版数： Version 1.0
発行日： 2018/12/20
国立研究開発法人産業技術総合研究所
情報・人間工学領域

# ABCI のセキュリティ ホワイトペーパー

Version 1.0

2018 年 12 月

国立研究開発法人　産業技術総合研究所
情報・人間工学領域

# 目次

# 1　本書の目的

本書は、ABCI の利用者が要求するセキュリティ要件を ABCI システムが満たしていることを確認するための参考資料として作成しました。

本書は以下の事項について解説しています。

・ABCI のセキュリティ管理体制
・ABCI のセキュリティ実装
・ABCI 利用者が活用できるセキュリティ機能
・ABCI 利用者と産業技術総合研究所のセキュリティ上の役割・責任の分担

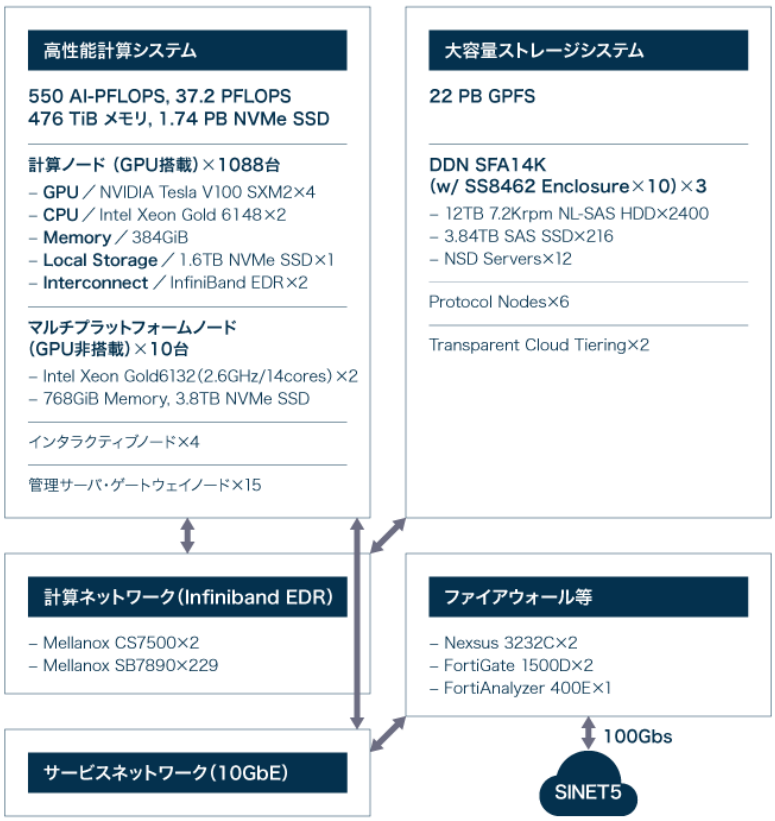
# 2　本書の想定読者

本書は、ABCI の利用を検討中の方、ABCI を利用中の方を読者として想定しています。

# 3　ABCI の概要

AI 橋渡しクラウド(AI Bridging Cloud Infrastructure, ABCI)は、国立研究開発法人産業技術総合研究所（産総研）が構築・運用する、世界最大規模の人工知能処理向け計算インフラストラクチャです。ABCI を産総研の役職員だけでなく、広く外部に利用を解放することにより、人工知能技術の社会実装を強力に支援することを目指しています。

ABCI は 1088 台の計算ノード、10 台のマルチプラットフォームノード、22PB の大容量ストレージシステム、ノード間およびストレージシステムを接続する高速な InfiniBand ネットワーク、それらを管理するサーバ群とネットワーク機器で構成されます。



ABCI では、ユーザのリソース要求に応じて以下の 5 つの資源タイプからマッチするものを選択できます。

| タイプ名 | CPU コア数 CPU コア数<br>割当量／総量 | CPU 数<br>割当量／総量 | メモリ (GB)<br>割当量／総量 | ローカルストレージ (TB)<br>割当量／総量 |
|---|---|---|---|---|
| F(ノード占有) | 40 / 40 | 4 / 4 | 360 / 384 | 1.4 / 1.6 |
| G.large | 20 / 40 | 4 / 4 | 240 / 384 | 0.7 / 1.6 |
| G.small | 5 / 40 | 1 / 4 | 60 / 384 | 0.175 / 1.6 |
| C.large | 20 / 40 | 0 / 4 | 120 / 384 | 0.7 / 1.6 |
| C.small | 5 / 40 | 0 / 4 | 30 / 384 | 0.175 / 1.6 |

ABCI では、処理スループットの最大化を可能とするバッチ型・対話型の実行サービスに加え、自由度の高い予約サービス、IDE、各種ストレージサービスを提供します。

| サービス名 | 説明 | 割当ノード数<br>(最小／最大) |
|---|---|---|
| Spot | バッチ実行型ジョブサービス | 1 / 512 |
| On-demand | インタラクティブ実行型ジョブサービス | 1 / 32 |
| Reserved | 日単位での資源予約サービス | 1 / 32 |
| Group Storage | グループ内で共有できるストレージサービス | N / A |

