

メールサーバ gmail対応 転送設定

安全に、確実にgmailに届ける

作成：Ituki Kirihara/NI

やりたいこと

受け取ったメールを、gmailにも転送したい

- 普段使うアドレスで受け取ったメールを以下に転送したい
 - gmail (スマホなどで即時確認するため)
 - PC用POP/IMAPサーバ (PCでも受信したい)
- 条件
 - gmailのアドレスは公開したくない
 - gmailには、なるべく早く届けたい

サンプル例示用アドレス

例で使うアドレス一覧

#	ドメイン	用途
1	example.com	外部向け（メアド用）ドメイン
2	example.net	内部向け（POP用）

#	メアド	用途
1	ituki@example.com	外から見た自分のアドレス
2	ituki-ex@gmail.com	転送したいgmail宛先
3	ituki@pc.example.net	PC用のメールボックス(POP/IMAP用)
4	ituki@gm.example.net	gmail用のメールボックス(POP用)

gmail固有の問題

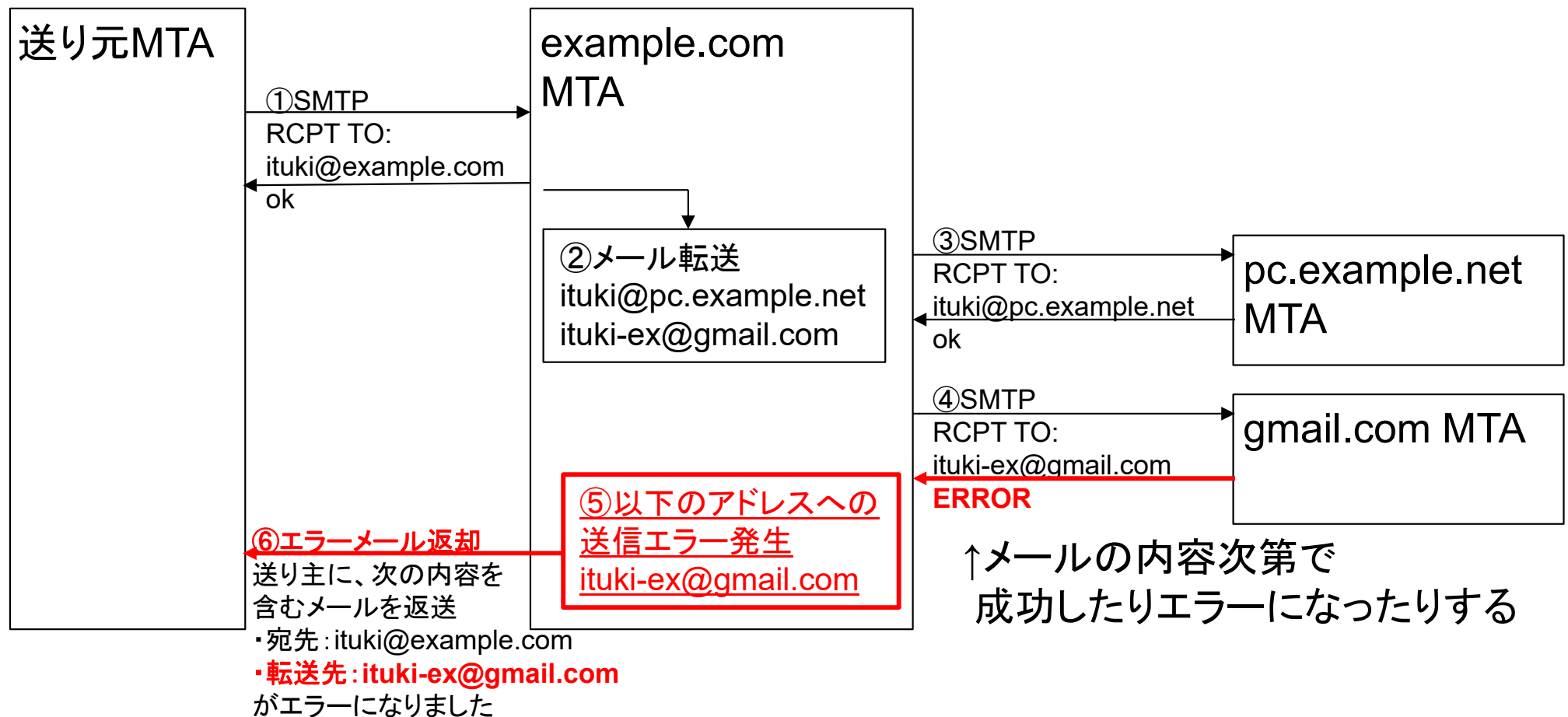
メールをgmailに送ると内容によっては拒否される
SPF,DKIM,DMARC必須化される

