Oracle® Solaris 11 セキュリティーコンプライアンスガイド

Part No: E53938
2014 年 7 月

ORACLE

目次

このドキュメントの使用

- **概要** – 指定されたセキュリティーベンチマークに対する Oracle Solaris システムのコンプライアンスを評価およびレポートする方法を説明します。
- **対象読者** – Oracle Solaris 11 システムのセキュリティーを評価するセキュリティー管理者と監査者。
- **必要な知識** – サイトのセキュリティー要件。

製品ドキュメントライブラリ

この製品に関する最新情報および既知の問題については、ドキュメントライブラリ (http://www.oracle.com/pls/topic/lookup?ctx=E56342) に記載されています。

Oracle サポートへのアクセス

Oracle のお客様は、My Oracle Support を通じて電子的なサポートを利用できます。詳細は、http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info を参照してください。聴覚に障害をお持ちの場合は、http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs を参照してください。

フィードバック

このドキュメントに関するフィードバックを http://www.oracle.com/goto/docfeedback からお聞かせください。

♦ ♦ ♦ 第 1 章

1 セキュリティー標準に対するコンプライアンスのレポート

この章では、セキュリティー標準 (*セキュリティーベンチマーク*や*セキュリティーポリシー*とも呼ばれる) に対する Oracle Solaris システムのコンプライアンスを評価およびレポートする方法を説明します。この章で扱う内容は、次のとおりです。

コンプライアンスについて

セキュリティー標準に準拠するシステムは、よりセキュアなコンピューティング環境を提供する上に、テスト、維持、および保護が容易になります。このリリースの Oracle Solaris には、Solaris セキュリティーベンチマークと PCI DSS (Payment Card Industry-Data Security Standard) という 2 つのセキュリティーベンチマークに対する Oracle Solaris システムのコンプライアンスを評価および報告するスクリプトが用意されています。

外部および内部のセキュリティーポリシーに対するシステムコンプライアンスをサポートするために構成の検証が重要です。ドキュメント、レポート、および検証自体を含めて、セキュリティーコンプライアンスおよび監査の要件処理は IT セキュリティー支出の大きな割合を占めています。銀行、病院、政府などの組織には専用のコンプライアンス要件があります。監査者がオペレーティングシステムに詳しくない場合、セキュリティー制御を要件に合わせるために苦労している可能性があります。そのため、セキュリティー制御を要件にマップするツールは、監査者を支援することにより時間とコストを削減できます。

コンプライアンススクリプトは、OVAL (Open Vulnerability and Assessment Language) で書かれた SCAP (Security Content Automation Protocol) に基づいています。また、Oracle Solaris の SCAP 実装は Script Check Engine (SCE) に準拠するスクリプトもサポートしています。これらのスクリプトは現在の OVAL スキーマおよびプローブが提供しないセキュリティー検査を追加します。グラム・リーチ・ブライリー法 (GLBA)、医療保険の相互運用性と説明責任に関する法律 (HIPAA)、サーベンス・オクスリー法 (SOX)、連邦情報セキュリティマネジメント法 (FISMA) など、ほかの規制の環境基準を満たすために追加のスクリプトを使用できます。これらの標準へのリンクについては、14 ページの「コンプライアンスのリファレンス」を参照してください。

Oracle Solaris セキュリティーベンチマーク

Oracle Solaris 11 は、2 つの標準 (Solaris と PCI DSS) のコンプライアンススクリプトを提供します。

Solaris セキュリティーポリシーベンチマーク

Solaris セキュリティーポリシーベンチマークは、Oracle Solaris の「デフォルトでのセキュリティー強化」(secure by default、SBD) のデフォルトインストールに基づく標準です。このベンチマークは 2 つのプロファイル (ベースラインと推奨) を提供します。これらのプロファイルについては、9 ページの「コンプライアンスの測定」で説明します。

