FAQ

Frequently Asked Question

いまさら聞けない

いまだから聞きたい

このコーナーでは読者の皆さんのインターネットに関する疑問や質問にお答えします。「？」と感じたことはどのようなことでも構いませんので、下記のメールアドレスまでご質問ください。なお、ご質問へのメールでの回答はできませんのでご了承ください。

○ご質問はこちらまで
im-faq@impress.co.jp

今月のポイント

1 SANとNASはどう違うのか

2 ハニーポットの甘い蜜とは

Q

SANとNASは両方似たような機能だと思うのですが、それぞれどのように違うのでしょうか？（Serioさん）

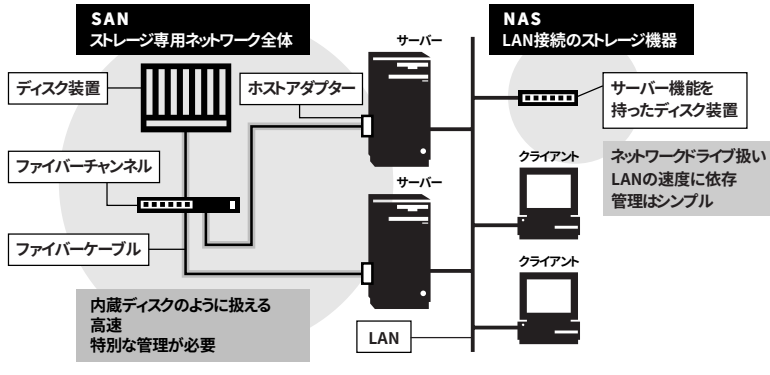
A

どちらもサーバーやクライアントが、ネットワークに接続されたストレージ（データ保存領域）を利用する仕組みです。

「SAN」は、Storage Area Networkの略で、サーバーとディスク装置の間を接続するデータストレージ専用のネットワークを指します。主にファイバーケーブルを使い、接続にはファイバーチャンネルとホストアダプターと呼ばれるインターフェイス装置が必要です。専用のファイバーケーブル接続で高速にデータをやりとりできるので、大容量のストレージを内蔵ディスク装置のように使えます。そのため、複数のサーバーから大量のデータアクセスが必要なデータベースのシステムなどで利用されます。また、専用のツールによりストレージを管理する必要があります。

「NAS」は、Network-Attached Storageの略で、イーサネットのLANに接続して利用するディスク装置のことです。NASの製品をLANにつなぎ、IPアドレスやユーザーなどを設定するだけで、LAN経由でディスクにアクセスできます。ウィンドウズやリナックスなどのOSが組み込んであり、ファイル共用ができるディスク装置だと考えるとわかりやすいでしょう。管理は楽ですが、LANを利用するため、シビアな転送速度が要求される用途には向かず、バックアップ用ファイルの格納や共有ファイルの保管などに利用されます。

SANはサーバー向けの大規模な製品がほとんどですが、NASならば一般向けに「LAN接続ハードディスク」などの製品が販売されていますので、デジカメ画像やムービーを家族のパソコンで共有するなどの利用方法があります。　（鈴木雅登）



SANはストレージ専用ネットワーク
NASはLANに接続するストレージ機器

Q ハッカーをつかまえる「ハニーポット」がインターネット中に仕掛けられていると聞きました。これにつかまると何かまずいことがあるのでしょうか？（大阪府　藤田さん）

攻撃者をおびき寄せる専用サーバー アタックを検知してさらに攻撃手法も調査

A

普通に電子メールやウェブなどでインターネットを利用している限り、誤ってハニーポットにつかまることはありません。

ここで言う「ハニーポット」とは、ネットワークセキュリティーのための仕組みです。インターネットで悪事を働く攻撃者が「カモを見つけた」と喜びそうな“甘いエサ”を置いておき、攻撃者をおびき寄せるシステムのことです。熊が甘い蜜に誘われてやってくるのにたとえて「ハニーポット（蜜つぼ）」と名づけられました。

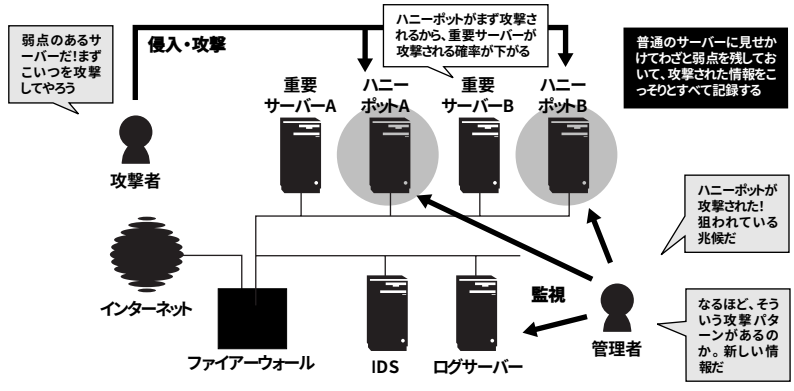
ハニーポットでは、わざとセキュリティー上問題のある状態にしたおとりサーバーをインターネットに接続します。このサーバーは普通のサーバーに見えますが、実はサーバーに対する行動、通信や、サーバーに侵入して中でとる行動を、攻撃者にはわからないように監視して記録するシステムになっています。

ハニーポットで「つかまえる」と言いますが、実際には攻撃者を逮捕するのが目的ではありません。ハニーポットを設置する目的は、大別すると2つあります。

1つは、“おとり”として攻撃の兆候を把握する用途です。ハニーポットを図のように重要なシステムに付随する形で設置すると、ハニーポットが攻撃されることで、重要なシステムが攻撃される危険を減らし、かつ攻撃が開始されたという合図を得ることができます。通常、ハニーポット以外の手段では、不正アクセス監視システム（IDS：Intrusion Detection System）で不正アクセスの兆候を検知させますが、IDSでは攻撃パターンをマッチングさせて不正アクセスを検知することから、攻撃が成功していても成功していなくても警告を発するという誤検知の問題が避けて通れません。その点ハニーポットは、あらかじめ、攻撃されてその受けた攻撃を確実に検知することを前提に構築されているため、誤検知することなく確実に不正アクセスの兆候を見つけることができます。ハニーポットは誤検知のない唯一の不正アクセス監視システムとも言えるのです。このような目的で構築されるハニーポットはさまざまなツールを組み合わせたり専用ソフトを使ったりして作られますが、商用ソフトではシマンテックのSymantec Decoy Server（旧名Mantrap）が、日本で販売されているものとしては唯一のものになります。

ハニーポットが設置されるもう1つの理由は、未知のセキュリティーホールやネットワークセキュリティーの最新テクニックを収集・研究することです。攻撃者が見つけた新しい脆弱性や攻撃手法を対策側ができるだけ早く知ることは、セキュリティー上重要です。実際に不正アクセスを受けて侵入されるハニーポットは、攻撃者の行動パターンやテクニックなどを収集して、新しい攻撃手法に対する防御手段や検知手段を研究するのに最適なのです。現在、世界では、いくつかのこのような研究目的のハニーポットプロジェクトが立ち上がっており、有名なプロジェクトとしては「The Honeynet Project」URL01や、日本では日本ネットワークセキュリティ協会URL02のハニーポットワーキンググループなどがあります。（濱本@connect24h）

URL01 http://www.honeynet.org/
URL02 http://www.jnsa.org/



［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp