AvePoint DocAve

DocAve® コンテンツ シールド

for SharePoint

v2.2

ユーザーガイド

SharePoint 2007 対応

リリース日: 2012 年 8 月 21 日

The Enterprise-Class **Management Platform** for **SharePoint**® Governance

目次

目次 2
DocAve コンテンツ シールド for SharePoint について 5
補助製品について 5
お使いになる前に 6
構成 6
エージェント 6
コンテンツ シールド for SharePoint のインストール 7
直接インストール 7
Web フロントエンド サーバーへの遠隔インストール 8
使用開始にあたって 9
コンテンツ シールド for SharePoint へのアクセス 9
ライセンスと設定 10
SharePoint 全体管理サーバーへのライセンス適用 10
各 Web フロントエンド サーバーへのライセンス適用 10
データベースの構成 11
既存データベースに接続 11
新規データベースの作成 12
グローバル設定の構成 12
電子メール プロファイルの構成 13
電子メールの設定 14
メール テンプレートの編集 14
コンテンツ シールドの機能 15
フィルター定義ファイル 15
コンテンツ定義ファイルの作成 16
ファイル タイプ定義ファイルの作成 16

スキャン エンジン 17
スキャン エンジンの作成 17
コンテンツ シールド ポリシー 18
コンテンツ シールド ポリシーの作成 18
フィルター 23
リアルタイム フィルター 24
スケジュール フィルター 26
レポート 28
リスク レポート 30
ファイルのリストア・削除 30
付録 A 32
HIPAA (医療保険の相互運用性と説明責任に関する法律) 対応定義ファイル 32
ビジネス定義ファイル 32
クレジットカード番号定義ファイル 32
日付定義ファイル 32
電子メール アドレス定義ファイル 34
ファックス番号定義ファイル 34
一般定義ファイル 34
行政定義ファイル 35
福祉厚生定義ファイル 35
IP アドレス定義ファイル 35
社会保障番号定義ファイル 35
URL 定義ファイル 36
米国住所定義ファイル 36
米国電話番号定義ファイル 37
車両識別番号定義ファイル 37
付録 B 38

ドキュメント リスク 38
リスク サマリー 39
付録 C 40

DocAve コンテンツ シールド for SharePoint について

DocAve コンテンツ シールドは、WSSv3、SharePoint 2007、SharePoint 2010 プラットフォームにおいてビジネスにふさわしくない操作などの防止を実現する、廉価性と高信頼性を備えたソリューションです。リアルタイム・スケジュールの 2 パターンから選択可能なコンテンツ スキャン機能では、コンテンツの検査をいつ、どのように実行するかを具体的に指定することができます。検疫機能は完全にカスタマイズ可能、電子メール通知機能と組み合わせることで DocAve コンテンツ シールドの能力を業務プロセスの確実な効率化へとつなげることが可能となります。DocAve コンテンツ シールドの活用により、SharePoint 2007/2010 におけるコンプライアンスを自動化し、有害なコンテンツを未然に防止する環境を構築することができるようになります。

すべての AvePoint 製品と同様、DocAve コンテンツ シールド for SharePoint では Microsoft に完全サポートされた手法および API のみを使用しています。

補助製品について

DocAve 6 プラットフォームに同梱された製品および製品群のいくつかは、DocAve コンテンツ シールド for SharePoint と組み合わせることで効力を発揮します。以下の製品については DocAve コンテンツ シールド for SharePoint との同時使用を推奨します:

- DocAve コンテンツ マネージャー – コンテンツ シールド ポリシーを使用して特定のコンテンツを SharePoint 上でブロックする方法ではなく、コンテンツへのタグ付けを実施し、コンテンツ マネージャーの機能によりタグ付けされたコンテンツを一括で指定の場所へ移動させることができます。

- DocAve レプリケーター – コンテンツ シールド ポリシーを使用して特定のコンテンツを SharePoint 上でブロックする方法ではなく、コンテンツへのタグ付けを実施することで、レプリケーターの機能によりタグ付けされたコンテンツを一括でレプリケートするノードを指定して構成することができます。

お使いになる前に

DocAve コンテンツ シールド for SharePoint では、SharePoint 上にアップロードされたコンテンツや既に SharePoint コンテンツ データベース上に保存されているコンテンツに対し、事前に作成したキーワードや定義を基にリアルタイムなスキャンを実行することができます。この機能は SharePoint Web フロントエンドサーバーへの展開と管理を迅速かつ簡単に実行するため、SharePoint の全体管理で統合管理されています。この機能へアクセスするためには SharePoint のファーム管理者権限が必要となります。

DocAve コンテンツ シールド for SharePoint のインストール・使用を開始する前に、システムおよびファーム要件内の構成セクションをご参照ください。

***注意:** Microsoft Office 2007 またはそれ以上のバージョンで作成されたファイルをフィルターしたい場合、Microsoft Office iFilter パックを SharePoint FEW 上にインストールしておく必要があります。Microsoft Office iFilter パックは こちら からダウンロードが可能です。

構成

SharePoint WFE および SharePoint 全体管理サーバーは、以下の動作環境が必要です:

- Microsoft Office SharePoint Server (MOSS) 2007 または Windows SharePoint Services (WSS) v3
- Windows Server 2003 または 2008
- *SQL Server 2005 SP1、SQL Server 2008、SQL Server 2008 R2 のいずれか
- .NET Framework v2 またはそれ以上

***注意:** DocAve コンテンツシールド for SharePoint は、 Built-in SQL サーバーを使用するスタンドアロン SharePoint サーバーにはインストールできません。また DocAve コンテンツシールド for SharePoint では、動作のために外部 SQL サーバーが必要となります。

エージェント

すべての DocAve 製品と同様、DocAve コンテンツシールド for SharePoint はマネージャー / エージェント構成で動作します。この構成では、マネージャーが SharePoint 全体管理にインストールされ、かつエージェントがユーザーによるコンテンツ作成・アップロードが可能な SharePoint Web フロントエンド (WFE) すべてに展開されている必要があります。すべての WFE に対してエージェントを展開することで、ファームに対して完全な保護を提供することができます。SharePoint の WFE および全体管理では以下の環境が必要です。

コンテンツ シールド for SharePoint のインストール

DocAve コンテンツ シールド for SharePoint の zip ファイルをダウンロードし、SharePoint 全体管理サーバー上でパッケージを解凍します。

コンテンツ シールド for SharePoint のインストール ウィザードを起動する前に、以下の項目を確認してください:

- コンテンツ シールド for SharePoint v2.1 のインストールの前に、古いバージョンのアンチウイルスおよびコンテンツ シールドをすべてアンインストールしてください。
- インストール ウィザードは、まず SharePoint 全体管理サーバー上で実行してください。これにより DocAve コンテンツ シールド for SharePoint の各 WFE サーバーへのインストールを遠隔で実行することができるようになります。

***注意:** DocAve コンテンツ シールド for SharePoint および DocAve アンチウイルス for Microsoft SharePoint が SharePoint 全体管理にインストールしてある状態で、DocAve アンチウイルス for Microsoft SharePoint をアンインストールすると、DocAve コンテンツ シールド for SharePoint も同時にアンインストールされます。

DocAve コンテンツ シールド for SharePoint の zip ファイル解凍を完了後、ディレクトリ内の setup.exe ファイルを実行します。DocAve コンテンツ シールド for SharePoint のインストールには、各 Web フロントエンド サーバーへ直接インストールする方法と、SharePoint 全体管理にインストールした後に各 Web フロントエンド サーバーへ展開する方法の 2 種類があります。

直接インストール

各サーバーへの直接インストールにつきましては以下の手順に従ってください。

1. *setup.exe* ファイルを実行します。
2. **名前** と **会社情報** を入力し、本製品をインストールする **ディレクトリ場所** を指定します。
3. 以下のメッセージがポップアップ表示されます:
   "DocAve コンテンツ シールド for SharePoint リアルタイム機能をご使用頂くには、SharePoint の LAYOUTS フォルダー配下のアップロードページ ファイルを置き換える必要があります。本当に置き換えますか？"
   a. **[はい]** を選択すると、*upload.aspx* ファイルをコンテンツ シールドのリアルタイム フィルター機能に使用するものへと置き換えます。コンテンツ シールドに使用される *upload.aspx* ファイルは、コンテンツ シールドによってファイルのアップロードがブロックされる際に、ファイルの所有者である SharePoint ユーザーの情報を提供します。

b. **[いいえ]** を選択すると、*upload.aspx* ファイルは SharePoint 内で置き換えられません。この際以下のメッセージが表示されます:

"インストールを完了することができません。*DocAve* コンテンツ シールド *for SharePoint* のリアルタイム機能のユーザビリティーに影響を及ぼす可能性があります。本当にインストールを続行しますか？"

[OK] をクリックすると、*upload.aspx* ファイルを SharePoint 内で置き換えずに残りのインストール作業を継続します。[**戻る]** をクリックすると 1 つ前の画面に戻ります。

***注意:** *upload.aspx* ファイルを置き換えずにインストール作業を終了すると、**[コンテンツと次のエラー メッセージを置換する]** が有効になった状態でコンプライアンス違反のドキュメントがリアルタイム フィルターによりブロックされた際、当該ドキュメントの編集によってエラーが発生する可能性があります。

***注意:** SharePoint Designer を使用してサイト内の *upload.aspx* ファイルを変更した場合、あるいは DocAve コンテンツ シールド for SharePoint のインストール以前にカスタム *upload.aspx* ファイルを使用していた場合、**[コンテンツと次のエラー メッセージを置換する]** が有効になった状態でコンプライアンス違反のドキュメントがリアルタイム フィルターによりブロックされた際、当該ドキュメントの編集によってエラーが発生する可能性があります。

***注意:** DocAve コンテンツ シールド for SharePoint をアンインストールすると、*upload.aspx* ファイルは元の SharePoint 既定 *upload.aspx* ファイルへ戻ります。

4. ツールのインストール後、インストールを完了するために IIS の再起動を示すダイアログが表示されます。[いいえ] を選択すると、後で IIS を再起動することができます。

   ***注意:** この IIS リセットは IIS サービスをただちには再起動せず、IIS プロセスのリセットを非強制で実行できます。現在実行しているプロセスは、このリセットが実行される前に終了します。IIS を後で再起動する場合、再起動されるまでインストールは完了しません。

Web フロントエンド サーバーへの遠隔インストール

遠隔インストールを実行する場合、まず SharePoint 全体管理サーバー上で *setup.exe* ファイルを実行します。インストール完了後、全体管理画面から **サーバー構成の管理 > *AvePoint* ツールとサービス > *DocAve* コンテンツシールド *for SharePoint* > *Web* フロントエンド設定** へと移動します。カーソルをサーバー名の上へ移動させてコンテンツ シールドをインストールしたい *Web* フロントエンド サーバーを選択し、クリックします。ドロップダウン メニューから **[今すぐ展開する]** を選択します。

