2015年2月23日
第51回JPドメイン名諮問委員会
資料3

レジストリ・レジストラへの攻撃について

2015年2月23日（月）

株式会社日本レジストリサービス

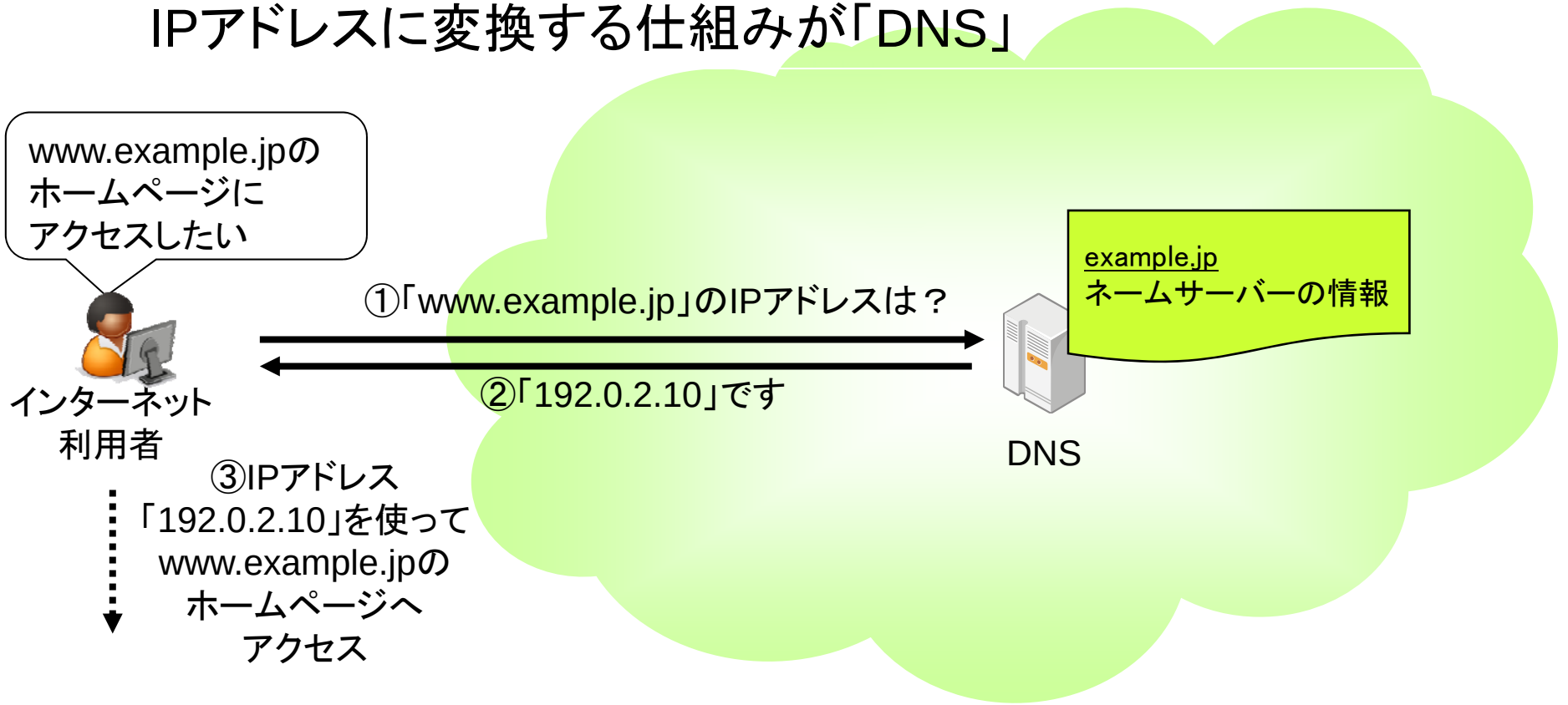
概要

- 最近、レジストリやレジストラが管理するドメイン名の登録情報に含まれるネームサーバー情報を不正に書き換える事例が、数多く発生している
- この登録情報はDNS（後述）に登録されている
- 登録情報の例
  - 登録者名
  - 公開連絡窓口
  - ネームサーバー
  - 署名鍵（DNSSEC）

```
Domain Information: [ドメイン情報]
[Domain Name]                   JPRS.JP

[登録者名]                      株式会社日本レジストリサービス
[Registrant]                    Japan Registry Services Co.,Ltd.

[Name Server]                   ns1.jprs.jp
[Name Server]                   ns2.jprs.jp
[Name Server]                   ns3.jprs.jp
[Signing Key]                   13747 8 2 (
                                DCD3F2BD0CB8A555CFC4D0866029A25C
                                4F79CEE38846DDE0A2B96AD6B6D7FD6B )
[Signing Key]                   13747 8 1 (
                                63000ECBA3DAD01FC3DFEA7DB67578DE
                                480EE0EB )

[登録年月日]                    2001/02/02
[有効期限]                      2014/02/28
[状態]                          Active
[最終更新]                      2013/03/01 01:05:07 (JST)

Contact Information: [公開連絡窓口]
[名前]                          株式会社日本レジストリサービス
[Name]                          Japan Registry Services Co.,Ltd.
[Email]                         dom-admin@jprs.co.jp
```

