2009年9月7日
第29回JPドメイン名諮問委員会
資料4

DNSSECの基本的仕組み

2009年9月7日

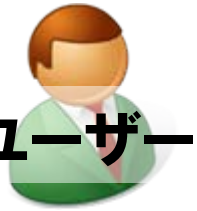
株式会社日本レジストリサービス

DNSとは

DNSはインターネットの電話帳

電話の場合

お店に
電話をかける



名前　電話帳　電話番号

○○株式会社の電話番号
○○株式会社　- 03-1234-XXXX

exampleの電話番号
example商店　- 03-3456-XXXX

△△△サービスの電話番号
△△△サービス　- 03-5678-XXXX

⋮

インターネットの場合

Webサイトに
アクセスする

ドメイン名　DNS　IPアドレス

YahooのIPアドレス
yahoo.co.jp　- 203.216.247.225

exampleのIPアドレス
example.jp　- 192.0.2.10

mixiのIPアドレス
mixi.jp　- 59.106.41.91

⋮

お店に電話をかけるとき（電話帳）

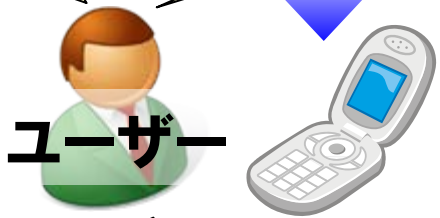
example商店
(03-3456-XXXX)

「電話」のやりとりの❸は、
「名前」ではなく「電話番号」
を利用しておこなわれる。

example商店
に電話をかける

❸

example商店
の電話番号は？



電話帳を調べる
❶
❷
03-3456-XXXX

名前　電話帳　電話番号

○○株式会社の電話番号
○○株式会社　- 03-1234-XXXX

example商店の電話番号
example商店　- 03-3456-XXXX

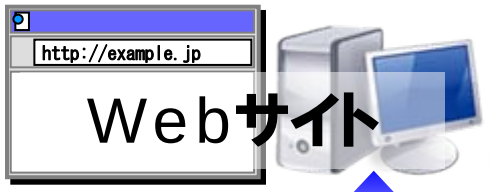
△△△サービスの電話番号
△△△サービス　- 03-5678-XXXX

⋮

ユーザー自身が電話帳から
「example商店」（名前）を探し、
「電話番号」（アドレス）を調べる

Webサイトにアクセスするとき（DNS）

example.jp
(192.0.2.10)



example.jp
にアクセスする

3

example.jp
のIPアドレスは？

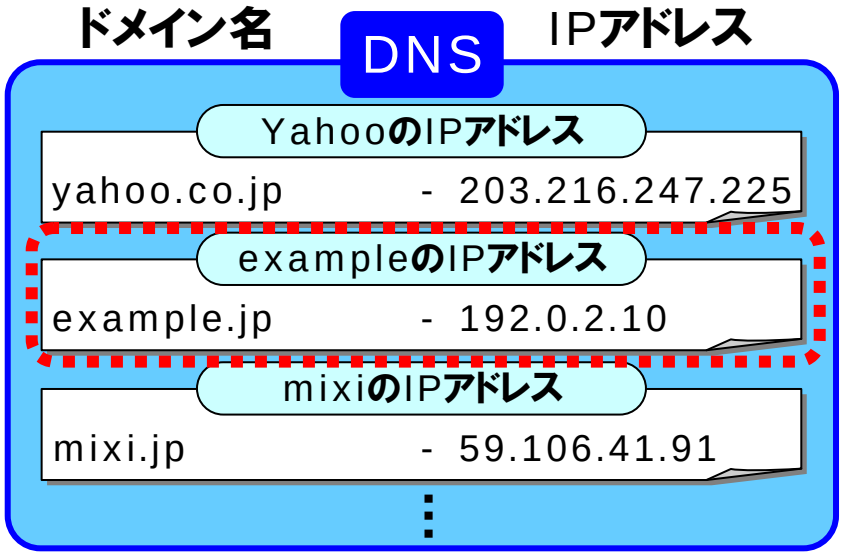
DNSを調べる
1

2
192.0.2.10

ユーザーがWebサイトにアクセスしようとすると、
ユーザーに代わってキャッシュサーバが
DNSから「example.jp」（名前）を探し、
「IPアドレス」（アドレス）を調べる

