DM6-03-051

ソフトウェア開発における情報セキュリティ対策実施規程

策定手引書

2006 年 2 月

内閣官房情報セキュリティセンター

改訂履歴

改訂日	改訂理由
2006/2/17	初版

商標について

本資料に記載されている会社名、製品名は、それぞれの会社の登録商標又は商標です。

1　本書の目的

本書は、府省庁において利用される「ソフトウェア開発手順書」にセキュリティに関する事項を追加し、改善するための参考文書（以下「ソフトウェア開発における情報セキュリティ対策実施規程」という。）を整備するための手引書である。

府省庁においては、「政府機関の情報セキュリティ対策のための統一基準（2005 年 12 月版（全体版初版））」（NISD-K303-052、以下「政府機関統一基準」という。）に準拠する省庁基準と、省庁基準を具体化する一連の実施手順群を整備することが求められている。「ソフトウェア開発における情報セキュリティ対策実施規程」は、これらの実施手順の一つとして策定し、府省庁内部でソフトウェアを開発する場合に適用するものである。すなわち、ソフトウェア開発に携わる行政事務従事者がこれに従うことにより、政府機関統一基準に基づく省庁基準の関係する規定を遵守することとなるものである。

ソフトウェアにおけるセキュリティの実現については、開発ライフサイクル（Software Development Life Cycle）である要件定義、設計、実装、テストの各工程におけるセキュリティ対策を的確に実施することが求められる。

本書は、これらの背景の下で、「ソフトウェア開発における情報セキュリティ対策実施規程」に含めるべき手順及び記述例を具体的に示し、もって統一基準及び省庁基準への準拠性、業務手順への適用性等において適切な規定の整備に資することを目的とする。

2　実施手順に記載すべき事項

「ソフトウェア開発における情報セキュリティ対策実施規程」には、以下の事項を具体化させて記載すること。

2.1　政府機関統一基準（K303-052）に定める「ソフトウェア開発における情報セキュリティ対策実施規程」に係る遵守事項

6.1.3　ソフトウェア開発（１）ソフトウェア開発体制の確立時　＊(b)を除く
6.1.3　ソフトウェア開発（２）ソフトウェア開発の開始時
6.1.3　ソフトウェア開発（３）ソフトウェアの設計時
6.1.3　ソフトウェア開発（４）ソフトウェアの作成時
6.1.3　ソフトウェア開発（５）ソフトウェアの試験時

3　文書構成例

「ソフトウェア開発における情報セキュリティ対策実施規程」は、セキュリティの高いソフトウェア開発を行うにあたって必要となるセキュリティ対策の観点を解説

しつつ、最終的にソフトウェア開発手順書に統合できる構成とすべきである。文書構成の例を以下に示す。

4　作成する上での留意事項

「ソフトウェア開発における情報セキュリティ対策実施規程」は、以下のことに留意して作成する。

(1) 政府機関統一基準はセキュリティの視点から遵守事項を記載している。これに対し「ソフトウェア開発における情報セキュリティ対策実施規程」は、ソフトウェア開発のライフサイクルに沿って記述すると既存のソフトウェア開発手順書に統合しやすく、かつ理解されやすいものとなる。

(2) 解説を補足するための図や実際に使用している帳票を使用し、個々のフェーズごとに具体的に説明を加えると理解されやすいものとなる。

(3) セキュリティの高いソフトウェアを開発するに当たって実施すべき標準的な事項を記述し、ソフトウェア開発を外部委託している場合においても、他の情報セキュリティ関係規程と併用することで、発注者として外部委託事業者を適切に管理するための資料として有効に活用されやすいものとなる。

(4) 2 章に示す事項を「ソフトウェア開発における情報セキュリティ対策実施規程」に反映するに当たっては、当該事項の内容に応じて、以下のいずれかの方針で記述するとよい。

[具体化]・・・一般的・抽象的に記述されており、具体化が必要と思われる遵守事項については、表現をより具体的に修正・追加することにより盛り込む。

[転記]・・・・記述内容がそのまま具体性を持ち、そのままの形で十分と思われる遵守事項については、これを転記することにより盛り込む。

[詳細化]・・・記述内容がそのまま具体性を持っているが、利用者の利便性を考慮して、より詳細な解説を付すべきと思われる遵守事項については、これを詳細化して盛り込む。

