スマート工場をセキュリティ脅威から守る DX with Cybersecurity

事業創生や生産改革のためにDXの一環としてスマート工場の整備が加速している。一方，運用やマネジメントを含めた制御システムにおいても，ネットワークの連携やオープン技術の活用などによりサイバーセキュリティの脅威が顕在化している。スマート工場を整備するためには，外部ネットワークとの連携，さらにはクラウドサービスの活用やサプライチェーンの確立などが必要になりつつあり，今まで以上にセキュリティ脅威への対応が必要となっている。

本稿では，日立のスマート工場構築の経験を生かした，セキュリティの確保されたDX推進を支えるソリューションについて紹介する。

亀田 貴之 | Kameda Takayuki
山田 勉 | Yamada Tsutomu
山口 耕平 | Yamaguchi Kohei

1. はじめに

製造事業者は魅力ある製品・サービスを提供することに加え，複雑化する製品・サービスの品質の維持・向上を合わせた対応も求められる。近年では，DX（デジタルトランスフォーメーション）により企業変革を進める例も増えている1)。一方，DX推進に伴い，セキュリティについても新たな考え方が必要になってきた。

本稿では，スマート工場化の例と，そこで必要になるセキュリティのコンセプト，セキュリティソリューションの例，製造業の将来に向けたセキュリティの提言を述べる。

2. 製造業におけるDX

製造業におけるDXでは，現場のデータの活用や，ビジネスの変革に追従する制御システムの実現が必要である。さらに現場システムと社内外のシステムとの連携，汎用IT機器・サービスの活用などが不可欠になる。これらを実現するために，スマート工場化が注目されている。

2.1
CPS

スマート工場と関連した概念としてCPS（Cyber Physical System）がある。CPSとは，現実世界（フィジカル空間）の情報を収集し，サイバー空間に集めて分析し，そこで得られた情報や価値を現実世界へフィードバックして課題を解決するシステムである2)。サイバー空間とフィジカル空間が高度に融合することで，必要な人へ必要な時に必要なモノやサービスを提供できるようになる。

CPSにおけるセキュリティについては，経済産業省のサイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）が解決のヒントを示している3)。CPSFにお

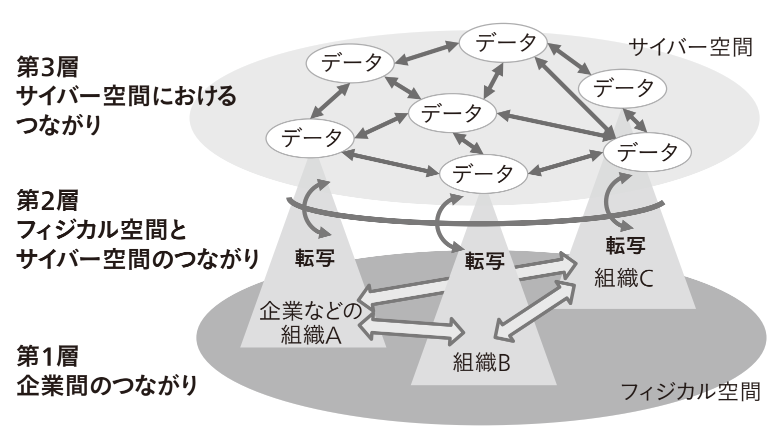
いて示される現場とサービスのつながりを**図1**に示す。CPSFは，マネジメントの信頼性を確保した企業と企業外のつながりを第1層，フィジカル空間とサイバー空間の間でデータを転写する第2層と，信頼あるデータを流通・加工・管理するサイバー空間のつながりを第3層と定義している。

CPSFにおいては，サイバー空間からの攻撃がフィジカル空間まで到達しやすくなる点や，複雑なサプライチェーンのつながりによりサイバーインシデントの影響範囲が拡大する点が懸念として挙がっている。

2.2

スマート工場の構成例

スマート工場の一例として，日立製作所大みか事業所の生産ラインにおける生産管理システムを**図2**に示す[4)]。物理空間にある作業者による進捗やモノの流れを収集し，サイバー空間において生産現場全体の動態をリアルタイムに俯瞰できる進捗・稼働監視システムを構築している。また，設計工程の効率向上や工場シミュレータによる生産計画の精度向上などを実現し，高効率生産モデルを確立している。



