ENCOURAGE TECHNOLOGIES

変革するビジネス、変化するシステム環境、一貫性ある運用基盤
ESS SmartIT Operation

エンカレッジ・テクノロジの PCI DSS関連ソリューションのご紹介

2012/7/25

エンカレッジ・テクノロジ株式会社
マーケティング部　日置　喜晴

ENCOURAGE TECHNOLOGIES

変革するビジネス、変化するシステム環境、一貫性ある運用基盤
ESS SmartIT Operation

Today's Agenda

- エンカレッジ・テクノロジ社のご紹介
- 弊社製品ラインナップとPCI DSSへの貢献ポイント
- ユニークなコントロール例

ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

会社概要

- **社名：エンカレッジ・テクノロジ株式会社**
  Encourage Technologies Co., LTD.

資本金：	1億2,650万円（2012年1月現在）
設立　：	2002年11月1日
事業内容：	コンピュータシステムソフトの開発・保守並びに販売 コンピュータ運用管理に関するコンサルティング
所在地：	東京都中央区日本橋小網町3-11 日本橋SOYICビル

Value & Satisfaction

お客様の視点で新たな価値を創造し、満足いただける製品とサービスを提供します。

Happiness

社員と会社の目的を一致させ、物心一体の幸福を追求します。

Compliance

国内外の法令と企業倫理を遵守し、誠実かつ公平に業務を遂行します。

ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

導入企業

大手金融、通信業をはじめ360社以上のお客様が弊社製品をご採用

- 株式会社アイ・エイチ・アイ　マリンユナイテッド
- 株式会社アイネス
- 株式会社アイネット
- アイフル株式会社
- 株式会社インテック
- 株式会社ウッドワン
- SMBCファイナンスサービス株式会社
- SCSK株式会社
- NTTコムウェア株式会社
- NTTコムウェア・ビリングソリューション株式会社
- 株式会社NTTデータ
- 株式会社NTTデータアイ
- 株式会社NTTデータSMS
- 株式会社NTTドコモ
- NTTビジネスアソシエ株式会社
- オリックス・システム株式会社
- オリンパス株式会社
- キヤノンITソリューションズ株式会社
- 財団法人建設業技術者センター
- 湘南信用金庫
- 新日鉄ソリューションズ株式会社
- 株式会社シンプレクス・コンサルティング
- スバルシステムサービス株式会社
- 双日株式会社
- ソフトバンクモバイル株式会社
- 第一生命保険株式会社
- TIS株式会社
- 東京海上日動システムズ株式会社
- ドコモ・システムズ株式会社
- 日興コーディアル証券株式会社
- ニッセイ情報テクノロジー株式会社
- あいおいニッセイ同和損害保険株式会社
- 日本システムウエア株式会社
- 日本電信電話株式会社
- 株式会社みずほ銀行
- 株式会社みずほコーポレート銀行
- 三菱ＵＦＪ信託銀行株式会社

