IBM Encryption Facility for z/OS (5655-P97)

ビジネス・データの安全な転送を提供

ハイライト

- ビジネス・パートナー、サプライヤー、顧客とのデータ転送を安全に実現
- テープとディスクの暗号化と鍵管理を実現
- リモート・サイトでのアーカイブのための大容量データの暗号化を実現
- IBM® z/OS の鍵管理を活用
- リモート・サイトのアーカイブ・データのための長期的な鍵管理を実現
- OpenPGP RFC 4880 フォーマットのサポートにより、柔軟性を向上
- ZIP と ZLIB のアルゴリズムを使用する圧縮をサポート、また可能な場合には z Data Compression (zDC) を活用する圧縮をサポート

機密データの保護は、世界中で普遍的な課題となっています。機密データを保護できなければ、高額なコストが発生する可能性や、さらには、顧客と投資家の信頼を失う可能性があるため、ビジネスのクリティカルなデータと顧客情報の保護の重要性は企業の経営陣にまで影響が及びます。また、業界や各国政府および機関の規制、ビジネス・パートナーとの契約上の義務により、データ保護が必要になることもあります。データをネットワーク上で移動する場合でも、テープに保管して物理的にデータを移動する場合でも、無許可ユーザーからのアクセスを許さず、許可されたユーザーだけがデータにアクセスできるようにする必要があります。

IBM Encryption Facility for z/OS V1.2 では、保管データを保護するために、メインフレームの暗号化サービスを利用できます。これは 20 年以上にわたって ATM を保護してきた暗号化サービスです。z/OS の鍵の一元管理を使用して、暗号鍵を極めて安全に交換できます。例えば、ビジネス・パートナー向けの重要な情報は、ビジネス・パートナーが所有する秘密暗号鍵がなければ復号できません。

IBM Encryption Facility for z/OS を使用すると、z/OS システム上でデータを暗号化して、z/OS システムを持っていないパートナーや顧客にでも、そのデータを転送できます。z/OS を持っているパートナーには、データを復号するために、Encryption Facility, Java™ クライアント、Decryption Client for z/OS、OpenPGP RFC 4880 準拠プログラムを使用するオプションがあります。z/OS を持っていないパートナーは、データの暗号化と復号のために Java テクノロジーのクライアントや OpenPGP RFC 4880 準拠プログラムを使用できます。

Encryption Facility for z/OS は、次の 2 つのオプション・フィーチャー (有料) で構成されています。

- **Encryption Services フィーチャー**は、z/OS 上の特定のファイル・フォーマットの暗号化と復号をサポート。企業内のリモート・サイト、パートナーやベンダーへのファイルの転送と、ファイルのアーカイブが可能。Encryption Services フィーチャーは、IBM z Systems フォーマット (Encryption Facility for z/OS V1.1 から提供) と OpenPGP フォーマット (Encryption Facility for z/OS V1.2 で使用可能) の両方をサポート。System z フォーマットは、暗号化の前にハードウェアによる高速圧縮をサポート
- **DFSMSdss Encryption フィーチャー**では、DFSMSdss ダンプ・データ・セットの暗号化が可能。また、暗号化の前にハードウェアによる高速圧縮をサポート

z/OS の機能と z Systems のフィーチャーの提供する最先端の暗号化と鍵の一元管理は、データ保護に役立ちます。

Encryption Services フィーチャー

System z フォーマット

Encryption Services フィーチャーは、データ暗号化により、複数のプラットフォームにわたってパートナー、ベンダー、顧客との機密情報の共有を実現します。Encryption Services フィーチャーを使用して、特定のファイルをアーカイブのために暗号化することもできます。Encryption Services フィーチャーでは、Integrated Cryptographic Services Facility (ICSF) の中で提供されている z/OS の鍵管理とアクセス認証、System z のハードウェア圧縮とハードウェア暗号化を使用できます。

Encryption Services フィーチャーは、3 倍の鍵長の Triple-DES (TDES) 鍵または 128 ビット AES 鍵を使用するデータ暗号化をサポートします。ファイル暗号化に使用する AES と TDES のデータ鍵のラップとアンラップのために、RSA 公開鍵/秘密鍵を指定できます。ラップされた鍵はファイル・ヘッダーに格納されます。この技法により、さまざまな暗号鍵を使用して多数のファイルを生成でき、各ファイルは、アーカイブして数年間が経過した後でも読み取りが可能であることが期待できます。Encryption Services フィーチャーでは、パスワード鍵の導出スキームも使用できます。

