Hybrid Data Security を使用する前に

Hybrid Data Security の概要

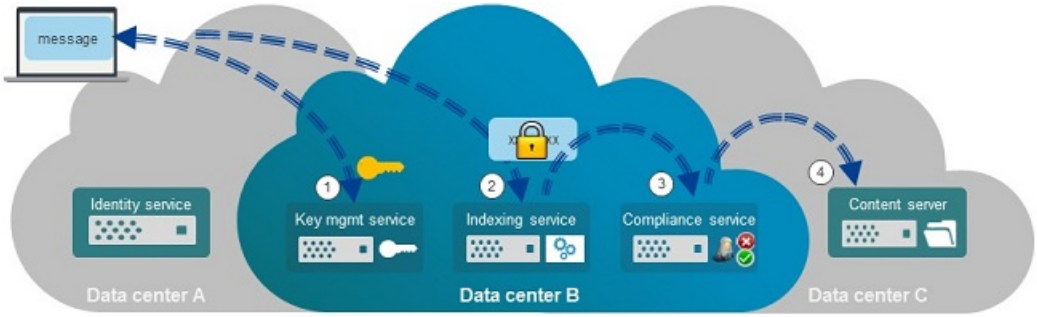
Webex アプリ を設計する際に当初から主な焦点とされていたのは、データ セキュリティです。このセキュリティの基盤は、Webex アプリ クライアントがキー管理サービス（KMS）とやり取りすることで実現されるエンドツーエンドのコンテンツ暗号化です。KMS は、クライアントがメッセージやファイルを動的に暗号化および復号化するために使用する暗号キーを作成および管理します。

Webex アプリ ではデフォルトで、シスコのセキュリティ レルム内のクラウド KMS に保管された動的キーによってエンドツーエンドの暗号化が行われます。ハイブリッド データ セキュリティは KMS とその他のセキュリティ関連の機能をユーザの企業データ センターに移すため、そのユーザのみが暗号化されたコンテンツのキーを保持します。

セキュリティ レルムのアーキテクチャ

Webex のクラウド アーキテクチャでは、次に示すように、サービスがタイプ別に異なるレルム、つまり信頼ドメインに分離されます。

図 *1:* 分離されたレルム（ハイブリッド データ セキュリティ なし）



ハイブリッド データ セキュリティ について理解を深めるため、最初にクラウドのレルム内でシスコのすべての機能が提供される純粋なクラウドの場合を見てみましょう。アイデンティティ サービスは、ユーザを電子メール アドレスなどの個人情報と直接関連付けることができる唯一の場所であり、データ センター B のセキュリティ レルムから論理的にも物理的にも分離されています。さらにこの2つのレルムも、暗号化されたコンテンツが最終的に保管されるデータ センター C のレルムから分離されています。

この図では、クライアントはユーザのラップトップ上で Webex アプリ を実行しており、アイデンティティ サービスによって認証されています。ユーザがスペースに送信するメッセージを作成すると、次の手順が実行されます。

1. クライアントがキー管理サービス（KMS）とのセキュアな接続を確立し、メッセージを暗号化するためのキーを要求します。このセキュア接続では ECDH が使用され、KMS は AES-256 マスター キーを使用してキーを暗号化します。
2. メッセージがクライアントから送信される前に暗号化されます。クライアントがインデックス サービスにメッセージを送信します。インデックス サービスは、その後のコンテンツ検索を支援するために暗号化された検索インデックスを作成します。
3. 暗号化されたメッセージがコンプライアンス チェックのためにコンプライアンス サービスに送信されます。
4. 暗号化されたメッセージが保管用のレルムに格納されます。

