Oracle® Universal Content Management

Content Tracker 管理ガイド

10*g* リリース 3（10.1.3.3.0）

部品番号 : E05638-01

2007 年 10 月

ORACLE®

Oracle Universal Content Management Content Tracker 管理ガイド, 10*g* リリース 3（10.1.3.3.0）

部品番号 : E05638-01

原本名 : Oracle Universal Content Management Content Tracker Administration Guide, 10*g* Release 3 (10.1.3.3.0)

原本部品番号 : A00076-01

原本協力者 : Deanna Burke, Evan Suits

目次

第 1 章： はじめに

第 2 章： 操作概要

第 3 章 : Content Tracker の使用

第 4 章： レポート生成

第 5 章 : サービス・コール構成

付録 A: Content Tracker の構成およびカスタマイズ

付録 B: トラブルシューティング

付録 C: サード・パーティ・ライセンス

索引

1

はじめに

概要

この項の内容は次のとおりです。

このガイドについて

この項の内容は次のとおりです。

Content Tracker の操作要約

Content Tracker では、Content Server インスタンスのアクティビティが監視され、これらのアクティビティの選択済の詳細が記録されます。次に、システムの使用状況の把握に役立つレポートが生成されます。この項の内容は次のとおりです。

注意 : この項では、Content Tracker およびコンテンツ・トラッキング・レポートの機能について簡単に概要を説明します。ここではコンポーネントの基本的背景についてまとめています。これは、第 2 章「操作概要」で説明されている詳細情報を理解するうえでの予備知識となります。

コンポーネントについて

Content Tracker とコンテンツ・トラッキング・レポートは別個のモジュールですが、連携動作してシステムの使用状況に関する情報を提供します。提供された情報を使用することで、最もアクセス頻度の高いコンテンツ・アイテムや、ユーザーまたは特定グループにとって最も価値の高いコンテンツを判断できます。

組織のコンテンツの消費パターンを理解することは、コンテンツ管理を適切に行うために不可欠です。これによって、ユーザーを中心に据えた適切な情報をより効率的に提供することが可能になります。この項では、両方のコンポーネントについて要約します。

Content Tracker の概要

Content Tracker では、システムが監視され、様々なアクティビティに関する情報が記録されます。この情報は様々なソースから収集され、マージされて Content Server データベース内の一連の表に書き込まれます。Content Tracker をカスタマイズして、収集される情報のタイプを変更または拡張できます。Content Tracker では、次のソースからのアクティビティが監視されます。

❖ **コンテンツ・アイテム・アクセス :**

Content Tracker では、コンテンツ・アイテムの使用状況に関する情報が収集されます。データは、Web フィルタ・ログ・ファイル、Content Server データベース、およびその他の外部アプリケーション（ポータルや Web サイトなど）から取得されます。コンテンツ・アイテム・アクセス・データには、日付、時刻、コンテンツ ID、現在のメタデータ、ユーザー名、およびユーザーに関するプロファイル情報が含まれます。

❖ **Content Server サービス :**

Content Tracker では、検索リクエストを処理するサービスと、コンテンツを返すすべてのサービスが追跡されます。また Content Tracker では、簡単な構成変更により、カスタム・サービスも含めてほとんどあらゆる Content Server サービスを監視できます。

コンテンツ・トラッキング・レポートの概要

Content Tracker によってデータが抽出され、適用可能なデータベース・リポジトリ表に値が移入されると、情報をレポート生成のために使用できるようになります。コンテンツ・トラッキング・レポートを使用すると、次のことを実行できます。

❖ **レポートの生成 :**

コンテンツ・トラッキング・レポートでは、Content Tracker によって作成された表が問合せされ、特定のコンテンツ・アイテムの各種アクティビティのサマリー・レポートおよび使用履歴が生成されます。これらのレポートを使用すると、コンテンツまたはユーザーの特定グループを、メタデータ、ファイル拡張子またはユーザー・プロファイルに基づいて分析できます。提供されている事前定義レポートを使用することも、各インストールに合せて事前定義レポートをカスタマイズすることもできます。あるいは、互換性のあるサード・パーティのレポート作成パッケージを使用することもできます。

❖ **コンテンツ管理プラクティスの最適化 :**

レポートされたデータを、コンテンツ保存管理に使用することもできます。つまり、特定のコンテンツ・アイテムの特定期間中のアクセス頻度に応じて、アイテムの一部をアーカイブまたは削除するように決定できます。同様に、アプリケーションはこのデータを使用して、特定タイプのユーザーの最頻アクセス・コンテンツをポートレットに提供できます。

データ・フローについて

Content Tracker とコンテンツ・トラッキング・レポートのコンポーネントは結合されて、主に 3 つの情報処理機能を実行します。

❖ データ記録（1-4 ページ）

❖ データ・リダクション・プロセス（1-5 ページ）

❖ データ・レポート作成（1-5 ページ）

データ記録

Content Tracker では、次のソースからのデータが記録されます。

- **Web サーバー・フィルタ・プラグイン :**

  コンテンツが静的 URL を介してリクエストされると、Web サーバー・フィルタ・プラグインによってリクエストの特定の詳細が記録され、1 つ以上のイベント・ログ・ファイルに情報が保存されます。イベント・ログ・ファイルは、情報が収集された日付に従って編成されます。イベント・ログ・ファイルは最終的に、Content Tracker データ・リダクション・プロセスで入力として使用されます。

- **サービス・ハンドラ・フィルタ :**

  Content Tracker には、監視対象となるサービスのリストがあります。これらのサービスの 1 つが呼び出されると、サービスの詳細がコピーされ、SctAccessLog 表に保存されます。監視されるサービスおよび記録される詳細は、変更できます。

- **Content Tracker ロギング・サービス :**

  Content Tracker では、汎用のロギング・サービス（イベントの記録に使用できる単一サービス・コール）がサポートされています。このサービスは、URL を介して直接呼び出す、サービス・スクリプト内のアクションとして呼び出す、または IdocScript から呼び出すことができます。

- **Content Server データベース表 :**

  Content Tracker データ・リダクション・プロセスでは、選択された Content Server データベース表が問合せされます。これは主に、レポート作成期間中にアクティブであったユーザーの名前およびアカウントに関する情報を取得するために行われます。

- **アプリケーション API:**

  Content Tracker には、他のコンポーネントやアプリケーションを追跡のために登録できるインタフェースが備わっており、それらのアクティビティに関する情報を記録できます。たとえば、このインタフェースを使用すると、Site Studio などの協調アプリケーションでイベント情報をリアルタイムで記録できます。

注意 : アプリケーション API は、SctApplicationFilter.hda ファイルに含まれています。このインタフェースは、Content Server サービスを使用しないコールをコーディングするためのコードとして設計されたものです。アプリケーション API は、汎用的には使用できません。このインタフェースを使用してアプリケーションを構築する場合は、コンサルティング・サービスにお問い合せください。

データ・リダクション・プロセス

データ・リダクション・プロセスでは、4 つのデータ記録ソースから取得されたデータが収集されてマージされます。このリダクション・プロセスが完了するまで、Content Tracker 表のデータは完成されません。通常は、毎日の収集データに対して 1 回、リダクションを実行します。リダクションは手動で実行することも、自動実行をスケジュールすることもできます。その場合、通常はシステム負荷が少ないピーク外の時間帯にスケジュールします。

データ・レポート作成

コンテンツ・トラッキング・レポートには、Content Server のアクティビティおよび使用状況に関するよくある質問の答えを示す一連のレポートが備わっています。たとえば、最もアクセス頻度が高い管理対象オブジェクト、最も使用頻度が高い検索、および最もアクティブなユーザーを特定できます。これらのレポートは、Content Tracker Report Generator のメイン・ページから直接使用することも、「Content Information」ページでアクションとして間接的に使用することもできます。レポート、基礎となる問合せ、および出力の形式設定は、カスタマイズできます。

対象読者

この管理ガイドは、Content Tracker およびコンテンツ・トラッキング・レポートのコンポーネントをインストールして構成する必要のあるシステム管理者を対象としています。また、システム管理者は、このガイドを使用して、データ収集の管理、使用状況レポートの生成、およびエンド・ユーザーの Content Server 機能の拡張を行うこともできます。このガイドでは、製品が正常にインストールされていること、および読者に Content Server 製品および Content Server のアーキテクチャに関する知識があることを前提としています。

新機能

この項では、バージョン 10*g* リリース 3 の Content Tracker およびコンテンツ・トラッキング・レポートのコンポーネントの新機能および拡張機能について説明します。

❖ **検索関連情報用のカスタム・メタデータ・フィールド:**

スナップショット機能を使用すると、アクティビティ・メトリックを、コンテンツ・アイテムの使用状況情報を移入可能なカスタム・メタデータ・フィールドにリンクできます。アクティビティ・メトリックによって収集されたデータには、2 つの異なる期間における最新アクセスの日付およびアクセス数が含まれます。収集されたデータは、様々な方法で使用できます。たとえば、先週最も人気の高かったコンテンツまたは最も多く表示されたコンテンツに従って、検索結果を並べ替えることができます。詳細は、3-11 ページの「「Snapshot」タブ」を参照してください。

- **チェックイン操作をアクセス・アクティビティとしてカウント :**

  コンテンツ・アイテムがチェックインされると、Content Server の DocMeta データベース表の「Last Access」フィールドは最初は空です。データ・リダクションの実行が完了すると、「Last Access」フィールドが最新アクセスの日時で更新されます。アクセスが発生していない場合は、チェックインの日時で更新されます。オプションの自動ロード機能を使用すると、コンテンツ・アイテムの「Last Access」フィールドのタイムスタンプが正確になるように、既存のコンテンツに対する最終アクセス・アクティビティ・メトリックを更新できます。詳細は、3-11 ページの「「Snapshot」タブ」の「Autoload」チェック・ボックス（3-14 ページ）を参照してください。

- **拡張サービス・ロギングによる柔軟性の向上 :**

  拡張サービス・ロギング機能を使用すると、ほとんどの Content Server サービスからのデータを、結合された出力データベース表（SctAccessLog）にマップおよび記録できます。つまり、サービスのコールを記録するのみでなく、それらのサービスに関連する特定のデータ値を追跡することもできます。詳細は、3-16 ページの「「Services」タブ」および 5-3 ページの「拡張サービス・コール・トラッキング機能」を参照してください。

- **失敗したユーザー認証 / 認可に対する監査証跡 :**

  コンテンツ・トラッキング・レポートには、システムまたは権限で保護されたコンテンツへの失敗したアクセス試行を監視できる監査機能が追加されました。セキュリティ違反の試行の分析に役立つ 2 つのレポートが使用可能です。これらのレポートには、失敗したユーザー・ログオンと、セキュアなコンテンツ・アイテムへの失敗したアクセスが示されます。この情報は、システムおよびコンテンツのセキュリティを確実にするために非常に重要です。詳細は、4-21 ページの「ユーザー認証 / 認可の管理および監査」を参照してください。

- **ユーザーのロール / アカウント権限に基づいてフィルタ処理されたレポート結果 :**

  このバージョンのコンテンツ・トラッキング・レポートでは、レポートをセキュア・モードまたは非セキュア・モードで生成することを選択できます。つまり、リクエストしたユーザーのロールおよびアカウント権限に基づいて、レポートの検索結果をフィルタ処理できるようになりました。生成されたレポートに含まれるコンテンツ・アイテムを制限するには、Content Server の検索結果を制限するときの基準と同じ基準を使用できます。詳細は、4-23 ページの「セキュリティ・チェックおよび問合せ結果」を参照してください。

- **外部ユーザー・アクセス・データと内部ユーザー・アクセス・データの両方をレポートに挿入 :**

  このバージョンの Content Tracker およびコンテンツ・トラッキング・レポートでは、外部で認証されたユーザーのロールおよびアカウント情報が、Content Server の UserSecurityAttributes データベース表に記録されます。その結果、2 つの事前定

義レポート（「Top Content Items by User Role」および「Users by User Role」）には、外部ユーザーによるコンテンツ・アイテム・アクセス・アクティビティが含まれます。詳細は、A-10 ページの「外部ユーザーおよびコンテンツ・アイテム・トラッキング」を参照してください。

- **拡張サービス・ロギング用のフィールド・マップをデバッグするための DataBinder ダンプ機能 :**

  拡張サービス・ロギング機能を使用する場合、フィールド・マップを設計およびデバッグする際に役立つ DataBinder ダンプ機能が使用可能です。この機能を使用すると、Content Tracker で DataBinder オブジェクトをダンプ・ファイルに書き込むことができ、サービス・イベントの記録時に使用可能なデータを確認できます。詳細は、B-4 ページの「DataBinder ダンプ機能」を参照してください。

- **Web サイト・アクセス・アクティビティ（Site Studio）:**

  このバージョンでは、Site Studio 固有のデータの生成および分析に使用できる事前定義レポートがあります。1 つのレポートに、Web サイト・ページからのコンテンツ・アクセスの要約が示されます。別のレポートに、Web サイト・ページへのアクセスの要約が示されます。詳細は、4-21 ページの「Site Studio の Web サイト・アクティビティ・レポート作成」を参照してください。

CONTENT TRACKER の用語

Content Tracker およびコンテンツ・トラッキング・レポートを使用する際は、次の用語を理解している必要があります。

- **データ・コレクション :** プログラムを使用してコンテンツ・アクセス情報を収集し、情報をイベント・ログ・ファイルに書き込むこと。
- **データ・リダクション :** データ・コレクションからの情報を処理してデータベース表にマージすること。
- **データ・エンジン・コントロール・センター :** データ・エンジンのユーザー制御機能にアクセスするためのアプレット・インタフェース。データ・エンジン・コントロール・センターは、データ・コレクションを有効化、スケジュールおよび監視する場合に使用されます。また、ユーザー・アクティビティとサービス・コールに関するデータを収集および管理する場合にも使用されます。
- **Collection:** データ・コレクションを有効化するために使用するタブ。
- **Reduction:** データ・リダクション（データをデータベース表内にマージすること）を停止および開始するために使用するタブ。
- **Schedule:** 自動データ・リダクションを有効化するために使用するタブ。

- **Snapshot:** アクティビティ・メトリックを有効化するために使用するタブ。また、スナップショットという語は、特定の時点で特定のコンテンツ・アイテムにアクセスしたユーザーを特定する瞬間的な履歴情報を示す場合に使用されます。
- **Services:** 記録される Content Server サービス・コールを追加、構成および編集するために使用するタブ。また、このタブは、特定のサービスに対して記録される特定のイベント詳細を定義する場合にも使用します。
- **サービス定義 :** サービス・コール構成ファイル（SctServiceFilter.hda）内の ResultSet 構造。記録される各 Content Server サービス・コールを定義するエントリが含まれます。サービス定義 ResultSet は、ServiceExtraInfo という名前です。
- **ServiceExtraInfo ResultSet:** 「サービス定義」を参照。
- **サービス・エントリ :** 記録される各 Content Server サービス・コールを定義する、サービス定義 ResultSet（ServiceExtraInfo）内のエントリ。ServiceExtraInfo ResultSet には、記録されるサービスごとにサービス・エントリが 1 つずつ含まれます。
- **フィールド・マップ :** サービス・コール・データおよび特定のデータ記録場所を定義する、サービス・コール構成ファイル（SctServiceFilter.hda）内の 2 次的な ResultSet。
- **最頻アクセス・コンテンツ・アイテム :** システム内で最もアクセス頻度の高いコンテンツ・アイテム。
- **コンテンツ・ダッシュボード :** 特定のコンテンツ・アイテムのアクセスに関する概要情報が示された HTML ページ。

一般的な制限事項

Content Tracker は、ほとんどのハードウェアおよびネットワーク構成でサポートされます。ただし、ハードウェアとソフトウェアの組合せによっては、特別な考慮が必要となります。次のような制限事項がすでに報告されています。

- 単一のサーバーにインストールされた複数ノードのクラスタを使用するアーキテクチャは、追跡およびレポート生成に対してサポートされていません。2-18 ページの「シングルボックス・クラスタにおける追跡の制限事項」を参照してください。
- 静的 URL を介して、または WebDAV によってリクエストされたコンテンツの正確なアクセス数が保証されない場合があります。2-18 ページの「静的 URL および WebDav に関連する追跡の制限事項」を参照してください。
- Content Server データベースとして Oracle または DB2 を使用している場合は、メタデータ値で大 / 小文字が区別されます。4-3 ページの「Oracle および DB2 の大 / 小文字の区別」を参照してください。

- Content Server インスタンスに対してアクセス制御リスト（ACL）が有効になっている場合、コンテンツ・トラッキング・レポートのセキュア・モードが機能しません。4-4 ページの「アクセス制御リストおよびコンテンツ・トラッキング・レポートのセキュア・モード」を参照してください。
- Content Server データベースとして Oracle を使用している場合、別名を使用して列名を表示するには、追加のカスタマイズ済ファイル構成が必要になります。4-16 ページの「カスタム・レポート問合せおよび Oracle」を参照してください。

一般的な考慮事項

現行バージョンの Content Tracker およびコンテンツ・トラッキング・レポートのコンポーネントには、次の一般的な考慮事項が適用されます。

- **ブラウザのハング :**

  データ・エンジン・コントロール・センターの実行中に Content Server が終了した場合、ブラウザもハングすることがあります。この問題は、ハングしたブラウザ・ウィンドウを閉じると簡単に解決します。

- **ローカル時間と GMT:**

  新しい構成パラメータによって、ユーザー・アクセス時間の記録にグリニッジ標準時（GMT）ではなくローカル時間を使用できます。

  - **SctUseGMT=true** を設定すると、GMT を使用するように Content Tracker が構成されます。
  - **SctUseGMT=false** を設定すると、ローカル時間を使用するように Content Tracker が構成されます。これがデフォルト設定です。

  新規の Content Tracker インストールを実行する場合、SctUseGMT にデフォルト設定を使用すると、ユーザー・アクセスはローカル時間で記録されます。以前のバージョンの Content Tracker をアップグレードする場合、SctUseGMT にデフォルト設定を使用すると、アクセス時間が 1 回前に戻り（地域によっては先に進み）ます。また、年 2 回のサマー・タイム実施に対応するため、記録されるユーザー・アクセス時間に中断が生じます（ローカル時間を使用しているかどうか、および地域によって異なります）。

表記規則

- *<install_dir>/* という表記は、製品がインストールされているシステム上の場所を参照するために使用されます。
- 文章内でファイル名とファイル・パスを示す場合は、*<install_dir>*/config/ ディレクトリの config.cfg ファイル、のように表記します。
- スラッシュ（/）は、パス名のディレクトリ・レベルの区切りとして使用されます。これは、ローカルの Windows ファイル・システムまたは UNIX システム上のファイルを表す場合に適用されます。ディレクトリ名の末尾には常にスラッシュが付きます。

このガイドでは次の表記規則を使用します。

記号	説明
	これは**注意**です。情報に対し、特に注意を喚起するために使用されます。
	これは**技術ヒント**です。タスクを容易にするために使用可能な情報を示すために使用されます。
	これは**重要な**通知です。必要な手順または必要な情報を示すために使用されます。
	これは**警告**です。データの損失または重大なシステム問題の原因となる可能性がある情報を示すために使用されます。

2

操作概要

概要

この章の内容は次のとおりです。

CONTENT TRACKER について

Content Tracker では、コンテンツ・アイテムの消費パターンに関する情報が取得されます。毎日、外部ユーザーと内部ユーザーの両方のアクティビティ情報が収集されます。これには、エンド・ユーザーが直接またはポータルや Web サイトなどの外部アプリケーションを介して Content Server からアクセスしたコンテンツの追跡が含まれます。

情報は、Content Server Web フィルタ・ログ・ファイル、Content Server データベース、およびその他の外部アプリケーション（ポータルや Web サイトなど）から収集されます。具体的なデータには、日付、時刻、コンテンツ ID、現在のメタデータ、ユーザー名、ユーザーに関するプロファイル情報、Content Server サービス・コールなどがあります。

データが収集されると、Content Tracker によってイベント情報が結合、分析および合成され、要約されたアクティビティがデータベース表にロードされます。リダクションの完了後、このデータをレポート作成目的で使用できるようになります。Content Tracker Report Generator のメイン・ページを使用して、コンテンツ使用状況傾向を示すレポートを生成できます。これはシステムの使用状況の把握に役立つため、コンテンツ管理の向上につながります。

CONTENT TRACKER のデータ・フロー

Content Tracker では、動的および静的なコンテンツ・アクセスやサービス・コールなどのイベント情報が収集されます。データの収集には、複数のメカニズムが使用されます。

- Web サーバー・フィルタ・プラグイン（2-5 ページ）：

  静的 URL からデータ値が収集され、RAW データ・ファイルに記録されます。

- サービス・ハンドラ・フィルタ（2-5 ページ）：

  Content Server サービス・リクエストが調査され、その中の特定の詳細がリアルタイムで直接 SctAccessLog 表に書き込まれます。SctServiceFilter.hda ファイルにリストされているサービスのみが記録されます。

- Content Tracker ロギング・サービス（2-6 ページ）：

  適切に構成されたアプリケーションによって生成されたイベント情報を記録するために使用されます。

この項の内容は次のとおりです。

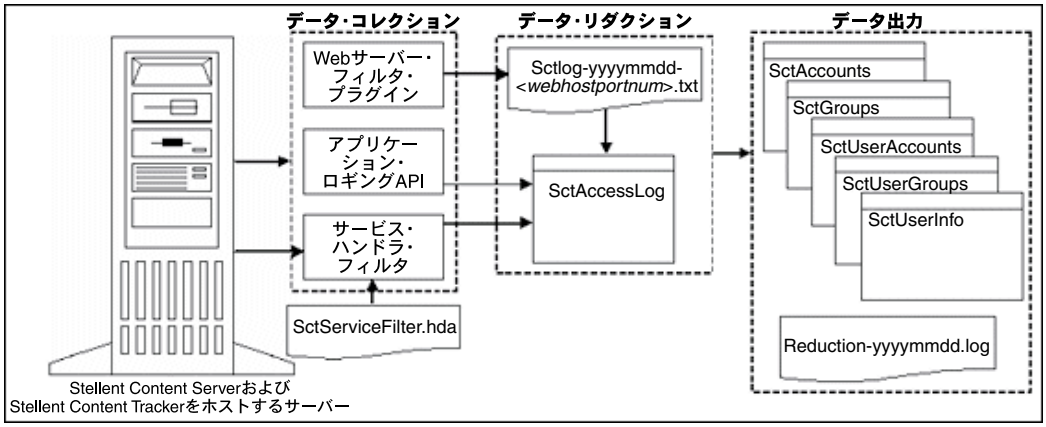
- データ・リダクション・プロセス（2-2 ページ）
- アクティビティ・メトリックを使用するデータ・リダクション・プロセス（2-3 ページ）

データ・リダクション・プロセス

データ・リダクション・プロセス中、静的 URL 情報が RAW データ・ファイルから抽出され（2-7 ページの「Content Tracker イベント・ログ」を参照）、すでに SctAccessLog 表に格納されているサービス情報と結合されます（2-8 ページの「結合された出力表」を参照）。

このリダクション・プロセスでは、次の処理が実行されます。

- 静的 URL コンテンツ・アクセスのアクセス情報がサービス詳細と結合されます。
- レポート作成期間中にアクティブであったユーザー・アカウントに関する情報が要約されます。この情報はロールアップされ、Content Tracker のユーザー・メタデータ・データベース表に書き込まれます。2-13 ページの「メタデータ取得」を参照してください。



アクティビティ・メトリックを使用するデータ・リダクション・プロセス

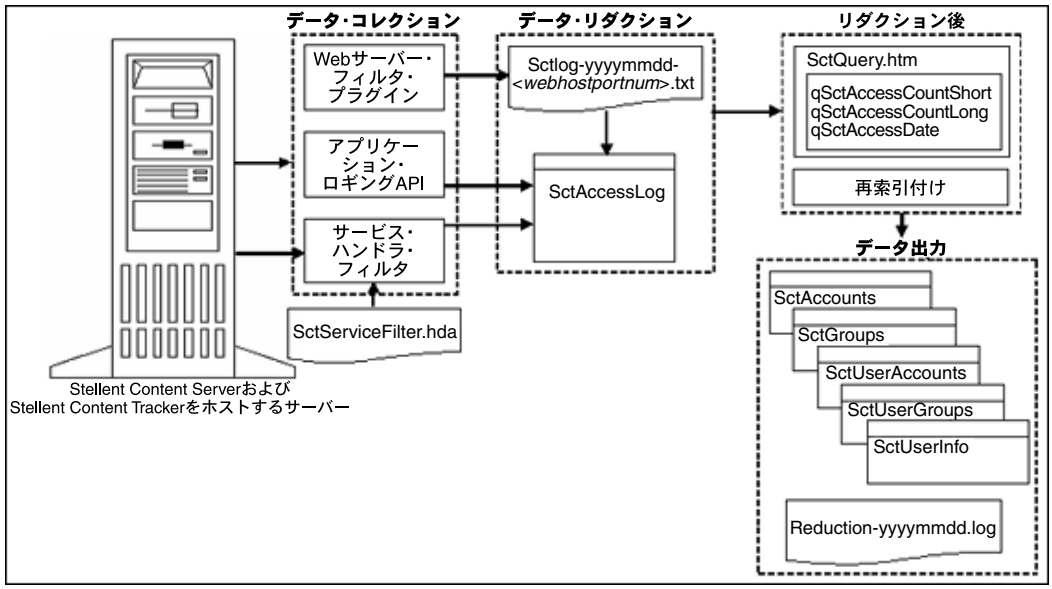
Content Tracker には、検索関連データを選択的に生成してカスタム・メタデータ・フィールドに格納するためのオプションが備わっています。スナップショット機能によって、アクティブにするアクティビティ・メトリックを選択できます。記録されたデータには、コンテンツ・アイテムの人気度を示すコンテンツ・アイテム使用状況情報が含まれます。

スナップショット機能およびアクティビティ・メトリックをアクティブにした場合、リダクション処理フェーズに続いて、カスタム・メタデータ・フィールドの値が更新されます。ユーザーがコンテンツ・アイテムにアクセスすると、適用可能な検索関連メタデータ・フィールドの値がそれに応じて変わります。その後、リダクション後の手順で、Content Tracker により、適用可能な SQL 問合せを使用して、レポート作成期間中にアクセスされたコンテンツ・アイテムが特定されます。

Content Tracker では、適用可能なデータベース表メタデータ・フィールドが新しい値で更新され、再索引付けサイクルが開始されます。ただし、再索引付けされるのは、アクセス・カウント・メタデータ値が変更されたコンテンツ・アイテムのみです。スナップショット機能、ユーザー・インタフェース画面、およびアクティビティ・メトリックのアクティブ化の詳細は、3-11 ページの「「Snapshot」タブ」を参照してください。アクティビティ・メトリックの SQL 問合せおよびそのカスタマイズ方法の詳細は、A-8 ページの「アクティビティ・メトリックの SQL 問合せ」を参照してください。

リダクション後の処理手順は、次の処理を実行するために必要です。

- 影響を受けるコンテンツ・アイテムごとにアクティビティ・メトリックを処理して表を作成し、割り当てられたカスタム・メタデータ・フィールドにデータをロードします。
- アクティビティ・メトリック値が変更されたコンテンツ・アイテムに対して再索引付けサイクルを開始します。これによって、確実にデータが検索索引に含まれるため、検索結果の選択および並替え用にアクセスできるようになります。



データ・コレクション

Content Tracker のデータ・コレクションには、静的 URL 参照および Content Server サービス・コール・イベントからの情報の収集が含まれます。どちらのタイプのデータも、結合された出力表（SctAccessLog）に記録されます。ただし、サービス・コールはリアルタイムでログに挿入されますが、静的 URL 情報は最初に（手動またはスケジュール実行で）リダクション・プロセスを実行する必要があります。

Content Tracker データの収集には、次のメカニズムが使用されます。

- Web サーバー・フィルタ・プラグイン（2-5 ページ）
- サービス・ハンドラ・フィルタ（2-5 ページ）
- Content Tracker ロギング・サービス（2-6 ページ）

サービス・ハンドラ・フィルタ

Content Server サービス・ハンドラ・フィルタは、主要な Content Tracker データ・コレクション・メカニズムです。このフィルタによって、Content Tracker は Web サーバー経由の動的コンテンツ・リクエストに関する情報や、その他のタイプの Content Server アクティビティ（たとえば、アプリケーションからのコールなど）を取得できます。サービス・リクエスト詳細は、サービス・コールに付随する DataBinder から取得され、情報は結合された出力表（SctAccessLog）にリアルタイムで格納されます。SctAccessLog 表の詳細は、2-8 ページの「結合された出力表」を参照してください。

記録する Content Server サービス・コールを指定するための、ユーザーが変更できる構成ファイルがあります。このファイル（SctServiceFilter.hda）では、記録されるサービスにつきサービス定義エントリが 1 つずつ含まれる ResultSet 構造が使用されています。拡張サービス・ロギング機能を使用している場合、SctServiceFilter.hda ファイルには、様々なサービス定義エントリに対応するフィールド・マップも含まれます。3-16 ページの「「Services」タブ」を参照してください。サービス・ハンドラ・フィルタを使用してサービス・コールを構成する方法の詳細は、第 5 章「サービス・コール構成」を参照してください。

注意 : SctServiceFilter.hda ファイルに含まれる ResultSet の名前は、ServiceExtraInfo です。この ResultSet には、記録されるサービスを定義する 1 つ以上のサービス・エントリが含まれます。拡張ロギング機能をサポートするために、追加の ResultSet が使用されます。これらは、フィールド・マップ ResultSet と呼ばれます。追加のデータ値を追跡する場合、そのサービスの SctServiceFilter.hda ファイル内に対応するフィールド・マップ ResultSet が存在している必要があります。フィールド・マップ ResultSet は、関連するサービスのデータ・フィールド、場所およびデータベース宛先列を定義します。

注意 : サービス・ハンドラ・フィルタを介して記録されるサービスと、Content Tracker ロギング・サービスを介して記録されるサービスとの間に、重複や競合はないはずです。サービスの名前が Content Tracker サービス・ハンドラ・フィルタ・ファイルに指定されていれば、このようなサービスは自動的に記録されるため、Content Tracker ロギング・サービスによりこの処理が行われる必要はありません。しかし、Content Tracker ではこのような重複の回避処理は試行されません。

Web サーバー・フィルタ・プラグイン

静的 URL を介して取得された管理対象コンテンツは、通常、Content Server サービスを起動しません。したがって、Content Tracker Web サーバー・フィルタ・プラグインによってアクセス・イベント詳細（静的 URL 参照）が収集され、RAW イベント・ログ（sctlog ファイル）に記録されます。これらのファイル内の情報は、サービス・コール・データとともに、結合された出力表（SctAccessLog）に挿入される前に、明示的なリダクションを（対話式またはスケジュール実行で）実行する必要があります。

sctlog ファイルの詳細は、2-7 ページの「Content Tracker イベント・ログ」を参照してください。SctAccessLog 表の詳細は、2-8 ページの「結合された出力表」を参照してください。

Content Tracker ロギング・サービス

Content Tracker ロギング・サービスは、URL を介して直接、またはサービス・スクリプト内のアクションとして呼び出すことのできる単一サービス・コールです。また、executeService() 関数を使用して、IdocScript から呼び出すこともできます。呼出し元アプリケーションによって、記録する必要のある付随のサービス DataBinder 内のすべてのフィールドが設定されます。これには、Content Tracker サービス・フィルタ構成ファイル（SctServiceFilter.hda）にリストされている記述フィールドが含まれます。Content Tracker ロギング・サービスを使用してサービスを構成する方法の詳細は、第 5 章「サービス・コール構成」を参照してください。

注意 : サービス・ハンドラ・フィルタを介して記録されるサービスと、Content Tracker ロギング・サービスを介して記録されるサービスとの間に、重複や競合はないはずです。サービスの名前が Content Tracker サービス・ハンドラ・フィルタ・ファイルに指定されていれば、このようなサービスは自動的に記録されるため、Content Tracker ロギング・サービスによりこの処理が行われる必要はありません。しかし、Content Tracker ではこのような重複の回避処理は試行されません。

