



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

2006年4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

<b>1. 背景</b> .....	1
1.1. あらゆるものがネットワークにつながる時代 .....	1
1.2. 脆弱性が狙われている .....	2
1.3. 本書の狙い .....	3
<b>2. 組み込み機器に潜む危険性</b> .....	4
2.1. 組み込み機器が抱えるリスク .....	4
2.2. 組み込み機器におけるトラブル事例.....	6
<b>3. 組み込み機器における情報セキュリティ対策のあり方</b> .....	9
3.1. 対策に取り組む姿勢.....	9
3.2. 組み込み機器におけるセキュリティ対策の取組み.....	10
3.2.1. セキュリティ確保のための体制.....	10
3.2.2. セキュリティに関する教育・ルール .....	11
3.2.3. セキュリティ評価・監査.....	12
3.2.4. 事後対応.....	13
3.3. その他の留意点.....	17
3.3.1. 製造物責任法 .....	17
3.3.2. ユーザとのインタフェース.....	17

# 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

### 組み込み機器の高付加価値化

1990年代後半から世界を席卷したインターネットは、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。今や家電機器や自動車、工場のFA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、組み込みソフトウェアを用いた機器（以下、「組み込み機器」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ーと同様に、組み込み機器メーカーにも何らかの対処が求められると考えられます。さらに、組み込み機器メーカー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。

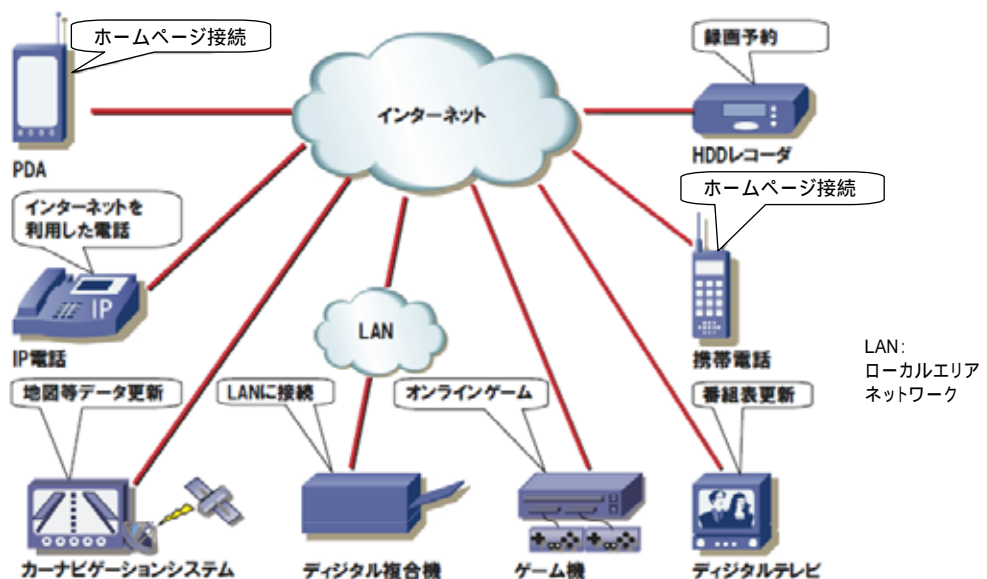


図 1 ネットワーク機能を備えた組み込み機器の利用例

## 1.2. 脆弱性<sup>1</sup>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<sup>2</sup>（以下ウイルスと言う）、スパイウェア<sup>3</sup>、システムへの不正侵入、サービス妨害攻撃<sup>4</sup>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

数年前から、脆弱性（ぜいじゃくせい）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。脆弱性により例えば想定外の入力データがメモリ上に溢れたり、本来許容しないはずの命令（コマンド）を受け入れてしまい、そうしたミスを悪用されて、ネットワーク越しに権限の奪取やデータの流出、サービス停止などの不正な操作をされてしまうのです。

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、それを攻略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。

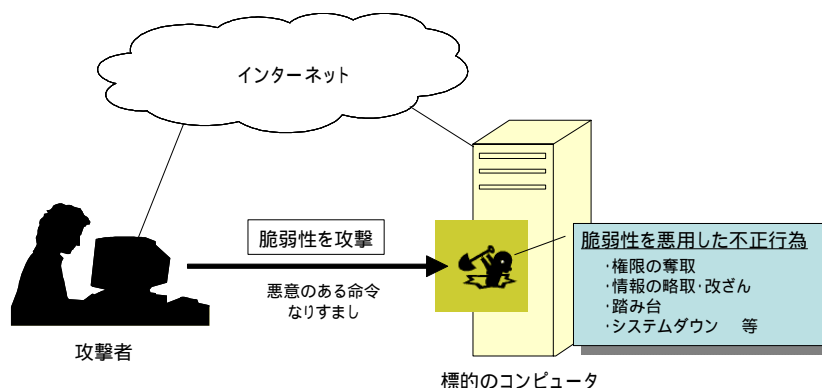


図 2 脆弱性を悪用するイメージ

<sup>1</sup> 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。

<sup>2</sup> 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、発病機能の一つ以上を有するもの。（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））

