環境の準備

Hybrid Data Security の要件

Cisco Webex ライセンスの要件

Hybrid Data Security を導入するには、次の要件を満たしている必要があります。

- Pro Pack for Cisco Webex Control Hub を使用していること（https://www.cisco.com/go/pro-pack を参照してください）。

Docker Desktop の要件

HDS ノードをインストールする前に、セットアッププログラムを実行するための Docker Desktop が必要です。Docker は最近、ライセンスモデルを更新しました。組織によっては、Docker Desktop の有料サブスクリプションが必要な場合があります。詳細については、Docker のブログ投稿「Docker is Updating and Extending Our Product Subscriptions」を参照してください。

X.509 証明書の要件

証明書チェーンは、次の要件を満たしている必要があります。

表 *1 : Hybrid Data Security* 導入に使用する *x.509* 証明書の要件

要件	詳細
• 信頼できる認証局（CA）によって署名されていること	デフォルトでは、Mozilla リスト（https://wiki.mozilla.org/CA:IncludedCAs）内の CA（WoSign と StartCom を除く）を信頼します。

要件	詳細
• ハイブリッドデータ セキュリティ 導入環境を識別する共通名（CN）ドメイン名を持っていること • ワイルドカード証明書ではないこと	この CN は、到達可能またはライブ ホストである必要はありません。組織を反映する名前（hds.company.com など）を使用することをお勧めします。 CN に *（ワイルドカード）を含めることはできません。 CNは、ハイブリッドデータ セキュリティノードを Webex アプリ クライアントに対して確認するために使用されます。クラスタ内の ハイブリッドデータ セキュリティ ノードすべてが同じ証明書を使用します。KMS は、x.509v3 SAN フィールドで定義されるドメインではなく、この CN ドメインを使用して自身を識別します。 この証明書を持つノードを登録すると、CN ドメイン名の変更はサポートされなくなります。トライアルと実稼働の両方の導入環境に適用できるドメインを選択してください。
• SHA1 シグニチャでないこと	KMS ソフトウェアは、他の組織の KMS への接続を検証する場合に SHA1 シグニチャをサポートしません。
• パスワードで保護された PKCS #12 ファイルとしてフォーマットされていること • アップロードする証明書、秘密キー、および中間証明書に kms-private-key というフレンドリ名を付けます。	証明書の形式は、OpenSSL などのコンバーターを使用して変更できます。 HDS セットアップ ツールを実行するときは、パスワードを入力する必要があります。

KMS ソフトウェアは、キー使用法または拡張キー使用法の制約を適用しません。一部の認証局は、各証明書（サーバ認証など）に対して拡張キー使用法の制約を適用することを要求します。サーバ認証やその他の設定を使用しても問題ありません。

仮想ホストの要件

クラスタ内で ハイブリッド データ セキュリティ ノードとしてセットアップする仮想ホストには、次の要件があります。

- 同じセキュアデータセンター内に少なくとも 2 つの個別のホスト（推奨は 3 つ）が配置されていること
- VMware ESXi 6.5 以降がインストールされ、実行されていること

重要 それ以前のバージョンの ESXi を使用している場合は、アップグレードする必要があります。

- サーバごとに少なくとも 4 つの vCPU、8 GB のメインメモリ、30 GB のローカルハードディスク容量があること

データベースサーバの要件

重要 キーストレージ用に新しいデータベースを作成します。デフォルトのデータベースは使用しないでください。HDS アプリケーションは、インストール時にデータベース スキーマを作成します。

データベース サーバには2つのオプションがあります。それぞれの要件は、次のとおりです。

表 *2:* データベースのタイプごとのデータベースサーバの要件

PostgreSQL	Microsoft SQL Server
• PostgreSQL 10 または 11 がインストールされて実行中であること	• SQL Server 2016、2017 または 2019（EnterpriseまたはStandard）がインストールされている。 （注） SQL Server 2016には、Service Pack 2 および累積アップデート 2 以降が必要です。
最小 8 個の vCPU、16 GB のメイン メモリ、十分なハード ディスク容量とこの容量を超えていないことを確認するためのモニタリング（記憶域を増やすことなく長期間データベースを実行したい場合は、2 TB を推奨）	最小 8 個の vCPU、16 GB のメイン メモリ、十分なハード ディスク容量とこの容量を超えていないことを確認するためのモニタリング（記憶域を増やすことなく長期間データベースを実行したい場合は、2 TB を推奨）

現在、HDS ソフトウェアはデータベース サーバとの通信用に次のドライバ バージョンをインストールします。

PostgreSQL	Microsoft SQL Server
Postgres JDBC ドライバ 42.2.5	SQL Server JDBC ドライバ 4.6 このドライバ バージョンでは、SQL Server Always On（Always On フェールオーバー クラスタ インスタンスと Always ON 可用性グループ）がサポートされています。

Microsoft SQL Server に対する Windows 認証の追加要件

HDS ノードが Windows 認証を使用して Microsoft SQL Server 上のキーストアデータベースにアクセスできるようにする場合は、環境に次の構成が必要です。

