インスタンスの保護

Version 2023.1
2024-01-02

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 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

1 セキュリティ戦略 1

2 インターシステムズのセキュリティのための準備 3
2.1 インターシステムズの初期セキュリティ設定 3
2.1.1 初期のユーザ・セキュリティ設定 4
2.1.2 初期のユーザ・アカウント・パスワード 6
2.1.3 初期のサービス・プロパティ 6
2.2 ユーザ・アカウントの構成 10
2.3 Kerberos を使用したセキュリティ環境の準備 10
2.3.1 Windows サーバ用の Windows サービス・アカウントの作成 11
2.3.2 Windows Kerberos クライアントの構成 12
2.3.3 非 Windows サーバ用の Windows サービス・アカウントの作成 12
2.3.4 KDC での非 Windows サーバのサービス・プリンシパルの作成 13
2.3.5 Kerberos KDC 機能のテスト 13

3 インスタンスのセキュリティの強化 15
3.1 監査の有効化 16
3.2 アプリケーションの認証メカニズムの変更 16
3.2.1 CSPSystem ユーザに %Service_WebGateway:Use 特権を付与 18
3.2.2 CSPSystem ユーザのパスワードを変更 18
3.2.3 ユーザ名とパスワードを提供するように Web ゲートウェイを構成 19
3.2.4 パスワード認証を要求するように %Service_WebGateway を構成 19
3.2.5 %Service_WebGateway:Use 特権のパブリック状態を削除 19
3.2.6 パスワード認証のみを受け入れるように管理ポータルを構成 20
3.2.7 インスタンスのユーザに対して適切な権限レベルを指定 20
3.2.8 クラス・ドキュメントを使用可能にする 22
3.2.9 新しいポリシーの施行を開始 22
3.3 パブリック・リソース数の制限 23
3.4 サービスへのアクセス制限 24
3.4.1 有効なサービス数の制限 24
3.4.2 パブリック・サービス数の制限 24
3.4.3 IP アドレスまたはマシン名を基準にしたサービスへのアクセスの制限 24
3.5 リモート特権アクセスの制限 25
3.6 特権ユーザ数の制限 25
3.7 _SYSTEM ユーザの無効化 26
3.8 UnknownUser のアクセスの制限 26
3.8.1 UnknownUser アカウントで発生する可能性のあるロックアウトの問題 27
3.9 サードパーティ・ソフトウェアの構成 27

4 セキュリティ・アドバイザ 29
4.1 監査 29
4.2 サービス 30
4.3 ロール 30
4.4 ユーザ 31
4.5 Web アプリケーション、特権ルーチン・アプリケーション、およびクライアント・アプリケーション 31

5 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 33
5.1 概要 33

5.2 InterSystems IRIS プロセス 33
5.2.1 コア・プロセス 33
5.2.2 ECP サーバ・プロセス 34
5.2.3 Web サーバ・プロセス 35
5.2.4 ミラー・システム・プロセス 35
5.3 IP プロトコル 35
5.3.1 TCP 35
5.3.2 UDP 36
5.3.3 SNMP 36
5.3.4 HTTP 36
5.3.5 ゲートウェイ 36
5.4 不要な InterSystems IRIS プロセスの削除 37
5.5 外部プロセス 37
5.6 相互運用性 38
5.6.1 アダプタ 38
6 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 41
6.1 ネットワークとファイアウォール 42
6.2 オペレーティング・システム 43
6.3 Web サーバ 44
6.4 ユーザ、パスワード、グループ、所有権、および権限 45
6.5 暗号化 (保管中のデータと伝送中のデータ) 45
6.6 インターシステムズのセキュリティ 46

テーブル一覧

テーブル 2-1: 有効化されるサービス 9
テーブル 3-1: 必須のパブリック・リソースおよびその許可 23

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。

2
インターシステムズのセキュリティのための準備

ここでは、InterSystems IRIS をインストールする前に検討する必要があるセキュリティ関連の問題をいくつか取り上げて説明します。インターシステムズのセキュリティ機能の概要は、“インターシステムズのセキュリティについて” を参照してください。認証や承認についても詳細を確認できます。

このセクションでは、以下のトピックについて説明します。

- インターシステムズの初期セキュリティ設定 ー 各種既定のセキュリティ設定の特徴について説明します。特に、通常またはロック・ダウンのインターシステムズのセキュリティを使用する場合に役立ちます。
- ユーザ・アカウントの構成 ー InterSystems IRIS を実行するユーザ・アカウントに必要な許可について説明します。
- Kerberos を使用したセキュリティ環境の準備 ー InterSystems IRIS で認証メカニズムとして Kerberos を使用する予定の場合に実行する必要がある追加のタスクを詳細に説明します。お使いの環境で Kerberos を使用しない場合、このトピックは省略してかまいません。

重要　　このドキュメントで説明する環境よりさらに複雑なセキュリティ環境を使用する場合、具体的な設定方法については、インターシステムズのサポート窓口までお問い合わせください。

″インターシステムズのセキュリティについて″ の説明を参照し、このセクションの手順を実行したうえで、″インストール・ガイド″ で説明されているように、インストール手順に必要なセキュリティ情報を指定してください。

2.1 インターシステムズの初期セキュリティ設定

インストール時に、**[最小]**、**[通常]**、または **[ロック・ダウン]** の 3 つの中から初期セキュリティ構成を選択します。概して、プロダクション環境で使用するインスタンスには [ロック・ダウン]、開発環境で使用するインスタンスには [通常] を選択することをお勧めします。以下のセクションでは、これらの各構成の違い、および各構成の初期のサービス・プロパティについて説明します。

- 初期のユーザ・セキュリティ設定
- 初期のユーザ・アカウント・パスワード
- 初期のサービス・プロパティ

プロダクション環境の場合、選択するオプションにかかわらず、インストール後に個々のセキュリティ設定を調整する必要があります。詳細は、以下のセクションを参照してください。

- インスタンスのセキュリティの強化
- セキュリティ・アドバイザ

- 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
- 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

重要　メモリ・イメージ内のデータの可視性 (コア・ダンプと呼ばれることが多い) に懸念がある場合は、"メモリ・イメージに存在する機密データの保護" を参照してください。

2.1.1 初期のユーザ・セキュリティ設定

InterSystems IRIS ユーザ・アカウントの一般情報は、"ユーザ・アカウント" を参照してください。

すべてのユーザ・アカウントで特定のパスワード要件および設定が共有されます。次の表に示しているように、これらの設定の初期値は選択したセキュリティ・レベルに基づきます。

セキュリティ設定	最小	通常	ロック・ダウン	説明
パスワード・パターン*	3.32ANP	3.32ANP	8.32ANP	既定で、パスワードには英数字および句読点を使用できます。長さの初期要件は、最小および通常のインストールの場合は 3 ～ 32 文字、ロック・ダウン・インストールの場合は 8 ～ 32 文字です。 パスワード・パターンの詳細は、"パスワードの強固さとパスワードのポリシー" を参照してください。
不活動上限*	0	90 日間	90 日間	アカウントがアクティブではなかった期間が、この値で指定された日数を超えると、このアカウントは無効になります。最小のインストールでは、この上限は 0 に設定されます。これは、アカウントがアクティブではない期間がどれだけ続いても、アカウントは無効化されないことを表します。通常のインストールやロック・ダウン・インストールに対する上限の既定値は 90 日間です。
_SYSTEM ユーザの有効化	あり	あり	なし	
UnknownUser に割り当てられるロール	%All	なし	なし	認証されていないユーザが接続した場合、InterSystems IRIS では、UnknownUser という特殊な名前が $USERNAME に割り当てられ、そのユーザに対して定義されているロールが $ROLES に割り当てられます。最小セキュリティのインストールでは、UnknownUser は %All ロールに割り当てられます。最小以外のセキュリティ・レベルを選択した場合、UnknownUser にはロールは割り当てられません。 $USERNAME および $ROLES の使用法の詳細は、"ユーザ" および "ロール" を参照してください。

* これらの設定は、管理ポータルの **[システム]→[セキュリティ管理]→[システムセキュリティ設定]→[システムワイドセキュリティパラメータ]** ページから管理できます。詳細は、"システム規模のセキュリティ・パラメータ" を参照してください。

2.1.2 初期のユーザ・アカウント・パスワード

InterSystems IRIS では、インストール時に複数のユーザ・アカウントが作成されます。事前定義の InterSystems IRIS ユーザ・アカウントが既定で備えるパスワードおよび動作内容は、インストールが最小のセキュリティ、通常のセキュリティ、またはロック・ダウン・セキュリティのいずれの条件で実行されたかによって異なります。これらの相違点は、以下のとおりです。

- 最小セキュリティ – 作成されたすべてのアカウントのうち、_PUBLIC を除くアカウントで、最初の既定のパスワードが“SYS”に設定されます。InterSystems IRIS インスタンスに対する承認されないアクセスを防止するために、UnknownUser を除くすべてのアカウントで、インストール完了後にアカウントのパスワードを変更する必要があります。

  _PUBLIC アカウントには既定のパスワードはありません。このアカウントが有効になることはないので、パスワードを指定しないでください。

- 通常セキュリティ – 作成されたすべてのアカウントのうち、_PUBLIC を除くアカウントで、特権ユーザ・アカウント用に選択されたものと同じパスワードを受け取ります。インストール完了後にこれらのパスワードを変更し、アカウントごとに独自のパスワードとすることをお勧めします。

  _PUBLIC アカウントには既定のパスワードはありません。このアカウントが有効になることはないので、パスワードを指定しないでください。

- ロック・ダウン・セキュリティ – 作成されたすべてのアカウントのうち、_PUBLIC を除くアカウントで、特権ユーザ・アカウント用に選択されたものと同じパスワードを受け取ります。インストール完了後にこれらのパスワードを変更し、アカウントごとに独自のパスワードとすることをお勧めします。

  _PUBLIC アカウントには既定のパスワードはありません。このアカウントが有効になることはないので、パスワードを指定しないでください。ロック・ダウン・インストールでは、_SYSTEM アカウントも無効になっています。

注意　特に最小のセキュリティによるインストールでは、既定のパスワードはセキュリティ面で脆弱です。この問題を解決するには、そのアカウントを無効にするか、パスワードを変更します。普通はアカウントを無効にすることをお勧めします。

これは特に、コンテナ化されたインスタンスでは重要な問題です。問題を解決する方法を含む詳細は、″認証とパスワード″ を参照してください。

2.1.3 初期のサービス・プロパティ

サービスは、ユーザとコンピュータが InterSystems IRIS に接続するための主要な手段です。インターシステムズのサービスの詳細は、″サービス″ を参照してください。

サービス・プロパティ	最小	通常	ロック・ダウン	説明

サービス・プロパティ	最小	通常	ロック・ダウン	説明
Use 許可が Public	はい	はい	いいえ	サービス・リソースに対する Use 許可が Public である場合、あらゆるユーザがそのサービスを利用できます。それ以外の場合は、権限を与えられているユーザのみがそのサービスを利用できます。
認証が必要	いいえ	はい	はい	初期設定が通常またはロック・ダウンであるインストールの場合、すべてのサービスで何らかの認証が必要になります (インスタンス認証、オペレーティング・システム・ベース、または Kerberos)。それ以外の場合は、非認証の接続が許可されます。

サービス・プロパティ	最小	通常	ロック・ダウン	説明
有効化されるサービス	最も多い	一部	最も少ない	インストールの初期セキュリティ設定によって、InterSys-tems IRIS を最初に起動したとき、どのサービスが有効になり、どのサービスが無効になるかが決定します。次の表 "有効化されるサービス" は、これらの初期設定を示しています。

テーブル 2-1: 有効化されるサービス

サービス	最小	通常	ロック・ダウン
%Service_Bindings	有効	有効	無効
%Service_CacheDirect	有効	無効	無効
%Service_CallIn	有効	無効	無効
%Service_ComPort	無効	無効	無効
%Service_Console*	有効	有効	有効
%Service_ECP	無効	無効	無効
%Service_Monitor	無効	無効	無効
%Service_Telnet*	無効	無効	無効
%Service_Terminal†	有効	有効	有効
%Service_WebGateway	有効	有効	有効

