ipswitch®

Secure. Control. Perform.

ファイル転送とGDPR

ipswitch

GDPRに備える

EUの一般データ保護規則（General Data Protection Regulation、GDPR）は、欧州議会と理事会で承認され、2018年5月25日から施行されます。GDPRは、データ保護のための極めて厳しい基準を定めており、EU住民の個人データを処理するか、処理をコントロールする組織に適用されます。GDPRに違反すると、最大の場合、2,000万ユーロまたは世界全体での年間売上高の4%のいずれか大きい方の額の罰金が課せられます。

GDPRは、規制が適用される組織を、管理者と処理者の2種類に分類しています。処理者とは、EU市民の個人情報を収集、処理、保管、送信する組織のことです。管理者は、個人情報の目的と処理手段を決定し指示する組織です。元のデータ収集者（この場合は管理者）の責任は、アウトソーシング業者またはビジネスパートナー（処理者）による実際のデータ処理に拡張されます。GDPRでは、データ収集者と処理者の両方がデータ保護を担当しており、両方がコンプライアンス違反の際の罰金を課されます。収集者/処理者の関係において、両当事者はデータ転送に関するコンプライアンスの取り組みを調整する必要があります。どちら側も、データ保護の管理、プロセス、および技術を見直し、必要に応じて改善する必要があります。当事者は、リスクに対して適切なセキュリティのレベルを要求するGDPR第32条に準拠した努力をする必要があります。

GDPR 第32条（1）
管理者および処理者は、リスクに対して適切なレベルのセキュリティを確保するための適切な技術的および組織的措置を実施しなければならない。

GDPR 第32条（2）
個人データの不慮または不法な破壊、喪失、改ざん、無断開示・アクセスに繋がる保護安全性の侵害は、一定の場合に監督機関およびデータ主体に通知しなければならない。

ipswitch

ファイル転送はリスクが高い処理

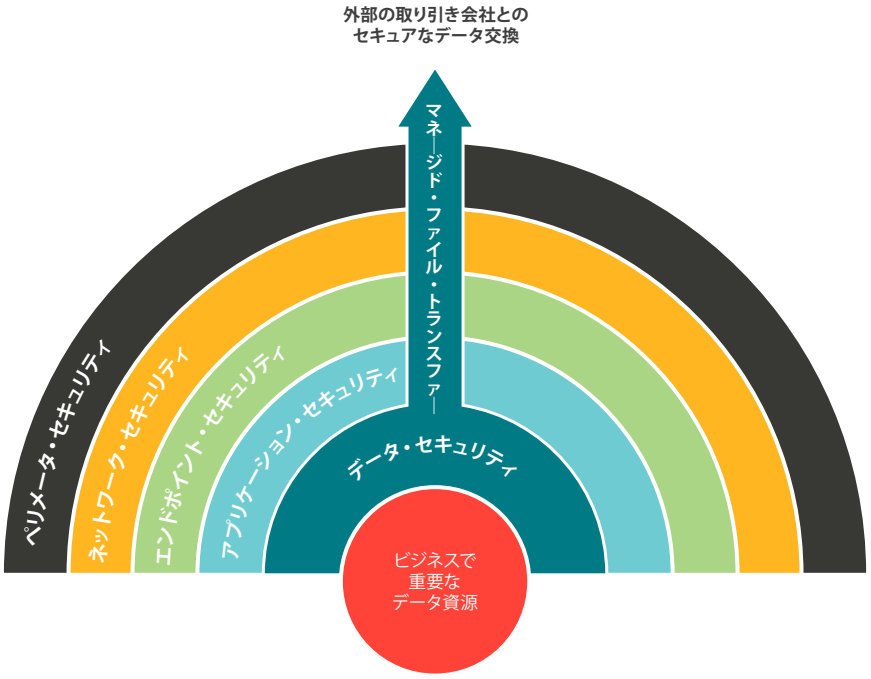
多くの会社が、すでにセキュリティ対策のためにかなりの予算を投入しているでしょう。GDPRによって、これまでのセキュリティ対策に加えて、社員への教育やこれまであまり考慮していなかった新しいプロセスや技術への予算投入も考えざるを得なくなってきます。

個人データの外部転送は、現在、様々な業種で中核的な業務プロセスになっています。セキュリティの観点からは、ファイル転送中のデータは、転送中の傍受、転送サーバー上でのダウンロードのための格納時の不正アクセス、意図しない受信者への配送、またはその宛先で処理されたときの取り扱いミスの可能性があるので、高いリスクにさらされていると言えます。

