メーカーの基幹システムが狙われている！

製造現場が情報高度化する中、制御システムはサイバー攻撃の危険に晒されている

問題

サイバー攻撃リスクの所在を可視化し、それぞれのセキュリティ対策を実施

課題

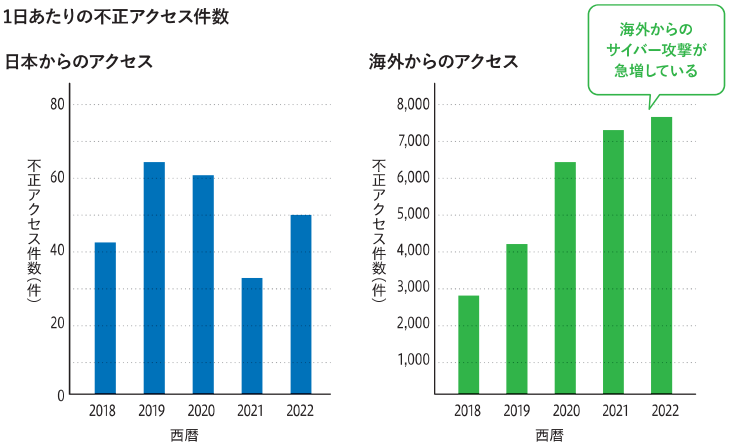
検知、侵入防止、書換防止の技術を開発。また書き換えられても製品自体の安全を担保

解決

問題　サイバー攻撃の増加･深刻化

電力会社や石油パイプライン、自動車メーカーの生産ラインといったインフラの制御システムを標的としたサイバー攻撃が増加し、サービスの持続的な提供自体が脅かされている。日本でも海外からのサイバー攻撃が急増しており（下図）、サイバー空間は既に国家間の争いの場の一部となっている。実際にロシアによるウクライナ侵攻でも発電所や通信施設がサイバー攻撃の標的となるなど、サイバー防衛の強化は急務である。

自動車、監視カメラ、ロボットなど、ネットワーク接続された IoT 機器を狙ったサイバー攻撃が増加している。自動車やドローンが乗っ取られ、人命が危険にさらされるリスクも現実のものとなりつつある。近年生成 AI が市場に出始めており、人間のコントロールを外れたサイバー攻撃プログラムや、新種のウイルスの生成が懸念される。AI の及ぼす影響の確認と規制検討は始まったばかりである。



（注）警視庁がインターネットに設置したセンサーで検知した１日あたりの不正アクセス数

警察庁広報資料「令和４年におけるサイバー空間をめぐる脅威の情勢等について」より三菱総合研究所作成

世界
ポテンシャル
インパクト試算

サイバー犯罪による経済的損失(知的財産や金融資産の窃取、企業の運営効率低下など)は2020年で1兆ドルを超える。この数字は世界のGDPの1%超、2018年比で1.5倍超である[104]。(B)

2018年のドローン世界市場規模は約1.6兆円。2020年から2025年までの年平均成長率(CAGR)は8.3%と予測されている。この市場の大部分は軍用需要が占める[105]。(A)

課題 Society 5.0時代のセキュリティ対策

課題解決のポイント

制御システム:サイバー・フィジカル・セキュリティの構築

制御システムでは、汎用化されたOSやプロトコルの使用が増え、インターネットを介し他のシステムとの連携が広がっている。この結果、サイバー攻撃を受けるリスクも増大している。また、制御システムは24時間継続稼働が重視されるため、セキュアな最新機器への入れ替えを困難にしている。構築済のシステムでは、後付けでセキュリティ強化が可能なソリューションに対するニーズが高まることが想定される。また、今後は、設計段階から両空間(サイバー空間、フィジカル空間)を視野に入れたサイバー攻撃対策を講じる必要がある。

