ハイブリッド、マルチクラウドの世界でデータ保護を維持

AN ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) WHITE PAPER

IBM向けホワイトペーパー

著者：PAULA MUSICH

発行日：2020 年 6 月

EMA™

IT とデータ管理
調査 | 業界分析 | コンサルティング

目次

ハイブリッド、マルチクラウドの世界でデータ保護を維持

近代的なクラウドに接続した企業にとって、デジタル・コラボレーション作業と、それに伴うデータ共有は、生活の一部になっています。企業の強化された境界内で作業し、適切に認証資格を得た社員や下請け業者に対する従来の信用度に対する期待は、近代的なクラウドベースのアーキテクチャーまで延長されています。事業目的を達成するために共同作業するチームは、プライベートのハイブリッドクラウド、マルチクラウド、およびオンプレミスベースのアプリケーションにわたるデータを自由に共有できます。ほぼすべての場合、このようなデータはプレーン・テキストで共有されます。クラウド内のデータに関する調査では、暗号化されているクラウド・データはわずか 9.4% です。そのデータがインターネットに露出されるなどして漏えいした場合、組織はそれを撤回したり削除する方法はほとんど、あるいはまったくありません。データが盗まれた場合、データが暗号化されていなければ手立てはありません。

これらのアクティビティーすべての原因は、信頼性の薄いエコシステムでデータを共有することにあり、このエコシステムは暗号化によって強化することが可能です。残念ながら、さまざまな状態にあるデータを保護するテクノロジーのコンパートメント化と、トランザクションの両側におけるユーザー摩擦の悪化のために、暗号化は一般的に利用されていません。さらに悪いことには、データの受信者が機密性を守らず、他者とデータを共有した場合 (過失の場合を含め)、データの所有者や保護者は、違反者が通知しない限り、信用が裏切られたことを知る方法はありません。企業データは、包括的でより緊密に統合されたテクノロジーによって、より強力に、より広範囲に守る必要があります。これにより、データの所有者や保護者による、データのライフサイクル全体を通した統制の維持とデータの追跡が可能になります。

McCumber Cube とリスクの三次元

1991 年に John McCumber 氏は McCumber Cube と呼ばれるサイバーセキュリティーのリスク・モデルを発表しました。このモデルは、サイバーセキュリティーのリスク要因を三次元の立方体として表現した点が画期的でした。立方体の眼に見える各表面には、管理する必要があるサイバー・リスクの 3 つの側面があります。三次元の各交差点は、各表面からの 3 つの構成要素の和を表します。赤で描かれた最前面の小立方体は、機密性、テクノロジー、処理の交差点です。これは、テクノロジー管理が、処理中のデータのプライバシーを守るという概念を表します。

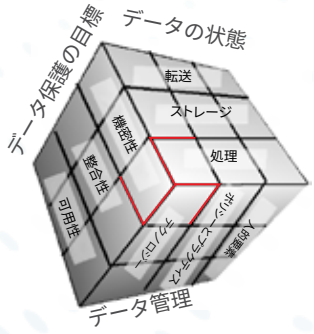

図 1：

本ホワイトペーパーでは、データのライフサイクル、移動、保管、処理の各段階で暗号化が適切に適用されることによって統制が強化され、保護とプライバシーが改善されるかについて説明します。デジタル・データ共有と共同作業の時代において、このような統制により、データの露出、漏えい、喪失、盗難のリスクが低減されます。本ホワイトペーパーでは、新しい暗号化統制を通した機密性の提供と、データのライフサイクルを通してあらゆる場所で暗号化を使用することによってデータ統制にどのような影響を与えるかという点に注目します。

移動中データの暗号化

機密性、テクノロジー、移動の交差点

暗号化を適切に適用することで、データ漏洩を大幅に低減できます。McCumber Cube では、機密性、テクノロジー、移動の交差点は、Transport Layer Security (TLS) プロトコルと、その前身、Secure Sockets Layer (SSL) を使用して説明されています。2019 年の終わりまで、インターネット上で移動中のデータの保護は、Web サイト中心のトラフィックの暗号化が 95% 近く改善しました。