* Windows サーバのみで使用できるサービス

† 非 Windows サーバのみで使用できるサービス

2.2 ユーザ・アカウントの構成

インストール・プロセス中に、InterSystems IRIS プロセスをインスタンス所有者として実行するアカウントを選択する必要があります。インストールにより、インスタンス所有者に対して %All ロールを持つ InterSystems IRIS アカウントが作成され、そのアカウントに InterSystems IRIS への完全な管理者アクセスが付与されます。

インスタンス所有者が必要な特権を確実に持つようにするために、新しいユーザ・アカウントを作成しなければならないこともあります。以下のセクションには、必要なアカウントと特権に関する OS 固有の詳細が示されています。

- Windows ― ″インストール・ガイド″ の “Microsoft Windows への InterSystems IRIS のインストール” の章の ″Windows ユーザ・アカウント″
- Unix® および Linux ― ″インストール・ガイド″ の “InterSystems IRIS の UNIX®、Linux、および macOS へのインストール” の章の ″所有者およびグループの決定″

2.3 Kerberos を使用したセキュリティ環境の準備

InterSystems IRIS でサポートされるすべてのプラットフォームには、ベンダが提供およびサポートするバージョンの Kerberos が備わっています。Kerberos を使用するには、Kerberos KDC (Key Distribution Center) または Windows ドメイン・コントローラがネットワークに接続されている必要があります。それぞれをインストールするための準備は、以下のとおりです。

- Windows ドメイン・コントローラ

  この構成では、InterSystems IRIS サーバとクライアントを Windows および非 Windows マシン上で実行し、Windows ドメイン・コントローラを使用して KDC 機能を実現します。ドメイン管理者は、InterSystems IRIS サーバ上で InterSystems サービスを実行するためのドメイン・アカウントを作成します。Windows および非 Windows の InterSystems IRIS サーバを使用する場合の要件については、以下のセクションを参照してください。

  - Windows サーバ用の Windows サービス・アカウントの作成
  - システムで使用するアプリケーションによっては、″Windows Kerberos クライアントの構成″ で説明されている手順も実行する必要があります。
  - 非 Windows サーバ用の Windows サービス・アカウントの作成

- 非 Windows の KDC

  この構成では、InterSystems IRIS サーバとすべてのクライアントを非 Windows マシン上で実行し、UNIX® または Kerberos の KDC を実現します。UNIX® または macOS KDC と InterSystems IRIS サーバを使用するための要件については、以下の 2 つのセクションを参照してください。

  - KDC での非 Windows サーバのサービス・プリンシパルの作成
  - Kerberos KDC 機能のテスト

用語に関するメモ

このドキュメントでは、以下の関連する個別のエンティティについて言及します。

- サービス・アカウント ― オペレーティング・システム (Window など) 内のエンティティ。ソフトウェア・アプリケーションまたはサービスを表します。
- サービス・プリンシパル ― Kerberos のエンティティ。ソフトウェア・アプリケーションまたはサービスを表します。

2.3.1 Windows サーバ用の Windows サービス・アカウントの作成

KDC と、ドメイン・コントローラ上で動作するその他のセキュリティ・サービスを統合することによって、Kerberos 認証プロトコルを実装します。InterSystems IRIS を Windows ドメインにインストールする前に、Windows ドメイン・コントローラを使用して、Windows マシン上の各 InterSystems IRIS サーバ・インスタンスのサービス・アカウントを作成する必要があります。

2.3.1.1 アカウントの特性

Windows ドメイン・コントローラにこのアカウントを作成する場合は、次のように設定します。

- アカウントの [**パスワードを無期限にする**] プロパティを設定します。
- 作成したアカウントを、InterSystems IRIS サーバ・マシン上の Administrators グループのメンバにします。
- このアカウントを [**サービスとしてログオン**] ポリシーに追加します。

重要　　ドメイン全体のポリシーが有効な場合、正常に InterSystems IRIS を機能させるには、このサービス・アカウントをポリシーに追加する必要があります。

2.3.1.2 名前および名前付け規約

クライアントとサーバが排他的に Windows 上に存在する環境でサービス・プリンシパルに名前を付ける方法には次の 2 種類があります。標準の Kerberos 名前付け規約に従うことも、一意の文字列を使用することもできます。Kerberos 名前付け規約に従うと、今後 Windows 以外のシステムを使用することになった場合にも互換性が保証されます。名前の作成方法の選択によって、サーバへの接続を設定するための手順は多少異なります。

- Kerberos 規約に従った名前では、以下の手順に従います。

  1. Windows の setspn コマンドを実行し、service_principal/fully_qualified_domain_name の形式でサービス・プリンシパルの名前を指定します。service_principal には、通常 `iris` を指定し、fully_qualified_domain_name には、マシン名をドメイン付きで指定します。例えば、`iris/irisserver.example.com` のようにサービス・プリンシパル名を指定します。setspn ツールの詳細は、Microsoft のドキュメントの "Setspn" のページを参照してください。
  2. [**InterSystems IRIS サーバ・マネージャ**] ダイアログで、新しい優先サーバを追加するために [Kerberos] を選択します。[**サービスプリンシパル名**] フィールドに指定する名前は setspn で指定したプリンシパル名と一致する必要があります。

- 任意の一意の文字列を使った名前では、以下の手順に従います。

  1. サービス・プリンシパルの名前を選択します。InterSystems IRIS サーバ・インスタンスを表す各アカウントについて推奨される名前付け規約は "`iris`HOST" の形式で、リテラル `iris` に続けてホスト・コンピュータ名を大文字で指定します。例えば、**WINSRVR** という Windows マシン上で InterSystems IRIS サーバを実行する場合、ドメイン・アカウント名は `irisWINSRVR` となります。
  2. [**InterSystems IRIS サーバ・マネージャ**] ダイアログで、新しい優先サーバを追加するために [Kerberos] を選択します。[**サービスプリンシパル名**] フィールドに、サービス・プリンシパルに対して選択した名前を指定します。

リモート・サーバ接続の構成手順の詳細は、"リモート・サーバへの接続" を参照してください。

2.3.2 Windows Kerberos クライアントの構成

Windows クライアントで Kerberos を使用している場合、ユーザに認証情報の入力を求めないよう、クライアントの構成が必要になることもあります。これは、資格情報を要求できないプログラムを使用している場合に必要となります。そうでないと、プログラムは接続不可能となります。

資格情報の入力を求めないように Windows を構成するには、以下の手順を実行します。

1. Windows クライアント・マシンで、レジストリ・エディタ regedit.exe を起動します。
2. HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Control¥Lsa¥Kerberos¥Parameters キーに進みます。
3. このキーで、AllowTgtSessionKey の値を 1 に設定します。

2.3.3 非 Windows サーバ用の Windows サービス・アカウントの作成

InterSystems IRIS を Windows ドメインにインストールする前に、Windows ドメイン・コントローラを使用して、非 Windows マシン上の各 InterSystems IRIS サーバ・インスタンスのサービス・アカウントを作成する必要があります。そのマシン上に存在する InterSystems IRIS サーバ・インスタンスの数にかかわらず、マシンごとにサービス・アカウントを 1 つ作成してください。

通常、これらのアカウントには“irisHOST”という名前を付けます。iris という文字列の後に、ホスト・コンピュータ名を大文字で指定してください。例えば、UNIXSRVR という非 Windows マシン上で InterSystems IRIS サーバを実行する場合、ドメイン・アカウント名は irisUNIXSRVR となります。非 Windows プラットフォーム上の InterSystems IRIS サーバの場合、このアカウントが Kerberos サービス・プリンシパルにマップされます。

重要　Windows ドメイン・コントローラでこのアカウントを作成する際、InterSystems IRIS では、そのアカウントに [パスワードを無期限にする] のプロパティを設定する必要があります。

Windows ドメインで非 Windows InterSystems IRIS サーバを設定するには、Windows ドメインから keytab ファイルを取得する必要があります。keytab ファイルは、InterSystems IRIS サーバのサーバ名とそのキーが格納されているファイルです。

そのためには、Windows サービス・アカウント (この例では irisUNIXSRVR) を InterSystems IRIS サーバ上のサービス・プリンシパルにマップし、ドメイン・コントローラで ktpass コマンドライン・ツールを使用して、アカウントからキーを取得します。これは、Windows サポート・ツールのひとつとして Microsoft が提供しています。

このコマンドを実行すると、設定したアカウントが UNIX®/Linux マシン上のアカウントにマップされます。さらに、そのアカウントのキーも生成されます。このコマンドでは以下のパラメータを指定する必要があります。

Parameter (パラメータ)	概要
/princ	iris/<fully qualified hostname>@<kerberos realm> の形式で表されたプリンシパル名。
/mapuser	作成されたアカウントの名前 (iris<HOST> の形式)。
/pass	アカウントの作成時に指定されたパスワード。
/crypto	使用する暗号化の種類。指定しない場合は、既定値が使用されます。
/out	生成する keytab ファイル。InterSystems IRIS サーバ・マシンに渡し、既存の keytab ファイルと交換またはマージします。

重要　UNIX®/Linux プラットフォームのプリンシパル名はこのテーブルに示す形式 (リテラル iris を先頭部分に置きます) で指定する必要があります。

キー・ファイルを生成した後、InterSystems IRIS サーバ上のファイルにそのキー・ファイルを移動します。キー・ファイルの特徴は以下のセクションで説明されています。

2.3.4 KDC での非 Windows サーバのサービス・プリンシパルの作成

非 Windows 環境では、UNIX®/Linux または macOS の KDC を使用する UNIX®/Linux または macOS の各 InterSystems IRIS サーバにサービス・プリンシパルを作成する必要があります。サービス・プリンシパル名は、iris/<fully qualified hostname>@<kerberos realm> の形式で表されます。

2.3.4.1 キー・ファイルの特徴

このプリンシパルを作成したら、InterSystems IRIS サーバ上のキー・ファイルにそのキーを抽出します。キー・ファイルの特徴を以下に示します。

- ほとんどのバージョンの UNIX® でのパス名は install-dir/**mgr/iris.keytab** です。macOS および SUSE Linux でのパス名は **/etc/krb5.keytab** です。
- このファイルは、InterSystems IRIS インストールを所有するユーザおよびグループ **irisusr** が所有します。
- このファイルのアクセス許可は、**640** です。

2.3.5 Kerberos KDC 機能のテスト

非 Windows のサーバとクライアントのみで構成したシステムで Kerberos を使用する場合は、Windows のドメイン・コントローラを使用するより、UNIX®/Linux のネイティブな KDC を使用した方が簡単です。KDC のインストール方法と構成方法については、各ベンダのドキュメントを参照してください。通常、KDC のインストールと構成はシステム管理者が行います。

Kerberos をインストールするときは、以下の 2 つのソフトウェア・セットをインストールします。

- KDC。Kerberos サーバ・マシンにインストールします。
- クライアント・ソフトウェア。Kerberos クライアントをホストするすべてのマシンにインストールします。このソフトウェア・セットは、オペレーティング・システムによって大きく異なる場合があります。クライアント・ソフトウェアの種類とそのインストール方法については、オペレーティング・システム・ベンダのドキュメントを参照してください。

必要な Kerberos ソフトウェアをインストールしたら、kadmin、kinit、および klist コマンドを使用した簡単なテストを実行できます。これらのコマンドは、ユーザのプリンシパルを Kerberos データベースに追加し、ユーザの TGT (Ticket-Granting Ticket) を取得したうえで、その TGT を列記します。

テストが完了し、登録されたプリンシパルのチケットを Kerberos が提供できることを確認したら、InterSystems IRIS をインストールする準備は完了です。

3

インスタンスのセキュリティの強化

InterSystems IRIS® データベースのセキュリティをさらに高めるには、ユーザからのアクセスをより厳密に制限するように構成できます。また、そうすることが必要です。これにより、承認されていないユーザは、ツールを使用したり、機密性の高いリソースにアクセスしたりできなくなります。ここでは、データベース・インスタンスの危険を回避し、セキュリティを向上させるためのさまざまな操作について説明します。ここでは、InterSystems IRIS インスタンスが最小の初期セキュリティでインストールされていることが前提となっています。通常またはロック・ダウンの初期セキュリティを選択した場合、これらの操作の一部は既に自動的に実行されています。