ユーザーには、IPアドレスを調べるDNSの通信
1 2 は見えない。

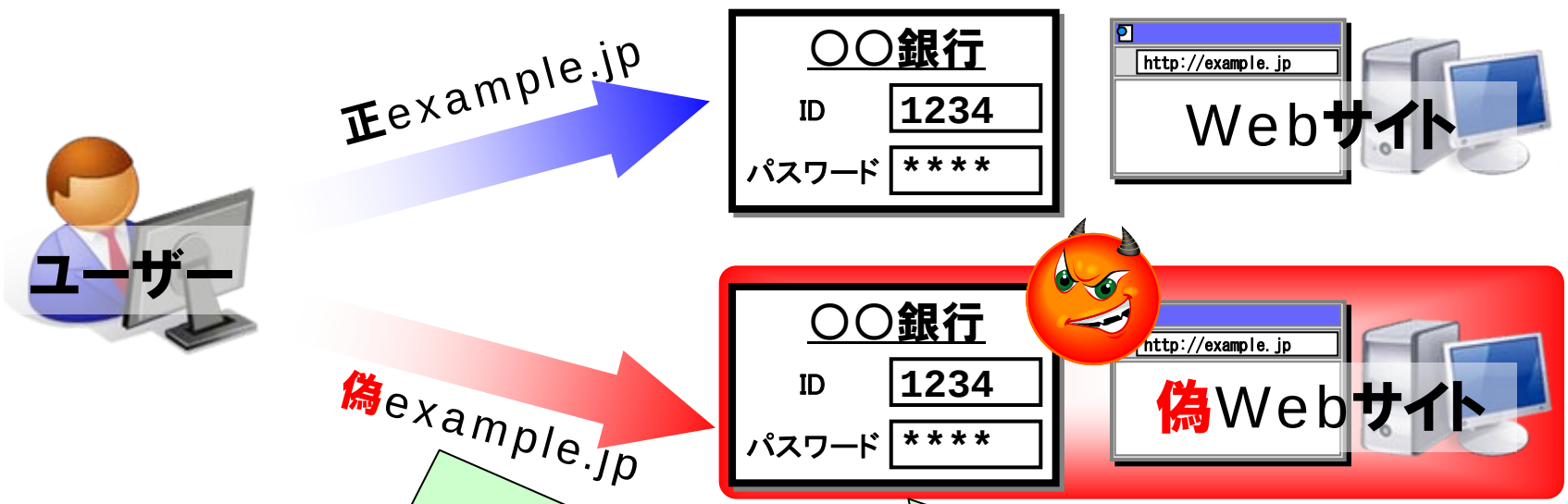
「Webサイト」のやりとりの 3 は、
「ドメイン名」ではなく「IPアドレス」
を利用しておこなわれる。



