

Amazon Web Services

ネットワーク入門

sizu

Caphter 5

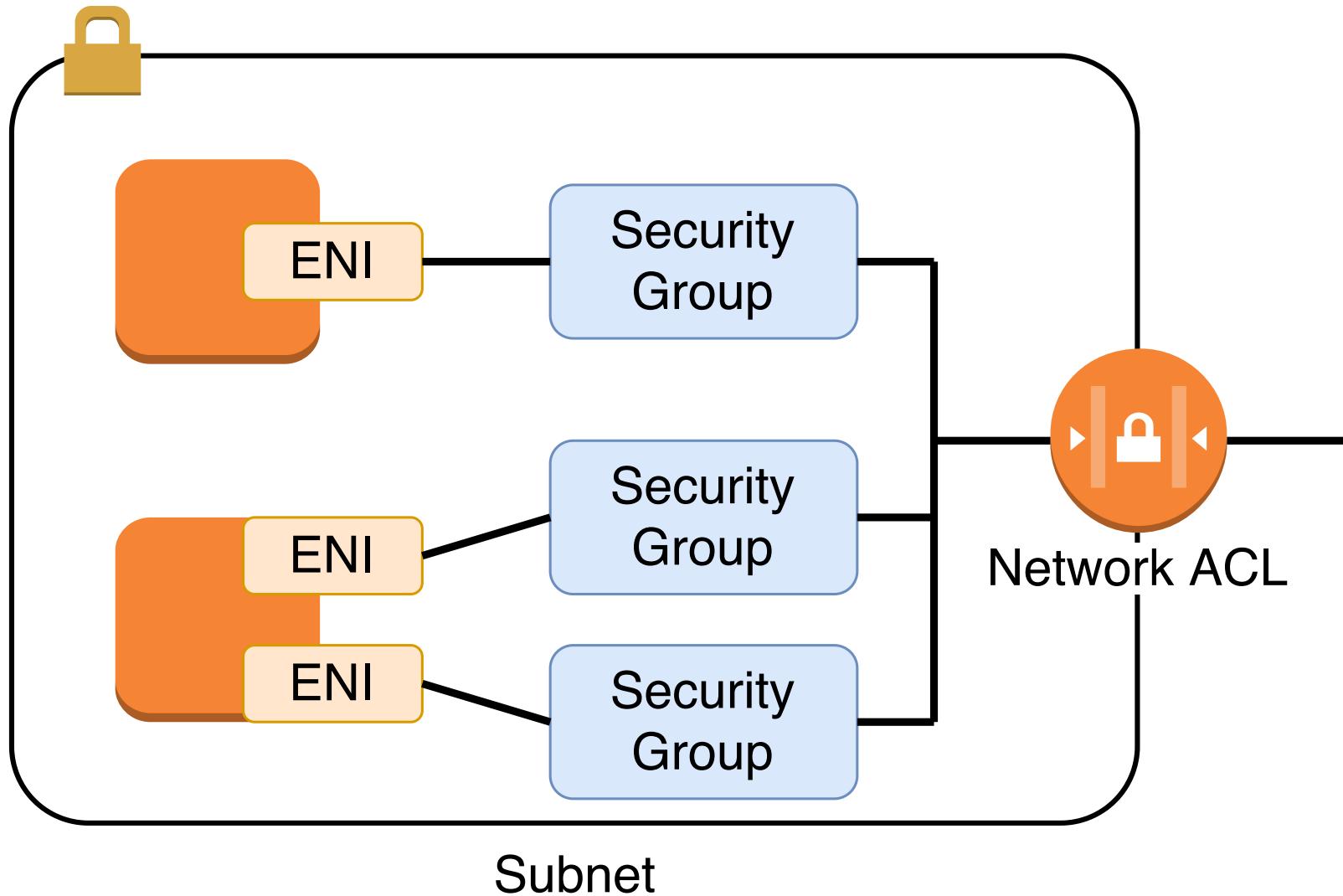
セキュリティグループと
ネットワーク ACL

AWS のファイアウォール機能

- ネットワーク ACL
 - サブネット全体のセキュリティを構成
 - ・ 「社内 LAN の IP アドレスからのみアクセス可能」
 - ・ 「特定のポートのみ通過可能」
- セキュリティグループ (SG)
 - EC2 インスタンスに対してセキュリティを構成
 - インスタンス上のサービスを考慮
 - ・ セキュリティグループのデフォルトは 22/TCP
 - ・ Web サーバを運用するなら 80/TCP (HTTP), 443/TCP (HTTPS)

