

アシスト、「ファイルサーバ情報漏えい防止ソリューション」を提供開始 ～データの暗号化で、情報資産の保護をよりセキュアに～

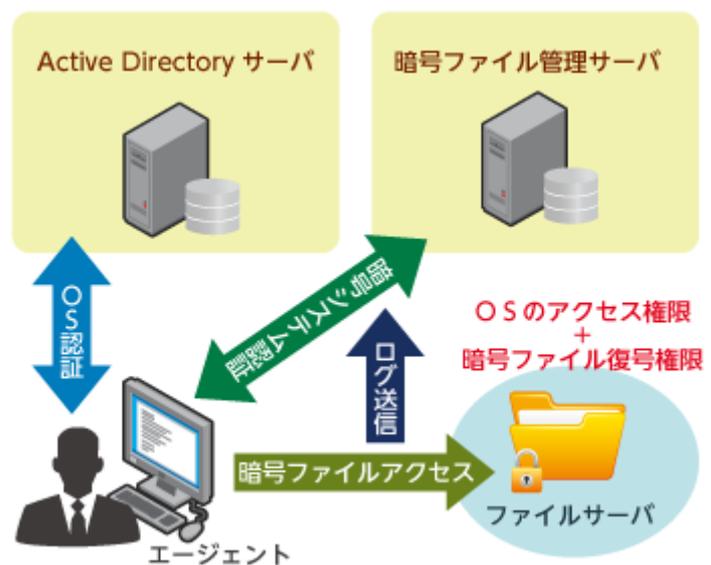
株式会社アシスト(本社:東京都千代田区、代表取締役社長:大塚 辰男、略記:アシスト)は、企業の重要な資産であるデータ保護を強化するために、「ファイルサーバ情報漏えい防止ソリューション」を本日付けで提供開始します。

業務を適正に遂行し、不正行為や情報漏えいを防止するためには、企業内の各種システムや重要な業務データ、経営データを含むサーバへのアクセス管理が必要不可欠です。アシストでは、特権 ID を含む ID 管理により、システムへの入り口を保護する「認証基盤」、暗号化、仮想化、アクセス・コントロールによりシステム内のデータが外部へ漏えいしないように保護する「データ保護基盤」、デバイス管理、資産管理、ログ管理、モニタリングにより迅速な実状把握や PDCA サイクルにて対策を強化する「インフラ基盤」という3つの基盤により、企業の重要な資産であるデータを護る「サーバアクセス管理ソリューション」を展開しています。

今回アシストでは、「データ保護基盤」を強化するために、暗号化によるデータ保護をベースとし、認証強化、ファイル単位の制御を組み合わせることでよりセキュアなデータ利用環境を実現する「ファイルサーバ情報漏えい防止ソリューション」を新たに提供します。「ファイルサーバ情報漏えい防止ソリューション」では、暗号化ツールを利用した基本モデルに加え、生体認証との連携など、データ保護をより強固にする追加モデルを用意、顧客企業が用途に応じて柔軟に選択できるようにしました。

●共有データ暗号化モデル(基本モデル)

特権 ID を使用した意図的なデータの不正利用を防止することは困難であり、またアクセス・ログを取得していたとしても、漠然と操作ログを取得しているだけではいざという時に必要なログを確認できず、不正利用の特定ができません。「基本モデル」では、ファイルサーバ上の共有データを暗号化し、OS のアクセス権限設定に加え、OS とは別のアクセス権限(復号権限)にて二重に保護します。また、専用エージェントの入っていない PC では暗号化データは利用できず、OS の特権 ID でもデータを利用させない環境を実現します。暗号化データへのアクセスログを取得することで、不正行為の抑止や問題発生時の調査を可能にし、さらに、重要データに絞ってアクセス・ログを取得できるため、事後監査を容易にします。



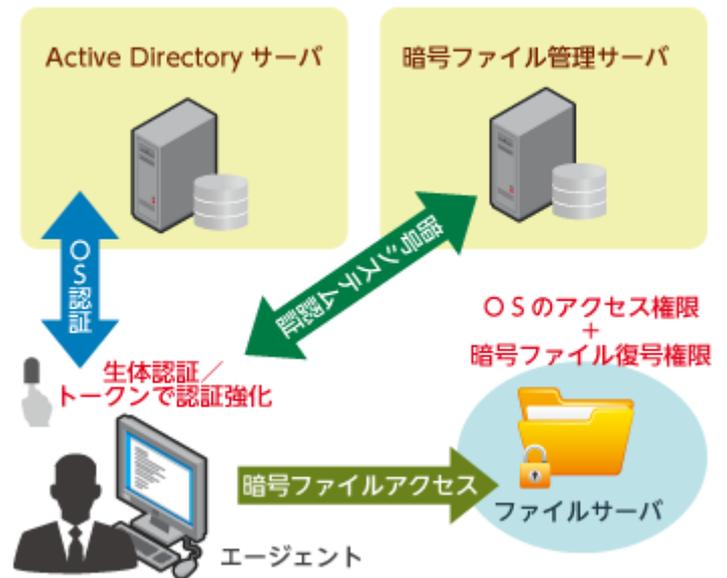
【最小構成価格(税別)】241.5万円～

※ 100クライアント(ユーザ)での価格。ライセンス、初年度プロダクトサポート費用含む。導入支援費用は含まない。

●認証強化連携モデル(基本モデル+認証強化)

