

# ディスクレスPCと大容量ストレージを使ったセキュリティ管理システム —STRAGEX

個人情報保護法やe文書法への対応、さらには日本版SOX法施行に備え、すべてのデータを集約して管理する「ストレージセントリック」が注目を集めている。これまでにない端末・データの集中管理技術として、NTT研究所が開発したiSCSIネットワークブート技術を用いたセキュリティ管理システム「STRAGEX」について、NTTの館 剛司プロデューサにうかがった。



日本電信電話(株) 第三部門  
サイバーセキュリティプロジェクト  
プロデューサ 館 剛司氏

## PCの情報漏洩防止と集中管理、耐災害性を実現

■■■■ 館プロデューサは、iSCSI ネットワーク・ブート技術によるセキュリティ管理システム「STRAGEX」をプロデュースされていますが、開発経緯からお聞かせください。

館 もともと、NTT研究所で広域イーサネットを使ったデータセンター間でのDR（ディザスタリカバリー）技術の研究開発を行っていたチームが、約5年前に、これからは構造化された業務用データベースだけでなく、個人管理に任されているクライアントPCに蓄積された非構造化データの管理が重要なテーマになると

いうことで、取り組んだのが始まりです。NTT研究所では、大容量ファイルの高速バックアップ転送技術として、当時ようやく製品が出始めたiSCSI（internet Small Computer System Interface）技術に着目しました。iSCSIは、FC（ファイバーチャネル）と比べ非常に安価で、効率的に大容量のファイル転送が行えるという特徴があります。このiSCSI技術は、ネットワーク上のディスクからOSをブート（起動）する際にも使えることから、まずはLinuxを使ったプロトタイプを作りました。これは、ディスクレス端末からネットワーク上のストレージにiSCSIインタフェースでアクセスし、

OSやアプリケーションをブートするとともに、ストレージ上のユーザーデータ領域を自動的に割り当てるもので、「ストレージセントリック・ネットワーク技術」と称していました。そして2005年の春に、Windowsマシンをターゲットにした商用版の開発プロジェクトを立ち上げ、2005年11月に第1版をリリースしました。

■■■■ STRAGEXでは、どのような機能を実現していますか。

館 図1に示すように、個々のPCのディスクを取り除き、センターの大容量ストレージ（iSCSIディスク）に集約させ、PCのOS、アプリケーション、データをセンター側で一元管理することによって、PCからの情報漏洩、ウイルス・ワーム対策などますます複雑化するPCのセキュリティ管理、災害・障害時のデータ消失などの課題を一挙に解決します。

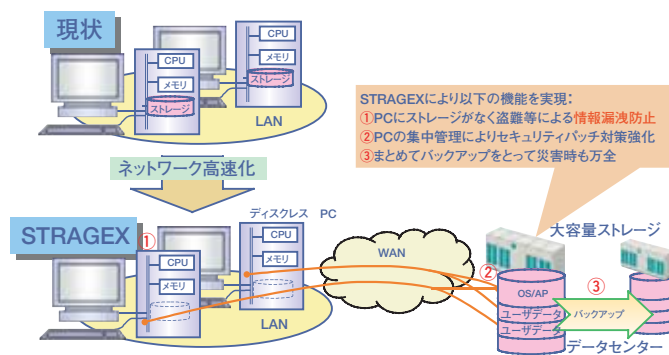


図1 STRAGEXとは



写真1 STRAGEXの中核部

方式 比較軸	SBC	ブレードPC	ネットワークブート型PC	STRAGEX (NTT)
端末からの 情報漏洩防止	○ 端末にデータ が存在しない	○ 端末にデータ が存在しない	○ 端末にデータ が存在しない	○ 端末にデータ が存在しない
導入の容易性 既存環境の 活用	○ 狭帯域NW上でも 動作可	○ 狭帯域NW上でも 動作可 <sup>*1</sup>	△ ブート時に広帯域 (クライアント当り 20-30Mbps)が必要	△ ブート時に広帯域 (クライアント当り 20-30Mbps)が必要
動作可能な アプリケーション	△ 動画、3D-CAD 等は不向き	△ 動画、3D-CAD 等は不向き <sup>*1</sup>	○ 通常のAPIは ほぼ動作可	○ 通常のAPIは ほぼ動作可
障害・災害 復旧対応	△ 災害復旧には別途、 バックアップシステム要	△ 災害復旧には別途、 バックアップシステム要	△ 災害復旧には別途、 バックアップシステム要	○ ストレージ冗長化で、 データ、端末OS、AP を復旧可