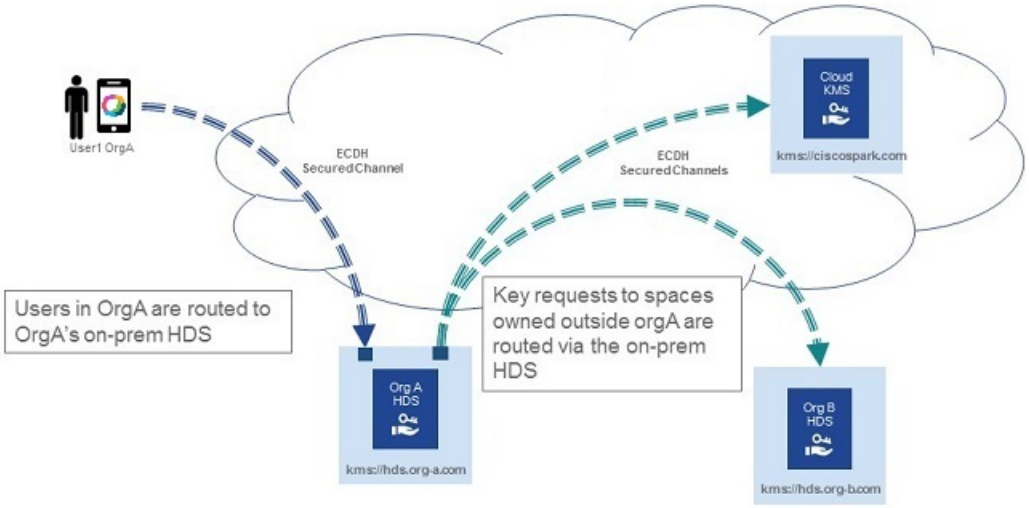
ハイブリッドデータ セキュリティ を導入する場合は、セキュリティ レルムの機能（KMS、インデックス作成、およびコンプライアンス）をオンプレミスのデータ センターに移動します。Webex を構成するその他のクラウド サービス（アイデンティティとコンテンツの保管を含む）は、シスコのレルムに残ります。

他の組織とのコラボレーション

組織内のユーザは定期的に Webex アプリ を使用して、他の組織の外部参加者と連携することができます。（ユーザの1人が作成したために）組織が所有しているスペースのキーをいずれかのユーザから要求された場合、KMS は ECDH で保護されたチャネルを介してクライアントにキーを送信します。ただし、そのスペースのキーを別の組織が所有している場合、KMS は

別の ECDH チャネルを介して Webex クラウドに要求をルーティングし、該当する KMS からキーを取得した後、そのキーを元のチャネルを介してユーザに返します。

図 *2:*



OrgA で実行されている KMS サービスは、x.509 PKI 証明書を使用して他の組織の KMS への接続を検証します。ハイブリッド データ セキュリティ 導入環境で使用する x.509 証明書を生成する方法の詳細については、「環境の準備」を参照してください。

Hybrid Data Security の導入時に期待されること

ハイブリッド データ セキュリティ の導入では、ユーザの深い関与と、暗号キーの所有に伴うリスクの認識が必要です。

ハイブリッド データ セキュリティ を導入するには、次のものを用意する必要があります。

- Cisco Webex Teams プランのサポート対象となっている国内に開設された安全なデータ センター。
- 「環境の準備」に記載されている機器、ソフトウェア、およびネットワークアクセス。

ハイブリッド データ セキュリティ 用に作成した構成 ISO、またはお客様提供のデータベースのいずれかが完全に失われると、キーが失われます。キーが失われた場合、ユーザは Webex アプリ 内のスペース コンテンツやその他の暗号化されたデータを復号化できなくなります。このような場合は、新しい導入を構築できますが、表示されるのは新しいコンテンツだけです。データへのアクセスが失われるのを避けるには、次のような対策が必要です。

- データベースおよび構成 ISO のバックアップとリカバリを管理します。
- データベース ディスクの障害やデータ センターの災害などの大災害が発生した場合に、迅速なディザスタ リカバリを実行できるように準備します。

