FORTRA™

導入事例 CASE STUDY (TRIPWIRE)

SaaSサービスの基盤を Tripwire Enterprise で監視し PCI DSSに準拠した安全性を担保

ネットワーク機器の変更監視を自動化 サービス品質の安全性・信頼性確保に貢献

課題	結果
SaaSサービスをPCI DSSに準拠させ、サービス基盤の安全性を担保したかった	PCI DSS準拠要件を満たし準拠証明書を取得することができ、セキュリティ面で安心できるサービスとしてのお墨付きを得た
エージェントが導入できないネットワーク機器類は手動で改ざんの有無を確認するため、作業負荷がかかっていた	Tripwire EnterpriseのSSH接続で、ネットワーク機器の変更監視作業を自動化することで、1台あたりの作業工数が50%以上削減できた。運用負荷軽減による効率化と自動化によるサービス品質安定化という、両面の課題を実現できた
ハッシュ値の比較だけでは、具体的にどこがどのように変更されたか把握するのが困難だったし、アクションもとれなかった	Tripwire Enterpriseはファイルのベースラインとの比較を行ってくれる製品なので、設定ファイルの変更点を詳細かつ素早く把握でき、さらに適切なアクションも取れるようになった

富士通エフ・アイ・ピー株式会社

導入製品
Tripwire Enterprise

会社概要

商号： 富士通エフ・アイ・ピー株式会社
FUJITSU FIP CORPORATION

本社： 東京都港区芝浦
1-2-1 シーバンス N 館

設立： 1977 年 11 月

代表者： 代表取締役社長 米倉 誠人

資本金： 180 億円

売上高： 1,220 億円(2017 年度、連結)

従業員数： 3,971名(2018 年4月1日現在、連結)

安心できるSaaSサービスの証明として、PCI DSSに準拠

今、市場では、経済産業省と日本クレジット協会が策定した「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」を踏まえ、PCI DSS対応を進める企業が増えています。2018年3月末までに対応が求められたカード会社や決済代行業者、ECサイトや通信販売事業などを運営する非対面取引加盟店に続き、クレジットカード情報を扱う店舗を持つ小売業者などの対面取引加盟店では、2020年3月末までの対応が求められており、準拠に向けて対策を進める企業は増えるばかりです。

富士通エフ・アイ・ピーは全国に設置された富士通のデータセンターを運用し、ITアウトソーシング&クラウドサービス、システムインテグレーションサービス、プロフェッショナルサービス、SaaSサービスを展開。近年はセキュリティ分野のサービス拡充に力を入れてきました。その1つが「PCI DSS準拠支援サービス」です。当サービスは2007年から対応を開始し、2010年に正式リリースしました。コンサルティングからソリューション構築、脆弱性検査など、PCI DSS準拠を目指す顧客をワンストップで支援してきました。

富士通エフ・アイ・ピーSaaSソリューション事業部 主席部長の仁木裕子氏は「支援していく中で、お客様が SaaSサービスを選定する際、セキュリティレベルが重要な選定基準になると感じていました。その基準のひとつが PCI DSSです」と語ります。外部の SaaSサービスを利用する際、セキュリティが懸念事項としてよく挙げられますが、第三者機関からセキュリティが担保されているという証明を得ることで、顧客が安心してサービスを利用できると考えたのです。

そこで、富士通エフ・アイ・ピーはデータセンターの物理的なセキュリティ強化に務めるとともに、自社SaaSのサービス基盤についても PCI DSSの準拠を進めました。

ネットワーク機器の改ざん検知、手作業頼りでは大きな負荷

PCI DSSに準拠するには、約400にも上る項目の遵守が求められます。その1つが、サーバやネットワーク機器、セキュリティ製品の改ざん検知です。同社はこれまで他のサービスにおいて、Windowsや Linuxで構築したサーバの改ざんは別のセキュリティ製品を用いてチェックしていましたが、ネットワーク機器のファームウェアや設定変更については、手動で設定ファイルを取得し、いったんテキストに落としてから差分を確認するという手作業の部分がありました。しかし、この方法で PCI DSSに準拠するには少なからぬ運用負担が予想されました。

