

# ETJPシステムにおけるセキュリティについて

2004-07-27 ETJP PandS活動報告資料

- この文書の目的
  - ETJPシステムに関する現状を記述する
  - ETJPシステムについての
    - セキュリティ的観点からの評価・要件整理を
    - 既存のENUMモデルに照らし合わせるにより実施する

# 1 . ETJP申請情報の分類

---

- 会員情報
  - 組織情報、活動への貢献内容、責任者情報、事務連絡先情報
- ETJP番号情報
  - +8100配下の7桁以上12桁以下の任意の番号
- DNS資源情報 (NS,NAPTR,DS)
  - ETJP番号に対し設定するDNSリソースレコード
  - NS登録はTier1 DNS機能、NAPTR登録はTier2 DNS機能
  - NS登録時にはDS (DNSSEC機能) 登録を併せて行うことが可能

## 2. 関連するユーザの分類

---

- **ETJP ENUMレジストリ**
  - Tier0相当のネームサーバ運用を行う
  - e164.jpをゾーンとして使用
  - e164.arpaの委任を受けるまでの暫定運用
  - 運用実体はJPRS
- **ETJP事務局 認証局相当**
  - ETJPにおいて会員入会管理を行う
  - 会員のID/パスワードを発行
- **ETJPレジストリ Tier1 + 2 レジストリ・レジストラ相当**
  - ETJP レジストリシステム・DNSの運用・管理を行う
  - 会員に電話番号空間の割り振りを行う
  - 会員からNS設定申請を受け、処理する
  - 会員からNAPTR設定申請を受け、処理する
- **ETJP会員 Tier2レジストリ・レジストラ + レジストラント相当**
  - JPRSに対し番号空間取得の申請を行う
  - ETJP番号に対するNAPTRまたはNSレコードを登録する
  - NSレコード登録時は、会員自身でTier2 DNSを設定する

### 3.用語について

---

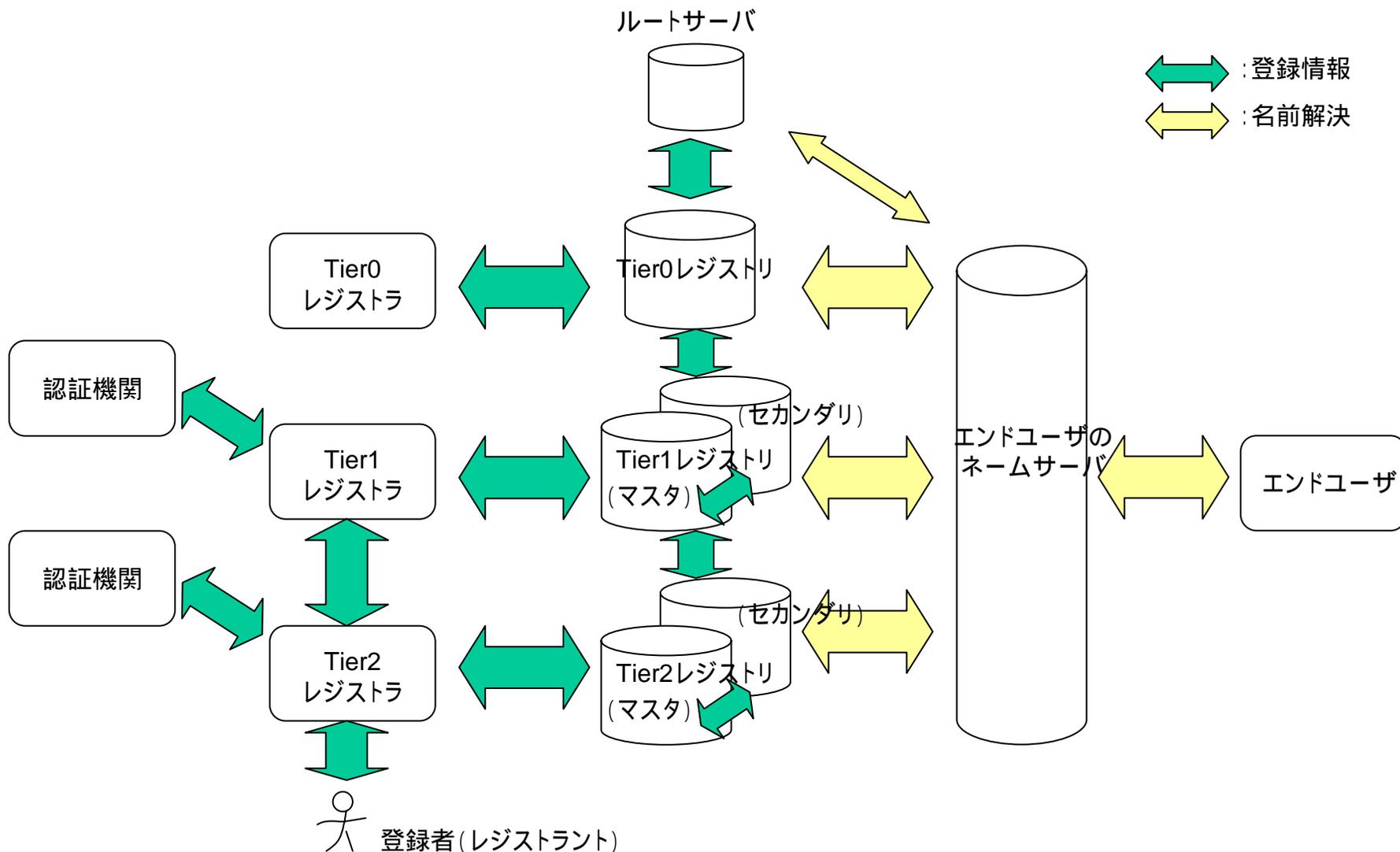
- **MUST** 要件を満たすためには実装・対応が必須
- **SHOULD** 要件を満たすためには実装・対応されるべき
- **RECOMMENDED** 要件を満たすためには実装・対応されるのが望ましい
- **MAY** 要件を満たす上で実装が行われてもよい