DNSにおけるセキュリティ上の脅威

フィッシング(phishing)とは

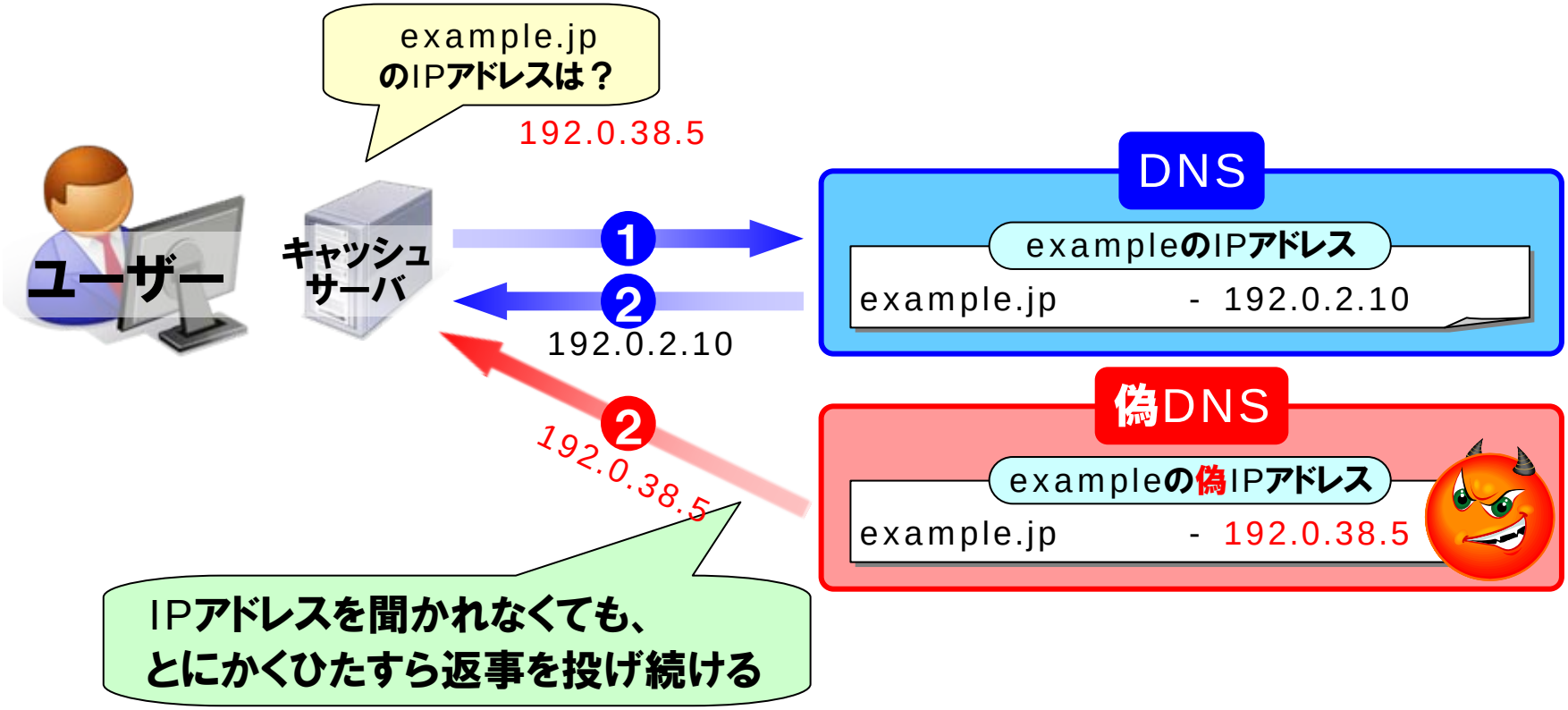
**本物Webサイトと良く似た偽Webサイトを利用し、
ユーザーID、パスワードなどの個人情報を入力させる。
入力した情報は第三者に盗まれてしまい、悪用される。**



ダイレクトメールなどを利用して、
ユーザーを偽Webサイトへ誘導する

本物のWebサイトと見た目がそっくりな
偽Webサイトを作る

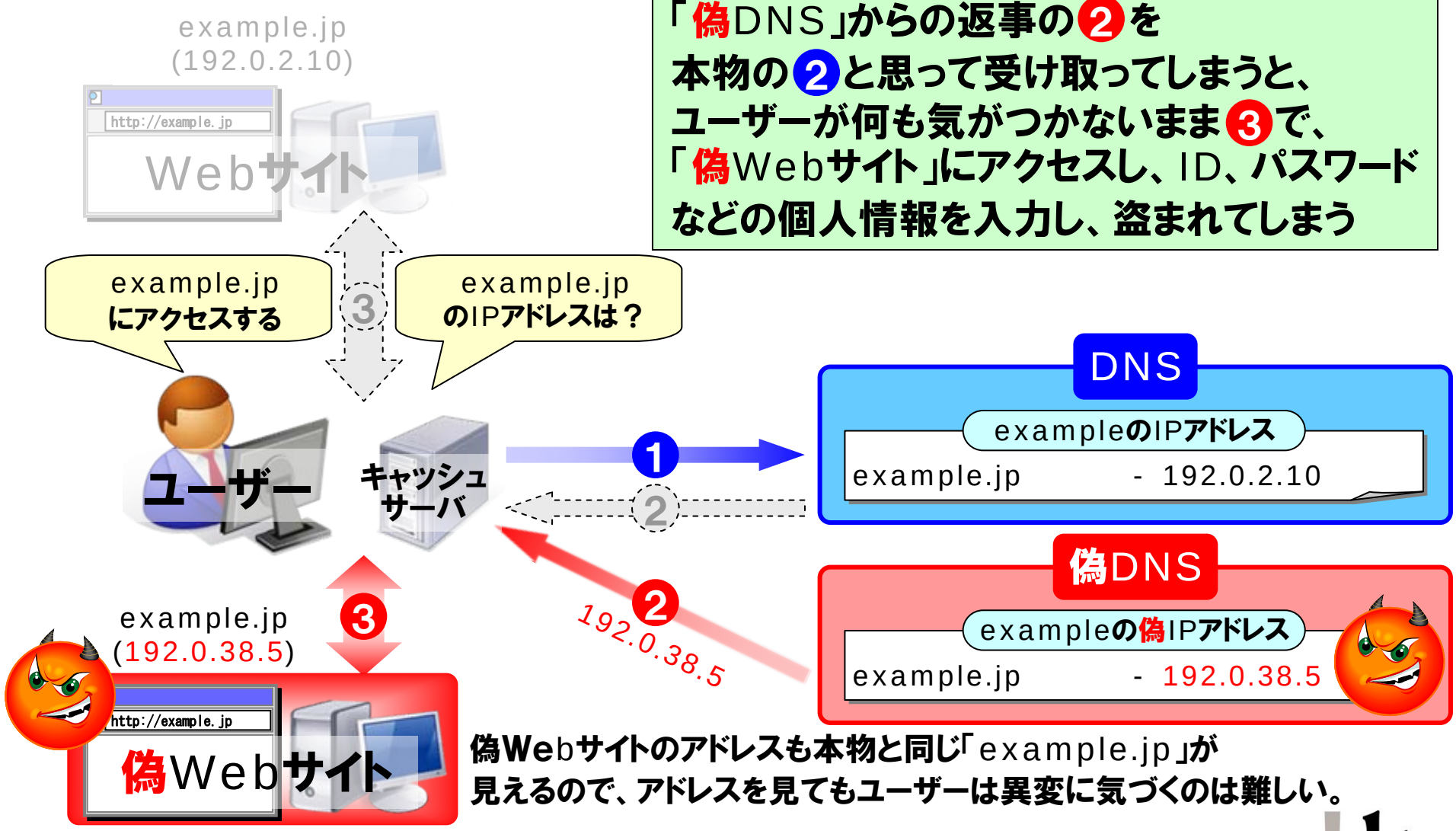
偽DNSを利用して、返事を偽装する



タイミングよく2の返事を受け取ると、それが1の正しい応答の2として処理され、「example.jp」のIPアドレスは偽の「192.0.38.5」が採用されて、そのまま処理が進む

