INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

組込みソフトウェアを用いた機器におけるセキュリティ（改訂版）

2010 年 3 月

独立行政法人 情報処理推進機構
セキュリティセンター

目　　次

1. 背景

1.1. あらゆるものがネットワークにつながる時代

組込み機器の高付加価値化

インターネットは、私たちのビジネスモデルやライフスタイルを大きく変えました。さらにネットワークは、コンピュータ間の接続から多様な機器間接続へと発展しつつあります。今や家電機器や携帯電話、自動車、工場の FA（Factory Automation）システムまで、あらゆるものがネットワークにつながる時代を迎えていると言っても過言ではありません。

ネットワーク化による負の側面

しかし、多様化・複雑化したネットワーク環境は、新たなトラブルをもたらしました。コンピュータの世界では、ネットワークを介した攻撃により、サービスの停止やファイルの損壊、情報流出等の被害が生じています。

今後は、組込みソフトウェアを用いた機器（以下、「組込み機器」という）もネットワーク化が進み、同様のトラブルに巻き込まれるかもしれません。その場合、コンピュータソフトウェアのメーカと同様に、組込み機器メーカにも何らかの対処が求められると考えられます。さらに、組込み機器メーカはそうした被害について、製造物責任法（PL 法）の観点から損害賠償責任を問われる可能性を考慮すれば、より難しい立場にあると理解すべきでしょう。

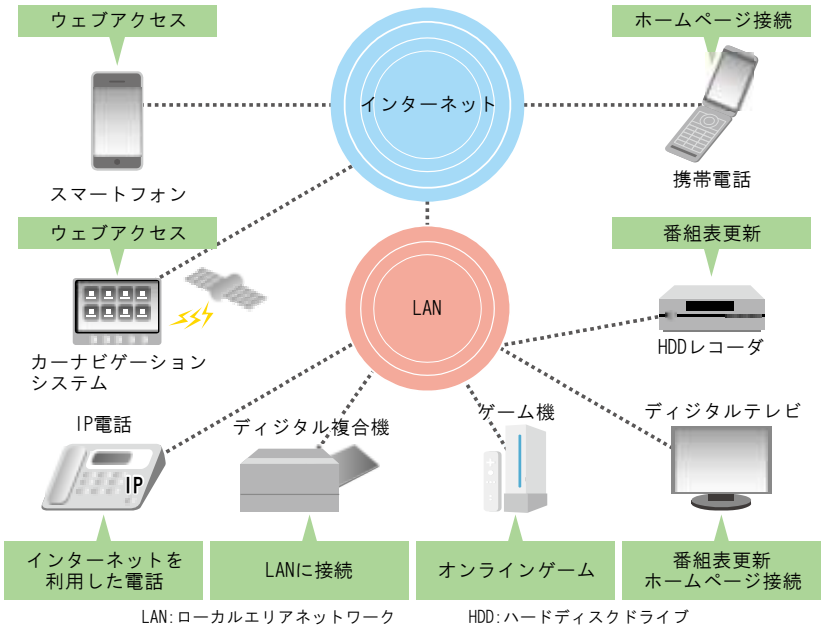


図 1　ネットワーク機能を備えた組込み機器の利用例

1.2. 脆弱性（ぜいじゃくせい）[1]が狙われている

トラブルの要因

コンピュータシステムを脅かすトラブルの要因には、ハードウェアの故障やソフトウェアの不具合、誤操作や誤設定等の人為的ミス、さらに、コンピュータウイルス[2]（以下ウイルスと言う）、スパイウェア[3]、システムへの侵入、サービス妨害攻撃[4]といった、悪意のある第三者の攻撃などが挙げられます。

悪用される脆弱性と悪意ある攻撃者の存在

数年前から、脆弱性を悪用した攻撃が目立つようになってきました。脆弱性は、プログラムや設定上の問題に起因する「弱点」です。

悪意ある攻撃者は、こうした脆弱性を利用し、ＰＣに攻撃するのと同様に、家電機器を標的に攻撃を行い、利用者の情報を盗み出すなどの犯罪的行為を行う可能性もあります。

インターネットにつながる機器の場合、昨日まで安全であっても、脆弱性が発見されれば、突如として危険になります。なぜなら、脆弱性の存在が知られると、それを悪用する攻撃プログラムやツールがインターネット上に公開され、これを搭載したウイルスが登場する可能性が急速に高まるからです。

脆弱性の根絶

脆弱性を根絶することは容易ではありません。しかし、脆弱性を悪用する攻撃がある以上、安全性向上のために、脆弱性を減らす努力が求められています。

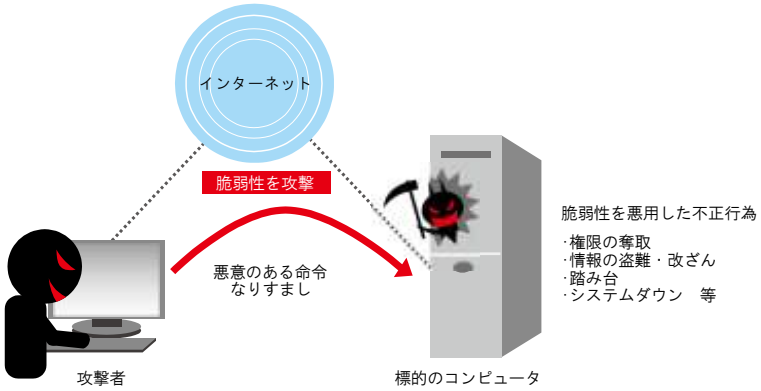


図　２　悪意ある攻撃者が脆弱性を悪用するイメージ

---

[1] ソフトウェア等において、コンピュータ不正アクセス、コンピュータウイルス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所。

[2] 第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能を一つ以上有するもの。（通商産業省（当時）告示「コンピュータウイルス対策基準」（平成 12 年 12 月 28 日最終改定））

