機密データの漏洩防止

この章で説明する内容は、次のとおりです。

機密データの漏洩防止の概要

Web セキュリティアプライアンス は以下の機能によってデータの安全を確保します。

オプション	説明
Cisco データ セキュリティ フィルタ	Web セキュリティアプライアンス の Cisco データ セキュリティ フィルタは、HTTP、HTTPS、FTP を介してネットワークから発信されるデータを評価します。
サードパーティ製データ漏洩防止（DLP）の統合	Web セキュリティアプライアンス は、機密データを識別して保護する代表的なサードパーティ製コンテンツ対応 DLP システムを統合します。Web プロキシは Internet Content Adaptation Protocol（ICAP）を使用して、プロキシ サーバーが外部システムにコンテンツ スキャンをオフロードできるようにします。

アップロード要求を受信すると、Web プロキシは要求をデータ セキュリティ ポリシー グループや外部 DLP ポリシー グループと比較して、適用するポリシー グループを決定します。両方

のタイプのポリシーが設定されている場合は、外部 DLP ポリシーと比較する前に、Cisco データ セキュリティ ポリシーと要求を比較します。ポリシー グループに要求を割り当てた後、その要求をポリシー グループの設定済み制御設定と比較し、要求に対して実行するアクションを決定します。アップロード要求を処理するためのアプライアンスの設定方法は、ポリシー グループのタイプによって異なります。

（注） サイズがゼロ（0）バイトのファイルのアップロードを試みているアップロード要求は、Cisco データ セキュリティ ポリシーまたは外部 DLP ポリシーに対して評価されません。

ネットワークから発信されるデータを制限したり制御するには、以下のタスクを実行します。

タスク	タスクへのリンク
Cisco データ セキュリティ ポリシーを作成する	アップロード要求の管理 （3 ページ）
外部 DLP ポリシーを作成する	外部 DLP システムにおけるアップロード要求の管理 （4 ページ）
データセキュリティポリシーおよび外部DLPポリシーを作成する	データ セキュリティ ポリシーおよび外部 DLP ポリシーの作成 （6 ページ）
Cisco データ セキュリティ ポリシーを使用してアップロード要求を制御する	アップロード要求の設定の管理 （9 ページ）
外部 DLP ポリシーを使用してアップロード要求を制御する	外部 DLP ポリシーによるアップロード要求の制御 （14 ページ）

最小サイズ以下のアップロード要求のバイパス

ログファイルに記録されるアップロード要求の数を減らすために、最小要求サイズを定義できます。このサイズを下回る場合、アップロード要求はCiscoデータセキュリティ フィルタや外部 DLP サーバーによってスキャンされません。

これを実行するには、以下の CLI コマンドを使用します。

- **datasecurityconfig**。Cisco データ セキュリティ フィルタに適用します。
- **externaldlpconfig**。設定されている外部 DLP サーバーに適用します。

デフォルトでは、どちらの CLI コマンドでも要求本文の最小サイズは 4 KB（4096 バイト）です。有効な値は 1 ～ 64 KB です。指定したサイズは、アップロード要求の本文全体のサイズに適用されます。

（注） すべてのチャンク エンコードされたアップロードとすべてのネイティブ FTP トランザクションは、Cisco データ セキュリティ フィルタまたは外部 DLP サーバーによってスキャンされます（有効な場合）。ただし、カスタム URL カテゴリに基づいてこれらをバイパスできます。

要求が機密データとしてブロックされた場合のユーザーエクスペリエンス

Cisco データセキュリティ フィルタや外部 DLP サーバーは、アップロード要求をブロックするときに、Web プロキシがエンド ユーザーに送信するブロック ページを提供します。すべての Web サイトでエンドユーザーにブロック ページが表示されるわけではありません。たとえば、一部の Web 2.0 Web サイトは静的な Web ページの代わりに JavaScript を使用して動的なコンテンツを表示し、ブロック ページを表示しない場合が多くあります。そのような場合でも、データ セキュリティ違反が発生しないようにユーザーは適切にブロックされていますが、そのことが Web サイトから通知されない場合もあります。

