1. **シェルおよびスクリプト**

シェル環境のカスタマイズ/シェルスクリプト

2. **ネットワークの基礎**

インターネットプロトコルの基礎/基本的なネットワーク構成/基本的なネットワークの問題解決/クライアント側のDNS設定

3. **システム管理**

アカウント管理/ジョブスケジューリング/ローカライゼーションと国際化

4. **重要なシステムサービス**

システム時刻の保守/システムのログ/メール転送エージェント(MTA)の基本

5. **セキュリティ**

セキュリティ管理業務の実施/ホストのセキュリティ設定/暗号化によるデータの保護/クラウドセキュリティの基礎

6. **オープンソースの文化**

オープンソースの概念とライセンス/オープンソースのコミュニティとエコシステム

5. セキュリティ

セキュリティ管理業務の実施

用語: find, passwd, chage, ss, fuser, lsof, nmap, sudo, /etc/sudoers, su, ulimit, who, w, last, TMOUT

SUID, SGIDを設定した場合、一般ユーザー、一般グループのユーザーがそのコマンドを実行した場合もroot権限で動作できる。そのため、SUID, SGIDが正しいファイルに付与されている事を確認することが必要。
find / -perm –u+s(or -4000): SUIDが付与されているファイルを検索する
find / -perm –g+s(or -2000): SGIDが付与されているファイルを検索する

who: システムにログインしているユーザの情報を表示。**/var/run/utmp**を参照する
w: ログインしているユーザ情報とシステム情報を詳細に表示
last: ユーザがログインした履歴を表示するコマンド。**/var/log/wtmp**を参照する

su: rootにユーザを変換してシェルを起動するコマンド
sudo: rootユーザとしてコマンドを実行するコマンド
-l 許可されているコマンドを表示

/etc/sudoers: sudoコマンドを利用できるユーザを設定するファイル
visudo: /etc/sudoersファイルを編集するコマンド

/etc/sudoersの記述内容
ユーザ名: コマンドをの実行を許可するユーザ名、グループ名、もしくはALL(頭に%を付けるとグループを指定する)
ホスト名: 実行を許可するホスト名、IPアドレス、もしくはALL
実行ユーザ名: コマンド実行時のユーザ名(省略時はroot)、もしくはALL
コマンド: 実行を許可するコマンドのパス、もしくはALL
NOPASSWD: 指定するとコマンド実行時にパスワードは問われない

5. セキュリティ

セキュリティ管理業務の実施

用語: find, passwd, chage, ss, fuser, lsof, nmap, sudo, /etc/sudoers, su, ulimit, who, w, last, TMOUT

fuser: 引数として渡されたファイルやポートを使用しているプロセスのPIDを表示するコマンド
fuser -v -n tcp ポート番号: 指定したポート番号のtcpポートを開いているプロセスを表示

lsof: プロセスが開いているファイル、ポートを表示するコマンド。
-p プロセスID: プロセスIDを指定して、そのプロセスが開いているファイルを表示
-i: 待機しているプロセスを表示
-Pi:待機しているプロセスとポートを表示

nmap:外部のサーバーが開いているポートを調べるポートスキャン(ネットワークスキャン)するコマンド。
nmap ホスト名: 開いているポート一覧を表示する
nmap –sT ホスト名: TCPプロトコルをスキャンする

ulimit: ユーザの使用できるプロセス数、ファイルサイズ、仮想メモリなどのリソース制限を設定する
-a: 制限の設定値を表示
-f サイズ:シェルが生成できるファイルの最大サイズをブラック単位で指定する
-n 数: 同時に開くことのできるファイルを指定する
-u プロセス数: ユーザーが利用できる最大プロセス数を指定する
-v サイズ: ユーザーとその子プロセスが利用できる最大仮想メモリサイズを指定する

TMOUT: 一定の時間が経過したらユーザーを自動的にログアウトさせる環境変数。秒単位で指定する

5. セキュリティ

セキュリティ管理業務の実施

用語: find, passwd, chage, ss, fuser, lsof, nmap, sudo, /etc/sudoers, su, ulimit, who, w, last, TMOUT

chage: パスワードの有効期限を変更するコマンド(change password age)。
-E yyyy/mm/dd: ユーザーアカウントが無効になる日付を設定する
-m: 次に変更を許可するまでの日数を指定する
-M: パスワードの有効な最長な日数を設定する
-l: パスワードの有効期限情報を表示

