルを含め本人確認の回答は表示されません。また、ユーザ定義の本人確認の質問は無効です。回答は、後で思い出せる内容にしてください。
- 3 ユーザ定義の質問を指定または修正します (入力必須)。同じ質問を 1 回以上使用することはできません。
- 4 **[送信]** をクリックします。
本人確認の回答を保存した後、ユーザアプリケーションにより本人確認の回答が正常に保存されたことを示すメッセージが表示され、「保存されている回答を使用しますか?」が選択された状態で本人確認の回答画面が再表示されます。

パスワードヒントの変更

パスワードヒントは、ログイン時に自分のパスワードを忘れてしまったときに、自分のパスワードを思い出すための手がかりとして使われます。**[パスワードヒントの変更]** ページで、自分のパスワードヒントを設定および修正できます。

- 1 **[Identity セルフサービス]** タブのメニューで、**[パスワードの管理]** カテゴリにある **[パスワードヒントの変更]** をクリックします。
[パスワードヒント定義] ページが表示されます。
- 2 自分の新しいパスワードヒントを入力します。
パスワードヒントの中にパスワード自体を含めることはできません。
- 3 **[送信]** をクリックします。
処理状況が表示されます。

パスワード変更

パスワード変更権限がシステム管理者から付与されている場合、**[パスワードの変更]** ページで自分のパスワードを随時変更できます。

- 1 **[Identity セルフサービス]** タブのメニューで、**[パスワードの管理]** カテゴリにある **[パスワードの変更]** をクリックします。
[パスワードの変更] ページが開きます。システム管理者によって自分に関するパスワードポリシーが設定されている場合、一般に **[パスワードの変更]** ページには、そのパスワードポリシーを反映したパスワード指定方法が表示されます。たとえば、次のような指定内容です。
パスワードポリシーが適用されていない場合、パスワードを変更するフィールドを表示するだけの **[パスワードの変更]** ページが表示されます。
ユーザアプリケーションは次のパスワード構文タイプをサポートしています。
 - ◆ Microsoft の複雑さのポリシー
このパスワード構文タイプは、Active Directory 2003 との後方互換性のために使用されます。
 - ◆ Microsoft Server 2008 パスワードポリシー

これは、Active Directory 2008 をサポートするために eDirectory 8.8.7 に追加された新しいパスワード構文タイプです。

Microsoft Server 2008 パスワードポリシーでは、次の設定がサポートされています。

- ◆ Microsoft Server 2008 パスワードポリシーの使用
- ◆ パスワードの複雑さのポリシー違反の最大数 (0 ~ 5)
- ◆ Novell 構文

Novell 構文では次の新しい設定がサポートされています。

- ◆ アルファベット以外の文字の最小数 (1 ~ 512)
- ◆ アルファベット以外の文字の最大数 (1 ~ 512)

3 つのパスワード構文タイプすべてについて、ユーザアプリケーションは次の機能をサポートしています。

- ◆ 現在のパスワードおよび履歴にあるパスワードと異なる文字の数 (0 ~ 6)
- ◆ 文字を除外するために考慮される履歴内のパスワードの数 (0 ~ 10)

管理者が Microsoft Server 2008 ポリシー構文を有効にしている場合、[パスワードの変更] ページで次のフィールドに値を入力してください。

- 2 [古いパスワード] テキストボックスに現在のパスワードを入力します。
- 3 [新しいパスワード] テキストボックスに新しいパスワードを入力します。
- 4 [パスワードを再入力してください] テキストボックスに、新しいパスワードをもう一度入力します。
- 5 [送信] をクリックします。

新しいパスワードが、管理者が定義したパスワードルールのいずれかに違反した場合、[パスワードの変更] ページにエラーメッセージが表示されます。Microsoft Server 2008 ポリシーを使用している場合、パスワードがルールに違反していると、ユーザインタフェースのページの最上部にこのメッセージが表示されます。

Password AD2008 complexity policy violation.

