【 公開版評価結果 】

申請企業の名称	NECプラットフォームズ株式会社
申請製品の名称	Aterm 7200D8BE
申請製品のファームウェアバージョン名	FW_7200D8BE Ver1.1.1以降
評価の方法	自己適合評価
評価完了日（YYYY/MM/DD）	2025/8/22

適合基準バージョン
JST-CR-01-01-2024/2024R1

適合確認
YES

★1適合基準番号	セキュリティ要件（大項目）	セキュリティ要件	☆1 適合基準	NAとなるための条件、基準の補足説明	評価結果
S1.1-01	1.脆弱な認証・認可メカニズム（例： 汎用のデフォルトパスワード、脆弱なパスワード）を使用しない 5. セキュアに通信する	1-3. 製品に対してユーザを認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。 5-5. ネットワークインタフェースを介してセキュリティに関連する設定の変更を可能にする製品の機能は、認証後にのみアクセス可能でなければならない。ただし、製品が依存するネットワークサービスプロトコルで、製品の動作に必要な設定を製造業者が保証できない場合は、例外とする。	IoT製品に対するIP通信を介した守るべき情報資産への他のIoT機器又はユーザからのアクセスに対して、適切な認証に基づくアクセス制御が行われていること。 なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けたIoT製品（技適[T]マーク又は[A]マークが付与されたIoT製品）は、本適合基準に適合しているとみなす。（この場合、「JC-STAR適合ラベル申請書」に「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）	【対象外（NA）となるための条件】 IP通信を介した守るべき情報資産への認証及びアクセスの仕組みがない （「対象外（NA）であることの理由」に、外部からの不正アクセスに対抗するために認証及びアクセスが必要ない根拠を記載すること） 【用語定義：守るべき情報資産】 以下のすべての情報： ・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・IoT機器の意図する使用において、IoT機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報	**適合（Y）**
S1.1-02	1.脆弱な認証・認可メカニズム（例： 汎用のデフォルトパスワード、脆弱なパスワード）を使用しない	1-1. パスワードが使用され、工場出荷時のデフォルト以外の状態にある製品において、すべてのパスワードは、機器ごとに固有であるか、又はユーザによって定義されるものでなければならない。 1-2. プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性をもつために、パスワードは十分なランダム性を保有しなければならない。	IoT製品に対するネットワークを介したユーザ認証の仕組み、又は、IoT機器初期設定時のクライアント認証の仕組みにてパスワードを使用するIoT製品において、IoT製品導入時にデフォルトパスワードが使用される場合に、以下の①・②のいずれかの基準を満たすこと。 ①デフォルトパスワードは、IoT機器毎に異なる一意の値で、容易に推測可能でない6文字以上のパスワードであること。 ②デフォルトパスワードは、初回起動時にユーザによるパスワード変更を必須とする機能を実装し、当該機能において設定可能なパスワードとして、8文字以上のパスワードの設定を強制させること。	【対象外（NA）となるための条件】 ネットワークを介したパスワードを利用したユーザ認証の仕組みがない （「対象外（NA）であることの理由」に、脅威に対抗するためにパスワードを利用したユーザ認証が必要ない根拠を記載すること）	**適合（Y）**
S1.1-03	1.脆弱な認証・認可メカニズム（例： 汎用のデフォルトパスワード、脆弱なパスワード）を使用しない	1-4. 製品に対するユーザ認証において、製品は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。	IoT製品に対するネットワークを介したユーザ認証において使用される認証値の変更について、認証の種類（パスワード、トークン、指紋等）に依らず、その認証値の変更を可能とすること。	【対象外（NA）となるための条件】 ネットワークを介したユーザ認証の仕組みがない（「対象外（NA）であることの理由」に、外部からの不正アクセスに対抗するためにユーザ認証が必要ない根拠を記載すること） 【用語定義：認証値】 IoT製品に対する認証の仕組みで使用される属性の個別値。（例：パスワードに基づく認証の仕組みである場合、認証値は文字列となる。生体指紋認証である場合、認証値は例えば左手の人差し指の指紋データとなる。）	**適合（Y）**
