HP Integrated Archive Platform
Version 2.1

管理者ガイド

製品番号: N/A
初版: 2010年3月

ご注意

Hewlett-Packard Companyは、本書についていかなる保証（商品性および特定の目的のための適合性に関する黙示の保証を含む）も与えるものではありません。Hewlett-Packard Companyは、本書中の誤りに対して、また本書の供給、機能または使用に関連して生じた付随的損害、派生的損害または間接的損害を含めいかなる損害についても、責任を負いかねますのでご了承ください。

本書には、著作権によって保護されている情報が掲載されています。本書のいかなる部分も、Hewlett-Packard Companyの事前の書面による承諾なしに複写、複製、あるいは他の言語に翻訳することはできません。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。HP製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載で追加保証を意図するものは一切ありません。ここに含まれる技術的、編集上の誤り、または欠如について、HPはいかなる責任も負いません。

Microsoft®およびWindows®は、米国におけるMicrosoft Corporationの登録商標です。Outlook™は、Microsoft Corporationの商標です。

ここに含まれる技術的、編集上の誤り、または欠如について、HPはいかなる責任も負いません。本書の内容は、“そのままの状態で”提供されるもので、いかなる保証も含みません。Hewlett-Packard Company製品に対する保証については、当該製品の保証規定書に記載されています。ここでの記載で追加保証を意図するものは一切ありません。

目次

図一覧

表一覧

本書について

このガイドは、HP Integrated Archive Platform（IAP）の管理についての情報を提供します。Exchange用またはDomino用HP Email Archiving（EA）ソフトウェアの管理については、当該製品のドキュメンテーションCDに収録されているそれぞれの管理者ガイドを参照してください。

対象読者

このガイドは、HP Integrated Archive Platformの管理者を対象としています。

参考資料

HPは、次の参考資料を用意しています。

管理者およびインストール担当者向け：

- 『HP Integrated Archive Platformインストレーションガイド』（IAPをインストールするHPの担当者用）
- Platform Control Center（PCC）のオンラインヘルプ（このヘルプは本管理者ガイドのサブセットです）
- 『Microsoft Exchange用またはIBM Lotus Domino用HP Email Archivingソフトウェアの管理者ガイド』（当該製品のドキュメンテーションCDに収録）
- 『Microsoft Exchange用またはIBM Lotus Domino用HP Email Archivingソフトウェアのインストレーションガイド』（当該製品をインストールするHPの担当者用）

ユーザー向け：

- 『HP Integrated Archive Platformユーザーガイド』（ドキュメンテーションCDに収録）
- IAP Content Search and Retrieve Web Interfaceのオンラインヘルプ（ユーザーガイドのサブセットです）
- 『Microsoft Exchange用またはIBM Lotus Domino用のHP Email Archivingソフトウェアのユーザーガイド』（当該製品のドキュメンテーションCDに収録）

開発者向け：

このリリースには、開発者向けの以下のガイドが含まれています。また、HP Developer and Solution Partner ProgramのWebサイトhttp://www.hp.com/go/ilmdspp/（英語）からも入手できます。

- 『HP Integrated Archive Platform Web Service API Developer Guide』
- 『HP Integrated Archive Platform ILM Object Storage API Developer Guide』

表記上の規則および記号

表1 表記上の規則

表記法	項目
ミディアムブルーの語句：図1	クロスリファレンスリンクおよびEメールアドレス

表記法	項目
ミディアムブルーの下線付き語句（http://www.hp.com）	Webサイトアドレス
太字	• ファイル名、アプリケーション名、および強調するべき語句
括弧（[ ]）で表示	• キー名 • ボックスなどのGUIで入力される文字列 • クリックおよび選択されるGUI（メニューおよびリスト項目、ボタン、チェックボックス）
`Monospace`フォント	• ファイル名およびディレクトリ名 • システムアウトプット • コード • コマンドラインで入力した文字列
イタリック体の`Monospace`フォント	• コード変数 • コマンドライン変数
太字体の **Monospace** フォント	ファイル名、ディレクトリ名、システム出力、コード、コマンドラインで入力される文字列の強調

⚠ 警告!

その指示に従わないと、人体への傷害や生命の危険を引き起こす恐れがある警告事項を表します。

△ 注意：

その指示に従わないと、装置の損傷やデータの消失を引き起こす恐れがある注意事項を表します。

重要：

詳細情報または特定の手順を示します。

注記：

補足情報を示します。

ヒント：

役に立つ情報やショートカットを示します。

サポート

HPソフトウェアサポートのWebサイトを参照するには、http://www.hp.com/go/hpsoftwaresupport にアクセスしてください。

HPソフトウェアサポートオンラインは、インタラクティブなテクニカルサポートツールへの効率的なアクセスを提供します。大切なサポートカスタマーである皆様は、サポートサイトを使用して、以下の利点を得ることができます。

- 関心のある技術ドキュメントの検索
- サポートケースと拡張要求の送信と追跡
- ソフトウェアパッチのダウンロード
- サポート契約の管理
- HPサポート契約の検索
- 使用可能なサービスの情報の確認
- 他のソフトウェアカスタマーとのディスカッションへの参加
- ソフトウェアトレーニングの検索と登録

ほとんどのサポートエリアでは、HPパスポートユーザーとして登録してサインインする必要があります。多くの場合、サポート契約も必要です。

アクセスレベルについて詳しくは、http://support.openview.hp.com/new_access_levels.jsp にアクセスしてください。

1 IAP製品の概要

この章では、HP Integrated Archive Platformの重要な概念を説明します。

IAPの概要

HPのIntegrated Archive Platform（IAP）は、データのアーカイブと保管を管理するための、ハードウェア、ソフトウェア、およびサービスが緊密に統合されたフォールトトレラントで安全なシステムです。IAPは、インタラクティブな高速検索/取得機能と結びついたスケーラブルな長期情報保管機能を提供することで、組織が規格の要件を満たすのに役立ちます。

コンポーネントについて

この章では、IAPのコンポーネントとその連携についての大枠を掴んでいただくために、コンセプト、主な利点と特長、ソフトウェアコンポーネント、ハードウェアコンポーネント、ネットワークアーキテクチャー、データフローなど、レベルの高いいくつかのテーマを取り上げます。ここで、IAPとそのコンポーネントの構成やアーキテクチャーを大まかに見ておけば、IAPシステムの操作、保守、最適化、およびトラブルシューティングの効率化を目指すうえでの支えになります。

コンセプト

大まかなとらえ方をすると、IAPには次の3つの側面があると考えることができます。

1. エンタープライズコンテンツ
2. アプリケーションアーカイブソフトウェア
3. アーカイブされたエンタープライズコンテンツのIAPの機能を介した効率的な運用

エンタープライズコンテンツ

IAPは、さまざまなタイプのエンタープライズコンテンツのプラットフォームの役割を果たします。IAPは、ファイル、電子メール（Exchange、Domino）、文書などの各種データを自動で自発的にアーカイブします（付録B（173ページ）を参照）。

アプリケーションアーカイブソフトウェア

HPは、データの取得と保存を目的に、IAPと連携して機能する各種アプリケーションアーカイブソフトウェアを提供します。これらのソフトウェアコンポーネントの持つ機能は、IAPにデータを取り込むことに向けられます。IAPは、組織のアーカイブポリシーや保管ポリシーに合わせて詳細にカスタマイズおよび設定できます。

IAPは、次のアプリケーションアーカイブソフトウェアを利用します。

HP Email Archiving software（EAs）for Exchange

HP Email Archiving software（EAs）for Exchangeは、メッセージと添付ファイルをアーカイブし、そのメッセージをIAPに保存するメール管理ソフトウェアです。ユーザーは、アーカイブしたメッセージをOutlookから直接検索して取得できます。HP EAs for Exchangeは、Microsoft ExchangeおよびOutlookと完全に統合されています。Outlook Integrated Archive Searchを使用すると、キーワードやデータ範囲を指定してOutlookから直接IAPレポジトリを検索できます。

HP Email Archiving software（EAs）for Domino

HP Email Archiving software（EAs）for Dominoは、メッセージと添付ファイルをアーカイブし、そのメッセージをIAPに保存するメール管理ソフトウェアです。ユーザーは、アーカイブしたメッセージをIBM Lotus NotesおよびiNotesから直接取得できます。また、EAs for DominoはLotus NotesおよびiNotesと完全に統合されています。

HP File Archiving software

HP File Archiving software（FAs）は、ポリシーベースのファイルアーカイブソリューションで、このソフトウェアを使用すると、Windows環境からファイルサーバー、Webサーバー、アプリケーションサーバーのデータを自動的にアーカイブして、IAPに移行できます（FAsは、以前は「FMA」と呼ばれていました）。

アーカイブ方式

HP EAs for ExchangeとHP EAs for Dominoは、次のアーカイブ方式をサポートします。

- Compliance Archiving。EAs for Exchangeでは、Compliance Archivingによりインバウンドとアウトバウンドのメッセージがすべて取得されます。EAs for Exchangeが提供するCompliance Archiving導入のためのメカニズムは2つあります。その技術の1つは、各インバウンド/アウトバウンドメッセージをジャーナルメールボックスにコピーします。そのメールボックスをArchive Gatewayが定期的にスキャンしてその内容をIAPにアーカイブします。Exchange 2007以降で利用できるもう1つの技術では、Simple Mail Transport Protocol（SMTP）を使用して各メッセージがすべて直接Archive Gatewayに転送され、Archive GatewayがそのメッセージをIAPにアーカイブします。EAs for DominoのCompliance Archivingでは、Advanced Filtering機能を使用すれば、メッセージを個人や、グループ、エンタープライズレベルで取得できます。
- Selective Archiving（メールデータベースマイニング）。Selective Archivingは、メールサーバーで使用するプライマリストレージの量の削減に役立ちます。Selective Archivingは、ユーザーのメールボックスからメッセージを取り出すためのポリシーを提供します。管理者は、アーカイブを実行するクォータのスレッショルド、メッセージの経過日数またはサイズ、送信者/受信者、特定のフォルダー、キーワードなどのポリシーを1か所から集中的に設定できます。ポリシーは、個人や、グループ、全エンタープライズレベルで設定できます。ポリシーが有効になると、メッセージは自動的にアーカイブされます。アーカイブの完了後、アーカイブされたメッセージへのリンク（「トゥームストーン」と呼ばれます）をメールデータベースに格納できます。
- 非アクティブメールデータベースのアーカイブ。EAsEとEAsDはオプションとして非アクティブであるPSTファイル（Exchange）およびNSFファイル（Domino）内にあるメッセージもアーカイブし、トゥームストーン化することができます。

IAPでのエンタープライズコンテンツの操作

IAPが包括的に力を注いでいることの1つが、保存したエンタープライズコンテンツを効果的に利用できるようにすることです。IAPに保存されたエンタープライズコンテンツには次のようなさまざまな操作を加えることができ、数多くの可能性と利点がもたらされます。

- 保存

- インデックス作成
- シングルインスタンス
- 保管ポリシー
- 暗号化
- 認証
- 複製
- 監視
- 検索
- 取得
- バックアップ/リストア

主な利点

以下では、IAPがもたらす利点を列挙します。

- 電子情報開示の準備、法的対応、規格準拠に関わるコストを削減し、ビジネスに対する影響を軽減できます。企業は、訴訟に加わる際、その企業の電子メールが改ざんされていないことを証明できなければなりません。また、各訴訟に関する情報を取り出すことも要求されます。
- 情報を効率的に、管理、保管し、取り出すことができます。IAPは、アーカイブしたコンテンツを高速で取り出せるようにすることで、データを情報に生まれ変わらせます。アーカイブシステムからのデータの取得は、ストレージグリッドアーキテクチャーを使用して高速で行われます。このアーキテクチャーでは、数多くのスマートセル(ストレージセル)間に全文インデックスと元のコンテンツが均一に配分されます。検索は、すべてのスマートセルを対象に並列で実行されます。
- 文書をサーバーからIAPに移動してサーバーの負荷を軽減することで、電子メールサーバー、ファイルサーバー、アプリケーションサーバーのパフォーマンスを向上させることができます。メールやファイルをIAPに保存することで、クエリやデータ取得を高速で行えるようになります。IAPは、任意のWebブラウザー経由でのフリーテキスト検索をサポートします。
- 電子メール、ファイルシステムストレージ、およびクオータの管理に伴うコストと複雑さを軽減できます。IAPでは、システム全体が標準のサーバーハードウェアで構成され、無駄なサーバーがなく、データの価値を基準にして電子メールを低価格のストレージに自動的に移動できます。
- 新しいプライマリストレージシステムを今すぐ手に入れる必要がなくなり投資を延期できます。

特長

IAPは、ファイル、電子メールメッセージなど各種データを自動で自発的にアーカイブします。また、インタラクティブなデータクエリにより、アーカイブされたデータをさまざまな基準に基づいて迅速かつ簡単に検索して読み込むことができます。認証されたユーザーには、IAPのWebユーザーインターフェイス経由でアーカイブされた情報にアクセスする権限が与えられます。

IAPでは、HPサーバーとグリッドストレージの技術、ネイティブで提供されるコンテンツのインデックス作成機能、検索、およびポリシー管理ソフトウェアが、工場で組み立て済みの1台のラックシステムに統合されるため、インストールと保守が簡単です。

以下では、IAPのハイレベルの機能を1つずつ説明します。

- グリッドコンピューティングアーキテクチャー。HP IAPはグリッドコンピューティングアーキテクチャーに基づいており、ユーザーは性能と容量を簡単に拡張できます。検索は、すべてのスマートセルを対象に並列で実行されます。
- 分散型のコンテンツインデックス作成機能と検索ツールの統合。IAPの分散型インデックス作成機能とグリッドアーキテクチャー技術を利用する包括的な統合検索機能により、多数の大容量オブジェクトを対象にして、統合され一元化されたマルチコンテンツ情報サイロ(電子メール、ファイルなど)に、多数のユーザーがすばやくアクセスできます。

- ストレージ削減アルゴリズム。IAPは、データ圧縮、オブジェクトレベルのシングルインスタンス化などの、ストレージ削減アルゴリズムを使用します。このアルゴリズムにより、IAPでは、重複している電子メールや文書を識別して、アーカイブされた電子メールの中から重複したものを削除して効率的に利用ができます。
- Exchange OutlookおよびLotus Notesと統合された検索ツール。ユーザーは、使い慣れた電子メールアプリケーションから直接、そのアーカイブメッセージを検索できます。このため、独立したユーティリティの習得はもちろん、起動さえも必要ありません。
- ビジネスポリシーベースの自動アーカイブアプリケーションのサポート。柔軟に設定できるポリシーに基づいて電子メールや文書を選択的にアーカイブします。
- Microsoft Exchangeサーバーなど、マネージドアプリケーションの管理に関わるオーバーヘッドの削減。IAPシステムの状態と管理の監視のために、HP IAP Platform Control Center（PCC）ソフトウェアを内蔵します。
- 改ざんを許さない環境。データの消去や改ざんを防止するために、デジタル署名、タイムスタンプ、およびデータ保管ポリシーが使用されます。データは、保管期間が過ぎるまで、アーカイブから削除できません。
- データ複製とミラーリング。データは、スマートセルのグループ全体で同時にミラーリングされるため、データの可用性が強化されます。
- 電子メールや、ファイルなど、非構造化データ、半構造データ、および構造化データをサポートします。
- 法規制に関わるリスクを軽減し、企業のガバナンス確立のためのイニシアチブをサポートします。HP IAPに保存されるデータは、SECなどによる法規制に従うものであり、保管ポリシーに基づいて管理され改ざんできないようになっています。適切な認証情報がなければデータを検索できません。また、必要に応じて、訴訟ホールドを適用できます。
- 柔軟な保管管理。柔軟な保管ポリシーに基づく情報の保護により、コンプライアンス、法的情報保管場所、ガバナンスなど満たすべき要件がどんなものであっても、保管期間が終わった時点でデータを正しく処分できます。

ソフトウェアコンポーネント

IAPと連携するソフトウェアコンポーネントには、大きく分けて2つのタイプ（ユーザーアプリケーションと管理者アプリケーション）があります。

ユーザーアプリケーション

次のアプリケーションは、すべてのIAPユーザーが利用できます。

表2 ユーザー向けのIAPアプリケーション

アプリケーション	タスク
IAP Webインターフェイス	Webブラウザーを、次の目的で使用します。 ・ システムにアーカイブされている文書の検索および検索条件と結果の保存および再利用。 ・ アーカイブされている電子メールの電子メールクライアントへの復元（Send to me）。 ・ ローカルコンピューターまたはネットワークフォルダーへのファイルのダウンロード。 ・ ユーザーのシステムに適切なエクスポートツールがインストールされている場合は、電子メールおよびファイルのエクスポート。 ・ 電子メールに法的情報保管場所を設定して、無期限に保管する。 ・ （コンプライアンス担当者）コンプライアンスシステムログに当たる、AuditLogの検証。

システムと対話するには、Outlookプラグイン、Notes Clientプラグイン、Local Cache、Export Search、IAP File Exportといった、オプションのEAsおよびFAsアプリケーションをユーザーが利用できなければなりません。これらのソフトウェアは、ユーザーのコンピューターにインストールします。Outlookプラグインは、Citrix Presentation Managerを実行するサーバーにもインストールできます。

表3 ユーザー向けのEAsおよびFAsアプリケーション

アプリケーション	タスク
Outlookプラグイン（カスタマーオプション）	Microsoft Exchangeメールサーバーでoutlookを使用して、アーカイブされた電子メールを検索、表示、利用する。電子メールをIAPからPSTファイルにエクスポートする。
OWA Extension（カスタマーオプション）	Microsoft Exchangeメールサーバーでoutlook Web Accessを使用して、アーカイブされた電子メールを表示および利用する。
Notes Clientプラグイン Local Cache Export Search （カスタマーオプション） （Windowsユーザーのみ）	IBM Dominoメールサーバーでlotus Notesを使用して、アーカイブされた電子メールを表示および利用する。 旅行中にアーカイブされた電子メールにオフラインでアクセスする。 IAPからNotes NSFファイルに電子メールをエクスポートする。
DWA Extension（カスタマーオプション）	IBM DominoメールサーバーでiNotes（Domino Web Access）を使用してアーカイブされた電子メールを表示および利用する。
IAP File Export（カスタマーオプション）	FAsを使用して移行されたファイルをローカルコンピューターまたはネットワークフォルダーにエクスポートする。

管理者用のツール

IAPには、次のようなトラブルシューティングと管理用の機能があります。

表4 管理者用のIAPツール

機能	タスク
Platform Control Center（PCC）	Webベースの管理者用インターフェイスを使用して、システムのステータスとパフォーマンスの監視およびトラブルシューティング、システムオプションの設定、ユーザーアカウントの管理を行う。（「Platform Control Center（PCC）の概要」（33ページ）を参照）。
コマンドラインインターフェイス	HP認定のサポート担当者がコマンドラインからシステムオプションを設定して有効にできるようにする。
AuditLog	規格準拠のためにAuditLogを使用できるようにする。（「AuditLogの有効化」（133ページ）を参照）。
外部アクセス	Archive GatewayへのVNCアクセスを使用してEAs for Exchangeのオプションを表示および設定する（「外部アクセス」（127ページ）を参照）。
リモートサーバーの管理	HP ProLiant Onboard Administrator Powered by Lights-Out 100またはIntegrated Lights-Out 2を使用してIAPサーバーのリモート管理を監督する。第13章（149ページ）を参照してください。

次の、EAs、FAs、およびバックアップアプリケーションをIAPと組み合わせて使用できます。

表5 管理者アプリケーション

アプリケーション	タスク
HP Email Archiving software for Exchange	Microsoft Exchangeを対象に、ジャーナルに保存されたメールのアーカイブ、アーカイブルールの設定、複数のOutlook PSTファイルのバッチ処理。EAs for Exchange製品付属のドキュメンテーションCDに収録されている『HP Email Archiving software for Microsoft Exchange管理者ガイド』を参照してください。
HP Email Archiving software for Domino	IBM Lotus Dominoを対象に、ジャーナルに保存されたメールのアーカイブ、アーカイブルールの設定、およびメールデータベースのバッチ処理。EAs for Domino製品付属のドキュメンテーションCDに収録されている『HP Email Archiving software for IBM Lotus Domino管理者ガイド』を参照してください。
HP File Archiving software	Windowsシステムからのファイルサーバー、Webサーバー、アプリケーションサーバーデータのアーカイブ。
HP Data Protector	スケーラブルなデータ保護機能を含み高性能バックアップとリカバリを自動化。

ハードウェアコンポーネント

IAPの基本システム

IAPの基本システムは、次のコンポーネントで構成されます。

- 42Uラック
- 管理サーバー(9)
- ユニバーサルスマートセル(1)
- KVM/Mon(1)
- 5406スイッチ(1)
- 2510G-48スイッチ、iLO用(1)
- 基本ラックで上記のコンポーネントが占める高さの合計(U単位): 19U
- アップグレードに使用できる高さ(U単位): 23U

管理サーバーは、次で構成されます。

- ゲートウェイ(オプション)
- ファイアウォール
- ロードバランサー
- クエリポータル(HTTP)
- ストアポータル(SMTP)
- メタサーバー
- クラウドルーター
- データベース(DB2)
- PCC(Platform Control Center)
- kickstartサーバー

基本システムには、ユニバーサルスマートセルを除くすべてのサーバーソフトウェアのインストール先になるDL360 G6サーバーが付属しています。ユニバーサルスマートセルはDL180 G6サーバーにインストール

します。システムには、5TBのストレージを提供する1組のスマートセルも含まれます。2組のスマートセルを追加注文して、基本システムを完全搭載することもできます。これにより、ストレージ容量が5TBから15TBに増えます。

拡張ラック

42Uラック

ユニバーサルスマートセル（10）

合計： 40U

1台の拡張ラックの総容量： 50TB

1つのHP IAPシステムで最大21台の拡張ラックを使用できます。

このため、現時点でのIAPの最大容量は10650TB（213グループ × 5TB）です。

オプションで、拡張ラックに、性能アップグレードのための装置（例：SMTPポータル、HTTPポータルを追加など）を収納することもできます。

拡張ラックは、増設用の10組のスマートセルを収納できるため、50TBのストレージ容量を提供できます。

その他のオプション

基本システムは、最大3組のスマートセルグループを収納できます。スマートセルを増設または追加する場合は、拡張ラックを入手する必要があります。拡張ラックは、最大10組のスマートセルを収納できます。また、増設用のクエリポータルやストアポータルなど、性能アップグレードのための装置も収納できます。このように、拡張ラックには目的に合わせてさまざまな装置を組み合わせて収納できます。

上記以外の工場統合オプション

次のオプション製品は工場で統合できます。

- 5TBスマートセルストレージ容量アップグレード
- クエリ（HTTP）ポータルパフォーマンスアップグレード
- ストア（SMTP）ポータルパフォーマンスアップグレード
- 複製パフォーマンスアップグレード
- IAPバックアップオプション（専用テープバックアップソリューション）

容量拡張パフォーマンスアップグレードオプション

容量拡張パフォーマンスアップグレードオプションを使用してIAPの規模を大きく（容量を拡張）すると、性能を向上させることができます。

複製オプション

上記のオプションの他に、IAP複製オプションが用意されており、1つのシステム全体を複製できます。複製オプションは、基本システムのローカルまたはリモートでの複製をサポートするソフトウェアライセンスです。

ネットワークアーキテクチャー

次の図に、ネットワークアーキテクチャーの概観を示します。この図は、IAPの基本ネットワーク構成図に当たります。IAPネットワークのバックボーンになるのが、VLAN 500です。ユーザーは、ファイアウォー

ル/NAT経由で接続し、管理機能はPCC経由で接続します。PCCでは、IAPとその稼動状態、サーバーの状態、IAPが保存中かどうかを監視できます。

IAP 2.1のハードウェア構成図

オプションのHPゲートウェイサーバーを除く、すべてのシステムがLinuxベースです。HPゲートウェイサーバーは、Windows Serverソフトウェアを実行します。

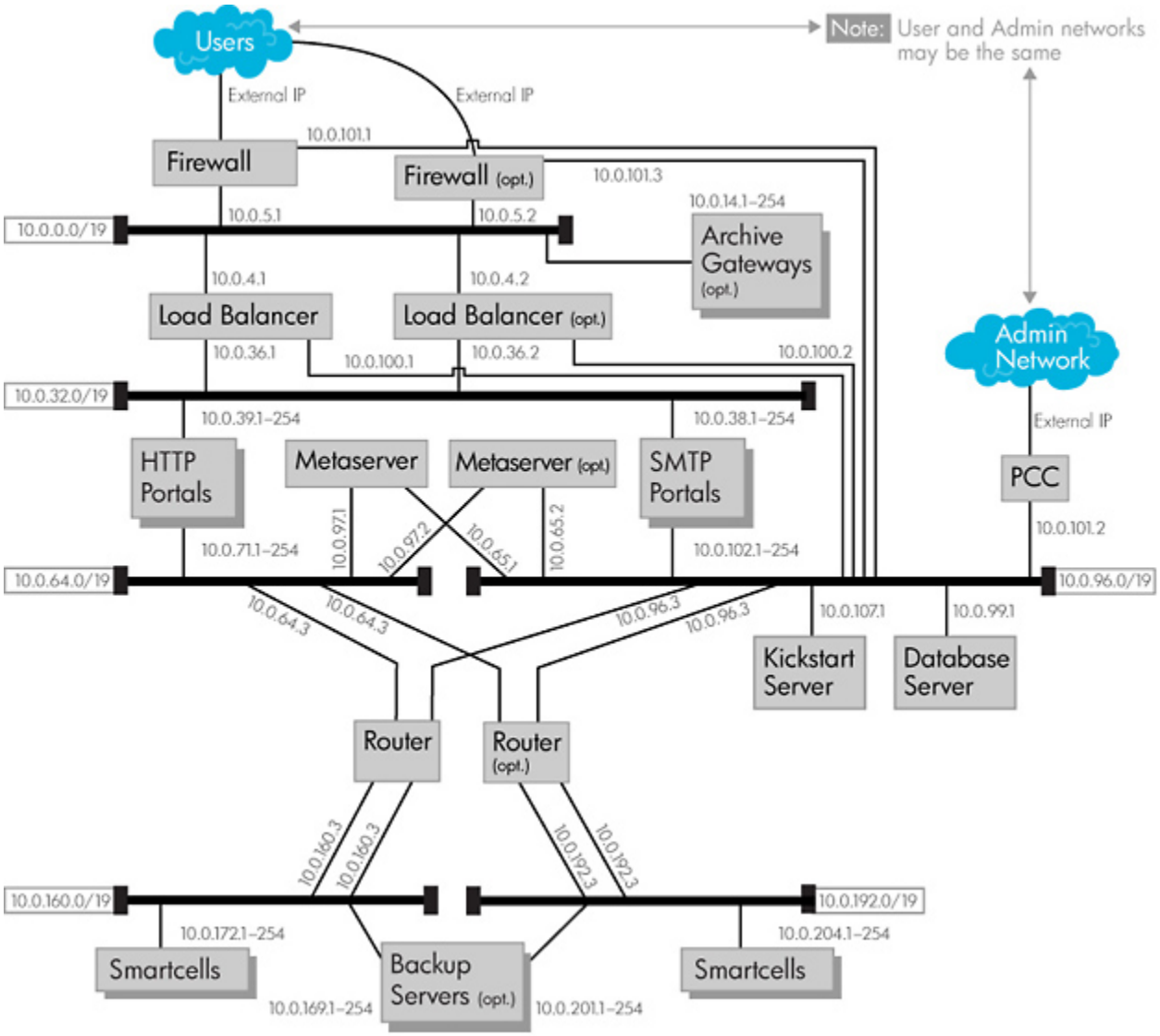


図1 アーキテクチャーの図

仮想LAN（VLAN）

IAPは、仮想LAN（VLAN）、すなわち仮想ローカルエリアネットワークを使用します。管理サーバーは、VLANを使用して相互接続されます。次に、VLANを介してさまざまなコンポーネントがどのように接続されるかを説明します。

- VLAN 200：ファイアウォール/NATとロードバランサーおよびゲートウェイサーバーを接続します。
- VLAN 300：ロードバランサーとHTTPポータルおよびSMTPポータルを接続します。
- VLAN 400：HTTPポータルはVLAN 400に接続されVLAN 300経由で通信できます。

- VLAN 500: IAPネットワークのバックボーン。PCCサーバー、データベースサーバー、kickstartサーバー、クラウドルーター、およびメタサーバーと接続されます。
- VLAN 600: クラウドルーター1およびバックアップサーバーと接続されます。
- VLAN 700: クラウドルーター2およびバックアップサーバーと接続されます。

グリッドアーキテクチャー

ユニバーサルスマートセルを使用したIAPのグリッドストレージは、内蔵型でデータレポジトリも全て組み込んだ分散コンピュータシステムです。このアーキテクチャーにより、大量のコンテンツと多数のオブジェクトをスマートセルのグリッド全体にインテリジェントに分散できます。また、このアーキテクチャーが並列検索を可能にするため、IAPは数テラバイトに及ぶ参照情報全体を3〜5秒で高速検索できます。

IAPのグリッドコンピューティングアーキテクチャーは、企業全体に分散する情報サイロを統合および一元化することで、情報の急激な増加に対するお客様の取り組みを支えます。このアーキテクチャーは、HP IAPへのユーザートラフィックや文書トラフィックの増加に対応する、最高レベルのパフォーマンスを保証します。

IAPに組み込まれるグリッドアーキテクチャーは、ドメインとレポジトリで構成されます。ドメインとは、グリッドアーキテクチャー内部に配置されるスマートセルのサブグループのことです。たとえば、4つのスマートセルペアでドメイン1を構成し、3つのスマートセルペアでドメイン2を構成する(両方のドメインが同じIAPグリッドに所属します)ことができます。各ドメインには、独自のポリシーを割り当てて大規模組織の別々の部署の意味をもたせることもできます。レポジトリは、1つまたは複数のスマートセルグループにまたがる論理要素です。1つのドメイン内に、複数のレポジトリを設定することができます。レポジトリは、1人のユーザーのメールボックスを意味することも、ユーザーグループのメールボックスを意味することもあります。特定のドメインやレポジトリにアクセスできるユーザーの決定には、アクセス制御が用いられます。

管理サーバー

基本IAPシステムは、9つの管理サーバーで構成されます。これらの管理サーバーは、DL360 G6サーバーを使用して構成されます。次の項では、各管理サーバーの主な機能について簡単に説明します。

ファイアウォール/NAT

ファイアウォール/NAT(Network Address Translation)は、IAPへのアクセスを制限します。このサーバーは、ユーザーにつながっています。情報が保存されるとき、その情報はファイアウォール/NATを通過します。ファイアウォール/NATは内部ネットワークと外部ネットワークの間でのネットワークアドレスの変換を担当します。ファイアウォール/NATの静的IPアドレスは、10.0.101.1です。2台目のファイアウォールを設置することもできます。

ロードバランサー

ロードバランサーは、受信トラフィックを均等化してSMTPポータルおよびHTTPポータルに振り分けます。ロードバランサーのIPアドレスは10.0.100.1です。2台目のロードバランサーを設置することもできます。

HTTPポータル

HTTPポータルは、文書のクエリと取得に使用します。クエリは、まず、ファイアウォールを通過して、ロードバランサーにたどり着きます。ロードバランサーは、利用できるHTTPポータルを選択します。HTTPポータルは、メタサーバーに問い合わせて、該当する文書を保存しているスマートセルグループを特定します。

HTTPポータルのIPアドレスは10.0.71.1です。HTTPポータルを追加すると、そのポータルには、既存のポータルのIPアドレスの最後の桁に1を加えたアドレスが割り当てられます。たとえば、追加されるポータルのアドレスは、 10.0.71.2、10.0.71.3、のように1つずつ増えていきます。

SMTPポータル

SMTPポータルは、メッセージの保存に使用されます。SMTPポータルは、メッセージにアクセスできるレポジトリを識別します。SMTPポータルのIPアドレスは10.0.102.1です。SMTPポータルを追加すると、そのポータルには、既存のポータルのIPアドレスの最後の桁に1を加えたアドレスが割り当てられます。たとえば、追加されるポータルのアドレスは、 10.0.102.2、10.0.102.3、のように1つずつ増えていきます。

メタサーバー

メタサーバーは、スマートセルの割り当て、システムの状態、Bias Dimensional Indexing（BDI）マッピングを管理します。メタサーバーは、データ保存のために新しくスマートセルを割り当てる必要があるかどうかを判断します。このサーバーは、中断中、停止中など、スマートセルの状態を常時監視します。

メタサーバーは、IAPドメインとスマートセルおよびユーザーとの対応関係も追跡します。たとえば、あるスマートセルグループがドメイン1、別のスマートセルグループがドメイン2に所属しているとします。メタサーバーは、DB2サーバーやHTTPポータル、SMTPポータルと情報を交換して、それぞれの保存要求やクエリ要求に適したスマートセルを決定します。

メタサーバーのIPアドレスは10.0.97.1です。2台目のメタサーバーを設置することもできます。メタサーバーが複数ある場合、プライマリまたはマスターメタサーバーを決めます。追加した（2台目の）メタサーバーには、IPアドレス10.0.97.2が割り当てられます。

クラウドルーター

クラウドルーターは、スマートセルへの内部のネットワークトラフィックおよびスマートセル間の内部ネットワークトラフィックの経路を決定します。データが保存または取得されるには、クラウドルーターを通過する必要があり、データはVLAN 600またはVLAN 700経由でスマートセルに到達します。クラウドルーターの静的IPアドレスは10.0.96.3です。2台目のクラウドルーターを設置することもできます。

データベースサーバー（DB2）

データベースサーバーは、ユーザー名、パスワードなどのアクセス制御情報を保存します。また、レポジトリに入ってくるメッセージのルーティング規則も保存して、そのレポジトリとメッセージに対するアクセス権の所有を明らかにします。データベースサーバーは、クエリの結果も保存します。これらのクエリ結果は、後で抽出できます。また、データベースサーバーは、スマートセルの状態に関する情報も保存します。スマートセルの状態に関する情報は、スマートセル自体にも保存され、こちらの情報のほうがDB2データベースの状態情報よりも優先されます。データベースサーバーは、複製オプションを使用する構成では、プライマリIAPと複製IAP間の複製フローの制御も行います。DB2サーバーのIPアドレスは、10.0.99.1です。

kickstartサーバー

kickstartサーバーは、すべてのIAP管理サーバーのハブとしての役割を担います。kickstartサーバーは、各管理サーバーで必要なオペレーティングシステム、ソフトウェアアプリケーション、および設定ファイルを保存します。管理サーバーの1つがPXEブートするとき、そのサーバーはkickstartサーバーにアクセスして情報を取得します。各管理サーバーには、固有のMACアドレスがあります。kickstartサーバーは、そのMACアドレスを手がかりに、管理サーバー、そのサーバーのオペレーティングシステム（OS）、サーバー上で実行されているアプリケーション、およびそのサーバーで必要な設定ファイルを認識します。kickstartサーバーのIPアドレスは10.0.107.1です。

Platform Control Center（PCC）

PCCは、Webベースのインターフェイスを提供します。管理者は、このインターフェイス経由でIAPを監視およびトラブルシューティングし、ユーザーアカウントを管理できます。PCCは、コマンドラインインターフェイスも提供します。次に、PCC経由で行う一般的な管理作業を示します。

- 全体的なシステムの状態と性能の確認
- スマートセルの状態と性能の確認
- システムステータスとRAIDサポートの監視
- システムサーバーの起動、停止、および再起動
- ユーザーアカウントの同期化
- ユーザーアカウントの管理
- システムアラートの監視

PCCのIPアドレスは、10.0.101.2です。

Archive Gateway（オプション）

Archive Gatewayサーバーは、お客様の要件に基づいて組み込まれるオプション装置です。Archive Gatewayは、電子メールのアーカイブに必要なソフトウェアコンポーネントを搭載します。このサーバーは、IAPへのコネクターに当たり、電子メールメッセージを実務メールサーバー（DominoまたはExchange）から抽出します。Archive Gatewayは、Selective Archivingが導入されている場合、クライアントメールボックスにメッセージスタブ（トゥームストーン）を作成します。

Archive Gatewayには、Exchange用とDomino用の2つのタイプがあります。Exchange用のArchive Gatewayは、HP Email Archiving software for Exchange（HP EAs for Exchange）を内蔵します。Exchange用のArchive GatewayのIPアドレスは10.0.14.xです。

Domino用のArchive GatewayはHP Email Archiving software for Dominoを内蔵します。このArchive GatewayはIAPファイアウォールの外側に配置されるため、Exchange環境で使われるものと同じIPアドレスは割り当てられません。

バックアップサーバー（オプション）

バックアップオプションを追加することもできます。バックアップオプションとは、HP Data Protectorソフトウェアを搭載するバックアップサーバーのことです。バックアップサーバーは、IAPのスマートセルおよびDB2データならびにIAPの設定情報をテープにバックアップします。バックアップサーバーは1台だけ設置することも複数台設置することもできます。

バックアップサーバーのIPアドレスは10.0.169.xおよび10.0.201.xです（各スマートセルネットワークで1つのインターフェイス）。

ユニバーサルスマートセル

ユニバーサルスマートセルは、IAPストレージの基本要素です。ユニバーサルスマートセルは、DL180 G6サーバー上で構成します。2つのスマートセルで1つのスマートセルグループを構成します。スマートセルは、必ず、プライマリスマートセルとセカンダリスマートセルのペアで構成します。スマートセルは、「インテリジェントなストレージ」サーバーで、取得、インデックス作成、圧縮、保存、検索、抽出といったデータ操作を自身で処理します。ユニバーサルスマートセルグループは、最大5TBのストレージ容量を備え、ADG保護を含むRAID6で構成されます。

プライマリスマートセルにはIPアドレス10.0.172.1または10.0.204.1を割り当てでき、VLAN 600経由でアクセスできます。セカンダリスマートセルにはIPアドレス10.0.172.1または10.0.204.1（ただし、プライマリスマートセルとは異なるアドレス）を割り当てでき、VLAN 700経由でアクセスできます。スマートセルの追加が必要

な場合、追加するプライマリスマートセルのIPアドレスは10.0.172.2、10.0.172.3、というように追加のたびに増やしていきます。追加するセカンダリスマートセルのIPアドレスも、10.0.204.2、10.0.204.3、というように追加のたびに増やしていきます。

データフロー

この項では、IAPとの間で行き来するデータの一般的な流れについて説明します。

ストアパス

ストアパスは、データがIAPに流入する部分に当たるデータフローの一部です。つまり、ストアパスは、アーカイブされている電子メールやファイルに注目した用語です。ストアパスで扱われるデータの実際の単位はbitfileです。以下ではデータフローについて詳しく説明しますが、その前に、bitfileについて理解しておく必要があります。

bitfile

bitfileは、IAPが使用する文書の基本保存単位です。bitfileは、次の4つの部分で構成されるZIPファイルです。

- マニフェスト
- データ
- メタデータ
- Sig

マニフェスト

マニフェストは、プレーンテキストで記述される日付です。マニフェストには、コンマで区切られた3つの情報が含まれます。最初の情報はプレーンテキストの日付（例：Tue Jul 10 17:45:18 JST 2007）、次の情報はバージョン番号（例：1）、最後の情報はキータイプの番号（例：1）です。たとえば、次のようなマニフェストがあります。

（Tue Jul 10 17:45:18 JST 2007,1,1）

データ

これは、元のデータです。電子メールの場合、メッセージはRFC822フォーマットでアーカイブされます。

メタデータ

IAPは、各bitfileにメタデータを追加します。メタデータは、bitfileのデータを説明します。メタデータは、日付、レポジトリ、インデックス作成が可能な文書構成、および電子メールのエンベロープ情報で構成されます。メタデータは、元をたどれば、bitfileに流し込まれるデータのスキャンを担当する、SMTPポータルが追加するデータです。メタデータは、基本的には、インデックス作成やアクセス制御に使用されます。

Sig

Sigは、デジタルコンテンツが改ざんされていないこと保証するために使用されるデジタル署名です。Sigの計算方法に基づき、データコンテンツのデジタル署名も確実に「タイムロック」されます。

SMTPポータルのデータ処理方法

ここまでで、bitfileについて一定の知識を得ることができましたので、ストアパスについて詳しく説明できます。

ストアパスでは、オブジェクトがネットワーク経由でシステムにデータ転送します。メールメッセージはExchangeまたはDominoメールサーバーからゲートウェイ経由で転送され、フロントファイアウォール/NATを通過してロードバランサーにより負荷分散されます。複数のSMTPポータルがある場合は、どのSMTPポータルを利用できるかをシステムが判断します。

SMTPポータルは、次の操作を行うことでオブジェクトを処理します。

- オブジェクトのデジタル署名と受信日時を作成する。
- 電子メールについては、アドレス解決を行う。
- データのレポジトリを見つける。つまり、SMTPポータルが「これは誰の文書ですか」と尋ねると考えてください。文書の持ち主がわかると、SMTPポータルは、その文書に対応するレポジトリを見つけます。たとえば、データがJan宛の電子メールメッセージの場合、メッセージはJan用にアーカイブされます。SMTPポータルは、Janがアクセス権を持つレポジトリを見つけます。
- クラウドルーターを介してデータをプライマリおよびセカンダリスマートセルに転送します。

スマートセルのデータ処理方法

スマートセルは、ストアパスのこのポイントで、データを受け取り、そのデータを次の操作を行って処理します。

- プライマリとセカンダリの両方のスマートセルにデータが正しく保存されたことを確認する。
- bitfileのインデックス作成（データを構文解析してキーワードを抽出し、検索が行われるときに関連データが見つかるようにします）のスケジューリング。
- 送信側のアプリケーションに、データが正常に保存されたことを示す応答を送り、次の項目に移る。

ここで説明するストアパスでの処理は、アーカイブのすべてのタイプで共通です。

クエリ/取得パス

クエリ/取得パスは、検索され取得されている電子メールやファイルに注目した用語です。このパスにより、IAPからユーザーへのデータフローが発生します。

クエリ

クエリは、システムのHTTPポータルを使用して行われ、IAPのWebインターフェイス（Webブラウザー経由）から実行されるかOutlook Integrated Archive Searchを介して実行されます。

クエリは、ファイアウォール経由で提出されます。HTTPポータルが複数ある場合は、ロードバランサーが使用できるHTTPポータルを判断します。

HTTPポータルは、クエリをフォーマットし、メタサーバーからの情報を使用してデータを返すスマートセルを判断します。

スマートセルは、マルチキャスト要求を並列で受け取りますが、ローカルクエリを実行するのは該当するデータを含むスマートセルです。

取得

マルチキャストが行われると、スマートセルは検索条件と一致する項目を検索します。各スマートセルは、その検索結果をデジタル署名を付けて戻します。

メタサーバーは結果を受け取ると、その結果を時間順に並べ、HTTPポータルに戻します。

HTTPポータルは、デジタル署名を計算し保存しているデジタル署名と照合します。これにより、クエリ側のアプリケーションにデータを戻す前に、改ざんがいっさい行われていないことが確認されます。

デジタル署名の確認後、システムはファイアウォール経由でユーザーのブラウザー画面またはOutlookクライアントにデータを戻して、結果が表示されるようにします。たとえば、過去3か月の間にアーカイブしたメッセージの「技術情報」の検索を行うと、システムはその検索クエリにあるキーワードを含む電子メールメッセージを返します。

IAPの電源投入と切断

ここでは、IAPの電源の投入/切断手順と電源障害時に行う手順について説明します。

電源の切断

IAPの電源を切るには、PCCから次のように入力します。

```
# /opt/bin/stop
# /opt/bin/shutdown
```

シャットダウンスクリプトが完了するまで待ってから、IAPシステムの電源を抜き取ります。

電源の投入

IAPの電源を入れるには、以下の手順に従います。

1. IAP内部のProCurveスイッチの電源が入っていることを確認します。電源が戻ると、ProCurveスイッチは自動的に起動するはずです。
2. kickstartサーバーの電源を入れます。5分待ちます。
3. 他の機器すべての電源を入れます。通常、順序は自由です。停電が発生した場合については下記を参照してください。
4. すべてのマシンが起動するのを待ち、PCCコンソールにログインし、コマンドを実行します。`/opt/bin/restart`

停電後のIAPの再起動

停電が発生した後では、特定の電源投入順序に従う必要があります。

1. すべてのシステムの電源を切ります。
2. kickstartサーバーの電源を入れます。
3. kickstartサーバーが起動したら、ログオンしてコマンドを実行します。

   ```
   /etc/init.d/postgresql stop
   /etc/init.d/postgresql start
   ```

4. 起動が正常に完了するのを待ちます。
5. DB2、ルーター、ファイアウォール、およびロードバランサーの電源を入れます。
6. スマートセルの電源を入れます。
7. メタサーバーの電源を入れます。
8. 残りのサーバーの電源を入れます。
9. すべてのマシンが起動するのを待ち、PCCコンソールにログインし、コマンドを実行します。`/opt/bin/restart`

10. IAPが再起動したら、(PCCのWebインターフェイスを使用して)IAPが正常に動作し、監視機能がシステムの可用性を報告することを確認します。

注記:

両方のルーターが停止している場合は、ルーターが起動してから、`/opt/bin/restart`でシステムを再起動する必要があります。

最大ファイルサイズ

IAP APIで有効なすべてのファイルタイプに対する最大ファイルサイズは、1.47GBです。

VPNアクセス

HPの認定サポート担当者がVPNアクセスオプションについてご提案させていただくことがあります。担当者は、お客様に最大限のメリットをもたらすこのオプションの選択と導入をお手伝いできます。

2 Platform Control Center（PCC）の概要

この章では、IAPとユーザーアカウントを監視し、トラブルシューティングを行うためのPlatform Control Center（PCC）管理ソフトウェアについて説明します。

