JISEC

2014 年3 月31 日発行

開発者のためのセキュリティ解説書（ガイダンス編）

IT 製品がセキュリティ機能を備えていても、利用者がその使用方法を正しく理解しないまま操作してしまうと、思わぬセキュリティ事故につながる恐れがあります。

本書は、IT 製品のガイダンス文書（マニュアル）について、あまり知られていないIT セキュリティの観点に焦点をあて、利用者がセキュアな運用を行うために必要な記述内容を、わかりやすく解説します。

独立行政法人
情報処理推進機構

技術本部セキュリティセンター
情報セキュリティ認証室
www.ipa.go.jp/security/jisec/

― 目次 ―

1 はじめに

本書で解説する「ガイダンス文書」とは、IT 製品の操作マニュアルやインストールマニュアルのことです。ガイダンス文書は、IT 製品をセキュアに運用するために、IT 製品の提供するセキュリティ機能の使用条件や使用方法を明確に説明し、利用者の理解不足や誤使用によるセキュリティ上の事故を未然に防止する重要な役割があります。

しかし、IT セキュリティのどのような観点でどのような内容を記述すれば良いかといったような、IT セキュリティに着目したガイダンス文書の書き方について、解説している文献はあまり知られていません。

IT セキュリティ評価の国際的な規格であるコモンクライテリア（Common Criteria、以下「CC」といいます。）には、IT 製品のガイダンス文書も含めて、IT 製品のセキュリティ機能がセキュアに運用可能であることを検査し保証するための評価方法が定められています。本書では、IT 製品のセキュアな運用のために、CC でガイダンス文書に要求されている内容をわかりやすく解説します。

セキュアな運用を保証するための CC のガイダンス文書評価の考え方は、実際に CC 認証を取得する場合だけでなく、CC 認証を取得する予定のない場合にも有効です。本書が、CC の理解とともに、ガイダンス文書を含む IT 製品のセキュリティ品質の向上に、参考になれば幸いです。

1.1 本書の対象読者

本書の対象読者は、IT 製品のセキュリティ機能の設計とマニュアル作成に携わる開発者や、CC に基づいて脆弱性評価を行う評価者を想定しています。

本書では、IT 製品の IT セキュリティに重点を置いて解説しています。一般的なわかりやすいマニュアルの書き方については、他の文献を参照してください。

1.2 本書の構成

本書は以下の 5 章で構成されています。

■ 1 章　はじめに
　本書の目的や対象読者について説明しています。

■ 2 章　CC のガイダンス文書評価の概要
　CC のガイダンス文書評価の全体的な概要を説明しています。

■ 3 章　製品の運用のガイダンス

製品のセキュアな運用のためにガイダンス文書に求められる内容を、CC 評価の観点に基づいて説明しています。

■ 4章　製品の受け入れと導入のガイダンス

製品のセキュアな受け入れと導入のためにガイダンス文書に求められる内容を、CC 評価の観点に基づいて説明しています。

■ 5章　おわりに

本書で解説している内容について、全体的な要約と注意点を説明しています。

1.3 コモンクライテリア規格文書

本書の評価基準及び評価方法は、以下の表 1-1 及び表 1-2 の規格文書に基づいています。評価基準は「CC」、評価方法は「CEM」という略称で呼ばれています。

表 1-1　CC/CEM の規格文書（日本語翻訳版）

CC / CEM バージョン 3.1 リリース 4（CC / CEM v3.1 Release4）
評価基準 情報技術セキュリティ評価のためのコモンクライテリア （CC バージョン 3.1 リリース 4）
パート 1: 概説と一般モデル　バージョン 3.1 改訂第 4 版［翻訳第 1.0 版］
パート 2: セキュリティ機能コンポーネント バージョン 3.1 改訂第 4 版［翻訳第 1.0 版］
パート 3: セキュリティ保証コンポーネント バージョン 3.1 改訂第 4 版［翻訳第 1.0 版］
評価方法 情報技術セキュリティ評価のための共通方法 （CEM バージョン 3.1 リリース 4）
評価方法　バージョン 3.1 改訂第 4 版［翻訳第 1.0 版］

表 1-2　CC/CEM の規格文書（原文）

CC / CEM v3.1 Release4
評価基準 Common Criteria for Information Technology Security Evaluation （CC v3.1 Release4）
Part 1:　Introduction and general model　Version 3.1　Revision 4
Part 2:　Security functional components　Version 3.1　Revision 4
Part 3:　Security assurance components　Version 3.1　Revision 4
評価方法 Common Methodology for Information Technology Security Evaluation （CEM v3.1 Release4）
Evaluation methodology　Version 3.1　Revision 4

本書は、CC/CEM の規格文書のうち、以下の記載内容に基づいています。

- CEM,「12　AGD クラス: ガイダンス文書」
- CC パート 3,「13 AGD クラス：ガイダンス文書」

1.4 用語集

本書で使用する CC/CEM に関係する用語を表 1-3 に示します。

表 1-3 CC/CEM 用語集

用語	説明
CC (Common Criteria：コモンクライテリア)	情報セキュリティの観点から、IT 製品が適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格「ISO/IEC 15408」のことです。
CEM (Common Evaluation Methodology：共通評価方法)	CC に基づいたセキュリティ評価を均質に行うために定められた評価の方法のことです。CC 規格を満たすための、評価すべき項目や評価の観点が定められています。

2　ガイダンス文書評価の概要

CC では、セキュリティの観点で、IT 製品のガイダンス文書が備えているべき評価内容が決められています。本章では、CC のガイダンス文書評価の概要を説明します。

2.1 ガイダンス文書評価の目的

IT 製品のガイダンス文書は、利用者が IT 製品を適切に運用できるように、製品の使用方法や注意点を記述しています。ガイダンス文書に記述すべき内容が漏れていたり、わかりにくい記述がされていたりすると、利用者が IT 製品に対して必要な管理をしなかったり、誤った使い方をしたりするかもしれません。その結果、利用者は IT 製品が安全でない状態になっていることに気が付かないまま運用してしまうかもしれません。そのような状況では、IT 製品が扱っている重要な情報が、利用者の知らない間に、改ざんされたり漏えいしたりするなどの問題が発生する恐れがあります。