[3] 利用者や管理者の意図に反してインストール（プログラムなどの導入・設定）され、利用者の個人情報やアクセス（接続）履歴などの情報を収集するプログラム等。

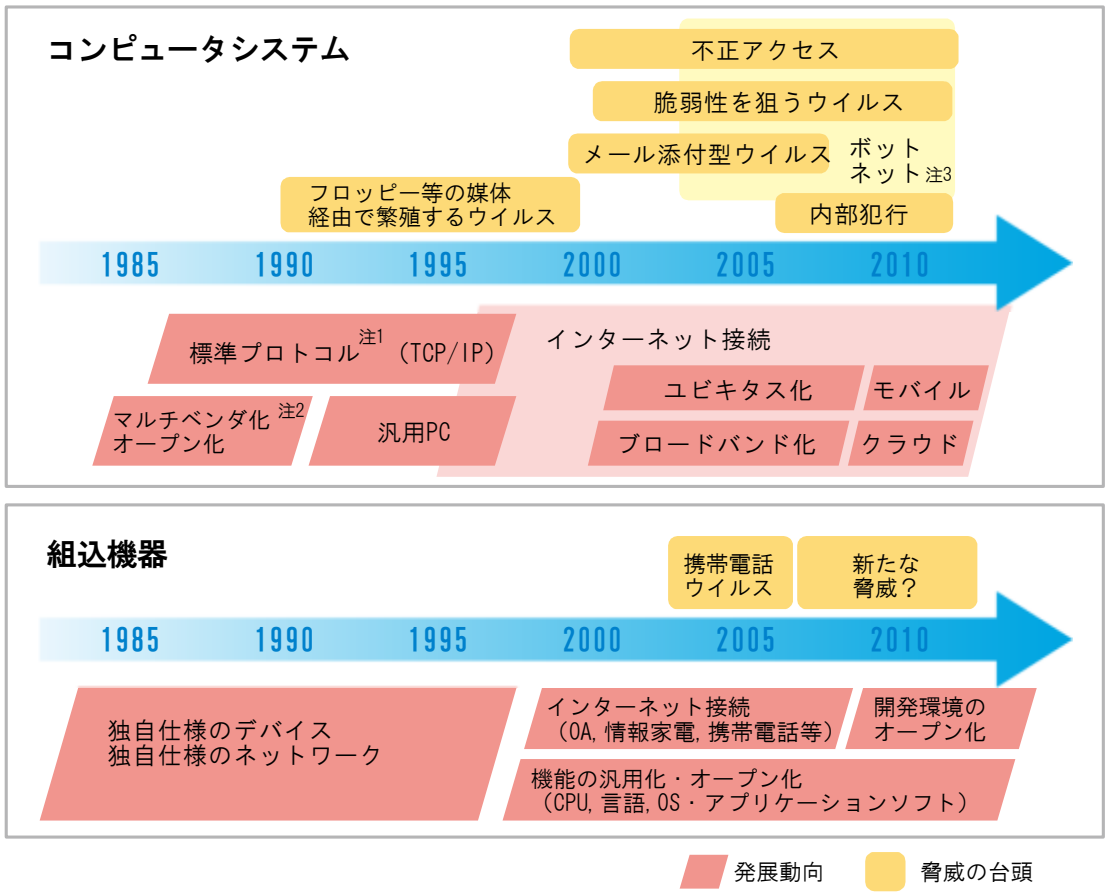
[4] インターネット上のサーバ等に接続要求等の大量のパケットを送り、サーバを機能不全に陥らせる攻撃。

1.3. 本書の狙い

コンピュータシステムの世界で深刻化しているセキュリティ問題が、近い将来、組込み機器においても問題化すると予想されます。組込み機器の分野において、実際に発生したトラブルの事例はまだ少ないですが、今後頻発する可能性は否定できません。では、どうしたらよいのでしょうか。

セキュリティ対策は品質向上の一部として適用していくことも可能です。ただし、従来の品質向上の枠組みにおいては十分にカバーされていなかった領域であり、今後は強化していく必要があります。

本書の狙いは、組込み機器を提供している企業が、安全なネットワーク社会の実現と製品の脆弱性等による事業リスクを回避するためになすべき取組みをご理解いただくことにあります。



注1　プロトコル：ネットワークを介してコンピュータ同士が通信をするときの通信規約など。
注2　マルチベンダ：様々な企業の製品から機器等を選んで組合せ、システムを構築すること。
注3　ボットネット：ボットとは外部からの指示を待ち、与えられた指示に従って、内蔵された処理を実行するプログラム（ロボットに似ているからボットといわれている）。同一の指令サーバの配下にある複数のボットは、指令サーバを中心とするネットワークを組む。これをボットネットとよぶ。指令に従い、特定サイトを攻撃したりする。

図 3　コンピュータシステムと組込み機器の発展動向と脅威

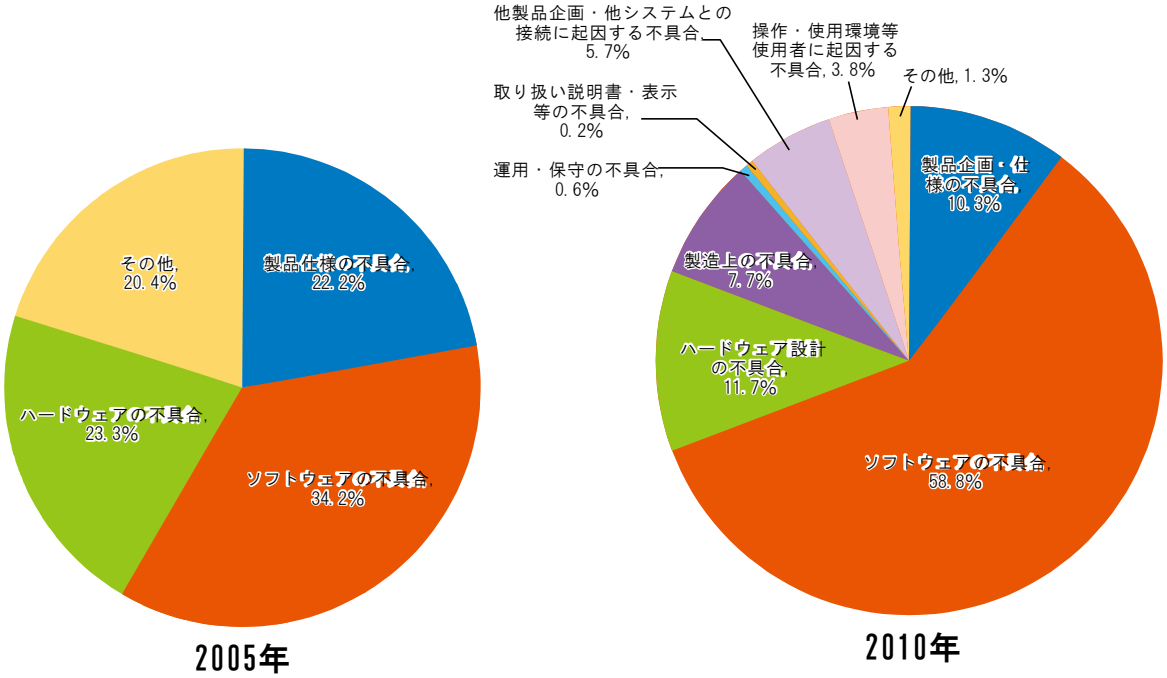
2. 組込み機器に潜む危険性

2.1. 組込み機器が抱えるリスク

組込み機器の不具合

経済産業省「2010 年版組込みソフトウェア産業実態調査報告書」[5]によると、組込み機器の出荷後に生じた不具合の主な原因として、ソフトウェアの問題が58.8%を占めており、組込みソフトウェアの品質が経営基盤を揺るがしかねない状況がうかがえます。

また、ソフトウェアの不具合は 2005 年度の同報告書では 32%と報告されていたことと比較して大幅に増加しています。近年ソフトウェアが複雑化してきたことから不具合原因に占めるソフトウェアの割合が増加しています。今後もソフトウェアに起因する不具合は様々な製品に拡大してくものと思われます。



（出所：（左図）IPA「2005 年版組込みソフトウェア産業実態調査報告書」2005 年６月、（右図）経済産業省「2010 年版組込みソフトウェア産業実態調査報告書」2010 年７月）

