内部網でacme対応CA発行のサーバ証明書を使う

Kazunori Fujiwara, 個人
fujiwara@wide.ad.jp

Disclaimer

- この資料に書かれていることは 、CA/Browser ForumのBaseline Requirements for TLS Server Certificates の範囲外のサーバ証明書、ブラウザの使い方を示すため、使えなくなる可能性があります
- また、そのような使い方を紹介する文書を企業名つきで出すわけにはいかないため、個人名義としています
- 私個人は、WebPKI/TLS関連の研究、開発、標準化にかかわっていないため、一介の利用者として使い方を述べてみます

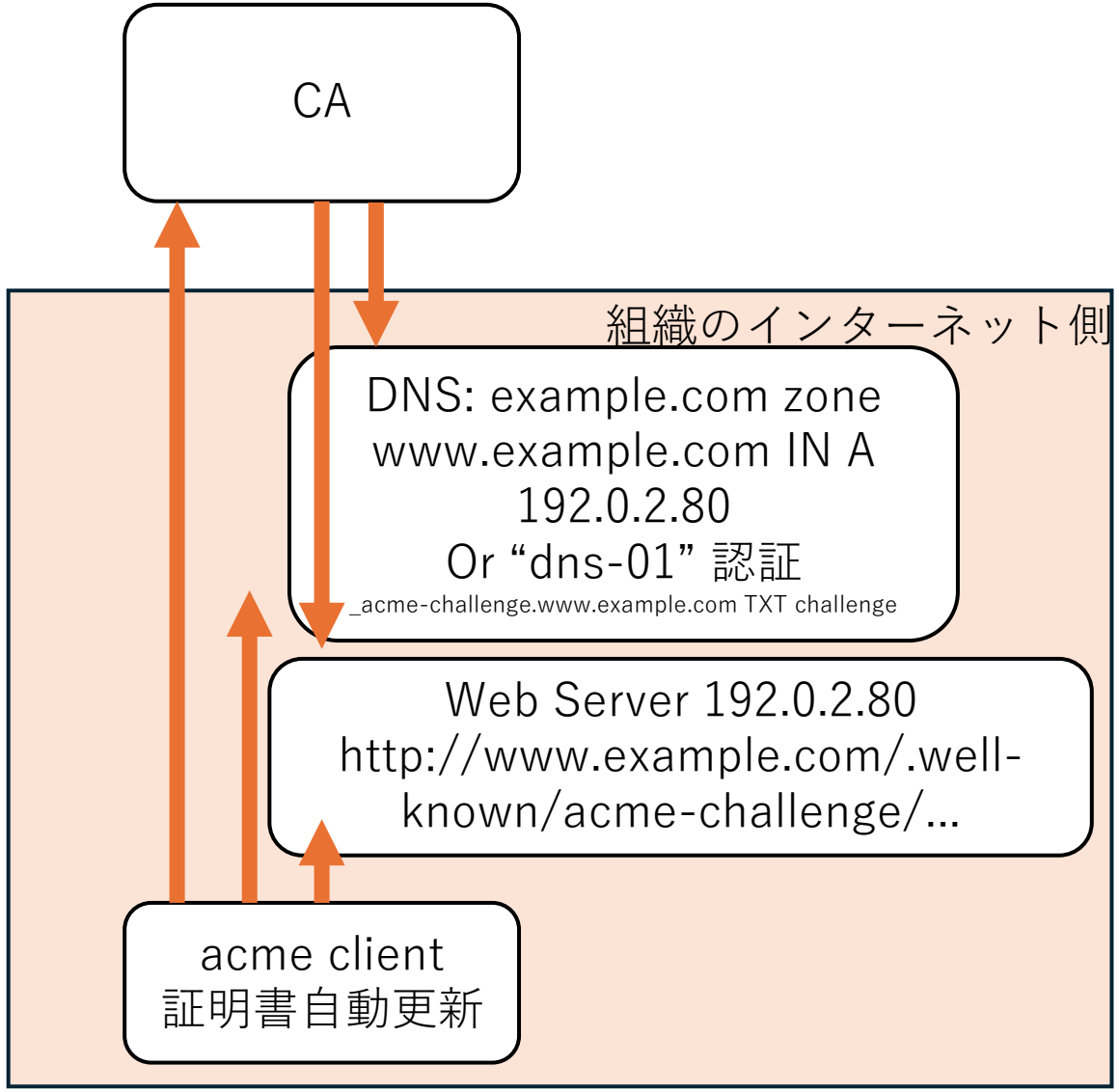
すこし背景: HTTPSのサーバ証明書

- サーバ証明書は認証局(Certificate Authority, CA)が発行する
- Webブラウザは多くのCAのルート証明書(Trust Anchor)を組み込んでいる
- CAとブラウザ開発組織などを会員とする証明書とCAの要求仕様を決める団体がCA/Browser Forum (CABF)
- CABFが決めた要求仕様がBaseline Requirements
- 証明書の最大有効期限が最大398日から200日に短縮され、2027年3月に100日、2029年3月には47日に短縮される