<sup>3</sup> 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。

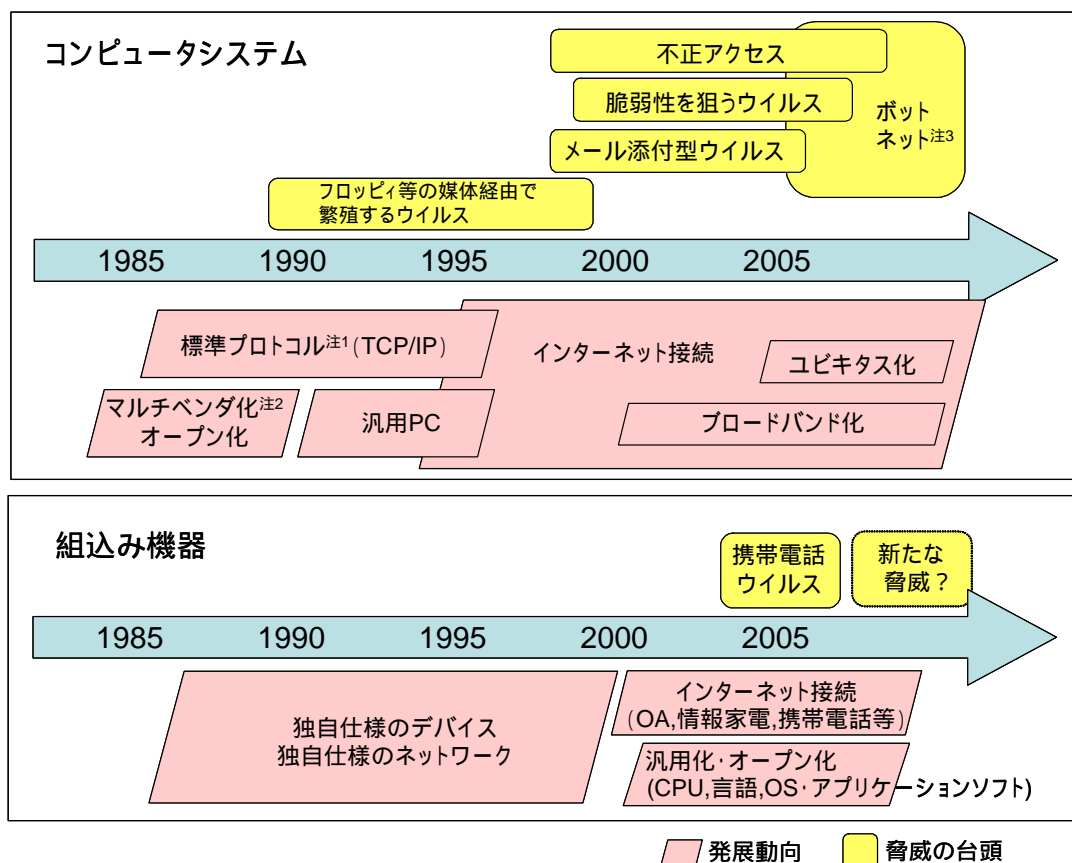
<sup>4</sup> インターネット上のサーバ等に大量の命令を送り、サーバを機能不全に陥らせる攻撃。

### 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、組み込み機器においても問題化すると予想されます。組み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、組み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欠陥による事業リスクを回避するためになすべき取り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 ポットネット：ポ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ポ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ポットは、指令サーバを中心とするネットワークを組む。これをポットネットとよぶ。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み込み機器の発展動向と脅威

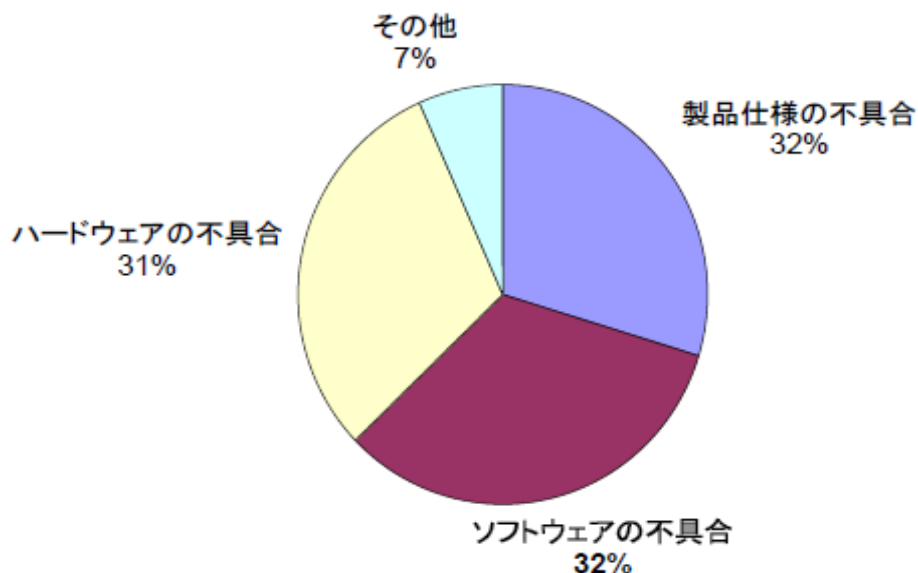
## 2. 組込み機器に潜む危険性

### 2.1. 組込み機器が抱えるリスク

#### 組込み機器の不具合

IPA「2005年版組込みソフトウェア産業実態調査報告書」<sup>5</sup>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34%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、経営指標の目的を達成するための最も有効な手段として経営者が「品質の向上」と回答した企業とそうでない企業の、出荷後の不具合の発生率を比較すると、不具合発生率10%以上の企業の割合は、「品質の向上」と回答した企業では約27%であるのに対し、そうでない企業では45%となっています。同報告書が「品質の向上は現場の努力も必要であるが、各種規定や制度、開発環境、専任の要員確保など経営判断を伴う施策が必要である場合も多い」と指摘している通り、製品の不具合との戦いは経営層の問題であるといえます。



(出所：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)

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

<sup>5</sup> <http://sec.ipa.go.jp/download/200506es.php>

## 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み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、組み込みソフトウェアの場合、コンピュータ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。2001年5月に報告された携帯電話の不具合の問題<sup>6</sup>では、機器回収に要した費用が120億円に達したとされています。

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、組み込み機器メーカの損害賠償責任を問われることは必至です。

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、組み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。

