DNS Summer Day 2020

NXNSAttackの水平展開

株式会社XACK

技術部

髙橋　平準

発表内容

- 会社・製品紹介　　1～2分程度
- NXNSAttackの説明　　5～6分程度
- NX○○Attack?　　7～8分程度

- スポンサー枠として発表の場を頂いていますので製品紹介をメインとすべきだとは思うのですが、DNSの話をしたいのでその辺りは簡単に済ませます。

会社・製品紹介

株式会社XACK　会社紹介

主な業務

- ネットワークアプリケーションシステム全般に関するソフトウェア開発

こんな製品を作っています。

製品名	概要
XACK RADIUS	大規模システム向け高性能RADIUSサーバー
XACK DHCP	DHCPv4/v6両対応高性能DHCPサーバー (GUI対応)
XACK DNS	通信事業者向けセキュアDNSサーバー (GUI対応)
XACK DNS Zone Editor	マルチテナント編集システム (GUI)
XACK EAP Tester	RADIUSクライアントシミュレーター

XACK DNS 製品紹介

XACK DNSの特徴

- フルスクラッチ開発の国産DNSサーバー
- マスター/スレーブ権威機能・フルリゾルバー機能・フォワーダー機能・etc…
- モジュール化による機能の足し引きが可能
  - 例えばマスター権威機能→フォワーダー機能と組み合わせることで、自身が管理するゾーンについては権威ある応答を、そうでないゾーンについてはどこかに転送を、等
- 仮想サーバー機能
  - 1つのインスタンスで複数のサーバーが動作しているかのように振舞うことが可能
- 通信事業者様や企業・大学様での採用実績あり

NXNSAttackとは

NXNSAttackとは

- フルリゾルバーと権威サーバーを同時に攻撃できるお得な手法
  - メインのターゲットは権威サーバー？
- 狙った権威サーバーに向けた、存在しない名前のNSレコード(NXNS)を大量に付与した委任応答を返すことで、フルリゾルバーと権威サーバーとの間に多くのやり取りを発生させるという攻撃
  - RFC通りに真面目に名前解決を行おうとしたら加害者になってしまう
  - DNSプロトコルの穴を突いたようなもので、結構な数の実装がこの脆弱性を踏みました
    - XACK DNS
    - BIND
    - Unbound
    - PowerDNS Recursor
    - Knot Resolver
- 次ページ以降で図解
  - 尚、説明の都合で権威サーバーのアドレス解決時に問い合わせるのは
    Aレコードのみ（AAAAレコードを解決しない）とします。

NXNSAttackとは

攻撃者

NXNSAttackとは

攻撃者が用意した
権威サーバー

NXNSAttackとは

今回の被害者

NXNSAttackとは

攻撃に利用されてしまう
フルリゾルバー

NXNSAttackとは

example.com

xack.jp

NXNSAttackとは

設定

sub.example.com. NS sub001.xack.jp.
sub.example.com. NS sub002.xack.jp.
sub.example.com. NS sub003.xack.jp.
...
sub.example.com. NS subXXX.xack.jp.

example.com

xack.jp

NXNSAttackとは

設定

“sub.example.com.” は
“sub001.xack.jp.” と
“sub002.xack.jp.” と
“sub003.xack.jp.” と
…
“subXXX.xack.jp.” に委任しています！

example.com

xack.jp

NXNSAttackとは

QNAME=“001.sub.example.com.” QTYPE=“A”

クエリー送信

“sub.example.com.” は
“sub001.xack.jp.” と
“sub002.xack.jp.” と
“sub003.xack.jp.” と
…
“subXXX.xack.jp.” に委任しています！

example.com

xack.jp

NXNSAttackとは

“001.sub.example.com.”のAレコードを教えて！

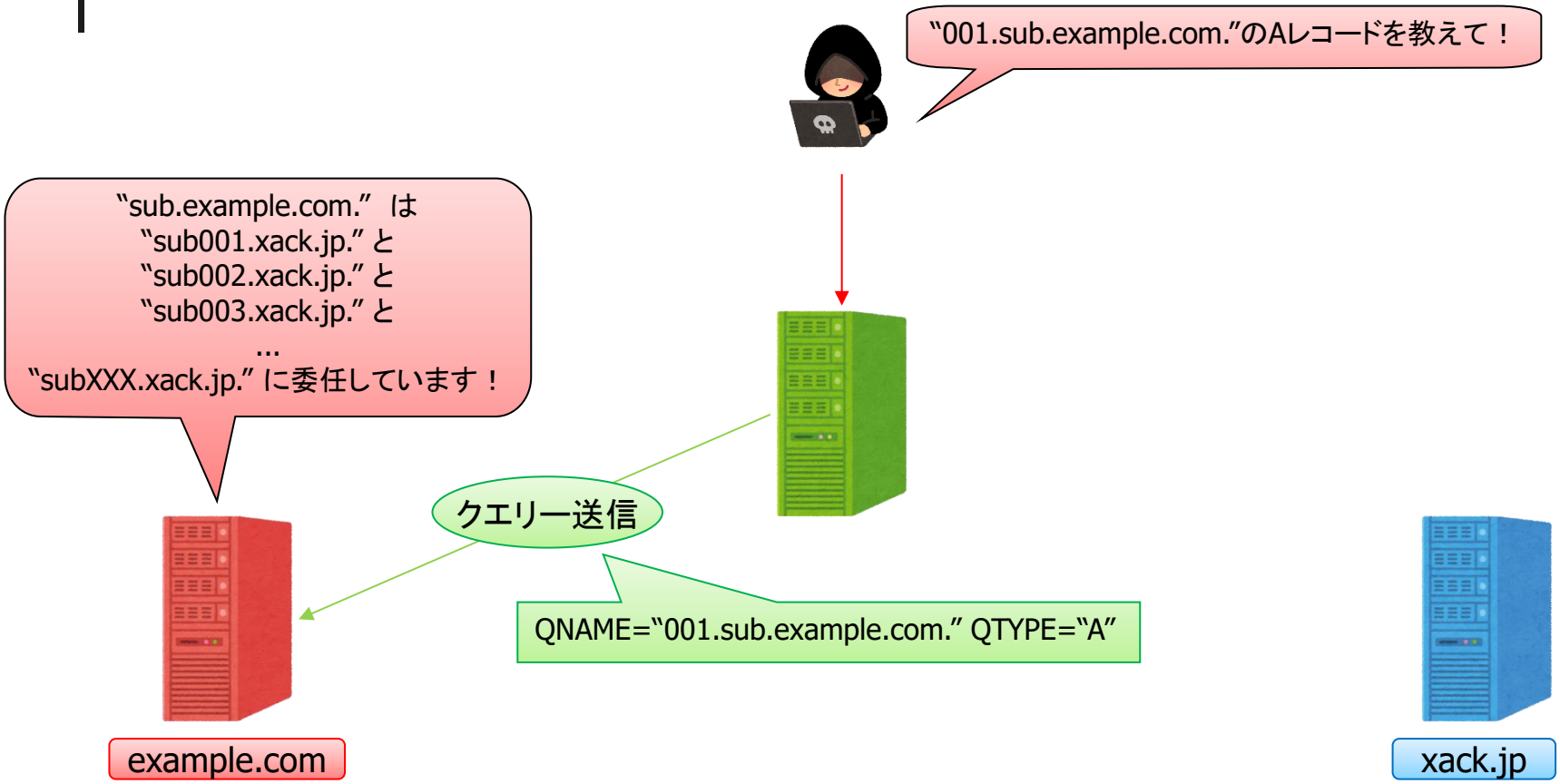
クエリー送信

“sub.example.com.” は
“sub001.xack.jp.” と
“sub002.xack.jp.” と
“sub003.xack.jp.” と
…
“subXXX.xack.jp.” に委任しています！

