情報セキュリティマニュアル

バージョン	報告者	報告日	承認者	承認日
1.0.2	杉浦悠太	2024-06-18	青木 光平	2024-06-18

組織的管理策

情報セキュリティのための方針群

- 情報セキュリティに関する規程を作成し、トップマネジメントの承認を得る。 （対象：組織管理者）
- 情報セキュリティに関する規程は、年1回、もしくは事業内容などに大きな変化があったときに見直しを行う。 （対象：組織管理者）

情報セキュリティの役割及び責任

- 情報セキュリティの推進のために、「トップマネジメント」「ISMS責任者」「ISMS担当者」「内部監査責任者」「内部監査員」を選任する。 （対象：組織管理者, 開発部）

職務の分離

- 1つのミスが大きな影響を与える業務（例えば、メールの一斉送信や、システムの変更など）は、可能な限り複数人体制で行う。 （対象：組織管理者）

管理層の責任

- 経営陣は、従業者が情報セキュリティに関する規程を遵守するよう、リーダーシップを発揮し、従業者を適切に指導する。 （対象：組織管理者, 開発部）

関係当局との連絡

- 情報セキュリティインシデントが発生した場合は、必要に応じて以下の組織と連絡を行う。
  ・個人情報の漏えい等があった場合（個人情報保護委員会） https://www.ppc.go.jp/personalinfo/legal/leakAction/
  ・特定個人情報の漏えい等があった場合（個人情報保護員会） https://www.ppc.go.jp/legal/rouei/
  ・情報セキュリティに関する相談（情報処理推進機構) https://www.ipa.go.jp/security/anshin/index.html （対象：組織管理者, 開発部）

専門組織との連絡

- 情報セキュリティに関する最新情報を入手するために、以下の情報源を参照する。
  ・情報処理推進機構 https://www.ipa.go.jp/security
  ・個人情報保護委員会 http://www.ppc.go.jp/ （対象：組織管理者, 開発部）

脅威インテリジェンス

- 情報セキュリティに関する最新情報を入手するために、以下の情報源を参照する。
  ・情報処理推進機構 https://www.ipa.go.jp/security
  ・個人情報保護委員会 http://www.ppc.go.jp/ （対象：組織管理者, 開発部）

プロジェクトマネジメントにおける情報セキュリティ

情報及びその他の関連資産の目録

- 情報資産を洗い出し、SecureNaviを利用して整理する。 （対象：組織管理者, 開発部）
- 各情報資産の責任者は、その情報資産の利用範囲や保管場所、保管期限を遵守することに責任を持つ。 （対象：組織管理者, 開発部）

情報及びその他の関連資産の許容される利用

- 各情報資産には、それぞれ利用可能範囲を定める。 （対象：組織管理者, 開発部）

資産の返却

- 従業員が退職するときは、「退職時のチェックリスト」に従い、貸与物品の返却や、アカウントの削除を行う。 （対象：組織管理者, 開発部）

情報の分類

- 情報資産は、以下の3つに分類する。
  ・機密：漏えいすると取引先や顧客に大きな影響がある（個人情報ならびに特定の顧客から守秘義務契約が課せられている情報を含む）
  ・社外秘：漏えいすると事業に大きな影響がある
  ・一般：漏えいしても事業にほとんど影響はない （対象：組織管理者, 開発部）

情報のラベル付け

- 機密情報を含む紙媒体を保管するキャビネットやバインダーには、管理を徹底するために、機密であることがわかるラベルをつける。 （対象：組織管理者, 開発部）

情報の転送

- インターネットブラウザを介して情報を送信する場合は、暗号化された通信（https通信など)を利用する。 （対象：組織管理者, 開発部）
- 業務で受信した電子メールは、個人のメールアドレスに転送してはならない。 （対象：組織管理者, 開発部）
- SNSには、業務情報や、社員のプライバシーに関する情報（写真への映り込みを含む）を、許可なく投稿してはならない。 （対象：組織管理者, 開発部）
- 一般的でない方法（例えば、SNSに付随するメッセージツールなど）で業務の情報をやり取りする場合は、事前に相手方の許可を取る。 （対象：組織管理者, 開発部）
- 電子メールを利用する場合は、一時保留機能や宛先確認機能など、誤送信を防止する機能を有効化する。 （対象：組織管理者）

