Focus Systems

C4CS™
Certified Suite

FIPS 140-2適合認定を取得した国内初の暗号ライブラリ
第三者評価によりアルゴリズムとモジュールの安全性を確保

C4CSは、暗号モジュールのセキュリティ要件FIPS 140-2に準拠して開発された暗号ライブラリです。高速処理が可能な自社開発暗号C4Custom®に加え、AES、RSA、SHA-1など、日本の電子政府推奨暗号も多数搭載しています。

特長

モジュール実装の安全性を追求

C4CSは、暗号モジュールの実装方法を規定した安全基準であるFIPS 140-2への適合認定#490を取得しました。CMVP（Cryptographic Module Validation Program:暗号モジュール評価プログラム）における第三者評価を経て認定を取得しているので、モジュール実装における安全性が保証されています。

搭載アルゴリズムも認定を取得

FIPS 140-2には、米国NIST（National Institute of Standards and Technology）が認定・推奨するアルゴリズムの搭載を義務付ける規定があり、準拠性のテストが行われます。C4CSに搭載されているAESやSHA-1、RSA、擬似乱数生成器は、準拠性及び互換性が認められており、それぞれ認定を取得しています。

高速なC4Customとの使い分けが可能

高速処理が求められる場合は、自社開発のストリーム暗号「C4Custom」を選んで使用することが可能です。C4Customも別途第三者評価を受けており、「NIST Special Publication 800-22」で規定された乱数性評価テストにおいて乱数性99.9%であることが証明されています。

データ軽減を実現した（k, L, n）しきい値秘密分散法

C4CSには、東京大学との共同研究により実用化された（k,L,n）しきい値秘密分散法を搭載しています。秘密分散法を鍵管理の方法として採用し、実装における利便性をさらに向上させています。（k,L,n）しきい値秘密分散法は分散データの縮小が可能なので、知られてはならない鍵データを、より効率的に分散管理することが可能です。

取得規格

FIPS 140-2（米国連邦情報処理規格 140-2）

FIPS 140-2は、暗号モジュールのセキュリティ要件を規定した規格です。暗号モジュールとは、音声システムを含むコンピュータ及び通信システムにおける機密情報の保護のためにセキュリティシステムに組み込まれるものです。

暗号モジュール仕様、暗号モジュールポート及びインターフェイス、ロール・サービス・認証、状態遷移図、物理セキュリティ、動作環境、暗号鍵管理、EMI/EMC、セルフテスト、設計保証、その他の攻撃の対処といった11分野にわたるセキュリティ要件があり、実装レベルでの安全性を追及しています。

FIPS 140-2は米国、カナダ、英国の政府調達基準であり、現在、ISO/IEC 19790として国際規格化が進められています。日本国内でも、FIPS 140-2は暗号モジュール評価基準のベースとして採用されています。

TM : A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

第三者評価

CMVPによる第三者評価

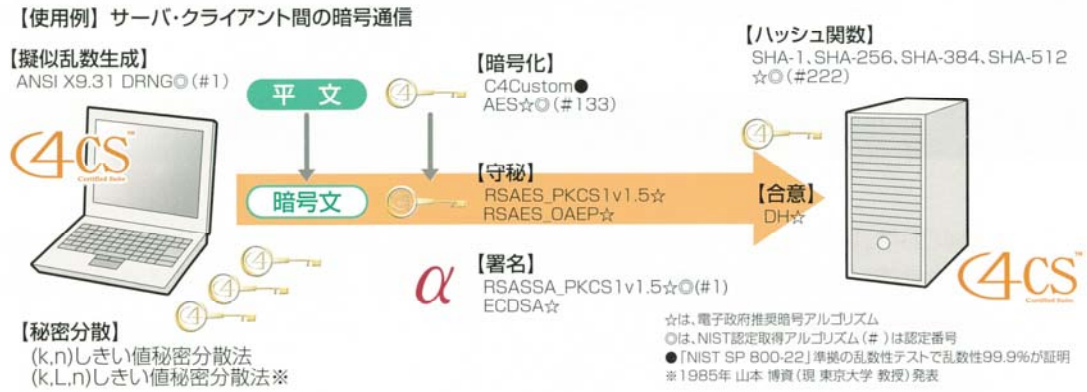
C4CSは、CMVP（Cryptographic Module Validation Program:暗号モジュール評価プログラム）の評価機関であるInfoGard Laboratories社によるテストを受け、認定機関である米国NIST及びカナダCSE（Communication Security Establishment）からFIPS 140-2(認定番号490)、AES（認定番号133）、RSASSA_PKCS#1v1.5（認定番号1）、SHA1/256/384/512（認定番号222）、RNG（認定番号1）を取得しています。

C4CS™
Certified Suite

FIPS 140-2適合認定を取得した国内初の暗号ライブラリ
第三者評価によりアルゴリズムとモジュールの安全性を確保

使用例

C4CSは、暗号ライブラリとしてさまざまな場面での利用が可能です。



搭載アルゴリズム

C4CSは、下記のアルゴリズムをサポートしています。

種類		アルゴリズム	特徴
共通鍵暗号	ストリーム暗号	C4Custom●	・シーフォーテクノロジーにより開発　・鍵長は可変長
	ブロック暗号	AES☆◎	・FIPS 197、AES認定取得 #133　・128/192/256ビットの鍵長に対応　・ECB/CBC/OFB/CFB/CTRモードに対応
公開鍵暗号	署名	RSASSA_PKCS1v1.5☆◎	・FIPS 186-2、PKCS#1 v1.5、RSA認定取得 #1
		ECDSA☆	・FIPS 186-2、ANSI X9.62
	合意	DH☆	・FIPS 140-2 Annex D、ANSI X9.42
	守秘	RSAES_PKCS1v1.5☆	・FIPS 140-2 Annex D、PKCS#1 v1.5
		RSAES_OAEP☆	・FIPS 140-2 Annex D、PKCS#1 v2.1
ハッシュ関数		SHA-1☆◎	・FIPS 180-2、SHS認定取得 #222　・ハッシュ長は160ビット
		SHA-256☆◎	・FIPS 180-2、SHS認定取得 #222　・ハッシュ長は256ビット
		SHA-384☆◎	・FIPS 180-2、SHS認定取得 #222　・ハッシュ長は384ビット
		SHA-512☆◎	・FIPS 180-2、SHS認定取得 #222　・ハッシュ長は512ビット
秘密分散法		(k,n)しきい値秘密分散法	・1979年 アディ・シャミアにより発表
		(k,L,n)しきい値秘密分散法	・1985年 山本 博資により発表　・パラメーターLの設定でシェアの縮小可能
擬似乱数生成器		ANSI X9.31 DRNG◎	・ANSI X9.31 Appendix A.2.4 DRNG認定取得 #1

☆は、電子政府推奨暗号アルゴリズム　◎は、NIST認定取得アルゴリズム(#)は認定番号　●「NIST SP 800-22」準拠の乱数性テストで乱数性99.9%が証明

【動作環境】

対応ＯＳ： Windows （32bit ／ 64bit）

※共通鍵暗号については、13OS 19モジュールのご用意がございます。（ダイナミックリンクライブラリ、スタティックリンクライブラリ）

【価格】下記までお問い合わせください。

https://www.focus-s.com

Focus Systems

株式会社フォーカスシステムズ

〒141-0022 東京都品川区東五反田5-24-10 テラサキ第3ビル 3階

TEL：03-5420-2470　E-Mail ： product@focus-s.com