インスタンスの保護

Version 2024.1
2024-06-03

InterSystems Corporation　1 Memorial Drive　Cambridge MA 02142　www.intersystems.com

インスタンスの保護
InterSystems IRIS Data Platform　Version 2024.1　2024-06-03

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

目次

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の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。