平成 27 年 2 月 20 日

Topic

MongoDB に対する探索行為の増加について

インターネット上に不用意に公開されている MongoDB を探索する目的と考えられるアクセスが増加しています。MongoDB 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 インターネット上に不用意に公開されている MongoDB について

MongoDB は米国 MongoDB 社によって開発され、オープンソースで公開されているデータベースソフトウェアです。

2月 10 日、ドイツのザールランド大学のグループが、インターネット経由で外部から認証を必要とせずにアクセスすることができる MongoDB データベースを約 4 万件確認したとの研究結果を公表[i]しました。同研究結果では、実際に膨大な顧客情報が外部から参照可能となっていたデータベースも存在したと指摘しています。また、日本国内の IP アドレスにおいても、外部から参照可能なデータベースが確認されていることが報告されています。

なお、同グループは本件について MongoDB 社に責任があるものではなく、利用者の不適切な設定に原因があるとしています。

2 MongoDB の探索行為と考えられるアクセスの増加について

MongoDB は初期設定では 27017/TCP ポートを使用します。警察庁の定点観測システムにおいても、宛先ポートを 27017/TCP とするアクセスの発信元 IP アドレス数が、2月 13 日から大きく増加しています（図1）。

また、アクセスの内容に着目すると、2月 12 日までは単にポートの開放状況を確認するポートスキャン行為が大多数を占めており、同一発信元 IP アドレスから他の複数のポートに対してもポートスキャン行為が行われていることが確認できました。

[i] https://cispa.saarland/index.html%3Fp=3068.html

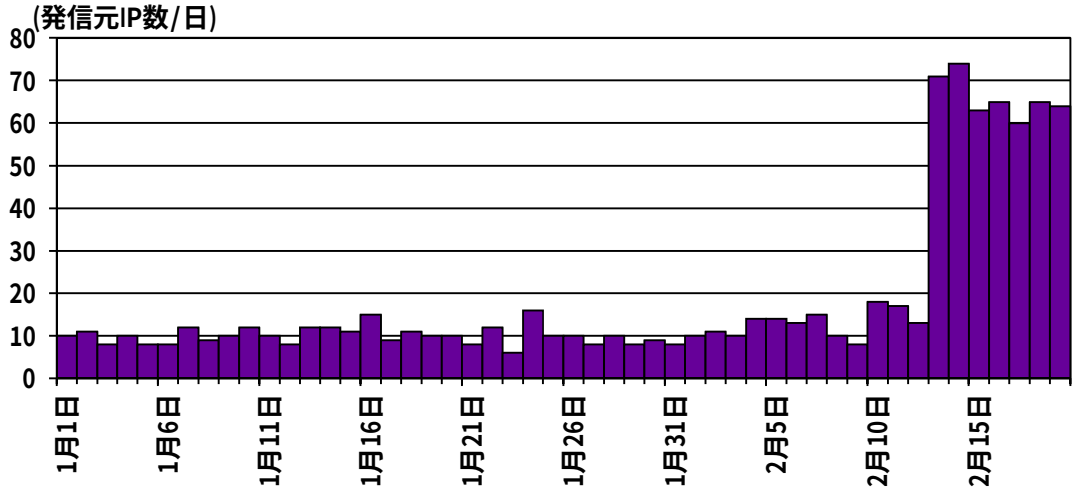

図1　宛先ポート 27017/TCP に対するアクセスの発信元 IP アドレス数の推移
（H27.1.1～2.19）

しかしながら、2月 13 日以降には、単なるポートスキャン行為だけではなく、実際に MongoDB データベースの情報収集を試みる問い合わせを継続して多数観測しています（図2）。

なお、2月6日に観測されたアクセスの多くは、ザールランド大学が管理する IP アドレスを発信元とするものでした。

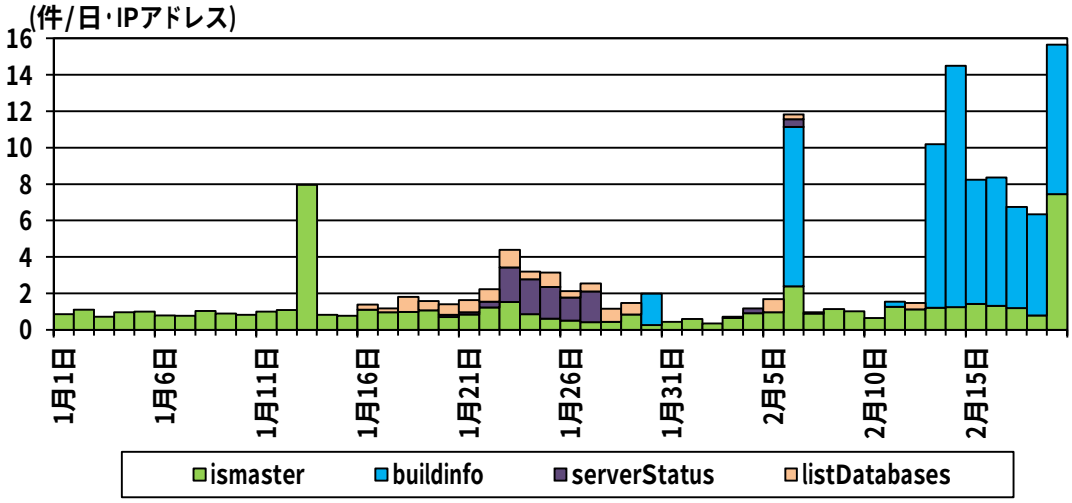

図2　MongoDB に対する問い合わせ内容別アクセス件数の推移（H27.1.1～2.19）

3 推奨する対策

MongoDB を利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。

また、MongoDB 社も研究結果の公表を受けて、利用者が実施するべきセキュリティ対策を公表[i]していますので、併せて確認してください。

(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 MongoDB 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。

[i] http://www.mongodb.com/blog/post/mongodb-security-best-practices