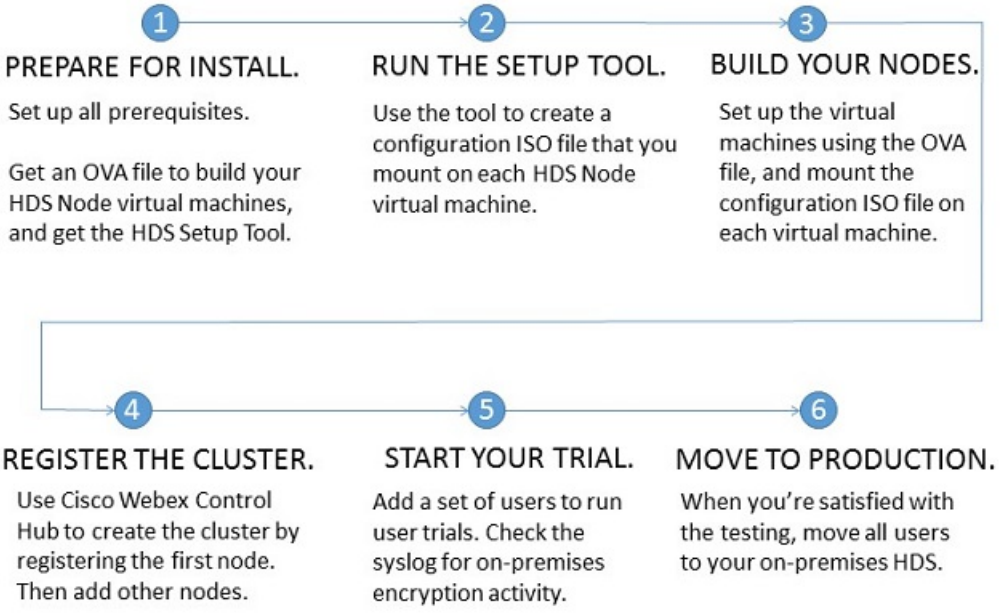
（注） HDS の展開後にキーをクラウドに戻すメカニズムはありません。

セットアップ プロセスの概要

このドキュメントでは、ハイブリッド データ セキュリティ 導入環境のセットアップと管理について説明します。

- **ハイブリッド データ セキュリティ** のセットアップ：これには、必要なインフラストラクチャの準備と ハイブリッドデータ セキュリティ ソフトウェアのインストール、ユーザのサブセットを使用したトライアルモードでの導入環境のテスト、テスト完了後の実稼働への移行が含まれます。これにより、組織全体がセキュリティ機能としてハイブリッドデータ セキュリティ クラスタを使用するようになります。

  セットアップ、トライアル、実稼働の各フェーズについては、以降の3つの章で詳しく説明します。



- **ハイブリッド データ セキュリティ 導入環境の保守**：Webex クラウドは自動的かつ継続的にアップグレードされます。IT部門は、この導入のティア1サポートを提供し、必要に応じてシスコ サポートと契約できます。Control Hub では、画面上の通知を使用したり、電子メールベースのアラートを設定したりできます。