ここでは、インスタンスのセキュリティを強化するための操作の概要について、実行すべき順序で説明します。

- 監査の有効化
- アプリケーションの認証メカニズムの変更
- サービスへのアクセス制限。これには以下が含まれます。
  - 有効なサービス数の制限
  - パブリック・サービス数の制限
  - IP アドレスまたはマシン名を基準にしたサービスへのアクセスの制限
- リモート特権アクセスの制限
- 特権ユーザ数の制限
- _SYSTEM ユーザの無効化
- UnknownUser のアクセスの制限
- サードパーティ・ソフトウェアの構成

インターシステムズのセキュリティ・アドバイザは、インスタンスのセキュリティを強化するために、インスタンスの自動解析機能や推奨される操作を提供します。

重要　InterSystems IRIS データベース・インスタンスには相互依存する要素が多数あります。このため、変更のために指定されていることのみを、過不足なく行うことをお勧めします。例えば、**%All** ロールから (その他の操作を一切行わずに) 単純に UnknownUser を削除すると、最小セキュリティ・インストールで問題が発生します。

3.1 監査の有効化

セキュリティの主要な要素は、認証 (Authentication)、承認 (Authorization)、および監査 (Auditing) の“3 つの A”で表されることがよくあります。監査には、以下の 2 つの機能があります。

- セキュリティ・イベントが発生した場合に、何が起こったかに関するデータを提供する。
- 攻撃が追跡、記録され、悪意のある行動に関する証拠がある場合、この機能が存在するとわかっていると、攻撃者に対する抑止力となる。

キー・イベントの監査を有効化する手順は以下のとおりです。

1. 管理ポータルのホーム・ページで、**[システム管理]→[セキュリティ]→[監査]→[監査を有効に]** を選択します。その選択肢が使用できない場合、監査はすでに有効化されています。
2. 管理ポータルのホーム・ページで、**[システムイベントを構成]** ページ (**[システム管理]→[セキュリティ]→[監査]→[システムイベントを構成]**) に移動します。
3. 以下のイベントがまだ有効化されていない場合、**[システムイベントを構成]** ページのそのイベントの行で **[状態変更]** をクリックして、これを有効化します。
   - %System/%DirectMode/DirectMode ー コンソール/ターミナルの使用に関する情報を提供します。コマンド行ユーティリティを重点的に使用するサイトでは、大量のデータが作成される可能性があります。データの増加が問題にならない場合に推奨されます。
   - %System/%Login/Login ー ログインに関する情報を提供します。大規模なサイトでは、大量のデータが作成される可能性があります。データの増加が問題にならない場合に推奨されます。
   - %System/%Login/LoginFailure ー 未承認で試行されたログインに関するフィードバックを提供します。推奨されます。
   - %System/%Security/Protect ー 保護されたデータの読み取り、書き込み、または使用の試行に関するデータを提供します。推奨されます。

3.2 アプリケーションの認証メカニズムの変更

データベースへのアクセス制限では、アプリケーションでより厳密な認証メカニズムが使用されるようにインスタンスを構成することが重要です。このセクションでは、この手順の実行方法について説明します。ここでは、サンプル・アプリケーションとして管理ポータルを使用し、より厳密な認証メカニズムへの移行の例として、最小セキュリティ・インストールのような認証なしのアクセスから、パスワードを要求するアクセスへ変更します。

重要　以下の手順を実行すると、変更されるインスタンスが、ポータルへのアクセス以上のさまざまな影響を受ける可能性があります。この詳細は、(1) インスタンスの構成、および (2) この手順のみを実行しているのか、それともここに示しているすべての手順を実行するのかによって異なります。具体的には、以下を行います。

- %Service_WebGateway:Use をパブリックにしないとは、Web アプリケーションのユーザすべてに、何か別の方法で **`%Service_WebGateway:Use`** を付与する必要があることを意味します。
- UnknownUser を %All ロールから削除すると、さまざまな影響があります。

適切に機能する認証をアプリケーションに提供するには、アプリケーションと、このアプリケーションが使用するサービスの両方に同一の認証メカニズムが必要です。Web アプリケーションでは、Web ゲートウェイ・サービスと一致するように

Web ゲートウェイを構成する必要もあります。したがって、管理ポータルに認証を提供するために、同時に機能させる必要のある以下の 3 つのレイヤがあります。

- **%Service_WebGateway** サービス
- Web ゲートウェイ
- 管理ポータル・アプリケーション

これらのレイヤに対応する認証メカニズムがない場合、通常、アクセスが拒否されます。例えば、ログイン・ページの表示や管理ポータルへのアクセスの代わりに、“ページを表示できません” エラーが表示されます。

重要　(1) Web アプリケーションが Web ゲートウェイや **%Service_WebGateway** よりも強力な認証メカニズムを使用している場合に、(2) 認証に成功すると、システムのセキュリティはそれほど強力ではないメカニズムを提供するものになります。

最小セキュリティ・インストールを持つインスタンスでは、Web ゲートウェイ、**%Service_WebGateway**、および管理ポータル・アプリケーションはすべて非認証アクセス用に設定されます。ポータルにパスワード・レベルの認証を提供するには、さまざまな InterSystems IRIS 要素を以下のように構成する必要があります。

- Web ゲートウェイ・サービスは、パスワード認証を要求する必要があります。
- Web ゲートウェイは、この認証のためにユーザ名とパスワードを提供する必要があります。
- このゲートウェイを表すユーザには、Web ゲートウェイ・サービスを使用するために十分な特権が必要です。
- 管理ポータルにはパスワード認証が必要です。
- ポータルのユーザすべてには、このポータルを使用するために十分な特権が必要です。

重要　ポータルでの 1 回のセッション中に、以下の手順をすべて実行します。そうしないと、ポータルからロックアウトされ、残りの手順を ^SECURITY ルーチンで実行しなければならなくなります。

このような変更を行う手順の概要は以下のとおりです。

1. 必要に応じて、インスタンスへの変更を追跡、記録するために監査を有効化します。詳細は、″監査の有効化″を参照してください。
2. CSPSystem ユーザに %Service_WebGateway:Use 特権を付与します。
3. CSPSystem ユーザのパスワードを変更します。
4. 認証用にユーザ名とパスワードを提供するように Web ゲートウェイを構成します。
5. パスワード認証を要求するように %Service_WebGateway を構成します。
6. %Service_WebGateway:Use 特権のパブリック状態を削除します。
7. パスワード認証のみを要求するように、管理ポータル・アプリケーションを構成します。
8. インスタンスのユーザに対して適切な権限レベルを指定します。
9. 必要に応じて、クラス・リファレンスを使用可能にします。
10. 新しいポリシーの施行を開始します。

この処理の完了後、ユーザがポータルに接続しようとすると、ログイン・プロンプトが表示されます。

注意　InterSystems IRIS データベース・インスタンスには相互依存する要素が多数あります。このため、変更のために指定されていることのみを、過不足なく行うことをお勧めします。そうしないと、インスタンスからロックアウトされる場合があります。また、インスタンスが一時的に動作不能になることもあります。

3.2.1 CSPSystem ユーザに %Service_WebGateway:Use 特権を付与

CSPSystem ユーザは、InterSystems IRIS インストール・プロセスにより作成されます。このユーザは、**%Service_WebGateway** サービスとのやり取りにおける Web ゲートウェイを表します。サービスのアクセスは制限されるので、このユーザは、認証プロセスのために **%Service_WebGateway:Use** 特権を持つ必要があります。

注釈　**%Service_WebGateway** と呼ばれるサービスと、**%Service_WebGateway** と呼ばれるリソースがあります。このリソースは、サービスへのアクセスを規制します。したがって、このサービスにアクセスするには、このリソースに対する Use 許可、つまり **%Service_WebGateway:Use** 特権がユーザに必要です。

%Service_WebGateway:Use 特権を CSPSystem ユーザに関連付けるには、以下の手順を実行します。

1. 管理ポータルのホーム・ページで、[**ロール**] ページ ([**システム管理**]→[**セキュリティ**]→[**ロール**]) に移動します。
2. [**ロール**] ページで、[**新規ロール作成**] をクリックします。[**ロール編集**] ページが表示されます。このページでは、[**名前**] フィールドが編集可能になっています。
3. **%Service_WebGateway:Use** 特権が含まれるように、ロールの名前を入力します (例 : “GatewayRole”)。
4. [**保存**] をクリックします。これにより、InterSystems IRIS にロールが作成されました。
5. [**ロール編集**] ページの [**一般**] タブにある [**特権**] セクションで、[**追加**] をクリックします。このロールについて使用可能なリソースのリストが表示されます。
6. このリストで [%Service_WebGateway] をクリックし、次に [**保存**] をクリックします。新たに作成されたロールには、**%Service_WebGateway:Use** 特権が含まれるようになります。
7. [**ロール編集**] ページの [**メンバ**] タブを選択します。
8. このタブで、新しく作成したロールに CSPSystem ユーザを割り当てることができます。[**使用可能**] リストのユーザから [CSPSystem] をクリックし、右向き矢印をクリックして、[**選択済み**] に移動します。
9. [**割り当てる**] をクリックして、CSPSystem をロールに割り当てます。(つまり、CSPSystem はこのロールのメンバになります)。これは、CSPSystem が **%Service_WebGateway:Use** 特権を持っていることを意味します。

注釈　システムは、Web ゲートウェイを表すために CSPSystem ユーザを作成します。必要であれば、別のユーザがこの機能を実行できます。この手順は CSPSystem ユーザのみを参照します。別のユーザを使用する場合、必要な箇所で CSPSystem をそのユーザ名で置き換えます。

3.2.2 CSPSystem ユーザのパスワードを変更

最小セキュリティ・インストールでは、CSPSystem ユーザに対してパスワード “SYS” が与えられるので、このパスワードを攻撃者の知らないもの、または推測できないものに変更することが重要です。以下はその方法です。

1. 管理ポータルで、[**ユーザ**] ページ ([**システム管理**]→[**セキュリティ**] [**ユーザ**]) に移動します。
2. [**ユーザ**] ページで、[CSPSystem] をクリックします。[**ユーザ編集**] ページが表示されます。
3. [**パスワード**] フィールドに CSPSystem に対する新しいパスワードを入力します。他のユーザは誰もこのパスワードを覚える必要はないので、必要なだけ長く、複雑にすることができます。このパスワードは、次の操作 ″ユーザ名とパスワードを提供するように Web ゲートウェイを構成″ を完了するまでの間、覚えておく必要があります。
4. [**パスワード (再入力)**] フィールドに新しいパスワードを再度入力して、[**保存**] をクリックします。ポータルからエラー・メッセージやダイアログが表示されない場合、パスワードの変更は正常に行われています。

必要に応じて、前の手順で認証のために作成されたロールに CSPSystem が割り当てられていることを確認することもできます。このためには、**[ロール]** タブをクリックします。**[CSPSystem が割り当てられているロール]** という名前の列を持つテーブルには、新しく作成したロールが表示されるはずです。

3.2.3 ユーザ名とパスワードを提供するように Web ゲートウェイを構成

パスワード認証を要求するように **%Service_WebGateway** を構成するため、Web ゲートウェイはユーザ名とパスワードのペアを提供する必要があります。適切な特権レベルを持つユーザをセットアップすると、ゲートウェイが提供できるユーザ名とパスワードのペアが作成されます。次の手順では、InterSystems IRIS サーバから要求されたときに、このユーザ名とパスワードのペアを提供できるようにゲートウェイを構成します。以下はその方法です。

1. 管理ポータルで、**[ウェブゲートウェイ管理]** ページ (**[システム管理]→[構成]→[ウェブゲートウェイ管理]**) に移動します。
2. **[ウェブゲートウェイ管理]** ページで、左側のリストから **[サーバ接続]** を選択します。**[サーバ・アクセス]** フレームが表示されます。
3. **[サーバ・アクセス]** フレームでは LOCAL サーバがハイライト表示されます。編集のために **[実行]** をクリックします。[サーバ・アクセス] パラメータや [エラー・ページ] パラメータの並んだページが表示されます。
4. このページには、**[接続セキュリティ]** セクションがあります。
5. **[接続セキュリティ・レベル]** ドロップダウンに [パスワード] が表示されていることを確認します。
6. **[ユーザ名]** フィールドに、「CSPSystem」と入力します。
7. **[パスワード]** および **[パスワード (確認)]** フィールドに、前のセクションで選択したパスワードを入力します。
8. ページの下部にある **[設定を保存]** をクリックします。
9. 管理ポータルに戻るには、左ペインにあるリスト下部の **[管理ポータルに戻る]** をクリックします。

