基本設計書 試験システム

第1.0版

産業用データ連携基盤	ドキュメント名	基本設計書 試験システム	作成者		作成日	2023/11/14
	章番号、章タイトル	変更履歴	更新者		更新日	2023/12/28
	サービスコンポーネント名					

変更履歴

#	版	日付	シート名	修正内容
1	0.9	2023年11月14日		新規作成
2	1.0	2023年12月28日	2.基本設計(インフラ)	「2-1.AWS全体構成図」NLBへのセキュリティグループの追加と、それに伴うEC2側セキュリティグループの修正
3			4.基本設計(VPC)	「4-3.接続制限」NLBへのセキュリティグループ追加に伴う文言の修正
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				
33				
34				
35				
36				
37				
38				
39				
40				
41				
42				
43				

産業用データ連携基盤	ドキュメント名	基本設計書 試験システム	作成者		作成日	2023/11/14
	章番号、章タイトル	目次	更新者		更新日	
	サービスコンポーネント名					

1. はじめに

1-1. 本書の目的

本書は、産業領域におけるデータ連携基盤等の構築事業において、2機関以上の参加者がデータの発見、授受を適切に行えるシステムとして構築する試験システムの環境部分について記載する。
※ 本書では、試験システム全体の内、日立担当分の領域について記載する。

1-2. 提供する機能

本システムで提供する機能及び構築する環境区分について以下に記載する。

サービス機能	機能	環境区分	備考
分野間データ連携サービスの提供機能	参加機関管理機能	支援サービス環境	認証サーバとして構築
	コネクタ管理機能	支援サービス環境	コネクタ識別子（コネクタ ID）の付与機能は認証サーバとして構築 コネクタ重複検出機能は認証サーバとして構築 コネクタロケーション管理機能はロケーションサーバとして構築
トラストサービス基盤の提供機能	参加者識別子（User ID）の発行管理機	支援サービス環境	認証サーバとして構築
コネクタ提供機能	認証機能 認可機能 データ授受機能 データ来歴登録機能	コネクタ環境	分野Ａ,分野Ｂ,分野Ｃの3環境を構築
支援サービス機能	カタログ作成ツールの提供	支援サービス環境	カタログ作成ツールサーバとして構築

