



# インスタンスの保護

Version 2024.1  
2024-06-03

## インスタンスの保護

InterSystems IRIS Data Platform Version 2024.1 2024-06-03

Copyright © 2024 InterSystems Corporation

All rights reserved.

InterSystems®, HealthShare Care Community®, HealthShare Unified Care Record®, IntegratedML®, InterSystems Caché®, InterSystems Ensemble®, InterSystems HealthShare®, InterSystems IRIS®, および TrakCare は、InterSystems Corporation の登録商標です。HealthShare® CMS Solution Pack™ HealthShare® Health Connect Cloud™, InterSystems IRIS for Health™, InterSystems Supply Chain Orchestrator™, および InterSystems TotalView™ For Asset Management は、InterSystems Corporation の商標です。TrakCare は、オーストラリアおよび EU における登録商標です。

ここで使われている他の全てのブランドまたは製品名は、各社および各組織の商標または登録商標です。

このドキュメントは、インターシステムズ社(住所: One Memorial Drive, Cambridge, MA 02142)あるいはその子会社が所有する企業秘密および秘密情報を含んでおり、インターシステムズ社の製品を稼働および維持するためにのみ提供される。この発行物のいかなる部分も他の目的のために使用してはならない。また、インターシステムズ社の書面による事前の同意がない限り、本発行物を、いかなる形式、いかなる手段で、その全てまたは一部を、再発行、複製、開示、送付、検索可能なシステムへの保存、あるいは人またはコンピュータ言語への翻訳はしてはならない。

かかるプログラムと関連ドキュメントについて書かれているインターシステムズ社の標準ライセンス契約に記載されている範囲を除き、ここに記載された本ドキュメントとソフトウェアプログラムの複製、使用、廃棄は禁じられている。インターシステムズ社は、ソフトウェアライセンス契約に記載されている事項以外にかかるソフトウェアプログラムに関する説明と保証をするものではない。さらに、かかるソフトウェアに関する、あるいはかかるソフトウェアの使用から起こるいかなる損失、損害に対するインターシステムズ社の責任は、ソフトウェアライセンス契約にある事項に制限される。

前述は、そのコンピュータソフトウェアの使用およびそれによって起こるインターシステムズ社の責任の範囲、制限に関する一般的な概略である。完全な参照情報は、インターシステムズ社の標準ライセンス契約に記載され、そのコピーは要望によって入手することができる。

インターシステムズ社は、本ドキュメントにある誤りに対する責任を放棄する。また、インターシステムズ社は、独自の裁量にて事前通知なしに、本ドキュメントに記載された製品および実行に対する代替と変更を行う権利を有する。

インターシステムズ社の製品に関するサポートやご質問は、以下にお問い合わせください:

InterSystems Worldwide Response Center (WRC)

Tel: +1-617-621-0700

Tel: +44 (0) 844 854 2917

Email: [support@InterSystems.com](mailto:support@InterSystems.com)

# 目次

インスタンスの保護.....	1
1 セキュリティ戦略 .....	1



# インスタンスの保護

## 1 セキュリティ戦略

InterSystems IRIS® インスタンスの保護について計画を開始するタイミングとしては、最初のインストールの前が最適です。“[インターシステムズのセキュリティのための準備](#)”では、InterSystems IRIS® インスタンスをインストールする前に検討すべきいくつかの問題について説明しています。一般的に、プロダクション・システムの場合、可能な限り最高のセキュリティ・レベルから始めて、必要に応じてのみ特権を付与することをお勧めします。まずは、初期セキュリティ設定を[ロック・ダウン]に指定してインストールを実行し、そこから調整していくことをお勧めします。

InterSystems IRIS をインストールした後の場合、またはインスタンスが既にインストールされている場合は、インスタンスへのアクセスを制限し、攻撃対象領域を軽減する方法について、“[インスタンスのセキュリティの強化](#)”を参照してください。[ロック・ダウン]の初期セキュリティ設定を使用してインストールを実行した場合、ここで説明している手順の一部は既に自動的に完了されています。ただし、その場合でも内容を調べて、インスタンスのセキュリティ強化のために実行できる追加措置を確認する必要があります。

InterSystems IRIS 管理ポータルには、[セキュリティ・アドバイザー](#)が組み込まれています。これを使用すると、インスタンスに関して調べる必要がある領域のリストを表示して、それらの領域のセキュリティを強化する必要があるかどうか確認できます。セキュリティ・アドバイザーでは、そのような領域別に管理ポータル内の該当ページへのリンクが提示されるので、関連する設定を必要に応じて調整できます。

言うまでもなく、安全なシステムの実行には、InterSystems IRIS 実行可能ファイルとは別に攻撃対象領域のセキュリティを強化することが必要です。InterSystems IRIS で使用されているその他のプロセスやリソースが悪意のある動作の標的になる可能性もあります。“[インターシステムズのプロセスおよびオペレーティング・システム・リソースの保護](#)”で、これらのトピックについて説明し、順守すべきガイドラインを提示します。

最後に、“[導入環境のセキュリティを強化するためのチェックリスト](#)”は、ネットワーク、オペレーティング・システム、Web サーバなど多数の広範なセキュリティ・カテゴリに分類されています。また、そのカテゴリ別にチェックリストが用意されており、これを使用して組織の導入環境全体のセキュリティを強化できます。

