

---

# Directory and Resource Administrator ユーザガイド

2018年9月

## 保証と著作権

© Copyright 2007-2018 Micro Focus or one of its affiliates.

Micro Focus、関連会社、およびライセンサ(「Micro Focus」)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。Micro Focus 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。

## 本書の内容 5

### 1 はじめに 7

1.1	Directory and Resource Administratorとは	7
1.2	Directory and Administratorのコンポーネントについて	8
1.2.1	DRA管理サーバ	8
1.2.2	Account and Resource Managementコンソール	8
1.2.3	Webコンソール	9
1.2.4	レポーティングコンポーネント	9
1.2.5	ワークフローエンジン	10
1.2.6	製品アーキテクチャ	11

### 2 ユーザインタフェースの使用 13

2.1	Webコンソール	13
2.1.1	Webコンソールの起動	13
2.1.2	Webコンソールの設定	14
2.1.3	Webコンソールのカスタマイズ	17
2.1.4	統合された変更履歴(UCH)	20
2.1.5	ユーザの変更履歴へのアクセス	20
2.1.6	自動ワークフロー	21
2.2	Account and Resource Managementコンソール	22
2.2.1	管理サーバまたは管理対象ドメインへの接続	23
2.2.2	コンソールのタイトル変更	23
2.2.3	リストの列のカスタマイズ	24
2.2.4	保存された高度なクエリの実行	24
2.2.5	コンソール設定の復元	25
2.2.6	特殊文字の使用	25
2.2.7	ワイルドカード文字の使用	26
2.2.8	割り当てられた権限と役割の表示	27
2.2.9	製品のバージョン番号とインストール済みのホットフィックスの表示	27
2.2.10	現在のライセンスの表示	28
2.2.11	BitLocker回復パスワード	28
2.3	DRA Reporting	29
2.3.1	DRA Reportingについて	30
2.3.2	DRAによるログアーカイブの使用	31
2.3.3	日付と時刻について	32
2.3.4	DRA Reportingタスク	32

### 3 ユーザアカウント、グループ、および連絡先の管理 37

3.1	ユーザアカウントの管理	37
3.1.1	信頼されたドメイン内のユーザアカウント	37
3.1.2	ユーザアカウントの管理タスク	37
3.1.3	ユーザアカウントの変換	40
3.2	グループを管理する	43
3.2.1	グループ管理タスク	43
3.2.2	一時グループの割り当て	45
3.3	ダイナミック配布グループの管理	46
3.4	ダイナミックグループの管理	48
3.5	連絡先を管理する	51

### 4 Exchangeのメールボックスとパブリックフォルダの管理 53

4.1	ユーザメールボックスの管理タスク	53
4.2	Office 365のメールボックスの管理タスク	56

4.3	リソースメールボックスの管理タスク . . . . .	56
4.4	共有メールボックスの管理タスク . . . . .	58
4.5	リンクされたメールボックスの管理タスク . . . . .	59
4.6	パブリックフォルダの管理タスク . . . . .	60
<b>5</b>	<b>リソースの管理</b>	<b>61</b>
5.1	部門(OU)の管理 . . . . .	61
5.2	コンピュータの管理 . . . . .	62
5.3	サービスの管理 . . . . .	63
5.4	プリンタとプリントジョブの管理 . . . . .	64
5.4.1	プリンタ管理タスク . . . . .	65
5.4.2	プリントジョブ管理タスク . . . . .	65
5.4.3	公開プリンタの管理タスク . . . . .	66
5.4.4	公開プリンタのプリントジョブ管理タスク . . . . .	67
5.5	共有の管理 . . . . .	68
5.6	接続ユーザの管理 . . . . .	68
5.7	デバイスを管理する . . . . .	69
5.8	イベントログの管理 . . . . .	69
5.8.1	イベントログの種類 . . . . .	69
5.8.2	イベントログ管理タスク . . . . .	70
5.9	オープンファイルの管理 . . . . .	71
<b>6</b>	<b>高度なクエリの管理</b>	<b>73</b>
<b>7</b>	<b>ごみ箱の管理</b>	<b>75</b>
<b>A</b>	<b>レガシのWebコンソールの使用</b>	<b>77</b>
A.1	レガシWebコンソールの起動 . . . . .	77
A.2	クイックスタートの使用による問題解決 . . . . .	77
A.3	レガシWebコンソールのカスタマイズ . . . . .	77

# 本書の内容

このユーザガイドでは、Directory and Resource Administratorという製品の概念について説明します。本書には、用語の定義および実装シナリオを記載しています。

## 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。

## その他のマニュアル

本書は、Directory and Resource Administratorのマニュアルセットの一部です。このリリースに対応する資料の一覧については、[Documentation Webサイト \(https://www.netiq.com/documentation/directory-and-resource-administrator-92/\)](https://www.netiq.com/documentation/directory-and-resource-administrator-92/)をご覧ください。

## セールスサポートへのお問い合わせ

製品、価格、および機能についてのご質問は、各地域のパートナーへお問い合わせください。パートナーに連絡できない場合は、弊社のセールスサポートチームへお問い合わせください。

各国共通:	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
米国およびカナダ:	1-888-323-6768
電子メール:	<a href="mailto:info@netiq.com">info@netiq.com</a>
Webサイト:	<a href="http://www.netiq.com">www.netiq.com</a>

## テクニカルサポートへのお問い合わせ

特定の製品に関する問題については、弊社のテクニカルサポートチームへお問い合わせください。

各国共通:	<a href="http://www.netiq.com/support/contactinfo.asp">www.netiq.com/support/contactinfo.asp</a>
北米および南米:	1-713-418-5555
ヨーロッパ、中東、アフリカ:	+353 (0) 91-782 677
電子メール:	<a href="mailto:support@netiq.com">support@netiq.com</a>
Webサイト:	<a href="http://www.netiq.com/support">www.netiq.com/support</a>

## マニュアルサポートへのお問い合わせ

弊社の目標は、お客様のニーズを満たすマニュアルの提供です。マニュアルを改善するための提案がございましたら、このマニュアルのHTML版で、各ページの下にある「[comment on this topic](#)」をクリックしてください。[Documentation-Feedback@netiq.com](mailto:Documentation-Feedback@netiq.com)宛てに電子メールを送信することもできます。貴重なご意見をぜひお寄せください。

## オンラインユーザコミュニティへのお問い合わせ

NetIQのオンラインコミュニティであるNetIQ Communitiesは、他のユーザやNetIQのエキスパートとやり取りできるコラボレーションネットワークです。NetIQ Communitiesでは、より迅速な情報、役立つリソースへの便利なリンク、およびNetIQエキスパートとのやり取りの場を提供しています。事業成功の鍵であるITへの投資効果を最大にするために必要な知識が確実に身につけられるよう手助けしています。詳細については、<http://community.netiq.com>を参照してください。

# 1 はじめに

Directory and Resource Administrator™(DRA)でActive Directoryのオブジェクト管理を始める前に、DRAの動作の基本理念と、製品アーキテクチャにおける各DRAコンポーネントの役割について理解しておく必要があります。

## 1.1 Directory and Resource Administratorとは

Directory and Resource Administratorは、Microsoft Active Directory(AD)の安全で効率的な特権ID管理を可能にします。DRAでは、「最小特権」を細かく委任することで、管理者およびユーザが特定の責務に必要なパーミッションだけが付与されるようにします。また、DRAは、ポリシーの遵守を徹底し、詳細なアクティビティの監査およびレポーティングを提供し、ITプロセスの自動化によって繰り返しの作業を簡素化します。これらの各機能により、特権昇格、エラー、悪意のあるアクティビティ、規制違反などのリスクから顧客のADおよびExchangeの環境を保護できるだけでなく、ユーザ、ビジネスマネージャ、ヘルプデスク担当者にセルフサービス機能を付与することで管理者の負担を軽減することができます。

Exchange管理者はDRAの強力な機能を活用して、Microsoft Exchangeをシームレスに管理することができます。また、単一の共通ユーザインタフェースを使用して、Exchange管理者はMicrosoft Exchange環境内のメールボックス、パブリックフォルダ、および配布リストをポリシーベースで管理することができます。

Active Directory、Microsoft Windows、Microsoft Exchange、およびMicrosoft Office 365の各環境の制御と管理に関する課題がDRAですべて解決できます。

- **Active Directory、Office 365、Exchange、およびSkype for Businessのサポート:** Active Directory、オンプレミスのExchange Server、オンプレミスのSkype for Business、Exchange Online、およびSkype for Business Onlineを管理できます。
- **ユーザおよび管理者の特権アクセスの細かい制御:** 特許取得済みのActiveViewテクノロジーにより、特定の責務に必要な権限だけを委任し、特権格上げを防止することができます。
- **カスタマイズ可能なWebコンソール:** 直観的な方法により、技術者でなくても、限定された(そして割り当てられた)機能および権限を通して、簡単かつ安全に管理タスクを行えます。
- **詳細なアクティビティの監査およびレポーティング:** 製品で実行されたすべてのアクティビティが包括的に監査レコードに記録されます。長期データを安全に保管でき、ADへのアクセスを制御するためのプロセスを実施していることを監査機関(PCDSS、FISMA、HIPAA、NERCIPなど)に証明できます。
- **ITプロセスの自動化:** プロビジョニングや認証の取り消し、ユーザとメールボックスの操作、ポリシーの適用、セルフサービスタスクの制御など、さまざまなタスクのワークフローを自動化できます。これにより、ビジネスの効率を高め、手動で繰り返し行う管理作業を削減することができます。
- **運用上の完全性:** 管理者にきめ細かいアクセスコントロールを提供し、システムおよびリソースへのアクセスを管理することで、システムおよびサービスのパフォーマンスと可用性に影響する悪意のある変更や間違った変更を防止できます。
- **プロセスの適用:** 重要な変更管理プロセスの完全性を維持し、生産性の向上、エラーの減少、時間の節約、管理効率の向上に貢献します。

- **Change Guardianとの統合:** DRAおよびワークフロー自動化機能とは無関係にActive Directoryで生成されたイベントの監査を強化します。

## 1.2 Directory and Administratorのコンポーネントについて

特権アクセスの管理に一貫して使用されるDRAのコンポーネントには、プライマリとセカンダリのサーバ、管理コンソール、レポートコンポーネント、およびワークフロープロセスを自動化するワークフローエンジンなどがあります。

次の表は、各タイプのDRAユーザが使用する典型的なユーザインタフェースと管理サーバを示しています。

DRAユーザのタイプ	ユーザインタフェース	管理サーバ
DRA管理者 (本製品の構成を管理する人)	Delegation and Configurationコンソール	プライマリサーバ
	DRA Reporting	セカンダリサーバ
	CLI	
	DRA ADSI Provider	
ヘルプデスクの臨時管理者	Account and Resource Managementコンソール	セカンダリサーバ
	Webコンソール	

### 1.2.1 DRA管理サーバ

DRA管理サーバは、構成データ(環境、委任されたアクセス、およびポリシー)を保管し、オペレータのタスクおよび自動化タスクを実行し、システム全体のアクティビティを監査します。このサーバは、コンソールおよびAPIレベルのクライアントをいくつかサポートしながらも、マルチマスタセット(MMS)のスケールアウトモデルにより、冗長性と地理的分離に対しても高い可用性を実現できるように設計されています。このモデルでは、すべてのDRA環境に、複数のセカンダリDRA管理サーバと同期する1つのプライマリDRA管理サーバが必要になります。

Active Directoryドメインコントローラには管理サーバをインストールしないようにすることを強くお勧めします。DRAが管理するドメインごとに、管理サーバと同じサイトにドメインコントローラを1つ以上配置してください。デフォルトでは、管理サーバはすべての読み込み/書き込み操作で最も近いドメインコントローラにアクセスします。そのため、パスワードリセットなどのサイト固有のタスクを実行する場合は、サイト固有のドメインコントローラを指定して操作を処理できます。ベストプラクティスとして、セカンダリ管理サーバ1台をレポーティング、バッチ処理、自動化されたワークロードのために専用で使用することを検討してください。

### 1.2.2 Account and Resource Managementコンソール

AccountandResourceManagementコンソールは、インストール可能なユーザインタフェースです。これを通じてDRAのアシスタント管理者が、接続されたドメインやサービスに関する委任されたオブジェクトを確認および管理することができます。



## 1.2.3 Webコンソール

Webコンソールは、Webベースのユーザインタフェースです。これを通じてDRAのアシスタント管理者が、接続されたドメインやサービスの委任オブジェクトを素早く簡単に確認し、管理することができます。

管理者は、Webコンソールの外観と使用方法をカスタマイズして、カスタマイズした企業ブランドとカスタマイズしたオブジェクトプロパティを組み込むことができます。また、DRAの外部で行われた変更監査を可能にするためにChange Guardianサーバとの統合を構成することもできます。

DRA管理者は、自動ワークフローフォームを作成および変更して、トリガされたときにルーチンの自動タスクを実行することもできます。

Webコンソールには「統合された変更履歴」という機能もあります。この機能により変更履歴サーバとの統合が可能になり、DRAの外部でADオブジェクトに対して行われた変更を監査することができます。変更履歴レポートのオプションには、次のものがあります。

- ◆ 次に対して行われた変更...
- ◆ 次によって行われた変更...
- ◆ 次によって作成されたメールボックス...
- ◆ 次によって作成されたユーザ、グループ、および連絡先の電子メールアドレス...
- ◆ 次によって削除されたユーザ、グループ、および連絡先の電子メールアドレス...
- ◆ 次によって作成された仮想属性...
- ◆ 次によって移動されたオブジェクト...

## 1.2.4 レポートینگコンポーネント

DRA ReportingにはDRA管理のためにカスタマイズ可能な標準のテンプレートが用意されており、DRA管理対象ドメインおよびシステムの詳細が確認できます。

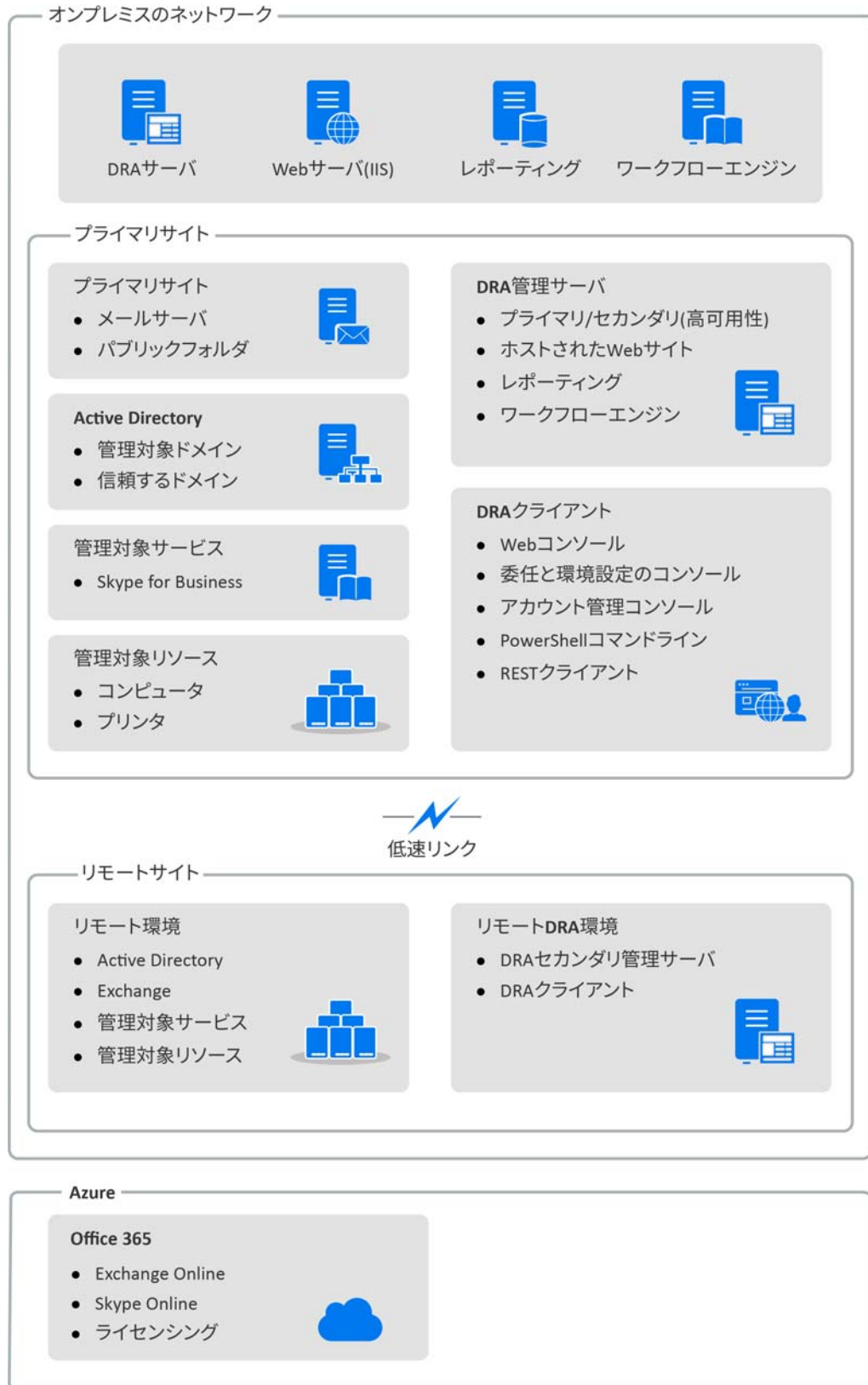
- ◆ ADオブジェクトのリソースレポート
- ◆ ADオブジェクトデータレポート
- ◆ ADサマリレポート
- ◆ DRA構成レポート
- ◆ Exchange構成レポート
- ◆ Office 365 Exchange Onlineレポート
- ◆ 詳細なアクティビティトレンドレポート(月別、ドメイン別、ピーク別)
- ◆ DRAアクティビティの要約レポート

DRAレポートは、SQL Server Reporting Servicesを使用してスケジュールおよび公開できるので、関係者に簡単に配布できます。

## 1.2.5 ワークフローエンジン

DRAには、Webコンソールでのワークフロータスクの自動化を可能にするワークフローエンジンが統合されています。Webコンソールを通じてアシスタント管理者がワークフローサーバの構成、カスタマイズされたワークフロー自動化フォームの実行、および各ワークフローの実行ステータスの表示を行うことができます。ワークフローエンジンについての詳細は、[DRAマニュアルサイト](#)でワークフロー自動化のマニュアルを参照してください。

## 1.2.6 製品アーキテクチャ



# 2 ユーザインタフェースの使用

DRAのユーザインタフェースはさまざまな管理ニーズに対応しています。主なインタフェースは次のとおりです。

## Webコンソール

Webベースのインタフェースを通じて、アカウントおよびリソースに関する一般的な管理タスクを行うことができます。Webコンソールには、Internet Explorer、Chrome、またはFirefoxを実行している任意のコンピュータからアクセスできます。

## Account and Resource Managementコンソール

任意の管理対象ドメイン内のオブジェクトが管理できます。AccountandResourceManagement (ARM)コンソールからは、アカウント、リソース、一時グループの指定、およびMicrosoft Exchangeのメールボックスを表示および変更することができます。このインタフェースは、基本的な管理からヘルプデスクに寄せられる高度な問題まで、企業の管理ニーズに応えることができます。

## PowerShell

PowerShellは、DRA以外のクライアントでもPowerShellのコマンドレットを使ってDRAの操作の要求を可能にするモジュールです。

## NetIQ Reporting Centerコンソール

管理レポートを表示し、展開することができます。これにより、企業セキュリティの監査および管理活動の追跡監視を行うことができます。管理レポートには、アクティビティレポート、環境設定レポート、および要約レポートなどがあります。これらのレポートは多くが図表形式で表示できます。

## 2.1 Webコンソール

Webコンソールは、ユーザアカウント、グループ、コンピュータ、リソース、Microsoft Exchangeメールボックスに関する多くのタスクにすばやく簡単にアクセスできるWebベースのユーザインタフェースです。オブジェクトのプロパティはカスタマイズ可能なため、繰り返し行う業務の効率を向上させることができます。また、所在地や携帯電話番号など、自分のユーザアカウントの一般プロパティを管理することもできます。

Webコンソールには、自分に実行権限があるタスクのみが表示されます。

### 2.1.1 Webコンソールの起動

WebコンソールはInternet Explorerを実行している任意のコンピュータから起動できます。Webコンソールを起動するには、Webブラウザのアドレスフィールドで適切なURLを指定してください。たとえば、HOUserverというコンピュータにWebコンポーネントをインストールした場合、Webブラウザのアドレスフィールドに「https://HOUserver.entDomain.com/draclient」と入力します。

---

注: アカウントおよびMicrosoft Exchangeの最新情報をWebコンソールに表示するには、キャッシュされたページが更新されていないかどうかをアクセスのたびにチェックするようにWebブラウザを設定してください。

---

## 2.1.2 Webコンソールの設定

適切な権限があれば、必要なサーバへの接続と統合、自動ログアウトの振る舞い、Advanced AuthenticationをすべてWebコンソールで設定することができます。

