# 教育･研究クラウドサービスのためのパターンランゲージ

長久勝（NII）、谷沢智史（e-ambition）、山中顕次郎（NII）、吉岡信和（NII）、横山重俊（NII）

## 概要

著者らの国立情報学研究所（NII）クラウド運用チームは、4年に渡って、教育･研究のために利用されるクラウドサービス(IaaS)の構築･運用を行ってきた。その中で得られた知見を、ユースケースを構成する要素に分解した上で、パターンとして書き下し、パターンランゲージへの構成を試みる。

## はじめに

著者らのグループではこれまでに、2つのIaaSを実用に供しており、更に1つのIaaSを実用に向け準備している。3つのIaaSの簡単な特徴は以下の通りである。

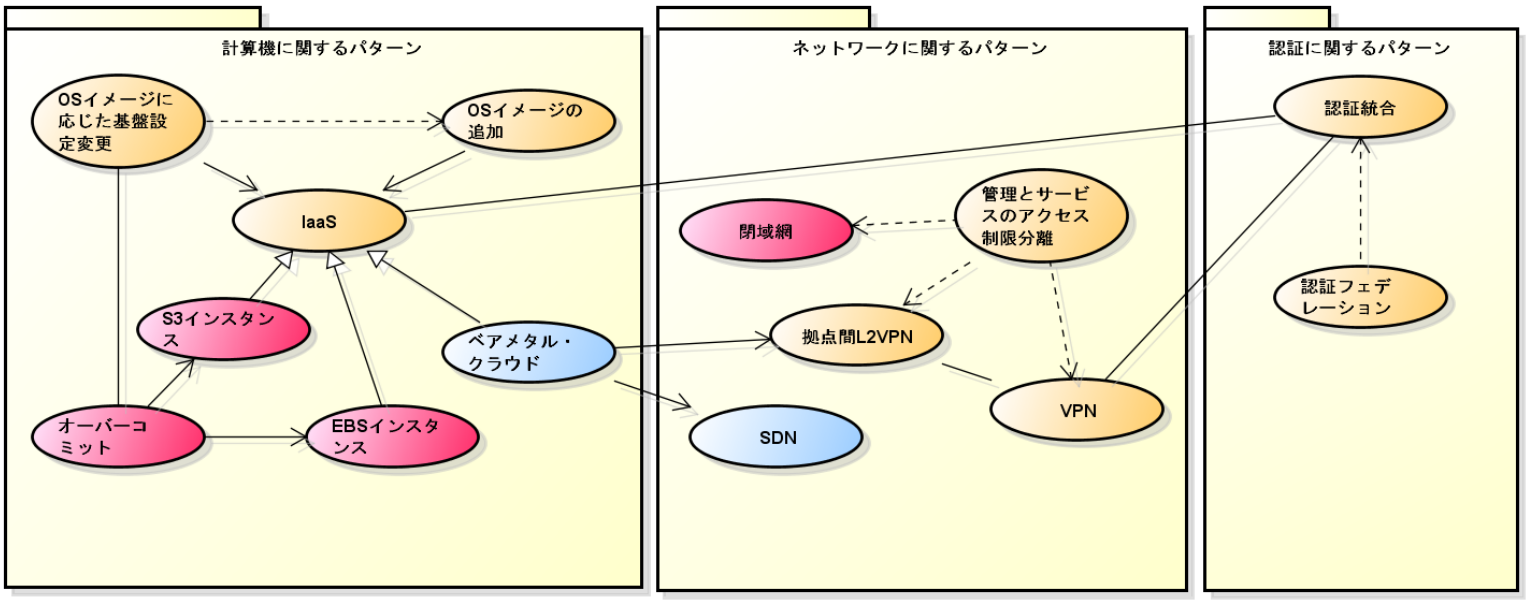
教育クラウド「edubaseCloud」2010-2015(予定)
EucalyptusベースのEC2互換IaaS
十数セットの独立したサイズ固定のクラウド基盤を閉域網で運用

研究クラウド「gunnii」2012-
OpenStack-dodaiベースのベアメタル･クラウド(IaaS)
基本的に所内研究者向けに提供
SDNにより所内ネットワークと透過的に接続され、
研究者が使っているネットワークにL2接続されたベアメタルマシンが貸し出される

