株式会社：会社名事業継続計画（BCP）

サイバーセキュリティ対策

部門：薬局名

初版：2023年12月1日

更新：2024年1月24日（第2版）

更新履歴

2024年1月24日：従業員の変更

1.業務継続の基本方針

【目的】

保護すべき患者情報のセキュリティを確保し、システムの迅速な復旧と業務の継続性を確保する。

【目標】

インシデントの影響を最小限に抑え、業務復旧までの時間を短縮する。

【方針承認】

この基本方針は経営層により承認され、全スタッフに対して周知される。

【経営陣の率先垂範】

上記の方針及び目的のもと、経営陣は、緊急事態対応及び事業継続対応への取り組みの重要性を十分に理解し、それをすべての従業員に周知・徹底する。

また、経営陣は、当社が必要と認める施策を推進するために必要な経営資源を配分する。

【適用範囲】

1) 緊急時対応

この計画における緊急事態対応は、すべての従業員（契約社員・派遣社員を含む）を対象とする。

2) 事業継続対応

この計画における事業継続対応は、原則として、すべての製品・サービス、組織を対象とする。

【本計画の見直し改定】

1) 変更管理

事業環境、事業内容、事業方針、組織変更等、本計画にかかる重要な事項が変更された場合、その他の理由によって変更が必要とされる場合、本計画を見直し、改定等必要な対応を行う

2) 定期的な見直し

本計画は、各店舗が毎年1月に見直し、改定等適切な対応を行う。

3) 改定にかかる承認

本計画を改定する場合は、経営陣（代表取締役）の決裁により行う。事業環境、事業方針、事業内容、大幅な組織変更などにより、基本方針や適用範囲などの重要な事項に見直し・改廃が生じた場合は、取締役会の決議を必要とする。

4) 最新版管理

本計画を改定する場合は、すべての従業員が最新版を入手できることを確実にする。また、廃止版が誤って使用されることを防ぐために識別し、管理を確実にする。

2. 運用体制の構築

チーム構成: セキュリティ専門家、ITスタッフ、経営者、法務顧問、コミュニケーション担当者から成る。

役割と責任: 各チームメンバーの役割と責任を文書化し、緊急連絡体制を確立する。

|  |  |  |  |
| --- | --- | --- | --- |
| チーム編成 | 所属 | 役職・部署 | 氏名 |
| 医療情報システム  安全管理責任者 | 株式会社：会社名 | 代表取締役 | 開設者名 |
| 医療情報システム  運用担当者 | 株式会社：会社名 | 管理薬剤師 | 開設者名 |
| 経営者 | 株式会社：会社名 | 代表取締役 | 開設者名 |
| コミュニケーション担当者 | 株式会社：会社名 | 取締役 | 社員名 |
| ITスタッフ | 株式会社：会社名 | 管理薬剤師 | 社員名 |
| セキュリティ専門家 | レセコン業者名 | システム担当 | 担当者名 |
| 法務顧問 | 弁護士法人 | 弁護士 | 弁護士名 |

3. 危機的事象の定義

事象の種類: データ侵害、システム障害、ランサムウェア攻撃。

基準の設定: 各事象を識別し、警告システムを通じて即時に識別する。

4. 被害状況の想定

リスク評価:シナリオごとのリスク評価を実施し、被害の範囲と影響を分析する。

■シナリオ1:データ侵害

|  |
| --- |
| 説明:不正アクセスにより患者の個人情報が露出する可能性があります。  リスク評価:  •影響の範囲: 患者情報の漏洩によるプライバシー侵害、信頼の損失。  •財務的影響: 法的責任による罰金や訴訟コスト。  •業務への影響: 患者からの信頼喪失によるリピートビジネスの減少。  対策:データの暗号化、アクセス管理の強化、定期的なセキュリティ監査。 |

■シナリオ2:システム障害

|  |
| --- |
| 説明:主要なシステムがハードウェアの故障、ソフトウェアのバグ、または外部からの攻撃により停止します。  リスク評価:  •影響の範囲:調剤情報システムのダウンによる調剤遅延。  •財務的影響:業務停止による直接的な収入の損失。  •業務への影響:患者ケアの質の低下、運用効率の悪化。  対策:冗長性のあるシステムの設計、定期的なバックアップ、故障復旧計画の策定。 |

■シナリオ3:ランサムウェア攻撃

|  |
| --- |
| 説明:マルウェアに感染してシステムがロックされ、データアクセスが拒否されます。  リスク評価:  •影響の範囲:重要なデータとシステムへのアクセス喪失。  •財務的影響:身代金支払いの圧力、運用コストの増大。  •業務への影響:重要な業務機能の停止、患者サービスの中断。  対策:アンチウイルスの導入と更新、従業員のサイバーセキュリティ教育、身代金支払いに依存しないデータ復旧策。 |