ENCOURAGE TECHNOLOGIES

加速するビジネス、変化するシステム環境、一貫性ある運用基盤
ESS SmartIT Operation

ET社製品戦略

加速するビジネス、変化するシステム環境、一貫性ある運用基盤

ESS SmartIT Operation

Technology for the People
人の業務を支える技術

Technology for the Business
ビジネスを推進する技術

System Independency
システムからの独立性を確保する運用基盤アーキテクチャー

業務システム、基幹システム

ENCOURAGE TECHNOLOGIES

加速するビジネス、変化するシステム環境、一貫性ある運用基盤
ESS SmartIT Operation

エンカレッジ・テクノロジの 特権ID管理ソリューション

システム操作と特権ID管理のための共通ワークフローコンポーネント
ESS SmartIT Operation ワークフロー

自動突合による特権ID利用内容の統制
ESS AutoAuditor

エージェントレスで実現する特権ID管理
ESS AdminControl

特権IDを利用したシステム操作の証跡管理
ESS REC

本人確認ソリューション
ID Inspector

ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

ET特権ID管理の機能概要

SIOワークフロー

作業申請 → 承認 → 作業 → 作業報告 → 確認

ESS AdminControl

- 定期パスワード変更
- 特権ID自動貸出
- 特権ID自動返却
- ログイン履歴突合レポート

ESS AutoAuditor

- クライアント用アカウント払出
- クライアント用アカウント抹消
- 操作内容突合レポート

ESS REC&IDI

- 操作内容の克明な記録本人確認
- 詳細点検

ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

EAC 専用クライアントによるセキュアな特権ID利用環境

承認され作業申請の中で作業者として指定されたユーザーだけに一覧が表示される。

自動ログオン機能により特権IDのパスワードは隠ぺいされたまま接続完了

共有IDでも使用した個人を特定できる履歴が残る

作業者A

作業者Aの個人IDで認証

Aさんの作業一覧

操作対象のサービスに自動接続

作業者B

作業者Bの個人IDで認証

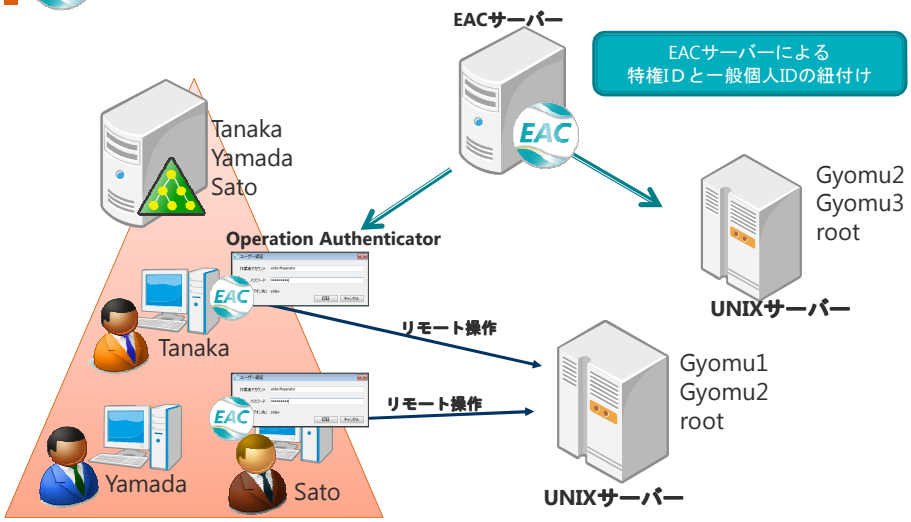
Bさんの作業一覧

操作対象のサービスに自動接続

パスワードは隠ぺいされているので、直接アクセスもできない

ENCOURAGE TECHNOLOGIES
ESS SmartIT Operation

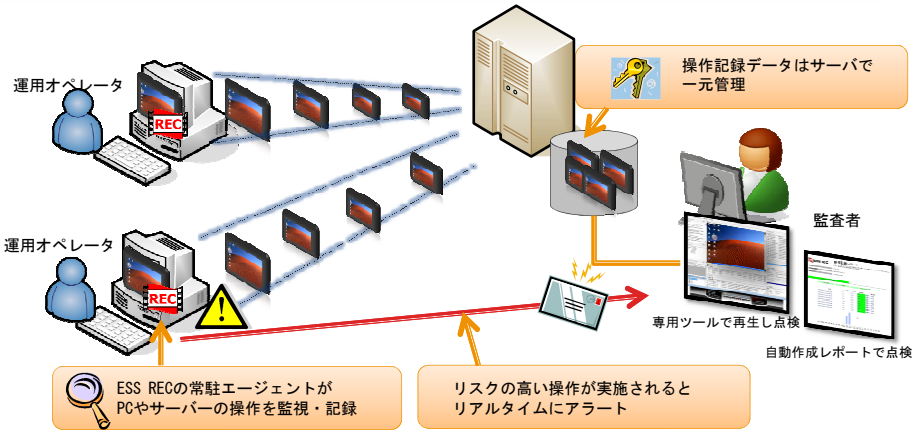
EACによる共有ID使用の個人特定



ENCOURAGE TECHNOLOGIES
ESS SmartIT Operation

システム証跡管理のデファクト ESS REC

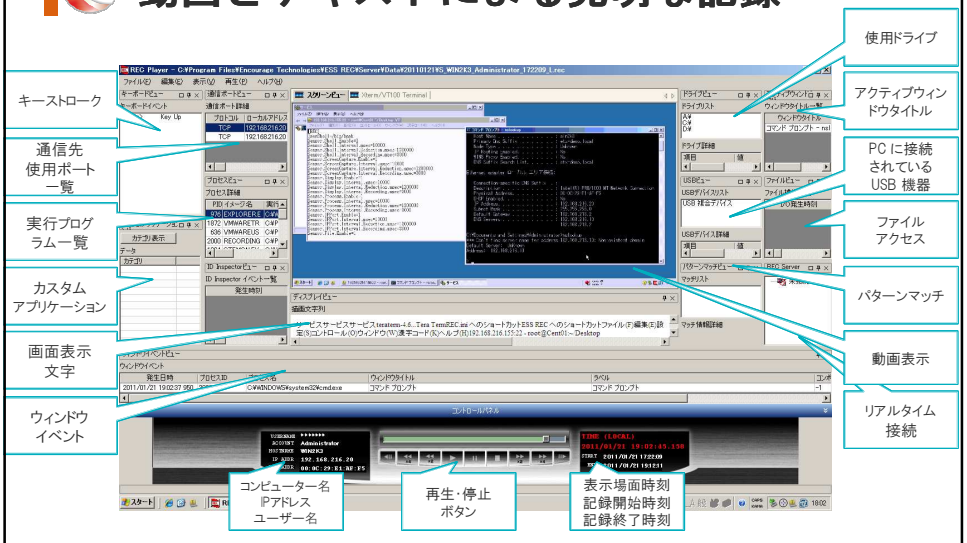
PCやサーバーの操作内容を動画・テキストで記録・蓄積、記録データをもとに操作内容の点検・監査を効果的に行うことにより、システム操作に関わるリスク管理を実現するシステム操作の点検・監査ソリューション



ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

動画とテキストによる克明な記録



ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