アカデミックインタークラウド(AIC、プロトタイプ扱い、2014-)
OpenStack-dodaiベースのベアメタル･クラウド(IaaS)
基本的に所内研究者を含む研究グループ向けに提供
SDNによりSINET L2VPLSと透過的に接続され、
研究者が使っているネットワークにL2接続されたベアメタルマシンが貸し出される

著者らのグループでは、設計、構築、運用、フィードバック、のサイクルを回しながら、将来の大規模な実用化を見据えて、OSSベースのクラウドに取り組んできた。

以下に、我々の経験から得られた知見をパターン形式で記述する。




まず最初に、パターンマップを示す。
14のパターンは、「計算機に関するパターン」、「ネットワークに関するパターン」、「認証に関するパターン」に分類した。
パターンマップはユースケース図の文法を流用して描かれており、関連、一方にのみ誘導可能な関連、汎化、依存の関係を使用した。

名前：「IaaS」

文脈：
ソフトウェア工学教育における演習環境をどう実現し、管理・運用するか。様々な演習が行われるので、それらの演習を全て実施可能な演習環境が必要となる。

問題：
・物理的に用意できる教室環境は限られている
・異なる演習の間で、ソフトウェアの相性の問題から、環境を共有できない場合がある
・サーバ構築などの演習では、学生の操作によって計算機の状態が変更されるため、管理・運用が困難
・サーバ構築などの演習で、学生が誤った手順を実行した場合、計算機を正しい状態に戻すのに時間がかかり、演習の進行に支障をきたす

フォース：
・柔軟な演習環境を実現したい
・低コストで演習環境を実現したい

解決：
「IaaS」を適用する。
「IaaS」とは仮想的に計算機を借り受けるクラウドサービスの一種である。ネットワーク越しにオンデマンドで借りたマシンを操作でき、各種サーバとして用いたり、リモートデスクトップ環境として用いたりできる。

結果：
演習環境を教室の端末から切り離し、ネットワーク越しの仮想計算機で賄うことで、教室の端末数を超える計算機が提供できる。演習毎に異なる仮想マシンイメージを用意することで、演習環境は分離できる。使い終わったり、壊してしまった仮想計算機は廃棄し、新しい仮想計算機を使うことができる。学生が自身で仮想計算機の起動や停止ができる。

関連：
「IaaS」の実現手法として、計算機の仮想化技術を用いた「S3インスタンス」「EBSインスタンス」、物理マシンにネットワークの仮想化を組み合わせた「ベアメタル・クラウド」がある。
「IaaS」を利用する際のアカウント管理の問題については「認証統合」に詳しく述べる。

適用例：
筆者らの運用する、教育用途の"edubaseCloud"、研究用途の"gunnii"、"AIC"、など。他、多くの教育機関で、構築・運用が予定されている。

名前：「S3インスタンス」

文脈：
柔軟で低コストの演習環境を「IaaS」でプライベートクラウドとして構築することになった。

問題：
・仮想マシンイメージや動作中の仮想マシンのストレージを大量に収容するには、大規模なストレージ装置が必要となる。そしてそれは高価である
・仮想マシンの実行環境としての計算機資源を減らすと、演習環境の規模の縮小に直結するため、減らせない

フォース：
・柔軟で低コストの演習環境を実現したい
・仮想マシンの実行環境としての計算機資源を減らしたくない
・大規模なストレージ装置を持てない

解決：
「S3インスタンス」を適用する。
「S3インスタンス」とは「IaaS」の一種で、元になる仮想マシンイメージをストレージ装置から仮想マシンの実行環境となる計算機上にコピーして起動する。動作中の仮想マシンのスナップショットを保存するなどの操作を行わない場合、コピーを起動しているだけなので、仮想マシンを停止すると、その動作中のイメージは失われる。動作中のイメージをストレージ装置に置かないため、ストレージ装置の使用量を抑えることができる。

結果：
仮想マシンを停止するとそのイメージが失われる制約がつくが、安価に「IaaS」を構築できる。教材として予め用意された仮想マシンイメージを学生が使用し、短期間（演習時間のみ、課題を終えるまで、など）で使用を終えて廃棄するなら、支障はない。

