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.com/ja

Forcepoint Data Loss Protection (DLP)

ForcepointでAI変革を保護

世界中の組織がAI変革に着手しており、特にGenAIアプリケーションとテクノロジーをビジネスプロセスに統合しようと取り組んでいます。これにより、大幅な生産性の向上が期待できますが、同時にデータセキュリティに新たな課題がもたらされています。たとえば、ユーザーはGenAIアプリケーションに機密データを入力したり、機密ファイルをアップロードしたりすることができるため、データ漏洩を助長する可能性があります。Forcepointは、最も価値のある資産となるデータを犠牲にすることなく、AIの可能性を活用できるソリューションを提供します。

Forcepointの最先端のAIメッシュテクノロジーが、データ分類において比類のない精度と効率を確保します。これにより、AI変革の複雑さを乗り越えていく過程でも安心感が得られます。ChatGPT、Copilot、GeminiなどのGenAIアプリを使用している場合でも、Forcepointなら一元化された可視性と制御を実現して、すべての環境にわたる機密データを保護できます。

従業員が働く場所やデータが保存される場所すべてでデータセキュリティを実現

Forcepoint DLP は、あらゆる規模の組織が直面する重要なデータ セキュリティの課題に対処します。規制要件が厳しくなるにつれて、個人識別情報 (PII) や保護対象医療情報 (PHI) などの機密情報の保護が最重要になります。クラウド アプリケーション、ハイブリッド セットアップ、BYOD のトレンドなど、現代の作業環境はデータ保護をさらに複雑にします。

アタックサーフェスが拡大しているため、包括的な可視性と制御が必要です。Forcepoint DLPを使用することで、データセキュリティチームは、エンドポイント、ネットワーク、クラウド、Web、プライベートアプリケーション、電子メールなどの主要チャネル全体にわたってグローバルなポリシーを管理することができるようになります。事前に定義済みのテンプレートと分類子によってインシデント管理は合理化され、リスクを最小限に抑えながら生産性に焦点を当てることができます。従業員の作業場所やデータの保存場所がどこであれ、Forcepoint DLPなら可視性と制御性を確保できます。

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。

コンプライアンスを効率化

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。

- → **カバレッジを調整**することで90か国、160以上の地域の規制要件に対応する1,700以上の事前定義されたテンプレート、ポリシー、分類子を使用して容易にコンプライアンスの遵守・維持が可能です。
- → **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mエック、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
- → **よりスマートな適用**により、個人用メールの使用増加など、データのやり取りに関連するユーザー行動の変化を特定します。Forcepoint DLPはリスク適応型保護により、行動分析を活用してユーザーのリスクを把握し、その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ことで、さらに効果的になります。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べると、個別化されたより動的なポリシーを導入することができます。

AI Mesh

ビジネスの最も貴重な資産である「データ」を犠牲にすることなく、AIの可能性を解き放ちます。Forcepointの最先端のAI Meshテクノロジーが、データ分類において比類のない精度と効率性を提供し、安心感をもたらします。ChatGPT、Copilot、GeminiなどのGenAIアプリを含むあらゆる場所で、一元化された可視性と制御でデータを保護します。GenAIやその他のアプリを安全に使用できる環境を整えて、チームの生産性を向上させます。簡素化された運用と統一されたポリシーでコストを削減します。

- → **Forcepoint Data Classificationと同期**Forcepoint Data Security Posture Management (DSPM) を使用して、高度に学習したAI MeshとLLMモデルを活用し、使用中のデータと保存中のデータを高い精度で分類する能力を提供します。

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るだけでなく、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。

情報漏えいをリアルタイムで阻止

情報漏えいは一瞬にして発生し、その結果は経済的および評判の双方で多大な損害をもたらす可能性があります。Forcepoint DLPはデータ侵害が発生した瞬間に特定し、防止するツールを組織に提供し、機密データを安全に保護します。高度なリアルタイム保護と効率化された管理を提供することで、お客様のチームが進化する脅威の一歩先を行くことを可能にします。

