

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。

株式会社パナグループ 様

約3,000台のPCを
安全な無線LAN環境に接続

社員のフレキシブルな働き方に応えるため、本社ビル内に無線LAN環境を導入したパナグループ。社内システムにアクセスするPCからの情報漏洩を防ぐため、無線LANにも有線LAN環境と同等のセキュリティの高さを求めていました。この要件を満たすソリューションが「秘文AE AccessPoint Control」(以下、秘文AE APC)でした。クライアントPC側で自動的に適正なアクセスポイントに接続できる利便性の高いビジネス環境を構築しました。



株式会社パナグループ

本社所在地 東京都千代田区大手町2-6-4
事業内容 エキスパートサービス(人材派遣)、
インソーシング(委託・請負)、
HRコンサルティング・教育・研修など
設立 1976年2月16日
U R L <http://www.pasonagroup.co.jp/>

課題と選定

全社のセキュリティポリシーを無線LANにも統一して適用する

雇用の創出を通じて、人々の心豊かな生活の創造や社会の課題解決をめざすパナグループ。人材派遣、委託・請負、コンサルティング、人材紹介、海外人材サービス、再就職支援、アウトソーシングといったソリューションを柱にビジネスを多角的に展開しています。近年は、新規就農者の支援や、地域活性化を担う若者の人材育成、多様な職場での障がい者の雇用促進にも力を入れています。多彩な人材と職場のマッチングを行うために、国内外のグループ会社は約60社を数えます。

このパナグループの本社機能が集まる東京・大手町のパナグループ本部では、2014年11月、オフィス内に無線LAN環境を導入しました。

「無線LANには、ハブやLANケーブルを床下や壁面にいくつも敷設せず、アクセスポイントの増設だけで同時接続する利用者を柔軟に追加できたり、ケーブルの取り回しも要らなくなったりと利用者・管理者双方にメリットがあります」と、パナグループ 情報システム部ITインフラグループ マネージャーの中安裕二氏は説明します。

とはいえ、自由な無線LAN接続を許せば、情報システム部の目が届かない「シャドーPC」が社内システムのセキュリティを脅かす恐れがありました。例えば、情報システム部が把握していない社員私有のPCやスマホ、タブレットが仮に、マルウェア(コンピューターウイルス)に感染している場合、それらが踏み台となって第三者に機密性の高い情報が、社内の無線LANアクセスポイント経由で持ち去られてしまう可能性があります。また、シャドーPCがマルウェアの感染源となって社内LANを混乱に落とし入れ、業務に支障を来すリスクが危惧されました。

社員が利用できる端末を、社内で貸与するPCに限定したとしても、まだセキュリティ上の懸念はあります。例えば、建物周辺に飛び交う、不特定多数の人が利用するアクセスポイントに、貸与したPCが知らない間に自動接続し、マルウェアに感染してしまうケースもあります。不特定多数が利用するアクセスポイントには、セキュリティ対策が脆弱なものが含まれるため、接続を許さない仕組みが必要でした。

「しかし、無線LANを利用する社員に『公衆無線LANや社内で管理されていないアクセスポイントに接続しないようにしてください』と言っても、コンピューターやセキュリティの知識には個人差があり、対策として万全とはいえません。そのため、情報システム部側でセキュリティを確保できる仕組みをつくることで安全性を担保する必要がありました」と同部ITインフラグループグループ長の椎名司氏は述べます。

同社は、統一した情報セキュリティポリシーを全社のLAN環境に適用しています。無線LAN環境の構築についても、有線LAN並みの堅牢なセキュリティを確保した上で、社内システムへアクセスできることが求められました。

「展示会などで情報収集する中で知ったのが、『秘文AE APC』でした。特徴を知り、これでやりたかったことが実現できるとピンと来ました」(中安氏)



株式会社パナグループ
グループ長
情報システム部
ITインフラグループ
椎名 司氏

導入

クライアントソフトを一斉に配布 許可されたアクセスポイントのみ接続

「秘文AE APC」は、社内で管理されたPCを用いて、許可された利用者が適切に安全なアクセスポイントに接続できる環境を提供できる製品です。利用者だけでなく管理者側にも大きな負荷をかけることなく運用できることも特徴です。

同社が製品選定で着目した大きな特徴が「Wi-Fi制御」機能です。秘文AE APCクライアントをインストールしたPCには管理者が許可したアクセスポイントにしか接続できません。そのため、利用者は意識しなくても、不正なアクセスポイントに接続するリスクを排除することができます。

「今回の無線LAN導入は、社内システムに接続する重要なネットワーク回線の構築という位置づけでした。そこで、社内の利用者の反応を確かめながら、段階的に導入しました」と中安氏は説明します。