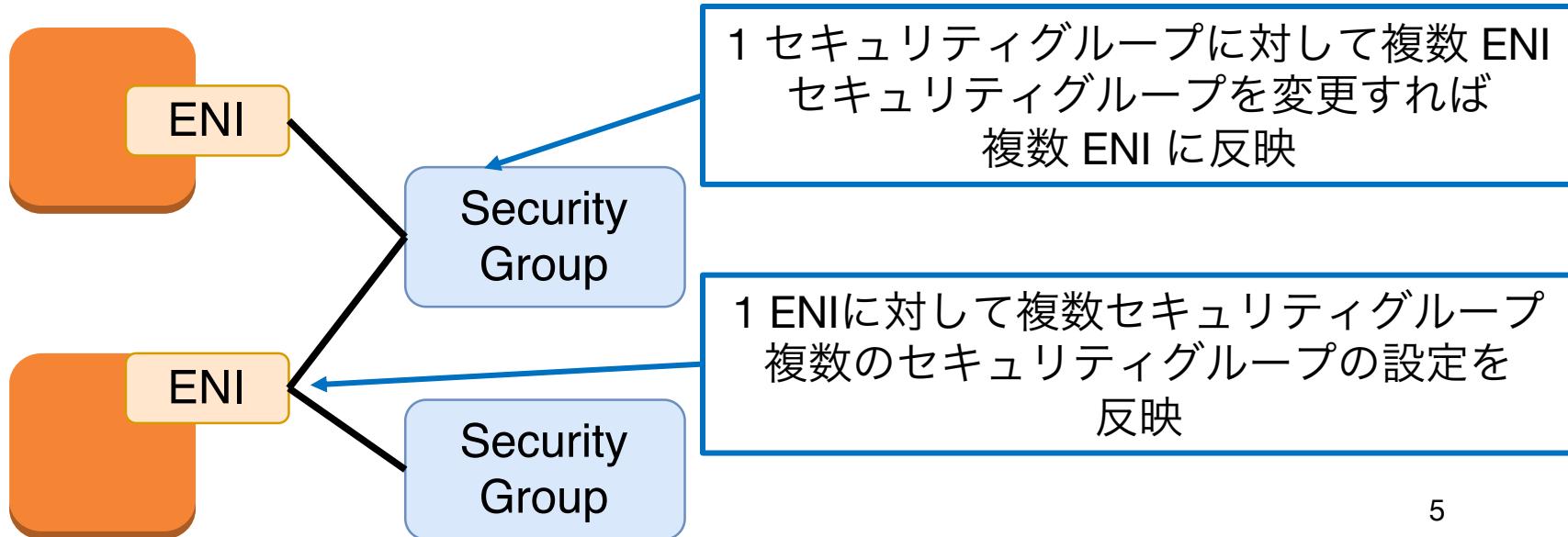
項目	セキュリティグループ	ネットワーク ACL
対象	ENI 単位	サブネット単位
設定メニュー	EC2 メニュー	VPC メニュー
ルール	許可ルールのみ	許可と拒否ルール
評価順序	全てをチェック	指定した順序でチェック
動作	stateful (何故...?)	stateless

VPC のファイアウォール模式図



セキュリティグループ

- ENI 向けのパケットフィルタリング機能
 - デフォルトでは SSH のための 22/TCP のみ
 - デフォルトの名前は “launch-wizard-<incremental number>”
 - Chapter 3 で “webserverSG” に改名
- ENI とセキュリティグループは多対多
 - 1 つの ENI に対して 5 つのセキュリティグループ
 - 1 つのセキュリティグループに対して複数の ENI



ENI から SG の確認

- EC2 ダッシュボードから確認

The screenshot shows the AWS EC2 Network Interface Details page. On the left, a sidebar menu is open under the 'Network & Security' section, with 'Network Interfaces' highlighted. The main content area displays a table of network interfaces. A specific row for interface 'eni-05c10f3cf4...' is selected. In the 'Security Groups' column, the value 'webserverSG' is shown, with a tooltip: 'セキュリティグループ: webserverSG. インバウンドルールの表示、アウトバウンドルールの表示'. This tooltip is highlighted with a red rectangle. The interface details table includes columns for Name, Subnet ID, VPC ID, Zone, Security Group, Description, Instance ID, Status, and IP.

Name	Subnet ID	VPC ID	Zone	Security Group	Description	Instance ID	Status	IP
eni-05c10f3cf4...	subnet-0e3f86...	vpc-03eae910...	ap-northeast...	webserverSG	Primary netwo...	i-07dd97edf70275668	in-use	52

Network Interface Details:

詳細	フローログ	タグ
ネットワークインターフェイス ID: eni-05c10f3cf4e23b2dc		
VPC ID: vpc-03eae910cc3d48377		
MAC アドレス: 06:e5:e7:e4:fd:88		
セキュリティグループ: webserverSG. インバウンドルールの表示、アウトバウンドルールの表示		
ステータス: in-use		
プライベート DNS (IPv4): -		
セカンダリプライベート IPv4 IP: -		
Elastic Fabric Adapter: 無効		
アタッチメント ID: eni-attach-0b68893b420582376		
アタッチメントの所有者: 546432839391		
アタッチメントのステータス: attached		
Elastic IP 所有者: amazon		
関連付け ID: -		
サブネット ID: subnet-0e3f8685bf82aca89		
アベイラビリティーゾーン: ap-northeast-1a		
説明: Primary network interface		
ネットワークインターフェイスの所有者: 546432839391		
プライマリプライベート IPv4: [REDACTED]		
IPv4 パブリック IP: [REDACTED]		
IPv6 IP: -		
送信元/送信先チェック: true		
インスタンス ID: i-07dd97edf70275668		
デバイスインデックス: 0		
終了時に削除: true		
割り当て ID: -		
Outpost ID: -		

EC2 インスタンスから SG の確認

- EC2 ダッシュボードから確認

The screenshot shows the AWS EC2 Instances dashboard. On the left, a sidebar lists navigation options like New EC2 Experience, Events, Tags, Reports, Quotas, and detailed sections for Instances, AMIs, and Elastic Block Store. The main area displays a single instance named 'mywebserver' with the following details:

フィールド	値
インスタンス ID	i-07dd97edf70275668
インスタンスの状態	running
インスタンスタイプ	t2.micro
アベイラビリティゾーン	ap-northeast-1a
パブリック IP	52.193.37.1
プライベート DNS	ip-10-0-0-81.ap-northeast-1.compute.internal
セカンダリプライベート IP	[REDACTED]
VPC ID	vpc-03eae910cc3d48377 (myvpc01)
サブネット ID	subnet-0e3f8685bf82aca89 (mysubnet01)
ネットワークインターフェイス	eth0
IAM ロール	-
キーペア名	mykey
パブリック DNS (IPv4)	-
IPv4 パブリック IP	[REDACTED]
IPv6 IP	-
Elastic IP	-
アベイラビリティゾーン	ap-northeast-1a
セキュリティグループ	webserviceSG. インバウンドルールの表示、アウトバウンドルールの表示
予定されているイベント	予定されているイベントはありません
AMI ID	amzn2-ami-hvm-2.0.20200406.0-x86_64-gp2 (ami-0f310fc6d6141e627)
Platform details	-
Usage operation	-
送信元/送信先チェック	True
T2/T3 無制限	無効

Two specific fields are highlighted with red boxes: 'セキュリティグループ' (Security Group) and its value 'webserviceSG. インバウンドルールの表示、アウトバウンドルールの表示'.