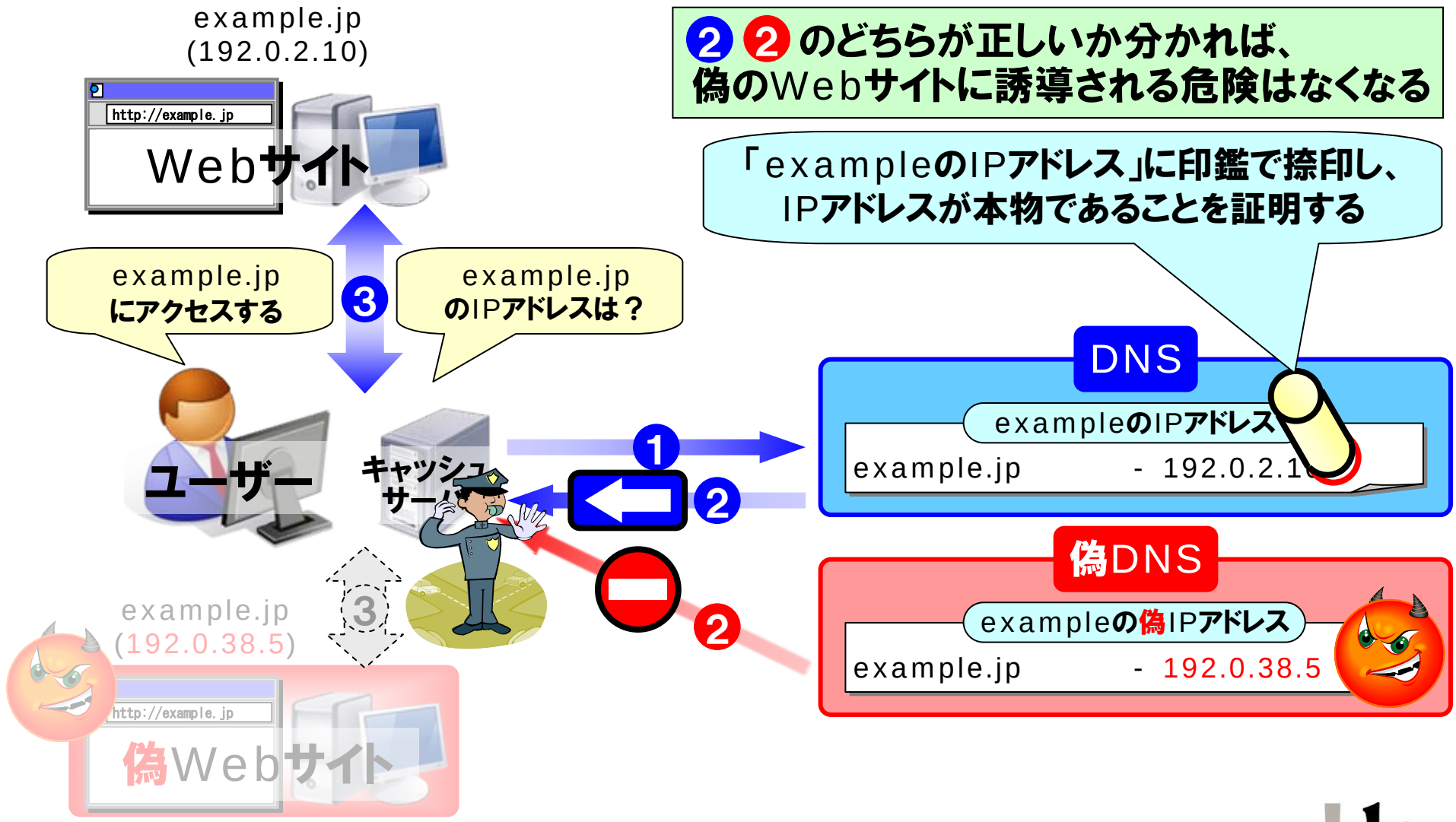
DNSを悪用したフィッシングの手口

「偽DNS」からの返事の❷を
本物の❷と思って受け取ってしまうと、
ユーザーが何も気がつかないまま❸で、
「偽Webサイト」にアクセスし、ID、パスワード
などの個人情報を入力し、盗まれてしまう



偽Webサイトのアドレスも本物と同じ「example.jp」が
見えるので、アドレスを見てもユーザーは異変に気づくのは難しい。

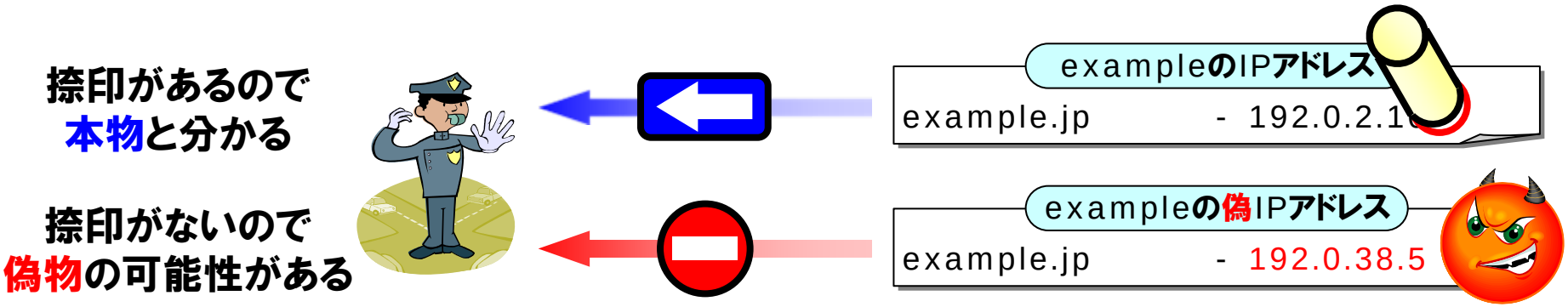
偽Webサイトに誘導されないようにするには？



DNSSECとは

DNSSEC(DNS Security Extensions)

