CHAPTER 11

データ消失防止

情報化時代では、組織のデータが組織の最も大切な財産の 1 つです。組織では多額の費用をかけ、従業員、顧客、パートナーがデータを利用できるようにしています。データは電子メールと Web を通して絶え間なく行き交っています。このようにデータ アクセスが増加したため、機密情報や占有情報の悪意または過失による消失をどのように防止するかの答えを見つけ出すことは、情報セキュリティの専門家にとって難問となっています。

IronPort 電子メール セキュリティ アプライアンスは、統合 Data Loss Prevention（DLP; データ損失防止）スキャン エンジンと RSA Security Inc. の DLP ポリシー テンプレートにより、機密データの識別と保護を行い、データの安全を確保します。RSA Email DLP 機能により、ユーザが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。従業員が電子メールで送付してもよいデータの種類と、機密情報を含むメッセージの検疫やコンプライアンス責任者への通知などアプライアンスが講じるアクションを定義します。

RSA Email DLP スキャンは、イネーブルになっていれば、ウイルス感染フィルタの段階の直後にアプライアンスの「ワーク キュー」で発信メールに対して実行されます。詳細については、「メッセージ分裂」（P.6-194）を参照してください。

この章は、次の内容で構成されています。

- 「コンテンツ照合分類子用の正規表現」（P.11-389）
- 「高度な DLP ポリシーのカスタマイズ」（P.11-391）
- 「RSA Email DLP の受信者ごとのポリシーの設定」（P.11-394）

Email DLP の動作を理解する

RSA Email DLP 機能では、3 段階のポリシー構造を使って、組織のデータ損失防止ルールと、メッセージがそのルールに違反したときに IronPort アプライアンスが講じるアクションを定義します。

- **検出ルール。**最も低いレベルの場合、DLP コンテンツ スキャンは、テキストのブロック内に特定のパターンがないかスキャンする*検出ルール*で構成されています。これらの検出ルールには、正規表現、単語やフレーズ、ディクショナリ、スマート ID に似たエンティティなどがあります。
- **コンテンツ照合分類子。**次のレベルは*コンテンツ照合分類子*で、発信メッセージと添付ファイルにクレジット カード データや他の個人データなどの機密情報がないかスキャンします。分類子には、さらなる条件を適用するコンテキスト ルールを伴う検出ルールが多数あります。例として、RSA が開発したクレジット カード番号分類子を検討します。この分類子は、メッセージがクレジット カード番号のパターンに一致するテキスト文字列を含むだけではなく、有効期限、クレジット カード会社（Visa、AMEX など）、名前および住所などの補足情報も含むように定めています。この追加情報を必須とすることで、メッセージ コンテンツの判断がより正確となり、false positive も少なくなります。分類子が、メッセージ内に組織の DLP ルールに違反している機密情報を検出すると、*DLP 違反*が発生します。
- **DLP ポリシー。**最も高いレベルは、*DLP ポリシー*で、条件のセットとアクションのセットからなります。条件には、送信者、受信者、添付ファイルのタイプなどの、メッセージのコンテンツに対する分類子とメッセージ メタデータのテストが含まれます。アクションでは、メッセージに対する全体的なアクション（配信、ドロップ、または検疫）、およびメッセージの暗号化、コピー、ヘッダーの変更、通知の送信といった二次的なアクションの両方を指定します。

DLP Policy Manager で組織の DLP ポリシーを定義し、発信メール ポリシーでそのポリシーをイネーブルにします。「ワーク キュー」のウイルス感染フィルタの段階の後で、アプライアンスは DLP ポリシー違反がないか発信メッセージをスキャンします。AsyncOS の DLP Assessment Wizard を使うと、最もよく使われる DLP ポリシーが簡単に設定できます。詳細については、「DLP Assessment

Wizard の使用」（P.11-377）を参照してください。

RSA Email DLP スキャン エンジンは、発信メール ポリシーでイネーブルになっている DLP ポリシーの分類子をすべて使って、各メッセージと添付ファイルをスキャンします。添付ファイルをスキャンするために、IronPort アプライアンスのコンテンツ スキャン エンジンが添付ファイルを抽出し、RSA Email DLP スキャン エンジンがその内容をスキャンします。スキャンが完了すると、RSA Email DLP エンジンが、イネーブルになっている DLP ポリシーのいずれかに対してメッセージが違反していないか確認します。違反が複数の DLP ポリシーに一致している場合、RSA Email DLP エンジンは、発信メール ポリシーのリストを上から順に調べ、最初に一致する DLP ポリシーを選択します。DLP Policy Manager で DLP ポリシーの順序を定義します。

RSA Email DLP エンジンは、最初に DLP 違反のリスク要因スコアを計算することで、メッセージの取り扱い方を決定します。リスク要因スコアは、DLP 違反の重大度を 0 ～ 100 の範囲で示します。RSA Email DLP エンジンは、リスク要因スコアを DLP ポリシー用に定義されている重大度基準と比較します。重大度基準は、想定される DLP 違反を次の重大度レベルの 1 つに区分します。

- Ignore
- Low
- Medium
- High
- Critical

重大度レベルにより、メッセージに適用されるアクション（設定されていれば）が決まります。

DLP インシデント レポートを使って、発信メールで発生した DLP 違反の情報を見ることができます。また、メッセージ トラッキングを使って、DLP 違反の重大度をもとにしたメッセージの検索もできます。

- DLP 電子メール ポリシーおよびコンテンツ照合分類子の詳細については、「DLP ポリシー」（P.11-366）を参照してください。
- コンテンツ照合分類子の詳細については、「コンテンツ 照合分類子」（P.11-382）を参照してください。
- DLP インシデント レポートの詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」の章を参照してください。

- メッセージ トラッキングでの、DLP 違反があるメッセージの検索については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Tracking Email Messages」の章を参照してください。

（注）　スキャン エンジンは、メッセージのスキャン時に分類子を 1 回だけ使用します。1 つの発信メール ポリシーに同じ分類子を使う 2 つ以上の DLP ポリシーがある場合、すべてのポリシーは分類子の 1 回のスキャンの結果を使用します。

ハードウェア要件

RSA Email DLP 機能は、すべての C-Series および X-Series アプライアンスでサポートされます。ただし、C10、C30、C60、C100、C300D、C350D および C360D は除きます。

RSA Email DLP グローバル設定

機密データがないか発信電子メールをスキャンするには、[Security Services] > [RSA Email DLP] ページを使って、最初にアプライアンス上で RSA Email DLP スキャンをイネーブルにします。DLP Assessment Wizard を起動して、最もよく使われる DLP ポリシーをアプライアンス上でイネーブルにするか、手動で RSA Email DLP 機能をイネーブルにするか選択できます。

DLP Assessment Wizard の起動方法については、「DLP Assessment Wizard の使用」（P.11-377）を参照してください。RSA Email DLP を手動でイネーブルにする方法については、「RSA Email DLP のイネーブル化とグローバル設定の設定」（P.11-365）を参照してください。