次の項目があります。

注記：

PCCの各ページの機能を使用するには、事前に、ブラウザーの進行状況バーまたはアイコンを確認して、ページを完全に読み込む必要があります。

PCCへのアクセス

PCCにアクセスするには、Webブラウザーを開き、PCCサーバーのIPアドレスを入力し、管理権限を持つユーザー名とパスワードを使用してログインします。

管理者権限は、アカウントマネージャーで設定します。詳細は、「ユーザーアカウント情報」（74ページ）を参照してください。

HPテクニカルサポートから指示があった場合は、スーパーユーザーとしてログインすることもできます。IAPスーパーユーザーのログイン名とパスワードは、システムのインストール時に設定します。

注記：

Mozilla Firefoxを使用してPCCを開く場合、例外要求が表示されたら、受け入れてください。

ユーザーインターフェイスのコンポーネント

PCCは、HTMLに基づくアプリケーションであり、ページの左側にメニューがあります（これを「左メニュー」と呼びます）。左メニューを使用すると、PCCのほとんどのページにアクセスできます。

図2 PCCのユーザーインターフェイス

ユーザーインターフェイスの使用方法

ユーザーインターフェイスを使用するときは、さまざまなPCCページの特長に注意してください。

- リンク テキスト: ページに移動するためのナビゲーションリンクは、ページの一般的な説明です。ページに移動するためのほとんどのリンクは、左メニューにあります。
- HTML名: 各PCCページには、ブラウザーに表示されるわかりやすいHTML名があります。

注記:

ページの機能は、PCCページが完全に読み込まれるまで待ってから使用してください。

共通作業用のページ

表6 共通のシステム管理作業用のページ

作業	ページ
全体的なシステムの状態と性能の確認	「Overview(概要)」(41ページ)
システムサーバーの起動、停止、および再起動	「Software Management(ソフトウェア管理)」(47ページ)
システムハードウェアの状態の監視またはサーバーのリモート管理	「Hardware Management(ハードウェア管理)」(49ページ)
プラットフォーム設定の確認	「Platform Settings(プラットフォームの設定)」(57ページ)

作業	ページ
システムでファイアウォールが有効になっているポートの表示	「Firewall Settings（ファイアウォールの設定）」（58ページ）
インストールされているIAPソフトウェアのバージョンコードの表示	「Software Version（ソフトウェアバージョン）」（62ページ）
ユーザーアカウントの同期化	「Account Synchronization（アカウントの同期化）」（63ページ）
ユーザーアカウントの管理	「Account Manager（AM、アカウントの管理）」（71ページ）
ドメイン複製の監視、開始、および停止	「Replication（複製）」（90ページ）
スマートセルのクローン作成（データのコピー）	「Smartcell Cloning（スマートセルのクローン作成）」（113ページ）
データベースのバックアップ履歴の確認	「Backup（バックアップ）」（105ページ）
システムイベントの監視	「Event Viewer（イベントビューアー）」（119ページ）
SNMPトラップのアクティブ化と電子メール通知の送信	「SNMP Management（SNMPの管理）」（121ページ）
システムステータスと性能の周期的な電子メールレポートの設定	「Email Reporter（電子メールレポーター）」（123ページ）
Archive Gatewayへのリンク	「Archive Gateway Management（Archive Gatewayの管理）」（127ページ）

印刷する前のページの更新

Webインターフェイスに表示されるPCCページは、自動的には更新されません。手動でページを更新するには、ブラウザーで[Refresh]（または[最新の情報に更新]）をクリックします。

ブラウザーがWebページをキャッシュする場合、ブラウザーの[戻る]ボタンをクリックすると表示されるキャッシュに保存されたページは、最新ではない場合があります。手動で更新してください。

一部のブラウザーは、ブラウザーの表示を更新せずに、更新されたWebページから印刷します。表示されるページが最新でない場合、印刷されるページが表示されるページと異なる場合があります。印刷と表示が一致するようにするには、印刷する前に手動でブラウザーを更新します。

左メニュー

左メニューを使用すると、迅速にPCCビューにアクセスできます。左メニューは、システムの設定方法によって異なります。たとえば、複製を使用しないシステムでは、[Replication]メニュー項目が使用できません。また、HPのサポート担当者は[Service Tools]メニュー項目を使用しますが、この項目を必要に応じてユーザーが使用できるようにすることがあります。

表7 左メニューからアクセスできるページ

左メニュー項目	説明
「Overview（概要）」（41ページ）	システム状態、ストレージステータス、ドメイン別のスマートセル性能、およびシステムアラートの表示
「Storage Status（ストレージステータス）」（46ページ）	文書の保存率および使用済み/空きディスク容量のドメイン別の概要の表示
「Software Management（ソフトウェア管理）」（47ページ）	サーバーソフトウェアの状態の表示、システムで1つ以上のサーバーを起動、停止、または再起動
「Hardware Management（ハードウェア管理）」（49ページ）	サーバーのハードウェアの状態の監視とサーバーのリモート管理
「Performance Graph（パフォーマンスグラフ）」（53ページ）	システムの保存率とインデックス作成率およびシステムパフォーマンスのグラフ化
[General Configuration（一般設定）]の各ページ	
「Platform Settings（プラットフォームの設定）」（57ページ）	IAPに関するハードウェアおよび設定情報の表示
「Firewall Settings（ファイアウォールの設定）」（58ページ）	システムでファイアウォールが有効になっている各ポートの表示
「SSL Configuration（SSLの設定）」（58ページ）	PCCおよびHTTPポータル用の第三者公開証明書要求の生成
「Software Version（ソフトウェアバージョン）」（62ページ）	システムで使用しているIAPソフトウェアのバージョンコードの表示
「Software Update（ソフトウェアアップデート）」（62ページ）	IAPソフトウェアへのパッチの適用
[User Management（ユーザー管理）]の各ページ	
「Account Synchronization（アカウントの同期化）」（63ページ）	LDAPサーバーから取得した情報でIAPユーザーを自動的に作成し、更新するように、動的アカウント同期化（DAS）を設定
「Account Manager（AM、アカウントの管理）」（71ページ）	IAPユーザーアカウントを提供、更新、および管理
「Account Error Recovery（アカウントエラー修復）」（85ページ）	アカウント同期化エラーの修復
[Archive Gateway Management（アーカイブゲートウェイ管理）]の各ページ	
「[Overview Archive Gateway]」（128ページ）	各ドメインについてArchive Gatewayに関するステータス情報の表示
「VNC Archive Gateway」（127ページ）	VNCを使用して、Archive Gatewayにアクセス
[Data Management（データ管理）]の各ページ	
「Duplicate Manager」（87ページ）	重複したマージジョブのステータスの表示と、重複したマージジョブのスケジュール設定
「Reprocessing（再処理）」（95ページ）	新しいルーティング規則に基づいて、再処理をスケジュールし、有効にする

左メニュー項目	説明
「Retention（保管）」（97ページ）	ドメインとレポジトリの保管期間の設定
「Backup（バックアップ）」（105ページ）	データベース、設定、およびスマートセルバックアップに関するステータス情報の表示。HP Data Protectorのユーザーインターフェイスにアクセスして、バックアップシステムの詳細情報と設定を取得します。
「Replication（複製）」（90ページ）	IAPドメインの複製を監視、開始、または停止
「Restoring a Smartcell group(スマートセルグループのリストア)」（110ページ）	スマートセルグループのテープからのリストア
「Smartcell Cloning（スマートセルのクローン作成）」（113ページ）	スマートセルのクローンを作成し（データをコピーし）、新しい実行可能なミラーセルを提供
[Reporting（レポーティング）]の各ページ	
「Event Viewer（イベントビューアー）」（119ページ）	システムサービスまたはアプリケーションあるいはシステムハードウェアで発生したイベントの表示
「SNMP Management（SNMPの管理）」（121ページ）	システム監視用のSNMPトラップを設定し、電子メール通知を送信します。
「Email Reporter（電子メールレポーター）」（123ページ）	電子メールの受信者へ送信されるシステム監視レポートを設定します。
「ログファイルの収集」（124ページ）	ログファイルレポートを収集して、電子メールまたはFTPでHPのサポート技術者などの受信者に送信

監視およびレポート

PCCは、システムを監視し、その状態とアクティビティをレポートします。PCCは、以下に関するレポートを提供します。

- システムヘルス
- システム性能
- スマートセルの状態

システム内のサーバー（およびそのサービス）は、「ホストグループ」という同じ種類のグループに分類されます。

サービスが正常に機能と表示されている限り、サーバーは正常と仮定されます。サーバーが正常に機能していないことを監視機能が報告する場合、サービスはいっさい利用できません。サービスがCRITICALステータスを持ち、ホストがUPの場合は、おそらくサービスを再起動する必要があります。

ステータスと状態

いくつかのPCCページは、スマートセルの現在のライフサイクル状態、または特定のホストまたはサービスのステータスの値を表示します。ステータスの値は相対的な状態の測定値であり、報告される値の信頼性を伝えるステータス条件に関連する場合があります。

たとえば、ライフサイクルの状態がSUSPENDEDのスマートセル状態は、ホストステータスの値がHEALTHYとして報告される場合があります。これは、IAPオペレーティングシステムとアプリケーションが正常に機能していることを示します。

PCCの各ページでは、ホストやサービスを参照するとき、*ステータス*と言う用語と*状態*という用語が曖昧に使われ互いの区別がないことがよくあります。スマートセルのライフサイクル状態を示すときは必ず「状態」が用いられますが、スマートセルの稼動状態を報告するときは「ステータス」と「状態」の両方が用いられます。これは、スマートセルが他のIAPサーバーと同様にホストと見なされているからです。また、PCCの各ページでは、ステータス条件を「状態」または「状態の種類」と呼びます。

スマートセルのライフサイクル状態

表8 スマートセルのライフサイクル状態

ライフサイクル状態	定義	重要性
ASSIGNED	スマートセルは、ドメインに割り当てられています。 スマートセルは、文書の保存、検索、および取得に使用できます。バックアップが有効の場合、スマートセルデータをバックアップすることができます。	正常
CLOSED	スマートセルは満杯です。 文書の検索と取得に使用できますが、保存には使用できません。バックアップが有効の場合、スマートセルがこの状態に入る前にすべてのスマートセルデータがバックアップされます。	正常
COMPLETE_PROCESSING	データのインデックス作成が完了しました。 スマートセルは満杯です。文書の検索と取得に使用できますが、保存には使用できません。バックアップが有効の場合、スマートセルデータをバックアップすることができます。	メンテナンス
RESTORE	スマートセルは、別のスマートセルからのデータリストア先です。 スマートセルは、文書の保存、検索、または取得に使用できません。	メンテナンス
DISCOVERY	メタサーバーとスマートセルは、スマートセルとそのミラースマートスマートセルの予想される状態に基づいて、スマートセルの開始状態（DISCOVERY後の状態）を決定しています。 スマートセルは、文書の保存、検索、または取得に使用できません。	メンテナンス（起動のみ）
RESET	スマートセルは、リサイクル中です。リサイクル中、保存された文書と文書インデックスのような対応する管理データは消去されます。 システム管理者は、既存のスマートセルデータが必要でないと決定しました。RESET状態は、手動で設定する必要があります。 スマートセルはどのドメインにも関連していないので、文書の保存、検索、または取得に使用できません。	メンテナンス

ライフサイクル状態	定義	重要性
SUSPENDED 	以下のいずれかです。 ・ スマートセルまたはそのミラースマートセルで、プロセスが失敗しました。 ・ ミラースマートセルはDEADです。 注記： スマートセルのステータスがOKの場合は、ミラースマートセルだけで障害が発生しました。 スマートセルは、保存に使用できません。文書の検索と取得には使用できます（失敗したプロセスが検索エンジンを無効にしていない場合）。バックアップが有効の場合、スマートセルは、まだバックアップされていない新しいデータをバックアップしています。	障害
DEAD 	スマートセルで障害が発生しました。 セルは、文書の保存、検索、または取得に使用できません。バックアップが有効な場合、一部またはすべてのスマートセルデータがバックアップされていない可能性があり、その場合は、今後データがバックアップされることはありません。	障害
UNKNOWN 	スマートセルの状態は不明です。	不明
FREE	スマートセルは未使用です（青色で表示されます）。ASSIGNEDにしたり、データ復元先に使用できます。 スマートセルはどのドメインにも関連していないので、文書の保存、検索、または取得に使用できません。	正常

3 System Status（システムステータス）

この章では、[System Status（システムステータス）]の各ページに表示される情報について説明します。

次の項目があります。

Overview（概要）

[Overview]には、システム状態の概要が表示されます。以下の情報が表示されます。

- システムで現在発生している問題についての警告。
- システムおよび各ドメインの文書の保存率と容量に関する情報。
- 保存または削除されたオブジェクトに関するプラットフォーム情報。
- システム内のIAPユーザー、グループ、およびレポジトリの数の概要（現時点では、グループはサポートされていないため、常に、「0」と表示されます）。
- 部分的にインデックスが作成されたオブジェクトおよびキャッチオールレポジトリオブジェクトの数の概要。
- 各スマートセルのステータス、状態、および保存率に関するドメイン別の情報。
- インストールされているIAPソフトウェアのバージョンコードに関する情報。
- 各ドメイン内のSMTP接続の数。

注記：

通常、[Overview]は、毎日監視してください。

ページを開くには、左メニューで [Overview] に移動します。

Current Platform Alerts（現在のプラットフォームアラート）

[Overview]の最上部にある、[Current Platform Alerts]ログは、システムハードウェア、サービス、またはアプリケーションで現在発生している問題のアラートを表示します。

注記：

システムで問題が発生していない場合は、[Overview]に[Current Platform Alerts]は表示されません。

アラートは、機能別にグループ分けされます。たとえば、ハードウェアに関するアラートは[Hardware]の下、インデックス作成に関するアラートは[Indexing]の下にすべてまとめて表示されます。各アラートには、問

題の説明、問題発生の状況、問題が発生したサーバー、問題の発生日時が含まれます。アラートのコンテキストに[More]が表示されている場合、これをクリックすると問題に関する詳細情報が表示されます。

アラートが発生またはクリアされると必ず、システムイベントが記録されます。[Go to Event Viewer]をクリックするかまたは次の順に移動して最近のすべてのシステムイベントを表示することもできます。[Reporting] > [Event Viewer]。詳細については、「Event Viewer（イベントビューアー）」（119ページ）を参照してください。

アラートレベル

アラートには以下の3つのレベルがあります。

- [クリティカル]：機能は完全に停止しています。システム全体にとって致命的な状態です。IAP管理者がすぐに対応する必要があります。
- [メジャー]：機能に重大な問題が発生していますが、システム全体にとっては致命的ではありません。
- [マイナー]：機能に何らかの内部的問題が発生していますが、機能の状態が致命的なわけではありません。

アプリケーションアラート

アプリケーションアラートは、IAPソフトウェアが生成します。このアラートは、問題が修正されるかまたは消滅するとPCCの[Overview]ページから自動的にクリアされます（アラートのクリアを参照）。各アプリケーションアラートの説明については、「IAPアプリケーション生成アラート」（163ページ）を参照してください。

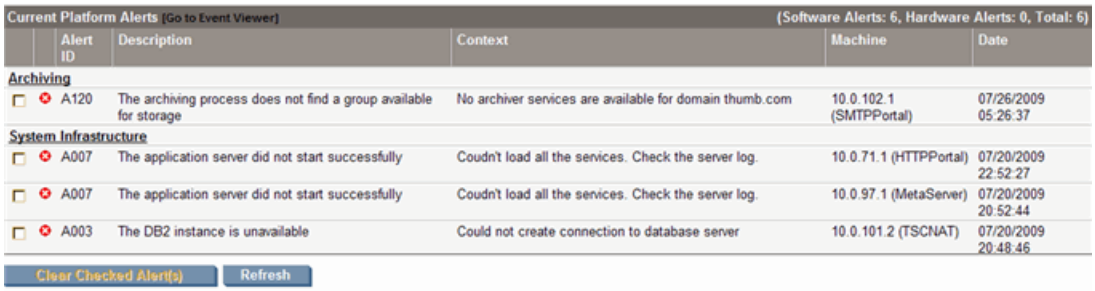


図3 アプリケーションアラートの例

アプリケーションアラートは、SNMPトラップとして外部のSNMPトラップリスナーに転送できます。また、指定した受信者に電子メールで送ることもできます。詳細については、「SNMP Management（SNMPの管理）」（121ページ）を参照してください。

ハードウェアアラート

ハードウェアアラートは、IAPシステムのマシンにインストールされるProLiant Service Packが生成します。通常、ハードウェアアラートはユーザーの操作を要求します。ハードウェアアラートは、問題が発生したサーバーを再起動する場合を除いて、自動的にはクリアされません。ハードウェアアラートには、すべてアラートID、H001が付けられます。

各ハードウェアアラートは、サーバーのHP System Management Homepageへのリンクを備えており、このページで詳細情報を確認できます。「ハードウェアの監視」（50ページ）を参照してください。

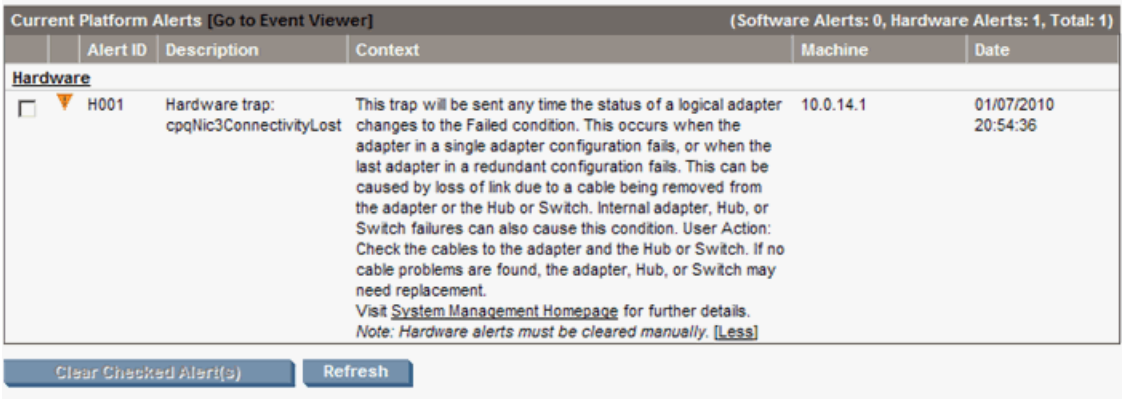


図4 ハードウェアアラートの例

アラートのクリア

アラートは、ランタイム情報として維持されます。生成されるのは問題が最初に発生したときだけで、2回目からは生成されません。次に示すように、アラートをクリアする方法は3つあります。

- 問題の解決。この場合、問題が解決されたことをシステムが確認し、PCCの[Overview]ページからアラートが自動的にクリアされます（アプリケーションアラートだけに該当します）。
- サーバーの再起動。サーバーはPCCに再起動したことを通知し、自身が以前に生成したアラートを削除するようにPCCに要求します。
- 問題の手動での解決。ユーザーは問題を解決した後PCCの[Overview]ページのアラートを手動でクリアできます。アラートの前のチェックボックスを選択し、[Clear Checked Alert(s)]をクリックしてください。

重要：

システムは問題が本当に解決されているかどうかの検証は一切行いません。このため、アラートを手動でクリアする場合は十分に注意してください。問題が存在しなくなったことを確認できないのであればアラートの手動でのクリアは避けるというのが原則です。

Platform performance（プラットフォームパフォーマンス）

[Overview]のこの領域は、[Storage Status]ページからの情報を提供します（「Storage Status（ストレージステータス）」（46ページ）を参照）。左側の表には、各ドメインでの保存されたオブジェクト（文書）の数、ディスクの合計容量と使用量、文書の保存率、および文書のインデックス作成率が表示されます。棒グラフは、システムのストレージ容量の比率を示します。右側の線グラフは、前日から現在の時刻までに格納または更新された1秒当たりのメッセージ数を示します。また、フォルダーの更新量も示します。

Account Manager Service

[Account Manager Service]は、PCCアカウントマネージャーからの情報の概要を提供します（「Account Manager（AM、アカウントの管理）」（71ページ）を参照）。この領域は、個々のIAPユーザーとグループの数、保留状態のユーザーとグループ、およびIAPレポジトリの数を表示します（現時点では、グループはサポートされていないため、常に「0」が表示されます）。この領域には、IAPユーザーアカウントに関する同期化エラーがある場合その数も表示されます。同期化エラーは、[Error Recovery]ページで訂正することができます（「Account Error Recovery（アカウントエラー修復）」（85ページ）を参照）。

CatchAll and Partially Indexed Object（キャッチオールおよび部分的なインデックス作成）

[Overview]のこの領域は、以下の情報を表示します。

- CatchAll Objects(キャッチオールオブジェクト): キャッチオールレポジトリ内の文書の数。このレポジトリには、次の項目と関連付けできないため正しいユーザーレポジトリにルーティングできない文書が格納されます。
  - DASによりインポートされた登録済みIAPユーザーの電子メールアドレス
  - ドメインルーティング規則

  メールリストメッセージは、メッセージの送信先として受信者の名前がない場合、ルーティングできません。

  キャッチオールレポジトリは、Account Manager（「Account Manager（AM、アカウントの管理）」（71ページ）を参照）で、[Repository]ラジオボタンをクリックし、[Other]タブをクリックして、キャッチオールレポジトリを開くと、表示することができます。
- Partially Indexed Objects（部分的なインデックス作成オブジェクト）: インデックス作成失敗レポジトリにある文書の数。このレポジトリには、インデックスの作成に失敗したかまたは部分的にしか作成できていない文書が含まれます（たとえば、システムは、特定のファイル タイプにインデックスを作成できない場合があります）。インデックス作成失敗レポジトリは、Account Manager（「Account Manager（AM、アカウントの管理）」（71ページ）を参照）で表示できます。Account Managerで[Repository]ラジオボタンをクリックし、[Other]タブをクリックし、インデックス作成失敗レポジトリを開きます。

キャッチオールレポジトリとインデックス作成失敗レポジトリは、システムの起動時に自動的に作成されます。

注記:

表示される文書の数が-1の場合、システムは値を読み取れていません。

Platform Statistics（プラットフォーム統計情報）

[Platform Statistics]領域は、IAPスマートセルに関するステータス、状態、および保存情報を提供します。タブをクリックすると、すべてのドメイン内のスマートセルまたは特定のドメイン内のスマートセルに関する情報を表示することができます。また、[Platform Statistics]領域には、システム内の空きスマートセルのIPアドレスも表示されます。

各スマートセルのライフサイクル状態は、色別に表示されます。

- 表の緑色の行は、スマートセルがASSIGNED（割り当て済み）であることを示します。
- 表の明るい緑色の行は、スマートセルがCLOSED（閉じている）であることを示します。
- 表のオレンジ色の行は、スマートセルがCOMPLETE_PROCESSINGまたはRESTORE状態にあることを示します。
- 表の明るい黄色の行は、スマートセルがDISCOVERYまたはRESET状態にあることを示します。
- 表の赤色の行は、スマートセルがSUSPENDED（保留中）であることを示します。
- 表の黒色の行は、スマートセルがDEAD（停止中）であることを示します。
- 表の灰色の行は、スマートセルの状態がUNKNOWN（不明）であることを示します。

詳細は、「スマートセルのライフサイクル状態」(38ページ)を参照してください。

表の各行の先頭にあるアイコンは、スマートセルのJBossステータスを示します。

- 緑色のチェックアイコンは、スマートセルが正常であり、マシンとJBossの両方が起動していることを示します。
- 黄色のアイコンは、スマートセルに問題があることを示します。マシンとJBossは起動していますが、いくつかのMBeanで障害または問題が発生しています。
- 赤色のXアイコンは、スマートセルの停止を示しています。マシン全体かまたはJBossが停止しています。
- 灰色のアイコンは、サービス監視が失敗したことを示します。サーバーのステータスは不明です。

ヒント:

アイコンにマウスカーソルを重ねると、ホスト名、アクティブスレッドカウント、スマートセルのMACアドレスなど、詳細な情報が表示されます。

[Platform Statistics]領域の機能

表9 [Platform Statistics]領域の機能

機能	説明
Platform	プラットフォームの名前、IPアドレス、および文書の保存率。
Domain	ドメインの名前。
Group Name	IAPが自動的に生成するスマートセルグループ識別子。この番号は、すべてのシステム全体で一意です。
Smartcell IP	スマートセルのIPアドレス。
Smartcell Role	スマートセルの役割は、Primary、Secondary、Replica-1、Replica-2のいずれかです。
State	スマートセルの現在のライフサイクル状態。(「スマートセルのライフサイクル状態」(38ページ)を参照)。
Stored Object(s)	スマートセルが割り当てられてから保存されたオブジェクトの数。 注記: システムがアクティブにオブジェクトを保存している場合、このカウントは、「Platform performance(プラットフォームパフォーマンス)」(43ページ)の保存済みオブジェクトカウントと異なる場合があります。この値は、スマートセルでのリアルタイムカウントです。プラットフォーム性能カウントは、(ローカルデータベースから取得され)毎分更新されます。
Indexed Object(s)	スマートセルが割り当てられてからインデックスが作成されたオブジェクトの数。
Store Rate	1秒当たりに保存されるオブジェクトの数。
Index Rate	1秒当たりにインデックスが作成される文書の数。
Index Queue	インデックスが作成されなかった文書の数。
Index Deletion Queue	削除を待っているインデックスが作成された文書の数。

機能	説明
Update Queue	更新を待っている文書の数（たとえば、電子メールフォルダーの更新）。
Other Smart Cells	FREE状態にあるスマートセルのIPアドレス

Version（RISSのバージョン）

[Overview]ページの下の方に、インストールされているIAPソフトウェアのバージョンコードの情報が表示されます。

SMTP Flow Control

[Overview]の最下部にある[SMTP Flow Control]領域は、以下の情報をドメイン別に表示します。

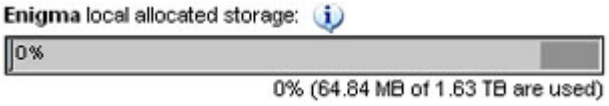
- 許可される接続の最大数
- 現在の接続の数
- アーカイバー接続の数

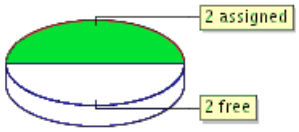
Storage Status（ストレージステータス）

[Storage Status]ページは、各ドメインについて詳細なオブジェクト保存情報を提供します。

ページを開くには、左メニューで [Storage Status] に移動します。

表10 [Storage Status]ページの機能

機能	説明
Platform Store	ドメイン当たりのオブジェクトの数と保存率、およびシステムで保存と複製用に割り当てられている容量。 下の例の保存棒グラフの右側にある暗い領域は、保存領域が上限の90%に達している位置を示しています。暗い領域は、通常、スマートセルのメンテナンスタスクの作業領域用に確保されているディスクスペースの量を示します。  注記： 保存棒グラフは、すべてのアクティブドメインで割り当て済みのスマートセルだけを表示します。IAPには、棒グラフに示されない未使用の未割り当てハードウェアがある場合があります。

機能	説明
Store Rate Graph	システムが前日から現在の時刻までに保存した1秒当たりのメッセージの数を示す線グラフ。フォルダーの更新量も示しています。 例: 
Smart Cell Allocation	各ライフサイクル状態にあるスマートセルの数（各状態については、「スマートセルのライフサイクル状態」(38ページ)で説明しています)。 例: 
Domain Details	ドメイングループID、保存されたオブジェクトの数、保存領域の総量と使用量、およびディスク/スペース比率(棒グラフで表示)。

Software Management(ソフトウェア管理)

[Software Management]ページを使用して、JBossを実行するすべてのIAPサーバーのステータスを表示してください。また、このページで1台または複数のIAPサーバーを起動、停止、または再起動することもできます。

このページは、サーバーのソフトウェアステータスの表示に役立ちます。ただし、起動/停止/再起動機能は、サーバーをアップグレードしているとき、停電が予定されているときなど、必要なときだけ使用してください。

ページを開くには、左メニューで [Software Management] に移動します。

[Software Management]ページの機能

[Software Management]ページには次の情報が表示されます。

表11 [Software Management]ページの機能

機能	説明
Hostname	ホストグループの種類、グループ内のサーバー、各サーバーのフルネーム。 ホストグループの種類は、次のとおりです。 ・ BACKUP Servers: バックアップサーバー ・ CLOUD ROUTER Servers: クラウドルーターサーバー ・ DB Servers: DB2データベースサーバー ・ FIREWALL Servers: ファイアウォールサーバー ・ HTTP Servers: HTTPポータルサーバー ・ KICKSTART Servers: システムソフトウェア/設定ファイルのロードおよびデプロイのためのサーバー ・ LOAD BALANCER Servers: ロードバランサーサーバー ・ PCC Servers: Platform Control Centerサーバー ・ META Servers: メタサーバー ・ SMARTCELL Servers: アーカイブされた文書を保存するサーバー ・ SMTP Servers: SMTPポータル サーバー バージョン2.1以降のIAPでは、Archive GatewayはJBossを使用しません。このため、[Software Management]ページに表示されません。
Status icon	ホスト名の前にあるステータスアイコンは、サーバーのJBossステータスを表示します。 ・ 緑色のチェックアイコンは、サーバーが正常であり、マシンとJBossの両方が起動していることを示します。 ・ 黄色のアイコンはサーバーで問題が発生していることを示します。マシンとJBossは起動していますが、いくつかのMBeanで障害または問題が発生しています。 ・ 赤色のXアイコンは、サーバーが停止していることを示します。マシン全体かまたはJBossが停止しています。 ・ 灰色のアイコンは、サービス監視が失敗したことを示します。サーバーのステータスは不明です。
IP Address	サーバーのIPアドレス。
Status	サーバーのステータス。[Hostname]列のサーバーの前のアイコンに対応します。

システムでのサーバーの起動、停止、および再起動

1台または複数のサーバーを停止、起動、または再起動するには、以下の手順に従います。

1. 操作を実行するマシンを選択します。
   - すべてのサーバーまたはサーバーグループのすべてのマシンを操作する場合は、[Machine Type]ラジオボタンをクリックして、ドロップダウンリストからサーバーを選択します。
   - 特定のマシンを操作する場合は、[Selected Machine(s) Below]ラジオボタンをクリックして、マシンの前にあるチェックボックスを選択します。

   注記:

   PCCサーバーはユーザーインターフェイスをホストするため、[Machine Type]リストには掲載されず、[Selected Machine(s) Below]を指定した場合も選択できません。

   PCCを停止または再起動するには、コマンドラインインターフェイスを使用してください。

2. [Action]ドロップダウンリストで、実行する操作を選択します。
   - Start: 1台のマシンを起動する、すべてのマシンを起動する、または選択したサーバーグループ内のすべてのマシンを起動します。
   - Stop: 1台のマシンを停止する、すべてのマシンを停止する、または選択したサーバーグループ内のすべてのマシンを停止します。
   - Restart: 1台のマシンを再起動する、すべてのマシンを再起動する、または選択したサーバーグループ内のすべてのマシンを再起動します。
   - Staggered Restart: 停止時間を最小に抑えて、すべてのマシンを順番に再起動する、またはすべてのサーバーグループマシンを順番に再起動します。

     [Staggered Restart]は、スマートセルサーバー、HTTPサーバー、およびメタサーバーだけで使用できます。
3. [Run Now]をクリックします。

Hardware Management(ハードウェア管理)

[Hardware Management]ページでは、IAPインフラストラクチャを構成するサーバーとそのサーバーに対応するHP System Management HomepageおよびRemote Management iLOページ(有効の場合)へのリンクを表示できます (リモート管理について詳しくは、第13章(149ページ)を参照してください)。

ページを開くには、左メニューで [Hardware Management] に移動します。

[Hardware Management]ページの機能

表12 [Hardware Management]ページの機能

機能	説明
Hostname	ホストグループの種類、グループ内のサーバー、各サーバーのフルネーム。 ステータスアイコンにマウスカーソルを重ねると、サーバーのIPアドレスを表示できます。 ホストグループの種類は、次のとおりです。 ・ ARCHIVEGATEWAY Servers: アーカイブゲートウェイ(電子メールマイニング)サーバー ・ BACKUP Servers: バックアップサーバー ・ CLOUD ROUTER Servers: クラウドルーターサーバー ・ DB Servers: DB2データベースサーバー ・ FIREWALL Servers: ファイアウォールサーバー ・ HTTP Servers: HTTPポータルサーバー ・ KICKSTART Servers: システムソフトウェア/設定ファイルのロードおよびデプロイのためのサーバー ・ LOAD BALANCER Servers: ロードバランサーサーバー ・ PCC Servers: Platform Control Centerサーバー ・ META Servers: メタサーバー ・ SMARTCELL Servers: アーカイブされたデータを保存するためのスマートセルサーバー ・ SMTP Servers: SMTPポータルサーバー
Status icon	ホスト名の前にあるアイコンは、各サーバーのハードウェアステータスを表示します。 ・ 緑色のチェックアイコンは、そのサーバーについてハードウェアアラートが発生していないことを示します。 ・ 赤色のXアイコンは、そのサーバーについて少なくとも1つのハードウェアアラートが発生していることを示します。 ステータスアイコンにマウスカーソルを重ねると、アラートの数が表示されます。アラートを表示するには、PCCの[Overview]ページの[Current Platform Alerts]に移動します。
MAC Address	サーバーのMACアドレス。
System Management	[View]をクリックして、サーバーのHP System Management Homepageに接続します。このページには、サーバーのハードウェアステータスなどのデータが表示されます。 詳細については、次のハードウェアの監視を参照してください。
Remote Management	サーバーでiLO/Lights-Out 100がセットアップされ、プロキシアクセスモードで設定されているかどうかを示します。 リモート管理を有効にすると、[Manage]リンクが表示されます。このリンクをクリックすると、iLOまたはLights-Out 100のWebインターフェイスが表示されます。このインターフェイスを使用してサーバーの電源入れ直しなどの操作を行えます。

ハードウェアの監視

IAPハードウェアの状態は、PCCのユーザーインターフェイス、各サーバーのHP System Management Homepage、または(使用できる場合)HP System Managementコンソールから監視できます。IAPサーバー

のハードウェア監視は、ProLiantマネジメントエージェントが担当します。IAPのソフトウェアには、標準的なHP ProLiantハードウェアマネジメントエージェントとシステムホームページエージェントが含まれています。マネジメントエージェントは、SNMPトラップという方法でハードウェア監視のためのSNMPサポートを提供します。

PCC上で実行されるスタンドアロンのIAPプロキシエージェントは、IAPの各サーバー上のProLiantエージェントからのSNMPハードウェアトラップを集約します。エージェントは、SIMによる検出とトラップの転送に使用されます。

SIMによる検出：IAPプロキシエージェントは、PCCの外部ネットワークIPアドレスについての外部SIMサーバーからのSNMP get要求に対応します。外部のSIMサーバーは、IAPアプライアンスを識別するように設定する必要があります。IAPアプライアンスがSIMのコンソールに表示される際、そのIPアドレスはPCCの外部ネットワークのIPアドレスになります。

トラップ転送：プロキシエージェントは、個々のIAPサーバーからのSNMPトラップを待ち受けます。

- SIM：PCCサーバーのプロキシエージェントは、SIMでの検出後、SIMサーバーのIPアドレスを使用して設定し、トラップを転送できるようにする必要があります。外部SIMサーバーの台数には制限はありません。SIMサーバーは、送信元のアドレスがIAPアプライアンスのアドレスであれば、IAPプロキシエージェントから受けとったトラップを表示します。このIAPアプライアンスのアドレスとは、PCCの外部IPアドレスのことです。プロキシエージェントは、トラップをSIMサーバーに転送する前に、送信元アドレスをPCCの外部アドレスに設定してIAPサーバーから受け取ったトラップを修正します。
- PCC：IAPプロキシエージェントは、ProLiantエージェントが使用する既知のMIB定義を読み込んで、SNMPトラップを構文解析し送信元と送信先の情報を取得します。IAPプロキシエージェントは、トラップをPCCにIAPアラートの形式で転送します。PCCでは、トラップは[Overview]ページ最上部の[Current Platform Alerts]ログに表示されます。アラートのコンテキストには、IAPサーバーのSystem Management Homepageへのリンクが表示されます。

ProLiantマネジメントエージェントは、ストレージ（RAIDコントローラーおよびディスク）、サーバー（CPU、メモリ、温度、および電源）、NICなどのハードウェアコンポーネントを監視します。ハードウェアトラップの完全なリストは、次のURLで提供されるProLiant Support Packのドキュメントに掲載されています。http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c00760188/c00760188.pdf（英語）

それ以外の情報は、次のURLで提供されるProLiant Support Packのユーザーおよびインストレーションガイドに掲載されています。http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c01527454/c01527454.pdf（英語）

IAPサーバーのハードウェア監視はProLiantマネジメントエージェントに依存するため、ハードウェア要件はProLiant Support Packの最小要件と深く関わります。詳細については、IAPのサポートマトリックスを参照してください。

IAPプロキシエージェントからのログメッセージは、`proxyagent.log`ファイル（PCCサーバーの`/opt/tools/snmpProxyAgent/`ディレクトリ内）に保存されます。

SIMコンソール

HP SIM中央管理サーバー（CMS）を使用する場合、CMSは、PCCの外部IPアドレスを使用してSNMP経由でSIMのコンソールからIAPアプライアンスを認識できます。IAPアプライアンスを識別するように設定しておくと、SIMのコンソールには、次の図に示すようにIAPが単一の管理対象システムとして表示されます。

図5 SIMコンソール

[ES]列には、IAPのイベントステータスが示されます。このステータスは、受信した中で最も深刻なイベントまたはトラップを意味します。トラップの詳細には、トラップの提供元になった実際のIAPサーバーの情報が含まれます。

重要:

プロキシエージェントからのトラップ転送を有効にするには、SIMサーバーのアドレスをテキストファイルで手動で設定する必要があります。トラップを転送するには、`/opt/tools/snmpProxyAgent/conf/ProxyAgent.properties`ファイルを作成して使用します。このファイルに、次の行を追加してください。`trapsink=<sim_server_ip>` （例：192.168.50.59）

IAPシステムの名前をクリックすると、次に示すようにSystem Homepageが起動します。

図6 System Homepage

IAPから受信したイベントは、[Events]タブをクリックすると表示できます。これにより、イベントテーブルが表示されます。トラップの詳細情報は、[Event Type]をクリックすると入手できます。詳細情報には、トラップの提供元になったIAPサーバーが含まれます。

図7 IAPイベント

SIMのマニュアルには、IAPの監視のための特別な使用法とは別に、HP SIMサーバーの使用、設定、およびユーザーインターフェイスについての説明が掲載されています。

- Windowsインストレーション用のHP SIMインストレーション/コンフィギュレーションガイド:
  http://docs.hp.com/en/418812-005/418812-005.pdf(英語)
- Linuxインストレーション用のHP SIMインストレーション/コンフィギュレーションガイド:
  http://docs.hp.com/en/418811-004/418811-004.pdf(英語)

Performance Graph(パフォーマンスグラフ)

指定した期限でのさまざまなシステムイベントを示すグラフを作成するには、このページを使用します。2種類のグラフを生成することができます。

- System Monitoringグラフ。CPUアイドル利用率、空きメモリ使用量、または使用済みスレッドの数を表示します。
- Platform store and indexingグラフ。システムに保存されたまたはインデックスが作成されたオブジェクトの数、および1秒当たりにオブジェクトが保存またはインデックスが作成される速度を表示します。

表13 [Performance Graph]の機能

機能	説明
Graph Type	グラフの種類またはサーバー名。
Assigned Smartcell or Domain	グラフで示すプラットフォーム、ドメイン、またはスマートセル。
Time Frame	報告される期間。

ページを開くには、左メニューで [Performance Graph] に移動します。

例: Platform Storeグラフ

次に、Platform Store and Indexingパフォーマンスグラフの例を示します。このグラフは、今日の5分間隔のDomain1保存率を示しています。

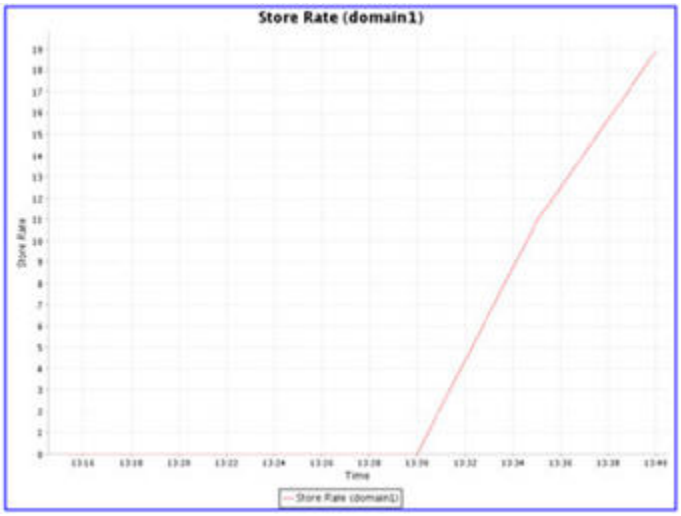


図8 パフォーマンスグラフ: 保存率

例: System Monitoringグラフ

次に、System Monitoringパフォーマンスグラフの例を示します。このグラフは、過去24時間における1時間間隔のデータベースサーバーの空きメモリを示しています。

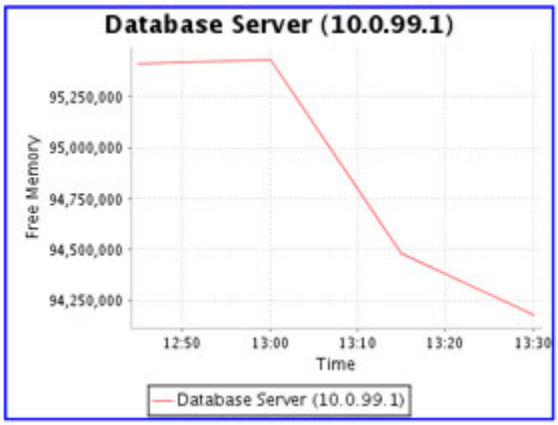


図9 パフォーマンスグラフ: 空きメモリ

パフォーマンスグラフの作成

1. 作成したいグラフの種類に応じて、[System Monitoring]タブまたは[Platform Store and Indexing]タブをクリックします。

2. グラフの種類を選択します。
   - Platform Store and Indexingグラフの場合、次のいずれかを選択します。
     - 保存率(オブジェクト/秒)
     - 保存率(MB/秒)
     - インデックス率
     - オブジェクト数
     - インデックス数
     - アクティブなトランザクション数
     - 更新率(オブジェクト/秒)
   - System Monitoringグラフの場合は、以下のいずれかを選択できます。
     - アイドル状態のCPU

       アイドル状態のCPUの割合
     - 空きメモリ

       Java仮想マシンでの総メモリ容量に対する空きメモリの割合(JVMヒープの空き容量 / JVMヒープの合計と同じ)
     - JVMヒープの合計

       Java仮想マシンの合計メモリ容量
     - JVMヒープの使用量

       Java仮想マシンの総メモリ容量から空きメモリ容量を引いたもの(JVMヒープの合計 - JVMヒープの空き容量と同じ)
     - 使用されているJVM仮想メモリ

       JVMプロセスが使用した仮想メモリの容量(バイト単位)(RAMとスワップメモリ内の容量を含む)。
     - IO

       システムのすべてのメインディスクのディスクリソース(I/O)の使用率。
     - アクティブなスレッド数

       JBossがその時点で実行していたJavaスレッドの数。
3. 次のいずれかのオプションを選択します。
   - Machine Type(System Monitoringグラフ): マシンの種類(たとえば、[PCC]または[SMTP])を選択します。
   - Assigned Smartcell/Domain(Platform Store and Indexingグラフ): [Entire Platform]、ドメイン名、またはスマートセルのIPアドレスを選択します。
4. 期間およびレポート間隔を選択します。
   - Time Frame: 選択済みの期間の場合は、[Select Time Frame]をクリックし、ドロップダウンリストから期間を選択します。
   - From Date、To Date: カスタム期間の場合は、[Custom Time Range]をクリックし、開始日時と終了日時を選択します。カスタム期間は、トラブルシューティングを行う場合に便利です。
   - Interval: ドロップダウンリストから報告する間隔を選択します。
5. [Generate Graph]をクリックします。

4 設定

この章では、次の情報について説明します。

Platform Settings（プラットフォームの設定）

[Platform Settings]ページは、IAPに関するハードウェアおよび設定情報を表示する管理ツールです。

このページは、2つの部分に分かれています。

- 上部には、各ドメインで有効になっているサービスに関する情報が表示されます。
- 下部には、IAPの設定に関する情報が表示されます。

ページを開くには、左メニューで [General Configuration] > [Platform Settings] に移動します。

ドメインの設定

[Platform Settings]ビューの上部には、各ドメインに関する情報が表示されます。これには、ドメインの種類（ExchangeまたはDomino）、有効になっているサービス（たとえば、インデックス作成、複製、フォルダーサポート、コンプライアンス、およびデータバックアップ）、サポートされるオブジェクト（文書）の種類、および保管期間が含まれます。

ドメイン設定情報は、kickstartサーバー上の`Domain.jcml`ファイルから取得されます。

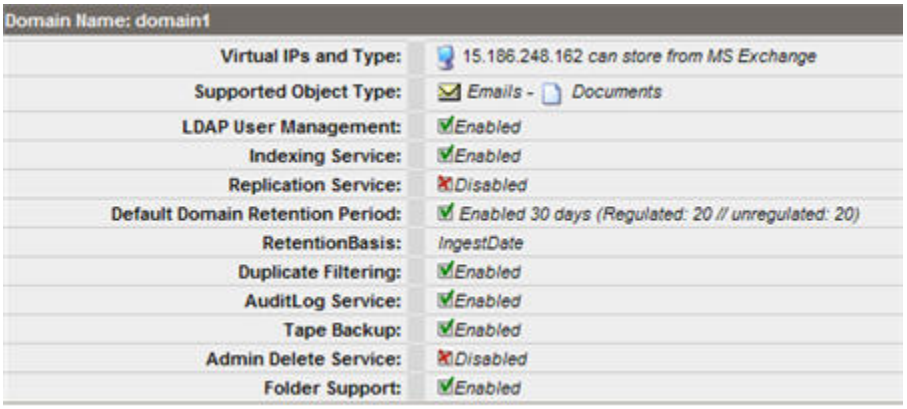


図10 ドメインの設定

Platform Settings（プラットフォームの設定）

[Platform Settings]ページの下部には、IAPのセットアップの詳細が表示されます。この情報は、kickstartサーバーの`BlackBoxConfig.bct`ファイルから取得されます。

