Safeguard for Privileged Sessions 7.0 LTS

リリースノート

Rev 1.1

2024/4/15

ジュピターテクノロジー

この文書の原本は、「SPS_7.0 LTS_Release Notes」です。この文書についてご不明な点やお気づきの点がございましたら、ジュピターテクノロジー株式会社までお問い合わせください。

このガイドの表記規則

注意：注意アイコンは、指示に従わない場合、ハードウェアの損傷やデータの損失が発生する可能性があることを示します。

変更履歴

版	発行日	変更内容
第 1.0 版	2023/05/12	新規作成（7.0.2.1 対応）
第 1. 1 版	2024/04/15	新規作成（7.0.5 対応）

目次

1　このリリースについて

Safeguard for Privileged Sessions （SPS） バージョン 7.0LTS は、新機能と解決した問題を含む長期サポートリリースです。詳細については、次を参照してください。

- 新機能
- 解決した問題
- 既知の問題

> **メモ：** SPS の主な機能の詳細については、管理者ガイドを参照してください。

2 Safeguarrd のプロダクトラインについて

Safeguard アプライアンスは、Safeguard 特権管理ソフトウェア用に特化して構築されており、プリインストールされているためすぐに使用することができます。アプライアンスは、ハードウェア、オペレーティングシステム、ソフトウェア の各レベルでシステムの安全性を確保するために、強化されています。 このアプローチにより、特権管理ソフトウェアを攻撃から保護すると同時に、導入と継続的な管理を簡素化し、価値を生み出すまでの時間を短縮します。

Safeguard 特権管理ソフトウェアスイート

Safeguard 特権管理ソフトウェアは、特権ユーザーアカウントとアクティビティを制御、監視、管理し、悪意のあるアクティビティの可能性を特定して資格リスクを検出し、改ざん防止の証拠を提供するために使用されます。 Safeguard 製品は、インシデント調査、フォレンジック、コンプライアンスの取り組みにも役立ちます。

Safeguard 製品独自の強みは次の通りです。

- すべての特権アクセス管理のニーズに対応するワンストップソリューション
- 導入と統合が簡単
- 比類のない記録の深さ
- 資格とアクティビティの包括的なリスク分析
- 特権アカウントの徹底的なガバナンス

このスイートには、次のモジュールが含まれます：

- **Safeguard for Privileged Passwords（SPP）**
  ロールベースのアクセス管理と自動化されたワークフローにより、特権資格情報の付与プロセスを自動化、制御、保護します。堅牢なアプライアンス上に展開される SPP は、ソリューション自体への安全なアクセスに関する懸念を払拭し、お客様のシステムや IT 戦略との統合を迅速に行うことができます。さらに、ユーザーを重視した設計のため短時間で習得でき、どこからでもほぼすべてのデバイスを使用してパスワードを管理することができます。企業のセキュリティを確保し、特権を持つユーザーに新たなレベルの自由と機能性を提供します。

- **Safeguard for Privileged Sessions（SPS）**
  One Identity の特権アクセス管理ポートフォリオの一部です。大企業のニーズに対応した特権セッション管理ソリューションで、業界最高水準のアクセスコントロールに加え、特権アカウントの悪用防止、コンプライアンスの推進、フォレンジック調査の迅速化を実現するセッション監視・記録を提供します。

  SPS は、クライアントやサーバーから完全に独立しているため、既存のネットワークにシームレスに統合でき、迅速に展開できるエンタープライズアプライアンスです。ユーザープロファイリングに必要なアクティビティデータを取得し、フォレンジック調査のためにユーザーセッションの完全なドリルダウンを可能にします。

- **Safeguard for Privileged Analytics（SPA）**
  Safeguard for Privileged Sessions（SPS）のデータを統合し、特権ユーザーの行動分析のベースとして使用します。SPA は、機械学習アルゴリズムを用いて行動の特徴を精査し、個々の特権ユーザーごとにユーザー行動プロファイルを生成します。SPA は、実際のユーザーの行動とユーザープロファイルをリアルタイムで比較し、プロファイルは機械学習により継続的に調整されます。SPA は、異常を検出し、リスクに基づいてランク付けを行うため、優先順位を付けて適切な対応を行い、最終的にデータ侵害を防ぐことができます。

3 新機能

SPS バージョン 7.0 LTS の新機能

- **SPS ユーザーインターフェイスの更新**

  SPS のユーザーインターフェイスが変更されました。 変更には、メインメニュー、ユーザーメニュー、および概要ページが含まれます。

- **MSSQL プロトコルのサポート**

  SPS では、MSSQL 接続を制御および監査できるようになりました。Web UI と REST API の両方を使用して、関連する設定を構成できます。 詳細については、管理者ガイドの「MSSQL 固有の設定（MSSQL-specific settings）」および REST API リファレンス ガイドの「MSSQL 接続（MSSQL connections）」を参照してください。

- **監査データアクセスルール**

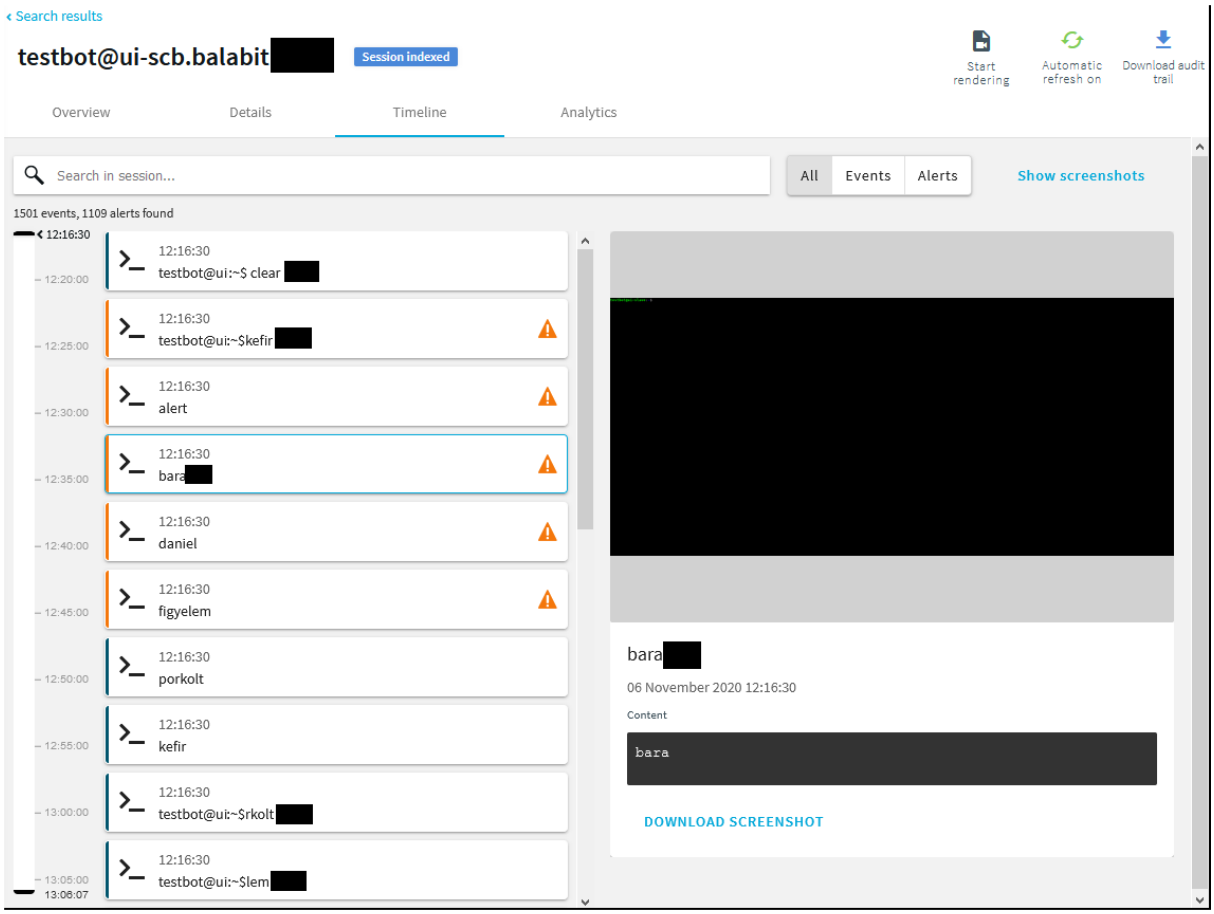
  ユーザーが権限を付与されたセッションの監査データのみにアクセスするように制限できるようになりました。
  監査データアクセスルールを使用すると、ユーザーが権限を付与されたセッションの監査データにのみアクセスできるように制限できます。 新しいルールを作成するときに、プレビューを使用して、検索クエリが関連する結果を返すことを確認できるようになりました。

- **ServiceNow との連携**

  SPS は、ターゲットサーバーでの認証および承認中にチケット ID の要求と検証を有効にすることで、ServiceNow と連携します。
  この連携により、ユーザーがサーバーにアクセスする正当な理由があることを確認することで、SPS で実行されるゲートウェイ認証に追加のセキュリティレイヤーが追加されます。
  SPS はユーザーに有効な ServiceNow チケット ID を要求し、認証が成功すると、ユーザーが情報システムにアクセスできるようにします。 詳細については、「ServiceNow - Tutorial」を参照してください。

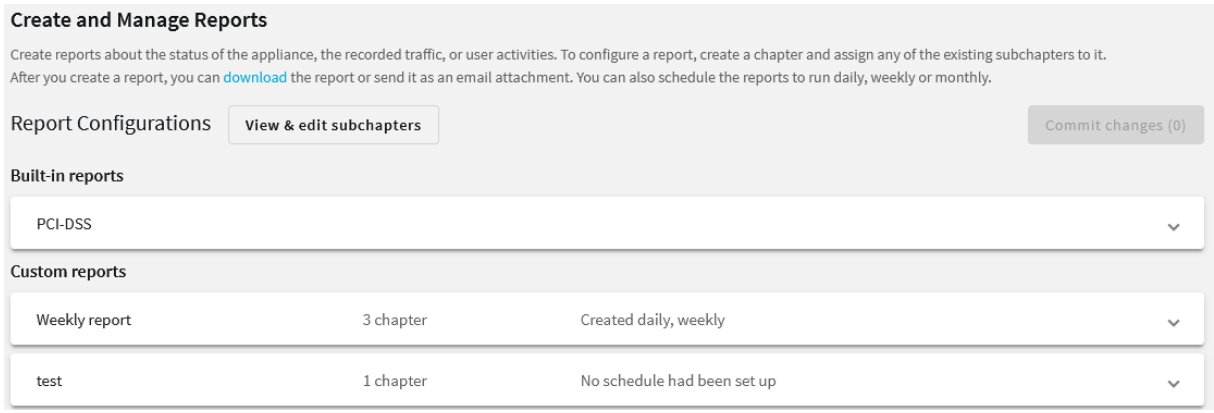
- **タイムラインタブ**

  検索インターフェイスから、SPS によって記録されたデータについて、セッションイベントとアラートをタイムラインで表示し、監査証跡の内容を検索できます。**[Timeline]** タブは、廃止された **[Events]**、**[Alerts]**、および **[Contents]** タブに代わるものです。



- **レポート作成の再設計とダウンロード**

  レポートのチャプターやサブチャプターを含む、レポートの作成およびダウンロード用のユーザーインターフェイスが再設計されました。 新しいレポートワークフローにより、レポートの作成とダウンロードのプロセスが簡素化され、ユーザーエクスペリエンスが向上します。



- **トラストストア**

信頼できる認証局 (CA) の証明書チェーンを保存するトラストストアを使用して、TLS 接続で証明書を検証できます。 新しく作成された**［Basic Settings］＞［Trust Stores］**ページで、カスタムトラストストアを追加および編集できます。

> ⚠ **注意：アップグレードすると、X.509 クライアント証明書を使用して Web インターフェイスのユーザーを認証するように変更されます。証明書は、信頼できる CA リストではなく、トラストストアに対して検証されます。 アップグレード中に、以前認証に使用されていた信頼できる CA リストが、失効チェックがデフォルトで無効になっているトラストストアにコピーされます。**
>
> **信頼できる CA リストの失効チェックを有効にし、以前に証明書失効リスト (CRL) の URL を追加した場合、または失効チェックを有効にしたい場合は、トラストストアの設定を手動で編集する必要があります。［Basic Settings］＞［Trust Stores］に移動し、トラストストアの失効チェックタイプとして［Leaf］または［Full］を選択し、ルート CA と中間 CA ごとに CRL URL を追加してください。**
>
> **トラストストアとその設定方法の詳細については、管理者ガイドの「トラストストアを使用した認証局による証明書の検証（Verifying certificates with Certificate Authorities using trust stores）」を参照してください。**

- **デフォルトのネットワークレベル認証 (NLA) 設定**

  RDP 接続のデフォルトのプロトコルレベル設定が変更され、RDP 設定ポリシーで NLA がデフォルトで有効になりました。
  この変更により:

  - デフォルトの RDP 設定は、NLA が有効になっている**［default_nla］** になりました。
    以前は default と呼ばれていた RDP 設定は、**［legacy_default］**に名前が変更されました。
  - **［Enable RDP4 style authentication］**オプションが削除されました。

    > ⚠ **注意：6.8.0 より前の SPS バージョンからアップグレードする場合で、［legacy_default］または［default_nla］という名前の既存の RDP 設定がある場合は、アップグレード前に名前を変更する必要があります。**

- **SPS での Sudo の使用**

  SPS と Sudo の統合により、Sudo 用語で iolog と呼ばれる Sudo セッションの記録を SPS で収集して分析できます。

SPS を使用して Sudo セッションの記録を収集および分析すると、Sudo の記録は SPS によって保存およびインデックス付けされます。たとえば、検索インターフェイスを使用して、記録を表示したり、Sudo セッション中に実行されたコマンドを一覧表示したりできます。

- **クレデンシャル インジェクション**

  SPP 側で開始された RDP アプリケーションセッションは、RemoteApp ランチャーのパスワードを自動的に提供します。
  クレデンシャルインジェクションを使用するには、クレデンシャルインジェクションフラグが選択されている RDP アプリケーションセッションの接続ポリシーを使用します。

- **SPS インスタンスから別の SPS インスタンスへのデータ移行**

  SPS インスタンスから別の SPS インスタンスに切り替える必要がある場合、たとえば、古い SPS アプライアンスを新しいものに切り替えたい場合は、コンソール メニューを使用して SPS インスタンス間のデータすべてをコピーできます。

- **SPP と共有される接続ポリシーでのカスタム AA プラグインの設定**

  詳細については、管理者ガイドの「Sharing RDP connection policies with SPP（RDP 接続ポリシーを SPP と共有）」および「Sharing SSH connection policies with SPP （SSH 接続ポリシーを SPP と共有）」を参照してください。

主な改善点

- **VNC over HTTP WebSocket のサポート**

  SPS は、WebSocket トラフィックの監査をサポートするようになりました。 すべての WebSocket トラフィックを制御および監査できますが、現在、Safeguard Desktop Player アプリケーションは、VNC over WebSocket トラフィックのみを再生できます。外部分析のために、他のタイプの監査済み WebSocket トラフィックを PCAP 形式にエクスポートできます。

- **SPP での SPS の使用**

  SPS と SPP の連携をさらに改善するために、セッションによって開始されるワークフローで 2 つのデプロイを使用することが大幅に改善されました。

- **SSH の改善**

  - SSH セッションでの Kerberos ベースの認証が改善されました。

- SSH チャネルポリシーでホスト名を解決すると、カスタムドメインネームサーバーを使用できるようになりました。

- **Ed25519 ホストキーのサポート**

  SPS では、次の公開 SSH ホストキーを使用できます。 I

  - RSA は、SSH キーの最も広く使用されている公開キーアルゴリズムです。

    > **メモ：** One Identity は、2048 ビット (またはそれよりも強力) の RSA キーを使用することを推奨しています。

  - Ed25519 は、RSA よりも優れたセキュリティと高速なパフォーマンスを提供します。

    SPS では、Ed25519 SSH ホストキーが OpenSSH と PKCS #8 形式の両方でサポートされています。

    SPS で複数の SSH キーを使用することもできます。 これにより、古い RSA SSH キーを保持し、Ed25519 を使用する新しいキーを生成できます。

- **ECDSA 256 (ecdsa-sha2-nistp256) SSH ホストキーのサポート**

  SPS は、デジタル署名アルゴリズム (DSA) の変形である ECDSA 256 (ecdsa-sha2-nistp256) SSH ホストキーをサポートするようになりました。

- サポートされている秘密鍵アルゴリズムは、RSA、DSA、および EC です。

- **AAA メニューとサブメニューの名前変更**

  以下のメニュー項目の名前が変更されました。 機能の変更はないことに注意してください。

Old name	New name
AAA	Users & Access Control
Group Management	Local User Groups
Access Control	Appliance Access
Permission Query	Access Rights Report
Accounting	Configuration History

