インターシステムズのセキュリティの概要

Version 2023.1
2024-01-02

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

インターシステムズのセキュリティの概要
InterSystems IRIS Data Platform　Version 2023.1　2024-01-02

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

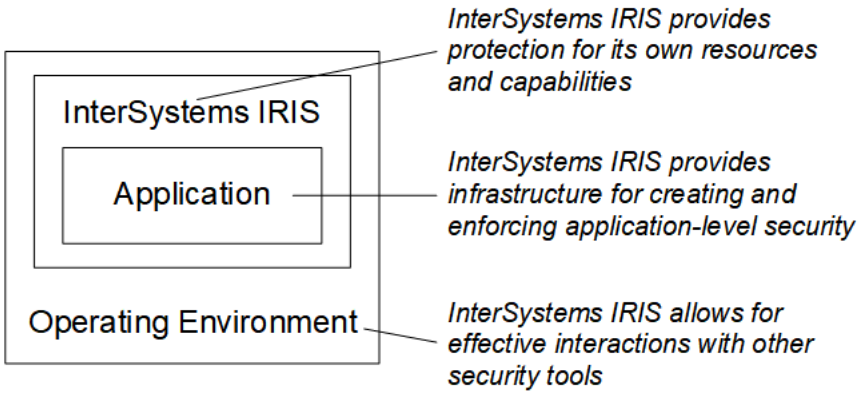
図一覧

インターシステムズのセキュリティの概要

InterSystems IRIS® データ・プラットフォームは、以下の特長を持つシンプルで統合されたセキュリティ・アーキテクチャを提供します。

- また、開発者が高パフォーマンスの強力なセキュリティ機能をアプリケーションに簡単に組み込むことができるようにするセキュリティ・インフラストラクチャを提供します。
- パフォーマンスと動作に対する負荷が最小限となります。
- InterSystems IRIS が、セキュリティで保護された環境の構成要素として効果的に機能し、他のアプリケーションとシームレスに連係して動作します。
- ポリシーの管理と適用のためのインフラストラクチャを提供します。

図 1: インターシステムズのセキュリティおよびさまざまなレベルのコンピューティング環境



インターシステムズのセキュリティは、重要な機能を数多く含み、広く使用されているテクノロジに対応しています。

- 認証では、すべてのユーザの身元が確認されます。
- 承認によって、ユーザがアクセスできるリソースを、そのユーザが必要とするもののみに制限できます。
- LDAP (Lightweight Directory Access Protocol) は、認証と承認の両方に対応した、広く使用されているツールです。
- TLS (Transport Layer Security プロトコル) では、通信とデータ送信用の保護されたチャンネルが構築されます。
- SQL セキュリティでは、データをリレーショナル・テーブルとして操作する場合のアクセスが制御されます。
- 暗号化では、保存データが承認されていないアクセスから保護されます。
- システム・セキュリティでは、インスタンスレベルのセキュリティの確保と強化のためのツールが提供されます。
- 監査では、事前定義したシステム・イベントとアプリケーション固有イベントのログが保持されます。
- PKI (公開鍵基盤) では、保護された通信で使用する鍵と証明書が管理されます。

コンピューティング環境を保護するための包括的なソリューションの要素として、InterSystems IRIS を他のセキュリティ製品やツール (ファイアウォールやオペレーティング・システムのセキュリティ機能など) と組み合わせて使用できます。この理由から、InterSystems IRIS のセキュリティ機能は、他の製品のセキュリティ機能と相互運用できるように設計されています。

明確かつ効果的で、適切に強制されるセキュリティ・ポリシーを確立することもお勧めします。テクノロジ、ポリシー、および強制によって、安全で生産性の高い環境を創出できます。

1 認証 : 身元の確認

認証は、InterSystems IRIS が各ユーザの身元を確認する方法です。信頼できる認証は、すべてのセキュリティの基礎です。承認とその他すべての機能が認証に依存しているからです。

