Ashisuto × Security

導入事例 Case Study

秘文、JP1/IT Desktop Management 2

アシスト
「お客様の最高」のために

b-en-g

東洋ビジネスエンジニアリング株式会社

国内第1号SAPユーザへの導入支援を行う等、製造業向けERPシステム導入のパイオニアとして培ってきたノウハウを生かし、基幹業務パッケージ「MCFrame」、グローバル経営管理ソリューション「A.S.I.A.」や、ビジネスコラボレーションのためのクラウドサービス「Business b-ridge」等、お客様の変革をサポートするITソリューションを多数提供。

本　　社：東京都千代田区大手町1-8-1 KDDI大手町ビル
事業開始：1999年4月1日
資 本 金：6億9,760万円
従業員数：連結:540名 単体:417名（2016年3月31日現在）
U　R　L：http://www.to-be.co.jp/

（取材日：2016年10月）

モバイルPCの利便性と安全性を両立 重要情報とユーザを守るための セキュリティ対策強化

製造業向けSIサービスやERPパッケージ開発／提供を広く手掛ける東洋ビジネスエンジニアリング株式会社では、社外業務を行う社員がモバイルWi-Fiやテザリングを利用してPCをインターネットに直接接続することによる、マルウェア感染や情報漏洩のリスクが懸念されていました。そこで同社は、社内同様安全にモバイルPCを使用するため、社外でのネットワーク接続時にVPN利用を強制する機能を持つ「秘文」と、IT資産管理製品である「JP1/IT Desktop Management 2」を導入し、セキュリティ対策の強化を実現しました。

POINT

1 社外でのネットワーク接続時、必ず社内ネットワークを経由するよう設定し、セキュリティレベルを確保

2 IT資産管理の徹底により、無許可ソフトウェアの導入やパッチ適用状況の可視化を実現

3 導入時だけではなく、最新情報の提供や細やかなサポート等アフターフォローにも期待

課　題

- シンクライアント化も検討に挙がったが、ネットワーク環境の面等で断念。端末にデータを保存する前提でのセキュリティ対策を模索していた
- モバイルWi-Fiやテザリングを利用してインターネットに直接接続することで生じるマルウェア感染や情報漏洩のリスクを回避する必要があった
- クライアント端末の詳細なセキュリティ情報の把握、内部不正を抑止するデバイス制御とログ取得が必要と考えていた

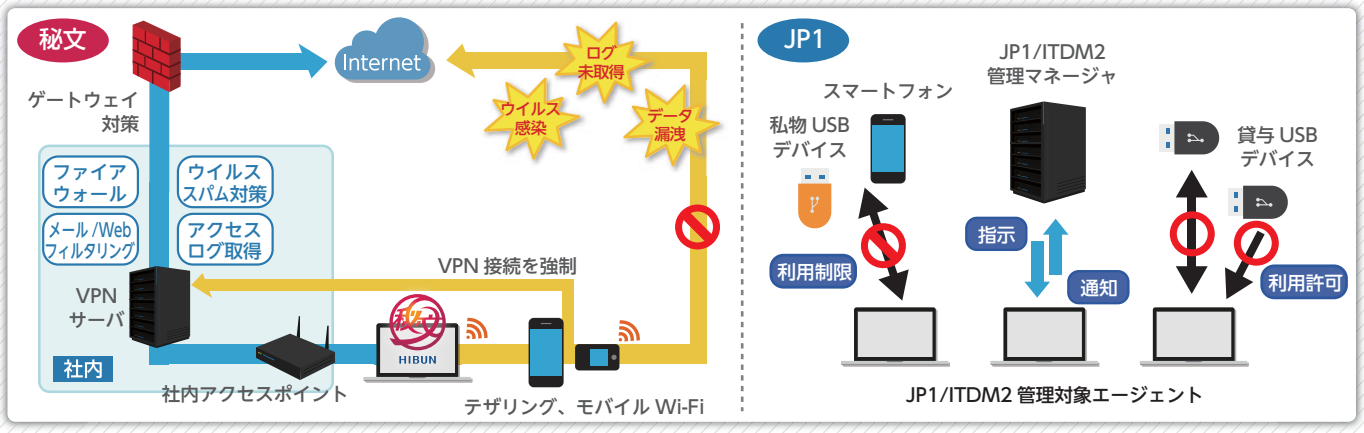
対　策

- 「秘文」により、モバイルWi-Fi等を経由した社外でのネットワーク接続時にはVPN利用を強制。合わせて接続先確認機能により、偽アクセスポイントへの接続を防止
- 「JP1/IT Desktop Management 2」により、クライアントPCへの導入ソフトウェアやセキュリティパッチ適用等、端末の利用実態を可視化。外部デバイスの利用制限や、操作ログ取得も合わせて実現