SBD を構成する機能については、『Oracle Solaris 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』の「デフォルトでのセキュリティー強化 (Secure By Default) 構成の使用」と、『Oracle Solaris 11 セキュリティーガイドライン 』の「Oracle Solaris 構成可能セキュリティー」で説明します。

このベンチマークは、PCI DSS、CIS (Center for Internet Security)、Oracle Solaris の DISA-STIG (Defense Information Systems Agency-Security Technical Information Guides) ベンチマークの要件を満たしていません。

PCI DSS セキュリティーポリシーベンチマーク

PCI DSS セキュリティーポリシーベンチマークは、主要なデビットカードやクレジットカードのカード所有者情報を扱う企業のための機密情報のセキュリティー標準です。この標準は PCI SSC

(Payment Card Industry Security Standards Council) で定義されています。その目的はクレジットカードの不正使用を削減することです。

Oracle Solaris システムには PCI DSS 標準に準拠する構成が必要です。コンプライアンスレポートは失敗したテストと成功したテストを示し、改善する手順を提供します。

コンプライアンスの測定

セキュリティーのコンプライアンス (以後は*コンプライアンス*と呼ぶ) を測定するには、セキュリティーベンチマークまたはプロファイル、そのベンチマークに対するコンプライアンスの測定 (*評価*と呼ばれる)、および結果のレポートが必要です。また、レポートはトレーニングやアーカイブ目的でガイド形式で出力することもできます。

Oracle Solaris は、Solaris ベンチマークで 2 つのセキュリティープロファイルを測定するスクリプトを提供します。

- Solaris ベンチマークのベースラインプロファイルは Oracle Solaris のデフォルトの SBD インストールと厳密に一致します。
- Solaris 推奨プロファイルは、セキュリティー要件がベースラインプロファイルよりも厳しい企業の要件を満たします。

  これらのプロファイルはネストします。推奨プロファイルに準拠するシステムはベースラインプロファイルにも準拠します。

PCI DSS ベンチマークは PCI DSS 標準に対するシステムのコンプライアンスを測定します。PCI DSS 要件にはコードの直接リンクがないため、コンプライアンスのレポートを調べる必要があります。詳細は、『Meeting PCI DSS Compliance with Oracle Solaris 11』を参照してください。

`compliance` パッケージ

コンプライアンス機能は、`solaris-small-server` および `solaris-large-server` パッケージグループとともにインストールされている `pkg:/security/compliance` パッケージから取得できます。

- パッケージグループについては、『Oracle Solaris 11 セキュリティーガイドライン 』の「Oracle Solaris OS のインストール」を参照してください。

- パッケージについては、『Oracle Solaris 11.2 Package Group Lists 』を参照してください。
- コンプライアンスパッケージの説明を表示するには、`pkg info compliance` コマンドを発行します。

Oracle Solaris のコンプライアンス評価

既知のベンチマークに対するシステムのコンプライアンスを評価およびレポートするには、`compliance` コマンドを使用します。Oracle Solaris のコンプライアンスコマンドは、特定要件のコンプライアンスを検証するコード、ファイル、またはコマンドの出力に対してベンチマークの要件をマップします。このコマンドについては、`compliance`(1M) のマニュアルページを参照してください。

`compliance` コマンドをサポートするツールの SCAP セットについては、`oscap`(8) のマニュアルページを参照してください。ツールの SCAP セットのバージョンを表示するには、`oscap -V` コマンドを発行します。

注記 - ツールの SCAP セットは、`oscap` コマンドが生成するレポートをローカライズすることも、テストの説明をローカライズすることもできません。(ローカライゼーションには、ローカル言語へのソフトウェアの翻訳が含まれます。)

サードパーティーのコンプライアンス評価

CIS サードパーティー標準化機構はベンチマークのコンプライアンスの自動検査ツールを提供します。これらのツールを使用して CIS ベンチマークのコンプライアンスを評価するコストを確認する場合は CIS に問い合わせてください。CIS ツールは、Oracle Solaris コンプライアンスを検査するために Microsoft Windows システム上で使用できます。

