沢井製薬グループ IT セキュリティスタンダード

1　目的と範囲

本規程の目的は、沢井のビジネス活動において生成される全ての電子情報資産（IT システム含む）を、関連社内規程や GxP 関連法規制を遵守しつつ、適切かつ安全に利活用・管理できるようにすることである。全ての沢井製薬グループの役職員は、本規程を遵守しなければならない。各社の IT 部門は、本規程に則した形で、各地域の特異性を考慮し、個別のポリシー・規程・手順を定義することができる。ただし、その場合は本規程の内容を、より厳格化・強化する内容で個別文書は定義しなければならない。文書構造図は、別紙１に記載。

2　役割と責任

- 沢井製薬グループの IT 部門は、全ての電子情報資産を管理・統制するためのプロセスを確立するために協調・連携し、沢井製薬グループの IT 環境を常に安全かつ健全に保ち、継続的に品質向上に努める責任を負う。
- 沢井製薬グループの電子情報資産へのアクセスを許可するにあたり、全ての利用者（役職員、契約業者、来訪者など）は、当規程で定義されている事項を充分に理解し、遵守する責務を負う。
- IT 部門責任者は、IT 基盤・業務システム・ネットワーク・全ての情報機器の導入、構成、保守運用について、その方向付けと管理監督責任を負う。これらの活動の一部として、IT 部門は これらの IT 環境を適切に運営維持する責任を負う。
- IT 部門責任者は、コンピュータ室や電子機器へのアクセスを許可された全ての IT 要員が、業務遂行のための適切な教育を受け、実務経験を有し、本規程に則した訓練を受けていることを保証する責任を負う。電子情報資産の利用は、管掌業務定義に従って許認可され、管掌範囲の業務目的用途に限定される。
- IT 部門責任者は、沢井製薬グループの全ての役職員がグループおよび各社のポリシー・規程・手順書類を理解できるように、定期的に情報セキュリティ教育・訓練を実施する責任を負う。

3　電子情報資産の利用

沢井製薬グループの全ての役職員は、管掌業務に従い、電子情報資産を適切に管理し、利活用する権利を有する。全ての電子情報資産は、各地域・各国での要求事項や関連規制に従い管理・統制される。

沢井製薬グループの全ての役職員は、適切なユーザ認証を経た上で、業務目的に限定して電子情報資産にアクセスすることが許可される。電子情報資産の所管責任者・部門（以下、所有者）は、必要最低限のアクセス権を利用者に付与し、定期的に電子情報資産へのアク

セス状況を監視・統制しなければならない。

4　各種ネットワークサービスの利用

沢井製薬グループの全ての役職員のインターネット・社内ネットワーク上で提供される各種 IT サービスの利用は、定義されたルールと手順に沿って実施されなければならない。電子情報資産へのアクセスは、その情報資産の所有者もしくは所有者の代理人によって承認され、利用者には個人別の唯一無二のユーザ ID が付与されなければならない。全ての会社貸与の電子情報機器は、格納・送受信されるデータの暗号化のための仕組みを有すべきである。全ての IT システムへのアクセスは、パスワードもしくは適切なユーザ認証の仕組みによって保護されていること。

各人が会社貸与以外の電子情報機器を業務目的に利用し、会社の電子情報資産にアクセスすることを、一定の条件下で許容する。その場合は、各地域・各国のローカルポリシーや規程文書で、具体的な条件などを定義すること。

IT 関連のクラウドサービス含め、外部のデータセンタサービスを活用する沢井製薬グループ各社は、電子情報資産が適切な方法で保持され、機密性・完全性・可用性が担保されていることを確証しなければならない。

5　データ保護

沢井製薬グループの IT 部門は、電子情報資産の機密性を守り、情報漏洩リスクを低減するために必要な適切な手段を講じる必要がある。会社貸与の電子情報機器および可搬型外部ストレージ装置（例 USB メモリ装置）については、データの暗号化が必須である。公衆エリアからの電子情報資産へのアクセスに際しては、不正アクセスやデータ漏洩を防ぐために、送受信データを暗号化するための手法を用いなければならない。

会社貸与の電子情報機器は、個人が識別できる形で発行され、電子情報機器およびサービスの利用状況は、安全性確保の観点より監視されるべきである。電子情報資産を守るために、全ての IT システムおよび電子情報機器はアンチウイルスシステム含め最も適切な最新のセキュリティレベルで保たれていることが基本であり、コンピュータ画面も 15 分を超えて放置されてはならない。

