マルチプラットフォームシステムでの
セキュリティ対策の PoC（概念実証）
報告書

2020 年 6 月 23 日

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

ORiN 協議会

Fraunhofer
IESE

目次

0. はじめに

製造システムの分野では、技術環境、市場環境の変化に対応して持続可能なエンジニアリングを目指した新しい考え方のプラットフォームが提案され、各国で展開されはじめている[1]。

独では、Industrie 4.0 のコンセプトに基づいた以下のプラットフォームが開発されている。

MindSphere[2]

BaSys 4.0[3]

日本では、各企業がコンソーシアムを形成して以下のプラットフォームが開発されている。

FIELD system[4]

Edgecross[5]

ORiN[6]

そして、IoT の導入並びにデジタルトランスフォーメーション（以降「DX」）の必要性が認識されてきている状況において、グローバルに展開されている製品が接続されていくのと同様に、グローバルに展開されているプラットフォームシステムの接続も進んでいくことが予想される。IPA 社会基盤センターは、そのような環境において懸念されるセキュリティリスクを認識し対策を検討していくことの重要性を示すために、独 Fraunhofer IESE 並びに日本の ORiN 協議会と協同で、IESE が Industrie 4.0 に基づいて開発中のプラットフォームである BaSys 4.0 と ORiN 協議会が仕様公開しているプラットフォームである ORiN とを連携したマルチプラットフォーム環境を作成し、そこで懸念されるセキュリティリスクへの対策機能の概念実証（以降「PoC」）を実施した。

本報告書は、上記 PoC で検討した懸念事項、対策の実施例と効果を示すものである。上記のように製造業の分野においては異なる複数のプラットフォームが運用され始めており、それらが1つの仕様に統一される、という状況は今のところ想定し難く、今後発生していくと思われる異なるプラットフォームの連携が必要な状況において、本書が役に立つことを期待する。

---

1 独では、国家プロジェクトで製造分野の標準的なプラットフォームのコンセプトである Industrie 4.0 が作成され、それを実現するいくつかのプラットフォームが考案され、展開されている。一方、日本では、製造分野のプラットフォームの標準的なコンセプトが作成されていない中で、いつくかの標準化団体がそれぞれ異なる仕様のプラットフォームを開発し、展開している。

2 独シーメンスが開発・販売しているクラウドベースのオープン IoT オペレーティングシステム。Industrie 4.0 のコンセプトを実現する有力なプラットフォームの1つとして独を中心にグローバルに展開。詳細は以下の URL を参照されたい。
https://new.siemens.com/global/en/products/software/mindsphere.html

3 独研究機関 Fraunhofer IESE が Industrie 4.0 のコンセプトに基づいて開発し公開しているオープンなプラットフォーム。詳細は以下の URL を参照されたい。
https://www.eclipse.org/basyx/

4 FIELD system (FANUC Intelligent Edge Link & Drive system)
製造業での更なる生産性向上と効率化を目指した、製造業向けオープンプラットフォーム。ファナック株式会社が開発・販売。詳細は以下の URL を参照されたい。
https://www.fanuc.co.jp/ja/product/field/index.html

5 一般社団法人 Edgecross コンソーシアムが仕様作成・開発・公開している製造業向けオープンプラットフォーム。詳細は以下の URL を参照されたい。
https://www.edgecross.org/ja/

6 一般社団法人 日本ロボット工業会 ORiN 協議会が仕様を作成し公開している製造システム向け標準ミドルウェア。詳細は以下の URL を参照されたい。
https://www.orin.jp/

1. 背景

“0. はじめに”で示したように、製造システムの分野において仕様の異なるいくつかのプラットフォームが展開されはじめており、今後海外のプラットフォームを含めたマルチプラットフォーム連携の機会が増えていくことが予想される。しかし、異なるプラットフォームを連携した事例がまだ少ないこともあり、そこで発生するセキュリティ脅威への対策が実施されている例もまだ少ないのが現状である。

一方で、工場の製造システムにおいては、接続されるシステムや機器が拡大していくことにより、システムに対するサイバー攻撃の増加が懸念され、また、実際にインシデント件数も増加しており、今後、製造システムへのセキュリティ脅威が増大していく要因として、各研究機関から以下が指摘されている[7]。

- フリーのデコンパイラを使って作成された Stuxnet[8]のソースプログラムと称するものがインターネット上で無償公開。高度な技術を使ったマルウェアを低予算で作成可能となる環境ができつつある。
- 特定 PLC[9]を標的とした情報収集ツールのソースプログラムがインターネット上で無償公開。これ以降、対象 PLC を標的としたとみられる不審な通信が増加。
- 産業ロボット・機器を利用した十分に可能性のある攻撃シナリオの実証が報告されており、それらを利用した製造システムにおいて使用不能な製品や危険な製品が製造されリコールや損害賠償を引き起こすリスク、及び産業ロボット・機器の損傷や製造従事者の怪我を発生させるリスクが指摘されている。また、その中で、数万台もの産業用機器がパブリックIPアドレスに存在していることが報告されている。

セキュリティインシデントの実態を示す情報も各研究機関から公開されており、その中で、標的型メール等を介して社内で入り込んだマルウェアが、多くのケースで PC や USB メモリを経由して工場内システムに持ち込まれていたことが報告されている[10]。また、情報システムと製造システムが接続されるケースも出てきており、マルウェアが情報システムから製造システムに入り込んできた事象も報告されている[11]。製造業を営む企業にとっては、事故の発生、稼働率低下、不良品製造が最も避けたい事態であり、上記のようにシステムへの攻撃の高度化が進み、また、実際のセキュリティインシデントが増加している状況において、対策が必須となってきている。

このようにマルチプラットフォーム化に伴うセキュリティ対策の必要性が増している製造システムに対して、有効と考えられる対策の効果を実証することは、上記の新しいコンセプトを実現するプラットフォ

---

7 本資料の付録 A.を参照されたい。

8 Stuxnet は、高度な技術により検知されずに持続的に方法を変えながらターゲットを探し出して攻撃を行う APT(Advanced Persistent Threat)と呼ばれるマルウェアの1つであり、おそらくイランの核燃料施設で利用されていたウラン濃縮用遠心分離機を誤動作させることを目的として開発されたと考えられている。実際に、2009 年から 2010 年にかけてイランの核燃料施設内のウラン濃縮用遠心分離機を制御するコンピュータに入り込み、その結果ほとんどすべての遠心分離機が稼働不能となる事態を引き起こした。

9 PLC(Programmable Logic Controller)は、小型のコンピュータの一種で、リレー回路用のプログラミング言語を使用したプログラムにより(ノイマン型コンピュータのプログラミング言語ではない)、接続されたロボットや機器を制御する。

10 本資料の付録 B.を参照されたい。

11 本資料の付録 B.を参照されたい。

ーム間の連携に寄与するものと考え、本 PoC（概念実証）を実施することを計画した。

PoC を実施するマルチプラットフォームシステムとしては、独 Industrie4.0 のコンセプトを実現した BaSys 4.0 を使ったシステムと産業用機器の標準ミドルウェア仕様として日本で考案・開発された ORiN を使ったシステムとを連携したシステムを想定した。また、PoC の内容は、このシステム上で、マルチプラットフォーム環境における脆弱性に対する脅威とそれに対する対策を実装し、その対策の必要性と効果を確認する、ということとした。（図 1-1）

この PoC を検討・実施するにあたり、BaSys 4.0 の開発元である独 Fraunhofer IESE と ORiN の仕様策定と展開を行っている ORiN 協議会、並びに本 PoC を推進する IPA とが協力して進めていくための MoU（了解覚書）を締結した。

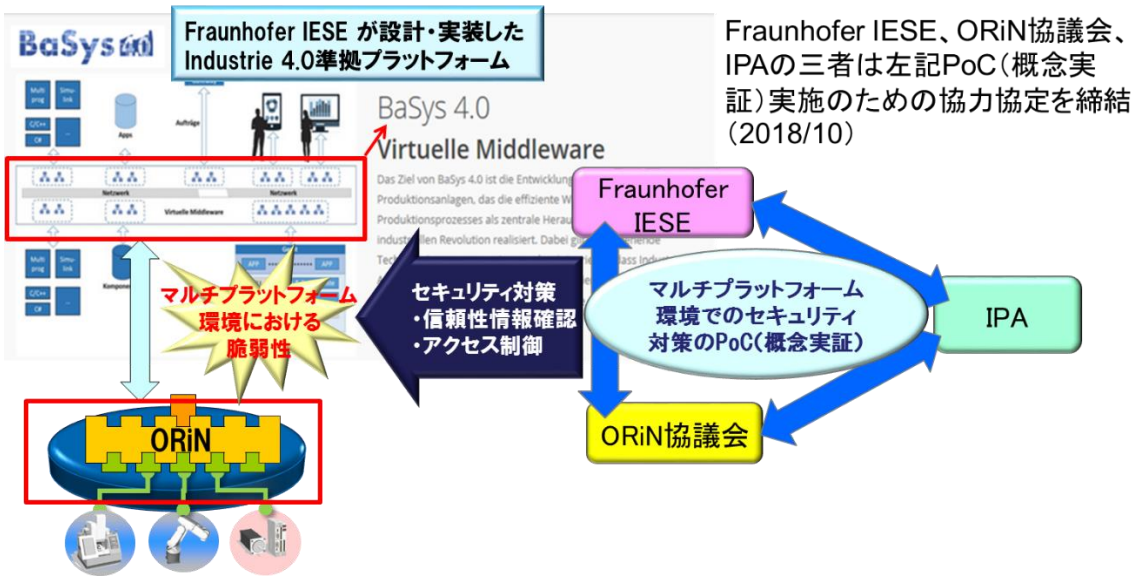


図 1-1 想定するマルチプラットフォーム環境と関係団体

2. 目的

本 PoC では、マルチプラットフォームシステムで懸念される脅威を検討し、一方のプラットフォームシステムの脆弱性を攻撃されて発生した影響が他方のプラットフォームシステムに及ぶことを防ぐための対策についてその実施例と効果を示すことを目的とした。そして、本 PoC の内容の公開が、産業界への以下の貢献に繋がることを期待するものである。

- 個々のプラットフォーム基盤ソフト（例えば、BaSys 4.0、ORiN、. . . ）に対して、他プラットフォームとの連携に備えたセキュリティ強化に貢献する。
- 日・独の産業界において今後増えていくと推測されるマルチプラットフォーム環境のセキュリティ対策向上に貢献する。
- 「IoT セキュリティガイドライン」の国際標準化活動[12]に対して、マルチプラットフォーム環境における脅威とその対策の効果並びに実現性を示すことにより、ガイドラインの内容が標準的な対策として実社会に浸透していくことに貢献する。

なお、対策の実施例は、IoT システムを想定した懸念事項に対する対策のガイドラインである「つながる世界の開発指針」[13]で示されている指針、並びに「『つながる世界の開発指針』の実践に向けた手引き」[14]で示されている IoT 高信頼化機能に基づいて検討し、実装した。（図 2-1）

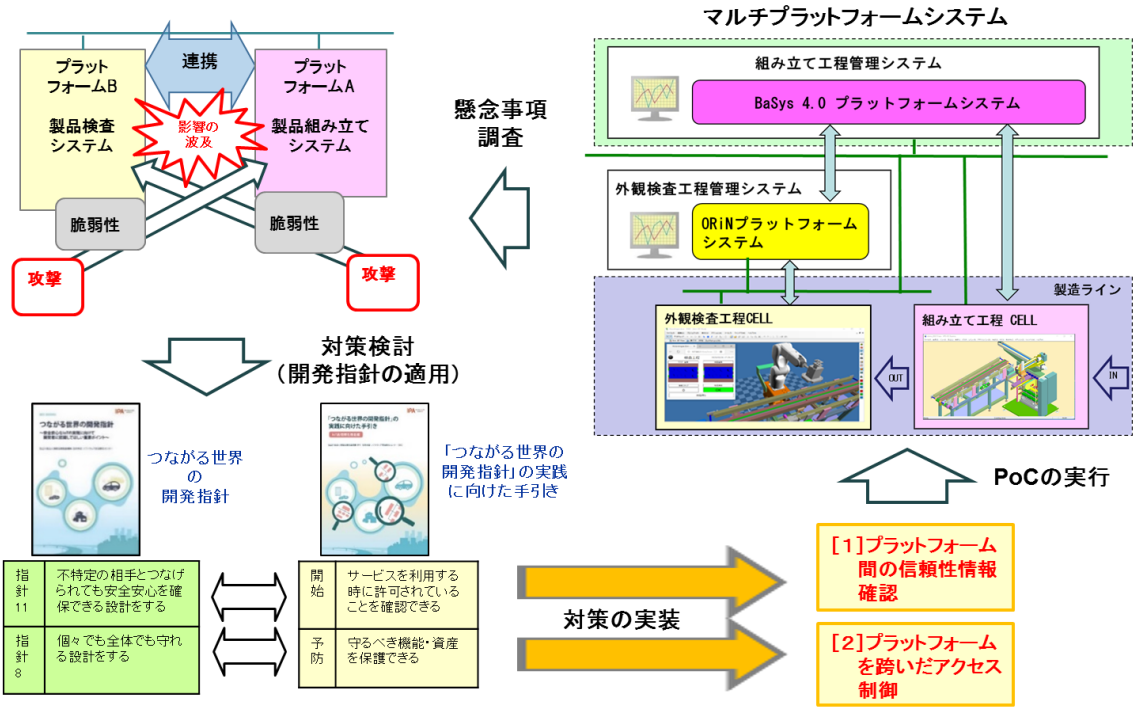


図 2-1 PoC で想定する懸念事項と対策

12 総務省の以下の資料を参照されたい。
https://www.soumu.go.jp/main_content/000556166.pdf

13 IPA の以下の URL で公開
https://www.ipa.go.jp/sec/publish/tn16-002.html

14 IPA の以下の URL で公開
https://www.ipa.go.jp/sec/publish/tn17-002.html

3. 体制と役割

“1. 背景”で記述したように、本 PoC は独 Fraunhofer IESE、ORiN 協議会、IPA の3者が MoU を締結し、協同で実施した。

各団体の役割を以下に示す。

表 3-1 体制と役割

団体	役割
IPA	・ PoCで実装するセキュリティ対策機能の仕様検討・調査 ・ PoCでのPCの調達とソフトウェア資材の購入 ・ アプリケーションプログラムの設計・開発 ・ PoCシステム開発のとりまとめ（含 PoCシステムの構築） ・ PoCの実施、評価、報告書作成
IESE	・ PoCで実装するセキュリティ対策機能の仕様検討・調査 ・ 検討結果において、IESEがBaSys4.0で有効と判断した機能の実装 ・ BaSys4.0プラットフォームSDK（含 ソースプログラム）の提供と技術サポート ・ BaSys4.0とORiNの連携インタフェースの開発支援とPoCでのアプリケーションプログラムの開発支援
ORiN協議会	・ PoCで実装するセキュリティ対策機能の仕様検討・調査 ・ 検討結果において、ORiNで有効と判断した機能の実装 ・ ORiNの技術サポート ・ BaSys4.0とORiNの連携インタフェースとPoCでのアプリケーションプログラムの設計・開発 ・ PoCの実施の支援

