

LinuC レベル 1 Version10.0

技術解説無料セミナー

2020/06/14 開催

主題	1.10.4 「クラウドセキュリティの基礎」
副題	「クラウド環境でのLinuxインスタンスの構成」「SSHによる公開鍵の利用」を含む（1.01.1より）

セミナー担当者

河原木忠司（KAWARAGI Tadashi）

- 講師プロフィール、LinuC ver.10のご紹介
- 今回の主題についての概要
- インスタンスの作成と接続、認証
- 脅威への対策例



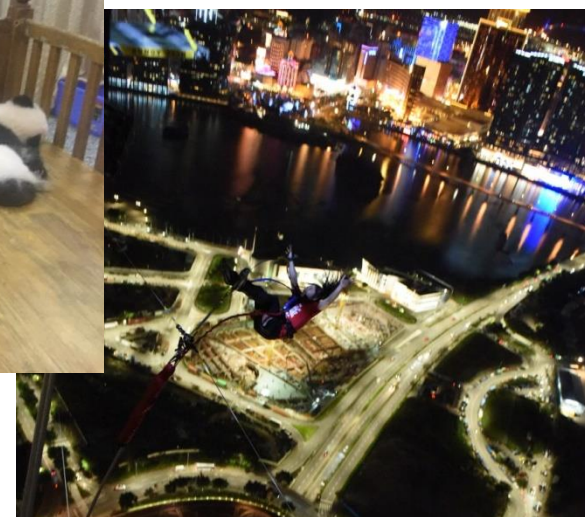
#LinuC学习中

■河原木忠司（かわらぎただし）



- 20数年ほど、講師/エンジニアとして活動しております。
- 最近は講師、研修コンサルティング、執筆業に従事させていただいております。
- サーバーインフラ系のコース、セキュリティ系のコースを中心に担当させていただいております。
 - Linuxを含むOSは専門で担当させていただいております。クラウドサービスは利用者としての立場です
- 好きなもの
 - パンダ、妻
 - うずらの卵
 - 音楽

「最短突破 LinuCレベル1 合格教本」(技術評論社)
好評発売中です。
※ver.10対応の改訂版は今夏発売予定です





#LinuC学習中

■LinuCとは

クラウド時代の即戦力エンジニアであることを証明するLinux技術者認定資格

✓現場で「今」求められている新しい技術要素に対応

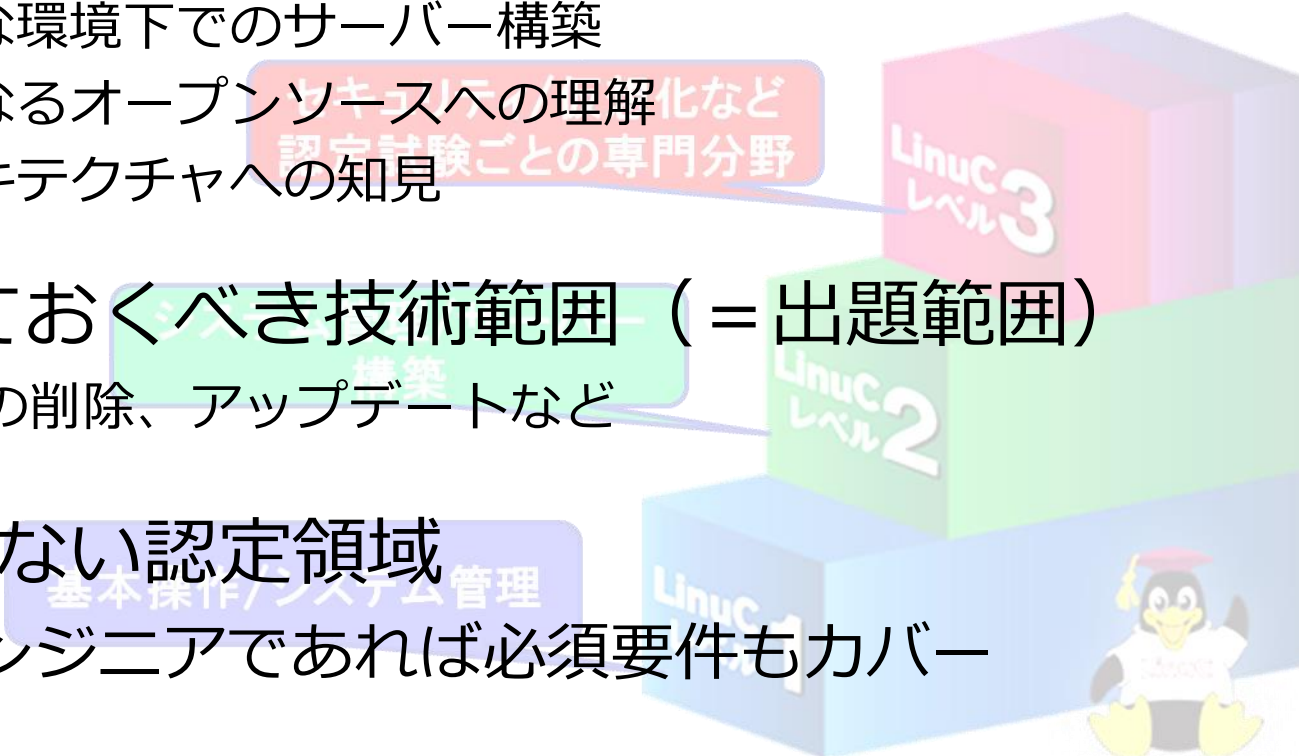
- ・ オンプレミス／仮想化を問わず様々な環境下でのサーバー構築
- ・ 他社とのコラボレーションの前提となるオープンソースへの理解化など
- ・ システムの多様化に対応できるアーキテクチャへの知見

