Database Exposure Survey2007
～無防備なDBサーバがインターネット上に50万台存在～

NGSSoftware Insight Security Research (NISR)
デービッド・リッチフィールド (David Litchfield)

世界のデータベースセキュリティ状況が悪化している！と英国NGSソフトウェア　マネージング・ディレクターであり、NGSソフトウェア・インサイト・セキュリティ・リサーチ(NISR)のDBセキュリティ研究者であるデービッド・リッチフィールド氏は、Database Exposure Survey2007の中で警鐘を鳴らした。本レポートによるとインターネット上に無防備なデータベースサーバが推定50万台存在しているという事実が判明した。

リッチフィールド氏は、2005年12月にはじめて「Database Exposure Survey」を発表した。その時の調査結果によると約35万台の無防備なSQL Server、Oracle DBが存在し、危険な状態であると警鐘を鳴らしていた。今回の結果は、これを大幅に上回る数のデータベースが無防備な状態で危険にさらされていることが明らかになった。

リッチフィールド氏は、「人々はファイアウォールで自衛もせず、パッチの適用水準は悪いままである。」と指摘し、さらに無防備なデータベースの存在がワーム急増の要因だとして警鐘を鳴らしている。

NGSソフトウェアの国内総代理店である三菱総研DCSは、従来からNISRからのDBセキュリティに関する調査報告レポートを翻訳し提供してきたが、本レポートの内容は特に重要であると考え、今回JNSAに寄稿し日本国内のデータベース管理者やセキュリティ責任者にも知らせるべきと判断した。

2007年版のDatabase Exposure Surveyは、2007年11月19日にリッチフィールド氏から発表され、三菱総研DCSのWebサイトから和訳版がダウンロード可能となっている。

http://www.dcs.co.jp/security/contact/index.html

三菱総研 DCS 株式会社 事業推進企画部
小林　秀雄

はじめに

この調査は、デフォルトのTCPポートをリスンし、ファイアウォールで保護されていないデータベースサーバーが、インターネット上にどのくらい存在するかに答えようとするものである。この数値は、インターネット上のホストをランダムに多数サンプリングし、その結果をインターネットアドレス空間に広げて見積もることで得ている。今後データベースワームや実際のハッカーや犯罪者からのデータベースセキュリティ侵害にさらされるリスクを決定する助けとなるだろう。前回この調査を行ったのは2005年12月で、今回の調査結果に目を向けると同時に、2005年の結果[1]との比較、対比を行う。

結果要旨

調査により、およそ368,000のMicrosoft SQL Serverがインターネット上で直接アクセス可能であり、およそ124,000のOracleデータベースサーバーがインターネット上で直接アクセス可能であると判明した。この2つのベンダーで492,000のデータベースサーバーがファイアウォールで保護されずにインターネット上にむき出しのまま置かれている。Oracleサーバーの数は、およそ140,000だった2005年以来、やや減少している。一方で、SQL Serverの数は2005年の210,000から劇的に増えている。SQL Serverのうち82%はSQL Server 2000で動作している。Service Pack 4で動作しているのは46%に過ぎず、残りはService Pack 3aまたはそれ以前で動作している。また、実に4%がまったくパッチを当てていないことがわかった。Oracleサーバーに関しては、深刻な脆弱性を持つことが判明しているバージョンで動作しているサーバーが66%あることがわかった。調査結果はまた、hotfixを配備せず、Service Packが出るまで待っていることも示唆している。たとえば、SQL Server 2000では臨時の修正が施されているものは129のシステムのうち8つで、残りは

RTM、Service Pack 3/3a、またはService Pack 4のいずれかで動作していた。

私見だが、この調査結果は重大なリスクがあることを表している。これらのシステムのうち商用に使用されているものがどの程度あるかわからないが、50万近くあるサーバーにアクセス可能であることから、外部のハッカーや犯罪者が商用システムや機密情報にアクセスできる可能性があるのは明らかである。Oracleは、DBAアカウントを含む多数のユーザーアカウントをデフォルトのパスワードでインストールし、古いバージョンのSQL Serverは、パスワードなしでスーパーユーザーアカウント(sa)をインストールすることはよく知られている。これら保護されていないデータベースサーバーのうちどの程度が、このデフォルト値で設置してあるだろうか。