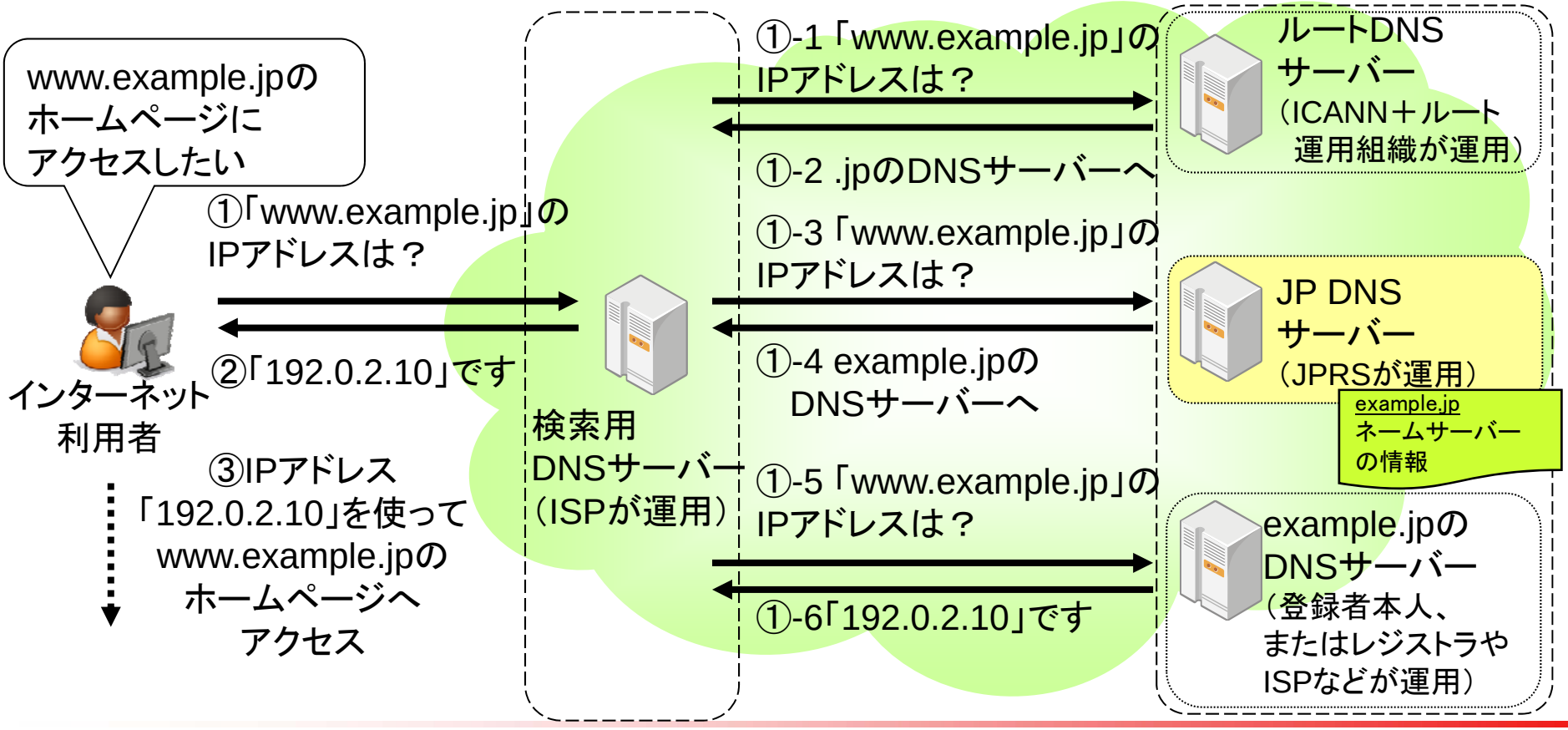
DNS:ドメイン名を利用するための仕組み

- インターネットでの通信はIPアドレスを利用
- ドメイン名をインターネット上で利用するために、対応するIPアドレスに変換する仕組みが「DNS」



