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)

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

データセキュリティは、今日のあらゆる種類や規模の組織にとって重要な問題です。IT組織は規制を順守しつつ、個人識別情報（PII）、保護医療情報（PHI）、その他の規制対象情報を狙った悪意ある攻撃や偶発的損失からデータを保護する必要があります。その一方で、クラウドアプリケーションやハイブリッドクラウドの導入、BYODトレンドへの対応など、マクロITの動向にも対応しなければなりません。これらは全て、組織からのデータ漏洩経路が増える要因となります。

このような攻撃対象領域の拡大は、重要データを保護する上で最重要課題となっています。データセキュリティチームはまた、組織「内部」からのデータ移動先や保存先として、あらゆる場所やチャネルへのデータ移動が急増している点も考慮しなければなりません。オンプレミスだけでなく、クラウド内の全データを可視化する必要があります。データセキュリティチームはさらに、あらゆるチャネル（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）を一元管理しながら可視化し、制御しなければなりません。

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。ほとんどの業界の規制に対応した定義済みテンプレート、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、従業員が働くあらゆる場所、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。

重要チャネルの保護

- **カスタムアプリケーション**
- **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**
- **エンドポイント**
- **ネットワーク**
- **ディスカバリー**
- **Web**
- **電子メール**

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、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は、クラウド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、ネットワーク全体に一貫性のない個別のポリシーを導入・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、1600以上の事前定義された分類子、ポリシー、テンプレートを提供することにより、コンプライアンスへの取り組みをサポートします。これによってDLPの初期導入を素早く完了できるほか、継続的なDLP管理も簡素化されます。Forcepoint DLPは、顧客の機密情報と規制対象データを効率的に保護し、お客様のコンプライアンス維持を確保します。

- → **規制をカバー：** 83カ国、150以上の地域の規制要項に対応可能な1,600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 遵守し、維持することができます。
- → **特定と修正：** ネットワーク 、クラウド、エンドポイントから規制対象データを検出し、修正します。
- → **一元 管理：**クラウド、エンドポイント、ネットワーク、ウェブ、 電子メールなど、あらゆるチャネルを一元管理し、一貫したポリシーを適用します。

データを保護する力を与える

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的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。

- → **データ検出とコントロール：** クラウド、ネットワーク 、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検出と コントロールを実行します。
- → **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の意図を検証します 。
- → **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、Gartner、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：

- → **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（時の経過とともに徐々に漏洩するデータ）の累積分析を実行します。
- → **Forcepoint Data Classificationとの統合**により、高度に訓練されたAI/機械学習モデルを活用して、使用中データの高精度分類を実行します。

- → **機械学習：** ユーザーは、以前に見たことがない関連データも識別できるよう、システムを訓練することができます。ユーザーは、類似のビジネス文書やソースコードなどにフラグを立てるための肯定例と否定例をエンジンに提供することができます。
- → **フィンガープリント：** 構造化データ（データベースなど）のフィンガープリントにより、データ所有者はデータの種類を定義し、ビジネス文書、設計計画、データベース間 で完全一致および部分一致を識別し、データに一致する適切な管理方法やポリシーを適用することができます。
- → **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ます。
- → **従業員意識の向上：** Forcepoint Data Clasification、Microsoft Purview Information Protectionといった分類ソリューションとの統合により、WindowsやmacOSの従業員コーチングを実行し、機密データやIPの取り扱いに対する従業員意識を高めます 。
- → **高度なDLPデータ識別機能の適用：** リモートワークのエンドポイントや企業のクラウドアプリケーションに対し、フィンガープリントなど高度なDLPデータ識別機能を適用します 。
- → **データ所有者と事業責任者** は、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。

オンプレミスやクラウドを含む、あらゆる場所に存在するデータを可視化

今日の企業は、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 CASB、SWG、ZTNAは、重要なクラウドアプリケーション、ウェブトラフィック、ウェブベースのプライベートアプリケーションにまで分析およびDLPポリシーを拡張できるため、あらゆる場所に存在するデータを保護することができます。Forcepoint DLP App Data Security APIなどのREST APIにより、社内でカスタム開発されたアプリケーションの可視化やDLP適用が可能となります。

