Case Study

株式会社アイネット　様

クレジットカード決済処理システムにおけるPCI DSS準拠でESS RECを採用、有効的かつ効率的なアクセス記録と点検・監査を実現

株式会社アイネット（以下、アイネット）は、1971 年の創立以来、データセンターを軸にシステム開発、運用・保守や BPO サービスを一貫して提供している独立系 IT サービスプロバイダーです。幅広い分野で長年培ったシステム開発経験・ノウハウを活かし、石油・エネルギー業や金融業の分野においては、稼働後の運用、クレジットカード決済処理、コールセンター業務等も含めた、トータル・アウトソーシングの実績が数多くあります。

2009 年 6 月には、国内最高クラスの安全性と最新のテクノロジーを備えた次世代型データセンターが稼働し、「仮想化オール・イン・ワン サービス（VAiOS：Virtualization All in One Services）」を開始するなど、最新技術を取り入れた新サービスの提供も積極的に行っています。

また、お客様に安心、安全、高付加価値の製品・サービスを提供するため、プライバシーマーク、ISO/IEC 27001（情報セキュリティマネジメントシステム）、ISO 9001/2000（品質マネジメントシステム）といった各種認証を取得し、従業員教育にも力を注いでいます。

お客様に常に最適なソリューションを提供しているアイネットに、PCI DSS への準拠対応について聞きました。

Profile

株式会社アイネット

設　　立　1971年（昭和46年）4月22日
本社所在地　横浜市西区みなとみらい 3 丁目 3 番 1 号 三菱重工横浜ビル 23 階
U R L　http://www.inet.co.jp/
事業内容　データセンターを軸にシステム開発、運用・保守をはじめクラウドコンピューティング、仮想化サービス、さらに BPO サービスなどの各種 IT サービスを、幅広い分野へワンストップで提供。

< 導入製品 >

ESS REC®

SS本部
第1SS事業部
クレジットサービス部
部長 大里　博司 氏

ITマネージドサービス事業部
SSサポート部
技術課
係長 石塚　秀樹 氏

課題　お客様システム環境におけるPCI DSS基準への準拠

✓ クレジットカード情報保護の要請

アイネットでは大量のクレジットカード情報の決済処理を行うシステムの設計・構築・運用、さらには関連するコールセンター業務を受注しました。

クレジットカード情報はセンシティブな情報であるため、個人情報同様にセキュアな対応が求められています。とりわけカード業界においては、PCI DSS（Payment Card Industry Data Security Standard）というセキュリティ基準が制定され、クレジットカード情報を取り扱う事業者に対して、準拠が求められていました。このような背景から、受注したシステムの PCI DSS 準拠に向けた検討が開始されました。

✓ 要件 10：カード情報のアクセスの証跡は、OS の機能だけでは足らない

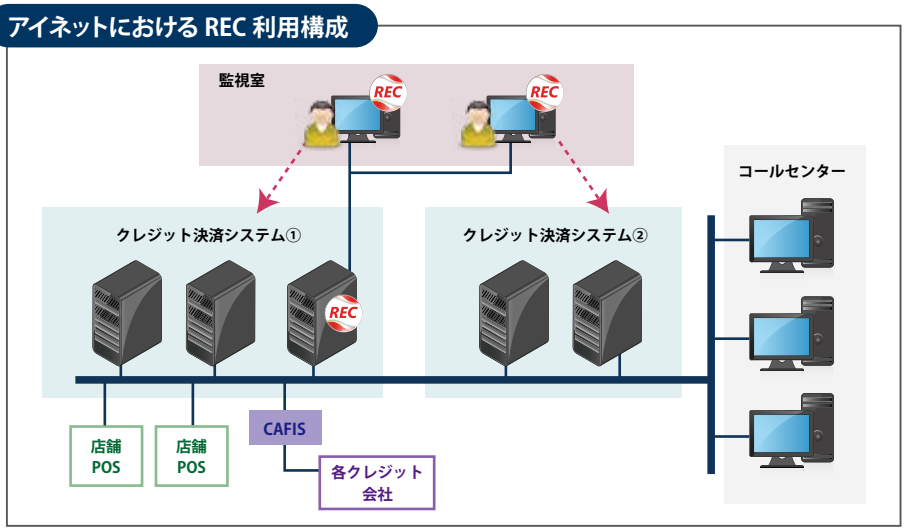
PCI DSS 基準は、12 項目からなる要件で構成されており、基準を満たすためには、いくつかのツール・ソリューションを導入する必要がありました。