ユーザーにログインさせないように設定する
usermod –s /sbin/nologin(または/bin/false) ユーザー名: ログインシェルを/sbin/nologinまたは/bin/falseに設定すると、一般ユーザーから設定したユーザーにログインができなくなる

ユーザーアカウントをロックしてログインできないようにする
passwd –l, usermod –L ユーザー名

netstat:ホストのネットワーク接続状態やソケット／インターフェイスごとのネットワーク統計などを確認するコマンド。
-a: すべての情報を表示。-n: IPアドレスに変換して表示。-l: リッスンしているもののみ表示。-p: PIDとプロセス名を表示
ss: 最近のディストリビューションで利用されるnetstatと同様の処理を行う

1. シェルおよびスクリプト

シェル環境のカスタマイズ/シェルスクリプト

2. ネットワークの基礎

インターネットプロトコルの基礎/基本的なネットワーク構成/基本的なネットワークの問題解決/クライアント側のDNS設定

3. システム管理

アカウント管理/ジョブスケジューリング/ローカライゼーションと国際化

4. 重要なシステムサービス

システム時刻の保守/システムのログ/メール転送エージェント(MTA)の基本

5. セキュリティ

セキュリティ管理業務の実施/ホストのセキュリティ設定/暗号化によるデータの保護/クラウドセキュリティの基礎

6. オープンソースの文化

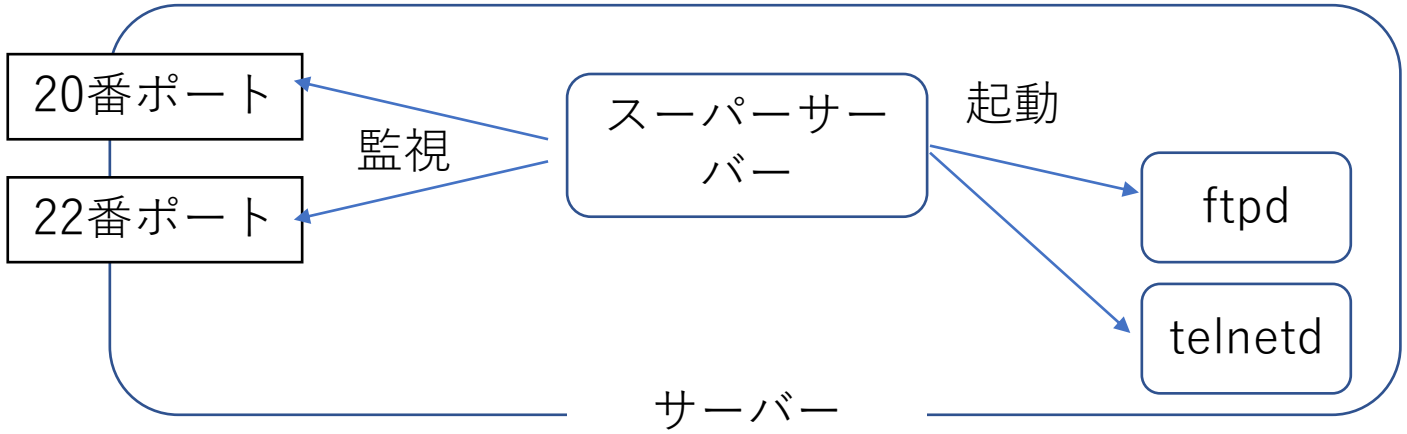
オープンソースの概念とライセンス/オープンソースのコミュニティとエコシステム

5. セキュリティ

ホストのセキュリティ設定

用語: /etc/nologin, /etc/xinetd.d/, /etc/xinetd.conf, /etc/inetd.d/, /etc/inetd.conf, chkconfig, iptables, firewalld

ネットワークを通じてサービスを提供して外部との接続を受け付けたり、常駐して処理を行うプログラムを**デーモン**と言う。デーモンは常時メモリ上に待機しておりリソースを消費している。リソースが過剰に使われすぎることを解消するために**スーパーサーバ**—が開発された
スーパーサーバー: ネットワーク上の各種接続要求を監視して、接続要求を検出した際に要求に応じたサーバプログラムを起動するデーモン。代表的なものとして**inetd**, **xinetd, systemd**がある。現在多くのディストリビューションで**systemd**が採用されている。