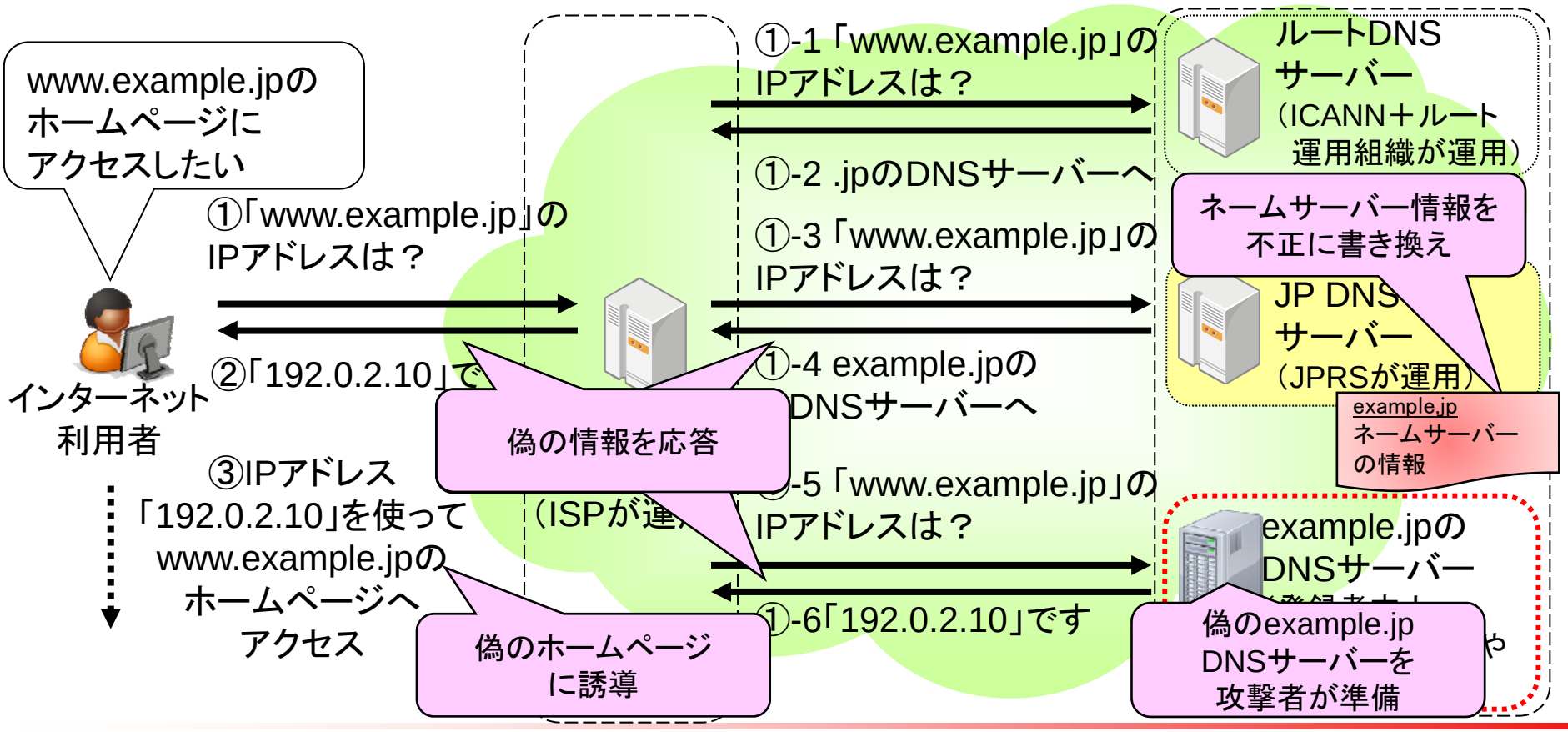
DNS：2種類のサーバー

- 2種類のDNSサーバー
  - 情報を検索するためのDNSサーバー群（キャッシュDNS）
  - 情報を公開するためのDNSサーバー群（権威DNS）
- 多数のDNSサーバーが連携して動作