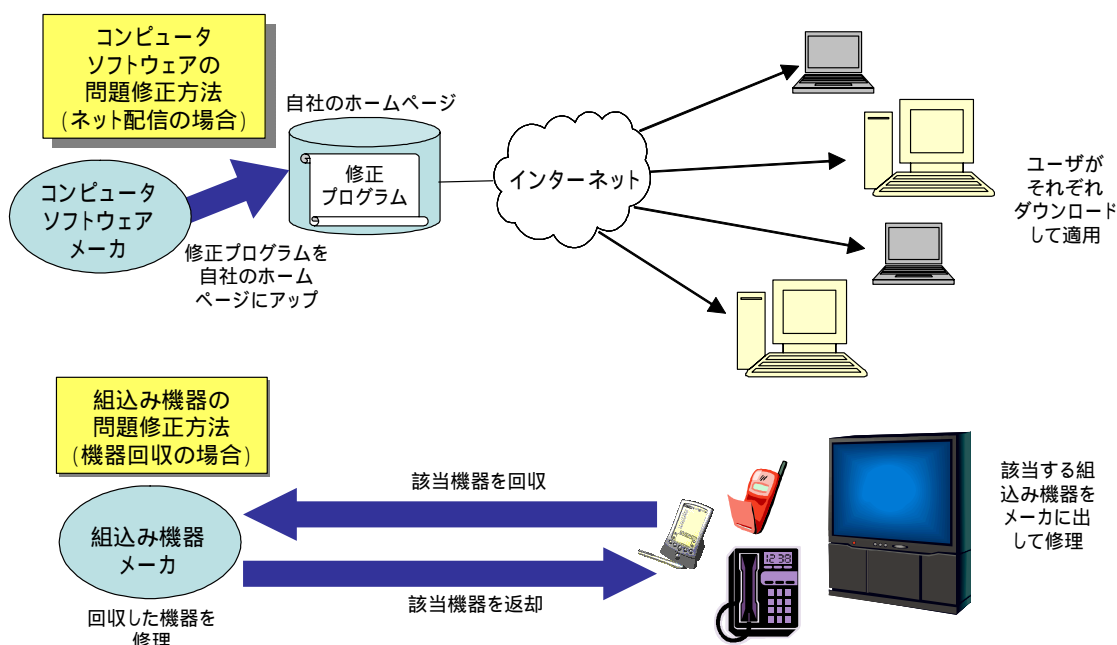


図 5 コンピュータソフトウェアと組み込み機器の問題修正方法

<sup>6</sup> i アプリの更新（バージョンアップ）を行なうと、データを上書きしたり、データが外部に読み出されたりする可能性があった。

## 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：携帯機器がウイルスに感染、起動できなくなる

海外では、「Symbian OS」を搭載した携帯電話に感染するウイルスが多数発見されています。2005年4月に発表されたものの多くはBluetooth<sup>7</sup>を通じて感染を広げ、システムのダウンを引き起こすという性質が報告されています。また、2005年9月には、北欧の企業で携帯電話ウイルスが猛威を振るった記事が報道されました。

2005年10月には、携帯ゲーム機を対象とするウイルスの存在が報告されています。感染すると、システムファイルを削除して正常な再起動をできなくしてしまう性質を持つとされています。



図 6 「Symbian OS」に感染するウイルスの特徴

<sup>7</sup> 携帯情報機器間をつなぐ無線通信技術の規格で、様々なデバイスが容易にかつ自律的にネットワークを構成できる、機器間の距離が10m以内であれば障害物があっても利用できるといった特長がある。その一方、接続時に認証を行わないため、ウイルスの伝播経路として悪用される可能性がある。

## トラブル事例 2 : ATM、POS 端末等の専用システムが感染し、サービス不能に陥る

2003年8月には、「MS Blaster」等のウイルスが全世界的に猛威を振るいました。このウイルスは、脆弱性があるパソコンを標的として自律的に感染を広げる性質があり、被害は急速に拡大しました。

北米では、パソコンだけでなく、金融機関のATMやPOS端末、飛行機のチェックインシステム等にまで感染が広がり、その多くがダウンしました。北米では、こうした専用システムにWindowsが広く採用されていますが、これらの専用システムにパッチを適用することは困難なため、脆弱性が残っていたことが原因と見られています。

