NEWS RELEASE

NTT

日本電信電話株式会社

２００５年４月２６日

ＮＴＴ研究所開発の情報漏洩対策ソリューションの本年度内での商用化に向けて
～ＮＴＴ本社ビルに「ストレージ・セントリック・セキュリティ・システム」を導入～

日本電信電話株式会社（以下NTT、本社：東京都千代田区、代表取締役社長：和田紀夫）では、ＮＴＴ研究所が開発した「ストレージ・セントリック・セキュリティ・システム」（以下、本システム）の本年度内での商用化に向けた取り組みを進めていますが、この度、その取り組みの一環として本社ビル（大手町逓信ビル）に本システムを本年度から全面導入します。（一部システムについては、２００４年度末に導入済。）

特に本年4月1日からの個人情報保護法の本格施行に伴い、情報漏洩対策として各種ソリューションがすでに製品化・サービス化されていますが、お客様（企業、官公庁、学校など）が本当に安心して使っていただくためには、次の３つがポイントになります（図１）。

<1>できるだけ人手を煩わせずシステムでセキュリティをカバーできること。

<2>システム自体の管理稼動やランニングコストが膨大にならないこと。

<3>既存のシステム・業務を前提としており導入障壁が低いこと。

本システムはこれらのポイントに着目し、エンドユーザの利便性を損なうことなく、システム管理部門の稼動削減に貢献し、経営者から見ても導入障壁の低い、より完成度の高い情報漏洩対策ソリューションとして、本年度内の商用化を目指して実証段階に入ります。

＜導入システムの概要＞（図２参照）

（１）デスクトップ端末のセキュリティ強化

本システムではまず、デスクトップ端末のセキュリティ管理、データのバックアップ管理などのメンテナンス作業を効率化するために、ユーザデータだけでなくＯＳやアプリケーションなどのソフトウエア資産もストレージで一括管理します。エンドユーザは、ディスクレスのＰＣ端末を利用するたびに、センターのストレージに直接アクセスして既設の社内ＬＡＮ経由で端末を起動しま

す。ここではＮＴＴ研究所が開発した「ストレージ・セントリック・ネットワーク技術」[*1]が適用されています。
　本技術により、端末の盗難やハードウエア故障に伴う情報漏洩・破壊のリスクを大幅に低減できるとともに、エンドユーザは従来の使い勝手をそのままに（起動後は通常のＰＣと全く同等）、端末毎のセキュリティ管理、データバックアップ管理などに煩わされることがなくなります。また、基本的には（ユーザ管理用サーバを除けば）端末と大容量ストレージ装置だけでシステムを構成できるため、大規模導入に際しても大量のサーバ設置に伴うコストや管理稼動は一切発生しません。

（２）持ち出しノートＰＣのセキュリティ強化
　より情報漏洩リスクの高いノートＰＣを利用する際には、外出先からリモートアクセス経由で、または会議室から無線ＬＡＮ経由で、社内ＬＡＮ上のディスクレス端末を遠隔操作で起動させます。このディスクレス端末は、各エンドユーザが社内のデスクトップ端末を利用する際と全く同じＯＳやアプリケーションの環境で起動されます。ノートＰＣ上ではそのディスクレス端末上の画面イメージだけを閲覧・操作することで、リモートアクセス時の比較的狭帯域の通信速度での利用を可能にしています。ノートＰＣ側には、社内ＬＡＮにリモートアクセスするためのＶＰＮ（IPsec対応）アクセス用ソフトウエア、および無線ＬＡＮ（802.1x対応）アクセス用ソフトウエアだけが搭載され、ユーザ認証用のＵＳＢキーを使って社内ＬＡＮにアクセスする技術「セキュア企業網アクセス制御技術」[*2]が適用されます。
　本技術により、システム管理者側でもアクセスシステム毎（リモートアクセス、無線ＬＡＮ、有線ＬＡＮなど）のユーザ管理（システムへのユーザ登録・削除など）を一元化できるため、ユーザアカウント管理や問合せ対応に要する稼動を数分の一に削減できる見込です。さらに、ノートＰＣにはネットワークアクセス用ソフトウエア以外のアプリケーションを搭載しませんので、既存のノートＰＣ（ディスク付き）をそのまま（ユーザ権限で）活用して頂いてもセキュリティを保つことができます。