3.2.4 パスワード認証を要求するように %Service_WebGateway を構成

ユーザ名とパスワードを提供するようにゲートウェイを構成し、CSPSystem ユーザに必要なレベルの特権を付与したら、次に、パスワード認証を要求するように、Web アプリケーションを管理するサービス (**%Service_WebGateway**) を構成します。以下はその方法です。

1. 管理ポータルのホーム・ページで、**[サービス]** ページ (**[システム管理]→[セキュリティ]→[サービス]**) に移動します。
2. **[サービス]** ページで、[%Service_WebGateway] をクリックします。**%Service_WebGateway** の **[サービス編集]** ページが表示されます。
3. **[サービス編集]** ページの **[許可された認証方法]** で **[認証なし]** アクセスが無効化されていること、および **[パスワード]** アクセスが有効化されていること (別名 : “ログイン認証”) を確認します。**[保存]** をクリックします。

3.2.5 %Service_WebGateway:Use 特権のパブリック状態を削除

%Service_WebGateway がパスワード認証を要求し、適切な権限を持つユーザを使用してゲートウェイで認証を行うことができるようになったら、次に、**%Service_WebGateway:Use** をパブリック許可から除外します。以下はその方法です。

1. 管理ポータルのホーム・ページで、**[リソース]** ページ (**[システム管理]→[セキュリティ]→[リソース]**) に移動します。
2. **[リソース]** ページで、**%Service_WebGateway** に対応する行の **[編集]** をクリックします。**%Service_WebGateway** の **[リソース編集]** ページが表示されます。
3. **[パブリック許可]** セクションで **[使用]** ボックスをオフにします。**[保存]** をクリックします。

重要　**%Service_WebGateway:Use** がパブリック特権ではなくなると、これが明示的に付与されたユーザのみが Web アプリケーションを使用できるようになります。これらのユーザのリストを作成し、その他の方法でこの特権を付与する必要が生じる場合もあります。

3.2.6 パスワード認証のみを受け入れるように管理ポータルを構成

ゲートウェイと InterSystems IRIS サーバの間の接続に新しい認証メカニズムが使用されるようになったら、次に、これに見合ったメカニズムが使用されるように管理ポータル・アプリケーションを構成します。この例ではインスタンス認証メカニズムを使用します。ポータルの認証メカニズムを変更するための手順は以下のとおりです。

1. 管理ポータルのホーム・ページで、[**ウェブ・アプリケーション**] ページ ([**システム管理**]→[**セキュリティ**]→[**アプリケーション**]→[**ウェブ・アプリケーション**]) に移動します。
2. [**ウェブ・アプリケーション**] ページでは、/csp/sys アプリケーションは管理ポータルのホーム・ページを表します。このアプリケーションを編集するには、この行の名前 [**/csp/sys**] をクリックします。/csp/sys アプリケーションの [**ウェブ・アプリケーションの編集**] ページが表示されます。
3. [**セキュリティの設定**] の [**許可された認証方法**] で、[**認証なし**] アクセスを無効化し、[**パスワード**] アクセスを有効化します。[**保存**] をクリックします。
4. ポータルのその他のページと選択肢を構成するすべてのアプリケーションに対しても、[**非認証**] アクセスを無効にし、[**パスワード**] アクセスを有効にします。これらのアプリケーションには以下のものがあります。
   - /csp/sys/exp
   - /csp/sys/mgr
   - /csp/sys/op
   - /csp/sys/sec

   注釈　アプリケーション /csp/sys/op を編集した後、さらなる変更を加えるためには認証が必要になります。

このように構成することで、ポータルを使用するにはパスワード認証 (別名は “インスタンス認証”) が必要になり、認証なしアクセスが許可されなくなるので、各構成部分が整合性のある動作をします。次の手順では、関連するユーザがすべて、ポータルへの適切なアクセス権を持つことを確認します。

3.2.7 インスタンスのユーザに対して適切な権限レベルを指定

認証なしアクセスを受け入れるようにポータルが構成されている場合、どのようなユーザでも UnknownUser として接続できます。最小セキュリティ・インストールでは UnknownUser は **%All** ロールのメンバになるので、ポータルからロックアウトされる心配はありません。ここで、ポータルによりパスワード認証が要求されるようになると、正当なユーザは **%Operator** ロール、**%Manager** ロール、または **%All** ロールのメンバとなる必要があります。

最小セキュリティ・インストールでは、SuperUser、Admin、_SYSTEM、および UnknownUser はすべて、このレベルの特権を持ちます。また、パスワードはすべて “SYS” です。

注釈　通常のインストールまたはロック・ダウン・インストールでは、UnknownUser は有効になりますが、ロールは割り当てられません。

通常のインストールまたはロック・ダウン・インストールでは、パスワードはインストール・プロセスで設定されますが、ここで変更することもできます。

適切にユーザのセキュリティを確保する手順は以下のとおりです。

1. UnknownUser を無効化します。または、**%All** ロールから UnknownUser を削除します。

- UnknownUser を無効化する手順は以下のとおりです。
  a. [ユーザ] ページ ([**システム管理**]→[**セキュリティ**]→[**ユーザ**]) で、[**名前**] 列の下の [UnknownUser] をクリックします。UnknownUser に対応する [**ユーザ編集**] ページが表示されます。
  b. [**ユーザ有効**] フィールドをクリアし、[**保存**] をクリックします。
- **%All** ロールから UnknownUser を削除するには、以下の手順を実行します。
  a. [**ユーザ**] ページ ([**システム管理**]→[**セキュリティ**]→[**ユーザ**]) で、[**名前**] 列の下の [UnknownUser] をクリックします。UnknownUser に対応する [**ユーザ編集**] ページが表示されます。
  b. [**ユーザ編集**] ページの [**ロール**] タブに進みます。
  c. [**ユーザ UnknownUser には以下のロールが割り当てられています**] テーブルの **[%All]** 行で、[**削除**] をクリックします。

重要　UnknownUserを通じたアクセスの制限は広い範囲に影響を及ぼします。これは、インスタンスのユーザが十分な特権を持っていない場合に特に顕著です。

2. 認証されていない可能性のあるその他のユーザが、**%All**、**%Developer**、**%Manager**、**%Operator**、**%SQL**、または特権を付与されたその他のユーザ定義ロールのメンバではないことを確認します。このためには、**%All** ロールから UnknownUser を削除するのと類似した処理を行います

   (特権を付与するユーザ定義ロールは、**%Admin...** リソースのいずれか、**%Development**、または **%Service** もしくは **%System** リソースのいずれかに対する Use 許可を持つか、**%DB_IRISLIB** もしくは **%DB_IRISSYS** に対する Write 許可を持つ可能性があります)。
3. ポータルへのアクセス権を持っているはずのユーザがすべて、**%All**、**%Developer**、**%Manager**、**%Operator**、**%SQL**、またはポータルへのアクセスを付与する任意のユーザ定義ロールに割り当てられていることを確認します。これらのユーザそれぞれについて、以下の手順を実行します。
   a. [**ユーザ**] ページ ([**システム管理**] > [**セキュリティ**] > [**ユーザ**]) で、[**名前**] 列の下にあるユーザの名前をクリックします。そのユーザに対応する [**ユーザ編集**] ページが表示されます。
   b. [**ユーザ編集**] ページの [**ロール**] タブに進みます。
   c. 目的のロールを [**使用可能**] から [**選択済み**] リストに移動します。このためには、ロールを選択し、右矢印ボタンをクリックし、[**割り当てる**] をクリックして、ユーザをロールに割り当てます。
4. SuperUser および Admin ユーザのパスワードを既定値から変更します。以下はその方法です。
   a. [**ユーザ**] ページ ([**システム管理**] > [**セキュリティ**] > [**ユーザ**]) で、[**名前**] 列の下にあるユーザの名前をクリックします。そのユーザに対応する [**ユーザ編集**] ページが表示されます。
   b. [**新規パスワード入力**] をクリックします。
   c. [**パスワード**] フィールドに新しいパスワードを入力します。
   d. [**パスワード (確認)**] フィールドでパスワードを確認し、[**保存**] をクリックします。

重要　少なくとも 1 人のポータル管理ユーザのパスワードを知っていることを確認してください。そうしないと、ポータルからロックアウトされ、緊急アクセスを使用してログインし、^SECURITY ルーチンを使って 1 つ以上のパスワードをリセットしなければならなくなる可能性があります。

3.2.8 クラス・ドキュメントを使用可能にする

サービス、Web ゲートウェイ、およびポータル・アプリケーションの構成が完了したら、クラス・ドキュメントを使用できるようにしましょう。以下はその方法です。

1. 管理ポータルのホーム・ページで、[**ウェブ・アプリケーション**] ページ ([**システム管理**] > [**セキュリティ**] > [**アプリケーション**] > [**ウェブ・アプリケーション**]) に移動します。
2. ドキュメントを使用できるようにするには、以下の操作を実行します。
   a. [**ウェブ・アプリケーション**] ページでは、/csp/documatic アプリケーションがクラスリファレンス・アプリケーションです。このアプリケーションを編集するには、この行の [**/csp/documatic**] をクリックします。/csp/documatic アプリケーションの [**ウェブ・アプリケーションの編集**] ページが表示されます。
   b. [**セキュリティの設定**] の [**許可された認証方法**] で、[**認証なし**] アクセスを無効化し、[**パスワード**] アクセスを有効化します。[**保存**] をクリックします。

      注釈　　通常のインストールの場合、パスワード・アクセスは既に有効になっています。

この手順を実行していない場合、サービスはパスワード・プロンプトを要求しますが、アプリケーションは認証なしアクセスを試行します。これにより、**%All** に割り当てられているユーザを含め、すべてのユーザがドキュメントにアクセスできなくなります。

3.2.9 新しいポリシーの施行を開始

この時点で、InterSystems IRIS インスタンスの構成は完了し、適切な動作をするようになっています。ただし、既存のすべての接続で、引き続き非認証アクセスが使用されています。新しいポリシーの施行を開始するには、次のイベントが発生しなければなりません。

- Web ゲートウェイは、認証接続を確立する必要があります。
- また、すべてのユーザも認証接続を確立する必要があります。

3.2.9.1 認証された Web ゲートウェイ接続の確立

Web ゲートウェイに認証接続を確立させるには、次の手順を実行します。

1. 管理ポータルのホーム・ページで、[**システム管理**]→[**構成**]→[**ウェブゲートウェイ管理**] を選択します。[**ウェブゲートウェイ管理**] ページが表示されます。
2. [**ウェブゲートウェイ管理**] ページで、左側のリストから [**接続を閉じる**] を選択します。[**接続を閉じる**] フレームが表示されます。
3. [**接続を閉じる**] をクリックします。これにより、ゲートウェイと InterSystems IRIS サーバ間の接続がすべて閉じられたことを示すメッセージが表示されます。

次回ユーザがページを要求すると、ゲートウェイにより、InterSystems IRIS サーバへの接続が再度確立されます。この接続では、選択された認証メカニズムが使用されます。

3.2.9.2 認証されたユーザ接続の確立

この時点では、管理ポータルへのすべての接続で、依然として認証なしアクセスが使用されています。すぐに認証アクセスが必要でない場合、何もする必要はありません。ユーザはポータルへの接続を順次終了し、再接続するときに認証が必要となります(接続の終了する理由には、マシンの再起動、ブラウザの停止と再開、ブラウザ・キャッシュのクリア、ポータルのログアウトなどがあります)。

接続で強制的に認証アクセスを使用する必要がある場合、以下のようにして InterSystems IRIS を停止し、再起動します。例えば、Windows で、InterSystems IRIS が既定の [スタート] メニューのページで利用できる場合、以下のようにします。

1. Windows の [スタート] メニューから **[プログラム]→[InterSystems IRIS]** を選択し、InterSystems IRIS インスタンスを再起動します。
2. InterSystems IRIS インスタンスのサブメニューで、**[インターシステムズの停止]** を選択します。
3. 表示されたダイアログで、**[再起動]** を選択し、[OK] をクリックします。