関連：
「IaaS」の実現手法として、計算機の仮想化技術を用いた「S3インスタンス」「EBSインスタンス」、物理マシンにネットワークの仮想化を組み合わせた「ベアメタル・クラウド」がある。
「S3インスタンス」は、消えても良いが同じものをたくさん、という場合に向いており、「EBSインスタンス」は、消えると困る異なるものをたくさん、という場合に向いている。ただし、大規模なストレージ装置を用意できる場合、「S3インスタンス」を選択する理由はなくなる。

適用例：
"edubaseCloud"において、演習やハンズオンセミナに使うLinux仮想マシンとして、多用されている。

名前：「EBSインスタンス」

文脈：
柔軟で低コストの演習環境を「IaaS」でプライベートクラウドとして構築することになった。

問題：
・「S3インスタンス」は仮想マシンの停止で、その動作中のイメージが失われる。これは、物理マシンや、一般的な計算機の仮想化と挙動が異なる
・仮想マシンが、稼働中、データを蓄積していく場合、仮想マシンの停止で、その動作中のイメージが失われる「S3インスタンス」は、障害時にデータを失う

フォース：
・柔軟で低コストの演習環境を実現したい
・仮想マシンの動作中のイメージを永続化したい

解決：
大規模なストレージ装置を用意し、「EBSインスタンス」を適用する。
「EBSインスタンス」とは「IaaS」の一種で、仮想マシンの実行環境に永続化されたストレージをルートデバイスとしてマウントし起動する。永続化されたストレージを使うため、仮想マシンを停止しても、その動作中のイメージは保持される。障害で仮想マシンが停止しても、物理マシンの電源断相等のリスクで済む。ストレージの内容が失われる「S3インスタンス」よりも挙動が直感的（物理マシンや、一般的な計算機の仮想化と挙動が同じでストレージの内容が失われない）で利便性も高い。

結果：
仮想マシンのイメージの保持について、物理マシンと同程度の利便性、耐障害性を確保し、「IaaS」を構築できる。通年など長期にわたり、仮想マシンを学生らが各自に作り込んでいく、PBLなどの演習形態の運用性を高めることができる。

関連：
「IaaS」の実現手法として、計算機の仮想化技術を用いた「S3インスタンス」「EBSインスタンス」、物理マシンにネットワークの仮想化を組み合わせた「ベアメタル・クラウド」がある。
「S3インスタンス」は、消えても良いが同じものをたくさん、という場合に向いており、「EBSインスタンス」は、消えると困る異なるものをたくさん、という場合に向いている。ただし、大規模なストレージ装置を用意できる場合、「S3インスタンス」を選択する理由はなくなる。
現在、多くのパブリッククラウドが、標準的に、「EBSインスタンス」による「IaaS」を提供しており、演習環境をパブリッククラウドで調達する場合には、「EBSインスタンス」を用いることとなる。

適用例：

"edubaseCloud"において、Windowsによるリモートデスクトップ環境として適用された。

名前：「オーバーコミット」

文脈：
「IaaS」でプライベートクラウドとして構築した演習環境について、物理的に所有する量を超える計算機資源が必要になった。

問題：
・計算機の仮想化技術を用いた「S3インスタンス」もしくは「EBSインスタンス」環境において、物理的な拡張なしに所有する量を超える計算機資源を使いたい

フォース：
・物理的に所有する量を超える計算機資源を使いたい
・処理性能およびその安定は求めない

解決：
「オーバーコミット」を適用する。
「オーバーコミット」とは、仮想化技術によって物理資源以上の資源があるようにみせかけて擬似的に資源を割り当てることの総称である。ここでは特に、タイムシェアリングを応用して、物理的なCPUコア数を超えて仮想的なCPUを割り当てることで、起動できる仮想マシンの数を増やす手法を指す。基盤の構成にもよるが、計算機の仮想化技術を用いた「S3インスタンス」もしくは「EBSインスタンス」環境において、基盤の設定変更により実現できる。

