わかる！
Box Shield

AI時代に欠かせないデータセキュリティを
AIで自動化・効率化する

box SHIELD

人間の故意・不注意、サイバー攻撃による情報漏えいを防ぐ

経営戦略資料、財務文書、顧客から受領した書類など、企業内には重要なコンテンツが膨大にあります。これらの情報の漏えいは、ビジネスに重大な影響を与えかねません。

機密情報は常に狙われています。社外からのサイバー攻撃、社内での内部不正から重要な情報を確実に保護する必要があります。不注意による意図しない情報漏えいもありえます。

情報漏えいから大切なデータを守るには、ファイル単位で保護する「データセキュリティ」が欠かせません。

情報セキュリティ10大脅威

順位	「組織」向け脅威	初選出年	10大脅威で取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	11年連続11回目
2	サプライチェーンや委託先を狙った攻撃	2019年	8年連続8回目
3	AIの利用をめぐるサイバーリスク	2026年	初選出
4	システムの脆弱性を悪用した攻撃	2016年	6年連続9回目
5	機密情報等を狙った標的型攻撃	2016年	11年連続11回目
6	地政学的リスクに起因するサイバー攻撃	2025年	2年連続2回目
7	内部不正による情報漏えい等	2016年	11年連続11回目
8	リモートワーク等の環境や仕組みを狙った攻撃	2021年	6年連続6回目
9	DDoS攻撃（分散型サービス妨害攻撃）	2016年	2年連続7回目
10	ビジネスメール詐欺	2018年	9年連続9回目

「情報セキュリティ10大脅威 2026」（情報処理推進機構 2026年1月）

ランサム攻撃による被害
- ✕ ランサムウェアを検出できない
- ✕ ランサムウェアの拡散を防げない

サプライチェーンや委託先を狙った攻撃
- ✕ 外部企業、外部ユーザーのセキュリティ管理が困難

内部不正による情報漏えい等
- ✕ 退職予定者による情報持ち出しを検出できない

機密情報等を狙った標的型攻撃
- ✕ 悪意のある攻撃ファイルを検出できない
- ✕ 攻撃ファイルの実行を防げない

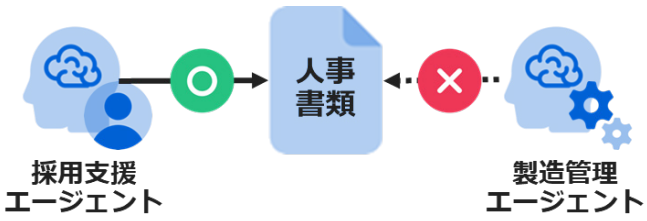
リモートワーク等の環境や仕組みを狙った攻撃
- ✕ 機密情報のダウンロードによる情報漏えいを防げない

不注意による情報漏えい等
- ✕ 不適切なアクセス権付与による情報漏えいを防げない

AIエージェント時代により重要となるデータセキュリティ

「AIエージェントは秘密を守れません。」たとえ間違っていても、与えられた情報はすべて利用します。AIによる情報漏えいを防ぐためには、データセキュリティが今まで以上に重要です。

AIエージェントがアクセスできる情報はAIを利用するユーザーと同一にして、AIからも機密情報を保護する必要があります。



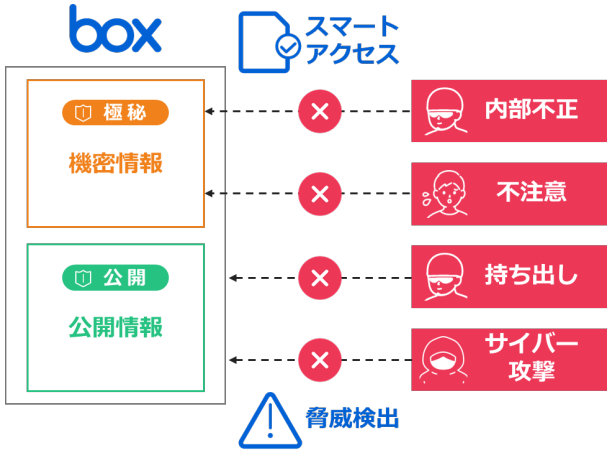
Box Shield 2つのアプローチで情報漏えいを防ぐ

スマートアクセス

- ✓ コンテンツを機密度で分類
- ✓ 機密度に応じて共有、招待、ダウンロード、印刷を制限
- ✓ 特定の識別子や用語で自動分類
- ✓ Microsoft Purview Information Protectionの秘密度ラベルと連携