個人データを外部にファイル転送する場合、GDPRに違反しないよう注意深く準備する必要があるのは明らかです。IT部門は、限られた時間とリソースを効果的に配分し

GDPR 第4条（2）

「処理」とは、収集、記録、編成、構造化、保管、...<中略>...などの、送信、配布または他の方法で行われる...<中略>...個人データまたは個人データのセットに対して実行される操作または一連の操作を意味する。



つつ、機密性の高い個人データをリスクにさらす可能性のある操作に関して、GDPRコンプライアンスを徹底する方策を講ずる必要があります。

GDPRで、データ転送が処理アクティビティとして明示的に特定されているのには、明確な理由があります。データ転送アクティビティは、個人データを高いリスクにさらす可能性があるからです。

ipswitch

データ転送は、以下のような点で高いリスクがあります。

- FTPにアップロードされたファイルに保存された個人データは暗号化されず、たいてい削除されません。
- FTP匿名モード、古くなったセキュリティパッチ、その他の脆弱性により、サイバー犯罪者に簡単にアクセスできます。
- ユーザーが、電子メールやクラウドベースのファイル共有サービスなどのセキュリティ保護されていない手段でITを迂回し、個人データを送信する可能性があります。
- アクセス権限をしっかり管理できないと、ユーザーのクレデンシャルが公開される危険があり、ハッカーがそれを使って保護されたデータをコントロールできてしまいます。
- 集中管理された不正開封防止監査ログがないと、許可されていない、または失敗した転送が見過ごされてしまうリスクが生じます。

GDPR データ保護の原則

GDPRには、組織が準拠しなければならないデータ保護の原則が記載されています。これらの原則の多くは、個人データ転送活動に適用されます。

GDPR原則	関連前文/条項	必要な事項
正当で、規則に準じた、明確なプロセス	前文第22項、第5条(1)(a)	アクティビティ処理を設計し、実装する際に、より行き届いた注意が必要。
データ・セキュリティ	前文第29, 71, 156項 第5条(1)(f), 第24条(1), 第25条(1), (2), 第28, 29, 32条	個人データが組織内・組織外での処理、偶発的な損失、破壊、損害に対して安全であることを保証する。
正確性	前文第39項、第5条(1)(d)	個人データが正確であることを確認するための合理的な措置を講ずる。
説明責任	前文第85項、第5条(2)	データ保護原則を遵守していることを明示する。
目的の限定	前文第50項、第5条(1)(b)	1つの目的のために収集された個人データは、新しい互換性のない目的のためには使用しない。
必要な最小限データ	前文第39項、第5条(1)(c)	目的を達成するために必要な個人データ処理のみを行う。
保持期間	前文第39項、第5条(1)(e)	個人データは、使用目的に必要な期間以上に長く保持しない。

