



Caché の高度なセキュリティに関するよくある質問

Version 5.1
2006-03-14

Caché の高度なセキュリティに関するよくある質問

Caché Version 5.1 2006-03-14

Copyright © 2006 InterSystems Corporation.

All rights reserved.

このドキュメントは、Sun Microsystems、RenderX Inc.、アドビ システムズ および ワールドワイド・ウェブ・コンソーシアム (www.w3c.org) のツールと情報を使用して、Adobe Portable Document Format (PDF) で作成およびフォーマットされました。主要ドキュメント開発ツールは、InterSystems が構築した Caché と Java を使用した特別目的の XML 処理アプリケーションです。



Caché 製品とロゴは InterSystems Corporation の登録商標です。



Ensemble 製品とロゴは InterSystems Corporation の登録商標です。



InterSystems という名前とロゴは InterSystems Corporation の登録商標です

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動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。

Caché および InterSystems Caché、Caché SQL、Caché ObjectScript および Caché Object は、インターシステムズ社の商標です。

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。

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 ワールドワイド カスタマサポート

Tel: +1 617 621-0700

Fax: +1 617 374-9391

Email: support@InterSystems.com

目次

Caché の高度なセキュリティに関するよくある質問.....	1
一般	1
システム管理	7
監査	13
プログラミング	15

Caché の高度なセキュリティに関するよくある質問

一般

Caché の高度なセキュリティの全体的な目的は何でしょうか？

Caché の高度なセキュリティの目的は単純で、入念に設計および実装されたアプリケーションに、悪意のあるユーザからの攻撃に対する優れた自己防御機能を提供することです。

認証と承認の違いは何でしょうか？

簡単に説明すると、次のようになります。

- ・ 認証は、ユーザの身元を確認することです。
- ・ 承認は、ユーザが意図する操作を実行できる権限を持っているかどうかを調べることです。

認証時に、ユーザは、セキュリティ担当者によって“チャレンジ”と呼ばれる質問を受けます。これは、安全管理施設に近づこうとするものに対して、守衛が以下のようなことを調べることに該当します。

- ・ 認められた機関から発行された正真正銘の ID ドキュメントを所持しているかどうか。
- ・ 現行のパスワードを知っているかどうか。
- ・ その人間だけが知っているような内容の質問に対して回答できるかどうか。

チャレンジには、指紋、網膜スキャン、筆跡などの生物学的なデータを収集して検証するものもあります。しかし、一般的な人物認証では、その人が有効なユーザ名とそれに対応するパスワードを知っていることが確認されます。

同様に、アプリケーションでも、アクセスを試行するとチャレンジを受けます。通常、アプリケーションでは、システム・サービスの実行を許可される前に、正真正銘の ID 証明書を提示する必要があります。

認証によってユーザ（またはアプリケーション）の身元確認に成功したら、承認プロセスによって以下のような項目が調べられます。

- ・ 名前や身分

- ・ 実行しようとしている操作
- ・ 使用するデータ

データベースで照合に成功すると、操作を続行できます。そうでない場合は、通常ではエラー例外などが表示され、操作を続行できなくなります。

Caché の高度なセキュリティはどのように機能するのでしょうか？

フォームと関数で、Caché の高度なセキュリティは、他の多くのコンピュータ・セキュリティ・システムと同じように機能します。これは、定義済みのサブジェクト・グループが特定の保護オブジェクト・セットに対して実行できるアクションを、管理および制御するものです。

Caché では、サブジェクトはロールまたはアプリケーションを表し、オブジェクトはリソースと呼ばれます。また、実行可能なアクションは、“読み取り (R)”、“書き込み (W)”、および “使用 (U)” で、リソースごとに適切に定義されます (これらの各項目は、このドキュメントのそれぞれのセクションで説明されています)。

アクセス制御は、サブジェクト名を各列の見出しにし、リソース名を各行のラベルにしたマトリックス表で視覚化できます。このモデルでは、各テーブル・セルに、各サブジェクトがオブジェクトに対して実行可能なアクションが記載されます。以下はその例です。

	Analyst	...	Clerk
%DB_CACHESYS	RWU	...	
%DB_DOCBOOK	R	...	
%Service_CSP	U	...	U
%Service_Bindings	U	...	
%Development		...	U
...

