プログラム名：社会リスクを低減する超ビッグデータプラットフォーム
PM 名：　　原田　博司
プロジェクト名：ファクトリセキュリティ

委 託 研 究 開 発

実 施 状 況 報 告 書（成果）

平成２８年度

研究開発課題名：

つながる工場シミュレーターおよび故障・攻撃検知アルゴリズムに関する研究開発

研究開発機関名：

三菱電機株式会社

研究開発責任者
米田　健

Ⅰ　当該年度における計画と成果

１．当該年度の担当研究開発課題の目標と計画

本研究開発では、工場の健全性維持と生産性向上の実現に向け耐故障・攻撃性を備えた超高精度工場機器稼働推計による「つながる工場」シミュレータを用いて「つながる工場」の健全性をリアルタイムに分析し，サイバー攻撃を一網打尽に捉える全く新しいシステムの開発を行う。平成 28 年度の計画と目標は以下の通りである。

１．つながる工場シミュレータ

平成 28 年度は 10 台規模のロボットで構成されるマスカスタム生産工場のシミュレーションを行う事を目標とする。その実現に向け、実プロト工場の設計・構築を通じて生産工場のモデル(設備構成や設備の制御方式)を検討し、同モデルに基づいてシミュレータのプロトタイプ開発を実施する。

2.、サイバー攻撃検知

平成 28 年度は攻撃検知にターゲットを絞り、アルゴリズムの基本設計及び試作を行う事を目標とする。その実現に向け、上述の生産工場のモデルから、想定される攻撃の分析と通信プロトコルの分析を行い、同結果をもとにアルゴリズムの検討及び試作を行う。また、試作した検知システムの有効性を実証するため、工場の動きを模倣する工場エミュレータと、同エミュレータ上で攻撃を再現する攻撃ツールの開発を行う。

２．当該年度の担当研究開発課題の進捗状況と成果

2-1 進捗状況

1.　つながる工場シミュレータ

今後の高齢化社会でニーズの高まるオーダメイドケア食弁当生産をターゲットとし、実プロト工場の設計・構築を通じた生産工場モデルの検討を実施した。その後同モデルに基づいてシミュレータの開発を実施した。シミュレータへ入力された生産計画から、適切な設備稼働スケジュールを導出するアルゴリズムの検討・試作は共同開発者である神戸大学が実施し、生成されたスケジュールに従って、設備への制御命令をシミュレートする部分の検討・試作を三菱電機が実施した。

2.　サイバー攻撃検知

生産工場のモデルから想定される攻撃の分析を行い、平成 28 年度ではコマンド改ざんにより、利用者の健康被害を引き起こすケア食弁当を製造させる攻撃を検知することを目標とした。その後、生産工場モデルの検討で得られた通信プロトコルを前提とし、コマンド改ざん攻撃を検出する攻撃検知アルゴリズムの検討と試作を実施した。また、工場エミュレータ及び同エミュレータ上でコマンド改ざん攻撃を再現する攻撃ツールを開発した。さらに、PM からの要請により、広く世の中の要件・要望等の意見を収集してファクトリセキュリティに関する知見を効率的に取得するためのツールとして、本事業の一環でプロモーションビデオを追加作成した。なお、工場エミュレータ開発は、工場のものの流れや攻撃の様子を可視化する仕様の策定が当初想定以上に時間を要したため、開発は年度を繰り越し 4 月末完成となった。その際、外注による開発を 3 月と 4 月の 2 段階に分け、ステップバイステップで検証することにより効率的に開発を進めるようにした。

2-2 成果

1. つながる工場シミュレータ

オーダメイドケア食弁当生産においては、顧客による嗜好のバリエーションが多様であり、それに対応して製造する種類やその製造にかかる時間が多様である事から、フレキシブルジョブショップ型の工場が適切であるとの結論に達した。また、同工場においては、多種多様な弁当が、有限の製造装置をスケジュールに従って共有しながら同時に複数生産される。そのため時間ベースで定められたスケジュールに基づいた製造装置制御では、ある工程の失敗・遅延の影響が他の弁当の製造工程に伝播してしまい、最悪の場合には弁当生産のスケジュールが破たんしてしまう恐れがある。そこで、そのような失敗や遅延の影響が他の弁当製造に伝播することを最小限とするため、スケジューラから渡された時間ベースの

