データ損失の防止

この章は、次の項で構成されています。

データ消失防止の概要

データ消失防止（DLP）機能により、ユーザが悪意を持ってまたは過失によって機密データを電子メールで送付しないように防止することで、組織の情報と知的財産を保護し、規制と組織のコンプライアンスを実施します。法または会社のポリシーに違反するデータがないか送信メッセージをスキャンするのに使われる DLP ポリシーを作成して、従業員が電子メールで送付できないデータの種類を定義します。

DLP スキャン プロセスの概要

	操作	詳細情報
1.	組織のユーザは組織外部の受信者に電子メールでメッセージを送信します。	E メール セキュリティ アプライアンスは、ネットワークに出入りするメッセージを処理する「ゲートウェイ」アプライアンスです。 ネットワーク内の他のユーザに送信されるメッセージはスキャンされません。
2.	E メール セキュリティ アプライアンスは DLP スキャン段階に到達する前に電子メールの「ワーク キュー」の段階でメッセージを処理します。	DLP スキャン前プロセスは、たとえばメッセージにスパムやマルウェアが含まれていないことを確認します。 DLP 処理がワークキューのどこで発生するかを確認するには、電子メール パイプラインのフローのワークキューフロー図を参照してください。
3.	アプライアンスは、DLP ポリシーで特定した重要なコンテンツのメッセージ本文、ヘッダー、添付ファイルをスキャンします。	データ消失防止の動作, （2 ページ）を参照してください。
4.	重要なコンテンツが見つかった場合、アプライアンスはメッセージを隔離するか、廃棄または制限をかけて提供するなどのデータを保護するための処理を行います。 それ以外は、メッセージはアプライアンスのワーク キューを通じて継続され、問題がない場合は、E メール セキュリティ アプライアンスで受信者に配信されます。	実行されるアクションを定義します。[メッセージアクション（Message Actions）], （23 ページ）を参照してください。

データ消失防止の動作

組織内の誰かが組織外部の受信者にメッセージを送信する場合、アプライアンスは、定義したルールに基づいてどの発信メール ポリシーをメッセージの送信者または受信者に適用するかを決定します。アプライアンスは、その発信メール ポシリーに指定された DLP ポリシーを使用してメッセージの内容を評価します。

具体的には、アプライアンスは、単語、語句、社会保障番号などの定義済みのパターン、または適用される DLP ポリシーで機密内容として特定される正規表現と一致するテキストがないかメッセージ内容（ヘッダーと添付ファイルを含む）をスキャンします。

また、アプライアンスは、誤検出の一致を最小限に抑えるため拒否されたコンテキストを評価します。たとえば、クレジット カード番号のパターンに一致する番号は、有効期限、クレジット カード会社名（VISA、AMEXなど）、または個人の名前や住所が伴っている場合のみ違反になります。

メッセージ内容が複数のDLPポリシーに一致したら、指定された順序に基づいてリストの最初に一致したDLPポリシーが適用されます。内容が違反であるかどうかを判断するために同じ基準を使用する複数のDLPポリシーが発信メール ポリシーにある場合でも、すべてのポリシーは、1つの内容スキャンの結果を使用します。

機密である可能性のある内容がメッセージに表示されると、アプライアンスは0～100間のリスク要因スコアを潜在的違反に割り当てます。このスコアは、メッセージにDLP違反が含まれる確率を示します。

アプライアンスは、そのリスク要因スコアに定義した重大度レベル（クリティカルまたは低いなど）を割り当て、適切なDLPポリシーでその重大度に指定したメッセージアクションを実行します。

データ消失防止のシステム要件

データ損失の防止は、D-Modeライセンスを使用するアプライアンスを除き、サポートされるすべてのCシリーズおよびX-Seriesアプライアンスでサポートされています。

データ漏洩防止の設定方法

次の手順を順番に実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ1	DLP機能を有効にします。	データ消失防止の有効化（DLP），（4ページ）
ステップ2	違反が見つかったか疑いがあるメッセージに対して実行できるアクションを定義します。たとえば、そのようなメッセージを隔離できます。	[メッセージアクション（Message Actions）]，（23ページ）
ステップ3	DLPポリシーの作成について次を行います。 • 組織から電子メールで送信しないコンテンツを識別します。 • 各違反について実行するアクションを指定します。	方法を選択します。 • ウィザードを使用したDLP防止の設定，（6ページ） • 事前定義されたテンプレートを使用したDLPポリシーの作成，（7ページ） • カスタムDLPポリシーの作成（詳細），（8ページ）

	コマンドまたはアクション	目的
ステップ 4	コンテンツが 1 つ以上の DLP ポリシーに一致する可能性がある場合に、DLP 違反のメッセージの評価に使用する DLP ポリシーを指定する場合は、DLP ポリシーの順序を設定します。	違反との一致に対する Email DLP ポリシーの順序の調整, （21 ページ）
ステップ 5	DLP 違反をスキャンするメッセージの送信者と受信者グループごとに発信メール ポリシーを作成したことを確認します。	参照先： メール ポリシー さらに個々の DLP ポリシーの許可および制限されたメッセージ送信者と受信者を改善するには、DLP ポリシーのメッセージのフィルタリング, （19 ページ）を参照してください。
ステップ 6	DLP ポリシーを発信メール ポリシーに割り付けることによって、どの DLP ポリシーをどの送信者と受信者に適用するかを指定します。	発信メール ポリシーとの DLP ポリシーの関連付け, （22 ページ）
ステップ 7	ストレージの設定を構成し、機密 DLP 情報にアクセスします。	• メッセージ トラッキングでの機密性の高い DLP データの表示, （30 ページ） • メッセージ トラッキングでの機密情報へのアクセスの制御

データ消失防止の有効化（DLP）

ステップ 1 [セキュリティ サービス（Security Services）] > [データ損失の防止（Data Loss Prevention）] の順に選択します。

ステップ 2 [有効（Enable）] をクリックします。

ステップ 3 ライセンス契約書ページの下部にスクロールし、[承認（Accept）] をクリックしてライセンス契約に合意します。

（注） ライセンス契約に合意しない場合、DLP はアプライアンス上で有効になりません。

ステップ 4 [データ漏洩防止グローバル設定（Data Loss Prevention Global Settings）] の下の [データ漏洩防止を有効にする（Enable Data Loss Prevention）] を選択します。

ステップ 5 （推奨）現段階では、このページの他のオプションの選択を解除します。
これらの設定は、後でこの章で説明する手順に従って変更できます。

ステップ 6 変更を送信し、保存します。

次の作業

データ漏洩防止の設定方法，（3 ページ）を参照してください。

データ損失防止のポリシー

DLP ポリシーの説明

DLP ポリシーは次が含まれます。

- 発信メッセージが機密データが含んでいるかどうかを判断する一連の条件
- メッセージがそのようなデータを含んでいる場合に実行するアクション。

メッセージ コンテンツの評価方法を以下から指定します。

- 拒否された特定のコンテンツまたは情報のパターン。ポリシーによっては、識別番号を検索する正規表現の作成が必須の場合があります。コンテンツ照合分類子を使用した拒否されたコンテンツの定義について，（10 ページ）を参照してください。
- メッセージ フィルタリング用の特定の送信者および受信者のリスト。DLP ポリシーのメッセージのフィルタリング，（19 ページ）を参照してください。
- メッセージ フィルタリング用の添付ファイルのタイプ一覧。DLP ポリシーのメッセージのフィルタリング，（19 ページ）を参照してください。
- 発生するさまざまなアクションを許可する設定は違反の重大度に基づいています。違反の重大度の評価について，（20 ページ）を参照してください。