調査の実施方法

2005年の調査では8000のアドレスをランダムに選択し、それに続く60のアドレスにデータベースサーバーが存在するか調べた。つまり、480,000のアドレスを調べている。今回の調査では別のやり方を用いた。1,160,000のランダムなIPアドレスに対して調べた。各IPアドレスのTCPのポート1433（SQL Server）と1521（Oracle）を調べ、ポートが開いていればバージョンのチェックを行った。誤判定を排除するために、バージョンチェックに正しい反応を返したシステムだけをカウントした。IPアドレスの範囲は2^32ビットだが、224.0.0.0より小さいアドレスのみを使用した。244.0.0.0以上のアドレスはマルチキャストアドレスである。つまり、3,753,869,056のアドレスがありえる。その範囲のうち、10.x.x.x、172.16.x.x、および192.168.x.xはプライベートアドレスとみなされ、127.x.x.xはローカルシステムを表している。これにより、使用可能なアドレスは3,720,183,560に減る。この3,720,183,560のうち、73%だけが実際にアドレスが割り当てられており[2a]、利用可能なホストは2,715,733,999になる。（注意：IANAは192.0.2.0/24（TEST-NET）などの範囲のアドレスも予約している[2b]が、これは除外していない。）調べたシステムのIPアドレスは、Windows上でCのrand()関数でランダムに生成した。これは、線形合同法による乱数生成関数である。カバレッジに関しては、この手法は調査で調べるアドレスをうまく分散させている。

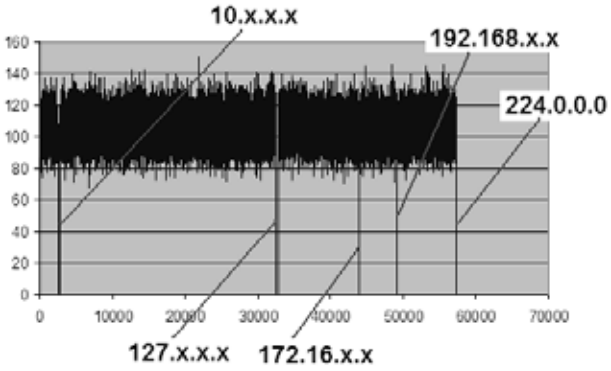

図1：ガバレッジ

図1のグラフは、16ビットずつのブロック(65,535のアドレスを含む)それぞれに対して、生成されたアドレスの数を表したものである。見てわかるとおり、プライベート領域(10.x.x.x、172.16.x.x、192.168.x.x、127.x.x.x)とマルチキャスト以外のすべてが調べられている。

結果

調査は1,160,000のアドレスに対して行った。157のSQL Serverが見つかり、53のOracleサーバーが見つかった。これは7388のホストのうち1つがSQL Serverを実行し(1,160,000 / 157)、21886のホストのうち1つがOracleを実行している(1,160,000 / 157)ことを意味する。7388のホストに対して1つのSQL Serverであることから、使用されているIPアドレス範囲(2,715,733,999)に広げて概算すると、推定367,587のSQL Server（2715733999 / 7388）がイ

ンターネット上でアクセス可能である。 21886のホストにつき1つのOracleサーバーが存在することから、2715733999 / 21886 = 124,085のOracleサーバーがインターネット上でアクセス可能である。これらのシステムの分析結果を検証しよう。

SQL Serverに対する結果

1,160,000のIPアドレスをランダムにチェックして見つかった157のシステムのうち、129がSQL Server 2000を実行し、28がSQL Server 2005を実行していた。

SQL Server 2000バージョン	検出数
8.0.194	5
8.0.311	3
8.0.760	25
8.0.766	31
8.0.818	6
8.0.2039	59