注釈　InterSystems IRIS の実稼動インスタンスを使用している場合、ユーザは一時的に、InterSystems IRIS 全体またはポータルへアクセスできなくなるため、再起動にはトラフィックが少ない時間を選択します。

3.3 パブリック・リソース数の制限

どのようなリソースでも、パブリック・リソースとして指定できます。つまり、どのようなユーザでも、パブリック設定に応じて、このリソースを読み取り、書き込み、または使用できます。以下のリソースおよび許可は、常にパブリックにする必要があります。

テーブル 3-1: 必須のパブリック・リソースおよびその許可

リソース	許可
%DB_IRISLOCALDATA	R
%DB_IRISLIB	R
%DB_IRISTEMP	RW

インスタンスのセキュリティを強化する場合は、パブリック・リソースの数を制限してください。そのための手順は以下のとおりです。

1. これらのリソースへのアクセスを本当に必要としているすべてのユーザに、必要な特権が与えられていることを確認します。

   重要　**%Service_WebGateway:Use** に対する特権を適切なユーザに提供しなかった場合、この手順により、管理ポータルやその他の Web アプリケーションからの大規模なロックアウトが発生する場合があります。

2. 管理ポータルのホーム・ページで、**[リソース]** ページ (**[システム管理]→[セキュリティ]→[リソース]**) に移動します。
3. リソースに対するパブリック許可が 1 つ以上ある場合、各リソースの所有する権限は、**[リソース]** ページのリソース・テーブルにある **[パブリック許可]** 列にリストされます。**[編集]** をクリックしてリソースを選択します。選択したリソースの **[リソースの編集]** ページが表示されます。
4. **[リソースの編集]** ページで、チェックマークが付けられている **[パブリック許可]** フィールドをすべてクリアし、**[保存]** をクリックします。このリソースはパブリックではなくなります。

すべてのパブリック・リソースについて、この操作を実行します。

3.4 サービスへのアクセス制限

ユーザが InterSystems IRIS と対話する経路にはさまざまな種類があります。サービスは、これらの経路へのアクセスを規制します。インターシステムズのサービスへのアクセスを制限するには、以下の選択肢があります。

- 有効なサービス数の制限。使用しているアプリケーションで必要なもののみにします。
- パブリック・サービス数の制限。使用しているアプリケーションで必要なもののみにします。
- IP アドレスまたはマシン名を基準にしたサービスへのアクセスの制限

3.4.1 有効なサービス数の制限

有効なサービス数を制限するには、以下の手順を実行します。

1. InterSystems IRIS インスタンスで必要なサービスを判断します。通常、これらは以下のとおりです。
   - ユーザ・アクセスの各形式で必要とされるサービス
   - 自動アクセスで必要とされるサービス
   - ローカルなプログラマ・モード・アクセスのための **%Service_Console** (Windows の場合) または **%Service_Terminal** (UNIX または UNIX® の場合)
2. 管理ポータルのホーム・ページで、[**サービス**] ページ ([**システム管理**] > [**セキュリティ**] > [**サービス**]) に移動します。
3. [**サービス**] ページで、必要のないサービスそれぞれの名前をクリックして選択します。選択したサービスの [**サービス編集**] ページが表示されます。
4. [**サービス編集**] ページで、[**サービス有効**] フィールドをクリアし、[**保存**] をクリックします。これで、このサービスは無効化されました。

必要のないサービスをすべて無効化すると、InterSystems IRIS への経路はサービスに必要な経路のみになります。

3.4.2 パブリック・サービス数の制限

各サービスはリソースに対応します。ほとんどの場合、リソースとサービスは同じ名前を持ちます (例 : **%Service_WebGateway**)。ただし、**%Service_Bindings** サービスは例外で、**%Service_Object** リソースおよび **%Service_SQL** リソースと関連付けられています。サービスは、それに関連付けられているリソースの設定のため、パブリックです。したがって、サービスを非パブリックにする手順は、その他のリソースを非パブリックにする手順と同じです。これについては、"パブリック・リソース数の制限" で説明しています。

3.4.3 IP アドレスまたはマシン名を基準にしたサービスへのアクセスの制限

一部のサービスでは、IP アドレスやマシン名に従って、サービスへのアクセスを制限することができます。これは、“許可された接続” を制限する機能と言われます。この機能をサポートしているサービスは以下のとおりです。

- **%Service_Bindings**
- **%Service_CacheDirect**
- **%Service_ECP**
- **%Service_Monitor**
- **%Service_Shadow**

- **%Service_WebGateway**

既定では、サービスはすべてのマシンからの接続を受け入れます。サービスにアドレスやマシン名が関連付けられていない場合、このサービスはすべてのマシンからの接続を受け入れます。サービスが接続を受け入れるアドレスやマシン名が 1 つ以上指定されている場合、サービスはこれらのマシンからの接続のみ受け入れます。

この機能は、**%Service_CallIn**、**%Service_ComPort**、**%Service_Console**、**%Service_DataCheck**、**%Service_Login**、**%Service_Mirror**、**%Service_Telnet**、および **%Service_Terminal** では使用できません。

IP アドレスを基準にサービスへのアクセスを制限するには、以下の手順に従います。

1. サービスへの正当なアクセスを持つマシンの IP アドレスを判断します。
2. 管理ポータルのホーム・ページで、[**サービス**] ページ ([**システム管理**]→[**セキュリティ**]→[**サービス**]) に移動します。
3. [**サービス**] ページで、IP アドレスを基準にアクセスを制限するサービスの名前を個別にクリックして選択します。選択したサービスの [**サービス編集**] ページが表示されます。
4. [**サービス編集**] ページの [許可された接続] セクションで、[**新規追加**] をクリックします。
5. 表示されたダイアログに、接続を許可する IP アドレスを入力します。[OK] をクリックします。
6. [**新しく追加**] をクリックし、必要なアドレスを入力します。

接続を許可する IP アドレスを制限するサービスそれぞれについて、この手順を実行します。

3.5 リモート特権アクセスの制限

InterSystems IRIS は、ECP リモート・ジョブ要求をサポートしています。ただし、リモート・ジョブはサーバ上で root として実行されるので、意図した以上の特権でユーザがサーバ上で作業できる可能性があります。リモート・ジョブの扱いを無効にして、サーバへのリモート特権アクセスを制限するには、"このパラメータの変更" の手順に従い、**netjob** を `false` に設定します。既定ではこの設定は `true` になっています。

3.6 特権ユーザ数の制限

すべての InterSystems IRIS インスタンスには、**%All** ロールに割り当てられたユーザが少なくとも 1 人必要です。実際、このロールに割り当てられたユーザが 1 人のみの場合、InterSystems IRIS はこのロールからこのユーザを削除できないようにします。しかし、時間の経過に従って、あるインスタンスの **%All** に必要以上のユーザが割り当てられてしまうことがあります。その原因には、割り当てられたユーザは組織を離れたがアカウントが無効化されていない、一時的な割り当てが削除されていないなどがあります。

%All ロールと共に、システム定義ロールの **%Manager**、**%Developer**、**%Operator**、および **%SQL** もユーザに過度の特権を与えることができます。また、このような動作を行うユーザ定義ロールもあります。このようなロールに割り当てられたユーザは、“特権ユーザ”と呼ばれることもあります。

特権ユーザの数を制限するには、どのユーザが各特権ロールに割り当てられているかを判断し、不要なユーザを削除します。以下はその方法です。

1. 管理ポータルのホーム・ページで、[**ロール**] ページ ([**システム管理**]→[**セキュリティ**]→[**ロール**]) に移動します。
2. [**ロール**] ページで、ロールの名前をクリックします。そのロールに対応する [**ロール編集**] ページが表示されます。

3. [**ロール編集**] ページの [**メンバ**] タブをクリックします。そのロールに割り当てられているユーザとロールのリストが表示されます。
4. 指定されたロールからユーザを削除するには、削除するユーザまたはロールの行にある [**削除**] をクリックします。

%All および前述のその他のロールを含め、特権ロールそれぞれについてこの手順を実行します。また、_SYSTEM ユーザを無効化することも重要です。その手順については、"_SYSTEM ユーザの無効化" で説明します。

重要　一見して特権のないロールが“代理特権”とも呼べる特権を持っていることもあります。この現象は、一見して特権のないロールを特権ロールに割り当てているときに発生します。この場合、代理特権を持つロールに割り当てられたすべてのユーザは、特権ロールに関連付けられたすべての特権を持ちます。

可能な限り、代理特権は作成しないようにしてください。どうしても避けられない場合、代理特権を持つロールに割り当てるユーザの数はできる限り少なくします。

3.7 _SYSTEM ユーザの無効化

InterSystems IRIS インストール・プログラムは _SYSTEM ユーザを作成します。このユーザは、SQL 標準に従って、SQL ルート・ユーザとして作成されます。最小セキュリティ・インストールでは、このユーザの既定のパスワードは“SYS”です。標準およびロックダウン・インストールの既定のパスワードは、インストール処理中に指定されたものになります。このユーザとパスワード“SYS”がどちらも SQL 標準により公開されているため、またこのユーザの SQL 特権のため、_SYSTEM を無効化することは、InterSystems IRIS インスタンスへのアクセスを制限するために重要です。

そのための手順は以下のとおりです。

1. 管理ポータルのホーム・ページで、[**ユーザ**] ページ ([**システム管理**]→[**セキュリティ**]→[**ユーザ**]) に移動します。
2. [**ユーザ**] ページで、名前 [**_SYSTEM**] をクリックして、_SYSTEM の [**ユーザ編集**] ページを開きます。
3. _SYSTEM の [**ユーザ編集**] ページで、[**ユーザ有効**] フィールドをクリアします。[**保存**] をクリックします。

注釈　_SYSTEM を無効化した後でルート・レベルの SQL 特権を確認する必要がある場合は、必要な操作を実行できるように、ユーザを一時的に有効化する必要があります。

3.8 UnknownUser のアクセスの制限

認証なしアクセスをサポートしているインスタンスでは、認証を使用しない接続は UnknownUser アカウントを使って確立されます。最小セキュリティ・インストールでは、既定の動作は以下のようになります。

- すべての接続で UnknownUser が使用されます。
- UnknownUser は **%All** ロールに割り当てられます。
- UnknownUser は SQL 特権をすべて保持しています。

UnknownUser のアクセスを制限するには、有効なすべてのサービスの認証なしアクセスを無効にします (その他の操作は効果がないか、管理ポータルからロックアウトされる可能性があります)。

注釈　このセクションでこれまでに示したすべての操作の実行を完了している場合、既に UnknownUser の無効化とパブリック・リソース数の制限が完了している可能性があります。

3.8.1 UnknownUser アカウントで発生する可能性のあるロックアウトの問題

あるインスタンスが最小セキュリティでインストールされている場合、UnknownUser のロールは **%All** になります。また、このインスタンスは、すべてのサービスおよびアプリケーションに対して、認証なしアクセスを提供します。このユーザのロールを単に **%All** から別のものに変更しても、認証なしアクセスを引き続き許可している場合は、基本機能を使用できない可能性があります。

これは、このような状況では、認証が行われないまま、InterSystems IRIS により、選択したツールへの接続が確立されるからです。認証が行われないと、システムにより、自動的にユーザ・アカウントが UnknownUser に設定されます。次に、ユーザ特権がチェックされます。UnknownUser が十分な特権を持っていない場合、ツールへのアクセスは制限されるか不可能になります。このような状況では、例えば、ターミナルには“アクセスが拒否されました”というメッセージが表示され、シャットダウンされます。ポータルではメイン・ページは表示されますが、オプションは一切選択できません。

この状態を正常に戻すには、以下の手順に従います。

1. InterSystems IRIS を緊急アクセス・モードで起動します。
2. UnknownUser アカウントに十分な特権を与えます。

UnknownUser を使用できないようにするには、管理ポータルに対する認証メカニズムをアップグレードする必要があります。

3.9 サードパーティ・ソフトウェアの構成

インターシステムズ製品は、ウイルス・スキャンなどのインターシステムズ製ではないツールと共に実行したり、そのようなツールとやり取りすることが頻繁にあります。このようなやり取りでもたらされる可能性がある影響に関する重要な情報については″インターシステムズ製品と連係して動作するようにサードパーティ・ソフトウェアを構成する方法″を参照してください。