発信メールポリシーのDLPポリシーをイネーブルにする場合に、各ポリシーを適用するメッセージ送信者と受信者を決定します。

定義済み DLP ポリシー テンプレート

DLPポリシーの作成を簡素化するために、アプライアンスには、定義済みのポリシーテンプレートの大規模なコレクションが含まれます。

テンプレートのカテゴリには次が含まれます。

- [規制コンプライアンス（Regulatory Compliance）]。これらのテンプレートは、個人識別情報、クレジット情報、その他の保護または非公開情報を含む添付ファイル、メッセージを識別します。
- [許可された使用（Acceptable Use）]。これらのテンプレートは、組織の機密情報が含まれる制限された受信者または競合他社に送信されたメッセージを指定します。
- [プライバシー保護（Privacy Protection）]。金融口座、税金記録、国民 ID の識別番号を含むメッセージおよび添付ファイルを識別します。

- [知的財産保護（Intellectual Property Protection）]。これらのテンプレートは、よく使われるパブリッシングおよびデザイン ドキュメント ファイル タイプで、組織が保護する知的財産を含む可能性があるものを識別します。
- [企業機密情報（Company Confidential）]。これらのテンプレートは、会社の財務情報や近い将来の合併および買収に関する情報を含むドキュメントとメッセージを識別します。
- [カスタム ポリシー（Custom Policy）]。この「テンプレート」を使用すると、定義済みのコンテンツ照合分類子または組織が指定した違反識別基準を使用して、独自のポリシーを最初から作成できます。このオプションは高度であり、事前定義されたポリシーテンプレートではユーザのネットワーク環境の独自の要件を満たせない、まれな場合にのみ使用されることを想定しています。

これらのテンプレートの中にはカスタマイズが必要になものもあります。

ウィザードを使用した DLP 防止の設定

DLP 評価ウィザードでは一般的な DLP ポリシーを設定し、アプライアンスのデフォルトの発信メール ポリシーでイネーブルにします。

（注） DLP Assessment Wizard を使って追加された DLP ポリシーでは、検出された DLP 違反の重大度にかかわらず、メッセージはすべて配信されます。ウィザードを使用して作成されたポリシーを編集する必要があります。

はじめる前に

- アプライアンスから既存の DLP ポリシーを削除します。DLP ポリシーがアプライアンスに存在しない場合は、DLP Assessment Wizard のみ使用することができます。
- クレジットカード番号、米国社会保障番号、および米国運転免許証番号以外の生徒識別番号またはアカウント番号を含むメッセージを検出する必要がある場合、それらの番号を特定する正規表現を作成します。詳細については、識別番号を識別する正規表現, （14 ページ）を参照してください。

ステップ 1 [セキュリティサービス（Security Services）] > [データ漏洩防止（Data Loss Prevention）] 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。

ステップ 3 [有効（Enable）] を選択し、[DLP 評価ウィザードを使用して DLP を設定します。（DLP using the DLP Assessment Wizard）] チェックボックスをオンにします。

ステップ 4 [送信（Submit）] をクリックします。

ステップ 5 ウィザードを完了します。
次の点を考慮してください。

- カリフォルニアでビジネスを営み、カリフォルニア州民のコンピュータ化した個人情報（PII）データを保有またはライセンスしている企業は、物理的な所在地にかかわらず、米国の規則（カリフォル

ニア SB-1386）に準拠することが必須となっています。この法律は、ウィザードのポリシーの選択肢の 1 つです。

- 自動生成されたスケジュール済み DLP インシデント サマリー レポートを受信する電子メール アドレスを入力しない場合、レポートは生成されません。
- 設定を確認し、変更を加える手順まで戻った場合は、再度このレビュー ページに至るまで、残りの手順を進める必要があります。以前に入力した設定は、すべて残っています。
- ウィザードを完了すると、デフォルトの送信メール ポリシーで DLP ポリシーがイネーブルな [送信メール ポリシー（Outgoing Mail Policies）] ページが表示されます。DLP ポリシー設定の要約が、ページの上部に表示されます。

ステップ 6 変更を保存します。

次の作業

- （任意）これらの DLP ポリシーを編集し、追加ポリシーを作成し、メッセージの全体的な処理を変更するか、または重大度レベルの設定を変更するには、[メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）] を選択します。詳細については、事前定義されたテンプレートを使用した DLP ポリシーの作成, （7 ページ）、カスタム DLP ポリシーの作成（詳細）, （8 ページ）、および重大度スケールの調整, （21 ページ）を参照してください。
- （任意）他の発信メール ポリシーのある既存の DLP ポリシーをイネーブルにするには、発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て, （22 ページ）を参照してください。

事前定義されたテンプレートを使用した DLP ポリシーの作成

ステップ 1 [メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）] を選択します。

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

ステップ 3 カテゴリ名をクリックし、使用可能な DLP ポリシー テンプレートの一覧を表示します。

（注） 各テンプレートの説明を表示するには、[ポリシーの説明を表示（Display Policy Descriptions）] をクリックします。

ステップ 4 使用する DLP ポリシー テンプレートの [追加（Add）] をクリックします。

ステップ 5 （任意）テンプレートの定義済みの名前と説明を変更します。

ステップ 6 ポリシーで、1 つ以上のコンテンツ照合分類子のカスタマイズが要求または推奨される場合は、組織の識別番号付けシステムのパターンを定義するための正規表現と、使用される識別番号に関連する、または通常は関連付けられている単語や語句のリストを入力します。
詳細については、次を参照してください。

コンテンツ照合分類子を使用した拒否されたコンテンツの定義について，（10 ページ）および識別番号を識別する正規表現，（14 ページ）。

（注） 定義済みのテンプレートに基づいたポリシーのコンテンツの分類子は追加または削除できません。

ステップ 7 （任意）特定の受信者、送信者、添付ファイルの種類、または以前に追加されたメッセージ タグを持つメッセージにのみ DLP ポリシーを適用します。

詳細については、DLP ポリシーのメッセージのフィルタリング，（19 ページ）を参照してください。

改行やカンマで、複数のエントリを分離できます。

ステップ 8 [重大度設定（Severity Settings）] の項で、以下を行います。

- 違反の重大度レベルごとに実行するアクションを選択します。詳細については、違反の重大度の評価について，（20 ページ）を参照してください。
- （任意）ポリシーに対して違反の重大度基準を調整する場合は、[スケールの編集（Edit Scale）] をクリックします。詳細については、重大度スケールの調整，（21 ページ）を参照してください。

ステップ 9 変更を送信し、保存します。

カスタム DLP ポリシーの作成（詳細）

（注） カスタム ポリシーの作成は非常に複雑です。定義済み DLP ポリシー テンプレートが組織のニーズを満たさない場合のみ、カスタム ポリシーを作成します。

Custom Policy テンプレートを使用して、カスタム DLP ポリシーを最初から作成し、定義されたコンテンツ照合分類子またはカスタム分類子をポリシーに追加できます。

ポリシーの定義によって、コンテンツが 1 つの分類子またはすべての分類子に一致した場合に、カスタム ポリシーは DLP 違反を返すことができます。

はじめる前に

推奨：コンテンツ違反を識別する基準を定義します。カスタム DLP ポリシーに対するコンテンツ照合分類子の作成，（12 ページ）を参照してください。次の手順の中で、これらの基準を定義することもできます。

