2026 年 7 月 27 日

自動車産業サプライチェーン関係者各位

一般社団法人 日本自動車工業会
総合政策委員会 ICT 部会サイバーセキュリティ分科会
一般社団法人 日本自動車部品工業会
総合技術委員会 DX 対応委員会サイバーセキュリティ部会

重要：AI 性能の高度化を踏まえたサイバーセキュリティ対策強化のお願い

■背 景

AI 技術は急速に進展・普及しており、サイバー攻撃に AI が悪用されることで、攻撃のスピード・規模が劇的に増加する等、サイバーセキュリティにおける脅威に直面しています。

特に、本年 4 月 7 日に米国アンソロピック社が公表した「Claude Mythos Preview(クロードミュトス)」を始めとする高性能な AI(フロンティア AI)は、サイバーセキュリティ対策に活用することで、サイバー対処能力の更なる強化が期待できる一方で、攻撃者に悪用されることにより、サイバー攻撃がより高速かつ大規模に行われる恐れがあり、悪用リスクを前提とした対策強化を早急に進めていくことが必要です。

経営層のリーダーシップの下、高性能 AI の悪用リスクに備えたサイバーセキュリティ対策の実施や、より高速かつ大量に脆弱性が発見・修正されることを前提とした対策強化をお願いいたします。

■お願い

経営層・ご担当者の皆様におかれましては、サイバー攻撃によって重要情報の窃取のみならず、事業活動の停止や製造サプライチェーンの停止など、ビジネスに大きな影響を及ぼす事態も想定されることから、自社のセキュリティ対策状況を今一度ご確認いただき、以下ご対応をお願いいたします。

1．発見された脆弱性に早期に対応してください

積極的に脆弱性関連情報を収集し、脆弱性が発見された場合には、ビジネスに於ける重要度及び、発生リスクの重大度による優先度を設定した上で、重要度・重大度に応じた速やかな対応を行ってください。

具体的には.....

・脆弱性情報通知サービスの導入、脆弱性管理ツールや診断サービスの導入、脆弱性対応プロセスの整備や強化など

・特に、攻撃者から狙われ易い、外部公開システム(VPN 装置、リモートアクセス装置、Web サーバなど)に対しては、最優先で、修正プログラム(＝脆弱性パッチ)の適用を行う

2. 組織のトップが主導して取り組んでください

サイバーセキュリティリスクは経営リスクとの認識を持ち、経営陣のリーダーシップの下、必要なリソースの確保と対応を行ってください。

具体的には.....

・上記 1.の脆弱性対応を担当者に指示すると共に、ツール・サービス導入の費用やプロセス強化に必要な人工など、リソースに対する経営的判断

・特に、外部公開システムへの緊急パッチ適用に際したシステムの一時停止といった高度な判断

・加えて、侵入された場合の代替手段など、事前に且つ確実な事業継続計画(BCP)の立案

※平時からの準備は、経営層の皆様のリーダーシップが何より重要です。

以 上

本件問い合わせ先：
一般社団法人 日本自動車工業会
ICT 部会 事務局
ict-cybersecurity@mta.jama.or.jp