RSA Email DLP をイネーブルにすると、DLP Policy Manager で DLP ポリシーおよびアクションを設定し、電子メール セキュリティ マネージャを使って発信メール ポリシーでそのポリシーとアクションをイネーブルにすることができます。詳細については、「DLP ポリシー」（P.11-366）および「RSA Email DLP の受信者ごとのポリシーの設定」（P.11-394）を参照してください。

RSA Email DLP のイネーブル化とグローバル設定の設定

（注）　DLP Assessment Wizard を使って、アプライアンスの DLP ポリシーを設定するには、「DLP Assessment Wizard の使用」（P.11-377）を参照してください。

RSA Email DLP をアプライアンスでイネーブルにするには、次の手順に従います。

ステップ 1　[Security Services] > [RSA Email DLP] を選択します。

ステップ 2　[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が表示されます。

（注）　ライセンス契約に合意しない場合、RSA Email DLP はアプライアンス上でイネーブルになりません。

ステップ 4　ページの下部までスクロールし、[Accept] をクリックしてライセンス契約に合意します。

ステップ 5　[Enable] をクリックします。

RSA Email DLP がアプライアンス上でイネーブルとなります。

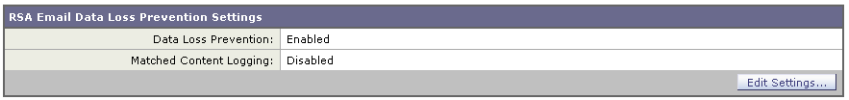
ステップ 6　[Edit Settings] をクリックします。

[Edit RSA Email Data Loss Prevention Global Settings] ページが表示されます。

ステップ 7　メッセージ トラッキングがアプライアンス上ですでにイネーブルになっている場合は、一致したコンテンツのログへの記録をイネーブルにするかしないか選択します。これを選択すると、IronPort アプライアンスは DLP 違反をログに記録し、AsyncOS は DLP 違反および周辺コンテンツをメッセージ トラッキングに表示します。その中には、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が含まれます。

ステップ 8　変更を送信して確定します。

図 11-1　RSA Email Data Loss Prevention のイネーブル化



DLP ポリシー

DLP ポリシーは、発信メッセージが機密データとアクションを含んでいるか AsyncOS および RSA Email DLP スキャン エンジンが判断するために使う条件と、メッセージにそのようなデータが含まれている場合 AsyncOS が講じるアクションとを組み合わせたものです。

DLP ポリシーには、RSA が開発したコンテンツ照合分類子が含まれます。分類子は、RSA Email DLP スキャン エンジンによって、メッセージおよび添付ファイル内の機密データ検出のため、使用されます。分類子は、クレジット カード番号や運転免許 ID のようなデータ パターンを探すだけでなく、パターンのコンテキストも検査するため false positive が少なくなります。詳細については、「コンテンツ 照合分類子」（P.11-382）を参照してください。

DLP スキャン エンジンが、メッセージや添付ファイルで DLP 違反を検出すると、DLP スキャン エンジンは、違反のリスク要因を決定し、その結果をマッチング DLP ポリシーに返します。ポリシーは、独自の重大度基準を使ってリスク要因をもとに DLP 違反の重大度を評価し、メッセージに対して適切なアクションを適用します。その基準には、Ignore、Low、Medium、High、Critical の 5 つの重大度レベルがあります。

Ignore 以外のすべてのセキュリティ レベルで講じることができるアクションには次のものがあります。

- 検査中のメッセージに適用する、配信、ドロップ、検疫といった全体的なアクション。
- メッセージの暗号化。
- 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。
- メッセージの代替送信先メールホストへの送信。
- メッセージのコピー（bcc）の他の受信者への送信（たとえば、重大な DLP 違反を含むメッセージのコピーを、以降の検査のためにコンプライアンス責任者のメールボックスに送信します）。

- 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。

（注）これらのアクションは相互排他的ではなく、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。同一ポリシー内で重大度レベルに応じて異なる対応になるように設定することも可能です。たとえば、重大な違反を含むメッセージは検疫し、コンプライアンス責任者に通知を送信しますが、重大度レベルが低いメッセージは配信する、といったことです。

ポリシーのコンテンツ

Email DLP ポリシーには次の情報が含まれます。

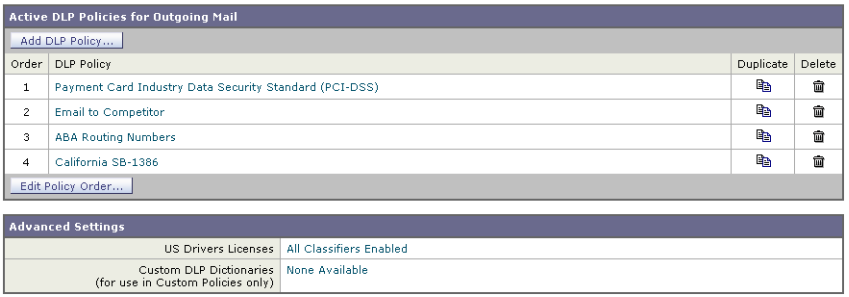
- ポリシーの名称と説明。
- コンテンツ照合分類子の一覧。ポリシーによっては、識別番号を検索する正規表現の作成が必須の場合があります。詳細については、「コンテンツ 照合分類子」（P.11-382）を参照してください。
- メッセージ フィルタリング用の特定の送信者および受信者のリスト。詳細については、「送信者および受信者のフィルタリング」（P.11-374）を参照してください。
- メッセージ フィルタリング用の添付ファイルのタイプ一覧。詳細については、「添付ファイルのフィルタリング」（P.11-375）を参照してください。
- 重大度の設定。設定に適用されるアクションおよび重大度基準の調整を含みます。詳細については、「重大度レベルの設定」（P.11-375）を参照してください。

DLP Policy Manager

DLP Policy Manager は、IronPort アプライアンス上で Email DLP ポリシーをすべて管理する単一のダッシュボードです。DLP Policy Manager は [Mail Policies] メニューからアクセスします。DLP Policy Manager から、次のアクションを実行できます。

- 事前定義されたテンプレートをもとにした DLP ポリシーの作成および管理。詳細については、「事前定義されたテンプレートをもとにした Email DLP ポリシーの作成」（P.11-371）を参照してください。
- カスタム テンプレートをもとにした DLP ポリシーの作成および管理。詳細については、「Custom Policy テンプレートを使用した DLP ポリシーの作成」（P.11-392）を参照してください。
- カスタム DLP ディクショナリの作成、インポートおよび管理。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Text Resources」の章を参照してください。
- 米国運転免許証分類子の管理。詳細については、「米国運転免許証分類子」（P.11-370）を参照してください。

図 11-2　アクティブな DLP ポリシーがある DLP Policy Manager

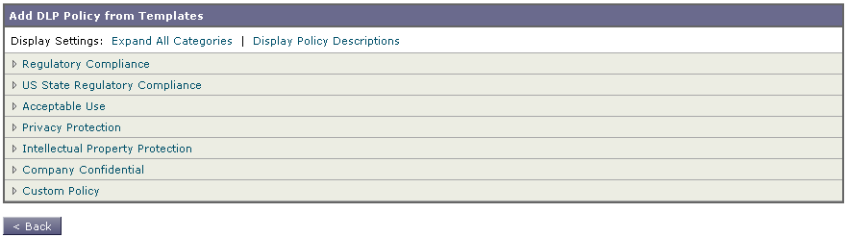


RSA Email DLP ポリシー テンプレート

AsyncOS には、組織の知的財産や極秘情報を保護する、RSA の開発による事前定義されたポリシー テンプレートが多数あり、法や業界標準で規定されているルールや規制を強制的に適用します。DLP Policy Manager を使って DLP ポリシーを作成するときには、最初に使用するテンプレートを選択します。