/etc/inetd.conf: inetdの設定ファイル。1行につき1つのサービスを記述する。

5. セキュリティ

ホストのセキュリティ設定

用語: /etc/nologin, /etc/xinetd.d/, /etc/xinetd.conf, /etc/inetd.d/, /etc/inetd.conf, chkconfig, iptables, firewalld

/etc/xinetd.conf: xinetdの全体的な設定ファイル
/etc/xinetd.d/: xinetdで各サービスの設定ファイルとそのサービスに関連したファイルが格納されているディレクトリ。サービスごとの設定を記述する

service: systemd以前のディストリビューションでサービスを起動・停止するコマンド(systemdの環境ではsystemctlを利用する)
chkconfig: サービスの自動起動設定するコマンド

/etc/systemd/system.conf: systemd全体の設定を行う設定ファイル
/etc/systemd/system/〇〇.service: systemdで管理するサービスの設定を記述するファイル
上に設定ファイルを配置すると
systemctl start 〇〇
で〇〇.serviceで設定した内容のサービスを起動できるようになる

systemctl: systemdのサービスを扱うコマンド

start: 起動
stop: 停止
restart:再起動
reload: 設定のリロード
status: ステータス表示
enable: 自動起動を有効
disable: 自動起動無効

is-enable: 自動起動設定確認
list-unit-files –type=service: サービス一覧表示
daemon-reload: 設定ファイルの再読み込み

5. セキュリティ

ホストのセキュリティ設定

用語: /etc/nologin, /etc/xinetd.d/, /etc/xinetd.conf, /etc/inetd.d/, /etc/inetd.conf, chkconfig, iptables, firewalld

/etc/nologin: rootユーザしかシステムにログインできないようにするファイル
passwd –l user, usermod –L user: ユーザーアカウントをロックしてログインできなくする

ファイアウォール・・・ネットワークを監視して、設定したルールを元に接続の許可、拒否を行う。

iptables: パケットフィルタリングのルールを細かく設定する。パケットフィルタリングルールは保存しないと、システムの終了・再起動により消えてしまう。
iptables-save: パケットフィルタリングルールを保存するコマンド
iptables-restore: ファイルからパケットフィルタリングルールを読み込んで設定する

firewalld: ファイアウォールを管理するデーモン。CentOS7以降はiptablesの代わりにこちらが利用される
firewall-cmd: firewalldを扱うコマンド。
--state: 動作状態を確認、**--list-service**: 許可されているサービスの一覧を表示
--add-service: 許可するサービスを追加、**--remove-service**: 許可を取り消す

firewalldにはゾーンという概念がある。ゾーンは、パケットフィルタリングルールをまとめたもので、各ゾーンに対してルールを追加・設定する

ゾーン	説明
public	インターネット上の公開サーバ用（デフォルト）
work	社内LANにあるクライアントPC用
home	家庭内LANにあるクライアントPC用
trusted	全ての通信を許可

1. **シェルおよびスクリプト**

シェル環境のカスタマイズ/シェルスクリプト

2. **ネットワークの基礎**

インターネットプロトコルの基礎/基本的なネットワーク構成/基本的なネットワークの問題解決/クライアント側のDNS設定

3. **システム管理**

アカウント管理/ジョブスケジューリング/ローカライゼーションと国際化

4. **重要なシステムサービス**

システム時刻の保守/システムのログ/メール転送エージェント(MTA)の基本

5. **セキュリティ**

セキュリティ管理業務の実施/ホストのセキュリティ設定/暗号化によるデータの保護/クラウドセキュリティの基礎

6. **オープンソースの文化**

オープンソースの概念とライセンス/オープンソースのコミュニティとエコシステム

5. セキュリティ

暗号化によるデータの保護

用語: ssh, ssh-keygen, ssh-agent, ssh-add, ~/.ssh/id_rsa and id_rsa.pub, ~/.ssh/id_dsa and, id_dsa.pub, ～/.ssh/id_ecdsaと id_ecdsa.pub, ～/.ssh/id_ed25519とid_ed25519.pub, /etc/ssh/ssh_host_rsa_key and ssh_host_rsa_key.pub, /etc/ssh/ssh_host_dsa_key and ssh_host_dsa_key.pub