なかでも要件 10 は「ネットワーク資源およびカード会員データに対するすべてのアクセスを追跡し、監視すること」と定められており、カード情報にアクセスされた記録を保存し、不正なアクセスの有無を監視する仕組みの構築が必要でした。

各サーバやネットワーク機器、ミドルウェアのログは専用のツールで管理していますが、システムに実際に触れる社員の不正アクセス監視・抑止には別の対策が必要でした。当初は Active Directory など Windows OS の機能を活用し、アクセスユーザーの管理を検討しましたが、管理方法や導入されているミドルウェアとの相性から最適なソリューションとはいえないと判断しました。

また、ログは収集していますが、有事の際にその保管された膨大な量のログによる解析は、担当者のスキルに依存するケースもあるため、属人的になること、また、解析の工数が膨大になってしまう恐れがありました。

アイネットにおける REC 利用構成



ENCOURAGE TECHNOLOGIES

効果　PCI DSS基準への準拠と点検・監査の工数削減

✓アクセス経路の絞り込みと操作内容そのものを記録

ESS REC に出会ったのは、2009 年 2 月に開催されたセミナー会場でした。操作内容そのものを動画で記録するというアプローチは「人によるカード情報へのアクセスの監視・追跡」という点で PCI DSS 基準に準拠するシステム要件に対応可能ではないかとの印象を持ちました。

検討を重ねた結果、システム要件への対策として、

・操作可能な端末を特定室へ設置する

・操作可能な端末へ ESS REC を導入し操作内容を記録する

の 2 点を採用しました。

✓製品の分かりやすさと抑止効果も評価

クレジット決済システムは 2010 年春に本格稼働を開始、同時に特定室内に設置された操作端末からの操作を ESS REC を利用して記録しています。

「ESS REC で取得した記録データは、監査において非常に有効だと考えています。PCI DSS の予備審査においても、担当のコンサルタントより効果のある対策だとお墨付きをいただきました」（石塚氏）

ESS REC では、動画で記録したデータの文字列検索や絞り込み検索ができるため、ログの抽出・チェック・分析をスムーズに行うことが可能です。その結果、点検・監査の有効性が高まるとともに、それにかかわる工数削減にも大きく貢献しています。

「さらに、ESS REC の管理や設定は GUI で行うため、直感的に理解しやすく、担当者のスキルに左右されません。また、操作画面が記録されていることを関係者へ事前に周知することで、システムに対する不正アクセスの抑止効果を期待しています。また、収集した記録を解析する際にも映像から文字列検索し、該当箇所から映像を再生することができるため、視覚的にも理解しやすく、調査や追跡に関わる工数の削減が可能であると認識しました」

展開　効果的かつ現実的な、更なるセキュリティ体制強化に向けて

✓コールセンターへの展開

アイネットでは、ESS REC を利用した要件 10 への準拠の範囲をさらに拡大する計画を進めています。

「現在は、特定室における内部オペレーションの使用に特化していますが、クレジットカード番号を使用するコールセンター業務にも導入し、オペレータの監視強化も図りたいと考えています」（石塚氏）

（写真：アイネット データセンター）

✓セキュリティ対策についてのお客様の理解が重要

大里氏は、インタビューの最後に、今回の PCI DSS 準拠への取り組みに関して、

「ESS REC のようなツールを入れたことが、社員の意識啓蒙につながります。平時における不正アクセス抑止というのはもちろん、万が一事故が起きた場合に操作内容の追跡ができるということは、システム要件として必要です。当社のようなデータセンター事業においては、セキュリティ対策は重要な取り組みであるとともに、企業の社会的責任として、有事に備えた対策をより強化していきたいと考えています。

また、最終的な目的である『クレジットカード保有者の保護』を実現させるためにお客様と共に考えていきたい。当社の取り組みとしてデータセンターの安全性、セキュリティ強化の追求は今後も図っていきますが、PCI DSS のような基準を満たすためには、求められるシステム、運用要件に特化した対策も必要になってきます。お客様自身もセキュリティ対策には一定のコストがかかることを是非ご理解いただきたいですね」とコメントされました。

お問い合わせは

ENCOURAGE TECHNOLOGIES

開発元

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
URL　：http://www.et-x.jp
Phone ：03-5623-2622
Fax　：03-3660-5822

<CS13-2013-11-01>