



Cisco pxGrid

- [Cisco pxGrid と ISE \(1 ページ\)](#)

Cisco pxGrid と ISE



(注) Cisco ISE リリース 3.1 以降、すべての pxGrid 接続は pxGrid 2.0 に基づく必要があります。pxGrid 1.0 ベース (XMPP ベース) の統合は、リリース 3.1 以降の Cisco ISE では動作しなくなります。

WebSocket に基づく pxGrid バージョン 2.0 は、Cisco ISE リリース 2.4 で導入されました。統合の中断を防ぐために、他のシステムを計画して pxGrid 2.0 準拠バージョンにアップグレードすることをお勧めします。

Cisco Platform Exchange Grid (pxGrid) は、オープンで拡張性のある Security Product Integration Framework であり、双方向の Any-to-Any パートナープラットフォーム統合を可能にします。

pxGrid 2.0 は REST および WebSocket インターフェイスを使用します。クライアントは、制御メッセージ、クエリ、アプリケーションデータに REST を使用し、イベントをプッシュするために WebSocket を使用します。pxGrid 2.0 の詳細については、『[Welcome to Learning Cisco Platform Exchange Grid \(pxGrid\)](#)』を参照してください。

Cisco pxGrid Direct の詳細については、[Cisco pxGrid Direct](#) を参照してください。

pxGrid は次のことができます。

- Cisco ISE セッションディレクトリからの状況依存情報を、Cisco ISE エコシステムのパートナーシステムなどの他のネットワークシステムや他のシスコプラットフォームと共有する。
- サードパーティシステムが適応型のネットワーク制御アクションを呼び出し、ネットワークまたはセキュリティイベントに応じてユーザーおよびデバイスを検疫できるようにする。タグ定義、値、説明などの TrustSec 情報を、TrustSec トピックを介して Cisco ISE から別のネットワークに渡す。

- 完全修飾名 (FQN) を持つエンドポイントプロファイルを、エンドポイントプロファイルメタトピックを通して Cisco ISE から他のネットワークに渡す。
- タグおよびエンドポイントプロファイルを一括ダウンロードする。
- pxGrid 経由で SXP バインディング (IP-SGT マッピング) を発行および登録する。SXP バインディングの詳細については、『[Segmentation chapter of the Cisco ISE Administrators Guide](#)』の「*Security Group Tag Exchange Protocol*」のセクションを参照してください。
- Cisco pxGrid Context-in を使用すると、エコシステムパートナーはトピック情報を Cisco ISE に公開できます。これにより、Cisco ISE は、エコシステムで特定された資産に基づいてアクションを実行できます。Cisco pxGrid Context-in の詳細については、「[pxGrid Context-In](#)」を参照してください。

pxGrid の概要

pxGrid には次のコンポーネントがあります。

- コントローラ：検出、認証、および許可を処理します。
- プロバイダー：クエリ結果を返すか、または発行します。
- Pubsub：プロバイダーとコンシューマに pxGrid サービスを提供します。
- サブスクリバ：サブスクリバは、承認されると、登録しているトピックからコンテキスト情報とアラートを取得します。

pxGrid には次の機能があります。

- 検出：サービス名に基づいてサービスプロパティを検出します。フローは、プロバイダーが pxGrid コントローラで「サービスの登録」を要求したときに開始されます。登録後、コンシューマは「ルックアップサービス」を使用してプロバイダーの場所を検出します。
- 認証：pxGrid コントローラは、サービスにアクセスするために pxGrid クライアントを認証します。ログイン情報は、ユーザー名とパスワード、または証明書 (推奨) です。
- 許可：pxGrid は操作要求を取得すると、pxGrid コントローラに問い合わせで要求を許可し、クライアントを事前定義されたグループに割り当てます。

pxGrid 2.0 の高可用性

pxGrid 2.0 ノードはアクティブ/アクティブ構成で動作します。高可用性を実現するには、導入環境に少なくとも 2 つの pxGrid ノードが必要です。大規模な導入では、拡張性と冗長性を高めるために最大 4 つのノードを使用できます。あるノードがダウンした場合に、そのノードのクライアントが動作中のノードに接続できるように、すべてのノードの IP アドレスを設定することをお勧めします。PAN がダウンすると、pxGrid サーバーは、アクティブ化処理を停止します。pxGrid サーバーをアクティブにするには、PAN を手動で昇格させます。pxGrid の展開の詳細については、『[ISE Performance & Scale](#)』を参照してください。

