Case Study

iret アイレット株式会社 cloudpack事業部 様

AWSのプレミアコンサルティングパートナーが SOC2取得のために選択した自社サービスの安全対策

アイレット株式会社（以下、アイレット）は、2003年に設立した、システム開発から保守・運用までを一貫して行うITソリューションプロバイダーです。

2010年にクラウドの設計導入、運用・保守を行うcloudpackサービスを開始し、翌年にはアマゾン ウェブ サービス(AWS)のソリューションプロバイダーに登録し、AWSクラウド（※1）を利用したシステムインテグレーションに注力、2013年にAWSの最上位パートナーであるプレミアコンサルティングパートナーに国内で初めて認定されるなど、AWSを中心にクラウドサービスを利用したITシステムの設計・導入、運用保守において多くの実績を有しています。

Profile

アイレット株式会社

設　　立	2003年（平成15年）10月15日
本社所在地	東京都港区虎ノ門 1-23-1 虎ノ門ヒルズ森タワー 7F
U R L	https://www.iret.co.jp/
事業内容	システムの開発から保守・運用までを行うITソリューションプロバイダー。特にAWSへの導入設計や環境構築、運用・保守、支払い代行までをサービスとして提供するなど、クラウドへの取り組みに力を入れる。

＜導入製品＞

REC ESS REC

セクションリーダー
情報セキュリティ管理責任者
齊藤 愼仁 氏

ソリューションアーキテクト
磯辺 和彦 氏

課題と選択

AWSと同等のセキュリティ認証を取得しお客様に安心と安全を

✓ 自社サービスにおける高度なセキュリティ対策の実現を目指す

お客様のシステムを24時間365日運用・保守を行うcloudpackに信頼を置いていただくためには、システムに対する安全性と可用性を担保する仕組みの整備、またそれを客観的に評価可能な認証制度の取得が必須です。AWSを基盤に利用している以上、AWSが取得している国際認証を取得することを目標に、アイレットでは体制と仕組みの整備を実施してきました。すでに数百社のお客様の数千以上にも及ぶサーバー群で構成される多くのシステムに、万が一支障が生じることは避けなければなりません。

ISO27001、PCI DSS等の認証取得を実現したアイレットが次に対応を目指したのが、SOC2報告書（※2）の取得です。監査法人による第三者評価の結果を報告書として受領し、お客様に開示することになるため、他の認証制度よりも厳格なルール、体制および仕組みを構築し、確実に実行していく必要があります。

✓ 運用上のセキュリティ保持：操作ログの取得と保存に課題

cloudpackではお客様のシステムに対し変更作業を行うため、スタッフが操作を行うことがあります。このような運用において、第三者が不正にお客様システムにアクセスしたり、スタッフが本来行うべき以外の作業を行ったりしないようにする仕組みが必要でした。

そこで、スタッフがお客様システムへアクセスする際に踏み台サーバーとなるインスタンスを設置し、お客様のシステムへは、踏み台インスタンスからしかアクセスできないようネットワークで制御する方式をとることとしました。

しかしこれだけでは、第三者の不正アクセスを防止できるものの、不正な操作を防ぐ対策にはなりません。そこで踏み台サーバー上での操作を監視、ログとして記録し保存する方法を検討しました。

「AWS上のインスタンスは9割以上がLinuxです。Linuxだと、基本的にコマンド操作なので、ログを取得するのはさほど難しくないと思っていました。しかしWindowsはGUI操作ですので、『これはどうやって証跡を取得しよう』と悩みました」（磯辺氏）

しかし詳細を調査してみると、Linuxコマンドでさえ、OSの標準機能やオープンソースでは、改ざんされることなく確実に記録することが難しいことがわかりました。

✓ コマンド・GUI操作の証跡取得、国内でのサポートの手厚さが選定のポイントに

「調査によって検討対象に浮上したESS RECの機能詳細を確認し、『本当にこんなことができるのであればすごい』と話したのを覚えています。Linuxコマンドであっても、Windows上の操作であっても、動画形式で克明にログとして記録できるのです。記録だけではなく、リアルタイムに監視することも可能というのは驚きました」（磯辺氏）

他の製品とも比較検証を行いましたが、結果として以下の2つのポイントが決め手となりESS RECの導入を決定しました。

■ コマンド記録の網羅性に加え、GUI証跡の取得も可能

ESS RECはLinux/Windowsといったプラットフォームによらず、共通のモニタリング手法が可能です。コマンド情報の網羅的取得、GUI操作の動画での証跡取得をひとつのアプリケーションで実現できる点が大きな選定のポイントとなりました。

■ 日本国内での一貫した開発からサポート体制

「海外の製品は、日本国内のユーザーを主たる対象として開発・販売しているわけではありません。また開発は海外の本社で行われています。そういった製品では『こうしたい、こうしてほしい』と思った時に期待通りの対応をしていただくのは難しいのが現状です。国内で作っているアプリケーションは、ユーザーの声が届きやすく、意思を汲み取ってくれます」（齊藤氏）

ENCOURAGE TECHNOLOGIES

導入と効果　お客様に安心してご利用いただける客観的な認証を取得

✓ 顧客システムへの操作を全て取得、インシデント発生時の記録確認にも有効

オンプレミスの場合では、サーバーのサイジングやネットワーク変更などインフラ設計が重要ですが、クラウドでは、展開後でも容易に見直し・変更ができます。そのため、ある程度の目安でサイジングをして、まず展開してみる方法をとることで、導入までの期間を大幅に短縮できます。

