

Oracle® Solaris 10 セキュリティーガイド ライン

このソフトウェアおよび関連ドキュメントの使用と開示は、ライセンス契約の制約条件に従うものとし、知的財産に関する法律により保護されています。ライセンス契約で明示的に許諾されている場合もしくは法律によって認められている場合を除き、形式、手段に関係なく、いかなる部分も使用、複写、複製、翻訳、放送、修正、ライセンス供与、送信、配布、発表、実行、公開または表示することはできません。このソフトウェアのリバース・エンジニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクル社までご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合は、次の通知が適用されます。

U.S. GOVERNMENT END USERS:

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

このソフトウェアもしくはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアもしくはハードウェアは、危険が伴うアプリケーション（人的傷害を発生させる可能性があるアプリケーションを含む）への用途を目的として開発されていません。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用する際、安全に使用するために、適切な安全装置、バックアップ、冗長性（redundancy）、その他の対策を講じることは使用者の責任となります。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用したこと起因して損害が発生しても、オラクル社およびその関連会社は一切の責任を負いかねます。

OracleおよびJavaはOracle Corporationおよびその関連企業の登録商標です。その他の名称は、それぞれの所有者の商標または登録商標です。

Intel, Intel Xeonは、Intel Corporationの商標または登録商標です。すべてのSPARCの商標はライセンスをもとに使用し、SPARC International, Inc.の商標または登録商標です。AMD, Opteron, AMDロゴ、AMD Opteronロゴは、Advanced Micro Devices, Inc.の商標または登録商標です。UNIXは、The Open Groupの登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

目次

はじめに	5
1 Oracle Solaris 10のセキュリティーガイドライン	9
Oracle Solaris 10のシステム強化に関するリファレンス	9
Oracle Solaris 10のセキュリティーに関するその他のリファレンス	10

はじめに

このガイドには、Oracle Solaris オペレーティングシステム (Oracle Solaris OS) のセキュリティガイドラインの参照先および説明が記載されています。システム強化に関するリファレンスには、Oracle Solaris 10 システムの強化方法および Oracle Solaris のセキュリティ機能を使ってデータやアプリケーションを保護する方法が説明されています。サイトのセキュリティポリシーに合わせてこれらのリファレンスの推奨事項を調整することができます。

さらに、このガイドには Oracle Solaris のセキュリティに関する背景情報や、一般的な実装方法をガイドするホワイトペーパーの参照先も記載されています。

対象読者

Oracle Solaris 10 セキュリティガイドラインは、次のタスクを行うセキュリティ管理者およびその他の管理者を対象としています。

- セキュリティ要件の分析
- ソフトウェアへのセキュリティポリシーの実装
- Oracle Solaris OS のインストールと構成
- システムおよびネットワークセキュリティの保守

このガイドを使用するには、UNIX 管理の一般知識、ソフトウェアセキュリティの適切な基盤、およびサイトのセキュリティポリシーの知識が必要です。

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することができます。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。

表記上の規則

次の表では、このマニュアルで使用される表記上の規則について説明します。

表 P-1 表記上の規則

字体	説明	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例を示します。	.login ファイルを編集します。 ls -a を使用してすべてのファイルを表示します。 machine_name% you have mail.
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して示します。	machine_name% su Password:
<i>aabbcc123</i>	Placeholder: 実際に使用する特定の名前または値で置き換えます。	ファイルを削除するには、rm <i>filename</i> と入力します。
AaBbCc123	書名、新しい単語、および強調する単語を示します。	『ユーザーズガイド』の第6章を参照してください。 キャッシュは、ローカルに格納されるコピーです。 ファイルを保存しないでください。 注: いくつかの強調された項目は、オンラインでは太字で表示されます。

コマンド例のシェルプロンプト

Oracle Solaris OS に含まれるシェルで使用する、UNIX のシステムプロンプトとスーパーユーザープロンプトを次に示します。コマンド例では、シェルプロンプトはコマンドが標準ユーザーまたは特権ユーザーのどちらによって実行されるべきかを示しています。

表 P-2 シェルプロンプト

シェル	プロンプト
Bash シェル、Korn シェル、および Bourne シェル	\$
Bash シェル、Korn シェル、および Bourne シェルのスーパーユーザー	#

表 P-2 シェルプロンプト (続き)