### 自動ログアウト

何もせずに時間が経過したらWebコンソールを自動的にログアウトするように時間を設定することができます。また、自動ログアウトしないように設定することもできます。

Webコンソールで自動ログアウトを設定するには、[管理] > [構成] > [自動ログアウト] の順に選択します。

### DRAサーバへの接続

Webコンソールにはログイン時のDRAサーバへの接続オプションが3つあり、そのうちの1つに設定することができます。

- ◆ 常にDRAサーバのデフォルトの場所を使用する([常に])
- ◆ DRAサーバのデフォルトの場所を常に使用しない([なし])
- ◆ 選択されている場合のみ、DRAサーバのデフォルトの場所を使用する([選択した場合のみ])

各オプションでのログイン時の振る舞いを以下に示します。

接続の設定	ログイン画面 - オプション	接続オプションの説明
常に	なし	オプションの設定が無効になります。
なし	自動ディスカバリの使用	DRAサーバを自動的に検出します。設定オプションはありません。
	特定のDRAサーバに接続する	ユーザがサーバとポートを設定します。
	特定のドメインを管理する DRAサーバに接続する	ユーザが管理対象ドメインを指定し、次の接続オプションから選択します。 <ul style="list-style-type: none"><li>◆ 自動ディスカバリの使用(指定のドメイン内)</li><li>◆ このドメインのプライマリサーバ</li><li>◆ DRAサーバの検索(指定のドメイン内)</li></ul>
選択した場合のみ	自動ディスカバリの使用	DRAサーバを自動的に検出します。設定オプションはありません。
	デフォルトのDRAサーバに接続する	デフォルトサーバが選択され、DRAサーバの設定は無効になっています。
	特定のDRAサーバに接続する	ユーザがサーバとポートを設定します。

接続の設定	ログイン画面 - オプション	接続オプションの説明
	特定のドメインを管理する DRAサーバに接続する	<p>ユーザが管理対象ドメインを指定し、次の接続オプションから選択します。</p> <ul style="list-style-type: none"> <li>◆ 自動ディスカバリの使用(指定のドメイン内)</li> <li>◆ このドメインのプライマリサーバ</li> <li>◆ DRAサーバの検索(指定のドメイン内)</li> </ul>

WebコンソールでDRAサーバの接続を設定するには、**[管理]** > **[構成]** > **[DRAサーバ接続]** の順に選択します。

## RESTサーバの接続

RESTサービスの接続の設定では、デフォルトのサーバの場所と接続タイムアウト(秒単位)などを設定します。Webコンソールには、ログイン時のRESTサービスへの接続オプションが3つあり、そのうちの1つに設定することができます。

- ◆ 常にRESTサービスのデフォルトの場所を使用する( **[常に]** )
- ◆ RESTサービスのデフォルトの場所を常に使用しない( **[なし]** )
- ◆ 選択されている場合のみ、RESTサービスのデフォルトの場所を使用する( **[選択した場合のみ]** )

各オプションでのログイン時の振る舞いを以下に示します。

接続の設定	ログイン画面 - オプション	接続オプションの説明
常に	なし	オプションの設定が無効になります。
なし	自動ディスカバリの使用	RESTサーバを自動で検出します。使用できる設定オプションはありません。
	特定のRESTサーバに接続する	ユーザがサーバとポートを設定します。
	特定のドメイン内のRESTサーバに接続する	<p>ユーザが管理対象ドメインを指定し、次の接続オプションから選択します。</p> <ul style="list-style-type: none"> <li>◆ 自動ディスカバリの使用(指定のドメイン内)</li> <li>◆ RESTサーバの検索(指定のドメイン内)</li> </ul>
選択した場合のみ	自動ディスカバリの使用	RESTサーバを自動で検出します。使用できる設定オプションはありません。
	デフォルトのRESTサーバに接続する	デフォルトのRESTサーバが選択され、RESTサーバの設定は無効になっています。
	特定のRESTサーバに接続する	ユーザがサーバとポートを設定します。
	特定のドメイン内のRESTサーバに接続する	<p>ユーザが管理対象ドメインを指定し、次の接続オプションから選択します。</p> <ul style="list-style-type: none"> <li>◆ 自動ディスカバリの使用(指定のドメイン内)</li> <li>◆ RESTサーバの検索(指定のドメイン内)</li> </ul>

WebコンソールでRESTサービスの接続を設定するには、[管理] > [構成] > [RESTサービス接続] の順に選択します。

## Advanced Authentication

Advanced Authenticationでは、ユーザ名とパスワードのみの単純な保護ではなく、多要素認証を使用することでより安全に機密情報を保護します。多要素認証とは、カテゴリの異なる資格情報に基づき、複数の認証方法でユーザが本人であることを確認することが求められる、コンピュータへのアクセスコントロールの1方式です。

DRA管理者がチェーンとイベントを構成した後に、必要な権限を持つユーザがWebコンソールにログインしてAdvanced Authenticationを有効にすることができます。認証が有効になると、Advanced Authenticationによる認証がすべてのユーザに求められ、その後にWebコンソールへのアクセス権が付与されます。

Advanced Authenticationを有効にするには、Webコンソールにログインし [管理] > [設定] > [Advanced Authentication] の順に選択します。[有効] チェックボックスを選択し、各フィールドの指示に従ってフォームを記入します。

Advanced Authenticationの詳細については、『*Directory and Resource Administrator管理者ガイド*』の「[認証](#)」を参照してください。

## 統合サーバ

DRAは自動ワークフローフォームへのアクセスを可能にするワークフロー自動化サーバと、統合された変更履歴(UCH)のレポートへのアクセスを可能にするChangeGuardianサーバに統合できます。必要な権限を持つユーザは、ワークフロー自動化サーバとの接続と、1つまたは複数のChangeGuardianサーバとの接続を設定することができます。

### ワークフロー自動化サーバの設定

DRAで自動ワークフローを使用するには、自動ワークフロー作成用のWindowsサーバにワークフローエンジンをインストールする必要があります。DRAへのワークフロー自動化サーバの統合はWebコンソールで設定されます。

ワークフロー自動化サーバを設定するには、Webコンソールにログインしてから、[管理] > [統合] > [ワークフローの自動化] の順に選択します。

### UCH (統合された変更履歴)サーバの設定

UCHサーバを設定するには:

- 1 Webコンソールを起動し、AAの資格情報を使用してログインします。
- 2 [管理] > [統合] > [統合された変更履歴] の順に選択し、[追加] アイコンをクリックします。
- 3 変更履歴の統合の設定で、UCHサーバ名またはIPアドレス、ポート番号、サーバタイプ、アクセス用アカウントの詳細を指定します。
- 4 サーバへの接続をテストし、[OK] をクリックして設定内容を保存します。
- 5 必要に応じてサーバを追加します。

## 2.1.3 Webコンソールのカスタマイズ

Webコンソール内のオブジェクトのプロパティとユーザインタフェースのブランディングをカスタマイズすることができます。プロパティを適切にカスタマイズすると、オブジェクト管理を伴うタスクの自動化に役立ちます。

### プロパティページのカスタマイズ

Active Directoryの管理の役割で使用するオブジェクトプロパティフォームをオブジェクトタイプごとにカスタマイズすることができます。たとえば、DRAに組み込まれているオブジェクトタイプに基づいた新しいオブジェクトページを作成しカスタマイズすることもできます。また、組み込みオブジェクトタイプに合わせてプロパティを変更することもできます。

プロパティオブジェクトはWebコンソールの「プロパティページ」リストに明確に定義されています。このリストを見れば、どのオブジェクトページが組み込み済みで、どの組み込みページがカスタマイズされ、どのページが組み込みではなく管理者によって作成されたかが簡単に識別できます。

### オブジェクトプロパティページのカスタマイズ

オブジェクトプロパティのフォームは、ページの追加または削除、既存のページやフィールドの変更、およびプロパティ属性のためのカスタムハンドラの作成といったカスタマイズを行うことができます。作成されたカスタムハンドラは、その設定方法によって、プロパティフィールドが変化したときか、クエリ実行のためのプロンプトに管理者が応答したときに、自動的に実行されます。

プロパティのページに表示されるオブジェクトのリストに関しては、オブジェクトタイプごとに「オブジェクトの作成」と「プロパティの編集」という2つの操作タイプが使用できます。これらは、Webクライアントで実行する主要な操作です。カスタマイズすることで、DRAでActive Directoryのオブジェクトを管理するときの作業効率と操作性を向上させることができます。

Webコンソールでオブジェクトプロパティページをカスタマイズするには:

- 1 「**カスタマイズ**」 > 「**プロパティページ**」の順に選択します。
- 2 「プロパティページ」のリストからオブジェクトと操作タイプ(作成または編集)を選択します。
- 3 「**編集**」ボタンをクリックします。✎
- 4 次のうち1つまたは複数の方法でオブジェクトプロパティのフォームをカスタマイズし、変更を適用します。
  - ◆ 新規にプロパティページを追加する(「**ページの追加**」)
  - ◆ プロパティページを選択し、そのページをカスタマイズする
    - ◆ ページ内の設定フィールドの順序を変える(↑ ↓)
    - ◆ フィールドまたはサブフィールドを編集する(✎)
    - ◆ 1つまたは複数のフィールドを追加する(+ または「**フィールドの追加**」)
    - ◆ 1つまたは複数のフィールドを削除する(✖)
  - ◆ スクリプト、メッセージボックス、クエリ(LDAP、DRA、REST)のいずれかを使用してプロパティのカスタムハンドラを作成する

カスタムハンドラの使用の詳細については、「**カスタムハンドラの追加**」を参照してください。





## カスタムハンドラの追加

カスタムハンドラは、プロパティ属性が互いに作用してワークフロータスクを完了するためにDRAで使用されます。たとえば、他のフィールド値のクエリ、値の更新、フィールドの読み込み専用状態の切り替え、および設定済み変数に基づいてフィールドを表示または非表示にするときにプロパティのカスタムハンドラが使用されます。

また、DRAではカスタムハンドラの作成が簡単です。選択可能なJavaScript (JS)マクロがいくつか用意されており、そのうちの1つをカスタムハンドラ作成検証プロセスで選ぶことができます。

### カスタムハンドラ作成の基本手順:


次の手順は、事前に選択済みのカスタムハンドラのページからの操作です。そこまで進むには、プロパティフィールドにある編集ボタン(  )からオブジェクトプロパティのカスタムハンドラにアクセスします。

- 1 [カスタムハンドラ] タブをクリックし、ページ(  )を有効にします。
- 2 ドロップダウンメニューからカスタムハンドラを選択して、実行時間を選択します。通常、実行時間には2番目か3番目のオプションを使用します。

---

**注:** 一般的にカスタムハンドラは1つで十分ですが、ハンドラ同士がリンクするようにスクリプト内のフロー制御を設定すれば複数のハンドラを使用することもできます。

---

- 3 その場合、このページに追加するカスタムハンドラごとに設定(  )する必要があります。設定オプションがハンドラの種類によって異なりますが、すべてのハンドラがJavaScriptから実行されます。

独自のVanilla JavaScriptエントリを作成したり、組み込みマクロを使用することもできます。

#### ◆ LDAPクエリまたはRESTクエリのハンドラ:


1. 静的な値を基にクエリを実行する場合、[接続情報] と [クエリパラメータ] を定義します。

クエリを動的にする場合、必須フィールドにプレースホルダのテキストを入力します。これはスクリプトの実行に必須です。スクリプトが仮の値を上書きします。

---

**注:** また、RESTクエリのヘッダとクッキーも設定できます。

---

2. [クエリ前アクション] で、マクロの種類として [グローバル]、[クエリ]、または [フォームフィールド] のいずれかを選択します。
3. ドロップダウンリストからマクロを選択し、マクロを挿入します(  挿入マクロ )。
4. 必要に応じて他のマクロを挿入し、必要な値を指定してスクリプトを完成させます。

例として、ユーザが入力したグループ名がActive Directoryにすでに存在しないことを、フォームが送信されたときに [クエリ前アクション] のスクリプトで検証します。

ユーザが入力した名前を使用してLDAPクエリを作成する必要があります。Field() というマクロを使用して名前フィールドの値にアクセスし、クエリ文字列を作ります。次にこれを、Filter() マクロを使用するクエリフィルタに設定します。

```
Filter() = '(&(objectCategory=group)(objectClass=group)(name=' + Field(name) + '))';
```

5. 前の例を実行して、[クエリ後アクション] でクエリの返す結果をチェックします。結果はクエリに一致したオブジェクトの配列として返されます。そこで、配列の長さが0より大きいかどうかを調べる必要があります。

一致するグループが見つかったら、Cancel()というマクロを使用してフォーム送信をキャンセルし、そのマクロにユーザに表示するオプションメッセージを渡します。

```
if (QueryResults().length > 0) { Cancel('その名前のグループはすでに存在します。固有の名前を入力してください');}
```

- ◆ **スクリプト:** JavaScriptのカスタムコードを挿入するか、マクロを使用してスクリプトを作成します。
  - ◆ **DRAクエリ:** クエリパラメータについては、JSON形式でペイロードを定義します。そして、前に説明したLDAPクエリとRESTクエリの場合と同様の方法でマクロを使用します。
  - ◆ **メッセージボックスハンドラ:** メッセージボックス自体のプロパティを定義した後、前に説明したLDAPクエリとRESTクエリの場合と同様の方法でマクロを使用します。ただし、ここではクエリ前アクションとクエリ後アクションではなく、表示前のアクションと閉じた後のアクションのマクロスクリプトを作成します。
- 4 フォームを保存する前に[ハンドラのテスト]をクリックしてスクリプトを検証します。  
これによりテスト結果の概要が生成され、それで実行結果が確認できます。

---

**注:** ハンドラがフォームの現在の状態に依存する(たとえばフィールドに値がある)場合、正常に実行されません。これはフォーム編集時にデータがロードされていないためです。この場合は、フォームエディタの外部でハンドラをテストする必要があります。つまり、カスタマイズ内容を保存し、適切なフォームに移動し、必要なデータを入力してテストします。

---

## オブジェクトプロパティページの新規作成

オブジェクトプロパティページを新規に作成するには:

- 1 Webコンソールにログインし [カスタマイズ] > [プロパティページ] を選択します。
- 2 [タスク] 中の [新しいアクションの作成] をクリックします。
- 3 名前、アイコン、オブジェクトタイプ、操作の設定を定義して最初のオブジェクトプロパティフォームを作成します。
- 4 必要に応じて、その新規のフォームをカスタマイズします。「[オブジェクトプロパティページのカスタマイズ](#)」を参照してください。

## ユーザインタフェースのブランディングのカスタマイズ

DRAのWebコンソールのタイトルバーを独自のタイトルやロゴイメージにしてカスタマイズすることができます。位置はDRAの製品名の右隣りです。この位置は最上位のナビゲーションにも使用されるため、ログインするとDRAの最上位のナビゲーションリンクに隠れます。ただし、ブラウザのタブにはカスタマイズされたタイトルが引き続き表示されます。

DRAでタイトルのブランディングをカスタマイズするには:

- 1 Webコンソールにログインし、[カスタマイズ] > [ブランディング] の順に選択します。
- 2 会社のロゴを追加するには、ロゴイメージをWebサーバのcomponents/libbingに保存します。
- 3 ブランディングのカスタマイズのページの3つのフィールドに該当する情報があれば、必要な情報を追加して変更内容を保存します。

## 2.1.4 統合された変更履歴(UCH)

UCHサーバの設定方法の詳細については、「[UCH \(統合された変更履歴\)サーバの設定](#)」を参照してください。

### 統合された変更履歴のレポートの検索と生成

統合された変更履歴のすべてのレポートから検索することも、検索オプションを使用して検索対象を絞り込むこともできます。UCHレポートはWebコンソールにのみ表示できます。パラメータなしで検索すると、すべてのUCHレポートが一覧表示されます。検索パラメータを追加すると、必要なレポートのみを検索結果に表示するフィルタとして機能します。

---

**重要:** UCHレポートを生成するには、**Generate UI Reports**という権限を持つ必要があります。

---

統合された変更履歴のレポートを検索し生成するには:

- 1 Webコンソールを起動します。
- 2 **[管理] > [検索]** の順に選択します。
- 3 検索を実行します。名前、場所、子コンテナなど検索条件を付加しても、しなくても構いません。  
検索条件をまったく使用しないと、すべてのオブジェクトの検索結果が表示されることになります。結果を絞り込むために検索条件を含めます。
- 4 **[検索]** アイコンをクリックして、検索結果を表示します。
- 5 生成するレポートに含める必要のあるオブジェクトを選択します。
- 6 **[変更履歴レポートの表示]** アイコンをクリックします。  
**[変更履歴レポートの条件]** で、レポートの種類、ターゲットオブジェクト、開始日、終了日、最大行数、サーバ(DRAまたはChange Guardianサーバ)などの条件を使用してレポートを編集および生成することができます。
- 7 **[生成]** をクリックすると、監査データにアクセスしてUCHレポートを生成します。
- 8 レポートは、ソートしたり、CSVやHTMLなどの必要な形式でエクスポートすることができます。

### 統合された変更履歴のプロパティの表示

UCHの構成済みサーバのプロパティを表示するには、**[管理] > [統合] > [統合された変更履歴]** の順に選択し、構成したサーバを選択してから、**[オプション]** メニューをクリックし、次のアクションのいずれかを実行します。

- **プロパティ:** UCHプロパティを表示し更新します。
- **接続のテスト:** サーバへの接続を検証します。
- **削除:** 設定済みのUCHサーバを削除します。

## 2.1.5 ユーザの変更履歴へのアクセス

Webコンソールを使用して、ユーザに加えられた変更やユーザが加えた変更の履歴を確認することができます。次のタイプの変更内容を表示できます。

- ユーザが行った変更

- ユーザに行われた変更
- ユーザが作成したユーザのメールボックス
- ユーザが削除したユーザのメールボックス
- ユーザが設定したグループおよび連絡先電子メールアドレス
- ユーザが削除したグループおよび連絡先電子メールアドレス
- ユーザが作成または無効化した仮想属性
- ユーザが移動したオブジェクト

**変更履歴レポートを表示または生成するには:**

- 1 Webコンソールを起動します。
- 2 履歴を確認したいオブジェクトを検索します。
- 3 **「変更履歴レポートの表示」** アイコンをクリックします。
- 4 レポート生成の条件を変更するには、**「変更」** をクリックします。  
開始日または終了日、追跡されているオブジェクト、レポートの種類、およびその他の条件を変更することができます。
- 5 レポートのCSVファイルを作成するには、**「生成」** をクリックします。

## 2.1.6 自動ワークフロー

ワークフローの自動化を使うと、ワークフローフォームを起動することでITプロセスを自動化することができます。ワークフローフォームは、ワークフローを実行したとき、またはワークフロー自動化サーバで作成された名前付きワークフローイベントが発生したときに実行されます。

ワークフローのフォームは、その作成時または変更時にWebサーバに保存されます。このサーバのWebコンソールにログオンするときに、委任された権限とフォームの構成方法に基づいてフォームが利用できます。フォームはWebサーバの資格情報を持つすべてのユーザが利用できます。フォームを送信するには適切な権限が必要です。

**ワークフローフォームを起動するには:** ワークフローは、Webコンソール経由でDRAと統合されたワークフロー自動化サーバ内に作成されます。新しいフォームを保存するには、フォームのプロパティで設定される**「イベントによるワークフローのトリガ」**または**「特定のワークフローの起動」**のいずれかのオプションが必要です。これらのオプションに関する詳細は以下のとおりです。

- **特定のワークフローの起動:** このオプションでは、DRAのワークフローサーバで稼働中の利用可能なワークフローをすべてリストで表示します。このリストに表示されるためには、ワークフローがワークフロー自動化サーバ内のDRA\_Workflowsというフォルダに作成される必要があります。
- **イベントによるワークフローのトリガ:** このオプションは、事前に定義されたトリガでワークフローを実行するために使用されます。トリガを用いるワークフローもワークフロー自動化サーバ内に作成されます。

---

**注:** **「特定のワークフローの起動」** で設定したワークフローフォームのみ実行履歴が付きます。履歴に対しては、**「管理」** > **「要求」** からアクセスする検索のメインの表示枠内からクエリを行うことができます。

---

ワークフロー自動化の詳細については、『*Directory and Resource Administrator 管理者ガイド*』を参照してください。

## 2.2 Account and Resource Managementコンソール

AccountandResourceManagementコンソールは、DRAのアシスタント管理者が行うタスクのほとんどに対応します。基本的なシステム管理から高度なヘルプデスクでの問題まで企業の管理ニーズを満たします。AccountandResourceManagementコンソールからは、アカウントおよびリソースの管理タスクを実行したり、Microsoft Exchangeのメールボックスを管理することができます。

Account and Resource Managementコンソールには、次のノードが含まれています。

### すべての管理対象オブジェクト

ユーザアカウント、グループ、連絡先、リソース、ダイナミックグループ、ダイナミック配布グループ、リソースのメールボックス、パブリックフォルダなど、操作権限のあるドメインの中のオブジェクトが管理できます。