  ［<Protocol name> Control］＞［Connections］＞［Access Control］＞［Permission］ の下にあるユーザーグループの権限設定も、**［Search&Authorize］**から **［Follow&Authorize］**および **［Search］**から**［Follow］**に名前が変更されました。

- **ブラウザーオプションでの監査証跡の再生機能の強化**

ブラウザーオプションで監査証跡を再生する機能が次のように強化されました。

- ビデオファイルの生成はバックグラウンド操作として実行され、UI にその痕跡はありません。 生成がバックグラウンドで進行している間に、監査証跡のビデオファイルを再生することができます。
- ブラウザーでアクティブなセッションをフォローできます。
- クラスターモードでは、検索マスターノードだけでなく、検索ミニオンノードからも監査証跡のビデオファイルを再生できます。
- 暗号化された監査証跡とスクリーンショットを復号化するために必要な秘密鍵を監査キーストアに保存できます。 監査キーストアは、定義したマスターパスワードによって保護されます。 監査キーストアは、キーストアに追加された秘密鍵に対応する証明書の保管には使用されません。必要な証明書をインデクサーサービスに追加する必要があります。
- 監査証跡のビデオファイルを見ているとき、またはアクティブなセッションをフォローしているときに、テキストベースのプロトコルの内容をクリップボードにコピーできます。
- 検索インターフェイスの詳細ビューの自動更新オプションが、**[User menu] > [Preferences]** で利用できるようになりました。

- **Safeguard Desktop Player の機能強化**

  Safeguard Desktop Player は、アプリケーション言語の設定、キーボードレイアウトの選択、シーカーやサブタイトルでのウィンドウタイトルイベントの表示方法の選択などに使用できる**[設定]** メニューが強化されました。

- HTTP コントロールの新しい設定プロファイルオプションの作成が強化され、再設計されました。**[HTTP Control] > [Settings]** で **[Create new]** をクリックした後、次のページで新しい設定プロファイルを構成できます。
  - Name and timeout
  - Session cookies
  - TLS settings
- RDP クライアントとサーバー間で転送されるサウンドの監査を有効にすることができます。この新しいオプションを有効にするには、**[RDP Control]** オプションの **[Channel Policies]** 設定で、この目的で使用するチャネルポリシーの **[Sound]** および **[Dynamic virtual channel]** の **[Record audit trail]** チェックボックスを選択します。

  Safeguard Desktop Player の **[Export audio]** オプションを使用すると、サウンドを監査証跡から .wav ファイルにエクスポートできます。 エクスポートされた .wav ファイルには、監査対象ユーザーからのサウンドが含まれています。
- SPS 6.12.0 より前では、LDAP、RADIUS、または X.509 認証方法が設定されている場合、管理者ユーザーは常にローカルで認証されていました。 他のユーザーは、ローカル資格情報でログインできませんでした。
  SPS 6.12.0 から、ログイン用に複数のデータベースを設定できるようになったため、認証に使用する正しいデータベースを選択する必要があります。アプライアンスが別の方法を使

用するように設定されているときにローカル管理者ユーザーとしてログインするには、ログイン画面でローカルログインリンクをクリックする必要があります。
この変更の結果、ローカルログインリンクを使用して、管理者ユーザーだけでなく、他のすべてのローカルユーザーを認証できるようになりました。不正なアクセスを防止するために、アプライアンスがローカルとは異なるログイン方法を使用するように設定されている場合、管理者以外のすべてのローカルユーザーのパスワードはアップグレード中にリセットされます。
アップグレード後、ロックアウトされた管理者以外のローカルユーザーのログインを再度有効にする場合は、新しいパスワードを設定できます。 ローカルログインは常にアクティブであるため、X.509 ログインの管理者フォールバックオプションは非推奨です。

- HTTP エラーテンプレートを作成およびカスタマイズして、カスタマイズされた HTTP エラーメッセージをユーザーに送信できます。 カスタマイズできるエラーメッセージに加えて、エラーページの名前、色、および必要に応じてロゴを設定できます。

- SPS UI では、次のオプションが**［Basic Settings］**から **［Users & Access Control］＞［Settings］**に移動されました。

    - Protecting against brute-force attacks
    - Authentication banner
    - Web interface timeout

  ログイン設定は、**［Basic Settings］**から **［Users & Access Control］＞［Settings］**、 **［Basic Settings］**から **［Users & Access Control］＞［Login Options］**に移動しました。**［Login Options］**で使用可能なログイン方法は、それぞれの認証方法に対応しています。

    - Local
    - X.509
    - RADIUS
    - Active Directory
    - POSIX LDAP

- SPS の Web およびコンソールログイン画面に、設定可能なテキストを含むバナーを表示できます。

- 暗号化された監査証跡の場合、秘密鍵に加えて、PEM でエンコードされた X.509 証明書をアップロードする必要がなくなりました。 これで、RSA 秘密鍵のみが必要になります。
- SPS バージョン 6.13.0 から、Internet Explorer 11 (IE11) はサポートされなくなりました。 SPS バージョン 6.12.0 およびそれ以前のバージョンは引き続き IE11 をサポートします。
- SPS は、AWS の Elastic Network Adapter (ENA) を介して強化されたネットワーク機能をサポートします。
- SPS ログインペインが視覚的に改善されました。 利用可能なすべてのログイン方法がドロップダウンメニューにまとめられました。
- 新しい認証方法を作成する場合、最初にログイン方法の名前を指定すると、SPS は**［Script reference］**フィールドに自動的に入力します。
- クリーンアップオプションは、アーカイブオプションから分離されました。 クリーンアップ オプションを使用すると、.zat ファイルと対応するセッションのメタデータを削除できます。

  クリーンアップ時間は、**［Connections］**または**［Global Options］**で設定できます。

SPS REST API リファレンス ガイド バージョン 7.0 LTS の変更点と改善点

- 利用可能なログイン方法のリスト： ログイン方法（ローカル、LDAP、RADIUS、または x509）を一覧表示して、SPS への認証に使用できるログイン方法を決定します。 詳細については、SPS REST API リファレンス ガイドの「Listing SPS login methods（SPS ログイン メソッドの一覧表示）」および「Authenticate to the SPS REST API（SPS REST API への認証）」を参照してください。
- HTTP 経由で SPS ファームウェアをダウンロードしてインストールします。 アップグレードする前に大きな SPS ファームウェア ISO ファイルを手動でアップロードする必要がないようにするには、SPS REST API を介して URL を提供することにより、SPS ファームウェア ファイルをダウンロードしてインストールします。 1 つのファイルをダウンロードすることも、複数のファイルを同時にダウンロードすることもできます。 詳細については、SPS REST API リファレンス ガイドの「Downloading and installing SPS firmware through HTTP（HTTP を介した SPS ファームウェアのダウンロードとインストール）」を参照してください。
- 強化されたアプライアンスのヘルス ステータス モニタリング： RAID およびインデクサー機能を監視するための新しいパラメーターが追加されました。 詳細については、SPS REST

API リファレンス ガイドの「Monitor appliance health status（アプライアンスのヘルス ステータスの監視）」を参照してください。

- /api/configuration/reporting/custom_subchapters エンドポイントを使用してカスタムクエリから統計を作成することは非推奨になりました。

4　非推奨の機能

target_ で始まる Authentication and Authorization および Credential Store プラグインの引数

target_host または target_server 引数にホスト名または IP アドレスが含まれていたため、これらの引数は廃止されました。

現在、非推奨の引数を置き換えるために、Authentication and Authorization および Credential Store プラグインに新しい引数が追加されています。新しい引数名は、含まれる値を明示的に定義します。つまり、server_ip 引数には常に IP アドレスが含まれ、server_hostname 引数には常にホスト名が含まれます。

非推奨の引数は次のとおりです。

認証および承認プラグイン: get_password_list および get_private_key_list 入力引数:

- target_username
- target_host
- target_port
- target_domain

Credential Store プラグイン: 認証方法:

- target_server
- target_port
- target_username

コンテンツ ポリシーの生体認証の廃止

- ポインティングデバイスの生体認証 - 非推奨：この機能は非推奨です。 代わりに、インデクサーポリシーで同じオプションを使用してください。
- タイピングの生体認証- 非推奨：この機能は非推奨です。 代わりに、インデクサーポリシーで同じオプションを使用してください。

RPC API

RPC API は廃止され、削除されました。代わりに REST API を使用することをお勧めします。

Splunk フォワーダー

Splunk フォワーダーは SPS 6.7 で廃止され、削除されました。代わりにユニバーサル SIEM フォワーダーを使用することをお勧めします。

Apache lucene データベース

SPS 7.0 LTS では、Elasticsearch データベースのみを使用するように、セッション データ内の画面コンテンツの検索を変更しました。 Apache lucene データベースのサポートは段階的に廃止されますが、クエリ言語は lucene に似たままです。

Elasticsearch データベースに切り替えた後、reindex ツールを使用してコンテンツを再生成した場合にのみ、Apache lucene データベースに保存されているコンテンツにアクセスできるようになります。 詳細については、「Regenerate content stored in lucene indices」を参照してください。

lucene インデックスが削除されたため、ユーザーは **/api/audit/sessions** および **/api/audit/sessions/stats** エンドポイントのコンテンツリクエストパラメーターを使用して lucene インデックス内のコンテンツを検索できなくなりました。

詳細については、REST API リファレンス ガイドの「Searching in the session database」と REST API リファレンス ガイドの「Session statistics」を参照してください。

さらに、**［Reporting］**では、**audit_content** フィルターを含む統計サブチャプターは機能しません。 または、検索ベースのサブチャプターと **screen.content** フィルターを使用して、監査証跡に特定のコンテンツを含む接続メタデータから統計レポートを作成できます。

詳細については、管理者ガイドの「Creating search-based report subchapters from search results」を参照してください。

コンテンツ検索オプションの廃止

［Search］ページで、**［Content search］**オプションが廃止されました。

Advanced statistics

［Reporting］＞［View & edit subchapters］＞［Advanced statistics］ページを使用したカスタムクエリからの統計の作成は廃止されました。
/api/configuration/reporting/custom_subchapters REST API エンドポイントも廃止されました。

アップグレード プロセス中に、既存の advanced statistics subchapters とその references が SPS 構成から削除されます。 さらに、ユーザーグループに割り当てられた advanced statistics ACLs も SPS 構成から削除されます。 ユーザー グループに**［Users & Access Control］＞［Appliance Access］**で割り当てられた advanced statistics ACL しかない場合は、アップグレード プロセス中に ACL エントリ全体が削除されることに注意してください。

代わりに、search-based のサブチャプターを使用して、接続メタデータをクエリすることもできます。 詳細については、管理者ガイドの「Creating search-based report subchapters from search results」を参照してください。

5　解決した問題

以下は、このリリースで対処された問題のリストです。

表 1 ：SPS7.0.5LTS で解決した問題

Resolved Issue	Issue ID
[Reporting] > [Create & Manage Reports] で、または REST API 経由でレポート内で参照されているサブチャプターの削除を含む変更をコミットしようとすると、SPS は次のような曖昧なエラーメッセージを含むエラーを表示しました。「The referenced subchapter 'subchapter-id' does not exist.」 この問題は修正され、サブチャプターを削除するときに、SPS がそのサブチャプターがレポート内で参照されているかどうかをチェックし、参照されている場合は、サブチャプターがレポート内で参照されており、参照する必要があることを示す意味のあるエラーメッセージを含むエラーを直ちに表示します。	393727
他のユーザーによって認証がブロックされる可能性がある問題が修正されました。 SPS は、ユーザーの認証と承認の試行が他のユーザーの認証をブロックする可能性がある方法で機能しました。 この制限は、認証または承認がほぼ瞬時に実行される間は問題を引き起こしませんでした。 ただし、プロセスがリモート AD/LDAP または RADIUS サーバーの遅い応答を待っていた場合、他のユーザーのすべての認証要求もブロックされます。 これは、リモート サーバーが過負荷になっている場合、またはユーザーとの何らかの対話 (MFA など) を待機している場合に特に顕著であり、この場合、ユーザーはページの読み込み時間の遅さや認証タイムアウトエラーを経験する可能性があります。 この問題は修正され、認証試行が同時に実行されるようになりました。 リモートリソースの消費は並行認証リクエストで発生しますが、リモートソースが過負荷になっている場合は依然として遅くなる可能性があることに注意してください。	420845
リモートデスクトップゲートウェイのパケット過負荷によりメモリ不足クラッシュの問題が発生する可能性がある問題を修正しました。 RDP プロキシがデスクトップゲートウェイとして機能する場合、クライアントがパケットを使用できない場合、パケットを一時的にキャッシュします。 パケ	340013

ット負荷が重くて永続的な場合、このキャッシュはリソース制限に達するまで増加する可能性があります。 この問題は修正され、バッファがフロー制御の決定に関与するようになりました。	
SPNEGO 応答にエラーコードのみが含まれている場合、サーバー認証中に RDP がクラッシュする問題を修正しました。 サーバーは SPNEGO 応答でのみベンダー固有のエラー コード (HResult 80090302: unsupported function) で応答しましたが、この形式は SPS が予期していませんでした。 この問題は修正され、SPS はそのような応答を適切に処理するようになりました。	439931
[SSH Control]> [Options]ページでは、他のユーザーにこのページへの書き込みおよび実行アクセスが許可されている場合でも、ローカル管理者に対して Kerberos キータブのアップロードまたは削除のみが許可されていました。 この問題は修正され、適切なアクセス権限を持つすべてのユーザーがキータブをアップロードおよび削除できるようになりました。	442599
DNS 解決タイムアウトの問題を修正しました。 以前は、SPS がドメイン名を解決しようとしたときに DNS サーバーが応答しなかった場合、SPS は待機時間が長すぎてタイムアウトになりました。 この問題は修正され、ドメイン名を解決するときにタイムアウトが正しく適用されるようになりました。	418170
プラグイン API チェック中のエラーのため、2 桁のプラグイン API バージョン (たとえば、1.7) のプラグインをアップロードできませんでした。 バージョン チェックが修正され、今後は 2 桁の API バージョンが使用できるようになります。	441702
以前は時間範囲が 3 つしかありませんでした。 • 時間：時間範囲が 1 日より短いか、1 日と等しい場合 • 日：期間が 30 日以下の場合 • 月：期間が 30 日より長い場合 新しい期間 (週) が導入され、期間の分布は次のように変更されました。 • 時間：時間範囲が 1 日より短いか、1 日に等しい場合 • 日：期間が 14 日以下の場合	340221

• 週：期間が 12 週間以下の場合 • 月：期間が 14 週間より長い場合 項目が 0 件の列も表示されます。	
SPS REST API の CSRF protection はオプションでした。 この修正により、ユーザーエージェントがブラウザーを参照する場合、SPS は CSRF protection を強制します。	428406
SPS UI または SPS REST API 経由でコンテンツのサブチャプターを含むレポートを生成する場合、約 1000 を超えるセッションがコンテンツクエリに一致すると、レポートの生成が失敗する可能性があります。 コンテンツのサブチャプターを含むレポートを生成する場合、レポートはコンテンツクエリに一致するセッションを収集します。 セッションごとに、QR コード画像が一時ファイルに生成され、生成された PDF ファイルに埋め込まれます。 残念ながら、これらの一時ファイルのファイル記述子は適切にクローズされていませんでした。 その結果、コンテンツクエリに一致するセッションが多すぎて、オープンしているファイル記述子の数がオペレーティングシステムの制限を超えた場合、レポートの生成は失敗し、次のバックトレースが /var/log/messages ログファイルに書き込まれました。「ERROR OSError: [Errno 24] Too many open files.」 この問題は、ファイル記述子が適切にクローズされていることを確認することで修正されました。	431434

表 2 ：SPS7.0.4LTS で解決した問題

Resolved Issue	Issue ID
10,000 人を超えるユーザーのベースラインを構築できるように修正されました。	424024
SPS のローカル SSH と SPS のローカル SSH の root パスワードは、シールドモードの REST API で設定できます。 構成の問題は解決され、ローカル SSH と root パスワードをシールドモードで構成できなくなりました。	340251
この問題を修正しました：ログインページのローカルログインモーダル背景が、遅いインターネット上で正しく表示されませんでした。	392712
LDAP 管理でバインド DN 値を削除できるようになりました。	403955
アップグレードの事前チェックで必要なスペースの計算を修正しました。	406696

