事　業　継　続　計　画
（BCP）
サイバー攻撃編

令和８年

有限会社徳栄会

目次

第１章　総則

（１）策定目的

本事業継続計画（以下、「本 BCP」という）は、有限会社徳栄会（以下、「当社」という）において、サイバーインシデント発生時における組織的対応の基本方針および職員の取るべき行動の基本原則を示すことによって、介護サービスにおける利用者の安全確保および事故防止、個人情報等の情報保全を担保しつつ、サイバー攻撃に対応するセキュリティ体制の構築、ならびに早期復旧までを視野に入れた活動の実現により、地域に信頼される介護施設として社会福祉に貢献することを目的とする。

（２）基本方針

当社は、個人情報の保護と介護サービスの継続性を確保するために、以下の方針に基づき、サイバーセキュリティ対策の水準を高めていく。

① 安全かつ持続的な介護サービス提供を実現する
② サイバーセキュリティに対する脅威からの被害から事業を保護する
③ リスクマネジメントの対象としてサイバーセキュリティを確保する
④ 平時、非常時を通じて事業継続に関する説明責任を果たす
⑤ 被害後、介護サービスにおける利用者の安全確保および事故防止を担保しつつ、迅速かつ合理的な業務復旧を行う

（３）対象範囲

1-3-1 対象とする情報システム

対象とする情報システムは以下のとおり。

① 介護ソフト
② 会計システム
③ 給与システム
④ サーバー（共有フォルダ含む）
⑤ VPN システム

1-3-2 想定できる事象

本 BCP で想定される事象において、業務に影響するものを以下に挙げる。なお、自然災害、震災等による大規模停電等による電源喪失などの計画は別に定めるものとする。

① ケース記録、日誌、参照情報および指示情報の確認・参照不能
② ケース記録、日誌、参照情報および指示情報の入力不能
③ 拠点間の連絡不能
④ 情報機器等の操作不能・誤動作