インターネット環境を通したトランスポート・ベースの暗号を使用することには長所と欠点があります。データの所有者にとっての主な利点は、正当な業務目的でデータを移動する際に高い機密性が提供される点です。データの所有者にとっての主な問題は、高機密性の暗号化が、盗まれたデータの移動に悪用されることです。セキュリティー・モニタリングではトラフィックの内容まで+は感知できないことが多く、許可を得た中間者攻撃により中身が何かを調べるためにトラフィックを傍受するゲートウェイ・プロキシー・ツールに投資する必要があります。この種の検査は、アプリケーションのレイテンシーの増加にもつながるため別の問題が発生し、トランスポート・ベースの暗号化を困難かつ、多くの場合、高コストなものにしています。

複数のブラウザに共通する SSL および TLS のためのデータ・トランスポート暗号化標準の構築と実装は、国際的なポリシーの策定、施行、および鍵共有よりも物流的に容易です。ただし、暗号化は、多くのインターネット・ユーザーに誤ったセキュリティー認識を与えます。ユーザーは暗号化されているから自分のトランスポート・データは守られていると考えがちですが、データが移動状態から処理または保管状態に移ると、TLS セキュリティは解除され、データの攻撃に対する脆弱性は増加します。

また、興味深いことは、トランスポート暗号化が注目される前でも、トランスポート暗号化に対する攻撃が成功した件数は少なく、保管中のデータが盗まれたレコード数は多かったことです。移動中の、特に特定のデータを盗むには、保管中のデータを盗む場合より技術的に高度な準備やタイミングが必要になります。

保存中データの暗号化

機密性、ストレージ、テクノロジーの交差点

窃盗の標的になるのは圧倒的に保管中のデータです。報告組織によって数値に差がありますが、リスクベースのセキュリティーからの数値では、データ漏洩レコード数は 2016, 40 億を越え、2017, 70 億レコードを越え、2018, 50 億レコードを越え、2019, 80 億レコードをわずかに下回りました。The Thales Security 2019 Data Threat Report では、重要な環境内に暗号化を導入している組織は 30% 未満であり、暗号化されているデータの割合は 1 桁に落ちると見積もられています。

歴史的に、暗号化システムはコストがかさみ、インストール、設定、運用、保守が難しいことが分かっています。データを操作するビジネス・ユーザーは、暗号化により仕事に摩擦が生じ、パフォーマンスに悪影響があり、さらにはリクエストの失敗や喪失の原因になると批判します。このため、操作性とセキュリティーを天秤にかけると、いまだに操作性の方が優先されています。

保管中のデータの場合、これらの問題を解決するには、暗号化キーの管理に注力することによって基盤となる暗号化システムの操作性を調整する必要があります。社内従業員または外部顧客であるデータ顧客からの摩擦を排除するデータ暗号化ツールの操作性を保証することも重要です。

処理中および使用中データの暗号化

機密性、処理、テクノロジーの交差点

McCumber Cube モデルは、コンピューター・システム内の自動化処理へ、またはデジタル化前後の手動のデータ処理に適用できるデータ処理を特定します。

処理中データの暗号化

アプリケーション内を移動するデータを保護することは、おそらく最も困難なデータ・リスク管理の側面です。最初の管理ゲートは通常のアクセス権付与です。アプリケーションの入口にユーザーがアクセスできなければ、データへのアクセスはさらに困難になります。この点を超えると、コントロールはサーバーを物理的に保護することや、システムを構成する電子部品の保護強化が重要になります。処理中のデータを攻撃するには、システムに直接アクセスして探りを入れ、操作されるデータに直接アクセスしたり、アプリケーションやシステム・ドライバーにマルウェアを挿入して、アプリケーションの操作中にデータを集める必要があります。

使用中データの暗号化

処理がどのように構造化されているかに従って、ユーザーがデータを処理している間にデータを吸い上げるユーザーに対して防御する制御を追加する必要があります。適切なデータが適切なユーザーによって処理されるよう注意する必要があります。従来、暗号化が最も多く展開されたのはこの段階です。信頼の輪に適切なユーザーだけが含まれている限り、データの所有者や保護者はデータが安全であると確信できます。ただし、最近まで、データが所有者や保護者の手を離れた後でも、情報の暗号を解読し、データの所有者や保護者の知らない他者に転送することが可能であるという決定的な限界がありました。

処理中および使用中データへの攻撃に対する防御

マルウェア対策ソフトウェアは攻撃に使用されるマルウェアに対応する上では効果的ですが、処理システムからユーザーを隔離するためには、ロックやセキュリティー・ガードが最も一般的に使用されています。暗号化は、処理中のデータの露出を制限するために処理やその他の領域に適用できます。データ自体を 露出することなく, 暗号化されたデータから関連のあるクエリー情報を抽出する準同型暗号化などのプロジェクトが進行中です。このようなプロジェクトは有望ではありますが、実用までに何年もかかると考えられます。

