OpenStack Identity (Keystone)

日本 OpenStack ユーザ会

吉山 晃 <akirayoshiyama@gmail.com>

OpenStack のコンポーネント

正式名	コードネーム
OpenStack Compute	Nova
OpenStack Object Storage	Swift
OpenStack Image Service	Glance
OpenStack Dashboard	Horizon
OpenStack Identity	**Keystone**
OpenStack Quantum	Quantum

OpenStack のリリース

リリース日	リリース名	バージョン番号
2010/10/21	Austin	2010.1
2011/2/3	Bexar	2011.1
2011/4/15	Cactus	2011.2
2011/9/22	**Diablo**	**2011.3**
2012/4/5	Essex	2012.1

Keystone とは

OpenStack の各コンポーネント
(Nova, Swift, Glance, Horizon 等)の
統合認証・認可管理サービス

- それぞれ独自にユーザ認証・認可機能を実装しなくても良い!
- Diablo で正式デビュー
  (する予定だった)
  - 実際には未熟な状態でのリリースとなった(涙)

Palazzo Borgazzi のキーストーン
(Wikipedia より引用)

ユーザ認証・認可とは

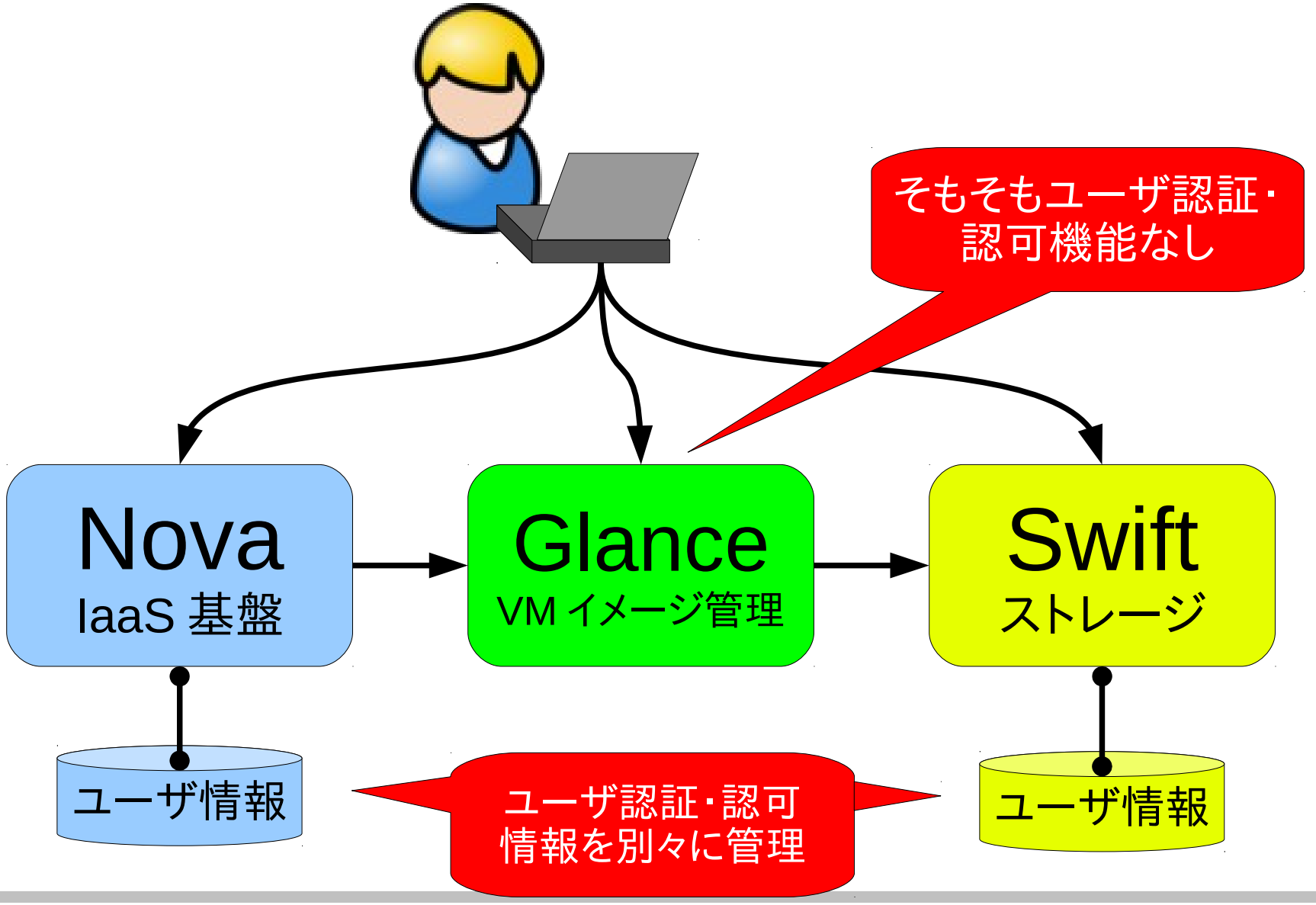
ユーザ認証（Authentication：Auth-n）

- ユーザから受け取ったリクエストが
  登録ユーザからのものである事を確認する事

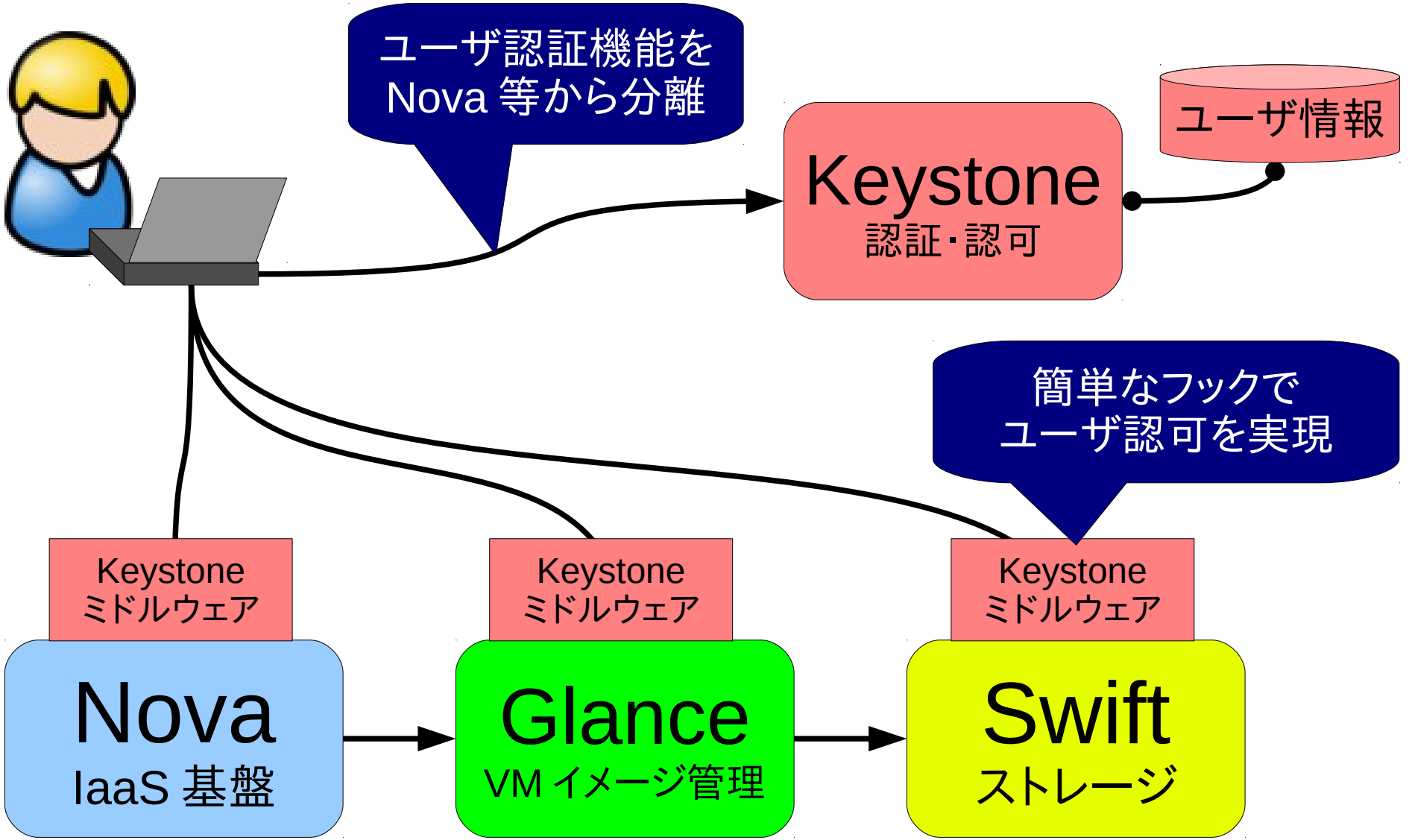
ユーザ認可（Authorization：Auth-z）

- ユーザから受け取ったリクエストについて、
  ユーザがその操作を行う権限を持っている事を
  確認する事

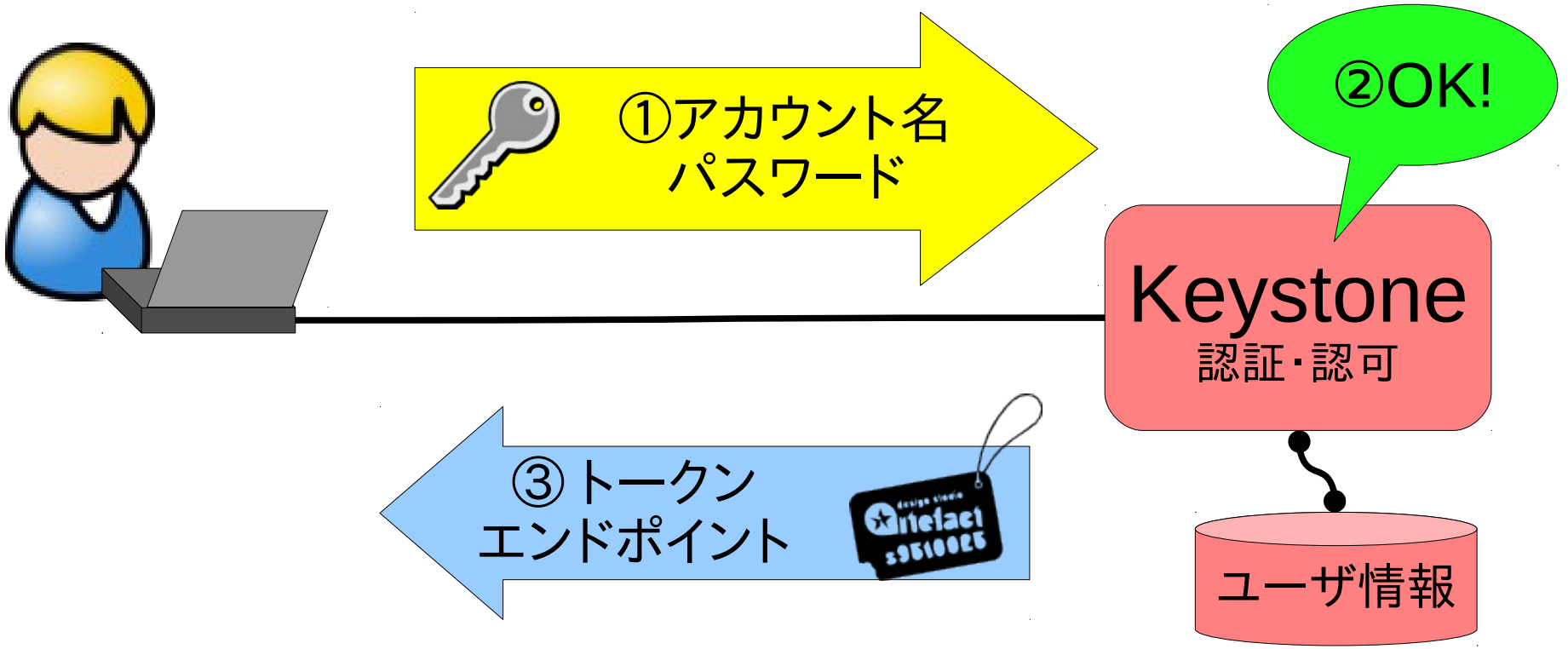
Keystone 登場以前



Keystone 登場以降



Keystone のユーザ認証



トークン、エンドポイント

トークン

- ユーザのアカウント名・パスワード情報に代わる
  ユーザを特定する為の情報（≒ COOKIE ）

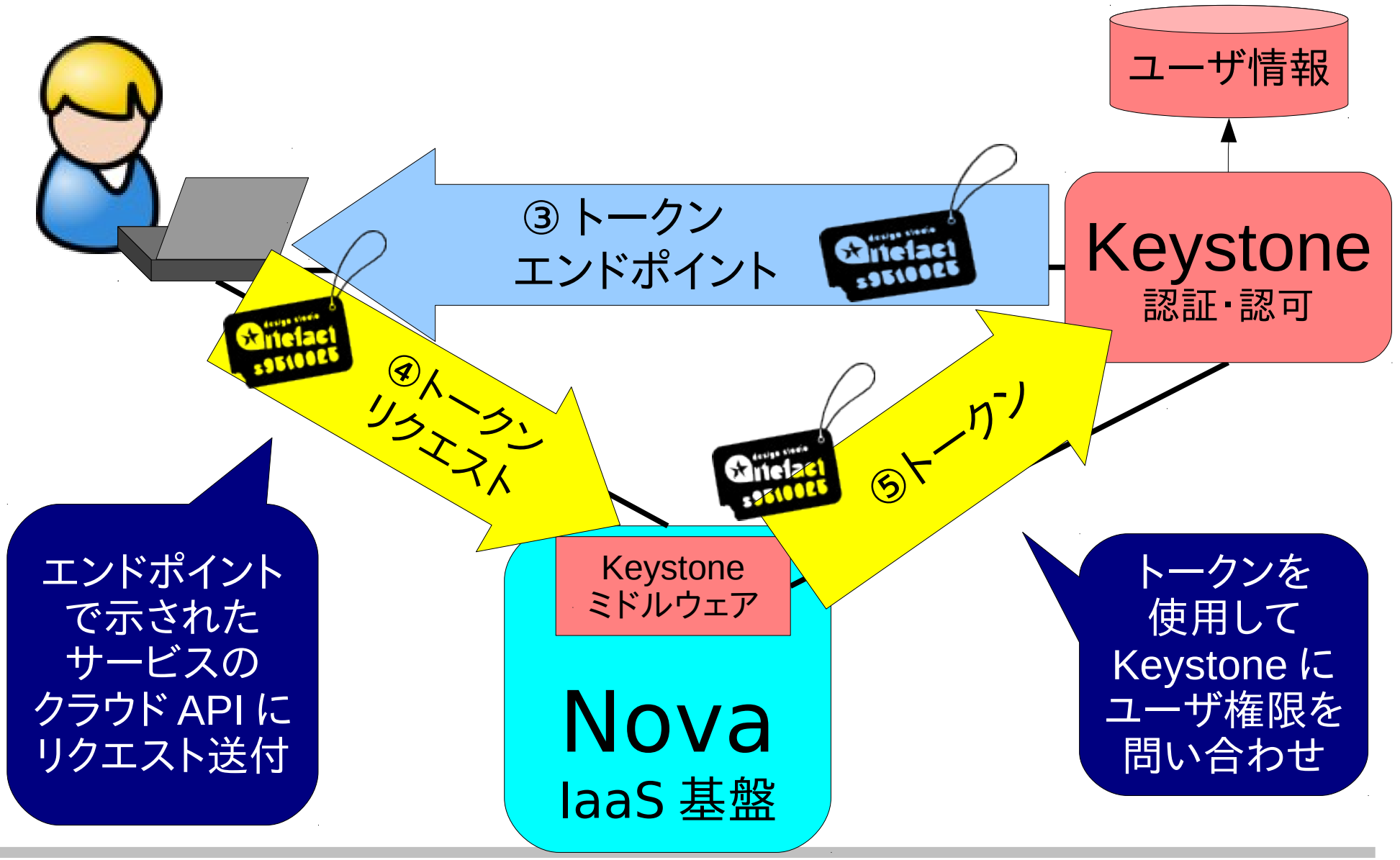
エンドポイント