アクセス制御

- 機密情報およびそれを扱う情報システムは、最小権限の原則に基づき、業務上必要な人のみにアカウント付与・アクセス権限の限定を行う。 （対象：組織管理者, 開発部）

識別情報の管理

- 各情報システムの管理者は、従業員の入社・退職時や部署異動時に、速やかにアカウント・アクセス権の付与・剥奪を行う。 （対象：組織管理者, 開発部）
- 各情報システムに対して、それぞれ管理者を定める。管理者は、その情報システムのアカウントならびにアクセス権の適切な設定について責任を持つ。 （対象：組織管理者）

認証情報

- 業務で用いるパスワードの桁数は10桁以上とし、可能な限り、複数の文字種（数字、アルファベット、記号など）を混在させる。 （対象：組織管理者, 開発部）
- パスワードは、会社が指定するパスワード管理ツールで管理し、紙媒体に記載してはならない。 （対象：組織管理者, 開発部）
- パスワードの使い回し（異なる情報システムで同じパスワードを利用すること。プライベートで利用しているパスワードを再利用することを含む）は禁止する。 （対象：組織管理者, 開発部）
- 共有アカウントのパスワードは、必要最小限の者のみがアクセスできる権限のもとに保管し、関係者以外の人に伝えないようにする。 （対象：組織管理者, 開発部）

アクセス権

- 各情報システムの管理者は、従業員の入社・退職時や部署異動時に、速やかにアカウント・アクセス権の付与・剥奪を行う。 （対象：組織管理者, 開発部）
- 各情報システムの管理者は、1ヶ月に1回、不要なアカウントやアクセス権が残っていないことを確認する。 （対象：組織管理者, 開発部）

供給者関係における情報セキュリティ

- 外部委託を行う場合、以下の委託先評価基準に基づき、委託先のセキュリティレベルのチェックを行う。
  1. 情報セキュリティに関する第三者認証（ISMS、Pマークなど）を取得していることを確認する
  2. 認証を取得していない場合は、IPA「5分でできる情報セキュリティ自社診断」への回答を依頼し、その回答内容に問題

ないことを確認する
3. これらの評価基準に基づいた選定が難しい場合は、責任者が総合的に判断する。（対象：組織管理者, 開発部）

供給者との合意における情報セキュリティの取扱い

- 委託先との契約には「機密保持に関する内容」および「情報漏えいが発生した場合の報告に関する取り決め」を含める。（対象：組織管理者）

情報通信技術（ICT）サプライチェーンにおける情報セキュリティの管理

- 供給者に対しては、委託した業務の再委託を原則禁止とする。やむを得ず再委託を実施する場合は、再委託先にも、当社が委託先に求めるものと同等のセキュリティレベルが確保できるようにする。（対象：組織管理者, 開発部）

供給者のサービス提供の監視、レビュー及び変更管理

- 年1回、現在の供給者が引き続き委託先評価基準を満たしていることを再確認する。（対象：組織管理者, 開発部）

クラウドサービスの利用における情報セキュリティ

- クラウドサービスを新しく利用する場合は、別項で定める「委託先評価基準」に従い選定を行う。（対象：組織管理者）
- データが保管される国を明らかにし、その国固有の法令や規制に自社のデータが悪影響を受けないかを確認する。（対象：Github, Google Workspace, Slack, freee, Figma, Linear）
- サービス利用終了時のデータのエクスポートが可能であるかを確認する。（対象：Github, Sentry, Notion, Google Workspace, Slack, freee, Figma, Linear, AWSリソース）

情報セキュリティインシデント管理の計画策定及び準備

- 情報セキュリティインシデントへの対応の責任者は、ISMS責任者とする。（対象：組織管理者, 開発部）

情報セキュリティ事象の評価及び決定

- 情報セキュリティに関する報告を受けたISMS担当者は、ISMS責任者に相談し、以下を参考にインシデントレベルを決定する。
  ・Low：経営や事業に影響なし（ヒヤリハット）
  ・Middle：当社の事業や、通常の業務に影響が及んだ
  ・High：顧客に影響が及んだ、もしくは個人情報が漏えいした （対象：組織管理者, 開発部）

情報セキュリティインシデントへの対応

- ISMS担当者から報告を受けたISMS責任者は、以下の手順に従って対応を行う。
  1. インシデントレベルがMiddleもしくはHighに該当する場合は、トップマネジメントに事象を報告する。
  2. ISMS責任者の指揮のもと、インシデントの原因分析と同時に、被害を拡大させないため、および二次被害を防止するための対応を実施する。
  3. 個人情報の漏えいを伴う場合には、個人情報保護委員会に報告する。（対象：組織管理者, 開発部）