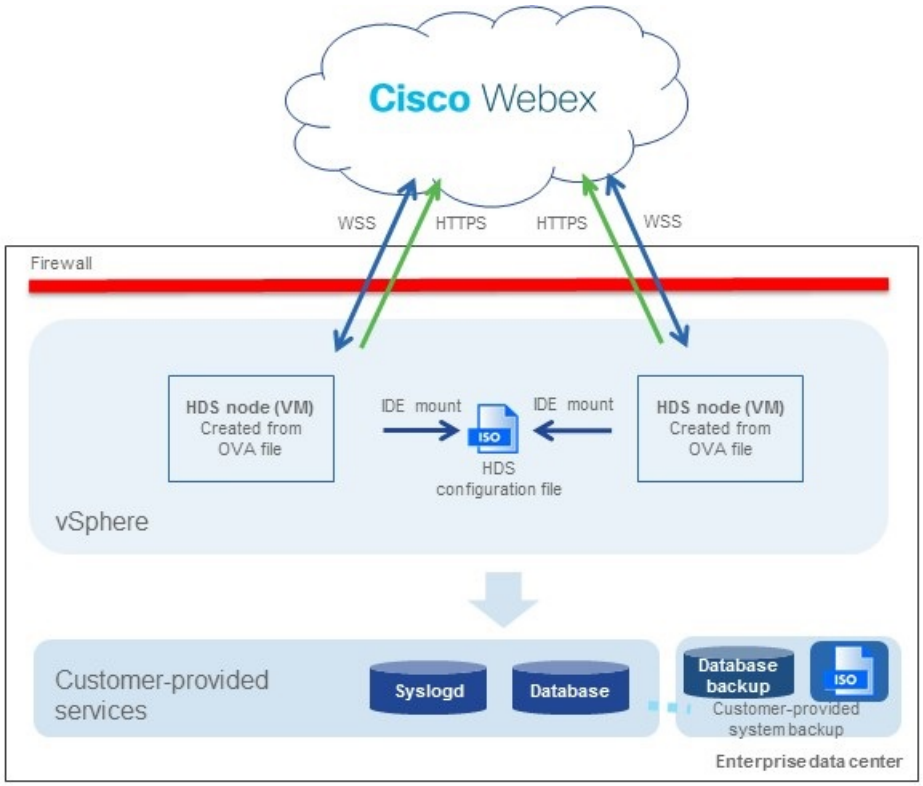
- **一般的なアラート、トラブルシューティング手順、および既知の問題の理解**：ハイブリッド データ セキュリティ の導入時または使用時に問題が発生した場合は、このガイドの最後の章と付録の「既知の問題」が問題の特定と修正に役立ちます。

Hybrid Data Security の導入モデル

企業データ センター内では、ハイブリッド データ セキュリティ を別個の仮想ホスト上のノードの単一クラスタとして導入します。ノードは安全な WebSocket と安全な HTTP を介して Webex クラウドと通信します。

インストール プロセスでは、ユーザが用意した VM に仮想アプライアンスをセットアップするための OVA ファイルが提供されます。ユーザは HDS セットアップ ツールを使用して、各ノードにマウントするカスタム クラスタ構成 ISO ファイルを作成します。ハイブリッド データ セキュリティ クラスタでは、お客様提供の Syslogd サーバと PostgreSQL または Microsoft SQL Server データベースを使用します。（Syslogd とデータベース接続の詳細は HDS セットアップ ツールで構成します）。

図 *3 : Hybrid Data Security* の導入モデル



クラスタには 2 つ以上のノードを含める必要があります。ノードの推奨数は 3、最大数は 5 です。複数のノードを導入すると、ノード上のソフトウェア アップグレードやその他のメンテナンス アクティビティ中にサービスが中断されなくなります。（Webex クラウドがアップグレードするノードは 1 度に 1 つのみです）。

クラスタ内のすべてのノードは同じキー データストアにアクセスし、同じ syslog サーバにアクティビティを記録します。ノード自体はステートレスであり、クラウドの指示に従ってラウンド ロビン方式でキー要求を処理します。

ノードは、ユーザが Control Hub に登録したときにアクティブになります。個別のノードの稼働を停止するには、そのノードを登録解除します。必要な場合は後で再登録できます。

サポートされるクラスタは組織ごとに 1 つのみです。

Hybrid Data Security のトライアル モード

ハイブリッド データ セキュリティ 導入をセットアップしたら、最初にパイロット ユーザを作成して導入を試用します。トライアル期間中、これらのユーザは暗号キーやその他のセキュリティ レルム サービスに関してオンプレミスの ハイブリッド データ セキュリティ ドメインを使用します。他のユーザは、クラウドのセキュリティレルムを使用し続けます。

