LACNOG-M³AAWG 共同作業による
顧客側通信機器 (CPE) が備えるべき
最低限のセキュリティ要件についての
Best Current Operational Practices
LAC-BCOP-1

May 2019

この文書の原文は LACNOG の Web サイト www.lacnog.net/docs/lac-bcop-1 で入手できます

この文書の原文は M³AAWG の Web サイト www.m3aawg.org/CPESecurityBP で入手できます

この文書は LACNOG[1] (Latin American and Caribbean Network Operators Group) と M³AAWG[2] (Messaging, Malware and Mobile Anti-Abuse Working Group) によって作成された共同の Best Current Operational Practices (BCOP)である。LACNOG のワーキンググループである LAC-AAWG[3] (Latin American and Caribbean Anti-Abuse Working Group) と BCOP Working Group[4]が作成した草案をもとに M³AAWG 会員と Senior Technical Advisor 及び M³AAWG 技術委員会との協調作業によって作成された。

目次

[1] Latin American and Caribbean Network Operators Group (LACNOG), https://www.lacnog.net/
[2] Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG), https://www.m3aawg.org/
[3] Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG), https://www.lacnog.net/lac-aawg/
[4] LACNOG BCOP Working Group, https://www.lacnog.net/wg-bcops/

エグゼクティブサマリ

CPE (Customer Premise Equipment: 顧客側通信機器) とは、利用者が自身の契約しているインターネットサービスプロバイダ (ISP) のネットワークに接続するために使用する通信機器を指す。CPE の例としてはモデム (ケーブルテレビ用、xDSL 用、光ファイバー用) や WiFi ルータなどがある。

ファームウェアやデフォルト設定の脆弱性によって、CPE は不適切に設定されたサービスやデフォルト設定の認証情報の悪用からマルウェアによる完全なセキュリティ侵害に至るまで、さまざまな不正利用の標的となっている。これらの多くの攻撃の目的には Denial-of-Service (DoS) 攻撃の実行、無許可の暗号通貨の採掘、マルウェアの頒布、スパム配信、フィッシング、認証情報の窃取などがある。

一般に、脆弱性には以下のようなものが含まれる。

- 多数のデバイスに共通の認証情報
- 変更不能な認証情報 (ハードコードされたもの)
- 危殆化等で既に非推奨となったセキュアでないプロトコルやアルゴリズムの使用
- 仕様にない方法によるアクセス (バックドア)
- セキュリティ上の問題を解決するための自動化されたセキュアなアップデート機構の欠如
- デフォルト設定で有効にされた不要あるいはセキュアでないサービス
- 無効にできないサービス
- セキュアでないリモートからの管理

この文書は、ISP が CPE を購入する際にそれらがセキュアな初期設定やリモート管理手法及びアップデート機構を持っていることを確認するためのセキュリティ要件の最小セットを明らかにすることを目的としている。この文書のゴールは、プロバイダのネットワークとインターネット全体の侵害リスクを低減し、サービスの品質低下や利用不能、技術サポートや復旧作業といった、攻撃者による機器の悪用によるコストと影響を最小限に抑えることである。

CPE がサポートしなければならない完全な機能セットあるいはハードウェア及びソフトウェアの仕様を提供することはこの文書の目的とするところではない。なお、この文書では便宜上、IPv6 プロトコルと IPv4 プロトコルはサポートされ実装され有効になっていることと仮定する [5]。

[5] CPE への要求仕様として IPv6 のサポートと実装に関する要件を含めないと、ISP が顧客に IPv6 接続を提供できない可能性があるため、ISP にとって事業リスクにつながる恐れが生じます。これは、IPv4 アドレスの枯渇による、事業成長に対するリスクとなります。

1. 用語について

この文書で使われている用語の定義について以下に記す。

1. CPE (Customer Premise Equipment: 顧客側通信機器): 顧客がインターネットサービスプロバイダ (ISP) のネットワークに接続するために使用する通信機器。この種の機器は、「カスタマーエッジ (CE) ルータ」、「住宅用ゲートウェイ (RG)」等と呼ばれることもある。

2. ファームウェア: CPE 上で稼働するソフトウェアでオペレーティングシステム及びネットワークインターフェースソフトウェアやサービスのソフトウェアとその設定を含む。