データ・リダクション

Content Tracker データ・リダクション中、Web サーバー・フィルタ・プラグインによって取得された静的 URL 情報が、サービス・コール・データとともに、マージされて出力表（SctAccessLog）に書き込まれます。さらに、リダクション時に、Content Tracker ユーザー・メタデータ・データベース表が、静的 URL アクセスから収集された情報、およびレポート作成期間中に収集されたサービス・コール・イベント・レコードから収集された情報で更新されます。

データ・リダクション処理では、Content Tracker によって次のものが使用されます。

- Content Tracker イベント・ログ（2-7 ページ）
- 結合された出力表（2-8 ページ）

Content Tracker イベント・ログ

Content Tracker Web サーバー・フィルタ・プラグインによってアクセス・イベント詳細（静的 URL 参照）が収集されると、情報が RAW イベント・ログ（sctLog ファイル）に記録されます。これらのファイル内の情報は、サービス・コール・データとともに、結合された出力表（SctAccessLog）に挿入される前に、明示的なリダクションを（対話式またはスケジュール実行で）実行する必要があります。

Content Tracker では、様々なイベント・ログ・タイプと、複数の Web サーバーからなる構成に対応するために、複数の入力ファイルがサポートされています。このため、Web サーバー・フィルタ・プラグイン・インスタンスごとに、Content Tracker イベント・ログ用のファイル名接尾辞としてそれぞれ固有のタグが使用されます。固有の識別接尾辞は、Web サーバー・ホスト名とサーバー・ポート番号で構成されます。リダクション・プロセスで、sctLog-yyyymmdd-<*myhostmyport*>.txt という名前の複数の RAW イベント・ログが検索され、マージされます。これらの RAW イベント・ログは、個別に処理されます。

この項の内容は次のとおりです。

コンテンツ・アクセス・エントリ内に記録されるユーザー名

RAW イベント・ログ・エントリを調べると、ユーザーが Content Server にログインしていても、Content Tracker によってコンテンツ・アクセス・イベントのユーザー名が取得されていないことがあります。たとえば、ログインしているユーザーが検索を実行し、アイテムのコンテンツ情報を表示し、Web ロケーション・リンクをクリックしたとします。RAW イベント・ログ・エントリには、ユーザー名を除く情報が含まれます。

この場合に、アイテムは静的 URL リクエストを介してアクセスされています。また、通常、Web サーバーによってユーザーの資格証明の送信を要求されないかぎり、ブラウザにユーザー名は表示されません。特に、アイテムがパブリック・コンテンツの場合、Web サーバーはユーザーの資格証明の送信をブラウザに要求しないため、URL にアクセスするユーザーは不明となります。

Content Tracker ですべてのドキュメント・アクセスについてユーザー名が記録されるようにするには、すべてのコンテンツ・アイテム・アクセスに対してユーザー・ログインが必要になるようにシステムを構成する必要があります。このためには、コンテンツをゲスト・ロールに対してアクセス不可能にしておく必要があります。つまり、コンテンツがパブリックでない場合、アイテムにアクセスするにはユーザーの資格証明が必要になります。これによって、ユーザー名は必ず RAW イベント・ログ・エントリに記録されます。

リダクション後のファイル記憶域

「new」サイクルの RAW データ・ログ・ファイルが縮小されると、データ・エンジンによってデータ・ファイルが次のサブディレクトリに移動されます。

- <*install_dir*>/custom/ContentTracker/data/recent/yyyymmdd/

  recent/ ディレクトリに格納可能なデータ・セットのデフォルト数は、入力データ・ログ・ファイルのうち 5 セット（日付）です。

- <*install_dir*>/custom/ContentTracker/data/archive/yyyymmdd/

  archive/ ディレクトリには、「recent」サイクルから移動されたすべての入力データ・ログ・ファイルが格納されます。

RAW データ・ファイルが縮小されると、別のファイル（*reduction_ts-yyyymmdd.txt*）がタイムスタンプ・ファイルとして生成されます。RAW データ・ファイル処理のためのリダクション・サイクル状態の詳細は、3-4 ページの「「Reduction」タブ」を参照してください。

結合された出力表

SctAccessLog 表には、静的および動的なすべてのコンテンツ・アクセス・イベント・レコードのエントリが含まれます。表の列には、タイプに従ってタグが付けられます。

- S は、サービス・コールについて記録されたレコードを表します。
- W は、静的 URL リクエストについて記録されたレコードを表します。

SctAccessLog 表は、レポート作成期間中のイベントにつき 1 行ずつ使用して編成されます。

注意 : デフォルトでは、Content Tracker によって GIF、JPG、JS、CSS、CAB および CLASS ファイル・タイプへのアクセスは記録されません。つまり、GIF、JPG、JS、CSS、CAB および CLASS が関連する Web アクティビティは、Web サーバー・フィルタ・プラグインのイベント・ログ・ファイルのエントリにはなりません。したがって、これらのファイル・タイプのエントリは、データ・リダクション後、結合された出力表（SctAccessLog）に挿入されません。

これらのファイル・タイプのロギング・ステータスを変更するには、<*install_dir*>/custom/ContentTracker/resources/ ディレクトリにある sct.cfg ファイル内で目的のファイル・タイプを有効化する必要があります。これらのファイル・タイプのロギングを有効化するには、SctIgnoreFileTypes（A-3 ページ）構成変数（gif、jpg、js、css）のデフォルト設定を調整してください。デフォルト設定では、これらのファイル・タイプは除外されます。これらのファイル・タイプの一部のみを含めるには、リストから目的のファイル・タイプをそれぞれ削除します。この変更を有効にするには、Web サーバーおよび Content Server を再起動する必要があります。

注意 : Content Tracker Web サーバー・フィルタ・プラグインでは、ユーザー・コンテンツの URL と、Content Server ユーザー・インタフェースによって使用される URL を区別できません。このため、client.cab などの UI オブジェクトへの参照が静的アクセス・ログ内に含まれることがあります。このような誤検出をなくすには、Content Tracker フィルタ・プラグインによって無視されるディレクトリ・ルートのリストを定義できます。

ディレクトリのリストは、<*install_dir*>/custom/ContentTracker/resources/ ディレクトリにある sct.cfg ファイル内の SctIgnoreDirectories（A-3 ページ）構成変数に格納されます。このリストによって、ユーザー・インタフェース・オブジェクト参照の（全部ではないにしても）ほとんどが排除されます。

SctIgnoreDirectories 値の内容を手動で変更して、コンテンツを無視する必要のあるすべてのディレクトリをリストできます。次の場合は、デフォルト値を変更する必要があります。

- ユーザー・コンテンツとともに記録する UI オブジェクトにアクセスする場合
- 記録するディレクトリと、ログから除外するディレクトリを変更する場合

次の表に、SctAccessLog 表の各レコードについて収集される情報を示します。

列名	タイプ / サイズ	フィールド定義
SctDateStamp	datetime	データが収集されたローカル日付 : YYYYMMDD（顧客のロケーションおよびイベントが発生した時間によっては、eventDate に記録された日付と異なる場合がある）。時刻は 00:00:00 に設定される。 日付ソース : 内部
SctSequence	int/8	エントリ・タイプに固有のシーケンス 日付ソース : 内部 クローニング元 : Revisions.dID
SctEntryType	char/1	エントリ・タイプ : "W" または "S" 日付ソース : 内部 クローニング元 : Revisions.dReleaseState
eventDate	datetime	リクエストが完了した GMT 日時（顧客のロケーションおよびイベントが発生した時間によっては、SctDateStamp に記録された日付と異なる場合がある）
SctParentSequence	integer	ツリー内の最外部のサービス・イベントのシーケンス（ある場合）
c_ip	varchar/15	クライアントの IP
cs_username	varchar/255	クローニング元 : Revisions.dDocAuthor

列名	タイプ / サイズ	フィールド定義
cs_method	varchar/10	"GET"
cs_uriStem	varchar/255	URI のステム
cs_uriQuery	varchar/[maxUrlLen]	問合せの一部（"IdcService=GET_FILE&dID=42..." など）
cs_host	varchar/255	Content Server のサーバー名
cs_userAgent	varchar/255	クライアント・ユーザー・エージェントの ID
cs_cookie	varchar/[maxUrlLen]	現在の Cookie
cs_referer	varchar/[maxUrlLen]	このリクエストに至る URI
sc_scs_dID	int/8	dID データソース : 問合せから、または URL から導出（逆引き参照） クローニング元 : Revisions.dID
sc_scs_dUser	varchar/50	dUser データソース : サービス DataBinder "dUser" クローニング元 : Revisions.dDocAuthor
sc_scs_idcService	varchar/255	IdcService の名前（例 : GET_FILE） データソース : 問合せまたはサービス DataBinder "IdcService"
sc_scs_dDocName	varchar/30	dDocName データソース : サービス DataBinder "dDocName" の問合せ クローニング元 : Revisions.dDocName
sc_scs_callingProduct	varchar/255	任意の識別子 データソース : SctServiceFilter 構成ファイルまたはサービス DataBinder "sctCallingProduct"
sc_scs_eventType	varchar/255	任意の識別子 データソース : SctServiceFilter 構成ファイルまたはサービス DataBinder "sctEventType"
sc_scs_status	varchar/10	サービス実行ステータス データソース : サービス DataBinder "StatusCode"

列名	タイプ / サイズ	フィールド定義
sc_scs_reference	varchar/255	"web"、"native"、"sdc_url" 値はアクセスされるファイルの形式を表す（"web" は変換済ファイル（PDF）、"native" は実際の元ファイル、および "sdc_url" は HTML）。 データソース : アルゴリズムを使用して問合せパラメータまたは ServiceFilter 構成ファイル
comp_username	varchar/50	計算されたユーザー名。サービスの場合、UserData サービス・オブジェクトから取得、あるいは HTTP_INTERNETUSER、REMOTE_USER または dUser。静的 URL の場合、認可ユーザーまたはインターネット・ユーザーから取得。
comp_validRef	char/1	アクセスが Web 参照（W）であった場合、ispromptlogin と isaccessdenied の両方が NULL であり、リダクション時に静的 URL が存在していれば、"1"。アクセスがサービス・コール（S）で、sc_scs_status フィールドが NULL の場合も "1"。 リダクション時に静的 URL が存在していなかった場合、ユーザー・ログインが失敗した場合、またはログオンは成功したがユーザーにオブジェクトの表示権限がなかった場合、"NULL"。 参照されるオブジェクトが存在しているかどうか、およびリクエスト側のユーザーに対して使用可能であるかどうかを示す。
sc_scs_isPrompt	char/1	true の場合は "1" データソース : プラグイン immediateResponseEvent フィールド "ispromptlogin" クローニング元 : Revisions.dReleaseState
sc_scs_ isAccessDenied	char/1	true の場合は "1" データソース : プラグイン immediateResponseEvent フィールド "isaccessdenied" クローニング元 : Revisions.dReleaseState
sc_scs_inetUser	varchar/50	インターネット・ユーザー名（セキュリティ問題の場合） データソース : プラグイン immediateResponseEvent フィールド "internetuser" クローニング元 : Revisions.dDocAuthor
sc_scs_authUser	varchar/50	認可ユーザー名（セキュリティ問題の場合） データソース : プラグイン immediateResponseEvent フィールド "auth-user" クローニング元 : Revisions.dDocAuthor

列名	タイプ / サイズ	フィールド定義
sc_scs_ inetPassword	varchar/8	インターネット・パスワード（セキュリティ問題の場合） データソース : プラグイン immediateResponseEvent フィールド "internetpassword"
sc_scs_ serviceMsg	varchar/255	Content Server サービス完了ステータス データソース : サービス DataBinder "StatusMessage"
extField_1 ～ extField_10	varchar/255	拡張サービス・トラッキング機能で使用する汎用目的の列。 フィールド・マップ ResultSet 内では、DataBinder フィールドがこれらの列にマップされる。

データ出力

Content Tracker では、静的 URL アクセスと同様にユーザー・メタデータのスナップショットが作成されます。また、サービス・コールも記録されて、結合された出力表にリアルタイムで書き込まれます。静的 URL 情報を処理して、結合された出力表に追加するためには、データ・リダクションが必要です。さらに、データ・リダクション・プロセスの結果、関連する Content Tracker ユーザー・メタデータ・データベース表は、静的 URL データおよびサービス・コール・データの処理から導出された情報で更新されます。

Content Tracker リダクション・プロセスでは、次のものが生成されます。

- メタデータ取得（2-13 ページ）
- リダクション・ログ・ファイル（2-17 ページ）

メタデータ取得

静的および動的なコンテンツ・アクセス・リクエスト情報の他に、すべてのメタデータ・フィールドが、コンテンツ・トラッキング・レポート・コンポーネントによって生成されるレポートで使用できるようにアクセス可能になります。次のメタデータが記録されます。

- コンテンツ・アイテム・メタデータ（2-13 ページ）
- ユーザー・メタデータ（2-13 ページ）

コンテンツ・アイテム・メタデータ

Content Tracker では、コンテンツ・アイテム・メタデータ情報は収集されず、コンテンツ・アイテム・メタデータ用の標準の Content Server メタデータ表が使用されます。つまり、Content Tracker は、必然的に現在のコンテンツ・アイテム・メタデータを反映します。このため、コンテンツ・アイテムがアクセスされた後にコンテンツ・アイテム・メタデータが変更された場合、生成されるレポートは変更済のメタデータを反映します。

ユーザー・メタデータ

データ・リダクション・プロセスの間、Content Tracker ユーザー・メタデータ・データベース表は、レポート作成期間中にアクティブであったユーザーに関して収集された情報で更新されます。これらの表には、履歴的に正確なユーザー・メタデータが保持されます。ユーザー・メタデータ表の名前は、ルート（含まれている情報のクラスを示す）と、Content Tracker 表とネイティブの Content Server 表とを区別するための接頭辞 "Sct" で構成されます。

ユーザー・メタデータ・データベース表の 2 つの完全セットが作成されます。

- プライマリ

  プライマリ表（たとえば、SctUserInfo など）には、「new」および「recent」サイクルにおけるリダクション・データの出力が含まれます。

- アーカイブ

  アーカイブ表（たとえば、SctUserInfoArchive など）には、「archive」サイクルにおけるリダクション・データの出力が含まれます。

リダクション・データ・ファイルが「recent」から「archive」に移行すると、関連付けられた表レコードがプライマリ表からアーカイブ表に移動されます。このため、プライマリ表に余分な行が構築されることがなく、最新データに対して実行された問合せは短時間で完了します。アーカイブ表の行は、削除されません。これらの行は、履歴レコード用の代替ストレージに移動したり、SQL 問合せツールを使用して削除することができます。リダクション・プロセスおよびデータ・サイクルの詳細は、3-4 ページの「「Reduction」タブ」を参照してください。

技術ヒント : アーカイブ表のすべての行を削除する場合は、単に表自体を削除します。これらの表は、Content Server が次に再起動されるときに再作成されます。

注意 : レポートは、アーカイブ・データに対しては実行されません。したがって、「recent」から「archive」に移行したデータは、生成されるレポートに含められません。

次のユーザー・メタデータ表が更新されます。

- SctAccounts 表（2-14 ページ）
- SctGroups 表（2-15 ページ）
- SctUserAccounts 表（2-15 ページ）
- SctUserGroups 表（2-16 ページ）
- SctUserInfo 表（2-16 ページ）

SctAccounts 表

SctAccounts 表には、すべてのアカウントのリストが含まれます。SctAccounts 表は、アカウントにつき 1 行ずつ使用して編成されます。

フィールド名	タイプ / サイズ / フィールド定義
SctDateStamp	datetime データが収集された GMT 日付
dDocAccount	varchar/30 Content Server アカウントの名前

SctGroups 表

SctGroups 表には、リダクション時のすべての現行ユーザー・グループのリストが含まれます。SctGroups 表は、コンテンツ・アイテム・グループにつき 1 行ずつ使用して編成されます。

フィールド名	タイプ / サイズ / フィールド定義
SctDateStamp	datetime データが収集された GMT 日付
dGroupName	varchar/30 コンテンツ・アイテム・グループの名前

SctUserAccounts 表

SctUserAccounts 表には、SctUserInfo 表にリストされていて、かつ現行インスタンス内で定義されているアカウントを割り当てられたユーザーのエントリが含まれます。ユーザーとアカウントの組合せごとに、個別のエントリが存在します。

特殊ですが、Content Tracker によってユーザーのグループおよびアカウント情報が判別されない状況があります。この状況は、複数のプロキシ・インスタンスが存在するプロキシ構成において発生します。現行インスタンスがプロキシの場合、別のプロキシで定義されているアクティブ・ユーザーのグループ情報が、そのユーザーの SctUserGroups 内の単一プレースホルダ行で置換されます。この行には、ユーザー名と、グループの "-" プレースホルダが含まれます。現行インスタンス内で少なくとも 1 つのアカウントが定義されていれば、別のプロキシで定義されているユーザーの SctUserAccounts 内に同様のエントリが作成されます。

SctUserAccount 表は、Content Server ユーザーおよびユーザーのアカウントにつき 1 行ずつ使用して編成されます。

フィールド名	タイプ / サイズ / フィールド定義
SctDateStamp	datetime データが収集された GMT 日付
dUserName	varchar/100 ユーザーの名前。プロキシ・インスタンスに対してローカルの場合、コンテンツ・サーバーの相対 URL（たとえば、cs_2/user1 など）が接頭辞として付加される。

フィールド名	タイプ / サイズ / フィールド定義
Account	varchar/30 ユーザーがアクセス権を持つアカウント名。複数のプロキシを経由する構成におけるプレースホルダ（現行プロキシ・インスタンスに少なくとも 1 つのアカウントが存在する場合）。

SctUserGroups 表

SctUserGroups 表は、データ収集期間中にログオンしたユーザーのみを参照します。Content Tracker がプロキシ Content Server 構成で実行されている場合は、現行インスタンス内で定義されているグループのみがリストされます。たとえば、"joe" という名前のユーザーがマスター・インスタンスで定義され、マスター・インスタンス内でグループ "Public" および "Plastics" へのアクセス権を持つとします。この場合、"joe" がプロキシ・インスタンスにログオンしたが、そのプロキシ内にグループ "Plastics" が定義されていなければ、SctUserGroups には "joe" と "Public" の関連のみが示されます。

SctUserGroups 表は、レポート作成期間中の各アクティブ・ユーザーのユーザー・グループにつき 1 行ずつ使用して編成されます。

フィールド名	タイプ / サイズ / フィールド定義
SctDateStamp	datetime データが収集された GMT 日付
dUserName	varchar/100 ユーザーの名前。プロキシ・インスタンスに対してローカルの場合、コンテンツ・サーバーの相対 URL（たとえば、cs_2/user1 など）が接頭辞として付加される。
dGroupName	varchar/30 ユーザーがアクセス権を持つグループ名。アクセスのタイプ（R、RW など）の区別はされない。

SctUserInfo 表

SctUserInfo 表には、現行インスタンスに既知のすべてのユーザーと、データ収集期間中に現行インスタンスにログオンした別のインスタンスからの追加ユーザーが含まれます。プロキシ構成においては、あるインスタンスに対してローカルなユーザーは通常、他のインスタンスに対して既知（UserAdmin アプリケーションから可視）となります。（この可視性を実現するために、通常、ローカル・ユーザーを追加した後は Content Server インスタンスを再起動する必要があります。）ただし、2 つのインスタンスにおいて 1 つ

のユーザーが同名でローカルに定義されている場合、これらの各インスタンスでローカル・ユーザーのみが可視になります。

たとえば、マスターで定義されているユーザー "sysadmin" は、プロキシの UserAdmin アプリケーションで表示される "sysadmin" ユーザーとは異なります。各プロキシには、それぞれの "sysadmin" ユーザーがローカルに定義されています。この 2 つの異なるユーザーがどちらも同じデータ収集期間にログオンすることも考えられます。たとえば、マスターからのユーザーが "sysadmin" としてログオンし、プロキシからのユーザーが "cs_2/sysadmin" などとしてログオンするような場合です。この場合、cs_2/ がプロキシ・ユーザー名に付加する必要のあるサーバー相対 URL です。この期間について生成される userinfo ファイルには、"sysadmin" と "cs_2/sysadmin" に対して別々のエントリが含められます。

SctUserInfo 表は、Content Server ユーザーにつき 1 行ずつ使用して編成されます。

フィールド名	タイプ / サイズ / フィールド定義
SctDateStamp	datetime データが収集された GMT 日付
dUserName	varchar/100 ユーザーの名前。プロキシ・インスタンスに対してローカルの場合、コンテンツ・サーバーの相対 URL（たとえば、cs_2/user1 など）が接頭辞として付加される。
dUserType	varchar/30 ユーザーのタイプ。ユーザーにタイプがない場合はプレースホルダ。

リダクション・ログ・ファイル

データ・リダクションが実行されると、Content Tracker データ・エンジンによって、<*install_dir*>/custom/ContentTracker/log/ 内にサマリー結果ログ・ファイルが生成されます。リダクション・ログ・ファイルは、reduction-yyyymmdd.log という書式を使用して名前が付けられます。リダクション・ログは、データ・リダクション・プロセス中に発生した診断エラーを診断する際に役立ちます。RAW イベント・ログ・ファイルおよびそれらに対応するリダクション・ログの詳細は、2-7 ページの「Content Tracker イベント・ログ」を参照してください。

追跡の制限事項

現行バージョンの Content Tracker およびコンテンツ・トラッキング・レポートには、次の追跡の制限事項が適用されます。

シングルボックス・クラスタにおける追跡の制限事項

現在、Content Tracker およびコンテンツ・トラッキング・レポートでは、単一サーバーにインストールされた複数ノードのクラスタはサポートされていません。これは、複数のネットワーク・カードがインストールされ、各クラスタ・ノードがそれぞれの IP アドレスを持つ場合でも同じです。この場合、各クラスタ・ノードの Content Server インスタンスは、その IntradocServerPort を固有の IP アドレスにバインドできます。

ただし、指定された IP アドレスに受信プロバイダ ServerPort をバインドできるクラスタ・ノードは、1 つのみです。したがって、すべてのクラスタ・ノードが同じ受信プロバイダ ServerPort を共有し、交替で使用します。その結果、Content Tracker の SctLock プロバイダは、一度に 1 つのクラスタ・ノードでしかドキュメント・アクセスを追跡できません。

静的 URL および WebDav に関連する追跡の制限事項

Content Tracker は、静的 URL を介して、または WebDAV クライアントによってリクエストされたコンテンツについて、正確なアクセス・カウントを保証できません。Content Tracker によって判別されたアクセス・カウントは通常は正確ですが、コンテンツが実際にリクエスト側のユーザーに配信されたかどうか、または配信された場合にコンテンツの特定リビジョンが配信されたかどうかを Tracker で判別できないという例外的な状況もあります。次のような場合は、アクセス・カウントが正確でなくなる可能性があります。

WebDAV 経由で繰返しリクエストされたコンテンツのアクセス・ミス

シナリオ : ユーザーが WebDAV クライアント経由でドキュメントにアクセスした後、同じ方法で同じドキュメントにアクセスしたとします。この場合、ドキュメントに対する最初の WebDAV リクエストのみが記録されます。このようなコンテンツについて報告されるアクセス・カウントは、実際よりも少なくなる傾向があります。

詳細 : WebDAV クライアントは通常、ネットワーク・トラフィックの量を減らすためになんらかの形態のオブジェクト・キャッシングを使用します。ユーザーが特定のオブジェクトをリクエストすると、クライアントはまず、ローカル・ストア内にオブジェクトのコピーが存在しているかどうかを判別します。存在していない場合、クライアントはサーバーに接続し、転送をネゴシエートします。この転送は、COLLECTION_GET_FILE サービス・リクエストとして記録されます。

クライアントにすでにオブジェクトのコピーが存在する場合、クライアントはサーバーに接続して、クライアント・ローカル・コピーが取得された後にオブジェクトが変更されているかどうかを判別します。変更されている場合、新しいコピーが転送され、COLLECTION_GET_FILE サービス詳細が記録されます。

クライアントのオブジェクト・コピーが現行のままである場合、転送は行われず、クライアントは保存済のオブジェクト・コピーをユーザーに表示します。この場合、ユーザーが元のコンテンツの新しいコピーを取得したようであっても、コンテンツ・アイテムはカウントされません。

保存済（失効）静的 URL によるアクセスの誤検出

シナリオ : ユーザーがコンテンツ・ファイルの Web ロケーション（URL）を保存します。その後、コンテンツが改訂されて、保存されている URL が無効になりました。次に、ユーザーが（失効した）URL を介してコンテンツにアクセスしようとして、「Page Cannot be Found」エラー（HTTP 404）を受け取ります。この場合、コンテンツが実際にユーザーに配信されていないのに、Content Tracker によって正常なアクセスとして記録されることがあります。このようなコンテンツについて報告されるアクセス・カウントは、実際よりも多くなる傾向があります。

詳細 : コンテンツ・ファイルの Web ロケーションは、ユーザーが静的 URL を介してコンテンツにアクセスするための手段です。URL 内の特定のファイル・パスは、わずかに異なる 2 つのコンテキストで使用されます。1 つは、Web サーバーが Content Server リポジトリ内でコンテンツ・ファイルを見つける場合で、もう 1 つは、Content Tracker がデータ・リダクション・プロセス中にコンテンツ・ファイルの dID および dDocName を判別する場合です。問題が発生するのは、コンテンツが改訂されて、URL の保存時とアクセス試行時で特定のコンテンツ ID の Web ロケーションが変更された場合です。

たとえば、Word ドキュメントがチェックインされ、その後 XML ドキュメントに改訂された場合、コンテンツの最新リビジョンの Web ロケーションは、

/stellent/groups/public/documents/adacct/xyzzy.doc

から次のように変更されます。

/stellent/groups/public/documents/adacct/xyzzy.xml

ここで、"xyzzy" は割り当てられたコンテンツ ID です。

元のリビジョンは次のように名前変更されます。

/stellent/groups/public/documents/adacct/xyzzy~1.doc

つまり、元の Web ロケーションは静的 URL として機能しなくなります。ただし、元の URL から取得されたコンテンツ ID は最新のリビジョンと一致します。したがって、Web サーバーがリクエストされたファイルをユーザーに配信できなかった場合でも、Content Tracker によってこれがコンテンツ ID"xyzzy" へのアクセスとして報告されます。

保存済の静的 URL によるアクセスについて報告される間違った dID

シナリオ : ユーザーが Web ロケーション（URL）を介してコンテンツにアクセスします。その後、Content Tracker でデータ・リダクション操作が実行される前に、コンテンツが改訂されたとします。この場合、ユーザーに表示されたのは実際の表示内容ではなく最新リビジョンであるとして報告されます。このようなコンテンツについて報告されるアクセス・カウントは、実際よりも新しいリビジョンに関して行われる傾向があります。Content Tracker データ・リダクションを定期的にスケジュールまたは実行することで、このような結果を最小限に抑えることができます。

詳細 : これは、前述の「保存済（失効）静的 URL によるアクセスの誤検出」に関連しています。つまり、Web サーバーでは Web ロケーション全体（たとえば、/stellent/groups/public/documents/adacct/xyzzy.doc など）を使用してコンテンツの検索および配信が行われるのに対し、Content Tracker では ContentID 部分のみを使用して dID および dDocName の値が判別されます。さらに、Content Tracker では、実際のアクセス発生時ではなく、データ・リダクション中にこの判別が行われます。その結果、Content Tracker では、アクセス時に現行であった内容でなく、リダクション時に現行であったリビジョンがユーザーに表示されたとして報告されます。

リビジョンのグループやセキュリティがオリジナルから変更された場合など、この問題がすぐには明らかにならない場合もあります。たとえば、ユーザーが静的 URL を介してドキュメントの "Public" リビジョン 1 にアクセスした場合、その後でドキュメントがリビジョン 2 に改訂され、Content Tracker データ・リダクションの実行前に "Secure" に変更されたとします。この場合、Tracker によって、Secure バージョンがユーザーに表示されたことが報告されます。これは、コンテンツ・ファイル・タイプが変更された場合にも起こる可能性があります。ユーザーが元の .xml バージョンにアクセスした後、データ・リダクションの実行前に .xml バージョンがまったく別の .doc に置き換えられた場合、Tracker によって、実際の .xml ではなく .doc リビジョンがユーザーに表示されたことが報告されます。

3

CONTENT TRACKER の使用

概要

この項の内容は次のとおりです。

概要

インタフェース

タスク

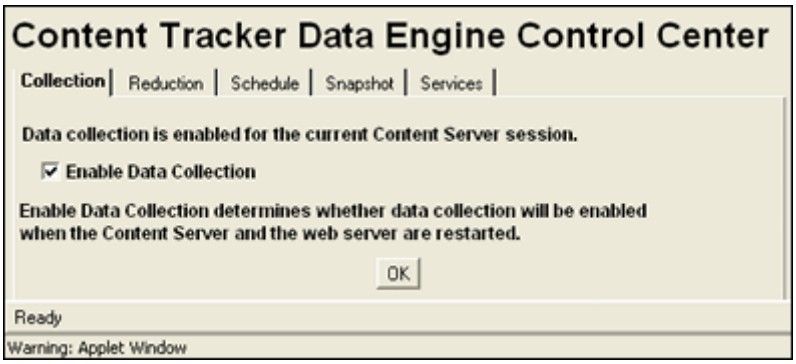
データ・エンジン・コントロール・センター

データ・エンジン・コントロール・センターは、データ・エンジンのユーザー制御機能にアクセスするためのアプレット・インタフェースです。アプレットにアクセスするには、「Administration」トレーの「Content Tracker Administration」リンクをクリックします。次に、結果のページで「Data Engine Control Center」アイコンをクリックします。

このインタフェースを使用すると、次の操作を実行できます。

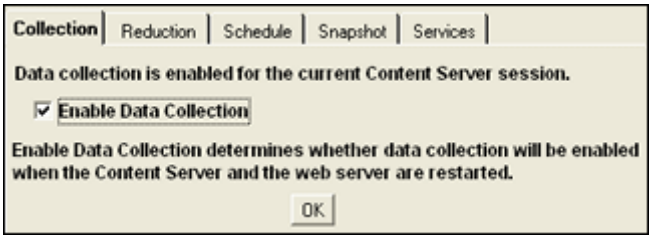
- データ・コレクションの有効化および無効化
- データ・リダクションの開始および停止
- データ・リダクションの進捗状況の監視
- データの削除
- データ・リダクションの自動実行のスケジュール
- アクティビティ・メトリックの有効化と、管理対象コンテンツ・アクセスの検索関連情報の収集

- ❖ 記録されるサービス・コールの追加、構成および編集
- ❖ 特定のサービスに対して記録される特定のイベント詳細の定義



「Collection」タブ

「Collection」タブを使用して、Content Server セッションに対して Web トラフィック・データ・コレクションを有効化します。データ・コレクションを有効化すると、Content Tracker データ・エンジンによって RAW データが収集されて、/data ディレクトリ（*<install_dir>*/custom/ContentTracker/data/）内のログに書き込まれます。これらのログは、リダクション・プロセスで使用される入力の一部を提供するもので、収集プロセスが正常に有効化されているかぎりは蓄積されます。データは、リダクション・プロセスが実行されているかどうかに関係なく蓄積されます。



機能	説明
「Enable Data Collection」チェック・ボックス	このチェック・ボックスを選択すると、現行の Content Server セッションに対してデータ・コレクションが有効化されます。
「OK」ボタン	現行のデータ・コレクション設定を実装します。

重要 : チェック・ボックスのステータスを変更しても、データ・コレクションは即時に有効化または無効化されません。変更を有効にするには、Content Server および Web サーバーを再起動する必要があります。チェック・ボックスの上の文をよく読んで、データ・コレクションが有効化されているかどうかを判断してください。

- 有効化されている場合は、「Data collection is enabled...」という文が表示されます。
- 無効化されている場合は、「Data collection is not enabled...」という文が表示されます。

「Reduction」タブ

「Reduction」タブを使用して、データ・リダクションの手動での開始と停止、データ・リダクション操作の進捗状況の監視、および表の行の生成に使用された RAW データ・ファイルの削除を行います。リダクション中、日付が適切な表に書き込まれ、リダクション・プロセスを反映するログ・ファイルが作成されます。これらのログ・ファイルは、log/ ディレクトリ（*<install_dir>*/custom/ContentTracker/log/）に格納されます。