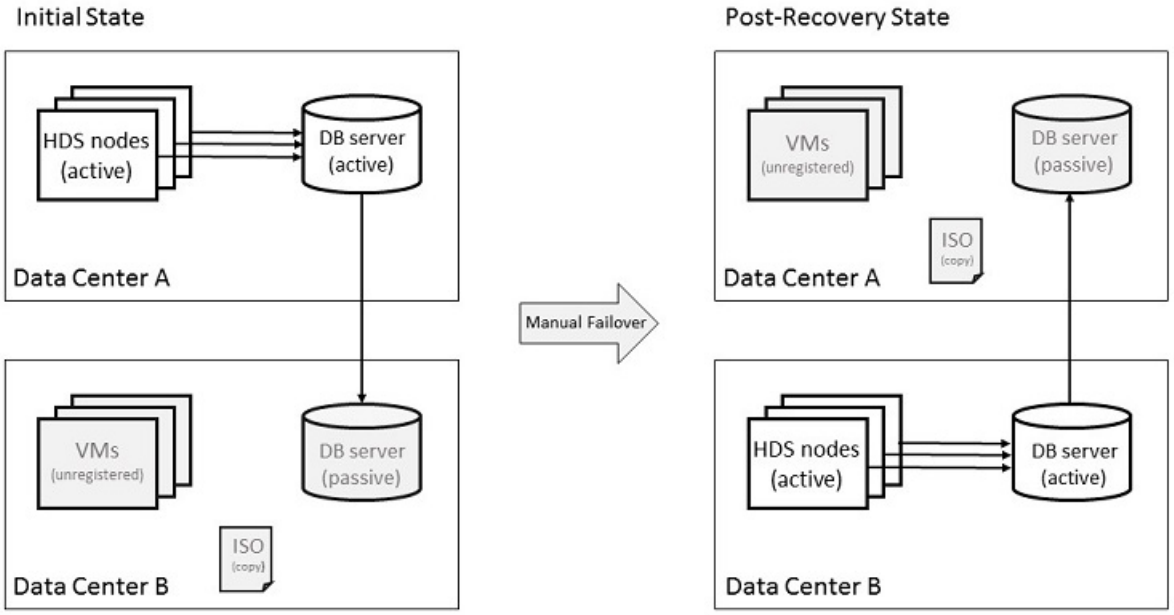
トライアル中に導入を続行しないことを決定し、サービスを非アクティブ化する場合は、パイロットユーザと、トライアル期間中に作成された新しいスペースを介してパイロットユーザとやり取りを行ったすべてのユーザは、メッセージやコンテンツにアクセスできなくなります。これらのユーザには、Webex アプリに「このメッセージを復号化できません（This message cannot be decrypted）」というメッセージが表示されます。

導入がトライアルユーザに対して適切に機能していることを確認し、ハイブリッド データ セキュリティをすべてのユーザに拡張する準備が整ったら、実稼働に移行できます。パイロット ユーザは、トライアル中に使用したキーに引き続きアクセスできます。ただし、実稼働と元のトライアルの間でモードを切り替えることはできません。ディザスタ リカバリの実施などの目的でサービスを非アクティブ化する必要がある場合は、再アクティブ化したときに新しいトライアルを開始し、新しいトライアル用のパイロットユーザを設定してから実稼働モードに戻る必要があります。この時点でユーザがデータに引き続きアクセスできるかどうかは、クラスタ内のキー データストアと ハイブリッド データ セキュリティ ノード用の ISO 構成ファイルのバックアップが適切に保持されているかどうかによります。

ディザスタ リカバリのためのスタンバイ データ センター

導入時に、セキュアなスタンバイ データ センターをセットアップします。スタンバイ データ センターに、PostgreSQL または Microsoft SQL Server データベースのバックアップ コピーと、ハイブリッド データ セキュリティ ノード用に生成された構成 ISO ファイルを保管します。データ センターで障害が発生した場合、導入環境を手動でスタンバイ データ センターにフェールオーバーできます。

図 *4:* スタンバイ データ センターへの手動フェールオーバー



データ センター A で障害が発生した場合は、次の手順に従います。

1. Control Hub から、データ センター A の HDS ノードを削除します。
2. データ センター B のデータベース サーバをアクティブ（プライマリまたはマスター）データベースにします。
3. データ センター B とデータ センター A のデータベース ログイン情報が異なる場合は、セットアップ ツールを実行して ISO 構成ファイルを更新します。
4. ISO 構成ファイルをデータ センター B の VM にマウントし、それらの VM を Control Hub に登録します。
5. できるだけ早く、ISO 構成ファイルとアクティブ データベースのバックアップ コピーがあることを確認します。

フェールオーバー手順の詳細については、「ディザスタ リカバリ後のクラスタの再構築」を参照してください。

（注） アクティブな Hybrid Data Security ノードは、常にアクティブなデータベース サーバと同じデータ センター内に存在する必要があります。

プロキシ サポート

Hybrid Data Security では、明示的かつ透過的な検査プロキシと非検査プロキシがサポートされています。これらのプロキシを導入環境に関連付けることで、企業からクラウドへのトラフィックを保護およびモニタリングできます。ノード上のプラットフォーム管理インターフェイスを使用して、証明書を管理できます。また、ノード上にプロキシをセットアップした後の全体的な接続ステータスも確認できます。

Hybrid Data Security ノードは、次のプロキシ オプションをサポートしています。

- **プロキシなし**：プロキシを統合するために HDS ノードセットアップの信頼ストアとプロキシ構成を使用しない場合、これがデフォルトになります。証明書の更新は必要ありません。
- **透過的な非検査プロキシ**：ノードは特定のプロキシ サーバ アドレスを使用するように構成されないため、非検査プロキシと連動するための変更は必要ありません。証明書の更新は必要ありません。
- **透過的なトンネリングまたは検査プロキシ**：ノードは特定のプロキシ サーバ アドレスを使用するように構成されません。ノード上の HTTP または HTTPS の構成を変更する必要はありません。ただし、ノードがプロキシを信頼するよう、ノードにはルート証明書が必要です。通常、IT は検査プロキシを使用して、アクセス可能な Web サイトおよび許可されないコンテンツのタイプに関するポリシーを適用します。このタイプのプロキシは、すべてのトラフィックを（HTTPS も）復号化します。
- **明示的なプロキシ**：明示的なプロキシを使用する場合、HDS ノードに使用するプロキシ サーバと認証方式を指示します。明示的なプロキシを構成するには、各ノードに次の情報を入力する必要があります。

  1. **[プロキシ IP/FQDN（Proxy IP/FQDN）]**：プロキシ マシンに到達可能なアドレス。
  2. **[プロキシポート（Proxy Port）]**：プロキシがプロキシ経由のトラフィックをリッスンするために使用するポート番号。
  3. **プロキシプロトコル**：プロキシ サーバのサポート対象に応じて、次のプロトコルの中から選択します。
     - HTTP：クライアントが送信するすべての要求を表示および制御します。
     - HTTPS：サーバへのチャネルを提供します。クライアントがサーバの証明書を受信して検証します。
  4. **[認証タイプ（Authentication Type）]**：次の認証タイプの中から選択します。
     - **[なし（None）]**：これ以上の認証は必要ありません。

       プロキシ プロトコルとして HTTP または HTTPS のいずれかを選択した場合に使用できます。

- **[基本（Basic）]**：要求を行うときにユーザ名とパスワードを入力する HTTP ユーザエージェントに対して使用されます。Base64 エンコーディングを使用します。

