● 稼動環境

ESS AdminGate コントローラー稼動要件

対応する仮想環境	・VMware vSphere (ESXi) ・Microsoft Hyper-V ・Citrix XenServer
管理対象サーバーのOS	・Microsoft Windows Server 2008(x64) /2008 R2 ・Microsoft Windows Server 2012 /2012 R2 ・Microsoft Windows Server 2016 ・Ubuntu Server 12.04 LTS, 14.04 LTS, 16.04 LTS ・CentOS 5, 6, 7 (x64) ・SUSE Linux Enterprise Server 10, 11, 12 (x64) ・Red Hat Enterprise Linux 5, 6, 7 (x64) ※Windows Serverにはエージェントプログラムが必要です
管理対象のアカウント	・上記管理対象サーバーOSのローカルアカウント ・Windows Active Directoryユーザーアカウント (Windows Server 2008 R2またはWindows Server 2012 機能レベル)
管理対象の接続方式	・Windowsサーバーに対するリモートデスクトップ接続 ・Linuxサーバーに対するID//パスワード認証方式のSSH接続

クライアント要件

サポートするブラウザ	・Internet Explorer 10, 11 ・Google Chrome 38以上
サポートするリモートデスクトップクライアント	・Remote Desktop Client Ver. 6.1以上

その他

・ESS AdminGateコントローラーを稼働させるハードウェア要件については、ご利用環境によって異なります。詳しくは弊社までお問い合わせください。
・本ソフトウェアは、不正アクセスを完全に防止するものではありません。
・本ソフトウェアは改良のため事前に告知することなくバージョンアップすることがあります。
・本ソフトウェアに使用されている一部の技術は特許出願中または取得済みです。
・ESS AdminGate, ESS REC, Remote Access Auditor, ID Inspector, Encourage Super Station, ESS AutoQuality, ESS AdminControl,ESS AutoAuditor, ESS FileGateは、エンカレッジ・テクノロジ株式会社の登録商標または商標です。
・Microsoft, Windows, Windows Serverは、米国 Microsoft Corporation、およびその他の国における登録商標または商標です。
・記載されているその他の会社名、製品名、サービス名は、各社の登録商標または商標です。

〈お問い合わせは〉

〈開発・販売元〉
エンカレッジ・テクノロジ株式会社
〒103-0007 東京都中央区日本橋浜町3-3-2 トルナーレ日本橋浜町 7F
TEL：03-5623-2622 FAX：03-3660-5822 URL：http://www.et-x.jp

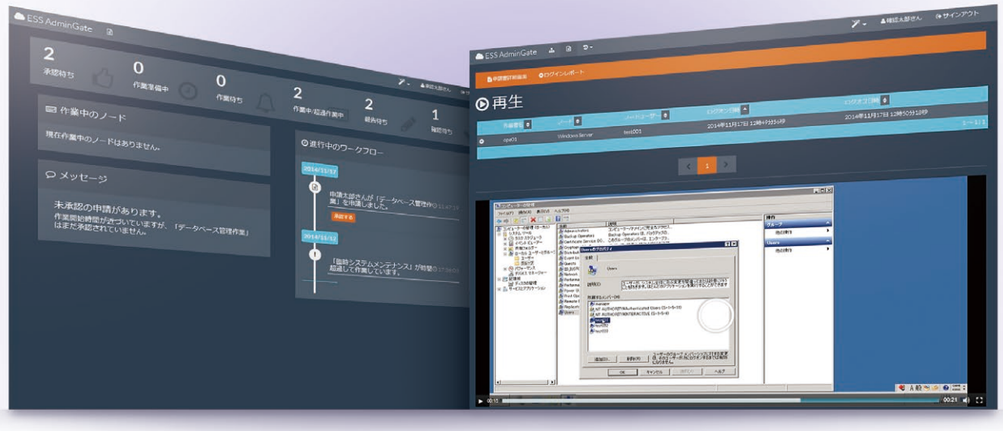
EAG-BR-2018-06-01

ENCOURAGE TECHNOLOGIES

オールインワンで実現するサーバーのセキュリティ対策

ESS AdminGate

ログ管理　アクセス制御（特権ID管理）　パスワード管理
情報漏洩対策　不正プログラム持ち込み防止



ENCOURAGE TECHNOLOGIES

ESS AdminGate オールインワンでサーバーのセキュリティ対策を実現

セキュリティ対策と効率性を両立することの重要性

今、サイバーセキュリティ、内部不正、コンプライアンス対応など多くの取り組みが企業に求められている反面、これらの取り組みによって発生するコストや管理負荷が課題になっています。手間をかけず効率的に必要な対策を講じることが重要になっています。

サーバーのセキュリティ対策に関わるビジネス課題

サイバーセキュリティ対策
巧妙化する攻撃手口にもはや完全には侵入を防ぐことが困難な状況の中、重要情報が保管されているサーバーを守ることが最後の砦です。

IT統制・内部統制
JSOXなどの法の要請だけでなく、企業統治の考え方が浸透する中、ITの統制の整備は企業としての重要な責務になっています。

ISMS/PCI DSS/FISC対応
客観的な認証システムや業界基準を満たすことが、事業を行う上での前提条件です。

監査指摘への対応
特権IDの管理不備、ログ管理の不備はIT監査において最も指摘されるポイントになっています。

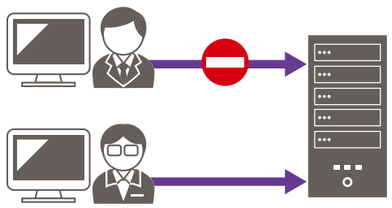
ESS AdminGateの特長・主な機能

アクセス制御（特権ID管理）

許可された者だけがサーバーにアクセスできるしくみ

誰がどのサーバーにアクセスできるのかといった「アクセス制御」を管理対象のサーバーに対して行うことができます。各管理対象サーバーの管理者が異なる場合もそれぞれ異なるユーザーだけがアクセスできるように制御可能です。