（３）ファイル管理のセキュリティ強化
　情報漏洩対策としては、端末やアクセスネットワークなどインフラとしてのセキュリティ強化だけでなく、情報（文書ファイル）の管理そのものを強化するアプリケーションと組合せることが有効です。本システムでは、ドキュメント管理システムとして市販製品である「Smart Leak Protect」（NTTアドバンステクノロジ（株））[*3]を採用し、各ユーザのファイル操作をセキュリティポリシーに則って監視し、違反操作を検出すると業務管理者にアラームを上げたり、外部記憶媒体への重要データのコピーを禁止します。
特に本システムでは、センターストレージ上で各端末のＯＳやユーザ環境領域が一元管理されているため、「Smart Leak Protect」のエージェントソフトのインストールやバージョンアップ、セキュリティポリシーの変更などが、システ

ム管理者側から漏れなく一括して行えますので、ドキュメント管理システムの導入に伴う管理稼動を最小限に抑えることができます。また本システムでは、端末側で一律に外部記録媒体への書き出しを禁止する設定も可能ですが、それだけではユーザ利便性を損ない、かえって不正な情報持出しを助長してしまう側面もあります。そこで、ドキュメント管理システムと組み合わせることで、重要データだけの書き出しを禁止するなど、セキュリティを強化しつつ従来の業務フローや利便性をなるべく損なわない導入が可能となります。

＜導入効果・今後の展開＞

　これらのシステムは２００６年度までに順次本社ビルへ導入し、全端末を置き換えることで、ＰＣ端末のセキュリティ管理やデータのバックアップ管理などに要していたトータルの管理・運用コストを、従来比で約５０％削減できる見込です。また、本システムは本社ビルでの運用開始と並行して、本年度中にＮＴＴグループを通して商用化していく予定です。
　なお、本システムを5月12日～13日に東京プリンスホテル パークタワーで開催される、RSA Conference 2005 Japanに出展いたします。

＜用語解説＞

*1　ストレージ・セントリック・ネットワーク技術
　NTT情報流通プラットフォーム研究所が開発した、ＰＣ端末のネットワークブートおよびディスク領域マウントのための技術。ディスクレス端末からストレージにiSCSIインタフェースでアクセスし、ＯＳ（WindowsおよびLinux）やアプリケーションをネットワーク経由で起動（ブート）するとともに、ストレージ上のユーザデータ領域を自動的に割り当て（マウント）できる。

*2　セキュア企業網アクセス制御技術
　NTT情報流通プラットフォーム研究所が開発した、ＰＣ端末からのネットワークアクセスに関するプロファイル情報を一元管理する技術。アクセスネットワーク（有線LAN、無線LAN、インターネットＶＰＮなど）毎に異なるＰＣ端末のプロファイル設定をサーバおよび端末側で一元管理し、ユーザはアクセスネットワークの違いを意識することなく、ＵＳＢキー認証を使って社内ＬＡＮにアクセスできる。

*3　Smart Leak Protect
　NTTアドバンステクノロジ（株）（本社：東京都新宿区、代表取締役社長：石川　宏、以下、ＮＴＴ－ＡＴ）の提供する内部情報漏洩対策システム。（株）インテリジェント ウェイブ(本社：東京都江東区、代表取締役社長：山本　祥之)開発の「CWAT(Cyber Warning Alert Termination)」をベースに、従来

の基本機能（情報漏洩に直結する各種操作やデバイス環境などの監視・防御機能、Eメール等によるネットワーク経由の情報漏洩の監視・防御機能）に加え、両社による共同開発機能（ＮＴＴ研究所開発の次世代暗号Camelliaを用いた重要情報の暗号化）やＮＴＴ－ＡＴ社独自開発機能（PC利用者の認証機能、監視ログ情報の編集機能など）をサポートする。

・図1　情報漏洩対策システムの普及のためのポイント
・図2　本社ビルに導入するストレージ・セントリック・　セキュリティ・システム

＜本リリースに関する報道機関からの問い合わせ先＞
日本電信電話株式会社
第一部門広報室
大道、阿部
03-5205-5550

＜本リリースに関する報道機関以外からの問い合わせ先＞
日本電信電話株式会社
第三部門プロデュース担当
舘
電話：　03-5205-5390