



Forcepoint Data Visibility

powered by Getvisibility

お客様のデータを俯瞰的に把握し、
データセキュリティを強化

Forcepoint

パンフレット

お客様のデータはいたるところに存在しており、それがお客様の悩みの種となっています。データはデータセンター、複数のクラウド、多くのノートPCにまたがって保管されている可能性が高く、データの問題はさらに深刻化しています。どのようなデータがどこにあり、さらに重要なことに、これらのデータが今現在お客様の会社にとどのようなリスクをもたらしているのか、正確に把握されているでしょうか。世界全体のデータの80%は非構造化データであり、その90%は分析されていない、とIDCでは推定しており¹、言い換えれば、それは組織の毎日の業務の一部として扱われていないデータであり、把握されていないデータです。そのデータは文字通り目に触れることはありません。コンプライアンスに対する要求がますます高まり、データ漏洩が多発する現在²、すべてのデータを可視化し、リスクとそれに伴うコストを最小限に抑えることが必要不可欠となっています。この問題については、あらゆる業種や規模の組織が絶えず注意を払っていく必要があるといえます。

リスクを最小化するには、オンプレミスでもクラウド上でも、データがどこに存在するかを確認することから始まります。Forcepoint Data Visibilityは、組織のすべてのデータを俯瞰できる可視性を提供します。Data Visibilityは、データセキュリティに対するForcepointのアプローチの中核をなすもので、お客様はすべてのデータを継続的に発見、分類、監視、保護することができます。Forcepoint Data Visibilityが提供する360°ビューは、データ漏えいの発生を徹底的に減らし、コンプライアンス上のリスクを排除し、最終的にはデータ漏えいやコンプライアンス違反に伴う莫大なコストを削減します。



IDCによると、世界のデータの80%は非構造化データであり、その90%は分析されておらず、「ダークデータ」とも呼ばれている。³



94%の組織が複数のクラウド環境上にデータを保存している。⁴



Equifaxは、従業員のユーザー名とパスワードのコピーが複数保存された共有ドライブにハッカーがアクセスしたことが原因でデータ漏えい5が拡大したとして、14億ドルの賠償請求訴訟に和解した。同社は、重複したファイルや古くなったファイルを検出・特定するツール備えていなかった。

1 [目に見えないデータの難問](#)、Forbes、2022年2月

2 [2022年情報漏えい調査報告書](#)、Verizon、2022年5月

3 [目に見えないデータの難問](#)、Forbes、2022年2月

4 [ダークデータ:クラウドの知られざるセキュリティとプライバシーリスク](#)、Forbes、2023年6月

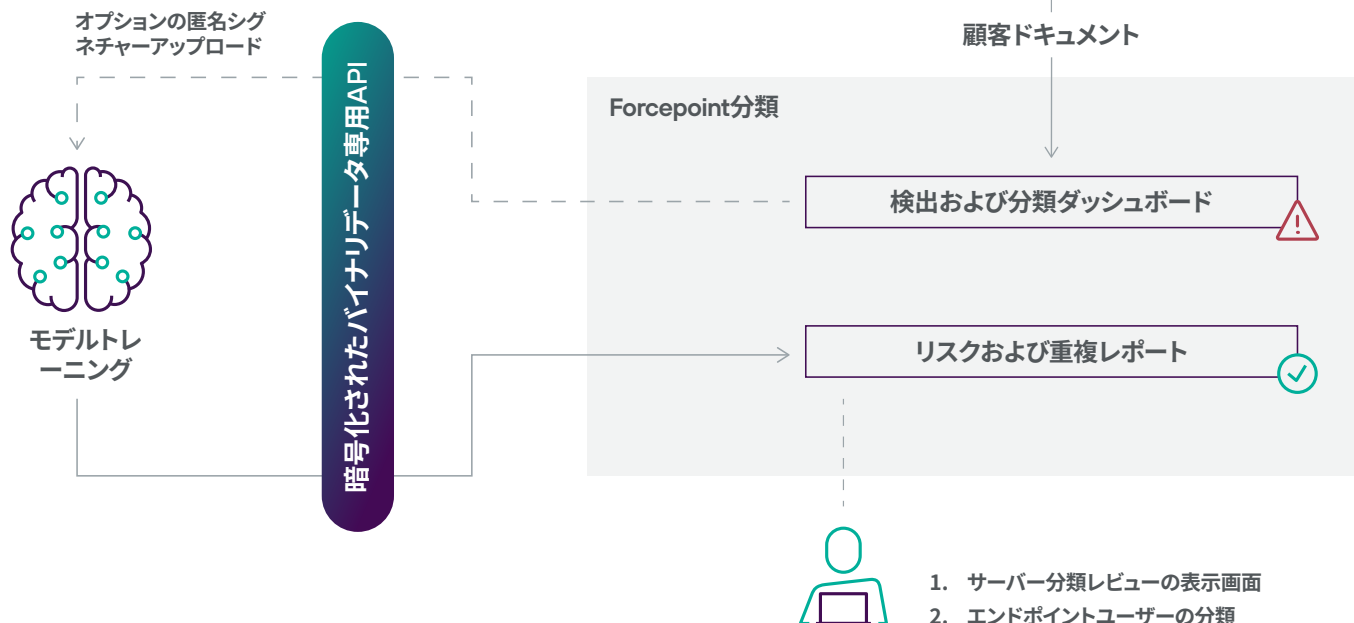
5 [Equifax、13.8億ドルのデータ漏えい訴訟和解に同意](#)、Finextra、2022年1月