結果：
物理的な計算機資源の拡張なしに、起動できる仮想マシンの数を増やすことができる。ただし、起動した全ての仮想マシンに対し、一斉に負荷を与えた場合、仮想マシン１台あたりの処理能力は低下する。また、仮想マシンがCPUコアを占有できず、仮想マシンの処理能力に揺らぎがでるため、ベンチマークなどの用途には不向きとなる。

関連：
「S3インスタンス」もしくは「EBSインスタンス」環境に適用が可能である。
現在、多くのパブリッククラウドが、主に経済性の問題から、「オーバーコミット」を適用した基盤でのサービス提供を行っている。演習環境をパブリッククラウドで調達する場合、一斉負荷の影響はあまりないと考えられるが、処理能力の保証されたサービスを明示的に使わないと、処理能力の揺らぎの問題がある。

適用例：
"edubaseCloud"において、基本的に「オーバーコミット」設定は行っていないが、Windowsによるリモートデスクトップ環境が不足した際に適用された。

名前：「ベアメタル・クラウド」

文脈：
研究環境を集約し、柔軟で低コストの研究環境を「IaaS」でプライベートクラウドとして構築することになった。研究目的の場合、貸し出される計算機の処理能力が重視される。

問題：
・計算機の仮想化技術を用いた「S3インスタンス」「EBSインスタンス」では、仮想化基盤が処理能力の一部を使うため、仮想マシンの処理能力に懸念がある
・計算機の仮想化技術を用いた「S3インスタンス」「EBSインスタンス」では、各種装置が仮想化されるため、仮想マシンの処理能力に懸念がある

フォース：
・柔軟で低コストの研究環境を実現したい
・計算機の仮想化は使いたくない

解決：
「ベアメタル・クラウド」を適用する。
「ベアメタル・クラウド」とは、計算機の仮想化技術を用いず、物理マシンを貸し出す「IaaS」である。
筆者らの構築した「ベアメタル・クラウド」では、「SDN」によるネットワークの仮想化を行っており、利便性を高めている。「ベアメタル・クラウド」は、研究や、柔軟に物理マシンのクラスタを構築するために使われ、ネットワークの柔軟性と、利用可能な処理能力を重視している。
「ベアメタル・クラウド」は、計算機の仮想化技術を経由しない分、「S3インスタンス」「EBSインスタンス」に比べ制限事項が少ない。計算能力の揺らぎに関する懸念もない。

結果：
「ベアメタル・クラウド」導入前と同じように物理マシンを研究環境として利用できる。不要な際に返却され、別の研究者が利用することで、個別に物理マシンを保有する場合に比べ、コストが低くなる。「SDN」によるネットワークの仮想化が行われている場合、物理マシンが所属するネットワークの切り替えがソフトウェアで即時に行われるため、結線変更などの物理的な操作なしに、オンデマンドで物理マシンを借りることができる。

関連：
「IaaS」の実現手法として、計算機の仮想化技術を用いた「S3インスタンス」「EBSインスタンス」、物理マシンにネットワークの仮想化を組み合わせた「ベアメタル・クラウド」がある。
筆者らの構築した「ベアメタル・クラウド」では、「SDN」によるネットワークの仮想化を行っている。

適用例：
"gunnii"、"AIC"。

名前：「OSイメージの追加」

文脈：
柔軟で低コストの研究･演習環境を「IaaS」でプライベートクラウドとして運用している。ユーザから、基盤に登録がないOSイメージ追加の、要望を受けた。また、基盤管理者は、安全性の観点から、サポート期限内のOSを使用させたい。

問題：
・「IaaS」上のマシンとして動作するには、基盤が前提とするデバイス構成、基盤の管理システムと正しく通信できるかなど、基盤に起因する制約があり、それを満たすように、OSイメージを作らなければならない
・OSイメージの登録に、基盤の管理者権限が必要な場合がある
・特定のOSが安全に使用できる期間は、そのライフサイクルに規定され、有限である

フォース：
・利用者は新しいOSイメージを使いたい
・基盤管理者はサポート期限内のOSを使用させたい
・OSイメージの作成、登録は簡単ではない

解決：
「OSイメージの追加」を適用する。
基盤の制約に沿った形で作成されたOSイメージを、基盤に登録し、利用者が使えるようにする。
OSイメージの作成は、基盤の制約が明文化されていたり、OSイメージ作成を支援するツールがある場合は、利用者自身が作成することができるが、そうでない場合は基盤に対する知識が要求され、利用者自身が作成することは困難となる。
作成されたOSイメージを基盤に登録する際、基盤の設計思想によっては、利用者権限で行えない場合があるが、これは利用者の利便性、基盤管理者の運用コスト、いずれの観点からも欠点となる。