### 一時グループの割り当て

特定の期間だけグループメンバーシップを必要とするユーザのためのグループメンバーシップが管理できます。

### 詳細検索クエリ

管理サーバで使用可能な高度なクエリが管理できます。

### ごみ箱

ごみ箱が有効になっているすべてのMicrosoft Windowsドメインに関し、削除されたユーザアカウント、グループ、連絡先、およびリソースが管理できます。

Account and Resource Managementコンソールのインタフェースを起動するには、Directory and Resource Administratorのプログラムフォルダ内の**Account and Resource Management**をクリックします。

AccountandResourceManagementコンソールを起動すると、ローカルドメイン内で利用できる最善な管理サーバに初期接続します。利用できる最善なAdministrationサーバは最も近くにあるサーバです。一般的にそれはネットワークサイト内のサーバです。DRAは、利用できる最善な管理サーバを探すことで、接続スピードとパフォーマンスを向上させています。

AccountandResourceManagementコンソールからは、次に挙げる共通ユーザインタフェースタスクが実行できます。

## 2.2.1 管理サーバまたは管理対象ドメインへの接続

デフォルトでDRAは、管理対象のドメインまたはコンピュータの管理サーバのうち、利用できる最善なものに接続します。利用できる最善なAdministrationサーバは最も近くにあるサーバです。一般的にそれはネットワークサイト内のサーバです。サイト内に管理サーバがない場合、DRAはその次に最も利用可能なサーバを管理対象ドメインまたは管理対象サブツリー内から探して接続します。また、接続先の管理サーバまたはドメインを指定することもできます。

ユーザインタフェースを最初に起動すると、DRAはまず、その起動に使用されたログオンアカウントのドメインに接続します。管理サーバの管理していないドメインにログオンしている場合や、DRAがそのドメインの管理サーバに接続できない場合は、DRAがエラーメッセージを表示することがあります。管理サーバが利用可能であることを確認して、再試行します。

管理サーバに接続には:

- 1 [ファイル] メニューから [Connect to DRA server (DRAサーバに接続する★)] をクリックします。
- 2 [Connect to this DRA server (このDRAサーバに接続する★)] をクリックします。
- 3 管理サーバの名前を入力します。入力形式: *computername*
- 4 [OK] をクリックします。

管理対象のドメインまたはコンピュータに接続するには:

- 1 [ファイル] メニューから [Connect to DRA server (DRAサーバに接続する★)] をクリックします。
- 2 適切なオプションを選択してから、管理対象のドメインまたはコンピュータの名前を入力します。
- 3 たとえば、HOULABというドメインに接続するには、[Connect to a DRA server that manages this domain (このドメインを管理するDRAサーバに接続する★)] をクリックしてから、「HOULAB」と入力します。
- 4 管理対象のドメインまたはコンピュータの管理サーバを指定するには、[Advanced (詳細設定★)] をクリックしてから、適切なオプションを選択します。
- 5 [OK] をクリックします。

## 2.2.2 コンソールのタイトル変更

Account and Resource Management コンソールのタイトルバーは、そこに表示される情報を変更することができます。便利さと明確さを向上させるために、コンソール起動時のユーザ名や、コンソール接続先の管理サーバを追加することができます。また、複数の管理サーバに異なる資格情報を使用して接続する必要のある複雑な環境では、この機能を応用することで、今どのコンソールを使用すべきかがすぐに判別できるようになります。

コンソールのタイトルバーを変更するには:

- 1 Account and Resource Management コンソールを起動します。
- 2 [表示] > [オプション] の順にクリックします。
- 3 [Window Title (ウィンドウタイトル★)] タブを選択します。
- 4 適切なオプションを指定してから、[OK] をクリックします。



## 2.2.3 リストの列のカスタマイズ

どのオブジェクトプロパティをDRAのリストカラムに表示させるかを選択することができます。この柔軟性のある機能により、検索結果のリスト表示などのユーザインタフェースをカスタマイズでき、企業のシステム管理における特定のニーズを満たすことができます。たとえば、カラムにユーザのログオン名またはグループの種類を表示されるよう設定できます。これにより、必要なデータを迅速かつ効率的に特定しソートすることができます。

リストカラムをカスタマイズするには:

- 1 適切なノードを選択します。たとえば、管理対象オブジェクトに関する検索結果を表示する場合に、結果を表示させるカラムを選択するには、**[すべての管理対象オブジェクト]**を選択します。
- 2 **[表示]**メニューから**[Choose Columns (カラムを選択★)]**をクリックします。
- 3 このノードで使用可能なプロパティのリストから、表示するオブジェクトプロパティを選択します。
- 4 カラムの順序を変更するには、カラムを選択し、**[上に移動]**または**[下に移動]**をクリックします。
- 5 カラムの幅を指定するには、カラムを選択し、所定のフィールドに適切なピクセル数を入力します。
- 6 **[OK]**をクリックします。

## 2.2.4 保存された高度なクエリの実行

高度なクエリを使用すると、ユーザ、連絡先、グループ、コンピュータ、プリンタ、OUIはもとより、DRAがサポートするオブジェクトならすべて検索することができます。「Execute Saved AdvancedQuery」という権限があれば、AccountandResourceManagementのノード内のどのコンテナに対しても**[Saved Queries (保存済みクエリ★)]**リストで利用可能な高度なクエリを実行できます。自分に割り当てられた権限の詳細については、「**割り当てられた権限と役割の表示**」を参照してください。

保存済みの高度なクエリを実行するには:

- 1 **[Account and Resource Management]** > **[すべての管理対象オブジェクト]**の順に開きます。
- 2 適切なコンテナを選択します。たとえば、DRAにユーザアカウント情報を検索させたい場合、**[ユーザ]**を選択します。
- 3 詳細検索の表示枠を表示するには、**[Advanced Search (詳細検索★)]**をクリックします。
- 4 詳細検索の表示枠内の**[Saved Queries (保存済みクエリ★)]**リストから高度なクエリを1つ選択します。
- 5 **[Load Query (クエリをロード★)]**をクリックして、**[Find Now (今すぐ検索★)]**をクリックします。

## 2.2.5 コンソール設定の復元

DRAでは、ウィンドウサイズの変更とウィンドウサイズの保持が可能です。この他にもDRAは、前回接続した管理サーバ、リスト結果から追加または削除されたカラム、カラムの幅など、多くの設定を保持します。これらの設定をDRAインストール直後の設定に戻す必要が生じた場合、[Restore Default Settings (デフォルトの設定に復元★)] というオプションを使用すれば戻すことができます。

デフォルトのコンソール設定に復元するには:

- 1 [表示] > [オプション] の順にクリックします。
- 2 [Saved Settings (保存済みの設定★)] タブを選択します。
- 3 ウィンドウに表示される情報を確認してから、[Restore Default Settings (デフォルトの設定に復元★)] をクリックします。

## 2.2.6 特殊文字の使用

ユーザアカウント、グループ、連絡先、OU、コンピュータ、ActiveView、AAグループ、役割、ポリシー、または自動化トリガに名前を付ける場合、次に挙げる特殊文字は名前に使用できません。これらの命名制限は、オブジェクト名にも、オブジェクトを定義するルールの名前にも適用されます。

### ユーザアカウント、グループ、コンピュータの命名

Windows 2000以前の名前を指定する場合、次に挙げる特殊文字が使用できません。

円記号	\
コロン	:
カンマ	,
二重引用符	"
等号(=)	=
スラッシュ(/)	/
大なり記号	>
左角カッコ	[
小なり記号	<
プラス記号(+)	+
右角カッコ	]
セミコロン	;
縦線	

**重要:** パブリックフォルダ管理にはバックスラッシュ(\)文字がサポートされていません。



ユーザアカウント、グループ、およびMicrosoft Windowsドメイン内のコンピュータに名前を付ける場合は、任意の特殊文字が使用できます。

### 連絡先とOUの命名

連絡先やOUに名前を付ける場合、任意の特殊文字が使用できます。

### Activeview、AAグループ、役割の命名

ActiveViews、AAグループ、および役割に名前を付ける場合、バックスラッシュ(\)が使用できません。

### ポリシーと自動化トリガの命名

ポリシーおよび自動化トリガに名前を付ける場合は、バックスラッシュ(\)が使用できません。

### Office 365のメールボックスで無効な文字

無効な文字を使用すると、Office 365と企業内システムのディレクトリとの同期が失敗する原因となります。使用できない文字の詳細については、Microsoft OfficeサポートのWebサイトにアクセスし、「[Directory object and attribute preparation \(ディレクトリ オブジェクトと属性の準備★\)](#)」というサブトピックを参照してください。

オンラインメールボックスのプロパティにこれらの文字が使用されていないことを確認するには、Policy and Automation Managementコンソールに移動して、[[Configure Exchange Policies \(Exchangeポリシーを構成★\)](#)] をクリックします。[[Office 365 Rules](#)] をクリックし、[[Enforce online mailbox policies for invalid characters and character length](#)] をクリックして、[OK] をクリックします。

## 2.2.7 ワイルドカード文字の使用

DRAでは、CLIコマンドとDRAコンソールの多くのフィールドでワイルドカード文字が使用できます。ワイルドカードを使って、複数のオブジェクトを特定の条件または規格(命名規則など)に一致させるルールを定義することができます。ルールの範囲を広げたり絞り込む場合、正規表現の代わりにワイルドカードが使用できます。ワイルドカードの照合では大文字と小文字を区別しません。疑問符(?)、アスタリスク(\*)、番号記号(#)といったワイルドカード文字の直前に円記号(\)を付けることで、そのワイルドカード文字を通常の文字として使用することもできます。たとえば、「abc\*」を検索するには、検索文字列として「abc\\*」を入力します。

DRAでは、次に示すワイルドカード文字が使用できます。ワイルドカード文字を名前に使用することはできません。

一致項目	文字	定義
任意の文字	疑問符(?)	1文字とだけ一致する
任意の桁	シャープ記号(#)	1桁一致
任意の文字、0個以上の一致	アスタリスク(*)	一致する文字がないか複数の文字と一致する

次の表に、ワイルドカード文字による指定例とそれぞれで一致する例と一致しない例を示します。

例	一致する	一致しない
Den???	Denton and Dennis	Denison

例	一致する	一致しない
El ????o	El Campo and El Indio	El Paso
Houston, TX #####	Houston, TX 77024	Houston, TX USOFA

DRAは論理演算子を含むワイルドカード指定をサポートしません。

## 2.2.8 割り当てられた権限と役割の表示

役割と権限によってオブジェクトの管理方法が決まります。役割とは、特定の管理タスク(ユーザーアカウントの作成や共有ディレクトリの移動など)を実行するために必要なパーミッションを提供する権限のセットです。

DRA管理者がユーザに役割を割り振り、特定のAAグループに追加し、ActiveView (管理可能なドメインオブジェクトのセット)に関連付けます。これらの割り当ては、Account and Resource Managementコンソールで確認することができます。自分に割り当てられた役割と権限を確認するために補助的な権限は必要ありません。

割り当てられた権限と役割を表示するには:

- 1 [ファイル] メニューから [DRA Properties (DRAプロパティ★)] をクリックします。
- 2 [権限] をクリックします。
- 3 適切なビューを選択します。たとえば、AAグループのメンバーシップ、各メンバーの権限と役割、および関連付けられたActiveViewで構成されるテーブルを表示するには、[Flat View (フラット表示★)] をクリックします。
- 4 適切な項目を開きます。たとえば、「HasPower」という列で [RolesandPowers(役割と権限★)] を開いて個々の役割と権限を表示します。
- 5 [OK] をクリックします。

## 2.2.9 製品のバージョン番号とインストール済みのホットフィックスの表示

製品のバージョン番号とインストール済みのホットフィックスを [DRA Properties (DRAプロパティ★)] ウィンドウに表示できます。このウィンドウには、管理サーバーとDRAのクライアントコンピュータに関するインストール済みのホットフィックスの一覧とバージョン番号が表示されます。

製品のバージョン番号とインストール済みのホットフィックスを表示するには:

- 1 [ファイル] メニューから [DRA Properties (DRAプロパティ★)] をクリックします。
- 2 [全般] をクリックします。
- 3 必要な情報を確認します。
- 4 [OK] をクリックします。

## 2.2.10 現在のライセンスの表示

DRAにはライセンスキーファイルが必要です。製品のライセンスを任意の管理サーバのコンピュータから確認することができます。製品のライセンスの確認をするために特別な権限は必要ありません。

自分のライセンスを表示するには:

- 1 [ファイル] メニューから [DRA Properties (DRAプロパティ★)] をクリックします。
- 2 [ライセンス] をクリックします。
- 3 ライセンスのプロパティを確認したら [OK] をクリックします。

## 2.2.11 BitLocker回復パスワード

Microsoft BitLockerでは、Active Directoryに回復パスワードを格納しています。必要な権限を持つユーザなら、DRAのBitLocker回復機能を使用してエンドユーザの紛失したBitLockerパスワードを検索し回復することができます。

---

**重要:** BitLocker回復パスワードの機能を使用する前に、自分のコンピュータがドメインに割り当てられ、BitLockerがオンになっているか確認してください。

---

### BitLocker回復パスワードの表示とコピー

コンピュータのBitLockerパスワードが失われた場合、Active Directoryでそのコンピュータのプロパティから回復用パスワードのキーを入手し、それを使用してリセットすることができます。そのパスワードキーをコピーし、エンドユーザに渡してください。

回復用パスワードを表示しコピーするには:

- 1 Account and Resource Management コンソールを起動し、[すべての管理対象オブジェクト] > [ドメイン] > [コンピュータ] の順に選択します。
- 2 コンピュータのリストから回復が必要なコンピュータを右クリックし、[プロパティ] > [BitLocker回復パスワード] の順に選択します。
- 3 右クリックしてBitLocker回復パスワードをコピーし、パスワードのテキストをテキストファイルに貼り付けます。

### 回復用パスワードの検索

コンピュータ名が変更されていた場合、パスワードIDの先頭から8文字を使ってそのドメインで回復用パスワードを検索する必要があります。

パスワードIDを使用して回復用パスワードを検索するには:

- 1 Account and Resource Management コンソールを起動し、[すべての管理対象オブジェクト] を表示させます。
- 2 右クリックし、[管理対象ドメイン] を右クリックしてから、[BitLocker回復パスワードの検索] をクリックします。

回復用パスワードの先頭から8文字を検索する方法については、「[BitLocker回復パスワードの表示とコピー](#)」を参照してください。

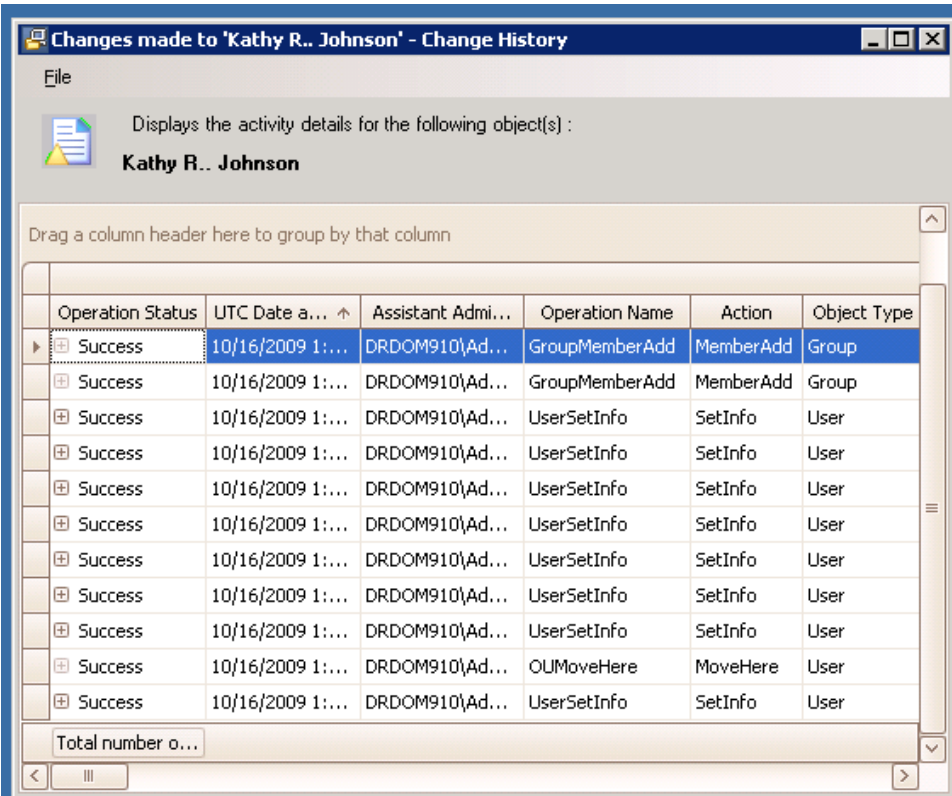
- 3 [BitLocker回復パスワードの検索] のページで、コピーした文字を検索フィールドに貼り付けてから [検索] クリックします。

## 2.3 DRA Reporting

DRAReportingは、すぐに利用できる組み込みのレポート機能です。これを使用して、重複アカウント、アカウントの直近のログオン、Microsoft Exchangeメールボックスの詳細など、多くの内容を迅速に追跡することができます。また、Reportingは、変更前と変更後のプロパティの値を含め、使用中の環境に加えられた変更の詳細をリアルタイムに提供します。レポートをエクスポート、印刷、表示でき、SQL Serverのレポーティングサービスにレポートを発行することもできます。

DRAには、ユーザアカウント、グループ、およびドメイン内のリソース定義を収集し確認できるレポートの生成方法が2つあります。**Activity Detailレポート**は、Delegation and Configurationコンソールに表示され、ドメイン内のオブジェクトに関する変更情報がリアルタイムに確認できます。たとえば、Activity Detailレポートを使用すれば、指定した期間中にオブジェクトに対して加えられた変更またはオブジェクトが加えた変更のリストを表示できます。

次の図にActivity Detailレポートのサンプルを示します。



Operation Status	UTC Date a...	Assistant Admi...	Operation Name	Action	Object Type
Success	10/16/2009 1:...	DRDOM910\Ad...	GroupMemberAdd	MemberAdd	Group
Success	10/16/2009 1:...	DRDOM910\Ad...	GroupMemberAdd	MemberAdd	Group
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	OU Move Here	Move Here	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User

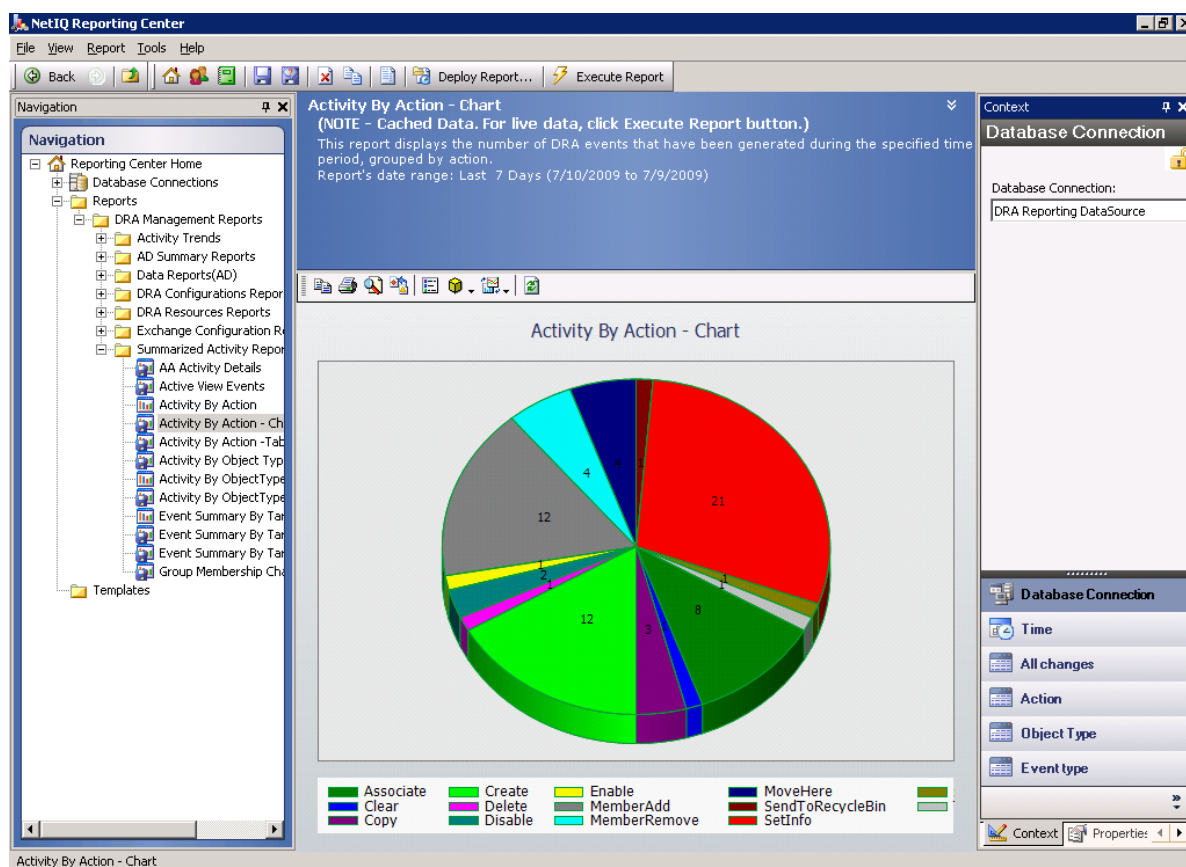
オプションの**DRA管理レポート**は、NetIQ Reporting Center (レポーティングセンター)に表示でき、管理対象ドメイン内のイベントに関する情報の要約、構成、およびアクティビティが確認できます。管理レポートの中にはデータがグラフ表示できるものがあります。これらの組み込みレポートは、必要とされる情報が正確に得られるようにカスタマイズすることもできます。