3. バックドア: システムやデータに対する本来の仕様にはないアクセスを可能にする全ての仕組み。バックドアの事例としては、パスワードなしで機能するハードコードされたユーザ名、固定されたパスワードや予測可能な「password-of-the-day (その日のパスワード)」、認証なしで管理機能を実行するサービスなどがある。バックドアは意図的に (後からアクセスできるように設計されたもの)、または意図せずに (開発目的で使用された後、不用意に製品ファームウェアに混入してしまうなど) 組み込まれることがあるほか、不適切なプログラミング手法の結果として発生する可能性もある。

4. 適切な暗号化/暗号手法: Internet Engineering Task Force (IETF) あるいは他の標準化団体によって公開されている最新のバージョンのオープンスタンダードな暗号化アルゴリズム/プロトコル。その実装では、最新の暗号スイートや鍵長を選択することを許可しなければならない。

5. ハードコードされた認証情報: ソースコードにパッチを適用すること (その結果として新しいバイナリ/ファームウェアをリリースすること) 以外では変更も無効化もできない、製品のソースコードに共通の値として固定された認証情報 (その製品の全ての実装で共通)。

6. サービス (サーバ型プロセスまたは daemon プロセス): 必要に応じてサービスへのクエリを実行するクライアントソフトウェアではなく、特定のポートでアクティブに接続を待つサーバプロセス。

7. DEFAULT: ベンダーによってセットされるデフォルト設定。

8. この文書中で使用される"MUST"、"MUST NOT"、"REQUIRED"、"SHALL"、"SHALL NOT"、"SHOULD"、"SHOULD NOT"、"RECOMMENDED"、"NOT RECOMMENDED"、"MAY"、"OPTIONAL"等のキーワードは、ここに書かれたように全て大文字で文章中に書かれている場合に限り、BCP 14 RFC 2119 [2]、及び RFC 8174 [3] に記述されているように解釈される。

2. 一般的要件 (General Requirements-GR)

GR-01: デバイスの説明にはその主要コンポーネントの識別情報を含めなければならない (MUST)。具体的には以下のとおり。

a. 製造元、モデルとチップセットのバージョン
b. ファームウェアと基本オペレーティングシステムの名称、バージョン及びリリース日

GR-02: ベンダーは最低でも以下を記述した資料を提供しなければならない (MUST)。

a. ファームウェアあるいは基本オペレーティングシステムの名称、機能、バージョン及びリリース日
b. デバイスに実装されている全てのアプリケーションとサービスの名称、バージョン、リリース日と工場出荷時の起動ステータス (例: 初期設定で on になっているか off になっているか、等)

GR-03: ベンダーは使用されている全てのオープンソースソフトウェアについて次の情報を提供しなければならない (MUST)。

a. 使用されているそれぞれのオープンソフトウェアに関連する全てのライセンスの一覧
b. CPE システムに組み込まれているそれぞれのオープンソースソフトウェアの完全な名称とバージョン

GR-04: 脆弱性開示のための連絡先情報 (VR-03) は CPE のグラフィカルユーザインターフェース (GUI) のどこか (例: ページ、タブ、等) に含まれるべき (SHOULD)。

GR-05: ベンダーは、CPE がサポート期間を終え (VR-01、VR-02 参照)、以後ファームウェアのアップデートを受けることがない場合に、ユーザに対して (例えば GUI を介して) 情報を提供すべき (SHOULD)。

3. ソフトウェアのセキュリティについての要件 (Software Security Requirements-SSR)

SSR-01: 認証情報はハードコードしてはならない (MUST NOT) 。FR-04、FR-05 も参照。

SSR-02: デバイスに保存される機微な認証情報 (例: パスワード、鍵、セキュリティトークン、等) は適切なハッシュ化/暗号化アルゴリズムによって保護されなければならない (MUST)。暗号化鍵は可能であればセキュアなハードウェアに保存されるべき (SHOULD)。

SSR-03: デバイスに保存される一般データは適切な暗号化で保護されるべき (SHOULD)。

SSR-04: ファームウェアかシステム開発に使われたすべてのソフトウェアツールやバックドアは大量生産バージョンでは削除されなければならない (MUST)。

4. アップデートと管理についての要件 (Update and Management Requirements-MR)

MR-01: CPE は最低でも適切な暗号化プロトコルを利用したリモート管理の仕組みを実装しなければならない (MUST)。要求されるプロトコル一覧については、付録 1 でチェックのこと。