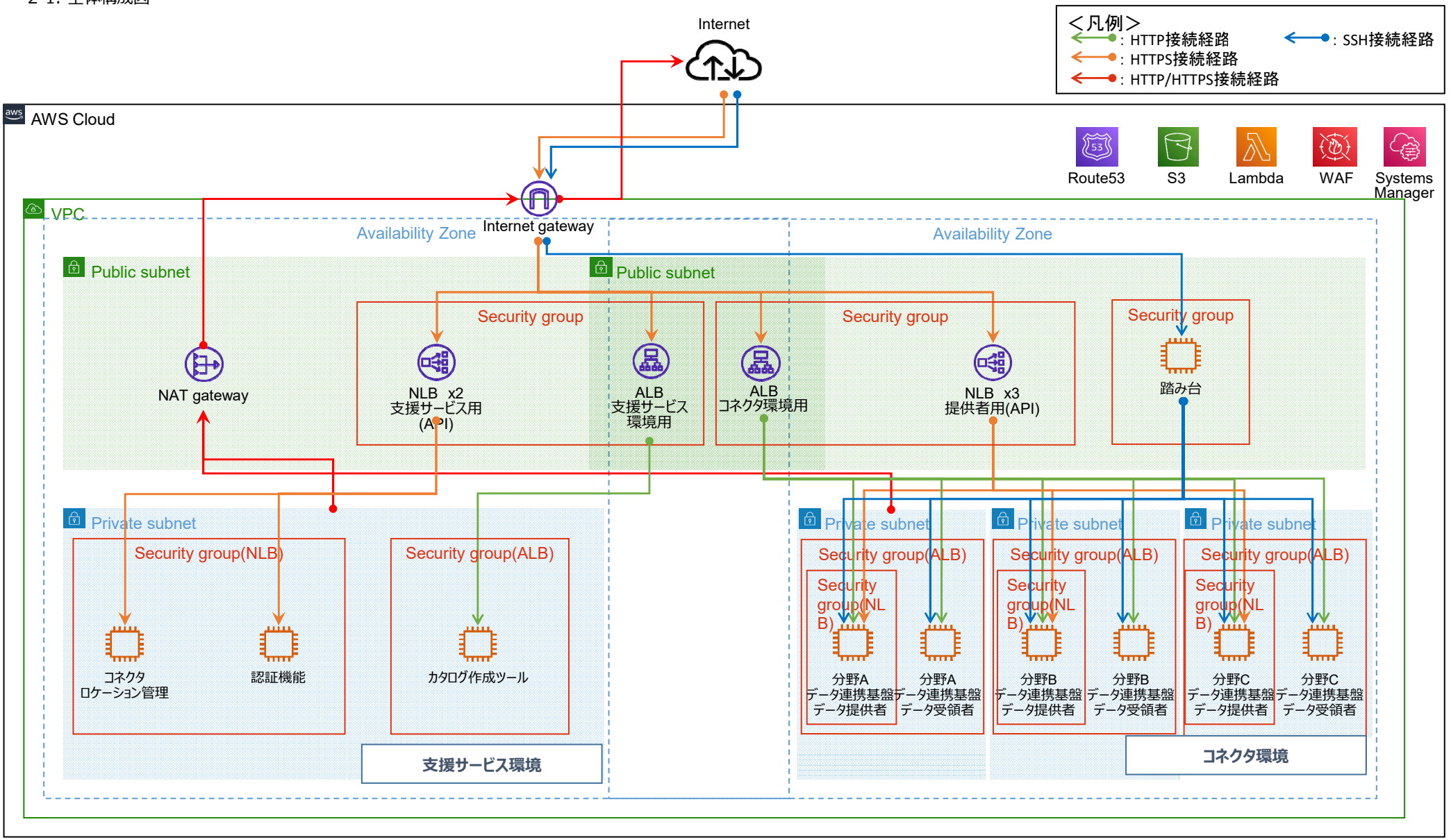
1-3. AWS主要利用サービス一覧

本システムで利用する主なAWSサービスの一覧を以下に記載する。

区分	サービス名	機能概要	当システムでの利用内容
ネットワーク	Route 53	DNS機能の提供	ユーザが接続する際に指定するURLの取得・管理を行う
	VPC	仮想ネットワーク環境の構築	仮想ネットワーク環境を構築する
	ELB	通信データの振り分け機能を提供	各機能を提供するサーバ(EC2)へ接続する際の振り分けを実施
コンピューティング	EC2	仮想サーバの提供	各機能を提供するサーバを構築する
	Lambda	プログラムコードの実行	サーバ起動・停止をコード化
ストレージ	EBS	ブロックストレージの利用	各サーバのストレージ環境(Disk)を提供
	S3	オブジェクトストレージ環境の提供	各種ログの保管領域、構築時のテンポラリ領域として利用
アプリケーション統合	SNS	サービス・ユーザ間の通信	運用監視における有事発生時にメッセージ通知(メール)機能を利用
	EventBridge	AWSと外部サービスのイベント共有	サーバ自動起動・停止スケジュールを登録
セキュリティ	IAM	サービス・リソースへのアクセスを制御	各種サービス・リソースのアクセスを制御
	GuardDuty	脅威の検出	脅威検出と継続的な監視を実施
	Certificate Manager	SSL/TLS証明書の管理	ELBで使用するTLS証明書(サーバ証明書)の管理
	Shield	DDoS攻撃からの保護	DDoS攻撃からの保護
	WAF	Webアプリケーションの保護	OWASPに記載されている一般的な脅威から保護する
運用・管理	Management Console	AWS環境の運用管理	AWS環境へのログイン、操作を実施
	Systems Manager	AWS環境の運用管理	EC2へのログイン機能を提供

2.　基本設計(インフラ)