たとえば、管理レポートを使用して、指定した期間中の各管理対象ドメインにおけるイベントの数をグラフで表示することができます。Reportingでは、ActiveViewの定義やAAグループの定義など、DRAのセキュリティモデルに関する詳細が表示できます。

これらのレポートを表示するには、事前にオプションの管理レポートをインストールし構成しておく必要があります。レポーティングコンポーネントのインストールの詳細については、『インストールガイド』を参照してくださいDRAのレポート機能の詳細については、「[29 ページの「DRA Reporting」](#)」を参照してください。

NetIQ > Reporting Centerプログラムグループの中にあるReporting Centerコンソールを起動します。

次の図は、DRA管理レポートが選択されたときのReporting Centerのインターフェースを示しています。



## 2.3.1 DRA Reportingについて

DRA Reportingにはレポート生成方法が2つあり、使用中の環境で最近変更された内容を確認するレポートと、ドメイン内のユーザアカウント、グループ、およびリソースの定義を収集し確認するためのレポートが生成できます。

### Activity Detailのレポート

AccountandResourceManagementコンソールからアクセスした場合、これらのレポートにドメイン内のオブジェクトに関する変更内容がリアルタイムで表示されます。



## DRA管理レポート

NetIQ Reporting Center (レポーティングセンター)からアクセスできるこれらのレポートは、管理対象ドメイン内のイベントに関するアクティビティ、構成、および要約情報を提供します。一部のレポートでは、データがグラフで表現されます。

たとえば、Activity Detailレポートを使用すれば、指定した期間中にオブジェクトに対して加えられた変更またはオブジェクトが加えた変更のリストを表示できます。また、管理レポートを使用して、指定した期間中の各管理対象ドメインにおけるイベントの数をグラフで表示することもできます。Reportingでは、ActiveViewの定義やAAグループの定義など、DRAのセキュリティモデルに関する詳細も表示できます。

ライセンスでサポートされていない機能やレポートは、自動的に無効にされます。また、レポートの実行と表示には、適切な権限が必要です。このため、一部のレポートを使用できないことがあります。

Activity Detailレポートは、ARMコンソールおよびDelegation and Configurationコンソールを通じてDRAをインストールするとすぐに使用でき、ネットワークの変化に関する最新の詳細を表示できます。

DRA管理レポートは、オプション機能としてインストールして設定することができ、Reporting Centerで表示できます。データの収集を有効にして設定すると、定義したスケジュールに従って、DRAが監査対象イベントに関する情報を収集してSQL Serverデータベースにエクスポートするようになります。Reporting Centerでこのデータベースに接続すると、以下をはじめとする60以上の組み込みレポートにアクセスできます。

- 誰がいつ何をしたかを示すアクティビティレポート
- 特定の時点でのADまたはDRAの状態を示す構成レポート
- アクティビティの量を示す要約レポート

管理レポート用にデータ収集を設定する方法については、『*管理者ガイド*』を参照してください。

## 2.3.2 DRAによるログアーカイブの使用

アシスタント管理者のアクションを調査したりレポートが生成できるように、DRAはユーザのあらゆる操作を管理サーバのコンピュータ上にあるログアーカイブに記録しています。ユーザ操作とは、ユーザアカウントの更新、グループの削除、ActiveViewの再定義など、定義の変更を試みるすべての操作を指します。DRAは、管理サーバの初期化など、内部操作や関連するサーバの詳細情報も記録します。DRAは、これらの監査イベントをログに記録するだけでなく、そのイベントの前と後の値も記録して、何が変わったかを正確に把握できるようにします。

アーカイブしたログデータを安全に保存するために、DRAは**NetIQLogArchiveData**というフォルダを使用しています。このフォルダを「**ログアーカイブ**」といいます。DRAは長期間にわたってログをアーカイブし、グルーミングというプロセスを通じて古いデータを削除して新しいデータののための場所を確保します。

DRAは、ログアーカイブファイルに保存された監査イベントを使用して、たとえば指定した期間中にオブジェクトに対してどのような変更が加えられたかを示すActivity Detailレポートを表示します。また、これらのログアーカイブファイルから、NetIQ Reporting Centerが管理レポートの表示に使用するSQL Serverデータベースに、情報をエクスポートするようにDRAを設定することもできます。

DRAは、常に監査イベントをログアーカイブに書き込みます。DRAがWindowsのイベントログにもイベントを書き込む機能を、有効または無効にすることができます。

DRAの監査の詳細については、『[管理者ガイド](#)』を参照してください。

## 2.3.3 日付と時刻について

DRAはレポートを表示するときに、コントロールパネルの「地域と言語のオプション」で指定されている「**短い形式**」と「**時刻**」を使用します。DRAのレポートには、イベントのローカル日付および時刻としてUTC日付および時刻が表示されます。DRAレポートでは、次の日付形式がサポートされます。

- ◆ m/d/yy
- ◆ m-d-yy
- ◆ m/d/yyyy
- ◆ m-d-yyyy
- ◆ mm/dd/yy
- ◆ mm-dd-yy
- ◆ mm/dd/yyyy
- ◆ mm-dd-yyyy
- ◆ dd/mm/yy
- ◆ dd-mm-yy
- ◆ dd/mm/yyyy
- ◆ dd-mm-yyyy

## 2.3.4 DRA Reportingタスク

DRA管理レポートを生成するには、ReportingCenterをインストールし、DRAでデータ収集を有効にします。データ収集を有効にする方法については、『[管理者ガイド](#)』を参照してください。Activity Detailのレポートを生成するには、オブジェクトを右クリックして「**レポーティング**」をクリックします。そのオブジェクトについて生成できるレポートの選択肢が表示されます。以下の各セクションで、さまざまなレポーティングタスクについて説明します。

### Activity Detailレポートの表示

Activity Detailレポートには、環境内の変化に関する情報が表示されます。レポートを表示したり印刷するほかに、Excel、CSV、またはTXT形式でレポートを保存することもできます。レポートを表示または印刷するには、Reporting Administrationという役割を持っている必要があります。

レポートを表示するときには、情報表示の対象にする期間を指定するために基準を入力します。レポートに表示する対象を特定のDRAサーバに加えられた変更だけに制限したり、レポートに含める行数を制限することもできます。レポートのサイズが次のいずれかの制限を超えると、レポートが完成しなかったことを知らせるメッセージが表示されます。

- ◆ サイズが500MBを超えた
- ◆ すべてのDRAサーバに対してクエリを実行するために要した時間が5分を超えた
- ◆ 表示される行の数が1000を超えた

いずれかの制限に達するまでに取得された情報だけを含んだレポートを表示することも、レポートの基準を変更してこれらの制限条件を満たすレポートを表示することもできます。

レポートを表示するには、次の手順を実行します。

- 1 左側の表示枠にある **[すべての管理対象オブジェクト]** を開きます。
- 2 レポート表示の対象にするオブジェクトを指定するには、次の手順を実行します。
  - 2a **オブジェクトの場所が分かっている場合は**、このオブジェクトを含むドメインとOUを選択します。
  - 2b 検索の表示枠でオブジェクトの属性を指定してから **[Find Now (今すぐ検索★)]** をクリックします。
- 3 リストの表示枠内で、オブジェクトを右クリックして **[Reporting (レポート生成★)]** をクリックします。
- 4 **[ChangesmadetoobjectName(オブジェクト名への変更★)]** や **[ChangesmadebyobjectName(オブジェクト名による変更★)]** など、レポートの種類を選択します。使用できるレポートは、選択したオブジェクトの種類によって異なります。
- 5 変更を表示する期間の開始日と終了日を選択します。
- 6 **表示する行数を変更したい場合は**、デフォルトの値(250)を必要な値に書き換えます。

---

注: 表示される行数は、環境内の各管理サーバに適用されます。レポートに3つの管理サーバを含めてデフォルト値の250行を使用すると、そのレポートに表示できる行数は最大で750行になります。

---

- 7 **特定のサーバだけをレポートに含めたい場合は**、**[Restrict query to these DRA servers (クエリをこれらのDRAサーバに制限★)]** を選択し、レポートに含めるサーバの名前を(1つまたは複数)入力します。複数のサーバ名を指定する場合はカンマで区切ります。
- 8 **[OK]** をクリックします。

---

注: DRAが最新の変更をレポートに表示するまでに、最大で5秒かかることがあります。したがって、行った変更をレポートに表示するには、その変更から少なくとも5秒たってからレポートを実行してください。

---

## Activity Detailレポートのエクスポート

Activity Detailレポートは、XLS、CSV、およびTXT形式でエクスポートできます。デフォルトの形式は、Microsoft Excel形式です。

Activity Detailレポートをエクスポートするには、次の手順を実行します。

- 1 レポートのウィンドウで、**[ファイル]** メニューから **[Preview and Export (プレビューとエクスポート★)]** をクリックします。
- 2 プレビューウィンドウの **[ファイル]** メニューから、**[Export Document (Export ドキュメントをエクスポート★)]** > **[Excel File (Excel ファイル★)]** の順にクリックします。
- 3 エクスポートのオプションを選択し、**[OK]** をクリックします。
- 4 **[名前を付けて保存]** ウィンドウで、ファイルの名前を入力して **[保存]** をクリックします。



## Activity Detailレポートの印刷

レポートを印刷するには、Reporting Administrationという役割を持っている必要があります。レポートを表示したり印刷するほかに、さまざまな形式で保存することもできます。

Activity Detailレポートを印刷するには、次の手順を実行します。

- 1 レポートのウィンドウで、[ファイル] メニューから [Preview and Export (プレビューとエクスポート★)] をクリックします。
- 2 [プレビュー] ウィンドウで [ファイル] メニューから [印刷] をクリックします。

## 管理レポートの表示

Reporting Centerで管理レポートを表示できるようにするには、DRA ReportingをインストールしてDRAデータコレクタを設定する必要があります。DRA ReportingのインストールとDRA Collectorの設定については、『[管理者ガイド](#)』を参照してください。

Reporting Centerにログオンすると、インストール時に設定した方法に従ってWebサービスがIISを使用してアカウントの資格情報を検証します。

管理レポートを表示するには、次の手順を実行します。

- 1 Reporting Centerコンソールを実行しているコンピュータにログオンします。
- 2 NetIQ > Reporting Centerプログラムグループの順に選択し、その中のReporting Centerコンソールを起動します。
- 3 [Logon (ログオン★)] ダイアログボックスに必要な情報を入力し、[Logon (ログオン★)] をクリックします。
- 4 ナビゲーションの表示枠内で、[レポート] > [DRManagemerReport(DRManagementのレポート★)] の順に開きます。
- 5 表示したいレポートに到達するまで、レポートのカテゴリを開いていきます。
- 6 [ナビゲーション] 表示枠内でレポート名をクリックすると、そのレポートが中央の結果表示枠内に読み込まれ、キャッシュされたデータが表示されます。
- 7 **最新のデータを使ってレポートを表示したい場合は**、結果の表示枠内で [Execute Report (レポートを実行★)] をクリックします。

デフォルトのコンテキスト設定を変更して、異なるレポート結果が表示されるようにすることができます。Reporting Centerでのコンテキスト設定の詳細については、『[管理者ガイド](#)』を参照してください。

## 管理レポートのカスタマイズ

DRAには、出荷時に60以上の管理レポートが付属しています。Reporting Centerは、これらのレポートをさまざまな方法でカスタマイズおよび展開できる柔軟性を備えています。Reporting Centerでの管理レポートのカスタマイズと展開の詳細については、『[管理者ガイド](#)』を参照してください。

管理レポートをカスタマイズするには:

- 1 作成したいレポートに似たレポートを表示します。詳細については、『[管理レポートの表示](#)』を参照してください。

- 2 レポートのプロパティとコンテキスト設定を変更し、必要な情報を表示するようにレポートをカスタマイズします。
- 3 **[Execute Report (レポートを実行★)]** をクリックします。
- 4 **[Report (レポート★)]** メニューで、**[Save Report As (名前を付けてレポートを保存★)]** をクリックし、レポートのタイトルと、新しいレポートを保存する場所を指定します。
- 5 **[保存]** をクリックします。

Reporting Centerでの管理レポートの操作の詳細については、『**管理者ガイド**』を参照してください。

# 3 ユーザアカウント、グループ、および連絡先の管理

この章では、AccountandResourceManagementコンソールとWebコンソールの両方でユーザアカウント、グループ、ダイナミックグループ、ダイナミック配布グループ、および連絡先を管理するための概念と手続きの情報を記載しています。ユーザアカウントに関しては、両方のクライアントアプリケーションで一般的なオブジェクトの管理方法の例を取り上げて、より包括的に説明します。

## 3.1 ユーザアカウントの管理

Microsoft Windowsでは、関連するユーザアカウントのアクセス権限がユーザアカウントの種類によって決まります。ユーザアカウントはグローバルかローカルです。DRAはInetOrgPersonオブジェクトもサポートしていますが、InetOrgPersonオブジェクトを通常ユーザとして認識します。

### グローバルユーザアカウント

ユーザアカウントが作成されたドメインを信頼するドメインならどこでも使用できるユーザアカウントです。ユーザアカウントに特定のパーミッションを付与することができます。ユーザアカウントをグループのメンバーにしてから、そのグループにパーミッションを割り当てる方法もあります。ユーザアカウントのグループ化により、ユーザアカウントが多数ある場合のネットワークパーミッションの管理プロセスが単純になります。

### ローカルユーザアカウント

ローカルユーザアカウントは、Windowsオペレーティングシステムにログインする際に使用するアカウントと同じです。これにより、自分のユーザスペースでシステムのリソースにアクセスできます。

### 3.1.1 信頼されたドメイン内のユーザアカウント

Microsoft Windowsでは、管理対象ドメインのディレクトリ内にユーザアカウントとグループ定義が保存されます。このため、管理サーバは、信頼されたドメインがDRAによって管理されている場合を除き、そのドメインのディレクトリ情報を変更することができません。

たとえば、変更できないユーザアカウントとグループがAccountandResourceManagementコンソールに表示されることがあります。これらのユーザアカウントとグループは、管理対象ドメインのうちの1つが信頼するドメインに定義されています。ただし、信頼されたドメインのアカウントとグループを管理対象ドメイン内の別のグループに追加することはできます。

### 3.1.2 ユーザアカウントの管理タスク

このセクションでは、Account and Resource ManagementコンソールおよびWebコンソールによるユーザアカウント管理について順を追って説明します。適切な権限があれば、アカウントの作成や削除など、さまざまなユーザアカウント管理タスクを実行することができます。複数のユーザアカウントを選択した場合、グループに対するユーザの追加、削除、移動など、選択したタスクを1回の操作で実行できます。自分に割り当てられた権限の詳細については、「[割り当てられた権限と役割の表示](#)」を参照してください。

---

**注:** ユーザアカウントを別のActiveViewにコピーすることは、Account and Resource Managementコンソールからのみ実行できます。

---

## Account and Resource Managementコンソールでのユーザアカウントタスク

次に示す該当タスクをすべて [タスク] メニュー、または右クリックメニューから実行できます。一般に、目的のユーザオブジェクトを見つけてそれを選択するには、[すべての管理対象オブジェクト] というノードを選択し、[Find Now(今すぐ検索★)] という操作を実行します。新しいユーザを作成する場合は、ユーザを作成する場所のドメインまたはOUを選択する必要があります。1つまたは複数のユーザアカウントを選択すると、実行できるタスクが [タスク] メニューに表示されます。

## Webコンソールでのユーザアカウントタスク

次に挙げるタスクのほとんどがWebコンソールの [管理] > [検索] タブから実行できます。一般に、検索操作は、必要なユーザオブジェクトを見つけて、それを選択する際に実行します。リストで1つまたは複数のオブジェクトを選択したら、ツールバーのボタンがアクティブになります。ボタンの上にマウスのカーソルを重ねると、その機能が表示されます。



---

**注:** ユーザアカウントを別のActiveViewにコピーすることは、Account and Resource Managementコンソールからのみ実行できます。

---

### ユーザアカウントを作成する

管理対象ドメインまたは管理対象サブツリー内にユーザアカウントが作成できます。また、プロパティの変更、メールボックスの作成、電子メールの有効化、および新しいアカウントへのグループメンバーシップの割り当てなどを実行することもできます。

#### 注

- ◆ 企業によっては、新規ユーザアカウントに割り当てる名前に対し、ポリシーによって強制的に命名規則が適用される場合があります。
- ◆ デフォルトにより、新規ユーザアカウントは管理対象ドメインのユーザOUの中に置かれます。
- ◆ DRAでInetOrgPersonオブジェクトを作成することはできません。

### ユーザアカウントのクローンを作成する

ユーザアカウントのクローンを作成すると、そのユーザがメンバーになっているすべてのグループが新しいユーザアカウントに自動的に追加されるため、クローンとして作成されたアカウントのための設定時間が省けます。クローンとして作成されたアカウントに対しては、グループの追加または削除、およびメールの有効化など、様々なプロパティ設定を新規アカウントのときと同様に行うことができます。

---

**注:** InetOrgPersonオブジェクトのクローンを作成するときには、ユーザアカウントを作成します。

---

## ユーザアカウントのプロパティを変更する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントのプロパティを管理できます。変更できるユーザアカウントのプロパティは、ユーザの権限により異なります。Exchangeをインストールし、Microsoft Exchangeのサポートを有効にすれば、ユーザアカウントを管理しながら対応するメールボックスのプロパティを変更することができます。

---

**注:** ホームディレクトリのポリシーを有効にすると、そのアカウントを管理するときにユーザアカウントのホームディレクトリが自動的に変更されます。たとえば、ホームディレクトリの場所を変更すると、指定されたホームディレクトリが作成され、前のホームディレクトリの内容が新しい場所に移動されます。元のディレクトリで割り当てられていたACLも、新しいディレクトリに適用されます。

---

## 自分のアカウントを管理する

電話番号など、一般プロパティを変更することにより、自分のアカウントを管理することができます。自分のアカウントを管理する前に、適切な権限があることを確認してください。

## ユーザアカウントの名前を変更する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントの名前を変更できます。ユーザのログオン名を変更すると、そのユーザアカウントに対応するメールボックスの名前も変更されます。

## ユーザアカウントを有効化する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントを有効にすることができます。Microsoft Windowsアカウントを管理している場合、この変更が適用されるドメインコントローラを指定することができます。

変更を特定のドメインコントローラに適用する場合、その変更は同じ管理対象ドメインのデフォルトのドメインコントローラにも適用されます。デフォルトのドメインコントローラを検証するには、ドメインのプロパティを表示します。

## ユーザアカウントを無効にする

管理対象ドメイン内のユーザアカウントを無効にすることができます。Microsoft Windowsアカウントを管理している場合、この変更が適用されるドメインコントローラを指定することができます。

変更を特定のドメインコントローラに適用する場合、その変更は同じ管理対象ドメインのデフォルトのドメインコントローラにも適用されます。デフォルトのドメインコントローラを検証するには、ドメインのプロパティを表示します。

## ユーザアカウントのロックを解除する

管理対象ドメインまたは管理対象サブツリー内にあるユーザアカウントのロックを解除できます。

DRAではユーザアカウントのステータスがアカウントキャッシュから取得されるため、選択したアカウントが実際にはロックされているのにロックが解除されているものとしてユーザインタフェースに表示されることがあります。そのような場合でも、DRAではユーザアカウントのロックを解除することができます。DRAコンソールを使用してユーザアカウントのロックを解除するとき、ドメインコントローラを指定することもできます。このとき、ユーザアカウントのパスワードをリセットする必要はありません。

## ユーザアカウントのパスワードをリセットする

管理対象ドメインまたは管理対象サブツリー内のアカウントのパスワードをリセットできます。ユーザアカウントについて変更できるフィールドは、ユーザの権限により異なります。

ユーザアカウントのパスワードをリセットすると、そのアカウントのロックが自動的に解除されます。ユーザアカウントの新しいパスワードがDRAで自動的に生成されるようにするかどうかを選択できます。また、アカウントのパスワード関連のオプションも変更できます。Microsoft Windowsのアカウントを管理している場合は、ドメインコントローラを指定して、そこに対してDRAにこれらの変更を適用させることができます。

---

**注:** 変更を特定のドメインコントローラに適用する場合、その変更は同じ管理対象ドメインのデフォルトのドメインコントローラにも適用されます。デフォルトのドメインコントローラを検証するには、ドメインのプロパティを表示します。

---

#### ユーザアカウントを別のActiveViewにコピーする

ユーザアカウントを別のActiveViewにコピーすることができます。この操作を、ユーザアカウントの「転送」と呼びます。ユーザアカウントを別のActiveViewにコピーするには、コピー元とコピー先のActiveViewの両方でCopy User to Another ActiveViewという権限を持っている必要があります。ユーザアカウントを別のActiveViewに転送しても、元のActiveViewのユーザアカウントは削除されません。