図 4　組込み機器の出荷後に生じた設計品質問題の主な原因の割合

5 http://www.meti.go.jp/policy/mono_info_service/joho/downloadfiles/2010software_research/10keiei_houkokusyo.pdf

製品回収が必要になるケースも

それでは、市場に供給している組込み機器に脆弱性が発見された場合はどうなるでしょうか。

コンピュータソフトウェアの場合、ソフトウェア製品のメーカ、販売会社（ベンダ）は脆弱性の存在を把握すると、それを修正するプログラム（パッチ）を開発し、インターネット経由でユーザに配布するという対応が一般化しています。

しかし、組込みソフトウェアの場合、コンピュータのソフトウェアのようにパッチをインターネット経由で配布する方法が適用できないケースもあります。そうした場合、製品を回収し、メモリや基板などのハードウェアを交換するなど、その対応に巨額のコストを必要とする可能性があります。具体的には機器回収にかかる費用は製造者だけでなく、販売店の費用も含まれることから組込みソフトウェアの改修は経営者にとって留意する必要があります。

さらに、脆弱性を悪用した攻撃の影響が制御系にまで波及し、物理的事故を引き起こす危険性もゼロとは言い切れません。そうした事故が発生した場合、組込み機器メーカの損害賠償責任を問われることにもなりかねません。

したがって、脆弱性対策は単なるセキュリティ対策の一つというより、組込み機器メーカの経営を揺るがしかねない経営リスクの一つとして捉えるべきでしょう。

近年では、放送用電波を用いてパッチを配信してデジタルテレビのソフトウェアを修正するといった方法も行われており、機器の機能や利用環境に合わせた自動更新の仕掛けを考えていくことも重要です。

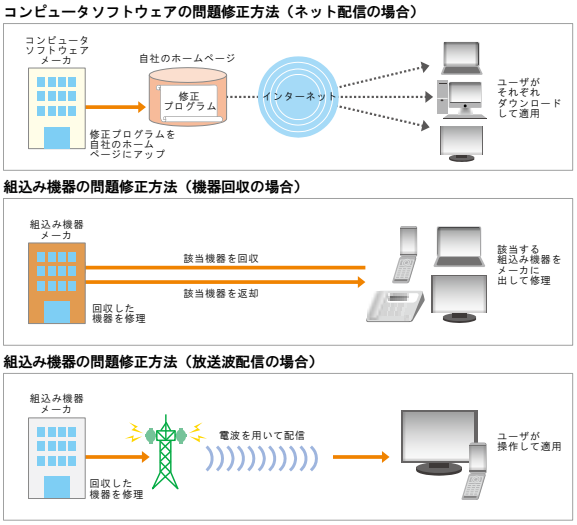


図５　コンピュータソフトウェアと組込み機器の問題修正方法

技術の進展に伴う危険性に対応した改修の必要性

技術は日進月歩で進展しています。過去に販売された組込み製品のソフトウェアは、技術の進歩に対応すべく改修（バージョンアップ）を行う必要も出てきていることから新製品だけでなく過去に販売された製品に関しても注意を払う必要があります。

例えば暗号技術の進展は安全・安心な機器の利用に多大な恩恵をもたらしました。現在では PC やサーバだけでなく携帯電話、ゲーム機、情報家電といったネットワークに接続する機器に暗号技術を駆使したソフトウェアが組込みまれ安全・安心な暮らしを支えています。

一方で計算機能力が向上することで当初安全と思われていた暗号のアルゴリズムが必ずしも安全とは言い切れない状況となりました。このような状況に対して米国標準技術研究所（NIST）はより安全な暗号への移行を促しており、過去に使用されていた暗号方式 RSA 1024[6]及びに ハッシュ関数 SHA-1[7]ついて暗号の利用を中止する方針を打ち出しています。

このように技術の進展によるソフトウェアの改修の必要性が高まっていますが、過去に販売された製品の改修に必要なコストの問題等、技術の進展によるソフトウェア改修は経営者にとっても重要な課題です。

[6] 桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つで、暗号やデジタル署名などに使われる。鍵長は 1024 ビットである。

[7] SHA((Secure Hash Algorithm)1 は、原データに対して 160 ビットのハッシュ値を生成する関数で、認証やデジタル署名などに使われる。

2.2. 組込み機器におけるトラブル事例

組込み機器の分野でも脆弱性に起因するトラブルは、絵空事ではなく実際に発生しています。

トラブル事例１：家庭用ルータ[8]がボットウイルスに感染する

インターネットに接続するための機器の一つであるルータの脆弱性を利用して、ボットウイルスというコンピュータウイルスの一種に感染してしまう事例が報告[9]されています。ボットウイルスはコンピュータに感染し、外部からネットワークを通じて操ることを目的としたプログラムです。このボットウイルスは、指令サーバからの攻撃命令によって感染したルータ等を踏み台としたDDoS[10]攻撃を可能としてしまい、感染ルータが加害者になるなどの脅威があります。

このような事例は 2009 年 3 月に組込み機器に感染するボット PsybOt がウェブサイト「DroneBL」に DDoS 攻撃をしたとして報告されており、組込み機器であっても、PC と変わらず、適切な ID/パスワード管理、脆弱性対策をする必要が有ります。

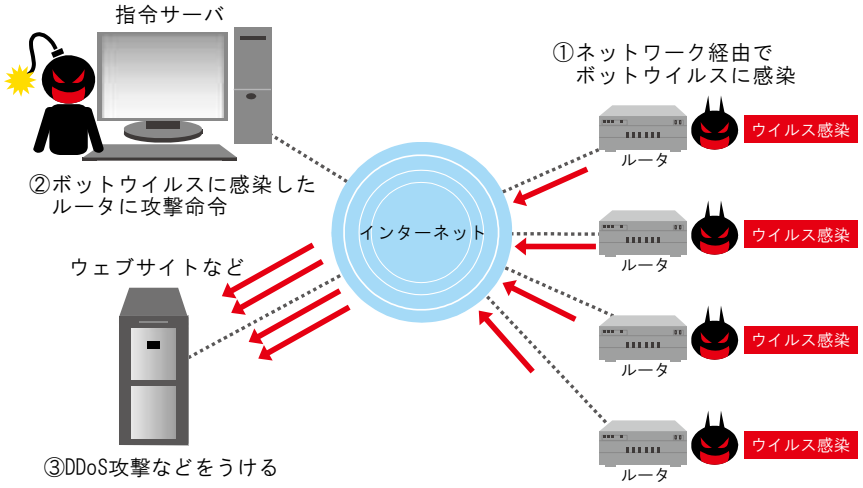


図 6　ボットウイルスに感染したときの攻撃

[8] ルータとは、ネットワーク上を流れるデータを他のネットワークに中継する機器。ネットワーク層のアドレスを読み取り、転送すべき経路を判断する経路選択機能を持つ。

[9] http://www.ipa.go.jp/security/vuln/documents/2008/200801_Yamaha.html

[10] DDoS(Distributed Denial of Service)。DoS はネット上のトラフィックを増大させることにより回線やサーバの処理能力を占有して本来の機能やサービスを妨害する攻撃で、DDoS は分散する大量のコンピュータが DoS を一斉に行う攻撃。