- **DNSに登録されているIPアドレスが本物かどうかを判断する仕組み**
- **本物かどうかは、IPアドレスにある捺印でチェック**



DNSSECに必要なもの

「example.jp」の印鑑

大切に保管する
（実印のようなもの。盗まれると大変！）

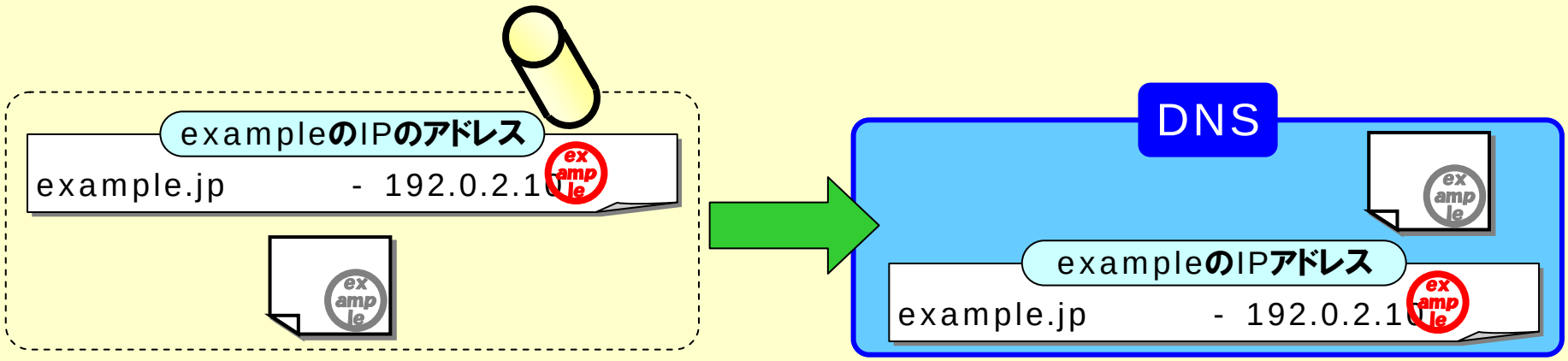
「example.jp」の印影

誰でも見ることができる
捺印が正しいかのチェックに利用

事前準備

「example.jp」の印鑑で
「example.jpのIPアドレス」に捺印する

「印影」と「捺印したIPアドレス」を
DNSに登録する



捺印と印影で本物かチェックする

example.jp
(192.0.2.10)

http://example.jp
Webサイト

DNSから「捺印のあるIPアドレス」と「印影」を受け取り、一致するかどうかをチェックする。

exampleのIPアドレ
example.jp - 192.0.2.

一致する ➡ IPアドレスは本物
一致しない ➡ IPアドレスは偽物

example.jp
にアクセスする

3

example.jp
のIPアドレス

ユーザー

キャッシュ
サーバ

1

2

DNS

exampleのIPアドレス
example.jp - 192.0.2.10

偽DNS

exampleの偽IPアドレス
example.jp - 192.0.38.5

example.jp
(192.0.38.5)