SG の一覧確認・設定

- EC2 ダッシュボードから確認
- インバウンド / アウトバウンドの 2 種類を設定
 - インバウンド: EC2 インスタンスに入る方向
 - アウトバウンド: EC2 インスタンスから出る方向

The screenshot shows the AWS EC2 Security Groups management interface. On the left, a sidebar lists various AWS services. The main area displays a table of security groups, with one row selected for detailed view. A red box highlights the 'セキュリティグループ New' link in the sidebar. Another red box highlights the 'インバウンドルール' tab in the detailed view. A blue arrow points from the text 'それぞれ 50 個のルールを設定可能' to the 'インバウンドルール' tab. A blue box highlights the 'アウトバウンドルール' tab.

aws サービス リソースグループ

New EC2 Experience Tell us what you think

▼ イメージ
AMI
バンドルタスク

▼ ELASTIC BLOCK STORE
ボリューム
スナップショット
ライフサイクルマネージャー

▼ ネットワーク & セキュリティ
セキュリティグループ New
Elastic IP New
プレイスメントグループ New
キーペア New
ネットワークインターフェイス
▼ ロードバランシング
ロードバランサー
ターゲットグループ

EC2 > セキュリティグループ

セキュリティグループ (1/3) 情報

セキュリティグループ... セキュリティグループ... VPC ID 説明 所有者

sg-0d1c69ae2ecec7a15 webserverSG vpc-03eae910cc3d48377 launch-wizard-1 create... 546432839391

sg-0d1c69ae2ecec7a15 - webserverSG

詳細 インバウンドルール アウトバウンドルール

それぞれ 50 個のルールを設定可能
拒否ルールは設定不可能

詳細

セキュリティグループ名: webserverSG
セキュリティグループ ID: sg-0d1c69ae2ecec7a15
説明: launch-wizard-1 created 2020-04-11T20:11:06.365+09:00
VPC ID: vpc-03eae910cc3d48377

ルールの設定

- ・編集 -> ルールの追加で設定可能

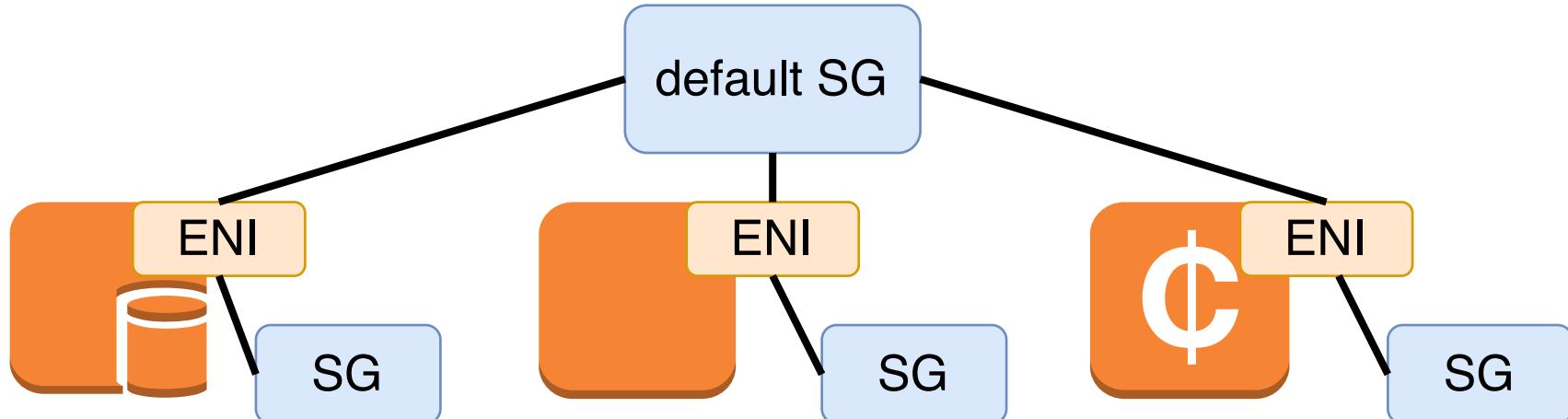
項目	内容	
タイプ	通信するタイプを指定 (TCP / UDP / ICMP / その他)	
プロトコル	<p>プロトコルを指定</p> <ul style="list-style-type: none">タイプで「カスタム ICMP ルール」を選ぶと どのプロトコルを通すか指定（「エコー応答」など）タイプで「カスタム」を選ぶとプロトコル番号を指定タイプで TCP / UDP を選ぶと指定なし	
ポート範囲	<p>ポートの範囲を指定</p> <ul style="list-style-type: none">単一のポート番号を入力（“80”）番号範囲を “-” で指定（“10000-10080”）	
送信元 または 送信先	カスタム	CIDR / IP アドレス / セキュリティグループで指定
	任意の場所	全ての場所を意味（0.0.0.0/0 と同意）
	マイ IP	AWS マネジメントコンソールを操作している端末 IP を設定

SG 同士での通信

- SG のルールで SG を設定できるという特徴
 - EC2 インスタンスの IP は動的割り当て
 - SG 指定の方がインスタンスの特定が容易
 - 運用上 SG 同士で通信できる構成
 - 「同じ SG 設定のインスタンス同士で無制限に通信可能」
- default SG
 - 同じ SG 設定のインスタンス間の通信を実現
 - 「送信元が自分自身の SG」 というインバウンドルール
 - default SG の設定から確認可能

