

USB シンククライアントシェア No.1※1 「SASTIK」、  
医療法人創起会くまもと森都総合病院（旧：NTT 西日本九州病院）へ導入  
～ドクターの安全なデータ活用として医療現場に広がる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 アカデミック版（以下：SASTIK）」を医療法人創起会くまもと森都総合病院（以下、くまもと森都総合病院）に導入しました。

2012年7月1日に、NTT西日本九州病院から名称変更したくまもと森都総合病院では、医師の業務効率改善を目的とし、SASTIKが導入されました。

SASTIK は専用の認証鍵であるUSB キーを用いて、院内データサーバやグループウェアへの安全アクセスを可能にするソリューションです。医局からの院内データへのアクセス、また出張時や学会などでの機密情報取り扱い時にSASTIKで安全にデータを利用できる環境を整えました。

導入製品：SASTIK III Thin-Client Layer

利用対象：くまもと森都総合病院 医師等 50名

**【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！】**

病院の中でも診察棟と医局でネットワークが違う場合、医師は診察棟に足を運ばなければ必要データにアクセス出来ません。このような同一組織間でネットワークが分かれているような時にもSASTIKは有効です。

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。そのため医局内にいても、わざわざ診察棟へいかずに、パソコンにUSBキーを挿すことで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。利用後はUSBキーを抜くだけで自動的に機能を終了し、利用したパソコンには一切のデータを残さないため、安心して利用できます。

USB メモリを用いた場合、例えば暗号化していても、紛失時には大量のデータそのものがなくなってしまいます。また暗号化されたデータのパスワードが突破されて、データを悪用される可能性も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\_\_