ANYでアップデート
-- 2009年7月のBIND 9の脆弱性 --

民田雅人　白井出
株式会社日本レジストリサービス
2009-09-04
dnsops.jp BoF@品川

それは何故か7月にやってくる

- 7月29日未明(日本時間)
  以下のリリースやアナウンス
  - BIND 9.6.1-P1
  - BIND 9.5.1-P3
  - BIND 9.4.3-P3
  - US-CERT　http://www.kb.cert.org/vuls/id/725188
  - ISC　https://www.isc.org/node/474

この日朝からメールも読まずに仕事をしていた
ため、声をかけられて初めて知った
良くも悪くもBoFネタには困らない日々

脆弱性情報の内容

- ISCのアナウンスより
  - Versions affected: BIND 9 (all versions)
  - Severity: High
  - Exploitable: remotely
  - **Urgent:** this exploit is public. Please upgrade immediately.
  - Workarounds: None.
  - Active exploits: An active remote exploit is in wide circulation at this time.

どっひゃ～！

今回の脆弱性のまとめ

- 該当するのは未対策バージョンで、マスターゾーンを設定してある場合
  - スレーブゾーンは問題ない
  - BIND 9に組込みのゾーンも問題ない
- キャッシュ専用の設定でも、localhostとその逆引きゾーン(0.0.127.in-addr.arpa)を持っている場合が多い
  ⇒ 対象は権威サーバに限らない

どういう問題?

- ゾーンのマスターに対して、ダイナミックアップデートでTYPE ANYを送ると発生する
  - アップデート時のANYの扱いに問題がある
- ANY
  - RFC1035で、**問い合わせに使う**TYPEとして定義
  - レコードを設定するものではない
    ⇒ ダイナミックアップデートはレコードを設定する

    注)　RFCにはUPDATE時のANYの扱いについてについて細かい記述あり

攻撃ツールを試してみる

- すぐに見つかって、簡単に試せます
  - BIND 9がコロコロ落ちます・落とせます
- そのままだと調査に不便
  - 自分で使いやすいように改造しました
  - 使いやすくって?

ということで実演!

実演:「BINDコロリ」

nsupdateコマンドでも攻撃可？

- もしnsupdateで攻撃できるなら、標準ツールでコマンドラインから攻撃できることになり極めて危険

- 結論：nsupdateではTYPE ANYは送れない
  - ソースを確認すると、送る前にDNSレコードとして正しいかどうかをチェックし、TYPE ANYはエラー