SG 同士での通信

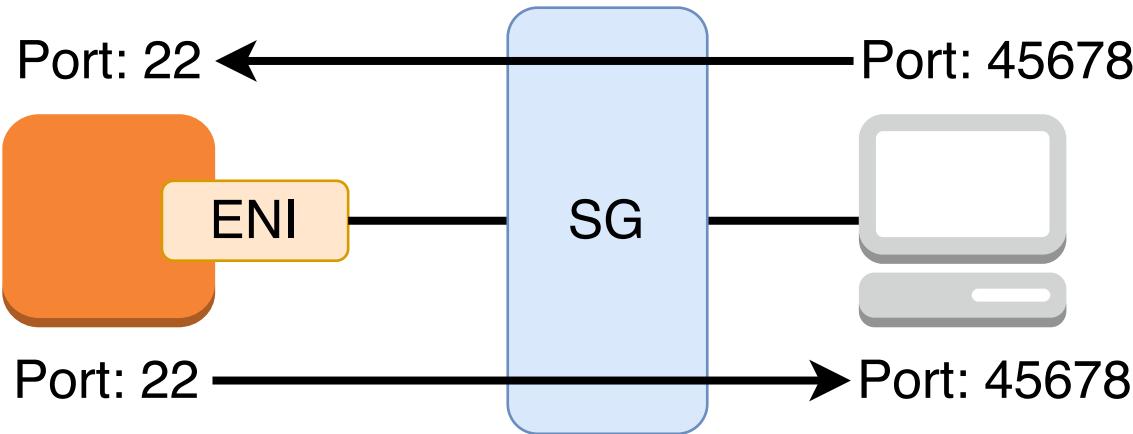
- SG のルールで SG を設定できるという特徴
 - EC2 インスタンスの IP は動的割り当て
 - SG 指定の方がインスタンスの特定が容易
 - 運用上 SG 同士で通信できる構成
 - ・ 「同じ SG 設定のインスタンス同士で無制限に通信可能」
- default SG
 - 同じ SG 設定のインスタンス間の通信を実現
 - 「送信元が自分自身の SG」 というインバウンドルール
 - ・ default SG の設定から確認可能



ステートフルなルール

- エフェメラルポート

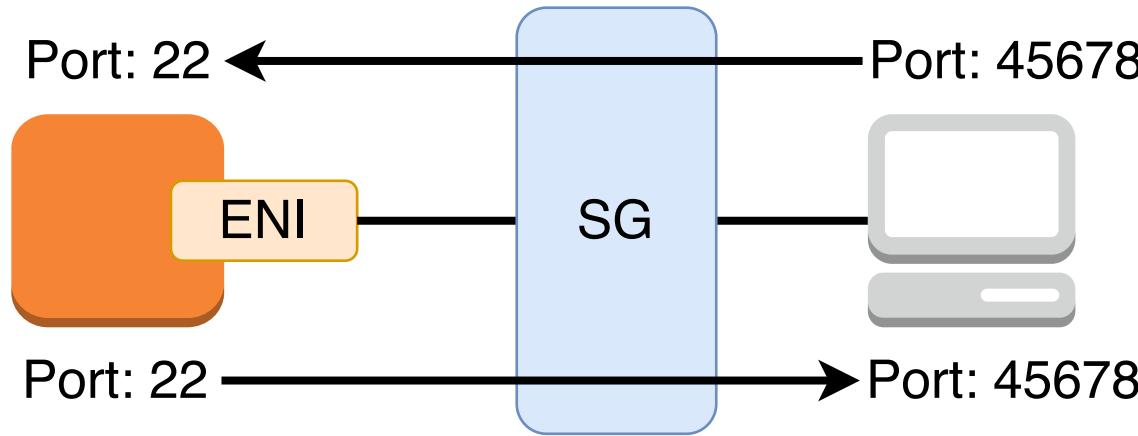
- クライアント - サーバ通信を行う際にクライアント側でランダムに割り当てられるポート番号
 - 予約されていないポート番号