2-1. 全体構成図



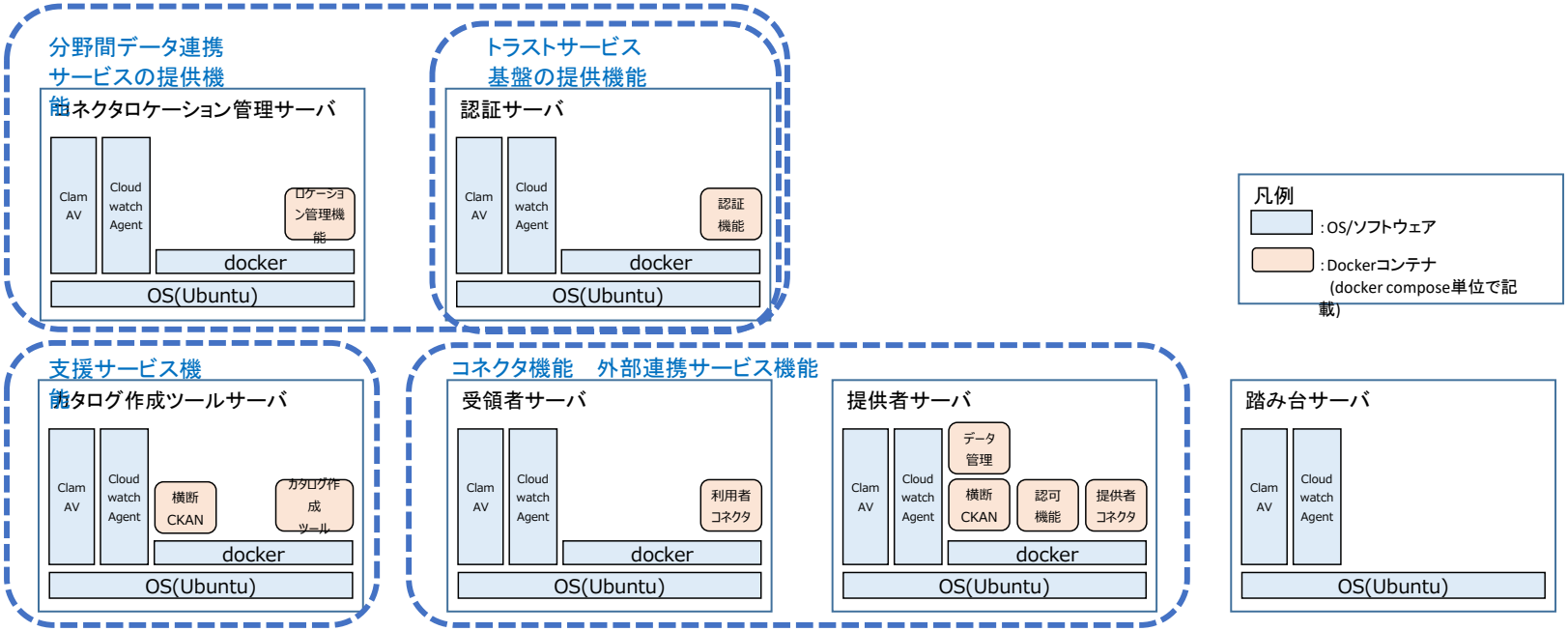
2-2. サーバ一覧

コネクタ環境には、コネクタが実装された受領者/提供者サーバを配置する。
支援サービス環境は、コネクタを利用するにあたり必要となる認証、コネクタロケーション管理、データカタログ登録を行う環境を配置する。
本システムで稼働するサーバの一覧を以下に記載する。

環境区分	サーバ名	提供する機能	OS	インスタンスタイプ	CPU	メモリ	Disk
コネクタ環境	受領者サーバ ※3環境	下記機能を有する受領者コネクタを実装 ・認証機能 ・データ授受機能 ・データ来歴登録機能	Ubuntu 22.04LTS	m5a.large	2.5 GHz x 2	8	30
	提供者サーバ ※3環境	下記機能を有する提供者コネクタを実装 ・認証機能 ・認可機能 ・データ授受機能 ・データ来歴登録機能 DDPを格納するためのデータ管理機能を実装 ・データ管理機能	Ubuntu 22.04LTS	m5a.large	2.5 GHz x 2	8	30
	踏み台サーバ	コネクタ環境へのSSH接続用	Ubuntu 22.04LTS	t3.medium	2.5 GHz x 2	4	30
支援サービス環境	認証サーバ	下記機能を有する認証機能を実装 ・参加機関管理機能 ・コネクタ管理機能(コネクタ識別子（コネクタ ID）の付与機能) ・コネクタ管理機能(コネクタ重複検出機能) ・参加者識別子（User ID）の発行管理機能	Ubuntu 22.04LTS	m5a.large	2.5 GHz x 2	8	30
	コネクタロケーション管理サーバ	下記機能を有するコネクタロケーション管理機能を実装 ・コネクタ管理機能(コネクタロケーション管理機能)	Ubuntu 22.04LTS	m5a.large	2.5 GHz x 2	8	30
	カタログ作成ツールサーバ	下記機能を有するカタログ作成ツール機能を実装 ・カタログ作成ツールの提供	Ubuntu 22.04LTS	m5a.large	2.5 GHz x 2	8	30

