ツチヨシ産業 IT セキュリティポリシー

総務部総務課

2022 年 12 月 14 日

目次

総則

0.1 序論

組織で導入している業務基幹システムは, 管理者と利用者によって運用される. 販売管理, 財務会計, 生産管理など様々あるが, 同一企業内である限り, 元を辿れば全てのシステム処理は単一の巨大な業務フローに帰属する. モジュール[*1]別に大別することはできるが, システム間の関連性は必ず存在する.

システム運用でインシデント[*2]が発生した場合, 影響範囲によっては, 他のシステムに波及する. 最悪, 顧客に損害を与えるケースも想定しなければならない. そのようなケースを未然防止するために緻密な運用設計はしておく必要がある. 現場の利用者およびシステム管理者が同じ視座で同様の業務フローを俯瞰することは, 運用の精度を高めることに寄与する.

また, セキュリティに対する共通認識を持つことも等しく重要であるため, セキュリティポリシーを策定する. セキュリティポリシーとは, 組織内の情報セキュリティを確保するための方針, 体制, 対策等を包括的に定めた文書をいう.

本システム運用定義書 (以下, ”本書” と称する.) は, 暗黙知も含めて明文化し, 組織のシステム運用状況が健全か不正か判定する規程として扱う.

0.2 本書の管理プロセス

本書の内容を更新する場合, 後述する策定手順に準じて実施する.

0.2.1 表記

本書では, 表記の統一性を守るために以下の制限が課される.

- 句読点は「,」「.」以外許可しない.
- 注釈以外の体言止めは許可しない.
- 第**??**部では, 新機能を青文字で表記する.
- 英字の後は必ず「 」半角スペースを使用する.
- 第**??**部を除き, 丁寧語や尊敬語は使用しない. (文字数増大抑制)
- 記号, 英数字の全角文字は許可しない.

また, 改竄リスクを低下させるために「Word」「Excel」「Markdown」での公開を禁じ, 編集ツールは組版処理システム「LaTeX」から生成した PDF に限定する. さらに, Git のプライ

[*1] 機器やシステムの一部を構成するひとまとまりの機能を持った部品のこと.
[*2] 好ましくない出来事. データ事故.

ベートリポジトリを利用して改訂履歴は全てバージョン管理する.

0.3 学術的根拠

セキュリティポリシー及びシステム開発の基準では, 以下を参考文献としている. また他には, ITIL[*3] の内容も広く適用している.

0.3.1 セキュリティ領域

セキュリティ領域は, IPA (独立行政法人情報処理推進機構) による「中小企業の情報セキュリティ対策ガイドライン」と総務省による「地方公共団体における情報セキュリティポリシーに関するガイドライン」を基に定義する. 情報セキュリティ対策に関する検討について, IPA の認識を以下に抜粋する.

> 中小企業等では IT の利活用が進む一方で, サイバー攻撃手法の巧妙化, 悪質化などにより事業に悪影響を及ぼすリスクはますます高まってきています. また, サプライチェーンを構成する中小企業においては発注元企業への標的型攻撃の足掛かりとされる懸念も指摘されており, 早急な対策実施が必須であると言えます.
> 本ガイドラインおよび「SECURITY ACTION」制度の活用によって, IT を利活用している中小企業が情報セキュリティ対策に取り組み, 経済社会全体のサイバーリスク低減につながることを期待しています.
>
> 独立行政法人情報処理推進機構 セキュリティセンター

> 多くの地方公共団体において, 情報セキュリティポリシーが策定されているが, 今後は情報セキュリティポリシーの定期的な評価・見直しを行い, 情報セキュリティ対策の実効性を確保するとともに, 対策レベルを高めていくことが重要である. 本ガイドラインは, 七次の改定を通じて, 新たな情報機器, サービス及び脅威等に対応した情報セキュリティ対策を追加しているので, 情報セキュリティポリシーの評価・見直しを行う際にも, 本ガイドラインが活用されることが期待される.
>
> 総務省

0.3.2 IT ガバナンス領域

IT ガバナンス領域は, 経済産業省による「システム管理基準」を基に定義する. システム管理基準について, 一部を以下に抜粋する.