「Reduction」タブの各行アイテムは、毎日収集および編成される RAW（入力）データです。RAW データは、Web サーバー・フィルタ・プラグインから収集された未処理のデータです。このデータは最終的に、Content Tracker リダクション・プロセスへの入力として使用されます。

データ・リダクションの主な概要は、次のとおりです。

- データ・リダクション・サイクル（3-4 ページ）
- アクセス・モードおよびデータ・リダクション（3-5 ページ）
- イベント・ログのリダクション順序（3-5 ページ）

データ・リダクション・サイクル

縮小された表データは、関連付けられた RAW データが「recent」ステータスから「archive」ステータスに移行すると、プライマリ表から対応するアーカイブ表に移動されます。プライマリ表には「new」サイクルおよび「recent」サイクルにおけるリダクション・データの出力が含まれ、アーカイブ表には「archive」サイクルにおけるリダクション・データの出力が含まれます。

データが縮小されて 1 日経過すると、RAW データは「new」から「recent」に移行します。このように、「new」サイクルは、データが現在の日付のものであり、以前の日付から縮小されていないことを示しています。「recent」サイクルは、データが前日以前のものであり、すでに縮小されていることを示します。

「recent」セットの数が構成済のしきい値に達した場合、手動またはスケジューラによりリダクション・プロセスが実行されると、RAW データは「archive」に移行します（また、SctAccessLog 表の対応する行が SctAccessLogArchive 表に移動されます）。「recent」セットのしきい値の構成方法の詳細は、A-4 ページの「SctMaxRecentCount」を参照してください。リダクション・プロセスが実行されていない場合、RAW データはいつまでも「recent」サイクルのままです。

アクセス・モードおよびデータ・リダクション

ユーザーがコンテンツ・アイテムにアクセスした方法によって、それらのアクセスが SctAccessLog 表に記録される方法が決まります。基本的なユーザー・アクセス・モードは、（実際のネイティブ・ファイルを表示する）サービス・アクセスと（Web ロケーション・ファイルを表示する）静的 URL アクセスの 2 つです。サービスを介してコンテンツ・アイテムがアクセスされると、イベントがリアルタイムで SctAccessLog 表に記録されます。この場合、アクティビティは即時に記録され、リダクション・プロセスには依存しません。

しかし、静的 URL を介してコンテンツ・アイテムがアクセスされると、Web サーバー・フィルタ・プラグインによって静的ログ・ファイルにイベントが記録されます。データ・リダクション・プロセス中、指定された日付の静的ログ・ファイルが収集され、データが SctAccessLog 表に移動されます。この場合、特定の日付についてデータ・リダクションが実行されないと、静的 URL は SctAccessLog に記録されず、これらのアクセスが行われた証拠は残りません。

このため、期間カウントについては、静的アクセスとサービス・アクセスの処理方法の違いを考慮する必要があります（3-11 ページの「「Snapshot」タブ」を参照）。たとえば、ユーザーが土曜日にコンテンツ・アイテムに 2 回アクセスしたとします。1 回は Web ロケーション・ファイルを介して（静的アクセス）、もう 1 回はネイティブ・ファイルを介して（サービス・アクセス）アクセスします。サービス・アクセスは SctAccessLog 表に記録されますが、Web ロケーション・アクセスは SctAccessLog 表に記録されません。

次に、日曜日のデータが縮小された場合、（静的アクセスでなく）サービス・アクセスのみが短期および長期のアクセス・カウント期間のサマリーに含められます。しかし、土曜日のデータも同様に縮小された場合は、サービス・アクセスと静的アクセスの両方が SctAccessLog 表に記録され、短期および長期のアクセス期間に含められます。

イベント・ログのリダクション順序

一般に、生成されるレポートにできるかぎり最新の情報が含められるように、データ・セットは発生時間順に縮小されます。特に、RAW データ・ログ・ファイルが縮小される順序によって、記録およびカウントされるユーザー・アクセス・データの種類が決まります。リダクション中、SctAccessLog 表およびユーザー・メタデータ・データベース表が、RAW データ・ファイルからのデータで更新されます。

スナップショット機能を使用して検索関連情報を収集する場合は、アクティブ化されたアクティビティ・メトリックに関連付けられているメタデータ・フィールドもデータ・リダクション中に更新されます。アクティビティ・メトリックでは、Content Server の DocMeta データベース表に含まれているカスタム・メタデータ・フィールドが使用されます。詳細は、3-11 ページの「「Snapshot」タブ」を参照してください。

様々なデータベース表の情報の最新性は、データ・セットを縮小した順序によって決まります。Content Tracker では常に、リダクション・データ・セット内の適用可能データに従ってアクティビティ・メトリック値が変更されます。通常、アクティビティ・メトリックが予測どおりに進行するように、データ・セットは日付順に縮小されます。実際に、常にデータ値を完全かつ最新に保つためには、毎日データ・リダクションを実行する必要があります。

注意 : データ・セットを順序どおりに縮小しない場合、現行または最新のデータ・セットを再縮小すると、カウントが訂正されます。しかし、データは常に日付順に縮小することをお薦めします。

次のシナリオに、リダクションの順序で格納されるデータがどのような影響を受けるかを示します。

シナリオ 1:

特定の日（たとえば、土曜日と日曜日など）のアクティビティが縮小されていない場合、コンテンツ・アイテムへのアクセス方法によっては、これらの日に発生したアクセスが記録またはカウントされないことがあります（3-5 ページの「アクセス・モードおよびデータ・リダクション」を参照）。同様に、火曜日にコンテンツ・アイテムがアクセスされ、月曜日と水曜日にリダクションが実行された場合、そのコンテンツ・アイテムの最後のアクセスに対して火曜日のアクセスがカウントされないことがあります。

シナリオ 2:

過去数日間でアクセス数が大幅に増加したが、2 週間前からのデータを縮小した場合、コンテンツ・アイテムの長期および短期のアクセス・メトリックは最新のアクティビティを反映しません。この場合、2 週間前からの期間値で本日の値が上書きされます。現在または最新のデータ・セットを縮小すると、カウントが訂正されます。

注意 : リダクションの順序は、「Last Access」日付に逆の影響を及ぼしません。リダクション・データ・セット内の最新のアクセスが Content Server の DocMeta データベース表の「Last Access」値よりも新しい場合にのみ、リダクション・プロセスによって「Last Access」日付が変更されます。

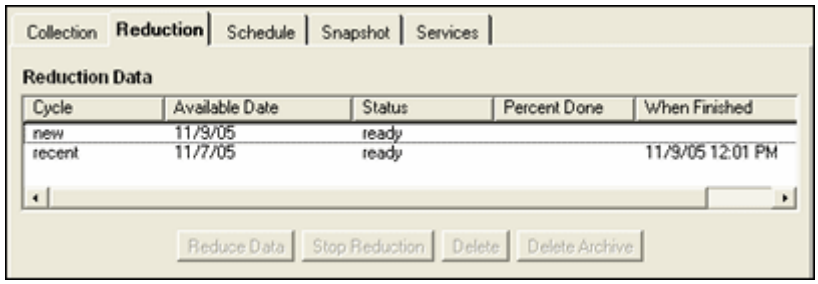
特定のコンテンツ・アイテムがアクセスされた後、最新のデータ・セットを縮小した場合、「Last Access」フィールドがリダクション・データ・セット内の最新のアクセス日付で更新されます。その後、それ以前のデータ・セットを再縮小した場合、現行値がこのコンテンツ・アイテムに対する以前のアクセス日付で上書きされることはありません。

長期および短期のアクティビティ・メトリックの詳細は、3-11 ページの「「Snapshot」タブ」および 3-15 ページの「「Enable Short Access Count updates」/「Enable Long Access Count updates」チェック・ボックスおよび対応する「Fields」/「Intervals」」を参照してください。

シナリオ 3:

任意の順序でデータ・セットを縮小した場合、最新データ・ファイルからアーカイブ・データ・ファイルへの移行が妨げられます。関連付けられた表レコードは、存続時間に基づいて移動されます。アーカイブ表は、最も古いデータを格納するように意図されています。データ・セットがランダムな順序で縮小された場合、どのデータが最も古いデータか明らかでありません。

最新データ・ファイルおよびアーカイブ・データ・ファイルの詳細は、2-13 ページの「ユーザー・メタデータ」、3-4 ページの「データ・リダクション・サイクル」および 3-8 ページの「「Cycle」列」を参照してください。



機能	説明
「Cycle」列	入力データの状態を示します。 **new:** 使用可能な日付の入力データは縮小されていません。入力データが縮小されると、サイクルは「recent」に変わります。ただし、現行システム日付の入力データが縮小された場合、サイクルには引き続きデータが「new」として表示されます。 **recent:** 入力データは縮小されていますが、まだアーカイブに移行していません。最新セットの数は、ユーザーが構成可能です。デフォルト数は、最近データ・リダクションが実行された 5 セット分の入力データであり、「recent」として表示されます。 **archive:** 入力データは縮小されており、サイクル「recent」に移行済です。データは、削除されるまで「archive」サイクルに残ります。
「Available Date」列	入力データが収集された日付を示します。
「Status」列	リダクション・データのステータスを示します。 **ready:** 入力データは縮小のために使用可能です。 **running:** 選択された入力データは縮小中です。 **archiving:** 入力データは「recent」サイクルから「archive」サイクルに移行中です。

機能	説明
「Percent Done」列	データ・リダクション・プロセスの進捗状況を示します。入力データが「running」のときにのみ表示されます。
「When Finished」列	データ・リダクション・プロセスが完了した日時を示します。
「Reduce Data」ボタン	このボタンを押すと、選択された入力データのデータ・リダクション・プロセスが開始されます。
「Stop Reduction」ボタン	このボタンを押すと、実行中のデータ・リダクション・プロセスが終了します。
「Delete」ボタン	このボタンを押すと、選択された入力データが削除されます。
「Delete Archive」ボタン	このボタンを押すと、「archive」サイクル内の入力データが削除されます。

注意 : 「Delete」および「Delete Archive」ボタンを使用すると、ユーザーが RAW データ・ログを削除できます。ただし、プライマリ表またはアーカイブ表から縮小済データ・レコードを削除するための規定の方法はありません。ユーザーは、データベース・ユーティリティを使用して、プライマリ表またはアーカイブ表を管理する必要があります。

ただし、「Delete」および「Delete Archive」ボタンを使用して RAW データが削除されても、表内の縮小済データは影響を受けません。

「Schedule」タブ

「Schedule」タブを使用して、自動データ・リダクションを有効化します。「Schedule」タブを使用すると、リダクションがスケジュールどおりに実行されるように構成できます。一般的な使用シナリオは、スケジューラを使用して定期的に RAW データを縮小することです。この場合、RAW データは、recent リポジトリおよび archive リポジトリに安定して移動されます。また同様に、縮小済データはプライマリ表からアーカイブ表に安定して移動されます。RAW データ、データ・ステータス、およびプライマリ表とアーカイブ表の詳細は、3-4 ページの「「Reduction」タブ」を参照してください。

Content Tracker リダクション・プロセスの主な特性は、次のとおりです。

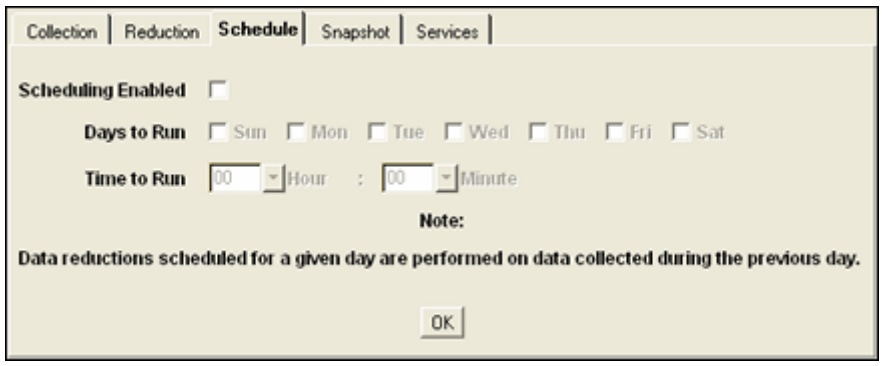
- Content Tracker データ・エンジンが、スケジュールされたリダクション実行の前日に無効化された場合、データは収集されません。Content Tracker データ・エンジンが、スケジュールされたリダクション実行の日に有効化された場合、使用可能なデータが存在しないため、スケジューラは実行されません。
- 特定の日にスケジュールされたデータ・リダクションは、その前日中に収集されたデータに対して実行されます。前日の定義は、真夜中（システム時間）に開始および終了する 24 時間です。

重要 : システム負荷の様々な条件によっては、スケジュールされたリダクションが真夜中を過ぎて数分以内に実行されるように設定されている場合、次のエラーが発行されることがあります。

```
<date_time>: Cannot reduce data. A request is in progress to delete raw data that
was generated on this date.
```

このメッセージが発行された場合、リダクション実行を 5 分または 10 分後にスケジュールしてみてください。

技術ヒント : CPU リソースを節約するためには、システム負荷が一般に最も低い早朝時間帯にリダクション実行をスケジュールします。



機能	説明
「Scheduling Enabled」チェック・ボックス	このチェック・ボックスを選択すると、データ・リダクションを自動的に実行できます。
「Days to Run」チェック・ボックス	1 つ以上のチェック・ボックスを選択すると、データ・リダクションの実行日が設定されます。
「Time to Run」フィールド	データ・リダクションの実行時刻を設定するために時間および分を選択する場合に使用します。
「OK」ボタン	現行のリダクション・スケジュール設定を保存します。

「Snapshot」タブ

「Snapshot」タブを使用して、特定のアクティビティ・メトリックを選択的に有効化して、自動的に事前定義のカスタム・メタデータ・フィールドに割り当てます。このタブをアクティブにすると、アクティビティ・メトリックおよび対応するメタデータ・フィールドに、コンテンツ・アイテムのユーザー・アクセスに関する検索関連情報が移入されます。オプションの自動ロード機能を使用すると、チェックインされたコンテンツ・アイテムのタイムスタンプが正確になるように、最終アクセス・アクティビティ・メトリックを更新できます。

Content Tracker によって、特定のコンテンツ・アイテムの人気度を示すコンテンツ・アイテム使用状況情報が検索関連カスタム・メタデータ・フィールドに挿入されます。この情報には、2 つの異なる期間における最新アクセスの日付およびアクセス数が含まれます。

ユーザーは、これらのアクティビティ・メトリック機能から生成された情報を様々な方法で適用できます。アクティビティ・メトリックを選択的に使用して、後でコンテンツ・アイテムの人気度に基づいて検索結果を並べ替えることができます。たとえば、最近表示されたコンテンツ・アイテムや、先週最も多く表示されたコンテンツ・アイテムに従って、検索結果を並べ替えることができます。

スナップショット機能がアクティブになっている場合、リダクション後の手順で検索関連メタデータ・フィールドの値が更新されます。処理手順の間、Content Tracker では SQL 問合せを使用して、アクティビティ・メトリックの値を変更したコンテンツ・アイテムが判別されます。Content Tracker によって、適用可能なデータベース表が新しい値で更新され、再索引付けサイクルが開始されます。ただし、再索引付けされるのは、メタデータ値を変更したコンテンツ・アイテムのみです。2-3 ページの「アクティビティ・メトリックを使用するデータ・リダクション・プロセス」を参照してください。

注意 : 「Snapshot」タブを使用すると、スナップショット機能を自動的にアクティブ化し、各アクティブ・メトリックを選択的に有効化できます。アクティブ化する各機能には、カスタム・メタデータ・フィールドが関連付けられている必要があります。

詳細は、3-28 ページの「スナップショット機能およびアクティビティ・メトリック・オプションの有効化」および 3-29 ページの「検索関連メタデータ・フィールドへの アクティビティ・メトリック機能のリンク」を参照してください。

あるいは、Content Tracker の sct.cfg ファイル内の適用可能な構成変数を手動で更新することもできます。付録 A「Content Tracker の構成およびカスタマイズ」を参照してください。

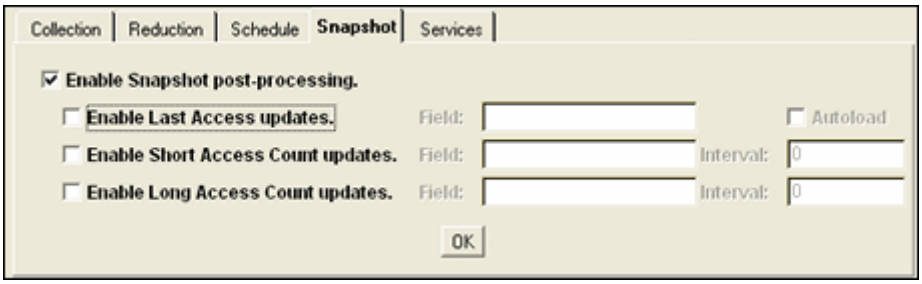
重要 : アクティビティ・メトリック機能をカスタム・メタデータ・フィールドにリンクする場合、これらのフィールドがすでに存在しており、適切なタイプが指定されている必要があります。「Last Access」メトリックに関連付けられたメタデータ・フィールドは、Date 型である必要があります。「Access Count」メトリックに関連付けられたメタデータ・フィールドは、Integer 型である必要があります。3-26 ページの「検索関連メタデータ・フィールドの作成」を参照してください。

警告 : アクティビティ・メトリックと組み合せて使用するカスタム・メタデータ・フィールドを作成する場合、検索索引に対してフィールドを有効化するオプションがあります。カスタム・メタデータ・フィールドが索引付けされている（および検索可能になっている）と、フィールドに格納されているアクセス値に、より効率的にアクセスできます。つまり、検索結果を関連別に選択したり並べ替える場合、索引付けされたフィールドのほうが便利です。

索引付けは、特に全文検索が有効化されていると、高コストになります。索引付けされたメタデータ・フィールドのデメリットは、検索関連メタデータ・フィールドの値が変更された場合、影響を受けるコンテンツ・アイテムを再索引付けして、データベース表の値を更新する必要があることです。このため、多数のコンテンツ・アイテム・アクセスのある大きなインスタンスの場合は、検索関連フィールドを更新するとパフォーマンスが低下します。

あるいは、カスタム・メタデータ・フィールドの索引付け機能を無効化することもできます。この場合、索引付けされていないメタデータ・フィールドを検索して値を検出することが可能ですが、検索のコストはより高くなります。

注意 : 影響を受けるコンテンツ・アイテムの再索引付けによってパフォーマンスが非常に低下する場合、オプションでスナップショット機能を非アクティブ化できます。ただし、この場合はアクティビティ・メトリック情報が収集されなくなります。その結果、現在の検索結果を使用状況別に並べ替える（たとえば、アクセスされたコンテンツ・アイテムを人気の高い順にリストするなど）ことができなくなります。



機能	説明
「Enable Snapshot post-processing」チェック・ボックス	このチェック・ボックスを選択すると、アクティビティ・メトリック機能がアクティブになり、ユーザーは個別に機能を選択して適用可能なメタデータ・フィールドに割り当てることができます。スナップショット機能を有効化すると、次のリダクション・サイクルの後にメタデータの自動ロードが行われます。デフォルトでは、スナップショット機能は無効化されています。
重要 : スナップショット機能をアクティブ化する前に、有効化されている各アクティビティ・メトリックと関連付けるカスタム・メタデータ・フィールドを決定する必要があります。また、カスタム・メタデータ・フィールドがすでに存在しており、適切なタイプが指定されている必要があります。 「Last Access」メトリックに関連付けられた検索関連メタデータ・フィールドは、Date 型である必要があります。「Access Count」メトリックに関連付けられた検索関連メタデータ・フィールドは、Integer 型である必要があります。3-26 ページの「検索関連メタデータ・フィールドの作成」を参照してください。	
「Enable Last Access updates」チェック・ボックスおよび対応する「Field」メタデータ・フィールド	このチェック・ボックスを選択すると、関連付けられた検索関連メタデータ・フィールドおよび「Autoload」チェック・ボックスがアクティブ化されます。「Field」フィールドには、このアクティビティ・メトリックにリンクされるメタデータ・フィールドの内部名を入力します。たとえば、xLastAccess のように入力します。
注意 : コンテンツがチェックインされると、Content Server の DocMeta データベース表の「Last Access」フィールドは最初は空です。データ・リダクションの実行が完了すると、「Last Access」フィールドが最新アクセスの日時で更新されます。アクセスが発生していない場合は、チェックインの日時で更新されます。しかし、一部のアプリケーションでは、「Last Access」フィールドに常に有効な値が含まれていることが必要です。このためには、「Default Value」フィールド、「Autoload」オプションまたはバッチ・ローダーを使用します。3-30 ページの「「Last Access」メタデータ・フィールドのチェックイン時刻値の設定」を参照してください。	

<table>
<tr><th>機能</th><th>説明</th></tr>
<tr><td colspan="2">  注意：「Last Access」メトリックの場合、Content Tracker では、リダクション日付のアクセスがチェックされるのみです。その結果、レコードに途切れが生じることがあります。詳細および例は、3-5 ページの「イベント・ログのリダクション順序」を参照してください。</td></tr>
<tr><td>「Autoload」チェック・ボックス</td><td>このチェック・ボックスを選択して「OK」ボタンをクリックすると、問合せが起動され、デフォルトでは、現在の日時を使用して Content Server の DocMeta データベース表の空の「Last Access」メタデータ・フィールドが移入されます。3-32 ページの「「Autoload」オプションを使用した「Last Access」フィールドの移入」を参照してください。</td></tr>
<tr><td colspan="2">  重要：「Autoload」オプションを使用する場合は、次の操作上の考慮事項に注意してください。
❖ Autoload は主に、アクセス・アクティビティとしてのチェックイン操作をカウントするアプリケーションでの使用を意図されています。詳細は、3-31 ページの「「Default Value」を使用した「Last Access」フィールドの移入」を参照してください。
❖ Autoload を実行すると、Content Server の DocMeta データベース表の各レコードが影響を受けることがあるため、このオプションは慎重に使用する必要があります。
❖ 影響を受ける DocMeta レコードは、「Last Access」メタデータ・フィールドが空（NULL）になっている DocMeta レコードのみです。
❖ Autoload は永続的です。「Autoload」チェック・ボックスの状態は、その他すべてのスナップショット設定とともに保存されます。このオプションを誤って使用することがないように、自動ロード機能の実行後はすぐに、「Autoload」チェック・ボックスの選択を解除し、アクティビティ・メトリック・フィールド設定を再保存する必要があります。
❖ Autoload での更新が完了した後、Content Tracker によって Content Server のインデクサは起動されません。コレクションの再構築の時期は自分で決定する必要があります。
❖ デフォルトでは、「Autoload」問合せによって「Last Access」メタデータ・フィールドが現在の日時に設定されます。ただし、アプリケーションのニーズにあわせて問合せをカスタマイズすることもできます。A-9 ページの「「Autoload」オプションの SQL 問合せのカスタマイズ」を参照してください。</td></tr>
</table>

<table>
<tr><th>機能</th><th>説明</th></tr>
<tr><td>「Enable Short Access Count updates」/「Enable Long Access Count updates」チェック・ボックスおよび対応する「Fields」/「Intervals」</td><td>これらのチェック・ボックスを選択すると、関連付けられた検索関連メタデータ・フィールドおよび時間間隔フィールドがアクティブになります。
「Field」フィールドに、アクティビティ・メトリックにリンクされるメタデータ・フィールドの内部名を入力します。たとえば、xShortAccess または xLongAccess のように入力します。
アクティビティ・メトリック・カウントの間隔を日数で指定します。</td></tr>
<tr><td colspan="2">  注意 : 2 つの「Access Count」メトリックで異なるのは、計算期間のみです。たとえば、過去 30 日間と過去 90 日間、先週と昨年、などです。また、アクティビティ・メトリックに指定されている時間間隔は互いに依存していません。たとえば、最初の時間間隔（Short Access）の日数を、2 番目の時間間隔（Long Access）の日数より多く設定することもできます。</td></tr>
<tr><td colspan="2">  注意 : アクセス・カウントを表にできるのは、日付がすでに縮小されている場合のみです。1 日以上データを縮小していない場合、この期間のアクセスは記録もカウントもされません。詳細および例は、3-5 ページの「イベント・ログのリダクション順序」を参照してください。</td></tr>
<tr><td colspan="2">  重要 :「Access Count」メトリックはリダクション日の順序によって影響を受けるため、ランダムな順序ではデータを縮小しないでください。詳細および例は、3-5 ページの「イベント・ログのリダクション順序」を参照してください。</td></tr>
<tr><td colspan="2">  注意 :「Snapshot」タブのフィールドでは、大 / 小文字が区別されます。このため、すべてのフィールド値は、大文字と小文字を区別して正確なスペルで入力することが重要です。Content Tracker では、次のエラー・チェックを使用して、有効化された各アクティビティ・メトリック・フィールド値が検証されます。
❖ Content Tracker では、DocMeta データベース表をチェックして、カスタム・メタデータ・フィールドが実際に存在していることが確認されます。
❖ Content Tracker では、カスタム・メタデータ・フィールドが正しいタイプであることが確認されます。つまり、「Last Access」メタデータ・フィールドは Date 型で、「Short Access Count」と「Long Access Count」フィールドは Integer 型である必要があります。
❖ Content Tracker によって、dID メタデータ・フィールドを明示的に除外するためのチェックが実行されます。</td></tr>
</table>

機能	説明
「OK」ボタン	スナップショット構成を保存し、Content Tracker の sct.cfg ファイルをアクティビティ・メトリック・フィールドの現在の設定で更新します。「Autoload」チェック・ボックスが選択されている場合、アクティビティ・メトリック設定が保存されるとすぐに、DocMeta データベース表の「Last Access」フィールドが更新されます。
 **重要 :** 構成を変更した場合、次のリダクション・サイクル中にすべてのコンテンツ・アイテムが更新されます。	

「Services」タブ

「Services」タブを使用して、追加の Content Server サービス・コールを、関連付けられたサービスに関連するデータ値とともに記録します。「Services」タブを使用すると、サービス・エントリを簡単に追加または編集できます。またオプションで、サービス・コール構成ファイル（SctServiceFilter.hda）内の対応するフィールド・マップ ResultSet も追加または編集できます。記録するサービスにはそれぞれ、SctServiceFilter.hda ファイル内にサービス・エントリが存在している必要があります。

SctServiceFilter.hda ファイル内のサービス・エントリによって、Content Tracker はイベントおよび使用状況の情報を収集できます。有効化されたサービスによって、各種の一般的な DataBinder フィールド（dUser や dDocName など）が自動的に記録されます。フィールド・マップ ResultSet をサービス・エントリにリンクすると、拡張サービス・コール・トラッキング機能を使用できます。フィールド・マップ ResultSet は、データ・フィールド名、ロケーション名、および出力データ表（SctAccessLog）内の関連付けられた汎用表列名のリストで構成されます。

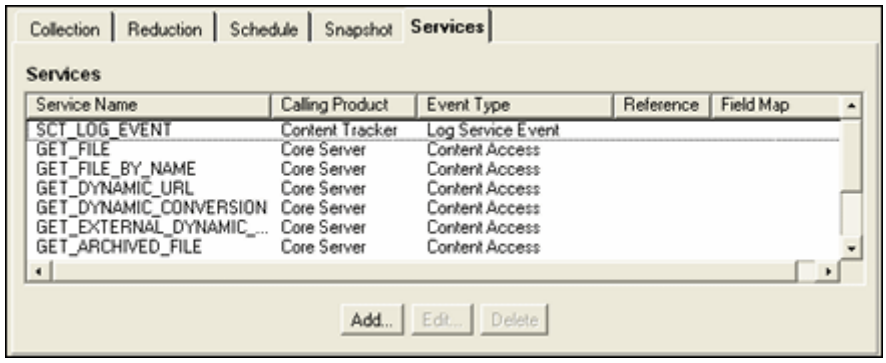
SctAccessLog 表には、拡張サービス・コール・トラッキング機能で使用するための追加の汎用列が用意されています。これらの列に、関連付けられたサービス・コールに適した任意のデータ値を挿入できます。フィールド・マップ ResultSet 内にデータ・フィールド名をリストする場合は、データ・フィールドのソースであるロケーション名と、データの記録先の表列名もリストする必要があります。拡張サービス・トラッキング機能によって特定のサービス・コールに対する特定のデータが記録および追跡されるため、アクセスおよび使用状況の情報が含まれるカスタマイズ済レポートを生成できます。

警告 : フィールド・マップ ResultSet 内では、データ・フィールドを既存の標準の SctAccessLog 表列に自由にマップできます。標準のフィールド・データ値が収集されると、拡張サービス・マッピングが実行されます。したがって、標準の表列フィールドをオーバーライドできます。

たとえば、記録するサービスのデータ・フィールドに特定のユーザー名（たとえば、MyUserName=john など）が含まれるとします。拡張トラッキング機能を使用して、sc_scs_dUser 列の内容をオーバーライドできます。この場合は、MyUserName と sc_scs_dUser を結合して、データ・フィールド、ロケーション、およびフィールド・マップ ResultSet 内の表列セットとして使用するのみです。

したがって、この場合も、記録されるデータが SctAccessLog 列タイプと適合しているかどうかは自分で確認する必要があります。

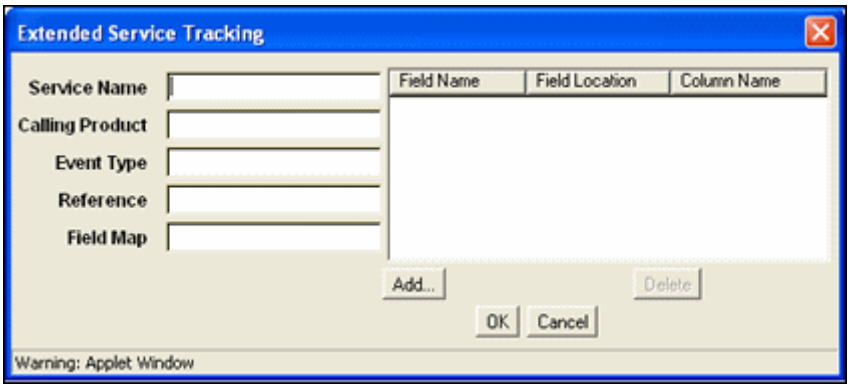
注意 : SctAccessLog 表および汎用列の詳細は、2-8 ページの「結合された出力表」を参照してください。SctServiceFilter.hda ファイル、拡張サービス・コール・トラッキング機能および ResultSet 構成の詳細は、第 5 章「サービス・コール構成」を参照してください。



機能	説明
「Services」リスト	Content Tracker によって記録された各サービスの名前および結果セット値が示されます。
「Add」ボタン	「Extended Services Tracking」画面（3-18 ページ）を開きます。
「Edit」ボタン	「Extended Services Tracking」画面（3-18 ページ）を開きます。適用可能なフィールドに、現在の結果セット値が移入されます。
「Delete」ボタン	選択されたサービスを削除します。

「Extended Services Tracking」画面

「Extended Services Tracking」画面を使用して、SctServiceHandler.hda ファイルに挿入される ServiceExtraInfo ResultSet に含まれるサービス・エントリを構成（追加、編集または削除）します。この画面にアクセスするには、「Services」タブ（3-16 ページ）の**「Add」**ボタンをクリックします。