- 主にはウイルスなど、好ましくないとgmailが判断したメールはSMTPレベルで拒否される
 - DKIM/DMARC違反がどうなるかは不明(同じと期待)
- 拒否されたメールはデフォルトでは送り主へ返送
 - これがヤバイ

何も考えない転送の場合

例：外部公開アドレス ituki@example.com

転送先：ituki@pc.example.net、ituki-ex@gmail.com



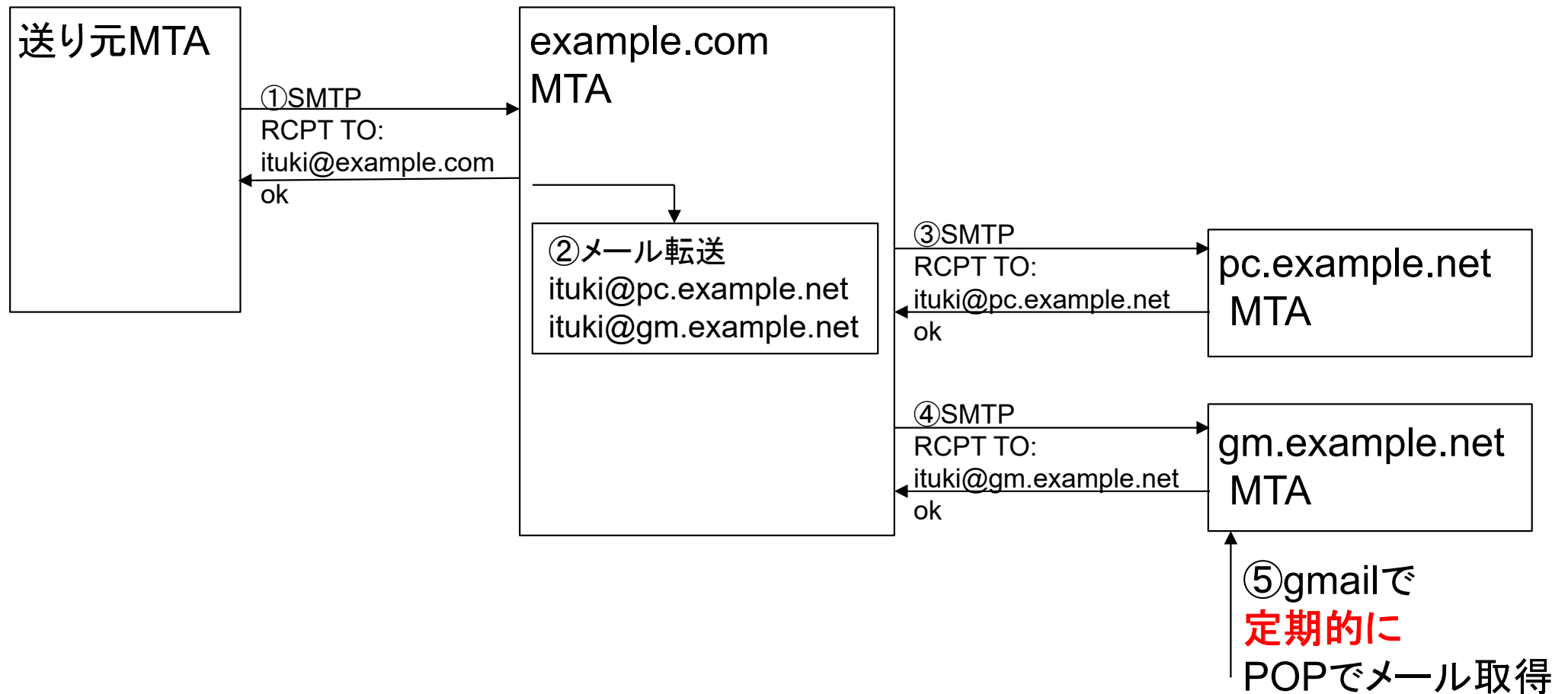
やらかしポイント

実用上もセキュリティ上もとても嫌

- ituki@pc.example.net宛てには送信済みなのに、
送り元に「送れませんでした」とメールが届く
- ituki-ex@gmail.comは隠しておきたいのに、送り元に「転送先はituki-ex@gmail.com」という情報が届く
 - gmailの転送先を知りたい攻撃者はgmailが受け取ってくれないメールを送ることで100%の確率で宛先を入手できる
- とても嫌