→ 従来、サーバ証明書は年に一度更新でよかったが、今後は毎月更新できるようにする必要がある→ 自動化必須

背景: Webサーバ証明書の自動更新

- RFC 8555 ACME: Automatic Certificate Management Environment
  - (CAがユーザを認証)
  - Key pairを作り
  - CSR作成とCAへの送信
  - ドメイン名利用権の確認
    - http-01: /.well-known/acme-challenge/ に指定されたtoken
    - dns-01: _acme-challenge TXT に指定されたtoken
  - 証明書の発行
  - 証明書の設定
- 主なソフトウェア
  - lego-cli, certbot, acme.sh, dehydrated, …



去年何度か聞いた相談

- イントラネットで使っているサーバ証明書の有効期間が短くなるらしいけど、どうすれば自動更新できるかな？
  これまでは年に一度手動で発行して入れ替えていたんだけど

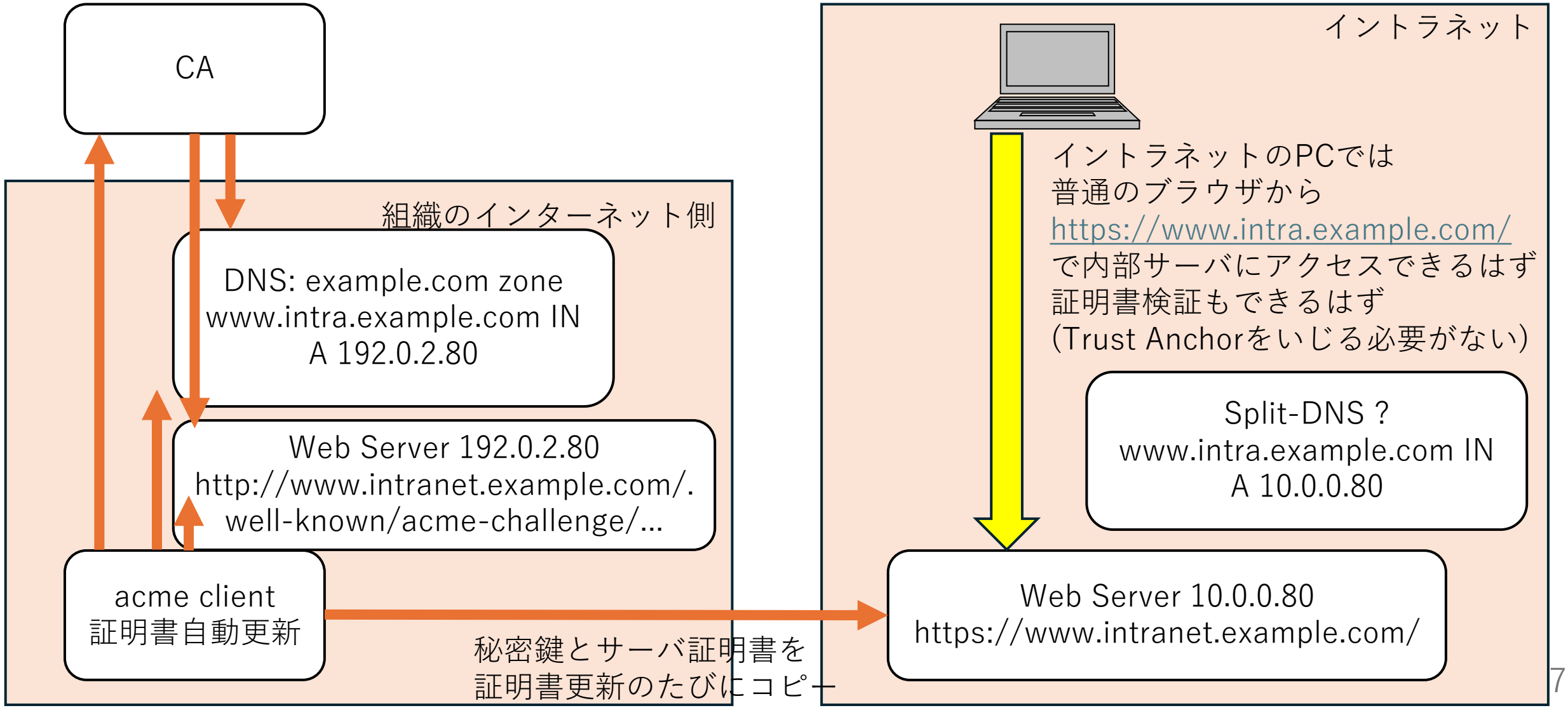
- どこで使っているか聞いた
  - 企業の内部網
  - 大学間の研究グループでVPN越し
  - 大学の内部向けサービス