「検証のために構築したインスタンスをそのまま本番環境用に転用しました。検討時、証跡が取れないという事象がありましたが、エンカレッジ・テクノロジの方にご協力いただいて終息しました。特に大変だったということはありませんでした」（齊藤氏）

スピード感を重視するアイレットでは、2014年11月末にESS RECに関する詳細調査を開始し、1か月後の12月末にはESS RECの検証を終了し最終選定、1月中旬には運用を開始し、SOC2監査に間に合わせるという短期間での課題解決を成し遂げました。

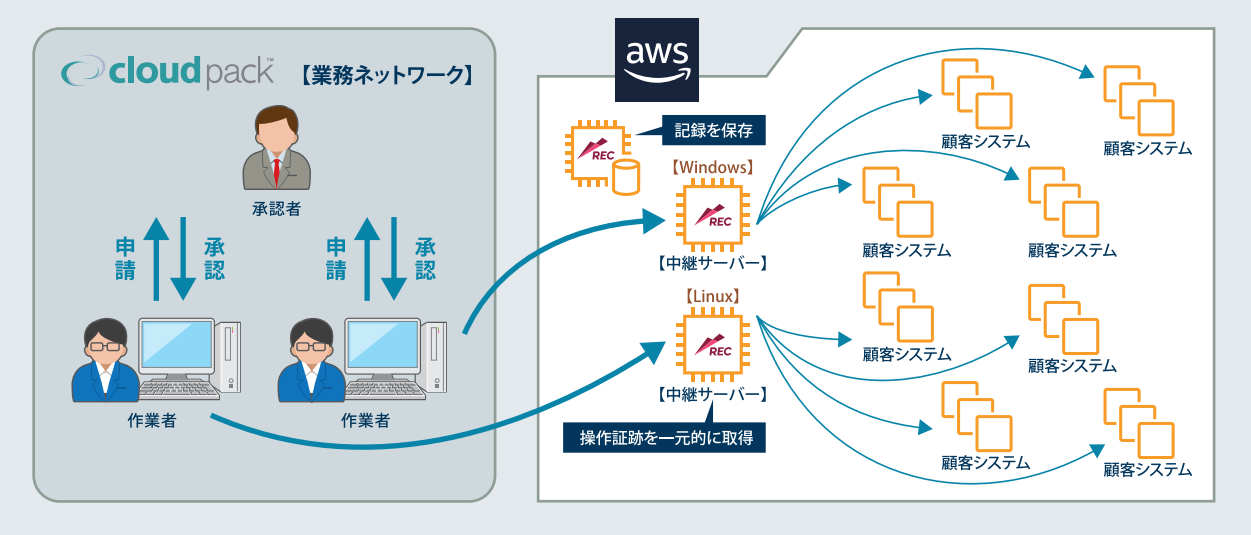
現在、お客様システムに対する作業を行う際は、cloudpack業務ネットワークからAWS上に設置されたWindows用、Linux用の踏み台インスタンスを経由しなければ、お客様システムにアクセスできないように制御されています。踏み台インスタンスへのアクセスには業務ネットワークとの統合認証により、作業者以外はアクセスできないように制御し、第三者による不正なアクセスを防止、踏み台インスタンス上で行われた操作を動画とテキストで取得しています。これにより、業務外の不正な操作の抑止と早期発見が可能になりました。

「アクセス方法を中継サーバー経由にすることで、ログの取得と合わせて、『いつ』『誰が』アクセスしたかを明確にすることも目的でした」（齊藤氏）

アイレットでは、顧客システムの障害対応時、ESS RECで取得した記録を確認したうえでの対応を実施しています。

アイレットは、2015年8月、SOC2 Type1の報告書を受領しました。課題の一つであったシステム操作のセキュリティ対策については、監査上、大きな問題を指摘されることはありませんでした。

「実際にお客様環境へのアクセス状況や、実際の作業の記録の取得状況を説明するとともに、サンプリングを抽出して実際の操作ログを開示する必要がありました。実績が豊富なため、監査人がESS RECを理解されており、仕組みを説明する必要はありませんでした」（齊藤氏）



（図 ESS RECを導入後のアイレット）

展開　さらなるセキュリティ強化を目指した取り組み

✓ 中継サーバーをより活用したアクセス制御を検討

システムへのアクセスがすべて中継サーバーを介した運用へ変わったことに対し、アイレットではこの中継サーバーを利用したさらなるセキュリティ強化を考えています。

「現在、中継サーバーへのアクセスは、作業内容を起票し、リーダーによるダブルチェックと承認がなされたうえで実施しています。この社内の承認作業に関して、『許可を得て作業をする』のではなく『許可を得なければ作業できない』という仕組みをシステム的に確立したいと考えています」（齊藤氏）

お客様への信頼を第一に考えるアイレットは、今後も高いセキュリティ体制の確立への取り組みを実施していきます。エンカレッジ・テクノロジはこうしたアイレット様の取り組みのサポートに努めてまいります。

お問い合わせは

※1 AWSクラウド：アマゾン ウェブ サービス(AWS)が提供しているクラウドサービス。
Amazon Elastic Compute Cloud(Amazon EC2)と呼ばれるIaaSを中心に様々なサービスを展開。
※2 SOC2：米国公認会計士協会(AICPA)が定めた委託業務の第三者による内部統制の有効性保証制度。SOC2は、セキュリティや可用性などから、少なくとも1項目以上が対象となり、報告書を特定の利用者に対してのみ開示できる。

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

<CS28-2019-10-01>