- → **集中対応 チームによる特定と保護：** クラウドアプリケーション、ネットワークデータストア、データベース 、管理対象・非対象のエンドポイントにわたってデータを特定し、保護します。
- → **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。
- → **統一ポリシーの施行：** 単一コンソールを介して 統一ポリシーを施行します。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：** フィンガープリントや機械学習などの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。
- → サードパーティツールによるインシデント表示と管理：公開されたREST APIを介し、サードパーティツールによるインシデント表示と管理を実行します。インシデント管理ワークフローを自動化し、ServiceNow、Nagios、Tableauなどの自動化ツール・サービスツール、およびSplunk、XSOARなどのSIEM/SOARソリューションを介し、DLPインシデントに依存するビジネスプロセスをサポートします。

Forcepoint DLPには高度な分析と規制ポリシーのテンプレートが含まれており、導入するたびに単一のコントロールポイントからデータを管理することができます。クラウドアプリケーション、ウェブトラフィック、ウェブベースのプライベートアプリケーションなど、あらゆる場所に存在するデータを保護します。

付録A：DLPソリューションコンポーネントの概要

Forcepoint DLP Endpoint	Forcepoint DLP Endpoint は、企業ネットワーク内外のWindowsおよびMacエンドポイント上の重要データを保護します。これには、保存中（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コントロールを実行します。DLPコーチングダイアログのガイダンスに基づき、従業員がデータリスクを自力で修復できるよう指導します。本ソリューションは、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 ONE CASB	Forcepoint ONE CASB 搭載により、Forcepoint DLPの高度な分析と単一制御をOffice 365、Salesforce、Box、Dropbox、Googleアプリケーション、Amazon AWS、ServiceNow、Zoom、Slackなどの認可されたクラウドアプリケーションに拡張できます。ユーザーがどこにいても、どのようなデバイスを使用していても、ビジネスの重要データをコントロールし続けることができます。
Forcepoint ONE SWG	Forcepoint ONE SWG を使用することで、チームは信頼度の高い高速ウェブパフォーマンスを得られ、あらゆるウェブサイトに安全にアクセスし、あらゆるドキュメントをダウンロードできるようになります。危険なサイトをセキュアコンテナでレンダリングするRBIや、ダウンロード可能なすべてのドキュメントを完全に無害化するZeroTrust CDRと統合します。
Forcepoint ONE ZTNA (coming 2H 2023)	Forcepoint ONE ZTNA は、管理対象デバイスと対象外デバイスの両方で、VPN不要のシンプル、安全、スケーラブルなゼロトラスト・リモートアクセスを社内およびプライベートクラウドアプリケーションに提供します。
Forcepoint DLP—Discover	Forcepoint DLP—Discovery は、ファイルサーバー、SharePoint（オンプレミスおよびクラウド）、Exchange（オンプレミスおよびクラウド）、SQL ServerやOracleなどのデータベース内の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や知的財産を保存状態で特定し、適切な暗号化と制御を適用してデータを保護します。Forcepoint DLP—Discoveryには、画像内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、ウェブチャネル、FTP　通じて移動中のデータ盗難を阻止するための重要な実行ポイントを提供します。本ソリューションは、外部からの攻撃や内部の脅威によるデータ漏洩、および偶発的なデータ損失を特定・防止するのに役立ちます。OCR　画像内のデータを認識します。分析を基に、レコードごとのデータ盗難や、その他リスクの高いユーザー行動を阻止するDrip DLPが提供されます。
Forcepoint DLP for Cloud Email	Forcepoint DLP for Cloud Email は、送信メールによるデータやIPから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、非クラウドソリューションとは異なり、予期しないメールトラフィックの急増にも対応可能な拡張性を備えています。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、組織内部のカスタムアプリケーションやサービスデータを簡単に保護することができます。ファイルやデータのトラフィック分析が可能であり、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要求、暗号化、共有解除、隔離などのDLPアクションを実行します。REST APIなので複雑なプロトコルに関する広範なトレーニングや知識がなくても理解しやすく、簡単に使用することができます。また、言語に依存していないため、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・使用が可能です。