トラブル事例２：スマートフォンの普及により、脆弱性対策の重要性が一段と高まる

インターネットに接続し様々なソフトウェアをインストールし利用出来るスマートフォンが登場し普及しています。利用者がインストールしたソフトウェアと組込まれていたソフトウェアの両方の脆弱性が報告されています。

2010 年 8 月にスマートフォンの脆弱性を悪用した攻撃の可能性についての情報が公開[11]されました。2010 年 8 月時点でこの脆弱性を利用したウイルス等はありませんでしたが、普及するスマートフォンに対する脆弱性対策の重要性は高まっています。これまでスマートフォンや携帯電話にはウイルス対策ソフトをインストールするといった習慣が無かったことから、脆弱性を利用したウイルスが出現した場合、被害範囲が大きくなる可能性があります。

スマートフォンに関するウイルスの報告は、ゲームに見せかけて利用者の位置情報を第三者に送信するといったものが報告されています。

また、スマートフォンで利用するソフトウェアの開発が利用者によっても行われるといった利用環境の変化も起こっています。これにより脆弱性を抱えるソフトウェアが利用者から配信される可能性もあり、そういった場合の対処方法等も検討課題の一つでしょう。

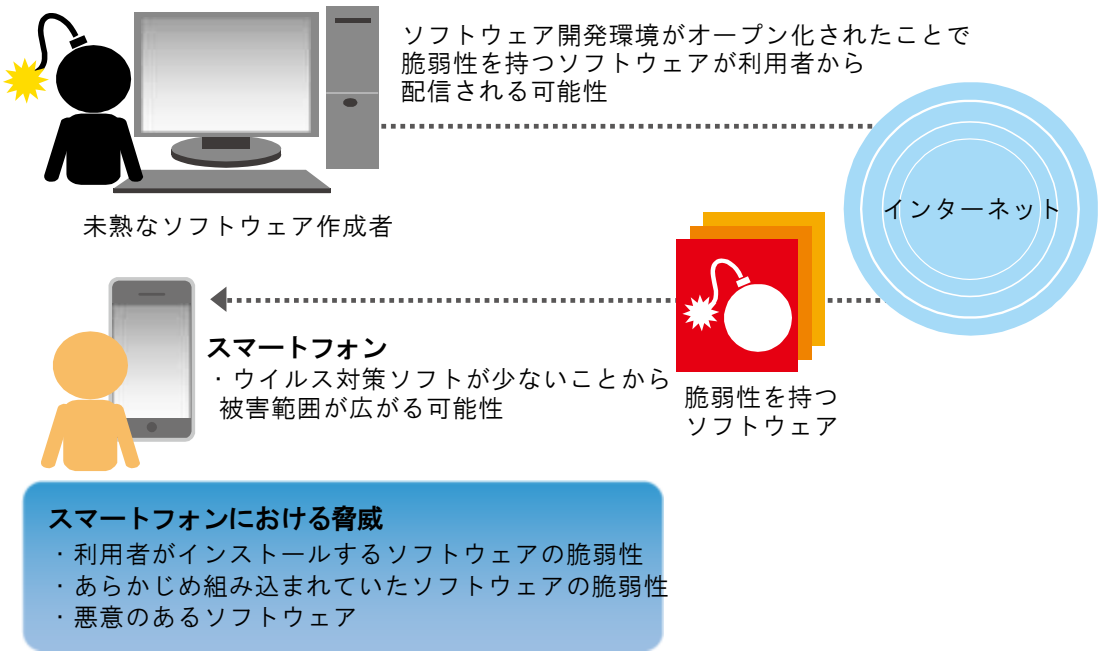


図 7　スマートフォンの普及と脅威の可能性

[11] http://www.lac.co.jp/info/alert/alert20100812.html

トラブル事例３：組込み機器の管理用ウェブ画面における脆弱性

近年ネットワーク接続機能を利用する家電製品が増加しています。これらの家電製品にはネットワークを介してウェブ画面からサービスを利用する製品や、設定変更を行う機能を有している製品があります。これらのウェブ画面がもつ脆弱性を利用することで悪意のある者が機器の設定変更が可能になるなど、組込み機器の機能が多様化する一方で脆弱性とその脅威の種類も多様化しています。

2009 年２月にはウェブブラウザを利用した映像モニタリング用カメラにおいて、組込まれていたウェブサーバにアクセスすると利用者側のコンピュータにおいて任意の命令が実行される可能性のある脆弱性のあるプログラムがインストールされることが判明し[12]、製品開発者は対策プログラムを作成、配付を行いました。

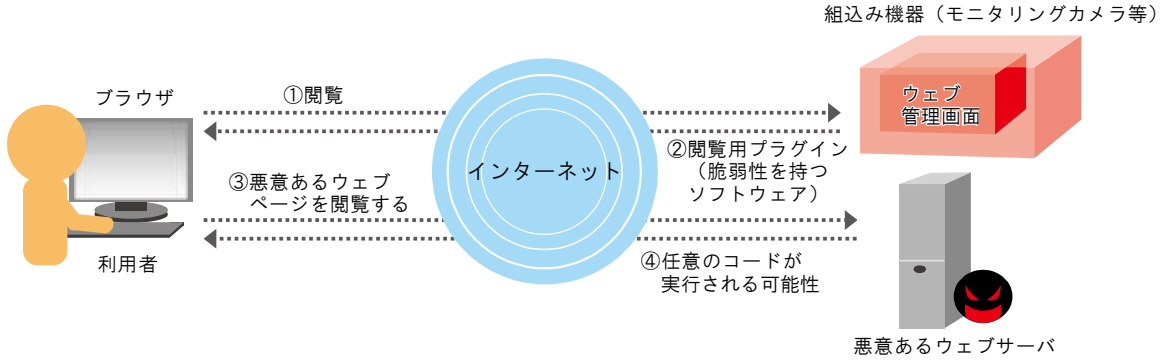


図 ８　組込み機器からインストールしたソフトウェアの脆弱性

[12] http://www.ipa.go.jp/security/vuln/documents/2009/200902_sonysnc.html

3. 組込み機器における情報セキュリティ対策のあり方

3.1. 対策に取り組む姿勢

組込み機器のセキュリティ対策を考えるべき時期

現在、PC に何のセキュリティ対策やパッチの適用も施さずにインターネットに接続すると、わずか数十秒でウイルスに感染すると言われています。そうした状況において、組込み機器を無防備にインターネットに接続することは危険と考えるべきでしょう。

組込み機器のネットワーク接続の流れが本格化しつつある今、組込み機器のセキュリティ対策に取り組むべき時期に来ているのではないでしょうか。

対策についての基本的な考え方

組込み機器の脆弱性の問題は、事後対応に要する莫大なコストを考えれば、潜在する問題点をいかに前工程でつぶすか、企画段階からの対応が重要になります。こうした方向からの安全性の追求は、製品・サービスの全工程において、品質向上の一環として取り組むことが可能です。ただし、これまでの品質向上で扱ってきた領域とは異なる専門性が要求される点に配慮する必要があります。

