ネット不正侵入・ウイルス対策

接続一時切り安全確保

中間サーバーが監視

イオノスが新技術

技術開発ベンチャーのイオノス（東京・世田谷、大穂園井社長）は、スイッチを使って物理的に接続を遮断する、新しいネットワーク・セキュリティー技術を開発した。通常インターネットでは、つながった回線上でソフトウエアを使って不正侵入を判断・防止するが、回線を接続している限り完全な防御は難しい。従来のファイアウオールのようなソフト的防御とは異なり、イオノスは一時的に「接続を切る」状態を作ることで、強固な安全性を追求する。

外のインターネットと企業内のネットワークの間に、シーソー型のスイッチが付いた中間サーバーを置く。「外部と中間サーバーが接続した状態」か「内部と中間サーバーが接続した状態」は、常にどちらか一方しか成立しない。外部からの接続要求やデータはいったん中間サーバーにたまり、その後外部との接続を切って内部と接続し直す。

中間サーバー部分には不正な接続要求、データやウイルスなどをチェックする機能と、サーバーの動作を監視する管制部があり、通信の異常を判定する。

ハッキング行為はファイアウオールの穴を見つけ、不正な方法で内部と直結する。この穴を通じ内部のデータを破壊したり盗み出したりする。新システムは外部からの命令やデータ送信を中間サーバーが仲介、外部からは中間サーバーの情報しか得られないため、外部から内部へ直接回線を接続することは不可能になる。

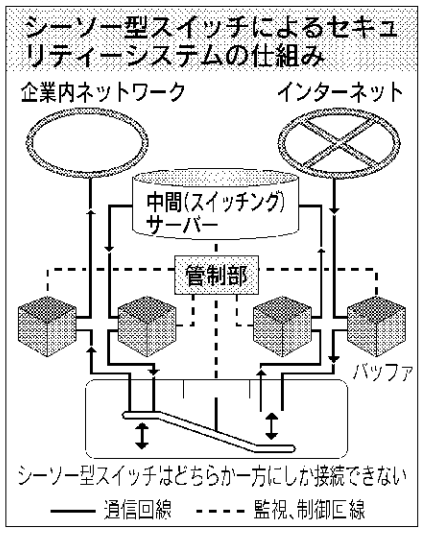
中間サーバーは外部・内部双方にそれぞれ二つ、バッファと呼ぶ機能を持つ。処理能力を超す大量データを送りつけサーバーを停止させるDOS（サービス拒否）攻撃を受けた場合、片方が処理不能でも一方が代行して機能を維持する。バッファは停止しても十数秒で復帰するため、継続的な攻撃にも強いという。

イオノスは三月中旬の情報処理学会で基本理論を発表した。試作品を設計中で四月には完成の予定。ハード面でのスイッチの耐久性、大容量データへの対応などの課題があるため、セキュリティー関連企業と共同で製品化する方針。

大穂社長がNTTのシステム開発技術者だった星野博一副社長のアイデアに着目、二人で昨年四月にイオノスを起業した。慶応大学などの学生、大学院生八人を開発チームとして集めた。星野副社長と連名で論文を発表した慶大環境情報学部三年生の岩崎弾氏は、セキュリティー関連の論文を二本発表するなど、業界で知られている。

富士通ビジネスシステム・営業推進統括部の岡田一馬セキュリティー担当部長は「スピードやスイッチ部分の詰めは必要だが、物理的な切断は究極のセキュリティー。従来にない面白いアイデア」と評価する。

（**ファイアウオール**は「Sangyo一語」参照）



掲載日 2001年04月02日 日経産業新聞 001ページ