日立ソリューションズ

HITACHI
Inspire the Next

秘文AE AccessPoint Control

導入事例

「秘文AE AccessPoint Control」は販売を終了しました。本機能は「秘文 Device Control」で提供しています。

株式会社アシスト 様

安全なリモートアクセス環境の実現により柔軟なワークスタイルを推進

社員がノートPCやタブレット端末を使って社外でも快適に業務を遂行できるよう、モバイルWi-Fiルーターやスマートフォンのテザリングを使ったリモートアクセス環境を利用しているアシスト。しかしこれらのデバイスや公衆Wi-Fiのアクセスポイントを介したインターネットアクセスには、どうしてもセキュリティ上のリスクが付き物です。そこで同社は、日立ソリューションズの「秘文AE AccessPoint Control」を導入。公衆Wi-Fiやテザリングを介したネットワーク接続を完全に制御することで、安全なリモートアクセス環境を実現し、リモートワークや在宅勤務による柔軟なワークスタイルを強力に推し進めています。

アシスト

株式会社アシスト

本社所在地	東京都千代田区九段北4-2-1 市ヶ谷東急ビル
事業内容	コンピュータ用パッケージ・ソフトウェアの販売、 技術サポート、教育およびコンサルティング
設立	1972年3月
URL	http://www.ashisuto.co.jp/

課題と選定

モバイルWi-Fiルーターや公衆Wi-Fiを通じた「直接インターネットアクセス」をいかに遮断するか?

株式会社アシスト（以下、アシスト）は、国内外のさまざまなIT製品・サービスの販売やサポートを総合的に手掛けるIT企業。Oracle Databaseのサポートや教育において国内屈指の実績を持つことで知られるほか、システム運用管理製品やセキュリティ製品、データ活用ツールなどの販売やサポートでも広く知られています。同社は「People Assisting People」というスローガンの下、人と人とのつながりを大切にしながら、単なるソフトウェア販売ビジネスの枠を超えて、顧客と社員の豊かさを追求することを社是としています。事実、同社は全国に拠点を構え、各地の顧客と密接な関係を築きながら質の高いITサービスを提供しています。

このようなサービスを展開する同社の社員は、顧客先に直接足を運ぶ機会が多く、自ずと社外で業務を行う時間が長くなります。そのため以前より、ノートPCのUSBポートに挿すタイプのデータカードを使って閉域通信網に接続し、社外から社内ネットワークにリモートアクセスできる環境を整えてきました。しかし数年前より、こうしたリモートアクセス環境の運用に限界が生じてきたといいます。アシスト サービス事業部 情報システム部 部長 石田昌光氏は、その背景を次のように説明します。

「ノートPCだけでなく、タブレット端末からも社内システムにアクセスしたいというニーズが多く寄せられるようになりました。タブレット端末はUSBポートを持たない代わりに、Wi-Fi機能を内蔵しています。そのため、従来のUSB接続型のデータカードを、モバイルWi-Fiルーターに切り替えることになりました」

株式会社アシスト
サービス事業部　情報システム部
部長　石田　昌光 氏

しかしこのことが、新たなセキュリティ上の懸念を呼び込むことになりました。それまでの閉域網接続とは異なり、モバイルWi-Fiルーターを利用するとユーザーが直接インターネットに接続できるようになるため、マルウェア感染をはじめとするセキュリティ上のリスクにさらされる危険性が高くなります。また、スマートフォンのテザリング機能を使ったインターネット接続が可能になったことも、同様のリスクを高める結果となりました。

もちろん、「ユーザーは直接インターネットに接続してはならず、必ずSSL-VPNを通じて社内ネットワークに接続するように」との社内ルールを設けてはいたものの、このルールが100%守られるという保証はありません。データカードの機種によっては、カード側の設定で「SSL-VPNのゲートウェイにしか接続できない」との制限をかけることも可能でしたが、すべての機種がこうした機能を備えているわけではありません。