図 11-3 は、使用可能な DLP ポリシー テンプレートのカテゴリを示しています。

図 11-3　テンプレートから DLP ポリシーを追加



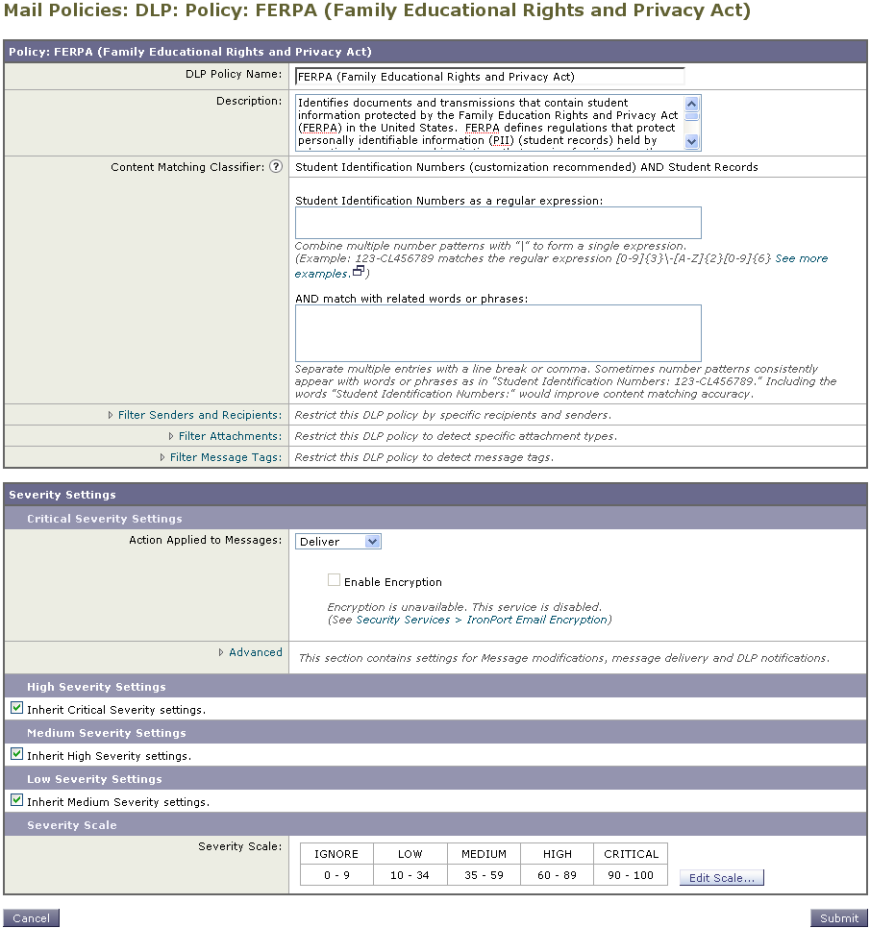
DLP ポリシー テンプレートは次のカテゴリに整理されます。

- **[Regulatory Compliance]。**個人情報、クレジット情報、他の保護情報や非公開情報を含むメッセージおよび添付ファイルを識別します。
- **[Acceptable Use]。**競合他社や制限された受信者に送信するメッセージで、組織に関する機密情報を含むものを識別します。
- **[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。
- **[Intellectual Property Protection]。**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。
- **[Company Confidential]。**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。
- **[Custom Policy]。**AsyncOS では、RSA や組織で開発された分類子を使って、独自のポリシーをゼロから作成するオプションもあります。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。詳細については、「高度な DLP ポリシーのカスタマイズ」（P.11-391）を参照してください。

カスタマイズが必要な DLP ポリシー テンプレートについては、「DLP ポリシーに対する分類子のカスタマイズ」（P.11-372）を参照してください。

図 11-4 に、Family Educational Rights and Privacy Act（FERPA; 家族教育権とプライバシー法）違反を検出する、事前定義された RSA ポリシー テンプレートを示します。

図 11-4　事前定義された RSA Email DLP ポリシー テンプレート



米国運転免許証分類子

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 50 州すべておよびコロンビア特別区の運転免許を検索します。カルフォルニア州の 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、51 タイプすべての運転免許を検索します。false positive またはアプライアンスのパフォーマンスが問題となるようであれば、DLP Policy Manager の [Advanced Settings] の下の米国運転免許証用のリンクをクリックして、検索を特定の米国の州に限定する、またはどの州も検索しないようにできま

す。RSA スキャン エンジンが運転免許分類子をどのように使用するかについては、「米国運転免許証」（P.11-387）参照してください。

事前定義されたテンプレートをもとにした Email DLP ポリシーの作成

DLP ポリシーは、事前定義されたテンプレートまたはカスタム テンプレートのいずれかを使用して、作成可能です。カスタム テンプレートの使用方法については、「Custom Policy テンプレートを使用した DLP ポリシーの作成」（P.11-392）を参照してください。

事前定義されたテンプレートをもとにした DLP ポリシーを追加する方法。

ステップ 1　[Mail Policies] > [DLP Policy Manager] を選択します。

ステップ 2　[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 RSA Email DLP ポリシー テンプレートの一覧を表示します。

（注）　[Display Policy Descriptions] をクリックして、使用可能なポリシー テンプレートの詳細な説明を表示することができます。

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

図 11-4（P.11-370）とほぼ同じページが開きます。事前定義されたテンプレートすべてに名前と説明がありますが、変更できます。テンプレートのほとんどには 1 つ以上の分類子があり、いくつかのテンプレートには事前定義された添付ファイルのタイプがあります。

ステップ 5　ポリシーが、カスタマイズされた分類子を必要とする場合は、組織の識別番号付けシステムのパターンと、識別番号に関連する単語やフレーズの一覧を定義するための正規表現を入力します。詳細については、「DLP ポリシーに対する分類子のカスタマイズ」（P.11-372）を参照してください。

（注）　事前定義されたテンプレートをもとにしたポリシーでは、分類子の追加および削除はできません。

ステップ 6　任意で、DLP ポリシーの適用を、特定の受信者や送信者、添付ファイルのタイプやメッセージ タグを持つメッセージに限定することができます。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」（P.11-374）を参照してください。

ステップ 7　[Critical Settings] セクションで、重大な DLP 違反を含むメッセージをドロップ、配信、または検疫するか選択します。

ステップ 8　任意で、メッセージの暗号化、ヘッダーの修正、代替ホストへのメッセージの送信、別の受信者へのコピーの配信（bcc）、DLP 通知メッセージの送信を選択できます。

DLP 通知については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Text Resources」の章を参照してください。