4. 想定モデル

4.1. 想定システム

PoC で想定するシステムのコンポーネント構成を図 4-1 に示す。

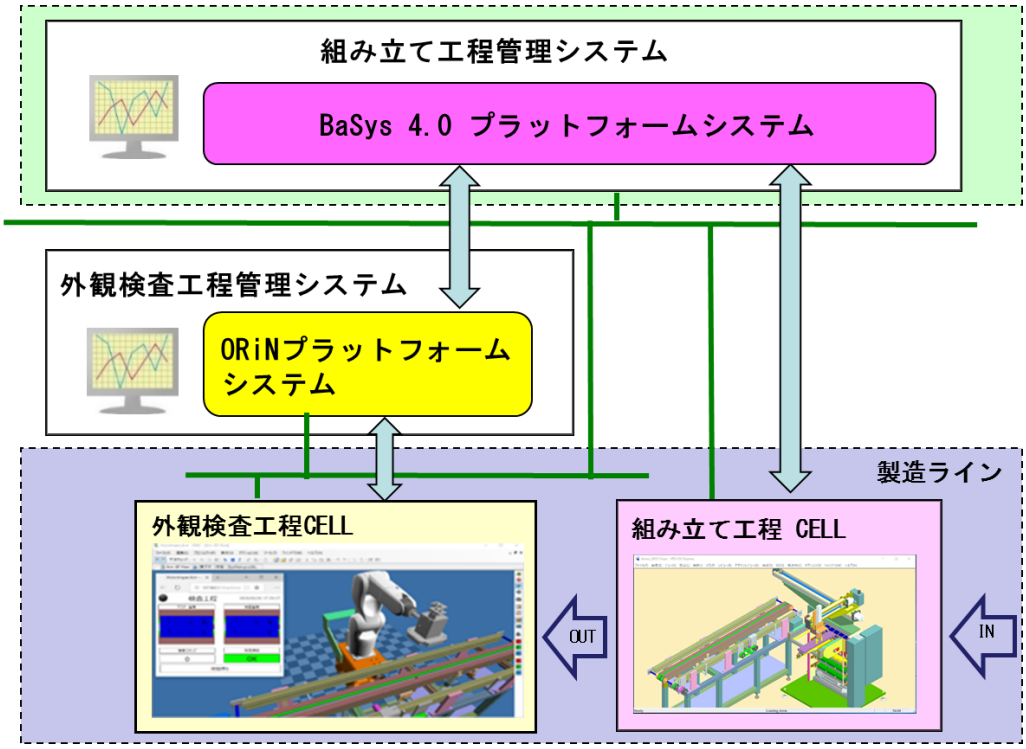


図 4-1 想定システムの構成

【組み立て工程 CELL 】

製品組み立てでは組み立てた製品を棚に積み込んでいく。検査対象抽出では、棚に積まれた製品から検査対象を取り出し、検査工程 CELL に渡す。この処理は、単軸ロボット並びに6軸ロボットを使って行う。組み立て工程 CELL の制御は、BaSys 4.0 上のアプリケーションによって行う。

【外観検査工程 CELL】

組み立て工程 CELL から渡された製品を指定された仕様に従って外観検査を行う。このシステムは ORiN プラットフォーム上で実現する。外観検査を行う装置を ORiN に接続し、ORiN 上のアプリケーションから制御する。

外観検査を行う装置は、汎用検査装置を想定し、ロボットがカメラを移動させて行う方式とする。

外観検査を行う装置は、一般に汎用検査装置と専用検査装置とがある。専用検査装置は特定の対象物では高い検査精度を実現できるが、費用が高く、かつ汎用性がない。汎用検査装置は、汎用性が高く、適切なセッティングを行うことにより費用を低くおさえることが可能である。中小企業では汎用検査装置を導入するのが現実的であり、本 PoC では汎用検査装置を想定した。ロボットがカメラを移動させて外観検査を行う汎用検査装置では、指定された仕様によってロボットの動作のパターンが登録されている。

4.2. 想定システムにおけるセキュリティ対象への攻撃と影響

想定システムにおけるセキュリティ対象と、考えられる攻撃、被害を以下に示す。

表 4-1 想定するセキュリティ対象への攻撃と影響

	セキュリティ対象	想定される脅威	想定される被害	
			分類	内容
A	各種PC/サーバ ・BaSys4.0実装 PC/サーバ ・ORiN実装 PC/サーバ	A-1 マルウェアのPC/サーバへの侵入と攻撃 ・DOS攻撃 ・OS(システムライブラリ、システムデータ)のなりすまし/改ざん/破壊/削除 ・基盤ソフトウェア(ブラウザ、DBMS等)のなりすまし/改ざん/破壊/削除 A-2 悪意ある第三者によるPC/サーバへの侵入と攻撃 ・ポートスキャニング ・メモリ改ざんによる悪意のあるコードの実行 ・OS(システムライブラリ、システムデータ)のなりすまし/改ざん/破壊/削除 ・基盤ソフトウェア(ブラウザ、DBMS等)のなりすまし/改ざん/破壊/削除 ・システムの乗っ取り	稼働率低下	・システムの異常停止 ・システムの破壊 ・PC/サーバ、ネットワークの負荷の増加
			セキュリティリスクの増加	・PC/サーバへ侵入するためのバックドアの生成 ・各種コンポーネント、各種データへの攻撃を可能とするためのアクセス制御情報の改ざん ・攻撃の準備(PC／サーバ上の脆弱性の分析ツールの実行)
			機密漏えい	・ファイル、DB上の秘密情報の漏えい
B	各種コンポーネント、データ ・各種アプリケーション ・BaSys4.0 実装コンポーネント ・ORiN実装コンポーネント ・各種プロバイダ ・各種プロファイルデータ ・制御データ ・監視データ	B-1 マルウェアのPC/サーバへの侵入と攻撃 ・各種コンポーネントのなりすまし/改ざん/破壊/削除 ・各種コンポーネント実行中のメモリ改ざん ・各種データの改ざん/削除 ・各種データの複写・転送 B-2 悪意ある第三者によるPC/サーバへの侵入と攻撃 ・各種コンポーネントのなりすまし/改ざん/破壊/削除 ・各種コンポーネント実行中のメモリ改ざん ・各種データの改ざん/削除 ・各種データの複写・転送	稼働率低下 損失増大	・システムの異常停止 ・システムの破壊 ・各種コンポーネントのプログラムの破壊 ・各種データの破壊 ・過少生産
			製造コスト増加	・過剰生産
			製品品質低下	・不良品製造(リコール発生) ・検査内容異常、検査結果異常
			機密漏えい	・機密情報(製造物に関する機密情報、産業ロボット・機器に関する機密情報)の漏えい
C	各種機器 ・産業ロボット・機器 ・PLC ・各種センサー類	C1 マルウェアによる産業ロボット、機器、PLCへのアクセスと攻撃 ・各種機器のファームウェアのなりすまし/改ざん/破壊/削除 ・各種データの改ざん/削除 ・各種データの盗み取り C2 悪意ある第三者による産業ロボット、機器、PLCへのアクセスと攻撃 ・各種機器のファームウェアのなりすまし/改ざん/破壊/削除 ・各種データの改ざん/削除 ・各種データの盗み取り ・非正規の部品による置き換え	製造環境安全性低下	・機器の破損(機器間の衝突、製造物と機器との衝突) ・機器と作業員との接触
			製造コスト増加	・消費電力増加
			製品品質低下	・不良品製造(リコール発生) ・製造物の破損 ・機器の乗っ取り
			機密漏えい	・機密情報(製造物に関する機密情報、産業ロボット・機器に関する機密情報)の漏えい

一般に複数のプラットフォームを連携させたシステムにおいては、以下の懸念事項が考えられる。

- 接続先のシステムにどの程度の脆弱性があるか
  （自システムの脆弱性は調査可能だが、他システムの脆弱性は調査が困難である）
- 接続先のシステムでの脆弱性に起因する脅威による影響が及んでくる可能性があるか

本 PoC で想定したシステムでは、BaSys 4.0 を利用したシステムあるいは ORiN プラットフォームを利用したシステムがなんらかの攻撃を受け、その影響が接続先である ORiN プラットフォームを利用したシステムあるいは BaSys 4.0 を利用したシステムに及ぶケースを想定した。

また、本 PoC では、本資料の付録Aで示している製造システムにおけるセキュリティ脅威の状況、並びに付録Bで示している実際のインシデントの状況を考慮し、セキュリティ対象としてシステム内のソフトウェア資材である各種コンポーネント、データを想定し、それらに対する脅威として、上記表の B-1 と B-2 を想定した。

B-1 マルウェアの PC/サーバへの侵入と攻撃

B-2 悪意ある第三者による PC/サーバへの侵入と攻撃

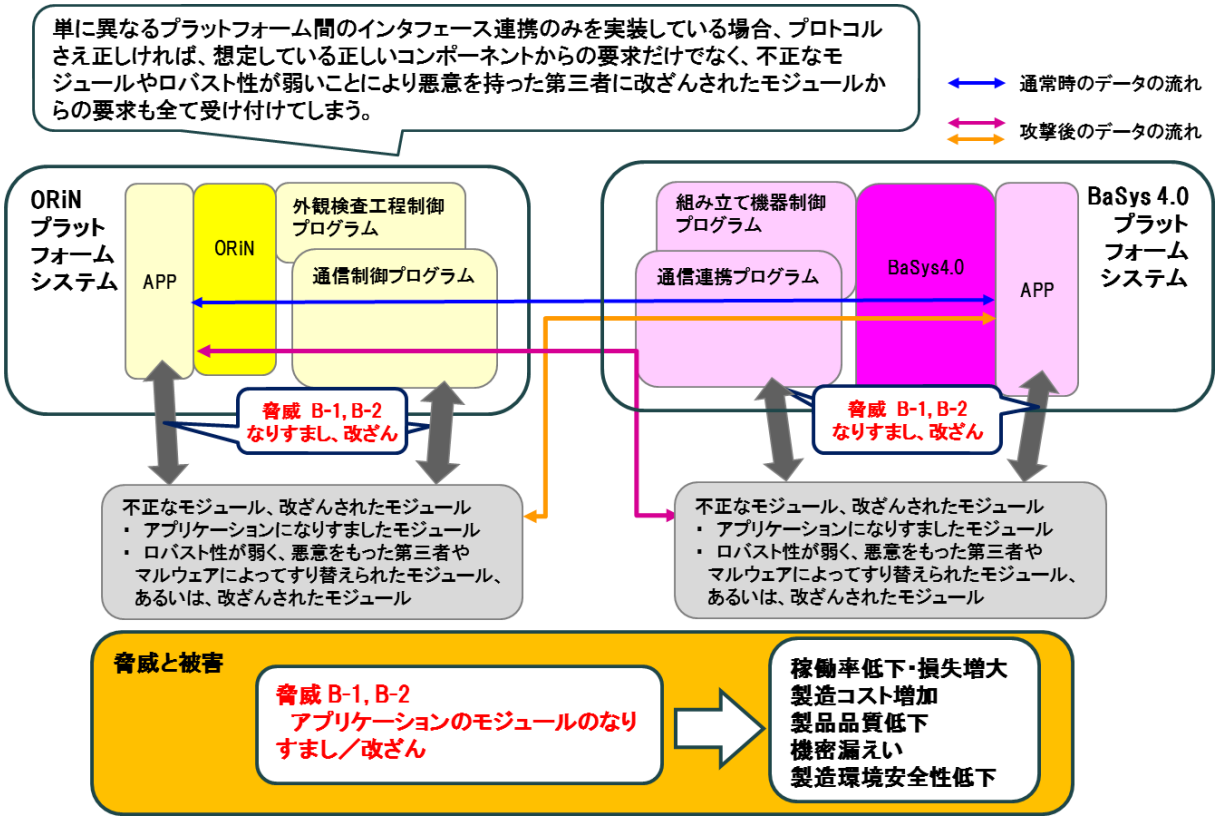


図 4-2 異なるプラットフォームを連携したシステムにおける攻撃と被害

本 PoC では、上記の脅威として以下の表 4-2 で示している攻撃を実現した。

表 4-2 PoC で実現した攻撃とその影響

攻撃の内容	システムへの影響（システムの挙動）
攻撃1. ORiNプラットフォームを利用したシステムにおいて、BaSys 4.0プラットフォームとの連携を実装したモジュールを不正なモジュールに置き換える。 ここで、不正なモジュールは、外観検査の結果をBaSys 4.0プラットフォームに返すとき、実際の検査結果とは異なる結果に書き換えるケースを想定した。	誤った検査結果が返されることにより、BaSys 4.0プラットフォーム上のシステムでは、例えば検査結果がNGであるのにOKが返された場合は、欠陥のある製品が市場に出てしまい、リコールに繋がる可能性がある。また、検査結果がOKであるのにNGが返される場合は、不要な品質調査を行うことになり、製造システムの稼働率が下がり、売り上げ減少に繋がる可能性がある。
攻撃2. ORiNプラットフォームを利用したシステムにおいて、BaSys 4.0プラットフォームとの連携を実装したモジュールの中の一部を不正なコードによって改ざんする。 ここで、不正なコードは、Basys 4.0との共用メモリ上のデータを誤った値により改ざんし、それがシステムに悪影響を及ぼすケースを想定した。	不正なコードは、BaSys 4.0プラットフォームシステムから製造物の検査を要求された直後にBaSys 4.0との共用メモリ上の検査対象製造物の種別を示す情報を別の値に更新する。これにより、BaSys 4.0プラットフォームシステムが検査対象製造物の正しい種別を指定しても、ORiNプラットフォームシステムに検査を要求した直後に誤った値となってしまい、正しい検査が実施されなくなる。また、BaSys 4.0プラットフォームシステムも共用メモリ上の誤った値を参照して動作することにより、誤動作する可能性がある。これにより、稼働率低下、歩留まりの想定外の低下が発生する。

