

TOSHIBA

生成AI利用時の個人情報保護対策

Fortra DLP

その生成AI利用、機密漏洩の「入り口」になっていませんか？

生成AIプロンプトからの情報漏洩のリスクは増加しています。
プロンプトにうっかり個人情報を入力していませんか？

- ☐ 社内チャットツールと同じ感覚でプロンプトに入力してしまう
- ☐ 作文するために顧客対応履歴や氏名・住所などをそのまま貼り付けてしまう
- ☐ 特許情報や知的財産が含まれたファイルを誤って生成AIにアップロードしてしまった

コピー漏洩

顧客情報や
設計値を誤って
AIに貼り付け送信

AI学習転用

入力データが
AIの学習に使われ、
他社回答に露出

攻撃の起点

流出情報を元に
標的型攻撃の
ターゲットに

クラウド上のAIモデルに機密情報が送信され、 漏洩リスクが生じる危険性があります！！

＜個人情報流出し悪用されるまでの流れ＞



Fortra DLP なら

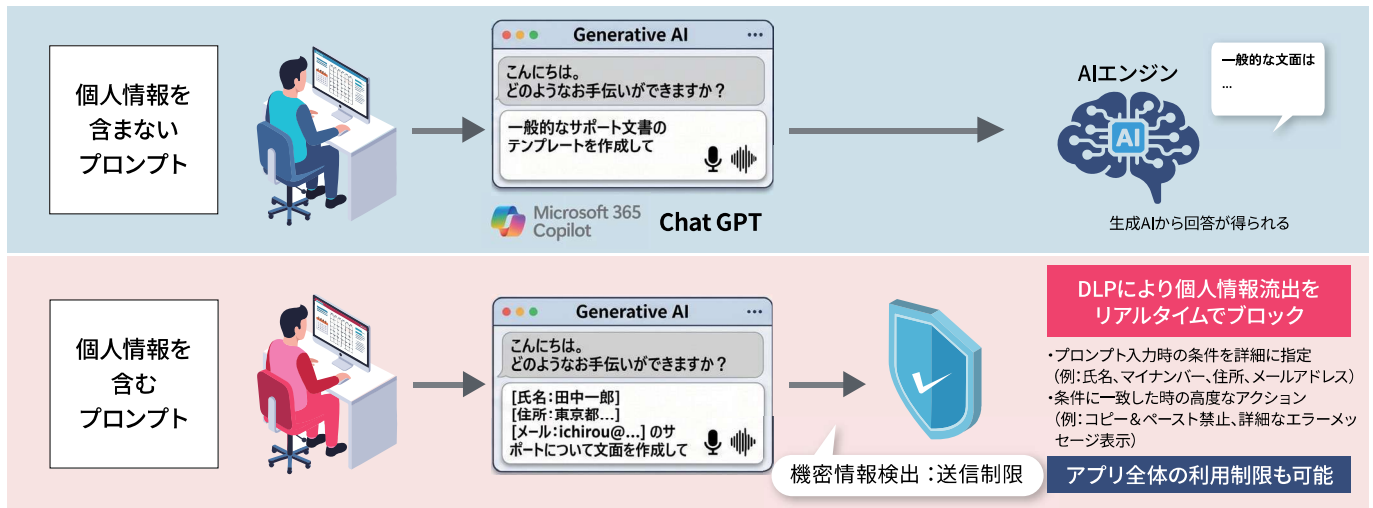
生成AI利用における個人情報流出対策が可能です！

Fortra DLPは、次世代のデータ保護プラットフォームです。

エンドポイント・ネットワーク・クラウド環境における機密データの外部流出を確実にブロック。エンドポイントに存在するデータのコピーや外部送信といったアクティビティを把握し、リスクを徹底的に可視化します。



生成AIからの情報漏洩を防止する仕組み



Fortra DLP の4つの鉄板ガード



東芝デジタルエンジニアリングの4つのサービス



□本文中の会社名および製品名は各社が商標または登録商標として使用している場合があります。
□本資料は内容は予告なく変更される場合がありますのでご了承ください。

(LS00066)

東芝デジタルエンジニアリング株式会社

E-mail : TDEN-sales@ml.toshiba.co.jp

<https://www.toshiba-tden.co.jp>