条件反射的な回答

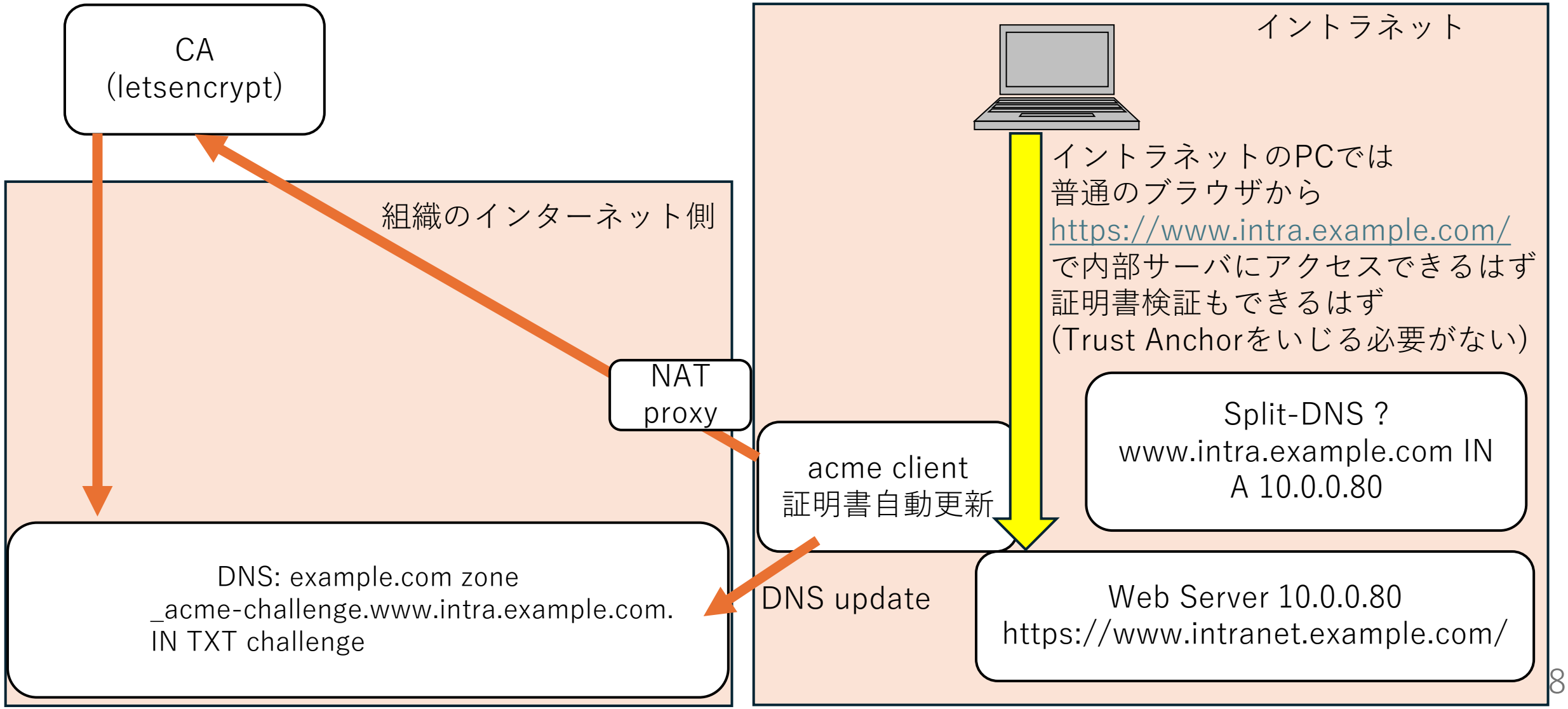
1. インターネット側で同じドメイン名のサーバを動かして
2. 自動更新の設定を行うと秘密鍵とサーバ証明書ができる
3. その秘密鍵とサーバ証明書を内部網のサーバにコピーして
4. 内部網でも同じドメイン名のサーバを動かせばいい