本書における用語を説明します。

| | |
|---|---|
| 利用法人 | 産総研との間で ABCI 利用サービスの利用契約を締結した主体である法人等 |
| 利用責任者 | 利用法人に所属する者の中から選任された ABCI 利用サービスの利用における責任者 |
| 利用管理者 | 利用責任者の下で利用者を管理するために置かれる者 |
| 利用者 | 利用責任者から指定された者のうち、産総研からアカウントを与えられて ABCI 利用サービスを利用する者 |
| 利用者等 | 利用法人、利用責任者、利用管理者および利用者を総称したもの |
| ABCI 運用者 | ABCI の運用に従事する担当者 |
| 利用グループ | 特定の研究のために ABCI 利用サービスを利用する利用責任者、利用管理者および利用者からなる利用者等の集合体 |
| 利用者等のデータ等 | 利用者等が ABCI を利用する際に ABCI の記憶装置に保存したプログラム、計算・学習に必要なデータおよび計算・学習結果 |

## 4 ABCI におけるセキュリティ方針

産総研は、所有する情報を適切に管理し、その安全性・信頼性を担保することが、社会に対する責務であることを自覚し、内閣が策定した「政府機関の情報セキュリティ対策のための統一規範」および「政府機関の情報セキュリティ対策のための統一基準」の内容を踏まえ、以下のとおり、総合的・体系的な情報セキュリティ対策に継続的に取り組むこととしています。

- 産総研の全役職員等は、取扱う情報を重要な資産と認識し、各々の自覚と責任の下に、情報セキュリティの確保に努める。
- 産総研は、情報セキュリティの確保のために必要な情報セキュリティ管理体制を確立する。
- 産総研は、改ざん、漏えい、破壊等の脅威から情報を保護するために、包括的な対策を実施する。
- 産総研は、情報セキュリティの水準の維持・向上のために、情報セキュリティ対策の遵守状況について、定期的に点検・評価・監査を実施する。
- 産総研は、全役職員等の情報セキュリティについての知識向上のために、情報セキュリティ対策についての教育・研修を定期的に実施する。

上記情報セキュリティ基本方針および国立研究開発法人産業技術総合研究所情報セキュリティ規程に従い、ABCI が提供するサービスのセキュリティを確保する方法や体制を確立しました。なお、ABCI のセキュリティ方針は本白書にて示されますが、ABCI の可用性、利用者等のデータ等のセキュリティおよびバックアップなど、国立研究開発法人産業技術総合研究所共用高性能計算機 ABCI 利用約款や国立研究開発法人産業技術総合研究所共用高性能計算機利用規約にて別途定められるものもあります。

# 5 想定されるリスク

## 5.1 保護すべき情報が漏洩するリスク

ABCI は主に以下に示す要因を想定して保護すべき情報が漏洩するリスクへの対策をとっています。

- 利用者・サービス間の情報隔離に失敗する
- 管理用ユーザインタフェースに不正にアクセスされ、使用、操作される
- データ転送途上における攻撃、データ漏洩（アップロード時、ダウンロード時、クラウド間転送時）
- 利用者別の情報削除、廃棄に失敗する

本リスクへの対策は、物理的セキュリティ、ネットワークセキュリティ、アクセス制限、モニタリング、技術的脆弱性管理等により行っています。

## 5.2 情報および処理が改竄されるリスク

ABCI は主に以下に示す要因を想定して情報および処理が改竄されるリスクへの対策をとっています。

- 利用者・サービス間の情報隔離に失敗する
- 管理用ユーザインタフェースに不正にアクセスされ、使用、操作される

本リスクへの対策は、物理的セキュリティ、ネットワークセキュリティ、アクセス制限、モニタリング、技術的脆弱性管理等により行っています。

## 5.3 サービス提供ができなくなるリスク

ABCI は主に以下に示す要因を想定してサービス提供ができなくなるリスクへの対策をとっています。

- 利用者・サービスの高集約、共有化により障害が派生、拡大する
- 物理／仮想環境の設計・設定・運用の不整合により機能不全となる
- ある利用者・サービスの停止、抑止に伴い、他利用者がサービスを利用できなくなる
- リソースの事前準備、動的割当が不足し、増大する利用者需要に対応できない
- クラウド内 DDoS/DoS 攻撃を受け、サービス不全となる

本リスクへの対策は、物理的セキュリティ、ネットワークセキュリティ、モニタリング、バックアップ、容量・パフォーマンス管理等により行うとともに、事業継続計画を準備し計画にしたがって実施することにより行っています。

## 5.4 クラウドサービス固有の情報セキュリティ管理策

JIS Q 27017:2016(ISO/IEC 27017:2015)「JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範」のクラウドサービスに固有の実施の手引に従い、以下の項目について対策を行っています。ただし、ABCI では仮想化セキュリティは採用していません。

- クラウドサービスの設計および実装に適用する、最低限の情報セキュリティ要求事項
- 許可された内部関係者からのリスク
- マルチテナンシおよびクラウドサービスカスタマの隔離（仮想化を含む）
- クラウドサービスプロバイダの担当職員による、クラウドサービスカスタマの資産へのアクセス
- アクセス制御手順（例えば、クラウドサービスへの管理上のアクセスのための強い認証）

- 変更管理におけるクラウドカスタマへの通知
- クラウドカスタマデータへのアクセスおよび保護
- クラウドカスタマのアカウントのライフサイクル管理
- 違反の通知、並びに調査およびフォレンジックを支援するための情報共有指針

