INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

組込みソフトウェアのセキュリティ

機器の開発等における
セキュリティ確保のための 40 のポイント

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

1.概要

1.1.背景

組込み機器における情報セキュリティの問題は、多くの組込み機器にとって重要な課題であり、組込み機器の開発者一人一人が問題意識を持って、この問題に対処する必要が生じている。特に、ネットワークに接続された組込み機器においては、他の組込み機器や PC 等からの不正なアクセスやウイルス等の感染、それによる重要データの消失や流出、および当該組込み機器が踏み台となっての他の組込み機器への攻撃の仲介等、従来とは全く異なる情報セキュリティに係わる新しいリスクが存在することが明らかになっている。

一方、インターネットに接続された PC やサーバにおいては、他のマシンからの不正アクセスや他のマシンへの踏み台攻撃は多くの人々が認識する現実となっており、そうしたリスクの原因は、攻撃によってソフトウェアの性能や機能を著しく損なう「脆弱性」である。現在、脆弱性は、製品出荷後に発見されることが多々あり、製品開発者はその対応に努めようとしているが、出荷後に脆弱性に対応することは多大なるコストがかかることも指摘され、一部企業においては負担の大きさのため対応困難となっている。

PC やサーバにおける脆弱性とそれに係わる情報セキュリティ上のリスクの問題は、組込み機器においても一層重要な問題となることが推測される。

このような状況を踏まえると、ネットワークに接続された組込み機器に関してそれに係わるリスクに備えるため、企画・設計・実装段階からのセキュリティの作り込みを行うことが喫緊の課題であり、そうしたセキュリティの作り込みの方向性を示す手引書が求められている。

（なお、本書の背景については、独立行政法人　情報処理推進機構編：「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」を参照のこと。）

1.2.目的

本手引きは、ネットワークに接続された組込み機器に関するセキュリティ対策の推進における主なポイントを製品開発者に提示することを目的とする。以下では、これらのポイントについて、脆弱性を作り込まないことを念頭に置き、製品のライフサイクルに沿って示す。

作成にあたっては、組込みソフトウェアの開発現場における諸事情に合わせて、幾つかのポイントを選び、段階的にセキュリティ対策を推進し充実させていくことを想定した。提示するポイントについては網羅性や詳細度に重点を置くものではない。

1.3.想定読者

本書の想定読者は、ネットワークに接続された組込み機器（以後、ネットワーク組込み機器）の開発に携わる技術者および開発プロジェクト責任者である。

1.4.用語の定義

組込み機器：家電等の汎用品において、内部にチップを搭載して特定目的のソフトウェアが稼動している機器。

ネットワーク組込み機器：ネットワークに接続された組込み機器。

リスク：主として脆弱性を悪用した攻撃により発生する事象。

脆弱性：当該組込み機器やネットワークに接続された他の機器・ネットワークの機能または性能に多大な影響を与える攻撃を受け入れる要因。

セキュリティ方針：機器ごとに定義されたリスクに対する対策方針。

2.組込み機器におけるセキュリティとは

2.1.組込み機器におけるリスクとは

組込み機器が脆弱性を有する場合、脆弱性を悪用した攻撃により当該組込み機器またはネットワークに様々な影響が発生する。こうした影響が組込み機器におけるリスクである。

こうしたリスクに関しては、「独立行政法人　情報処理推進機構発行：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」の「２．組込み機器に潜む危険性」を参照のこと。

2.2.ネットワーク組込み機器におけるセキュリティ対策の概要

本手引きでは、組込み機器の、企画、設計、実装、運用というライフサイクルに沿って対策の主なポイントを述べ、管理面、技術面から以下の視点にて整理を行った。

管理面：経営層およびプロジェクトの管理者が実行する事項

技術面：技術者が実行する事項

なお、企画、設計、実装、運用以外に、ライフサイクル全体、およびその他注意事項に関してもまとめた。本手引きは、以下の図におけるセキュリティ対策ガイドラインおよびチェックリストの位置づけとなっている。