最近の暗号化機能は、データのライフサイクル全体を通してデータに永続的に権利を保証するよう進化しています。共有後もデータ所有者があらゆるユーザーに対する使用権限を追加、変更、または撤回することができるよう飛躍的に進化しています。

あらゆる場所での暗号化によるリスク低減

あらゆる場所と状態のデータとプライバシーを保護

2018 年のなりすましによる損失は、米国だけでも 17 億ドルと 見積もられています。Commission on the Theft of American Intellectual Property は、米国の企業からの中国の知的財産の窃盗による損害は 年間 6000 億ドルと 見積もられています。これらの損失を回避し、データのライフサイクル全体を通して真の保護を保証するには、アプローチを根本的に変える必要があります。最近まで、ターゲットにデータがいったん送信されると、元のデータの保護者は管理できなくなっていました。データ所有チェーンの次のユーザーを完全に信用していたのです。そのユーザーが信用の輪を拡張することを決めた場合、元の所有者の許可を得る必要はありませんでした。

データの保護者は必要な情報のみ共有する必要があり、要件の側面は流動的なまま、何が必要かを決定します。このため、立場が不安定になります。過去に社内共有が許可されていたことが、今では適用範囲外とみなされます。現在の共有データの文脈では、暗号化されているか、いないかにかかわらず、変更されたポリシーを実装することにより組織を守り、適用範囲外となったデータを再取得するには、多大の工数がかかります。多くの場合、社内複製データすべてが返却、または破壊されたことを確認することは可能です。悪意がなくても、共有データのコピーが、バックアップ、電子メール、共有フォルダ、個人用ドライブなどの他のレポジトリに保存されている可能性があります。この問題は、保存中、移動中、保管中、クラウドにあるかどうかにかかわらず企業全体の保護およびプライベート・データを維持する、あらゆる場所での暗号化の概念によって解決されます。

機密性、ポリシー、プロセス、人的要因の交差点

ポリシーとプロセスは、あらゆる強固な暗号化システムの基本要素です。ポリシーは、何が共有できるか、あるいはできないか、および保護されたデータ要素ごとに信頼の輪の中に入れるユーザーを規定します。残念なことに、従来の暗号化システムでは、ポリシーは、データが規定された場所とユーザーの所有下にあることを保証するために、事前に規定されたポリシーに人間が従う信用度を基に規定されることが多くなります。人的要因がミスを犯せば、データの漏えいや露出が起こる可能性があります。

暗号化アルゴリズムがいかに強固なもので、ポリシーがどれほど文書化されても人が意図的にそれらに従わないことを選択したり、判断を誤ると、保護すべきデータが危険にさらされます。ほとんどの場合、これは単に迷惑なだけですが、深刻な風評被害や経済的な影響が出る場合もあります。American Semiconductor 社の 知的財産の盗難事件は 組織に与えうる損害を示す最も有名な例です。盗用が報道されてから、American Semiconductor 社の株価は 50% 近く下落しました。

人的要因からデータを守る第一歩は、保護されていないデータを開示または共有できる人間の数を減らすことです。データ所有者はデータ権利をいつでも制御でき、提供メカニズムや共有環境から隔離してその制御を維持できます。これにより、意図しないデータの開示を防止するための 2 つの統制が確立できます。

あらゆる場所での暗号化の概念には、データのライフサイクル全体を通じた、事前防止的なデータ・ガバナンスが必要になります。データ保護は、データ内に埋め込まれた暗号化システムを構築する、施行可能なポリシーに転換される必要があります。社内に配信される前にデータにポリシーが適用され、データの移動中も継続された場合、データ所有者はそのデータの状態にかかわらずデータに規定した資格がついてくることを保証できます。所有者は、管理サーバーの再確認が必要になるまでの時間の長さを規定する必要もあるため、企業内のどこにデータが移動しても共有データにアクセスできるユーザーを一貫して制御できます。その上で、テクノロジーを使用してデータのライフサイクル全体を通して監視し、ポリシーを強制します。これにより、従業員やビジネスパートナーの変更に始まり、その他の運用上の要件にいたるまで、変化するビジネス需要に適合しながら永続的に保護できます。