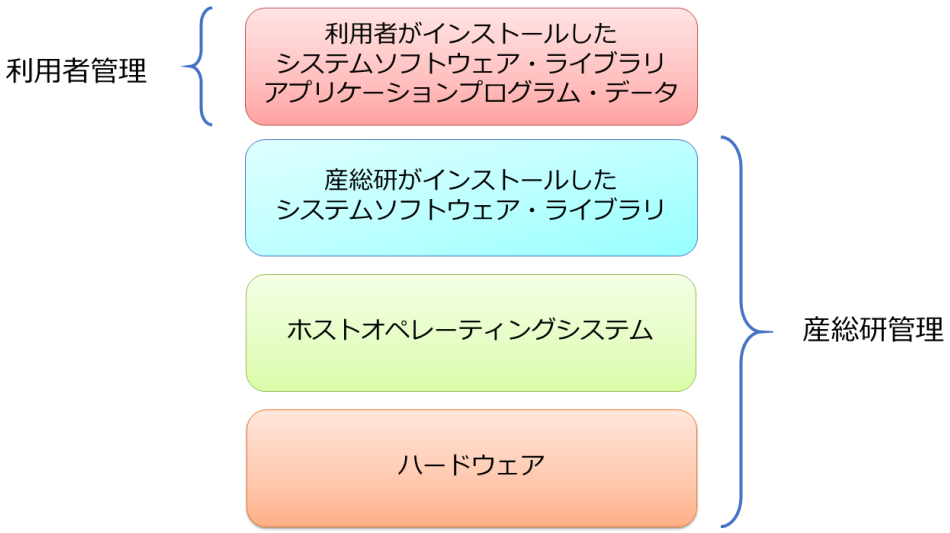
なお、ABCI はマルチテナントによるクラウドサービスを提供しているため、他の利用者の影響を受ける可能性があります。ABCI は適切に監視を行い、異常への対応を行う仕組みや体制を整えていますが、マルチテナントに起因するリスクを完全に回避することは困難です。利用者はこのことを理解した上で ABCI を適切に利用する必要があります。

### 5.5 ガバナンスとリスク管理

産総研情報セキュリティ規定に従った情報セキュリティ体制を整備し、ABCI に係る情報、情報システムおよび情報セキュリティの管理を行うとともに、管理状況を定期的に確認することによるリスク管理を進めます。定期的に自己監査を行うとともに、1 年に 1 度程度の外部監査を実施します。また、情報セキュリティインシデントへの対応手順を明確にし、情報セキュリティインシデント発生時の被害を最小限に食い止めます。ABCI 運用者に対して情報セキュリティに関する教育を定期的に行うことにより人的資源のセキュリティ向上につとめます。

## 6 責任分界点

ABCI の利用においては、利用者等と ABCI を運用する産総研の間で責任を分担してセキュリティ対策に取り組みます。ABCI ではホストオペレーティングシステム、もしくはホストオペレーティングシステムが提供する仮想化環境に、人工知能や高性能計算に利用されるシステムソフトウェアやライブラリがインストールされ、利用環境として利用者に提供されます。データを格納するストレージもあわせて提供されます。ABCI およびその付帯設備の物理セキュリティ、ホストオペレーティングシステム、利用環境に産総研がインストールしたシステムソフトウェアやライブラリのセキュリティについては産総研が責任を負います。利用者は提供される実行環境上に自身がインストール・利用するシステムソフトウェア、ライブラリ、アプリケーションプログラムやアプリケーションが扱うデータのセキュリティについて責任を負います。



# 7 情報セキュリティ体制

産総研情報セキュリティ規程に従い、情報セキュリティに取り組む体制を以下の通り整えています。

- ABCI 情報セキュリティ責任者（産総研情報・人間工学領域長） は、ABCI に係る情報セキュリティ対策に関する業務を統括し、並びに ABCI に係る情報および情報システムの管理を監督します。
- ABCI 情報システムセキュリティ責任者は、ABCI 情報セキュリティ責任者に指名され、ABCI 情報システムのセキュリティに関する責任者として ABCI に対する情報セキュリティ対策を実施します。また、ABCI の管理状況を、産総研情報・人間工学領域が研究業務に供するために構成および管理する大規模研究業務ネットワークの１つであり、ABCI が接続されている Grid 実験線のネットワーク管理責任者（産総研情報・人間工学領域長）に定期的に報告します。
- Grid 実験線のネットワーク管理責任者は、Grid 実験線の情報セキュリティ対策に関する業務を統括します。また、Grid 実験線に接続されている ABCI を含むすべての機器の管理を監督します。さらに、Grid 実験線に接続されている全ての機器の管理状況を、産総研の情報セキュリティに関する業務を統括する統括情報セキュリティ責任者に定期的に報告します。
- 産総研において発生した情報セキュリティインシデントに対処するために設置された体制（以下「CSIRT」という。） は、国立研究開発法人産業技術総合研究所情報セキュリティ規程に規定する者のほか、CSIRT 責任者代理およびメンバーをもって組織されます。CSIRT 責任者代理およびメンバーは、情報セキュリティに関する専門的な知識または適性を有すると認められる職員等のうちから、CSIRT 責任者が指名します。CSIRT 責任者は、CSIRT 内の業務統括および外部との連携等を行います。
- CSIRT は、産総研における情報セキュリティ対策の推進に係る企画立案および総合調整を担うとともに、情報セキュリティインシデントに対処するため、情報セキュリティの確保、情報サービスの復旧その他の必要な措置を講じ、または指示するものとします。