✓全面的に見直した身につけておくべき技術範囲（＝出題範囲）

今となっては使わない技術やコマンドの削除、アップデートなど

✓Linuxの範疇だけにとどまらない認定領域

セキュリティや監視など、ITエンジニアであれば必須要件もカバー



■Version10.0と従来の出題範囲の比較

 #LinuC学習中

テーマ	Version 10.0	従来
LinuC-1	仮想技術 ・仮想マシン／コンテナの概念 ・<u>クラウドセキュリティの基礎</u>	← (Version10.0で新設)
	オープンソースの文化 ・オープンソースの定義や特徴 ・コミュニティやエコシステムへの貢献	← (Version10.0で新設)
	その他 → (Version10.0で削除)	アクセシビリティ、ディスククォータ、プリンタの管理、SQLデータ管理、他
LinuC-2	仮想化技術 ・仮想マシンの実行と管理(KVM) ・コンテナの仕組みとDockerの導入	← (Version10.0で新設)
	システムアーキテクチャ ・クラウドサービス上のシステム構成 ・高可用システム、スケーラビリティ、他	← (Version10.0で新設)
	その他 ・統合監視ツール(zabbix) ・自動化ツール(Ansible)	← (Version10.0で出題範囲に含む)
	→ (Version10.0で削除)	RAID、記憶装置へのアクセス方、FTPサーバーの保護、他

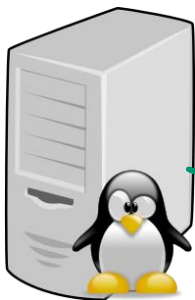
<https://linuc.org/linuc1/range/>
2021年3月末まではver.4と共に運用

■様々なシステム環境で利用されている



#LinuC学習中

■サーバー



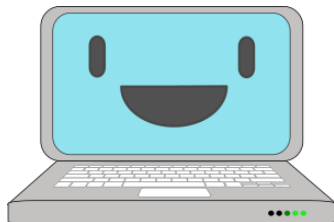
■モバイル 端末



■IoT端末



■ユーザー PC



■通信機器



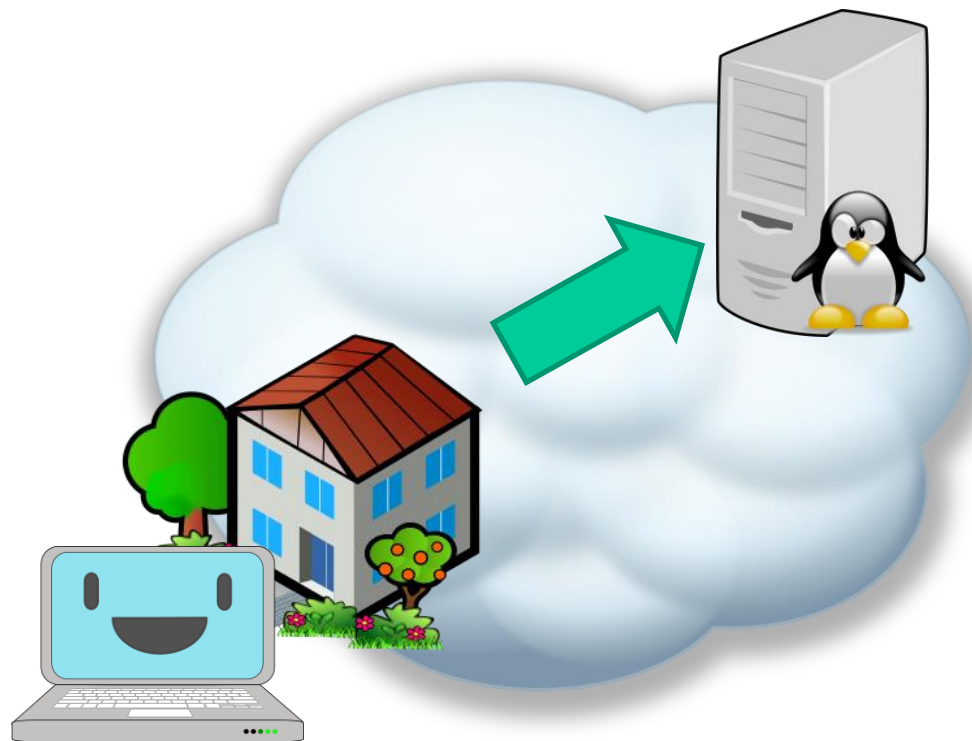
中でも、「サーバー」としての
Linux環境は重要

- 実機にLinux環境を構築
- 実機上で、仮想マシンを起動し、Linux環境を構築
 - KVM, Oracle VirtualBox
 - Vagrant, Docker
- クラウドサービスを利用
 - GCP, AWS, さくらのクラウド...