5. dns-01 なら、DNS Updateさえなんとかすれば、秘密鍵のコピーも不要

実装案: http-01 https://www.intra.example.com



実装案: dns-01 https://www.intra.example.com



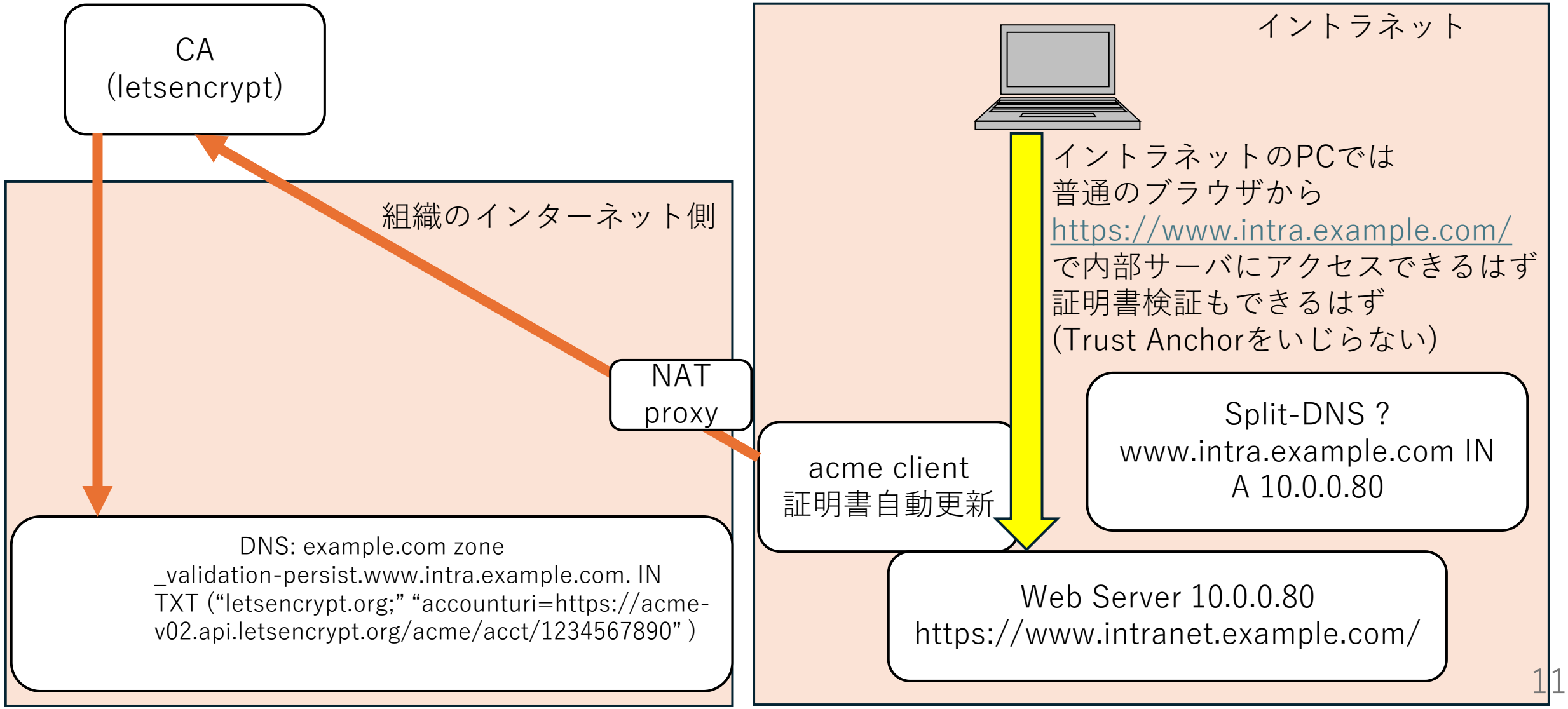
問題点

1. インターネット側で同じドメイン名のサーバを動かして
   - 内部ドメイン名は、組織のドメイン名のサブドメイン名であること
     - 無関係のドメイン名を使う場合はドメイン名登録すること
   - 内部のドメイン名が外から見える
   - 内部と外部で、同じドメイン名で別のものを指す必要がある (Split DNS)
2. 自動更新の設定を行うと秘密鍵とサーバ証明書ができる
   - CTlogに、内部で使っているドメイン名が漏洩する
3. その秘密鍵とサーバ証明書を内部網のサーバにコピーして
   - dns-01なら、コピーしない方法も考えられる
   - 秘密鍵までコピーするの？という意見あり
   - コピーのタイミング制御とか、コピーの通信方向の制御とか
4. 内部網でも同じドメイン名のサーバを動かせばいい
   - インターネット側ではできあがったサーバ証明書を使わないほうがいい

朗報: dns-persist-01

- https://letsencrypt.org/2026/02/18/dns-persist-01
  - 標準化提案: draft-ietf-acme-dns-persist-01
- ドメイン名管理者の確認方法の拡張 dns-persist-1
  - _validation-persist.ドメイン名 TXT に、CAドメイン名、acmeアカウントuriを設定
    例: _validation-persist.example.com. IN TXT (“letsencrypt.org;” “accounturi=https://acme-v02.api.letsencrypt.org/acme/acct/1234567890”)
