NESCO

機密情報ファイル 保護・管理システム

DataClasys

データクレシス

アプリを問わずに暗号化！
操作は変わらず漏洩防止！

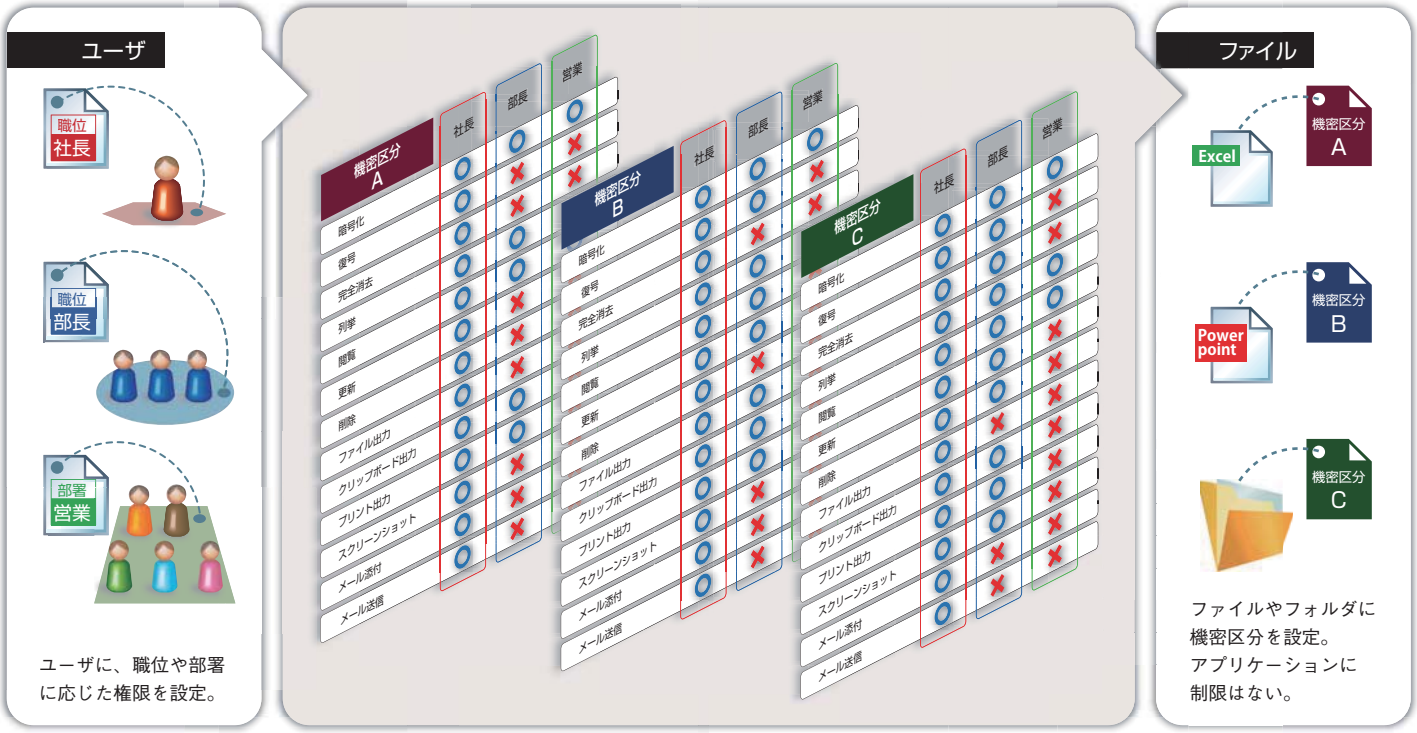
株式会社ネスコ

DataClasysによって実現される「情報共有」と「機密情報保護・管理」

▶▶ キーワードは、「ファイル単位」、「機密区分」、「権限設定」。

DataClasysは、企業や行政といった組織の内外を通じて機密性の高いファイルを安全に共有するDRM製品です。

DataClasysは、Microsoft Officeはもとより、AutoCADやSolidWorksなどのCADアプリケーションを含むほぼ全てのアプリケーションで利用でき、暗号化ファイルを暗号化したまま閲覧・更新できます。暗号化したまま利用するため、第三者にファイルが流出しても、管理者が許可した利用者しか暗号化ファイルを解読することができません。その上、コピー&ペーストや印刷、ウェブ送信など、暗号化ファイルの内容を抜き取る操作も制限できるため、第三者による不正アクセスや流出だけでなく、利用を許可した者からの情報漏洩も防止します。また、OSのドライバレベルで制御されるため、セキュリティホールの少ない安全性の高いDRM製品です。