ステップ 9　一致する重大度レベルが High、Medium、Low のメッセージに、別々の設定を定義するときは、適切なセキュリティ レベルの [Inherit settings] チェックボックスをオフにします。メッセージへの全体的なアクションや他の設定を編集します。

ステップ 10　ポリシーに対して DLP 違反の重大度基準を調整する場合は、[Edit Scale] をクリックして設定を調整します。詳細については、「重大度レベルの設定」（P.11-375）を参照してください。

ステップ 11　変更を送信して確定します。

ポリシーが DLP Policy Manager に追加されます。

DLP ポリシーに対する分類子のカスタマイズ

DLP ポリシー テンプレートには、より効果的にするためカスタマイズされた分類子を必要とするものもあります。このような分類子は、発信メッセージ内に患者や学生の識別番号など極秘の識別番号がないか検索しますが、組織の記録番号付けシステムのパターンを定義する正規表現を 1 つ以上必要とします。補足情報の記録識別番号に関連する単語およびフレーズの一覧を追加することもできます。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。これにより、false positive が少なくなります。

たとえば、Health Insurance Portability and Accountability Act（HIPAA; 医療保険の相互運用性と説明責任に関する法律）テンプレートを使ってポリシーを作成するとします。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。この分類子に正規表現 `[0-9]{3}\-[A-Z]{2}[0-9]{6}` を入力します。この正規表現

では、123-CL456789 というパターンの番号が検出されます。関連フレーズとして「Patient ID」を入力します。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。変更を送信して確定します。これで、ポリシーが発信メッセージ内の番号のパターンを検出し、その近くに「Patient ID」というフレーズがある場合、ポリシーは DLP 違反を返すようになります。

次の DLP ポリシー テンプレートには、カスタマイズ可能なコンテンツ照合分類子があります。

- **Health Insurance Portability and Accountability Act（HIPAA; 医療保険の相互運用性と説明責任に関する法律）。**患者識別番号分類子はカスタマイズ可能ですが、必須ではありません。患者識別番号分類子または患者 ID および HIPAA ディクショナリ分類子に一致すると、DLP 違反を返します。
- **Family Educational Rights and Privacy Act（FERPA; 家族教育権とプライバシー法）。**生徒識別番号分類子のカスタマイズが必要です。生徒識別番号および生徒記録分類子に一致すると、DLP 違反となります。
- **Gramm-Leach Bliley Act（GLBA; グラム リーチ ブライリー法）。**カスタム アカウント番号分類子はカスタマイズ可能ですが、必須ではありません。次の分類子に 1 つ以上一致すると、DLP 違反となります。カスタム アカウント番号、米国運転免許証、クレジット カード番号または米国社会保障番号。
- **California AB-1298。**グループ保険番号、医療記録番号、患者識別番号分類子はカスタマイズ可能ですが、必須ではありません。次の分類子に 1 つ以上一致すると、DLP 違反となります。グループ保険番号、医療記録番号、患者識別番号、米国運転免許証、患者 ID、クレジット カード番号、HIPAA ディクショナリ。
- **Massachusetts CMR-201**。米国銀行口座番号分類子はカスタマイズ可能ですが、必須ではありません。次の分類子に 1 つ以上一致すると、DLP 違反になります。米国銀行口座番号、米国運転免許証、クレジット カード番号、米国社会保障番号、ABA ルーティング番号分類子。このポリシー テンプレートは、AsyncOS 7.1.1 以降で使用可能です。
- **カスタム アカウント番号。**カスタム アカウント番号分類子のカスタマイズが必須です。カスタム アカウント番号分類子に一致すると DLP 違反となります。
- **患者識別番号。**患者識別番号分類子はカスタマイズ可能ですが、必須ではありません。患者識別番号または患者 ID 分類子に一致すると、DLP 違反になります。

- **合併および買収。**合併および買収コード名分類子のカスタマイズには、単語またはフレーズの一覧を使いますが、必須ではありません。正規表現を使う必要ありません。合併および買収コード名または合併キーワード分類子に一致すると DLP 違反になります。

正規表現の作成方法については、「コンテンツ照合分類子用の正規表現」（P.11-389）を参照してください。コンテンツ照合分類子がどのようにして DLP 違反を検出するかの詳細については、「コンテンツ 照合分類子」（P.11-382）参照してください。

DLP ポリシーのメッセージのフィルタリング

AsyncOS が検出した特定の情報に基づいて、DLP ポリシーの適用をメッセージのスキャンのみに限定できます。次の情報に従って、DLP ポリシー スキャンを制限できます。

- 送信者および受信者
- 添付タイプ
- メッセージ タグ

送信者および受信者のフィルタリング

次の方法の 1 つで、DLP ポリシーを特定の受信者または送信者のメッセージだけをスキャンするように限定できます。

- 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。

発信メッセージに対して、AsyncOS は最初に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ます。受信者または送信者が一致したら、RSA Email DLP は、送信者または受信者がメール ポリシーでイネーブルとなっている DLP ポリシーと一致するか照合します。

添付ファイルのフィルタリング

DLP ポリシーの適用を特定の添付ファイルのタイプを持つメッセージに限定することができます。最初に添付ファイルが AsyncOS のコンテンツ スキャン エンジンにより抽出され、次に添付ファイルの内容が RSA Email DLP スキャン エンジンによってスキャンされます。アプライアンスでは、多数の事前定義されたファイル タイプをスキャンで使用できますが、一覧にないファイル タイプを指定することもできます。事前定義されていないファイル タイプを指定すると、AsyncOS は、添付ファイルの拡張子をもとにファイルタイプを検索します。RSA Email DLP のスキャンを、最小ファイル サイズ（バイト）以上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。DLP ポリシー作成時に、発信メッセージのフィルタリングに使用するメッセージ タグを選択します。詳細については、「コンテンツ フィルタのアクション」（P.6-208）、および『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Mail Policies」を参照してください。

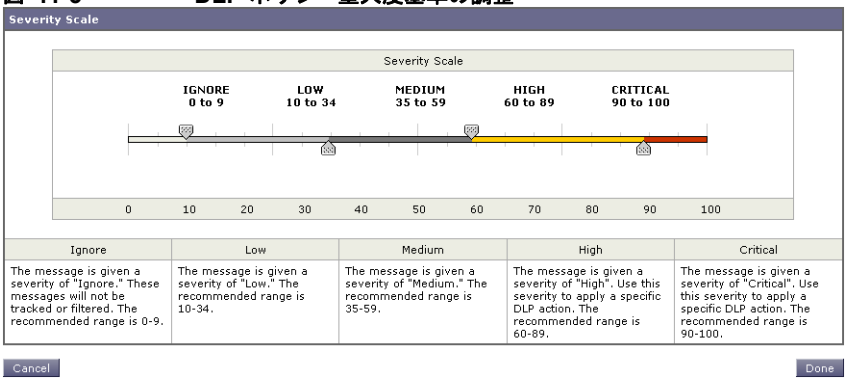
重大度レベルの設定

RSA Email DLP スキャン エンジンが DLP 違反を検出すると、DLP 違反の重大度を示すリスク要因スコア（0 ～ 100 の範囲）を計算します。ポリシーは、リスク要因スコアを重大度基準と比較します。重大度基準には、Ignore、Low、Medium、High、Critical の 5 つの重大度レベルがあります。重大度レベルで、メッセージに適用されるアクションが決まります。デフォルトで、すべての重大度レベル（Ignore を除く）で高位の重大度レベルの設定を継承するようになっています。High の重大度レベルは Critical から設定を継承し、Medium は High から、Low は Medium から継承します。レベルを編集し、異なる重大度に対して別々のアクションを指定することができます。