また、開発時のセキュリティ対策の障害となるのはリソース（人、資産）の問題です。より手間をかけて安全に開発することが商品の価値・価格に必ずしも直接反映できないわけですが、それでも、自社の社会的責任に鑑み、相応の対策を行えるよう、トップの判断として必要なリソースを確保すべきでしょう。

さらに、組込み機器の脆弱性が出荷後に発覚した場合には、顧客や消費者が被害に遭わないようにできる限りの努力をすること、また、万が一、事件・事故が発生してもそれが深刻な事態に陥ることのないよう適切な対応をとることは、メーカとしての責務と言えるでしょう。そのため出荷時に個人情報を消去するための機能に関するセキュリティ検証を行うことで、利用が終了した後に入力された個人情報が機器に残ってしまうことを未然に防いでいる事例もあります。

3.2.組込み機器におけるセキュリティ対策の取組み

3.2.1. セキュリティ確保のための体制

体制については、いくつかの考え方があります。例えば、脆弱性対策を含む製品セキュリティの推進を図る専任チームを設置する方向、事業部間を横断的につなぐ委員会を組織し情報共有と共通認識・合意を形成する方向、既存の組織（例：品質向上）の新たな使命として付与する方向などが考えられます。いずれにせよ、全社的なセキュリティ管理部門や品質管理部門との整合・連携が必要になります。特に、既存の品質保証体制と、セキュリティ固有の技術問題に関する比較的新しい知見をうまく組み合わせることが重要です。近年ではセキュリティ検証をシステムテストの最終段階で行う部門、部署を設置するといった取り組みも行われています。

メーカ A 社では、全社横断的な情報セキュリティの統轄部署を社長直下に設置し、「社内の情報セキュリティ」、「個人情報・営業秘密情報の保護」、「製品セキュリティ」の３つのカテゴリに係る全社的な推進を使命として位置づけました。脆弱性は「製品セキュリティ」の範疇であり、社内分社や子会社を含む全社的な委員会で推進しています。また、脆弱性情報等の情報展開については、委員会の下の技術部会で実施しています。さらに、脆弱性も含む技術的な指針、対策などの検討、出荷前のテストなどは、本社研究開発（R&D）の中のグループで担当しています。

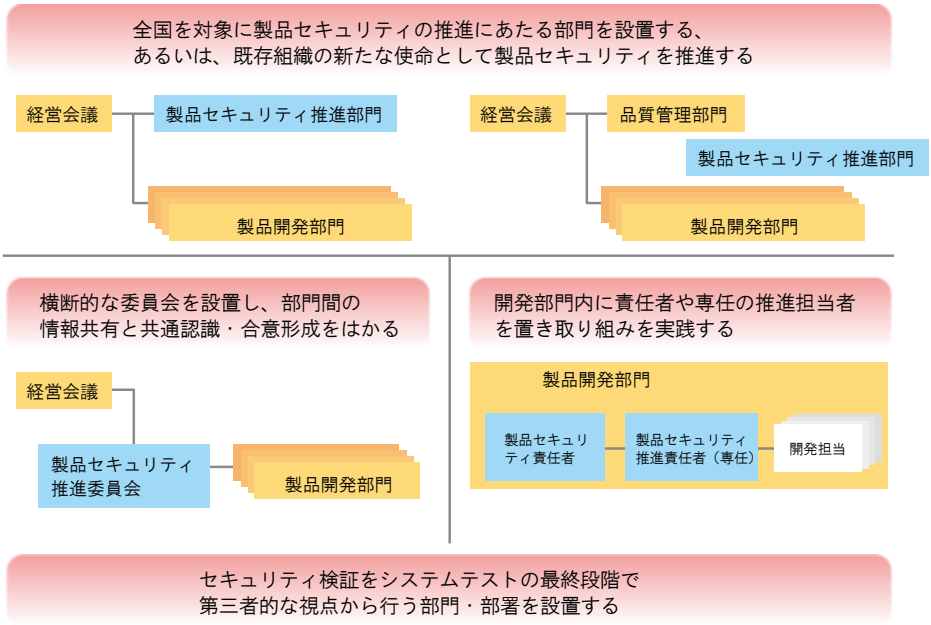


図９　セキュリティ確保のための体制の例

3.2.2. セキュリティに関する教育・ルール

開発スタッフは、内包された脆弱性を排除するとともに、そうした取組みが必要な理由を正しく認識することが期待されます。そのためには、セキュリティ確保のためのチェックリストや「べからず集」のような指針・ガイドラインを開発プロセスに応じた形で整備するとともに、その教育を徹底する必要があります。

また、組込み機器の開発は多くの場合、プロジェクト単位で稼動しており、プロジェクトが終わってチームが解散すると、情報が散逸することがあります。そのため、後に脆弱性が発見された場合の事後対処に必要不可欠な各工程の記録・情報を収集・管理する仕組みや、それを共有し必要に応じて利用するルールが必要になります。

メーカ B 社では、R&D の組織内でセキュリティを専門とする研究者が中心になって、組込みソフトウェア開発ガイドラインの作成に着手しています。

また、メーカ C 社では、国際標準 ISO/IEC15408（コモンクライテリア）[13] の認証取得および同レベルの開発品質を設定し、開発プロセスの中に脆弱性を排除する仕様・設計・検査を組み込んでいます。ISO/IEC15408 は、IC カードや複合機などで認証取得が進んでいるだけでなく、政府システム調達要件としても位置付けられていることから、有用な取組みと言えるでしょう。

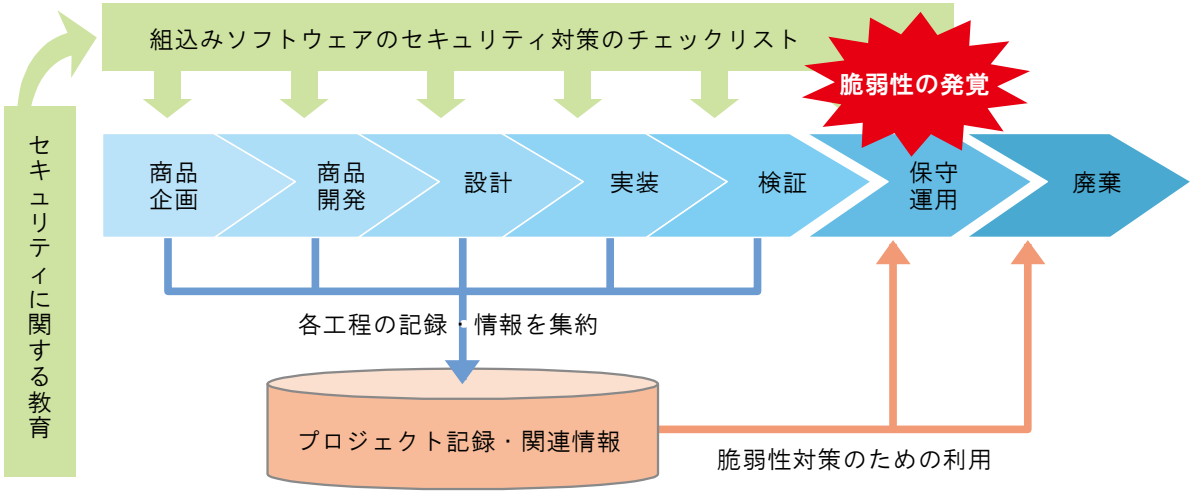


図１０　セキュリティに関する教育・ルールの仕組み

[13] IT 製品・システムに関する情報セキュリティの国際標準。これに基づき、IT 製品･システムのセキュリティ機能や目標とするセキュリティ保証レベルを第三者機関が評価し、その結果を検証する「IT セキュリティ評価・認証制度」が運用されている。

