Cisco Identity Services Engine リリース 2.7 リリースノート

（注） content.cisco.com のコンテンツハブに移動します。ここでは、ファセット検索機能を使用して、必要なコンテンツを正確に拡大できます。参照用にカスタマイズした PDF ブックを簡単に作成するなど、数多くのことが可能です。

早速始めましょう。content.cisco.com をクリックしてください。

また、コンテンツハブをすでに体験したことがある場合は、ご意見をお聞かせください。

ページの [フィードバック（Feedback）] アイコンをクリックして、ご意見をお寄せください。

Cisco Identity Services Engine の概要

Cisco Identity Services Engine（ISE）は、ネットワークリソースへのセキュアなアクセスを提供するセキュリティポリシー管理プラットフォームです。企業は、Cisco ISE を使用して、ネットワーク、ユーザー、およびデバイスからコンテキスト情報をリアルタイムで収集できます。その後、管理者はこの情報を使用して、積極的に管理上の決定を下すことができます。これを行うには、アクセススイッチ、ワイヤレスコントローラ、バーチャルプライベートネットワーク（VPN）ゲートウェイ、5GaaS ネットワーク、データセンタースイッチなどのさまざまなネットワーク要素のアクセス コントロール ポリシーを作成します。Cisco ISE は、Cisco TrustSec ソリューションのポリシーマネージャとして機能し、TrustSec ソフトウェアによって定義されたセグメンテーションをサポートします。

Cisco ISE は、異なるパフォーマンス特性を持つセキュアなネットワーク サーバー アプライアンス上で使用できます。また、仮想マシン（VM）上で実行できるソフトウェアとしても使用可能です。パフォーマンス向上のためにアプライアンスを展開に追加できます。

Cisco ISE は、スタンドアロンおよび分散展開をサポートする拡張性の高いアーキテクチャを使用しますが、設定および管理は一元化されています。また、ペルソナとサービスの設定と管理を個別に行うこともできます。このため、ネットワーク内で必要なサービスを作成して適用することができますが、Cisco ISE 展開を完全な統合システムとして運用することもできます。

Cisco ISE の詳細な発注およびライセンス情報については、 *Cisco IdentityServices Engine 注文ガイド* [英語] を参照してください。

システムのモニタリングおよびトラブルシューティングに関する詳細については、『*Cisco Identity Services Engine Administrator Guide*』の「Monitoring and Troubleshooting Cisco ISE」のセクションを参照してください。

システム要件

Cisco ISE の設定を継続使用する場合は、次のシステム要件が満たされていることを確認してください。

この Cisco ISE リリースのハードウェア プラットフォームおよびインストールの詳細については、『Cisco Identity Services Engine Hardware Installation Guide』を参照してください。

サポート対象ハードウェア

Cisco ISE リリース 2.7 は、次のプラットフォームにインストールできます。

表 *1:* サポートされるプラットフォーム

ハードウェア プラットフォーム	設定
Cisco SNS-3515-K9（小規模）	アプライアンスハードウェアの仕様については、『*Cisco Secure Network Server Appliance Hardware Installation Guide*』を参照してください。
Cisco SNS-3595-K9（大規模）	
Cisco SNS-3615-K9（小規模）	
Cisco SNS-3655-K9（中規模）	
Cisco SNS-3695-K9（大規模）	

インストール後、上記の表に記載されているプラットフォームで、管理、モニターリング、pxGrid などの特定のコンポーネントペルソナを使用して Cisco ISE を設定できます。これらのペルソナに加えて、Cisco ISE では、プロファイリングサービス、セッションサービス、脅威中心型 NAC サービス、TrustSec 用の SXP サービス、TACACS+ デバイス管理サービス、およびパッシブ ID サービスなど、ポリシーサービス内に他のタイプのペルソナが含まれています。

注意

- Cisco ISE 3.1 以降のリリースは、Cisco Secured Network Server（SNS）3515 アプライアンスをサポートしていません。
- Cisco SNS 3400 シリーズ アプライアンスは、Cisco ISE リリース 2.4 以降ではサポートされていません。
- 16 GB 未満のメモリの割り当ては、VM アプライアンスの設定ではサポートされていません。Cisco ISE の動作に問題が発生した場合、すべてのユーザーは、Cisco Technical Assistance Center に連絡する前に割り当てメモリを 16 GB 以上に変更する必要があります。
- レガシー アクセス コントロール サーバー（ACS）およびネットワーク アクセス コントロール（NAC）アプライアンス（Cisco ISE 3300 シリーズを含む）は、Cisco ISE リリース 2.0 以降ではサポートされていません。

連邦情報処理標準（FIPS）モードのサポート

Cisco ISE は、組み込みの連邦情報処理標準（FIPS）140-2 検証済み暗号化モジュール、Cisco FIPS オブジェクト モジュール バージョン 6.2（証明書 #2984）を使用します。FIPS コンプライアンス要求の詳細については、Global Government Certifications を参照してください。

Cisco ISE で FIPS モードが有効になっている場合は、次の点を考慮してください。

- すべての FIPS 非準拠暗号スイートは無効になります。
- 証明書と秘密キーには、FIPS 準拠ハッシュと暗号化アルゴリズムのみを使用する必要があります。
- RSA 秘密キーには、2048 ビット以上を指定する必要があります。
- 楕円曲線デジタル署名アルゴリズム（ECDSA）の秘密キーには、224 ビット以上を指定する必要があります。
- Diffie–Hellman Ephemeral（DHE）暗号方式は 2048 ビット以上の Diffie–Hellman（DH）パラメータを使用して動作します。
- SHA1 は、ISE ローカルサーバー証明書の生成を許可されていません。
- EAP-FAST の匿名 PAC プロビジョニングオプションは無効です。
- ローカル SSH サーバーは FIPS モードで動作します。
- RADIUS の場合、次のプロトコルは FIPS モードではサポートされていません。
  - EAP-MD5
  - PAP
  - CHAP

- MS-CHAPv1
- MS-CHAPv2
- LEAP

サポートされる仮想環境

Cisco ISE は次の仮想環境プラットフォームをサポートしています。

- VMware ESXi 5.x、6.x、7.x
- Microsoft Windows Server 2012 R2 以降の Microsoft Hyper-V
- QEMU 1.5.3-160 上の KVM

仮想マシンの要件に関する情報については、お使いの Cisco ISE バージョンの『*Cisco Identity Services Engine インストールガイド*』を参照してください。

注意 Cisco ISE は、ISE データのバックアップ用の VMware スナップショットをサポートしていません。これは、VMware スナップショットが特定の時点で VM のステータスを保存するためです。マルチノード Cisco ISE 環境では、すべてのノードのデータは、現在のデータベース情報と継続的に同期されます。スナップショットを復元すると、データベースのレプリケーションと同期の問題を引き起こす可能性があります。データのバックアップおよび復元用に、Cisco ISE に含まれるバックアップ機能を使用することを推奨します。

VMware スナップショットを使用して ISE データをバックアップすると、Cisco ISE サービスが停止します。ISE ノードを起動するには、再起動が必要です。

サポートされるブラウザ

管理者ポータルでサポートされているブラウザは次のとおりです。

- Mozilla Firefox 96 以前のバージョン（バージョン 82 以降）
- Mozilla Firefox ESR 91.3 以前のバージョン
- Google Chrome 97 以前のバージョン （バージョン 86 以降）
- Microsoft Edge の最新バージョンと最新バージョンより 1 つ前のバージョン

Microsoft Active Directory のサポート

Cisco ISE は、すべての機能レベルで Microsoft Active Directory サーバー 2003、2003 R2、2008、2008 R2、2012、 2012 R2、2016、および 2019 と連携して動作します。

（注）

- Windows サーバーをサポート対象バージョンにアップグレードすることをお勧めします。Microsoft は Windows サーバー 2003 および 2003 R2 のサポートを終了しています。
- Microsoft Active Directory バージョン 2000 またはその機能レベルは、Cisco ISE ではサポートされていません。

Cisco ISE は、マルチドメインフォレストと Active Directory インフラストラクチャとの統合をサポートし、大規模なエンタープライズネットワーク全体の認証および属性の収集をサポートしています。Cisco ISE は最大 50 個のドメイン参加ポイントをサポートしています。

ユーザー識別の改善

Cisco ISE は、ユーザー名が一意でなくても Active Directory ユーザーを識別できます。マルチドメインの Active Directory 環境で短いユーザー名を使用する場合、一般的にユーザー名が重複します。ソフトウェア資産管理（SAM）、顧客名（CN）、またはその両方を使用してユーザーを識別できます。Cisco ISE は、ユーザーを一意に識別するために属性を使用します。

次の値を更新します。

- SAM：クエリで SAM のみを使用するには、この値を更新します（デフォルト）。
- CN：クエリで CN のみを使用するには、この値を更新します。
- CNSAM：クエリで CN および SAM を使用するには、この値を更新します。

Active Directory ユーザーの識別用に上記の属性を設定するには、Active Directory を実行しているサーバーのレジストリで **IdentityLookupField** パラメータを更新します。

```
REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField
```

サポート対象のウイルス対策およびマルウェア対策製品

Cisco ISE ポスチャエージェントでサポートされているウイルス対策およびマルウェア対策製品の詳細については、Cisco AnyConnect ISE ポスチャのサポート表を参照してください。

サポート対象の暗号方式

Cisco ISE のクリーンインストールまたは新規インストールでは、SHA1 暗号はデフォルトで無効になっています。ただし、既存のバージョンの Cisco ISE からアップグレードする場合、SHA1 暗号は以前のバージョンのオプションのままです。SHA1 暗号の設定は、[SHA1暗号を許可する（Allow SHA1 Ciphers）] フィールド（[管理（Administration）]>[システム（System）]>[設定（Settings）]>[セキュリティ設定（Security Settings）]）を使用して表示および変更できます。

（注） この暗号は、管理者ポータルには適用されません。連邦情報処理標準モード（FIPS）で実行している場合、アップグレードでは管理者ポータルから SHA1 暗号が削除されません。

Cisco ISE は、TLS バージョン 1.0、1.1、および 1.2 をサポートします。

Cisco ISE は、RSA および ECDSA サーバー証明書をサポートしています。次の楕円曲線をサポートしています。

- secp256r1
- secp384r1
- secp521r1

（注） Cisco ISE は、OpenJDK 1.8 の現在の導入における制限により、楕円曲線に関する SHA256withECDSA 署名アルゴリズムを含む中間証明書をサポートしていません。

次の表に、サポートされている暗号スイートが表示されています。

暗号スイート	**Cisco ISE** が **EAP** サーバーとして設定されている場合 **Cisco ISE** が **RADIUS DTLS** サーバーとして設定されている場合	**Cisco ISE** が、**HTTPS** またはセキュア **LDAP** サーバーから **CRL** をダウンロードする場合 **Cisco ISE** がセキュアな **LDAP** クライアントとして設定されている場合 **Cisco ISE** が **CoA** の **RADIUS DTLS** クライアントとして設定されている場合

TLS 1.0 のサポート	TLS 1.0 が許可されている場合 （DTLS サーバーは DTLS 1.2 のみをサポート） Cisco ISE 2.3 以上では、[TLS 1.0 を許可（Allow TLS 1.0）] オプションがデフォルトで無効になっています。このオプションが無効の場合、TLS 1.0 では、TLS ベースの EAP 認証方式（EAP-TLS、EAP-FAST/TLS）および 802.1 X サプリカントがサポートされません。TLS ベースの EAP 認証方式を TLS 1.0 で使用するには、[セキュリティ設定（Security Settings）] ウィンドウの [TLS 1.0 を許可（Allow TLS 1.0）] チェックボックスをオンにします。このウィンドウを表示するには、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [セキュリティ設定（Security Settings）] を選択します。	TLS 1.0 が許可されている場合 （DTLS クライアントは DTLS 1.2 のみをサポート）
TLS 1.1 のサポート	TLS 1.1 が許可されている場合 Cisco ISE 2.3 以上では、[TLS 1.1 を許可（Allow TLS 1.0）] オプションがデフォルトで無効になっています。このオプションが無効の場合、TLS 1.1 では、TLS ベースの EAP 認証方式（EAP-TLS、EAP-FAST/TLS）および 802.1 X サプリカントがサポートされません。TLS ベースの EAP 認証方式を TLS 1.1 で使用するには、[セキュリティ設定（Security Settings）] ウィンドウ（[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [セキュリティ設定（Security Settings）]）で [TLS 1.1を許可（Allow TLS 1.1）] チェック ボックスをオンにします。	TLS 1.1 が許可されている場合

ECC DSA 暗号方式		
ECDHE-ECDSA-AES256-GCM-SHA384	対応	対応
ECDHE-ECDSA-AES128-GCM-SHA256	対応	対応
ECDHE-ECDSA-AES256-SHA384	対応	対応
ECDHE-ECDSA-AES128-SHA256	対応	対応
ECDHE-ECDSA-AES256-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
ECDHE-ECDSA-AES128-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
ECC RSA 暗号方式		
ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES256-SHA384	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES128-SHA256	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES256-SHA	ECDHE-RSA/SHA-1 が許可されている場合	ECDHE-RSA/SHA-1 が許可されている場合
ECDHE-RSA-AES128-SHA	ECDHE-RSA/SHA-1 が許可されている場合	ECDHE-RSA/SHA-1 が許可されている場合
DHE RSA 暗号方式		
DHE-RSA-AES256-SHA256	×	対応
DHE-RSA-AES128-SHA256	×	対応
DHE-RSA-AES256-SHA	×	SHA-1 が許可されている場合
DHE-RSA-AES128-SHA	×	SHA-1 が許可されている場合
RSA 暗号方式		
AES256-SHA256	対応	対応

AES128-SHA256	対応	対応
AES256-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
AES128-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
3DES 暗号方式		
DES-CBC3-SHA	3DES/SHA-1 が許可されている場合	3DES/DSS および SHA-1 が有効になっている場合
DSS 暗号方式		
DHE-DSS-AES256-SHA	×	3DES/DSS および SHA-1 が有効になっている場合
DHE-DSS-AES128-SHA	×	3DES/DSS および SHA-1 が有効になっている場合
EDH-DSS-DES-CBC3-SHA	×	3DES/DSS および SHA-1 が有効になっている場合
弱い RC4 暗号方式		
RC4-SHA	[許可されているプロトコル（Allowed Protocols）] ページで [脆弱な暗号を許可（Allow weak ciphers）] オプションが有効になっていて、SHA-1 が許可されている場合	×
RC4-MD5	[許可されているプロトコル（Allowed Protocols）] ページで [脆弱な暗号を許可（Allow weak ciphers）] オプションが有効になっている場合	×
EAP-FAST 匿名プロビジョニングのみの場合： ADH-AES-128-SHA	対応	×
ピア証明書の制限		

KeyUsage の検証	クライアント証明書では、以下の暗号に対し、KeyUsage=Key Agreement および ExtendedKeyUsage=Client Authentication が必要です。 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	
ExtendedKeyUsage の検証	クライアント証明書では、以下の暗号に対し、KeyUsage=Key Encipherment および ExtendedKeyUsage=Client Authentication が必要です。 • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • RC4-SHA • RC4-MD5	サーバー証明書では ExtendedKeyUsage=Server Authentication が必要です

Cisco ISE リリース 2.7 の新機能

スポンサー承認後の自己登録ゲストの自動ログイン

スポンサーの承認後に、自己登録ゲストの自動ログインを有効にすることができるようになりました。

ビジネス成果：ゲストユーザーは、スポンサーがゲストアクセス要求を承認すると自動的にログインします。これにより、プロセスが簡素化され、カスタマーエクスペリエンスが向上します。

Cisco Support Diagnostics Connector

Cisco Support Diagnostics Connector は、Cisco Technical Assistance Center（TAC）とシスコのサポートエンジニアがプライマリ管理ノードから展開の情報を取得するのに役立ちます。

ビジネス成果：TACは、展開内の特定のノードのサポート情報を取得するのにコネクタを使用します。このデータにより、トラブルシューティングがより迅速になり、向上します。

CLI の show logging の機能強化

コマンドラインインターフェイス（CLI）で show logging コマンドを実行すると、そのコンテンツは Unix の less 環境に表示されます。「H」を入力すると、サポートされている less コマンドが表示されます。

ビジネス成果：大規模なファイルの内容を表示するには、less のほうが役に立ちます。これにより、ログファイルを調査する時間が短縮されます。

EAP TEAP のサポート

Cisco ISE 2.7 は Tunnel Extensible Authentication Protocol（TEAP）をサポートしています。トンネル内では、EAP ピアと EAP サーバー間の認証関連データを伝送するために、Type-Length-Value（TLV）オブジェクトが使用されます。内部メソッドとして、EAP-MS-CHAPv2 または EAP-TLS を使用できます。EAP チェーニングは TEAP でサポートされています。EAP チェーンを使用すると、Cisco ISE は、同じ TEAP トンネル内でユーザーとマシンの両方の認証の内部方式を実行できます。これにより、Cisco ISE は認証の結果を関連付け、EAPChainingResult 属性を使用して適切な許可ポリシーを適用することができます。

ビジネス成果：TEAP は、トンネルを確立し、以降の通信を暗号化するために Transport Layer Security（TLS）プロトコルを使用して、サーバーとピア間のセキュアな通信を可能にするトンネルベースの EAP メソッドです。

エンドポイントの所有権の拡張

エンドポイント所有権情報が、Light Session Directory（LSD）を使用してすべてのポリシーサービスノード（PSN）に保存されるようになりました。

ビジネス成果：これにより、エンドポイント所有権のフラッピングが回避されます。

フィードサービスの更新

プロファイラ条件をカスタマイズしていて、プロファイラフィードでこれらの条件を置き換える必要がない場合は、ポリシーの更新をダウンロードせずに OUI の更新を手動でダウンロードできます。

ビジネス成果：プロファイラの精度が向上し、オーバーヘッドが低下しました。

グレースアクセス

社内ネットワークへのスポンサーの承認を待機している自己登録ゲストに、5 ～ 30 分のインターネットアクセスを付与できます。

ビジネス成果：ゲストユーザーが承認待ちの間にインターネットにアクセスできます。

ゲストパスワードのリカバリ

自己登録ゲストのゲストポータルで [パスワードのリセット（Reset Password）] オプションを有効にすることができるようになりました。有効なゲストアカウントを持つ自己登録ゲストが、パスワードを忘れた場合にこのオプションを使用できます。このオプションをクリックすると、セルフ登録ページが起動します。電話番号または電子メールアドレス（登録先）を入力し、新しいパスワードを入力できます。

ビジネス成果：カスタマーエクスペリエンスを向上させ、カスタマーサポートチームへのコールを削減します。

インタラクティブヘルプ

インタラクティブヘルプを使用すると、タスクを簡単に実行するためのヒントと段階的なガイダンスが表示されます。

ビジネス成果：これにより、エンドユーザーが作業フローを容易に理解し、タスクを簡単に実行できるようになります。

ゲストユーザー識別子としての電話番号

電子メールアドレスまたはユーザー名に加えて、ゲストユーザーが自分の電話番号をゲストアクセスのユーザー ID として使用できるようになりました。

ビジネス成果：ゲストユーザーが、自分の携帯電話番号をユーザー ID として使用できるようになりました。これにより、ユーザーが自分のユーザー ID を覚えやすくなります。

