IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2010 年 9 月 7 日
独立行政法人情報処理推進機構

「組込みシステムのセキュリティへの取組みガイド（2010 年度改訂版）」を公開
～情報家電で利用が拡大する IPv6 等の新技術を安全に利用する上で考慮すべき対応策を掲載～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、ネットワークへ接続する組込みシステムのセキュリティ対策推進のため、IPv6 等の新技術への対応策等について追記した「組込みシステムのセキュリティへの取組みガイド（2010 年度改訂版）」を、2010 年 9 月 7 日（火）から、IPA のウェブサイトで公開しました。本ガイドを活用することにより、情報家電を含む組込みシステムのセキュリティへ取り組むための、具体的な指針を得ることができます。
URL：http://www.ipa.go.jp/security/fy22/reports/emb_app2010/index.html

【改訂の背景】

近年、インターネット接続機能を持つデジタルテレビ等の情報家電の普及が進んでいます。ネットワークにつながる組込みシステムは、PC と同じくネットワークを介した脅威にさらされる恐れがあります。IPv6[1]や NGN[2]等の新しいネットワーク環境が整備されつつある中で、ネットワークに接続される組込みシステムのセキュリティを確保するための対応策普及のため、「組込みシステムのセキュリティへの取組みガイド」を改訂し、公開しました。

【主な改訂点】

(1) 「新技術への対応」を追加

組込みシステムに今後取り入れられると考えられる新技術について、必要とされるセキュリティへの対応策を追加しました。特に、IPv6 技術の利用については下記のような対応策が考えられます。

■グローバルな IP アドレスに対する保護

IPv6 技術ではアドレス空間の拡大により、ネットワークに接続するあらゆる機器に世界で唯一かつ固定的な IP アドレスを割り当てることが可能になります。これにより、攻撃者が組込みシステムを特定しやすくなり、特定の組込みシステムを狙って攻撃する可能性が高まります。

＜対策＞

組込みシステムに対して、脆弱性対策等の IPv4 と同様のセキュリティ対策を実施すると同時に、IPA が提供している「TCP/IP に係る既知の脆弱性検証ツール」[3]のような、IPv6 の脆弱性検証にも対応しているツールを用いてセキュリティ検証を行う必要があります。また、IPv6 への移行は段階的に進むと考えられるため、多くの組込み機器が IPv6 と IPv4 の両方の機能を持つと考えられます。そのような場合には、両機能に対するセキュリティ対策を実施する必要があります。

■IPv6 特有のアドレス付与方式による攻撃機会の増加への対策機能

IPv6 を利用した機器がネットワークに接続する際、IP アドレスの一部に装置ベンダ特有の情報が組み込まれる場合があります。これは、組込みシステムの利用しているハードウェアを特定す

---

[1] IPv6（Internet Protocol version 6）
ネットワーク規格の一つ。約 340 澗個（43 億の 4 乗個）の IP アドレスが用意されており、IPv4 アドレスの枯渇対策として、IPv6 アドレスへの移行が進められている。

[2] NGN（Next Generation Network）
IP（Internet Protocol）をベースとして、誰もがいつでもどこでも、アクセス手段に依存することなく、データ通信や情報提供サービス、認証サービスなどを享受できるマルチサービスの基幹インフラストラクチャ。

[3] TCP/IP に係る既知の脆弱性検証ツール
IPA が無償で貸出している、IPv4 環境で 19 項目、IPv6 環境で 5 項目の脆弱性を体系的に検証できるツール。
http://www.ipa.go.jp/security/vuln/documents/2009/200901_vuln_TCPIP.html

る情報として、攻撃者が特定の機器の脆弱性をついた攻撃を行う際の参考情報として利用される可能性があります。

＜対策＞

ネットワークに接続する組込みシステムの開発時に、機器が推測されないアドレスを用いる、通信に応じて適宜アドレスを変更する等の機能を実装する必要があります。

(2) 組込みシステム開発組織等へのヒアリング結果を反映

2009 年 6 月に公開した本ガイドについて、デジタルテレビ等の組込みシステムの開発組織やネットワーク関連組織等にヒアリングを実施して現場の声を取り入れ、より製品開発者が理解しやすくなるように内容の整理を行いました。また、既に下記項目について、ヒアリングにより明らかになった組込みシステム開発を行う上での考慮点を追加しました。

■製品の長期利用
■オープンソースの利用
■暗号の危殆化
■開発工場における PC 管理

【本ガイドの活用法】

組込みシステムのセキュリティ対策を確実に実行するには、製品の技術的な対策だけでなく、製品開発企業が組織として、製品のライフサイクル（企画・開発・運用・廃棄）全体を通して取り組むことが必要となります。本ガイドでは、組込みシステムのライフサイクルの各フェーズについて、セキュリティを考慮すべき具体的な取組み項目を 16 個設定し、各項目について 4 つのレベルを設定しています。本ガイドを参考に自組織の「セキュリティへの取組み」のレベルを把握し、上位のレベルを目指すことで、よりセキュアな製品の開発が可能になります。

IPA では、本ガイドが、安心・安全な組込みシステムの開発に寄与し、情報セキュリティ上の脅威が減少することを期待するとともに、今後も組込みシステムのセキュリティに関して、「IPv6 普及・高度化推進協議会」[4]、「IPv6 技術検証協議会」、「社団法人 組込みシステム技術協会」[5]等の関係団体等と協力の下、利用者やメーカー、サービス事業者の情報リテラシー向上に向けた活動を継続していきます。

本書（全 50 ページ）は、次の URL よりダウンロードの上、ご参照ください。

URL：http://www.ipa.go.jp/security/fy22/reports/emb_app2010/index.html

■ 本件に関するお問い合わせ先
IPA　セキュリティセンター　小林／中野／長谷川
Tel : 03-5978-7527　Fax : 03-5978-7518　E-mail : vuln-inq@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA　戦略企画部広報グループ　横山／大海
Tel : 03-5978-7503　Fax : 03-5978-7510　E-mail : pr-inq@ipa.go.jp

[4] IPv6 普及・高度化推進協議会
http://www.v6pc.jp/jp/index.phtml
[5] 社団法人 組込みシステム技術協会（Japan Embedded Systems Technology Association）
http://www.jasa.or.jp/top/