加えて、公衆Wi-Fiのアクセスポイントを介したインターネットアクセスに対する懸念もありました。

「弊社では2年ほど前からWi-Fi機能を内蔵したクライアントPCを導入し、それに合わせて社内ネットワーク環境もすべて無線化しました。この社内ネットワークに関しては、アクセスポイントに接続できる端末を厳格に制限するなどしてセキュリティを担保していますが、一方で社外の公衆Wi-Fiへのアクセスを制御する術は持ち合わせていませんでした。そのため、公衆Wi-Fiを通じて直接インターネットに接続されることで、既に社内のゲートウェイで実施しているウイルス対策や、URLフィルタリング、アクセスログ取得等の対策がスルーされ、マルウェア感染や情報漏えいが発生する恐れがありました」（石田氏）

こうした課題をクリアするためには、社外からのアクセス時には強制的に必ずSSL-VPNのゲートウェイにつなぎ、社内ネットワークにログインさせる仕組みがどうしても必要でした。そこで同社が導入を検討したのが「秘文AE AccessPoint Control」（以下、秘文AE APC）でした。 実はアシストでは「秘文AE APC」の販売を手掛けており、その経験から同製品の機能や品質に高い信頼を置いていました。

「秘文AE APC」は、PCにインストールして利用するソフトウェア製品。あらかじめネットワーク接続ポリシーを設定しておけば、同製品を導入したPCをネットワークに接続した際には、必ずそのポリシーに則った接続しか行えないよう制御できます。例えば「許可した接続先しか利用させない」「VPN接続以外の通信を遮断する」といった具合です。まさに、アシストが抱えていた課題を解決するためにぴったりの製品だったのです。

「社内で『秘文AE APC』を取り扱っている部署の人間から紹介を受け、その機能について説明してもらったのですが、まさにこれこそ私たちが求めていたソリューションだと直感しました。また、社内に『秘文AE APC』のスキルを持つ人間が多くいたことも、決め手の1つになりました」（石田氏）

導入

初期導入も運用も極めて簡単に行うことができる「秘文AE APC」

早速同社は、検証に取り掛かりました。まずは情報システム部のメンバー、社内で「秘文AE APC」を取り扱っているチームのメンバー、それに普段からリモートアクセス環境を通じて在宅勤務を行っている社員のPCに導入しました。この導入作業に直接当たった、同社サービス事業部 情報システム部 濱野恭行氏によれば、その作業は驚くほど簡単だったといいます。

「初期導入時は、インストール作業を各ユーザーにお願いしたのですが、インストーラを起動して数回ボタンをクリックするだけのわずか数分で作業が完了します。ユーザーに余分な手間を掛けさせない上、やろうと思えばサイレントインストールも可能になっていますから、極めて簡単に導入できるツールだと思います」

株式会社アシスト
サービス事業部　情報システム部
濱野　恭行 氏

また同氏が導入作業以上に高く評価するのが、その運用の簡単さです。特に設定変更が極めて容易に行える点は、運用する側にとって非常にありがたいと述べます。

「接続先など頻繁に変更される項目については、その一覧を記したCSVファイルをサーバ上で一元管理しておけば、それを自動的に読み込ませることができるため、最小限の手間で設定内容を更新できます。また、接続を許可するIPアドレスや、社内外を識別する際の判断基準など、その他の設定変更が発生した場合でも、設定をあらかじめ埋め込んだインストーラを作成することが可能なので、ユーザー側では『秘文AE APC』のアンインストールは不要で、単にもう一度インストールと同様の手順を踏んでもらうだけで設定変更が完了します」

それまでは、接続先の変更などを行う際には、データカードをユーザーから回収して、メーカーから取り寄せたツールを使って1枚1枚設定を書き換えていました。これに比べれば、リモートアクセスの設定変更の手間は劇的に削減されたといいます。こうして、「秘文AE APC」の導入と運用の初期検証を終えたアシストは、同製品の本格導入を決定。現在では適用範囲を広げ、さらに多くのユーザーが日々活用しています。

