IBM Software
Smarter Commerce

ファイルベースのデータ移動に関する、セキュリティーのベスト・プラクティス – IT プラクティショナーズ・ガイド

Rod Gifford, IBM Managed File Transfer - Market Segment Manager

IBM

要旨

ファイルベースのデータ移動のデータ・セキュリティーが、ようやくそれに見合った注目を集めるようになりました。非セキュアなファイル移動に関する責任やリスクは、かつては金融サービス業界でのみ懸念されていたことですが、今やあらゆる業界でそれらに目が向けられるようになり、重要なこととして扱われるようになっています。

ただし、このように関心が高まっていても、企業が適切にリスクを軽減できているというわけではありません。Privacy Rights Clearinghouse のレポート **「The Top Half Dozen Most Significant Data Breaches in 2011」**では、以下のように説明されています。「史上最大級のデータ漏洩が何件も報告された 2011 年は、データ・セキュリティーにとって意義深い年でした。2011 年に入ってから現在までに、既に 3,040 万件の機密レコードに影響する、 535 件のデータ漏洩が把握されています。」[1] また、これ以外にも、報告されていないデータ漏洩があった可能性もあります。

多数の企業が、どのようなときも (フライト中であれ、休息中であれ) データの保護が必要であることを既に認識していますが、多くの場合、特定の問題があると懸念される箇所に対する、適用範囲の狭いソリューションに焦点が絞られています。しかし、ファイルベースのデータ移動は、もはや、2点間やシステム間のファイル移動という単純なものではありません。インターネット、クラウド・ベースのファイル転送サービス、個別のファイル転送やアドホック・ファイル転送のさまざまな活用と、40 年の歴史を持つファイル転送プロトコル (FTP) への依存により、ファイルの移動が複雑になり、企業は組み込みデータを保護するのが難しくなってきています。

IBM Smarter Commerce アプローチによるデータ・セキュリティーのサポート

IBM® Smarter Commerce アプローチは、ビジネスの中心にお客様を戻します。また、お客様はかつてないほどパワフルに、ネットワークに接続し、データにアクセスするようになっています。モバイル機器を保有し、ソーシャル・ネットワークによってつながり、大容量データにほんの数秒でアクセスしてそれを送信できます。こうしたお客様の間では、情報共有におけるセキュリティーやプライバシーに対する要求が高まっています。しかしながら、企業のバリュー・チェーン全体で交換されるデータが増えるにつれて、ネットワークに対するリスクとデータ漏えいの危険性が増しています。

ファイル転送アクティビティーを管理し、監視しようとしている企業には、IBM Smarter Commerce アプローチに基づくベスト・プラクティスの採用を検討されることをお薦めします。目下のセキュリティーにおける課題は、内部およびインターネットベースのファイル転送に集中しているように見えますが、企業には現在、インターネットやクラウド・ベース・サービスによるファイル転送、内部や外部での 2 点間におけるファイル転送やユーザー開始ファイル転送など、すべてのファイルベースの転送を管理するためのベスト・プラクティスを確立する、大きな機会が存在しています。

このホワイト・ペーパーでは、企業がシステム周辺のセキュリティー、認証、そしてセキュリティー・ポリシーの適切な構成と実装を使用して、自社のデータを保護するために役立つベスト・プラクティスを提供します。また、クラウド・ベースのファイル転送サービスや、ユーザー主導型転送 (アドホック転送) を使用するためのガイドラインも提供します。大半の企業では、十分な管理機能やデータ保護機能が実装されていないため、アドホック転送は特に重要となってきています。

データ・セキュリティーの全体像変更によるリスクの軽減

ファイルベースのデータ移動を保護することは、多くの理由から、企業にとって重要です。国の法規定や業界の規制に準拠したセキュリティー・ポリシーを適時実装し、また更新できるようにすることは、ファイルベースのデータ移動のセキュリティーにおけるベスト・プラクティスを採用する、最も説得力のある理由の 1 つです。しかし、監査要件、ブランド保全、パートナーの要求、リスク軽減など、他の要因も企業にとっては同様に重要です。