Firewall Settings（ファイアウォールの設定）

[Firewall Settings]ページは、PCCサーバーとIAP HTTPポータルのファイアウォールのステータスと設定とその仮想IPアドレスを表示します。

次の情報が含まれています。

表14 ファイアウォールポート

機能	説明
Virtual IP	仮想IPアドレス。
Port	ポート番号。
Service	ポートで動作しているサービス。
Type	ポートで使用されている転送プロトコル：TCPまたはUDP
Inbound/Outbound	ポートのインバウンドトラフィックとアウトバウンドトラフィックで、ファイアウォールが☑有効になっているか、☒無効になっているかを表示します。アウトバウンドトラフィックは、PCCサーバーポートでフィルタリングされません。

ページを開くには、左メニューで [General Configuration] > [Firewall Settings] に移動します。

SSL Configuration（SSLの設定）

SSL（Secure Socket Layer）は、Webブラウザーと Webサーバーが安全な接続経由で通信するためのテクノロジーです。このとき、データは送信側で暗号化されてから送信され、受信側で復号されてから処理されます。これは双方向プロセスであり、サーバーとブラウザーは、データを送信する前にすべてのトラフィックを暗号化します。

[SSL Configuration]ページを使用すると、IAP上の安全な接続のために、証明書署名要求（CSR）とそれに対応する秘密鍵を生成できます。CSRは2種類作成することができます。PCCポータルにアクセスするためのCSRとHTTPポータルにアクセスするためのCSRです。

CSRを生成した後で、プロセスを完了するために必要な手順について、
「PCCポータルへの第三者証明書のインストール」(60ページ)および
「HTTPポータルへの第三者証明書のインストール」(61ページ)を参照してください。

[SSL Configuration]ページには、2つの領域があります。上の領域には、システム内の現在の証明書署名要求が表示されます。下の領域には、証明書署名要求(CSR)とRSA秘密鍵を生成するために入力するフォームが表示されます。

ページを開くには、左メニューで [General Configuration] > [SSL Configuration] に移動します。

使用できる証明書署名要求

表15 IAPで使用できる証明書署名要求(CSR)

機能	説明
Machine Type	CSRが生成されたホスト。ホストは、PCCまたはHTTPポータルです。
Virtual IP	ホストの仮想IPアドレス。
Creation Date	CSRが作成された日付。
Path	CSRのパス。CSRファイルは、常にPCCホストに配置されます。

証明書署名要求の作成

証明書署名要求(CSR)を作成するには、以下の手順に従います。

1. [SSL Configuration]ページの一番下にあるフォームに入力します。

   2種類のCSRファイルを作成することができます。PCCにアクセスするためのCSRファイルとHTTPポータルマシンにアクセスするためのCSRファイルです。

2. [Generate CSR]をクリックします。

   PCCポータルに証明書をインストールする手順は、
   「PCCポータルへの第三者証明書のインストール」(60ページ)を参照してください。

   HTTPポータルに証明書をインストールする手順は、
   「HTTPポータルへの第三者証明書のインストール」(61ページ)を参照してください。

注記:

フォームに誤った情報を入力したため、新しいCSRを生成する必要がある場合は、手順について「証明書署名要求の削除」(59ページ)を参照してください。

証明書署名要求の削除

PCCまたはHTTPポータル用の証明書署名要求(CSR)が生成されると、再生成することができません。証明書要求に正しくない情報を入力した場合は、[SSL Configuration]ページで新しいCSRを作成する前に、手動でファイルを削除する必要があります。

CSRを削除するには、以下の手順に従います。

1. PCCコンソールにログインします。

2. /opt/keysへ進み、次のコマンドのいずれかを使用して、CSRを削除します。

   rm -f pccCert.pem(PCC証明書要求を削除する場合)

   rm -f httpCert.pem(HTTP証明書要求を削除する場合)

3. /opt/keysディレクトリでpccCert.pem、httpCert.pem、またはその両方を削除したら、ログオフするか、PCC UIを閉じます。これを行わない場合、PCC UIを更新するとこれらのファイルが再作成され、[SSL Configuration]ページで新しいCSRを作成することができません。

重要:

重要 秘密鍵ファイル(pcckey.pemまたはhttpkey.pem)は、削除しないでください。

注記:

/opt/keysディレクトリでpccCert.pem、httpCert.pem、またはその両方を削除したら、必ず、ログオフするか、PCC UIを閉じます。これを行わないと、PCC UIでこれらのファイルが再作成されます(また、[SSL Configuration]ページで新しいCSRを作成することができません)。

証明書の生成とPCCポータルへのインストール

IAP PCCポータル用の証明書を生成し、インストールするには、以下の手順に従います。

1. PCC用の証明書署名要求(CSR)を作成します。
   a. PCCのWebインターフェイスにログインし、[General Configuration] > [SSL Configuration]を選択します。
   b. CSR生成フォームに入力します。
   c. PCCのWebインターフェイスからログアウトします。

   PCCに2つのファイルが生成されます。

   - /opt/keys/pccCert.pem(証明書要求)
   - /opt/keys/pcckey.pem(RSA秘密鍵)
2. 証明書要求ファイルをローカルマシンに手動でコピーします。

   scp root@[PCCの外部IPアドレス]:/opt/keys/pccCert.pem
3. VeriSignなどの認証局(CA)に署名のために証明書要求を送信します。

   CAが提供する手順に従います。
4. CAから受信した証明書をIAP PCCにインポートします。
   a. CAから受信した証明書を(たとえば、pccCertSigned.pemとして)ローカルマシンに保存します。
   b. 証明書をPCCにコピーします。

      scp pccCertSigned.pem root@[PCCの外部IPアドレス]:/opt/keys/pccCertSigned.pem

5. 証明書をPCCのApacheサーバーにインポートします。

   ```
   /usr/local/bin/ssl_cert_update.pl --pcc --cert /opt/keys/
   pccCertSelfSigned.pem --key /opt/keys/pcckey.pem
   ```

6. 次のコマンドを実行して、PCCのApacheサーバーを再起動します。

   ```
   /etc/init.d/httpd restart
   ```

証明書の生成とHTTPポータルへのインストール

IAPのHTTPポータルに証明書をインストールするには、以下の手順に従います。

1. HTTPポータル用の証明書署名要求(CSR)を作成します。
   a. PCCのWebインターフェイスにログインし、[General Configuration] > [SSL Configuration]を選択します。
   b. CSR生成フォームに入力します。
   c. PCCのWebインターフェイスからログアウトします。

   PCCに2つのファイルが生成されます。

   - `/opt/keys/httpCert.pm`(証明書要求)
   - `/opt/keys/httpkey.pem`(RSA秘密鍵)

2. 証明書要求ファイルをローカルマシンに手動でコピーします。

   ```
   scp root@[PCCの外部IPアドレス]:/opt/keys/httpCert.pm
   ```

3. VeriSignなどの認証局(CA)に署名のために証明書要求を送信します。

   CAが提供する手順に従います。

4. CAから受信した証明書をIAP PCCにインポートします。
   a. CAから受信した証明書を(たとえば、`httpCertSigned.pem`として)ローカルマシンに保存します。
   b. 証明書をPCCにコピーします。

      ```
      scp httpCertSigned.pem root@[PCCの外部IPアドレス]:/opt/keys/
      httpCertSigned.pem
      ```

5. PCCコンソールから、次の操作を行います。
   a. Apacheサーバーの各HTTPポータルに証明書をインポートします。

      ```
      /usr/local/bin/ssl_cert_update.pl --http --cert /opt/keys/
      httpCertSelfSigned.pem --key /opt/keys/httpkey.pem
      ```

   b. 次のコマンドを実行して、HTTPポータル上のすべてのサービスを再起動します。

      ```
      /opt/bin/restarthttp
      ```

      (また、PCCのWebインターフェイスで[Platform Control]を使用して、サービスを再起動することもできます。「Software Management(ソフトウェア管理)」(47ページ)を参照)。

Software Version（ソフトウェアバージョン）

このページは、システム内のホストが使用するソフトウェアバージョンとインストールされているソフトウェアアップデートを表示します。

表16 [Software Version]ページの機能

機能	説明
Software Version（ソフトウェアバージョン）	インストールされているIAPソフトウェアのバージョンコード。
Patches Applied	システムに適用されたIAPソフトウェアパッチ（アップデート）の履歴。

ページを開くには、左メニューで [General Configuration] > [Software Version] に移動します。

Software Update（ソフトウェアアップデート）

[Software Update]リンクからは、パッチのインストールに使用できるIAPツールに接続されます。ページを開くには、左メニューで[General Configuration] > [Software Update]に移動します。

5 Account Synchronization（アカウントの同期化）

動的アカウント同期化（DAS）を設定するには、このページを使用します。 DASでは、IAP上で電子メールユーザーアカウントを自動的に作成および更新します。特定のIAPドメイン用の1つまたは複数のLDAPサーバーからユーザーの集合を追跡する複数の設定を定義することができます。

注記：

この章では、EAs for Exchangeに対するDASの例を説明します。EAs for Dominoの管理者は、『HP Email Archiving software for IBM Lotus Domino管理者ガイド』でDASについての情報を参照してください。

ページを開くには、左メニューで [User Management] > [Account Synchronization] に移動します。

アカウント同期化の概要

[Account Synchronization]ページは、3つの領域に分かれています。

- [DAS Available Jobs]領域には、作成され、HTTPポータルに割り当てられたすべてのジョブが表示されます。
- [LDAP Server Connectors]領域には、使用できるLDAP接続が表示されます。
- [Jobs History Logs]領域には、DASジョブ実行履歴が表示されます。

DASジョブの作成と実行

DASジョブを作成し、実行するための基本手順は、次のとおりです。

1. LDAP接続を作成します（「LDAPサーバー接続の作成」（64ページ）を参照）。
2. ジョブを作成します。新しいジョブを作成するときは、ジョブに名前とLDAP接続を割り当て、LDAPサーバーでジョブクエリを設定します（「ジョブの作成」（64ページ）を参照）。
3. ジョブをHTTPポータルに割り当てます（「HTTPポータルの割り当て」（67ページ）を参照）。
4. ジョブを実行します（「DASジョブの実行」（68ページ）を参照）。

LDAPサーバー接続の作成

LDAP接続を作成するには、以下の手順に従います。

1. [LDAP Server Connectors]領域で、[New LDAP]をクリックします。
2. フォームに次の情報を入力して、LDAPサービス接続を作成します。

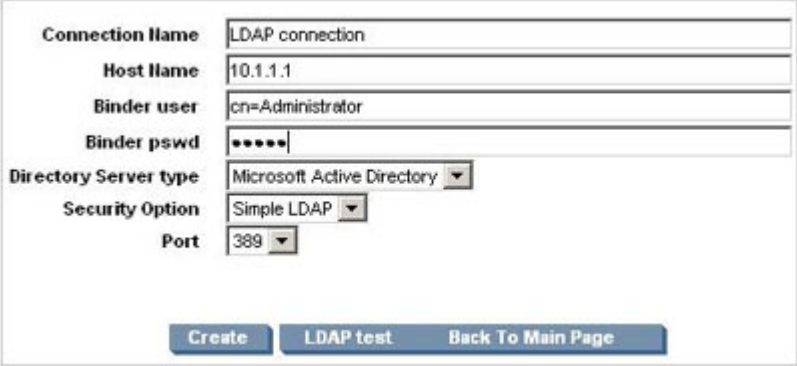


図11 新しいLDAP接続

- Connection Name: LDAP接続を識別するために使用される名前。
- Hostname: LDAPサーバーのIPアドレス。
- Binder user: バインドしたいLDAPディレクトリツリー内のユーザー。少なくとも、ユーザーは、すべてのユーザーオブジェクトに読み取りアクセス権を持っている必要があります。たとえば、次のように入力してください。`cn=admin,o=ou_ldap`
- Binder pswd: Binder userのパスワード。
- Directory Server type: 接続しているLDAPサーバーの種類: Microsoft Active Directory
- Security Option: LDAPセキュリティのタイプ: 単純な認証またはSSL。
- Port: LDAPサーバーで開いているLDAPポート。単純な認証には、ポート389を使用します。SSLサポートには、ポート636を使用します。

3. 作成する前にLDAPサーバーの接続をテストするには、[LDAP test]をクリックします。

   コンテンツペインに、LDAP接続のステータスが表示されます。接続とバインドが正常終了したかどうかと、LDAPサーバーがサポートしている認証の種類が表示されます。エラーは、赤色で表示されます。
4. [Create]をクリックします。
5. [Account Synchronization]ページに戻り、新しいLDAPサーバー接続が[LDAP Server Connectors]に表示されていることを確認します。

ジョブの作成

DASジョブを作成するには、以下の手順に従います。

1. [DAS Available Jobs]領域で、[New JOB]をクリックします。

2. [Job Name]ボックスに名前を入力して、ジョブに名前を付けます（下記の図に示されている文字やスペースを、名前に入れることはできません）。[Next Step]をクリックします。

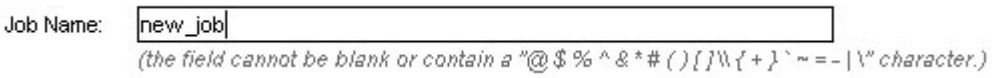


図12 [Create DAS]ジョブ

3. ドロップダウンリストから、ジョブで使用したいLDAP接続を選択します。

   LDAP接続を作成する必要がある場合は、[Create New LDAP Connection]をクリックし、以後の手順について「LDAPサーバー接続の作成」（64ページ）を参照してください。

4. [Next Step]をクリックします。

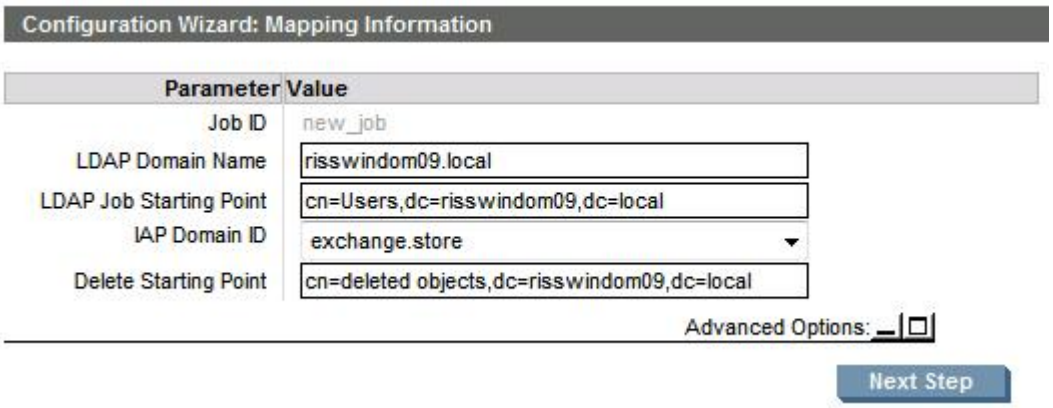


図13 マッピング情報

5. フォームに以下を入力します。

   - LDAP Domain name：ユーザーが属するドメイン。たとえば、次のように入力してください。`ldaptest.com`
   - LDAP Job Starting Point(LDAPジョブの開始点)：ユーザーアカウントが保存されるルートノード。

     例：Exchangeの場合、`ldaptest.com`ドメインの`Users`ノードには、`cn=Users,dc=ldaptest,dc=com`と入力します。値は、親ノードとドメイン名を含むLDAPディレクトリ内の相対的な位置を指定する必要があります（たとえば、`ou=stest,dc=sandbox2k_12,dc=com`。ここで、ouは、Exchange内の組織名です）。
   - IAP DomainID：ユーザーがLDAPサーバー上のユーザーと同期化されるIAPドメインID（ドメイン名ではありません）。これは、`Domain.jcml`に設定されるdomainIDと同じです。
   - Delete Starting Point(開始点の削除)：削除されたユーザーオブジェクトがLDAPサーバーで保存されるルートノード。

     例：Exchangeの場合、`ldaptest.com`ドメインの`deletedObjects`ノードには、`cn=deletedObjects,dc=ldaptest,dc=com`と入力します。値は、親ノードとドメイン名を含むLDAPディレクトリ内の相対的な位置を指定する必要があります。

6. 詳細設定オプションを完了するには、「マッピングの詳細設定オプション」（65ページ）を参照してください。

マッピングの詳細設定オプション

[Advanced Options]アイコン（⊡）をクリックして、詳細設定オプションを表示します。

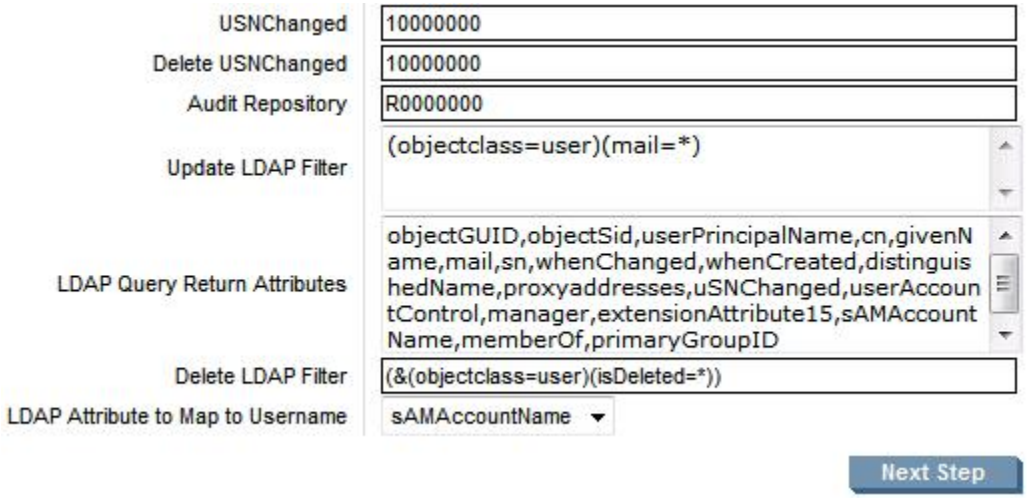


図14 詳細設定オプション

1. 詳細設定オプションのフォームに、以下の情報を入力します。

   - USNChanged: Active DirectoryのUSN(Unique Sequence Number)。Active Directoryは、そのユーザーアカウントが変化するたびに、USNを1ずつ増やします。DASは、増分したUSNを見つけると、新しい情報を抽出します。初期設定では、DASがすべてのユーザーを抽出するように、USNChangedを1に設定します。それ以後は、この値を変更しないでください。
   - Delete USNChanged: 削除されたユーザーディレクトリにあるUSN。これは、USNChangedと同じですが、削除されたオブジェクトに関するものです。初期設定で、この値を0に設定します。その後、この値は変更しないでください。マッピングを初期設定するときは、この値を0に設定する必要があります。
   - NextRepID: 新しいユーザーに割り当てられるIAPレポジトリID。DASはデータベースからこの値を取得しますが、この機能を使用すると、DASの実行時に挿入される最初のユーザー用のレポジトリIDを指定することができます。たとえば、67を入力すると、最初にインポートされるユーザー用に作成され、割り当てられるレポジトリは、R0000067になります。ユーザーがすでにシステムに存在する場合、またはレポジトリIDを予約するために、この機能を使用することができます。既存のレポジトリIDより低い値を指定すると、DASは自動的に次に高い数に値を変更します。デフォルトは、5に設定されます。
   - Audit Repository: 変更しません。
   - Update LDAP filter: 特定のユーザーを収容または除外する基準。たとえば、次のように入力してください。

     Exchangeでは、少なくともデフォルト(objectclass=user)(mail=*)を使用します。これは、電子メールアカウントを持たないユーザーを除外します。
   - LDAP Query return attributes: リターン属性のリスト。例:

     Exchangeでは、LDAPスキーマがマッピング変更を要求しない場合、デフォルトの属性を使用します。
   - Delete LDAP Filter: LDAP削除ユーザーディレクトリ内の特定のユーザーを収容または除外する基準。特殊な場合に、デフォルトに追加されます。
   - LDAP Attribute to Map to Username: ユーザーのユーザー名にマッピングされるActive Directory属性。選択された属性は、webuiユーザー名のログイン名になります。IAPユーザー名マッピングとして、Active DirectoryフィールドのsAMAccountName、userPrincipalName、またはmailを使用できます。

   > 注記:
   >
   > ユーザー名マッピングのために、HTTPポータルのLoadChanges.dseファイルを変更する必要はなくなりました。

2. [Next Step]をクリックして、ジョブを作成します。
3. コンソールに、"Do you want to attach the job to an HTTP portal"と表示されます。このジョブをHTTPポータルに割り当てるには、[Assign Job]をクリックします。 以後の手順については、HTTPポータルの割り当てを参照してください。

HTTPポータルの割り当て

DASジョブを実行する前に、ジョブを実行するHTTPポータルを割り当てます。HTTPポータルには、1つのジョブしか割り当てることができません。

すべてのHTTPポータルが使用されている場合は、別のジョブからHTTPポータルを割り当て直します(HTTPポータルを割り当て直すには、既存のDASジョブを選択し、[Unassign HTTP]ボタンをクリックします)。

HTTPポータルをジョブに割り当てるには、以下の手順に従います。

1. [Assign Job]をクリックします。

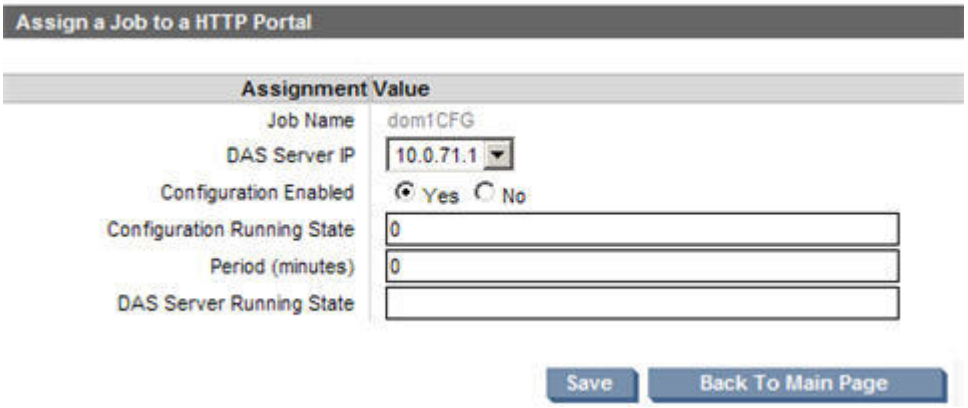


図15 ジョブをポータルに割り当てる

2. フォームに以下の情報を入力します。
   - DAS server IP: DASが設定を実行するDAS HTTPポータルのIP。
   - Configuration Enabled: 有効にするには、[Yes]を選択します。有効にしないと、このコンソールでジョブをスケジューリングしたり、起動することができません。
   - Configuration running state: 変更しません。
   - Period: ジョブ実行の間隔(分)。ジョブを1回実行するには、0を入力します。
   - DAS server running state: 変更しません。
3. [Save]をクリックします。

DASジョブの起動、スケジューリング、および停止

1. [DAS Available Jobs]で、ジョブを選択します。
2. スケジュールを変更せずにジョブを起動するには、[Start]をクリックします。
3. ジョブを起動する前にスケジュールを変更するには、以下の手順に従います。
   a. [Schedule]をクリックします。
   b. ジョブ実行の間隔(分)を入力します。ジョブを一度だけ実行する場合は、0を入力します。DASのスケジュールの間隔は、60分より短くしないでください。
   c. [Confirm Schedule]をクリックして、変更を保存します。
   d. 選択したジョブを起動するには、[Start]をクリックします。

   ジョブが正常に起動したことを示すメッセージが表示されます。
4. [Back to Main Page]をクリックして、DASページに戻ります。

DASジョブの実行を停止するには、以下の手順に従います。

1. [DAS Available Jobs]ページで、ジョブを選択し、[Start/Stop]をクリックします。

   ジョブが停止したことを示すメッセージが表示されます。DASジョブを停止すると、DASが自動的にスケジュールを解除するため以降のDASジョブは実行されなくなります(現在実行中のDASジョブは停止されません)。
2. [Back to Main Page]をクリックして、DASページに戻ります。

注記：

初めてDASを実行している場合やDASを別のHTTPポータルに移動した場合は、初期化オプションをtrueに設定してDASを実行する必要があります。

ジョブの編集または削除

アクティブなジョブや設定済みのジョブを編集または削除するには、以下の手順に従います。

1. [DAS Available Jobs]領域で、編集または削除したいジョブの名前をクリックします。
2. ジョブを編集するには、[Edit]をクリックし、ジョブ マッピングを編集します。

   [Advanced Options]アイコン(□)をクリックして、詳細設定オプションを編集します。ジョブ オプションについては、「ジョブの作成」(64ページ)を参照してください。
3. ジョブを削除するには、[Delete]をクリックします。

利用可能なHTTPポータルの管理

[Account Synchronization]ページからHTTPポータルを起動、停止、または再起動するには、以下の手順に従います。

1. [DAS Available Jobs]領域で、ジョブの名前をクリックします。
2. 特定のサーバーについて、[Assign HTTP Server]または[Unassign HTTP]をクリックします。

利用可能なLDAP接続の編集または削除

LDAP接続を編集または削除するには、以下の手順に従います。

1. [LDAP Server Connectors]領域で、編集または削除したい接続の名前をクリックします。
2. 接続を編集するには、[Edit]をクリックし、フォームに入力し、[Save]をクリックします。
3. 接続を削除するには、[Delete]をクリックします。

DAS履歴ログの表示

DASジョブ履歴ログは、設定した各アクティブジョブに関するジョブ実行のリストを提供します。ログには、ジョブ名、追加、削除、および更新されたIAPユーザーの数、ジョブ実行の周期、ジョブのステータス、ジョブが完了した日時が記録されます。

また、履歴には、追加、削除、および更新されたIAPグループの数も表示されます。

履歴ログを表示するには、[Account Synchronization]ページの一番下にある[Jobs History Log]領域まで移動します。

特定のDASジョブの前の実行履歴を表示するには、ジョブ名前をクリックします。

ジョブのステータスをチェックするには、[State]列にあるプロセスアイコンを確認します。たとえば、アイコンはジョブが完了したことを示します。

また、プロセスアイコンをポイントして、ステータスを表示することもできます。赤色のXアイコンが表示される場合、DASの実行中に問題が検出されているか、または、以前にジョブを実行した際にエラーが発生しそのエラーがAccount Error Recoveryで修正されていません。この問題の詳細については、ステータスア

イコンのツールチップ、Account Error Recoveryツール、およびHTTPポータルのDASログを調べてください。

6 Account Manager（AM、アカウントの管理）

ユーザーアカウントを準備し、更新するには、[Account Manager (AM)]ページを使用します。

この章には以下の項目が含まれています。

ページを開くには、左メニューで [User Management] > [Account Manager] に移動します。

Account Managerの概要

Account Manager（AM）を使用して、ユーザーアカウントとレポジトリを表示および更新するのは、IAPでも特別な場合に限られます。ユーザーアカウントの初期設定および日常的な追加や削除は、Active DirectoryまたはDomino Directoryとの同期化を通じて自動的に行われます。

IAPは、電子メールなどの文書をレポジトリに保存します。レポジトリは、ルーティング規則（保存）とアクセスリスト（取得）別に特定のユーザーに関連付けられた文書の仮想集合です。

AMを使用してアカウントを更新するには、以下の手順に従います。

- 動的アカウント同期化（DAS）を通じてインポートされないユーザーを追加します。
- ユーザーのアクセス権を変更します。
- ユーザーに他のレポジトリへのアクセスを許可します。
- 監査レポジトリなど特別な目的を持つレポジトリを追加します。
- ルーティング規則を追加または編集します。
- いくつかのレポジトリの保管期間を編集します。

注記：

複製ドメインにアカウントを表示できますが、AMを使用して追加または編集することはできません。別のドメインの複製ドメインを選択すると、フィールドは編集できず、操作ボタンも使用できません。

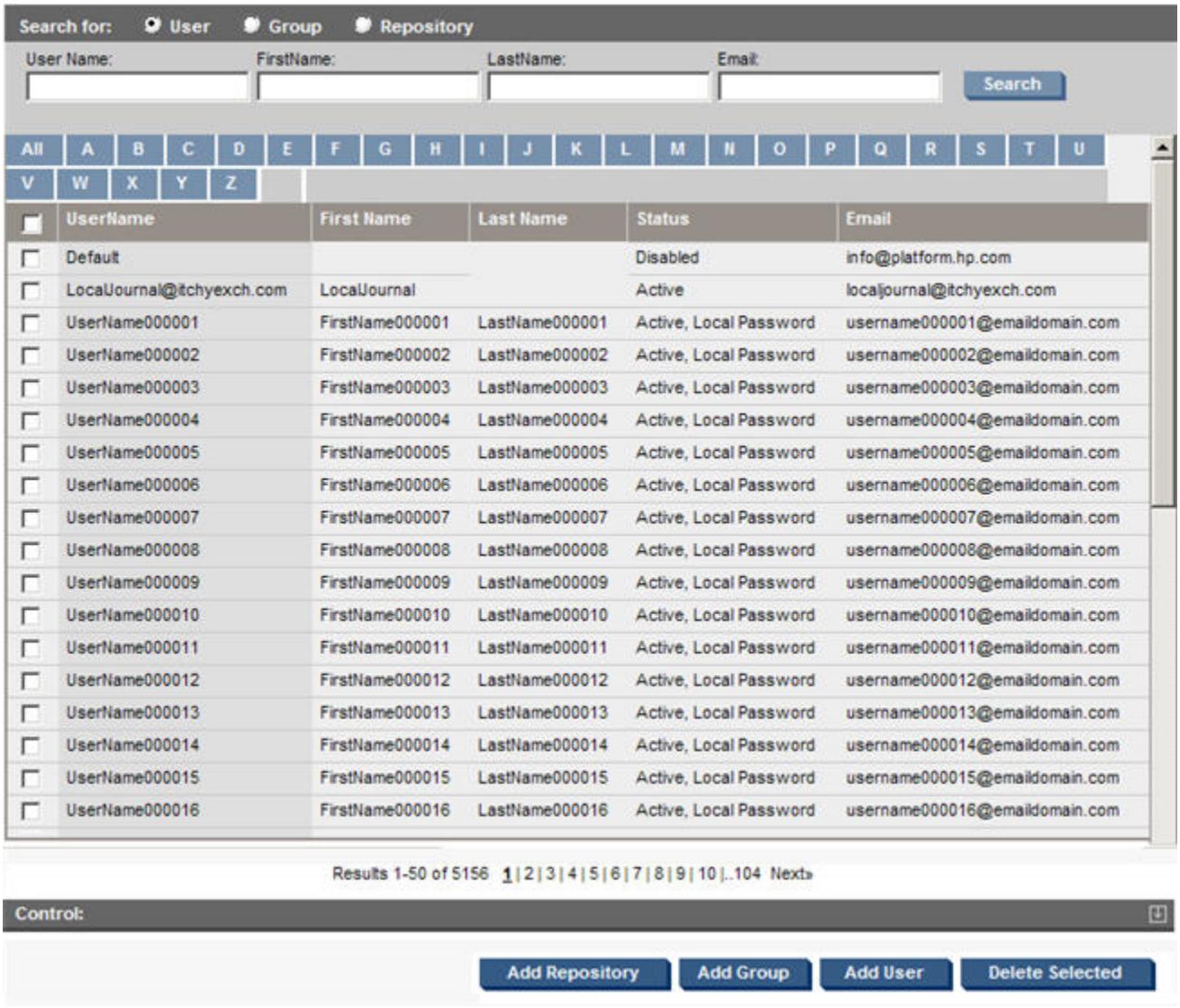


図16 [Account Manager]ページ

ページの右上部に、ドメインのユーザーとグループの総数が表示されます。

[Account Manager]ページの機能

表17 [Account Manager]ページの機能

機能	説明
[Search]ボタン	ユーザー、グループ、またはレポジトリを検索するために使用します。 検索機能は、SQLの“Like”データベース機能を使用します。たとえば、[ユーザー]パネルに「*jack*」と入力すると、jackdoeやjacksmithを検索することができます。*%doe*と入力すると、ユーザーjackdoe、janedoe、またはmaryjanedoeを検索できます。*%ja%*と入力すると、ユーザーjadams、jackdoe、janedoe、jacksmith、またはmaryjanedoeを検索できます。 検索では大文字小文字が区別されません。 ユーザーやグループは、電子メールアカウント名で検索できます。

機能	説明
[All]チェックボックス	フィルター名（ユーザー、グループ、またはレポジトリ）で指定した種類のすべてのオブジェクトを表示するには、このチェックボックスを選択します。たとえば、[ユーザー]フィルターと[All]ボタンを選択すると、すべてのユーザーが表示されます。
[A]ボタン～[Z]ボタン	ボタンの文字で始まる名前だけを表示する場合に使用します。名前は、現在のフィルターパネルのオブジェクトに対応します。 フィルターパネルの中で、検索機能を使用することができます。
パネル	ユーザー、グループ、またはレポジトリラジオボタンを選択すると、対応するパネルが表示されます。 · [Users]（「ユーザーアカウントの管理」（73ページ）を参照） – ユーザーの追加、ユーザー情報の表示と編集、ユーザーのステータスと特権の変更、およびシステムからのユーザーの削除を行うことができます。 · [Groups] – IAPでは現在グループはサポートされません · [Repositories]（「レポジトリの管理」（76ページ）を参照）。既存のレポジトリは、削除できません。
ナビゲーションボタン	以下の場合、ページの一番下にある操作ボタンをクリックします。 · レポジトリを追加する。 · ユーザーを追加する。 · システムからユーザーを削除する。レポジトリへのアクセス権限を付与または剥奪する。

ユーザーアカウントの管理

IAPで個々のユーザーアカウントを表示、追加、削除、または変更するには、[Users]パネルを開きます。

Account Managerでユーザーを追加すると、自動的にユーザー用のプライマリレポジトリが作成されます。また、ユーザーの連絡先電子メールアドレス用のルーティング規則とフィルターが追加され、ユーザー個人のレポジトリへのアクセスが許可されます。

IAPを初めてインストールしたときは、[Users]パネルにDefaultというユーザーアカウントがひとつ表示されています。システムにDASを使用してユーザーをインポートしたら、このエントリーを削除できます。

新しいユーザーの追加

ユーザーは、Account Managerを使用してシステムに直接追加できます。たとえば、DASでインポートした特定のユーザーに管理権限を付与する方法よりもシステムで直接IAP管理者を作成する方法の方がよく用いられます。

システムで作成されローカルパスワードを与えられるユーザーを、*ローカル*ユーザーと呼びます。それに対して、DASでインポートしたユーザーを、*リモート*ユーザーと呼びます。

新しいユーザーを追加するには、以下の手順に従います。

1. [Account Manager]ページの一番下にある[Add User]をクリックします。
2. 表示される[Integrated Archive Platform Account and LDAP Information]フォームに入力します。

   このフォームの記入法について詳しくは、「ユーザーアカウント情報」（74ページ）を参照してください。
3. [Save Now!]をクリックしてユーザー情報を保存します。

ユーザー情報の編集

ユーザー情報を編集するには、以下の手順に従います。

1. [User]ラジオボタンをクリックし、編集するユーザーアカウントを見つけ、ユーザー名をクリックします。

   ユーザーの検索については、「[Account Manager]ページの機能」(72ページ)を参照してください。

2. 表示される[Integrated Archive Platform Account and LDAP Information]フォームで、[Deactivate this check box and then edit the user entries]のチェックボックスをクリアします。

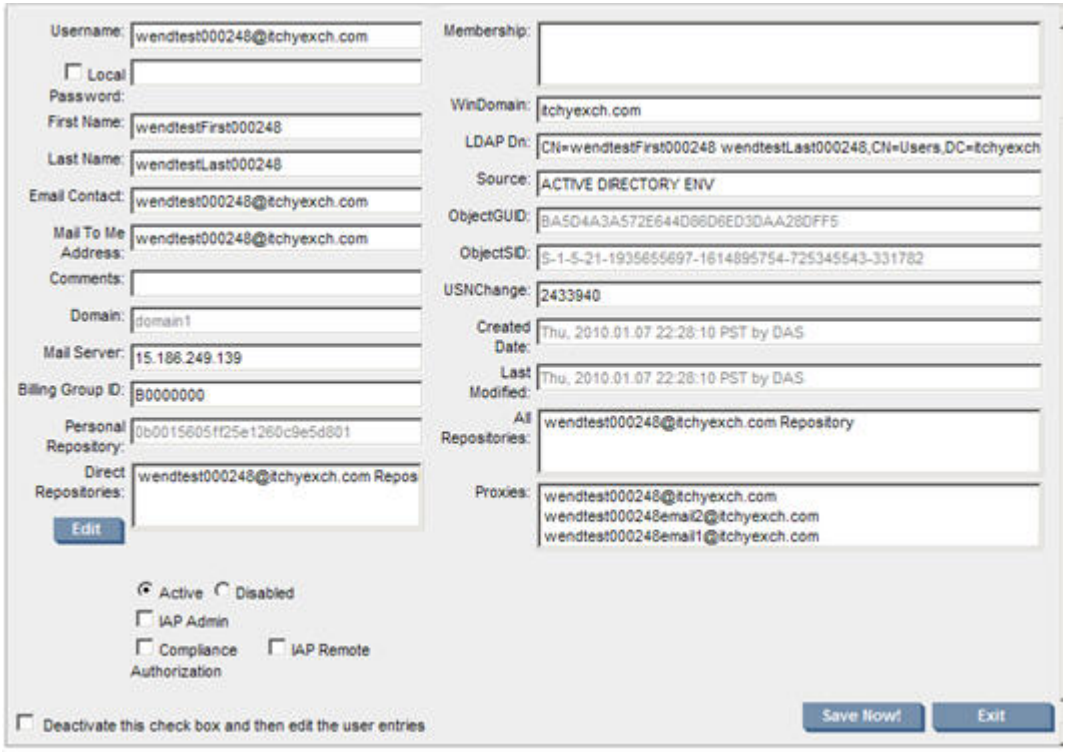


図17 ユーザーアカウント情報の編集

3. 関連するユーザーエントリーを編集します。
4. 完了したら[Save Now!]をクリックします。

注記:

ユーザーのレポジトリ保管期間を変更するには、レポジトリを編集します。
(「レポジトリ情報の編集」(80ページ)を参照)。

ユーザーアカウント情報

表18 ユーザーアカウント情報

機能	説明
[Integrated Archive Platform Account Information]	

機能	説明
Username	（必須）選択したユーザーのシステムログイン名。 ユーザー名は一意でなければなりませんが、ドメイン以外は同じであってもかまいません。たとえば、johnkdoe@company.comが動的アカウント同期化（DAS）を通じてシステムにインポートされたActive Directoryユーザーである場合、IAP内のローカルのユーザーとしてユーザーjohnkdoeを作成することができます。
Local Password	選択したユーザー用のIAPのパスワード。DAS経由でシステムにインポートされたActive Directoryユーザーは、ローカルパスワードが必要ありません。ただし、ローカルユーザーにはパスワードが必要です
First Name	選択したユーザーの名。
Last Name	選択したユーザーの姓。
Email Contact	（必須）選択したユーザーの電子メールアドレス。
Mail To Me Address	（必須）電子メールの宛先です。選択したユーザーがWebインターフェイスからアーカイブされた文書のコピーを送信するために[送信]をクリックすると、この宛先にメールが送られます。
Comments	選択したユーザーアカウントに関するシステム管理者の注記。
Domain	（必須）選択したユーザーが属するIAPドメイン。ドロップダウンリストでドメインを選択します。この選択により、検索の範囲が絞られ、[A]～[Z]のフィルターボタンも限定されます。
Mail Server	選択したユーザー用のメールサーバーのIPアドレス（オプション。ただし、Microsoft Outlook内のクエリが必要な場合は必須）。
Billing Group ID	この番号は、バージョン1.5より前のRISSで、サービスを課金するアカウントを識別する番号です。それ以降のRISSおよびIAPバージョンでは使用されません。
Personal Repository	選択したユーザー用に作成されたレポジトリのID。
Direct Repositories	ユーザーがアクセスできるレポジトリのID。ユーザーは、自動的に自身のレポジトリへのアクセス権を持っています。ユーザーがグループのメンバーである場合は、自動的にグループのプライマリレポジトリへのアクセス権も持っています。 [Edit]をクリックし、レポジトリ用のチェックボックスを選択し、[Add]をクリックし、[Exit]をクリックすると、ユーザーに他のレポジトリへのアクセスを許可することができます。 レポジトリの名前を選択し、[Remove]をクリックすると、リストからレポジトリ（ユーザーの個人レポジトリを除く）を削除することができます。
LDAP Information	
Membership	リモートユーザーが属するグループ。
WinDomain	リモートユーザーが属するWindowsドメイン。
LDAP Dn	リモートユーザーのオブジェクト名、LDAPツリー内の相対的位置、およびドメイン。CN（共通名）はオブジェクト名、cnはツリー内のそのブランチ、およびdcはドメイン名です。この値は、DASが提供します。
Source	アカウント同期化で保守されるフィールド。情報を作成または管理するために使用されるDASジョブを指定します。
Object GUID	LDAPサーバー上のユーザーアカウントのグローバルー意識別子。これは、LDAPサーバー上の正しいアカウントを示すアカウント同期化のキーです。

機能	説明
Object SID	Active Directoryが自動的に生成し、保守するユーザー用の識別子。(編集不能)
USNChange	アカウント同期化が最後に実行された時にLDAPサーバー上の対応するアカウントからインポートされたUSN(Active DirectoryのUnique Sequence Number)。
Created Date	ユーザーアカウントが作成された日付。
Last Modified	ユーザーアカウントが最後に変更された日付。
All Repositories	ダイレクトアクセスまたはグループメンバーシップ経由でユーザーがアクセスできるすべてのレポジトリ。
Proxies	ユーザーのプライマリレポジトリを示す電子メールアドレスを表示します。
チェックボックス等	
Active/Disabled	IAP上のユーザーアカウントを有効または無効にするには、このチェックボックスを選択またはクリアします。
IAP Admin	PCC上のユーザーに管理権限を許可するには、このチェックボックスを選択します。 管理者用に新しいローカルアカウントを作成することが最善です。また、必ず、ローカルパスワードを定義してください。
Compliance	ユーザーがアクセスできるレポジトリで(BCCの宛先を含む)すべての受信者を表示できる場合は、このチェックボックスを選択します。一般に、この機能は、規格準拠担当者に制限されます。コンプライアンス担当者がすべてのBCC情報を参照するには、メールサーバーでBCCまたはエンベロープジャーナリングが有効であり、ゲートウェイサーバーで対応する設定が有効になっている必要があります。この機能はSelective Archivingでは利用できないため、Compliance Archiving(ジャーナルメールボックスのアーカイブ)を有効にする必要があります。
IAP Remote Authorization	[Replication]ページに複製統計情報を正しく表示するには、システムにIAPリモート認可ユーザーがいなければなりません。この目的のためのユーザーアカウントは自動的に作成され、AuthorizationUserという名前と無作為に生成されたパスワードが割り当てられます。 このアカウントのパスワードは、変更することができます。また、必要に応じて、新しいIAPリモート認可ユーザーアカウントとパスワードを作成することもできます。新しいアカウントを作成する場合は、必ず、AuthorizationUserアカウントのこのチェックボックスをクリアするか、システムからAuthorizationUserを削除してください。
Delete Admin	このユーザーは、保管期間が過ぎていないメッセージをIAPから削除する権限を与えられます。このチェックボックスは、`Domain.jcml`で、Admin Deleteサービスが有効になっている場合のみ表示されます。「Administrative Delete」(116ページ)を参照してください。

グループの管理

IAPでは、現在グループはサポートされていません。

レポジトリの管理

レポジトリのルーティング規則の変更や、一部のレポジトリの保管期間の変更、レポジトリの追加を行うには、[Repositories]ペインを使用します。たとえば、特殊なルーティング用のコンテナー(電子メールアドレスまたは電子メールドメイン)を提供するために、レポジトリを追加することができます。

Account Managerでは、レポジトリを削除できません。

レポジトリの概要

IAPは、1つまたは複数のレポジトリに、電子メールなどの文書を保存します。レポジトリは、ルーティング規則別（文書の保存）およびアクセス制御リスト別（文書の取得）に、特定のユーザーに関連付けられた文書の仮想集合です。

レポジトリは、IAPに保存された文書の保管とアクセスの管理に使用されます。レポジトリはクエリの範囲を限定します。ユーザーが検索できるのは、そのユーザーがアクセス権限を持つレポジトリの文書だけです。

IAPに保存された電子メールメッセージは、複数のレポジトリに関連付けられる可能性があります。たとえば、電子メールは複数の受信者に送信され各受信者のレポジトリにアーカイブされることがあります。メッセージ自体はシステムに一度だけ保存されますが、関連付けられたすべてのレポジトリへの参照を含みます。保存されたメッセージは、そのメッセージに関連付けられたすべてのレポジトリの保管期間が過ぎるまで、IAPに残されます。

IAPに格納されるレポジトリにはいくつかのタイプがあります。そのタイプとは、ユーザーレポジトリ、アクセス専用レポジトリ、隔離レポジトリ、AuditLogレポジトリ、およびシステムレポジトリです。これらのレポジトリの詳細については、以下の各項で説明します。

ユーザーレポジトリのタイプ

IAPは、ユーザーレポジトリの次のタイプをサポートします。

- 非規定レポジトリ
- 規定レポジトリ

非規定レポジトリ

非規定レポジトリは、DASによりActive DirectoryまたはDomino Directoryからインポートされたユーザーを対象に自動生成されるレポジトリです。非規定レポジトリは、IAP管理者のローカルユーザーアカウントのセットアップなどのために、Account Managerで直接作成することもできます（システムで作成されローカルパスワードを与えられるユーザーを、ローカルユーザーと呼びます。それに対して、DASでインポートされたユーザーをリモートユーザーと呼びます）。