ipswitch

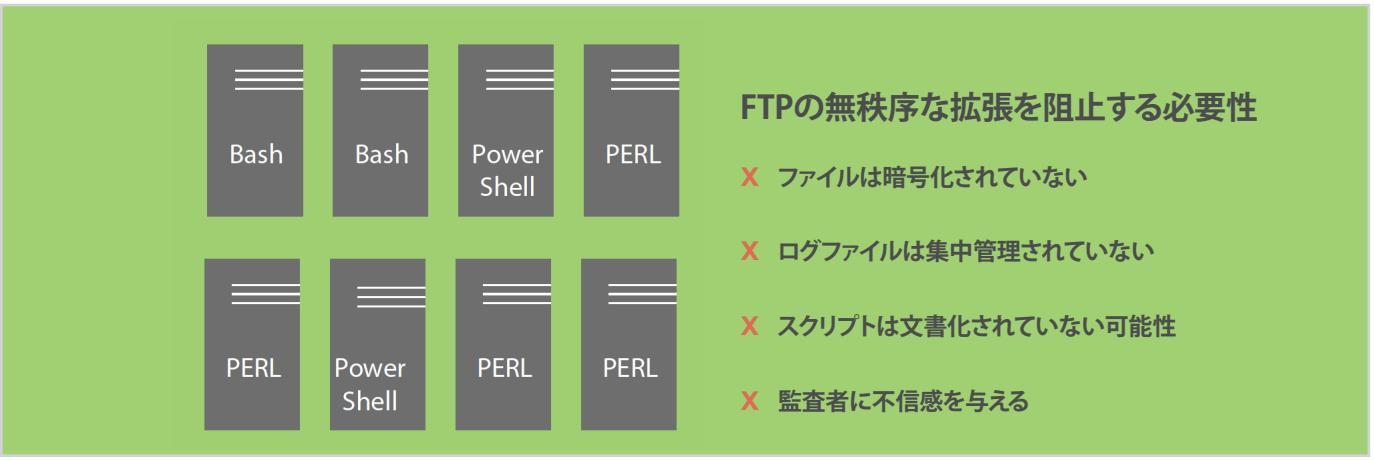
セキュアなFTPサーバーでは遵守困難

既存のFTP環境をGDPRコンプライアントにアップグレードしようとするのは得策ではありません。すべての外部転送プロセスで、セキュアなプロトコル（SFTP、FTPS、HTTPS）と暗号化（SSH、TLS、SSL）を使用する必要があります。データを保護するために、すべてのアップロードプロセスにAES-256暗号化を追加する必要があります。それでもまだ十分ではありません。セキュアなFTPは、FTPサーバーを置き換えるときに、多くのリスクと脆弱性を継承します。

様々なソフトウェア、異なるプラットフォーム、異なるソフトウェア・リビジョン、OSのリビジョン、セキュリティパッチを持つFTPサーバーの混乱で、FTPが無秩序に拡張してしまうかもしれません。そうなると統制がきかなくなり、サイバー犯罪者が個人データにアクセスできてしまう脆弱性が生じます。

	セキュアなFTP								スクリプト			
	転送中のデータ保護	保存中のデータ保護	ファイル整合性チェック	否認防止	常時スキャン	ゲートウェイ・サーバー	アドホック・ファイル転送	詳細なアクセス管理	不正開封防止監査ログ	タスクベースのファイル転送	集中管理コントロール	リアルタイム警告	分析
データ・セキュリティ	✓		✓									✓	
目的の限定													
必要な最小限データ													
正確性													
保持期間													
説明責任	✓		✓										
正当で規則に準じた明確な処理	✓		✓										

FTPデータ転送は通常、スクリプトに依存しています。スクリプトは、PERL、BASH、VB、PowerShellなどの異なる言語で記述することができますが、多くの場合文書化されておらず、標準化は極めて困難です。これらを集中管理コントロールできなければ、複数のFTPサーバーにインストールされたスクリプトを使ったワークフローが原因で、個人データが不正に処理される可能性があります。



さらに、GDPRは、IT部門とセキュリティ部門にコンプライアンスの証拠を提出するよう要求します。複数のFTPサーバーから監査ログを収集しレポート作成するには時間がかかります。それがうまくいかなければ、統一された形式のログデータを単一ソースにまとめて、不正開封防止データベースに格納することを望ましく思う監査人からの評価は下がります。

これらの問題点への対策を練り、GDPR標準に準拠したデータ転送環境を構築するには、相当の時間と費用が必要です。そうすることが本当に正しい選択でしょうか？

MOVEit を導入するメリット

GDPRデータ保護原則: 正当で規則に準じた明確な処理、データ・セキュリティ、正確性

イプスイッチのMOVEitは、第5条、第24条、第25条、第28条、第32条および第39条に記載された特定の要件を満たすセキュリティ機能を提供します。

- 転送中および保存中の個人データの暗号化
- 許可された送信者と受信者の間でのみ個人データが転送されることを検証する否認防止
- データ損失防止およびアンチウィルス・ソリューションとの統合
- ブラウザとMicrosoft Outlookの統合により、デスクトップ・クライアントがIT認定の安全なデータ転送ソリューションを使用することを保証
- 暗号化されていない個人データをDMZ内に放置しないペリメータ・セキュリティ
- ユーザーのクレデンシャル、アクセス許可、個人データを保護する、集中管理された詳細なアクセスコントロール

MOVEitは、SFTP、FTPS、HTTPSなどの安全なデータ転送プロトコル、SSH、TLS、SSL暗号化プロトコルを使用して、転送中の個人データを保護します。また、AES-256暗号化を使用して保存中のデータを保護します。

MOVEitの否認防止機能は、個人データが承認された送信者と受信者の間でのみ転送されることを検証します。移動中のデータが盗まれたり改ざんされたりする攻撃に対する保護策です。自動ファイル整合性チェックにより、ファイルが改ざんされていないことが検証されます。これはGDPRの正確性の原則に対する追加的な保護手段です。