#### ユーザアカウントを別のコンテナに移動する

管理対象ドメインまたは管理対象サブツリー内の別のコンテナ(OUなど)にユーザアカウントを移動することができます。

#### ユーザアカウントを削除する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントを削除することができます。そのドメインでゴミ箱が無効になっている場合、ユーザアカウントを削除すると、そのユーザアカウントはActive Directoryから永久に削除されます。そのドメインでゴミ箱が有効になっている場合、ユーザアカウントを削除すると、そのユーザアカウントはゴミ箱に移動します。

---

**警告:** ユーザアカウントを作成すると、Microsoft WindowsによってそのアカウントにSID (Security Identifier)が割り当てられます。SIDは、アカウント名からは生成されません。Microsoft Windowsは、SIDを使用して各リソースのACL (Access Control Lists)に特権を記録します。ユーザアカウントを削除した場合、同じ名前のユーザアカウントを新規に作成しても、削除前のアクセス権を復活させることはできません。

---

#### ユーザアカウントにグループメンバーシップを指定する

管理対象ドメインまたは管理対象サブツリー内の特定グループにユーザアカウントを追加したり削除することができます。このアカウントが属す既存のグループのプロパティを表示し、変更することもできます。

### 3.1.3 ユーザアカウントの変換

DRAでは、ユーザアカウントを簡単かつ効率的に変換できます。ユーザアカウントを持つ個人の職責が変更になったときに、DRAの変換機能が使用できます。職務内容テンプレートを使用して、アカウントに設定されたグループメンバーシップを簡単に追加、削除、または更新することができます。昇進、部署移動、退職のいずれであっても、ユーザアカウントの変換機能により、時間、お金、労力などが節約できます。

## 変換プロセスの概要

ユーザアカウントの変換機能は、次の目的に使用できます。

- ◆ ユーザアカウントに設定されたグループメンバーシップの削除
- ◆ ユーザアカウントへのグループメンバーシップの追加
- ◆ ユーザプロパティの変更
- ◆ 特定のグループメンバーシップを削除して同時に他のグループメンバーシップをユーザアカウントに追加する

ユーザアカウントを変更する前に、次のプロセスを検討してください。

- 1 グループメンバーシップの追加、削除、またはその両方を行う必要性を判断します。
- 2 現在の削除および追加テンプレートを見直して、必要なテンプレートユーザアカウントがあることを確認します。
- 3 必要に応じてテンプレートアカウントを作成します。
- 4 [Transform User (ユーザの変換★)] ウィザードを終了します。

DRAによるユーザの変換により、削除テンプレートによって指定されたグループメンバーシップはユーザアカウントから削除され、追加テンプレートによって指定されたグループメンバーシップがユーザアカウントに割り当てられます。削除テンプレートまたは追加テンプレートにないメンバーシップは影響を受けません。たとえば、1人の海外営業部員が米国営業課から欧州営業課へと転属になったとします。その会社には配布グループとセキュリティグループの両方があり、それぞれが対応する営業課独自のグループであり、数はすべての営業課で共有されています。米国営業課には「米国重点地域DL」および「米国営業管理DL」という流通グループがあり、欧州営業課には「欧州重点地域」および「欧州営業管理」という流通グループがあります。両課とも「グローバル営業セキュリティ」というセキュリティグループのメンバーですが、個別に地域固有のセキュリティグループも持っています。

削除テンプレート「米国営業テンプレート」には次のグループメンバーシップが指定されています。

- ◆ 米国重点地域DL
- ◆ 米国営業管理DL
- ◆ グローバル営業セキュリティ
- ◆ 米国セキュリティ

追加テンプレート「欧州営業テンプレート」には次のグループメンバーシップが指定されます。

- ◆ 欧州重点地域DL
- ◆ 欧州営業管理DL
- ◆ グローバル営業セキュリティ
- ◆ 欧州セキュリティ

変換プロセス中に、転属された営業部員のユーザアカウントはまず、「米国営業テンプレート」によって指定されたすべてのグループメンバーシップから削除され、「欧州営業テンプレート」によって指定されたすべてのグループメンバーシップに追加されます。仮にこの社員が「ポーカー仲間」という配布グループのメンバーでもある場合、このグループメンバーシップは変更されません。

次の権限を付与すれば、アシスタント管理者が変換プロセス中にユーザアカウントをさらに変更することができます。

- ◆ ユーザアカウントの変換と同時に所在地プロパティを変更

- ユーザアカウントの変換と同時に説明を変更
- ユーザアカウントの変換と同時に事務所を変更
- ユーザアカウントの変換と同時に電話プロパティを変更

また、グループメンバーシップを追加または削除する権限を限定することもできます。それには、次に挙げる権限のいずれかのみをアシスタント管理者に与えます。

- テンプレート内に存在するグループにユーザを追加
- テンプレート内に存在するグループからユーザを削除

権限を応用したこのような制限オプションのいずれかを使うことで自社のセキュリティに厚みが増します。テンプレートに存在するグループだけを削除するだけの権限を特定の社員に付与する形で、暫定のユーザアカウントが作成できます。これらの暫定アカウントは、別のアシスタント管理者が追加テンプレートのアカウントを使って新しいグループメンバーシップを付与してしまう前に、検証することができます。

## ユーザ変換テンプレートの作成

ユーザアカウントの変換は、社内での役割と職務に直接連携しています。社内の役割や職務ごとにテンプレートを作成することを検討してください。DRAでは、削除テンプレートとして使用されるユーザアカウントと追加テンプレートとして使用されるユーザアカウントを区別しません。社内での役割ごとにテンプレートユーザアカウントを1つ作成してください。変換中に、テンプレートを削除または追加として選択します。削除テンプレートとして選択したテンプレートを、後の変換処理で追加テンプレートとして使用することもできます。

ユーザ変換テンプレートを作成するには、ユーザアカウントを作成し、そのユーザアカウントに適切なグループを割り当てる権限がなければなりません。これらの権限をは、適切なActiveViewでCreate and Delete User AccountsおよびGroup Administrationという各役割をアカウントに関連付けるか、個々の権限を割り当てることで、取得できます。

## ユーザアカウントの変換

ユーザアカウントを変換することで、ユーザアカウントグループメンバーシップの追加と削除のいずれか、またはその両方が実行できます。社内での人事異動の際に、このワークフローを使用します。Transform a Userという役割か、ユーザアカウントを変更するための権限を含んでいる役割を持っていないければなりません。この機能は、AccountandResourceManagementコンソールからのみ実行できます。

ユーザアカウントを変更するには、次の手順を実行してください。

- 1 左側の表示枠にある **[すべての管理対象オブジェクト]** を開きます。
- 2 管理するユーザアカウントを指定するには、**[Find Now (今すぐ検索★)]** という操作を実行してユーザオブジェクトを見つけ、それを選択します。
- 3 **[タスク]** > **[変換]** をクリックします。
- 4 **[ようこそ]** ウィンドウを確認してから、**[次へ]** をクリックします。
- 5 **[Select User Template (ユーザテンプレートの選択★)]** ウィンドウで、**[ブラウズ]** を使用して適切な削除テンプレートユーザを選択します。
- 6 削除テンプレートのユーザアカウントのプロパティを確認する必要がある場合は、**[表示]** をクリックします。
- 7 **[ブラウズ]** を使用して、適切な追加テンプレートユーザを選択します。
- 8 追加テンプレートユーザアカウントのプロパティを確認するには、**[表示]** をクリックします。



- 9 適切な権限があるユーザであれば、[Change other properties of the user (このユーザの他のプロパティを変更する★)] にチェックマークを入れて、変更するプロパティを選択することができます。[次へ] をクリックして、使用可能なプロパティまで移動します。
- 10 [次へ] をクリックします。
- 11 [Summary(概要★)] ウィンドウの内容を確認したら、[Finish(終了★)] をクリックします。

## 3.2 グループを管理する

アシスタント管理者として、DRAを使用してグループ管理およびグループプロパティの変更を行うことができます。グループ化により、定義された一連のユーザアカウントに特定のパーミッションを与えることができます。グループを使用して、任意のドメイン内でユーザアカウントがアクセスできるデータとリソースを管理することができます。

任意の種類および範囲のグループを管理することができます。たとえば、グループをネストして、1つのグループに別のグループのパーミッションを継承させることができます。信頼するドメインのグループを管理対象ドメイン内の別のグループに追加したり、一時的なグループ指定を管理することにより、ドメイン全体のグループメンバーシップを効率的に管理することもできます。

### 3.2.1 グループ管理タスク

このセクションでは、AccountandResourceManagementコンソールを使用して、グループを管理する方法について説明します。適切な権限があれば、グループメンバーシップの変更など、さまざまなグループ管理タスクを実行することができます。複数のグループを選択した場合、グループに対するメンバーの追加、削除、移動など、選択したタスクを1回の操作で実行できます。1つまたは複数のグループを選択すると、実行できるタスクが[タスク]メニューに表示されます。

#### グループにアカウントを追加する

ユーザアカウント、連絡先、およびコンピュータを管理グループに追加することができます。

---

**注:** このタスクは、複数のアカウントを指定グループに追加します。1つのアカウントをグループに追加するには、アカウントを選択して、[タスク]メニューの[グループに追加] をクリックします。

別のグループへのアカウントの追加により、そのアカウントに対する権限が増える場合には、そのアカウントの追加は許可されません。

---

#### グループを他のグループに追加する

別の管理対象グループにグループを追加することによってグループを入れ子にすることができます。グループが別のグループの入れ子になっている場合、子のグループは親のグループからパーミッションを継承できます。

---

**注:** 別のグループにグループを追加することにより、そのグループに対する権限が増える場合には、そのグループの追加は許可されません。

---

#### グループのプロパティを変更する

ローカルグループとグローバルグループのプロパティを変更することができます。所有する権限により、管理対象ドメインまたは管理対象サブツリー内のグループに対して変更できるプロパティが異なります。Exchangeをインストールし、Microsoft Exchangeのサポートを有効にすれば、グループを管理しながら配布リストのプロパティを変更することができます。

## グループを作成する

管理対象ドメインまたは管理対象サブツリー内にグループを作成することができます。新しいグループのグループメンバーなどのプロパティを変更することもできます。

---

### 注

- ◆ 企業によっては、新しいグループに割り当てる名前にポリシーを通して命名規則が適用される場合があります。
  - ◆ デフォルトでは、新しいグループが管理対象ドメインのユーザOUの中に置かれます。
- 

## グループメンバーを指定する

管理グループに対して、ユーザアカウント、連絡先、コンピュータ、または他のグループを追加または削除できます。DRAは、外部のセキュリティプリンシパルの削除のみ許可します。既存グループメンバーのプロパティを表示および変更することもできます(外部のセキュリティプリンシパルを除く)。

グループからメンバーを削除しても、メンバーであるオブジェクトは削除されません。メンバーをグループに追加するときには、追加するメンバーオブジェクトを変更する権限がなければなりません。

---

**注:** Windowsの管理者または特別なグループのメンバーでない限り、Windowsの特別なグループ (Administratorsグループ、アカウントオペレータグループ、バックアップオペレータグループ、サーバーオペレータグループなど)にユーザアカウントやグループを追加することはできません。

---

## グループにグループメンバーシップを指定する

管理対象ドメインまたは管理対象サブツリー内の別のグループにグループを追加したり削除することができます。グループが属す既存のグループのプロパティを表示し、変更することもできます。

## グループメンバーシップのセキュリティパーミッションを設定する

グループメンバーシップにActive Directoryのセキュリティ権限を設定することができます。これらのパーミッションにより、Microsoft Outlookを使用してグループメンバーシップを表示(読み込み)および変更(書き込み)できるユーザが指定されます。これらの設定を使用して、環境内の配布リストおよびセキュリティグループの安全性を高めることができます。継承したセキュリティパーミッションを変更することはできません。

---

**注:** グループメンバーシップのセキュリティを管理するときに、オフになっているパーミッションが継承されたパーミッションを示す場合があります。

---

## グループの所有権を設定する

Microsoft Windowsの配布グループおよびセキュリティグループの所有権を設定することができます。グループ所有権のパーミッションは、ユーザアカウント、グループ、または連絡先に付与することができます。グループ所有権が付与されると、ユーザアカウント、グループ、または連絡先がそのグループのメンバーシップを変更することができます。

---

**注:** グループメンバーシップがMicrosoft Exchangeサーバから隠れている場合は、DRAが [Managercanupdatemembershiplist(マネージャがメンバーシップリストを更新できる★)] というチェックボックスを無効にします。このチェックボックスを有効にするには、[Group Properties (グループプロパティ★)] ウィンドウで [Exchange (変換★)] タブの [Expose Group Membership (グループメンバーシップを表示する★)] をクリックします。

---

## グループのクローンを作成する

管理対象ドメイン内のローカルグループとグローバルグループの両方でクローンが作成できます。グループのクローンを作成することにより、元のグループと同じ種類および属性を持つ新しいグループを作成することができます。また、元のグループのすべてのメンバーが新しいグループに追加されます。

グループのクローンを作成することにより、同様のプロパティを持つ他のグループをベースとして簡単にグループを作成することができます。グループのクローンを作成すると、選択されたグループの値が「Clone Group (グループのクローン作成★)」ウィザードに設定されます。新しいグループのプロパティを変更することもできます。

---

### 注

- ◆ 企業によっては、新しいグループに割り当てる名前にポリシーを通して命名規則が適用される場合があります。
  - ◆ デフォルトでは、新しいグループが管理対象ドメインのユーザOUの中に置かれます。
- 

## グループを削除する

管理対象ドメインまたは管理対象サブツリー内のローカルグループとグローバルグループが削除できます。そのドメインでごみ箱が無効になっている場合、グループを削除すると、そのグループはActive Directoryから永久に削除されます。そのドメインでごみ箱が有効になっている場合は、グループを削除すると、そのグループはごみ箱に移動し、グループのプロパティが無効になります。

ごみ箱の詳細については、「[ごみ箱の管理](#)」を参照してください。

---

**警告:** グループを作成すると、Microsoft WindowsによってそのグループにSID (Security Identifier)が割り当てられます。SIDは、グループ名からは生成されません。Microsoft Windowsは、SIDを使用して各リソースのACL (Access Control Lists)に特権を記録します。グループを削除する場合は、同一名を使用して新規のグループを作成することにより、そのグループのアクセス権を戻すことはできません。

---

## 別のコンテナにグループを移動する

管理対象ドメインまたは管理対象サブツリー内の別のコンテナ(OUなど)にグループを移動することができます。

## グループメンバーシップを配布リストに表示させる

管理対象ドメインまたは管理対象サブツリー内のグループのメンバーシップを配布リストに表示させることができます。

## 配布リストでグループメンバーシップを非表示にする

管理対象ドメインまたは管理対象サブツリー内のグループのメンバーシップを配布リストで非表示にすることができます。

## 3.2.2 一時グループの割り当て

一時グループに指定することで、特定の期間だけグループメンバーシップを必要とするユーザのグループメンバーシップを管理することができます。このセクションでは、Account and Resource Managementコンソールを使用して、一時グループ割り当てを管理する方法について説明します。適切な権限があれば、新しい一時グループ割り当ての作成や期限が切れた一時グループ割り当ての削

除などのタスクを実行することができます。これらのタスクは、プライマリ管理サーバ上でのみ実行することができます。1つまたは複数の一時グループ割り当てを選択すると、実行できるタスクが「タスク」メニューに表示されます。

#### 一時グループ割り当てのプロパティを管理する

一時グループ割り当てまたは保存された期限切れのグループ指定のプロパティは、プライマリ管理サーバ上でのみ管理できます。権限により、変更可能な一時グループ割り当てのプロパティは異なります。

#### 一時グループ割り当てを新規に作成する

一時グループ割り当ては、プライマリ管理サーバ上でのみ作成することができます。新しい一時グループ割り当てのプロパティ(スケジュールなど)を変更することもできます。

#### 一時グループ割り当てでユーザアカウントを管理する

プライマリ管理サーバ上で、一時グループ割り当てにユーザアカウントを追加または削除することができます。

---

**注:** アクティブになっていない一時グループ割り当てのユーザアカウントのみ管理できます。

---

#### 一時グループ割り当てのスケジュールを変更する

プライマリ管理サーバ上でのみ一時グループ割り当てのスケジュールを変更することができます。保存された期限切れの一時グループ割り当てのスケジュールも変更することができます。

---

**注:** 一時グループ割り当ての期限が切れると、今後のために保存しない限り、DRAにより自動的に削除されます。

---

#### 一時グループ割り当てを削除する

一時グループ割り当ては、プライマリ管理サーバ上で削除することができます。

## 3.3 ダイナミック配布グループの管理

ダイナミック配布グループとは、メールが有効なActive Directoryのグループオブジェクトです。電子メールメッセージやその他の情報を迅速に大量送信するために作成することができます。

ダイナミック配布グループのメンバーシップリストは、グループにメッセージが送信されるたびに、定義するフィルタおよび条件に基づいて計算されます。これは、定義されたメンバーセットを含む正規の配布グループとは異なります。電子メールメッセージがダイナミック配布グループに送信されると、組織内でそのグループに定義されている条件に一致する受信者に届きます。

DRAがサポートする機能は次のとおりです。

- ◆ 監査とUIレポート
- ◆ ダイナミック配布グループの列挙のサポート
- ◆ ダイナミック配布グループのNetIQ Reporting Center (NRC) レポート
- ◆ ダイナミック配布グループのトリガ操作のサポート
- ◆ Exchangeのダイナミック配布グループのUI拡張機能のサポート

ダイナミック配布グループのタスク:

## ダイナミック配布グループを作成する

管理対象ドメインまたは管理対象サブツリーの中にダイナミック配布グループを作成することができます。また、新規のダイナミック配布グループに関し、グループメンバーなどのプロパティを変更することもできます。

---

### 注

- ◆ 企業によってはポリシーで命名規則が定められている場合があります。その場合は、その規則に従って新規のダイナミック配布グループに割り当てられる名前が決まります。
  - ◆ デフォルトでは、DRAが新規のダイナミック配布グループを管理対象ドメインのユーザOUの中に配置します。
- 

## ダイナミック配布グループのクローンを作成する

管理対象ドメイン内のローカルとグローバルのダイナミック配布グループの両方でクローンを作成することができます。ダイナミック配布グループのクローンを作成することにより、元のダイナミック配布グループと同じ種類および属性を持つダイナミック配布グループを新たに作成することができます。

ダイナミック配布グループのクローンを作成することにより、同様のプロパティを持つ別のダイナミック配布グループをベースにして簡単にダイナミック配布グループを作成することができます。ダイナミック配布グループのクローンを作成すると、その選択されたダイナミック配布グループの値を使って「ダイナミック配布グループのクローンを作成する」ウィザードの設定が行われます。新しいダイナミック配布グループのプロパティを変更することもできます。

## ダイナミック配布グループを別のコンテナに移動する

管理対象ドメインまたは管理対象サブツリー内にある別のコンテナ(OUなど)にダイナミック配布グループを移動することができます。

## ダイナミック配布グループを削除する

管理対象ドメインまたは管理対象サブツリーの中のローカルおよびグローバルのダイナミック配布グループを削除できます。そのドメインでごみ箱が無効になっている場合、ダイナミック配布グループを削除すると、そのダイナミック配布グループはActive Directoryから永久に削除されます。そのドメインでごみ箱が有効になっている場合、ダイナミック配布グループを削除すると、そのダイナミック配布グループはごみ箱に移動し、ダイナミック配布グループのプロパティが無効になります。

ごみ箱の詳細については、「[ごみ箱の管理](#)」を参照してください。

---

**警告:** ダイナミック配布グループを作成するとき、Microsoft WindowsによってSID (Security Identifier)がそのダイナミック配布グループに割り当てられます。SIDはダイナミック配布グループ名から生成されるものではありません。Microsoft Windowsは、SIDを使用して各リソースのACL (Access Control Lists)に特権を記録します。ダイナミック配布グループを削除した場合、それと同じ名前で新規にダイナミック配布グループを作成しても、削除前のダイナミック配布グループのアクセス権を復活させることはできません。

---

## ダイナミック配布グループのプロパティを変更する

ローカルおよびグローバルのダイナミック配布グループのプロパティを変更することができます。所有する権限により、管理対象ドメインまたは管理対象サブツリー内のグループに対して変更できるプロパティが異なります。