ユーザーの電子メールアドレスに送信されIAPに取り込まれる電子メールは、そのユーザーのレポジトリに関連付けられます。ユーザーがActive DirectoryまたはDomino Directoryから削除された後DASジョブが実行されると、ユーザーのレポジトリは無効になります。

非規定レポジトリの文書の保管期間は、多くの場合、そのIAPドメインの保管期間と一致しますが、それより長くすることもできます。この値は、`Domain.jcml`で設定します。詳細については、「保管期間」（98ページ）を参照してください。

規定レポジトリ

規定レポジトリは、そのアクティビティで非規定レポジトリのユーザーとは異なる保管期間が必要なユーザーを対象に作成できます。規定レポジトリと非規定レポジトリの違いは、保管期間だけです。規定レポジトリは、Account Managerで作成できます。また、Account Managerでレポジトリ情報を編集して既存の非規定レポジトリを規定レポジトリに変換することもできます（「レポジトリ情報」（81ページ）を参照）。

組織で規定レポジトリを使用しない場合でも、`Domain.jcml`で規定レポジトリの保管期間を設定する必要があります。詳細については、「保管期間」（98ページ）を参照してください。

アクセス専用（監査）レポジトリ

IAPに送信された文書は、各ユーザーのレポジトリの他に監査レポジトリにもルーティングして、法令遵守や法的な目的での検索に対応できます。

監査レポジトリは、コンプライアンス担当者が複数のユーザーのアーカイブ文書を検索範囲にして検索を行えるようにするという特別な目的を持つレポジトリです。ここでいう複数のユーザーには組織のすべての従業員や特定の電子メールドメインに含まれる従業員の中の小グループなどがあります。

バージョン2.0より前のIAPでは、監査レポジトリは、規定タイプまたは非規定のタイプのレポジトリを使用して作成できました。IAP 2.0では、目的を監査だけに絞った*アクセス専用*レポジトリという新しいタイプのレポジトリが導入されました。アクセス専用レポジトリは、規定または非規定レポジトリを監査レポジトリとして使用する場合に発生することがある保管に関する2つの問題、（レポジトリの保管期間が長すぎるとIAPのストレージ容量の問題が発生し、短すぎると監査レポジトリから電子メールが削除され法令遵守のための検索が困難になる）を避けるために作成されました。

アクセス専用レポジトリは、対応するユーザーレポジトリまたは隔離レポジトリに文書が保管されている間は必ずその文書を維持することで、この状況に対応します。その文書に関連付けられた最後のユーザーレポジトリで保管期間が過ぎたときや隔離ホールドが取り消されたとき、文書はアクセス専用レポジトリから削除され消されます。このタイプのレポジトリには、独自の保管期間は設定されません。

ご使用のシステムが以前のバージョンのIAPからアップグレードされ、現在、監査のために1つまたは複数のレポジトリを所有している場合、規定または非規定レポジトリタイプからアクセス専用レポジトリタイプに変換できます。この変換は、必須ではありません。現在の編成では有用な保管ポリシーを組み込めない場合を除いては、既存の監査レポジトリをアクセス専用レポジトリに変換しないでください。変換は、必ず、HPのテクニカルサポートが行うようにしてください。

新しい監査レポジトリのセットアップに必要な手順については、「監査レポジトリのセットアップ」（82ページ）を参照してください。

隔離レポジトリ

隔離レポジトリに文書を配置すると、その文書は自動削除されません。文書などの項目をこのレポジトリに配置しておけば、それらの項目は法的情報保管場所で保護され保管期間を過ぎても削除されません

（ただし、Administrative Deleteユーザーの隔離項目削除メッセージによって削除されることはあります。詳細については、「Administrative Delete」（116ページ）を参照してください）。

隔離レポジトリの内容は、ホールドが不要になった時点で削除できます。ただし、レポジトリの内容を削除しても、IAPから項目が削除されることはありません。この操作により、文書は法的情報保管場所から解放され、その文書に設定されている保管期間の制約を再び受けるようになります。

コンプライアンス担当者は、1つまたは複数の隔離レポジトリをWebインターフェイスで直接作成できます。PCCの[Account Manager]ページでは、これらのレポジトリはユーザーのアカウント情報フォームで示され、[Repositories]パネルの[Quarantine]タブの下に表示されます。

ユーザーが所有できるアクティブ隔離レポジトリの数には、制限はありません。

隔離レポジトリの文書は保管処理から外されるため、IAPのレポジトリフォームでは、このレポジトリタイプの保管期間は「-1」と表示されます。

隔離レポジトリの作成と削除に関わる手順については、IAPユーザーガイドの「隔離レポジトリの使用」を参照してください。

AuditLogレポジトリ

AuditLogは、コンプライアンスプロセスに準拠していることを証明するために必要な会社用の監視システムログを提供します。ログはWebインターフェイスでの各ユーザーセッション、各Duplicate Managerジョブ、およびPCCでのAdministrative Delete権限の付与に対応して作成されます。ログは、ドメインのAuditLogレ

ポジトリ(*<domain>.auditlog*)に保存されます。`Domain.jcml`ファイルでAuditLog機能が有効になっている場合、このレポジトリは自動的に作成されます。このレポジトリのデフォルトの保管期間は7年間です。

> **注記:**
> 許可される最短の保管期間は、どのレポジトリの場合も、30日です。

AuditLogレポジトリのセットアップとコンプライアンス担当ユーザーへのAuditLogレポジトリへのアクセス権限付与については、「AuditLogの有効化」(133ページ)を参照してください。

AuditLogの検索について詳しくは、IAPユーザーガイドの「AuditLogの検索」を参照してください。

システムレポジトリタイプ

次の各レポジトリは、IAPドメインを対象に自動作成されます。

- Recycle Binレポジトリ(<domain>.recyclebin): ドメインに対してフォルダーの取得やエンドユーザー削除機能が有効になっている場合、そのメッセージに関連付けられた電子メールフォルダーまたはユーザーレポジトリのないメッセージはRecycle Binレポジトリに配置されます。Recycle Binレポジトリの保管期間が過ぎると、文書は保管処理の間にIAPから自動削除されます。このレポジトリのデフォルト保管期間は、30日ですが延長できます。
- キャッチオールレポジトリ(<domain>.catch all): キャッチオールレポジトリは、次の項目に関連付けできないために、ユーザーレポジトリや監査レポジトリにルーティングできない文書を格納します。
  - DASによりインポートされた登録IAPユーザーの電子メールアドレス
  - ドメインルーティング規則

  このレポジトリのデフォルト保管期間は、30日ですが延長できます。
- インデックス作成失敗レポジトリ(<domain>.failed.indexing.repository): このレポジトリは、インデックスを作成できないかまたは部分的にしか作成できない文書を格納します (たとえば、システムは特定の文書タイプの電子メール添付ファイルにはインデックスを作成できないことがあります)。

PCCの各ページでのレポジトリのグループ分け

[Account Manager]および[Retention]ページでは、レポジトリは次のタブの下に表示されます。

- [Unregulated(非規定)]
- [Regulated(規定)]
- [Quarantine(隔離)]
- [Other]または[Other Type]

  ドメインのAuditLog、インデックス作成失敗、キャッチオール、Recycle Bin、およびアクセス専用レポジトリを含みます。

レポジトリの追加

DASプロセスでインポートされた各ユーザーについては、ユーザーアカウントとレポジトリが自動的に作成されます。また、Account Managerで次のタイプのレポジトリを手動で作成することもできます。

- 非規定レポジトリ
- 規定レポジトリ
- アクセス専用レポジトリ

これらのレポジトリタイプについて詳しくは、「レポジトリの概要」(77ページ)を参照してください。

[Account Manager]ページから手動でレポジトリを追加するには、以下の手順に従ってください。

1. [Account Manager]ページで、[Add repository]をクリックします。
2. 表示されるIAPレポジトリフォームで次の操作を行います。
   - [Name]ボックスにレポジトリの一意の名前を入力します。
   - [Domain]ボックスで、レポジトリを所属させるIAPドメインを選択します。
   - [Retention]ボックスで、レポジトリに文書を保管する日数を入力します。このフィールドには、`Domain.jcml`の設定に従って、各レポジトリタイプのデフォルト値が埋め込まれます。この値は変更できますが、`Domain.jcml`ファイルでドメインおよびレポジトリタイプについて指定された日数以上の値を設定する必要があります。

     アクセス専用(監査)レポジトリの場合、このフィールドは変更できません。
   - [Type]ボックスで、ドロップダウンメニューからレポジトリタイプを選択します。

     作成できるレポジトリタイプは、[Unregulated(非規制)]、[Regulated(規制)]、および[Access Only(アクセス専用)]レポジトリです。

     [Access Only]を選択すると、ダイアログボックスが表示され、そのレポジトリタイプは監査レポジトリとしてのみ使用すべきであることが説明されます。[OK]をクリックしてこのダイアログボックスを閉じます。
   - [Add Email]ボックスで、ユーザーの電子メールアドレスを指定します(例:user@company.com)。

     アクセス専用(監査)レポジトリでは、このフィールドにはアドレスを入力しないでください。
   - [Add Email Domain]ボックスで、レポジトリに関連付ける電子メールルーティングドメインを指定します(例:company.com)。

     ユーザーレポジトリでは、このフィールドにデータを入力する必要はありません。
3. [Save Now!]をクリックします。

IAPレポジトリフォームの各フィールドについて詳しくは、「レポジトリ情報」(81ページ)を参照してください。

アクセス専用(監査)レポジトリの作成については、「アクセス専用(監査)レポジトリ」(78ページ)を参照してください。

レポジトリ情報の編集

IAPレポジトリフォームを編集するには、以下の手順に従います。

1. [Account Manager]ページで[Repository]ラジオボタンをクリックします。
2. レポジトリのタイプを示すタブ([Unregulated](非規制)、[Regulated](規制)、または[Other](アクセス専用レポジトリ用))をクリックします。
3. 編集するレポジトリの名前を見つけてクリックします。

4. [IAP Repository]フォームで、[Deactivate this check box and then edit the user entries]チェックボックスをクリアします。

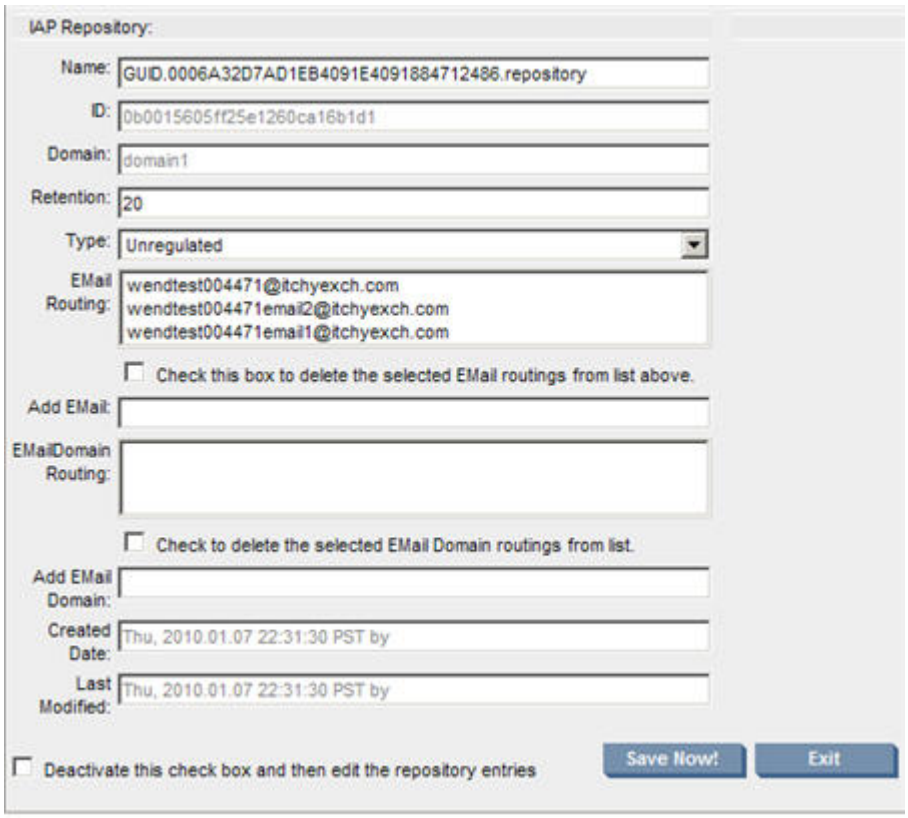


図18 レポジトリ情報の編集

5. レポジトリ情報の説明を参照して、関連エントリーを編集します。
6. [Save Now!]をクリックしてレポジトリ情報を保存します。

レポジトリ情報

表19 レポジトリ情報

機能	説明
Name	（必須）レポジトリを追加する場合は、名前を入力します。
Domain	選択したレポジトリが属するIAPドメイン。ドロップダウンリストでドメインを選択します。この選択により、検索の範囲が絞られ、[A]～[Z]のフィルターボタンも限定されます。
Retention	文書をレポジトリに保管する日数を入力します（例:「30」と入力すると30日になります）。 規制レポジトリまたは非規制レポジトリの場合は、`Domain.jcml`ファイルで設定されている次の2つの値より低い値は指定できません。 ・ ドメインについて指定された保管期間 ・ レポジトリタイプについて指定された保管期間 （これらの値の詳細については、「保管の概要」（97ページ）を参照してください） アクセス専用レポジトリを作成している場合は、このフィールドに入力しないでください。

機能	説明
Type	レポジトリを追加する場合は、次のいずれかのタイプを選択できます。 ・ Regulated（規定） ・ Unregulated（非規定） ・ Access Only（アクセス専用） レポジトリのタイプを変更する場合、次の変更は許可されます。 ・ 規制レポジトリを非規制レポジトリに ・ 非規制レポジトリを規制レポジトリに アクセス専用レポジトリは、別のレポジトリタイプに変更することはできません。
Email routing	電子メールルーティング用のメールアドレス。1つまたは複数のアドレスを削除するには、リストで関連するアドレスを選択し、フィールドの下にあるチェックボックスを選択します。
Add Email	このレポジトリに関連付ける電子メールアドレスを指定します（例：user@company.com）。このエントリーは、レポジトリ情報の保存後、[EMail]ルーティングボックスに表示されます。
Email Domain Routing	レポジトリに関連する電子メールドメイン。
Add Email Domain	このレポジトリに関連付ける電子メールルーティングドメインを指定します（例：company.com）。このエントリーは、レポジトリ情報の保存後、[EMail Domain Routing]ボックスに表示されます。
Created Date	レポジトリが作成された日付。（編集不能）
Last Modified	レポジトリが最後に変更された日付。（編集不能）

監査レポジトリのセットアップ

監査レポジトリは、コンプライアンス担当者が複数のユーザーのアーカイブ文書を検索範囲にして検索を行えるようにするという特別な目的を持つレポジトリです。ここでいう複数のユーザーには、ある組織の全従業員やその一部（法的に重大な問題にさらされているユーザーなど）が該当します。

監査のためにレポジトリをセットアップするには、以下の手順に従います。

1. レポジトリを作成します。
   a. 「レポジトリの追加」（79ページ）の説明に従ってください。
   b. [Add Email Domain]ボックスで、レポジトリに関連付ける電子メールルーティングドメインを指定します。
      詳細は、監査レポジトリのルーティング規則の設定を参照してください。
2. 1人以上のコンプライアンス担当者に監査レポジトリへのアクセス権限を付与します。
   - ユーザーにコンプライアンス権限を付与するには、ユーザーのアカウントフォームで[Compliance]チェックボックスを選択します。
   - コンプライアンスユーザーに監査レポジトリへのアクセス権限を付与するには、ユーザーのアカウントフォームの [Direct Repositories]ボックスでレポジトリを選択します。

   「ユーザー情報の編集」（74ページ）を参照してください。

監査レポジトリのルーティング規則の設定

監査レポジトリは、電子メールルーティングドメインを基準にして電子メールメッセージへのアクセス権限を付与します。IAP Repositoryフォームの[Add Email Domain]ボックスでレポジトリと関連付ける電子メールルーティングドメインを指定します。ドメインは、フォームを保存した時点で[Email Domain Routing]フィールドに保存されます（「レポジトリ情報」（81ページ）を参照）。

次の例では、@company.com電子メールドメインを含む1つ以上の電子メールアドレスを持つメッセージがAuditという名前のレポジトリにルーティングされます。このレポジトリへのアクセス権限を持つコンプライアンス担当者は、電子メールアドレスパターン `<user>@company.com`と一致する任意のユーザーに送信されたメッセージを検索できます。

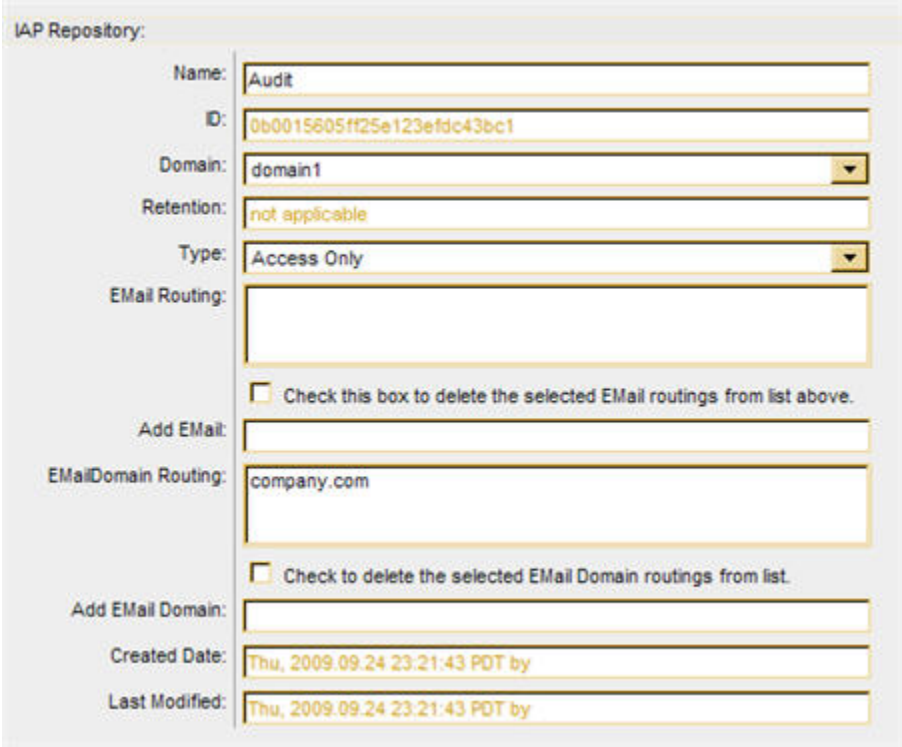


図19 監査レポジトリ用のレポジトリフォーム

監査レポジトリは、電子メールドメインを基準にメッセージを隔離する場合にも利用できます。たとえば、組織が複数の電子メールドメインを持つ場合、電子メールドメインごとに個別の監査レポジトリを作成できます。

また、その組織のすべての電子メールドメインに関連付けられたマスター監査レポジトリを作成し、その後で、各電子メールドメインに対応する個別の監査レポジトリを作成できます。こうしておけば、コンプライアンス担当者は、必要に応じて検索範囲を縮小/拡大できます。

7 Account Error Recovery（アカウントエラー修復）

[Account Error Recovery]ページは、正常に実行されなかったアカウント同期化アクティビティを表示します。

ページを開くには、左メニューで [User Management] > [Account Error Recovery] に移動します。

エラー修復の概要

アカウント同期化アクティビティの失敗には、次のような理由があります。

- ユーザー名またはオブジェクトGUID（グローバルー意識別子）がすでに存在するため、新しいユーザーを追加できない。
- ユーザーのエントリーがないため、ユーザーを更新できない。
- ユーザーのエントリーがないため、ユーザーを削除できない。
- ユーザーのレポジトリ用のエイリアスまたは電子メールルーティング規則を追加できない。
- グループにメンバーシップを追加できない。

アクティビティエラーは、オブジェクトGUID別に最新のエラーから順番に表示されます。アクティビティを選択して再試行したり、アクティビティを削除することができます。

アクティビティは、ページの一番上にある[ユーザー]、[Group]、または[Membership]をクリックして、フィルタリングすることができます。

[Error Recovery]ビューの機能

表20 [Error Recovery]ビューの機能

機能	説明
Date	エラーが発生した日付。
Error	アクティビティエラーの種類。ユーザーのレポジトリ用のエイリアスまたは電子メールルーティング規則を追加できない、など。
USN	Active Directoryの一意順序番号（ユーザーフィルターとGroupフィルターのみ）。
UserName	ユーザーアカウントの名前（ユーザーフィルターのみ）。
GroupName	グループアカウントの名前（Groupフィルターのみ）。
Group	選択したグループ用に自動的に生成されるシステムで一意の識別子（Membershipフィルターのみ）。
Member	レポジトリの名前（Membershipフィルターのみ）。

機能	説明
MemberType	レポジトリの種類: • Regulated(規定) • Unregulated(非規定) • Quarantine(隔離) • Other(ドメインのAuditLog、インデックス作成失敗、キャッチオール、Recycle Bin、およびアクセス専用レポジトリ) (Membershipフィルターのみ)。
Object GUID LDAP DN	LDAPサーバーのユーザーアカウントのGlobal Unique Identifier、対応するオブジェクト名、LDAPツリーの関連ロケーション、およびドメイン CN(共通名)はオブジェクト名、cnはツリー内のそのブランチ、およびdcはドメイン名です。これらの値は、アカウント同期化(DAS)が提供します。 (ユーザーフィルターのみ)。

同期化エラーの修復

同期化アクティビティエラーを修復し、再試行または削除したいアクティビティを識別するには、エントリーをクリックして、そのJava User Management Services(UMS)データベースエントリーなど、アクティビティに関するより多くの情報を表示します。ただし、UMSデータベースエントリーがアクティビティと一致する場合のみ表示されます。

アクティビティを再試行または削除する順序を決定する必要があります。

同期化エラーを修復または削除するには、以下の手順に従います。

1. 再試行したいアクティビティを識別し、それらのエントリーの前にあるチェックボックスを選択します。

   [UserName]列または[GroupName]列のエントリーをクリックすると、エラーの詳細を確認できます。
2. [Apply Selected]をクリックします。

   再試行が正常終了すると、エントリーはリストから削除されます。
3. 削除したいアクティビティを識別し、それらのエントリーの前にあるチェックボックスを選択します。

   [UserName]列または[GroupName]列のエントリーをクリックすると、エラーの詳細を確認できます。
4. [Delete Selected]をクリックします。

   アクティビティを削除すると、リストから削除され、回復することができません。

8 データ管理

この章では、以下の項目について説明します。

Duplicate Manager

[Duplicate Manager]ページによって、重複したマージジョブをスケジュールし、重複したマージジョブのステータスを表示させることができます。

注記：

重複したマージはExchangeの電子メールだけでサポートされます。

ページを開くには、左メニューで [Data Management] > [Duplicate Manager] に移動します。

Duplicate Managerの概要

Duplicate Managerは、シングルインスタンス化に対応してデータを保存する組織向けの機能です。シングルインスタンス化とは、電子メールのコピーを1つだけ保存して複数のユーザーレポジトリで使えるようにすることです。電子メールは、ハッシュと呼ばれる暗号化チェックサムで他と区別されます。ある電子メールクライアントが同じ電子メールを2度保存（メッセージのハッシュにより判断されます）しようとしても、物理的には1つのコピーだけが保存され両方の保存要求に対して同じ参照URIが返されます。

重複している電子メールを保存するとスマートセルでスペースが無駄に使われ、同じ電子メールが複数回示されるため検索結果がまとまりのないものになります。電子メールファイルが保存されると、そのファイルにメタデータと呼ばれる追加データが添付されます。電子メールは誕生から消滅までの間に、何度かその属性（ユーザーのアクセス権限やフォルダー情報など）が変更されます。メタデータもその変更に合わせて変わっていきます。Duplicate Managerツールの目的は、関連するメタデータをすべて確保しながら、重複する電子メールを除去することです。この目的のために、Duplicate Managerは、すべてのメタデータをまとめたものを抽出し、それを電子メールの単一コピーに添付して、重複するすべてのコピーを削除します。

あるユーザーが以前にクエリを実行して成功し、その結果、重複する電子メールが返され、そのクエリ結果が保存されたとします。この場合、このツールの実行後、重複している電子メールのうちの1つを除くす

べてにアクセスできなければなりません。このツールの実行後、ユーザーが保存したクエリ結果セットの中のファイルを隔離すると、残っている電子メールの単一コピーも隔離され、その状態が維持されます。

スマートセルの保存閾値は、ハードディスクの総容量よりも少なく設定されています。これは、スマートセル上で実行されるサービスが操作のために一定割合のディスクスペースを必要とするからです。スマートセルは、この閾値に達するとCLOSED状態に移行します。重複する電子メールは複数のスマートセルグループにまたがって保存されている可能性があり、スマートセルが保存閾値を超え追加のメタデータを受け取れなくなると、そのことが理由で、重複した一連の電子メールに対してマージジョブが機能を発揮できない可能性があります。これらの重複電子メールはCLOSED状態のスマートセルで追加スペースを利用できるようになるまでマージできません。そのためには、一部の電子メールを新しいグループに移動するかまたは保管機能が電子メールを削除して追加ストレージスペースを解放するのを待つしかありません。

マージジョブが完了するまでにかかる時間は、保存されているファイルの数、それらのファイルのうち重複しているものの割合、およびハッシュ当たりの保存されている重複電子メールの平均数によって決まります。最初のマージジョブは完了までに数多くの日数を要することがありますが、以降のマージジョブははるかに早く終わる可能性があります。

重複電子メールのマージ中にエラーが発生しなければ、システム内の重複電子メールは大幅に削減されます。ただし、重複電子メールがすべて削除されるという保証はありません。一部の電子メールにはハッシュが関連付けられていないことがあり、そのため1つのコピーにマージすることはできません。重複電子メールのマージ手順では、最初の試みでいくつかの重複電子メールが見落とされる可能性もあります。これは、重複電子メールのマージ速度を確保するということと重複電子メールの削除を徹底的に行うということの間で取引が行われたからです。重複電子メールのマージ機能は、1回の試みですべての電子メールをマージしようとはしません。この機能は、デフォルトバッチサイズまたはユーザーが設定したバッチサイズに基づき、システム内のすべての電子メールを管理可能な範囲でまとめてマージします。このようなバッチ処理の結果、最初のバッチまたは最後のバッチで重複している電子メールがマージされないことがよくあります。残った重複電子メールは、以降に重複している電子メールのマージを試みる際に削除されます。

Duplicate Managerジョブスケジュール

[Duplicate Manager]ページの上部の[Duplicate Manager Schedule]には、各ドメイン、ドメインポータルIPアドレス、重複したマージジョブのスケジュールされた週間の日数、スケジュールされている時刻、およびジョブステータスが有効かどうかが表示されます。

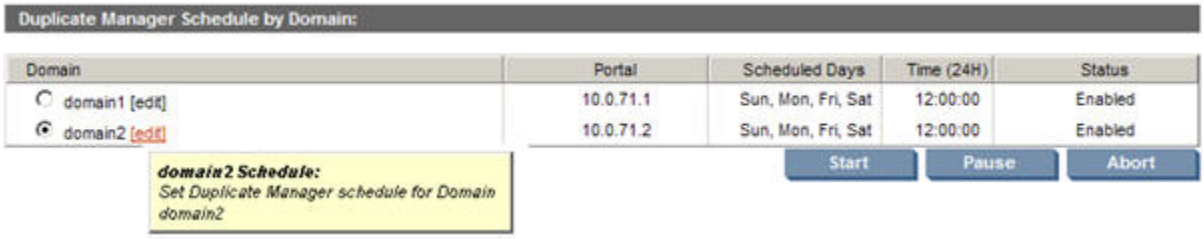


図20 Duplicate Managerジョブスケジュール

ジョブのスケジュール

重複したマージジョブのスケジュールを設定するには、以下の手順に従ってください。

1. [Duplicate Manager Schedule by Domain]セクションで、ジョブをスケジュールするドメインの横の[edit]リンクをクリックします。
2. 表示されるスケジュールページで、ジョブを有効にするチェックボックスを使用し、ジョブの動作するHTTPポータル、ジョブの動作する週間の日数、ジョブの動作する時刻を選択し、[Save Schedule Now]をクリックします。

ヒント：

性能を最大限に活かすために、このツールはDASおよび複製とは別のHTTPポータルで実行してください。

ジョブの有効化と無効化

重複したマージジョブを有効にしたり無効にしたりするには、以下の手順に従ってください。

1. [Duplicate Manager Schedule by Domain]セクションで、ジョブを有効にしたり無効にしたりするドメインの横の[edit]リンクをクリックします。
2. 表示されるスケジュールページで、[Un-check this box to disable the job]（ジョブを有効にする）チェックボックスを選択するか選択解除し、[Save Schedule Now]をクリックします。

ジョブの開始、一時停止、中止

重複したマージジョブを開始にしたり一時停止したり中止したりするには、以下の手順に従ってください。

目的のドメインの左のラジオボタンを使用して、[Start]、[Pause]、または[Abort]を適切にクリックします。[Start]は、選択したドメインでただちに重複したマージジョブを開始します。[Pause]は、選択したドメインで現在動作している重複したマージジョブを一時停止します。[Abort]は、選択したドメインで現在動作しているまたは一時停止している重複したマージジョブを中止します。

Duplicate Managerジョブの履歴

[Duplicate Manager]ページの下部の[Duplicate Manager History Logs]には、重複したマージジョブの最新5つの実行についての情報が表示されます。ドメインをクリックして、そのドメインのすべての（最大50）重複したマージジョブ履歴ログを表示することができます。

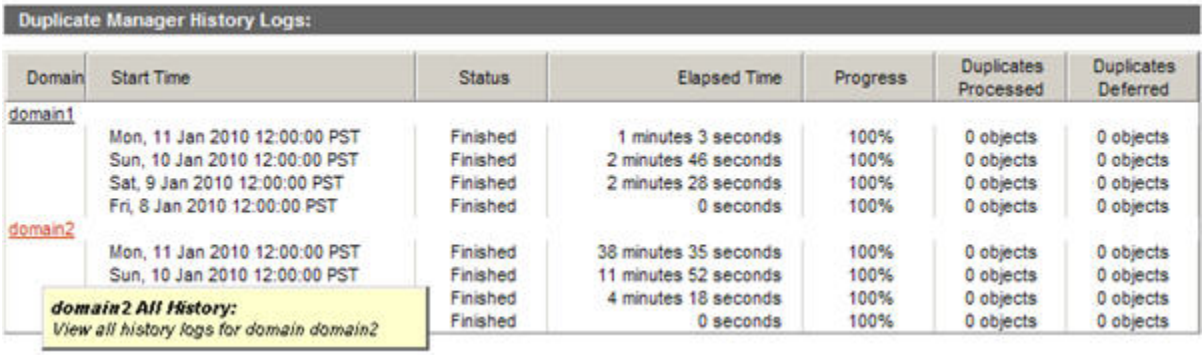


図21 Duplicate Managerジョブの履歴

[Duplicate Manager History Log]には、次のジョブ履歴情報が表示されます。

機能	説明
Domain	ドメインの名前
Start Time	Duplicate Managerジョブが開始したタイムスタンプ
Status	Initializing（初期化中）、Started（開始）、Not Available（利用不可）、Failed（失敗）、またはFinished（完了）

機能	説明
Elapsed Time	ジョブが開始してから完了、中止、または一時停止されるまでの時間
Progress	Duplicate Manager処理済みセットの合計との比率
Duplicated Processed	処理された重複の数
Duplicates Deferred	ジョブ内のDuplicate Managerによって処理されなかった複製の数。

Replication（複製）

注記：

このページは、複製システムが設定されている場合のみ使用できます。

リモートシステム上のドメインの複製を監視、開始、または停止するには、[Replication]ページを使用します。

ページを開くには、左メニューで [Data Management] > [Replication] に移動します。

複製の概要

複製ステータスは、ポーリング周期ごとに更新されます。したがって、複製を開始してから複製率グラフに結果が表示されるまでに最大5分かかる場合があります。ただし、エラーと警告は、システムで発生するとただちに表示されます（[Replication]ページは、PCCホストシステムで1つ以上のドメインが複製用に設定されていないと使用できません）。

複製プロセスでは、プライマリスマートセルグループは次のような動きをします。デフォルトでは、電子メールの複製を担当するのは、プライマリグループのプライマリスマートセルです。このプライマリスマートセルが停止するとフェイルオーバーが発生します。フェイルオーバーとは、セカンダリスマートセルが、そのグループの電子メール複製の任務を引き継ぐ動作のことです。プライマリスマートセルが再起動すると、電子メールの複製の制御権はプライマリスマートセルに移ります。これはフェイルバックと呼ばれます。フェイルオーバーとフェイルバックのメカニズムの目的は、IAPが提供するスマートセルの冗長性を利用してフォールトトレラントな構成を実現し、プライマリスマートセルが停止しても複製を継続でき、かつプライマリスマートセルが正常な状態に復帰したら、複製をプライマリスマートセルが行なうようにするためです。

設置されているIAP内部での複製スマートセルグループの動作は、基本的には、そのプライマリスマートセルグループからのメッセージを取り込むことです。この取り込みを行うには、レプリカ1とレプリカ2のスマートセルがともに利用でき正常に動作していなければなりません。また、設置されているIAPが複製スマートセルを1つだけ持つように構成されている場合は、レプリカ1が利用可能で正常に動作している必要があります。複製グループがいったん割り当てられると、複製スマートセルが何らかの理由で利用できなくなっても新しい割り当ては行われません。複製スマートセルが何らかの理由で利用できない場合、複製スマートセルの割り当ては行われず、複製スマートセルが再び利用できるようになるまで、複製は停止します。

プライマリサイトがクエリに使用できない場合、ユーザーは、ブラウザーでプライマリサイトの代わりに複製サイトのアドレスを入力する必要があります。

注記：

[Replication]ページにリモートシステムからの統計情報を表示するには、Account ManagerでIAPリモート認可ユーザーを設定する必要があります。「ユーザーアカウント情報」（74ページ）で、「IAPリモート認可」を参照してください。

データベース複製

[Replication]ページの上部には、データベースの複製に関する説明が表示されます。

表21 データベース複製の機能

機能	説明
Local Server/ Source Server	複製されたシステムにログインしている場合の複製システムとプライマリシステム。
Local Server/ Target Server	プライマリシステムにログインしている場合のプライマリシステムと複製システム。
Replication Set	複製セットは、複製される1つまたは複数のDB2テーブルから構成されます。
Inbound Sync Time/ Outbound Sync Time	複製セット内のデータベーステーブルが最後に同期化された時刻。同期化の時刻は、緑と赤の2色で表示されます。緑色は、プライマリDB2と複製DB2上のデータベーステーブルが、直前の30分以内に正常に同期化されたことを示します。赤色は同期化が30分以上行われていないことを示します。これは、DB2の複製に問題があることを意味する可能性があるためHPのテクニカルサポートからアドバイスを受ける必要があります。
Inbound Status/ Outbound Status	複製システムとプライマリシステムでの複製のステータス。

DB2複製の再初期化

プライマリシステムと複製システムでDB2複製を削除して再初期化するには、以下の手順に従います。手順では、各ステップが完全に終わるのを待ってから次のステップに進むようにしてください。

1. 複製システムのIAPアプリケーションを停止します。

   複製システムのPCCサーバー: `/opt/bin/stop`

2. 複製システムのDB2を再起動します。

   複製システムのDB2サーバー: `/etc/init.d/db2_app start`

3. プライマリシステムのIAPアプリケーションを停止します。

   プライマリシステムのPCCサーバー: `/opt/bin/stop`

4. プライマリシステムのDB2を再起動します。

   プライマリシステムのDB2サーバー: `/etc/init.d/db2_app start`

5. 複製システムのDB2複製の設定を解除します。

   複製システムのDB2サーバー: `/opt/bin/repl/dbRepl rm`

6. プライマリシステムのDB2複製の設定を解除します。

   プライマリシステムのDB2サーバー: `/opt/bin/repl/dbRepl rm`

7. プライマリシステムのDB2複製を再初期化します。

   プライマリシステムのDB2サーバー: `/opt/bin/repl/dbRepl init`

8. 複製システムのDB2複製を再初期化します。

   複製システムのDB2サーバー: `/opt/bin/repl/dbRepl init`

9. 複製プロセスが完了するのを待ちます。

   平均では、DB2データベースの同期化は30分足らずで完了します。

   DB2複製を監視し、プライマリシステムと複製システムのDB2データベースが同期化されるタイミングを確認するには、以下の手順に従います。

   a. 複製IAPシステムのDB2サーバーにログオンし、次のコマンドを入力します。

```
ssh db2
su - db2udb
db2 connect to ark01db
while true
do
   date
   db2 "select set_name,status,synchpoint,synchtime from asn.ibmsnap_subs_set"
   sleep 10
done
```

   b. 次の状態になるまで待ちます。

   - STATUSにリストされているすべての項目が0になっている。

   > **注記:**
   >
   > STATUSで-1の項目が少なくとも1つある場合、複製はおそらく成功していません。最初から開始し、手順1～8を繰り返すことをお勧めします。

   - SYNCHPOINTにリストされているすべての項目に値がある。
   - SYNCHTIMEにリストされているすべての項目に値があり、今から数分以内である。

   次に、成功した複製の例を示します。

```
SET_NAME            STATUS SYNCHPOINT                 SYNCHTIME
------------------- ------ ------------------------ --------------------------
DB2UDB.base              0 x'4A9DA0D8000000010000' 2009-09-04-16.08.39.244175
DB2UDB.base              0 x'4A9DA113000000010000' 2009-09-04-16.08.51.000000
HAPPY.UBQ                0 x'4A9DA122000000010000' 2009-09-04-16.09.51.955488
HAPPY.UBQ                0 x'4A9DA0D8000000010000' 2009-09-04-16.08.39.244175
GRUMPY.UBQ               0 x'4A9DA0D8000000010000' 2009-09-04-16.08.39.244175
GRUMPY.UBQ               0 x'4A9DA122000000010000' 2009-09-04-16.09.51.955488
HAPPY.D2D                0 x'4A9DA122000000010000' 2009-09-04-16.09.16.904729
HAPPY.D2D                0 x'4A9DA0D8000000010000' 2009-09-04-16.08.04.184687
GRUMPY.D2D               0 x'4A9DA0D8000000010000' 2009-09-04-16.08.04.184687
GRUMPY.D2D               0 x'4A9DA122000000010000' 2009-09-04-16.09.51.955488
CSFR                     0 x'4A9DA0D8000000010000' 2009-09-04-16.08.39.244175
CSFR                     0 x'4A9DA122000000010000' 2009-09-04-16.09.16.904729
```

   次に、失敗した複製の例を示します。

```
SET_NAME            STATUS SYNCHPOINT                 SYNCHTIME
------------------- ------ ------------------------ --------------------------
DB2UDB.base              0 x'4A9DA0D8000000010000' 2009-09-04-16.08.39.244175
DB2UDB.base             -1 x'4A9DA113000000010000' 2009-09-01-15.32.51.000000
HAPPY.UBQ                0 x'4A9DA122000000010000' 2009-09-04-16.09.51.955488
HAPPY.UBQ                0 x'4A9DA0D8000000010000' 2009-09-04-16.08.39.244175
GRUMPY.UBQ               0 x'4A9DA0D8000000010000' 2009-09-04-16.08.39.244175
GRUMPY.UBQ               0 x'4A9DA122000000010000' 2009-09-04-16.09.51.955488
HAPPY.D2D                0 x'4A9DA122000000010000' 2009-09-04-16.09.16.904729
HAPPY.D2D                0 x'4A9DA0D8000000010000' 2009-09-04-16.08.04.184687
GRUMPY.D2D               0 x'4A9DA0D8000000010000' 2009-09-04-16.08.04.184687
```

```
GRUMPY.D2D              0 x'4A9DA122000000010000' 2009-09-04-16.09.51.955488
CSFR                    0 x'4A9DA0D8000000010000' 2009-09-04-16.08.39.244175
CSFR                    0 x'4A9DA122000000010000' 2009-09-04-16.09.16.904729
```

10. 複製が完了したら、プライマリシステムのアプリケーションを再起動します。

    プライマリシステムのPCCサーバー： `/opt/bin/start`

11. 複製システムのアプリケーションを再起動します。

    複製システムのPCCサーバー： `/opt/bin/start`

データ複製のフローと詳細情報

[Replication]ページの中央部には、複製されるデータの流れが表示されます。また、この領域から、ドメインごとに複製プロセスを一時停止または再開することができます。

表22 データ複製の流れ

機能	説明
Domain	複製されているドメインのドメイン名とグループIDおよび以下の情報。 ・ 複製されているスマートセルのIPアドレス、複製のステータス、およびコピーされている保存およびインデックスが作成される文書の数。 チェックアイコンは、正常動作を示します。 Xアイコンは、最後の複製試行が失敗したことを示します。 アイコンは、複製が再試行されていることを示します。 ・ 矢印は、データの方向を示します。方向は、左から右、プライマリシステムから複製システムです。クロス複製構成では、方向は右から左で、リモートに設置されたIAPのプライマリスマートセルグループがこのIAPの複製スマートセルグループに複製中であることを示します。 ・ 複製ドメインにコピーされている保存およびインデックスが作成された文書の数。 ・ 複製ドメインにコピーされているデータの比率(%)。
Suspend/Resume	複製を停止するには、[Suspend]をクリックします。複製は、現在のバッチが複製された後で停止します。 複製を開始するには、[Resume]をクリックします。複製が停止したときに次に複製されるはずだったバッチが複製されます。

[Data Replication Flow and Detail Information]セクションには、[More Details]リンクも用意されています。[More Details]をクリックすると、[Data Replication Detail Information]ページが表示されプライマリシステムと複製システムについての詳しい統計情報が表示されます。統計情報は、システムグループ名ごとに提供され、[Stored Objects]、[Indexed Objects]、[Active Transactions]、[Active Entries]、[Stored Resources]、[Stored Chunks]、[Stored References]、[Used Diskspace]などの情報を含みます。

複製のステータス

[Replication]ページの下部には、複製のステータスが表示されます。

表23 複製サービスの一般的なステータス

機能	説明
Domain	複製されているドメインのドメイン名。

機能	説明
Group ID	複製されているドメインのグループID。
State	複製が進行中かどうかを示します。
File Batch Count	複製のために繰り返し適用されたファイルバッチの数。バッチは100個のメッセージで構成されるため、[File Batch Count]は100個のメッセージから成るバッチの複製の試行回数になります（特定の状況では、バッチが部分的に複製されることがあります。これは、100個のうち *x*個のファイルだけが正常に複製されることを意味します。この状況では、残りの100–*x*個のファイルを含むバッチの複製が試みられますが、その場合も[File Batch Count]は増えます）。
Update Time	最後の複製更新時刻。
Next Retry Time	次の複製更新の日時。
Message	最後の複製更新に関するメッセージ。

Reprocessing（再処理）

[Reprocessing]ページは、各ドメインを表示し、再処理が有効かどうか、再処理がスケジュールされている日時、および履歴ログレポートを表示します。再処理は、最近保存されたデータをスキャンし、適当なレポジトリにメッセージを割り当てなおすエンジンサービスです。

ほとんどの再処理は、自動化された透過的なバックグラウンドプロセスとして実行され、監視以外の操作は不要です。

ほとんどの場合、変更が行われる前に短時間だけ適用される、最近追加されたルーティング規則を再適用するために、メッセージが再処理されます。[Reprocessing]ビューを使用すると、新しいルーティング規則に基づいて、再処理をスケジューリングし、有効にすることができます。

注記：

Reprocessing Utilityを使用して変更を行う場合、変更はただちには行われません。変更はジョブキューに入り、再処理自体は24時間後に実行されます。

ページを開くには、左メニューで [Data Management] > [Reprocessing] に移動します。

すべての再処理スケジュールの変更

すべてのドメインのスケジュールを同じ再処理スケジュールに変更するには、以下の手順に従います。

1. [Reprocessing]ページで、[Reschedule All]をクリックします。
2. ステータスとスケジュールを設定するフォームに入力します。
3. [Reschedule All]をクリックします。
4. すべてのスケジュールが有効になっていることを確認するには、すべての[Reprocessing Status]チェックボックスが選択されていることを確認します。

   選択されている場合は、チェックボックスの横に*Enabled*が表示されます。

再処理スケジュールの編集

ドメインの再処理スケジュールを編集するには、以下の手順に従います。

1. [Reprocessing]ページで、編集するドメインの横にある[edit]リンクをクリックします。

図22 再処理スケジュールの編集

2. ステータスとスケジュールを設定するフォームに入力します。
3. [Save Schedule Now]をクリックします。
4. スケジュールが有効になっていることを確認するには、対応する[Reprocessing Status]チェックボックスが選択されていることを確認します。

   選択されている場合は、チェックボックスの横に*Enabled*が表示されます。

再処理ステータスの変更

特定のドメインまたはリストされているすべてのドメインの再処理スケジュールを有効または無効にすることができます。

再処理スケジュールを変更するには、以下の手順に従います。

1. [Reprocessing]ページで、スケジュールを有効または無効にするドメインを探します。
2. ステータスを変更するために、次の作業のいずれかを行います。

図23 再処理ステータスの変更

- 特定のドメインの再処理を有効にするには、対応する[Reprocessing Status]チェックボックスを選択します。
- 特定のドメインの再処理を無効にするには、対応する[Reprocessing Status]チェックボックスをクリアします。
- すべてのドメインの再処理を有効にするには、[Resume All]をクリックします。
- すべてのドメインの再処理を無効にするには、[Suspend All]をクリックします。