DLP スキャン エンジンのリスク要因の計算については、「Email DLP の動作を理解する」（P.11-362）を参照してください。

重大度基準をポリシーに対して調整し、スキャン エンジンが返す DLP 違反の推定重大度を規定できます。図 11-5 は重大度基準を示します。基準の矢印を使って、重大度レベルに対するスコアを調整します。

図 11-5　DLP ポリシー重大度基準の調整



Email DLP ポリシーの順序の設定

DLP Policy Manager でのポリシーの順序は重要です。DLP 違反が発生した場合、RSA Email DLP は、その違反を発信メール ポリシーでイネーブルな DLP ポリシーと照合します。違反が複数の DLP ポリシーに一致する場合、RSA Email DLP は上から順に調べ、最初に一致した DLP ポリシー を選択します。

ステップ 1　[DLP Policy Manager] ページで、[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、変更を送信して確定します。

Email DLP ポリシーの編集

既存の DLP ポリシーを編集するには、次の手順に従います。

ステップ 1　[DLP Policy Manager] ページに一覧表示されている RSA Email DLP ポリシーの名前をクリックします。

[Mail Policies: DLP] ページが表示されます。

ステップ 2　DLP ポリシーを変更します。

ステップ 3　変更を送信して確定します。

（注）　ポリシーの名前を変更すると、電子メール セキュリティ マネージャで再度イネーブルにする必要があります。

Email DLP ポリシーの削除

DLP ポリシーを削除するには、一覧のポリシーの隣にあるゴミ箱アイコンをクリックします。確認メッセージが表示されます。このメッセージは、DLP ポリシーが 1 つ以上の複数の発信メール ポリシーで使用されているかを示しています。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。変更を送信して確定します。

Email DLP ポリシーの複製

既存のポリシーとほぼ同じで設定が異なる DLP ポリシーを作成する場合は、DLP Policy Manager で複製ポリシーを作成することができます。

Email DLP ポリシーを複製するには、次の手順に従ってください。

ステップ 1　[DLP Policy Manager] ページで、一覧の中から複製対象のポリシーの隣にある複製アイコンをクリックします。

ステップ 2　ポリシーの名前を入力します。

ステップ 3　ポリシーの設定を変更します。

ステップ 4　変更を送信して確定します。

DLP Assessment Wizard の使用

AsyncOS のブラウザ ベース DLP Assessment Wizard を使うと、よく使われる DLP ポリシーの設定と、そのポリシーを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する 3 つの手順のプロセスを簡単に行えます。

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。DLP Policy Manager を使って、メッセージに適用される全体的なアクション、受信者または送信者のフィルタリング、添付ファイルのタイプのフィルタリング、および重大度レベルの設定を編集します。DLP ポリシーの編集の詳細については、「DLP Policy Manager」（P.11-367）参照してください。

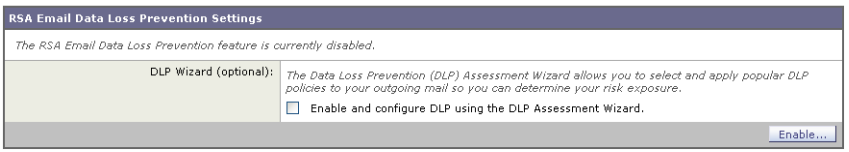
DLP Assessment Wizard により、メッセージ トラッキング用に、一致したコンテンツをログに記録できます。電子メール セキュリティ アプライアンスは検出した DLP 違反をログに記録し、AsyncOS はメッセージ トラッキングにある、クレジット カードや番号や社会保障番号など機密データを含む違反と周辺のコンテンツを表示します。DLP Assessment Wizard は、メッセージ トラッキングがイネーブルでなかった場合、アプライアンス上で自動的にイネーブルにします。アプライアンスがこのデータをログに記録しないようにする場合は、[Security Services] > [RSA Email DLP] ページを使って、一致したコンテンツのログへの記録をディセーブルにします。

DLP Assessment Wizard を起動するには、[Security Services] > [RSA Email DLP] ページを開きます。[Enable] をオンにし、[DLP using the DLP Assessment Wizard] チェックボックスを設定します。次に [Enable] をクリックします。

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。

図 11-6 は、DLP Assessment Wizard の実行オプションを示しています（[RSA Email Data Loss Prevention Settings] ページより）。

図 11-6　[RSA Email Data Loss Prevention Settings] ページ



DLP Assessment Wizard の実行

DLP Assessment Wizard を使用すると、次の DLP 設定作業が簡単にできます。作業は、3 つの手順に分けることができます。

ステップ 1　ポリシー

- ネットワーク上で保護する情報のタイプに合わせて DLP ポリシーを選択します。
- 機密データを検出するために追加情報を必要とする DLP ポリシーをカスタマイズします。

ステップ 2　レポート

- DLP Incident Summary レポート配信設定を設定します。

ステップ 3　レビュー

- DLP ポリシーをレビューしてイネーブルにします。

各手順を完了させたら、[Next] をクリックして、DLP Assessment Wizard の手順を進めていきます。[Previous] をクリックすると、前の手順に戻ることができます。プロセスの最後に、変更を確定するようプロンプトが表示されます。確定するまで、変更は有効になりません。

手順 1：ポリシー

DLP ポリシーの選択

アプライアンスが発信メッセージ内で検出対象とする機密情報のタイプ用の DLP ポリシーを選択します。

次のポリシーを使用できます。

- [Payment Card Industry Data Security Standard (PCI-DSS)]、クレジット カード トラック データおよびクレジット カード。
- [HIPAA (Health Insurance Portability and Accountability Act)] は、HIPAA ディクショナリとコードセット、米国社会保障番号、米国国家プロバイダー認証を検出し、患者識別番号を検出するようにカスタマイズできます。
- [FERPA (Family Educational Rights and Privacy Act)] は、生徒記録を検出し、生徒識別番号を検出するようにカスタマイズできます。
- [GLBA (Gramm-Leach Bliley Act)] は、クレジット カード番号、米国社会保障番号、米国運転免許証番号を検出し、カスタム アカウント番号を検出するようにカスタマイズできます。
- [California SB-1386] は、カルフォルニア SB-1386（民法 1798）で規制されている、米国社会保障番号、クレジット カード番号、米国運転免許証番号などの Personally Identifiable Information（PII; 個人情報）を含むドキュメ

ントと送信を検出します。カルフォルニアでビジネスを営み、カルフォルニア州民のコンピュータ化した 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、準拠することが必須となっています。

- [Restricted Files] は、.mdb、.exe、.bat および Oracle 実行ファイル（.fmx、.frm）など制限されているファイルを含む電子メールを検出します。このポリシーは付加的なファイル属性をポリシー違反ルールに追加してカスタマイズできます。