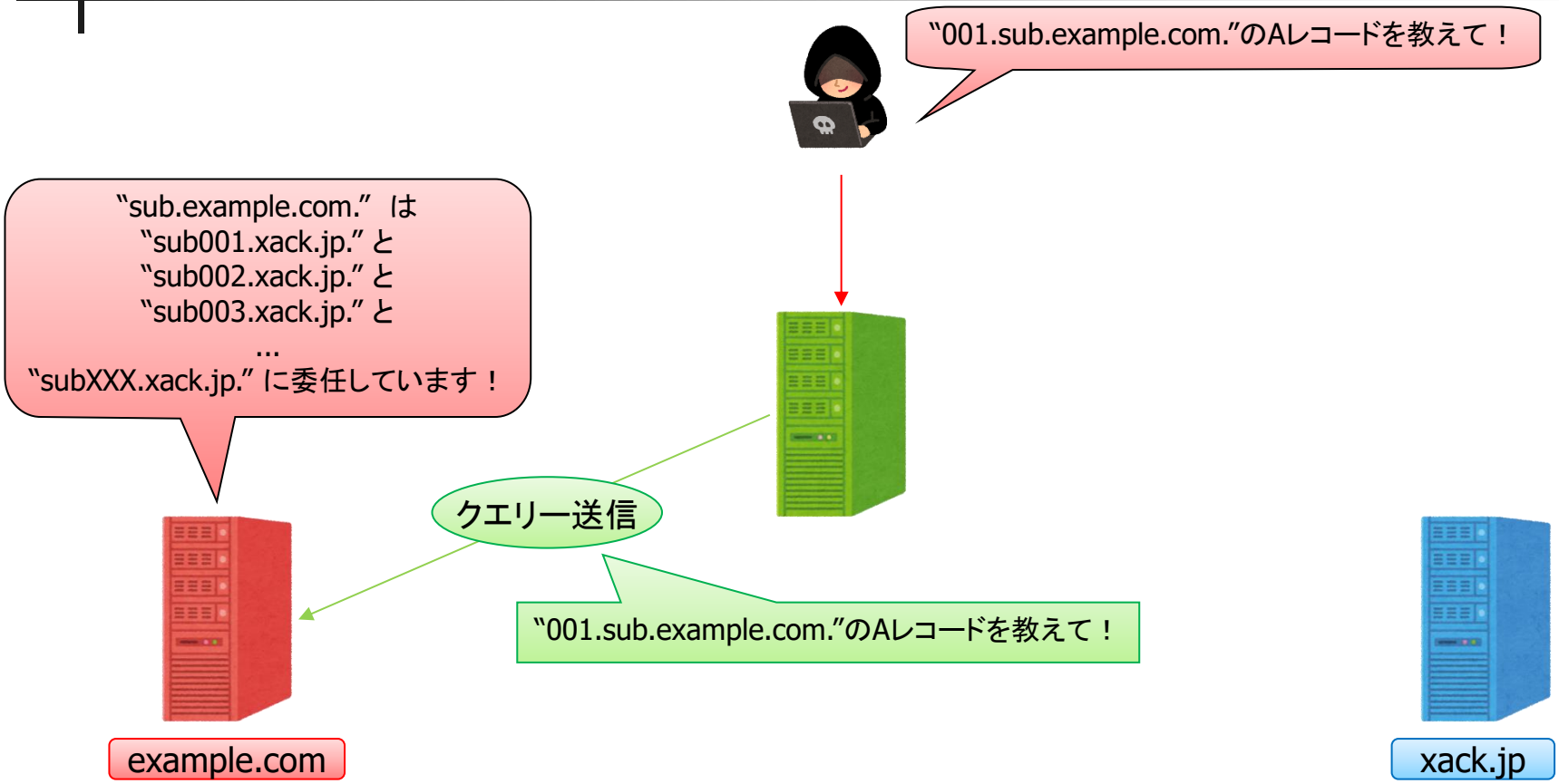
example.com

xack.jp

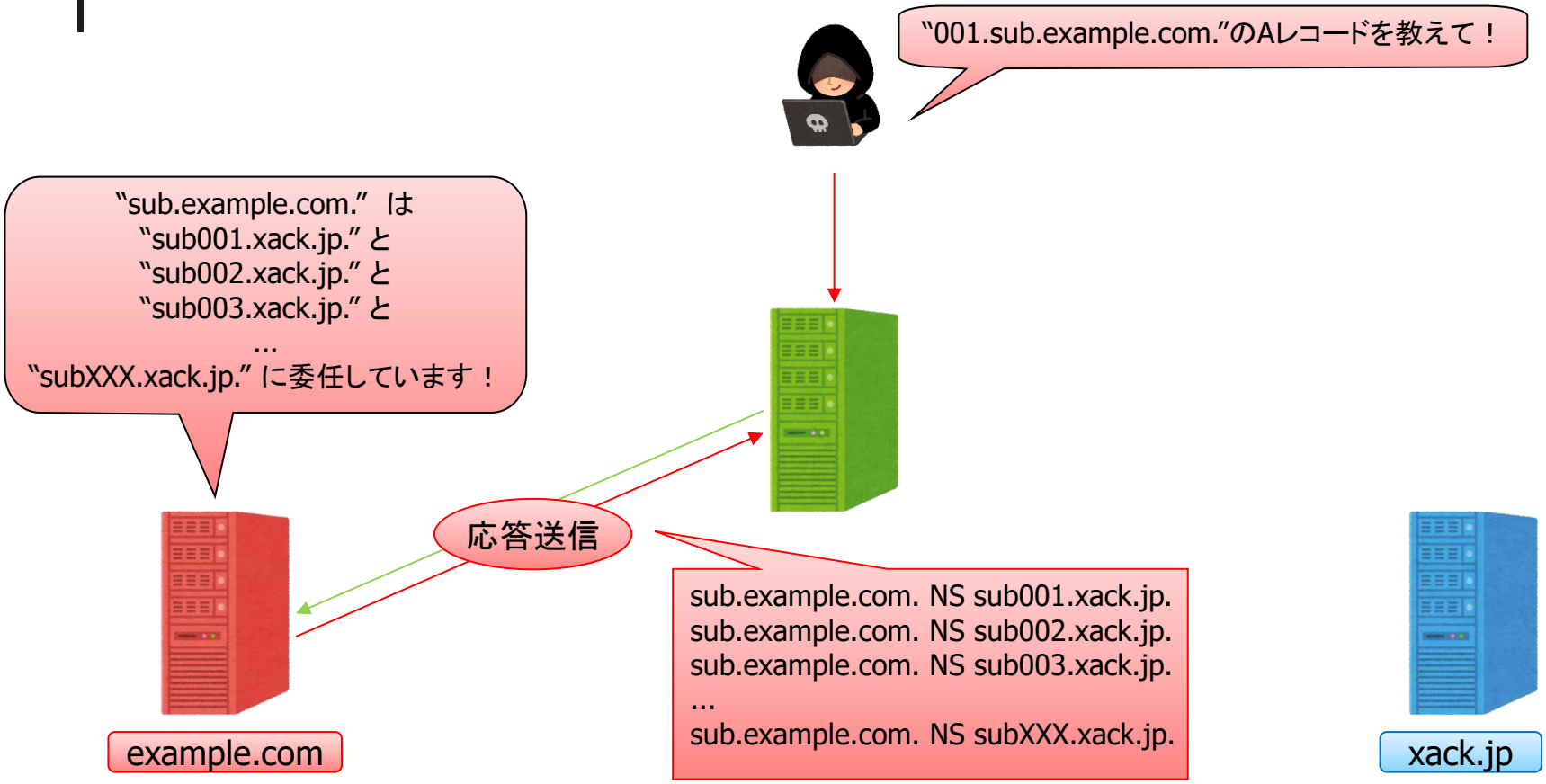
NXNSAttackとは



NXNSAttackとは



NXNSAttackとは



NXNSAttackとは

“001.sub.example.com.”のAレコードを教えて！

“sub.example.com.” は
“sub001.xack.jp.” と
“sub002.xack.jp.” と
“sub003.xack.jp.” と
…
“subXXX.xack.jp.” に委任しています！

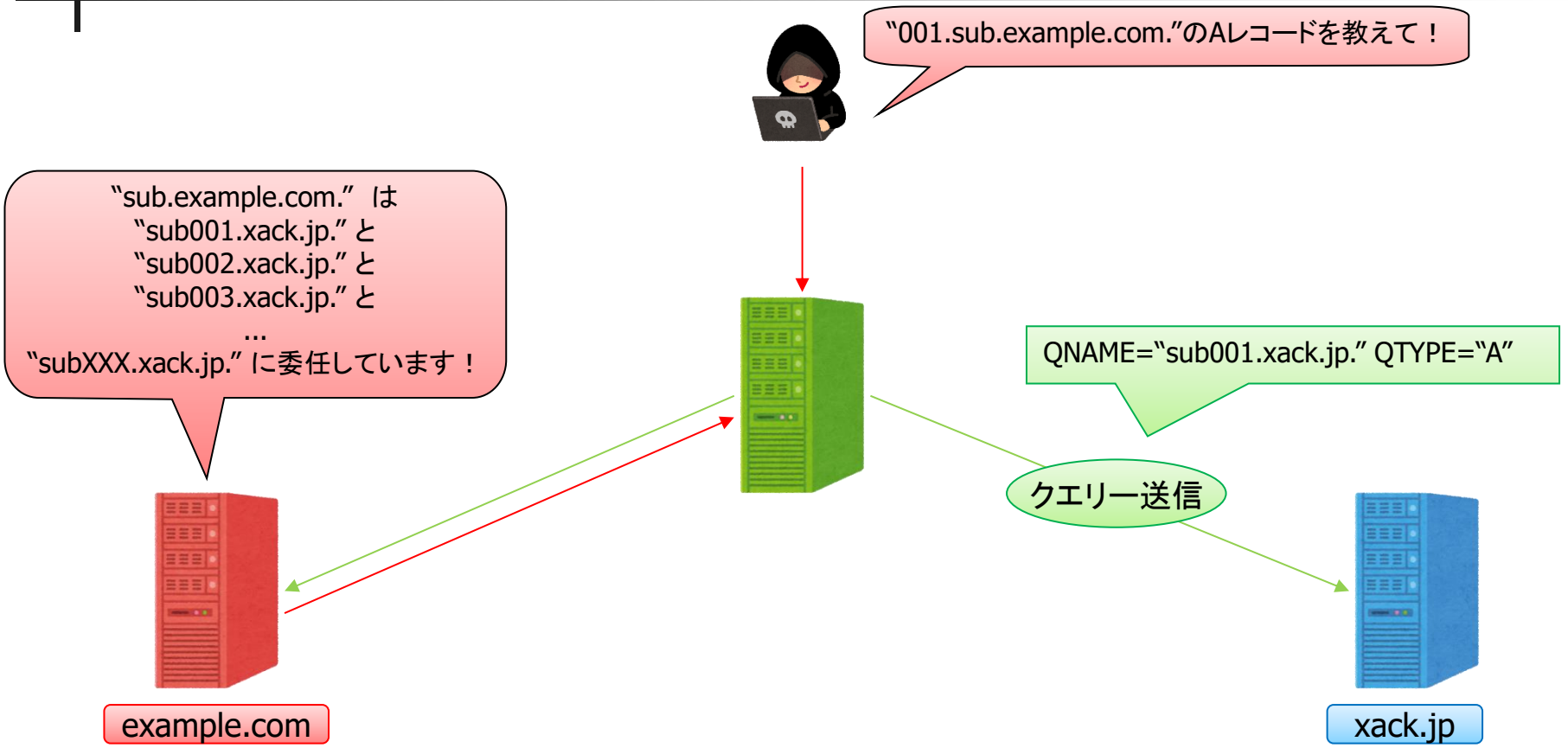
example.com

応答送信

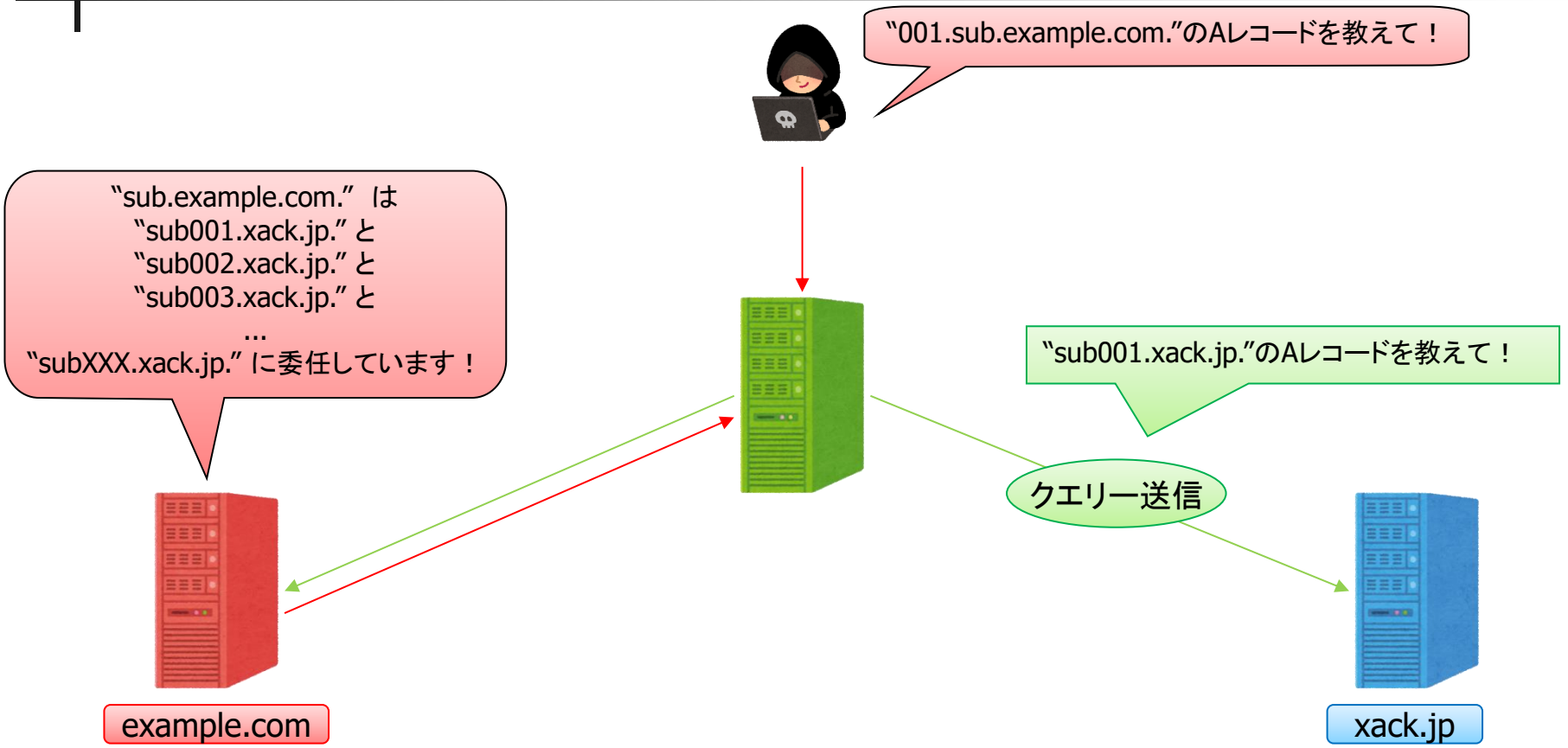
“sub.example.com.”は
“sub001.xack.jp.”と”sub002.xack.jp.”と
“sub003.xack.jp.”と
…
“subXXX.xack.jp.”に委任しているよ！