3. [Reprocessing Status]チェックボックスの横にある*Disabled*または*Enabled*を見て、ステータスを確認します。

Reprocessing Utilityの使用

ユーザーが処理に含まれていない場合は、ユーザーレポジトリを再処理することができます。

ページの[Reprocessing Utility]領域で、以下の手順に従います。

図24 Reprocessing utility

1. テキストボックスに、次の情報を入力します。
   - ユーザーの電子メールアドレス
   - ユーザーのレポジトリID

   電子メールアドレスとレポジトリがIAPに存在する場合のみ、ユーザーを再処理することができます。その場合、ユーザーはAccount Managerに表示されます。
2. [Domain Name]ドロップダウンリストで、ユーザーレポジトリが存在するドメインを選択します。
3. 日付範囲を指定し、[Add in Reprocessing Queue]をクリックします。

   ジョブがキューへ送信され、24時間後に再処理が実行されます。

再処理履歴ログの表示

[Reprocessing]ページの一番下にある再処理履歴ログには、設定されている各ドメインの最後に正常に実行された再処理のリストが表示されます。ログには、各ドメイングループ、ドメインが最後に再処理された日時、処理されたファイルの数、および実行の経過時間が含まれます。このレポートは、各グループの個々のスマートセルからのデータを平均した、スマートセルグループからのデータに基づいています。

Retention(保管)

保管期間は、システムがインストールされる際に、IAPドメインとそのレポジトリに対して設定されます。文書の保管期間(この期間を過ぎると文書はシステムから削除されます)を変更するには、[Retention]ページを使用します。

保管と呼ばれる機能は、企業がすべての電子メールを指定年数にわたって保管する必要があるとき、コンプライアンス要件に適合する場合に便利です。

ページを開くには、左メニューで [Data Management] > [Retention] に移動します。

保管の概要

保管を使用すると、文書をIAPに保管する期間(この期間を経過するとその文書は自動削除の対象になりシステムから永久に削除されます)を決めることができます。保管期間はIAPドメインとレポジトリに適用できます。文書は、その文書に関連付けられたすべての保管期間が過ぎるまで物理的にIAPに残ります。

この項では、システムに文書を保管する方法について、以下のトピックを取り上げ説明します。

- 保管ベース
- 保管期間
- エンドユーザー削除
- 保管期間が過ぎたとき

保管ベース

文書は、送信日またはアーカイブ日(「取り込み日」とも呼びます)を基準にして保管されます。

電子メールの送信日とは、電子メールクライアントで電子メールが送信または受信された日付のことです。また、HP File Archivingソフトウェアまたは Object Storage APIインターフェイス経由で保存されるファイルの送信日は、ファイルの「最終変更時のタイムスタンプ」と一致します。

電子メールまたはファイルの取り込み日(アーカイブ日)とは、IAPに保存された日付のことで、設定にはSMTPサーバーの現地時間が用いられます。

保管ベースは、kickstartサーバーの`Domain.jcml`ファイルで設定します。ファイルには、次のうちいずれかのオプションが記述されます。

```
RetentionBasis=IngestDate
RetentionBasis=SendDate
```

`Domain.jcml`ファイルでどちらのオプションも指定されていない場合、保管ベースはデフォルトでアーカイブ日に設定されます。

保管ベースがアーカイブ日から送信日に変更されると、送信日はかなり前だがアーカイブされたのは最近の電子メール(たとえば、HP EAs Exchange PST Importer経由の電子メール)は、その送信日がドメインおよびレポジトリの保管期間に含まれていない場合、次回の保管ジョブの際に削除される可能性があります。

PCCの[ドメインの設定]ページおよび[Retention]ページには、保管ベースが表示されます。

注記:

`Domain.jcml`ファイルで保管設定を行う場合は、必ず、

kickstartサーバーで`regloader.pl –cv –clearallConfirm=<IAP name>` コマンドの実行および、PCCで`/opt/bin/restart`コマンドを実行してIAPを再起動してください。

保管期間

システムのセットアップ時に、`Domain.jcml`ファイルで次の3つの保管期間が設定されます。

- ドメインの保管期間:

  `DomainRetentionPeriodDays=[日数]`

  文書は一定期間IAPドメインのレポジトリに保管されその期間が過ぎるとシステムから自動的に削除されますが、これは、その期間の最短日数です。値は「-1」(保管は無効になります)または30(日)～2,147,483,647(日)の範囲で設定できます。

  システムの実務環境への導入後は、ドメインの保管期間はPCCの[Retention]ページ以外では変更できません。このページでは、保管の有効/無効の切り替えやドメイン保管期間の延長を行えます。IAPが文書のアーカイブを始めた後で、ドメイン保管期間を短縮することはできません。

  [Retention]ページで保管を有効にすると、`Domain.jcml`の「-1」設定は無効になります。PCCの[Retention]ページで行った設定変更は、`Domain.jcml`ファイルの設定よりも優先されます。

- 非規制レポジトリの保管期間:

UnregulatedRetentionPeriodDays=[日数]

非規制レポジトリは、Active DirectoryまたはDomino DirectoryからDASでインポートされるユーザーを対象に作成されます。このレポジトリが作成される際、非規制レポジトリ用の保管期間がデフォルト保管期間として使用されます。必要な場合は、後で、PCCの[Account Manager]ページを使用して個々のレポジトリの保管期間を変更できます。

値を「-1」に設定しても保管は無効になりません。

非規制レポジトリの保管期間は、Domain.jcmlファイルの値を増やすことで変更できます。

- 規制レポジトリの保管期間:

  RegulatedRetentionPeriodDays=[日数]

  規定レポジトリは、そのアクティビティで非規定レポジトリのユーザーとは異なる保管期間が必要なユーザーを対象に作成できます。規制レポジトリは[Account Manager]で作成できますが、[Account Manager]のレポジトリ情報を編集して既存の非規制レポジトリを規制レポジトリに変換することもできます。

  所属する組織で規制レポジトリを使用する場合、通常、保管期間はドメインの保管期間より長くなります。このフィールドの値は、規制レポジトリを使用しない場合でも、設定する必要があります。値を「-1」に設定しても保管は無効になりません。

  規制レポジトリの保管期間は、Domain.jcmlファイルの値を増やすことで変更できます。

保管が機能するには、3つの保管期間をすべて設定する必要があります。保管期間は、PCCの[ドメインの設定]ページおよび[Retention]ページに表示されます。

「ドメイン保管期間の編集」(101ページ)および「レポジトリ保管期間の編集」(104ページ)を参照してください。

例外

ここまで設定が可能な保管期間についての説明をしてきましたが、次のケースにはこの説明は該当しません。

- 隔離レポジトリ: 隔離レポジトリに配置された文書は、法的情報保管場所の間は保護され、その保管期間が過ぎても削除できません。このようなレポジトリの詳細については、「隔離レポジトリ」(78ページ)を参照してください。
- Admin Delete: Administrative Delete権限を持つユーザーは文書を隔離レポジトリから手動で削除できます。また、規制または非規制レポジトリから文書をその最短保管期間が経過する前に手動で削除できます。詳細については、「Administrative Delete」(116ページ)を参照してください。

エンドユーザー削除

エンドユーザー削除について

ユーザーがアーカイブされた電子メールをOutlookのフォルダーから削除しても、その電子メールはIAPからは自動削除されません。このとき、ユーザーは現在IAPに保存されている実際の電子メールへのポインターに当たる「トゥームストーン」を削除しています(ユーザーが電子メールクライアントでそのメッセージを選択するときは、メッセージの取得済みコピーが表示されます)。

Domain.jcmlファイルで保管とエンドユーザー削除が有効な場合にトゥームストーンが削除されると、ユーザーのレポジトリへの参照がアーカイブされているメッセージから取り除かれます。フォルダーの取得が有効な場合、トゥームストーンが配置されていたOutlookフォルダーへの参照もアーカイブされた項目から削除されます。メッセージはユーザーのレポジトリから削除され、ユーザーはOutlookからも、Webインターフェイスからも、Outlook Integrated Archive Searchからもそのメッセージにはアクセスできなくなります(このことで、自身のレポジトリを介してそのメッセージにアクセスする他のユーザーが影響を受けることはありません)。

エンドユーザー削除機能は、規制レポジトリおよび非規制レポジトリの項目に適用され、HP EAs Exchange Outlookクライアントとの連携で使用されます。アーカイブイベントのSynchronize Deleted ItemsをEAs

Exchangeでスケジュール設定して、トゥームストーンの削除がユーザーレポジトリでのメッセージの削除と同期されるようにする必要があります。

エンドユーザー削除は、ユーザーレポジトリからメッセージを削除します。アーカイブされたメッセージ自体をIAPから削除できるのは、そのメッセージからすべてのレポジトリ（およびフォルダー）参照が削除されている場合だけです。ドメインでフォルダーサポートやエンドユーザー削除が有効な場合、関連付けられた電子メールフォルダーまたはユーザーレポジトリを持たなくなったメッセージは、Recycle Binレポジトリに移されます。Recycle Binレポジトリの保管期間（デフォルトでは30日）が経過すると、メッセージは次の保管ジョブでインデックスとスマートセルから自動的に削除されます。

注記：

メッセージがRecycle Binレポジトリに移されると、そのメッセージのインデックスが作成し直されます。このメッセージ項目はRecycle Binレポジトリで検索できますが、削除前に配置されていたユーザーレポジトリでは検索できません。

エンドユーザー削除の設定

エンドユーザー削除を設定するには、`Domain.jcml`ファイルの次のフィールドを使用します。

- `MinUnregulatedRetentionPeriodDays`
- `MinRegulatedRetentionPeriodDays`

各フィールドの値は、Outlookからトゥームストーンが削除された後、電子メールがユーザーレポジトリに残る時間を決定します。`-1`に設定すると、エンドユーザー削除は無効になります。`0`以上の値に設定すると、エンドユーザー削除はそのレポジトリタイプ（規制または非規制）について有効になります。

値を`0`に設定すると、メッセージをユーザーのレポジトリからただちに削除できます。値がレポジトリタイプの保管期間（`RegulatedRetentionPeriodDays`または`UnregulatedRetentionPeriodDays`）と一致する場合、メッセージをOutlookクライアント経由で削除することはできません（これは、コンプライアンス環境で広く行われる設定です）。

アーカイブされたメッセージは、そのメッセージが配置された各レポジトリで保管期間が経過すると、IAPから自動的に削除されます。

次の図に、このプロセスがどのように機能するかを示します。

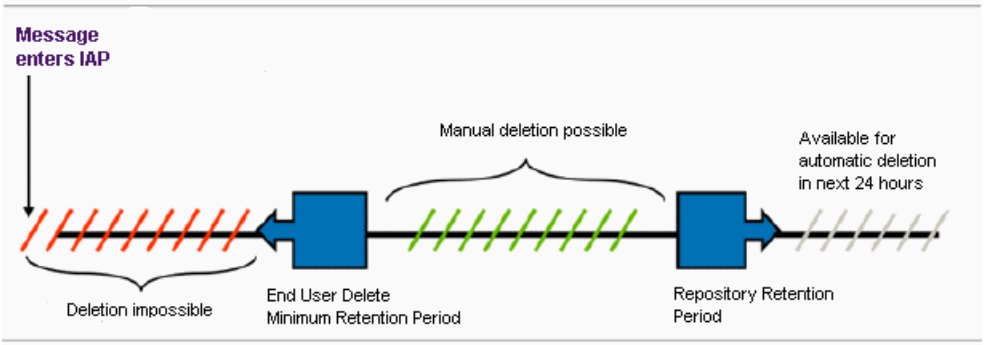


図25 エンドユーザー削除と保管

例

次に、エンドユーザー削除を使用した設定の例を示します。

```
DomainRetentionPeriodsDays=30
UnregulatedRetentionPeriodsDays=30
```

```
RegulatedRetentionPeriodDays=365
MinUnregulatedRetentionPeriodDays=0
MinRegulatedRetentionPeriodDays=365
```

この設定により、次のことが可能になります。

- ユーザーは、Outlookクライアントを使用して非規制レポジトリからメッセージをすぐに削除できます。
- 非規制レポジトリでは、最短保管期間(`MinUnregulatedRetentionPeriodDays`)が過ぎ最長保管期間(`UnregulatedRetentionPeriodsDays`)が来るまでの間にメッセージを手動で削除できます。
- メッセージを規制レポジトリ(存在する場合)から削除することはできません。これは、規制レポジトリについては、最短保管期間が最長保管期間と同じ日数に設定されているからです。
- メッセージに関連付けられたすべてのレポジトリで保管期間が経過すると、メッセージは次の保管ジョブで自動削除できるようになります。

保管期間が過ぎたとき

保管期間が有効な場合、保管ジョブは毎深夜に実行されます。スマートセルのretention managerは、まず、ドメインの保管期間をチェックして最短日数を調べ、保管処理が有効になっていることを確認します。保管が有効な場合、レポジトリの保管期間を含むレポジトリの情報を取得して、そのレポジトリについて指定された日数制限より前に取り込みまたは送信された文書を見つけます。期限が切れたレポジトリへの参照および対応するフォルダー参照は、その文書から削除されます。文書が他のレポジトリにも存在し、まだその保管期間を過ぎていない場合は、インデックスが作成し直されます。

レポジトリ参照を持たなくなった文書は、スマートセルから物理的に削除され、このときインデックスからも削除されます。

ドメイン保管期間の編集

[Retention]ページの[Setting and Configuration]領域には、各IAPドメインの保管ベースと保管期間が表示されます。また、ドメインで保管が有効になっているかどうかも表示されます。

このページでドメインの保管期間の延長や保管処理の有効化を行うには、以下の手順に従います。

1. [Retention]ページで、[Set Domain Retention]の下の[Edit]をクリックします。
2. ドロップダウンリストからプリセットされた期間を選択するか、テキストボックスに特定の期間を入力して、新しい保管期間を設定します。

   期間は、[Minimum Domain Retention Period]よりも長く設定する必要があります。

図26 ドメイン保管期間の編集

3. ドメインで保管処理を有効にする必要がある場合は、[Enable Retention]チェックボックスを選択します

   (保管処理を無効にする場合はチェックを外します)。
4. [Save Retention Now]をクリックして、変更した設定を保存します。

[Resume All]をクリックすると、すべてのドメインの保管処理を有効にできます。保管処理は、[Suspend All]をクリックすると、無効にできます。

注記：

システムが文書のアーカイブを開始した後は、PCCの[Retention]ページ以外では保管処理の有効/無効を切り替えることはできません。`Domain.jcml`ファイルの各retentionフィールドを編集して無効にすることはできません。

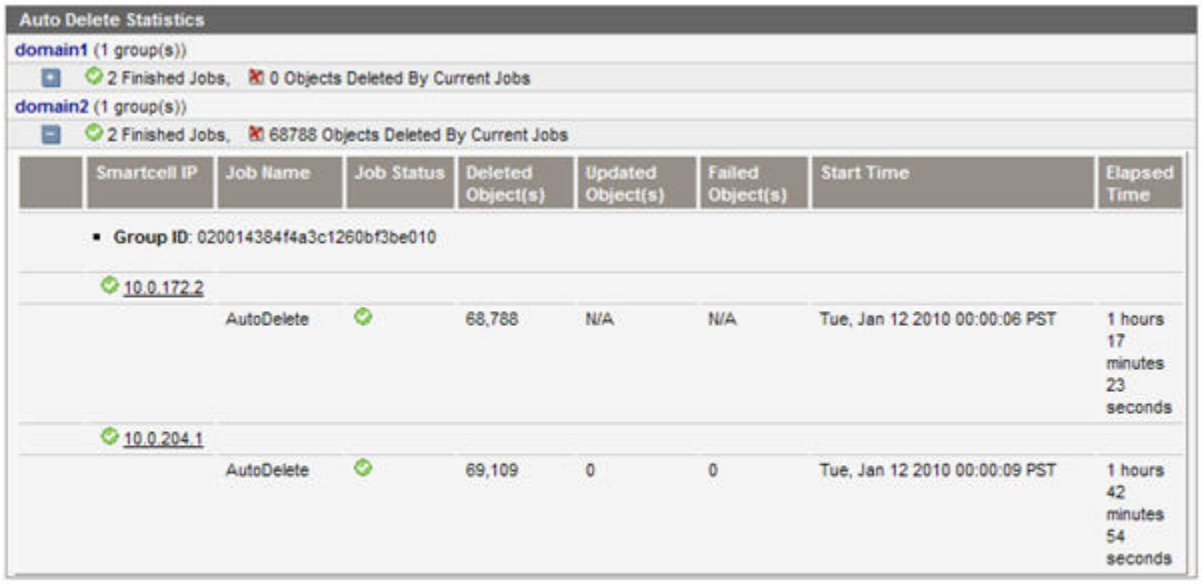
削除に関する統計情報の表示

文書はその保管期間が過ぎるとIAPから自動削除できます。また、手動で削除することもできます。[Retention]ページには、[Auto Delete Statistics]テーブルと[Manual Delete Statistics]テーブルが表示され、最近実行された保管ジョブから収集された情報が掲載されます。

これらのテーブルは、[Retention]ページの下部にあり、ドメインおよびスマートセルについてまとめられたデータが示されます。

自動削除に関する統計情報

[Auto Delete Statistics]テーブルには、スマートセルごとに現在（または最新）の保管ジョブの情報が掲載されます。[Smartcell]リンクをクリックすると、各スマートセルに対する保管ジョブの履歴を表示できます。



Auto Delete Statistics

domain1 (1 group(s))

2 Finished Jobs, 0 Objects Deleted By Current Jobs

domain2 (1 group(s))

2 Finished Jobs, 68788 Objects Deleted By Current Jobs

Smartcell IP	Job Name	Job Status	Deleted Object(s)	Updated Object(s)	Failed Object(s)	Start Time	Elapsed Time
▪ Group ID: 020014384f4a3c1260bf3be010							
10.0.172.2							
	AutoDelete	✓	68,788	N/A	N/A	Tue, Jan 12 2010 00:00:06 PST	1 hours 17 minutes 23 seconds
10.0.204.1							
	AutoDelete	✓	69,109	0	0	Tue, Jan 12 2010 00:00:09 PST	1 hours 42 minutes 54 seconds

Manual Delete Statistics

List of Domain(s)	Deleted Object(s)	Deleted Reference(s)
domain1	0	0
domain2	7	0

図27 [Auto Delete Statistics]および[Manual Delete Statistics]

ドメイン名の下の+アイコンをクリックすると、スマートセルの詳細なアクティビティを表す統計情報が表示されます。統計情報は、ジョブの実行中は、5分ごとに更新されます。

表24 [Auto Delete Statistics]

フィールド	説明
Smartcell IP	ドメイン内の各スマートセルのIPアドレス。 スマートセルのIPアドレスの前にあるアイコンにマウスカーソルを重ねると、スマートセルサーバーの名前、スマートセルのタイプ(プライマリまたはセカンダリ)、スマートセルの状態とステータス、アクティブスレッドの数、およびMACアドレスが表示されます。 スマートセルのIPアドレスをクリックすると、[Platform Auto Delete History]テーブルが表示され、そのスマートセルの保管履歴を表示できます。
Job Name	常に、AutoDeleteです。
Job Status	保管ジョブのステータスは次のいずれかです。 ・ ✓ 完了 ・ ✗ 障害発生 ・ >>>> 実行中 [ジョブのステータス]列のアイコンにマウスカーソルを重ねると、ジョブの進行状況(完了率)が表示されます。ジョブの実行中、ステータスは5分ごとに更新されます。
Deleted Objects	実行中に削除された文書の数。
Updated Objects	レポジトリの保管期間が過ぎたため、レポジトリ参照が削除された文書の数。 レポジトリ参照が残っていない文書にはマークが付けられ、削除の対象になります。レポジトリ参照が残っている文書のインデックスは作成し直されます。

フィールド	説明
Failed Objects	削除できなかった文書の数と更新できなかった文書の数。
Start Time	ジョブが開始された日時。 保管ジョブは、毎深夜（午前0時）に自動で実行されます。
Elapsed Time	ジョブの完了までにかかった時間。

[Manual Deletion Statistics]

[Manual Delete Statistics]テーブルには、`Domain.jcml`でエンドユーザー削除機能が有効になっている場合に、この機能のドメインレベルの統計情報が表示されます（「エンドユーザー削除」（99ページ）を参照）。エンドユーザー削除は、ユーザーが自身のOutlookフォルダーからメッセージのトゥームストーン（アーカイブされたメッセージのポインター）を手動で削除すると発生します。エンドユーザー削除の最短保管期間が経過すると、ユーザーのレポジトリへの参照がメッセージから削除されます。フォルダーの取得が有効な場合、トゥームストーンが配置されていたOutlookフォルダーへの参照もメッセージから削除されます。削除されたレポジトリ参照の数は、[Deleted References]列に表示されます。

IAPからメッセージを削除できるのは、メッセージからすべての参照が削除された場合だけです。

レポジトリ保管期間の編集

非規定および規定レポジトリの保管期間を変更するには、以下の手順に従います。保管期間は、その長さがレポジトリタイプのデフォルト保管期間より長い場合に限り、変更できます。

ドメイン内のAuditLog、キャッチオール、およびRecycle Binレポジトリの保管期間も編集できます。隔離レポジトリに所属する文書は保管処理からは除かれており、このレポジトリタイプには保管期間はありません（IAPレポジトリの詳細については、「レポジトリの概要」（77ページ）を参照してください）。

1. [Retention]ページの[Configuration and Setting]領域で、ドメインの名前をクリックします。
2. レポジトリのタブ（[Regulated]、[Unregulated]、[Other Type]）をクリックして、レポジトリを見つけます。

   AuditLog、キャッチオール、およびRecycle Binレポジトリは、[Other Type]タブの下にあります。

   [Edit User Repositories]ボックスにユーザー名を入力して[Search]ボックスをクリックすると、ユーザーレポジトリを検索できます。

   検索機能は、SQLの“Like”データベース機能を使用します。たとえば、*jack*と入力すると、ユーザーjackdoeまたはjacksmithを検索できます。*%doe*と入力すると、ユーザーjackdoe、janedoe、またはmaryjanedoeを検索できます。*%ja%*と入力すると、ユーザーjadams、jackdoe、janedoe、jacksmith、またはmaryjanedoeを検索できます。

   検索では大文字小文字が区別されません。
3. レポジトリの名前をクリックして、その保管期間を編集します。
4. 表示されるフォームの、[Set New Retention Period]のドロップダウンリストをクリックするかまたはテキストボックスに日数を入力します。

   保管期間は、日数で表示されます。指定する日数は、ドメインの保管期間以上でなければなりません。ドメインの保管期間より短い値は無視されます。
5. [Save Retention Now]をクリックします。

注記：

複製ドメイン上のユーザーレポジトリは、表示できますが、編集できません。別のドメインの複製であるドメインを選択すると、保管期間や他のフィールドは編集できず、操作ボタンも使用できません。

Backup（バックアップ）

PCCの[Backup]の各ページは、プラットフォーム上で実行されている標準的なバックアップサービスとオプションのバックアップサービスに関するステータス情報を提供します。また、これらのページからオプションのバックアップサーバー上で稼動するHP Data Protectorにアクセスできます。

注記：

テープバックアップが設定されているIAPドメインがない場合（`DataBackupEnabled=false`が`Domain.jcml`で指定されている）は、IAPではテープバックアップは無効です。テープバックアップが無効な場合、テープバックアップのステータスは、バックアップページには掲載されません。

IAPのバックアップデータ：

- kickstartサーバーからのIAP設定、SSL証明書、SSOキーなどについての、各種設定ファイルは、ローカルでバックアップされます（標準バックアップ）。kickstartサーバーからのIAP設定ファイルは、コンバータースクリプトが実行されるとき、ローカルでPCCにバックアップされます。設定ファイルは、フルバックアップおよび増分バックアップ方式を使用してテープ（オプションのバックアップシステム）にバックアップすることもできます。
- データベースデータは、ローカルでバックアップされます。DB2データベースのローカルバックアップは、プラットフォームのローカルディスク上に毎日作成されます。ローカルバックアップのコピーは、安全強化のためにデータベースサーバーとkickstartサーバーで保存されます。データベースのデータファイルも、フルバックアップおよび増分バックアップ方式を使用してテープ（オプションのバックアップシステム）にバックアップできます。
- スマートセルデータ：このデータは、フルバックアップおよび増分バックアップ方式を使用してテープ（オプションのバックアップシステム）にバックアップできます。内容のインデックスもテープにバックアップされます。

バックアップの各ページを開くには、左メニューで [Data Management] > [Backup] に移動します。

Data Protectorを実行するオプションのバックアップシステムについて詳しくは、「オプションのバックアップシステム」（135ページ）を参照してください。

[Backup]の[Overview]ページ

[Backup]の[Overview]ページは、設定、データベース、およびスマートセルデータに関するバックアップのステータス情報を掲載しています。また、オプションのバックアップサーバーが装備されている場合は、このページからテープバックアップを無効にすることや有効にしてスケジュールに合わせて実行することができます。

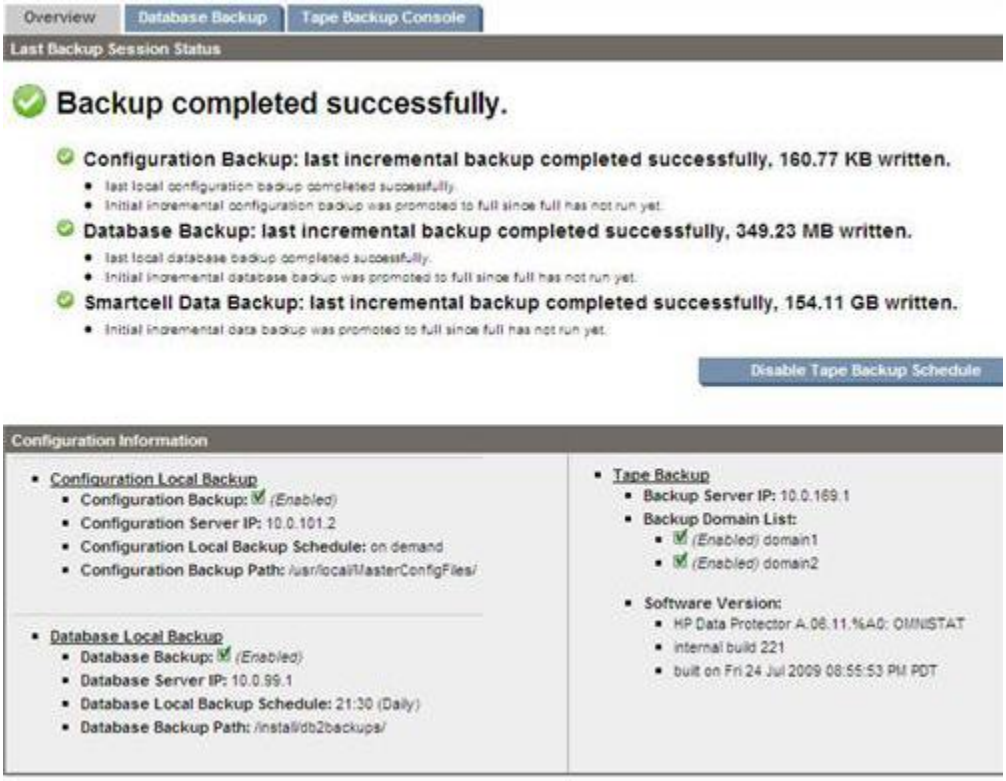


図28 [Backup]の[Overview]タブ

バックアップサービス全体のまとめ

バックアップサービスの全体的なまとめは、ページ上部に表示されます。

チェックマークのアイコンは、バックアップサービスが正常に完了したことを示します。このステータスは、3つのデータセットの最新のバックアップがすべてエラーなしで正常に完了した場合に表示されます。

感嘆符(!)のアイコンは、バックアップサービスは完了したが警告が発生していることを示します。このステータスは、3つのデータセットの最新のバックアップがすべて完了したが完了した少なくとも1つのバックアップで警告が生成された場合に表示されます。

X印のアイコンは、バックアップサービスの失敗を示します。このステータスは、3つのデータセットのいずれかで最新のバックアップが失敗した場合に表示されます。

情報アイコン は、バックアップサービスについての情報が提供されていることを示します。このステータスは、エラーが発生していない状況で表示されます。バックアップサービスを最初にセットアップするとき、情報アイコンはバックアップセッションがまだ一度も実行されていないことを示します。

個々のバックアップサービスの概要

[Backup]の[Overview]ページには、各データセット（設定、データベース、およびスマートセル）のバックアップステータスも表示されます。

成功を示すチェックアイコン は、最近28日間でフルバックアップ、最近24時間で増分バックアップがそれぞれ少なくとも1回行われた場合に表示されます。これらの間隔はデフォルト値であり、カスタマイズできます。上記の条件が満たされていない場合は、警告アイコン またはエラーアイコン が表示されます。完了した最後のフルバックアップまたは増分バックアップで警告が生成された場合は、警告が表示されます。最後のバックアップが失敗した場合や完了したがエラーが発生した場合、あるいは最後のフル

バックアップの実行後28日を経過している場合、最後の増分バックアップの実行後24時間を経過している場合は、エラーが表示されます。

情報アイコン は、そのバックアップタイプで提供されているバックアップサービス情報を示します。このステータスは、エラーが発生していない状況で表示されます（バックアップサービスを最初にセットアップするとき、情報アイコンはバックアップセッションがまだ一度も実行されていないことを示します）。

また、次の状況が発生した場合にもユーザーに通知が行われます。

- そのバックアップタイプでバックアップスケジュールが有効または無効になった。
- 現在実行中のバックアップセッションがありそのステータス（存在する場合）が存在する。
- 最後にフルバックアップが行われてから一定の期間（デフォルトでは、28日）が経過した。
- 最後に増分バックアップが行われてから一定の期間（デフォルトでは、1日）が経過した。

設定タイプおよびデータベースデータタイプ（これらのタイプにはIAP上で実行されたローカルバックアップがあります）については、最後のバックアップセッションのステータスに関する情報が箇条書きで示されます。

設定データのバックアップステータス

PCC、HTTPポータル、kickstartサーバーなど、各サーバーにはバックアップの対象になる設定データがあります。これらのサーバーは、バックアップクライアントと呼ばれます。

チェックアイコンは、すべてのバックアップクライアントで設定データの最新のバックアップが決められた日付（増分バックアップの場合は1日前、フルバックアップの場合は28日前）より後に行われ、エラーを伴うことなく正常に完了している場合に表示されます。

感嘆符（!）のアイコンは、すべてのバックアップクライアントで設定データの最新のバックアップが完了しているが、一部のバックアップクライアントで最後の増分バックアップの実行後2日を経過している（たとえば、「Last completed incremental backup on kickstart is older than 1 day」）場合に表示されます。

Xのアイコンは、いずれかのクライアントで最後の設定データのフルバックアップ後28日が経過している（たとえば、「Last completed full backup on PCC is older than 28 days」）かまたはいずれかのバックアップクライアントでバックアップのステータスが見つからない（たとえば、「No backup found on backup server”」）場合に表示されます。

データベースデータのバックアップステータス

IAPのローカルディスク（kickstartおよびデータベースサーバー）で上でバックアップされたデータベースデータも、テープバックアップが有効であれば、テープにバックアップされます。テープにバックアップされるデータベースデータは、kickstartサーバーに常駐します。

チェックアイコンは、データベースデータの最新のローカルバックアップとテープバックアップがエラーを伴うことなく正常に完了し、最後のテープバックアップが決められた日付（増分バックアップの場合は1日前、フルバックアップの場合は28日前）より後に行われている場合に表示されます。

感嘆符（!）のアイコンは、データベースデータの最後のバックアップが完了しているが、ローカルデータベースのバックアップで警告が発生している（たとえば、「Local backup 1 completed with warnings」）か、または最後の増分バックアップ後1日が経過している（たとえば、「Last completed incremental backup on kickstart is older than 1 day」）場合に表示されます。

Xのアイコンは、最後のフルテープバックアップ後28日が経過している（たとえば、「Last completed full backup on kickstart is older than 28 days」）場合や、テープバックアップのステータスが見つからない（たとえば、「No backup found on tape」）場合、ローカルバックアップのステータスが見つからない（たとえば、「No backup found on DB2 server」）場合に表示されます。

テープバックアップが無効の場合、テープへのデータベースバックアップのステータスは、ダッシュボードに表示されません。

スマートセルデータのバックアップステータス

バックアップされるスマートセルデータは、割り当てられたスマートセルに常駐します。これらのスマートセルもバックアップクライアントです。スマートセルバックアップクライアントの名前は、*gid*、スマートセルが所属するグループのID、およびIAPのドメイン名で構成されます。

チェックアイコンは、割り当てられたすべてのスマートセルでデータの最後のバックアップが決められた日付（増分バックアップの場合は1日前、フルバックアップの場合は28日前）より後に行われ、エラーを伴うことなく正常に完了している場合に表示されます。

感嘆符（!）のアイコンは、割り当てられたすべてのスマートセルでデータの最後のバックアップが完了しているが、一部のスマートセルで最後の増分バックアップ後1日が経過している（たとえば、「Last completed incremental backup on gidxxx1 is older than 1 day」）場合に表示されます。

Xのアイコンは、割り当てられているスマートセルのいずれかで最後のフルバックアップ後28日が経過している（たとえば、「Last completed full backup on PCC is older than 28 days」）場合かまたはいずれかの割り当て済みスマートセルでバックアップのステータスが見つからない（たとえば、「No backup found on gidxxx1」）場合に表示されます。

テープバックアップが無効な場合、スマートセルデータのバックアップはダッシュボードに表示されません。

テープバックアップスケジュールの無効化/有効化

テープバックアップ機能は、[Backup]の[Overview]ページで設定します。このページには、スケジュール設定されたテープバックアップの無効と有効を切り替えるためのボタンが表示されます。テープバックアップのスケジュールが無効になっている場合は、テープバックアップは発生しません。以前にバックアップされたテープ上のデータが消去されることはありません。テープバックアップのスケジュールが無効になると、3つのバックアップタイプの下にそれぞれ丸い記号が表示され、バックアップが無効になっていることを示します。

[Configuration Information]

[Backup]の[Overview]ページの下の部分には、ローカルバックアップおよびテープバックアップの設定情報が表示されます。

[Configuration Information]領域には、設定サーバーおよびデータベースサーバーの内部IAP IPアドレス、ローカルバックアッププロセスの実行時間スケジュール、およびローカルバックアップファイルの位置が示されます。

[Configuration Information]領域には、バックアップサーバーの内部IAP IPアドレス、使用されているData Protectorバックアップソフトウェアのバージョン、およびテープバックアップが有効になっているIAPドメインのリストも表示されます。

注記：

テープバックアップが無効になっている場合は、このセクションには「Tape Backup is disabled」と表示されます。テープバックアップが有効なのにバックアップサーバーを利用できない場合は、[Backup Server IP]セクションに「Backup application Server is down, cannot retrieve information」と表示されます。

データベースバックアップ

IAPのローカルディスク（kickstartおよびデータベースサーバー）で上でバックアップされたデータベースデータも、テープバックアップが有効であれば、テープにバックアップされます。[Database Backup]ページには、最新の2つのローカルバックアップ（1つはローカルデータベースサーバー上、もう1つはkickstartサー

バー上）の詳細情報が表示されます。このページには、データベースデータのテープ（オプションのバックアップサーバー）への最新のフルバックアップと増分バックアップの詳細情報も表示されます。この情報には、完了までの時間、サイズ、タイプ(フルまたは増分)といった情報、ならびに情報メッセージが含まれます。

ローカルデータベースバックアップの[Last Database Backup]テーブルのエントリーには、データベースバックアップジョブに関する情報が含まれます。このジョブによりDB2データベースから情報が抽出され、復元可能な形式で保存されます。

PCCには、データベースバックアッププロセス自体の統計情報も表示されます。特に、[Completion Time]列には、データベースからの抽出プロセスが完了した時刻が表示されます。ジョブに関する他のログに、その後完了するローカルバックアップジョブについての情報が表示されることがあります。情報にはプロセスの後半で追加されるタイムスタンプも含まれますが、これにはデータベースバックアップのアーカイブのためのディスクストレージスペースの管理という余分なタスクにかかった時間が含まれます。これは、厳密にはデータベースバックアッププロセスには当たりません。

バックアップデータのリカバリにどれくらいの時間がかかるのかをそのデータの抽出にかかった時間から判断できる状況では、[Local Completion Time]をバックアップに含まれているデータの確認に利用すると便利です。

Tape Backup Console（テープバックアップコンソール）

[Tape Backup Console]ページからは、HP Data Protectorのグラフィカルユーザーインターフェイス（GUI）にVNCアクセスできます。このソフトウェアは、オプションのバックアップサーバー上で稼動します。オプションのバックアップサーバーの詳細なステータス情報や設定を確認するには、HP Data Protector GUIを使用してください。

ローカルバックアップファイルの位置

`install/config/primary`ディレクトリの内容は、バックアップされます。

- データベースバックアップファイル：データベースバックアップファイルとDB2トランザクションログファイルは、データベースサーバー（パーティション`/db2/VolBack`）に保存されます。ファイルは、kickstartサーバー上のディレクトリ（`/install/db2backups`）へミラーリングされます。DB2データベースは、1日に1回バックアップされ、最新の2つのバックアップファイルがディスクに残されます。
- マスター設定ファイル：kickstartサーバーには、`BlackBoxConfig.jcml`、`Domain.jcml`、および`UserKeyStore`という3つのマスター設定ファイルが`/install/configs/primary`ディレクトリにあります。コンバーターとRegistry Loaderが動作しているときにこれらのファイルのいずれかが変更されると、変更されたファイルは、PCCマシンの`/usr/local/MasterConfigFiles`ディレクトリにコピーされます。
  （設定ファイルを変更した後でRegistryLoaderを実行するには、kickstartサーバーで`regloader.pl -cv`スクリプトを実行します）。

> **注記：**
>
> `BlackBoxConfig.bct`ファイルは、`BlackBoxConfig.jcml`（`/install/tools/converter/dumpBCT`）から生成できるため、ローカルバックアップに含まれません。`createBBC.zr`スクリプトは、バックアップされる`.jcml`バージョンを生成します。

DB2ローカルバックアップファイルからのリストア

DB2データベースは、データベースサーバーの/db2/VolBackパーティションにあるバックアップファイルからリストアできます。データベースマシンを再インストールしたためにデータが失われたときは、最初にバックアップファイルをリストアします。kickstartサーバー上のコピー、またはテープバックアップ（アプリケーションバックアップが有効の場合）から、バックアップファイルをリストアします。

データベースバックアップパーティションとデータベース自体をリストアする機能は、データベースサーバー上の/opt/bin/backup/db2BackupUtilityスクリプトに実装されています。詳細な使用に関する情報を取得するには、引数のないコマンドを実行します。

データベースをリストアするには、以下の手順に従います。

1. データベースをリストアする前に、PCCサーバーで/opt/bin/stopを実行して、すべてのIAPアプリケーションを停止します。
2. データベースシステムにログオンします。
3. データベースサーバーを再インストールした場合は、次のコマンドを実行して、kickstartサーバーに保存されたバージョンから/db2/VolBackパーティションをリストアします。

   ```
   /opt/bin/backup/db2BackupUtility -restore_from_kickstart
   ```

   注記：

   VolBackディレクトリの内容が削除されます。

4. データベースをリストアするには、次のコマンドを実行して、データベースが稼動していることを確認します。

   ```
   su - db2udb -c db2start
   ```

5. DB2をリストアするには、次のコマンドを実行します。リストアするバックアップのタイムスタンプを求められます。

   ```
   /opt/bin/backup/db2BackupUtility -restore_db2
   ```

   通常、データベースの最後の2つのバックアップが、保存されています。

6. インストールが完了したら、PCCサーバーで/opt/bin/startを実行してIAPを起動し、正常に動作していることを確認します。

マスター設定ファイルのリストア

マスター設定ファイルのコピーは、PCCサーバーの/usr/local/MasterConfigFilesディレクトリに保存されます。コンバーターが動作しているときにkickstartサーバーでいずれかのファイルが変更されると、マスター設定ファイルがPCCサーバーにコピーされ、ファイル名がYYYY-MM-DD-hh.mm.ss_FileNameに変更されます。

Restoring a Smartcell group(スマートセルグループのリストア)

[Restore Smartcell Group]ページには、テープからリストアできる壊れたグループ、リストア中のグループ（進行状況の情報を含む）、および完了したリストア操作や中断されたリストア操作の情報が表示されます。

グループのスマートセルのいずれかを失った場合は、[Smartcell Cloning]ページを使用してスマートセルのクローンを作成してグループを再編成します。クローンの作成はテープからのリストアよりはるかに高速です。また、正常なスマートセルがテープバックアップ上にはない最新データを格納していることがあります。

グループ内の両方のスマートセルが失われた場合は、[Restore Smartcell Group]ページを使用して一方のスマートセルをテープからリストアします。テープから一方のスマートセルをリストアしたら、クローン操作を使用してもう一方のスマートセルを取得し、グループを再編成します。

注記:

テープからのリストアが必要なのは、クローン作成が不可能な場合だけです。スマートセルのクローン作成はテープからのリストアよりも高速なだけでなく、データが完全であることも保証します。テープ上のデータは最後にバックアップが行われた瞬間は最新データですがそれを過ぎると古いデータになります。

[Restore Smartcell Group]ページを開くには、左メニューで [Data Management] > [Restore Smartcell Group] に移動します。

[Smartcell Group Restore candidates]

[Smartcell Group Restore candidates]セクションは、テープからリストアできる壊れたグループが1つ以上あるときに[Restore Smartcell Group]ページに表示されます。ここには、プライマリスマートセルとセカンダリスマートセルの両方を利用できないグループだけが表示されます。グループ内の一方のスマートセルだけをリストアする必要がある場合は、グループの復元にはクローン作成の方がよく使われます。

グループの各エントリーで、ドメイン名、グループID、および(入手できる場合)はプライマリスマートセルやセカンダリスマートセルのIPアドレスが示されます。

[Start Restore]ボタンをクリックすると、指定したグループのテープリストアが開始されます。ボタンをクリックした時点で、指定したグループのテープリストアが開始され、現在のリストアジョブのリストに操作を示すエントリーが現れます。

[Current Smartcell Group Restore Jobs]

[Current Smartcell Group Restore Jobs]セクションには、実行中または失敗したリストアジョブとその現在の進行状況が表示されます。各エントリーは、次の情報を提供します。

表25 [Current Smartcell Group Restore Jobs]の情報

フィールド	説明
Group ID	テープからリストアするグループのグループID。
Status	Running(実行中)またはFailed(失敗)。
Smartcell IP	データのリストア先になるスマートセルのIPアドレス。このフィールドには、空きスマートセルがリストア対象として割り当てられた時点でデータが埋め込まれます。
Started	この操作が開始された日時。
Completed Step	現在実行中のリストアステップについての情報。
Action	ジョブの制御に使用できる1つまたは複数の操作。

実行できる操作は次のとおりです。

- リセット

スマートセルが割り当てられるとただちに実行できます。この操作により現在のジョブが中止され、リストアターゲットとして割り当てられたスマートセルがリセットされます。リストアされた可能性のあるすべてのデータがすでに削除されており、セルは空きスマートセルのプールに戻されます。

- 再試行

  現在のステップが失敗した場合にだけ利用できます。この操作により、リストア操作が再開され、最後に失敗したステップから再び操作が試みられます。

- クローン

  スマートセルが完全にリストアされ、クローン作成の準備ができている場合にのみ利用できます。この操作を選択すると、PCCの[Cloning]ページが表示され、このスマートセルのリストア操作に「完了」のマークが付けられます。

構成済みスマートセルの登録解除

IAPで構成済みのスマートセルを何らかの理由で「キックスタートし直す」必要がある場合は、[Tape Backup Console]でスマートセルの登録を解除してリストアで使えるようにします（これがIAPに追加された新しいスマートセルの場合、この手順は不要です）。

スマートセルの登録を解除するには、以下の手順に従います。

1. IAP PCC UIの[Backup]ページのタブを使用して[Tape Backup Console]を開きます。
2. [Tape Backup Console]からVNCでバックアップサーバーへ接続し、[File] > [Connect to Cell Manager]をクリックしてHP Data Protector Cell Managerに接続します。接続するプライマリバックアップサーバーを選択します。接続が済んでいる場合は、接続ステップは省略できます。
3. 接続が完了したら、[Clients]ドロップダウンセクションからスマートセルのホスト名を選択します。右クリックして、[Delete]を選択します。次の図では、削除対象として選択されているスマートセルはsc-s1-172-1.persistcorp.comです。