国内でも、MS Blasterがプリンタサーバに感染する恐れがあることがメーカーから発表されました。

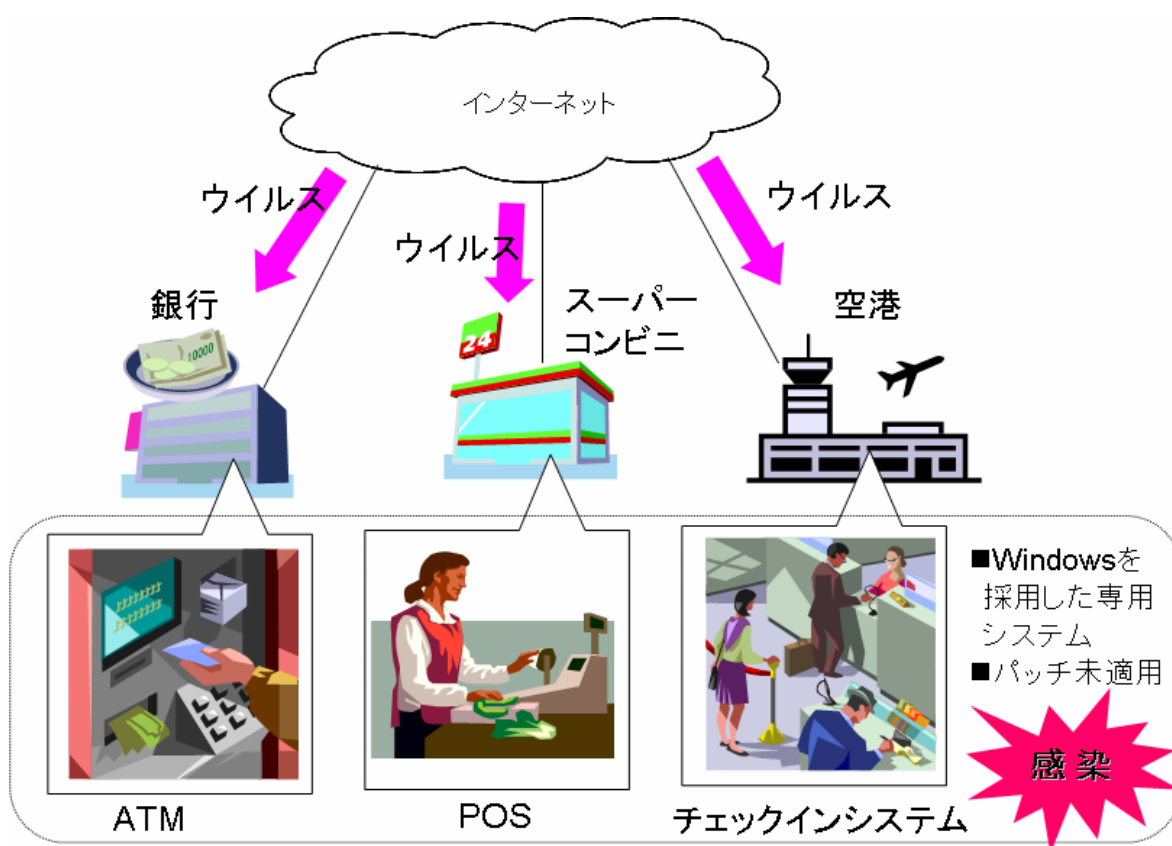


図 7 北米で MS Blaster が専用システムに感染した流れのイメージ

## トラブル事例 3 : ルータ<sup>8</sup>の脆弱性が悪用され、コントロールが奪われる

通信制御装置であるルータについても、OS を中心に、これまでいくつかの脆弱性が報告されています。

2005 年 7 月には、米国のセキュリティ研究者がセキュリティ関連イベントにおいて、某社のルータの脆弱性を悪用しコントロールを奪うデモを実施しました。同社は、研究者がこの情報を違法に入手したとして告訴しました（その後和解）。デモでは攻撃方法の詳細については開示されませんでした。インターネットインフラを支えるルータに対してそうした攻撃が可能であるという事実は、情報通信業界に大きなインパクトを与えました。

もし、このような攻撃方法がネット上で公開され、ウイルスに組み込まれたとすれば、世界中のルータに当該脆弱性を修正するパッチ等の対策を適用しない限り、大混乱を招くことは必至と考えられます。特に、対策が公表される前にウイルスが出現した場合は最悪の状況となります（図 8 ケース 3 参照）。

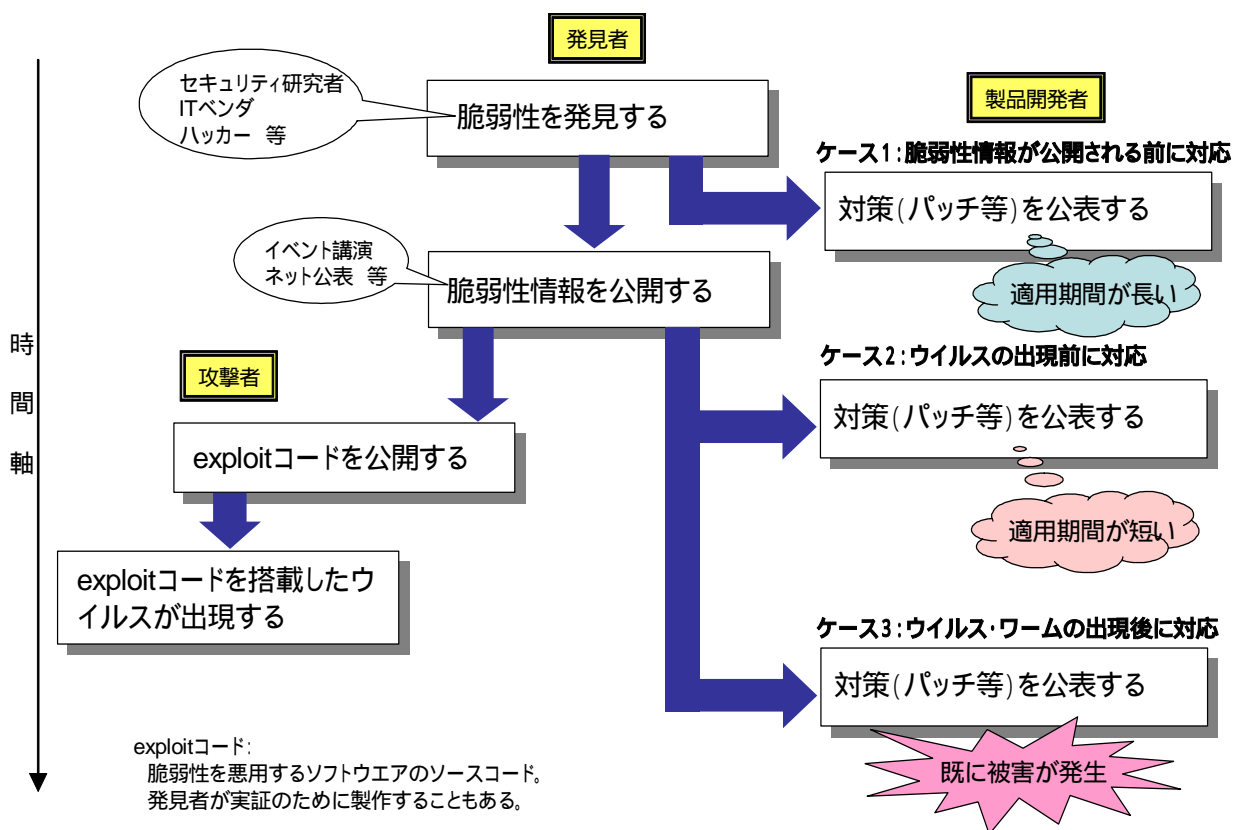


図 8 脆弱性の発見から攻撃・対策に至る流れ

<sup>8</sup> 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見て、どの経路を通して転送すべきかを判断する経路選択機能を持つ。

## **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、パソコン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のでしょうか。

#### **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、メーカーとしての責務と言えるでしょう。

## 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・連携は必要になります。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。

メーカー 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、委員会の下で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。