xack.jp

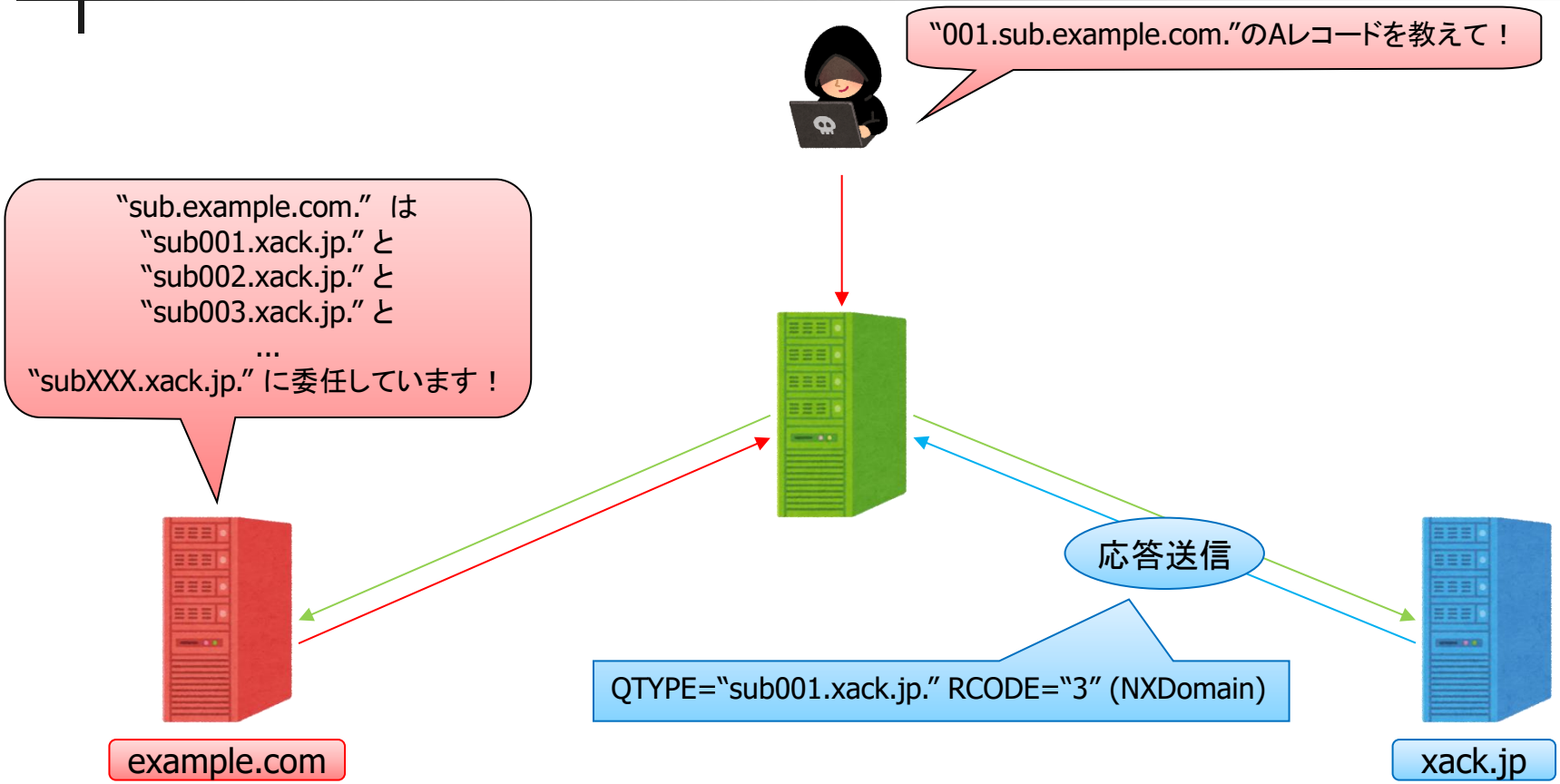
NXNSAttackとは



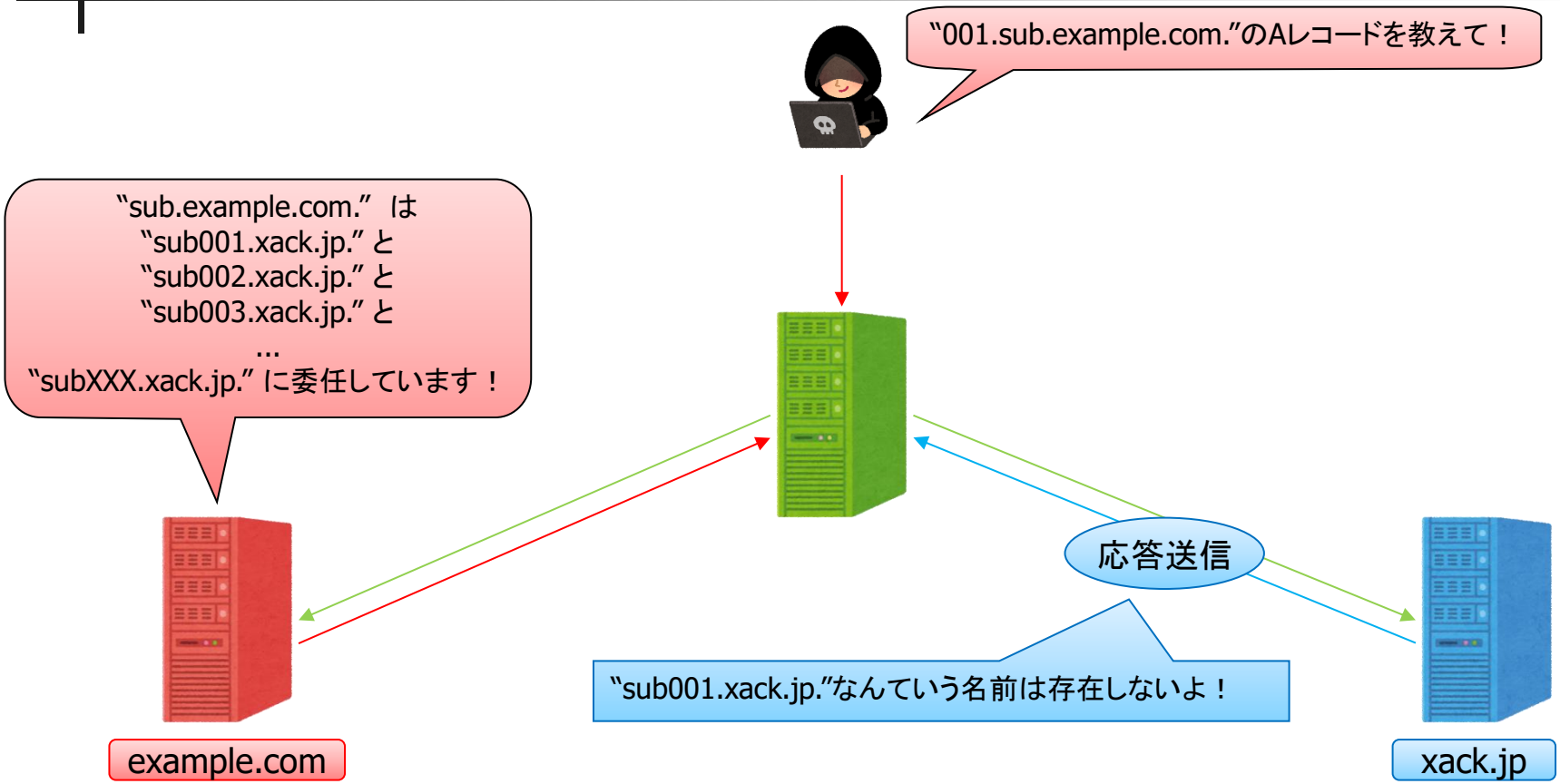
NXNSAttackとは



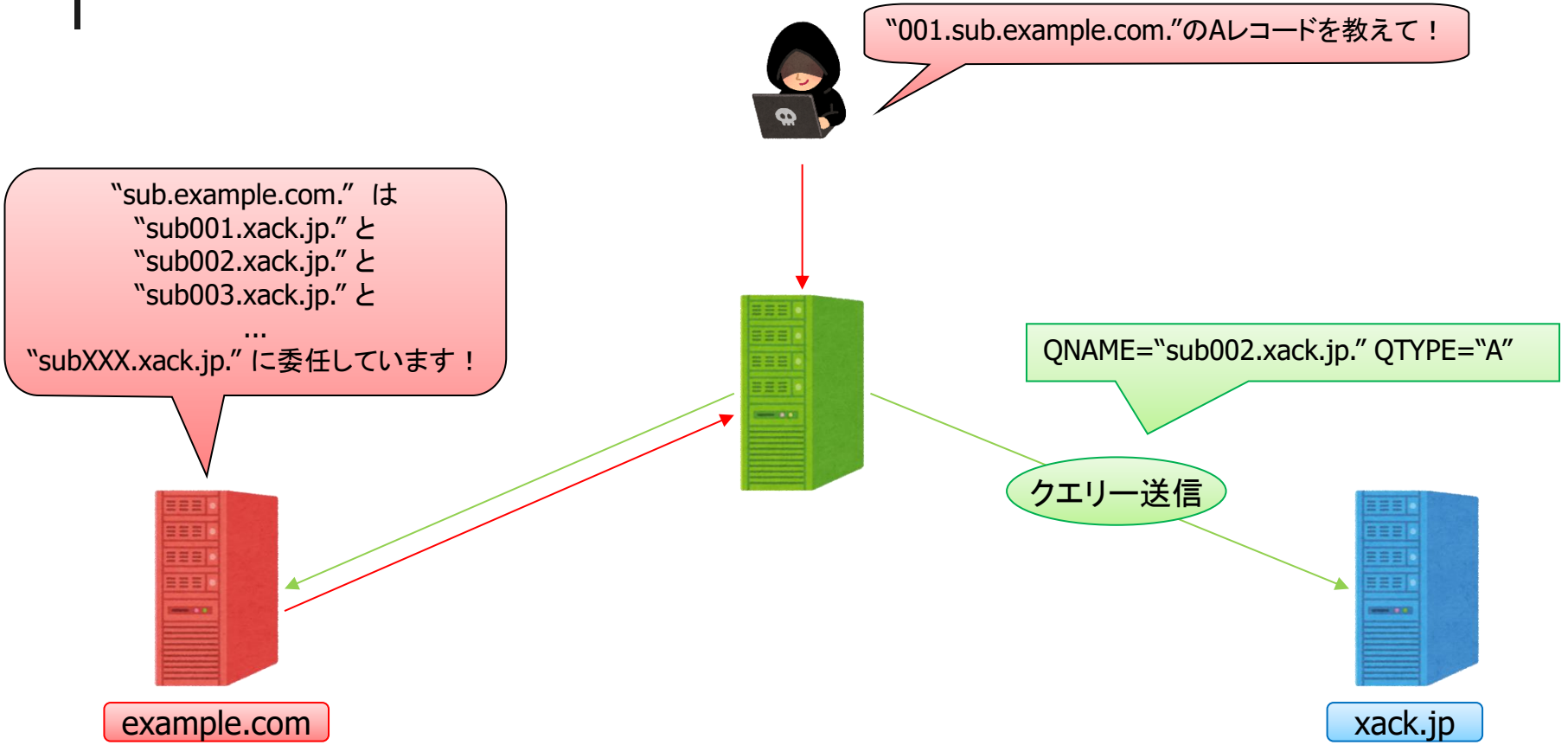
NXNSAttackとは