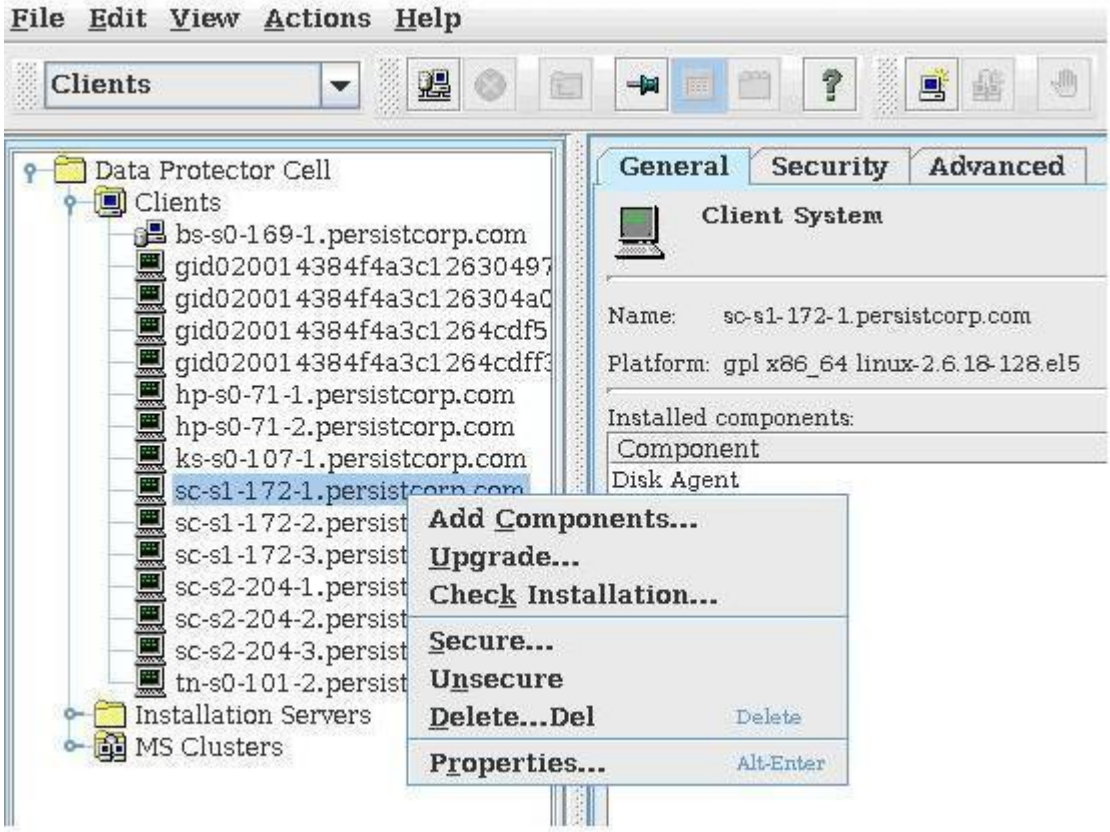


図29 スマートセルの登録解除

4. Data Protectorソフトウェアを削除するかどうかを尋ねられたら、[No]をクリックします。このステップが終了すると、スマートセルはいつでも「キックスタートし直し」てリストアに利用できます。

smartcell cloning（スマートセルのクローン作成）

現在および過去のクローン操作のステータスを表示し、スマートセルのクローンを作成するには、[Smartcell Cloning]ページを使用します。

ページを開くには、左メニューで [Data Management] > [Smartcell Cloning] に移動します。

クローン作成の概要

ミラースマートセルがSUSPENDED、DEAD、またはFAILEDの場合、スマートセルのクローンを作成できます（「スマートセルのライフサイクル状態」（38ページ）を参照）。スマートセルのクローンを作成すると、すべての情報がFREE状態にある別のスマートセルにコピーされ、そのスマートセルは、新しい実行可能なミラーになります。クローンされる情報量によっては、クローン操作に長時間（1日）がかかる場合があります。

ソーススマートセルを空きプールに入れる方法については、HPの認定サポート担当者に問い合わせてください。

[Cloning]ページにアクセスすると、PCCは、進行中のクローン操作を検索し、現在のデータをロードします。一度に1つのスマートセルしかクローンを作成できないので、進行中のクローン操作の進行状況が表示されます。

[Cloning]ページの機能

表26 [Cloning]ページの機能

機能	説明
Source	実行可能なミラーのないスマートセルのIPアドレス。すべてのスマートセルに実行可能なミラーがある場合、[Source]に[No Broken Groups Found]が表示されます。複数のスマートセルにミラーが必要な場合は、自動的に選択されるIPアドレスの下に[Change Source]ボタンが表示されます。
Free Cells	現在FREE状態にあるスマートセルの数。この数は、クローン操作が開始した後で1つ減ります。
Assigned/Free	割り当てられたスマートセルと空きスマートセルのグラフィカル表現。
Clone Cell	クローン操作を開始します（「スマートセルのクローン作成（データのコピー）」（114ページ）を参照）。
Cloning Area	この領域は、進行中のクローン操作に関する以下の情報を提供します。 ・ Source selected: 複製されているスマートセルのIPアドレス。 ・ Target selected: 重複するデータを受信するスマートセルのIPアドレス。 ・ Current Step Percentage: 複製されたデータ量を示す棒グラフ。 ・ Overall Percentage: クローン操作の現在の段階。 クローン操作の段階は、次のとおりです。 ・ 初期化中 ・ ターゲットホストを割り当て中 ・ データを転送中 ・ インデックスを転送中 ・ インデクサーの完了を待機中 ・ 履歴ログを更新中 ・ 完了または失敗 一部の段階は非常に短時間であるため、ユーザーには認識できない場合があります。 クローンを作成するデータが大量の場合、「データを転送中」や「インデックスを転送中」のような段階で時間がかかる場合があります。
History Logs Table	起動以降の各クローン操作に関する以下の情報。 ・ Source ・ Target ・ Time Elapsed ・ Status ・ Date

スマートセルのクローン作成（データのコピー）

スマートセルのクローンを作成するには、以下の手順に従います。

1. 次のどちらかの操作を実行します。
   - [Source]フィールドからスマートセルを選択します。
   - オプションが存在する場合は、[Change Source]をクリックして、クローンを作成する別のスマートセルを選択します。選択ボックスが表示されたら、ドロップダウンリストからスマートセルを選択し、[Select]をクリックします。
2. [Clone Cell]をクリックします。

   クローンを作成するスマートセルがない場合、このボタンは使用できません。

   クローン操作が正常終了すると、PCCにポップアップパネルが表示されます。
3. [Status]領域で、クローン操作の結果を確認します。

   チェックアイコンは、クローン操作が正常に進行していることを示します。

   クローン操作が失敗すると、Xアイコンが表示されます。

フォルダーの取得のサポート

IAP 2.xは、Email Archiving software for Exchange（HP EAs Exchange）バージョン2.xを対象にフォルダーの取得をサポートします。

この機能は、アーカイブされたメッセージに対する元のOutlook上の場所を取得し、IAP内の対応する文書を更新します。フォルダーの場所（例：`/Inbox/project`）は、アーカイブされた電子メールにメタデータとして保存されます。

フォルダーの取得を機能させるには、IAPとHP EAs Exchangeの両方で有効にする必要があります。HP EAs Exchangeでは、フォルダーの取得はデフォルトで有効にされています。IAPのデフォルト設定では、この機能は無効になっており、`Domain.jcml`で有効にする必要があります。

フォルダー情報のインデックスを作成すると、IAPに保存されているメッセージをフォルダー名で検索して取得できます。フォルダー情報が追加されたときにインデックスを付け直すアーカイブメッセージの数を制限するには、`Domain.jcml`で期限日を指定します。期限日以前に保存されたメッセージは、メタデータだけが更新されますが、期限日以後に保存されたメッセージは、メタデータとインデックスの両方がフォルダー情報を使って更新されます。

注記：

IAPにCLOSED状態のスマートセルがいくつか含まれる場合、インデックス化されたフォルダー情報を追加すると、空きディスク容量がただちに枯渇する可能性があります。

このエラーを防止するために、期限日をシステムのアップグレードを行う日に設定して、新しいメッセージに対してのみインデックスが作成されるようにすることを強くお勧めします。

フォルダーサポートの詳細については、『HP Email Archiving software for Microsoft Exchange Version 2.x管理者ガイド』の「フォルダの取得の使用」の章を参照してください。

フォルダーの取得の有効化

`Domain.jcml`のFolderSupportEnabledオプションは、IAP内のドメインでフォルダーサポートが有効かどうかを示します。このオプションが有効の場合、IAPでは、このドメインから電子メールをフォルダー単位で検索して、電子メールが保存されているフォルダーを表示できます。フォルダーサポートを有効にするには、このオプションをtrueに設定する必要があります。`FolderSupportEnabled=true`

`Domain.jcml`を設定した後、kickstartサーバーで`regloader.pl -cv -clearallConfirm=<IAP name>`コマンドの実行および、PCCで`/opt/bin/restart`コマンドを実行してIAPを再起動してください。

フォルダーサポートが有効かどうかは、PCCの[ドメインの設定]に表示されます。

日付には、IAP 2.xのインストールまたはアップグレードの日付を使用します（例：07/30/2008）。

Administrative Delete

Administrative Delete機能を使用すると、指定されたユーザーがアーカイブに保存されている電子メールを手動で削除できます。この機能は、通常、たとえば、誤って配布されたメッセージをアーカイブから削除するなど、行政分野で機密扱いのデータを処理するのに使用されます。電子メールは、規制、非規制、および隔離レポジトリから手動で削除できます。

重要：

Administrative Deleteを使用することが組織の記録保管ポリシーに抵触しないことを確認するのは、お客様の責任です。この機能の無責任な使用については、HPは責任を負いかねます。HPは、システムからデータが意図せず削除されることを防ぐ正しい制御とロギングを実現することに努めてきました。

Administrative Deleteの有効化

Administrative Deleteは、ドメインレベルで有効化または無効化できます。有効な場合は、適切な権限のあるユーザーは電子メールを削除することができます。

1. 次の操作を行い、`Domain.jcml`ファイルを開きます。
   a. コンソールで、Ctrl キーを2回押します。表示されるメニューで、01（on IAP 2.1 hardware）をダブルクリックして、kickstartサーバーを選択します。
   b. プロンプトで、以下のように入力します。

      ```
      cd /install/configs/primary
      ```

   c. テキストエディターで、`Domain.jcml`を開きます。

      例：

      ```
      vi Domain.jcml
      ```

2. `[AdminDeleteEnabled]`フィールドをtrueに設定して、Administrative Deleteを有効にします。

   ```
   AdminDeleteEnabled=true
   ```

   ファイルにこのフィールドがない場合は、追加します。

   注記：

   Administrative Deleteを有効にする場合は、「AuditLogの有効化」（133ページ）の説明に従って、AuditLogも有効にする必要があります。

   （Administrative Deleteは、`AdminDeleteEnabled`フィールドを`false`に設定することで無効にできます。）

3. ファイルを保存して閉じます。

4. 次のコマンドを入力し、RegistryLoaderを実行します。

   ```
   regloader.pl –cv –clearallConfirm= <BlackBoxName>
   ```

   プロンプトでYESを入力して確認を行います。

5. RegistryLoaderが完了したら、PCCに移動します。コンソールで、Ctrl キーを2回押します。表示されるメニューで、02（on IAP 2.1 hardware）をダブルクリックして、PCC NATを選択します。

6. 次のコマンドを使用して、PCCからIAPを再起動します。

   ```
   # /opt/bin/restart
   ```

7. PCC Web管理にログインします。

   [General Configuration]の[Platform Settings]ページに、Admin Deleteサービスが有効であることが表示されます。

Delete Admin権限の付与

すべてのIAP Adminユーザーには、スーパーユーザーを除き、Delete Administration権限を付与したり剥奪したりすることができます。リモートユーザー（Active Directoryに存在し、DASによってインポートされたユーザー）に対してのみ、Delete Administration権限を付与することができます。

この権限をユーザーに付与するには、以下の手順に従います。

1. PCCにスーパーユーザーとしてログインします。
2. PCCの[Account Management]ページを開き、IAP Admin権限をユーザーに付与します。
3. PCCにこのIAP Adminユーザーとしてログインし、PCCの[Account Management]ページを開きます。
4. Administrative Deleteを実行する必要のあるユーザーを選択し、[Delete Admin]チェックボックスを選択してこのユーザーを編集します

   このユーザーが所属するドメインでAdministrative Deleteを有効にする必要があります。そうしないと、[Delete Admin]チェックボックスが表示されません。

5. 変更した内容を保存します。

Admin Delete権限を剥奪するには、以下の手順に従います。

1. PCCにリモートIAP Adminユーザーにログインします。
2. PCCの[Account Management]ページを開き、Administrative Delete権限のあるユーザーを選択し、[Delete Admin]チェックボックスを選択解除してこのユーザーを編集します。
3. 変更した内容を保存します。

Administrative Deleteの実行

Delete Admin権限を取得したら、ユーザーはIAPに格納されたあらゆるメッセージを削除することができるようになります。メッセージを削除するには、以下の手順に従ってください。

1. IAPのWebインターフェイスに、Delete Admin権限のあるユーザーとしてログインします。
2. 削除するメッセージを検索して選択します。
3. [追加オプション]をクリックします。
4. [削除 チェック項目]を選択します。
5. 削除を確認するには、[削除の確認]をクリックします。

6. 削除を確認したら、削除の実行が成功したか失敗したかについてのレポートを含むステータスページが表示されます。

   メッセージの削除が申し込まれた後で、メッセージがインデックスから削除されるまで最長で2時間かかります。その間は、メッセージの内容は検索可能ですが、取得することはできません。

Administrative Deleteによってメッセージが削除されると、次のようになります。

- 削除は、メッセージとそのメッセージへのすべての参照をIAPから物理的に除去します。
- メッセージが隔離されている場合は、削除されます。
- [保存した結果]のメッセージは、インデックスから削除されメッセージの本文は検索できなくなりますが、ただし、メッセージは[保存した結果]のリストに残ります。
- プライマリおよびセカンダリスマートセルの両方で、削除が完了します。IAPが複製環境で動作している場合は、メッセージは複製スマートセルでも削除されます。
- IAPが複製環境で動作している場合は、Administrative Deleteはプライマリ IAPに格納されたメッセージを削除するためだけに実行することができます。削除は複製環境プロセスによって複製IAP上でトリガーされます。Administrative Deleteは、複製IAPに格納されたメッセージを直接削除することはできません。

AuditLogへの記録

Administrative DeleteでのアクティビティはAuditLogに記録され、AuditLogレポジトリに保存されます。

- ユーザーがDelete Admin権限を取得したり喪失したりした場合は、その変更内容はAuditLogに記録されます。
- Administrative Deleteによってメッセージが削除されると、その動作はAuditLogに記録されます。

現時点での限界

次に、Administrative Deleteの現時点での限界を示します。

- IAP 2.xでは、Administrative Deleteは電子メールのみを削除します。Object Store API(BIBO)またはHP File Archiving software(旧名、FMA)で保存されている文書は削除しません。また、監査証跡も削除しません。
- IAPバックアップ機能によって電子メールがバックアップされている場合は、電子メールはAdministrative Deleteを使用してIAPから削除することができます。しかし、テープ上の電子メールおよび関連情報は削除されません。そのため、スマートセルのリカバリが実行されたときに、すべてのadministrative delete動作を再実行しなければなりません(こういった場合は、そう頻繁には起こりません)。AuditLogによって、どの削除動作を再実行しなければならないかを知るために必要な情報を得ることができます。
- このとき、Webインターフェイスで保存された結果を再ロードすると、保存されたクエリ結果内の削除されたメッセージが表示されます。しかし、削除されたメッセージをクリックすると、`Error displaying message`が表示されます。保存されたクエリは、保存されたクエリがクリーンアップされるまで、ファイルへの参照を保管します。
- この機能は、DoDまたはNSAのデータ破壊基準を満たしていません。

9 レポート

この章では、以下の項目について説明します。

Event Viewer（イベントビューアー）

[Event Viewer]には、システムサーバーおよびシステムサービスとアプリケーションで発生中のイベントや発生したイベントが表示されます。

注記：

PCCでは、すべてのアラートがイベントとして記録され、[Event Viewer]ページに他のイベントに混ざって表示されます。「Current Platform Alerts（現在のプラットフォームアラート）」（41ページ）を参照してください。

[Event Viewer]ページは次の2とおりの方法で開くことができます。

- 左メニューで [Reporting] > [Event Viewer] に移動します。
- 左メニューで、[Overview]を選択し、[Current Platform Alerts]で[Go to Event Viewer]をクリックします。

[Event Viewer（イベントビューアー）]の概要

Event Viewer（イベントビューアー）には、次の情報が表示されます。

表27 Event Viewer（イベントビューアー）の機能

機能	説明
Description	文章によるイベントの説明。 説明の前に、イベントレベルを示す次の各アイコンが表示されます。 ・ [クリティカル]：システム全体に影響を及ぼす致命的な問題です。 ・ [メジャー]：サーバーまたはアプリケーションの機能に重大な問題が発生していますが、システム全体にとって致命的ではありません。 ・ [マイナー]：サーバーまたはアプリケーションの機能に何らかの内部的な問題が発生していますが、サーバーや機能の状態にとって致命的ではありません。 ・ [Resolved/Manually resolved]：問題は自動的に解決されたかまたはユーザーが解決しました。 ・ [不明]：問題の原因を特定できません。 ・ [情報]：システムの通常の動作の中で発生したイベントです。
Context	イベントが発生した状況。

機能	説明
Machine	イベントが発生したサーバーのタイプとマシンのIPアドレス。
Date	イベントが最初に発生した日時または解決した日時。

Event Viewer（イベントビューアー）での検索

ビューアーの検索領域で指定した検索タイプや基準を満たすイベントだけが表示されるように選択できます。

Event Viewer（イベントビューアー）で検索するには、以下の手順に従います。

1. 各ページに表示するイベントの数を選択します。

   デフォルト値は、ページ当たり20イベントです。

2. ドロップダウンリストで[Search Type]を選択します。

   以下の検索を選択できます。

   - Show All Events（すべてのイベントを表示）
   - Level（イベントのレベル）
   - Machine Type（イベントが発生したマシンのタイプ）
   - IP Address（イベントが発生したマシンのIPアドレス）
   - Host Name（イベントが発生したマシンのホスト名）

3. [Search Criteria]テキストボックスに、検索条件を入力します。

   [Show All Events]を除くすべての検索で、検索条件を入力する必要があります 検索では大文字小文字が区別されません。

   - [Level]を選んだ場合は、[Event Viewer]ページ下部の凡例を参照してください。
   - [Machine Type]タイプを選んだ場合は、たとえば、[Event Viewer]ページの[Machine]列を参照してください。
   - [IP Address]を選んだ場合は、[Event Viewer]ページの[Machine]列や[Software Management]ページを参照してください。
   - [Host Name]を選んだ場合は、[Software Management]ページを参照してください。

   検索機能は、SQLの“Like”データベース機能を使用します。たとえば、[Search Type]で [Host Name]を選び、[Search Criteria]で*sc%*と入力すると、ホスト名sc-s1-172-1.company.comやsc-s2-204-1.company.comを検索できます。*%204%*と入力すると、sc-s2-204-1.company.comやsc-s2-204-2.company.comを検索できます。

   また、解決済みのイベントを検索するには、[Search Type]として [Level]を選択し、[Search Criteria]で*%resolved* を入力します。これにより、解決済みイベントと手動で解決されたイベントが表示されます。

4. [Submit]をクリックします。

イベントの削除

[Event Viewer]ページからのイベントの削除には、いくつかの方法があります。

1. 次のどちらかを選択してください。
   - 1つまたは複数のイベントで、そのイベントの前にあるチェックボックスを選択します。
   - ページ下部にあるドロップダウンリストで期限を選択します（例：発生後2週間を超えたイベント）。
   - ビューアーのすべてのイベントを削除する場合は、ページ下部のドロップダウンリストで[All Events]を選択します。
2. 選択後、[Delete]をクリックします。

注記：

レコードの数が20,000に達すると、システムはイベントを古い順に自動的にクリアします。エントリーの最大数の10%に当たる2,000個のイベントが削除されます。現在、イベントの保管は設定できません。

SNMP Management（SNMPの管理）

IAPシステム内部で発生するアプリケーション生成のアラートは、PCCの[Overview]ページの[Current Platform Alerts]に表示されます。これらのアラートを、ネットワーク内の外部モニターや電子メール受信者にSNMPトラップとし転送することができます。

次の機能を実行するには、[SNMP Management]ページを使用します。

- 監視側の管理サーバーにインポートするIAP MIBファイルをダウンロードする。
- 監視するSNMPトラップを選択する。
- アラートを受信したときに通知する監視サーバーや電子メール受信者を設定する。
- SNMPコミュニティを設定する。
- テストトラップを送信して、構成が正しくセットアップされていることを確認する。

注記：

このページでSNMPトラップとして選択できるのはアプリケーションが生成したアラートだけです。IAPサーバーのハードウェア監視は、Proliantマネジメントエージェントが担当します。詳細については、「ハードウェアの監視」（50ページ）を参照してください。

ページを開くには、左メニューで [Reporting] > [SNMP Management] に移動します。

IAP MIBのダウンロード

HP SIMのような監視アプリケーションは、IAP MIB（管理情報ベース）を使用して、IAPから来るSNMPイベントを認識することができます。

IAP SNMPトラップは、IAPシステムがMIBファイル`iap.mib`の生成に使用する、SNMP XMLファイルに記述されます。生成された`iap.mib`は、SNMPバージョン2を使用しますが、これは転送プロトコルSNMPバージョン1に従う規格です。

システムにIAPソフトウェアの最新バージョンをインストールする場合は、必ず、PCCサーバーから`\opt\mibs\iap.mib`をダウンロードして、ご使用の監視管理ソフトウェアにインポートし、モニターがIAP SNMPトラップを認識できるようにしてください。IAP MIBファイルをローカルマシンにコピーするには、[MIB Manager Service]領域で[ダウンロード]をクリックします。

監視サーバーにMIBをインポートするには、監視管理ソフトウェアのドキュメントを参照してください。

SNMPトラップの選択

[SNMP Trap Manager Service]領域で、監視するSNMPトラップを選択します。アラートのいずれかが生成されると、対応するトラップが[SNMP Management]ページで入力したSNMP監視サーバーや電子メール受信者に送信されます。

SNMPトラップを設定するには、以下の手順に従います。

1. トラップをアクティブにするシステムを選択します。

   これは常にIAPです。

2. 送信するトラップを選択します。

   トラップは、機能別にグループ分けされます。すべてのトラップを有効にすることも、機能別に有効にすることもできます。また、個々のトラップを有効にすることもできます。

   アラートIDに対応するトラップIDは、「IAPアプリケーション生成アラート」(163ページ)に示されています。

3. 完了したら[Save]をクリックします。

SNMPサーバーの設定

[SNMP Trap Server Monitors]領域で、SNMPトラップの送信先にするサーバーのIPアドレスを入力して[Add]をクリックします。

SNMP情報は複数のサーバーまたは受信者にブロードキャストできるため、複数のIPアドレスを入力することができます。

注記:

必ず、サーバーのホスト名ではなく、IPアドレスを入力してください。

HP SIMサーバーを、SNMP受信者として使用できます。システムは、SIMサーバーに準拠するために、SNMPプロトコルバージョン1を使用します。すべてのSNMP受信者がこのバージョンと互換性を持つ必要があります。

サーバーエントリーの前にあるラジオボタンをクリックし、[Toggle Enabled/Disabled]をクリックすると、サーバーの使用を有効または無効にすることができます。

サーバーエントリーの前にあるラジオボタンをクリックし、[Delete]をクリックすると、リストからサーバーを削除することができます。

SNMPトラップ監視サーバーがない場合は、電子メールでSNMPイベント通知を受信することができます(電子メールでのSNMPイベントの送信を参照)。

電子メールでのSNMPイベントの送信

SNMPトラップ監視サーバーがない場合は、電子メールでSNMP通知を受信することができます。また、このオプションは、オフィスから離れている場合に便利です。

サービスを有効にするには、通知を受信する人の電子メールアドレスを入力し、[Add]をクリックします。

さらに受信者を追加する場合は、この手順を繰り返します。

電子メール受信者の有効と無効を切り替えるには、個人名の前にあるラジオボタンをクリックして[Toggle Enabled/Disabled]をクリックします。

電子メール受信者を削除するには、個人名の前にあるラジオボタンをクリックして[Delete]をクリックします。

重要:

SNMP電子メール通知を送信するには、[Email Reporter]ページでメールホストのIPアドレスを入力する必要があります。詳細については、「電子メールレポートの作成とスケジューリング」(123ページ)を参照してください。

SNMPコミュニティの設定

SNMPコミュニティ文字列は、パスワードとして機能するテキスト文字列です。管理ステーション(SNMPマネージャー)とデバイス(SNMPエージェント)間で送信されるメッセージを認証するために使用されます。コミュニティ文字列は、SNMPマネージャーとSNMPエージェント間で送信されるすべてのパケットに含まれます。

SNMPコミュニティ文字列は、デフォルトではPublicに設定されています。

構成のテスト

設定の構成または更新が完了したら、[Send Test Trap]をクリックして構成が正しくセットアップされたかどうかを確認できます。

Email Reporter(電子メールレポーター)

選択した電子メール受信者へ定期的に送信される概要監視レポートを設定するには、Email Reporter(電子メールレポーター)を使用します。

送信する情報とレポートの頻度(1回だけ～7日おき)を選択することができます。これらのレポートには、PCCの各ページからシステム ステータス、保存率、ノード状態、およびその他の情報を入れることができます。

ページを開くには、左メニューで [Reporting] > [Email Reporter] に移動します。

電子メールレポートの作成とスケジューリング

電子メールレポートを作成してスケジュールを設定するには、以下の手順に従います。

1. 初めて電子メールレポートを使用する場合は、[Mail Configuration]の各フィールドで設定を行います。
   a. メールホストのIPアドレスを入力します。
   b. レポートの送信者の電子メールアドレス(例:IAPAdmin@mycompany.com、iap-no-reply@mycompany.com)を入力します。これは、実在の電子メールアドレスでなくてもかまいません。
   c. [Save]をクリックして、メール設定を保存します。

2. [Generate Report With]で、以下のいずれかを選択します。
   - すべての情報を送信する場合は[All Contents]、選択する場合は[Custom Contents]を選択します。

   注記:

   HPテクニカルサポートへ電子メールを送信するときは、必ず、[All Contents]を使用してください。

   -

レポート対象	レポートの抽出元
[Alerts]	[Overview] > [Current Platform Alerts]
[Archive Gateway (EAs Exchange only)]	[Archive Gateway Management] > [Overview Archive Gateway]
[Auto Delete Statistics]	[Data Management] > [Retention Information] > [Auto Delete Statistics]
[Backup]	[Data Management] > [Backup]
[DAS Statistics]	[User Management] > [Account Synchronization] > [DAS Available Job(s)]
[Domain Settings]	[General Configuration] > [Platform Settings]
[Node Health]	[Software Management]
[Platform Performance]	[Overview] > [Platform Performance]
[Smartcell Metrics]	[Overview] > [Platform Statistics]
[Version]	[Software Version]

3. [Send to Recipient(s)]テキストボックスに、1つ以上の電子メールアドレスを入力します。

   ボックスに複数の電子メールアドレスを入力するときは、スペース、コンマ、またはセミコロンで区切ります。たとえば、次のように入力してください。recipient1@mycompany.com,recipient2@mycompany.com.
4. [Frequency]リストで、レポートを送信する頻度を選択します。

   選択できる頻度には、「1回のみ」や「1週間に1回」があります。
5. [Schedule]をクリックします。

ページの[Current Active Schedules]領域には、頻度を「1回のみ」に設定した場合を除き電子メールレポート情報が表示されます。好きなときに[Send Now]をクリックすると、予定した時間を待たなくても定義済みレポートのコピーをただちに受け取ることができます。

受信者を削除するには、受信者の電子メールアドレスの前にあるラジオボタンを選択して[Delete]をクリックします。

ログファイルの収集

[Collect Log Files]ページでは、システムの稼動時のイベントやエラーを説明するログを収集できます。これらのログは、特定のサーバーから収集することもIAPのすべてのサーバーから収集することもできます。

たとえば、HTTPサーバーからログを収集しそのログを電子メールでHPのサポート技術者に送信してトラブルシューティングに役立てることができます。

ログの記録レベルは、INFO（システムの正常な動作についての通知を収集するため）に設定することも、DEBUGまたはTRACE（詳しい情報を収集するためや稼動時のエラーの診断に役立てるため）に切り替えることもできます。この切り替えはHPのサポート技術者が、Archive Gateway（ゲートウェイサーバーでのエラーを記録するため）上またはPCCのサービスツール（他のシステムサーバーでのエラー記録するため）を使用して行います。HPサポートの指示で、ログ記録のレベルの変更を要請されることもあります。

[Collect Log Files]ページを開くには、左メニューで [Reporting] > [Collect Log Files] に移動します。

ログの収集

ログファイルを収集するには、以下の手順に従います。

1. ログの収集元にするサーバーのタイプを選びます。

   以下のいずれかを選択できます。

   - SMARTCELL servers
   - META servers
   - DB server
   - SMTP servers
   - HTTP servers
   - SMTP and HTTP servers
   - PCC server
   - ARCHIVEGATEWAY servers (Exchange only)
   - BACKUP servers
   - All Servers (except Exchange ARCHIVEGATEWAY)

2. 次のいずれかの方法を選択して、ログの収集方法を決定します。

   - [Download log file] ログをダウンロードして.tarファイルに格納する。
   - [Email Logs to]ログを電子メールで送信する。

     [Email Logs]フィールドに、受信者の電子メールアドレスを入力します。複数の電子メールアドレスに送信する場合は、アドレスをスペース、コンマ、またはセミコロンで区切ります。

     ログを電子メールで送信するには、kickstartサーバー上の`BlackBoxConfig.bct`のnms-mail-relayを正しく設定する必要があります。

     注記:

     ログのサイズが非常に大きくなることがあります。お客様の環境の添付ファイルのサイズに関する電子メールサーバーの規則によっては、電子メールが通過しないことがあります。電子メールが受信者に正しく送られたかどうかを確認するためのチェックは行われません。

   - [FTP Logs] ログをFTPで送信する。

     [Destination Host]、[Username]、[Password]、[Destination Directory]および、必要に応じて[Encryption Password]を入力します。HPのサポートエンジニアがログを開けるように、パスワードを知らせておく必要があります。

注記:

ログファイルは、Archive Gatewayからのログの場合は.zip形式、それ以外のシステムサーバーからのログの場合は.tgz形式で圧縮されます。ログをダウンロードする場合は、.zipまたは.tgzファイルが.tarファイルに格納されます。

3. [Run Now]をクリックします。

10 外部アクセス

PCCの左メニューには、[Archive Gateway Management]セクションがあります。[Archive Gateway Management]セクションには、各EAs for Exchangeドメインに対するArchive Gatewayステータスの概要へのリンク、およびArchive GatewayにアクセスするVNCアクセスへのリンクがあります。

Archive Gateway Management（Archive Gatewayの管理）

[Overview Archive Gateway]ページについては、「[Overview Archive Gateway]」（128ページ）を参照してください。

ページを開くには、左メニューで [Archive Gateway Management] に移動します。

VNC Archive Gateway

EAs for Exchangeドメインに対するArchive Gatewayにアクセスするには、以下の手順に従ってください。

1. 左メニューで、[Archive Gateway Management]に移動し、[VNC Archive Gateway]リンクを選択します。

   [VNC Viewer: Connection Details]ダイアログボックスが表示されます。

2. [OK]をクリックします。

   [VNC Authentication]ダイアログボックスが表示されます。

3. HPのサポート窓口から提供されたパスワードを入力し、[Enter]キーを押します Enter。

   Windowsの[ようこそ]画面が表示されます。

4. VNCビューアーにマウスポインターを置き、F8キーを押します。表示されるメニューで[Send Ctrl-Alt-Del]を選択して、Windowsのログイン画面を表示します。

   また、[Shift]+[Ctrl]+[Alt]+[Delete] または [AltGr]+[Delete]を押して、Windowsのログイン画面を呼び出すこともできます。

5. HPから提供されたパスワードを使用して、VNCにログインします。

> **注記：**
>
> 重要! [Ctrl]+[Alt]+[Delete]は使用しないでください。PCCからVNCにログインするとき、このキーの組み合わせは動作しません。

[Overview Archive Gateway]

このページは、サービスのステータスや状態など、各ドメインのAarchive Gatewayシステムに関する情報を提供します。

表28 [Overview Archive Gateway]ページの機能

機能	説明
Header	ヘッダーは、Archive Gatewayの名前（たとえば、EM-S0-110-1）および電子メールアーカイブソフトウェアのバージョン（たとえば、1.05.0000）を表示します。
Statistics Collected	統計情報が収集された日時（たとえば、5/11/2009 2:10:17 PM）。
Sections	概要にある各セクションは、Archive Gateway内部の主な領域とその領域の全体的なヘルスステータスを説明します。セクションには、以下に関する情報が表示されます。 ・ システムサービス ・ 設定されたタスク ・ ジャーナルマイニング ・ セレクティブアーカイブ ・ 同期化された削除された項目 ・ Tombstoneのメンテナンス 無効になっているアイコンが表示される場合は、セクションが無効であるか、統計情報が収集されたとき、データが使用できませんでした。

System Services

[System Services]セクションは、Archive Gatewayで動作する特定のシステムサービスの状態を表示します。

表29 [System Services]の機能

機能	説明
Name	サービスの名前。
Status	次の種類のステータスを使用できます。 ・ サービスは動作していますが、サービスアカウントはLocalSystemに設定されていません（VNCサーバーは、そのサービスアカウントがLocalSystemであると予期しています）。 ・ サービスが停止しているか、サービスアカウントがLocalSystemに設定されています（VNCサーバーは、そのサービスアカウントがLocalSystemであると予期しています）。 [Service Information]概要は、サービスが停止しているか、サービスアカウントがLocalSystemに設定されている場合、赤いアイコンを表示します。そうでない場合、概要は緑のアイコンを表示します。
Startup Type	起動の種類は、Auto、Manual、またはDisabledです。
Service Account	サービスアカウントの名前。

Configured Tasks

[Configured Tasks]セクションは、スケジューラーを使用して作成および編集されたタスクに関する設定情報を表示します。

表30 [Configured Tasks]の機能

機能	説明
Task Name	タスクの名前。
Status	次の種類のステータスを使用できます。 ・ タスクは有効になっています。 ・ タスクは無効になっています。 [Task Information]概要は、設定されているすべてのタスクは無効になっている場合、黄色のアイコンを表示します。そうでない場合、概要は緑のアイコンを表示します。
Task Type	セレクティブアーカイブやジャーナルマイニングのようなタスクの種類。
Process Count	ジャーナルマイニングのみ：同時に実行するように設定されたプロセスの数を表示します。
Schedule Frequency	ジャーナルマイニングのみ：同時に実行するように設定されたプロセスの頻度を表示します。

Journal Mining

[Journal Mining]セクションは、マイニングされる各ジャーナルメールボックスに関する情報を表示します。このセクションには、3つの領域（[Exchange Statistics]、[Process Information]、[Message Statistics]）があります。これらの領域のいずれかがマイナーまたはメジャーエラー条件にある場合、4番目のセクションが表示されます。[Processes in Failed or Retry State]という4番目の領域には、エラーになった特定のプロセスに関する情報が含まれています。

表31 [Journal Mining]の機能

機能	説明
Exchange Statistics	・ Connection Status： Exchangeサーバーは稼動中で、電子メールマイナーと通信しています。 Exchangeサーバーとの接続を完了できません。 ・ Exchange Server：ジャーナルメールボックスが存在するExchangeサーバー。 ・ Journal Mailbox Name：マイニングされるジャーナルメールボックスの名前。 ・ Journal Message Count：統計情報が収集されたときのジャーナルメールボックス内のメッセージの数。 ・ Journal Folder Size：統計情報が収集されたときのジャーナルメールボックスのサイズ（KB）。 ・ Failed To Archive Count：統計情報が収集されたときのジャーナルメールボックスのFailedToArchiveフォルダー内のメッセージの数。 ・ Failed To Archive Size：統計情報が収集されたときのジャーナルメールボックスのFailedToArchiveフォルダーのサイズ（KB）。

機能	説明
Process Information	• Status: ジャーナルメールボックス上のジャーナルマイニングプロセスにエラー条件がありません。 ジャーナルマイニングプロセスは、再試行状態にあります。 ジャーナルマイニングプロセスは、障害状態にあります。 • Active: 統計情報が収集されたときに実行されていたジャーナルマイニングプロセスの数。 • Failed: 統計情報が収集されたときに障害状態にあったジャーナルマイニングプロセスの数。 • Retry: 統計情報が収集されたときに再試行状態にあったジャーナルマイニングプロセスの数。 • Completed: 統計情報が収集されたときに処理が完了したジャーナルマイニングプロセスの数。 • Queued: 統計情報が収集されたときに実行待ちだったジャーナルマイニングプロセスの数。
Message Statistics	• Processed: 処理されたメッセージの数。なお、「*processed*」とは、表示される文脈で意味が異なります。 • Submitted: 保存するためにIAPへ送信されたメッセージの数。 • Tombstoned: Exchangeサーバーでスタブに置き換えられたメッセージの数。 • Ignored: 無視されたメッセージの数。なお、「*ignored*」とは、表示される文脈で意味が異なります。 • Rejected: Exchangeサーバーでメッセージが壊れているなど、元のMAPIメッセージに問題があったために拒否されたメッセージの数。 • Average Processing Rate (msg/sec): 平均処理率。
Processes in Failed or Retry State	• Entry: この情報は、障害状態または再試行状態に入ったプロセスを特定する場合に有用です。アイコンが状態を識別します。 マイナーエラーが発生しました。これらのエラーは再試行されます。 メジャーエラーが発生しました。これらのエラーは再試行されません。 • Status: プロセスが障害状態または再試行状態に入ることになった問題。 • Proc: 条件が発生する前に処理されたメッセージの数。 • Tomb: 条件が発生する前に廃棄されたメッセージの数。 • Sub: 条件が発生する前にIAPへ送信されたメッセージの数。 • Rej: 条件が発生する前に拒否されたメッセージの数。 • Ign: 条件が発生する前に無視されたメッセージの数。 • Elapsed: 条件が発生する前に処理にかかった時間(秒)。 • Last Run: 条件が発生した日時。

Selective Archiving

[Selective Archiving]セクションには、ジャーナルマイニングで説明した以下の領域があります。

- Process Information
- Message Statistics
- Processes in Failed Or Retry State

これらの領域の詳細については、「Journal Mining」(129ページ)を参照してください。

Synchronize Deleted Items

[Synchronize Deleted Items]セクションには、「Journal Mining」で説明した以下の領域があります。

- Process Information
- Message Statistics
- Processes in Failed Or Retry State

これらの領域の詳細については、「Journal Mining」(129ページ)を参照してください。

Tombstone Maintenance

[Tombstone Maintenance]セクションには、「Journal Mining」で説明した以下の領域があります。

- Process Information
- Message Statistics
- Processes in Failed Or Retry State

これらの領域の詳細については、「Journal Mining」(129ページ)を参照してください。

11 AuditLogの有効化

AuditLogは、コンプライアンスプロセスに準拠していることを証明するために必要な会社用の監視システムログを提供します。AuditLogには、次のタイプのアクションの詳細が記録されます。

- 電子メールの検索、ファイルのダウンロード、メッセージの表示など、ユーザーがWebインターフェイスから実行したアクション。
- IAPから電子メールを手動で削除するために行われたアクション。記録されるアクションには、IAPのPlatform Control Center(PCC)からのユーザーへのAdministrative Delete権限の付与、WebインターフェイスでのAdministrative Delete機能を使用した電子メールのIAPからの削除などが含まれます。
- IAPのDuplicate Managerで重複する電子メールコピーをマージするために実行されたアクション。

記録されるアクションの詳細なリストはIAPユーザーガイドの「AuditLogの検索」に掲載されています。ここには、AuditLogレポジトリのクエリ実行についての情報も掲載されています。

この章では、AuditLog機能の有効化、保管期間の設定、ステータスの監視、およびレポジトリへのユーザーアクセスの許可の方法について説明します。

AuditLog機能の有効化

AuditLog機能は、ドメインごとに有効化されます。ドメインに対してAuditLog機能を有効にするには、AuditLog機能を有効にする必要があるドメインごとに`/install/configs/primary/Domain.jcml`ファイルに次の属性を追加してください。

- `AuditLogEnabled=true`
- `domainLog_IP=<VIP for this domain>`

  IAPが複製されたサイトの一部である場合は、domainLog_IP属性の値はプライマリサイトのVIPでなければなりません。
- `DocClass=email,windoc`

AuditLogレポジトリへのユーザーアクセスの許可

デフォルトでは、AuditLogレポジトリにユーザーはアクセスできません。規格準拠担当者やその他のユーザーにアクセスを許可するには、以下の手順に従います。

1. PCC(Platform Control Center)にログインします。
2. [Account Manager]ページにアクセスします([User Management]、[Account Manager])。
3. ページ上部の[User]ラジオボタンをクリックします。

4. リストからユーザーの名前を確認します。

   ユーザーは、文字ボタンを使用して検索することも、検索機能を使用して検索することもできます。

   ユーザー名の検索については、「[Account Manager]ページの機能」(72ページ)を参照してください。
5. 表示される[Integrated Archive Platform Account and LDAP Information]フォームで、[Deactivate this check box and then edit the user entries]のチェックボックスをクリアします。
6. [Direct Repositories]ボックス内の任意のエントリーをクリックします。

   ボックスには、ユーザー個人のレポジトリとして少なくとも1つのエントリーがあります。
7. 表示される[Adding Repository Access]フォームで、[Other]タブをクリックします。
8. AuditLogレポジトリのチェックボックスを選択します(例: `<domainname>.userauditlog.repository`)。

> **注記:**
>
> ユーザー個人のレポジトリは、AuditLogレポジトリと同じドメインに所属する必要があります。

9. [Save to List]をクリックします。
10. [Exit]をクリックします。

    レポジトリがユーザーの直接レポジトリに追加されます。

ステータスの監視

PCCの[Platform Settings]ページ([General Configuration] > [Platform Settings])を使用して、特定のドメインでAuditLog機能(AuditLogサービス)が有効かどうかをチェックします。

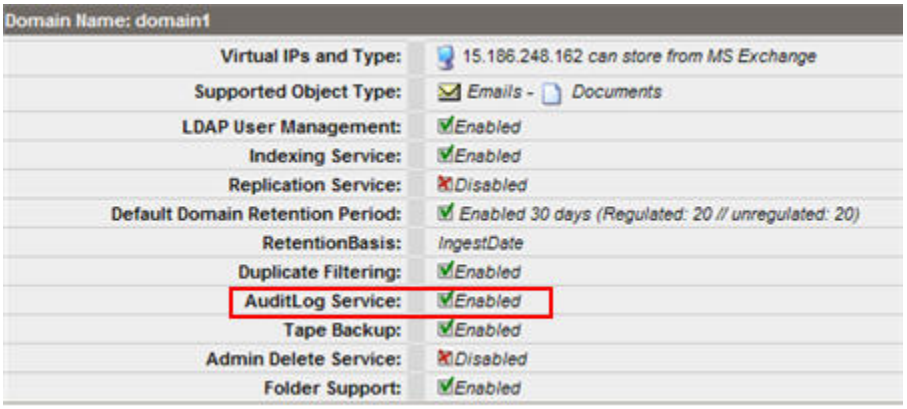


図30 AuditLogが有効

AuditLogレポジトリの保管期間

AuditLogレポジトリのデフォルト保管期間は7年間ですが変更できます。保管期間の変更については、「レポジトリ保管期間の編集」(104ページ)を参照してください。

12 オプションのバックアップシステム

HPでは、IAPの設定、DB2データベース、およびスマートセルデータのテープバックアップを必要とするお客様に、オプションとして、HP Data Protectorバックアップサービスソフトウェアを実行するバックアップシステムを提供します。バックアップシステムオプションの追加（1台以上のバックアップサーバーのIAPへの追加とバックアップシステムの事前設定）はHPの認定担当者がお引き受けできます。担当者は、`BlackBoxConfig.bct`ファイルでハードウェアとアプリケーションのバックアップ（APP）を有効にし、次に示すように`Domain.jcml`のDataBackupEnabledフラグをtrueに設定します。

```
DataBackupEnabled=true
```

設定が正しく行われれば、その後、バックアップサーバーを手動で操作する必要はありません（テープの管理は別です。たとえば、ライブラリには、必ず、十分な量の空きテープを準備してください）。管理者は、テープのスキャンとフォーマットを行う必要があります。フォーマットされたテープはバックアップ以外には使用できません。詳細については、Data Protectorのマニュアルを参照してください。

また、メディアのバックアップサーバーへの接続や単一または増設のバックアップサーバーのデバイス設定も管理者の任務と考えられています。詳細については、Data Protectorのマニュアルを参照してください。

PCCの[Backup]の各ページには、データベース、設定、およびスマートセルデータの全般的なバックアップステータス情報が表示されます。

この章の項目は次のとおりです。

詳細情報とベストプラクティスについては、『Data Protector 6.1 Concepts Guide』（http://www.hp.com/support/manualsで入手可能）およびData Protectorのオンラインヘルプを参照してください。

デフォルト設定

IAPでは、バックアップソリューションとして、Data Protectorが自動でインストールされ、あらかじめ設定されています。この設定には、次の操作が含まれています。

- 接続されているテープライブラリのData Protectorによる自動設定。
- バックアップ仕様へのIAPスマートセル、DB2データベース、および設定データの追加。
- デフォルトバックアップスケジュールのセットアップ

HPの担当者によるバックアップのセットアップが完了すると、接続されたテープライブラリを使用してバックアップが定期的に行われるようになります。ただし、この設定に変更を加え、特定のニーズに合わせたセットアップのカスタマイズやオフサイト保管機能の導入を行っておくと便利です。この章では、Data Protectorを使用してこれらの変更を行う方法について例を用いて説明します。

テープライブラリ

HPのサービス担当者または管理者が[Autoconfigure Devices]オプションを使用して接続されているテープライブラリを自動検出すると、Data Protectorがそのライブラリを自動設定します（このオプションを使用するには、VNCを使用してData Protector UIを開き、[Device & Media]コンテキストを選択し、[Device]を右クリックして、[Autoconfigure Devices]をクリックします。システムのインストール後にテープライブラリを接続するかまたは追加する場合、この手順は管理者が実行できます）。

設定は、Data Protector UIで[Devices & Media]コンテキストを選択すると表示できます。Data Protector UIを開くには、PCCまたはローカルデスクトップからバックアップサーバーへのVNC接続を開始します。

[Devices]セクションを展開すると、ドライブ、ロボット機構パス、およびスロットが表示されます。この例では、テープライブラリに2台のテープドライブといくつかのテープスロットがあり、スロットの一部にはテープが挿入されています。Data Protectorは、テープローテーションのためのその標準アルゴリズムを使用して、テープライブラリで利用できるテープを平等に使用します。