ssh: SSHプロトコルを使ってリモートホストと暗号化して通信するコマンド。sshで端末にログインする。データを暗号化して送受信し、よりセキュリティの高い接続を行う。Linuxでは、OpenSSHが利用されている
-l: ログインユーザ名を指定。**-p**: ポート番号を指定。**-i**: 秘密鍵ファイルを指定

ssh –p 11000 test@192.111.11.11 # 192.111.11.11のアドレスにtestユーザで11000のポート番号を用いてsshプロトコルで接続する

ssh-keygen: SSHで公開鍵と秘密鍵のペアを作成するコマンド。-t: 生成する鍵の指定
ssh-agent: 認証エージェント。
ssh-add: 認証エージェントにRSA, DSA秘密鍵を追加するコマンド

ssh_host_rsa_key and ssh_host_rsa_key.pub: RSA暗号方式のホスト認証用の鍵。
ssh_host_dsa_key and ssh_host_dsa_key.pub: DSA暗号方式のホスト認証用の鍵。
ssh_host_ecdsa_key and ssh_host_ecdsa_key.pub: ECDSA暗号方式のホスト認証用の鍵。
ssh_host_ed25519_key and ssh_host_ed25519_key.pub: DSA暗号方式のホスト認証用の鍵。

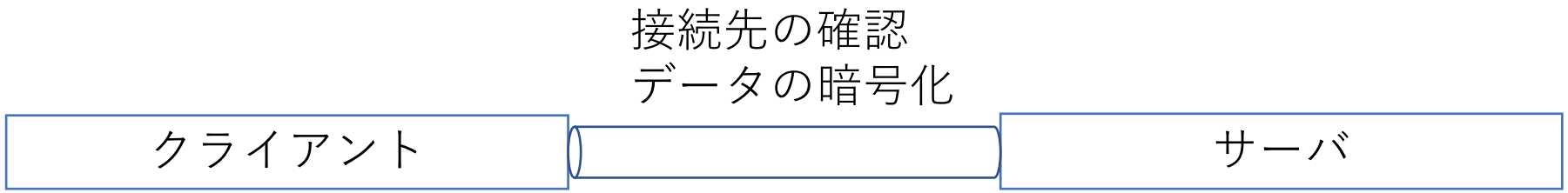
【暗号アルゴリズム】
RSA: 広く普及したアルゴリズム
DSA: 以前は利用されていた安全性に懸念のあるアルゴリズム
ECDSA: 小さな鍵長で済み、高速に操作できる
ED25519: 安全性が高く、高速で。DSA、ECDSAよりも安全性が高い

