THE NEW VALUE FRONTIER
KYOCERA

自社導入事例　エンジニアリング部門

「つい、うっかり」では許されない
メール誤送信や端末紛失による情報漏えいなどのリスクを回避

ビジネスで利用されるスマートデバイスは、いつでも、どこでもメールなどにより情報共有ができる利便性の高いツールである。その一方、メールの宛先を間違えて送信したり、端末を紛失すれば情報漏えいの事故になりかねないというリスクもある。
こうしたリスクを回避し、スマートデバイスを安全に利用できるのが、京セラコミュニケーションシステム株式会社（KCCS）のリモートアクセスサービス「BizWalkers+ Mobile」だ。現場作業者との業務連絡の手段としてスマホを利用する、KCCSエンジニアリング部門とパートナー会社のBizWalkers+ Mobileによるセキュリティ対策事例を紹介する。

（左から）
京セラコミュニケーションシステム株式会社 技術統括部 ISO推進部 部長 坂本 昭博
同社 インテグレーション部 セキュリティサービス課 片寄 友貴

背景・課題

- 約300社のパートナー会社との業務報告メールは1日数百件
- KCCSとパートナー会社のセキュリティレベルがバラバラ
- メール誤送信や紛失・盗難時の情報漏えいのリスクあり

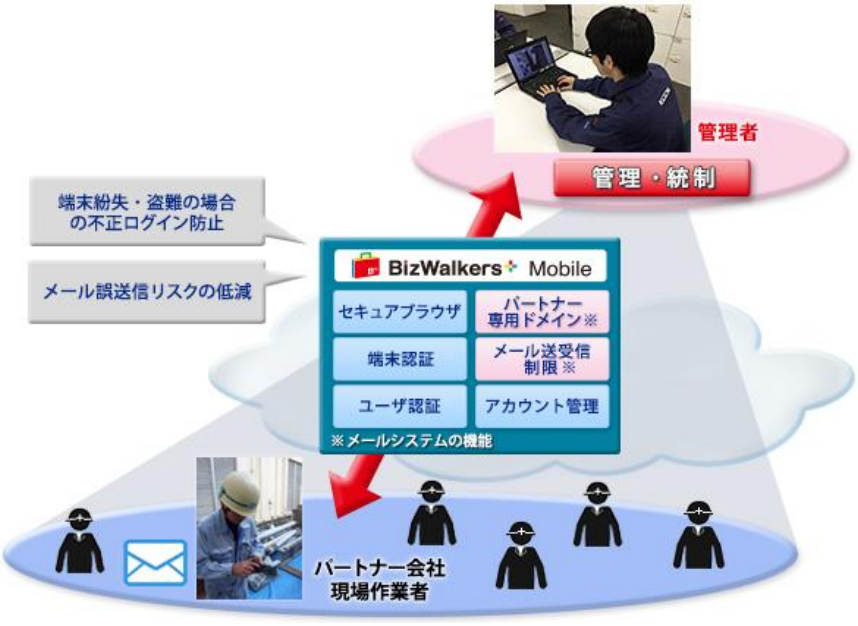
選定のポイント

- 端末上にデータを残さない**セキュアブラウザ機能**
- 端末認証とユーザ認証で**セキュアなリモートアクセス**
- 利用者負担が少なく簡単導入

導入効果

- メール誤送信や端末紛失など**情報漏えいリスクを低減**
- KCCSとパートナー会社間の**メールセキュリティを一元管理**
- 将来的にタブレット端末での図面やマニュアル閲覧で**作業効率の向上**

サービスイメージ図



背景・課題　業務報告メールは1日数百件、メール誤送信リスクの低減が急務

エンジニアリング部門では、スマートデバイスの普及で通信トラフィックが急増する中、通信キャリアが全国に展開する無線基地局の設計・施工や運用・保守を担い、その現場作業をパートナー会社とともに行っている。約300社におよぶパートナー会社が全国各地の無線基地局で日々作業しており、「エンジニアリング部門と現場作業者との間でやり取りされるメールは1日に数百件におよび、これまでさまざまな懸念を抱えていました」とISO推進部の坂本 昭博は語る。

例えば無線基地局の点検保守の場合、パートナー会社の現場作業者がメールでエンジニアリング部門に作業開始の連絡を入れ、エンジニアリング部門が現場作業者へ作業指示や各種連絡事項をメールで連絡。現場から作業状況の報告や終了連絡を受け取っている。

このようなやり取りの中で課題として挙げられるのは、メール誤送信のリスクだ。「これまでは業務で利用するメールアドレスの設定について、エンジニアリング部門として統一したルールがありませんでした。そのため、間違えやすいメールアドレスの使用抑止や、パートナー会社のメールアドレスであることの確認ができていないという課題がありました。加えて、パートナー会社の現場作業者がどんな端末を使っているのかも把握・管理できていない状態でした」と坂本は説明する。