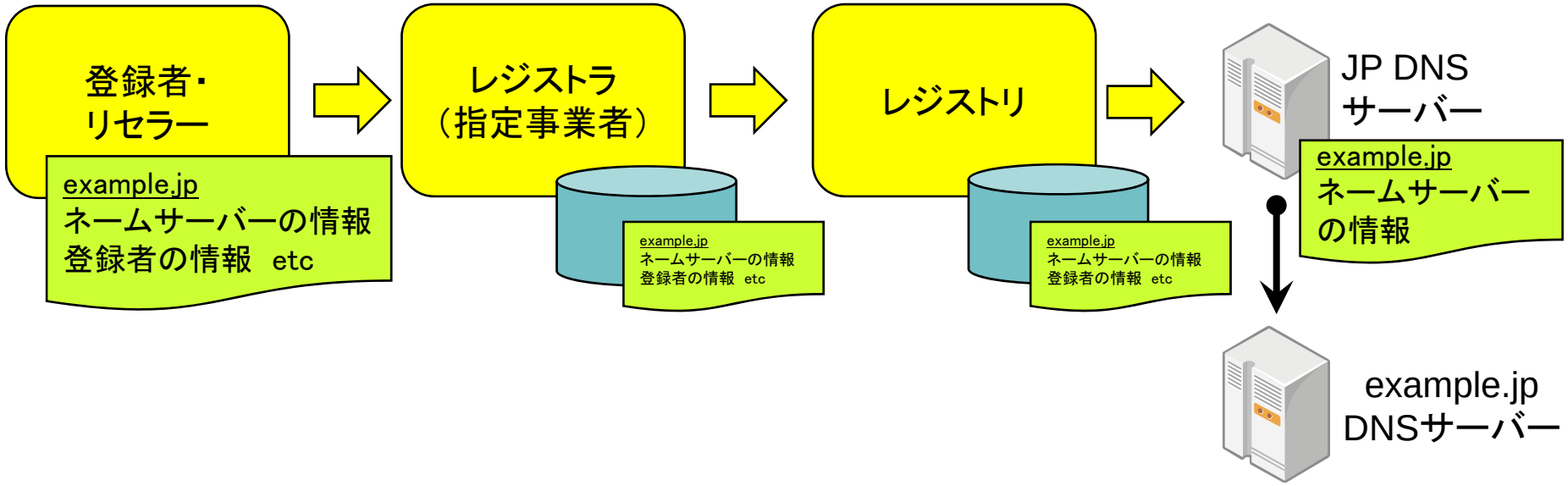
ドメイン名ハイジャック

- 登録情報に含まれるネームサーバー情報を不正に書き換え、偽のホームページに誘導



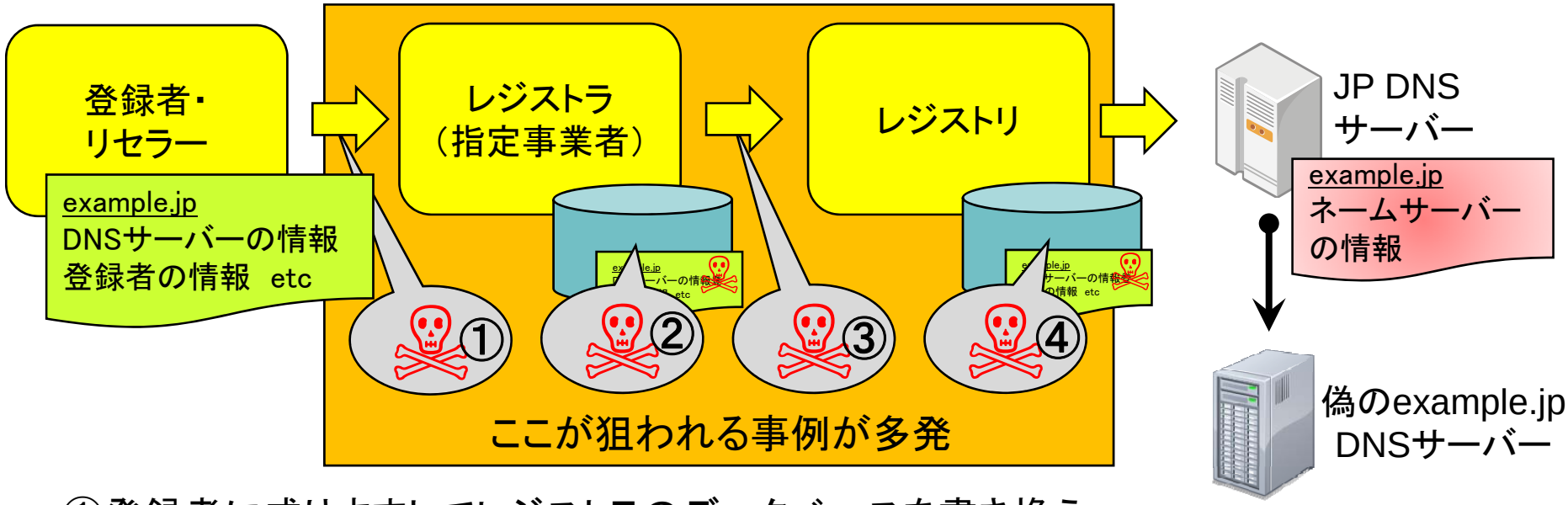
登録情報の流れ

- 登録者（リセラー）⇒レジストラ⇒レジストリ
- レジストリは登録情報をもとに権威DNSを設定



登録情報の不正な書き換え