4.3. 攻撃への対策

4.3.1. 対策の検討

一般にシステムへの攻撃に対しては、攻撃要因の侵入の抑止、並びに攻撃の効果の抑止を目的とした防御の対策と、攻撃によって発生した被害をいち早く検知して必要に応じて復旧を行うための被害抑止の対策の両者を実装するのが望ましい。

被害抑止の対策は、守るべきシステムの具体的な仕様並びに実現方式を考慮して検討する必要性が大きく、今回の PoC での検討対象からははずすこととした。

マルチプラットフォーム環境を想定した防御の対策は産業界においてはまだそれほど実装されていないと考えられる。通常、防御の対策はシステムの脆弱性とセキュリティ脅威を想定し、その対策を検討して導出される（攻撃要因の侵入の抑止）。この脆弱性とセキュリティ脅威はセキュリティリスク分析から検出されるが、製造システムのセキュリティ分析に関する情報については、例えば、IPA から以下の資料を公開しており、参考とすることができる。

- 制御システム　セーフティ・セキュリティ要件検討ガイド[15]
- 制御システムのセキュリティリスク分析ガイド　第 2 版[16]
- 制御システムのセキュリティリスク分析ガイド補足資料「制御システム関連のサイバーインシデント事例」 シリーズ[17]

本 PoC では、セキュリティ分析で検出されるシステムの脆弱性とセキュリティ脅威に関して、マルチプラットフォームシステム特有の懸念事項として、個々のプラットフォームシステムにおける脆弱性をついた攻撃の影響が接続先のプラットフォームシステムに及ぶケースを重視した。そして、この懸念事項への対策として、信頼性情報の中にどのような対策をとられているかを示す情報（例えばモジュール間認証の有無、データ秘匿で使用している暗号方式の仕様等）を含め、他プラットフォームと接続するときは採用されている対策の内容に応じて接続する/しないを判断する、という対策を実装し、効果を確認した。

他方、上記のように防御の対策で攻撃要因の侵入の抑止を目的とした対策では、攻撃技術の高度化によってすり抜けられてしまう可能性を考慮しておくことが望ましい。そのため、攻撃を受けてしまったとしてもその影響をできる限り小さく抑えるための対策（攻撃の影響の抑止）も必要である。その対策の1つとして資源に対するアクセス制御がある。アクセス制御機能は、それを実装するコンポーネントのロバスト性を強化するための対策は時間とともに変化していくのに対し、アクセス制御そのものは、基本的に時間の経過に関わらず有効である。そこで、本 PoC では、プラットフォーム間で共用するデータに対するアクセス制御機能を実装し、その効果を確認した。

なお、一般的な防御の対策として、不正コードや不正データの侵入の検知と防御、難読化等の耐攻撃性強化、といったことも考える必要があるが、それらの機能は広く検討・活用されており、また、耐攻

15 IPA の以下の URL で公開。
https://www.ipa.go.jp/sec/reports/20180319.html

16 IPA の以下の URL で公開。
https://www.ipa.go.jp/files/000069436.pdf

17 IPA の以下の URL で公開。
https://www.ipa.go.jp/security/controlsystem/incident.html

撃性強化の実装方式はシステムの固有部分に非常に大きく依存するため、システム固有の対策として検討されるのが適切である。そのため、本 PoC では、それらの対策は検討対象からはずした。

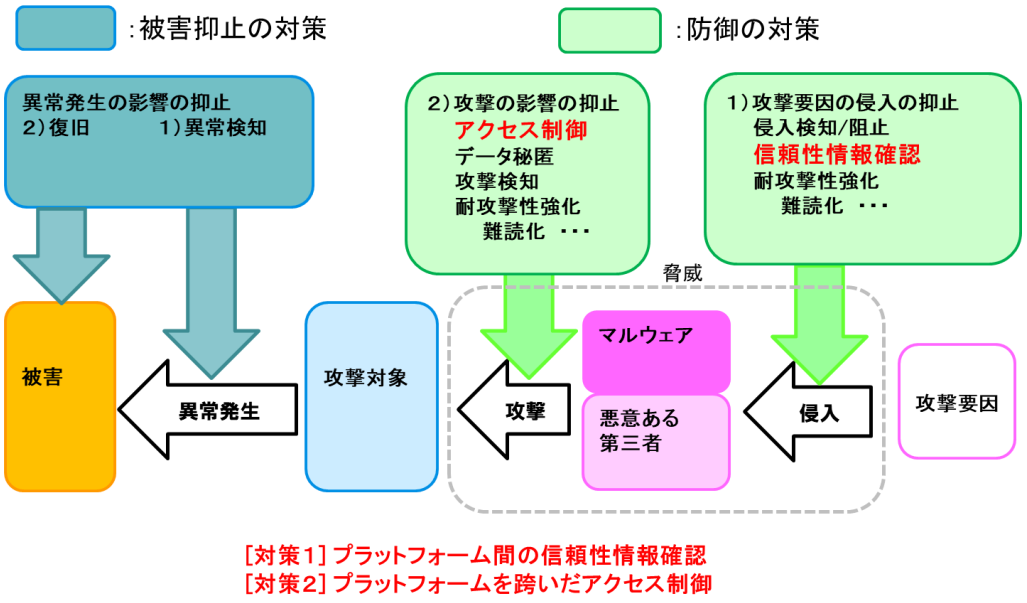


図 4-3 PoC で検討した対策

本 PoC では、4.2 の表 4-2 で示した攻撃を想定システム上で実現し、また、上記防御の対策として以下の機能を実装し、その効果を確認した。

［攻撃 1 への対策］

［対策1］プラットフォーム間の信頼性情報確認

プラットフォーム間の接続時に、それぞれのプラットフォームがお互いの信頼性情報の内容を確認し、想定される脅威に対して一定レベル以上の対策がとられていないとみなされる場合は、接続環境を確立しない。

［攻撃 2 への対策］

上述のように、攻撃要因の侵入抑止を目的とした[対策1]では影響を抑止できないケースが考えられ、[対策1]に加えて攻撃の影響抑止を目的とした[対策2]を実装した。

［対策2］プラットフォームを跨いだアクセス制御

他プラットフォームからの要求を受け付けて、その延長でデータや機器へのアクセスを行うにあたり、要求の内容が不正な値に置き換わっていた場合、アクセスしてはならないデータや機器へのアクセスが起こる可能性がある。要求元プラットフォームとその要求の延長でアクセス可能なデータや機器との組み合わせをあらかじめアクセス制御情報として登録しておき、登録されていない組み合わせでデータや機器へのアクセスが発生した場合はそれをエラーとする。

4.3.2. 対策の効果の確認方法

上記の2つの対策について、それらの効果を確認した方法を以下に示す。

(1)攻撃 1 と［対策1］プラットフォーム間の信頼性情報確認

攻撃 1 では、マルウェアまたは悪意をもった第三者が、2つのプラットフォームシステム間のセキュアな通信環境を実装しているコンポーネントライブラリの外側にあるアプリケーションのモジュールを以下の被害を発生させることを目的とした不正なプログラムですりかえる。

- 機器の異常動作による設備破損、製造物破損、不良品製造
- システムの稼働率低下、製造コスト悪化
- 機器や製品に関する秘密情報の漏えい

通常、プラットフォーム間の接続では相互認証を前提としたセキュアな通信環境を開設するのが一般的であり、これを実装しているモジュールの範囲においては、不正なモジュールへのすり替えは困難といえる。しかし、その範囲外のモジュール、特にシステム毎に開発されたアプリケーションプログラムは、モジュールのすり替えへの対策がとられているケースは少なく、モジュールのすり替えを比較的容易に行うことが可能なケースが多い。そして、あるプラットフォームのシステムにおけるモジュールのすり替えは、それと接続している他のプラットフォームでは検知することがほぼ不可能である。そこで、攻撃1では、セキュアな通信環境を実装しているモジュールの範囲外にあるアプリケーションプログラム内のモジュールを誤った処理を引き起こすモジュールに置き換えた状態を作り、誤った処理が行われることを確認する。

［対策1］では、それぞれのプラットフォームにおいて、呼び出し先／呼び出し元モジュールの正当性確認を行うことを前提とする。プラットフォーム間通信を行うモジュールでは、接続するプラットフォームとの間で信頼性情報を相互に確認する処理を追加し、信頼性情報の中にはモジュール間の正当性確認を行っているか否かを示す情報を設ける。プラットフォーム間の信頼性情報確認では、信頼性情報の真正性検証により接続先プラットフォームの正当性を確認するに加え、信頼性情報の中のモジュール間正当性確認を行っているかどうかをチェックする。モジュール間正当性確認を行っていないプラットフォームについては、不正モジュールにより置き換えられている可能性があるとみなし、接続を拒否する。PoC では、以下のケースの動作を確認した。

① 相手のプラットフォームが信頼性情報自体を持っていない場合、システムが想定外の動作をする前に、プラットフォーム間の接続がエラーで終了する。

② 相手のプラットフォームの信頼性情報の真正性が確認でき、かつモジュール間正当性確認を行っていることを確認できた場合、接続を完了させ、エラーが発生せずに正常に処理が行われる。

なお、以下のケースについても対策の効果の検証を検討したが、効果の見える化が難しく、本 PoC では実装しなかった。

- 相手のプラットフォームの信頼性情報の真正性は確認できたが、信頼性情報の内容によると相手のプラットフォームではモジュール間正当性確認を行っていない場合、やはり、システムが想定外の動作をする前に、プラットフォーム間の接続をエラーで終了させる。

(2)攻撃 2 と［対策2］プラットフォームを跨いだアクセス制御

攻撃 2 では、高度な技術を持ったマルウェアまたは悪意のある第三者が、アプリケーションプログラムの一部あるいはアプリケーションプログラムが処理するデータの一部を改ざんする。攻撃 2 の目的は攻撃 1 と同じである。

- 機器の異常動作による設備破損、製造物破損、不良品製造
- システムの稼働率低下、製造コスト悪化
- 機器や製品に関する秘密情報の漏えい

［対策1］で前提としているモジュールの正当性確認では、主に性能的な要件から、モジュールやデータの全領域をチェックできるわけではない。クリティカルな範囲の正当性確認を行ったとしても、正当性確認が行われていない箇所に想定外の動作を引き起こす処理が組み込まれてしまった場合、その攻撃を防ぐことができていない。

［対策1］ で前提としているモジュールの正当性確認ではチェックしていない処理部分に想定外の動作を引き起こす処理を組み込み、［対策1］ が機能している状態であっても、攻撃 2 により異常な動作が引き起こされることを確認する。

［対策2］ では、他プラットフォームからの要求に応じてデータの参照・更新やプログラムの実行を行うケースにおいて、要求元を主体としたアクセス制御を可能とする。つまり、接続対象プラットフォームと対象資源との組み合わせにおいて可能なアクセスを登録し、そこに登録されていないパターンのアクセスが発生した場合はエラーとする。この対策は、各プラットフォームの中で他プラットフォームとの通信の内容を確実に確認できる場所で実装するのが適切であり、他プラットフォームとの連携を実現するコンポーネント（例えば、本 PoC で想定するシステムでは、図 4-1 の中の「プラットフォーム連携アプリケーション」）で実装する。本 PoC では、以下のケースの動作を確認する。

① PoC システムを、［対策1］ を実装した状態にしておく。
② ORiN プラットフォーム側のコンポーネント内のモジュールの一部を改ざんし、BaSys 4.0 プラットフォーム上のデータが誤った値で更新される状態を発生させ、ORiN プラットフォーム上での製造物の検査結果が BaSys 4.0 プラットフォーム上で誤って認識される状態を引き起こす。
③ ［対策2］ を実装したとき、BaSys 4.0 プラットフォーム上のデータに対して、許可されていないアクセスが発生したことを示すエラーが起こることを確認する。