情報セキュリティインシデントからの学習

- 情報セキュリティインシデントへの対応が終了した後は、同様のインシデントを再発させないために、SecureNaviを利用して是正処置（再発防止策）を策定、実施する。（対象：組織管理者）

証拠の収集

- 情報セキュリティインシデントに対する対応の結果や、インシデントの証拠となるようなログは、記録して保管する。（対象：組織管理者）

事業の中断・阻害時の情報セキュリティ

- 危機や災害などの発生時における可用性に関する目標（例えば、目標復旧時間など）を定める。（対象：LeanQuest）
- 危機や災害などの発生時における可用性に関する目標（例えば、目標復旧時間など）を達成するための、復旧計画を定める。（対象：LeanQuest）

事業継続のためのICTの備え

- 定めた復旧計画が引き続き有効であることを確認するために、定期的に計画のテスト実施を行う。（対象：LeanQuest）

法令、規制及び契約上の要求事項

- 自社に関連する法令や規制を洗い出し、法規制リストにまとめる。（対象：組織管理者）

- 外国に機器やソフトウェアを輸出、持ち出しする場合は、当該国の暗号化法令を事前に確認し、遵守する。（対象：開発部）

知的財産権
- ソフトウェアを利用する場合は、事前に利用規約などを確認し、規約に違反する利用を防止する。（対象：組織管理者）

記録の保護
- 法律や規制により、一定期間の保管が求められる文書（経理関係書類、労務関係書類など）は、滅失や改ざんを防ぐため、適切なアクセス権のもとで、所定の期間、保管する。（対象：組織管理者, 開発部）

プライバシー及び個人識別可能情報（PII）の保護
- 事業において利用する個人情報は、個人情報保護法に基づいて管理を行う。（対象：組織管理者）

情報セキュリティの独立したレビュー
- 年1回、内部監査を実施し、情報セキュリティに関する規程の遵守状況の確認を行う。（対象：組織管理者, 開発部）

情報セキュリティのための方針群、規則及び標準の順守
- 年1回、内部監査を実施し、情報セキュリティに関する規程の遵守状況の確認を行う。（対象：組織管理者, 開発部）
- 毎月、監視・測定を実施し、情報セキュリティに関する規程の遵守状況の確認を行う。（対象：組織管理者）

操作手順書

人的管理策

選考
- 従業員の採用においては、採用候補者の履歴書の確認やリファレンスチェックなどを実施し、信頼に足る人物であることを確認する。（対象：開発部）

雇用条件
- 採用が決まった従業者とは、秘密保持に関する誓約書（秘密保持に関する内容が記載された「雇用契約書」でもよい）を締結する。（対象：組織管理者, 開発部）

情報セキュリティの意識向上、教育及び訓練
- 従業者に対して、少なくとも年1回、情報セキュリティに関する教育を実施する。（対象：開発部）

懲戒手続
- 就業規則では、社内規程（情報セキュリティに関する規程を含む）に違反したときの懲戒手続きについて定めておく。（対象：組織管理者）

雇用の終了又は変更後の責任
- 従業員が退職するとき、もしくは契約終了となるときは、「退職時の秘密保持に関する誓約書」を締結するか、雇用契約書・業務委託契約書に退職・契約終了時の秘密保持に関して定めておくこと。（対象：組織管理者, 開発部）
- 従業員が退職するときは、「退職時のチェックリスト」に従い、貸与物品の返却や、アカウントの削除を行う。（対象：組織管理者, 開発部）

秘密保持契約又は守秘義務契約
- 機密情報のやり取りは、原則として事前に秘密保持あるいは守秘義務に関する内容を含んだ契約が締結されている組織に対してのみとする。ただし個人情報など、法令や他社との契約で定められていないものであれば、信頼できる組織に限り上記契約の締結前に情報をやりとりしてもよい。（対象：組織管理者）

リモートワーク
- パスワードが不要なフリーWi-Fiや、提供元がわからない野良Wi-Fiに接続しない。（対象：個人用デバイス）

情報セキュリティ事象の報告

- 情報セキュリティインシデント（もしくはその疑い）を発見した場合は、速やかにISMS担当者に報告する。（対象：組織管理者, 開発部）
- 情報セキュリティの弱点（将来的にインシデントにつながる可能性のある事象）を発見した場合は、速やかにISMS担当者に報告する。（対象：組織管理者, 開発部）