- 流れのどこかで登録情報を不正に書き換え
- レジストリ･レジストラが狙われる事例が多発



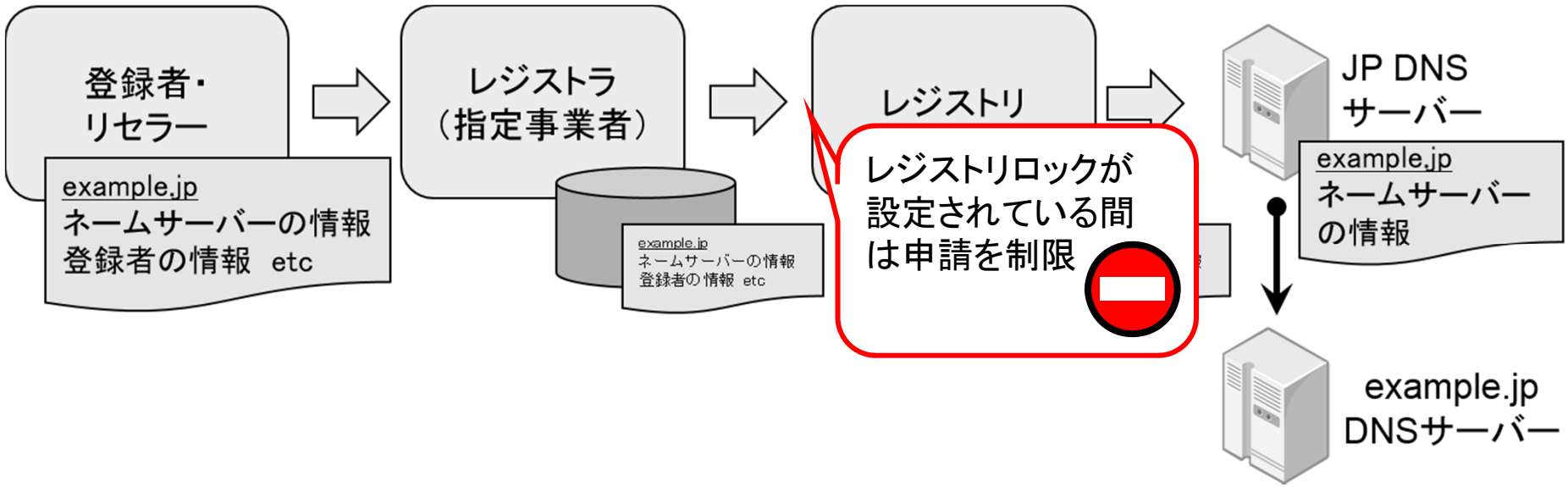
①登録者に成りすましてレジストラのデータベースを書き換え
②レジストラのシステムに不正侵入し、レジストラのデータベースを書き換え
③レジストラに成りすましてレジストリのデータベースを書き換え
④レジストリのシステムに不正侵入し、レジストリのデータベースを書き換え