割り当てられた権限は、構造化されていないデータ内で有効になり、そこに常駐して保護され続けます。データ・アクセスが試みられると、要請はデータ所有者の環境内にある鍵管理システムに送信されます。要請者に適切な資格が割り当てられている場合は、情報のロックを解除し資格を実行するための一時的なトークンが送信されます。l構造化されたデータは、属性またはデータ・レベルで保護できます。受信者の場所で維持されるデータは、ずっとデータ所有者または保護者の制御下に残ります。データの所有者がアクセス・パラメーターを変更する、あるいは完全に削除する必要があると決定した場合、ポリシーに変更を加えるだけで、いつでもリモート・データ・コピーに適用されます。

ライフサイクル全体を通してデータを保護するための適応型ポリシー

共有関係が終了した場合、またはデータ所有者が資格を変更する必要があると考えた場合は、いつでもポリシー・エンジンの資格を更新できます。資格を確認する次の要請があったときに、更新された権限が施行されます。更新された権限は、アクセスされる前に作成されたコピーに適用されます。完全な撤回が適用された場合、鍵は破壊され、暗号化データは無効になります。受信者は鍵へのアクセス権を持っていないため、データは不正利用から保護されます。

あらゆる場所での暗号化によるデータ保護

テクノロジーによって強制されるポリシー、永続的なデータ資格、厳格な鍵管理システム、強力な暗号化は高度な防御の確固とした基盤になります。あらゆる場所での暗号化の概念と適用の独自性は、データセンターにまたがる継続的な保護と、JDBC 接続を通してアクセスできる適格なデータの統制を維持できることにあります。あらゆる場所での暗号化の概念を現実に機能させるには、データ所有者はポイント・ソリューションだけでなくテクノロジー・エコシステムを活用する必要があります。現在、ポイント・ソリューションは、局所的な解決策としては有効ですが、包括的な、あらゆる場所での暗号化エコシステム向けには設計されていません。幅広い統合は、ポイント・ソリューションが必要な場所には必要ありません。このため、包括的なデータ保護を達成するためには、設計目標として作り込まれた高度の相互運用性と緊密に統合する必要があります。そうすることで、データはその存在の各段階で保護されます。

あらゆる場所での暗号化のユースケース

一覧のユースケースから、データ保護とプライバシーを継続的に提供するために使用できる IBM と IBM 以外のコンポーネントが特定できます。他のベンダー・ソリューションを使用してあらゆる場所での暗号化概念全段階を達成できますが、IBM は現在、IBM Z 上で適格なデータの保護とプライバシーを継続的に提供するために緊密に統合されたエコシステムを提供している唯一のベンダーです。ユース・ケースでは以下のコンポーネントが使用されました:

1. IBM z15 または 全方位型暗号化機能を使用する Linux on Z
2. IBM Data Privacy Passports
3. IBM Z Fibre Channel アダプター
4. IBM DS8900F Storage
5. IBM Z Fibre Channel Endpoint Security
6. IBM Hyper Protect Virtual Servers
7. TLS または IPSec
8. 任意のパブリックおよび/またはプライベートクラウド
9. IBM Data Privacy for Diagnostics (Vendors and Suppliers)
10. ハードウェア・セキュリティー・モジュール (HSM)
11. データの処理と保管のためのコモディティー・ハードウェア

ユース・ケース 1:IBM On-Premises ソリューション・ファミリーのデータ保護とプライバシー

大手小売業、大手銀行、クレジット・カード処理、その他大規模決済システムなどの多くの高要件環境では、IBM 処理インフラがすでに使用されており、z15 が基礎テクノロジーである可能性が高くなります。z15 の中では、全方向型暗号化を有効化して、システム内で資格のあるデータとプロセスを保護することが可能です。対象データの保護とプライバシーは Data Privacy Passports の適切なポリシー統制を使用して、IBM z15 環境から、企業内の他の環境に拡張できます。[1] Passport Controller for IBM Data Privacy Passports をインストールして、JDBC 接続を通してアクセスできるデータ・ソースからの資格のあるデータの資格と資格検証を管理し維持することができます。全方向型暗号化を使って対象となるボックス上のデータを保護することにより、システム内外を移動する必要があるデータの保護に集中できます。