MR-02: CPE はセキュアなリモートアップデートの仕組みを実装しなければならない (MUST)。要求されるプロトコル一覧については、付録 1 でチェックのこと。

MR-03: リモート管理とリモートアップデートの仕組みは以下の全てをサポートしなければならない (MUST)。

a. セキュアな認証
b. 暗号化された接続
c. 特定の接続元に限るアクセス制限 (例: 選択されたネットワークセグメント、 特定の URL、等)
d. 接続ポートを選択する自由度 (DEFAULT のポート番号またはサービスに割り当てられたポート番号から接続ポート番号の変更が可能であること [17])

MR-04: 自動化されたセキュアなアップデートの場合、ソースリポジトリを認証し検証する仕組みを実装しなければならない (MUST)。

MR-05: CPE において、実際に (通常はフラッシュメモリ内で) アップデートを実行する前に、ダウンロードされたファイルの完全性と制作者を検証し、そのファイルがそのデバイスのためのものであるかどうか (デバイスのアーキテクチャ、モデル、バージョンなどに対応しているかどうか) を検証する仕組みを実装しなければならない (MUST)。

MR-06: アップデート処理では既存の設定を保存しなければならない (MUST)。ベンダーは設定変更がデバイスのセキュリティを改善する場合には既存設定を変更してもよい (MAY)。そのような変更は明確に文書化されなければならない (MUST)。

MR-07: アップデートの確認に関する CPE の要件は以下のとおり。

a. 自動化されたスケジュールベースで、アップデートを定期的にチェックする能力を持たなければならない (MUST)。
b. ユーザがアップデートのチェックを開始できるようにしなければならない (MUST)。
c. オンデマンドベースで、ISP 主導のプッシュ型アップデートをサポートすべき (SHOULD)。

MR-08: CPE はファームウェアアップデートの失敗の結果、機器が使用不能になること (文鎮化) を防ぐ仕組みを実装しなければならない (MUST)。復旧手順は明確に文書化され

なければならず (MUST)、ハードウェアの内部の部品にアクセスすることを要求してはならない (MUST NOT)。

5. 機能についての要件 (Functional Requirements-FR)

この文書は RFC 7084 [8] に従った IPv6 サポートが一般的な購買要件文書の一部であることを想定している。

CPE でサポートすべき機能、CPE から除外すべき機能は以下のとおり。

FR-01: CPE は機密情報の開示を許可したり、増幅攻撃のために悪用され得る、デフォルト設定 (DEFAULT) で WAN を利用するサービス (例: Telnet、FTP、SOCKS、CHARGEN、SNMP、等) を有効にしてはならない (MUST NOT)。

FR-02: CPE はこの文書の アップデートと管理についての要件 (MR) の章に書かれているリモートアップデートとリモート管理の機能を実装しなければならない (MUST)。

FR-03: LAN/WAN から CPE へのすべてのエンドユーザ管理の通信は、必ず認証を経なければならず (MUST) [6]、かつ、暗号化されるべき (SHOULD)。

FR-04: 全ての認証情報 (例: パスワード) はマスター管理 (root) のパスワードを含めて変更可能でなければならない (MUST)。ユーザ識別情報 (例: ユーザ名) は変更可能であるべき (SHOULD)。

FR-05: 管理インターフェースへのアクセスのためのパスワードに関する要件は以下のとおり。

a. 初期パスワードはそれぞれのデバイスに対して一意でなければならない (MUST)。また、パケットキャプチャやその類いの観測方法で得られる情報 (例: MAC アドレス) から導出されるものであってはならない (MUST NOT)。

b. パスワードが変更あるいはリセットされる全ての過程において、パスワードが空 (empty あるいは blank) あるいはユーザ名と同じになることがあってはならず (MUST NOT)、また、パスワードの複雑さに対するベストプラクティスに従わなければならない (MUST)。

FR-06: 製品版のファームウェアはシステムやデータへのアクセスのための文書に記されていない仕組みを持ってはならない (MUST NOT)。

FR-07: デバイスはベンダーや第三者にデータを送信する仕様にない仕組みを持ってはならない (MUST NOT)。ベンダーや第三者に対する通信や送信されるデータは明示的に文書に記されなければならない (MUST) [7]。