#LinuC学習中

- ・ アカウントの登録さえ完了すれば、すぐにLinux環境を利用できます。
- ・ LinuCの出題範囲にもなりました(特定のサービスについての問題は出題されない)



■101試験

- 1.01 : Linuxのインストールと仮想マシン・コンテナの利用
 - 1.01.1Linuxのインストール、起動、接続、切断と停止
- 1.02 : ファイル・ディレクトリの操作と管理
- 1.03 : GNUとUnixのコマンド
- 1.04 : リポジトリとパッケージ管理
- 1.05 : ハードウェア、ディスク、パーティション、ファイルシステム

101試験でもsshについて出題

■102試験

- 1.06 : シェルおよびスクリプト
- 1.07 : ネットワークの基礎
- 1.08 : システム管理
- 1.09 : 重要なシステムサービス
- 1.10 : セキュリティ
 - 1.10.3暗号化によるデータの保護
 - 1.10.4クラウドセキュリティの基礎
- 1.11 : オープンソースの文化

タイトルになっているように1.10.4はもちろんのこと、ssh接続が必須となるため、1.01.1や1.10.3も関連

■パブリッククラウドの管理機能とLinuxサーバーの機能分担について理解している。

- ・管理コンソール、ファイアウォール、ルーティング

■リージョン選択（国内外の制約も含む）の意味を理解している。

■パブリッククラウドの揮発性ストレージの利用方法を理解している。

■クラウドサービス事業者の制約による管理

- ・メンテナンス、再起動

■パブリッククラウドの管理コンソール(システムコンソール)へのアクセス経路と認証方式について知っている。

- ・インターネット経由でのアクセス、クラウドサービス事業者提供の認証方法
- ・多段階・多要素認証、ワンタイムパスワード

- ・ IaaSのサービスでLinuxインスタンス(仮想マシン)を利用するという前提
- ・ この範囲を理解するには、そもそもクラウドサービスを利用する上での基礎知識が必要
- ・ セキュリティについては上記の通り、基本的な内容が出題



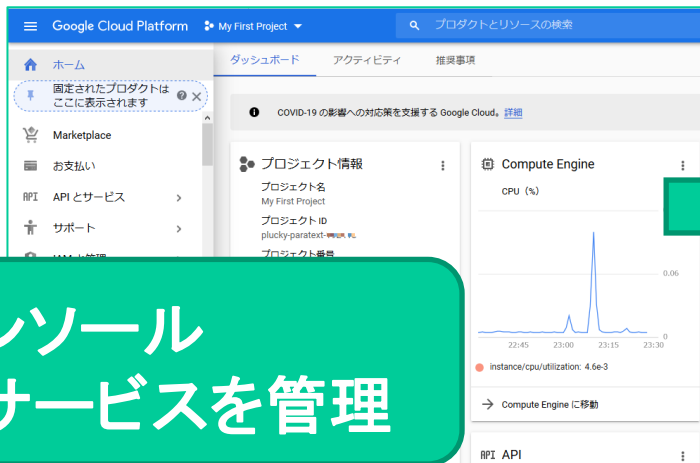
#LinuC学習中

■GCP（Google Cloud Platform）を利用

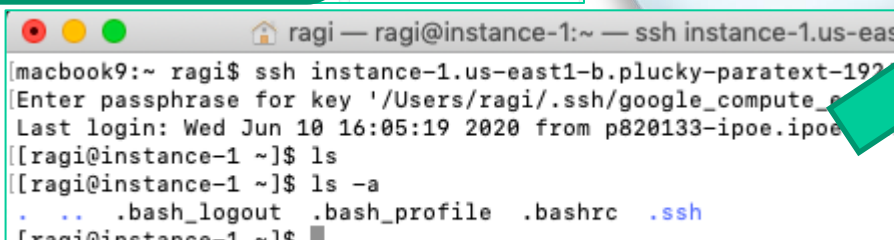
- Web管理コンソールを利用するほか、CUIでの管理コマンド（gcloudコマンド）も利用
→ 後者はGoogle Cloud SDKをインストールすると利用できます。
- Linuxの操作はssh接続をして、端末上でコマンドを実行



