暗号化標準および RFC

Version 2023.1
2024-01-02

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

暗号化標準および RFC
InterSystems IRIS Data Platform　Version 2023.1　2024-01-02

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

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 ー FIPS (Federal Information Processing Standards) 197
- AES Key Wrap ー
  - 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 ー RFC 3548
- ブロック埋め込み ー PKCS (Public-Key Cryptography Standard) #7 および RFC 2040
- CBC (Cipher Block Chaining) 暗号化モード ー 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 ー
  - The Kerberos Version 5 GSS-API Mechanism ー RFC 1964
  - Generic Security Service Application Program Interface, Version 2, Update 1 ー RFC 2743
  - Generic Security Service API Version 2: C Bindings ー RFC 2744
  - Generic Security Service API Version 2: Java Bindings ー RFC 2853
- Kerberos Network Authentication Service (V5) ー RFC 1510
- Hash-based Message Authentication Code (HMAC) ー FIPS 198 および RFC 2104
- Message Digest 5 (MD5) hash ー RFC 1321
- Password-Based Key Derivation Function 2 (PBKDF2) ー PKCS #5 v2.1 および RFC 8018
- Secure Hash Algorithm (SHA-1) ー FIPS 180-2 および RFC 3174
- Secure Hash Algorithm (SHA-512) ー 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)