2-3. ソフトウェア構成

各サーバに導入するソフトウェア及びDockerコンテナについて以下に記載する。



2-4. OS設計

本システムで稼働するサーバのOSは、ubuntuを採用する。

以下設定項目を各環境共通で設定する。

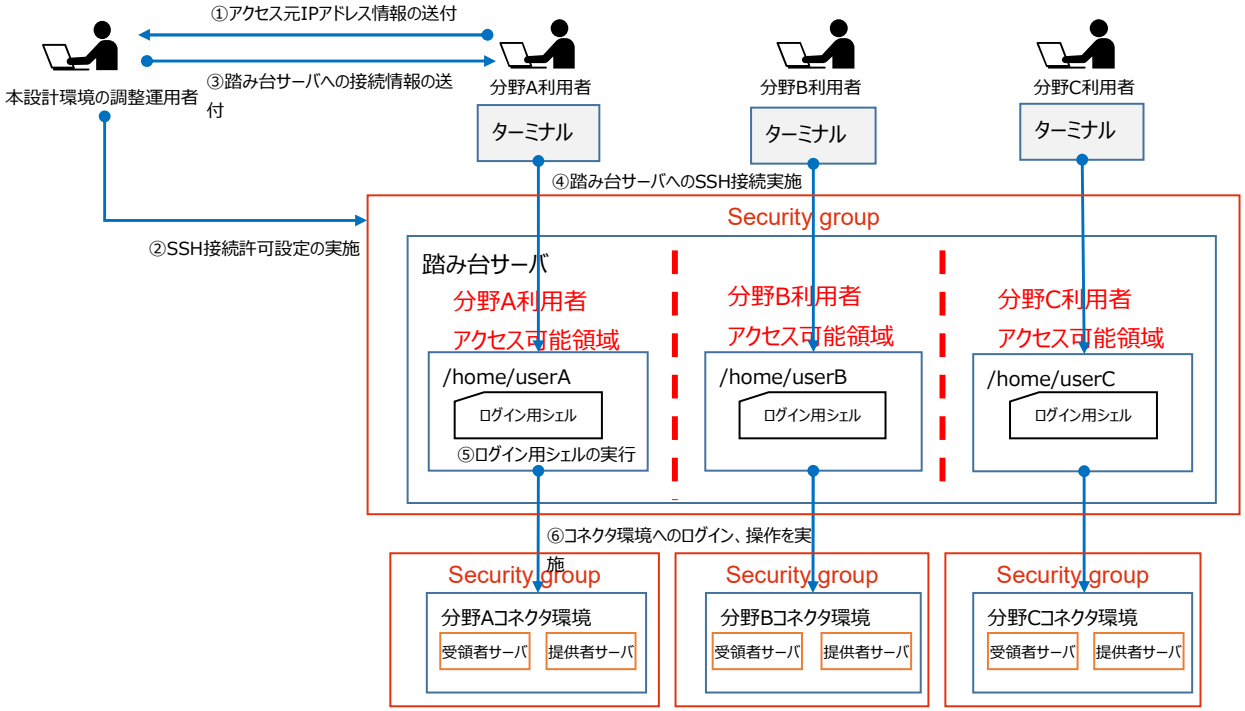
区分	設定項目	設定値	備考
OS基本情報・設定	カーネルバージョン	22.04	
	ディストリビューションバージョン	Ubuntu 22.04.1 LTS	
	タイムゾーン	UTC	
	言語	LANG=C.UTF-8	
時刻同期設定	時刻同期先	169.254.169.123	Amazon Time Sync Service(169.254.169.123)と同期
セキュリティ設定	ファイアウォール	inactive	セキュリティGrにて制御を行うため無効
	SE Linux	Disabled	
	ウィルス対策ソフト	ClamAV	
ログ設定	標準ログ	weekly / 4 / 圧縮する ※	/var/log/syslog
	ログイン履歴ログ	weekly / 4 / 圧縮する ※	/var/log/auth.log
	不正ログインログ	monthly / 1 / 圧縮しない ※	/var/log/btmp
	カーネルログ	weekly / 4 / 圧縮する ※	/var/log/kern.log
	起動時ログ	daily / 7 / 圧縮しない ※	/var/log/boot.log