結果：
利用者は、サポート期限内の、目的に合わせたOSを使うことができる。

関連：
基盤が設計･構築された時点で要求になかったOSや、その後に新しくリリースされたOSを提供するには、基盤自身の改変が必要なことがある。ソフトウェアの改修が必要な場合は、簡単に対応することができないが、「OSイメージに応じた基盤設定変更」で済む場合もある。

適用例：
筆者らの運用する「IaaS」では、ユーザの権限で「OSイメージの追加」が行えない（スナップショットはこれにあたらない）ため、利用者からの要望に合わせて、CentOSやUbuntuLTSを中心に運用チームが対応してきた。基盤構築時以降に、最初に用意したOSのサポートが終

了したり、メジャーバージョンアップが起こるため、「OSイメージの追加」なしに実用的な運用は困難である。

名前：「OSイメージに応じた基盤設定変更」

文脈：
柔軟で低コストの研究･演習環境を「IaaS」でプライベートクラウドとして運用している。
特定の「OSイメージの追加」に際して、現状の基盤のままでは対応できないことが分かった。

問題：
・基盤を構成するソフトウェアに対して、追加したいOSが新しい場合、OSのコアモジュールの変更などの影響で、基盤が要求する制約が満たせない場合がある
・基盤を構成するソフトウェアに対して、追加したいOSが設計の想定を超える場合（例えば、Linuxを想定した基盤におけるFreeBSDのサポートなど）、基盤が要求する制約が満たせない場合がある
・運用中の基盤は、そのように設計されていない限り、基盤を構成するソフトウェアの更新が困難である

フォース：
・ある特定のOSについて「OSイメージの追加」を行いたい
・ある特定のOSが運用中の基盤で動作しない
・運用中の基盤を構成するソフトウェアの更新は困難である

解決：
「OSイメージに応じた基盤設定変更」を適用する。
運用中の基盤を構成するソフトウェアの更新は困難であるが、それらの設定を変更することは更新に比べれば容易である。計算機の仮想化技術を使っている基盤の場合、計算機の仮想化層の設定を変更することで、特定のOSを動作させられる可能性がある。

結果：
利用者は、目的に合わせた特定のOSを使うことができる。ただし、技術的に実現できないこともある。

関連：
本パターンは「OSイメージの追加」の際に現れ得る問題への対策である。
基盤の設定変更は「オーバコミット」においても実施される。

適用例：
"edubaseCloud"では、1つの基盤について、計算機の仮想化層の設定を変更し、FreeBSDに対応した実績がある。この設定変更により、当該基盤上でのLinux利用の利便性が低下したが、"edubaseCloud"は複数の独立した基盤からなるため、当該基盤をFreeBSD専用と位置付け、他の基盤と区別して運用を行った。

名前：「管理とサービスのアクセス制限分離」

文脈：
柔軟で低コストの研究･演習環境を「IaaS」でプライベートクラウドとして構築することになった。「IaaS」内外の通信に関して、ポリシーを決めなければならない。

問題：
・利用者は借りたマシンの管理のために自由なアクセスを要求する
・公開サーバとして外部からのアクセスを要求する場合がある
・基盤の管理上、アクセスを制限したい

フォース：
・利用者は借りたマシンへのアクセスを、公開も含めて、自由にしたい
・基盤管理者は貸したマシンへのアクセスを制限したい

解決：
「管理とサービスのアクセス制限分離」を適用する。
貸し出されたマシンへのアクセスを管理とサービスに分けて考えることで、その制限に関する要件を整理しやすくなる。計算機資源が小さい場合には、個々のサーバの設定で実現することも可能だが、教育や研究においては、貸し出されたマシンの管理者が増える傾向があるため、管理を集約し、上位の管理者が対応した方がよい。

