Distributed via @police
http://www.npa.go.jp/cyberpolice/

平成 27 年3月 30 日

Topic

「ビッグデータ」等で利用されている NoSQL データベースに対する探索行為について

「ビッグデータ」[i]等で利用され、注目を浴びている NoSQL データベースである MongoDB に対する探索行為が依然として高水準で推移しているとともに、その他2種類の NoSQL データベースに対しても探索行為が増加していることを確認しました。これらのデータベース管理システムを利用している企業や組織においては、インターネットへの不要な公開を停止する、適切な認証を実施する等の対策を実施することを推奨します。

1 MongoDB に対する探索行為が依然として高水準で推移

近年、「ビッグデータ」といった用語で表現される大規模データの取扱いの需要が増大しています。このため、既存の RDBMS[ii]では実現できない性能や特性を持つ新たなデータベース管理システムが多数開発されており、「NoSQL」[iii]といった呼称で総称されています。MongoDB も、この「NoSQL」に分類されるデータベースです。

平成 27 年2月 20 日に、MongoDB に対する探索行為の増加について注意喚起[iv]を実施しているところですが、その後も MongoDB データベースの情報収集を試みる問い合わせを依然として高い水準で観測しています（図1）。

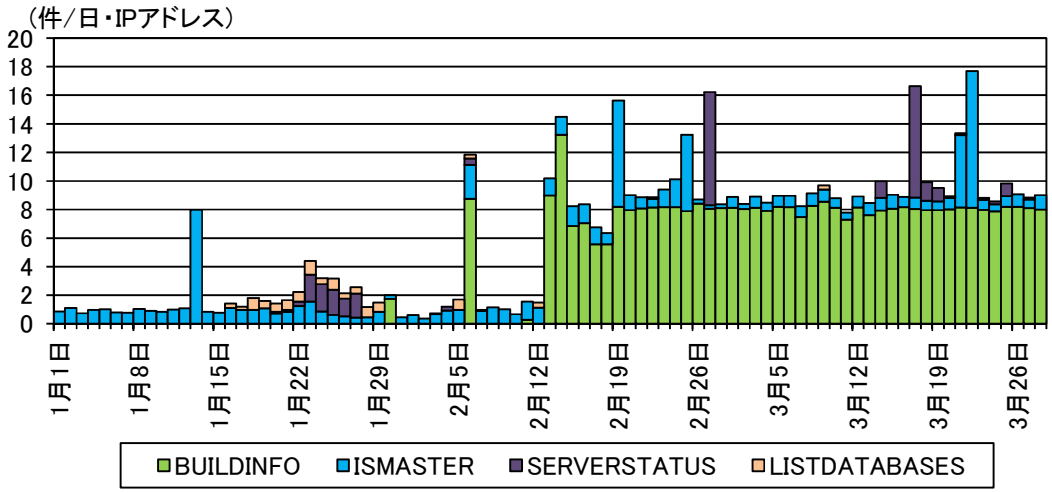

図1 MongoDB に対する問い合わせ内容別アクセス件数の推移（H27.1.1～3.28）

[i] ビッグデータについては明確な定義はありませんが、総務省の情報通信審議会 ICT 基本戦略ボード「ビッグデータの活用に関するアドホックグループ」資料において、「ICT（情報通信技術）の進展により生成・収集・蓄積等が可能・容易になる多種多量のデータ」と説明されています。

[ii] 「Relational DataBase Management System」の略。多くの場合、行と列から構成される表（テーブル）の構造でデータを扱い、データベース言語として SQL が使用されます。

[iii] 一般的には「Not only SQL」の略とされています。

[iv] 「MongoDB に対する探索行為の増加について」（平成 27 年2月 20 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20150220.pdf

さらに、MongoDB データベースの情報収集を試みる問い合わせを行っている発信元 IP アドレスについて調査を実施したところ、その多くは、インターネットセキュリティの向上を目的として、攻撃を受ける可能性があるサービスが稼動している IP アドレスの探索等の活動を実施している非営利組織（以下「非営利組織A」といいます。）や、あらゆるサービスに対して探索を実施して結果を蓄積するとともに、同結果の検索サービスを提供するサイト（以下「検索サイトB」といいます。）が管理すると考えられる IP アドレスからのアクセスでした。また、ドイツのザールランド大学が管理する IP アドレスからのアクセスも確認できました。しかしながら、クラウドコンピューティングサービス等を利用してアクセスを試みており、その背景や目的が判明しないアクセスも観測しています（図2）。このことから、データの窃取等を目的としてアクセスを実施している者が存在する可能性も十分に考えられるため、注意が必要です。