Oracle Solaris のコンプライアンス評価

`compliance` コマンドはコンプライアンスの改善ではなく評価を自動化します。このコマンドは評価とレポートをリスト、生成、および削除するために使用されます。すべてのユーザーがコンプライアンスレポートにアクセスできます。評価の管理とレポートの生成には権利が必要です。詳細は、`compliance`(1M) のマニュアルページを参照してください。

compliance コマンドはローカルのファイルのみを検査します。使用しているシステムでファイルシステムをマウントする場合は、クライアントとサーバーのコンプライアンスを個別にテストする必要があります。たとえば、中央サーバーからユーザーのホームディレクトリをマウントする場合、ユーザーシステム上とホームディレクトリをエクスポートするすべてのサーバー上で compliance コマンドを実行します。

compliance コマンドを実行する権利

Oracle Solaris は、コンプライアンス評価とレポート生成を処理する 2 つの権利プロファイルを提供します。

- Compliance Assessor 権利プロファイルを使用すると、ユーザーは評価の実行、評価ストアへの評価の格納、レポートの生成、ストアからの評価の削除ができます。
- Compliance Reporter 権利プロファイルを使用すると、ユーザーは既存の評価から新しいレポートを生成できます。

コンプライアンスサブコマンドには次の権利が必要です。

- compliance assess コマンド – すべての権限と solaris.compliance.assess 承認が必要です。コンプライアンス評価者の権利プロファイルはこれらの権利を提供します。
- compliance delete コマンド – 評価ストアへの書き込み権限と solaris.compliance.assess 承認が必要です。コンプライアンス評価者の権利プロファイルはこれらの権利を提供します。
- compliance list コマンド – 基本的な権利を持つユーザーであればだれでも実行できます。このコマンドはベンチマークおよび評価に対する完全な可視性を提供します。
- compliance report コマンド – だれでも実行できますが、機能の範囲はユーザーの権利に応じて異なります。コンプライアンス評価者またはコンプライアンスレポータのプロファイルに割り当てられたユーザーは評価ストアに新しいレポートを生成できます。すべてのユーザーは既存のレポートを表示できますが、基本的な権利のみを持つユーザーはレポートを生成できません。

コンプライアンスの評価およびレポートの作成

コンプライアンス評価が完了します。レポートには評価のすべての項目を含めるか、評価の情報のサブセットを含めることができます。定期的に評価を実行します。たとえば cron ジョブとしてシステムのコンプライアンスをモニターします。

▼ コンプライアンスレポートの実行方法

`solaris-small-server` および `solaris-large-server` パッケージにはデフォルトで `compliance` パッケージが含まれます。`solaris-desktop` および `solaris-minimal` パッケージには `compliance` パッケージが含まれません。

始める前に システムにパッケージを追加するために Software Installation 権利プロファイルを割り当てる必要があります。11 ページの「`compliance` コマンドを実行する権利」で説明されているとおり、ほとんどのコンプライアンスコマンドに対して管理権利を割り当てる必要があります。詳細は、『Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティー保護 』の「割り当てられている管理権利の使用」を参照してください。

1. **`compliance` パッケージをインストールします。**

```
# pkg install compliance
```

次のメッセージは、そのパッケージがインストールされていることを示します。

```
No updates necessary for this image.
```

詳細は、pkg(1) のマニュアルページを参照してください。

注記 - コンプライアンステストを実行する予定のあるすべてのゾーンにパッケージをインストールします。

---

2. **評価を作成します。**

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
solaris: Baseline, Recommended
Assessments:
 No assessments available
# compliance -p profile -a assessment-directory
```

-p　プロファイルの名前を示します。プロファイル名は大文字と小文字が区別されます。

-a　評価のディレクトリ名を示します。デフォルト名にはタイムスタンプが含まれます。

たとえば、次のコマンドは推奨プロファイルを使用して評価を作成します。