成果と今後

セキュアなリモートアクセス環境がもたらすワークスタイル変革を全社レベルまで拡大

アシストでは「秘文AE　APC」を導入した結果、その本来の導入目的である「接続先の制御」を極めて高いレベルで達成できたといいます。社外からモバイルWi-Fiルーターやスマートフォンのテザリングを使って、あるいは公衆Wi-Fiを使ってネットワークに接続する際には、SSL-VPNのゲートウェイ以外には接続できないよう「秘文AE APC」で制御をかけられるようになりました。

しかも、こうした新たな施策を導入したにもかかわらず、ユーザーには余分な負担を一切強いることがない点も「秘文AE　APC」の特徴の1つと石田氏は語ります。

「従来よりセキュリティポリシーをきちんと順守し、社外からは必ずSSL-VPNを使って接続するというルールを守ってきたユーザーにとっては、これまで使ってきたリモートアクセス環境と何ら変わるところはありません。ただし管理する側にとっては、社外からのアクセスが制御でき、ルールからの逸脱を確実に防げるようになったことには、極めて大きな価値があります」

こうして社外からのリモートアクセスをセキュアに行える環境を整えたことで、モバイルワークや在宅勤務といった新たなワークスタイルが促進され、ひいては社員の生産性向上と、顧客に提供するサービスのさらなる品質向上が期待できるようになったといいます。

既に「秘文AE　APC」を導入して半年が経とうとしていますが、何の問題もなく導入・運用できています。同社では、現在の規模での運用が順調に運べば、近いうちに全社員にまでその適用範囲を拡大していく予定です。その際には、より「秘文AE　APC」の導入や運用を効率化するとともに、現在はまだ利用していない機能も積極的に活用していきたいと濱野氏は抱負を述べます。

「ユーザーの数が増えれば、サイレントインストール機能を使って効率的に導入や設定更新を行うことも検討していきたいと考えています。既に『秘文AE APC』の主だった機能は大いに活用しているのですが、ログ管理などまだ活用し切れていない機能もあるので、それらの利用も検討してみる価値があるでしょう。とにかく導入も運用も極めて簡単な製品なので、今後の利用規模拡大に対する不安は一切ありません。セキュリティレベルの担保と、ユーザー・管理者の利便性を高いレベルで両立させた、稀有な製品だと思います」

※本事例の内容は初版作成時点（2015年5月）の情報です。
※本文中の会社名、商品名は、各社の商標、または登録商標です。 ※本文中および図中では、TM、®マークは表記しておりません。
※本文中の製品の仕様は、改良のため、予告なく変更する場合がございます。
※本製品を輸出される場合には、外国為替および外国貿易法並びに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。なお、ご不明な場合は、弊社担当営業にお問い合わせください。
※本カタログ中の情報は、カタログ作成時点のものです。

こちらのQRコードより、本事例の詳細ページをご覧いただけます。
http://www.hitachi-solutions.co.jp/hibun/case09/

商品・サービスに関するお問い合わせ・ご相談受付

【電話による受付】
0120-421-126［通話料無料］
受付時間 10:00～17:30　月曜日～金曜日（祝日、弊社休業日を除く）

【メールによる受付】
webmaster@hitachi-solutions.com

※ご相談、ご依頼いただいた内容は、回答などのため、弊社のグループ会社に情報を提供し対応させていただくことがあります。取り扱いには十分注意し、お客さまの許可なく他の目的に使用することはありません。

本カタログ掲載商品・サービスの詳細情報
http://www.hitachi-solutions.co.jp/hibun/

このカタログは資源保護のため、再生紙を使用しています。

H27K-13-01	2017.07

株式会社 日立ソリューションズ
http://www.hitachi-solutions.co.jp/