---

[6] CPE は、ユーザ名/パスワードによる単純な認証の代わりに、より高度なセキュリティを提供する認証機構をサポートしてもよい。

[7] 多くの国/地域におけるデータ保護法においては、個人データの処理に関する特別な要件を定めており、それらを詳細かつ明示的に文書化することが要求される場合がある。

FR-08: 認証されたエンドユーザは GUI から以下の全てのことができなければならない (MUST)。

a. ユーザ固有の設定 (例: WiFi ネットワーク名、ファイアウォールやパケットの転送ルール、等) を適切に変更すること
b. デバイスの操作または管理に不必要なサービスを無効にすること

FR-09: CPE の LAN/WAN インターフェース上でユーザに対してサービスの操作を可能にする場合、それらのサービスは WAN/Internet からアクセスできるものであってはならない (MUST NOT)。具体的には、DNS、NTP、SSDP、UPnP やその他トラフィック増幅攻撃に使われる可能性があるプロトコルでのサービス等が該当する。

FR-10: モニタリングや管理のためのサービス/エージェントを使用する際の要件は以下のとおり。

a. 値の設定及び/または情報・機密データを取得するための適切な認証の仕組みの設定が要求されなければならない (MUST)。
b. WAN インターフェースからのアクセスは認証を使用しなければならない (MUST)。また特定の接続元 (例: 選択されたネットワークセグメントかアドレス) からのアクセスに制限されなければならない (MUST)。

FR-11: デバイスは暗号スイートと鍵長について安全なパラメータを選択できる、現在のバージョンのオープンスタンダードベースの暗号化方法を実装しなければならない (MUST)。

FR-12: デバイス認証のための鍵と電子証明書の生成に関連する暗号化サービスあるいはアプリケーションはデバイスごとに異なる鍵を生成しなければならない (MUST)。例えば秘密鍵は異なるデバイスで共用してはならない (MUST NOT)。

FR-13: CPE は Network Time Protocol (NTP) のような従属同期型プロトコルによる時刻同期をサポートしなければならない (MUST)。NTP クライアントのみのソフトウェアが必要である。CPE は NTP サーバについてハードコードされた設定を持ってはならない (MUST NOT)。またベンダーが利用許可を得ていないサーバをデフォルト設定 (DEFAULT) に使用してはならない (MUST NOT)。

FR-14: CPE は RFC 6092 "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service"[6] をサポートすべき (SHOULD)。RFC6092 とこの文書の間に矛盾がある場合はこの文書の要件が優先される。

FR-15: CPE は IPv4 と IPv6 の両方で BCP38/RFC2827 [12] に従った送信元アドレスの詐称対策のフィルタリングをサポートしなければならない (MUST)。それはデフォルト設定

(DEFAULT) によって有効にされる選択可能なオプションでなければならない (MUST)。送信元 IP アドレスの検証方法の決定はこの文書のスコープに含まれない。

FR-16: CPE は 特別な目的を持つ IP アドレスに対するパケットフィルタリングをサポートすべき (SHOULD)。RFC 6890 [13] と RFC 8190 [14]に従って、"Globally Reachable" FALSE かつ"Forwardable" FALSE なアドレスはフィルタされるべき (SHOULD)。この場合、CPE は IANA (Internet Assigned Numbers Authority) によって管理されている“IANA IPv4 Special-Purpose Address Registry” [15] と“IANA IPv6 Special-Purpose Address Registry” [16] に従った IPv4 と IPv6 のアドレスを含めて設定できるような能力を持つべき (SHOULD)。

FR-17: CPE はオープンリゾルバとして振る舞ってはならない (MUST NOT)。DNS サービスに関する要件は以下のとおり。

a. WAN ポートで受信され CPE 自体に向けられた DNS クエリはいかなる場合も許可または応答されてはならない (MUST NOT)

b. WAN ポートで受信され、LAN ポートに転送されることを意図した DNS クエリは、CPE の設定に明示的な規則 (例: 転送規則、ファイアウォール規則、等) が存在する場合に限り、許可されることがある (MAY)。[8]

c. CPE がローカルな DNS サーバを実行している場合、そのサーバが外に送出する DNS クエリに関して DNSSEC 検証を実施するよう設定すべき (SHOULD)。

d. CPE がローカルな DNS サーバを実行せず、代わりに DNS クエリを別のサーバに転送する場合、DNS クエリに DNSSEC 検証のマークがある場合はそれを削除してはならない (MUST NOT)。