アップロード要求の管理

始める前に

[セキュリティ サービス（Security Services）] > [データ セキュリティ フィルタ（Data Security Filters）] に移動し、Cisco データ セキュリティ フィルタを有効にします。

データ セキュリティ ポリシー グループを作成して設定します。

Cisco データ セキュリティ ポリシーは、アップロード要求を評価する際に、URL フィルタリング、Web レピュテーション、およびアップロードコンテンツ情報を使用します。これらのセキュリティ コンポーネントを個々に設定し、アップロード要求をブロックするかどうかを決定します。

Web プロキシはアップロード要求を制御設定と比較する際に、順番に設定を評価します。各制御設定は、Cisco データ セキュリティ ポリシーの次のアクションのいずれかを実行するように設定できます。

アクション	説明
ブロック（Block）	Web プロキシは、接続を許可せず、ブロックの理由を説明するエンド ユーザー通知ページを表示します。

アクション	説明
許可（Allow）	Web プロキシは、データ セキュリティ ポリシーの残りのセキュリティ サービス スキャンをバイパスし、最終アクションを実行する前にアクセス ポリシーに対して要求を評価します。 Cisco データ セキュリティ ポリシーでは、残りのデータ セキュリティ スキャンをバイパスできますが、外部 DLP やアクセス ポリシーのスキャンはバイパスしません。Web プロキシが要求に対して実行する最終アクションは、該当するアクセス ポリシー（または、要求をブロックする可能性がある適切な外部 DLP ポリシー）によって決まります。
モニター（Monitor）	Web プロキシは、引き続き、トランザクションと他のデータ セキュリティ ポリシー グループの制御設定を比較し、トランザクションをブロックするか、またはアクセス ポリシーに対して評価するかを決定します。

Cisco データ セキュリティ ポリシーの場合、Web プロキシがクライアント要求に対して実行する最終アクションは「ブロック」アクションだけです。「モニター」および「許可」アクションは中間アクションです。いずれの場合も、Web プロキシは、トランザクションを外部 DLP ポリシー（設定されている場合）およびアクセス ポリシーに対して評価します。Web プロキシは、アクセス ポリシー グループの制御設定（または、要求をブロックする可能性がある適切な外部 DLP ポリシー）に基づいて適用する最終アクションを決定します。

次のタスク

関連項目

- 外部 DLP システムにおけるアップロード要求の管理 （4 ページ）
- アップロード要求の設定の管理 （9 ページ）

外部 DLP システムにおけるアップロード要求の管理

外部 DLP システムでアップロード要求を処理するように Web セキュリティアプライアンス を設定するには、以下のタスクを実行します。

ステップ 1 [ネットワーク（Network）] > [外部 DLP サーバー（External DLP Servers）] を選択します。外部 DLP システムを定義します。スキャンのためにアップロード要求を外部 DLP システムに渡すには、少なくとも 1 つの ICAP 準拠 DLP システムを Web セキュリティアプライアンス で定義する必要があります。

ステップ 2 **外部 DLP ポリシー グループを作成して設定します。**外部 DLP システムを定義したら、外部 DLP ポリシー グループを作成して設定し、スキャンのために DLP システムに送信するアップロード要求を決定します。

ステップ 3 アップロード要求が外部 DLP ポリシーに一致した場合、Web プロキシは、Internet Content Adaptation Protocol（ICAP）を使用して、スキャンのためにアップロード要求を DLP システムに送信します。DLP システムは、要求本文のコンテンツをスキャンし、Web プロキシにブロックまたは許可の判定を返します。許可の

判定は、アップロード要求がアクセス ポリシーと比較される Cisco データ セキュリティ ポリシーの許可アクションに似ています。Web プロキシが要求に対して実行する最終アクションは、適用されるアクセス ポリシーによって決まります。