プロファイラフォワーダ永続キュー

プロファイラフォワーダ永続キューは、イベントがさらなる処理のためにプロファイラモジュールに送信される前に、それらの着信イベントを保存します。

ビジネス成果：これにより、イベントの急激なバーストによるイベントの損失が低減されます。このキューはISEメッセージングサービスを使用し、デフォルトで有効になっています。すべての Cisco ISE ノード間でポート 8671 が開かれている必要があります。

ロールベースのアクセスポリシー

ISE 管理者ポータルでは、[管理（Administration）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] の下にある [ポリシー（Policy）] メニューのオプションは [RBAC ポリシー（RBAC Policy）] という名前に変更されました。[RBAC ポリシー（RBAC Policy）] ウィンドウは、管理者グループのポリシーを追加および設定するために使用されます。

セキュアな SMTP

ゲスト電子メール通知が、セキュアなSMTPサーバーを介して送信できるようになりました。

ビジネス成果：ネットワーク内のゲスト電子メールのセキュリティが向上しました。

セキュアなロック解除クライアント

セキュアなロック解除クライアントメカニズムが、Cisco ISE CLIで一定期間にわたってルートシェルへのアクセスを提供するために使用されます。

ビジネス成果：セキュアなロック解除クライアント機能は、同意トークンツールを使用して実装されており、信頼できる方法でシスコ製品の特権アクセスを安全に付与します。

TrustSec の機能拡張

HTTPS REST API が既存の RADIUS プロトコルを置換して、必要なすべての TrustSec 情報をネットワークデバイスに提供します。

ビジネス成果：これにより、既存のRADIUSプロトコルと比較して、短時間で大規模な設定をダウンロードする効率と能力が向上します。

既知の制限事項と回避策

アップグレード後の LDAP サーバーの再設定

制限事項

プライマリホスト名または IP が更新されないため、認証が失敗します。これは、Cisco ISE 展開のアップグレード中に、展開 ID がリセットされる傾向があるためです。

条件

[接続（Connection）] ウィンドウ（**[管理（Administration）]** > **[ID管理（Identity Management）]** > **[外部IDソース（External Identity Sources）]** > **[LDAP]** > **[追加（Add）]**）で [各ISEノードのサーバーの指定（Specify server for each ISE node）] オプションを有効にするか、既存のサーバーを選択し、PSN を使用して Cisco ISE 展開をアップグレードすると、展開 ID がリセットされる傾向があります。

回避策

各ノードのLDAPサーバー設定を再設定します。詳細については、Cisco Identity Services Engine 管理者ガイド、リリース 2.4 [英語] の「Administrative Access to Cisco ISE Using an External Identity Store」の章の「LDAP Identity Source Settings」の項を参照してください。

pxGrid 証明書の問題

pxGrid 証明書に「Netscape Cert Type」を使用している場合、Cisco ISE はパッチ 2 の適用後にその証明書を拒否することがあります。その証明書の古いバージョンではSSLサーバーが指定

されていましたが、クライアント証明書が必要なためSSLサーバーは失敗します。別の証明書を使用するか、または既存の証明書に「SSLクライアント」を追加します。

認証の Radius ログ

認証イベントの詳細は、[Radius認証（Radius Authentications）] ウィンドウの [詳細（Details）] フィールドで確認できます。認証イベントの詳細を使用できるのは7日間のみで、その後は認証イベントのデータを表示することはできません。すべての認証ログデータは、パージがトリガーされると削除されます。

デフォルトの自己署名証明書を使用する場合の Radius EAP 認証のパフォーマンス

Cisco ISE 2.7 では、セキュリティを強化するために、デフォルトの自己署名証明書のキーサイズが 4096 に拡大されています。デフォルトの自己署名証明書が EAP 認証に使用されている場合、Radius EAP 認証のパフォーマンスが影響を受ける可能性があります。

一部の TLS 暗号を無効にできない

Cisco ISE では、次の暗号を無効にすることはできません。

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

次に、これらの暗号方式を使用できる Cisco ISE のシナリオを示します。

- EAP サーバーまたは ERS サーバーとしての Cisco ISE
- Cisco ISE が HTTPS またはセキュアな LDAP サーバーから証明書失効リストをダウンロードする
- セキュアな TCP syslog または LDAP のクライアントとしての Cisco ISE

これらの暗号方式を使用できる Cisco ISE コンポーネントには、管理者 UI、すべてのポータル、MDM クライアント、pxGrid、および PassiveID Agent エージェントなどがあります。

セキュリティ グループ アクセス コントロール リスト

セキュリティグループ ACL（SGACL）を作成しようとすると、次のエラーメッセージが表示されます。

```
Failed to create policy, CFS provision failed.
```

これは、Cisco ISE の複数のマトリックスで出力マトリックスセルフローの作成と更新がサポートされていないためです。次の外部 RESTful サービス（ERS）要求も、複数マトリックスモードではサポートされません。

/config/egressmatrixcell/*

/config/sgt/*

/config/sgacl/*

したがって、[TrustSec マトリックスの設定（TrustSec Matrix Settings）]（**[作業（Work）]** > **[TrustSec]** > **[設定（Settings）]** > **[TrustSec マトリックスの設定（TrustSec Matrix Settings）]** ウィンドウの [複数の SGACL を許可（Allow Multiple SGACL）] チェックボックスをオフにする必要があります。これにより、SGACL を作成することができ、エラー メッセージは表示されなくなります。

有効なユーザーエージェントヘッダー

Cisco ISE では、Cisco ISE リリース 2.7 以降、Cisco ISE スポンサーポータルなどの Cisco ISE エンドユーザー向けポータルで正常な応答またはリダイレクト応答を受信するため、Web 要求で送信される有効なユーザーエージェントヘッダーが必要です。

応答ステータス行

Cisco ISE リリース 2.7 以降、Cisco ISE Web サービスおよびポータルは、HTTP バージョンとステータスコードのみを含む応答ステータス行を返しますが、対応する理由フレーズは返しません。

[TrustSec AAAサーバー（Trustsec AAA Server）] リストのサーバー IP の更新

Cisco ISE インスタンスの IP が CLI 経由で変更されると、Cisco ISE はサービスを再起動します。サービスが起動したら、TrustSec AAA サーバーの IP を変更する必要があります。**[ワークセンター（Workcenters）]** > **[TrustSec]** > **[コンポーネント（Components）]** > **[Trustsecサーバー（Trustsec Servers）]** > **[TrustSec AAAサーバー（Trustsec AAA Servers）]** を選択します。

アップグレード情報

リリース 2.7 へのアップグレード

次の Cisco ISE リリースからリリース 2.7 に直接アップグレードできます。

- 2.2

- 2.3
- 2.4
- 2.6

Cisco ISE リリース 2.2 より前のバージョンの場合は、まず上記のリリースのいずれかにアップグレードしてから、リリース 2.7 にアップグレードする必要があります。

（注） アップグレードの開始前に、既存のバージョンで最新のパッチにアップグレードすることをお勧めします。

Cisco ISE リリース 2.7 には、Cisco ISE パッチリリース（2.2 パッチ 15、2.3 パッチ 7、2.4 パッチ 10、および 2.6 パッチ 2）とのパリティがあります。

アップグレードパッケージ

アップグレードパッケージおよびサポートされているプラットフォームに関する情報は、Cisco ISE Software Download から入手できます。

ライセンスの変更

デバイス管理ライセンス

デバイス管理ライセンスには、クラスタとノードの2つのタイプがあります。クラスタライセンスでは、Cisco ISE クラスタ内のすべてのポリシーサービスノードでデバイス管理を使用できます。ノードライセンスでは、1つのポリシーサービス ノードでデバイス管理を使用できます。ハイ アベイラビリティ スタンドアロン展開では、ノードライセンスによって、ハイアベイラビリティペアの 1 つのノードでデバイス管理を使用することが許可されます。

デバイス管理ライセンスキーは、プライマリおよびセカンダリポリシー管理ノードに対して登録されます。クラスタ内のすべてのポリシーサービスノードは、ライセンス数に達するまで必要に応じてデバイス管理ライセンスを消費します。

クラスタライセンスは Cisco ISE 2.0 のデバイス管理のリリースで導入され、Cisco ISE 2.0 以降のリリースで適用されています。ノードライセンスは後でリリースされ、リリース 2.0 ～ 2.3 で部分的にのみ適用されています。Cisco ISE 2.4 以降では、ノードライセンスはノード単位で完全に適用されています。

クラスタライセンスは廃止されました。現時点ではノードライセンスのみを販売しています。

ただし、有効なクラスタライセンスでこのリリースにアップグレードする場合は、アップグレード時に既存のライセンスを引き続き使用できます。

評価ライセンスを使用すると、1 つのポリシーサービスノードでデバイスを管理できます。

仮想マシンノードのライセンス

Cisco ISE は仮想マシン（VM）としても販売されています。このリリースでは、展開に VM ノードの適切な VM ライセンスをインストールすることをお勧めします。VM ノードの数と CPU やメモリなどの各 VM ノードのリソースに基づいて、VM ライセンスをインストールします。そうでない場合、VM ライセンスキーを調達してインストールする警告と通知が表示されます。ただし、インストールプロセスは中断されません。Cisco ISE リリース 2.4 以降、GUI から VM ライセンスを管理できます。

VM ライセンスは、小、中、大の 3 つのカテゴリで提供されます。たとえば、8 コアと 64 GB RAM を備えた 3595 相当の VM ノードを使用している場合、VM で同じ機能をレプリケートするには、中カテゴリの VM ライセンスが必要になります。展開の要件に応じて、VM とそのリソースの数に基づいて、複数の VM ライセンスをインストールできます。

VM ライセンスはインフラストラクチャ ライセンスです。このため、展開で使用可能なエンドポイントライセンスに関係なく、VM ライセンスをインストールできます。展開に Evaluation、Base、Plus、Apex ライセンスのどれもインストールされていない場合でも、VM ライセンスをインストールできます。ただし、Base、Plus、または Apex ライセンスによって有効になる機能を使用するには、適切なライセンスをインストールする必要があります。

VM ライセンスは永久ライセンスです。VM ライセンスの変更は、Cisco ISE GUI にログインするたびに表示され、通知ポップアップウィンドウで [今後、このメッセージを表示しない（Do not show this message again）] チェックボックスをオンにすると表示されなくなります。

以前に ISE VM ライセンスを購入していない場合、『Cisco Identity Services Engine Ordering Guide』を参照して購入する適切な VM ライセンスを選択します。

（注） PAK を使用せずに ISE VM ライセンスを購入した場合は、licensing@cisco.com に電子メールを送信して VM PAK を要求できます。電子メールに ISE VM の購入を示す SO 番号とシスコ ID を記載してください。購入した各 ISE VM ごとに 1 つの中規模 VM ライセンスキーを提供します。

使用中の Cisco ISE バージョンと VM の互換性に関する詳細については、該当するリリースの『Cisco Identity Services Engine Installation Guide』の「Hardware and Virtual Appliance Requirements」の章を参照してください。

ライセンスの詳細については、『Cisco Identity Services Engine Administrator Guide』の「Cisco ISE Licenses」の章を参照してください。

アップグレード手順の前提条件

- 設定されたデータを必要な Cisco ISE バージョンにアップグレードできるかどうかを確認するには、アップグレードの前にアップグレード準備ツール（URT）を実行します。ほとんどのアップグレードの失敗は、データのアップグレードの問題が原因で発生します。URT により実際のアップグレード前にデータを検証し、問題があれば報告します。URT は Cisco ISE Download Software Center からダウンロードできます。

- アップグレードの開始前に関連するすべてのパッチをインストールすることをお勧めします。

詳細については、『Cisco Identity Services Engine Upgrade Guide』を参照してください。

テレメトリ

インストール後の管理者ポータルへの初回ログイン時には、Cisco ISE テレメトリバナーが表示されます。この機能を使用して、Cisco ISE は、ユーザーの展開、ネットワーク アクセス デバイス、プロファイラ、およびユーザーが使用している他のサービスに関する非機密情報を安全に収集します。このデータは、今後のリリースでサービスを向上させ、より多くの機能を提供するために使用されます。デフォルトでは、テレメトリは有効になっています。アカウント情報を無効または変更するには、[管理（Administration）]>[設定（Settings）]>[ネットワーク設定診断（Network Settings Diagnostics）]>[テレメトリ（Telemetry）] を選択します。アカウントは、各展開に固有です。各管理者ユーザーが個別に提供する必要はありません。

テレメトリは、Cisco ISE のステータスと機能に関する貴重な情報を提供します。シスコは、Cisco ISE を導入した IT チームのアプライアンス ライフサイクル管理を改善するためにテレメトリを使用します。このデータを収集することで、製品チームは顧客により優れたサービスを提供できるようになります。このデータと関連する分析情報により、シスコは潜在的な問題をプロアクティブに特定し、サービスとサポートを改善し、ディスカッションを促進して新規および既存の機能からより多くの価値を収集し、IT チームによるライセンス権限のインベントリレポートと今後の更新を支援します。

Cisco ISE でテレメトリ機能が無効になり、テレメトリデータの共有が停止するまでに最大 24 時間かかる場合があります。 パッチ 1 以降では、テレメトリはすぐに無効になります。

収集されるデータのタイプには、製品使用状況テレメトリや Cisco Support Diagnostics などがあります。

Cisco Support Diagnostics

Cisco Support Diagnostics Connector は、Cisco Technical Assistance Center（TAC）とシスコのサポートエンジニアがプライマリ管理ノードから展開の情報を取得するのに役立つ新機能です。デフォルトでは、この機能は無効になっています。この機能を有効にする手順については、『Cisco Identity Services Engine Administrator Guide』を参照してください。

Cisco ISE ライブアップデートポータル

Cisco ISE ライブアップデートポータルは、**サプリカント プロビジョニング** ウィザード、AV/AS サポート（コンプライアンスモジュール）、およびクライアントプロビジョニングとポスチャポリシーサービスをサポートするエージェントインストーラ パッケージを自動的にダウンロードするのに役立ちます。このライブアップデートポータルは、Cisco ISE を使用して Cisco.com から該当するデバイスに最新のクライアントプロビジョニングおよびポスチャソフトウェアを直接取得するように、初期展開時に Cisco ISE で設定します。

デフォルトのアップデートポータルURLにアクセスできず、ネットワークにプロキシサーバーが必要な場合は、プロキシを設定します。ライブアップデートポータルにアクセスする前に、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロキシ（Proxy）] の順に選択します。プロキシ設定でプロファイラ、ポスチャ、およびクライアントプロビジョニング フィードへのアクセスが許可されている場合、Cisco ISE は MDM 通信のプロキシサービスをバイパスできないため、モバイルデバイス管理（MDM）サーバーへのアクセスがブロックされます。これを解決するには、MDM サーバーとの通信を許可するようにプロキシサービスを設定できます。プロキシ設定の詳細については、『Cisco Identity Services Engine Administrator Guide』の「Specify Proxy Settings in Cisco ISE」の項を参照してください。

クライアント プロビジョニングとポスチャのライブアップデートポータル

次の場所からクライアント プロビジョニング リソースをダウンロードできます。

[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアアップデート（Software Updates）] > [クライアント プロビジョニング（Client Provisioning）]。

次のソフトウェア要素は、次の URL から入手できます。

- Windows および Mac OS X ネイティブサプリカント向けのサプリカント プロビジョニング ウィザード
- 最新の Cisco ISE の永続的なエージェントおよび一時的なエージェントの Windows バージョン
- 最新の Cisco ISE の永続的なエージェントの Mac OS X バージョン
- ActiveX および Java アプレット インストーラ ヘルパー
- AV/AS コンプライアンス モジュール ファイル

クライアント プロビジョニング アップデート ポータルで利用可能なソフトウェアパッケージを Cisco ISE に自動的にダウンロードする方法については、『Cisco Identity Services Engine Administrator Guide』の「Configure Client Provisioning」の章の「Download Client Provisioning Resources Automatically」の項を参照してください。

次の場所からポスチャ更新をダウンロードできます。

[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアアップデート（Software Updates）] > [ポスチャ更新（Posture Updates）]

次のソフトウェア要素は、次の URL から入手できます。

- シスコで事前定義されたチェックとルール
- Windows および Mac OS X の AV/AS サポート表
- Cisco ISE オペレーティングシステムのサポート

このポータルで利用可能なソフトウェアパッケージを Cisco ISE に自動的にダウンロードする方法については、『Cisco Identity Services Engine Administrator Guide』の「Download Posture Updates Automatically」の項を参照してください。

自動ダウンロード機能を有効にしていない場合、更新をオフラインでダウンロードすることができます。

Cisco ISE オフライン更新

このオフライン更新オプションを使用すると、Cisco ISE を使用してデバイスから Cisco.com にインターネット経由で直接アクセスできない場合、またはセキュリティポリシーによって許可されていない場合に、クライアントプロビジョニングおよびポスチャ更新をダウンロードできます。

オフラインのクライアント プロビジョニング リソースをアップロードするには、次の手順を実行します。

手順

ステップ 1 https://software.cisco.com/download/home/283801620/type/283802505/release/2.7.0に進みます。

ステップ 2 ログインクレデンシャルを入力します。

ステップ 3 Cisco Identity Services Engine のダウンロードウィンドウに移動し、リリースを選択します。

次のオフライン インストール パッケージをダウンロードできます。

- **win_spw-**<*version*>**-isebundle.zip**：Windows 向けのオフライン SPW インストールパッケージ
- **mac-spw-**<*version*>**.zip**：Mac OS X 向けのオフライン SPW インストールパッケージ
- **compliancemodule-**<*version*>**-isebundle.zip**：オフライン コンプライアンス モジュール インストール パッケージ
- **macagent-**<*version*>**-isebundle.zip**：オフライン Mac エージェント インストール パッケージ
- **webagent-**<*version*>**-isebundle.zip**：オフライン Web エージェント インストール パッケージ

ステップ 4 [ダウンロード（Download）] または [カートに追加（Add to Cart）] のいずれかをクリックします。

ダウンロードしたインストールパッケージを Cisco ISE に追加する方法については、『Cisco Identity Services EngineAdministrator Guide』の「Add ClientProvisioning Resources from a Local Machine」のセクションを参照してください。

ポスチャ更新を使用して、ローカルシステムのアーカイブから Windows および Mac オペレーティングシステムのチェック、オペレーティングシステム情報、ウイルス対策とスパイウェア対策サポート表を更新できます。

オフライン更新の場合は、アーカイブファイルのバージョンが設定ファイルのバージョンと一致していることを確認します。Cisco ISE を設定した後にオフラインでポスチャ更新を使用し、ポスチャポリシーサービスの動的更新を有効にします。

オフラインのポスチャ更新をダウンロードするには、次のようにします。

手順

ステップ 1 https://www.cisco.com/web/secure/spa/posture-offline.htmlに進みます。

ステップ 2 ローカルシステムに **posture-offline.zip** ファイルを保存します。このファイルを使用すると、WindowsおよびMacオペレーティングシステムのオペレーティングシステム情報、チェック、ルール、ウイルス対策とスパイウェア対策サポート表が更新されます。

ステップ 3 Cisco ISE 管理者ユーザーインターフェイスを起動し、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] を選択します。