選定のポイント　メール誤送信や不正利用を防ぐ「BizWalkers+ Mobile」を活用

メール誤送信や端末の紛失・盗難にかかわるリスクを低減し、パートナー会社の現場作業者と安全にメールをやり取りする仕組みを検討してきた。そこで着目したのが、KCCSのリモートアクセスサービス「BizWalkers+ Mobile」である。

すでにKCCS社内では同サービスのセキュアブラウザや端末認証の機能を使用し、会社が認めたスマホやタブレットから、端末にデータを残さずメールやグループウェアを利用していた。これを拡張し、以下の要件を実現できないかと考えたのである。

(1)通信キャリアのメールアドレスおよびフリーメールアドレスの使用を禁止すること
(2)利用する端末を限定し、特定のドメイン間でのみメールの送受信ができること
(3)エンジニアリング部門とパートナー会社の情報伝達が相互にできること
(4)人に頼らずヒューマンエラーを防止できること
(5)短期間での導入が可能なこと
(6)将来的な業務改善が可能なこと

「BizWalkers+ Mobileはビジネスで使用するさまざまなシステムに、モバイルからセキュアに利用できる機能を提供するサービスです。メールシステムの持つ配信制限機能と、BizWalkers+ Mobileのセキュアブラウザ・端末認証の機能を組み合わせることで、エンジニアリング部門の要件にマッチすると考えました」と、導入を支援したセキュリティサービス課の片寄 友貴は語る。

そして、メール誤送信や紛失・盗難などのリスクを低減すべく、『メールシステム』と『BizWalkers+ Mobile』で以下の改善を行った。

■メールシステムでの改善点
- **エンジニアリング部門が管理するドメインとしてパートナー会社専用のメールアドレスを用意**
- **あらかじめ管理者が許可したドメイン間でのみメールの送受信ができるように設定**

■BizWalkers+ Mobileでの改善点
- **パートナー会社のアカウントはBizWalkers+ Mobileからのみ利用できるように設定**
- **端末認証を利用し、許可された端末のみ利用できるように限定**
- **アカウントの登録や停止がリアルタイムに対応できるようになり、万一の場合でも、すぐにアカウントの停止や端末に紐付く固有識別子の無効化が可能**
- **端末にデータが残らないようにセキュアブラウザを利用**

こうした改善を行うことで、メール誤送信のリスク低減および、端末の紛失・盗難の場合でも不正利用を防ぐことができるようになった。「外出中や夜間はスマホからBizWalkers+ Mobileにログインして現場からのメールを確認したり、現場作業者へ指示を出しています。無線基地局は24時間・365日の保守体制をとっており、緊急時のメール連絡も安全に行えるようになりました」と坂本は説明する。

導入効果・展望　管理者の負担なく、業務部門が容易に端末の登録・管理を実施

BizWalkers+ Mobileの特長は、ITに熟知した情報システム部門でなくても、業務部門でユーザ・端末の管理を行える直感的なインターフェイスを用意していることだ。エンジニアリング部門は、あらかじめパートナー会社から業務連絡に使用するスマホの申請を受け、電話番号などを登録するだけで、アプリのインストールはパートナー会社に任せている。約300ユーザを登録しているが、パートナー会社からはインストールに関する問い合わせもなく、簡単に導入できたという。

「システム管理者や利用者に大きな負担をかけることなく、端末の登録・管理が行えるので、専任のIT部門がない中小規模の企業でも早期導入が可能です」と片寄は説明する。

導入効果はどうだろうか。エンジニアリング部門やパートナー会社では従来から現場作業者に対してメール送受信時のセキュリティについて注意を喚起してきたが、「導入後、現場作業者は必要以上にセキュリティを意識することなくメールをやり取りできるようになったため、安心感があるとともに報告や連絡の作業効率が上がったとの声が届いています」と坂本は手ごたえを話す。

現在はスマホでのメール利用だが、今後はタブレット端末などを活用して作業に必要な図面やマニュアルなどの配布・閲覧に利用する構想もあるという。「紙で配布している図面や作業のマニュアルを電子化し、セキュアブラウザで端末にデータを残さず配布・閲覧できるようにすることで、紙の紛失のリスクを回避できます。今後も、パートナー会社の作業効率やセキュリティを高めるための取り組みを続けていきます」と坂本は展望する。

KCCSでは今後も業種や規模問わず、セキュアなリモートアクセスが必要な企業や、私有端末の業務利用（BYOD）を検討している企業などにBizWalkers+ Mobileでスマートデバイスの業務活用支援をしていく考えだ。

本事例の詳細は ⇒ http://www.kccs.co.jp/case/1504/index.html

KYOCERA

京セラ コミュニケーションシステム株式会社

随時セミナー開催！
詳しくは https://www.kccs.co.jp/events/index.html

KCCSカスタマーサポートセンター
フリーコール 0120-911-901
携帯電話・PHS・IP電話など 050-2018-1827
受付時間 平日9:00～17:00
（17:00以降のお問い合わせは自動応答になります。）
KCCSホームページ http://www.kccs.co.jp/
E-mail：kccs-support@kccs.co.jp

2015-12