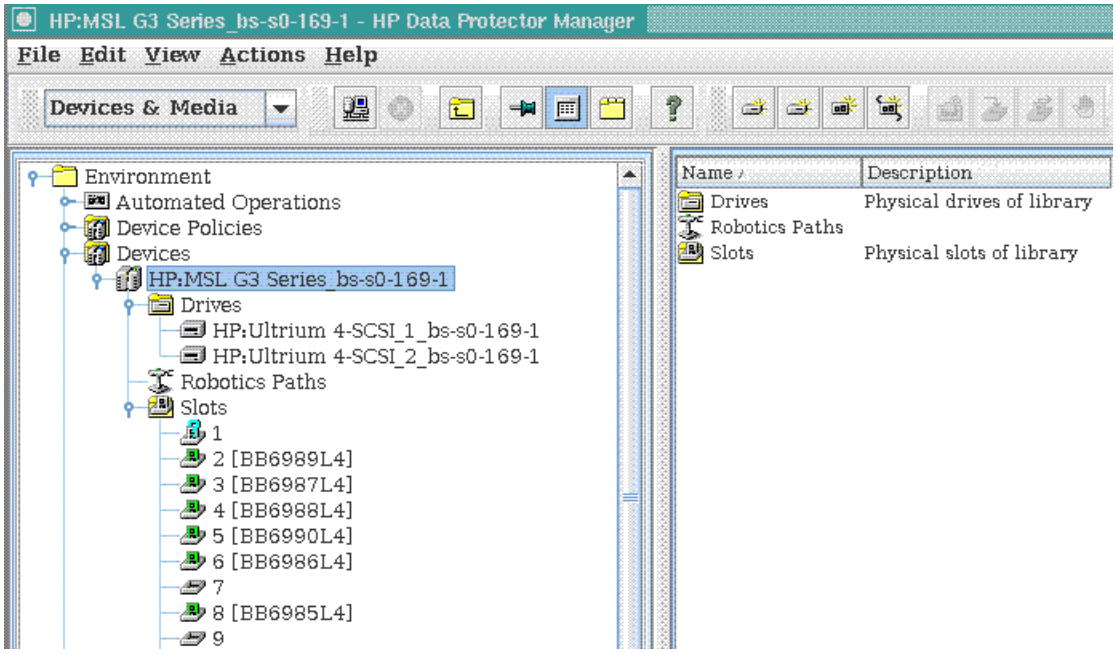


図31 Data Protectorの[Devices & Media]

注記：

バックアップ仕様で、テープライブラリのドライブを指定するには、Data Protectorの[Backup]コンテキストにアクセスし、ツリーを展開して、バックアップ仕様（例：IAP_DATA）を1つ選択します。次に、[Destination]タブを選択して、テープライブラリドライブを選び、[Apply]をクリックします。他のバックアップ仕様（IAP_CONFIGおよびIAP_DB2）でも同じ手順を実行すると、バックアップがスケジュールに基づいて実行されるようになります。

バックアップ仕様とスケジュール設定

auto-configurationは、次の図に示す、データソースを含むバックアップ仕様もセットアップします。バックアップ仕様には、コンテキストドロップダウンボックスで[Backup]を選択するとアクセスできます。左ペインには、IAPを正しくバックアップするのに必要なすべてのバックアップ仕様（IAP_CONFIG、IAP_DATA、およびIAP_DB2）が表示されます。右ペインには、データソース内の各バックアップ仕様のプロパティが表示されます。含まれるスマートセルは、IAPのスマートセルのセットアップが変更されるたびに、自動更新され

ます。ここには、変更を加えないでください。ここで設定の間違いを見つけた場合は、HPに連絡してください。

注記:

IAPの構成が変更され、既存のいくつかのスマートセルグループが削除され、新しいグループが追加された場合、削除された古いグループは、[Tape Backup Console]には登録済みのバックアップクライアントとして表示されます。これらのグループは[Tape Backup Console]では使用できますが、仕様ではバックアップのソースとしては選択されません。有効なグループだけが選択され、バックアップの対象になります。

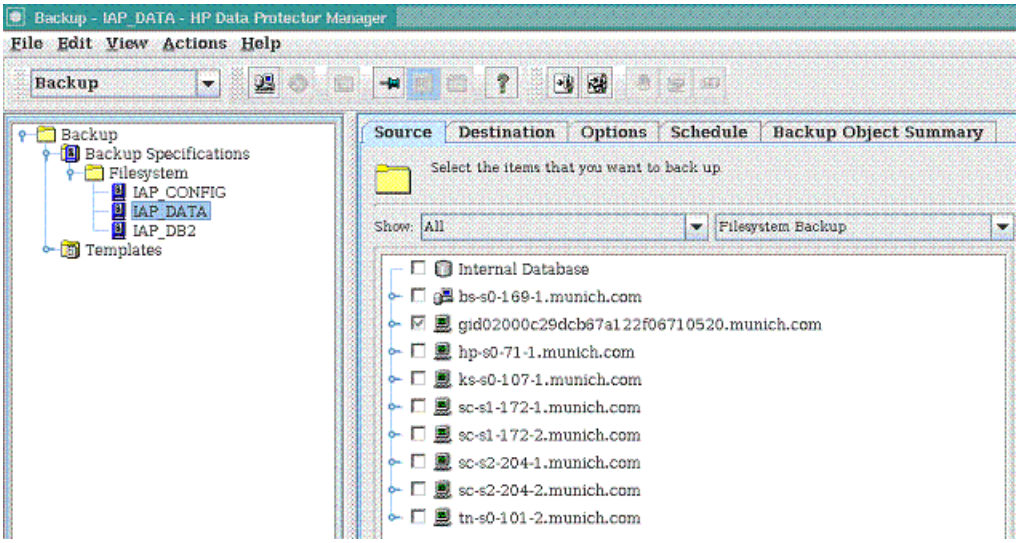


図32 バックアップ仕様とソース

[Schedule]をクリックすると、あらかじめ定義されたスケジュールが表示されます。図から確認できるように、スケジュールはフルバックアップを4週間に1回、増分バックアップを毎日おこなうように自動的にセットアップされます。

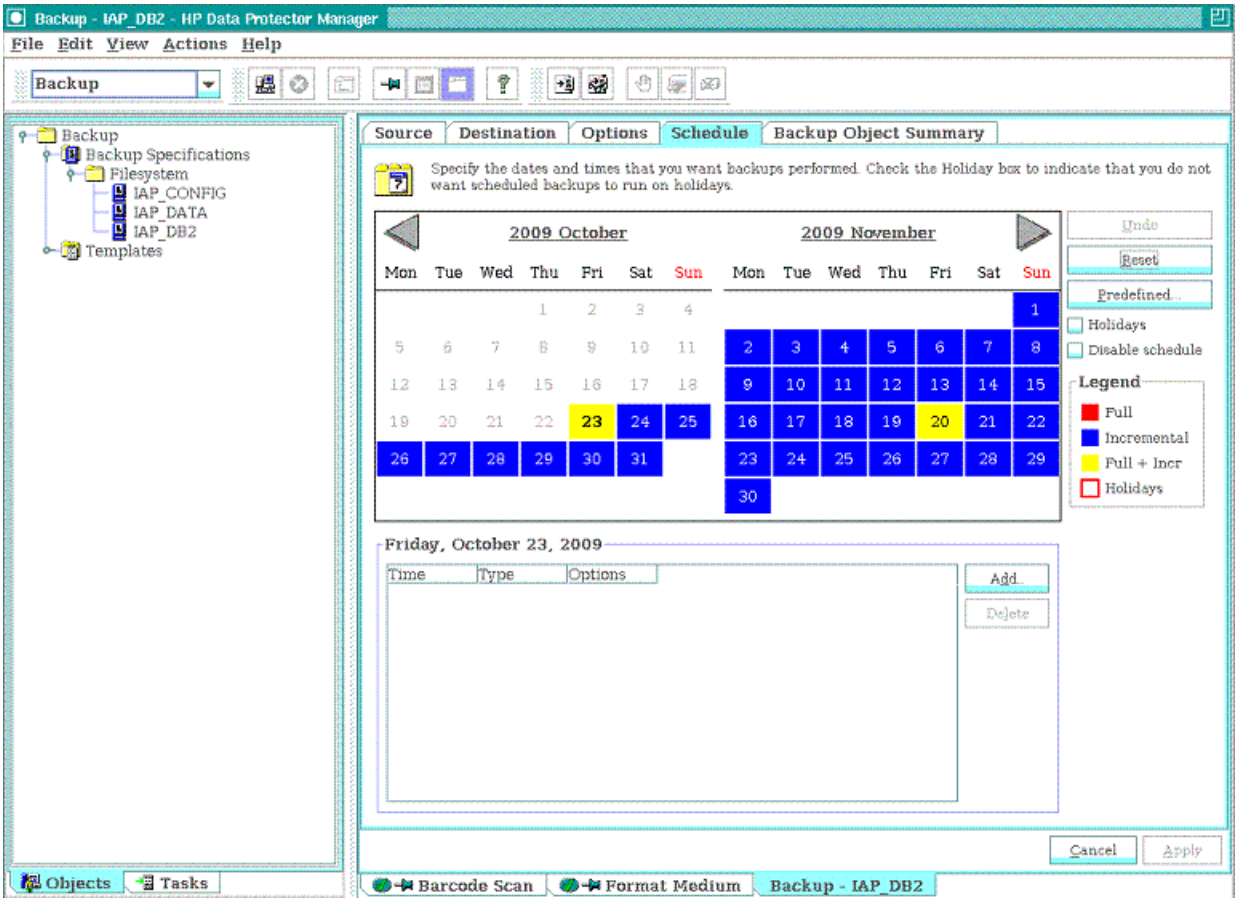


図33 バックアップスケジュール

設定の変更

前の項では、Data Protectorについて説明し、IAPで使用されるデフォルトバックアップ設定についても説明しました。ここでは、このデフォルト設定に手を加えてバックアップ方式をカスタマイズし、フルバックアップを隔週で行い、増分バックアップを毎日行うとするとどのような手順が必要になるのかを説明します。

注記:

オフサイト保管方式(この章の後半で説明します)を使用する場合は、IAP_CONFIG、IAP_DATA、およびIAP_DB2の同じ時点でのフルバックアップを確保しておくのが得策です。

まず、各バックアップ仕様のバックアップスケジュールを変更します。バックアップスケジュールを変更するには、[Schedule]タブを選択し、[Reset]をクリックします。これにより設定済みのすべてのスケジュールが削除されます。次に、[Add]をクリックして、次に示すようにフルバックアップのスケジュールをセットアップします。[OK]をクリックすると、カレンダーの隔週金曜日にすべて赤いマークが付けられます。

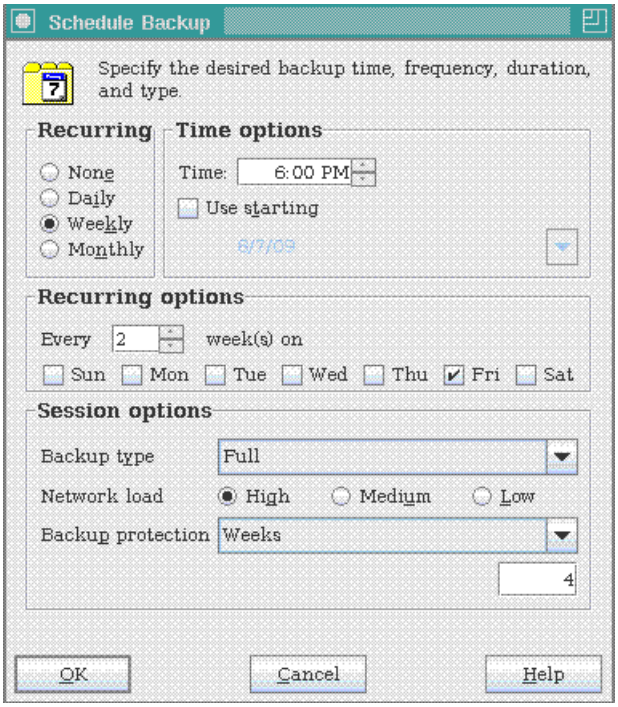


図34 フルバックアップ

次に、増分バックアップについても同じ操作を行います。両方のスケジュールで、[Backup Protection]は、必ず、Weeksに指定してください。これにより、Data Protectorが4週間後テープを再利用できます。

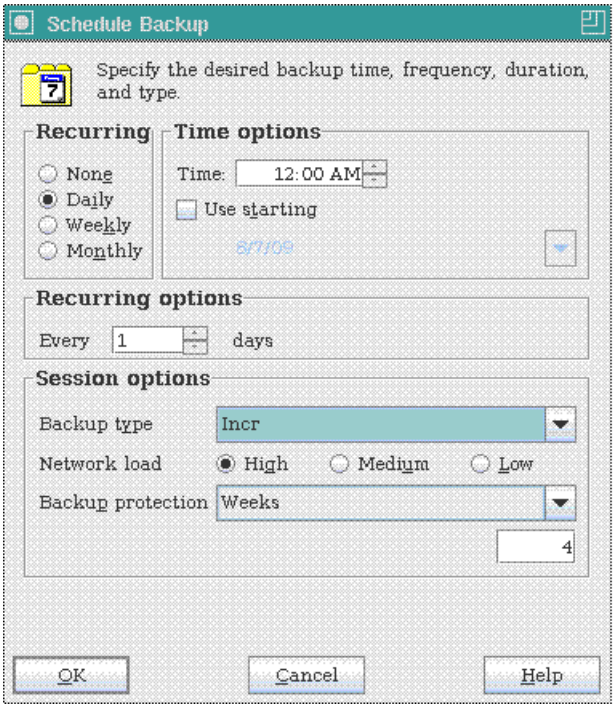


図35 増分バックアップ

変更したバックアップは、設定の変更が完了した時点で機能します。オフサイト保管が必要ない場合は、ここで作業を終了できます。Data Protectorは、利用可能なテープを自動的に使用して保存を行い、お客様のデータを確実に保護します。ただし、何らかのオフサイト保管機能を組み込んでテープセットをオフサイトに保管しておくと安全です。次の項では、その手順について説明します。

オフサイト保管のための操作ワークフロー

データのオフサイト保管には、推奨できるいくつかの方法がありますが、その1つがテープのセットを3つ用意し、そのセットをローテーションするという方法です。つまり、

- 最初のバックアップサイクルで、テープライブラリ内のテープセットに最初のフルバックアップとその後に頻繁に適用される増分バックアップのデータを保存します。
- 最初のバックアップサイクルが終わった時点で、バックアップに使ったテープセットをすべて2番目のテープセットと入れ替えます。1番目のテープセットはオフサイトの位置に移動して保管できます。
- 2回目のバックアップサイクルの完了後に、2番目のテープセットを3番目のセットと入れ替えます。この時点で、2番目のテープセットもオフサイトの位置に移動して保管できます。
- 3回目のバックアップサイクルの完了後、3番目のテープセットを最初のセットと入れ替え、古いバックアップを上書きします。

前の項で説明したサンプルシナリオでは、1サイクルが4週間になります。1つのバックアップサイクルは、常に、フルバックアップで始まり何回（選択可能）かの増分バックアップが続き、新しいフルバックアップが行われる前の最後の増分バックアップで終わります。

データを念には念を入れて保護するために、シナリオを拡大することもできます。テープセットのコピーを作成してそのコピーを1つのオフサイト位置に移動します。そのコピーを、さらに別のオフサイト位置に移動することもできます。

必要なテープ数の予測

IAPにスマートセルペアが1組だけあると仮定します。その場合、バックアップするデータの容量は5TBになります。このため、フルバックアップでは大まかに考えて最大7巻のテープ（LTO-4を想定）が必要になります。それ以外に、1回のバックアップサイクルの間に行われる変更の量に左右されますが、増分バックアップに対応する適切な量のテープも必要です。ここでは、もう1巻必要とします。オフサイト保管のために用意する3つのテープセットでは、24巻のテープが必要です。

同じ条件でLTO-3を使う場合は、2倍の数のテープが必要です。

これは概算であり、使用状況によって増減する可能性があります。1つのセットアップで長年にわたり行われる変更の量もそれぞれ異なります。そのため、ライブラリには常に十分な数のテープを確保しておく必要があります。このように必要なテープの数は条件に左右されますが、大まかな数を一目で掴めるように、次の表に1つのバックアップサイクルで必要なテープの数を示します（オフサイト保管を導入する場合は、3倍のテープが必要です）。

スマートセル	LTO-3テープ	LTO-4テープ
1（5TB）	16	8
2（10TB）	32	16
3（15TB）	48	24

詳細については、『Data Protector Concepts Guide』の第3章「Media management and devices」を参照してください。

テープの交換

最初のテープセットがすでにライブラリにあり、バックアップが有効になっているとします。各バックアップサイクルの完了後、テープの交換作業が必要になります。

1つの完全なバックアップサイクルの終了は、バックアップスケジュールを確認すれば判断できます。バックアップサイクルは、新しいフルバックアップの前の最後の増分バックアップで終わります。

交換作業をしている間に次のフルバックアップが始まることが絶対にないようにしたい場合は、PCCのWebインターフェイスに移動してバックアップスケジュールをすべて無効にします。また、Data Protectorのグラフィカルユーザーインターフェイスを参照してバックアップが進行中でないことも確認します。作業が終了したら、必ず、バックアップスケジュールを有効にしてください。

テープへのラベル付け、テープの取り出し、新しいテープとの交換は、Data Protectorの[Devices & Media]コンテキストで行えます。[Devices]、ご使用のテープライブラリ名、[Slots]ノードの順に移動して、このノードを展開します。ご使用のテープライブラリのすべてのテープが表示されます。

バックアップに使われ取り出す必要があるテープを調べるには、各テープを選択して[Objects]タブをクリックします。このタブをクリックすると、テープに収録されているバックアップオブジェクトが表示されます。バックアップ時間([Start Time]/[End Time])も表示されます。この情報を参照して、テープが現在のバックアップサイクルで使用されたかどうかを判断できます。

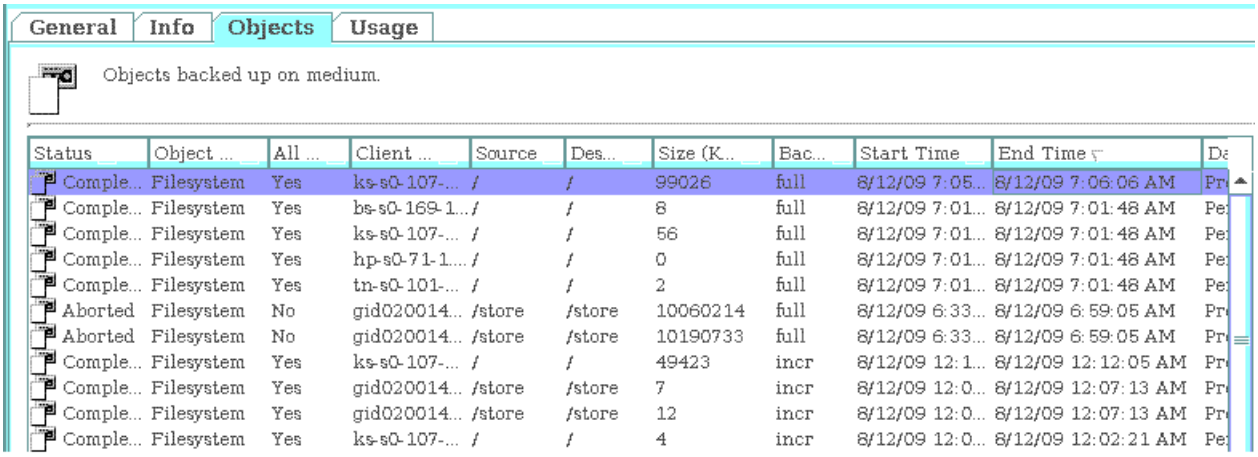


図36 バックアップオブジェクト

注記:

Data Protectorでは、バックアップスケジュールで設定される保管期間が忠実に守られます。つまり、テープ上のバックアップオブジェクトは、その保管期間が過ぎるまでは上書きされることはありません。また、Data Protectorがテープ上にスペースが必要と判断すると自動的にバックアップオブジェクトを削除するため、ユーザーが特定のバックアップオブジェクトを削除する必要はありません。

テープを取り出す前に、以下の手順に従います。

1. Data Protector UIで[Device & Media]、[Device]、[Slots]の順に移動して、オフサイト保管のために取り出す必要があるテープを選択し、右クリックして[Recycle]を選択します。
2. ここでもう一度、テープを選択し、[Export]をクリックします。
3. テープを選択して、[Eject]をクリックします。
4. これによりテープが取り出され、オフサイトの位置に移動して保管できるようになります。

取り出したテープは、すべて次のテープセットのテープと交換する必要があります。

ヒント:

取り出すテープの数が多い場合は、Ctrlキーを押しながらテープを1つずつ選ぶか、またはShiftキーを押しながら範囲全体を選んで一度に選択します。次に、コンテキストメニューを開き、[Eject]を選択します。

Ctrl+Ejectキーを押している間にページが表示され、このページにテープの保管位置を入力できます。複数のテープについては、1か所ずつ位置を尋ねられます。すべてのテープについて位置を入力すると、テープは取り出されます。

重要:

ライブラリパネルから直接テープを取り出さないでください。ライブラリパネルから取り出すと、Data Protectorがテープの移動を追跡できなくなります。バックアップテープの取り出しには、必ず、Data Protectorを使用してください。テープを挿入するには、テープライブラリに入れ、Data Protectorで空きスロットに対して[Enter]を選択します。

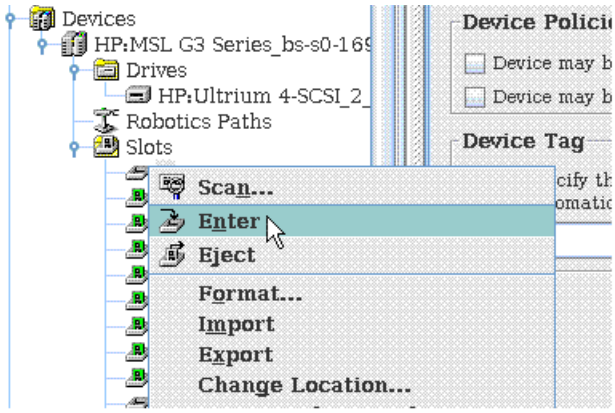


図37 テープの挿入

セットの使用済みテープをすべて新しいテープセットと取り替えたら、取り出したテープセットをオフサイトの位置に移動して保管する必要があります。テープ交換のためにバックアップスケジュールを無効にした場合は、必ず、スケジュールを有効にしてください。以上で、交換作業は完了です。次のバックアップサイクルの完了後、作業を繰り返してください。

保管したテープからのスマートセルグループのリストア

グループ内の両方のスマートセルが消失した場合、最新のバックアップを使用してスマートセルグループをリストアできます（消失したのがグループ内の一方のスマートセルだけの場合は、PCCの[Smartcell Cloning]メニュー機能を使用して失われたスマートセルを復元します）。テープから両方のスマートセルを復元する場合は、PCCの[Data Management]、[Backup]ページに移動して、必ず、バックアップのスケジュール設定を無効にします。

バックアップのスケジュール設定を無効にしたら、Data Protectorコンソールの[Monitor]コンテキストで進行中のバックアップがないことを確認します。たとえば、[Current Sessions]ビューに「No running sessions」と表示されるはずです。

進行中のバックアップがないことを確認したら、テープライブラリから現在あるテープセットを取り出し、スマートセルグループの最新のフルバックアップで生成したテープセットと入れ替えます。

テープがテープライブラリ内にある状態で、Data Protectorコンソールの[Devices & Media]コンテキストを使用してテープのバーコードをスキャンします。テープが別のバックアップサーバーで作成された場合や保管されているテープについての情報がバックアップサーバーのData Protector内部データベース（IDB）で消去されている場合、テープのテープフォーマットは「DataProtector Foreign」または「unknown」と表示されます。スキャンバードコード機能の実行後、このうちいずれかのフォーマットが表示される場合は、テープをハイライトして[Import Catalog]機能を選択します。

メディアをインポートするとメディア上のバックアップデータに関する詳細情報がIDBに書き込まれるので、その情報をブラウズしてリストアを実行できます。メディアのインポート機能は、メディアをData Protectorセル間で移動するときに使用してください。この操作は、空きプール内のメディアには実行できません。メディアの管理について詳しくは、『HP OpenView Storage Data Protector Administrator's Guide』を参照してください。

保管していたテープを挿入したら、以下の手順に従います。

1. デバイスをスキャンします。
2. スロット/テープを右クリックして、[Import]をクリックします。セッションがインポートされます。

注記：

オブジェクト、メディアサイズなど、属性情報は、インポートでは再構築されません。このため、インポートされるオブジェクトのサイズは、「0KB」と表示されます。インポートには、使用するデバイスやメディアによって違いますが、かなりの時間がかかることがあります。

重要：

1つのバックアップセッションで使用されたメディアをすべて同時にインポートします。バックアップセッションで使用したメディアの一部をインポートしなかった場合、他のメディアにまたがっているデータをリストアできなくなります。

カタログのインポートが完了したら、Data Protectorコンソールの[Devices & Media]コンテキストを使用して、正しいテープがマウントされ、そのテープにカタログが作成されているかを確認します。また、[Objects]タブでテープライブラリの各スロットを調べて、1つまたは複数のスロット上のテープにスマートセルグループのデータが収録されていることを確認します。つまり、[Client]見出しの下に、バックアップされたスマートセルグループのgroupid（gid0200...）が表示されるはずです。各テープを観察してテープがロードされていることを確認します。スマートセルグループのIDを探してください。

最新のフルバックアップで生成されたテープをテープライブラリに配置した状態で、PCCの[Restore Smartcell Group]メニュー機能を使用して、スマートセルグループのリストアを開始します。PCCがリストアデータを格納するスマートセルを割り当てると、Data Protectorがテープからデータの読み出しを開始し、新しく割り当てられたスマートセルにリストアします。

リストアプロセスの進行中、このプロセスにより以降の増分バックアップで生成されたテープの追加を要求されることがあります。Data Protectorの[Monitor]コンテキストを使用して、リストアの進行状況を追跡し、Data Protectorから別のメディアのマウント要求が出されたら応じます。マウントメッセージで表示されるデバイスおよびスロット情報に十分注意して、正しいテープを要求されたデバイスおよびスロットに挿入してください。Data Protectorのデバイスおよびメディア管理について詳しくは、Data Protectorのマニュアルを参照してください。

データがすべてリストアされると、PCCはデータリストア後の処理の管理を開始します。この処理では、クローンの作成を開始してリストアプロセスを完了するためにユーザーの操作が求められます。

スマートセルグループ以外でデータが失われた場合のリストア

スマートセルグループ以外でデータが失われたがその情報をバックアップしている場合は、Data Protectorを使用してリストア処理を行います。[Restore]コンテキストに切り替え、[Filesystem]ノードを展開します。リストアするクライアントとバックアップオブジェクトを選択して、[Start restore session]をクリックします。Data Protectorは、必要なテープを自動的に認識します。テープがライブラリにない場合は、Data Protectorからユーザーにそのことが通知されます。テープの位置は、ロケーションラベルで確認します。

IAP設定情報のリストア

テープバックアップシステムは、一部のIAP設定情報をテープに保存します。Data Protectorのバックアップ仕様に当たるIAP_CONFIGには、テープに保存される具体的な情報が定義されています。

IAP_CONFIGバックアップ仕様は、PCC、kickstart、およびバックアップサーバーからの情報を保存します。

- PCCサーバーの情報には、サーバーの証明書やホストキーが含まれます。
- kickstartサーバーの情報には、IAPの構成やArchive Gatewayのバックアップデータが含まれます。
- バックアップサーバーの情報には、バックアップ仕様やスケジュールが含まれます。

設定情報が消失した場合、上書きされた場合、あるいは壊れた場合、テープバックアップから復元できます。情報のリストアは必要な場合にのみ行ってください。というのは、テープ上の情報がサーバー上の情報と比べて古い可能性があるからです。テープバックアップ上の情報は、ディザスタリカバリを目的に保存されており、ほとんどの動作状態では、リストアが必要になることはありません。

IAP_CONFIG情報のリストアには、Data Protectorのグラフィカルユーザーインターフェイスに当たる[Tape Backup Console]を使用します。コンソールを起動するには、以下の手順に従います。

1. IAP PCC UIの[Backup]ページのタブをクリックして、[Tape Backup Console]を開きます。
2. [Tape Backup Console]からVNCでバックアップサーバーへ接続し、次の順に選択してHP Data Protector Cell Managerに接続します。[File] > [Connect to Cell Manager]。接続するプライマリバックアップサーバーを選択します。接続が済んでいる場合、接続ステップは省略できます。
3. 接続が完了すると、Data Protectorの[Restore]コンテキストを使用してリストアする情報を選択できます。情報をリストアするには、マシンを選択し、[Source]タブでテープからリストアするファイルを選択します。次の例では、PCCサーバー（tn-s0-101-2.viap11.com）の証明書とホストキーのファイルがリストアされます。

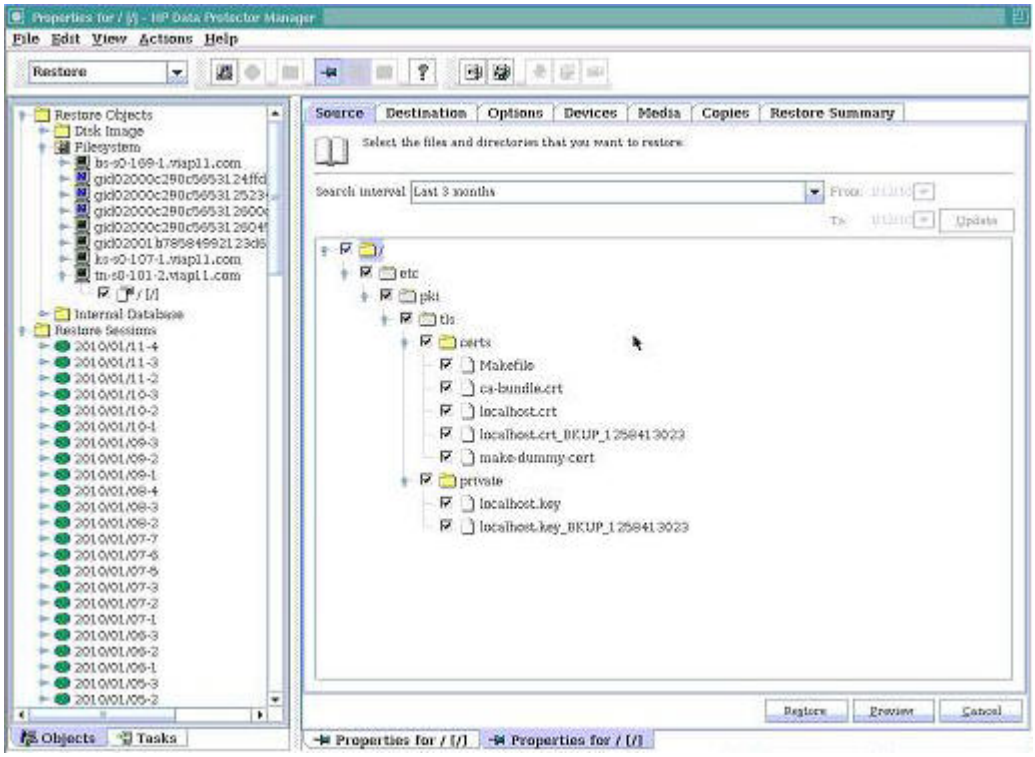


図38 情報のリストア

4. [Destination]タブをクリックして、ファイルが元の位置にリストアされることと最新のファイルが使用されることを確認します。
5. オプションをすべて選択したら、ページ下部にある[Restore]ボタンをクリックします。[Preview]ボタンを使用すると、ファイルを実際に復元先に保存しないで、リストアを行ってみることができます。[Restore]または[Preview]のクリック後、リストアするオブジェクトが複数か単一かの選択を求められることがあります。この質問に答えない場合、手順7に進みます。答える場合は、単一を選択して[Next]をクリックします。
6. ホスト(オブジェクト)の選択を求められたら、必ず、以前(手順3)に選択したホストをドロップダウンボックスから選択します。この例では、PCC(tn-s0-101.2.viap11.com)をリストアします。
7. 提案されるリストアの概要が表示されます。正しい場合は、[Finish]をクリックします。正しくない場合は、[Back]ボタンを使用して前に戻り変更します。[Finish]をクリックすると、Data Protectorリストアセッションとしてリストアが開始され、進行状況を示すメッセージが次々に表示されます。リストアが完了すると、完了メッセージが表示されます。

複数のバックアップサーバーの設定

IAP 2.1では、フルバックアップのサイクルを短縮するために複数のバックアップサーバーを追加できます。データ50TBごとにバックアップサーバーを1台追加することをお勧めします。最大3台のバックアップサーバーがサポートされます。これは、バックアップサーバー1台当たり、2TBスマートセルであれば25グループ、5TBスマートセルであれば10グループを意味します。3台を超えるバックアップサーバーが必要な場合は、複製を使用してください。

追加するバックアップサーバーのインストール方法は、プライマリバックアップサーバーのインストールと同じです。

HP Data Protector Cell Managerは、そのインストール/構成で、プライマリバックアップサーバー(`BlackboxConfig.bct`ファイルで設定される最初のバックアップサーバーで、IPアドレスは、通常10.0.169.1です)からだけ稼動するように設定されます。[Tape Backup Console](Data Protectorのグラフィ

カルユーザーインターフェイス）は、プライマリバックアップサーバー上で動作し、すべてのバックアップ仕様とメディア構成はプライマリバックアップサーバーから設定および制御されます。デフォルトの仕様が提供されていますが、お客様のニーズに合わせてカスタマイズできます。

2台目と3台目のバックアップサーバーは、メディアエージェントとしてのみ機能し、同時にバックアップできるデータの量を増やすための追加バックアップデバイスとして使用されます。これらのバックアップサーバーには、追加のテープデバイスが接続されます。追加したバックアップサーバーにデバイスとメディアを接続したら、追加したバックアップサーバーからのデバイスとしてバックアップデバイスをプライマリバックアップサーバーにインポートできます。デバイスのインポートは、プライマリバックアップサーバー上で稼動する[Tape Backup Console]を使用して行います。

プライマリバックアップサーバーが何らかの理由で停止すると、テープバックアップは実行されなくなります。プライマリバックアップサーバーを起動できる状態に戻せない場合、IAPを再設定して追加したバックアップサーバーのうちのいずれかをプライマリバックアップサーバーとして使用するように設定する必要があります。

IAP 2.1では、プライマリバックアップサーバーの追加バックアップサーバーのいずれかへの自動フェイルオーバーはサポートされていません。構成を変更してプライマリバックアップサーバーを別のサーバーに切り替える場合は、すべてのバックアップサーバーを新たに起動します。

バックアップサーバーの設定を変更するには、`BlackboxConfig.bct`ファイルで、「停止した」バックアップサーバーをコメントアウトするかまたは削除して、すべてのバックアップサーバーを起動します。`regloader.pl -cv`コマンドを、必ず、`Blackbox.bct`ファイルの変更後に実行してください。

追加したバックアップサーバーに接続したデバイスを設定するには、以下の手順に従います。

1. IAP PCC UIの[Backup]ページのタブを使用して[Tape Backup Console]を開きます。
2. [Tape Backup Console]からVNCでバックアップサーバーへ接続し、次の順に選択してHP Data Protector Cell Managerに接続します。[File] > [Connect to Cell Manager]。接続するプライマリバックアップサーバーを選択します。接続が済んでいる場合、接続ステップは省略できます。
3. 接続が完了したら、[Devices & Media]ドロップダウンメニューを使用して追加したバックアップサーバーに接続されているデバイスを設定します。次の図では、bs-s0-169-2.paris.comが2台目のバックアップサーバーです。

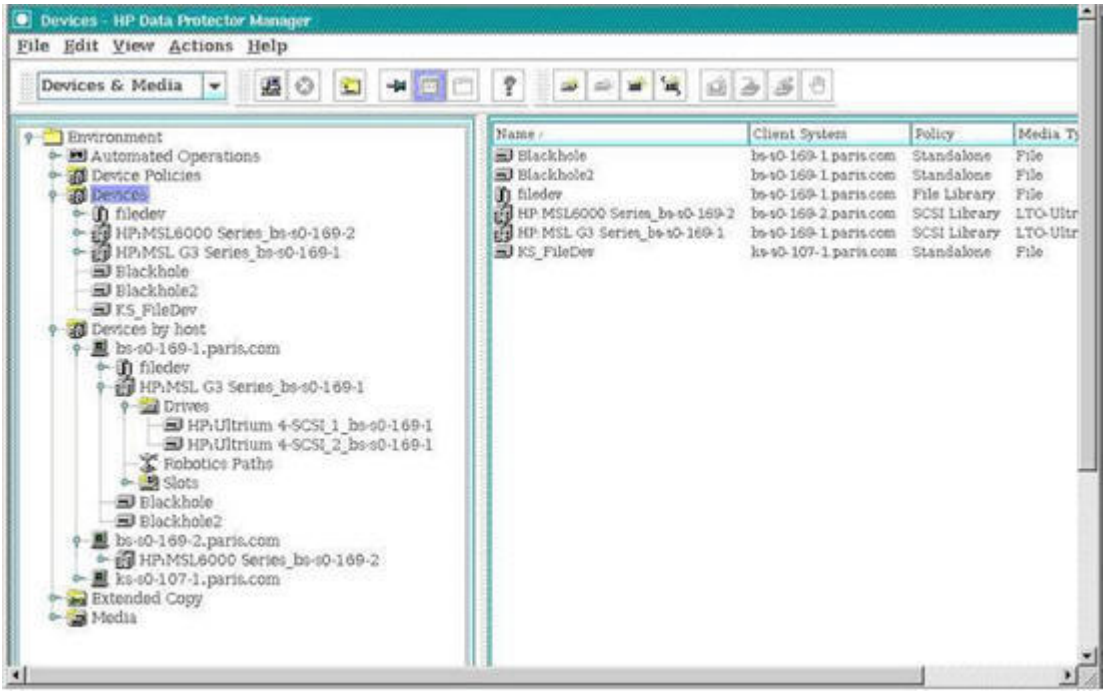


図39 デバイスの設定

4. バックアップデバイスを追加するには、[Devices by host]メニュー項目を右クリックして、ドロップダウンメニューから[Add Device]を選択します。[Client]フィールドで、追加したバックアップサーバーを選択します。すでに説明しているように、この例ではそのサーバーはbs-s0-169-2.paris.comです。
5. デバイスを選択して、デバイスの設定を完了します。
6. 追加したバックアップサーバー上のバックアップデバイスを設定しそのメディアをバックアップに向けて準備したら、Data Protectorの[Backup]コンテキストに移動して[Backup]ドロップダウンメニューでIAP_DATAバックアップ仕様を修正し、新しく設定したこのデバイスをバックアップ先として追加します。
7. バックアップは、スケジュールに基づいて実行され、データは選択されたすべてのメディアに同時にバックアップされます。リストアに必要なテープは、Data Protectorが自動的に識別するため、これ以外のセットアップは不要です。

トラブルシューティング

バックアップサーバーの詳細なステータス情報については、バックアップサーバー上で稼動するData Protectorのグラフィカルユーザーインターフェイス（VNC経由で接続）を参照します。スマートセル、kickstrartサーバー、およびDB2サーバーのバックアップサービスは、最近のイベントのログファイルを保管します。

Data Protectorは、バックアップサーバーのログファイルを保管します。このログファイルは、IAPのログ収集スクリプトにも含まれます。

IAPのバックアップに関わる問題が発生したら、原因がIAP側とData Protector側のどちらにあるかを確認してください。PCCのステータスページとアラートフレームワークを介して送信されたアラートをチェックしてください。たとえば、ライブラリに空きテープがないことを通知するアラートが表示される場合、そのエラーメッセージからData Protector側の問題であることがはっきりとわかります。また、IAP側とData Protector側のログファイルは、問題が元々どちらの側で発生したのかを判断するのに役立ちます。

注記：

現時点では、Data Protectorに1つの制約があります。Data Protectorでは、[Objects]タブでデータがインポートされたことが正しく示されていても、[Devices & Media]の [Usage]タブのテープ/スロットに関する情報で使用率が「0」と表示されることがあります。

13 サーバーのリモート管理

サーバーのリモート管理機能を利用すると、IAPサーバーを、そのサーバーのコンソールの前に実際に座って操作しなくても管理できます。リモート管理機能では、リモート電源管理、リモートコンソールなど、iLOおよびLights-Out 100がサポートする機能を使用できます。IAP内部のすべてのサーバーをiLOまたはLO100を使用してリモートで管理できます。

この章では、HP ProLiant Onboard Administrator Powered by Lights-Out 100またはHP ProLiant Onboard Administrator Powered by Integrated Lights-Out 2を使用したIAPサーバーのリモート管理を監督するために広く行われる作業について説明します。この章では、全体を通じて、HP ProLiant Onboard Administrator Powered by Lights-Out 100またはIntegrated Lights-Out 2を「LO100」、「iLO」、または「リモートプロセッサー」と呼びます。

この章の項目は次のとおりです。

IAPハードウェアのバージョン2.1（DL180 G6、DL360 G6）以降では、出荷時にサーバーにiLO/LO100 Advanced Packのライセンスがインストールされています。以前のハードウェアリリースを所有しているお客様の中でAdvanced Packの機能が必要なお客様は、標準的な販売網を介してライセンスを入手しインストールする必要があります。この章では、Advanced Packライセンスがすでにサーバーにインストールされていることを前提にして説明を進めます。ライセンスは、iLO/LO100のWebインターフェイス経由かまたはコマンドラインツールの`hponcfg`および`lo100cfg`を使用してサーバーにインストールできます。詳細については、次に示すiLO/LO100のユーザーガイドを参照してください。

リモート管理の設定と使用に関する包括的な説明は、HP ProLiant Onboard Administrator Powered by Lights-Out 100またはIntegrated Lights-Out 2の製品マニュアルに掲載されています。

- 『HP ProLiant Lights-Out 100 Remote Management User Guide for HP ProLiant DL140 G2, ML110 G3, and ML150 G2 Servers』(http://bizsupport.austin.hp.com/bc/docs/support/SupportManual/c00857454/c00857454.pdf（英語）
- 『HP ProLiant Onboard Administrator Powered by Lights-Out 100 User Guide for HP ProLiant ML150 G6, DL160 G6, and DL180 G6 Servers』(http://bizsupport1.austin.hp.com/bc/docs/support/SupportManual/c01716486/c01716486.pdf)（英語）
- 『HP Integrated Lights-Out User Guide for HP Integrated Lights-Out firmware 1.91』(http://bizsupport.austin.hp.com/bc/docs/support/SupportManual/c00209014/c00209014.pdf)（英語）
- 『HP Integrated Lights-Out 2 User Guide for Firmware 1.75 and 1.77』(http://bizsupport1.austin.hp.com/bc/docs/support/SupportManual/c00553302/c00553302.pdf)（英語）

リモート管理ソリューションの概要

以下の各項では、IAPのリモート管理ソリューションの概要を紹介します。

目的

IAPのリモート管理ソリューションは、主に、次の目的で使用します。

- お客様が次のいずれかを選択できるようにします。
  - ご使用の管理ネットワーク経由でiLOリモート管理プロセッサーに直接アクセスする。この方法は、使いやすく、1つの機器の障害がシステム全体の障害につながらないため高い可用性を備えます。
  - 各iLOリモート管理プロセッサーにプロキシ経由でアクセスする。この方法は、管理しやすく、より安全です。
- どのタイプのIAPサーバーに対しても、次のことが可能になります。
  - iLOリモート管理プロセッサーへの安全な接続の確立。
  - リモートサーバーの電源の入れ直し、電源のオン/オフ。
  - リモートサーバーのブートシーケンスの監視や操作。
  - サーバー上のローカルメディアまたはISOイメージへのアクセス。これにより、リモートでのファームウェアのアップグレードが可能になります。

ネットワークトポロジ

IAPのリモート管理ネットワークは、iLOリモート管理プロセッサーを物理的にも論理的にも分離した状態で運用されます。管理者は、IAPリモート管理ネットワークをお客様の管理ネットワークに接続する方法として、直接接続とプロキシ経由での接続のうちどちらかを選択できます。直接アクセスでもプロキシ経由でのアクセスでも、PCCのリモート管理プロセッサーは、必ず、お客様の管理ネットワークに接続する必要があります。

直接接続モード

直接接続モードでは、各IAPサーバーのiLOインターフェイスがお客様の管理ネットワークに直接接続されます。IAPのリモート管理ネットワークは自立型のネットワークであるため、お客様のリモート管理ネットワークに直接接続しても誤ってIAPの内部ネットワークが公開され無防備になる危険性はありません。このネットワークトポロジでは、いずれかの専用リモート管理ネットワークスイッチのポートがお客様の管理ネットワークのスイッチにアップリンクされます。接続の完了後、管理者には、IAP内部のリモートプロセッサーへのアクセスを設定して管理する責任があります。たとえば、管理者は、IAP内部の各リモート管理プロセッサーに管理するネットワークのIPアドレスを割り当てる必要があります。特定のIAPサーバーとそのリモート管理プロセッサーのこの関連付けは、たとえば、スプレッドシートを使用して管理者が維持および管理する必要があり、このスプレッドシートをIAPでの物理サーバーの追加や交換のたびに更新しなければなりません。HPでは、セットアップ作業に役立つように、リモート管理プロセッサーのネットワーク設定およびユーザー管理のセットアップに使用できるPCCコマンドを用意しています。このスクリプトと必要な設定手順については、後で説明します。

利点:

- 使いやすい
  - すべてのリモート管理プロセッサーに同時にアクセスできます。
  - お客様のネットワーク管理ソリューションと統合でき、その管理コンソールからアクセスできます。
- 可用性: リモート管理プロセッサーに直接アクセスできるため、IAP内の1つの機器が停止してもネットワーク全体が停止することはありません。

欠点または制約:

- セキュリティ: IAP内部のすべてのサーバーにそのリモート管理プロセッサーを介してアクセスできるため、IAPのファイアウォールが回避されます。
  - このため、IAPサーバーへの不正アクセスが行われる可能性があります。

