

「半導体デバイス工場における OT セキュリティガイドライン（案）」に対する意見 公募要領

令和 7 年 6 月 27 日
経済産業省商務情報政策局
サイバーセキュリティ課・情報産業課

1. 意見公募の趣旨・目的・背景

サイバー攻撃はますます多様化・高度化しており、多くの制御装置等が攻撃され、工場における生産が停止する等の被害が発生しています。また、各種の開発機密（知的財産）がサイバー攻撃によって流出する危険も増しており、半導体産業の経済及び安全保障上の重要性や足下でのサイバー脅威・リスクの高まりを踏まえると、高度なサイバー攻撃への対応を含めたセキュリティ対策を進めていく必要があります。

国外では、国際的な半導体関連の業界団体である SEMI により、半導体製造装置に係る E187/E188 規格が策定され、また、米国立標準技術研究所（NIST）においても Cybersecurity Framework 2.0（CSF 2.0）について、半導体製造プロファイルの策定が進められています。

一方、我が国では、経済産業省が 2022 年に汎用的な組立型の工場を対象とした「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」を策定し公表していますが、一般的にプロセスオートメーション型の工場であり、工場の規模が大きく、汎用 OS を用いた製造装置の台数が多い等の特徴を有する半導体工場には、当該ガイドラインがなじまないといった実態があります。

こうした課題意識の下、経済産業省では、2024 年 11 月より産業サイバーセキュリティ研究会の下で半導体産業サブワーキンググループ（座長：東京大学 江崎教授）を開催し、半導体デバイスメーカーや半導体製造装置メーカーを含めた国内外の様々な企業・団体関係者を交えて、我が国の半導体デバイス工場における制御システム（OT）のセキュリティ対策のあり方について議論を行ってきました。

今般、その議論の成果を、国際的な半導体産業における各種セキュリティ規格とも整合した、半導体デバイス工場向けの工場セキュリティ対策の指針である「半導体デバイス工場における OT セキュリティガイドライン（案）」として取りまとめました。我が国半導体産業は国際的な供給網を前提として成立していること等に鑑み、同ガイドライン（案）について国内外の利害関係者から広く御意見をいただくべく、同ガイドライン（案）の日本語版・英語版の両方について、本日より 60 日間のパブリックコメントを実施することとしました。

2. 意見公募の対象

- ・ 半導体デバイス工場における OT セキュリティガイドライン（案） 日本語版
- ・ 半導体デバイス工場における OT セキュリティガイドライン（案） 英語版

3. 資料入手方法

電子政府の総合窓口（e-Gov）における掲載

4. 意見募集期間（意見募集開始日及び終了日）

2025 年 6 月 27 日（金曜日）から 2025 年 8 月 26 日（火曜日）必着（日本時間）

5. 意見提出先・提出方法

電子政府の総合窓口（e-Gov）から本件の意見提出フォーム（※ 案内は日本語のみ）に進み、日本語又は英語で御記入の上、ご提出ください。

なお、電子政府の総合窓口（e-Gov）のご利用が難しい場合は、別紙の意見提出用紙に日本語又は英語で記入の上、下記のメールアドレス宛にお送りください。

・ メールアドレス：bzl-cybersec_comment@meti.go.jp

（件名は「半導体デバイス工場における OT セキュリティガイドライン（案）に対する意見」とし、意見提出用紙を添付してお送りください。）

※ 電話での意見提出はお受けしかねますので、あらかじめ御了承下さい。

6. その他

皆様からいただいた御意見につきましては、最終的な決定における参考とさせていただきます。なお、いただいた御意見についての個別の回答はいたしかねますので、あらかじめ、その旨を御了承下さい。

御提出いただきました御意見については、氏名、住所、電話番号、FAX番号及びメールアドレスを除き、すべて公開される可能性があることを、あらかじめ御承知おき下さい。ただし、御意見中に、個人に関する情報であって特定の個人を識別しうる記述がある場合及び個人・法人等の財産権等を害するおそれがあると判断される場合には、公表の際に当該箇所を伏せさせていただきます。

御意見に附記された氏名、連絡先等の個人情報につきましては、適正に管理し、御意見の内容に不明な点があった場合等の連絡・確認といった、本案に対する意見公募に関する業務にのみ利用させていただきます。