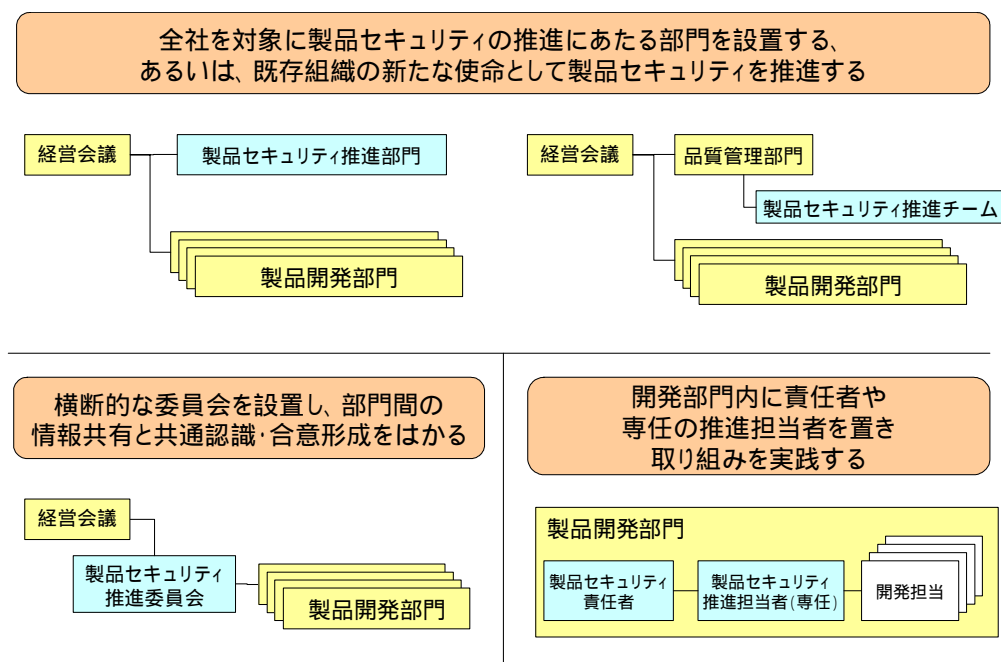


図 9 セキュリティ確保のための体制の例

### 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/IEC 15408 (コモンクライテリア)<sup>9</sup> 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/IEC 15408 は、政府調達要件として位置付けられており、メーカとしては今後対応が必須となる可能性もあることから、有用な取組みと言えるでしょう。

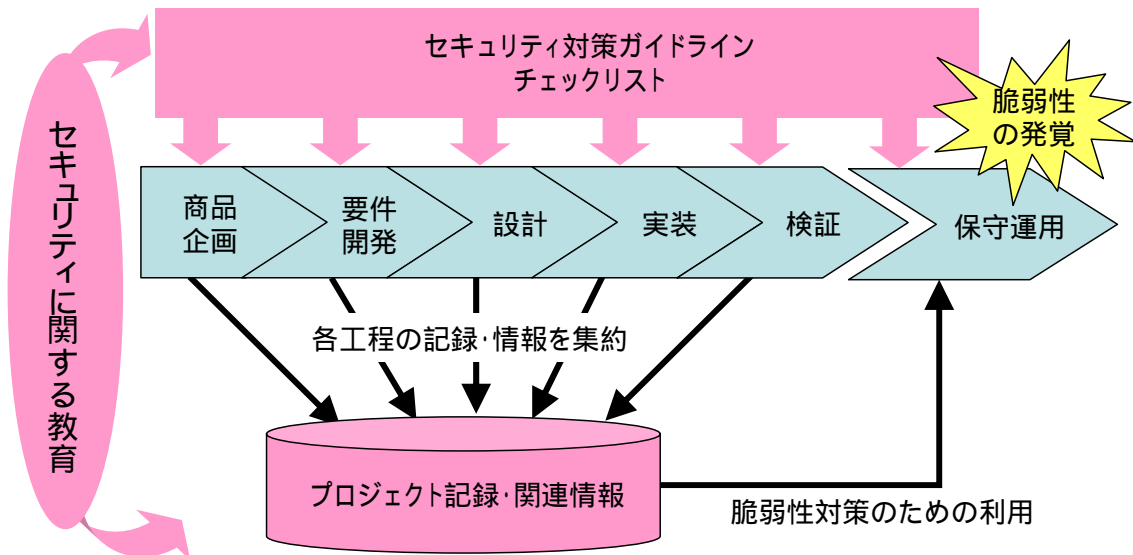


図 10 セキュリティに関する教育・ルールの構造

<sup>9</sup> 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、セキュリティ企業に出荷直前の製品を対象としたセキュリティ監査サービスを委託したところ、攻撃者がネットワーク越しに任意のタイミングで当該機器の動作不全を起こすことができる脆弱性が発見されました。D 社で開発したソフトウェアの入力チェックのミスが原因でした。該当製品の初期出荷予定 2 万台を対象に修復作業がなされ、対外的には無事に出荷することができました。