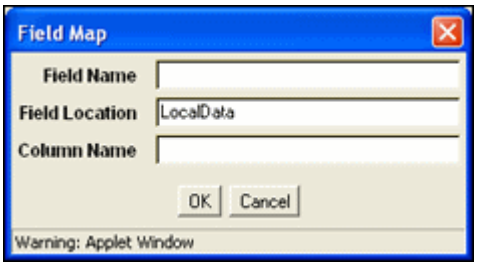


機能	説明
 **注意 :** Content Tracker では、データ・エンジン・コントロール・センターの拡張サービス・トラッキング機能に対するエラー・チェック（フィールド・タイプやスペルの検証など）は実行されません。リダクションを実行するまで、エラーは生成されません。「Extended Services Tracking」画面のフィールドでは、大 / 小文字が区別されます。このため、サービス・エントリ・フィールドの値（特にサービス・コール名）は正確に入力するように注意してください。すべてのフィールド値が、大文字と小文字を区別して正確なスペルで入力されていることを確認してください。	
 **注意 :** SctServiceHandler.hda ファイル内の ServiceExtraInfo ResultSet には、記録されるサービスごとにサービス・エントリが 1 つずつ含まれます。「Service Name」フィールドから既存のサービス・エントリを選択すると、適用可能なフィールドに既存のサービス・エントリのフィールド値が移入されます。ただし、サービスを追加する場合は、新規のサービス・エントリに、「Service Name」フィールド、「Calling Product」フィールド、「Event Type」フィールド、「Reference」フィールドおよび「Field Map」フィールドに入力した値が使用されます。 サービス・エントリおよびフィールド・マップ ResultSet の構成要件の詳細は、5-5 ページの「サービス・コール構成ファイルの内容」を参照してください。	
「Service Name」フィールド	記録されるサービスの名前。たとえば、GET_FILE などです。サービス・エントリにサービス名用の行が含まれていない場合、サービスは記録されません。
「Calling Product」フィールド	任意の文字列。標準の Content Server エントリではすべて、このフィールドは通常 "Core Server" に設定されます。
「Event Type」フィールド	任意の文字列。標準の Content Server エントリではすべて、このフィールドは通常 "Content Access" に設定されます。
「Reference」フィールド	SctAccessLog 表の sc_scs_reference フィールドを設定するために使用します。空白にした場合、内部の getReference ロジックが使用されます。

機能	説明
「Field Map」フィールド	SctServiceFilter.hda ファイルに追加されるフィールド・マップ ResultSet の名前。このフィールドは、拡張サービス・コール・トラッキング機能を使用する場合にのみ必須です。この機能を使用すると、任意の DataBinder フィールド情報を SctAccessLog 表の 1 つ以上の汎用列に記録できます。  **注意 :** フィールド・マップを設計する場合、サービスが呼び出されたときにオブジェクトを書き出すような構成変数を設定すると役立ちます。これによって、イベントの記録時に使用可能なデータが確認できます。詳細は、B-3 ページの「SctDebugServiceBinderDumpEnabled」を参照してください。
「Field Name」/「Field Location」/「Column Name」リスト	データ・フィールド、ロケーション、およびフィールド・マップ ResultSet に関連付けられた表列名の各セットがリストされます。「Field Map」画面（3-21 ページ）のフィールド値が、このリストへの移入に使用されます。
「Add」ボタン	「Field Map」画面（3-21 ページ）を開きます。
「Delete」ボタン	選択されたフィールド・マップ ResultSet を削除します。
「OK」ボタン	フィールド値を保存し、サービス・エントリを ServiceExtraInfo ResultSet に追加または更新します。また、「OK」をクリックすると、フィールド・マップ ResultSet（作成した場合）が SctServiceFilter.hda ファイルに追加されます（3-21 ページの「「Field Map」画面」を参照）。
「Cancel」ボタン	変更を保存せずに「Extended Services Tracking」画面を閉じます。

「Field Map」画面

「Field Map」画面を使用して、サービス・エントリにリンクされ SctServiceHandler.hda ファイルに含められるフィールド・マップ ResultSet を構成します。この画面にアクセスするには、「Extended Services Tracking」画面（3-18 ページ）の**「Add」**ボタンをクリックします。



機能	説明
注意 : Content Tracker では、データ・エンジン・コントロール・センターの拡張サービス・トラッキング機能に対するエラー・チェック（フィールド・タイプやスペルの検証など）は実行されません。リダクションを実行するまで、エラーは生成されません。「Field Map」画面のフィールドでは、大 / 小文字が区別されます。このため、フィールドおよび列の名前は正確に入力するように注意してください。すべてのフィールド値が、大文字と小文字を区別して正確なスペルで入力されていることを確認してください。	
注意 : 拡張サービス・コール・トラッキング機能を使用するには、サービス・エントリを SctServiceHandler.hda ファイル内のフィールド・マップ ResultSet にマップする必要があります。「Extended Services Tracking」画面（3-18 ページ）の「Field Map」フィールドの値は、フィールド・マップ ResultSet の名前です。	
「Field Name」フィールド	SctAccessLog 表の汎用列にデータ値が記録される Content Server サービス DataBinder 内のデータ・フィールドの名前。ターゲット列は、「Column Name」フィールドで指定されます。
重要 : フィールド・マップ ResultSet 内の値は、記録されるフィールドとしては使用できません。	

機能	説明
「Field Location」フィールド	記録されるデータ・フィールドが存在する Content Server サービス DataBinder 内のセクション。次の 3 つの値がサポートされています。 LocalData: デフォルト値。 Environment BinderResultSet: ResultSet 内のすべての値が含まれたカンマ区切り文字列を返します。SctAccessLog 表では空白に制限があるため、この値は ResultSet が小さい場合に有用です。サイズは 255 文字（カンマなどは使用可能）に制限されています。
 **技術ヒント :** 256 文字以上使用できるようにするには、標準のデータベース・ツールを使用して、SctAccessLog 表列を拡大または再定義できます。たとえば、extField_3 を 2047 に拡大した場合、同等のデータ量が格納されます。ただし、ほとんどのデータベースにはページ・サイズ制限があり、考慮が必要です。また、SQL では文字列が効率的に解析されないことも実質的に考慮する必要があります。	
「Column Name」フィールド	指定された DataBinder フィールドからデータ値が記録される SctAccessLog 表内の特定の汎用列。データ・フィールドは、「Field Name」フィールドで指定されます。
「OK」ボタン	値を保存し、フィールド・マップ ResultSet を SctServiceFilter.hda ファイルに追加します。
「Cancel」ボタン	DataBinder フィールド名および対応する SctAccessLog 列名のリストを保存せずに、「Field Map」画面を閉じます。
 **技術ヒント :** Content Tracker には、DataBinder オブジェクトをダンプ・ファイルに書き出すようにサービス・ハンドラ・フィルタを構成するデバッグ構成変数（有効化されている場合）が備わっています。フィールド・マップ画面を開発する際は、これらを診断ツールとして使用できます。ダンプ・ファイルを使用すると、特定のサービス・イベントの記録時に使用可能なデータを確認できます。詳細は、B-3 ページの「SctDebugServiceBinderDumpEnabled」を参照してください。	

データ・エンジン・コントロール・センターへのアクセス

データ・エンジン・コントロール・センターは、データ・コレクションおよびリダクションを有効化、スケジュールおよび監視する場合に使用されます。

データ・エンジン・コントロール・センターにアクセスするには、次のようにします。

1. Content Tracker の「Administration」ページを開きます。

   これには、「Administration」トレーから「Content Tracker Administration」を選択します。

2. 下へスクロールし、**「Data Engine Control Center」**アイコンをクリックします。

   「Content Tracker Data Engine Control Center」インタフェースが表示されます。

データ・コレクションの有効化または無効化

データ・コレクションが有効化されている場合、Content Tracker によってコンテンツ・サーバーの Web トラフィック・アクティビティが記録されます。デフォルトでは、「Data Engine Control Center」の「Collection」タブで、「Enable Data Collection」チェック・ボックスが選択されています。このチェック・ボックスを選択すると、データ・コレクションが有効化されます。このチェック・ボックスの選択を解除すると、データ・コレクションが無効化されます。

データ・コレクションを有効化または無効化するには、次のようにします。

1. **「Data Engine Control Center」**を開きます（3-23 ページの「データ・エンジン・コントロール・センターへのアクセス」を参照）。

2. 「Collection」タブで、**「Enable Data Collection」**チェック・ボックスを選択（コレクションを有効化する場合）または選択解除（コレクションを無効化する場合）します。

3. **「OK」**をクリックします。

重要：「OK」をクリックした後すぐにアプレットを終了しないでください。「Updated Data Collection」という状態確認メッセージが表示されるまで待つ必要があります。これには、数秒間かかることがあります。確認メッセージが表示される前にアプレットを終了すると、要求した変更が有効にならないことがあります。

4. 「Updated Data Collection」という状態確認メッセージが表示されたら、**「OK」**をクリックします。

5. Content Server を再起動します。

重要 : チェック・ボックスの上のテキストをよく読んで、データ・コレクションが有効化されているか無効化されているかを判断してください。

- ❖ 有効化されている場合は、「Data collection is enabled...」というテキストが表示されます。
- ❖ 無効化されている場合は、「Data collection is not enabled...」というテキストが表示されます。

データ・リダクションの手動実行

データを手動で縮小するには、次のようにします。

1. **「Data Engine Control Center」**を開きます（3-23 ページの「データ・エンジン・コントロール・センターへのアクセス」を参照）。
2. 「Reduction」タブで、縮小する入力データのセットをクリック（して選択）します。
3. **「Reduce Data」**ボタンをクリックします。

   確認ダイアログ・ボックスが表示されます。
4. **「Yes」**をクリックして、データを縮小します。

   「Status」は「ready」から「running」に変わり、「Percent Done」にデータ・リダクションの進捗状況が示されます。データ・リダクションが完了すると、「When Finished」にタイムスタンプが表示され、「Cycle」に「recent」が表示されます。

注意 : 現在の日付のデータを縮小するように選択した場合、データは縮小されますが、「Cycle」には引き続きデータ・セットが「new」として表示されます。

データ・リダクションの自動実行の設定

データ・リダクションが自動的に実行されるように設定するには、次のようにします。

1. **「Data Engine Control Center」**を開きます（3-23 ページの「データ・エンジン・コントロール・センターへのアクセス」を参照）。
2. 「Schedule」タブで、**「Scheduling Enabled」**チェック・ボックスを選択します。
3. データ・コレクションを実行する日のチェック・ボックスを選択します。
4. データ・コレクションを実行する時間および分を選択します。
5. **「OK」**をクリックします。

重要 : 「OK」をクリックした後すぐにアプレットを終了しないでください。「Updated reduction scheduling information」という確認メッセージが表示されるまで待つ必要があります。これには、数秒間かかることがあります。確認メッセージが表示される前にアプレットを終了すると、要求した変更が有効にならないことがあります。

6. 「Updated reduction scheduling information」という確認メッセージが表示されたら、「**OK**」をクリックします。

   データは、選択した日時に自動的に縮小されます。

データ・ファイルの削除

データ・ファイルは、2 つのサイクル中に削除できます。

- 任意のサイクルのデータ・ファイルの削除（3-25 ページ）
- 「archive」サイクルのデータ・ファイルの削除（3-25 ページ）

任意のサイクルのデータ・ファイルの削除

警告 : データの削除は永続的であり、Content Tracker からも Content Server からも元に戻すことはできません。

1. 「**Data Engine Control Center**」を開きます（3-23 ページの「データ・エンジン・コントロール・センターへのアクセス」を参照）。
2. 「Reduction」タブで、削除する入力データのセットをクリック（して選択）します。
3. 「**Delete**」ボタンをクリックします。

   確認ダイアログ・ボックスが表示されます。
4. 「**OK**」をクリックして、データを削除します。

   選択したデータ・セットが削除され、ウィンドウに表示されなくなります。

「archive」サイクルのデータ・ファイルの削除

警告 : データの削除は永続的であり、Content Tracker からも Content Server からも元に戻すことはできません。

1. 「**Data Engine Control Center**」を開きます（3-23 ページの「データ・エンジン・コントロール・センターへのアクセス」を参照）。
2. 「Reduction」タブで、「**Delete Archive**」ボタンをクリックします。

   確認ダイアログ・ボックスが表示されます。
3. 「**OK**」をクリックして、データを削除します。

   「archive」サイクルのすべてのデータ・セットが削除され、ウィンドウに表示されなくなります。

検索関連メタデータ・フィールドの作成

スナップショット機能を実装する前に、有効化されている各アクティビティ・メトリックと関連付けるカスタム・メタデータ・フィールドを決定する必要があります。また、カスタム・メタデータ・フィールドがすでに存在しており、適切なタイプが指定されている必要があります。有効化するアクティビティ・メトリックに応じて、適宜、次の手順を使用して、1 つ以上のカスタム・メタデータ・フィールドを作成する必要があります。

- 「Last Access」メトリック用のカスタム・メタデータ・フィールドの作成（3-26 ページ）
- 「Short Access Count」および「Long Access Count」メトリック用のカスタム・メタデータ・フィールドの作成（3-27 ページ）

「Last Access」メトリック用のカスタム・メタデータ・フィールドの作成

「Last Access」フィールドに割り当てるカスタム・メタデータ・フィールドを作成するには、次のようにします。

1. Content Tracker の「Administration」ページを開きます。

   これには、「Administration」トレーから「Content Tracker Administration」を選択します。

2. **「Configuration Manager」**アイコンをクリックします。

   「Configuration Manager」インタフェースが表示されます。

3. 「Information Fields」タブで、**「Add」**をクリックします。

   「Add Custom Info Field」画面が表示されます。

4. 「Last Access」メトリックに割り当てるメタデータ・フィールドの名前を入力します。たとえば、LastAccess のように入力します。

5. **「OK」**をクリックします。

   「Add Custom Info Field」画面が表示されます。

6. 「Field Type」ドロップダウン・メニューから**「Date」**を選択します。

注意 : 通常、「Default Value」フィールドに値を入力する必要はありません。ただし、指定されたデフォルト値がない場合にこのフィールドに値を入力しないと、コンテンツ・アイテムがチェックインされてデータ・リダクションが実行されるまで、「Last Access」フィールドは移入されません。ただし、一部のアプリケーションでは、「Last Access」フィールドに常に有効な値が含まれていることが必要です。この場合、「Last Access」フィールドにコンテンツのチェックインの日時が移入されるように、「Default Value」フィールドに値を入力する必要があります。詳細は、3-31 ページの「「Default Value」を使用した「Last Access」フィールドの移入」を参照してください。

注意 :「Last Access」カスタム・メタデータ・フィールドに必須の属性は、値が Date であるフィールド・タイプのみです。ただし、「Last Access」カスタム・メタデータ・フィールドを検索可能にする場合は、「Enable for Search Index」チェック・ボックスが選択されていることを確認する必要があります。

このカスタム・メタデータ・フィールドの索引付けはオプションですが、索引付けによってこのフィールドでの検索はより効率的になります。さらに、索引付けによって、蓄積された検索関連統計に問い合せ、有用なデータを生成できます。たとえば、人気順に並べたコンテンツ・アイテムのリストを作成することなどができます。

検索関連メタデータ・フィールドの索引付けのメリットおよびデメリットの詳細は、3-11 ページの「「Snapshot」タブ」を参照してください。

7. **「OK」**をクリックします。

   カスタム・メタデータ・フィールドが「Information Fields」タブの「Field Info」リストに追加されます。

8. **「Update Database Design」**をクリックして、現行データベースを検証し、カスタム・メタデータ・フィールドをシステムに追加します。

「Short Access Count」および「Long Access Count」メトリック用のカスタム・メタデータ・フィールドの作成

短期および長期のアクセスのフィールドに割り当てるカスタム・メタデータ・フィールドを作成するには、次のようにします。

1. Content Tracker の「Administration」ページを開きます。

   これには、「Administration」トレーから「Content Tracker Administration」を選択します。

2. **「Configuration Manager」**アイコンをクリックします。

   「Configuration Manager」インタフェースが表示されます。

3. 「Information Fields」タブで、**「Add」**をクリックします。

   「Add Custom Info Field」画面が表示されます。

4. 「Short Access Count」および「Long Access Count」メトリックに割り当てるメタデータ・フィールドの名前を入力します。たとえば、ShortAccess または LongAccess のように入力します。

5. **「OK」**をクリックします。

   「Add Custom Info Field」画面が表示されます。

6. 「Field Type」ドロップダウン・メニューから**「Integer」**を選択します。

注意 :「Short Access Count」および「Long Access Count」カスタム・メタデータ・フィールドに必須の属性は、値が Integer であるフィールド・タイプのみです。ただし、「Short Access Count」および「Long Access Count」カスタム・メタデータ・フィールドを検索可能にする場合は、両方のフィールドに対して「Enable for Search Index」チェック・ボックスが選択されていることを確認する必要があります。

これらのカスタム・メタデータ・フィールドの索引付けはオプションですが、索引付けによってこれらのフィールドでの検索はより効率的になります。さらに、索引付けによって、蓄積された検索関連統計に問い合せ、有用なデータを生成できます。たとえば、人気順に並べたコンテンツ・アイテムのリストを作成することなどができます。

検索関連メタデータ・フィールドの索引付けのメリットおよびデメリットの詳細は、3-11 ページの「「Snapshot」タブ」を参照してください。

7. **「OK」**をクリックします。

   カスタム・メタデータ・フィールドが「Information Fields」タブの「Field Info」リストに追加されます。

8. **「Update Database Design」**をクリックして、現行データベースを検証し、カスタム・メタデータ・フィールドをシステムに追加します。

スナップショット機能およびアクティビティ・メトリック・オプションの有効化

デフォルトでは、スナップショット機能およびアクティビティ・メトリックは無効化されています。これらのオプション機能を使用するには、まず、アクティビティ・メトリック選択項目をアクティブにするスナップショット後処理機能を有効化する必要があります。すると、必要なアクティビティ・メトリックを選択的に有効化し、すでに選択されているカスタム・メタデータ・フィールドを割り当てられることができるようになります。

スナップショット機能を有効化し、アクティビティ・メトリックをアクティブ化するには、次のようにします。

1. **「Data Engine Control Center」**を開きます（3-23 ページの「データ・エンジン・コントロール・センターへのアクセス」を参照）。
2. **「Snapshot」**タブをクリックします。
3. 「Enable Snapshot post-processing」チェック・ボックスを選択します。

   スナップショット機能が有効になり、アクティビティ・メトリック・オプションがアクティブになります。

4. **「OK」**をクリックします。

   確認ダイアログ・ボックスが表示されます。

5. 「**OK**」をクリックします。

   スナップショット状態および Content Tracker の構成ファイル（sct.cfg）が更新されます。

注意 : スナップショット機能およびアクティビティ・メトリックが有効化されていることを確認するには、次のディレクトリ内の Content Tracker の sct.cfg ファイルにアクセスします。

<*install_dir*>/custom/ContentTracker/resources/sct.cfg

注意 : オプションで、手動でスナップショット機能を有効化し、アクティビティ・メトリック・オプションをアクティブ化できます。特定のスナップショット構成変数の詳細は A-2 ページの「構成変数」を、その手動での編集方法は A-7 ページの「Content Tracker 構成変数の手動設定」を参照してください。

検索関連メタデータ・フィールドへのアクティビティ・メトリック機能のリンク

アクティビティ・メトリック・オプションは、アクティブ化した後、個別に選択して有効化する必要があります。アクティビティ・メトリックを有効化すると、対応するカスタム・メタデータ・フィールドもアクティブになります。

アクティビティ・メトリックを有効化し、対応するカスタム・メタデータ・フィールドをアクティブ化するには、次のようにします。

1. 「**Data Engine Control Center**」を開きます（3-23 ページの「データ・エンジン・コントロール・センターへのアクセス」を参照）。
2. 「**Snapshot**」タブをクリックします。

   スナップショット機能が有効化されている必要があります。そうでない場合、アクティビティ・メトリック・オプションはアクティブになりません。3-28 ページの「スナップショット機能およびアクティビティ・メトリック・オプションの有効化」を参照してください。
3. 1 つ以上のアクティビティ・メトリック・チェック・ボックスを選択します。

   選択した各アクティビティ・メトリックが有効化され、対応するカスタム・メタデータ・フィールドがアクティブになります。
4. 「Field」フィールドに、アクティビティ・メトリックにリンクされるカスタム・メタデータ・フィールドの内部名を入力します。たとえば、xLastAccess、xShortAccess または xLongAccess のように入力します。
5. 「Short Access Count」および「Long Access Count」には、適用可能な時間間隔を日数で入力します。たとえば、「Short Access Count」に 7 日間を、「Long Access Count」に 28 日間を入力します。

6. 「**OK**」をクリックします。

   確認ダイアログ・ボックスが表示されます。

7. 「**OK**」をクリックします。

   スナップショット状態および Content Tracker の構成ファイル（sct.cfg）が更新されます。

注意 : Content Tracker では、アクティビティ・メトリック・フィールド名に対して最小のエラー・チェックが実行されます。「Snapshot」タブのフィールドでは大 / 小文字が区別されますので注意してください。すべてのフィールド値を、大文字と小文字を区別して正確なスペルで入力することが重要です。スナップショット機能に対する特定の Content Tracker エラー・チェックの詳細は、3-11 ページの「「Snapshot」タブ」を参照してください。

注意 : アクティビティ・メトリックが適切なカスタム・メタデータ・フィールドにリンクされていることを確認するには、次のディレクトリ内の Content Tracker の sct.cfg ファイルにアクセスできます。

<*install_dir*>/custom/ContentTracker/resources/sct.cfg

注意 : オプションで、手動でアクティビティ・メトリックを各々のカスタム・メタデータ・フィールドにリンクできます。特定のアクティビティ・メトリック構成変数の詳細は A-2 ページの「構成変数」を、その手動での編集方法は A-7 ページの「Content Tracker 構成変数の手動設定」を参照してください。

「Last Access」メタデータ・フィールドのチェックイン時刻値の設定

「Last Access」日付フィールドは通常、管理対象オブジェクトがユーザーおよびデータ・リダクション実行によってリクエストされると、Content Tracker によって更新されます。このため、Content Server の DocMeta データベース表の「Last Access」フィールドは、次のデータ・リダクションが実行されるまで空（NULL）になることがあります。

ただし、一部のアプリケーションでは、「Last Access」フィールドにコンテンツ・チェックインの日時が即時に記録されることが必要です。この要件を満たすため、「Last Access」フィールドに適切な日時の値を移入する必要があります。Content Tracker では、「Last Access」フィールドに値を移入するための複数の方法があります。

- 「Default Value」を使用した「Last Access」フィールドの移入（3-31 ページ）
- 「Autoload」オプションを使用した「Last Access」フィールドの移入（3-32 ページ）
- バッチロードおよびアーカイブのための「Last Access」フィールドの移入（3-33 ページ）

「Default Value」を使用した「Last Access」フィールドの移入

通常、デフォルト値を持つフィールドに値を入力する必要はありません。ただし、指定されたデフォルト値がない場合にこのフィールドに値を入力しないと、コンテンツ・アイテムのチェックイン時にフィールドは移入されません。チェックイン日付または最新アクセス日付は、データ・リダクションが実行されて初めて記録されます。

特定のアプリケーションの要件をサポートするには、「Autoload」オプションを使用して、既存のコンテンツの「Last Access」フィールドに値を再び入力することができます(3-32 ページの「「Autoload」オプションを使用した「Last Access」フィールドの移入」を参照)。将来のコンテンツ・アイテム・チェックインのすべてについて、「Default Value」フィールドを設定することにより、「Last Access」カスタム・メタデータ・フィールドを構成できます。

入力する値は、フィールドにコンテンツ・チェックインの日時を移入する関数または式である必要があります。これによって、確実に現在の日時が「Last Access」フィールドに自動的に入力されます。

「Default Value」フィールドを使用して「Last Access」フィールドに値を移入するには、次のようにします。

1. Content Tracker の「Administration」ページを開きます。

   これには、「Administration」トレーから「Content Tracker Administration」を選択します。

2. **「Configuration Manager」**アイコンをクリックします。

   「Configuration Manager」インタフェースが表示されます。

3. 「Information Fields」タブで、「Last Access」メトリックにリンクしたカスタム・メタデータ・フィールドを選択し、**「Edit」**をクリックします。

   「Edit Custom Info Field」画面が表示されます。

注意 : 「Last Access」カスタム・メタデータ・フィールドがすでに存在している必要があります。存在していない場合は作成して、「Last Access」アクティビティ・メトリック機能にリンクする必要があります。3-26 ページの「「Last Access」メトリック用のカスタム・メタデータ・フィールドの作成」を参照してください。

4. 「Default Value」フィールドに、フィールドにコンテンツ・チェックインの日時を移入する式を入力します。

   たとえば、「Last Access」フィールドに現在のチェックインの日時を移入する場合は、デフォルト値の <$dateCurrent()$> を指定します。

5. **「OK」**をクリックします。

   「Last Access」カスタム・メタデータ・フィールドが更新されます。

6. 既存のコンテンツの「Last Access」フィールドに再び移入します（3-32 ページの「「Autoload」オプションを使用した「Last Access」フィールドの移入」を参照）。

「Autoload」オプションを使用した「Last Access」フィールドの移入

「Snapshot」タブの「Autoload」オプションを使用すると、「Last Access」フィールドの NULL 値を遡って現在の日時で置き換えることができます。「Autoload」オプションの使用で影響を受ける DocMeta レコードは、「Last Access」メタデータ・フィールドが空（NULL）になっている DocMeta レコードのみです。

「Autoload」オプションを使用して「Last Access」フィールドに値を移入するには、次のようにします。

1. **「Data Engine Control Center」**を開きます（3-23 ページの「データ・エンジン・コントロール・センターへのアクセス」を参照）。
2. **「Snapshot」**タブをクリックします。

   スナップショット機能が有効化されている必要があります。そうでない場合、アクティビティ・メトリック・オプションはアクティブになりません。3-28 ページの「スナップショット機能およびアクティビティ・メトリック・オプションの有効化」を参照してください。
3. **「Enable Last Access updates」**チェック・ボックスを選択します。
4. 「Last Access」メトリックを適用可能なカスタム・メタデータ・フィールドにリンクします（3-29 ページの「検索関連メタデータ・フィールドへの アクティビティ・メトリック機能のリンク」を参照）。
5. **「Autoload」**チェック・ボックスを選択します。
6. **「OK」**をクリックします。

   確認ダイアログ・ボックスが表示され、Content Server の DocMeta データベース表の適用可能な（NULL 値を持つ）「Last Access」フィールドに現在の日時が挿入されます。

技術ヒント : デフォルトでは、「Autoload」問合せによって「Last Access」メタデータ・フィールドが現在の日時に設定されます。ただし、問合せをカスタマイズして、「Last Access」フィールドを「dCreateDate」、「dReleaseDate」、またはアプリケーションのニーズを満たすその他の時刻に設定することもできます。A-9 ページの「「Autoload」オプションの SQL 問合せのカスタマイズ」を参照してください。

バッチロードおよびアーカイブのための「Last Access」フィールドの移入

アーカイブおよびバッチロードされたコンテンツが適切に保存されるように、インポートまたは挿入用の「Last Access」フィールド日付を設定する必要があります。そうしない場合、これらのコンテンツ・アイテムのアクセス日付は NULL になり、このフィールドに基づく保存は失敗します。

重要 : 「Last Access」日付を保存マネージャと組み合せて使用すると、保存スケジュールを保持できます。保存を成功させるには、バッチロードおよびアーカイブ中にこのフィールドが適切に設定されていることを確認することが重要です。コンテンツが最後にアクセスされた時期を最も反映している日付を慎重に考慮してください。たとえば、1998 のデータのインポートは、インポートを実行する日付よりもその日付を使用したほうがタグ付けがうまくいく場合があります。

「Last Access」フィールドの名前は、構成マネージャで指定した名前に基づいています（3-26 ページの「「Last Access」メトリック用のカスタム・メタデータ・フィールドの作成」を参照）。「Last Access」の場合、xLastAccess がインポートまたは挿入で使用されます（3-13 ページの「「Enable Last Access updates」チェック・ボックスおよび対応する「Field」メタデータ・フィールド」を参照）。

Content Server のバッチ・ローダーを使用して「Last Access」フィールドに値を移入するには、次のようにします。

1. バッチ・ローダーにアクセスします。
2. 適切な「Last Access」日付を確立するファイル・レコードを作成します。適用可能なファイル・レコードの例を次に示します。

```
# This is a comment
Action=insert
dDocName=Sample1
dDocType=ADACCT
xLastAccess=5/1/1998
dDocTitle=Batch Load record insert example
dDocAuthor=sysadmin
dSecurityGroup=Public
primaryFile=links.doc
dInDate=8/15/2001
<<EOD>>
```

3. バッチ・ローダーを実行して、ファイル・レコードを処理します。

注意 : 詳細は、『Managing System Settings and Processes』ガイドを参照してください。

スナップショット構成の編集

現行のスナップショット・アクティビティ・メトリック設定を変更するには、次のようにします。

1. 「**Data Engine Control Center**」を開きます（3-23 ページの「データ・エンジン・コントロール・センターへのアクセス」を参照）。
2. 「**Snapshot**」タブをクリックします。

   スナップショット機能が有効化されている必要があります。そうでない場合、アクティビティ・メトリック・オプションはアクティブになりません。3-28 ページの「スナップショット機能およびアクティビティ・メトリック・オプションの有効化」を参照してください。
3. アクティビティ・メトリック・フィールドに必要な変更を加えます。
4. 「**OK**」をクリックします。

   確認ダイアログ・ボックスが表示されます。
5. 「**OK**」をクリックします。

   スナップショット状態および Content Tracker の構成ファイル（sct.cfg）が更新されます。

注意 : Content Tracker では、アクティビティ・メトリック・フィールド名に対して最小のエラー・チェックが実行されます。「Snapshot」タブのフィールドでは大 / 小文字が区別されますので注意してください。すべてのフィールド値を、大文字と小文字を区別して正確なスペルで入力することが重要です。スナップショット機能に対する特定の Content Tracker エラー・チェックの詳細は、3-11 ページの「「Snapshot」タブ」を参照してください。

注意 : スナップショットおよびアクティビティ・メトリック構成変数の変更済の値を確認するには、次のディレクトリ内の Content Tracker の sct.cfg ファイルにアクセスします。

<*install_dir*>/custom/ContentTracker/resources/sct.cfg

注意 : オプションで、手動でスナップショット・アクティビティ・メトリックの構成設定を編集できます。特定のアクティビティ・メトリック構成変数の詳細は A-2 ページの「構成変数」を、その手動での編集方法は A-7 ページの「Content Tracker 構成変数の手動設定」を参照してください。

サービス・エントリの追加または編集

サービスを追加または編集するには、次のようにします。

1. **「Data Engine Control Center」**を開きます（3-23 ページの「データ・エンジン・コントロール・センターへのアクセス」を参照）。
2. **「Services」**タブをクリックします。
3. **「Add」**をクリックして、新規のサービス・エントリを作成します。

   あるいは、「Service Name」リストから既存のサービス・エントリを選択し、**「Edit」**をクリックします。

   「Extended Service Tracking」画面が表示されます。新規のサービス・エントリを追加する場合、フィールドは空です。

   既存のサービス・エントリを編集する場合、フィールドにこれらの値が移入されます。この場合、「Service Name」フィールドが非アクティブになります。
4. （「Field Map」フィールド内以外の）適用可能なフィールド値を入力または変更します。

   このサービス・エントリをフィールド・マップ ResultSet にリンクする場合、「Field Map」フィールドに適用可能な名前を入力します。その後、3-36 ページの「フィールド・マップ ResultSet の追加およびサービス・エントリへのリンク」の手順を参照してください。
5. **「OK」**をクリックします。

   確認ダイアログ・ボックスが表示されます。
6. **「OK」**をクリックします。

   「Extended Service Tracking」画面が閉じ、データ・エンジン・コントロール・センターの「Services」タブが表示されます。

   新規のサービス・エントリを追加した場合は、「Services」リストにそのエントリが追加されます。既存のサービス・エントリを編集した場合、「Services」リストに更新済のフィールド値が追加されます。

   サービス状態および Content Tracker の SctServiceFilter.hda が更新されます。

注意 : Content Tracker では、データ・エンジン・コントロール・センターの拡張サービス・トラッキング機能に対するエラー・チェック（フィールド・タイプやスペルの検証など）は実行されません。リダクションを実行するまで、エラーは生成されません。これらのフィールドでは大 / 小文字が区別されます。このため、新規のサービスを追加する場合や、既存のサービスを編集する場合は、サービス・コール名を正確に入力するように注意してください。すべてのフィールド値が、大文字と小文字を区別して正確なスペルで入力されていることを確認してください。

注意 : サービス・エントリの値が SctServiceFilter.hda ファイルに追加されていること、または既存のサービス・エントリの値が適切に変更されていることを確認するには、次のディレクトリ内の Content Tracker の SctServiceFilter.hda ファイルにアクセスします。

<*install_dir*>/custom/ContentTracker/resources/SctServiceFilter.hda

注意 : オプションで、手動でサービスを追加または編集できます。SctServiceFilter.hda ファイル内のサービス・エントリの詳細は 5-2 ページの「サービス・コール構成ファイルについて」を、その手動での編集方法は 5-9 ページの「SctServiceFilter.hda ファイルの手動編集」を参照してください。