これまで、アップグレードの事前チェックプロセスでは、必要なスペースが適切に計算されませんでした。 この問題は修正されました。	
ファームウェアのアップグレード中、または古いコンフィグレーションバンドルをインポートするときに、計算コストのかかる検証ルールが複数回評価されました。コンフィグレーションが非常に複雑な場合、プロセスの実行時間が長くなり、Web ユーザーインターフェイスのサーバー側リクエストハンドラーの最大実行時間を超え、操作が失敗する可能性があります。 この検証は 1 回だけ実行されるようになりました。そのため、ファームウェアのアップグレード中またはコンフィグレーションのインポート中に複雑な構成を検証しても、実行時間制限を超えることはありません。	413675
ユーザーが新しいカスタムレポートを作成すると、[Reporting]> [Create and Manage Reports] の UI で変更がコミットされる前に、[Create report] ボタンの背後でアクションが利用可能でした。 この問題は修正されました。	416981
Microsoft リモートデスクトップアプリ 10.8.2 以降を使用して Mac OS 上で開始された RDP 接続は失敗しました。 Microsoft リモートデスクトップアプリ 10.8.2 では、SPS によって処理されない、文書化されていない新しいプロトコル機能が有効になっており、RDP 接続が失敗します。 この問題は修正され、SPS がこの機能を適切に認識して無効にするようになりました。	417054
SPS インスタンスが AWS EC2 で最初に起動されたとき、ブートストラップシステムが失敗することがありました。 この場合、顧客は HTTPS 経由で新しくプロビジョニングされたインスタンスに接続しようとすると、無期限に接続拒否が発生します。 この信頼性の低さは、ブートストラップ手順を安定させるために修正されました。	421194
アップグレードノート内のドキュメントリンクは解決できませんでした。 特定のファームウェアバージョンのアップグレードノートが表示される場合、アップグレードガイドとリリースノートへのリンクが正しくありませんでした。 ドキュメントサイトが更新され、過去のバージョンのコンテンツも提供されました。	422264
Windows Azure 環境では、SPS コンソールのネットワーク設定と Azure ゲストエージェント間の相互作用が原因で、失敗したネットワーク サービスが SPS コンソールで報告されることがあります。 SPS ネットワーキングシステムは、このような外部変化に耐えられるように強化されました。	414452

SPP と SPS がリンクされている場合、SPS は SPP クラスターのメンバーの最新のリストを維持する必要があります。 このリストは定期的に照会されましたが、SPP クラスターの 1 次ノードからのみ照会されました。 これは、SPS がプライマリ SPP ノードに到達できない場合に、SPS が、最後に確認された SPP クラスターメンバーのセットに基づいて、SPP クラスターの他のノードから SPP クラスターメンバーのクエリを試みるように変更されました。	414457
SPS がリモート デスクトップゲートウェイとして機能するように構成されており、接続の初期段階でクライアントが切断されると、すべての RDP 接続が終了する可能性があります。 この場合、コアファイルが生成され、「Timer expired; description='I/O timeout」という行とともにバックトレースがシステムログに書き込まれました。 この問題は現在修正されています。	411111
7.3.0 より前の SPS の次のバグは、SPS REST API を介してのみ発生する可能性がありました。 ユーザーが次のエンドポイント https://SPS_IP/api/configuration/reporting/restbased_subchapters に POST リクエストを送信し、「fields」値リストに日付型のフィールドを含む restbased_subchapter を作成したとします。 SPS 7.3.0 では、ユーザーが日付タイプの列を含む検索ベースのサブチャプターを作成した場合に、SPS UI の [Reporting]> [Create & Manage Reports] メニュー項目でも、[View & edit subchapters]ボタンを押すと発生する可能性があります。 このバグは、レポート内のセッションの日付タイプのフィールドに値がなく、予期される“n/a”の代わりに空白のテキスト "　" が表示された場合に、生成されたレポートで見つかる可能性があります。 この問題は修正され、レポートに日付型のセッションフィールドを含む検索ベースのサブチャプター（REST API では REST ベースのサブチャプターと呼ばれる) が含まれており、生成されたレポートにその値を含まないセッションが含まれるようになりました。 日付フィールドの場合、レポートにはフィールド値として“n/a”が含まれます。	412721
ユーザーがトラストストアに証明書を追加または削除しただけの場合、これらのアクションでは [Save] ボタンは有効になりませんでした。 この問題は修正されました。	340419
LDAP サーバーを作成または編集するための名前検証がありません。 ユーザーが未使用のものを選択できるように、一意の名前検証ツールが LDAP サーバー名フィールドに追加されました。	340503

Enter キーハンドラーを LDAP サーバー共有シークレットダイアログに追加しました。	340505
リスト内に完全に一致するものがあった場合、その結果がリストの最後に表示されることがあります。これは、リストが大きすぎてスクロール可能な場合、ユーザーは結果をすぐに見ることができないことを意味します。 この問題は修正されました。	340507
[User Preferences]> [Search page settings]> [Automatic refresh]トグルは、検索ページのバックグラウンドデータの更新には影響しませんでした。 この問題は修正されました。	340519
EU データハウスは starling で利用できますが、UI にはまだサポートされていないことが示されました。 この問題は修正されました。	340520
固定時間枠またはカスタム時間枠のレポートを作成すると、ページには自動リダイレクトの代わりにリダイレクト候補のポップアップが表示されます。また、カスタム時間枠レポートの作成中にエラーが発生した場合でもリダイレクトされません。	340540
今後、ユーザーが前方シークボタンを押すと、オンラインビデオプレーヤーが停止します。 これは、ビデオ内で前に進むのと後ろに進むのを同じにするために実装されました。	340542
[About]サイドシートにある[read the release notes]リンクをクリックすると、古いページに移動しました。 このリンクは修正され、ユーザーが正しいページに移動できるようになりました。	386176
コンテンツ ベースのサブチャプターのクエリでは、内部エラーが発生するため、検索ワード内の対になっていない二重引用符は除外されなくなりました。このことは、コンテンツサブチャプターエンドポイントの REST スキーマでも表されます。	387790
10,000 以上のセッションがある場合、最後のページのページネーション範囲が正しくありませんでした。 この問題は修正されました。	422663
Windows 11 でリモートデスクトップ 10.0.22621 を使用した RDP プロトコルのネゴシエーションが失敗します。 Windows 11 バージョン 22H2 では、RDP プロトコルネゴシエーションが変更され、最初のチャネル参加メッセージをスキップできるようになりました。 これは SPS によって処理されなかったため、RDP 接続の開始に失敗しました。 この問題は修正され、SPS は RDP チャネル参加スキップをサポートするようになりました。	425560

SPS UI の [Reporting] ＞[Create & Manage Reports] で新しいコンテンツサブチャプターを作成し、ユーザーが特定のプロトコルの [Connections] メニューポイントにアクセスせずにプロトコルの [Connections]ポリシーフィルターを使用してコンテンツサブチャプターを作成した場合、SPS は「403 Forbidden: The client is not authorized to access the given resource.」エラーを返しました。さらに、ユーザーがプロトコルの [Connections]ポリシーフィルターを使用して新しいコンテンツサブチャプターを作成しようとした場合、SPS も前のエラーで応答し、サブチャプターを作成できませんでした。 この問題は修正され、プロトコルの [Connections]メニューポイントにアクセスしなくても、プロトコルの [Connections]ポリシーフィルターが期待どおりに機能するようになりました。	425741

表３：SPS7.0.3.1LTS で解決した問題

Resolved Issue	Issue ID
4000 シリーズアプライアンスではネットワークインターフェイスの順序が間違っていたため、適切なケーブル接続でも高可用性構成が機能しませんでした。 この問題は修正されました。	424781
事前チェック段階で legacy RAID ステータスチェックが行われましたが、4000 シリーズアプライアンスでは失敗しました。 従来の RAID ステータスチェックは廃止され、新しい事前チェック手順が導入されました。	425584

表４：SPS7.0.3LTS で解決した問題

Resolved Issue	Issue ID
接続ウィザードページのタイプミス。 接続ウィザードの [Connection] の作成ページに SPS アドレスがありませんでした。 これは修正されました。	340527
スクリーンショット生成許可エラー通知が表示されすぎる。 読み取り権限を持つユーザーがすでに生成されたスクリーンショットを表示しようとすると、SPS はスクリーンショット生成エラーを表示しました。 この問題は修正され、スクリーンショットを生成したいユーザーに検索アクセス制御リストの読み取りおよび書き込み権限がない場合にのみ、スクリーンショット生成権限エラーが表示されるようになりました。	340529
[Login Options]＞[LDAP servers]：同じアドレスのバリデータがありません。	340563

LDAP サーバーのアドレスリストにバリデータが追加され、同じホスト名とポートを持つアドレスが複数ある場合にユーザーがリストを保存できないようになりました。 アドレス リストには一意の値のペアが含まれている必要があります。	
ライセンスの問題はサイドバーには表示されません。 [About] メニューで、拡張可能なパネルを閉じたときに警告アイコンが表示されませんでした。 この問題は修正され、警告がある場合、拡張可能なパネルが閉じていても警告アイコンが表示されるようになりました。	340598
コンフィグレーション要素が多すぎると、UI で Reference_id エラーが発生する可能性があります。 Web GUI で非常に大規模なコンフィグレーション変更をコミットすると、「Form reference id received does not match stored value」というエラーが発生して失敗することがありました。 この問題は修正され、このような非常に大規模なコンフィグレーション変更が 1 回のコミット内で可能になりました。 また、エラーメッセージは、エラー状態とその考えられる解決策をより適切に説明するために書き直されました。	403615
RDP チャネルポリシーで許可されたリダイレクトデバイスが、コミット中にコンフィグレーションに保存されませんでした。 この問題は修正されました。	406786
インストール後に RAID ステータスが表示されない。 以前は、Safeguard 4000 のインストールの最後に RAID 同期ステータスが表示されませんでした。 この問題は修正されました。	407479
OpenSSH 7.4 以前を実行しているリモート SSH サーバーへの SPS 経由の接続は失敗することがあります。 SSH 認証ポリシーで[Agent]が選択され、リレーされた認証方法が[Public key]に設定されており、ターゲット SSH サーバーが OpenSSH 7.4、7.3、または 7.2 を実行している場合、SPS を介したサーバーへの接続が失敗する可能性があります。 この場合、次の行がログに書き込まれました：「Client side public key signature algorithm is unsupported by the server; signature_algo='...'」 この問題は修正されました。 OpenSSH 7.4、7.3、または 7.2 を実行しているリモート SSH サーバーへの公開キー認証が機能するようになりました。	415489

表５：SPS7.0LTS で解決した問題

Resolved Issue	Issue ID
アップグレード後に初めてユーザーインターフェイスにアクセスすると、エラーメッセージまたは空白のページが表示されました。 エラーが原因で、以前のバージョンの SPS では、永続的なリダイレクトでユーザーをログインページにリダイレクトしていました。 ブラウザーはこの情報を記憶しており、URL を使用できなくなったため、SPS はアップグレード後のユーザーインターフェイスへの最初のアクセス時に、空白のページまたはエラーメッセージを表示しました。 これは修正され、SPS はログインページに正しくリダイレクトされるようになりました。	PAM-16656
RDP でクリップボードを介してファイルをコピーすると、すべての接続が終了する可能性がありました。 ごくまれに、クリップボードのコピーと貼り付けを使用して RDP セッションホストとの間でファイルをコピーすると、貼り付け操作中にすべての RDP 接続が終了する可能性があります。 この場合、コアファイルが生成されました。この問題は、RDP クライアントまたはサーバーがクリップボードから無効なファイルを要求した場合に、不十分な安全性チェックが原因で発生しました。 これは、安全性チェックを修正することで修正されました。 無効な貼り付け要求の場合、「Invalid file index in cliprdr file content request」というメッセージがシステムログに表示され、要求はすべての場合に適切に破棄されます。	PAM-16569
オンラインプレーヤーのビデオ共有が機能しませんでした。 他のユーザーが SPS にログインしていない場合、ビデオ共有が機能しませんでした。 この問題は修正されました。	PAM-16519
生成されたレポートには、セッションの開始時刻とセッションの終了時刻が月の精度でのみ表示しました。 残念ながら、日次レポートのグラフの解像度を修正した［Session history］および［Verdicts history by sessions］サブチャプターの以前のパッチには、望ましくない副作用があり、［Top 10 longest sessions］や［Top 10 shortest sessions］のようなセッションの開始時間とセッション終了時間を表示する他のサブチャプターが発生しました。 または、セッションの開始時刻とセッションの終了時刻を秒精度ではなく月精度でのみ表示しました。 この問題は修正され、生成されたレポートでセッションの開始時刻と終了時刻が秒精度で表示されるようになりました。	PAM-16485

SPS は、mssql セッションの［Play video］ボタンとスクリーンショットを誤って表示する可能性がありました。 ビデオを再生したり、mssql セッションのスクリーンショットを表示したりする機能はまだ実装されていません。	PAM-16461
ライセンスが構成されていない場合、ファームウェア テストは理由を表示せずにアップグレードを拒否しました。 ライセンスが構成されておらず、［Test firmware］アイコンをクリックした場合、または［Basic Settings］＞［System］＞［Firmwares］で、再起動後に別のファームウェアをアクティブにするように選択した場合、ファームウェア テストは失敗しましたが、どのテスト結果も問題を示していませんでした。 . この問題は修正されました。	PAM-16450
監査された接続 (主に RDP) は、監査証跡の書き込みに失敗し、接続が終了する可能性がありました。 場合によっては、監査対象のトラフィックに非常に大きなメッセージが含まれていると、接続の監査で問題が発生する可能性がありました。 この場合、監査は失敗し、接続は終了しました。 また、「Failed to send request to audit writer service;」というメッセージが表示され、システムログに追加されました。 この問題は、RDP セッションホストと RDP クライアントホストの間で画像データがコピーされた場合など、主に RDP クリップボード転送に影響を与えました。 この問題は、単一転送の制限を 128 メガバイトに増やすことで緩和され、圧縮されていない 4K 32bpp イメージを RDP にコピーできるようになりました。また、ロギングが改善され、この制限により接続が閉じられたかどうかを判断できるようになりました。	PAM-16379
ウェルカムウィザードの最後の手順でサーバー証明書または秘密鍵を設定すると、エラーが発生して失敗しました。 Web サーバーの証明書と秘密鍵は、ウェルカムウィザードを終了する前の最後のステップで構成できますが、エラーが原因で、カスタムの証明書と鍵のペアを設定することも、自動生成されたものを表示することもできませんでした。これは修正されました。	PAM-16282
場合によっては、LDAP 接続が短期間で蓄積されることがありました。 Open LDAP 接続は、匿名バインドが使用された場合など、いくつかのケースで蓄積される可能性がありました。 この理由は、不適切な内部キャッシュでした。 これは修正されました。	PAM-16198

API のヘルス ステータス情報が最新ではありませんでした。 SPS 6.13.0 にアップグレードした後、{{/api/health-status}} 情報が更新されませんでした。 これは修正されました。	PAM-16197
特定のサーバーからの SSH SFTP ファイル転送が失敗する場合がありました。 SFTP プロトコルを使用して特定のサーバーからファイルを転送すると、パケットサイズの制限が原因で失敗する場合がありました。 この場合、「Invalid packet length;」というメッセージが表示され、システムログに書き込まれました。 これらのサーバーとの相互運用性は、サーバーの制限と一致するようにパケットサイズの制限を増やすことで改善されました。	PAM-16188
5.0.11 から 6.0.12 にアップグレードした後、無効な nodeid.json が原因で SPS が起動に失敗しました。 アップグレードは正常に終了しますが、システムを起動する前に SPS が停止します。 Web UI が「Firmware is starting up, please wait...」でスタックし、画面の最後のメッセージに「Fatal error: could not start core firmware because makeworld has failed」と表示されました。 この問題は修正されました。	PAM-16172
ログインオプション ページは、何も変更または表示する権限を持たないユーザーにも表示されました。 この問題は修正され、［Login options］ページはアクセス許可を持つユーザーにのみ表示され、読み取り専用モードが追加されました。	PAM-16125
検索ページのタイムラインでセッション データを視覚化しようとすると、タイムラインに含まれるセッションの開始時間属性が欠落している場合、UI に「InternalError 」が表示されました。 SPS 検索 UI は、検索ページの日付フィルターによって指定された時間範囲内のタイムラインチャートでセッションメタデータを視覚化する機能を提供します。 タイムラインを構築するために、検索ページの日付フィルターで指定された特定の時間範囲に該当するセッションが収集されます。 残念ながら、セッションの開始時刻プロパティが欠落している場合があります。 この場合、セッションがタイムラインに含まれていると、UI に「InternalError 」が表示されました。 この問題を解決するために、開始時間属性が指定されていないセッションはタイムラインに含まれないようにしました。	PAM-16086
Gateway authentication、4-eyes、Active connections は、Web インターフェイスでは使用できませんでした。	PAM-16029

