



## 情報漏えい事故 御社は大丈夫 ですか？

### 企業の情報セキュリティに最適な情報漏えい防止ソリューション

電子文書を暗号化してユーザー認証及び権限を制御することにより情報漏えいを防止する根本的な対策

業務環境がデジタル化されて文書をデジタル環境へ保存及び共有することで業務の効率性は高くなりましたが、代わりに情報漏えい事故が非常に増えています。

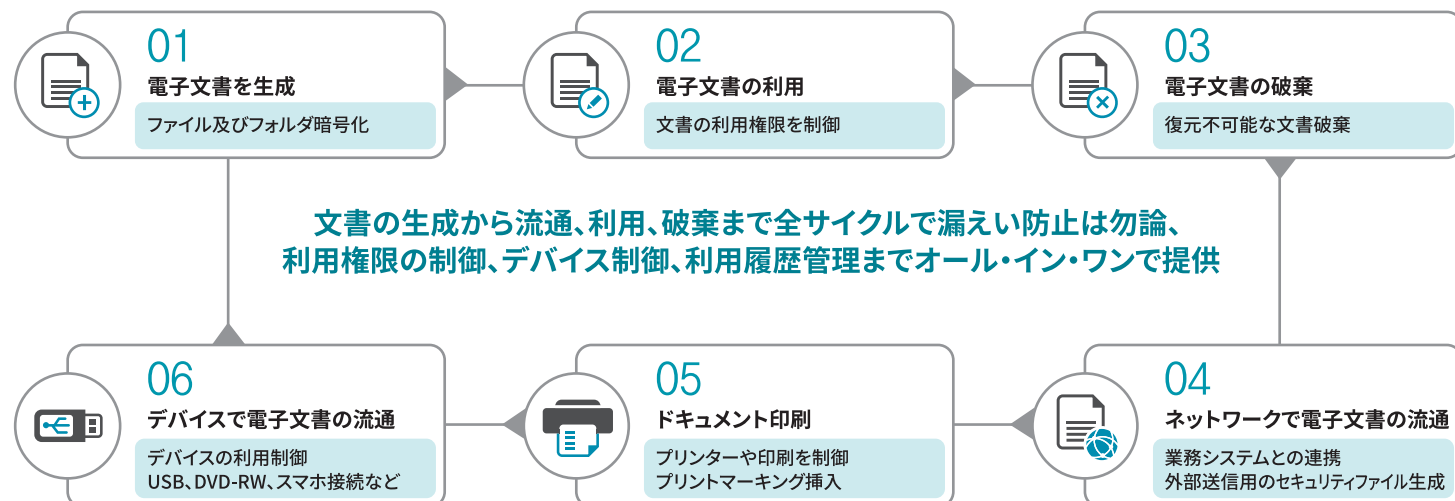
最近では内部関係者による個人情報漏えい事故やAPT攻撃のようなインテリジェンスなサイバーテロなど予測できない多様な脅威も企業内の機密情報を狙っているため情報漏えいに対する危険性が一段と高まっています。

そのため、内部関係者と外部攻撃による情報漏えいから根本的に防止できるドキュメントDRMソリューションが注目されています。



### Document Security

電子文書の生成、利用、流通、廃棄に至るまで全ての過程で情報漏えいを防止する最適な対策を提供します。



# ドキュメントE-DRM

# Document Security

## 01 導入対象

1	経営情報、企画、営業情報、個人情報など漏えいされると莫大な被害を発生する重要情報を保有している企業及び機関	2	外部とのやり取りが多く、漏えいしてはいけない情報を共有する必要がある企業及び機関
3	KMS、ERP、CRM、EDMSなど情報管理システムが導入されている企業及び機関	4	個人情報保護法、マイナンバー対策など情報セキュリティ関連法律に準拠する対策が必要な企業及び機関

## 02 製品機能

 <p><b>文書の利用権限制御</b> 閲覧(閲覧回数)/編集/印刷(印刷回数)/権限変更/透かし印刷の有無/有効期間/自動破棄などの権限制御 ユーザー/グループ別、文書の用途やカテゴリ別で権限設定が可能</p>	 <p><b>外部送信用のセキュリティファイル生成</b> DocumentSecurityが設置されていない環境でも認証や権限制御が可能 パスワード認証、印刷、保存、有効期間、閲覧回数、印刷回数、自動破棄などの権限を設定して共有</p>
 <p><b>ファイル暗号化</b> MS Office文書、PDF、TXT、イメージをセキュリティポリシーにより自動で暗号化、暗号化されたまま利用可能</p>	 <p><b>業務システムとの連携</b> グループウェア、ワークフロー、KMS、ERPなど既存業務システムと連携可能な暗号/復号ツール(API)を提供</p>
 <p><b>オフライン ログイン</b> セキュリティが維持された状態で業務の連続性をサポート 外出/出張、在宅勤務など管理サーバーへ接続できない状況でも文書の利用及び権限制御サポート 社内環境へ復帰時、オフライン状態での利用履歴を管理サーバーへ伝送と同時にオンライン ログイン状態へ自動切り替え</p>	 <p><b>統合履歴(ログ)の管理</b> 暗号化文書の生成/閲覧/編集/印刷/抽出/復号化など利用状況を収集 権限ポリシー設定や変更など管理者の設定履歴をログで収集</p>
	 <p><b>グループ管理者とサブ管理者設定機能</b> 業務特性に合わせたポリシー設定のためグループ単位の管理者機能 ログ閲覧のみの監査担当や一部の設定権限を制限するサブ管理者機能</p>

## 03 システム構成