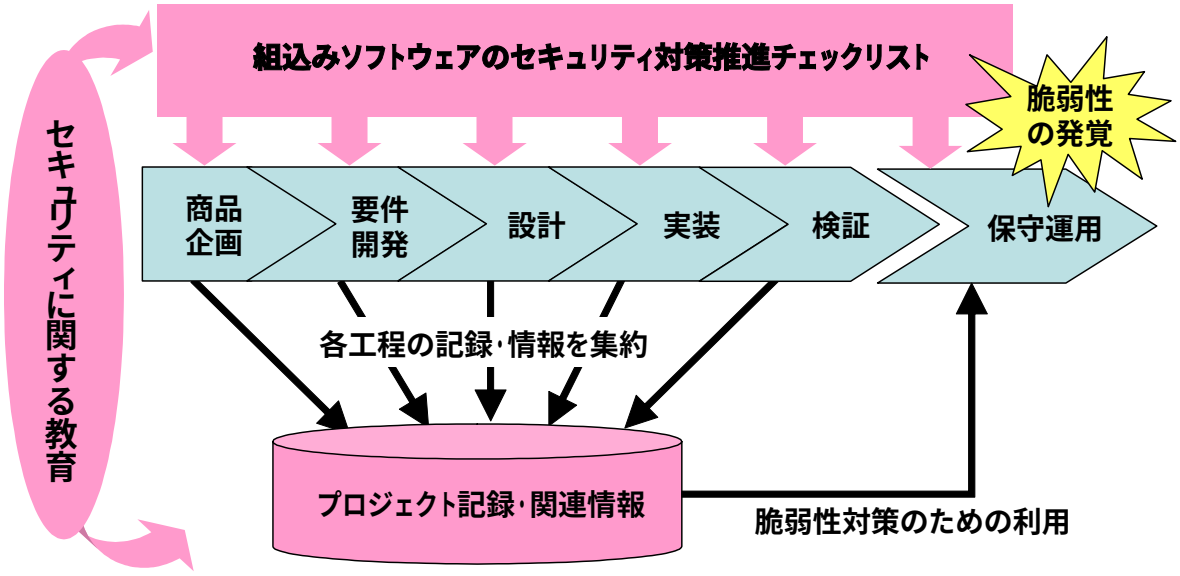


図１　本手引きの位置づけ

3.組込み機器におけるセキュリティ対策のポイント

3.1.ライフサイクル全体に係わる事項

3.1.1.管理面

Point_1)　プロジェクト監査組織（プロジェクトマネジメントオフィス）にセキュリティ専門家を配置する

プロジェクト監査組織（プロジェクトマネジメントオフィス）に、セキュリティ専門家を配置することが望ましい。

セキュリティ専門家とは、以下の条件を備えていることが必要である。

- 情報処理技術者試験における「テクニカルエンジニア（情報セキュリティ）」を取得していること
- セキュアプログラミングの知識を有すること
- 暗号技術および認証技術に係わる知識を有していること
- 最新のインターネットセキュリティを中心とする情報セキュリティの動向を把握していること

セキュリティ専門家は、プロジェクト監査組織にて、以下の業務を担当する。

- 企画、設計、実装それぞれのフェーズにおけるデザインレビューへの参加による、セキュリティ対策上の問題点の指摘とチェックを行う
- 日常的に脆弱性情報や攻撃情報を収集する
- 日常的に開発チームに対するセキュリティ教育を行う
- 企画、設計、実装時において発現した脆弱性に関して、開発チームに対応方法をアドバイスする

Point_2)　開発技術者と開発管理者全員に対してセキュリティ教育を実施する

開発部署においては、開発技術者と開発管理者向けのセキュリティ教育体制を整え教育を実施する。その際には、担当講師および現場の実情に合わせたカリキュラムについて計画を立て実践する。特に、最新のセキュリティ動向についての講義には重点を置く。

担当講師は、社内外のセキュリティ専門家を招く。

カリキュラムの例を以下に示す。

開発技術者向け　カリキュラム例
1．最近の組込み機器のソフトウェアに関係するセキュリティの話題
2．セキュアなプログラミング
3．セキュリティを確保するためのテスト方法

開発管理者向け　カリキュラム例
1．最近の組込み機器のソフトウェアに関係するセキュリティの話題
2．セキュリティを確保するための開発体制
3．セキュリティを確保するための開発管理の方法（レビューとテスト管理）

Point_3)　セキュリティに係わる開発の外部委託先等に対して、自社と同程度のセキュリティ技術レベルの向上を求める

開発の外部委託を行う際、セキュリティ技術のレベルの向上を求める。具体的には、以下の 2 項目を実施する。

- 社内と同様のセキュリティ技術のレベルを確保することを目的として、本手引きに概要を示すセキュリティ対策・体制の整備を要求する
- 外部委託先の開発担当者に情報処理技術者試験のテクニカルエンジニア（情報セキュリティ）の取得を促す

Point_4)　開発プロセス標準の全てのフェーズにおいて、セキュリティに係わる実施項目を設定する

全てのアクティビティにおいて、セキュリティに係わる実施項目を設定する。各アクティビティにおけるセキュリティに係わる実施項目は本手引きを参照し設定するとよい。以下は代表例である。

フェーズ	管理面	技術面
企画	・セキュリティ要件の文書化 ・コールセンターと不具合対応部署へのセキュリティ教育 ・対策プログラムの発信方法の策定	・セキュリティに係わるリスクの定義 ・セキュリティ方針の明確化 ・誤操作・誤設定に対する対応の決定 ・なじみ無い機能の安全側設定 ・組込み機器の仕様の決定 ・セキュリティログ保全機能の設定 ・ネットワーク経由の不正なアクセスに対するユーザへの警告方法の決定 ・機密データ廃棄手順の実装方法の決定
設計	・セキュリティ技術専門家の参画 ・外部ソフトウェアに対するセキュリティに関する基準の明確化 ・完成時のセキュリティ検査の明確化 ・インターネットのアプリケーション利用における専門家の担当	・データの機密度に応じた論理的物理的配置の決定 ・プログラムの実行単位とプロセッサへの配置の決定 ・機密データの推測が可能とならない設計法の決定 ・ネットワークデバイスとプロトコルスタックの利用法の決定 ・一般ユーザが利用しない機能におけるアクセス制限の決定
実装	・実利用環境における攻撃実験環境の整備 ・コードの出所・版管理の実行	・ネットワークに接続されるインタフェース全てにおける攻撃試験の実施 ・機器の動作状態観測による攻撃テストの実施 ・入力データのために準備したバッファサイズ以上に読み込むことが無いことのチ