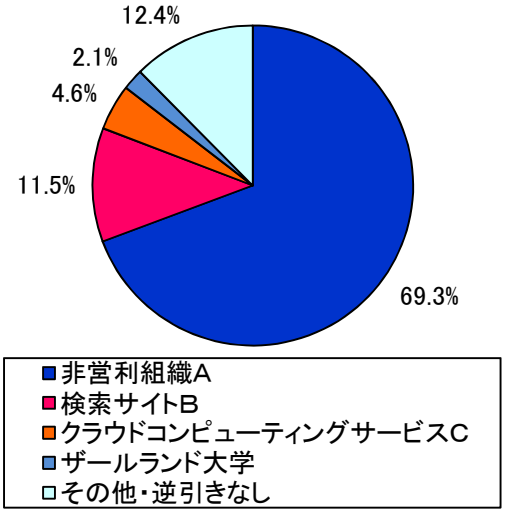

図2　発信元 IP アドレスの DNS 逆引き結果別の MongoDB 問い合わせ件数割合（H27.1.1～3.28）

2　その他の NoSQL データベースに対する探索行為について

「NoSQL」に分類される代表的なデータベース管理システムが初期値として使用するポートに対するアクセスの観測状況を調査したところ、Redis[i]で使用される 6379/TCP 及び memcached[i] で使用される 11211/TCP に対するアクセスにおいて、1月中旬から発信元 IP 数が高い水準で推移していることを確認しました（図3、4）。

[i] いずれも、メモリ上に Key-Value データストア（値とそれを識別するためのキーのペアといった単純な構造でデータを扱うデータベースの方式）を構築することができるデータベース管理システム。