	起動時カーネルログ	weekly　/ 4 / 圧縮する　※	/var/log/dmesg

※ローテーション間隔 / 世代数 / 圧縮

2-5. 踏み台サーバ利用方式

コネクタ環境の利用には踏み台サーバを経由してSSHにて接続可能な機能を提供する。
踏み台サーバからコネクタ環境へ接続するための利用方式について以下に記載する。



踏み台サーバを経由したコネクタ環境へのSSH接続に伴う実施内容は以下の通り

項番	実施者	実施内容	備考
①	分野X利用者	踏み台サーバにアクセスする端末のIPアドレスを本設計環境の調整運用者に申告する	
②	本設計環境の調整運用者	踏み台サーバへのSSH接続許可設定を実施する	
③	本設計環境の調整運用者	接続情報を分野X利用者に送付する	
④	分野X利用者	接続情報を基に踏み台サーバへSSH接続する	踏み台サーバのログインユーザは論理的に区分けし、他ユーザ領域へのアクセスは許可しない
⑤	分野X利用者	踏み台サーバへログイン後、ホームディレクトリに配置されているログイン用シェルを実行	シェルにて操作対象のサーバ(受領者サーバまたは提供者サーバ)を選択して接続する
⑥	分野X利用者	受領者サーバまたは提供者サーバへSSH接続して操作を開始する	各環境は論理的に区分けし、VPC内のローカル通信は許可しない(インターネットを経由したコネクタ間通信は可

3. 基本設計(セグメント)

3-1. 概要

本システムでは、以下のネットワーク環境(セグメント)を使用する。

環境区分	概要
コネクタ環境	コネクタ提供機能を有する受領者サーバ及び提供者サーバが稼働する環境 分野A、分野B、分野Cはそれぞれセグメントを分割する
支援サービス環境	認証、コネクタロケーション管理、カタログ作成ツールを提供する環境

要件により更に分割する必要がある場合は、セグメント構成を都度検討する。

3-2. 接続方式

本システムへ接続する事が想定されるユーザ及びその接続方式について以下に記載する。

環境区分	アクセス先	機能	アクセス元	接続方式	プロトコル	クライアント認証
コネクタ環境	受領者サーバ	受領者コネクタ	分野X利用者	API	HTTP/HTTPS	無
			国際連携機能	API	HTTP/HTTPS	無
		OSログイン	踏み台サーバ	SSH(鍵認証)	SSH	無
	提供者サーバ	提供者コネクタ	受領者コネクタ	API	HTTP/HTTPS	有
			国際連携機能	API	HTTP/HTTPS	有
		認可機能	提供者コネクタ	API	HTTP/HTTPS	有
			分野X利用者	GUI	HTTP/HTTPS	無
		カタログサイト	提供者コネクタ	API	HTTP/HTTPS	無
			カタログ作成ツール	API	HTTP/HTTPS	無
			分野X利用者	GUI	HTTP/HTTPS	無
		OSログイン	踏み台サーバ	SSH(鍵認証)	SSH	無
	踏み台サーバ	コネクタ環境へのSSH接続	分野X利用者	SSH(鍵認証)	SSH	無
支援サービス環境	認証サーバ	認証機能	受領者コネクタ	API	HTTP/HTTPS	有
			提供者コネクタ	API	HTTP/HTTPS	有
			カタログ作成ツール	API	HTTP/HTTPS	無
			来歴管理	API	HTTP/HTTPS	有
			電子証明書管理	API	HTTP/HTTPS	有
			電子署名管理	API	HTTP/HTTPS	有
			本設計環境の調整運用者	GUI	HTTP/HTTPS	無
	コネクタロケーション管理サーバ	コネクタロケーション管理機能	受領者コネクタ	API	HTTP/HTTPS	有
			提供者コネクタ	API	HTTP/HTTPS	有
	カタログ作成ツールサーバ	カタログ作成ツール	分野X利用者	GUI	HTTP/HTTPS	無

4. 基本設計(VPC)

4-1. VPC

本システムでは、AWS上に以下のネットワーク環境(VPC)を構築する。

区分	概要	備考
試験システム(日立環境分)	試験システム用VPCを一つ構築する	リージョンはap-northeast-1(アジアパシフィック (東京))とする

上記ネットワーク環境内に、パブリックサブネットおよびプライベートサブネットを複数のアベイラビリティゾーンに分けて配置する。
各機能を提供するサーバはプライベートサブネットに配置する。