ステップ 1 [メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）] を選択します。

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

ステップ 3 [カスタムポリシー（Custom Policy）] をクリックします。

ステップ 4 Custom Policy テンプレートの [追加（Add）] をクリックします。

ステップ 5 ポリシーの名前と説明を入力します。

ステップ 6 DLP 違反を構成するコンテンツとコンテキストを特定します。

a) コンテンツ照合分類子を選択します。

b) [追加（Add）] をクリックします。

- [分類子を作成（Create a Classifier）] を選択した場合、カスタム DLP ポリシーに対するコンテンツ照合分類子の作成，（12 ページ）を参照してください。
- それ以外の場合は、選択された分類子がテーブルに追加されます。

c) （任意）ポリシーに追加分類子を追加します。
たとえば、別の分類子を追加し、[NOT] を選択して、既知の誤検出である可能性の高い一致を削除できます。

d) 複数の分類子を追加した場合、テーブル見出しのオプションを選択し、インスタンスを違反としてカウントするために分類子の一部またはすべてを一致させるかどうかを指定します。

ステップ 7 （任意）特定の受信者、送信者、添付ファイルの種類、または以前に追加されたメッセージ タグを持つメッセージにのみ DLP ポリシーを適用します。
詳細については、DLP ポリシーのメッセージのフィルタリング，（19 ページ）を参照してください。

改行やカンマで、複数のエントリを分離できます。

ステップ 8 [重大度設定（Severity Settings）] の項で、以下を行います。

- 違反の重大度レベルごとに実行するアクションを選択します。詳細については、違反の重大度の評価について，（20 ページ）を参照してください。
- （任意）ポリシーに対して違反の重大度基準を調整する場合は、[スケールの編集（Edit Scale）] をクリックします。詳細については、次を参照してください。 重大度スケールの調整，（21 ページ）

ステップ 9 変更を送信し、保存します。

コンテンツ照合分類子を使用した拒否されたコンテンツの定義について

コンテンツ一致分類子は、電子メールで送信できないコンテンツと、任意選択でそのコンテンツがデータ消失防止違反と見なされるために発生する必要があるコンテキストを定義します。

患者識別番号が組織から電子メールで送信されることを回避する必要があるとします。

これらの番号をアプライアンスに認識させるために、1 つ以上の正規表現を使用して組織の記録番号付けシステムのパターンを指定する必要があります。補足情報として記録番号を伴うかもしれない単語およびフレーズのリストを追加できます。分類子が発信メッセージ内に番号パターンを検出すると、補足情報を検索し、そのパターンが識別番号か、また、ランダムな番号の文字列でないかを確認します。コンテキストと一致する情報を含むことにより、誤検出の一致が減少します。

この例では、HIPAA および HITECH テンプレートを使用する DLP ポリシーを作成します。このテンプレートには、患者識別番号コンテンツ照合分類子という患者識別番号を検出するようにカスタマイズ可能な分類子が含まれます。パターン 123-CL456789 の番号を検出するには、分類子の正規表現 [0-9]{3}\-[A-Z]{2}[0-9]{6} を入力します。関連フレーズとして「Patient ID」と入力します。ポリシーの作成を完了し、発信メール ポリシーでイネーブルにします。変更を送信し、保存します。フレーズ「患者 ID」が番号パターンの近くに設定された発信メッセージからポリシーが番号パターンを検出した場合、DLP ポリシーは DLP 違反を返します。

DLP ポリシーでのコンテンツ照合分類子の使用方法について

定義済み DLP ポリシー テンプレートの多くは、RSA のコンテンツ照合分類子が含まれます。これらの分類子の一部は、組織のデータに使用されるパターンを識別するためにカスタマイズする必要があります。

カスタム DLP ポリシーを作成すると、事前定義された分類子を選択するか、独自の分類子を作成できます。

コンテンツ照合分類子の例

次の例は、分類子がメッセージの内容を照合する方法を示します。

クレジット カード番号

DLP ポリシーテンプレートのいくつかは、クレジットカード番号分類子を含みます。クレジットカード番号はそれ自体、数と句読点のパターン、発行者固有のプレフィックス、最後のチェックデジットなどさまざまな制約があります。この分類子で一致するには、有効期限やカード発行者の名前など、追加の補足情報が必要です。これで false positive の数が減ります。

例：

- `378734493671000`（補足情報がないため一致せず）
- `378734493671000 VISA`（一致）

- `378734493671000 exp: 12/2019`（一致）

米国社会保障番号

米国社会保障番号分類子では、正しい形式の番号と誕生日や名前および「SSN」という文字列などの補足データが必要です。

例：

- `321-02-3456`（補足情報がないため一致せず）
- `SN: 281234123458`（一致）

米国銀行協会銀行支店コード

ABA 送金番号分類子は、クレジット カード番号分類子とほぼ同じです。

例：

- `119999992`（補足情報がないため一致せず）
- `ABA No.800000080`（一致）

運転免許証番号（米国）

米国運転免許証分類子を使用するポリシーは多数あります。デフォルトでは、この分類子は、米国で発行された運転免許証を検索します。カリフォルニア州のAB-1298およびモンタナ州のHB-732など米国の州固有のポリシーでは、それぞれの州の米国運転免許のみを検索します。

各州の分類子はその州のパターンと照合し、対応する州の名前または略称および追加の補足データを定めています。

例：

- `CA DL: C3452362`（番号と補足データのパターンが正しいため一致）
- `California DL: C3452362`（一致）
- `DL: C3452362`（補足データ不足のため一致せず）
- `California C3452362`（補足データ不足のため一致せず）
- `OR DL: C3452362`（一致）
- `OR DL: 3452362`（オレゴン州の正しいパターンのため一致）
- `WV DL: D654321`（ウェスト バージニア州の正しいパターンのため一致）
- `WV DL: G6543`（一致）

国内のプロバイダー ID（米国）

米国の国内のプロバイダー ID の分類子は、チェック デジットを含む 10 桁の数字である国家プロバイダー認証（NPI）をスキャンします。

例：

- `NPI No. 1245319599`（NPI があるため一致）
- `NPI No. 1235678996`（NPI があるため一致）
- `3459872347`（補足情報がないため一致せず）
- `NPI: 3459872342`（誤ったチェック デジットのため一致せず）

学歴（英語）

事前定義された Family Educational Rights and Privacy Act（FERPA; 家族教育権とプライバシー法）DLP ポリシーテンプレートは、生徒記録分類子を使用します。より正確に検出するため、この分類子とカスタマイズされた生徒識別番号分類子を組み合わせて、特定の生徒 ID パターンを検出します。

例：

- `Fall Semester Course Numbers: CHEM101, ECON102, MATH103`（一致）

財務諸表（英語）

事前定義された Sarbanes-Oxley（SOX）ポリシーテンプレートは、企業財務情報分類子を使用し、非公開の企業の財務情報を検索します。

例：

`Gross Profits, Current Assets, and Cash Flow Statement for the Quarter ended June 30, 2016.`（一致）

カスタム DLP ポリシーに対するコンテンツ照合分類子の作成

作成したカスタム分類子は、カスタム DLP ポリシーの作成時に使用できる分類子のリストに追加されます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	潜在的な DLP 違反を特定するためにコンテンツ照合分類子がどのように使用されているかを理解します。	参照先： • コンテンツ照合分類子を使用した拒否されたコンテンツの定義について，（10 ページ）