ステップ 4 矢印をクリックすると、ポスチャの設定が表示されます。

ステップ 5 [更新（Updates）] をクリックします。
[ポスチャ更新（Posture Updates）] ウィンドウが表示されます。

ステップ 6 [オフライン（Offline）] オプションをクリックします。

ステップ 7 [参照（Browse）] をクリックし、システムのローカルフォルダからアーカイブファイル（posture-offline.zip）を検索します。

（注） [更新するファイル（File to Update）] フィールドは必須フィールドです。適切なファイルを含むアーカイブファイル（.zip）を 1 つだけ選択できます。.zip、.tar、.gz 以外のアーカイブファイルはサポートされていません。

ステップ 8 [今すぐ更新（Update Now）] をクリックします。

設定要件

- 関連する Cisco ISE ライセンス料金を支払う必要があります。
- 最新のパッチをインストールする必要があります。
- Cisco ISE ソフトウェア機能がアクティブになっている必要があります。

Cisco ISE を設定するには、次のリソースを参照してください。

- Getting started with Cisco ISE
- YouTube の Cisco ISE チャンネルのビデオ
- *Cisco ISE Design and Integration Guides*
- *Cisco Identity Services Engine Administrator Guide*

モニターリングおよびトラブルシューティング

システムのモニタリングおよびトラブルシューティングに関する詳細については、『*Cisco Identity Services Engine Administrator Guide*』の「Monitoring and Troubleshooting Cisco ISE」のセクションを参照してください。

発注情報

Cisco ISE の詳細な発注およびライセンス情報については、*Cisco IdentityServices Engine* 注文ガイド [英語] を参照してください。

Cisco ISE と Cisco Digital Network Architecture Center との統合

Cisco ISE は Cisco DNA Center と統合できます。Cisco DNA Center と連携するように Cisco ISE を設定する方法については、*Cisco DNA Center* のドキュメントを参照してください。

Cisco ISE と Cisco DNA Center との互換性については、「Cisco SD-Access Compatibility Matrix」を参照してください。

新しいパッチのインストール

Cisco ISE にパッチを適用するために必要なパッチファイルを取得するには、Cisco ダウンロードソフトウェア サイト（https://software.cisco.com/download/home）にログインし（Cisco.com ログイン情報の入力が必要になる場合があります）、[セキュリティ（Security）] > [アクセス制御およびポリシー（Access Control and Policy）] > [Cisco Identity Services Engine] > [Cisco Identity Services Engine ソフトウェア（Cisco Identity Services Engine Software）] に移動し、ローカルマシンにパッチファイルのコピーを保存します。

システムへのパッチの適用方法については、『*Cisco Identity Services Engine Administrator Guide*』の「Install a Software Patch」セクションを参照してください。

CLI を使用したパッチのインストール方法については、『*Cisco Identity Services Engine CLI Reference Guide*』の「Patch Install」セクションを参照してください。

（注） Cisco ISE リリース 2.7 パッチ 4 以降のリリースでは、Smart Software Manager（SSM）オンプレミス接続ライセンス方式がサポートされています。この機能を有効にした後、リリース 2.7 パッチ 3 以前にロールバックする必要がある場合は、パッチをアンインストールする前にこの機能を無効にする必要があります。

警告

「不具合」セクションには、バグ ID とそのバグの簡単な説明が含まれています。特定の不具合の症状、条件、および回避策に関する詳細については、シスコのバグ検索ツール（BST）を使用してください。バグ ID は英数字順にソートされます。

（注） 「未解決の不具合」セクションには、現在のリリースに適用され、Cisco ISE 2.7 よりも前のリリースにも適用されている可能性のある未解決の不具合が記載されています。これまでのリリースで未解決で、まだ解決されていない不具合は、解決されるまで、今後のすべてのリリースに適用されます。

BST は Bug Toolkit の後継オンラインツールであり、ネットワークリスク管理およびデバイスのトラブルシューティングにおいて効率性を向上させるように設計されています。製品、リリース、またはキーワードに基づいてソフトウェアのバグを検索し、バグの詳細、製品、バージョンなどの主要データを集約することができます。ツールの詳細については、http://www.cisco.com/web/applicat/cbsshelp/help.html のヘルプ ページを参照してください。

Cisco ISE リリース 2.7.0.356 の新機能：累積パッチ 8

Cisco Secure Client のサポート

Cisco ISE は、Cisco ISE ポスチャ要件の Cisco Secure Client で統合モジュールを使用します。

Cisco ISE をエージェントと統合すると、Cisco ISE は次のように機能します。

- Cisco Secure Client を展開するためのステージングサーバーとして機能
- Cisco ISE ポスチャ要件のエージェント ポスチャ コンポーネントとやり取りする
- エージェントプロファイル、カスタマイズおよび言語パッケージ、および OPSWAT のライブラリ更新の展開をサポートする

Cisco ISE リリース 2.7.0.356 の解決済みの不具合：累積パッチ 8

次の表に、リリース 2.7 累積パッチ 8 の解決済みの不具合を示します。

パッチ 8 は古いバージョンの SPW で機能しない可能性があります。MAC ユーザーは SPW を MACOSXSPWizard 2.2.1.43 以降にアップグレードする必要があります。また、Windows ユーザーはその SPW を WinSPWizard 2.2.1.53 以降にアップグレードする必要があります。

パッチ 8 を Cisco ISE 2.7 パッチ 7 にインストールする前に、ホットパッチをアンインストールしてパッチ 7 の CSCwa47133 を修正します。

ID	見出し
CSCwc74531	ise hourly cron は、95% のメモリ使用量ではなく、キャッシュされたバッファをクリーンアップする必要がある
CSCwa80359	CIAM：sqlite 3.7.17
CSCwa80547	CIAM：unixodbc 2.3.0
CSCwb07442	SystemTest：PAN のフェールオーバー後に Pxgrid 接続が起動しない
CSCwa80679	CIAM：net-snmp 5.7.2
CSCwd35608	前回ポートバウンス CoA が成功した後も、ISE が reath CoA で古い監査セッション ID を送信している
CSCwa96229	ISE で、ユーザーが現在のパスワードを検証せずに管理者パスワードを変更可能
CSCvv54351	Radius を使用したデバイス管理が基本ライセンスを使用しない
CSCwb29140	nss rpm が更新された最新のパッチに移行した後、スレッドが枯渇する（3.0p5 と 2.7p7、3.1P1 のみ）
CSCwa84447	ISE 2.7 パッチ 3 で ISE 2.2 のバックアップを復元すると、ヘルスチェックの [開始（start）] ボタンが表示されない。
CSCwa35293	ISE 2.7：認証成功設定が成功/成功 URL を示す
CSCwb33727	ISE 3.1：属性の特殊文字がサポートされていない
CSCwb24002	ISE ERS SDK の authenticationSettings が API 呼び出しを介して無効になっていない
CSCwb55232	ERS API を使用してネストされたエンドポイントグループを作成する
CSCvv87286	ISE 2.7P2 ～ 3.0 で内部 CA とキーをインポートできない
CSCwc93253	ISE：フィルタが 1 つのネットワークデバイスのみに一致する場合にのみプロンプトを表示する、ネットワークデバイスのキャプチャ
CSCwa55996	条件スタジオに新しいオブジェクトが存在しない
CSCwb14106	CIAM：cyrus-sasl 2.1.27
CSCwb19256	Pingnode 呼び出しにより、CRL 検証中にアプリサーバーがクラッシュする（OOM は除く）
CSCvx58736	3.1：Maxscale：/opt/CSCOcpm/prrt/diag/bin/diagRunner によって生成されたコアが開始される

ID	見出し
CSCwc12303	インスタンスが使用する PGA メモリが MNT ノードで PGA_AGGREGATE_LIMIT を超えている
CSCwa97123	2 つ以上の NTP サーバーが設定されている NTP 同期エラーアラーム。
CSCwa40040	セッションディレクトリの書き込みに失敗する。SQLException：ISE3.0P4 で文字列データの右側が切り捨てられる
CSCvs96530	Cisco Identity Services Engine のフォーミュラ インジェクションの脆弱性
CSCwa80710	CIAM：jszip 2.5.0
CSCwa06912	認証ポリシーに日時条件がある Tacacs+ 要求で高遅延が発生する
CSCwb75954	Cisco Identity Services Engine クロスサイト リクエスト フォージェリの脆弱性
CSCwc30019	CIAM：openssl 1.0.2n
CSCwb07504	ユーザー ID グループに基づいた内部ユーザーの並べ替えが、[IDの管理（Identity Management）] > [ID] で機能しない
CSCwa80520	CIAM：libpng 1.6.20
CSCwc69492	ISE 3.1：メタスペースを使い果たすと ISE ノードでクラッシュが発生する
CSCwb75959	Cisco Identity Services Engine のストアド クロスサイト スクリプティングの脆弱性
CSCwb61614	ゲストユーザー（AD または内部）が特定のノードで自分のデバイスを削除または追加できない
CSCwc72251	アカウンティング終了のために変更された pxgrid パブリッシング
CSCvy32277	ポート 8084 で TLSv1.1 が有効になっている
CSCvz85074	CSCvu35802 の修正により、EAP チェーンのアイデンティティとして証明書属性をもつ AD グループの取得が中断される
CSCwb27857	ISE 3.0 P5：分散型展開で RSA 2FA を使用して MnT ノードの GUI にログインできない
CSCwd03009	2.7 p7 の platform.properties でハードウェアアプライアンスに基づいて制御する RMQForwarder スレッド
CSCwb52396	ISE PRA フェールオーバー
CSCwa95892	間違った期間を示す ui_time_left 変数

ID	見出し
CSCwa76896	RADIUS 認証レポートの「Failure Reasons」列が重複する
CSCwc06638	3.0P6：パッチロールバックおよびパッチインストール後にシステムサマリーが更新されない
CSCwa17925	失敗したアップグレード前チェックを修正しても、[続行（Proceed）]ボタンが使用できない
CSCwa25731	レポートで過去 7 日間のフィルタが機能しない
CSCwd45843	GC アクティビティによるポリシー評価の認証ステップの遅延
CSCwb26965	ISE 3.1：REST API を介してネットワーク デバイス グループを作成中にエラーが発生する。
CSCwc57939	ISE が大規模な VM をサポート対象外として検出する
CSCwb86283	ISE 展開：不正な証明書の有効期限チェックの結果として、すべてのノードが OUT_OF_SYNC をスローする
CSCwa49859	属性値 dc-opaque がライブログの問題を引き起こす
CSCwa80484	CIAM：nss 3.44.0
CSCvz99311	Cisco Identity Services Engine ソフトウェアのリソース枯渇による脆弱性
CSCwb26227	CIAM：jackson-databind 2.9.8
CSCwb88360	アップグレードされたノードで一時的な MnT ペルソナを無効化すると、分割アップグレードで失敗する
CSCwb85456	CIAM：openssl を 1.0.2ze および 1.1.1o にアップグレード
CSCwb91392	サードパーティの CA 証明書が管理者に使用されている場合、ヘルスチェックとフルアップグレードの事前チェックがタイムアウトする
CSCwa80501	CIAM：perl 5.16.3
CSCwc65711	MAC - CSC 5.0554 ウェブ展開パッケージが [ISE] > [CP] > [リソース（resources）] [100MB] へのアップロードに失敗する
CSCwa18443	展開ノードのエンドポイントに 8 オクテット MAC が存在する場合、ポスチャの有効期限を処理する必要がある
CSCvv10712	Sec_txnlog_master テーブルは、レコード数が 200 万を超えたら切り捨てる必要がある
CSCvz63643	ISE 2.7：EndpointPersister スレッドが停止する

ID	見出し
CSCvx49736	containerd.io RPM パッケージ openssl 1.0.2r CIAM CVE-2021-23841 + その他
CSCwb09861	CIAM：glib 2.56.4
CSCvz43123	CIAM：jspdf 2.3.0
CSCwa90930	RMQ にハード Q キャップが必要
CSCvz24558	Spring Hibernate TPS アップグレード（Hibernate 5.5.2、Spring 5.3.8）
CSCwa75348	ODBC 動作のフェールオーバーの問題
CSCvz94133	「EDF_DB_LOG」が原因で設定のバックアップが失敗する
CSCwd31405	Session.PostureStatus のクエリ中に遅延が発生する
CSCwb27894	EAP-TLS を使用した EAP-TEAP が「CERTIFICATE.Issuer - Common Name」を持つ条件に一致しない
CSCvz91479	3.1 から 3.2.0.804 へのアップグレードの制約を変更中にスキーマのアップグレードが失敗した
CSCwb05532	「場所」と「デバイスタイプ」の場所が、[ネットワークデバイス（Network Devices）] > [追加（Add）] をクリックするたびに交換される
CSCwc23593	LSD によって CPU が高くなる
CSCwc93451	プロファイラは、デフォルトの RADIUS プローブからの転送について、否定的な RADIUS Syslog メッセージを無視する必要がある
CSCwb03231	テーブルが見つからないため、p5 または p6 をインストールするとアプリケーションサーバーが初期化中にスタックする
CSCwb41741	ISE：管理者グループの無効な文字エラー
CSCwb32466	ISE 3.1：説明が設定されていない場合、REST API を介して作成されたエンドポイント ID グループを削除できない
CSCwa59237	200 以上の内部証明書を持つ PAN ノードで、Deployment-RegistrationPoller がパフォーマンスの問題を引き起こす
CSCwc27765	SYS_EXPORT_SCHEMA_01 が原因で ISE 設定のバックアップが失敗する
CSCwb09045	正しくない cryptoLib 初期化が原因で ISE PSN ノードがクラッシュする
CSCwb67934	CIAM：openjdk - 複数のバージョン
CSCwc62413	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性

ID	見出し
CSCwa27766	ISE 3.0 P4 でのバックアップの復元後にコンテキストの可視性が壊れる
CSCwa77161	3.0P5 -> 3.0P3 で PLR が返される
CSCwb23028	パスワードの不正確な辞書の単語評価
CSCwb62192	ISE インデックスエンジンのバックアップが失敗するとスケジュール済みバックアップが失敗する
CSCwb29498	高稼働時の DB 使用率アラームのパーセンテージを設定可能にする必要がある。
CSCwc15013	有用性を追加し、ISE 3.0 の「プールが枯渇しているためリソースを取得できませんでした（Could not get a resource since the pool is exhausted）」エラーを修正する
CSCwb84779	親 ID グループ名を変更すると、認証リファレンスが壊れます
CSCwb03479	hotpatch.log をサポートバンドルに含める必要がある
CSCwb40349	ISE 3.X：外部 RADIUS トークン共有秘密の無効な文字。
CSCwb01843	DST/TZ が自動的に更新される
CSCwd24304	ISE 3.2 ERS POST /ers/config/networkdevicegroup が失敗する：破損した属性 othername/type/ndgtype
CSCvu41087	ライブログの ISE 3.0 RADIUS のドロップレポートで、エンドポイントの詳細に ISE の管理者ユーザー名が表示される
CSCvx94685	CIAM：rpm 4.11.3 CVE-2021-20271
CSCwa80553	CIAM：samba 4.8.3
CSCwa60903	ISE で、CRL の nextUpdate の日付に 6 時間追加される
CSCwa55866	シングル接続が有効になっていると、Tacacs応答が送信されないことがある
CSCwa80689	CIAM：c3p0 0.9.1.1
CSCwb02346	Cisco Identity Services Engine の機密情報の開示における脆弱性
CSCwb93156	TrustCertQuickView がすべての信頼できる証明書について同じ情報を提供する
CSCwb40131	Rest API を使用して外部パスワードタイプで内部ユーザーを有効にしているときに 400 Bad Request が発生する

ID	見出し
CSCwb32492	プライマリ PAN の管理証明書を変更した後、すべてのノードでアプリケーションサーバーが再起動する
CSCvz88327	PAN での CA の初期化中、ルート CA の再生成が「メッセージが定義されていません」というエラーで失敗する
CSCvv02086	ISE PIC ノードで TLS 1.0 および 1.1 を無効にする機能を追加
CSCwa80532	CIAM：jsoup 1.10.3
CSCvo79976	セキュリティ：コンソールに出力される RESTClientAlertHelper.java の、エンコードされたログイン情報のログが削除される

Cisco ISE リリース 2.7.0.356 の未解決の不具合：累積パッチ 8

Cisco ISE リリース 2.7 パッチ 8 には未解決の不具合はありません。

Cisco ISE リリース 2.7.0.356 の解決済みの不具合：累積パッチ 7

次の表に、リリース 2.7 累積パッチ 7 の解決済みの不具合を示します。

パッチ 7 は古いバージョンの SPW で機能しない可能性があります。MAC ユーザーは SPW を MACOSXSPWizard 2.2.1.43 以降にアップグレードする必要があります。また、Windows ユーザーはその SPW を WinSPWizard 2.2.1.53 以降にアップグレードする必要があります。

ID	見出し
CSCvv96532	DOC：この OCSP 応答の更新に対する不明な最大時間差
CSCvz37241	キューリンクエラー：WARN:{socket_closed_unexpectedly;'connection.start'}
CSCvz91603	ISE を 3.0 パッチ 3 にアップグレードすると、ODBC から属性を取得できない
CSCwa17718	専用の MNT を使用した PxGrid セッションディレクトリでセッションサービスを利用できない
CSCwa07580	ユーザー名に $ が含まれている場合、アイデンティティユーザーを作成できない
CSCvz18044	VN が作成者からリーダーに複製されない
CSCwa23393	ISE 2.7 p 4、5、6 で「デバイスのIPアドレスが重複しています（There is an overlapping IP Address in your device）」というエラーが報告される
CSCvz87476	サポートされていないメッセージコード 91104 および 91105 アラーム

ID	見出し
CSCvz90468	API フローを使用してユーザーを作成すると、外部パスワードストアを使用する内部ユーザーが無効になる。
CSCvz21417	CiscoSSL 1.0.2za を使用した ISE 3.0 以前のパッチのアップグレード
CSCvz84905	DOC：ISE バックアップで「負荷平均が高い（High Load Average）」アラームが発生することがある
CSCvz56358	ISE 3.0 で最初の SAN エントリのみがチェックされる
CSCvz46560	jquery v1.10.2 を使用する ISE が脆弱になっている。
CSCwa20309	「不明なNAD（Unknown NAD）」および「正しく設定されていないネットワークデバイスを検出（Misconfigured Network Device Detected）」アラーム
CSCvy84989	POST /ers/config/internaluser/ の Cookie を有効にすると、「IDグループが存在しません（Identity Group(s) does not exist）」というエラーが発生する
CSCwa08484	セッションに IPv4 アドレスと IPv6 アドレスの両方がある場合に、IPv4 マッピングがない
CSCvz99405	OpenSSL が 2.7p4 または 2.7p5 でアップグレードされない
CSCvy96761	EAP チェーンフローを実行して関連する ID を処理する際に、セッションキャッシュを更新する必要がある
CSCvz57551	ポーリング間隔と準拠デバイス再認証クエリの間隔
CSCvz86020	「開かれているファイルが多すぎます（too many files open）」エラーにより、ライブログ/セッションに最新のデータが表示されない
CSCvs95495	再認証の問題：Aruba：サードパーティのデバイス
CSCvz63405	ISE クライアントの pxgrid 証明書が DNAC に配信されない
CSCvz00706	「関心のあるグループ」が、改行が 1 つ入った単一文字列として返される
CSCwa20354	[運用データの消去（Operational Data purging）] -> [データベース使用率（Database utilization）] -> [ノード情報（Node info）] が断続的に表示されない。
CSCwa05404	「Tacacsで確認された古いセッションで選択したサービスが見つかりませんでした（Stale Sessions observed for Tacacs Could not find selected service）」というエラー
CSCwa47566	ISE 条件スタジオ - [IDグループ（Identity Groups）] ドロップダウンを 1000 個に制限