FORCEPOINT DATA CLASSIFICATION (AWS)

顧客ネットワーク



顧客ドキュメント



人工知能 (AI) の力を活用し、迅速な可視化を実現

オンプレミスを含む複数のクラウド環境にデータを保存している組織では、クラウドサービス内のデータしか可視化できないクラウドプロバイダに依存すると、データセキュリティの有効性が著しく限定されることになります。また、典型的な発見・分類ツールでは、結果を出すために管理者が手動で介入する必要があり、機械学習 (ML) を限定的に利用するツールでも、トレーニングの決定を下すために誰かが介入する必要があります。

Forcepoint Data Visibilityは、自己学習型AIと大規模言語モデル (LLM) を適用することで、データがクラウドに保存されているかオンプレミスに保管されているかを問わず、データの発見、カテゴライズ、分類のプロセスを自動化し、これらの課題を解消します。Forcepointの強力な事前学習済み発見・分類モデルは、あらゆる主要産業にわたる多くの組織から寄せられた数億件の実際のデータファイルによって学習された50次元モデルに基づいています。この革新的なアプローチにより、実データに関連するデータプライバシーを損なうことなく、比類のない分類精度と継続的な改善のための高品質な合成データが生成されます。Forcepointエンジンがデータを取り込む際にも、AIを活用した継続的学習が自然言語でデータ分類の提案を行い、精度の高いデータ分類、PII検出、データコンプライアンスリスクのスコアリングを行います。

Forcepointは、高精度のダッシュボードとレポートを介してこれらの情報をお届けします。これらのダッシュボードはまた、発見されたすべてのファイルのIPアドレス、パス、詳細なアクセス許可を明らかにします。Forcepointの分類精度は時間の経過とともに向上し、Forcepoint Data Loss Prevention (DLP) と組み合わせることで、最高レベルのデータセキュリティのためのより高い可視性を実現します。

- AI の活用による精度:** 時間のかかる手作業によるデータから解放されます。Forcepointの自己学習型AIは、クラウドとオンプレミスを問わず、すべてのデータを自動的に検出、分析、分類し、時間の節約と精度の向上をもたらします。
- データの死角はもうありません:** 場所、権限、リスクスコアなど、ファイルの詳細な情報をダッシュボードに鮮明に表示します。直感的でわかりやすいデータ可視化により、豊富な情報に基づいた迅速な意思決定が可能です。
- より高度なセキュリティ:** ForcepointのAIは絶えず学習と適応を行い、わかりやすい表現でデータを分類し、機密性の高い個人情報を検出することで、データ漏洩やコンプライアンス違反を未然に防ぎます。

最も機密性の高い情報を誰が見ることができるかを可視化する

パートタイムの契約社員に、顧客の個人情報や営業上の密情報を見せる必要があるでしょうか。多くの組織では「特権クリープ特権の忍び込み」が発生し、従業員が業務を遂行するために必要な範囲をはるかに超えるアクセス許可が与えられることがよくあります。Zero Trustのセキュリティ原則を確立しようとしている企業であっても、最も機密性の高い情報へのアクセスの管理はしばしば見落とされ、誤った管理が行われています。過度の特権を持つユーザーは、最終的に、違反やコンプライアンス違反によって企業に莫大な損失をもたらす可能性があります。⁶

Forcepoint Data Visibilityでは、すべてのファイルとユーザーのアクセス許可を検査できます。データ管理者は、組織全体でどの個人がファイルやファイル共有にアクセスできるかを把握できます。定期的なスキャンにより、特権クリープを阻止し、データ侵害の機会を飛躍的に減らすことができます。ワンクリックで、スキャンされたすべてのファイルのアクセス許可を即座に表示できます。これにより、ユーザーの業務に必要な適切なレベルの権限を適用できます。