JPRSの主な取り組み

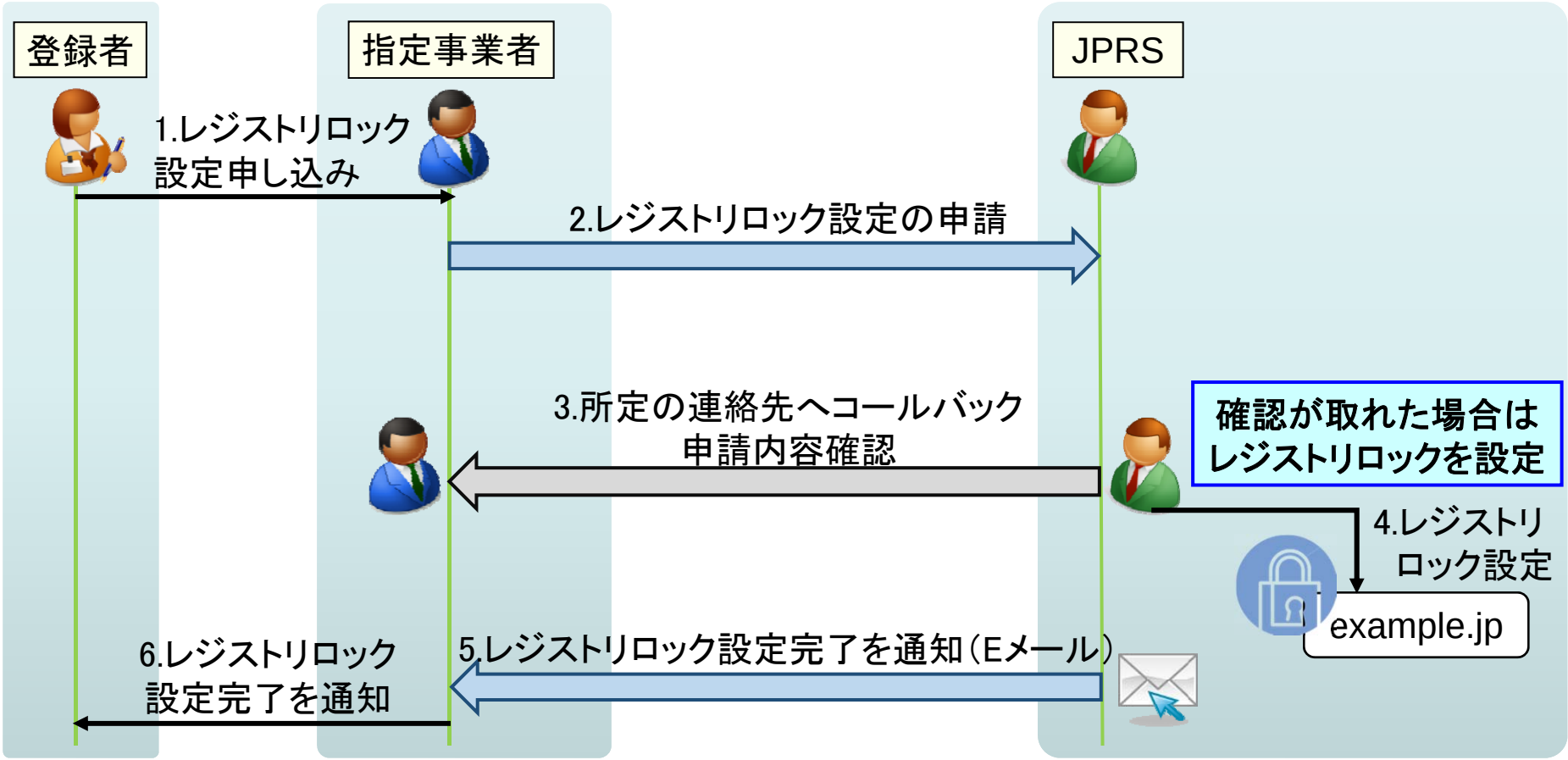
- 脆弱性情報の収集と対応
- システムの脆弱性試験と対応
- 指定事業者に認証情報管理の徹底を注意喚起
- 成りすましの事実が判明した指定事業者アカウントの緊急停止
- レジストリロックサービスの導入（後述）
- 申請インターフェースの認証強化（後述）