## フィルタを指定する

ダイナミック配布リストのメンバーシップは、そのフィルタで決まり、そのフィルタはユーザが定義できます。

## 条件を指定する

条件には、ダイナミック配布グループのメンバーになるためにオブジェクトが満たす必要のある基準が定義されます。

## 3.4 ダイナミックグループの管理

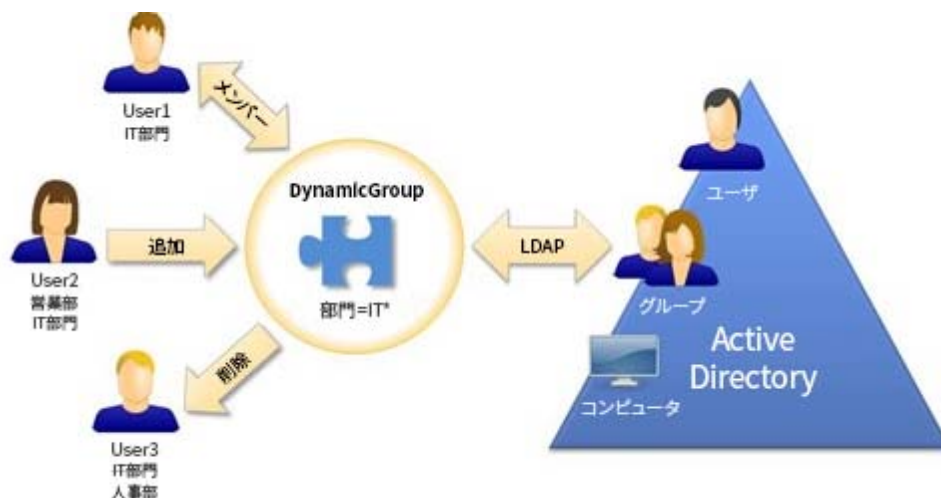
ダイナミックグループとは、定義された一連の基準に基づいてメンバーシップが変わるグループです。これまで、ダイナミックグループはExchangeの環境でのみ可能でしたが、Active Directoryの設定でも作成できるようになりました。

Active Directoryのダイナミックグループでの一般的な使用について、次の図で説明します。この図には、ダイナミックグループが3つあります。各グループに一連の基準があり、その基準によってそのグループに追加できるユーザとできないユーザが決まります。各グループが、ファイル、フォルダ、およびアプリケーションへのアクセスを制御します。

---

ヒント: ダイナミックグループの永続メンバーを含める「スタティックメンバーリスト」と、特定のユーザにダイナミックグループのメンバーシップを持たせないようにする「除外されたメンバーリスト」が作成できます。

---



最近User2がIT部門に加わりました。そのユーザは、IT部門のダイナミックグループが更新されると、グループに追加されます。User2は、営業部のダイナミックグループが更新されるときに、そのメンバーのリストから削除されます。

---

ヒント: ダイナミックグループのメンバーリストは、それを右クリックし [Update Members (メンバーを更新★)] を選択すると更新されます。

---

User3は、IT部門から人事部に異動したため、IT部門のダイナミックグループから削除され、人事部のダイナミックグループに追加されます。

### ダイナミックグループを作成する

管理対象ドメインまたは管理対象サブツリーの中にダイナミックグループを作成することができます。また、新しいダイナミックグループのグループメンバーなどのプロパティを変更することもできます。



---

## 注

- 企業によってはポリシーで命名規則が定められている場合があります。その場合は、その規則によって新規のダイナミックグループに割り当てられる名前が決まります。
  - デフォルトでは、DRAが新規のダイナミックグループを管理対象ドメインのユーザOUの中に配置します。
- 

### フィルタを作成する

ダイナミックグループは、グループが更新されるたびに、フィルタを使用してメンバーシップリストからユーザを追加または削除します。

### スタティックメンバーリストを管理する

ダイナミックグループのスタティックメンバーリストに入っているユーザは、手動で削除されない限り、永続的にそのグループのメンバーです。

ダイナミックグループからメンバーを削除しても、メンバーであるオブジェクトは削除されません。メンバーをダイナミックグループに追加するときには、追加するメンバーオブジェクトに対し変更できる権限がなければなりません。

### 除外されたメンバーリストを管理する

ダイナミックグループの除外されたメンバーリストに入っているユーザは、手動でこのリストから削除されない限り、グループに加わることはできません。

### メンバーリストを更新する

ダイナミックグループ内のメンバーを **[Update Members (メンバーを更新★)]** という操作で更新することができます。

### ダイナミックグループのクローンを作成する

管理対象ドメイン内のローカルとグローバルのダイナミックグループの両方でクローンを作成することができます。ダイナミックグループのクローン作成では、元のダイナミックグループと同じ種類および属性を持つダイナミックグループが新たに作成されます。

ダイナミックグループを作成することにより、同様のプロパティを持つ他のダイナミックグループをベースにして簡単にダイナミックグループを作成することができます。ダイナミックグループのクローンを作成するときは、その選択されたダイナミックグループの値を使って **[ダイナミックグループのクローンを作成する]** ウィザードの設定が行われます。新しいダイナミックグループのプロパティは変更することもできます。

### ダイナミックグループを別のコンテナに移動する

管理対象ドメインまたは管理対象サブツリー内にある別のコンテナ(OUなど)にダイナミックグループを移動することができます。

### ダイナミックグループを削除する

管理対象ドメインまたは管理対象サブツリーの中のローカルとグローバルのダイナミックグループを削除できます。そのドメインでごみ箱が無効になっている場合、削除されたダイナミックグループはActive Directoryから永久に削除されます。そのドメインでごみ箱が有効になっている場合、ダイナミックグループを削除すると、そのダイナミックグループはごみ箱に移動し、ダイナミックグループのプロパティが無効になります。

ごみ箱の詳細については、「[ごみ箱の管理](#)」を参照してください。

---

**警告:** ダイナミックグループを作成するとき、Microsoft WindowsによってSID (Security Identifier)がそのダイナミックグループに割り当てられます。SIDはダイナミックグループ名から生成されるものではありません。Microsoft Windowsは、SIDを使用して各リソースの



ACL (Access Control Lists)に特権を記録します。ダイナミックグループを削除した場合、それと同じ名前で新規にダイナミックグループを作成しても、削除前のダイナミックグループのアクセス権を復活させることはできません。

---

### ダイナミックグループのプロパティを変更する

ローカルおよびグローバルのダイナミックグループのプロパティを変更することができます。所有する権限により、管理対象ドメインまたは管理対象サブツリー内のグループに対して変更できるプロパティが異なります。

### ダイナミックグループを別のダイナミックグループを追加する

別の管理対象グループにダイナミックグループを追加することによって、ダイナミックグループをネストさせることができます。ダイナミックグループが別のダイナミックグループの中にネストされると、子のダイナミックグループは親のダイナミックグループからパーミッションを継承できます。

---

**注:** ダイナミックグループを別のダイナミックグループに追加することによってそのダイナミックグループに対する権限が増える場合、DRAはそのダイナミックグループの追加を許可しません。

---

### グループメンバーシップのセキュリティパーミッションを設定する

ダイナミックグループのメンバーシップに対しActive Directoryのセキュリティパーミッションを設定することができます。これらのパーミッションで、Microsoft Outlookを使用してダイナミックグループのメンバーシップの表示(読み込み)が行えるユーザと、変更(書き込み)も行えるユーザを指定します。これらの設定を使用することで、環境内の配布リストおよびセキュリティダイナミックグループの安全性をより効率的に確保することができます。継承したセキュリティパーミッションを変更することはできません。

---

**注:** ダイナミックグループメンバーシップのセキュリティを管理するとき、オフになっているパーミッションが継承されたパーミッションを示している場合があります。

---

### ダイナミックグループの所有権を設定する

ダイナミックグループの所有者のパーミッションをユーザアカウント、グループ、または連絡先に付与することができます。ダイナミックグループの所有者の権限を付与されると、指定されたユーザアカウント、グループ、または連絡先がそのダイナミックグループのメンバーシップを変更できるようになります。

### ダイナミックグループのメンバーシップを配布リストに公開する

ダイナミックグループのメンバーシップは、管理対象ドメインまたは管理対象サブツリー内のグループのための配布リストに表示させることができます。

### ダイナミックグループのメンバーシップを配布リストで非表示にする

ダイナミックグループのメンバーシップは、管理対象ドメインまたは管理対象サブツリー内のグループのための配布リストに表示されないようにすることができます。

---

**注:** Microsoft Exchange 2007の配布リストでは、**[Hide Group Membership(グループのメンバーシップを隠す★)]** というオプションが無効になっています。

---

## 3.5 連絡先を管理する

連絡先や関連する電子メールアドレスなど、多数のネットワークオブジェクトがDRAで管理できます。連絡先は、混合モードまたはネイティブMicrosoft Windowsドメインでのみ使用できます。連絡先には、ユーザアカウントやグループと同様に、SID (Security Identifier)があります。連絡先を使用して、ネットワークサービスへのアクセスを許可せずにメンバーを配布リストやグループに追加することができます。

混合モードまたはネイティブモードドメインの中のセキュリティまたは配布グループに連絡先を追加することができます。Microsoft Windowsでは配布リストとしてセキュリティグループを使用できるため、連絡先をこれらのグループに追加すると便利な場合があります。グローバルセキュリティグループに連絡先が含まれていても、ネイティブモードのMicrosoft Windowsドメインに移行するときにそのグループをユニバーサルセキュリティグループに変換することができます。

### 連絡先のプロパティを変更する

連絡先のプロパティは変更することができます。所有する権限により、管理対象ドメイン内の連絡先に対して変更できるプロパティが異なります。Exchangeをインストールし、Microsoft Exchangeのサポートを有効にすれば、連絡先を管理しながら電子メールアドレスのプロパティを変更することができます。

### 連絡先を作成する

管理対象ドメインまたは管理対象サブツリー内に連絡先を作成できます。また、プロパティの変更、電子メールの有効化、電子メールアドレスの指定、新しい連絡先へのグループメンバーシップの割り当てなどを実行することもできます。

### 連絡先のクローンを作成する

連絡先のクローンを作成することにより、同様のプロパティを持つ他の連絡先をベースとして簡単に連絡先を作成することができます。連絡先のクローンを作成すると、選択された連絡先から値が取り込まれ、[Clone Contact (連絡先のクローン作成★)] ウィザードに設定されます。また、プロパティの変更、電子メールの有効化、電子メールアドレスの指定、新しい連絡先へのグループメンバーシップの割り当てなどを実行することもできます。

### 連絡先のグループメンバーシップを管理する

管理対象ドメインまたは管理対象サブツリー内の特定のグループに連絡先を追加したり削除することができます。この連絡先が属す既存のグループのプロパティを表示し、変更することもできます。

### 別のOUに連絡先を移動する

管理対象ドメインまたは管理対象サブツリー内の別のコンテナ(OUなど)に連絡先を移動することができます。

### 連絡先を削除する

管理対象ドメインまたは管理対象サブツリー内の連絡先を削除することができます。そのドメインでごみ箱が無効になっている場合、連絡先を削除すると、その連絡先はActive Directoryから永久に削除されます。そのドメインでごみ箱が有効になっている場合は、連絡先を削除すると、その連絡先はごみ箱に移動します。

ごみ箱の詳細については、「[ごみ箱の管理](#)」を参照してください。

# 4 Exchangeのメールボックスとパブリックフォルダの管理

DRAを使用すると、Microsoft Exchangeのメールボックスをユーザアカウントプロパティの一環として管理することができます。この統合によりシステム管理のワークフローが単純化されるため、Exchangeのプロパティが効率的に管理できます。また、ユーザアカウントとExchangeアカウントの各フォレストからメールボックスをリンクでき、リソースメールボックス、共有メールボックス、およびパブリックフォルダの管理もできます。

## Account and Resource Managementコンソールでのメールボックスタスクの管理

ARMコンソールの使用時に、オブジェクトのプロパティの [ExchangeTasks(Exchangeタスク★)] タブから( [タスク] や、選択されたオブジェクトの右クリックメニューからもアクセス可能)、該当するメールボックスタスクを実行します。一般的には、 [すべての管理対象オブジェクト] ノードを選択し、 [FindNow(今すぐ検索★)] の操作を実行して目的のオブジェクトを見つけて、それを選択します。

## Webコンソールでのメールボックスタスクの管理

Webコンソールを使用している場合、次に挙げる該当メールボックスタスクを [管理] > [検索] タブから実行します。一般的には、検索操作を実行して目的のメールボックスオブジェクトを見つけて、それを選択します。リストで1つまたは複数のオブジェクトを選択したら、ツールバーのボタンがアクティブになります。ボタンの上にマウスのカーソルを重ねると、その機能が表示されます。メールに関連するオプションはすべて、ツールバーの右側にあります。



## 4.1 ユーザメールボックスの管理タスク

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントが所有するMicrosoft Exchangeのメールボックスを管理することができます。Microsoft Exchangeメールボックスの各管理機能により必要な権限が異なります。ユーザが持っている権限により、変更可能なメールボックスプロパティの種類や、Exchangeメールボックスの作成、クローン作成、表示、削除が可能かどうかが決まります。また、ユーザアカウントと関連付けられたメールボックスの権限とパーミッションも管理できます。これにより、Microsoft Exchange環境のセキュリティをコントロールすることができます。選択したメールボックスのタブやフィールドを変更する権限がユーザにない場合、DRAは変更できないタブやフィールドを無効にします。

以下に定義されているタスクに加え、DRA管理者がSkypeおよびSkype Onlineの設定を構成するためにオブジェクトのプロパティでユーザアカウントに対しオプションを有効にしている場合があります。Skypeの設定は、ARMコンソールとWebコンソールの両方でユーザアカウントから行うことができます。Skype OnlineはWebコンソールからのみ設定できます。

## メールボックスを作成する

Microsoft Exchangeのメールボックスを既存のユーザアカウント用に作成できます。新しいメールボックスのプロパティを変更することもできます。

---

**注:** メールボックスを作成するとき、Exchangeポリシーの設定に基づいてExchangeが必要なプロキシ文字列を生成します。Microsoft Exchangeでも、デフォルトのプロキシ文字列を生成します。この結果、新しく作成されたメールボックスのプロパティを表示すると、2種類のプロキシ文字列が表示されます。

---

## ユーザアカウントのクローンを作成する

ユーザアカウントのクローンを作成すると、そのユーザがメンバーになっているすべてのグループが新しいユーザアカウントに自動的に追加されるため、クローンとして作成されたアカウントのための設定時間が省けます。クローンとして作成されたアカウントに対しては、グループの追加または削除、およびメールの有効化など、様々なプロパティ設定を新規アカウントのときと同様に行うことができます。

---

**注:** InetOrgPersonオブジェクトのクローンを作成するときには、ユーザアカウントを作成します。

---

## メールボックスを移動する

ユーザアカウント用のMicrosoft Exchangeのメールボックスを、別のメールボックスストアやMicrosoft Exchangeのサーバーに移動することができます。

## メールボックスのプロパティを変更する

Microsoft Exchangeのメールボックスのプロパティを変更しつつ、関連するユーザアカウントの管理を行うことができます。所有する権限により、変更できるメールボックスプロパティが異なります。

---

**注:** メンバーサーバ上で管理されるユーザアカウントのメールボックスプロパティを変更することはできません。

---

## メールボックスのセキュリティパーミッションを設定する

特定のMicrosoft Exchangeメールボックスを使用して電子メールを送受信する機能を付与する(または付与させない)ユーザアカウント、グループ、またはコンピュータを指定することができます。これらの設定により、Exchange環境の安全性を高めることができます。継承したセキュリティパーミッションを変更することはできません。

---

**注:** メールボックスのセキュリティを管理するとき、オフになっているパーミッションは継承されたパーミッションを示す場合があります。

---

## メールボックスのセキュリティパーミッションを削除する

Microsoft Exchangeメールボックスと関連付けられたユーザアカウント、グループ、またはコンピュータからメールボックスのセキュリティパーミッションを削除することができます。メールボックスのセキュリティパーミッションを削除すると、ユーザアカウント、グループ、またはコンピュータアカウントは、指定されたメールボックスから電子メールを送受信できなくなります。継承したセキュリティパーミッションを削除することはできません。

## メールボックスの権限を設定する

他のユーザアカウント、グループ、またはコンピュータに特定のMicrosoft Exchangeメールボックスへの権限を付与したり付与させないようにすることができます。これらの設定により、Exchange環境の安全性を高めることができます。継承したメールボックス権限を変更することはできません。

---

**注:** メールボックスの権限を管理するとき、オフになっているパーミッションが継承されたパーミッションを示す場合があります。

---

## メールボックスの権限を削除する

特定のMicrosoft Exchangeメールボックスと関連付けられたユーザアカウント、グループ、またはコンピュータからメールボックスの権限を削除することができます。メールボックスの権限を削除すると、ユーザアカウント、グループ、またはコンピュータアカウントは、指定されたメールボックスが使用できなくなります。継承したメールボックス権限を削除することはできません。

## メールボックスを削除する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントに関連付けられたメールボックスを削除することができます。メールボックスを削除すると、メールボックスの中すべてのメッセージが削除されます。

## 電子メールアドレスを追加または変更する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントに関連付けられたメールボックスに電子メールアドレスを指定することができます。メールボックスを所有していないユーザアカウントに電子メールアドレスを割り当てることもできます。Microsoft Exchangeメールボックスを管理するときに、プロキシ生成ポリシーによって定義された電子メールアドレスの種類だけを追加することができます。

## 返信アドレスを指定する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントに関連付けられたメールボックスに返信アドレスを設定することができます。1つのメールボックスに複数の返信アドレスを設定することができます。ただし、1つの返信アドレスとして複数種類の電子メールアドレスを設定することはできません。たとえば、1つの返信アドレスとして複数のインターネットアドレスを指定することはできません。

## 電子メールアドレスを削除する

メールボックスからアドレスを削除することにより、電子メールアドレスを削除することができます。

## 配信オプションを指定する

メッセージ送信にユーザが使用できるメールボックスの指定、転送オプションの設定、受信者制限の指定を行うことができます。

## 配布制限を指定する

配布制限を設定することにより、特定のメールボックスに関する着信および送信メッセージのサイズや着信メッセージの受け取りを制限することができます。

## ストレージの制限を指定する

メールボックスのサイズに基づく警告など、保存限度を指定することができます。削除された項目の保持期間を指定することもできます。

### メールボックスの移動ステータスをチェックする

メールボックスの移動ステータスを確認してアクション(ステータスのクリア、移動のキャンセル、中断された移動の再開など)を実行することができます。

## 4.2 Office 365のメールボックスの管理タスク

このセクションには、Account and Resource ManagementコンソールおよびWebコンソールからMicrosoft Office 365のメールボックスを管理するための情報が掲載されています。適切な権限があれば、訴訟ホールドの配置や電子メール転送を設定など、さまざまなユーザアカウント管理タスクが実行できます。

### 訴訟ホールドを設定する

訴訟が合理的に予期できる状況では、場合によって訴訟ホールドが必要になります。組織には、訴訟に関連する電子的に保存された情報(電子メールなど)を保管しておく義務があります。

メールボックスに対し訴訟ホールドを設定すると、削除された項目、変更された項目の元版を含め、メールボックス内のすべてのコンテンツが保持できます。また、ユーザのメールボックスを訴訟ホールドにすることで、ユーザのアーカイブメールボックス(もしあれば)内のコンテンツも保管できます。このホールドは、指定された期間、または手動でメールボックスの訴訟ホールドを解除するまで、効力を保ちます。

訴訟ホールドを使用するには、Exchange OnlineのEnterprise E3のライセンスが必要です。この機能はユーザオブジェクトプロパティ内の **[Litigation Hold (訴訟ホールド★)]** タブで設定します。

### メールボックスのパーミッションを委任する

ユーザオブジェクトのプロパティの中の **[メールボックスの委任]** タブでOffice 365のメールボックスパーミッションを委任することができます。委任できるパーミッションには、「メールボックス所有者として送信する」、「代理人として送信する」、「フルアクセス」の3種類があり、委任できるパーミッションのタイプは受信側のオブジェクトタイプによって異なります。

### 電子メールの転送を設定する

ユーザアカウントのメール転送は、ユーザオブジェクトのプロパティの中のメールフローのオプションで有効にすることができます。

## 4.3 リソースメールボックスの管理タスク

Microsoft Exchangeのリソースメールボックス機能を使えば、会議室などリソースのメールボックスが作成できます。会議室なら、参加予定の人と共に会議室のメールボックスにも会議招待メールを送ることでその会議室が予約できます。DRAには、一連の役割、権限、およびポリシーが含まれています。これによりリソースのメールボックスが効率的に管理できます。

DRAでは、リソースのメールボックスを使うためのUI拡張と、監査やUIレポートの生成がサポートされています。ADSIスクリプトのサポートもDRAに組み込まれています。

### リソースメールボックスを作成する

管理対象ドメインまたは管理対象サブツリー内にリソースメールボックスを作成することができます。

### **リソースメールボックスを別のコンテナに移動する**

リソースメールボックスを管理対象ドメインまたは管理対象サブツリー内の別のコンテナ(OU など)に移動することができます。

### **リソースのメールボックスを別のメールボックスストアまたはExchangeサーバに移動する**

リソースのメールボックスを別のメールボックスストアやMicrosoft Exchangeサーバに移動することができます。

### **リソースメールボックスのクローンを作成する**

リソースのメールボックスのクローンを作成することで、似たプロパティを持つ他のリソースのメールボックスが素早く作成できます。リソースのメールボックスのクローンを作成するときは、選択されたリソースからの値がDRAによって [Clone Resource Mailbox (リソースメールボックスのクローン作成★)] ウィザードに設定されます。