***注意:** このプロセスでコンテンツ シールドをインストールする Web フロントエンド サーバーは、全体管理に接続されており、かつ起動している必要があります。

使用開始にあたって

DocAve コンテンツ シールド for SharePoint のインターフェイスは SharePoint 全体管理に統合されています。本ユーザーガイドでは Sharepoint 2007 での全体管理インターフェイスをご説明します。SharePoint 2010 での全体管理インターフェイスの使用法につきましては、DocAve コンテンツ シールド for SharePoint ユーザーガイド: SharePoint 2010 対応版 をご参照ください。

コンテンツ シールド for SharePoint へのアクセス

コンテンツ シールド for SharePoint にアクセスし、本製品の機能を使用する場合、以下の手順に従ってください:

- SharePoint 全体管理 > サーバー構成の管理 へ移動します。
- [AvePoint ツールとサービス] セクションから **[DocAve コンテンツ シールド for SharePoint]** を選択します。

画像 1: SharePoint 全体管理画面よりコンテンツ シールドへアクセス

DocAve コンテンツ シールド for SharePoint ページでは、ライセンスを適用した後に適切な構成およびカスタマイズを適用することで、お使いの SharePont 環境に合わせたコンテンツ シールドの機能を活用することができるようになります。

ライセンスと設定

コンテンツ シールドの SharePoint 環境保護機能を適切に起動するため、はじめに以下の構成を実行する必要があります:

- **[Web フロントエンド設定]** から、ご購入いただいたコンテンツ シールドのライセンスを SharePoint 全体管理サーバーおよび各 Web フロントエンド サーバーへ適用します。
- **[アプリケーション データベース]** でコンテンツ シールドが接続するデータベースを構成します。DocAve コンテンツ シールド for SharePoint では、設定や構成を保存するためのアプリケーション データベースが必要となります。このアプリケーション データベースは、SharePoint 環境と同一のインスタンスに展開することを推奨しますが、お使いのネットワーク ドメイン内の別の SQL インスタンスに展開されたアプリケーション データベースを使用することもできます。
- **[グローバル設定]** では、機能性能や問題発生時の対応などを構成できます。
- **[電子メール プロファイル]** では、コンテンツ シールドで違反コンテンツを検知した際に、指定した受取人に対し通知を送信する設定を構成できます。
- **[電子メールの設定]** で通知メッセージのテンプレートを構成します。

SharePoint 全体管理サーバーへのライセンス適用

SharePoint 全体管理サーバーにライセンスを適用したい場合、以下の手順をご参照ください。

1. DocAve コンテンツ シールド for SharePoint トップ画面で、画面左側ペインから **[Web フロントエンド設定]** をクリックします。
2. ライセンス管理セクションで **[参照]** をクリックし、適用したいコンテンツ シールドのライセンスを選択します。
3. **[適用]** をクリックします。 ライセンスの適用が完了すると、ライセンス管理セクションにライセンスのタイプ、有効期間、許可される SharePoint フロントエンド Web サーバーの台数などの情報が表示されます。

各 Web フロントエンド サーバーへのライセンス適用

各 Web フロントエンド サーバーにライセンスを適用したい場合、以下の手順をご参照ください。

1. DocAve コンテンツ シールド for SharePoint トップ画面で、画面左側ペインから **[Web フロントエンド設定]** をクリックします。
2. ライセンスを適用したい Web フロントエンド サーバーを選択します。
3. ドロップダウン メニューから **[ライセンスの適用]** を選択します。

データベースの構成

コンテンツ シールドのインストールには、設定や構成を保存するためのアプリケーション データベースが必要です。既存データベースに接続するか、新規データベースを作成するかを選択してください。コンテンツ シールドのデータベースはお好みで構成可能ですが、以下の内容を必ずご確認ください:

- アプリケーション データベースはお使いの SharePoint 環境と同一のインスタンスに展開してください。お使いのネットワーク ドメイン内の別の SQL インスタンスに展開されたアプリケーション データベースを使用することもできますが、本製品は SharePoint に統合されるため、SharePoint と同一の SQL インスタンスを使用すれば必要な権限を有効に活用することができます。
- DocAve コンテンツ シールド for SharePoint で事前に作成されたデータベースがある場合、既存データベースの使用を選択することができます。
- DocAve コンテンツ シールド for SharePoint 1.3 から DocAve コンテンツ シールド for SharePoint 2.1 へアップグレードし、旧バージョンで使用していたデータベースを再利用しようとする場合、まずデータベースのアップグレードを実行する必要があります。データベースのアップグレード完了後、2.1 バージョンで表示されるポリシー名は以下の形式となります:
  ポリシー名_エンジン名
  (1.3 で構成されたフィルター プランに合わせ、エンジン名がポリシー名に追加される形となります)

DocAve コンテンツ シールド for SharePoint のトップ画面からデータベースを構成する場合、まず画面左側ペインから **[アプリケーション データベース]** を選択します。コンテンツ シールドにデータベースが割り当てられていない場合、まず割り当て設定を実行するようメッセージが表示されます。

既存データベースに接続

既存のデータベースに接続するには、以下の手順に従ってください:

1. [アプリケーション データベース タイプの選択] セクションで、ドロップダウン メニューから **[既存データベースに接続]** を選択します。

2. [データベース名と認証] セクションで以下の設定を入力します:

   - **データベース サーバー** – 接続するデータベース サーバーのアドレスを入力します。

   - **データベース名** – サーバー内で接続するデータベースの名前を入力します。

- **データベース認証** – 認証方法を選択します。ここでは **Windows 認証** の使用を推奨します。**SQL 認証** を選択した場合、アクセス用の **アカウント** および **パスワード** も設定する必要があります。

3. **[接続]** をクリックすると指定したデータベースに接続します。

新規データベースの作成

新規データベースを作成するには、以下の手順に従ってください:

1. [アプリケーション データベース タイプの選択] セクションで、ドロップダウン メニューから **[新規データベースの作成]** を選択します。

2. [データベース名と認証] セクションで以下の設定を入力します:

   - **データベース サーバー** – 接続するデータベース サーバーのアドレスを入力します。

   - **データベース名** – サーバー内で接続するデータベースの名前を入力します。

   - データベース認証 – 認証方法を選択します。ここでは **Windows 認証** の使用を推奨します。**SQL 認証** を選択した場合、アクセス用の **アカウント** および **パスワード** も設定する必要があります。

3. **[作成]** をクリックするとデータベースが作成されます。

グローバル設定の構成

グローバル設定では、コンテンツ シールドの性能やストレージ容量などに関連する設定を行います。ここではコンテンツ シールドのフィルターやレポートに使用するログ設定や、DocAve コンテンツ シールド for SharePoint のシステム ログ設定などを構成することができます。ログとは、DocAve コンテンツ シールド for SharePoint の使用中に万一問題などが発生した場合、サポートチームによって調査が行われる際に必要となる情報を含むものです。これら設定の構成を行うには、DocAve コンテンツ シールド for SharePoint のトップページから **[グローバル設定]** へと移動します。

- **スレッド数** –スキャンを実行する際に DocAve コンテンツシールド for SharePoint で使用するスレッドの数を指定できます。スレッド数が多いとスキャンにかかる時間は短くなりますが、SharePoint Web フロントエンド上で

の読み込みパフォーマンスが悪くなります。スレッド数が多いとスキャンにかかる時間は短くなりますが、SharePoint Web フロントエンド上での読み込みパフォーマンスが悪くなります。

- **コンテンツ フィルター ログとレポートの設定** - コンテンツ フィルター ログには、ページ リダイレクトやフィルター ジョブ情報、スキャン済みファイル情報、エラー メッセージなど、コンテンツ シールドのジョブ プロセス情報が含まれます。以下の設定を構成してください:
    - ログ レベル -現在のフィルター ログのログ レベルを選択して表示します。ドロップダウン メニューから**エラー**、**警告**、**情報**、**デバッグ**が選択できます。**エラー**はエラー レベルのログのみ表示します。**警告**はエラー レベルと警告レベルのログを表示します。**情報**は情報レベル、警告レベル、エラー レベルのログが表示されます。**デバッグ**はデバッグ レベル、情報レベル、警告レベル、エラー レベルすべてのログを表示します。
    - 最大保管時間 –レポートを削除するまでの期間を選択します。
- **DocAve コンテンツ シールド for SharePoint のシステム ログ設定** –現在のシステム ログのログ レベルを選択して表示します。ドロップダウン メニューから**エラー**、**警告**、**情報**、**デバッグ**が選択できます。**エラー**はエラー レベルのログのみ表示します。**警告**はエラー レベルと警告レベルのログを表示します。**情報**は情報レベル、警告レベル、エラー レベルのログが表示されます。**デバッグ**はデバッグ レベル、情報レベル、警告レベル、エラー レベルすべてのログを表示します。

これらの設定を変更した場合、保存するには **[保存]** ボタンをクリックします。設定を消去するには **[リセット]** ボタンをクリックします。

***注意:** 本製品で問題が発生した場合、AvePoint テクニカルサポートへお問い合わせいただく前に、すべての [ログレベル] 設定を **[デバッグ]** に変更し、新しいログ レベルでエラーを再度実行してみることを推奨します。

電子メール プロファイルの構成

電子メール プロファイルでは、コンテンツ シールドのスキャン ジョブで違反ファイルが検知された際や、スキャン完了後にレポートが生成された際などに通知を送る先のユーザーを、フィルター構成ごとに設定できます。

電子メール プロファイルを構成するには、DocAve コンテンツ シールド for SharePoint のトップ画面の左側ペインから **[電子メール プロファイル]** に移動します。画面左側のメール プロファイル セクションに構成済みの電子メール プロファイルが表示されます。

新規に電子メール プロファイルを作成する場合、画面右下の **[新規]** をクリックします。既存の電子メール プロファイルを変更したい場合は、まず電子メール プロファイルを選択してから設定を変更します。いずれの場合も以下の設定が必要です:

- **電子メール プロファイル名** – 電子メール プロファイルの名前を入力します。
- **SMTP 電子メール サーバー** – お使いの Microsoft Exchange 送信メール サーバー (SMTP) のホスト名および IP アドレスを入力し、対応するポート番号を指定します。一般的な環境では、既定 SMTP ポート番号は 25 です。メールサーバー上の認証を手動で構成した場合、**[電子メール サーバー認証]** チェックボックスをオンにして、適切な **ユーザー名** および **パスワード** を入力してください。
- **差出人** – 電子メールを送信する元のメールアドレスを入力してください。
- **受取人** – このメール プロファイルを使用する際にメールを受信するアドレスを入力します。受取人を複数指定したい場合、各アドレスは改行して追加してください。

