

# 情報漏洩防止ソリューション 秘文



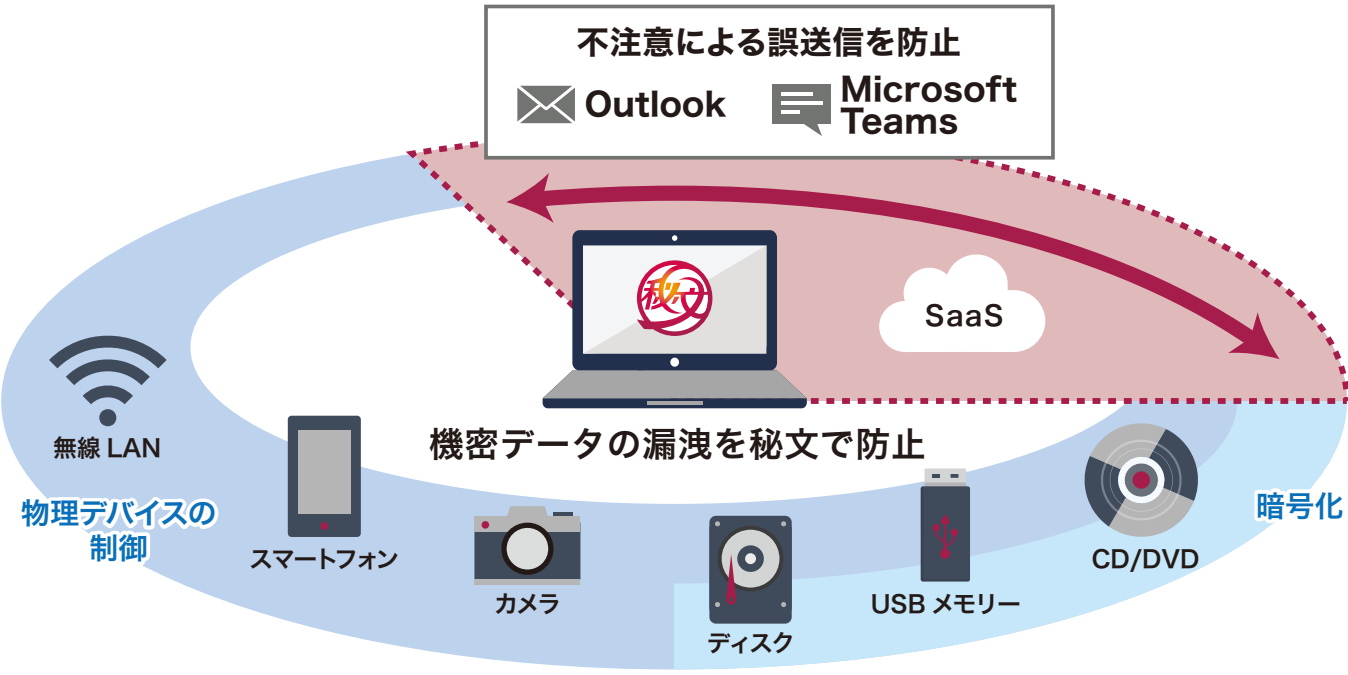
さまざまなセキュリティ脅威から  
エンドポイントを守り  
企業に安全・安心を提供します

# 情報漏洩のきっかけは“持ち出し”から“共有”へ クラウド利用などで変化するリスクに、適応できる対策を

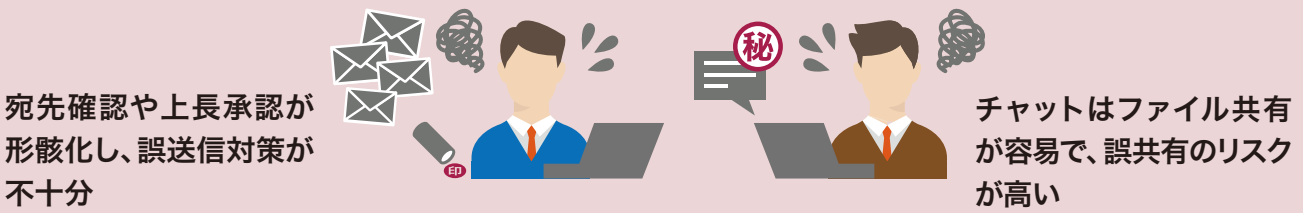
秘文は、1996年にリリースして以来、長年にわたり培ってきたセキュリティ対策のノウハウや開発技術を生かし、時代のニーズや変化するセキュリティリスクに対応した製品・機能を提供してきました。

最近では、Microsoft Outlook や Microsoft Teams の活用によりデータ共有方法が変化しています。社外との情報共有がより迅速かつ円滑になっている一方で、改めて課題となっているのが、人の不注意に起因する情報漏洩リスクです。秘文はこうした環境の変化に対応し、Outlook や Microsoft Teams からの情報漏洩対策を提供することで、安全な情報共有を支援します。