実際、法律や財務に関するリスクは、極めて大きくなることがあります。Privacy Rights Clearinghouse レポートでは、TRICARE の 510 万人の患者の社会保障番号 (SSN) を漏えいした 2011 年 9 月のデータ漏洩を取り上げています。このデータ漏洩では、49 億ドルの訴訟が起こされました。[2] この一件は、データ漏洩に伴う潜在的な責任と、お客様への影響を明確に示しています。また、Ponemon Institute によって実施された 2010 Annual Study: U.S. Cost of a Data Breachの調査では、米国におけるデータ漏洩に対するセキュリティー対策の平均コストは、 1 件あたり 720 万ドルであることが明らかになりました。[3]

残念ながら、データ保護対策の実装について、積極的な取り組みを行っていない企業が多くあります。そのような企業は、業界のベスト・プラクティスではなく、個人の経験や勘を活用して個別の問題に対応しています。Ponemon Institute のBest Practices in Data Protection の調査に回答した企業は、データ・セキュリティーにおけるベスト・プラクティスのための戦略について、以下のように説明しています。[4]

- 回答企業の 19 % は、企業全体に展開された正式な戦略を保有している。
- 回答企業の 26 % は、部分的に実装された戦略を保有している。
- 回答企業の 30 % は、略式の戦略を保有している。
- 回答企業の 25 % は、データ保護戦略を保有していない。

驚くべきことに、回答企業の 55 % が、データ移動のセキュリティーを管理するための正式な戦略を保有していません。このような状況で、コストがかさむセキュリティー違反によるデータ漏洩が 2011 年に多発したことは、果たして驚くべきことでしょうか。お客様がパワフルにデータにアクセスするこの時代に、このようなレベルのリスクを喜んで受け入れる人はどれだけいるでしょうか。

企業は、自己防衛のために、信頼性の高いネットワーク区画や企業のデータを、どのようなときも (フライト中であれ休息中であれ) 保護する必要があります。また、企業内でも、パートナーとのデータ交換中もデータを保護する必要があります。さらに、セキュリティー・ポリシーやベスト・プラクティスをサポートする、集中化されたセキュリティー管理が必要です。また、企業は規制や所有権の問題も考慮する必要があります。ファイルの転送や保管時には、国内および国際的な規制を理解するのと同時に、データの所有者は誰か、データの所在はどこか、データにアクセスできるのは誰か、暗号化の必要はあるかを把握することも重要です。

企業がファイルベースのデータ移動のベスト・プラクティスの採用を検討する場合、ニュースで取り上げられた新たな規制や、連続的に発生するデータ漏洩が、行動を起こす大きな動機となります。しかし、企業のバリュー・チェーン・コミュニティーにとって、これらのベスト・プラクティスが重要かどうかについては、十分に考慮されません。企業は、お客様中心の考え方を進め、これらのベスト・プラクティスを、新規のお客様を獲得するための競争上の差別化要因として使用すると同時に、バリュー・チェーン全体で共有されるデータを保護するためのガイドとして使用することをお薦めします。

はじめに

基本的な考慮すべき事項

ガバナンスおよびリスクのベスト・プラクティスを検討する場合の最初のステップは、企業がデータを安全に移動させるために従わなければならない、法規定や規制を特定することです。

お客様の企業や業界に適用される規制はどれですか。取引パートナーとの関係に適用される規制はどれですか。規制には以下のようなものがあります。

- サーベンス・オックスレー法 (SOX)
- グラム・リーチ・ブライリー法 (GLBA)
- 連邦金融機関検査委員会 (FFIEC)
- 医療保険の相互運用性と説明責任に関する法律 (HIPAA)
- EU データ保護指令
- 個人情報保護および電子文書法 (PIPEDA)
- PCI データ・セキュリティー基準 (PCI DSS)
- 自動車デジタル・サプライ・チェーン向けの ODETTE

適用される法規定や規制を特定したら、各要件の順守による効果を測定するスコアカードを作成します。次に、順守されていない範囲 (ギャップ) を特定し、お客様の企業が完全に順守できるようにするための取り組みを優先順位付けします。

お客様のファイル転送アクティビティーの背後にあるビジネス推進要因や、内部およびバリュー・チェーン・コミュニティー全体の両方で使用する、基本テクノロジーを検討します。このような全体像を把握することは、より多くの商取引をインターネットに移行する場合には、特に重要です。データを転送する目的と方法を明確に把握することは、お客様が直面するデータとネットワーク・セキュリティーに関するさまざまな問題を認識し、適切なベスト・プラクティスを適用できるようにするのに役立ちます。