# 8 ABCI のセキュリティ解説

## 8.1 物理的セキュリティ

### 8.1.1 セキュリティの目的

ABCI コンピューティング環境を形成する情報処理装置およびその上で処理される利用者環境、利用者等のデータ等を、物理的破壊、持ち去り、情報の窃取、改ざん、消去、覗き込み、盗聴等の物理的脅威および自然災害や電源障害等の環境的脅威から保護します。

### 8.1.2 実装と運用

- ABCI は、東京大学柏 II キャンパス内に建設された、専用の AI データセンター棟内に設置されています。
- AI データセンター棟の出入口および AI データセンター棟内のサーバ室出入口は、常時施錠します。また、AI データセンター棟の空調関係設備への出入口は必要時以外施錠します。サーバ室内のラック扉は常時施錠し、メンテナンス等の必要な場合にのみ開錠し作業を行います。
- AI データセンター棟および AI データセンター棟内サーバ室への入退棟や入退室に際しては、許可された者のみが所有する鍵カードにより解錠・施錠します。解錠・施錠は鍵カードの情報や日時とともに記録されます。
- 運用保守作業を行う執務室は常時施錠し、部外者が立ち入らないよう入退出管理を行います。ABCI 運用者の帰宅時には管理用端末をキャビネットに保管・施錠します。また、書類の不正帯出の禁止、ABCI への接続端末の制限、USB メモリ等記録媒体利用の原則禁止な

どのセキュリティ対策を行います。ABCI の起動や運用保守作業に USB メモリ等記憶媒体の使用が不可避となる場合は、台帳により利用状況を管理するとともに、持ち出し時には USB メモリを初期化します。

- 管理サーバ、ストレージ、およびネットワークスイッチは無停電電源装置による電源保護を行っています。計算ノードは電源保護を行っていません。
- 付帯設備の一部（室温やサーバの温度、漏水、一部停電による FCU 停止等）は常時監視しており、異常が検知されると担当者の携帯電話にメールで通知が入り、迅速な対応が可能な仕組み・体制を整えています。
- ABCI システムは、鉄骨造平屋建て、耐震構造を備えたデータセンターに設置され、サーバラック等装置は床コンクリートスラブに直接固定されています。またデータセンター内には火災センサと消火器が設置されています。

**■ 利用の手引き**

- 物理的セキュリティに関しては基本的に産総研に責任があります。
- 産総研は ABCI の見学ツアーの機会を設けていますが、利用者等による物理セキュリティの監査を目的とした見学の機会は提供していません。

## 8.2 ネットワークセキュリティ

### 8.2.1 セキュリティの目的

利用者等のデータ等は、データセンター内ネットワークやインターネットのように利用者等が直接管理できない伝送路で運ばれます。データセンター内設備から利用者内設備を結ぶネットワークの経路制御および盗聴、伝送遅延等への対応を行い、伝送路の信頼性と安全性を確保します。

### 8.2.2 実装と運用

- ABCI は、Grid 実験線に接続され、日本全国の大学、研究機関等の学術情報基盤として国立情報学研究所が構築、運用している情報通信ネットワークである SINET を通じてインターネットに接続されています。産総研は Grid 実験線のセキュリティに責任を負っています。
- 通信回線はファイアウォールによる防御を実施しています。ファイアウォールで不要な通信を遮断することで、外部からの攻撃や内部からの情報流出を防止します。また、インターネットからアクセスされる機器については、OS が持つファイアウォール機能も用いて不正通信を防御します。
- 外部からの侵入・攻撃への対策（防御、検知）として、改竄検知および不正アクセスに関するログの記録を行っています。侵入発覚後に改竄記録や不正アクセス記録を確認・解析することが可能です。
- 通信回線に対する盗聴行為や ABCI 利用者の不注意による情報漏洩を防ぐため、通信は暗号化します。ABCI との通信に利用する SSH と HTTPS については SSL/TLS1.2 以降による暗号化を行います。
- ネットワークを用途別にセグメント分割し、各セグメント間で不要な通信が行われないよう、通信経路を分離しています。また、ファイアウォールについても、用途毎に仮想ドメインを構成し、通信経路の分離を実現しています。通信経路は分離されているため、他の仮想ドメインのトラフィックの受信や傍受は不可能です。

**■ 利用の手引き**

- ABCI の利用に際しては、利用者側（クライアント）のネットワーク環境のセキュリティを確認し、SSH や HTTPS など暗号化された通信を利用してください。
- 許可のないポートスキャンは産総研の情報セキュリティ基本方針に違反します。利用者が利用者の環境に対してポートスキャンやその他ネットワーク負荷をかける操作を行う場合は事前に ABCI 運用担当に連絡し、許可を得てください。
- 産総研のネットワークやインターネット網、それらに接続されたサーバ設備等に不正にアクセスする行為など、ネットワークセキュリティに影響を与える行為を行ってはなりません。

## 8.3 アクセス制限

### 8.3.1 セキュリティの目的

ABCI サービスへのアクセス制御および ABCI サービス上の利用者環境、利用者データへの未許可アクセスおよび誤用、悪用から保護するための、本人認証をベースにしたアクセス制御を行います。

### 8.3.2 実装と運用

#### 8.3.2.1 利用者のアクセス管理

- 利用者の登録および登録削除： 利用者の登録は、利用責任者または利用管理者からの申請により、利用資格の審査を実施した上で行います。また、利用者の登録削除は、利用責任者または利用管理者からの申請に基づき、当該利用者アカウントを無効とすることにより実施します。
- 一意アカウントの徹底： 利用者、ABCI 運用者とも、一人に対し一意アカウントを割り当てます。また、アカウント名は他の利用者が容易に推測できないものをシステムが割り当てます。
- ABCI は定められたパスワードポリシーに従い、安易なパスワードや辞書に載った単純なパスワードを設定不能としています。
-