CC のガイダンス文書評価では、利用者のセキュアな運用を支援するために、以下のような内容を評価し、利用者が理解不足や誤使用をしないようなガイダンス文書の記述を保証します。

- セキュリティに影響を与える前提条件、設定値や入力、操作間の相互作用、操作の影響などが、利用者が操作する前に理解できるよう明確に記述されていること。
- 利用者が次に何をすべきかとまどうことがないように、セキュリティに影響を与える操作の説明は漏れなく記述されていること。
- セキュリティに影響を与える重要事項は、警告等による注意喚起をするなど、利用者が見落とさないように記述されていること。

2.2 ガイダンス文書評価の範囲

CC のガイダンス文書評価では、図 2-1 に示すように、調達者が購入した製品を受け取ってから運用に至るまでの手続きに対するガイダンス文書を対象としています。

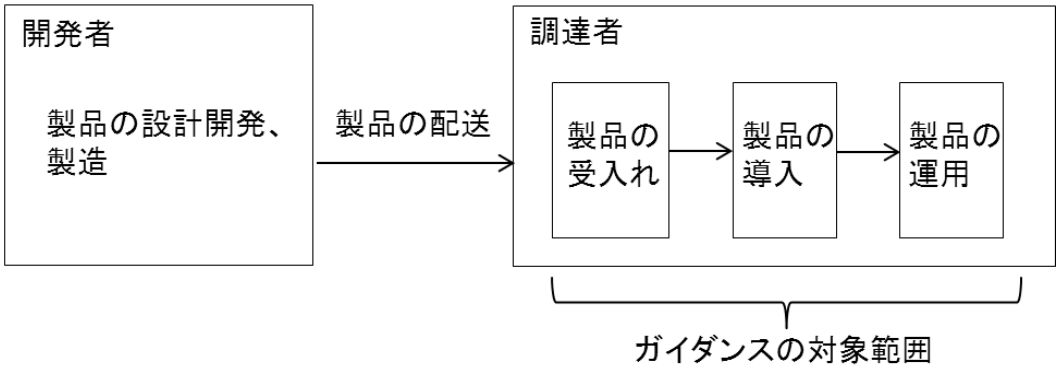

図 2-1　ガイダンスの対象範囲

調達者の手続きには、次の 3 つの段階が含まれています。

■　**製品の受け入れ**

調達者が、購入した製品を受領する段階です。セキュリティの観点では、製品の配送途中で製品が改ざんされたり、何らかのミスで間違った構成の製品が配送されたりすることによる、脆弱性の混入が懸念されます。ガイダンス文書では、調達者の受領した製品が購入した正しいバージョンの製品であり、間違いなく配送されたことを、調達者が確認するための手続きの記述が必要です。

■　**製品の導入**

調達者が、製品の設置やインストールをする段階です。セキュリティの観点では、開発者の想定していないような動作環境や設定で製品が導入されることによる脆弱性の混入が懸念されます。ガイダンス文書では、製品をインストールするための動作環境の要件や手続きについて、調達者が誤解なく確実に実施できるような記述が必要です。

■　**製品の運用**

調達者が、製品を運用する段階です。セキュリティの観点では、調達者が意図せず、製品の理解不足や誤使用等によって、セキュリティが損なわれるような状態で運用をしてしまうことが懸念されます。また、運用中だけでなく、製品の使用が終了し廃棄等をした後に、製品から重要な情報が漏れてしまうことも懸念されます。ガイダンス文書では、製品を安全に運用するための要件や使用方法について、調達者が誤解なく確実に実施できるような記述が必要です。

以下の章では、３つの段階について、製品の運用、製品の受け入れと導入の順に、ガイダンス文書に対する CC の要求内容を詳細に説明します。

3　製品の運用のガイダンス

本章では、製品のセキュアな運用のために、製品のガイダンス文書に求められる内容について、CC のガイダンス文書評価に基づいて説明します。

3.1　製品の想定する利用者役割

(1) 目的

IT 製品のガイダンス文書では、利用者が製品のセキュリティ機能を理解し、製品をセキュアに利用するための運用方法を記述しますが、その内容は、管理者や一般利用者といった利用者の役割によって異なります。そのため、IT 製品のガイダンス文書では、まず、製品の想定する利用者役割と、各利用者役割に与えられたセキュリティ上の権限を明確に記述することが必要です。

そのような記述によって、各利用者は、自身に許可された機能の範囲と、自身が注意しなければならないセキュリティ上の要求事項を、明確に把握することができます。また、製品を導入する組織が、製品を運用していくためにどのような管理が必要であり、自組織の利用者にどのような役割と権限を与えるべきかといった、運用計画を策定する際にも参考になります。

(2) ガイダンス文書に記述すべき内容

利用者役割に関して、IT 製品のガイダンス文書では、以下の内容を明確に記述することが必要です。

■　**利用者役割の提示**

一般に、IT 製品の利用者には様々な役割が存在します。典型的な例は、製品の管理を行う管理者と、製品の機能を利用する一般利用者です。さらに、製品によっては、管理者と監査者が分離されているなど、管理者や一般利用者の権限が細分化されている場合があります。また、製品の提供するインタフェースを使ってプログラムを開発するプログラマなど、他の役割が存在する場合もあります。

ガイダンス文書には、製品の運用のために想定している利用者役割を漏れなく記述することが必要です。

■　**利用者役割毎の機能と権限**

ガイダンス文書には､想定している利用者役割毎に､使用できる IT 製品の機能、与えられる権限、管理しなければならない内容、そのためのコマンド等を記述す

ることが必要です。

なお、ガイダンス文書の具体的な構成方法としては、管理者向けガイダンスと一般利用者向けガイダンスが分離していたり、あるいは、一冊のガイダンス文書の中に利用者役割毎に記述がされていたりすることがあります。CC ではそのようなガイダンスの構成について規定していませんが、利用者役割毎に、必要な内容がわかりやすく記述されていることが重要です。