上のものほど要求度合いが高くなる  
基本的にはRFC2119の定義に従う

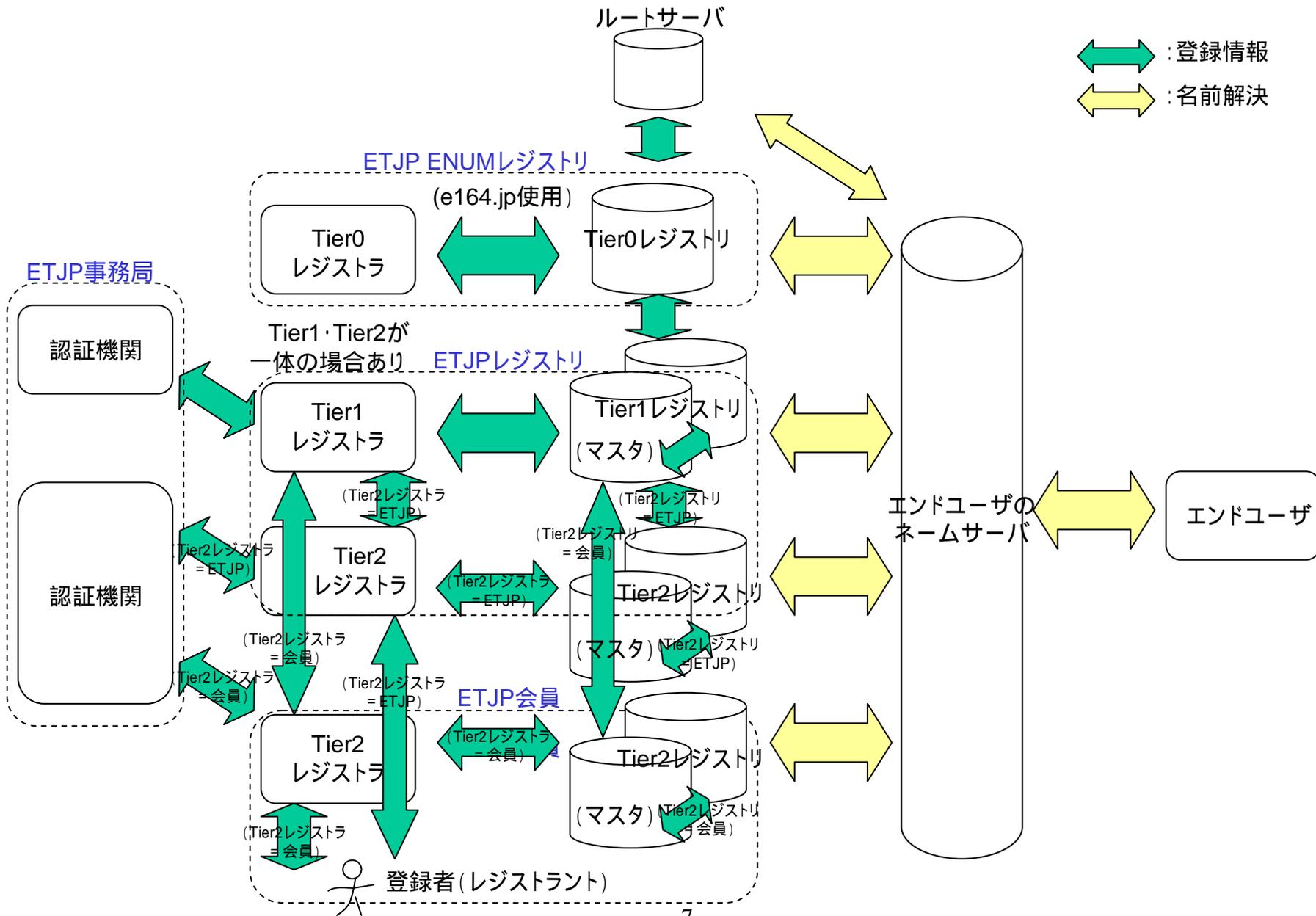
## 4. ENUMにおける役割定義について

(参考:ENUM研究G報告書 P64

米ENUMフォーラム ENUM Forum Specification for US implementation of ENUM P13-14)