FR-18: WiFi が提供される場合の CPE の要件は以下のとおり。

a. 適切な暗号化を用いたセキュリティ機構を実装しなければならない (MUST)。

b. 最新バージョンの Wi-Fi Protected Access (WPA)® セキュリティ機能仕様をサポートすべき (SHOULD)。

FR-19: 全ての管理インターフェースでは、デフォルト設定 (DEFAULT) でパスワードがクリアテキストとして表示されてはならない (MUST NOT)。パスワードはユーザが要求した場合には可視化されてもよい (MAY)。

FR-20: デバイスの設定を、全ての機密情報 (例: パスワード、SNMP 等のコミュニティ文字列、等) を削除した上でクリアテキストフォーマット (ASCII か UTF-8) でダウンロードする方法を用意すべき (SHOULD)。

[8] CPE は、ユーザが LAN 内で DNS サーバをホスティングすることを妨げるべきではない。この場合の転送規則/ファイアウォール規則は、権威 DNS サーバが LAN 内で実行しているがために意味を成すものである。

6. 初期設定についての要件 (Initial Configuration Requirements-IR)

デバイスは以下の工場出荷時初期設定を持たなければならない (MUST)。

IR-01: CPE は許容的に設定されるよりはむしろ制限的に設定されなければならない (MUST)。 初期設定のプロセス (bootstrapping) に厳密に必要とされない全てのサービス (サーバ型プロセス) は無効にされなければならない (MUST)。具体的には、(実装があれば) SSDP、SNMP、UPnP、SOCKS、SMB、帯域テスト (ergo に埋め込まれた iperf など) 等が該当する。加えて、有効になっているか有効にすることができるサービスは、制限的で安全な初期設定モードで動作すべき (SHOULD)。

IR-02: DNS サーバアドレスに関連するパラメータ (リゾルバのアドレス) は未設定でなければならない (MUST)。また DNS リレーオプションは (実装されている場合には) 無効でなければならない (MUST)。

IR-03: ポートフォワーディングや DMZ ホストオプションは、利用可能な場合には、デフォルト設定 (DEFAULT) では無効でなければならない (MUST)。

IR-04: グラフィカルなものとコマンドライン両方の管理インターフェースにアクセスするための初期パスワードはデバイスごとに固有でなければならない (MUST)。またデバイスラベル上で視認できなければならない (MUST)。

IR-05: WiFi が提供される場合、WiFi ネットワークはその SSID とは異なる固有の初期パスワードを持たなければならない (MUST)。そしてそれはデバイスラベル上で視認できなければならない (MUST)。そのパスワードはデフォルト設定 (DEFAULT) の管理パスワードとは異なるものにすべき (SHOULD)。

IR-06: WiFi が提供される場合、WiFi の Service Set Identifier (SSID) のデフォルト設定 (DEFAULT) 値はベンダー名や製品名に関連したものであってはならない (MUST NOT)。またそれはカスタマイズ可能でなければならない (MUST)。ISP でカスタマイズされる初期設定値については [9]、付録 1 の表で確認のこと。

IR-07: SSH サービスの場合、サーバ鍵のペアは工場で事前に生成されたものであってはならない (MUST NOT)。鍵は最初のサービスの初期化と起動の後に生成されなければならず、またデバイスの工場出荷時設定へのリセット後には新たな鍵が生成されなければならない (MUST)。生成された鍵ペアはサービスへの適用時点でセキュアと見なすに十分なセキュリティ強度を提供すべき。

IR-08: 送信元の詐称を防ぐフィルタリング [FR-15] はデフォルト設定 (BY DEFAULT) で有効でなければならない(MUST)。

[9] 初期設定(BY DEFAULT)で SSID がどう設定されるか（例：全てのデバイスで同一の ID またはデバイスごとに固有の ID）を ISP が決めたい場合には、どのように設定されなければならないかをベンダーに説明する必要がある(MUST)。さもなければ、ベンダーの初期設定(DEFAULT)が選択される場合がある。

IR-09: IPv6 移行メカニズム、トンネル、VPN や同様なサービスはデフォルト設定 (DEFAULT) では無効でなければならない (MUST)。

7. ベンダーについての要件 (Vendor Requirements-VR)