3.2 警告による注意喚起

(1) 目的

IT 製品のガイダンス文書に必要なことが漏れなく記述されていたとしても、利用者が重要な内容を見過ごしてしまい、IT 製品の誤った運用をしてしまうかもしれません。

IT 製品のセキュリティ上の重要な事項については、利用者に注意喚起をするために、ガイダンス文書に一般的な内容と区別して警告として記述することが必要です。そのような記述をすることによって、利用者はセキュリティ上の重要な事項を見過ごすことなく確実に認識することができます。また、セキュリティの保証できない運用について、製品の責任範囲を警告によって明確にすることは、開発者にとっても重要なことです。

(2) ガイダンス文書に記述すべき内容

ガイダンス文書に記述すべき警告の内容について、以下に説明します。

①警告が必要な場合

利用者の運用しだいで製品のセキュリティが保証できなくなったり、利用者に不利益が発生したりする恐れがある場合には、警告を伴う記述が必要と考えられます。警告が必要な場合の例を以下に示します。

- **製品のセキュリティ機能の前提条件**

製品のセキュリティ機能は、利用者の重要なデータを様々な脅威から保護するよう設計されますが、製品の機能では対処することができない利用者側の条件が、必ずと言ってよいほど存在します。

例えば、利用者の ID とパスワードで利用者を識別認証し、識別認証に成功した利用者のみに製品の使用を許可するセキュリティ機能の場合を考えます。開発者は、単に ID とパスワードによる識別認証を実現するだけでなく、パスワードを繰

り返し試行するなど、セキュリティ機能の弱点を悪用した攻撃を防止できるようなセキュリティ機能を実現することが求められます。しかし、開発者がどんなに製品のセキュリティ機能を強化しても、利用者の不注意によってパスワードが他人に漏れてしまうような場合には、製品のセキュリティ機能では対処することができません。つまり、IDとパスワードによる識別認証機能の場合、利用者が自分のパスワードを他人に漏らさないようにすることは、セキュリティ機能が有効に働くための前提条件となります。

そのような、製品のセキュリティ機能が有効に動作するための前提条件は、警告による注意喚起が必要です。

■ **製品のセキュリティ機能が低下あるいは停止するような操作**

製品によっては、製品のセキュリティ機能を管理者がオンオフしたり、製品のセキュリティ機能の動作を管理者がカスタマイズしたりする機能を提供している場合があります。製品がそのような機能を提供している場合には、管理者の設定によって、セキュリティ機能が十分に機能しなくなる恐れがあります。

製品のセキュリティ機能が低下あるいは停止するような操作は、警告による注意喚起が必要です。

■ **製品の脆弱性を回避するための制約条件**

製品に既知の脆弱性が存在する場合に、開発者が製品を改修する代わりに、脆弱性が発生しないように製品の運用方法の制約で対処する場合があります（一般に「ワークアラウンド」と呼ばれています）。製品の脆弱性を回避するための制約条件は、警告による注意喚起が必要です。

例えば、製品の電源を入れてから製品が完全に運用可能な状態になるまでの間に、製品の機能ではLANを経由した攻撃を防止できないとします。その期間のセキュリティ対策として、ガイダンス文書で、製品が運用可能な状態になるまで、製品をLANに接続しないように警告することが考えられます。

ただし、ワークアラウンドは、後の「3.6 記述上の注意」で説明するように、利用者に受け入れられる合理的な内容であることが必要です。例えば、運用可能な状態になるまでLANに接続しないという対策は、遠隔運用を想定した製品の場合には、利用者に到底受け入れられないでしょう。ワークアラウンドの内容が合理的でない場合、開発者は製品を改修して問題が発生しないように対処しなければなりません。

■ 元の状態に戻せない操作

製品の機能の中には、いったん実行してしまうと、利用者のデータが失われ、元に戻すことができない場合があります。例えば、ハードディスクの暗号化設定を行うと、暗号化のための初期化時に、利用者のデータが消えてしまう場合があります。

そのように、利用者に影響を及ぼし、元の状態に戻すことができない操作は、警告による注意喚起が必要です。

②警告の記述形式

警告は、利用者が見過ごすことがないように、通常の記述とは区別して、明確に識別できるようにガイダンス文書に記述することが必要です。一般には、警告は、警告を表すマーク等を用いて、強調して記述されます。

また、警告の記述として、単に「警告：～しないでください。」といった記述だけでは、利用者が警告の意味を十分に理解することができず、警告の内容が順守されない恐れがあります。そのため、警告の記述では、その必要性が利用者に理解できるように、補足説明と共に記述することが必要です。例えば、以下の 2 つの記述を比較してみてください。

a) 警告：電源を入れてから運用開始画面が出るまでの間、LAN に接続しないでください。

b) 警告：電源を入れてから運用開始画面が出るまでの間、LAN に接続しないでください。セキュリティ機能がまだ動作していないため、重要な情報に不正にアクセスされる恐れがあります。

a)の記述では、警告の内容がなぜ必要かが明確ではありません。利用者によっては、製品の運用に明確な支障が発生するまで、LAN に接続したまま電源を入れる運用を継続するかもしれません。一方、b)の記述では、補足説明によって警告の意味が明確に理解できます。

警告の補足説明には、次の 3 つのタイプがあります。

・発生する可能性のある副作用
・予期される効果
・他の機能や権限に与える相互作用

3 つのタイプのどれを選択すればよいかの明確な基準はありません。開発者は、警告の内容を説明するために適切なタイプを選択します。

なお、警告を表す用語としては、一般的に、「警告」だけでなく「重要」や「注意」といった用語が使われる場合もあります。また、重要度の違いによって複数の用語を使い分けている場合もあります。CC では、警告を意味する用語として、どの用語を使用するかは、特に規定していません。

③警告の記述例

3 つのタイプの警告の記述例を以下に説明します。

■ **副作用を伴う警告の例**

次の例では、警告が、発生する可能性のある副作用と共に記述されています。その記述により、利用者は自身に不利益となるセキュリティ上の影響を把握することができ、警告の意味を理解することができます。警告の記述としては、最も多く見られる形式です。

