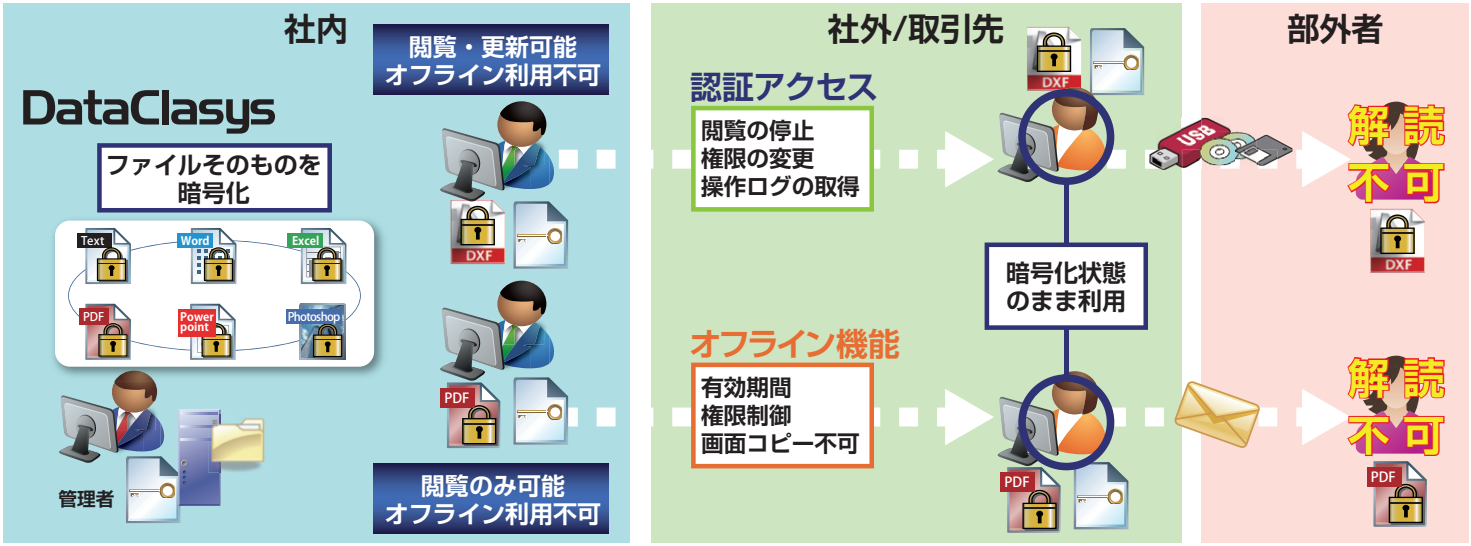
アプリを問わずに暗号化！
操作は変わらず漏洩防止！

DataClasys は、個人情報・顧客情報・営業情報・特許情報・図面・技術情報などの機密情報保護・管理と情報の共有化を両立するために、弊社独自の暗号化・DRM 技術を元に開発された機密情報保護・情報漏洩対策製品です。情報の重要性に基づいた「機密区分」を設定することで、あらゆるファイルを「ファイル単位」で暗号化、様々なアプリケーションで暗号化したまま利用することができます。
部署や職位に応じた「権限設定（閲覧・更新・印刷・オフライン利用等）」を行うことで、文書ごとの情報保護・管理を実現します。

データクレシス
DataClasys

充実のセキュリティと高い利便性を実現



ファイル形式に依存せずほぼ全てのファイルを暗号化して利用。持ち出されても情報の漏洩を防止！

✓ あらゆるWindows系ファイルを暗号化

- Microsoft Office、PDF などにも対応
- DTP、動画などのマルチメディア系ソフトにも対応
- CAD ソフト、エンジニアリング系ソフトにも対応
  ※異なるソフト間で暗号化ファイルを共有可能

✓ 暗号化したまま閲覧 / 更新可能

- ファイル名、アイコンおよび拡張子は変更されませんので通常の平文ファイルと同じ操作で利用可能
- 暗号化状態は保持されたまま利用することが可能

✓ 細やかな運用ルールを設定できます

- 閲覧 / 更新のほか、印刷 / スクリーンショット / コピー & ペースト / メール添付などを禁止
- ファイル更新時、外部ファイルへの書き出しを禁止（画像、CAD の中間ファイルなどを作らせない）

✓ 既存システムへの組込 / 連携が容易

- 既存の文書管理システムや PDM などとの連携や暗号化と他の動作と連携させることにより一連の動作を自動化することが可能

✓ 社外・委託先でも安全に利用可能

- 国内外の拠点へ機密ファイルを暗号化して配布
- 社外や通信環境がない環境での利用でも暗号化したまま利用が可能、漏洩を防止
- 利用期限、利用端末の制限により安全に利用可能

✓ 自社開発ならではの柔軟な対応

- お客様の具体的な利用シーンでの求められるご要望をバージョンアップで実現
- OS やアプリケーションのバージョンアップに迅速に追随

電子政府推奨暗号アルゴリズム、特許取得した鍵配信技術に裏打ちされた高信頼システム

様々な業種で、様々な部門で、様々な情報を保護します！

利用実績のある主なアプリケーション

マイクロソフト	Word/Excel/PowerPoint（32/64bit）、OneNote、Access、Publisher、Visio、メモ帳、ワードパッド、ペイント、Windows Media Player、Windows フォトギャラリー、OfficeViewer（Word/Excel/PowerPoint/Access Snapshot Viewer）
アドビシステムズ	Acrobat、Reader、Photoshop、Illustrator
ジャストシステム	一太郎、花子
富士ゼロックス	DocuWorks、TIFF Viewer
Apache ソフトウェア財団	OpenOffice
The Document Foundation	LibreOffice
ファイルメーカー	FileMaker Pro
シーメンス PLM ソフトウェア	NX、JT2Go