新しいパスワードがルールに違反している場合、管理者が定義したパスワードルールを確認して、再度実行してください。

- 6 管理者が設定したセキュリティポリシーによっては、パスワードヒントの入力を要求される場合があります。その場合は、[73 ページの「パスワードヒントの変更」](#)を参照してください。
- 7 処理状況が表示されます。

パスワードポリシーステータス

管理者によって、パスワードポリシーが割り当てられています。このポリシーは、パスワードに関連するセキュリティ対策を決定します。次のようにして、自分のパスワードポリシーの要件を確認できます。

- 1 [Identity セルフサービス] タブのメニューで、[パスワードの管理] カテゴリにある [パスワードポリシーの状態] をクリックします。すると [パスワードポリシーの状態] ページが表示されます。

無効となっている項目は、変更できない項目です。

パスワード同期ステータス

[パスワード同期ステータス] ページを使用して、アプリケーション間でパスワードが同期されているかを判断します。パスワードが必ず同期されてから他のアプリケーションにアクセスします。同期が完了する前にアプリケーションにアクセスすると、アプリケーションアクセスの問題が発生します。

- 1 [Identity セルフサービス] タブのメニューで、[パスワードの管理] カテゴリにある [パスワード同期ステータス] をクリックします。すると [パスワード同期ステータス] ページが表示されます。フルカラー表示のアイコンは、パスワードが同期されたアプリケーションを示します。淡色表示のアイコンは、同期が済んでいないアプリケーションを示します。

注: [ユーザの選択] ボックスを表示できるのは、管理者だけです。

IV ユーザ、グループ、およびチームの管理

Identity アプリケーション内で適切な役割を有している場合は、ユーザ、グループ、およびチームを作成および管理できます。ユーザとチームの作成は、ダッシュボードとユーザアプリケーションで実行できます。グループの作成と管理は、ユーザアプリケーションで実行します。

システム管理者は、ユーザとグループを作成することができます。システム管理者は、この機能へのアクセス権限を他のユーザ（通常、管理または経営者によって選ばれた人々）に付与できます。

この項で説明している機能とご使用の環境とが異なっている可能性があります。理由としては、自分のジョブ役割、自分の権限レベル、および組織内のカスタマイズが考えられます。詳細は、システム管理者にお問い合わせください。

チームは、チームに関連するプロビジョニング要求と承認タスクを実行可能な一連のユーザ、グループ、またはユーザとグループを表します。チームはユーザディレクトリに存在するグループに一致する可能性があります。チームはグループと同じものではありません。つまり、グループまたはグループのメンバーはチームに割り当てられているときを除いて、チームの機能を実行することはできません。詳細については、[83 ページの第 14 章「チームの管理」](#)を参照してください。

13 ユーザの管理

この項では、ダッシュボードおよびユーザアプリケーションでユーザとグループを作成する方法について説明します。主なトピックは次のとおりです。

- ♦ 79 ページの「ユーザの作成」
- ♦ 79 ページの「ユーザ情報を編集する」
- ♦ 80 ページの「ユーザの一覧表示」
- ♦ 81 ページの「ユーザの検索」
- ♦ 82 ページの「ユーザのソート」

ユーザの作成

[ユーザの作成] ページには、[検索] と [読み取り] のアクセスが有効化されたユーザ属性が表示されます。これらのアクセスプロパティは、ディレクトリ抽象化レイヤ (DAL) で設定できます。詳細については、『[NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications](#)』の「[Attribute Properties](#)」を参照してください。

ユーザを作成するには、ダッシュボードで以下を選択します。

[人] > [ユーザ] > [+]

Identity 管理者は、ユーザに指定できる値を定義します。また、ユーザの作成時に、ユーザの [コンテナ] を表示できますが、その値を変更することはできません。この制限により、すべてのユーザが同じコンテナ内に確実に格納されます。

詳細については、ダッシュボードの ⓘ をクリックしてください。

ユーザ情報を編集する

リストビューからユーザを選択し、 をクリックして、タイトル、電子メール、電話番号、マネージャなどのユーザ情報を変更します。管理者によって設定されたユーザ属性を変更できます。ユーザ属性の設定に関する詳細については、『[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)』の「[Customizing the Views](#)」を参照してください。[ユーザの管理] ビューで、ユーザを削除できます。

次の図では、ユーザ情報を編集する例を示しています。

図13-1 ユーザ情報を編集する



Hall Aliyah

役職

Marketing Director

+

Marketing Director

×

電話番号

552538

+

552538

×

直接報告

🔍 次の条件でユーザを検索: 名,姓

ログイン無効

☒

×

電子メール

aliyah@example.com

+

aliyah@example.com

×

マネージャ

🔍 次の条件でユーザを検索: 名,姓

保存

キャンセル

注: [Login Disabled (ログイン無効)] トグルスイッチを使用して、ユーザアカウントを無効にできます。このスイッチは、管理者が[設定]>[カスタマイズ]ページの[カードビュー]と[編集可能な属性]に Login Disabled 属性を追加した場合にのみ表示されます。詳細については、ダッシュボードの❓をクリックしてください。