Encryption Services フィーチャーは、物理的な順次入力ファイルからの入力や、区画データ・セット (PDS) と拡張区画データ・セット (PDSE) のメンバーからの入力、z/OS UNIX System Services ファイル・システムに保管されているファイルからの入力をサポートします。また、入力ファイルを暗号化して出力ファイルに書き込む前に圧縮できます。Encryption Services フィーチャーは、テープに書き込まれる出力ファイル用に大容量ブロック・インターフェースを使用することで、パフォーマンスとメディアのスペースも最適化します。

OpenPGP RFC4880 フォーマット

Encryption Facility for z/OS は、V1.2 から、OpenPGP フォーマットのサポートを提供するようになりました。OpenPGP サポートにより、ビジネス・パートナーとのデータ交換に使用可能な選択肢がさらに多くなり、柔軟性が向上します。Encryption Facility の OpenPGP サポートは、OpenPGP 標準の要件に準拠し、さらに、OpenPGP (RFC 4880) に準拠した製品との互換性も備えるように設計されています。このサポートにより、Encryption Facility for OpenPGP サポート を使用する内部のデータセンターと、z/OS やその他のオペレーティング・システムで稼働する OpenPGP (RFC 4880) 準拠クライアントを導入している外部のビジネス・パートナーやベンダーとの間で、暗号化、圧縮、デジタル署名が実行されたファイルを交換できます。Encryption Facility の OpenPGP サポートには、ランダムに生成されたセッション鍵のパスフレーズ・ベースの暗号化、RSA と ElGamal のアルゴリズムを使用してランダムに生成された対称鍵の非対称暗号化、データのデジタル署名などの多くの新機能と、お客様のオペレーティング環境と要件において重要な可能性がある多数の機能が組み込まれています。

Encryption Facility for z/OS V1.2 の OpenPGP フォーマット・サポートは、System z フォーマット・サポートよりも多くの CP を消費するため、並列処理を増やすことで、複数の CP を活用するように構成できます。OpenPGP フォーマット・サポートの CPU 使用率が高くなることの影響は、z13 上の z Integrated Information Processor (zIIP) プロセッサー、z13 上の zIIP プロセッサーと zEnterprise Application Assist Processor (zAAP) プロセッサーによって軽減できます。OpenPGP フォーマット・サポートは Java で作成され、Java ワークロードは専用エンジン・プロセッサーに適切であるため、ソフトウェア使用料金を節約できる可能性があります。そのため、オンライン CPU を4個以上構成した場合などでは、OpenPGP フォーマット・サポートのタスクにかかる時間は、System z フォーマット・サポートにかかる時間よりも短く済む可能性があります。

これらの機能は、ICSF とハードウェア暗号化を活用できます。ハードウェア暗号化には、適切な環境が必要であり、暗号化モジュールの取り付けが必要になる可能性があります。

Encryption Facility for z/OS V1.2 は、現在サポートされている z Systems と z/OS の各リリースで使用できます。

DFSMSdss Encryption フィーチャー

DFSMSdss Encryption フィーチャーは、テープや DASD に書き込まれた DFSMSdss ダンプ・データ・セットを暗号化できるようにします。DFSMSdss Encryption フィーチャーは、z/OS の鍵管理とアクセス認証のほか、z Systems のハードウェア暗号化とハードウェア圧縮を活用する設計になっています。

DFSMSdss Encryption は、3 倍の鍵長の TDES 鍵または 128 ビット AES 鍵を使用するデータ暗号化をサポートします。Encryption Services フィーチャーと同様に、ファイル暗号化に使用する AES と TDES のデータ鍵のラップとアンラップのための RSA 公開鍵/秘密鍵の使用のほか、指定されたパスワード

を使用する AES と TDES の鍵生成をサポートします。また、DFSMSdss によってデータを暗号化する前に圧縮するように指定できます。

DFSMSdss Encryption フィーチャーには、DUMP コマンドの処理中にデータを暗号化する機能と、RESTORE コマンドの処理中にデータを復号する機能が組み込まれています。

Encryption Facility for z/OS Client を z Systems フォーマットで使用
Encryption Facility for z/OS Client は、ライセンスが別に提供されるプログラム (無保証で現状のまま提供されます) です。Encryption Facility がインストールされている z/OS システムと、サポートされている機能を必要とする z/OS またはその他のプラットフォームで稼働しているシステムとの間で、暗号化データを交換できるように設計されています。

