プレスリリース
2020 年 1 月 14 日
独立行政法人情報処理推進機構

「産業用制御システムのセキュリティ 10 大脅威と対策」を発表
～ドイツ連邦政府 情報セキュリティ庁の Top10 Threats and Countermeasures 2019 を翻訳～

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）は、国内の産業用制御システム保有事業者のセキュリティ対策を促進するために「産業用制御システムのセキュリティ 10 大脅威と対策」を発表しました。これはドイツ連邦政府 情報セキュリティ庁が作成したものを IPA が許可を得て翻訳したものです。

URL：https://www.ipa.go.jp/security/controlsystem/bsi2019.html

産業用制御システムは、電力、ガス、水道、鉄道等の社会インフラや、石油、化学、鉄鋼・自動車・輸送機器、精密機械、食品、製薬、ビル管理等の工場・プラントにおける監視・制御や生産・加工ラインにおいて用いられています。

IPA では、2017 年 10 月「制御システムのセキュリティリスク分析ガイド(*1)」を発刊。制御システムの資産や事業被害のリスクレベルを明確化するリスクアセスメント手法を解説しています。また、2019 年 7 月には、過去のサイバー攻撃の事例をもとに、その概要と攻撃の流れを紹介する「制御システム関連のサイバーインシデント事例(*2)」シリーズを公開しています。

現在の制御システムは我々の社会や産業の基盤を支えており、サイバー攻撃等で稼働が阻害された場合、社会的な影響や事業継続上の影響が大きいため、セキュリティ対策の向上が急務です。

本日発表した「産業用制御システムのセキュリティ -10 大脅威と対策 2019-」はドイツ連邦政府 情報セキュリティ庁（BSI）が作成したもの(*3)を、IPA が許可を得て翻訳したものです。

＜表紙＞

(*1) https://www.ipa.go.jp/security/controlsystem/riskanalysis.html
(*2) https://www.ipa.go.jp/security/controlsystem/incident.html
(*3) Industrial Control System Security: Top10 Threats and Countermeasures [English] v1.3
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_005E.html
ランキングはこれまで 2014 年、2016 年に出されている。

ランクインした脅威は、日本国内でも共通の事項が多く、事業者にとってこれらの脅威とその発生要因、具体的な手口、および対策を体系的に理解することに役立ちます。

2019 年の順位は、2016 年に比べて、制御システムにおける利用増加に伴い、クラウドコンポーネントや外部ネットワークへの攻撃の脅威が上昇しています。一方で、ソーシャルエンジニアリングやフィッシングの脅威は、相対的に降下しています。

産業用制御システムのセキュリティ 10 大脅威（2019 年）		2016 年
1 位	リムーバブルメディアや外部機器経由のマルウェア感染	2 位
2 位	インターネットおよびイントラネット経由のマルウェア感染	3 位
3 位	ヒューマンエラーと妨害行為	5 位
4 位	外部ネットワークやクラウドコンポーネントへの攻撃	8 位
5 位	ソーシャルエンジニアリングとフィッシング	1 位
6 位	DoS/DDoS 攻撃	9 位
7 位	インターネットに接続された制御機器	6 位
8 位	リモートアクセスからの侵入	4 位
9 位	技術的な不具合と不可抗力	7 位
10 位	スマートデバイスへの攻撃	10 位

なお、資料には、制御システムを保有する事業者のセキュリティレベルの自己評価に役立つ、セルフチェックリストを用意しています。また、チェックリスト実施後に得られたスコアに対して、実施すべき推奨事項を示しています。これらを材料に自組織の現状把握ができ、対策の方針検討の着手が可能です。

■ 本件に関するお問い合わせ先
IPA セキュリティセンター　辻／松島
Tel: 03-5978-7527　E-mail: isec-ics@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部　広報戦略グループ　白石
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp