DataClasys FAQ

バージョン5.11　第30版

目次

概要、機能

Q1. DataClasys はどのようなことができるシステムですか。

A1. DataClasys は、ほとんどのファイルを対象に、極秘や社外秘などのカテゴリ（機密区分）を付けて暗号化し、暗号化したまま編集、印刷などの操作と制限ができる DRM 製品です。

Q2. DataClasys は他の DRM 製品とどこが違いますか。

A2. 他の DRM 製品との相違点は大きく２点あります。
１点目として、他の多くの DRM 製品は、対応しているアプリケーションが Microsoft Word 、Microsoft Excel 、Microsoft PowerPoint 、Adobe Reader などに限定されています。一方、DataClasys は、ほとんどのアプリケーションを対象に暗号化したまま、編集、印刷などの操作と制限ができる DRM 機能を持ち、弊社では Advanced IRM と称しています。２点目は、企業や行政などの組織で利用されることを前提に権限管理できるよう作られています。ファイル単位でグループや個人の権限をひとつひとつ設定する面倒な作業の必要はありません。また、異動や組織変更にも柔軟に対応できます。

Q3. 管理可能なファイルに条件や制限はありますか。

A3. DataClasys の仕様によるファイルのフォーマットには利用制限はありません。Windows で扱えるファイルは一部を除き全て暗号化でき、暗号化したまま、編集・印刷などの操作が可能です。Microsoft Office （2003-2013：Word 、Excel 、PowerPoint 、Access ）、Adobe Reader 、OpenOffice 、一太郎などのビジネス系ソフトウェアから AutoCAD 、CATIA 、CADVANCE 、Adobe Illustrator 、Adobe Photoshop などのデザイン・CAD ソフトウェアまで、それらで作成したファイルを暗号化したまま利用可能です（当社での動作実績）。

Q4. どこにあるファイルが暗号化の対象となりますか。

A4. 共有ファイルサーバ上や PC のハードディスク、USB メモリ内など、どこにあっても暗号化可能です。Windows 上の読み取り、書き込み権限は必要です。

Q5. どのような制限をかけることができますか。

A5. DataClasys バージョン５では下記の権限と設定ができます。
「暗号化」：暗号化できる権限です。
「復号」：暗号化ファイルを元の平文に戻す権限です。
「完全消去」：復元ソフトウェアでも復元はできないように完全消去する権限です。
「列挙」：暗号化ファイルの存在を隠す機能です(次版以降で実装予定です)。
「閲覧」：暗号化ファイルを閲覧する権限です。
「更新」：暗号化ファイルを編集、上書き更新できる権限です。
「削除」：暗号化ファイルを削除できる権限です。
「ファイル出力」：暗号化ファイルから平文のファイルを出力制限する権限です。
「クリップボード出力」:クリップボードへの出力を制限してコピー＆ペーストを制限する権限です。
「プリント出力」：印刷する権限です。
「スクリーンショット」：OS 付属のスクリーンショットを制限する権限です。
「メール添付」：暗号化ファイルをメールに添付することを制限する権限です。

「メール送信」: アプリケーションからメールを送信するのを制限する権限です。
「ウェブ送信」: アプリケーションから IP を用いた通信を制限する権限です。
その他の設定項目
「オフライン状態での暗号化ファイルの利用の可否」
「暗号化ファイルの有効期限」
「ネットワーク上の暗号化ファイルの復号」
「オフライン状態時の ID ファイルの更新期間」
「オフライン状態での暗号化の可否」
「特定 PC での ID ファイルの利用制限」
「オフライン優先モードの指定」
注：ファイル列挙の設定は可能ですが、本版では制御は実装されていません。次版以降で実装していく予定です。

Q6. 利用権限はどのようにコントロールされるのでしょうか。

A6. DataClasys では利用者やアプリケーションが暗号化ファイルを開く都度に、DataClasys ユーザクライアントがその暗号化ファイルを開こうとした人の情報（ID ファイル）と暗号化ファイルにつけられたカテゴリ（機密区分）に対してどのような権限を有しているかを DataClasys サーバへ自動的に問い合わせます。DataClasys ユーザクライアントはなんらかの利用権限があれば復号用の鍵情報と権限情報をサーバから受け取ります。DataClasys ユーザクライアントは受け取った情報に基づき、暗号化ファイルの復号データを直接アプリケーションに渡し、また権限情報に基づき操作をコントロールします。更新できる権限でファイルを利用させたり、閲覧するだけでファイルの複製/移動/持ち出しを禁止して利用させたり、またファイルを開くこと自体を拒否したりします。基本的にはサーバから鍵情報と権限情報を受け取れない場合や、権限がない場合は暗号化ファイルを利用することができません。したがって、権限のある人がサーバにアクセスできない社外に暗号化ファイルを持ち出しても利用できず、その結果、情報漏えいを未然に防止します。

Q7. 営業マンなどが社外秘ファイルをお客にプレゼンテーションとして見せたい時や、DataClasys サーバに接続できない出張先でも社外秘ファイルを利用したい場合は、どうしたらいいでしょうか。