次のタスク

関連項目

- 外部 DLP ポリシーによるアップロード要求の制御 （14 ページ）
- 外部 DLP システムの定義 （11 ページ）

データ セキュリティおよび外部 DLP ポリシー グループのメンバーシップの評価

各クライアント要求に ID が割り当てられ、次に、それらの要求が他のポリシー タイプと照合して評価され、タイプごとに要求が属するポリシー グループが判定されます。Web プロキシは、データ セキュリティおよび外部 DLP ポリシーに対してアップロード要求を評価します。Web プロキシは、クライアント要求のポリシー グループ メンバーシップに基づいて、設定されているポリシー制御設定をクライアント要求に適用します。

クライアント要求とデータ セキュリティおよび外部 DLP ポリシー グループとの照合

クライアント要求と一致するポリシー グループを判定するために、Web プロキシは、特定のプロセスを実行してグループ メンバーシップの基準と照合します。グループ メンバーシップの以下の要素が考慮されます。

- **ID。**各クライアント要求は、識別プロファイルに一致するか、認証に失敗するか、ゲスト アクセスが許可されるか、または認証に失敗して終了します。
- **権限を持つユーザー。**割り当てられた識別プロファイルが認証を必要とする場合は、そのユーザーがデータ セキュリティまたは外部 DLP ポリシー グループの承認済みユーザーのリストに含まれており、ポリシー グループに一致している必要があります。承認済みユーザーのリストには、任意のグループまたはユーザーを指定でき、識別プロファイルがゲスト アクセスを許可している場合はゲスト ユーザーを指定できます。
- **高度なオプション。**データ セキュリティおよび外部 DLP ポリシー グループのメンバーシップに対して複数の詳細オプションを設定できます。一部のオプション（プロキシ ポート、URL カテゴリなど）は、ID 内に定義することもできます。ID 内に詳細オプションを設定する場合、データ セキュリティまたは外部 DLP ポリシー グループ レベルでは設定できません。

この項では、Web プロキシがアップロード要求をデータ セキュリティおよび外部 DLP の両方のポリシー グループと照合する方法について概要を説明します。

Webプロキシは、ポリシーテーブルの各ポリシー グループを順番に読み取ります。次に、アップロード要求のステータスを最初のポリシー グループのメンバーシップ基準と比較します。一致した場合、Web プロキシは、そのポリシー グループのポリシー設定を適用します。

一致しない場合は、その以下のポリシー グループとアップロード要求を比較します。アップロード要求をユーザー定義のポリシー グループと照合するまで、Web プロキシはこのプロセスを続行します。ユーザー定義のポリシー グループに一致しない場合は、グローバル ポリシー グループと照合します。Webプロキシは、アップロード要求をポリシー グループまたはグローバル ポリシー グループと照合するときに、そのポリシー グループのポリシー設定を適用します。

データ セキュリティ ポリシーおよび外部DLPポリシーの作成

宛先サイトの URL カテゴリや 1 つ以上の識別プロファイルなど、複数の条件の組み合わせに基づいてデータ セキュリティおよび外部 DLP ポリシー グループを作成できます。ポリシー グループのメンバーシップには、少なくとも1つの条件を定義する必要があります。複数の条件が定義されている場合、アップロード要求がポリシー グループと一致するには、すべての条件を満たしていなければなりません。ただし、アップロード要求は設定された識別プロファイルの 1 つとのみ一致する必要があります。

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [Cisco データ セキュリティ（Cisco Data Security）]（データ セキュリティ ポリシー グループ メンバーシップを定義する場合）、または [Web セキュリティ マネージャ（Web Security Manager）] > [外部データ漏洩防止（External Data Loss Prevention）]（外部 DLP ポリシー グループ メンバーシップを定義する場合）を選択します。

ステップ 2 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドにポリシー グループの名前を入力し、[説明（Description）] フィールドに説明を追加します。

（注） 各ポリシー グループ名は、英数字またはスペース文字のみを含む、一意の名前とする必要があります。

ステップ 4 [上記ポリシーを挿入（Insert Above Policy）] フィールドで、ポリシー テーブル内でポリシー グループを配置する場所を選択します。