## Outlook、Microsoft Teams のセキュリティ対策機能を強化

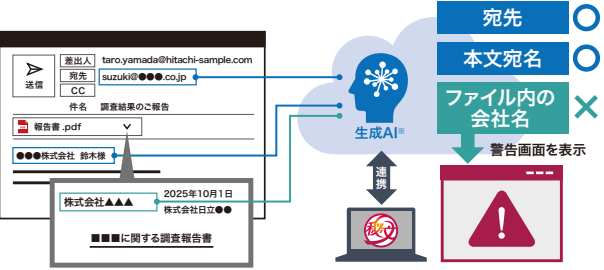


## 社外とのデータ共有でこのような課題はありませんか？



## 生成AIと連携した宛先・添付ファイルの自動チェック

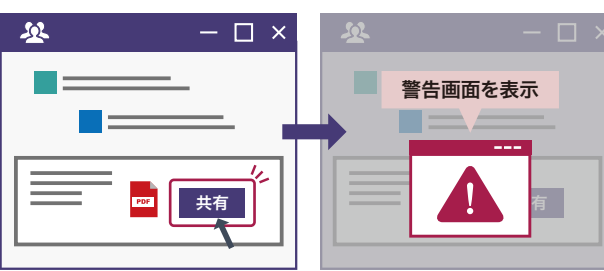
メールの宛先に指定しているメールアドレス、メール本文に記載している宛名、添付ファイル内の会社名に矛盾がないか、生成AIと連携して自動でチェック。ユーザーに気づきを与えることで、宛先間違いや添付ファイルの誤りといった不注意による情報漏洩を防止します。



※本機能を利用する場合、お客さまにて別途 Azure OpenAI の契約、構築・運用が必要です。  
なお、Azure OpenAI の対応モデル以外の利用や、ローカル LLM (Large Language Model) との連携を希望される場合は、個別にご相談ください。

## 社外メンバーへのデータ共有時の警告

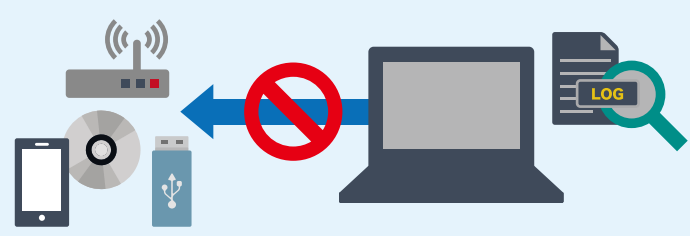
社外メンバーが参加している Microsoft Teams のチャットやチャンネルに、ファイルや Microsoft SharePoint のファイルリンクを共有した際、秘文が警告アラートを表示。警告画面を表示することで、確認不足による情報漏洩のリスクを低減します。



## エンドポイントからの情報漏洩を防ぐさまざまな機能

### 内部不正対策

USBメモリやスマートフォンなどのデバイス利用やネットワーク接続を制御し、不正なデータ持ち出しを防止。操作ログの取得・管理によりデータの持ち出し内容の確認・不正行為の抑止が可能です。



### 盗難紛失対策

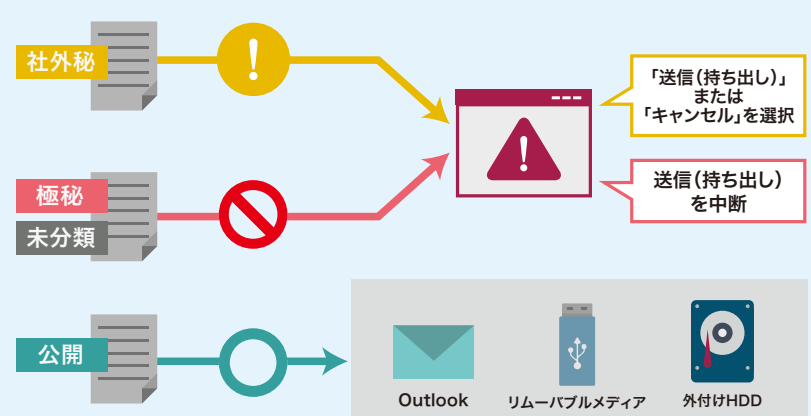
PCのハードディスクや記録メディア、ファイルサーバー上のフォルダなどを暗号化し、情報漏洩を防止。外部媒体への持ち出し時に暗号化を強制することで、暗号化し忘れたデータの社外持ち出しを防止できます。



### 機密情報分類サービス連携オプション

※機密情報分類サービスの利用が前提となります

機密情報分類サービスが付与する秘密度ラベルに応じて、社外宛メールや外部記憶媒体（リムーバブルメディア、外付けHDD）経由でのファイル持ち出しを制御。秘密度が未判定のファイルについては判定を必須化することで、企業の情報管理規則に沿った持ち出し運用を支援します。