#LinuC学習中



・管理コンソール
クラウドサービスを管理



・コマンド端末（SSH接続）
インスタンス（仮想マシン）に接続し、OS操作

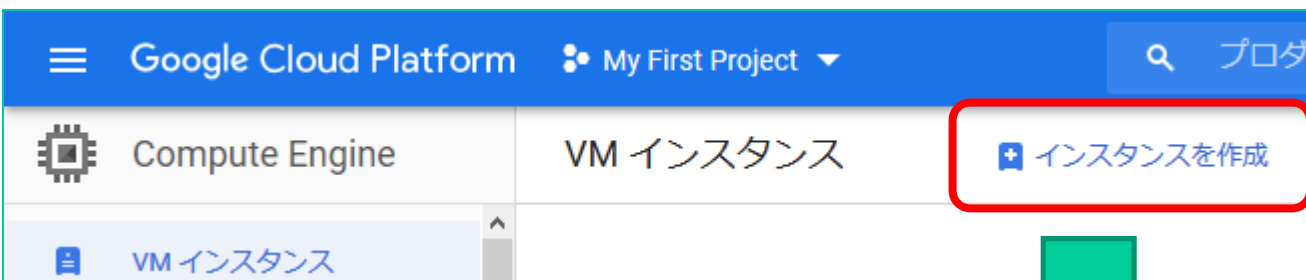
アカウント登録、プロジェクトの作成まで参考となるWebページ

<https://book.mynavi.jp/manatee/detail/id=65673>

<https://qiita.com/Brutus/items/22dfd31a681b67837a74>



#LinuC学習中



← インスタンスの作成

VM インスタンスを作成するには、次のいずれかのオプションを選択します。

- 新規 VM インスタンス**
最初から単一の VM インスタンスを作成します
- テンプレートから VM インスタンスを新規作成
既存のテンプレートから単一の VM インスタンスを作成します
- マシンイメージからの新しい VM インスタンス
既存のマシンイメージから単一の VM インスタンスを作成します
- Marketplace
VM インスタンスにすぐに使えるソリューションをデプロイします

名前 ?
名前は変更できません
instance-1

ラベル ? (省略可)
+ ラベルを追加

リージョン ?
リージョンは変更できません
us-central1 (アイオワ)

ゾーン ?
ゾーンは変更できません
us-central1-a

マシンの構成

マシンファミリー
汎用 | メモリ最適化 | コンピューティング最適化
費用と柔軟性を考慮して最適化された、一般的なワークロード向けのマシンタイプシリーズ

N1
Intel Skylake CPU プラットフォーム、またはそれ以前のプラットフォームが使用されます

マシンタイプ
f1-micro (1 vCPU、614 MB メモリ)

vCPU
1 個の共有コア

メモリ
614 MB

\$4.28 の月間予測
これは 1 時間に約 \$0.006 です
料金は使用分に対してのみ発生: 事前コストは不要、1 秒単位で課金
今月の f1-micro インスタンス使用量は、最初の 720 時間分が無料です。 [詳細](#)

リージョン(後述)を選択

マシンスペックを選択

リージョンやスペックなどにより予測費用を算出



ブートディスク ?

新しい 10 GB の標準の永続ディスク
イメージ
Debian GNU/Linux 10 (buster) 変更

ID と API へのアクセス ?

サービス アカウント ?
Compute Engine default service account

アクセス スコープ ?

- ☒ デフォルトのアクセス権を許可
- ☐ すべての Cloud API に完全アクセス権を許可
- ☐ 各 API にアクセス権を設定

ファイアウォール ?

タグとファイアウォールルールを追加して、インターネットからの特定のネットワークトラフィックを許可します

- ☐ HTTP トラフィックを許可する
- ☐ HTTPS トラフィックを許可する

管理、セキュリティ、ディスク、ネット

このインスタンスについては課金が発生します。Compute Engine の料金「?

作成

ブートディスク

イメージまたはスナップショットを選択してブートディスクを作成するか、既存のディスクを持つ VM ソリューションをご覧ください。

公開イメージ カスタム イメージ スナップショット 既存のディスク

オペレーティング システム

Debian

- CentOS
- Container Optimized OS
- ☒ Debian
- Deep Learning on Linux
- Red Hat Enterprise Linux
- Red Hat Enterprise Linux for SAP
- SQL Server on Windows Server