脅威検出

- ✓ 機械学習を活用して脅威を検出
- ✓ 異常なダウンロード、悪意のあるコンテンツ、不審な場所からのアクセス、不審なセッションを検出



ランサム攻撃による被害
- ○ ランサムウェアの検出、拡散防止
- ○ プレビューによる業務継続、ファイル復元

サプライチェーンや委託先を狙った攻撃
- ○ ドメイン許可リストによるサプライチェーンの弱点排除

内部不正による情報漏えい等
- ○ 大量ダウンロードなどの不正の検出
- ○ 最大7年間の監査ログ

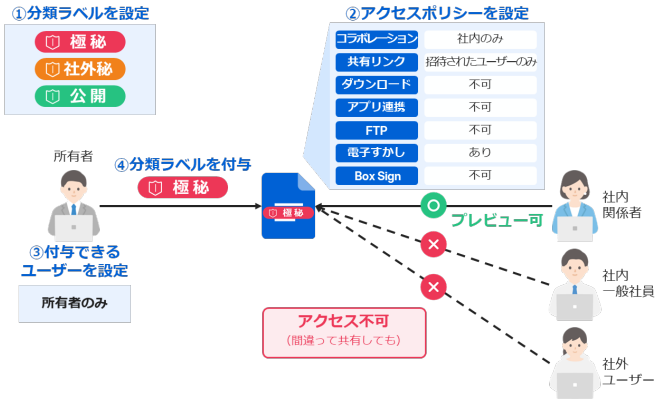
機密情報等を狙った標的型攻撃
- ○ 攻撃ファイルの検出
- ○ プレビューによる攻撃実行の抑制

リモートワーク等の環境や仕組みを狙った攻撃
- ○ ダウンロードを禁止しながらプレビューやオンラインで業務可能

不注意による情報漏えい等
- ○ 分類ラベルによるアクセス制御
- ○ 分類ラベルの自動付与

Box Shield　内部不正・不注意・マルウェア攻撃からコンテンツを保護

スマートアクセス



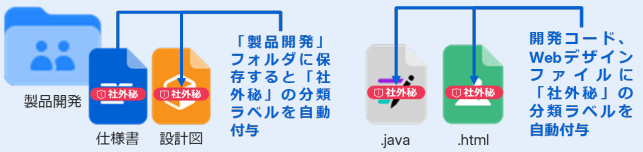
コンテンツに分類ラベルを付与することで、分類ラベルに設定されたアクセスポリシーを適用し、コンテンツを保護できます。

アクセスポリシーでは、共有範囲、社外ユーザーの招待、ダウンロード、印刷などの制限、電子すかしの表示ができます。

分類ラベルは手動で付与するほかに、自動付与することもできます。特定のフォルダへの保存、特定の拡張子、特定の識別子や用語で、対応する分類ラベルを自動的に付与できます。

また、Microsoft Purview Information Protectionの秘密度ラベルをインポートして、対応する分類ラベルを付与することもできます。

保存先フォルダ、拡張子による自動分類

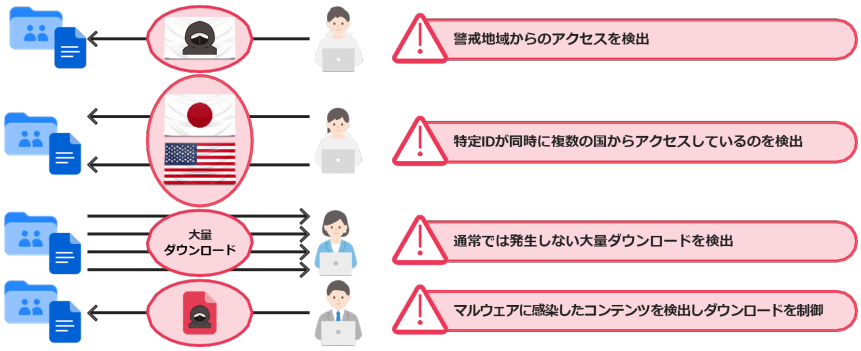


特定の識別子、用語による自動分類

クレジットカード番号やパスポート番号など

特定の用語

脅威検出



ユーザーの異常な行動、不審な場所やセッションのアクティビティ、特定された悪意のあるコンテンツに基づいて、アカウントの侵害やデータの盗難などの潜在的な脅威に関する詳細なアラートが表示されます。

さらに、不審な行動をしているアカウントのアクセスを制限したり、悪意のあるファイルのダウンロードを制限したりできます。

Box Shield Pro　AIでデータセキュリティを自動化・効率化

コンテンツのデータ分類には、課題があります。手作業による分類は属人的で、必ずしも適切に分類されるわけではありません。そして、これまでに自動分類は、特定の識別子や特定のキーワードがコンテンツに含まれている必要がありました。

これらの課題をAIが解決します。AIでデータセキュリティを自動化、効率化することで、コンテンツをこれまで以上に適切に保護できます。

手作業	✕ 属人的 ✕ 分類し忘れることがある ✕ 必ずしも適切に分類されるわけではない
これまでの自動分類	✕ 特定の識別子を含んでいる必要がある（クレジットカード番号、パスポート番号など） ✕ 特定のキーワードが書かれている必要がある（「極秘」「社外秘」など）
AIによる自動分類	○ AIがコンテンツの意味、価値、目的を理解して内容に応じて適切に分類

