暗号モジュール

MonoCrypt AES

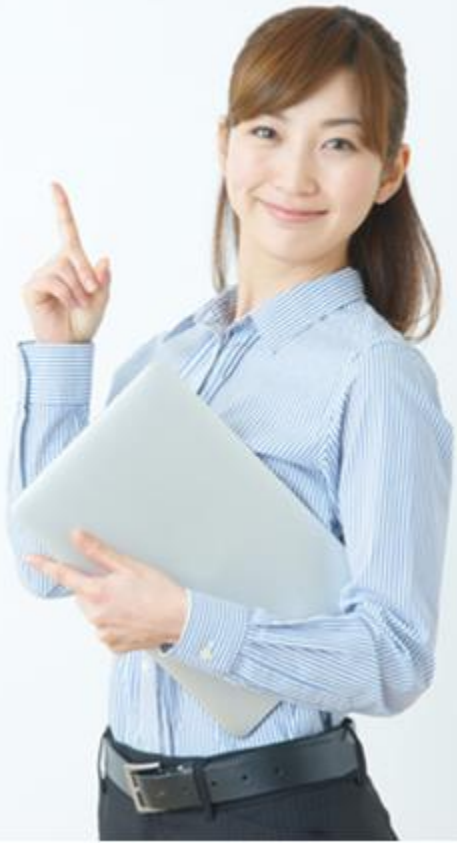
FIPS140-2
対応

MonoCrypt AES とは？

（モノクリプト　エーイーエス）

高いセキュリティ規格を取得し、多数の対象OSに適用・互換が可能な暗号モジュールです。

システムに組み込んで頂くことで使用データを暗号化することが可能となります。



こんなお悩みございませんか？

個人情報を扱うシステムのため、きちんと第三者認証のある暗号モジュールを使いたい。

自社製品の対応OSの種類が多く、それに対応したモジュールが見つかりません。

フリーの暗号モジュールを使っていますが、メーカーサポートもなく、正直心配です。

特徴

FIPS 140-2 の取得

アメリカ、カナダでの政府調達基準規格となります。
日本国内の基準のベースにもなっているため、安心してご利用いただけます。

豊富な実績

暗号モジュールメーカーとして10年以上の実績があります。
多くのお客様にご利用いただいています。

OSの互換性

暗号化・復号化を異なるOSで対応可能です。
対象OSも多くご用意させて頂いてます。

ご提案内容

政府調達基準規格

求められるセキュリティ基準が高い場合でも、選定頂くことができます。

安心のメーカーサポート

新しいOSへの動作確認や技術的なお問い合わせに対応します。

システムへの組込

システムへの組み込み暗号モジュールとしてご利用いただけます。

暗号モジュールの更新

FIPS140-2取得の暗号モジュールへ切り替えませんか。

主な機能

暗号・復号

項目	内容
方式	暗号時と復号時で同じ鍵を使用する共通鍵暗号アルゴリズムです。 対象データを一定のサイズに分割したブロックごとに処理を行う ブロック暗号方式となっています。
入力可能な鍵サイズ	128 bit、192 bit、256 bit のうちいずれか。
選択可能な暗号モード	ECB モード、CBC モード、CTR モードのうちいずれか。

鍵包みKey WrapZ

項目	内容
方式	共通鍵暗号方式を用いた鍵交換機能です。暗号鍵の受け渡しを 安全に行えるように機能として搭載されています。 CDC（NIST内の機関）が発行しているSP800-38Fに準拠しています。
入力可能な鍵サイズ	128 bit、192 bit、256 bit のうちいずれか。
選択可能な暗号モード	KWPモード、KWモードのうちどちらか。

動作OS

以下のOSに対応しています。詳細のバージョンや開発環境などにつきましては別途お問い合わせください。
また一部のOS及びバージョンにつきましては、FIPS140-2に対応しておりません。

Windows	Linux	AIX
HP-UX	Solaris	OS400/i5OS ※FIPS140-2非対応
Power Linux ※FIPS140-2非対応	zLinux ※FIPS140-2非対応	その他ご希望のOSが ございましたら、お気軽に お問い合わせください。

提供形態

CD1枚にて以下をご提供いたします。

- MonocryptAES DLL版　モジュール
- API仕様書（PDFファイル）

上記の他スタテック版（FIPS-120非対応）の提供も可能です。別途お問い合わせください。

価格

別途お問い合わせください。

導入事例（C4シリーズ含む）

- **某メーカ様**
  ファイル転送ソフトのシステム内セキュリティと、データ転送部分の暗号オプションに採用
- **某シンクタンク様**
  汎用機、UNIX系、Windowsにおけるデータ受け渡しのセキュリティに採用
- **某独立行政法人様**
  政府機関が発行する個人情報システムの情報保護に。
- **某重機メーカー様**
  監視システムの障害情報の外部出力の秘匿に採用
- **某メーカ様**
  POSシステムの通信セキュリティに採用
- **某工業系商社**
  医療データ保管システムのデータセキュリティに採用

・本製品は、原則日本国内のみでご使用ください。

・本製品は、外国為替および外国貿易管理法で規制される貨物・技術に該当します。

・本製品の輸出（日本国外への持ち出しおよび非居住者へ技術を提供する場合も含む）する場合は同法に従い、日本政府の輸出許可または役務取引許可が必要です。

・文中の内容は予告なく変更する場合がありますのでご了承ください。

【開発／販売】
株式会社フォーカスシステムズ

ITイノベーション第二事業本部 セキュアサービス室

〒141-0022　東京都品川区東五反田5-24-10 テラサキ第3ビル 3F
TEL：03-5420-2470　FAX：03-5420-9510
product@focus-s.com