3.2.3. セキュリティ評価・監査

開発プロセスの各工程で適切なレビュー（検査）を実施することで、全体としての大幅な手戻りを削減することが期待されます。実際にどれだけ実施するかは予算や開発期間との兼ね合いであり、基本的にはプログラム不具合の修正（バグフィックス）など品質向上の取組みと同様な考え方で判断することができます。特に、開発部隊とは別の、セキュリティ担当者を含むスタッフによるプロジェクト監査等を実施することは重要です。

例えば、メーカ D 社では、セキュリティ検証をシステムテストの最終段階で第三者的な視点から行う部門・部署を設置することで、セキュリティ機能が正しく実装され動作しているか、セキュリティ上の脆弱性が残されていないかを確認している。このセキュリティ検証は企画段階での脅威分析と対をなし、システムテストの最終段階におけるセキュリティ対策として検証を行っています。

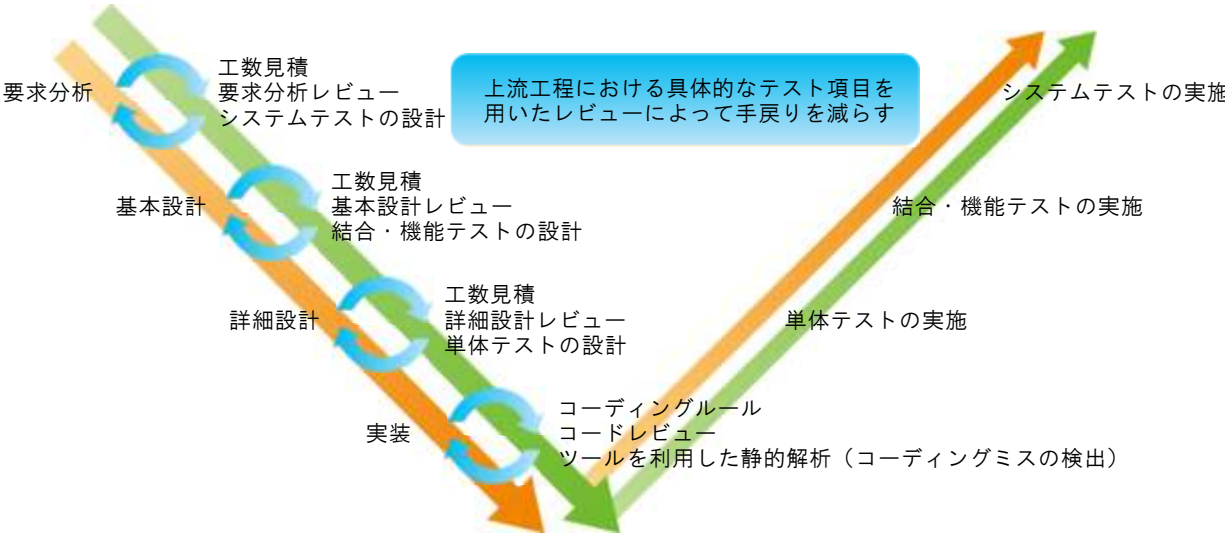


図１１　各プロセスにおけるレビューの実施

3.2.4. 事後対応

トラブル発生時の事後対応としての改修方法が変化しています。具体例としてウェブアクセスによるパッチダウンロード、販売店への持ち込み、放送波による改修プログラムの配信について紹介します。

対処事例（1）：ウェブアクセスによるパッチダウンロード

ユーザが事業者から提供されたソフトウェアで改修を行う事例として、ルータに対する改修プログラム適用の例を紹介します。メーカ側は、既に数万台出荷されていた当該製品について、ネットワークを通じた修正プログラムの配布と並行して、サービスマンがユーザに電話をかけて修正プログラム適用を依頼する作業を実施しました。この作業ではユーザが修正プログラム（パッチ）をダウンロードし、機器に適用するといったユーザが関与する方法が取られました。

後に同メーカでは、本件を品質問題の一つとして捉え、社内告知するとともに、対策チームを結成し、こうした問題を未然に防ぐためのチェック項目を追加することとなりました。

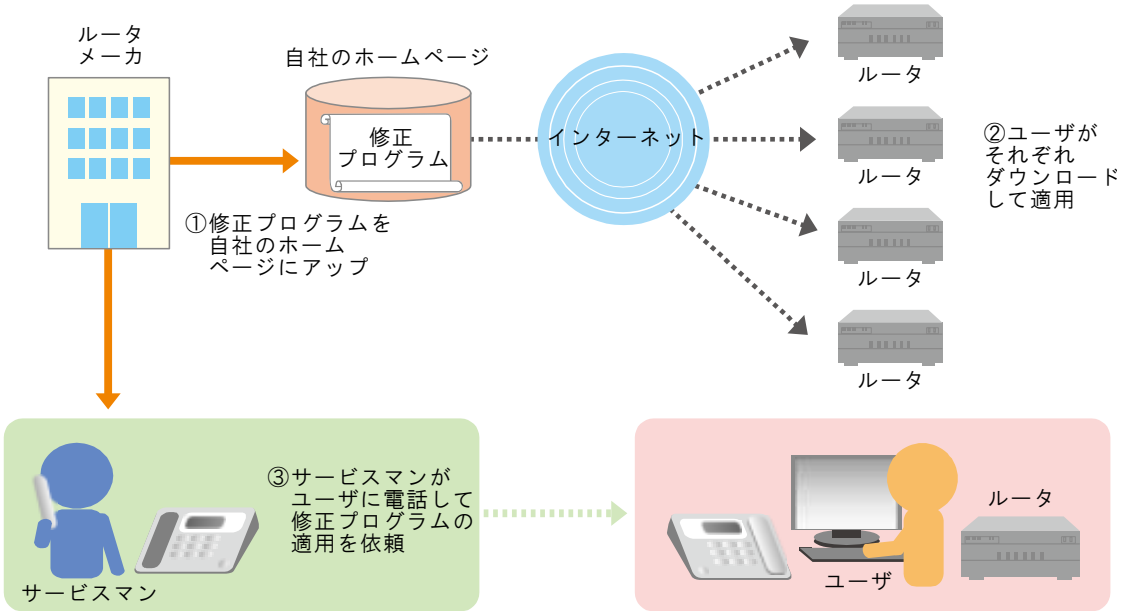


図１２　ルータの改修方法

対処事例（2）：販売店への持ち込み

事業者が製品を回収しソフトウェアの改修を行う事例として、携帯電話に組み込まれていたソフトウェアの一つであるブラウザの改修の例を紹介します。携帯電話のブラウザの改修を行うにあたってサービス会社では、携帯電話の販売店において、無償でソフトの書換えを実施しました。1 回の書換えに 30 分～1 時間程度を要したとされます。