すべての pxGrid サービスプロバイダーのクライアントは、7.5 分以内に pxGrid コントローラに定期的に再登録します。クライアントが再登録しない場合、PAN ノードは非アクティブである

と見なし、そのクライアントを削除します。PAN ノードが 7.5 分を超えてダウンした場合、再度起動すると、タイムスタンプ値が 7.5 分よりも古いすべてのクライアントが削除されます。これらのクライアントはすべて、pxGrid コントローラに再度登録する必要があります。

pxGrid 2.0 クライアントでは、PubSub やクエリに WebSocket および REST ベースの API を使用しています。これらの API は、ポート 8910 で ISE アプリケーションサーバーによって提供されます。show logging application pxgrid を実行して表示される pxGrid プロセスは、pxGrid 2.0 には適用されません。



(注) GUI および CLI では、pxGrid 1.0 プロセスへのすべての参照が削除されています。

損失検出

Cisco ISE 3.0 では、pxGrid トピックにシーケンス ID が追加されました。送信に中断がある場合、サブスクライバは ID のシーケンスのギャップをチェックすることで中断を認識できます。サブスクライバはトピックシーケンス ID の変更気付、最後のシーケンス番号の日付に基づいてデータを要求します。パブリッシャがダウンして復帰した場合、トピックシーケンスは 0 から始まります。サブスクライバはシーケンス 0 を確認したら、キャッシュをクリアして一括ダウンロードを開始する必要があります。サブスクライバがダウンした場合、パブリッシャはシーケンス ID を割り当て続けます。サブスクライバが再接続し、シーケンス ID にギャップがある場合、サブスクライバは最後のシーケンス番号の時刻からデータを要求します。損失検出は、セッションディレクトリおよび TrustSec 構成で機能します。セッションディレクトリを使用している場合、損失を検出したクライアントは、キャッシュをクリアして一括ダウンロードを開始する必要があります。

シーケンス ID を使用しない既存のアプリケーションがある場合は、シーケンス ID を使用する必要はありません。ただし、シーケンス ID を使用すると、損失検出と損失からの回復という利点を得られます。

セッションディレクトリのセッションは、/topic/com.cisco.ise.session への通知間隔ごとに MnT によって非同期的にバッチ処理され、公開されます。

TrustSec セキュリティグループへの変更

は、/topic/com.cisco.ise.config.trustsec.security.group に公開されます。

損失検出は pxGrid 2.0 でのみサポートされ、デフォルトで有効になっています。

損失検出を使用したコード例、<https://github.com/cisco-pxgrid/pxgrid-rest-ws/tree/master/java/src/main/java/com/cisco/pxgrid/samples/ise> を参照してください。

モニタリングとデバッグ

pxGrid では、次のログを使用できます。

- pxgrid-server.log : pxGrid 2.0 のアクティビティとエラー

[ログ (Logs)] ページには、すべての pxGrid 2.0 管理イベントが表示されます。イベント情報には、クライアント名と機能名、およびイベントタイプとタイムスタンプが含まれています。

[管理 (Administration)] > [pxGridサービス (pxGrid Services)] > [診断 (Diagnostics)] > [ログ (Log)] の順に移動して、イベントリストを表示します。ログを消去して、リストを再同期またはリフレッシュすることもできます。

pxGrid の概要ページ

pxGrid の [概要 (Summary)] ページには、現在の pxGrid 2.0 環境の統計情報が表示されます。

- [現在の接続 (Current Connections)] : コントローラへの接続のリストが表示されます。
- [制御メッセージ (Control Messages)] : 認証、認可、およびサービスディスカバリ。
- [REST API] : WebSocket または XMPP を使用して接続したクライアントの数。
- [PubSub スループット (Pubsub Throughput)] : クライアントにパブリッシュされたデータの量。
- [クライアント (Clients)] : REST または WebSocket によって接続されたクライアント。
- [エラー (Errors)] : クライアントがデータ転送の再開を要求する原因となった送信エラーの数。

pxGrid クライアント管理

クライアントは、Cisco ISE で pxGrid サービスを使用するためにアカウントを登録して承認を受ける必要があります。クライアントは、登録するために pxGrid SDK を介して pxGrid クライアントライブラリを使用します。Cisco ISE は、自動と手動両方の登録をサポートします。