ポリシーが有効化されたら、保護を受けるためにデータが IBM Z 上にある必要はありません。ポリシーに関連するデータはホスト・ストレージの外に出る前に暗号化されます。完全な IBM エコシステム内で動作する場合、超高スループットの IBM Fibre Channel アダプターとスイッチを使用してデータをデータセンター内を高速で移動できます。これは、他の Fibre Channel 仲介システムとも互換性がありますが、IBM DS8900F ストレージで使用された場合、移動中のデータをハードウェア・レベルで保護する IBM Fibre Channel Endpoint Security を追加することによって、保護を強化できます。Fibre Channel と DS8900F を組み合わせることにより、移動中のデータの暗号化と認証も追加されます。

1 免責事項: Data Privacy Passports は、JDBC 接続経由でアクセスできるデータ・ソースをサポートします。

ユース・ケース 2: 異機種環境のエンタープライズ・データセンターにおけるデータ保護とプライバシー

他のコンピューティング・プラットフォームがすでに展開されている組織の大部分は、現在のコンピューティング・インフラを破壊して交換することは現実的でありません。Data Privacy Passports は、このようなデータセンターのネットワーク接続されたハードウェアに仮想的に常駐し重要な機密データを強力に保護します。一度 IBM z15 に接続されると、対象データの保護はデータが存在する限り、データセンターのどこにでも適用できます。z15 は、FIPS 140-2 level 4 認定の暗号法 HSM を使用したセキュリティー用に設計されています。また、1 日当たり 190 億を超えるの暗号化されたトランザクションを処理できる速度と能力を備えています。[2]

ユース・ケース 3: あらゆるクラウドと 共有データにわたるデータ保護とプライバシー

IBM z15 with Linux on Z は、セキュアなプライベート・クラウド・インフラストラクチャーの構築 IBM Hyper Protect Virtual Servers を提供します。Hyper Protect Virtual Servers ワークロードを使用することにより、所有者はワークロードとデータに対する完全な制御を維持できます。データ所有者が許可しない限り、システム管理者やクラウド管理者でもワークロードにアクセスできません。Data Privacy Passports は、ポリシーを施行する Passport Controller にクラウドがアクセスできる限り、広範囲に分散されたハイパーコンバージド、マルチクラウド環境でも資格のあるデータに適用できます。インターネット・ビューから隠す必要がある通信エンドポイントでは、TLS トンネルをインターネット・ゲートウェイに追加してトランスポート・セキュリティーを強化できます。

データ制御を実装すれば、データ所有者は企業全体で誰とでもデータを共有できます。企業内のどんなビジネス・ニーズ、データ・アクセス、配布、使用期間でも、ポリシー・マネージャーによって完全に管理できます。データの所有者は、ニーズが変わってもポリシーをニーズに合わせて簡単に変更できるため安心できます。ニーズが必要なくなっても、保護とプライバシーのいずれにも変更を加える必要はありません。Data Privacy Passports を使用してポリシー・マネージャーを通してローカル・キーを破壊することによって、企業内のあらゆる場所にある適格なデータを無効化できます。

ユース・ケース 4: シャドー IT の影響を最小限化

シャドー IT は、組織内の誰かが、許可されていない場所にデータを移動またはコピーすると発生します。許可なくデータを移動またはコピーすると、セキュリティーの抜け穴につながり、ビジネス・リスクが増大します。データ漏洩やデータの露出が発生すると、それが意図的でなくも、重大な風評や財務上の影響が発生します。すべての重要な、あるいは構造化された機密データに Data Privacy Passports を実装することで、シャドー IT の影響を最小限化できます。データがコピー、または移動されても、許可がないと使用できなくなります。l制御されたデータベースにアクセスする権限はあるが、データ・アクセス権限を持っていないユーザーが許可されていない場所にデータを移動しても、データは暗号化されたままで、会社の露出が最小限に抑えられます。

2 免責事項: このトランザクション速度は、データセット暗号化と CF 暗号化を有効化した、8-way LPAR 2 台と 4-way ICF 1 台で構成される z15 構成の社内測定値を基にしています。この結果を基に、標準の LSPR MIPS を使用した、フルサイズの z15 トランザクション速度を予想しました。ユーザーが体験する実際のパフォーマンスは異なる場合があります。

まとめ: あらゆる場所での暗号化によるライフサイクル全体を通したデータの保護

データの機密性を維持することにより、所有者にビジネスおよび運営上の優位性が提供されます。この事実があるにもかかわらず、ほぼすべての組織がデータの保護に暗号化を十分活用しておらず、多くの企業は悪意のある脅威アクターや個人の不注意の犠牲になります。

