平成 29 年2月 17 日

「ビッグデータ」等の蓄積及び分析に使用される複数のソフトウェアに対する探索行為の急増等について
（平成 29 年1月期）

- 「ビッグデータ」等の蓄積及び分析に使用される複数のソフトウェアに対する探索行為が急増
- 「Apache Commons Collections」ライブラリに起因する「OpenNMS」の脆弱性を標的としたアクセスを観測

1 「ビッグデータ」等の蓄積及び分析に使用される複数のソフトウェアに対する探索行為が急増

近年、技術の発展に伴い多種多量のデータが蓄積及び分析可能となったことから、この様なデータが「ビッグデータ」と呼称されて、注目を集めています。さらにビッグデータ等の蓄積及び分析のために、既存のソフトウェアでは実現できない性能や特性を持つソフトウェアの開発及び利活用が進んでいます。これまでも警察庁では、ビッグデータ等に利用されており、「NoSQL」[i]と総称される新しいデータベース管理システムに対する探索行為について注意喚起を実施[ii]してきました。

警察庁のインターネット定点観測システムにおいては、NoSQL データベースの1種であるMongoDB に対する探索行為を平成 27 年2月から継続して観測していましたが、29 年1月1日以降に探索行為の急増がみられました（図1）。これまで、MongoDB に対する探索行為の大多数は、以下の組織を発信元[iii]とするものでした。

- 非営利組織A

  攻撃を受ける可能性があるサービス等が稼動している IP アドレスの探索等の活動を、インターネットセキュリティの向上を目的として実施している非営利組織です。探索結果は当該 IP アドレス帯域の管理者等に限定して公開されています。

- 検索サイトB

  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です。同サイトでは、探索の結果を誰もが検索可能であるため、以前から攻撃に悪用される可能性も指摘されています。

---

[i] 一般的には「Not only SQL」の略とされています。

[ii] 「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/topics/?seq=15480
「「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」（平成 27 年3月 30 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=15905
「インターネット観測結果等（平成 27 年上半期（1月～6月））」（平成 27 年9月 17 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=16886