認証エラーが原因で、Web インターフェイスで Gateway authentication、4-eyes、Active connections のページを使用できませんでした。 この問題は修正されました。	
UI は、ecdsa-sha2-nistp384、ecdsa-sha2-nistp521 ホスト キーアルゴリズムを受け入れませんでした。 SSH オプションページで、ホスト キーアルゴリズムフィールドを ecdsa-sha2-nistp384 または ecdsa-sha2-nistp521 に設定することは、クライアント側とサーバー側では不可能でした。 この問題は修正されました。	PAM-15959
コミットログが必要な場合、［Quick Connection Setup］の構成を完了できませんでしたが、そのダイアログはキャンセルされました。 この問題は修正されました。コミットログをキャンセルすると、［Quick Connection Setup］構成の ［Review］ページが表示されます。	PAM-15913
暗号化された sudo-iolog セッションは、復号化キーなしで再生できました。 ユーザーは暗号化された sudo-iolog セッションの復号化キーを持っていませんでしたが、スクリーンショットとビデオを検査することができました。 この問題は修正されました。 現在、暗号化された sudo-iolog セッションは、復号化キーなしでは再生できません。	PAM-15862
TLS が構成されている場合、一部の Mssql 接続が失敗しました。 TLS が構成されている場合、Windows または Linux で実行されているクライアントからの Mssql 接続が失敗する可能性がありました。 Windows では、タイミング関連の問題により、Microsoft コマンドラインツールが複数のフラグメントで送信された TDS メッセージを解析できなかったため、接続が失敗する可能性がありました。 Linux では、OpenSSL 1.1.1 以降がインストールされていると、接続が失敗する可能性がありました。これは、Microsoft コマンドラインツールが TLS v1.3 のサポートを誤って提供したためです。 現在、TDS プロトコルの制限により、この TLS バージョンは使用できません。 両方の問題が修正されました。 TDS プロトコルに適切なサポートが実装されるまで、TLS v1.3 のネゴシエーションは一時的に無効になっています。 さらに、TLS ハンドシェーク中に初期パケット サイズが増加しました。	PAM-15839
ボールトの詳細情報ボックスの幅が小さすぎて読めませんでした。 情報ボックスの幅が修正され、読みやすくなりました。	PAM-15825
ユーザーは、サポートされているすべての証明書をトラストストアにアップロードできませんでした。	PAM-15822

一部の証明書は表示されず、ユーザーはそれらをトラスト ストアにアップロードできませんでした。 この問題は修正されました。	
［Disk fill-up prevention］は、アクティブな接続を停止しませんでした。 エラーが発生したため、［Disk fill-up prevention］のしきい値に達した後、アクティブな接続が停止されませんでした。 これは修正されました。	PAM-15785
RDP セッションの「Accepted」の判定が、誤って「Rejected」になることがありました。 まれに、複数の TCP 接続を使用して RDP セッションが確立され、中間接続に失敗すると、同じセッション内の後続の接続が受け入れられた場合でも、セッションの UI 検索ページに「Rejected」ステータスが表示されました。 これは、最終セッション判定を正しく表示することで修正されました。	PAM-15616
SPS は、pubkey 認証を使用する openssh 8.5 以降のクライアントをサポートしてませんでした。 openssh 8.5 以降、pubkey 署名アルゴリズムに関連するいくつかの変更がありました。 したがって、クライアントは、サポートされているサーバー署名アルゴリズムを含むサーバーからのメッセージを待ちます。 このメッセージがない場合、クライアントは接続を閉じました。 これは修正され、SPS は openssh 8.5 以降のクライアントで pubkey 認証をサポートするようになりました。	PAM-15596
エラーテンプレートの編集時に、ロゴを変更しました。 その後、ロゴを再度変更し、この変更をキャンセルしたところ、ロードがスタックしました。 この問題は修正され、ファイルが選択されている場合にのみロードが表示されるようになりました。	PAM-15588
アプリスイッチャーの使用時に構成ロックが解除されませんでした。 ユーザーが構成ロックを保持している間にアプリスイッチャーを使用した場合、ロックが解除されず、別のユーザーが SPS を構成できませんでした。	PAM-15562
再起動後、tsadaemon のトレースバックをしました。 openssl-ts ツールには既知のバグがあり、タイムスタンプ要求中に終了すると、シリアルファイルが破損する可能性があります。 この修正により、この状況が回避され、フェイルセーフモードでシリアルファイルが処理されます。	PAM-15401
アップグレード後に、ディスク領域がいっぱいになるのを防ぐことができます。 SPS 6.10.0 では、ディスクスペースフィルアップ防止に変更が導入され、構成されたディスク スペース フィルアップ防止値に加えて、+3 GB の空きディス	PAM-15005

ク スペースが必要になりました。 アップグレード前の事前チェックで新しいルールが使用されなかったため、事前チェックが成功しても、アップグレードと再起動後にディスク フィルアップ防止がトリガーされるという状況が発生する可能性があります。 この状況を回避するために、新しいルールでディスク容量を確認するように事前チェックが変更されました。	
iolog セッションでは、［Terminate］ボタンが Safeguard Desktop Player から削除されました。 場合によっては、iolog セッションの再生中に Safeguard Desktop Player に機能しない［Terminate］ボタンが表示されることがありました。 この問題は修正されました。 iolog セッションの終了はサポートされていないため、iolog セッションの［Terminate］ボタンが削除されました。	PAM-14611
PDF を生成せずに失敗したレポートを削除すると、内部サーバーエラーが発生する場合がありました。 レポートの PDF 作成中にエラーが発生する場合がありました。［Reporting］>［Download Reports］ページでそのようなレポートを削除しようとすると、SPS が存在しない PDF を削除しようとしたため、内部サーバーエラーが発生しました。 この問題は修正され、失敗したレポートを削除できるようになりました。	PAM-13632
SPS 検索 UI の高度な検索フィルターで、非推奨の「psm.index_status」フィールドに、INDEXING_ABORTED インデックスステータスのセッションを検索するための有効なオプションがありませんでした。 「recording.index_status」フィールドに INDEXING_ABORTED という新しいインデックスステータスが導入されたとき、廃止されたフィールド「psm.index_status」には、INDEXING_ABORTED インデックスステータスのセッションを検索するためのオプションが用意されていませんでした。 その結果、INDEXING_ABORTED ステータスのセッションは、「psm.index_status」フィールドで検索できませんでした。 これは、値「7」を有効なオプションとして「psm.index_status」フィールドに追加することで修正されました。これは、「recording.index_status」フィールドの INDEXING_ABORTED ステータスの値にマップされます。	PAM-12584
RDP ログオンにより、すべての接続が終了する可能性があります。 まれに、ドメインユーザーが SPS を介してドメインに参加している RDP サーバーに正常にログインすると、すべての RDP 接続が終了する可能性があります。 この場合、コアファイルも生成されます。 この問題は主に、透過的な接続、または SPS が RD ゲートウェイとして機能している接続、および SPNEGO	388421

ベースの NLA 認証中にサーバーが特定の不適切な方法で動作していた接続に影響を与えました。 これは修正され、非標準のサーバーの動作が適切に処理されるようになり、影響を受けた接続が通過するようになりました。	
NFS マウントのデフォルトのタイムアウトを使用します。 以前は、NFS タイムアウトはデフォルト値の 60 秒ではなく、15 秒に設定されていました。 これは修正され、デフォルト値が使用されるようになりました。	389010
アップグレード前に Elasticsearch の再インデックス作成が完了していない場合、データが失われる可能性があるアップグレード シナリオがありました。この問題は解決されました。	392760
セッションが終了した場合、［Search］ページのセッション詳細ビューの［Monitoring Info］>［Verdict］フィールドの下に、次のメッセージが表示されました："Terminated by a content policy“　同じメッセージが、角かっこで囲まれた値”ACCEPT_TERMINATED“の横にある”Advanced Search recording.verdict“フィルター候補リストにも見つかりました。 このテキストの問題は、セッションがコンテンツポリシーだけでなくユーザーによっても終了される可能性があるため、誤解を招くことでした。 "ACCEPT_TERMINATED" recording.verdict メッセージが "Terminated by user or content policy" に修正されました。 このメッセージは、コンテンツポリシーだけでなく、ユーザーもセッションを終了できることを反映しています。	340185
“Four Eyes Authorizers”サブチャプターを含むレポートを生成するときに、“Four-eyes Authorizers”のないセッションがあった場合、値の円グラフに“-1”が表示されました。 同様に、ユーザー名が不明な場合、“Top 10 username/four-eyes authorizer ...”のサブチャプターでは、“-1”が値を表示していました。 “-1”は未知のデータを表す直感的な値ではないため、“n/a”に置き換えられました。	340215
テキスト入力フィールドは、SSH アルゴリズムおよび TLS 暗号文字列に対して短すぎる場合があります。 ［SSH Control］>［Settings］ページでアルゴリズムを指定すると、テキスト入力フィールドに 150 文字を超えるテキストを入力できませんでした。“MSSQL”、“RDP”、“Telnet”、および“VNC ”［Control］>［Settings］ページでは、［Cipher strength］フィールドも同じ制限の影響を受けていました。	340518

この問題は修正されました。 SSH アルゴリズムの制限は 512 文字に、TLS 暗号文字列の制限は 4096 文字に引き上げられました。	
トラストストアで、ユーザーが何かを証明書のアップロードフィールドにドラッグアンドドロップし始めると、テキストフィールドに小さなオーバーレイが表示されました。 ユーザーが気が変わってそこにファイルをドロップしなかった場合、このオーバーレイは動かなくなりました。 ［Audit keystore］＞［Add new key］（アップロード-key component）でも同じ問題が発生しました。 ドラッグ アンドドロップは、ドラッグイベントがページを離れるか、間違ったターゲットにドロップされたときに、証明書のアップロードとキーのアップロードのドラッグ状態でスタックしなくなりました。	340528
2022 年 1 月 11 日の Windows 更新プログラムをインストールした後、RDP 接続が失敗することがあります。 CVE-2022-21857 に対する保護を含む 2022 年 1 月 11 日の Windows 更新プログラムまたはそれ以降の Windows 更新プログラムをインストールした後、次の条件が当てはまる場合、RDP 接続は失敗しました。 • 信頼関係を持つ複数のドメイン（ドメイン A と B など） • RDP 接続が透過的であったか、SPS がリモート デスクトップゲートウェイとして機能 • NTLM 認証は、［Require domain member-ship］が有効な状態で設定 • SPS はドメイン A • 対象のサーバーとユーザーはドメイン B これらの場合、システム ログに次の行が表示されました："DC refused user authentication;" この問題は修正されました。NTLM 認証プロセスが改善され、新しいセキュリティチェックで動作するようになりました。	340538
/api/audit/sessions/<session-id>/screenshots/_generate および /api/audit/sessions/<session-id>/video/ _generate を使用して、REST API 経由で MSSQL セッションにビデオおよびスクリーンショットファイルを生成しようとする場合、それぞれエンドポイントを使用すると、インデクサーは、スクリーンショットとビデオファイルの生成が MSSQL セッションでサポートされていないことをユーザーに通知する代わりに、ジョブを受け入れました。	340553

これは修正されました。 現在、ユーザーが REST API を介して MSSQL セッションのスクリーンショットまたはビデオを生成しようとすると、REST API で 400 ContentGenerationNotSupported エラーが発生します。	
多数のゲートウェイ認証により、すべての接続が終了する可能性があります。 場合によっては、非常に多数のゲートウェイ認証の後、影響を受けるプロトコルのすべての接続が、double-free issue により終了する可能性があります。 これらのケースでは、コアファイルも生成され、スタックダンプがシステムログに書き込まれました。 この問題は主に HTTP 接続に影響し、SPS がリモートデスクトップゲートウェイとして機能している RDP 接続にも影響がありました。 この問題は修正されました。	340554
分析スコア関連フィールド（ホスト ログイン、ログイン時間、キーストローク、マウスまたはウィンドウ タイトル) で［Search］ページの下の SPS UI のセッションを並べ替えようとすると、選択した分析フィールドのデータがセッションにない場合、SPS の REST API 受信した検索クエリが無効であることを示す誤った“ 400 NotParsableQuery ”エラーを返しました。 これは現在修正されており、分析スコア関連のフィールドでデータが利用できない場合でも、並べ替えは失敗しません。	340583
開始日または終了日フィールドに月の部分が含まれていない ISO-8061 日付形式を使用して SPS REST API からレポートを生成しようとすると、エラーが返されます。 開始日または終了日のフィールドパラメーターに有効な ISO 8061 日付形式を指定して SPS レポート生成 API エンドポイント（/api/reports）にリクエストを送信すると、日付フィールドの 1 つに次の日付が含まれている場合、SPS はエラーメッセージで応答します。 月の部分はありません。 この結果、レポートの生成は開始されません。 これは修正され、ユーザーは SPS REST API の開始日フィールドと終了日フィールドで、以前のすべての形式と ISO 8061 形式で日付を指定できるようになりました。 これは、ISO 日付パーサーを導入し、古い日付パーサーも保持することによって達成されました。 これで、SPS は目的の日付の間でレポート生成を正常に実行します。	340592
開始日または終了日フィールドに週番号を含む ISO-8061 日付形式（2022-W37-1 など）を使用して SPS REST API からレポートを生成しようとすると、エラーメッセージが表示されました。 開始日または終了日のフィールドパラメーターに週番号を含む有効な ISO 8061 日付形式でレポート生成 API エンドポイント（/api/reports）にリクエストを送	340607

信すると、SPS は 400 "InvalidDate" エラーで応答しました。 この結果、レポートの生成が開始されませんでした。 これは修正され、ユーザーは SPS REST API の開始日フィールドと終了日フィールドで、以前のすべての形式と ISO 8061 形式で日付を指定できるようになりました。 修正には、ISO 日付パーサーの導入と、古い日付パーサーの保持も含まれていました。 SPS は、目的の日付の間でレポート生成を正常に実行するようになりました。	
ユーザーが集中検索展開でアーカイブされたセッション監査証跡をダウンロードしようとすると、SPS が監査証跡を見つけることができず、ユーザーがブラウザーで新しいタブを開くときにエラー メッセージが表示されるため、ダウンロードが失敗する可能性があります。 集中検索展開で SPS からアーカイブされた監査証跡をダウンロードしようとすると、ブラウザーで新しいタブを開くときにエラーメッセージが返されました。 これは、SPS が中央検索ノードのローカルコンテンツサービスを介して監査証跡ファイルを取得しようとしたことが原因でしたが、特定の監査証跡は、特定の記録されたセッションがあったミニオンノードのコンテンツサービスを介してのみ利用可能であったため、成功しませんでした。 この問題は修正されました。 ユーザーが中央検索ノードからアーカイブされた証跡をダウンロードしようとすると、SPS はセッションが記録されたミニオンノードのコンテンツサービスに接続します。	340626
接続ポリシーごとのアクセス許可で手動バックアップ、リストア、またはアーカイブ操作を開始しようとすると、アクセス許可エラーが発生します。 プロトコル内のいくつかの選択された接続ポリシー（ただし、そのプロトコルのすべての接続ポリシーではない）に対してのみ読み取りおよび書き込み/実行のアクセス許可を持っているユーザーが、そのような接続ポリシーのバックアップ、リストア、またはアーカイブ操作を手動で開始しようとすると、操作を開始できず、”Permission error / Access denied to object; object='/config/scb//connections/connection[@id = '...']', access='write'“という許可エラーが表示されました。 . この問題は修正されました。 これでユーザーは、読み取りおよび書き込み/実行アクセス許可が付与されたすべての接続ポリシーのバックアップ、リストア、およびアーカイブ操作を開始できるようになりました。	380785
［Indexer policy］フィールドは、インデクサーポリシーの値が選択されていない場合でも、［Next］ボタンを使用できました。	387412

［Indexer policy］フィールドでは、［Quick Connection Setup］でインデックス作成が有効になっている場合に、インデクサーポリシー値を設定する必要があります。	
"Status"が"Enabled"の場合、ユーザーは［X.509 editing］を保存できましたが、トラストストアを選択しませんでした。 ［X.509 login method form］＞［Trust store］フィールドで'required'の検証が欠落していた問題を修正しました。 現在、ユーザーは［Trust store］が選択されていないとフォームを送信できません。	387447
一部の SSH ホストキーが一覧表示されませんでした。 SSH ターゲットサーバーが"ecdsa-sha2-nistp384"または"ecdsa-sha2-nistp521" ホスト キーを使用した場合、これらのキーは［SSH Control］＞［Server host keys］の下に表示されませんでした。 このエラーは修正されました。 結果として、上記のキー タイプは REST API の /api/ssh-host-keys エンドポイントでもサポートされます。	388635
プロトコル TLS 1.0 および 1.1 はインデクサーサービスから削除されました。外部インデクサーの TCP ポートでは、TLS 1.2 以降のプロトコルバージョンのみがサポートされます。	389039
［User & Access Control］＞［Login Options］＞［Manage AD/LDAP servers］で既に指定されているトラストストアの場合に AD/LDAP サーバーを編集すると、"None"ステータスの"Certificate"を選択できたにもかかわらず、エラーが変更のコミット中に発生しました。 この問題は修正されました。 AD/LDAP サーバーを編集するときに、変更を保存してコミットできます。	400763
REST API の FQDN で“_”文字が許可されていても、ユーザーは Web UI を使用してこの名前のサーバーを設定できませんでした。 UI での FQDN 検証が修正されました。	400765
MSSQL インバンドターゲットサーバーが存在しない場合に、誤解を招くエラーメッセージ表示されました。 インバンドターゲット選択を使用する MSSQL 接続で、ターゲットサーバーのホスト名の DNS 名前解決が失敗すると、誤解を招くログインエラーメッセージ"Gateway authentication failed"が MSSQL クライアントに表示されました。この場合、トレースバックもシステムログに書き込まれます。	404204