シェル	プロンプト
Cシェル	machine_name%
Cシェルのスーパーユーザー	machine_name#

Oracle Solaris 10 のセキュリティーガイドライン

Oracle Solaris 10 は、実証済みのセキュリティー機能を提供する、堅牢かつ最高級のエンタープライズオペレーティングシステムです。Oracle Solaris 10 では、ユーザーによるファイルアクセス、システムデータベースの保護、およびシステムリソースの使用の方法を制御する、洗練されたネットワーク規模のセキュリティーシステムを使って、あらゆる層のセキュリティーニーズに対応します。従来のオペレーティングシステムにはセキュリティーに関する固有の脆弱性が含まれていることがありますが、Oracle Solaris 10 ではその柔軟性によって、エンタープライズサーバーからデスクトップクライアントに至るまで、さまざまなセキュリティー目標を満たすことができます。

Oracle Solaris 10 のシステム強化に関するリファレンス

次の2つのドキュメントには、Oracle Solaris の強化方法、そのセキュリティー機能を使って、アプリケーションやユーザーをシステムに追加する際にシステムが安全に動作するように構成する方法、および特定のセキュリティー機能を使ってネットワークベースのアプリケーションを保護する方法が記載されています。各ドキュメントのタイトルと簡単な説明を示します。

- **CIS Solaris 10 Benchmark v5.0.0** (<http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.solaris10.500>)、2010年7月9日。

このドキュメントの別の名前は『Security Configuration Benchmark for Solaris 10 11/06 through 10/09』です。このベンチマークは、多くの貢献者による7年にわたる作業の成果です。それらの貢献者には、Sun Microsystems、Defense Information Systems Agency (DISA)、Center for Internet Security (CIS)、National Institute of Standards and Technology (NIST)、National Security Agency (NSA)、および多数の個々の企業、学術機関、個人が含まれます。このベンチマークによって、Sun、CIS、NSA、およびDISAの同意を得た1組の基本的な強化ガイドラインが確立されます。

- [An Overview of Oracle Solaris 10 Security Controls \(http://www.oracle.com/technetwork/server-storage/solaris/documentation/o11-076-s10-cis-appendix-487450.pdf\)](http://www.oracle.com/technetwork/server-storage/solaris/documentation/o11-076-s10-cis-appendix-487450.pdf)、Glenn Brunette 著、2011年9月

『Security Configuration Benchmark for Solaris 10 11/06 through 10/09』のこの付録は、システム強化およびセキュリティー構成の検証の分野に入らない、Oracle Solaris 10のセキュリティー制御に重点が置かれています。この付録では、Oracle Solaris 10のセキュリティー機能の概要をすべて説明し、可能な場合は個別の推奨事項を提供します。

Oracle Solaris 10のセキュリティーに関するその他のリファレンス

次のガイドと記事は、前のセクションのシステム強化のガイドラインを補足するものです。

- 『Solarisのシステム管理:セキュリティーサービス』

このセキュリティーガイドは、OracleがOracle Solaris 10管理者のために発行したものです。このガイドには、Oracle Solaris 10 OSのセキュリティー機能、およびシステム構成時のそれらの使用方法が説明されています。『Security Configuration Benchmark for Solaris 10 11/06 through 10/09』とは異なり、このガイドはシステム強化やベストプラクティスに関するドキュメントとして書かれたものではありません。

- 『Solaris 10 Security Essentials』, Sun エンジニア、2009年。ISBN 978-0137012336

この一般書では、Solaris エンジニアおよびテクニカルライターがSolarisに関する12のセキュリティー技術を例をもって説明しています。『Security Configuration Benchmark for Solaris 10 11/06 through 10/09』とは異なり、このガイドはシステム強化やベストプラクティスに関するドキュメントとして書かれたものではありません。

- [Using Oracle® Solaris 10 to Overcome Security Challenges \(http://www.oracle.com/technetwork/server-storage/solaris/solaris-10-security-167783.pdf\)](http://www.oracle.com/technetwork/server-storage/solaris/solaris-10-security-167783.pdf)、2010年8月。

このOracleのホワイトペーパーは、包括的なシステムセキュリティー機能を必要とする組織を対象としています。コンピュータセキュリティーの効果的かつ効率的なソリューションを必要とするIT部門は、Oracle Solaris 10固有の強力なセキュリティー機能を使って、潜在的な脅威から企業を保護し、企業および法的基準に準拠し、セキュリティーへの取り組みに後れを取らないようにすることができます。このホワイトペーパーでは、Oracle Solarisのセキュリティー機能の概要を説明しています。これは強化やベストプラクティスに関するドキュメントとして書かれたものではありません。