携帯電話のように消費者へ大量に普及する製品は、対策適用の実施が容易ではありません。販売店の店頭における対策の適用は、店舗にも消費者にも時間的なコストを強いる点で難しい選択であったと考えられます。

また、近年では自動車に関する製品回収も発生しており、リコールの結果として発生する費用や企業イメージの低下も懸念となっています。

このような対策は機器がインターネットなどを利用した改修に対応していない場合の対処としての改修方法であり、コストがかかりますが、一方で対策の徹底などは行ないやすくなります。

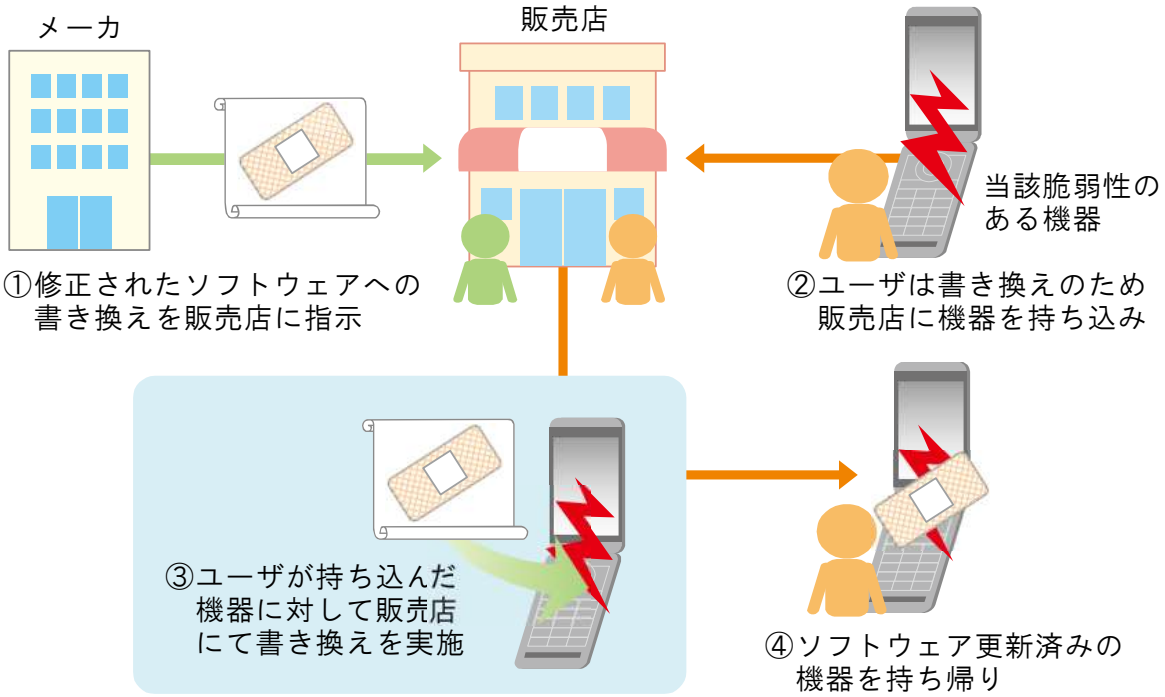


図１３　携帯電話ブラウザの改修方法

対処事例（３）：放送波による改修プログラムの配信

近年新たに見られる事例として、放送波による改修プログラムの配信の例を紹介します。デジタルテレビには、放送波を通じて、利用者には無料でプログラムのダウンロードが行われる仕組みがあります。これによってソフトウェアの不具合などを改修し性能を向上させることができます。インターネットによる方法は、特定の Web サイトから改修プログラムをダウンロード（プル）して改修しますが、放送波による方法は、放送局から改修プログラムが送信（プッシュ）される形態となります。

テレビ機器メーカは放送波を利用したファームウェアアップデートを行うことが可能であり、不具合のある製品のソフトウェアを改修するために改修プログラムを放送波経由で自社製品に配信し、ユーザが利用していない時間帯にアップデートを行う機能を備えています。近年では機能改修のためのアップデートだけでなく録画したデジタル放送のコピー回数を制限する「ダビング 10」などの機能を追加するためのアップデートにも利用されています。

しかしながらこれらのソフトウェアを配信する際に不具合のあるプログラムを配信すると、脅威を広げてしまう可能性があります。

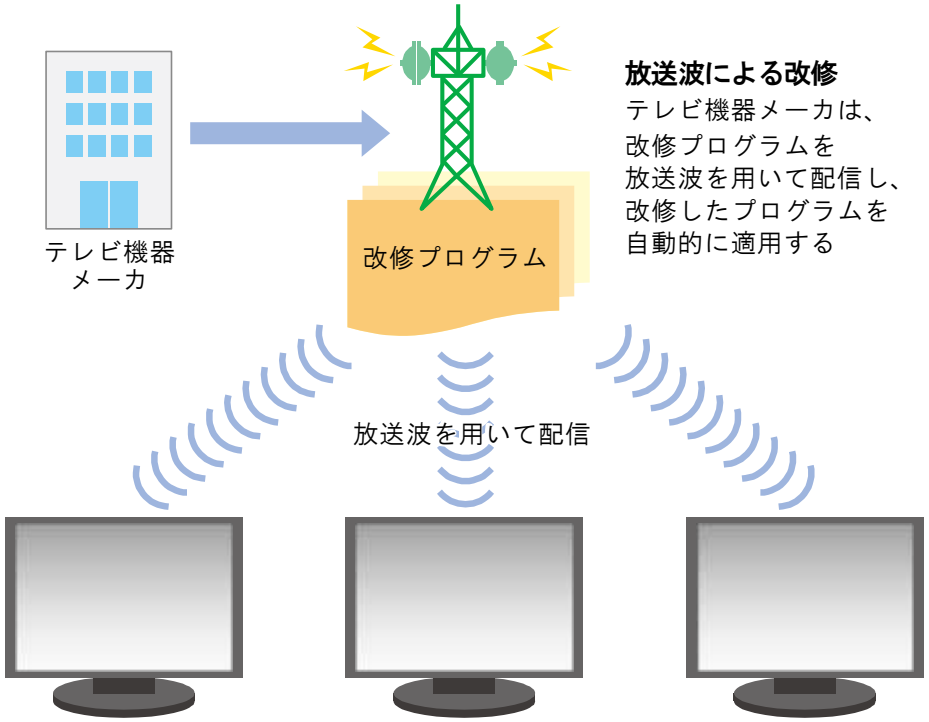


図１４　放送波を用いた改修プログラムの配信

3.3.その他の留意点

3.3.1. 法制度

(1) 製造物責任法

経済企画庁国民生活局消費者行政第一課「逐条解説　製造物責任法」[14] においては、「ソフトウェア自体については、無体物であり、製造物責任の対象とはしていない。ただし、ソフトウェアを組込んだ製造物については、本法の対象と解される場合がありうる。ソフトウェアの不具合が原因でソフトウェアを組込んだ製造物による事故が発生した場合、ソフトウェアの不具合が当該製造物自体の欠陥と解されることがあり、この場合、その欠陥と損害との間に因果関係が認められるときには、当該製造物の製造業者に本法に基づく損害賠償責任が生ずる」と記載されています。

