

IBM Enterprise Key Management Foundation

全社的な鍵と証明書管理

ハイライト

- 鍵の管理を一元化することにより、要件への対応を推進
 - 標準化された一連の手順と操作を使用して複数のシステムを管理
 - IBM® System z のハードウェア暗号化機能への投資を活用
-

ネットワークの相互接続が進む世界では、機密情報のセキュリティは極めて重要です。データ違反は大きなニュースになるほどの。そのため、PCI-DSS (ペイメント・カード業界のデータ・セキュリティ規格)、HIPAA (医療保険の携行性と責任に関する法律)、および SOX 法 (サーベンス・オクスリー法) などの新たな要件や規制機関は、情報の保護に暗号化を使用する企業に対してさまざまな課題を要求しています。また、暗号化を採用するシステムの増加に伴い、企業は増え続ける一連の暗号鍵にも対応しなければなりません。暗号化された情報の可用性とセキュリティを確保するには、これらの鍵を効果的に管理することが極めて重要です。鍵と証明書の生成、更新、バックアップ、およびリカバリーに関する複雑な作業を実行するには、鍵と証明書を一元的に管理する必要があります。

IBM Enterprise Key Management Foundation (EKMF) は、企業向けの柔軟かつ極めてセキュアな鍵管理システムです。EKMF は、IBM zEnterprise と分散プラットフォームにおける鍵の管理を一元化することにより、鍵と証明書の管理業務を簡素化・効率化するとともにセキュリティを確保します。EKMF は、EMV (ユーロペイ・マスターカード・ビザ) や PCI (ペイメント・カード業界) の要件への対応が必要な、銀行、ペイメント・カード処理機関、およびその他の企業に最適なソリューションです。コンプライアンス問題を特定し、鍵の管理責任者が鍵情報へのアクセス権限を持つ利用者を識別できるように、暗号解析機能が組み込まれています。EKMF は、さまざまな業界のニーズに応じて調整可能な基盤を提供し、コンプライアンス問題を特定するとともに、鍵の管理責任者が企業の鍵管理ポリシーの要件を実施できるようサポートします。

鍵管理の一元化

鍵の一元管理ソリューションは、システムが要求する鍵や証明書のフォーマットに対応し、かつ規制機関が要求するポリシーに準拠できる場合のみ有用です。EKMF は証明書および対称鍵と非対称鍵に関する全社的な管理機能を提供します。EKMF は多数のプラットフォームや暗号化処理カードに対し、さまざまな種類の DES (Data Encryption Standard) 鍵、AES (Advanced Encryption Standard) 鍵、および RSA (Rivest Shamir Adleman) 鍵をサポートします。また、ペイメント・カード・ソリューションのための EMV 規格など、一連の特化された業界規制に対する準拠性を確保します。EKMF の機能は、お客様のニーズ、業界標準、および規制構想に応じて継続的に拡張および強化されています。

EKMF では、鍵は対象プラットフォームとは別に管理されます。EKMF は、暗号化コプロセッサ、ハードウェア・セキュリティ・モジュール (HSM)、ソフトウェア実装 (Java 鍵ストア、ATM、POS 端末装置など) の鍵と証明書を管理します。また EKMF は、カードの発行および決済機関やカード・ブランドに対して、EMV チップ・カードの対応を奨励します。



複数システムの管理

大多数のコンピューティング・センターには複数のサーバー・システムが存在し、多くの場合それらは地理的に分散しています。EKMFにより、システム全体の鍵と証明書の管理機能をすべて単一のワークステーションから実行できます。EKMFはネットワーク上のあらゆる暗号化エンティティー（端末装置、機関、暗号化コプロセッサ、サーバーなど）をサポートできます。各エンティティー・タイプは独自の鍵階層を持ちますが、それぞれを定義して管理できます。鍵ストアを実装する暗号化コプロセッサの場合、EKMFはそのストアのコンテンツを維持します。

System z への投資の活用

EKMFはIBM System zの能力を活用し、柔軟かつ極めてセキュアな鍵の一元管理システムを企業に提供します。System zは、市販のあらゆるサーバーにとって実質的に最高のセキュリティー等級（区分）であるコモン・クライテリア評価保証レベル5（EAL5）の認定を取得しています。

市場には数多くの鍵管理アプライアンスが存在しますが、アプライアンスは単一障害点となるおそれがあるため、高可用性構成を実現するには至りません。機密情報を扱う鍵、証明書、およびメタデータを System z 上に保持することにより、企業で既に実施されている事業継続性と災害復旧の計画を活用して、極めてセキュアで可用性の高い鍵の中央リポジトリを作成できます。

IBM をお勧めする理由

System z ベースのシステムを使用する多くの銀行やカード処理会社は、既に EKMF の機能を活用して EMV ペイメント・カード仕様やエンドポイント・デバイスに対する鍵のリモート・ロードを実装しています。当初、欧州の金融機関との提携によって開発された EKMF は、堅固で拡張可能な成熟したソリューションで、今日さまざまな業界において標準となりつつあるセキュリティーとコンプライアンスの厳しい要件に対応できます。EKMF はその成熟度によって企業の信頼に応えるソリューションを実現しています。

詳細情報

IBM Enterprise Key Management Foundation についての詳細は、日本 IBM の営業担当員または IBM ビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。

ibm.com/systems/services/labservices/platforms/labservices_z.html



© Copyright IBM Corporation 2013

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 2013

IBM、IBM ロゴ、ibm.com、System z、および zEnterprise は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、ibm.com/legal/copytrade.shtml をご覧ください。

本書の情報は最初の発行日の時点で得られるものであり、予告なしに変更される場合があります。すべての製品が、IBM が営業を行っているすべての国において利用可能なものではありません。

本書に掲載されている情報は特定物として現存するままの状態を提供され、第三者の権利の侵害の保証、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されています。IBM 製品は、IBM 所定の契約書の条項に基づき保証されます。



Please Recycle