DLP（Data Loss Prevention）やアンチウィルス・ソフトウェアなどのソリューションと統合できるので、プロテクションはより強力になります。データの損失やマルウェアが検出されたときに、すべてのコンテンツ・スキャン・アクティビティを記録し、警告を送信します。

IpswitchのGatewayはDMZに置かれたプロキシサーバーで、個人データがDMZ内に保管されないようにします。パブリック・ネットワークからのインバウンド接続がDMZネットワーク内で終結し、ファイル転送タスクが多層のセキュリティ策によって保護されることを保証します。

デスクトップ・クライアントは、簡単に使えるAd Hoc機能を使って、安全にデータ転送することができます。大量のファイルをWebブラウザまたはMicrosoft Outlookから安全に送信できます。これにより、ユーザーがIT部門のコントロールが及ばないところで、セキュリティの点で問題があるクラウドベースのファイル共有ソリューションを使用し、機密データを公共にさらしてしまうリスクが減少します。

MOVEitには、ユーザーのクレデンシャルとアクセス許可を保護するための独自の安全なデータベースが組み込まれています。暗号化されたストレージとセキュリティ保護されたパーミッションの組み合わせで、ハッカーが既知の脆弱性を悪用できるOSのセキュリティに依存しません。

GDPRデータ保護原則: 説明責任

説明責任の原則は、組織にGDPRデータ保護原則の遵守を証明することを要求しています。組織は、個人データを含むすべてのデータ転送活動の監査証跡を収集し、保護する必要があります。MOVEitは、改ざんのないデータベースの認証やワークフローの変更を含む、すべてのファイル転送アクティビティを追跡します。

GDPRデータ保護原則: 目的の限定、必要な最小限データ、保持期間

目的の限定の原則は、個人データの処理を特定の目的のみに制限します。必要な最小限データの原則と保持期間の原則を遵守するには、目的に必要なデータのみを処理し、その後データを削除する必要があります。

MOVEitは、スクリプトを、より安全な標準化されたデータ転送タスクを提供するフォーム・ベースのソリューションに置き換えます。すべてのデータ転送アクティビティを集中管理してコントロールすることができます。組み込みのスケジューラによって、繰り返し行わなわれるデータ転送タスクをスケジュールできます。一定時間経過後の個人データ削除などの転送後処理も指定できます。包括的な分析機能によって、GDPRのデータ保護原則を継続的に遵守するために必要な転送アクティビティの詳細情報を得ることができます。

MOVEit でGDPRデータ保護原則を遵守

GDPRコンプライアンスのために、リスクが最も低く、コスト効率の高いオプションは、イプスイッチの MOVEitのようなマネージド・ファイル・トランスファー・ソリューションです。MOVEitは、統合された集中管理データ転送ソリューションです。セキュアなデータ転送に、集中管理されたワークフロー、アクセスコントロール、監査ログ収集を統合します。高可用性を保証するフェイルオーバーも利用可能です。MOVEit を利用することで、個人データ処理に伴うリスクが低減され、データ転送処理アクティビティの管理とサポートに要する時間とコストが削減できます。

	MOVEit TRANSFER								MOVEit AUTOMATION				
	転送中のデータ保護	保存中のデータ保護	ファイル整合性チェック	否認防止	常時スキャン	ゲートウェイ・サーバー	アドホック・ファイル転送	詳細なアクセス管理	不正開封防止監査ログ	タスクベースのファイル転送	集中管理コントロール	リアルタイム警告	分析
データ・セキュリティ	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
目的の限定									✓	✓	✓		✓
必要な最小限データ									✓	✓	✓		✓
正確性			✓	✓	✓				✓				
保持期間									✓	✓	✓		✓
説明責任	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
正当で規則に準じた明確な処理	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓

イプスイッチについて

イプスイッチは、複雑なIT問題をシンプルなソリューションで解決します。クラウド、仮想環境、ネットワーク環境での途切れないパフォーマンスでIT部門を支援します。ネットワーク、アプリケーション、サーバーを監視するために、そしてシステム、パートナー会社、顧客との間のファイル転送のために、世界中の多くのお客様から信頼を得ています。マサチューセッツ州の本社のほか、米国各地、ヨーロッパ、アジア、中南米に拠点があります。詳しくはホームページ、https://jp.ipswitch.com/ をご覧ください。

GDPR準備のために MOVEit の導入をご検討ください

ipswitch

30日間の無料試用版をお試しいただけます:
jp.ipswitch.com/forms/free-trials/moveit-transfer