ユーザの一覧表示

Identity Applications でユーザを一覧表示する方法を以下に示します。

- リストビュー: ユーザをリスト形式で表示するには、☰をクリックします。これにより、ユーザ情報が右側に表示されます。電話番号、電子メール、マネージャなどのユーザ情報を編集するには、✎をクリックします。特定のユーザの組織図を表示するには、👤をクリックします。
- カードビュー: ユーザをカード形式で表示するには、☐をクリックします。これにより、ユーザの基本情報がカードに表示されます。管理者は、ユーザのカードに表示する情報を設定できます。詳細については、『[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)』の「Customizing the Views」を参照してください。✎をクリックすると、[電話番号]、[電子メール]、[マネージャ]、その他の属性などのユーザ情報を編集できます。特定のユーザの組織図を表示するには、👤をクリックします。

- ◆ **マネージャユーザビュー**: ユーザを表形式で表示するには、をクリックします。これにより、ユーザが表形式で表示されます。このビューでは、電話番号、電子メール、部署などのユーザ属性に従ってユーザをソートすることができます。このビューに表示するカラムをカスタマイズすることができます。カラムのカスタマイズの詳細については、ダッシュボードの⑦をクリックしてください。

このビューでは、システムからユーザを削除することもできます。ユーザを削除するには:

1. 削除するユーザを選択します。
2. をクリックします。

ユーザの検索

Identity Applications でユーザを検索する方法を以下に示します。

- ◆ **クイック検索**: ユーザ属性を指定し、選択したフィルタに基づいてユーザを一覧表示します。フィルタオプションを変更するには:

1. をクリックします。
2. ユーザを検索するフィルタオプションを選択します。

次の例では、クイック検索用に選択されたユーザ属性を示しています。

フィルタ
リセット
キャンセル

- ☒ 名
- ☒ 姓
- ☐ 役職
- ☐ 部署
- ☐ リージョン
- ☒ 電子メール
- ☒ 電話番号

3. **[フィルタ]**をクリックします。

たとえば、名と姓のフィルタを選択して、名前が Smith のユーザを検索することができます。クイック検索には、名または姓に Smith を含むすべてのユーザが一覧表示されます。

- ◆ **高度な検索**: このオプションは、クイック検索よりも詳細なユーザのリストを取得します。定義されたユーザ属性を持つユーザを検索することができます。高度な検索を使用するには:

1. をクリックします。
2. 各ユーザ属性に正確なユーザ情報を指定します。

次の例では、詳細検索用に指定されたユーザ属性を示しています。

高度な検索



検索条件

名 ▼	Emily	×
姓 ▼	Cameron	×
電子メール ▼	emily.cameron@example.com	×
電話番号 ▼	5552368	×
+ 追加		

3. **[フィルタ]** をクリックします。

たとえば、**[名]** を Aliyah、**[姓]** を Hall、**[役職]** をディレクターとして検索するとします。高度な検索でこれらの属性を指定すると、正確な属性セットを持つユーザを見つけることができます。

最下部にインデックスを設定することで、ページ上に検索結果を設定することもできます。ダッシュボードでは、LDAP OID 2.16.840.1.113730.3.4 で実行される Virtual List View (VLV) コントロールを使用します。これはソート制御と組み合わせて機能します。

Identity Manager ダッシュボードには、結果を表示する際に次の 2 つの異なる数が表示されます。

- ◆ **総数** : これは、システムで検出されたユーザの総数です。
- ◆ **検索数** : これは、特定の検索に対して表示されるユーザの数です。

ユーザのソート

[マネージャユーザ] ビューでは、ユーザの属性に応じてユーザをソートすることができます。管理者は、ソートするためにユーザ属性の複合インデックスを設定する必要があります。複合インデックス作成の詳細については、『[NetIQ Identity Manager インストールおよびアップグレードガイド \(Windows 用\)](#)』の「[複合インデックスの作成](#)」を参照してください。

注 : ユーザ属性を使用してユーザをソートできない場合は、管理者に連絡して、ユーザをソートするために必要な属性の複合インデックスを設定してください。

14 チームの管理

チームは、次のような2種類のユーザで構成されています。

要求者

他のチームメンバー(受信者)に代わって許可要求を実行します。チームの設定内容に応じて、要求者は個々のプロビジョニング要求、1つ以上の要求カテゴリ、またはすべての要求に対応することができます。

また、チームメンバーの代理人割り当ても管理します。

受信者

要求者が代理として対応することが可能なチームのメンバー。

チーム受信者には、ディレクトリ内のユーザまたはグループを指定できます。または、ディレクトリ関係から生成することもできます。たとえば、メンバーのリストは組織内の「マネージャ-従業員」の関係から生成できます。この場合のチーム受信者は、チームマネージャの部下であるすべてのユーザを指します。