要件により更に分割する必要がある場合は、VPC、サブネットの構成を都度検討する。

4-2. サブネット

VPC内に配置するサブネットについて以下に記載する。
全てのサーバをプライベートサブネットに配置することで、パブリックサブネットへの不正アクセスや攻撃があった場合でも影響範囲を限定し、情報漏洩のリスクを低減する。

サブネット	用途	アベイラビリティゾーン	備考
パブリックサブネット1	NATゲートウェイ、支援サービス用NLB、ALBの配置	ap-northeast-1a	ALBは両パブリックサブネットに跨るように配置する
パブリックサブネット2	踏み台サーバ、コネクタ(提供者)用NLB、ALBの配置	ap-northeast-1c	ALBは両パブリックサブネットに跨るように配置する
プライベートサブネット1	支援サービス用EC2インスタンス配置	ap-northeast-1a	
プライベートサブネット2	分野A向けコネクタ用EC2インスタンスの配置	ap-northeast-1c	
プライベートサブネット3	分野B向けコネクタ用EC2インスタンスの配置	ap-northeast-1c	
プライベートサブネット4	分野C向けコネクタ用EC2インスタンスの配置	ap-northeast-1c	

4-3. 接続制限

試験システムへの接続については各リソースに紐づけられたセキュリティグループにてIPアドレスによる接続制限を行う。
アクセス種別ごとの接続制限については以下に記載する。

アクセス種別	制限内容	備考
インターネットからのアクセス(HTTPS)	ロードバランサ(ALB、NLB)を経由したHTTP/HTTPSアクセスに限定 ALBへのアクセスはALBに設定されたセキュリティグループにて制御 NLBへのアクセスはNLBに設定されたセキュリティグループにて制御	クライアント証明書を必要としない通信についてはALBを経由での通信となる。 クライアント証明書を必要とする通信はNLB経由での通信となる。
インターネットからのアクセス(踏み台サーバ)	踏み台サーバに対しての接続はSSH鍵認証によるアクセスに限定 踏み台サーバに対して設定されたセキュリティグループにて制御	
ALB-EC2インスタンス間	EC2が利用する必要最低限のポートへのアクセスを許可	
NLB-EC2インスタンス間	EC2が利用する必要最低限のポートへのアクセスを許可	
EC2インスタンスへのログイン(コネクタ環境)	踏み台サーバからのSSH接続のみ許可	構築及び調整運用時においてはAWSサービスであるSession Managerを利用する。
EC2インスタンスへのログイン(支援サービス環境)	外部からのSSH接続は許可しない	サーバへのログインにはAWSサービスであるSession Managerを利用する。

5. 非機能要件設計

5-1. セキュリティ

本システムは、内閣官房内閣サイバーセキュリティセンターの「政府機関等の情報セキュリティ対策のための統一基準群（令和5年度版）」（以下、「統一基準群」という。）に基づき、
クラウドサービス利用における適切なセキュリティ対策を実施する。

情報システムのセキュリティ機能一覧について、以下に記載する。

対策項目	想定される脅威・リスク	概要
主体認証機能	不正アクセス なりすまし 情報漏洩	AWS及びサーバ向けのアクセスについては、MFA認証による多要素認証を行う。 コネクタ間、認証機能、コネクタロケーション管理機能との接続はクライアント証明書を設定し、クライアント認証を行う。
アクセス制御機能	不正アクセス 情報漏洩	AWSサービスのVPC、Subnet、Network ACL、SG（Security Group）を使用して、アクセス制御を実施する。
権限の管理	情報漏洩 なりすまし	AWS IAM（ロール）を使用して、ユーザID、グループ、ロールを認証する。
ログの取得・管理	不正アクセス 不正行為の検知困難 不正行為の被害拡大	Amazon CloudWatch Logs、AWS Cloud Trailを使用して、監査ログ取得を実施する。 GuardDutyを使用して、不正行為の検知を行う
暗号・電子署名	情報漏洩 盗聴	通信経路上の盗聴防止、保存情報の機密性確保のため、通信プロトコルの暗号化、保存データの暗号化、ネットワークの暗号化を行う。
監視機能	不正アクセス 不正行為の検知	Amazon CloudWatch Logs、AWS Cloud Trailを使用して、ログの監視を行う

