令和 5 年 2 月 20 日

お客様各位

トヨタコネクティッド株式会社

H2V ファームウェア更新のお知らせ

平素より弊社製品をご利用いただき、誠にありがとうございます。
現在、ご利用いただいております H2V Gateway（【対象製品】参照）ですが、セキュリティに関する脆弱性を検知したため、セキュリティ対策したファームウェアの公開を 2023 年 2 月 20 日実施いたしました。大変お手数ではございますがファームウェア更新をお願いいたします。

【対象製品】

H2V Gateway

【H2V Manager 用　H2V α用】

【H2V eneli 用】

【対象ファームウェア】

対象商品	更新後のファームウェアバージョン
H2V Manager	Ver1.94
H2V α	Ver1.94
H2V eneli	Ver2.03

【更新方法】

対象商品の下記サイト**「お知らせ」**より、「**H2V Gateway ファームウェア更新設定ガイドのご案内**」を、ご覧いただき、ファームウェア更新をお願いいたします。

H2V Manager　：http://tsc-h2v.com/support/index.html
H2V α　：https://toyotaconnected.co.jp/H2V/alpha/support/index.html
H2V eneli　：https://toyotaconnected.co.jp/H2V/eneli/home/support.html

＜ファームウェア更新方法に関するお問い合わせ先＞

「H2V ファームウェアサポートセンター」
TEL：03-3570-7934　受付時間 9：00～18：00（年中無休）
※本デスクは 2023 年 7 月 31 日までの開設予定ですが、状況により前倒しすることがございます。

＜よくあるご質問＞

Q１．ファームウェアの更新は必要ですか？

A１．セキュリティ強化のためファームウェアをアップデートしておりますので、更新お願いします。
脆弱性及び想定される脅威については下記表をご確認ください。

	脆弱性	想定される脅威
1	機器の設定画面へのログイン後に、デバッグ機能（プログラムの欠陥を探し出すための開発者用機能）を利用することが可能となります。	LAN に接続している攻撃者が事前に機器のログイン ID、パスワードを取得している場合、機器内部のプログラムへ指示を出したり、設定の取得、変更、初期化などが行われたりする可能性があります。
2	機器の設定画面へのログインをすることなしに、不正に機器の設定画面にアクセスされる可能性があります。	LAN 内の攻撃者が悪意を持って機器の設定画面へ指示を送信することにより、機器の設定画面が操作可能になり、機器の設定の取得、変更、初期化などが行われる可能性があります。

Q２．ファームウェアを更新しないとサービスへの影響はあるのでしょうか？

A２．サービスの利用は可能ですが、セキュリティ上の観点から、更新をお願します。

Q３．ファームウェアを前のバージョンに戻したい。

A３．一度更新したファームウェアを以前の状態に戻す事はできません。 今回のバージョンアップは、セキュリティ向上を目的としておりますので、このままでのご利用をお願いします。

Q４．ファームウェア更新時間を教えて下さい。

A４．ファームウェア更新時間は約 6 分です。また、「H2V Gateway ファームウェアの更新設定ガイド」に記載している、更新にかかる全体の作業時間は約１０分程度となります。ご利用の環境などにより前後します事ご了承ください。

Q５．タブレット（スマートフォン）でのファームウェアの更新は可能でしょうか？

A５．パソコンでの更新を推奨しています。ただし、 H2V Gateway とタブレット（スマートフォン）を Wi-Fi に接続して更新する方法がありますが、推奨以外の方法では更新できない可能性がありますのでご了承ください。

＜H2V に関するお問い合わせについて＞

ファームウェア更新を除く【製品・サービス・操作方法・会員情報変更】に関するお問い合せはこれまで通り、
「Ｈ２Ｖサポートセンター」までお問い合わせください。

TEL：0561-57-6829 受付時間 9 時～18 時（年中無休）