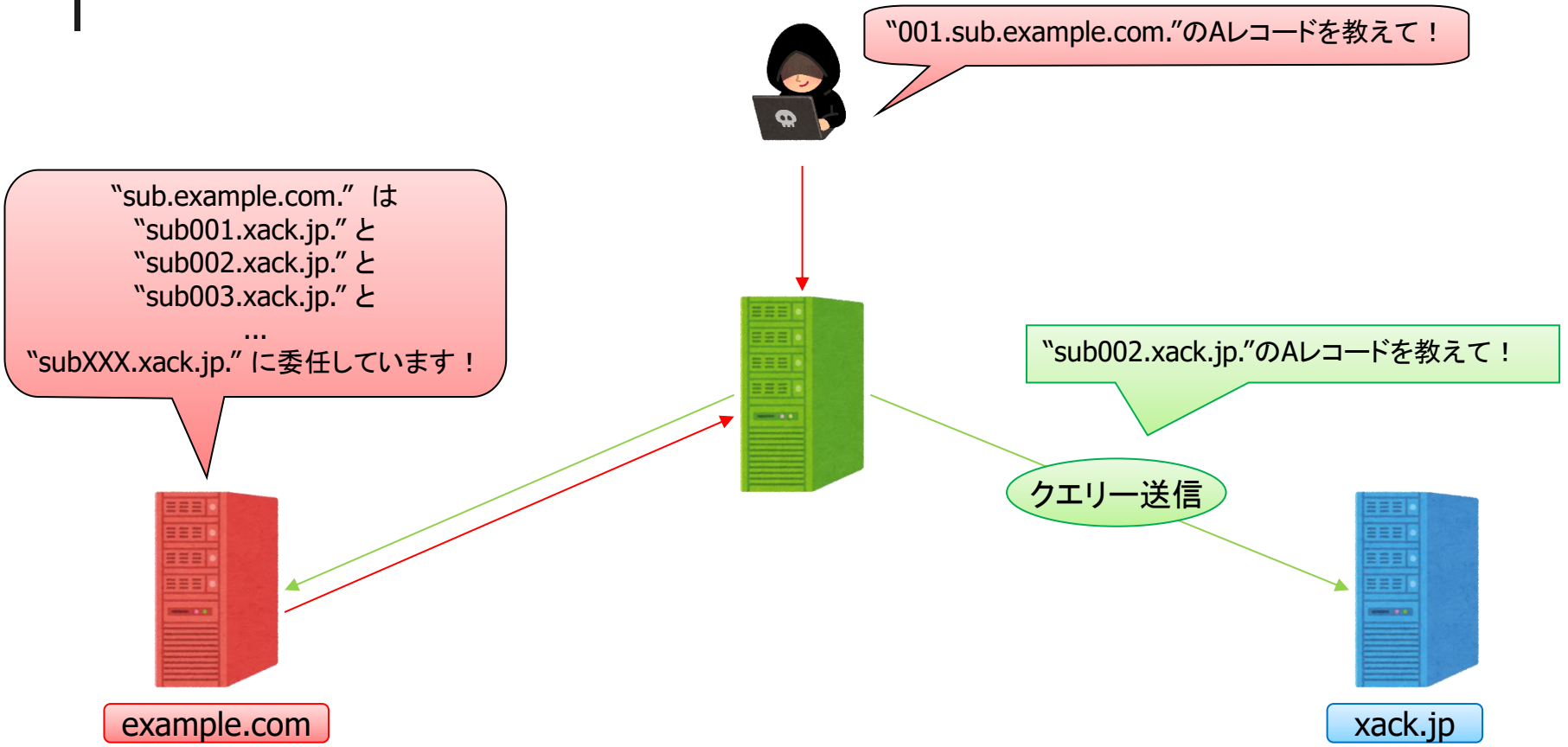
NXNSAttackとは



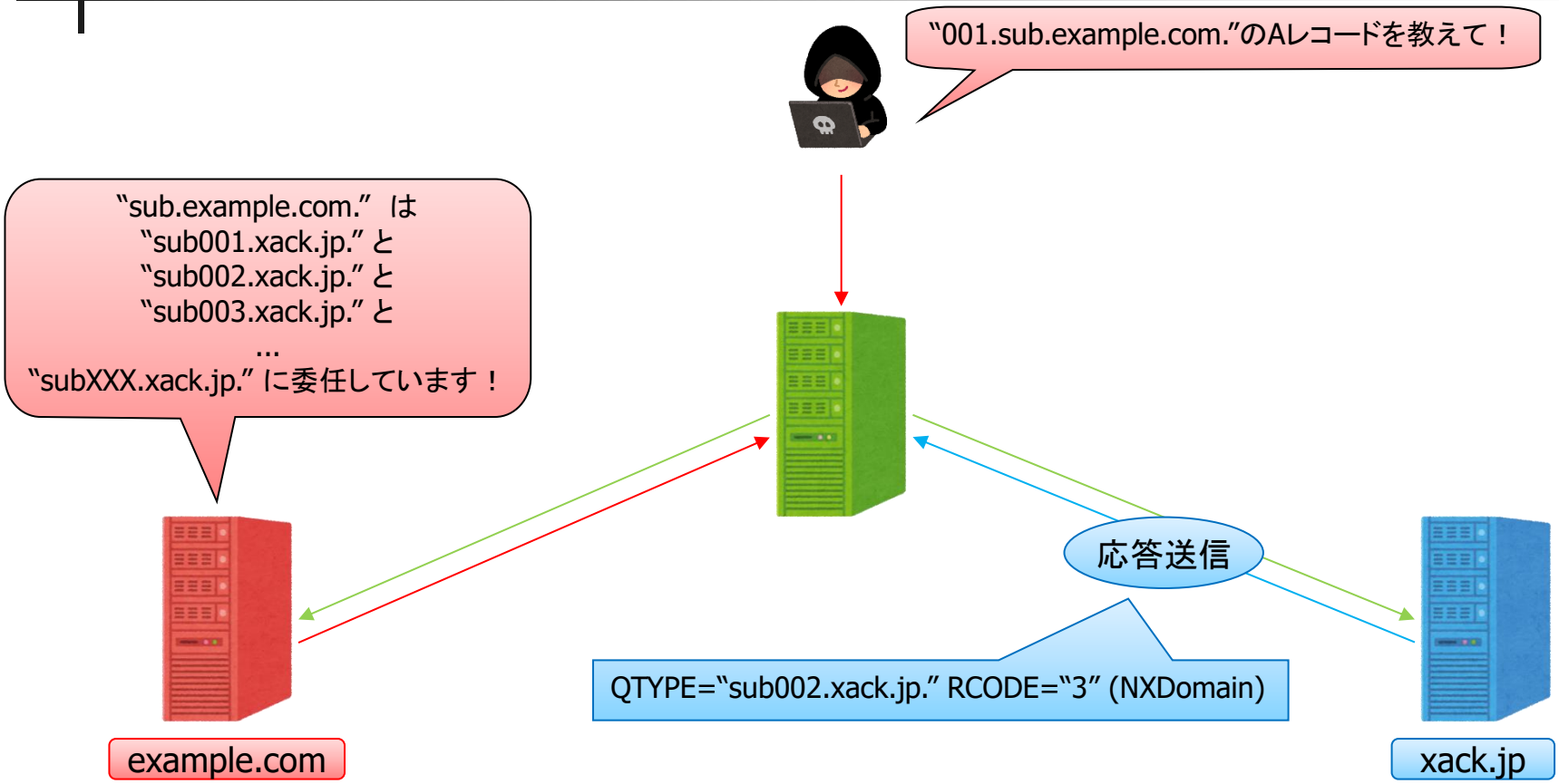
NXNSAttackとは



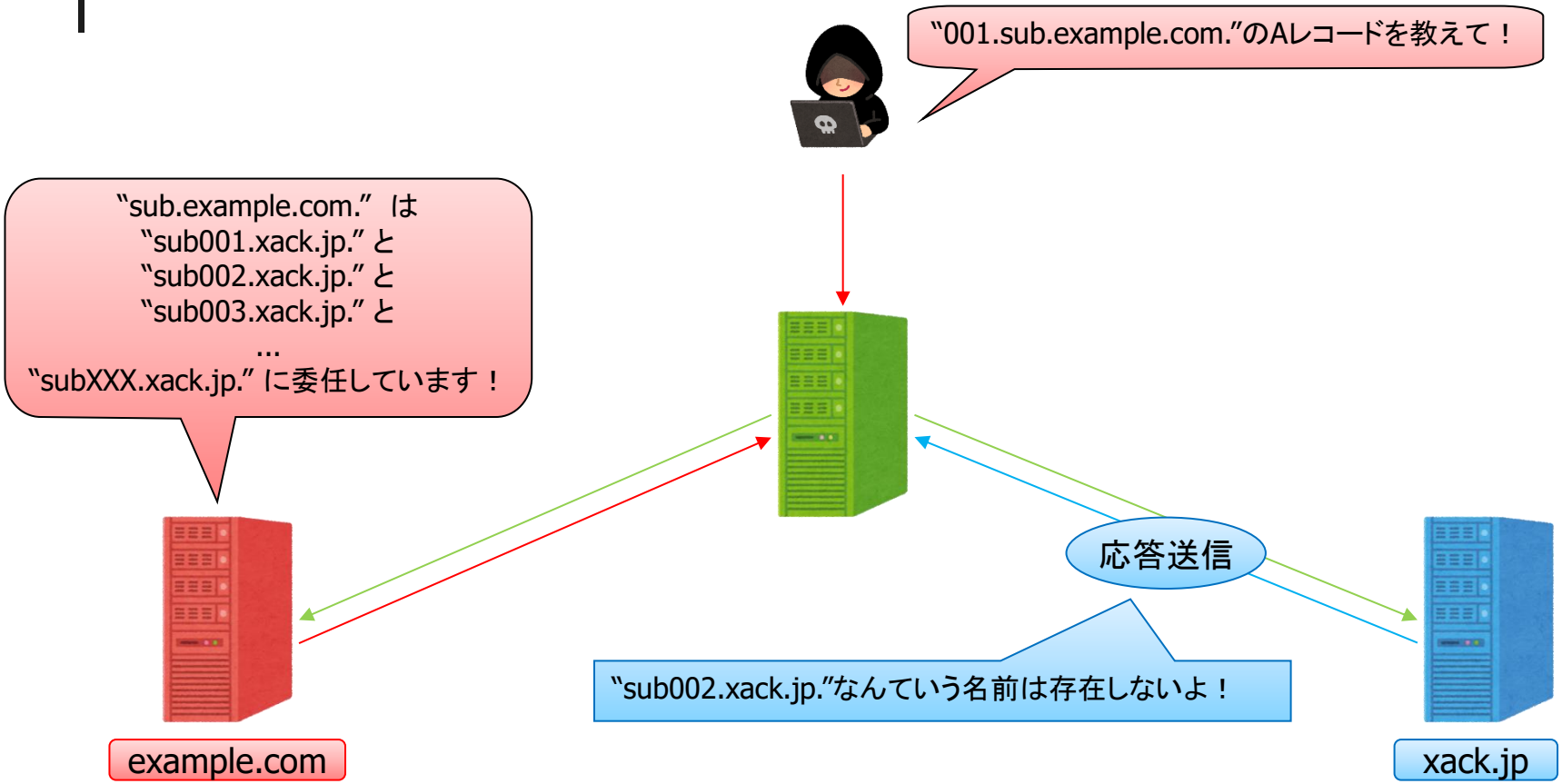
NXNSAttackとは



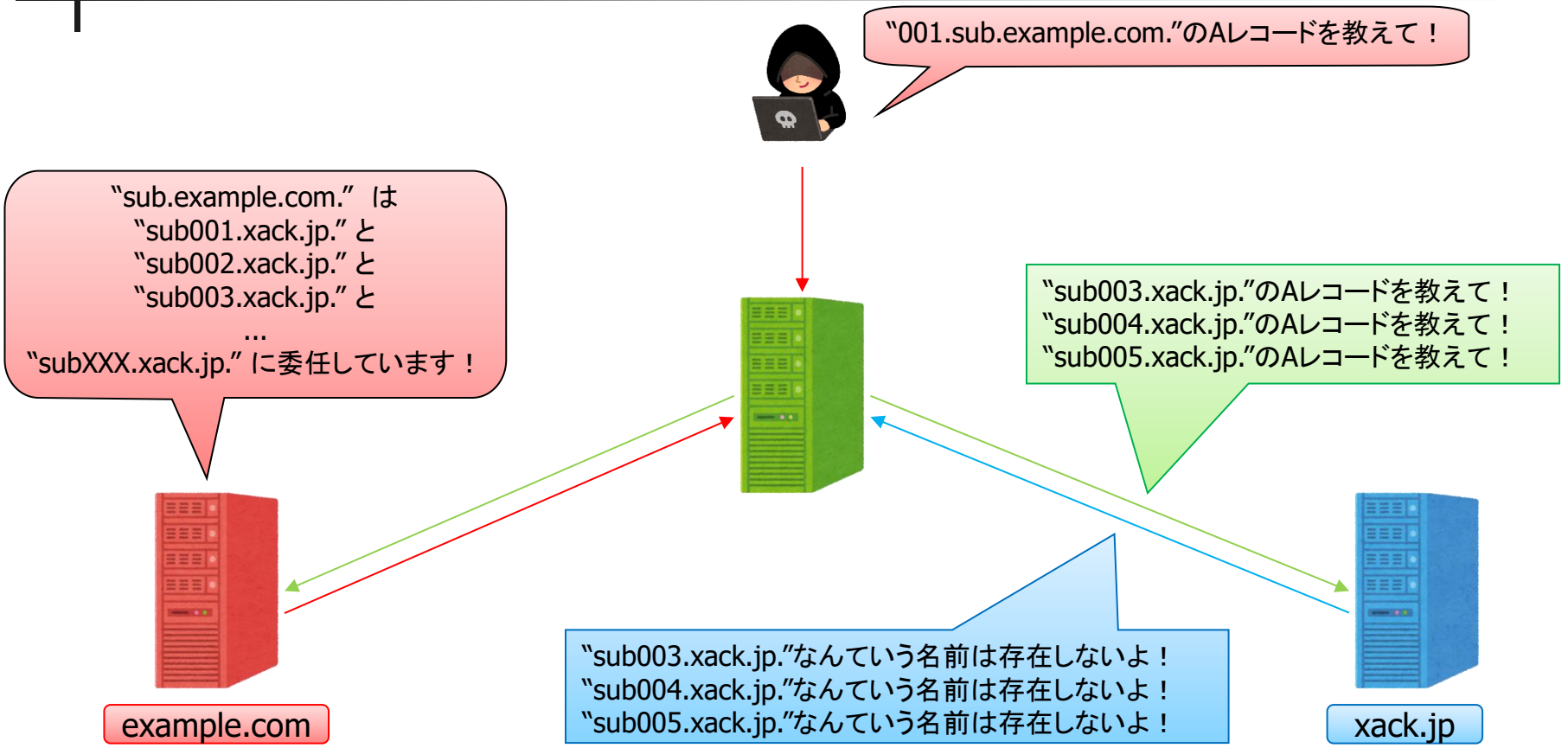