ID	見出し
CSCvz80829	3.2 のフルアップグレードでバージョンの事前チェックが失敗する
CSCwa41166	TACACS コマンドセットの正規表現が間違っている
CSCwa78479	CVE-2021-4034 Polkit の Cisco Identity Services Engine 評価
CSCvz95326	ISE で ACI 統合を有効にしようとすると、複数の ACI IP アドレスまたはホスト名を追加できなくなる
CSCwa19573	SSL 監査イベントが原因で Catalina.out ファイルが巨大化する
CSCwa13877	ISE スマートライセンス認証更新の失敗：詳細 = ライセンスクラウドからの無効な応答
CSCwa23207	メモリ割り当ての不整合が原因で複数のランタイムがクラッシュする
CSCvz71284	SNMPv3 COA 要求が ISE 2.7 によって発行されない
CSCvz93230	Gig0 とは異なるインターフェイスでホストされている場合に、ゲストポータルがロードされない
CSCwa32312	セッションキャッシュが入力されていないため、RCM および MDM フローが失敗する
CSCvz88188	セッションキャッシュのユーザー名が null であるため、ユーザー名に対する TACACS 認証ポリシーのクエリ実行に失敗する
CSCwa56771	ISE 3.0p2：[すべてをモニター（Monitor All）] 設定が複数のマトリックスと異なるビューで正しく表示されない
CSCvz67479	すべてのフィールドの [ローカルログの設定（Local Log Settings）] ツールチップに、無関係で役に立たない「信頼できる証明書（Trust Certificates）」が表示される
CSCwa26210	「GET /ers/config/radiusserversequence」API の JSON 応答に nextPage フィールドがない
CSCwa15191	EP が不明なポスチャでスタックする：MAC で LSD のセッションが見つからない
CSCvz56171	ISE Doc：SXP バインディングに関する ISE SDK ドキュメントに使用できないキーが含まれている
CSCwa11659	CIAM：libx11 1.6.8
CSCvy40956	[DOC] CoA API ドキュメントをより明確にしてください
CSCvz60870	TPS が高いときに Active Directory の遅延が大きいと、ADRT で HOL ブロッキングが発生する

ID	見出し
CSCwa47133	ISE 評価 log4j CVE-2021-44228
CSCvz50255	CIAM：bind 9.11.20
CSCwa47221	クライアント プロビジョニング ポリシーの AD セキュリティグループで OU の末尾をドット文字にできない
CSCvy82023	不適切なポスチャ複合条件のホットフィックス
CSCvz79665	Microsoft Intune Graph の URL を graph.windows.net/tenant から graph.microsoft.com に変更
CSCwa52667	プロファイル名に波カッコを含めると、認証プロファイルを保存できない
CSCwa20152	マトリックスが変更されていないスイッチの ISE で CoA が開始されなかったため、ポリシーの同期に失敗した
CSCvz83753	AuthZ の高度な属性設定に含まれる空のユーザーカスタム属性により、誤った AVP が発生する
CSCvz65576	CLI リポジトリまたはディスクリポジトリが使用されている場合、パッチでフルアップグレードが機能しない
CSCwa11633	ISE 3.0：APIC 統合：secGroup を作成できない
CSCvz85117	ISE ヘルスチェックおよび I/O 帯域幅のパフォーマンスチェックの誤報
CSCwa60873	PAN のパフォーマンスを向上させるために bouncy-castle クラスを最適化する
CSCvy33615	ISE 3.1 BH のデフォルトのプロファイリングポリシーの説明にスペースではなく余白文字の 16 進コードが含まれている
CSCwa43187	ISE キューリンクエラー：Message=From Node1 To Node2、Cause=Timeout in NAT'ed deployment
CSCwa16401	Get-By-Id サーバーシーケンスが GUI を介してシーケンスで最初の変更を行った後に空のサーバーリストを返す
CSCvz00034	ログ「この更新フィールドは現在の時刻よりも1週間以上前です（this update field is earlier than currunet time more than week）」のログレベルを変更する
CSCvy89317	ISE：DST ルート CA X3 認証局：2021 年 9 月 30 日で失効（90 日以内）
CSCvw65181	CIAM で POI の脆弱性が検出された
CSCvy05713	2.7 P4、2.6 P10 から ISE 3.0 にアップグレードする場合は、スマートライセンス（サテライト/PLR）を無効にする必要がある

ID	見出し
CSCwa59621	ID グループに対する ERS API の並べ替えが一貫していない
CSCvz74457	ERS API で「ネットワーク デバイス グループ」名にドット文字の使用または作成/更新が許可されていない
CSCvo39514	コレクタログ権限のため、MnT ログプロセッサが動作しない
CSCvz55258	Cisco:cisco-av-pair AuthZ 条件の機能が停止した
CSCwa46758	削除されたルート ネットワーク デバイス グループがネットワークデバイスでエクスポートされた CSV レポートで引き続き参照されている
CSCwa52110	ネットワークデバイスに設定された SNMP 構成で SNMP レコードの処理中に 20 秒の遅延が発生する
CSCvz71872	CIAM：nss - 複数のバージョン
CSCvz83204	ISE で、ポスチャフロー中に発生した不適切なインデックスから URL 属性値を取得できない

Cisco ISE リリース 2.7.0.356 の未解決の不具合：累積パッチ 7

不具合 ID 番号	説明
CSCvy86859	Mac OS Beta Monterey（MacOS 12 beta 2）で NSP MacOsXSPWizard 3.1.0.2 に失敗する
CSCwb07442	Pxgrid 接続が PAN のフェールオーバー後に開始されない
CSCwb29140	nss rpm が更新された最新のパッチに移行した後、スレッドが使い果たされる（3.0p5 と 2.7p7、3.1P1 のみ）

次のホットパッチファイルは、CSCwb29140 の CCO で入手できます。

- ホットパッチをインストールするには、以下を実行します。

  ise-apply-CSCwb29140_2.7.0.356_patch7-SPA.tar.gz

- ホットパッチをロールバックするには、以下を実行します。

  ise-rollback-CSCwb29140_2.7.0.356_patch7-SPA.tar.gz

Cisco ISE リリース 2.7.0.356 の解決済みの不具合：累積パッチ 6

次の表に、リリース 2.7 累積パッチ 6 の解決済みの不具合を示します。

パッチ 6 は古いバージョンの SPW で機能しない可能性があります。MAC ユーザーは SPW を MACOSXSPWizard 2.2.1.43 以降にアップグレードする必要があります。また、Windows ユーザーはその SPW を WinSPWizard 2.2.1.53 以降にアップグレードする必要があります。

不具合 ID 番号	説明
CSCvn27270	ISE：名前、場所、またはデバイスタイプを使用してネットワーク デバイス グループを作成できない
CSCvw90586	ネットワーク デバイス グループの名前と説明を同時に変更できない
CSCvx23375	編集/保存中に ISE 認証プロファイルオプションが切り捨てられる（Chrome のみ）
CSCvx48255	CIAM：画面 4.1.0 CVE-2021-26937
CSCvx58520	PLR でプロファイラオンライン更新エラー：ライセンスファイルデータの取得に失敗：Null
CSCvy14905	CTS-SXP-CONN：デバイスから ISE SXP 接続への ph_tcp_close：Hawkeye
CSCvy45345	マシン認証フラグが誤って「True」に設定されているため、EAP チェーン認証が失敗する
CSCvy51210	ISE 2.7 で NAD の IP デフォルトラベルを GUI で削除しようとすると、エラーが表示される。
CSCvy53842	特定の証明書監査中に証明書の検証の Syslog メッセージが送信された - ISE
CSCvy71229	CIAM：libx11 1.6.8
CSCvy71261	CIAM：nettle 3.4.1
CSCvy71313	CIAM：cpio 2.12
CSCvy75191	Cisco Identity Services Engine の XML 外部エンティティ インジェクションの脆弱性
CSCvy76328	[ネットワークデバイス（Network device）] タブの [複製（duplicate）] オプションを使用すると、ipv6 の [サブネット（Subnet）] が /128 に変更される
CSCvy92040	[ISE復元（ISE restore）] ポップアップメニューに誤ったテキストが表示される
CSCvy94818	nmap が積極的な推測を実行したため、EP が「cisco-router」として不適切にプロファイリングされる
CSCvz00258	Tacacs 認証でセッションキャッシュがクリアされないエラーにより、ヒープの使用率が高くなり、認証の遅延が発生する

不具合 ID 番号	説明
CSCvz13783	ライセンスページのパッチ 13 へのアップグレード後のカウントが 0 になる
CSCvz18627	PEAP セッションのタイムアウト値が最大で 604800 に制限されている
CSCvz22331	1 日の特定の時間（分）について時刻と日付の条件で設定されたポリシーで認証がブロックされない。
CSCvz33839	メニューアクセスのカスタマイズが機能していない
CSCvz34849	DELETE /ers/config/networkdevicegroup/{id} が機能していない。CRUD の例外
CSCvz36192	/ers/config/downloadableacl を使用した DACL の GET に、存在する nextPage または previousPage が追加されない。
CSCvz43183	「名前による」呼び出しの場合、スポンサーのアクセス許可がゲスト REST API に渡されない。
CSCvz44655	ISE 管理アカウントの選択に関する問題
CSCvz51536	ISE ワイルドカード証明書が内部エラーで失敗する
CSCvz70947	ATZ プロファイルの下の SG にあるサブネット/IP の [プール名を追加（Add Pool Name）] が Chrome で表示されない（2.7P5 に固有）
CSCvz71459	ポーリング間隔の Microsoft_intune MDM ISE 変更がキャッシュに反映されない
CSCvz99405	OpenSSL が 2.7p4 または 2.7p5 でアップグレードされない
CSCwa00729	1 つの特定の NAD を削除すると、すべての NAD が削除される。

Cisco ISE リリース 2.7.0.356 の未解決の不具合：累積パッチ 6

Cisco ISE リリース 2.7 パッチ 6 には未解決の不具合はありません。

Cisco ISE リリース 2.7.0.356 の解決済みの不具合：累積パッチ 5

次の表に、リリース 2.7 累積パッチ 5 の解決済みの不具合を示します。

パッチ 5 は古いバージョンの SPW で機能しない可能性があります。MAC ユーザーは SPW を MACOSXSPWizard 2.2.1.43 以降にアップグレードする必要があります。また、Windows ユーザーはその SPW を WinSPWizard 2.2.1.53 以降にアップグレードする必要があります。

（注） Cisco ISE パッチ 5 がインストールされ、PAN にのみロールバックされ、PAN に登録されているノードにはロールバックされない場合、ノード上のアプリケーションサーバーが初期化状態でスタックします。この問題を回避するには、ノードに Cisco ISE パッチ 5 をインストールしてロールバックしてから、ノードを PAN に登録する必要があります。

不具合 ID 番号	説明
CSCvi53134	Passive-ID サービスを有効にすると、Cisco ISE と AD の統合操作に使用されるアカウントがロックされることがある。
CSCvi59005	スクロールバーを使用すると、AD グループの完全なリストを表示できない。
CSCvn25548	「非アクティブのため、アカウントが無効になっています（account was disabled due to inactivity）」という誤ったエラーメッセージが表示される。
CSCvo56767	Cisco ISE-PIC GUI 管理者ユーザー設定を変更しようとするとエラーが発生する。
CSCvr03959	[承認要求電子メール送信先（Email approval request to）] ドロップダウンリストで [訪問先担当者（Person Being Visited）] オプションを選択しても、必須にならない。
CSCvr76539	ネットワーク デバイス グループへの変更が変更監査ログに反映されない。
CSCvs66551	Apache log4j の複数の脆弱性。
CSCvt52104	Jetty の複数の脆弱性。
CSCvt94587	Cisco ISE ルート CA の再生成中に表示される「Plusライセンスがコンプライアンス違反状態です（Plus License is out of Compliance）」というメッセージが無効になる。
CSCvu04874	io.netty.buffer.PoolChunk での疑わしいメモリリーク
CSCvu56753	CIAM：openjdk の複数の脆弱性。
CSCvu72744	すべての認証および認可のルールとプロファイルで「blacklist」が「blocked list」に置換される。
CSCvu84184	ゲストポータルで証明書チェーンが送信されない。
CSCvv04957	GRUB2 の任意のコード実行の脆弱性。
CSCvv07101	エンドポイントが Cisco ISE にある場合、PKCS11 キーストアによりメモリリークが発生する。
CSCvv55602	ポリシーエンジンの機能強化。

不具合 ID 番号	説明
CSCvv68293	ローカルまたはグローバルの例外を使用する場合、Cisco ISE は Plus ライセンスを消費しない。
CSCvv77928	プライマリ PAN で障害が発生すると、「予期しないエラーが発生しました（An unexpected error occurred）」というメッセージと共に証明書の一括生成が失敗する。
CSCvw09827	PSN の CPU 使用率が高い：CSCvt34876 の拡張機能。
CSCvw69977	[すべてのSXPマッピング（All SXP Mapping）] テーブルに終了したセッションが含まれる
CSCvw78019	Cisco ISE リリース 2.7 へのアップグレード後に NTP が同期しなくなる。
CSCvw89326	PKI ベースの SFTP の場合、MnT ノードの GUI キーのエクスポートは PAN に昇格した場合にのみ可能となる。
CSCvx01272	証明書の一括生成に Cisco ISE の自己署名証明書が含まれていない。
CSCvx22229	結合インターフェイスの IP アドレスを変更すると、Cisco ISE の「ipv6 address autoconfig」が削除される。
CSCvx47691	セッションディレクトリのトピックで、ダイナミック認証後もユーザーの SGT 属性が更新されない。
CSCvx53205	NIC ボンディングにより、MAR キャッシュが複製されない。
CSCvx60818	ERS 自己登録ポータルの更新で PSN フィールドが期待どおりに削除されない。
CSCvx69701	データベース接続が利用できないため、展開の同期に失敗した。
CSCvx78643	電子メールアドレスが設定されていない場合でも、すべてのシステムアラームについて電子メールが送信される。
CSCvx85675	競合状態が原因で Cisco ISE が SXP から IP へのマッピングの伝播の削除/追加を処理できない。
CSCvx86921	RADIUS トークン ID ソースプロンプトと TACACS 認証の内部ユーザープロンプト。
CSCvx96190	上位認証レポートで、スケジュールされたレポートのフィルタが表示されない。
CSCvx99151	Cisco ISE 内部 ERS ユーザーが外部 ID ストア経由で認証を試行すると、REST の遅延が発生する。

不具合 ID 番号	説明
CSCvx99675	バックアップ インターフェイスが設定されている場合に、Cisco ISE セカンダリ PAN がリンクローカルアドレスを使用して他のノードにパケットを送信する。
CSCvy04443	再認証用の MNT REST API が分散型展開で使用されると失敗する。
CSCvy04665	完全な数値 ID エントリを照合すると、TACACS レポートの詳細フィルタが機能しない。
CSCvy05954	[すべてのSXPマッピング（All SXP Mappings）] ウィンドウにセッション経由で学習した IPv6 マッピングが表示されない。
CSCvy06417	Cisco ISE の永続的な XSS 管理者グループ。
CSCvy06719	[手動アクティブセッション（Manual Active Session）] レポートが空になっている。
CSCvy14342	PIP クエリの評価が原因で Cisco ISE リリース 2.6 パッチ 3 以降のリリースの PSN で CPU 使用率が高くなる。
CSCvy15058	API 経由でドメインを「ブロック/許可する」に更新できない
CSCvy17893	ISE REST API が IP-SGT マッピングに重複する値を返す。
CSCvy18560	[RADIUSアカウンティングの詳細（RADIUS Accounting Details）] レポートにアカウンティングの詳細が表示されない。
CSCvy20277	一部のオブジェクトの [説明（Descriptions）] フィールドで以前は許可されていた特殊文字が使用できなくなった。
CSCvy23354	Mozilla Firefox 88 を使用している場合に、[説明（Description）] フィールドを読み取ることができない。
CSCvy24303	ライセンスの使用状況の推移グラフに間違った情報が表示される。
CSCvy24370	Cisco ISE で RADIUS シーケンス属性において 7 個以上の属性を変更できない。
CSCvy25533	CLI バックアップ中に「/opt/CSCOcpm/config/cpmenv.sh:line 396:<ipv6>:command not found」というエラーが表示される。
CSCvy25550	Cisco ISE が認証プロファイルで Framed-IPv6-Address のカスタム属性名を受け入れない。
CSCvy30119	オプションに他の変更を加えると、LDAP グループがスポンサーグループから消える。

不具合 ID 番号	説明
CSCvy32461	[電話（phone）] フィールドまたは [電子メール（email）] フィールドが入力されている場合に、スポンサーユーザーはデータを編集できない。
CSCvy34977	証明書テンプレートの曲線タイプ P-192 が原因でアプリケーションサーバーが「初期化（initializing）」状態でスタックする。
CSCvy36868	Cisco ISE リリース 2.3 以降のリリースはコマンドセットで「改行」<cr> 文字をサポートしていない。
CSCvy36968	ライセンスの詳細を取得できず、機能が無効になっている。
CSCvy38459	Cisco ISE リリース 2.7 パッチ 3 GUI にすべてのデバイス管理認証ポリシーが表示されない。
CSCvy38896	Framed-IP 値のない AAA 要求により、SXP プロセスで例外が発生する。
CSCvy40845	ERS リクエストを通じてカスタム属性を更新すると、別の属性も更新される。
CSCvy41066	ポリシーの条件としての TACACS カスタム AV ペアが機能していない。
CSCvy42885	設定のバックアップがキャンセルされたために Cisco ISE アプリケーションサーバーがクラッシュまたは再起動する。
CSCvy43246	ユーザーがポータルの作成手順でゲスト SSID を作成できない。
CSCvy45015	[電話番号をユーザー名として使用（Use Phone number as username）] オプションが有効な場合に、重複ユーザーの Cisco ISE ゲスト自己登録エラーが発生する。
CSCvy46504	Cisco DNA Center からポリシーを展開しようとしているときに、Cisco DNA Center で断続的なエラーが発生する。
CSCvy48766	all-numbers サブドメインが使用されている場合、Cisco ISE のインストールがデータベースのプライミング失敗エラーで失敗する。
CSCvy51073	Cisco ISE 認証プロファイル ERS の更新で accessType 属性の変更が無視される。
CSCvy58771	NAD の編集中に、間違ったデバイスプロファイルがマッピングされる。
CSCvy60865	エンドポイントが認証済みのスイッチまたはポートから移動され、認証ポリシーによって参照されている ID グループが変更されると、Cisco ISE は CoA の送信に失敗する。
CSCvy61564	Cisco ISE リリース 2.7 パッチ 3 の ERS コールが 3 文字の RADIUS 共有秘密を受け入れない。