テーブル・セルに権限設定が含まれない場合、そのロールには指定されたリソースに対するアクセス権がありません。

Caché のロールは SQL のロールと同じでしょうか？

いいえ。Caché によって定義されるロールと SQL 標準によって定義されるロールは同じではありません。これらは 2 種類の異なる承認モデルを表し、それぞれ異なるリソースを管理します。Caché では、読み取り、書き込み、使用、および開発の各権特権が定義され、セキュリティ・データベースに定義されたリソースの使用が管理されます。SQL では、選択、挿入、更新、および削除が使用され、それらは主にユーザ、データベース、テーブルなどの SQL 独自の “リソース” に適用されます。さ

らには、不確定さを相互に対応付ける 2 つのアプローチ間に相違があります。これらは、権限が決定される方法と、それらが無効化されるときに顕在化します。

しかし、これらは同じ基盤認証メカニズムを共有するため、Caché と SQL ではユーザ認証に同じ名前が使用されます。

ルールとユーザの関係を教えてください。

Caché の高度なセキュリティでは、特権はユーザに直接割り当てられません。代わりに、特権は、組織内の特定の職責や役割を表す名前となるロールに割り当てられます。例えば、Adam Smith が持つ特権は、彼に割り当てられたロール (CFO ロールなど) から導き出すことができます。

この公式化によって、ある程度の抽象化が可能となり、システム管理者の管理業務が軽減されます。なぜなら、ロールに関連付けられる特権は、通常、そのロールに割り当てられるユーザほど変更されないためです。

アプリケーションにロールが割り当てられるのはなぜでしょうか？

アプリケーションにロールを割り当てることで、アプリケーションは、それを起動したユーザが持つ特権とは異なる特権によって、ユーザの代わりに操作を実行できます。これによって、十分にテストされ信頼されたアプリケーションの制御下でのみ特権の実行が許可されるため、特権がさらに効果的に制御されます。

さらには、ユーザのロールをチェックした後で、ユーザが特定のロール (“マッチ” ロール) を保持している場合は、アプリケーションによって、アプリケーションの使用時のみ有効な 1 つまたは複数の追加ロール (“ターゲット” ロール) を付与できます。このプロセスは、“ロールのエスカレーション” と呼ばれます。

Caché の高度なセキュリティで使用される特権を教えてください。

Caché には、以下の特権が定義されています。

- ・ 読み取り – リソースの内容の表示は許可されますが、変更は許可されません。
- ・ 書き込み – リソースの内容の表示および変更が許可されます。
- ・ 使用 – アプリケーションやサービスなどのリソースの呼び出しが許可されます。

特権はその名前の最初の文字によって表されることが多く、それぞれ “R”、“W”、“U” となります。

Caché の高度なセキュリティには、どのようなリソースが定義されていますか？

Caché には、以下のリソースが既定で定義されています。

- ・ データベース

- %DB_<DatabaseResourceName>

システムに付属するデータベースには、%DB_USER や %DB_CACHESYS などがあります。事前に定義されたリソースの %DB_%Default には、以下の場合にデータベースに適用される特権が指定されています。

- ・ データベースに (旧式の) 2 KB ブロック形式が使用されている
- ・ リソース名が割り当てられていない
- ・ マウントされているが現行の構成に記述されていない