結果：
貸し出されたマシンに利用者が管理のためにアクセスする場合については、組織内のIPアドレスからポート制限なしに許可、外部へのサービス公開については、IPアドレスの制限なくhttpsのみ許可、などのポリシーを設定できる。事前にユースケースを検討した上でうえでポリシーを設定すれば、基盤管理者が個別対応を迫られる事案を減らせる。

関連：
貸し出されたマシンに利用者が管理のためにアクセスする必要はあるが、サービスは必ずしも公開するものではないため、「閉域網」で外部からのアクセスを遮断することも考えられる。管理のためのアクセスの柔軟性を確保するために「VPN」を使う場合がある。
筆者らの構築した「ベアメタル･クラウド」では、「SDN」を用いて、利用者がネットワークを持ち込むように作られており、通信に関するポリシーを利用者自身が決められるようになっている。

適用例：
"edubaseCloud"では、クラウド基盤毎に、サービス公開の有無を決め、そのポリシーに従って、ネットワーク機器の設定を設計している。

名前：「閉域網」

文脈：
柔軟で低コストの研究･演習環境を「IaaS」でプライベートクラウドとして構築することになった。ユースケースを検討した結果、サービスの外部公開は行わず、「IaaS」の安全性を優先した設計とする。

問題：
・利用者は借りたマシンの管理のために自由なアクセスを要求する
・不正アクセスを防ぎたい
・基盤の管理上、アクセスを制限したい

フォース：
・利用者は借りたマシンへのアクセスを自由にしたい
・基盤管理者は貸したマシンへのアクセスを制限したい

解決：
「閉域網」を適用する。
外部からのアクセスを遮断したネットワーク環境を”閉域網”と呼ぶが、ここでは特に、広く一般のユーザが、基盤内の計算機が提供するサービスを受けるためのアクセスについて、アクセスが遮断される環境を指すものとして「閉域網」を定義する。
外部からのアクセスを遮断するとしても、計算機資源を使う上での利便性のために、OSのリポジトリなど外部リソースへのアクセスが必要となるため、外部へのアクセスを許可することが一般的である。ただし、利用者の操作や不注意で不正なファイルを読み込み踏み台になる恐れは残るため、利便性と安全性のバランスを考慮した上で、外部へのアクセスを制限するポリシーを採用することもできる。
また、正規の権限を有した利用者が計算機資源にアクセスするために必要な外部からのアクセスを受け入れる必要はあり、特定のネットワークセグメントからのみ特定ポートへのアクセスを許可するなど、F/Wやスイッチにおいて、主にL3の機能を用いて設定を行う。

結果：
許可されたネットワーク以外からのアクセスを遮断することで、基盤内の計算機が外部からの不正なアクセスを受けることがなくなり、安全性が高まる。

関連：
「管理とサービスのアクセス制限分離」に照らすと、外部へのサービス公開を禁止したポリシーに該当する。
正規の権限を有した利用者が計算機資源にアクセスするために必要な外部からのアクセスを受け入れるために「VPN」を使うことができる。

適用例：
"edubaseCloud"では、特定のネットワークからしかアクセスを許さない設定を、標準としている。

名前：「VPN」

文脈：
柔軟で低コストの研究･演習環境を「IaaS」でプライベートクラウドとして構築することになった。ユースケースを検討した結果、アクセス元ネットワークで制限するのではなく、利用者単位でアクセスを制限したい。

問題：
・利用者は借りたマシンの管理のために自由なアクセスを要求する
・基盤の管理上、利用者単位でアクセスを制限したい

フォース：
・利用者は借りたマシンへのアクセスを自由にしたい
・基盤管理者は貸したマシンへのアクセスを利用者単位で制限したい

解決：
「VPN」を適用する。
アクセス元ネットワークで制限する場合は、ネットワーク機器の設定で実現できるが、利用者単位で制限する場合は、認証付のアクセス経路を用意する必要がある。「VPN」サーバを運用することで、アクセスが許可されたネットワークを経由して、もしくは基盤のネットワークセグメントに直接、アクセスを行うことができる。
また、殆どの「VPN」ソリューションは通信を暗号化して行うため、安全性にも寄与する。
ただし、多くの組織において、外部への「VPN」アクセスを認めないポリシーが採用されており、適用の障害となる場合がある。