5. 実験環境

5.1. 設備・場所

本 PoC では、産業用ロボット並びに産業用機器を実機ではなくエミュレータとシミュレータを使って PC 上で実現した。

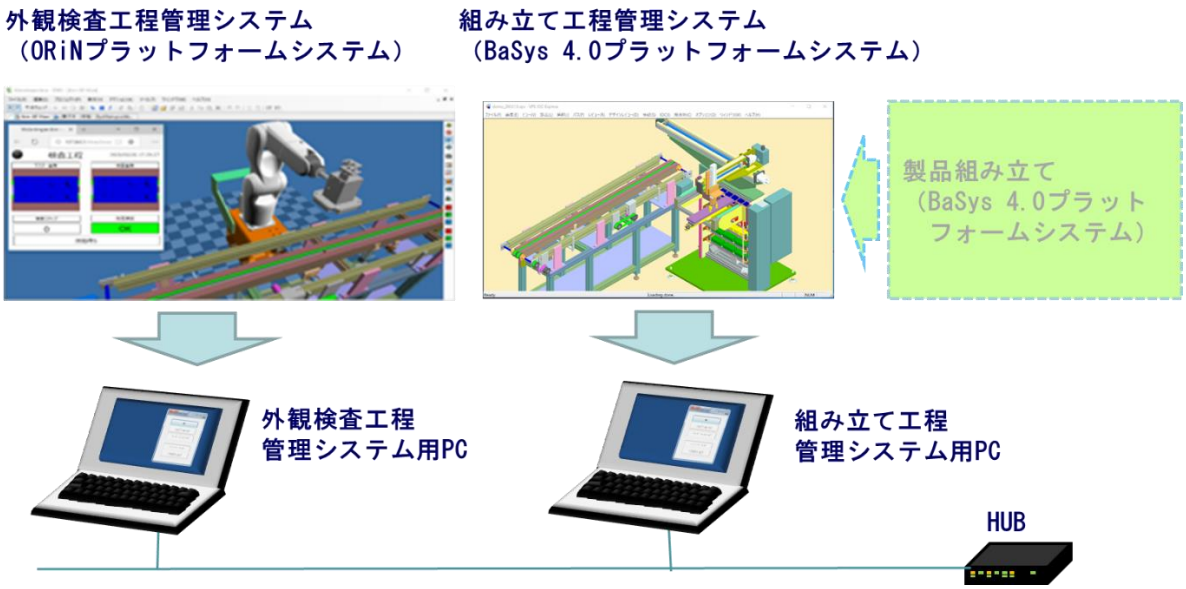


図 5-1 構築した PoC システムの概要

近年、製造業の分野において、製造システムの事前検証を目的として、デジタル化が進んでいる。製造システムの刷新・改良、新しい製品や改良した製品の製造にあたっては、事前にサイバー空間上で製造システムを実現して製品を製造し、そこで十分に製造システムの検証をした上で、実機を使ったラインに製造システムを適用する。より進んだ企業では、すでに数年前から製造した製品の検証まで含めてサイバー空間上で実現している。

Industrie 4.0 の世界になると、Digital Twin が実現され、現実世界でセンサー等によって得られた情報がリアルタイムでサイバー空間上に反映され、時間経過に伴う環境や物の変化もサイバー空間上で実現されることになる。これにより、製造システムにおける異常状態の再現や新しい機器や機能の試行・検証を行うのに必要となる空間・資源・時間は、実機を使うケースと比べて圧倒的に少ない量で済む。そのため、環境変化に対応できるより柔軟な製造システムの実現や、より精度の高い検証が短時間で可能となる。エミュレータ並びにシミュレータは、それを実現するための不可欠な基盤技術である。サイバー空間上で、セキュリティ脅威の影響や対策の効果、対策の実現性を示すことは、デジタル化が進んでいく産業界において、意義のあることと考えた。

本 PoC の実施風景を以下に示す。(独立行政法人情報処理推進機構　事務所内)

図 5-2　PoC 実施風景

PC1 ： 組み立て工程管理システムを実装

VPS IOC	：	制御系ソフト開発支援用シミュレータの表示
Assembly Equipment	：	組み立て工程の機器の動作結果
Syslog	：	組み立て工程管理システムが Syslog に出力した結果

PC2 ： 外観検査工程管理システムを実装

EMU	：	制御系ソフト開発支援用エミュレータ＋シミュレータの表示
VisionInspection	：	外観検査結果
IoTDataView	：	管理対象機器からの取得データ集計結果
Syslog	：	組み立て工程管理システムが Syslog に出力した結果

5.2. ソフトウェアコンポーネント構成

PoC システムの各 PC のソフトウェアコンポーネントの構成を以下に示す。

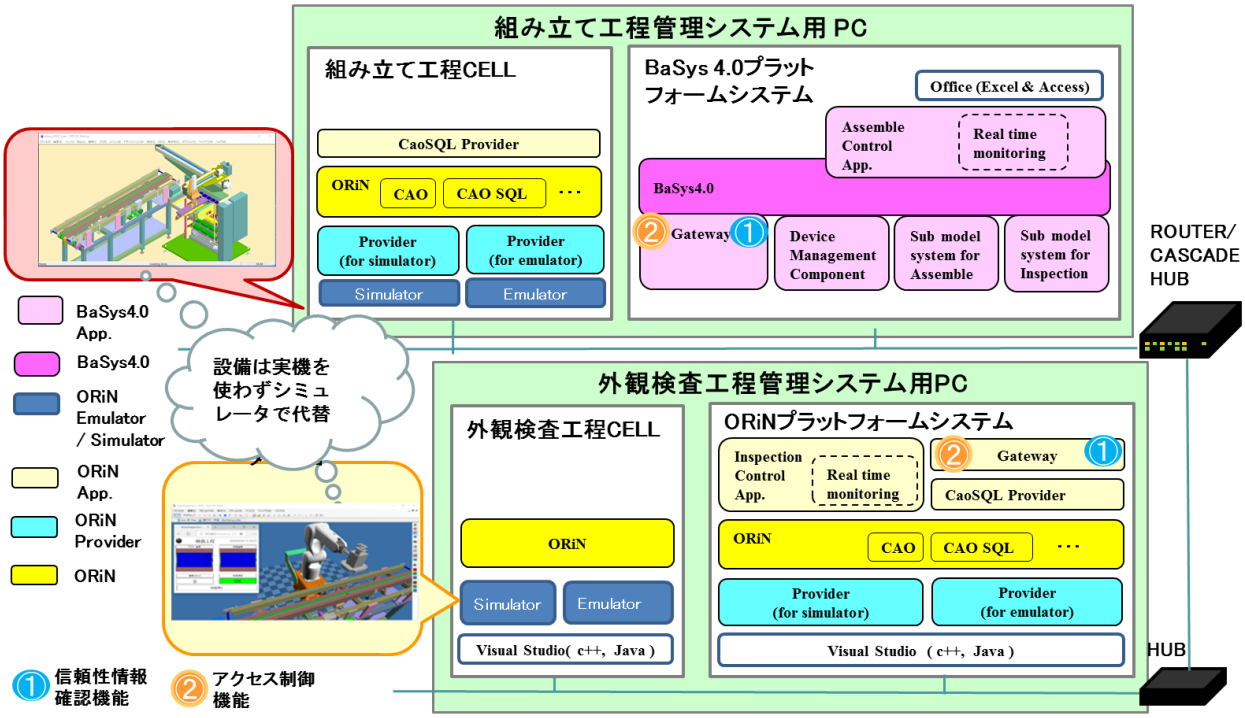


図 5-3 PoC システムのソフトウェアコンポーネント構成

各ソフトウェアコンポーネントの概要を以下に示す。

表 5-1 PoC システム内の各ソフトウェアコンポーネント

コンポーネント名	プラットフォーム	分類	分類
Assemble Control App	BaSys 4.0	アプリケーション	組み立て工程 CELL を制御するアプリケーション
Realtime monitoring	BaSys 4.0	アプリケーション	組み立て工程セル並びに検査工程セルのそれぞれのセルの中で動作し、各セルのシステムをリアルタイムに監視する。
BaSys 4.0	BaSys 4.0	ミドルウェア	BaSys 4.0 ライブラリ全体
Sub model system for Assemble	BaSys 4.0	アプリケーション	組み立て工程セルの機器やプログラムの監視データのメタデータと監視データそのものを蓄積し、管理する。
Sub model system for Inspection	BaSys 4.0	アプリケーション	検査工程セルの機器やプログラムの監視データのメ

			タデータと監視データそのものを蓄積し、管理する。
Device management component	BaSys 4.0	アプリケーション	ORiN プラットフォーム上の検査工程セルシステム内の各機器やプログラムの監視情報を取得する。ORiN プラットフォームとの通信は、Gateway を経由して行う。
Gateway	BaSys 4.0	アプリケーション	BaSys 4.0 上で動作し、BaSys 4.0 上のアプリケーションと ORiN 上のアプリケーションとの間のデータ転送を制御する。
Gateway	ORiN	アプリケーション	ORiN 上で動作し、ORiN 上のアプリケーションと BaSys 4.0 上のアプリケーションとの間のデータ転送を制御する。
Inspection Control App	ORiN	アプリケーション	検査工程 CELL を制御するアプリケーション。
CaoSQL Provider	ORiN	アプリケーション	ORiN プラットフォーム上の各機器やプログラムの監視データを ORiN の機能（CaoSQL）を使って取得する。
ORiN	ORiN	ミドルウェア	ORiN のコアライブラリ全体。CaoSQL、CAO 等のライブラリを含む。
Provider	ORiN	ドライバ	機器や PLC、他プラットフォームと接続して、制御並びにアクセスするためのソフトウェア。
Emulator	ORiN	機器代替ソフト	ORiN に接続した産業機器の動作を PC 上でエミュレートする。
Simulator	ORiN	機器代替ソフト	ORiN に接続した産業機器の動作を PC 上でシミュレート（表示）する。

5.3. 基本動作概要

想定したシステムでは、組み立て工程管理システムが組み立て工程セル内の産業ロボットを制御する。具体的には、指定された製造物を棚から取り出し、検査工程セルに製造物の仕様に関する情報（種類）と製造物を渡す。組み立て工程管理システムは、BaSys 4.0 プラットフォーム上で動作する。

外観検査工程管理システムは、検査工程セル内の産業ロボットを制御する。検査工程セルは組み立て工程セルから渡された製造物の仕様に関する情報に従って製造物の外観検査を行う。外観検査工程管理システムは、ORiN プラットフォーム上で動作する。

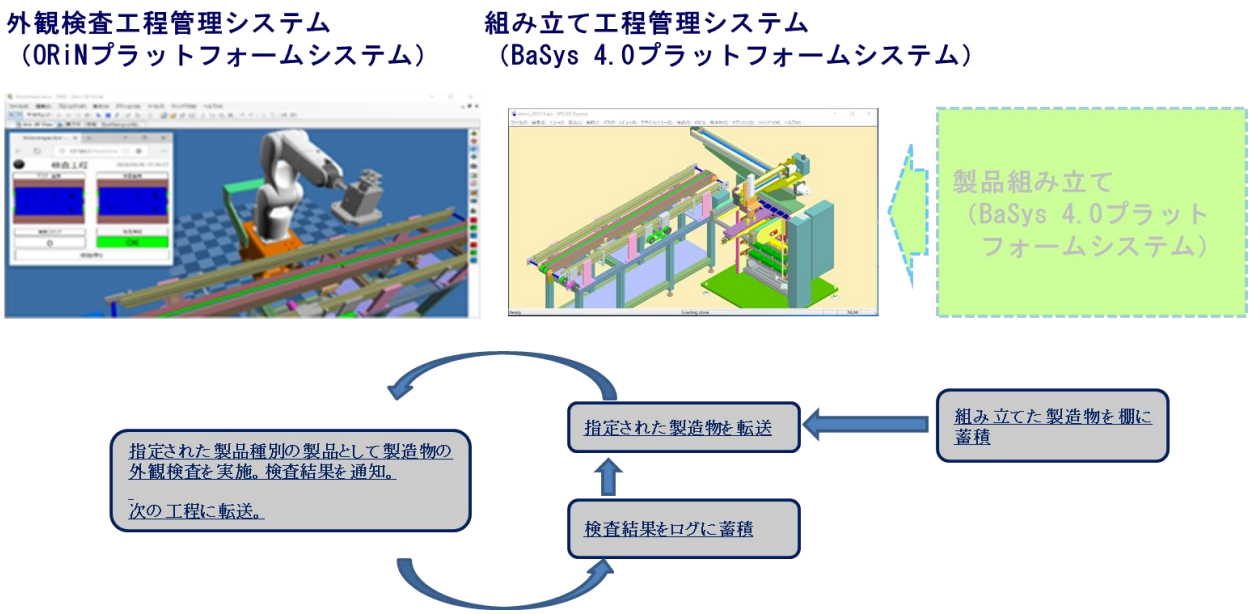


図 5-4 PoC システムの基本動作

組み立て工程管理システムと外観検査工程管理システムは、相互に通信して同期をとることにより、組み立て工程セルと検査工程セルとの間の製造物の受け渡しと検査結果の通知を実現する。

各システムの機能の概要を以下に示す。

1） 組み立て工程管理システム

組み立て工程制御画面で指定された値に従って、製造物を選択して外観検査工程管理システムに渡す。

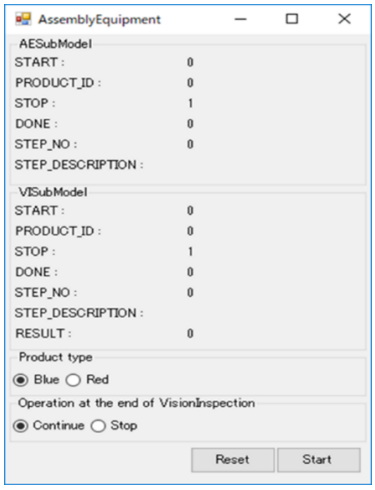


図 5-5 組み立て工程制御画面

[Start]ボタンが押された場合、製造物の種類（1:Blue、2:Red）、製造物の識別 ID (PRODUCT_ID)、START＝1を設定して組み立て工程の開始を指示する。