課題解決のポイント

自動化機器:潜在リスクの見える化と重要技術の国産化

自動運転車、ドローン、ロボットといった次世代の自動化機器類は、多様で複雑な部品構成であるため、操作時にIoT機器を使った膨大な情報通信が発生する。そのため、サイバー攻撃される場面(いつ、どこで)を特定しにくくなり、リスクの所在を可視化するソリューションが求められる。また、この検討に際しては、自社内の対策にとどまらず、サプライチェーン全体を視野に入れることが肝要である。さらに、国外への機密情報漏洩リスクが高まる中、国内企業によるサイバーセキュリティ技術・サービスの開発が期待される。

課題解決のポイント

Webアクセス:ゼロトラストによる総合的なセキュリティ環境

従来、ネットワークの安全性は境界線を設けることにより担保してきた。ネットワークを内側と外側に分離し、「内部は安全」、「外部は危険」との考えに基づく対応である。その後クラウドの普及により、すべての通信アクセスを同じレベルで検査し、個別にセキュリティ対策を講じるゼロトラストの考え方が広まった。今後は、サイバーセキュリティに関するリテラシーの向上(専門人材の育成も含む)を踏まえた総合的なセキュリティ環境を構築することが重要である。

さらに、SNS等で氾濫する個人情報の取扱い、AI技術を悪用したディープフェイクに対する規制方法など、セキュリティ対策の対象範囲が拡大している。

解決 解決への糸口【技術動向】

① 制御システム

実用化時期

システムのセキュリティを高める技術

- 制御システムの可用性を損なわないセキュリティ・リスク・アセスメント、ペネトレーションテスト等のサイバー攻撃演習といったソリューションサービスが広がりつつある。 — 2020-25
- 経済産業省はソフトウェアを構成するプログラムを一覧化した「SBOM(エスボム、ソフトウェア部品表)」[106]の作成を促している。 — 2020-25

ネットワークのセキュリティを高める技術

- 制御システムを含む情報系ネットワークと各現場における産業用ネットワークをつなぐ産業用IoTゲートウェイにおいて、「産業用IoTゲートウェイの資産管理」、「産業制御システム内の機器の脆弱性の確認・対策」、「産業用通信プロトコルに対応した産業用ファイアウォールの導入」というセキュアな装置の開発や対策が求められている[107]。 — 2025-35

② 自動化機器

機器のセキュリティを高める技術

- ビル内の空調設備をはじめとする多様な機器を自動管理するシステム(Building Automation System、BAS)においてセキュリティ対策への関心が高まっている。 — 2020-25

参考事例

パナソニックは森ビルと、ビルオートメーションシステム向けのセキュリティ技術（AIによって異常を検知する技術）の開発に向けて、2019年1月末より実証実験を開始した[108]。

- 車の自動運転化に向けて、外部からのハッキングによる遠隔操作等を防ぐためのセキュリティ技術ニーズが高まっている。 — 2025-35

参考事例

SafeRide Technologies社（イスラエル）は、AIと異常検知技術を組み合わせたサービス「vSentry」を開発し、自動車を対象とするサイバー攻撃のリスク評価や、リアルタイムにサイバー攻撃を検知するサービスを提供している[109]。

機器のセキュリティを高める技術

- AIの判断ミスを招いたり、学習データを書き換えたりするサイバー攻撃の増加が今後予測される中、AIシステムのセキュリティ強化に向けた研究が進んでいる。 — 2020-25

参考事例

米サンフランシスコのスタートアップRobust Intelligence社は、AIセキュリティプラットフォームを構築し、NTTデータなどAIを活用する企業に導入が進んでいる[110]。

■ 自動化機器等の位置を特定するためのGNSS(全球測位衛星システム)に対するスプーフィング(ハッキング)対策として、アンテナ技術や信号認証技術の開発が日本で始まっているが、まだ開発途上の段階である[111]。 2025-35

サプライチェーンのセキュリティを高める技術

■ 自動車へのサイバー攻撃対策に関する国際標準規格(ISO/SAE 21434)を受け、サイバーセキュリティの基本ルールや体制構築、各製造工程における脆弱性診断、継続的なセキュリティ評価等、ソリューションサービスの提供が広がりつつある。 2025-35