# 4 - 1 . ETJPにおける役割定義について



# 5 . ETJPの役割(間)において扱う情報について

：会員情報

：ETJP番号情報、DNS資源情報

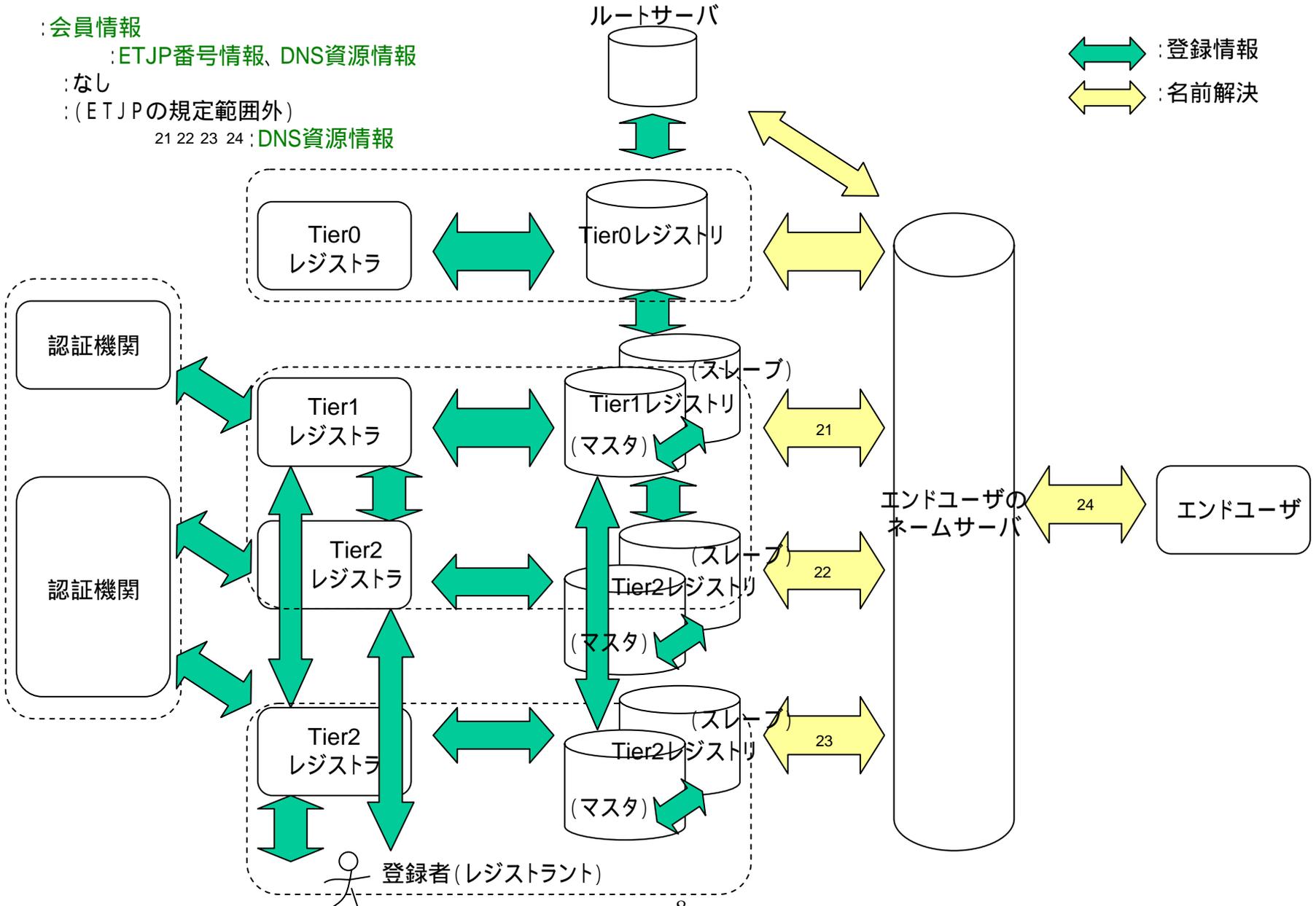
：なし

：(ETJPの規定範囲外)