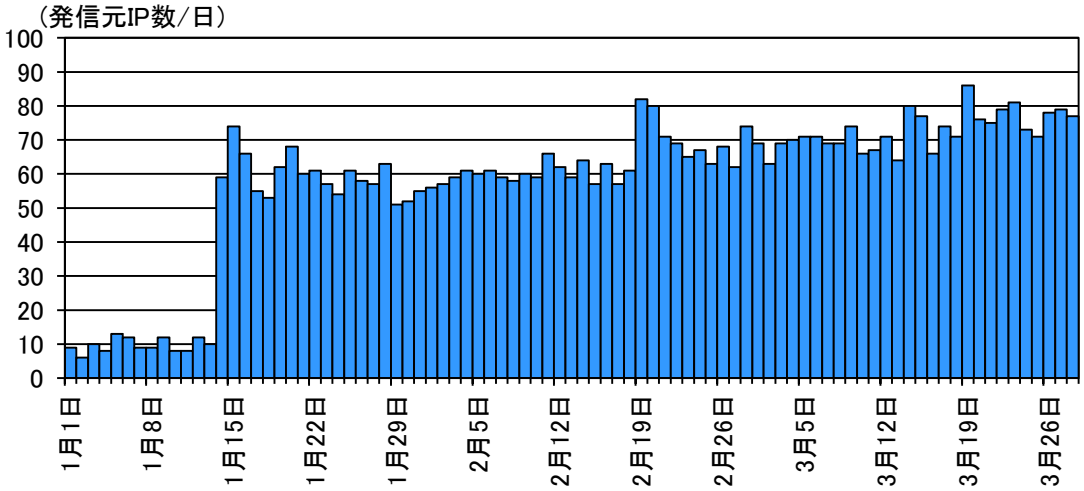

図3　宛先ポート 6379/TCP に対するアクセスの発信元 IP アドレス数の推移（H27.1.1～3.28）

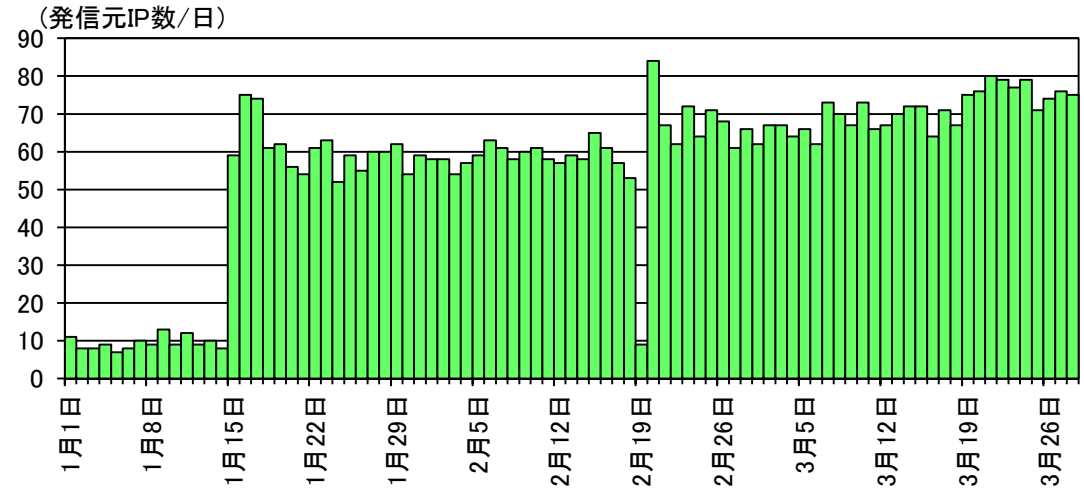

図4　宛先ポート 11211/TCP に対するアクセスの発信元 IP アドレス数の推移（H27.1.1～3.28）

また、これらのデータベースについても、実際に情報収集を試みる問い合わせを継続して観測しています（図5）。同アクセスの大多数は非営利組織A、検索サイトB及びザールランド大学が管理すると考えられる IP アドレスを発信元とするものでした。しかしながら、その背景や目的が判明しないアクセスも少数ながら観測していることから、これらのデータベースの管理においても細心の注意を払う必要があります。

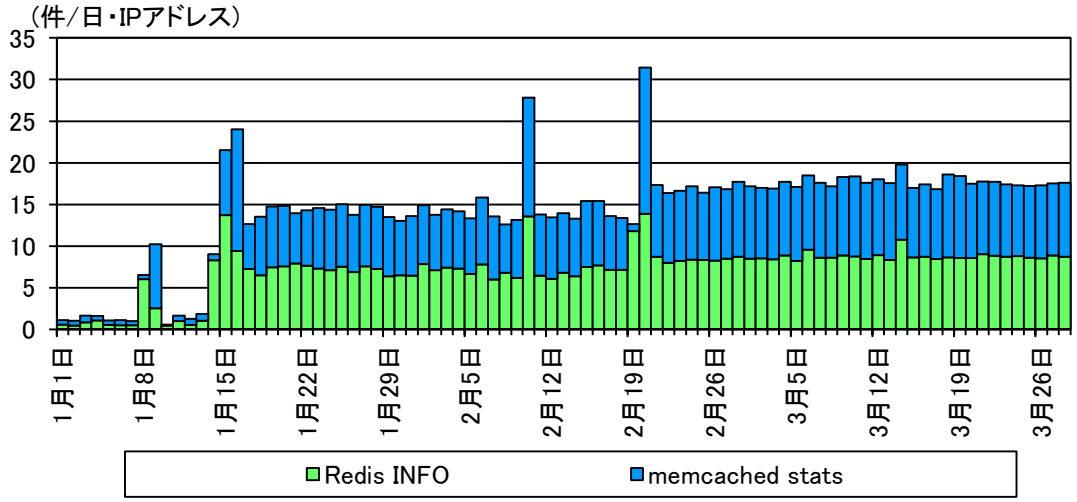

図5　Redis 及び memcached に対する問い合わせ内容別アクセス件数の推移（H27.1.1～3.28）

3　推奨する対策

再掲となりますが、これらのデータベース管理システムを使用している企業や組織においては、以下の対策を早急に実施することを推奨します。

(1) 外部からのアクセスを制限する。

インターネット経由で外部のコンピュータがデータベースにアクセスする必要がない場合には、外部ネットワークからのアクセスを制限する、もしくはローカルホストのみで運用を行う等の設定変更してください。

(2) 適切な認証を実施する。

他のコンピュータからのアクセスを許可する必要がある場合には、適切な認証を実施するようにしてください。また、認証情報等の窃取を防止するため、通信の暗号化も検討してください。