



Forcepoint Data Loss Prevention

境界線のない世界における
データ保護

Forcepoint

パンフレット

Forcepoint Data Loss Protection (DLP)

Data Security Everywhere: 従業員が働き、データが存在するすべての場所に

今日、あらゆる規模の組織がデータセキュリティ上の重大な課題に直面しています。個人を特定できる情報 (PII)、保護対象保健情報 (PHI)、その他の規制対象データなどの機密情報を保護するため関連規制を遵守しなければなりません。一方でクラウドアプリケーション、ハイブリッドワーク環境、BYODのトレンドなど、昨今のワークスタイルの変化にも対応しなければなりません。そうした環境ではデータが組織から流出する可能性が高まります。

今日、このように攻撃対象が拡大していることが、重要なデータを保護する上で最大の課題となっています。データセキュリティチームは組織に出入りするデータの急増に対処しなければなりません。それにはクラウド、ウェブ、オンプレミスのデータを包括的に可視化する必要があります。さらに、エンドポイント、ウェブトラフィック、ネットワーク、電子メール、クラウドアプリケーション、プライベートアプリケーションなどすべてのチャンネルを一元的に管理し、統制と監視を行うことが不可欠です。



Forcepoint DLPは、業界で最も信頼されているソリューションであり、エンドポイント、ネットワーク、クラウド、ウェブ、プライベートアプリケーション、電子メールといったすべての主要チャンネルのグローバルポリシーを簡単に管理できるツールを提供します。業界のDLPプロバイダーの中で最も多くの事前定義されたテンプレート、ポリシー、分類子を使用して作業を簡素化することができます。その結果、インシデント管理が大幅に効率化され、リスクが排除されて最も重要な作業に集中できるようになるため、従業員の生産性が向上します。Forcepoint DLPは、従業員が働き、データが存在するあらゆる場所を可視化し、コントロールすることでリスクに対処しています。

データ保護の必須条件:

- › **規制データの保護:** データ作成、保存、移動に使用するすべてのアプリケーションを一元的にコントロールします。
- › **機密データの保護:** 最新のDLPソリューションにより、ユーザーがデータをどのように使用するかを分析し、従業員がデータを使用して適切な決断を下せるよう指導し、リスク別インシデントに優先順位を付けます。
- › **生成AIの使用を保護:** エンドポイントからウェブ、クラウドまで、すべての場所とアプリケーションで生成AIの使用を保護する堅牢なDLPコントロールとポリシーを実装することで、その安全な使用が保証されます。



コンプライアンスの推進



データ保護権限の付与



最新式の検出とコントロール



リスクへの対処と修復



コンプライアンスの推進

現代のIT環境は、データセキュリティに関する数十ものグローバル規制への準拠を目指す企業に対して困難な課題を突き付けています。特にクラウドアプリケーションやモバイルワークフォースへの移行により、その傾向は強まっています。多くのセキュリティソリューションでは、CASBやSWGアプリケーション内に導入するタイプなど、何らかの形式で統合型DLPを提供しています。

しかし、エンドポイント、クラウドアプリケーション、ウェブトラフィック全体に一貫性のない個別のDLPポリシーを導入・管理してしまうと、セキュリティチームは複雑さや追加費用といった問題に直面します。Forcepoint DLPは、他の大手ベンダーよりも多くの事前定義済み分類子、ポリシー、テンプレートを提供することで、お客様のコンプライアンスへの取り組みを加速します。これによってDLPの初期導入をすばやく完了できるほか、継続的なDLP管理も簡素化されます。

- **規制をカバー：** 90か国、150以上の地域の規制要項に対応可能な1,700以上の事前定義されたテンプレート、ポリシー、分類子を使用することで容易にコンプライアンスを遵守・維持することができます。
- **一元管理：** クラウドアプリケーション、ウェブ、電子メール、エンドポイントなど、あらゆるチャネルの一元管理と一貫したポリシーが可能になります。



データ保護の実現

予防制御のみのDLPソリューションはタスク完了のみを目標としているユーザーを苛立たせ、ユーザーはこれを回避しようとします。ユーザーがセキュリティを回避すると、不要なリスクや不注意によるデータ漏洩が発生します。

Forcepoint DLPは、今日のサイバー脅威の最前線にいるのはユーザーだと認識しています。

- クラウドアプリケーション、ウェブトラフィック、電子メール、エンドポイントなど、**データが存在するあらゆる場所でデータを検出して制御します。**

- **従業員へのコーチング：** ユーザーの行動をガイドするカスタムメッセージにより、従業員が適切な意思決定を行えるように指導し、ポリシーに関する教育を行い、重要データを操作する際はユーザー意図を検証します
- **セキュリティ連携：** 組織外にデータを移行する際は、データを保護するポリシーベースの自動暗号化を使用し、信頼できるパートナーと連携したセキュリティ管理を実行します。
- **データのラベリングと分類の自動化：** Forcepoint Data ClassificationやMicrosoft Purview Information Protectionとの統合により、データのラベリングと分類を自動化します。