電子メールの構成の完了後 **保存** をクリックします。

***注意**: メールを送信するアカウントがプロファイルの受取人リストに含まれていないことを確認してください。含まれている場合、メッセージ システムでエラーが発生するおそれがあります。

電子メールの設定

このセクションでは、ファイル タイプに合わせた電子メール通知のテンプレートを構成することができます。これにより送信する通知の内容にどの情報を含めるかを指定できます。

電子メールのテンプレートは、それぞれの既定メッセージなどで構成済みのものが設定されています。 メールの設定を構成する場合、DocAve コンテンツ シールド for SharePoint のトップ画面の左側ペインから **[電子メールの設定]** に移動します。ここでは [リアルタイム フィルター通知設定]、[スケジュール フィルター通知設定] の 2 種類のテンプレートを構成可能です。**[メール テンプレートの編集]** をクリックして、対応するファイル タイプのメールテンプレートを編集します。

メール テンプレートの編集

以下の設定を編集します。

- **件名** – メール通知のテンプレートに使用する名前を入力します。
    - キーワードの追加 – 含めたいキーワードをドロップダウン メニューから選択し、**[追加]** をクリックします。この構成を行うと、レポートから引用された情報が件名に追加されます。
- **メッセージ** – メール通知の本文を構成編集します。
    - キーワードの追加 – 含めたいキーワードをドロップダウン メニューから選択し、**[追加]** をクリックします。この構成を行うと、レポートから引用された情報が件名に追加されます。

メール テンプレート編集の完了後、**OK** をクリックして編集を保存します。**キャンセル** をクリックすると、変更を保存せずに前の画面に戻ります。

コンテンツ シールドの機能

DocAve コンテンツ シールド for SharePoint は、以下の機能で構成されています:

- フィルター定義ファイル – カスタム可能なフィルター定義ファイルにより、不適切なコンテンツを識別します。
- スキャン エンジン – 設定したスキャン エンジンとフィルター定義ファイルを組み合わせることで、特定の有害コンテンツを対象としたフィルタリングを実施できます。
- コンテンツ シールド ポリシー – スキャン エンジンで検知した有害コンテンツに対する処理を定義することができます。
- フィルター (リアルタイム / スケジュール) – ポリシーを適用する SharePoint 環境に制限を設定するフィルターを作成します。スキャン エンジンで指定したフィルター定義ファイルを元に、適用するポリシーによって検索の範囲を指定することができます。

フィルター定義ファイル

コンテンツ シールドを有効にして有害なコンテンツを検知できるようにするには、まずご自身の組織にとっての有害コンテンツを定義する必要があります。フィルター定義ファイルには以下の 2 種類があります:

- コンテンツ定義ファイル – コンテンツ定義ファイルは、有害なコンテンツを含むアイテムをフィルタリングします。フィルターの定義はキーワード、フレーズ、表現などで設定可能です。
- ファイル タイプ定義ファイル – ファイル タイプ定義ファイルは、特定のファイル タイプをフィルタリングします。フィルターの定義はファイルの拡張子やヘッダーで識別することができます。

フィルター定義ファイルのページに移動するには、DocAve コンテンツ シールド for SharePoint のトップ画面の左側ペインから **[フィルター定義ファイル]** に移動します。構成済みのフィルター定義ファイルはすべてここに表示されます。フィルター定義ファイルの表示数を変更したい場合、画面右上の **[サイズ]** ドロップダウン メニューから数を指定できます。 表示するフィルター定義ファイルの順番を変更する場合は、各列のヘッダーをクリックしてソートすることができます。

フィルター定義ファイルを削除する場合、削除したいアイテムの左側にあるチェックボックスをオンにし、画面右上の **[選択部分を削除]** をクリックします。すべて削除したい場合は、[すべてを空にする] をクリックします。

主なキーワードおよび表現をリスト形式で表示する場合は、付録 A をご参照ください。.

コンテンツ定義ファイルの作成

コンテンツ定義ファイルを新規作成するには、[新規定義ファイルの追加] の隣にあるドロップダウン メニューから **[コンテンツ定義ファイル]** を選択します。コンテンツ定義ファイルの編集画面が表示されますので、新規に作成したいコンテンツ定義ファイルについての以下の情報を入力します:

- **定義ファイル名** – 新規コンテンツ定義ファイルの名前を入力します。
- **カテゴリ** – 新規コンテンツ定義ファイルが分類される先のカテゴリを指定します。
- **定義ファイルの説明** – 新規コンテンツ定義ファイルの説明を入力します。この設定は必須ではありません。
- **リスク値** – リスク値を 0 ~ 100 の数字で入力します。このコンテンツ定義ファイルで設定した有害ファイルがドキュメント内で見つかった際に、リスク値がここで指定する数値まで上昇します。
- **定義ファイル キーワード** – 新規コンテンツ定義ファイルのキーワードを指定します。ここでは単語、フレーズ、表現などで指定可能です。複数のキーワードを入力する場合は改行して追加してください。

コンテンツ定義ファイル構成の完了後、**OK** をクリックして編集を保存します。**キャンセル** をクリックすると、変更を保存せずに前の画面に戻ります。作成後にコンテンツ定義ファイルを変更するには、フィルター定義ファイルの表示画面で変更したいアイテムをクリックします。編集画面で、上記の手順に従って編集を行ってください。

ファイル タイプ定義ファイルの作成

コンテンツ定義ファイルを新規作成するには、[新規定義ファイルの追加] の隣にあるドロップダウン メニューから **[ファイル タイプ定義ファイル]** を選択します。コンテンツ定義ファイルの編集画面が表示され、新規に作成したいコンテンツ定義ファイルについての以下の情報を入力します:

- **定義ファイル名** – 新規ファイル タイプ定義ファイルの名前を入力します。
- **カテゴリ** – 新規ファイル タイプ定義ファイルが分類される先のカテゴリを指定します。
- **定義ファイルの説明** – 新規ファイル タイプ定義ファイルの説明を入力します。この設定は必須ではありません。
- **リスク値** – リスク値を 0 ~ 100 の数字で入力します。このファイル タイプ定義ファイルで設定した有害ファイルがドキュメント内で見つかった際に、リスク値がここで指定する数値まで上昇します。
- **ブロックするファイルの種類** – ファイル タイプの一覧が表示されます。フィルター定義ファイルの表示数を変更したい場合、画面右上の **[サイズ]** ドロップダウン メニューから数を指定できます。ドロップダウン メニューの左隣にある矢印ではページ移動ができます。

ファイル拡張子の右にあるチェックボックスをオンにすることでブロックすることが可能です。既定では **ファイル ヘッダー** 列のチェックボックスが選択されており、アイテムの拡張子が変更された場合でもスキャン対象とすることができます。

リストに含まれていないファイル タイプについては **ブロックするファイルの種類** チェックボックスをオンにし、JPG、DOCX、EXE など拡張子の形式で入力します。拡張子はそれぞれ改行して入力してください。このフィールドでは大文字・小文字の区別はありません。

ファイル タイプ定義ファイル構成の完了後、**OK** をクリックして編集を保存します。**キャンセル** をクリックすると、変更を保存せずに前の画面に戻ります。作成後にファイル タイプ定義ファイルを変更するには、フィルター定義ファイルの表示画面で変更したいアイテムをクリックします。編集画面で、上記の手順に従って編集を行ってください。

スキャン エンジン

スキャン エンジンは、アイテムが有害コンテンツを含んでいた場合にどのコンテンツ シールドのフィルターを使用するかを決定する機能です。スキャン エンジンではフィルター定義ファイルとファイル サイズ制限が指定されます。

スキャン エンジンを使用するには、DocAve コンテンツ シールド for SharePoint のトップ画面の左側ペインから **[スキャン エンジン]** に移動します。既に構成済みのスキャン エンジンがここに表示されます。スキャン エンジンの表示数を変更したい場合、画面右上の **[サイズ]** ドロップダウン メニューから数を指定できます。 表示するスキャン エンジンの順番を変更する場合は、**[エンジン名]** 列のヘッダーをクリックしてソートすることができます。

スキャン エンジンを削除する場合、削除したいアイテムの左側にあるチェックボックスをオンにし、画面右上の **[選択部分を削除]** をクリックします。すべて削除したい場合は、[すべてを空にする] をクリックします。

スキャン エンジンの作成

スキャン エンジンを新規作成するには、リスト上部の **[新規スキャン エンジンの追加]** を選択します。スキャン エンジンの編集画面が表示され、新規に作成したいスキャン エンジンについての以下の情報を入力します:

- **エンジン名** – 新規スキャン エンジンの名前を入力します。
- **エンジンの説明** – 新規スキャン エンジンの説明を入力します。この設定は必須ではありません。
- **エンジン定義ファイル** – **ファイル サイズ フィルター** セクションでフィルタリングするファイル サイズの設定をおこなった後、このスキャン エンジンで使用するフィルター定義ファイルを選択します:
    - **ファイル サイズ フィルター** チェックボックスをオンにし、フィルタリングの基準としてファイルのサイズを使用するかどうかを選択します。このオプションを選択した場合、ドロップダウン メニューから **次の値以上**、**次の範囲**、**次の値以下** の中から一つを選択し、任意の数値を入力した後、続くドロップダウン メニューから単位を選択します。**次の範囲** が選択された場合、ファイル サイズの上限および下限を設定する必

要があります。**次の値以上** を選択した場合、例えばボックスに **1** と入力して単位から **MB** を選択すると、1MB を超えるファイルがすべてフィルタリングの対象となり、1MB 以下のファイルはこのスキャン エンジンを使用するコンテンツ シールド フィルターによって自動的に排除されます。

- コンテンツ定義ファイル – 既存のフィルター定義ファイルがすべてここに表示されます。
  チェックボックスをオンにして、このスキャン エンジンを使用したいフィルター定義ファイルを選択します。**[すべてを選択]** チェックボックスをオンにすると全コンテンツ定義ファイルを選択できます。
- ファイル タイプ定義ファイル -既存のファイル タイプ定義ファイルがすべてここに表示されます。
  チェックボックスをオンにして、このスキャン エンジンを使用したいファイル タイプ定義ファイルを選択します。**[すべてを選択]** チェックボックスをオンにすると全ファイル タイプ定義ファイルを選択できます。

スキャン エンジン構成の完了後、**保存** をクリックして編集を保存します。**キャンセル** をクリックすると、変更を保存せずに前の画面に戻ります。作成後にスキャン エンジンを変更するには、スキャン エンジンの表示画面で変更したいエンジン名をクリックします。編集画面で、上記の手順に従って編集を行ってください。

コンテンツ シールド ポリシー

コンテンツ シールド ポリシーは、スキャン エンジンが有害コンテンツを検知した場合にどのような処理を行うかを決定するコンテンツ シールド フィルターを指定します。

コンテンツ シールド ポリシーを使用するには、DocAve コンテンツ シールド for SharePoint のトップ画面の左側ペインから **[コンテンツ シールド ポリシー]** に移動します。既に構成済みのコンテンツ シールド ポリシーが画面左側に表示されます。

