



導入事例 CASE STUDY

オフショア開発の提供において 効率的なデバイス制御で 強固な情報漏えい対策を実現し 顧客に安心感を提供

設計・製造分野におけるオフショア開発について、業界を牽引するアールテクノ。同社はインドとベトナムに現地法人を持ち、さまざまなメーカーにサービスを提供しているが、業務上、開発データなど顧客の機密情報を扱うことが多い。そこで同社はより強固な情報漏えい対策を実現するため、DeviceLock（デバイスロック）を導入。これにより、きめ細かなデバイス制御が可能になり、顧客にも安全なサービスを提供している。



オフショア開発における顧客の機密情報に 万全のセキュリティ対策を講じたい

アールテクノは1993年の創業。「設計・製造分野のオフショア開発」や「CAD/CAMシステムの販売」などをビジネスの柱としており、中でもオフショア開発についてはいち早くサービス化に踏み切っている。2001年にインド・チェンナイへ事業所を開設し、2005年には技術者派遣およびオフショア開発をスタート。2006年11月にはベトナム・ホーチミンに現地法人を設立し、同様に技術者派遣とオフショア開発を開始。2016年1月にホーチミンテクノセンター2号館を、12月にホーチミンテクノセンター3号館を設立するなど、事業を順調に拡大させており、先駆者としてこの業界を牽引している。

アールテクノのオフショア開発サービスでは、あたかも海外に顧客の開発拠点の「分室」を作るようなかたちで、完全に独立した専用開発室、専用システム、専用サーバー、専用ネットワーク回線、専任エンジニアをまとめて提供している。さらには、入室に指紋認証を採用し、室内にも監視カメラを設置して作業を録画。操作ログも取得している。この点について常務取締役の淡路 眞吾氏は「お客様は自動車をはじめ、造船、機械など多分野にわたっている。オフショア開発では業務上、開発データなど重要なデータ資産をお客様から借りたり委託されたりしますので、その管理は極めて重要です。そこで情報漏えい対策を検討する中で、課題のひとつとしてデバイス制御がありました。USBメモリやCD/DVDなどは便利な存在ですが、これらを使って不正が行われるリスクもあり、お客様からどのような対策をとっているのか説明を求められることもありました」と語る。



所在地：東京都国立市富士見台2-14-1

創業：1993年12月

資本金：90,038,000円

従業員数：187名

事業内容：CAD/CAMシステムに関するシステムソリューションの提供、マシンングセンター/3次元デジタイザー/3Dプリンターの販売、オフショア開発、オフショアミリング、外国人技術者の派遣・紹介

URL：http://www.r-techno.co.jp/

導入製品・ソリューション

DeviceLock

課題

サービスとしてオフショア開発を提供しているが、開発データなど顧客の機密情報を扱うことが多く、データ資産を確実に保護し、顧客に安全なサービスを提供できる環境を構築しなかった。

解決

端末単位で導入でき、管理サーバー不要の「DeviceLock」を導入することにより、確実かつ利便性を損ねないデバイス制御の管理を低コストで実現できた。

10以上の製品の中から「DeviceLock」を選定 決め手はコストパフォーマンス

アールテクノが対策の検討を行った際、10以上の製品について情報収集を行った。同社が製品を選定する上で評価の基準となったのが機能とコストのバランスだ。デバイス管理製品はサーバーでクライアント（エージェント）を一括管理する製品が一般的だが、これだとひとつの開発室ごとに管理サーバーを立てる費用が発生するため、結果として高くついてしまう。システム事業部 本社 技術サブマネージャーの森田敏彦氏は「そこで管理サーバー不要で利用可能な製品に絞り込み、使い勝手も吟味した結果、低コストにもかかわらず、豊富な機能がスタンドアロン環境でも利用できるDeviceLockの採用を決めました」と当時を振り返る。

また、DeviceLockは管理サーバーを用意しなくても、管理者のPCにインストールした管理コンソールを使ってネットワーク内にあるクライアントに対しポリシー適応などの一元管理を行うことが可能で、最終的にこれが採用の決め手となった。



システム事業部 常務取締役
淡路 真吾 氏



システム事業部 本社 技術サブマネージャー
森田 敏彦 氏

デバイス制御における堅牢性と可用性を実現 上場企業の顧客も安心

現在、アールテクノではDeviceLockをインドとベトナムの開発室に導入している。主としてUSBメモリとDVDが制御対象とのことだが、一律に利用を禁止するのではなく、業務の実態に合わせてきめ細かく設定しているという。

例えばUSBメモリの場合、開発室の共有PCから必要なデータを取り出し、自分のPCへデータを移して作業するといったケースが多い。そこでこうした特定の用途に合わせ、許可したUSBメモリだけを使用できるようにしている。また、作業に必要なツールをPCへインストールする際、DVDを利用するケースがあるが、そうした際は読込のみを許可し、書込できないよう設定もできる。

そのほかの利用についても、現地からの求めに応じて森田氏が許可を出すしくみをとっているが、これにより、本社側で各開発室の状況を確実に把握できるようになったことは大きなメリットだという。

「当社のお客様の1/3が上場企業ですが、こうした会社はセキュリティポリシーもきちりしており、高いレベルのセキュリティ対策を求めています。お客様に対し、DeviceLockを活用した当社のセキュリティ対策を説明すると、安心・信頼できるという声をいただきます」(淡路氏)

全ての環境へDeviceLockの導入を目指す 制御対象の拡張も検討

今のところアールテクノでは、特に重要な端末に対し優先的にDeviceLockを導入しているが、今後は他の環境に対しても積極的にDeviceLockの採用を検討していきたいとしている。

「これからはDeviceLockも当社のサービスの標準装備になっていくことでしょう。また、オプション機能の活用も検討していきたいと考えています」と淡路氏は抱負を語る。

DeviceLockには外部デバイス制御を中心とする機能に加え、ネットワーク通信による情報漏えいを防ぐためにWindowsのさまざまな通信プロトコル(インターネット、クラウドストレージ、メール、SNS、IM、その他)の制御/証跡の取得をクライアント単位で実現できるNetworkLock(ネットワークロック)というオプションがある。同社ではこうした機能も使えないか検討中だ。

同社にとって、オフショア環境の管理は将来に向けての大きな課題となっている。この点について森田氏は「お客様にとってより良い開発環境をご提供するために役立つ製品があれば、ぜひ導入を検討したいですね」と語ってくれた。

スタンドアロン環境でも、大規模環境でも利用可能なDLPソリューション



DeviceLockは、ユーザーの利用環境に合わせて運用方法を柔軟に変更することが可能です。

例えば1台のPCのみに対策を実施したい場合は、その対象PCのみで完結した運用が可能です。対象PCが複数台ある場合は、管理者による集中管理を行なうことができます。

集中管理を行う際は、DeviceLock管理用ツール(無償)を利用することで、ネットワークに接続されている管理対象のクライアント用エージェント「DeviceLock Service」に対し、ポリシーなどを適応させることができます。

DeviceLock管理用ツールはシステム管理者などのPCにインストールできますので、別途高額のハードウェアを準備して管理サーバーを構築する必要がありません。それゆえ、低コストかつ効率的にセキュリティ対策の一元管理を実現できます。

ライセンス形態・価格、体験版のダウンロードなど詳細はこちら

<http://deviceclock.jp/>



株式会社 ラネクシー
<http://www.runexy.co.jp>

〒101-0003 東京都千代田区一ツ橋2-5-5 岩波書店一ツ橋ビル11F
TEL:03-6261-4711 E-Mail:d_sales@runexy.co.jp

お問合せ