NXNSAttackとは



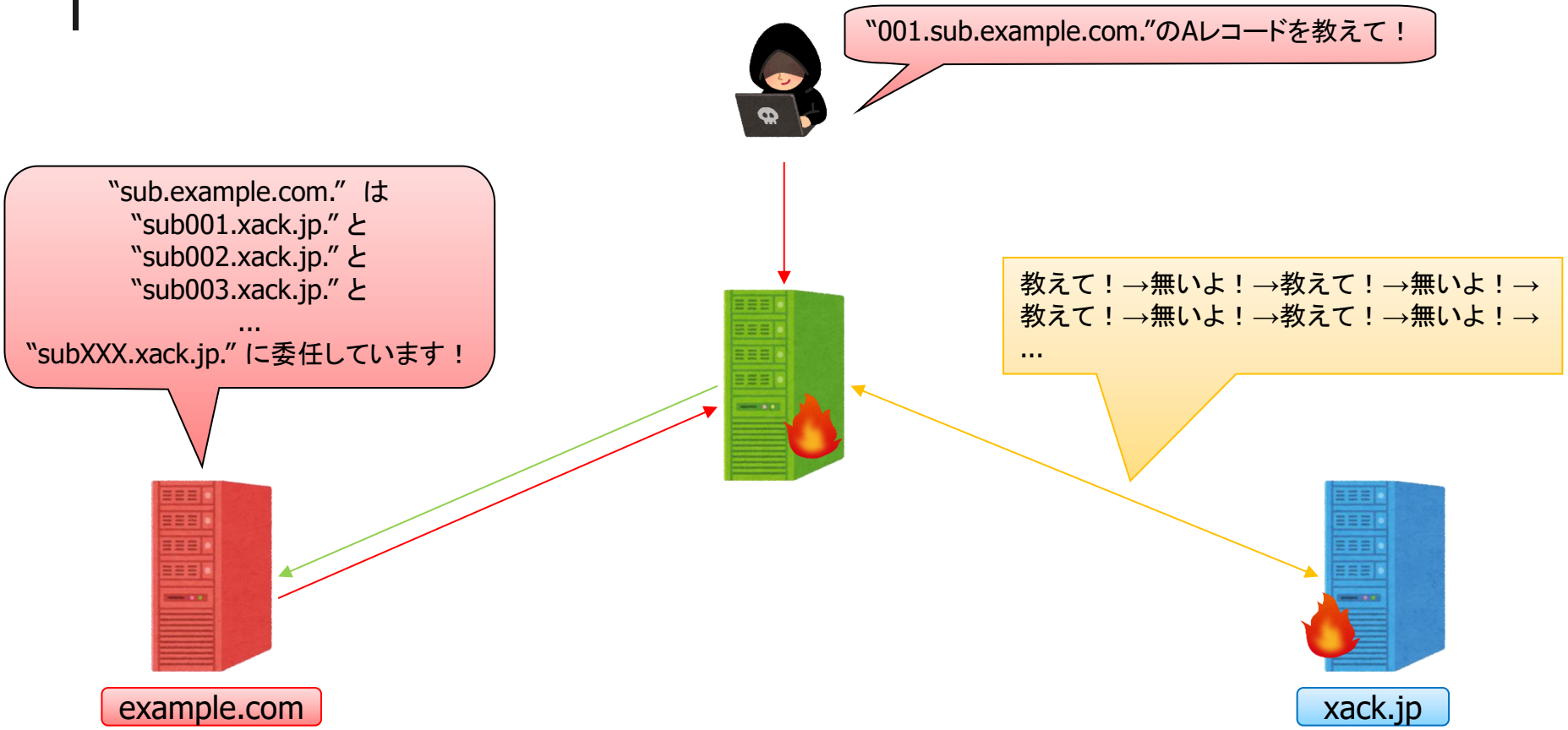
NXNSAttackとは



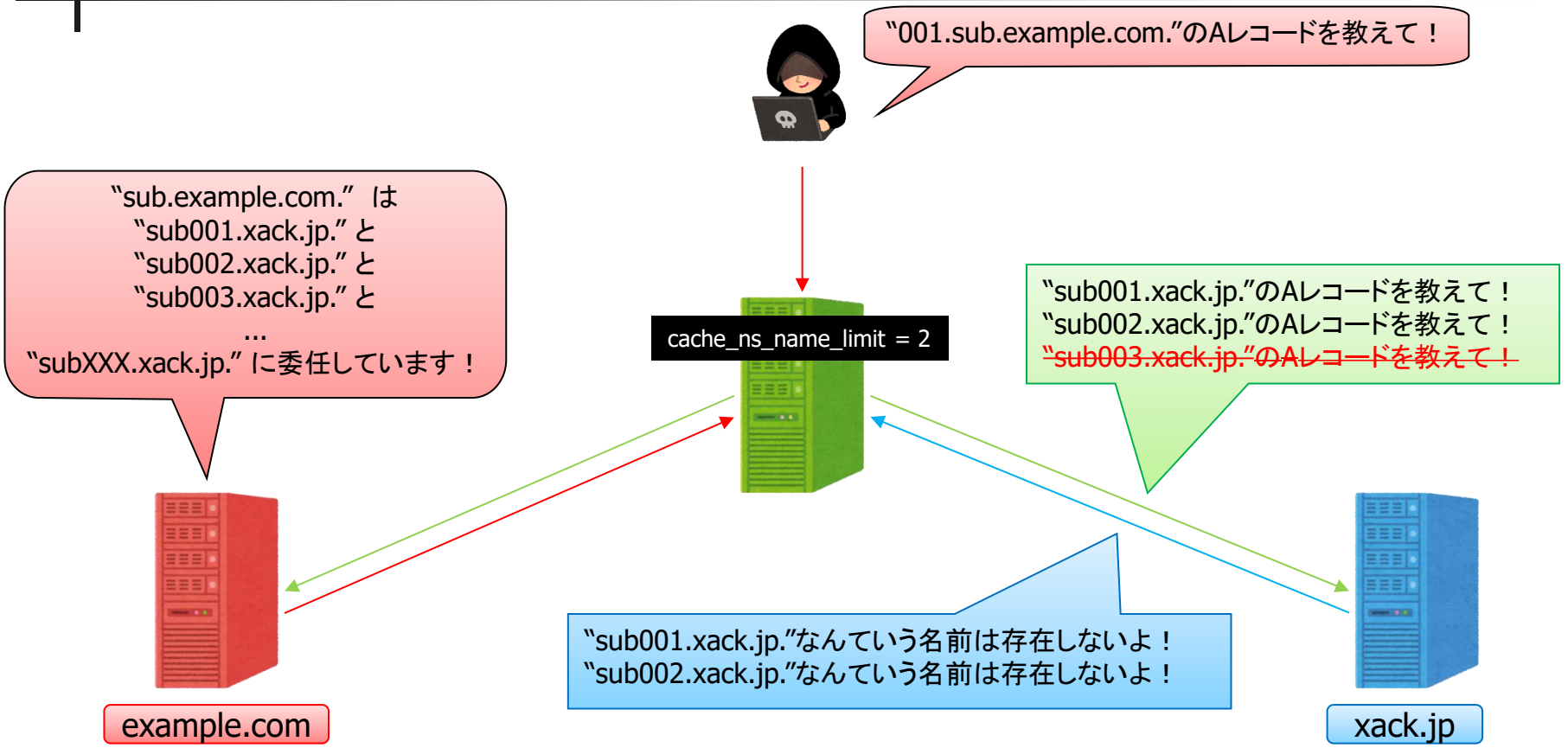
NXNSAttackとは



NXNSAttackとは



NXNSAttackとは



NXOOAttack ?