SBC : Server Based Computing  
\*1:ClearCUBE I/Portの場合

表1 端末・データの集中管理技術の比較

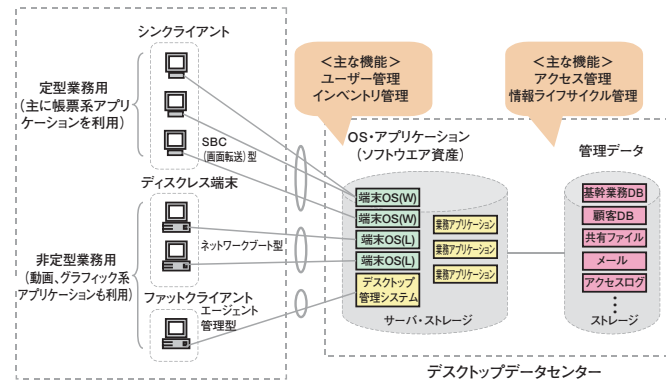


図2 STRAGEX開発計画の最終ターゲット

## 高負荷アプリの動作に加え、高拡張性・高可用性が特長

■ ■ ■ シンククライアント・システムの一つだと思えますが、他と比べどんな点が優れているとお考えですか。

**館** SBC (Server Based Computing) やブレードPCなど、いわゆるシンククライアントソリューションは、センター装置側のCPU、メモリで処理が行われ、画面データ、キー入力データがネットワーク上で転送されるため、動きの激しい画面表示や素早いレスポンスを求められるアプリケーションには不向きです。これに対し、ネットワークブート型は、ローカルのCPU、メモリの能力をフルに活かしますので、例えば動画のストリーミング再生やTV電話、細かいトレーディングチャートや3D-CADなどのアプリケーションも問題なく動作します。また市販のネットワークブート型ソリューションでは、多数のディスクレスPCがブート用サーバに常にアクセスしますので、サーバに処理負荷がかかります。これに対しSTRAGEXは、基本的にサー

バを使わずにストレージに直接アクセスして動作しますので、より多くのPCを取容できます。さらに、障害や災害時の復旧対応に特別にバックアップシステムを設けなくとも、ストレージのバックアップ機能を活用することで障害・災害対策が可能になります (表1参照)。

## 統合的なデータ管理、ソフトウェア資産管理の実現を目指す

■ ■ ■ 昨年11月にプロダクトをリリースされて、事業会社を含め反応はいかがでしたか…。

**館** 情報漏洩対策の観点で注目を集めているシンククライアントの一つとして、お客様や事業会社から着目されております。本格的な展開はこれからですが、すでにいくつかお客様へのご提案を始めています。

■ ■ ■ 今後の展開として、どのような取り組みを行っていくお考えですか。

**館** まず、私どもの本社ビルに2005年度末から2006年度にかけて全面導入し、実際の業務に活用することで、STRAGEXの有効性を実証していきます。さらに今後のオフィス用端末

の動向として、シンククライアントやファットクライアントも含め、それぞれの適性に応じて併存することになると考えています。そうした時に重要なのは、複数の端末方式を使い分けながらも、データやソフトウェア資産をいかに統合管理するかであり、これをiSCSI技術を活用して実現することが、STRAGEX計画の最終ターゲットです (図2参照)。

■ ■ ■ なぜiSCSIなのですか…。

**館** 冒頭で述べたように、iSCSIはIPネットワーク上での大容量のファイルのバックアップや情報管理に非常に適した新しい技術です。例えば、各ロケーションごとに分散的に管理されたユーザーデータやソフトウェア資産を、iSCSIインタフェースを使うことによって広域ネットワークをまたがって、一括でボリュームコピーをしたり、メンテナンスが行えます。こういった特徴を持つiSCSI製品とNTT研究所が開発した技術を上手く活用することで、企業内における情報やソフトウェア資産の一元管理が可能になると考えています。

■ ■ ■ 本日は有り難うございました。