栃木県警察サイバー対策センター
TOCHIGI POLICE
CYBERCRIME CONTROL CENTER

# USBメモリにも危険が…

陸上自衛隊が2025年2月まで約1年間、中国系マルウェアに感染したUSBメモリを機密システムの端末で使用していたことが報じられました。このUSBメモリは、記憶容量を偽装した中国製品であり、大手ECサイトにおいて同種製品が安価で販売されているとのことです。

USBメモリのマルウェアには、

**① ファイルとして保存されたもの**

**② 制御チップのファームウェアに書き込まれたもの**

があります。

対策を次の表にまとめたので、参考にしてください。

| | 対策 | 効果 | ファイル型への有効性 | ファームウェア型への有効性 |
|---|---|---|---|---|
| 調達時 | 製造元の確認 | 信頼性の確認 | ○ | ○ |
| | 正規調達経路からの購入 | 第三者混入・再販品の回避 | ○ | ○ |
| | 極端に安価な製品への注意 | 偽造・改造品の回避 | ○ | ○ |
| 運用時 | セキュリティソフトでの検知 | ファイル型マルウェアの検知・除去 | ○ | × |
| | 自動実行（AutoRun）の無効化 | 自動実行による感染防止 | ○ | △ |
| | USBデバイスの接続制御 | 不正デバイスの接続防止 | ○ | ○ |
| | 接続ログの取得・監視 | 不審な挙動の早期発見 | ○ | ○ |
| | USBメモリの管理 | 利用統制・追跡 | ○ | ○ |

陸上自衛隊では、調達時の確認やセキュリティソフトでの検知といった多重チェックのルールがあったものの、きちんと機能していなかったとのことです。

調達や運用のルールを整備するだけでなく、ルールの運用状況をチェックすることが重要です。