Encryption Facility for z/OS Client の構成は、以下のとおりです。

- **Java クライアント**。Java クライアントは、Java で作成されており、z/OS のほか、Java をサポートするすべてのプラットフォームで使用できます。Java クライアントは、z/OS システムで Encryption Facility z Systems フォーマットを使用して作成されたデータの復号と、z/OS システムに送信されるデータの暗号化の両方をサポートします。z/OS システムでは、ファイルは Encryption Facility z Systems フォーマットを使用して復号されます。注: Java クライアントを使用してデータを処理する場合は、圧縮は使用できません。
- **Decryption Client for z/OS**。Decryption Client for z/OS は、z/OS システムでのみサポートされています。Decryption Client for z/OS は、z/OS システム上で Encryption Facility z Systems フォーマットを使用して作成されたデータの復号をサポートします。Decryption Client for z/OS を使用してデータを処理する場合は、圧縮を使用できます。Decryption Client は、のデータ暗号化をサポートしません。Decryption Clientには、パフォーマンス向上のメリットがある可能性や交換に必要なメディアが少なくて済む可能性はありますが、ビジネス・パートナーは暗号化されたフォーマットでデータを返すことはできません。

メインフレームの暗号化という価値

IBM のメインフレーム暗号化サービスは、ハードウェアとソフトウェアの統合、つまり、メインフレーム・サーバーによる暗号化と圧縮のテクノロジーと、z/OS オペレーティング・システムによる鍵の一元管理との統合に基づいています。

メインフレーム暗号化ハードウェアには、2 つの重要な機能があります。ソフトウェア・ベースの暗号化より高速に暗号化する機能と、適切なフィーチャーとともに提供される Secure Key サービスです。高速の暗号化機能は、IBM z Systems の CPU に組み込まれた CP Assist for Cryptographic Function (CPACF) で提供されます。IBM System z10 Enterprise Class (z10 EC) 以降のサーバーではさらに機能を強化し、SHA-512 ハッシュ・アルゴリズムと、急速に事実上の暗号化標準となっている 256 ビット Advanced Encryption Standard (AES-256) のサポートが含まれます。

オプションのフィーチャーである Crypto Express2、Crypto Express3、Crypto Express4s は、Secure Key テクノロジーを提供し、公開鍵/秘密鍵を使用する信頼性の高い交換を実現します。Secure Key は、ホストと ATM との通信など、銀行の機能にとって重要です。Crypto Express2 は、TDES と Trusted Key Entry をサポートして、Secure Key オプションを提供します。Crypto Express3、Crypto Express4s は、TDES と 128 ビット、192 ビット、256 ビットの AES のデータ暗号鍵をサポートします。最新世代の Crypto Express5s は、Encryption Facility for z/OS が z13 CPACF におけるパフォーマンス向上とともに活用できるよう、パフォーマンスを強化しています。

z/OS の ICSF 機能は、暗号化が必要なアプリケーション間のインターフェースと、ハードウェア暗号化サービスを提供します。20 年以上にわたって世界中のメインフレームのお客様によって使用されてきた実績ある ICSF は、企業における暗号鍵の保護と管理に役立ちます。これには、鍵の生成、ポリシーに基づく鍵の管理、鍵のリカバリーが含まれます。ICSF のもう 1 つの重要な機能は、監査コンプライアンス情報とアクセス制御を提供できることです。

これらの暗号化機能は、IBM メインフレームの回復力と可用性を通じてさらに拡張されます。メインフレームの高い可用性、スケール、回復力、リモート・リカバリー機能は、暗号鍵の保管と管理に最適な選択肢となります。IBM メインフレームが提供する暗号化機能は、z/OS オペレーティング・システムに組み込まれたセキュリティーとともに、長期的な鍵管理のための優れた基盤を提供します。Encryption Facility for z/OS (V1.2) は、テープやディスクへの包括的なデータ暗号化アプローチを提供します。