指定された種類の製造物を選択し、その仕様に関する情報と製造物の識別 ID を外観検査工程管理システムに渡し、選択した製造物を転送する。

外観検査工程管理システムから結果が返されてきたら、その結果を組み立て工程制御画面の(RESULT)に設定して表示する。

2） 外観検査工程管理システム

組み立て工程管理システムから送信された製造物に関する情報をもとに、転送されてきた製造物の外観検査を行う。

外観検査が終わったら、その結果を組み立て工程管理システムに返信する。

組み立て工程管理システムから送信されてきた製造物に関する情報、並びに外観検査の結果は、外観検査工程制御画面に表示される。(以下は、製造物の種類が “1:Blue” のケース)

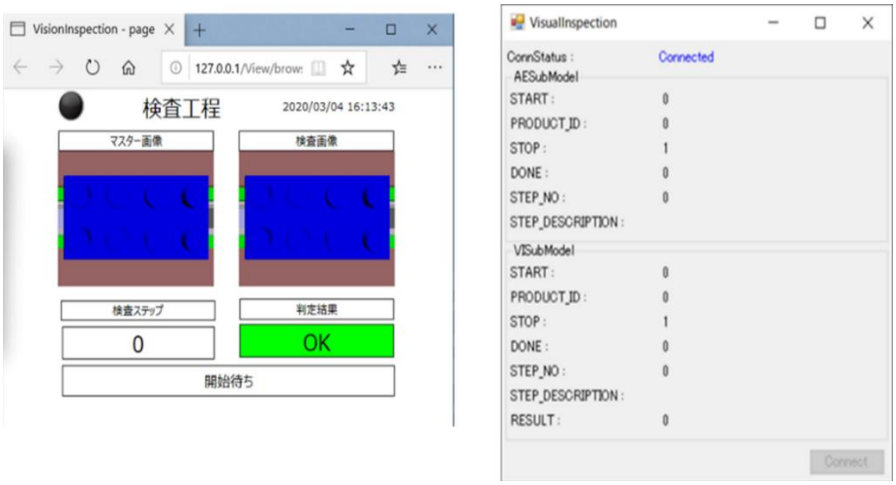


図 5-6 外観検査工程制御画面

5.4. PoC システムにおけるプラットフォーム連携方式

BaSys 4.0 プラットフォーム上において、本 PoC で想定する製造システム全体を1つの AAS（Asset Administration Shell）に対応させ、組み立て工程管理機能をサブモデルの1つとして登録した。一方、ORiN プラットフォーム上の外観検査工程管理システムは、BaSys 4.0 プラットフォーム上のシステムとは別のシステムとして存在している。本 PoC では、BaSys 4.0 プラットフォーム上のシステムと ORiN プラットフォーム上のシステムとを連携させるが、これを、ORiN プラットフォームシステム上の外観検査工程管理のミラーリング機能を上記 AAS のサブモデルの1つによって実装することにより実現した。これにより、組み立て工程管理システムからは、外観検査工程管理システムが BaSys 4.0 プラットフォーム上に存在するシステムであるかのようにコミュニケーションをとることを可能とした。

ORiN プラットフォーム上の外観検査工程管理と BaSys 4.0 プラットフォーム上のミラーリング先との間のデータ通信は、双方のプラットフォーム上でプラットフォーム連携用の Gateway アプリケーションを介して行う。そして、ORiN プラットフォーム上のアプリケーションと Gateway アプリケーションとは、ORiN の Gateway 専用プロバイダを経由してデータのやりとりを行い、BaSys 4.0 プラットフォーム上のアプリケーションと Gateway アプリケーションとは、AAS を介してデータのやりとりを行う。

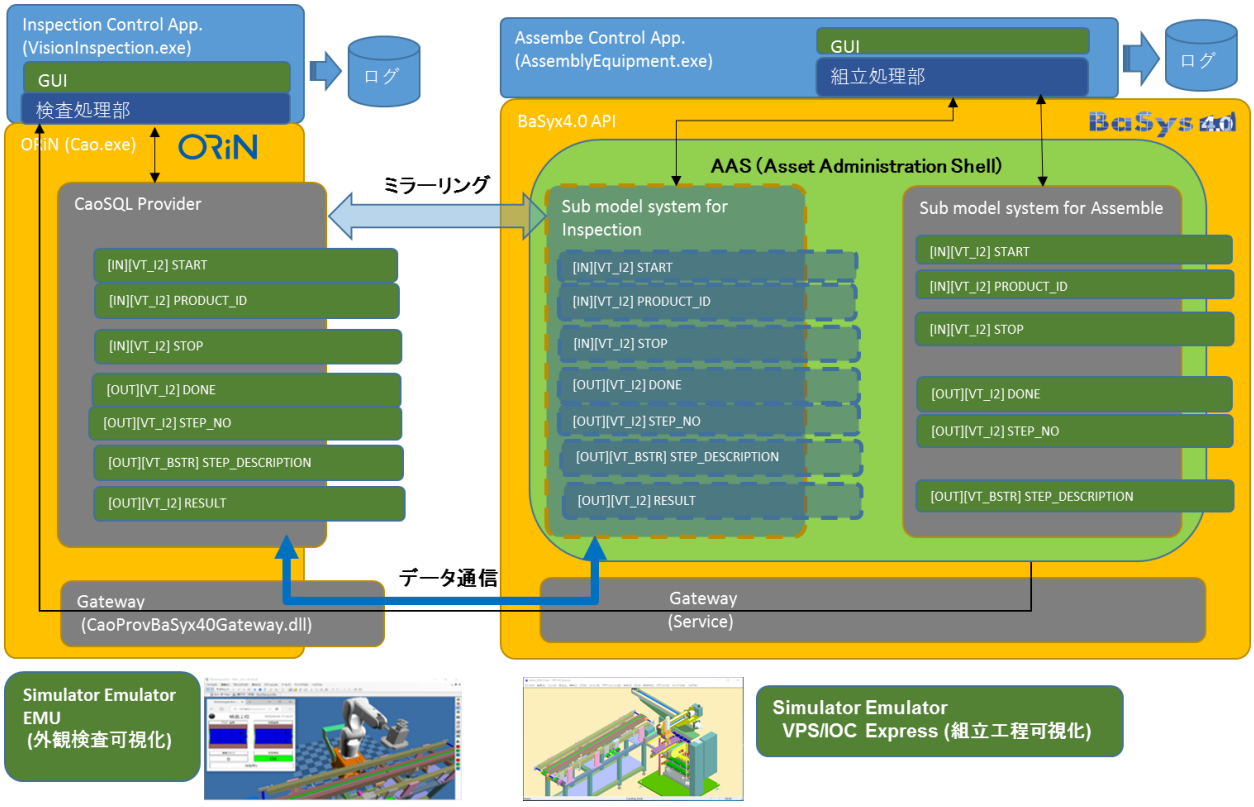


図 5-7 BaSys 4.0 プラットフォームシステムと ORiN プラットフォームシステムの連携

6. 対策の概念実証

6.1. 概要

PoC では、一方のプラットフォームシステムが攻撃を受けたときの他方のプラットフォームシステムへの影響を確認し、対策機能を有効にしたときに攻撃の影響がなくなることを確認した。(図 6-1)

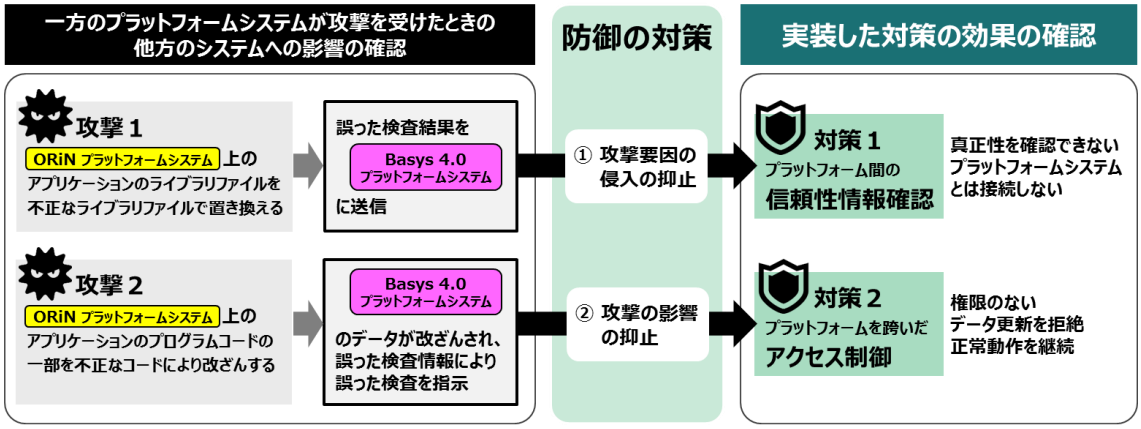


図 6-1 攻撃の影響と対策による効果の確認

6.2. [対策 1] プラットフォーム間の信頼性情報確認

6.2.1. 攻撃の実装と影響

ORiN プラットフォームシステム上の Gateway アプリケーションのライブラリファイルを不正な処理を行うライブラリファイルで置き換える。(図 6-2)

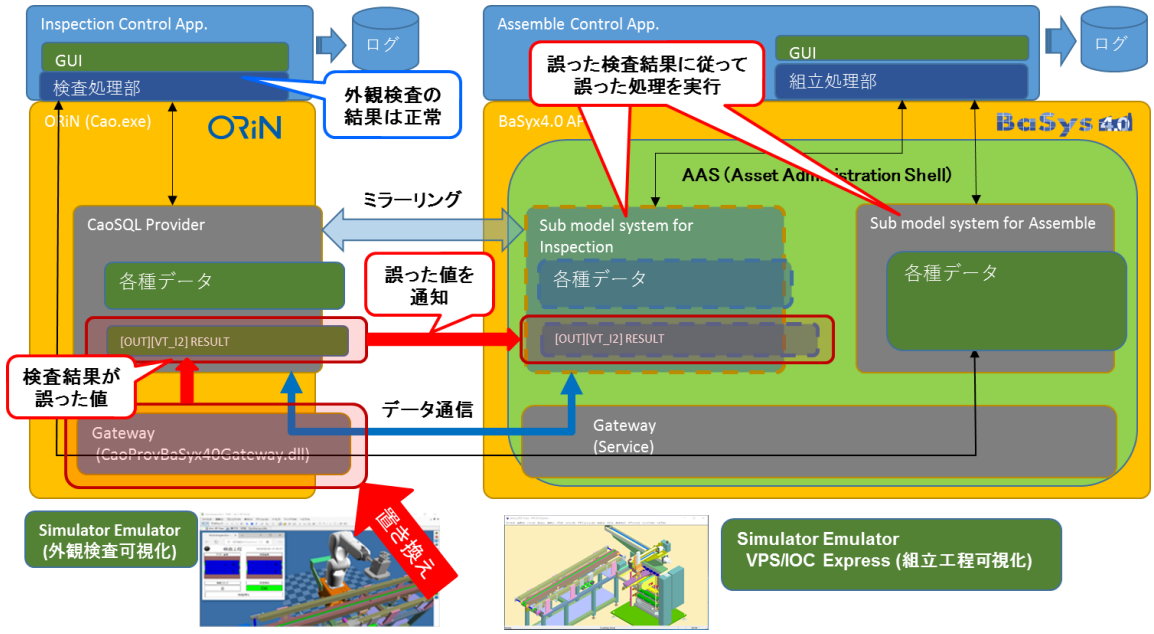


図 6-2 不正なモジュールによる置き換えと影響

この不正なライブラリファイルは、外観検査の結果を実際の結果とは異なる値にして BaSys 4.0 プラットフォームシステムに返す。BaSys 4.0 プラットフォームシステム側は、正しくない検査結果を受け取るため、不良品を正常品と判断したり、逆に正常品を不良品と判断してしまうことが発生する。

本 PoC では、不正なモジュールの動作結果をわかりやすくするために、実際の外観検査の結果に関わらず、常に不良を示す結果を BaSys 4.0 プラットフォームシステムに返すようにした。(図 6-3)

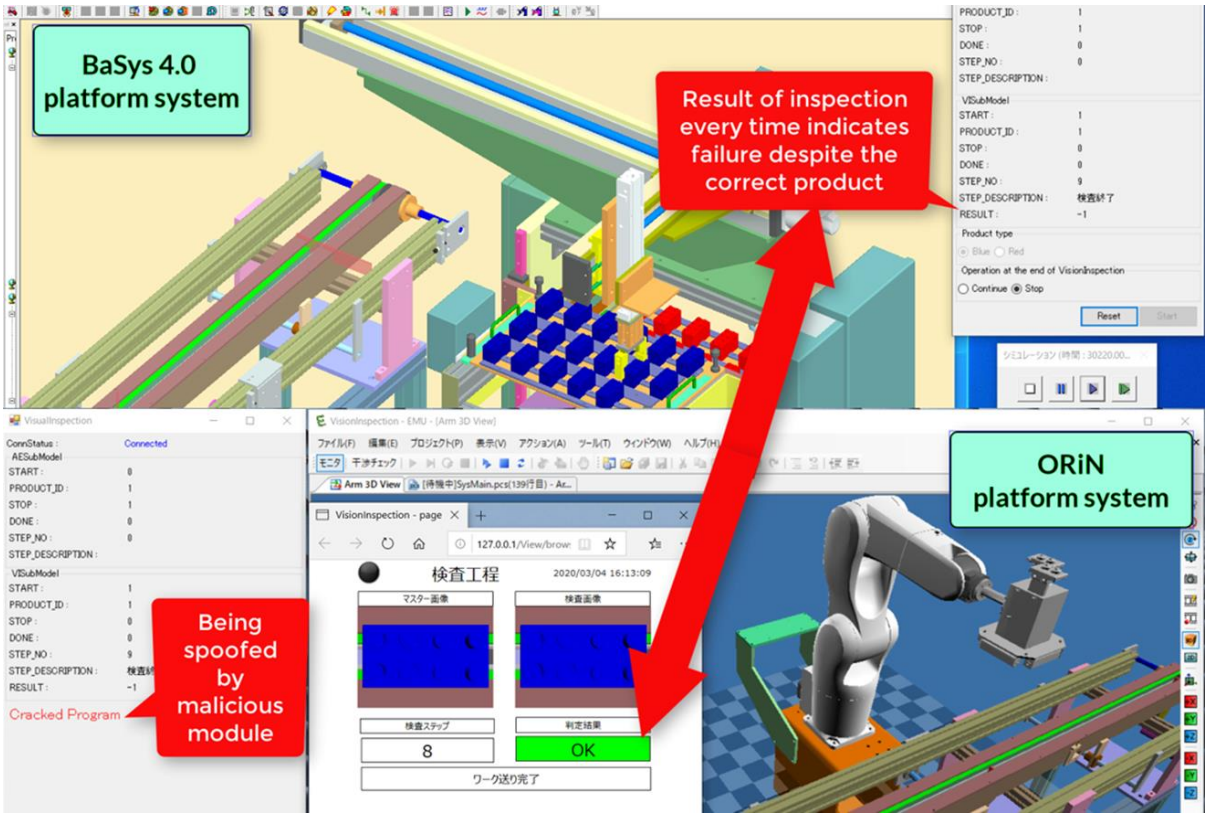


図 6-3 不正なモジュールにより検査結果とは異なる結果が返却される

6.2.2. 対策と効果

BaSys 4.0 プラットフォームシステムと ORiN プラットフォームシステムとのデータ通信は、それぞれの Gateway アプリケーションを経由して行う。それぞれの Gateway アプリケーションは、セキュアな通信環境を開設し、その中でデータのやりとりを行っている。