A7. DataClasys には社外利用型オフライン機能が標準であり、それによって対応可能です。
外部利用可能なカテゴリ（機密区分）で暗号されたファイルは DataClasys ユーザクライアントがインストールされている PC と ID ファイルがあれば、一定時間 DataClasys サーバに接続出来なくても暗号化ファイルを利用することができます。

Q8. 取引先・パートナーに機密性の高いファイルを配信する、共有する場合に DataClasys は利用できますか。

A8. DataClasys のクライアント～サーバ間は HTTP で通信を行いますので、インターネットを介した安全なファイルの配信、利用も可能です。ただし、お客様のポリシーまたはその他の理由により、社外からのアクセスを許可するサーバの構築や運用が難しい場合には、DataClasys を使った ASP/SaaS 型によるサービスを提供している弊社パートナー企業様がございます。同サービスの詳しい内容につきましては、弊社までお問い合わせください。

Q9. 暗号化ファイルに有効期限を設定できますか。その場合、有効期限が過ぎたファイルをどうしても利用したい場合はどうなりますか。

A9. ファイルを暗号化するときにファイルの有効期限を設定できます。有効期限が過ぎた暗号化ファイルは更新・閲覧権限では開くことはできませんが、復号権限がある人は期限に関係なく元の平文に戻すことができます。

Q10. エンドユーザの暗号化ファイルの利用方法は？

A10. エンドユーザが暗号化ファイルを利用する場合、あらかじめ DataClasys ユーザクライアントを起動し、後は暗号化ファイルのアイコンをダブルクリック、同ファイルを指定してアプリケーションから開く、などの操作となります。ただし、開くときに暗号化ファイルを開く確認表示や権限の表示がありますので、権限の限定されたファイルを開く場合は、他に開いているファイルの保存などの一定の操作が必要となります。

Q11. 既存のファイルサーバ内のファイルは機密管理できますか。

A11. オプションソフトウェアの暗号化監視機能で、既存ファイルサーバの暗号化監視設定を行えば可能です。Windows Storage Server（NAS）でも暗号化監視フォルダの設定は可能です。

Q12. 社員や職員が異動、退職、昇格した場合はどうなりますか。

A12. 社員や職員の方の DataClasys サーバ上の登録情報を変更するだけです。
例えば、管理部から営業部に異動した場合、その人の登録情報のグループ（所属グループ）を管理部から営業部に変更します。変更後、その人は管理部の暗号化されたファイルを自分の PC 内に保存していても使用できなくなります。逆に営業部の暗号化ファイルが利用できるようになります。個々の暗号化ファイルへの変更は必要ありません。

Q13. 異動や組織変更などの情報を事前に予約設定できますか。

A13. 可能です。ユーザ設定やグループ設定で開始時期と終了時期の設定が可能です。したがって、開始時期を設定すると開始時期に到達したらその設定が有効となります。

Q14. 所属組織の兼任はできますか。

A14. 利用者登録情報の所属グループは複数登録できます。グループを複数登録することにより兼任できます。

Q15. マイクロソフト社のアクティブディレクトリと連携できますか。

A15. オプション製品のツール（AccountSync）にて、アクティブディレクトリユーザの新規追加・更新編集・削除・認証失効を、DataClasys に自動同期させることができます。
標準機能では、アクティブディレクトリのユーザ情報などを CSV ファイル形式にしてエクスポート（出力）し、DataClasys でのインポート作業が必要です。

Q16. DataClasys のシステム構成を教えてください。

A16. 基本構成は、DataClasys サーバ、DataClasys マネージャクライアント、DataClasys 暗号化監視フォルダ、DataClasys ユーザクライアントの各アプリケーションソフトウェアと、ユーザを識別するための ID ファイルとなり、それぞれの役割は下記の通りです。

・DataClasys サーバ：

鍵管理、権限判断、鍵配信、ログ収集などを行います。PostgreSQL をデータベースとして利用しています。

・DataClasys マネージャクライアント：

DataClasys サーバの管理コンソール、グループ（組織）、ポスト（職位）、ユーザ（利用者）、カテゴリ（機密区分）、暗号化/復号/閲覧/更新/クリップボード出力/印刷のポリシー（権限設定）などの設定を行います。

・DataClasys 暗号化監視：

ファイルサーバなどの共有フォルダを監視し、フォルダ内に入った平文ファイルを自動・強制的に暗号化するオプションソフトウェアです。

・DataClasys ユーザクライアント：

利用者の PC にインストールします。暗号化、復号、OS のドライバ制御を行います。

・ID ファイル：

利用者の認証、暗号化を行う秘密鍵を格納したファイルです。

・コマンドラインオプション：

他の文書管理システムなどとの連携、DataClasys ユーザクライアントのログオンスクリプトでの自動で起動などを行うためのコマンドラインオプションがあります。ただし、このオプションを使うためには「開発用ライセンス契約」が必要となります。

Q17. DataClasys の社外利用型オフライン機能を利用する場合、セキュリティは大丈夫なのでしょうか。

A17. DataClasys の外部利用型暗号においても DRM 制御が可能です。通常のオンラインモードと同様にファイルを暗号化したままの利用ですので、他の単純な暗号製品よりも安全に利用することができます。ただし、通常のオンラインモードでの利用と比較すると、セキュリティはどうしても低くなりますので、暗号化ファイルの有効期限や ID ファイルの更新期間の設定、パスワードの設定などを厳しく運用されることを推奨します。ID ファイルに暗号化ファイルを復号するための情報を持っていますので、解析される可能性は皆無ではありません。本機能を利用する際には、暗号化ファイル、ID ファイルを紛失したり他人にコピーされたりしないように十分注意を払う必要があります。