不具合 ID 番号	説明
CSCvy62875	Cisco ISE リリース 2.7 パッチ 2：[400] Apple デバイスでの SAML SSO OKTA による不正な要求。
CSCvy63778	CoA の REST API が任意のサーバー IP で動作する。
CSCvy65786	% 文字を含む AD アカウントパスワードを使用して WMI を設定すると、エラーになる。
CSCvy68023	Cisco ISE-PIC 2.7 以前ではドメインコントローラで TLS 1.2 を使用する必要がある。
CSCvy71690	ゲストポータルの [顧客（Customer）] フィールドに &、- $、# が含まれる。
CSCvy72028	Cisco ISE 2.7 パッチ 4：pxGrid の [サービス（Services）] > [すべてのクライアント（All Clients）] ウィンドウが java.lang.NullPointerException で終了する。
CSCvy74456	Cisco ISE を介した外部 Cisco DNA Center 認証が「無効なログイン情報（Invalid login credentials）」というエラーで失敗する。
CSCvy74919	非アクティブタイマーに達した後も Cisco ISE 内部ユーザーが無効にならない。
CSCvy76262	Cisco ISE DACL 構文バリデータが ASA のコード要件に準拠していない。
CSCvy76617	Cisco ISE：NAD ウィンドウのフィルタの有無にかかわらず、デバイスの [すべて選択（Select All）] チェックボックスをオンにする必要がある。
CSCvy81435	Cisco ISE ゲスト SAML 認証が [アクセス権が検証されました（Access rights validated）] HTML ウィンドウで失敗する。
CSCvy82114	[ネットワークアクセスユーザー（Network Access Users）] の [姓名（First/Last name）] に誤った中国語の Unicode が表示される。
CSCvy90691	RADIUS ベンダー ID が重複すると、PSN がクラッシュすることがある。
CSCvy94427	Cisco ISE リリース 2.7 で EAP チェーンのポスチャリースが中断する。
CSCvy94511	EPOCH 時間が Null になっているため、TACACS レポートに重複したエントリが表示される。
CSCvy94553	TACACS 認証レポートに重複したエントリが表示される。
CSCvy96144	Cisco ISE の GUI に UDI 情報がない。
CSCvy99582	外部 RADIUS サーバーが設定されている場合に、Cisco ISE リリース 2.4 パッチ 13 から Cisco ISE リリース 2.7 へのアップグレードが失敗する。

不具合 ID 番号	説明
CSCvz01485	Cisco ISE リリース 2.7 パッチ 4 で Umbrella セキュリティプロファイルの .json ファイルをアップロードできない。
CSCvz05704	ディスクサイズが 1 TB を超える Cisco ISE のプラットフォームチェックが失敗する。
CSCvz07823	Cisco ISE リリース 2.7 でエンドポイントをグループに追加できない。
CSCvy11865	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性。
CSCvy62395	アップグレードログはログディレクトリに記録し、サポートバンドルに追加する必要がある。
CSCvx85051	セキュリティグループの VLAN フィールドにサフィックスではなく完全なディクショナリ属性値が入力されている。
CSCvw90778	[展開（Deployment）] ウィンドウでデバイスの管理プロセスを無効にしても、T+ ポート（49）が開いている。

Cisco ISE リリース 2.7.0.356 の未解決の不具合：累積パッチ 5

不具合 ID 番号	説明
CSCvz70947	セキュリティグループに追加されたサブネット/IP アドレスのプール名が Chrome ブラウザの [認証プロファイル（Authorization Profiles）] ウィンドウに表示されない
CSCwa00729	1 つの特定の NAD を削除すると、すべての NAD が削除される。

Cisco ISE リリース 2.7.0.356 の新機能：累積パッチ 4

Cisco ISE GUI に追加されたフルアップグレードと分割アップグレードのオプション

[管理（Administration）] > [システム（System）] > [アップグレード（Upgrade）] > [アップグレードを選択（Upgrade Selection）] ウィンドウで次のオプションのいずれかを選択して、Cisco ISE 展開をアップグレードできます。

- [フルアップグレード（Full Upgrade）]：フルアップグレードは、Cisco ISE 展開の連続した完全なアップグレードを可能にするマルチステッププロセスです。この方法により、すべてのノードが並行してアップグレードされ、分割アップグレードプロセスよりも短時間でアップグレードされます。すべてのノードが並行してアップグレードされるため、アップグレードプロセス中にアプリケーションサービスがダウンします。

（注） フルアップグレード方法は、Cisco ISE 3.1 以降でサポートされています。フルアップグレード方法の詳細については、「Cisco Identity Services Engine Upgrade Journey, Release 3.1」を参照してください。

- [分割アップグレード（Split Upgrade）]：分割アップグレードは、アップグレードプロセス中にサービスを引き続き利用できるようにしながら、Cisco ISE 展開のアップグレードを可能にするマルチステッププロセスです。このアップグレード方法では、展開時にアップグレードする Cisco ISE ノードを選択できます。

エアギャップネットワークのライセンス方式

Smart Software Manager（SSM）オンプレミスは、Cisco ISE 対応ネットワークでスマートライセンスを管理する SSM オンプレミスサーバーを設定する接続方式です。この接続方法では、Cisco ISE はインターネットへの永続的な接続を必要としません。

詳細については、『Cisco Identity Services Engine Administrator Guide』の「Licensing」の章を参照してください。

Cisco ISE リリース 2.7.0.356 の解決済みの不具合：累積パッチ 4

次の表に、リリース 2.7 累積パッチ 4 の解決済みの不具合を示します。

パッチ 4 は古いバージョンの SPW で機能しない可能性があります。MAC ユーザーは SPW を MACOSXSPWizard 2.2.1.43 以降にアップグレードする必要があります。また、Windows ユーザーはその SPW を WinSPWizard 2.2.1.53 以降にアップグレードする必要があります。

不具合 ID 番号	説明
CSCuo73496	ISE RADIUS session-timeout 値が 65535 までに制限される
CSCvh04231	「ゲストユーザー情報を保存」の RADIUS アカウンティングおよびアクセス許可でゲストユーザー名が送信されない
CSCvo04728	MIT Kerberos 5 KDC krbtgt チケット S4U2Self リクエストのサービス妨害の脆弱性
CSCvq26124	ISC BIND managed-keys トラストアンカーのサービス妨害の脆弱性
CSCvq58506	show running-config を完了できない
CSCvr55906	cURL および libcurl tftp_receive_packet() 関数ヒープ バッファ オーバーフローの脆弱性 CVSS v3.1 Base：9.8
CSCvr77653	cURL および libcurl tftp_receive_packet() 関数ヒープ バッファ オーバーフローの脆弱性 CVE-2019-5436

不具合 ID 番号	説明
CSCvr77655	GNU パッチ pch_write_line 関数のサービス妨害の脆弱性
CSCvr80914	SSSD グループポリシーオブジェクトの実装における不適切なアクセス制御の脆弱性
CSCvr80921	ISC BIND Dynamically Loadable Zones における不正アクセスの脆弱性
CSCvr80934	Samba シンボリックリンクのトラバーサルの脆弱性 CVSS v3.1 Base：5.4
CSCvr81463	libssh2 packet.c の整数オーバーフローの脆弱性 CVSS v3.1 Base：8.1
CSCvr94153	TPS：prrt における curl lib の更新
CSCvr97388	Samba ファイル名パス区切り文字の不正アクセスの脆弱性
CSCvs39800	gllibc LD_PREFER_MAP_32BIT_EXEC 環境変数の ASLR バイパスの脆弱性
CSCvs45350	サプリカントからユーザークレデンシャルが送信されず、マシンクレデンシャルしか使用できない場合に、ISE でのユーザー名の表示が匿名になる
CSCvs52211	CiscoSSL を更新して CSCvg56800 を修正：nginx の脆弱性に関する ISE の評価（2017 年 10 月）
CSCvs76914	libxml2 xmlParseBalancedChunkMemoryRecover メモリリークの脆弱性
CSCvs91984	systemd button_open のメモリリークの脆弱性
CSCvt11130	sh version コマンドが管理者以外の CLI ユーザーで動作しない
CSCvt11664	「createLicenseSource」メソッド「FlexlmListException: Error」で ISE フィードサーバーが失敗する
CSCvt30558	python の複数の脆弱性
CSCvt44403	Showtech の SSLDUMP() ログが監査ログで出力され、showtech ファイルが大幅に大きくなる
CSCvt51244	activemq-all の複数の脆弱性
CSCvt76509	SFTP リポジトリにスペースがないが、ISE バックアップファイル転送ログに [Success] と表示される
CSCvt85370	ポスチャ条件が「vc_visInst_v4_CiscoAnyConnectSecureMobilityのチェックでClient_4_xが見つかりません（Check vc_visInst_v4_CiscoAnyConnectSecureMobility Client_4_x is not found）」エラーで失敗する
CSCvt95762	ISE 2.6/2.7 で RHEL を SFTP リポジトリとして使用している場合にファイルがリストされない

不具合 ID 番号	説明
CSCvu13139	2.4.50 より前の OpenLDAP の slapd の filter.c で、ネストされたブール式を使用したLDAP検索フィルタによってサービス妨害が発生することがある
CSCvu16067	IP-TABLES の変更によって TCP 遅延と TACACS 遅延が発生する
CSCvu18256	PAN および SAN ノードでの application stop ise で「Service 'stunnel' -- doesn't exist」と表示される
CSCvu22058	DUO を外部 RADIUS プロキシとする ISE で access-reject がドロップされる
CSCvu38918	操作監査レポートに「backend」アカウントで実行されたアクションのログが含まれる
CSCvu58927	ISE UI およびコード内のいかなる場所においても「blacklist portal」を「blocked list portal」に更新する
CSCvu58954	ISE UI およびコード内のいかなる場所においても「blacklist identity group」を「blocked list identity group」に更新する
CSCvu59038	「show interface」コマンドの「master/slave」という用語を「primary/subordinate」に更新する
CSCvu62938	プライマリ PSN/PAN に到達できない場合にポスチャが失敗する
CSCvu63833	AD がアイデンティティソースとして選択されている場合、監査レポートに ISE GUI への失敗したログインが表示されない
CSCvu68240	日次消去が行われていないため、消去するデータがリポジトリにコピーされない
CSCvu82889	netstat コマンドによって ISE で carssh シェルがクラッシュする
CSCvv09167	TACACS 集約テーブルが正しく消去されない
CSCvv14390	最大セッション数制限がユーザーとグループに対して機能しない
CSCvv19065	ISE ユーザーが DNAC アシュアランスページでゲスト ID を確認できない
CSCvv29737	DNA Center のスケーラブルグループの同期が「JDBCException：ステートメントを準備できませんでした（JDBCException:could not prepare statement）」エラーで失敗する
CSCvv30161	ライブセッション詳細レポートで、VPNポスチャシナリオについて誤った認証プロファイルと認証ポリシーが表示される
CSCvv43383	NFS リポジトリが GUI から機能しない
CSCvv45340	実行コンフィギュレーションを保存するとスタートアップ コンフィギュレーションが失われる

不具合 ID 番号	説明
CSCvv61732	異なる SNMP サーバーに対して一意のコミュニティストリングを作成できない
CSCvv63548	メモリリーク：PSN rmi GC の収集が正しく機能せず、パッシブ ID フローでメモリリークが発生する
CSCvv67091	Cisco Identity Services Engine の信頼できないファイルアップロードの脆弱性
CSCvv74361	ISE 3.0 ヘルスチェックライセンス検証の誤ったアラーム
CSCvv77007	ISE で内部のネットワーク管理者ユーザーに対するリクエストが外部の RADIUS トークンサーバーに送信される
CSCvv79940	ISE で SAN の hostname-x を使用して CSR を生成するとエラーになる
CSCvv83510	RuleResultsSGTUpgradeService ステップで ISE 3.0 アップグレードが失敗する
CSCvv85588	メモリリーク：PassiveID ストレス時の使用者 CAD_ValidateUser で割り当てが高くなる
CSCvv90612	WebUI の復元が IE11 で機能しない
CSCvv93442	ISE 2.6p3 で SFTP サーバーのファイルパスに二重のスラッシュ「//」が追加される
CSCvw02887	AD グループの追加後にパッシブ ID フローでメモリリークが発生する
CSCvw06722	スポンサーが自身のユーザー ID でポータルにアクセスしたときに、作成されたゲストユーザーのリストを表示できない
CSCvw08602	IP オーバーラップの場合にエラーがスローされない
CSCvw10671	GNU.org bash rbash BASH_CMDS の変更特権昇格の脆弱性
CSCvw16237	PMNT のリロード後にスケジュール済みの OPS のバックアップがトリガーされない
CSCvw17908	デフォルトルートにタグ付けされている場合、ISE からスイッチへの SGT マッピングに対する IP のプッシュが機能しない
CSCvw20060	Windows ネットワーク インターフェイスよりも先にエージェントサービスが起動した場合、エージェントで DC がダウンとしてマークされる
CSCvw22228	pxGrid ANC applyEndpointPolicy ですべての MAC アドレス形式を正しく扱われない

不具合 ID 番号	説明
CSCvw24268	Cisco Identity Services Engine の信頼できないファイルアップロードの脆弱性
CSCvw25285	パッシブ ID がマルチ接続 syslog クライアントで安定して動作しない
CSCvw26415	ISE 3.0 で CN および SAN が欠落している証明書が信頼できる証明書ストアにインポートされない
CSCvw29490	内部ユーザーのカスタム属性が CoA プッシュで送信されない
CSCvw31269	SAML グループがスポンサーポータルグループで適用した場合に機能しない
CSCvw33115	VPN のユースケースで ISE MNT ライブセッションのステータスが「ポスチャ済み」に変わらない
CSCvw37844	ISE で内部コールにホスト名が使用されるため ANC CoA が機能しない
CSCvw48396	Cisco ADE-OS のローカル ファイル インクルードの脆弱性
CSCvw48403	エンドポイントについての収集された SNMPv3 情報が ISE で処理されない
CSCvw48697	API IP SGT マッピングが [No Devices] の結果を返さない
CSCvw49938	TACACS コマンドの前にスペースを含むサードパーティデバイスについて、TACACS コマンド アカウンティング レポートが生成されない
CSCvw50381	猶予アクセスの期限が切れたときに Aruba WLC に対する CoA-disconnect が ISE で発行されない
CSCvw50829	RBAC ポリシーで AD セキュリティグループの OU の末尾をドット文字にできない
CSCvw51801	ISE ライブセッションの「ポスチャ済み」セッションが暫定アップデートを受け取ると「開始済み」に 切り替わる
CSCvw53412	サポートバンドルで Hibernate.log を収集する必要がある
CSCvw53740	GNU Bash SHELLTOPTS および PS4 環境変数におけるローカルの任意のコマンドインジェクションの脆弱性
CSCvw58538	GNOME GLib file_copy_fallback 関数の不適切な権限の脆弱性
CSCvw58824	バージョン 1.4.15 より前の XStream の複数の脆弱性
CSCvw59312	Freetype の CVE-2020-15999 および CVE-2018-6942 のヒープ バッファ オーバーフロー

不具合 ID 番号	説明
CSCvw59314	moment モジュールの日付文字列の正規表現に関するサービス妨害の脆弱性
CSCvw59920	c3p0 の複数の脆弱性
CSCvw60197	glibc の複数の脆弱性
CSCvw61589	ISE ポリシー評価：ポリシーセットの削除後に RADIUS 要求がドロップされる
CSCvw61786	スキーマオブジェクトをドロップする前に復元プロセスを停止する必要がある
CSCvw66483	選択した外部サーバーのリストが変更された後に RADIUS サーバーの順序が間違った順序になる
CSCvw68480	ISE 展開で複数の SXP ノードを使用している場合にマッピングの総数が正しく表示されない
CSCvw73529	スマートライセンスと永久ライセンスの予約に [オンプレミスサテライト（OnPrem Satellite）] オプションがない
CSCvw73928	NTP 同期エラーアラームを変更する必要がある
CSCvw75397	IP アクセスが有効な場合に MNT ノード名が NULL に設定される
CSCvw75563	パスコードフィールドに特殊文字が含まれていると、ホットスポット ゲスト ポータルでページロードエラーが表示される
CSCvw77219	Dot1x 認証がマネージャの重複で失敗する：add=false
CSCvw78289	50 文字を超えるプロファイル名を使用している場合、認証に成功したことを示すライブログが表示されない
CSCvw80520	ISE メッセージングサービスが無効になっている場合、RADIUS 認証の詳細レポートに時間がかかる
CSCvw82774	ユーザー ID グループでユーザー名に基づくソートが機能しない
CSCvw82784	TACACS+ のエンドステーション ネットワーク条件のスクロールバーが機能しない
CSCvw84127	設定監査の詳細に変更されたポリシーセットが表示されない
CSCvw85860	ISE pxGrid の例外のログレベルは DEBUG ではなく ERROR である必要がある
CSCvw87147	ライブセッションで正しいアクティブセッションが表示されない

不具合 ID 番号	説明
CSCvw87173	MAB の認証されたエンドポイントの AD 認証が失敗する
CSCvw87175	Active Directory を使用した MAB 認証が AD オブジェクトが無効でも成功する
CSCvw88881	データベースクリーンアップの毎時 cron で DB ロックが取得される結果、展開の登録に失敗する
CSCvw90961	RBAC ルールが 2.7 で適用されない
CSCvw93570	ISE 2.4 パッチ 8：ゲストポータルを編集、複製、削除できない
CSCvw94096	ISE BYOD ポータルで iPod がオプションとして表示されない
CSCvw94603	ポーリング間隔の変更が外部 MDM サーバー（Microsoft_intune）に反映されない
CSCvw95488	ISE 2.6：ソケットストリームで TACACS+ get_handle が呼び出されるとランタイムがクラッシュする
CSCvw96371	API からカスタム属性を更新すると、エンドポイントから静的ポリシーとグループの割り当てが失われる
CSCvw97905	暗号キーに特定の文字が使用されていると、内部ユーザーのエクスポートがエラーなしで失敗する
CSCvx01798	ISE RBAC：ネットワークデバイスの追加中に「ネットワークデバイスをロードできません（Unable to load Network Devices）」エラーが表示される
CSCvx04512	login.jsp に直接アクセスすると証明書ベースの認証による管理アクセスがバイパスされる
CSCvx09383	実行中のプロセスに基づいてエンドポイントアプリケーションをソートすると「すべてのシャーディングが失敗しました（All shards failed）」例外がスローされる
CSCvx10186	スマートライセンスに登録した後も ISE が評価期限切れ状態のままになる
CSCvx15427	ヘルスチェック：ISE FQDN が CNAME（エイリアス）として設定されている場合に DNS 解決可能性の誤ったエラーが表示される
CSCvx15448	ディスク容量ヘルスチェックのエラーメッセージは情報である必要がある
CSCvx18730	シスコ製品に影響する Sudo 権限昇格の脆弱性：2021 年 1 月
CSCvx23205	IdenTrust Commercial Root CA 1 証明書を ISE トラストストアに追加
CSCvx27632	認証では [ODBCストアドプロシージャ（ODBC Stored-Procedures）] ウィンドウで設定された形式で MAC アドレスを検索する必要がある