データに追従する高度な検出とコントロール

悪意あるデータ漏洩や偶発的なデータ漏洩は複雑なインシデントであり、単一事象ではありません。Forcepoint DLPは、Forrester、Radicati Group、Frost & Sullivanにより、DLPソリューションの業界リーダーとして認められています。Forcepoint DLPの重要な特徴の一つは、保存中、移動中、使用中のデータを識別できるという点です。主要なデータ識別内容としては：

- **光学式文字認識(OCR)：** 保存中や移動中の画像に埋め込まれたデータを識別します。
- **堅牢な識別：** 個人識別情報(PII)に対し、データ検証チェック、実名検出、近接分析、コンテキスト識別子(CID)を実行します。
- **カスタム暗号化識別：** 検出や適用制御から隠れていたデータを明らかにします。
- **累積分析：** ドリップDLP検出(時の経過とともに)
- **Forcepoint Data Classificationとの統合：** 高度に訓練されたAI/LLMモデルを活用し、[Forcepoint Data Security Posture Management \(DSPM\)](#) を使用して、使用中および保存中のデータを高精度で分類します。



→ **分析:** 個人的な電子メールの使用増加など、データのやり取りに関するユーザー行動の変化を特定します。Forcepoint DLPはRisk-Adaptive Protectionを使用して行動分析を実行し、ユーザーのリスクを理解し、リスクレベルに基づいて自動化されたポリシー適用を実施するため、さらに高い効果が得られます。これにより、セキュリティチームは、静的なグローバルポリシーと比較して、個別化された動的なポリシーを実装することができます。

データ保護リスクの特定、管理、修復

ほとんどのDLPソリューションには、事前定義された強力な分類ライブラリによる堅牢性や、あらゆるデータへの機密性の高い可視性が備わっていないため、誤検知による過負荷がユーザーにかかり、リスクのあるデータを見逃すことになってしまいます。するとセキュリティチームの効率が下がらだけでなく、従業員やエンドユーザーがセキュリティソリューションをビジネス生産性を妨げるものとして認識し、不満を抱くようになります。Forcepoint DLPは、分析および業界最大規模の事前構築テンプレートとポリシーのライブラリを活用することによって誤検知を大幅に削減し、セキュリティ運用の効率化をサポートします。DLPはまた、従業員のセキュリティ意識を高めるため、従業員へのコーチングやデータ分類ソリューションとの統合をサポートします。

- **集中対応チーム** が最重要リスクに対応します。インシデントに優先順位を付け、リスク責任者、リスクにさらされている重要データ、ユーザー全体に共通の行動パターンなどを強調して可視化します。
- **従業員コーチング** は、組織の名前をパーソナライズできるポップアップ、ポップアップの理由を簡潔に説明するトレーニングステートメント、ユーザーがクリックして組織に関連するセキュリティポリシーの詳細を確認できるURLの形で提供されます。
- **データ所有者と事業責任者:** 電子メールベースの分散インシデントワークフローを活用してDLPインシデントを確認し、これに対処できるようになります。
- **ユーザーのプライバシー保護:** 匿名化オプションやアクセス制御でユーザーのプライバシーを保護することができます。
- **データのコンテキスト追加:** Forcepoint Risk-Adaptive Protectionとの緊密な統合により、より広範なユーザー分析にデータのコンテキストを追加できます。

クラウドやオンプレミスなどあらゆる場所でデータを可視化

今日において企業はデータがあらゆる場所に存在するという複雑な環境にあるため、企業が管理または所有していない場所でのデータ保護も必要となっています。Forcepoint ONE Data Security for CASB and SWGは、分析とDLPポリシーを重要なクラウドアプリケーションやウェブトラフィックに拡張し、データがどこにあっても保護されます。

- **集中対応チームは、Forcepoint ONE for EmailおよびForcepoint ONE for Endpointsを使用して、クラウドアプリケーション、ウェブ、メール、エンドポイントにまたがるデータを特定し、保護することができます。**
- **特定と自動阻止:** 社外ユーザーや権限を持たない社内ユーザーとの機密データ共有を特定し、自動的に阻止します。
- **データ保護:** Office 365、Teams、Sharepoint、OneDrive、Salesforce、Box、Dropbox、Google アプリケーション、AWS、ServiceNow、Zoom、Slackなど、重要なクラウドアプリケーションへのアップロードおよびダウンロード時に、リアルタイムでデータ保護を実行します。
- **統一ポリシーの適用:** 単一コンソールを介して統一ポリシーを適用します。クラウド、ネットワーク、エンドポイント、ウェブ、電子メールなどあらゆるチャネルを移動中のデータとデータ検出ポリシーを定義し、適用します。
- **Forcepointホスト型ソリューションの導入:** DLPポリシー機能をクラウドアプリケーションに拡張できるForcepointホスト型ソリューションを導入。一方で、インシデントやフォレンジックデータをデータセンター内で管理するオプションも利用できます。