DataClasys

利用しようとしているファイルに設定された機密区分と、職位・部署に基づいて
ユーザに付与された権限を元に、DataClasysがユーザアクションの可否を決定し情報の管理・保護を行う。

DataClasysのコンセプト Concept

ファイルの重要度による効果的な管理

DataClasysはファイルの重要度に応じて「極秘」、「社外秘」、「取り扱い注意」などといった「機密区分」を設定し、ファイル単位、フォルダ単位での管理が可能なため、本来守るべき情報資産を的確に管理できます。また、「機密区分」に対し、利用者の所属や職位に応じて権限を付与します。例えば、「営業部のA課長」には「極秘ファイルは閲覧のみ」、「社外秘ファイルは更新・印刷を許可」といったような、画一的ではない、ユーザの利用実態に応じた権限設定が可能です。

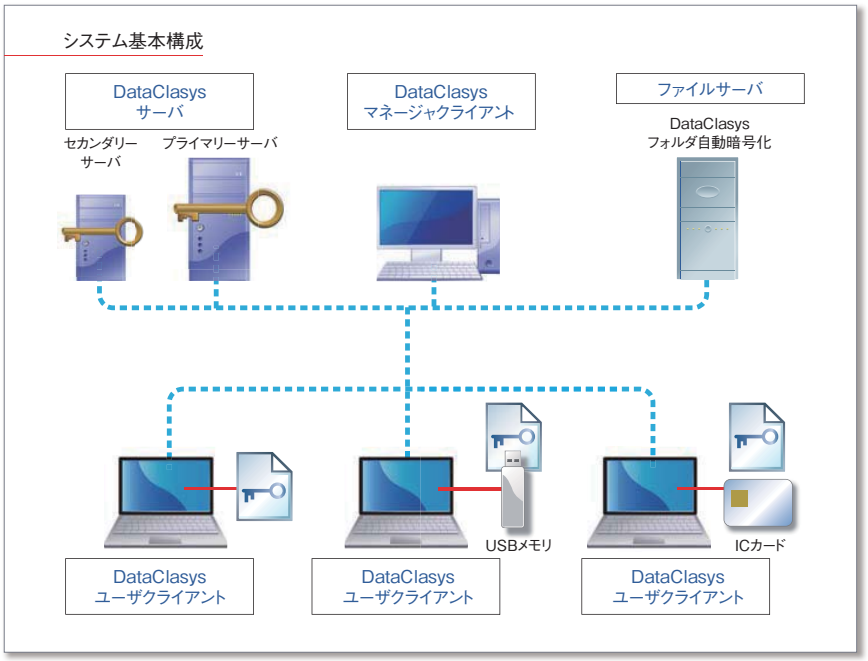
ファイルを重要度に応じて管理することは、単なる情報漏洩対策だけでなく、ISMS（ISO/IEC27001）やBS7799などの情報セキュリティ認証基準に則した管理です。また、SOX法や不正競争防止法や証券取引法などの企業ガバナンス＝内部統制強化のための前提となります。

経済産業省の不正競争防止法に関する営業機密管理指針では「営業秘密を適切に管理することは、不正競争防止法による営業秘密保護のための要件の1つである秘密管理性の重要な要素となるため、法的保護を受けるための前提条件である。いかに価値の高い情報であったとしても、その情報が秘密として適切に管理されていなければ、法的保護を受けることはできない」と記述されています。したがって、ファイルの機密管理は個人情報保護だけではなく、企業の営業上重要な顧客情報や技術情報、知的財産、ノウハウなどの法的保護を受け、企業を防衛していくための前提条件となる管理です。