S1.1-04	1.脆弱な認証・認可メカニズム（例： 汎用のデフォルトパスワード、脆弱なパスワード）を使用しない	1-5. 機器が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない	IoT機器が、制約のある機器ではない場合、IoT機器に対するネットワークを介したユーザ認証の仕組みについて、総当たり攻撃を困難とすること。	【対象外（NA）となるための条件】 以下のいずれかの条件に該当する。（OR条件） ・IoT機器に対するネットワークを介したユーザ認証の仕組みがない（「対象外（NA）であることの理由」に、外部からの不正アクセスに対抗するためにユーザ認証が必要ない根拠を記載すること） ・IoT機器が「制約のある機器」に該当する（「対象外（NA）であることの理由」に、機器が「制約のある機器」に該当することを示す根拠を記載すること） 【用語定義：制約のある機器】 データを処理する機能、データを通信する機能、データを保存する機能、又はユーザと対話する機能のいずれかにおいて、意図された使用のために物理的な制約がある機器。（このようなIoT機器の例は「用語集」を参照。）	**適合（Y）**

★1適合基準番号	セキュリティ要件（大項目）	セキュリティ要件	☆1 適合基準	NAとなるための条件、基準の補足説明	評価結果
S1.1-05	2. 脆弱性の報告を管理するための手段を導入する	2-1. 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない。 ・問題を報告するための連絡先情報 ・以下のタイムラインに関する情報 1)最初の受領確認 2)報告された問題が解決されるまでの状況の更新	製造業者は、以下の①～③のすべての情報を含む脆弱性開示ポリシーを公開（例：製造業者のウェブサイトへの掲載）すること。 ①IoT 製品のセキュリティの問題に関して、製造業者へ報告するための連絡先（例：製造業者等のウェブサイトのURL、電話番号、メールアドレス） ②製造業者がIoT製品のセキュリティに関する報告を受領した後に行う手続き及びその概要 ③脆弱性が解決されるまでのIoT製品や脆弱性の状況更新に関する手続き及びその概要	【対象外（NA）となるための条件】 該当事項なし	**適合（Y）**
S1.1-06	3. ソフトウェアを最新の状態に保つ	3-1. 製品に含まれる特定のソフトウェアコンポーネントについて、アップデート可能にしなければならない。 3-2. 機器が、制約のある機器でない場合、アップデートをセキュアにインストールするためのアップデートメカニズムを備えていなければならない。	IoT製品に含まれるソフトウェアコンポーネントのアップデート機能について、以下の①～③のすべての基準を満たすこと。 ①IoT製品のファームウェア（ソフトウェア）パッケージについて、アップデートが可能であること。 ②ファームウェア（ソフトウェア）パッケージのバージョンの確認が行えるなど、最新のファームウェア（ソフトウェア）がインストールされていることを確認する手段を有すること。 ③アップデートされたファームウェア（ソフトウェア）パッケージのバージョンが電源OFF後も維持されること。 なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けたIoT製品（技適[T]マーク又は[A]マークが付与されたIoT製品）は、本適合基準に適合しているとみなす。（この場合、「JC-STAR適合ラベル申請書」に「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）	【対象外（NA）となるための条件】 該当事項なし	**適合（Y）**
S1.1-07	3. ソフトウェアを最新の状態に保つ	3-3. 製品においてアップデートメカニズムが実装されている場合、そのアップデートは、ユーザが簡単に適用できるものでなければならない。	ユーザがアップデートを適用する際、容易かつ分かりやすい手順でソフトウェアのアップデートを実行可能とすること。	【対象外（NA）となるための条件】 該当事項なし	**適合（Y）**
