

RSA BSAFE® CRYPTO

汎用暗号化コンポーネント

世界各国で情報の取り扱いに関する法規制が強化されており、個人情報の保護やアプリケーションの脆弱性に対策を施す必要が生じています。日本では個人情報保護法、米国ではクレジットカード業界が設定したセキュリティのガイドライン、カリフォルニア州の消費者プライバシー法、医療保険の相互運用性と責任に関する法律(HIPAA)、ヨーロッパではデータ保護条例などが現在、施行されています。トランザクションの開始から満了に至るまで、トランザクションの全ライフサイクルを通じて一貫したデータセキュリティを提供することが求められているため、設計者や開発者は、法令への準拠、信頼性の確保にプレッシャーが増すばかりです。

RSA BSAFE® Crypto-C/Jは、強力な暗号化技術を提供します。アプリケーションに対する信頼性を強化し、機密データに対して一貫した保護を提供できます。

特徴

- データプライバシー関連の各種規制への適合作業を支援
- 既存のデータモデルで提供されるセキュリティを緩めることなく、保管中のデータを一貫して保護
- ハイパフォーマンスの実装により、アプリケーションの要求条件に制限を与えることなく、効果的なセキュリティを提供
- 各種オープン・スタンダードのサポートにより、既存のインフラとの互換性を確保。将来起こり得る規制の変更にフレキシブルに対応
- オープンソース製品では得られない高信頼性、迅速な導入を提供

保管中のデータを一貫して保護

保護機能の一貫性を確保するには、通常のネットワーク・セキュリティ管理に加え、バックオフィスのデータベース・システムにある機密データについても適切にセキュリティを確保する必要があります。RSA BSAFE Crypto-C/Jは、既存のデータモデルとの統合を容易にする強力な暗号化技術を用いて、保管されている機密データを保護します。業界標準の暗号アルゴリズムを幅広くサポートしており、ユーザーのニーズに合わせて柔軟に選択可能です。

セキュリティ機能がアプリケーションのスループットのボトルネックにならないよう、多くのパフォーマンス最適化オプションが提供されています。Crypto-C/Jの機能をアプリケーションに活用すれば、一貫したレベルでデータを保護し、内外からのセキュリティ侵害の可能性を軽減します。

各種標準のサポートによりユーザー環境へ容易に統合可能

RSA BSAFE Crypto-C/Jが世界中の開発者に広く愛用されているもう一つの理由は、セキュリティに関する数多くの国際標準をサポートしていることです。グローバル・ビジネス、財務、電子商取引のネットワークにはITU-T、ISO、ANSI、IEEEのサポートが不可欠です。さらに、RSAセキュリティの暗号化ツールキット製品は、米国政府によるFIPS 140の認定を受けています。FIPS 140は、連邦政府および関連機関が採用する暗号化モジュールのセキュリティ要件を規定する厳格な規格です。FIPS 140の認定は、強力かつ効果的、かつ最新の暗号化ソリューションを常に提供するRSAセキュリティの製品開発ポリシーそのものです。

RSA BSAFE Crypto-CはC言語開発者向け製品です。RSA BSAFE Crypto-Jは、Javaアプリケーション開発者向け製品です。ともに開発者向けデータセキュリティ・ラインアップ「RSA BSAFE」の中核となる汎用暗号化ツールキットとして最適化された最新の暗号アルゴリズムを豊富に有し、あらゆる組込み用途に最適なツールキットです。