データベース・リソース名を持たない既存データベースをマウントしたときは、既定リソースの %DB_%DEFAULT がデータベースに割り当てられます。

- ・ アプリケーション

- %Application/CSP/CSPApp - ユーザがローカル CSP ページを実行するのを許可します。
- %Application/CSP/CSPBroker - クライアントが CSP ページをサーバに送信し、応答を受け取るのを許可します。
- %Application/CSP/CSPDocBook - オンライン・ドキュメント・アプリケーションの使用法を参照します。
- %Application/<ApplicationName> - ユーザ定義のアプリケーションに対するアクセスを制御します。

- ・ サービス

- %Service_CacheDirect - Caché Direct を使用した Caché への接続を表します。
- %Service_Callin - CALLIN を介した Caché への接続を表します。
- %Service_ComPort - Microsoft Windows 通信ポートを介した Caché への接続を表します。
- %Service_Console - css または csession コマンドによって開始される Caché 接続を表します。
- %Service_CSP - CSP ページを実行する機能を表します。
- %Service_LAT - Microsoft Windows LAT サービスを介した Caché への接続を表します。
- %Service_Object - オブジェクト要求を実行する ODBC、JDBC、または SQL による Caché への接続を表します。
- %Service_Bindings - 使用可能なオブジェクト・バインディングの 1 つによる Caché への接続を表します。
- %Service_Telnet - Microsoft Windows 用の Caché Telnet サービスを介した Caché への接続を表します。

- %Service_Terminal - 非 Windows システム上のターミナルを介した Caché への接続を表します。
- %Service_DCP - DCP を介した Caché への接続を表します。
- %Service_ECP - ECP を使用した Caché への接続を表します。
- %Service_Monitor - BMC Patrol の使用など、モニタ・インタフェースを介した Caché への接続を表します。
- %Service_MSMActivate - MSM Activate からの Caché への接続を表します。
- %Service_Shadow - Caché データベース・シャドウ・システムへの接続を表します。
- %Service_WebLink - WebLink アプリケーションを介した Caché への接続を表します。
- %Service_WebService - CSP を使用した Caché Web サービス機能への接続を表します。

管理

- %Admin_Manage - Caché 構成、バックアップ定義、データベース、およびネームスペース・マッピングを作成、変更、および削除する機能と、データベースおよびジャーナル・リストアを実行する機能を表します。
- %Admin_Operate - Caché、そのプロセス、サービス、およびバックアップの起動と停止、データベースのマウントとマウント解除、整合性チェックの実行、データベース・バックアップの実行、ロックの変更、ログの調査などの機能が含まれます。
- %Admin_Secure - Caché セキュリティを管理する機能を表します。
- %Admin_Secure/<RoleName> - 指定されたロールの割り当てまたは取り消しを実行する機能が含まれます。
- %Development - 開発ツールと機能を呼び出す機能を表します。

名前がパーセント文字 (%) で始まるリソースは、Caché で定義および管理されるリソースです。システム管理者によって特定のサイト用に定義されるリソースは、この文字で始めてはいけません。

ネームスペースがリソースとならないのはなぜでしょうか？

ネームスペースに関する機能を表すリソースはありません。ネームスペースに対して実行可能な操作は、そのネームスペースにマップされたデータベースから導き出されます。

基本データベースの特権の使用によって、明らかに変則的な動作が発生する可能性があることは理解しておく必要があります。例えば、3つのデータベース A、B、および C にマップされているネームスペース X があり、ロール AverageUser が %DB_A:R および %DB_C:R の特権を持っていて B にはアクセスできないとします。

この場合、B のデータにアクセスする試みは、すべて失敗します。

特権とは何ですか？

特権はリソースを操作する権利を意味します。特権は、%DB_USER:R のように、リソース名と権限によって構成されます。複数の特権が同じリソースに対して設定される場合は、%DB_USER:RW のように、権限を結合するのが一般的です。