大規模ネットワークにも適応できる運用性 Operation

サーバの二重化により、大規模ネットワークでの運用にも対応

DataClasys は、大規模ネットワークでの運用に不可欠な耐障害性の向上を、サーバの二重化により実現しております。
通常版の DataClasys サーバは PostgreSQL を搭載しており、ダンプ、リストアすることでコピーサーバを構築する事ができます。
2 台の DataClasys サーバがネットワーク内で稼動していると、DataClasys ユーザクライアントはプライマリの DataClasys サーバと通信できない場合に、セカンダリの DataClasys サーバに自動的に接続します。
これにより、アンストッパブルなネットワーク環境が要求されるクリティカルな業務環境においても、より安定性の高い堅実なセキュリティ環境を構築する事が可能です。
また、既存のファイルサーバ内のファイルも、フォルダ自動暗号化設定を行えば管理できるため、既に運用されているネットワーク環境への導入も簡単に行う事が可能です。



DataClasys サーバ
利用者の利用権限についての判断を行い、権限に応じた復号用の鍵情報などを配信するプログラムです。DataClasys ID ファイルを持つ利用者に対し、DataClasys ユーザクライアントがインストールされていれば、どの PC からでも各々の権限に応じた機密ファイルの利用を可能とします。

DataClasys マネージャクライアント
ユーザ登録、利用権限の付与、管理者権限の付与、ユーザ操作履歴の管理などを行うプログラムです。

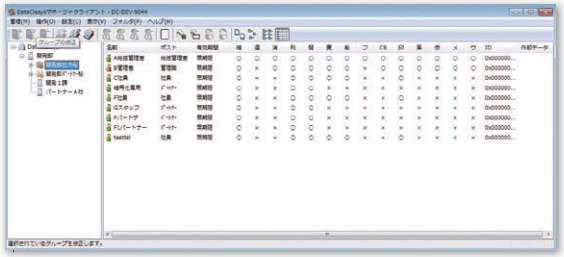
DataClasys ユーザクライアント
利用者の PC で動作するプログラムです。

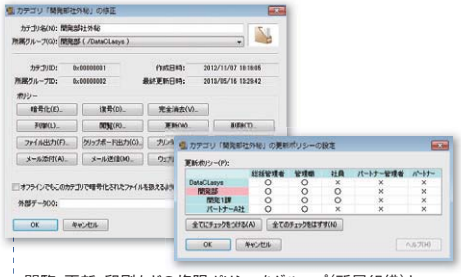
DataClasys ID ファイル
利用者が持つ鍵情報ファイルです。機密ファイルを利用する際に必須であり、本人認証などを行ったりする重要なファイルです。USB メモリ・トークンや IC カードなどに格納し、より安全に管理することが可能です。退職や異動などの決まっている社員に対しては事前に有効期間の設定も可能です。

フォルダ自動暗号化
ファイルサーバなどの共有フォルダ内に新しいファイル、更新されたファイルが保存されたかを監視し自動的に暗号化します。どの機密区分で暗号化するかは設定時に指定します。既存のサーバ・フォルダも自動暗号化設定可能です。また、クライアント PC 内の特定のフォルダ内のファイルを自動暗号化することも可能です。

社員の異動や退職、大量のユーザ情報登録などにも迅速に柔軟に対応

DataClasys は、企業や行政などの大規模な組織で利用されることを前提に権限管理できるよう設計されています。
グループや個人の権限をひとつひとつ設定するような面倒な作業の必要はありません。また、大規模組織でのユーザ管理で非常に負荷のかかる異動や組織変更などの処理にも柔軟に対応しております。
管理画面からの設定方法に加え、CSV フォーマットのファイルでのインポートによるユーザ登録・変更の一括入力機能や、異動・組織変更情報の事前登録による予約設定機能、操作範囲（組織範囲）を限定してのアドミニストレータ権限の委譲機能による管理業務の分担化・組織化など、運用する上で想定される様々なシーンに迅速・簡単に対応できるよう、豊富な機能を実現しております。


DataClasysマネージャクライアント画面


閲覧、更新、印刷などの権限ポリシーをグループ（所属組織）とポスト（職位）のマトリックスに○×で設定します。


DataClasysマネージャクライアントユーザ設定画面
部署別に開始、終了期限を設定することにより予約、兼任期間を設定することが可能です。

ActiveDirectoryとの連携に対応（※オプション製品「AccountSync」）

DataClasys のオプション製品「AccountSync」では、ActiveDirectory のユーザ情報を DataClasys へ連携することが可能です。
ユーザ同期機能により、ActiveDirectory ユーザの登録・変更・削除・認証失効を自動で DataClasys へ反映します。ユーザの属性値（メールアドレスや有効期限）は、運用に応じて ActiveDirectory の任意の項目から設定することが可能です。
ActiveDirectory ユーザの任意の属性値を指定することで、DataClasys のグループやポストへ自動的に振り分けることができます。