AI分類エージェント

コンテンツの機密性をわかりやすいプロンプトで定義して、その定義やコンテンツのコンテキストに応じて適切な分類ラベルを自動適用

ランサムウェアアクティビティ検出

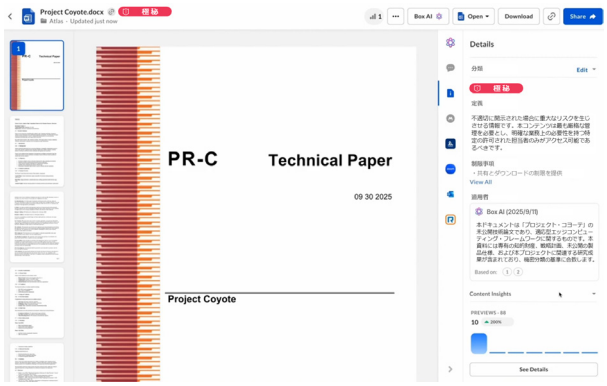
Box Drive内でランサムウェア攻撃を検出し、アラートとともに、セッションを終了したり、影響を受けたコンテンツを復元

AI脅威分析エージェント

提供予定

AIエージェントがBox Shieldの脅威アラートを分析し、重要な情報をわかりやすく要約

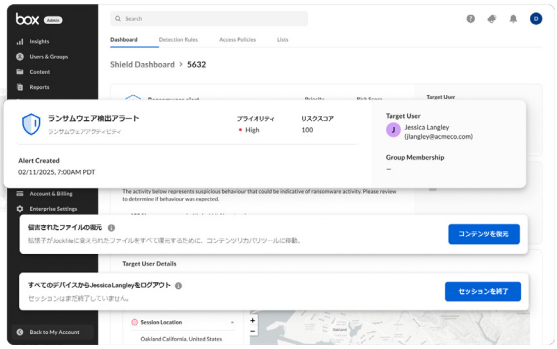
AI分類エージェント



デモを見る

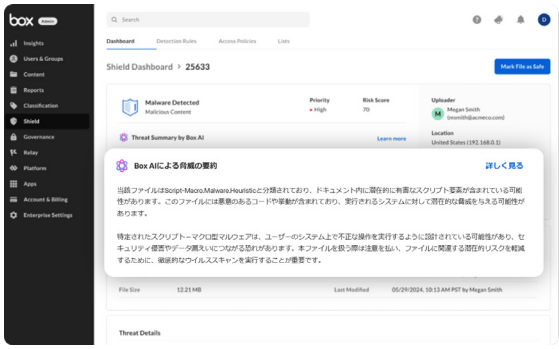
各分類ラベルの定義をわかりやすい言葉で記述できます。たとえば、「将来の財務戦略に関する重要な説明」が含まれている場合は「機密」、「従業員研修に関連するコンテンツ」には必ず「社内限り」を適用するよう指示できます。そして、AI分類エージェントがコンテンツの内容を分析し、微妙なニュアンスを理解して、適切な分類ラベルを自動的に付与します。

ランサムウェアアクティビティ検出



Box Drive内でランサムウェア攻撃を検出し、アラートとともに、侵害されている可能性のあるセッションを終了したり、影響を受けたコンテンツを復元できます。

AI脅威分析



AIエージェントがBox Shieldの脅威アラートを分析し、重要な情報をわかりやすく要約。セキュリティ担当者は、脅威を優先順位付けしてより迅速に対応できます。

Box Shield/Box Shield Proは、Enterpriseプラン以上でご利用いただけます

プランの詳細

	Business	Business Plus	Enterprise	Enterprise Plus	Enterprise Advanced
Box Shield			追加可	●	●
Box Shield Pro			**追加可**	**追加可**	**追加可**

エバンジェリストがお届けする
Box導入検討中なら必見！
すべての機能がまるわかり
Box製品セミナー
毎週水曜日 15:00開催

Boxの導入を検討している人必見！ すべての機能がまるわかり

Box製品セミナー

Boxのエバンジェリストが、お客様が抱えているビジネス課題を「Box」でどのように解決できるかを導入事例を交えてご紹介します。さらに、プランごとに使えるBoxの機能、最新機能を活用して業務を変革する具体的な方法もご紹介します。

参加申し込みはこちら
（オンライン・無料）

株式会社Box Japan
〒100-0005
東京都千代田区丸の内1-8-2 鉄鋼ビルディング15階
japan.box.com
Box導入に関するお問い合わせ
japan.box.com/inquiry
Box製品ご購入後のサポートに関するお問い合わせには返信できませんので、予めご了承ください。

販売代理店