フィールド・マップ ResultSet の追加およびサービス・エントリへのリンク

拡張サービス・コール・トラッキング機能を実装するには、サービス・エントリを SctServiceFilter.hda ファイル内のフィールド・マップ ResultSet にリンクする必要があります。

フィールド・マップ ResultSet を追加してサービス・エントリにリンクするには、次のようにします。

1. **「Data Engine Control Center」**を開きます（3-23 ページの「データ・エンジン・コントロール・センターへのアクセス」を参照）。
2. **「Services」**タブをクリックします。
3. 「Service Name」リストから必要なサービス・エントリを選択します。

   新規のサービス・エントリを追加する必要がある場合は、3-35 ページの「サービス・エントリの追加または編集」の手順 3 ～ 6 を参照してください。
4. **「Edit」**をクリックします。

   「Extended Service Tracking」画面が表示され、選択したサービス・エントリの値がフィールドに移入されます。この場合、「Service Name」フィールドが非アクティブになります。必要な場合は、フィールド・マップ ResultSet の追加以外に、このサービス・エントリの値をここで編集できます。

   このサービスがすでにフィールド・マップ ResultSet にリンクされている場合は、「Field Map」フィールドに名前がリストされ、「Field Name」、「Field Location」および「Column Name」フィールドに、1 つ以上のデータ・フィールド、ロケーションおよび表列セットがリストされます。既存のデータ・フィールド、ロケーションおよび表列セットを編集または削除する場合は、3-38 ページの「フィールド・マップ ResultSet の編集」の手順を参照してください。

5. 選択したサービスがすでにフィールド・マップ ResultSet にリンクされている場合は、この手順をスキップしてください。ただし、選択したサービスがセカンダリ ResultSet にリンクされていない場合、「Field Map」フィールドは空になります。フィールド・マップ ResultSet の名前を入力してください。
6. **「Add」**をクリックします。

   「Field Map」画面が表示されます。
7. フィールドに適切な値を入力します。
8. **「OK」**をクリックします。

   「Field Map」画面が閉じ、値が「Field Name」および「Column Name」フィールドに追加されます。

注意 : 複数のデータ・フィールド、ロケーションおよび表列セットを追加する必要がある場合は、必要に応じて手順 6 ～ 8 を繰り返します。

9. **「OK」**をクリックします。

   確認ダイアログ・ボックスが表示されます。

   「Extended Service Tracking」画面が閉じ、データ・エンジン・コントロール・センターの「Services」タブが表示されます。

   サービス状態および Content Tracker の SctServiceFilter.hda ファイルが更新されます。
10. **「OK」**をクリックします。

注意 : Content Tracker では、データ・エンジン・コントロール・センターの拡張サービス・トラッキング機能に対するエラー・チェック（フィールド・タイプやスペルの検証など）は実行されません。リダクションを実行するまで、エラーは生成されません。これらのフィールドでは、大 / 小文字が区別されます。このため、新規のフィールド・マップ ResultSet を追加する場合や、既存のフィールド・マップ ResultSet を編集する場合は、DataBinder フィールド名および SctAccessLog 表列名を正確に入力するように注意してください。すべてのフィールド値が、大文字と小文字を区別して正確なスペルで入力されていることを確認してください。

注意 : フィールド・マップ ResultSet の値がサービス・コール構成ファイルに追加されていること、または値が適切に変更されていることを確認するには、次のディレクトリ内の Content Tracker の SctServiceFilter.hda ファイルにアクセスします。

<*install_dir*>/custom/ContentTracker/resources/SctServiceFilter.hda

注意 : オプションで、手動でフィールド・マップ ResultSet を追加し、手動でサービス・エントリにリンクできます。SctServiceFilter.hda ファイル内のサービス・エントリおよびフィールド・マップ ResultSet の詳細は 5-2 ページの「サービス・コール構成ファイルについて」を、その手動での編集方法は 5-9 ページの「SctServiceFilter.hda ファイルの手動編集」を参照してください。

フィールド・マップ ResultSet の編集

フィールド・マップ ResultSet を編集するには、次のようにします。

1. **「Data Engine Control Center」**を開きます（3-23 ページの「データ・エンジン・コントロール・センターへのアクセス」を参照）。
2. **「Services」**タブをクリックします。
3. 「Service Name」リストから必要なサービス・エントリを選択します。
4. **「Edit」**をクリックします。

   「Extended Service Tracking」画面が表示され、選択したサービス・エントリの値がフィールドに移入されます。この場合、「Service Name」フィールドが非アクティブになります。必要な場合、フィールド・マップ ResultSet の編集以外に、このサービス・エントリの他のフィールド値も編集できます。
5. セカンダリ ResultSet を編集するには、次のいずれかの方法を使用します。
   - ❖ 1 つ以上のデータ・フィールド、ロケーションおよび表列セットを追加します。3-36 ページの「フィールド・マップ ResultSet の追加およびサービス・エントリへのリンク」の手順 6 ～ 8 を参照してください。
   - ❖ 次のようにして、1 つ以上のデータ・フィールド、ロケーションおよび表列セットを削除します。
     a. 削除するフィールド、ロケーションおよび表列セットを選択します。
     b. **「Delete」**をクリックします。
6. **「OK」**をクリックします。

   確認ダイアログ・ボックスが表示されます。

   「OK」をクリックします。

   「Extended Service Tracking」画面が閉じ、データ・エンジン・コントロール・センターの「Services」タブが表示されます。サービス状態および Content Tracker の SctServiceFilter.hda ファイルが更新されます。

注意 : Content Tracker では、データ・エンジン・コントロール・センターの拡張サービス・トラッキング機能に対するエラー・チェック（フィールド・タイプやスペルの検証など）は実行されません。リダクションを実行するまで、エラーは生成されません。これらのフィールドでは、大 / 小文字が区別されます。このため、1 つ以上のデータ・フィールド、ロケーションおよび表列セットを追加することによりフィールド・マップ ResultSet を編集する場合は、データ・フィールド名、ロケーション名および SctAccessLog 表列名を正確に入力するように注意してください。すべてのフィールド値が、大文字と小文字を区別して正確なスペルで入力されていることを確認してください。

注意 : フィールド・マップ ResultSet 内のデータ・フィールド、ロケーションおよび表列セットの変更済の値を確認するには、次のディレクトリ内の Content Tracker の SctServiceFilter.hda ファイルにアクセスできます。

<*install_dir*>/custom/ContentTracker/resources/SctServiceFilter.hda

注意 : オプションで、手動でフィールド・マップ ResultSet 内のデータ・フィールド、ロケーションおよび表列セットの値を変更できます。SctServiceFilter.hda ファイル内のフィールド・マップ ResultSet の詳細は 5-2 ページの「サービス・コール構成ファイルについて」を、その手動での編集方法は 5-9 ページの「SctServiceFilter.hda ファイルの手動編集」を参照してください。

サービス・エントリの削除

サービスを削除するには、次のようにします。

1. 「**Data Engine Control Center**」を開きます（3-23 ページの「データ・エンジン・コントロール・センターへのアクセス」を参照）。
2. 「**Services**」タブをクリックします。
3. 「Services」リストで、削除するサービス・エントリを選択します。

4. 「**Delete**」をクリックします。

   このサービス・エントリのサービス・ロギングを削除することを確認するように求められます。

5. 「**Yes**」をクリックします。

   選択したサービス・エントリが「Services」リストから削除され、SctServiceFilter.hda ファイルから削除されます。

注意 : サービス・エントリが削除されたことを確認するには、次のディレクトリ内の Content Tracker の SctServiceFilter.hda ファイルにアクセスします。

<*install_dir*>/custom/ContentTracker/resources/SctServiceFilter.hda

注意 : オプションで、手動で特定のサービス・エントリを削除できます。詳細は、5-9 ページの「SctServiceFilter.hda ファイルの手動編集」を参照してください。

フィールド・マップ ResultSet の削除

フィールド・マップ ResultSet を削除するには、次のようにします。

1. 「**Data Engine Control Center**」を開きます（3-23 ページの「データ・エンジン・コントロール・センターへのアクセス」を参照）。
2. 「**Services**」タブをクリックします。
3. 「Services」リストで、削除するフィールド・マップ ResultSet にリンクされているサービス・エントリを選択します。
4. 「**Edit**」をクリックします。

   「Extended Service Tracking」画面が表示され、選択したサービス・エントリの値がフィールドに移入されます。

5. 「Field Map」フィールドから、フィールド・マップ ResultSet 名を削除します。
6. データ・フィールド、ロケーションおよび表列セットを選択し、「**Delete**」をクリックします。

   リストからデータ・フィールド、ロケーションおよび表列セットが削除されます。（必要に応じて）データ・フィールド、ロケーションおよび表列セットごとに、この手順を繰り返します。

7. 「**OK**」をクリックします。

   フィールド・マップ ResultSet が SctServiceFilter.hda ファイルから削除されます。このフィールド・マップ ResultSet からサービス・エントリへのリンクが解除されます。

注意 : フィールド・マップ ResultSet が削除されたことを確認するには、次のディレクトリ内の Content Tracker の SctServiceFilter.hda ファイルにアクセスできます。

<*install_dir*>/custom/ContentTracker/resources/SctServiceFilter.hda

注意 : オプションで、手動でフィールド・マップ ResultSet を削除できます。詳細は、5-9 ページの「SctServiceFilter.hda ファイルの手動編集」を参照してください。

4

レポート生成

概要

この項の内容は次のとおりです。

概要

インタフェース

タスク

コンテンツ・トラッキング・レポートについて

コンテンツ・トラッキング・レポートでは、取得されて縮小されたデータを使用して、特定のコンテンツ部分の使用状況履歴の概要を示すレポートが生成されます。提供されている事前定義レポートを使用することも、追跡する情報に対するカスタム問合せを作成することもできます。オプションで、外部の市販レポート作成ツールを使用することもできます（4-34 ページの「外部レポート・ジェネレータ」を参照）。

レポートは、特定のユーザー、ユーザー・グループ、およびメタデータ値の問合せやグループによって定義可能なコンテンツのセットなど、広範な基準から導出できます。コンテンツ・トラッキング・レポートでは、システム内の変数（ユーザーの数、コンテンツの量、メタデータ・カウントなど）に基づいて、何百個もの主要なメトリックをレポートに含めることができます。特殊化したレポートによって、ユーザーに最も関連性の高いコンテンツを理解し、公開することができます。

一般的な考慮事項

この項の内容は次のとおりです。

Oracle および DB2 の大 / 小文字の区別

Oracle または DB2 を Content Server データベースとして使用する場合、メタデータ値では大 / 小文字が区別されるため、適用可能な問合せレポート基準でコンテンツ・メタデータ値を入力する際に注意する必要があります。このため、対応するフィールドに値を入力した方法によっては、コンテンツ・トラッキング・レポートによって使用可能な一致ファイルの一部が返されないことがあります。

Oracle または DB2 の Content Server データベースを使用する場合、値は Content Server で入力されたとおりに正確に入力する必要があります。このため、Content Server 内の値の文字構造に基づいて、問合せメタデータ・フィールドに、すべて小文字、すべて大文字、または大文字と小文字の組合せを入力する必要があります。そうしない場合、コンテンツ・トラッキング・レポートでは、一致するファイルの一部が返されません。

たとえば、Oracle または DB2 の Content Server データベースが AdAcc であるのに、ユーザーが問合せフィールドに adacc、ADACC または Adacc と入力した場合、コンテンツ・トラッキング・レポートでは結果が返されません。この場合、大文字と小文字の組合せを使用してコンテンツ・タイプ・メタデータ値を入力する必要があります。これは、各事前定義問合せレポートのすべてのメタデータ・フィールドについて適用されます。

アクセス制御リストおよびコンテンツ・トラッキング・レポートのセキュア・モード

コンテンツ・トラッキング・レポートのコンポーネントをインストールすると、セキュリティ・チェック・プリファレンス変数（SctrEnableSecurityChecks）が設定されます。基本的に、このプリファレンス変数では、2 つのセキュリティ・モード（セキュア・モードおよび非セキュア・モード）のいずれかを選択できます。セキュリティ・チェック・プリファレンスには、個々のユーザー・ロールおよびアカウント情報を使用して、レポート結果におけるコンテンツ・アイテム情報の表示を制限するためのオプションがあります。

つまり、生成されるレポートでユーザーに表示されるコンテンツ・アイテム（およびその後のメタデータ）を制御するということです。ユーザーが Content Server 検索で見つけられなかった内容はコンテンツ・トラッキング・レポートでも表示されないようにすることが理想的です。このため、セキュア・モードを選択すると、生成されるレポートの情報が、ユーザーのロールおよびアカウント権限に基づいてフィルタ処理されます。

ただし、Content Server インスタンスに対してアクセス制御リスト（ACL）を有効化した場合、コンテンツ・トラッキング・レポートのセキュア・モード・オプションは機能しません。インストール中、「security checks preference」チェック・ボックスを空白にしておく必要があります。つまり、ACL ベースのシステムでは、セキュア・モードが無効になっている必要があります。この場合、システム管理者以外のユーザーに、本来アクセスと表示の権限を与えられていないコンテンツ・アイテムに関する情報が表示される可能性があります。

注意 : セキュリティ・チェック・インストール・プリファレンスの詳細、およびそれがレポート問合せとレポート結果に与える影響は、4-23 ページの「セキュリティ・チェックおよび問合せ結果」を参照してください。インストール・プリファレンスのプロンプトおよび 2 つのセキュリティ・チェック・オプションの詳細は、『Content Tracker Installation Guide』を参照してください。

既存の SQL レポートの互換性 : コンテンツ・トラッキング・レポート 7.0 以前

Content Tracker 7.5 以上では、Content Tracker およびコンテンツ・トラッキング・レポートのコンポーネントのアーキテクチャが両方とも大きく変更されています。コンポーネントのスキーマおよび設計に大きな変更があるため、7.0 以前のバージョンの Content Tracker およびコンテンツ・トラッキング・レポートで使用した SQL レポート問合せと 7.5 以上のバージョンとの互換性を保証する実現可能な方法はありません。

ただし、次のリストに、変更された内容の詳細とその理由を示しています。この情報を見ると、ほとんどのユーザーは、それほどの問題もなく、アーキテクチャおよびスキーマの新しい変更に問合せを適合させることができます。

- アクセス情報収集は Web サーバーから Content Server に変更されたため、Content Tracker は Web サーバー・タイプに依存しません。このため、Content Tracker はイベント・ログを特定の書式で記述するために Web サーバーに依存する必要がなくなります。
- Web サーバー依存がなくなった結果、Content Tracker およびコンテンツ・トラッキング・レポートのコンポーネントのインストールが大幅に簡素化されています。さらに、サポートされるサーバー構成の数およびタイプが大幅に増加しました。たとえば、Content Tracker では、複数の Web サーバーで構成される場合や、Web サーバーが Content Server ストレージ・ボリュームに直接アクセスできない場合のインストールもサポートされるようになりました。
- Content Tracker では、コンテンツ・アイテムのメタデータが記録されなくなったため、コンテンツ・メタデータ表は生成されません。コンテンツ・アイテムのメタデータには標準の Content Server メタデータ表が使用されます。これにより、必要な処理が少なくなります。また、Content Tracker からすべてのメタデータにアクセス可能であること、およびメタデータ値が最新かつ正確であることが保証されます。さらに、冗長な出力表をなくすことで、冗長なコンテンツ・メタデータ・ロギングを中止しています。
- Content Tracker では、これまでどおり、ユーザー・メタデータが記録され、リダクション・プロセス中にデータベース内の適用可能な Content Tracker メタデータ表が更新されます。これにより、ユーザー・メタデータ履歴の正確性が保証されます。
- 静的 URL 参照は Web サーバー・フィルタ・プラグインによって収集および記録され、Content Server サービス・コールはサービス・ハンドラ・フィルタによって記録されます。どちらのタイプのイベント詳細も、SctEnhanced 表に換わる表（SctAccessLog）に記録されます。この表は、Content Tracker v7.0 以上で使用されます。
- Content Tracker v7.5 以上での構造上の変更によって、対象範囲が拡大され、管理対象コンテンツの使用状況レポート作成の精度が向上しました。これは、Web サーバー・ログ・ファイルが使用されなくなったこと、静的 URL アクセスと Content Server サービス・コール両方のコレクションが拡張されたこと、および Content Tracker がすべてのメタデータ値（ユーザーおよびコンテンツ・アイテムの両方）に確実にアクセスできるようになったことによるものです。

  Content Tracker では、URL レベルでページおよびオブジェクト・アクセスについてレポートを作成するのではなく、テンプレートおよびフラグメント・レベルでアクティビティを追跡できるようになりました。これにより、ユーザーは様々なコンテンツ・アイテム要素の使用状況を確認できます。つまり、Content Tracker では、Site Studio サイトや Content Server のネイティブ・インタフェースを使用しないそ

の他のアプリケーションに対しても、より興味深い分析を実行できるようになりました。

- 検索結果は、ユーザー・アクセスに関する特定のデータと統合できます。ユーザー・アクセス・アクティビティの記録には、カスタム・メタデータ・フィールドが使用されます。レポートに含まれるトラッキング結果により、特定のコンテンツ・アイテムの人気度や、特定の期間中のアクセス・データなどが示されます。アクセス・トラッキングは、内部ユーザーと外部ユーザーの両方を対象とすることができます。
- セキュリティ・チェック機能によって、オプションで、ユーザーのロールおよびアカウント権限の検証を実施できます。セキュリティ・チェック機能が有効になっている場合、レポートをリクエストしたユーザーのロールおよびアカウント権限に基づいてデータがフィルタ処理されます。このため、ユーザーが異なれば、同じレポートを生成しても結果が異なることがあります。セキュリティ・チェック機能が有効になっていない場合、デフォルトの SQL レポート問合せによって、ユーザーおよびアカウントのメンバーシップに関係なく、すべてのユーザーに対して同じデータでレポートが生成されます。

事前定義問合せレポート

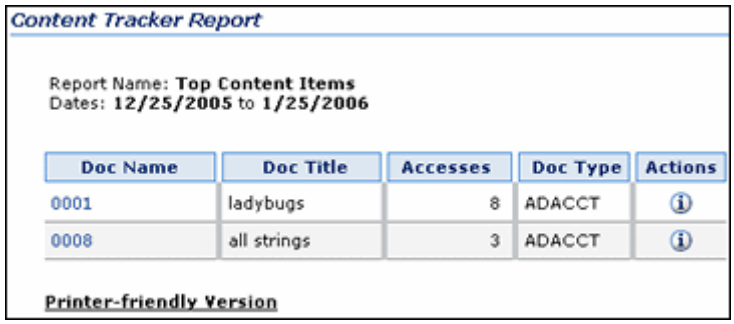
この項の内容は次のとおりです。

デフォルトのレポート書式

Content Tracker Report Generator のメイン・ページを使用して生成されたレポートの一般的な書式およびビジュアル・レイアウトは、いずれも同じです。Content Tracker Report Generator のメイン・ページがアクセスされたときにデフォルトで選択される「Top Content Items」レポートを、次に示します。レポートによって提供される情報は、必要に応じて SctAccessLog データベース表およびその他の Content Server データベース表の縮小済データから抽出されたものです。

注意 : Content Tracker Report Generator のコンパイル済結果に含まれるのは、コンテンツ・アイテムを物理的に開いたユーザーのみです。開かれるコンテンツ・アイテムは、Web ロケーション・ファイル（コンテンツ・アイテムへの絶対パス）、HTML バージョン（Dynamic Converter を使用）、または実際のネイティブ・ファイルです。「Content Information」ページのみを開いたユーザーは、追跡データに含まれません。

注意 : 通常、ユーザーがコンテンツ・アイテムにアクセスしてから、その情報が Content Tracker Report Generator のアクセス履歴結果に含められるまでに、1 日の遅れがあります。情報は最初に Content Tracker によって蓄積されてから、データ・リダクション・サイクルを経過する必要があります。このため、コンテンツ・アイテム・アクセス履歴結果は、SctAccessLog およびその他の Content Server データベース表の縮小済データから導出されます。データを手動で縮小すると、即時にデータベース表が更新されます。その後、生成された問合せレポートにも更新済の情報が表示されます。リダクション・プロセスの詳細は、3-4 ページの「「Reduction」タブ」を参照してください。


Content Tracker Report

Report Name: **Top Content Items**
Dates: **12/25/2005** to **1/25/2006**

Doc Name	Doc Title	Accesses	Doc Type	Actions
0001	ladybugs	8	ADACCT	
0008	all strings	3	ADACCT	

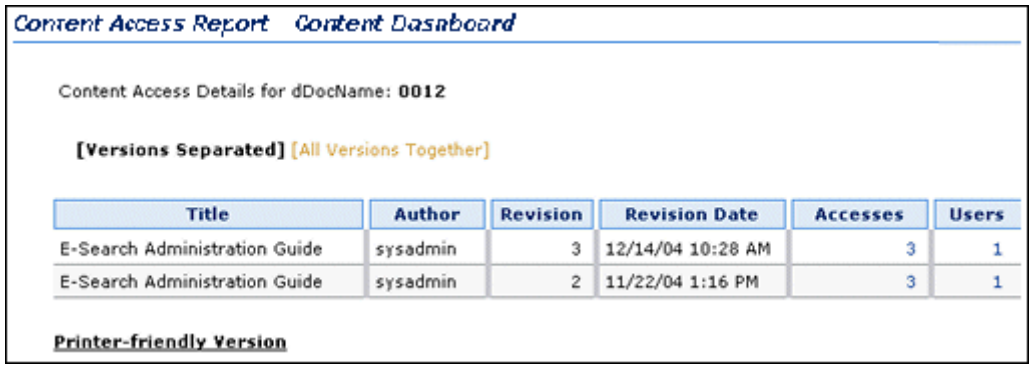
Printer-friendly Version

フィールド	説明
「Report Name」フィールド	選択された問合せレポートの名前。
「Dates」フィールド	「Start Date」および「End Date」フィールドに入力された日付。特定の日付を入力しない場合、デフォルトの日付が問合せに使用されます。

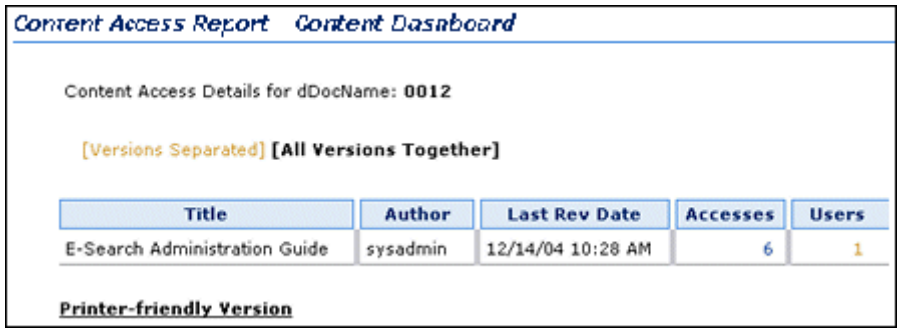
フィールド	説明
結果表の列	選択されたレポートに関連する情報を示します。
「Printer-friendly Version」リンク	新しいブラウザ・ウィンドウを開き、ナビゲーション・トレーなしでレポートを表示します。

コンテンツ・ダッシュボード機能

生成された問合せレポートに特定のコンテンツ・アイテムへのアクティブ・リンクが含まれる場合、リンクをクリックすると、対応するコンテンツ・ダッシュボードが表示されます。次の画面キャプチャのコンテンツ・ダッシュボードは、特定のコンテンツ・アイテムの 2 つのバージョンがそれぞれ 3 回アクセスされたことを示しています。このビューでは、リビジョン・アクセス結果が個別に示されています。

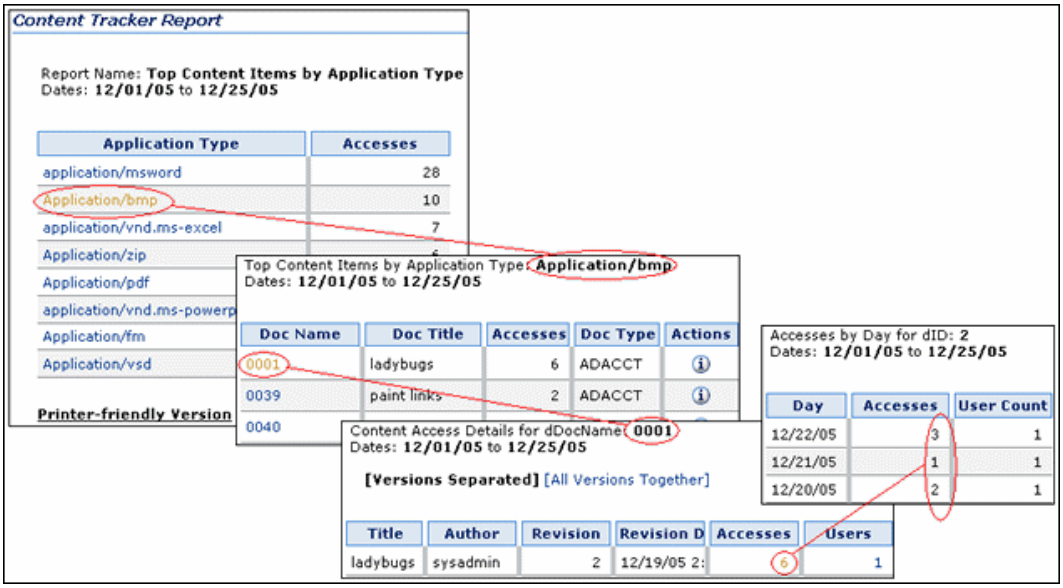


コンテンツ・ダッシュボードの「All Versions Together」リンクをクリックすると、両方のバージョンのアクセス結果が結合されます。



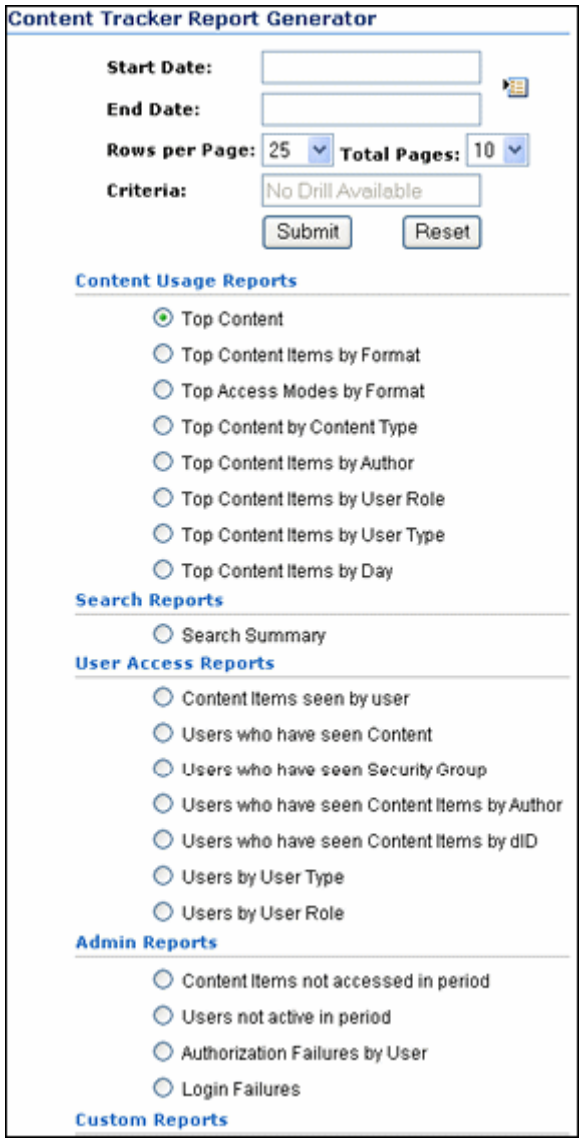
ドリルダウン・レポート機能

事前定義レポートごとに、様々なレベルのレポート結果が生成されます。Content Tracker Report Generator のメイン・ページに入力した検索基準に基づいて、結果が適宜フィルタ処理されます。最上位レベルのレポートはサマリー・レポートで、一般性の高い情報が示されます。最上位レベルのレポートのリンクを使用すると、より具体的な情報にドリルダウンできます。



Content Tracker Report Generator のメイン・ページ

コンテンツ・トラッキング・レポート・コンポーネントには、複数のメイン・カテゴリ別に編成された事前定義問合せが用意されています。これらの事前定義レポートは、システム・アクティビティに関する最も共通性の高い質問に答えるような設計になっています。個々のレポートには、適用可能な基準に基づくドリルダウン・レポートが示されます。Content Tracker Report Generator のメイン画面にアクセスするには、「Administration」トレーの「Content Tracker Reports」リンクをクリックします。



フィールド	説明
「Start Date」フィールド	レコードを検索する特定期間の開始日を指定します。
「End Date」フィールド	レコードを検索する特定期間の終了日を指定します。
日付ドロップダウン・メニュー	**Yesterday:** 「Start Date」フィールドに前日の日付を、「End Date」フィールドに今日の日付を入力します。 **Latest Week:** 「Start Date」および「End Date」フィールドに前週の開始日および終了日を入力します。 **Latest Month:** 「Start Date」および「End Date」フィールドに前月の開始日および終了日を入力します。 **Latest Year:** 「Start Date」および「End Date」フィールドに前年の開始日および終了日を入力します。
「Rows per Page」フィールド	レポートの各ページに含めることのできる結果行の数を指定します。
「Total Pages」フィールド	レポートに含めることのできる結果ページの最大数を指定します。
「Criteria」フィールド	検索結果をフィルタ処理し、適用可能なドリルダウン・レポートに即時にアクセスします。たとえば、作成者別の上位コンテンツ・アイテムを検索する場合、「Criteria」フィールドに特定の作成者を入力すると、そのユーザーが作成したコンテンツ・アイテムがリストされたドリルダウン・レポートが表示されます。このフィールドを空白のままにすると、最上位レベルの問合せが実行され、システムの作成者のリストが表示されます。
「Submit」ボタン	選択されたレポート・タイプを生成して表示します。
Content Item Usage Reports	
Top Content	システム内で最も頻繁にアクセスされたコンテンツ・アイテムをリストします。
Top Content Items by Format	最も頻繁にアクセスされたコンテンツ・アイテムを、アプリケーション・タイプ（pdf、txt など）別にリストします。
Top Access Modes by Format	最も頻繁にアクセスされたコンテンツ・アイテム・アプリケーション・タイプ（pdf、txt など）を、アクセス・モード別にリストします。

フィールド	説明
Top Content by Content Type	最も頻繁にアクセスされたコンテンツ・アイテムを、コンテンツ・アイテム・タイプ別にリストします。
Top Content Items by Author	最も頻繁にアクセスされたコンテンツ・アイテムを、作成者別にリストします。
Top Content Items by User Role	最も頻繁にアクセスされたコンテンツ・アイテムを、ユーザー・ロール別にリストします。
Top Content Items by User Type	最も頻繁にアクセスされたコンテンツ・アイテムを、ユーザー・タイプ別にリストします。
Top Content Items by Day	最も頻繁にアクセスされたコンテンツ・アイテムを、日別にリストします。
Search Reports	
Search Summary	実行された検索のタイプおよび検索基準をリストします。
User Access Reports	
Content Items seen by user	指定されたユーザーによって最も頻繁に開かれたコンテンツ・アイテムの数を、特定のユーザー別にリストします。
Users who have seen Content	コンテンツ・アイテムにアクセスしたユーザーを、特定のコンテンツ・アイテム別にリストします。
Users who have seen Security Group	特定のセキュリティ・グループ内で最も頻繁にアクセスされたコンテンツ・アイテムを、特定のユーザー別にリストします。
Users who have seen Content Items by Author	特定のユーザーによって作成（チェックイン）され、最も頻繁にアクセスされたコンテンツ・アイテムを、特定のユーザー別にリストします。
Users who have seen Content Items by dID	内部コンテンツ・アイテム識別番号に基づいて最も頻繁にアクセスされたコンテンツ・アイテムを、特定のユーザー別にリストします。
Users by User Type	ユーザー・タイプに基づいて最も頻繁にアクセスされたコンテンツ・アイテムを、特定のユーザー別にリストします。