企業について考慮する必要もあります。多くの場合、データ・セキュリティーの責任は、シニア IT マネージャーまたはシニア業務 (LOB) リーダーが負います。さらに、連携してデータ・セキュリティー・ポリシーを提言し、ベスト・プラクティスの順守を監視する、 IT や LOB の担当者からなる部門間協力チームを設置している企業も多数あります。

使用事例に関する資料

お客様のバリュー・チェーンを成功させたり、各パートナーのデータ・セキュリティー要件を順守したりするために重要な、ファイル転送の使用事例を特定することから始めます。以下の表に、特定レベルのデータ・セキュリティーを必要とする、標準的なファイル転送の使用事例を示します。

業界	導入事例
金融サービス	• 銀行間の Automated Clearing House (ACH) 取引の実施 • 金融機関間のクレジット・カード取引の実施
小売	• 店舗から本社への、日次の売上情報のアップロード • 金融機関間のクレジット・カード取引の清算
製造	• 工場、サプライヤー、および下請けメーカーに対する分散生産計画の更新 • 第三者業者への、給与計算データの送信
流通	• お客様、サプライヤー、および第三者物流会社との、注文、出荷、受領、および在庫の状況の交換
保険	• 州の機関や医療サービス提供機関との保険契約者情報の交換
公益/情報通信およびメディア	• パートナー・チャネルからの発注情報の取り込み

表 1:業界別のファイル転送の例

ファイルベースのデータ移動のユース・ケースを文書に記録する場合には、以下の問いに対する答えを明確にする必要があります。

- どのデータを移動させますか。データを、どこに、どのように移動させますか。
- データの機密性またはリスク・レベルは、どの程度まで高める必要がありますか。
- データが時間通りに送信されない場合、それによるビジネス・プロセスの中断によって、どのような影響がありますか (サービス・レベル・アグリーメント [SLA] が関連する場合も、しない場合もあります)。
- データが配信されない場合、財務的にはどのような影響がありますか。

業界のベスト・プラクティスの基盤

このセクションでは、データ保護、システム周辺のセキュリティー、認証、セキュリティー・ポリシーの構成と実装、クラウド・ベースのファイル転送サービスの使用、およびユーザー主導型転送 (アドホック転送) 向けの特定のベスト・プラクティスについて、そのリストを示します。

データ保護

- データ移動の操作を行う国や、データが通過する国の、プライバシー・ポリシーを把握します。
- 操作を行う国の外に移動可能なデータのタイプと、操作を行うユーザーを管理するポリシーを設定します。
- お客様が操作を行う国の国境から離れた後に、データが物理的に存在する場所を文書に記録する手段を確立します。
- DMZ (非武装地帯) にデータが書き込まれたり保管されたりしないようにします。
- 組織によりデータ保全性の確保を管理します。
- 連邦情報処理標準 (FIPS) の規制の順守を含む、強力な暗号化オプションを採用します。
- Secure Sockets Layer (SSL) および Transport Layer Security (TLS) プロトコルをサポートします。
- ハードウェア・セキュリティー・モジュール (HSM) と連動させて暗号鍵を保管し、保護機能を高めます。

システム周辺のセキュリティー
- DMZ ベースのプロキシーを使用します。
- SSL セッション・ブレークによって DMZ 内の受信した通信セッションを終了することにより、インターネットと保護された内部のサーバーとの直接接続を防止します。
- パートナー・ユーザーが適切に認証された後にのみ、DMZ から信頼性の高いネットワーク区画へのセッションを確立します。
- データ、ファイル、またはユーザー資格情報を 、DMZ に保管することはできません。
- ファイアウォール内では、 着信保留を要求できません。
- DMZ 内では Web サービスやユーザー・インターフェース (UI) ポートを、オープンのままにすることはできません。
- データの検索は、信頼度の高いゾーンから低いゾーンの順に行います。
- 単一のトンネルを使用して、多重化セッションを実行します。
- プロトコル検査、コマンドのフィルター処理、および共通 URL 利用の妨害により、悪質な攻撃から保護します。

認証
- 信頼性の高いネットワーク区画ではなく、 DMZ 内でユーザーを認証します。
- Microsoft Active Directory データベースなどの外部のユーザー・リポジトリーで、ユーザーを集中管理します。
- 多要素認証を使用して、「知識 (something you know) 」および「所有物 (something you have)」の要件を備えたユーザーであることを確認します。
- ログオン・ポータルを使用して、シングル・サインオンを行います。
- ユーザー・パスワード管理のためのセルフサービス・ツールを備えたログオン・ポータルを採用して、ヘルプ・デスクのサポート・コストを削減します。
- 役割ベースのアクセス権限を提供します。