**■ 利用の手引き**

- ABCI 利用ポータルは、インターネットからアクセス可能です。ABCI 利用ポータルへのアクセス時は、2 段階の認証によりアクセス制御を行います。
- ABCI を利用するには、ファイアウォール内の機器へのアクセスが必要です。当該機器へのアクセスには、2 段階の SSH 接続を必要とします。SSH 認証は公開鍵認証に限定しています。
- 利用者は ABCI 利用ポータル上でパスワードを設定・変更することができます。ABCI 利用ポータルへの初回アクセスやパスワード再発行時には、ABCI 利用者の依頼に基づき、アカウント管理担当者が仮パスワードを発行します。利用者は仮パスワードから本パスワードへの変更を実施しないと、ABCI を利用することができません。
- ABCI にアクセスするための SSH 認証に必要な公開鍵は、利用者が作成して ABCI 利用ポータル上で登録します。

#### 8.3.2.2 権限と特権アカウントの管理

- ABCI システム管理者権限等の特権は、役割に応じた最小限の権限の付与、最少人数への付与を原則に割り当てます。
- ABCI 運用者に割り当てられたアカウントと、付与された権限、接続先サーバを一元把握可能な権限マトリクスを作成し、権限を管理します。アカウント設定の変更を権限マトリクスに適宜反映させます。
- 定期的に ABCI 運用者への権限割当を見直して権限マトリクスを更新します。また、同時に権限マトリクスと実際のサーバ設定が一致していることを確認します。不要になった離職者アカウントや長期間利用実績のないアカウント、無許可のアカウントを無効にします。
- リモートアクセス時は sudo コマンドを唯一の利用手段に制限するなど、特権アカウントや root パスワード入力が必要な作業を極力減らします。
- 特権アカウントでの作業は作業を行った ABCI 運用者を特定できるようにします。特権アカウントでの作業の前後でのファイルやシステム設定の変更状況をログやシステム整合性監視ツールなどを活用して把握し、事前の作業届出と変更内容を照合することで作業内容の妥当性を確認します。
- 管理用端末の不正利用を防ぐため、管理用端末での ABCI 運用者の認証を徹底します。また、スクリーンロックやセッションロックアウトなどを実施して離席時に管理用端末が不正利用されることを防ぎます。

**■ 利用の手引き**

- 利用者等は特権を取得することはできません。

#### 8.3.2.3 利用者等によるデータアクセスおよび保護

- 利用グループのデータは、他の利用グループから論理的に分離し、アクセスできないようにしていますが、利用者がインストールしたプログラムや利用者のデータに対するアクセス制限は、利用者等が行う権限設定に依存します。
- ABCI 運用者は、次の場合を除き、利用者等のデータ等の閲覧、参照を行わず、第三者に開示しません。
  - ABCI 利用サービスの提供･維持のために第三者に業務委託を行う場合であって、かつ運用上必要な場合。ただし、産総研は、業務委託先の第三者に対し、産総研と同等レベルの利用者等のデータ等の取扱いを遵守させるものとします。
  - 裁判所または行政機関より法令、判決、決定または命令に基づき開示が要求され、これに応じて産総研および役職員等が、当該裁判所または行政機関に対し、利用者等のデータ等の内容の開示および提供を行う場合。なお、この場合、産総研および役職員等は、上記の開示の要求があった旨を利用法人に通知します。

**■ 利用の手引き**

- 利用者等のデータ等のセキュリティおよびバックアップは、利用者等の責任で実施する必要があります。(ABCI 利用約款第 19 条)
- 利用グループのデータは、他の利用グループからアクセスできないように初期設定されていますが、この設定は利用グループの利用者等が変更できるようになっています。利用グループのデータに対するアクセス制御の設定は利用者等の責任で実施してください。

## 8.4 モニタリング

### 8.4.1 セキュリティの目的

システム障害やセキュリティインシデントの検知、記録、原因究明のため、ならびに運用の正当性の裏付けとして各種ログを取得し、各種監視機能によりモニタリングを行います。

### 8.4.2 実装と運用

- ABCI 運用者が、システム障害、セキュリティインシデントの検知、原因究明に用いるため、各種サーバのログイン記録、ポータルへのアクセス記録、ファイアウォールの通信記録、各種サーバや計算ノードのシステムログ、ABCI 上で利用者等が行った操作のうち一部のログ、ABCI 運用者が行った操作ログを運用管理サーバに収集・蓄積しています。
- システムの正常運用を図るために、利用者等のファイル情報を収集・参照することがあります。ファイル情報とは、利用者等のデータ等を格納したファイルの情報（ファイルサイズ、作成日、更新日時等の情報）をいいます。ファイル情報にはシステム上の利用者およびグループの ID が含まれることがありますが、利用者等のデータ等は含まれません。
- プログラムの性能向上および利用状況の分析等、利用者等の利便性向上およびシステムの効率的な運用を目的として、利用者等の利用情報および性能情報を収集することがあります。利用情報とは、利用者等による ABCI の使い方に関する情報（使用資源種類および量、使用プログラムの種類等の情報）を、性能情報とは、プログラムの性能に関する情報（CPU、GPU、メモリー等の資源利用率）をいいます。利用情報と性能情報にはシステム上の利用者およびグループの ID が含まれることがありますが、利用者等のデータ等は含まれません。
- ログの蓄積期間は最低 1 年間としています。
- ログは、ABCI システムの性能管理の目的で取得するものですので、利用者等の個別要求に応じてログを開示することは原則致しません。
- 産総研は、技術開発促進および学術貢献を目的として、ファイル情報、利用情報、性能情報から利用者等が特定される情報を除外したデータおよびその統計データを公開することがあります（ABCI 利用約款第２８条３）。