【警告】
デフォルト値は変更しないでください。デフォルト値を変更すると、セキュリティ機能が無効になり、重要な情報が意図せず漏えいする恐れがあります。

■ **予期される効果を伴う警告の例**

次の例では、警告が、予期される効果と共に記述されています。その記述により、利用者は警告の意味を理解することができます。

【警告】
設定を変更した場合には必ず再起動してください。設定を変更しただけでは、製品の動作は変わりません。次回の起動時に新しい設定が反映されます。

■ **相互作用を伴う警告の例**

次の例では、警告が、他の機能の相互作用と共に記述されています。その記述により、利用者は警告の意味を理解することができます。

【警告】
本機能を有効にする場合には、あらかじめ暗号化機能の設定を実施してください。本機能で使用するデータは、暗号化機能の設定に従って暗号化されます。

3.3 利用者インタフェースのセキュアな使用方法

(1) 目的

「利用者インタフェース」とは、操作画面、コマンド、プログラムインタフェースなど、利用者の操作のために製品が提供しているインタフェースのことです。

利用者が、利用者インタフェースを操作する際に、開発者が想定している使用方法と異なる使い方をすると、製品がセキュリティ機能を備えていても、正常に動作せず、製品が安全でない状態に陥る恐れがあります。

そのため、ガイダンス文書には、利用者インタフェースのセキュアな使用方法を、利用者が理解できるように明確に記述することが必要です。

(2) ガイダンス文書に記述すべき内容

ガイダンス文書には、利用者役割毎に、製品が提供しているセキュリティ機能の概要と、製品が提供しているすべての利用者インタフェースについてセキュアな使用方法を記述することが必要です。以下に、ガイダンス文書に記述すべき内容を説明します。

①セキュリティ機能の概要

ガイダンス文書には、製品が提供するセキュリティ機能の概要を、利用者役割毎に、関連する利用者インタフェースと共に記述することが必要です。それにより、利用者はセキュリティ機能の全体像と、自分にできる操作とセキュリティ機能との関係を、把握することができます。

②利用者インタフェースの目的、ふるまい、相互関係

ガイダンス文書には、利用者インタフェースの目的とふるまい、及び他のインタフェースとの相互関係を記述することが必要です。

利用者インタフェースには、通常、インタフェースの本来の目的の機能と、それに付随するセキュリティ機能があります。開発者は、インタフェースの本来の目的の機能の説明に注力しがちですが、利用者がインタフェースを操作することによって、セキュリティ機能に関係のある動作が実行される場合には、その内容を漏れなく記述しなければなりません。

例（ファイルを印刷するコマンドの場合）

目的：本コマンドは、利用者の指定したファイルを印刷します。
機能：本コマンドは以下を実行します。
(1) 指定されたファイルのアクセス権限をチェックします。
(2) 利用者の権限でアクセス可能な場合にはファイルを印刷します。

※アクセス権限のチェックの結果は監査ログに記録されます。監査ログの閲覧方法や記録形式については、audit コマンドを参照してください。

※上記では、本インタフェースの本来の目的であるファイルの印刷だけでなく、それに伴って実行されるアクセス制御や監査ログの記録といったセキュリティ機能が記述されています。また、監査ログの閲覧方法など、他のインタフェースとの相互関係が記述されています。

③利用者インタフェースの起動方法

ガイダンス文書には、利用者インタフェースの起動方法を、利用者が間違えることがないように記述することが必要です。利用者インタフェースの種類に応じて、例えば、以下のような内容を記述します。

・画面の場合
目的の画面を表示させる手順を記述します。

・コマンドの場合
コマンドラインの起動形式を記述します。オプションの指定が可能な場合には、その指定方法も含みます。

・プログラムインタフェースの場合
関数やメソッド等を呼び出す形式を記述します。C言語の include 文のように、関数等を使用するために必要な宣言文がある場合には、その指定も含みます。

④利用者インタフェースのパラメタ

ガイダンス文書には、利用者インタフェースのパラメタについて、その意味やセキュリティに対する影響が理解できるようにするために、以下のような内容を記述することが必要です。

・利用者が設定することのできるパラメタとその目的
・パラメタの取り得る値とデフォルト値
・パラメタのセキュアな値とセキュアでない値

以下に、パラメタの記述の例を示します。

例（パスワードの最低長を設定する管理者向けコマンドの場合）

パラメタ：パスワードの最低長
目的：利用者がパスワードを設定する時の最低長を制限します
設定可能な値：4～16 の整数（デフォルト値 8）

【警告】安全のために 8 以上の値を使用してください。
8 未満の値は不正ログインの可能性が高くなります。

※上記では、パラメタの取り得る値は 4～16、デフォルト値は 8、セキュアな値は 8～16、セキュアでない値は 4～7 となります。

なお、製品によっては、パラメタの設定は単独ではなく、いくつかのパラメタの組合せによって、取り得る値やセキュアな値が変わってくる場合もあります。ガイダンス文書には、そのような組合せ条件も明確に記述します。

例えば、ある管理コマンドで、第 1 パラメタが暗号アルゴリズム、第 2 パラメタが暗号鍵長の場合を考えます。暗号鍵長の取り得る値やセキュアな値は、DES、AES、RSA といった暗号アルゴリズムによって異なります。

⑤利用者インタフェースの出力メッセージや応答

ガイダンス文書には、利用者インタフェースを利用した際に出力されるメッセージや応答を記述することが必要です。それにより、利用者は、自分の実行した内容が正常に実行されたかどうか、また失敗時にはどのようなエラーが発生したのかを把握することができます。

エラーが発生した場合の対処方法もガイダンス文書に記述することが必要です。詳しくは「3.4 セキュリティ関連事象の対応方法」「3.6.1 すべての操作についてセキュアな運用方法を記述すること」を参照してください。

⑥利用者インタフェースのセキュアな使用方法のアドバイス

ガイダンス文書には、利用者インタフェースのセキュアな使用方法のアドバイスを記述することが必要です。セキュアな使用方法には次のものが含まれます。

・製品をセキュアに運用するための使用方法
・セキュリティ機能を効果的に使用するための使用方法

なお、セキュアな使用方法として、製品が提供しているセキュリティ機能の説明に着目しがちですが、セキュリティ機能を備えていないインタフェースについても、製品を安全に運用するための説明が必要です。
以下に、セキュアな使用方法のアドバイスの例を示します。