S1.1-08	3. ソフトウェアを最新の状態に保つ	3-2. 機器が、制約のある機器でない場合、アップデートをセキュアにインストールするためのアップデートメカニズムを備えていなければならない。 3-7. 製品においてアップデートメカニズムが実装されている場合、セキュアなアップデートメカニズムを容易にするために、ベストプラクティスの暗号技術を使用しなければならない。 3-10. 製品においてアップデートメカニズムが実装され、ソフトウェアアップデートがネットワークインタフェースを介して配信される場合、製品は、信頼関係を介して各アップデートの真正性及び完全性を検証しなければならない。	ソフトウェアをネットワーク経由でアップデートする際、ソフトウェアの完全性をアップデート前に確認できる仕組みを有すること。	【対象外（NA）となるための条件】 ソフトウェアをネットワーク経由でアップデートする仕組みが存在しない （「対象外（NA）であることの理由」に、想定するアップデートの仕組みを記載すること）	**適合（Y）**
S1.1-09	3. ソフトウェアを最新の状態に保つ	3-8. 製品においてアップデートメカニズムが実装されている場合、セキュリティアップデートは、適時でなければならない。	製造業者は、セキュリティ課題に対する迅速なアップデートを目的として、セキュリティアップデートの優先度を決定するための方針や指針を文書化すること。	【対象外（NA）となるための条件】 該当事項なし	**適合（Y）**
S1.1-10	3. ソフトウェアを最新の状態に保つ	3-14. 製品のモデル名称は、製品上のラベル又は物理的インタフェースを介して、ユーザに対して明確に認識可能でなければならない。	IoT製品の型番は、以下のいずれかの方法でユーザへ提供すること。 ①IoT製品本体に、IoT製品の型番を直接記載すること。 ②IoT製品のGUI、ウェブUI等や、IoT製品に付帯するソフトウェア、アプリケーション（スマホアプリなど）のGUI、ウェブUI等から、ユーザが型番を認識できるようにすること。	【対象外（NA）となるための条件】 該当事項なし	**適合（Y）**
S1.1-11	4. 機密セキュリティパラメータをセキュアに保存する	4-1. 製品のストレージにある機密セキュリティパラメータは、製品によってセキュアに保存されなければならない。	IoT製品のストレージに保存される守るべき情報資産（SDカード等、ストレージメディアに保存される守るべき情報資産も含む。）は、セキュアに保存されること。	【対象外（NA）となるための条件】 該当事項なし 【用語定義：守るべき情報資産】 以下のすべての情報： ・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・IoT機器の意図する使用において、IoT機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報	**適合（Y）**

★1適合基準番号	セキュリティ要件（大項目）	セキュリティ要件	☆1 適合基準	NAとなるための条件、基準の補足説明	評価結果
S1.1-12	5. セキュアに通信する	5-1. 製品は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。 5-7. 製品は、リモートアクセス可能なネットワークインタフェースを介して通信される重要なセキュリティパラメータの機密性を保護しなければならない。	ネットワーク経由で伝送される守るべき情報資産について、情報の盗聴に対する以下のいずれかの保護対策が行われていること。 ①他のIoT機器やサーバ（クラウド上のサーバを含む）へネットワークを介して伝送される守るべき情報資産について、情報の盗聴に対する保護対策をIoT機器自らが行う。 ②他のIoT機器やサーバ（クラウド上のサーバを含む）へネットワークを介して伝送される守るべき情報資産について、保護された通信環境（VPN環境や専用線を経由した接続環境）においてのみ伝送される。	【対象外（NA）となるための条件】 ネットワーク経由で伝送される守るべき情報資産が存在しない（「対象外（NA）であることの理由」に、ネットワーク経由で伝送される守るべき情報資産が存在しないことを示す根拠を記載すること） 【用語定義：守るべき情報資産】 以下のすべての情報： ・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・IoT機器の意図する使用において、IoT機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報	**適合（Y）**