  プロキシ プロトコルとして HTTP または HTTPS のいずれかを選択した場合に使用できます。

  各ノードでユーザ名とパスワードを入力する必要があります。

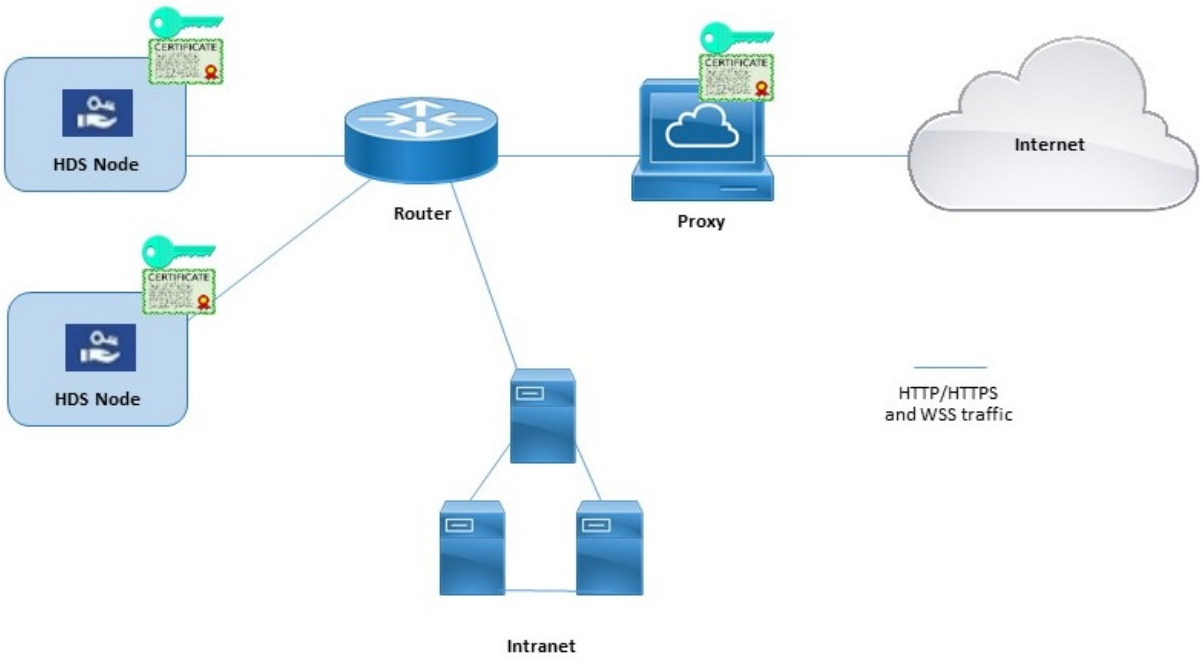
- **[ダイジェスト（Digest）]**：機密情報を送信する前にアカウントを確認するために使用されます。ネットワーク経由で送信する前に、ユーザ名とパスワードにハッシュ関数を適用します。

  プロキシ プロトコルとして HTTPS を選択した場合にのみ使用できます。

  各ノードでユーザ名とパスワードを入力する必要があります。

Hybrid Data Security ノードとプロキシの例

次の図は、Hybrid Data Security、ネットワーク、プロキシ間の接続例を示しています。透過的な検査プロキシと明示的な HTTPS 検査プロキシのオプションでは、プロキシと Hybrid Data Security ノードに同じルート証明書がインストールされている必要があります。



ブロックされた外部 DNS 解決モード（明示的なプロキシ設定）

ノードを登録するか、ノードのプロキシ設定を確認すると、プロセスは、Cisco Webex クラウドへの DNS ルックアップと接続をテストします。内部クライアントに対する外部 DNS 解決を許可しない明示的なプロキシ設定を導入している環境で、ノードが DNS サーバに照会できな

い場合、そのノードは自動的にブロックされた外部 DNS 解決モードに入ります。このモードでは、ノード登録およびその他のプロキシ接続テストを続行できます。

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。