### **リソースメールボックスの名前を変更する**

管理対象ドメインまたは管理対象サブツリー内のリソースメールボックスの名前を変更することができます。ユーザのログオン名を変更すると、そのユーザアカウントに対応するメールボックスの名前も変更されます。

### **リソースメールボックスをグループに追加する**

管理対象ドメインまたは管理対象サブツリー内の特定のグループにリソースメールボックスを追加することができます。

### **リソースメールボックスをコンテナから削除する**

管理対象ドメインまたは管理対象サブツリーからリソースメールボックスを削除することができます。そのドメインでゴミ箱が無効になっている場合、削除されたリソースメールボックスはActive Directoryから永久に削除されます。そのドメインでゴミ箱が有効になっている場合、削除されたリソースメールボックスはゴミ箱に移動します。

### **リソースメールボックスを削除する**

管理対象ドメインまたは管理対象サブツリー内のリソースメールボックスを削除することができます。リソースメールボックスを削除すると、その中にあったすべてのメッセージも削除されます。

### **削除されたリソースメールボックスを復元する**

ドメインでゴミ箱が有効になっていれば、削除されていたリソースメールボックスを復元することができます。

### **リソースメールボックスのプロパティを変更する**

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントのプロパティを管理することができます。所有する権限により、変更できるプロパティが異なります。



## 4.4 共有メールボックスの管理タスク

共有メールボックスは、複数のユーザがアクセスできる1つのメールボックスにすべての応答が入るように設定できるため、ヘルプデスクの管理者やテクニカルサポートのスタッフにとって便利な機能です。このメールボックスは、Exchangeポリシーを有効にしたDRAの管理対象ドメイン内に存在する必要があります。使用するには、共有メールボックスの管理権限が委任されている必要があります。

共有メールボックスを作成する場合、ユーザに委任できるパーミッションが2種類あり、「メールボックス所有者として送信する」と「フルアクセス」です。「メールボックス所有者として送信する」は、電子メールの閲覧と送信が可能なパーミッションです。パーミッションはユーザに対してもグループオブジェクトに対しても委任することができます。また、配信制限、配信オプション、ストレージ制限、フォルダパーミッション、およびその他のいくつかのオプションをオブジェクトのプロパティで指定することもできます。

共有メールボックスの管理はWebコンソールでのみサポートされています。

### 共有のメールボックスを作成する

管理対象ドメインまたは管理対象サブツリー内に共有メールボックスを作成することができます。

### 共有メールボックスを別のコンテナに移動する

共有メールボックスを管理対象ドメインまたは管理対象サブツリー内の別のコンテナ(OUなど)に移動することができます。

### 共有メールボックスを別のメールボックスストアに移動する

共有メールボックスを別のメールボックスストアに移動することができます。

### 共有メールボックスのクローンを作成する

共有メールボックスのクローンを作成することで、プロパティが類似する別の共有メールボックスを素早く作成することができます。

### 共有メールボックスの名前を変更する

管理対象ドメインまたは管理対象サブツリー内の共有メールボックスの名前を変更することができます。ユーザのログオン名を変更すると、そのユーザアカウントに対応するメールボックスの名前も変更されます。

### コンテナから共有メールボックスを削除する

管理対象ドメインまたは管理対象サブツリーから共有メールボックスを削除することができます。そのドメインでゴミ箱が無効になっている場合、削除された共有メールボックスはActive Directoryから永久に削除されます。そのドメインでゴミ箱が有効になっている場合、削除された共有メールボックスはゴミ箱に移動します。

### 共有メールボックスを削除する

管理対象ドメインまたは管理対象サブツリー内の共有メールボックスを削除することができます。共有メールボックスを削除すると、その中にあったすべてのメッセージも削除されます。

### 削除された共有メールボックスを復元する

共有メールボックスが削除されても、そのドメインからのゴミ箱が有効になっていれば、共有メールボックスを復元することができます。

### アーカイブ共有メールボックスを作成する

アーカイブ共有メールボックスは管理対象ドメインまたは管理対象サブツリー内に作成することができます。

### アーカイブ共有メールボックスを削除する

管理対象ドメインまたは管理対象サブツリー内のアーカイブ共有メールボックスは削除することができます。

### 共有メールボックスのプロパティを変更する

管理対象ドメインまたは管理対象サブツリー内の共有メールボックスのプロパティは変更することができます。所有する権限により、変更できるプロパティが異なります。

## 4.5 リンクされたメールボックスの管理タスク

リンクされたメールボックスは、メールボックスのマイグレーションがよく行われる大規模な組織変更(企業の合併、買収、分社)の際に便利です。この機能により、異なるExchangeフォレストからメールボックスをリンクさせてユーザの電子メールの混乱を回避することができます。Exchangeポリシーを有効にしたDRAの管理対象ドメインにすべてのメールボックスが存在する必要があります。また、使用するには、リンクされたメールボックスを管理する権限が委任されている必要があります。リンクされたメールボックスを作成するとき、**「リンクされたメールボックス」**タブがユーザオブジェクトプロパティに追加されます。

リンクされたメールボックスの管理は、Webコンソールでのみサポートされています。リンクされたメールボックスは、選択したユーザアカウントのツールバーから作成します。このオプションは、選択されたユーザのドメインがDRAの他の管理対象ドメインと外部フォレストの信頼を有している場合にのみ、有効になります。別のDRA管理対象ドメインにあるリンク先アカウントを検索する際、無効なユーザアカウントのみがリスト表示されます。

### リンクされたメールボックスを作成する

異なる管理対象Exchangeフォレストから選択した2つのユーザアカウントで、リンクされたメールボックスが作成できます。

### リンクされたメールボックスを削除する

リンクされたメールボックスは、リンクされたメールボックスを持つユーザを選択してから、そのツールバーから削除することができます。

### リンクされたメールボックスのプロパティを変更する

リンクされたメールボックスのプロパティは、選択したユーザプロパティ内の**「リンクされたメールボックス」**タブで変更できます。

### リンクされたアーカイブメールボックスを作成する

リンクされたアーカイブメールボックスは、リンクされたメールボックスを持つユーザを選択して、そこから作成することができます。

### リンクされたアーカイブメールボックスを削除する

リンクされたアーカイブメールボックスは、リンクされたアーカイブメールボックスを持つユーザを選択してから、そのツールバーから削除することができます。

### 削除されたリンクされたメールボックスを復元する

リンクされたメールボックスが削除されても、そのドメインのごみ箱が有効になっていれば、リンクされたメールボックスを復元することができます。

## 4.6 パブリックフォルダの管理タスク

DRA管理者がDRA管理下の企業内にパブリックフォルダのフォレストを作成し、そのDRA管理者からDRAでパブリックフォルダを管理する権限をもらった場合、パブリックフォルダの作成、プロパティの変更、変更履歴のレポート生成ができるようになります。パブリックフォルダの作成および変更は、Webコンソールでのみ実行できます。パブリックフォルダのタスクは、**[管理]** > **[パブリックフォルダ]** タブから実行します。

### パブリックフォルダを作成する

Webコンソールを使用して指定のパブリックフォルダのドメイン、サブツリー、およびメールボックスに新規のパブリックフォルダを作成することができます。選択されたドメインのデフォルトのメールボックスを使用することも、1つを選択することもできます。

### パブリックフォルダの電子メールを有効にする

リストツールバーの**[メールを有効にする]**というオプションを使用してパブリックフォルダの電子メールを有効にすることができます。これにより、電子メールアドレスをパブリックフォルダに関連付けて、パブリックフォルダのプロパティを変更することができます。

### パブリックフォルダの電子メールを無効にする

リストツールバーの中の**[メールを無効にする]**というオプションを使用すればパブリックフォルダの電子メールを無効にすることができます。

### パブリックフォルダのプロパティを変更する

既存のパブリックフォルダに対してメールを有効にした後は、そのフォルダの統計情報を表示したり、そのパブリックフォルダのプロパティを変更することができます。これらのプロパティでは、ユーザ配信と制約のオプション、サイズ制限と割り当て量の警告、メールのプロパティ、ストレージの経過時間制限、承認メールへの管理者の包含、およびカスタム属性が変更できます。

---

**注:** また、複数のフォルダが選択されたとき、複数のパブリックフォルダに関して一部のプロパティ(ストレージの制限など)を更新することもできます。

---

### パブリックフォルダを削除する

サブフォルダが1つもなく、電子メールのオプションが無効な場合、パブリックフォルダを削除することができます。

# 5 リソースの管理

DRAでは、コンピュータ、プリンタ、その他のデバイスなどのリソースとともに、これらのリソースに関連付けられているプロセスも管理することができます。たとえば、管理対象コンピュータで特定サービスを起動する必要がある場合、DRAでそのコンピュータオブジェクトを検索してオブジェクトプロパティからそのサービスにアクセスし、そのコンピュータに対し(リモート操作する必要なしに) DRAから特定サービスを再起動できます。

## 5.1 部門(OU)の管理

このセクションでは、AccountandResourceManagementコンソールを使用して、OUを管理する方法について説明します。適切な権限を使用して、OUの別のコンテナへの移動など、さまざまなOU管理タスクを実行することができます。

### OUプロパティの変更

OUのプロパティを変更することができます。所有する権限により、管理ドメインまたは管理サブツリーの中のOUに対して変更できるプロパティが異なります。

### OUの作成

管理ドメインまたは管理サブツリーの中にOUを作成することができます。OUの説明など、一般的なプロパティも変更することができます。

### OUの複製

管理ドメインまたは管理サブツリーの中の既存のOUを複製することにより、OUを新規作成することができます。OUの説明など、新しいOUの一般的なプロパティも変更することができます。OUを複製しても、OUの中のオブジェクトは複製されません。

### Active DirectoryツリーをOUの場所に開く

管理ドメインまたは管理サブツリーの中の特定のOUの場所にActive Directoryツリーを簡単に開くことができます。

### 別のコンテナへのOUの移動

管理ドメインの中の異なるコンテナにOUを移動することができます。ドメインのサブツリーを管理するときに、そのサブツリーの階層内でOUを移動することができます。

---

#### 注

- ◆ 別のコンテナへのOUの移動により、移動されたOUに対するユーザーの権限が増える場合には、そのOUの移動は許可されません。
  - ◆ OUをドラッグすることにより新しい場所に移動することもできます。
-

## OUの削除

管理ドメインまたは管理サブツリーの中のOUを削除することができます。削除できるのは空のOUのみです。OUにオブジェクトが含まれていると、そのOUは削除できません。オブジェクトを含むOUを削除するには、最初にすべてのオブジェクトを削除してから、そのOUを削除します。

## 5.2 コンピュータの管理

管理対象ドメインまたは管理対象サブツリー内にあるコンピュータをDRAで管理することができます。たとえば、管理対象ドメインへのコンピュータアカウントの追加や削除、各コンピュータ上のリソースの管理が可能です。ドメインにコンピュータを追加すると、DRAによってドメインの中にそのコンピュータのアカウントが作成されます。次に、そのドメインのコンピュータに接続して、そのコンピュータアカウントを使用するようにコンピュータを設定します。コンピュータアカウントのプロパティを表示し、変更することもできます。DRAでは、管理対象ドメイン内のコンピュータをシャットダウンしたり、ドメインコントローラを同期させることもできます。

---

**注:** 非表示のドメインコントローラを管理することはできません。ドメインキャッシュには、非表示のドメインコントローラは含まれません。このため、DRAは非表示のドメインコンピュータをリストやプロパティウィンドウに表示しません。

---

### コンピュータにグループメンバーシップを指定する

管理対象ドメインまたは管理対象サブツリー内の特定のグループにコンピュータを追加したり削除することができます。このコンピュータが属する既存のグループのプロパティを表示し、変更することもできます。

### コンピュータアカウントのプロパティを管理する

コンピュータアカウントのプロパティを管理することができます。所有する権限により、管理対象ドメインまたは管理対象サブツリー内のコンピュータに対して変更できるプロパティが異なります。

### ドメインにコンピュータを追加する

新しいコンピュータアカウントを作成することにより、管理対象ドメインまたは管理対象サブツリーにコンピュータを追加することができます。

### ドメインからコンピュータを削除する

コンピュータアカウントを削除することにより、管理対象ドメインまたは管理対象サブツリーからコンピュータを削除することができます。

### コンピュータを移動する

管理対象ドメインまたは管理対象サブツリー内にある別のコンテナ(OUなど)にコンピュータを移動することができます。

### コンピュータをシャットダウンまたは再起動する

コンピュータをシャットダウンして、即座にまたは指定された日付と時刻に再起動することができます。

### 管理者アカウントのパスワードをリセットする

コンピュータの管理者アカウントパスワードをリセットするには、Reset Password for Local Administrator権限か、この権限を含む役割を持っている必要があります。管理対象ドメインまたは管理対象サブツリー内のメンバーサーバの管理パスワードをリセットすることができます。ドメインコントローラの管理者パスワードをリセットすることはできません。

### コンピュータアカウントをリセットする

管理対象ドメインまたは管理対象サブツリー内のメンバーサーバのコンピュータアカウントをリセットすることができます。ドメインコントローラのコンピュータアカウントをリセットすることはできません。

### コンピュータアカウントを削除する

管理対象ドメインまたは管理対象サブツリー内のコンピュータアカウントを削除することができます。Microsoft Windowsドメインを管理している場合は、共有リソースなど、他のオブジェクトを含むコンピュータアカウントを削除することができます。そのドメインでゴミ箱が無効になっている場合、コンピュータアカウントを削除すると、そのコンピュータアカウントはActive Directoryから永久に削除されます。そのドメインでゴミ箱が有効になっている場合は、コンピュータアカウントを削除すると、そのコンピュータアカウントはゴミ箱に移動します。

---

**注:** 管理対象ドメインまたは管理対象サブツリー内のメンバーサーバのコンピュータアカウントを削除することはできません。

---

### コンピュータアカウントを無効にする

管理対象ドメインまたは管理対象サブツリー内のコンピュータアカウントを無効にすることができます。コンピュータのアカウントを無効にすると、そのコンピュータのユーザはどのドメインにもログオンすることができなくなります。

### コンピュータアカウントを有効化する

管理対象ドメインまたは管理対象サブツリー内のコンピュータアカウントを有効にできます。コンピュータのアカウントを有効にすると、そのコンピュータのユーザがどのドメインにもログオンできるようになります。

### コンピュータのリソースを管理する

管理対象ドメインまたは管理対象サブツリー内の各コンピュータアカウントごとに、サービス、共有リソース、プリンタ、プリントジョブなど、関連リソースを管理することができます。

## 5.3 サービスの管理

サービスとは、Windowsオペレーティングシステムから特別な処理を取得するアプリケーションの種類です。コンピュータにログオンしているユーザが1人もいないときでも、サービスが実行されることがあります。DRAでは、適切な権限を持つアシスタント管理者がAccount and Resource Managementコンソールからサービスを管理することができます。

### サービスのプロパティを管理する

管理対象ドメインまたは管理対象サブツリー内のコンピュータ上で実行されるサービスのプロパティを管理することができます。コンピュータのリソース管理の一貫としてサービスを管理することができます。

### サービスを起動する

管理対象ドメインまたは管理対象サブツリー内のコンピュータ上でサービスを起動することができます。

### パラメータを使用してサービスを起動する

パラメータを受け入れるサービスを起動すると、起動時にこれらのパラメータを指定することができます。管理対象ドメインまたは管理対象サブツリー内のコンピュータ上でサービスを起動することができます。

### サービスの起動タイプを指定する

マニュアルでの起動を必要とするなど、サービスの起動タイプを変更することができます。

### サービスのログオンアカウントを指定する

サービスログオンアカウントを、現在のシステムアカウント以外のアカウントに変更することができます。管理対象ドメインまたは管理対象サブツリー内のコンピュータ上で実行されるサービスのログオンアカウントを指定することができます。ローカルシステムのアカウントまたは特定のユーザアカウントを指定することができます。

### サービスを再開する

管理対象ドメインまたは管理対象サブツリー内のコンピュータ上で実行されるサービスを再起動することができます。

サービスを再起動するには、Stop a ServiceおよびStart a Service権限の両方か、Start and Stop Service役割など、これらの権限を含む役割を持っている必要があります。

### サービスを停止する

管理対象ドメインまたは管理対象サブツリー内のコンピュータ上で実行されるサービスを停止することができます。

### サービスを一時停止にする

管理対象ドメインまたは管理対象サブツリー内のコンピュータ上で実行されるサービスを一時停止にすることができます。サービスの種類によっては、サービスを一時停止にできない場合があります。たとえば、他のサービスに依存されているサービスの場合、一時停止にできないことがあります。

### 一時停止中のサービスを再開する

管理対象ドメインまたは管理対象サブツリー内のコンピュータ上で一時停止になっていたサービスを再開することができます。

## 5.4 プリンタとプリントジョブの管理

プリンタを管理するには、そのプリンタのプリントキューを管理します。DRAでリソースプリンタおよび公開プリンタを一時停止/再開、起動、変更、停止、および表示することができます。DRAでは、プリントジョブのプロパティや優先順位を変更することもできます。プリンタの追加や削除を実行するには、ネイティブのWindowsツールを使用してください。

プリントサーバとは、1台以上の論理プリンタがインストールされたコンピュータです。論理プリンタは、プリンタデバイスドライバを持つコンピュータ上に定義されます。論理プリンタには、プリンタドライバ、プリントキュー、およびプリンタポートが含まれます。プリントサーバは、論理プリンタとプリンタデバイスを関連付けます。



接続されたプリンタは、印刷のために文書が選択されたコンピュータ上に定義されます。接続されたプリンタは、ネットワーク上の印刷共有リソースに接続されます。このため、関連付けられたコンピュータを通してプリンタとプリントジョブを管理することができます。

公開プリンタとは、Active Directory内で公開されたプリンタです。公開プリンタは、サーバに直接接続されていないネットワークプリンタや、クラスタサーバによってホストされたプリンタである場合もあります。

## 5.4.1 プリンタ管理タスク

管理対象ドメインまたは管理対象サブツリー内のコンピュータと関連付けられたプリンタを管理することができます。DRAでは、コンピュータのリソース管理の一貫としてプリンタを管理することができます。

このセクションでは、AccountandResourceManagementコンソールを使用して、プリンタを管理する方法について説明します。適切な権限を使用して、プリンタの停止など、さまざまなプリンタ管理タスクを実行することができます。

### プリンタのプロパティを管理する

管理対象ドメインまたは管理対象サブツリー内のプリンタのプロパティを管理することができます。DRAでは、コンピュータのリソース管理の一貫としてプリンタを管理することができます。

### プリンタを一時停止にする

管理対象ドメインまたは管理対象サブツリー内のコンピュータに関連付けられたプリンタを一時停止にすることができます。DRAでは、コンピュータのリソース管理の一貫としてプリンタを管理することができます。

### プリンタを再開する

管理対象ドメインまたは管理対象サブツリー内のコンピュータに関連付けられたプリンタを再開することができます。DRAでは、コンピュータのリソース管理の一貫としてプリンタを管理することができます。

## 5.4.2 プリントジョブ管理タスク

管理対象ドメインまたは管理対象サブツリー内のプリンタに関連付けられたプリントジョブを管理することができます。プリントジョブはプリンタと関連付けられるため、プリンタ管理の一貫としてプリントジョブを管理することができます。

このセクションでは、AccountandResourceManagementコンソールを使用して、プリントジョブを管理する方法について説明します。適切な権限を使用して、プリントジョブのキャンセルなど、さまざまなプリントジョブ管理タスクを実行することができます。

### プリントジョブプロパティを管理する

プリントジョブのプロパティは、プリンタ管理ワークフローの一部として変更することができます。プリントジョブはプリンタと関連付けられるため、対応するプリンタの管理の一貫としてプリントジョブを変更することができます。変更可能なプリントジョブのプロパティは、ユーザの権限の種類によって異なります。プリントジョブのプロパティを変更するには、関連するプリンタとコンピュータにアクセスできなければなりません。

### プリントジョブを一時停止にする

管理対象ドメインまたは管理対象サブツリー内のプリンタ上のプリントジョブを一時停止にすることができます。プリントジョブを一時停止するには、関連するプリンタとコンピュータにアクセスできなければなりません。プリントジョブが一時停止になっても、そのプリントジョブはプリントキューから削除されません。

### プリントジョブを再開する

一時停止になっていたプリントジョブを再開することができます。プリントジョブを再開するには、関連するプリンタとコンピュータにアクセスできなければなりません。

### プリントジョブを再起動する

停止されたプリントジョブを再起動することができます。プリントジョブを再起動するには、関連するプリンタとコンピュータにアクセスできなければなりません。

### プリントジョブをキャンセルする

プリンタキューの中のプリントジョブをキャンセルすることができます。プリントジョブをキャンセルすると、DRAはそのプリントジョブをプリンタキューから永久に削除します。プリントジョブをキャンセルするには、関連するプリンタとコンピュータにアクセスできなければなりません。