Q18. ID ファイルのオフライン有効期限とはなんですか。

A18. DataClasys の社外利用型オフライン機能を利用する場合、ID ファイルの更新を一定期間行わないと ID ファイル自体の利用が一時的にできなくなります。オフラインでの利用に一定の制限を付けて安全性を高めるための機能です。例えば、有効期限を１日間と設定した場合、社外で利用可能と設定された暗号化ファイルでも１日経過すると、そのままでは利用できなくなります。DataClasys サーバに接続し ID ファイルの更新を行うとその時点からまた 1 日間、オフライン状態で利用できます。2 日目以降は DataClasys サーバに接続して ID ファイルの更新を行わないと、ID ファイル自体が利用できなくなり社外利用可と設定された暗号化ファイルも利用できなくなります。

Q19. パスワードやパスワードポリシーの設定が可能ですか。

A19. DataClasys ではファイルを暗号化するときに、パスワードは設定しません。DataClasys ユーザクライアントの起動時、つまり ID ファイルを利用するときの起動パスワードでプロテクトをかけることができます。また、そのポリシーについては桁数、英数字の含まれる数、大文字小文字区分、同一文字数の桁数などの設定が可能です。ただし、配布型オフラインオプションの際のパスワードは４桁以上のパスワードを設定するポリシーとなっています。

Q20. DataClasys ユーザクライアントをログイン時に自動起動することは可能ですか。

A20. スタートアップメニューに登録することにより可能です。
アクティブディレクトリとの連携オプション製品（AccountSync）では、アクティブディレクトリのユーザと DataClasys ユーザの紐付けが可能です。この機能を用いて PC ログイン時のアカウントに応じて、所定の DataClasys ユーザで DataClasys ユーザクライアントを自動起動することもできます。

Q21. 評価版はありますか。

A21. 無償の評価版を用意しております。評価版に機能制限はありませんが、DataClasys サーバを初期化してから 30 日間に限りご利用いただけます。

Q22. スマートフォンやタブレットなどでの利用はできますか。

A22. ファミリー製品の「DataClasys Mobile Viewer」により、DataClasys で暗号化・管理している機密ファイルをスマートフォンやタブレットなどのスマートデバイスでも PC 同様にオフライン下においてシームレスかつセキュアに利用することが可能です。スマートデバイス内では全てのデータは分割・暗号化され、利用可能なファイルとしては存在せず、専用アプリケーションでしか開くことができないために、ファイルとして漏洩することはありません。標準構成では PDF、画像（JPEG, TIFF, PNG, GIF）、テキストファイルを対象としていますが、「PDF 変換モジュール」を利用することで、Microsoft Office、その他の文書（DocuWorks、一太郎など）は自動的に PDF ファイルに変換され、スマートデバイス用の暗号化ファイルとして利用することが可能になります。

コンセプト、他社比較

Q23. ファイル自体を暗号化するメリットはどこにありますか。

A23. Windows のアクセス制御は、基本的に一定の領域内でしか有効ではありません。共有サーバから権限者が PC へダウンロードしたファイルはアクセス制御されません。また、ハードディスクを抜き取られて他の PC で読み込まれた場合もアクセス制御されません。しかし、暗号化しておけば、暗号化したときの鍵情報が入手できない限り、ファイルがどこにコピーされても、またハードディスクを抜き取られても元の平文ファイルを開くことはできません。

Q24. Pretty Good Privacy などの他の暗号化製品と DataClasys はどこが違いますか。

A24. Pretty Good Privacy などの暗号化製品は、配信先の人が暗号化ファイルを利用する時に、一度暗号化ファイルを復号して平文ファイルを生成します。そのため、配信先の PC がウイルスに感染したり、P2P ソフトウェアが動作していた場合、また、配信先の利用者の操作ミスなどによる２次漏えいのリスクがあります。
DataClasys は、ファイルを暗号化したまま利用するため、配信先からファイルがたとえ流出しても、暗号化された状態のままのため、２次漏えいを防止できます。

Q25. DataClasys では Windows OS のドライバを制御していますが、どのようなメリットがあるのですか。

A25. DataClasys では暗号化したままファイルを開いて権限に応じて利用します。他の暗号化ソリューションでは復号（平文）ファイルを一次的に作成し、そのファイルを開いて利用させているケースがありますが、DataClasys ではアプリケーションがディスクから読み出した暗号データのみを権限に応じて復号してアプリケーションに渡しています。したがって、電源がダウンしたり、OS がフリーズしたりしたときに復号したファイルが残ることはありません。
DataClasys ではこれを実現するために OS のドライバを制御しています。例えば、閲覧権限しかない場合は、共有サーバにある暗号化ファイルを PC やリムーバブルメディアにコピーすることができず、共有サーバ上で閲覧のみ許可し、ファイルサーバからの持ち出しを禁止することができます。また、OS のドライバを制御することにより、どのアプリケーションでも上記の制御が可能です（一部のアプリケーションでは動作しない場合もありますので、事前に確認してください）。