ベンダーに関する要件は以下のとおり。

VR-01: 販売終了日より後の期間を含め、特にセキュリティ脆弱性の修正の入手可能性について、明確な製品サポートポリシーを持たなければならない (MUST)。

VR-02: 最低でもデバイスを販売している間はセキュリティ脆弱性の修正を提供しなければならない (MUST)。ベンダーは製品の販売終了日から 3 年間セキュリティ脆弱性の修正の提供を継続すべき (SHOULD)。

VR-03: ISP の顧客、エンドユーザ、第三者 (研究者など) が製品に発見されたセキュリティ脆弱性を報告できるコミュニケーションチャネル/連絡先を含む、連携のとれた脆弱性の開示能力を持たなければならない (MUST)。理想的には製品セキュリティインシデント対応チーム (PSIRT) を持つべき (SHOULD)。

VR-04: 事前登録やアカウントを必要としない誰でも利用可能なサポートチャネルを持ち、英語の Web サイトを通じて最低でも下記を提供しなければならない (MUST)。

a. その製品に関連する既存の脆弱性、緩和策、セキュリティ修正の通知
b. その製品に関連するセキュリティ修正や新しいバージョンのファームウェア、ソフトウェアの提供
c. デバイスの設定、アップデートとセキュリティに関するマニュアルやその他の資料の提供

8. 略語一覧

BCOP: Best Current Operational Practices

BBF: Broadband Forum

CE: Customer Edge Router

CPE: Customer Premises Equipment (顧客側通信機器)

CWMP: CPE WAN (Wide Area Network) Management Protocol

IANA: Internet Assigned Numbers Authority

ISP: Internet Service Provider

PSIRT: Product Security Incident Response Team (製品セキュリティインシデント対応チーム)

RG: Residential Gateway (住宅用ゲートウェイ)

SSID: Service Set Identifier

WLAN: Wireless LAN (Local Area Network)

9. 謝辞

多くの人たちが Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG)での草案の作成から公開に至るまでの間、この文書の作成に貢献してくださいました。著者陣は多くの有益な指摘、いくつかのケースでの詳細なレビューの提供に対し、貢献者全員に感謝の意を表します。貢献者 (アルファベット順) は次の方たちです。
Nicolas Antoniello, John Brown, Dennis Dayman, Carmen Denis, Yuri Ferreira, Alexandre Giovaneli, Steve Goeringer, Cristine Hoepers, Markus Lintula, Jason Livingood, Art Manion, Jordi Palet Martínez, Roney Medeiros, Luciano Minuchin, Eduardo Barasal Morales, Massimiliano Pala, Ricardo Patara, Nathalia Sautchuk Patrício, Fernando Quintero, Marcelo Batista Sarmento, Joe St Sauver, Klaus Steding-Jessen, Italo Valcy, Severin Walker, Ariel Weher, Gilberto Zorello, Jan Žorž.

特に次の方たちには心より感謝いたします。

- Lucimara Desiderá (LAC-AAWG 共同設立者、著者/編集者)
- Christian O'Flaherty (LAC-AAWG 共同設立者)
- LACNOG BCOP Working Group コミュニティとそのチェア: 文書化とレビュープロセスのサポート
- LACNIC WARP (Warning Advice and Reporting Point) of the Latin American、Caribbean Internet Address Registry (LACNIC): 会議インフラの提供
- The Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG): LAC-AAWG のイニシアチブのサポートとこの文書のテクニカルレビューの受け入れ

10. 参考情報

[1] Abuse of Customer Premise Equipment and Recommended Actions
https://resources.sei.cmu.edu/asset_files/WhitePaper/2014_019_001_312679.pdf

[2] Key words for use in RFCs to Indicate Requirement Levels, BCP 14, RFC 2119
http://www.rfc-editor.org/info/rfc2119

[3] Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words, RFC 8174
https://tools.ietf.org/html/rfc8174

[4] Internet Security Glossary, Version 2, RFC 4949
https://tools.ietf.org/html/rfc4949

[5] Common Security Requirements for IP-Based MSO-Provided CPE - Version I01
https://apps.cablelabs.com/specification/common-security-requirements-for-ip-based-mso-provided-cpe

[6] Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service, RFC 6092
https://tools.ietf.org/html/rfc6092

[7] Data-Over-Cable Service Interface Specifications DOCSIS® 3.1, Security Specification, CM-SP-SECv3.1-I07-170111
https://apps.cablelabs.com/specification/CM-SP-SECv3.1