本 PoC では、各プラットフォームシステム毎に、そのセキュリティ対策のレベルを示す情報を組み込んだ信頼性情報をもつようにし、セキュアな通信環境を開設した直後に双方のプラットフォームシステムで接続相手の信頼性情報の真正性と内容を相互に確認した上で通信を開始する、という対策を実装した。信頼性情報は表 6-1 で示す内容とした。信頼性情報自体のなりすましも考えられるため、電子署名をつけて真正性の確認を行った。

表 6-1 PoC で実装した信頼性情報

項目種別	項目名	備考
モジュール情報	モジュール名	
	製品情報	製品名、VL情報、製品番号
	製造元情報	会社名、団体名 会社ID,団体ID
	製造年月日	YYYYMMDD
	…	…
信頼性情報	準拠プロトコル	プロトコル名
	公開鍵証明書のサブジェクトID	電子署名用公開鍵証明書のサブジェクトID
	脆弱性対策レベル	JVN/CVSS 対策状況を示す情報
	モジュール間の信頼性情報の確認	確認する／しない
	ロバスト性	耐タンパー性の内容 モジュール、データの正当性チェックの方法 モジュール、データの改ざん、破損検出時の処理
	セキュリティレベル	FIPS 140-2 対応状況
	認定情報	認定日時、有効期限
	失効	失効する単位（証明書の発行単位との関係）、失効ポリシー
	…	…
…		
電子署名情報	署名方式	暗号方式・暗号パラメタ・鍵長・ハッシュ方式・・・
	信頼性情報認定機関電子署名	認証局情報、信頼性情報認定機関公開鍵証明書、認定機関電子署名
	製造元電子署名	認証局情報、製造元公開鍵証明書、製造元電子署名
…		

接続先プラットフォームシステムの信頼性情報の内容を確認する機能は、それぞれのプラットフォームシステムの Gateway アプリケーションで実装した。攻撃の実装では、ORiN プラットフォームシステム上の Gateway アプリケーションのライブラリファイルを不正なライブラリファイルで置き換えた。（図 6-4）

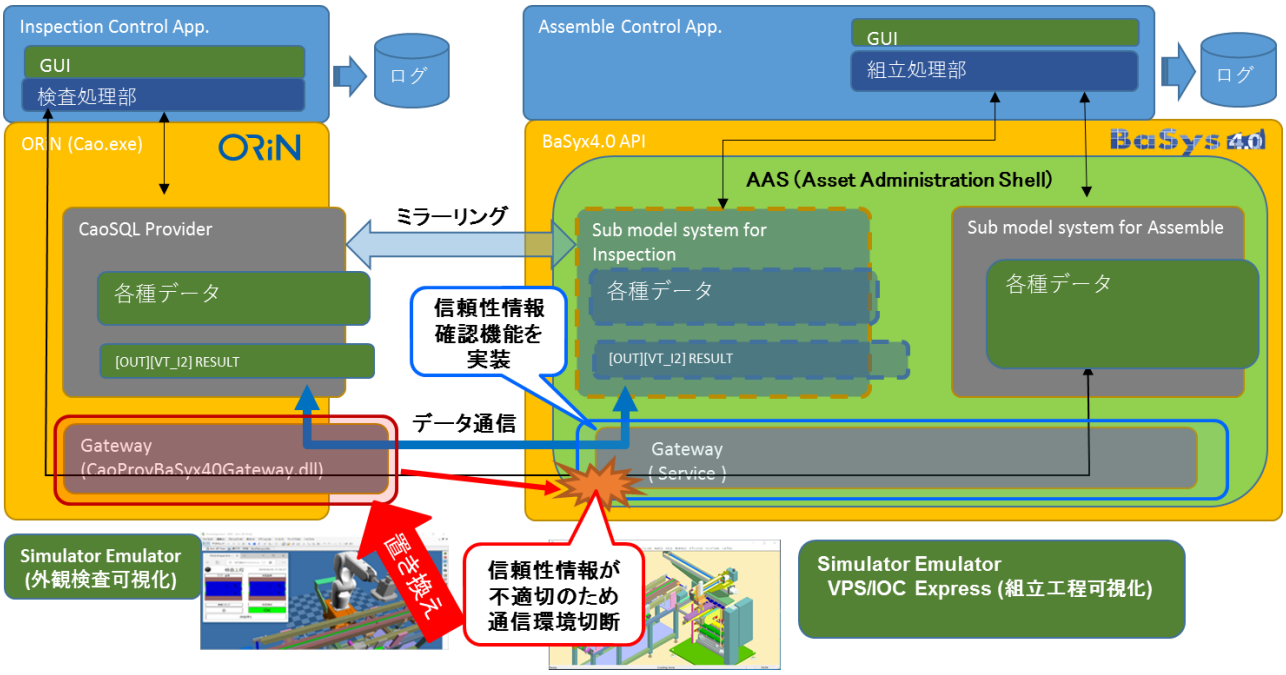


図 6-4 プラットフォーム間の信頼性情報の確認機能の実装

対策の効果の検証では、BaSys 4.0 プラットフォーム上の Gateway アプリケーションが ORiN プラットフォームから送られてきた信頼性情報が適切でないと判断し、開設した通信環境を切断することを確認した。また、これにより ORiN プラットフォーム側がエラーを出力することを確認した。(図 6-5～図 6-7)

① BaSys 4.0 プラットフォームシステム上で信頼性情報確認機能を起動

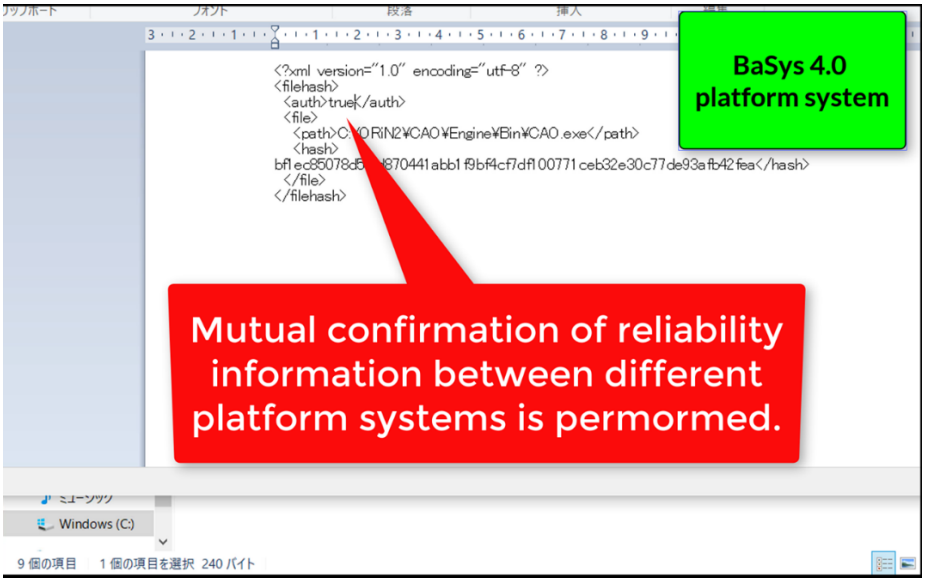


図 6-5 信頼性情報確認機能の有効化

② ORiN プラットフォームシステムから BaSys 4.0 プラットフォームシステムに接続

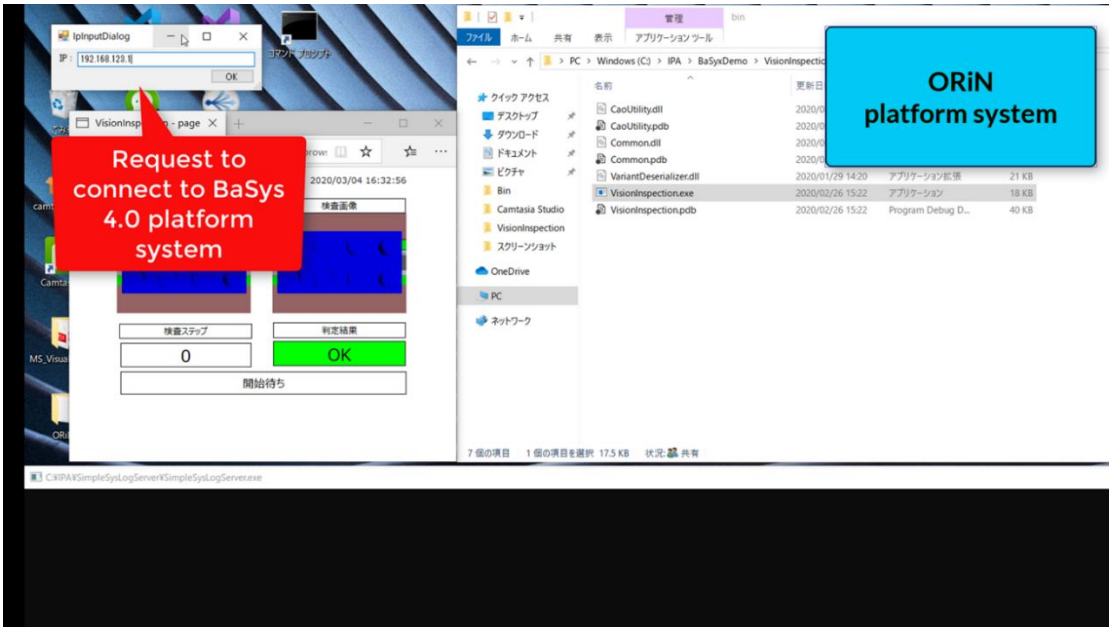


図 6-6 ORiN プラットフォームから BaSys 4.0 プラットフォームへの接続

③ BaSys 4.0 プラットフォームシステムが ORiN プラットフォームシステムからの接続要求を拒絶

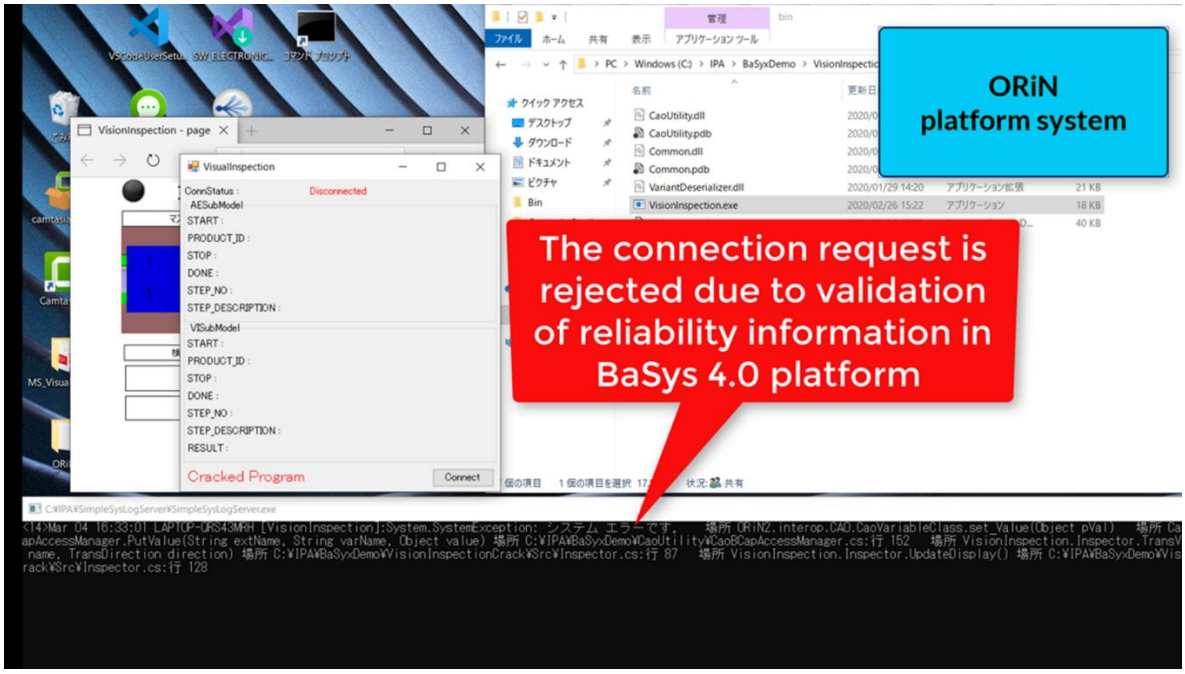


図 6-7 不正なモジュールからの接続要求を拒絶

6.2.3. 評価と考察

マルチプラットフォームシステムにおいては、一方のプラットフォームシステムのセキュリティレベル並びにロバスト性が高くても他方のプラットフォームシステムのセキュリティレベルが低い場合、セキュリティレベルの低いプラットフォームシステムが攻撃されて正しくない動作をするようになったとき、セキュリティレベルの高いプラットフォームシステムもその影響を受けて正常に動作しなくなるケースがある。本 PoC では、ORiN プラットフォームシステムが攻撃を受けてその結果製造物の検査結果として正しくない値が BaSys 4.0 プラットフォームシステムに返され、BaSys 4.0 システムの異常動作につながることを確認した。