■ **アドバイスの例 1（セキュアな運用）**

製品が、電子メールの受信用に、暗号化をしない POP と、暗号化を行う POP over SSL の両方のインタフェースを提供しているとします。その場合、セキュアな使い方として、POP over SSL インタフェースの使用方法を記述するだけでなく、暗号化機能が適用されない POP インタフェースの安全な使用方法の説明も必要です。

【警告】
メールの受信には POP over SSL に対応したメールソフトの使用を推奨します。
POP では、受信メールは暗号化されないためメールが盗聴される恐れがあります。

POP を使用せざるを得ない場合には、使用するネットワーク環境やメールの内容には十分に注意してご使用ください。

※上記では、警告に続いて、POP インタフェースを使用する場合のセキュアな使用方法が記述されています。

■ **アドバイスの例 2（効果的な使用）**

【使い方のヒント】
本製品では、利用者の管理等を行う管理者と、監査ログを閲覧することのできる監査者を別々に設定することができます。本機能を活用して、管理者と監査者を分離することにより、管理者の操作に対しても客観的な監査を実施することができます。

※上記では、製品固有の機能を活用した、セキュリティ上望ましい効果的な使

用方法が記述されています。

■ **アドバイスの例 3（効果的な使用）**

【使い方のヒント】
監査ログは定期的にバックアップすることを推奨します。本製品では、監査ログを最大 10,000 レコード保存することができます。最大何日保存できるかは、製品の使用状況に依存します。例えば、製品を数日間運用して監査ログの出力量を把握し、バックアップの頻度を見積もると良いでしょう。

※上記では、多くの管理者が悩むことが予想されるバックアップの頻度について、効果的な使用方法のアドバイスが記述されています。

3.4 セキュリティ関連事象の対応方法

(1) 目的

「セキュリティ関連事象」とは、製品の利用者の登録変更や障害対応など、製品の運用に伴って発生し、利用者が対処しなければならない、セキュリティに関連する事象のことです。

利用者がそういったセキュリティ関連事象に遭遇した場合に、本来実施すべき操作をしなかったり、対処すべき操作がわからずに試行錯誤をしたりすると、製品の安全性が保てなくなり、危険な状態に陥る恐れがあります。

ガイダンス文書では、利用者が遭遇する可能性のあるセキュリティ関連事象について、利用者が確実に安全な運用を継続することができるように、その対処方法を記述することが必要です。

また、それらの記述は、利用者がセキュリティ関連事象に遭遇した場合だけでなく、製品の運用前に利用者が対処しなければならない管理内容を把握したい場合にも役立ちます。

(2) ガイダンス文書に記述すべき内容

ガイダンス文書に記述すべきセキュリティ関連事象の内容について、以下に説明します。

①セキュリティ関連事象の提示

ガイダンス文書には、製品の運用に伴って、利用者が遭遇する可能性のあるセキュリティ関連事象を、漏れなく記述することが必要です。

そのために、開発者は、製品が提供しているセキュリティ機能の使用方法を分析し、利用者が遭遇する可能性のあるセキュリティ関連事象を洗い出します。以下のような、利用者が製品の設定変更等の操作を必要とするような事象は、セキュリティ関連事象に該当すると考えられます。

■ **利用者の事情によって発生する事象**

利用者の事情により、製品の設定を変更しなければならない場合があります。例えば、次のようなものが該当します。

・利用者の登録、変更、削除
・ファイアウォールのフィルタリングルール等の変更

■ **セキュリティ機能によって発生する事象**

製品の提供するセキュリティ機能によって、運用中に発生する事象があります。例えば、次のようなものが該当します。

・利用者がパスワードを繰り返し失敗した場合のロック
・監査ログ等のアラーム通知

■ **障害**

様々な障害もセキュリティ関連事象に該当します。

・製品が検出し通知するエラー
・その他、予期しない障害

開発者は、上記のように分析し抽出した内容を、「利用者を登録するには」「パスワードがロックされた場合には」といったように、利用者の視点で発生する事象としてガイダンス文書に記述します。

②セキュリティ関連事象毎の対処方法

ガイダンス文書には、各セキュリティ関連事象について、どの利用者役割が、どのような操作を実施するのかを記述することが必要です。記述にあたっては、次のような注意が必要です。

・セキュリティ関連事象ごとに、必要な操作をすべて記述します。
・セキュリティ上、注意しなければならないことは、漏れなく記述します。

以下にセキュリティ関連事象の記述例を示します。

利用者を登録するには

管理者権限でログインし、USER_ADD コマンドで新規の利用者名を登録し、続いて PASSWORD コマンドでパスワードを設定します。

以下に利用者「taro」を登録する例を示します。

```
# USER_ADD taro
  ユーザ「taro」を新規に作成しました
# PASSWORD taro
  新しいパスワードを入力してください： ********
  確認のためパスワードを再入力してください：********
  「taro」のパスワードを設定しました
#
```

【注意】パスワードの文字列は、設定されている制限値以上の長さの文字列で、特殊文字を１文字以上含む、英数字を設定する必要があります。
詳細は、PASSWORD コマンドの説明を参照してください。

※上記では､利用者登録に必要なすべての操作を､例をあげて説明しています。

3.5 セキュアな運用のための運用環境の条件

(1) 目的

IT 製品では、多くの場合、その製品をセキュアに運用するために、製品の設置場所、製品の利用者、他の IT 機器といった運用環境に対する条件が存在します。運用環境の条件が守られていない場合には、製品がセキュリティ機能を備えていても、セキュリティ機能が適切に機能せずに、利用者の重要なデータ等が保護されなくなる恐れがあります。

ガイダンス文書には、製品の提供している機能の使い方だけではなく、製品をセキュアに運用するために、製品が依存している運用環境の条件を明確に記述するこ

とが必要です。

(2) ガイダンス文書に記述すべき内容

ガイダンス文書には、製品をセキュアに運用するための運用環境の条件を漏れなく記述することが必要です。運用環境の条件の多くは、3.2 節で説明したように、利用者が確実に実施するように、警告等によって注意喚起することも必要です。