DataClasys のコアテクノロジー Core technology

アプリを問わずに暗号化！操作は変わらず漏洩防止！

アプリを問わずに暗号化！

DataClasys は、当社独自の暗号化・DRM 技術により、アプリを問わずに暗号化・DRM 管理を実現します。PDF や TIFF などに変換することなく、オリジナルのアプリケーションでオリジナルなフォーマット・拡張子のまま暗号化し、暗号化したままファイルを利用することができます。さらにポリシーに基づき、操作制御が可能です。

操作は変わらず漏洩防止！

利用者は与えられた権限情報に基づき、従来通りの操作で編集などの業務を遂行できます。一方、ファイル自体は暗号化されたままのため、ファイルを開く権限を持つ人が不正に外部に持ち出しても、DataClasys サーバ（鍵管理サーバ）に接続、認証、復号用の鍵の配信を受けないと暗号化ファイルは開けません。また、ファイルの中身を持ち出すコピー&ペースト、印刷、スクリーンショットなどを制御できるので利用を許可した者からの二次漏洩も防止します。

独自のWindowsのフィルタードライバとAPIの制御によるファイル操作制御

独自のフィルタードライバ

DataClasys では暗号化ファイルを読み込む際に、ドライバ層で復号し、復号データをアプリケーションに渡します。通常の操作で自動的に復号データがアプリケーションに渡されるので、暗号化ファイルのための特別な操作を必要としません。
復号ファイルを一時的に作成することなく、暗号化されたまま、通常のファイルと同じように利用することが可能で、安全性の高いシステムです。

Windows APIの制御

DataClasys サーバから取得した権限情報に基づき、クリップボード出力・プリンタ出力・スクリーンショット・メール添付等の操作を Windows API を制御することにより実現しています。アプリケーションに依存することなく実装されているため、ほとんどのアプリケーションの操作制御が可能です。

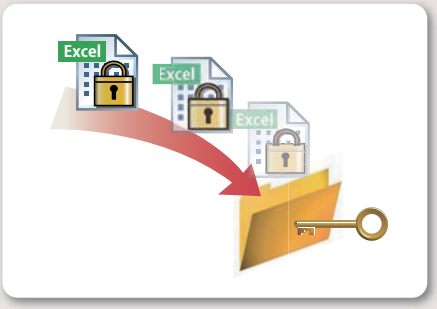
全てのファイル制御が、このドライバと API を通して行われるため、特定のアプリケーションやファイル形式に依存せず、「アプリを問わずに暗号化!操作は変わらず漏洩防止!」を実現します。

DataClasys 機能一覧

- ファイル形式に依存しない、ほぼ全てのファイルを暗号化
- 暗号化状態を保持したままでのファイルクリックによる利用
  注）アプリケーションによっては機能に制限を受ける場合があります。
- 暗号化後の暗号化状態のままでの、マクロやリンク、全文検索、他のシステムとの連携が可能
- 暗号化監視フォルダ、ダイレクト暗号化フォルダにより自動暗号化（ファイル単位／フォルダ単位で暗号化も可）
- 暗号化 / 復号 / 完全消去 / 列挙 / 閲覧 / 更新 / 削除 / ファイル出力 / クリップボード出力 / プリンタ出力 / スクリーンショット / メール添付 / メール送信 / ウェブ送信の権限設定
- 暗号化ファイルの有効期間の設定
- 同一ファイルの複数機密区分での暗号化
- 所属組織と職位とのマトリックスによる権限ポリシー設定
- サーバへの利用者設定変更のみでの人事異動・退職等に対応（予約機能付き）
- 操作範囲（組織範囲）を限定しての、DataClasys 管理者権限の委譲
- 機密情報ファイルを扱うアプリケーション制限
- マルウェア対策
- 暗号化ファイルの操作ログ記録
- CSV ファイルでの人事情報一括登録
- ActiveDirectory連携でのユーザ情報同期（※オプション製品）
- 管理者権限の管理
- ID ファイル利用時のパスワードポリシーの設定
- 暗号化ファイルのオフライン利用
- ID ファイル利用 PC 制限
- コマンドラインインターフェースによる他の文書関連システムへの組み込みが可能（※オプション製品）
- 多言語対応：日本語、韓国語、中国語（簡体字）、英語