5. セキュリティ

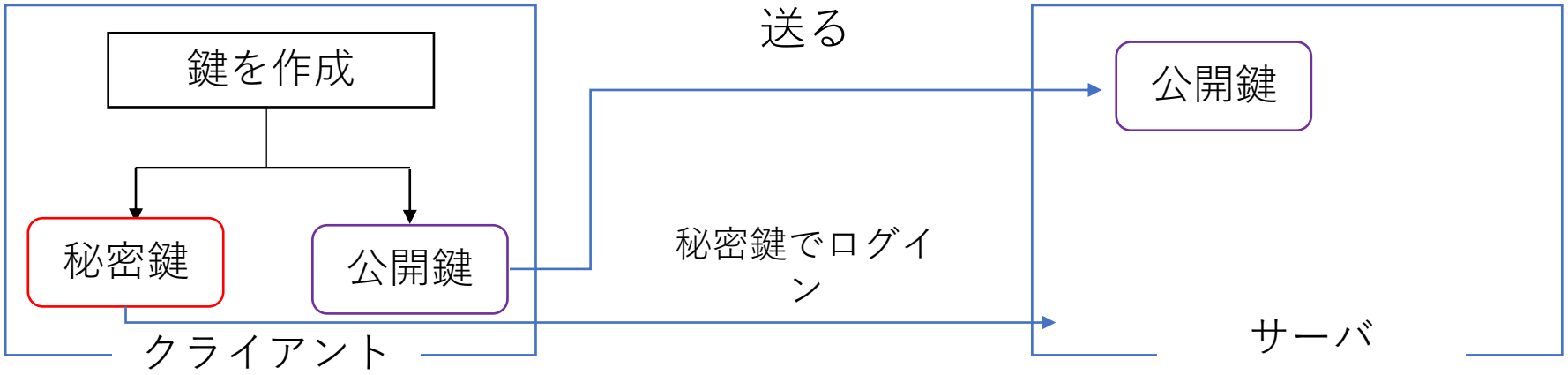
暗号化によるデータの保護

用語: ssh, ssh-keygen, ssh-agent, ssh-add, ~/.ssh/id_rsa and id_rsa.pub, ~/.ssh/id_dsa and, id_dsa.pub, ~/.ssh/id_ecdsaとid_ecdsa.pub, ~/.ssh/id_ed25519とid_ed25519.pub, /etc/ssh/ssh_host_rsa_key and ssh_host_rsa_key.pub, /etc/ssh/ssh_host_dsa_key and ssh_host_dsa_key.pub

SSH



~/.ssh/known_hosts: 一度もssh接続をしていないサーバにssh接続した際に接続したサーバの情報が保存されるファイル
~/.ssh/authorized_keys: 公開鍵認証でクライアントの公開鍵を登録するファイル
~/.ssh/id_rsa: 公開鍵認証で利用する秘密鍵
~/.ssh/id_rsa.pub: 公開鍵認証で利用する公開鍵



6. セキュリティ

暗号化によるデータの保護

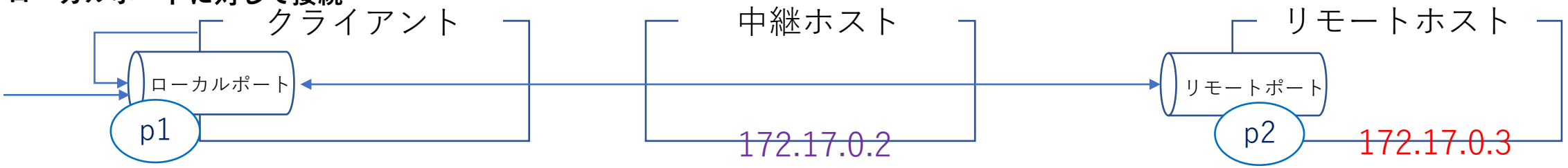
用語: /etc/ssh/ssh_host_ecdsa_keyおよびssh_host_ecdsa_key.pub, /etc/ssh/ssh_host_ed25519_keyおよびssh_host_ed25519_key.pub, ~/.ssh/authorized_keys, ssh_known_hosts, gpg, gpg-agent, ~/.gnupg/

scp: SSHを用いてホスト間でファイルをコピーするコマンド。
-p: パーミッションを保持したままコピー。**-r**: ディレクトリ内を再帰的にコピー。**-P ポート番号**: ポート番号を指定する(デフォルトは22)

scp コピー元ファイル [ユーザ名@]コピー先ホスト:[コピー先ファイル名]
例) scp /etc/file sample.com:/tmp/file

SSHポート転送(ポートフォワーディング)・・・特定のポートに送られたTCPパケットをSSHを用いた安全な通信路を経由して、リモートホストのポートに転送すること
下の図の場合、クライアントサーバのローカルポート当ての処理をそのままリモートホストに転送することができる。(中継ホストをクライアントと同じサーバに指定することもできる)
ssh –L [ローカルポート]:[リモートホスト]:[リモートポート] [中継ホストのログインユーザ名]@[中継ホスト]

ローカルポートに対して接続



ssh –L p1:172.17.0.3:p2 user@172.17.0.2

6. セキュリティ

暗号化によるデータの保護

用語: /etc/ssh/ssh_host_ecdsa_keyおよびssh_host_ecdsa_key.pub, /etc/ssh/ssh_host_ed25519_keyおよびssh_host_ed25519_key.pub, ~/.ssh/authorized_keys, ssh_known_hosts, gpg, gpg-agent, ~/.gnupg/

GnuPG: ファイルの暗号化と復号をするソフトウェア。共通鍵暗号方式と公開鍵暗号方式のどちらでも利用できる。
gpg: 暗号化、復号に用いるコマンド
gpg –-gen-key: 暗号化、復号に用いる公開鍵(pubring.gpg), 秘密鍵(secring.gpg)を作成する。鍵は~/.gnupgディレクトリに作成される
gpg –-list-keys: 鍵の一覧を確認する