[*3] IT サービスマネジメントにおけるベストプラクティス (成功事例) をまとめた書籍群

本基準は, どのような組織体においても情報システムの管理において共通して留意すべき基本的事項を体系化･一般化したものである. したがって, 本基準の適用においては, 基準に則って網羅的に項目を適用するような利用法は有効ではない. 事業目的, 事業分野における特性, 組織体の業種・業態特性, 情報システム特性などに照らして, 適切な項目の取捨選択や各項目における対応内容の修正, 情報システムの管理に関連する他の基準やガイドから必要な項目を補完するなど, 監査及び管理の主旨が実現できるように独自の管理基準を策定して適用することが望ましい.

経済産業省

0.3.3 IT マネジメント領域

IT マネジメント領域は, デジタル庁による「標準ガイドライン」を基に定義する. 標準ガイドラインについて, 一部を以下に抜粋する.

IT ガバナンスと IT マネジメントが包括的かつ一体的に行われるように, 標準ガイドラインを規定しています.

デジタル庁

0.4 構成

第**??**部では, 業務基幹システムのマニュアル, 業務フロー, その他運用に関することを網羅的に定義する. 第 I 部では, 組織内の情報セキュリティを確保するための方針, 体制, 対策等を包括的に定める.

第 I 部

セキュリティポリシー

第 1 章

組織的対策

1.1　情報セキュリティ委員会の設置

1.2　体制図

1.3　監査計画

1.4　情報セキュリティに関する情報共有

第 2 章

人的対策

第 3 章

情報資産管理

3.1　情報資産の機密性評価

3.2　評価の表示

3.3　管理責任者と利用者の定義

3.4　社外持ち出し

3.5　破棄と再利用

3.6　バックアップ

第 4 章

物理的対策

4.1　セキュリティ領域の定義

4.2　関連設備

4.3　搬入物の授受

第 5 章

ソフトウェアとハードウェア

第 6 章

IT 基盤運用管理

6.1　管理体制

情報システム管理者は, IT 基盤の運用に当たり情報セキュリティ対策を考慮し製品又はサービスを選択する. IT 基盤の情報セキュリティ対策及び関連仕様は, 情報セキュリティ責任者が承認する.

6.2　IT 基盤の情報セキュリティ対策

IT 基盤の運用の際には以下の技術的情報セキュリティ対策を考慮すること.

6.3　サーバー機器の情報セキュリティ要件

IT 基盤で利用するサーバー機器に求める情報セキュリティ要件は, 情報システム管理者が決定する. 新規にサーバー機器を導入する場合は, 情報セキュリティ要件を満たす製品を選択し, 情報システム管理者の許可を得て導入する. サーバー機器の情報セキュリティ要件は,「6.1 サーバー機器情報セキュリティ要件」を参照のこと.

6.4　サーバー機器に導入するソフトウェア

6.5　ネットワーク機器の情報セキュリティ要件

6.6　IT 基盤の運用

6.7　脅威や攻撃に関する情報の収集

6.8　クラウドサービス情報セキュリティ対策評価基準

6.9　廃棄・返却・譲渡

6.10　IT 基盤を構築するスペック標準

第 7 章

システム開発基準

7.1　新規システム開発・改修

7.2　脆弱性対策

7.3　開発環境の構築要件

7.4　変更管理ポリシー

第 8 章

ベンダー管理

8.1　ベンダー評価基準

情報セキュリティ部門責任者は「情報資産管理台帳」の重要度が 1 以上である情報資産の取り扱う業務を, 外部の組織に委託する場合は, 委託先の情報セキュリティ管理について, 委託先評価基準に基づいて評価する.