レジストリロックサービスの導入

- 2015年1月19日、JPドメイン名においてレジストリロックサービス導入
  - ドメイン名の登録情報（登録者の氏名、組織名、ネームサーバー情報など）をロックし、意図せず書き換えられることを防ぐ
  - レジストリロックの設定／解除にあたっては、所定の連絡先へのコールバックで指定事業者の本人性を確認する
  - 登録情報の変更には、そのレジストリロックを解除する手続きが必要であるため、利便性は下がるが、安全性は向上する



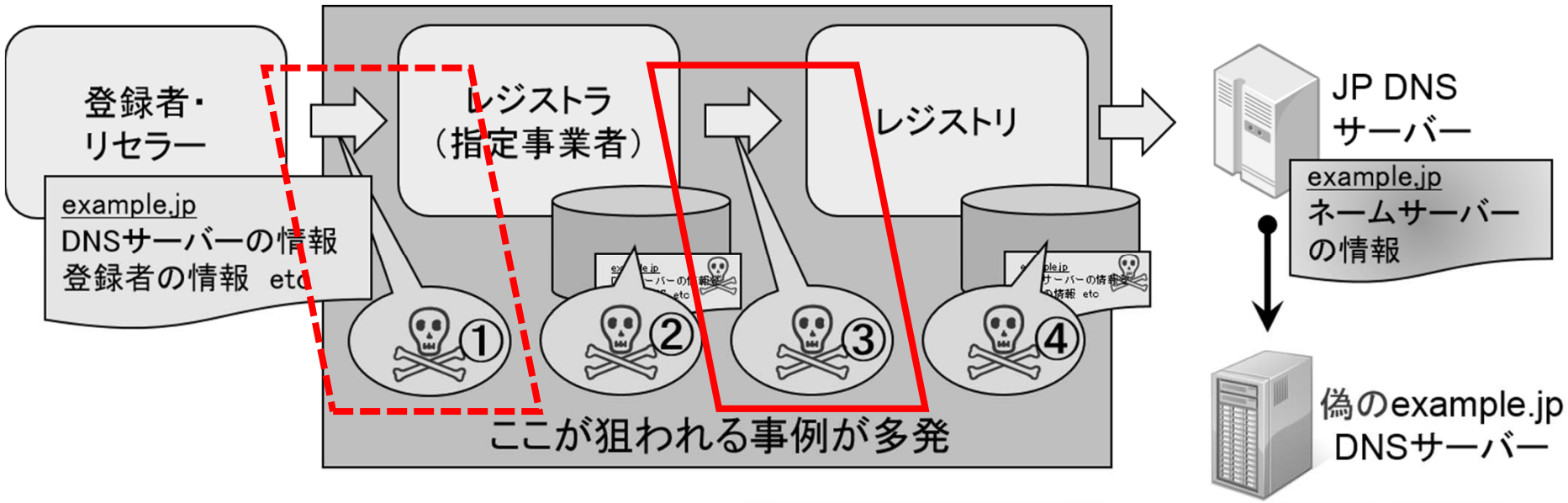
レジストリロックの設定／解除の手続き



※レジストリロックの解除手続きも同様

レジストリロックサービスで防げること

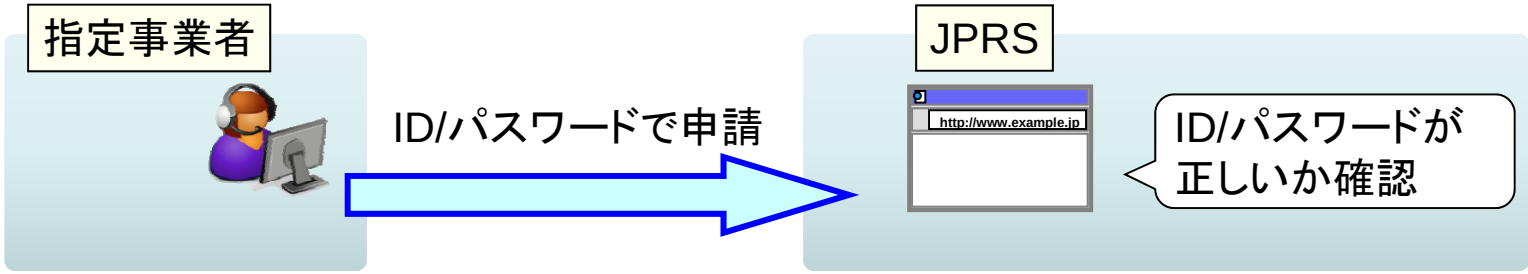
- レジストリは、レジストリロックの設定／解除を行うに当たり、指定事業者へのコールバックによる指定事業者の本人確認を行うことで、指定事業者の意図しない書き換えを防ぐ（実線部分）
- 指定事業者は、レジストリロックの設定／解除の申し込み受け付けに当たり、登録者の本人確認を行うことで、登録者の意図しない申請を防ぐ（点線部分）