**■ 利用の手引き**

- アプリケーションの実行ログは利用者がとる必要があります。OS に搭載されている機能を用いてログをとることができます。他の機能を利用したい場合は利用者が自ら用意してログを取得してください。
- アプリケーション実行に不具合等が生じ、システム障害が疑われる場合はアプリケーションの実行ログとともに ABCI 運用サポート（qa@abci.ai）に問い合わせてください。

## 8.5 バックアップ

### 8.5.1 セキュリティの目的

システム障害やインシデントによりクラウドサービスが利用できなくなる、あるいはデータが消失したといった状況が発生することを想定し、事業の継続および速やかな復旧のためのバックアップを実施します。

### 8.5.2 実装と運用

- ABCI 運用者が、システム障害時の復旧やサービス継続のために不可欠なデータのバックアップを定期的に実施します。
- バックアップデータからの情報漏洩を防ぐために、バックアップデータに対して本体データと同一強度以上のアクセス制限を実施します。
- バックアップは、ABCI システムの障害時等における復旧のために行うものですので、利用者の個別の要求に応じてバックアップデータを提供することは原則致しません。

**■ 利用の手引き**

- 利用者等のデータ等のバックアップは利用者等の責任で実施してください（ABCI 利用約款第 19 条）。
- 産総研は利用者等のデータ等のバックアップのための設備や機能は提供しませんので、利用者等が自ら用意する環境で行ってください。

## 8.6 技術的脆弱性管理

### 8.6.1 セキュリティの目的

システムには何らかの脆弱性が存在します。システムの脆弱性を放置しておくとマルウェアや攻撃者に利用され、設定の変更、情報の窃取、改ざん、削除、遠隔操作等の被害を受けます。脆弱性がリスクの顕在化の原因にならないようにするために適切に脆弱性管理を行います。

### 8.6.2 実装と運用

- 6 節「責任分界点」に示したとおり、ハードウェア、ホストオペレーティングシステム、産総研がインストールしたシステムソフトウェアおよびライブラリに関する脆弱性については産総研が責任を有します。
- ABCI 運用者は Common Vulnerabilities and Exposures（CVE®）、JPCERT コーディネーションセンター（JPCERT/CC）などから脆弱性情報を収集し、ABCI システムへの影響の有無を評価します。
- 収集した脆弱性については、脆弱性のレベルに応じてアップデートやパッチ適用の要否およびスケジュールを検討します。緊急性の高い脆弱性が発見された場合は、利用者に通知をした上でシステム停止を伴うアップデート、パッチ適用を実施することがあります。
- 一部のシステムに対してはウィルスチェックを実施しています。

**■ 利用の手引き**

- 利用者等がインストールしたプログラムの脆弱性管理は利用者等が責任をもって実施する必要があります。
- 利用者等による ABCI システムの脆弱性検査は許可しません。

## 8.7 容量・パフォーマンス管理

### 8.7.1 セキュリティの目的

クラウドサービスではシステムのリソース（処理能力、メモリ容量、ストレージ容量）やネットワーク帯域を、利用者の必要に応じて自由に増減できることが利点の一つになっています。

利用料金も考慮しながら可用性を維持するために、適時必要な容量やパフォーマンスを監視する必要があります。

### 8.7.2 実装と運用

- ABCI はマルチテナントによるクラウドサービスであるため、他の利用者の利用状況によりネットワーク帯域等の性能が影響を受ける可能性があります。
- 次の各号に該当する場合は、ABCI が利用者等に提供可能なシステムのリソースやネットワーク帯域の容量やパフォーマンスが低下する可能性があります。
  - 産総研の設備等の保守、工事、移設、障害等により ABCI を縮退運転する場合
  - 提供される電力や空調など付帯設備の能力に応じて ABCI を縮退運転する場合
  - 産総研による ABCI の利用を優先する場合
- 産総研は、ABCI 利用サービスの提供に支障が出ると判断した場合には、産総研所定の通信手段を用いて行う通信について、当該通信に割り当てる帯域を制御することがあります(ABCI 利用約款第 32 条)。

**■ 利用の手引き**

- 他の利用者の利用状況により利用環境の性能等に影響が出る可能性は高くありませんが、マルチテナントによるクラウドサービスとして提供される ABCI の特性を理解して利用する必要があります。

## 8.8 システム障害、インシデント対応

### 8.8.1 セキュリティの目的

クラウド設備、インターネット、利用者内システムが複合的に連携したクラウドコンピューティング環境では、システム障害やインシデントの原因の切り分けが難しく、また、責任分界や障害対応の役割が曖昧であると速やかな対応が取れません。障害の検知、原因究明、復旧のための関係者の協力体制、対応手順を整備します。