Q26. 暗号化ファイルにカテゴリ（機密区分）を付ける意味はなんですか。

A26. そのファイルの重要度による管理という意味があります。PC や人単位での制限だけでは、業務に則した持ち出し制限はできません。ファイルの重要度と利用者の権限により制御される必要があります。そのため、ファイルを重要度、機密度レベルに分けて管理するためにカテゴリ（機密区分）を使います。
ファイルを機密性に応じて管理することは、単なる情報漏えい対策だけでなく、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 法や改正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。

Q27. 株式会社日立ソリューションズ社製の「秘文」との違いは何でしょうか。

A27. 「秘文」は元々一定の領域（共有サーバや PC の論理ディスク）を暗号化/アクセス制御する製品です。現在の製品はいくつかの性格の異なるオプション製品によって構成されています。

1) 共有サーバ内のフォルダのアクセス制御とフォルダ内のファイルの暗号化/アクセス制御
2) PC の C:ドライブシステムフォルダ以外の論理ディスクもしくは D:ドライブなどの自動暗号化
3) パスワードでファイルを暗号化

ユーザは自社のニーズに従って機能を選択して導入します。複数の機能が必要であれば、ユーザはそれぞれの機能に合わせた設定、操作を複数行う必要があります。いわば、ファイルの存在する場所、PC 、ネットワーク、共有領域などにそれぞれの対策を行っていく製品です。DataClasys はファイルというコンテンツの重要性、機密性に基づいて情報管理をする製品です。一度、暗号化してしまえば、そのファイルはどこにあろうと権限管理されます。その結果、情報漏えいを防止します。つまり、DataClasys は情報資産としてのファイルをその価値に応じて管理し、企業内の内部統制を強化し、情報漏えいを防止する製品です。暗号化すること自体を目的とした製品ではありません。

Q28. 他社の持ち出し防止製品との違いはどこにありますか。

A28. 多くの持ち出し防止製品は、ネットワーク内の PC や利用者の PC 操作を監視し、一定の操作を禁止したり、無効にしたりします。したがって、対象となる PC や人の一定の操作は全て無効・禁止としてしまうので、持ち出してよいファイルや印刷の必要なファイルはその都度、権限者に制御の解除を依頼する必要が生じる可能性があり、例外処理が多発する可能性があります。例外処理が多いため、結局ポリシーを緩めることになり、セキュリティホールを作る結果に陥りやすいという欠点があります。

DataClasys はファイルにつけられた機密区分と利用する人（所属組織と職位）の関係により利用権限を制限します。どのようなファイルはどの機密区分で暗号化するのか、どの機密区分はどの組織のどの職位にどの権限を付与するのかというポリシーを決めておけば、不注意や誤操作、管理不十分などによる漏えい、非権限者の漏えい・持ち出しを効率よく禁止できます。

Q29. DataClasys ではどのようなログを収集していますか。

A29. DataClasys では利用者の暗号化ファイルの利用ログを記録する他、権限設定者（マネージャ操作者）、DataClasys サーバの操作などのログを記録します。利用者ログ（ユーザログ）はアクセス日時、PC 名、ログインアカウント名、利用 ID、ユーザの要求、サーバ回答、対象ファイル名（フルパス表示）、対象ファイルの機密区分、暗号化者、利用アプリケーションなどを記録します。

Q30. PC の操作ログを収集する他社のシステムと DataClasys のログとはどこが違いますか。

A30. PC 操作のログは相当のボリュームになります。特にファイル操作のログだけでも利用者が直接操作したログと OS やアプリケーションが自動的にファイルへアクセスしたログとを区別することが技術的に難しいため、高度なアプリケーションになるほどそのファイルのログは大きくなります。例えば、他社のシステムではオフィスアプリケーションのファイルを一度開いて閉じるだけでそのファイルに対するアクセスログを全て記録すると 5MB 前後となる場合もあ

ります。そのため、ログは一度 PC に保存して負荷の少ないときに送信する、また、ログサーバを複数必要とする、などの対応が必要となります。DataClasys では機密区分を付けた暗号化ファイルのログのみを収集しますので、重要なファイルのログを効率的に収集します。ログは DataClasys サーバ側でリアルタイムに収集されます。

運用性

Q31. 個々の利用者に機密ファイルを暗号化させるのは利用者の意識やリテラシーの現状からすると難しい面があります。利用者が DataClasys を利用してファイルの機密管理を徹底して行うためにはどのような運用方法がありますか。

A31. DataClasys には暗号化監視というオプション機能があります。この機能を有効に活用することにより利用者への機密区分別暗号化の徹底を図ることができます。一例として・・・、

1) 既存の共有サーバ上の部署別フォルダの中で、該当する部署（のフォルダ）を〇〇部外秘で管理者が一括で暗号化します。
2) そのフォルダを〇〇部外秘の暗号化フォルダに指定します。その後、利用者がそのフォルダにファイルを保存するとフォルダに設定された機密区分で自動的に暗号化されます。利用者は共有サーバ上にあるフォルダにファイルを保存するだけで、機密区分付きの暗号化を行うことができます。
3) 利用者はそのフォルダ内にあるファイルを利用するためには、DataClasys ユーザクライアントソフトウェア、ID ファイルを使用せざるをえず、日常的に機密管理を意識していくことになります。