また、これらの被害を引き起こすサイバー攻撃の例として以下が挙げられる。

① 不正アクセス

② 標的型メール攻撃

③ マルウェア感染（ランサムウェアを含む）

④ 分散型サービス妨害（DDoS 攻撃）

⑤ 上記の予兆と思われる現象

（4）文書の管理および周知

本 BCP は法人本部にて、現状を適切に反映した原本および関連資料の整備ならびに管理を行い、役員会の承認を受けた上で、当社の全職員に開示周知する。

第 2 章　体制整備

（1）情報機器等の把握と適切な管理

平時において、非常時に備えたサイバーセキュリティの体制整備を以下のとおり行う。

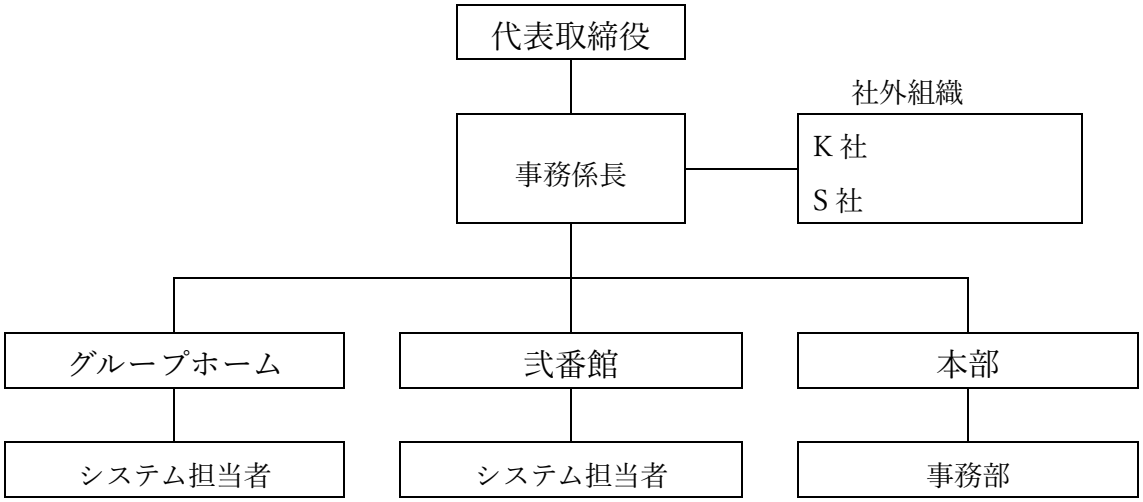
2 - 1 - 1　情報セキュリティ管理者

法人本部事務係長を、情報セキュリティ管理者として定める。代表取締役を当社におけるサイバーセキュリティに関する最高責任者（情報セキュリティ統括責任者）とする。

2 - 1 - 2　組織体制図

事業継続および情報システムの復旧を目的としたサイバーセキュリティの組織体制を以下のとおり定める。担当部署、担当者、役割についても示す。

（図 1）平時の組織体制図



（図２）担当者の役割

役割	担当部署・担当者	役割の概要
情報セキュリティ統括責任者	代表取締役	事業継続および情報システムの復旧の計画策定を統括し、最終的な責任を負う。
情報セキュリティ管理者	事務係長	情報システム復旧の計画策定に関する各種検討作業を行う。
本部　事務部	本部　事務部	事業継続の計画策定に関する各種検討作業を行う。
各拠点システム担当者	グループホーム 弐番館　各管理者	各部門システムの運用継続計画策定に関する各種検討作業を行う。
委託先	K 社 S 社	情報システムの運用保守および緊急時の状況に関する情報提供・対策調整。

2 - 1 - 3　情報機器台帳

情報セキュリティ管理者は、情報機器の現況を反映した管理台帳を別紙１のとおり整備する。併せて、定期的に棚卸しを行い、機器の所在と稼働状況の確認を行う。

2 - 1 - 4　ネットワークシステム構成図

情報セキュリティ管理者は、当社で導入している情報システムの全体図を整備する。併せて、構成、接続等に変更が生じた場合には構成図の更新を行い、常に最新の状態を保つ。

2 - 1 - 5　リスク評価・代替運用

各システムが利用できなくなった場合、その業務内容の代替手段を以下のとおり定める。また、代替運用方法については別途、システム停止時の代替運用マニュアル等にて定める。

（図３）業務内容に対する代替手段

業務内容	システム	代替手段
ケース記録等	介護ソフト	紙運用
ケアプラン等	介護ソフト	紙運用
請求等	介護ソフト	紙運用、未収扱いを検討
会計	会計ソフト	オフラインでの運用、未収扱いを検討
給与	給与ソフト	オフラインでの運用、紙運用

2-1-6 脆弱性に関する対策

情報セキュリティ管理者は、契約等で定められた責任分界をもとに、サーバー、端末 PC、ネットワーク機器について脆弱性情報の収集を行う。脆弱性が発見された機器について、脆弱性対応プログラムの適応を行う。万が一、適応できない場合の代替手段（隔離運用、隔壁の追加、監視の強化、機器の入れ替え等）について事業者と合意したうえで取り決め、実施する。