- [クライアント (Clients)] : [管理 (Administration)] > [pxGridサービス (pxGrid Services)] > [クライアント管理 (Client Management)] > [クライアント (Clients)] を選択して、このウィンドウを表示します。pxGrid 2.0 の外部クライアントアカウントが一覧表示されます。
- [pxGridポリシー (pxGrid Policy)] : [管理 (Administration)] > [pxGridサービス (pxGrid Services)] > [クライアント管理 (Client Management)] > [pxGridポリシー (pxGrid Policy)] を選択して、このウィンドウを表示します。クライアントが登録できる使用可能なサービスのリストが表示されます。ポリシーを編集して、そのポリシーにアクセスできるグループを変更できます。まだポリシーがないサービスに新しいポリシーを作成することもできます。
- [グループ (Groups)] : [管理 (Administration)] > [pxGridサービス (pxGrid Services)] > [クライアント管理 (Client Management)] > [グループ (Groups)] を選択して、このウィンドウを表示します。ANC は事前定義されたグループです。他のグループを追加し、それらのグループを使用してサービスへのアクセスを制限できます。

pxGrid クライアントは、REST API を介してユーザー名を送信することで、pxGrid コントローラに自身を登録できます。pxGrid コントローラは、クライアント登録時に pxGrid クライアントのパスワードを生成します。管理者は接続要求を承認または拒否できます。

- [証明書 (Certificates)] : [管理 (Administration)] > [pxGridサービス (pxGrid Services)] > [クライアント管理 (Client Management)] > [証明書 (Certificates)] を選択して、このウィンドウを表示します。Cisco ISE 内部認証局を使用する新しい証明書を生成できます。

pxGrid の証明書の作成については、次を参照してください。

- [Cisco pxGrid での証明書の展開 : Cisco ISE 2.0/2.1/2.2 への自己署名証明書の更新の使用 \[英語\]](#)
- [Cisco pxGrid での証明書の展開 : Cisco ISE 2.0/2.1/2.2 へのアップデートでの外部 CA の使用 \[英語\]](#)

pxGrid ポリシーの制御

pxGrid クライアントがアクセスできるサービスへのアクセスを制御する pxGrid 認証ポリシーを作成できます。これらのポリシーは、pxGrid クライアントで使用できるサービスを制御します。

さまざまなタイプのグループを作成して、pxGrid クライアントで使用可能なサービスをこれらのグループにマッピングできます。[クライアント管理 (Client Management)] > [グループ (Groups)] ウィンドウの [グループの管理 (Manage Groups)] オプションを使用して、新しいグループを追加します。[Client Management] > [Policies] ウィンドウでは、許可ルールの例を表示できます。

pxGrid クライアントの認証ポリシーを作成するには、次の手順を実行します。

ステップ 1 [管理 (Administration)] > [pxGridサービス (pxGrid Services)] > [クライアント管理 (Client Management)] > [ポリシー (Policy)] を選択し、[追加 (Add)] をクリックします。

ステップ 2 [サービス (Service)] ドロップダウン リストから、次のいずれかのオプションを選択します。

- com.cisco.ise.radius
- come.cisco.ise.sxp
- com.cisco.ise.trustsec
- com.cisco.ise.session
- com.cisco.ise.system
- com.cisco.ise.mdm
- com.cisco.ise.config.trustsec
- com.cisco.ise.config.profiler
- com.cisco.ise.pxgrid.admin
- com.cisco.ise.config.deployment.node
- com.cisco.ise.endpoint
- com.cisco.ise.config.anc

- com.cisco.ise.dnac
- com.cisco.ise.config.upn
- com.cisco.ise.pubsub

ステップ 3 [操作 (Operations)] ドロップダウン リストから、次のいずれかのオプションを選択します。

- <ANY>
- パブリッシュ
- publish /topic/com.cisco.ise.session
- publish /topic/com.cisco.ise.session.group
- publish /topic/com.cisco.ise.anc
- <CUSTOM>—このオプションを選択すると、カスタム操作を指定できます。

ステップ 4 [グループ (Groups)] ドロップダウンリストから、このサービスにマッピングするグループを選択します。

(EPSやANCなどの) 事前に定義されたグループ、および手動で追加したグループがこのドロップダウンリストに表示されます。

(注) ポリシーに含まれるグループの一部であるクライアントのみが、そのポリシーで指定されたサービスに登録できます。

ステップ 5 [Submit] をクリックします。

pxGrid サービスの有効化

始める前に

- Cisco pxGrid クライアントからの要求を表示するには、少なくとも 1 つのノードで pxGrid ペルソナを有効にします。
-

ステップ 1 Cisco ISE GUI で [メニュー (Menu)] アイコン (☰) をクリックして次を選択します。 [管理 (Administration)] > [pxGrid サービス (pxGrid Services)]。