Caché では、特権はロールに割り当てられます。

ユーザとアプリケーションの両方にロールが付与されるのはなぜでしょうか？

Caché モデルでは、アプリケーションはユーザのエージェントとして動作できます。アプリケーションがタスクを完了するには、アプリケーションを呼び出したユーザとは異なる特権が必要になる場合があるため、アプリケーションにも独自のロールを付与できるようになっています。

アプリケーションへのアクセスはどのように制御されるのでしょうか？

アプリケーションは、リソースによって表されます。アプリケーションを Caché セキュリティ対応にすると、そのアプリケーションに対応するアプリケーション・リソースが自動的に作成されます。

このリソースに設定可能なプロパティの 1 つに、[保護] という名前プロパティがあります。このプロパティは、ユーザがこのリソースにアクセスするのに必要なロール、つまりアプリケーションを実行するのに必要なロールを決定します。[保護] プロパティには、以下の値を設定できます。

- ・ パブリック – すべてのユーザが、このアプリケーションを実行できます。
- ・ 制限 – %Application/<application-name>:Use 特権を含むロールを持つユーザだけが、このアプリケーションを実行できます。
- ・ ロック – %All ロールを持つユーザだけが、このアプリケーションの実行を許可されます。

[ロック] 設定は、セキュリティ侵害が発生したと疑われる場合に、アプリケーションをロックする目的で緊急使用することが意図されています。日常的な操作では、アプリケーションを [制限] に設定し、対応するロールをそのアプリケーションの実行に必要なユーザに割り当てれば十分です。

Caché セキュリティで使用される暗号化アルゴリズムを教えてください。

Caché には、米国商務省標準技術局 (NIST) による Advanced Encryption Standard (AES) が実装されています。この規格は、連邦情報処理規格 197 (FIPS PUB 197) にもなっています。これは、128、192、または 256 ビットの鍵を使用する高速で強力な対称型アルゴリズムです。また、このアルゴリズムは輸出が規制されていません。

この規格は、以下の NIST Web サイトから入手できます。

- ・ csrc.nist.gov/publications/fips/fips197/fips-197.pdf

このアルゴリズムの物理的な実装は、以下の著作権によって保護されています。

Copyright (c) 2003, Dr Brian Gladman, Worcester, UK. All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product may be distributed under the terms of the GNU General Public License (GPL), in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

Caché の高度なセキュリティの使用は必須でしょうか？

はい。Caché のセキュリティは、常に有効化されています。しかし、適切な権限が認められた管理者は、システムの動作が従来のアプリケーションにも対応するようにセキュリティを構成できます。

Caché の高度なセキュリティは何らかのセキュリティ認定を受けていますか？

インターシステムズは、Caché バージョン 5.1 に対して、Common Criteria のレベル EAL3 認定を取得する手続きを開始しました。この基準と各レベルの要件の詳細は、Common Criteria の Web サイトの www.commoncriteria.org で入手できます。

システム管理

特権の変更は、どの時点で有効になるのでしょうか？

Caché は、セキュリティ設定が格納されたデータベースを永続的に保持しています。Caché が起動されると、その情報が抽出され共有メモリのセグメントに配置されるため、統合化された設定への迅速なアクセスが可能になります。プロセスが実行されている間、そのプロセスに付与されている特権のキャッシュが独自に保持されます。これは、新しい特権が必要になり認可されると更新されます。

ルールや特権などを編集すると、その情報の永続コピーに変更が反映されます。この変更は、ユーザまたはアプリケーションの次の認証時に認識されます。

Caché インストールに使用できる認証メカニズムを教えてください。

ユーザの身元確認には、以下の 4 つの選択肢があります。

- ・ Kerberos
- ・ オペレーティング・システム・ログイン
- ・ Caché ログイン
- ・ 非認証 (身元確認なし)

Kerberos は、最も安全な認証手段を提供します。Kerberos 認証システムは MIT によって開発され、数学的に証明された強力な認証を、セキュリティ保護されていないネットワークで実現します。Kerberos の詳細は、web.mit.edu/kerberos/www/で入手できます。