組織内でデータ保護に関する第一の問題は、最も一般的なツールでは、異なる状態のデータを保護するために、異なるインターフェースと個別のポリシーが必要になることです。ツールと管理インターフェースが緊密に統合されていないため、独立して動作します。独立しているためにポリシーや施行の一貫性と検証が難しくなり、多くの場合、防御の抜け穴ができます。

共同作業環境では、ユーザー摩擦とデータ制御の維持は、最も困難な 2 つの側面です。ユーザー摩擦が増加すると従来の暗号化プラットフォームをユーザーが敬遠します。ポリシー統制と現場のデータへの施行に柔軟性がないと、データ所有者や保護者が保護を展開しづらくなります。

各ライフサイクル段階でデータを保護するテクノロジーは一般的ですが、そのライフサイクル全体を通した定期的な変更データ体験から、データ暗号化管理の特定の側面が難しくなります。企業は、このような障害を乗り越えて、移動中、処理中、保管中の機密データすべてを保護するためのビジネス要件を規定する必要があります。コスト・ベネフィット分析を必ず行う必要がありますが、現実的なアセスメントでは、機密データに対する暗号化の使用を拡張することが有利であると結果が出る場合がほとんどです。

これは容易ではなく、暗号化されたデータの保管に移行するには、数年かかることもあります。データの量は 1 つの要素ではありますが、最も影響が大きいものではありません。調整が最も難しい要件は、データ・タイプや場所の多様性、ユーザーおよびアプリケーションの資格、データ更新と共有のためのアプリケーション・インターフェースの目録化と定義です。レガシー・アプリケーションでは暗号化の実行にアップグレードや交換が必要ですが、データが真のビジネスまたは運用上の優位性を提供する場合は、それを維持する価値があると同時に保護する価値もあります。

機密性が高いデータ、またはトランザクション量が多いシステムのある組織では、IBM z15 with z/OS または Linux on Z を実行して全方位型の暗号化と Data Privacy Passports を導入することが推奨されます。IBM z15 エコシステムは、社内アプリケーションに対し比類のないパフォーマンスを提供し、あらゆる種類のクラウド環境の基礎となります。そのネイティブ・セキュリティー・アーキテクチャーには、内蔵型暗号化アクセラレーター・チップ、埋め込みハードウェアセキュリティ・セキュリティー・モジュール・チップおよびサービス、暗号化鍵作成およびライフサイクル管理サービス、暗号化 multi-Gbpsインターフェース、暗号化互換の高速ストレージが含まれています。このプラットフォームは、あらゆる暗号化要件にも対応する永続的なデータ機密性、ポリシー管理、および施行を提供します。現在、これ以上包括的で高性能の大量生産システムはありません。

どのソリューションを選択したかにかかわらず、あらゆる場所で暗号化戦略を実装することで、プライバシーとコンプライアンス関連の違反にかかるコストを大幅に削減できます。データ所有者または保護者が、データが漏洩、窃盗、または他の方法で侵害されたことの証明を十分に提供できれば、通知、フォレンジック、被害者修復、罰金が大幅に減額、場合によっては免除される可能性があります。ブランドに対する悪影響も大幅に低減、あるいは回避できます。これらの要素を低減することで、最終的な利益認識を低減できます。

全方向型暗号化機能を持つ IBM z15 や Data Privacy Passports を使用した IBM アプローチによる包括的なデータ暗号化エコシステムがお客様の組織にどのように利益をもたらすかの詳細については以下をご覧ください。https://www.ibm.com/it-infrastructure/z/capabilities/enterprise-security

Enterprise Management Associates, Inc. について

1996 年に創立された Enterprise Management Associates® (EMA) は、幅広い種類の IT およびデータ管理テクノロジーにわたって豊富な知見を提供する大手産業アナリスト企業です。EMA のアナリストは、実践的な経験と業界のベストプラクティスに対する知見と、EMA の顧客が目標を達成するための現在および未来のベンダー・ソリューションを独自の方法で組み合わせて活用します。EMA がエンタープライズ・ビジネス・ユーザー、IT プロフェッショナルおよび IT ベンダーに提供している、調査、分析およびコンサルティング・サービスの詳細については、以下をご覧ください。
www.enterprisemanagement.com または blog.enterprisemanagement.com. EMA の Twitter, Facebook、または LinkedInをフォローすることもできます。

本社:
1995 North 57th Court, Suite 120
Boulder, CO 80301
電話: +1 303.543.9500
www.enterprisemanagement.com

3933.03022020-06032020.revision9