物理的管理策

物理的セキュリティ境界

- オフィスのフロア図を作成し、以下に従ってゾーンを区切り、フロア図に明記する。
  ・来客エリア：受付や会議室など、来客が入室可能なエリア
  ・執務エリア：執務室や営業所など、従業員のみが入室可能なエリア
  ・サーバエリア：サーバ機器の保管場所など、従業員の中でも許可された者のみがアクセス可能なエリア（対象：本社オフィス）

物理的入退

- 無人状態になる場合は、時間帯に限らず、必ず出入口の施錠を行う。（対象：本社オフィス）
- 入退室管理システムや電子錠を利用し、オフィスへの入退室ログを取得する。（対象：本社オフィス）
- 執務エリアは、来客を含めた従業者以外の入室は原則禁止する。入室の必要がある場合は、従業者が必ず帯同する。（対象：本社オフィス）
- 荷物の受け取りは来客エリアで行い、宅配スタッフが執務室に入室しないようする。やむを得ず入室する場合は、必ず従業者が帯同する。（対象：本社オフィス）

オフィス、部屋及び施設のセキュリティ

- サーバやネットワーク機器など、重要機器の設置場所は、むやみに第三者に口外しない。（対象：本社オフィス）

物理的セキュリティの監視

- 入退室管理システムや電子錠を利用し、オフィスへの入退室ログを取得する。（対象：本社オフィス）

物理的及び環境的脅威からの保護

- 重要な機器や紙媒体は、盗難や火災、火災時のスプリンクラーによる浸水リスクを考慮した場所に設置・保管する。（対象：本社オフィス）

セキュリティを保つべき領域での作業

- 個人情報（従業者の個人情報を含む）を取り扱う業務は、盗み見に考慮し、背後に壁のある環境で行う。（対象：本社オフィス）
- 執務エリア内での写真撮影は、情報の映り込みに十分に注意する。（対象：本社オフィス）
- ホワイトボードの利用は、利用が終わり次第、速やかに内容を消去する。（対象：本社オフィス）

クリアデスク・クリアスクリーン

- PCやサーバなど、ディスプレイを有する機器の近くから離れる場合は、必ず手動でスクリーンロックを有効にする。（対象：本社オフィス）
- 机上やプリンタなど、容易に盗み見ができる場所に、紙媒体を放置しない。（対象：本社オフィス）

機器の設置及び保護

- 重要な機器や紙媒体は、盗難や火災、火災時のスプリンクラーによる浸水リスクを考慮した場所に設置・保管する。（対象：本社オフィス）

構外にある資産のセキュリティ

- 社外で利用する場合、たとえ一時的であっても、無人状態で放置しない。（対象：個人用デバイス）

記録媒体

- 社外に持ち出す場合は、事前に責任者の許可を得る。（対象：ルーター）

- 機密情報・社外秘情報が保存された状態で輸送する場合は、盗難や破損を防ぐため、適切な保護（例えば、配達記録が残る手法を用いた輸送方法を選択する、十分な梱包を行うなど）を実施する。（対象：個人用デバイス, ルーター）

サポートユーティリティ

- 停電やビルのメンテナンスにそなえ、安定稼働が必要な装置（サーバ、デスクトップPC、ネットワーク機器）に対してUPS（無停電電源装置）を設置するか、停止時の代替策を準備しておく。（対象：本社オフィス）

ケーブル配線のセキュリティ

- 付随するケーブル類（通信ケーブル・電源ケーブルなど）は、つまずきによる断線や抜線の防止のために、通路をまたいだ敷設を行わない。（対象：ルーター）

装置の保守

- ベンダーの推奨するタイミングで、定期的に保守メンテナンスを実施する。（対象：ルーター）

装置のセキュリティを保った処分又は再利用

- 廃棄する場合は、社内で内部メモリを物理的に破壊するか、専門の廃棄業者に依頼する。（対象：個人用デバイス, ルーター）
- 廃棄を専門の廃棄業者に依頼する場合は、廃棄証明書もしくはデータ消去証明書を受領する。（対象：個人用デバイス, ルーター）