コンテンツ シールド ポリシーを削除する場合、削除したいコンテンツ シールド ポリシーの名前をクリックし、画面右下の **[削除]** ボタンをクリックします。

コンテンツ シールド ポリシーの作成

コンテンツ シールド ポリシーを新規作成するには、画面右下の **[新規]** をクリックします。コンテンツ シールド ポリシーの編集画面が表示され、新規に作成したいコンテンツ シールド ポリシーについての以下の情報を入力します:

- **ポリシー名** – 新規コンテンツ シールド ポリシーの名前を入力します。
- ***スキャン エンジン** – このコンテンツ シールド ポリシーを使用して有害コンテンツの検知を行うスキャン エンジンを選択します。

- ファイル フィルター – このオプションでは、スキャン エンジンに使用されているフィルター定義ファイルへの例外および追加を構成します。フィルター定義ファイル自体の修正は必要ありません。この機能により、複数のバージョンのフィルター定義ファイルやスキャン エンジンを作成する必要がなくなります。なお、ファイル フィルターはファイル タイプでのみ構成可能です。**ファイル フィルターから排除する** か **ファイル フィルターに含む** のいずれかを選択し、対象ファイル タイプをフィールドに入力します。複数のファイル タイプを入力する場合は改行して追加してください。
- コンテンツ フィルター アクション – スキャン エンジンが有害コンテンツを検知した場合、コンテンツ シールドでどのような処理を行うかを構成します。コンテンツ シールド ポリシーはリアルタイム フィルター・スケジュール フィルターのいずれでも使用できますが、コンテンツ フィルター アクションはコンテンツ シールド ポリシーを使用するフィルターがリアルタイムかスケジュールかによって異なる動作を行います。

  以下はこれら構成に基づくリアルタイム フィルターの動作です:

  - **アクション – リスクが次の値と同じかそれ以上である場合、SharePoint から有害なアイテムをブロックします** チェックボックスをオンにしてリスク値を指定した際に、有害コンテンツをブロックするかどうかを指定します。ブロックしたコンテンツが保存される予定だった移動先には A *_BLOCK.txt* ファイルが作成されます。 このチェックボックスをオンにすると、以下の構成も必要になります:
    - **コンテンツと次のエラー メッセージを置換する** – このチェックボックスをオンにすると、ブロックしたコンテンツが保存される予定だった移動先にダミー ファイルを作成します。ダミー ファイル内に含める **エラー メッセージ** を構成するか、以下の既定メッセージを使用することもできます:
      ドキュメント内で不適切なコンテンツが見つかりました。
    - **有害なファイルを検疫フォルダーに保存する** – このチェックボックスをオンにすると、ブロックしたファイルを保存する検疫フォルダーを作成します。このライブラリへアップロードする際にブロックされたファイルはすべて検疫フォルダーへ移動します。同じ名前の有害ファイルが複数検疫ファイルにアップロードされると、各ファイルの名前の末尾に数字が追加されます。例えば複数の *testfile.doc* という名前の有害ファイルが同一フォルダー内に存在する場合、ファイル名は *testfile_0.doc*、*testfile_1.doc*、*testfile_2.doc*… となります。
      有害ファイルを検疫フォルダーへ移動する際、通知する AD ユーザー / AD グループを指定することができます。この機能を有効にするには、あらかじめこのポリシーを使用するフィルターで電子メール プロファイルを構成しておく必要があります。また、ここで指定したユーザーが SharePoint サイトへアクセスする適切な権限をもっていれば、検疫フォルダーへもアクセスすることができます。ユーザーが SharePoint サイトへのアクセス権を持っていない場合は、検疫フォルダーへアクセスすることができません。この機能はスケジュール フィルターのみで使用することができます。

  ***注意:** 検疫フォルダー内では、 *_BLOCK.txt* という名前のファイルは必ず 1 つのみ存在できます。新規に *_BLOCK.txt* ファイルが作成される場合、古いファイルは削除されます。

***注意: リスクが次の値と同じかそれ以上である場合、SharePoint から有害なアイテムをブロックします** チェックボックスがオンになっている場合、**コンテンツと次のエラー メッセージを置換する** および **有害なファイルを検疫フォルダーに保存する** が選択されていても、有害ファイルは例外なくブロックされます。

- **タグ** – 有害ファイルに対してタグ付けを行うかを選択します。**タグ** チェックボックスをオンにし、**名前** および **説明** フィールドを入力すると、SharePoint 上にタグを示す列が追加されます。 既定の名前は **ブロック**、既定の説明は **このドキュメント内で不適切なコンテンツが見つかりました。** です。
  注意:** エラーメッセージ内にファイル名および有害と判断された理由を表示したい場合、説明欄に ***%file name% および ***%invalid string%*** という形式で含めることでエラーメッセージ内に表示されるようになります。
- **チェックアウトを破棄する** – このオプションはスケジュール フィルターでのみ使用できます。スケジュール フィルターで、このオプションが有効になっているポリシーを使用してスキャン ジョブを実行すると、以下の影響があります。
  - ファイルがチェックアウトされており、かつ最新の未チェックアウト バージョンに不適切なコンテンツが含まれている場合、このファイルのチェックアウトは破棄され、不適切なコンテンツを含む最新バージョンが検疫されます。この場合、チェックアウト バージョンへの変更は無視されます。
  - ファイルがチェックアウトされており、かつ最新の未チェックアウト バージョンには不適切なコンテンツが含まれていない場合、チェックアウト済みバージョンに不適切なコンテンツが含まれていても、アイテムは現在の状態を保持します。このファイルが再度チェックインされた場合、リアルタイム フィルターによって不適切なコンテンツがスキャンされます。他のユーザーは、このファイルのチェックインが完了するまで、不適切なコンテンツへの編集を見ることができません。
- アップロードされたファイルが自動的にチェックアウトされ、その後スケジュール フィルターが不適切なコンテンツを検出した際、このファイルは削除されます。**DocAve コンテンツ シールド for SharePoint へエラーを送信する** – このチェックボックスをオンにすると、DocAve コンテンツ シールド for SharePoint によるリアルタイム フィルター ジョブ中に検知した有害アイテムを一覧で表示させることができます。
- **リスク レポートを有効にする** – このチェックボックスをオンにすると、スキャン済みのリスク情報およびサマリーを含めたリスク レポートを生成することができます。**ファイル内の不適切なタイプの最初のインスタンスのみを表示する** および **ファイル内の不適切なタイプのすべてのインスタンスを表示する** のいずれかを選択します。なお、リスク レポートはスケジュール フィルター時のみ有効です。リスク レポートについてのさらなる情報については、本ユーザーガイド内の リスク レポート セクションをご参照ください。
- **作成者または更新者にメールを送信する (リアルタイム フィルターのみで使用)** – このチェックボックスをオンにすると、コンプライアンスに違反するファイルの作成者および更新者に対し、電子メール通知を送信します。

- **コンテンツ タイプを設定する:** – このチェックボックスをオンにすると、有害ファイルを特定のコンテンツ タイプに変更できます。任意のコンテンツ タイプ名をフィールドに入力してください。
  ***注意:** SharePoint レポート ライブラリでは、このオプションを選択するとコンテンツ タイプが変更されるため、処理後のファイルは既定ビューでは表示されなくなります。（全レポート・ダッシュボード表示モードでは表示されます）
- **次の拡張子をファイル名に追加して識別する** – このチェックボックスをオンにすると、すべての有害ファイルに対し特定の拡張子を追加することができます。追加したい拡張子は **拡張子** フィールドに入力してください。

以下はこれら構成に基づくスケジュール フィルターの動作です:

- **アクション – リスクが次の値と同じかそれ以上である場合、SharePoint から有害なアイテムをブロックします** チェックボックスをオンにしてリスク値を指定した際に、有害コンテンツをブロックするかどうかを指定します。
  ***注意:** スケジュール フィルターでは、ブロックされたコンテンツは SharePoint から削除されます。ブロックしたコンテンツが保存される予定だった移動先には A *_BLOCK.txt* ファイルが作成されます。
  このチェックボックスをオンにすると、以下の構成も必要になります:
  - **コンテンツと次のエラー メッセージを置換する** – このチェックボックスをオンにすると、ブロックしたコンテンツが保存される予定だった移動先にダミー ファイルを作成します。ダミー ファイル内に含める **エラー メッセージ** を構成するか、以下の既定メッセージを使用することもできます:
    ドキュメント内で不適切なコンテンツが見つかりました。
  - **有害なファイルを検疫フォルダーに保存する** – このチェックボックスをオンにすると、ブロックしたファイルを保存する検疫フォルダーを作成します。このライブラリへアップロードする際にブロックされたファイルはすべて検疫フォルダーへ移動します。同じ名前の有害ファイルが複数の検疫ファイルにアップロードされると、各ファイルの名前の末尾に数字が追加されます。例えば複数の *testfile.doc* という名前の有害ファイルが同一フォルダー内に存在する場合、ファイル名は *testfile_0.doc*、*testfile_1.doc*、*testfile_2.doc*… となります。
    有害ファイルを検疫フォルダーへ移動する際、通知する AD ユーザー / AD グループを指定することができます。この機能を有効にするには、あらかじめこのポリシーを使用するフィルターで電子メール プロファイルを構成しておく必要があります。また、ここで指定したユーザーが SharePoint サイトへアクセスする適切な権限をもっていれば、検疫フォルダーへもアクセスすることができます。ユーザーが SharePoint サイトへのアクセス権を持っていない場合は、検疫フォルダーへアクセスすることができません。この機能はスケジュール フィルターのみで使用することができます。

***注意:** 検疫フォルダー内では、 *_BLOCK.txt* という名前のファイルは必ず 1 つのみ存在できます。新規に *_BLOCK.txt* ファイルが作成される場合、古いファイルは削除されます。

***注意: リスクが次の値と同じかそれ以上である場合、SharePoint から有害なアイテムをブロックします** チェックボックスがオンになっている場合、**コンテンツと次のエラー メッセージを置換する** および **有害なファイルを検疫フォルダーに保存する** が選択されていても、有害ファイルは例外なくブロックされます。

- **タグ** – 有害ファイルに対してタグ付けを行うかを選択します。**タグ** チェックボックスをオンにし、**名前** および **説明** フィールドを入力すると、SharePoint 上にタグを示す列が追加されます。 既定の名前は **ブロック**、既定の説明は **このドキュメント内で不適切なコンテンツが見つかりました。** です。

  注意:** エラーメッセージ内にファイル名および有害と判断された理由を表示したい場合、説明欄に ***%file name% および ***%invalid string%*** という形式で含めることでエラーメッセージ内に表示されるようになります。