DLP Policy Manager を使って、DLP ポリシーの他のタイプを作成できます。

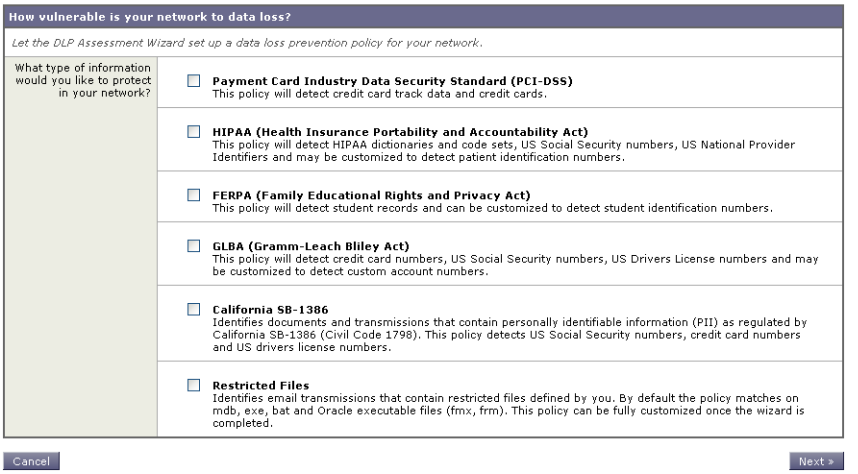
DLP ポリシーのカスタマイズ

DLP ポリシーには、発信メッセージ内の機密情報を検出するようにカスタマイズできるコンテンツ照合分類子を使うものがいくつかあります。HIPAA、FERPA および GLB 用のカスタマイズされた分類子、ポリシーは正規表現を使い、発信メッセージ内に識別番号パターンがないか検索します。Restricted Files ポリシーを選択した場合は、DLP ポリシーで検出する添付ファイル タイプを選択します。Restricted Files ポリシーはデフォルトで .exe および .mdb ファイルを検出しますが、これらのファイル タイプを削除できます。Restricted Files ポリシーを暗号化またはパスワードで保護されたファイルのみに適用するように設定できます。

これらの DLP ポリシー用のコンテンツ照合分類子のカスタマイズの詳細については、「DLP ポリシーに対する分類子のカスタマイズ」（P.11-372）参照してください。

[Next] をクリックして続行します。

図 11-7　DLP Assessment Wizard：手順 1：ポリシー



手順 2：レポート

スケジュール済み DLP Incident Summary レポート用に電子メール アドレスを入力します。複数のアドレスを区切るには、カンマを使います。この値を空白のままにしておくと、スケジュール済みレポートは作成されません。DLP Incident Summary レポートの詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」の章を参照してください。

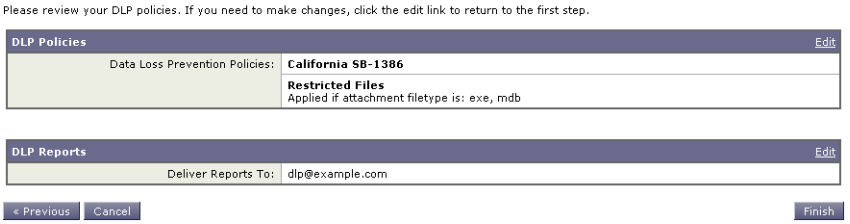
[Next] をクリックして続行します。

図 11-8　DLP Assessment Wizard：手順 2：レポート
DLP Reports

手順 3：レビュー

DLP 設定情報の要約が表示されます。[Previous] ボタンをクリックするか、各セクションの右上にある対応する [Edit] リンクをクリックして、[Policies and Reporting] 情報を編集することができます。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。

図 11-9　DLP Assessment Wizard：手順 3：レビュー
Review DLP Policies



表示されている情報が十分であれば、[Finish] をクリックします。AsyncOS により、[Outgoing Mail Policies] ページに、デフォルトの発信メール ポリシーでイネーブルになっている DLP ポリシーが表示されます。DLP ポリシー設定の要約が、ページの上部に表示されます。変更を確定します。

DLP ポリシーの編集と追加作成については、「DLP Policy Manager」（P.11-367）を参照してください。DLP ポリシーを他の発信メール ポリシーに対してイネーブルにする方法については、「RSA Email DLP の受信者ごとのポリシーの設定」（P.11-394）を参照にしてください。

コンテンツ 照合分類子

コンテンツ照合分類子は、RSA Email DLP スキャン エンジンの検出コンポーネントです。クレジット カード番号や運転免許識別番号などのデータ パターン、およびそのパターンが出現するコンテキストがないか、メッセージと抽出した添

付ファイルの内容を検索します。たとえば、クレジット カード番号を検出する分類子は、クレジット カード番号の形式に一致する数値のパターンだけではなく、有効期限やクレジット カード会社名などの補足データもないかスキャンします。データのコンテキストを評価することで、false positive が減少します。

RSA のポリシー テンプレートの多くは、分類子の事前定義されたセットを含みます。Custom Policy テンプレートをもとにしてポリシーを作成するときは、RSA 分類子を選択するか、独自の分類子を 1 つ追加できます。カスタム DLP ポリシーで使用する独自の分類子の作成については、「コンテンツ照合分類子の作成」（P.11-393）を参照してください。

多くのポリシー テンプレートでは、機密データ検出のために 1 つ以上の分類子をカスタマイズする必要があります。カスタマイズには、識別番号と、その識別番号とともに決まって出現する可能性がある単語とフレーズの一覧を検索するための正規表現を作成することが含まれます。たとえば、Family Educational Rights and Privacy Act（FERPA; 家族教育権とプライバシー法）テンプレートをもとにしたポリシーを追加するには、生徒 ID 番号に一致する正規表現を作成する必要があります。ID 番号が決まって「Student ID」というフレーズとともに出現するならば（「Student ID: 123-45-6789」など）、そのフレーズをポリシーに追加すればコンテンツ マッチングがより正確になります。DLP ポリシーで必須であるカスタマイズの詳細については、「DLP ポリシーに対する分類子のカスタマイズ」（P.11-372）参照してください。

（注） 分類子を持たないポリシーに対しては、メッセージがポリシーに違反した場合、スキャン エンジンは常に「75」のリスク要因値を返します。このようなポリシーには、発生する可能性のある DLP 違反のタイプによって重大度基準を調整します。詳細については、「重大度レベルの設定」（P.11-375）を参照してください。

分類子検出ルール

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**。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**。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、「DLP 用の正規表現の例」（P.11-391）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。RSA Email DLP には、RSA が作成したディクショナリがありますが、独自のディクショナリを作成できます。詳細については、第 14 章「テキスト リソース」を参照してください。
- **エンティティ**。スマート ID と同様に、エンティティはデータ内のパターン（ABA ルーティング番号、クレジット カード番号、住所、社会保障番号など）を識別します。

分類子は、メッセージ内で検出ルールと一致したものが見つかると数値を割り当て、メッセージのスコアを計算します。メッセージの DLP 違反の重大度の決定に使われるリスク要因は、分類子の最終的なスコアの範囲を 0 ～ 100 としたものです。分類子は、次の値を使ってパターンを検出し、リスク要因を計算します。