【共通鍵を用いた暗号化/復号】
gpg –c ファイル名: 共通鍵を使った暗号化する
実行後、ファイル名.gpgが作成される
gpg ファイル名.gpg: 共通鍵で復号する

【公開鍵を用いた暗号化/復号】
共通鍵を用いた場合、共通鍵を知られたら誰でも複合できてしまう。そのため、秘密鍵と公開鍵のペアを作成して公開鍵を外部に配り暗号化をする。そして、暗号化されたファイルを共通鍵で復号する。

gpg –o 公開鍵ファイル –a –export メールアドレス: 対象するメールアドレスの公開鍵を作成する
gpg –-import 公開鍵ファイル: 公開鍵を環境にインポート
gpg –e –a –r メールアドレス ファイル名: 公開鍵を利用したファイルの暗号化を行う
gpg –-sign-key メールアドレス: 公開鍵が信用するように設定する（実行しない場合、暗号化の際に警告が表示される）
gpg 暗号化されたファイル: 秘密鍵を利用したファイルの復号を行う
gpg-agent: GnuPG の中核コンポーネントで，秘密鍵の管理を行い一定期間キャッシュする

1. **シェルおよびスクリプト**

シェル環境のカスタマイズ/シェルスクリプト

2. **ネットワークの基礎**

インターネットプロトコルの基礎/基本的なネットワーク構成/基本的なネットワークの問題解決/クライアント側のDNS設定

3. **システム管理**

アカウント管理/ジョブスケジューリング/ローカライゼーションと国際化

4. **重要なシステムサービス**

システム時刻の保守/システムのログ/メール転送エージェント(MTA)の基本

5. **セキュリティ**

セキュリティ管理業務の実施/ホストのセキュリティ設定/暗号化によるデータの保護/クラウドセキュリティの基礎

6. **オープンソースの文化**

オープンソースの概念とライセンス/オープンソースのコミュニティとエコシステム

5. セキュリティ

クラウドセキュリティの基礎

パブリッククラウド・・・クラウド事業者が、オンラインでサーバー、DB、ストレージ、ネットワークなどを提供する
AWS(Amazon Web Service), GCP(Google Cloud Platform), Microsoft Azure
*) クラウド内で動作する仮想サーバをインスタンスと呼ぶ

オンプレミス・・・自前でサーバーを購入して管理してシステムに利用すること

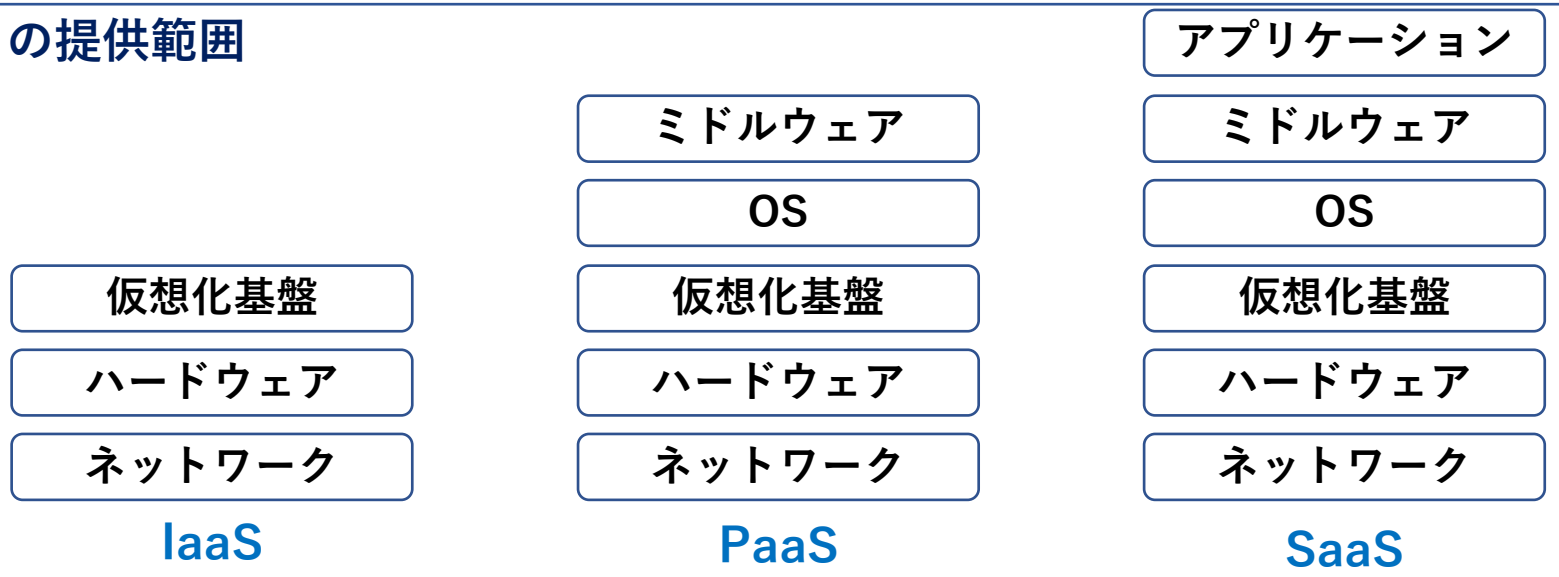
*) オンプレミスは、OSの更新、ファイアウォールの設定などは全て自分たちで行って脆弱性の管理をしないといけないが、パブリッククラウドでは、セキュリティの脆弱性の対策はクラウド事業者がある程度までしてくれる。