S1.1-13	6. 露出した攻撃面を最小化する	6-1. すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。	IoT製品において、外部からサイバー攻撃を受けるリスクを低減するために、IoT製品の利用上不要かつ攻撃を受けるリスクがあるインタフェースを無効化するとともに、IoT製品に対する脆弱性検査を実施すること。具体的には、以下の①・②のすべての基準を満たすこと。 ①IoT製品において、高頻度で利用され、脆弱性などのリスクが想定される以下のインタフェースについて、IoT製品の利用上不要かつ攻撃を受けるリスクがあるインタフェースを無効化すること。 A)TCP/UDPポート B)Bluetooth C)USB ②IoT製品に対して脆弱性スキャンツールによる既知の脆弱性検査を実施し、攻撃に悪用される可能性がある脆弱性が検出されないこと。	【対象外（NA）となるための条件】 該当事項なし	**適合（Y）**
S1.1-14	9. 停止に対してレジリエントなシステムにする	9-1.データネットワークと電源の停止の可能性を考慮して、レジリエンスを製品とサービスに組み込まなければならない。	停電等による電力供給の停止やネットワークの停止により、IoT機器の電源がOFFになった後、電力供給が再開され、ネットワーク機能が復帰した際に、アクセス制御の際に使用する認証値（パスワード、秘密鍵など）の設定及びアップデートが完了したソフトウェアが工場出荷時の初期状態に戻ることなく、電源OFFになる直前の状態を維持できること。 なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けたIoT製品（技適[T]マーク又は[A]マークが付与されたIoT製品）は、本適合基準に適合しているとみなす。（この場合、「JC-STAR適合ラベル申請書」に「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）	【対象外（NA）となるための条件】 該当事項なし	**適合（Y）**
S1.1-15	11. ユーザが簡単にデータを消去できるようにする	11-1. ユーザが、簡単な方法で製品からユーザデータを消去できるような機能を提供しなければならない。	IoT製品利用中にIoT製品のストレージに保存されたデータの削除機能について、以下の①・②のすべての基準を満たすこと。 ①ユーザによって、IoT機器本体や必須付随サービス（モバイルアプリケーション等）を介して、ユーザに関する少なくとも以下のデータを削除できること。 A)IoT製品利用中に取得した情報資産（個人情報含む） B)ユーザ設定値 C)ユーザが設定した認証値、IoT製品利用中に取得した暗号鍵やデジタル署名 ②データ削除後も、アップデートされたセキュリティ機能に関するファームウェア（ソフトウェア）パッケージのバージョンは維持されること。	【対象外（NA）となるための条件】 該当事項なし	**適合（Y）**
S1.1-16	17. 製品に関する情報提供を行う	17-2. 製造業者は、製品をセキュアに設定・利用・廃棄する方法について、ユーザに提供しなければならない。 17-3. アップデートメカニズムが実装されている場合、製造業者は、セキュリティアップデートが必要であることを、そのアップデートによって軽減されるリスクに関する情報とともに、認識可能で明らかな方法でユーザに通知しなければならない。 17-5. 製造業者は、ユーザが製品を廃棄する手順について、指定された方法でユーザに提供しなければならない。 17-8. 製造業者は、定められたサポート期間を、ユーザにとって明確で透明性のある方法で公表しなければならない。 17-10. 製造業者は、セキュリティリスクを引き起こす可能性がある製品の利用状況に関する情報について、指定された方法でユーザに提供しなければならない。	製造業者は、IoT製品のサイバーセキュリティに関する情報提供について、以下の①～⑤のすべての基準を満たす対応を行うこと。 ①初期設定の方法など、IoT製品の利用上、サイバーセキュリティに影響が生じる設定や使用方法について、安全に利用できる手順を周知すること。 ②IoT製品のセキュリティアップデートのリリース時にそのアップデートの内容や必要性、アップデートを行わない場合の影響などを周知する仕組みがあること。 ③アップデートを行わなかったときに想定される事故や障害・一般的に想定される事故や障害に対して、免責事項を周知すること。 ④対象製品やサービスのサポート期限又はサポート終了時の方針を周知すること。 ⑤IoT製品内に守るべき情報資産が残留したまま廃棄や中古販売することで想定されるリスクや、データ消去を含むIoT製品の安全な利用終了方法を周知すること。	【対象外（NA）となるための条件】 該当事項なし 【用語定義：守るべき情報資産】 以下のすべての情報： ・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・IoT機器の意図する使用において、IoT機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報	**適合（Y）**