これを踏まえると、脆弱性自体が、「欠陥」と考えられる場合に、他の要件を満たせば、損害賠償責任が生じると考えることができます。脆弱性が「欠陥」と考えられる場合とは、たとえば、提供時[15]において通常備えられている「セキュリティ」を備えていない状況が挙げられます。ネットワークでの利用が前提となっている機器については、外部からの攻撃を想定し、それに耐えられるものとされるべきと考えてよいのではないでしょうか。

(2) 消費生活用製品安全法

消費生活用製品安全法では、製品事故情報報告・公表制度が設けられています。この制度は、重大製品事故（一般消費者の生命又は身体に対する危害が発生した事故、または消費生活用製品が滅失し、又はき損した事故であって、一般消費者の生命又は身体に対する危害が発生するおそれのあるもの）が発生した場合に、消費生活用製品を製造・輸入する事業者が、消費者庁に報告することを義務化している制度です。

経済産業省「消費生活用製品安全法に基づく製品事故情報報告・公表制度の解説～事業者用ハンドブック～」[16]には、ソフトウェアについて以下の記述があります。

---

[14] 出版社: 商事法務研究会 (1995/01)、ISBN-10: 4785706988、ISBN-13: 978-4785706982、発売日：1995/01

[15] 製造物責任法上は、「当該製造物の特性、その通常予見される使用形態、その製造業者等が当該製造物を引き渡した時期その他の当該製造物に係る事情を考慮して、当該製造物が通常有すべき安全性を欠いていることをいう」と定義されている（法 2 条 2 項）。

[16] 経済産業省ウェブサイト「製品安全ガイド」
http://www.meti.go.jp/product_safety/producer/guideline/download.html　。

「ソフトウェアは無体物であり、消費生活用製品に該当しません。通常、ソフトウェアの場合、それを組み込んだ製品が消費生活用製品に該当します。」

これを踏まえると、ソフトウェアを組み込んだ家電機器等において、ソフトウェアの脆弱性が原因となる製品事故が発生またはそのおそれがあることを認識した事業者は、報告義務があるといえるでしょう。

3.3.2. ユーザとのインタフェース

幅広いユーザ層を対象とする組込み機器では、ユーザに負担感や誤解を与えることなく、セキュリティに配慮した設定や操作方法を選択するように誘導する必要があります。また、ユーザが危険な操作・変更を行おうとした場合には警告画面を提示するなどの配慮も有効です。単に機器そのものの機能だけでなく、リモコン等を含むユーザインタフェースについても、安全寄りの配慮について十分に検討しておくことが望まれます。

また、ユーザとメーカの接点であるマニュアルには、ソフトウェアの不具合や脆弱性が発覚した際の対処方法、その機器を廃棄する際にユーザが行うべきプライバシー情報の削除方法なども記載しておくことが望まれます。

さらに、トラブルが発生した場合、最初に連絡が来るのはお客様相談窓口です。窓口のスタッフに対し、従来の不具合だけでなく、攻撃によるトラブル発生の可能性やその際の適切な応対・処理について教育しておく必要があります。

参考文献

- 「組込みシステムのセキュリティへの取り組みガイド（2010 年改訂版）」
  http://www.ipa.go.jp/security/fy22/reports/emb_app2010/

- 「情報家電におけるセキュリティ対策　検討報告書」
  http://www.ipa.go.jp/security/fy22/reports/electronic/

- 「自動車と情報家電の組込みシステムのセキュリティに関する調査報告書」（2008 年度）　http://www.ipa.go.jp/security/fy20/reports/embedded/

- 「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」（2007 年度）
  http://www.ipa.go.jp/security/fy19/reports/embedded/

- 「組込みシステムの脅威と対策に関するセキュリティ技術マップの調査報告書」（2006 年度）　http://www.ipa.go.jp/security/fy18/reports/embedded/

情報セキュリティに関する届出について

IPA セキュリティセンターでは、経済産業省の告示に基づき、コンピュータウイルス・不正アクセス・脆弱性関連情報に関する発見・被害の届出を受け付けています。

ウェブフォームやメールで届出ができます。詳しくは下記のサイトを御覧ください。

URL: http://www.ipa.go.jp/security/todoke/

コンピュータウイルス情報

コンピュータウイルスを発見、またはコンピュータウイルスに感染した場合に届け出てください。

不正アクセス情報

ネットワーク（インターネット、LAN、WAN、パソコン通信など）に接続されたコンピュータへの不正アクセスによる被害を受けた場合に届け出てください。

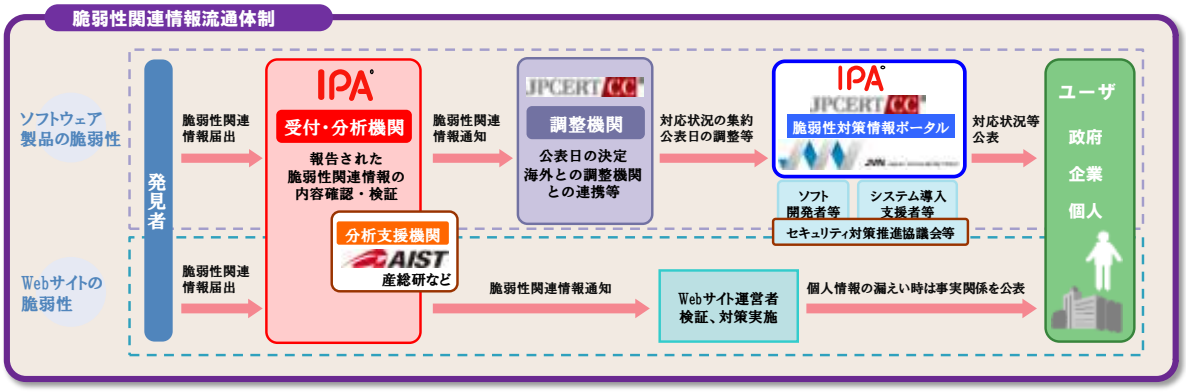
ソフトウェア製品脆弱性関連情報

OS やブラウザ等のクライアント上のソフトウェア、ウェブサーバ等のサーバ上のソフトウェア、プリンタや IC カード等のソフトウェアを組み込んだハードウェア等に対する脆弱性を発見した場合に届け出てください。

ウェブアプリケーション脆弱性関連情報

インターネットのウェブサイトなどで、公衆に向けて提供するそのサイト固有のサービスを構成するシステムに対する脆弱性を発見した場合に届け出てください。

脆弱性関連情報流通の基本枠組み「情報セキュリティ早期警戒パートナーシップ」



※IPA：独立行政法人 情報処理推進機構、JPCERT/CC：有限責任中間法人 JPCERT コーディネーションセンター、産総研：独立行政法人 産業技術総合研究所

独立行政法人 情報処理推進機構

〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコートセンターオフィス 16 階
http://www.ipa.go.jp

セキュリティセンター

TEL: 03-5978-7527　FAX　03-5978-7518
http://www.ipa.go.jp/security/