情報セキュリティの脅威への対策一覧について、以下に記載する。

対策項目	想定される脅威・リスク	概要
ソフトウェアに関する脆弱性対策	脆弱性起因によるサイバー攻撃	Nessusを使用し、EC2インスタンスに脆弱性がないか定期的に確認する。
不正プログラム対策	マルウェア感染 情報漏洩 改ざん	EC2インスタンスにClamAVを導入し、不正プログラム対策を行う。 Amazon GuardDutyにて、EC2インスタンスへのマルウェア感染を検知する。
サービス不能攻撃	サービス不能攻撃	AWS ShieldによりDDoS攻撃を防止する。 AWS WAFにより、OWASPやCVEに記載されている一般的な脅威から保護する
標的型攻撃対策	不正アクセス 不正行為の検知困難 標的型攻撃	Amazon GuardDutyにて、AWSリソースへの既知・未知の脅威・異常検知する。

5-2. 可用性

本システムにおいて可用性は考慮しないものとする。

5-3. バックアップ設定

本システムにおけるバックアップ方針についてはDSAの方針に従うものとするが、特に指定がない場合、以下の方針でシステムバックアップを実施する。

バックアップ対象	取得方法	取得タイミング	システム停止の可否	バックアップ保持世代	備考
サーバデータ	フルバックアップ	システム構成変更時	○	3世代	システム構成変更時にAMIを手動で取得する。
	差分バックアップ	日次	○	7世代	EBSスナップショットを日次で取得するようにAWSライフサイクルマネージャに登録する

5-4. 監視設定

本システムにおける監視についてはDSAの方針に従うものとするが、特に指定がない場合、以下の方針で監視を行う。

種別	監視項目	監視方法	備考
死活	サーバの死活状態	EC2のステータスチェック機能により検知	
リソース	CPU使用率 メモリ使用率 Disk使用率	各リソースごと閾値を超えたら検知	メモリ、Disk使用率は、カスタムメトリクスを使用して監視
プロセス	Dockerコンテナの起動状態	各種コンテナのダウンを検知	コネクタ：スクリプトによる監視 コネクタ以外：ALBヘルスチェックによる監視
ログ	管理者アカウントでのログイン失敗 S3バケットの設定変更 ネットワークコンポーネントの設定変更	Cloud TrailによるAWS操作ログの監視を実施	
ジョブ	サーバ自動起動 サーバ自動停止	ジョブ実行エラーで検知	
セキュリティ	EC2のマルウェア感染 AWSアカウントやAWS環境に対する脅威	GuardDutyにより検知	検知後、EBSスナップショットに対してスキャンを実施 CloudTrailイベントログ・VPCFlowLogs・各種リソースからのDNSログなどをもとに

5-5. ログ収集、保管設定

本システムにおけるログ収集、保管についてはDSAの方針に従うものとするが、特に指定がない場合、以下の方針でログ収集、保管を行う。

収集対象サービス	ログ取得対象	ログ保管先	保管期限	備考
EC2(OSログ)	cron実行結果	Cloudwatch	1年(※)	(※)各種ログの保管期間は最低1年とする。
	SSH、sudo履歴			
	システムメッセージ			
	ログイン履歴			
VPC	アクセスログ	S3		
System Manager	コマンド実行履歴			
WAF	アクセスログ			
ALB	アクセスログ			
AWS Lambda	ジョブ実行ログ			
CloudTrail	AWS操作ログ			

5-6. 構成管理

本システムにおける構成管理についてはDSAの方針に従うものとするが、特に指定がない場合、以下の方針で構成管理を行う。

種別	管理項目	管理方法	備考
OS	OS名 バージョン パッチレベル	設計書による管理	
ソフトウェア	ソフトウェア名称 バージョン	設計書による管理	
クラウド環境サービス	AWS上の構成情報 全体構成図	設計書による管理	

5-7. 性能要件

本システムにおける性能については要件が定められていないため、対象外とする。
総合テスト及び、試験運用においてハードウェア起因のボトルネックが発生した場合は、スケールアップ、スケールアウトを実施することで対応することとする。

産業用データ連携基盤	ドキュメント名	基本設計書 試験システム	作成者		作成日	2023/11/14
	章番号、章タイトル	5.非機能要件設計	更新者		更新日	
	サービスコンポーネント名					