データ保護に関し、当規程記載内容に対する例外措置が必要な場合は、各地域・各国の IT 部門責任者の承認を必要とする。

6　ユーザ認証管理

全社レベル IT 環境（全社 Windows ドメインユーザ）は、各社の IT 部門の責任において定められた手順に沿って発行するものとする。全てのユーザ ID は、その適格性が唯一無二であるとして認証されなければならない。沢井製薬グループの電子情報資産への匿名でのアクセスは、如何なる場合でも認められない。セキュリティリスク評価に基づき、IT 部門責任者は多元要素認証の必要性を判断する。

全社 Windows ドメインのパスワードポリシー：

パスワードの長さ	８文字以上
複雑性	下記要素から３つ以上を組み合わせること 英大文字、英小文字、数字、記号
変更周期	最長 90 日毎
アカウントロック	10 回連続でログイン失敗

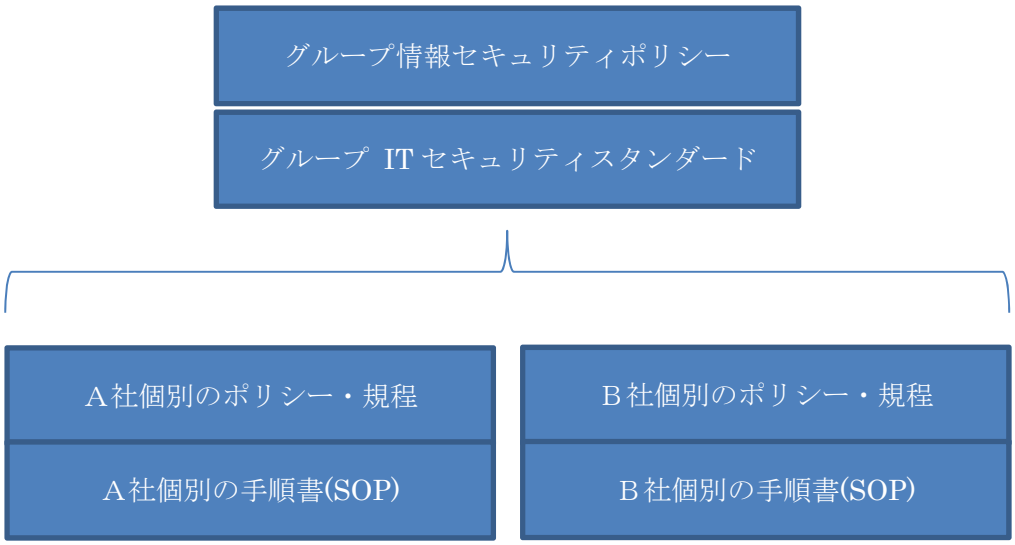
初期設定パスワードは、利用者が初回ログイン時に変更する。パスワードは、コンピュータ画面上・デスク上など他者から見える場所に貼付してはならない。ユーザ登録情報の定期的な棚卸しを行い、不必要な情報は削除し、退職者のユーザ情報は、即座に無効化する。

7　セキュリティインシデント(注)対応

各社の IT 部門は、それぞれの情報セキュリティインシデント管理体制を構築し、インシデント処理手順を文書化する。ビジネスの協業や生産性向上を促進していくために相互接続されたネットワークを有するグローバル企業として、各社の IT 部門は他のグループ会社に悪影響を及ぼす恐れのあるインシデントの発生を低減することに努めなければならない。複数の沢井製薬グループ会社に影響するインシデントが発生した場合は、各社の IT 部門は定められた手順に従い、連絡・連携してインシデント解決にあたり、影響度の大きなインシデントの場合は、迅速に各社の情報セキュリティ責任担当役員に報告する責任を負う。IT 部門責任者は、定期的に再発防止策について見直しを行い、再発防止に努めなければならない。

(注) コンピュータやネットワークのセキュリティを脅かす事象のこと。

別紙１　文書構造図



附則

本規程の管轄部門は沢井製薬管理本部とする。

本規程の改廃には沢井製薬取締役会決議が必要である。

2018 年 1 月 29 日制定・施行