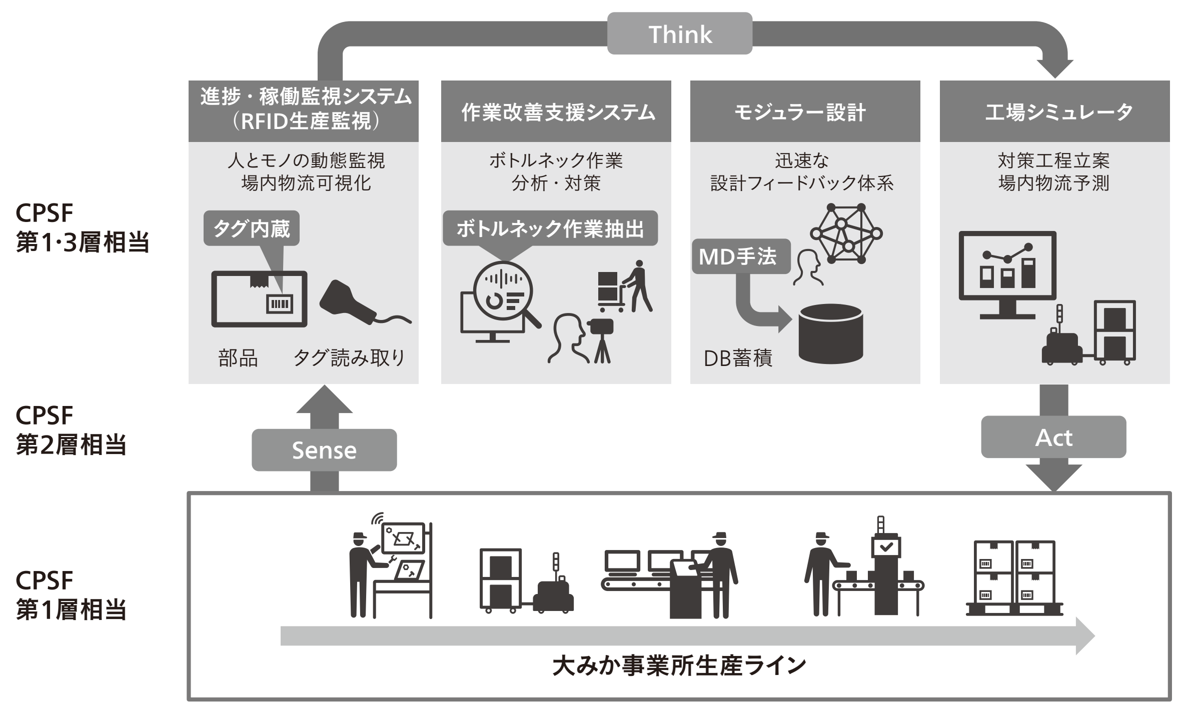
注：本図は，経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク」を参考に日立で加筆したものである。

図1｜**CPSFのイメージ図**

Society 5.0における産業社会を三つの層に整理し，セキュリティ確保のための信頼性の基点を明確化した，CPSF（Cyber Physical Security Framework）三層構造モデルを示す。

図2｜**スマート工場の例**

RFID生産監視と作業改善支援，モジュラー設計，工場シミュレータを連携させて，人・モノ・設備情報をサイバー・フィジカル間で活用する高効率生産モデルを確立した。



注：略語説明
RFID（Radio Frequency Identifier），MD（Modular Design），DB（Database）

2.3
スマート工場の課題

製造業における制御システムの目的は，事業継続性（BC：Business Continuity）の視点から，製品の生産や供給を計画されたSQDC［Safety（安全），Quality（品質），Delivery（生産計画），Cost（コスト）］を確保して提供することにある。これらの目的に対して，セキュリティインシデントはBC+SQDCを混乱させる業務障害要因の一つに位置づけられる。

これまでBC+SQDCを維持してきた装置やシステムであっても，スマート工場化に際して構成を変える場合には，信頼できるということを前提にしてきた範囲を見直す必要がある。すなわち製造事業者がコントロールできていた範囲が変化することになる。例えば，従来の制御システムは設計時に仕様が確定し，システム設置以降は構成も利用形態も変化させることはほとんどなかった。しかし，スマート工場においては次に示す新たな利用形態の広がりが予想される（**図3**参照）。

（1）ITシステム連携

例えば，生産の合理化のために，必要に応じて制御システムが業務システムやエンジニアリングシステムと連携する。

（2）外部システム連携

サーバ資産や既製サービスを柔軟にどこからでも利用するために，クラウドシステムなどの外部システムと接続する。

（3）市中での利用（端末）

遠隔保守などのために，タブレット端末を利用して工場以外の場所から現場状況を監視する。

スマート工場では，従来のような境界内の通信相手を一律信用する境界防御から考え方を見直し，さまざまな環境変化を想定した制御システムの構成とセキュリティ対応が必要になる。

3. スマート工場セキュリティ

3.1
スマート工場のセキュア化に必要な考え

事業継続と安全・品質（BC+SQDC）などを確保しつつ，オープン技術を活用してDX化するスマート工場では，新たな利用形態（ITシステム連携，外部システム連携，市中での利用）を取り入れる将来像が予想される。そこでは，「機密性，完全性，可用性」や「健康，安全，環境保護」といった従来のセキュリティの考え方に加え，次に示す性質を守る必要があると考える。