NX○○Attack？

- 何かあったら水平展開！
  →NSレコード以外でも同様の攻撃が可能なのでは？

- 必要と思われる条件
  1. 向き先を設定できる（攻撃対象となるサーバーを何らかの方法で指定できる）
  2. その向き先にフルリゾルバーが名前解決を行い、
     NXDomainを得るように仕向けることができる
  3. フルリゾルバーが目的のレコードを得られるまで
     複数回問い合わせを行うように細工することができる

NX○○Attack？

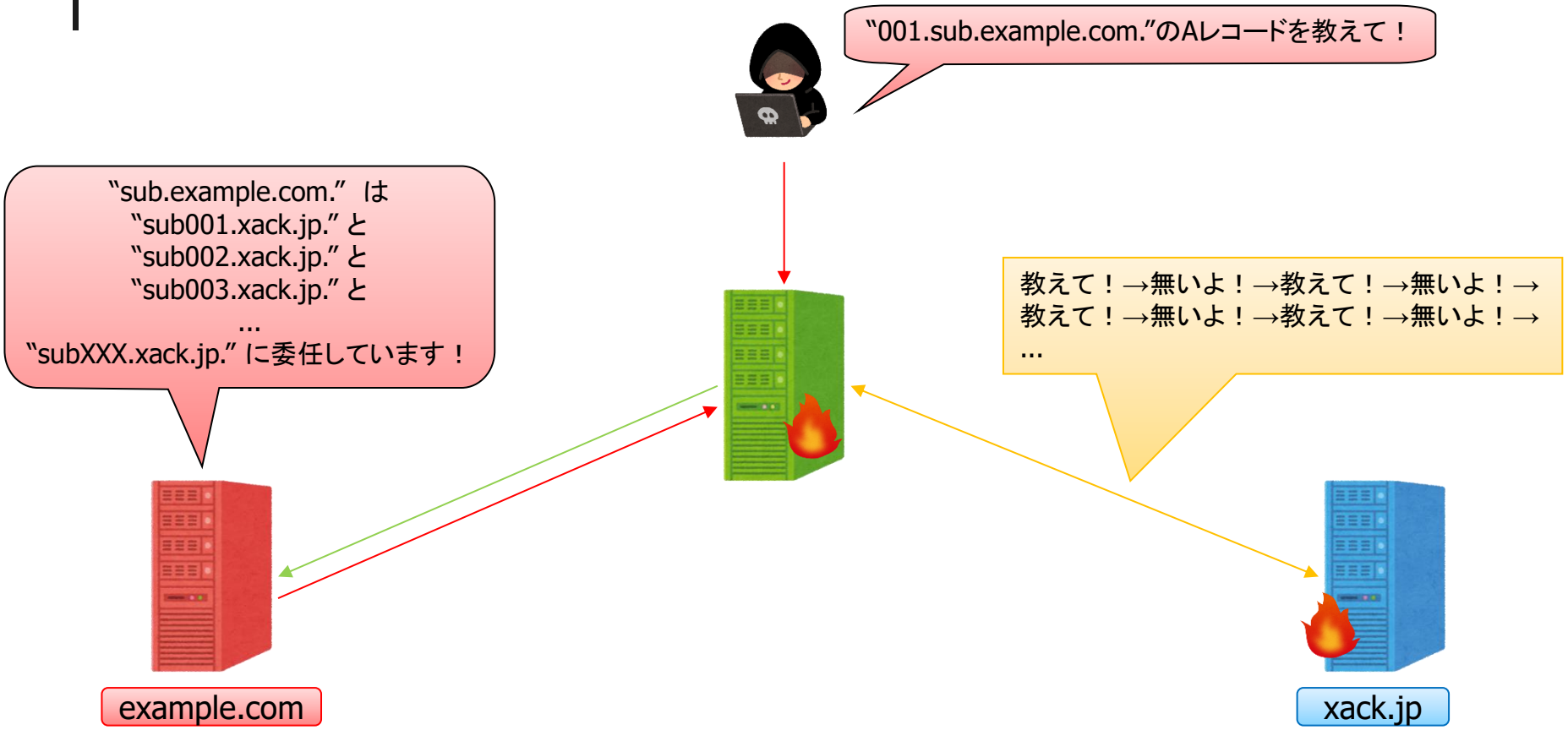
1. 向き先を設定できる（攻撃対象となるサーバーを何らかの方法で指定できる）
2. その向き先にフルリゾルバーが名前解決を行い、NXDomainを得るように仕向けることができる
3. フルリゾルバーが目的のレコードを得られるまで複数回問い合わせを行うように細工することができる

■ 例：NXNSAttack

- ✓ NSDNAMEに向き先を設定できる（ゾーンの権威サーバーに向けられる）
- ✓ NSDNAMEを存在しないであろう名前にすることで、フルリゾルバーがNSDNAMEのA/AAAAレコードを解決しに行き、NXDomainを得るように仕向けることができる
- ✓ 権威部に大量にNSレコードを付与することで、目的のA/AAAAレコードを得られるまでフルリゾルバーが複数回問い合わせを行うようにすることができる

→条件達成！

NXOOAttack ?



NX○○Attack ?

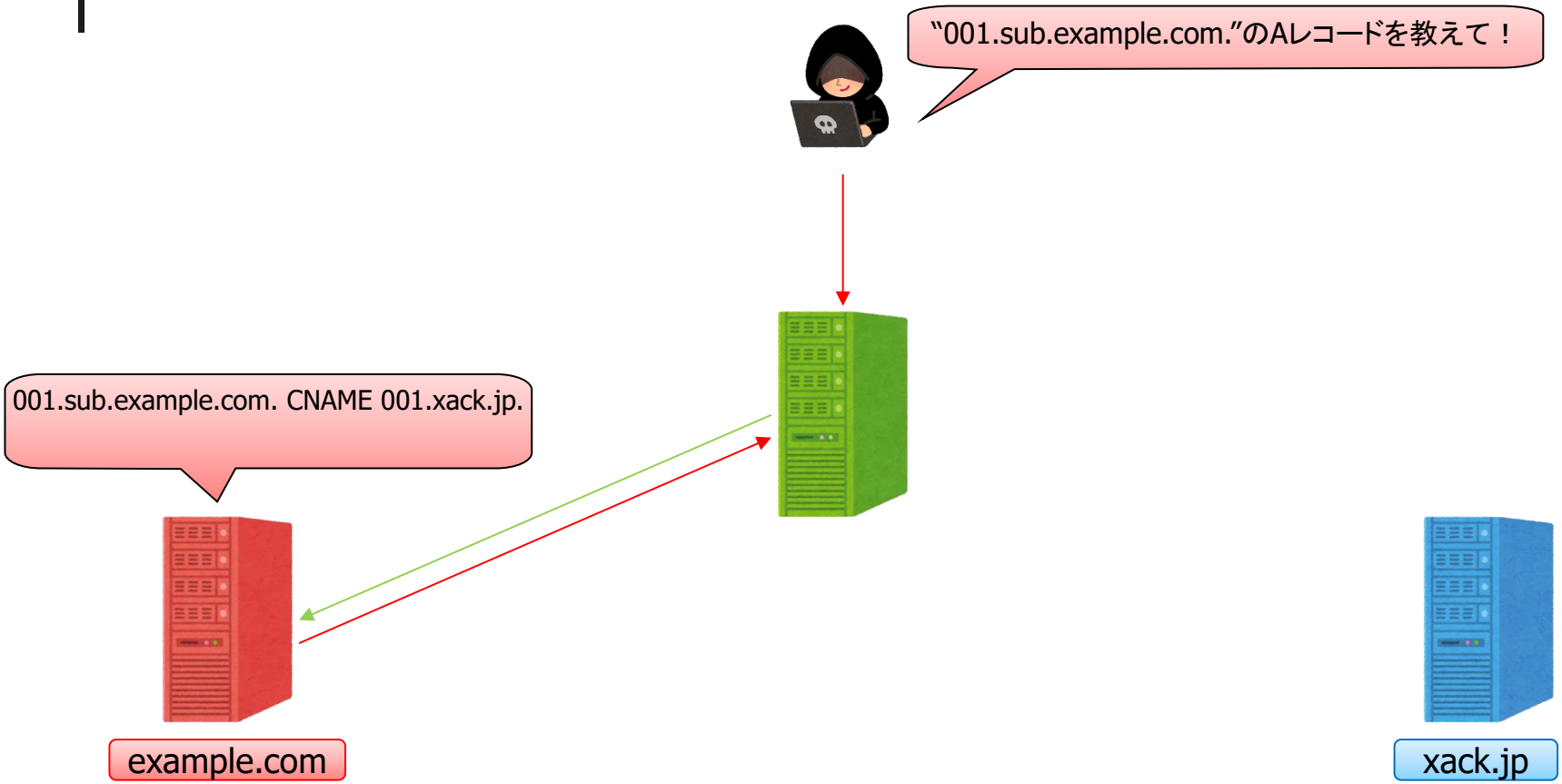
1. 向き先を設定できる（攻撃対象となるサーバーを何らかの方法で指定できる）
2. その向き先にフルリゾルバーが名前解決を行い、NXDomainを得るように仕向けることができる
3. フルリゾルバーが目的のレコードを得られるまで複数回問い合わせを行うように細工することができる

■ NXCNAMEAttack

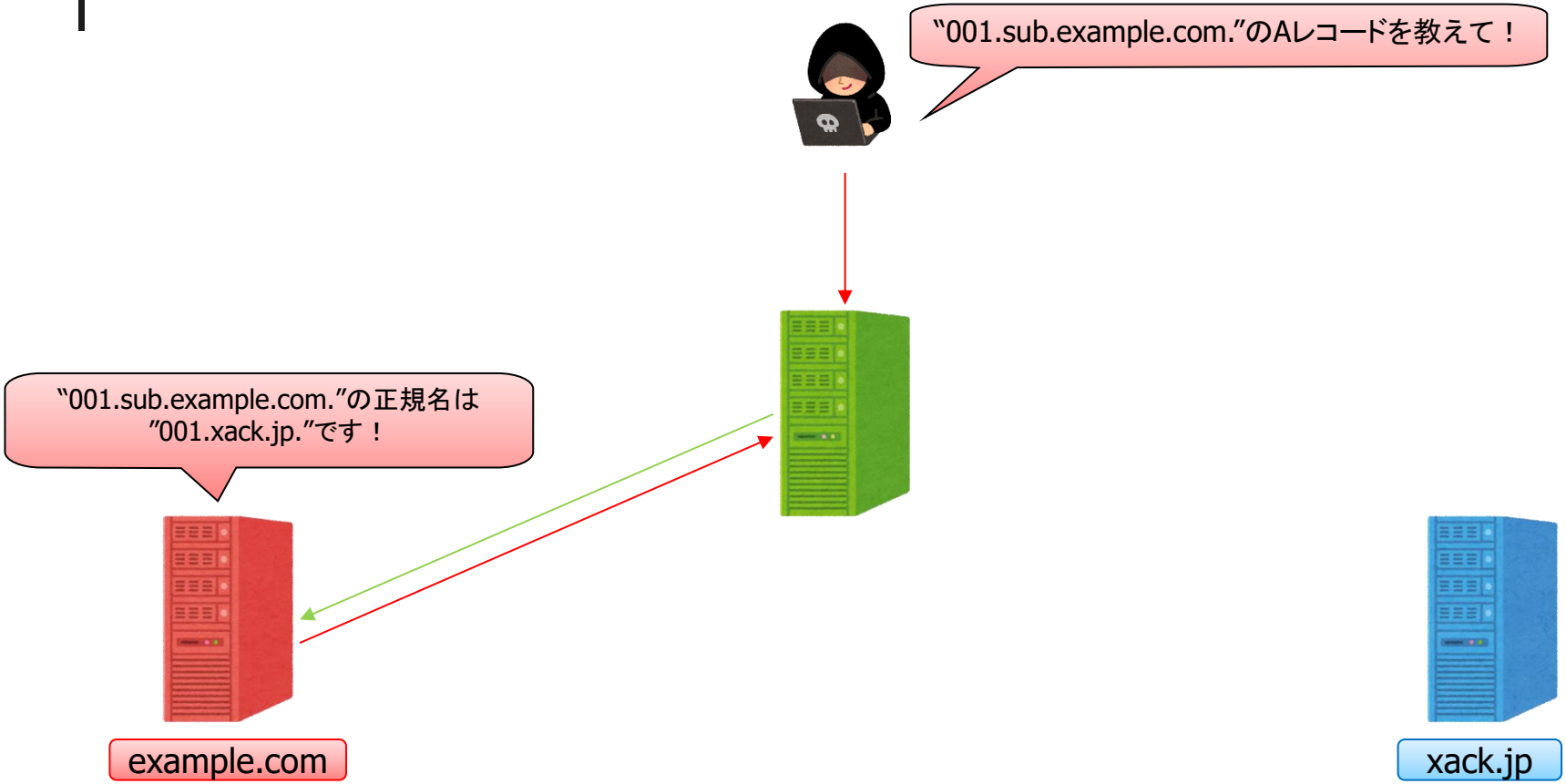
- ✓ CNAMEに向き先を設定できる（ゾーンの権威サーバーに向けられる）
- ✓ CNAMEを存在しないであろう名前にすることで、フルリゾルバーがCNAMEを解決しに行き、NXDomainを得るように仕向けることができる
- ✕ CNAMEは通常、1つの名前につき1つしか設定できず、複数回問い合わせを行うように細工することができない