[8] Basic Requirements for IPv6 Customer Edge Routers, RFC 7084

https://tools.ietf.org/html/rfc7084

[9] Functional Requirements for Broadband Residential Gateway Devices, TR-124 Issue 5
https://www.broadband-forum.org/technical/download/TR-124_Issue-5.pdf

[10] CPE WAN Management Protocol, TR-069 Issue 1 Amendment 6
https://www.broadband-forum.org/technical/download/TR-069.pdf

[11] IPv4 and IPv6 eRouter Specification CM-SP-eRouter-I19-160923
https://apps.cablelabs.com/specification/ipv4-and-ipv6-erouter-specification/

[12] Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, BCP 38, RFC 2827
https://tools.ietf.org/html/rfc2827

[13] Special-Purpose IP Address Registries, BCP 153, RFC 6890
https://tools.ietf.org/html/rfc6890

[14] Updates to the Special-Purpose IP Address Registries, BCP 153, RFC 8190
https://tools.ietf.org/html/rfc8190

[15] IANA IPv4 Special-Purpose Address Registry
https://www.iana.org/assignments/iana-ipv4-special-registry

[16] IANA IPv6 Special-Purpose Address Registry
https://www.iana.org/assignments/iana-ipv6-special-registry

[17] Service Name and Transport Protocol Port Number Registry
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

[18] Addressing the challenge of IP spoofing
https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-AntiSpoofing-20150909-en-2.pdf

[19] ISO/IEC 29147:2014 Information technology - Security techniques - Vulnerability disclosure
https://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip

[20] BSI TR-03148: Secure Broadband Router
Requirements for a secure Broadband Router Version: 1.0
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf?__blob=publicationFile&v=2

付録 1 – 要件の一覧表

以下の表はこの文書で提示されている要件セットをまとめたものであり、組織 (ISP など) が RFP を準備したり、ベンダーから求められる要求仕様を指定するのに役立ちます。

その要求仕様が「必須」である場合をはじめ、いくつかの欄はすでに推奨設定で埋められていますが、多くの要求仕様についてはその組織がその設定が必要かどうかを決定し、デフォルト設定 (DEFAULT) を定義する必要があります。

この文書に記載された項目は最低限のセキュリティ要件であり、低い方のレベルへの選択 (例えば、「必須」から「推奨」または「任意」の実装への選択) は行わないよう、強く推奨します。可能な限り、最も高いオプションへの選択を行ってください。

一般的要件 (GR)		
要件	**M 必須** **R 推奨** **O 任意**	**デフォルト設定値**
GR-01	M	
GR-02	M	
GR-03	M	
GR-04	R	脆弱性情報の開示についての連絡先がグラフィカルユーザインターフェース上にあること
GR-05	R	アップデート状況の表示
ソフトウェアについてのセキュリティ要件 (SR)		
要件	**M 必須** **R 推奨** **O 任意**	**デフォルト設定値**
SSR-01	M	
SSR-02	M	機密情報が保護されていること
SSR-03	R	
SSR-04	M	開発ツールやバックドアが削除されていること

アップデートと管理についての要件 (MR)		
要件	**M 必須** **R 推奨** **O 任意**	**デフォルト設定値**
MR-01	M (a)	(a)
MR-02	M (b)	(b)
MR-03	a. M b. M c. M d. M	(c)
MR-04	M	
MR-05	M	
MR-06	M	
MR-07	a. M b. M c. R	
MR-08	M	
機能についての要件 (FR)		
要件	**M 必須** **R 推奨** **O 任意**	**デフォルト設定値**
FR-01	M	Telnet、FTP、SOCKS、CHARGEN、SNMP が無効になっていること
FR-02	M	(c)
FR-03	M: 認証 R: 暗号化	
FR-04	M	
FR-05	a. M b. M	デバイスごとに固有の初期パスワード
FR-06	M	

FR-07	M	
FR-08	a. M b. M	
FR-09	M	DNS、NTP、SSDP、UPnP が WAN からアクセスできないこと
FR-10	a. M b. M	(d)
FR-11	M	
FR-12	M	
FR-13	M	NTP クライアントのみ。設定をハードコードしないこと
FR-14	R	
FR-15	M	送信元詐称防止フィルタが有効なこと
FR-16	R	未設定 (e)
FR-17	a. M b. R c. R d. M	b. 転送規則が有効でないこと
FR-18	a. M b. R	適切な暗号化が有効なこと
FR-19	M	
FR-20	R	