3年連続 市場シェアNo. 1

本人確認ソリューション ID Inspector(IDI)

① Windowsシステム認証後、一定時間端末が未使用の後再使用する場合や、**操作途上にあらかじめルール設定した特定のアプリケーション利用や通信利用が発生すると**、本人確認画面が表示され、操作が一旦ロックされます。

② 本人確認要求に対し、個人のIDとパスワードまたはFeliCaカードを提示することで、現在のシステムの使用者を特定し、画面ロックを解除します。

③ 本人確認した情報を蓄積、解析し、本人確認総合レポートを出力

PCI DSSへの貢献

要件7 PCI DSS	要件8 PCI DSS	要件10 PCI DSS
カード会員データへのアクセスを、業務上必要な範囲内に制限すること	コンピュータにアクセスできる各ユーザーに一意の ID を割り当てる	ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡及び監視する

～エンカレッジ・テクノロジ製品～
ESS SmartIT Operation がトータルにサポート！

ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

要件別 適用ポイント

要件7　カード会員データへのアクセスを、業務上必要な範囲内に制限すること

項　番	要件	弊社製品による対応
7.1	システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。	**ESS AdminControl**は、特権IDを承認ベースによって貸出し、承認がなければ通常は利用できない環境を提供します。 ・ワークフローによる申請・承認プロセスの自動化 ・承認ベースで作業者に貸出し、作業終了後に返却する手続きの自動化 ・未承認アクセスをチェックするためのログ収集とレポーティング
7.2	複数のユーザーを持つシステムコンポーネントに対して、ユーザーの必要な範囲に基づいてアクセスを制限し、特に許可されていない限り「すべてを拒否」に設定した、アクセス制御システムを確立する。	

ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

要件別 適用ポイント

要件8　コンピュータにアクセスできるユーザーに一意のIDを割り当てる

項　番	要件	弊社製品による対応
8.1	すべてのユーザに、システムコンポーネントまたはカード会員データにアクセスするための一意の ID が割り当てられていることを確認する	**ESS AdminControl**は、共有IDであっても、承認ベースで指定されたユーザーのみが利用できる環境を提供することで、一意にIDを割り当てられない環境に対して妥当な代替コントロールを提供します。 **ID Inspector**は、個人IDでの利用が想定されていないアプリケーションをカスタマイズすることなく、利用者の特定を行います。
8.2	一意の割り当てに加え、以下の方法の少なくとも１つを使用してすべてのユーザーを認証する。 1)パスワードまたはパスフレーズ 2)2因子認証（トークンデバイス、スマートカード、生体認証、公開鍵等）	**ID Inspector**は、認証機能を持たない設計のアプリケーションをカスタマイズすることなく、IDとパスワードまたはFeliCaカードを利用した本人確認を行うことで、一意のユーザーの確認と代替的な認証手段を提供します

ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

要件別 適用ポイント

要件8　コンピュータにアクセスできるユーザーに一意のIDを割り当てる(続き)