構成と実装
- DMZ フットプリントを最小化するアーキテクチャーを導入します。
- セキュリティー・チームとネットワーク・インフラストラクチャー・チームの、両方のニーズに対応します。
- クラスタリングおよびロード・バランサー用オプションにより、運用の継続性と高可用性を提供します。
- 追加コンポーネントを購入することなく、セキュリティーとネットワークの要件の変更に合わせて、構成を変更する機能をサポートします。
- 高まるファイル転送のニーズをサポートする、スケーラビリティーを提供します。
- SSL を使用して、トラステッド・ゾーン内のソリューション・コンポーネントと内部サーバーの間の接続を保護します。
- 多層 DMZ のための導入オプションを活用します。
- 監査、コンプライアンス、トラブルシューティングの目的で、ロギングを使用してセッション・アクティビティーやイベントをリアルタイムで追跡します。

クラウド・ベースのファイル転送サービス・プロバイダー
- 第三者のサービスを通るファイル転送アクティビティーのパフォーマンス監視を支援する SLA を定義します。
- 第三者業者が自社のセキュリティー管理を維持できるようにします。
- ベンダーのデータセンターを利用できるユーザーを把握することにより、データ・プライバシーをサポートします。

- 退職した従業員のアクセス資格情報を、即座に無効にします。
- 監査員のオンサイト監査を積極的に受けます。
- お客様のポリシーによって承認される国にのみ、データが存在するようにします。
- 国際送信が許容される実際の例や、データ・タイプの概要を示します。
- 他のお客様が企業のデータにアクセスできないようにする、アーキテクチャーを備える必要があります。
- セキュリティー・パッチを当てて、常にアーキテクチャーを最新の状態に保つようにします。
- 退職時のデータの削除と返却の明確な方法を示します。

ユーザー主導型転送 (アドホック転送)

- e メールへの添付やサムドライブへのコピーが可能なデータの種類や機密レベルについて、明確なポリシーを設定します。
- データ損失防止のテクノロジーを導入し、機密データが企業から流出する前に阻止します。例えば、e メールの添付文書や FTP ファイルに含まれる SSN、クレジット・カード番号のスキャンなどです。

ファイル転送パターンとセキュリティー・リスク

以下の表に、代表的なファイル転送パターンと、転送されるデータに対する潜在的なリスクを示します。以下に示す 2 点間の パターンは、最新のものではありません。ただし、ファイル転送でのクラウド・ベース・サービスの利用は最近の動向であり、その利用によって、あらゆる企業が考慮すべき、新しい一連のリスクが生み出されています。

ファイル転送パターン	説明および使用するテクノロジー	データ・セキュリティーのリスク
Point-to-Point (アプリケーション間)	• アプリケーションが転送を開始 • サーバーベースのアプリケーションが、ファイルを送受信	• 通常、セキュリティー・リスクが内在する FTP を使用する • ファイルが暗号化されないため、ファイルへのアクセス権限を持つユーザーは、誰でも内容を見ることができる
Point-to-point (クラウド・ベース)	• アプリケーションが転送を開始 • クラウド・サービス・プロバイダーがデータ転送を支援	• プロバイダーのテクノロジーは管理できない • データ・セキュリティーの提供は、プロバイダーに依存 • データの物理的な保管場所や、データにアクセス権限を与えるユーザーを管理できない
企業間	• ファイルは、インターネットを介して取引パートナーと交換される • プロセスは、メールボックスまたはサーバーベースのファイル・ディレクトリーに依存して、ファイルの送受信を行う	• データや内部ネットワークが、セキュリティー・リスクにさらされる • 通常、セキュリティー・リスクが内在する FTP を使用する • ファイルが暗号化されないため、ファイルへのアクセス権限を持つユーザーは誰でも内容を見ることができる • ファイアウォール内で発生する基本的な認証 (ログイン、パスワード) のみをサポートする • お客様のペリメーター・サーバーに直接接続されたセッションを含む
ユーザー主導 (アドホック)	• 個人がユーザー、e メール・アドレス、またはサーバーベースのファイル・ディレクトリーに対して、ファイル転送を開始する • プロセスには、e メール添付文書、FTP スクリプト、およびサムドライブが含まれる	• ネットワーク・セキュリティー管理は行われず、内部および外部で機密データを移動できる • ファイルは暗号化されないため、ファイルへのアクセス権限を持つユーザーは誰でも内容を見ることができる

