

CaseStudy | 導入事例



User Profile

所在地：〒163-0216

東京都新宿区西新宿2-6-1 新宿住友ビル16階

URL：http://www.agrex.co.jp/

1965年に保険証券発行サービスを開始して以来、「プロセスづくり」のプロとして、業務プロセスを最適化するサービス/ソリューションを提供。BPOサービスからシステム開発・運用まで幅広いサービスをワンストップで提供し、お客様の価値創造を支援している。2013年度にベトナムに合併会社を設立、BPO事業のグローバル展開を開始。

事業拡大と競争力強化のために

アグレックスは2012年、それまで社内のコミュニケーションシステムとして活用していた「Lotus Notes」から「Google Apps」へ移行することを決定した。

同社は業務上、アグレックスの社内ネットワークに接続できない環境で作業を行う社員が多い。そのため、社内勤務者のみがNotesを利用できるという制約を取り除き、全社員が同じ情報/システムを公平に使える環境を整える必要があった。また、スマートデバイスの普及を考慮すると、将来性の高いクラウドサービスを活用すべきだという判断もあった。

情報システム部長の蓬萊 啓八氏は、「当社は、競争力強化のために「コスト・品質」「人材」「経営管理」という3つの分野でのイノベーションを推進しています。Google Appsの採用には、運用負担を軽減してコストを削減するだけでなく、情報共有やワークスタイルの変革によってイノベーションをもたらしたいという思いがありました」と述べる。

その上で、蓬萊氏が経営層から強く指示され

「業務利用を許可した社員」「業務利用を許可した端末」
「データが端末に残らない」をコンセプトにBYODを含む
スマートデバイスからGoogle Appsへの安全なアクセスを実現

導入の効果

- 1 ユーザー認証 / 端末認証 / セキュアブラウザによる3要素認証で安全性を確保
- 2 運用面を含む様々な課題をソリトンのトータルソリューションで払拭
- 3 「スキマ時間」を有効活用し、業務効率の向上を実現

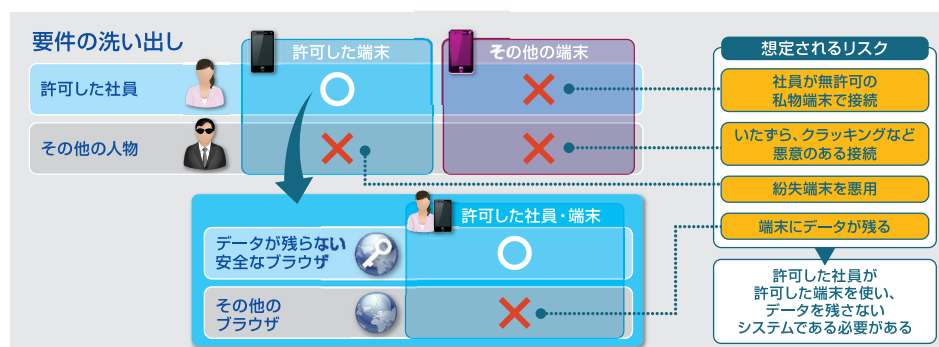
たのがセキュリティ対策だ。蓬萊氏は「細心の注意を払い、最新の技術や考え方を取り入れて、有効活用するようにという指示の下、システム化を進めているところです」と語る。

様々なセキュリティ要件を統合的に実現する手法とは

Google Appsの採用決定に伴い、蓬萊氏はまず、メールやワークフロー、勤怠管理といった対象システムと、社内PC、モバイルPC、スマートデバイスといった端末種別を洗い出した。さらに会社支給やBYODといった端末の

提供形態も追加し、どのデバイスがどのシステムを利用できるべきかを決めていった。

次に確認したのは、セキュリティ対策の現状だ。社内PC・モバイルPC・スマートデバイスにおいて、情報漏洩や成り済まし、盗聴、マルウェアといったリスクに対応できているかどうかを細かくチェックしていったところ、社内PCやモバイルPCでは十分に対策できている一方で、これからスマートデバイスを業務利用していく上では、いくつかの点においては十分ではないことが判明した。蓬萊氏は「当社のBPOサービスをお客様に安心して活用していただくために、従来からありとあらゆるセキュリティ対策を施してきました。スマートデバイス



は、紛失したり盗まれたりするのとは当たり前と捉えるべきです。しっかりと対策が出来ていなければ、社員に使わせるわけにはいきません」と述べる。

こうした細かなセキュリティ要件を満たす手法を検討した結果、Google Appsへ安全にアクセスできて情報が端末に残らない「セキュアブラウザ」を使うこと、認証にはユーザー認証/端末認証/専用ブラウザによる「3要素認証」を採用することが要件として定められた。

蓬萊氏ら情報システム部のスタッフは、厳しいセキュリティ要件を実現できるツールや技術の情報収集に奔走した。その中で、あるセミナーでソリトンシステムズのセッションに足を運んだのが、今回のシステム導入のきっかけとなった。