何も考えない解決法

Gmailにはメールを直接送らず、POPサーバを経由



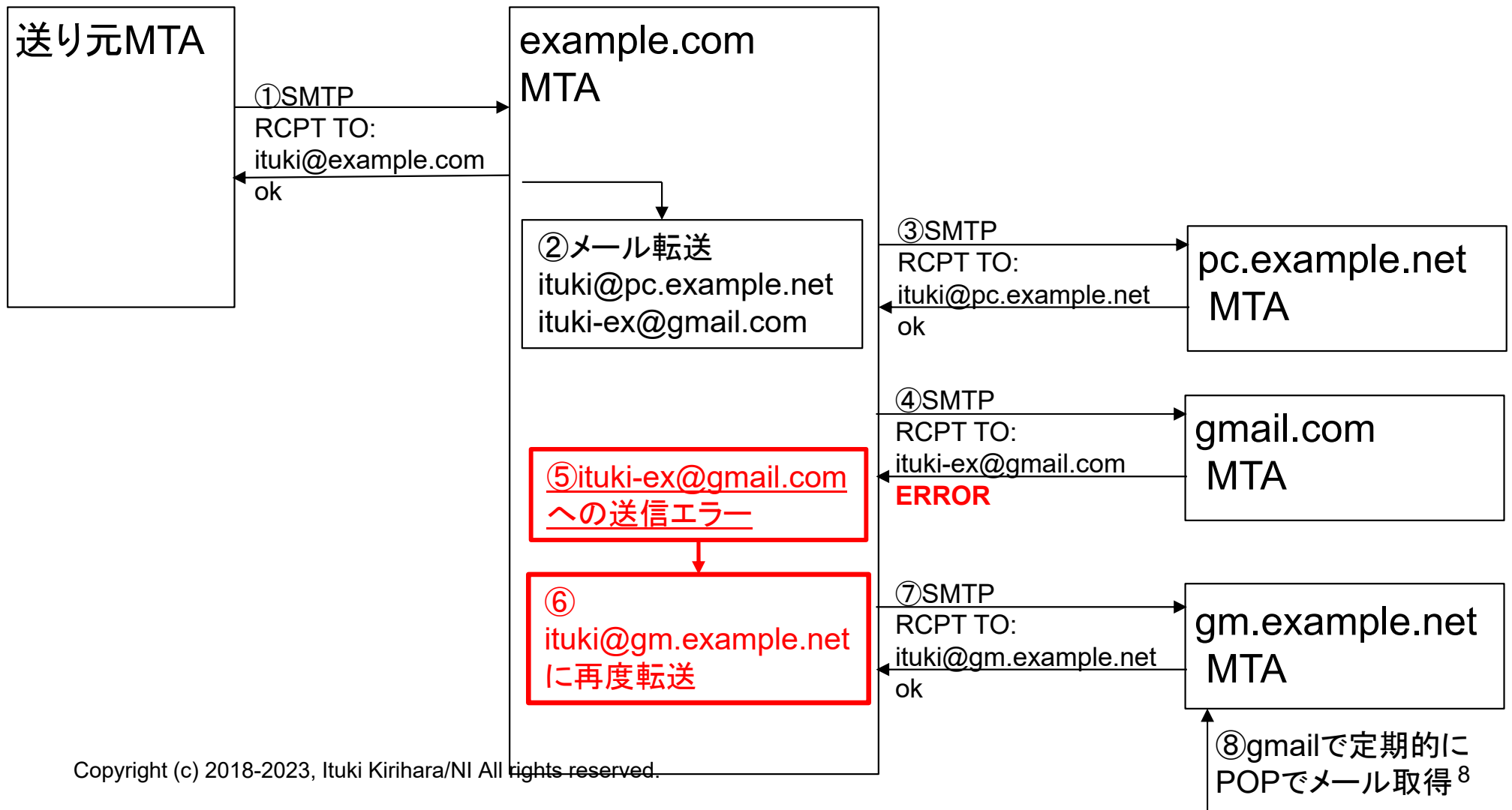
何も考えない解決法の問題

タイムラグが酷い

- タイムラグが酷い
 - gmailがPOPサーバにアクセスしに来るのは結構遅い
 - 体感的には数分～数十分感覚
 - 2ファクター認証とか、○分有効なURLを……みたいな認証系は大体受信する頃にはタイムアウトしてる
 - 手動でPOP読み込み開始指示も可能だが、めんどくさい

解決方法の概念図

Gmail宛て(ituki-ex@gmail.com)にSMTPメールを送るのに
失敗したときだけ、別のアドレスに再転送



解決方法について 利点

届けられるものは早く届く。無理なものはPOP経由で。

- 一度gmailにメール送信を試すので、そこで成功すればほぼ即時メールが届く
- gmailが一度拒否したメールはPOP経由で届く
 - ▶ gmailが拒否しても、送信者にエラーが返らない
 - ▶ メールを受信漏れが起きにくい