表 2: ファイル転送パターンおよびセキュリティー・リスク

ベスト・プラクティスの実装

ベスト・プラクティスを確立したら、その展開計画を作る必要があります。以前に特定したコンプライアンスとのギャップから、重要度や必要な労力に従って、それらを優先順位付けします。

パスワードや内部情報共有を管理するプロジェクトなど、重要なセキュリティー・ポリシーの実装が容易なだけでなく、企業全体でそのポリシーの認識や実施が促進されそうなプロジェクトを最初に選択します。これらの最初のプロジェクトは、あまり時間がかからず、コストがかからないものである必要があります。

ギャップと優先順位に基づいて他のプロジェクトを特定し、そこにソリューションを割り当てる場合は、技術的なソリューションと推奨されるソリューションをはっきりさせます。例えば、従業員がパートナー企業との情報交換でインターネットをより頻繁に使用する場合には、DMZ ベースのセキュリティー・ソリューションのニーズが高まり、プロジェクトはプロジェクト・リストの上位に配置されることになります。どのような場合も、予算見積もりを策定し、IT や LOB のスポンサーと連携して、資金やプロジェクト開始について承認を得る必要があります。

技術要件

技術はあらゆるセキュリティー・プロジェクトの重要な要素であり、それを実装する計画が必要になります。まず、計画のサポートに必要な技術を特定し、調達および実装のための予算を作成します。お客様の使用事例やデータ・セキュリティーの要件に従って、ポイントとなる多数のソリューションを利用できます。

セキュリティー・ソリューションを評価する場合、スケーラビリティー、パフォーマンス、およびサポートの要件を評価します。グローバルな運用では、大容量データに対応する強力なグローバル機能と十分なキャパシティーを保有し、サポートが十分期待できるベンダーが必要となります。また、ファイル移動戦略にセキュリティー機能を統合しなければならないことも考慮し、特定の問題を解決するためのポイントとなるソリューションが必要なのか、ファイル転送インフラストラクチャー全体に及ぶ広範な機能セットが必要なのかを判別します。このようにシステムの運用状態を把握することにより、単一のベンダーと契約するか、複数のベンダーを利用するかを決定できます。

先進的な考えを持つ多くの企業は広範な機能セットの適用を選択し、マルチベンダー戦略関連の潜在的に高い総所有コストを避けるために、単一ベンダーのアプローチを支持するようになります。実際に、Ponemon Institute のベスト・プラクティス調査に対する回答企業の 40 % が、単一ベンダーのソーシング・アプローチを選択する意向を示していました。[5]

教育と認識

ファイル転送セキュリティー・ポリシーの効果的な採用と実施のためには、教育を提供し、企業全体の認識を高めることが重要です。従業員は、なぜセキュリティーが重要なのかを理解し、セキュリティーが企業のブランドを守り、大切なお客様に最高の利益を提供することを理解する必要があります。セキュリティー違反によるデータ漏洩は、適切に対応しなかった場合は特に、お客様との関係に回復不可能な損傷を与え、企業の評判を落とすことになりかねません。データが気付かないうちにどのように漏えいするか、およびリスクを最小限に抑えてブランドとバリュー・チェーンの関係を保護するためにはどうすればよいか、これらに関して従業員を教育する計画を立てる必要があります。

従業員を教育する**方法** は、教育する内容と同様に重要です。コミュニケーション戦略やメッセージに細心の注意を払い、従業員の日常の責務に関連した内容となるように教材を調整します。教育計画には必ずテストを組み込み、各従業員が自社のデータ・セキュリティー・ポリシーを理解したことを検証するようにします。

多くの企業では、ベスト・プラクティスが完全に実装されるまで、毎月または四半期ごとにミーティングを持ち、その後は毎年、または規制の新設や更新などの状況の変化に応じてミーティングを持っています。先進的な考えを持つ企業のなかには、マネージド・ファイル転送の拠点を設立している企業もあります。拠点があることにより、戦略的かつ構成的なアプローチでファイル転送テクノロジーの合理化、導入、管理を行い、ファイル転送テクノロジーを広範な IT セキュリティー戦略に組み込むことができます。