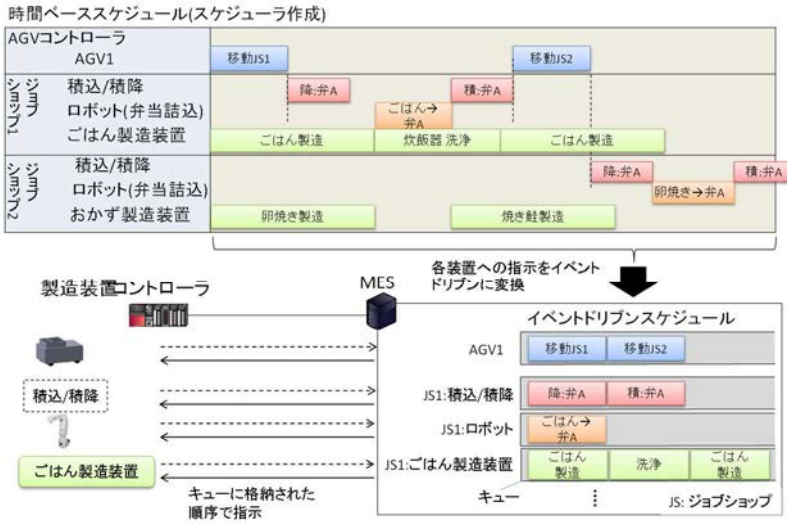

Figure 1 イベントドリブンベースの通信方式

スケジュールをイベントドリブンベースのスケジュールに変換、装置が空き状態になった時点で次の製造コマンドを与える通信方式を得た(Figure 1)。

以上の検討により得られた設備構成及び通信方式に基づき、スケジューラの生成したスケジュールに従って動作する MES シミュレータ及び製造装置コントローラシミュレータを試作、各シミュレータ間で実際の MES 及び製造装置コントローラと同様の製造コマンドを通信するつながる工場シミュレータを得た。

2. サイバー攻撃検知

イベントドリブンベースのスケジュールを適用することにより、工場内のネットワークを流れる制御コマンドは、工程遅延等によりシミュレータの出力結果とずれが発生する可能性がある。そのようなずれに対し耐性をもつ検知アルゴリズムとするため、シミュレータの予測した制御コマンド列を、宛先となる製造装置毎に分類し、各製造装置に対して発生するコマンドが、予測した通りの順序に従っているかを確認することによる検知方式を開発した(Figure 2)。

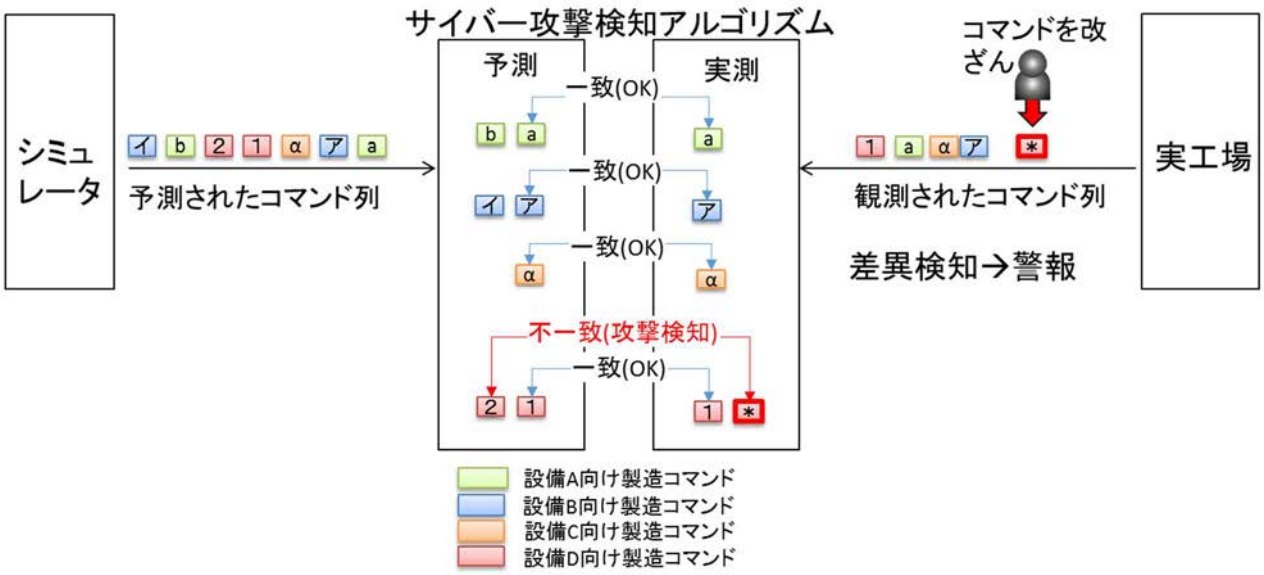

Figure 2 サイバー攻撃検知アルゴリズム

2-3 新たな課題など

故障等の障害発生時のリカバリーを行うには製造スケジュールの再スケジューリングが必要であるが、今回の開発を通じ、スケジューラによる再スケジューリングは時間がかかるため、障害が発生する度に製造を中断しスケジューラで再スケジュールされるのを待って再開するのは現実的ではないという知見を得た。この課題に対し、一旦は MES のレベルで製造を継続するために最低限必要な再スケジュールを行い、製造を継続しつつ、スケジューラでより最適な再スケジュールを生成する階層型のスケジューリング方式に取り組む。

その際、サイバー攻撃検知アルゴリズムも故障等で再スケジュールが発生したことを検出し、MES やスケジューラからの情報を基に、予測コマンド列を修正する必要がある。そのためのインタフェースと予測コマンド列の修正方法について取り組んでいく。

3．アウトリーチ活動報告

無し