

トヨタ自動車グループ、朝日航洋株式会社にて SASTIK が導入されました。

～安全なデータ活用として空の現場でも広がる SASTIK の活用～

株式会社サスライト(東京都港区 代表取締役植松真司:以下サスライト)は、情報漏洩事故のリスクを低減するセキュリティシステム「SASTIK III Thin-Client Layer(以下:SASTIK)」を朝日航洋株式会社へ(以下、朝日航洋)に導入しました。

朝日航洋はトヨタグループの子会社として、ヘリコプターの高度な運航技術と最先端の測量技術を基盤に全国54拠点を展開している、ヘリコプター業界シェアNo.1の企業です。今回利用対象となる「航空事業」の部門では、ドクターヘリの運航・整備、またテレビのCMやドラマ、映画をはじめ、マラソン中継、ニュース等の報道向け、レジャー関連まで幅広く事業を手がけています。その朝日航洋がBYODも見据えてセキュリティツールとして選んだのが、SASTIKでした。現在ではSASTIKを前提とした社内システム改善を行っており、また航空事業本部での導入を皮切りに全社導入に向けてもご検討されています。

導入製品:SASTIK III Thin-Client Layer

利用対象:航空事業従事者 50名



＜山間部での物資輸送にヘリコプターは有用＞



＜臨場感ある空からの映像をお届け＞

【異なるネットワーク間をセキュアに接続する、セキュアアクセスの決定打！】

朝日航洋では、出張先で業務を安全に効率的に遂行したいという現場からのニーズに応えるべく、安全かつ安価なシステム導入が課題でした。SASTIKはサーバ1台だけで、VPNや特別なWindowsライセンスを追加することなく安価にソリューションを実現出来る上、リモートPCにデータを一切残さないセキュアな環境の構築が可能です。

SASTIKはネットワークに繋がったPCにUSBキーを挿すだけで、セキュアに指定のサーバにアクセスすることができます。そのため出張先でも、わざわざ事務所へ戻ることなく、USBキーによる本人認証を基に、指定のシステムに安全に接続し閲覧や編集といった作業が簡単に行えます。SASTIKの利用中、通信とデータは暗号化され、利用後にUSBキーを抜くと、利用したPCから痕跡を削除します。利用したPCには一切のデータを残さないため、安心して利用することができます。

USBメモリの場合、仮に暗号化していても、紛失時には大量のデータそのものがなくなってしまい、パスワードが突破されてデータが悪用される可能性はゼロではありません。データ漏洩事故を防ぐためにはデータを持ち運ばないことが最も確実です。SASTIKの場合、持ち運ぶのはUSBのキーのみであり、その中にはデータが入っておりません。そのため、万が一キーを紛失してもデータの紛失は起こりません。さらに紛失したキーからのアクセスの切断や、アクセスログの採取も可能なので、事後に安全性を確保できるのに加え、データ漏洩が起こらなかったことを客観的に証明することが可能です。SASTIKはサーバ管理者の方にとっても安心して導入できるシステムです。

■プレスリリースに関するお問い合わせ先

株式会社サスライト(<http://www.saslite.com>) 社長室 上田 Tel : 03-5575-2211 e メール: pr-sas@saslite.com