当初、ソリトンシステムズは別のソリューションを紹介したものの、要望を満たすことができなかった。

「すると次に“実はこんなことを考えている”と、開発・企画段階にあったソリューションを紹介してくれたのです。私は、まさにこれだと思いました」と蓬萊氏は当時を振り返る。

それが「Soliton SecureBrowser (以下SSB) /Soliton SecureGateway (以下SSG)」だった。

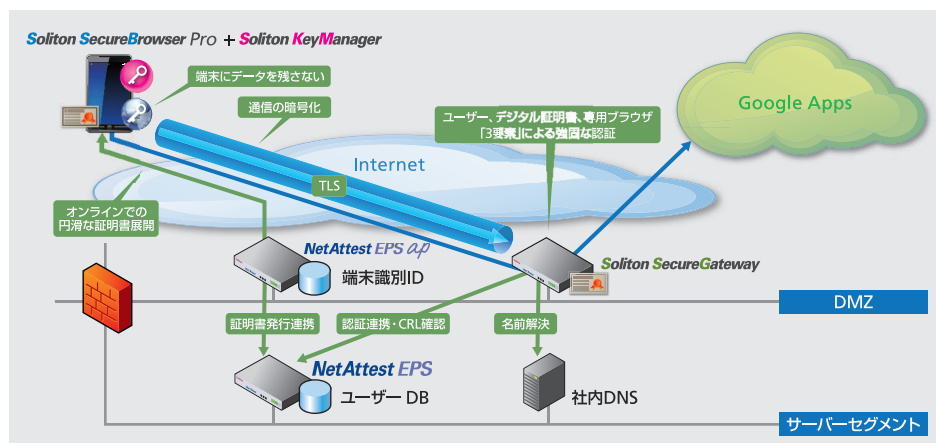
このほかにも、いくつかのSlerからソリューションの提案を受けたが、他社の提案は、複数のベンダー製品を組み合わせるものが多く、運用やサポートの面で不安があった。

蓬萊氏は「端末の個体識別と情報が端末に残らないという当社のニーズを1つのメーカーのソリューションとして提供されていることは、私たちにとっては大きなメリットでした。だからこそ、何か月も待つことができたのです」と語る。

そして、両社による導入に向けたプロジェクトが始まった。2013年8月に同製品はリリースされたが、中には、両社のやりとりにおいて



株式会社アグレックス
情報システム部長
蓬萊 啓八氏



生まれた機能も存在するという。

証明書展開の自動化で多数の デバイスをスムーズに利用可能に

アグレックスが導入したシステムは、図のとおりである。

スマートデバイス(iOS/Android)ユーザーは、端末にデータが残らないSSBを利用して、SSBからのアクセスのみを許可するSSGを通じて、Google Appsへアクセスする。SSBとSSGの間の通信は暗号化されており、別途VPN等を利用する必要がない。

端末の個体識別のための証明書の発行/展開には、「NetAttest EPS」「NetAttest EPS-ap」「Soliton KeyManager」を導入し、運用の効率化を図った。

蓬萊氏は「将来的に多くのデバイスに証明書を発行することを考えた場合、他社の提案にはこれを自動化できる仕組みがありませんでした。それが、ソリトンシステムズを選んだ理由の1つです」と選定のポイントを挙げる。

奇しくもアグレックスでは、別のシステムでNetAttest EPSやその他のソリトンシステムズ製品を導入しており、安定的に活用できていたことも安心感を生んだという。

蓬萊氏は「とはいえ、試験運用の当初は、つながらなかったり、Webの表示がおかしかったりといくつかの問題が発生していました。しかし、ソリ

トンシステムズが迅速に対応してくれたおかげで、環境はどんどん良くなっていきました」と語る。

「スキマ時間」を有効活用し 既になくならないシステムに

本システムは2013年11月より試験運用を開始し、2014年3月時点で、BYODを含む約140台のiOS/Androidで利用されている。将来的には、600~800台に導入台数を増やすことが想定されている。

エンドユーザーにとっての導入効果としては、移動中などの“スキマ時間”を有効活用できるようになったことがあげられる。従来のモバイルPCは、PCを開く場所を確保することからはじめなければならず、スキマ時間はほとんど活用できていなかった。今では、むしろ本システムは“なくなったら困る”という意見すら出ているとのことだ。

取材時点での蓬萊氏の採点は「80点」。当初の想定通り、管理負担は小さく、安心して運用できる点に満足しているという。ただし同氏は、ソリトンシステムズの技術力を信頼しているとしながらも、「エンドユーザーが簡単に使えるように、わかりやすいマニュアルがあると良いですね。90点台に向けて、いっしょに製品を育てていければと思います」と、さらなる期待を寄せている。

※記載の製品名は、各社の商標または登録商標です。

Soliton

株式会社ソリトンシステムズ <http://www.soliton.co.jp/>

〒160-0022 東京都新宿区新宿 2-4-3

TEL 03-5360-3811 FAX 03-5360-3880 netsales@soliton.co.jp

大阪営業所 06-6821-6777 福岡営業所 092-263-0400

名古屋営業所 052-963-9700 東北営業所 022-716-0766

札幌営業所 011-242-6111