4

セキュリティ・アドバイザ

InterSystems IRIS システムの保護においてシステム・マネージャを支援するために、InterSystems IRIS 管理ポータルにはセキュリティ・アドバイザと呼ばれるツールが組み込まれています。これは、セキュリティに関連してシステム構成に収められている現在の情報を表示する Web ページです。セキュリティ・アドバイザでは、推奨される変更点や見直すべき領域が示され、推奨される変更を行うための管理ポータル内のページへのリンクが提供されます。

重要　セキュリティ・アドバイザが提供するのは一般的な推奨内容であり、そこではインスタンス固有のニーズや要件は考慮されていません。InterSystems IRIS のインスタンスにはそれぞれ固有の要件と制約がある点を念頭に置くことは重要です。セキュリティ・アドバイザには、目的のインスタンスに無関係な問題が表示されることもあれば、重要度の高い問題が表示されないこともあります。例えば、サービスで Kerberos 認証のみを使用することがセキュリティ・アドバイザで推奨されていても、実際の稼動環境によっては、オペレーティング・システムによる認証やインスタンス認証、さらには非認証のアクセスが適切な場合もあり得ます。

セキュリティ・アドバイザには、以下のような一般的な機能があります。

- **[詳細]** ボタン ― 各選択項目には **[詳細]** ボタンがあります。このボタンを選択すると、その選択項目に関連する InterSystems IRIS の詳細を管理するためのページが、セクションの制限内容に応じて表示されます。
- **[名前]** ボタン ― 各セクションで指定されている項目は、それぞれがリンクとして表示されます。これらの項目のいずれかを選択することで、その項目を管理するためのページが表示されます。
- **[無視]** チェック・ボックス ― 各セクションで指定されている項目ごとに、その項目に関連付けられた **[無視]** チェック・ボックスがあります。項目が特定の要件に該当しないと判断した場合にこのチェック・ボックスにチェックを付けると、指定した項目の行がグレー表示になります。セキュリティ・アドバイザの推奨に従って InterSystems IRIS を設定している場合は、**[無視]** チェック・ボックスの設定に関係なく、この行は表示されなくなります。

4.1 監査

このセクションには、監査そのものおよび特定の監査イベントに関する推奨事項が表示されます。これには以下のものがあります。

- 監査を有効にするべきです ― 監査を実行すると、注意の必要なシステム・イベントや異常なシステム・イベントが発生した後で、検討作業に有用な情報を収めた記録が作成されます。
- この種類の監査イベントは有効にするべきです ― 特定のイベントを監査することで、さまざまなトピックに関する詳細な情報が得られます。特に、監査が有効になっていないときに注目されるイベントは以下のとおりです。

- DirectMode イベント ー このイベントを監査することで、ユーザに重大な特権を与える InterSystems IRIS 接続に関する情報が得られます。
- Login イベント ー このイベントを監査することで、疑義のあるログインに関する情報が得られます。
- LoginFailure イベント ー このイベントを監査することで、システムに対する不適切なアクセス権を得ようとする操作に関する情報が得られます。

4.2 サービス

ここでは、インターシステムズのサービスに関する推奨事項について説明します。セキュリティ・アドバイザでは、サービスごとにその設定に応じて以下の点が指摘されます。

- % グローバルを更新できる設定は無効にするべきです ー パーセントで始まるグローバルにはシステム情報が保持されていることが多いので、ユーザがこれらのグローバルを操作できるようになっていると、深刻で広範囲に及ぶ予測不能な影響が出る可能性があります。
- 非認証は無効にされるべきです ー 未認証の接続があると、身元が不確かな UnknownUser アカウントを含むすべてのユーザが、該当のサービスを通じて InterSystems IRIS に無制限にアクセスできます。
- 要求があるまでサービスを無効にするべきです ー セキュリティ・アドバイザで監視されているサービスを介したアクセスでは、システムに対する過剰なレベルのアクセスが可能になります。
- サービスは Kerberos 認証を使用するべきです ー Kerberos 以外の認証メカニズムを通じたアクセスでは、Kerberos 以上のレベルのセキュリティ保護が得られません。
- サービスにはクライアント IP アドレスを割り当てるべきです ー 接続を受け入れる IP アドレスの数を制限することで、より確実に InterSystems IRIS への接続を監視できるようになります。
- サービスはパブリック ー パブリック・サービスがあると、身元が不確かな **UnknownUser** アカウントを含むすべてのユーザが、そのサービスを通じて InterSystems IRIS に無制限にアクセスできます。

4.3 ロール

このセクションでは、過剰な特権を持っている可能性のあるすべてのロールに関する推奨事項について説明します。それ以外のロールについては取り上げません。ロールごとに、セキュリティ・アドバイザでは以下の点が指摘されます。

- ロールが監査データベースに対する権限を保持しています ー 監査データベースに対する読み取りアクセスによって、不適切な範囲まで監査データが公開される可能性があります。また、書き込みアクセスによって、監査データベースにデータが不適切に挿入される可能性があります。
- このロールは **%Admin_Secure** 権限を所有しています ー この権限を使用すると、アセットに対するユーザのアクセスを設定、変更、および拒否できます。また、セキュリティ関連の他の機能を変更できます。
- このロールは **%IRISSYS** データベースの書き込み権限を所有しています ー **%IRISSYS** データベースに対する書き込みアクセスによって、システムのコードおよびデータが漏洩する可能性があります。

4.4 ユーザ

ここでは、ユーザ全般に関する推奨事項および個々のユーザ・アカウントに対する推奨事項について説明します。この領域では、セキュリティ・アドバイザで以下の点が指摘されます。

- 少なくとも 2 名から最大 5 名のユーザが **%All** ロールを保持する必要があります ー **%All** ロールを持つユーザが少なすぎると、緊急時にアクセス上の問題につながることがあります。また、多すぎると、システムの公開性が高くなりすぎて機密漏洩につながる可能性があります。
- このユーザは **%All** ロールを所有しています ー どのユーザが %All ロールを持っているかを明示的に公表することで、無関係なユーザが %All ロールを持つことを防止できます。
- UnknownUser アカウントは **%All** ロールを持つべきではありません ー 匿名のユーザがすべての権限を持っていると、システムのセキュリティが確保できません。最小のセキュリティ・レベルを持つインスタンスでは、UnknownUser アカウントに %All ロールが与えられていますが、このようなインスタンスのセキュリティを計画的に確保することはできません。
- アカウントが使用されていません ー 承認されないアクセスを得ようとする侵入者にとって、使用されていないアカウントは絶好の侵入ポイントになります。
- アカウントが休眠状態のようですので無効にするべきです ー 承認されないアクセスを得ようとする侵入者にとって、休止状態のアカウント (31 日以上使用されていないアカウント) は絶好の侵入ポイントになります。
- パスワードを既定のパスワードから変更するべきです ー 既定のままのパスワードは、承認されないアクセスを得ようとする侵入者によって侵入ポイントとしてよく利用されます。

4.5 Web アプリケーション、特権ルーチン・アプリケーション、およびクライアント・アプリケーション

アプリケーションごとに専用のセクションがあり、そこではそれぞれのアプリケーション・タイプの詳細を容易に確認できます。これらのセクションには、アプリケーションへのアクセスおよびアプリケーションによって与えられている特権に関連する推奨事項が表示されます。この領域では、セキュリティ・アドバイザで以下の点が指摘されます。

- アプリケーションがパブリックです ー パブリックなアプリケーションがあると、身元が不確かな **UnknownUser** アカウントを含むすべてのユーザが、そのアプリケーションに関連付けられたデータおよびそのアプリケーションでサポートされているアクションに無制限にアクセスできます。アプリケーションによって **%All** ロールも与えられている場合は、それが条件付きでも無条件でも、この影響はさらに大きくなります。
- 条件によりアプリケーションは **%All** ロールを付与します ー ユーザがすべての権限を持つ可能性があると、システムのセキュリティを確保できなくなります。アプリケーションがパブリックでもある場合、この影響はさらに大きくなります。
- アプリケーションは **%All** ロールを付与します ー ユーザがすべての権限を持っていると、システムのセキュリティを確保できなくなります。アプリケーションがパブリックでもある場合、この影響はさらに大きくなります。

5

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

5.1 概要

このドキュメントでは、InterSystems IRIS® データ・プラットフォームのインスタンスを実行しているオペレーティング・システムのセキュリティを強化することによって、侵入者の攻撃対象となり得る領域を減らす方法を説明します。トピックは以下のとおりです。

- InterSystems IRIS インスタンスで必要なオペレーティング・システム・サービス
- さまざまなタイプの InterSystems IRIS プロセス、および各プロセスの目的
- 実行中インスタンス内の InterSystems IRIS プロセスの機能を特定する方法
- 自身のサイトには不要と思われるオプションの InterSystems IRIS プロセスを削除または無効化する方法
- UNIX® 上の **iris** プロセスまたは Windows 上の **irisdb.exe** プロセスに加えて、実行中のインスタンスに必要なプロセス
- InterSystems IRIS プロセスに使用する TCP ポートと UDP ポート、および各ポートの目的

5.2 InterSystems IRIS プロセス

InterSystems IRIS インスタンスが含まれているほとんどのプロセスでは、UNIX® の場合は iris 実行可能ファイル、Windows の場合は irisdb.exe 実行可能ファイルが使用されます。これらの実行可能ファイルはそれぞれ、インストール・ディレクトリ下の **bin** ディレクトリにあります。実行中のインスタンスは、さまざまなシステム・プロセスを使用して、ユーザ・コードを実行しているプロセスを調整およびサポートします。InterSystems IRIS プロセスは、管理ポータルで **[システムオペレーション]→[プロセス]** に移動して調べることができます。

5.2.1 コア・プロセス

コア・システム・プロセスは、インスタンス初期化の早期段階で開始され、**User** 列に値を持っていません。これらのプロセスは **Routine** 列の値によって識別できます。システム・プロセスの場合、この列に InterSystems IRIS ルーチンの名前が常に含まれているわけではありません。**Routine** 列には、以下のコア・システム・プロセスが名前別に表示されます。

- CONTROL – 共有メモリを作成および初期化して、各種の制御関数を提供します。
- WRTDMN – データベースおよび WIJ へのすべての書き込みを実行します (ライト・デーモン)。
- GARCOL – サイズの大きいキルをガーベッジ・コレクションします。
- JRNDMN – ジャーナル書き込みを実行します。
- EXPDMN – データベース拡張を実行します。
- AUXWD – ライト・デーモン・タスクを実行します (ライト・デーモン予備ワーカ)。
- MONITOR – アラートをアラート・ファイルに書き込んで、電子メール・アラートを送信します。
- CLNDMN – 停止しているプロセスを検知して、立ち往生しているリソースをクリーンアップします。
- RECEIVE – ECP ワーカ・プロセスを管理します。
- ECPWork – ECP タスクを実行します (ECP ワーカ・プロセス)。
- %SYS.SERVER – TCP 要求を受け取り、それらの要求を処理するようにワーカをディスパッチします (スーパーサーバ・プロセス)。
- %CSP.Daemon – Web セッションの期限切れを管理します。
- LMFMON – InterSystems IRIS ライセンスを監視して、使用状況データを UDP 経由でライセンス・サーバに送信します。
- %SYS.Monitor.xxx – システム監視タスクを実行します (さまざまなシステム監視ワーカ)。
- SYS.Monitor.xxx – アラートをアラート・ファイルに書き込んで、電子メール・アラートを送信します。

コア・システム・プロセスを停止することはできません。これらのプロセスを停止すると、InterSystems IRIS インスタンスは正常に動作できなくなります。

他のさまざまな InterSystems IRIS システム・プロセスがコア・システム・プロセスの後に開始されます。これらの多くは動的に開始されます。これらのプロセスについては、User 列に値が表示されます。これらのプロセスの多くは必須ではないため、必要な場合や構成されている場合を除いて開始されません。これらのプロセスは通常、プロセス表示の **Routine**、**User**、および **Client EXE** の各列の値によって識別できます。

インスタンス開始時に、タスク・マネージャ・プロセス (TASKMGR) が作成されます。このプロセスは、各種のスケジュールされたシステム定義タスクとユーザ定義タスクを開始して、次の設定に基づいて実行されます。