- **チェックアウトを破棄する** – このオプションはスケジュール フィルターでのみ使用できます。スケジュール フィルターで、このオプションが有効になっているポリシーを使用してスキャン ジョブを実行すると、以下の影響があります。
  - ファイルがチェックアウトされており、かつ最新の未チェックアウト バージョンに不適切なコンテンツが含まれている場合、このファイルのチェックアウトは破棄され、不適切なコンテンツを含む最新バージョンが検疫されます。この場合、チェックアウト バージョンへの変更は無視されます。
  - ファイルがチェックアウトされており、かつ最新の未チェックアウト バージョンには不適切なコンテンツが含まれていない場合、チェックアウト済みバージョンに不適切なコンテンツが含まれていても、アイテムは現在の状態を保持します。このファイルが再度チェックインされた場合、リアルタイム フィルターによって不適切なコンテンツがスキャンされます。他のユーザーは、このファイルのチェックインが完了するまで、不適切なコンテンツへの編集を見ることができません。
  - アップロードされたファイルが自動的にチェックアウトされ、その後スケジュール フィルターが不適切なコンテンツを検出した際、このファイルは削除されます。

- **DocAve コンテンツ シールド for SharePoint へエラーを送信する** – このチェックボックスをオンにすると、DocAve コンテンツ シールド for SharePoint によるスケジュール フィルター ジョブ中に検知した有害アイテムを一覧で表示させることができます。

- **リスク レポートを有効にする** – このチェックボックスをオンにすると、スキャン済みのリスク情報およびサマリーを含めたリスク レポートを生成することができます。**ファイル内の不適切なタイプの最初のインスタンスのみを表示する** および **ファイル内の不適切なタイプのすべてのインスタンスを表示する** のいずれかを選択します。なお、リスク レポートはスケジュール フィルター時のみ有効です。リスク レポートについてのさらなる情報については、本ユーザーガイド内の リスク レポート セクションをご参照ください。

- **作成者または更新者にメールを送信する (リアルタイム フィルターのみで使用)** – このチェックボックスをオンにすると、コンプライアンスに違反するファイルの作成者および更新者に対し、電子メール通知を送信します。
- **コンテンツ タイプを設定する:** – このチェックボックスをオンにすると、有害ファイルを特定のコンテンツ タイプに変更できます。任意のコンテンツ タイプ名をフィールドに入力してください。
  ***注意:** SharePoint レポート ライブラリでは、このオプションを選択するとコンテンツ タイプが変更されるため、処理後のファイルは既定ビューでは表示されなくなります。（全レポート・ダッシュボード表示モードでは表示されます）
- **次の拡張子をファイル名に追加して識別する** – このチェックボックスをオンにすると、すべての有害ファイルに対し特定の拡張子を追加することができます。追加したい拡張子は **拡張子** フィールドに入力してください。

- スキャン設定 – スキャン設定を選択してフィルター ポリシーを最適化します。
  - **禁則文字が 1 つ検出された段階でスキャンを停止する** – このチェックボックスをオンにすると、禁則文字が 1 つでも検出された時点でファイルのスキャン ジョブを停止します。ジョブはここで指定したポリシーに従い、禁則文字が存在したファイルの残りは飛ばして次のファイルへと移ります。このオプションを有効にするとスキャン ジョブにかかる時間を削減できますが、すべての禁則文字を検知することができなくなります。
- **リストア済みファイルを無視する** – このチェックボックスをオンにすると、それ以降のスキャンでリストア済みファイルをすべて無視します。この場合、リストア済みファイルが不適切なコンテンツを含んでいても検疫されなくなります。

コンテンツ シールド ポリシー構成の完了後、**保存** をクリックして編集を保存します。**キャンセル** をクリックすると、変更を保存せずに前の画面に戻ります。作成後にコンテンツ シールド ポリシーを変更するには、コンテンツ シールド ポリシーの表示画面で変更したいポリシー名をクリックします。編集画面で、上記の手順に従って編集を行ってください。

フィルター

フィルター機能では、構成したコンテンツ シールド ポリシーでコンプライアンスに違反するコンテンツをブロックしたり、コンテンツ シールド ポリシー内のアクション設定に従って有害ファイルをタグ付けすることができます。ここでは以下の 2 種類のタイプのフィルターが選択できます:

- リアルタイム フィルター – このフィルター タイプでは、SharePoint 上でアップロード・編集されたファイルをスキャンし、SharePoint 上のコンテンツをここで構成するコンテンツ シールド ポリシーに準拠させることができます。

- スケジュール フィルター – このフィルター タイプでは時間と期間を設定して、既に SharePoint 上に存在するコンテンツに対してオンデマンドのスキャンを実行することができます。スケジュール フィルターではコンテンツ シールド ポリシーに準拠したフィルタリングを実施します。

リアルタイム フィルター

リアルタイム フィルターを使用するには、DocAve コンテンツ シールド for SharePoint のトップ画面の左側ペインから **[リアルタイム フィルター]** に移動します。既に構成済みのリアルタイム フィルターがフィルター リスト セクションに表示されます。リアルタイム フィルターの表示数を変更したい場合、画面右上の **[サイズ]** ドロップダウン メニューから数を指定できます。表示するリアルタイム フィルターの順番を変更する場合は、各列のヘッダーをクリックしてソートすることができます。

リアルタイム フィルターを削除する場合、削除したいアイテムの左側にあるチェックボックスをオンにし、画面右上の **[選択部分を削除]** をクリックします。すべて削除したい場合は、**[すべてを空にする]** をクリックします。

リアルタイム フィルターの新規作成

リアルタイム フィルターを新規作成するには、画面右上の **[新規]** を選択します。リアルタイム フィルターの編集画面が表示されますので、新規に作成したいリアルタイム フィルターについての以下の情報を入力します:

- **URL 検索** – 画面左側より、SharePoint 内でこのフィルターを適用する場所を構成します。適用するサイト・サイト コレクションの URL を入力して検索アイコンを使用するか、ツリーを展開していき対象のチェックボックスをオンにして指定します。
  ***注意:** SharePoint のオブジェクトをクリックし、選択したノード内で新規オブジェクトを含めるかどうかを指定することができます。 右下の小さな黄色い三角アイコンは、新規オブジェクトを含むことを示しています。
- ***コンテンツ シールド ポリシー** – リアルタイム フィルターで使用するコンテンツ シールド ポリシーを選択します。
- **電子メール プロファイル** – リアルタイム フィルターで使用する電子メール プロファイルを選択します。

リアルタイム フィルター構成の完了後、**フィルターの追加** をクリックして編集を保存します。作成後にリアルタイム フィルターを変更するには、リアルタイム フィルターの [フィルター リスト] セクションの [マッピング コンテンツ] 列からアイテムを選択します。編集画面で、上記の手順に従って編集を行ってください。

***注意:** 新規のフィルターを作成する際、対象のノードを選択してください。選択したノードが既に他のフィルターによって選択されていた場合、以下のメッセージが表示されます:
“この Web アプリケーションのいくつかのノードには既にコンテンツ シールド ポリシーが適用されています。これらのポリシーを無効にしますか?”

OK をクリックして、選択したノードに新規フィルターを適用します。この段階でこのノードに関連付けられていた既存フィルターは接続が解除されます。**キャンセル** をクリックすると、作成した新規フィルターと選択したノードの接続を解除します。この場合、既存フィルターとノードとの関連が保持されます。

リアルタイム フィルターの使用

***注意:** リアルタイム フィルターを適用・使用する前に、画面右下にある **フィルター ポリシーを有効にする** ボタンをクリックしてください。すべてのフィルターを有効に設定している場合新規のフィルターも自動的に有効化されますので、使用する際は適用処理のみを行ってください。

リアルタイム フィルターは、作成しても適用処理を行うまでは使用できません。適用するには、リアルタイム フィルター画面のフィルター リスト セクションから対象のノードを選択し、画面右下の **すぐに実行** をクリックします。リアルタイム フィルターを自動的に適用するには、画面右ペイン内の **スケジュール** タブをクリックし、以下の手順に従ってください:

1. **スケジュールを有効にする** チェックボックスをオンにし、適用するリアルタイム フィルターのスケジュール構成を有効にします。
2. リアルタイム フィルターを適用する **開始時間** を決定し、カレンダー アイコンから日時を指定します。ドロップダウン メニューから時、分を指定します。
3. **間隔**セクションでは、既定では **1 回のみ** が選択されています。 はじめの適用の後にもリアルタイム フィルターを適用したい場合、ここを構成してください。適用ジョブを繰り返し行いたい場合は、フィールドに数値を入力し、繰り返す時間の単位をドロップダウン メニューから選択します。
4. **スケジュールの更新** をクリックして、スケジュールを保存します。

リアルタイム フィルター機能により有害ファイルを検知した際に通知メールが大量に送信されることを防ぐため、メール通知のスケジュールを設定することも可能です。スケジュールを元に送信されるメール通知は、前回のメール通知以降のジョブ レポートがすべて含まれます。メール通知のスケジュールについては、画面右ペインの **メール設定** タブをクリックし、以下の手順に従ってください:

1. **メール スケジュールを有効にする** チェックボックスをオンにし、電子メールの構成を有効にします。
2. カレンダーをクリックして、通知メールの受信を開始したい **開始時刻** を指定します。ドロップダウン メニューから時、分を指定します。
3. **間隔** フィールドを構成します。適用ジョブを繰り返し行いたい場合は、フィールドに数値を入力し、繰り返す時間の単位をドロップダウン メニューから選択します。
4. **スケジュールの更新** をクリックして、スケジュールを保存します。

リアルタイム フィルターの有効化・無効化

DocAve プラットフォーム バックアップを使用して、プラットフォーム全体のバックアップの取得や DocAve コンテンツ マネージャーを使用して SharePoint 環境の全体的な再構築を行うなど大規模なバックアップ ジョブを実行する際は、リソース確保のためリアルタイム フィルター機能を無効化した方が効率的な場合があります。

すべてのリアルタイム フィルターを無効にするには、画面右下の **フィルター ポリシーを無効にする** をクリックします。 この操作ではスキャン機能も同時に無効化されます。**フィルター ポリシーを有効にする** をクリックすると、すべてのフィルターが有効化されます。ただし、**フィルター ポリシーを有効にする** をクリックするのみではスキャン機能は再有効化されません。特定のリアルタイム フィルター上でスキャン機能を再有効化したい場合、対象のリアルタイム フィルターを選択して、画面右下の **すぐに実行** をクリックします。

スケジュール フィルター

スケジュール フィルターを使用するには、DocAve コンテンツ シールド for SharePoint のトップ画面の左側ペインから **[スケジュール フィルター]** に移動します。既に構成済みのリアルタイム フィルターがプラン一覧セクションに表示されます。スケジュール フィルターの表示数を変更したい場合、プラン一覧セクション右上の **[サイズ]** ドロップダウン メニューから数を指定できます。表示するスケジュール フィルターの順番を変更する場合は、各列のヘッダーをクリックしてソートすることができます。

スケジュール フィルターを削除する場合、削除したいアイテムの左側にあるチェックボックスをオンにし、画面右上の **[選択部分を削除]** をクリックします。すべて削除したい場合は、**[すべてを空にする]** をクリックします。