- ▶ **「特権クリープ」の阻止:** ユーザーが必要なデータにのみアクセスできるようにし、内部脅威や偶発的な情報漏えいを防止する。ワンクリックでスキャンされたすべてのファイルのアクセス許可が表示されるため、適切なレベルのアクセスを高速で適用可能。
- ▶ **法規制に準拠:** すべてのファイルとユーザーのアクセス許可を可視化することで、コストのかかる訴訟や罰則を回避。
- ▶ **データ漏えいリスクの低減:** 攻撃者の格好の標的となる過度の権限を持つユーザーの排除。定期的なスキャンにより、特権クリープの発生を検出・阻止し、データ漏えいの可能性を飛躍的に削減する。

ROTを一掃してデータに関する責任を軽減

貴社はデータの管理に関して、貯め込む傾向がありませんか？ 人気テレビ番組では、何も捨てることができない人々を取り上げ、最終的に完全に管理できなくなったゴミの塊の中で生活している様子を描いていました。多くの企業はデータをため込み、データを維持することが良いことであり、リスク軽減につながると信じています。実際はその逆が正しい。データは資産にもなり得ますが、負債にもなり得ます。企業がデータにしがみついた結果、大量のROT（冗長な、時代遅れの、あるいは些細な）データが蓄積されることとなります。企業はコンプライアンスを遵守するどころか、データ侵害に対して極めて脆弱になり、増え続けるデータ規制へのコンプライアンス違反がさらに大きくなる可能性があるのです。ROTとは何か、詳しく見てみましょう。

- **冗長データ** とは、クラウドまたはオンプレミス上の複数の場所に保存されたファイルの多数のコピーまたはバージョンのことです。企業は、ユーザーが特定のコピーに依存している場合や、削除によってコンプライアンス違反のリスクが生じることを懸念して、誤って削除することを避ける傾向があります。
- **時代遅れのデータ** とは、もはや正確でない、あるいは使用されていない情報のことです。通常、時代遅れのデータは、すでに最新の有用なデータに置き換えられています。
- **些細なデータ** 保管する必要のない情報のことです。些細なデータは、企業にとって何の有益性ももたらしません。



6 2020年世界デジタル損失テクノロジー市場シェア：DLPは終わり、新たなDLPの時代が始まる、IDC、2021年10月
7 2020年世界デジタル損失テクノロジー市場シェア：DLPは終わり、新たなDLPの時代が始まる、IDC、2021年10月



ROT データは機密情報を含むことが多いため、そこには責任が生じます。削除すべきデータを可視化できなければ、企業は潜在的なデータ漏えいや規制上の罰則を受ける可能性を自ら負ってしまうことになります。ROTの高額な例として、13億8,000万ドルの訴訟和解に至ったEquifaxの情報漏えいが挙げられます。この情報漏えいの本質は、ユーザー名とパスワードのコピーが保存された共有ドライブにあり、従業員は、ユーザー名とパスワードのコピーを複数作成することで業務を効率化していると考えていました。ひとたびハッカーが共有ドライブに侵入できれば、ユーザー名とパスワードの複数のコピーの存在により、ハッカーにとって作業は容易なものでした。Equifax社は、冗長なファイルや古いファイルのコピーを検出・特定するためのツールを持ち合わせていなかったのです。

“「ROT と考えられる企業データは3分の1にも上る (さらに残りの52%は価値が不明なダークデータである)」

クラウド上でデータのROT化を阻止する方法、Forbes、2023年1月

ROTリスクを排除するには、自動制御ときめ細やかな洞察が必要です。Forcepoint Data Visibilityは、データの所在場所を問わず、すべてのデータを迅速にスキャンする検出・分類機能を搭載しています。AIを駆使した高精度の分析により、ファイルの重複、各ファイルの作成日と最終使用日、各ファイルの分類とコンプライアンスリスクを明確に把握することができます。Forcepoint Data Visibilityダッシュボードでは、これらのさまざまな領域を徹底的に掘り下げ、各ファイルの細部を確認し、重複に関するレポートを作成することが可能です。このような情報を活用することで、ROTを効果的に一掃することができます。Forcepoint Data Visibilityを導入した企業は、必要な頻度で追加のコストをかけずに完全なデータスキャンとリスクレポートを実施できるため、データROTの問題に積極的に対処できるようになります。