3

2

http://example.jp
偽Webサイト

「捺印」「印影」が本物とは限らない

「example.jp」の印鑑

「example.jp」の印影

「example.jp」の印鑑で捺印した
「example.jpのIPアドレス」

exampleのIPアドレス

example.jp - 192.0.2.10

「example.jp」の偽印鑑

「example.jp」の偽印影

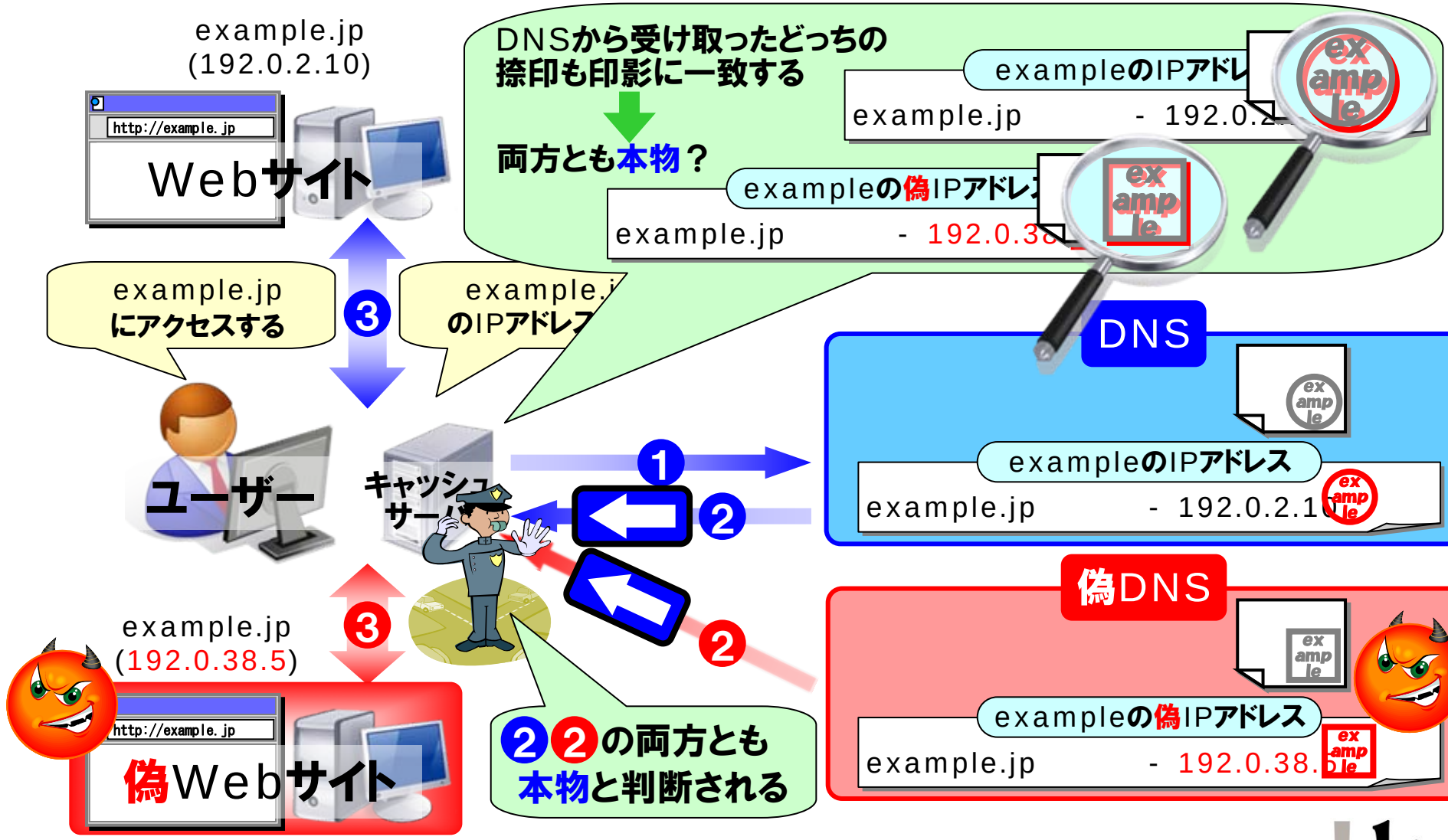
「example.jp」の偽印鑑で捺印した
「example.jpの偽IPアドレス」

exampleの偽IPアドレス

example.jp - 192.0.38.

偽Webサイトの運用者が、
「偽印鑑」、「偽印影」、偽印鑑で捺印した「偽アドレス帳」
を用意すれば、やはりユーザーは偽Webサイトへ誘導される

どっちの「印影」が本物？



「印影」にJPRSが捺印

「example.jp」の印鑑

JPRSに渡す

「example.jp」の印影

「example.jp」の印鑑で捺印した
「example.jpのIPアドレス」

exampleのIPアドレス

example.jp - 192.0.2.1

「example.jp」の偽印鑑

「example.jp」の偽印影

「example.jp」の偽印鑑で捺印した
「example.jpの偽IPアドレス」

exampleの偽IPアドレス

example.jp - 192.0.38.