	コマンドまたはアクション	目的
		• コンテンツ照合分類子の例, （10 ページ）
ステップ 2	[メール ポリシー（Mail Policies）] > [DLP ポリシーのカスタマイズ（DLP Policy Customizations）] を選択し、[カスタム分類子の追加（Add Custom Classifier）] をクリックします。分類子の名前と説明を入力します。	—
ステップ 3	近接性および最小合計スコアを入力します。	参照先： 疑わしい違反のリスク要因の判別子, （18 ページ）
ステップ 4	次の検出規則タイプから 1 つを選択し、関連するコンテンツの一致基準を定義します。 • 単語またはフレーズ • ディクショナリのテキスト • 正規表現、または • 既存のデータ消失防止エンティティ	参照先： • 機密情報を特定する分類子検出ルール（カスタム DLP ポリシーのみ）, （13 ページ） • 機密 DLP 用語（カスタム DLP ポリシーのみ）のカスタム ディクショナリの使用, （16 ページ） • 識別番号を識別する正規表現, （14 ページ）
ステップ 5	（任意）[ルールの追加（Add Rule）] をクリックして、追加ルールを追加します。	重み付けや最大スコアの詳細については、疑わしい違反のリスク要因の判別子, （18 ページ）を参照してください。
ステップ 6	複数のルールを含める場合は、ルールのすべて一致といずれか一致を指定します。	この設定は、[ルール（Rules）] セクションの上部にあります。
ステップ 7	変更を送信し、保存します。	—

次の作業

カスタム DLP ポリシーでカスタム コンテンツ分類子を使用します。カスタム DLP ポリシーの作成（詳細）, （8 ページ）を参照してください。

機密情報を特定する分類子検出ルール（カスタム DLP ポリシーのみ）

コンテンツ照合分類子では、メッセージやドキュメント内の DLP 違反を検出するルールが必要となります。分類子では、次の検出ルールの 1 つ以上のルールを使用できます。

- 単語またはフレーズ（Words or Phrases）。分類子が探す単語およびフレーズの一覧。複数のエントリは、カンマまたは改行で区切ります。

- 正規表現（Regular Expression）。メッセージや添付ファイルの検索パターンを定義する正規表現。false positive を防止するため、照合から除外するパターンも定義できます。詳細については、「識別番号を識別する正規表現，（14 ページ）」と「識別番号を識別する正規表現の例，（15 ページ）」を参照してください。
- ディクショナリ.単語とフレーズに関連するディクショナリ。アプライアンスには定義済みディクショナリがあります。または独自に作成できます。機密 DLP 用語（カスタム DLP ポリシーのみ）のカスタム ディクショナリの使用，（16 ページ）を参照してください。
- エンティティ（Entity）.定義済みのパターンは、クレジット カード番号、アドレス、社会保障番号、または ABA 送金番号などの機密データの一般的なタイプを識別します。エンティティの説明については、[メール ポリシー（Mail Policies）]>[DLP ポリシー マネージャ（DLP Policy Manager）] に移動し、[DLP ポリシーの追加（Add DLP Policy）] をクリックし、[プライバシー保護（Privacy Protection）] をクリックして、[ポリシーの説明を表示（Display Policy Descriptions）] をクリックします。

識別番号を識別する正規表現

ポリシー テンプレートによっては、1 つ以上のコンテンツ照合分類子をカスタマイズする必要であり、カスタマイズには、カスタム アカウント番号、患者識別番号または生徒識別番号などの極秘情報に結び付く可能性がある識別番号を検索するための正規表現の作成があります。Perl 互換正規表現（PCRE2）構文を使用して、コンテンツ照合分類子またはDLPポリシーテンプレートに一致する正規表現を追加できます。アプライアンスでDLP機能が有効な場合にのみ、PCRE2互換の正規表現が検証されます。

（注） 正規表現では大文字と小文字は区別されるため、`[a-zA-Z]` のように大文字と小文字を含める必要があります。特定の文字のみ使用する場合は、その文字に合わせて正規表現を定義します。

8 桁の数字など、あまり特殊ではないパターンほど、ランダムな 8 桁の数字を実際の顧客番号と区別するため、追加の単語とフレーズを検索するポリシーが必要になります。

次の表を、分類子用の正規表現の作成ガイドとして使用してください。

要素	説明
正規表現（abc）	正規表現の一連の命令が文字列の一部に一致すると、分類子用の正規表現はその文字列に一致するということになります。 たとえば、正規表現 ACC は、文字列 ACCOUNT と ACCT に一致します。
[ ]	大カッコは文字のセットを示すために使用します。文字は個々または範囲で定義できます。 たとえば、[a-z] は、a から z までのすべての小文字に一致し、[a-zA-Z] は、A から Z までのすべての大文字と小文字に一致します。[xyz] は、x、y または z の文字のみに一致します。

要素	説明
バックスラッシュ特殊文字（\）	円記号は特殊文字のエスケープに使用します。シーケンス「\.」はピリオドそのもののみに一致し、「\$」はドル記号のみに一致し、「\^」はキャレット記号のみに一致します。 円記号は、「\d」などトークンの始まりともなります。 重要：円記号はパーサーでも特殊なエスケープ文字として使用します。そのため、正規表現で円記号を使用する場合、*2* つの円記号が必要です。解析後には「実際に」使用される円記号 1 つのみが残り、正規表現システムに渡されます。
\d	数字（0～9）に一致するトークン。複数の数字に一致させるには、整数を {} に入れ、数の長さを規定します。 たとえば、「\d」は、5 などの 1 桁の数字のみに一致しますが、55 には一致しません。「\d{2}」を使うと、55 などの 2 桁の数に一致しますが、5 には一致しません。
\D	数字以外の文字に一致するトークン。複数の数字以外の文字に一致させるには、{} で囲んだ整数で長さを定義します。
\w	任意の英数字と下線に一致するトークン（a ～ z、A ～ Z、0 ～ 9、および _）。
繰り返し回数 {min,max}	1 つ前のトークンの繰り返し回数を指定する正規表現表記がサポートされています。 たとえば、式「\d\{8\}」は 12345678 および 11223344 と一致しますが、8 とは一致しません。
または (|)	代替、つまり「or」演算子に相当します。「A および B」が正規表現である場合、式「A|B」は「A」または「B」のいずれかと一致する文字列と一致します。これは、正規表現で複数の数値パターンを組み合わせるために使用できます。 たとえば、「foo|bar」という表現は「foo」や「bar」とは一致しますが、「foobar」とは一致しません。

識別番号を識別する正規表現の例

識別または口座番号に数字と文字のパターンを記述する単純な正規表現には、次のように表示される可能性があります。

- 8 桁の数：`\d{8}`
- 数字のセットの間にハイフンがある識別コード：`\d{3}-\d{4}-\d`

- 大文字または小文字の英字 1 つで始まる識別コード：`[a-zA-Z]\d{7}`
- 3 桁の数字で始まり、大文字が 9 つ続く識別コード：`\d{3}[A-Z]{9}`
- | を使い、検索する 2 つの異なる数字パターンを定義：`\d{3}[A-Z]{9}|\d{2}[A-Z]{9}-\d`

機密 DLP 用語（カスタム DLP ポリシーのみ）のカスタム ディクショナリの使用

AsyncOS には、事前定義された一連のディクショナリが提供されますが、DLP スキャン機能に一致する用語を指定するカスタム DLP ディクショナリを作成することもできます。