フィールド	説明
Users by User Role	ユーザー・ロールに基づいて最も頻繁にアクセスされたコンテンツ・アイテムを、特定のユーザー別にリストします。
Admin Reports	
Content Items not accessed in period	アクセスされていないコンテンツ・アイテムに続いて、最も頻繁にアクセスされたコンテンツ・アイテムをリストします。
Users not active in period	コンテンツ・アイテムにアクセスしていないユーザーに続いて、コンテンツ・アイテムにアクセスしたユーザーをリストします。
Authorization Failures by User	認可権限を持っていないコンテンツ・アイテムにアクセスしようとして失敗したユーザーをリストします。
Login Failures	システムにログインしようとして失敗したユーザーをリストします。
Custom Reports	
カスタム・レポート名	ユーザー定義の検索問合せに基づいて、カスタマイズされたレポートを生成します。

レポートの生成

事前定義レポートまたはカスタム・レポートを生成するには、次のようにします。

1. 「Administration」トレーの**「Reports」**リンクをクリックして、Content Tracker Report Generator のメイン画面を開きます。
2. 必要なレポート・タイプのラジオ・ボタンを選択します。
3. 適用可能なフィールドに、必要な検索基準およびフィルタ処理基準を入力します。
4. **「Submit」**をクリックします。

   選択したレポート・タイプが表示されます。

ドリルダウン・レポートへのアクセス

1 つ以上のドリルダウン・レポートにアクセスするには、次のようにします。

1. 事前定義レポートまたはカスタム・レポートを生成します。4-13 ページの「レポートの生成」を参照してください。
2. 事前定義レポートを生成すると、各行のアイテム結果にアクティブなドリルダウン・レポート・リンクが設定されます。必要なリンクをクリックします。

   選択したドリルダウン・レポートが表示されます。

注意 : 一部のレポートには、複数のレベルのドリルダウン・レポートが含まれます。たとえば、「Top Content Items」レポートには「DocName」ドリルダウン・レポート・リンクが含まれます。このリンクをクリックすると、選択したコンテンツ・アイテムの適用可能なコンテンツ・アイテム詳細を示す別のレポートが生成されます。このレポート内に、さらに 2 つの使用可能なドリルダウン・レポート（アクセス用とユーザー用）があります。

「Information」ページからのレポートへのアクセス

コンテンツ・アイテムの「Access History Report」は、次のようにして、そのコンテンツ・アイテムの「Information」ページから生成できます。

1. コンテンツ・アイテムを検索し、関連付けられた「Info」アイコンをクリックします。

   「Content Information」ページが表示されます。
2. 「Global Actions」リストから**「View Access History Report」**を選択します。

   コンテンツ・アイテムの最新の「Content Access Report」が表示されます。
3. 「Content Access Report」で、アクティブな**「Accesses」**リンクをクリックします。

   コンテンツ・アイテムの最新の「Accesses by Day」レポートが表示されます。
4. 「Content Access Report」で、アクティブな**「Users」**リンクをクリックします。

   コンテンツ・アイテムの最新の「Accesses by User」レポートが表示されます。

個別のアクセス結果の表示

デフォルトでは、1 つのコンテンツ・アイテムの複数バージョンのアクセス結果は、コンテンツ・ダッシュボードで個別に表示されます。コンテンツ・ダッシュボード・レポートで個別のアクセス結果ビューを表示するには、次のようにします。

1. Content Tracker Report Generator のメイン・ページから、コンテンツ・アイテム・ベースの問合せレポートを生成します。4-13 ページの「レポートの生成」を参照してください。たとえば、(Content Tracker Report Generator のメイン・ページの)「Content Items Usage Reports」リストから「Top Content（4-11 ページ)」を選択して、適用可能なレポートを生成します。
2. 結果レポートからコンテンツ・アイテムを選択し、「DocName」列にリストされているコンテンツ識別番号をクリックします。

   選択したコンテンツ・アイテムのコンテンツ・ダッシュボードが表示されます。デフォルトでは、このビューに、選択したコンテンツ・アイテムのうちアクセスされたコンテンツ・アイテムの各リビジョンについてアクセス結果が表示されます。詳細は、4-8 ページの「コンテンツ・ダッシュボード機能」を参照してください。

結合されたアクセス結果の表示

コンテンツ・ダッシュボード・レポートで結合されたアクセス結果ビューを表示するには、次のようにします。

1. Content Tracker Report Generator のメイン・ページから、コンテンツ・アイテム・ベースの問合せレポートを生成します。4-13 ページの「レポートの生成」を参照してください。たとえば、(Content Tracker Report Generator のメイン・ページの)「Content Items Usage Reports」リストから「Top Content（4-11 ページ)」を選択して、適用可能なレポートを生成します。
2. 結果レポートからコンテンツ・アイテムを選択し、「DocName」列にリストされているコンテンツ識別番号をクリックします。

   選択したコンテンツ・アイテムのコンテンツ・ダッシュボードが表示されます。
3. **「All Versions Together」**リンクをクリックします。

   結果のコンテンツ・ダッシュボード・ビューに、両方のバージョンの結合されたアクセス結果が表示されます。

カスタム問合せレポート

コンテンツ・トラッキング・レポートで提供されているサンプル・レポート以外にも、情報を追跡するためのカスタム問合せを作成することができます。

この項の内容は次のとおりです。

考慮事項

カスタム・レポート問合せの作成を開始する前に、問合せの設計方法に関連するいくつかの問題に注意する必要があります。次のような問題があります。

カスタム・レポート問合せおよび Oracle

Oracle および別名を使用して、生成されるレポートに列名を表示するには、次のファイルに別名を追加する必要があります。

<*install_dir*>/shared/config/resources/upper_clmns_map.htm

例 :

たとえば、次のような列ヘッダーを表示するとします。

Name
Access_Date_GMT

この場合、upper_clmns_map.htm ファイル内に次の行を入力する必要があります。

```
<tr>
<td>NAME</td>
<td>Name</td>
</tr>
<tr>
<td>ACCESS_DATE_GMT</td>
<td>Access_Date_GMT</td>
</tr>
```

カスタム・レポート問合せおよび拡張サービス・トラッキング

拡張サービス・トラッキング機能を使用する場合、SQL 問合せを設計する前に、SctAccessLog 表の特定の列に書き込まれるデータ値に注意する必要があります。特に、サービス名が常に sc_scs_idcService 列に記録されることに注意してください。このため、問合せで拡張されたフィールドのコンテンツを使用する場合は、修飾子としてサービス名を含める必要があります。

拡張サービス・トラッキング機能の詳細は、3-16 ページの「「Services」タブ」および 5-2 ページの「サービス・コール構成ファイルについて」を参照してください。

カスタム・レポート問合せの作成：例

この項では、非セキュアなカスタム・レポート問合せを作成する方法の例を示します。この特定の問合せでは、ユーザーとその個人属性がリストされたレポートが生成されます。データは、Content Server の Users データベース表から導出されます。

注意：この項の例では、非セキュアな問合せを使用しています。このため、生成されたレポート結果は、ユーザーのロールおよびアカウント権限に関係なくどのユーザーでも表示できます。すべてのレポートは、非セキュアまたはセキュアな問合せを使用して生成されます。問合せの選択項目は、セキュリティ・モードによって異なります。オプションのセキュリティ・チェック・プリファレンス変数の詳細は、4-23 ページの「セキュリティ・チェックおよび問合せ結果」を参照してください。セキュアなレポート問合せを作成する場合は、4-32 ページの「セキュア・レポート問合せの作成」を参照してください。

カスタム・ユーザー・レポートを作成するには、次のようにします。

1. SQL レポート問合せを設計します。
2. カスタム・レポート問合せをコンテンツ・トラッキング・レポートの問合せファイルに入力します。
   a. テキスト・エディタで、contenttrackerreports_query.htm ファイルを開きます。

      <*install_dir*>/custom/ContentTrackerReports/resources/contenttrackerreports_query.htm

   b. カスタム・レポート名、列名およびソース・データベース表を入力します。

      たとえば、問合せファイルの次の部分は、カスタム問合せレポートによって Users データベース表のすべての列から情報が抽出されることを示しています。

```
<tr>
    <td>qCustomUsers</td>
    <td>
SELECT *
FROM Users
    </td>
    </tr>
```

3. Content Tracker Report Generator のメイン・ページ・ファイル内に、カスタム・レポートへのリンクを入力します。

   a. 次のディレクトリを開きます。

      <install_dir>/custom/ContentTrackerReports/templates

   b. テキスト・エディタで、次のファイルを開きます。

      contenttrackerreports_main_page.htm

   c. 属性を入力して、Content Tracker Report Generator のメイン・ページにリンクを表示します。

      たとえば、メイン・ページ・ファイルの次の部分は、カスタム・レポート・リンクが選択可能なラジオ・ボタンとして表示され、ページに "Custom Users Report" としてリストされることを示しています（4-19 ページの「「Custom Report」リンク」を参照）。

      ```
      <h4 class=xuiSubheading>Custom Reports</h4>
      <table width=80% border=0>
      <tr>
          <td> <span class="tableEntry"><input type="radio"
          name="radiobutton" value="qCustomUsers">
          Custom Users Report </span></td>
      </tr>
      </table>
      ```

4. コンテンツ・トラッキング・レポートのテンプレート・リソース・ファイル内に、書式設定の要件を入力します。

   a. 次のディレクトリを開きます。

      <install_dir>/custom/ContentTrackerReports/resources

   b. テキスト・エディタで、次のファイルを開きます。

      contenttrackerreports_template_resource.htm

      結果のカスタム・レポート書式を表示するには、4-20 ページの「生成されたカスタム・レポート」を参照してください。

c. 生成されたカスタム・レポートおよび必要なドリルダウン・レポートに対して使用する表示機能を入力します（4-20 ページの「ドリルダウン・レポート」を参照）。

たとえば、テンプレート・リソース・ファイルの次の部分は、リンクのリストの他に、レポート・タイトルが "Deanna's First Report" であり、「Content Items seen by user」レポートに基づいてドリルダウン・レポートが生成されることを示しています。

```
<!-- Custom Template -->
<@dynamichtml qCustomUsers_vars@>
    <$reportWidth = "100%"$>
    <$title = "<i>Content Access Report</i>"$>
    <$reportTitle="Deanna's First Report"$>
    <$column1Width="35%"$>
    <$column0Drill="qSctrDocsSeenByUser_Drill"$>
<@end@>
```

5. Content Server を再起動して、変更を適用します。

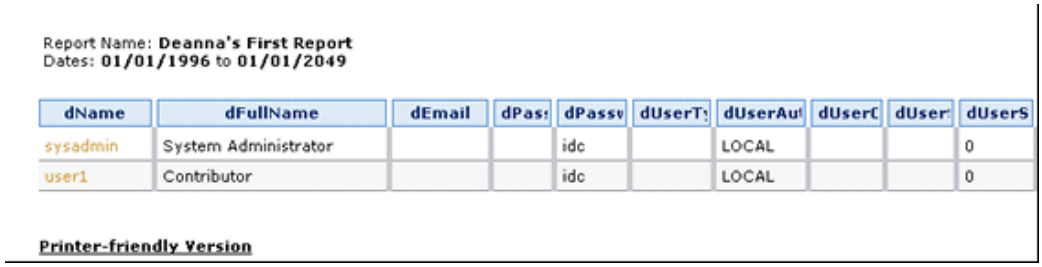
カスタム・レポート問合せの表示結果

カスタム・レポート問合せをレポート問合せファイルに追加した後は、それを使用し、結果を表示できるようになります。

- 「Custom Report」リンク（4-19 ページ）
- 生成されたカスタム・レポート（4-20 ページ）
- ドリルダウン・レポート（4-20 ページ）

「Custom Report」リンク

生成されたカスタム・レポート

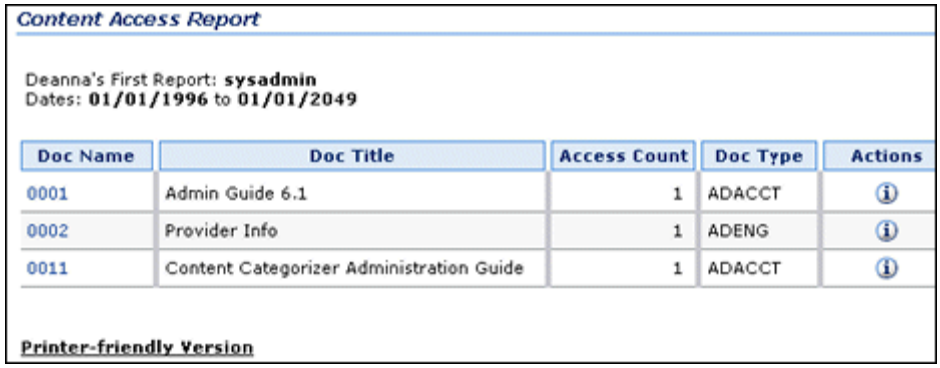


Report Name: **Deanna's First Report**
Dates: **01/01/1996** to **01/01/2049**

dName	dFullName	dEmail	dPas:	dPassv	dUserT:	dUserAu:	dUserC	dUser:	dUserS
sysadmin	System Administrator			idc		LOCAL			0
user1	Contributor			idc		LOCAL			0

Printer-friendly Version

ドリルダウン・レポート



Content Access Report

Deanna's First Report: **sysadmin**
Dates: **01/01/1996** to **01/01/2049**

Doc Name	Doc Title	Access Count	Doc Type	Actions
0001	Admin Guide 6.1	1	ADACCT	
0002	Provider Info	1	ADENG	
0011	Content Categorizer Administration Guide	1	ADACCT	

Printer-friendly Version

補足的なレポート機能

この項の内容は次のとおりです。

ユーザー認証 / 認可の管理および監査

コンテンツ・トラッキング・レポートには、システムまたは権限で保護されたコンテンツ・アイテムへの失敗したアクセス試行を監視できる監査機能が備わっています。セキュリティ違反の試行の分析に役立つ 2 つのレポートが使用可能です。これらのレポートには、失敗したユーザー・ログオンと、セキュアなコンテンツ・アイテムへの失敗したアクセスが示されます。この情報は、システムやコンテンツのセキュリティを保護したり、監査証跡およびレコードを適切にメンテナンスするうえで不可欠です。

次の監査レポートが使用可能です。

- **Authorization Failures by User（4-13 ページ）**

  このレポートには、ユーザー名とその IP アドレスを含むアクセス認可否認情報が示されます。これらのユーザーにはシステム・アクセス権限がありますが、ユーザーのロールまたはアカウントのメンバーシップによって特定のコンテンツ・アイテムへのアクセス（給与コンテンツへのアクセスなど）が制限されることがあります。

- **Login Failures（4-13 ページ）**

  このレポートには、ユーザー名とその IP アドレスを含む、ログインおよび認証の失敗情報が示されます。記録されたデータでは、外部ユーザー、内部ユーザーおよびグローバル・ユーザーは区別されていません。これは、ログインが成功しなければ、ユーザー・タイプを区別することができないためです。

Site Studio の Web サイト・アクティビティ・レポート作成

Site Studio を使用している場合、Site Studio アクティビティが追跡されるように Content Tracker が自動的に構成されます。コンテンツ・トラッキング・レポートでは、記録されたデータを使用して、Web サイト・アクセス結果を要約する事前定義レポートが生成されます。コンテンツ・トラッキング・レポートでは、次のような Site Studio 固有のアクティビティをサポートしています。

- メイン・ページの Site Studio レポート・リンク（4-22 ページ）
- Site Studio の事前定義レポート（4-22 ページ）

メイン・ページの Site Studio レポート・リンク

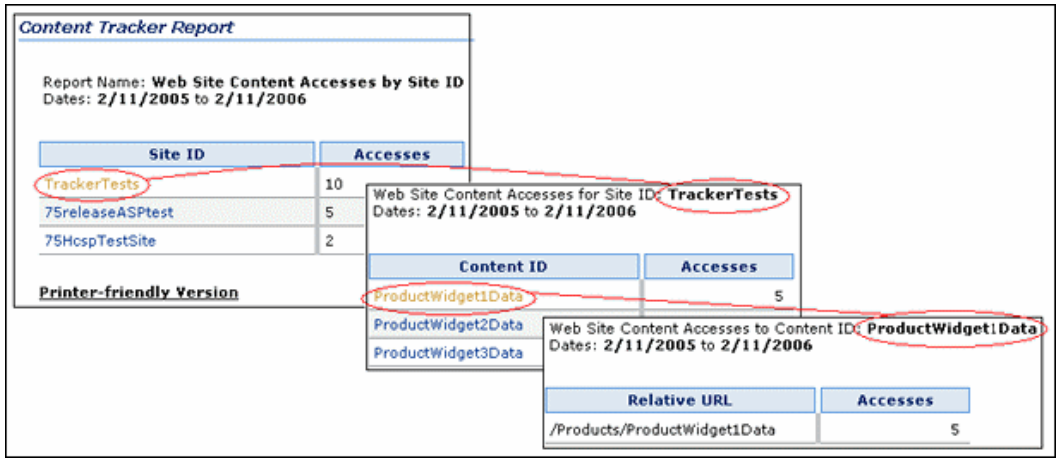
Site Studio をインストールした場合、コンテンツ・トラッキング・レポートのメイン・ページに、Site Studio に固有の Web アクセス・レポートが表示されます。これらのレポートは、User Access Reports（4-12 ページ）の事前定義レポート・グループに続いて表示されます。

Site Studio の事前定義レポート

Site Studio の事前定義レポートでは、デフォルトのコンテンツ・トラッキング・レポート書式設定が使用され、ドリルダウン・レポート機能が提供されます。どちらの場合も最上位レベル・レポートは、「Site ID」および「Accesses」を汎用基準として使用したサマリー・レポートです。ドリルダウン・レポートには、関連する統計が示されます。

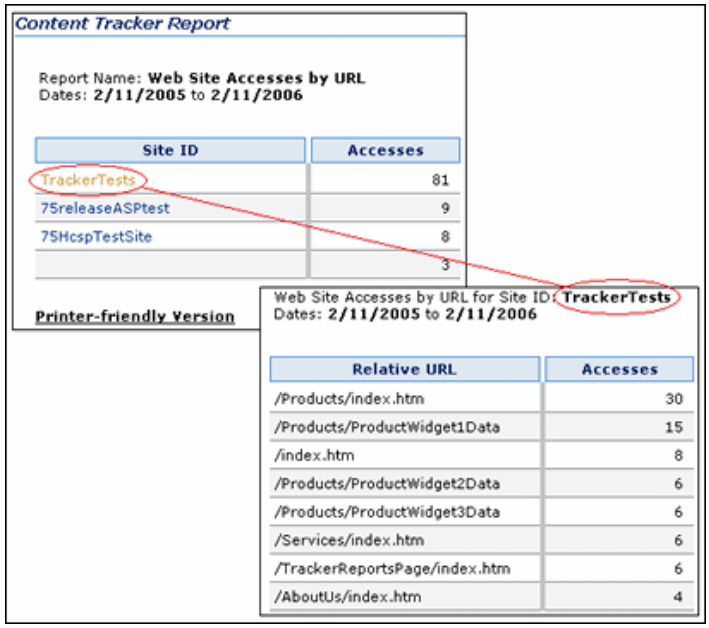
❖ **Web サイト・コンテンツ・アクセス**

このレポートは最上位レベルでは ID ベースです。それ以降のドリルダウン・レポートでは、結果がコンテンツ ID および相対 URL 別にリストされます。Web サイトへのアクセスに使用されている URL が、情報に示されます。しかし実際には、同じページが多数の異なる URL で表示される場合もあります。このため、このレポートの結果には、ユーザーがノードにアクセスした方法に関係なく、ノードの合計ヒット数も含まれます。



❖ **URL 別の Web サイト・アクセス**

このレポートには、サイト関連 URL および関連するアクティビティの合計が要約されます。



セキュリティ・チェックおよび問合せ結果

コンテンツ・トラッキング・レポートのインストール・プロセス中、個々のユーザー・ロールおよびアカウント情報を使用してレポート結果におけるコンテンツ・アイテム情報の表示を制限するように選択できます。つまり、生成されるレポートでユーザーに表示されるコンテンツ・アイテム（およびその後のメタデータ）を制御するということです。ユーザーが Content Server 検索で見つけられなかった内容はコンテンツ・トラッキング・レポートでも表示されないようにすることが理想的です。

警告 : Content Server インスタンスに対してアクセス制御リスト（ACL）を有効化した場合、コンテンツ・トラッキング・レポートのセキュア・モード・オプションは機能しません。詳細は、4-4 ページの「アクセス制御リストおよびコンテンツ・トラッキング・レポートのセキュア・モード」を参照してください。

この項の内容は次のとおりです。

セキュリティ・チェック・プリファレンス変数

コンテンツ・トラッキング・レポートのコンポーネントをインストールすると、セキュリティ・チェック・プリファレンス変数（SctrEnableSecurityChecks）が設定されます。基本的に、このプリファレンス変数では、2 つのセキュリティ・モード（セキュア・モードおよび非セキュア・モード）のいずれかを選択できます。セキュア・モードでは、レポート問合せを実行しているユーザーが考慮されますが、非セキュア・モードでは考慮されません。

注意 : インストール中、「security checks」チェック・ボックスを選択するか、または空白にしておくことにより、使用するモードを選択します。セキュリティ・チェック・プリファレンス変数およびコンテンツ・トラッキング・レポート・コンポーネントのインストールの詳細は、『Content Tracker Installation Guide』を参照してください。インストール後に、コンポーネント・マネージャを使用して設定を変更するためのオプションもあります（4-30 ページの「セキュリティ・チェック・プリファレンス設定の変更」を参照）。

この項の内容は次のとおりです。

セキュリティ・チェック・プリファレンス変数の値

セキュリティ・チェック・プリファレンス変数の値は、次のとおりです。

- **`SctrEnableSecurityChecks=True`**（チェック・ボックスが選択された状態）を設定すると、セキュリティ・チェック・インストール・プリファレンスが有効化され、コンテンツ・トラッキング・レポートがセキュア・モードで動作するように構成されます。

  セキュア・モードでは、Content Server 検索結果の制限に使用された同じセキュリティ基準（ロールおよびアカウントの制限）が、Content Tracker Report Generator の問合せおよび生成されるレポートにも適用されます。このため、2 つの異なるユーザーが「Top Content Items」レポートを実行した場合、それぞれに異なる結果が表示されることがあります。4-25 ページの「セキュア・モードの例 :」を参照してください。

- **`SctrEnableSecurityChecks=False`**（チェック・ボックスが選択解除された状態）を設定すると、セキュリティ・チェック・インストール・プリファレンスが無効化され、コンテンツ・トラッキング・レポートが非セキュア・モードで動作するように構成されます。これがデフォルト設定です。

  非セキュア・モードでは、Content Server 検索結果の制限に使用された追加のロールおよびアカウント基準は、Content Tracker Report Generator の問合せおよび生成されるレポートには適用されません。このため、システム管理者以外のユーザーに、アクセスと表示の権限を付与していないコンテンツ・アイテムに関する情報が表示される可能性があります。4-25 ページの「非セキュア・モードの例 :」を参照してください。

セキュリティ・モードの例

ユーザーが、管理者権限、コントリビュータ権限、ゲスト権限およびシステム・マネージャ権限を持っている（準管理者ユーザー）が、特定のコンテンツ・アイテム（給与レポートなど）を表示するための適切なロールまたはアカウントのメンバーシップを持っていないとします。割り当てられた権限を使用すると、このユーザーは Content Server の管理ページ（結果的には、Content Tracker Report Generator のメイン・ページ）にアクセスできます。しかし、このユーザーが Content Server で標準検索を実行した場合、結果ページには給与レポートが存在することは示されません。

セキュリティ・チェック・プリファレンス変数が有効化されている場合、コンテンツ・トラッキング・レポートでは、同じロールおよびアカウントのメンバーシップ・チェックが実施されます。次に、特定のレポートをリクエストしたユーザーに基づいて、ロールおよびアカウントの照合アクティビティによって、どのコンテンツ・アイテム使用状況データが含められるかが決まります。

次の各例に示すように、特定のユーザー（前述の準管理者ユーザー）に対して生成されるレポート結果は、プリファレンス変数が有効化されているかどうかによって異なります。

- **セキュア・モードの例 :**

  セキュリティ・チェック・プリファレンスが有効化されている場合、コンテンツ・トラッキング・レポートはセキュア・モードで実行され、ロールおよびアカウントの一致がチェックされます。この場合、準管理者ユーザーは機密データを取得および表示する資格がありません。このユーザーのロールおよびアカウント権限に関連付けられた制限により、給与コンテンツ・アイテムは常にまったく表示されません。データはレポート結果に含まれず、ユーザーはデータの存在も認識できません。

- **非セキュア・モードの例 :**

  セキュリティ・チェック・プリファレンスが無効化されている場合、コンテンツ・トラッキング・レポートは非セキュア・モードで実行され、ロールおよびアカウントの一致はチェックされません。この場合、準管理者ユーザーは、給与レポートを

アクセスまたは表示する資格がないにもかかわらず、給与コンテンツ・アイテムに関連付けられた機密情報の一部を取得できます。

少なくとも、ユーザーは給与レポートが存在することを知り、そのメタデータの一部を表示できます。このような状況における危険性は、メタデータにどのような種類の情報が含まれるかによって異なります。場合によっては、コンテンツ・アイテムが存在することを知るだけでも、重大なセキュリティ違反になることがあります。

注意 : このようなセキュリティ違反は、準管理者ユーザーにかぎらず発生します。たとえば、権限のないユーザー（つまり、通常は検索結果ページの特定のコンテンツ・アイテムの表示権限のない人）が Content Tracker Report Generator のメイン・ページにアクセスできることがあります。これは、管理ページへのアクセス、または URL の推測によって可能になります。この場合、禁止されたコンテンツ・アイテムを記述するメタデータの一部が含まれたレポートがユーザーに表示されます。

レポート問合せおよびセキュリティ・モード

contenttrackerreports_query.htm ファイルには、事前定義レポートおよびカスタム・レポートを生成する Content Tracker Report Generator のすべての問合せが含まれます。非セキュア・モードおよびセキュア・モードをサポートするため、このファイルには基本的に 2 つの問合せセットが含まれます。一方のセットでは、問合せを実行するユーザーが考慮され（セキュア・モード）、もう一方のセットでは考慮されません（非セキュア・モード）。セキュリティ・チェック・プリファレンス設定によって、使用される問合せのセットが決まります（4-24 ページの「セキュリティ・チェック・プリファレンス変数」を参照）。

この項の内容は次のとおりです。

注意 : ローカライゼーションのサポートのために、事前定義レポート名における "document" は "content item" に変更されています。ただし、これまでと同様、対応するレポート問合せには Word ドキュメントの略語（doc）が含まれます。contenttrackerreports_query.htm ファイル内のレポート問合せ名は変更されていません。

たとえば、「Top Content Items」レポートは、Content Tracker Report Generator メイン・ページにリストされる事前定義レポートの 1 つです。contenttrackerreports_query.htm ファイル内の対応するレポート問合せには、既存のネーミング規則が使用されます。

- qSctrTopDocs（非セキュア・バージョン）
- qSctrTopDocs_SEC（セキュア・バージョン）

事前定義レポートおよびセキュリティ・モード

ほとんどすべての事前定義レポート問合せでは、contenttrackerreports_query.htm ファイルにセキュア・フォームと非セキュア・フォームの両方が含まれます。一般に、問合せの検索結果がユーザー・ロールおよびアカウント権限の影響を受ける可能性がある場合、非セキュアな問合せのセキュアな変数が含められます。また、セキュリティ・チェック・プリファレンス変数が有効化されている場合、問合せのセキュア・フォームが優先され、対応する非セキュアな問合せにかわって実行されます。

レポート問合せごとにセキュリティ・チェック・プリファレンス変数を選択的に有効化または無効化することはできません。ただし、contenttrackerreports_query.htm ファイルをカスタマイズして、セキュアな問合せおよび非セキュアな問合せを管理することは可能です。実際には、特定の問合せのセキュア・フォームを削除または名前変更することで、その問合せのセキュリティ・チェック（アカウント照合）を無効化できます。このため、セキュリティ・チェック・プリファレンス変数が有効化されていても、特定の問合せのセキュア・フォームが contenttrackerreports_query.htm ファイル内に見つからなければ、レポートの生成には問合せの非セキュア・フォームが使用されます。

特定の事前定義問合せに対してセキュリティ・チェックを使用する方法の詳細は、4-31 ページの「レポート問合せのセキュリティ・チェックの有効化および無効化」を参照してください。すべてのレポート問合せに対してセキュリティ・チェックをまとめて有効化または無効化する方法の詳細は、4-30 ページの「セキュリティ・チェック・プリファレンス設定の変更」を参照してください。

カスタム・レポートおよびセキュリティ・モード

事前定義レポートの他に、特定のニーズに合せて調整した検索問合せに基づくカスタム・レポートを作成することもできます。カスタム・レポートを作成するだけでなく、カスタム・レポートにセキュリティ・チェックを選択的に実装することもできます。つまり、新しいカスタム・レポートに対してセキュリティ・チェックを実行する場合は、contenttrackerreports_query.htm ファイルに問合せの非セキュア・フォームとセキュア・フォームの両方を含めることができます。

たとえば、両方の問合せフォームを持つカスタム・レポートを追加できます。非セキュアな問合せの名前が qMyTopTwenty の場合、セキュアな問合せの名前は qMyTopTwenty_SEC になります。セキュリティ・チェック・プリファレンス変数が有効化されている場合は、セキュアな問合せ（qMyTopTwenty_SEC）を使用してレポートが生成されます。セキュリティ・チェック・プリファレンス変数が有効化されていない場合は、非セキュアな問合せ（qMyTopTwenty）を使用してレポートが生成されます。

注意 : カスタム問合せのセキュア・フォームは、contenttrackerreports_query.htm ファイル内の既存のセキュアな問合せの特定パターンに準拠している必要があります。詳細は、4-32 ページの「セキュア・レポート問合せの作成」を参照してください。

特定のカスタム問合せに対してセキュリティ・チェックを使用する方法の詳細は、4-31 ページの「レポート問合せのセキュリティ・チェックの有効化および無効化」を参照してください。すべてのレポート問合せに対してセキュリティ・チェックをまとめて有効化または無効化する方法の詳細は、4-30 ページの「セキュリティ・チェック・プリファレンス設定の変更」を参照してください。

セキュリティ・モードの確立

リクエストされたレポートを生成するために、コンテンツ・トラッキング・レポートでは、適用可能な非セキュアまたはセキュアな問合せを選択して実行する必要があります。

この項の内容は次のとおりです。

問合せタイプ選択プロセス

コンテンツ・トラッキング・レポートでは、次のプロセスに基づいてレポート問合せが選択されます。

❖ ユーザーがレポート・リクエストを発行すると、レポート問合せの名前が専用のコンテンツ・トラッキング・レポート・サービスに送信されます。

❖ コンテンツ・トラッキング・レポート・サービスによって、次のようにしてセキュリティ・チェック設定が実施されます。

- **セキュリティ・チェック・プリファレンスが無効化されている場合 :**

  コンテンツ・トラッキング・レポートは非セキュア・モードで実行され、ロールおよびアカウント照合（ユーザー・ロールおよびアカウント権限の検証）は実行されません。コンテンツ・トラッキング・レポート・サービスでは、問合せの非セキュア・バージョンが検索され、リクエストされたレポートの生成に使用されます。これは、レポート問合せのセキュア・バージョンが存在しているかどうかに関係なく行われます。

  非セキュア・モードでは、非セキュアな問合せのみがレポートの生成に使用されます。したがって、ユーザーの各ロールおよびアカウントのメンバーシップに関係なく、すべてのユーザーに同じレポート結果が表示されます。

- **セキュリティ・チェック・プリファレンスが有効化されている場合 :**

  コンテンツ・トラッキング・レポートはセキュア・モードで実行され、ロールおよびアカウント照合（ユーザー・ロールおよびアカウント権限の検証）が実行されます。

  処理の開始時 :

  コンテンツ・トラッキング・レポート・サービスによって、発行された問合せ名に接尾辞 "_SEC" が付加され、contenttrackerreports_query.htm ファイル内で、リクエストされた問合せのこの変数が検索されます。