ステップ 2 クライアントの隣にあるチェックボックスをオンにして [承認 (Approve)] をクリックします。

ステップ 3 [リフレッシュ (Refresh)] をクリックすると、最新のステータスが表示されます。

ステップ 4 有効にする機能を選択し、[有効 (Enable)] をクリックします。

ステップ 5 [リフレッシュ (Refresh)] をクリックすると、最新のステータスが表示されます。

pxGrid 診断

- [WebSocket] : [管理 (Administration)] > [pxGridサービス (pxGrid Services)] > [診断 (Diagnostics)] > [WebSocket] ウィンドウには、pxGrid 2.0 クライアント (外部および内部) のリストが表示されます。また、使用可能な pxGrid 2.0 トピック、および各トピックを公開または登録するクライアントのリストも表示されます。
- [ログ (Log)] : [管理 (Administration)] > [pxGridサービス (pxGrid Services)] > [診断 (Diagnostics)] > [ライブログ (Live Logs)] ウィンドウに管理イベントのリストが表示されます。
- [テスト (Tests)] : [管理 (Administration)] > [pxGridサービス (pxGrid Services)] > [診断 (Diagnostics)] > [テスト (Tests)] > [ヘルスマonitoringテスト (Health Monitoring test)] を選択し、[テストの開始 (Start Test)] をクリックして、クライアントがセッションディレクトリサービスにアクセスできることを確認します。テストが完了すると、テストアクティビティのログを表示できます。

pxGrid 設定

[管理 (Administration)] > [pxGridサービス (pxGrid Services)] > [設定 (Settings)] ウィンドウで、次のオプションのいずれかを選択します。

- [新しい証明書ベースのアカウントを自動的に承認する (Automatically approve new certificate-based accounts)] : このオプションはデフォルトで無効になっています。これにより、pxGrid サーバーへの接続を制御できます。環境内のすべてのクライアントを信頼している場合にのみ、このオプションを有効にします。
- [パスワードベースのアカウント作成の許可 (Allow password based account creation)] : このチェックボックスをオンにすると、pxGrid クライアントのユーザー名/パスワードベースの認証が有効になります。このオプションを有効にした場合、pxGrid クライアントを自動的に承認することはできません。

Cisco pxGrid 証明書の生成

始める前に

- Cisco ISE pxGrid サーバーと pxGrid クライアントに同じ証明書を使用しないでください。pxGrid クライアントにはクライアント証明書を使用する必要があります。クライアント証明書を生成するには、[Administration] > [System] > [Certificates] を選択します。
- Cisco ISE の一部のバージョンには NetscapeCertType を使用する Cisco pxGrid の証明書があります。新しい証明書を生成することを推奨します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- pxGrid 証明書はプライマリ PAN から生成する必要があります。

- Cisco pxGrid 証明書がサブジェクト代替名 (SAN) の拡張を使用する場合、DNS 名のエントリとしてサブジェクト ID の FQDN が含まれるようにします。
- デジタル署名を使用して証明書テンプレートを作成し、新しい Cisco pxGrid 証明書を生成します。



(注) FIPS モードが有効になっている場合、pxGrid 証明書テンプレートの RSA 秘密キーのサイズは 2048 ビット以上である必要があります。それ以外の場合、pxGrid 証明書を生成しようとするとエラーが表示されます。証明書テンプレートの秘密キーサイズを変更するには、[pxGrid 証明書テンプレートのキーサイズの変更 \(10 ページ\)](#) を参照してください。

ステップ 1 Cisco ISE GUI で [メニュー (Menu)] アイコン (☰) をクリックして次を選択します。[管理 (Administration)] > [pxGrid サービス] > [クライアント管理] > [証明書 (Certificates)]。

ステップ 2 [処理の選択 (I want to)] ドロップダウンリストから、次のオプションのいずれかを選択します。

- [単一の証明書の生成 (証明書署名要求なし) (Generate a single certificate (without a certificate signing request))] : このオプションを選択した場合は、共通名 (CN) を入力する必要があります。
- [単一の証明書の生成 (証明書署名要求あり) (Generate a single certificate (with a certificate signing request))] : このオプションを選択した場合は、証明書署名要求の詳細を入力する必要があります。

ステップ 3 (オプション) この証明書の説明を入力します。

ステップ 4 [pxGrid_Certificate_Template] のリンクをクリックして証明書テンプレートをダウンロードし、必要に応じて編集します。

ステップ 5 [サブジェクト代替名 (SAN) (Subject Alternative Name (SAN))] を指定します。複数の SAN を追加できます。次のオプションを使用できます。