8.2　ベンダーの選定

8.3　委託契約の締結

8.4　ベンダーの継続的な評価

第 9 章

インシデント管理及び BCP

9.1　対応体制

9.2　インシデントレベルの定義

9.3　報告フロー

9.4　インシデント発生時の暫定対応

9.5　ディザスタリカバリポリシー

9.6　ビジネス継続性ポリシー

第 10 章

個人番号及び特定個人情報の取扱い

10.1　関係法令・ガイドライン等の遵守

10.2　利用目的

10.3　安全管理措置に関する事項

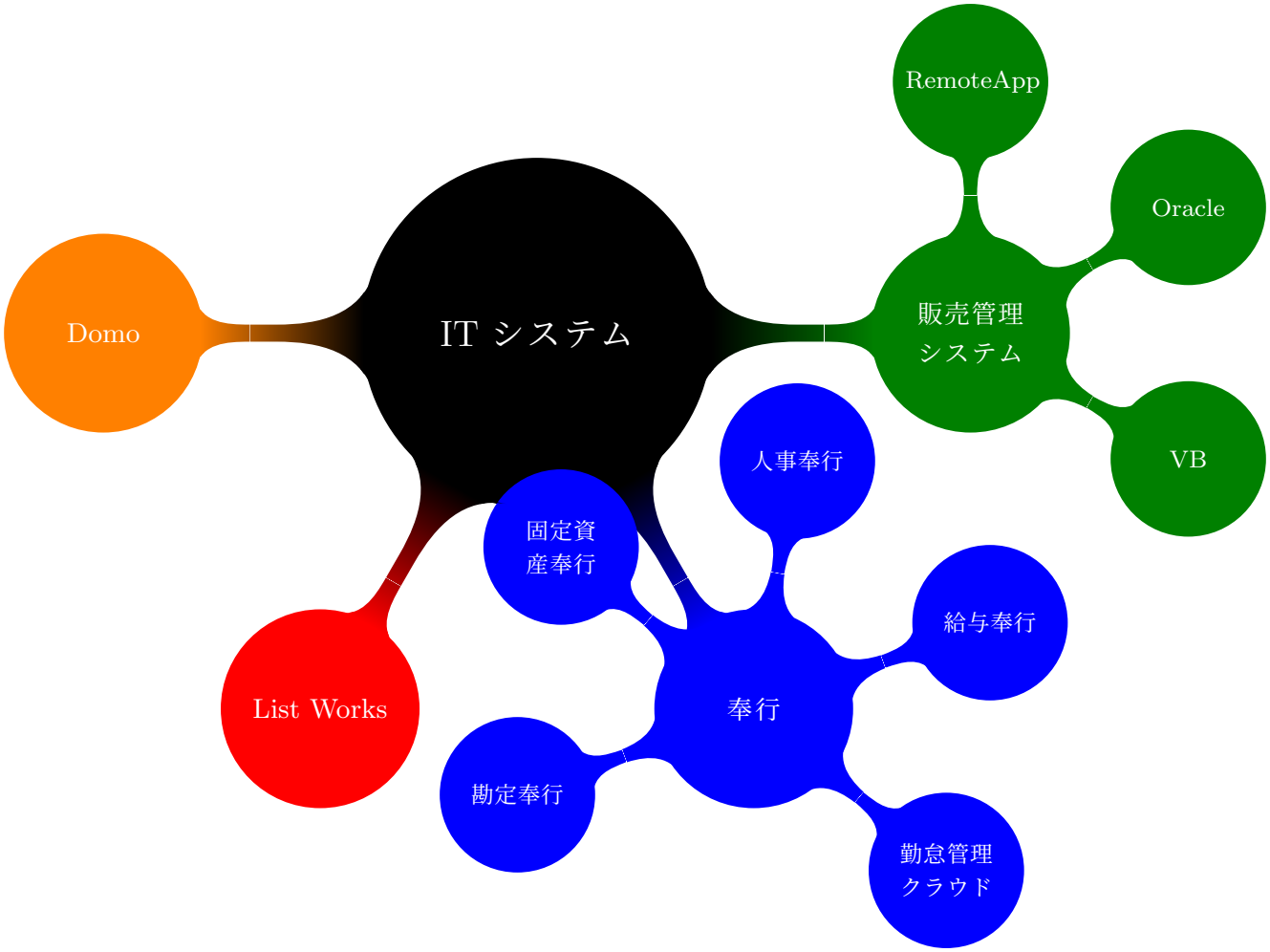
10.4　委託の取扱い

10.5　継続的改善

10.6　特定個人情報等の開示

補遺 A

システム俯瞰図


RemoteApp
Oracle
Domo
IT システム
販売管理
システム
VB
人事奉行
固定資
産奉行
給与奉行
List Works
奉行
勘定奉行
勤怠管理
クラウド