5. システムごとの復旧優先度を設定

優先度の決定: 業務の重要性とシステムの相互依存性に基づき優先度を設定する。

復旧優先度の評価は5段階として1が最も優先順位が高く、5が最も優先順位が低く評価

優先順位１の復旧は薬局業務の受付可能ラインとして、優先順位1が復旧することで業務再開を可能と評価する。

6. システム継続に必要な構成要素を整理

リソースリスト:必要なハードウェア、ソフトウェア、人的リソースを明確にリストアップする。

サーバー

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 機器 | 用途 | 所在地・識別ナンバー・IPアドレス | 主な利用者属性 | 復旧優先度 |
| データベースサーバー | 患者情報、在庫データ | 1階・001・192.168.\*\*\* | 薬剤師・事務員・システム管理者 | 1 |
| バックアップサーバー | データバックアップ | 2階・002・192.168.\*\*\* | 薬剤師・事務員・システム管理者 | 1 |
| マイナンバーカード受付 | マイナンバーカード受付 | 1階・EPSON00・192.168.\*\*\* | 薬剤師・事務員・システム管理者 | 3 |

ワークステーション

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 受付用コンピュータ | 受付入力 | 1階・DELL01・192.168.\*\*\* | 薬剤師・事務員・システム管理者 | 1 |
| 服薬指導用コンピュータ | 薬歴作成 | 1階・端末A・B・192.168.\*\*\* | 薬剤師 | 2 |
| マイナンバーカード | 顔認証 | 1階・Caora01・192.168.\*\*\* | 薬剤師・事務員・システム管理者 | 3 |
| タブレット | 服薬指導用 | 1階・iPad01・192.168.\*\*\* | 薬剤師・事務員・システム管理者 | 5 |
| POSレジシステム | 会計 | 1階・レジ | 薬剤師・事務員・システム管理者 | 5 |
| 発注用コンピューター | オンライン発注 | 1階・Panasonic01・192.168.\*\*\* | 薬剤師・事務員・システム管理者 | 5 |

ネットワーク機器:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ルーター | ネットワーク | 2階・201 | 薬剤師・事務員・システム管理者 | 1 |

周辺機器

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| プリンター | 薬情・薬袋作成 | 1階・EPSON01 | 薬剤師・事務員・システム管理者 | 4 |
| プリンター | 手帳シール作成 | 1階・104 | 薬剤師・事務員・システム管理者 | 4 |
| FAX・スキャナー | 処方箋受付・医療機関連携 | 1階・CANON | 薬剤師・事務員・システム管理者 | 3 |
| 無停電電源装置 | 無停電電源 | 1階・UPS01 | 薬剤師・事務員・システム管理者 | 3 |

7. 事前対策計画の作成

リスク軽減措置: データのバックアップ、アクセス制御の強化、定期的なセキュリティチェックを実施する。

8. 非常時対応の計画策定

■非常時における連絡体制図

インシデント報告

■データ侵害

■システム障害:

■ランサムウェア攻撃:

9. 教育訓練計画や維持改善計画の策定

教育訓練: 全スタッフに対する定期的なセキュリティ教育と訓練を実施。

維持改善: インシデント後のレビューを基に、計画の不備を特定し、継続的に改善する。

10. 薬局におけるサイバーセキュリティ対策チェックリストへの適合確認

|  |  |
| --- | --- |
| 医療情報システムを導入、運用している | 〇 |
| 医療情報システム安全管理責任者を設置している | 〇：項目2 |
| リモートメンテナンスを利用している機器を事業者に確認 | 確認して保管 |
| 利用者の職種・担当業務別の情報区分ごとのアクセス権限を設定している | 〇：項目6 |
| 退職者や使用していないアカウント等、不要なアカウントは削除されている | 各システムで削除確認 |
| アクセスログを管理している | 〇：管理確認 |
| セキュリティパッチを適用している | 〇：適用済み |
| 接続元制限を実施している | 〇：有線接続のみ |
| バックグラウンドで動作しているふようなソフトウェアおよびサービスは停止している | 〇：対策済み |
| インシデント発生時における組織内と外部関係機関の連絡体制図がある | 〇：項目8 |
| インシデント発生時に診療を継続するために必要な情報を検討しデータシステムのバックアップの実施と復旧手順を確認している | 〇 |
| サイバー攻撃を想定した事業実施計画（BCP）を策定、又は令和6年度中に作成予定 | 〇：本紙 |

≪チェックリスト最終確認日：2024年4月12日≫