21 22 23 24 :DNS資源情報

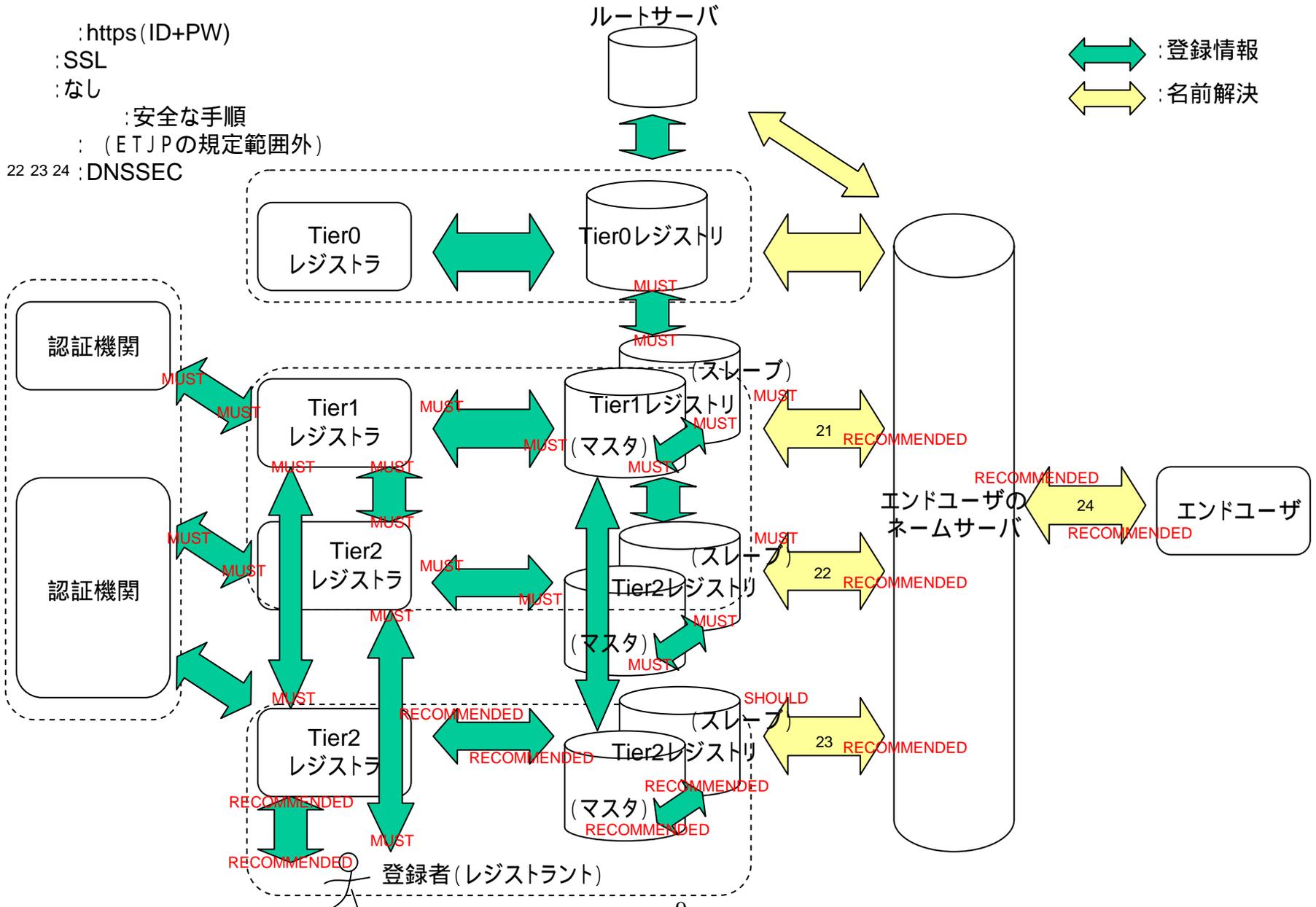
↔ :登録情報

↔ :名前解決



# 6. ETJPの役割(間)に適用するセキュリティについて

- : https (ID+PW)
- : SSL
- : なし
- : 安全な手順
- : (ETJPの規定範囲外)
- 21 22 23 24 : DNSSEC



- について、ENUM ForumではEPP/HTTPSが規定されることへの検討事項：
  - については、ETJPではユーザ認証をID・パスワードベースとし、データ通信路にhttpsを利用しているため、十分なセキュリティを有すると考える
  - については、ETJPでは同一マシン内にて実装されており、一体運用されるため、通信プロトコルとしてSSLで十分と考える
  - については、ETJPではTier0/Tier1ともにJPRSがccTLD管理のノウハウ・経験を活用し運用を行っているため、十分な安全性があると考え
- ⑳～㉒の名前解決はDNSSEC対応済みであるが、DNSSEC実装の普及状況を鑑みて、ユーザサイドでは“RECOMMENDED”扱いとする
- ㉓の名前解決についてのサーバサイドの要件は“SHOULD”に設定するが、上記と同様の理由から、各組織においては、DNSSEC実装の状況に応じて対応するものとする
- については、ENUM ForumではTSIGが規定されるが、ETJPではTier1/Tier2ともにJPRSがccTLD管理のノウハウ・経験を活用し運用を行っているため、十分な安全性があると考え
- については、特段のプロトコル規定は行わないが、ユーザ情報の漏洩、DNS資源情報の改竄防止について、各組織における十分な検討が行われることが望まれる

## 7. その他 考慮すべき項目とセキュリティ対応について

---

(参考: 米ENUMフォーラム ENUM Forum Specification for US implementation of ENUM P26)

### Tier1 (& 2) DNS (ETJP事務局保有) について

- ・物理的対処

DNSサーバ設置場所の規定/サーバ室への入室人員の制限/  
セキュリティスタッフの配置/他LANとの接続制限 など……

- ・ネットワークのセキュリティ

- ・バックアップの規定

- ・セキュリティ監査と報告

→ ETJPトライアルにおいては、

- 会員内実験運用に閉じている

- レジストリシステム、Tier0/1/2 (JPRS保有) DNSについては、  
物理的にはJPRS担当者以外立ち入ることができない場所  
において、ccTLD管理のノウハウ・経験に基づき管理されている

ため、上記要件のうち、物理的対処の一部とネットワークセキュリティのみを対象としたうえで、これら要件を満足すると考える

### Tier2 DNS (会員保有) について

→ 前項6-2において記述されるレベルでの運用が行われることで  
要件を満たすと考える