注: プロビジョニング管理者は、階層関係をサポートするようにディレクトリ抽象化レイヤを設定できます。これにより、組織内の複数のレベルを1チームに含めることができます。管理者は含めるレベルの数を設定できます。

次のいずれかの操作を実行するには、[人]>[チーム]に移動します。

- [83 ページの「チームの表示」](#)
- [84 ページの「チームの作成」](#)
- [84 ページの「チームの変更」](#)

チームの表示

[チーム] ページには、表示する許可を持つすべてのチームが一覧表示されます。ユーザは、一覧表示されたチームすべてのメンバーである場合があります。ただし、メンバーでなくても、特定のチームを表示、変更、または削除する許可を持つ管理者である場合もあります。

チームメンバーとして、他のチームメンバーの代わりに要求することが可能な、「要求者」である場合があります。また、チームの他はユーザが「受信者」に代わってこれらのアクションを実行することができる場合があります。詳細については、ダッシュボードの②をクリックしてください。

チームの作成

管理者として、チームを作成できます。チームは、チームに関連するプロビジョニング要求と承認タスクを実行可能な一連のユーザ、グループ、またはユーザとグループを表します。

各チームに対して、チームの許可を受信するチームメンバー ([受信者]) と、受信者の代わりにアクションを実行可能なメンバー ([要求者]) を指定します。チームを作成した後で、チームメンバーに適用される [許可] (リソースおよびプロビジョニング要求定義) を指定できます。たとえば、チームメンバーが持っていない場合があるラップトップリソースを追加できます。

詳細については、ダッシュボードの①をクリックしてください。

チームの変更

管理者として、チームを変更および削除することができます。チームの次の機能を変更できます。

- チームの名前と説明の変更
- チームの要求者の変更
- チームメンバーの追加または削除
- チームマネージャの許可の追加または削除

詳細については、ダッシュボードの①をクリックしてください。

15 グループを管理する

グループは、共通の特性を持つユーザおよびその他のアカウントで構成されます。たとえば、財務部門の全従業員で構成される財務グループなどです。

グループを説明に基づいて検索できます。ただし、[設定] ページにアクセスできる管理者は、グループエンティティを検索する際の基準となる属性をカスタマイズできます。つまり、グループに役割を割り当てているとき、リソースの所有者としてグループを作成しているとき、または[グループ] ページで単純検索を実行しているときに特定のグループを検索すると、結果として、検索された属性に一致するグループの名前が返されます。詳細については、『[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)』の「[Entity Settings](#)」を参照してください。

グループの作成

Identity アプリケーションに管理役割がある場合は、グループを作成できます。

- 1 Identity Manager ダッシュボードで、[人] > [グループ] に移動します。
- 2 [+] をクリックします。
- 3 次の属性 (必須) の値を指定します。

属性	指定する内容
名前	作成するグループに対するグループ名。 重要: [名前] フィールドには、次の特殊文字を使用しないでください。<;\"+#/ *~
説明	作成するグループの説明。説明は、ダッシュボードのグループ検索条件として使用されます。 重要: [説明] フィールドには、次の特殊文字を使用しないでください。 ~
コンテナ	作成するグループの格納先となる内の、部門 (部門によって命名されたグループ)。たとえば、次のような指定内容です。 ou=groups,ou=MyUnit,o=MyOrg コンテナ指定時に使用可能なボタンについては、 79 ページの「ユーザの作成」 を参照してください。 注: この種類のオブジェクトに対するデフォルトのコンテナがシステム管理者によって設定されている場合は、[コンテナ] の指定を要求されません。

- 4 [作成] をクリックします。

グループが正常に作成されると、[グループメンバー] パネルが表示され、新しく作成されたグループにユーザを追加できます。

- 5 グループにユーザを追加するには、グループメンバーの横にある [+] アイコンをクリックします。
- 6 モーダルウィンドウで必要なユーザを選択します。
- 7 [追加] をクリックします。

V 付録

次の付録には、Identity Manager ユーザアプリケーションに関する追加の参照情報と高度なトピックが記載されています。

A Identity Manager 承認アプリケーションの使用

Identity Manager のお客様が使用するユーザアプリケーションのユーザインタフェースに加えて、新しい iOS アプリケーションを使用できるようになりました。このアプリケーションを使用すると、Identity Manager ユーザは、Identity Manager の Roles Based Provisioning Module を介してリモートで要求を承認または拒否することができます。

承認アプリケーションをインストールして設定すると、ユーザアプリケーションのインタフェースに通常表示されるのと同じ承認タスクがそのアプリケーションに表示されます。すべての変更は、承認アプリケーションとユーザアプリケーションの間で同期されます。