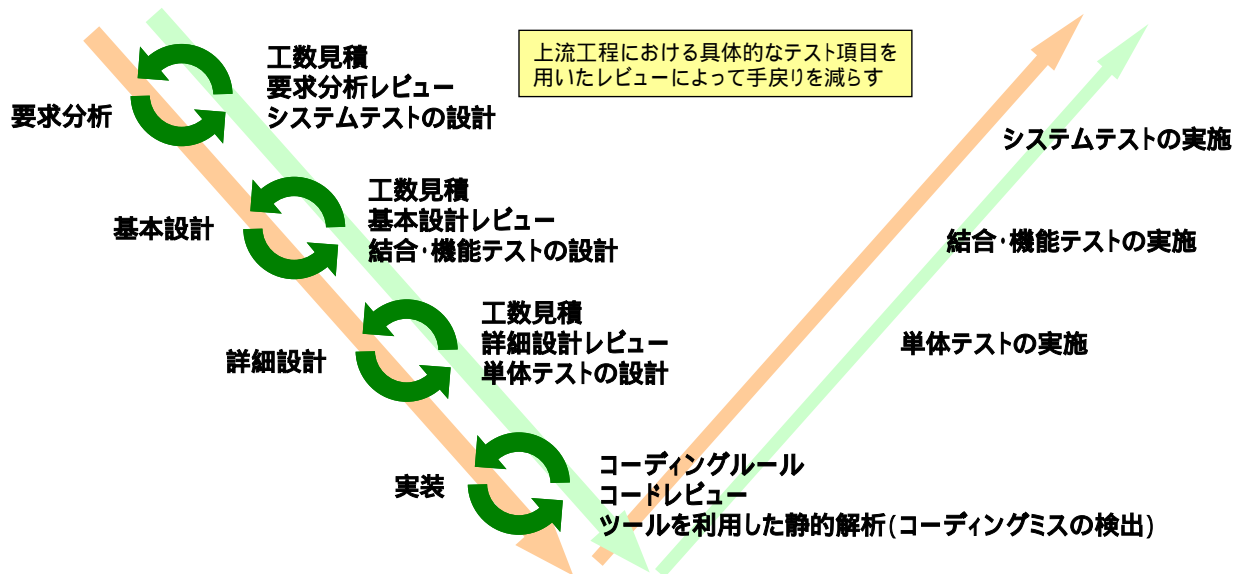


図 11 各プロセスにおけるレビューの実施

### 3.2.4. 事後対応

トラブル発生時の事後対応については、事例を中心に紹介します。

#### 対処事例 1：踏み台<sup>10</sup>にされたハードディスクレコーダの改修

インターネット対応のハードディスク DVD レコーダをインターネット上に接続すると、anonymous proxy<sup>11</sup>として動作してしまう脆弱性が発覚しました。こうした使用法は、メーカー側では想定していませんでしたが、実際にこの脆弱性を悪用して、レコーダを踏み台にする形で特定の電子掲示板に大量のコメントを書き込む攻撃が行われ、攻撃者の発信元を調べていくうちにその問題が明らかになりました。

同メーカーでは対策として、ソフトの修正版への更新（バージョンアップ）もしくはセキュリティ設定の変更を行うよう、当該機器のユーザに呼びかけました。さらに、今後発売する機種に関しては、セキュリティ設定が危険な形に設定できないよう、企画の基本方針から変更することを明らかにしています。

脆弱性が悪用され踏み台にされた典型的なケースですが、情報家電分野では先行事例もなく、担当者は手探りで対処に臨んだと考えられます。

なお、デジタルテレビ等では、放送波を通じたソフトウェアの配信・更新が行われており、同様な手段で修正プログラムを配信・適用することも可能です。

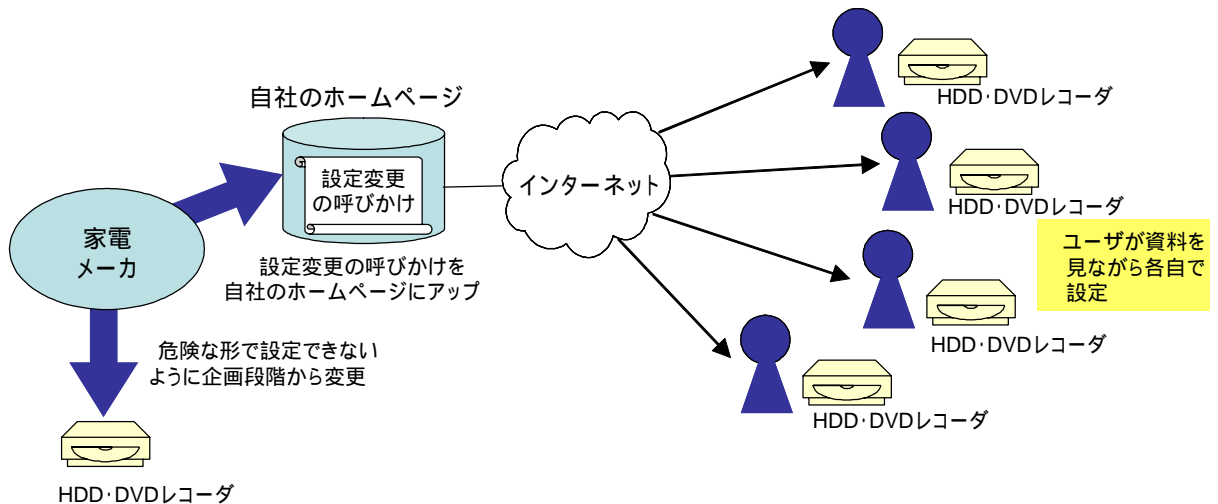


図 12 ハードディスク DVD レコーダの改修方法

<sup>10</sup> 悪意の第三者が、ユーザに気づかれないようにコンピュータ等を乗っ取り、不正アクセス等の中継地点に悪用すること。

<sup>11</sup> 誰でも利用できる中継サーバ。これを経由することで、攻撃者は自身の存在を隠して攻撃することができる。

## 対処事例 2：踏み台にされたルータ<sup>12</sup>の改修

某社製のルータ製品が踏み台にされサービス妨害攻撃の攻撃元にされていたことが明らかになりました。TCP/IP<sup>13</sup>の処理部分に存在した脆弱性を悪用されたと考えられています。当該ルータから攻撃を受けた機関では、サービス停止等の被害が発生しました。メーカー側は、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。

後に同メーカーでは、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。

ルータはインターネットインフラを支える基盤であり、そのトラブルは企業の事業継続にも影響を及ぼす可能性があります。単なる対処療法にとどまらず、品質管理の問題としてフィードバックした点も注目されます。