スケジュール フィルターの新規作成

スケジュール フィルターを新規作成するには、プラン一覧セクション右上の **[新規]** を選択します。プランの編集画面が表示され、新規に作成したいスケジュール フィルターについての以下の情報を入力します:

- **URL 検索** – 画面左側より、SharePoint 内でこのフィルターを適用する場所を構成します。適用するサイト・サイト コレクションの URL を入力して検索アイコンを使用するか、ツリーを展開していき対象のチェックボックスをオンにして指定します。
- **完全スケジュール** – **完全スケジュールを有効にする** チェックボックスをオンにすると、**URL 検索** で指定した場所内の全てのコンテンツに対してスキャンを実行します。カレンダーをクリックして、スキャンを開始したい **開始時刻** を指定します。ドロップダウン メニューから時、分を指定します。**説明** を入力することもできますが、必須ではありません。

- **増分スケジュール** – 前回のジョブ以降に追加・修正されたコンテンツに対して実行するスキャン ジョブのスケジュールを指定します。**完全スケジュールを有効にする** チェックボックスを有効にし、スケジュールを構成します。カレンダーをクリックして、スキャンを開始したい **開始時刻** を指定します。ドロップダウン メニューから時、分を指定します。はじめの適用の後にもリアルタイム フィルターを適用したい場合、**間隔**セクションを構成してください。フィールドに数値を入力し、繰り返す時間の単位をドロップダウン メニューから選択します。
- ***コンテンツ シールド ポリシー** – リアルタイム フィルターで使用するコンテンツ シールド ポリシーを選択します。
- **電子メール プロファイル** – リアルタイム フィルターで使用する電子メール プロファイルを選択します。
- **高速スキャンには SharePoint の検索インデックス データを使用する** – このチェックボックスをオンにすると、フィルタリング ジョブを高速化できます。フィルター定義ファイルで複雑なキーワードを構成したり、大量のキーワードやコンテンツを登録すると、CPU 使用率が 100% に近くなってしまいます。設定によってはコンテンツ シールドのデータ読み込み作業が頻繁に発生するため、システム内リソースを圧迫する可能性があります。このオプションを有効にすることで、スケジュール フィルターを SharePoint 検索インデックスを通して実行するため、この問題を防ぐことができます。

  ***注意:** この機能を使用するためには、事前に SharePoint 検索インデックスを作成しておく必要があります。

スケジュール フィルター構成の完了後、**プランの保存** をクリックして編集を保存します。作成後にスケジュール フィルターを変更するには、プラン一覧セクションからプラン名を選択します。編集画面で、上記の手順に従って編集を行ってください。

***注意:** 新規のフィルターを作成する際、対象のノードを選択してください。選択したノードが既に他のフィルターによって選択されていた場合、以下のメッセージが表示されます:
"この Web アプリケーションのいくつかのノードには既にコンテンツ シールド ポリシーが適用されています。これらのポリシーを無効にしますか?"
OK をクリックして、選択したノードに新規フィルターを適用します。この段階でこのノードに関連付けられていた既存フィルターは接続が解除されます。**キャンセル** をクリックすると、作成した新規フィルターと選択したノードの接続を解除します。この場合、既存フィルターとノードとの関連が保持されます。

スケジュール フィルターの使用

スケジュール フィルターは、作成しても開始時間を構成するまではスキャン機能を開始できません。すぐにスキャン機能を使用する場合は、プラン一覧セクションから対象のプラン名を選択し、画面右側の **すぐに実行** をクリックします。

レポート

DocAve コンテンツ シールドのフィルター ジョブが実行されるたびにレポートが生成されます。ジョブ レポートを確認するには、DocAve コンテンツ シールド for SharePoint のトップ画面の左側ペインから **[レポート]** に移動します。ジョブ レポートには以下の 3 種類があります:

- スケジュール フィルター ジョブ レポート – スケジュール フィルターのスキャン ジョブについての情報を含みます。
- リアルタイム フィルター コンテンツ レポート – リアルタイム フィルターで検知した有害ファイルの情報を含みます。
- リアルタイム フィルター ジョブ レポート – リアルタイム フィルターのスキャン ジョブについての情報を含みます。

コンテンツ フィルター レポート タイプを選択 ドロップダウン メニューから表示したいレポートを選択します。現在実行中、および過去に実行したジョブが一覧に表示されます。ジョブの表示数を変更したい場合、ジョブ一覧セクション右上の **[サイズ]** ドロップダウン メニューから数を指定できます。表示するジョブの順番を変更する場合は、各列のヘッダーをクリックしてソートすることができます。

各種フィルター ジョブのボタンをリボン上でクリックして、以下の指定アクションを実行することができます。

スケジュール フィルター ジョブ レポート

マウス カーソルをジョブ ID に移動して、下向き矢印をクリックします。以下のアクション一覧が表示されます:

- **ジョブ統計** - ジョブ ID、プラン名、実行中のアイテム、実行中のファイル、排除ファイルなどのジョブ詳細情報を表示します。
- **レポートの表示** - コンテンツ フィルター レポート ページに移動して、不適切なコンテンツを含むファイルおよびアイテムの一覧を表示します。
- **プラン詳細の表示** - スケジュール フィルター ページに移動して、選択したジョブのフィルター プランを表示します。
- **リスク レポートの表示** - 選択したスケジュール フィルター ジョブのリスク レポートを表示します。リスク レポートの詳細については、リスク レポートをご参照ください。
- **ダウンロード** - スケジュール フィルター ジョブ一覧に表示されている列をすべて含むスケジュール フィルター ジョブ レポートをダウンロードすることができます。
- **ジョブの削除** - スケジュール フィルター ジョブ レポートをスケジュール フィルター ジョブ一覧から削除することができます。

スケジュール フィルター ジョブ一覧の右上からは、以下のアクションを実行することができます:

- **選択したジョブをダウンロード** - 選択したフィルター ジョブのスケジュール フィルター ジョブ レポートを .csv ファイルとしてダウンロードすることができます。

- **すべてのジョブをダウンロード** - すべてのスケジュール フィルター ジョブのレポートを .csv ファイルとしてダウンロードすることができます。
- **選択部分を削除** - 選択したスケジュール フィルター ジョブ レポートをスケジュール フィルター ジョブ一覧から削除することができます。
- **すべて削除** - すべてのスケジュール フィルター ジョブ レポートをスケジュール フィルター ジョブ一覧から削除することができます。

リアルタイム フィルター コンテンツ レポート

マウス カーソルをアイテム名に移動して、下向き矢印をクリックします。以下のアクション一覧が表示されます:

- **アイテムの削除** - 不適切なコンテンツを含むアイテム / ファイルのリアルタイム フィルター コンテンツ レポートを削除することができます。
- **ダウンロード** - リアルタイム フィルター コンテンツ一覧に表示されているすべての列を含むリアルタイム フィルター コンテンツ レポートをダウンロードすることができます。

リアルタイム フィルター コンテンツ一覧の右上で次のアクションを実行することができます。

- **選択したジョブをダウンロード** - 選択した不適切なコンテンツを含むアイテム / ファイルのリアルタイム フィルター コンテンツ レポートをダウンロードすることができます。
- **すべてのジョブのダウンロード** - すべての不適切なコンテンツを含むアイテム / ファイルのリアルタイム フィルター コンテンツ レポートを .csv ファイルとしてダウンロードすることができます。
- **選択部分を削除** - 選択した不適切なコンテンツを含むアイテム / ファイルをリアルタイム ファイルター コンテンツ一覧から削除することができます。
- **すべて削除** - すべての不適切なコンテンツを含むアイテム / ファイルをリアルタイム フィルター コンテンツ一覧から削除することができます。

リアルタイム フィルター ジョブ レポート

マウス カーソルをジョブ ID に移動して、下向き矢印をクリックします。以下のアクション一覧が表示されます:

- **ジョブの削除** - リアルタイム フィルター ジョブ レポートをリアルタイム フィルター ジョブ一覧から削除することができます。
- **ダウンロード** - リアルタイム フィルター ジョブ一覧に表示されているすべての列を含むリアルタイム フィルター ジョブ レポートをダウンロードすることができます。

リアルタイム フィルター ジョブ一覧の右上で次のアクションを実行することができます。

- **選択したジョブをダウンロード** - 選択したフィルター ジョブのリアルタイム フィルター ジョブ レポートを .csv ファイルとしてダウンロードすることができます。
- **すべてのジョブをダウンロード** -すべてのリアルタイム フィルター ジョブのレポートを .csv ファイルとしてダウンロードすることができます。
- **選択部分を削除** -選択したリアルタイム フィルター ジョブをリアルタイム フィルター ジョブ一覧から削除することができます。
- **すべて削除** -すべてのリアルタイム フィルター ジョブ レポートをリアルタイム フィルター ジョブ一覧から削除することができます。

リスク レポート

スケジュール フィルターのジョブ レポートで表示できるスキャン ジョブ全体のレポートとは別に、スケジュール フィルター ジョブで検知した特定の有害ファイルについてのリスク レポートを生成することもできます。

スケジュール フィルター ジョブのリスク レポートを表示するには、レポート画面の **コンテンツ フィルター レポート タイプを選択** ドロップダウン メニューから **スケジュール フィルター ジョブ レポート** を選択します。リスク レポートを表示したいスケジュール フィルター ジョブの上にカーソルを合わせ、ジョブ ID で表示される矢印から **リスク レポートの表示** を選択します。リスク レポートについての更なる情報は 付録 B をご参照ください。

ファイルのリストア・削除

検疫済みファイルは、サイトの管理者もしくはコンテンツ シールド ポリシーで指定した AD ユーザー / AD グループ内のユーザーにより、リストア / 削除することができます。AD ユーザー / AD グループ内のユーザーが投稿 (リスト アイテムおよびドキュメントを表示、追加、更新、削除することが可能) 以上の権限を持つ場合、検疫済みファイルをリストア / 削除することができます。検疫済みファイルをリストア / 削除するには、次の手順を完了してください:

1. 検疫済みアイテムが存在する SharePoint サイトに移動します。
2. **サイトの操作** > **サイトの設定** > **AvePoint ツールとサービス** > **DocAve コンテンツ シールド for SharePoint リストア コントローラ** へ移動します。
3. 画面左側でサイト コレクション URL をクリックしてツリーを展開します。検疫済みアイテムの場所まで展開していきます。
   ***注意:** 画面左側でのツリー展開はサイトの管理者、指定の AD ユーザー、指定の AD グループ内のユーザーのみ実行可能です。