Identity Manager Roles Based Provisioning Module サーバから切断されているときにオフラインモードで作業することもできます。接続を復元すると、承認アプリケーションにより、すべての変更が自動的に同期化されます。

この付録では、新しい承認アプリケーションのインストールと使用について説明します。ユーザがアプリケーションを使用できるように Identity Manager 管理者が環境を設定する方法については、『[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)』の「[Configuring the Identity Manager Approvals App](#)」を参照してください。

承認アプリケーションの詳細については、次の項を参照してください。

- [89 ページの「製品の要件」](#)
- [90 ページの「承認アプリケーションのインストール」](#)
- [90 ページの「承認アプリケーションの設定」](#)
- [94 ページの「承認アプリケーションの概要」](#)
- [97 ページの「承認アプリケーションの表示言語の変更」](#)

製品の要件

承認アプリケーションには、Apple iOS 6 または iOS 7 がインストールされた Apple iPhone または iPad、あるいは Android 5.0 以降がインストールされたデバイスが必要です。

注：管理者が承認アプリケーションの使用を有効にしていない場合、インストール後にそのアプリケーションを設定できないことがあります。承認アプリケーションを使用できるように管理者が Identity Manager 環境を設定する方法については、『[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)』の [Configuring the Identity Manager Approvals App](#) を参照してください。

承認アプリケーションのインストール

NetIQ Identity Manager 承認アプリケーションは、Apple App Store の[承認アプリケーションページ](#)からデバイスにインストールできます。

承認アプリケーションをインストールしたら、Roles Based Provisioning Module サーバと接続できるようにそのアプリケーションを設定する必要があります。

注: ユーザアプリケーションのパスワードが期限切れしている場合、パスワードを変更してから承認アプリケーションをインストールおよび設定することをお勧めします。ご使用の環境のパスワードポリシーで、パスワードが期限切れしたときの猶予ログイン回数が制限されている場合、承認アプリケーションは、Identity Manager タスクをデバイスに同期しようとして、それらのログイン回数をすべて使い果たしてしまうことがあります。

承認アプリケーションの設定

ご使用の環境ニーズや、管理者が Identity Manager をどのように設定しているかに応じて、さまざまな方法で NetIQ Identity Manager 承認アプリケーションを設定できます。

- 承認アプリケーションへのアクセス要求をユーザアプリケーションインタフェースで作成し、Identity Manager 管理者によって提供された電子メールリンクからデバイスでそのアプリケーションを起動します。このリンクには、必要な設定情報がすべて含まれています。
- デバイスを使用して設定リンクをクリックするか、設定 QR コードをスキャンします。リンクまたは QR コードによって、必要なすべての設定情報や会社の一般的な設定情報が提供されます。
- 承認アプリケーションで、ご使用の環境の設定情報を手入力します。

重要: ユーザがリンクまたは QR コードを使用して承認アプリケーションを自動的に設定できるようにするには、Identity Manager 環境の管理者が最初にリンクまたは QR コードを有効にする必要があります。

ユーザアプリケーションからのモバイルアクセスの要求

管理者が設定した場合、ユーザアプリケーションを使用して承認アプリケーションへのアクセスを要求できます。Identity Manager によって、カスタマイズされたリンクを含む電子メールが送信されます。その電子メールをデバイスで開くと、自分自身の情報でアプリケーションを自動的に設定できます。

ユーザアプリケーションからモバイルアクセスを要求するには、次の手順を実行します。

- 1 Web ブラウザで、HTTPS (https://) プロトコルを使用して Identity Manager ユーザアプリケーションにログインします。

注: 承認アプリケーションへのアクセスを要求するには、HTTPS プロトコルを使用してユーザアプリケーションにログインする必要があります。

- 2 [プロセス要求の作成] をクリックします。
- 3 [プロセス要求カテゴリ] ドロップダウンメニューをクリックし、[アカウント] を選択します。
- 4 [続行] をクリックします。
- 5 [モバイル承認アプリケーションの要求] をクリックします。

注：プロセス要求カテゴリと名前は、管理者が承認アプリケーションの要求プロセスをどのように設定しているかに応じて異なる場合があります。

- 6 必要な情報をプロセス要求フォームに入力し、[送信] をクリックします。
- 7 Identity Manager 管理者から電子メールを受信したら、その電子メールをデバイスで開き、提供されたリンクをクリックしてデバイスを Roles Based Provisioning Module サーバに接続します。

注：すでにアプリケーションをインストールしている場合、既存の設定が上書きされることを示す警告メッセージが表示されることがあります。警告メッセージに表示されているホスト名が、アプリケーションへのアクセス要求でアクセスしたホストと同じであることを確認してください。不明な場合はリンクをクリックしないで、管理者にお問い合わせください。

