

## USB シンククライアントシェア No.1<sup>※1</sup> 「SASTIK」、京都女子大学へ導入

～大学でも広がる活用。機密情報取り扱いの決定打～

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 アカデミック版（以下：SASTIK）」を京都女子大学に導入しました。

SASTIKは専用のUSBキーを用いて、サーバへと認証、WEBサーバやファイルサーバへの安全アクセスを可能にするソリューションです。京都女子大学ではSASTIKを用いて、ファイルサーバやグループウェアサーバへの安全アクセスを実現。出張時や、学外での機密情報取り扱い時に安全にデータを利用する環境を整えました。

導入製品：SASTIK III Thin-Client Layer アカデミック版

導入対象：京都女子大学の教職員



### 【ハードウェアによる確実な本人認証とデータセキュリティ】

現在自治体や企業、大学などで多くのサーバが導入されていますが、その大部分はセキュリティの観点からLANの中でのみの運用に留まっています。SASTIKではリモートの接続を躊躇させる二つの課題、「成りすましログイン」や、「接続元PCのデータ残留」を解決する機能を標準で搭載しています。ID/PWによる認証に加えUSBキーでのハードウェア認証によりなりすましを防御、また、これまで使用していたPCを仮想シンククライアント化した上でサーバに接続。接続元PCにデータを残せない仕組みになっています。これらの標準機能によって、サーバへのリモート接続の安全性を高め、LANの外からでも安全に接続できる環境を構築することができます。

### 【後を絶たないデータ漏洩事故対策への決定打！】

未だ後を絶たないデータ漏洩事故。仮に暗号化USBメモリを採用していても、データの入ったまま紛失してしまうと、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、データ漏洩が起らなかったことを客観的に証明することが出来ます。SASTIKはサーバ管理者の方も安心して導入できるシステムです。

※1 富士キメラ総研「月刊BT 2009年6月号」調べ

### ■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](mailto:pr-sas@saslite.com)