オペレーティング・システム・ベースの認証は、UNIX および OpenVMS で使用できます。OS ベースの認証では、Caché に対するユーザの身元確認に、オペレーティング・システムのユーザ ID が使用されます (Windows プラットフォームでは、基本認証メカニズムが Kerberos のため、OS ベースのオプションはありません)。

Caché ログイン・メカニズムでは、各ユーザ・アカウントのパスワードのハッシュ計算値を格納するテーブルが保持されます。Caché は、テーブル内のその値と、ログイン時にユーザによって入力されたパスワードのハッシュ値を比較することで、ユーザの身元を確認できます。

認証をいっさい実行することなく、すべてのユーザの接続を許可することもできます。このオプションは、外部との境界が強力に保護されている組織や、アプリケーションとデータの両方が攻撃の対象としてまったく興味を引かない場合に適用できます。

これらとは別に、ユーザは以下の 3 つの場所からアクセスを要求する可能性があります。

- ・ ローカル - ユーザは Caché と同じシステムで操作を実行しています。
- ・ クライアント - ユーザ・アプリケーションが ODBC や CSP ゲートウェイなどのサービスを介して接続しています。
- ・ プロキシ - ユーザはユーザの代わりに Caché とやり取りする CSP アプリケーションを実行しています。

これらとの組み合わせによって、以下のテーブルに示すオプションが実現されます。

	ローカル	クライアント	プロキシ
非認証	可	可	可
Caché ログイン	可	可	可
オペレーティング・システム・ログイン	可	不可	不可
Kerberos	可、ただし不可の場合もある	可、ただし不可の場合もある	可、ただし不可の場合もある

Kerberos のエントリが “可、ただし不可の場合もある” となっている理由は、Kerberos では、ユーザの身元確認にさまざまな方法が提供されるためです。ただし、実際に使用可能なオプションは、使用される場所とサービスの詳細によって異なります。詳細な説明は、このドキュメントの対象ではありません。

Caché に事前定義されているロールを教えてください。

Caché には、以下の 5 つのロールが組み込まれています。

- ・ %All
- ・ %Developer
- ・ %Manager
- ・ %Operator
- ・ %SQL

各ロールに関連付けられている既定の特権を以下のテーブルに示し、その後で説明を加えます。

	%Developer	%Manager	%Operator	%SQL
%Admin_Manage		U		
%Admin_Operate		U	U	
%Admin_Secure		U		
%DB_CACHEAUDIT/<Role>		R		
%DB_CACHELIB/<Role>	R	RW		
%DB_CACHESYS		RU		
%DB_CACHETEMP	RW	RW	RW	
%DB_DOCBOOK	R	RW	R	
%DB_SAMPLES	RW	RW		

	%Developer	%Manager	%Operator	%SQL
%DB_USER	RW	RW		
%DB_%Default	RW	RW		
%Development	U	U		
%Service_CacheDirect				
%Service_Callin				
%Service_ComPort				
%Service_Console	U	U		
%Service_CSP	U	U	U	
%Service_LAT				
%Service_Object	U	U		
%Service_Bindings	U	U		U
%Service_Telnet	U	U		
%Service_Terminal	U	U		
%Service_DCP				
%Service_ECP				
%Service_Monitor				
%Service_MSMAActivate				
%Service_Shadow				
%Service_WebLink				
%Service_WebService				

%All を除いて、これらの事前定義ロールの使用はオプションです。ただし、%All ロールには、以下のような特別な運用が適用されます。

- ・ %All ロールはシステムから削除できません。
- ・ %All ロールの特権は変更できません。
- ・ %All ロールには、システムに定義されるすべての新規リソースに対する特権が自動的に付与されます。
- ・ %All ロールには、少なくとも 1 人のユーザが常に割り当てられている必要があります。Cache は、以下の操作をいずれも実行しません。
 - %All に割り当てられている最後のユーザの無効化