ユーザへの負担を強いない利便性 Convenience

多様な自動暗号化



DataClasys では、右クリックメニューから暗号化する操作以外にも、フォルダに保存するだけで自動的に暗号化できる機能やシステムとの連携による自動暗号化など、ユーザのシステム環境に応じた多様な暗号化が可能です。

共有フォルダの監視による暗号化

共有フォルダに「極秘」などの機密区分を指定して自動暗号化する設定が可能です。利用者はファイルを指定の共有フォルダに保存するだけで、自動的に設定した機密区分で暗号化されます。

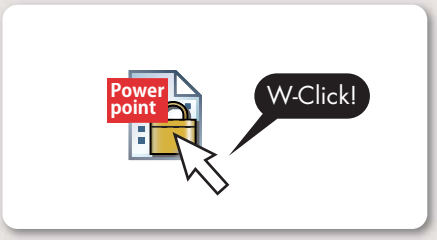
システム連携による暗号化

ファイル管理システムからファイルをダウンロードする時に、管理者が設定した機密区分で自動暗号化してダウンロードされるなど、システムへの組み込みも可能です。(開発キットによる組み込みが必要となります)

ダイレクト暗号化

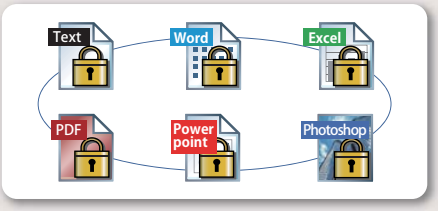
アプリケーションによっては特殊なバックアップファイルや中間ファイルなどを自動生成する場合があります。これらのファイルが重要な内容を含むファイルの場合はダイレクト暗号化の設定を行い直接暗号化ファイルを書き込むことにより安全に保存することが可能です。(ダイレクト暗号化設定がない場合はファイルの保存はされず、セキュリティホールとなることはありません)

ダブルクリックで利用、暗号化したまま閲覧 / 更新可能



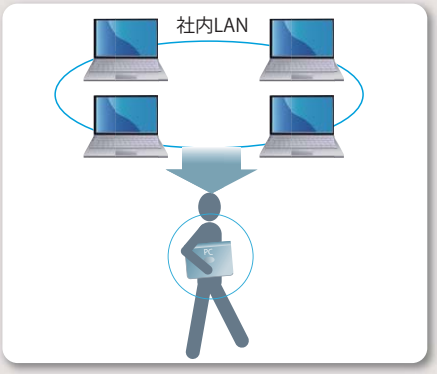
暗号化されたファイルは、通常の平文ファイルと同様にダブルクリックするなどの今までと同じ操作で利用可能です。また、暗号化ファイルを閲覧・更新する際、復号した平文ファイルを生成しテンポラリーフォルダなどに保存したりすることなく、読み込まれた暗号化データのみをメモリ上で復号してアプリケーションに渡します。ファイルの暗号化状態は保持されたまま利用する事が可能なため、ウィルスに感染したり Winny などが動作している PC からファイルを操作したとしても、平文ファイルが流出する事はなく、二次漏洩を防止する事ができます。

ファイル形式に依存せず、あらゆる文書をファイル単位で



DataClasys で暗号化できるファイル形式に制限はありません。あらゆる文書をファイル単位で暗号化します。Microsoft 社のワードやエクセル、パワーポイントなどのオフィス系のファイルや、一太郎、PDF などの文書データ、AutoCAD、CATIA、MicroStation、Visio、Illustrator、Photoshop などの技術系文書、画像系文書などもコントロール可能です。