[iii] 発信元組織は発信元 IP アドレスの DNS 逆引き結果に基づいています。

しかしながら、1月1日以降に急増した探索行為は、これらの組織を発信元としたものではなく、探索を実施している者の背景や目的ははっきりとしていません（図2）。

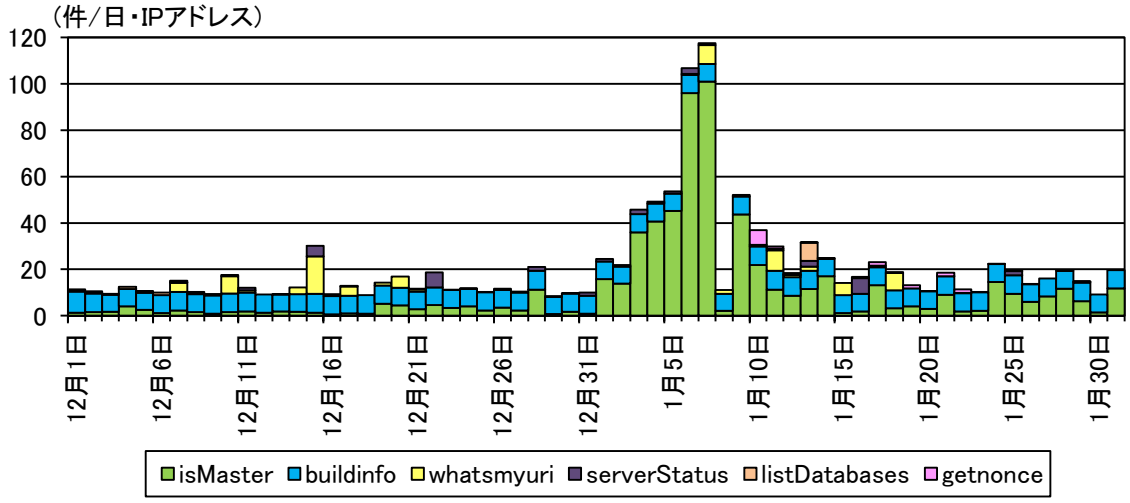

図1　宛先ポート27017/TCPに対するMongoDBの探索行為の問い合わせ内容別のアクセス件数の推移（H28.12.1～H29.1.31）

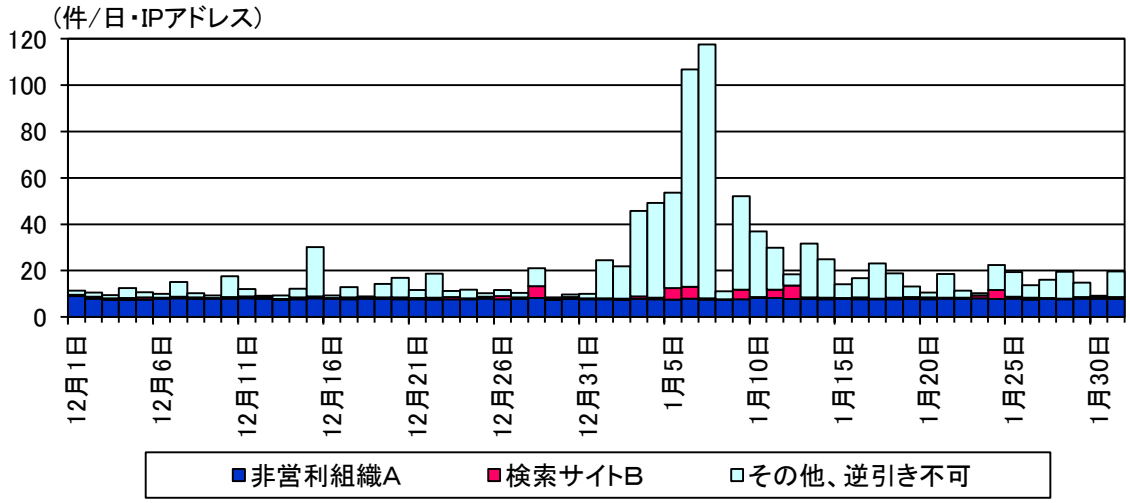

図2　宛先ポート27017/TCPに対するMongoDBの探索行為の発信元組織別のアクセス件数の推移（H28.12.1～H29.1.31）

また12月から1月にかけてはMongoDBに留まらず、11月以前にはほとんど観測されていなかった以下のソフトウェアに対する探索行為も観測しました。

- Apache CouchDB（以下「CouchDB」という。）
  MongoDBと同様にNoSQLデータベースに分類されるデータベース管理システムです。12月下旬から探索行為を観測したとともに、1月下旬からは探索に使用される問い合わせ内容にも変化がみられました(図3)。

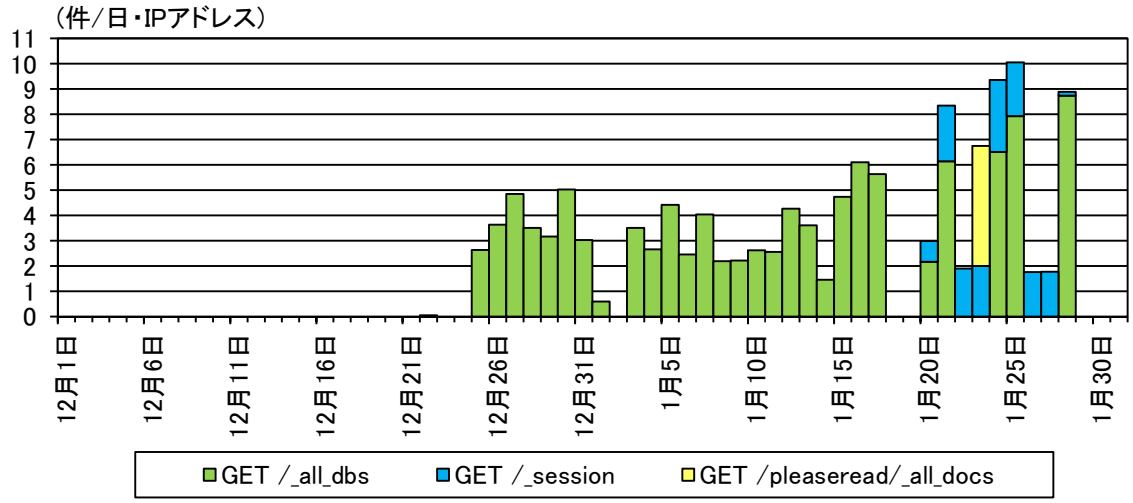

図3　宛先ポート 5984/TCP に対する CouchDB の探索行為の問い合わせ内容別のアクセス件数の推移（H28.12.1～H29.1.31）

- Elasticsearch

  データを蓄積するとともに、蓄積したデータから目的のものを検索する全文検索の機能を提供するソフトウェアです。1月中旬から断続的に探索行為を観測しました（図4）。

  Elasticsearch については、これらの探索行為以外にも、平成 27 年2月に明らかとなっている脆弱性を標的としたアクセス[i]も引き続き観測していることから、注意が必要です。