③ Webアクセス

不正アクセスによる被害を防ぐ技術

■ スマートフォンによる決済や送金サービスの拡充に伴い、不正アクセス・ログインの検知や、なりすましによる購入などを防ぐための、セキュリティ技術のさらなる向上が求められている。 2020-25

■ 量子コンピューターの性能向上によって、インターネット通信や仮想通貨で用いられる既存の暗号が解読される危険性があり、量子暗号の研究が進展している[112]。 2020-25

■ インターネット上に投稿されたニュースや画像の信憑性をチェックするツールの開発が進んでおり、災害時のSNS情報の活用促進のほか、フェイクニュース等を悪用した詐欺行為の防止に向け、実用化が期待されている。 2020-25

参考事例

米サンディエゴのスタートアップTruepic社は画像が撮影された日付や時刻、位置情報を正確にデータに紐付けすることができるスマートフォン用アプリを開発した[113]。

アクセスを快適にする技術

■ 既存のSNSに加えて、招待制、音声のみ、匿名など、より安全に他者と交流できるSNSが登場している。 2020-25

参考事例

コロナ禍において、ユーザーによって招待されなければ登録できず、音声のみで参加するSNS「Clubhouse」が急速に広まった。
大学生専用の匿名SNS「Dtto」が2021年4月にオープンし、本人確認をはじめ、AIを活用した発言のモニタリング、ダイレクトメッセージの禁止など、SNSによる犯罪を抑制するような徹底的なセキュリティ対策を講じている[114]。

■ 選挙投票のオンライン化ニーズはあるが、本人確認と匿名性の担保をいかに両立させるかが課題となっている。 2025-35

解決 解決への糸口【規制動向】

- 警察庁では、深刻化するサイバー攻撃に対応するため、2022年度にサイバー局を設置する方針を決定した。
- 政府は2020年に「政府情報システムのためのセキュリティ評価制度」(Information system Security Management and Assessment Program：ISMAP)を制定した。政府が求める高いセキュリティ要求を満たすクラウドサービスを評価・登録することによって、そうしたサービスの円滑な導入を目指している[115]。
- 経済産業省は、産業に求められるセキュリティ対策の全体像を整理した「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)」を策定している[116]。
- アメリカや中国など、世界ではディープフェイクによるなりすましやポルノといった犯罪行為を防ぐための規制が広がっており、日本でも公職選挙法においてディープフェイク規制が必要との議論が持ち上がっている[117]。
- 2022年3月、防衛省は「自衛隊サイバー防衛隊」を発足させた。2024年にもサイバー分野を担う自衛官を民間から初採用する予定である[118]。
- 2022年12月に日本政府は「国家安全保障戦略」などの安保関連3文書を改定した。文書内では、国や重要インフラに重大な影響を与える可能性のあるサイバー攻撃に対して先手を打って対抗措置を取る「能動的サイバー防御」の導入が新たに明記された[119]。また、サイバー防衛人材を2万名規模に拡充することを示しており、2023年1月には内閣官房に「サイバー安全保障体制整備準備室」を設置し、法整備の検討に入っている。
- 2023年5月に公布された「経済安全保障推進法」では、基幹インフラを担う企業は委託会社も含め、重要機器導入前に政府が事前審査を行う制度が導入されている[120]。各インフラ企業にはより一層のサイバーセキュリティ対策が求められている。
- 日本、アメリカ、オーストラリア、インドは重要インフラ施設を狙ったサイバー攻撃に対し、各政府のサイバー部門が情報を即時に共有する体制を作ろうとしている[121]。この情報共有にはインフラ系民間企業も含まれる予定である。

SDGsとの対応

問題 サイバー攻撃の増加・深刻化　課題 Society 5.0時代のセキュリティ対策

対応するSDGsターゲット

9.1 全ての人々に安価で公平なアクセスに重点を置いた経済発展と人間の福祉を支援するために地域・越境インフラを含む質の高い、信頼でき、持続可能かつ強靱(レジリエント)なインフラを開発する。