初期設定値についての要件 (IR)

要件	**M 必須** **R 推奨** **O 任意**	**デフォルト設定値**
IR-01	M	SSDP、SNMP、UPnP、SOCKS、SMB、帯域テストが無効であること
IR-02	M	事前設定された DNS サーバのアドレスが存在しないこと。また DNS リレーが無効であること

IR-03	M	無効であること
IR-04	M	(f)
IR-05	M	(f)
IR-06	M	(g)
IR-07	M	事前生成された SSH 鍵が存在しないこと
IR-08	M	有効であること
IR-09	M	移行メカニズム、トンネル、VPN が無効であること
ベンダーについての要件 (VR)		
要件	**M 必須 R 推奨 O 任意**	**デフォルト設定値**
VR-01	M	
VR-02	M	
VR-03	M	
VR-04	M	

(a) ISP はデバイスをリモート管理する能力を持たなければなりません (例: 設定のため等)。プロバイダが使用しているテクノロジ (ケーブルテレビ用、光ファイバー用、xDSL 用) によりますが、関連する産業は既に特有のプロトコルを持っている可能性もあります。この項目で、ISP はそのテクノロジに応じてデバイスでサポートされなければならないプロトコル (例: ブロードバンド用の BBF TR-069 CWMP 等) を選択し、デフォルト設定 (DEFAULT) でそれを有効にするか、さらに必要なデフォルト設定を選択する必要があります。複数のプロトコルをサポートする必要がある場合、ISP はそれら全てをこの項目に含める必要があります。

(b) ISP はデバイスをリモートでアップデートする能力 (主にファームウェア) が必要です。プロバイダが使用しているテクノロジ (ケーブルテレビ用、光ファイバー用、xDSL 用) によりますが、関連する産業は既に特有のプロトコルを持っている可能性もあります。この項目で、ISP はそのテクノロジに応じてデバイスでサポートされなければならないプロトコル (例: ブロードバンド用の BBF TR-069 CWMP 等) を選択し、デフォルト設定 (DEFAULT) でそれを有効にするか、さらに必要なデフォルト設定を選択する必要があります。複数のプロトコルをサポートする必要がある場合、ISP はそれら全てをこの項目に含める必要があります。

(c) CPE と管理・アップデートサーバの間のトランザクションで最低限のアクセス制限の仕組み、機密保持、完全性のチェックがされなかった場合、しばしばプロバイダのインフラストラクチャが侵害される結果になり得ます。全てのアクセスで暗号化された接続 (例: TLS/HTTPS) を使用し、全てのデバイスに対して事前定義された単一のユーザ名/パスワードに依らない認証とアクセスを特定の接続元 (例: 選択されたネットワークセグメントや特定の URL 等) に制限することを強く推奨します。

(d) ISP が監視や管理サービス/エージェントをデフォルト設定 (DEFAULT) で有効にしたい場合は、認証とネットワークアクセス制限に適切なパラメータを提供する必要があります。

(e) ISP が CPE で直接 Special-Purpose IP Addresses に対するフィルタリングを実装したい場合、デフォルト設定 (DEFAULT) でフィルタされる prefix のリストを提供できます。そうでないと、フィルタリングのデフォルト設定 (DEFAULT) が「未設定」になり、CPE はどの prefix に対してもフィルタを適用できません。

(f) ISP が初期パスワードがどのように設定されるかをカスタマイズしたい場合、ISP はベンダーにパスワード選択プロセスについて情報提供する必要があります。そうでないとベンダーは初期値(DEFAULT)としてランダムに固有の値を設定するかもしれません。

(g) ISP が WiFi ネットワーク名をカスタマイズしたい場合、ISP はどのように WiFi 識別子 (SSID) を設定するか情報提供する必要があります。そうでないとベンダーはベンダーが選んだ初期値を選択するかもしれません。

この文書は産業界への貢献と LAC-AAWG と M³AAWG の著者陣に敬意を表すことを目的に Broadband Security, Inc.が和訳したものです。https://www.bbsec.co.jp/

LACNOG-M³AAWG が発行する全ての文書と同様に、アップデートに関しては M³AAWG の Web サイト (www.m3aawg.org) あるいは LACNOG の Web サイト(www.lacnog.net)を確認してください。