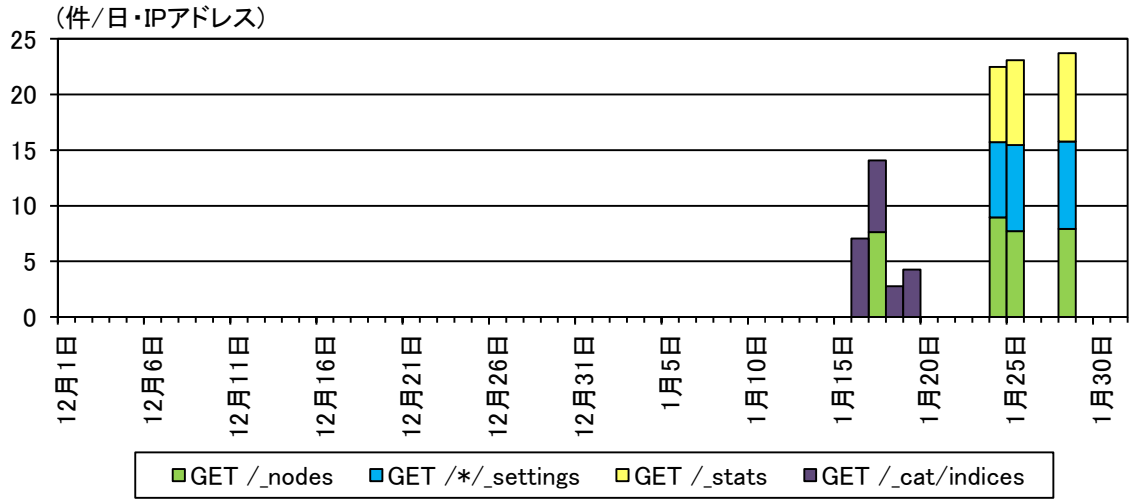

図4　宛先ポート 9200/TCP に対する Elasticsearch の探索行為の問い合わせ内容別のアクセス件数の推移（H28.12.1～H29.1.31）

[i] 「Elasticsearch の脆弱性を標的としたアクセスの観測について」（平成 27 年3月 16 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=15728

- Apache Hadoop（以下「Hadoop」という。）

  データの分散処理を行うためのソフトウェア群です。Hadoop を構成するソフトウェアの1つとして、独自の分散ファイルシステムである HDFS（Hadoop Distributed File System）が存在します。件数は多くないものの1月 18 日に、HDFS に対する探索行為を観測[i]しました。

なお、12 月から1月に観測した CouchDB、Elasticsearch 及び Hadoop に対する探索行為の発信元には非営利組織Aや検索サイトBは含まれていませんでした。このため、これらのアクセスについても探索を実施している者の背景や目的ははっきりとしていません。

12 月下旬から1月にかけては、インターネット上に不用意に公開されており、認証不要で誰もがアクセス可能となっていた MongoDB、CouchDB、Elasticsearch 及び Hadoop において、攻撃者によりデータが消去される事案の報告[ii]が相次ぎました。これらの事案の中には、消去したデータのバックアップを攻撃者が保持しておりデータを取り戻すことが可能であるため、身代金を支払うように要求するメッセージが残されていたものも存在したとされています。

警察庁において観測したアクセスと、データ消去事案の直接の関連性は不明です。しかしながら、データを消去する攻撃を実施した者又は同攻撃の模倣を企図した者が、これらのアクセスを実施した可能性も考えられます。このため、一部再掲となりますが、MongoDB、CouchDB、Elasticsearch、Hadoop 及びこれらと同種のソフトウェアを利用している管理者等は、以下の対策を実施することを推奨します。また、各ソフトウェアの開発元からも、データ消去事案の多発を受けて、推奨する対策等が公表[iii]されていますので参考としてください。

- 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から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したり、ローカルホストのみで運用してください。インターネット経由でアクセスする必要がある場合にも、特定の IP アドレスのみにアクセスを許可したり、VPN を用