これらのエラーは修正され、名前解決が失敗したことを反映するようにエラーメッセージが更新されました。	
Citrix ICA 接続の監査証跡とイベントの日付が正しくない場合があります。 影響を受ける SPS バージョンで記録された ICA 監査証跡のチャネルは、将来、具体的には 2035-10-29T06:32:22 (UTC) 以降に記録されているように見える可能性があります。 監査証跡は監査イベントの基礎としても機能するため、検索インターフェイスに表示される日付と時刻も、影響を受けるセッションでは正しくありません。 この機能が監査証跡に対して有効になっている場合、タイムスタンプ機関によって作成されたデジタル署名されたタイムスタンプは影響を受けません。 また、新しいチャネルの開始を示すレコードだけが、監査証跡に間違ったタイムスタンプを持っています。 キーストローク、マウス イベント、グラフィック コンテンツなど、実際に監査されたトラフィックは、内部的に正しいタイムスタンプを持っていますが、インデックス作成中の自動時刻修正により、これらのイベントも誤って調整された日付と時刻で表示されます。 監査証跡の記録エラーが修正され、SPS は新しいチャネルを開くときに監査証跡に正しい時刻を書き込むようになりました。 ただし、影響を受ける SPS で記録された既存の監査証跡は、依然として誤った日付と時刻を示します。	405227
インストール後、RAID ステータスは表示されませんでした。 以前は、Safeguard 4000 のインストールの最後に、RAID 同期ステータスが表示されませんでした。 この問題は修正されました。	407479
ユーザーが「読み取りおよび書き込み/実行」権限を持っていても、ローカル管理者を除くすべてのユーザーのポリシー編集ページからアイコンが消えていました。 Web ユーザー インターフェイスでは、ユーザーが特定ページの「読み取りと書き込み/実行」権限を持っていたとしても、ローカル管理者を除くほとんどのユーザーのポリシー編集ページから、行の追加と削除などのアイコンが消えていました。 これは修正され、ポリシーまたは構成の編集に必要なアクセス許可を持つすべてのユーザーに対してアイコンが再び表示されるようになりました。	410511
エージェント認証を使用して SPS 経由でリモート SSH サーバーに接続すると、SSH 接続が終了することがありました。 SSH 認証ポリシーでリレー認証方式が「公開鍵」に設定され「エージェント」が選択された状態で、ユーザーが SSH エージェントに少なくとも 1 つの RSA キーを持つ複数のキーを持っている場合、SPS を介してリモート SSH サーバー	412260

に接続すると、すべての SSH 接続が 終了しました。 この場合、コアファイルが生成され、バックトレースがシステムログに書き込まれます。 この問題は修正され、複数のキーを含む SSH エージェントによる認証が再び可能になりました。	
サポートされているアップグレードパスが拡張されました。つまり、SPS 7LTS バージョンを次のバージョンから直接アップグレードできます。 • SPS6.0.0 • SPS 6.0.11 以降のパッチ バージョン • SPS 6.9.4 以降のパッチ バージョン • SPS 6.11、SPS 6.12、SPS 6.13 • 7LTS の以前のバージョンの SPS 7 製品ライン (7.x) の機能バージョンへのアップグレードは、SPS 7LTS のすべてのパッチバージョンおよび以前の SPS 7 機能バージョンからサポートされています。	412382
ハードウェアのインストールでデータの移行に失敗しました。 以前は、停止したコアファームウェアによってターゲットマシンがセカンダリ状態になり、データがターゲットマシンにコピーされなかったため、ハードウェアインストールでのデータ移行が失敗していました。 この問題は修正されました。 現在、すべてのハードウェアで、データ移行により、ターゲットマシンが確実にプライマリ状態になります。	412397

表 6 ：SPS7.0.5LTS で解決した脆弱性（CVE）

Resolved Issue	Issue ID
avahi:	CVE-2023-38469 CVE-2023-38470 CVE-2023-38471 CVE-2023-38472 CVE-2023-38473
bind9:	CVE-2023-4408 CVE-2023-50387 CVE-2023-50868 CVE-2023-5517 CVE-2023-6516
curl:	CVE-2023-38546

	CVE-2023-46218
freerdp2:	CVE-2017-2834 CVE-2017-2835 CVE-2017-2836 CVE-2017-2837 CVE-2017-2838 CVE-2017-2839 CVE-2019-17177 CVE-2020-11042 CVE-2020-11044 CVE-2020-11045 CVE-2020-11046 CVE-2020-11047 CVE-2020-11048 CVE-2020-11049 CVE-2020-11058 CVE-2020-11095 CVE-2020-11096 CVE-2020-11097 CVE-2020-11098 CVE-2020-11099 CVE-2020-11521 CVE-2020-11522 CVE-2020-11523 CVE-2020-11524 CVE-2020-11525 CVE-2020-11526 CVE-2020-13396 CVE-2020-13397 CVE-2020-13398 CVE-2020-15103 CVE-2020-4030 CVE-2020-4031 CVE-2020-4032 CVE-2020-4033 CVE-2021-41159 CVE-2021-41160 CVE-2022-24882 CVE-2022-24883

	CVE-2022-39282 CVE-2022-39283 CVE-2022-39316 CVE-2022-39317 CVE-2022-39318 CVE-2022-39319 CVE-2022-39320 CVE-2022-39347 CVE-2022-41877 CVE-2023-39350 CVE-2023-39351 CVE-2023-39352 CVE-2023-39353 CVE-2023-39354 CVE-2023-39356 CVE-2023-40181 CVE-2023-40186 CVE-2023-40188 CVE-2023-40567 CVE-2023-40569 CVE-2023-40589
glibc:	CVE-2023-4806 CVE-2023-4813
gnutls28:	CVE-2023-5981 CVE-2024-0553
jinja2:	CVE-2020-28493 CVE-2024-22195
krb5:	CVE-2023-36054
less:	CVE-2022-48624
libssh:	CVE-2023-48795 CVE-2023-6004 CVE-2023-6918
ibuv1:	CVE-2024-24806
libvpx:	CVE-2023-44488 CVE-2023-5217
libx11:	CVE-2023-43785 CVE-2023-43786 CVE-2023-43787
libxml2:	CVE-2024-25062

libxpm:	CVE-2023-43786 CVE-2023-43787 CVE-2023-43788 CVE-2023-43789
linux:	CVE-2021-4001 CVE-2023-0597 CVE-2023-1206 CVE-2023-31083 CVE-2023-31085 CVE-2023-3212 CVE-2023-34319 CVE-2023-37453 CVE-2023-3772 CVE-2023-3863 CVE-2023-39189 CVE-2023-39192 CVE-2023-39193 CVE-2023-4132 CVE-2023-4194 CVE-2023-42752 CVE-2023-42753 CVE-2023-42754 CVE-2023-42755 CVE-2023-42756 CVE-2023-45863 CVE-2023-45871 CVE-2023-4622 CVE-2023-4623 CVE-2023-4881 CVE-2023-4921 CVE-2023-5178 CVE-2023-51781 CVE-2023-5717 CVE-2023-6040 CVE-2023-6606 CVE-2023-6915 CVE-2023-6931 CVE-2023-6932 CVE-2024-0565

	CVE-2024-0646
nghttp2:	CVE-2023-44487
open-vm-tools:	CVE-2023-34058 CVE-2023-34059
openjdk-lts:	CVE-2023-22081 CVE-2024-20918 CVE-2024-20919 CVE-2024-20921 CVE-2024-20926 CVE-2024-20945 CVE-2024-20952
openldap:	CVE-2023-2953
openssh:	CVE-2021-41617 CVE-2023-48795 CVE-2023-51385
openssl:	CVE-2023-3446 CVE-2023-3817 CVE-2023-5678 CVE-2024-0727
pam:	CVE-2024-22365
perl:	CVE-2023-47038
php7.4:	CVE-2023-3823 CVE-2023-3824
pillow:	CVE-2023-44271 CVE-2023-50447
postfix:	CVE-2023-51764
postgresql-12:	CVE-2023-5868 CVE-2023-5869 CVE-2023-5870 CVE-2024-0985
procps:	CVE-2023-4016
python-cryptography:	CVE-2023-23931
python-urllib3:	CVE-2023-43804 CVE-2023-45803
python3.8:	CVE-2023-40217
rabbitmq-server:	CVE-2023-46118
samba:	CVE-2023-4091 CVE-2023-4154

	CVE-2023-42669
shadow	CVE-2023-4641
sqlite3:	CVE-2023-7104
strongswan:	CVE-2023-41913
tar:	CVE-2023-39804
tiff:	CVE-2022-40090 CVE-2023-1916 CVE-2023-3576 CVE-2023-52356 CVE-2023-6228 CVE-2023-6277
vim:	CVE-2022-1725 CVE-2022-1771 CVE-2022-1897 CVE-2022-2000 CVE-2022-3234 CVE-2022-3256 CVE-2022-3324 CVE-2022-3352 CVE-2022-3520 CVE-2022-3591 CVE-2022-3705 CVE-2022-4292 CVE-2022-4293 CVE-2023-46246 CVE-2023-4733 CVE-2023-4735 CVE-2023-4750 CVE-2023-4751 CVE-2023-4752 CVE-2023-4781 CVE-2023-48231 CVE-2023-48233 CVE-2023-48234 CVE-2023-48235 CVE-2023-48236 CVE-2023-48237 CVE-2023-5344 CVE-2023-5441

	CVE-2023-5535

表６：SPS7.0.4LTS で解決した脆弱性（CVE）

Resolved Issue	Issue ID
avahi:	CVE-2023-1981
bind9:	CVE-2023-2828
cups:	CVE-2023-32324 CVE-2023-34241
curl:	CVE-2023-28321 CVE-2023-28322
glib2.0:	CVE-2023-24593 CVE-2023-25180 CVE-2023-29499 CVE-2023-32611 CVE-2023-32636 CVE-2023-32643 CVE-2023-32665
libcap2:	CVE-2023-2602 CVE-2023-2603
libssh:	CVE-2023-1667 CVE-2023-2283
libx11:	CVE-2023-3138
linux:	CVE-2020-36691 CVE-2022-0168 CVE-2022-1184 CVE-2022-27672 CVE-2022-4269 CVE-2023-0461 CVE-2023-1075 CVE-2023-1118 CVE-2023-1380 CVE-2023-1611 CVE-2023-1670 CVE-2023-1859 CVE-2023-2124 CVE-2023-2612 CVE-2023-30456 CVE-2023-3090

	CVE-2023-3111 CVE-2023-3141 CVE-2023-31436 CVE-2023-32233 CVE-2023-32629 CVE-2023-3390 CVE-2023-35001
ncurses:	CVE-2021-39537 CVE-2022-29458 CVE-2023-29491
nghttp2:	CVE-2020-11080
open-vm-tools:	CVE-2023-20867
openjdk-lts:	CVE-2023-22006 CVE-2023-22036 CVE-2023-22041 CVE-2023-22045 CVE-2023-22049 CVE-2023-25193
openssh:	CVE-2020-14145 CVE-2023-38408
openssl:	CVE-2022-4304 CVE-2023-2650
perl:	CVE-2023-31484
php7.4:	CVE-2023-3247
postgresql-12:	CVE-2023-2454 CVE-2023-2455 CVE-2023-39417
python3.8:	CVE-2023-24329
requests:	CVE-2023-32681
samba:	CVE-2022-2127 CVE-2023-34966 CVE-2023-34967 CVE-2023-34968
sysstat:	CVE-2023-33204
tiff:	CVE-2022-48281 CVE-2023-25433 CVE-2023-26965 CVE-2023-26966

	CVE-2023-2908 CVE-2023-3316 CVE-2023-3618 CVE-2023-38288 CVE-2023-38289
vim:	CVE-2022-2208 CVE-2022-2210 CVE-2022-2257 CVE-2022-2264 CVE-2022-2284 CVE-2022-2285 CVE-2022-2286 CVE-2022-2287 CVE-2022-2289 CVE-2022-2598 CVE-2022-3016 CVE-2022-3037 CVE-2022-3099 CVE-2023-2609 CVE-2023-2610

表２：SPS7.0.3LTS で解決した脆弱性（CVE）

Resolved Issue	**Issue ID**
cloud-init:	CVE-2023-1786
erlang:	CVE-2022-37026
freetype:	CVE-2023-2004
ipmitool:	CVE-2020-5208
ldb:	CVE-2023-0614
libwebp:	CVE-2023-1999
libxml2:	CVE-2023-28484 CVE-2023-29469
linux:	CVE-2022-3108 CVE-2022-3903 CVE-2023-1281 CVE-2023-1829 CVE-2023-26545
openjdk-lts:	CVE-2023-21930 CVE-2023-21937

	CVE-2023-21938 CVE-2023-21939 CVE-2023-21954 CVE-2023-21967 CVE-2023-21968
openssl:	CVE-2023-0464 CVE-2023-0465 CVE-2023-0466
samba:	CVE-2023-0614 CVE-2023-0922
sqlparse:	CVE-2023-30608
sudo:	CVE-2023-2848 CVE-2023-28486 CVE-2023-28487
vim:	CVE-2021-4166 CVE-2021-4192 CVE-2021-4193 CVE-2022-0213 CVE-2022-0261 CVE-2022-0318 CVE-2022-0319 CVE-2022-0351 CVE-2022-0359 CVE-2022-0361 CVE-2022-0368 CVE-2022-0408 CVE-2022-0413 CVE-2022-0443 CVE-2022-0554 CVE-2022-0572 CVE-2022-0629 CVE-2022-0685 CVE-2022-0714 CVE-2022-0729 CVE-2022-1629 CVE-2022-1674 CVE-2022-1720 CVE-2022-1733 CVE-2022-1735

	CVE-2022-1785 CVE-2022-1796 CVE-2022-1851 CVE-2022-1898 CVE-2022-1927 CVE-2022-1942 CVE-2022-1968 CVE-2022-2124 CVE-2022-2125 CVE-2022-2126 CVE-2022-2129 CVE-2022-2175 CVE-2022-2183 CVE-2022-2206 CVE-2022-2207 CVE-2022-2304 CVE-2022-2344 CVE-2022-2345 CVE-2022-2571 CVE-2022-2581 CVE-2022-2845 CVE-2022-2849 CVE-2022-2923 CVE-2022-2946 CVE-2022-2980

表 2 ：SPS7.0.2.1LTS で解決した脆弱性（CVE）

Resolved Issue	**Issue ID**
bind9:	CVE-2022-3094
curl:	CVE-2022-43552 CVE-2023-23916 CVE-2023-27533 CVE-2023-27534 CVE-2023-27535 CVE-2023-27536 CVE-2023-27538
gnutls28:	CVE-2023-0361
heimdal:	CVE-2021-44758

	CVE-2022-3437 CVE-2022-42898 CVE-2022-44640 CVE-2022-45142
krb5:	CVE-2021-36222 CVE-2021-37750 CVE-2022-42898
ldb:	CVE-2021-3670 CVE-2022-32745
libksba:	CVE-2022-47629
libxpm:	CVE-2022-44617 CVE-2022-46285 CVE-2022-4883
linux:	CVE-2022-2663 CVE-2022-3061 CVE-2022-3545 CVE-2022-3643 CVE-2022-41218 CVE-2022-4139 CVE-2022-42896 CVE-2022-43945 CVE-2022-45934 CVE-2022-47520 CVE-2023-0266 CVE-2023-0461
net-snmp:	CVE-2022-4479 CVE-2022-44792 CVE-2022-44793
nss:	CVE-2023-0767
openjdk-lts:	CVE-2023-21835 CVE-2023-21843
openssl:	CVE-2022-4304 CVE-2022-4450 CVE-2022-0215 CVE-2023-0286
pam:	CVE-2022-28321
php7.4:	CVE-2022-31631 CVE-2023-0567