- 管理者は、IAPのリモート管理プロセッサーへのアクセス権限を持つユーザーだけに限定する責任があります。

- 管理性：各IAPサーバーのIPアドレスがそのリモート管理プロセッサーのIPアドレスに自動でマッピングされることはありません。
  - このため、IAPサーバーIPをリモート管理プロセッサーのIPに手動でマッピングして管理する必要があります。
  - また、このようなマッピングを、IAPのリモート管理プロセッサーにアクセスする必要があるHPのサポート担当者に伝える必要があります。
- お客様のネットワークで、IAP用に余分なIPアドレスが必要になります。IAPサーバーのリモート管理プロセッサーごとに、IPアドレスが1つ必要です。

プロキシモード

プロキシモードでは、すべてのIAPサーバーのiLOインターフェイスが、PCCへの独立したネットワーク経由で接続されます。PCCに搭載される専用NICがIAPリモート管理ネットワークへのゲートウェイの役目を果たします。iLOネットワークへのアクセスは、プロキシとして機能するPCCに追加される別のIPアドレス経由で行われます。IAPは、すべてのiLOとPCCゲートウェイに内部IPアドレスを割り当てます。PCCのiLOは、お客様の管理ネットワークに接続されます。また、UIからのプロキシアクセスには、PCCのIPアドレスと同じネットワーク上の仮想IP（VIP）アドレスが使用されます。

ネットワークは、プロキシによって接続される場合、IAP内部に閉じこめられます。リモートプロセッサーには、アクセスを要求するアクションが起動されない限り、外部からはアクセスできません。このネットワークトポロジでは、PCCまたはPCCのWeb UIで正しく認証されたユーザーは、（1）HPが提供するコマンドを使用してPCCのコマンドラインインターフェイス経由または（2）PCC Web UI経由でリモートプロセッサーへのアクセスを要求する必要があります。IAPのファイアウォールは、リモート管理プロセッサーへのアクセス権限を動的に付与しますが、同時に複数のプロセッサーへのアクセスを許可することはありません。リモートプロセッサーへアクセス要求は、すべて監査ログに記録されます。

利点：

- セキュリティ
  - どのIAPサーバー（PCCを除く）のリモート管理プロセッサーにも直接接続はできません。
  - リモート管理プロセッサーへのプロキシアクセスを有効にするための要求が監査ログに記録されます。
- 管理性

  PCC UIでIAPサーバーのリストが表示され、ユーザーはこのリストで選択したサーバーのリモート管理プロセッサーに透過的にリダイレクトされます。
- お客様のネットワークでIAP用に必要なIPアドレスが直接接続モードの場合より少なくなります。

  このモードでは、PCCのリモート管理プロセッサー用のIPアドレスが1つとユーザーインターフェイスからのプロキシアクセス用のVIPが1つあれば接続が可能になります。

欠点または制約：

- 使いやすさ

  プロキシ経由で一度にアクセスできるリモート管理プロセッサーは1つだけです。
- 可用性：PCCが停止すると、IAPのリモート管理ネットワークに接続できなくなります。
  - 内部のリモート管理プロセッサーへのアクセスはPCC上のプロキシ経由で行います。これを可能にするには、少なくともPCCのオペレーティングシステムとネットワーク機能が稼動していなければなりません。
  - リモート管理へのアクセスはPCCのUIを介して行いますが、リモート管理プロセッサーへのアクセスを可能にするためにJBossが稼動している必要はありません。ユーザーはUIを回避してPCCからiLOへの直接SSH接続を使用できます。

- プロキシは、コマンドラインからiloproxyスクリプトを実行して有効にすることができます。

- PCCには、必ず、ProLiant DL320 G5以降のサーバーを使用します（DL360 G4/G4pには、リモート管理ネットワークをPCCに接続するのに必要なeth2ネットワークインターフェイスがありません）。
- DL140 G2のLO100のWebユーザーインターフェイスには、プロキシモードでPCCからアクセスすることはできません。LO100のコマンドラインインターフェイスには、PCCにログオンしてLO100リモートプロセッサーのIPアドレスにtelnetで接続すればアクセスできます。

ハードウェアの配線

LO100s/iLOs for IAPs hardware generation 2.1以降は、すべて工場出荷時にプロキシアクセスモードで配線されています。

PCCのiLOは、デプロイメントの際に、お客様の管理ネットワークに配線されます。お客様が直接アクセストポロジを希望する場合は、PCCのeth2インターフェイスへの接続を切断し、スイッチをお客様の管理ネットワークにアップリンクすることで配線を変更できます。

iLOモードのチェック

IAPのiLOアクセスモードを確認するには、kickstartマシンの`/install/configs/primary/BlackBoxConfig.bct`設定ファイルの[REMOTE MANAGEMENT]セクションを参照します。[iLO Access Mode]というフィールドがあり、directまたはproxyの値が指定されています。設定ファイルにこのセクションがない場合、そのIAPではリモート管理は無効です。

リモート管理の無効化

IAPでは、リモート管理をプロキシモードで使用できるように工場出荷時の配線が行われていますが、デフォルトでは有効にされていません。管理者がリモート管理を有効にしている場合は、以下の手順に従い、無効にすることができます。

1. kickstartマシンの`/install/configs/primary/BlackBoxConfig.bct`ファイルを編集して、ファイルから[REMOTE MANAGEMENT]セクションを削除します。
2. `createBBC.zr`を実行します。
3. `converter.zr` を実行します。
4. `regloader.pl -cv` を実行します。

プロキシモードの使用

前提条件

次を設定する必要があります。

- iLOサブネット – iLOの設定に使用するデフォルトサブネットは10.1.0.0/16ですが、ご使用のネットワークと競合する場合は、お好みに合わせてX.X.0.0/16に変更できます。

  「iLOサブネット」を意味する値10.1.0.0はデフォルト値であり、環境に合わせた値に変更できます。プロキシモードでは、iLOの静的IPアドレスはサーバーのIPアドレスから自動的に抽出され、設定対象のiLOサブネットで割り当てられます。たとえば、サーバーのIPアドレスが10.0.172.1でiLOサブネットが14.0.0.0/16の場合、iLOにはIPアドレス14.0.172.1が割り当てられ、PCCサーバーのeth2インターフェイスにはiLOネットワーク上の静的ネットワークアドレス14.0.0.1が割り当てられます。デフォルトiLOサブネットの10.1.0.0が使用される場合、そのIPアドレスが10.0.172.1のサーバーのiLOには、IPアドレス

10.1.172.1が割り当てられ、PCCサーバーのeth2インターフェイスにはIPアドレス10.1.0.1が割り当てられます。

- iLOプロキシVIP – iLOプロキシVIPは、iLOプロキシへのアクセスを許可されるお客様の側のネットワーク上のIPです。このIPをBCTファイルにCIDR表記で入力します。このIPは、PCCの外部IPと同じサブネット上のアドレスでなければなりません。
- PCC iLOのIP – PCC iLO IPは、PCCのリモート管理プロセッサーのIPです。このIPは、PCCの外部IPと同じサブネット上に存在する必要はありません。プロキシモードでは、そのiLOデバイスがお客様の側のネットワーク上にあるサーバーはPCCだけです。PCC以外のサーバーは、内部IPを使用します。PCCサーバーにアクセスできない場合に備えて、PCCのiLOデバイスにアクセスできるようにしておく必要があります。

リモート管理の設定

リモート管理をプロキシモードで設定するには、以下の手順に従います。

1. kickstartマシンで/install/configs/primary/BlackBoxConfig.bctファイルを編集して、次のセクションを追加します。

   ```
   ##########################

   ### REMOTE MANAGEMENT ###

   ##########################

   iLO Access Mode: proxy

   iLO Subnet: 10.1.0.0/16

   iLO Proxy VIP: <proxy_VIP>/??
   ```

2. createBBC.zrを実行します。
3. converter.zr を実行します。
4. regloader.pl -cv を実行します。
5. 次のコマンドをPCCサーバー上で実行すると、すべてのIAPサーバー上のiLOが設定され、iLOのAdministratorユーザーが作成されます。これにより、そのユーザーについて管理者が提供するパスワードを設定できます。/opt/tools/ilo/configure_ilo -v -set -f /opt/tools/ilo/ilo_ips.csv all

   ilo_ips.csvファイルは、コマンドの実行元にするディレクトリに配置しておく必要があるテキストファイルです。このファイルには、

   *<PCCの内部IP>,<PCC iLOのIP>,<iLOネットマスク>,<iLOサブネットのゲートウェイIP>*を記述する必要があります。

   例: 10.0.101.2,15.1.2.30,255.255.0.0,15.1.2.1
6. プロンプトが表示されたら、Administratorアカウントのパスワードを入力します。

リモート管理Webインターフェイスへのアクセス

PCC以外のすべてのサーバーのリモート管理Webインターフェイスにアクセスするには、以下の手順に従います。

1. PCCの外部VIPアドレスを使用してPCCにログインします。
2. 左メニューで、[Hardware Management]を選択します。
3. [Hardware Management]ビューで、リモート管理が必要なサーバーの[Manage]リンクをクリックします。iLOの場合、これにより[Remote Management]ログインページが表示され、ログイン認証情報の入力を求められます（LO100の場合は、まず、中間的なアクセスページが開き、LO100のWeb UIとLO100

仮想KVM/メディアアプレットへのアクセスリンクが提供されます。仮想KVM/メディア機能を利用できるのは、ユーザーがILO/LO100 Advanced Packのライセンスを持っている場合だけです）。

4. ユーザーIDおよびパスワードログイン認証情報を入力して、リモート管理Webインターフェイスにアクセスします。

PCCのリモート管理Webインターフェイスにアクセスするには、URL *https://<PCC iLOのIPアドレス>*に直接接続します。

注記：

プロキシモードが設定されている場合は、必ず、PCCの[Hardware Management]ページのリンクからiLO/LO100リモート管理にアクセスしてください。というのは、プロキシモードでは、どのIAPサーバーのiLO/LO100のURLも同じであり、[Hardware Management]ページのサーバーのリンクをクリックすることで、そのサーバーに搭載された各iLO/LO100へのアクセスが要求されるからです。また、PCCページからログアウト（または、タイムアウト）すると、iLO/LO100アクセスは無効になります。このため、[Hardware Management]ページのリンク経由で少なくとも1回リモート管理Webインターフェイスにアクセスし、PCCのWebページにそのままログインしていない場合は、URL*https://<PCC iLOのIPアドレス>*に直接接続しても機能しません。

注記：

Webブラウザーを使用してiLO/LO100にアクセスすると、ブラウザーで、提示されている証明書が別のサーバーに対応するものであることを説明するメッセージが表示されることがあります。IEでは、[このサイトの閲覧を続行する]をクリックしてこの警告を無視してください。Firefoxでは、以前に保存した証明書を削除して、警告の表示を避けてください。

コマンドラインインターフェイスへのアクセス

リモート管理のコマンドラインインターフェイスにアクセスするには、以下の手順に従います。

1. `ssh`を使用して、PCCサーバーに`root`でログインします。
2. iLO経由でのアクセスが必要なサーバーに対して`ssh Administrator@<iLOのIPアドレス>`コマンドを入力します。

   たとえば、`ssh Administrator@10.1.172.1`を使用してiLO IP 10.1.172.1に接続します。
3. プロンプトが表示されたら、パスワードを入力して、そのサーバーのiLOコマンドラインインターフェイスにアクセスします。

コマンドラインインターフェイスを使用したサーバー電源の入れ直し

コマンドラインインターフェイスでサーバーの電源を入れ直すには、以下の手順に従います。

1. `ssh`を使用して、PCCサーバーに`root`でログインします。

注記：

DL140 G2サーバーのLO100へのアクセスには、`ssh`ではなく、`telnet`を使用します。

2. iLO経由でのアクセスが必要なサーバーに対して`ssh Administrator@<iLOのIPアドレス>`コマンドを入力します。

たとえば、ssh Administrator@10.1.172.1を使用してiLO IP 10.1.172.1に接続します。

3. プロンプトが表示されたら、パスワードを入力して、そのサーバーのiLOコマンドラインインターフェイスにアクセスします。
4. iLOまたはiLO2を搭載している場合は、hpiLO->プロンプトで、power resetと入力します。
5. LO100を搭載している場合は、EMS->プロンプトでEnterキーを押して、Lights-Out>プロンプトを表示し、reset [WARM|COLD]コマンドを入力します。

Webインターフェイスを使用したサーバー電源の入れ直し

Webインターフェイスを使用してサーバーの電源を入れ直すには、以下の手順に従います。

1. 上記のリモート管理Webインターフェイスへのアクセスの説明に従って、リモート管理Webインターフェイスにログインします。
2. iLOを使用している場合は、[Virtual Devices]タブ、[Virtual Power]の順にクリックします。
3. iLO2を使用している場合は、最上部の[Power Management]タブをクリックします。
4. LO100を使用している場合は、左メニューで[Power Control Options]リンクをクリックし、プルダウンメニューから[Power Control Options]オプションのいずれかを選択し、[Apply]ボタンをクリックします。
5. iLOのタイプに合わせて、電源入れ直しオプションのいずれかを選択します。

KVMコンソールへのアクセス

KVMコンソールにアクセスするには、以下の手順に従います。

1. 上記のリモート管理Webインターフェイスへのアクセスの説明に従って、リモート管理Webインターフェイスにログインします。
2. LO100を使用している場合は、中間的なアクセスページで[KVM]リンクをクリックします。
3. iLOまたはiLO2を使用している場合は、最上部の[Remote Console]タブをクリックします。
4. iLOを使用している場合は、[Remote Console]リンクをクリックします。
5. iLO2を使用している場合は、[Integrated Remote Console]リンクをクリックします。

サーバーコンソールが新しいウィンドウに表示されます。

注記:

仮想KVM機能は、ILO/LO100 Advanced Packのライセンスがないと、使用できません。

サーバー再起動の監視

サーバーの再起動を監視するには、以下の手順に従います。

1. 上記のリモート管理Webインターフェイスへのアクセスの説明に従って、リモート管理Webインターフェイスにログインします。
2. 最上部の[Remote Console]タブをクリックします。
3. iLOを使用している場合は、[Remote Console]リンクをクリックします。
4. iLO2を使用している場合は、[Integrated Remote Console]リンクをクリックします。
5. 新しいウィンドウにサーバーコンソールが開いたら、rootとしてIAPサーバーにログインします。
6. 次のコマンドを入力します。reboot
7. コンソールウィンドウで、サーバーのブートシーケンスを監視します。

サーバーのUIDライトの点灯

サーバーのUIDライトを点灯するには、以下の手順に従います。

1. 上記のリモート管理Webインターフェイスへのアクセス の説明に従って、リモート管理Webインターフェイスにログインします。
2. iLOを使用している場合は、最上部の[Virtual Devices]タブをクリックし、[Virtual Indicators]リンク、[Turn Unit ID On]ボタンの順にクリックします。
3. iLO2を使用している場合は、最上部の[System Status]タブをクリックし、[Turn UID On]ボタンをクリックします。
4. LO100を使用している場合は、左メニューの[Power Control Options]リンクをクリックして、プルダウンメニューから[Chassis Locator]オプションのいずれかを選択して、[Identify]ボタンをクリックします。

応答しないプロキシサーバー(PCC)の電源入れ直し

応答していないプロキシサーバー(PCC)の電源を入れ直すには、以下の手順に従います。

1. URL `https://<iLOのIPアドレス>` に接続して、プロキシサーバー(PCC)のiLOにアクセスします。
2. ユーザーIDとパスワードを使用してリモート管理のWebインターフェイスにログインします。
3. iLOを使用している場合は、[Virtual Devices]タブ、[Virtual Power]の順にクリックします。
4. iLO2を使用している場合は、最上部の[Power Management]タブをクリックします。
5. LO100を使用している場合は、左メニューの[Power Control Options]リンクをクリックし、プルダウンメニューから[Power Control Options]オプションのいずれかを選択して、[Apply]ボタンをクリックします。
6. プロキシサーバー(PCC)の電源を入れ直すために、iLOのタイプごとに使用できる電源入れ直しオプションのいずれかを選択します。

すべてのiLOでの管理者パスワードの変更

すべてのiLOについて管理者パスワードを変更するには、以下の手順に従います。

1. SSHを使用してPCCサーバーに`root`でログインします。
2. 次のコマンドを入力します。

   ```
   /opt/tools/ilo/configure_ilo -changepassword all
   ```

3. プロンプトが表示されたら、管理者アカウントの新しいパスワードを入力します。新しいパスワードは、設定済みのすべてのiLO Administratorアカウントに適用されます。

iLOファームウェアの更新

iLOファームウェアを更新するには、以下の手順に従います。

1. iLOやiLO2デバイスを使用している場合、ファームウェアは、iLOデバイスの設定時にIAPに付属の最新のファームウェアを使用して自動更新されます。IAPに付属のファームウェアより新しいファームウェアに更新するには、以下の手順に従います。
   a. iLOのbinファイルを抽出して、/opt/tools/ilo/firmware/<ilo|ilo2>の下に配置します。
   b. 次のコマンドを入力します。

      ```
      /opt/tools/ilo/configure_ilo -query all
      ```

2. Lights-Out 100デバイスを使用している場合は、以下の手順に従いファームウェアの更新を手動で行う必要があります。

a. ファームウェアパッケージを使用して、binファイルを作成します。
b. 作成したbinファイルを、PCCの/tftpboot/firmware/lo100/<バージョン番号> の下に配置します。バージョン番号のピリオドは取ります。
c. PCCのコマンドラインから、次のコマンドを入力します。

   /opt/tools/ilo/flashLO100 <iLO IP> <adminの名前> <adminのパスワード>

   たとえば、IP 10.1.172.1のLO100ファームウェアを更新するには、次のコマンドを入力します。

   /opt/tools/ilo/flashLO100 10.1.172.1 Administrator <adminパスワード>

   iLOのIPは、iLOサブネットの先頭から2つ目までのオクテット(BlackBoxConfig.bctファイルの[REMOTE MANAGEMENT]セクションで設定)とホストIPの最後の2つのオクテットから生成されます。

新規または交換サーバーのiLOプロセッサーの設定

PCCサーバーでconfigure_iloコマンドを使用して新しいIAPサーバーまたは交換したIAPサーバーのiLOを設定し、iLOのAdministratorユーザーを作成し、そのユーザーのパスワード(パスワードはお客様が決めます)を設定します。

1. /opt/tools/ilo/configure_ilo -v -set -f ilo_ips.csv <IP Address> を実行します。

   *<IP Address>*は、新しいサーバーまたは交換したサーバーのIAP IPアドレスです。たとえば、そのIPアドレスが10.0.172.11のサーバーのiLOを設定するには、/opt/tools/ilo/configure_ilo -v -set -f ilo_ips.csv 10.0.172.11を使用します。

2. プロンプトが表示されたら、Administratorアカウントのパスワードを入力します。

ilo_ips.csvファイルは、次の内容を含むテキストファイルで、カレントディレクトリに配置する必要があります。

<IAPサーバーの内部IP>、*<PCC iLOのIP>*、*<iLOのネットマスク>*,*<iLOサブネットのゲートウェイIP>*

次に、ilo_ips.csvファイルに含まれる行の例を示します。

10.0.101.2,15.1.2.30,255.255.0.0,15.1.2.1

直接接続モードの使用

前提条件

iLOアクセスを設定する各サーバーに、IPアドレスを1つずつ割り当てる必要があります。

リモート管理の設定

リモート管理を直接接続モードで設定するには、以下の手順に従います。

1. kickstartマシンで/install/configs/primary/BlackBoxConfig.bctファイルを編集して、次のセクションを追加します。

   ##########################

```
### REMOTE MANAGEMENT ###

########################

iLO Access Mode: direct
```

2. createBBC.zrを実行します。
3. converter.zr を実行します。
4. regloader.pl -cv を実行します。
5. 次のコマンドをPCCサーバー上で実行すると、すべてのIAPサーバー上のiLOが設定され、iLOのAdministratorユーザーが作成されます。これにより、そのユーザーについて管理者が提供するパスワードを設定できます。/opt/tools/ilo/configure_ilo -v -set -f ilo_ips.csv

   ilo_ips.csvファイルは、コマンドの実行元にするディレクトリに配置しておく必要があるテキストファイルです。ファイルには、iLOアクセスを設定するサーバーごとに、次のエントリーを記述する必要があります。各エントリーで1行を使用してください。

   <IAPサーバーの内部IP>、*<iLOのIP>*、*<iLO のネットマスク>*、*<iLOサブネットのゲートウェイIP>*

   例: 10.0.204.2,16.1.2.40,255.255.254.0,16.1.2.1
6. プロンプトが表示されたら、Administratorアカウントのパスワードを入力します。

注記:

iLOのIP(16.1.2.40)は、お客様の管理ネットワーク上のアドレスです。ilo_ips.csvファイルには、搭載するiLOを設定する必要があるサーバーごとに、お客様の管理ネットワーク上のIPアドレスを記述する必要があります。

直接接続モードでのリモート管理Webインターフェイスへのアクセス

IAPサーバーに接続してリモート管理を行うには、以下の手順に従います。

1. URL https://<サーバーiLOのIPアドレス> に接続します。
2. これにより、リモート管理のログインページが表示され、ログイン認証情報の入力を求められます。リモート管理のユーザーIDとパスワードを入力して、リモート管理のWebインターフェイスにアクセスします。

注記:

直接接続モードでは、PCCの[Hardware Management]ページの[Remote Management]列のリンクは「Not Enabled」と表示されます。

コマンドラインインターフェイスへのアクセス

リモート管理のコマンドラインインターフェイスにアクセスするには、以下の手順に従います。

1. iLO経由でのアクセスが必要なサーバーに対してssh Administrator@*<iLOのIPアドレス>* コマンドを入力します。

   たとえば、iLO IP 16.1.2.40に接続するには、ssh Administrator@16.1.2.40を使用します。
2. プロンプトが表示されたら、パスワードを入力して、そのサーバーのiLOコマンドラインインターフェイスにアクセスします。

コマンドラインインターフェイスを使用したサーバー電源の入れ直し

コマンドラインインターフェイスでサーバーの電源を入れ直すには、以下の手順に従います。

1. iLO経由でのアクセスが必要なサーバーに対して`ssh Administrator@<iLOのIPアドレス>`コマンドを入力します。
2. プロンプトが表示されたら、パスワードを入力して、そのサーバーのiLOコマンドラインインターフェイスにアクセスします。
3. iLOまたはiLO2を搭載している場合は、`hpiLO->`プロンプトで、`power reset`と入力します。
4. LO100を搭載している場合は、`EMS->`プロンプトでEnterキーを押して、`Lights-Out>`プロンプトを表示し、`reset [WARM|COLD]`コマンドを入力します。

Webインターフェイスを使用したサーバー電源の入れ直し

Webインターフェイスを使用してサーバーの電源を入れ直すには、以下の手順に従います。

1. 上記の直接接続モードでのリモート管理Webインターフェイスへのアクセス の説明に従って、リモート管理Webインターフェイスにログインします。
2. iLOを使用している場合は、[Virtual Devices]タブ、[Virtual Power]の順にクリックします。
3. iLO2を使用している場合は、最上部の[Power Management]タブをクリックします。
4. LO100を使用している場合は、左メニューで[Power Control Options]リンクをクリックし、プルダウンメニューから[Power Control Options]オプションのいずれかを選択し、[Apply]ボタンをクリックします。
5. iLOのタイプに合わせて、電源入れ直しオプションのいずれかを選択します。

KVMコンソールへのアクセス

KVMコンソールにアクセスするには、以下の手順に従います。

1. 上記の直接接続モードでのリモート管理Webインターフェイスへのアクセス の説明に従って、リモート管理Webインターフェイスにログインします。
2. 最上部の[Remote Console]タブをクリックします。
3. iLOを使用している場合は、[Remote Console]リンクをクリックします。
4. iLO2を使用している場合は、[Integrated Remote Console]リンクをクリックします。

サーバーコンソールが新しいウィンドウに表示されます。

注記：

仮想KVM機能は、ILO/LO100 Advanced Packのライセンスがないと、使用できません。

サーバー再起動の監視

サーバーの再起動を監視するには、以下の手順に従います。

1. 上記の直接接続モードでのリモート管理Webインターフェイスへのアクセス の説明に従って、リモート管理Webインターフェイスにログインします。
2. 最上部の[Remote Console]タブをクリックします。
3. iLOを使用している場合は、[Remote Console]リンクをクリックします。
4. iLO2を使用している場合は、[Integrated Remote Console]リンクをクリックします。
5. 新しいウィンドウにサーバーコンソールが開いたら、`root`としてIAPサーバーにログインします。

6. 次のコマンドを入力します。`reboot`
7. コンソールウィンドウで、サーバーのブートシーケンスを監視します。

サーバーのUIDライトの点灯

サーバーのUIDライトを点灯するには、以下の手順に従います。

1. 上記の直接接続モードでのリモート管理Webインターフェイスへのアクセス の説明に従って、リモート管理Webインターフェイスにログインします。
2. iLOを使用している場合は、最上部の[Virtual Devices]タブをクリックし、[Virtual Indicators]リンク、[Turn Unit ID On]ボタンの順にクリックします。
3. iLO2を使用している場合は、最上部の[System Status]タブをクリックし、[Turn UID On]ボタンをクリックします。
4. LO100を使用している場合は、左メニューの[Power Control Options]リンクをクリックして、プルダウンメニューから[Chassis Locator]オプションのいずれかを選択して、[Identify]ボタンをクリックします。

すべてのiLOでの管理者パスワードの変更

すべてのiLOについて管理者パスワードを変更するには、以下の手順に従います。

1. SSHを使用してPCCサーバーに`root`でログインします。
2. 次のコマンドを入力します。

   ```
   /opt/tools/ilo/configure_ilo -changepassword all
   ```

3. プロンプトが表示されたら、管理者アカウントの新しいパスワードを入力します。新しいパスワードは、設定済みのすべてのiLO Administratorアカウントに適用されます。

iLOファームウェアの更新

iLOファームウェアを更新するには、以下の手順に従います。

1. iLOやiLO2デバイスを使用している場合、ファームウェアは、iLOデバイスの設定時にIAPに付属の最新のファームウェアを使用して自動更新されます。IAPに付属のファームウェアより新しいファームウェアに更新するには、以下の手順に従います。
   a. iLOのbinファイルを抽出して、/opt/tools/ilo/firmware/<ilo|ilo2>の下に配置します。
   b. 次のコマンドを入力します。

      ```
      /opt/tools/ilo/configure_ilo -query all
      ```

2. Lights-Out 100デバイスを使用している場合は、以下の手順に従いファームウェアの更新を手動で行う必要があります。
   a. ファームウェアパッケージを使用して、`bin`ファイルを作成します。
   b. 作成したbinファイルを、PCCの`/tftpboot/firmware/lo100/<バージョン番号>` の下に配置します。バージョン番号のピリオドは取ります。
   c. PCCのコマンドラインから、次のコマンドを入力します。`/opt/tools/ilo/flashLO100 <iLO IP> <adminの名前> <adminのパスワード>`

      たとえば、IP 16.1.2.40のLO100ファームウェアを更新するには、次のコマンドを入力します。`/opt/tools/ilo/flashLO100 16.1.2.40 Administrator <管理者パスワード>`

新規または交換サーバーのiLOプロセッサーの設定

PCCサーバーでconfigure_iloコマンドを使用して新しいIAPサーバーまたは交換したIAPサーバーのiLOを設定し、iLOのAdministratorユーザーを作成し、そのユーザーのパスワード（パスワードはお客様が決めます）を設定します。

1. /opt/tools/ilo/ilo_ips.csvファイルを編集して、新しいサーバー用にエントリーを追加または削除します。交換用サーバーについては、IPアドレスを変更しない場合は、ファイルの修正は不要です。
2. /opt/tools/ilo/configure_ilo -v -set -f ilo_ips.csv を実行します。
3. プロンプトが表示されたら、Administratorアカウントのパスワードを入力します。

ilo_ips.csvファイルは、次の内容を含むテキストファイルで、カレントディレクトリに配置する必要があります。

<IAPサーバーの内部IP>、*<iLOのIP>*、*<iLO のネットマスク>*、*<iLOサブネットのゲートウェイIP>*

次に、ilo_ips.csvファイルに含まれる行の例を示します。

```
10.0.204.11,16.1.2.50,255.255.254.0,16.1.2.1
```

注記：

iLOのIP（16.1.2.50）は、お客様の管理ネットワーク上のアドレスです。

A IAPアプリケーション生成アラート

次の表では、アプリケーションにより生成され、IAPシステムで表示されるアラートを示します。

これらのアラートは、IAPの機能に影響を及ぼす重大な問題を、予想されるものも含めてIAPの管理者に通知します。

アラートは、PCCの[Overview]ページの上部にある[Current Platform Alerts（現在のプラットフォームアラート）]領域に表示されます。また、外部モニターや電子メール受信者に送信することもできます（「SNMP Management（SNMPの管理）」（121ページ）を参照）。

アラートは、イベントとしてPCCの永続ストレージ（postgres）に記録され、[Event Viewer]ページに他のイベントに混ざって表示されます（「Event Viewer（イベントビューアー）」（119ページ）を参照）。

注記：

一部のアラートは、その生成またはクリアが最長30分遅れます（実際の遅れは、アラートの細目により異なります）。

表32 IAPアプリケーション生成アラート

Alert ID	説明	コンテキスト	PCC/サーバーの再起動後の状態	PCCの[Overview]ページからの手動での削除後の状態	アラートレベル
システムインフラストラクチャ					
A010-01	サービスが停止したため、スマートセルが一時停止しています。	理由はさまざまな機能により示されます。	*PCCの再起動後：* アラートは表示されます。 *サーバーの再起動後：* 通常アラートは消えますが、スマートセルが一時停止していると再び表示されます。	アラートは消え、問題が未解決でも表示されません。	メジャー
A010-03	DB2インスタンスを使用できません。	DB2への接続を確立できませんでした。	*PCCの再起動後：* DB2が起動して稼動していない場合、PCCは起動できません。 *サーバーの再起動後：* DB2の再起動後アラートは消えます。	アラートは消え、問題が未解決でも表示されません。	クリティカル

Alert ID	説明	コンテキスト	PCC/ サーバー の再起動後の状態	PCCの[Overview]ページからの手動での 削除 後の状態	アラートレベル
A010-06	DB2のトランザクションログファイルが消失しています。	DB2トランザクションログに欠落が見つかりました。消失したログファイルは<missing_tx_log>です。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	クリティカル
A010-07	アプリケーションサーバーが正常に起動しませんでした。	JBossが一部のサービスをロードできませんでした。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* 問題が修正されない場合、アラートが再び表示されます。	アラートは消え、問題が未解決でも表示されません。	クリティカル
A010-09	スマートセルのMySQLインスタンスを使用できません。	MySQLへの接続を確立できませんでした。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* MySQLの再起動後アラートは消えます。	アラートは消え、問題が未解決でも表示されません。	クリティカル
A010-11	ランタイム環境でメモリ不足の問題が検出されました。	サーバー<ip_address>でのメモリ不足エラー。	*PCCの再起動後:* アラートは表示されません。 *サーバーの再起動後:* これは、メモリ不足アラートに対するリカバリ状態です。マシンが再起動すると、アラートは消えます。	アラートは消えます。	クリティカル
A010-12	マシンにアクセスできません。	マシンは '<command>の要求に応答していません。ここで<command>は 'pingまたは 'ポート22のnetcatです。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは消えます。	アラートは消え、問題が未解決でも表示されません。	クリティカル
A010-13	このマシン上のアプリケーションサーバーは停止しています。	JBossが停止しています。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは消えます。	アラートは消え、問題が未解決でも表示されません。	クリティカル

Alert ID	説明	コンテキスト	PCC/ サーバー の再起動後の状態	PCCの[Overview]ページからの手動での 削除 後の状態	アラートレベル
A010-14	kickstartのPostgresインスタンスを利用できません。	Postgres（PCCの永続ストレージ）への接続を確立できませんでした。	*PCCの再起動後：* アラートは表示されます。 *サーバーの再起動後：* アラートは表示されます。	アラートは消え、問題が未解決でも表示されません。	クリティカル
A010-15	空きスワップスペースが閾値よりも少なくなっています。	空きスワップスペースは<free_swap>%（閾値は<threshold_free_swap>%）です。	*PCCの再起動後：* アラートは表示されます。 *サーバーの再起動後：* アラートは表示されます。	アラートは表示されます。	マイナー
A010-16	ディスクパーティションのサイズが下側の閾値（95%）に達しました。	ディスクパーティション<disk_partition_name>の使用量が全体の<used_percentage>に達しています。<total_size>のうち<used_absolute>が使われています。	*PCCの再起動後：* アラートは表示されます。 *サーバーの再起動後：* 次回にディスクサイズのチェックが行われ、そのときもディスクサイズが閾値を超えている場合は、アラートが再び表示されます。	次回にディスクサイズのチェックが行われ、そのときもディスクサイズが閾値を超えている場合は、アラートが再び表示されます。	マイナー
A010-17	ディスクパーティションのサイズが上側の閾値（99%）に達しました。	ディスクパーティション<disk_partition_name>の使用量が全体の<used_percentage>に達しています。<total_size>のうち<used_absolute>が使われています。	*PCCの再起動後：* アラートは表示されます。 *サーバーの再起動後：* 次回にディスクサイズのチェックが行われ、そのときもディスクサイズが閾値を超えている場合は、アラートが再び表示されます。	次回にディスクサイズのチェックが行われ、そのときもディスクサイズが閾値を超えている場合は、アラートが再び表示されます。	メジャー
		アーカイブ			
A020-01	アーカイブプロセスで、使用できるスマートセルグループが見つかりませんでした。	ドメイン<domain>では、アーカイバーサービスを利用できません。	*PCCの再起動後：* アラートは表示されます。 *サーバーの再起動後：* アラートはしばらく消えますが、再び表示されます。	アラートは消え、問題が未解決でも表示されません。	クリティカル

Alert ID	説明	コンテキスト	PCC/ サーバー の再起動後の状態	PCCの[Overview]ページからの手動での 削除 後の状態	アラートレベル
			インデックス作成		
A030-01	インデックスが壊れています。	インデックス<index>は使用できません。修復が必要です。検索結果が不完全な可能性があります。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* スマートセルの起動時に問題が修復されると、アラートは消えます。	アラートは消え、問題が未解決でも表示されません。	メジャー

ID	説明	コンテキスト	PCC/ サーバー の再起動後の状態	PCCの[Overview]ページからの手動での 削除 後の状態	アラートレベル
			クエリサービス		
A040-01	クエリサービスがスマートセルグループにアクセスできません。	グループ<group>をクエリに利用できません。検索結果が不完全な可能性があります。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* スマートセルの再起動中に問題が修復されるとアラートは消えます。	アラートは消え、問題が未解決でも表示されません。	メジャー
			複製		
A050-01	複製SMTPサーバーにアクセスできません。	<smtp_server>への接続に失敗したため、データを複製できませんでした。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	クリティカル
A050-02	複製SMTPサーバーはビジーです。	<smtp_server>で複製SMTPサーバーにより接続が閉じられたため、ドメイン<domain>のグループ<group>のデータを複製できませんでした。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	メジャー

ID	説明	コンテキスト	PCC/ サーバー の再起動後の状態	PCCの[Overview]ページからの手動での 削除 後の状態	アラートレベル
A050-03	複製SMTPサーバーへの接続がタイムアウトしました。	<smtp_server>で複製SMTPサーバーへの接続がタイムアウトしたため、データを複製できませんでした。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	クリティカル
A050-04	複製プロセスでデータの送信に失敗しました。	ドメイン<domain>のグループ<group>のデータを複製できませんでした。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	クリティカル
A050-05	複製システムでグループの複製アーカイブサービスを利用できません。	ドメイン<domain>のグループ<group>で複製アーカイブサービスを利用できません。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	クリティカル
A050-06	複製プロセスで、グループのファイルをリストできませんでした。	ドメイン<domain>のグループ<group>の複製のためのファイルリストを取得できませんでした。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	クリティカル
A050-07	複製プロセスはソースグループからのデータにアクセスできません。	ドメイン<domain>のグループ<group>で複製のためのデータを取得できませんでした。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	クリティカル
A050-08	グループの複製プロセスが失敗しました。	ドメイン<domain>のグループ<group>でデータを複製できませんでした。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	クリティカル
A050-09	グループの複製アーカイブサービスを利用できません。	ドメイン<domain>のグループ<group>で複製アーカイブサービスを利用できません。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	クリティカル
データベース複製					

ID	説明	コンテキスト	PCC/サーバーの再起動後の状態	PCCの[Overview]ページからの手動での削除後の状態	アラートレベル
A051-01	データベース複製が要求するDB2トランザクションログが消失しています。	DB2複製が要求するDB2トランザクションログ<missing_tx_log>が見つかりませんでした。DB2複製は停止しており、手動で初期化し直す必要があります。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	クリティカル
A051-02	IPCファイルが消失しています。	DB2複製(<program>)が要求するIPCファイル<missing_ipc_queue_file>が見つかりませんでした。このためDB2複製は、停止要求を行っても停止できない可能性があります。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	マイナー
A051-03	DB2複製にエラーがあります。	DB2複製はエラー状態です。詳細: <error_msg>	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	クリティカル

ID	説明	コンテキスト	PCC/サーバーの再起動後の状態	PCCの[Overview]ページからの手動での削除後の状態	アラートレベル
A051-04	プライマリデータベースと複製データベースの同期がとれていません。	プライマリと複製のDB2データベースの同期が取れなくなって<threshold_latency>秒を経過しました(実際の遅延: <actual_latency>秒)。詳細: <error_msg>	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	メジャー
A051-05	DB2複製がアップデートを取得していません。	DB2複製が最後にDB2データベースにアップデートを取得してから<threshold_latency>秒を超えました(実際の遅延: <actual_latency>秒)。詳細: <error_msg>	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	メジャー

ID	説明	コンテキスト	PCC/サーバーの再起動後の状態	PCCの[Overview]ページからの手動での削除後の状態	アラートレベル
		ユーザー管理とユーザー同期化			
A060-01	ユーザーの動的アカウント同期化ジョブが失敗しました。	DASジョブ<das_job>がユーザーをインポートできませんでした。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* ジョブが再度実行されるとアラートが表示されます。	ジョブが再度実行されるとアラートが表示されます。	クリティカル
A060-02	グループの動的アカウント同期化ジョブが失敗しました。	DASジョブ<das_job>がグループをインポートできませんでした。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* ジョブが再度実行されるとアラートが表示されます。	ジョブが再度実行されるとアラートが表示されます。	クリティカル
A060-03	削除したオブジェクトの動的アカウント同期化ジョブが失敗しました。	DASジョブ<das_job>がユーザーおよびグループを無効にできませんでした。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* ジョブが再度実行されるとアラートが表示されます。	ジョブが再度実行されるとアラートが表示されます。	クリティカル
A060-04	動的アカウント同期化ジョブは完了しましたがエラーが発生しています。	[Account Error Recovery]をチェックして、開始ポイント=<ldapdn>、サーバー=<ldap_server>についてインポートの問題がないか調べます。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* ジョブが再度実行されるとアラートが表示されます。	ジョブが再度実行されるとアラートが表示されます。	メジャー

ID	説明	コンテキスト	PCC/サーバーの再起動後の状態	PCCの[Overview]ページからの手動での削除後の状態	アラートレベル
		データベースバックアップ			

ID	説明	コンテキスト	PCC/サーバーの再起動後の状態	PCCの[Overview]ページからの手動での削除後の状態	アラートレベル
A070-01	DB2のオンラインバックアップが古すぎます。	<online_backup_dir>のDB2オンラインバックアップが作成後<max_days>日を超えています。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	メジャー
A070-02	DB2のオンラインバックアップが見つかりません。	<online_backup_dir>でDB2のオンラインバックアップが見つかりませんでした。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* アラートは表示されます。	アラートは表示されます。	メジャー
		テープバックアップ			
A071-01	テープリストアが失敗しました。手動操作が必要です。	リストア対象のスマートセルの割り当ての際にエラーが発生しました。グループID: <group_id>	*PCCの再起動後:* ジョブを再度実行したときに問題が解決されていない場合はアラートが表示されます。 *サーバーの再起動後:* ジョブを再度実行したときに問題が解決されていない場合はアラートが表示されます。	ジョブを再度実行したときに問題が解決されていない場合はアラートが表示されます。	クリティカル
A071-02	テープリストアが失敗しました。手動操作が必要です。	スマートセルでテープリストアが中断されました。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* ジョブを再度実行したときに問題が解決されていない場合はアラートが表示されます。	ジョブを再度実行したときに問題が解決されていない場合はアラートが表示されます。	クリティカル
A071-03	テープリストアが失敗しました。手動操作が必要です。	スマートセルでテープリストア手順が失敗しました。	*PCCの再起動後:* アラートは表示されます。 *サーバーの再起動後:* ジョブを再度実行したときに問題が解決されていない場合はアラートが表示されます。	ジョブを再度実行したときに問題が解決されていない場合はアラートが表示されます。	クリティカル

ID	説明	コンテキスト	PCC/ サーバー の再起動後の状態	PCCの[Over-view]ページからの手動での 削除 後の状態	アラートレベル
			管理		
A080-01	PCC上のPostgresインスタンスを使用できません。	Postgres（PCCの永続ストレージ）への接続を確立できませんでした。	*PCCの再起動後：* アラートは表示されます。 *サーバーの再起動後：* Postgresの再起動後アラートは消えます。	アラートは消え、問題が未解決でも表示されません。	クリティカル
			保管		
A090-01	保管は正しく設定されていないため実行されません。	ドメイン保管期間の<domain_ret_period>が、ドメイン<domain>の最短保管期間<min_ret_period>よりも短く設定されています。	*PCCの再起動後：* アラートは表示されます。 *サーバーの再起動後：* マシンの再起動後も問題が解決されない場合は、アラートが表示されます。	アラートは消え、問題が未解決でも表示されません。	クリティカル

B インデックスが作成されるドキュメントタイプ

IAPでは、電子メールメッセージの他に、次の表で示すファイルタイプにインデックスが付けられます。これらのファイルには、電子メールの添付ファイルやHP File Archivingソフトウェアで IAPに移行されたファイルなどがあります。

Microsoft Access、Project、およびVisioファイルには、インデックスは付けられません。これらのファイルがアーカイブされる場合、ファイルの検索に使えるのは、ファイル名、ファイル拡張子など、外部の識別情報だけです。

IAP 2.1では、いくつかのアプリケーション（WordPerfect Office、WordPerfect Presentations、WordPerfect for DOS、Quattro Pro for Windows、およびQuattro Pro for DOS）のファイルタイプとコンテンツタイプのサポートが追加されています。

ドキュメントのインデックス作成について詳しくは、IAPユーザーガイドの「IAPの概要」の章を参照してください。

表33 IAPでインデックスが作成されるドキュメントMIMEタイプ

ファイル拡張子	ファイルタイプ	MIMEコンテンツタイプ
.xml	XMLドキュメント	text/xml
.txt	テキストファイル（特別な指定がない限りISO-8859-1として処理）	text/plain
.htm、.html、.stm	HTMLドキュメント	text/html、rtf/html
.rtf	リッチテキスト形式	rtf/text、application/rtf
.dat	TNEF（Microsoft Exchange向け）	ms/tnef
.mht、.mhtml、.nws、.eml	電子メールメッセージ	message/RFC 822
.doc、.dot	Microsoft Word 97～2003文書	application/msword
.xla、.xlc、.xlm、.xls、.xlt、.xlw	Microsoft Excel 97～2003文書	application/vnd.ms-excel、application/ms-excel
.pot、.pps、.ppt	Microsoft PowerPoint 97～2003文書	application/vnd.ms-powerpoint、application/vnd.msppt
.pdf	Adobe Portable Document形式	application/pdf
.zip	ZIPアーカイブ	application/zip
.docx	Microsoft Word 2007 文書	application/vnd.openxmlformats-officedocument.wordprocessingml.document

ファイル拡張子	ファイルタイプ	MIMEコンテンツタイプ
.docm	Microsoft Word 2007マクロ有効文書	application/vnd.ms-word.document.macroEnabled.12
.dotx	Microsoft Word 2007テンプレート	application/vnd.openxmlformats-officedocument.wordprocessingml.template
.dotm	Microsoft Word 2007マクロ有効文書テンプレート	application/vnd.ms-word.template.macroEnabled.12
.xlsx	Microsoft Excel 2007ブック	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
.xlsm	Microsoft Excel 2007マクロ有効ブック	application/vnd.ms-excel.sheet.macroEnabled.12
.xltx	Microsoft Excel 2007テンプレート	application/vnd.openxmlformats-officedocument.spreadsheetml.template
.xltm	Microsoft Excel 2007マクロ有効ブックテンプレート	application/vnd.ms-excel.template.macroEnabled.12
.xlam	Microsoft Excel 2007アドイン	application/vnd.ms-excel.addin.macroEnabled.12
.pptx	Microsoft PowerPoint 2007プレゼンテーション	application/vnd.openxmlformats-officedocument.presentationml.presentation
.pptm	Microsoft PowerPoint 2007マクロ有効プレゼンテーション	application/vnd.ms-powerpoint.presentation.macroEnabled.12
.ppsx	Microsoft PowerPoint 2007スライドショー	application/vnd.openxmlformats-officedocument.presentationml.slideshow
.ppsm	Microsoft PowerPoint 2007マクロ有効スライドショー	application/vnd.ms-powerpoint.slideshow.macroEnabled.12
.potx	Microsoft PowerPoint 2007テンプレート	application/vnd.openxmlformats-officedocument.presentationml.template
.potm	Microsoft PowerPoint 2007マクロ有効プレゼンテーションテンプレート	application/vnd.ms-powerpoint.template.macroEnabled.12
.wpd	Windows用Corel WordPerfect – Version 12.0、X3まで	application/wordperfect、application/wpd
.qpw、.wb1、.wb2、.wb3	Windows用Corel Quattro Pro – Version 12.0、X3まで	application/qpw、application/wb1、application/wb2、application/wb3
.shw	Corel Presentations – Version 12.0、X3まで	application/presentations

索引