また、本 PoC では、ORiN プラットフォームシステムから BaSys 4.0 プラットフォームシステムに接続要求を出したとき、BaSys 4.0 プラットフォームシステムが ORiN プラットフォームシステムから適切な信頼性情報が送られてこなかったために接続要求を拒絶し、通信環境を切断したことを確認した。これにより、ORiN プラットフォームシステム上の不正なモジュールの影響が BaSys 4.0 プラットフォームシステムに波及しないことを確認した。

現実には、セキュリティレベルの低いプラットフォームシステムはより多くのバリエーションの攻撃が有効となり、影響への対策でも多くの考慮事項が必要となる。それに対して、本 PoC で実装したように他のプラットフォームシステムと接続する前に、お互いに信頼性情報を確認し、適切な内容でないか、あるいは信頼性情報自体が送られてこなかった場合は通信環境を切断する、という対策は、悪影響のありそうなシステムとは接続しない、という点において有効な防御の対策といえる。

6.3. [対策 2] プラットフォームを跨いだアクセス制御

6.3.1. 攻撃の実装と影響

上記 “[対策1] プラットフォーム間の信頼性情報の確認” の対策が ORiN プラットフォームシステム並びに BaSys 4.0 プラットフォームシステムの Gateway アプリケーションで実装されている状態とする。つまり、ORiN プラットフォームシステムと BaSys 4.0 プラットフォームシステムとは、通信環境開設時に、相互に信頼性情報を確認する。

ORiN プラットフォームシステム上の Gateway アプリケーションの一部を改ざんして検査対象製造物の種別を示すデータに誤った値を設定するようにする。これにより、ORiN プラットフォームシステムの外観検査工程管理機能のミラーリング先である BaSys 4.0 プラットフォームシステム上のサブモデルも検査対象製造物の種別を示すデータに誤った値を設定する。(図 6-8)

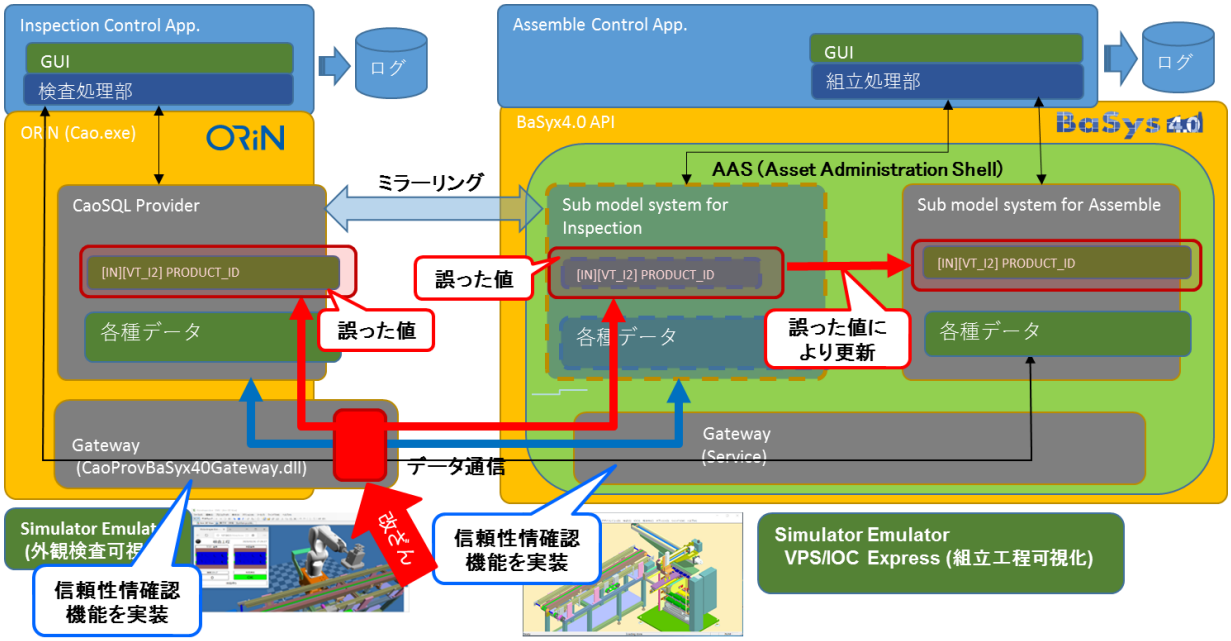


図 6-8 プログラムの一部を不正なコードにより改ざん

この攻撃により、BaSys 4.0 プラットフォームシステムから ORiN プラットフォームシステムに製造物の検査要求を出すとき、検査対象物の種別として誤った値が通知され、ORiN プラットフォームシステムは検査対象製造物を誤った種別の製造物として検査することになり、正しい検査が行われなくなってしまう。本 PoC では、プラットフォームシステム間の信頼性情報の相互確認ではこのモジュールやデータの一部改ざんといった高度な攻撃を防ぐことはできないことを示した。(図 6-9)

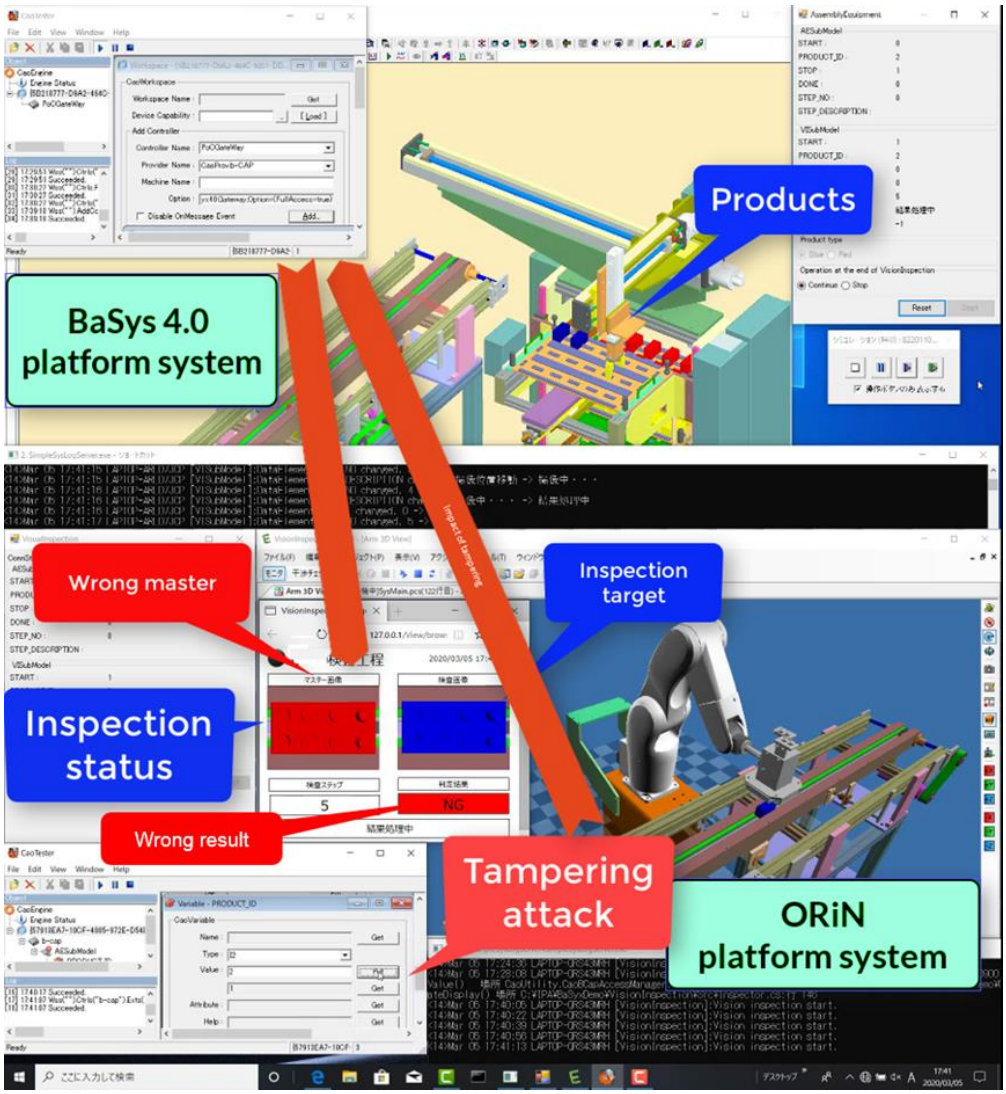


図 6-9 誤った種別に従った外観検査により誤った検査結果が出される

6.3.2. 対策と効果

マルチプラットフォームシステムにおいて、2つのプラットフォームシステムがレプリケーションを使ってデータを共有する場合、各データ毎に個々のプラットフォームシステムが可能なアクセス種別を限定することにより、接続している他のプラットフォームシステムからの不適切な影響を効果的に防ぐことができる。

本 PoC では、ORiN プラットフォームシステムの外観検査工程管理機能をミラーリングした機能を BaSys 4.0 プラットフォームシステム上で AAS のサブモデルとして実装し、オリジナルの機能とミラーリングされた機能との間で十分に短い時間間隔でデータを共有することにより、BaSys 4.0 プラットフォームシステムと ORiN プラットフォームシステムとを連携したマルチプラットフォームシステムを実現している。共有しているデータの中で、検査対象製造物の種別を示すデータ(PRODUCT_ID)は、外観検査を依頼する BaSys 4.0 プラットフォームシステムが更新するデータであり、外観検査を行う ORiN プラットフォームシステムは参照するのみで更新はしない。そのため、BaSys 4.0 プラットフォームシステム上

の Gateway アプリケーションで、共有データに対するアクセス制御機能を実装し、検査対象製造物の種別を示すデータについては、BaSys 4.0 プラットフォームシステム内部からの更新要求に対してはアクセスを許可し、ORiN プラットフォームシステムからは参照要求のみを許可、更新要求は拒絶するようにした。

PoC で実装したアクセス制御機能の定義情報を表 6-2 に示す。

表 6-2 PoC で実装したアクセス制御機能の定義情報

項目種別	項目名	説明
アクセス対象情報	対象の種別	ファイル、データ
	ファイル名	種別がファイルの場合
	データオブジェクトID	種別がデータの場合
	内容の説明	ファイル、データの内容
	…	…
アクセス主体情報	アクセス主体ID	コンポーネントの公開鍵証明書ID（サブジェクト名）
	コンポーネント名	上記公開鍵証明書の発行先コンポーネントの名前
	製品名	コンポーネントの属する製品名
	…	…
アクセス方法	実行可能な指示タイプ（動作／状態参照／…）	種別が機器に対応するプロバイダの場合
	可能なアクセスタイプ（参照／更新…）	種別がデータの場合
…		
電子署名情報	署名方式	暗号方式・暗号パラメタ・鍵長・ハッシュ方式…
	アクセス制御情報管理元の電子署名	PoCではb-CAP Server の秘密鍵で作成した電子署名
	…	…
…		

アクセス制御機能の動作の概要を図 6-10 に示す。

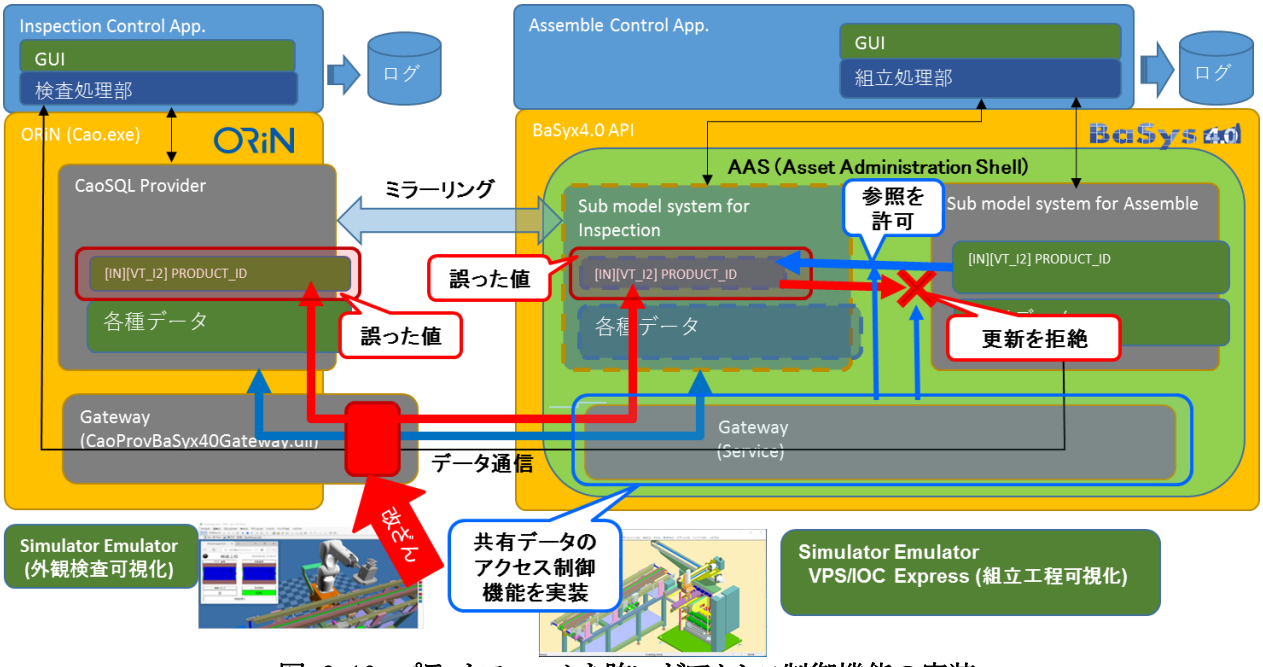


図 6-10 プラットフォームを跨いだアクセス制御機能の実装

このアクセス制御機能を実装したところ、ORiN プラットフォームシステム上の不正なコードで改ざんされたモジュールから、検査対象製造物の種別に対応するデータの更新依頼が出されても、その更新処理が BaSys 4.0 プラットフォーム上で実装したアクセス制御機能により拒絶され、PoC システムが正常に動作し続けることを確認した。(図 6-11)