→条件未達成

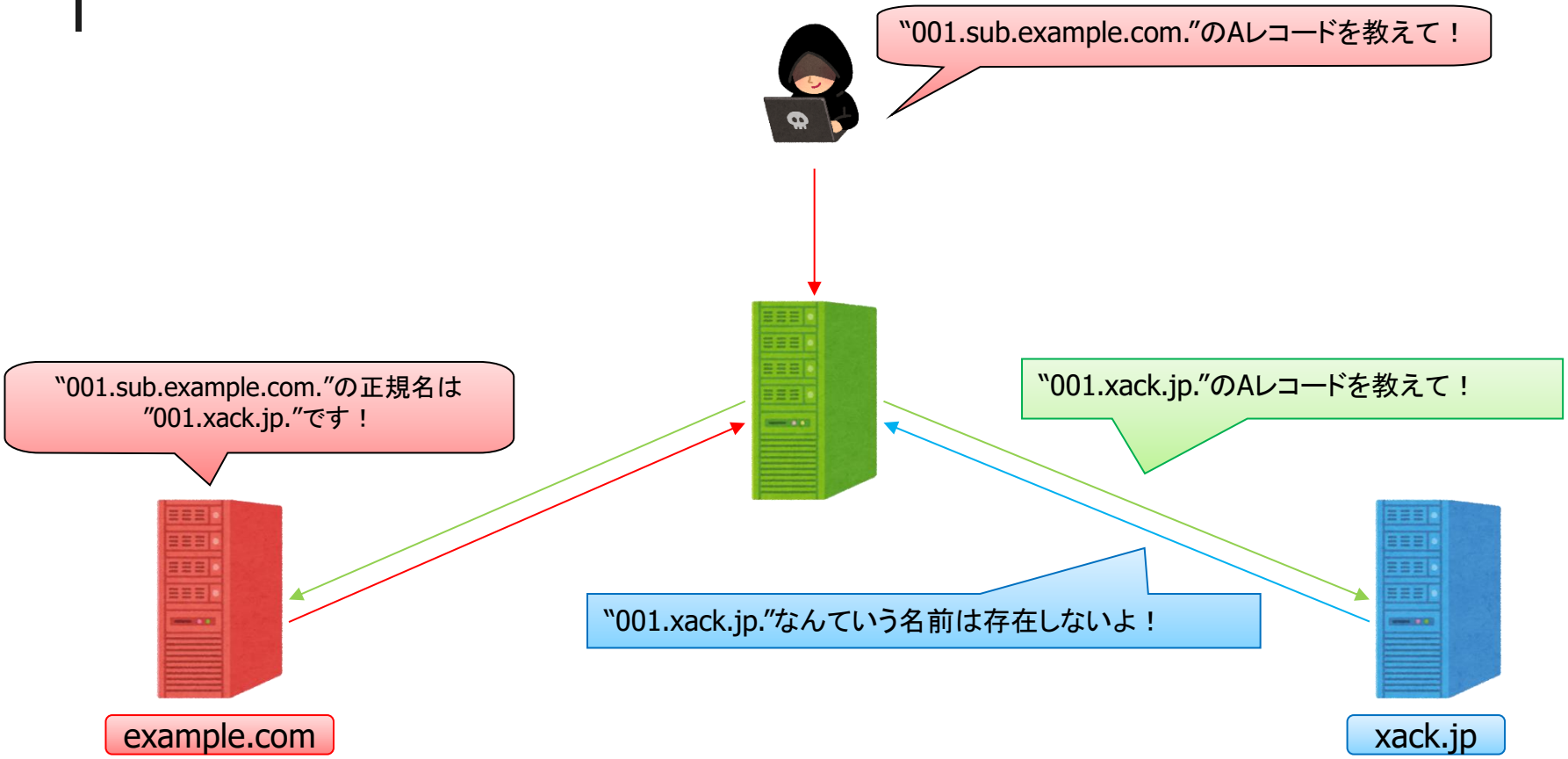
NXOOAttack ?



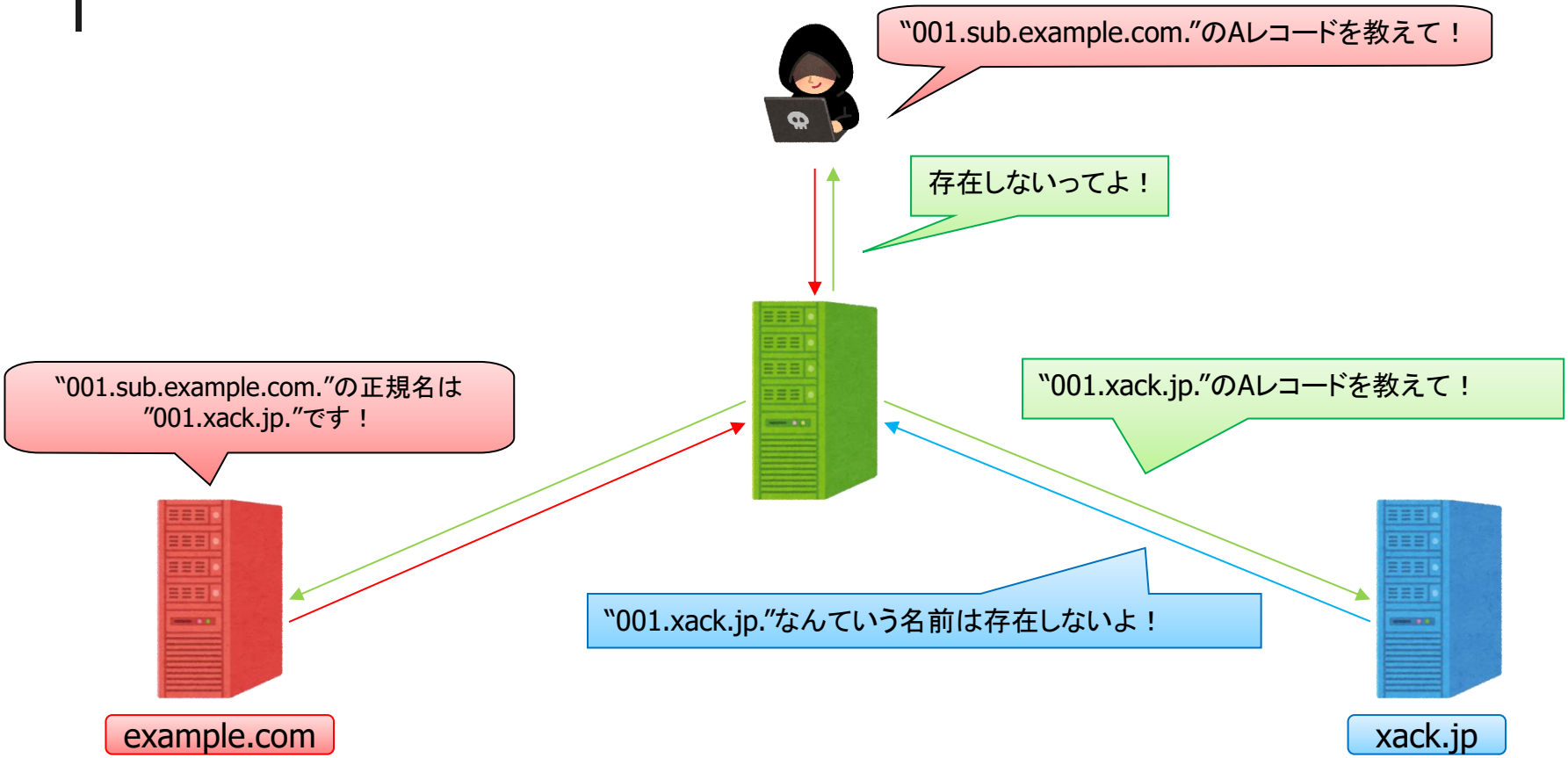
NXOOAttack ?



NXOOAttack ?



NXOOAttack？



NX○○Attack？

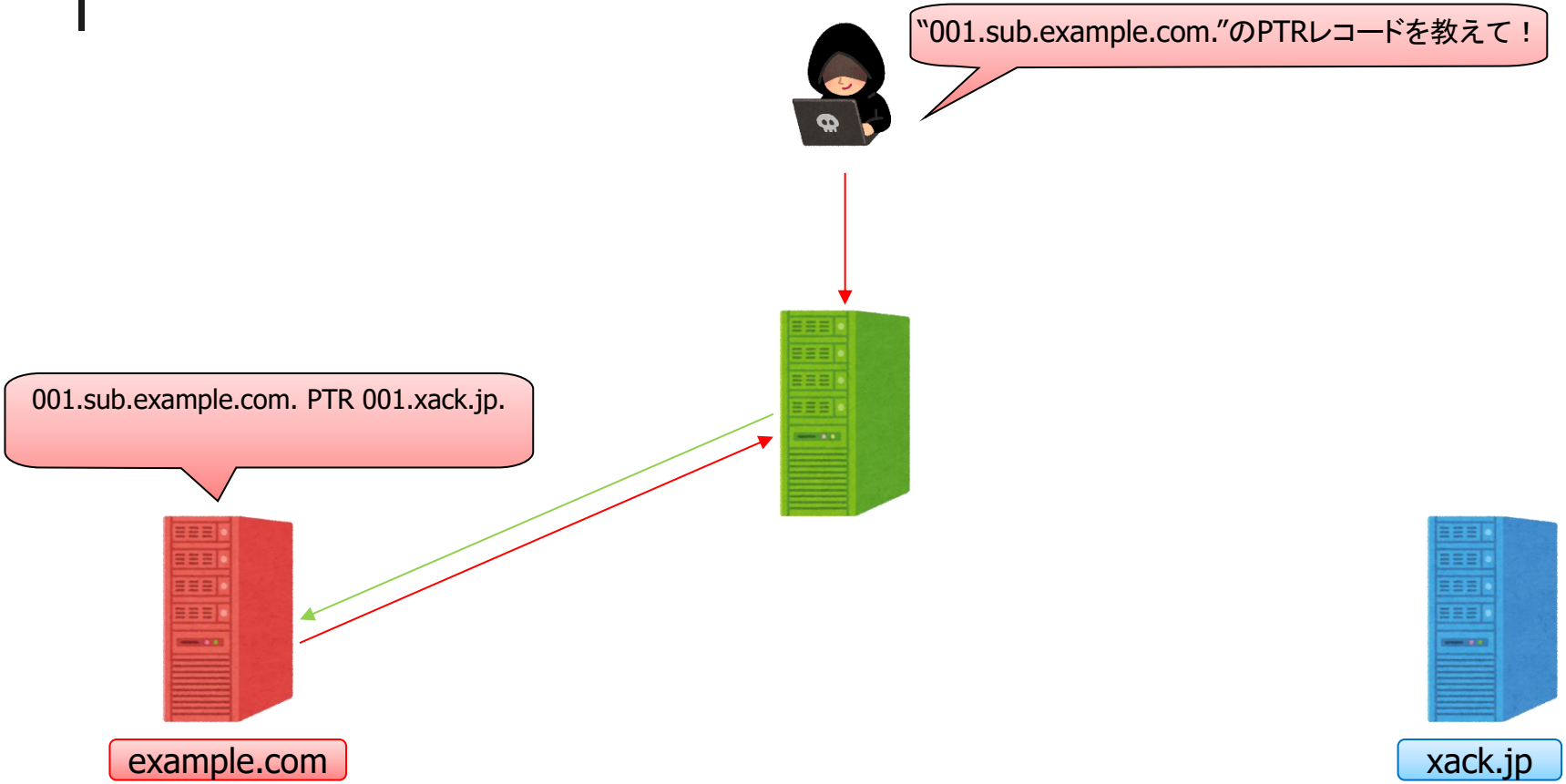
1. 向き先を設定できる（攻撃対象となるサーバーを何らかの方法で指定できる）
2. その向き先にフルリゾルバーが名前解決を行い、NXDomainを得るように仕向けることができる
3. フルリゾルバーが目的のレコードを得られるまで複数回問い合わせを行うように細工することができる