## 5.4.3 公開プリンタの管理タスク

管理対象ドメインまたは管理対象サブツリー内の公開プリンタを管理することができます。Active Directory内で公開されているすべてのプリンタ、またはクラスタサーバによってホストされるプリンタを、追加または検索することができます。

このセクションでは、AccountandResourceManagementコンソールを使用して、公開プリンタを管理する方法について説明します。適切な権限を使用して、プリンタの停止など、さまざまなプリンタ管理タスクを実行することができます。

### 公開プリンタのプロパティを管理する

管理対象ドメインまたは管理対象サブツリー内の公開プリンタのプロパティを管理することができます。DRAでは、リソース管理の一貫として公開プリンタを管理することができます。

### 公開プリンタの情報を更新する

管理対象ドメインまたは管理対象サブツリー内の公開プリンタの情報を更新することができます。DRAでは、リソース管理の一貫として公開プリンタを管理することができます。

### 公開プリンタを一時停止にする

管理対象ドメインまたは管理対象サブツリー内にある公開プリンタを一時停止させることができます。DRAでは、リソース管理の一貫として公開プリンタを管理することができます。

### 公開プリンタを再開する

管理対象ドメインまたは管理対象サブツリー内にある一時停止中の公開プリンタを再開させることができます。DRAでは、リソース管理の一貫として公開プリンタを管理することができます。

### 公開プリンタを移動する

管理対象ドメイン内の1つのコンテナ内にある公開プリンタを同ドメイン内の別のコンテナに移動させることができます。DRAでは、リソース管理の一貫として公開プリンタを管理することができます。

## 公開プリンタの名前を変更する

Active Directoryの中の共有公開プリンタの名前を変更することができます。DRAでは、リソース管理の一貫として公開プリンタを管理することができます。

---

**注:** Active Directoryの中の公開プリンタの名前を変更しても、リソースプリンタの共有名が変更されることはありません。また、名前の変更が管理するリソースプリンタに伝播されることはありません。たとえば、「Emerald」という名前のリソースプリンタがあり、Active Directoryでプリンタ名を「Ruby」に変更する場合、他のユーザに表示されるプリンタ名はRubyですが、リソースプリンタ名はEmeraldのままです。

---

## 5.4.4 公開プリンタのプリントジョブ管理タスク

管理対象ドメインまたは管理対象サブツリー内にある公開プリンタに関連付けられたプリントジョブを管理することができます。プリントジョブはプリンタと関連付けられるため、公開プリンタ管理の一貫としてプリントジョブを管理することができます。

このセクションでは、AccountandResourceManagementコンソールを使用して、公開プリンタを管理する方法について説明します。適切な権限を使用して、プリントジョブのキャンセルなど、さまざまなプリントジョブ管理タスクを実行することができます。

### プリントジョブプロパティを管理する

プリントジョブのプロパティは、公開プリンタ管理のワークフローの一部として変更することができます。プリントジョブはプリンタと関連付けられるため、対応する公開プリンタの管理の一貫としてプリントジョブを変更することができます。変更可能なプリントジョブのプロパティは、ユーザの権限の種類によって異なります。プリントジョブのプロパティを変更するには、関連する公開プリンタにアクセスできなければなりません。

### プリントジョブを一時停止にする

管理対象ドメインまたは管理対象サブツリー内にある公開プリンタ上のプリントジョブを一時停止させることができます。プリントジョブを一時停止にするには、関連する公開プリンタにアクセスできなければなりません。プリントジョブが一時停止になっても、そのプリントジョブはプリントキューから削除されません。

### プリントジョブを再開する

管理対象ドメインまたは管理対象サブツリー内にある一時停止中のプリントジョブを再開させることができます。プリントジョブを再開するには、関連する公開プリンタにアクセスできなければなりません。

### プリントジョブを再起動する

管理対象ドメインまたは管理対象サブツリー内にある停止したプリントジョブを再起動することができます。プリントジョブを再起動するには、関連する公開プリンタにアクセスできなければなりません。

### プリントジョブをキャンセルする

管理対象ドメイン内または管理対象サブツリー内にあるプリンタキューに入ったプリントジョブをキャンセルすることができます。プリントジョブをキャンセルすると、DRAはそのプリントジョブをプリンタキューから永久に削除します。プリントジョブをキャンセルするには、関連する公開プリンタにアクセスできなければなりません。

## 5.5 共有の管理

共有は、ファイルやプリンタなどのリソースをネットワーク上の他のユーザに使用できるようにする手段です。各共有に共有名があり、共有名がサーバ上の共有フォルダを参照しています。DRAは、管理対象ドメイン内のコンピュータ上にある共有だけを管理します。共有を管理するには、リソースを管理するすべてのコンピュータに対する管理者権限(ローカル管理者グループのメンバーなど)がアクセスアカウントに付与されていなければなりません。これらのパーミッションを割り当てるには、コンピュータのドメイン内のDomain Adminsというネイティブグループにアクセスアカウントを追加します。

### 共有プロパティを管理する

管理対象ドメインまたは管理対象サブツリー内にある共有のプロパティを管理することができます。DRAでは、コンピュータのリソース管理の一貫として共有を管理することができます。

### 共有を作成する

管理対象ドメインまたは管理対象サブツリー内にあるコンピュータ上で共有を作成することができます。共有のプロパティを変更することもできます。

### 共有のクローンを作成する

管理対象ドメインまたは管理対象サブツリー内にあるコンピュータ上で共有のクローンを作成することができます。共有のクローンを作成することにより、同様のプロパティを持つ他の共有をベースとして簡単に共有を作成することができます。この機能を利用して、特定のドメインの中に作成するすべての共有を同一の設定にすることができます。

共有のクローンを作成すると、選択された共有から値が取り込まれ、[Clone Share (共有のクローン作成★)] ウィザードに設定されます。新しい共有のプロパティを変更することもできます。

### 共有を削除する

管理対象ドメインまたは管理対象サブツリー内にあるコンピュータから共有を削除することができます。

## 5.6 接続ユーザの管理

ユーザがリモートコンピュータ上のリソースに接続するたびにセッションが確立されます。接続ユーザとは、ネットワーク上の共有リソースに接続されたユーザです。

DRAは、管理対象ドメイン内のコンピュータ上の接続ユーザのみを管理します。アクセスアカウントには、接続ユーザを管理するすべてのコンピュータに対する管理者権限(ローカル管理者グループのメンバーなど)がなければなりません。これらのパーミッションを割り当てるには、コンピュータのドメイン内のDomain Adminsというネイティブグループにアクセスアカウントを追加します。

### ユーザを接続解除する

管理対象ドメインまたは管理対象サブツリー内のコンピュータから接続ユーザを接続解除することができます。ただし、該当するコンピュータとオープンセッションにアクセスできなければなりません。接続ユーザを切断するとオープンセッションが終了します。

### 接続ユーザのリストを更新する

コンピュータ上のオープンセッションに関して今表示されている情報が最新であることを確信する必要がある場合は、接続されたユーザのリストを手動で更新してください。ただし、該当するコンピュータとオープンセッションにアクセスできなければなりません。

## 5.7 デバイスを管理する

デバイスは、コンピュータ、プリンタ、モデム、またはその他の周辺装置など、ネットワークに接続された装置です。

デバイスがコンピュータ上にインストールされている場合でも、Windowsは適切なドライバがインストールされ、構成されるまで、そのデバイスを認識できません。デバイスドライバは、ハードウェアとオペレーティングシステムとの通信を有効にします。

DRAでは、管理対象ドメイン内のコンピュータ上でのみデバイスを構成および管理することができます。デバイスを管理するすべてのコンピュータに対する管理者権限(ローカル管理者グループのメンバーなど)がアクセスアカウントに付与されていなければなりません。これらのパーミッションを割り当てるには、コンピュータのドメイン内のDomain Adminsというネイティブグループにアクセスアカウントを追加します。

### デバイスのプロパティを管理する

特定のコンピュータ上のデバイスのプロパティを変更することができます。デバイスのデバイスプロパティを変更することにより、デバイスの起動タイプを変更することができます。

### デバイスを起動する

管理対象ドメインまたは管理対象サブツリー内にある特定のコンピュータ上のデバイスを起動することができます。

### デバイスを停止する

管理対象ドメインまたは管理対象サブツリー内にある特定のコンピュータ上のデバイスを停止させることができます。

## 5.8 イベントログの管理

イベントは、重要なシステムまたはアプリケーションの出来事です。Windowsオペレーティングシステムは、イベントに関する情報をイベントログファイルに記録します。各コンピュータ上に複数のイベントログが保管されていることがあります。イベントログを表示するには、ネイティブのWindowsイベントビューアを使用します。DRAは、管理対象ドメイン内にあるコンピュータ上のイベントログだけを管理します。

DRAは、ユーザによって行われた操作を、セキュリティが確保されたリポジトリであるログアーカイブに記録します。ユーザによって行われた操作をDRAのログアーカイブだけでなくWindowsのイベントログにも記録するように、DRAを設定することもできます。詳細については、「[日付と時刻について](#)」を参照してください。

### 5.8.1 イベントログの種類

Microsoft Windowsを実行しているコンピュータでは、さまざまなログに追加情報が記録されます。これらのログについて、以下に簡単に説明します。

ログの種類	説明
ADAM	ADAMリポジトリによって記録されるイベントが書き込まれます。
アプリケーション	サービスの起動や失敗など、コンピュータ上のアプリケーションに関するイベントを記録します。たとえば、DRAではアプリケーションログにイベントを保存します。

ログの種類	説明
ディレクトリサービス	セキュリティデータベースを管理するドメインコントローラに関するイベントを記録します。
ファイルリプリケーションサービス	オペレーティングシステムによって提供されるファイルリプリケーションサービスに関連するイベントを記録します。
セキュリティ	ログオンの試行、ファイルおよびディレクトリアクセス、監査ポリシーオプションに基づくセキュリティポリシーの変更などのイベントを記録します。
システム	ドライバの失敗やサービスの起動や停止など、Windowsシステムのコンポーネントによってログ取りされたイベントを記録します。

## 5.8.2 イベントログ管理タスク

イベントログファイルの最大サイズおよびイベントログが一杯になったときの処理を指定することができます。プロパティウィンドウには、ログ名、ログファイルのパスとファイル名、ログの作成日付、最終変更日付、最終アクセス日付なども表示されます。ログファイルのバックアップを選択すると、DRAは選択されたコンピュータの標準の場所に一意のファイル名が付いたイベントログを保存します。

DRAでは、コンピュータのリソース管理の一貫としてイベントログを管理することができます。適切な権限を使用して、イベントログのプロパティの管理など、さまざまな共有管理タスクを実行することができます。

### WindowsのイベントログによるDRAの監査を有効/無効にする

DRAをインストールしても、監査イベントはデフォルトではWindowsイベントログに記録されません。このタイプのログ記録は、レジストリキーを変更することによって有効にできます。

**警告:** Windowsレジストリを編集するときには十分に注意してください。レジストリ内にエラーがあると、コンピュータが動作不能になる場合があります。エラーが発生した場合は、レジストリを最後にコンピュータを問題なく起動したときの状態に戻すことができます。詳細については、Windowsレジストリエディタのヘルプを参照してください。

### イベントログのプロパティを管理する

特定のコンピュータのイベントログのプロパティを変更することができます。

### イベントログのエントリを表示する

管理対象ドメインまたは管理対象サブツリー内にあるコンピュータ上の特定のイベントログに記録されたエントリを表示することができます。イベントログを表示するときに、ネイティブのWindowsイベントビューアが起動されます。

### イベントログをクリアする

管理対象ドメインまたは管理対象サブツリー内にあるコンピュータ上の特定のイベントログに記録されたエントリをクリアすることができます。ログをクリアする前に、イベントログエントリを保存することもできます。

## 5.9 オープンファイルの管理

オープンファイルは、ファイルやパイプなどの共有リソースへの接続です。パイプとは、1つのプロセスがローカルまたはリモートの別のプロセスと通信できるようにするプロセス間通信メカニズムです。

DRAは、管理対象ドメインまたは管理対象サブツリー内にあるコンピュータ上のファイルだけを管理します。オープンファイルはコンピュータと関連付けられるため、コンピュータのリソース管理の一貫としてオープンファイルを管理することができます。たとえば、システムをシャットダウンしたり、新しいデバイスやサービスをインストールするときに、オープンファイルを閉じる必要があるかもしれません。最も頻繁にユーザにアクセスされるファイルを監視して、ファイルのセキュリティの評価に役立てることもできます。

### ファイルを閉じる

ネットワーク上のリソースからオープンファイルを閉じることができます。オープンファイルを閉じるときには、ユーザに通知することをお勧めします。データを保存する時間が必要な場合があります。オープンファイルを閉じるには、該当するコンピュータにアクセスする必要があります。

### オープンファイルのリストを更新する

コンピュータ上のオープンセッションに関して今表示されている情報が最新であることを確信する必要がある場合は、接続されたユーザのリストを手動で更新してください。オープンファイルのリストを更新するには、該当するコンピュータにアクセスする必要があります。



# 6 高度なクエリの管理

DRAの通常の検索機能では、Active Directory内のオブジェクトの属性(ユーザ、コンピュータ、プリンタ、グループ、OUなど)について検索ができます。またワイルドカード文字での検索を指定することもできます。ただし、DRAの検索機能では、アカウントのロックアウトステータスやアカウントの期限切れステータスなど、カスタマイズされた属性を検索することはできません。詳細検索クエリを使用すると、DRAの検索機能ではできないカスタマイズされた属性を使った検索が実行できます。DRAは、LDAPを使って高度なクエリ機能をサポートしています。高度なクエリを使用すると、ユーザ、連絡先、グループ、コンピュータ、プリンタ、OU、およびDRAがサポートする他のあらゆるオブジェクトを検索できます。

## 高度なクエリを新規作成する

高度なクエリは、プライマリ管理サーバでもセカンダリ管理サーバでも作成できます。また、新しい高度なクエリについて、クエリ文字列などのプロパティを変更することもできます。

## 高度なクエリを変更する

Public Queriesの下に保存された高度なクエリの特定のプロパティを変更できるのは、共有の高度なクエリを変更するために必要なパーミッションが付与されている場合のみです。My Queriesの下に保存されたクエリはどれも、プロパティを変更できます。

## 高度なクエリをコピーする

高度なクエリをPublic QueriesとMy Queriesとの間でコピーできます。高度なクエリをPublic Queriesにコピーすると、必要な権限を持つアシスタント管理者がその高度なクエリを変更および実行することができます。

## 高度なクエリの結果をカスタマイズする

DRAが表示する検索結果リストには、デフォルトの列のセットがあります。検索結果のリストに列を追加したり削除したりして、検索結果をカスタマイズできます。検索結果をカスタマイズできるのは、新規の高度なクエリを作成するときと、高度なクエリに変更を加えるときです。

## 高度なクエリをインポートする

ADUCで作成した高度なクエリを、DRAを使ってそれらのクエリを再作成する代わりに、DRAにインポートすることができます。インポートできる高度なクエリは、XML形式のものだけです。

## 高度なクエリをエクスポートする

DRAで作成した高度なクエリを、ADUCを使ってそれらのクエリを再作成する代わりに、ADUCにエクスポートすることができます。

## 高度なクエリを削除する

Public Queriesの下にある高度なクエリが削除できるのは、共有の高度なクエリを削除するために必要なパーミッションが付与されている場合のみです。My Queriesの下にある高度なクエリは、どれも削除できます。

# 7 ごみ箱の管理

ごみ箱は、ユーザアカウント、グループ、連絡先、コンピュータアカウントを一時的に削除することができるセーフティネットです。ごみ箱に入ったこれらのオブジェクトは、SID、ACL、グループメンバーシップなど、データをすべて損なわずに元の状態に戻すこともでき、永久に削除することもできます。この柔軟性により、ユーザアカウント、グループアカウント、連絡先、およびコンピュータアカウントをより安全に管理することができます。

## ごみ箱からオブジェクトを復元する

削除したオブジェクトを元の場所に戻すことができます。DRAは、SID、ACL、グループメンバーシップを含めすべてのデータと共にオブジェクトを元の状態に復元します。オブジェクトとは、ユーザアカウント、グループ、連絡先、ダイナミックグループ、リソースメールボックス、ダイナミック配布グループ、コンピュータアカウントなどです。

## すべてのオブジェクトを復元する

管理対象ドメインのためのごみ箱からすべてのオブジェクトを復元することができます。選択したドメインまたはすべての管理対象ドメインのごみ箱からオブジェクトを復元することができます。特定のドメインのごみ箱からオブジェクトを復元するには、そのドメインのごみ箱が有効になっている必要があります。

## ごみ箱からオブジェクトを削除する

管理対象ドメインのためのごみ箱からオブジェクトを永久に削除することができます。ごみ箱からオブジェクトを削除すると、そのオブジェクトを元に戻すことはできません。オブジェクトとは、ユーザアカウント、グループ、連絡先、ダイナミックグループ、リソースメールボックス、ダイナミック配布グループ、コンピュータアカウントなどです。

## ごみ箱を空にする

管理対象ドメインのためのごみ箱を空にすることができます。ごみ箱を空にすると、ごみ箱中のオブジェクトはすべて完全に削除されます。ごみ箱を空にする操作は、選択したドメインまたはすべての管理対象ドメインに対して実行できます。特定のドメインのごみ箱を空にするには、そのドメインのごみ箱が有効になっている必要があります。ごみ箱をいったん空にすると、削除されたオブジェクトは復元できなくなります。

# A

## レガシのWebコンソールの使用

レガシのWebコンソールは、DRA9.0.1のリリースから新しいWebコンソールに置き換えられましたが、まだ使用は可能です。このバージョンのWebコンソールのインストールについては、

『*Directory and Resource Administrator管理者ガイド*』の中の「[DRA管理サーバをインストールする](#)」を参照してください。

レガシのWebコンソールは、ユーザアカウント、グループ、コンピュータ、リソース、およびMicrosoft Exchangeメールボックスに関する多くのタスクに素早く簡単にアクセスできるWebベースのユーザインタフェースです。また、所在地や携帯電話番号など、自分のユーザアカウントの一般プロパティを管理することもできます。

レガシのWebコンソールは習得が楽で使いやすいため、非常勤や経験の浅い管理者に適したツールです。このWebコンソールには、各タスクの手順に合わせて順々に説明するヘルプが付属しています。タスクが1つ完了すると、それに関連する別のタスクへのリンクが表示されるため、ワークフロー全体に素早く取り組むことができます。Webコンソールには、自分に実行権限があるタスクのみが表示されます。

### A.1 レガシWebコンソールの起動

WebコンソールはInternet Explorerを実行している任意のコンピュータから起動できます。このWebコンソールを起動するには、Webブラウザのアドレスフィールドに適切なURLを入力するか、AccountandResourceManagementコンソールに表示されるリンクを使用します。たとえば、WebコンポーネントをHOUserServerというコンピュータにインストールした場合、Webブラウザのアドレスフィールドに「http://HOUserServer/dra」と入力します。

---

注: アカウントおよびMicrosoft Exchangeの最新情報をWebコンソールに表示するには、キャッシュされたページが更新されていないかどうかをアクセスのたびにチェックするようにWebブラウザを設定してください。

---

### A.2 クイックスタートの使用による問題解決

クイックスタートで、アカウントの問題を迅速かつ簡単に解決することができます。特定のユーザアカウント、コンピュータ、またはグループに関して主要な統計情報とプロパティを表示することができます。そして、ユーザアカウントのパスワードのリセットなど、適切なタスクにリンクさせて問題に対処することができます。

### A.3 レガシWebコンソールのカスタマイズ

次の方法で、Webコンソールを素早く簡単にカスタマイズできます。

### 指定されたタスクを変更する

たとえば、ユーザのプロパティを更新するタスクを、独自の設定を管理するための新規フィールドを含めるように変更することができます。アシスタント管理者(AA)に使用させたくないタスクがあれば、権限が委任されているかどうかに関係なく、そのような特定タスクをAAに対し非表示にすることができます。Directory and Resource Reportingから生成されたレポートを発行することもできます。

### 新しいタスクを開発する

たとえば、ユーザのプロパティを更新する新しいタスクを、固有の管理ニーズを満たすように開発することができます。組み込まれた機能を失うことなく、提供されたタスクをカスタムタスクに置き換えることができます。

### ワークフローを変更する

たとえば、Webコンソールのフレームワークとナビゲーションを変更してAAによる個々のタスクの処理手順を変えることができます。この柔軟性により、手順を追加、削除、移動させながら所望のソリューションを正確に作成することができます。

### 複数のWebコンソールアプリケーションの展開

複数のWebコンソールアプリケーションをインストールして設定することができます。たとえば、カスタマイズしたWebコンソールアプリケーションをヒューストン市の自社施設に1つ、そして別のカスタマイズしたWebコンソールアプリケーションをアトランタ市の自社施設に1つ配置するということも可能です。各アプリケーションが、個々の施設の特定ニーズを満たすように独自のタスクセットをサポートすることができます。詳細は、『Unique Environments Technical Reference (独自環境の技術リファレンス★)』の「Deploying DRA (DRAの展開★)」を参照してください。Webコンソールのカスタマイズに関する詳細については、『Directory and Resource Administratorソフトウェア開発キット』を参照してください。