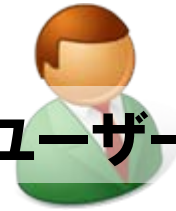
DNSSECとは

株式会社日本レジストリサービス（JPRS）

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

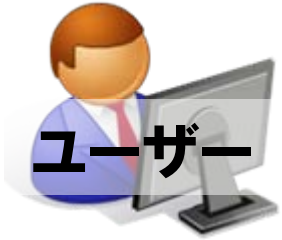


名前　**電話帳**　電話番号

- ○○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
  - www.yahoo.co.jp - 203.216.247.225
- exampleのIPアドレス
  - www.example.jp - 192.0.2.1
- 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）

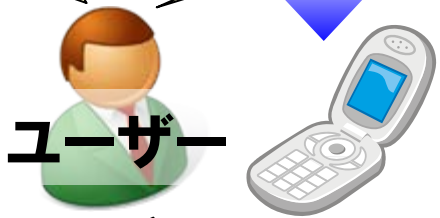
example商店
(03-3456-XXXX)

「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

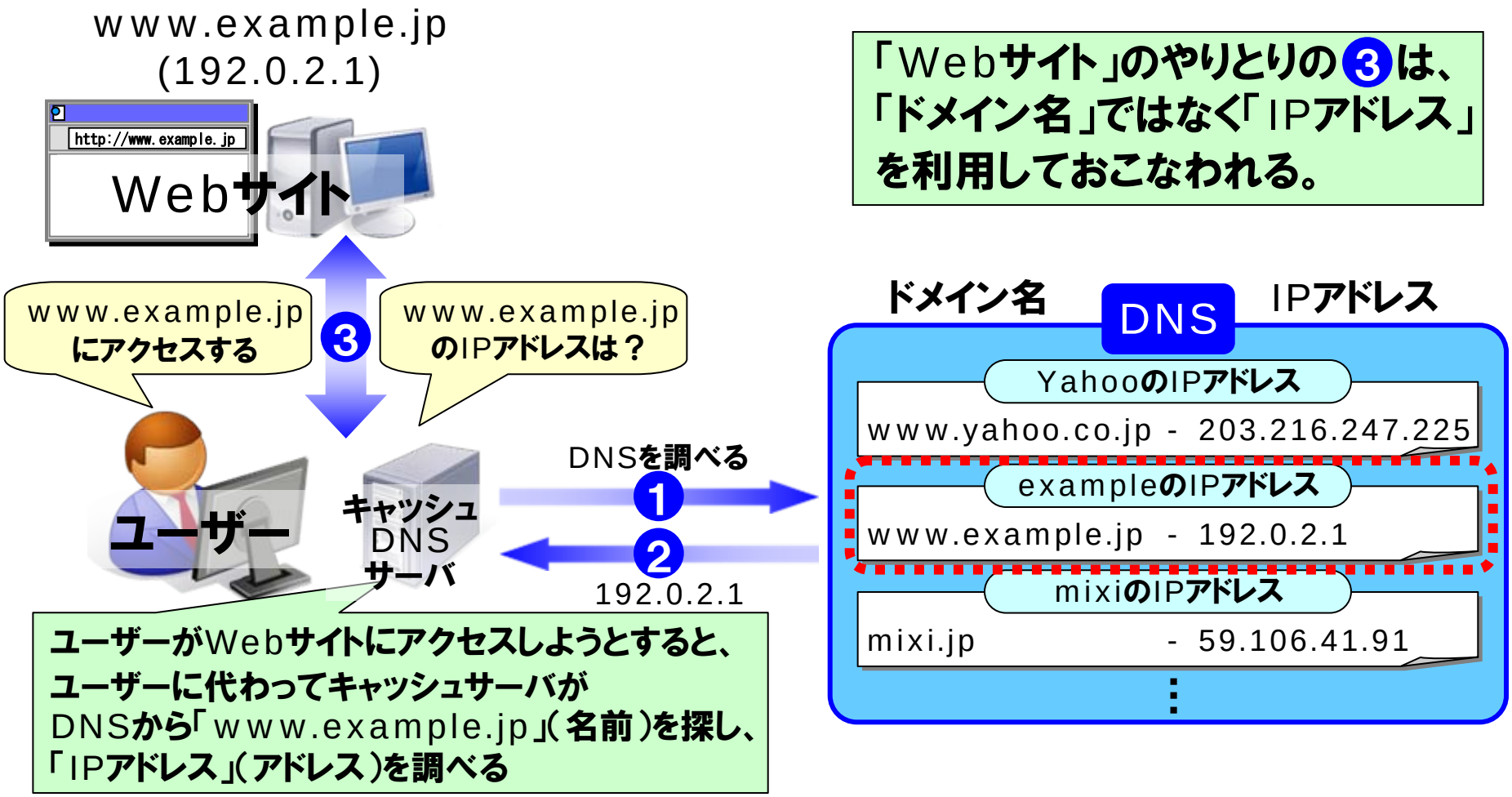
example商店の電話番号
example商店　- 03-3456-XXXX

△△△サービスの電話番号
△△△サービス　- 03-5678-XXXX

⋮

ユーザー自身がアドレス帳から
「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）



「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。

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「www.example.jp」（名前）を探し、「IPアドレス」（アドレス）を調べる

正常なアクセス（1回目）

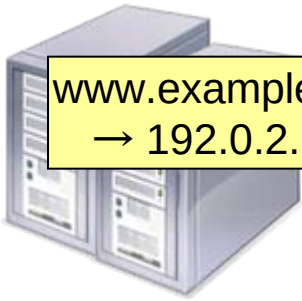
問い合わせ元

キャッシュDNSサーバ

権威DNSサーバ

① www.example.jp のIPアドレスは？