複数のポリシー グループを設定する場合は、各グループに論理的な順序を指定します。正しく照合されるようにポリシー グループの順序を指定してください。

ステップ 5 [アイデンティティとユーザー（Identities and Users）] セクションで、このポリシー グループに適用する 1 つ以上の識別プロファイル グループを選択します。

ステップ 6 （任意）[詳細設定（Advanced）] セクションを展開して、追加のメンバーシップ要件を定義します。

ステップ 7 いずれかの拡張オプションを使用してポリシー グループのメンバーシップを定義するには、拡張オプションのリンクをクリックし、表示されるページでオプションを設定します。

高度なオプション	説明
プロトコル	クライアント要求で使用されるプロトコルによってポリシー グループのメンバーシップを定義するかどうかを選択します。含めるプロトコルを選択します。 [その他のすべて（All others）]は、このオプションの上に一覧表示されていないプロトコルを意味します。 （注） HTTPSプロキシをイネーブルにすると、復号化ポリシーのみがHTTPSトランザクションに適用されます。アクセス、ルーティング、アウトバウンド マルウェア スキャン、データ セキュリティ、外部 DLP のポリシーの場合は、HTTPSプロトコルによってポリシー メンバーシップを定義できません。
プロキシ ポート（Proxy Ports）	Webプロキシへのアクセスに使用するプロキシ ポートで、ポリシー グループ メンバーシップを定義するかどうかを選択します。[プロキシ ポート（Proxy Ports）]フィールドに、1つ以上のポート番号を入力します。複数のポートを指定する場合は、カンマで区切ります。 明示的な転送接続のために、ブラウザに設定されたポートです。透過接続の場合は、宛先ポートと同じです。あるポート上に要求を明示的に転送するように設定されたクライアントのセットがあり、別のポート上に要求を明示的に転送するように設定された別のクライアントのセットがある場合、プロキシ ポート上でポリシー グループのメンバーシップを定義することがあります。 シスコでは、アプライアンスが明示的な転送モードで配置されている場合、またはクライアントがアプライアンスに要求を明示的に転送する場合にだけ、プロキシ ポートでポリシー グループのメンバーシップを定義することを推奨します。クライアント要求がアプライアンスに透過的にリダイレクトされるときにプロキシ ポートでポリシー グループのメンバーシップを定義すると、一部の要求が拒否される場合があります。 （注） このポリシー グループに関連付けられているIDがこの詳細設定によってIDメンバーシップを定義している場合、非IDポリシー グループ レベルではこの設定項目を設定できません。
サブネット（Subnets）	サブネットまたは他のアドレスでポリシー グループのメンバーシップを定義するかどうかを選択します。 関連付けられた識別プロファイルで定義できるアドレスを使用するか、または特定のアドレスをここに入力できます。 （注） ポリシー グループに関連付けられている識別プロファイルがアドレスによってグループのメンバーシップを定義している場合は、識別プロファイルで定義されているアドレスのサブセットであるアドレスを、このポリシー グループに入力する必要があります。ポリシー グループにアドレスを追加することにより、このグループ ポリシーに一致するトランザクションのリストを絞り込めます。

高度なオプション	説明
URL カテゴリ（URL Categories）	URL カテゴリでポリシー グループのメンバーシップを定義するかどうかを選択します。ユーザー定義または定義済みの URL カテゴリを選択します。 （注） このポリシー グループに関連付けられている ID がこの詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。
ユーザー エージェント（User Agents）	クライアント要求で使用されるユーザー エージェント（アップデータや Web ブラウザなどのクライアント アプリケーション）ごとにポリシー グループ メンバーシップを定義するかどうかを選択します。一般的に定義されているユーザー エージェントを選択するか、正規表現を使用して独自に定義できます。メンバーシップの定義に選択したユーザー エージェントのみを含めるか、選択したユーザー エージェントを明確に除外するかどうかを指定します。 （注） このポリシー グループに関連付けられている識別プロファイルが、この詳細設定によって識別プロファイル メンバーシップを定義している場合、非識別プロファイル ポリシー グループ レベルではこの設定項目を設定できません。
ユーザーの場所（User Location）	ユーザーのリモートまたはローカルの場所でポリシー グループのメンバーシップを定義するかどうかを選択します。 このオプションは、セキュアモビリティがイネーブルの場合にのみ表示されます。