オートデスク	AutoCAD、AutoCAD Mechanical、AutoCAD LT（2009 以降）、Inventor、Inventor View、DWG TrueView、Vault
ダッソー・システムズ	SolidWorks、CATIA、eDrawings Viewer、SmarTeam
PTC	Creo Parametric、WindChill
Jiro Shimizu & Yoshifumi Tanaka	Jw_cad
富士通	iCAD SX、iCAD MX
ECAD ソリューションズ	ECAD dio
アンドール	CADSUPER FXII
シスプロ	Walkinside、DesignDraft
IdeaMK Inc.	IGS Viewer
ラティス・テクノロジー	XVL Player

連携実績のある主なアプリケーション

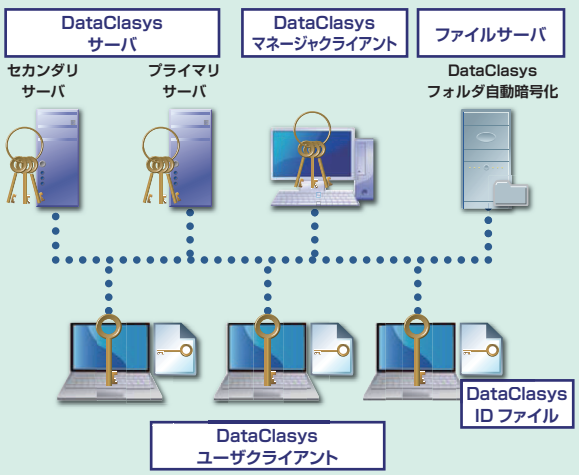
インフォコム	MySAFER
ウイップス	SecureFiles+
シャープマーケティングジャパン	データセキュリティサービス
Aras Corporation	Aras Innovator
アララ	P-Pointer File Security

ジャストシステム	ConceptBase Enterprise Search
NSD ビジネスイノベーション	eTransporter
富士ゼロックス	ArcSuite Engineering
日本 CA	Arcserve Replication

※上記以外にも検証結果により随時対応が可能です。　※動作を保証するものではありません。お客様環境によって個別設定が必要になる場合があります。

DataClasys 利用環境

基本構成



動作環境（ソフトウェア／対象 OS）	
DataClasys ユーザクライアント	Windows XP（32bit）、Windows Vista（32/64bit）、Windows 7（32/64bit）、Windows 8（32/64bit）、Windows 8.1（32/64bit）、Windows 10（32/64bit） 注）仮想デスクトップの上記ゲスト OS でも動作可能。＊1 注）ドライバ無し版でインストールする場合は上記に加え Windows Server 2008/2008 R2、Windows Server 2012/2012 R2/2016 で動作可能。
DataClasys マネージャクライアント	Windows XP（32bit）、Windows Vista（32/64bit）、Windows 7（32/64bit）、Windows 8（32/64bit）、Windows 8.1（32/64bit）、Windows 10（32/64bit）、Windows Server 2008（32/64bit）/2008 R2（64bit）、Windows Server 2012（64bit）/2012 R2（64bit）、Windows Server 2016（64bit） 注）仮想デスクトップの上記ゲスト OS でも動作可能。＊1
DataClasys サーバ	Windows Server 2008（32/64bit）/2008 R2（64bit）、Windows Server 2012（64bit）/2012 R2（64bit）、Windows Server 2016（64bit） 注）仮想プラットフォームの上記ゲスト OS でも動作可能。
DataClasys 自動暗号化サーバ＊2	Windows Server 2008（32/64bit）/2008 R2（64bit）、Windows Server 2012（64bit）/2012 R2（64bit）、Windows Server 2016（64bit） 注）仮想プラットフォームの上記ゲスト OS でも動作可能。
データベース	PostgreSQL
暗号方式	公開鍵暗号方式と共通鍵暗号方式のハイブリット ◎公開鍵：RSA（鍵長 2048 ビット）　◎共通鍵：AES（鍵長 256 ビット）

※仮想環境での動作は、仮想プラットフォームを提供するベンダにより動作保障範囲が異なるため、お客様による障害切分けを前提としてお使いいただくことがあります。
＊1 仮想デスクトップは VDI/SBC 方式に対応。（方式によって個別設定が必要になる場合があります）
＊2 NAS などの専用 OS で動作するファイルサーバを対象にフォルダ自動暗号化を設定する場合に必要となります。

※記載の商品名、会社名は一般に各社の商標または登録商標、サービスマークです。※本カタログに記載された仕様・意匠については改良のため予告なく変更することがありますのでご了承ください。
※既存システムへの組込み連携が可能な DataClasys 開発キット（オプション）をご用意しています。※メーカーによるサポート終了製品への対応はご相談ください。

株式会社 DataClasys（データクレシス）

本　　社：〒101-0032 東京都千代田区岩本町1-10-5 TMMビル7F
TEL.03-3861-2348
大阪支店：〒532-0003 大阪市淀川区宮原5-1-28 新大阪八千代ビル別館2F
TEL.06-7174-8632
福岡支店：〒812-0013 福岡市博多区博多駅東2-15-19 KS･T駅東ビル7F
TEL.092-472-1792
URL：https://www.dataclasys.com/

お問い合わせは

180928