② www.example.jp のIPアドレスは？



④ www.example.jp は192.0.2.1です

③ www.example.jp は192.0.2.1です

⑤ 192.0.2.1 へ接続

受け取った応答はしばらくキャッシュされる

Webサイト

正常なアクセス（2回目以降）

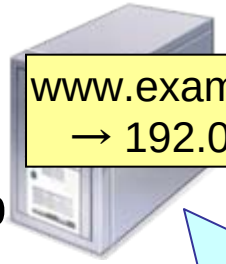
問い合わせ元

キャッシュDNSサーバ

権威DNSサーバ

① www.example.jp のIPアドレスは？

② www.example.jp は192.0.2.1です



www.example.jp → 192.0.2.1

③ 192.0.2.1 へ接続

Webサイト

以前のアクセスと情報が一致していれば、キャッシュサーバで応答する

DNSへの毒入れ攻撃

問い合わせ元

キャッシュDNSサーバ

権威DNSサーバ

② www.example.jp のIPアドレスは？

www.example.jp → 192.0.2.100

③ www.example.jp は192.0.2.100です

① www.example.jp は192.0.2.100です

④ 192.0.2.100 へ接続

偽の情報をキャッシュさせる

Webサイト

フィッシングWebサイト

ISPのキャッシュDNSサーバが狙われたら…

ISPのキャッシュDNSサーバ

利用者全員が
被害に会う

DNS毒入れ攻撃の特徴

- ユーザが正常なアクセスを行っても、フィッシングサイトに誘導される
  - 攻撃されたことに気づきにくい
- 同じキャッシュサーバのユーザ全員が影響を受ける
  - ISPのキャッシュサーバが攻撃されると被害は甚大
- 攻撃そのものの検出が容易ではない
  - キャッシュへの毒入れは、見た目は通常のDNSパケットであるため、正常な応答と攻撃の区別が簡単ではない

カミンスキー型攻撃手法の発見

- キャッシュDNSに偽IPアドレスの応答を送りフィッシングをおこなう手法は、かなり以前から認識されていた
- しかし、成功する確率が非常に小さかったため、あまり問題視されていなかった