	CVE-2023-0568 CVE-2023-0662
postgresql-12:	CVE-2022-41862
protobuf:	CVE-2021-22570 CVE-2022-1941
python-future:	CVE-2022-40899
python-urllib3:	CVE-2021-33503
python3.8:	CVE-2023-24329
rsync:	CVE-2022-29154
samba:	CVE-2022-3437 CVE-2022-3796 CVE-2022-37966 CVE-2022-37967 CVE-2022-38023 CVE-2022-42898 CVE-2022-44640 CVE-2022-45141
setuptools:	CVE-2022-40897
sudo:	CVE-2023-22809
systemd:	CVE-2022-3821 CVE-2022-4415
tar:	CVE-2022-48303
tiff:	CVE-2023-0795 CVE-2023-0796 CVE-2023-0797 CVE-2023-0798 CVE-2023-0799 CVE-2023-0800 CVE-2023-0801 CVE-2023-0802 CVE-2023-0803 CVE-2023-0804
vim:	CVE-2022-0392 CVE-2022-0417 CVE-2022-47024 CVE-2023-0049 CVE-2023-0054 CVE-2023-0288

	CVE-2023-0433 CVE-2023-1170 CVE-2023-1175 CVE-2023-1264

表 3：SPS7.0LTS で解決した脆弱性（CVE）

Resolved Issue	Issue ID
bash:	CVE-2019-18276
bind9:	CVE-2021-25220
cifs-utils:	CVE-2020-14342 CVE-2021-20208 CVE-2022-27239 CVE-2022-29869
cups:	CVE-2019-8842 CVE-2020-10001 CVE-2022-26691
curl:	CVE-2022-22576 CVE-2022-27774 CVE-2022-27775 CVE-2022-27776 CVE-2022-27781 CVE-2022-27782
cyrus-sasl2:	CVE-2022-24407
dbus:	CVE-2020-35512
dpkg:	CVE-2022-1664
expat:	CVE-2021-45960 CVE-2021-46143 CVE-2022-22822 CVE-2022-22823 CVE-2022-22824 CVE-2022-22825 CVE-2022-22826 CVE-2022-22827 CVE-2022-23852 CVE-2022-23990 CVE-2022-25235 CVE-2022-25236 CVE-2022-25313

	CVE-2022-25314 CVE-2022-25315
fribidi:	CVE-2022-25308 CVE-2022-25309 CVE-2022-25310
glibc:	CVE-2016-10228 CVE-2019-25013 CVE-2020-27618 CVE-2020-29562 CVE-2020-6096 CVE-2021-27645 CVE-2021-3326 CVE-2021-35942 CVE-2021-3999 CVE-2022-23218 CVE-2022-23219
gzip:	CVE-2022-1271
klibc:	CVE-2021-31870 CVE-2021-31871 CVE-2021-31872 CVE-2021-31873
libinput:	CVE-2022-1215
libsepol:	CVE-2021-36084 CVE-2021-36085 CVE-2021-36086 CVE-2021-36087
libxml2:	CVE-2022-23308 CVE-2022-29824
linux:	CVE-2020-27820 CVE-2021-26401 CVE-2022-0001 CVE-2022-0435 CVE-2022-0492 CVE-2022-0516 CVE-2022-0847 CVE-2022-1016 CVE-2022-1055 CVE-2022-1116

	CVE-2022-23960 CVE-2022-25636 CVE-2022-26490 CVE-2022-27223 CVE-2022-27666 CVE-2022-29581
mysql-8.0:	CVE-2022-21412 CVE-2022-21413 CVE-2022-21414 CVE-2022-21415 CVE-2022-21417 CVE-2022-21418 CVE-2022-21423 CVE-2022-21425 CVE-2022-21427 CVE-2022-21435 CVE-2022-21436 CVE-2022-21437 CVE-2022-21438 CVE-2022-21440 CVE-2022-21444 CVE-2022-21451 CVE-2022-21452 CVE-2022-21454 CVE-2022-21457 CVE-2022-21459 CVE-2022-21460 CVE-2022-21462 CVE-2022-21478
nginx:	CVE-2020-11724 CVE-2020-36309 CVE-2021-3618
nss:	CVE-2020-25648
openjdk-lts:	CVE-2022-21248 CVE-2022-21277 CVE-2022-21282 CVE-2022-21283 CVE-2022-21291

	CVE-2022-21293 CVE-2022-21294 CVE-2022-21296 CVE-2022-21299 CVE-2022-21305 CVE-2022-21340 CVE-2022-21341 CVE-2022-21360 CVE-2022-21365 CVE-2022-21366 CVE-2022-21426 CVE-2022-21434 CVE-2022-21443 CVE-2022-21476 CVE-2022-21496
openldap:	CVE-2022-29155
openssl:	CVE-2022-0778 CVE-2022-1292
pcre3:	CVE-2019-20838 CVE-2020-14155
php7.4:	CVE-2017-8923 CVE-2017-9118 CVE-2017-9119 CVE-2017-9120 CVE-2021-21707 CVE-2021-21708
postgresql-12:	CVE-2022-1552
python3.8:	CVE-2022-0391
redis:	CVE-2022-0543
rsync:	CVE-2018-25032
sqlite3:	CVE-2021-36690
tar:	CVE-2021-20193
tcpdump:	CVE-2018-16301 CVE-2020-8037
tiff:	CVE-2020-35522 CVE-2022-0561 CVE-2022-0562 CVE-2022-0865

	CVE-2022-0891
xz-utils:	CVE-2022-1271
zlib:	CVE-2018-25032

表 4：リリース 6.0.0 と 6.13.0 の間で解決した脆弱性（CVE）

Resolved Issue	**Issue ID**
apt:	CVE-2014-0487 CVE-2019-3462 CVE-2020-27350 CVE-2020-3810
avahi:	CVE-2021-3468
bash:	CVE-2019-18276
bind9:	CVE-2018-5738 CVE-2018-5740 CVE-2018-5743 CVE-2018-5744 CVE-2018-5745 CVE-2019-6465 CVE-2019-6471 CVE-2019-6477 CVE-2020-8616 CVE-2020-8617 CVE-2020-8618 CVE-2020-8619 CVE-2020-8620 CVE-2020-8621 CVE-2020-8622 CVE-2020-8623 CVE-2020-8624 CVE-2020-8625 CVE-2021-25214 CVE-2021-25215 CVE-2021-25216 CVE-2021-25219 CVE-2021-25220
bubblewrap:	CVE-2020-5291
busybox:	CVE-2011-5325 CVE-2017-15873

	CVE-2018-1000500 CVE-2018-1000517 CVE-2018-20679 CVE-2019-5747 CVE-2021-28831 CVE-2021-42374 CVE-2021-42378 CVE-2021-42379 CVE-2021-42380 CVE-2021-42381 CVE-2021-42382 CVE-2021-42384 CVE-2021-42385 CVE-2021-42386
bzip2:	CVE-2008-1372 CVE-2016-3189 CVE-2019-12900
cairo:	CVE-2018-19876
cifs-utils:	CVE-2020-14342 CVE-2021-20208 CVE-2022-27239 CVE-2022-29869
cloud-init:	CVE-2020-8632
cpio:	CVE-2015-1197 CVE-2016-2037 CVE-2021-38185
cron:	CVE-2017-9525
cryptsetup:	CVE-2016-4484 CVE-2020-14382 CVE-2021-4122
cups:	CVE-2018-4180 CVE-2018-4181 CVE-2018-4182 CVE-2018-4183 CVE-2018-4700 CVE-2018-6553 CVE-2019-2228 CVE-2019-8675

	CVE-2019-8696 CVE-2019-8842 CVE-2020-10001 CVE-2020-3898 CVE-2022-26691
curl:	CVE-2018-0500 CVE-2018-1000120 CVE-2018-1000121 CVE-2018-1000122 CVE-2018-1000300 CVE-2018-1000301 CVE-2018-14618 CVE-2018-16839 CVE-2018-16840 CVE-2018-16842 CVE-2018-16890 CVE-2019-3822 CVE-2019-3823 CVE-2019-5435 CVE-2019-5436 CVE-2019-5481 CVE-2019-5482 CVE-2020-8169 CVE-2020-8177 CVE-2020-8231 CVE-2020-8284 CVE-2020-8285 CVE-2020-8286 CVE-2021-22876 CVE-2021-22890 CVE-2021-22898 CVE-2021-22924 CVE-2021-22925 CVE-2021-22946 CVE-2021-22947 CVE-2022-22576 CVE-2022-27774 CVE-2022-27775

	CVE-2022-27776 CVE-2022-27781 CVE-2022-27782
cyrus-sasl2:	CVE-2019-19906 CVE-2022-24407
db5.3:	CVE-2019-8457
dbus:	CVE-2019-12749 CVE-2020-12049 CVE-2020-35512
dpkg:	CVE-2022-1664
e2fsprogs:	CVE-2019-5094 CVE-2019-5188
elfutils:	CVE-2018-16062 CVE-2018-16402 CVE-2018-16403 CVE-2018-18310 CVE-2018-18520 CVE-2018-18521 CVE-2019-7146 CVE-2019-7148 CVE-2019-7149 CVE-2019-7150 CVE-2019-7664 CVE-2019-7665
expat:	CVE-2018-20843 CVE-2019-15903 CVE-2021-45960 CVE-2021-46143 CVE-2022-22822 CVE-2022-22823 CVE-2022-22824 CVE-2022-22825 CVE-2022-22826 CVE-2022-22827 CVE-2022-23852 CVE-2022-23990 CVE-2022-25235 CVE-2022-25236

	CVE-2022-25313 CVE-2022-25314 CVE-2022-25315
ffmpeg:	CVE-2018-12458 CVE-2018-12459 CVE-2018-12460 CVE-2018-13300 CVE-2018-13301 CVE-2018-13302 CVE-2018-13303 CVE-2018-13304 CVE-2018-14394 CVE-2018-14395 CVE-2018-15822 CVE-2019-1000016 CVE-2019-11338 CVE-2019-11339 CVE-2019-12730 CVE-2019-13312 CVE-2019-17539 CVE-2019-17542 CVE-2019-9718 CVE-2019-9721 CVE-2020-12284 CVE-2020-13904
file:	CVE-2018-10360 CVE-2019-18218 CVE-2019-8904 CVE-2019-8905 CVE-2019-8906 CVE-2019-8907
freerdp2:	CVE-2020-11097 CVE-2020-15103 CVE-2020-4030
freetype:	CVE-2018-6942 CVE-2020-15999
fuse:	CVE-2018-10906
gettext:	CVE-2018-18751

glib2.0:	CVE-2012-3524 CVE-2019-12450 CVE-2020-6750 CVE-2021-2721 CVE-2021-27218 CVE-2021-27219 CVE-2021-28153
glibc:	CVE-2016-10228 CVE-2016-10739 CVE-2018-11236 CVE-2018-11237 CVE-2018-19591 CVE-2019-19126 CVE-2019-25013 CVE-2019-6488 CVE-2019-7309 CVE-2019-9169 CVE-2020-27618 CVE-2020-29562 CVE-2020-6096 CVE-2021-27645 CVE-2021-3326 CVE-2021-35942 CVE-2021-3999 CVE-2022-23218 CVE-2022-23219
gnupg2:	CVE-2018-12020
gnutls28:	CVE-2019-3829 CVE-2019-3836 CVE-2020-13777 CVE-2020-24659 CVE-2021-20231 CVE-2021-20232
graphite2:	CVE-2016-1977 CVE-2016-2790 CVE-2016-2791 CVE-2016-2792
grub2:	CVE-2020-10713

	CVE-2020-14308 CVE-2020-14309 CVE-2020-14310 CVE-2020-14311 CVE-2020-15705 CVE-2020-15706 CVE-2020-15707
gzip:	CVE-2022-1271
heimdal:	CVE-2018-16860 CVE-2019-12098 CVE-2019-14870
icu:	CVE-2018-18928 CVE-2020-10531 CVE-2021-30535
isc-dhcp:	CVE-2017-3144 CVE-2018-5732 CVE-2018-5733 CVE-2021-25217
jinja2:	CVE-2019-10906
json-c:	CVE-2020-12762
klibc:	CVE-2021-31870 CVE-2021-31871 CVE-2021-31872 CVE-2021-31873
krb5:	CVE-2007-0956 CVE-2007-1216 CVE-2014-9422 CVE-2018-20217 CVE-2018-5729 CVE-2018-5730 CVE-2020-28196
lcms2:	CVE-2018-16435
ldb:	CVE-2019-3824 CVE-2020-25718 CVE-2020-27840 CVE-2021-20277
libdbi-perl:	CVE-2014-10402
libgcrypt20:	CVE-2018-0495

	CVE-2019-13627 CVE-2021-33560 CVE-2021-40528
libgd2:	CVE-2017-6363 CVE-2018-1000222 CVE-2018-14553 CVE-2018-5711 CVE-2019-11038 CVE-2019-6977 CVE-2019-6978 CVE-2021-38115 CVE-2021-40145
libinput:	CVE-2022-1215
libjpeg-turbo:	CVE-2018-19664 CVE-2018-20330 CVE-2020-13790
libmspack:	CVE-2018-14679 CVE-2018-14680 CVE-2018-14681 CVE-2018-14682 CVE-2018-18584 CVE-2018-18585 CVE-2018-18586
libonig:	CVE-2019-13224 CVE-2019-13225 CVE-2019-16163 CVE-2019-19012 CVE-2019-19203 CVE-2019-19204 CVE-2019-19246
libpcap:	CVE-2018-16301 CVE-2019-15165
libpng1.6:	CVE-2014-0333 CVE-2018-13785 CVE-2019-7317
librabbitmq:	CVE-2019-18609
libseccomp:	CVE-2019-9893
libsepol:	CVE-2021-36084

	CVE-2021-36085 CVE-2021-36086 CVE-2021-36087
libssh2:	CVE-2019-3855 CVE-2019-3856 CVE-2019-3857 CVE-2019-3858 CVE-2019-3859 CVE-2019-3860 CVE-2019-3861 CVE-2019-3862 CVE-2019-3863
libtasn1-6:	CVE-2018-1000654
libtirpc:	CVE-2016-4429 CVE-2018-14622
libwebp:	CVE-2018-25009 CVE-2018-25010 CVE-2018-25011 CVE-2018-25012 CVE-2018-25013 CVE-2018-25014 CVE-2020-36328 CVE-2020-36329 CVE-2020-36330 CVE-2020-36331 CVE-2020-36332
libx11:	CVE-2018-14598 CVE-2018-14599 CVE-2018-14600 CVE-2020-14344 CVE-2020-14363 CVE-2021-31535
libxkbcommon:	CVE-2018-15853 CVE-2018-15854 CVE-2018-15855 CVE-2018-15856 CVE-2018-15857 CVE-2018-15858

	CVE-2018-15859 CVE-2018-15861 CVE-2018-15862 CVE-2018-15863 CVE-2018-15864
libxml2:	CVE-2016-9318 CVE-2017-16932 CVE-2017-18258 CVE-2018-14404 CVE-2018-14567 CVE-2018-9251 CVE-2019-19956 CVE-2019-20388 CVE-2020-24977 CVE-2020-7595 CVE-2021-3516 CVE-2021-3517 CVE-2021-3518 CVE-2021-3537 CVE-2021-3541 CVE-2022-23308 CVE-2022-29824
libxslt:	CVE-2019-11068 CVE-2019-13117 CVE-2019-13118 CVE-2019-18197
libzstd:	CVE-2021-24031 CVE-2021-24032
linux:	CVE-2017-5715 CVE-2018-6559 CVE-2018-9363 CVE-2019-12614 CVE-2019-14895 CVE-2019-14896 CVE-2019-14897 CVE-2019-14901 CVE-2019-15098 CVE-2019-15791

	CVE-2019-15792 CVE-2019-15793 CVE-2019-15794 CVE-2019-16089 CVE-2019-17052 CVE-2019-17053 CVE-2019-17054 CVE-2019-17055 CVE-2019-17056 CVE-2019-17666 CVE-2019-19050 CVE-2019-19076 CVE-2019-19078 CVE-2019-19332 CVE-2019-19449 CVE-2019-19642 CVE-2019-19770 CVE-2019-3016 CVE-2019-3460 CVE-2019-3874 CVE-2019-9857 CVE-2020-0543 CVE-2020-11494 CVE-2020-11884 CVE-2020-11935 CVE-2020-12351 CVE-2020-12352 CVE-2020-12888 CVE-2020-13143 CVE-2020-14351 CVE-2020-14386 CVE-2020-16119 CVE-2020-16120 CVE-2020-24490 CVE-2020-24586 CVE-2020-24587 CVE-2020-24588 CVE-2020-26139 CVE-2020-26141

	CVE-2020-26145 CVE-2020-26147 CVE-2020-26541 CVE-2020-27170 CVE-2020-27171 CVE-2020-27777 CVE-2020-27820 CVE-2020-28374 CVE-2020-29372 CVE-2020-36385 CVE-2020-4788 CVE-2020-8694 CVE-2020-8835 CVE-2021-1052 CVE-2021-1053 CVE-2021-26401 CVE-2021-27363 CVE-2021-27364 CVE-2021-27365 CVE-2021-29154 CVE-2021-29650 CVE-2021-33200 CVE-2021-33909 CVE-2021-3428 CVE-2021-3444 CVE-2021-3492 CVE-2021-3653 CVE-2021-3656 CVE-2021-3759 CVE-2021-4002 CVE-2021-40490 CVE-2021-4083 CVE-2021-4155 CVE-2022-0001 CVE-2022-0185 CVE-2022-0330 CVE-2022-0435 CVE-2022-0492 CVE-2022-0516