- %All ロールに割り当てられている唯一のユーザの削除

Caché セキュリティを誤って構成し、すべてのユーザをロックしてしまう可能性はありますか？

前述のように、Caché では、特別なチェックによって、少なくとも 1 人の有効なユーザが %All ロールに割り当てられていることが保証され、また %All ロールにはすべてのリソースに対するすべての特権が付与されています。このため、システム管理に必要なアクセス権を持つユーザが少なくとも 1 人は存在します。

ただし、これは万能薬ではないことに注意してください。他のすべてのユーザが削除された場合を想定してください。この唯一のユーザも、Caché に認証される必要があることは同じです。認証プロセスがパスワードを要求したときに、誰も入力できなかった場合は、誰も Caché にアクセスできません。

“パブリック”、“制限”、および“ロック”という用語がアプリケーションに適用されるときは、どのような意味を持つのでしょうか？

Caché のアプリケーションは、以下の 3 つのグループに分類されます。

- ・ “パブリック”というラベルの付いたアプリケーションは、任意のユーザが実行できます。
- ・ “制限”カテゴリに属すアプリケーションを実行するユーザは、そのアプリケーションに対する“使用”特権が付与されたロールに割り当てられる必要があります。
- ・ “ロック”アプリケーションは、%All ロールが割り当てられたユーザのみが実行できます。

Caché の高度なセキュリティのインストール時または Caché の高度なセキュリティへのアップグレード時に、知っておく必要のあることを教えてください。

Caché の高度なセキュリティのインストールが起動される方法は、以前のバージョンの Caché とは多少異なっています。このことは新規インストールと旧バージョンからのアップグレードの両方に当てはまります。システム管理者は、インストール後の以下の相違点を知っておく必要があります。

- ・ インストール後は、システム・セキュリティ・パラメータの PercentGlobalWrite の値が RESTRICTED に設定されます。

Caché では、パーセント記号 (%) で始まるルーチンとグローバル名が特別なものとして扱われます。それらは、各自が格納されているデータベースが属するネームスペースだけでなく、すべてのネームスペースで認識されます。PercentGlobalWrite パラメータは、他のデータベースに格納されている非パーセント・ルーチンによる“パーセント”グローバルへのアクセスを制御します。

RESTRICTED 値は、パーセント・グローバルに対する変更に、通常セキュリティ制御が適用されることを意味します。PercentGlobalWrite が PUBLIC に設定されている場合は、すべての

ユーザがパーセント・グローバルに対する書き込み特権を暗黙的に持ちます (旧バージョンの既定の動作)。

- ・ アップグレード・インストール後は、すべてのユーザが新しいパスワードを設定する必要があります。

Caché の高度なセキュリティで使用されるパスワード・ハッシュ関数は、以前のバージョンの Caché で使用されたものよりも堅牢です。新旧どちらでも Caché はパスワードのハッシュ値を比較目的でのみ格納するため、ハッシュ値を反転させて (平文のパスワードに戻して)、それを新しい関数を使用したハッシュ値に置き換える簡単な方法がありません。したがって、この堅牢さを活用するには、新しいパスワードを使用する必要があります。

- ・ DefaultSecurityDomain パラメータ値は、Caché がインストールされているマシン名に初期化されます。

ドメイン名がないユーザ ID が使用されたときは、既定ドメインであるとみなされます。例えば、既定ドメインが InterSystems.com の場合、ユーザ ID の Paul と Paul@InterSystems.com は同等です。単一のドメイン構成では、既定ドメイン以外のドメイン名の使用は許可されません。

通常使用時におけるドメイン名の可視性は、SecurityDomains 構成パラメータによって制御されます。このパラメータの値が SINGLE で \$USERNAME にドメイン名が含まれない場合は、システム・ユーティリティによるユーザ名の表示時にドメイン名が表示されません。このパラメータの値が MULTIPLE で \$USERNAME にドメイン名が含まれる場合は、システム・ユーティリティによるユーザ名の表示時にドメイン名が表示されます。

