IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2008 年 1 月 29 日
独立行政法人 情報処理推進機構

「複数の組込み機器の組み合わせに関するセキュリティ調査報告書」の公開について
～情報家電、カーナビ、携帯電話の連携時に潜む脅威と対策を整理～

独立行政法人 情報処理推進機構（略称：IPA、理事長：藤原 武平太）は、組込みシステムの情報セキュリティ対策を推進するため、3 分野（情報家電、カーナビ、携帯電話）の組込みシステムの連携時におけるセキュリティ課題の調査を行い、「複数の組込み機器の組み合わせに関するセキュリティ調査報告書」として 2008 年 1 月 29 日（火）より、IPA のウェブサイトで公開しました。
（URL：http://www.ipa.go.jp/security/fy19/reports/embedded/index.html）

「複数の組込み機器の組み合わせに関するセキュリティ調査研究」では、今後利用が拡大すると予測される、複数の組込み機器が組み合わさって利用される環境でのセキュリティ課題の調査を行いました。調査対象として「情報家電」「カーナビ」「携帯電話」を取り上げ、これらの組込み機器がネットワーク等を利用して組み合わせて使われる事を想定しています。今回の調査では、様々な利用シナリオやそこに発生する脅威を洗い出し、組込み機器の連携上の注意すべき 5 つのポイントについてまとめました。

【利用シナリオと発生し得る脅威】
以下に挙げる 4 つの脅威のそれぞれに対して、対象機器の例や保護すべき対象情報の例、発生し得る脅威、基本的な対策の例に関して調査を行い、検討結果をまとめました。ここでの脅威の定義は「経済的に被害を受けること」「利用者が身体的被害を受けること」「利用者のプライバシーが侵害されること」としています。

- プラグアンドプレイ[1]に潜む脅威
- 生活インフラとの接続に潜む脅威
- 想定外の利用方法に潜む脅威
- 他機器やサービスとの接続に潜む脅威

「利用シナリオ」や「発生し得る脅威」は、実際に開発・提供されている機器やサービスを基に有識者による研究会（「複数の組込み機器の組み合わせに関するセキュリティ調査研究委員会」、委員長：松本 勉　国立大学法人横浜国立大学大学院教授）で検討を行い、その内容を、図を交えて分かりやすく解説しています（図 1 、図 2）。

利用シナリオ　－家の外から玄関のドアの鍵の確認－
ネット対応ドアをインターネットにつなげることで、外出時にパソコンや携帯電話から自宅の鍵の開閉をチェックしたり、施錠したりすることができる。また、ネット対応カメラを設置することで、外出時にパソコンや携帯電話から自宅の様子を確認することもできる。これらにより、外出時でも防犯を行うことができる。

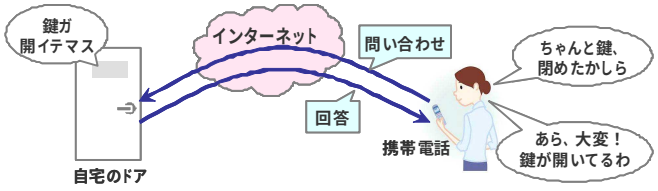

図 1 ：利用シナリオの例

[1] プラグアンドプレイ：周辺機器等を接続した際、利用者が特別な事をしなくても利用できる仕組み

発生し得る脅威

ここで対象としている生活インフラに関しては、誤ってエアコンのスイッチが入って風邪をひいたり、ドアの鍵が開いているのを知られて空き巣に入られたりするなど、深刻な被害をもたらす可能性がある。

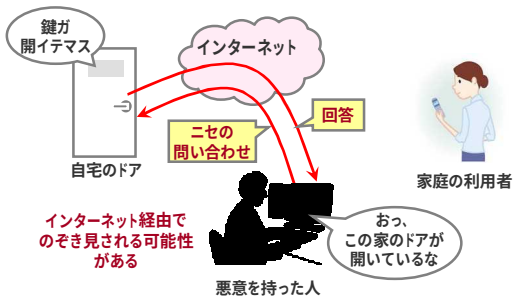

図２：発生し得る脅威の例

【組込み機器の連携上の注意すべき５つのポイント】

今回の調査では、それぞれの利用シナリオにおいて発生した脅威を整理し、５つのポイントにまとめました。研究会での検討の結果、開発社側で実施可能な対策だけでは不十分であり、利用者に適切な利用を促すことが、より安全な組込み機器の利用につながることが明らかになりました。このため、注意すべき５つのポイントに関して、「開発者側が考慮すべき事項」と「利用者側に注意を促すべき事項」の二つの視点から、考えられる対策例を整理しました。以下に５つのポイントと、その対策例を示します。

① 保護すべき情報種別の拡大

－開発者：組込み機器が蓄積、通信する情報を必要最小限の範囲に絞り込む

－利用者：組込み機器に入力する情報がネットワーク等を介して漏えいする危険性がある事を操作説明書や画面表示などで注意を与える

② 中間に位置する機器の脆弱性

－開発者：通信時に一定のセキュリティを保てる仕組みを検討する

－利用者：組込み機器に、設計・開発時に想定していない機器やメディアの接続を行うことの危険性を利用者に注意喚起する

③ 意図していない情報の拡散

－開発者：組込み機器に格納された情報への外部からのアクセス管理を厳密に行う

－利用者：情報を読み出すパスワードなどに、想定されやすい文字を設定しないよう、利用者に注意喚起する

④ 利用者や連携する組込み機器の多様化・不特定化

－開発者：他の組込み機器との接続状況や通信状況を利用者にわかりやすい形で画面表示する

－利用者：画面に表示される用語や略語等について解説を行う

⑤ 社会・生活への影響の深刻度

－開発者：生活インフラを設置する施工業者にも、セキュリティに関して認識してもらえるようにする

－利用者：メーカからのアナウンス等に注意するよう、利用者に促す

組込みシステムの高度化がもたらす利便性の裏に潜むセキュリティの脅威を、各分野のメーカや業界団体等とも協調しつつ継続的に把握していくと共に、組込みシステム利用者に安全な利用を促す必要があります。本報告書が、安心・安全な組込みシステムの開発に寄与し、セキュリティ脅威が減少することとなれば幸いです。

本書(全 42 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/fy19/reports/embedded/index.html）

■ 本件に関するお問い合わせ先
独立行政法人 情報処理推進機構 セキュリティセンター 小林／中野
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
独立行政法人 情報処理推進機構 戦略企画部広報グループ 横山／佐々木
Tel: 03-5978-7503 Fax:03-5978-7510 E-mail: pr-inq@ipa.go.jp