版数： 別添 Ver 1.0
発行日： 2019/8/9
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

別添 Ver 1.0

ABCI-WebUI ベース開発環境実証プログラムのセキュリティについて

2019 年 8 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

版数： 別添 Ver 1.0
発行日： 2019/8/9
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

改版履歴

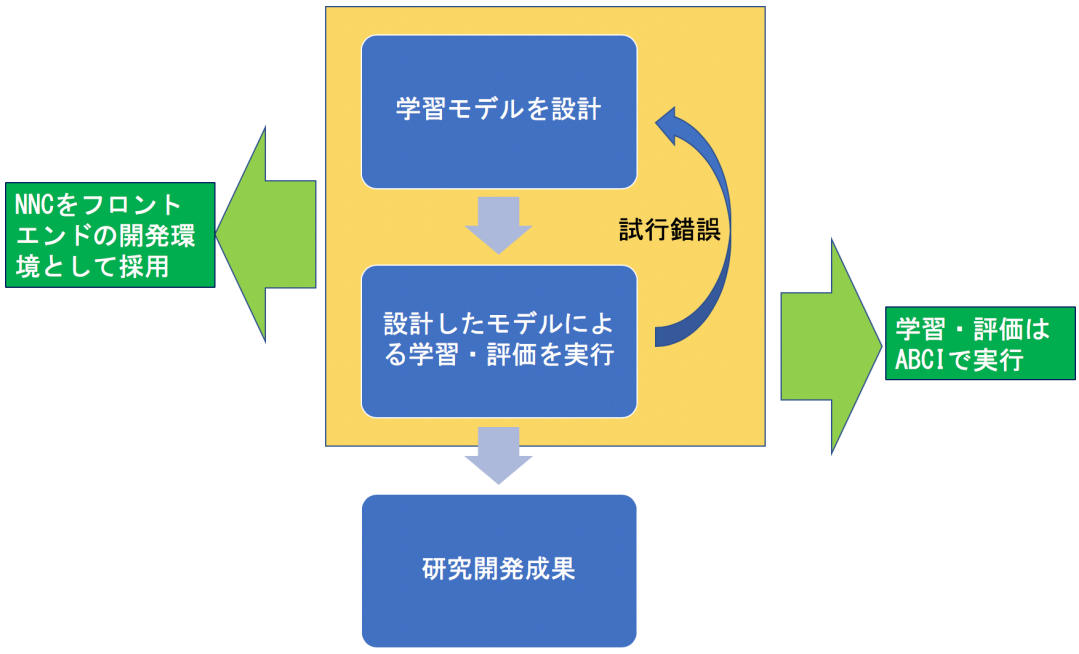
版数	発行日	改版内容
別添 VER 1.0	2019/8/9	初版発行

版数： 別添 Ver 1.0
発行日： 2019/8/9
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

1. ABCI-WebUI ベース開発環境実証プログラムの概要

ABCI-WebUI ベース開発環境実証プログラム（以下、「ABCI-WebUI」という。）は、ABCI の利用者層を拡大して、ABCI を活用した AI ユースケースの開発を目的とし、ディープラーニングの初学者にも使いやすい WebUI ベースの開発環境を ABCI のフロントエンドとして提供する事業者を公募した上で実証を委託するプログラムです。

この度、公募によってソニーの Neural Network Console (NNC)を採択し、クラウドサービスを提供することになりました。NNC クラウド版の利用者は、GPU として産総研の「ABCI」を選択可能となります。ご利用に当たっては、NNC のサイトから「ABCI 利用申請」が必要となります。



ABCI-WebUIの概要

2. 責任分界点

ABCI-WebUI の利用においては、NNC を運用するソニーネットワークコミュニケーションズと 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 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。ソニーネットワークコミュニケーションズ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。ABCI-WebUI の利用者は、NNC の事前同意事項(「クラウド版 ABCI 連携サービス利用規約」*を含む）に従う必要があります。

＊ https://dl.sony.com からご参照ください。

NNC のセキュリティについては、ソニーネットワークコミュニケーションズまでお問い合わせください。お問合せフォームは下記からアクセスできます。

https://support.sonynetwork.co.jp/IoT/web/form113.html

3. ABCI-WebUI ベース開発環境実証プログラムのセキュリティ解説

3-１ NNC による ABCI の利用

NNC は、ABCI の仕様に合わせて次の処理を実行するプログラムを ABCI のインタラクティブノードにインストールしています。これらのプログラムは、NNC からの制御によってのみ動作します。

- ジョブの投入
- データのアップロード
- データのダウンロード

これらのプログラムの脆弱性管理はソニーネットワークコミュニケーションズが責任をもって実施します。

3-２ NNC による ABCI 利用のモニタリング

NNC から投入されるジョブには、NNC によって、ABCI グループ ID 並びに NNC ユーザ ID が付与されます。これによって、ABCI では、投入されたジョブがどの NNC 利用者によるものかを一意に識別することができます。これらのジョブ投入履歴情報は ABCI に保存され、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利用します。

4. 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
inquiry@abci.ai

以上