- ・ 既定では、開発者は、以前のバージョンで所持していた多くの Caché サービスに対する特権を所持していません。

Caché の既定インストールは保守的に構成されています。事前定義済みのロールには、大半の顧客が必要としなくなった COM ポートや LAT などの従来のリソースに対する特権が含まれません。これらが必要になった場合、管理者は、事前定義済みのロールを変更するか新しいロールを作成して、各サイトの要件に合った別の特権セットを定義できます。

Caché の高度なセキュリティと以前のバージョンの Caché で動作が異なる分野は他にもありますか？

システム管理者が定義するセキュリティ設定によって適用される明確な制約以外にも、Caché の高度なセキュリティのインストールの動作は、以前のバージョンの Caché とは多少異なります。このことは新規インストールと旧バージョンからのアップグレードの両方に当てはまります。以下はその例です。

- ・ CSP アプリケーションでは、セキュリティ情報が CSP セッションの一部として保持されます。これは、異なるプロセスを使用して複数のページ要求が実行される場合であっても、\$USERNAME および \$ROLES の値がそれらの要求間で保持されることを意味します (より具体的に言うと、CSP ページに対する処理が開始されたとき、\$ROLES にはユーザのロールに加えて、アプリケーションに定義されたロールも含まれます)。

\$ROLES には、SET \$ROLES または \$SYSTEM.Security. AddRoles() によって以前のページ処理時に動的に追加されたロールが含まれません。このことは“ステートレス”と“ステートフル”のどちらのセッションにも当てはまります。

- ・ 特権付きのルーチンをリコンパイルすると、そのすべての特権が自動的に取り消されます。リコンパイル後に、適切な特権を認められたユーザが、リコンパイルしたルーチンに対して特権を再構築する必要があります。
- ・ Caché ObjectScript には、2 つの新しいシステム特殊変数 \$USERNAME と \$ROLES が組み込まれました。これらは、アプリケーションに Caché の高度なセキュリティを使用して、それぞれのセキュリティ要件を個別管理する際に役立ちます。これらの変数の意味は、このドキュメントの“プログラミング”セクションに説明されています。

Caché ではデータベースを暗号化できますか？

はい。管理者は、Caché で使用されるデータベース (cache.dat ファイル) の 1 つまたは複数が増号化されるようにシステムを設定できます。

Caché のデータベース暗号化機能は、完全に Caché アプリケーション内で動作します。これは、Windows 暗号化ファイル・システム (EFS) や Red Hat Linux で使用できる Loop-AES 機能などの、データの暗号化用に提供されているホスト・オペレーティング・システムの機能とは完全に別です。Caché は、鍵管理、暗号化操作、および復号化操作を提供します。

詳細は、“Caché セキュリティ管理ガイド”の“データベース暗号化”の章を参照してください。

監査

Caché の高度なセキュリティには監査追跡は組み込まれていますか？

はい。Caché では、改ざんから保護されたログに重要なイベントを記録できます。また、Caché ではアプリケーションにも同じ機能が提供され、アプリケーション定義のイベントを同じログに記録できます。

イベント監査は、システム管理者が完全に有効化または無効化できます。監査が有効化されているとき、一部のシステム・イベントは必須とみなされ、必ず記録されます。その他のイベントについては、それらのエントリを監査ログに記録するかどうかを、より細かく制御できます。