運用環境の条件として考慮すべき観点には以下のようなものがあります。

■ **物理的条件**

IT 製品の設置場所等の物理的な条件です。例えば、製品が、製品内部の HDD 装置を取り外して解析するような攻撃を防止することは考慮されていない場合、入退出管理がされ信頼できる管理者だけが操作可能なコンピュータ室に設置しなければならないといった条件が考えられます。

■ **人的条件**

IT 製品の利用者が守るべき条件です。例えば、製品が ID とパスワードによる識別認証機能を提供している場合に、利用者がパスワードを他人に漏らさないように管理しなければならないといった条件が考えられます。

■ **構成条件**

IT 製品が依存する他の IT 機器に対する条件です。例えば、IT 製品がアプリケーションプログラムの場合、その動作環境の OS が攻撃に悪用されないようにするために、OS の利用者アカウントやアクセス権限を適切に設定し、OS に既知の脆弱性がないようにしなければならないといった条件が考えられます。また、IT 製品の動作を保証するための、他の IT 機器に要求する仕様や設定条件も該当します。

開発者は、上記のような観点を考慮し、製品のセキュアな運用に必要な運用環境の条件を漏れなく抽出しなければなりません。そのためには、製品のセキュリティ機能を改ざんしたりバイパスしたりする様々な攻撃に対して、製品の機能で攻撃を防止することができるかどうかを分析することが有効です。それにより、製品単独で対処可能な限界が明らかになり、製品の機能で対処できない部分を補うための運用環境の条件が導き出されます。

セキュリティ機能に対する攻撃とその防止メカニズムの分析については、以下の参考文献を参照してください。

IPA: 開発者のためのセキュリティアーキテクチャ解説,
http://www.ipa.go.jp/security/jisec/apdx.html#ADV_ARC_GUIDE

3.6 記述上の注意

前節までに説明したセキュリティ上の観点を、ガイダンス文書に記述するにあたっては、以下のような注意が必要です。

3.6.1 すべての操作についてセキュアな運用方法を記述すること

ガイダンス文書には、製品が利用者に提供しているすべての操作について、セキュリティに及ぼす影響やセキュアな運用方法を、利用者が理解できるように明確に記述することが必要です。利用者が、ガイダンス文書に記述されていないような操作を求められる状況に遭遇して試行錯誤をしたり、操作のもたらす影響を十分に理解しないままに使用したりすると、製品の安全性が保てなくなり、危険な状態に陥る恐れがあります。

すべての操作について記述するためには、特に「操作モード」に注意が必要です。以下に、操作モードについて説明します。

(1) すべての操作モードの説明

「操作モード」とは、製品の動作に何らかの違いがある運用状態のことです。例えば、次のようなものが操作モードに該当します。

- Windows のセーフモードのような運用モード
- 製品の保守のために使用される運用モード
- 製品の設定変更等で異なる動作をする場合
  （セキュリティ機能がオフの状態や、機能の動作が異なる状態など）
- エラー発生等で正常時とは異なる特別な操作が要求される状態
  （文書編集プログラムで破損したファイルを開く時の「ファイルの回復モード」のような操作も含みます）

ガイダンス文書には、製品が提供している操作モードについて、目的、使用方法、現在どの操作モードであるかを確認する方法を記述することが必要です。操作モードの説明は、ガイダンス文書に独立して記述されることもあれば、3.3 節で説明した使用方法や、3.4 節で説明したセキュリティ関連事象の対処方法に含まれる場合もあります。

(2) 操作モードのセキュリティに及ぼす影響の説明

操作を実行した後にセキュリティに影響を及ぼす恐れがある場合、ガイダンス文書には、操作前にセキュリティへの影響が理解できるように記述することが必要です。重要な内容については、利用者が見落とすことがないように、警告等によって注意喚起することも必要です。

(3) 操作をした後の回復方法

ガイダンス文書には、セキュリティに影響を及ぼすような操作を実行した後や、障害発生等を契機として特殊な操作モードに遷移した後に、元のセキュアな運用状態に復帰する方法を記述することが必要です。

記述にあたっては、特に以下の注意が必要です。

■ 操作誤りを含むすべての操作の回復

操作の実行には操作誤りも含みます。すなわち、製品の前提条件として禁止されている操作であったとしても、利用者がその操作を実行してしまった場合を想定して、回復方法をガイダンス文書に記述しなければなりません。

開発者の多くは、「製品の運用の前提条件として禁止している操作に対しては、動作を保証していないので、ガイダンスは提供しない。」と考えるかもしれません。しかし、製品が利用者に操作を提供している限り、開発者の責任として、発生し得るすべての操作について、利用者の安全のためのガイダンスを提供することが必要です。それは、日常的な製品における、人体に対する安全のためのガイダンスの場合と同じです。 例えば、強力な洗浄液の製品では、一般に「注意：絶対に目に入れないようにしてください。失明のおそれがあります。」といった警告と共に、「目に入った場合にはただちに流水で洗い流し、必ず医師に相談してください。」といった、警告で禁止されている行動に対する回復方法が記述されています。それと同様の記述が、IT 製品のガイダンス文書にも求められます。

■ セキュアな運用状態への復帰

セキュアな運用状態への復帰方法は、実行した操作に関係するセキュリティ機能によって異なります。

例えば、製品から外部機器へのネットワーク送信の際に、製品が提供している通信の暗号化機能をオフに設定して運用したとします。その場合、影響を受けるのは、送信したデータだけです。したがって、製品を元のセキュアな運用状態に復帰するためには、通信の暗号化機能をオンの設定に戻すだけで済みます。

一方、製品のログイン機能の設定を変更し、管理者権限で誰でもログイン可能な

状態で運用したとします。その場合、製品の運用中に、製品の様々な設定や監査ログが変更されるかもしれません。したがって、元のセキュアな運用状態に復帰するためには、ログイン機能の設定を元に戻すだけでは不十分です。ガイダンス文書では、様々な設定が運用管理者の意図どおりになっていることを確認する手順や、あるいは、工場出荷時の設定に戻して最初からすべての設定をやり直す手順などを提供する必要があります。