2014年6月、PCを貸与している内勤者のうち、無線LAN利用に関心の高い200人の利用者を選び、貸与するPCに秘文AE APCクライアントをインストールしました。

「当初は、Active Directoryのグループポリシーを利用することも考えていたのですが、要求仕様を満たすにはかなり複雑な仕組みをつくる必要があり、実現が難しいということで今回は見送りました。『秘文AE APC』はサーバーからクライアントPCにソフトを配布するだけですので、非常に短時間で対応を完了することができました」(中安氏)

約1カ月間の試行を経た結果、モニターとなった利用者からの反応は上々。業務に支障なく無線LANを順調に活用できたことが分かりました。これを受けて、2014年11月にグループ本部のアクセスポイントを利用する約3,000台のPCすべてに秘文AE APCクライアントを導入。さらに大阪のオフィスにおいても、同様の無線LAN環境を構築し、運用を開始しています。

成果と今後

VPN利用の強制により柔軟なワークスタイルの実現へ

「ヘルプデスクへの問い合わせ数も少なく、大きな混乱はありません。利用者も安心して利用しているようです」と椎名氏は述べます。社員にも業務プロセスの変更や遵守するルールの追加などを強わずに済みました。通信もストレスなく行われています。

管理者側のメリットも小さくありません。実は、オフィス内で有線LANのみを利用していた以前は、管理部門に社員からしばしば「会議室のハブにPCをつないだが、有線LANを使ってネットワークに接続できない」といった問い合わせが寄せられていました。

原因を調べてみると、有線LANをループ状に接続していた、など初歩的なミスによるものがほとんどでした。ただ、問題を解決するためにエレベータで階

を移動したり、ケーブルの断線がないか、念のためフロアを点検したりするなど対応に時間を割く場面が多々ありました。

無線LAN利用が増えた結果、負担が軽減され、その分、管理者側はシステム部門としてより付加価値の高い企画業務などに集中しやすくなっています。

現在、同社では、「秘文AE APC」の特徴的な機能に注目しています。それは、「VPN利用の強制」機能です。社内のシステム環境は現在、社屋の無線LANアクセスポイントを介して、建物の中にいる社員のみが利用できる状態です。「VPN利用強制を使えば、社外から社内システムへの安全なリモートアクセスを実現することができます」(中安氏)。

これが実現すると、例えば、自宅に設置した固定型のWi-Fiルーターや、携行可能なスマートフォンを用いたテザリング経由での社内システムへのリモートアクセスが可能になり、現場からの直行直帰といったワークスタイルの柔軟性が高まります。

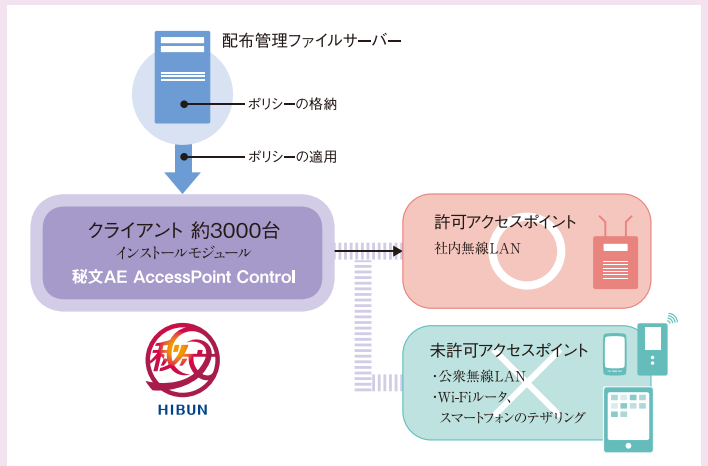
椎名氏は「日本企業ならではのセキュリティの高さと、運用上の使いやすさなどの要求にきめ細かく対応されているツールだと評価しています。日立ソリューションズには、私たちユーザーの声を取り入れて、より良い製品開発に反映してほしいですね」と述べます。中安氏も「企業文化に優しいものを提供し続けてください」と、日立ソリューションズへの期待を語ります。

多様な生き方や価値観を尊重しながらそれぞれの特徴を活かしてビジネスを展開するパナグループ。その柔軟なワークスタイルを「秘文AE APC」が安全に見守っています。

株式会社パナグループ
マネージャー
情報システム部
ITインフラグループ
中安 裕二氏



システム概要



※本事例の内容は初版作成時点(2015年3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、®マークは表記していません。
※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。

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きます。取り扱いは十分注意し、お客様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。

H26S-22-01 | 2017.07

こちらのQRコードより、本事例の詳細ページをご覧ください。

<http://www.hitachi-solutions.co.jp/hibun/case08/>



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