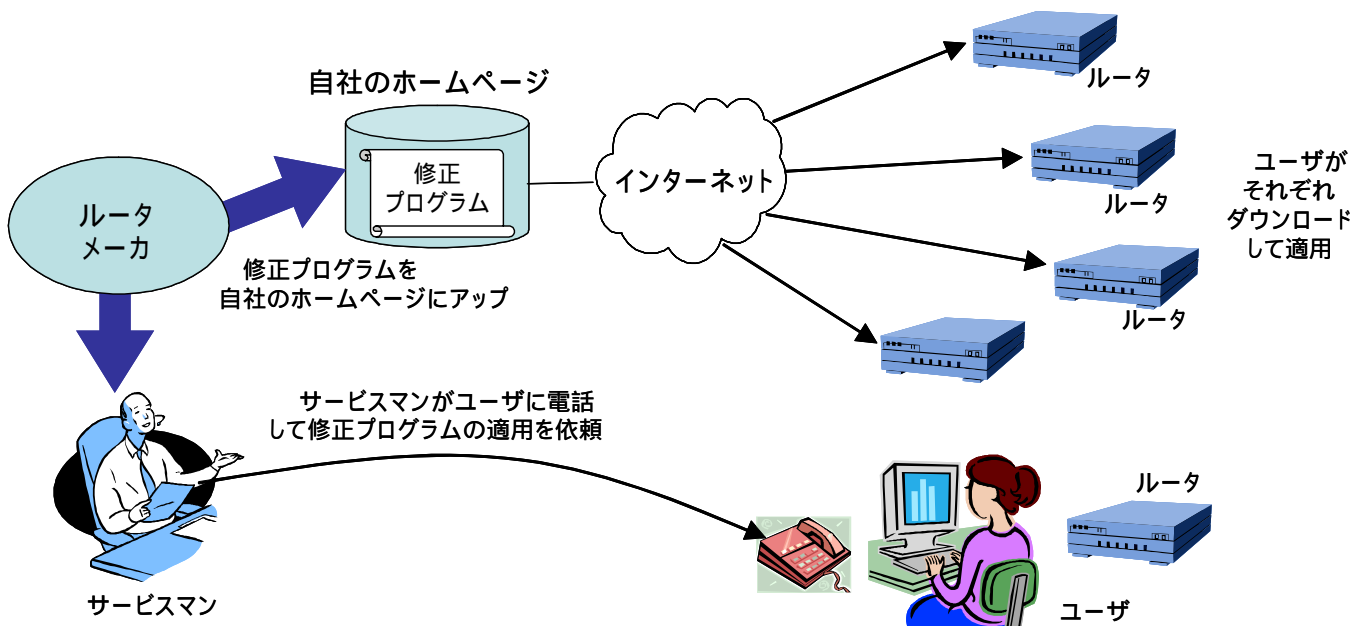


図 13 ルータの改修方法

<sup>12</sup> 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見て、どの経路を通して転送すべきかを判断する経路選択機能を持つ。

<sup>13</sup> インターネットにおいて標準的に使用される通信規約（プロトコル）。

### 対処事例 3：不具合が発生した携帯電話ブラウザの改修

携帯電話サービスにおいて閲覧中のホームページの URL<sup>14</sup>が次に閲覧するホームページへ送出される不具合が報告されました。もともと一般的なブラウザでも、閲覧中の画面から別のページへのリンクを選択した場合には、元のページの URL を付加情報としてリンク先に送る機能があります。この不具合では、特定の操作を行うと、リンクを選択していない場合でも、元のページの URL を次のホームページに送出される、というものでした。

サービス会社では、携帯電話の販売店において、無償でソフトの書き換えを実施しました。1 回の書き換えに 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。

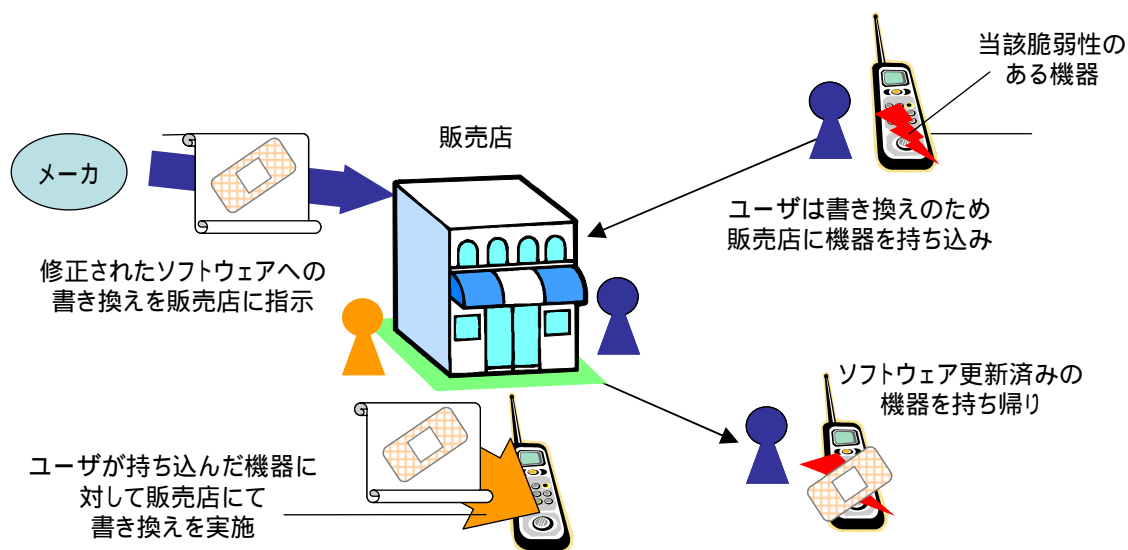


図 14 携帯電話ブラウザの改修方法

<sup>14</sup> Uniform Resource Locator：インターネット上の情報資源（文書や画像など）の場所を一意に特定する記述方式。インターネット上の、いわば住所のようなものにあたる。

## 対処事例 4：広範に影響する通信プロトコルの脆弱性への対処

多様な機器に採用されている通信プロトコル IPsec<sup>15</sup>の脆弱性が、英国のセキュリティ機関 NISCC<sup>16</sup>から公開され、悪用されると機能停止の可能性があるとして話題となりました。仕様の記載が曖昧で、解釈に幅があったため、実装段階で複数の脆弱性を内在する結果となったと見られます。