技術的管理策

利用者エンドポイント機器

- 社外で利用する場合、たとえ一時的であっても、無人状態で放置しない。（対象：個人用デバイス）
- パスワードが不要なフリーWi-Fiや、提供元がわからない野良Wi-Fiに接続しない。（対象：個人用デバイス）

特権的アクセス権

- 特権的アクセス権（管理者権限や、管理者ユーザーを含む）の付与は、必要最小限とする。（対象：Github, Sentry, Notion, Google Workspace, Slack, freee, Figma, Linear, AWSリソース）

情報へのアクセス制限

- 機密情報およびそれを扱う情報システムは、最小権限の原則に基づき、業務上必要な人のみにアカウント付与・アクセス権限の限定を行う。（対象：組織管理者, 開発部）

ソースコードへのアクセス

- ソースコードへのアクセスは、最小権限の原則に基づき、業務上必要な人のみにアカウント付与・アクセス権限の限定を行う。（対象：組織管理者, 開発部）

セキュリティを保った認証

- ログイン認証には、シングルサインオン認証、もしくは2要素認証を利用する。（対象：Github, Sentry, Notion, Google Workspace, Slack, freee, Figma, Linear, AWSリソース）
- ログインに関するセキュリティ設定（例えば「ログインに失敗したときのロック設定」「2要素認証の強制」など）ができる場合は、これらの設定の有効化を行う。（対象：Github, Linear）

容量・能力の管理

マルウェアに対する保護

- マルウェア対策ソフトをインストールする。（対象：個人用デバイス）
- マルウェア対策ソフトは、定義ファイル（更新プログラム）の自動更新設定を有効にし、常に最新の状態を保つ。（対象：個人用デバイス）

技術的ぜい弱性の管理

- インストールするOSやソフトウェアは、常に最新のバージョンを利用する。何らかの理由で、最新のバージョンを利用できない場合は、現在利用しているバージョンにぜい弱性がないことを確認する。（対象：個人用デバイス, ルーター）

- 年1回、内部監査を実施し、情報セキュリティに関する規程の遵守状況の確認を行う。（対象：組織管理者, 開発部）

構成管理

- 機器管理台帳を作成し、社内で利用している機器と、その情報（インストールされているOSやソフトウェア、有効なセキュリティ設定など）を管理する。（対象：個人用デバイス, ルーター）
- 定期的（目安として6ヶ月に1回）に機器管理台帳を見直し、台帳の内容と実態にズレがないかを確認する。（対象：個人用デバイス, ルーター）

情報の削除

- 機密情報に該当する情報は、SecureNaviの資産リストにおいて保管期間を明記し、保管期間を終えた資産は、速やかに削除を行う。（対象：組織管理者）

データマスキング

- 個人情報の利活用を行う場合は、個人情報保護法に基づき、仮名化もしくは匿名化を行う必要がないかを確認し、必要に応じて実施する。（対象：組織管理者, 開発部）
- システムのテストで用いるデータに、本番環境のデータを用いてはならない。やむを得ず利用する場合は、機密情報をマスキングした上で利用する。（対象：LeanQuest）

データ漏えい防止

- 外部にファイルを送信したり共有する機能がある場合は、その機能の操作ログの取得、あるいは利用禁止などの措置により、意図しない情報の外部漏えいを防止する。（対象：Google Workspace, Slack, freee）

情報のバックアップ

- 故障に備え、保存される情報は、定期的に、クラウドサービスへのアップロードもしくは別媒体へのバックアップを行う。（対象：個人用デバイス）
- 定期的にデータのバックアップを取得する。（対象：Figma）

情報処理施設・設備の冗長性

- 停止により会社にとって大きなインパクトを与える情報システムは、適切なシステムの冗長化を行う。（対象：LeanQuest）

ログ取得

- 取得したログデータには、アクセス制御を実施し、ログが消去・改ざんされないようにする。（対象：Google Workspace, Slack, freee）

監視活動

クロックの同期

- ログに記録される時間は、NTPの利用などにより、正確な時刻が記録されるようにする。（対象：LeanQuest）

特権的なユーティリティプログラムの使用

- ユーザーによる変更・カスタマイズが想定されていない設定の変更（例えば、Windowsにおけるレジストリの変更）は、禁止する。（対象：SwitchBot）

運用システムへのソフトウェアの導入

- 以下のソフトウェアは、原則インストールおよび利用してはならない。
  ・不特定多数の機器間でファイル共有ができるソフトウェア（いわゆるP2Pを利用したファイル共有ソフトウェア）
  ・作成元が不明、もしくは不審なベンダーが提供するソフトウェア
  ・非正規のライセンス情報を利用したソフトウェア（対象：個人用デバイス, ルーター）
- 本番環境におけるソフトウェアの変更（リリース、利用しているソフトウェアの変更やバージョンアップなど）は、変更が失敗したときに切り戻し（ロールバック）ができるようにする。（対象：LeanQuest）