不具合 ID 番号	説明
CSCvx28402	ISE 2.7 以降のバージョンのサポートバンドルで ise-jedis.log ファイルがキャプチャされない
CSCvx30276	ルート CA の再作成時に Jedis DB 接続プールが再作成されない
CSCvx32666	ポリシーセットのエントリの評価で認証方式の条件が照合されない
CSCvx32764	予期しない電源イベントの後に TC-NAC サービスが実行されない
CSCvx36013	ISE ヘルスチェック プラットフォーム サポートが結果に従って UI を直接更新する
CSCvx37149	すべてのペルソナを同じノードで実行している SNS3515 の SGA 値が Under-Provisioned になる
CSCvx37297	シングルサインオン/Kerberos ユーザーによるスポンサーポータルへの認証でエラー 400 が発生する
CSCvx41826	Tenable SC 5.17 ですべての tenable アダプタリポジトリを取得できない
CSCvx43566	外部のユーザー名を使用している場合にパスワードの誤りによるログインの失敗がログに記録されない
CSCvx43825	NAS-IP アドレスが指定されていない acct stop を受信した場合にセッションが開始状態のままになる
CSCvx44815	ISE AD ランタイムで a1-a2-a3-a4-a5-a6 から a1a2a3a4a5a6 への書き換えをサポートする必要がある
CSCvx45481	スイッチポートとエンドポイント ID グループが変更された場合にエンドポイントの CoA が失敗する
CSCvx46638	EAP チェーンの場合にポスチャポリシーでマシン AD グループメンバーシップを取得できない
CSCvx47891	ISE で新しいエンドポイントの AMP イベントが正しくマッピングされない
CSCvx48922	TACACS フローのメモリリーク
CSCvx50752	Smart Call Home およびスマートライセンス用に IdenTrust Commercial Root CA 1 証明書を追加
CSCvx51738	Network Success Diagnostics 用に IdenTrust Commercial Root CA 1 証明書を追加
CSCvx53761	sxplocalbindings の REST クエリでコード500「CRUD 操作の例外（CRUD operation exception）」が返される

不具合 ID 番号	説明
CSCvx54213	[ネットワークデバイス（Network Devices）] > [デフォルトのデバイス（Default Device）] ページで Plus ライセンスが要求される
CSCvx57545	isedailycron temp1 のトラッキングにより AWR レポートで遅延が発生する
CSCvx58516	ネットワークデバイス別上位 N の認証の詳細が正しく表示されない
CSCvx61664	ISE で AnyConnect 出力設定ファイルの JSON ファイルの情報が更新されない
CSCvx70633	[TrustSec の詳細設定（Advanced Trustsec setting）] での [デバイス設定の展開（Device configuration deployment）] の設定で、[EXECモードパスワード（EXEC Mode password）] と [イネーブルモードパスワード（Enable Mode Password）] に % を使用できない
CSCvx71286	2.4 から 2.7P2 へのアップグレード後に SGT マッピングの重複が原因で SXP エンジンを起動できない
CSCvx78796	RADIUS 認証のトラブルシューティングレポートに誤ったデータが表示される、またはデータが表示されない
CSCvx79693	ISE との Qualys の統合が失敗する
CSCvx83663	ISE 2.7P3 でリンクローカルアドレス 169.254.2.2 の他のノードにパケットが送信される
CSCvx85391	ISE 内部データベースに保存されているユーザー名と認証ユーザー名で大文字と小文字が異なる場合、非アクティブタイマーが更新されない
CSCvx86571	ログインページのメッセージが空の場合は説明のボックスを削除する必要がある
CSCvx86915	TrustSec のページの UI に問題がある
CSCvx94452	2.7 p2 以降で EST サービスが実行されない
CSCvx96915	XStream 1.4.16 で修正された脆弱性
CSCvx99176	IP アドレス範囲に - または * を使用した NAD について、誤った IP オーバーラップエラーが報告される
CSCvy07333	パッチのインストール後にポスチャおよび BYOD のフローに影響がある
CSCvy15172	Cisco Identity Services Engine のセルフ クロスサイト スクリプティングの問題

Cisco ISE リリース 2.7.0.356 の未解決の不具合：累積パッチ 4

不具合 ID 番号	説明
CSCvx35960	TACACS+認証が「最大接続限度に達しました（Maximum Connection Limit Reached）」エラーで突然失敗する。

Cisco ISE リリース 2.7.0.356 の新機能：累積パッチ 3

ヘルス チェック

展開内のすべてのノードを診断するオンデマンド正常性チェックオプションが導入されています。運用の前にすべてのノードでヘルスチェックを実行すると、ダウンタイムやブロッカーを引き起こす可能性のある重大な問題を特定できます。ヘルスチェックは、すべての依存コンポーネントの動作ステータスを提供します。コンポーネントに障害が発生すると、問題を解決するためのトラブルシューティングの推奨事項が即座に提供され、シームレスな操作が実行されます。

アップグレードプロセスを開始する前に、ヘルスチェックを実行するようにしてください。

ビジネス成果：重要な問題を特定し、ダウンタイムやブロッカーを回避します。

DNS キャッシュ

ホストの DNS 要求をキャッシュできるため、DNS サーバーの負荷が軽減されます。

この機能は、次のコマンドを使用してコンフィギュレーション モードで有効にできます。

service cache enable hosts ttl *ttl*

この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

no service cache enable hosts ttl *ttl*

管理者は、キャッシュを有効にしながら、キャッシュ内のホストの存続可能時間（TTL）値を秒単位で設定できます。ttl のデフォルト設定はありません。1 ～ 2147483647 の範囲の値を指定できます。

（注） TTL 値は、否定応答に対して受け入れられます。DNS サーバーで設定された TTL 値は、肯定応答に対して受け入れられます。DNS サーバーで TTL が定義されていない場合は、コマンドで設定された TTL が受け入れられます。機能を無効にするとキャッシュも無効になります。

ビジネス成果：DNS サーバーの負荷が軽減されます。

設定済みの TCP パラメータ

TCP パラメータを設定するには、 **application configure** コマンドで [TCP パラメータの設定（Configure TCP params）] オプション（オプション 25）を使用します。管理 CLI を使用していることを確認します。

変更を有効にするには、管理 CLI の reload を使用してパラメータの変更時に Cisco ISE サーバーをリロードします。

例

TCP パラメータを設定するには、オプション 25 を使用します。

```
ise/admin#application configure ise

Selection configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[17]Enable/Disable Wifi Setup
[18]Reset Config Wifi Setup
[19]Establish Trust with controller
[20]Reset Context Visibility
[21]Synchronize Context Visibility With Database
[22]Generate Heap Dump
[23]Generate Thread Dump
[24]Force Backup Cancellation
[25]Configure TCP params
[0]Exit

25
This CLI allows admins to modify the TCP parameters recycle/reuse/fin_timeout
For the changes to take effect, RELOAD ISE server on modifying any of the parameter using
 the admin cli 'reload'. Until reload is done, the changes will not be persisted.
Select the option to configure/display tcp params.
                        1. tcp recycle
                        2. tcp reuse
                        3. tcp fin_timeout
                        4. display tcp param values
                        0. Exit
                        [1/2/3/4/0]: 1
Enable/Disable tcp recycle parameter? [e/d]: e
param recycle is already enabled..
Select the option to configure/display tcp params.
                        1. tcp recycle
                        2. tcp reuse
                        3. tcp fin_timeout
                        4. display tcp param values
```

```
                        0. Exit
                        [1/2/3/4/0]: 2
Enable/Disable tcp reuse parameter? [e/d]: e
param reuse is already enabled..
Select the option to configure/display tcp params.
                        1. tcp recycle
                        2. tcp reuse
                        3. tcp fin_timeout
                        4. display tcp param values
                        0. Exit
                        [1/2/3/4/0]: 3
Set tcp fin_timeout (60 default) <0-180> : 60
updated timeout param..
Select the option to configure/display tcp params.
                        1. tcp recycle
                        2. tcp reuse
                        3. tcp fin_timeout
                        4. display tcp param values
                        0. Exit
                        [1/2/3/4/0]: 4
Current values of the tcp parameters:
Recycle = ENABLED
Reuse = ENABLED
Fin_timeout = 60
Select the option to configure/display tcp params.
                        1. tcp recycle
                        2. tcp reuse
                        3. tcp fin_timeout
                        4. display tcp param values
                        0. Exit
                        [1/2/3/4/0]:
```

（注） tcp recycle および tcp reuse パラメータは、デフォルトでは無効になっています。tcp fin_timeout はデフォルトで 60 秒に設定されています。tcp fin_timeout の有効な値の範囲は 0 ～ 180 秒です。この属性を低い値に設定すると、TACACS+ のパフォーマンスが向上します。

Cisco ISE リリース 2.7.0.356 の解決済みの不具合：累積パッチ 3

次の表に、リリース 2.7 累積パッチ 3 の解決済みの不具合を示します。

パッチ 3 は古いバージョンの SPW で機能しない可能性があります。MAC ユーザーは SPW を MACOSXSPWizard 2.2.1.43 以降にアップグレードする必要があります。また、Windows ユーザーはその SPW を WinSPWizard 2.2.1.53 以降にアップグレードする必要があります。

不具合 ID 番号	説明
CSCvf61114	「認証プロファイル」に対する ERS の更新/作成で XML スキーマの検証が失敗する
CSCvg50777	nas-update=true アカウンティング属性が含まれていると、アクティブセッションが削除されない

不具合 ID 番号	説明
CSCvi27454	pxGrid サービスが実行中/無効ではなくアクティブ/スタンバイとして表示される
CSCvm47584	ポスチャリースが原因で 1 日以上の猶予期間を設定できない
CSCvn31249	GNU gettext default_add_message ダブルフリーの脆弱性
CSCvq12204	リロード後に SNMPv3 ユーザーが誤ったハッシュで追加され、SNMPv3 認証が失敗する
CSCvq44063	DNS の不正な設定により、TACACS+ または RADIUS 認証に失敗する
CSCvq48503	「ヘルスステータスが使用不可」という誤ったアラームが表示される
CSCvr22065	共有秘密キーに特殊文字（8o\v|）が含まれている場合、インポート NAD がサポートされていないエラーで失敗する
CSCvr47716	Info-ZIP UnZip ファイルの重複したサービス拒否の脆弱性 CVSS v3.0 Base 7.5
CSCvs14743	EgressMatrixCell で ERS コールを介して重複が作成される
CSCvs29611	ISE 2.4 p5 が深夜に継続的にクラッシュし、コアファイルが生成される
CSCvs38176	[信頼できる証明書（Trusted Certificate）] ウィンドウでエラーメッセージが修正される
CSCvs69726	ISE 2.2 がメモリリークの影響を受ける PORT_Alloc_Util() によってネイティブメモリが毎日 1 ～ 2% 増加する
CSCvs85273	libcurl の複数の脆弱性
CSCvs96516	複数ある Cisco Identity Services Engine のストアド クロスサイト スクリプティングの脆弱性
CSCvs98094	ISE 2.7 でファイル修復チェックが失敗する
CSCvt11179	この OS 属性が AD サーバーで変更されると、「AD-Operating-System」属性が取得されない
CSCvt18613	TEAP EAP チェーンの AD グループが一致しない認可条件
CSCvt43844	runtime-aaa デバッグでパケットの詳細が ascii で印刷されない
CSCvt50572	ERS API 経由でホワイトリストポリシーを作成できない
CSCvt53541	SMS over HTTPS でゲートウェイにユーザー名/パスワードが送信されていない

不具合 ID 番号	説明
CSCvt55312	Apple CNA を使用した ISE BYOD が 9800 で失敗する
CSCvt63119	一部の MnT 操作後に ISE 2.7 サーバーでプロセスが不足する
CSCvt64739	アプリケーションサーバーの初期化に時間がかかる
CSCvt65332	プロファイルの説明の作成中に Enter キーを使用するとエラーがスローされる
CSCvt65853	再認証用の MnT REST API が分散型展開で使用されると失敗する
CSCvt68108	ISE サーバー側の認証チェックが不十分
CSCvt81194	ポリシー HitCountCollector で CPU スパイクが観察される
CSCvt82384	diagnostics.log のローテーションが機能しない
CSCvt83547	ISE PxGrid Web クライアントが 25 を超えるサブスクライバをリストできない
CSCvt85757	スポンサーポータルで英語以外の文字が表示される
CSCvt85836	セッションキャッシュが不完全なセッションでいっぱいになる
CSCvt89098	失敗したノードのワイルドカード複製が ISE で再試行されない
CSCvt91871	ISE RADIUS アカウンティングレポートの [アカウンティングの詳細（Accounting Details）] に [データが見つかりません（No data found）] と表示される
CSCvt99349	スマートライセンスコンプライアンスステータス「リリースされた権限」に説明が必要
CSCvu01181	古い接続を削除するため、TacacsConnectionManager を拡張する必要がある
CSCvu05121	SMTP サーバーの変更後にゲスト電子メールが送信されない
CSCvu06604	[TrustSecワークセンター（TrustSec Work Center）] > [コンポーネント（Components）] > [TrustSec AAAサーバー（TrustSec AAA Servers）] ページでRADIUS ノードを参照していることがドキュメントに記載されている
CSCvu13368	CLI からの設定バックアップがエラーで失敗する
CSCvu14215	AD グループの追加/削除中にスポンサー グループ メンバーシップが削除される
CSCvu15948	TC-NAC アダプタが nexpose によるスキャンを停止した

不具合 ID 番号	説明
CSCvu19221	スポンサーポータルの設定時に、サポート情報がフローチャートに正しく表示されない
CSCvu21093	ポータルの背景が正しく表示されない
CSCvu25625	ISE が DNAC からの REST API コールに対して誤ったバージョンを返す
CSCvu25975	TACACS コマンドセットでインポートオプションが機能しない
CSCvu28305	ISE ロギングタイムスタンプに将来の日付が表示される
CSCvu29434	SNS 3655 PSN でのリロード後に ISE 2.6 パッチ 6 サービスを初期化できない
CSCvu30286	複数のマトリックスから単一のマトリックスへの移動後、ERS SGT の作成が許可されない
CSCvu31176	ISE 2.4 パッチ 11 VPN + ポスチャ：Apex ライセンスが消費されない
CSCvu31853	ERS によって追加された NDG が、データベース内のすべてのネットワークデバイスに関連付けられる
CSCvu32240	内部ユーザーの更新に ISE ERS API を実行すると、既存の ID グループ値が null に設定される
CSCvu33416	有効なライセンスでもコンプライアンス違反アラームが表示される
CSCvu33861	MAC アドレスでデバイスを取得する REST API MnT クエリに 2 秒以上かかる
CSCvu33884	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCvu34433	isehourlycron.sh cron スクリプトに従って Undo テーブルスペースの空き領域がクリアされない
CSCvu34895	レポートリポジトリのエクスポートが専用 MnT ノードで機能しない
CSCvu37873	不明な NAD アラームの詳細をクリックするとエラーが表示される
CSCvu39653	MAC アドレスのセッション API が「Char 0x0 out of allowed range」というエラーを返す
CSCvu41815	承認プロファイルが異なる SG の同じ VN にマッピングされている場合、SG から VN を削除すると GBAC 同期が中断する
CSCvu45697	システム内の messages.x ファイルの圧縮
CSCvu47395	ハイメモリの問題があるシステムには Drop_Cache が必要

不具合 ID 番号	説明
CSCvu48417	ISE ERS API DELETE デバイスが複数のコールでエラー 500 を返す
CSCvu49019	Elasticsearch での疑わしいメモリリーク
CSCvu53836	ISE 承認のみの要求が内部ユーザーグループに対して評価されない
CSCvu55332	REST API コールで、ポリシーセットで参照されているネットワーク デバイス グループを削除できる
CSCvu55557	NAD の作成に REST API を使用する場合、RADIUS シークレットの最小文字要件がチェックされない
CSCvu58476	ID ストアの問題を示す際の My Device ポータルにおけるエラーメッセージの改善
CSCvu58793	ロケーション別フィル処理のオプションが使用されていると、 ERS REST API が重複する値を複数回返す
CSCvu58892	ISE GUI のすべてで「マスターゲストレポート」を「プライマリゲストレポート」に更新
CSCvu59093	セッションデータベースの列が欠落している
CSCvu59491	ISE が insiteVM（tc-nac サーバー）に新しいサイトを作成する
CSCvu63642	コンテキストの可視性により、ユーザー名の更新時にエンドポイントパラメータが融合される
CSCvu68700	無効なクレデンシャルを持つ XML または JSON 要求に対する ERS API 応答が、予期しない HTML body タグを含む HTTP 401である
CSCvu70683	ERS クエリでは、iselocalstore.log での抑制とともにアラーム抑制が必要
CSCvu70768	アラームとシステムの概要が ISE GUI に表示されない
CSCvu73387	「12308 クライアントはTLVが失敗を示す結果を送信した（12308 Client sent Result TLV indicating failure）」というエラーによる失敗の認証
CSCvu74198	LDAP および ODBC ID ストア名にハイフンを使用できない
CSCvu84773	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCvu87742	ACI が ISE で SXP 統合用に設定されている場合、サードパーティ証明書を使用すると認証に失敗する
CSCvu87758	ゲストパスワードポリシー設定がアルファベットまたは数字で設定されていると保存できない

不具合 ID 番号	説明
CSCvu90107	ISE ではすべてのバージョンの ERS フローでのデバイス ID の重複が許可される
CSCvu90703	CLDAP スレッドがハングし、無限に実行している
CSCvu90761	ISE の [Radiusライブセッション（Radius Live Sessions）] ページで [データが見つかりません（No Data Found）] と表示される
CSCvu91039	ISE 2.6 パッチ 7 が MAC リスト内のすべての MAC アドレスのルックアップを行わず、リダイレクトなしのポスチャが失敗する
CSCvu91601	ISE 認証ステータス API のコール期間が期待どおりに機能しない
CSCvu94025	ISE が syslog ターゲットに対してのみ IP を許可するか、DNS キャッシングを提供する
CSCvu94733	不正なパスワードに対して「アカウントはまだアクティブではありません（Account is not yet active）」というメッセージが表示され、ゲスト認証が失敗する
CSCvu97657	エンドポイントのデバッグを有効にすると、アプリケーションサーバーが初期化状態になる
CSCvv00377	サブネットと IP 範囲を使用しているネットワークデバイスの重複
CSCvv00951	停止状態への移行中にアプリケーションサーバーがクラッシュする
CSCvv01681	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCvv04416	エンドポイントデータがセカンダリ管理ノードに表示されない
CSCvv07049	ODBC ID ソースに接続できない
CSCvv08466	ログ収集エラーアラームが ISE ダッシュボードに繰り返し表示される
CSCvv08784	ISE 2.4 パッチ 12 のバックアップを復元できない
CSCvv08885	Cisco Identity Services Engine の権限昇格の脆弱性
CSCvv09910	CSCvr96003 の修正にもかかわらず SYSAUX テーブルスペースが満杯である
CSCvv10572	2.4 パッチ 13 で ISE に IND を登録できない
CSCvv10683	ドロップされたセッションのセッションキャッシュがクリアされず、PSN で高い CPU 使用率が発生する
CSCvv14001	認証プロファイルが適切な属性で保存されない