ID やパスワードが窃取されると、暗号化で保護したデータであっても不当なユーザや本人以外が利用できてしまう可能性があります。「認証強化連携モデル」では、Windows ログオンを生体認証と連携して本人以外のシステムの不正利用を防止します。また、暗号化システムの認証も生体認証や USB トークンなどの物理デバイスと組み合わせることにより、不当なユーザのアクセスを防ぎます。

【最小構成価格(税別)】295.5 万円～
 ※USB トークン利用の場合
 ※100 クライアント(ユーザ)での価格。ライセンス、初年度プロダクトサポート費用含む。導入支援費用は含まない。



●ワークフロー連携モデル(基本モデル+持ち出し制御)

データを暗号化しても、権限のあるユーザの不正行為による外部への持ち出しや、マルウェアなどによる外部へのデータ流出を防ぐことは困難です。「ワークフロー連携モデル」では、外部メディアへの保存、メール添付、Web アップロード等を申請/承認制にすることで、未許可ファイルの外部持ち出しを防止します。また、申請/承認の記録や、実際に申請されたデータをログとして取得することで、より厳密な管理を可能にします。

【最小構成価格(税別)】657.5 万円～
 ※100 クライアント(ユーザ)での価格。ライセンス、初年度プロダクトサポート費用含む。導入支援費用は含まない。

上記に加え以下の強化モデルを実施することで、より強固な情報漏えい対策を行うことが可能です。



●サーバアクセス制御

特権ユーザに対するアクセス制御は、OS の機能では不十分です。アクセス制御製品を追加導入することで、個人情報格納されているデータベースや、各種アプリケーションサーバ、ファイルサーバといった個人情報が格納されているサーバへのアクセスを制限し、個人情報の漏えい、監査ログの改ざん/削除を防ぎ、特権ユーザを含めたユーザの不正を防止します。

●ログの統合管理

暗号化システムやサーバで取得したログ、OS ログ等を自動的に収集し、一元的に統合管理を行うことや、その内容を定期的にチェックすることで、セキュリティ対策状況の PDCA の実施、大量データのダウンロード等の通常処理と異なる異常値の発見につなげることができます。

アシストの「ファイルサーバ情報漏えい防止ソリューション」は、ファイルサーバ上の共有データの暗号化対策を基本モデルとし、さらなる強化対策として各種リスクに応じた対応策を網羅的に提供することで、完全な「データ保護基盤」を実現します。アシストでは今後も顧客企業様の様々なセキュリティ・ニーズに対応できるよう、「サーバアクセス管理ソリューション」を順次拡充していきます。

■株式会社アシストについて

代表取締役会長:ビル・トッテン／代表取締役社長:大塚 辰男

設立:1972年3月

社員数:850名(2014年4月現在)

本社:東京都千代田区九段北4-2-1

URL:<http://www.ashisuto.co.jp/>

アシストは、特定のハードウェア・メーカーやソフトウェア・ベンダーに偏らない、幅広いパッケージ・ソフトウェアを取り扱う会社です。「パッケージ・インテグレーター」として複数のソフトウェアと支援サービスにアシストのノウハウを組み合わせ、企業の情報システムを情報活用、運用、データベースのそれぞれの分野で支援しています。今年も“「お客様の最高」のために”というスローガンのもと、この3分野にさらに注力し、顧客企業の立場に立った製品選定と独自の組み合わせによる製品／サービスの提供を一層強化し、活動していきます。

■ニュースリリースに関するお問い合わせ

株式会社アシスト 広報部 担当:田口

TEL:03-5276-5850 FAX:03-5276-5895

E-Mail:press@ashisuto.co.jp

■「ファイルサーバ情報漏えい防止ソリューション」に関するお問い合わせ

株式会社アシスト システムソフトウェア事業部 担当:山崎、蓮子(はつし)

TEL:03-5276-3475 FAX:03-5276-5879

E-Mail:secsol_svr_web@ashisuto.co.jp

製品 URL:http://www.ashisuto.co.jp/product/theme/security/file_server_leakage.html

※ 記載されている会社名、製品名は、各社の商標または登録商標です。

※ ニュースリリースに記載された製品／サービスの内容、価格、仕様、お問い合わせなどは、発表日現在のものです。その後予告なしに変更されることがあります。あらかじめご了承ください。