【パブリッククラウドの種類】
IaaS(Infrastructure as a service)・・・クラウド事業者がネットワークやハードウェア、利用できるOSを提供して、仮想マシン上のOS、アプリケーションなどの実行環境は利用者が準備・管理する

PaaS(Platform as a Service)・・・クラウド事業者がOSからアプリケーションの実行環境まで提供する。利用者はアプリケーションだけ用意する

SaaS(Software as a Service)・・・アプリケーションまでクラウドサービスとしてクラウド事業者が用意する。

クラウドサービスごとの提供範囲



クラウドサービスごとの事業者と利用者の責任範囲

項目	IaaS	PaaS	SaaS
認証情報	利用者	利用者	利用者
送受信データ	利用者	利用者	利用者
保存データ	利用者	利用者	利用者
アプリケーション	利用者	利用者	クラウド事業者
ミドルウェア	利用者	クラウド事業者	クラウド事業者
OS	利用者	クラウド事業者	クラウド事業者
クラウドの仮想化基盤	クラウド事業者	クラウド事業者	クラウド事業者
ネットワーク	クラウド事業者	クラウド事業者	クラウド事業者
電源やハードウェア	クラウド事業者	クラウド事業者	クラウド事業者

5. セキュリティ

クラウドセキュリティの基礎

【クラウドサービスの基本要素】

管理コンソール・・・新しいインスタンスの作成・管理、パフォーマンス・ログの監視などをボタンで行う画面。管理用のユーザーのrootユーザーと通常作業用の一般ユーザーで行う

ファイアウォール・・・クラウドでファイアウォールを直接作成する。どのポート番号への通信を許可するのか、どのIPアドレスからのアクセスを許可するのかなどの設定をする

ルーティング・・・クラウド内でネットワークを構成することができる。内部ネットワークと外部ネットワークをそれぞれ作成して、インターネットに接続できるサーバーを分けることができる。

【クラウド利用時のセキュリティ/注意事項】

メンテナンス・・・クラウドサービス事業者によっては、メンテナンスの時間がある。メンテナンススケジュールは原則メールで通知されるため、確認することが必要。

リージョンの選択・・・AWSなどの大規模なクラウド事業者では、アジア、北米など地域ごとのデータセンターがあり、選択することができる。一つのリージョンに障害が発生した場合にサービスを継続できるように他のリージョンを障害時用の環境として用意することもできる。リージョンが遠いとネットワークの伝送時間がかかるのと保管されるデータが特定のリージョンでは違法になる場合もあるから注意が必要

特権ユーザーと非特権ユーザー・・・クラウドでは、ユーザーに応じて実行できる機能の範囲が異なる。特権ユーザーを利用できる人の範囲を制限する

API認証キー・・・クラウドサービスを外部から接続するにはAPIのキーを用いる。このAPIキーは外部に漏れないように管理することが必要