不具合 ID 番号	説明
CSCvv15811	IP アドレスが割り当てられたシャットダウン インターフェイスがある場合、ISE TCP ポート 84xx が開かない
CSCvv18317	データベース内の無効なオブジェクト
CSCvv23256	ISE 認証ステータス API コールが、指定された時間範囲のすべてのレコードを返さない
CSCvv25102	ISE で TACACS+ および TCP を強化するための TCP 設定の変更
CSCvv26811	[暗号キーを使用したエクスポート（Export with Encryption Key）] オプションの使用後、暗号キーを使用しないポリシーのエクスポートが正しく動作しない
CSCvv27690	HTTPS、EAP、DTLS、および PORTAL の ISE 証明書を更新すると、PORTAL および Admin ロールのみが適用される
CSCvv29190	iOS 14 beta で BYOD フローが破損している
CSCvv30133	ディスカバリホストの説明テキストが紛らわしい
CSCvv30226	Livelog セッションで、VPN ポスチャシナリオに誤った認証ポリシーが表示される
CSCvv35921	内部 ID ストアで選択したユーザーの CSV エクスポートを開始できない
CSCvv36189	無効な IPv6 アドレスが原因で RADIUS に認証済みライブログが送信されない
CSCvv38249	カスタムポートのみが有効な場合、手動 NMAP が動作しない
CSCvv39000	LANDESK のポスチャ条件を作成できない
CSCvv39584	ISE 2.6 および 2.7 パッチブランチから ojdbc8 jar を削除
CSCvv41935	キーに <or> 記号が含まれている場合、PSK cisco-av-pair がエラーをスローする
CSCvv42857	ISE の MAC 11.x およびそのマイナーバージョンサポートが使用できない
CSCvv43558	Apache Struts Aug20 の脆弱性に対する ISE の評価
CSCvv45063	ノードが展開から削除されたときに内部 CA 証明書が削除されない
CSCvv46034	Tacacs 設定の更新中にデバイス管理サービスが無効になる
CSCvv46958	NDG 列が 255 文字を超えると、TrustSec が有効な NAD が TrustSec マトリックスに表示されない

不具合 ID 番号	説明
CSCvv47849	Cisco DNA Center で SG 名が変更された場合、マッピングされた SGT エントリが認証ルールからクリアされる
CSCvv48544	ISE で NIC チーミングが有効になっていると、ヘルスチェックが機能しない
CSCvv49403	8084/TCP EST サービスにより、脆弱で非 FIPS 準拠の暗号化が可能
CSCvv50028	ISE ノードのリセット設定後にヒープダンプの生成が失敗する
CSCvv50721	Aruba ダイナミック URL リダイレクトを使用して NetworkSetupAssistant.exe のダウンロードリンクを取得できない
CSCvv52637	ISE ホットスポット ゲスト ポータル フローが破損している
CSCvv53221	ISE_EST_Local_Host の RADIUS 共有秘密が見つからない場合、ISE アプリケーションサーバーが初期化状態になる
CSCvv54761	現在アクティブなセッションレポートのエクスポートには、午前 0 時以降に更新されたセッションのみが表示される
CSCvv54798	CLI からエクスポートされたコンテキストの可視性の CVS に IP アドレスが表示されない
CSCvv55663	ISE ノードのリロード後に ISE 2.6/2.7 リポジトリが削除される
CSCvv57628	一時停止されたゲストユーザーがエンドポイントグループから自動的に削除されない
CSCvv57639	TACACS コマンドセットでカッコ付きのコマンドを保存するとエラーが発生する
CSCvv57830	コンテキストに空の値が追加され、グループの検索に失敗する
CSCvv58629	EST サービスを初期化する認証局サービスが ISE 2.7 パッチ 2 へのアップグレード後に実行しない
CSCvv59233	ISE RADIUS ライブログの詳細で、[その他の属性（Other Attributes）] セクションに AD グループ名がない
CSCvv60686	ISE SXP にはセッションから学習した古いマッピングをクリアするメカニズムが必要
CSCvv60923	内部ユーザーのカスタム属性の IP データ型にスラッシュを使用する機能が必要
CSCvv62382	プロキシバイパス設定で大文字を使用できない
CSCvv62549	エンドポイントの GUI ページに Clinda のカスタム属性が表示されない

不具合 ID 番号	説明
CSCvv62729	存在しないネットワークデバイスを照会すると、ネットワークデバイス API コールがエラー 500 をスローする
CSCvv64190	ユーザー ID グループで大文字と小文字が区別されると、[スポンサーグループメンバーの選択（Select Sponsor Group Members）] ウィンドウがロードされない
CSCvv67051	[RADIUSサーバー順序（RADIUS Server Sequences）] ページに「no data available（使用可能なデータがありません）」と表示される
CSCvv67743	状態別ポスチャ アセスメント レポートに、状態ステータスフィルタなしのデータが表示される
CSCvv67935	認証プロファイルのセキュリティグループの値が取得直後に表示されない
CSCvv68028	AUP テキストを変更できない
CSCvv72306	スイッチ/ルータ CLI を介して ISE 内部ユーザーパスワードを変更した後、パスワード監査が生成されない
CSCvv74373	ISE 3.0 DNS 解決可能性の誤アラーム
CSCvv77530	バインドパスワードで % 文字が 2 回以上使用されている場合、LDAP グループ/サブジェクト属性を取得できない
CSCvv77894	アップグレードおよびデータベースでの偏向のないテキスト/コード
CSCvv80113	ISE ポスチャ自動更新が実行されていない
CSCvv82806	ネットワークデバイス IP フィルタがサブネット内の IP と一致しない
CSCvv91007	接続に失敗すると、[スマートライセンスの権限付与（Smart Licensing Entitlement）] タブが [更新（Refreshing）] でスタックする
CSCvv91234	プライマリ MnT ノードがダウンしていると、ISE 2.6 のスケジュール済みレポートが機能しない
CSCvv91684	ISE コレクションフィルタが GUI に表示されない
CSCvv92203	「Employees」という名前で SGT を作成しようとすると「入力された名前の NetworkAuthZProfileが存在します（NetworkAuthZProfile with entered name exists）」というエラーメッセージが表示される。
CSCvv94791	DNAC と ISE の間で GBAC 設定を同期できない
CSCvw00375	ISE 2.7p2 のカスタムビューの [コンテキストの可視性（Context Visibility）] ページをロードできない

不具合 ID 番号	説明
CSCvw01225	ISE Config Restore が 40% で失敗し、「IMPDPを使用したDBの復元が失敗しました（DB Restore using IMPDP failed）」というエラーメッセージが表示される
CSCvw01829	Chrome 85/86で ISE GUI ログインページに次のエラーが表示される：問題が発生しました（Something went wrong）
CSCvw08330	サードパーティの NAD のダイナミック リダイレクションでポスチャが機能しない
CSCvw08765	アップグレードライセンスのチェックでは、スマートライセンス登録の ISE データベースが確認される
CSCvw19706	ISE のタイムゾーンがアメリカ/サンティアゴに設定されていると、オフライン/オンラインフィードが失敗する
CSCvw19785	外部データソースポスチャ条件の編集中に正しい AD が表示されない
CSCvw20021	NAD の場所が [コンテキストの可視性のエラスティック検索（Context Visibility ElasticSearch）] で更新されない
CSCvw20636	NAD プロファイルが削除されると、認証プロファイルに「No data available（データがありません）」と表示される
CSCvw24227	例外が原因でエンドポイントが消去されない
CSCvw25615	ISE TACACS ロギングタイムスタンプに将来の日付が表示される
CSCvw28441	API の使用中に NAD の共有秘密がログに表示される
CSCvw36743	パスワードに特殊文字を使用すると、ISE サービスアカウントがロックされ、WMI が確立されない
CSCvw38853	MAC OSX のマルウェア対策条件に Sophos 10.x の定義がない
CSCvw54878	日本語 GUI に 50 以上のルールがある場合、認証ポリシーが正しく表示されない
CSCvw56938	スマートライセンスが有効になっていない場合でも SCH 接続が試行される
CSCvw59855	影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要がある

Cisco ISE 2.7 パッチ 3 の既知の制限事項

SNMP ユーザーパスワード形式と SNMP ハッシュの最小長の変更

Cisco ISE 2.7 パッチ 3 の適用後、SNMP ユーザーパスワード形式の変更により、SNMP ユーザー設定が削除される可能性があります。SNMP ユーザーパスワードはハッシュ形式で表示されるようになりました。SNMP ユーザー設定をもう一度再設定する必要があります。

80 文字未満の SNMP ハッシュは機能せず、次のエラーが表示されます。

```
snmp-server user FT10 v3 hash fe7c35f09ff1238e369968a0be273f22
fe7c35f09ff1238e369968a0be273f22
          % Error: Decryption Failed. Could not add SNMP User
```

[名前（Name）] および [説明（Description）] フィールドでの特殊文字の使用に関する制限

- TACACS+ プロファイルおよびデバイス管理ネットワーク条件の [説明（Description）] フィールドでは、特殊文字 [%\<>*^:"|',=/()$.@;&-!#{}.?] は使用できません。サポートされる文字は、英数字、アンダースコア（_）、およびスペースです。
- 認証プロファイルの [名前（Name）] および [説明（Description）] フィールドでは、特殊文字 %\<>*^:\"|',= は使用できません。[名前（Name）] および [説明（Description）] フィールドでサポートされる文字は、英数字、ハイフン（-）、ドット（.）、アンダースコア（_）、およびスペースです。
- 時刻と日付の条件の [名前（Name）] および [説明（Description）] フィールドでは、 特殊文字 [%\#$&()~+*@{}!/?;:',=^`]"<>" は使用できません。[名前（Name）] および [説明（Description）] フィールドで サポートされる文字は、英数字、ハイフン（-）、ドット（.）、アンダースコア（_）、およびスペースです。

Cisco ISE リリース 2.7.0.356 の新機能：累積パッチ 2

ユーザー定義ネットワーク

ユーザー定義ネットワークは、Cisco DNA Center ソリューションです。ユーザー定義ネットワークは、ホットフィックスを通じて Cisco ISE リリース 2.7 パッチ 2 でサポートされます。エンドユーザーは、ユーザー定義ネットワークを使用してプライベートネットワークまたはユーザー定義ネットワークルームを作成し、自分のパーソナルデバイスをグループ化できます。

たとえば、ネットワーク内でユーザー定義ネットワークが有効になっている大学寮の学生は、自分のデバイスを登録して、個人のユーザー定義ネットワークルームに追加できます。

ユーザー定義ネットワークのエンドユーザーは、他のユーザーを招待し、自分のデバイスを一時的にユーザー定義ネットワークルームに持ち込むことができます。その逆も同様です。

ユーザー定義ネットワークを有効にするには、Cisco ISE をオンプレミスの Cisco DNA Center アカウントに追加する必要があります。

Cisco ISE 管理者ポータルから Cisco ISE と Cisco DNA Center の統合を検証します。**[管理（Administration）] > [pxGridサービス（pxGrid Services）] > [すべてのクライアント（All**

Clients）] を選択します。**[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）]**を選択します。Cisco DNA Center が pxGrid クライアントのリストに表示されます。

ユーザー定義ネットワークソリューションが有効になっている場合、Cisco DNA Center クラウドは、ネットワーク上のすべてのユーザー定義ネットワーク登録デバイスの設定情報を、Cisco ISE に自動的に送信します。この設定情報には、各デバイスが存在しているユーザー定義ネットワークルームに関する情報が含まれます。

Cisco ISE は、ユーザー定義ネットワークソリューションの一部として設定されているシスコワイヤレス LAN コントローラ（WLC）とこの情報を共有します。この共有は、Cisco ISE と接続された Cisco WLC 間の通常の RADIUS プロトコル交換の一部として実行されます。

ユーザー定義ネットワークによる Cisco ISE のプロファイリングとロギングの変更については、該当するリリースの『Cisco ISE 管理者ガイド』を参照してください。関連するプロファイリングの変更については「セグメンテーション」の章を、関連するロギングの変更については「トラブルシューティング」の章を参照してください。

Cisco ISE リリース 2.7.0.356 の解決済みの不具合：累積パッチ 2

次の表に、リリース 2.7 累積パッチ 2 の解決済みの不具合を示します。

パッチ 2 は古いバージョンの SPW で機能しない可能性があります。MAC ユーザーは SPW を MACOSXSPWizard 2.2.1.43 以降にアップグレードする必要があります。また、Windows ユーザーはその SPW を WinSPWizard 2.2.1.53 以降にアップグレードする必要があります。

不具合 ID 番号	説明
CSCuo02920	ISE が access-reject で設定済みの Radius AVP 18 を返さない
CSCvb55884	ISE RBAC ネットワークデバイスタイプ/ロケーションビューが機能しない
CSCvd38796	AD が authC と authZ の両方に使用されている場合、RA-VPN/CWA に対して AD ドメイン属性が取得されない
CSCvh77224	ENH // HTTPS プロキシを使用したスマートライセンスの登録が失敗する
CSCvi35647	マルチノード展開では、ポスチャセッション状態を PSN 間で共有する必要がある
CSCvi62805	CSCvi62805 ISE ODBC が設定されたストアドプロシージャに従って MAC アドレスを変換しない
CSCvj47301	ノードグループメンバーが到達不能の場合、ISE はアクティブ準拠のセッションに CoA を送信する
CSCvm62775	ISC BIND krb5-subdomain と ms-subdomain のアップデートポリシーの脆弱性
CSCvn12644	AD 属性のポリシー評価中に ISE がクラッシュする

不具合 ID 番号	説明
CSCvn50531	tcpdump print_prefix 関数スタックベースのバッファオーバーリードの脆弱性
CSCvn73729	脅威イベントのパブリッシュ中にエラーが発生した：AMP アダプタ
CSCvn73740	エンドポイントプロファイルが不明に設定されていない EAP-TLS 認証は、2 番目の認証で失敗する。
CSCvo28970	Cisco 経時的エージェントを使用すると、AnyConnect に Cisco NAC エージェントエラーが表示される
CSCvp17458	libssh2 SSH_MSG_CHANNEL_REQUEST パケット処理が領域外メモリ参照の...
CSCvp59038	ISE セカンダリ PAN ノードが送信元アドレス 169.254.2.2 で RST を他の ISE ノードに送信する
CSCvp85813	TACACS ライブログの特定のネットワークデバイス IP アドレスによるフィルタ
CSCvp93322	有効期限テスト中に MNT でメモリが大幅に増加する
CSCvq13431	ポスチャと RADIUS フロー中、コンテキスト属性を取得している間に ISE PSN ノードがクラッシュする
CSCvq43600	PSN ペルソナが無効になっていても、TACACS ポート 49 が開いたままになる
CSCvq48396	レプリケーション失敗アラームが生成され、ise-psc.log に ORA-00001 例外が表示される
CSCvq61089	SAML 認証を使用した BYOD オンボーディング後、デバイスポータルにデバイスが表示されない
CSCvq73677	GNU パッチ OS シェル コマンド インジェクションの脆弱性
CSCvq86746	jquery の複数の脆弱性 - ゲストポータル
CSCvq90601	EAP チェーン：動的属性値が使用できない
CSCvr07294	RADIUS 認証と RADIUSアカウントレポートのパフォーマンスが遅い
CSCvr09749	GNU パッチ do_ed_script OS シェルコマンドの実行の脆弱性
CSCvr47732	FasterXML jackson-databind ポリモーフィック型入力の脆弱性 CVSS v3.1 Base：9.8
CSCvr56785	大きなコアファイルに対応するためにローカルディスクサイズを拡大する必要がある

不具合 ID 番号	説明
CSCvr61108	セッション ID に対する PxGrid ANC API のサポート
CSCvr68432	REST を介して追加された 2.4P10 エンドポイントには「編集」モードでのみポリシーの割り当てが表示される
CSCvr68971	ISE IP ルーティングの優先順位の問題
CSCvr77676	libmspack chmd_read_headers 関数サービス妨害の脆弱性
CSCvr81384	ネットワークデバイスの CSV インポートが失敗し、理由なくサイレントにプロセスが中止される
CSCvr85513	PSN でコアファイルが生成される
CSCvr87373	ACI マッピングは SXP pxGrid トピックにパブリッシュされない
CSCvs05260	App server と EST サービスが毎朝 1 時にクラッシュ/再起動する
CSCvs09981	ISE のグループノード間の MAR キャッシュチェックが原因で失敗した COA を除外する機能を追加する
CSCvs25569	無効なルート CA 証明書が受け入れられた
CSCvs38883	古いデータをプッシュする TrustSec マトリックス
CSCvs39880	Xms 値を持つ Mnt ノードの高負荷
CSCvs40406	信頼できる CA 証明書の削除中に SEC_ERROR_BAD_DATABASE がシステム/アプリデバッグログに表示される
CSCvs44006	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCvs44795	ISE が SGT を正しく更新しない
CSCvs46399	URL リダイレクトの AuthZ プロファイルの詳細プロファイルでカスタム HTTPS 宛先が許可されない
CSCvs47941	ISE2.6 で内部 CA とキーをインポートできない
CSCvs51519	NFS マウントが原因でクラッシュする
CSCvs53606	ISE 2.4：管理者ログインレポートが証明書ベースの管理者認証を使用すると認証に失敗する
CSCvs55464	スポンサーポータルで新しいユーザーを作成すると、「無効な入力（invalid input）」が表示される
CSCvs62081	コレクタログが pxgid および dnac メッセージとともにダンプされる

不具合 ID 番号	説明
CSCvs62586	REST API を使用すると Tacacs プロファイルが正しく取得されない
CSCvs62597	認証プロファイルが REST API を使用して正しくプルされていない（改ページがない）
CSCvs67785	セルフ登録ポータルのポータルページのカスタマイズで、日数が更新されない
CSCvs70997	ISE：SCEP RA の設定時に 2.4p9 CA 中間証明書がインストールされない
CSCvs75274	「証明書プロビジョニングポータル」のポータルカスタマイズを実行できない
CSCvs78160	INetworkAuthZCheck の ConditionsData 句で URT が失敗する
CSCvs79836	期限切れの証明書が削除対象としてリストされていない
CSCvs82557	SXP バインディングが pxGrid 2.0 クライアントに公開されない
CSCvs83303	中間更新が DB に保存されていない場合、API がデータを取得しない
CSCvs85970	AD join-point に文字列「TACACS」があると、AuthZ 条件で AD joinpoint が表示されない
CSCvs86344	ゲストユーザー名に @ 記号（guest@example.com）が含まれていると、ISE 2.4 Guest ERS Call Get-By-Name が失敗する
CSCvs86686	パッチの複数の脆弱性
CSCvs86697	sudo の複数の脆弱性
CSCvs86775	ISE 2.6 インストール：検証の入力 - IP ドメイン名の確認
CSCvs88222	パッケージ展開の脆弱性 - RHEL 7
CSCvs88368	ハッシュパスワードを使用すると ISE SNMP サーバーがクラッシュする
CSCvs91808	特殊文字を含むメタデータ XML ファイルをインポートすると、サポートされていないタグエラーが発生する
CSCvs96541	OP バックアップの復元後に TACACS の認証/アクセスレポートが表示されない
CSCvs97302	.dmp ファイルが ISE の reset-config の後でも /opt/oracle/base/admin/cpm10/dpdump から削除されない
CSCvs98602	X.Org libX11クライアント セグメンテーションの障害によるサービス拒否の脆弱性