- 2008年7月、セキュリティ研究家のダン・カミンスキー氏により、非常に効率よく偽IPアドレスの応答を送り込む方法が公開され、対応が急務となった。

毒入れへの対策

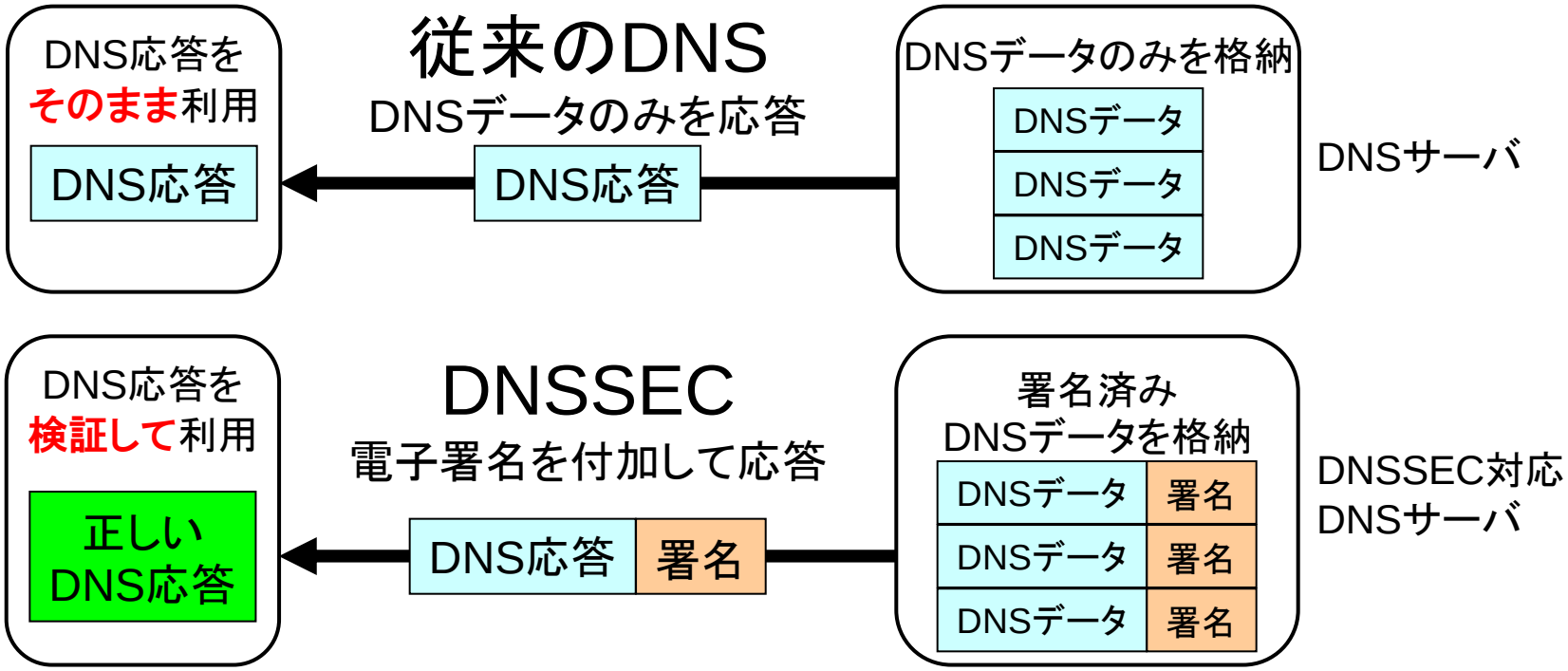
- カミンスキー型攻撃手法への対策
  - 攻撃成功確率を下げるパッチや、その手法を取り込んだ実装の採用
    ⇒ 対症療法であり、執拗な攻撃には無力
- 毒入れへの根本対策
  - DNSプロトコルそのものが持つぜい弱性であり、完全対処にはDNSのセキュリティ面でのプロトコル拡張が必要
    ⇒ このための技術が**DNSSEC**

DNSSECとは

- DNSセキュリティ拡張
（DNS SECurity Extensions）
  - 公開鍵暗号を使い、検索側が受け取ったDNSレコードの**出自・完全性**（改ざんのないこと）を検証できる仕組み
  - 従来のDNSとの**互換性を維持した拡張**
- キャッシュへの毒入れを防ぐことができる、現時点で唯一の現実解
  - 他の技術も存在するが標準化が成されていない