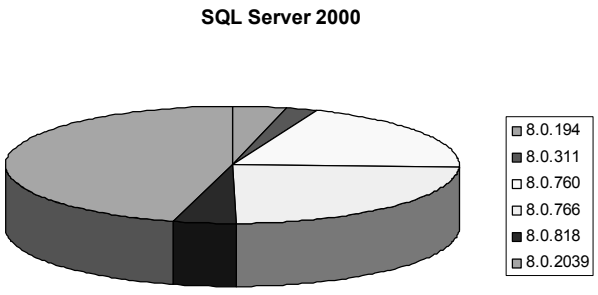

図2：SQL Server 2000 のバージョンの解析結果

ここで、129のSQL Server 2000システムのうち56（43%）が未だにSP3/SP3a上で動作していることがわかる。これは2005年よりも30%低下している。129のうち59（46%）がSP4で動作しており、2005年から26%上昇している。これはよいことだ。あいにく、8つのシステムがSQL Server 2000 RTMおよびRTMaで動作している。ただしRTMaのシステムは、Slammerワームに悪用される欠陥に対するパッチが当てられている。

臨時のパッチまたはhotfixを当てているシステムは8だけだった。ほかは、RTM、SP3/3a、Service Pack 4のいずれかである。これは、そのような人たちがhotfixはインストールせず、Service Packが出るまで待っていることを示唆している。

SQL Server 2005バージョン	検出数
9.0.1399	12
9.0.1406	2
9.0.2047	4
9.0.3042	4
9.0.3054	6

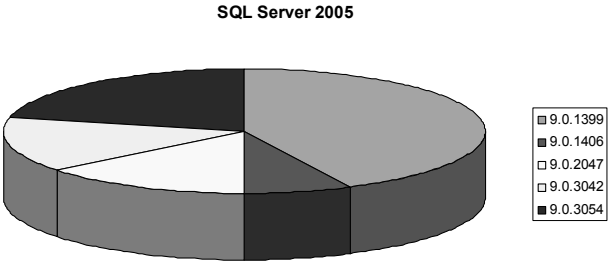

図3：SQL Server 2005 のバージョン

SQL Server 2007の調査結果の2005年との比較

2005年の調査結果では、保護されていないSQL Serverがおよそ210,000あることが示唆された。2年後の今回の調査結果では、現在およそ368,000あることがわかった。これは大幅な増加である。これがSQL Serverのインストール数が増えたことによるのかMSDEのインストール数が増えたことによるのかはわからない。どちらにせよ、数が増加したことで、Slammer、Spida、Voyager Alpha Forceなどの潜在的なデータベースワームに関するリスクも増大している。ここで救いとなるのが、SQL Serverには2003年以来大きな欠陥が見つかっていないことである。しかし、2005年からの増加がSQL Serverの増加に起因するのなら、これは潜在的なデータベースセキュリティ侵害のリスクの増大を意味し、したがってIDの盗難や不正使用の増加を意味するので、一般消費者にとってよい前兆ではない。潜在的な

ワームに限定すると、SQL Serverによる増加であろうとMSDEによる増加であろうと、リスクに影響する。

Oracleに対する結果

2005年の調査結果では、ファイアウォールで保護されずにインターネット上でアクセス可能なOracleデータベースサーバーがおよそ140,000あった。今回の調査では、およそ124,000あると見積もられている。この減少はスキャン方法が変わったことによるかもしれないが、おそらくそうではない。もしそれが正しければ、SQL Serverの数も同様の減少が見られると考えられるからである。

検出されたシステムを見てみる。

Oracleバージョン	検出数
8.0.5.0.0	5
8.0.6.0.0	1
8.1.7.0.0	4
8.1.7.4.0	2
9.0.1.1.1	1
9.2.0.1.0	16
9.2.0.3.0	6
9.2.0.4.0	3
9.2.0.6.0	4
9.2.0.8.0	1
10.2.0.1.0	5
10.2.0.2.0	1
10.2.0.3.0	4

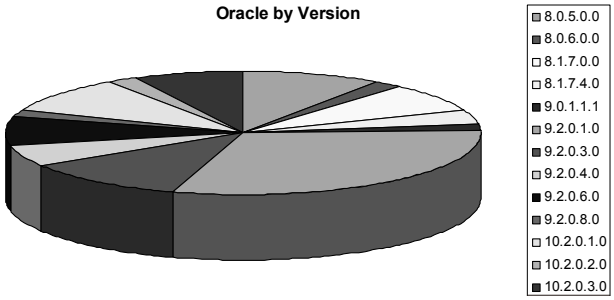

図4：Oracleのバージョン

13もの多数のサーバーが、ユーザー名が長いとバッファオーバフローを起こし、ユーザーIDとパスワードなしに悪用される脆弱性が知られている古いバージョンで動作している。35（66%）がextprocのバッファオーバーフロー[3],[4]を持つことが知られているバージョンで動作している。この長いユーザー名とextprocのオーバーフローにより、攻撃者はユーザー名とパスワードなしに悪用できる。