Zero Trustデータセキュリティ戦略における最初のステップとしては、すべての既存情報を検出・分類し、どの情報に価値があり、法令遵守のために必要なかを迅速に判断することです。つまり、それ以外のものはすべてROTであり、防衛的に削除することができるのです。

ユーザーフレンドリーなダッシュボードで全データの俯瞰が可能

The screenshot shows the Forcepoint Data Visibility dashboard. The top navigation bar includes 'Dashboard', 'Agent', 'Analytics (BETA)', and 'Administration'. A sidebar on the left contains icons for 'SCAN PROGRESS', 'CLASSIFICATION TAGS', 'COMPANY OVERVIEW', 'EXPLORE', 'ML TAG TRAINING', and 'DATA RISK SURVEY'. The main area features a search bar with the placeholder 'Type file or folder name' and a 'Switch to advanced search' toggle. Below the search bar are several filter dropdowns: File Extension, Source, Risk, Keyword Hits, Group, Category, Subcategory, Classification, Alias, Flow, Compliance, and Trustees. At the bottom right of the filters are 'EXPORT' and 'CLEAR SEARCH' buttons. The main table displays data with columns: Path, Cate..., Subc..., Class..., Key..., Dete..., Compli..., Com..., Risk, Crea..., Last..., Class..., and Actions. The table contains five rows of data, each with a checkbox in the Path column and icons in the Actions column.

Path	Cate...	Subc...	Class...	Key...	Dete...	Compli...	Com...	Risk	Crea...	Last...	Class...	Actions
☐ files/Data Visibility/DataSet/	Technical Documents	License agreement	Internal						Mar 30, 2023	Jan 4, 2024	0.32	
☐ files/Data Visibility/DataSet/	Financial Documents	Quotation/P	Internal						Mar 30, 2023	Jan 4, 2024	0.84	
☐ files/Data Visibility/DataSet/	Technical Documents	Guide/Manu	Public						Mar 30, 2023	Jan 4, 2024	0.66	
☐ files/2022DLPTTestFiles/a_Da									Oct 12, 2022	Jan 4, 2024		
☐ files/Data Visibility/DataSet/	Technical Documents	Policy/Proce	Internal						Mar 30, 2023	Jan 4, 2024	0.52	

Forcepoint Data Visibility は、管理者のニーズに合わせて簡単に検索、フィルタリング、並べ替えができるユーザーフレンドリーなダッシュボードを搭載しています。また、オプションとして、AIモデルからの結果の確認、カテゴリとサブカテゴリの変更、ドキュメント内の個人情報 (PII) の有無の調整などがあり、これらは自動および手動でAIモデルを更新することができます。セキュリティ運用をさらに合理化するために、これらの結果は、リスク領域に対処するための修復やその他のタスクのために、実行可能な形式でエクスポートすることができます。

このユーザー主導のトレーニングAIモデルを活用することで、継続的な自己学習が可能になり、企業のパーソナライゼーションと精度が向上します。

パーソナライゼーションと精度を高める継続的な自己学習モデル

Forcepoint Data Visibilityは、生成AIと複数の主要な大規模言語モデル (LLM) のパワーを活用し、以下の方法でデータセキュリティを強化します。

- **精度の向上:** 当社の先進的なAI モデルは予めトレーニングされており、さまざまな企業や業界の広範囲に及ぶ膨大な数のファイルから構成されるリポジトリから学習します。この包括的なアプローチにより、さまざまな企業組織の微妙な違いを理解してデータを正確に分類し、意味のある実用的な分類を実現します。
- **高品質な合成データ:** これは、AIモデルから正確な合成データを生成するという革新的なアプローチであり、実データに関連するプライバシーやセキュリティの懸念を損なうことなく、比類のない分類精度と継続的な改善を保証します。
- **個別化されたAIモデル:** 当社のAIモデルは、ユーザー主導型で継続的に向上していくため、お客様のデータの状況に合わせて特定の企業や業界のニーズに合わせた最適なソリューションとなり、より優れた個別化と精度を実現しています。

これらすべての要素がシームレスに連携し、70の分類分野で98%以上の分類精度を実現することで、組織全体のデータの可視性が向上します。これにより、DLPの誤検知が減少し、情報漏えいや流出に対する防御が強化されます。