- **近接性**。有効と見なすには、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、社会保障番号に似た数値のパターンが長いメッセージの上部に出現し、末尾の送信者の署名に住所が現れた場合、それらはおそらく関連がなく、分類子は一致と見なしません。
- **最小総合スコア**。分類子が結果を返すのに必要な最小スコア。メッセージの一致のスコアが最小総合スコアに達しなかった場合、そのデータは機密であるとは見なされません。
- **重み**。各ルールで、ルールの重要度を示す「重み」を指定します。分類子は、検出ルールに一致した数にルールの重みを乗算してメッセージのスコアを計算します。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、重みが低いルールに一致するものが大量に発生しても、スキャンの最終スコアがゆがめられないようにするものです。

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過した場合、分類子は最大スコアを使用します。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。分類子は表 11-1 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 11-1　リスク要因計算用の対数目盛り

ルールのスコア	リスク要因
10	10
20	20
30	30
50	40
100	50
150	60
300	70
500	80
1000	90
10000	100

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、別のクレジット カード番号、有効期限、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。

例を示します。

- `4999-9999-9999-9996`（補足情報がないため一致せず）
- `4999-9999-9999-9996 01/09`（一致）
- `Visa 4999-9999-9999-9996`（一致）
- `4999-9999-9999-9996 4899 9999 9999 9997`（複数のクレジット カード番号があるため一致）

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。

例を示します。

- `321-02-3456`（補足情報がないため一致せず）
- `321-02-3456 July 4`（一致）
- `321-02-3456 7/4/1980`（一致）
- `321-02-3456 7/4`（一致せず）
- `321-02-3456 321-02-7654`（複数の SSN があるため一致）
- `SSN: 321-02-3456`（一致）
- `Joe Smith 321-02-3456`（一致）
- `321-02-3456 CA 94066`（一致）

ABA ルーティング番号

ABA ルーティング番号分類子は、クレジット カード番号分類子とほぼ同じです。

例を示します。

- `119999992`（補足情報がないため一致せず）
- `routing 119999992 account 1234567`（一致）

米国運転免許証

DLP ポリシー テンプレートのいくつかは、米国運転免許証分類子を使用します。この分類子には、米国の各州およびコロンビア特別区用の検出ルールの一式が含まれています。DLP Policy Manager で [Advanced Settings] の下の米国運転免許証用のリンクをクリックすることで、組織のポリシーにとって重要でない州を選択してイネーブルまたはディセーブルにすることができます。

（注） California SB 1386 など特定の州用の事前定義された DLP ポリシー テンプレートは、すべての州向けの検出ルールを使用し、カルフォルニア州以外の運転免許のデータに対して DLP 違反を返します。これは、プライバシー違反と考えられるからです。

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。

例を示します。

- `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`（オレゴン州の正しいパターンではないため一致せず）
- `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: G654321`（ウェスト バージニア州の正しいパターンでないため一致せず）

HIPAA ディクショナリ

事前定義された HIPAA ポリシー テンプレートは、医療関連のデータを検出するため、HIPAA ディクショナリ分類子を使用します。この分類子は、患者 ID 分類子とともに動作し、個人情報を検出します。HIPAA DLP ポリシーで DLP 違反を返すには、この分類子での一致に加えて、米国社会保障番号や米国国家プロバイダー認証などの個人情報との一致も必要となります。

例を示します。

- angina, cancer（一致）
- angina（複数の用語を必要とするため一致せず）
- headache, fever（一致）
- camphor glycerin（一致）
- fracture paralysis（一致）
- bite cut（一致）

患者 ID

患者 ID 分類子では、HIPAA ポリシー テンプレートの個人情報コンポーネントを使用できます。このコンポーネントは、米国社会保障番号と米国 National Provider Identifier（NPI; 国家プロバイダー認証）番号があるかスキャンします。NPI は、チェック デジットを含む 10 桁の数字です。

例を示します。

- 321-02-4567 7/4/1980（米国社会保障番号および誕生日と考えられるもの）
- NPI: 3459872347（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）

生徒記録

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：

- Joe Smith, Class Rank: 234, Major: Chemistry Transcript（一致）

企業財務情報

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。

例を示します。

2009 Cisco net sales, net income, depreciation（一致）

FORM 10-Q 2009 I.R.S.Employer Identification No.（一致）

コンテンツ照合分類子用の正規表現

多くのポリシー テンプレートで 1 つ以上の分類子をカスタマイズする必要があります。カスタマイズには、カスタム アカウント番号や患者識別番号など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。コンテンツ照合分類子に使用される正規表現の形式は、**POSIX 基本正規表現**形式の正規表現です。

次のテーブルを、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。

表 11-2　　分類子での正規表現

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。

表 11-2　分類子での正規表現（続き）

バックスラッシュ特殊文字（\）	バックスラッシュは特殊文字をエスケープします。したがって、\. と続けると、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。 バックスラッシュ文字は、\d などトークンの始まりともなります。 **重要な注意事項：**バックスラッシュは、パーサーに対しても特殊なエスケープ文字となります。結果として、正規表現にバックスラッシュを含める場合には、*2* つのバックスラッシュを使います。そうするとパージングの後、「本物」のバックスラッシュが 1 つだけ残り、正規表現の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。
繰り返しの回数 { 最小、最大 }	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、「\d{8}」という表現は、12345678 および 11223344 には一致しますが、8 には一致しません。
論理和（|）	代替、つまり「or」演算子 A と B を正規表現とすると、「A|B」という表現は「A」と「B」のいずれかに一致するすべての文字列に一致します。1 つの正規表現で数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 または bar のどちらかに一致しますが、foobar には一致しません。

DLP 用の正規表現の例

コンテンツ照合分類子で正規表現を使用する主なケースは、特定の口座、患者や生徒の識別番号を定義することです。これらは、数や文字のパターンを記述する通常の単純な正規表現です。次の例を参考にしてください。

- 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`

（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。

高度な DLP ポリシーのカスタマイズ

使用可能な RSA ポリシー テンプレートでは組織の独自の要件に適合しない場合、ゼロから独自の DLP ポリシーを作成するためのオプションがいくつかあります。オプションには次のものがあります。

- Custom Policy テンプレートを使って独自の DLP ポリシーを作成
- カスタム ポリシーで使用する独自の分類子を作成
- カスタム ポリシーで使用する独自の DLP ディクショナリを作成しインポート

（注） これらのオプションは高度であり、事前定義された設定が組織のニーズに適合しない場合にのみ使用されることを想定しています。

Custom Policy テンプレートを使用した DLP ポリシーの作成

Custom Policy テンプレートを使用して、カスタム DLP ポリシーを作成できます。事前定義された RSA 分類子をポリシーで使用することも、カスタム分類子を追加することもできます。分類子の作成の手順については、「コンテンツ照合分類子の作成」（P.11-393）を参照してください。

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。false positive 防止のため、DLP ポリシーには、メッセージの内容と一致する場合、違反とは見なさなくなる分類子を含めることができます。分類子の [NOT] チェックボックスをオンにすると、その分類子に一致する内容を含むメッセージは、DLP 違反として報告されません。