- ユーザ名 = TASKMGR
- ルーチン = %SYS.TaskSuper.1
- オペレーティング・システム・ユーザ名 = TASKMGR

ECP を使用していない場合、次の手順を実行することで、ECPWork プロセスが開始されることを防止できます。

1. 管理ポータルから、**[システム管理]→[構成]→[接続性]→[ECP設定]** を選択して、アプリケーション・サーバとデータ・サーバの最大数をゼロに設定します。
2. ECP サービスを無効にします。

5.2.2 ECP サーバ・プロセス

動的に開始される ECP サーバ・プロセスは、“ECP” で始まるルーチン名を持ちます。ユーザ名またはオペレーティング・システム・ユーザ名は通常は **Daemon** または **%System** ですが、Windows 上のインスタンス・サービス・ユーザの名前である場合もあります。以下にプロセス名の例を示します。

- ECPCliR – ECP クライアント・リーダ

- ECPCliW – ECP クライアント・ライター
- ECPSrvR – ECP サーバ・リーダ
- ECPSrvW – ECP サーバ・ライター

5.2.3 Web サーバ・プロセス

Web サーバ・プロセスは動的に開始されます。これらのプロセスは、アイドル状態でタスクを待っているときは、User 列に CSPSystem と表示されます。これらのプロセスがアクティブのときは、Web セッションの InterSystems IRIS ユーザと現在のルーチン名が表示されます。OS Username 列には Web Gateway と表示されます。

- %SYS.cspServer および %SYS.cspServer2 – Web アプリケーション要求を処理するためにプロセスで使用される Web サーバ・ルーチン。
- %SYS.cspServer3 – 非同期通信を処理し、Web ゲートウェイ管理を行うためにプロセスで使用される Web サーバ・ルーチン。

これらのプロセスは、他のインターシステムズ製品の従来のアプリケーションに関連付けられています。このようなアプリケーションにおけるこれらのルーチンの詳細は、この機能に関するよくある質問で該当する質問を参照してください。

注釈　これらのルーチンはライセンスを使用しません。ライセンスは、Web アプリケーション・セッションに関連付けられます。

これらのサーバそれぞれの実行可能ファイルは、Windows では CSPAP.dll であり、UNIX® では CSPap.so です。オペレーティング・システム・ユーザ名は `Web Gateway` です。プログラム名は、プロセスでタスクが変更されるたびに変化する可能性があります。

5.2.4 ミラー・システム・プロセス

ミラー・システム・プロセスが開始されるのは、ミラーリングが構成されている場合です。これらのプロセスは、ミラーリングに関するさまざまな機能を実行します。

- MIRRORMGR – ミラー・マスター。ユーザ名は、実行されるミラー機能を表します (`Mirror Master`、`Mirror Primary`、`Mirror Dejournal`、`Mirror Prefetch`、または `Mirror JrnRead`)。オペレーティング・システム・ユーザ名は `Daemon` です。TCP ポートは開かれません。デバイスはオペレーティング・システムの NULL デバイスです。
- MIRRORCOMM – ミラー通信プロセス。ユーザ名は `Mirror Arbiter`、`Mirror Backup`、または `Mirror Svr:RdDmn` です。オペレーティング・システム・ユーザ名は `Daemon`です。デバイスは `|TCP|XXX`です。TCP ポートは、デバイス名またはミラー構成から確認できます。

5.3 IP プロトコル

5.3.1 TCP

InterSystems IRIS インスタンスは、構成オプションで指定されている TCP/IP ポート上の接続を受け付けます。ポートの使用に関するオペレーティング・システム側の制約事項 (ファイアウォールに関するものなど) がある場合は、InterSystems IRIS 向けに構成されているポートと一貫したポート設定によって着信アクセスを許可する必要があります。ファイアウォールで実行可能ファイルのルールが設定されている場合は (Windows 上のファイアウォールでルールが設定されているの

と同様に)、必要に応じてプログラムにも許可を付与してください。例えば、irisdb.exe、licmanager.exe、ISCAgent.exe、および httpd.exe の各実行可能ファイルはこのような許可を必要とします。

InterSystems IRIS で使用される TCP/IP ポートは、インスタンス構成によって設定されています。構成されているポートは、インストール・ディレクトリ内の `iris.cpf` ファイルで調べることができます。`[Startup]` セクションでは、`DefaultPort`、`DefaultPortBindAddress`、および `WebServerPort` を構成します。`DefaultPort` では、スーパーサーバが接続を受け付けるポートを指定します。既定値は 1972 です。`DefaultPortBindAddress` では、必要に応じてスーパーサーバのバインド先であるインタフェース・アドレスを指定します。`WebServerPort` では、プライベート Web サーバが接続を受け付けるポートを指定します。既定値は 52773 です。

プライベート Web サーバはほとんどの場合は開発環境で使用されるため、運用環境で使用することは推奨されません。

`[SQL]` セクションにある `JDBCGatewayPort` では、Java Database Connectivity (JDBC) ゲートウェイ・ポート番号を定義します。既定値は 62972 です。

`[Telnet]` セクションにある `Port` 値では、InterSystems Telnet サービス (ctelnetd.exe) が Windows 上の InterSystems IRIS への Telnet 接続を受け付けるポートを指定します。

5.3.2 UDP

InterSystems IRIS とライセンス・サーバ (licmanager または licmanager.exe) は、主に UDP プロトコルを使用して通信します。InterSystems IRIS は、メッセージを UDP パケットとしてライセンス・サーバのポートに送信します。このポートは既定では 4002 であり、管理ポータルの [システム管理]→[ライセンス]→[ライセンスサーバ] で設定します。ライセンス・サーバが InterSystems IRIS に応答するために使用するポートは、InterSystems IRIS が元のメッセージを送信するために使用したポートです (ライセンス・サーバはパケット・ヘッダで該当ポートを確認します)。TCP は、クエリ要求時に InterSystems IRIS とライセンス・サーバの間でのみ使用されます。InterSystems IRIS は、受け付け/リッスンのために TCP ポートをオープンして、このポート番号をクエリ要求に格納して送信します。ライセンス・サーバはそのポートに接続して、結果を TCP 接続を介して送信します。ポート番号はライセンス・サーバのポート番号とします。そのようにしないとポート 0 が使用され、開いているポートを無作為に選択するようにオペレーティング・システムに指定することになります。ここで指定したポートは、クエリ結果の送信時にのみ開きます。

5.3.3 SNMP

%System_Monitor サービスを使用すると、InterSystems IRIS は管理対象システム上の SNMP エージェントに対するサブエージェントとして機能します。このサービスは、InterSystems IRIS の管理とデータの監視 (提供されている MIB で定義) のための SNMP 要求 (GET または GETNEXT) と、SNMP トラップ (InterSystems IRIS によって送信される非同期通知) の両方をサポートしています。%System_Monitor サービスを無効にすると、ローカル・システム上の SNMP エージェントと InterSystems IRIS の間のすべての通信が無効になり、その結果としてすべてのリモート SNMP マネージャ・アプリケーションとの通信も無効になります。

5.3.4 HTTP

HTTP 要求を処理するために InterSystems IRIS で使用される Web ゲートウェイのコンポーネントに関する説明を参照してください。このためには、[ドキュメント]→[InterSystems IRIS Web 開発]→[Web ゲートウェイ・ガイド]→[Web ゲートウェイの概要] の順に選択して、オンライン・ドキュメントにアクセスします。プライベート Web サーバは、インストール・ディレクトリ下の **httpd¥bin** サブディレクトリにある httpd.exe (UNIX® 上では httpd) です。プライベート Web サーバの開始を制御するには、管理ポータルで [システム管理]→[構成]→[追加設定]→[開始] を選択して、[ウェブサーバ] を true または false に設定します。

5.3.5 ゲートウェイ

InterSystems IRIS は、外部データに対するいくつかのゲートウェイを提供しています。これらのゲートウェイには、SQL ゲートウェイ、JDBC ゲートウェイ、オブジェクト・ゲートウェイ、および XSLT 2.0 ゲートウェイのサーバが含まれます。使

用される TCP/IP ポートを定義するには、管理ポータルで [システム管理]→[構成]→[接続性] を選択してアクセスできるゲートウェイ・セットアップ・ページを使用します。これらのゲートウェイが依存しているオペレーティング・システムのサービスやプロセスの詳細は、各ゲートウェイのドキュメントを参照してください。

5.4 不要な InterSystems IRIS プロセスの削除

InterSystems サービス・プロセスが作成されるのは、これらのプロセスがサポートしているサービスが有効化および構成されている場合のみです。InterSystems サービス・プロセスが実行されることを防止するために、追加の操作を実行する必要はありません。

5.5 外部プロセス

InterSystems IRIS インスタンスは、このインスタンスをサポートするいくつかの機能を実行するために、iris[.exe] 以外の実行可能ファイルを実行するプロセスを開始します。これらの実行可能ファイルのインスタンス固有バージョンは (これらの実行可能ファイルは通常はインスタンス・バージョンごとに異なります)、インストール・ディレクトリの bin サブディレクトリにあります。複数の InterSystems IRIS インスタンスによって共有される可能性のある実行可能ファイルは、共通のディレクトリに格納されています。

以下に、永続プロセスによって実行される可能性のある実行可能ファイルを示します。これらの実行可能ファイルは Windows 上の bin ディレクトリに格納されています。

- irisdb.exe — InterSystems IRIS 実行可能ファイル。
- licmanager.exe — InterSystems IRIS ライセンス・サーバ。
- CStudio.exe — スタジオ。
- iristray.exe — システム・トレイ内の InterSystems IRIS ランチャー。
- Iristerm.exe — ターミナル。
- iristrmd.exe — ローカルのターミナル接続デーモン。ローカルのターミナル接続 (Telnet ではなく) を受け付けて、その接続を処理するための InterSystems IRIS サーバ・プロセスを作成します。
- irisirdimj.exe — InterSystems IRIS の始動時とシャットダウン時に WIJ ファイルを処理する実行可能ファイル。

以下に、永続プロセスによって実行される可能性のある実行可能ファイルを示します。これらの実行可能ファイルは UNIX® 上の bin ディレクトリに格納されています。

- iris — InterSystems IRIS 実行可能ファイル。
- licmanager — InterSystems IRIS ライセンス・サーバ。
- irisirdimj — InterSystems IRIS の始動時とシャットダウン時に WIJ ファイルを処理します。

bin ディレクトリ内の他のプログラムもたまに使用されますが、これらのプロセスは短時間しか実行されないため、プロセスのリスト表示で長時間表示されることはあまりありません。

複数の InterSystems IRIS インスタンスによって共有される実行可能バイナリは、Windows 上の C:¥Program Files (x86)¥Common Files¥InterSystems のサブディレクトリに格納されています。これらのプロセスは、これらの実行可能バイナリを Windows 上の共通ディレクトリから実行しているものとして表示されることがあります。

- ISCAgent.exe – ミラーのフェイルオーバーを制御します。
- Iristerm.exe – ターミナル。

共有バイナリは通常、UNIX®上の /usr/local/etc/irissys にインストールされます。

- ISCAgent* – ミラーのフェイルオーバーを制御します。

実行可能バイナリに加えて、いくつかの共有ライブラリ・バイナリが共通ディレクトリに格納されています。

5.6 相互運用性

5.6.1 アダプタ

InterSystems IRIS は、アダプタを使用して外部インタフェースとの通信を可能にします。

5.6.1.1 電子メール

電子メール・アダプタは InterSystems IRIS プロセスです。これらのアダプタは、TCP/IP を使用して電子メール・サーバとの間で電子メールを送受信します。発信アダプタは、SMTP サーバにメールを送信します。着信アダプタは、POP3 サーバからの該当する (フィルタ処理された) メッセージをポーリングします。電子メール・サーバはリモート・サーバ上に配置されている可能性が高いため、ローカル・プロセスは存在しない一方で、リモート・システムにファイアウォールを介してアクセスできる必要があります。

5.6.1.2 ファイル

ファイル入力アダプタは InterSystems IRIS プロセスです。これらのアダプタは、監視対象として構成されたディレクトリを定期的に調べて、そのディレクトリにあるファイルを読み取って、サポート対象として構成されたビジネス・サービスにそれらのファイルを渡して、構成されたアーカイブ・ディレクトリにそれらのファイルを移動します。EnsLib.File.InboundAdapter クラスは実装を提供します。FilePath、WorkPath、および ArchivePath の各プロパティは、それぞれ入力ディレクトリ、一時作業ディレクトリ、およびアーカイブ・ディレクトリを定義します。