ステップ 8 変更を送信します。

ステップ 9 データ セキュリティ ポリシー グループを作成する場合は、その制御設定を設定して、Web プロキシがアップロード要求を処理する方法を定義します。

新しいデータ セキュリティ ポリシー グループは、各制御設定のオプションが設定されるまで、グローバル ポリシー グループの設定を自動的に継承します。

外部 DLP ポリシー グループを作成する場合は、その制御設定を設定して、Web プロキシがアップロード要求を処理する方法を定義します。

新しい外部 DLP ポリシー グループは、カスタム設定が設定されるまで、グローバル ポリシー グループの設定を自動的に継承します。

ステップ 10 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次のタスク

関連項目

- データ セキュリティおよび外部 DLP ポリシー グループのメンバーシップの評価 （5 ページ）
- クライアント要求とデータ セキュリティおよび外部 DLP ポリシー グループとの照合 （5 ページ）

アップロード要求の設定の管理

各アップロード要求は、データセキュリティポリシーグループに割り当てられ、そのポリシーグループの制御設定を継承します。データ セキュリティ ポリシー グループの制御設定によって、アプライアンスが接続をブロックするか、またはアクセスポリシーに対して接続を評価するかが決まります。

[Web セキュリティ マネージャ（Web Security Manager）] > [Cisco データ セキュリティ（Cisco Data Security）] ページで、データ セキュリティ ポリシー グループの制御設定を設定します。

以下の設定項目を設定して、アップロード要求で実行するアクションを決定できます。

オプション	リンク
URL カテゴリ（URL Categories）	URL カテゴリ （9 ページ）
Web レピュテーション	Web レピュテーション （9 ページ）
目次	コンテンツのブロック （10 ページ）

データ セキュリティ ポリシー グループがアップロード要求に割り当てられた後、ポリシー グループの制御設定が評価され、要求をブロックするかアクセスポリシーに対して評価するかが決定されます。

URL カテゴリ

AsyncOS for Web では、アプライアンスが特定の要求の URL カテゴリに基づいてトランザクションを処理する方法を設定できます。定義済みのカテゴリ リストを使用して、カテゴリ別にコンテンツをモニターするかブロックするかを選択できます。カスタム URL カテゴリを作成し、カスタム カテゴリの Web サイトに対してトラフィックを許可、モニター、またはブロックするかを選択することもできます。

Web レピュテーション

Web レピュテーションの設定はグローバル設定を継承します。特定のポリシー グループ用に Web レピュテーション フィルタリングをカスタマイズするには、[Webレピュテーション設定（Web Reputation Settings）] プルダウン メニューを使用して Web レピュテーション スコアのしきい値をカスタマイズします。

Cisco データ セキュリティ ポリシーの Web レピュテーションのしきい値には、負またはゼロの値のみ設定できます。定義では、すべての正のスコアがモニターされます。

コンテンツのブロック

[Cisco データ セキュリティ（Cisco Data Security）] > [コンテンツ（Content）] ページの設定項目を使用し、Webプロキシが次のファイル特性に基づいてデータのアップロードをブロックするように設定できます。

- **[ファイルサイズ（File size）]。**許容される最大アップロード サイズを指定できます。指定した最大値以上のサイズのアップロードはすべてブロックされます。HTTP/HTTPSおよびネイティブ FTP 要求に対して異なる最大ファイル サイズを指定できます。

  アップロード要求サイズが最大アップロード サイズと最大スキャン サイズ（[セキュリティ サービス（Security Services）] > [マルウェア対策（Anti-Malware）] ページの [DVS エンジン オブジェクト スキャンの制限（DVS Engine Object Scanning Limits）] フィールドで設定）のどちらよりも大きい場合、アップロード要求はブロックされますが、ファイル名とコンテンツ タイプはデータ セキュリティ ログに記録されません。アクセス ログのエントリは変更されません。