不具合 ID 番号	説明
CSCvs98604	X.Org libX11 オフバイワンメモリ書き込みで任意のコードが実行される脆弱性
CSCvt00283	ゲストスポンサーポータルの成功ページ更新時の 404 エラー
CSCvt01161	NMAP：ISE のバージョン 2.6 で MCAFeeEPROOrchestratorClientscan を実行できない
CSCvt03094	ISE の期限切れの tacacs セッションがセッションキャッシュからタイムリーにクリアされない
CSCvt03292	Cert Revoke と CPP が APEX ライセンスなしで機能しない
CSCvt03935	TrustSec ポリシーマトリックス -- ISE の [表示（View）] オプションの表現を変更する
CSCvt04047	バックアップ/復元メニューに移動した後、すべての ISE ページで POST getBackupRestoreStatus が発生する
CSCvt04144	アラーム設定での高ディスク使用率のしきい値オプションがない
CSCvt05201	トンネルグループポリシー評価によるポスチャが Java Mem を減らしている
CSCvt07230	ISE がインポート時にイーグレスポリシーで ANY を許可しない
CSCvt08143	ISE 2.6 の時差
CSCvt10214	[ENH] ネットワークデバイスの API を使用して「GET|PUT|DELETE by Name」機能を追加する
CSCvt11366	CLI からエンドポイントをエクスポートすると Java の例外が発生する
CSCvt12236	IP SGT スタティックマッピングのインポートがホスト名で正しく動作しない
CSCvt13198	FasterXML jackson-databind xbean-reflect/JNDI のブロッキングの脆弱性
CSCvt13707	pxGrid 2.0 WebSocket 分散アップストリーム接続の問題
CSCvt13719	pxGrid 2.0 WebSocket ping pong がアイドル状態のスタンドアロンでも遅すぎる
CSCvt13746	追加の authz ポリシーと例外がある場合、ISE はすべてのデバイス管理 authz ルールを表示しない
CSCvt14248	EST サービスを初期化する認証局サービスが ISE 2.6 へのアップグレード後に実行しない

不具合 ID 番号	説明
CSCvt15787	TCPDump：ノードとインターフェイスフィールドが使用できない
CSCvt15893	ISE 2.6 へのアップグレード後、エラーサプリカント/不良構成サプリカントの Radius テーブルが存在しない
CSCvt15935	システムサマリーダッシュボードと一致する高負荷アラームが一部のノードに表示されない
CSCvt16882	Apple CNA と AUP をリンクとして使用して iPad にアクセスすると、400 Bad 要求エラーが発生する。
CSCvt17335	WMI と REST を同時に使用すると Pxgrid でバッチロジックをパブリッシュする
CSCvt17783	ISE では、SGT のインポートまたはエクスポートで ANY SGT または値 65535 を公開できない
CSCvt19657	多数のエンドポイントが存在する場合、ISE ERS API エンドポイントの更新が遅い
CSCvt24276	許可された値をシステム使用ディクショナリへの 7 つ以上の属性に追加/変更できない
CSCvt25610	ISE2.7 コンプライアンスカウンタが 0 になっている
CSCvt26108	ISE 2.7 の Anyconnect の設定の遅延アップデートが保存されない
CSCvt31275	アップグレードされたセットアップで upscsnconfig テーブルに 2 つの行が作成される
CSCvt35044	EP ルックアップに時間がかかり、ゲストフローの遅延が大きくなる
CSCvt36117	アイデンティティグループが ISE の内部ユーザーを更新する
CSCvt36322	リダイレクト値が URL に存在する場合、ISE 2.6 MDM フローが失敗する
CSCvt37910	[ENH] /ers/config/internaluser の API を使用して「GET|PUT|DELETE by Name」機能を追加する
CSCvt38308	ISE：min pwd の長さを増やすと、既存の短い pwd の GUI を使用したログインがエラーなしで失敗する
CSCvt40534	MNT ノード選択プロセスが適切に設計されない
CSCvt46850	すでに作成されている複合条件の場合、それらの条件を変更できない
CSCvt49961	FQDN を使用して設定された Syslog ターゲットによってネットワークが停止する可能性がある

不具合 ID 番号	説明
CSCvt57571	IP-access がエントリなしで送信された場合、App-server がクラッシュする
CSCvt57805	REST API 更新操作の断続的なパスワードルールエラー
CSCvt61181	ISE ERS API：SNMP 設定の処理中のネットワークデバイスの GET コールが遅い
CSCvt69912	ISE が誤検出アラーム「アラーム：パッチ障害（Alarms：Patch Failure）」を生成する
CSCvt69941	ISE 2.6 の冗長アラーム「アプリケーションパッチのインストールが正常に完了しました（Application patch install has completed successfully" Alarm）」
CSCvt70689	MAR キャッシュレプリケーションが有効になっていると、アプリケーションサーバーがクラッシュすることがある
CSCvt71355	pxGrid で INIT 状態のユーザーを削除できない
CSCvt71559	アラームダッシュレットに「データが見つかりません（No Data Found）」と表示される
CSCvt73927	パッチ 1 のインストール後に ISE 2.7 証明書認証サービスが無効になる
CSCvt73953	CLI エクスポートとコンテキストの可視性の情報が一致しない
CSCvt80285	定義用のマルウェア対策条件の作成時にすべての製品を個々に選択できない
CSCvt85722	動作していない MNT ウィジェットのデバッグログがない
CSCvt87409	ISE DACL 構文チェックで IPv4 形式エラーが検出されない
CSCvt93117	ise-psc.log が「TTConnection のチェックが有効です（check TTConnection is valid）」でいっぱいになり、関連するログがロールオーバーする
CSCvt96594	ISE 2.6：ERS を介した外部スポンサーユーザーを使用したゲストユーザーの作成が 401 Unauthorized Error で失敗する
CSCvu03572	ISE UI で upn.log をアップロードに使用できない
CSCvu05164	ISE で、NAD の Radius を API を使用して無効にできない
CSCvu10009	req 格納ファイルの /ers/config/internaluser/name/{username}makes id&password&name mandatory の PUT verb
CSCvu26008	ポータルページのカスタマイズの変更が証明書プロビジョニングポータルに反映されない
CSCvu32865	ISE 2.7 で CPU 使用率が高く、認証遅延が発生する

不具合 ID 番号	説明
CSCvu39890	ISE：ロールバックがパッチ 12 からのロールバックを無期限に試行する
CSCvu42244	EAP-TLS を介したマシン認証が、ユーザーが見つからないというエラーを示して許可フロー中に失敗する
CSCvs42441	SMS と LDAP ページでサーバーから返されたサービス アカウント パスワード

Cisco ISE リリース 2.7.0.356 の新機能：累積パッチ 1

マルチ DNAC のサポート

Cisco DNA Center システムは、25,000 ～ 100,000 のエンドポイントの範囲を超えて拡張できません。Cisco ISE は 200 万エンドポイントまで拡張できます。現在、1 つの Cisco DNA Center システムと 1 つの Cisco ISE システムのみを統合できます。大規模な Cisco ISE 展開では、複数の DNA Center のクラスタを 1 つの Cisco ISE に統合することでメリットが得られます。シスコは、Cisco ISE 展開ごとに複数の Cisco DNA Center のクラスタ（マルチ DNAC とも呼ばれる）をサポートするようになりました。

ビジネス成果：Cisco DNA Center のアクセス制御アプリケーションのこの機能を使用すると、1 つの Cisco ISE システムに最大 4 つの Cisco DNA Center クラスタを統合できます。

Cisco AI エンドポイント分析サポート

Cisco AI エンドポイント分析は、エンドポイント プロファイリングの忠実度を改善する Cisco DNA Center のソリューションです。きめ細かいエンドポイント識別を提供し、さまざまなエンドポイントにラベルを割り当てます。ディープ パケット インスペクション、および Cisco ISE、Cisco SD-AVC、ネットワークデバイスなどのソースからのプローブによって収集された情報は、エンドポイント プロファイリングのために分析されます。

Cisco AI エンドポイント分析は、人工知能と機械学習機能を使用して、同様の属性を持つエンドポイントを直感的にグループ化します。IT 管理者は、これらのグループを確認してラベルを割り当てることができます。割り当てられたエンドポイントラベルは、Cisco ISE アカウントがオンプレミスの Cisco DNA Center に接続されている場合、Cisco ISE で使用できます。

Cisco AI エンドポイント分析の結果割り当てられたエンドポイントラベルは、Cisco ISE 管理者がカスタム認証ポリシーを作成するために使用できます。それらの認証ポリシーを使用して、エンドポイントまたはエンドポイントグループに適切なアクセス権限のセットを提供できます。

Cisco ISE リリース 2.7.0.356 の解決済みの不具合：累積パッチ 1

次の表に、リリース 2.7 累積パッチ 1 の解決済みの不具合を示します。

パッチ 1 は古いバージョンの SPW で機能しない可能性があります。MAC ユーザーは SPW を MACOSXSPWizard 2.2.1.43 以降にアップグレードする必要があります。また、Windows ユーザーはその SPW を WinSPWizard 2.2.1.53 以降にアップグレードする必要があります。

不具合 ID 番号	説明
CSCuz18895	CoA REST API が ASA VPN セッションで動作していない
CSCve89689	MNT API が特殊文字をサポートしない
CSCvf59076	ライブセッションに、VPN+ポスチャのシナリオの不正な認証プロファイルと認証ポリシーが表示される
CSCvj67437	procps-ng の複数の脆弱性
CSCvk50684	ホスト名の変更後に証明書を削除できない
CSCvo22887	ISE 2.4 URT は、ノードがサポートされているアプライアンス上にあることを確認しない
CSCvo49755	CLI clock timezone コマンドを有効にする
CSCvo87602	バージョン 2.4.44 を実行している openldap rpm を使用した ISE ノードでのメモリリーク
CSCvp07591	UTF-8 検証チェックの失敗により、EAP-GTC マシン認証がパスワードの不一致で失敗する
CSCvp24085	セカンダリ管理者ノードの ISE 2.4 の CPU 使用率が高い
CSCvp73335	calling-station-id に CLIENTVPN が含まれている場合、Radius セッション詳細レポートが破損する
CSCvp88443	新しい論理プロファイルが認証ポリシーの例外で使用されている場合でも、ISE CoA が送信されない
CSCvq11008	ISE OCSP 応答側証明書の更新のデータが設定変更監査レポートに表示されない
CSCvq60564	「既知のゲストを通知（Notify Known Guests）」の自動電子メールに「インポートされたゲストを通知（デスクトップのみ）（Notify Imported Guests (Desktop only)）」というテキストが使用される
CSCvq61878	CVE-2018-20685 の ISE の評価
CSCvq85414	iOS CNA ブラウザでリンクが機能しない場合のログインページ AUP
CSCvr12350	ISE：「MDM：MDM サーバーへの接続に失敗しました（MDM: Failed to connect to MDM server）」というログエントリにエンドポイント情報を含める必要がある

不具合 ID 番号	説明
CSCvr13481	ISE ERS SDK NetworkDeviceGroup の削除で ID の場所が指定されない
CSCvr25197	UCP を使用してパスワードを変更した後、「ユーザー変更パスワードの監査（User change password audit）」レポートに「ID（Identity）」がない
CSCvr35719	すべての tenable アダプタリポジトリを取得できない
CSCvr39943	脅威イベントに対するアクションの空白のコースが CTA クラウドから TC-NAC アダプタに受信された
CSCvr40359	ISE がエンドポイントデータベースで device-public-mac 属性を使用していない
CSCvr40545	秘密キーの暗号化に失敗したときに、共有暗号がないため EAP-FAST 認証に失敗した
CSCvr40574	秘密キーの暗号化で ISE GUI にエラーメッセージがあったときに、ISE GUI でエクスポートに失敗した
CSCvr43077	Day0：iPad OS 13.1 BYOD フローが失敗した
CSCvr44495	pxGrid アラブ銀行の防御コードの変更
CSCvr48101	予期しない COA が SCCM MDM で観測される場合がある
CSCvr51959	ISE 2.4 の fqdn 全体ではなく文字のフラグメントが一致する
CSCvr57378	DHCP メッセージによってエンドポイントがアクティブとしてマーキングされるため、アクティブなエンドポイント数が増加する
CSCvr60339	[カウンタの有効期限（Counter time limit）] タブの [最大セッション数（Max Sessions）] ページに入力ミスがある
CSCvr62517	ISE 2.4 p9 セッションディレクトリの書き込みに失敗した：文字列インデックスが範囲外：-1
CSCvr63504	システム証明書を参照しているため、SCEP プロファイルを削除できない
CSCvr67988	ゲストのパスワードの表示/印刷が無効になっている場合でも、ISE スポンサーの電子メールが CC される
CSCvr70044	高負荷時に ISE ポスチャモジュールに「ポリシーサーバーが検出されません（No policy server detect）」が表示される
CSCvr70581	RADIUS 認証詳細レポートに Called-Station-ID がない
CSCvr71796	SCCM フローに SCCMException と表示され、MDMServerReachable 値が MDMServersCache に false として ISE 更新される

不具合 ID 番号	説明
CSCvr81522	McAfee や Symantec など、一部の AM 製品の定義日が誤表示される
CSCvr83696	ISE：アカウント OU の変更後、キャッシュ済みの AD OU を新しい OU よりも優先させる
CSCvr84143	ISE ゲスト OS で tzdata を更新する必要がある
CSCvr84753	ISE 2.2 パッチ 14 AD ステータスが「更新しています...（updating ..）」と表示され、プロセスがハングしていることを示す
CSCvr84978	ISE：LDAP バインドテストでは、ノードごとに定義されている場合は正しいサーバーが使用されない
CSCvr85363	ユーザー API による ISE アプリのクラッシュ
CSCvr87936	有効な Base ライセンスと Plus ライセンスのコンプライアンス違反が表示される
CSCvr90773	ライブログの「5436 通知 RADIUS：RADIUSパケットはすでにプロセスにあります（5436 NOTICE RADIUS: RADIUS packet already in the process）」というメッセージに誤ったユーザー名が表示される
CSCvr92420	非同期 HTTP クライアントの不正な入力検証の脆弱性
CSCvr95948	接続の切断後に ISE が外部 syslog 接続を再確立できない
CSCvr96003	SYSAUX テーブルスペースが AWR および OPSSTAT データでいっぱいになる
CSCvr98395	IP ベースのプロファイルポリシーのプロファイル CoA が送信されない
CSCvs01949	ISE メッセージングサービスが basic_cancel という理由でキューリンクエラーのアラームをトリガーする
CSCvs02166	API コールが GUI として異なる結果を表示する
CSCvs03195	最大セッションカウンタの有効期限オプションが機能しない
CSCvs03810	ユーザーの入力が 2 回異なると、ISE は RADIUS レポートに正しいユーザーを表示しない
CSCvs04433	ISE：TACACS：TACACS+ の PSN クラッシュ
CSCvs05104	エンドポイントのデフォルトの間隔を無効にすると、最大時間フレームが 60 分に設定される
CSCvs07344	ISE：正常に終了しているにもかかわらず、2.4 パッチ 9 のリセット設定がいくつかのエラーをスローする

不具合 ID 番号	説明
CSCvs12409	ゲストユーザーの有効日数の ISE ゲスト作成 API 検証に時間が考慮されない
CSCvs14297	PassiveID：$ を含む AD アカウントパスワードを使用して WMI を設定するとエラーになる
CSCvs19481	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCvs20356	Apple ミニブラウザ：自己登録のゲストログインページのパスワードのリセットリンクが機能しない
CSCvs20357	Apple ミニブラウザ：[キャンセル（Cancel）] ボタンがゲストの自己登録ページで機能しない
CSCvs23628	ルールが一致した後でも、ポリシーエンジンがすべてのポリシーセットの評価を続行する
CSCvs25258	ブルートフォースのパスワード攻撃に対する動作を改善する
CSCvs27310	ISE 2.6 と 2.7：dACL の説明フィールドに ' の文字を追加できない
CSCvs36036	ISE 2.6 では、ユーザーが IPv4 または IPv6 を選択しても、dACL シンタックスに複数の空白行が許可される必要がある
CSCvs36150	ISE 2.x ネットワーク デバイス スタックのローディング
CSCvs36758	ISE 2.6 で 2 つのカッコを使用して CRL URL を設定できない
CSCvs39633	NAD グループ CSV のインポートでは、説明フィールドにサポートされているすべての文字を許可する必要がある
CSCvs40813	<sns3615>、<sns3655>、および <sns3695> の platform.properties で次のプロパティが欠落している
CSCvs41571	自己登録済みゲストポータルがゲストタイプの設定を保存できない
CSCvs42072	静的グループの割り当てを編集できない
CSCvs42758	CRL が特定の条件で期限切れになる
CSCvs46853	DNA-C との統合中に、信頼できるストアから削除されたものと同じ CN の ISE 2.6 CA 証明書
CSCvs46998	条件はライブラリから削除されたが、DB 内にはまだある
CSCvs51296	ISE では、コマンドセットのコマンドの前にスペースを挿入できる
CSCvs51537	暗号化キーの特殊文字でバックアップがトリガーされない

不具合 ID 番号	説明
CSCvs53148	複数の EP が 1 秒ごとにプロファイリングされ、ISE ノードが同期しなくなる
CSCvs55594	ランダム認証の場合、期限切れまでの日数が 0 としてマークされる
CSCvs58106	NAD CSV のインポートでは、サポートされているすべての文字を TrustSecDeviceID に許可する必要がある
CSCvs60518	ISE 管理者ユーザーが内部ユーザーのグループを変更できない
CSCvs65467	Cisco Identity Services Engine のストアドクロスサイトスクリプティングの脆弱性
CSCvs65989	ネットワークデバイス/グループをインポートした後、新しいロケーションを追加できない
CSCvs67042	ISE 2.2+ がメモリリークの影響を受ける Inflater() によってネイティブメモリが毎日 1 ～ 2% 増加する
CSCvs68914	DNAC から送信された _（アンダースコア）を使用して SG が作成されたときにエラーが発生する
CSCvs76257	RadiusProxyFlow::stripUserName() にユーザー名ではなく空の文字列があるために ISE がクラッシュする
CSCvs77182	ISE：属性「url-redirect」を HTTPS で使用できず、HTTP を使用する同じ URL は正常に機能する
CSCvt02530	国コード属性が携帯電話番号の一部である場合、SMS がゲストに到達しない
CSCvt15256	「ゲストユーザー」ID ストアを使用すると、認証プロセスが失敗する。
CSCvr63698	セッションディレクトリに pxGrid 2.0 認証プロファイル属性がない

Cisco ISE リリース 2.7 の解決済みの不具合

次に、リリース 2.7 では解決されているバグを示します。

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283801589&rls=2.7&sb=anfr&sts=fd&scs=hSc&bt=custV

Cisco ISE リリース 2.7 の未解決の不具合

次の表に、リリース 2.7 では解決されていない不具合を示します。

不具合 ID 番号	説明
CSCvq11008	ISE OCSP 応答側証明書 CSR の使用状況データの更新が設定変更監査レポートに表示されない
CSCvp54416	デバイス SGT のトラブルシューティングで誤った診断が発生する
CSCvr86006	ノードのステータスが [システム概要（System Summary）] ダッシュレットに正しく表示されない
CSCvr91946	10% を超えるエンドポイントで証明書の発行が失敗する
CSCvr93902	管理者が [ネットワークデバイスの展開（Network Device Deployment）] ウィンドウで承認要求にコメントを追加できるポップアップウィンドウが正しく表示されない
CSCvr95284	RADIUS マッピングは SXP pxGrid トピックにパブリッシュされない
CSCvr99920	「show timezone」コマンドで CLI にタイムゾーンが表示されない
CSCvs02589	自己署名サーバー証明書の有効期限を 5 年に設定すると、macOS 10.15 の Chrome に NET::ERR_CERT_REVOKED エラーが表示される
CSCvs03195	最大セッションカウンタの有効期限オプションが機能しない
CSCvs10238	CSV ファイルからのポリシーのインポート中にポリシーをダウンロードすると、一部の更新が観測される
CSCwc83059	フルアップグレード後の VCS 情報がない

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services にアクセスしてください。
- サービスリクエストを送信するには、シスコサポート にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.

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。