ステートフルなルール

- エフェメラルポート

- クライアント - サーバ通信を行う際にクライアント側でランダムに割り当てられるポート番号
 - 予約されていないポート番号

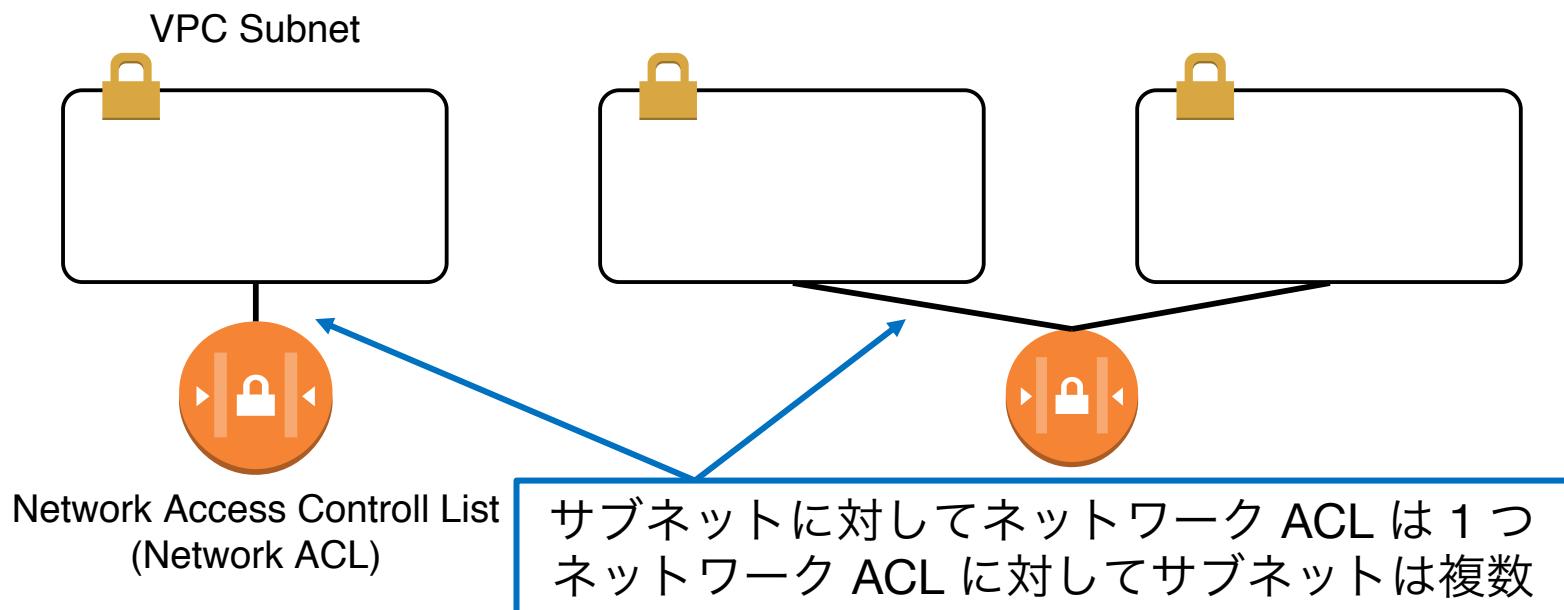


- アウトバウンドの設定が難しい

- 何故ならエフェメラルポートは動的割り当てだから
- SG はエフェメラルポートを自動追跡してくれる
 - ステートフル
 - インバウンドだけ設定すればよい

ネットワーク ACL

- サブネットに備わるパケットフィルタリング機能
- サブネットに対して 1 対多
 - 1 ネットワーク ACL に対して複数のサブネット
 - 1 サブネットに対して 1 ネットワーク ACL
- インバウンド / アウトバウンドの 2 種類のルール



VPC のネットワーク ACL 確認

- VPC ダッシュボードから確認
 - 明示的に設定しなければ
デフォルトのネットワーク ACL が設定

The screenshot shows the AWS VPC Network ACL configuration page. On the left, a sidebar lists various VPC-related services: VPC, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IP, Endpoints, Endpoints Services, NAT Gateways, Peering Connections, and Security Groups. The 'Subnets' item is highlighted with a red box.

The main content area displays a table of subnets. One subnet, 'mysubnet01', has its 'Network ACL' tab selected, also highlighted with a red box. The table includes columns for Name, Subnet ID, Status, VPC, IPv4 CIDR, IPv6 CIDR, and Availability Zone.

Below the table, a section titled 'Network ACL' shows the associated Network ACL (acl-02ee6a59e7e011bc6) and its inbound rules:

ルール #	タイプ	プロトコル	ポート範囲 / ICMP タイプ	ソース	許可 / 拒否
100	すべての ト...	すべて	すべて	0.0.0.0/0	ALLOW
*	すべての ト...	すべて	すべて	0.0.0.0/0	DENY

ネットワーク ACL の確認

- VPC ダッシュボードから確認
 - 全ネットワーク ACL の確認 / 作成 / 設定変更などが可能
 - VPC 領域あたり最大 200 個
 - インバウンド / アウトバウンドの 2 種類を設定
 - デフォルトではどちらも「全ての通信を許可する」

The screenshot shows the AWS VPC Dashboard. On the left sidebar, under the 'セキュリティ' section, the 'ネットワーク ACL' item is highlighted with a red box. The main content area displays a table of Network ACLs. A red box highlights the 'インバウンドのルール' tab in the navigation bar below the table. The table data is as follows:

Name	ネットワーク ACL	関連付け	デフォルト	VPC	所有者
acl-02ee6a59e7e0...	subnet-0e3f8685b...	はい	vpc-03eae910cc3d48377 myvpc01	546432839391	
acl-d2823eb4	3 個のサブネット	はい	vpc-6a9d920d	546432839391	

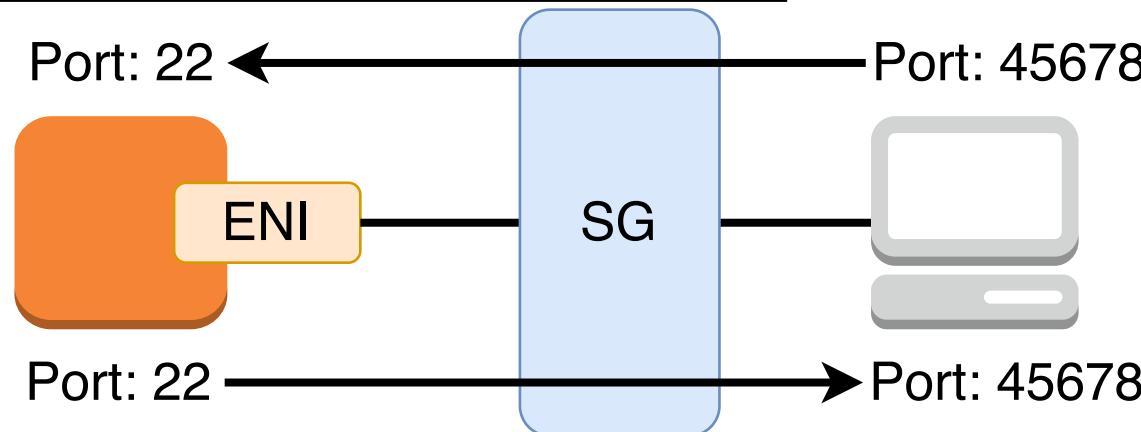
Below the table, a detailed view for 'Network ACL: acl-02ee6a59e7e011bc6' is shown. The 'インバウンドのルール' tab is selected and highlighted with a red box. The details are:

- ネットワーク ACL ID: acl-02ee6a59e7e011bc6
- 関連付け: subnet-0e3f8685bf82aca89
- 所有者: 546432839391
- デフォルト: はい
- VPC: vpc-03eae910cc3d48377 | myvpc01

ネットワーク ACL の SG との差分

- 拒否ルールを設定可能
- 順序番号の若い順に適応
 - ルールには番号が設定可能, 若い順に判定 / 適応
 - 一度適応されると, それ以降は判定されない
- ステートレス
 - アウトバウンドも設定する必要

基本的には SG の設定項目と一緒に



- 最後は必ず拒否ルール
 - 全てのトラフィックを拒否する設定
 - 通したいトラフィックは明示的に指定

ネットワーク ACL の使い所さん

- ネットワーク ACL はサブネットに対する設定
 - 誤った EC2 インスタンスの SG 設定を仕込んでも外側のネットワーク ACL の時点で drop 可能
- ネットワーク ACL はステートレス
 - TCP / UDP のポート単位で設定を仕込むのはしんどい
 - そこはSG よりも難しい

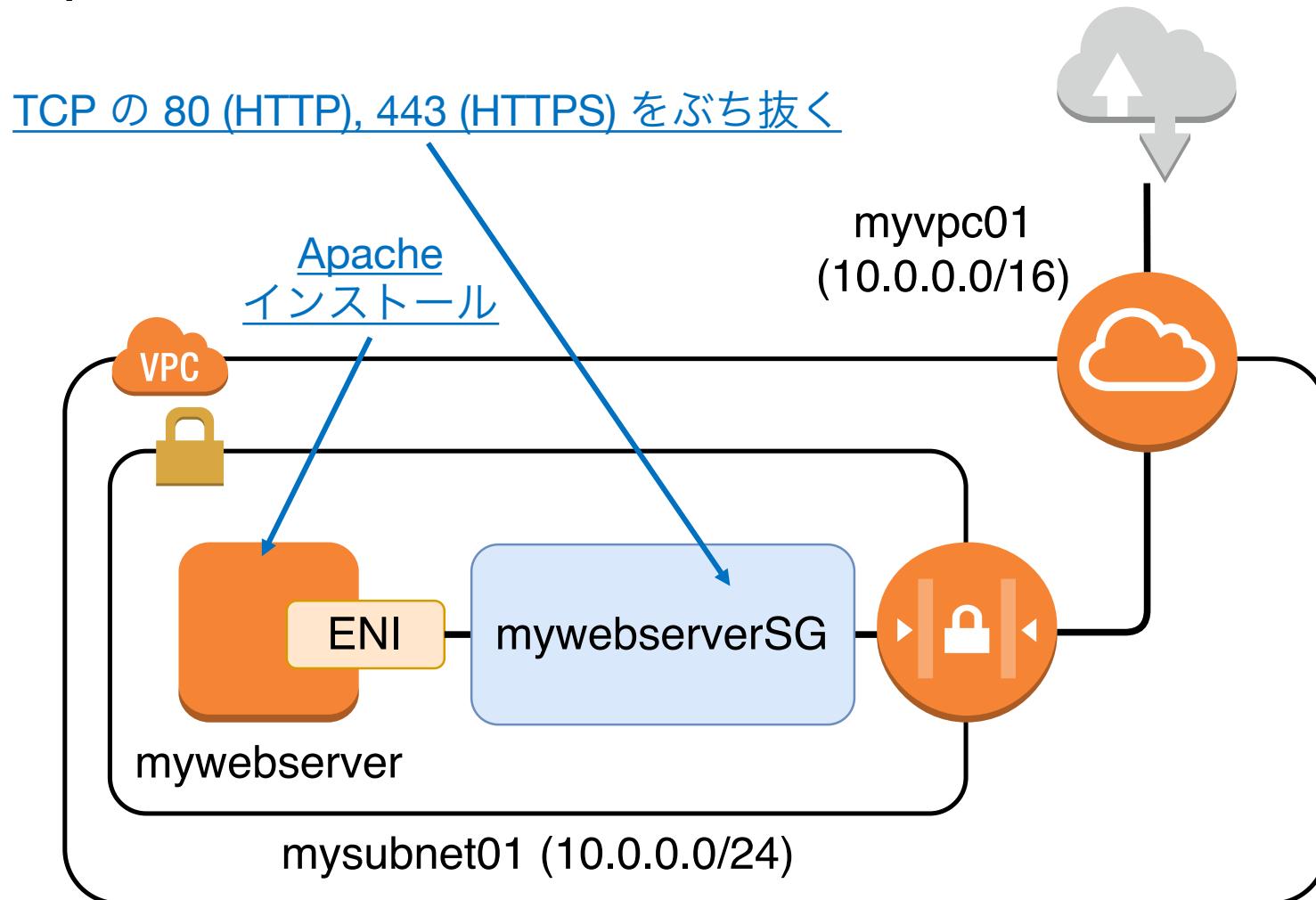
ネットワーク ACL の使い所さん

- ネットワーク ACL はサブネットに対する設定
 - 誤った EC2 インスタンスの SG 設定を仕込んでも外側のネットワーク ACL の時点で drop 可能
- ネットワーク ACL はステートレス
 - TCP / UDP のポート単位で設定を仕込むのはしんどい
 - そこはSG よりも難しい
- 「IP アドレスの粒度で設定をする」のがオススメ
 - 「社内 IP アドレスからのみ通信可能」
 - EC2 インスタンスの SG 設定に関係せず
社内からのみアクセス可能

実習

HTTP / HTTPS 通信可能な SG 設定

- mywebserver (EC2 インスタンス) に Apache をインストールして Web サーバ化



Apache インストール

1. EC2 インスタンスに SSH
 2. Apache インストール
 - \$ sudo yum install -y httpd
 3. Apache の起動
 - \$ sudo service httpd start
- Apache ってなあに？
 - <https://httpd.apache.org/>
 - Web サーバソフトウェア
 - (httpd としてインストールできるということは標準化されているの?)