セキュリティー監査

このホワイト・ペーパーに示すすべてのベスト・プラクティスが、お客様の企業に当てはまるわけではありません。そのため、監査員の支援を受けてお客様のセキュリティー・ニーズを評価することは重要です。監査員とのレビュー・セッションにより、実装すべき内部ポリシー、パスワードの管理方法、クラウド・ベース・サービスの監査を実施すべきかどうかとその頻度、および追跡すべき基準が明確になります。これらの基準は、ファイル転送のパフォーマンスを含み、SLA への順守を評価するものである必要があります。説明責任を果たすためには、特定の基準を管理職レベルのレビューと関連付けなければならない場合があります。これらの基準を使用して、セキュリティー・ギャップやリスク調整に焦点を合わせたプロジェクトの特定、優先順位付け、監視を行い、成功を確実にすることができます。

ビジネスの確信

ファイルベースのデータ移動におけるセキュリティーに関するベスト・プラクティスを実装する上で、最も重要な部分の 1 つは、投資対効果検討書の作成です。影響力のある検討書を作成するには、まず最初に、このタイプのセキュリティーの大きなニーズの概要を把握し、その後、お客様の企業に適用する特定の業務に焦点を絞ります。これらの業務が企業全体のデータ・セキュリティー計画とどのように関係するかを明確にして、その関連性を広げます (業務によってどのようにして監査要件を満たすかなど)。セキュリティー違反による情報漏洩によって、企業のブランドや財務にもたらされるであろう影響や、お客様のバリュー・チェーン・コミュニティーでの問題の重要性など、企業にとっての価値や利益が対象となるようにします。

必要に応じて、過去の損失を取り上げたり、または、お客様の業界で有害事象に見舞われた他の企業の事例について話し合ったりします。データ・セキュリティーのベスト・プラクティスは、取引パートナーとの競争優位性として使用することができるほか、法規定や業界規制の順守を促進し、内部または外部での機密データの移動を保護します。

他の企業でのベスト・プラクティス採用の推進要因について、インサイト (見識) を共有します。Ponemon Institute のベスト・プラクティスの調査によれば、企業がデータ・セキュリティーに対してベスト・プラクティス・アプローチを採用する主な理由は、以下の 3 つです。[6]

- 26 % - 内部ポリシー、手順、および契約を十分に順守するため
- 25 % - 規制、法規定、および公的基準を十分に順守するため
- 21 % - データ保護のベスト・プラクティスで業界をリードするため

このように、データ・セキュリティーに対してベスト・プラクティス・アプローチを採用する背景には、法令順守や業界リーダーシップへの欲求という推進要因があるようにみえます。最近の傾向は、さまざまな政府機関が継続的に新たな規制を強要している状況を裏付けています。英国の Information Commissioner's Office が発表した文書 **「Guidance on data security breach management」**は、企業がセキュリティー違反による情報漏洩への対応に備える際に役立ちます。[7] また、米国上院司法委員会は、最近3 つのセキュリティー法案を通過させました。これは「機密個人情報の侵害を個別に通知するための連邦基準」を要求するものです。[8]

データ・セキュリティーのベスト・プラクティスを企業に受け入れさせる、その最も効果的な方法は、エグゼクティブのスポンサーシップを獲得することです。2011 年の Ponemon Institute によるベスト・プラクティスの調査で、データ・セキュリティーのベスト・プラクティスを使用している企業と他の主な企業とが異なる点を調査したところ、エグゼクティブ・スポンサーシップが主要な要因として際立っていました。この調査では以下のように説明されています。「ベスト・プラクティスを採用している企業は、C レベル・マネジメントやシニア・マネジメントからのサポートや資金を適切に確保しています。なぜなら、彼らには情報資産の保護に対する大きな責任があり、また、企業の良好な評判を守りたいという思いがあるためです。」[9] ここで得られる教訓は、何でしょうか。それは、データ保護を積極的な視点で捉え、外部要因を待たずに行動するベスト・プラクティスを採用している企業は、適切に情報漏洩に対応し、新たなコンプライアンスを支持し、業界リーダーとしての立場を維持できるということです。

目標は、データ漏洩の新たな例を発生させないように努め、データ漏洩の影響から復旧するためにかかるであろう数百万ドルものコストを回避することです。ファイルベースのデータ移動のセキュリティー機能周辺にベスト・プラクティスを導入する企業は、ファイルベースのデータ移動における先端企業であるようにみえます。