JPRS

「example.jpの印影」に
「jpの印鑑」で捺印して、
JPRSがDNSに登録

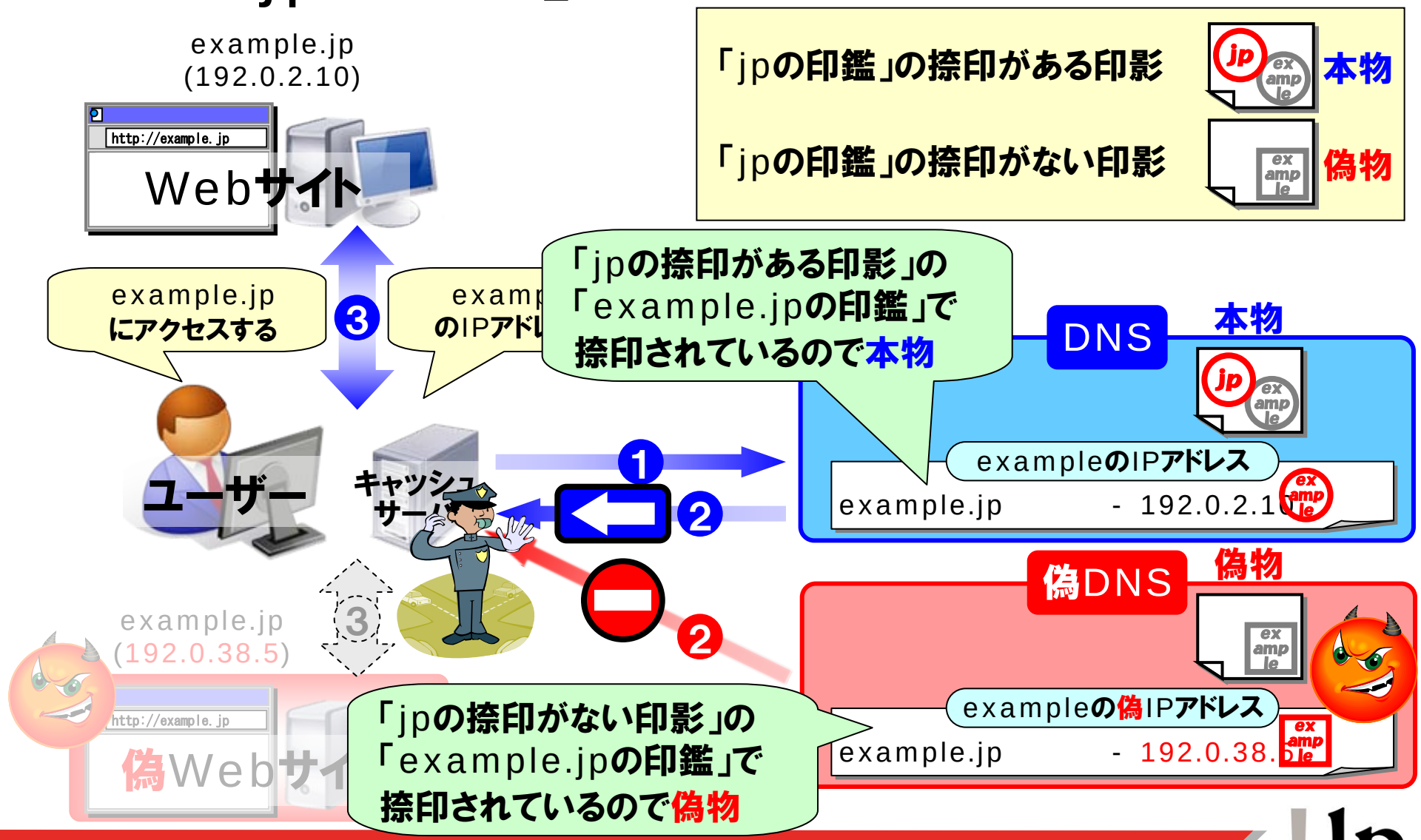
「jpの印鑑」の捺印がある印影

→ 本物の「example.jpの印影」

「jpの印鑑」の捺印がない印影

→ 偽物の「example.jpの印影」

「jpの捺印」は本物の証



まとめ

- DNSに登録されているIPアドレスが本物かどうかを判断する仕組み
- 本物かどうかは、IPアドレスにある捺印でチェック
- 捺印があっても、「jpの捺印がある印影」と一致しないと偽物と判断される