ホスト名が正しい場合は、[受諾] をクリックして既存の設定を上書きします。

- 8 アプリケーションが起動されたら、パスワードを入力し、[接続のテスト] アイコン



をクリックして設定を確認します。

設定リンクまたは QR コードの使用

Identity Manager 管理者から、承認アプリケーションを設定するための設定リンクが提供されることがあります。デバイスのブラウザでリンクを開くと、アプリケーションが自動的に設定されます。

ただし、このリンクで提供できるのは、必要な設定の一部のみです。通常、リンクまたはコードで提供できるのは、承認アプリケーションが機能するために必要な Roles Based Provisioning Module サーバの詳細のみです。リンクをクリックした後、ユーザ名やパスワードなど、自動的に設定されない情報を手動で設定する必要があります。

環境によっては、デバイスから電子メールにアクセスできない場合があります。デバイスで電子メールを受信できない場合は、Identity Manager 管理者から提供された、パーソナライズされた QR コードをデバイスでスキャンすることができます。

必要に応じて、提供された QR コードをコンピュータに表示するか、印刷し、デバイスの QR コードリーダーを使用してコードをスキャンしてください。ご使用の環境で使用できるように、QR コードによって承認アプリケーションが自動的に設定された後、ユーザ名とパスワードを手動で設定します。

承認アプリケーションの手動設定

承認アプリケーションの設定時に使用するリンクまたは QR コードが Identity Manager 環境の管理者から提供されなかった場合、必要な情報を手動で設定することもできます。

警告: デバイスでアプリケーションを手動設定するには Identity Manager コンポーネントについての詳しい知識が必要なので、社内の Roles Based Provisioning Module およびユーザアプリケーション環境に精通している上級ユーザのみがアプリケーションを手動で設定することをお勧めします。その他のユーザがアプリケーションを設定する場合は、Identity Manager 管理者にお問い合わせください。

アプリケーションで、[設定] アイコン  をクリックして必要な設定を指定し、[接続のテスト] アイコン  をクリックして設定を確認します。

承認アプリケーションを使用するには、次の設定が必要です。

ログイン設定の名前	ログイン設定の説明
Username	Roles Based Provisioning Module サーバへのアクセスに使用するユーザ名を指定します。
Password (パスワード)	Roles Based Provisioning Module サーバへのアクセスに使用するパスワードを指定します。
Data Sync (データ同期)	アプリケーションと Roles Based Provisioning Module サーバとの間でデータをアクティブに同期する場合に指定します。
[詳細] > [Server Details (サーバの詳細)] > [サーバ]	Roles Based Provisioning Module サーバの完全修飾ドメイン名または IP アドレスを指定します。
[詳細] > [Server Details (サーバの詳細)] > [Secure Port (セキュアポート)]	アプリケーションがサーバへの接続に使用する HTTPS ポートを指定します。
[詳細] > [Server Details (サーバの詳細)] > [コンテキスト]	ユーザアプリケーションの WAR ファイルをインストールする際に使用されるコンテキストを指定します。デフォルト値は IDMPProv です。
[詳細] > [Server Details (サーバの詳細)] > [ユーザコンテナ]	ユーザ情報を保存するアイデンティティボールドコンテナの完全 DN を指定します。
[詳細] > [Server Details (サーバの詳細)] > [タイムアウト]	サーバへの接続を試行する際、接続を取り消すまでにアプリケーションが待機する秒数を指定します。デフォルト値は 5 秒です。
[詳細] > [Data Definition Settings (データ定義設定)] > [User Entity (ユーザエンティティ)]	アイデンティティボールドでユーザを表す LDAP エンティティを指定します。デフォルト値は user です。
[詳細] > [Data Definition Settings (データ定義設定)] > [Name Format (名前書式)]	アプリケーションがユーザのフルネームの書式設定に使用する DAL 属性の表記を指定します。デフォルト値は FirstName LastName です。