結果：
アクセス元ネットワークで制限するのではなく、利用者単位でのアクセス制限が実現でき、基盤内の計算機が、利用者以外からの不正なアクセスを受けることがなくなり、安全性が高まる。

関連：
「管理とサービスのアクセス制限分離」に照らすと、貸し出されたマシンに利用者が管理のためにアクセスするためのポリシーの設定に該当する。
ユースケース上はアクセス元ネットワークの制限に該当するが、「VPN」と同じ技術で、拠点間の通信を暗号化する「拠点間L2VPN」がある。
「認証統合」が利用できると、「VPN」のためだけにアカウント管理をする必要がなくなる。

適用例：
"edubaseCloud"では、特定のネットワークからしかアクセスを許さないため、そのネットワーク内に「VPN」サーバを設置している。

名前：「拠点間L2VPN」

文脈：
柔軟で低コストの研究・演習環境を「IaaS」でプライベートクラウドとして構築することになった。ユースケースを検討した結果、キャンパスを跨いだ遠隔講義や組織を跨いだ共同研究のため、拠点を跨いで計算機資源を透過的に利用したい。

問題：
・拠点を跨いでL3で通信設定を行う場合、経路の安全性と、設計が複雑化する懸念がある

フォース：
・拠点に関わらず、利用者は論理的に同じ環境を使いたい

解決：
「拠点間L2VPN」を適用する。
拠点間をVPNでブリッジ接続し、L2レベルで繋がった、同一のネットワークセグメントに設定することができる。

結果：
異なる拠点で、同一のネットワークセグメントに属することができる。拠点に関わらず統一されたポリシーで、ネットワークを運用できる。

関連：
「管理とサービスのアクセス制限分離」に照らすと、貸し出されたマシンに利用者が管理のためにアクセスするためのポリシーの設定に該当する。
ユースケース上はアクセス元ネットワークの制限に該当するが、「VPN」と同じ技術で、拠点間の通信を暗号化する「拠点間L2VPN」がある。

適用例：
日本国内で教育・研究目的であれば、学術基盤ネットワーク”SINET”の、複数拠点間をL2VPNで結べる”L2VPLS”サービスを利用できる。”AIC”は、指定した”L2VPLS”上に物理マシンを借りる「ベアメタル・クラウド」となっており、複数拠点にまたがる安全なネットワーク上で計算機資源共有を実現している。

名前：「SDN」

文脈：
柔軟で低コストの研究･演習環境を「IaaS」でプライベートクラウドとして構築することになった。ユースケースを検討した結果、ネットワーク構成を柔軟に変更できるようにしたい。

問題：
・L3/L2の機器で階層的に構築されたネットワークでは、柔軟な設定変更が困難である
・L3/L2の機器で階層的に構築されたネットワークでは、ネットワーク構成の変更に、物理的な結線の変更が必要となる場合が多い

フォース：
・ネットワーク構成を柔軟に変更したい
・L3/L2の機器で階層的に構築されたネットワークは、柔軟に変更できない

解決：
ネットワークの仮想化技術である「SDN」を適用する。
ソフトウェアによりネットワーク構成を定義する「SDN」を用いることで、複雑な構成の仮想ネットワークを、単純な結線構造の物理ネットワーク上に実現できる。物理的な結線構造を変えることなく、仮想ネットワークを柔軟に変更できる。

結果：
必要な時に、柔軟に、論理的なネットワーク構成を変更できる。異なるネットワーク間の基盤内での直接通信を遮断しつつ、必要に応じて、計算機の属するネットワークを変更するなどできる。

関連：
計算機の仮想化技術を用いた「S3インスタンス」「EBSインスタンス」は、ネットワークについての柔軟性を確保しやすいが、物理マシンのネットワークに柔軟性を持たせる必要がある「ベアメタル･クラウド」では「SDN」でそれを達することができる。

適用例：
"gunnii"、"AIC"では、SDN実装技術OpenFlowを採用することで、利用者が保有するネットワークをクラウド基盤上に延伸し、そのネットワーク内に計算機資源を借りることができる。計算機資源とネットワークの結びつきはクラウド基盤上のソフトウェアによって設定され、柔軟に変更できる。