- **[ファイル タイプ（File type）]。**定義済みのファイル タイプまたは入力したカスタム MIME タイプをブロックできます。定義済みファイル タイプをブロックする場合は、そのタイプのすべてのファイルまたは指定したサイズよりも大きいファイルをブロックできます。ファイル タイプをサイズによってブロックする場合は、最大ファイル サイズとして、[セキュリティ サービス（Security Services）] > [マルウェア対策（Anti-Malware）] ページの [DVS エンジン オブジェクト スキャンの制限（DVS Engine Object Scanning Limits）] フィールドの値と同じ値を指定できます。デフォルトでは、この値は 32 MB です。

  Ciscoデータ セキュリティ フィルタは、ファイル タイプによってブロックする場合にアーカイブ ファイルのコンテンツを検査しません。アーカイブ ファイルは、ファイル タイプまたはファイル名によってブロックできます。コンテンツによってブロックすることはできません。

（注） 一部の MIME タイプのグループでは、1 つのタイプをブロックすると、グループ内のすべてのMIMEタイプがブロックされます。たとえば、application/x-java-applet をブロックすると、application/java や application/javascript など、すべての MIME タイプがブロックされます。

- **[ファイル名（File name）]。**指定した名前のファイルをブロックできます。ブロックするファイル名を指定する場合は、リテラル文字列または正規表現をテキストとして使用できます。

（注） 8 ビット ASCII 文字のファイル名のみを入力してください。Webプロキシは、8ビットASCII文字のファイル名のみを照合します。

外部 DLP システムの定義

Web セキュリティアプライアンス では、アプライアンスに複数の DLP サーバを定義することにより、同じベンダーの複数の外部 DLP サーバを統合できます。Web プロキシが DLP システムに接続する際に使用するロード バランシング技術を定義できます。これは、複数の DLP システムを定義する場合に役立ちます。外部 DLP サーバーとのセキュアな通信に使用されるプロトコルの指定については、SSL の設定を参照してください。

（注） 外部 DLP サーバーが Web プロキシによって変更されたコンテンツを送信しないことを確認します。AsyncOS for Web は、アップロード要求をブロックまたは許可する機能のみをサポートしています。外部 DLP サーバーによって変更されたコンテンツのアップロードはサポートしません。

外部 DLP サーバーの設定

ステップ 1 [ネットワーク（Network）] > [外部 DLP サーバー（External DLP Servers）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

設定	説明
外部 DLP サーバーのプロトコル（Protocol for External DLP Servers）	以下のいずれかを選択します。 • [ICAP]：DLPクライアント/サーバーの ICAP 通信は暗号化されません。 • [セキュアICAP（Secure ICAP）]：DLP クライアント/サーバー の ICAP 通信は暗号化トンネルを介して行われます。追加の関連オプションが表示されます。

設定	説明
外部 DLP サーバー（External DLP Servers）	以下の情報を入力して、ICAP 準拠 DLP システムにアクセスします。 • [サーバー アドレス（Server address）] と [ポート（Port）]：DLP システムにアクセスするホスト名/IP アドレスと TCP ポート。 • [再接続の試行（Reconnection attempts）]：失敗するまでに Web プロキシが DLP システムへの接続を試行する回数。 • [サービスURL（Service URL）]：特定の DLP サーバーに固有の ICAP クエリー URL。Web プロキシは、ここに入力された情報を外部 DLP サーバーに送信する ICAP 要求に含めます。URL は、ICAP プロトコル（icap://）から始める必要があります。 • [証明書（Certificate）]（任意）：各外部 DLP サーバー接続を保護するために提供する証明書は、認証局（CA）の署名付き証明書でも自己署名証明書でもかまいません。指定されたサーバーから証明書を取得し、アプライアンスにアップロードします。 • 証明書ファイルを参照して選択し、[ファイルのアップロード（Upload File）] をクリックします。 （注） この単一ファイルには、暗号化されていない形式でクライアント証明書と秘密キーを含める必要があります。 • [セキュアICAPを使用するすべてのDLPサーバーにこの証明書を使用する（Use this certificate for all DLP servers using Secure ICAP）]：ここで定義するすべての外部 DLP サーバーに同じ証明書を使用する場合は、このチェックボックスをオンにします。サーバーごとに異なる証明書を入力するには、このオプションをオフのままにします。 • [テスト開始（Start Test）]：このチェックボックスをオンにすると、Web セキュリティアプライアンスと定義済み外部 DLP サーバ間の接続をテストできます。