ネットワークのセキュリティ

- ログイン認証を設定し、許可されていない者が接続できないようにする。（対象：業務用ネットワーク）
- 通信経路の暗号化を行う。（対象：業務用ネットワーク）

- ネットワークを通過する情報を鑑み、適切なネットワーク分離を行う（来客用ネットワークと業務用ネットワークの分離、社内利用ネットワークと社外向けサービス用ネットワークの分離など)。（対象：業務用ネットワーク）

ネットワークサービスのセキュリティ
- ネットワーク構築ベンダーとの契約においては、ネットワークの機密性や可用性が、業務を行う上で問題がないレベルであることに注意する。（対象：業務用ネットワーク）

ネットワークの分離
- ネットワークを通過する情報を鑑み、適切なネットワーク分離を行う（来客用ネットワークと業務用ネットワークの分離、社内利用ネットワークと社外向けサービス用ネットワークの分離など)。（対象：業務用ネットワーク）

ウェブフィルタリング
- 業務に関係のないWebサイトにはアクセスを行わない。（対象：個人用デバイス）
- Webフィルタリングツールを導入し、危険なWebサイトへのアクセスを未然に防ぐ。（対象：業務用ネットワーク）

暗号の使用
- インターネットブラウザを介して情報を送信する場合は、暗号化された通信（https通信など)を利用する。（対象：組織管理者, 開発部）

セキュリティに配慮した開発のライフサイクル
- 利用しているプログラミング言語やフレームワークにおける、セキュリティのベストプラクティスやガイドラインを特定し、自らのシステム開発に確実に実装されるようにする。（対象：LeanQuest）

アプリケーションセキュリティの要求事項
- インターネットを経由する通信は、SSL通信を利用するなどし、暗号化ならびに不正な改ざんを防止する。（対象：LeanQuest）

セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則
- 一般的な開発におけるセキュリティ対策（認証と認可、セッション管理、入力値の検証など）については、原則としてすべてのシステム開発において適用する。（対象：LeanQuest）

セキュリティに配慮したコーディング
- 利用しているプログラミング言語やフレームワークにおける、セキュリティのベストプラクティスやガイドラインを特定し、自らのシステム開発に確実に実装されるようにする。（対象：LeanQuest）

開発及び受入れにおけるセキュリティテスト
- システム内部に実装されているセキュリティ機能（認証と認可、セッション管理、入力値の検証など）については、正しく実装されていることを確認するため、テストを実施する。（対象：LeanQuest）

外部委託による開発
- 外部委託によって開発が行われたシステムは、必ず受け入れテストやレビューを実施し、情報セキュリティ品質に問題がないことを確認する。（対象：LeanQuest）

開発環境、テスト環境及び本番環境の分離
- 開発環境には、開発者以外はアクセスできないよう、アクセス制御を行う。（対象：LeanQuest）
- 開発環境・試験環境・運用環境（本番環境）は分離する。（対象：LeanQuest）

変更管理
- OSやミドルウェア（DB、フレームワークなどを含む）を変更する場合は、リリースの前のレビューやテストを徹底する。（対象：LeanQuest）
- システム開発において利用するパッケージソフトウェア（ミドルウェア・OSSなど）は、原則として改造や、想定されていないカスタマイズを行わない。（対象：LeanQuest）
- 開発におけるソースコードやドキュメントは、バージョン管理システムを用いて管理する。（対象：LeanQuest）

テスト用情報

- システムのテストで用いるデータに、本番環境のデータを用いてはならない。やむを得ず利用する場合は、機密情報をマスキングした上で利用する。（対象：LeanQuest）

監査におけるテスト中の情報システムの保護

- システム監査やぜい弱性診断を行う場合は、原則、本番環境と構成を同じくした、異なる環境で実施する。やむを得ず本番環境にて行う場合は、システムの運用に影響がないよう十分に注意する。（対象：LeanQuest）