		ェック ・実装工程におけるテストの実施
運用	・セキュリティに係わる障害情報のユーザへの適切な告知 ・脆弱性情報取扱い体制の構築 ・脆弱性情報の収集の実施	・コールセンターの適切な対応の実施
その他	・マニュアルにおける緊急避難措置の掲載 ・マニュアルにおける機密データ廃棄手順の掲載 ・製品カタログとマニュアルにおけるセキュリティ上の注意事項の掲載	

Point_5)　脆弱性情報、攻撃情報をはじめとする各種のセキュリティ関連情報を収集し、技術者に対して周知徹底する

JVN（JP Vendor Status Notes）を中心とするインターネット上のセキュリティ関連情報を収集し、技術者に対してそれらの情報と対策に係わる情報を提供することにより、周知徹底に努める。

セキュリティ関連情報を示すサイトの URL を以下に示す。

- JP Vendor Status Notes http://jvn.jp/
- IPA 緊急対策情報一覧 http://www.ipa.go.jp/security/announce/alert.html
- CERT Advisory http://www.cert.org/advisories/
- CVE http://cve.mitre.org/
- SecurityFocus http://www.securityfocus.com/vulnerabilities

3.1.2.技術面

Point_6)　脆弱性情報、攻撃情報をはじめとする各種のセキュリティ関連情報を参照し、各工程において適切な対策を実践する

上記 Point_5)で挙げた URL を参照し、各工程において適切な対策を実践する。

対策に関する情報を示すサイトの URL を以下に示す。

- IPA　情報セキュリティ対策実践対策情報
  http://www.ipa.go.jp/security/awareness/awareness.html

3.2.企画フェーズに係わる事項

3.2.1.管理面

Point_7)　組込み機器の非機能要件の一つとしてセキュリティに対する要件が明確化され、かつ文書化されていることを確認する

組込み機器において、セキュリティ対策が必要である場合、セキュリティ要件を明確にする。セキュリティ要件は、Common Criteria Ver3.0 を参照し、明確にするとよい。セキュリティ要件に関しては、以下を参照する。

IPA　セキュリティ評価認証参考資料　http://www.ipa.go.jp/security/jisec/apdx0504.html

以下から製品の特性を勘案し、取捨選択する。

- 識別と認証
- 利用管理
- アクセス管理
- 信頼パス
- 保管データの秘匿性と完全性
- 残存データの管理
- 証拠性の確保
- 監査ログデータの収集
- プライバシ保護
- 情報フロー管理
- 転送データの秘匿性、完全性
- 不正再送／削除／挿入防止
- セキュリティ管理
- 暗号鍵管理
- セキュリティ機構の保護

Point_8)　コールセンターと不具合対策部署に対するセキュリティ教育を、製品出荷前から以後定期的に実施する

コールセンターと不具合対策部署に対するセキュリティ教育を実施する。このセキュリティ教育の内容としては、セキュリティに関する最新の用語、最新の脆弱性情報、ウイルスおよび不正アクセス情報が含まれる。

以下を参照する。

IPA　緊急対策情報　http://www.ipa.go.jp/security/announce/alert.html

IPA ウイルス一覧　http://www.ipa.go.jp/security/virus/virus_main.html

IPA 新種ウイルス情報

http://www.ipa.go.jp/security/topics/newvirus/newvirus-top.html

IPA 不正アクセス対策　http://www.ipa.go.jp/security/fusei/ciadr.html

Point_9)　セキュリティ上のトラブルを解消するための対策の発信方法を策定する

出荷後に、製品の脆弱性が発現した場合に備え、以下の方法による脆弱性の修正手段の提供について可否を予め検討する。

・ネットワーク経由の修正プログラム配信
・CD-ROM 等の媒体による提供
・店頭におけるソフトウェア交換
・ROM など部品の交換
・製品全体の交換　等

3.2.2.技術面

Point_10)　製品が利用される可能性のある接続形態や動作環境および利用形態を想定して、セキュリティに係わるリスクを定義する

製品を企画する際には、製品がネットワーク上の他の製品に影響を及ぼし、単独の製品では発生し得ない現象が発生しうることを念頭に置く。この時、製品が利用される可能性のある接続形態や動作環境を想定することが重要である。想定される接続形態や動作環境において、他の製品とのネットワークを介した関係を念頭に置いて製品を企画する。セキュリティに係わるリスクとは、以下を想定できる。

1)　当該ネットワーク組込み機器における機密データの消失や流出
攻撃を受け、当該ネットワーク組込み機器に蓄積されている個人情報等の機密データが消失するまたは流出するリスクがある。

2)　当該ネットワーク組込み機器における機能面での障害
攻撃を受け、当該ネットワーク組込み機器がフリーズや再起動する等の機能面での障害が発生するリスクがある。

3)　ネットワークや他の機器への悪影響
当該ネットワーク組込み機器を踏み台にする攻撃、またはウイルス等の感染により、当該ネットワーク組込み機器が異常なパケットを発信し、ネットワークや他の機器に影響を及ぼすリスクがある。