DLPの詳細

[デモを依頼する](#)





Forcepointのデータセキュリティソリューション

Forcepoint ONE Data Security	<p>クラウドネイティブソリューションであるForcepoint ONE Data Securityは、機密データを保護し、侵害を防ぎ、グローバルコンプライアンスを保証します。迅速な導入とポリシー管理によりデータ保護を合理化します。クラウドアプリケーション、ウェブ、電子メール、エンドポイントを統合管理します。Forcepoint Risk-Adaptive Protectionにより、リアルタイムのユーザーリスク洞察機能を提供します。Forcepoint ONE Data Securityで、コスト削減、リスク削減、生産性の向上をぜひご体験ください。</p>
Forcepoint DSPM	<p>Forcepoint DSPMは、比類のない可視性と制御を提供することで、クラウドプラットフォームやサーバー間でのデータ拡散という課題に取り組みます。AIによる機械学習を使用して、データの検出と分類精度を継続的に改善します。修復やレポート作成などのタスクを自動化して、プロセスを合理化し、コストを削減します。</p>
Risk-Adaptive Protection	<p>当社のRisk-Adaptive Protection (RAP) は、従来のポリシー中心のDLPソリューションとは異なり、行動を把握してリスクを積極的に軽減するためにユーザーの振る舞いにフォーカスします。RAPは、リアルタイムのリスク解析、130以上の行動指標、スムーズな導入を提供し、リスクの高いユーザーを洗い出します。見やすいダッシュボードで洞察されたリスク行動を把握し、きめ細かなポリシー適用で生産性を高め、ダイナミックな自動化で内部脅威に対するリスクを未然に軽減します。</p>
Forcepoint Data Classification	<p>Forcepoint Data Classificationは、AI主導の高精度と自動化により、データ分類を再定義し、手作業によるエラーを排除して、DLPの有効性を高めます。生成AIと大規模言語モデル(LLM)を活用し優れた分類精度を実現します。継続的な学習と改善を通じて信頼性の高い推奨を行い、ポリシーの適用とコンプライアンスを強化します。ワークフローとシームレスに統合し、生産性を向上させ、誤検知を削減します。</p>
Forcepoint ONE Data Security for Email	<p>Forcepoint ONE Data Security for Emailは、重要な電子メールチャンネル全体の機密データ漏洩を防ぎます。この完全にクラウドネイティブなソリューションは、エンドポイントとモバイルデバイスの両方で、電子メールによる情報漏えいやデータ損失を防ぎます。一般的な電子メールプロバイダーとシームレスに統合され事前構築されたセキュリティポリシー、分類子、テンプレートにより管理が簡素化されます。</p>
Forcepoint DLP for Cloud Email <small>オンプレミス Enterprise DLP)</small>	<p>Forcepoint DLP for Cloud Emailは、送信メールによるデータや知的財産の漏洩を阻止します。エンドポイント、ネットワーク、クラウド、ウェブなど、他のForcepoint DLPチャンネルソリューションと組み合わせることでDLP管理を簡素化し、同一ポリシーを作成し、そのポリシーを複数チャンネルで展開することができます。Forcepoint DLP for Cloud Emailは、予期しない電子メールトラフィックの大規模なスケーラビリティを実現します。追加のハードウェアリソースの設定・管理も不要で、ビジネスの成長に合わせて送信電子メールトラフィックを増やすことができます。</p>
Forcepoint ONE CASB and SWG	<p>Forcepoint ONE Data Security for CASB and SWGは、Forcepoint ONE Data Security for EndpointおよびForcepoint Data Security for Emailと同じ完全なクラウドネイティブDLPソリューションを提供します。単一のユーザーインターフェースから4チャンネルのいずれかまたはすべてを管理し、同じポリシー管理コンソールからすべてのポリシーを同期させることができます。ポリシーを一度作成すれば、Forcepoint ONE Data Securityのすべてのチャンネルに展開できるため、複数のサービス間でポリシーを同期させる時間とリソースを節約できます。</p>



forcepoint.com/contact

Forcepointについて

Forcepointは、グローバルビジネスおよび政府機関のセキュリティを簡素化します。Forcepointのクラウドネイティブプラットフォームによって、Zero Trustを簡単に採用し、どこで仕事しているのであれ、機密データや知的財産の盗難や損失を防ぐことができます。テキサス州オースティンに拠点を置くForcepointは、150カ国以上に所在するお客様とその従業員に対して、安全で信頼できる環境を作り出しています。www.forcepoint.com、Twitter、LinkedInでForcepointをご覧ください。