（1）真正性（Authenticity）

通信相手が意図した相手であり，通信内容が正しい内容であること。例えば，外部サービスの利用時になりすましの脅威から守るために必要である。

（2）信頼性（Reliability）

通信相手が，一貫して意図したとおりに実行する（意図しない実行をしない）こと。例えば，外部サービスの提供するサービス内容は期待している品質を維持されている必要がある。

（3）保護性（Protectiveness）

通信相手の装置や通信情報に対するセキュリティ脅威に対応した施策が必要である。例えば，リスク分析により必要と判明した防御策や検知策を備えることである。

DX化するスマート工場において，将来を見据えてセ

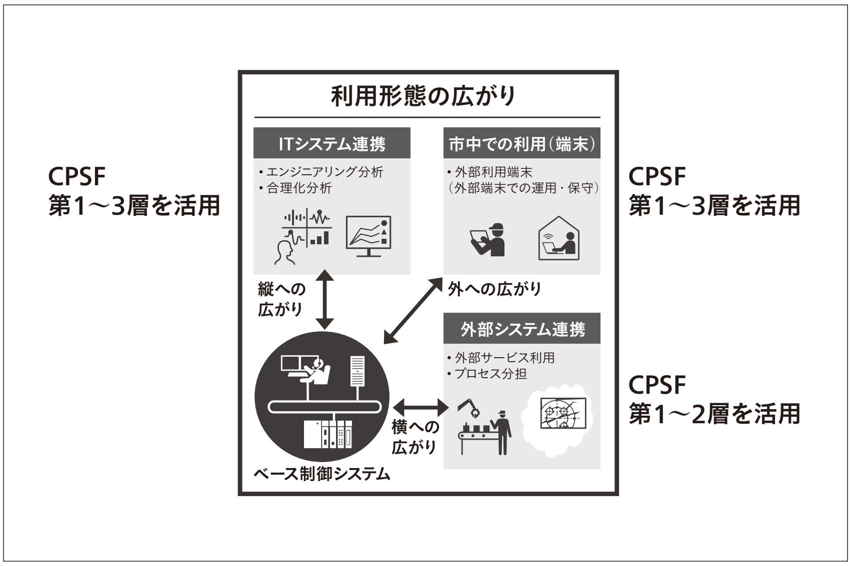


図3｜DXに向けた利用形態の広がり

DXに向けてセキュリティを考慮する際には，従来のような固定的な連携だけではなく，ITシステム連携や外部システム連携，市中での利用など利用形態の広がりを想定した対策が必要となる。

キュリティを保つには，これらARP（Authenticity, Reliability, Protectiveness）の性質を実装および維持することが重要である。

3.2
スマート工場のセキュリティ対応策の例

真正性を保つには，なりすましを防ぐ認証技術が対応策の候補である。例えば，知識による認証，所有による認証，生体による認証などから二つ以上を使った多要素認証が有効である。また，信頼性を保つ候補として，例えば装置が標準規格に適合していることを示す規格認証が当てはまる。保護性については，情報の暗号化や装置の物理的保護などが候補である。ただし制御システムとしての要件に対する考慮が必要と考える。

4. セキュリティを支える日立のソリューション

これまで日立は，セキュリティの視点，制御システムの視点を融合したソリューションを提供してきた。また，スマート工場化に伴い，3.1節で示したような新たな課題を解決するためのDX化対応セキュリティソリューションを提供している（**表1**参照）。

4.1
戦略立案

事業改革や生産改革に合わせてこれらを支えるシステムの整備を，DXを活用して進める必要がある。この事業改革や生産改革は広範囲にかつ継続的に行われるため，個別システムごとに実施策を検討すると施策に過不足が発生する場合がある。

戦略立案ソリューションでは，DXを活用した制御システムの整備に対して，セキュリティや制御システムとして満足すべき要件を整理し，スマート工場実現のために必要なセキュリティ戦略を提供する。

4.2
現状把握・施策立案

現状把握・施策立案ソリューションは，スマート工場として実現したい内容（**図3**参照）に併せて現状のシステムや運用，問題が発生した時の対応についてマネジメント視点で現状を調査し，リスクや課題を抽出する。その結果に基づき，スマート工場として実現したい内容に対して制御システムの視点を考慮した形で必要になるセキュリティ施策を立案する。

DX向けセキュリティとして，なりすましなどの脅威に対し，真正性や信頼性，保護性をこの時点で考慮することが重要である。

4.3
システム構築

DXを活用したスマート工場を実現する制御システムにおいて，セキュリティを確保するための実現策について設計から実装までを支援する。

DXを活用したスマート工場では多様な機器がネットワークにダイナミックに接続される。日立はこの接続における真正性を統制・管理する機能，および信頼性や保護性を支援する機能を「NX NetMonitorシリーズ」として提供する（**表2**参照）。