Point_11)　制約条件を考慮して、実装予定の機能に対して、定義されたリスクに対する対策方針（セキュリティ方針）を明確にする

組込み機器の機能や稼動する環境およびユーザの特性を考慮して、リスクに対するセキュリティ方針を明確にする。リスクに対応する方針としては機能の削除、機能の変更も考

えられる。

セキュリティ方針は、以下のように設定する。

a) リスクが大きく、対策の策定が不可能であるため、機能を実装しない

b) 予定通りの機能ではリスクが大きすぎるため、機能の変更を行う

c) リスクを回避する方法を実装し、機能の変更は行わず予定通り実装する

Point_12) ユーザによる設定変更の可否や手法および誤操作・誤設定に関して、セキュリティ上のリスクを勘案して決定する

製品ごとに、セキュリティに係わるデフォルトの設定およびユーザによる設定に関して、利便性とリスクを勘案し、その可否と方法を決定する。検討項目には、以下のようなものがある。

- 設定を変更するためのパスワード
- ネットワークを介した設定の変更
- ネットワークを介した組込み機器の操作
- 使用可能とするポート番号　等

Point_13) 一般のユーザに馴染みの無い機能または普段使用されることが少ない機能については、特に安全側を意識した設定を行う

ユーザが、セキュリティ上の誤操作・誤設定を起こさないようにわかりやすい警告表示画面、初期設定のフロー等に関して企画する。これらに関しては、以下において特に留意する。

- マニュアルに操作法が、分かりやすくかつ正確に記述されていること
- ユーザインタフェース（特にボタンと画面）について、ユーザの誤操作を招くことがないように工夫されていること
- ヘルプ機能により操作法を解説すること
- デフォルトの設定は、安全側とすること

Point_14) セキュリティ方針を考慮し、組込み機器の仕様を決定する

上記 11)でセキュリティ方針を決定した後、組込み機器の各機能に関して機能仕様をセキュリティ方針の下に決定する。具体的には、各機能について以下の方向で決定する。

- ソフトウェアとして実装する
- ハードウェアとして実装する

また、上記の決定の際に、以下を含む留意事項を付記し文書化する。

- 暗号化プロセッサや暗号化メモリおよび暗号化ハードディスクの利用の有無
- 認証用特殊デバイス（IC カードやバイオメトリクスデバイス）の利用の有無

Point_15) セキュリティに関するログ保存機能を設定する

セキュリティに関連するログを取り保存する機能を製品に備える。ログを参照することで原因を追究し問題を解決する手がかりが得られる。セキュリティに関連するログは、以下に例示する。

- パケットの受信に係わるログ（送信元 IP アドレス、送信元ポート番号、受信元ポート番号、パケットサイズ、時刻）
- パケットの発信に係わるログ（送信先 IP アドレス、発信元ポート番号、送信先ポート番号、パケットサイズ、時刻）
- ユーザの認証に係わるログ（システムが受信したユーザ ID、時刻）

なお、ログの保存期間は、メモリやハードディスクとの関係で可能ならば、ユーザがサービスセンターに連絡してサービスセンターが対応可能となるまでの時間以上とする。

Point_16) ネットワーク経由で正当と想定されるアクセスとは異なるアクセスを検知した場合、他の警告と区別できる形でユーザに警告する機能を備える

ネットワークに接続されている機器においては、正当なアクセスを判定する機能を備え、ネットワークを介した正当ではないアクセスを検知した際に、ユーザに警告する機能を備える。正当ではないアクセスを、以下に例示する。

- 特定期間における多すぎるパケットの受信
- 特定期間における多すぎるパスワード誤入力
- 尋常ではない非常に大きなサイズのパケットの受信
- 閉じられているポートへのアクセス（これに関しては、必ずしも警告を発する必要は無い場合もあるため、製品ごとに検討する）

また、ユーザへの警告に関しては、以下の点にも配慮する。

- 警告メッセージにて、異常な状況であることおよびネットワーク切断等の緊急避難の方法を分かりやすく表示すること
- ヘルプ機能において、警告メッセージの詳細な解説を表示し、正当ではないアクセスの技術的詳細を示すこと

Point_17) ユーザの機密データの廃棄をサポートする機能を実装する

ユーザが機密データを消去できる機能を実装する。そのためには、ユーザの機密データの特定方法、廃棄のための技術的手法を実装する。具体的には、ユーザの機密データを特定するためには、あらかじめそうしたデータを一般のデータとは別の領域（別のパーティション）に格納する。ハードディスクにおけるデータの物理的消去機能（通常のファイル削除機能は、リンクを切るのみであることが普通である）を実装する。

3.3.設計フェーズに係わる事項

3.3.1.管理面

Point_18) ソフトウェア開発にセキュリティ技術に関するドメインスペシャリスト（セキュリティ専門家）を参画させる

設計物のレビューにあたっては、セキュリティ面からのチェックを行う。チェック項目の作成は、セキュリティ専門家を中心とした体制により、本手引きにおける Point_22)～Point_27)を参照し、製品ごとに策定する。セキュリティ専門家は、チェック項目の作成だけではなく、設計フェーズ中に少なくとも一度は、チェック項目に基づいた設計文書のレビューを行う。レビューの結果は必ず文書化し、最終的な設計文書に反映させる。

総括すると、設計フェーズにおいて、セキュリティ専門家は以下を実施する。

- 設計文書に対するチェック項目を作成する
- チェック項目に基づき設計文書をレビューする
- レビュー結果を文書化する
- 文書化されたレビュー結果が、最終的な設計文書に反映されていることを確認する
- インターネットアプリケーションに係わる一連の作業（選定、調整、動作設定、テスト）を行う（Point_21）参照）