項　番	要件	弊社製品による対応
8.3	従業員、管理者、および第三者によるネットワークへのリモートアクセス（ネットワーク外部からのネットワークレベルアクセス）には2因子認証を組み込む。RADIUS, TACACSとトークン、またはVPNと個々の証明書などのテクノロジを使用する。	**ID Inspector**は、2因子認証に対応していないアプリケーションをカスタマイズすることなく、パスワードとFeliCaカードによる本人確認を行う代替策を提供します。
8.5	すべてのシステムコンポーネントで、以下のように、消費者以外のユーザおよび管理者に対して適切なユーザ識別と認証管理を確実に行う。 8.5.1 ユーザIDなど識別子の管理 8.5.3 初期パスワードの変更 8.5.4 契約終了したIDの取り消し 8.5.5 90日ごとの未使用IDの棚卸	**ESS AdminControl**は、特権IDについて申請・承認フローに従い、確実な貸出管理を行い、共有IDの利用者の識別と、利用者しか利用できない特別な認証の仕組みを提供します。 また使用されていないアカウントの棚卸しを行います。

ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

要件別 適用ポイント

要件8　コンピュータにアクセスできるユーザーに一意のIDを割り当てる(続き)

項　番	要件	弊社製品による対応
8.5	8.5.6 リモートアクセスのためにベンダが使用するアカウントは、必要な期間のみ有効にする。ベンダのリモートアクセスアカウントが使用されている間、そのアカウントを監視する。	**Remote Access Auditor**は、外部ベンダーによるリモートアクセスの実施中の操作内容を監視・記録します。
	8.5.8 グループ、共有、または汎用のアカウントとパスワードなどの認証方法を使用しない	**ESS AdminControl**は、特権IDの定期的なパスワード変更を、使用文字数、複雑性などのポリシーに従い自動的にランダム化します。
	8.5.9 少なくとも 90 日ごとにユーザパスワードを変更する	
	8.5.11 数字と英文字の両方を含むパスワードを使用する。	
	8.5.12 ユーザが新しいパスワードを送信する際、最後に使用した 4 つのパスワードと同じものを使用できないようにする。	

ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

要件別 適用ポイント

要件10　ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する

項　番	要件	弊社製品による対応
10.1	システムコンポーネントへのすべてのアクセス（特にルートなど管理者権限を使用して行われたアクセス）を各ユーザにリンクするプロセスを確立する。	**ESS REC**は、Windows、UNIX、Linuxのオペレーションシステムおよびアプリケーションに対する操作内容を動画と20項目以上のテキスト情報によって記録し、人の操作に関わる様々なインベント追跡を可能にします。 **ESS AdminControl**は、Windows, UNIX/Linuxオペレーティングシステムのログオンイベントを収集し、未許可のアクセスの有無を点検する仕組みを提供します。
10.2	重要なイベントを追跡するために、すべてのシステムコンポーネントの自動監査証跡を実装する。	
10.3	イベントごとに、すべてのシステムコンポーネントについて重要情報の監査証跡エントリを記録する。	
10.4	変更できないよう、監査証跡をセキュリティで保護する。	**ESS REC**の操作記録は鍵方式によって暗号化され保護されています。

ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

要件別 適用ポイント

要件10　ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する（続き）

項　番	要件	弊社製品による対応
10.5	監査証跡の履歴は少なくとも1年間は保持する。少なくとも3ヶ月はすぐに分析できる状態にしておく。（オンライン、アーカイブ、バックアップから復元可能など）。	**ESS REC**の操作記録はファイル形式によって保存されるため、通常のファイルに対する世代管理の考え方にのっとってバックアップ、アーカイブを行うことが可能です。
10.6	少なくとも日に一度、すべてのシステムコンポーネントのログを確認する。ログの確認には、侵入検知システム（IDS）や認証、認可、アカウンティングプロトコル（AAA）サーバ（RADIUS など）のようなセキュリティ機能を実行するサーバを含める必要がある。	**ESS AutoAuditor**と**ESS REC**は、ログの確認作業を「要点検個所」の有無を自動的に解析する機能を提供し、ログ確認作業の工数を大幅に削減します。 **ESS AdminControl**は、Windows, UNIX/Linuxオペレーティングシステムのログオンイベントを収集することで、確認作業を効率化します。

ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

特長① 共有IDの使用者を特定

- **PCI DSSでは、基本的に共有IDの使用を禁止（要件8)していますが、対応が困難な場合も想定されます。**
  - メインフレームなど個人IDとパスワード等で認証を必要としないシステム。
  - 24時間常時監視など交代勤務等でログオフ、ログオンが困難な端末

ESS AdminControlまたはID Inspectorを使用すると、共有IDを使用しながら、利用者を特定するという代替コントロールが可能

■**ESS AdminControl**はWindows/UNIX/Linux OSの共有IDの使用者個人を特定
■**ID Inspector**は、**アプリケーションのカスタマイズを行わなくても**共有IDの使用時に使用者を特定することが可能

ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

特長② 要素認証に対応できない アプリケーションの代替コントロール

PCI DSSでは、リモートアクセス時の認証には2要素以上の認証を要求しています。しかし、アプリケーションが多要素認証に対応いていない場合、アプリケーションのカスタマイズが必要になってしまいます。

ID Inspectorはリモートアクセス時の認証画面が表示されると、FeliCaカードを要求した本人確認を行う設定が可能です。FeliCaカードの提示がなければ、デスクトップがロックされるため、リモートアクセスのアプリケーションを利用できなくなります。

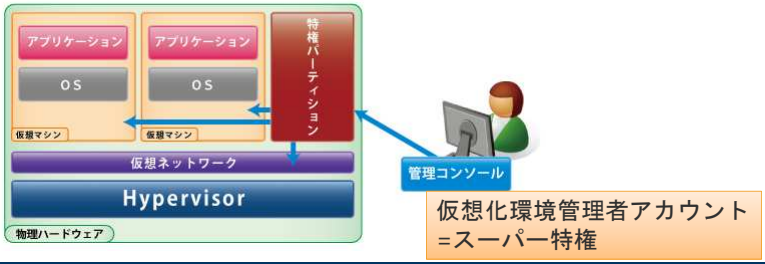
アプリケーションを一切カスタマイズせず、
FeliCaカード＋パスワードによる多要素認証を事実上実現

ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

特長③仮想環境における管理者操作を透過的に記録する

- 仮想化環境におけるカード情報セキュリティに関して、11におよぶ固有の課題と留意点を**「Information Supplement: PCI DSS Virtualization Guidelines」**の中で定義
  - 「Immaturity of Monitoring Solutions」
    -「ログ取得などのソリューションが未成熟」
  - 「Lack of Separation of Duties」-「職務分掌が欠落」



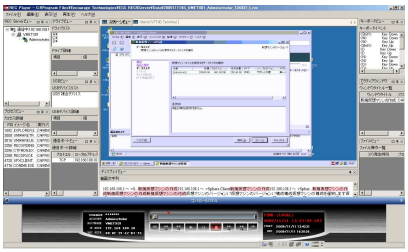
仮想化環境管理者アカウント
=スーパー特権

ENCOURAGE TECHNOLOGIES

ESS SmartIT Operation

特長③仮想環境における管理者操作を透過的に記録する

- **解決策**
  - ESS RECによる、仮想環境の管理者の透過的な操作記録
- **解決内容**
  - デスクトップの動画記録により、仮想化レイヤ（ハイパーバイザー、仮想ネットワーク、仮想マシン、および仮想マシン上のOSやDB、アプリケーションに対する操作）を透過的に記録する
  - 職務分掌が未成熟である点の代替コントロールとして操作内容を詳細に記録し、モニタリング。



トータルソリューションとしてのメリット

- **共通のアーキテクチャーと相互互換性**
  - 同一製品群として、共通のアーキテクチャーとコンポーネント間の連携が、設計・導入工数を抑えます。
  - 機能拡張時にも、製品群としての機能連携や整合性を保証します。
- **ワンストップでのサービス提供**
  - 障害、ノウハウなどの問い合わせサービスなど、ワンストップでの提供が可能です。

まとめ

- **弊社特権ID管理ソリューション各製品は、PCI DSSの要件7,8および10の広範な要件に対して、広くカバーするソリューションです。**
- **特に以下の3つのポイントは、要件上、比較的対応が困難な部分について、妥当かつ有効な代替コントロールとしても活用可能**
- **共通のアーキテクチャーや機能連携により、導入時のSIなどコストを圧縮し、将来にわたって、ワンストップでのサポートを提供。**

ご清聴ありがとうございました。

http://www.et-x.jp

メールアドレス：etx-mktg@et-x.jp