ログイン設定の名前	ログイン設定の説明
[詳細] > [Data Definition Settings (データ定義設定)] > [First Name Attr (名属性)]	ユーザの名を表す DAL 属性の名前を指定します。デフォルト値は FirstName です。
[詳細] > [Data Definition Settings (データ定義設定)] > [Last Name Attr (姓属性)]	ユーザの姓を表す DAL 属性の名前を指定します。デフォルト値は LastName です。
[詳細] > [Data Definition Settings (データ定義設定)] > [User Photo Attr (ユーザ写真属性)]	ユーザの写真を格納する DAL 属性の名前を指定します。デフォルト値は UserPhoto です。 注 : Identity Manager で写真を設定していない場合や、写真を表示しないように Identity Manager を設定している場合は、代わりに汎用の画像が表示されます。
[詳細] > [Data Definition Settings (データ定義設定)] > [Work Phone Attr (勤務先電話番号属性)]	ユーザの勤務先電話番号を表す DAL 属性の名前を指定します。デフォルト値は TelephoneNumber です。
[詳細] > [Data Definition Settings (データ定義設定)] > [Mobile Phone Attr (携帯電話番号属性)]	ユーザの携帯電話番号を表す DAL 属性の名前を指定します。デフォルト値は mobile です。
[詳細] > [Data Definition Settings (データ定義設定)] > [Email Attr (電子メール属性)]	ユーザの電子メールアドレスを表す DAL 属性の名前を指定します。デフォルト値は Email です。
[詳細] > [Data Definition Settings (データ定義設定)] > [Photo LDAP Attr (写真 LDAP 属性)]	ユーザの写真を格納する LDAP 属性の名前を指定します。デフォルト値は photo です。
[詳細] > [Data Definition Settings (データ定義設定)] > [名前付け属性]	名前を表すためにアイデンティティボールドで使用される名前付け DAL 属性を指定します。デフォルト値は cn です。
[詳細] > [Data Definition Settings (データ定義設定)] > [Provisioning Admin (プロビジョニング管理者)]	Roles Based Provisioning Module サーバのプロビジョニング管理者であるかどうかを指定します。
[詳細] > [Accepted Certificates (受諾された証明書)]	承認アプリケーションで受諾されるようにする、Roles Based Provisioning Module サーバからの無効な証明書または自己署名証明書を指定します。 承認アプリケーションが自己署名証明書または無効な証明書を検出すると、証明書の受諾または拒否を確認するメッセージが表示されます。証明書を受諾すると、証明書が [Accepted Certificates (受諾された証明書)] リストに追加されます。[Accepted Certificates (受諾された証明書)] リストから証明書を削除するには、証明書の名前をクリックし、アプリケーションを再起動します。 注 : Roles Based Provisioning Module サーバ証明書が有効な場合、証明書は [Accepted Certificates (受諾された証明書)] リストに追加されません。有効な証明書はデフォルトで受諾されます。

ログイン設定の名前	ログイン設定の説明
[詳細] > [Rejected Certificates (拒否された証明書)]	承認アプリケーションで受諾されないようにする、Roles Based Provisioning Module サーバからの無効な証明書または自己署名証明書を指定します。 承認アプリケーションが自己署名証明書または無効な証明書を検出すると、証明書の受諾または拒否を確認するメッセージが表示されます。証明書を拒否すると、証明書が [Rejected Certificates (拒否された証明書)] リストに追加されます。拒否された証明書をサーバが提示した場合、アプリケーションはサーバへの接続を確立できません。 [Rejected Certificates (拒否された証明書)] リストから証明書を削除するには、証明書の名前をクリックします。

承認アプリケーションの概要

この項では、NetIQ Identity Manager 承認アプリケーションのユーザインタフェースの概要を説明します。主なトピックは次のとおりです。

- [94 ページの「\[タスク\] ビュー」](#)
- [95 ページの「詳細ビュー」](#)
- [95 ページの「Bulk Mode \(一括モード \)」](#)
- [96 ページの「\[Completed Tasks \(完了したタスク \)\] ビュー」](#)
- [96 ページの「\[ログイン設定\] ビュー」](#)
- [96 ページの「\[Advanced Settings \(詳細設定 \)\] ビュー」](#)

[タスク] ビュー

承認アプリケーションのデフォルトビューは [タスク] ビューです。このビューには、ユーザに現在割り当てられているタスク、またはユーザが所有するタスクがすべて表示されます。タスクのタイトル、およびタスク受信者の名前と写真も表示されます。タスクは有効期限に基づいて表示されます。有効期限が最も早いタスクが上位に、有効期限がないタスクが下位に表示されます。

注

- ユーザが Identity Manager で写真を設定していない場合や、写真を表示しないように Identity Manager を設定している場合は、代わりに汎用の画像が表示されます。

- 承認アプリケーションを使用して、複雑なフォームを使用しているタスクを承認または拒否することはできません。
- 現在は、iOS および Android プラットフォームの両方で、承認アプリケーションは新しい JSON フォームをサポートしていません。その結果、エラーメッセージが表示されるか、タスクの詳細を表示できない場合があります。