Point_19) 外部から導入するソフトウェアについて、セキュリティに関する基準を明確に定義し文書化する

外部から導入するソフトウェアの選定にあたって、セキュリティ面から評価する基準を明確にする。以下に基準例を挙げる。

- ソフトウェアの保守運用が自社または外部組織で可能であること
- ソフトウェアの版管理が外部組織にて明確になされていること
- 報告された脆弱性に対して、導入を予定する版では修正がなされていること
- 脆弱性が報告された場合、外部組織が対応できる体制であること

さらに、これらの基準により、外部のソフトウェアの導入に際し、採否の判断を下した結果と理由を文書化する。

Point_20) 完成時のセキュリティ検査について観点・項目を整理しておく

組込み機器としての納品検査手順を明確化する。以下のような点に留意する。

- 悪意を持った攻撃による影響の確認（ポートスキャン、不正なパケットの送付、大量のパケットの送付など）
- ユーザによる設定変更の適切さ（ユーザ層、使用環境を考慮して判断する）
- 廃棄時における個人情報を含む機密データ消去の適切さ（ユーザ層、使用環境を考

慮して判断する）

- ヘルプ機能の適切さ
- マニュアルにおけるセキュリティ関連記載事項の適切さ

Point_21) インターネットアプリケーションの利用にあたっては、選定から動作設定・テストに係わる一連の作業をセキュリティ専門家に担当させる

インターネットアプリケーションの開発に際しては、設計、実装、運用の全てのフェーズにおいてセキュリティ専門家に任せる。インターネットアプリケーションとは、インターネット上で稼動するというだけではなく、IP ネットワーク上で稼動するアプリケーションを含む。これは、アプリケーションが IP 上で稼動している場合、ユーザの稼動環境によっては、インターネットに接続される可能性があるためである。インターネットアプリケーションは、以下を含む

- 各種サーバ（ウェブサーバ、プロキシサーバ、メールサーバ、DNS サーバなど）
- ブラウザ
- ブラウザ上で稼動するツール
- ストリーミングツール
- メーラ
- 通信路暗号化ツール
- ミドルウェア　など

3.3.2.技術面

Point_22) データを機密度に応じて区分し、ハードウェアおよびソフトウェアの保護機能を考慮し、データの物理的および論理的配置を決定する

データの機密度を考慮し、物理的配置および論理的配置を決定する。例えば、スタックには個人情報を含む重要情報を配置することは極力避け、常に、外部記憶装置にこうした重要情報を配置する等の配慮を挙げることができる。

以下にデータの機密度に応じた配置方針の例を挙げる。

機密度	例	論理的配置	物理的配置
非常に高い	ID、パスワード、氏名、住所、電話番号　など	ファイル	暗号化されたハードディスク
高い	アクセス履歴、トラフィックログ　など	ファイル	ハードディスク、不揮発性メモリ
その他	処理中のテンポラリデータ　など	バッファ、スタック	揮発性メモリ

Point_23) 機密度の異なるデータの扱い方を考慮し、プログラムの実行単位とプロセッサへの配置を決定する

機密度の異なるデータに関して、データの物理的配置および論理的配置のみではなく、実行単位の分け方とプロセッサへの配置をデータの機密度を考慮の上、それらを扱うプログラムに関しても決定する。この際には、以下の点に留意する。

- 機密性の高いデータは、特定のプロセッサのみが利用可能なローカルメモリに保持する
- 複数のプロセッサ間での共有メモリに、機密性の高いデータを保持しない
- 機密性の高いデータでないデータについても、タスクスイッチの前に共有メモリから消去する
- 非常に高い機密度を有するデータに関しては、メモリ上でも暗号化されることが望ましく、その場合は暗号化プロセッサにて実装する

Point_24) 特権モードをサポートする実行環境においては、特権モードによるプログラムの実行は必要最小限にする

特権モードをサポートする実行環境においては、悪用された際の被害を軽減するため、特権モードによるプログラムの利用は極力避ける。特に、以下の処理を行う場合、特権モードの利用は避ける。

- ファイルの入出力
- データベースへの問い合わせ
- デバイス（入出力デバイス、通信デバイスなど）へのアクセス　など

Point_25) ハードウェアの物理的な破壊や記憶領域の覗き見などの攻撃にも配慮する

組込み機器内部に個人情報等の機密情報が蓄積されている場合、攻撃者は物理的破壊による攻撃や記憶領域の覗き見等を行う可能性がある。こうした攻撃から機密情報を保護するためには、以下の機能を実装する。

- 筐体の物理的破壊を検知した場合、記憶領域のデータを消去する
- 記憶領域を取り外してもデータを読むことができないように、記憶領域が特定の環境でのみ稼動するように設計する

Point_26) ネットワークに接続される組込み機器においては外部からの攻撃を受けることを想定し、ネットワークデバイスとプロトコルスタックに関して、攻撃を無視する設定で使用する

ネットワークに接続される組込み機器においては、攻撃を無視する設定を行う。そのためには、ネットワークデバイスとプロトコルスタックの利用に際して、ネットワークから

の不正なアクセスの場合には無視するという設定を実施する。無視すべき不正なアクセスとは、以下の通りである。

- 特定期間における多すぎるパケットの受信
- 特定期間における多すぎるログインの試行
- 尋常ではない非常に大きなサイズのパケットの受信
- 閉じられているポートへのアクセス

なお、Point_16)で述べたように、ユーザには、不正なアクセスがあったことをわかりやすく伝える。

Point_27) 出荷テスト用インタフェース回路など出荷検査や開発時のテストに用いられる機能等一般ユーザの利用を想定していない機能には、厳密なアクセス制限を設ける