---

[i] 観測した探索行為は、宛先ポート 50070/TCP に対して「GET /webhdfs/v1/?op=LISTSTATUS」を問い合わせるものでした。

[ii] https://twitter.com/0xDUDE/status/813865069218037760
https://twitter.com/nmerrigan/status/819502435978870785
https://twitter.com/0xDUDE/status/820189787239960576
https://twitter.com/nmerrigan/status/822016754490765312
「GDI.Foundation treft eerste ransomware op Elasticsearch aan」
http://www.gdi.foundation/single-post/2017/01/13/GDIFoundation-treft-eerste-ransomware-op-Elasticsearch-aan
「Ransom attack on Elasticsearch cluster?」
https://discuss.elastic.co/t/ransom-attack-on-elasticsearch-cluster/71310
「Revenge of the DevOps Gangster: Open Hadoop Installs Wiped Worldwide」
http://www.threatgeek.com/2017/01/open-hadoop-installs-wiped-worldwide.html

[iii] 「How to Avoid a Malicious Attack That Ransoms Your Data」
https://www.mongodb.com/blog/post/how-to-avoid-a-malicious-attack-that-ransoms-your-data
「CouchDB Ransom Notes」
https://blog.couchdb.org/2017/01/24/couchdb-ransom-notes/
「ランサム攻撃からデータを守るには」
https://www.elastic.co/jp/blog/protecting-against-attacks-that-hold-your-data-for-ransom

いて接続することを検討してください。

- 適切な認証を実施する。
  外部からのアクセスを許可する必要がある場合には、適切な認証を実施してください。ユーザ名とパスワードによる認証を実施する場合には、推測されにくいものを使用してください。
- データのバックアップを取得する。
  万が一、攻撃者にデータを消去されても、バックアップを取得していればデータを回復することが可能です。適切なバックアップを取得してください。
- データの暗号化を実施する。
  データを消去する前にバックアップを取得した旨の攻撃者の主張が正しいとは限りませんが、その様な行為があった場合には、保存されていたデータが外部に流出している可能性があります。意図しないデータの流出を防止するため、データの暗号化を検討してください。
- ソフトウェアのバージョンアップを適切に実施し、最新の状態に保つ。
  データ消去事案と直接の関連はありませんが、今後ソフトウェアに脆弱性が明らかとなった場合には、インターネット上からアクセス可能なサーバは、脆弱性を悪用する攻撃に直接晒される可能性があります。ソフトウェアを常に最新の状態に保ってください。

２ 「Apache Commons Collections」ライブラリに起因する「OpenNMS」の脆弱性を標的としたアクセスを観測

平成 27 年 11 月６日に、研究者グループから Java 言語のライブラリのひとつである「Apache Commons Collections」に起因して同ライブラリを使用する複数のソフトウェア群に存在する脆弱性の詳細と具体的な検証コードが公開されました。同脆弱性が悪用された場合、遠隔から任意のコードが実行可能であるとされています。この問題が明らかとなった直後に、脆弱性が明らかとなったソフトウェアのひとつである「WebLogic Server」の脆弱性探索が目的と考えられるアクセスを警察庁のインターネット定点観測システムにおいて観測したことから、注意喚起を実施[i]しました。

さらに平成 29 年1月 10 日からは、同脆弱性の影響を受けることが明らかとなっているオープンソースのネットワーク監視ツールである「OpenNMS」に存在する同脆弱性を標的としていると考えられる宛先ポート 1099/TCP に対するアクセスを継続して観測しています（図5）。

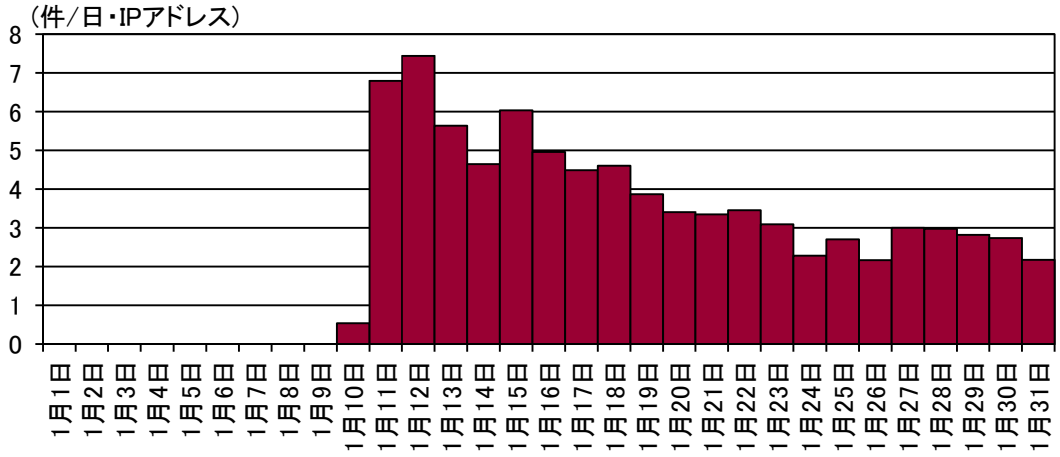

図5 宛先ポート 1099/TCP に対する「Apache Commons Collections」ライブラリに起因する「OpenNMS」の脆弱性を標的としたアクセス件数の推移