IBM が提供するその他の暗号化機能

IBM は、暗号化ソリューションを幅広く提供し、データ保護要件に対応します。

IBM のテープ・ドライブによる暗号化
IBM System Storage TS1120 以降のテープ・ドライブは、データ暗号化をサポートする高性能で柔軟なデータ・ストレージを提供します。暗号化機能は、新規に注文されるすべてのテープ・ドライブ (TS1120 以降のモデル)に標準で搭載されています。暗号化可能な TS1120 モデル以降のテープ・ドライブでは、暗号化機能をサーバーからテープ・ドライブにオフロード (サーバーのオーバーヘッドを回避) 可能なデータ保護ソリューションを提供するとともに、データのアーカイブとバックアップに伴う大容量データのコスト効率の良い暗号化ソリューションを提供します。z/OS とともに使用することで、TS1120 モデル以降のテープ・ドライブは、z Systems 独自のセキュリティーと暗号化機能を活用し、企業全体で暗号鍵を保管、管理する強力なソリューションを実現します。

IBM Security Key Lifecycle Manager (ISKLM)
IBM Security Key Lifecycle Manager (ISKLM) for z/OS は、暗号化対応の IBM テープ・ドライブとシステム・ストレージ・デバイスと連携します。ISKLM は、デバイスに書き込まれる情報の暗号化と、デバイスから読み取られる情報の復号に使用する暗号鍵の生成、保護、保管、保守に役立ちます。デバイスへの鍵の提供を管理するコマンドライン・インターフェースがあります。さらに、ISKLM for z/OS は、暗号化対応の 3592 テープ・ドライブと Linear Tape-Open (LTO) テープ・ドライブをサポートします。サポートするドライブ・タイプは、以下のとおりです。

- データを暗号化可能な TS1120、TS1130、TS1140、TS1150 テープ・ドライブ
- データを暗号化可能な LTO Ultrium 4、LTO Ultrium 5、LTO Ultrium 6 テープ・ドライブ。テープ・ドライブでフル回線速度でデータ圧縮後に暗号化を実行

ISKLM for z/OS は、適切なマイクロコード・バンドル・バージョン、ライセンス内部コード (LIC) レベル 64.2 以降とともに IBM DS8000 Storage Controller をサポートします。

IBM Data Encryption for IMS and DB2 Databases
IBM Data Encryption for IMS and DB2 Databases は、IMS と DB2 の両方のz/OS データベースに対応するデータ暗号化ツールを提供します。この製品は、機密データとプライベート・データを、IMS ではセグメント・レベルで、DB2 では行レベルで保護するように設計されています。IBM Data Encryption for IMS and DB2 Databases は、標準の IMS 出口ルーチンと DB2 出口ルーチンを介して実装されます。これらの出口ルーチンは、z Systems 暗号化ハードウェアを呼び出して、保管のためにデータを暗号化し、アプリケーションで使用するためにデータを復号します。

これらのソリューションは、暗号化機能を幅広く提供します。各機能はお客様の環境における特定のエレメントを保護する設計になっています。これらの暗号化ソリューションのうちどのソリューションがお客様のセキュリティー要件に適切かを評価し判断する際は、IBM 営業担当員またはビジネス・パートナーに詳細をお問い合わせください。

ハードウェア要件:

Encryption Facility for z/OS の Encryption Services フィーチャーと DFSMSdss Encryption フィーチャーは、以下の IBM サーバー上で稼働します。

- IBM z13
- IBM zEnterprise EC12 (zEC12) または IBM zEnterprise BC12 (zBC12)
- IBM zEnterprise 196 (z196) または IBM zEnterprise 114 (z114)
- IBM System z10 Enterprise Class (z10 EC) または IBM System z10 Business Class (z10 BC)
- IBM System z9 Enterprise Class (z9 EC) または IBM System z9 Business Class (z9 BC)

ハードウェア暗号化オプションの最小要件は、以下の「IBM United States Announcement 207-008 (2007 年 1 月 16 日)」に記載されています。

詳細については、次の発表をご覧ください。**ibm.com**/common/ssi/rep_ca/8/897/ENUS207-008/ENUS207008.PDF

詳細情報

IBM メインフレームのセキュリティーの詳細については、次の Web サイトをご覧ください。**ibm.com**/systems/jp/z/solutions/security/

本資料に含まれる内部スループット率 (ITR) 比によるパフォーマンス・データは、管理環境下で標準の IBM ベンチマークを使用し得られた測定結果と予測に基づくものです。ユーザーが実際に得られるスループットは、ユーザーのジョブ・ストリームにおけるマルチプログラミングの量、I/O 構成、記憶域構成、および処理されるワークロードなどの考慮事項によって異なります。従って、個々のユーザーがここで述べる比率と同等のスループットまたはパフォーマンスの向上を得られるという保証はありません。

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町 19-21

Produced in Japan
January 2015

ZSD01450-JPJA-04