管理者権限（特権ID）を使用する場合には承認が必要といった、申請承認ベースのアクセス制御により、許可された期間だけ一時的にアクセスを許可する仕組みも提供可能です。

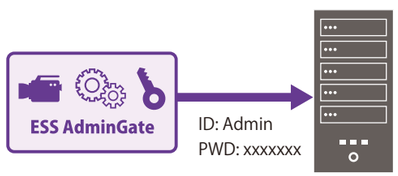


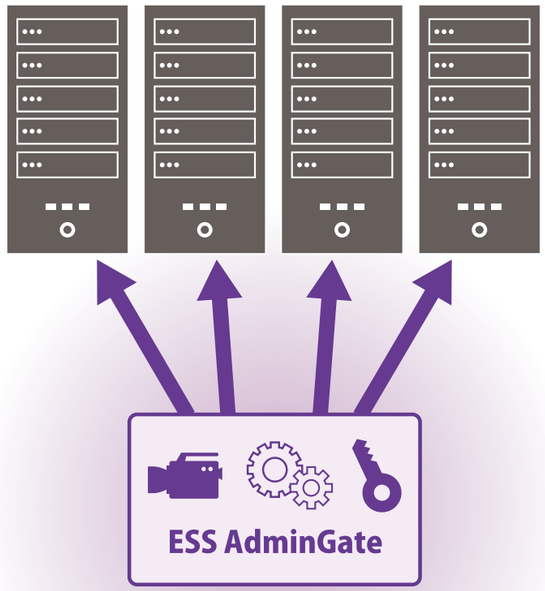
パスワード管理

パスワードの漏洩リスクを低減／パスワード管理負荷を排除

管理対象サーバーの各アカウントのパスワードの定期変更を自動実行します。パスワードの複雑性や変更頻度、変更処理の実行時間はサーバーごとに設定が可能です。

設定したパスワードはESS AdminGateが管理し、アクセスする際に自動投入されるため、各サーバー、IDごとに異なるパスワードをユーザーが管理する必要はありません。





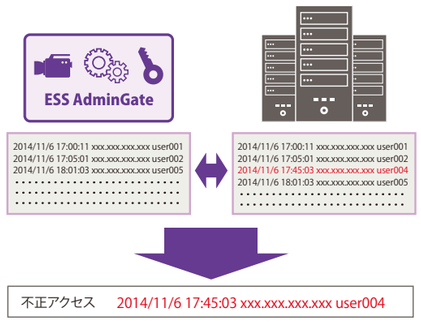
ESS AdminGateサーバーを設置するだけで社内の複数のサーバーのセキュリティ対策を包括的に実現

ログ管理（アクセスログ）

サーバーへの不正アクセス・未許可アクセスを発見

管理対象のサーバーから定期的にアクセスログを収集し、ESS AdminGateを介していない不審なアクセスを抽出します。

これによりサーバーへの不正なアクセスを早期に発見し、水際の対策を講じることで、情報漏洩などの被害を防止します。



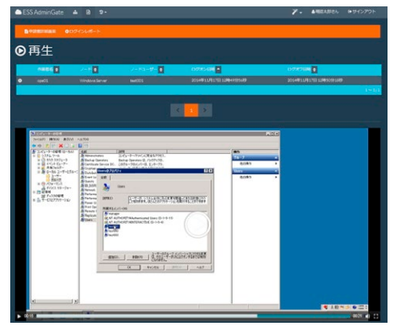
ログ管理（操作ログ）

システム管理作業時の誤操作や不正操作を抑止・発見

アクセス許可に基づくサーバーに対する操作中のデスクトップの動きを動画で記録します。

操作内容の録画は、不正操作への高い抑止効果を発揮するほか、システムトラブル発生時に記録データを再生し確認することで、トラブルの原因究明を行い、作業品質を向上させることができます。

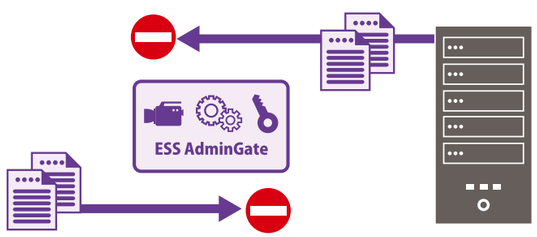
※Linuxサーバーに対するコマンド操作はテキストで記録します。



情報漏洩対策・不正ファイル持ち込み防止

情報漏洩防止 サーバーのマルウェア感染を防止

サーバーからのファイル持ち出しやサーバーへのファイル持ち込みを無断で行えないように制御します。また持ち出しファイルの内容を検査し、個人情報やマイナンバーの有無を検出します。



小規模システムにも適用可能な導入のしやすさ・管理のしやすさ

導入が簡単
仮想アプライアンス形式でご提供するため、仮想環境にインストール済のイメージをインポートするだけでインストール作業は不要です。簡単な設定後、すぐに使用開始できます。

管理が簡単
蓄積した記録データ等のアーカイブや過去データの削除は、管理画面からの簡単な操作で行えるなど、設定や管理が簡単に行えます。

初期投資が不要
年間サブスクリプション型のライセンス体系のため、初期費用がかかりません。また規模拡大や縮小に応じて順次費用を見直せますので、不要な支出を抑えることが可能です。