SG の変更

- 現段階でアクセスしても何も出ない
 - http://EC2 インスタンスのパブリック IP アドレス/
 - SG の 80, 443/TCP をぶち抜いてないから
- ぶち抜く方法は 2 つ

SG の変更

- 現段階でアクセスしても何も出ない
 - http://EC2 インスタンスのパブリック IP アドレス/
 - SG の 80, 443/TCP をぶち抜いてないから
- ぶち抜く方法は 2 つ
 - 既存の SG の設定変更
 - 簡単かつ理解しやすい
 - 80, 443/TCP を許可する別の SG を作成して適応
 - メリットは... ?

SG の変更

- 現段階でアクセスしても何も出ない
 - `http://<EC2 インスタンスのパブリック IP アドレス>/`
 - SG の 80, 443/TCP をぶち抜いてないから
- ぶち抜く方法は 2 つ
 - 既存の SG の設定変更
 - 簡単かつ理解しやすい
 - 80, 443/TCP を許可する別の SG を作成して適応
 - 複数の Web サーバにこの設定を適応させる場合,
SG の使い回しが可能になる
 - 今回は簡単のため前者のアプローチを採用

80, 443/TCP を通す (1/2)

1. インバウンドを編集

- EC2 ダッシュボードからアクセス

The screenshot shows the AWS EC2 Security Groups interface. On the left sidebar, under the 'Network & Security' section, the 'Security Groups' item is highlighted with a red box. In the main content area, a security group named 'sg-0d1c69ae2ecec7a15' is selected. Below it, the 'Inbound Rules' tab is selected and highlighted with a red box. A second red box highlights the 'Edit inbound rules' button in the top right corner of the rule table.

EC2 > セキュリティグループ

セキュリティグループ (1/3) 情報

セキュリティグループ... webserverSG

VPC ID: [vpc-03eae910cc3d48377](#)

説明: launch-wizard-1 create...

所有者: 546432839391

sg-0d1c69ae2ecec7a15 - webserverSG

詳細 インバウンドルール アウトバウンドルール タグ

インバウンドルール

タイプ	プロトコル	ポート範囲	ソース	説明 - オプション
SSH	TCP	22	0.0.0.0/0	-

80, 443/TCP を通す (1/2)

2. ルールを追加

3. 80 (HTTP) / 443 (HTTPS) のルールを追加

The screenshot shows the AWS EC2 Security Groups inbound rules editor. The top navigation bar includes the AWS logo, service dropdowns (サービス), resource group dropdown (リソースグループ), and account information (suzu, 東京, サポート).

The current path is: EC2 > セキュリティグループ > sg-0d1c69ae2ecec7a15 - webserverSG > インバウンドのルールの編集.

The main title is "インバウンドのルールの編集" (Edit Inbound Rules) with a "情報" (Information) link.

A note below states: "インバウンドルールは、インスタンスに到達できる着信トラフィックを制御します。" (Inbound rules control incoming traffic to your instances.)

A red box highlights the instruction: "任意の場所 (0.0.0.0/0) を設定" (Set to Anywhere (0.0.0.0/0)).

The rule table has four columns: Type, Protocol, Port Range, and Source. The first row (SSH) is disabled. The second row (HTTP) and third row (HTTPS) are selected and highlighted with red boxes.

Type	Protocol	Port Range	Source
SSH	TCP	22	カスタム
HTTP	TCP	80	カスタム
HTTPS	TCP	443	カスタム

A red box also highlights the "ルールを追加する" (Add Rule) button at the bottom left.

A warning message in a box states: "注意: 既存のルールを編集すると、編集されたルールが削除され、新しい詳細で新しいルールが作成されます。これにより、そのルールに依存するトラフィックは、新しいルールが作成されるまでの短い期間、ドロップされます。" (Warning: When you edit an existing rule, the edited rule is deleted and a new rule is created with the new details. As a result, traffic dependent on that rule will be dropped during the short period it takes for the new rule to be created.)

At the bottom right, there are three buttons: "キャンセル" (Cancel), "変更のプレビュー" (Preview changes), and a red-highlighted "ルールの保存" (Save rule) button.