InterSystems IRIS には、以下のようなさまざまな認証メカニズムが用意されています。

- Kerberos ー 最も高いセキュリティで保護された認証方法です。Kerberos 認証システムでは、数学的に立証された強力な認証がネットワーク上で実現します。
- オペレーティング・システム・ベース ー OS ベースの認証では、オペレーティング・システムでユーザごとに割り当てられている身元情報を使用して、InterSystems IRIS 向けにユーザを識別します。
- LDAP ー LDAP (Lightweight Directory Access Protocol) により、InterSystems IRIS では LDAP サーバとして知られる一元管理リポジトリにある情報に基づいてユーザを認証します。
- インスタンス認証 ー インスタンス認証では、ユーザにパスワードを要求し、ユーザが入力したパスワードのハッシュ値を格納値と比較します。
- 代行認証 ー 代行認証により、カスタマイズされた認証メカニズムを作成する方法が実現します。アプリケーション開発者は、代行認証コードのコンテンツを完全に制御します。

InterSystems IRIS では、2 種類の形式の 2 要素認証もサポートされています。

- エンドユーザの携帯電話にセキュリティ・コードを送信する。
- エンドユーザの携帯電話上のアプリケーションを使用して、タイムベースのワンタイム・パスワード (TOTP) を作成する。

境界ネットワークが強力に保護されているか、攻撃者の標的になるようなアプリケーションもデータもない状況の場合は、認証なしでユーザ接続を受け入れるよう InterSystems IRIS を構成できます。

2 承認 : ユーザ・アクセスの制御

ユーザが認証された後、セキュリティに関連する次の手順は、そのユーザに使用、閲覧、または変更が認められているリソースが何であるかを確認することです。この判断とそれに基づくアクセスの制御を、承認といいます。承認では、ユーザと保護対象のリソース (エンティティ) との関係を管理します。このリソースは、データベース、インターシステムズの各種サービス (Web アクセスの制御など)、ユーザが作成したアプリケーションなど、広範囲に及びます。

InterSystems IRIS の承認の仕組みは、以下のとおりです。

- 各ユーザに 1 つ以上のロールが割り当てられます。
- 各ロールに 1 つ以上の特権が割り当てられます。各特権は、特定のリソースを使用して特定のアクティビティを実行する権限です。
- ユーザ、ロール、およびその他のセキュリティ・エンティティを管理するためのツールがあります。

InterSystems IRIS では、ユーザにロールを割り当てることができる内部ツールと外部ツールの両方がサポートされます。InterSystems IRIS では、これらの割り当てを使用して、各ユーザの許可済みアクティビティを決定します。これらのツールは、ロール割り当てメカニズムと呼ばれます。ロール割り当てメカニズムは、以下のとおりです。

- インターシステムズの承認 ー InterSystems IRIS 内部でロール割り当てが行われます。Kerberos、OS ベース、およびインスタンスの認証メカニズムで使用できます。
- LDAP ー LDAP (Lightweight Directory Access Protocol) サーバによってロール割り当てが行われます。OS ベースおよび LDAP の認証メカニズムで使用できます。
- 代行承認 ー 承認アクティビティを排他的に処理するユーザ指定コードでロール割り当てが行われます。Kerberos および OS ベースの認証メカニズムで使用できます。
- 代行認証 ー 認証アクティビティも処理するユーザ指定コードの一部としてロール割り当てが行われます。代行認証メカニズム内でのみ使用できます。

すべてのロール割り当てメカニズムで、ロール管理 (つまり、特定のロールへの特定の特権の関連付け) は、InterSystems IRIS 内部で行われます。

3 LDAP : 広く使用されている認証および承認ツール

LDAP (Lightweight Directory Access Protocol) は、認証アクティビティと承認アクティビティに対応した、広く使用されている業界標準プロトコルです。Windows の場合、LDAP は Active Directory として実装されます。