従来のDNS vs DNSSEC

- DNSサーバが応答に電子署名を付加し出自を保証
- 問合せ側でDNS応答の改ざんの有無を検出できる

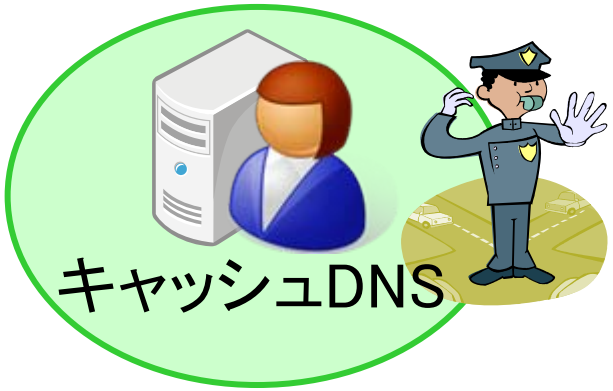


公開鍵暗号による電子署名のイメージ

印鑑 ： 自分だけが持っている ⟷ 秘 秘密鍵

印影 ： 誰でも見ることができる ⟷ 公 公開鍵

exampleのIPアドレス
example.jp - 192.0.10.100
印鑑で捺印した書類 ⟷ 署名



exampleのIPアドレス
example.jp - 192.0.10.100
印影

DNSSECで正しい応答を見分ける

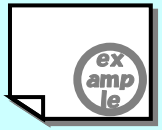
受け取った捺印と
印影を照合して
応答が正しいか
どうかを判断

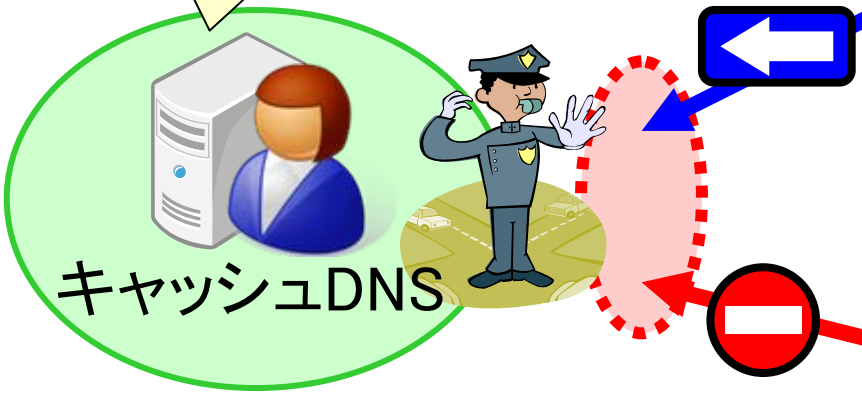
印鑑で捺印したアドレスと、
その印鑑の印影をDNSに登録する

exampleのIPアドレス

example.jp - 192.0.10.100