4.4
運用支援

制御システムに発生するセキュリティインシデントは装置や機能の異常（アラーム）として検出されることが多い。運用支援では，このアラームが発生する要因がセキュリティに起因する異常なのか，機器故障などの通常の異常なのかの判断を支援するソリューションを提供する。

表1｜DX化対応セキュリティソリューションの一覧
従来のセキュリティソリューションに加え，DX化に対応して取り揃えたセキュリティ対応策の一覧を示す。

区分	ソリューション
戦略立案	DX対応セキュリティ戦略立案
現状把握・施策立案	目的別DXに向けた現状把握，リスク分析
	目的別DXセキュリティ計画立案
システム構築	DX対応セキュリティシステム構築支援
	制御向けセキュリティ装置・パッケージ提供
運用支援	アラート統合（制御・セキュリティ）監視
人財育成	DXに必要な「プラス・セキュリティ」人財育成
	DXインシデント対応訓練（セキュリティ＋制御）

表2｜NX NetMonitorシリーズの機能一覧

DXを活用したスマート工場において，セキュリティを確保するための機能一覧を示す。

機能		概要	ツール名
装置の真正性の統制・管理		・不正装置のネットワークへの接続検出 ・不正装置の排除	アプライアンス
通信の真正性の統制・管理		・ネットワークの通信を監視 ・不正な通信を検出・通知	IDS
運用支援	機器情報分析（保護性支援）	・機器の物理的な接続場所（スイッチングハブ物理ポート），オープン論理ポートを特定	Crawler
	統合管理（信頼性支援）	・上記機能を統合管理 ・他のシステムへの通知	Manager

注：略語説明
IDS（Intrusion Detection System）

4.5
人財育成

日立は，「NX Security Training Arena」としてサイバーセキュリティ訓練施設を活用したセキュリティ人財育成を実施している。これからのDXを推進するうえで必要になる「プラス・セキュリティ」人財の育成について，「（制御システム×DX）＋セキュリティ」の視点を網羅した人財育成教育および訓練を提供する。

5. おわりに

本稿では，スマート工場化の背景を示し，その概念としてCPSについて説明した。さらに，スマート工場化に伴い発生する脅威や，それに対処するためのセキュリティソリューションを紹介した。

スマート工場化により，製品やサービスの価値を高めるための生産の変更に対応しやすくなる。また，遠隔地の工場の保守にもリモートで対応でき，働き方を変えることが可能になる。

一方でスマート工場化により，さまざまな人とモノがさまざまな情報を工場の内外でやり取りするようになり，サイバーインシデントの可能性は高まる。

今後ますます進展していくスマート工場のセキュリティを支えるには，情報のやり取りが意図したものであるかを都度検証していく仕組みが必要になる。日立は，セキュリティ方針のコンサルティング，セキュリティコンポーネントの提供やシステム構築により，顧客のスマート工場化実現を全面的に支援していく。

参考文献など

1）経済産業省，デジタルトランスフォーメーションを推進するためのガイドライン（DX推進ガイドライン）Ver. 1.0（2018.12），
https://www.meti.go.jp/press/2018/12/20181212004/20181212004-1.pdf
2）日立製作所，Cyber-physical system（CPS），
https://www.hitachi.com/rd/glossary/c/cyber_physical_system.html
3）経済産業省，サイバー・フィジカル・セキュリティ対策フレームワーク Ver1.0（2019.4），
https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf
4）日立製作所，生産現場の全体最適化，
https://www.hitachi.co.jp/products/it/lumada/cs/00008/index.html

執筆者紹介

亀田 貴之
日立製作所 サービス&プラットフォームビジネスユニット
制御プラットフォーム統括本部 大みか事業所
制御セキュリティ設計部 所属
現在，制御システム向けセキュリティ製品の設計・開発に従事

山田 勉
日立製作所 サービス&プラットフォームビジネスユニット
制御プラットフォーム統括本部 大みか事業所
制御セキュリティ設計部 所属
現在，制御システムのセキュリティコンサルティングに従事
IEC TC 65/WG 10（制御システムセキュリティIEC 62443規格策定）Expert，技術士（総合技術監理部門，情報工学部門），CISSP，IEEE会員，計測自動制御学会会員，電子情報通信学会会員

山口 耕平
日立製作所 サービス&プラットフォームビジネスユニット
制御プラットフォーム統括本部 大みか事業所
制御セキュリティ設計部 所属
現在，制御システムのセキュリティコンサルティングに従事
CISSP，情報処理安全確保支援士