付録B：DLPソリューションコンポーネントの概要

	FORCEPOINT DLP ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT DLP—DISCOVER	FORCEPOINT DLP— NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT ONE SWG	FORCEPOINT DLP APP DATA SECURITY API	FORCEPOINT ONE ZTNA (COMING 2H 2023)
主な機能は?	アプリケーション、ウェブ、印刷、リムーバブルメディアチャネルなどを介したユーザーのエンドポイントでデータを検出し、データ保護ポリシーを適用します。	クラウドまたはクラウド配信アプリケーションのデータ検出およびポリシー適用	データセンターその他のオンプレミス環境内の保存データ検出、スキャン、修復	ネットワーク内のウェブやウェブ電子メール経由で移動中のデータ可視化と制御	ネットワーク内のウェブやウェブ電子メール経由で移動中のデータ可視化と制御	送信メール経由で移動中のデータ可視化と制御	社内カスタムアプリケーションおよびサービス内のデータ可視化と制御	企業のプライベートアプリケーション内を移動中（アップロード・ダウンロード）のデータ可視化とデータ保護ポリシーの適用
保存データはどこで検出・保護されるのですか?	Windowsエンドポイント、Mac OSエンドポイント	OneDrive、Sharepoint Online、Exchange Online、Google Drive、Box、DropBox、Salesforce、ServiceNow	オンプレミスのファイルサーバーとネットワークストレージ、Sharepointサーバー、Exchangeサーバー、およびデータベース（Microsoft SQLサーバー、Oracle、IBM Db2など）					
移動中のデータはどこで保護されるのですか?	電子メール、ウェブ（HTTP）、プリンタ、リムーバブルメディア、ファイルサーバ / NAS	Office 365、Googleアプリケーション、Salesforce.com、Box、Dropbox、ServiceNow（API経由）、その他あらゆる主要アプリ（プロキシ経由）のアップロード時、ダウンロード時、および共有時		電子メール、プリンタ、FTP、ウェブ（HTTP）、ICAP	電子メール	HTTP(S)	社内カスタムアプリケーションとカスタムサービス	ZTNAコネクタを介したプライベートアプリへのアップロードとダウンロード
使用中のデータはどこで保護されるのですか?	Zoom、Webex、Google Hangouts、IM、VOIP ファイル共有、M365 Teams共有、アプリケーション（クラウドストレージクライアント）、OSクリップボード	クラウドアプリケーションを使用した作成時、変更時、およびコラボレーション活動時					社内カスタムアプリケーションとカスタムサービス	

付録B：DLPソリューションコンポーネントの機能比較

	FORCEPOINT DLP—ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT DLP—DISCOVER	FORCEPOINT DLP—NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT ONE SWG	FORCEPOINT DLP APP DATA SECURITY API	FORCEPOINT ONE ZTNA (COMING 2H 2023)
リスク適応型保護	アドオン		アドオン	アドオン	アドオン	アドオン：現在はForcepoint ONE SWGを使用するGRE/IPSecトンネルでサポートされています		
光学式文字認識（OCR）			含まれる内容：	含まれる内容：	含まれる内容：			DLP実行のためのOCRサポート
Data classificationとラベリング統合	Forcepoint Data ClassificationとMicrosoft Purview Information Protection。							
フィンガープリント機能が利用できるデータは?*	構造化（データベース）、非構造化（ドキュメント）、バイナリ（非テキストファイル）							Available 2H2023
統合ポリシー管理	エンドポイントからクラウドアプリケーションまで単一コンソールを介したポリシー設定と適用							Available 2H2023
堅牢なポリシーライブラリ	業界最大のコンプライアンスポリシーライブラリからの検出と適用							

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。

© 2023 Forcepoint. ForcepointおよびFORCEPOINTのロゴは、Forcepointの商標です。本文書で使用しているその他の商標はすべて、各商標権者に帰属します。[FP-DLP-Brochure-JA] 18Aug2023