印影





exampleの偽IPアドレス

example.jp - 192.0.99.149

DNSSECの関係者

ユーザー

ISP

キャッシュDNS

DNSプロバイダ

権威DNS

JP DNS

JPレジストリ
データベース

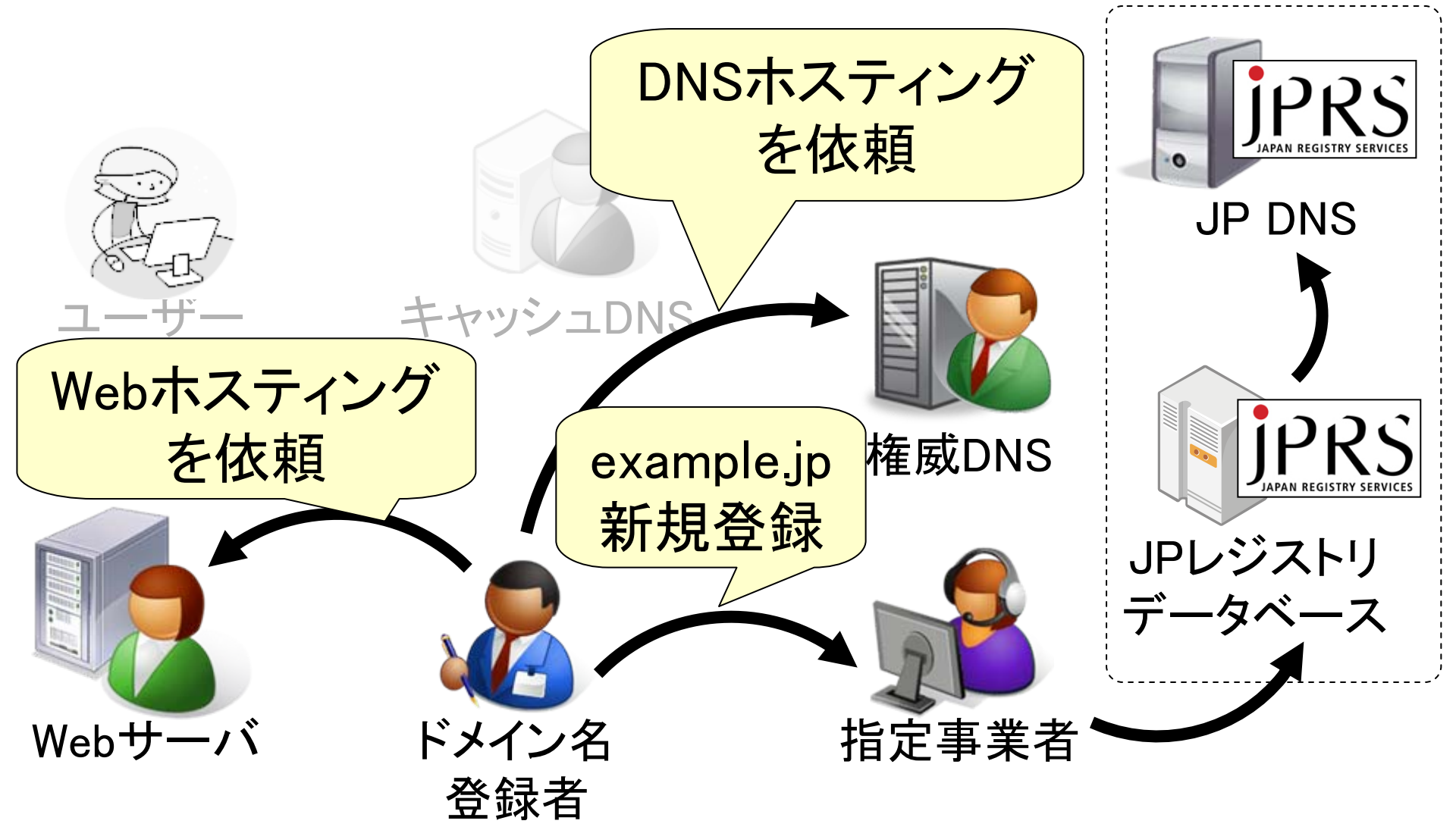
ホスティング
プロバイダ

Webサーバ

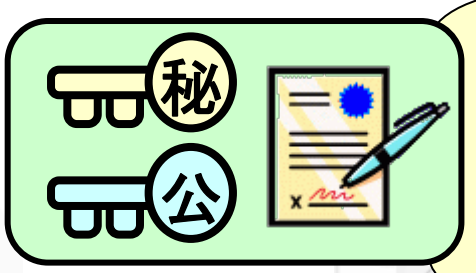
ドメイン名
登録者

指定事業者

ドメイン名利用までの流れ



DNSSEC利用までの流れ

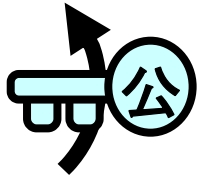


公開鍵、秘密鍵、
署名を作成し、
DNSに登録

ユーザー

キャッシュDNS

JP DNS



JPレジストリ
データベース

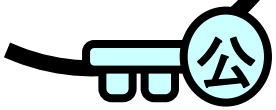
DNSSECの
申し込み

権威DNS

Webサーバ

ドメイン名
登録者

指定事業者



公開鍵の登録

DNSSECを利用したWebアクセス