このように暗号化監視オプションを活用することにより､利用者の機密ファイル管理を徹底させていくことができます。また、DataClasys ユーザクライアントがインストールされている個々の PC に、ある書式で記述した DataClasys ユーザクライアント用の設定ファイルをあらかじめ読み込ませておくことによって､クライアント側で暗号化実行のメニューを非表示にすることも可能です。

Q32. グループウェアの文書管理機能や決裁機能を使っていますが、DataClasys で暗号化したファイルもグループウェア上で管理できますか。

A32. WEB 系のグループウェアであれば、DataClasys で暗号化したファイルも扱えます。当社で確認しているのは、サイボウズとデスクネッツです。DataClasys で暗号化したファイルをグループウェアの文書管理機能でアップします（ただし、ウェブ送信と更新権限のあるファイルのみ、両権限がないファイルはアップできません)。利用者は更新権限およびウェブ送信権限のあるファイルは保存（PC にダウンロード）できますが、ウェブ送信権限がなかったり、ウェブ送信権限はあっても閲覧権限しかない場合はファイルの保存はできません。尚、グループウェアによっては特殊なファイル操作をする場合があります。DataClasys で暗号化したファイルを取り扱えない場合もあります。30 日間無償評価版でご確認ください。

Q33. 一太郎のデフォルトの設定では、バックアップファイルを作成しますが、バックアップファイルも自動的に暗号化されますか。

A33. 一太郎に限らず、暗号化されたファイルから生成されたバックアップファイルは自動的に暗号化されます。

Q34. 読み取り専用属性のついたファイルも暗号化できますか。

A34. 可能です。読み取り専用ファイルを暗号化しようとした場合、そのファイルが[Read Only ですが暗号化しますか]と確認のメッセージが表示され、[OK]を選択すると暗号化が実行されます。尚、暗号化後もそのファイルの読み取り専用属性はそのまま保持されます。

Q35. 暗号化したファイルを USB メモリや CD-R などのリムーバブルメディアにコピーできますか。

A35. 更新権限のある暗号化ファイルであれば、異なるドライブへのコピー、移動、共に可能です。したがって、リムーバブルメディアにもコピーができます。更新権限がない（閲覧権限しかない、更新/閲覧権限の両方がない）場合にはその操作はできません。

Q36. 暗号化したファイルをメールに添付できますか。

A36. メール添付の権限があれば可能です。ただし、ご使用のメールクライアントにより動作が制限される場合もありますので、必ず事前に検証してください。尚、添付対象となるファイルを自らが管理するフォルダなどに一旦複製するタイプのメールクライアントでは、更新権限のある暗号化ファイルは添付可能ですが、更新権限がない（閲覧権限しかない、更新/閲覧権限の両方がない）暗号化ファイルは添付できません。また、添付対象となるファイルを送信時に直接読み込むタイプのメールクライアントでは添付可能です。いずれにしろ、機密区分付で暗号化されていますので、権限のある人しか暗号化ファイルを読むことはできません。

Q37. Microsoft Access で顧客管理を行っていますが、DataClasys で暗号化できますか。

A37. Microsoft Access の MDB ファイルも暗号化可能です。DataClasys で暗号化し、更新権限がある場合は、データの入力、フォームの追加/変更などが可能です。プリント出力権限がない場合は印刷できません。閲覧権限の場合は、データの入力、フォームの追加/変更ができません。印刷もできません。

Q38. DataClasys でファイルを暗号化したまま全文検索ができますか。

A38. 可能です。DataClasys マネージャクライアントでアプリケーションリストに全文検索のプログラムを登録していただければ、DataClasys で暗号化したファイルの内、更新/閲覧権限のあるファイルについては、全文検索可能です。これまでに弊社で確認した全文検索エンジンは、ジャストシステム社の CBES(ConceptBase Enterprise Search)です。他の全文検索システムでは確認できていませんので、評価版にて確認してください。

Q39. 社員や職員の新規登録、変更の一括入力は可能ですか。

A39. DataClasys マネージャクライアントから CSV フォーマットのファイルをインポートすることができますので、CSV ファイルを用意いただければ、一括での登録/変更が可能です。また、アクティブディレクトリのユーザユニーク No などを入力する欄も入力可能ですので、変更時にマッチングできます。

Q40. DataClasys でポリシーに基づいたファイルの機密管理が統一できるのは良いのですが、ファイル（文書）管理責任者の負担が著しく増加することはありませんか。

A40. DataClasys ではユーザの登録/変更、組織の登録/変更、機密区分の登録/ポリシー設定などを行うための DataClasys マネージャクライアントという管理画面があります。このマネージャクライアントを最初に操作するためには「Admin.cid 」という ID ファイルが必要です。この「Admini.cid 」を持つ人を DataClasys システムのアドミニストレータと呼びます。このアドミニストレータが全社の文書管理責任者に相当します。この人は他の利用者に DataClasys のマネージャ操作権限を、組織範囲を限定して与えることができ、このマネージャ操作権限を与えられた利用者は各部門の文書管理責任者に相当します。各部門内のプロジェクト管理や人事/労政などの横断業務に関わる機密区分の設定/運用は、この各部門の文書管理責任者に任せ、