LDAP サーバは、ユーザ情報の一元管理リポジトリであり、InterSystems IRIS はそこから認証および承認の情報を取得します。

- LDAP 認証の場合、InterSystems IRIS により、ユーザにユーザ名とパスワードの入力を求めるプロンプトが表示されます。インスタンスは LDAP サーバに関連付けられ、LDAP サーバが認証を実行し、オプションでユーザのロールなどの承認情報を取得します。インスタンスが LDAP サーバに接続できない場合に、キャッシュされた認証情報を使用してユーザを認証するようにインスタンスを構成することもできます。LDAP 認証で代行承認を使用することもできます。
- LDAP 承認の場合、InterSystems IRIS では、LDAP グループを使用してユーザにロールが割り当てられます。これにより、ユーザはそれらのロールの特権に基づいてアクションを実行できるようになります。LDAP 承認は、ローカルの InterSystems IRIS ターミナルからログインする場合に OS ベースの認証と共に使用することも、代行認証と共に使用することもできます。

サポートされている LDAP 機能には以下のものがあります。

- Windows 向け Active Directory ドメイン・コントローラ
- OpenLDAP
- LDAP バージョン 3 プロトコル
- 複数の LDAP ドメイン

4 TLS : 送信中データに対する業界標準の保護

TLS (Transport Layer Security プロトコル) では、エンティティ・ペア間における通信が強力に保護されます。TLS では、認証、データ整合性保護、およびデータ暗号化がサポートされます。TLS は、SSL (Secure Sockets Layer) の後継で、SSL に置き換わるものです。

InterSystems IRIS では、TLS がサポートされており、以下のような接続が保護されます。

- InterSystems IRIS スーパーサーバと対話する xDBC などのクライアント・アプリケーションからの接続

- InterSystems Telnet サーバと対話する Telnet クライアントからの接続
- InterSystems IRIS がクライアント、サーバ、または両方である場合の TCP 経由の接続
- ECP（エンタープライズ・キャッシュ・プロトコル）を使用する接続

5 SQL セキュリティ：リレーショナル・アクセスの保護

InterSystems IRIS には、認証ツールや承認ツールをはじめ、セキュリティ・インフラストラクチャとシームレスに統合される一連の SQL セキュリティ・ツールが用意されています。これらのツールを使用すると、リレーショナル・テーブル・データのセキュリティを確保でき、ユーザは適切にかつ簡単に必要なデータにアクセスできるようになります。ツールの機能としては、以下のものがあります。

- テーブル・レベルまたはビュー・レベルでの特権の付与、確認、および削除
- SQL ロールの作成および削除
- ユーザおよびロールに対するシステム全体の変数の使用

6 暗号化：保管中のデータの保護

InterSystems IRIS には、保管中のデータ、つまりディスクまたはクラウドに保存されているデータへの承認されていないアクセスを防ぐ、一連の暗号化テクノロジが用意されています。これらの一連のツールに実装されている暗号化では、AES（Advanced Encryption Standard）アルゴリズムが採用されています。AES のテクノロジには、次のようなものがあります。

- ブロックレベルのデータベース暗号化 – InterSystems IRIS は、ディスクに対して書き込みおよび読み取りを行うときに、データベースの暗号化と解読を実行します。暗号化されるコンテンツとしては、データ自体、インデックス、ビットマップ、ポインタ、割り当てマップ、インクリメンタル・バックアップ・マップなどがあります。
- アプリケーションで使用するためのデータ要素暗号化 – データ要素暗号化では、シンプルで包括的な一連のメソッドが使用され、必要に応じてアプリケーションでコンテンツの暗号化と解読を行えます。
- 暗号化キー管理 – InterSystems IRIS には、暗号化操作をサポートするために、データ暗号化キーの作成と管理のためのツールが用意されています。これらのキーは、キー・ファイル、または Key Management Interoperability Protocol（KMIP）を使用するキー・サーバのいずれかに保存できます。

InterSystems IRIS のあらゆる側面と同様に、暗号化と解読も最適なパフォーマンスが得られるように最適化されています。データベースに書き込む場合、パフォーマンスにはまったく影響がありません。データベースを読み取る場合、影響は確定的でわずかです。