出荷検査や開発時に用いられる機能等一般ユーザの利用を想定していない機能に関しては、厳密なアクセス制限を設ける。最低限パスワードによるアクセス制限を設けるとともに、パスワード情報の厳密な管理を実施する。

以下に、一般ユーザの利用を想定していない機能に係わる設定については以下のように設定する。

- 運用時に、サービスセンター等が利用しないのであれば、無効化しておく
- 通常の操作で、こうした機能にアクセスできないようにする
- こうした機能にアクセスしようとするユーザには警告メッセージを出す
- パスワードによるアクセス制限を設ける
- パスワードの管理は厳密にし、絶対に一般に流出することの無いようにする
- マニュアルには、こうした機能には絶対に触れない旨の記述をする

3.4.実装フェーズに係わる事項

3.4.1.管理面

Point_28) 開発成果物の実利用環境における攻撃実験体制を整備する

開発成果物の検査に際しては、実利用環境にて攻撃実験を行う。その際には、複数の組込み機器が接続されている環境およびセキュリティ専門家を含む攻撃実験体制を整備する。

以下に留意点をまとめる。

- 攻撃実験環境には、他の機器も複数台接続する
- 接続する機器は複数の種類とする
- セキュリティ専門家には、攻撃実験仕様書の作成を依頼し、それに基づき攻撃実験を行う
- 実験環境の問題等で攻撃実験仕様を実現できない場合、セキュリティ専門家の判断を仰ぐ

Point_29) 脆弱性対応に備えたコードの出所・版管理を行う

脆弱性が発見された際に修正を行うため、ソフトウェアの開発に際して、内部開発および外部調達に係わらず、それらの出所および版管理を実施する。この場合の留意点を以下にまとめる。

- 内部開発の場合、脆弱性を発見した際、特定の版の脆弱性であるのか、多くの版に共通したものであるかについて、迅速に開発チーム内で情報共有を図る
- 外部調達の場合、脆弱性が発表された際、特定の版の脆弱性であるのか、多くの版に共通したものであるかについて、適切な情報収集と情報共有を図る

3.4.2.技術面

Point_30) 攻撃者が処理系のメモリ管理の弱点を悪用して攻撃コードを実行することが不可能にする

ネットワークから不正に組込み機器に侵入する攻撃者は、処理系のメモリ管理の弱点を悪用して攻撃コードを実行することがある。この攻撃を防止するために、プロトコルスタックからの入力データに関して、入力データのために準備したバッファサイズ以上に読み込むことがないように毎回チェックする。

なお、このポイントは、セキュアプログラミングで最も注意すべきことであり、インターネット上では、バッファサイズ以上のデータを送りつけ、その中に攻撃コードを混入する攻撃が頻繁に発生している。

Point_31） ネットワーク接続されるインタフェース全てについて、（不正侵入テストを含む）攻撃テストを実施する

ネットワーク接続される全てのインタフェースに関して、不正侵入テストを含む、悪意を持った攻撃によるテストを実施する。このテストのテスト項目の策定に関しては、セキュリティ技術の専門家に依頼する。悪意を持った攻撃の例を、以下に示す。

- 短時間の間に、膨大な数のパケットを送信する
- 非常に大きなサイズのパケットを送信する
- 複数のインタフェースに同時にパケットを送信する　など

Point_32） 機器の動作状態の観測による攻撃テストを実施する

重要な機密データを有する組込み機器においては、動作状態により機器の外部にこうした情報が漏洩しないことを攻撃テストにより検証する。この攻撃テストのテスト項目の策定は、セキュリティ技術の専門家に依頼する。動作状態の例を以下に示す。

- 電力消費量
- 漏洩電磁波の強さ
- 処理時間　など

Point_33） セキュリティの視点に係わるテスト項目を定義し、それらに基づくテストを行う

単体テスト、結合テスト、総合テストの全てのフェーズにおいて、セキュリティの視点に基づくテスト項目を定義し、それらに基づくテストを実施する。テスト項目の定義に関しては、セキュリティ技術の専門家に依頼する。

セキュリティの視点とは、以下を含む。

- 短時間に多量のパケットを送りつける
- 想定外の大きなサイズのパケットを送りつける
- 規格外の壊れたパケットを送りつける
- ネットワークに接続された複数の機器から同時にパケットを送りつける
- パスワードジェネレータを用いて偽造パスワードで何度もログインを繰り返す
- 物理的に記憶装置を取り出し、他の環境で読み出す
- 強力な電磁波を浴びせる

3.5.運用フェーズに係わる事項

3.5.1.体制面

Point_34) セキュリティの障害に係わる情報は、ユーザに対して適切に告知を行う

セキュリティの障害に係わる情報と判断された情報に関して、ユーザに対して適切に告知を行う。以下の点に留意する。

- マニュアルと製品カタログにおいて、将来的にセキュリティに係わる障害が発生する可能性があることを掲載する
- 脆弱性情報が発見された場合、自社のホームページでは、攻撃者が攻撃方法を特定できる情報を掲載するのではなく、脆弱性の概要と対応方法を掲載する
- 脆弱性情報が発見された場合は、電子メール、販売チャネル等のうち製品の特性に応じた告知を行う