（2）非常時に備えたサイバーセキュリティ体制

2-2-1 法人内 CSIRT の位置付け

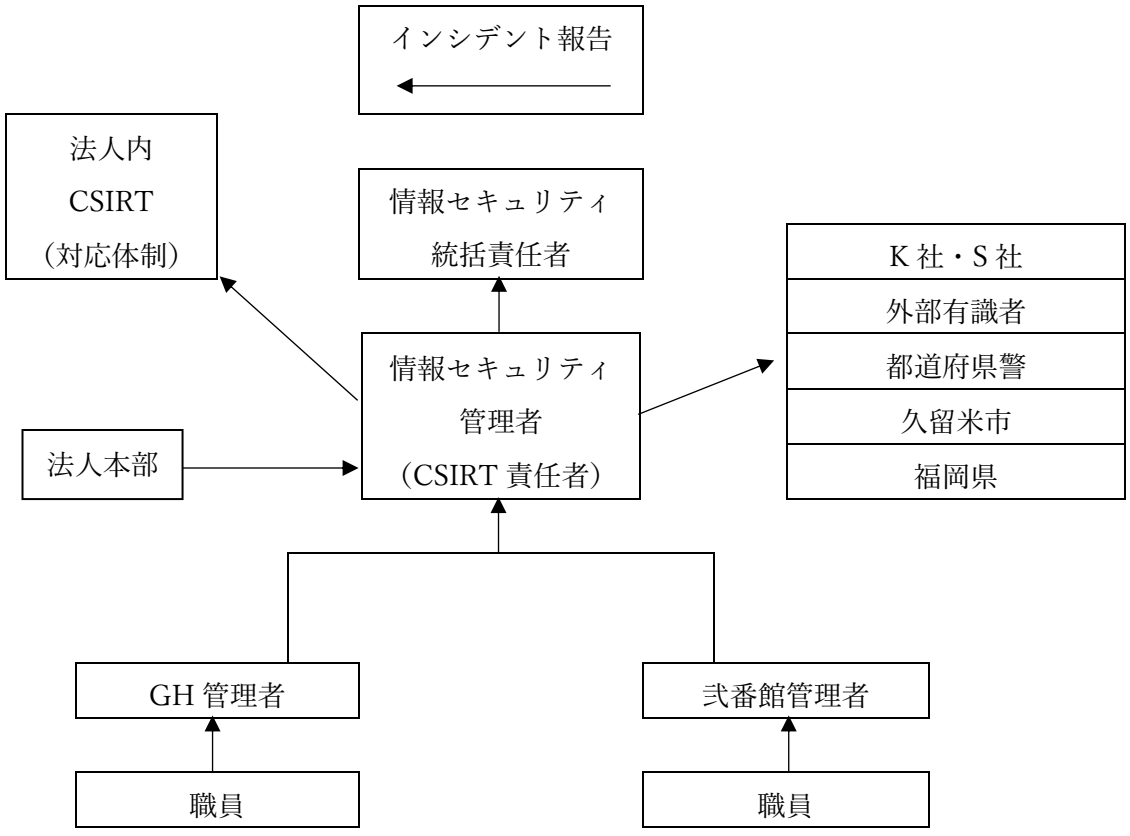
CSIRT（Computer Security Incident Response Team）とは、当社において発生した、または発生が疑われる情報セキュリティインシデントに対し、被害拡大防止、事実確認、意思決定支援、関係機関への報告および再発防止策を目的として対応する体制をいう。

当社においては、小規模法人であることを踏まえ、専任の組織としての CSIRT は設置せず、情報セキュリティ管理者を中心として、事案の内容に応じて関係者を招集し、法人内 CSIRT として対応するものとする。

2-2-2 連絡体制図

事業継続および情報システムの復旧に資するアクションを迅速に行う目的で、サイバーセキュリティの連絡体制および外部関係機関の連絡先を以下のとおり定める。

（図４）連絡体制図



（図５）外部関係機関の連絡先一覧　※個人情報のため電話番号は割愛

外部関係機関	連絡先
久留米市介護保険課	
久留米市長寿支援課	
福岡県警本部（サイバー犯罪対策課）	
K 社	
S 社	

2-2-3 情報収集体制

当社における各システムの脆弱性情報について事業者等から情報提供を定期的に受け取ることができる体制を以下のとおり構築する。

（図６）事業者等の連絡先　※個人情報のため電話番号は割愛

システム	担当	連絡先
介護ソフト	N 社	
保守委託先	K 社	
	S 社	

2-2-4 教育体制

本 BCP が迅速かつ適切に利用できるよう、年 1 回以上の教育、訓練を実施する。教育および訓練の企画・実施にあたっては、情報セキュリティ管理者（法人内 CSIRT 責任者）が中心となり、必要に応じて各管理者および関係者と連携して行うものとする。

教育・訓練の結果により、事前対策やサイバーインシデント発生時の対応計画等に課題が認められた場合は、当該課題について見直しまたは改善を行う。

2-2-5 バックアップ体制

サイバーインシデント発生時に備えた、データとシステムのバックアップの頻度、作成方法および復旧方法について以下のとおり定める。

（図7）バックアップの作成と復旧方法

システム	頻度	作成方法	復旧方法
介護ソフト	毎日	外付け HDD 等にデータベースとシステムファイルのバックアップを作成する。	システムの OS を再構築後、ミドルウェアおよびアプリケーション環境を構築し、システムファイルを復元。その後、データベースを復元し、最後にバックアップデータを復元する。
共有フォルダ	7日	同上	同上
マネージド	7日	同上	同上
会計ソフト	7日	同上	同上
給与ソフト	7日	同上	同上