IBM を選択する理由

実装したいと思うベスト・プラクティスの適切なガイドを入手したら、そのベスト・プラクティスを適切なテクノロジー・ソリューションと整合させる必要があります。ファイルベースのデータ移動では、これはマネージド・ファイル転送ソリューションに分類されます。技術要件を考慮するときには、単一ベンダーの製品に統合することによる、総所有コスト削減の機会を見逃さないでください。

IBM では、セキュリティーはビジネス・プロセス、開発、および日常業務に組み込まれるべきものと考えています。セキュリティーは、IT プラットフォームや重要なインフラストラクチャー・ソリューションの初期の設計に組み込む必要があり、後から追加するべきではありません。DMZ ベースのプロキシー・ソリューションの実装に IBM Sterling Secure Proxy を使用しているか、IBM Sterling Connect:Direct ソフトウェア (25 年以上使用されており、いまだに情報漏洩が発生していないセキュリティー機能を備えた業界標準の Point-to-Point ファイル転送プロトコル) を使用しているかに関わらず、企業は IBM のテクノロジーを使用して、データやネットワークのセキュリティーを確保することができます。

同時に、この、お客様がパワフルにネットワークに接続し、データにアクセスするような時代には、データ・セキュリティーがより強調され、取引パートナーはセキュリティー重視のアプローチを活用して、データや内部ネットワークを保護することが必要となります。お客様中心のアプローチにより、ファイルベースのセキュリティーのベスト・プラクティスを開発すると、企業はそのポリシーをバリュー・チェーン・プロセスと整合させることができるようになります。

IBM Smarter Commerce アプローチの一部であるバリュー・チェーンの同期では、強力な企業間統合機能が必要となります。これらの機能のうちの 1 つのコンポーネントが、マネージド・ファイル転送です。IBM のマネージド・ファイル転送ソリューションは、企業のビジネス・コミュニティー全体での同期を実現するだけでなく、ベスト・プラクティスの技術的な基盤を提供します。

IBM Business Value Assessment は、マネージド・ファイル転送テクノロジーの特定と導入について、経験に基づくアドバイスが必要な企業に対し、有益なオプションを提供します。
IBM とのコラボレーティブな関係として、IBM Business Value Assessment では、お客様の現行のファイル転送のインフラストラクチャーと運用を評価することができます。この評価では、お客様の拡大されたバリュー・チェーンや、同期の維持に必要なファイルベースのデータ移動全体が、十分に検討されます。IBM は適用可能なベスト・プラクティスを検討し、技術とプロセス、およびそれらの使用を可能にする IBM 製品とのよりよい組み合わせを支援します。

詳細情報

Business Value Assessment のセットアップについては、日本IBM の営業担当員にお問い合わせください。

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

IBM のホーム・ページは次の通りです。
ibm.com/jp/ja/

本資料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のではありません。

本資料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で提供され、第三者の権利の不侵害の保証、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。

お客様は自己の責任で、適用される法規定および規制を順守しなければならないものとします。IBM は法律上の助言を提供することはいたしません。また、IBM のサービスまたは製品が、お客様においていかなる法を順守していることの裏付けとなることを表明し、保証するものでもありません。

[1,2] Privacy Rights Clearinghouse, **The TopHalf Dozen Most Significant Data Breaches in 2011**, December 16, 2011, http://www.privacyrights.org/data-breach-year-review-2011

[3] Ponemon Institute, **2010 Annual Study: U.S. Cost of a Data Breach**, March 2011.

[4,5,6,9] Ponemon Institute, **Best Practices in Data Protection: Survey of U.S. IT & IT Security Practitioners**, October 2011, sponsored by McAfee, http://www.mcafee.com/us/resources/reports/rp-ponemon-data-protection-full.pdf

[7] Information Commissioner's Office, **Guidance on data security breach management**, July 2011, http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Practical_application/GUIDANCE_ON_DATA_SECURITY_BREACH_MANAGEMENT.ashx

[8] Harley Geiger, "Senate Judiciary Committee Passes Three Data Security Bills," Center for Democracy & Technology, September 23, 2011, https://www.cdt.org/blogs/harley-geiger/239senate-judiciary-committee-passes-three-data-security-bills

Please Recycle

ZZW03114-JPJA-00