ファイル出力アダプタは、プロダクションのビジネス・オペレーションによってデータをファイルに書き込むために使用されます。ファイルのパスと名前はビジネス・オペレーションによって指定され、ファイルに対する処理は、EnsLib.File.OutboundAdapter クラスのメソッドを呼び出すことで実行されます。メッセージは通常、実際の出力処理を実行するワーカ・ジョブのキューに格納されます。このことは、Ens.Queue プロセスの存在を暗黙的に意味します。

5.6.1.3 FTP

InterSystems IRIS は、%Net.FtpSession クラスを使用したリモート FTP サーバとの FTP 通信用のクライアントとして機能します。%Net.FtpSession クラスは、着信接続を回避するために、データ・チャンネルに対して PASV を使用するように構成できます。InterSystems IRIS は、FTP の着信アダプタと発信アダプタを提供します。どちらも FTP クライアントとして機能して、ユーザによって作成されたビジネス・サービスの管理下で get (入力) または put (出力) を実行します。FTP のサーバとポートは構成可能です。FTP アダプタは InterSystems IRIS プロセスです。

5.6.1.4 HTTP

HTTP アダプタ (EnsLib.HTTP.InboundAdapter および EnsLib.HTTP.OutboundAdapter) は、プロダクションが HTTP 要求と HTTP 応答を送受信することを可能にします。HTTP アダプタは InterSystems IRIS プロセスによって実装されます。着信 HTTP アダプタのポートとインタフェースの IP アドレスは構成可能です。発信 HTTP アダプタの対象であるサーバとポートは、クラス設定によって指定されます。

5.6.1.5 Java ゲートウェイ

プロダクションのアダプタは、Java ゲートウェイを使用して Java 中間プロセスを介して通信します。Java 仮想マシンの存在に依存する Java プロセスが開始されます。InterSystems IRIS サーバ・プロセスは、TCP 接続を介して Java プロセスと通信します。使用される TCP ポートは構成可能です。

5.6.1.6 LDAP

ビジネス・サービスは、EnsLib.LDAP.OutboundAdapter クラスを他のアダプタと同じように使用して LDAP サーバに要求を送信したり応答を受信したりできます。

5.6.1.7 MQSeries

EnsLib.MQSeries.InboundAdapter クラスと EnsLib.MQSeries.OutboundAdapter クラスを使用すると、プロダクションは、IBM WebSphere MQ のメッセージ・キューとの間でメッセージを送受信できます。動的に読み込まれる共有ライブラリ・バイナリが通信用に使用されます。

5.6.1.8 パイプ

EnsLib.Pipe.InboundAdapter クラスと EnsLib.Pipe.OutboundAdapter クラスを使用すると、プロダクションはオペレーティング・システムのコマンドやシェル・スクリプトを実行できます。これらは、InterSystems IRIS の外部プロセスを作成して、パイプを介してこのプロセスと通信するため、パイプ・アダプタが外部プロセスと通信している間は外部プロセスは存続します。このプロセスによって実行されるコマンドは、アダプタ・クラスの CommandLine プロパティに指定された値によって決まります。

5.6.1.9 SAP

Java ゲートウェイは、EnlLib.SAP.BootStrap クラスの ImportSAP メソッドを使用してインポートされたクラスを使用して SAP Java コネクタと通信するために使用されます。

5.6.1.10 SQL

SQL 着信アダプタおよび発信アダプタは、プロダクションが JDBC または ODBC に準拠したデータベースと通信することを可能にします。一般に、着信 SQL アダプタ (EnsLib.SQL.InboundAdapter) はクエリを定期的に実行してから、結果セットの行を繰り返し処理して、関連付けられたビジネス・サービスに 1 行ずつ渡します。SQL アダプタは、InterSystems SQL ゲートウェイと JDBC ゲートウェイの基盤機能を使用します。

5.6.1.11 TCP

InterSystems IRIS は、入力 TCP アダプタと出力 TCP アダプタを提供します。各 TCP 着信アダプタは、指定されたポート上でデータの有無を確認して、入力を読み取り、関連付けられたビジネス・サービスに入力をストリームとして送信します。プロダクション内では、発信 TCP アダプタは、ユーザによって作成および構成されたビジネス・オペレーションと関連付けられています。このビジネス・オペレーションは、そのプロダクション内からのメッセージを受信して、メッセージ・タイプを調べて、発信 TCP アダプタ内で適切なメソッドを実行して、TCP を介してデータを送信します。

5.6.1.12 Telnet

InterSystems IRIS が提供する EnsLib.Telnet.OutboundAdapter を使用すると、別のシステム上の telnet 機能への発信 telnet 接続が可能になります。このアダプタが提供するメソッドを使用して、telnet クライアント・ソフトウェアを使用してリモート・システムに手動でログインする機能をプログラムによってエミュレートします。InterSystems IRIS TCP デバイスは基盤テクノロジです。

6

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

このチェックリストの目的は、環境のセキュリティ・レベルを検証するためのガイドラインを提示すること、および環境のセキュリティを強化するためのヒントを提示することです。これらのヒントは、組織のセキュリティ侵害を回避および防止するのに役立ちます。このチェックリストは“ハウツー・リスト”として使用されるべきものではなく、全網羅的なものでもありません。以下に示す項目は考慮すべき事項であり、適用すべきルールの絶対的なリストではありません。

インフラストラクチャのセキュリティについて全責任を負っている担当者として、セキュリティ強化と保護のための手法について不安がある場合、セキュリティ専門家にご相談ください。

6.1 ネットワークとファイアウォール

ID	トピック	説明
1.	ネットワーク、ハードウェア、ソフトウェア、およびポリシー	セキュリティ・ポリシー、ファイアウォール・ログ、ファイアウォールの構成とパッチ・レベル、公開されている IP アドレス、ネットワーク図、およびファイアウォール・トポロジの情報を取得してレビューします。
2.	物理的環境の監査	ファイアウォールと管理サーバが、許可された人物のみがアクセスできる物理的に安全な場所にあることを確認します。また、それらに最新のパッチが適用されていることを確認します。
3.	変更管理プロセス、ルール・ベース変更のレビュー	変更の手順と承認プロセスをレビューします。このための自動化ツールが提供されています。
4.	脆弱性のテスト	自動化されたツールを実行して、安全性の低いサービス、プロトコル、およびポートを分析して特定します。
5.	総当たり攻撃検知システムの使用	パスワードが不特定の人々に推測されることを阻止して、サーバ・ファイアウォールで不特定の人々の現在の IP アドレスをブロックすることで、サーバに接続することを防止します。
6.	継続的な監査およびリアルタイムの監視とアラート発行	ファイアウォールを継続的に監査するためのプロセスを実行します。ファイアウォールに変更が加えられたときにアラートを発行するためのリアルタイム監視を実行します。これらに関するログを定期的にレビューします。

6.2 オペレーティング・システム

ID	トピック	説明
1.	インストール計画	サーバ・ロールを理解して、インストール手順を文書化します。詳細は、オペレーティング・システムの適切なセキュリティ強化ガイドをダウンロードして参照してください。
2.	パッチ・レベル	オペレーティング・システムに最新のパッチが適用されていることを確認します (特にセキュリティ・パッチ)。自動更新を無効にします。
3.	エンドポイント保護ソフトウェア	このソフトウェアをインストールし、適切に構成します (これまでは、ウイルス対策ソフトウェアとしていました)。
4.	不要なソフトウェア、サービス、およびポートの無効化	不要なネットワーク・サービスを無効にします (IPv6、telnet、FTP など)。 使用されていない不要なデーモンを無効にします (DHCP、スケジューリングとキューイングのサービス、ラップトップ・サービスなど)。 使用されているサービスのセキュリティを可能な限り高めます。例えば、SSH プロトコルをバージョン 2 に限定することで SSH のセキュリティを向上させます (バージョン 1 はセキュリティが不十分です)。
5.	ログ	サーバ・ログを保持して、それらのログを別個のログ・サーバにミラーリングします。
6.	監視とアラート発行	監視とアラート発行の設定を通じて、システムに対する変更や未承認アクセスなどのイベントが通知されるようにします。
7.	物理的なセキュリティ	BIOS の構成を通じて、CD/DVD、フロッピー、および外部デバイスから起動できないようにして、これらの設定を保護するためのパスワードを設定します。

6.3 Web サーバ

ID	トピック	説明
1.	インストール計画	Web サーバのロールとコンテンツを理解して、ページが静的かどうか、および提供される Web サービスの内容を確認します。インストール手順を文書化します。適切なセキュリティ強化ガイドをダウンロードして参照します。
2.	パッチ・レベル	Web サーバが最新状態であることを確認します (特にセキュリティ・パッチのバージョン)。
3.	Web サーバのヘッダ情報	実行されている Web サーバ・ソフトウェアや、システムのタイプとバージョンに関する情報が HTTP ヘッダに含まれないようにサーバを構成します。
4.	HTTP TRACE の無効化	HTTP TRACE が有効化されているときは、HTTP TRACE 要求を使用してすべての受信情報がエコー・バックされます。
5.	エラー処理	汎用のエラー・ページとエラー処理ロジックを使用して、アプリケーションで既定のエラー・ページを強制的に回避させることで、適切なエラー処理を実現します。既定のエラー・ページは多くの場合、システムとアプリケーションに関する機密情報を漏洩させます。
6.	モジュールの無効化	使用されていないモジュールをすべて無効化することで、Web サーバの外部にさらされる領域を減らします。これらのモジュールによって多くの場合は必要以上の情報が提供されます。 Apache: autoindex、cgi、imap、info、status、userdir、actions、negotiation… IIS: ASP、ASP.NET、WebDAV、CGI、ディレクトリ参照…
7.	ユーザとグループ	Apache: Apache を別個のユーザおよびグループとして実行することで、Apache プロセスを他のシステム・プロセスによって使用できないようにします。 IIS: 使用されていないアカウントを削除して、Guest アカウントを無効にします。

6.4 ユーザ、パスワード、グループ、所有権、および権限

ID	トピック	説明
1.	ユーザ管理	root ログインを無効にします。すべての管理者は名前を持つユーザである必要があります。使用されていないユーザ・アカウントがないこと、および既定のユーザ・アカウントとパスワードが使用されていないことを定期的に確認します。
2.	パスワード・ポリシー	大文字と小文字、数字、および特殊文字を組み合わせた非常に強力なパスワードを使用することを義務付けます。 パスワードを定期的に変更します。 ログインの失敗が一定回数を超えた場合は、そのアカウントをロックします。
3.	UNIX®	インストール前にグループとユーザを作成します。 InterSystems IRIS を root としてインストールします。InterSystems IRIS データベースのグループ、所有権、および権限が指定されたとおりに保持されていることを確認します。
4.	Windows	Windows Administrator を使用して InterSystems IRIS をインストールしてから、既定の Windows Administrator アカウントを無効にします。Guest アカウントと Help Assistant アカウントも無効にします。

6.5 暗号化 (保管中のデータと伝送中のデータ)

ID	トピック	説明
1.	保管中のデータ	ディスク上に保管されているすべての実運用データが暗号化されていることを確認します。
2.	キー管理	キー管理のポリシーと手順をレビューします。
3.	伝送中のデータ	すべての HTTP データ通信が暗号化されていることを確認します (TLS などを使用)。 すべての TLS 構成で最新バージョンが使用されていることを確認します。

6.6 インターシステムズのセキュリティ

ID	トピック	説明
1.	インストール	常に、ロック・ダウン初期セキュリティ設定タイプを指定してインストールします。
2.	認証	ユーザとパスワードを定期的にレビューします。
3.	承認	アプリケーションの要件をレビューします。ロール、リソース、およびサービスを定義します。
4.	監査	監査が有効になっていることを確認します。ログを定期的にレビューします。
5.	サービスの無効化	ECP やミラーリングなどのサービスが使用されていない場合は、それらのサービスを有効にしないでください。
6.	使用されていないデータベースとアプリケーションの削除	USER などの使用されていないデータベースを削除します。