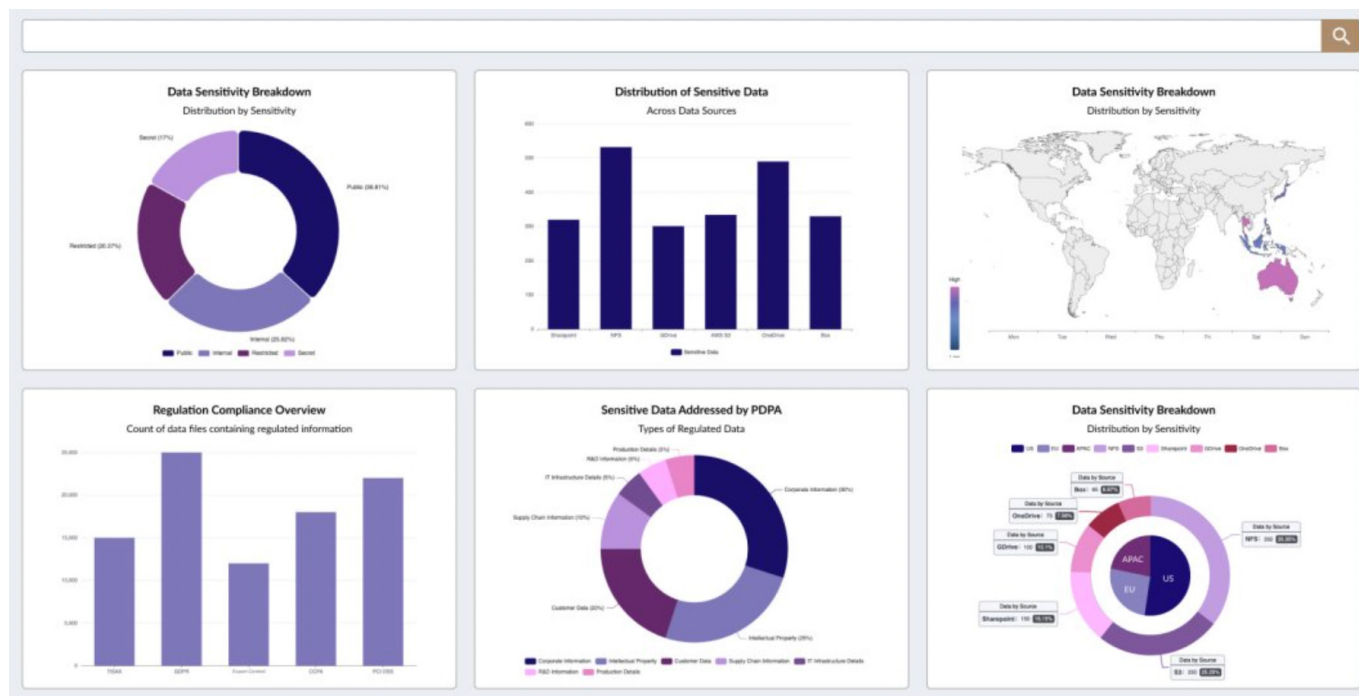
最小特権アクセスによりZero Trust戦略を強固にする

Zero Trust戦略を強固にする重要な要素は、最小特権アクセスの原則です。必要不可欠なアクセスのみに厳しく制限することで、より安全なデータ環境を創出します。このアプローチは、データ全体の可視性を高めるだけでなく、潜在的な脅威に対する強固な防御にも貢献し、Zero Trustセキュリティの取り組みを加速させます。

Forcepoint Data Visibilityレポートングスイートは管理者ダッシュボード内に設置され、用途に応じたレポートをワンクリックで作成することができます。これにより、ユーザー、グループ、パスワードに関する主要なリスク領域に関する情報を入手でき、適切なアクセス許可を確保することができます。

ご利用可能なレポートには以下が含まれますが、これらに限定されるものではありません。

- 機密ファイル
- アクセス許可
- 重複ファイル
- 冗長な時代遅れまたは些細な(ROT)
- データリスク評価



AIモデルと高度な自動制御を駆使したForcepoint Data Visibilityは、従来の方法よりも迅速かつ正確なデータの可視化、分類、継続的な監視を実現します。機密性の高い知的財産、個人情報と無意味なファイルの山を簡単に識別し、区別することができます。エンドユーザーが容易に生産性を維持しながら、最小限の特権アクセスで流出を防ぐことができます。さまざまな情報ソース（ファイルサーバー、Microsoft OneDrive、SharePoint、Google Drive、Box、Confluence、Azureなど）のデータを俯瞰できるForcepoint Data Visibilityは、完全なデータセキュリティアプローチに必要な不可欠な構成要素です。

AIベースのData Visibilityに移行する準備はお済みですか？



詳細を見る

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](#) で [LinkedIn](#) で Forcepointをご覧ください。