4. 該当のチェックボックスをオンにしてリストを選択します。URL 検索機能を使用して、サイト URL で対象のサイトを検索することもできます。選択したリスト内の検疫済みアイテムが画面右側に表示されます。一覧には各検疫済みアイテムの次の情報が含まれています: タイプ、名前、元の場所、更新日時、更新者
5. 該当のチェックボックスをオンにして、リストアまたは削除する検疫済みアイテムを選択します。
6. 次のオプションを選択します:
    a. [コンテンツの表示] をクリックして検疫済みアイテムを表示し、アイテムが存在する検疫フォルダーに移動します。
    b. [ファイルをリストア] をクリックして、選択した検疫済みアイテムをリストアします。ポップアップ ウィンドウが表示されると、次のリストア オプション (追加する、上書きする、上書きしない) から 1 つを選択します。[デジタル署名を入力する] チェックボックスをオンにして、このファイルをメタデータとしてマークするかどうかを選択します。署名の入力が終わったら、[OK] をクリックしてリストアを開始します。
    c. [選択部分を削除] をクリックして選択した検疫済みアイテムを削除するか、[すべて削除] をクリックして検疫済みアイテムをすべて削除します。
7. 各ジョブの完了後 **[レポートの表示]** をクリックして、ジョブレポートを表示することができます。
8. 検疫済みアイテムの表示数を変更したい場合、ジョブ一覧セクション右上の **[サイズ]** ドロップダウン メニューから数を指定できます。

検疫済みのファイルと同一のライブラリ内に同一の名前で新しいファイルがアップロードされた場合、このライブラリ内で検疫済みファイルをリストアする際に以下のアクションを選択できます:

- **上書きする** – ライブラリ内のファイルがリストアされた検疫済みファイルに置き換わります。
- **追加する** –リストアされる検疫済みファイル名の末尾に数字が追加されます。例えば検疫済みファイルと新しくアップロードされたファイルが同じ TestFile.docx という名前で同一フォルダー内に存在する場合、検疫済みファイルがリストアされると TestFile_1.docx という名前になります。
- **上書きしない** – リストア ジョブを中止します。リストア レポートにはジョブ中止の理由が含まれます。

***注意:** いずれのオプションを選択した場合でも、_BLOCK.txt ファイルはリストア ジョブ後に削除されます。

付録 A

HIPAA (医療保険の相互運用性と説明責任に関する法律) 対応定義ファイル

DocAve コンテンツ シールド for SharePoint では、米国 HIPAA に対応した 14 の既存フィルター定義ファイルが設定されています。これらには SharePoint へアップロードするべきでない個人情報および経営情報が登録されています。また各ファイルごとにリスク値が設定されており、指定値を超えるような状況に対しても対応できます。必要に応じて既存定義ファイルの編集、および新規定義ファイルの作成も可能です。

ビジネス定義ファイル

ビジネス定義ファイルでは情報保護および企業秘密の観点から、経営情報に関連するコンテンツが SharePoint にアップロードされるのを防ぐための既存キーワードが登録されています。

リスク値 – 1

キーワード – NDA, Non-Disclosure Agreement

クレジットカード番号定義ファイル

クレジットカード番号定義ファイルでは個人情報の SharePoint アップロードを防ぐため、クレジットカード番号に対応した一般的な表現が予め登録されています。ここでは、次のクレジットカードがサポートされています: ビザ、マスターカード、ディスカバーカード、アメリカン・エクスプレス

リスク値 – 5

既定の一般表現 – (?<=^|¥b)(((34|37)¥d{2}[¥-]?¥d{6}[¥-]?¥d{5})|((4¥d{3}|5[1-4]¥d{2}|6011)[¥-]?¥d{4}[¥-]?¥d{4}[¥-]?¥d{4}))(?=$|¥b)

既定一般的な表現はビザ、マスターカード、ディスカバーカード、アメリカン ・ エクスプレスなどのクレジットカード番号ルールに従う番号文字列のみを検索します。

代替の般表現 – (?<=^|¥b)(?:¥d[-]*?){13,16}(?=$|¥b)

代替の一般表現では、13 もしくは 16 桁の番号文字列を検索します。この番号は有効なクレジットカード番号ではない可能性があります。

日付定義ファイル

日付定義ファイルでは、SharePoint 上にアップロードすべきでない日付に対応する一般的な表現が登録されています。

リスク値– 5

一般的な表現– (?<=^|[^¥d])(¥d{4})¥-((((0?[13578])|(1[02]))¥-(([1-2][0-9])|(3[01])|(0?[1-9])))|(((0?[469])|(11))¥-(([1-2][0-9])|(30)|(0?[1-9])))|(0?2¥-(([1-2][0-9])|(0?[1-9]))))(?=$|[^¥d])

(?<=^|[^¥d])(¥d{4})¥.((((0?[13578])|(1[02]))¥.(([1-2][0-9])|(3[01])|(0?[1-9])))|(((0?[469])|(11))¥.(([1-2][0-9])|(30)|(0?[1-9])))|(0?2¥.(([1-2][0-9])|(0?[1-9]))))(?=$|[^¥d])

(?<=^|[^¥d])(¥d{4})¥/((((0?[13578])|(1[02]))¥/(([1-2][0-9])|(3[01])|(0?[1-9])))|(((0?[469])|(11))¥/(([1-2][0-9])|(30)|(0?[1-9])))|(0?2¥/(([1-2][0-9])|(0?[1-9]))))(?=$|[^¥d])

(?<=^|[^¥d])((((0?[13578])|(1[02]))¥-(((0?[1-9])|([1-2][0-9]))|(3[01])))|(((0?[469])|(11))¥-(((0?[1-9])|([1-2][0-9]))|(30)))|(0?2¥-((0?[1-9])|([1-2][0-9]))))¥-(¥d{4})(?=$|[^¥d])

(?<=^|[^¥d])((((0?[13578])|(1[02]))¥/(((0?[1-9])|([1-2][0-9]))|(3[01])))|(((0?[469])|(11))¥/(((0?[1-9])|([1-2][0-9]))|(30)))|(0?2¥/((0?[1-9])|([1-2][0-9]))))¥/(¥d{4})(?=$|[^¥d])

(?<=^|[^¥d])(((((0?[1-9])|([1-2][0-9]))|(3[01]))¥-((0?[13578])|(1[02])))|((((0?[1-9])|([1-2][0-9]))|(30))¥-((0?[469])|(11)))|(((0?[1-9])|([1-2][0-9]))¥-0?2))¥-(¥d{4})(?=$|[^¥d])

(?<=^|[^¥d])(((((0?[1-9])|([1-2][0-9]))|(3[01]))¥/((0?[13578])|(1[02])))|((((0?[1-9])|([1-2][0-9]))|(30))¥/((0?[469])|(11)))|(((0?[1-9])|([1-2][0-9]))¥/0?2))¥/(¥d{4})(?=$|[^¥d])

(?<=^|[^¥d¥w])((((Jan|January)|(Mar|March)|May|(Jul|July)|(Aug|August)|(Oct|October)|(Dec|December))¥s+(([0-2]?((1(st)?)|(2(nd)?)|(3(rd)?)|([0456789](th)?)))|((30(th)?)|(31(st)?))))|(((Apr|April)|(Jun|June)|(Sep|September)|(Nov|November))¥s+(([0-2]?((1(st)?)|(2(nd)?)|(3(rd)?)|([0456789](th)?)))|(30(th)?)))|((Feb|February)¥s+[0-2]?((1(st)?)|(2(nd)?)|(3(rd)?)|([0456789](th)?))))¥s*[¥,]¥s*(¥d{4})(?=$|[^¥d])

(?<=^|[^¥d¥w])((((([0-2]?((1(st)?)|(2(nd)?)|(3(rd)?)|([0456789](th)?)))|((30(th)?)|(31(st)?)))¥s+((Jan|January)|(Mar|March)|May|(Jul|July)|(Aug|August)|(Oct|October)|(Dec|December)))|((([0-2]?((1(st)?)|(2(nd)?)|(3(rd)?)|([0456789](th)?)))|(30(th)?))¥s+((Apr|April)|(Jun|June)|(Sep|September)|(Nov|November)))|([0-2]?((1(st)?)|(2(nd)?)|(3(rd)?)|([0456789](th)?))¥s+(Feb|February)))¥s*[¥,]¥s*(¥d{4})(?=$|[^¥d])

例 – Jan 1st, 2012

電子メール アドレス定義ファイル

電子メール アドレス定義ファイルでは個人情報の保護および経営情報守秘の観点から、SharePoint 上にアップロードすべきでないメールアドレスに対応した一般的な表現が登録されています。

リスク値 – 1

一般的な表現 – (?<=^|¥b)[a-zA-Z0-9!#$%*+/=?^_`{|}~-]+(?:¥.[a-zA-Z0-9!#$%*+/=?^_`{|}~-]+)*@(?:[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?¥.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?(?=$|¥b)

例 – accountname@hotmail.com

ファックス番号定義ファイル

ファックス番号定義ファイルでは、SharePoint 上にアップロードすべきでないファックス番号に対応した一般的な表現が登録されています。

リスク値 – 2

一般的な表現 – (?<=^|¥b)([¥(¥+])?([0-9]{1,3}([¥s])?)?([¥+|¥(|¥-|¥)|¥s])?([0-9]{2,4})([¥-|¥)|¥.|¥s]([¥s])?)?([0-9]{2,4})?([¥.|¥-|¥s])?([0-9]{4,8})(?=$|¥b)

例 – (089)1234-5678

一般定義ファイル

一般定義ファイルでは、SharePoint 上にアップロードすべきでない重要情報に対応した一般的な表現が登録されています。

リスク値 – 1

キーワード – Do not distribute, Do not copy, Do not print, Do not scan, Do not photocopy, Restricted, Sensitive Information, For Official Use Only, No Carbon Copy

行政定義ファイル

行政定義ファイルでは、SharePoint 上にアップロードすべきでない行政関連の機密情報に対応した定義済みキーワードが登録されています。

リスク値 – 1

キーワード – Top Secret, Confidential, Redact, Redacted, Eyes Only

福祉厚生定義ファイル

福祉厚生定義ファイルでは、SharePoint にアップロードすべきでない健康・保険に関する情報に対応した定義済みキーワードが登録されています。

リスク値 – 1

キーワード – Confidentiality, Patient Confidentiality, HIV, Human Immune Virus, AIDS, Auto Immune Deficiency Syndrome, Hepatitis, Abortion, Drug Dependence, Alcohol Dependence

IP アドレス定義ファイル

IP アドレス定義ファイルでは、SharePoint 上にアップロードすべきでない IP アドレスに対応する一般的な表現が登録されています。

リスク値 – 1

一般的な表現 – (?<=^|¥b)(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)¥.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)¥.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)¥.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)(?=$|¥b)

例 – 210.202.118.123

社会保障番号定義ファイル

社会保障番号定義ファイルでは、SharePoint 上にアップロードすべきでない米国社会保障番号に対応する一般的な表現が登録されています。

リスク値 – 5

一般的な表現 – (?<=^|[^¥w¥d])(00[1-9]|0[1-9]0|0[1-9][1-9]|[1-6]¥d{2}|7[0-6]¥d|77[0-2])(-?|[¥.])([1-9]0|0[1-9]|[1-9][1-9])(-?|[¥.])(¥d{3}[1-9]|[1-9]¥d{3}|¥d[1-9]¥d{2}|¥d{2}[1-9]¥d)(?=$|[^¥w¥d])