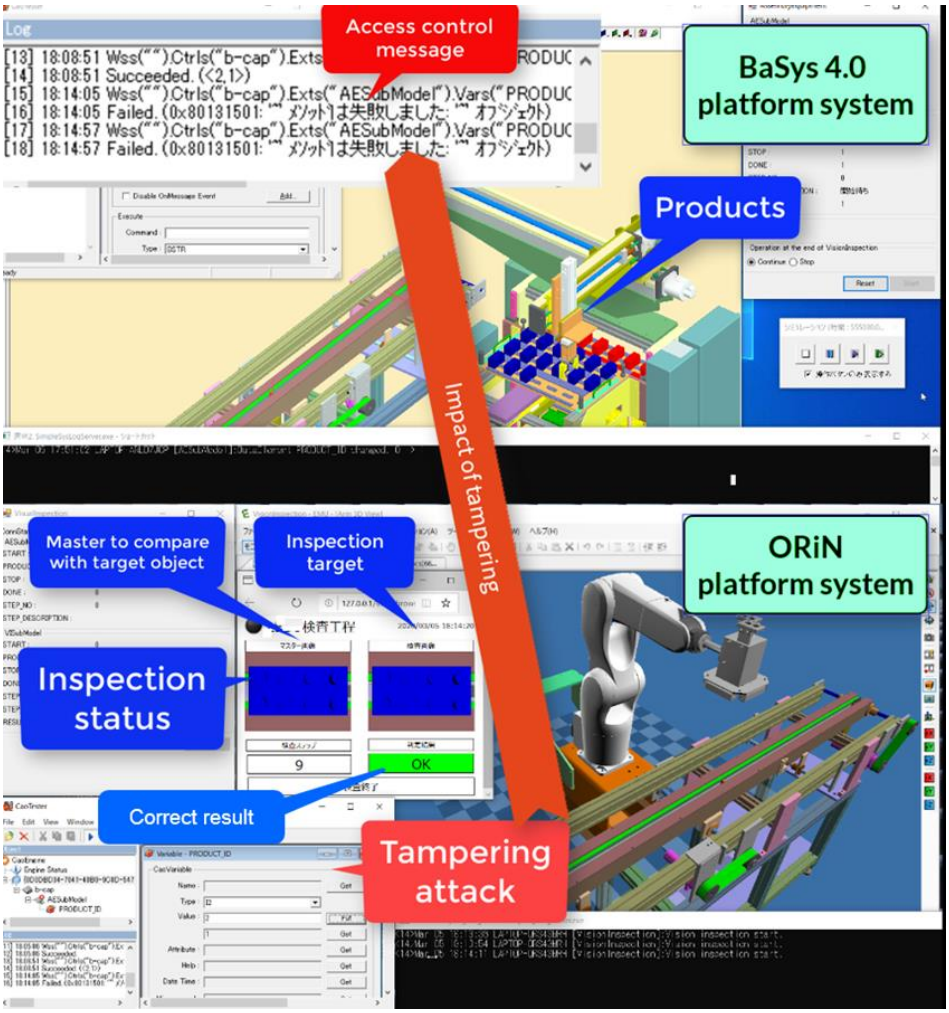


図 6-11 プラットフォームを跨いだアクセス制御機能により共用データの不正な更新を拒絶

6.3.3. 評価と考察

マルチプラットフォームシステムにおいて、不正なモジュールやデータがプラットフォームシステム内に侵入することを防ぐにあたっては、プラットフォームシステム間の信頼性情報の確認による対策が有効であり、本 PoC でもその効果を示した。ただし、本書“4.3 攻撃への対策” でも記載したように、不正なモジュールやデータの侵入を防ぐ対策をすり抜けてくる高度な技術をもった攻撃が生み出される可能性が懸念される。本 PoC では、プラットフォーム間の信頼性情報の確認による対策をすり抜けてくる高度な攻撃を想定した環境を実装し、プラットフォームを跨いだアクセス制御機能が、その攻撃の影響を抑止する効果をもつことを確認した。

7. おわりに

製造システムの分野でのデータ活用を目的としていくつかのプラットフォーム仕様が考案・実装され、現実のシステムで利用されつつある。そして、複数のプラットフォームを連携したシステムが必要になってくると予想されるが、異なる仕様のプラットフォームを連携した製造システムの例はまだ少ないようである。本 PoC では、この状況に先駆けて独 Fraunhofer IESE が開発しているプラットフォームである BaSys 4.0 と、日本の ORiN 協議会が仕様公開しているプラットフォームである ORiN とを連携したシステムを実装し、このマルチプラットフォームシステムにおいて想定される懸念事項と脅威に対する以下の対策の効果を確認した。

［対策1］ プラットフォーム間の信頼性情報確認

［対策2］ プラットフォームを跨いだアクセス制御

本書では、マルチプラットフォームシステムでの脅威・攻撃・被害の分析と対策の考え方として、「一方のプラットフォームシステムの脆弱性の他方のプラットフォームシステムへの影響の考慮」並びに「攻撃要因の侵入の抑止と攻撃の影響の抑止」について示した。そして、PoC で構築したマルチプラットフォームシステム上で実行した攻撃の影響と対策の効果について確認した結果を示した。これらが、マルチプラットフォームシステムを実現する際の考慮事項として、また、プラットフォーム実装時の要件として、参考となることを期待する。

なお、本 PoC においては、BaSys 4.0 プラットフォームシステムと ORiN プラットフォームシステムを連携したマルチプラットフォームシステムの実施例として、データの高速レプリケーションによるミラーリングを使った方式を示した。製造システムで導入されるネットワークの高速化とコンピュータの処理能力の高速化に伴い、TSN (Time Sensitive Network) の活用が進み、異なるプラットフォーム間での制御連携もリアルタイム性が要求されていくことが予想される。これに伴い、プラットフォームシステム間の連携は、ミラーリングを活用した方式も使われていくようになると考えられ、本 PoC で示したシステムと対策の実装例は、今後マルチプラットフォーム連携システムにおいて、有効性が増していくものと考える。

プラットフォーム間のセキュリティ対策を含めた連携の仕様が実システムで展開されていくケースとしては、特定の実施例での連携仕様が実績を通して汎用化されていくケースと、国家プロジェクトで標準仕様を作成し、その実装を推進していくケース[18]とが考えられる。セキュリティ対策を含めた連携仕様の展開に関する取り組みについては、今後の課題としたい。

18 製造システムのセキュリティの標準仕様の作成と実装の推進を国家プロジェクトで進めている例としては、独の IUNO(National Reference Project IT Security in Industrie 4.0)がある。詳細は以下の URL を参照されたい。
https://www.dik.tu-darmstadt.de/forschung_dik/projekte/abgeschlosseneprojekte/iuno/inhalt_mit_marginalienspalte_125.en.jsp

謝辞

本 PoC（概念実証）の実施にあたり、ご協力いただいた皆様に心から謝意を表する。

本 PoC システムは、独 Fraunhofer IESE、ORiN 協議会と協同で実施したが、システムを開発するにあたり、特に ORiN 協議会の以下の会員企業様からご協力をいただき、ソフトウェア資材を貸与いただいたことをここに記す。

・組み立て工程 CELL

シミュレータ（富士通製 VPS） : デジタルプロセス株式会社

エミュレータ : 株式会社デンソーウェーブ

各種産業用機器 3D データ : 同上

・検査工程 CELL

シミュレータ : 株式会社デンソーウェーブ

エミュレータ : 同上

各種産業用機器 3D データ : 同上

IPA 関係者一同

ORiN 協議会 関係者一同

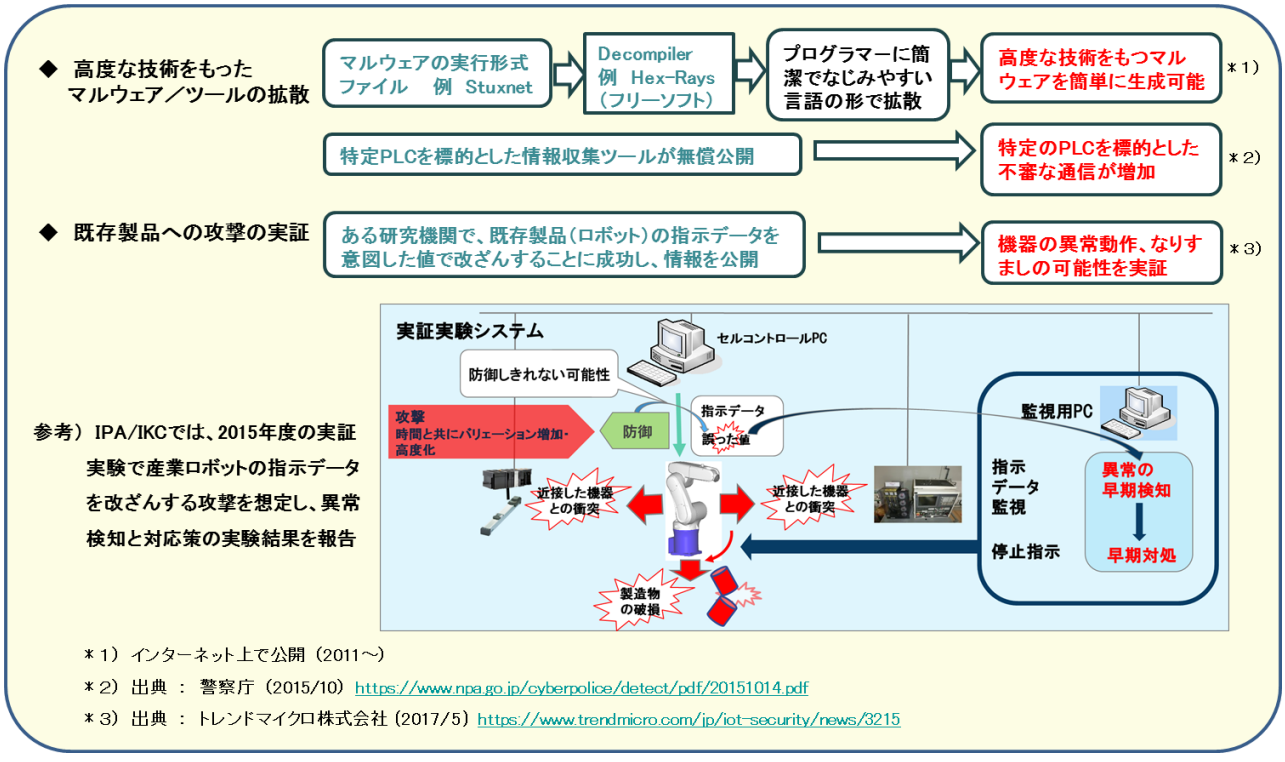
Fraunhofer IESE 関係者一同

付録 A. 製造システムをターゲットにしたセキュリティ脅威の増大

高度なマルウェアを作成するのに利用可能なソースコードやツールがインターネット上で公開されており、不特定多数の人々が比較的簡単に高度なマルウェアを開発可能な状況となっている。

- 多額の費用を使って作成された高度なマルウェア（APT：Advanced Persistent Threats）のバイナリコードが、フリーのデコンパイラ（Hex-Rays）によりソースコード化されたものが、インターネット上で公開されている。
- 特定の PLC(Programmable Logic Controller)を標的とした情報収集ツールがインターネット上で無償公開され、その直後から、その PLC を狙ったとみられる不審な通信がインターネット上で増加したことが観測されている。

IPA 社会基盤センターでは産業ロボットの指示データを改ざんする攻撃の出現を想定し、その脅威に対して異常検知と対応策の実証実験を実施し、結果を公開[19]したが、その後、ある研究機関は、実際に製品として流通している産業用機器の指示データを改ざんする攻撃が可能であることを実験で実証し、その結果を公開[20]している。



＊1）インターネット上で公開（2011～）

＊2）出典 ： 警察庁（2015/10）https://www.npa.go.jp/cyberpolice/detect/pdf/20151014.pdf

＊3）出典 ： トレンドマイクロ株式会社（2017/5）https://www.trendmicro.com/jp/iot-security/news/3215

19 IPA の以下の URL で公開
https://www.ipa.go.jp/sec/reports/20170531.html

20 トレンドマイクロ株式会社の以下の URL で公開 （2020 年 6 月現在）
https://www.trendmicro.com/jp/iot-security/news/3215

付録 B. 実際の製造システムで発生したセキュリティインシデント

製造システムは、サプライチェーンを効率的に管理するために、情報システムと必要に応じて接続するケースがあり、そのとき、情報システムから製造システムにマルウェアが侵入し、被害が発生したケースが報告されている。また、製造システムでの作業者が、主に製造システムのメンテナンスを目的として作業用の PC や USB メモリを製造システムに接続するケースがあり、それらの PC や USB メモリからマルウェアに感染して被害が発生しているケースも報告されている。