アドミニストレータは全社で共有するファイルの機密管理と各部の運用監査/監視を行うなどの業務分担を行えます。

Q41. 暗号化/復号に時間がかかりますか。

A41. 一般の業務で使われる 数 MB 程度の文書ファイル、ワークシートファイルの類であれば、暗号化、復号、共にほんのわずかな時間で終了してしまいますが、ひとつひとつの容量は少なくても大量のファイルを一度に暗復号する場合や、CAD などの巨大な容量のファイルなどは比較的時間がかかってしまいます。
また、最近の PC においては、暗号化速度とディスク（HDD ）への書き込み速度とを比較すると、ディスクへの書き込み時間の方が暗号化時間よりもかかる傾向が強く、実はそこが一番のボトルネックとなっています。また、平文を最初に暗号化する場合は、暗号化されたデータファイル全体を書き換えますので、ディスクへの書き込み時間がかかります（これはどの暗号ソフトウェアでも基本的に同じです）。
暗号化監視を実行しているファイルサーバなどで、どうしても暗号化に時間がかかるようであれば[ワイプ無し暗号]という高速暗号化の設定をすることも可能です。ただし、この設定にした場合はセキュリティレベルが若干低下しますので、PC や共用フォルダへのアクセスコントロールなど、セキュリティ対策をきちんとするようにしてください。
更新権限でファイルを開く場合、DataClasys ではアプリケーションが読み出したデータのみ復号してアプリケーションに渡します。したがって、ファイルの大きさによる差異は少なく、アプリケーションのファイル読み込み方法による差異のほうが大きく影響します。DataClasys 30 日間無償評価版の提供が可能ですので、実際にご使用されるアプリケーションで検証されることをお勧めします。

Q42. DataClasys で機密管理を行うと利用者の利便性が落ちませんか。

A42. DataClasys では一度、機密区分を付けてファイルを暗号化すると、その機密区分に対する権限者しかそのファイルの利用ができなくなります。一方、権限者は暗号化されていてもほぼ従来通りの操作でアプリケーションが立ち上がり、利用できます。Microsoft Excel のマクロなどにおいて、他の暗号化されたファイルへの参照なども権限者であれば以前と同じようにマクロを実行することができます。また、閲覧権限があれば全文検索も可能です。権限管理されるため、権限設定ポリシーが業務・運用の実態と乖離している場合は、利用者は不便を感じることがあるかもしれません。いずれにしろ、権限設定ポリシーを事前によく社内や部門内で検討しておく必要があります。尚、DataClasys では機密情報管理方針・基準作成ウィザードがありますので、雛形としてご利用いただけます。

Q43. DataClasys のユーザが自身に付与された ID ファイルを紛失したり、壊してしまったり、設定していたパスワードを失念してしまった場合はどうなりますか。

A43. DataClasys では、ユーザー人一人に ID ファイル（鍵情報ファイル）を持ってもらいますが、再発行することが可能です。ただし、再発行前の ID ファイルを他の人が使う可能性もありますので、管理画面（DataClasys マネージャクライアント）でその ID を無効処理とした上であらためて再作成する（ID ファイルを発行する）ことを推奨します。いずれも管理画面から操作できます。いずれにしろ、再発行の手続きや、手順を定めて「他人によるなりすまし」を防ぐことが必要です。

Q44. グループ会社との間で DataClasys を利用できますか。

A44. 例えば親会社を組織の頂点とし、各グループ会社を下部組織（部門）として、DataClasys サーバに設定/登録していくことにより利用は可能です。各グループ会社内での機密管理や会社間をまたがる機密管理を実現することができますが、会社間のネットワーク構成やポリシーなどにより DataClasys サーバの構築/配置などは検討する必要があります。DataClasys サーバと DataClasys ユーザクライアント、DataCasys マネージャクライアント間の通信方式は HTTP ですので、インターネットを介したシステムも構築することが可能です。

Q45. 自社の文書管理システムと DataClasys を連携させたいのですが、プログラム的に暗号化監視や復号はできますか。

A45. 可能です。連携の内容にもよりますが、DataClasys 本体については、各種のコマンドラインインターフェスを「開発キット」という形で別途用意しています。暗号化・復号・削除などのコマンドがありますので、バッチプログラムや連携先プログラムに組み込んでご利用いただくことが可能です。

Q46. DataClasys サーバを二重化、冗長化できますか。

A46. 可能です。DataClasys サーバはデータベースとして PostgreSQL を搭載しています。そのデータをダンプ、リストアすることにより、コピーサーバを別途構築できます。また仮に 2 台の DataClasys サーバを常時起動させている場合には、DataClasys ユーザクライアントはプライマリサーバと通信できないと、セカンダリサーバに自動的に接続します。またデータベース側の仕組みで、同期やログ収集を設定できますので、システム構築費、運用費用を低減でき、システム全体の安全性を高めることが可能です。

Q47. DataClasys サーバをファイルサーバと同居させても問題はないですか。

A47. 仕様、技術的な制約は少ないのですが、基本的にはあまりお奨めしておりません。利用ユーザ数やファイルサーバの負荷にもよりますが、もしも同居させる場合には、HDD の RAID 構成、設定情報の定期的なバックアップは強く推奨します。ホットもしくはコールドスタンバイの予備機も別途ご用意いただけると安心して運用ができます。