検索中 :

- 問合せのセキュア・フォームが見つかると、リクエストされたレポートの生成にそのフォームが使用されます。

  つまり、ロールおよびアカウント照合を実施するためのセキュリティ・チェックが実行され、問合せ結果は、レポートをリクエストしたユーザーのロールおよびアカウント権限によって制限されます。したがって、ユーザーごとに異なるデータ結果を表示できます。

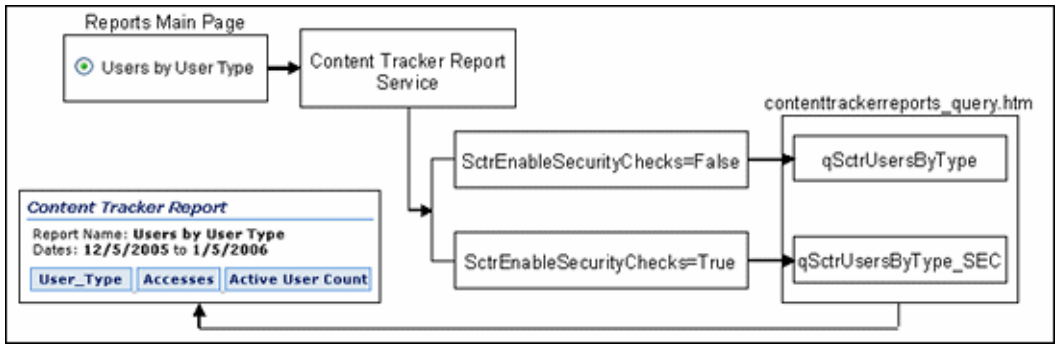
- 問合せのセキュア・フォームが見つからない場合は、非セキュアな変数が使用されます。

  この場合、事実上、セキュリティ・チェック・プリファレンスが無効化されているときと同じ結果になります。つまり、ロールおよびアカウント権限は認証されず、コンテンツ・アイテム・データはフィルタ処理されません。したがって、レポートに表示される結果はすべてのユーザーについて同じになります。適切な権限のないユーザーに機密情報が表示される可能性もあります。

例：レポート問合せ選択

ユーザーが Content Tracker Report Generator のメイン・ページ（4-10 ページ）から「Users by User Type」レポートをリクエストした場合、次の処理が行われます。

1. レポート問合せ名（qSctrUsersByType）が、コンテンツ・トラッキング・レポート・サービスに渡されます。
2. コンテンツ・トラッキング・レポート・サービスによって、セキュリティ・チェック・プリファレンス変数に基づいてリクエストが評価されます。
   a. セキュリティ・チェックが無効化されている（false に設定されている）場合、サービスによって、contenttrackerreports_query.htm ファイル内で qSctrUsersByType 問合せが検索されます。
   b. セキュリティ・チェックが有効化されている（true に設定されている）場合、サービスによって、問合せ名にセキュリティ接尾辞が追加され（qSctrUsersByType_SEC）、contenttrackerreports_query.htm ファイル内でこの変数が検索されます。
3. コンテンツ・トラッキング・レポートによって、セキュリティ・チェック・ステータスに応じて、適用可能な問合せを使用して「Users by User Type」レポートが生成されます。



セキュリティ・チェック・プリファレンス設定の変更

オプションで、手動で ScrtEnableSecurityChecks プリファレンス設定を有効化または無効化できます。

1. 管理者として Content Server にログインします。
2. 「Administration」メニューから**「Admin Server」**を選択します。

   「Content Admin Server」ページが表示されます。
3. セキュリティ・チェック・プリファレンス設定を変更する Content Server インスタンスの名前をクリックします。

   「Content Admin Server <*instance_name*>」ページが表示されます。
4. **「Component Manager」**をクリックします。

   「Component Manager」ページが表示されます。
5. 「Update Component」構成フィールドで、ドロップダウン・リストから**「ContentTrackerReports」**を選択します。
6. **「Update」**をクリックします。

   「Update Component Configuration」ページが表示されます。
7. 「ScrtEnableSecurityChecks preference」フィールドに、新しい設定（true または false）を入力します。
8. **「Update」**をクリックします。

   コンテンツ・トラッキング・レポートが新しい設定で正常に更新され、即時に有効になります。Content Server を再起動する必要はありません。

レポート問合せセキュリティのカスタマイズ

セキュア・モードでは、コンテンツ・トラッキング・レポートによって常にセキュア・フォームの問合せが優先されます。つまり、セキュア・フォームの問合せが contenttrackerreports_query.htm ファイル内に見つかると、レポートの生成には、対応する非セキュアな問合せのかわりにセキュア・フォームの問合せが使用されます。

レポート問合せごとにセキュリティ・チェック・プリファレンス変数を選択的に有効化または無効化することはできません。ただし、contenttrackerreports_query.htm ファイルをカスタマイズして、セキュアな問合せおよび非セキュアな問合せを管理することは可能です。レポート・データのセキュリティ要件に応じて、オプションでレポート問合せファイルをカスタマイズすることもできます。

レポート問合せファイルのカスタマイズでは、次の操作を行います。

- 特定のレポート問合せに対してセキュリティ・チェック（アカウント照合）を選択的に有効化または無効化します。
- 1 つ以上の非セキュア・カスタム・レポート問合せを作成し、情報のセキュリティ要件に応じて、対応するセキュア・バージョンを選択的に追加します。

この項の内容は次のとおりです。

レポート問合せのセキュリティ・チェックの有効化および無効化

セキュリティ・チェック・プリファレンス変数が有効化されていて、セキュア・バージョンの問合せが contenttrackerreports_query.htm ファイル内に存在する場合、コンテンツ・トラッキング・レポートでは、リクエストされたレポートの生成にセキュアな問合せが使用されます。ただし、レポートによってはセキュリティ・チェックを使用して生成する必要がないこともあります。その場合は適宜、任意のレポート問合せのセキュア・バージョンを選択的に無効化できます。

特定のレポート問合せに対してセキュリティ・チェック（アカウント照合）を無効化するには、次のようにします。

1. テキスト・エディタで、contenttrackerreports_query.htm ファイルを開きます。

   <*install_dir*>/custom/ContentTrackerReports/resources/contenttrackerreports_query.htm

2. 無効化する問合せのセキュア・バージョンを見つけます。

3. 問合せの名前を変更します。たとえば、qSctrUsersByType_SEC 問合せを無効化する場合は、接尾辞 "_disabled" を問合せ名に追加します。

   ```
   qSctrUsersByType_SEC_disabled
   ```

   問合せの名前を変更すると、コンテンツ・トラッキング・レポート・サービスでは contenttrackerreports_query.htm ファイル内にセキュアな問合せを見つけられなくなります。このため、かわりに非セキュア・バージョン（qSctrUsersByType）が使用されます。

注意 : セキュアな問合せを名前変更することは、一時的な無効化のソリューションです。後で、セキュア・バージョンの問合せを使用することにした場合、問合せを元の名前に戻すことで、セキュア・バージョンを簡単に再有効化できます。

あるいは、セキュア・バージョンの問合せを削除することもできます。ただし、その後考えが変わった場合は、セキュア・バージョンの問合せを改めて作成する必要があります。

4. contenttrackerreports_query.htm ファイルを保存して閉じます。
5. Content Server を再起動して、変更を適用します。

セキュア・レポート問合せの作成

ほとんどの事前定義レポート問合せでは、contenttrackerreports_query.htm ファイル内に非セキュア・バージョンとセキュア・バージョンの両方が存在します。オプションで、セキュア・バージョンが存在しない問合せに対して、セキュア・バージョンを作成できます。具体的には、すでに追加した非セキュアなカスタム問合せなどがあります。

非セキュア・レポート問合せのセキュア・バージョンを作成するには、次のようにします。

1. テキスト・エディタで、contenttrackerreports_query.htm ファイルを開きます。

   <*install_dir*>/custom/ContentTrackerReports/resources/contenttrackerreports_query.htm

2. セキュア・バージョンを作成する問合せを見つけます。一貫性を持たせるため、セキュアな問合せは対応する非セキュア・バージョンのすぐ後に追加してください。
3. セキュアな SQL レポート問合せを設計します。4-17 ページの「カスタム・レポート問合せの作成 : 例」の手順 2 を参考にしてください。
4. 既存のセキュアな問合せのパターンに従って問合せを調整します。
   a. FROM 句に Revisions 表を含めます。
   b. WHERE 句に %SCTR_SECURITY_CLAUSE% トークンを含めます。これは、コンテンツ・トラッキング・レポート・サービスによって挿入される WHERE 句のプレースホルダとなります。

c. 既存のセキュアな問合せで確立されているパターンに従って、問合せを完成します。

「非セキュア・バージョンおよびセキュア・バージョンのレポート問合せの例 (4-33 ページ)」に、一般的なレポート問合せのペアを示します。

5. contenttrackerreports_query.htm ファイルを保存して閉じます。
6. Content Server を再起動して、変更を適用します。

非セキュア・バージョンおよびセキュア・バージョンのレポート問合せの例

非セキュア・バージョン

```
<td>qSctrUsersByType</td>
<td>SELECT  u.dUserType AS wwSctrCHUser_Type,
                  COUNT(s.sc_scs_dID) AS wwSctrCHAcc,
                  COUNT(DISTINCT s.comp_username) AS wwSctrCHAct_Usr_Cnt
      FROM  SctAccessLog s, Users u
      WHERE       (s.comp_validRef IS NOT NULL) AND
                  (SctDateStamp >= ?) AND (SctDateStamp <= ?) AND
                  s.comp_username = u.dName
      GROUP BY u.dUserType
      ORDER BY wwSctrCHAcc DESC
<td>
      SctFmtFromDate date
      SctFmtToDate date
```

セキュア・バージョン

```
<td>qSctrUsersByType_SEC</td>
<td>SELECT  u.dUserType AS wwSctrCHUser_Type,
                  COUNT(s.sc_scs_dID) AS wwSctrCHAcc,
                  COUNT(DISTINCT s.comp_username) AS wwSctrCHAct_Usr_Cnt
      FROM  SctAccessLog s, Users u, Revisions
      WHERE       %SCTR_SECURITY_CLAUSE% s.sc_scs_dID = Revisions.dID AND
              (s.comp_validRef IS NOT NULL) AND
                  (SctDateStamp >= ?) AND (SctDateStamp <= ?) AND
                  s.comp_username = u.dName
      GROUP BY u.dUserType
      ORDER BY wwSctrCHAcc DESC
<td>
      SctFmtFromDate date
      SctFmtToDate date
```

外部レポート・ジェネレータ

Content Tracker で収集されたデータから基本的なテキスト・レポートや、より高度なグラフィック（棒グラフや円グラフなど）を生成するために、市販のレポート生成ツールを使用できます。この項では、格納されている Content Server データベース表にサード・パーティの製品を接続してカスタム・レポートを生成する方法に関する一般的なガイドラインを示します。

注意 : このガイドでは、カスタム・レポートの作成で使用する外部レポート作成ツールについての包括的な操作知識がユーザーにあること、またはユーザーがツールを使い慣れていることを前提としています。このため、この項では、ほとんどの市販のレポート作成製品に適用されるごく基本的なガイドラインしか示していません。

外部レポート・ジェネレータの使用

外部レポート作成ツールからカスタム・レポートを生成するには、次のようにします。

1. 外部レポート作成ツール・アプリケーションを開きます。
2. Content Server データベースへの ODBC 接続（適用可能な場合）を設定します。
3. レポートに使用するデータベース表を選択します。
4. ファイル内で共通のキー ID またはフィールドに基づいて、選択した表どうしをリンクします。選択した各表は、それらに共通している同じキー ID またはフィールドを使用してリンクすることが理想的です。
5. 各表から必要なフィールドを選択して、レポート・フォームに統合します。ほとんどの場合、フィールドは選択してフォームにドラッグ・アンド・ドロップできます。

   この手順では、カスタマイズ・レポートを設計します。外部レポート作成アプリケーションによって生成される最終的な基本テキスト・レポートでは、選択した特定のフィールドは列として表示されます。
6. 外部レポート作成アプリケーションでサポートされている場合は、オプションで、カスタム・パラメータや基準を作成できます。

   たとえば、問合せされた情報を最終レポートでハードコードにしたり、プロンプトを使用してエンド・ユーザーから直接入力を取得するようなタイプのカスタム・パラメータを作成できます。また、特定のソート基準を作成すると、最終レポートに含められる集計データを戦略的に制限および最適化できます。
7. 選択したフィールドのソート順序を指定し、最終レポート出力を形式設定します。
8. 最終レポートをプレビューします（オプション）。

9. レポートを配信メカニズムにチェックインします。

   一般に、最終レポートは、Web 表示可能ページまたは印刷可能ファイルとして形式設定して配信できます。また、外部レポート作成アプリケーションでデータ結果を使用して、棒グラフや円グラフなどの役立つグラフを作成することもできます。

   さらに、保存したファイルを Microsoft Excel や Word ファイルなどの他の製品にインポートすることもできます。

5

サービス・コール構成

概要

この項の内容は次のとおりです。

概要

タスク

サービス・コール構成ファイルについて

Content Tracker サービス・ハンドラ・フィルタを使用すると、コンテンツ・リクエスト以外の Content Server アクティビティに関する情報が収集できます。サービス・ハンドラ・フィルタによってサービス・リクエスト詳細が収集され、リアルタイムで SctAccessLog 表に格納されます。詳細は、サービス・コールに付随する DataBinder から取得されます。Content Server サービス・コールを記録するためには、サービス・コール構成ファイル（SctServiceFilter.hda）内にそのエントリが存在している必要があります。

SctServiceFilter.hda ファイルはユーザー変更可能な構成ファイルであり、記録されるサービス・コールの数を制限するために使用されます。これによって、記録されるサービスを選択的に制御できます。さらに、オプションで、SctServiceFilter.hda ファイルに含まれているサービス・コールのデータ記録機能を拡張できます。つまり、特定のサービスに関連する特定の DataBinder フィールドのデータ値を記録および追跡することもできます。5-3 ページの「拡張サービス・コール・トラッキング機能」を参照してください。

注意 : サービス・トラッキングは、サーバー・ソケット・ポートを介して呼び出される最上位レベルのサービスに制限されます。サブサービスや、内部で呼び出されるサービスを追跡することはできません。

注意 : SctServiceFilter.hda ファイルの目的は、ユーザーの具体的な関心の対象である Content Server の部分を定義することにあります。SctServiceFilter.hda ファイルにリストされていない Content Server サービスは、Content Tracker によって無視されます。また、このファイルにリストされていないサービスは、Content Tracker ロギング・サービスによってしか記録できません。5-10 ページの「Content Tracker ロギング・サービスについて」を参照してください。

注意 : SctServiceFilter.hda ファイルを変更する方法は、2 通りあります。ファイルへの新規サービスの追加、およびファイル内の既存サービス・コール・パラメータの編集は、データ・エンジン・コントロール・センターから実行できます（3-16 ページの「「Services」タブ」を参照）。あるいは、手動で SctServiceFilter.hda ファイルを編集することもできます（5-9 ページの「SctServiceFilter.hda ファイルの手動編集」を参照）。

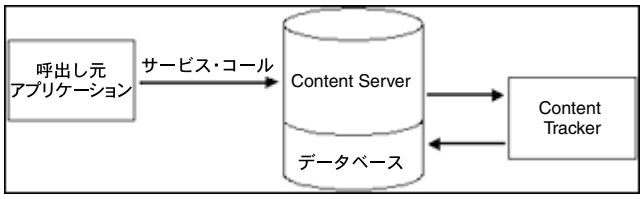
技術ヒント : 記録するサービスを制御するには、SctServiceFilter.hda ファイルにそれらのサービスを追加するか、ファイルから除外します。特定のサービスまたはすべてのサービスに対するロギングを制御する場合、この方法が効率的です。また、拡張サービス・コール・トラッキング機能を使用すると、特定のサービスに対して記録されるデータのタイプをカスタマイズできます。

一般的なサービス・コール・ロギング

Content Tracker サービス・ハンドラ・フィルタによって、SctServiceFilter.hda ファイルにリストされたサービスが検出され、選択されたデータ・フィールドの値が取得されます。その後 Content Tracker によって、指定されたサービス・コールが記録されます。タイムスタンプなどとともに、情報が動的に SctAccessLog 表に書き込まれます。

Content Tracker によって、有効化されているサービスごとに、特定の標準 DataBinder フィールド（dUser、dDocName など）が自動的に記録されます。また、拡張サービス・コール・トラッキング機能に関連付けられた DataBinder フィールドが、SctAccessLog 表の汎用列に記録されます。

データは、Content Tracker 固有のサービス順序番号およびサービスのタイプ指定 "S" を使用して、リアルタイムで SctAccessLog 表に挿入されます。("W" 指定は、静的 URL イベント・タイプを示します。）手動リダクションまたはスケジュール・リダクション（あるいはその両方）が必要になるのは、Web サーバー・フィルタ・プラグインによって収集された静的 URL アクセス情報を処理する場合のみです。2-5 ページの「Web サーバー・フィルタ・プラグイン」を参照してください。



拡張サービス・コール・トラッキング機能

拡張サービス・コール・トラッキング機能を使用すると、Content Server サービス・コールを記録できます。またオプションで、構成されている各サービス・コールによって記録される標準の DataBinder フィールド以外の 1 つ以上の追加 DataBinder フィールドから関連データ値を記録することにより、この情報を補完することもできます。この機能をサポートするには、次のものを使用します。

- ❖ サービス・コール ResultSet の組合せ（5-3 ページ）
- ❖ 出力表の汎用列（5-4 ページ）

サービス・コール ResultSet の組合せ

SctServiceFilter.hda ファイルに含まれる ServiceExtraInfo ResultSet 内に、Content Tracker によって記録される各サービスのエントリが存在している必要があります。これらのエントリによって、各種の標準の DataBinder フィールド（dUser や dDocName など）が自動的に記録されます。ただし、補完的な DataBinder フィールドから関連データ

値を記録および追跡することで、Content Tracker によって記録されるサービス関連データを拡張できます。

拡張サービス・コール・トラッキング機能を実装するには、ServicesExtraInfo ResultSet 内のエントリをフィールド・マップ ResultSet にリンクします。各フィールド・マップ ResultSet には、データ・フィールド名、ソース・ロケーション、および SctAccessLog 表内の宛先表列名の 1 つ以上のセットが含まれます。このような分類によって、関連付けられたサービス・コールに関連するデータ・フィールドを選択し、SctAccessLog 表の指定された列にデータ値を記録することができます。

注意 : 拡張トラッキング機能を使用する場合は複数の拡張サービスを記録できるため、どのサービスが記録されているかがわからないと、SctAccessLog 表の汎用列の内容を適切に解釈できません。サービス名は常に、sc_scs_idcService（2-10 ページ）列に記録されます。問合せは、必要なサービス名を持つこの列と一致させてください。

警告 : フィールド・マップ ResultSet 内では、データ・フィールドを既存の標準の SctAccessLog 表列に自由にマップできます。標準のフィールド・データ値が収集されると、拡張サービス・マッピングが実行されます。したがって、標準の表列フィールドをオーバーライドできます。

たとえば、記録するサービスのデータ・フィールドに特定のユーザー名（たとえば、MyUserName=john など）が含まれるとします。拡張トラッキング機能を使用して、sc_scs_dUser 列の内容をオーバーライドできます。この場合は、MyUserName と sc_scs_dUser を、データ・フィールド、ロケーション、およびフィールド・マップ ResultSet 内の表列セットとして結合するのみです。

したがって、この場合も、記録されるデータが SctAccessLog 列タイプと適合しているかどうかは自分で確認する必要があります。

注意 : リンクされたサービス・エントリおよび ResultSet の例は、5-8 ページの「リンクされたサービス・エントリおよびフィールド・マップ ResultSet」を参照してください。SctAccessLog 表の内容、およびデータ・フィールドへのマップ用の汎用列の詳細は、2-8 ページの「結合された出力表」を参照してください。サービス・コール・ユーザー・インタフェースの詳細は、3-16 ページの「「Services」タブ」を参照してください。

出力表の汎用列

拡張サービス・トラッキング用のフィールド・マップ ResultSet 内で、DataBinder フィールドを SctAccessLog 表の列にマップする必要があります。汎用列（extField_1 ～ extField_10）は、マッピングに使用可能です。これらの列には、特定のサービスに対するロギングおよびトラッキングに適した任意のデータ値を挿入できます。標準の表列が上書きされることを回避するため、これらの列を使用することが推奨および期待されます。

技術ヒント : サービスの名前は常に、sc_scs_idcService 列に記録されます。このため、問合せで拡張されたフィールドのコンテンツを使用する場合は、修飾子としてサービス名を含める必要があります。SctAccessLog 表の列が関連する特定の SQL 問合せが含まれたカスタム・レポートの詳細は、4-17 ページの「カスタム・レポート問合せの作成 : 例」を参照してください。

サービス・コール構成ファイルの内容

サービス・コール構成ファイル（SctServiceFilter.hda）は、最初に、共通して使用される Content Server に固有のコンテンツ・アクセス、検索およびユーザー認証サービスで構成されます。このファイルには、記録されるサービスごとに 1 つずつエントリが存在する ResultSet 構造が含まれます。オプションで、拡張サービス・コール・トラッキング機能をサポートするために、ServiceExtraInfo ResultSet 内のサービス・エントリにリンクされたフィールド・マップ ResultSet をこのファイルに含めることもできます。

SctServiceFilter.hda ファイルに新規のエントリを追加したり、既存のエントリを編集するには、データ・エンジン・コントロール・センターからアクセスする「Services」ユーザー・インタフェースを使用できます。あるいは、オプションでファイル内のエントリを手動で変更することもできます。3-16 ページの「「Services」タブ」または 5-9 ページの「SctServiceFilter.hda ファイルの手動編集」を参照してください。

注意 : Content Tracker によって SctAccessLog 表に記録される最初のサービスのセットを確認するには、次のディレクトリ内の SctServiceFilter.hda ファイルにアクセスします。

<*install_dir*>/custom/ContentTracker/resources/SctServiceFilter.hda

これらのサービス、またはサービス・コール構成ファイルに追加するその他のサービスの詳細は、『Content Server Services Reference Guide』を参照してください。

次の表に、サービス・コール構成ファイルの結果セット・スキーマの詳細を示します。値は、SctAccessLog 表内の対応する列に直接コピーされます。

機能	説明
ServiceExtraInfo ResultSet の内容 :	
Service Name（sctServiceName）	記録されるサービスの名前。たとえば、GET_FILE などです。指定されたサービスについて ResultSet 内に行が存在しない場合、そのサービスは記録されません。
Calling Product（sctCallingProduct）	任意の文字列。標準の Content Server エントリではすべて、このフィールドは通常 "Core Server" に設定されます。

機能	説明
Event Type（sctEventType）	任意の文字列。標準の Content Server エントリではすべて、このフィールドは通常 "Content Access" に設定されます。
Reference（sctReference）	SctAccessLog 表の sc_scs_reference フィールドを設定するために使用します。空白にした場合、内部の getReference ロジックが使用されます。
Field Map（sctFieldMap）	SctServiceFilter.hda ファイルに追加されるフィールド・マップ ResultSet の名前。このフィールドは、拡張サービス・コール・トラッキング機能を使用する場合にのみ必須です。この機能を使用すると、DataBinder フィールド情報を SctAccessLog 表の 1 つ以上の汎用列に記録できます。
フィールド・マップ ResultSet の内容 :	
「Field Map」リンク	フィールド・マップ ResultSet の名前。  **注意 :** フィールド・マップを作成する場合、サービス DataBinder オブジェクトを書き出す構成変数を設定すると役立ちます。これによって、イベントの記録時に使用可能なデータが確認できます。詳細は、B-3 ページの「SctDebugServiceBinderDumpEnabled」を参照してください。
「DataBinder」フィールド（dataFieldName）	SctAccessLog 表の汎用列にデータ値が記録される DataBinder フィールドの名前。3-21 ページの「「Field Name」フィールド」も参照してください。
Data Location（dataLocation）	フィールドが記録される Content Server サービス DataBinder 内のセクション。3-22 ページの「「Field Location」フィールド」も参照してください。
「Access Log」列（accessLogColumnName）	指定された DataBinder フィールドからデータ値が記録される SctAccessLog 表内の特定の汎用列。3-22 ページの「「Column Name」フィールド」も参照してください。

注意 : DataBinder からコピーされて SctAccessLog 表に挿入されるフィールドには、dID、dDocName、IdcService、dUser、SctCallingProduct、SctEventType および SctReference があります。最後の 3 つのフィールドの値が SctServiceFilter.hda ファイル内のサービス・エントリに含まれている場合、それらの値がデータ・フィールド内の対応する値をオーバーライドします。

技術ヒント : 必要なサービス・コールを SctServiceFilter.hda ファイルに追加し、この方法を使用して特定のアクティビティを記録する場合、CallingProduct、EventType および Reference フィールドの値を指定できるメリットがあります。割り当てた値は、SctAccessLog 表内の対応する列に直接コピーされます。

注意 : サービス・ハンドラ・フィルタを介して記録されるサービスと、Content Tracker ロギング・サービスを介して記録されるサービスとの間に、重複や競合はないはずです。サービスの名前が Content Tracker サービス・ハンドラ・フィルタ・ファイルに指定されていれば、このようなサービスは自動的に記録されるため、Content Tracker ロギング・サービスによりこの処理が行われる必要はありません。

ResultSet の例

デフォルトの SctServiceFilter.hda ファイルには、各種の共通のサービス・コールが含まれます。これらのコールは、次のように分類されます。

- ServiceExtraInfo ResultSet のエントリ（5-7 ページ）
- リンクされたサービス・エントリおよびフィールド・マップ ResultSet（5-8 ページ）

注意 : Content Tracker によって SctAccessLog 表に記録される最初のサービス・セットと、サービス・エントリおよびフィールド・マップ ResultSet を確認するには、次のディレクトリ内の SctServiceFilter.hda ファイルにアクセスします。

<*install_dir*>/custom/ContentTracker/resources/SctServiceFilter.hda

これらのサービス、またはサービス・コール構成ファイルに追加するその他のサービスの詳細は、『Content Server Services Reference Guide』を参照してください。

ServiceExtraInfo ResultSet のエントリ

次のリストに、SctServiceFilter.hda ファイルの ServiceExtraInfo ResultSet に含まれる複数のサービス・エントリの例を示します。

- `GET_FILE_BY_NAME`
  `Core Server`
  `Content Access`

- GET_DYNAMIC_URL
  Core Server
  Content Access
- GET_DYNAMIC_CONVERSION
  Core Server
  Content Access
- GET_EXTERNAL_DYNAMIC_CONVERSION
  Core Server
  Content Access
- GET_ARCHIVED_FILE
  Core Server
  Content Access
- COLLECTION_GET_FILE
  Folders
  Content Access

リンクされたサービス・エントリおよびフィールド・マップ ResultSet

次の表に、フィールド・マップ ResultSet にリンクされたサービス・エントリの例をリストします。これらの例またはその他の類似の例は、最初の SctServiceFilter.hda ファイルに含まれています。

サービス・エントリ	フィールド・マップ ResultSet
GET_SEARCH_RESULTS Core Server Search SearchFieldMap	@ResultSet SearchFieldMap 3 dataFieldName 6 255 dataLocation 6 255 accessLogColumnName 6 255 MiniSearchText LocalData extField_1 TranslatedQueryText LocalData extField_2 • • • IsSavedQuery LocalData extField_7 @end
PNE_GET_SEARCH_RESULTS Core Server Search SearchFieldMap	

サービス・エントリ	フィールド・マップ ResultSet
GET_FILE Core Server Content Access GetFileFieldMap	@ResultSet GetFileFieldMap 3 dataFieldName 6 255 dataLocation 6 255 accessLogColumnName 6 255 RevisionSelectionMethod LocalData extField_1 Rendition LocalData extField_2 @end

SctServiceFilter.hda ファイルの手動編集

SctServiceFilter.hda ファイルのエントリを追加または変更するには、次のようにします。

1. テキスト・エディタで、SctServiceFilter.hda ファイルを開きます。

   <*install_dir*>/custom/ContentTracker/resources/SctServiceFilter.hda

2. 既存のエントリを編集するか、新規のサービス・エントリを追加します。たとえば、GET_FILE_FORM サービスを追加する場合は、次のサービス・エントリをファイル内の ServiceExtraInfo ResultSet に入力します。

   ```
   GET_FORM_FILE
   Threaded Discussion
   Content Access
   <optional_reference_value>
   <optional_field_map_link_value>
   ```

   詳細は次のとおりです。

   optional_field_map_link_value は、拡張サービス・コール・トラッキング機能を実装する場合に使用します。この場合、対応するフィールド・マップ ResultSet も追加または編集する必要があります。別の方法で拡張サービス・トラッキングを実装する場合は、手順 3 をスキップします。

3. 拡張サービス・トラッキングを使用する場合、対応するフィールド・マップ ResultSet も追加または編集する必要があります。たとえば、SS_GET_PAGE サービスを追加し、追加のデータ・フィールド値を追跡するには、次のサービス・エントリおよび対応するフィールド・マップ ResultSet をファイルに入力します。

サービス・エントリ	フィールド・マップ ResultSet
SS_GET_PAGE Site Studio Web Hierarchy Access web SSGetPageFieldMap	@ResultSet SSGetPageFieldMap 3 dataFieldName 6 255 dataLocation 6 255 accessLogColumnName 6 255 <*DataBinder_field_name*> <*data_field_location_name*> <*access_log_column_name*> @end
注意 : DataBinder フィールド、ロケーションおよび表列名のセットは、必要なだけ含めてください。	

4. ファイルを保存して閉じます。
5. Content Server を再起動して、新しい定義を適用します。

注意 : 検索リクエスト・イベントはリアルタイムで SctAccessLog 表に記録されます。縮小する必要はありません。

注意 : オプションで、データ・エンジン・コントロール・センターに組み込まれているユーザー・インタフェースを使用して、サービスを追加または編集できます。詳細は、3-2 ページの「データ・エンジン・コントロール・センター」および 3-16 ページの「「Services」タブ」を参照してください。

CONTENT TRACKER ロギング・サービスについて

Content Tracker ロギング・サービスは単一サービス・コール（SCT_LOG_EVENT）であり、アプリケーションにより単一のイベントが SctAccessLog 表に記録されることを可能にします。このサービスは、URL を介して直接、またはサービス・スクリプト内のアクションとして呼び出すことができます。また、executeService() 関数を使用して、IdocScript から呼び出すこともできます。呼出し元アプリケーションによって、記録されるサービス DataBinder 内のフィールドが設定されます。これには、Content Tracker SctServiceFilter.hda 構成ファイルにリストされている記述フィールドが含まれます。

SCT_LOG_EVENT サービスによって、サービス DataBinder から情報がコピーされます。このデータは、Content Tracker 固有のサービス順序番号およびサービスのタイプ指定 "S" を使用して、リアルタイムで SctAccessLog 表に挿入されます。手動リダクションまたはスケジュール・リダクション（あるいはその両方）が必要になるのは、Web サーバー・フィルタ・プラグインによって収集された静的 URL アクセス情報を処理する場合のみです。2-5 ページの「Web サーバー・フィルタ・プラグイン」を参照してください。

注意 : サービス・ハンドラ・フィルタを介して記録されるサービスと、Content Tracker ロギング・サービスを介して記録されるサービスとの間に、重複や競合はないはずです。サービスの名前が Content Tracker サービス・ハンドラ・フィルタ・ファイルに指定されていれば、このようなサービスは自動的に記録されるため、Content Tracker ロギング・サービスによりこの処理が行われる必要はありません。しかし、Content Tracker ではこのような重複の回避処理は試行されません。

Content Tracker ロギング・サービスを呼び出すための必要な DataBinder フィールドの設定

次の表に、Content Tracker ロギング・サービス（SCT_LOG_EVENT）が呼び出されたときに Content Tracker によって検索される SctAccessLog 列名および対応する DataBinder フィールドを示します。アプリケーションは Content Tracker ロギング・サービスを呼び出すときに、Content Tracker で検索されるサービス DataBinder 内の必要なフィールドを設定します。SctAccessLog フィールドの詳細は、2-8 ページの「結合された出力表」を参照してください。