Point_35) 外部から脆弱性情報およびそれに関係する情報がもたらされた際に適切な取扱いが行えるようにする

外部から自社製品の脆弱性について指摘された際に、適切に取り扱える体制を確立する。適切な体制とは、以下のような例を挙げることができる。

- 外部（JPCERT/CC や CERT/CC など）からの受付窓口（これをセキュリティ担当部署と呼ぶ）の設置
- 受付窓口にて情報を受け付けた際の、対応策策定の体制

なお、対応策には、応急措置（設定変更)、恒久的な措置（ソフトウェアの修正）があるため、各製品と脆弱性の特性に応じて、適切な選択を行う。

Point_36) 脆弱性の発見に備えて情報管理・収集・分析に努める

運用時においても、脆弱性の発見に備えて情報管理・収集・分析を行う。セキュリティ担当部署または開発チームメンバが行うことが望ましい。脆弱性情報については以下の URL に示すサイトを参照する。

- IPA 緊急対策情報一覧 http://www.ipa.go.jp/security/announce/alert.html
- JP Vendor Status Notes http://jvn.jp/
- CERT Advisory http://www.cert.org/advisories/
- CVE http://cve.mitre.org/
- SecurityFOCUS http://www.securityfocus.com/vulnerabilities

3.5.2.技術面

Point_37) コールセンターが最新のセキュリティに係わる状況を踏まえ適切に対応する

コールセンターには、製品に関する一般的質問と共に、製品の脆弱性に関する問い合わせが寄せられる。セキュリティ担当部署等は、コールセンターにおいて適切な回答が行えるように、予め以下の情報を渡す。

- 現在の脆弱性情報の公開状況
- 製品ごとの脆弱性の発見状況と対応状況
- 製品ごとの脆弱性修正の提供や適用手段に関する最新情報
- 脆弱性やセキュリティ上の問題に関して、質問を受け付けるオペレータが判断するのではなく、セキュリティ担当部署に転送する旨の指示

3.6.その他の配慮事項（マニュアル、製品カタログ、パッケージとユーザインタフェースなど）

Point_38) マニュアルに、ネットワーク接続を行う機器において、他の機器やネットワークとの接続を切断する等の緊急避難的処理の手段を明記する

ネットワーク接続を行う組込み機器において、他の機器やネットワークに対して異常なパケットを発信する状況となった場合については、ネットワークケーブルを抜く等の緊急避難的処理をユーザが取ることを、画面上に表示するとともにマニュアルに明記する。マニュアルに明記すべきことは、以下の通りである。

- ユーザの利用している機器が、ネットワーク上の他の機器に影響を与えており、緊急避難が必要であること
- 緊急避難を回避するための方法（ネットワークケーブルを抜いた状態で設定変更を行う等）
- その他ユーザがなすべきこと（サービスセンターに連絡するなど）

Point_39) マニュアルに、ユーザが行うべき機密データの廃棄手順を明記する

携帯電話やカーナビ等の個人情報を含む機密データを保持する機器においては、マニュアルにユーザが行うべき廃棄手順を明記する。

マニュアルにおける記載事項例は以下の通りである。

1) データ消去はユーザの責任で行うべきこと
2) データ消去機能の呼び出し方法
3) データ消去機能の使い方（特に機密データの特定方法）
4) データ消去の確認方法

Point_40) 製品カタログ・マニュアル等にネットワークに接続する際のセキュリティ上の注意事項を示す

製品カタログ・マニュアル等に、ネットワークに接続する際には、外部から悪意を持った攻撃がなされる可能性があり、組込み機器が影響を受けうることを明記する。具体的には、以下の事項を記載する。

- 機器をネットワークに接続すると、外部から攻撃を受ける可能性があること
- 将来において、脆弱性が発見される可能性があること
- 将来において脆弱性が発見されると、それの悪用により、外部へ悪影響を及ぼす可能性があること
- 将来において発見される脆弱性に関して、対応策を施した後でないと、ネットワー

クに機器を接続することは不適切であること

- 脆弱性への対応法は、マニュアルに明記されるまたは、メーカのホームページに詳しく記載されること

組込みソフトウェアのセキュリティ対策推進チェックリスト

１．ライフサイクル全体

管理面		
1	プロジェクト監査組織（プロジェクトマネジメントオフィス）にセキュリティ担当者を配置する	p4
2	開発技術者と開発管理者全員に対してセキュリティ教育を実施する	p4
3	セキュリティに係わる開発の外部委託先等に対して、自社と同程度のセキュリティ技術レベルの向上を求める	p5
4	開発プロセス標準の全てのアクティビティにおいて、セキュリティに係わる実施項目を設定する	p5
5	脆弱性情報、攻撃情報をはじめとする各種のセキュリティ関連情報を収集し、技術者に対して周知徹底する	p6
技術面		
6	脆弱性情報、攻撃情報をはじめとする各種のセキュリティ関連情報を参照し、各工程において適切な対策を実践する	p6

２．企画フェーズ

管理面		
7	組込み機器の非機能要件の一つとしてセキュリティに対する要件が明確化され、かつ文書化されていることを確認する	p7
8	コールセンターと不具合対策部署に対するセキュリティ教育を、製品出荷前から以後定期的に実施する	p7
9	セキュリティ上のトラブルを解消するための対策プログラムの発信方法を策定する	p8
技術面		
10	製品が利用される可能性のある接続形態や動作環境および利用形態を想定して、セキュリティに係わるリスクを定義する	p8
11	制約条件を考慮して、実装予定の機能に対して、定義されたリスクに対する対策方針（セキュリティ方針）を明確にする	p8
12	ユーザによる設定変更の可否や手法および誤操作・誤設定に関して、セキュリティ上のリスクを勘案して決定する	p9
13	一般のユーザに馴染みの無い機能または普段使用されることが少ない機能については、特に安全側を意識した設定を行う	p9