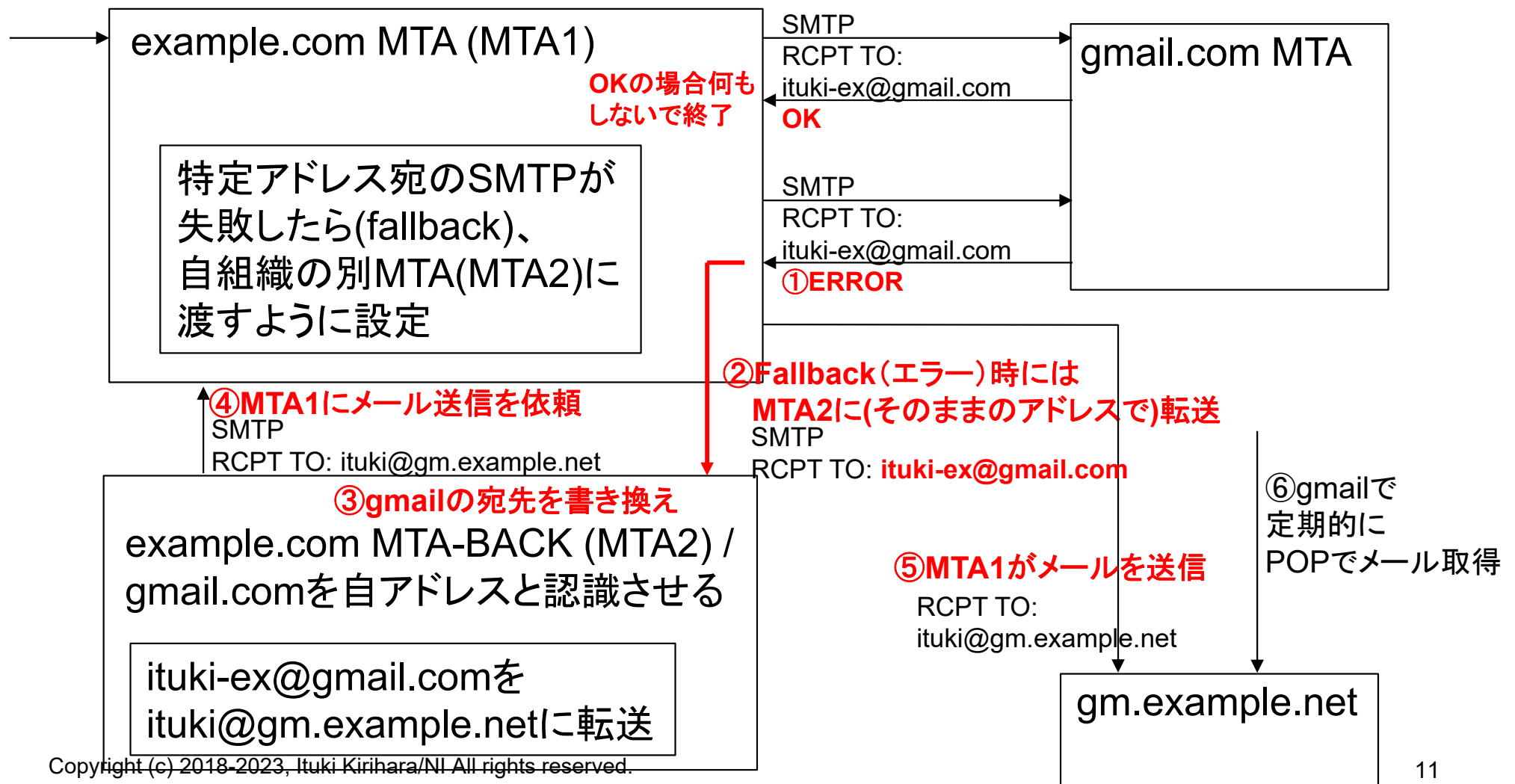
解決方法について 欠点

実際の構成はより複雑

- 実際の構成は若干面倒
 - 送信に失敗したメールを全部別のアドレスに飛ばす設定はあるが、今回は使えない
 - ①「特定のアドレス宛て」の場合に、
 - ②「通常のSMTP送信でエラー」になった場合のみ、
 - ③「宛先を別の（好きな）アドレス」に書き換える
(※宛先=RCPT TO)のは見当たらない
 - ①②③は別の機能として存在するので、それを利用する

解決方法の実構成

MTA1で特定のgmailアドレス宛のsmtpのfallbackだけを
MTA2に宛て、MTA2でforwardして、MTA1に戻す



実構成例

Postfixの場合

MTA1

master.cf

```
fbsmtp unix -- n -- smtp -o smtp_fallback_relay=127.0.0.1:8025 -o soft_bounce=yes
```

transport_maps

```
ituki-ex@gmail.com fbsmtp:
```

main.cf

DKIMの署名を行うように設定

MTA2

- ・127.0.0.1のport 8025でSMTPサーバを起動
- ・gmail.comを受信するように設定
- ・ituki-ex@gmail.comをituki@gm.example.netに転送する設定にする
- ・全てのメールを127.0.0.1のport 25(MTA1)に転送するよう設定

まとめ

特定のGmailアドレスへの送信に失敗したときだけ別の
(gmailでない) 任意のアドレスに転送した

もっと簡単な方法募集中！

END

