Spectre (スペクター) と Meltdown (メルトダウン) 脆弱性に関する情報

2018 年 7 月 6 日
更新 2020 年 3 月 11 日

「Spectre」と「Meltdown」は、CPU を高速化するための技術「投機的実行」の仕組みがそのまま情報流出を招くセキュリティホールとなっている問題で、Intel 製、AMD 製および ARM 製の CPU に関連する脆弱性です。

Spectre は I ntel 製、AMD 製、ARM 製の CPU を対象とした脆弱性です。

Meltdown は Intel 製の CPU が対象の脆弱性です。

本脆弱性が影響する製品かどうかの判断として、搭載している CPU の種類、その機器でアプリケーションがインストール・実行できるかがポイントとなります。

当社製品において、本脆弱性を利用した被害は現時点で確認されておりませんが、より安心して製品をお使いいただくため、本脆弱性への対応方法等を以下の通りご案内致します。

1.対象となる製品

・当社製品で Spectre の攻撃対象に該当し、Spectre の対策ファームウェアを準備している製品は下記製品となります。

スキャントロニクス CL4/6NX-J シリーズ、プチラパン PW208 シリーズ、
プチラパン PW208NX シリーズ、タフアーム LR4NX-FA シリーズ

・2019 年 10 月以降に販売開始された新製品では対応の必要はございません。

・当社製品では、Meltdown の攻撃対象になる製品はございません。

2.対応に関して

上記製品に関して、Spectre に対する修正ファームウェアを準備しております。
なお、当社製品の本体ファームウェア更新に関して、ファームウェア更新後の各種機能設定、ご使用のサプライに対する印字位置等の各種設定が必要となる事があり、ファームウェアの更新作業に関しては、弊社 CE による作業とさせていただいております。

本件に関するお問い合わせ先：0120-696310　（受付時間：24 時間 365 日）