- NXPTRAttack
  - ✓ PTRDNAMEに向き先を設定できる（ゾーンの権威サーバーに向けられる）
  - × フルリゾルバーはPTRDNAMEの名前解決を行わない
  - × そもそも問い合わせ自体が行われない

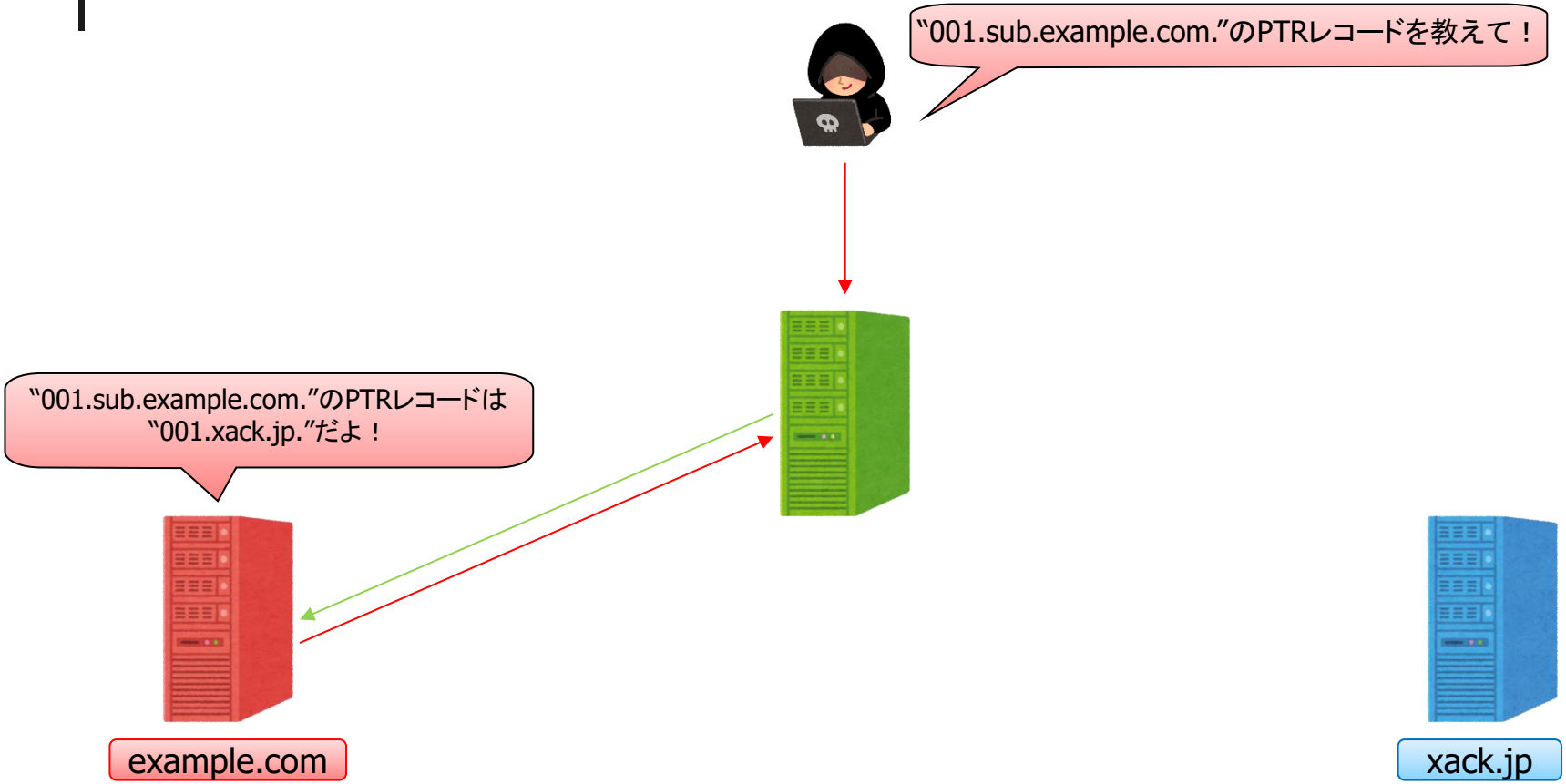
→条件未達成

（PTRDNAMEを解決しようとするようなアプリケーション等があれば或いは？）

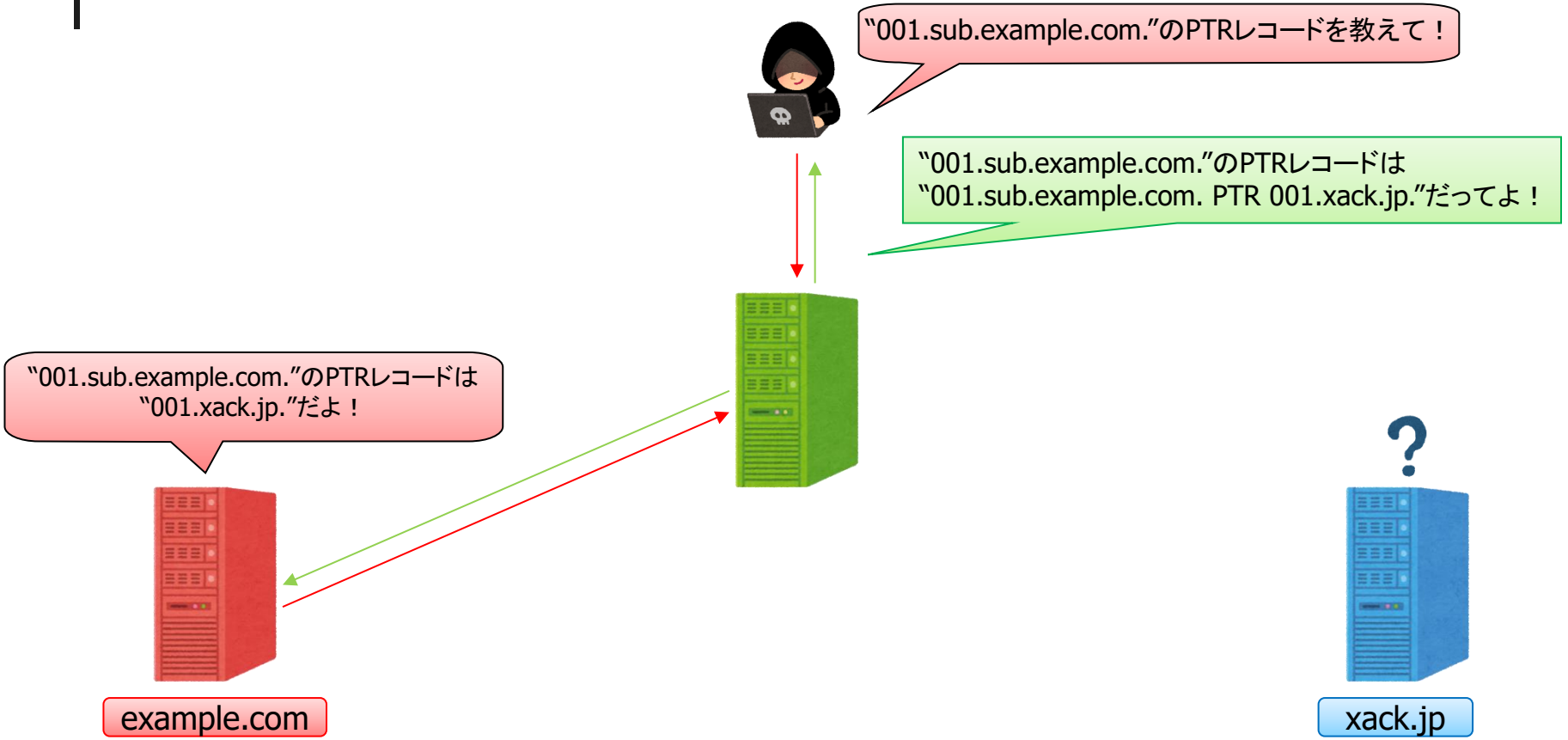
NXOOAttack ?



NXOOAttack ?



NXOOAttack ?



NX○○Attack？

1. 向き先を設定できる（攻撃対象となるサーバーを何らかの方法で指定できる）
2. その向き先にフルリゾルバーが名前解決を行い、NXDomainを得るように仕向けることができる
3. フルリゾルバーが目的のレコードを得られるまで複数回問い合わせを行うように細工することができる

■ NX■■■Attack

- ✓ ■■■に向き先を設定できる（ゾーンの権威サーバーに向けられる）
- ✓ ■■■を存在しないであろう名前にすることで、フルリゾルバーがNXDomainを得るように仕向けることができる
- ✓ 回答部に大量に■■■レコードを付与することで、目的の■■■レコードを得られるまで■■■が問い合わせを繰り返し、フルリゾルバーが複数回問い合わせを行うようにすることができる

→条件達成！

NXOOAttack？

- 実際にやってみた

```
$GENERATE 0-255          foo        IN          ■■■    ■■■
```

```
20200525215405.961683 000100821 [INFO]:   C XXX.XXX.XXX.XXX:38936:U 61620 38 Query Q 1/0/0/1 - 0.xack.jp. A IN
20200525215405.961719 000100821 [NOTICE]: C XXX.XXX.XXX.XXX:38936:U 61620 97 Query R 1/0/1/1 NXDomain AA - -
20200525215405.989364 000100821 [INFO]:   C XXX.XXX.XXX.XXX:50525:U 28425 38 Query Q 1/0/0/1 - 1.xack.jp. A IN
20200525215405.989401 000100821 [NOTICE]: C XXX.XXX.XXX.XXX:50525:U 28425 97 Query R 1/0/1/1 NXDomain AA - -
20200525215405.989364 000100821 [INFO]:   C XXX.XXX.XXX.XXX:50525:U 35813 38 Query Q 1/0/0/1 - 2.xack.jp. A IN
20200525215405.989401 000100821 [NOTICE]: C XXX.XXX.XXX.XXX:50525:U 35813 97 Query R 1/0/1/1 NXDomain AA - -
 ...
 ...
 ...
```

- ただ実際に攻撃に使えるかというと微妙です。
- 一応伏せてはおきます。

まとめ

まとめ

- NXNSAttackは、RFC通りに真面目に名前解決を行おうとしたフルリゾルバーが加害者になってしまう、DNSプロトコルの穴を突いた攻撃手法
  - 利用されているのはDNSの根幹となる部分
  - DNSプロトコルの難しさを再認識

  - 一部のアナウンスで「実装上の不具合」と表現されていましたが、この評価は開発者側からすると少し手厳しいです…。

- 今回の経験と水平展開の結果を踏まえ、今後もキャリアグレードの製品を開発してまいります。

https://www.xack.co.jp