- 各種サービス（ Nova 、Swift 等）が持つ
  クラウド API の URL

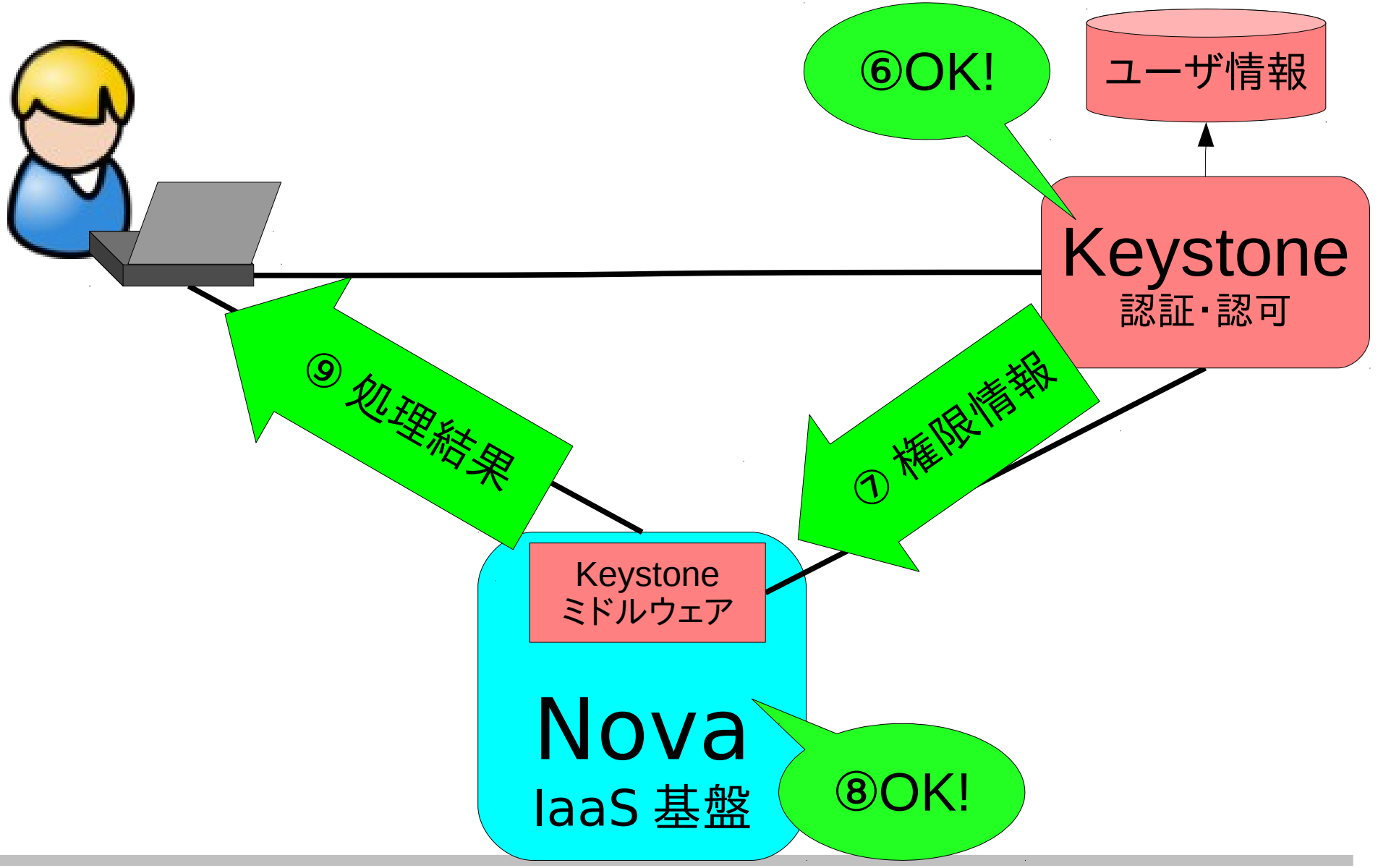
情報

ユーザ認証時に提供されるエンドポイント情報は
認証ユーザに許可されたサービス分だけ

Keystone のユーザ認可



Keystone のユーザ認可



Keystone の API

パブリック API (5000/TCP)

- 主にユーザが「認証」を行うのに使用される

管理 API (5001/TCP ⇒ 35357/TCP)

- 主に OpenStack コンポーネントが「認可」を行うのに使用される

情報

- どちらも RESTful API
- 値は JSON か XML

エンドポイント

パブリック URL

- 主にエンドユーザによるインターネット経由のアクセス用

インターナル URL

- 主に管理者や他の OpenStack コンポーネント用による LAN 経由のアクセス用

管理用 URL

- 主に管理者や他の OpenStack コンポーネント用による管理操作用

エンドポイント（続き）

サービス	サービス ID	エンドポイントテンプレート例 (パブリック URL/ 管理 URL)