  - ➢ これらにより、全体として登録者の意図しない書き換えを防ぐ



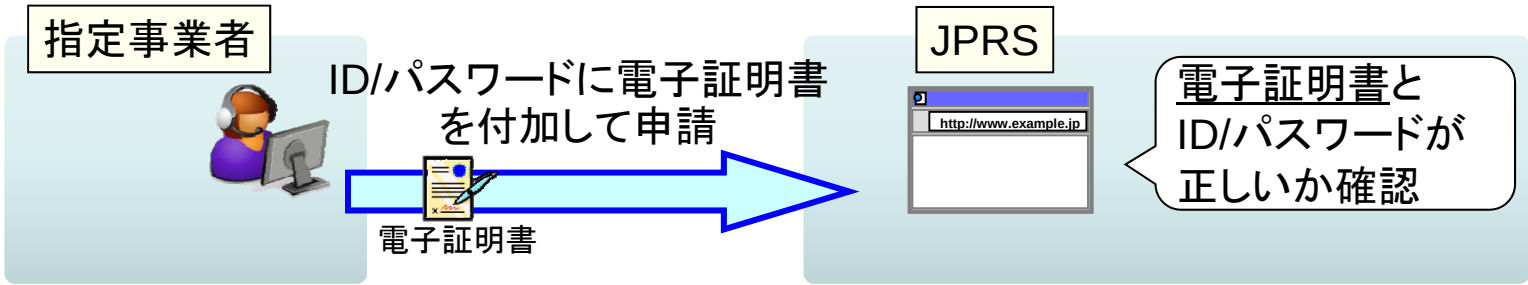
申請インターフェースの認証強化

- 2014年11月3日、従来のID/パスワードによる認証に加え、電子証明書による認証を実施することで指定事業者の認証を強化し、第三者が指定事業者に成りすますことを防止
  - ID/パスワードは人が記憶できる範囲の情報であるため、推測・漏洩のリスクがある
  - 電子証明書の偽造は困難であるため、セキュリティの強化になる

申請I/F（電子証明書認証なし）※2016年4月17日をもって提供終了予定



申請I/F（電子証明書認証あり）



申請インターフェースにおける IPアドレス制限

- 申請インターフェースにおいて申請用IPアドレス登録制度を導入し、セキュリティを確保

電子証明書あり		電子証明書なし	
申請用Web画面	申請用API	申請用Web画面	申請用API
2015年5月17日導入予定	導入済み	導入済み	導入済み
2015年5月17日導入予定	導入済み	導入済み	導入済み