名前：「認証統合」

文脈：
柔軟で低コストの研究･演習環境を「IaaS」でプライベートクラウドとして構築することになった。「VPN」などのサブシステムも含め、設備利用に対して、利用者を認証しなければならない。

問題：
・教育･研究目的の場合、学科全体など、利用者が多くなる傾向がある
・教育･研究目的の場合、入学、卒業、転籍など、利用者の入れ替わりが多くなる傾向がある
・アカウント管理は、データの安全性なども求められ、運用コストが高い

フォース：
・利用者を認証しなくてはならない
・複数のシステムで認証しなくてはならない
・アカウント管理は高コスト

解決：
「認証統合」を適用する。
クラウドサービスは相対的に多くのユーザを抱える傾向があり、かつ、サービス全体が複数のサブシステムで構成される場合があるため、個々のサブシステム単位でアカウント管理を行うことは非現実的である。従って、認証サーバを中核とした認証統合を構成する必要がある。

結果：
利用者を適切に認証し、かつ、アカウント管理を最低限に抑えることができる。

関連：
アカウント管理の主体を「認証フェデレーション」に移譲することで、アカウント管理のコストを更に下げることができる。

適用例：
"edubaseCloud"では、「IaaS」、「VPN」、付帯する教育用システム（シンクライアントやLMS、講義動画視聴システム）の認証を統合しており、全て同じアカウント情報で利用できる。

名前：「認証フェデレーション」

文脈：
柔軟で低コストの研究･演習環境を「IaaS」でプライベートクラウドとして構築することになった。「VPN」などのサブシステムも含め、設備利用に対して、利用者を認証しなければならない。利用者のアカウント管理の手間をかけたくない。

問題：
・「認証統合」を行っても、アカウント管理は必要である
・申請者の実在証明が必要になった場合、対応が困難である

フォース：
・「認証統合」にアカウント管理が必要である
・アカウント管理をしたくない

解決：
「認証フェデレーション」を適用する。
アカウントを管理し、認証問い合わせに対応する、アイデンティティプロバイダを利用する。複数のアイデンティティプロバイダを透過的に利用できる「認証フェデレーション」を使うことで、特定の1つの組織ではなく、さまざまな組織からの利用者を受け入れることができる。保有するさまざまなシステムで、「認証フェデレーション」が提供する認証方式を用いることで、アカウント管理を移譲できる。

結果：
利用者を適切に認証し、かつ、自前の認証サーバを不要とできる。

関連：
「認証フェデレーション」が提供する認証方式で技術的にカバーできない部分については、自前の認証サーバによる「認証統合」で対応することも考えられる。

適用例：
“学認”はShibboleth認証を基盤とする「認証フェデレーション」であり、認証サーバ（IdP）とサービス(SP)を多対多で結びつけることができる。1つのサービスの認証に複数の認証サーバが使えるようになっており、異なる組織に属するメンバからなる研究グループであっても、認証は各々の所属機関のIdPが使える。これにより、サービス側でユーザ認証機構を独自に設計、実装、管理するコストが減らせる。
"gunnii"、"AIC"は、“学認”のSPとなっており、認証時のパスワードは、基盤側に保有していない。
筆者らのグループでは、“学認”上でグループを作ることができる"mAP"に注目し、“学認”上でグループと、設備の利用権限を紐付ける仕組みを検討中である。

## さいごに

パターンの中には、経験から有用であることがはっきりしているものと、今後さらに考察を重ねなければならないものが混在している。例えば、「オーバコミット」は、その文脈において定番として適用できるだろうが、「OSイメージの追加」は、今後の基盤設計において、課題となる部分である。14のパターンをプラクティスとしてだけではなく、教育・研究目的のIaaSを構築・運用する際の視点として活用いただけるのではないかと考えている。

筆者らのグループは、ベンダロックインされない、OSSベースのIaaS基盤にこだわり、我々が先行事例となって、後に続く取り組みに先駆けて、問題点を洗い出す存在になれればと考えている。内外の事例との関係など、より有益な情報をまとめていく活動も進めていく必要もあるが、十分なアウトプットをできないでいる。今後は情報共有にも力を入れていきたい。