事前定義された Caché の監査イベントには、どのようなものがありますか？

Caché によって事前定義されているイベントを、以下のテーブルに示します。

タイプ	イベント	説明	必須かどうか
%System	Start	Caché の起動	はい
%System	ConfigurationChange	前回の起動とは異なる構成での Caché の起動の成功、または Caché 実行中における新しい構成の有効化	はい
%System	Stop	Caché の終了	はい
%Login	Login	ログインの成功	いいえ
%Login	LoginFailure	ログイン試行の失敗	いいえ
%Login	Logout	ユーザのシステムからの退去	いいえ
%Security	UserChange	ユーザ定義の作成、変更、または削除	はい
%Security	ApplicationChange	アプリケーション定義の作成、変更、または削除	はい
%Security	RoleChange	ロール定義の作成、変更、または削除	はい
%Security	AuditChange	監査の停止と開始、エントリの消去、または監査対象のイベント・リストの変更	はい
%Security	ServiceChange	サービスのセキュリティ設定の変更	はい
%Security	SystemChange	システムのセキュリティ設定の変更	はい
%Security	ResourceChange	リソース定義の作成、変更、または削除	はい
%Security	DomainChange	ドメイン定義の作成、変更、または削除	はい
%Security	Protect	プロセスに対するセキュリティ保護エラーの発生	いいえ
%Security	AuditReport	標準的な監査レポートの実行	はい
%DirectMode	DirectMode	ダイレクト・モードでのコマンドの実行	いいえ

これらに加えて、任意の数のアプリケーション定義イベントを監査ログに記録できます。この目的で %SYSTEM.Security.Audit クラスが用意されています。

監査ログにはどのような項目が記録されますか？

監査ログには、イベントが発生した日時、イベントの名前とタイプ、イベントを報告したアプリケーションまたはシステム関数、その作業の実行元となるユーザなどが必ず記録されます。また、イベントには、特定のイベントに関連付けられている他の説明情報も含まれます。

プログラミング

\$USERNAME の目的を教えてください。

\$USERNAME は、Caché の高度なセキュリティの一部として ObjectScript に追加された特殊変数です。\$USERNAME は読み取り専用変数です。この変数には、現行ユーザの認証名を示す文字列が格納されます。

\$ROLES の目的を教えてください。

\$USERNAME と同様、\$ROLES はセキュリティに関連付けられた特殊変数です。\$ROLES には、現行ユーザに割り当てられたロール名のコンマ区切りのリストが格納されます。リスト内のすべてのロールに付与されているすべての特権の集合によって、ユーザが持つ特権が決められます。

ユーザが認証されたとき、そのユーザに割り当てられているロールが、初期ロールとして \$ROLES に格納されます。このロール名のセットは、“ログイン・ロール”と呼ばれます。

アプリケーションは、リストにロール名を追加して \$ROLES の内容を変更することで、ユーザ特権に影響を与えることができます。このロールはアプリケーションの実行中に適用され、“アクティブ・ロール”と呼ばれます。

アクティブ・ロールの変更を支援する目的で、NEW コマンドが変数 \$ROLES を特別な方法で処理します。NEW コマンドは、\$ROLES を空にするのではなく、以前の \$ROLES の内容を新しく作成されたインスタンスにコピーします（これは、ほとんどの場合に開発者が希望する処理で、不要な場合は簡単に元の状態に戻すことができます）。この段階でアプリケーションはリストを変更でき、制御によってその収容ブロックが正常または非正常な状態で放置されても、終了時に変更が元に戻されます。

ただし、忘れてはいけない1つの事実があります。アクティブ・ロールが決められるとき、それに使用されるロール名は、ログイン・ロールを構成するロール名と、現在の \$ROLES のロール名の集合になります。したがって、ユーザが認証時に持つ特権セットよりもさらに制限的な特権セットで実行することはできません。

認証が実行されない場合、\$USERNAME の値はどのようになるのでしょうか？

ユーザ認証が実行されない場合、\$USERNAME の値は、ユーザが実行しようとしているサービスに応じて決められます。各サービスには \$USERNAME の既定値があり、サービスが実行される前に、

この値が設定されます。この既定値は空の文字列にはできず、それ以外の値をシステム管理者が設定できます。