Nova	nova	http://<IP アドレス>:8774/v1.1/%tenant_id% http://<IP アドレス>:8774/v1.1/%tenant_id%
Swift	swift	http://<IP アドレス>:**3333**/v1/AUTH_%tenant_id% http://<IP アドレス>:**3333**/
Glance	**glance**	***http://<IP アドレス>:9292/*** ***http://<IP アドレス>:9292/***
Keystone	identity	http://<IP アドレス>:5000/v2.0 http://<IP アドレス>:***35357***/v2.0

注意

Diablo リリース時点。今後変更になる可能性あり

Keystone の FAQ

Q. 動きません。助けて!

- Devstack で自動設定して下さい。
- 以下を確認して下さい。
  - Keystone サービスが起動しているか
  - Keystone のデータベース中の情報が正しいか
    - エンドポイントテンプレート
    - ユーザ認証・認可情報

Keystone の FAQ（続き）

Q. 動きません。助けて!

- 以下を確認して下さい。
  - 各 OpenStack コンポーネントの
    Keystone ミドルウェアの設定項目が
    Keystone サーバの管理用 API 仕様になっているか

情報

- auth_host=<Keystone サーバの IP アドレス >
- auth_port=< 通常は 35357>

Keystone の FAQ（続き）

Q. 動きません。助けて!

- 以下を確認して下さい。
  - nova,swift,glance クライアントの接続先が Nova,Swift,Glance のクラウド API になってないか（正しくは Keystone のパブリック URL ）

注意

Euca2ools 等の EC2/S3 クライアントは
従来通り Nova, Swift の EC2/S3 API にアクセス

Keystone の FAQ（続き）

Q. Keystone 使用時、Nova で Euca2ools が使えません。(Keystone Bug #869778)

- 最近まで Nova EC2 API 用 Keystone ミドルウェア (ec2_token.py) がバグっていました

Q. Keystone 使用時、Swift で Euca2ools が使えません (Keystone Bug #874280)

- Swift S3 API 用 Keystone ミドルウェアが存在しません。

情報

拙作の Swift S3 API 用 Keystone ミドルウェアを公開中

参考 URL

- OpenStack Identity Starter Guide
  http://docs.openstack.org/diablo/
  openstack-identity/admin/os-identity-starter-guide-trunk.pdf
- Keystone-manage コマンド　オンラインマニュアル
  http://keystone.openstack.org/man/keystone-manage.html
- Keystone バグレポート
  https://bugs.launchpad.net/keystone
- OpenStack API 資料
  http://docs.openstack.org/api/
- 拙作の Swift S3 API 用 Keystone ミドルウェアと関連パッチ
  http://www.debian.or.jp/~yosshy/openstack-diablo/


おぷ☆すた
Open ★ Stack