SctAccessLog 列名	サービス DataBinder LocalData フィールド
SctDateStamp	[計算される]
SctSequence	SctSequence
SctEntryType	"S"
eventDate	[計算される]
SctParentSequence	SctParentSequence
c_ip	REMOTE_HOST
cs_username	HTTP_INTERNETUSER
cs_method	REQUEST_METHOD
cs_uriStem	HTTP_CGIPATHROOT
cs_uriQuery	QUERY_STRING
cs_host	SERVER_NAME
cs_userAgent	HTTP_USER_AGENT
cs_cookie	HTTP_COOKIE

SctAccessLog 列名	サービス DataBinder LocalData フィールド
cs_referer	HTTP_REFERER
sc_scs_dID	dID
sc_scs_dUser	dUser
sc_scs_idcService	IdcService（または SctIdcService）
sc_scs_dDocName	dDocName
sc_scs_callingProduct	sctCallingProduct
sc_scs_eventType	sctEventType
sc_scs_status	StatusCode
sc_scs_reference	sctReference（... も同様）
comp_username	[計算される - HTTP_INTERNETUSER または ...]
sc_scs_isPrompt	該当なし
sc_scs_isAccessDenied	該当なし
sc_scs_inetUser	該当なし
sc_scs_authUser	該当なし
sc_scs_inetPassword	該当なし
sc_scs_serviceMsg	StatusMessage

アプリケーションからの Content Tracker ロギング・サービスの呼出し

SCT_LOG_EVENT サービスをアプリケーションから呼び出すことができます。これを行うことができるのは、アプリケーション開発者か、アプリケーション・サービス・スクリプトを変更しようとするユーザーです。アプリケーションは Java から SCT_LOG_EVENT を呼び出すことができます。あるいは、アプリケーションでサービス・スクリプトに SCT_LOG_EVENT へのコールを含めることもできます。

IdocScript からの Content Tracker ロギング・サービスの呼出し

executeService( ) 関数を使用して、IdocScript から間接的に SCT_LOG_EVENT サービスを呼び出すことができます。これは、アプリケーションから SCT_LOG_EVENT サービスを呼び出すことと同じですが、アプリケーション Java コードではなく IdocScript から行われます。Content Tracker では、SCT_LOG_EVENT サービスの呼出し元が Java か IdocScript かは区別できません。

A

CONTENT TRACKER の構成およびカスタマイズ

概要

この項の内容は次のとおりです。

概要

タスク

構成変数

次の表に、現行バージョンの Content Tracker で使用される構成設定のデフォルト値を示します。これらの構成変数は、Content Tracker 構成ファイルに含まれています。

<*install_dir*>/custom/ContentTracker/resources/sct.cfg

構成設定	デフォルト値	備考
SctAutoTruncateDataStrings	FALSE	使用 : JAVA リダクション・プロセスでデータ文字列を対応する表列に収まるように切り捨てるかどうかを指定します。
SctComponentDir	<*install_dir*>/custom/ContentTracker/	使用 : JAVA Content Tracker がインストールされているディレクトリのパス。
SctDebugLogEnabled	FALSE	使用 : JAVA TRUE を設定すると、Java コード実行トレースが有効化されます。SctDebugLogFilePath とともに使用されます。トラブルシューティングでのこの変数の使用方法の詳細は、B-3 ページの「SctDebugLogEnabled」を参照してください。
SctDebugLogFilePath	<*install_dir*>/custom/ContentTracker/log/SCT_DEBUG_TRACE.log	使用 : JAVA Java コード実行トレースのディレクトリ。SctDebugLogEnabled とともに使用されます。トラブルシューティングでのこの変数の使用方法の詳細は、B-3 ページの「SctDebugLogFilePath」を参照してください。
SctDebugServiceBinderDumpEnabled	FALSE	使用 : JAVA TRUE を設定すると、サービス・ロギング中にサービス DataBinder オブジェクトの診断出力が有効化されます。トラブルシューティングでのこの変数の使用方法の詳細は、B-3 ページの「SctDebugServiceBinderDumpEnabled」を参照してください。
SctExternalUserLogEnabled	TRUE	使用 : JAVA TRUE を設定すると、外部ユーザー・アカウントおよびロールの情報の UserSecurityAttributes 表へのレプリケーションが有効化されます。

構成設定	デフォルト値	備考
SctFilterPluginLogDir	<*install_dir*>/custom/ContentTracker/data/	使用 : フィルタ・プラグイン フィルタ・プラグインによってイベント・ログが格納されるディレクトリのパス。
SctIdcAuthExtraConfigParams	SctFilterPluginLogDir, SctLogEnabled, SctIgnoreFileTypes, SctLogSecurity, SctUseLock, SctLockPort	フィルタ・プラグインに渡され、Content Tracker 起動フィルタによって idcAuthExtraConfigParams にプログラムでマージされる Content Tracker 構成パラメータのリスト。
SctIgnoreDirectories	/stellent/resources/; /stellent/common/	使用 : フィルタ・プラグイン リストされたディレクトリ・ルート内に含まれる URL を無視するようにフィルタ・プラグインに指示します。
SctIgnoreFileTypes	gif、jpg、js、css	使用 : フィルタ・プラグイン リストされたファイルタイプを持つ URL を無視するようにフィルタ・プラグインに指示します。
SctLockPort	4477	使用 : フィルタ・プラグイン フィルタ・プラグインで Content Server Lock Provider への接続に使用されるネットワーク・ポート。
SctLogDir	<*install_dir*>/custom/ContentTracker/data/	使用 : JAVA Content Tracker が RAW イベント・ログ（sctLog など）を検索するディレクトリのパス。複数の値にすることもできます（たとえば、dir1;dir2;...;dir*n* など）。
SctLogEnabled	TRUE	使用 : フィルタ・プラグイン、JAVA False の場合、すべてのイベントを無視して何もログを作成しないようにサービス・ハンドラ・フィルタおよび Web サーバー・フィルタ・プラグインに指示します。これは、Content Tracker Master のオン / オフのスイッチです。
SctLogSecurity	TRUE	使用 : フィルタ・プラグイン、JAVA TRUE の場合、IMMEDIATE_RESPONSE_PAGE イベントを sctSecurityLog イベント・ログに記録するようにフィルタ・プラグインに指示し、イベント・ログを読み取るようにリダクション・プロセスに指示します。

構成設定	デフォルト値	備考
SctMaxRecentCount	5	使用 : JAVA 縮小済のデータが「Recent」状態として保持される最大日数。「Recent」からオーバーフローしたデータは「Archive」状態に移行します。
SctMaxRereadTime	3600	使用 : JAVA 特定のユーザーが特定のコンテンツ・アイテム（たとえば、PDF ファイルなど）を連続して参照したとき、連続する参照が 1 つの持続するアクセスとしてみなされる最大の秒間隔。次の参照との時間間隔が大きい場合は、別個のアクセスとしてカウントされます。
SctPostReduction Exec	[なし]	使用 : JAVA リダクション後実行可能ファイルのパス（<cs_root>/custom/ContentTracker/bin/ 内と想定）。
SctProxyNameMax Length	50	使用 : JAVA 構成内の Content Server プロキシ・サーバー名の最大文字数。Content Tracker 表作成におけるユーザー名フィールドのサイズを拡大する場合に使用されます。
SctReductionAvail ableDatesLookback	0	使用 : JAVA 「Available Dates」範囲を制限するために SctReductionRequireEventLogs とともに使用されます。単位は日数です。0 を指定すると、範囲は制限されません。
SctReductionLogDir	<*install_dir*>/custo m/ContentTracker/ log/	使用 : JAVA Content Tracker リダクション・ログが格納されるディレクトリのパス。
SctReductionRequire EventLogs	TRUE	使用 : JAVA 連結解除された構成で使用されます。FALSE は、イベント・ログが見つからなくてもリダクションを続行することを示します。
SctScheduledReduct ionEnable	TRUE	使用 : JAVA 複数 JVM 構成において、リダクションを実行する Content Server インスタンスを選択するために使用されます。

構成設定	デフォルト値	備考
SctSnapshotEnable	FALSE	使用 : JAVA TRUE を設定すると、スナップショット機能が有効化されます。データ・エンジン・コントロール・センターから設定します。
SctSnapshotLast AccessEnable	FALSE	使用 : JAVA TRUE を設定すると、「Last Access Date」スナップショット機能が有効化されます。データ・エンジン・コントロール・センターから設定します。
SctSnapshotLast AccessField	[なし]	使用 : JAVA 「Last Access Date」のメタデータ・フィールド名（たとえば、xLastAccessDate など）。データ・エンジン・コントロール・センターから設定します。
SctSnapshotLong CountEnable	FALSE	使用 : JAVA TRUE を設定すると、長期間のアクセス・カウントのスナップショット機能が有効化されます。データ・エンジン・コントロール・センターから設定します。
SctSnapshotLong CountField	[なし]	使用 : JAVA 「Long Interval Count」のメタデータ・フィールド名（たとえば、xAccessesInLast90Days など）。データ・エンジン・コントロール・センターから設定します。
SctSnapshotLong CountInterval	[なし]	使用 : JAVA 長期間の日数。データ・エンジン・コントロール・センターから設定します。
SctSnapshotShort CountEnable	FALSE	使用 : JAVA TRUE に設定すると、短期間のアクセス・カウントのスナップショット機能が有効化されます。データ・エンジン・コントロール・センターから設定します。
SctSnapshotShort CountField	[なし]	使用 : JAVA 「Short Interval Count」のメタデータ・フィールド名（たとえば、xAccessesInLast10Days など）。データ・エンジン・コントロール・センターから設定します。

構成設定	デフォルト値	備考
SctSnapshotShort CountInterval	[なし]	使用 : JAVA 短期間の日数。データ・エンジン・コントロール・センターから設定します。
SctTrackerInfoFile	*<install_dir>*/custom/ContentTracker/bin/trackerinfo.txt	使用 : JAVA Content Tracker Scheduler パラメータを保持するために使用される特殊な構成ファイルのパス。
SctUrlMaxLength	3000	使用 : JAVA URL フィールドの予測される最大長（文字数）。表の作成時の列幅を決定するために使用されます。特定の表にこのような列が複数存在することがあります。
SctUseGMT	FALSE	使用 : フィルタ・プラグイン、JAVA 記録されたイベント時間を Universal Coordinated Time に変換する場合は、TRUE を設定します。FALSE を設定すると、ローカル時間が使用されます。
SctUseLock	TRUE	使用 : フィルタ・プラグイン TRUE の場合、RAW ログ・ファイル（sctLog-yyyymmdd.txt など）に書き込む前に Content Server Lock Provider からロックを取得するようにフィルタ・プラグインに指示します。そうでない場合、ロックは適用されず、順序番号が内部的に割り当てられます。

CONTENT TRACKER 構成変数の手動設定

Content Tracker 構成変数を設定または編集するには、次のようにします。

1. テキスト・エディタで、sct.cfg ファイルを開きます。

   <*install_dir*>/custom/ContentTracker/resources/sct.cfg

2. 編集する構成ファイルを見つけます。
3. 適用可能な値を入力します。
4. sct.cfg ファイルを保存して閉じます。
5. Content Server を再起動して、変更を適用します。

注意 : オプションで、データ・エンジン・コントロール・センターに組み込まれているユーザー・インタフェースを使用して、アクティビティ・メトリック・メタデータ・フィールドの構成変数を追加または編集できます。次のような変数があります。

- SctSnapshotEnable（A-5 ページ）
- SctSnapshotLast AccessEnable（A-5 ページ）
- SctSnapshotLast AccessField（A-5 ページ）
- SctSnapshotLong CountEnable（A-5 ページ）
- SctSnapshotLong CountField（A-5 ページ）
- SctSnapshotLong CountInterval（A-5 ページ）
- SctSnapshotShort CountEnable（A-5 ページ）
- SctSnapshotShort CountField（A-5 ページ）
- SctSnapshotShort CountInterval（A-6 ページ）

ユーザー・インタフェースおよびアクティビティ・メトリック機能の詳細は、3-2 ページの「データ・エンジン・コントロール・センター」および 3-11 ページの「「Snapshot」タブ」を参照してください。

アクティビティ・メトリックの SQL 問合せ

スナップショット機能を使用すると、検索関連カスタム・メタデータ・フィールドを記録して追跡できます。Content Tracker によって、これらのフィールドに、特定のコンテンツ・アイテムの人気度を反映するコンテンツ・アイテム使用状況およびアクセス情報が挿入されます。この情報には、2 つの異なる期間における最新アクセスの日付およびアクセス数が含まれます。スナップショット機能の詳細は、3-11 ページの「「Snapshot」タブ」を参照してください。

スナップショット機能およびアクティビティ・メトリックが有効化されている場合、リダクション処理フェーズに続いて、カスタム・メタデータ・フィールドの値が更新されます。ユーザーがコンテンツ・アイテムにアクセスすると、適用可能な検索関連メタデータ・フィールドの値がそれに応じて変わります。その後、Content Tracker により、リダクション後の処理手順として 3 つの SQL 問合せが実行され、レポート作成期間中にアクセスされたコンテンツ・アイテムが特定されます。リダクションの後処理手順の詳細は、2-3 ページの「アクティビティ・メトリックを使用するデータ・リダクション・プロセス」を参照してください。

この項の内容は次のとおりです。

アクティビティ・メトリックの SQL 問合せのカスタマイズ

SQL 問合せはリソースとして使用可能であり、特定のニーズに合せてカスタマイズできます。最終トラッキング・データから、特定の情報をフィルタで除外できます。たとえば、表形式の結果から、特定のユーザーによるアクセスを除外することができます。これらの SQL 問合せは、sctQuery.htm ファイルに含まれています。

<*install_dir*>/custom/ContentTracker/resources/SctQuery.htm

注意 : 一般に、SQL 問合せ内の WHERE 句は自由に変更できます。ただし、その他のものは変更しないでおくことをお薦めします。

検索関連カスタム・メタデータ・フィールドには、次の SQL 問合せが使用されます。

qSctLastAccessDate

「last access」機能の場合、qSctLastAccessDate SQL 問合せによって SctAccessLog 表が使用されます。この問合せによって、リダクション日付におけるすべてのコンテンツ・アイテム・アクセスがチェックされ、dID ごとに最新のタイムスタンプが収集されます。問合せのパラメータは、リダクション日付です。この場合、日付はランダムな順序で縮小できます。これは、最終アクセス日付の比較テストによって変更が示されるのは、既存の DocMeta 値が提示された新しい値よりも古い場合のみであるためです。

「Snapshot」タブの「last access」フィールドの詳細は、3-13 ページの「「Enable Last Access updates」チェック・ボックスおよび対応する「Field」メタデータ・フィールド」を参照してください。

qSctAccessCountShort および qSctAccessCountLong

「short access count」および「long access count」機能の場合、SQL 問合せの qSctAccessCountShort および qSctAccessCountLong は、カウントの列名以外は同じです。これらの問合せでは、SctAccessLog 表を使用して、それぞれに指定された期間（日数）にわたる各 dID のすべてのアクセスについて合計が計算されます。パラメータは、適用可能なロールアップの開始日および終了日です。

「Snapshot」タブの「short access count」および「long access count」フィールドの詳細は、3-15 ページの「「Enable Short Access Count updates」/「Enable Long Access Count updates」チェック・ボックスおよび対応する「Fields」/「Intervals」」を参照してください。

「Autoload」オプションの SQL 問合せのカスタマイズ

データ・エンジン・コントロール・センターの「Snapshot」タブで「Autoload」オプションを使用すると、すべての既存コンテンツの「Last Access」フィールドに再度値を移入できます。「Autoload」を起動すると、qSctLastAccessDateAutoload 問合せが実行され、Content Server の DocMeta データベース表の空（NULL）の「Last Access」フィールドに現在の日時が移入されます。

ただし、qSctLastAccessDateAutoload 問合せはリソースとして使用可能であり、特定のニーズに合せてカスタマイズできます。たとえば、「Last Access」フィールドを「dCreateDate」、「dReleaseDate」、またはアプリケーションの要件を満たすその他の時刻に設定できます。qSctLastAccessDateAutoload 問合せは、sctQuery.htm ファイルに含まれています。

<*install_dir*>/custom/ContentTracker/resources/SctQuery.htm

「Snapshot」タブの「last access」フィールドおよび「Autoload」オプションの詳細は、3-13 ページの「「Enable Last Access updates」チェック・ボックスおよび対応する

「Field」メタデータ・フィールド」および 3-14 ページの「「Autoload」チェック・ボックス」を参照してください。

外部ユーザーおよびコンテンツ・アイテム・トラッキング

Content Tracker で適用可能レポートに外部ユーザー・アクセスに関するデータを含めるかどうかを制御するオプションがあります。これらの認証済ユーザーは、ユーザー・ロールおよびアカウントに基づいて権限を与えられています。デフォルトでは、構成パラメータ SctExternalUserLog Enabled（A-2 ページ）は TRUE（有効）に設定されています。このため、Content Tracker では、外部ユーザー・ログオンが監視され、そのロールおよびアカウント情報が UserSecurityAttributes 表に自動的に伝播されます。

SctExternalUserLogEnabled 構成変数が有効化されているか無効化されているかにかかわらず、外部ユーザーのコンテンツ・アイテム情報はすべて追跡されて記録されます。しかし、この構成変数が有効化されている場合は、外部で認証されたユーザー名とそれに関連付けられたユーザー・ロールおよびアカウントとの相関関係を明示的に示すレポートに、このデータが含められます。具体的には、「Top Content Items by User Role（4-12 ページ）」レポートおよび「Users by User Role（4-13 ページ）」レポートに、外部ユーザーによるすべてのコンテンツ・アイテム・アクティビティが含められます。

注意 : オプションで、手動で SctExternalUserLogEnabled 構成変数を無効化できます。ただし、無効化するように選択した場合、外部で認証されたユーザーによるコンテンツ・アイテム・アクセスは、より一般的なレポート（「Top Content Items」レポートなど）に含められます。このデータは、ユーザー・ロールによって限定されたドキュメント・アクセス・カウントおよびアカウント情報を使用するレポートからは除外されます。

SctExternalUserLogEnabled 構成変数を手動で無効化するには、A-7 ページの「Content Tracker 構成変数の手動設定」を参照してください。

B

トラブルシューティング

概要

この項の内容は次のとおりです。

概要

タスク

CONTENT TRACKER のトラブルシューティングについて

Content Tracker 10*g* リリース 3 には、Web サーバー・フィルタ・プラグインと Java コードという 2 つの実行トレース・メカニズムが備わっています。これらは、顧客のインストールにおける問題を診断することを目的としたものであり、本番環境では使用されません。

Web サーバー・フィルタ・プラグインのデバッグ・サポート

Web サーバー・フィルタ・プラグインでは、PLUGIN_DEBUG が重要です。Content Server の「Filter Administration」ページでこれを設定すると、Content Tracker Web サーバー・フィルタ・プラグインによって実行トレース情報が発行されます。トレースは、ソースにアクセスできる人にとってのみ意味があります。問題が発生した場合は、PLUGIN_DEBUG を有効し、テスト・シナリオを実行し、評価用にログ・セグメントをカスタマ・サービスに送信することになっています。それ以外の場合は、PLUGIN_DEBUG をオフのままにしておいてください。

デバッグ・プラグインの設定

PLUGIN_DEBUG を設定するには、次のようにします。

1. Content Server で、「Administration」トレーの**「Admin Applets」**リンクをクリックします。

   「Administration」ページが表示されます。

2. **「Filter Administration」**アイコンまたはリンクをクリックします。

   「Configure Web Server Filter」ページが表示されます。

3. 「PLUGIN_DEBUG option」チェック・ボックスを選択します。

4. 「Update」をクリックします。

Java コードのデバッグ・サポート

Java コード・デバッグに使用可能な構成変数はそれぞれ、次のディレクトリ内の sct.cfg ファイルで設定する必要があります。

<*install_dir*>/custom/ContentTracker/resources/sct.cfg

Content Tracker 構成変数の詳細は、付録 A「Content Tracker の構成およびカスタマイズ」を参照してください。sct.cfg ファイル内で変数値を手動設定する方法の詳細は、A-7 ページの「Content Tracker 構成変数の手動設定」を参照してください。

Java コードによって、次のデバッグ構成変数がサポートされるようになりました。

- SctDebugLogEnabled（B-3 ページ）
- SctDebugLogFilePath（B-3 ページ）
- SctDebugServiceBinderDumpEnabled（B-3 ページ）

SctDebugLogEnabled

この構成変数の値は、次のとおりです。

- **`SctDebugLogEnabled=True`** を設定すると、Java コードによって日付スタンプ付きのログ・ファイルに実行トレースが書き込まれるように Content Tracker が構成されます。このファイルに書き込まれる情報の量は非常に多いため、デバッグ目的以外には使用しないでください。
- **`SctDebugLogEnabled=False`** を設定すると、Java コードによって日付スタンプ付きのログ・ファイルに実行トレースは書き込まれません。これがデフォルト値です。

この構成変数の詳細は、A-2 ページの「SctDebugLogEnabled」を参照してください。

SctDebugLogFilePath

SctDebugLogEnabled=True を設定すると、SctDebugLogFilePath を使用してトレース・ログが存在するディレクトリを判別するように Content Tracker が構成されます。SctDebugLogFilePath のデフォルト値は次のとおりです。

<*install_dir*>/custom/ContentTracker/log/SCT_DEBUG_TRACE.log

SctDebugLogFilePath は、SctDebugLogEnabled=True の場合にのみ有効です。この構成変数の詳細は、A-2 ページの「SctDebugLogFilePath」を参照してください。

SctDebugServiceBinderDumpEnabled

この構成変数は、ロギング・サービス・イベントで使用される Content Tracker サービス・ハンドラ・フィルタ（2-5 ページ）によって、記録されるイベントのサービス DataBinder が書き出されるかどうかを制御します。
SctDebugServiceBinderDumpEnabled の詳細は、次の項を参照してください。

- この構成変数の詳細は、B-4 ページの「DataBinder ダンプ機能」を参照してください。
- DataBinder ダンプ・ファイルの内容を表示する方法の詳細は、B-5 ページの「DataBinder オブジェクトのダンプ・ファイルへのアクセス」を参照してください。
- この構成変数の詳細は、A-2 ページの「SctDebugService BinderDumpEnabled」を参照してください。
- サービス用にカスタマイズされたフィールド・データの記録に関連するフィールド・マップの詳細は、3-21 ページの「「Field Map」画面」および 5-3 ページの「拡張サービス・コール・トラッキング機能」を参照してください。

DataBinder ダンプ機能

この項の内容は次のとおりです。

DataBinder ダンプ機能の値

この構成変数の値は、次のとおりです。

- **`SctDebugServiceBinderDumpEnabled=False`** を設定すると、Content Tracker サービス・ハンドラ・フィルタによって DataBinder オブジェクトはダンプ・ファイルに書き出されません。これがデフォルト値です。
- **`SctDebugServiceBinderDumpEnabled=True`** を設定すると、DataBinder オブジェクトがダンプ・ファイルに書き出されるように Content Tracker サービス・ハンドラ・フィルタが構成されます。したがって、ダンプ・ファイルを、拡張サービス・ロギング用のフィールド・マップを開発する際の診断ツールとして使用できます。サービス用のフィールド・マップを作成する場合、ダンプ・ファイルを使用すると、サービス・イベントの記録時に使用可能なデータを確認できます。

DataBinder オブジェクトのダンプ・ファイルについて

Content Tracker によって特定のサービスがログ・ファイルに記録されるとすぐに、そのサービスの DataBinder オブジェクトが、シリアライズされたダンプ・ファイルに書き込まれます。拡張サービス・コール・トラッキング機能を使用するためのフィールド・マップを作成する場合、これらのファイルの内容がデバッグに役立ちます。これらのダンプ・ファイルによって、記録されたサービスに使用可能な LocalData フィールドを確認できます。

注意 : Content Tracker サービス・ハンドラ・フィルタによって DataBinder オブジェクトのダンプ・ファイルが作成されるのは、関連付けられたサービスが SctServiceFilter.hda ファイル内に定義されている場合のみです。このファイルの詳細は、5-2 ページの「サービス・コール構成ファイルについて」を参照してください。

警告 : DataBinder オブジェクトのダンプ・ファイルは、手動で削除しないかぎり、蓄積され続けます。このため、必要な場合以外には SctDebugServiceBinderDumpEnabled 構成変数を使用しないよう注意することをお薦めします。

DataBinder オブジェクトのダンプ・ファイルの場所

シリアライズされた DataBinder オブジェクトは、次の場所に書き込まれます。

<*install_dir*>/custom/ContentTracker/DEBUG_BINDERDUMP/<*dump_file_name*>

DataBinder オブジェクトのダンプ・ファイルの名前

DataBinder オブジェクトのダンプ・ファイルはテキスト・ファイルであり、その名前は次のように 3 つの部分で構成されます。

<*service_name*>_<*filter_function*>_<*serial_number*>.hda

詳細は次のとおりです。

- *service_name* は、記録されたサービスの名前（たとえば、GET_FORM_FILE など）です。
- *filter_function* は次のうちの 1 つです。

End	フィルタ・イベント "onEndServiceRequestActions": 正常なサービス終了イベント。
EndSub	フィルタ・イベント "onEndScriptSubServiceActions": サブ・サービスとして呼び出されたサービスの正常なサービス終了。
Error	フィルタ・イベント "onServiceRequestError": エラーが発生したサービスの終了。End に加えて発生することがあります。

- *serial_number* は、ファイルに割り当てられた一意の識別番号です。これによって、Content Tracker では特定のサービスに対して複数の DataBinder オブジェクト・ダンプ・ファイルを作成できます。

例 :

GET_SEARCH_RESULTS_End_1845170235.hda

DataBinder オブジェクトのダンプ・ファイルへのアクセス

特定の記録済サービスの DataBinder オブジェクトのダンプ・ファイルにアクセスするには、次のようにします。

1. テキスト・エディタで、次のディレクトリ内の特定のデータ・バインダ・ファイルを開きます。

   <*install_dir*>/custom/ContentTracker/DEBUG_BINDERDUMP/

2. 内容の確認

   DataBinder オブジェクトのダンプ・ファイルは、無限に蓄積され続けます。このため、完了したらダンプ・ファイルを手動で削除することをお薦めします。

デバッグ構成変数の設定

Content Tracker 構成変数の設定の詳細は、A-7 ページの「Content Tracker 構成変数の手動設定」を参照してください。

C

サード・パーティ・ライセンス

概要

この付録には、この製品に付属するすべてのサード・パーティ製品のサード・パーティ・ライセンスの説明が含まれます。

APACHE SOFTWARE LICENSE

```
* Copyright 1999-2004 The Apache Software Foundation.
* Licensed under the Apache License, Version 2.0 (the "License");
* you may not use this file except in compliance with the License.
* You may obtain a copy of the License at
*      http://www.apache.org/licenses/LICENSE-2.0
*
```

```
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
```

W3C® SOFTWARE NOTICE AND LICENSE

```
* Copyright © 1994-2000 World Wide Web Consortium,
* (Massachusetts Institute of Technology, Institut National de
* Recherche en Informatique et en Automatique, Keio University).
* All Rights Reserved.  http://www.w3.org/Consortium/Legal/
*
* This W3C work (including software, documents, or other related items) is
* being provided by the copyright holders under the following license.By
* obtaining, using and/or copying this work, you (the licensee) agree that
* you have read, understood, and will comply with the following terms and
* conditions:
*
* Permission to use, copy, modify, and distribute this software and its
* documentation, with or without modification, for any purpose and without
* fee or royalty is hereby granted, provided that you include the following
* on ALL copies of the software and documentation or portions thereof,
* including modifications, that you make:
*
*   1. The full text of this NOTICE in a location viewable to users of the
*      redistributed or derivative work.
*
*   2. Any pre-existing intellectual property disclaimers, notices, or terms
*      and conditions.If none exist, a short notice of the following form
*      (hypertext is preferred, text is permitted) should be used within the
```

```
*      body of any redistributed or derivative code: "Copyright ©
*      [$date-of-software] World Wide Web Consortium, (Massachusetts
*      Institute of Technology, Institut National de Recherche en
*      Informatique et en Automatique, Keio University).All Rights
*      Reserved. http://www.w3.org/Consortium/Legal/"
*
*   3. Notice of any changes or modifications to the W3C files, including the
*      date changes were made.(We recommend you provide URIs to the location
*      from which the code is derived.)
*
* THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS
* MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT
* NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR
* PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE
* ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.
*
* COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR
* CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR
* DOCUMENTATION.
*
* The name and trademarks of copyright holders may NOT be used in advertising
* or publicity pertaining to the software without specific, written prior
* permission.Title to copyright in this software and any associated
* documentation will at all times remain with copyright holders.
*
```

ZLIB LICENSE

* zlib.h -- interface of the 'zlib' general purpose compression library
version 1.2.3, July 18th, 2005

Jean-loup Gailly jloup@gzip.org
Mark Adler madler@alumni.caltech.edu

一般的な BSD ライセンス

Copyright (c) 1998, Regents of the University of California

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

"Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

"Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

"Neither the name of the <ORGANIZATION> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

一般的な MIT ライセンス

Copyright (c) 1998, Regents of the Massachusetts Institute of Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,

DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

UNICODE ライセンス

UNICODE, INC. LICENSE AGREEMENT - DATA FILES AND SOFTWARE

Unicode Data Files include all data files under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/ .Unicode Software includes any source code published in the Unicode Standard or under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/.

NOTICE TO USER: Carefully read the following legal agreement.BY DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING UNICODE INC.'S DATA FILES ("DATA FILES"), AND/OR SOFTWARE ("SOFTWARE"), YOU UNEQUIVOCALLY ACCEPT, AND AGREE TO BE BOUND BY, ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT.IF YOU DO NOT AGREE, DO NOT DOWNLOAD, INSTALL, COPY, DISTRIBUTE OR USE THE DATA FILES OR SOFTWARE.

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1991-2006 Unicode, Inc. All rights reserved.Distributed under the Terms of Use in http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) the above copyright notice(s) and this permission notice appear with all copies of the Data Files or Software, (b) both the above copyright notice(s) and this permission notice appear in associated documentation, and (c) there is clear notice in each modified Data File or in the Software as well as in the documentation associated with the Data File(s) or Software that the data or software has been modified.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS.IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.

_____Unicode and the Unicode logo are trademarks of Unicode, Inc., and may be registered in some jurisdictions.All other trademarks and registered trademarks mentioned herein are the property of their respective owners

その他の帰属

Adobe, Acrobat, and the Acrobat Logo are registered trademarks of Adobe Systems Incorporated.

FAST Instream is a trademark of Fast Search and Transfer ASA.

HP-UX is a registered trademark of Hewlett-Packard Company.

IBM, Informix, and DB2 are registered trademarks of IBM Corporation.

Jaws PDF Library is a registered trademark of Global Graphics Software Ltd.

Kofax is a registered trademark, and Ascent and Ascent Capture are trademarks of Kofax Image Products.

Linux is a registered trademark of Linus Torvalds.

Mac is a registered trademark, and Safari is a trademark of Apple Computer, Inc.

Microsoft, Windows, and Internet Explorer are registered trademarks of Microsoft Corporation.

MrSID is property of LizardTech, Inc. It is protected by U.S. Patent No. 5,710,835. Foreign Patents Pending.

Oracle is a registered trademark of Oracle Corporation.

Portions Copyright © 1994-1997 LEAD Technologies, Inc. All rights reserved.

Portions Copyright © 1990-1998 Handmade Software, Inc. All rights reserved.

Portions Copyright © 1988, 1997 Aladdin Enterprises.All rights reserved.

Portions Copyright © 1997 Soft Horizons.All rights reserved.

Portions Copyright © 1995-1999 LizardTech, Inc. All rights reserved.

Red Hat is a registered trademark of Red Hat, Inc.

Sun is a registered trademark, and Sun ONE, Solaris, iPlanet and Java are trademarks of Sun Microsystems, Inc.

Sybase is a registered trademark of Sybase, Inc.

UNIX is a registered trademark of The Open Group.

Verity is a registered trademark of Autonomy Corporation plc

索引

C

D

I

L

O

R

S

W

あ

さ

し

す

せ

そ

た

ち

つ

て

と

ひ

ふ

め

ゆ

よ

り

れ