対象製品は非常に幅広く、ネットワーク関連の製品のほぼすべてに影響したメーカーもありました。対処策としては、通常のコンピュータソフトウェアと同様に、メーカーは修正プログラムを提供し、ネットワークを通じてユーザ自身が適用する手法が採用されました。

通信プロトコルの脆弱性は、コンピュータだけでなく、組み込み機器にも影響を及ぼしうるため、公表された脆弱性情報や対処方針について、コンピュータ部門と組み込み機器部門が共有・整合を図る必要があります。

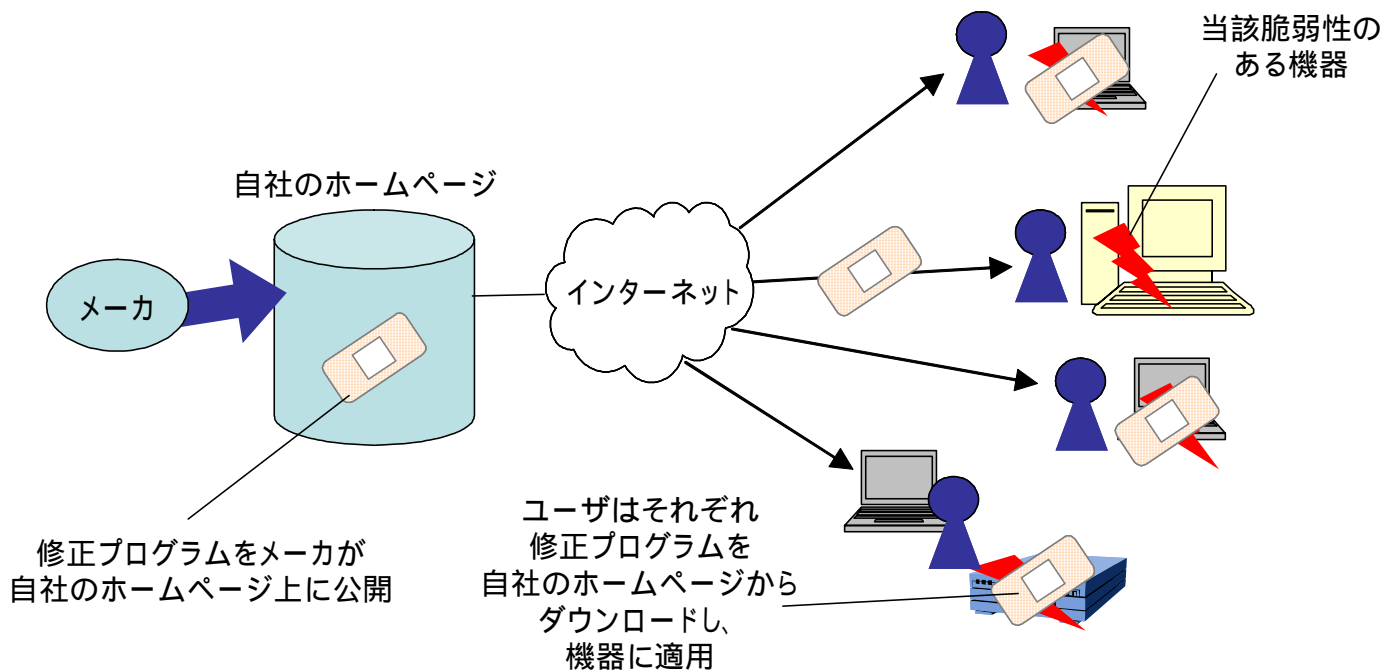


図 15 広範に影響する通信プロトコルの脆弱性への対処方法

<sup>15</sup> IPsec : ( Security Architecture for Internet Protocol ) インターネットにおいて、暗号通信をするための規格。

<sup>16</sup> 英国の国家インフラストラクチャ安全調整局 ( National Infrastructure Security Co-ordination Centre )、重要インフラ保護に関する責任を有し、脆弱性情報の収集・分析や重要インフラへの対策適用を行っている。

### 3.3.その他の留意点

#### 3.3.1. 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」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、ソフトウェアを組み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み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<sup>17</sup>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のでしょうか。

#### 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み込み機器では、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、ユーザとメーカー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対応・処理について教育しておく必要があります。

---

<sup>17</sup> 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）。

# 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。

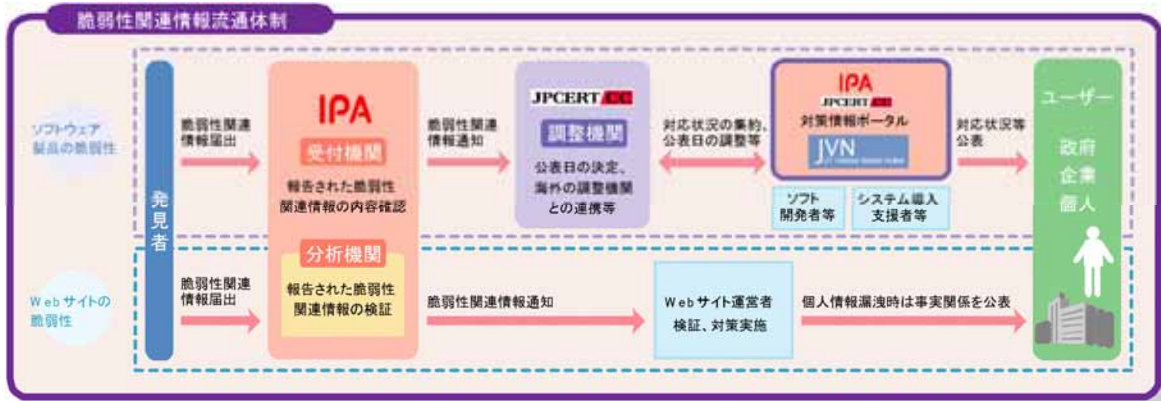
## ソフトウェア製品脆弱性関連情報

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<sup>®</sup>

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/>