  - acmeアカウントを作り、一度だけDNS設定しておけばよい
    - dns-01で必要なDNS Update不要
  - acmeクライアントからacmeサーバへ、NATなど経由で直接通信できれば、認証は_validation-persist TXTの記述とacme認証情報で行う
  - acmeクライアントがInternetからアクセスできなくてよく、DNSに認証キーを書かなくてよい
- Let’s Encryptは実装するらしい → acme clientにも実装される
  - dehydratedには実装されているようにみえる

dns-persist-01例: https://www.intra.example.com



ところで、、、

契約書の確認

- CA Browser Forum Baseline Requirements
  - https://cabforum.org/working-groups/server/baseline-requirements/
  - CA発行の証明書は、インターネットからアクセスできるサーバ証明書を対象としている
  - 内部向けの独自PKI基盤は対象としない
  - 2014年から、インターネットでGlobally UniqueでないInternal Nameには発行禁止
    - http-01, dns-01 は？
- CAの契約書
  - Let‘s Encrypt Subscriber Agreement
    - アカウント生成時 (register) のときに同意するもの

まとめ

- 閉域網内のサーバ証明書として、CAに発行された証明書を使い、自動更新することは可能
  - インターネット側で同じドメイン名の証明書を発行してコピー
  - dns-01 (dns-persist-01)
  - ただし、ドメイン名の存在は外から見える
- 実験レベルでは可能で、プロトコルや実装も用意されているが、実際に使う場合はサーバ証明書発行時の契約書を確認してください