例 – 618-89-9988

URL 定義ファイル

URL 定義ファイルでは、SharePoint 上にアップロードすべきでない URL に対応する一般的な表現が登録されています。

リスク値 – 1

一般的な表現 – (?<=^|¥b)(ht|f)tps?://([-¥w¥.]+)+(:[¥d¥w]+)?([¥@][¥d¥w]+)?(/([¥w/_¥.¥-]*(¥?¥S+)?)?)?(?=$|¥b)

例 – http://www.avepoint.com

米国住所定義ファイル

米国住所定義ファイルでは、SharePoint 上にアップロードすべきでないアメリカ合衆国内の住所に対応する一般的な表現が登録されています。

リスク値 – 1

一般的な表現 – (?<=^|¥b)(?n:((¥d{1,5}(¥ 1¥/[234])?(¥x20[A-Z]([a-z])+)+)|(P¥.O¥.¥ Box¥¥d{1,5}))¥s{1,2}(?i:((((APT|BLDG|DEPT|FL|HNGR|LOT|PIER|RM|S(LIP|PC|T(E|OP))|TRLR|UNIT)¥x20¥w{1,5})|(BSMT|FRNT|LBBY|LOWR|OFC|PH|REAR|SIDE|UPPR)¥.?)¥s{1,2})?)([A-Z]([a-z])+(¥.?)(¥x20[A-Z]([a-z])+){0,2})¥,¥x20(A[LKSZRAP]|C[AOT]|D[EC]|F[LM]|G[AU]|HI|I[ADLN]|K[SY]|LA|M[ADEHINOPST]|N[CDEHJMVY]|O[HKR]|P[ARW]|RI|S[CD]|T[NX]|UT|V[AIT]|W[AIVY])¥x20((?!0{5})¥d{5}(-¥d{4})?))(?=$|¥b)

例 – 123 Park Ave Apt 123 New York City, NY 10002

米国電話番号定義ファイル

米国電話番号定義ファイルでは、SharePoint 上にアップロードすべきでないアメリカ合衆国内の電話番号に対応する一般的な表現が登録されています。

リスク値 – 3

一般的な表現 – (?<=^|¥b)(?:(?:¥+?1¥s*(?:[.-]¥s*)?)?(?:¥(¥s*([2-9]1[02-9]|[2-9][02-8]1|[2-9][02-8][02-9])¥s*¥)|([2-9]1[02-9]|[2-9][02-8]1|[2-9][02-8][02-9]))¥s*(?:[.-]¥s*)?)?([2-9]1[02-9]|[2-9][02-9]1|[2-9][02-9]{2})¥s*(?:[.-]¥s*)?([0-9]{4})(?:¥s*(?:#|x¥.?|ext¥.?|extension)¥s*(¥d+))?(?=$|¥b)
(?<=^|¥b)(?:¥+?1¥s*(?:[.-]¥s*)?)?(?:¥(¥s*([2-9]1[02-9]|[2-9][02-8]1|[2-9][02-8][02-9])¥s*¥)|([2-9]1[02-9]|[2-9][02-8]1|[2-9][02-8][02-9]))¥s*(?:[.-]¥s*)?([2-9a-z]1[02-9a-z]|[2-9a-z][02-9a-z]1|[2-9a-z][02-9a-z]{2})([0-9a-z]{4})(?=$|¥b)
(?<=^|¥b)(?:¥+?1¥s*(?:[.-]¥s*)?)?(?:¥(¥s*([2-9]1[02-9]|[2-9][02-8]1|[2-9][02-8][02-9])¥s*¥)|([2-9]1[02-9]|[2-9][02-8]1|[2-9][02-8][02-9]))¥s*(?:[.-]¥s*)?([2-9a-z]1[02-9a-z]|[2-9a-z][02-9a-z]1|[2-9a-z][02-9a-z]{2})([0-9a-z]{4})([0-9a-z]*)(?=$|¥b)

例 – +1-(212)-800-5353

車両識別番号定義ファイル

車両識別番号とは、自動車産業界ですべての車両に個別に付与される、一意のシリアルナンバーです。

車両識別番号定義ファイルでは、全世界の車両識別番号に対応する一般的な表現が登録されています。

リスク値 – 3

一般的な表現 – (?<=^|[^¥w¥d])([A-HJ-NPR-Z0-9]{3})[A-HJ-NPR-Z]{2}¥d{2}([A-HJ-NPR-Z]|¥d)(¥d|X)[A-HJ-NPR-Z¥d]{2}¥d{6}(?=$|[^¥w¥d])

例 – 1G1BL52P7TR115520

付録 B

ドキュメント リスク

以下のドキュメント リスク ワークシートでは、定義ファイルに抵触する有害ファイルの一覧を示します。

名前	説明
ドキュメント名	コンプライアンスに違反するファイルの名前です。
GUID	ファイルの GUID です。
URL	違反ファイルが存在する SharePoint 内 URL です。
最終スキャン日付	最後にスキャンを実行した日時です。
作成日時	ファイルを作成した日時です。
作成者	ファイルを作成したユーザーです。
最終更新者	最後に変更したユーザーです。
最終更新日付	最後に変更した日時です。
トリガー ルール	有害と認識した定義ファイルです。
トリガー数	特定の定義ファイルで有害と認識した回数です。
合計リスク	有害ファイルのリスク値の合計です。
合計禁則文字	禁則文字の合計数です。
不適切なストリング	有害ストリングです。
初めて検出した場所	有害ファイルが特定された場所です。 ***注意**: この列は、コンテンツ シールド ポリシー内で **ファイル内の不適切なタイプの最初のインスタンスのみを表示する** オプションが選択されている時のみ有効です。
検出したすべての場所	有害ファイルが特定されたすべての場所です。 ***注意**: この列は、コンテンツ シールド ポリシー内で **ファイル内の不適切なタイプのすべてのインスタンスを表示する** オプションが選択されている時のみ有効です。

リスク サマリー

リスク サマリー ワークシートでは、コンテナ レベルでのリスク情報を示します。

名前	説明
レベル	コンテナ レベルです。コンテナ レベルにはサイト コレクション レベル、サイト レベル、リスト / ライブラリ レベルを含みます。
名前	コンテナ レベルの名前もしくはタイトルです。
URL	コンテナ レベルの URL です。
トリガー ルール	有害と認識した定義ファイルです。
トリガー数	特定の定義ファイルで有害と認識した回数です。
リスク	全コンポーネントを含む コンテナ レベルのリスク値の合計です。
最終更新日付	最後に変更した日時です。
最終スキャン日付	最後にスキャンを実行した日時です。

付録 C

以下の表は DocAve コンテンツ シールド for SharePoint で検知できるファイル タイプの一覧です。

ファイル タイプ	拡張子	ヘッダー	コンテンツ
.xls	サポートされている	サポートされている	サポートされている
.xlsx	サポートされている	サポートされている	サポートされている
.xml	サポートされている	サポートされていない	サポートされている
.pptx	サポートされている	サポートされている	サポートされている
.ppt	サポートされている	サポートされている	サポートされている
.log	サポートされている	サポートされていない	サポートされている
.html	サポートされている	サポートされていない	サポートされている
.ini	サポートされている	サポートされていない	サポートされている
.rtf	サポートされている	サポートされている	サポートされている
.docx	サポートされている	サポートされている	サポートされている
.doc	サポートされている	サポートされている	サポートされている
.txt	サポートされている	サポートされていない	サポートされている
.zip	サポートされている	サポートされている	サポートされている
.pdf	サポートされている	サポートされている	サポートされていない (iFilter パックのインストール前)
			サポートされている (iFilter パックのインストール後)
.lic	サポートされている	サポートされていない	サポートされていない
.rar	サポートされている	サポートされている	サポートされていない
.mht	サポートされている	サポートされていない	サポートされている

.msg	サポートされている	サポートされていない	サポートされている
.dot	サポートされている	サポートされている	サポートされている
.dotx	サポートされている	サポートされている	サポートされている
.jpg	サポートされている	サポートされている	サポートされていない
.png	サポートされている	サポートされている	サポートされていない
.avi	サポートされている	サポートされている	サポートされていない
.gif	サポートされている	サポートされている	サポートされていない
.tif	サポートされている	サポートされている	サポートされていない
.mp3	サポートされている	サポートされている	サポートされていない
.wma	サポートされている	サポートされている	サポートされていない
.rmvb	サポートされている	サポートされている	サポートされていない
.wmv	サポートされている	サポートされている	サポートされていない
.rm	サポートされている	サポートされている	サポートされていない
.bmp	サポートされている	サポートされている	サポートされていない

***注意**: 上の表には iFilter パックのインストールによってサポートの有無が変わるファイル タイプが含まれています。ファイル タイプによっては、iFilter パックの有無によって有害ファイルと認識されるものもあります。

注意

本発行物に記載された内容は AvePoint Japan 株式会社に帰属し、その所有権は AvePoint および実施権許諾者にあるものとします。当該内容は著作権、商標登録、その他知的財産の所有に関わる法律によって保護されており、本発行物上に記載されたこれらの記述はいかなる場合においても削除・変更を禁じます。

著作権

© 2012 AvePoint Japan K.K. All rights reserved.
著作権は、AvePoint Japan 株式会社に帰属します。本書に掲載 されている情報の無断複製 ・ 転載を禁じます。
本書のいかなる部分も、いかなる書式および電子通信、機械的送信、複写、記録などのいかなる方法、あるいは AvePoint Japan 株式会社 (〒 108-0075 東京都港区港南 2 丁目 4-15 品川サンケイ ビル 2 階) による事前の文書による許諾なしに複製、保存、送信を禁じます。

登録商標

AvePoint、 DocAveおよびAvePointロゴはAvePoint Japan 株式会社の商標です。
Microsoft、MS-DOS、InternetExplorer、Microsoft Office SharePoint Servers 2007/2010、SharePoint Portal Server 2003、Windows SharePoint Services、Windows SQL server、および Windows はマイクロソフト株式会社の商標または登録商標です。
Adobe Acrobat、および Acrobat Reader はAdobe Systems, Incの商標です。
その他記載の会社名および製品名は、各社の商標または登録商標です。

変更

当社では最新、そして正確な情報を提供するよう努力しておりますが、あらゆるコンテンツの誤りもしくは脱落に起因する間接的、派生的に生じた損害に対し、一切の責任を負わないものとします。当社は、ユーザーに対し予告、通知をすることなく記載内容を変更する権利を所有しています。

AvePoint Japan 株式会社
〒 108-0075 東京都港区港南 2 丁目 4-15
品川サンケイビル 2 階