効　果

- VPN接続強制機能および接続先確認機能により、ユーザの利便性を損なわずに、社内ネットワーク利用時と同等のセキュリティレベルを常に確保
- 各クライアント端末の詳細状況を把握し、マルウェア対策を後押し
- 外部デバイスの利用制限やクライアントPCのログモニタリングにより、内部不正による情報漏洩リスクを軽減

システム概要



秘文、JP1/IT Desktop Management 2

社外持ち出し用モバイルPCにまつわるセキュリティリスク

製造業を中心にERPのSIサービスや自社パッケージ製品の開発／提供、近年ではクラウドサービスやIoTソリューションの提供等、幅広いITサービスを提供する東洋ビジネスエンジニアリング株式会社（以下、B-EN-G）。「MCFrame」「A.S.I.A.」といった製造業向け業務パッケージ製品で広く知られていますが、もともとは外資系ERPパッケージ製品を核に据えたSIビジネスを柱としており、現在でも同社のエンジニアの多くは顧客先に常駐しながら構築作業に従事しています。

そのため、同社の従業員が利用するクライアント端末のほとんどは携帯可能なモバイルPCを採用しており、それを社外の作業場所に持ち出した際に、モバイルWi-Fiやスマートフォンを利用してインターネットに接続していました。こうした利用形態は、同社の社内ネットワークに施したセキュリティ対策を経由することなく直接インターネットにアクセスできてしまうため、かねてからマルウェア感染や情報漏洩等のリスクが懸念されてきました。当時の状況を、経営企画本部　情報システム部　部長佐藤雅彦氏は次のように振り返ります。

佐藤氏　社外に持ち出した端末からの情報漏洩のリスクを排除するには、シンクライアントが最も有効だと思われましたが、社外の作業場所は必ずしもネットワーク品質が安定しているとは限りません。そのため、シンクライアントの導入は時期尚早と判断し、既存のモバイルPCをよりセキュアに利用できる方法を模索することにしました。

要件にピタリとフィット「アシスト」+「秘文」+「JP1/ITDM2」

社外で使われるモバイルPCのセキュリティレベルを全体的に底上げするには、複数の対策を同時に導入する必要があると同社は考えていました。中でも重視したのが「外部デバイス制御の強化」「ソフトウェア脆弱性対策の強化」「ファイル操作ログの取得」、そして「VPN接続の強制」でした。

これらの対策を実現するには、まずはIT資産管理ツールを導入してソフトウェアの資産管理を厳密化し、セキュリティ上問題のあるソフトウェアの有無や、セキュリティパッチの適用状況等を監視できる体制を整える必要がありました。またUSBメモリやスマートフォン等、外部デバイスの接続を制御したり、クライアント端末上でファイル操作ログを取得する上でも、IT資産管理ツールが威力を発揮します。

一方、モバイルPCからモバイルWi-Fiやテザリング等を利用してインターネットに接続する際、必ず社内ネットワークを経由するよう強制できれば、社内のセキュリティ対策が適用されます。そのようなことを実現できる製品が存在することを、当初、佐藤氏は認識していなかったと言います。

佐藤氏　アシストさんから紹介いただいた「秘文」を使えば、社員が不正な無線アクセスポイントへの接続を防止できる他、モバイルWi-Fi等を利用してインターネットにアクセスする時にVPN接続を強制できると知り、弊社が抱えていた課題の多くを解決できると直感しました。また、セキュリティ製品は「一度入れたら終わり」ではなく、導入後の運用こそが大事ですから、アフターフォローに期待できるベンダーさんから導入したいと考えていました。アシストさんと秘文の組み合わせは、こうした弊社の要件にぴったりだったのです。