複数の方法でカスタム DLP ディクショナリを作成できます。

- カスタム DLP ディクショナリの直接追加, （16 ページ）
- テキスト ファイルとして DLP ディクショナリを作成, （16 ページ）さらに、DLP ディクショナリのインポート, （17 ページ）。
- DLP ディクショナリのエクスポート, （17 ページ）別の E メール セキュリティ アプライアンスから。さらにDLP ディクショナリのインポート, （17 ページ）。

カスタム DLP ディクショナリの直接追加

ステップ 1 [メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）] を選択します。

ステップ 2 [詳細設定（Advanced Settings）] セクションで、[カスタム DLP 辞書（Custom DLP Dictionaries）] の側のリンクをクリックします。

ステップ 3 [辞書を追加（Add Dictionary）] をクリックします。

ステップ 4 カスタム ディクショナリの名前を入力します。

ステップ 5 用語のリストに新規ディクショナリのエントリ（単語とフレーズ）を入力します。
ディクショナリの単語は大文字と小文字が区別され、非 ASCII 文字を含めることができます。

複数のエントリを入力する場合は、改行でエントリを区切ります。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 変更を送信し、保存します。

テキスト ファイルとして DLP ディクショナリを作成

ユーザ独自のディクショナリをテキストファイルとしてローカルマシンに作成し、アプライアンスにインポートすることもできます。ディクショナリのテキスト ファイルにおける各単語には、強制改行を使用します。ディクショナリの単語は大文字と小文字が区別され、非 ASCII 文字を含めることができます。

DLP ディクショナリのエクスポート

（注） 事前定義された DLP ディクショナリはエクスポートできません。

ステップ 1 [メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）] を選択します。
ステップ 2 [詳細設定（Advanced Settings）] の [カスタム DLP 辞書（Custom DLP Dictionaries）] セクションのリンクをクリックします。
ステップ 3 [辞書をエクスポート（Export Dictionary）] をクリックします。
ステップ 4 エクスポートするディクショナリを選択します。
ステップ 5 ディクショナリのファイル名を入力します。
ステップ 6 エクスポートされたディクショナリを保存する場所（ローカル コンピュータまたはアプライアンスの configuration ディレクトリのいずれか）を選択します。
ステップ 7 ファイルのエンコード方式を選択します。
ステップ 8 [送信（Submit）] をクリックし、ファイルを保存します。

DLP ディクショナリのインポート

はじめる前に

E メール セキュリティ アプライアンスに非 DLP ディクショナリからエクスポートしたファイルをインポートする場合は、最初にテキスト ファイルから重み値を削除し、正規表現を単語または語句に変換する必要があります。

ステップ 1 [メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）] を選択します。
ステップ 2 [詳細設定（Advanced Settings）] セクションで、[カスタム DLP 辞書（Custom DLP Dictionaries）] の側のリンクをクリックします。
ステップ 3 [辞書をインポート（Import Dictionary）] をクリックします。
ステップ 4 ファイルをローカルマシンからインポートするか、アプライアンスの configuration ディレクトリからインポートするかを選択します。
ステップ 5 エンコード方式を選択します。
ステップ 6 [Next] をクリックします。
「成功」を伝えるメッセージが表示され、インポートされたディクショナリが [辞書の追加（Add Dictionary）] ページに表示されます。ただし、このプロセスはまだ完全ではありません。
ステップ 7 ディクショナリの名前を指定し、編集します。
ステップ 8 [送信（Submit）] をクリックします。

疑わしい違反のリスク要因の判別子

アプライアンスはDLP違反に対してメッセージをスキャンすると、メッセージにリスク要因スコアを割り当てます。このスコアは、メッセージにDLP違反が含まれる確率を示します。スコアが0であれば、メッセージにはほぼ確実に違反が含まれないことを意味します。スコアが100であれば、ほぼ確実に違反が含まれます。

定義済みのテンプレートに基づいたDLPポリシーについて

定義済みのテンプレートから作成されたDLPポリシーに対するリスク要因のスコアリング パラメータを表示または変更することはできません。ただし、特定DLPポリシーに大量の誤検出の一致がある場合、そのポリシーに対して重大度スケールを調整できます。違反の重大度の評価について，（20ページ）を参照してください。コンテンツ照合分類子のないテンプレート（SOX（Sarbanes-Oxley）テンプレートなど）に基づくポリシーの場合、メッセージがポリシーに違反していると、スキャン エンジンは常にリスク要因の値として「75」を返します。

カスタムDLPポリシーについて

カスタムDLPポリシーに対するコンテンツ照合分類子を作成すると、リスク要因スコアを決定するために使用される値を指定します。

- 近接性。違反と見なすには、メッセージや添付ファイルの中でルールと一致する箇所がどのくらい近くで発生する必要があるかを定義します。たとえば、長いメッセージの先頭近くに社会保障番号のような数値パターンが出現し、一番下の送信者の署名にアドレスが含まれている場合、この数値パターンとアドレスには関連性がないと見なされ、一致としてカウントされません。
- 最小総合スコア。機密情報がDLP違反として分類されるために必要な最小限のリスク要因スコア。メッセージの一致スコアが最小総合スコアに満たない場合、そのデータは機密データとして見なされません。
- 重み。作成するカスタム ルールのそれぞれに、ルールの重要度を表す「重み」を指定します。スコアは検出ルールに一致した数にルールの重みを乗算することで取得できます。重みが10のルールで違反が2つある場合は、スコアは20となります。あるルールが分類子にとって他より重要であれば、より大きい重みをアサインすることになります。
- 最大スコア。ルールの最大スコアは、多数の低い重みのルールによってスキャンの最終スコアにゆがみが生じるのを防ぎます。

リスク要因を計算するため、分類子は検出ルールに一致する数にルールの重みを乗算します。この値が検出ルールの最大スコアを超えている場合、分類子では最大スコアの値が使用されます。分類子が複数の検出ルールを持つ場合、すべての検出ルールのスコアを合計して1つの値にします。分類子は次の表にあるように、検出ルールのスコア（10～10000）を10～100の対数目盛りにマッピングし、リスク要因を算出します。

表 *1*：検出ルール スコアからのリスク要因スコアの計算方法

ルールのスコア	リスク要因
10	18
20	36
30	33
50	41
100	50
150	72
300	65
500	72
[1000]	82
10000	100

カスタム コンテンツ分類子が使用されるポリシーの表示

ステップ 1 [メール ポリシー（Mail Policies）] > [DLP ポリシーのカスタマイズ（DLP Policy Customizations）] を選択します。

ステップ 2 [カスタム分類子（Custome Classifiers）] セクションで、[カスタム分類子（Custome Classifiers）] テーブルの見出しにある [ポリシー（Policies）] をクリックします。