第3章 サイバーインシデント発生時の対応

（1）異常発見時の連絡先

異常発見時の連絡先経路は、2-2-1の図1に示すとおりとする。併せて、各担当部門の連絡先は以下のとおり示す。なお、部門システムの管理者は連絡先が全職員に把握されるように明示して、常に最新版で管理し連絡経路が機能することを担保する。

（図8-1）部門連絡先一覧　※個人情報のため、氏名、連絡先は割愛

部署名	担当者	連絡先
グループホーム	（管理者）	
弐番館	（管理者）	
情報セキュリティ管理者	（CISO）	

（図8-2）部門連絡先一覧　※個人情報のため、氏名、連絡先は割愛

システム	事業者	担当者	連絡先
介護ソフト	N 社		
PC、ネット環境	K 社		
セキュリティ	S 社		

（２）システム異常の検知と経営層への情報伝達

システム異常を検知した場合、あらかじめ定めた項目（発生場所、発生個所、発生日時、連絡者、異常の内容・範囲）について担当部門に報告できるように周知する。なお、口頭による連絡後、「報告様式」を用いて記録を残す。また、職員から発せられた異常において、情報セキュリティ管理者によりサイバー攻撃の可能性が思慮された場合、２-２-１で作成した連絡体制図を基に、速やかに役員会ならびに関係各所・外部関係機関に共有され、意思決定できるように努める。

（３）初期対応

サイバーインシデント発生後は、以下のとおり対応する。

３-３-１ 原因調査

情報セキュリティ管理者はサイバーインシデントの原因や被害範囲の特定のために、情報システム・サービス事業者へ以下の調査依頼を指示または実施する。

① ネットワーク機器やケーブル等の調査

② 電気系統、ブレーカー、ハードウェア、ソフトウェア等の調査

③ 情報漏洩の有無に関する調査

④ メンテナンスやデータ移行等の作業に関する調査

３-３-２ 被害拡大防止

被害拡大防止のための対応を行う。まずは、バックアップに通ずるネットワークの遮断を行う。次に、外部の通信経路を遮断する。そのうえで、被害個所から攻撃範囲および侵入経路の推定を行ったうえで、セグメーション境界において、通信を遮断して感染拡大を図る。

３-３-３ 役員会への報告

情報セキュリティ管理者はサイバーインシデントについて役員会に対して、現在の被害状況を報告するとともにインシデント対応方法と利用者安全を担保する運営方針案を提案する。この内容を踏まえて、役員会はシステム停止に伴う事業継続方針を検討し意思決定する。決定した内容は、速かに２-２-１の連絡体制図で定める組織内ならびに外部関係者へ周知を行う。

（４） 事業継続

サイバーインシデント発生時においては、情報システムの復旧対応と並行して事業継続を図るものとする。この際、ICT 障害時においても、服薬管理、食事提供、排泄介助等の生命・生活に直結する介護サービスを最優先に継続する。

サイバーインシデント対応と事業継続について報告を受けた役員会は以下のとおり対応する。

３-４-１ 情報システムの縮退運転判断

役員会は情報セキュリティ管理者からの報告を受け、情報システム等の縮退運転または運転中止を判断する。また、インシデント対応中の事業継続については、紙でのケース記録の運用等、自然災害時を想定した事業継続計画に則り運用する。

3-4-2 被害状況等調査（フォレジック調査＋証拠保全）

情報セキュリティ管理者は、証拠保全の作業と事業継続に関する作業を調整しながら両立させる。具体的にはアクセスログの分析や情報の改ざん、暗号化の有無等からサイバー攻撃の範囲、個人情報漏洩の有無等の調査について介護サービスにおける利用者の安全確保および事故防止を担保しつつ行う。

3-4-3 組織対応方針の確認と外部関係機関への報告

情報セキュリティ管理者の被害状況および調査結果に基づき、役員会は復旧対応方針（復旧に向けた対応、後方への対応）を決定し、その対応を関係者に指示する。また、2-2-1で定める外部関係機関へ報告を行う。外部関係機関へは被害拡大防止等の観点からできる限り早く連絡する。