要求を承認または拒否する場合や、特定のタスクの詳細を表示する場合は、タスクまたはタスク受信者の名前をクリックします。タスク受信者に連絡するには、受信者の写真をクリックします。

詳細ビュー

[詳細] ビューには、ユーザに割り当てられている特定のタスクの詳細が表示されます。表示されるフィールドは、要求によって異なります。

タスクを承認または拒否するには、必要な情報を入力し、[承認] または [拒否] をクリックします。

Bulk Mode (一括モード)

類似する多数のタスクを承認または拒否する必要がある場合、[タスク] ビューでデフォルトの単一タスクモードから一括モードに切り替えることができます。

注: すべてのタスクを一括モードで承認することはできません。検証タスクのような、より複雑なタスクについては、各タスクを単一タスクモードで別個に承認する必要があります。[Bulk Mode (一括モード)] アイコンをクリックすると、一括モードで承認できるタスクのみがリストに表示されます。

複数のタスクを承認または拒否するには、次の手順を実行します。

- [タスク] ビューで、[Bulk Mode (一括モード)] アイコン  をクリックします。
- 承認または拒否するタスクを選択します。特定のタスクを承認しながら、同時にそれ以外のタスクを拒否することはできません。
- (オプション) すべてのタスクを承認または拒否するには、[すべて] をクリックします。
- (オプション) 考えが変わって、いずれかのタスクを承認または拒否しないようにするには、単一タスクモードのアイコン  をクリックします。
- [承認] または [拒否] をクリックします。
- (オプション) 一括操作に関するコメントを入力します。
- [Confirm (確認)] をクリックします。

[Completed Tasks (完了したタスク)] ビュー

完了したタスクを表示するには、[Completed Tasks (完了したタスク)] アイコン  をクリックします。このビューには、完了したタスクが、そのタスクが承認または拒否された時間とともに表示されます。完了したタスクをクリックすると、そのタスクの詳細を表示できます。より複雑な要求については、[Form Values (フォームの値)] をクリックして、要求に関する詳細情報を表示することができます。

必要に応じて、1 つまたは複数の完了したタスクを [Completed Tasks (完了したタスク)] ビューから削除できます。タスクを削除するには、[Bulk Mode (一括モード)] アイコン  をクリックし、削除するタスクを選択して、[削除] をクリックします。

注 : [Completed Tasks (完了したタスク)] ビューに表示されるのは、デバイスで完了したタスクのみです。ユーザアプリケーションや、承認アプリケーションがインストールされた別のデバイスで完了したタスクを表示することはできません。

[ログイン設定] ビュー

[ログイン設定] ビューでは、ログイン設定を表示したり、変更することができます。

警告 : アプリケーションを自動的に設定するためのリンクまたは QR コードが Identity Manager 管理者から提供された場合、管理者からの指示がない限り、デフォルトの設定を変更しないことをお勧めします。

[Advanced Settings (詳細設定)] ビュー

[Advanced Settings (詳細設定)] ビューでは、Roles Based Provisioning Module サーバからのデータ受信方法を決定する詳細な設定を表示したり、変更することができます。

警告 : アプリケーションを自動的に設定するためのリンクまたは QR コードが Identity Manager 管理者から提供された場合、管理者からの指示がない限り、デフォルトの設定を変更しないことをお勧めします。

[Advanced Settings (詳細設定)] ビューでデータ定義設定を誤って変更した場合は、[Restore Defaults (デフォルトに戻す)] クリックして、Identity Manager によって提供されたデフォルトの設定に戻してください。[Restore Defaults (デフォルトに戻す)] は、ユーザ名、パスワード、および [Server Details (サーバの詳細)] の設定は変更されません。

承認アプリケーションの表示言語の変更

承認アプリケーションには、複数の言語でローカライズされたテキスト文字列が用意されています。承認アプリケーションで使用する言語を変更するには、iOS デバイスで [言語] と [Region Format (地域に応じた書式)] の設定を変更します。[Region Format (地域に応じた書式)] の設定では、日付、時刻、および電話番号がデバイスでどのように表示されるかを設定します。

言語および地域の設定を変更するには、次の手順を実行します。

- 1 iOS デバイスで、[設定] をクリックします。
- 2 [一般] をクリックします。
- 3 [International (言語環境)] をクリックします。
- 4 (オプション) デバイスの使用言語を変更するには、[言語] をクリックして使用言語を選択してから、[完了] をクリックします。
- 5 (オプション) デバイスの日付や時刻の地域に応じた書式を変更するには、[Region Format (地域に応じた書式)] をクリックして使用する書式を選択してから、[International (言語環境)] をクリックします。
- 6 デバイスのホーム画面に戻ります。