5　参考資料

「ソフトウェア開発における情報セキュリティ対策実施規程」の作成に際しては、以下のような資料が参考となる。

5.1　国際規格及び諸外国を含む政府及び政府関係機関の資料

(1) ISO/IEC 15408 「Common Criteria」（JIS X 5070）

(2) ISO/IEC 17799「Information technology - Security techniques - Code of practice for information security management」（JIS X 5080）

(3) IPA「セキュア・プログラミング講座」
（http://www.ipa.go.jp/security/awareness/vendor/programming/）

(4) IPA :「セキュアな Web サーバーの構築と運用」
（http://www.ipa.go.jp/security/awareness/administrator/secure-web/）

(5) IPA :「消費者向け電子商取引サイトにおける注意点」
（http://www.ipa.go.jp/security/vuln/20050304_ec_security.html）

(6) IPA :「脆弱性関連情報に関する届け出状況」
（http://www.ipa.go.jp/security/vuln/20050304_ec_security.html）

(7) SLCP-JCF／共通フレーム 98（ISO/IEC 12207）

(8) NIST Special Publication 800-53「Recommended Security Controls for Federal Information Systems」

(9) NIST Special Publication 800-64「Security Considerations in the Information System Development Life Cycle」

5.2　政府・政府関係機関以外の資料

(1) Microsoft :「信頼できるコンピューティングのセキュリティ開発ライフサイクル」
（http://www.microsoft.com/japan/msdn/security/general/sdl.asp）

(2) Microsoft :「Web アプリケーション セキュリティ強化」
（http://www.microsoft.com/japan/msdn/security/guidance/secmod71.mspx）

6　雛形の利用方法

別紙 1 の雛形を参考にして、「ソフトウェア開発における情報セキュリティ対策実施規程」を策定すると効率的である。別紙 1 の雛形は、前記 2 の実施手順に記載すべき事項を、前記 3 の文書構成例の枠組みの中に記載したものである。

6.1　雛形において想定する前提

本雛形は、以下を前提として記述している。

- 標準化されたソフトウェアの開発手順書が存在している。

そのため、使用する環境が上記の前提と異なる場合には、適宜、修正、追加又は削除する必要がある。

6.2　手直しポイント

各府省庁において政府機関統一基準におけるセキュリティの遵守事項を盛り込んだソフトウェア開発手順書を作成するには、大別して、新規で作成する場合と既存の文書を修正する場合とがあるが、そのどちらの場合でも、以下の事項を踏まえて作業を行う必要がある。

(1) ソフトウェアは、その開発規模、開発期間、予算的制約等によって、最適な開発方法が異なることから、雛形の全要求事項を画一的に適用することは好ましくない。特に、比較的小規模なソフトウェアについては本書の要求事項の適用が現実的ではない場合が多い。このため、適用させる前に要求事項に所要の変更を加える必要性の有無を検討する必要がある。なお、雛形では、要求事項を箇条書きにして「●」記号を付加している。各府省庁においては、自組織における業務の内容と省庁基準にかんがみ、適宜、要求事項を追記又は削除する。また修正が必要となる箇所等には、以下の記号を付加している。

(a) 雛形中に、*[・・・]* 形式で明記される部分（省庁名、担当者等）については、各府省庁内の定めに合わせる。

(b) 雛形中に、【・・・の場合】形式で明記される記述については、想定される案を記したものであり、各府省庁の判断により適宜、選択又は修正する。

(c) ≪図・・・≫は、開発手順書の策定者向けの解説資料であり、適宜判断の上、修正又は削除する必要がある。

(d) ≪参考文献≫は、セキュリティの高いソフトウェアを開発するための参考資料であり、適宜判断の上、修正する必要がある。

(2) ソフトウェア開発における役割分担については、組織や開発プロジェクトによって様々であるため、各府省庁の開発手順書では、自組織の構成や各担当者のソフトウェア開発に関する責務を考慮した上で、主語の追記又は変更を検討する。

(3) 雛形において使用しているソフトウェア開発に関わる用語等については、府省庁において既に用いられている用語と平仄を揃える。例えば、ソフトウェア開発の工程を意味する「要件定義」「設計」という用語等は共通化された呼称ではなく、組織やプロジェクトによって定義や利用方法が異なっているため、必要に応じて修正を加える。

(4) 既存の情報セキュリティ関係規程との整合性を考慮し、適切な分割、統合、相互参照を検討する。

(5) 情報セキュリティ対策の観点以外の一般的な記述について、雛形の内容では不足があると思われる場合には、適宜、補う。