\*秘文 Device Controlのリムーバブルメディア／外付けHDD経由の対策機能は、2026年10月末にリリース予定です。

お客さまの環境やニーズに合わせてクラウドやオンプレミスを選択できます

■主な機能 ●は標準機能 \*は秘文 Serverが必要な機能

| 機 能                     |                              | 概 要                                                                                                                                                              | サービス版<br>(クラウド版)<br>秘文 Endpoint<br>Protection Service | オンプレミス版<br>(一部スタンドアロン利用可能)<br>秘文 Device<br>Control    秘文 Data<br>Encryption |    |
|-------------------------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|-----------------------------------------------------------------------------|----|
| Microsoft 365<br>情報漏洩対策 | Outlook 向け<br>情報漏洩防止         | ユーザーが Outlook でメールを送信する際、<br>秘文が生成AIと連携してメールの宛先(メー<br>ルアドレス、メール本文に記載している宛名、<br>添付ファイル内の会社名)をチェックします。<br>※生成AI連携機能の利用には、お客さまにて<br>別途 Azure OpenAI の契約、構築・運用が必要です。 | ●                                                     | ●                                                                           | —  |
|                         | Microsoft Teams 向け<br>情報漏洩防止 | 社外メンバーが参加している Microsoft Teams<br>のチャットやチャンネルに、ファイルや Microsoft<br>SharePoint のファイルリンクを共有した際、<br>秘文が警告アラートを表示します。                                                  | ●                                                     | ●                                                                           | —  |
| 内部不正対策                  | デバイス制御                       | PCからファイルを持ち出すことができるデバイ<br>スを制御することで、不正コピーを防止します。                                                                                                                 | ●                                                     | ●                                                                           | —  |
|                         | ネットワーク制御                     | スマートフォンのテザリング防止や、接続先の<br>ネットワークを制御することで、ネットワークを<br>経由した情報漏洩を防止します。                                                                                               | ●                                                     | ●                                                                           | —  |
|                         | ログ取得・管理                      | ファイル操作やアプリケーション操作、ブラウ<br>ザー操作などPC上でのユーザー操作をログと<br>して取得します。(一部オプションです)                                                                                            | ●                                                     | ●*                                                                          | —  |
|                         | ユーザーへの<br>アラート通知             | 秘文のポリシーによって禁止している操作を<br>行った際に、ユーザーにアラートを通知します。                                                                                                                   | ●                                                     | ●                                                                           | —  |
|                         | アプリインストール<br>制御              | 管理者が許可したアプリケーションのみインス<br>トールを可能にすることで、ユーザーが勝手に<br>未許可のアプリケーションをインストールする<br>ことを防ぎます。                                                                              | ●                                                     | ●                                                                           | —  |
| 盗難紛失対策                  | ハードディスクの<br>暗号化              | PCに保存されたファイルをドライブ単位で強<br>制的に暗号化します。                                                                                                                              | ●                                                     | —                                                                           | ●  |
|                         | ファイル暗号化                      | 社外に提供するファイルを、ユーザー自身がパ<br>スワード入力で復号できる形式に暗号化します。                                                                                                                  | ●                                                     | —                                                                           | ●  |
|                         | ファイルサーバーの<br>暗号化             | ファイルサーバー上のファイルを共有フォルダ<br>単位で自動的に暗号化して保護できます。                                                                                                                     | ●                                                     | —                                                                           | ●* |
| 外部脅威対策                  | ファイル保護                       | 信頼できる証明書で署名されているなど安全<br>性が確認できるプログラムのみ、機密データや<br>OS管理領域(Master Boot Recordなど)への<br>アクセスを許可します。                                                                   | ●                                                     | —                                                                           | ●  |

■その他の秘文製品 (オプション製品)

秘文AE ContentsGate / 秘文AE ContentsFilter \*1

より厳密な持ち出し制限を実現

✔ファイル単位の持ち出し制御    ✔申請・承認ワークフロー

秘文 File Encryption

簡単にファイル暗号化が可能

✔ファイル暗号化

秘文AE 開発キット

秘文の暗号化/復号機能をAPIで提供

✔ファイル暗号化/復号用API

\*1: 秘文 Device Controlが前提です。

※秘文は、株式会社日立ソリューションズの登録商標です。※Microsoft(Azure、Microsoft 365、Microsoft Teams、Outlook、SharePoint)は、マイクロソフトのグループ企業の、米国およびその他の国における商標または登録商標です。※その他、本カタログ中の会社名、商品名は各社の商標、または登録商標です。※本文中および図中では、TMマーク、®マークは表記しておりません。※製品の仕様は、改良のため、予告なく変更する場合があります。※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認のうえ、必要な手続きをお取りください。なお、ご不明な場合は、当社担当営業にお問い合わせください。※本カタログ中の情報は、カタログ作成時点のものです。最新の情報はWebサイトをご確認ください。