### 8.8.2 実装と運用

- ABCI 運用者は、情報セキュリティインシデントや重大なシステム障害の可能性を認知した場合には、直ちに ABCI 情報セキュリティ責任者に報告し、その指示に従わなければなりません。
- ABCI 運用者は、重大なシステム障害が確認できた場合はウェブ等で情報を周知するとともに、ABCI の保守を行うベンダ等と連携して復旧作業を進めます。復旧の目途などは適宜ウェブ等で情報を周知します。
- ABCI 情報セキュリティ責任者は、報告を受けた場合には、速やかに必要な指示を行うとともに、CSIRT その他関係者にその旨を報告します。また、必要に応じて利用者等に情報を通知します。
- ネットワーク管理責任者は、Grid 実験線上の情報セキュリティインシデントを認知した場合には、Grid 実験線に接続されている機器の管理者に適切な指示を行うとともに、CSIRT に報告します。
- CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行います。CSIRT が情報セキュリティインシデントを認知した場合には、当該事象について速やかに、経済産業省を通じて内閣官房

組織令（昭和 32 年政令第 219 号）第 1 条により内閣官房に置かれる内閣サイバーセキュリティセンターに連絡し、その指示に従うものとします。この場合において、認知した情報セキュリティインシデントがサイバー攻撃またはそのおそれのあるものであるときについては、その連絡方法は、別に定めるものとします。

- CSIRT は、定められた手順にしたがって原因解析、影響範囲の調査、復旧、再発防止策検討を主導して進めます。

**■ 利用の手引き**

- 利用者は情報セキュリティインシデントの可能性を認知した場合には、至急 ABCI のセキュリティに関するお問合せ窓口（abci-inquiry-ml@aist.go.jp）に報告してください。報告後は指示に従って対応してください。
- 情報セキュリティインシデントを報告した場合、関係する可能性のあるアカウントを無効にする（ログインできないようにする）ことがあります。
- 利用者はシステム障害の可能性を認知した場合には、ABCI 運用サポート窓口（qa@abci.ai）に報告してください。
- ABCI のセキュリティに関するお問合せ窓口の対応時間帯は、土曜日、日曜日、祝祭日並びに研究所が定める年末年始休暇を除く平日の午前 9 時から午後 5 時までです。

## 8.9 事業継続

### 8.9.1 セキュリティの目的

クラウドサービスの可用性が失われた場合の利用者業務に及ぼす影響を考慮して、事業継続計画を準備し計画に従い実施します。

### 8.9.2 実装と運用

- ABCI は高可用性を実現するため、十分な冗長性を備えた構成となっています。
- 次の各号に該当する場合は、ABCI 利用サービスの提供を中止できるものとしています。(ABCI 利用約款第 11 条)
  - 産総研の設備等の保守、工事、移設等のため必要である場合
  - 天災その他の非常事態が発生し、またはそのおそれがあるため、産総研による ABCI の運用を優先させる必要がある場合
  - 電気通信事業者等が、産総研の電気通信サービスの提供を中止した場合
  - その他、産総研が ABCI 利用サービスを提供するにあたり、合理的理由により、中止が必要であると判断した場合
- 産総研は、ABCI 利用サービスの提供に支障が出ると判断した場合には、利用法人または利用責任者に予告したうえでジョブのキャンセルを実行することがあります。また、緊急の場合は利用法人または利用責任者に対して予告することなくジョブのキャンセルを実行することがあります（ABCI 利用約款第 31 条)。
- 事業継続計画については、以下の通り計画、実施、検証・評価を行います。
  - 計画：ABCI サービスを継続して提供することが困難な状況（例えば、危機または災害）に備えて、情報セキュリティおよび情報セキュリティマネジメントの継続計画(BCP)を策定します。
  - 実施：必要な権限、経験および力量を備えた要員を任命し、困難な状況に備え、これを軽減し、対処するための十分な管理構造を設けます。

- 検証、評価：1 年に 1 回、BCP に基づいて予行演習を行います。情報セキュリティ継続のための妥当性と有効性を評価し、必要に応じて BCP を変更します。

**■ 利用の手引き**

- 産総研が ABCI 利用サービスの提供を中止する場合は、利用法人に対して産総研が適切と判断する方法（ウェブサイトでの表示、電子メールでの通知等の方法を含みますが、これに限定されません。）で通知します。ただし、緊急やむを得ない場合はこの限りではありません。

## 8.10 クラウドサービス利用終了・解約時の利用者データの扱い

### 8.10.1 セキュリティの目的

ABCI サービス利用終了の条件、解約の手続きおよびデータ移行、残留データの消去といった確認事項を明らかにします。

### 8.10.2 実装と運用

- ABCI サービス利用（利用契約）が終了した場合、産総研は終了後 6 か月が経過した時点で、記録されている利用者等のデータ等を含む利用者等に関わる一切のデータ（ただし、利用者等の登録情報や利用者等に関係するログ等を除きます）を削除します。
- 利用責任者から利用契約が終了する前に前項のデータを保存する旨の申し出があれば、利用契約終了後も産総研が認める期間に限り当該データを保存するものとし、この期間は産総研から利用責任者に通知します。
- ハードディスク等記憶装置については、ディスクの初期化や物理的な破壊は行いません。

**■ 利用の手引き**

- 利用者は利用契約終了前にプログラムやデータを自身の環境に回収し、ABCI 上のプログラムやデータは削除することを推奨します。

## 8.11 法令、契約上の責任

### 8.11.1 セキュリティの目的

クラウドサービス上の利用者のデータは、データセンターの所在地のデータ保護法令、個人情報保護法令等の影響を受けます。また、法執行機関による捜査の過程で自社の情報が提供されるかことも考えられます。