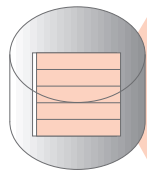
Confidence Inspired™

主な機能

RSA BSAFE Crypto-Cは、CおよびC++によるプログラム開発用の製品です。

RSA BSAFE Crypto-JはSun® Java® 開発者向けで100%ピュアJavaです。

- 多くの公開鍵暗号アルゴリズム、対称鍵暗号アルゴリズム、メッセージ・ダイジェストにより、幅広いセキュリティニーズに柔軟に対応。
- 乱数生成は、疑似乱数生成器とIntel®の乱数生成器(RNG)をサポート。
- 鍵生成サービスにより、鍵の生成を自動化し、暗号化鍵の生成機能を提供。
- PKCSに準拠した暗号化シンタックス、データ符号化サービスで、よりシームレスな互換性を提供。
- メモリの管理と保護サービスは、きめ細かなメモリ管理により、巨大な計算の出力が可能。
- RSA CMP(Cryptographic Multi-Precision)ライブラリの活用による高速数値計算処理は、絶大なパフォーマンスを実現。
- ハードウェアへの最適化は、RSA秘密鍵の処理パフォーマンスを向上するHP MultiPrime™テクノロジーをサポート。インテルのItanium®とPentium®4プロセッサ、SunのSPARC、Hewlett-PackardのPA-RISC、AMDのAthlon™とOpteron™の各プロセッサに最適化し、暗号化処理、鍵の保存、取出をスピードアップ。
- 置き換え可能なメモリ管理機構(Crypto-Cのみ)により、計算結果の出力に割り当てられるメモリを柔軟に拡張可能。
- ネイティブコード・サービス(Crypto-Jのみ)は、ネイティブコードの使用によりパフォーマンスの向上を実現。
- 抽象化機能(Crypto-Jのみ)は利用しない機密データに対してメモリの抽象化機能を提供。さらに、バイトコード単位の抽象化により、機密扱いのメソッドやクラスを未許可で使用できないようにします。



サポートプラットフォーム

オペレーティングシステム

- Microsoft® Windows®, Sun® Solaris™, HP-UX,
- Red Hat® Linux®, IBM® AIX®, z/OS, OS/390, OS/400

サポートJDK

- Sun, HP, IBM

上記以外のプラットフォームへのポーティングが可能。アセンブリやアルゴリズムの最適化をカスタマイズ可能

サポートアルゴリズム

公開鍵暗号アルゴリズム

- RSA®, MultiPrime™ DSA, Diffie-Hellman
- ECDSA, ECDiffie-Hellman, ECAES(Crypto-Cのみ)

対称鍵暗号アルゴリズム(秘密鍵暗号)

- AES, RC5®, RC4®, RC2®, DES, 3DES, DESX
- SEED(韓国政府標準暗号) (Crypto-Cのみ)

メッセージ・ダイジェスト

- MD2, MD5, HMAC, SHA-1, SHA-256, SHA-384, SHA-512
- RIPEMD-160(Crypto-Jのみ)

準拠する技術標準

- FIPS 140
- ANSI(米国規格協会) X9.30, X9.31, X9.32, X9.42, X9.56, X9.62, X9.63, X9.80(Crypto-Cのみ)
- PKCS(Public Key Cryptography Standards)
 - #1, #5, #8, #11
 - #12(Crypto-Jのみ)

プログラミング・インターフェース	C/C++ Java
エンコード/デコードサービス	公開鍵暗号アルゴリズム 対象鍵暗号アルゴリズム メッセージ・ダイジェスト
暗号化サービス	高速演算 シンタックス 鍵生成
アプリケーション・サービス	メモリ管理 データエンコーディング 抽象化(Javaのみ)
ハードウェア・インターフェース	プロセッサによる最適化 鍵管理 PKCS #11



RSAセキュリティ株式会社

〒100-0005 東京都千代田区丸の内1-3-1 東京銀行協会ビルディング
デベロッパ営業本部
Tel(03)5222-5210
<http://www.rsasecurity.co.jp>
info-j@rsasecurity.com

RSAは、RSA Security Inc.の登録商標です。BSAFEおよびRC4は、RSA Security Inc.の米国およびその他の国における登録商標です。本文中に記載されている製品名およびサービス名は、各社の商標または登録商標です。