なお、障害発生時も、保守員を呼ぶといった画一的な対応方法ではなく、セキュリティへの影響に応じてガイダンス文書に記述すべき内容が異なる場合があります。

例えば、ハードディスクの読み書き時にエラーが発生した場合を考えます。しかし、ハードディスクのエラー発生箇所と異なるブロックは読み出せるかもしれません。そのため、ハードディスクからの情報漏えいを考慮すると、単に保守員にハードディスクの交換を依頼するのではなく、ハードディスクの内容が読み出せないことを確実にするためのアドバイスが必要と考えられます。

3.6.2 誤解や誤使用がないよう明確であること

ガイダンス文書には、前節までに説明したセキュリティ上の観点が、漏れなく記述されていることが必要です。記述漏れがある場合や、適切な記述がされていない場合には、誤解や誤使用につながる恐れがあります。

特に以下のような内容には注意が必要です。

- **警告の記述不足**

  重要事項であるにもかかわらず警告の記述がない場合や、あるいは、警告に相当する内容が記述されてはいるが強調されていない場合には、利用者に重要度が理解されず、見落とされる恐れがあります。

- **依存性の説明不足**

  製品のセキュリティ機能の依存性の説明が不十分である場合には、利用者がセキュリティ機能の設定変更等をした際に、別のセキュリティ機能に影響が及んでいることに気付かずに運用してしまう恐れがあります。

  また､製品のセキュリティ機能や安全な運用方法が他の IT 機器に依存しており、それらの依存性の説明が不十分な場合にも、依存する IT 機器の影響で製品が安全でない状態に陥っていても、利用者が気付かずに運用してしまう恐れがあります。

- **誤解されやすい機能**

製品のセキュリティ機能に一貫性がなくその説明が不十分である場合には、利用者が、ある機能を使用する際に、同じセキュリティ機能が当然適用されると思い込んで、運用してしまう恐れがあります。

セキュリティ機能に一貫性がない例を以下に示します。

・リモートプリンタの設定で、選択する通信プロトコルによって、利用者認証が適用される場合と適用されない場合がある。

・製品のコンソールと Web 画面といった利用者インタフェースの違いによってセッションのタイムアウト時間やパスワード誤り時の試行可能回数が異なる。

そのような一貫性のないセキュリティ機能が存在する場合には、利用者が誤解しないようにガイダンス文書で注意喚起することが必要です。しかし、本来は、一貫性のないセキュリティ機能は望ましくありません。開発者は、製品の開発において、すべての機能に一貫したセキュリティ方針が適用されるように設計することが推奨されます。

上記の他に、ガイダンスの文章自体が、利用者の視点でわかりやすく記述されており、記述内容が一貫していることも重要です。そのような一般的な文章の書き方については、他の参考文献を参照してください。

3.6.3 運用内容が合理的であること

ガイダンス文書の内容は、利用者に受け入れられるような合理的な内容であることが必要です。製品の運用や製品の運用環境に要求される内容が、利用者に過度な負担がかかる場合には、セキュアな運用を維持することが困難になり、合理的な内容とは言えません。

特に、製品のセキュリティ機能に脆弱性が発見され、それを製品の運用で回避するために、特別な制約条件を要請する場合があります。そのような必要が発生した場合には、開発者は、制約条件が現実的に対処可能な内容であり、利用者に無理なく受け入れられるかどうかを検討することが必要です。理論的には実現可能な回避策であったとしても、現実問題として運用に負担がかかり、利用者に受け入れられないような内容の場合には、製品の機能を改善することが必要です。

4　製品の受け入れと導入のガイダンス

本章では、製品のセキュアな受け入れと導入のために、製品のガイダンス文書に求められる内容について、CC のガイダンス文書評価に基づいて説明します。

4.1 製品のセキュアな受け入れ

(1) 目的

調達者が製品を購入し受領する際に、調達者の意図した製品と異なるものが届けられるかもしれません。例えば、製品が配送途中で改ざんされたり、何らかのミスで間違った構成の製品や部品が不足したまま配送されたりする恐れがあります。その結果、製品がセキュアでないにもかかわらず、調達者がそのことに気付かずに製品を運用した場合、様々なセキュリティ上の問題が発生する恐れがあります。

ガイダンス文書では、調達者の購入した正しいバージョンの製品が、間違いなく配送されたことを、調達者が確認するための手続きの記述が必要です。

(2) ガイダンス文書に記述すべき内容

調達者が製品をセキュアに受け入れるために、ガイダンス文書に記述すべき内容を説明します。

■　**製品が改ざんされていないことの確認**

ガイダンス文書には、調達者の受け取った製品が、配送途中で改ざんされていないことを確認する手順の記述が必要です。製品の受け取り時の確認手順は、製品の発送時に、開発者が製品の改ざんを防止するために採用したセキュリティ手段に依存します。

ソフトウェア製品や電子データのガイダンスの場合には、例えば、製品発送前に付与した電子署名やハッシュ値を検証することで、調達者の受け取った製品が改ざんされていないことを確認することができます。また、ハードウェア製品や製本されたガイダンスの場合には、例えば、製品発送時に付けた開封検知シールを確認することで、配送途中に開封や改ざんがされていないことを確認することができます。ガイダンス文書には、そのような確認手順を記述します。

■　**製品のすべての部分が含まれていることの確認**

ガイダンス文書には、調達者の受け取った製品に、製品のすべての部分が含まれていることを確認する手順の記述が必要です。特に、ソフトウェア製品の場合、

セキュリティに関係する機能を使用するために、オプションのライセンスが必要となる場合があります。そのようなオプション類も含めて、製品のすべての部分が含まれていることを確認する手順を記述することが必要です。

例えば、ソフトウェア製品が、媒体とライセンスキーで構成されている場合には、ソフトウェア製品を格納した媒体の確認に加えて、製品の設定時に投入するライセンスキー等の設定情報がそろっているかどうかの確認手順を記述します。また、ソフトウェア製品が、オプションのライセンスが投入された状態で配送される場合には、製品を起動して投入済のライセンスを表示させるなど、当該ライセンスが間違いなく投入済であることを確認する手順を記述します。