警察庁では、平成 27 年に公表された同脆弱性の検証コードを基に作成されたと考えられる OpenNMS を標的とした複数の攻撃ツールが、平成 28 年2月以降、インターネット上に公開されていることを確認しています。今回観測したアクセスは、これら攻撃ツールにおいて設定されているリクエストの内容と酷似していました。また、同アクセスで実行を試みられているコマンドは、OpenNMS が稼動しているサーバにおいて外部からファイルをダウンロードするものでした（図6）。ここで、ダウンロードが試みられているファイルは、Linux 上で動作する実行ファイルであったことから、何らかの不正プログラムであると考えられます。

[i] 「「WebLogic Server」の脆弱性探索が目的と考えられるアクセスの観測について」（平成 27 年 11 月 15 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=17214

図6　観測したアクセスに含まれていたコマンドの内容（一部をマスキング）

今回観測したアクセスは、外部からファイルのダウンロードを試みるものであり、他のコマンドについては確認できませんでした。しかしながら、当該アクセスにより、不正プログラムのダウンロードが成功したサーバでは、引き続き同ファイルが実行され、不正プログラムに感染させられるものと考えられます。

OpenNMS の開発元の情報[i]によると、平成 27 年 12 月には、同脆弱性の対策がなされた Apache Commons Collections ライブラリを導入した OpenNMS のバージョン「17.0.0」が公開されており、同バージョン以降を使用している場合、今回観測したアクセスによる影響は受けないものと考えられます。しかし、Apache Commons Collections ライブラリの開発元は、認証を受けておらず信頼できない相手から送られたデータを処理することは避けるべきであり、加えて、攻撃に悪用可能なクラスは他にも存在する可能性があることから、同ライブラリを対策版に置き換えるだけではこの脆弱性の完全な対策とはならないとしています[ii]。

OpenNMS を含め、同ライブラリを使用するその他のソフトウェア群において、今後、同様の脆弱性が明らかとなる可能性も考えられます。また、Apache Commons Collections ライブラリを使用していない製品にも、同様の脆弱性が存在することが明らかとなっています。これらのことから、当該脆弱性に関する対策のみならず、一般的にソフトウェアを利用する場合には、以下の対策を実施することを推奨します。

- 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から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したり、ローカルホストのみで運用してください。インターネット経由でアクセスする必要がある場合にも、特定の IP アドレスのみにアクセスを許可したり、VPN を用いて接続することを検討してください。
- 適切な認証を実施する。
  外部からのアクセスを許可する必要がある場合には、適切な認証を実施してください。ユーザ名とパスワードによる認証を実施する場合には、推測されにくいものを使用してください。
- ソフトウェアのバージョンアップを適切に実施し、最新の状態に保つ。
  インターネット上からアクセス可能なサーバは、脆弱性を悪用する攻撃に直接晒される可能性があります。ソフトウェアを常に最新の状態に保ってください。

---

[i] http://docs.opennms.org/opennms/releases/latest/releasenotes/#releasenotes-changelog-17.0.0

[ii] 「Apache Commons statement to widespread Java object de-serialisation vulnerability」
https://blogs.apache.org/foundation/entry/apache_commons_statement_to_widespread

また、Apache Commons Collections ライブラリを利用して Java 言語で開発した独自のソフトウェアを使用している場合には、個別の対応が必要となります。同ライブラリに起因する脆弱性については、JVN に掲載されている情報[i]も参考としてください。加えて、独自にソフトウェアを開発する場合も、同様の脆弱性を発生させないためにセキュリティに留意する必要[ii]があります。

[i] 「Apache Commons Collections ライブラリのデシリアライズ処理に脆弱性」
http://jvn.jp/vu/JVNVU94276522/
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-005930.html

[ii] 詳細については「Java セキュアコーディングスタンダード CERT/Oracle 版」の「13. シリアライズ (SER)」を参照してください。
https://www.jpcert.or.jp/java-rules/#c13