

システム開発規程

1.0 版

システム開発規程

1	趣旨	3
2	対象者	3
3	対象システム	3
4	遵守事項	3
4.1	企画・設計	3
4.1.1	企画の申請・承認	3
4.1.2	要件定義	3
4.1.3	設計	4
4.2	開発・導入	4
4.2.1	開発環境	4
4.2.2	本番データの使用	4
4.2.3	システム開発の委託	5
4.2.4	製品の調達	5
4.2.5	導入	5
4.3	仕様書等の取扱い	5
4.3.1	仕様書等の管理	5
5	運用確認事項	5
6	例外事項	6
7	罰則事項	6
8	公開事項	6
9	改訂	6

システム開発規程

1 趣旨

本規程は、情報システムの開発（企画、設計、開発、導入）及び更新に際し、情報セキュリティの維持・向上を図るため、必要な事項を定めるものとする。

2 対象者

当社の従業員及び協力会社社員で情報システムの企画、設計、開発及び導入に関わる全ての者。

3 対象システム

社内で利用される全ての情報システム。開発を伴わないパッケージシステムの導入も対象とする。

4 遵守事項

4. 1 企画・設計

4. 1. 1 企画の申請・承認

(A.14.2.1)

システム開発の企画にあたっては、以下を遵守しなければならない。

- (1) 新規システムの開発又は既存システムの変更を企画する者は、設計・開発に先立ち、情報セキュリティ委員会に申し出て、関連する各種規定について、提示・説明を受ける。
- (2) 情報システム主管部門は、提示された規定に従い、新規システム開発又は既存システム変更が可能であることを情報セキュリティ委員会に報告し、開発の承認を受ける。
- (3) 情報セキュリティ委員会は、システム開発及び運用開始後に必要となる各種規程類を提示し、この範囲の中で適切なシステムが開発されることを求める。また、開発プロジェクト遂行においても順守されるべき規定を提示する。

4. 1. 2 要件定義

(A.14.2.1)

システム開発の要件定義フェーズにおいては、以下を遵守しなければならない。

- (1) システムの企画、設計を行う場合、セキュリティ設計を担当する者を、システム機能設計を担当する者とは別に置く。
- (2) セキュリティ設計を担当する者は、セキュリティ要件を明確にする。
- (3) セキュリティ設計担当者は、セキュリティ要件に従い、設計フェーズで実施す

る開発システムに関するリスクアセスメントの実施要項を明確にし、情報セキュリティ委員会に報告する。

- (4) 要件定義が完了した段階で、セキュリティ設計担当者は情報システム主管部門とともに、プロジェクト遂行の為のリスクアセスメントを実施し、抽出した対応すべきリスクへの対策の取組み状況について情報セキュリティ委員会に報告する。

4. 1. 3 設計

(A. 14. 2. 1)

システム開発の設計フェーズにおいては、以下を遵守しなければならない。

- (1) セキュリティ設計を担当する者は、企画書及び設計書等はドキュメントとして残す。
- (2) セキュリティ設計担当者は、設計書を元に、情報システム主管部門とともにリスクアセスメントを実施し、抽出した対応すべきリスクへの対策の取組み状況について情報セキュリティ委員会に報告する。

4. 2 開発・導入

4. 2. 1 開発環境

(A. 14. 2. 6)

システム開発環境は、以下を遵守しなければならない。

- (1) 開発環境と本番環境は切り分ける。但し、開発作業による本番環境への影響が少ない場合は、この限りではない。
- (2) 本番環境を開発に用いる場合は、開発用に追加・変更した要件を明らかにし、本番開始後は適切な対処を行う。
- (3) 本番環境を開発に用いる場合、開発用に追加・変更される一般的な内容は、以下の通りである。
 - ・開発用アカウントの追加
 - ・管理者権限を持つアカウントのパスワードの変更
 - ・テストデータの追加
 - ・開発環境用のログデータ取得設定およびログデータ

4. 2. 2 本番データの使用

(A. 14. 3. 1)

システム開発における本番データの取扱いは、以下を遵守しなければならない。

- (1) システム開発又はテストにおいて本番データを使用する際は、事前に情報管理責任者の承認を受ける。

- (2) システム開発又はテストにおいて使用する本番データは、厳密に保管・管理し、使用後の結果データ等は、直ちに復元不可能な措置を講じた上で破棄処分する。

4. 2. 3 システム開発の委託

システム開発を委託する場合は、以下を遵守しなければならない。

- (1) システム開発を外部事業者に委託する場合、『外部委託先管理規程』に従う。

4. 2. 4 製品の調達

製品を調達する場合は、以下を遵守しなければならない。

- (1) 調達する製品は、次にあげる事項を満たすものとする。
- ・当該製品がセキュリティ要件を満たす機能を備えていること
 - ・購入先又は開発元の事業者の連絡先が明らかなものであること
 - ・該当製品に関する更新情報の提供が受けられること

4. 2. 5 導入

(A.14.2.8、A.14.2.9)

開発システムの導入にあたっては、以下を遵守しなければならない。

- (1) システム開発の終了時又は外部委託先からの情報システム受け入れ時の情報セキュリティ上の検査項目を明確にする。
- (2) 本番環境へ移行する際は、リスクアセスメントにより抽出した対応すべきリスクへの対策の取組み状況について、不備・欠陥等の問題がないか確認する。
- (3) 導入する情報システムが、既に稼働中の情報システムと連携する場合は、不具合等が発生しないか十分に確認する。

4. 3 仕様書等の取扱い

4. 3. 1 仕様書等の管理

開発仕様書等の取扱いは、以下を遵守しなければならない。

- (1) システム管理者およびネットワーク管理者は、システム設計及び開発等に係る仕様書等を、情報システム毎に整理するとともに、システム管理者以外が取り扱えないように厳重に保管・管理する。
- (2) システム管理者及びネットワーク管理者は、情報システムの変更の都度、仕様書に反映させ、常に最新の状態で管理する。

5 運用確認事項

システム開発において、以下が行われていることを確認しなければならない。

- (1) セキュリティ設計担当者が、フェーズ毎に情報セキュリティ委員会に、リスクア

セメントで抽出した対応すべきリスクへの対策の取組み状況について報告していることを確認する。

(2) システム管理者及びネットワーク管理者は、情報システムの変更の都度、情報セキュリティ委員会にリスクアセスメント結果を報告していることを確認する。

6 例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

7 罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

8 公開事項

本規程は対象者にのみ公開するものとする。

9 改訂

- ・本規程は、平成 x x 年 x x 月 x x 日に情報セキュリティ委員会によって承認され、平成 x x 年 x x 月 x x 日より施行する。
- ・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。
- ・本規程は、定期的（年 1 回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。