DLP ポリシーのメッセージのフィルタリング

パフォーマンスや精度を向上させるために、次の基準に基づいて特定のメッセージだけに適用されるように DLP ポリシーを制限できます。

オプション	説明
送信者および受信者に基づいたフィルタリング	DLP ポリシーを制限し、次のいずれかを使用して指定する送信者または受信者を含むまたは含まないメッセージに適用する。 • 完全な電子メール アドレス：`user@example.com` • 電子メール アドレスの一部：`user@` • ドメインのすべてのユーザ：`@example.com` • 部分ドメインのすべてのユーザ：`@.example.com` 改行やカンマで、複数のエントリを分離できます。 AsyncOS は最初に発信メッセージの受信者または送信者が発信メール ポリシーと一致するか照合し、次に送信者または受信者がそのメール ポリシーでイネーブルとなっている DLP ポリシーで指定した送信者および受信者フィルタと一致するか照合します。 たとえば、パートナー ドメインの受信者を除いて、すべての送信者に対し特定のタイプの情報を送信することを拒否する場合があります。パートナー ドメイン内のすべてのユーザを除外するフィルタを含め、その情報に対し DLP ポリシーを作成し、すべての送信元に適用される発信メール ポリシーにこの DLP ポリシーを含めます。
添付ファイルの種類に基づいたフィルタリング	特定の種類の添付ファイルを含むまたは含まないメッセージのみをスキャンするよう DLP ポリシーを限定できます。添付ファイルのカテゴリを選択し、次に定義済みのファイル タイプを選択するか、リストされていないファイル タイプを指定します。事前定義されていないファイル タイプを指定した場合、AsyncOS は添付ファイルの拡張子に基づいてファイル タイプを検索します。 DLP のスキャンを、最小ファイル サイズの添付ファイルに限定することができます。
メッセージ タグによるフィルタリング	DLP ポリシーを特定のフレーズを含むメッセージのスキャンに限定する場合は、メッセージまたはコンテンツ フィルタを使って発信メッセージにそのフレーズがないか検索し、カスタム メッセージ タグを当該メッセージに挿入することができます。詳細については、コンテンツ フィルタのアクションおよびメッセージ フィルタを使用した電子メール ポリシーの適用を参照してください。

違反の重大度の評価について

DLP スキャン エンジンが潜在的な DLP 違反を検出すると、そのインスタンスが実際に DLP 違反である確率を表すリスク要因スコアを計算します。ポリシーでは、リスク要因スコアをそのポリ

シーに定義されている重大度スケールと比較して、重大度レベル（たとえば、[低（Low）]、[重大（Critical）] など）を判別します。各重大度レベルでの違反に対して実行するアクションは、ユーザが指定します（ただし、[無視（Ignore）] の場合に実行されるアクションはありません）。各重大度レベルに達するために必要なリスク要因スコアは、調整することができます。

重大度スケールの調整

すべてのポリシーにはデフォルトの重大度スケールがあります。各ポリシーに対してこのスケールを調整できます。

たとえば、リスク要因スコアが 90 から 100 の場合、デフォルトで違反の重大度レベルはクリティカルになります。ただし、特定のポリシーに一致する違反についてはデータ消失の可能性があり、機密度を上げることが必要になることがあります。この DLP ポリシーには、クリティカルな重大度レベルを 75 ～ 100 のリスク要因スコアを持つ違反に変更できます。

ステップ 1 [メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）] を選択します。
ステップ 2 編集するポリシーの名前をクリックします。
ステップ 3 [重大度設定（Severity Settings）] セクションで、[スケールの編集（Edit Scale）] をクリックします。
ステップ 4 スケールの矢印を使用して、重大度レベルのスコアを調整します。
ステップ 5 [完了（Done）] をクリックします。
ステップ 6 [重大度スケール（Severity Scale）] のテーブルで、必要なときにスコアがあることを確認します。
ステップ 7 [送信（Submit）] をクリックします。

違反との一致に対する Email DLP ポリシーの順序の調整

DLP 違反が、発信メール ポリシーでイネーブルな DLP ポリシーに 1 つ以上一致する場合、リストで最初に一致した DLP ポリシーのみが使用されます。

ステップ 1 [DLP ポリシー マネージャ（DLP Policy Manager）] ページで、[ポリシーの順番の編集（Edit Policy Order）] をクリックします。
ステップ 2 移動するポリシーの行をクリックし、新しい順序の場所にドラッグします。
ステップ 3 ポリシーの順序の変更を完了したら、変更内容を送信し、確定します。

発信メール ポリシーとの DLP ポリシーの関連付け

デフォルトの発信メール ポリシーとの DLP ポリシーの関連付け

デフォルトの発信メールポリシーは、他の発信メールポリシーが送信者または受信者に一致しない場合に使用されます。

はじめる前に

データ漏洩防止の設定方法, （3 ページ）のテーブルの、ここまでのすべてのアクティビティを実行します。たとえば、デフォルトの発信メールポリシーに含めるDLPポリシーを作成したことを確認します。

ステップ 1 [メール ポリシー（Mail Policies）] > [メール ポリシー（Mail Policies）] を選択します。

ステップ 2 テーブルの [デフォルト ポリシー（Default Policy）] の行で、[DLP] の列の [ディセーブル（Disabled）] リンクをクリックします。

ステップ 3 [DLP を有効にする（設定をカスタマイズ）（Enable DLP（Customize Settings））] を選択します。

ステップ 4 デフォルトの発信メール ポリシーでイネーブルにする DLP ポリシーを選択します。

ステップ 5 変更を送信し、保存します。

次の作業

追加の発信メール ポリシーの DLP ポリシーを選択します。発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て, （22 ページ）を参照してください。

発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て

発信メールポリシーでイネーブルにすることによって、どの送信者と受信者にどのDLPポリシーを適用するかを指定します。発信メールポリシー内でDLPポリシーだけを使用することができます。

はじめる前に

デフォルトの発信メール ポリシーの DLP ポリシーを設定します。デフォルトの発信メール ポリシーとの DLP ポリシーの関連付け，（22 ページ）を参照してください。

ステップ 1 [メール ポリシー（Mail Policies）] > [メール ポリシー（Mail Policies）] を選択します。
ステップ 2 テーブルの任意の行の DLP 列のリンクをクリックします。
ステップ 3 この発信メール ポリシーに関連付ける DLP ポリシーを選択します。
ステップ 4 変更を送信します。
ステップ 5 他の発信メール ポリシーに対して、必要に応じて繰り返します。
ステップ 6 変更を保存します。

DLP ポリシーの編集または削除に関する重要な情報

操作	情報
DLP ポリシーの編集	ポリシーの名前を変更すると、発信メール ポリシーで再度イネーブルにする必要があります。
DLP ポリシーの削除	ポリシーを削除すると、DLP ポリシーが 1 つ以上の発信メール ポリシーで使用された場合に、通知を受信します。DLP ポリシーの削除により、このようなメール ポリシーからポリシーが削除されます。

[メッセージアクション（Message Actions）]

発信メッセージから DLP 違反の可能性が検出されると、E メール セキュリティ アプライアンスが実行するプライマリおよびセカンダリ アクションを指定します。さまざまなアクションに対して、異なる違反タイプおよび重大度を割り当てることができます。

プライマリ アクションは次のとおりです。

- デリバリ
- 削除
- 検疫（Quarantine）

セカンダリ アクションは次のとおりです。

- メッセージを配信する場合は、コピーをポリシー隔離に送信します。このコピーは、メッセージ ID を含む元のメッセージの完全なクローンです。コピーの隔離は、DLP 違反を監視

する別の方法を提供する他、導入前にDLPシステムをテストすることができます。隔離からコピーをリリースすると、アプライアンスはすでに元のメッセージを受信した受信者にコピーを配信します。

- メッセージの暗号化このアプライアンスは、メッセージ本文だけを暗号化します。メッセージ ヘッダーは暗号化されません。
- DLP 違反があるメッセージの件名ヘッダーの変更
- メッセージへの免責事項の追加。
- 代替宛先メールホストへのメッセージの送信。
- 他の受信者にメッセージのコピー（bcc）の送信。（たとえば、重大な DLP 違反があるメッセージを調べてもらうために、そのメッセージをコンプライアンス担当者のメールボックスにコピーできます）。
- DLP 違反の通知メッセージを、送信者や、マネージャまたは DLP コンプライアンス責任者といった他の連絡先に送信します。DLP 通知のドラフト，（26 ページ）を参照してください。