オペレーティングシステム別のOracleの解析結果

オペレーティングシステム別のOracleの解析結果はじつに興味深い。保護されていないOracleサーバーの多数がWindows上で動作していることがわかる。これは、Windowsユーザーがセキュリティに関して何をすればよいか知らないという神話を裏付けているのだろうか?おそらくそうではない。SolarisとLinuxシステムの検出数の合計がそれと大差なく、Windowsがほかより悪いとみなすことはできない。

OS	検出数
Windows	30
Solaris	7
Linux	16

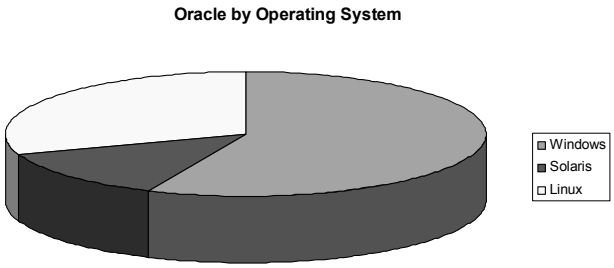

図4：OS別のOracle

次に何をすべきか

データベース管理者の多数が自分たちのシステムがインターネットからアクセスできるかどうかさえ知らないのかもしれない。あるアプリケーションのテスト用にファイアウォールに穴を空け、テスト完了後に閉じ忘れているのが見つかることは、一般的でないとは言えない。このステップを行えば、関連したリスクを最小限に抑えることができる。

- 自分たちのデータベースサーバーがインターネットからアクセスできないと思うのなら、その理解が正しいかどうかテストして確かめる。これは、データベースサーバーがリスンしているTCPポートに対して、たとえばTCPポートスキャナを使用してTELNETを試みればよい。
- もし、サードパーティに自分たちのデータベースサーバーへのアクセスを許可しなければならないなら、誰彼かまわずアクセスを許してはならない。設定したIPアドレスやアドレス範囲からの接続のみを許すようにファイアウォールを設定する。
- デフォルトのユーザーアカウントのパスワードを必ず変更しておく。使われていないアカウントをロックする。使用しているアカウントには、強固で異なるパスワードを使用する。
- 最新のパッチを当てておく! これはたやすいことと思えるが、そうでないことが証拠からわかる。
- データベース固有の脆弱性監査スキャナを用いて、定期的に脆弱性監査を実行する。そのようなツールの例としては、NGSSQuirreL、Appdetective、Shadow DB Scannerなどがある。
- ハッカーがシステムに侵入しようとしていないか、ログを定期的に検査する。

結論

推定368,000のMicrosoft SQL Serverと124,000のOracleデータベースサーバー。この調査の結果から、じつに多数のデータベースサーバーがインターネット上で攻撃に対して無防備に存在していることが示唆される。パッチを完全に当てていないことがわかったシステムの数、およびSQL Server数の大幅な増加は、世界のデータベースセキュリティ状況が悪くなっていることを示している。最後に注意しておきたいのは、この数値がデフォルトのTCPポートをリスンするシステムの数から見積もったものであることである。疑いなく、デフォルト以外の2433や1526といったポートをリスンするものはもっとたくさん存在する。今回の調査ではそのようなシステムを探さなかったが、ハッカーや犯罪者が探すことは確実であると言える。

[1] http://www.databasesecurity.com/dbsec/database-exposure-survey-2005.pdf
[2a] http://www.isi.edu/ant/address/
[2b] http://tools.ietf.org/html/rfc3330
[3] http://www.nextgenss.com/advisories/ora-extproc.txt
[4] http://www.ngssoftware.com/advisories/oracle23122004/