- HDS ノード、Active Directory インフラストラクチャ、および MS SQL Server は、すべて NTP と同期する必要があります。
- HDS ノードに提供する Windows アカウントには、データベースへの読み取り/書き込みアクセス権が必要です。
- HDS ノードに提供する DNS サーバは、キー発行局（KDC）を解決できる必要があります。
- Microsoft SQL Server の HDS データベースインスタンスを Active Directory のサービスプリンシパル名（SPN）として登録できます。Kerberos 接続のサービスプリンシパル名の登録を参照してください。

  HDS セットアップツール、HDS ランチャー、およびローカル KMS はすべて、Windows 認証を使用してキーストアデータベースにアクセスする必要があります。これらは、Kerberos 認証でアクセスを要求するときに、ISO 構成の詳細を使用して SPN を構築します。

外部接続の要件

HDS アプリケーション用に次の接続を許可するように、ファイアウォールを設定します。

アプリケーション	プロトコル	ポート	アプリケーションからの方向	宛先

ハイブリッド データ セキュリティ ノード	TCP	443	アウトバウンド HTTPS および WSS	• Webex サーバ：
				  • *.wbx2.com
				  • *.ciscospark.com
				• すべての共通 ID ホスト
				• 「*Webex* ハイブリッド サービスの追加 *URL*」（Webex サービスのネットワーク要件の表内）にリストされているその他の URL

HDS セットアップ ツール	TCP	443	アウトバウンド HTTPS	• *.wbx2.com • すべての共通 ID ホスト • hub.docker.com

（注） 上記の表にリストされているドメイン宛先へのアウトバウンド接続が NAT またはファイアウォールで許可されている限り、ハイブリッド データ セキュリティ ノードはネットワーク アクセス変換（NAT）と連動するか、ファイアウォールの背後に配置されます。ハイブリッド データセキュリティ ノードへのインバウンド接続の場合、インターネットから可視になるポートはありません。データ センター内でクライアントが管理目的で Hybrid Data Security ノードにアクセスするには、TCP ポート 443 および 22 を使用する必要があります。

共通アイデンティティ（CI）ホストの URL は、リージョン固有のものです。現在の CI ホストは次のとおりです。

リージョン	共通アイデンティティ ホストの URL
アメリカ地域	• https://idbroker.webex.com • https://identity.webex.com • https://idbroker-b-us.webex.com • https://identity-b-us.webex.com
欧州連合	• https://idbroker-eu.webex.com • https://identity-eu.webex.com
Canada	• https://idbroker-ca.webex.com • https://identity-ca.webex.com

プロキシ サーバの要件

- Hybrid Data Security ノードに統合できるプロキシ ソリューションとして公式にサポートされているのは、次のプロキシです。
  - 透過的なプロキシ：Cisco Web セキュリティ アプライアンス（WSA）
  - 明示的なプロキシ：Squid

（注） HTTPS トラフィックを検査する Squid プロキシは、WebSocket（wss）の接続確立に干渉する可能性があります。この問題を回避するには、「Hybrid Data Security の Squid プロキシの構成」を参照してください。

- 明示的なプロキシでは、次の認証タイプの組み合わせがサポートされています。
  - HTTP または HTTPS を使用した認証なし

- HTTP または HTTPS を使用した基本認証
- HTTPS のみを使用したダイジェスト認証

- 透過的な検査プロキシまたは明示的な HTTPS プロキシの場合、プロキシのルート証明書のコピーが必要です。このガイドの導入手順で、Hybrid Data Security ノードの信頼ストアにコピーをアップロードする方法を説明しています。
- HDS ノードをホストするネットワークは、ポート 443 でアウトバウンド TCP トラフィックを強制的にプロキシ経由でルーティングするように構成されている必要があります。
- Web トラフィックを検査するプロキシは、WebSocket 接続に干渉する可能性があります。この問題が発生した場合、`wbx2.com` および `ciscospark.com` へのトラフィックをバイパスする（検査しない）と、問題が解決します。

Hybrid Data Security の前提条件への対応

次のチェックリストを使用して、ハイブリッド データ セキュリティ クラスタをインストールして構成できるよう準備してください。

手順

ステップ 1 Webex 組織が Pro Pack for Cisco Webex Control Hub に対して有効になっていることを確認し、完全な組織管理者権限を持つアカウントのクレデンシャルを取得します。このプロセスの詳細については、シスコ パートナーまたはアカウント マネージャにお問い合わせください。

ステップ 2 HDS 導入環境に使用するドメイン名を選択し（たとえば、`hds.company.com`）、x.509 証明書、秘密キー、およびすべての中間証明書を含む証明書チェーンを取得します。証明書チェーンは、「X.509 証明書の要件 （1 ページ）」に記載されている要件を満たしている必要があります。