Q48. DataClasys サーバのハードディスク容量はどの程度を考えておけばいいでしょうか。

A48. DataClasys サーバの鍵管理データベースは、大きな組織でも 1GB は越えることはほとんどありませんが、ログデータベースの容量は機密ファイルをどの程度利用されるかにより異なります。例として、暗号化された Microsoft Excel ファイルを 1 回開いて更新するとそのログは 50KB 程度となります。(Microsoft Excel ファイルを操作したログは、他のオフィスアプリケーションに比較すると多い部類になります。)

ログデータベースは月別に生成されますので、サーバ上から古いログは吸い上げて、ディスク容量を確保してください。

また、容量の目安は下記の計算を参考にしてください。

(50KB × 1 日に利用する暗号化ファイルの数 × 30 日/月 × DataClasys サーバ上に保存しておく月数)

例えば、暗号化ファイルを 1 日に 1000 回利用すると仮定し、DataClasys サーバ上にログを保存するのは 3 ヶ月とした場合、50KB × 1000 × 30 × 3 = 4,500,000KB = 4.5GB となります。

Q49. ID ファイルはどのように保存しておけば良いですか。

A49. DataClasys の ID ファイルは利用者の認証とファイルの暗号、復号のいずれにも使用し、中でも認証の機能は特に重要です。担当者が広範な権限を持つ（例えば管理職などの職位の）ID ファイルを使って極秘ファイルを読むなどの不正使用がおきないように厳格な管理をしておく必要があります。また、DataClasys の ID ファイルにはクライアントソフトウェアを起動するためのパスワード設定ができます。さらに DataClasys サーバ側での設定により、そのパスワードにポリシーを設定することが可能で、ポリシー通りのパスワードを設定・入力しないクライアントソフトウェアを起動できなくすることも可能です。さらに、USB トークンや IC カード、生体認証システムと連携させて ID カードを使用することも可能です。ネットワーク上の利用者本人しかアクセスできないフォルダに、ID ファイルを保存して利用する例もあります。

Q50. 閲覧権限を持っているのに、暗号化ファイルを開くと正しく表示されない場合がありますが。

A50. アプリケーションリストに登録されていないアプリケーションで、暗号化ファイルを開こうとしたことが考えられます。DataClasys マネージャクライアントで、該当するアプリケーションが正しく登録されているかどうかを確認してください。また、上記のように未登録のアプリケーションで暗号化ファイルを開いた場合、まれに暗号化ファイルが壊れる可能性がありますので、ご注意ください。

Q51. DataClasys マネージャクライアントでログを取得したときに、ログが存在しなかったにもかかわらず、ファイルが作成されますが。

A51. ログの取得を行ったという結果に対して、サイズが「0」のログファイルが生成されます。

Q52. 期限切れ ID 、削除された ID から DataClasys ユーザクライアントを起動、ログインできてしまうのですが問題はないのでしょうか。

A52. オンライン状態の場合には、DataClasys ユーザクライアントはそれらの ID でも起動しますが、特に問題はありません。DataClasys は、ID ファイルを使用して DataClasys ユーザクライアントを起動した段階では、またサーバと通信は行いません。ID ファイルを更新するなど、サーバと通信が開始された時点で、初めて有効期限が切れているというエラーが返り、クライアント側にはその時にエラーメッセージが表示されます。しかしながら、運用上の不要な混乱を避けるためにも、不必要な ID ファイルは速やかに消去するようお願いいたします。ただし、ID ファイルのオフライン有効期限を過ぎている場合は、オフライン状態のままでは DataClasys ユーザクライアントの起動自体ができません（オンライン状態でのみ起動します）。

Q53. DataClasys ユーザクライアント起動中、PC 画面の右下にポップアップされるサブウィンドウに表示されるメッセージにはどんな意味があるのですか。

A53. 使用中のファイルに対して DataClasys がどのような制御や処理を実行しているのか、を表示しています。アプリケーションによっては実際の操作感よりも、かなり頻繁にメッセージが表示される場合もありますが、それはそのアプリケーションがバックグラウンドで多くの処理を行っていることを意味しています。DataClasys 自身は個々のアプリケーションのフォアグラウンド、バックグラウンドの区別は行いませんので、関連する全ての処理について都度表示しています。尚、[アプリケーションリストの登録・編集]から「暗号化ファイルを開いたこと」、「暗号化ファイルを上書きしたこと」、「ファイルの保存が行われないこと」についての表示を

しない（止める）ことが可能です。詳しくは別紙の『DataClasys マネージャクライアントマニュアル』をご参照ください。

Q54. 暗号化ファイルを開く際に、ポップアップされる警告メッセージの内容がわかりにくいのですが。

A54. DataClasys バージョン4.6から暗号化ファイルを読み込む際に、平文データの保存ができなくなる旨の警告を表示するようにしています。それ以前のバージョンではそのような警告が一切現れないため、せっかく作成していた（平文の）データが保存出来なくなる、という不便をおかけしておりましたが、あらたに表示を出すことにより、現在開いている平文ファイルを一度保存してから暗号化ファイルを開く、という操作を確実に行っていただけるようにいたしました。尚、サーバへの設定により本警告メッセージを表示させなくすることも可能です。