おまけ

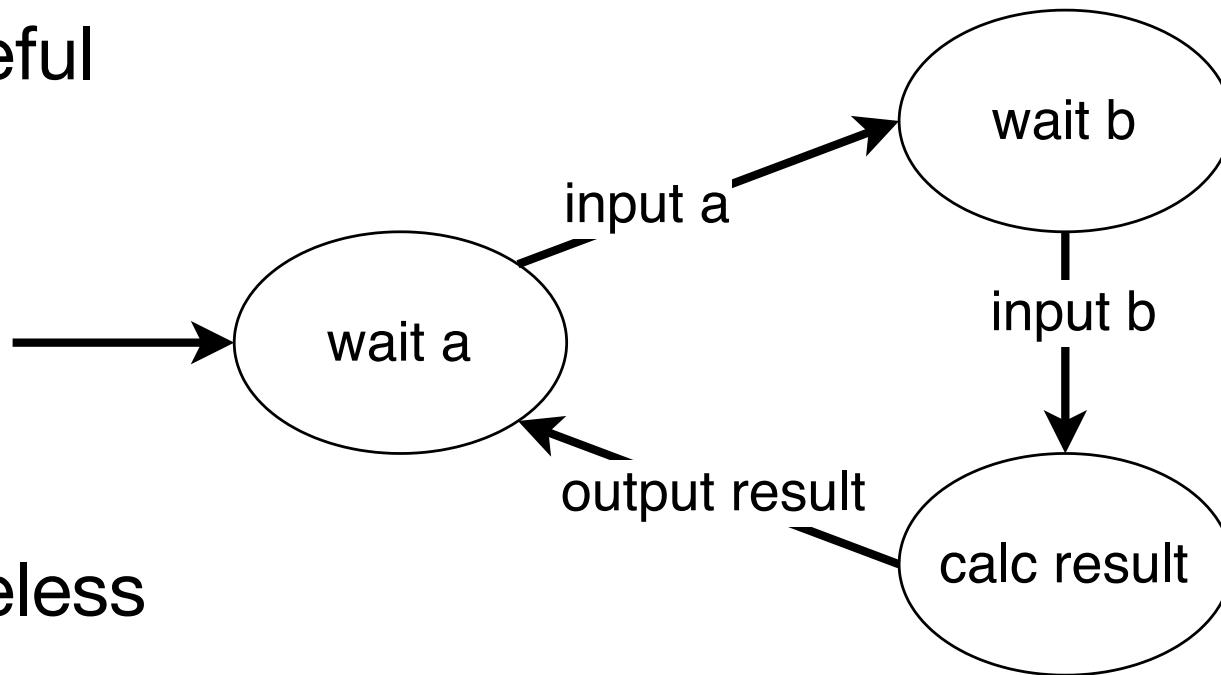
- これでアクセス可能
 - `http://<EC2 インスタンスのパブリック IP アドレス>/`
- Apache 関連のコマンド
 - 起動
 - `$ sudo service httpd start`
 - 停止
 - `$ sudo service httpd stop`
 - 再起動
 - `$ sudo service httpd restart`
 - 自動起動有効化
 - `$ chkconfig httpd on`
 - 自動起動無効化
 - `$ chkconfig httpd off`
 - サービス一覧
 - `$ chkconfig --list`

EC2 インスタンス再起動時に
自動で Apache 再起動

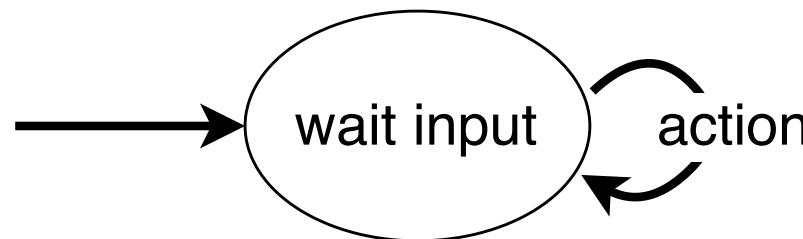


補足: stateful / stateless

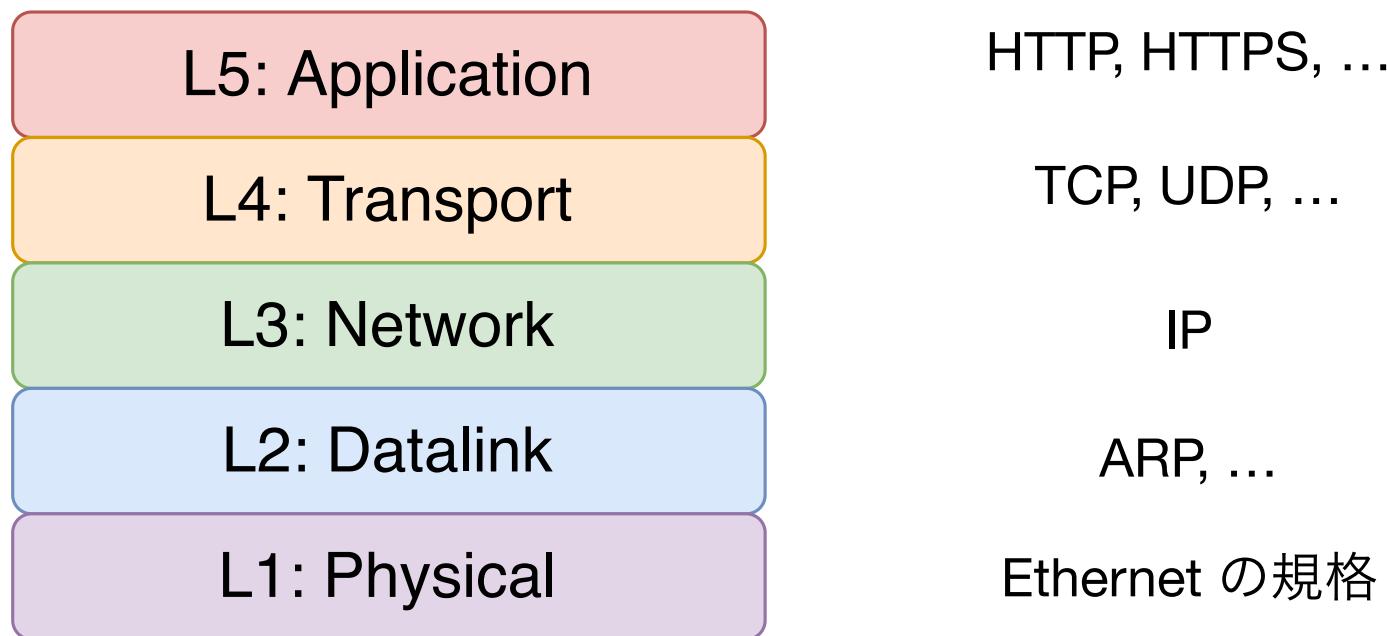
- stateful



- stateless



補足: ネットワーク 5 階層モデル



Protocol (?)

HTTP, HTTPS, ...

TCP, UDP, ...

IP

ARP, ...

Ethernet の規格

補足: ポート