ファイアウォールルールを設定
※ここで許可をしないと、インスタンス側で設定しても接続不可

ここをクリックし、インスタンスを作成

インスタンス上で利用するOSを選択

■暗号化通信を有効にする ■多要素認証を有効にする

- ・パスワードの他、別の要素による認証
 - ワンタイムパスワード
 - モバイルアプリでの認証
 - バックアップコード など

多段階認証は、パスワード(同じ要素)を複数回で認証でもOK



#LinuC学習中

パスワードだけだと、悪意のある第三者による不正な認証試行が成功してしまう可能性がある

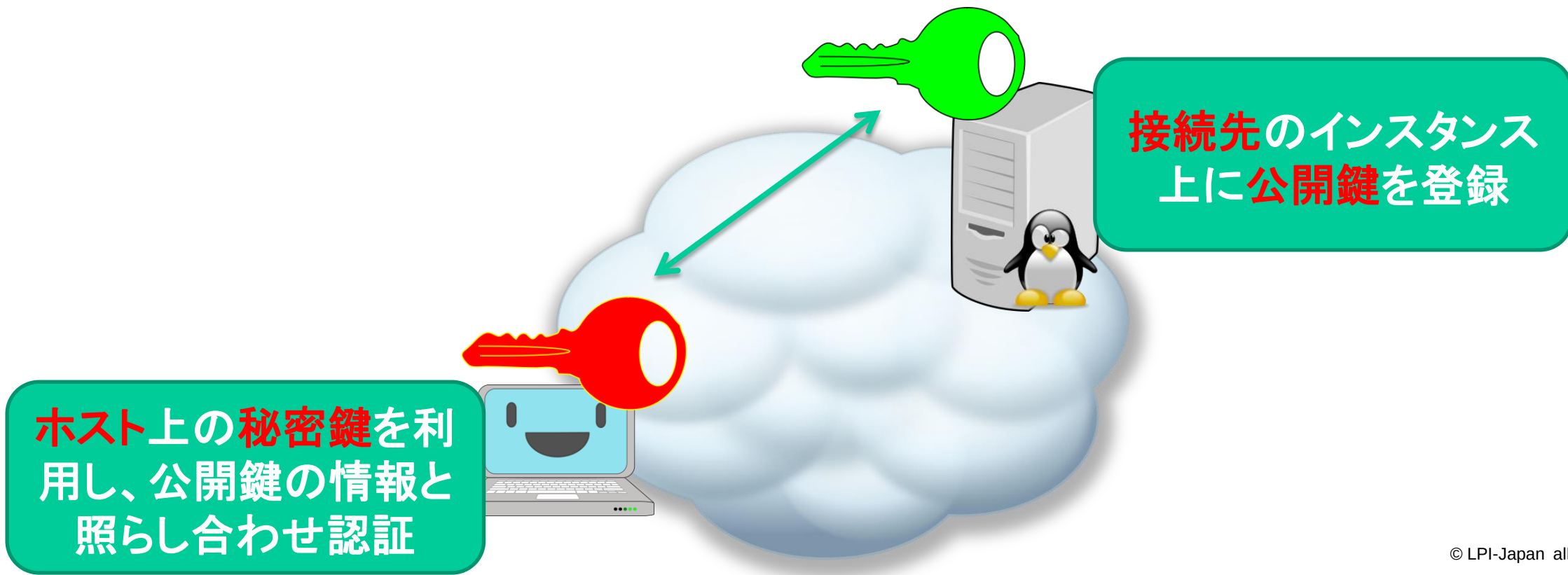


■SSH接続を利用

- ・クラウドサービス上のインスタンスへの接続は、パスワードでの認証は許可しない
- ・公開鍵認証方式を利用
 - 公開鍵で暗号化した情報を秘密鍵で復号
 - データを復号できる = 正当なユーザーということで認証にも利用



#LinuC学習中



【デモ】公開鍵ペアを構成し、インスタンスに接続(1)

macbook9:~ ragi\$ **gcloud compute instances list**

NAME	ZONE	MACHINE_TYPE	PREEMPTIBLE	INTERNAL_IP	EXTERNAL_IP	STATUS
instance-1	us-east1-b	f1-micro		10.142.0.4	34.73.159.1xx	Running

macbook9:~ ragi\$ **gcloud compute config-ssh**

:

Generating public/private rsa key pair.

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /Users/ragi/.ssh/google_compute_engine.

Your public key has been saved in /Users/ragi/.ssh/google_compute_engine.pub.

:

For example, try running:

\$ ssh instance-1.us-east1-b.plucky-paratext-1924xx



#LinuC 学習中

インスタンス一覧
を表示
※インスタスへの
接続に利用する
IPアドレスは
NAT変換して利用

インスタンス、ホ
スト双方で、SSH
接続をするための
設定を有効化
※公開鍵ペアの
作成など

【デモ】公開鍵ペアを構成し、インスタンスに接続(2)



#LinuC学習中

```
macbook9:~ ragi$ ls .ssh
```

```
config          google_compute_engine.pub id_rsa.pub
```

```
google_compute_engine id_rsa
```

```
macbook9:~ ragi$ cat .ssh/config
```

```
:
```

```
Host instance-1.us-east1-b.plucky-paratext-1924xx
```

```
HostName 34.73.159.1xx
```

```
IdentityFile /Users/ragi/.ssh/google_compute_engine
```

```
UserKnownHostsFile=/Users/ragi/.ssh/google_compute_engine
```

```
:
```

```
macbook9:~ ragi$ ssh instance-1.us-east1-b.plucky-paratext-1924xx
```

```
The authenticity of host 'compute.60254852432001294xx (34.73.159.1xx)' can't be
established.
```

```
:
```

```
Enter passphrase for key '/Users/ragi/.ssh/google_compute_engine':
```

```
[ragi@instance-1 ~]$
```

公開鍵ペアを作成し、~/sshに配置
~.pubが公開鍵、拡張子無しが秘密鍵

~/ssh/config
sshコマンド実行時に設定として参照
gloud ~ config-ssh実行時に出力されたsshコ
マンドを入力した際の設定が追加

gloud ~ config-ssh実行時に出力されたsshコ
マンドを入力して接続

```
[ragi@instance-1 ~]$ ls .ssh
```

```
authorized_keys
```

```
[ragi@instance-1 ~]$ cat .ssh/authorized_keys
```

```
# Added by Google
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQADviYtqtuAgtqTfUgwta5anHvFLIhqp3uYQ4rr6tgEU+
7p4tvlr+kxnYvxbOgd/V8UmD0O2x469hB01xBJ7F4Ps1RE+9OSMH/J+aOyMI11yQ84UZqIG9
e9H5PAAtVGt/vb2lqyisAaZJVzDjdSCnFUurDzD3XLvCpBlONNR4RqIMBEqRsHxRNLeFQrLaF/gxF
r2YVqK5PkLAlsRWc7uN3+7UvVkZ1COqebe8I50ekMfBq3Fdd+UkiUGTCybkLwg7FNAq9eYcA
muRDbNz3k4bKg97VOd2HNWiu+fRsy0aS+7Z+Q5fRxxxxx ragi@macbook9.local
```



#LinuC学習中

サーバーの ~/.ssh/authorized_keys に公開鍵を
登録して利用



#LinuC学習中

```
[ragi@instance-1 ~]$ sudo su
[root@instance-1 ragi]# yum -y install httpd
[root@instance-1 ragi]# echo test > /var/www/html/index.html
[root@instance-1 ragi]# systemctl start httpd
[root@instance-1 ragi]# systemctl status httpd
httpd.service - The Apache HTTP Server
```

