



暗号化標準および RFC

Version 2023.1
2024-01-02

暗号化標準および RFC

InterSystems IRIS Data Platform Version 2023.1 2024-01-02

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。

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

暗号化標準および RFC.....	1
-------------------	---

暗号化標準および RFC

インターシステムズのセキュリティで使用されている暗号化の基本とアルゴリズムは、以下の基準と RFC (Requests for Comments) で定義されています。

- ・ AES (Advanced Encryption Standard) 暗号化 – FIPS (Federal Information Processing Standards) 197
- ・ AES Key Wrap –
 - NIST (National Institute of Standards and Technology) のドキュメント “Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping” (https://csrc.nist.gov/CryptoToolkit/kms/AES_key_wrap.pdf)
 - IETF (Internet Engineering Task Force) RFC 3394
- ・ Base64 エンコード – RFC 3548
- ・ ブロック埋め込み – PKCS (Public-Key Cryptography Standard) #7 および RFC 2040
- ・ CBC (Cipher Block Chaining) 暗号化モード – NIST 800-38A
- ・ 決定論的乱数ジェネレーター –
 - FIPS PUB 140-2 の Annex C
 - FIPS PUB 186-2 の Change Notice 1、Appendix 3.1、および Appendix 3.3
- ・ GSS (Generic Security Services) API –
 - The Kerberos Version 5 GSS-API Mechanism – RFC 1964
 - Generic Security Service Application Program Interface, Version 2, Update 1 – RFC 2743
 - Generic Security Service API Version 2: C Bindings – RFC 2744
 - Generic Security Service API Version 2: Java Bindings – RFC 2853
- ・ Kerberos Network Authentication Service (V5) – RFC 1510
- ・ Hash-based Message Authentication Code (HMAC) – FIPS 198 および RFC 2104
- ・ Message Digest 5 (MD5) hash – RFC 1321
- ・ Password-Based Key Derivation Function 2 (PBKDF2) – PKCS #5 v2.1 および RFC 8018
- ・ Secure Hash Algorithm (SHA-1) – FIPS 180-2 および RFC 3174
- ・ Secure Hash Algorithm (SHA-512) – FIPS 180-2 および RFC 6234

これらのドキュメントはすべてオンラインで入手できます。

- ・ [FIPS ドキュメント](#)
- ・ [NIST ドキュメント](#)
- ・ [RFC \(IETF\)](#)