- → **リアルタイムの監視と阻止:** 機密情報が漏えいする前に、情報漏えいを検知し阻止します。
- → **統合ポリシー管理:** 単一のコンソールでセキュリティを簡素化し、「Data Security Everywhere」の環境全体でポリシーを管理します。
- → **フォレンジック:** データ移動の全容を明らかにして、インシデント調査、データ侵害阻止、ポリシー強化し、コンプライアンス遵守を実現します。
- → **クロスチャネル・インシデントの可視性:** Web、クラウド、電子メール、エンドポイン全体にわたるデータ移動の完全な可視性を確保し脅威に迅速に対応します。
- → **リスク適応型保護:** ユーザーの行動とリスクレベルに基づいてセキュリティ管理を動的に調整し、生産性を損なうことなく機密データの保護を維持します。

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 (DLP SaaS)	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。
Forcepoint DSPM	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全体に拡散しているデータ問題に取り組みます。AI Meshテクノロジーを使用して、データの検出と分類精度を継続的に改善します。また、修復やレポート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。
Risk-Adaptive Protection	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。
Forcepoint ONE Data Security for Email (DLP SaaS)	Forcepoint ONE Data Security for Emailは、重要な電子メールチャ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。
Forcepoint ONE Data Security for Cloud Apps and Web (DLP SaaS)	Forcepoint ONE Data Security for Cloud Apps and Webは、Forcepoint ONE Data Security for EndpointおよびForcepoint Data Security for Emailと同様に、完全にクラウドネイティブなDLPソリューションを提供し、単一のユーザーインターフェイスから4つのチャネルのすべて、またはいずれかを管理し、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することができます。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。
Forcepoint Data Classification	Forcepoint Data Classificationが、AI Meshから得られる精度と自動化で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の有効性を強化します。 AI Meshテクノロジーと大規模言語モデルを活用して、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、確信のある推奨事項を提供し、ポリシーの施行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、誤検知を低減します。
Forcepoint DLP Endpoint	Forcepoint DLP Endpointは、企業ネットワークの内外で、WindowsおよびMacのエンドポイントにある重要なデータを保護します。これには、静止時（検出）、移動中、使用中のデータに対する高度な保護と制御が含まれます。Microsoft Azure Information Protectionとの統合により暗号化されたデータを分析し、適切なDLPコントロールを適用します。DLPのコーチングダイアログのガイダンスに基づいて、従業員はデータリスクを自己修復できるようになります。このソリューションは、ウェブアップロード（HTTPSを含む）やクラウドサービス（Office 365やBox Enterprise）へのアップロードを監視します。Outlook、Notes、電子メールクライアントとの完全統合が可能です。
Forcepoint DLP Discover	Forcepoint DLP Discoveryは、ファイルサーバ、SharePoint（オンプレミスとクラウド）、Exchange（オンプレミスとクラウド）、およびSQLサーバやOracleなどのデータベース内の検出において機密データを特定し保護します。高度なフィンガープリント技術により規制対象データと知的財産を静止状態で特定し、適切な暗号化と制御を適用してこれらのデータを保護します。Discoveryには、画像内のデータを可視化するOCRも含まれています。
Forcepoint DLP Network	Forcepoint DLP Networkは、電子メール、Webチャネル、FTPを通じて移動中のデータ窃取を防ぐための重要な適用ポイントを提供します。このソリューションは、外部からの攻撃や内部の脅威によるデータ流出、および偶発的なデータ損失を特定し防止するのに役立ちます。OCRは画像内のデータを認識します。分析は、データ盗難を1レコードずつ阻止するドリップDLPやその他のリスクの高いユーザー行動を提供します。
Forcepoint DLP for Cloud Email	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。
Forcepoint DLP App Data Security API	Forcepoint DLP App Data Security APIの使用により、組織内のカスタムアプリケーションやサービス内のデータを簡単に保護することができます。ファイルやデータトラフィックの分析を可能にし、許可、ブロック、パーソナライズされたポップアップによる確認、暗号化、共有解除、隔離などのDLPアクションを適用します。これは複雑なプロトコルに関する広範なトレーニングや知識を必要とせず理解しやすく、簡単に使用できるREST APIです。また、特定の言語に依存しないため、あらゆるプログラミング言語やプラットフォームでの開発と利用が可能です。

Forcepoint

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。