同じ理由からIT資産管理ツールも、アシストが高いサポート実績を持つ「JP1/IT Desktop Management 2（JP1/ITDM2）」を採用することに決め、秘文と合わせて2015年秋よりアシストの技術支援の下、順次導入作業を進めていきました。

業務影響を極小化しつつセキュリティレベルを大幅向上

現在、B-EN-Gの社員が社外に持ち出して利用するモバイルPCには、原則として秘文が導入され、社外でネットワーク接続する際には、必ずVPNを経由するよう設定されています。かつて直接インターネットにアクセスできていた頃と比べ、VPNにログオンする操作が新たに加わりましたが、ユーザからは特に不満が出ることなく、順調に運用が回っていると言います。その理由として佐藤氏は、「焦らず丁寧に導入を進めたこと」を挙げています。

佐藤氏　VPN接続が強制されることで顧客先のプリンタやサーバが見えなくなる等、既存業務に影響が出る場合もあります。またどうしても業務の都合上、VPN接続強制を外さざるを得ないケースもあります。こうした個々の事情をきちんと理解し、少しずつ現場のニーズに即した設定を行っていくことで、現場からの理解を得ながらスムーズに運用を根付かせることができました。また、これらの対策は「意図しない情報漏洩から、ユーザを守るための策である」ということも重ねて説明してきました。

佐藤雅彦氏

こうして同社では、モバイルPCからインターネットに直接アクセスすることによるセキュリティリスクを大幅に低減したとともに、秘文の「アクセスポイント制限機能」を活用することで、社内の無線LAN利用時の偽アクセスポイント対策も実現しました。

同時にJP1/ITDM2を導入したことで、不正ソフトウェアのダウンロードや脆弱性パッチの適用漏れ、ユーザによる不正操作等のリスクの芽を、IT資産管理とファイル操作ログ取得の機能で排除できるようになりました。

今後はグループ全社へと適用範囲を拡大

B-EN-Gでは、今回導入した秘文とJP1/ITDM2によるエンドポイント・セキュリティの取り組みを、同社のみならず海外拠点やグループ会社も含めたグループ全社に広げていく予定です。それと同時に、秘文およびJP1/ITDM2が備える豊富な機能をさらに使いこなし、その導入効果をより一層高めていきたいとしています。

こうした取り組みを進めていく上でも、また同社のセキュリティ対策全般をより強化していく上でも、今後ともアシストの支援には大いに期待していると佐藤氏は言います。

佐藤氏　サイバー攻撃を仕掛ける側は組織化・分業化が進み、その攻撃手法は高度化する一方です。これに対抗するには、ユーザ企業側も互いに手を携えて、密接に協力し合う必要があります。弊社でもCSIRTを組織して外部との連携体制を強化していますが、アシストさんもベンダーの立場から是非ユーザ間の情報共有の機会を設けていただけるとありがたいですね。

お問い合わせは　株式会社アシスト　https://www.ashisuto.co.jp/prod/hibun/　https://www.ashisuto.co.jp/prod/jp1/　E-Mail ssj_info@ashisuto.co.jp

東　京　〒102-8109　東京都千代田区九段北4-2-1 市ヶ谷東急ビル　TEL: 03-5276-5862
札　幌　〒060-0003　札幌市中央区北3条西4-1-1 日本生命札幌ビル 13F　TEL: 011-281-1161
仙　台　〒980-0013　仙台市青葉区花京院1-1-20 花京院スクエア 19F　TEL: 050-3816-0970
名古屋　〒460-0003　名古屋市中区錦1-11-11 名古屋インターシティ 4F　TEL: 052-232-8211
金　沢　〒920-0853　金沢市本町2-15-1 ポルテ金沢 8F　TEL: 050-3816-0972
大　阪　〒530-0011　大阪市北区大深町4-20 グランフロント大阪タワーA 13F　TEL: 06-6373-7113
広　島　〒730-0011　広島市中区基町12-3 COI広島紙屋町ビル 3F　TEL: 050-3816-0974
福　岡　〒812-0013　福岡市博多区博多駅東2-6-1 九勧筑紫通ビル 9F　TEL: 092-481-7156
沖　縄　〒900-0014　那覇市松尾1-10-24 ホークシティ那覇ビル4F　TEL: 050-3816-0976