設定	説明
ロード バランシング	複数の DLP サーバーを定義する場合は、Web プロキシがさまざまな DLP サーバーにアップロード要求を分散する際に使用するロードバランシング技術を選択します。以下のロード バランシング技術を選択できます。 • **[なし（フェールオーバー）（None(failover）]**。Web プロキシは、1 つの DLP サーバーにアップロード要求を送信します。一覧表示されている順序で DLP サーバーへの接続を試みます。ある DLP サーバーに到達できない場合、Web プロキシはリストの以下のサーバーへの接続を試みます。 • **[最少接続（Fewest connections）]**。Web プロキシは、各 DLP サーバーが扱っているアクティブな要求の数を追跡し、その時点で接続数が最も少ない DLP サーバーにアップロード要求を送信します。 • **[ハッシュベース（Hash based）]**。Web プロキシは、ハッシュ関数を使用して、DLP サーバーに要求を分散します。ハッシュ関数はプロキシ ID と URL を入力として使用し、同じ URL の要求が常に同じ DLP サーバーに送信されるようにします。 • **[ラウンド ロビン（Round robin）]**。Web プロキシは、リストされた順序ですべての DLP サーバー間にアップロード要求を均等に分散します。
サービス要求タイムアウト（Service Request Timeout）	Web プロキシが DLP サーバーからの応答を待機する時間を入力します。この時間が経過すると、ICAP 要求は失敗し、[失敗のハンドリング（Failure Handling）] の設定に応じて、アップロード要求はブロックまたは許可されます。 デフォルトは 60 秒です。
最大同時接続数（Maximum Simultaneous Connections）	Web セキュリティアプライアンス から設定されている各外部 DLP サーバへの同時 ICAP 要求接続の最大数を指定します。このページの [失敗のハンドリング（Failure Handling）] 設定は、この制限を超えるすべての要求に適用されます。 デフォルトは 25 です。
失敗のハンドリング（Failure Handling）	DLP サーバーがタイムリーに応答できなかった場合に、アップロード要求をブロックするか許可するか（評価のためにアクセス ポリシーに渡される）を選択します。 デフォルトは、許可（[すべてのデータ転送をスキャンなしで許可する（Permit all data transfers to proceed without scanning）]）です。
信頼できるルート証明書（Trusted Root Certificate）	外部 DLP サーバーによって提供された証明書に対して、信頼できるルート証明書を参照して選択し、[ファイルのアップロード（Upload File）] をクリックします。詳細については、証明書の管理（Certificate Management）を参照してください。
無効な証明書オプション（Invalid Certificate Options）	さまざまな無効な証明書の処理方法（[ドロップ（Drop）] または [モニター（Monitor）]）を指定します。

設定	説明
サーバー証明書（Server Certificates）	このセクションには、アプライアンスで現在使用可能なすべての DLP サーバー証明書が表示されます。

ステップ 3 （任意）[行を追加（Add Row）] をクリックし、表示される新しいフィールドに DLP サーバー情報を入力することによって、別の DLP サーバーを追加できます。

ステップ 4 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

外部 DLP ポリシーによるアップロード要求の制御

Webプロキシは、アップロード要求ヘッダーを受信することにより、スキャン用に要求を外部 DLP システムに送信する必要があるかどうかを判定するための必要情報を得ます。DLP システムは要求をスキャンし、Webプロキシに判定（ブロックまたはモニター）を返します（要求はアクセス ポリシーに対して評価されます）。