- [IP アドレス (IP address)] : この証明書に関連付ける Cisco pxGrid クライアントの IP アドレスを入力します。
- [FQDN] : pxGrid クライアントの FQDN を入力します。

ステップ 6 [証明書のダウンロード形式 (Certificate Download Format)] ドロップダウンリストから、以下のいずれかのオプションを選択します。

- [Private Enhanced Electronic Mail (PEM) 形式の証明書、PKCS8 PEM 形式のキー (証明書チェーンを含む) (Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain))] : ルート証明書、中間 CA 証明書、およびエンドエンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「-----BEGIN CERTIFICATE-----」タグで始まり、「-----END CERTIFICATE-----」タグで終わります。エンドエンティティの秘密キーは PKCS* PEM を使用して格納されています。

「-----BEGIN ENCRYPTED PRIVATE KEY-----」タグで始まり、「-----END ENCRYPTED PRIVATE KEY-----」タグで終わります。

- [PKCS12形式 (証明書チェーンを含む。つまり証明書チェーンとキーの両方で1ファイル) (PKCS12 format (including certificate chain; one file for both the certificate chain and key))] : 1つの暗号化ファイルにルート CA 証明書、中間 CA 証明書、およびエンドエンティティの証明書と秘密キーを格納するバイナリ形式。

ステップ 7 証明書のパスワードを入力します。

ステップ 8 [作成 (Create)] をクリックします。

作成した証明書は、[発行された証明書 (Issued Certificates)] ウィンドウに表示されます。このウィンドウを表示するには、[メニュー (Menu)] アイコン (☰) をクリックして次を選択します。[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [認証局 (Certificate Authority)] > [発行された証明書 (Issued Certificates)]。

(注) Cisco ISE 2.4 パッチ 13 以降、pxGrid サービスの証明書要件がより厳格になりました。pxGrid 証明書に Cisco ISE のデフォルトの自己署名証明書を使用している場合、Cisco ISE 2.4 パッチ 13 以降の適用後に証明書が Cisco ISE によって拒否されることがあります。これは、その証明書の以前のバージョンに、**SSL サーバー**として指定された **Netscape Cert Type** 拡張があるためです。これは現在は失敗するようになっています (現在はクライアント証明書も必要)。

非標準の証明書を持つクライアントは、Cisco ISE と統合できません。内部 CA によって発行された証明書を使用するか、適切な Usage 拡張を指定して新しい証明書を生成します。

- 証明書の [キーの使用法 (Key Usage)] の拡張には、[デジタル署名 (Digital Signature)] フィールドと [キー暗号化 (Key Encipherment)] フィールドが含まれている必要があります。
- 証明書の [拡張キーの使用法 (Extended Key Usage)] の拡張には、[クライアント承認 (Client Authentication)] フィールドと [サーバー承認 (Server Authentication)] フィールドが含まれている必要があります。
- 証明書に [Netscape 証明書タイプ (Netscape Certificate Type)] の拡張は必要ありません。その拡張を含める場合は、**SSL Client** と **SSL Server** の両方を拡張に追加します。
- 自己署名証明書を使用している場合は、**Basic Constraints CA** フィールドを **TRUE** にし、**Key Usage** の拡張に **Key Cert Sign** フィールドを含める必要があります。

pxGrid 証明書の生成における既知の制限

Cisco ISE での pxGrid 証明書の生成は、次に説明する表形式のロジックに従います。

シリアル番号	システム証明書 (EAP)	発行元証明書	pxGrid 形式	サポート
1	複数の共通名	単一の共通名	PKCS8、PKCS12	サポート対象
2	複数の共通名	複数の共通名	PKCS12	サポート対象

シリアル番号	システム証明書 (EAP)	発行元証明書	pxGrid 形式	サポート
3	複数の共通名	複数の共通名	PKCS8	サポート対象外

pxGrid 証明書テンプレートのキーサイズの変更

次のタスクは、pxGrid 証明書テンプレートのキーサイズを変更するのに役立ちます。

-
- ステップ 1** Cisco ISE GUI で [メニュー (Menu)] アイコン (☰) をクリックして次を選択します。 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [認証局 (Certificate Authority)] > [証明書テンプレート (Certificate Templates)] を選択します。
- ステップ 2** テンプレート **pxGrid_Certificate_Template** の横にあるチェックボックスをオンにします。
- ステップ 3** [編集 (Edit)] をクリックします。
- ステップ 4** [キーサイズ (Key Size)] ドロップダウンリストから、[2048] を選択します。
- ステップ 5** [Save] をクリックします。
-

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。