そこで目を向けたのが Tripwire Enterpriseでした。市場を見渡すと、Webコンテンツの改ざん検知に特化した製品はいくつもありますが、サービス基盤を構成するコンポーネントの改ざん検知を実現する製品は多くありません。ハッシュ値ベースの比較ではなく、ファイルのベースラインとの比較を行ってくれる製品となると、選択肢はほぼ1つでした。さらに大きな要因が、ネットワーク機器の改ざん検知です。同社セキュリティサービス部の佐藤大起氏は、「ネットワーク機器にはエージェントをインストールすることはできませんが、Tripwire Enterpriseの場合、SSHで接続さえできれば監視ができます」と振り返っています。

さらに仁木氏は「PCI DSSの要件の1つに『正しい構成を維持し定期的に確認すること』『セキュリティを考慮した妥当なパラメータ（設定値）を維持すること』といった項目が明記されています。われわれのお客様もこれを満たすため Tripwire Enterpriseを利用していると聞いており、デファクトスタンダードだととらえています」と付け加えました。

デファクトスタンダードのTripwire Enterpriseを採用し、PCI DSSに準拠

富士通エフ・アイ・ピーではデータセンターで利用していた OSを独自に堅牢化していたことから、当初、インストール作業にやや手間を要したこともありました。これはTripwireに限らず全てのセキュリティ製品に共通する課題でしたが、販売パートナーである京セラコミュニケーションシステムの支援を得つつ導入を進め、稼動を実現したそうです。

今では Tripwire Enterpriseを用いて、ネットワーク機器の他、Windowsサーバや Linuxサーバ数十台の変更監視を行っています。これにより、求められる条件の一つを満たして PCI DSSに準拠し、顧客向けにサービスを提供する際のアピールポイントとして生かしています。

Tripwire Enterpriseは、他のサービスでは手動で対応していたことを自動で対応できるため、運用負荷は大きく軽減されました。加えて、「中にはハッシュ値の比較しか行わず、改ざんの有無しか知らせてくれないものもありますが、それでは設定のどこがどのように変わったのかが分かりませんでした。Tripwire Enterpriseではデータベース側に設定情報が保持されており、アラートメールでもどの行に変更が加えられたかがすぐ分かることもありがたいです」（佐藤氏）

何らかの変更を検出すると管理者にメールで通知するとともに、インシデント管理ツールにトラップを投げ、担当者が対応するフローでサービス基盤を運用しています。このときのアクションを細かく定義できることもポイントの1つです。佐藤氏はさらに「これからは、受け取ったアラートを生かし、より素早く対応できるようにしていきたいと考えています。例えば作業ワークフローシステムと連携し、作業申請書などと付き合わせて、正しい変更か、それとも異常かを自動的に判断できるような仕組みがあれば、もっと助かります」と期待しています。

セキュリティの担保されたサービスを通じて今後も顧客を支援

同社セキュリティサービス部の長澤駿氏は、「PCI DSSでは定期的な監査が求められます。最初の1年だけならば管理者が手作業で監視することも可能でしょうが、それを継続的に回していくとなると、Tripwire Enterpriseのような仕組みが必要だと思います」と述べています。

仁木氏も「何かあったときには検知してくれるという安心感が得られました。お客様から見たときの差別化にもつながるのではないかと期待しています」と述べます。今後は、Tripwire Enterprise自体を SaaSサービスの形で提供することも視野に入れているそうです。

富士通エフ・アイ・ピー
SaaS ソリューション事業
部主席部長

仁木 裕子氏

「導入によって安心感が得られました。お客様から見たときの差別化にもつながると期待しています」

富士通エフ・アイ・ピーセキュリティサービス部

佐藤 大起氏

「Tripwire Enterpriseではデータベース側に設定情報が保持されており、どの行に変更が加えられたかがすぐ分かります」

富士通エフ・アイ・ピーセキュリティサービス部

長澤 駿氏

「監査を継続的に回していくとなると、Tripwire Enterpriseのような仕組みが必要だと思います」

FORTRA™

Fortra.com

Fortraについて

Fortra は、他に類を見ないサイバーセキュリティ企業です。私たちはお客様のために、よりシンプルで強力な未来を創造します。当社の信頼できるエキスパートと統合されたスケーラブルソリューションは、世界中の組織にバランスとコントロールをもたらします。私たちはポジティブ・チェンジメーカーであり、サイバーセキュリティの旅路のあらゆる段階において、お客様の味方となります。詳細については、fortra.com をご覧ください。