Apache httpdをインストールし、公開用のファイルを配置。サービスを起動。

```
Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
```

```
Active: active (running) since 2020-06-10 17:29:
:
```

Active: active (running) → サービスが起動中



Webサービスが起動中だと、左図のようにWebブラウザで接続確認可能



#LinuC学習中

■障害/災害が発生し、インスタンスに接続できない

- AWS東京リージョンで4月20日夜に大規模障害か、複数のオンラインサービスに影響 | 日経クロステック (xTECH)

<https://xtech.nikkei.com/atcl/nxt/news/18/07639/>

- Googleのクラウドサービスで障害発生 「G Suite」 「GCP」 など利用できない状況に - ITmedia NEWS

<https://www.itmedia.co.jp/news/articles/2003/27/news118.html>

■悪意のあるユーザーにより不正なアクセスがされてしまった

- クラウドサービス上のインスタンスは世界中の様々なユーザーから接続が可能



■障害が発生した際、情報収集がまずは重要

- 公式サイト
- 管理コンソール
- ニュースサイト
- SNS
- :



#LinuC学習中

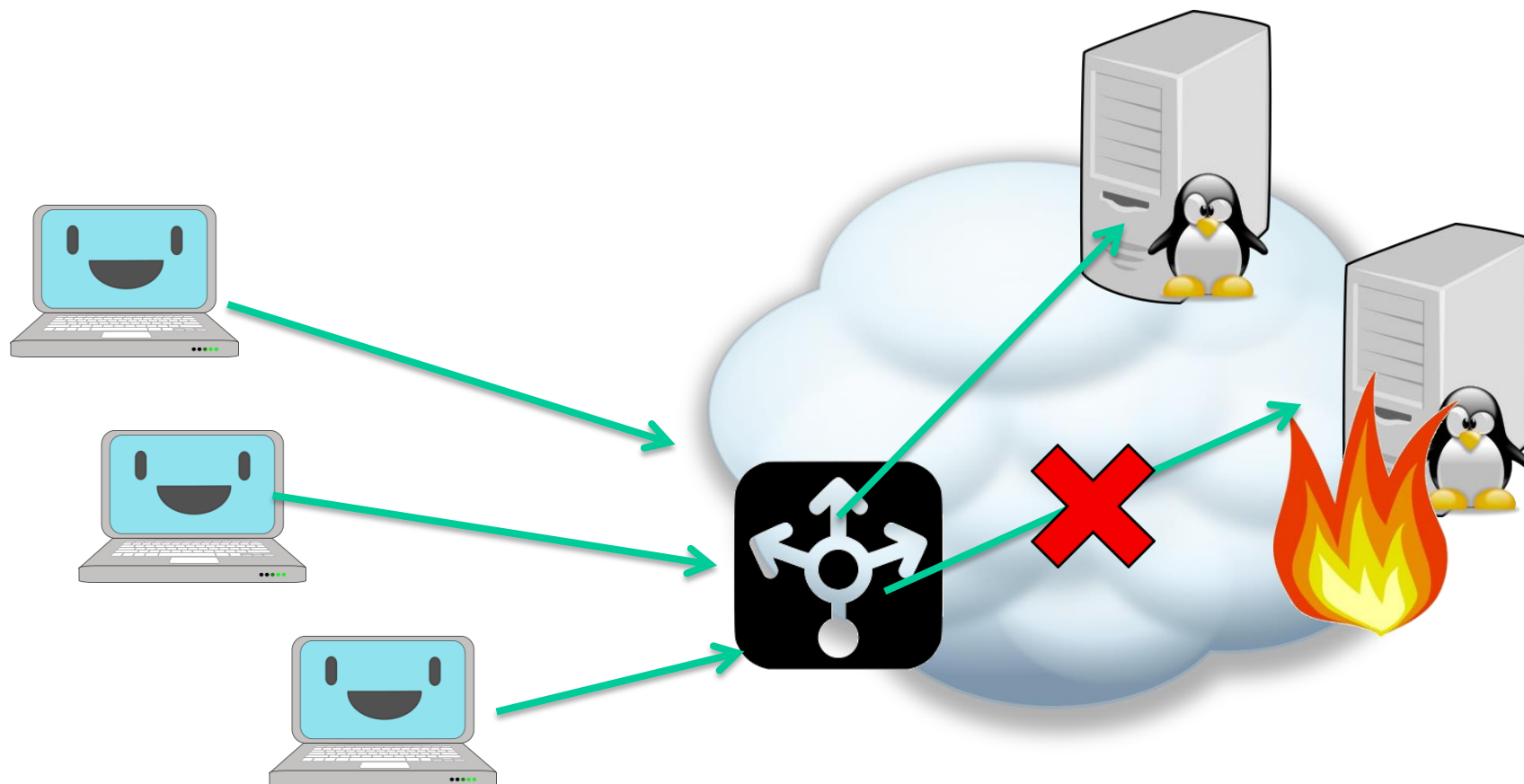


■あるサービスを提供するインスタンスに接続できない

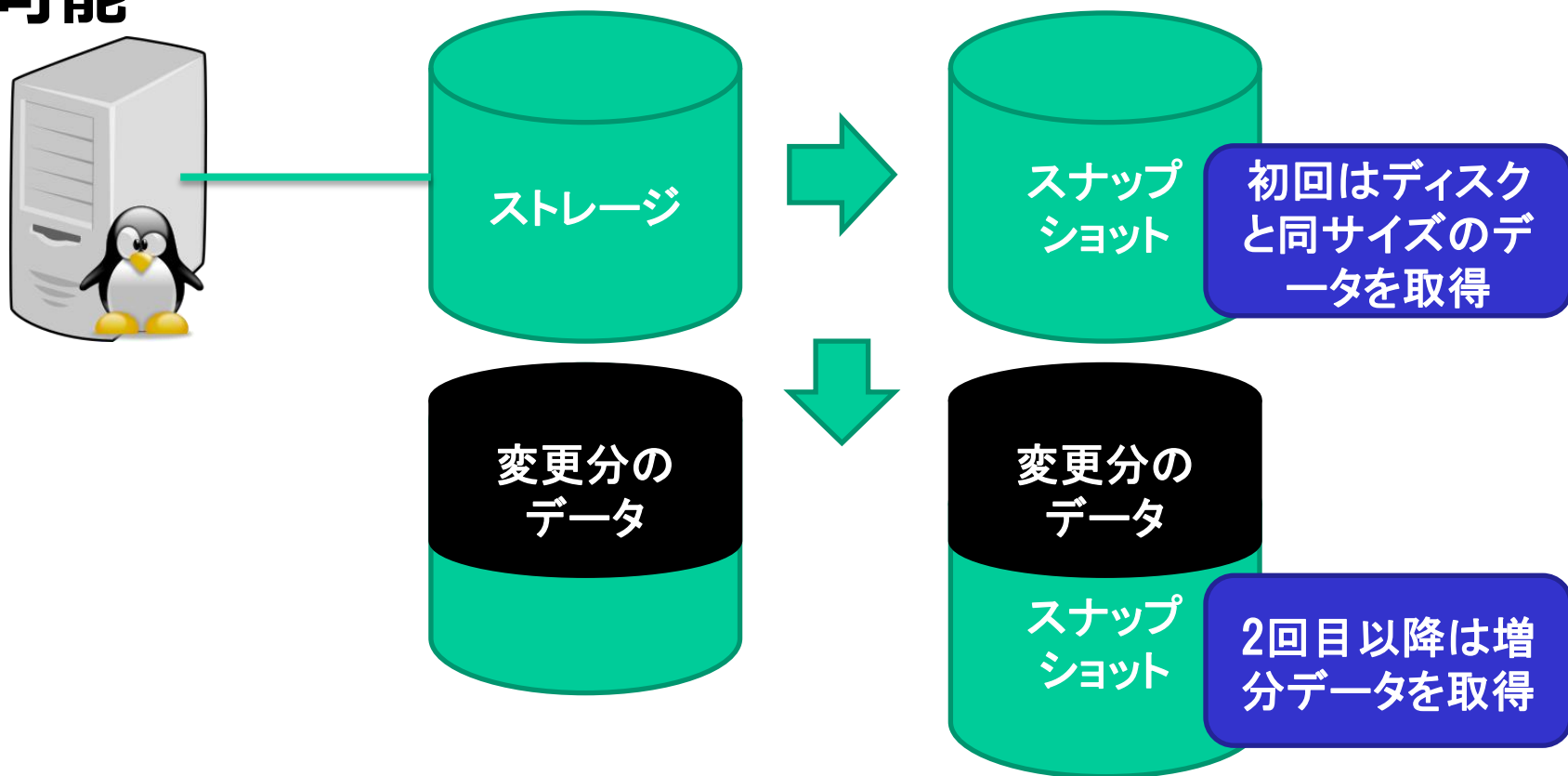
- 1台で構成している場合は、スナップショットなどから環境を再構成
 - サービスの再開までに時間がかかる
- 複数台で構成をして、フェイルオーバー



#LinuC学習中



- インスタンスを構成するストレージのある時点の状態のデータを取得
- 次回取得時から差分を取得
- 取得したスナップショットを元に、別のインスタンスを構成することなどが可能