	CVE-2022-0847 CVE-2022-1016 CVE-2022-1055 CVE-2022-1116 CVE-2022-22942 CVE-2022-23960 CVE-2022-25636 CVE-2022-26490 CVE-2022-27223 CVE-2022-27666 CVE-2022-29581
lxml:	CVE-2020-27783 CVE-2021-28957 CVE-2021-43818
lz4:	CVE-2019-17543 CVE-2021-3520
mysql-5.7:	CVE-2016-9843 CVE-2018-0739 CVE-2018-2755 CVE-2018-2758 CVE-2018-2759 CVE-2018-2761 CVE-2018-2762 CVE-2018-2766 CVE-2018-2767 CVE-2018-2769 CVE-2018-2771 CVE-2018-2773 CVE-2018-2775 CVE-2018-2776 CVE-2018-2777 CVE-2018-2778 CVE-2018-2779 CVE-2018-2780 CVE-2018-2781 CVE-2018-2782 CVE-2018-2784 CVE-2018-2786

	CVE-2018-2787 CVE-2018-2810 CVE-2018-2812 CVE-2018-2813 CVE-2018-2816 CVE-2018-2817 CVE-2018-2818 CVE-2018-2819 CVE-2018-2839 CVE-2018-2846 CVE-2018-3054 CVE-2018-3056 CVE-2018-3058 CVE-2018-3060 CVE-2018-3061 CVE-2018-3062 CVE-2018-3064 CVE-2018-3065 CVE-2018-3066 CVE-2018-3070 CVE-2018-3071 CVE-2018-3077 CVE-2018-3081 CVE-2018-3133 CVE-2018-3143 CVE-2018-3144 CVE-2018-3155 CVE-2018-3156 CVE-2018-3161 CVE-2018-3162 CVE-2018-3171 CVE-2018-3173 CVE-2018-3174 CVE-2018-3185 CVE-2018-3187 CVE-2018-3200 CVE-2018-3247 CVE-2018-3251 CVE-2018-3276

	CVE-2018-3277 CVE-2018-3278 CVE-2018-3282 CVE-2018-3283 CVE-2018-3284 CVE-2019-14775 CVE-2019-2911 CVE-2019-2914 CVE-2019-2920 CVE-2019-2922 CVE-2019-2923 CVE-2019-2924 CVE-2019-2938 CVE-2019-2946 CVE-2019-2948 CVE-2019-2950 CVE-2019-2957 CVE-2019-2960 CVE-2019-2963 CVE-2019-2966 CVE-2019-2967 CVE-2019-2968 CVE-2019-2969 CVE-2019-2974 CVE-2019-2982 CVE-2019-2991 CVE-2019-2993 CVE-2019-2997 CVE-2018-3276 CVE-2018-3277 CVE-2018-3278 CVE-2018-3282 CVE-2018-3283 CVE-2018-3284 CVE-2019-14775 CVE-2019-2911 CVE-2019-2914 CVE-2019-2920 CVE-2019-2922

	CVE-2019-2923 CVE-2019-2924 CVE-2019-2938 CVE-2019-2946 CVE-2019-2948 CVE-2019-2950 CVE-2019-2957 CVE-2019-2960 CVE-2019-2963 CVE-2019-2966 CVE-2019-2967 CVE-2019-2968 CVE-2019-2969 CVE-2019-2974 CVE-2019-2982 CVE-2019-2991 CVE-2019-2993 CVE-2019-2997 CVE-2019-2998 CVE-2019-3003 CVE-2019-3004 CVE-2019-3009 CVE-2019-3011 CVE-2019-3018 CVE-2020-14539 CVE-2020-14540 CVE-2020-14547 CVE-2020-14550 CVE-2020-14553 CVE-2020-14559 CVE-2020-14568 CVE-2020-14575 CVE-2020-14576 CVE-2020-14586 CVE-2020-14591 CVE-2020-14597 CVE-2020-14619 CVE-2020-14620 CVE-2020-14623

	CVE-2020-14624 CVE-2020-14631 CVE-2020-14632 CVE-2020-14633 CVE-2020-14634 CVE-2020-14641 CVE-2020-14643 CVE-2020-14651 CVE-2020-14654 CVE-2020-14656 CVE-2020-14663 CVE-2020-14672 CVE-2020-14678 CVE-2020-14680 CVE-2020-14697 CVE-2020-14702 CVE-2020-14765 CVE-2020-14769 CVE-2020-14771 CVE-2020-14773 CVE-2020-14775 CVE-2020-14776 CVE-2020-14777 CVE-2020-14785 CVE-2020-14786 CVE-2020-14789 CVE-2020-14790 CVE-2020-14791 CVE-2020-14793 CVE-2020-14794 CVE-2020-14800 CVE-2020-14804 CVE-2020-14809 CVE-2020-14812 CVE-2020-14814 CVE-2020-14821 CVE-2020-14827 CVE-2020-14828 CVE-2020-14829

	CVE-2020-14830 CVE-2020-14836 CVE-2020-14837 CVE-2020-14838 CVE-2020-14839 CVE-2020-14844 CVE-2020-14845 CVE-2020-14846 CVE-2020-14848 CVE-2020-14852 CVE-2020-14853 CVE-2020-14860 CVE-2020-14861 CVE-2020-14866 CVE-2020-14867 CVE-2020-14868 CVE-2020-14869 CVE-2020-14870 CVE-2020-14873 CVE-2020-14878 CVE-2020-14888 CVE-2020-14891 CVE-2020-14893 CVE-2020-2570 CVE-2020-2572 CVE-2020-2573 CVE-2020-2574 CVE-2020-2577 CVE-2020-2579 CVE-2020-2584 CVE-2020-2588 CVE-2020-2589 CVE-2020-2627 CVE-2020-2660 CVE-2020-2679 CVE-2020-2686 CVE-2020-2694 CVE-2020-2759 CVE-2020-2760

	CVE-2020-2762 CVE-2020-2763 CVE-2020-2765 CVE-2020-2780 CVE-2020-2804 CVE-2020-2812 CVE-2020-2892 CVE-2020-2893 CVE-2020-2895 CVE-2020-2896 CVE-2020-2897 CVE-2020-2898 CVE-2020-2901 CVE-2020-2903 CVE-2020-2904 CVE-2020-2921 CVE-2020-2923 CVE-2020-2924 CVE-2020-2925 CVE-2020-2926 CVE-2020-2928 CVE-2020-2930 CVE-2021-2002 CVE-2021-2010 CVE-2021-2011 CVE-2021-2021 CVE-2021-2022 CVE-2021-2024 CVE-2021-2031 CVE-2021-2032 CVE-2021-2036 CVE-2021-2038 CVE-2021-2046 CVE-2021-2048 CVE-2021-2056 CVE-2021-2058 CVE-2021-2060 CVE-2021-2061 CVE-2021-2065

	CVE-2021-2070 CVE-2021-2072 CVE-2021-2076 CVE-2021-2081 CVE-2021-2087 CVE-2021-2088 CVE-2021-2122 CVE-2021-2146 CVE-2021-2162 CVE-2021-2164 CVE-2021-2166 CVE-2021-2169 CVE-2021-2170 CVE-2021-2171 CVE-2021-2172 CVE-2021-2179 CVE-2021-2180 CVE-2021-2193 CVE-2021-2194 CVE-2021-2196 CVE-2021-2201 CVE-2021-2203 CVE-2021-2208 CVE-2021-2212 CVE-2021-2215 CVE-2021-2217 CVE-2021-2226 CVE-2021-2230 CVE-2021-2232 CVE-2021-2278 CVE-2021-2293 CVE-2021-2298 CVE-2021-2299 CVE-2021-2300 CVE-2021-2301 CVE-2021-2304 CVE-2021-2305 CVE-2021-2307 CVE-2021-2308

	CVE-2021-2339 CVE-2021-2340 CVE-2021-2342 CVE-2021-2352 CVE-2021-2354 CVE-2021-2356 CVE-2021-2357 CVE-2021-2367 CVE-2021-2370 CVE-2021-2372 CVE-2021-2374 CVE-2021-2383 CVE-2021-2384 CVE-2021-2385 CVE-2021-2387 CVE-2021-2389 CVE-2021-2390 CVE-2021-2399 CVE-2021-2402 CVE-2021-2410 CVE-2021-2417 CVE-2021-2418 CVE-2021-2422 CVE-2021-2424 CVE-2021-2425 CVE-2021-2426 CVE-2021-2427 CVE-2021-2429 CVE-2021-2437 CVE-2021-2440 CVE-2021-2441 CVE-2021-2478 CVE-2021-2479 CVE-2021-2481 CVE-2021-35546 CVE-2021-35575 CVE-2021-35577 CVE-2021-35584 CVE-2021-35591

	CVE-2021-35596 CVE-2021-35597 CVE-2021-35602 CVE-2021-35604 CVE-2021-35607 CVE-2021-35608 CVE-2021-35610 CVE-2021-35612 CVE-2021-35613 CVE-2021-35622 CVE-2021-35623 CVE-2021-35624 CVE-2021-35625 CVE-2021-35626 CVE-2021-35627 CVE-2021-35628 CVE-2021-35630 CVE-2021-35631 CVE-2021-35632 CVE-2021-35633 CVE-2021-35634 CVE-2021-35635 CVE-2021-35636 CVE-2021-35637 CVE-2021-35638 CVE-2021-35639 CVE-2021-35640 CVE-2021-35641 CVE-2021-35642 CVE-2021-35643 CVE-2021-35644 CVE-2021-35645 CVE-2021-35646 CVE-2021-35647 CVE-2021-35648 CVE-2022-21245 CVE-2022-21249 CVE-2022-21253 CVE-2022-21254

	CVE-2022-21256 CVE-2022-21264 CVE-2022-21265 CVE-2022-21270 CVE-2022-21301 CVE-2022-21302 CVE-2022-21303 CVE-2022-21304 CVE-2022-21339 CVE-2022-21342 CVE-2022-21344 CVE-2022-21348 CVE-2022-21351 CVE-2022-21358 CVE-2022-21362 CVE-2022-21367 CVE-2022-21368 CVE-2022-21370 CVE-2022-21372 CVE-2022-21374 CVE-2022-21378 CVE-2022-21379 CVE-2022-21412 CVE-2022-21413 CVE-2022-21414 CVE-2022-21415 CVE-2022-21417 CVE-2022-21418 CVE-2022-21423 CVE-2022-21425 CVE-2022-21427 CVE-2022-21435 CVE-2022-21436 CVE-2022-21437 CVE-2022-21438 CVE-2022-21440 CVE-2022-21444 CVE-2022-21451 CVE-2022-21452

	CVE-2022-21454 CVE-2022-21457 CVE-2022-21459 CVE-2022-21460 CVE-2022-21462 CVE-2022-21478
ncurses:	CVE-2019-17594 CVE-2019-17595
net-snmp:	CVE-2018-18065 CVE-2019-20892 CVE-2020-15861 CVE-2020-15862
nettle:	CVE-2021-20305 CVE-2021-3580
nfs-utils:	CVE-2019-3689
nghttp2:	CVE-2018-1000168
nginx:	CVE-2019-9511 CVE-2019-9513 CVE-2019-9516 CVE-2020-11724 CVE-2020-36309 CVE-2021-23017 CVE-2021-3618
nss:	CVE-2018-12384 CVE-2018-18508 CVE-2019-11719 CVE-2019-11727 CVE-2019-11745 CVE-2019-17023 CVE-2020-12399 CVE-2020-12400 CVE-2020-12401 CVE-2020-12402 CVE-2020-12403 CVE-2020-25648 CVE-2020-6829 CVE-2021-43527
ntp:	CVE-2016-1549

	CVE-2018-7170 CVE-2018-7182 CVE-2018-7183 CVE-2018-7184 CVE-2018-7185 CVE-2019-8936
opencv:	CVE-2016-1516 CVE-2016-1517 CVE-2017-1000450 CVE-2017-12597 CVE-2017-12598 CVE-2017-12599 CVE-2017-12600 CVE-2017-12601 CVE-2017-12602 CVE-2017-12603 CVE-2017-12604 CVE-2017-12605 CVE-2017-12606 CVE-2017-12862 CVE-2017-12863 CVE-2017-12864 CVE-2017-14136 CVE-2017-17760 CVE-2017-18009 CVE-2018-5268 CVE-2018-5269
openldap:	CVE-2019-13057 CVE-2019-13565 CVE-2020-12243 CVE-2020-25692 CVE-2020-25709 CVE-2020-25710 CVE-2020-36221 CVE-2020-36222 CVE-2020-36223 CVE-2020-36224 CVE-2020-36225

	CVE-2020-36226 CVE-2020-36227 CVE-2020-36228 CVE-2020-36229 CVE-2020-36230 CVE-2021-27212 CVE-2022-29155 CVE-2018-15473 CVE-2018-20685 CVE-2019-6109 CVE-2019-6111 CVE-2021-28041
openssl:	CVE-2018-0732 CVE-2018-0734 CVE-2018-0735 CVE-2018-0737 CVE-2019-1543 CVE-2019-1547 CVE-2019-1549 CVE-2019-1551 CVE-2019-1563 CVE-2020-1967 CVE-2020-1971 CVE-2021-23840 CVE-2021-23841 CVE-2021-3449 CVE-2021-3711 CVE-2021-3712 CVE-2022-0778 CVE-2022-1292
p11-kit:	CVE-2020-29361 CVE-2020-29362 CVE-2020-29363
pam:	CVE-2009-0887
pango1.0:	CVE-2011-0020 CVE-2011-0064 CVE-2019-1010238
patch:	CVE-2018-1000156

	CVE-2019-13636 CVE-2019-13638
pcre3:	CVE-2019-20838 CVE-2020-14155
perl:	CVE-2018-12015 CVE-2018-18311 CVE-2018-18312 CVE-2020-10543 CVE-2020-10878 CVE-2020-12723
php-pear:	CVE-2020-2894 CVE-2020-28948 CVE-2020-28949 CVE-2020-36193 CVE-2021-32610
postgresql-10:	CVE-2018-1058 CVE-2020-14349 CVE-2020-14350 CVE-2020-1720 CVE-2020-25694 CVE-2020-25695 CVE-2020-25696 CVE-2021-23214 CVE-2021-23222 CVE-2021-32027 CVE-2021-32028 CVE-2021-32029 CVE-2021-3393 CVE-2021-3449 CVE-2022-1552
postgresql-common:	CVE-2019-3466
procps:	CVE-2017-18078 CVE-2018-1123 CVE-2018-1124 CVE-2018-1125 CVE-2018-1126
python-babel:	CVE-2021-20095
python-crypto:	CVE-2018-6594

python-cryptography:	CVE-2018-10903 CVE-2020-25659
python-urllib3:	CVE-2019-11236 CVE-2020-26137
python2.7:	CVE-2013-1752 CVE-2018-1000802 CVE-2018-14647 CVE-2019-16056 CVE-2019-17514 CVE-2019-18348 CVE-2019-20907 CVE-2019-5010 CVE-2019-9636 CVE-2019-9674 CVE-2019-9948 CVE-2020-26116 CVE-2020-8492 CVE-2021-3177
pyyaml:	CVE-2020-14343 CVE-2020-1747
qtbase-opensource-src:	CVE-2015-9541 CVE-2018-15518 CVE-2018-19870 CVE-2018-19873 CVE-2020-0569 CVE-2020-0570 CVE-2021-38593
rabbitmq-server:	CVE-2016-9877 CVE-2017-4965 CVE-2017-4966 CVE-2017-4967 CVE-2021-22116
redis:	CVE-2018-11218 CVE-2018-11219 CVE-2022-0543
requests:	CVE-2018-18074
rpcbind:	CVE-2015-7236 CVE-2017-8779

rsync:	CVE-2018-25032 CVE-2018-5764
samba:	CVE-2016-2124 CVE-2018-1050 CVE-2018-1057 CVE-2018-10858 CVE-2018-10918 CVE-2018-10919 CVE-2018-1139 CVE-2018-1140 CVE-2018-14629 CVE-2018-16841 CVE-2018-16851 CVE-2018-16852 CVE-2018-16853 CVE-2018-16857 CVE-2018-16860 CVE-2019-10197 CVE-2019-10218 CVE-2019-12435 CVE-2019-12436 CVE-2019-14833 CVE-2019-14861 CVE-2019-14870 CVE-2019-14902 CVE-2019-14907 CVE-2019-19344 CVE-2019-3870 CVE-2019-3880 CVE-2020-10700 CVE-2020-10704 CVE-2020-10730 CVE-2020-10745 CVE-2020-10760 CVE-2020-14303 CVE-2020-14318 CVE-2020-14323 CVE-2020-14383