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [外部データ漏洩防止（External Data Loss Prevention）] を選択します。

ステップ 2 [接続先（Destinations）] 列で、設定するポリシー グループのリンクをクリックします。

ステップ 3 [接続先設定の編集（Edit Destination Settings section）] セクションで、[接続先スキャンのカスタム設定の定義（Define Destinations Scanning Custom Settings）] を選択します。

ステップ 4 [スキャンする接続先（Destination to Scan）] セクションで、以下のオプションのいずれかを選択します。

- **[どのアップロードもスキャンしない（Do not scan any uploads）]。**アップロード要求は、スキャンのために設定済みDLPシステムに送信されません。すべてのアップロード要求がアクセス ポリシーに対して評価されます。
- **[すべてのアップロードをスキャンする（Scan all uploads）]** すべてのアップロード要求が、スキャンのために設定済みDLPシステムに送信されます。アップロード要求は、DLPシステムのスキャン判定に応じて、ブロックされるか、アクセス ポリシーに対して評価されます。
- **[指定したカスタムおよび外部 URL カテゴリ以外へのアップロードをスキャン（Scan uploads except to specified custom and external URL categories）]。**特定のカスタム URL カテゴリに該当するアップロードの要求が、DLP スキャン ポリシーから除外されます。[カスタムカテゴリリストを編集（Edit custom categories list）] をクリックして、スキャンする URL カテゴリを選択します。

ステップ 5 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

データ損失防止スキャンのロギング

アクセス ログは、アップロード要求が Cisco データ セキュリティ フィルタまたは外部 DLP サーバーのいずれかによってスキャン済みかどうかを示します。アクセス ログエントリには、

Cisco データ セキュリティ ポリシーのスキャン判定用のフィールド、および外部 DLP スキャン判定に基づく別のフィールドが含まれています。

アクセス ログに加えて、Web セキュリティアプライアンス には、Cisco データ セキュリティ ポリシーや外部 DLP ポリシーをトラブルシューティングするための次のようなログ ファイルが用意されています。

- **データ セキュリティ ログ。**Cisco データ セキュリティ フィルタで評価されたアップロード要求のクライアント履歴を記録します。
- **データ セキュリティ モジュール ログ。**Cisco データ セキュリティ フィルタに関するメッセージを記録します。
- **デフォルト プロキシ ログ。**Web プロキシに関連するエラーの記録に加えて、デフォルト プロキシ ログには外部 DLP サーバーへの接続に関連するメッセージが含まれています。これにより、外部 DLP サーバーとの接続や統合に関する問題をトラブルシューティングできます。

以下のテキストは、データ セキュリティ ログのエントリのサンプルを示しています。

```
Mon Mar 30 03:02:13 2009 Info: 303 10.1.1.1 - -
<<bar,text/plain,5120><foo,text/plain,5120>>
BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting ns server.com
nc
```

フィールド値	説明
`Mon Mar 30 03:02:13 2009 Info:`	タイムスタンプおよびトレース レベル
`303`	トランザクション ID
`10.1.1.1`	ソース IP アドレス
`-`	ユーザー名（User name）
`-`	承認されたグループ名。
`<<bar,text/plain,5120><foo,text/plain,5120>>`	一度にアップロードされる各ファイルのファイル名、ファイル タイプ、ファイル サイズ （注） このフィールドには、設定されている最小の要求本文サイズ（デフォルトは 4096 バイト）よりも小さいテキスト/プレーン ファイルは含まれません。
`BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting`	Cisco データ セキュリティ ポリシーおよびアクション

フィールド値	説明
ns	Web レピュテーション スコア
server.com	発信 URL
nc	URL カテゴリ

（注） サイトへのデータ転送（POST 要求など）がいつ外部 DLP サーバーによってブロックされたかを確認するには、アクセス ログの DLP サーバーの IP アドレスまたはホスト名を検索します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。