Q55. 暗号化監視が正しく機能していないようなのですが。

A55. マニュアル、ガイドに従って、正しくインストールと設定を行ったのにもかかわらず暗号化監視ソフトウェアが正しく機能しない場合には、主に次のような原因が考えられます。
まず最も多い原因が、暗号化監視ソフトウェアを起動したマシンのアカウントに、暗号化対象フォルダへのアクセス権が正しく設定されていない場合です。特にリモートフォルダを対象にして設定を行う場合には注意が必要です。またローカルの（暗号化監視ソフトウェアが入っているマシン自身の）フォルダを対象に設定した場合でも、Windows OS の設定によっては上手く行かない場合もございます。その場合は各フォルダへのアクセス権やセキュリティの設定をもう一度見直していただき、使用するアカウントも Admin 権限を持つ他のアカウントで試してみる、などを行ってください。
次に多い原因はインストールするソフトウェアを取り違えている場合です。暗号化監視ソフトウェアが使うDataClasys ユーザクライアントは、一般ユーザにインストールするモードとは異なるモード（ドライバ無しモード）とすることが必要です。もしも一般ユーザ用モードでインストールしてしまったとしても、一見しただけでは両者の区別がつきません。別紙『DataClasys 暗号化監視設定･導入マニュアル』を参考にして、現在インストールされているユーザクライアントの種類を確認し、間違っているようでしたら入れ直してください。
次に多い原因として一度に多量の平文ファイルを暗号化実行フォルダにアップしたことにより、暗号処理に時間がかかり、それが暗号化監視の不具合と判断されるケースです。特に新規に導入した場合、暗号化監視ソフトウェアは最初にファイルのリストを作成します。その数が膨大な場合、リストの作成そのものに時間がかかり、暗号化がなかなか実行されないので、不具合が起こったと勘違いされることがあります。一度に多量のファイルを暗号化する場合には、しばらく放置して様子を見ていただくか、クライアントマシン側で事前に暗号化してから暗号化フォルダにアップするかのいずれかの措置を講ずるようにしてください。尚、暗号化監視を実行しているファイルサーバなどで、どうしても暗号化に時間がかかるようであれば[ワイプ無し暗号]という高速暗号化の設定をすることも可能です。ただし、この設定にした場合はセキュリティレベルが若干低下しますので、サーバやフォルダへのアクセスコントロールなど、セキュリティ対策をきちんとするようにしてください。

Q56. DataClasys は海外でも利用できますか。

A56. 中国語版（簡体字）、英語版、韓国語版を別途用意しております。ただし、中国国内で販売及び保守サポートはしていませんので、お客様ご自身が日本から中国に持ち込んでいただく必要があります。尚、中国では外国製の暗号システムの使用については個々に許可制となっていますので、中国の公安局への申請が必要です。弊社でも申請し、許可を得た経験がありますので、

お問い合わせください。

Q57. DataClasys の利用できる PC を特定の PC に限定したいのですが。

A57. 可能です。バージョン5.2以後では ID ファイルを利用できる端末を固定することができます。ID ファイルを発行する（ユーザを登録する）時に[接続端末を固定する]にチェックを入れて発行すると、最初にその ID ファイルを利用した PC 以外ではその ID ファイルは利用できなくなります。

Q58. DataClasys の利用できる PC を特定の PC に限定して運用していたのですが、PC を入れ替えることになりました。その場合、どうしたらいいのでしょうか。

A58. ID ファイルを再発行することにより対応可能です。管理者が DataClasys マネージャクライアントで ID ファイルを再発行し、新しい ID ファイルを新 PC 上で最初に利用すれば、その ID ファイルは新 PC に固定されます。

サポート

DataClasys についてのお問い合わせは、別紙『DataClasys 製品サポートのご案内』をご参照ください。

履歴

第一版： 2006 年 3 月 27 日（初版）
第二版： 2006 年 9 月 15 日
第三版： 2006 年 9 月 27 日
第四版： 2007 年 1 月 22 日
第五版： 2007 年 2 月 8 日
第六版： 2007 年 3 月 27 日
第七版： 2007 年 4 月 24 日
第八版： 2007 年 5 月 30 日
第九版： 2007 年 11 月 16 日
第十版： 2007 年 12 月 5 日
第十一版：2009 年 3 月 23 日
第十二版：2009 年 8 月 24 日
第十三版：2009 年 10 月 26 日
第十四版：2010 年 8 月 17 日
第十五版：2010 年 8 月 19 日
第十六版：2011 年 11 月 30 日
第十七版：2012 年 1 月 31 日
第十八版：2012 年 6 月 29 日
第十九版：2012 年 9 月 21 日
第二十版：2013 年 3 月 14 日
第二十一版：2013 年 5 月 28 日
第二十二版：2013 年 11 月 25 日
第二十三版：2014 年 2 月 21 日
第二十四版：2014 年 7 月 23 日
第二十五版：2014 年 11 月 21 日
第二十六版：2015 年 3 月 23 日
第二十七版：2015 年 4 月 9 日
第二十八版：2015 年 6 月 17 日
第二十九版：2016 年 2 月 3 日