	CVE-2020-1472 CVE-2020-25717 CVE-2020-25718 CVE-2020-25719 CVE-2020-25721 CVE-2020-25722 CVE-2021-20254 CVE-2021-23192 CVE-2021-3738 CVE-2021-43566 CVE-2021-44142 CVE-2022-0336
screen:	CVE-2021-26937
smarty3:	CVE-2009-5052 CVE-2009-5053 CVE-2017-1000480 CVE-2018-16831
sqlite3:	CVE-2018-8740 CVE-2019-19242 CVE-2019-19244 CVE-2019-19603 CVE-2019-19645 CVE-2019-19880 CVE-2019-19923 CVE-2019-19924 CVE-2019-19925 CVE-2019-5018 CVE-2019-5827 CVE-2019-8457 CVE-2019-9936 CVE-2019-9937 CVE-2020-11655 CVE-2020-13434 CVE-2020-13435 CVE-2020-13630 CVE-2020-13631 CVE-2020-13632 CVE-2020-15358

	CVE-2020-9327 CVE-2021-36690
strongswan:	CVE-2014-9221 CVE-2015-8023 CVE-2018-10811 CVE-2018-16151 CVE-2018-16152 CVE-2018-17540 CVE-2018-5388 CVE-2021-41990 CVE-2021-41991 CVE-2021-45079
sudo:	CVE-2019-14287 CVE-2021-23239 CVE-2021-3156
sysstat:	CVE-2018-19416 CVE-2018-19517 CVE-2019-16167 CVE-2019-19725
systemd:	CVE-2018-15686 CVE-2018-15687 CVE-2018-15688 CVE-2018-16864 CVE-2018-16865 CVE-2018-20839 CVE-2018-6954 CVE-2019-15718 CVE-2019-3842 CVE-2019-3843 CVE-2019-3844 CVE-2019-6454 CVE-2020-13529 CVE-2020-1712 CVE-2021-33910 CVE-2021-3997
tar:	CVE-2018-20482 CVE-2019-9923 CVE-2021-20193

tcpdump:	CVE-2017-16808 CVE-2018-16301 CVE-2020-8037
tiff:	CVE-2018-10963 CVE-2018-12900 CVE-2018-17000 CVE-2018-17100 CVE-2018-17101 CVE-2018-18557 CVE-2018-18661 CVE-2018-19210 CVE-2018-8905 CVE-2019-14973 CVE-2019-6128 CVE-2020-19143 CVE-2020-35522 CVE-2020-35523 CVE-2020-35524 CVE-2022-0561 CVE-2022-0562 CVE-2022-0865 CVE-2022-0891
util-linux:	CVE-2018-7738 CVE-2021-3995 CVE-2021-3996
vim:	CVE-2019-12735 CVE-2021-3770 CVE-2021-3778 CVE-2021-3796 CVE-2021-3872 CVE-2021-3903 CVE-2021-3927 CVE-2021-3928 CVE-2021-3974 CVE-2021-3984 CVE-2021-4019 CVE-2021-4069
walinuxagent:	CVE-2019-0804

wget:	CVE-2018-0494 CVE-2018-20483 CVE-2019-5953
xfsprogs:	CVE-2012-2150
xz-utils:	CVE-2022-1271
zlib:	CVE-2018-25032

6 既知の問題

以下は、リリース時に存在が確認されている、サードパーティ製品に起因する問題を含む問題のリストです。

表 5：一般的な既知の問題

Known Issue

⚠	注意：バージョン 7.0 LTS にアップグレードした後、SPS には新しいライセンスが必要です。 特定の機能が利用できないことによるダウンタイムの可能性を回避するには、アップグレードを開始する前に、7.0 LTS の有効な SPS ライセンスがあることを確認してください。 次のようにアップグレードします。 1. 現在のライセンスで 7.0 LTS へのアップグレードを実行します。 2. SPS ライセンスを 7.0 LTS に更新します。 7.0 LTS の新しい SPS ライセンスについては、弊社カスタマーポータルにお問い合わせください。

inWebo、Okta、または One Identity Starling 2FA プラグインを使用する場合、TLS バージョン 1.3 はサポートされません。 ネゴシエーション中に SPS で TLS 1.2 が使用されるようにするには、TLS の最小バージョンと最大バージョンを次のように指定します。

- TLS の最小バージョンとして、TLS バージョン 1.2 を選択します。
- TLS の最大 バージョンとして、TLS バージョン 1.3 を選択します。

詳細については、管理者ガイドの「Verifying certificates with Certificate Authorities using trust stores」を参照してください。

アジア言語 (繁体字中国語、韓国語) での監査証跡の再生の精度が向上しました。 この変更により、SPS をバージョン 6.11.0 にアップグレードすると、すべてのセッションが再インデックス化され、再インデックス化の進行中は、検索インターフェイスのセッションが不完全になります。 このため、それに応じて SPS 6.11.0 へのアップグレードを計画してください。

レポートのサブチャプターが、以前に削除された接続ポリシーを参照している場合、レポートの生成に失敗することがあります。

SPS は、すべての接続ポリシーの接続に関する詳細情報を提供するレポートを作成できます。 このために、ユーザーはレポート設定ウィザードの**［Reporting］＞［Create & Manage Reports］**で接続のサブチャプターを追加できます。

レポートを正常に生成するには、参照されている接続ポリシーがアプライアンスに存在する必要があります。 ただし、接続のサブチャプターとして参照されている接続ポリシーを削除すると、レポートのサブチャプターを削除する必要があるという警告がユーザーに表示されません。そうしないと、後続のレポートの生成に失敗します。

これは、スケジュールされたレポートの生成にも影響します。

表 6 ：一般的な既知の問題

Known Issue	Issue ID
証明書の有効期限が切れると、外部インデクサーが切断されました。 外部インデクサー証明書が 800 日の制限で作成された SPS バージョン 6.0.4 または 6.4.0 以降の実行中に外部インデックス作成を有効にした場合にのみ、この問題の影響を受けます。	PAM-16883

7　システム要件

SPS 7.0 LTS をインストールする前に、システムが次のハードウェアおよびソフトウェアの最小要件を満たしていることを確認してください。

SPS アプライアンス は、すでにインストールされており、SPS ソフトウェア用に特化して構築されており、すぐに使用できます。 アプライアンスは、ハードウェア、オペレーティング システム、ソフトウェア の各レベルでシステムの安全性を確保するために、強化されています。

SPS を仮想アプライアンスとしてインストールするための要件については、次のドキュメントのいずれかを参照してください。

> **メモ**：仮想環境をセットアップするときは、CPU、メモリの可用性、I/O サブシステム、ネットワークインフラストラクチャなどの構成面を慎重に検討して、仮想レイヤーで必要なリソースが利用可能であることを確認してください。 仮想化環境の詳細については、「One Identity's Product Support Policies」を参照してください。

7.1　サポートされている Web ブラウザーとオペレーティング システム

> ⚠ **注意**：バージョン 6.13.0 以降、SPS は Internet Explorer 11 (IE11) をサポートしなくなりました。 SPS バージョン 6.12.0 およびそれ以前のバージョンは引き続き IE11 をサポートします。
> SPS バージョン 6.10 以降、ブラウザーで監査証跡を再生するために Microsoft Internet Explorer プラグイン用の Google WebM ビデオは必要ありません。 サポートされているブラウザーは次のとおりです。
>
> - Google Chrome
> - Firefox
> - Safari
> - Internet Explorer 11 (IE11) - SPS バージョン 6.12.0 までサポート
>
> SPS バージョン 6.9 以前のバージョンでは、SPS の Web インターフェイスは Internet Explorer と Microsoft Edge を一般的にサポートしていますが、監査証跡を再生するに

は、Internet Explorer 11 を使用し、Microsoft Internet Explorer プラグインとして Google WebM ビデオをインストールする必要があります。

Internet Explorer 11 またはサポートされている別のブラウザーをコンピューターにインストールできない場合は、Safeguard Desktop Player アプリケーションを使用してください。 詳細については、管理者ガイドおよび Safeguard Desktop Player ユーザー ガイドの「ブラウザーでの監査証跡の再生」を参照してください。

注意：SPS バージョン 4 F3 以降のバージョンは、IE9 および IE10 の公式サポートが 2016 年 1 月に終了したため、Internet Explorer 9 (IE9) および Internet Explorer 10 (IE10) をサポートしていません。

メモ：ブラウザーがサポートされていない場合、または JavaScript が無効になっている場合、SPS は警告メッセージを表示します。

メモ： SPS の Web インターフェイスを表示するために推奨される最小画面解像度は、14 インチワイドスクリーン（標準の 16:9 比率）ラップトップ画面で 1366 x 768 ピクセルです。これらの値以上の画面サイズと画面解像度は、Web インターフェイスの最適な表示を保証します。

サポートされているブラウザー

次のブラウザーがサポートされています。

- Mozilla Firefox（最新バージョン）
- Google Chrome
- Microsoft Edge（Microsoft Edge レガシはサポートされていません）

ブラウザーは、TLS で暗号化された HTTPS 接続、JavaScript、および Cookie をサポートする必要があります。 JavaScript と Cookie の両方が有効になっていることを確認します。

SPS Web インターフェイスには、TLS 暗号化と強力な暗号アルゴリズムを使用してのみアクセスできます。

複数のブラウザー ウィンドウまたはタブで Web インターフェイスを開くことはサポートされていません。

サポートされているオペレーティングシステム

次のオペレーティングシステムがサポートされています。

- Windows 2008 Server
- Windows 2012 Server
- Windows 2012 R2 Server
- Windows 2016
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Linux

7.2 Safeguard Desktop Player のシステム要件

Safeguard Desktop Player アプリケーションは、次のオペレーティング システムをサポートしています。

- Microsoft Windows：

  Windows 7 以降の 64 ビット バージョン。 グラフィック カードに適切なドライバをインストールします。

- Linux：

  RHEL 7、CentOS 7 以降。 Safeguard Desktop Player アプリケーションは、少なくとも libc6 バージョン 2.17 がインストールされている他のディストリビューションでも動作する可能性があります。

  ディストリビューションに応じて、次のパッケージをインストールする必要があります。

  - On Debian-based GNU/Linux:
    - libxcb-render-util0
    - libxcb-keysyms1
    - libxcb-image0
    - libxcb-randr0
    - libxcb-xkb1
    - libxcb-xinerama0

        - libxcb-icccm4
    - CentOS/Red Hat の場合:
        - xcb-util-renderutil
        - xcb-util-keysyms
        - xcb-util-image
- Mac:

  macOS Catalina 10.15 以降

  Safeguard Desktop Player アプリケーションをインストールするには、約 200MB のディスク容量と、再生される監査証跡を保存するために一時的に使用されるディスク容量が必要です。 一時ファイルのサイズは、再生された監査証跡のサイズによって異なります。

  ユーザー権限で Safeguard Desktop Player アプリケーションをインストールできます。

8 ハードウェア仕様

SPS アプライアンスは、標準のラック マウントに簡単に取り付けられる高性能でエネルギー効率が高く、信頼性の高いハードウェア上に構築されています。

表 7 : ハードウェア仕様

Product	Redundant PSU	Processor	Memory	Capacity	RAID	IPMI
Safeguard Sessions Appliance 3000	Yes	1x Intel Xeon E3-1275 v6 3.80GHz	2 x 16 GB	4x2 TB NLSAS	LSI MegaRAID SAS 9361-4i Single	Yes
Safeguard Sessions Appliance 3500	Yes	2x Intel Xeon Silver 4110 2.1GHz	8 x 8 GB	9x2 TB NLSAS	1 x Broadcom MegaRAID SAS 9361-16i + LSI Avago CacheVault Power Module 02 (CVPM02) Kit	Yes
Safeguard Sessions Appliance 4000	Yes	1x Intel Xeon Silver ICX 4310T @ 2.30GHz, 10C/20T	8 x 8 GB	4x20 TB SAS/SATA	1 x Broadcom 9560-8i RAID controller 1 x Broadcom CacheVault battery	Yes

Safeguard Sessions Appliance 3500 には、デュアルポート 10Gbit インターフェイスが装備されています。 このインターフェイスには、A と B のラベルが付いた SFP+ コネクタ (RJ-45 ではない) があり、ラベル 1 と 2 のイーサネット インターフェイスの右側にあります。 データ負荷が高い場合など、より高速な通信が必要な場合は、最大 2 つの 10Gbit ネットワーク カードを接続できます。 これらのカードは元のパッケージには同梱されていないため、別途購入する必要があります。

9　アップグレードとインストールの手順

SPS アプライアンス は、すでにインストールされており、SPS ソフトウェア用に特化して構築されており、すぐに使用できます。

SPS7.0.5LTS へのアップグレード手順

SPS 7.0.5LTS へのアップグレード手順については、「アップグレード ガイド」を参照してください。

> **メモ**：法的な理由により、外部インデクサーアプリケーションのインストールパッケージは、SPS の Web インターフェイスからのみ利用できます。 SPS バージョン 6.4 および 6.0.3 のリリース後、インストールパッケージは Web サイトから削除されます。

> ⚠ **注意**：6.10.0 以降、SPS は強化された SSL 設定に変更されました。 その結果、TLS セッションの確立中に、次の項目は安全とは見なされません。
>
> - 2048 ビット未満の RSA または DSA キー、または 224 ビット未満の ECC キーを持つ秘密キーおよび X.509 証明書
> - SHA-1 または MD5 ハッシュ アルゴリズムを使用する署名付きの証明書 (ルート CA 証明書以外)
>
> 強化された SSL 設定では、SPS は脆弱な証明書で保護されているリモートシステムに接続しません。
>
> SPS のコンフィグレーションの次のいずれかに、安全でない証明書、キー、または証明書チェーンが含まれている場合、SPS をアップグレードすることはできません。
>
> - SPS Web インターフェイス
> - 内部 CA 証明書
> - 接続ポリシーの TLS 設定
> - 外部 LDAP、SMTP、または Syslog 接続用のクライアント X.509 クレデンシャル
> - サーバー 外部 SMTP または Splunk サーバー用の X.509 証明書

- 外部インデクサー資格情報 (REST API 経由でのみ書き込み可能)
- 信頼できる CA リストと信頼ストアの CA 証明書

署名、タイムスタンプ、暗号化または復号化に使用される証明書とキーは、この変更の影響を受けないことに注意してください。

LTS リリースについて

これは長期サポート (LTS) リリースです。

長期サポートおよび機能リリースの完全な説明については、管理者ガイドを参照してください。

MBX ハードウェアに基づく物理アプライアンスがある場合

Pyramid ハードウェアで SPS を実行しておらず、次のいずれかに該当する場合、One Identity は SPS 7.0 LTS にアップグレードすることをお勧めします。

- 新しい機能のいずれかを利用したいと考えている場合
- 以前の機能リリースを実行している場合
- 以前の長期サポート リリースを実行している場合

Pyramid ハードウェアベースの物理アプライアンスがある場合

Pyramid ハードウェアで SPS を動作している場合は、SPS 7.0 LTS にアップグレードしないでください:

9.1 インストール成功の確認

［Basic Settings ］＞［System ］＞［Version details ］に移動し、SPS がファームウェアのバージョン 7.0 LTS を実行していることを確認します。 そうでない場合は、アップグレード プロセスが正常に完了せず、SPS がロールバックを実行して以前のファームウェア バージョンに戻したということです。 この場合、次の手順を実行します。

1. **［Basic Settings ］＞［Troubleshooting］＞［Create support bundle］**に移動し、**［Create support bundle ］**をクリックします。
2. 結果の ZIP ファイルを保存します。

3. 弊社サポートポータルにて、ファイルを送信してください。その内容を分析して、アップグレードが完了しなかった理由を調査し、問題の解決を支援します。

One Identity 社について

One Identity 社のソリューションは、アイデンティティの管理、特権アカウントの管理、アクセスの制御に必要とされる複雑で時間のかかるプロセスを排除します。One Identity 社のソリューションは、オンプレミス、クラウド、ハイブリッド環境における IAM の課題に対応しながら、ビジネスの俊敏性を向上させます。

お問い合わせ

ライセンス、サポート、更新などについては、こちらからお問い合わせください。

お問い合わせ

この資料についてご不明な点やお気づきの点などがございましたら、お問い合わせください。

ジュピターテクノロジー株式会社（Jupiter Technology Corp.）

URL：　https://www.jtc-i.co.jp/

購入前のお問い合わせ先：https://www.jtc-i.co.jp/contact/scontact.php

購入後のお問い合わせ先：https://www.jtc-i.co.jp/support/customerportal/

発行日 2024 年 4 月 15 日

本マニュアル原文 SPS 7.0 LTS Release Notes

ジュピターテクノロジー株式会社