オフライン環境でも暗号化したまま利用可能、二次漏洩を防止

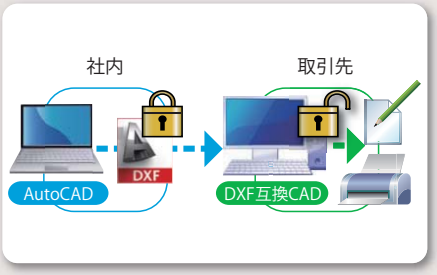


メール添付で取引先などへ送付されたデータや、外出先でのプレゼンテーションなどのために持ち出されたノートパソコン上のデータなど、従来であれば情報漏洩の原因になる可能性が大きく管理し切れなかったアクションに対しても、セキュリティコントロールが可能です。

DataClasys では、出張先や社外のパートナーなど、通信環境が無い、あるいは不安定な環境でも、暗号化ファイルを暗号化したまま利用できます。オフラインでの利用を許可された暗号化ファイルは、DataClasys サーバに接続できなくても、付与された権限の範囲で暗号化したまま利用することができます。オフライン状態で利用可能な期限も設定でき、プロジェクト終了後は暗号化ファイルの利用を禁止できます。

また、海外などの管理の行き届かない場面では、DataClasys ユーザクライアント認証ファイル(ID ファイル)の利用を特定端末に限定することで、他の PC での暗号化ファイルの利用を制限できます。

複数のアプリケーション間で暗号化ファイルを利用



CSV、DXF、SXF、JT などの共通フォーマットファイルを、許可されたアプリケーション間で共有できます。支給元会社では AutoCAD、協力会社では DXF を読み込める互換 CAD をご利用の場合、協力会社で利用されている CAD アプリケーションも DataClasys サーバに登録します。

DataClasys ユーザクライアントのインストーラ、ID を協力会社に事前に支給しておけば、暗号化された DXF ファイルを協力会社の互換 CAD アプリケーションでも暗号化したまま利用でき、二次漏洩を防止できます。

動作環境

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）仮想デスクトップ環境の上記ゲスト OS でも動作可能。＊1
注）アプリケーション共有型仮想環境の場合はご相談ください。
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 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）
注）仮想デスクトップ環境の上記ゲスト 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）
注）仮想デスクトップ環境の上記ゲスト OS でも動作可能。＊1

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）
注）仮想デスクトップ環境の上記ゲスト OS でも動作可能。＊1

DataClasys サーバデータベース

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 仮想デスクトップ環境は VMware や Citrix の VDI 型であれば動作可能です。 ＊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。

利用実績のある主なアプリケーション

ほとんどのアプリケーションで動作します。（アプリケーションによっては機能に制限を受ける場合があります）

マイクロソフト	Office 2003/2007/2010/2013 (Word/Excel/PowerPoint/Access/OneNote/Publisher/Visio/Picture Manager)（32/64bit）、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、Office Viewer（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	Apache OpenOffice
ファイルメーカー	FileMaker Pro
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
シーメンス PLM ソフトウェア	NX、JT2Go
三菱電機エンジニアリング	図王
Jiro Shimizu & Yoshifumi Tanaka	Jw_cad

富士通	iCAD SX、iCAD MX
デザイン・クリエィション	CADPAC-CREATOR
ワコム	ECAD dio
エーティ	WINSTAR CAD
タナックシステム	CADCity
キヤノン IT ソリューションズ	TurboCAD
フォトロン	図脳 RAPID17
アンドール	CADSUPER FXⅡ
ベントレー・システムズ	MicroStation
シスプロ	Walkinside、DesignDraft
CHAM-Japan	ZWCAD
IdeaMK Inc.	IGS Viewer
ラティス・テクノロジー	XVL Player
Aras Corporation	Aras Innovator
CGTech	VERICUT

連携実績のある主なアプリケーション

インフォコム	MySAFER	レピカ	P-Pointer	富士ゼロックス	ArcSuite Engineering
シャープビジネスソリューション	データセキュリティサービス	ジャストシステム	ConceptBase Enterprise Search	NSD ビジネスイノベーション	eTransporter
ウイップス	SecureFiles+				

※上記以外にも検証結果により随時対応が可能です。 ※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。 ※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。

企画・開発

NESCO

株式会社ネスコ

ITシステム事業部 ITソリューション DataClasysチーム

〒108-0075 東京都港区港南1-8-27 日新ビル4F
TEL：03-5462-8511 FAX：03-5462-8519
E-mail：dataclasys@notes.nesco.co.jp
URL：http://www.nesco.co.jp/
製品サイト：http://www.dataclasys.com/

お問い合わせは

160208