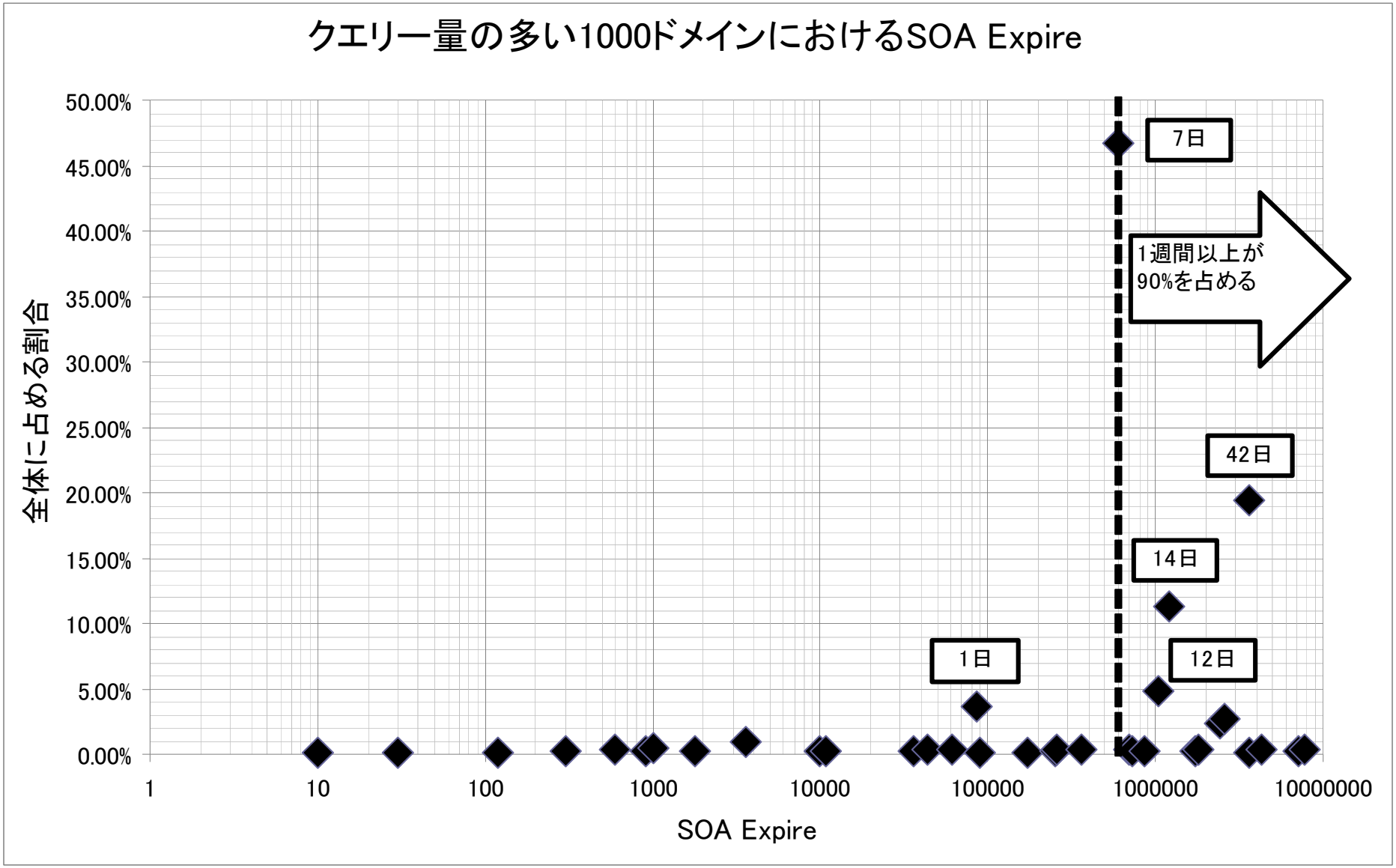
マスターサーバがキケーン

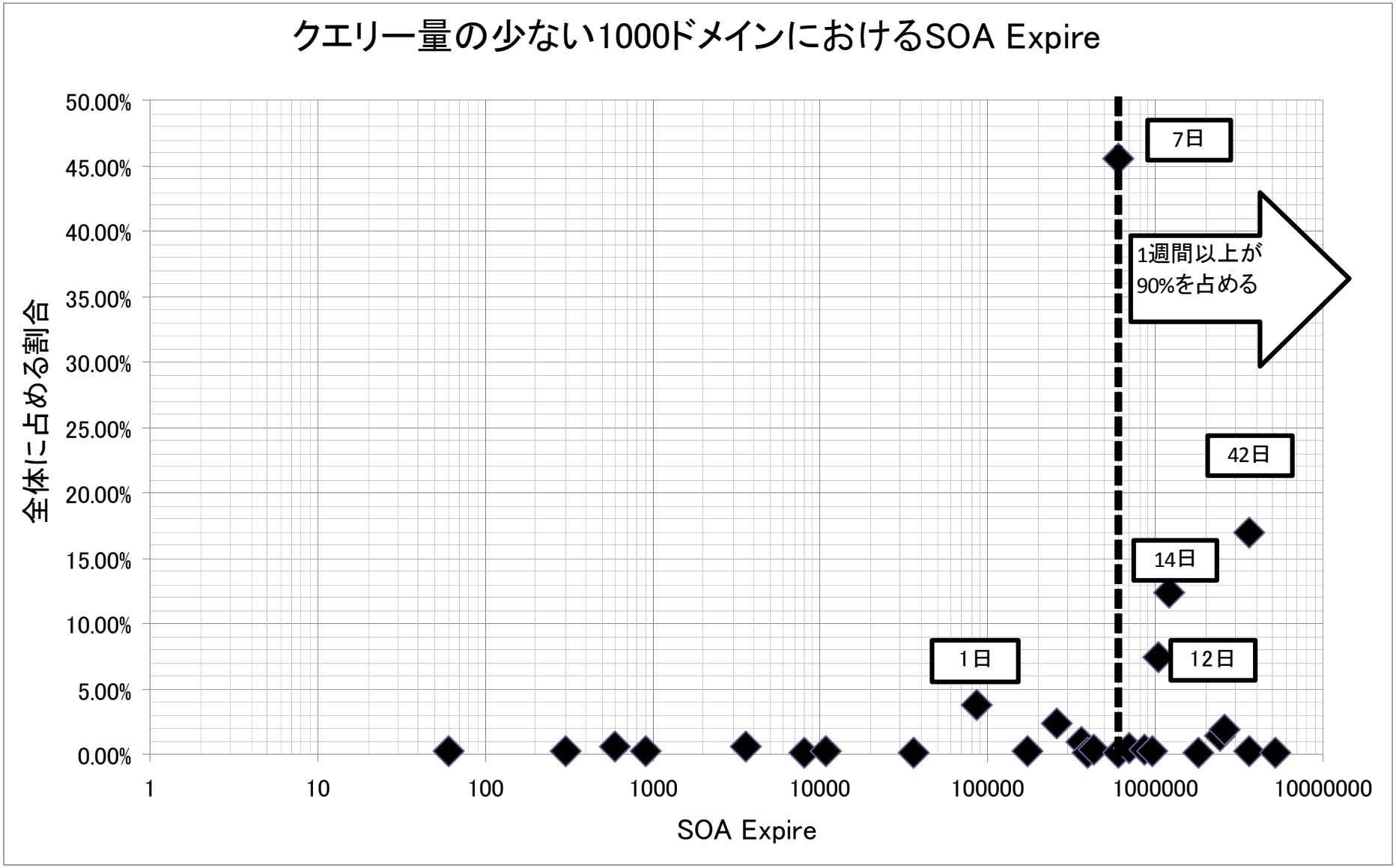
- ということは…

  マスターが落とされても、(スレーブのおかげで)気づかないところがあるのでは?
- 1週間ぐらいしたら大騒ぎになっていたりして
  - ゾーンのexpireの設定は1週間が多いんじゃ？

    本当?

ゾーンがexpireするまでの時間ってどうなの?
SOAのexpireを調べてみよう!





ところで Workarounds: None. ってどういうこと？

- そもそもダイナミックアップデートは、許可したところから受け付けるものじゃないの？
  - アクセスコントロールが効かないって一体??

よし、ソースを追っかけてみよう！

今回の対策パッチ

- bin/named/update.cのtemp_check()内
  - temp_check()は対象RRsetの有無などを調べる
  - パッチ行の後でdns_db_findrdataset() を呼ぶ
- lib/dns/db.cのdns_db_findrdataset()で、TYPEとしてANYが来たらassert()で終了
  - つまり対策パッチはTYPE ANYをdns_db_findrdataset()に渡さなくする

temp_check()を呼ぶ前後はどうなっているの？

UPDATE処理の振る舞い

- bin/named/update.cのupdate_action()内でtemp_check()を呼んでいる
- その数行後でcheckupdateacl()を呼び出す
  - つまりアクセスコントロールチェックが後！
- ん？その前にこんなコメントが

```
/* Check Requestor's Permissions.
 * It seems a bit silly to do this only after
 * prerequisite testing, but that is what
 * RFC2136 says.
 */
```

超訳: 要求が正当かチェックしてるんだが、この順番変でしょ。でもRFC2136にそう書いてあるんだよ。

え゛～RFC2136なの？

- RFC2136 - Dynamic Updates in the Domain Name System (DNS UPDATE)
  - セクション3にサーバのダイナミックアップデートの処理を、処理順に記述 (以下は見出しを引用)
    3 - Server Behavior
    3.1 - Process Zone Section
    3.2 - Process Prerequisite Section ← temp_check()
    3.3 - Check Requestor‘s Permissions
    3.4 - Process Update Section

さすがBIND 9、RFCに忠実ですね～(棒読み)

まとめ

- 今回の脆弱性は、BIND 9が産声を上げたときからソースに記述してあったもの
  - 例えBIND 9.0.0であっても、同様の攻撃が可能
- SOAのexpireは1週間が最も多く、それ以上も多いが、中には極端に短いものも存在する
  - 短すぎて問題になったりしてないの?
- BIND 9はRFCに忠実すぎて困ることもある

おしまい

JAPAN REGISTRY SERVICES