法令による影響とサービス利用に際しての留意すべき事項を明らかにします。

### 8.11.2 実装と運用

- ABCI 利用約款および利用に関する契約等は日本法に準拠し、日本法にしたがって解釈されるものとします（ABCI 利用約款第 40 条）。
- 産総研は、事故もしくは違法行為による漏洩、滅失または毀損から利用者等のデータ等を保護するために、合理的で適切な対策を実施します（ABCI 利用約款第 27 条）。
- 産総研および役職員等は、次の各号の場合を除き、利用法人または利用責任者による明示の承諾なくして ABCI に保存された利用者等のデータ等の閲覧、参照を行わず、第三者に

開示しません（ABCI 利用約款第 27 条）。

- ABCI 利用サービスの提供・維持のために第三者に業務委託を行う場合であって、かつ運用上必要な場合。ただし、産総研は業務委託先の第三者に対し、ABCI 利用約款における利用者等のデータ等の取扱を遵守させるものとします。
- 裁判所または行政機関より法令、判決、決定または命令に基づき開示が要求され、これに応じて研究所および役職員等が、当該裁判所または行政機関に対し、利用者等のデータ等の内容の開示および提供を行う場合。なお、この場合、研究所および役職員等は、上記の開示の要求があった旨を利用法人に通知します。

・ 利用者等が ABCI 利用サービスの利用により得られた知的財産権は、原則として利用者等に帰属するものとします。ただし、当該知的財産権に役職員等の寄与がある場合または産総研と利用法人との間で別途取り決めがある場合はこの限りではありません（ABCI 利用約款第 15 条）。

**■ 利用の手引き**

・ 利用者等は、ABCI を適切に利用し、利用者等のデータ等について、セキュリティを確保し保護すること、および定期的に保存することを含め、適切なセキュリティおよび保護を行うことを誓約していただきます（ABCI 利用約款第 19 条）。
・ 利用者等のデータ等に個人情報が含まれる場合は、「国立研究開発法人産業技術総合研究所個人情報の保護に関する規程」に従った適切な安全性確保の措置をとってください。
・ 次の各号に該当する行為を行ってはなりません。
  - 産総研もしくは第三者の著作権・商標権等の知的財産権を侵害する行為またはそのおそれがある行為
  - 研究所もしくは第三者の財産、プライバシーもしくは肖像権を侵害する行為またはそのおそれがある行為
  - 産総研の電子情報を改ざんまたは消去する行為
  - ウイルス等の有害なコンピュータプログラム等を開発する行為
  - 産総研のネットワークやインターネット網、それらに接続されたサーバ設備等に不正にアクセスする行為
  - ABCI 利用サービスの提供を妨害する行為または妨害するおそれのある行為
  - 法令に違反する行為またはそのおそれがある行為

# 9 支援体制

## 9.1 利用申請受付

受付メールアドレス： abci-application-ml@aist.go.jp
対応する項目（時間帯は 平日 9:00-17:00）
・ ABCI 利用申請の受付窓口
・ ABCI 利用料金に関するお問合せ
・ ABCI 利用申請、ABCI 利用グループ管理全般に関するお問合せ

## 9.2 情報セキュリティに関する問い合わせ、報告

受付メールアドレス： abci-inquiry-ml@aist.go.jp
対応する項目（時間帯は 平日 9:00-17:00）
・ 情報セキュリティインシデントの疑いが認知された場合の報告

・　ABCI のセキュリティに関するお問合せ
情報セキュリティインシデントの疑いが認知された場合には、別途定める様式に従って abci-inquiry-ml@aist.go.jp に至急報告してください。

### 9.3　運用サポート

受付メールアドレス：　qa@abci.ai
対応する項目（時間帯は 平日 9:00-17:00）
質問対応
・　ログイン手順
・　データ転送手順・データ回収手順
・　導入済みのソフトウェア環境への質問
・　典型的なフレームワークソフトウェアの導入手順（利用手引き）の開示
・　ジョブの投入方法・予算コードの指定方法の手順、等
・　不具合対応
・　H/W 障害
・　Network 障害
・　ノードハング、等

qa@abci.ai へ質問する際には、下記を記載してメールを送付してください。
[氏名]:
[ABCI アカウント名]:
[ABCI 利用グループ名]:
[所属機関]:
[登録メールアドレス]:
[質問内容]:
ABCI 利用サービスに係る利用の支援は、土曜日、日曜日、祝祭日並びに研究所が定める年末年始休暇を除く平日の午前 9 時から午後 5 時までです。

## 10　本書に関するお問い合わせ窓口

ABCI のセキュリティに関するお問合せ窓口
abci-inquiry-ml@aist.go.jp

## 11　参考文献

・　国立研究開発法人産業技術総合研究所　情報セキュリティ規程
・　内閣官房　内閣サイバーセキュリティセンター「政府機関等の対策基準策定のためのガイドライン」（平成３０年度版）
・　国立情報学研究所学術情報ネットワーク加入細則
・　国立研究開発法人産業技術総合研究所　共用高性能計算機 ABCI 利用約款
・　JIS Q 27017:2016（ISO/IEC 27017:2015）「JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範」
・　JASA-クラウドセキュリティ推進協議会 公開資料「基本言明要件に関わる基本リスク」
　　http://jcispa.jasa.jp/documents/

・ 文部科学省 「成長分野等における中核的専門人材養成等の戦略的推進」事業成果物 「実践クラウドセキュリティ」教科書（平成 29 年度版）