```
# compliance -p Recommended -a recommended
```

このコマンドは、3 種類のファイル (ログファイル、XML ファイル、および HTML ファイル) の評価を含む recommended という名前のディレクトリを /var/share/compliance/assessments 内に作成します。

```
# cd /var/share/compliance/assessments/recommended
# ls
recommended.html
recommended.txt
recommended.xml
```

このコマンドを再実行した場合、ファイルは置換されません。評価ディレクトリを再使用する前にファイルを削除する必要があります。

3. **(オプション) カスタマイズしたレポートを作成します。**

```
# compliance report -s -pass,fail,notselected
/var/share/compliance/assessments/recommended/report.-pass,fail,notselected.html
```

このコマンドは、失敗した項目と選択されていない項目を含むレポートを HTML 形式で作成します。このレポートは最新の評価に対して実行されます。

カスタマイズされたレポートを繰り返し実行できます。ただし、完全なレポート (つまり評価) は元のディレクトリで 1 回のみ実行できます。

4. **完全なレポートを表示します。**

テキストエディタによるログファイル表示、ブラウザによる HTML ファイル表示、XML ビューアによる XML ファイル表示が可能です。

たとえば、前述の手順でカスタマイズされた HTML レポートを表示するには、次のブラウザエントリを入力します。

```
file:///var/share/compliance/assessments/recommended/report.-pass,fail,notselected.html
```

5. **使用しているセキュリティーポリシーが合格するために必要な障害をすべて修正してください。**

   a. **失敗したエントリに対する修正を完了します。**

   b. **修正にシステムのリブートが含まれている場合、評価を再度実行する前にシステムをリブートします。**

6. **(オプション) compliance コマンドを cron ジョブとして実行します。**

```
# cron -e
```

毎日午前 2:30 にコンプライアンスを評価する場合、root で次のエントリを追加します。

```
30 2 * * * /usr/bin/compliance assess -b solaris -p Baseline
```

毎週日曜日の午前 1:15 にコンプライアンスを評価する場合、root で次のエントリを追加します。

```
15 1 * * 0 /usr/bin/compliance assess -b solaris -p Recommended
```

毎月 1 日の午前 4:00 に評価する場合、root で次のエントリを追加します。

```
0 4 1 * * /usr/bin/compliance assess -b pci-dss
```

月の第 1 月曜日の午前 3:45 に評価する場合、root で次のエントリを追加します。

```
45 3 1,2,3,4,5,6,7 * 1 /usr/bin/compliance assess
```

7. **(オプション) システムにインストールされている一部またはすべてのベンチマークのガイドを作成します。**

```
# compliance guide -a
```

ガイドには各セキュリティー検査の根拠と失敗した検査の修正手順が含まれています。ガイドはトレーニングに役立ち、将来のテストのガイドラインとしても役立ちます。デフォルトでは、各セキュリティープロファイルのガイドはインストール時に作成されます。ベンチマークを追加または変更する場合は新規ガイドを作成できます。

コンプライアンスのリファレンス

コンピュータセキュリティーのコンプライアンス領域では、多くの標準、頭字語、および処理に関する高度な知識があることが前提とされます。用語およびリファレンスの次のリストが利便性のために提供されます。

次のプログラムはコンプライアンスの評価およびレポートを実装しています。

- Security Content Automation Protocol (SCAP)
- SCAP ツール (OpenSCAP)
- Open Vulnerability and Assessment Language (OVAL)
- eXtensible Configuration Checklist Description Format (XCCDF)

次の各本文では、コンプライアンスの標準または法律について説明しています。

- Center for Internet Security (CIS)

- 連邦情報セキュリティマネジメント法 (FISMA)
- グラム・リーチ・ブライリー法 (GLBA)
- 医療保険の相互運用性と説明責任に関する法律 (HIPAA)
- Payment Card Industry-Data Security Standard (PCI DSS)
- サーベンス・オクスリー法 (SOX)