■ **製品のすべての部分が正しいバージョンであることの確認**

ガイダンス文書には、調達者の受け取った製品が、調達者の購入した正しいバージョンであることを確認する手順の記述が必要です。また、実行プログラムとそのガイダンス文書など、別々に識別可能なすべての部分について、バージョンの確認手順の記述が必要です。

例えば、製品のバージョンは、製品自身や製品を格納した媒体に貼られたラベルや、ソフトウェア製品の表示するバージョン情報等によって確認することができます。ガイダンス文書には、それらのバージョンを確認する手順を、調達者が間違いなく実行できるように記述します。

4.2 製品のセキュアな導入

(1) 目的

調達者は、購入した製品を受け入れた後、製品の様々な設定等の導入作業を行い、製品の運用を開始します。製品の導入作業時に、開発者が意図していないような構成や設定が行われると、製品のセキュリティ機能が正常に動作せず、セキュリティ上危険な状態で運用される恐れがあります。

ガイダンス文書では、製品を導入するための動作環境の要件や手続きについて、調達者が誤解なく確実に実施できるような記述が必要です。

(2) ガイダンス文書に記述すべき内容

調達者が製品をセキュアに導入するために、ガイダンス文書に記述すべき内容を説明します。

①製品導入の要件

ガイダンス文書には、セキュリティ機能が確実に動作するための要件の記述が必要です。例えば、以下のような要件があります。

・最小限のシステム要件
・製品が依存する他の IT 機器で、動作保証がされているもの
・設置場所をはじめとする運用環境の要件

②製品導入の手順

ガイダンス文書には、製品をセキュアな運用状態にするために、調達者が実行しなければならない設定作業等の手順の記述が必要です。

製品導入の手順は、以下のような詳細度で記述することが必要です。

・実行しなければならないステップ毎に記述すること
・各ステップの成功・失敗が確認できること
・各ステップの結果に応じて、次に実行するステップが明確に理解できること

製品のデフォルトの設定のままではセキュリティ機能が停止あるいは低下しているような場合には、製品導入の手順にセキュリティ機能が十分に機能するように設定するための手順を含めることが必要です。

ただし、開発者は、デフォルトの設定でセキュリティ機能が十分に機能するように設計することが推奨されます。そのような「デフォルト・セキュア」の製品では、製品出荷時から安全な状態になっており、利用者が運用上の都合でセキュリティ機能を停止させたい場合には、利用者の責任で設定を変更することになります。それにより、利用者が気付かずに安全でない状態の製品を運用してしまうリスクが軽減されます。

③問題発生時の対処方法

ガイダンス文書には、手順書と異なる状態に遷移したり、エラーが表示されたりなど、例外的な事象や問題が発生した場合の対処方法の記述が必要です。

例えば、利用者が間違いやすい内容の確認方法や、想定外の問題が発生した場合のサポート窓口への連絡方法などを記述します。

4.3 記述上の注意

ガイダンス文書を記述する際には、3 章の運用のガイダンスの場合と同じような注意が必要です。ただし、製品の受け入れと導入のためのガイダンスでは、利用者が実施しなければならない手順の記述が中心となります。そのため、特に、以下のような点に注意が必要です。

■ 完全であること

ガイダンス文書には、セキュアな受入れや導入に必要な手順や前提条件が、漏れなく記述されていることが必要です。必要な手順や前提条件の記述が不足している場合、利用者がセキュアでない状態で製品を運用してしまう恐れがあります。

特に開発者は、開発の際に自分の使用している環境に既に様々な設定を行っています。そのため、開発者の環境においては、本来設定すべき手順が漏れていても問題とはならず、ガイダンスの記述漏れに気が付かない場合もあるので、注意が必要です。

■ 明確であること

ガイダンス文書に記述する手順は、利用者が操作途中でとまどうことがないように、すべてのステップを明確に記述することが必要です。手順が明確でない場合、利用者は、試行錯誤を行い、開発者の意図と異なる操作をする恐れがあります。

特に開発者は、製品の操作に習熟しているため、導入する利用者にとってわかりにくい記述であっても気が付かない場合もあるので、注意が必要です。

■ 合理的であること

ガイダンス文書の記述内容は、利用者に過度な負担がかかることなく実施できるように、合理的であることが必要です。例えば、製品のバージョンを確認するために、製品の立ち上げの途中に一瞬だけ表示されて消えてしまう情報の確認を要求する場合は、合理的とは言えません。

5　おわりに

本書では、IT 製品のガイダンス文書について、IT セキュリティの評価の国際規格である CC に基づいて、利用者が製品を安全に使用するために求められる記述内容や注意点について説明しました。

重要なことは、利用者が、製品が安全でない状態に陥っていることに気付かないまま運用することがないようにすることです。

そのために、CC では、IT 製品をセキュアに運用するための前提条件や使用方法について、利用者が見過ごしたり誤解したりしないように、警告等を交えて明確に記述することを求めています。

また、IT 製品のセキュアな使用方法についても、単に操作画面やコマンド毎に使い方を記述するだけでなく、利用者の役割、利用者が実施すべき管理、利用者が遭遇する事象といったように、利用者がガイダンスを参照する様々な利用ケースを想定し、それらの利用ケースに応じて、利用者が試行錯誤せずに間違いなく操作ができるような記述を求めています。

さらに、ガイダンス文書の記述内容は、製品に実装されたセキュリティ機能やセキュリティアーキテクチャと一貫している必要があります。製品の機能とガイダンスに従った運用によって、利用者の大切なデータ等が保護されることになります。

開発者は、製品を開発する際には、運用方法も考慮した上で、製品のセキュリティ機能やセキュリティアーキテクチャを設計することが大切です。また、開発した製品については、適切な内容のガイダンスを提供しなければ、利用者が製品の機能を正しく使用することができず、セキュリティの事故につながりかねません。

本書が、製品の運用方法も含めたセキュリティの向上に、少しでも役立つことができれば幸いです。

開発者のためのセキュアガイダンス解説

2014 年 3 月 31 日　　初版発行

著作・発行　　独立行政法人情報処理推進機構（IPA）

執　筆　者　　情報セキュリティ認証室