カスタム ポリシーを追加するには、次の手順に従ってください。

ステップ 1　[Mail Policies] > [DLP Policy Manager] を選択します。

ステップ 2　[Add DLP Policy] をクリックします。

ステップ 3　Custom Policy カテゴリの名前をクリックします。

ステップ 4　Custom Policy テンプレートの [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　ポリシー用に分類子を選択します。既存の分類子の使用または [Create a Classifier] オプションの選択が可能です。

ステップ 7　[Add] をクリックします。

[Create a Classifier] を選択すると、[Add Content Matching Classifier] ページが開きます。それ以外の場合は、事前定義された分類子がポリシーに追加されます。

ステップ 8　複数の分類子をポリシーに追加する場合は、手順 6 ～ 7 を繰り返します。

ステップ 9　任意で、特定の受信者または送信者を持つメッセージにのみ DLP ポリシーを適用するよう限定できます。改行やカンマで、複数のエントリを分離できます。詳細については、「送信者および受信者のフィルタリング」（P.11-374）を参照してください。

ステップ 10　任意で、DLP ポリシーを特定の添付タイプを持つメッセージにのみに適用するよう限定できます。詳細については、「添付ファイルのフィルタリング」（P.11-375）を参照してください。

ステップ 11　[Critical Violations Settings] セクションで、重大な DLP 違反を含むメッセージをドロップ、配信、または検疫するか選択できます。

ステップ 12　任意で、メッセージの暗号化、ヘッダーの修正、代替ホストへのメッセージの送信、別の受信者へのコピーの配信（bcc）、DLP 通知メッセージの送信を選択できます。

DLP の通知については、「テキスト リソース」（P.14-429）を参照してください。

ステップ 13　一致する重大度レベルが High、Medium、Low のメッセージに、別々の設定を定義するときは、適切なセキュリティ レベルの [Inherit settings] チェックボックスをオフにします。メッセージへの全体的なアクションや他の設定を編集します。

ステップ 14　ポリシーの DLP 違反の重大度基準を調整する場合は、[Edit Scale] をクリックして、設定を調整します。詳細については、「重大度レベルの設定」（P.11-375）を参照してください。

ステップ 15　変更を送信して確定します。

ポリシーが DLP Policy Manager に追加されます。

コンテンツ照合分類子の作成

カスタム ポリシー作成時は、[Create a Classifier] オプションを選択すると、カスタム分類子を作成できます。分類子の作成に必要なルールと値の詳細については、「分類子検出ルール」（P.11-384）を参照してください。

分類子を作成して送信すると、カスタム ポリシー作成時に使用可能な分類子の一覧に表示されます。

分類子を作成するには、次の手順に従います。

ステップ 1　分類子の名前と説明を入力します。

ステップ 2　文字数を入力します。分類子のルールの出現場所と、他のルールの出現場所の間の文字数がこの文字数以下の場合、違反と見なします。

ステップ 3　分類子の最小総合スコアを入力します。

ステップ 4　重みや最大スコアなど分類子のルールを定義します。

ステップ 5　[Add Rule] をクリックし、ルールを分類子に追加します。複数のルールを追加できます。

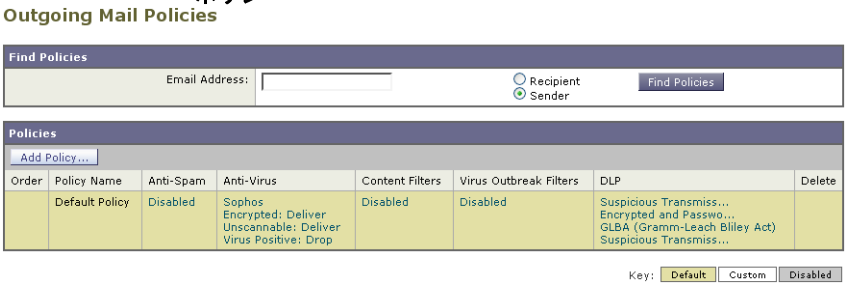
ステップ 6　分類子を送信し、カスタム ポリシーの作成を続けることができます。

RSA Email DLP の受信者ごとのポリシーの設定

電子メール セキュリティ マネージャの機能を使って受信者ごとの RSA Email DLP ポリシーをイネーブルにすることができます。[Mail Policies] > [Outgoing Mail Policies (GUI)] ページまたは、`policyconfig` コマンド（CLI）を使います。異なる発信メール ポリシーに対して別々の DLP ポリシーをイネーブルにすることができます。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。図 11-10 を参照してください。

電子メールの「ワーク キュー」のウイルス感染フィルタの段階の後に、DLP スキャンが行われます。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の章の「Email Security Manager」を参照してください。

図 11-10　イネーブルになっている DLP ポリシーを伴うデフォルトの発信メール ポリシー

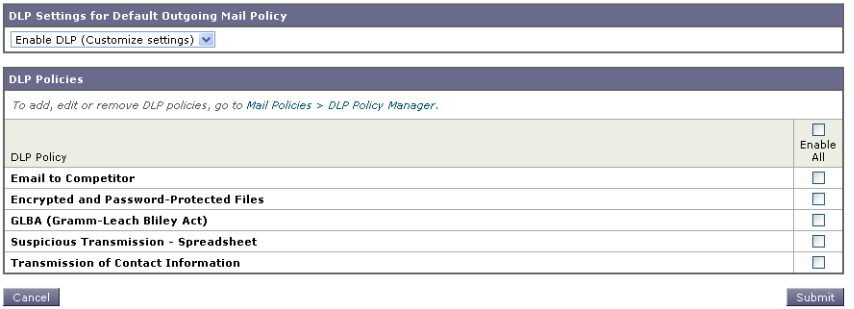


メール ポリシーの DLP 設定の編集

発信メール ポリシーに対するユーザごとの DLP 設定を編集するプロセスは、基本的にデフォルトのポリシーと個々のポリシーに対するものと同じです。個々のポリシー（デフォルトでない）には、DLP 設定を [Enable DLP (Inherit default mail policy settings)] にするという追加のオプションがあります。これを選択すると、ポリシーはデフォルトの発信メール ポリシーの DLP 設定をすべて採用します。

図 11-11 に、デフォルトの発信メール ポリシーでイネーブルな DLP ポリシーの一覧を示します。

図 11-11　デフォルトの発信メール ポリシーで DLP ポリシーをイネーブルにする



発信メール ポリシー（デフォルトを含む）に DLP 設定を編集するには、次の手順に従ってください。

ステップ 1　電子メール セキュリティ マネージャの発信メール ポリシー テーブルの任意の行にある DLP セキュリティ サービスのリンクをクリックします。

DLP 設定のページが表示されます。

ステップ 2　デフォルト ポリシーの設定を編集するには、デフォルト行のリンクをクリックします。

ステップ 3　メール ポリシーの [Enable DLP (Customize Settings)] を選択します。

DLP Policy Manager で定義されているポリシーの一覧が表示されます。

ステップ 4　発信メール ポリシーで使用する RSA Email DLP ポリシーを選択します。

ステップ 5　変更を送信して確定します。