7 システム・セキュリティ：インスタンスの強化

セキュリティを確保するには、インスタンス内と、インスタンスが属するより大きな環境でのアクションが必要です。そのため、InterSystems IRIS にはインスタンスの保護に役立つガイドとツールの両方が用意されています。これには、以下のものがあります。

- InterSystems IRIS の導入を準備する際に確認するトピックのチェックリスト

- 組み込み機能を使用するインスタンスを保護するためのガイドとツール
- オペレーティング・システム・レベルで、インスタンスのプロセスを管理することによってインスタンスのセキュリティを強化するためのチェックリスト

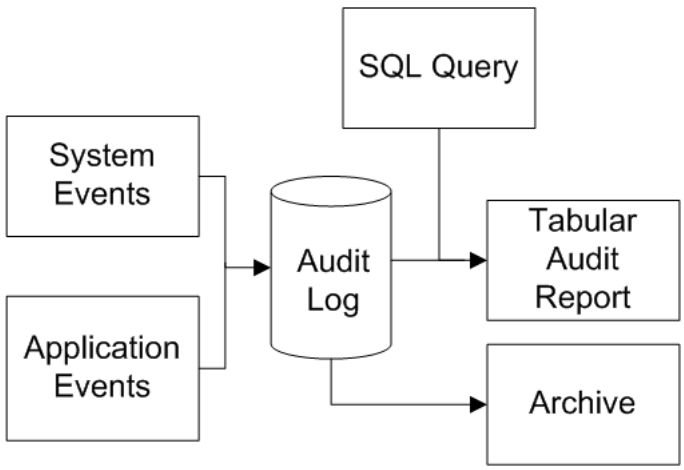
8 監査 : 動作状況の確認

監査では、システムに関連するアクションについて、検証可能で信頼できる追跡が得られます。監査では、以下のセキュリティ機能が提供されます。

- InterSystems IRIS およびそのアプリケーションの認証システムと承認システムで発生したアクションを記録した証明を提供します。これは一般にも認められている“書面による証跡”です。
- セキュリティに関連するどのような問題が発生した後でも、イベントのシーケンスを再構築するための基盤を提供します。
- 攻撃者が監査の存在を知っているか、存在を想定すれば、攻撃者は攻撃を思いとどまります (攻撃時に攻撃者のアクションに関する情報が記録されるからです)。

監査機能では、さまざまなシステム・イベントやユーザ定義イベントを記録できます。それによって、承認されたユーザは、InterSystems IRIS に付属するツールを使用して、この監査ログに基づくレポートを作成できます。付属の InterSystems IRIS ツールは、監査ログのアーカイブ処理およびその他のタスクをサポートしています。

図 2: InterSystems IRIS 監査システム



9 公開鍵基盤 (PKI) : 証明書および秘密鍵と共に使用

InterSystems IRIS には、PKI 実装が含まれています。公開鍵基盤 (PKI) では、秘密鍵、公開鍵、および証明書を作成、管理する暗号化操作がサポートされます。これらの操作としては、暗号化、解読、デジタル署名、およびデジタル・シグニチャの検証があります。

インターシステムズの PKI の実装によって、以下のことが可能になります。

- InterSystems IRIS のインスタンスが認証局 (CA) として機能できます。CA サーバとしてのインスタンスは、自己署名 CA 証明書を生成して使用するか、商用のサード・パーティまたは製品により発行された CA 証明書を使用できます。

- InterSystems IRIS のインスタンスを、InterSystems IRIS CA のサービスを使用する CA クライアントとして設定できます。CA クライアントとしてのインスタンスは、CA サーバと関連付けられます。CA クライアントの証明書は、TLS、XML 暗号化、およびシグニチャの検証で使用できます。
- InterSystems IRIS のインスタンスは、CA サーバとしても CA クライアントとしても機能できます。例えば、中間 CA としても機能するように CA クライアントを構成できます。

InterSystems IRIS では、PKI 通信の実行に Web サービスが使用されます。