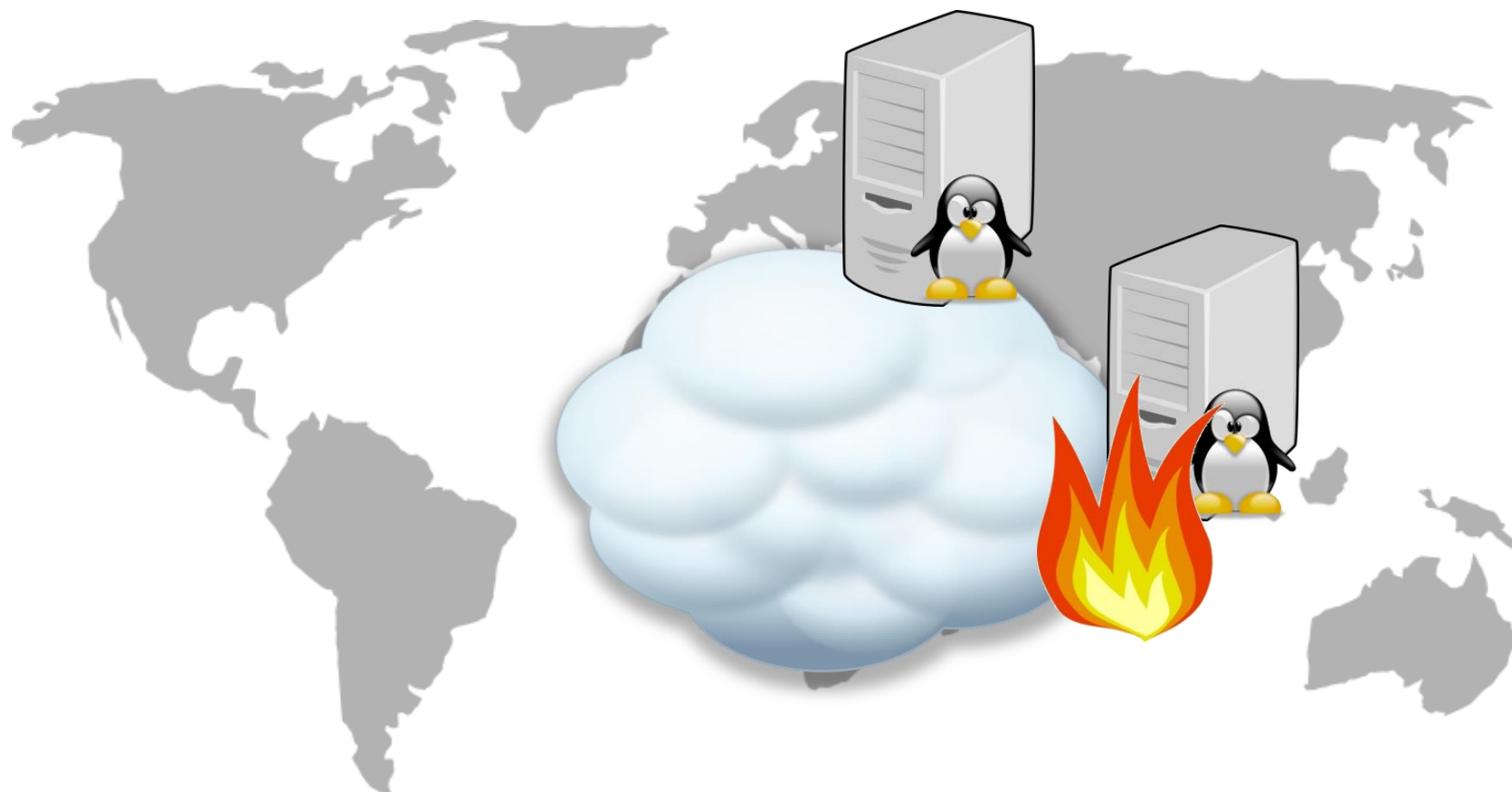


■複数のリージョンにインスタンスを構成し、運用

- 特定のリージョンで障害が発生した場合、別のリージョンにフェイルオーバー
- スナップショットの配置などに注意



#LinuC学習中





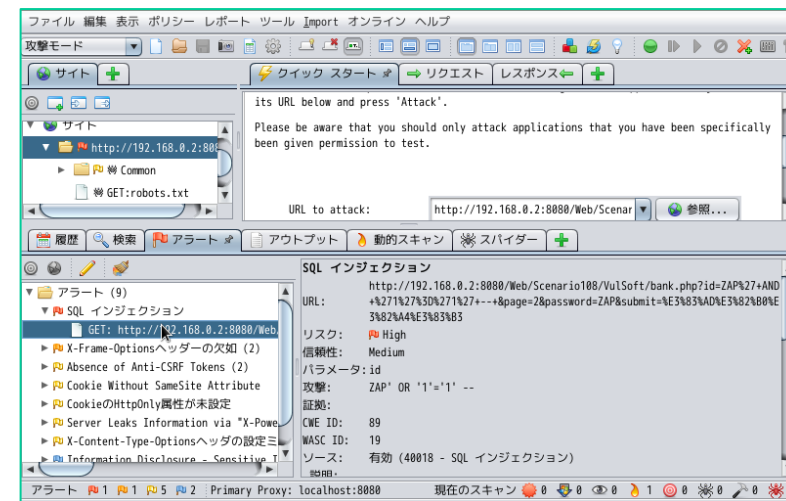
#LinuC学習中

■動作しているインスタンスやインスタンス上のプログラムに脆弱性がないか検査を行う

- 脆弱性検査用のツールなどもあり
 - 例：OWASP ZAP: Webアプリの脆弱性を検査
- 脆弱性が発見された場合、すぐにプログラムを更新するなどの対応が必要

■検査内容によっては、サービス事業者への事前連絡が求められることもあり

- ペネトレーションテスト（侵入テスト） - AWS セキュリティ
<https://aws.amazon.com/jp/security/penetration-testing/>
- クラウドのセキュリティに関するよくある質問 - Google Cloud Platform Console ヘルプ
<https://support.google.com/cloud/answer/6262505?hl=ja>





#LinuC学習中

「最短突破 LinuCレベル1 合格教本」(技術評論社)
好評発売中です。
※ver.10対応の改訂版は今夏発売予定です



■ご参加いただき、ありがとうございました！

・アンケートのご協力をよろしくお願いいたします。