ステップ 3 クラスタ内の ハイブリッド データ セキュリティ ノードとしてセットアップする同等の仮想ホストを準備します。「仮想ホストの要件 （2 ページ）」に記載されている要件を満たす個別のホストが、同じセキュア データ センターに少なくとも 2 つ（推奨は 3 つ）が配置されている必要があります。

ステップ 4 「データベースサーバの要件 （3 ページ）」に従って、クラスタのキーデータストアとして機能するデータベース サーバを準備します。このデータベース サーバは、仮想ホストと同じセキュアなデータ センター内に配置されている必要があります。

a) キー ストレージのデータベースを作成します。（このデータベースは新規作成する必要があります。デフォルトのデータベースは使用しないでください。HDS アプリケーションは、インストール時にデータベース スキーマを作成します。）

b) ノードがデータベース サーバとの通信に使用する次の詳細情報を収集します。

- ホスト名または IP アドレス（ホスト）とポート
- キー ストレージとして使用するデータベースの名前（dbname）

- キー ストレージ データベースに対するすべての権限を持つユーザのユーザ名とパスワード

ステップ 5 迅速にディザスタ リカバリを行えるように、別のデータ センターにバックアップ環境をセットアップします。バックアップ環境には、VM の実稼働環境とバックアップ データベース サーバをミラーリングします。たとえば、実稼働環境に HDS ノードを実行する 3 つの VM がある場合、バックアップ環境にも 3 つの VM が必要です。

ステップ 6 クラスタ内のノードからログを収集する Syslog ホストをセットアップします。Syslog ホストのネットワーク アドレスと Syslog ポート（デフォルトは UDP 514）を収集します。

ステップ 7 ハイブリッド データ セキュリティ ノード、データベース サーバ、および syslog ホストのセキュア バックアップ ポリシーを作成します。回復不能なデータ損失を防ぐために、少なくともハイブリッド データ セキュリティ ノードで生成されたデータベースと構成 ISO ファイルをバックアップする必要があります。

注意 ハイブリッド データ セキュリティ ノードにはコンテンツの暗号化と復号に使用されるキーが保管されるため、運用中の導入環境が保守されていないと、そのコンテンツが**回復不能**になります。

Webex アプリ クライアントは自身のキーをキャッシュするため、停止してもすぐには認識されず、その状態は徐々に明らかになります。一時的な停止は防ぐことができませんが、回復可能です。ただし、データベースまたは構成 ISO ファイルのいずれかを完全に損失すると（使用可能なバックアップがない状態）、顧客データが回復不能になります。ハイブリッド データ セキュリティ ノードのオペレータは、データベースと構成 ISO ファイルを頻繁にバックアップし、壊滅的な障害が発生した場合にハイブリッド データ セキュリティ データ センターを再構築できるよう準備する必要があります。

ステップ 8 ファイアウォールが、「外部接続の要件 （4 ページ）」で説明されている ハイブリッド データ セキュリティ ノードに対する接続を許可するように構成されていることを確認します。

ステップ 9 サポート対象の OS（Microsoft Windows 10 Professional または Enterprise 64 ビット、あるいは Mac OSX Yosemite 10.10.3 以降）で稼働し、http://127.0.0.1:8080 でアクセスできる Web ブラウザがインストールされている任意のローカル マシンに Docker（https://www.docker.com）をインストールします。

Docker インスタンスを使用して HDS セットアップ ツールをダウンロードして実行します。これにより、すべての ハイブリッド データ セキュリティ ノードのローカル構成情報が形成されます。組織によっては、Docker Desktop ライセンスが必要な場合があります。詳細については、「Docker Desktop の要件 （1 ページ）」を参照してください。

HDS セットアップ ツールをインストールして実行するには、ローカル マシンが「外部接続の要件 （4 ページ）」に記載されている接続要件を満たしている必要があります。

ステップ 10 プロキシを ハイブリッド データ セキュリティ に統合する場合は、「プロキシ サーバの要件 （5 ページ）」を満たしていることを確認します。

ステップ 11 組織でディレクトリ同期を使用している場合は、Active Directory に `HdsTrialGroup` という名前のグループを作成し、そのグループにパイロット ユーザを追加します。トライアル グループには、最大 250 のユーザを含めることができます。`HdsTrialGroup` オブジェクトをクラウドに

同期してからでないと、組織でトライアルを開始できません。グループ オブジェクトを同期するには、ディレクトリ コネクタの **[構成（Configuration）]** > **[オブジェクト選択（Object Selection）]** メニューからグループ オブジェクトを選択します。（詳細な手順については、『Cisco Directory Connector 導入ガイド』を参照してください）。

注意 所定のスペースのキーは、そのスペースの作成者によって設定されます。パイロット ユーザを選択する際は、ハイブリッド データ セキュリティ 導入環境を永久に非アクティブ化することにした場合、パイロットユーザが作成したスペース内のコンテンツにすべてのユーザがアクセスできなくなることに留意してください。アクセスできなくなったことは、ユーザのアプリがキャッシュされたコンテンツのコピーを更新した時点ですぐに明らかになります。

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。