IPC プラットフォーム NY シリーズにおける境界外読み取りの脆弱性

公開日 2025 年 11 月 17 日
オムロン株式会社

■概要

産業用 PC プラットフォーム NY シリーズの TPM 2.0 において、境界外読み取り（CWE-125）の脆弱性が存在することが判明しました。攻撃者は当該脆弱性を用いて、機密情報を読み取ったり、クラッシュを引き起こしたりする可能性があります。

この脆弱性の影響を受ける製品、バージョン、および軽減策・回避方法を以下に示します。弊社が推奨する軽減策・回避策を実施することで、本脆弱性の悪用リスクを最小限に抑えることができます。また、お客様に製品をより安心して利用いただくために、今回製品セキュリティ強化の対策バージョンを用意いたしました。各製品の対策バージョンの提供について本文の対策方法に示しますので、対策の実施をお願いいたします。

■対象製品

本脆弱性の影響を受ける製品の形式、およびバージョンは以下の通りです。

産業用 PC プラットフォーム NY シリーズ

型式	対象 TPM バージョン	ロット番号（製造年月日）
NYB27-□□□□□	5.63 以前	23X25 (2025 年 10 月 23 日)以前
NYB35-□□□□□		
NYB2C-□□□□□		
NYB2A-□□□□□		
NYB55-□□□□□	7.85 以前	
NYB65-□□□□□		
NYB13-□□□□□		
NYB37-□□□□□		
NYB3A-□□□□□		
NYB2E-□□□□□		
NYP27-□□□□□	5.63 以前	
NYP35-□□□□□		
NYP2C-□□□□□		
NYP2A-□□□□□		
NYP55-□□□□□	7.85 以前	
NYP65-□□□□□		
NYP13-□□□□□		
NYP37-□□□□□		
NYP3A-□□□□□		
NYE2A-□□□□□	5.63 以前	

NY シリーズにおける TPM のバージョンの確認方法は、「別紙 TPM バージョンの確認方法」を参照してください。

ロット番号の確認方法は以下のマニュアルの「識別情報表示ラベル」を参照してください。

- NYB シリーズ 産業用ボックス型 PC ユーザーズマニュアル ハードウェア編（SBCA-431）
- NYP シリーズ 産業用パネル型 PC ユーザーズマニュアル ハードウェア編（SBCA-433）

■脆弱性内容

Trusted Computing Group が公開した TPM 2.0 リファレンス実装コード（Rev 1.83、1.59、1.38）に境界外読み取り（CWE-125）の脆弱性が見つかり、TPM の情報漏えいまたはサービス拒否につながる可能性があります。

本脆弱性は産業用 PC の Trusted Platform Module（TPM）に影響します。BitLocker で保護されたデータを含む、TPM によって保護される任意のデータが影響を受ける可能性があります。

なお、NYB/NYP/NYE シリーズの産業用 PC において、TPM のセキュリティ機能を利用していないユーザーは本問題の影響を受けません。

■CWE、CVE、CVSS スコア

境界外読み取り (CWE-125)

CVE-2025-2884

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:H 基本値 6.6

■対策方法

各製品における TPM を対策バージョンに更新することで、本脆弱性の対策が可能です。

以下に各製品の対策バージョン、および対策バージョンの提供時期を示します。

産業用 PC プラットフォーム NY シリーズ

型式	対象 TPM バージョン	ロット番号	対策バージョン提供時期
NYB27-□□□□□	5.66 以降	24X25 以降	2025 年 10 月 24 日
NYB35-□□□□□			
NYB2C-□□□□□			
NYB2A-□□□□□			
NYB55-□□□□□	7.86 以降		
NYB65-□□□□□			
NYB13-□□□□□			
NYB37-□□□□□			
NYB3A-□□□□□			
NYB2E-□□□□□			
NYP27-□□□□□	5.66 以降		
NYP35-□□□□□			
NYP2C-□□□□□			
NYP2A-□□□□□			
NYP55-□□□□□	7.86 以降		
NYP65-□□□□□			
NYP13-□□□□□			
NYP37-□□□□□			
NYP3A-□□□□□			
NYE2A-□□□□□	5.66 以降		