14	セキュリティ方針を考慮し、組込み機器の仕様を決定する	p9
15	セキュリティに関するログ保存機能を設定する	p10
16	ネットワーク経由で正当と想定されるアクセスとは異なるアクセスが検出できた場合、他の警告と区別できる形でユーザに警告する機能を備える	p10
17	ユーザの機密データの廃棄をサポートする機能を実装する	p10

３．設計フェーズ

	管理面	
18	ソフトウェア開発にセキュリティ技術に関するドメインスペシャリスト（専門家）を参画させる	p11
19	外部から導入するソフトウェアについて、セキュリティに関する基準を明確に定義し文書化する	p11
20	完成時のセキュリティ検査について観点・項目を整理しておく	p11
21	インターネットアプリケーションの利用にあたっては、選定から動作設定・テストに係わる一連の作業をセキュリティ専門家に担当させる	p12
	技術面	
22	データを機密度に応じて区分し、ハードウェアおよびソフトウェアの保護機能を考慮し、データの物理的および論理的配置を決定する	p12
23	機密度の異なるデータの扱い方を考慮し、プログラムの実行単位とプロセッサへの配置を決定する	p13
24	特権モードをサポートする実行環境においては、特権モードによるプログラムの実行は必要最小限にする	p13
25	ハードウェアの物理的な破壊や記憶領域の覗き見などの攻撃にも配慮する	p13
26	ネットワークに接続される組込み機器においては外部からの攻撃を受けることを想定し、ネットワークデバイスとプロトコルスタックに関して、攻撃を無視する設定で使用する	p13
27	出荷テスト用インタフェース回路など出荷検査や開発時のテストに用いられる機能等一般ユーザの利用を想定していない機能には、厳密なアクセス制限を設ける	p14

４．実装フェーズ

管理面		
28	開発成果物の実利用環境における攻撃実験体制を整備する	p15
29	脆弱性対応に備えたコードの出所・版管理を行う	p15
技術面		
30	攻撃者が処理系のメモリ管理の弱点を悪用して攻撃コードを実行することが不可能にする	p15
31	ネットワーク接続されるインタフェース全てについて、(不正侵入テストを含む）攻撃テストを実施する	p16
32	機器の動作状態の観測による攻撃テストを実施する	p16
33	セキュリティの視点に係わるテスト項目を定義し、実装工程における必要な項目に基づくテストを行う	p16

５．運用フェーズ

管理面		
34	セキュリティの障害に係わる情報は、ユーザに対して適切に告知を行う	p17
35	外部から脆弱性情報およびそれに関係する情報がもたらされた際に適切な取扱いが行えるようにする	p17
36	脆弱性の発見に備えて情報管理・収集・分析に努める	p17
技術面		
37	コールセンターが最新のセキュリティに係わる状況を踏まえ適切に対応する	p18

６．その他の配慮事項（マニュアル、製品カタログ、パッケージとユーザインタフェースなど）

管理面		
38	マニュアルに、ネットワーク接続を行う機器において、他の機器やネットワークとの接続を切断する等の緊急避難的処理の手段を明記する	p19
39	マニュアルに、ユーザが行うべき機密データの廃棄手順を明記する	p19
40	製品カタログ・マニュアル等にネットワークに接続する際のセキュリティ上の注意事項を示す	p19

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。

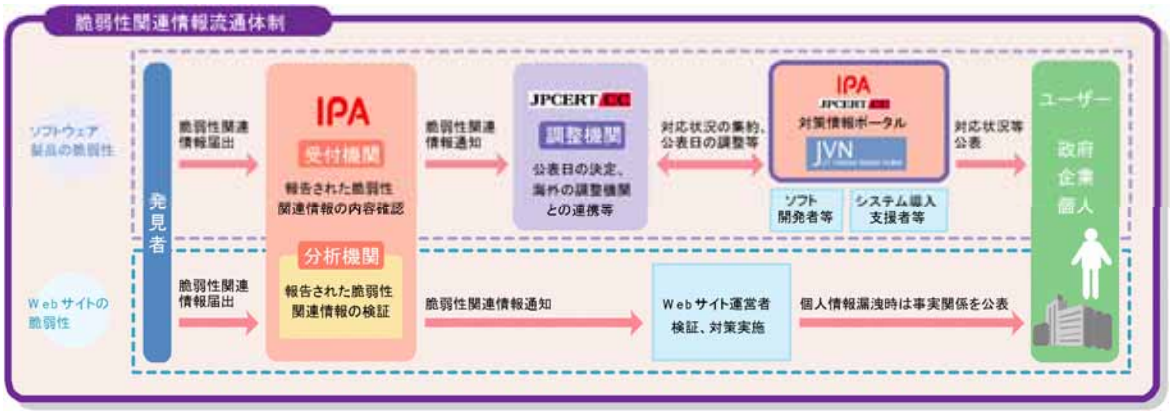
ソフトウェア製品脆弱性関連情報

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」



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/