（注） これらのアクションは相互排他的ではなく、各ユーザ グループのさまざまな要求を処理するために、異なるDLPポリシー内でアクションをいくつか組み合わせることができます。また、同じポリシーの異なる重大度レベルに基づいて別の処理を設定できます。たとえば、重大なDLP違反を含むメッセージを隔離し、コンプライアンス担当者に通知を送信しますが、重大度レベルの低いメッセージを配信することもできます。

DLP違反アクション（メッセージアクション）に対して実行するアクションの定義

はじめる前に

- DLPポリシーに違反したメッセージ（またはメッセージのコピー）を保持する専用隔離を少なくとも 1 つ作成します。

  これは、電子メール セキュリティ アプライアンスの内部隔離またはセキュリティ管理アプライアンスの集中型隔離に指定できます。

  詳細については、次の資料を参照してください。 集約されたポリシー、ウイルス、およびアウトブレイク隔離
- 配信前にメッセージを暗号化する場合は、暗号化プロファイルを設定してください。参照先： Cisco Email Encryption
- DLP違反またはその疑いがあるメッセージを配信する場合、免責事項を含めるには、[メールポリシー（Mail Policies）] > [テキスト リソース（Text Resources）] で、免責事項のテキストを指定します。詳細については、次の資料を参照してください。 免責事項テンプレート

- DLP違反の送信者またはコンプライアンス責任者などの他の人に通知を送信するには、まずDLP 通知テンプレートを作成します。DLP 通知のドラフト，（26 ページ）を参照してください。

ステップ 1 [メール ポリシー（Mail Policies）] > [DLP ポリシーのカスタマイズ（DLP Policy Customizations）] を選択します。

ステップ 2 [メッセージ アクション（Message Actions）] セクションで [メッセージ アクションの追加（Add Message Action）] をクリックします。

ステップ 3 メッセージ アクションの名前を入力します。

ステップ 4 メッセージ アクションの説明を入力します。

ステップ 5 DLP 違反を含むメッセージをドロップ、配信、または隔離するか選択します。

（注） [配信（Deliver）] を選択すると、ポリシー隔離に送信されたメッセージのコピーを取ることを選択できます。メッセージのコピーはメッセージ ID を含む完全なクローンです

ステップ 6 配信にメッセージの隔離からリリースを暗号化する場合は、[暗号化を有効にする（Enable Encryption）] チェックボックスを選択して、次のオプションを選択します。

- [暗号化ルール（Encryption Rule）]。メッセージを常に暗号化するか、TLS 接続を介した送信試行が最初に失敗した場合だけ暗号化します。
- [暗号化プロファイル（Encryption Profile）]。Cisco IronPort 暗号化アプライアンスまたはまたはホステッド キー サービスを使用する場合、指定した暗号化プロファイルを使用してメッセージを暗号化し、配信します。
- [暗号化されたメッセージの件名（Encrypted Message Subject）]。暗号化されたメッセージの件名です。既存のメッセージ件名を保持するには、$Subject の値を使用します。

ステップ 7 アクションとして隔離を選択した場合は、DLP違反を含むメッセージに使用するポリシー隔離を選択します。

ステップ 8 次のオプションのいずれかを使用してメッセージを変更する場合は、[詳細（Advanced）]をクリックします。

- カスタム ヘッダーを追加します。
- メッセージの件名を変更します。
- 代替ホストに配信します
- 他の受信者にコピー（bcc）を送信します
- DLP 通知メッセージを送信します。

ステップ 9 変更を送信し、保存します。

メッセージ アクションの表示および編集

ステップ 1 [メール ポリシー（Mail Policies）] > [DLP ポリシーのカスタマイズ（DLP Policy Customizations）] を選択します。

ステップ 2 [メッセージ アクション（Message Actions）] セクションでアクションを選択します。

目的	操作内容
各アクションが割り当てられているメール ポリシーを表示します。	メッセージ アクション表の見出しで [ポリシー（Policies）] のリンクをクリックします。
アクションごとに入力した説明を表示します。	メッセージ アクション表の見出しで [説明（Description）] のリンクをクリックします。
メッセージ アクションの詳細を表示または編集します。	メッセージ アクションの名前をクリックします。
メッセージ アクションを削除します。	削除対象のメッセージ アクションの横にあるゴミ箱のアイコンをクリックします。 確認メッセージは、1 つ以上の DLP ポリシーでメッセージ アクションが使用されているかどうかを通知します。
メッセージ アクションを複製します。 この機能は、メッセージ アクションを変更する前にバックアップ コピーを作成するか、または新たな、または類似のメッセージ アクションの出発点として使用するために使用できます。	複製するメッセージ アクションの横にある [重複（Duplicate）] アイコンをクリックします。

ステップ 3 変更を送信し、確定します。

DLP 通知のドラフト

以下の手順に従って、組織のデータ漏洩防止ポリシーに違反する情報がメール メッセージに含まれている場合に送信する通知のテンプレートを作成します。この通知は、DLP ポリシーに違反しているメッセージの送信者、または別のアドレス（マネージャまたは DLP コンプライアンス責任者）に送信できます。

はじめる前に

- DLP 通知テンプレートの変数の定義, （27 ページ） の内容についてよく理解しておきます。各違反についての詳細を含む通知をカスタマイズするためにこれらの変数を使用できます。

ステップ 1 [メール ポリシー（Mail Policies）] > [テキスト リソース（Text Resources）] を選択します。

ステップ 2 [テキスト リソースを追加（Add Text Resource）] をクリックします。

ステップ 3 [タイプ（Type）] に、[DLP 通知テンプレート（DLP Notification Template）] を選択します。
DLP 変数は通常の通知テンプレートでは利用可能ではありません。

ステップ 4 通知テキストおよび変数を入力します。
この通知で受信者に対し、発信メッセージに組織のデータ漏洩防止ポリシーに違反する機密データが含まれている可能性があることを知らせる必要があります。

次の作業

DLP Policy Manager の DLP ポリシーで [メッセージ アクション（Message Action）] にこの DLP 通知テンプレートを指定します。

DLP 通知テンプレートの変数の定義

通知に、各 DLP 違反に関する特定の情報を含めるには、次の変数を使用します。

変数	置き換える値
$DLPPolicy	違反があった Email DLP ポリシーの名前に置き換えられます。
$DLPSeverity	違反の重大度に置き換えられます。値は [低（Low）]、[中（Medium）]、[高（High）]、または [重大（Critical）] のいずれかです。
$DLPRiskFactor	メッセージの機密内容のリスク要因スコアに置き換えられます（スコア 0 ～ 100）。
$To	メッセージの To: ヘッダーに置き換えられます（エンベロープ受信者には置き換えられません）。
$From	メッセージの From: ヘッダーに置き換えられます（エンベロープ送信者には置き換えられません）。
$Subject	元のメッセージの件名に置き換えられます。

変数	置き換える値
$Date	現在の日付（MM/DD/YYYY 形式）に置き換えられます。
$Time	現在の時刻（ローカル時間帯）に置き換えられます。
$GMTimestamp	現在の時刻および日付（GMT）に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。
$MID	メッセージを内部で識別するために使用するメッセージ ID（MID）に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください（「Message-Id」を取得するには $Header を使用します）。
$Group	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
$Reputation	送信者の SenderBase レピュテーション スコアに置き換えられます。レピュテーション スコアがない場合は「None」に置き換えられます。
$filenames	メッセージの添付ファイルのファイル名のカンマ区切リストに置き換えられます。
$filetypes	メッセージの添付ファイルのファイル タイプを示すカンマ区切りリストに置き換えられます。
$filesizes	メッセージの添付ファイル サイズのカンマ区切りリストに置き換えられます。
$remotehost	メッセージを Cisco アプライアンスに送信したシステムのホスト名に置き換えられます。
$AllHeaders	メッセージ ヘッダーに置き換えられます。
$EnvelopeFrom	メッセージのエンベロープ送信者（Envelope From、<MAIL FROM>）に置き換えられます。
$Hostname	Cisco アプライアンスのホスト名に置き換えられます。

変数	置き換える値
$bodysize	メッセージのサイズ（バイト単位）に置き換えられます。
$header[‘*string* ’]	元のメッセージに一致するヘッダーが含まれる場合、引用符付きヘッダーの値に置き換えられます。二重引用符が使用される場合もあります。
$remoteip	メッセージを Cisco アプライアンスに送信したシステムの IP アドレスに置き換えられます。
$recvlistener	メッセージを受信したリスナーのニックネームに置き換えられます。
$dropped_filenames	$filenames と同様に、ドロップされたファイルのリストを表示します。
$dropped_filename	直近にドロップされたファイル名のみを返します。
$recvint	メッセージを受信したインターフェイスのニックネームに置き換えられます。
$timestamp	現在の時刻および日付（ローカル時間帯）に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。
$Time	現在の時刻（ローカル時間帯）に置き換えられます。
$orgid	SenderBase 組織 ID（整数値）で置き換えられます。
$enveloperecipients	メッセージのエンベロープ受信者すべて（Envelope To、<RCPT TO>）に置き換えられます。
$dropped_filetypes	$filetypes と同様に、ドロップされたファイルタイプのリストを表示します。
$dropped_filetype	直近にドロップされたファイルのファイルタイプのみを返します。

メッセージ トラッキングでの機密性の高い DLP データの表示

DLP 導入では、DLP ポリシーに違反するコンテンツを、周囲のコンテンツとともにログに記録するオプションが提供され、これは後でメッセージ トラッキングで表示できます。この内容は、クレジット カード番号や社会保障番号などの機密データを含む場合があります。

はじめる前に

メッセージ トラッキングをイネーブルにします。参照先： メッセージ トラッキングの有効化

ステップ 1 [セキュリティ サービス（Security Services）] > [データ損失の防止（Data Loss Prevention）] の順に選択します。

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

ステップ 3 [一致したコンテンツのログへの記録（Enable Matched Content Logging）] チェックボックスを選択します。

ステップ 4 変更を送信し、保存します。

次の作業

この情報を表示できる管理者ユーザを指定します。メッセージ トラッキングでの機密情報へのアクセスの制御を参照してください。

DLP エンジンおよびコンテンツ照合分類子の更新について

Cisco DLP エンジンとアプライアンスの定義済みコンテンツ照合分類子の更新は別のセキュリティ サービスの更新に依存しません。

DLP エンジンの現在のバージョンの決定

ステップ 1 [セキュリティ サービス（Security Services）] > [データ損失の防止（Data Loss Prevention）] の順に選択します。

ステップ 2 [最新 DLP バージョン ファイル（Current DLP Version Files）] のセクションを参照してください。

（注） また、`dlpstatus` CLI コマンドを使用して、DLP エンジンの現在のバージョンを表示することもできます。詳細については、『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

DLP エンジンとコンテンツ照合分類子の手動による更新

はじめる前に

その場合は、次のトピックを参照してください。

- （該当する場合）一元化された（クラスタ化された）アプライアンスの DLP 更新, （32 ページ）

ステップ 1 [セキュリティ サービス（Security Services）] > [データ損失の防止（Data Loss Prevention）] の順に選択します。

ステップ 2 [最新 DLP バージョンファイル（Current DLP Version Files）] セクションで [今すぐ更新（Update Now）] をクリックします。
このボタンは、ダウンロード可能な新規アップデートがある場合にだけ使用できます。

（注） DLP エンジンを更新するには、`dlpupdate` CLI コマンドも使用できます。詳細については、『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

自動アップデートの有効化（推奨されません）

アプライアンスが定期的に更新をチェックし、ダウンロードすることを有効にするには、この手順を使用します。

（注） シスコは、自動更新を使用しないことを推奨します。これらの更新は、DLP ポリシーで使用されるコンテンツ照合分類子を変更する場合があります。代わりに、手動で DLP 更新をダウンロードし、実稼働環境で使われるアプライアンスを更新する前に、ラボ環境でテストします。

はじめる前に

- [セキュリティ サービス（Security Services）] > [サービスのアップデート（Service Updates）] ページで、自動アップデートをイネーブルにし、すべてのサービス契約更新に更新間隔を指定してください。

- 一元化された（クラスタ化された）アプライアンスの DLP 更新, （32 ページ）を参照してください。

ステップ 1 [セキュリティ サービス（Security Services）] > [データ損失の防止（Data Loss Prevention）] の順に選択します。

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

ステップ 3 [自動アップデートを有効にする（Enable automatic updates）] チェックボックスを選択します。

ステップ 4 変更を送信し、保存します。

一元化された（クラスタ化された）アプライアンスの DLP 更新

次の点に注意してください。

- クラスタ化された導入でのアプライアンスでは、自動 DLP 更新を有効にできません。
- DLP の更新は、クラスタ、マシンまたはグループ レベルで設定されている DLP に関係なく、マシン レベルで常に実行されます。
- マシン レベルで dlpstatus CLI コマンドを使用したときのみ、アプライアンスの DLP エンジンの状態をチェックできます。

DLP インシデントのメッセージとデータの使用

（注） 導入が該当する場合は、セキュリティ管理アプライアンスに関するドキュメントも参照してください。

目的	操作内容
DLP ポリシー名、違反の重大度、行われるアクションなどの基準を使って DLP 違反が含まれるメッセージを検索し、検出されたメッセージの詳細情報を表示します。	メッセージ トラッキングを参照してください。
疑わしい DLP 違反として隔離されたメッセージを表示または管理できます。	ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作を参照してください。
DLP インシデントのサマリーを表示します。	DLP インシデント サマリー レポートについては、電子メール セキュリティ モニタの使用方法を参照してください。

目的	操作内容
発信メールで検出された DLP 違反に関する情報を表示します。	DLP インシデント レポートについては、電子メール セキュリティ モニタの使用方法を参照してください。

トラブルシューティング データ消失防止

DLP が電子メールの添付ファイルの違反を検出しない

問題

定義済みの DLP ポリシーを使用すると、DLP は電子メールの添付違反を検出しません。次の原因が考えられます。

- 定義済みの DLP ポリシーのプロキシミティ パラメータの値が小さい

（注） 定義済みの DLP ポリシーのプロキシミティは変更できません。

- 定義済みの DLP ポリシーで定義されている重大度スケール パラメータが大きい

ソリューション

- カスタム ポリシーを作成し、プロキシミティを必要に応じて調整します。参照先： カスタム DLP ポリシーの作成（詳細）, （8 ページ）
- 定義済みの DLP ポリシーの重大度スケール パラメータを小さくします。参照先： 重大度スケールの調整, （21 ページ）