パッチイメージのリリース日：2025 年 11 月 4 日

注意：TPM のアップデートに失敗した場合、IPC が起動しなくなる可能性があります。
リスクを受け入れられる場合のみ、以下の手順を実施してください。

TPM の更新手順

1. オムロンのダウンロードページ[https://www.fa.omron.co.jp/member/product/tool/ipc-platform/index.htm]にアクセスします
2. ページ下部のソフトウェア使用許諾契約を読み、最新バージョンの「規約に同意し、ダウンロードページを開く」をクリックします
3. [Trusted Platform Module ファームウェア]から、使用している IPC モデルに対応するイメージをダウンロードします
   ダウンロードしたイメージの SHA256 ハッシュがダウンロードページ記載の値と一致することを確認します
4. Rufus [https://rufus.ie/ja/] を用いて、ダウンロードしたイメージから起動用 USB フラッシュドライブを作成します
5. [DEL]キーを繰り返し押し、IPC を BIOS で起動します
6. [Advanced]→[Trusted Computing]を選択します
7. [Security Device Support]を選択し、[Disable]に設定します
8. 変更を保存(F10)して再起動します
9. UEFI シェル用 USB メモリを接続します
10. IPC を再起動し、USB メモリから起動します
11. TPM アップデートスクリプトが自動的に実行されるので、完了まで待ちます
12. IPC を再起動して BIOS で起動します
13. [Advanced]→[Trusted Computing]→[Security Device Support]を選択し、[Enable]に戻します

■軽減策・回避策

本脆弱性の悪用リスクを最小限に抑えるため、以下に示す軽減策を講じることを推奨します。

1. アンチウィルス保護

   制御システムに接続するパソコンに最新の商用品質のウイルス対策ソフトの導入・保守

2. 不正アクセスの防止

   以下に示す対策を講じることを推奨します。

   - 制御システムや装置のネットワーク接続を最小限に抑え、信頼できないデバイスからのアクセス禁止
   - ファイアウォールの導入による IT ネットワークからの分離（未使用通信ポートの遮断、通信ホストの制限）
   - 制御システムや装置へのリモートアクセスが必要な場合、仮想プライベートネットワーク (VPN)の使用
   - 強固なパスワードの採用と頻繁な変更
   - 権限保有者のみを制御システムや装置へのアクセスを可能とする物理的統制の導入
   - 制御システムや装置で USB メモリなど外部ストレージデバイスを使用する場合の事前ウイルススキャン
   - 制御システムや装置へのリモートアクセス時の多要素認証の導入

3. データ入出力の保護

   制御システムや装置への入出力データの意図せぬ改変に備えた、バックアップや範囲チェックなどの妥当性の確認

4. 紛失データの復元

   データ紛失対策としての定期的な設定データのバックアップと保守

■お問い合わせ先

当社営業または販売店にお問い合わせください。

国内お問い合わせ先：https://www.fa.omron.co.jp/sales/local/

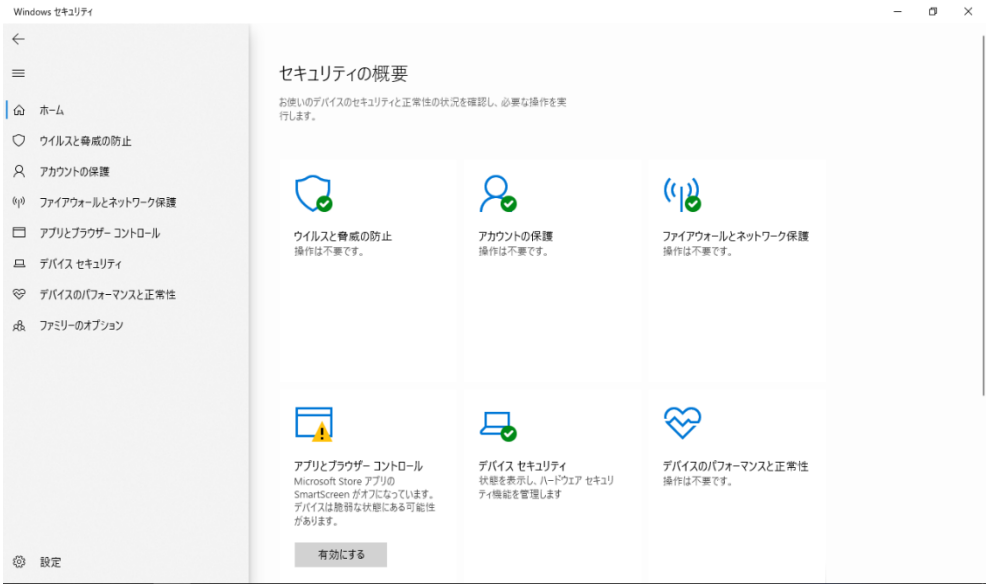
海外お問い合わせ先：https://www.ia.omron.com/global_network/index.html

■更新履歴

2025 年 11 月 17 日: 新規作成

別紙 TPM バージョンの確認方法

1. Windows で、[**Windows セキュリティ**] に移動します
   Windows セキュリティ情報が表示されます。



2. **[デバイス セキュリティ]** を選択します。
   デバイスセキュリティ情報が表示されます。

3. **[セキュリティ プロセッサの詳細]** を選択します。

TPM の製造元バージョンを含むセキュリティ プロセッサの詳細が表示されます。