（5）復旧処理

復旧計画に基づいて、以下のとおり対応する。情報セキュリティ管理者は情報システムの事業者およびサービス事業者等と協力して復旧を行う。

3-5-1 復旧指示と復旧作業

情報セキュリティ管理者は、役員会からの復旧指示を起点とする復旧対応方針に基づき、システムの復旧作業（システムの再設定、再インストール、バックアップデータからの復元等）ならびに検証作業を行う。必要に応じ情報システム・サービス事業者に対応を依頼する。あわせて、システム停止中に生じたアナログ情報についてシステムに反映させる選択肢を提示する。役員会は、アナログ情報の反映時期ならびに程度を、介護サービスにおける利用者の安全確保および事故防止、個人情報等の情報安全の観点を踏まえて意思決定する。

3-5-2 結果の確認

情報セキュリティ管理者は、復旧作業により復旧したシステムが安全な状態で正常に稼働したことを確認する。正常に稼働することが確認できた時点で、役員会に報告する。役員会は業務遂行状況を総合的に勘案し、緊急時運用から通常運用への復旧を宣言する。

第4章 事後対応

（1）報告

復旧後、復旧結果と情報漏洩事実の有無について、役員会および組織内に報告する。不足していたと考えられる事前対策、連絡先ならびに連絡内容について振り返りを行う。

また、個人情報の漏洩、滅失または毀損が発生し、または発生したおそれがある場合であって、個人情報保護法に基づく報告義務が生じると判断されるときは、情報セキュリティ管理者を中心として事実関係を確認のうえ、個人情報保護委員会への報告および関係者への対応を適切に行う。

（2）再発防止

4-2-1 再発防止対策検討・策定

前項の後、サイバー攻撃により発生した被害を抑止する手段について検討を行い、実施可能な選択肢を整備し、役員会に提案する。役員会は長期的視点と事業継続性の両立について検討し、安全性を維持するため再発防止策の選択を決定する。役員会は決定した再発防止策について、連絡経路を用いて全職員に周知する。

4-2-2 事業者への指示

役員会によって決定された再発防止策は、情報セキュリティ管理者等により、事業者が有するサービスや機器に対して対策を講じる必要があるかどうかを調査し、再発防止策の効果が出るよう対策実施を事業者へ打診する。事業者は、対策実施の時期や方法について、当社と誠実に議論し、計画を立てて実施する。

（3）情報公開

役員会は、類似のサイバー攻撃による被害拡大に対する警鐘を鳴らす目的、また当施設を利用する高齢者およびその家族へサービス利用に関連する注意を喚起する目的で、速やかに情報公開を行う。情報公開内容は、知覚日時、現象、被害範囲、想定される攻撃経路、一次対応、利用者対応、復旧状況、事後対策などを含める。報告については、サイバー被害が発生した可能性が高い段階から迅速に行い、情報の更新を含めて複数回行う中で情報の確度を高めていく。

第5章 附則

（1）本計画は、令和8年2月1日より施行する。

（別表１）情報機器台帳　※機器台帳は機密情報含むため割愛

管理番号	メーカー	OS	コンピューター名	設置場所	利用者	状態	ソフト
001							
002							
003							
004							
005							
006							
007							
008							
009							
010							
011							
012							
013							
014							
015							
016							
017							
018							

（別表２）

サイバーインシデント初動対応フロー

① 職員が異常を見つけたら（最初の１分）

例）変な音/動作が重い/勝手に送信/ファイルが開かない/身代金要求画面など

【やること】

１．ネットを切る（LAN ケーブルを抜く/Wi-Fi OFF）

２．画面の撮影（警告文、エラー文、時刻が分かるように）

３．すぐ報告（拠点管理者→情報セキュリティ管理者）

【やってはいけない】

１．勝手に再起動しない

２．勝手に削除、初期化しない

３．勝手に業者、警察、市役所に連絡しない

４．SNS や私的連絡で外部に話さない

② 拠点管理者（一次対応：３分）

【確認】

１．他の PC でも同様の症状があるか

２．同じメール（添付ファイル）を開いた人がいないか

３．介護ソフト/共有フォルダ/ネットが使えるか

【指示】

１．該当端末は隔離継続（ネット遮断）

２．全職員へ注意喚起

３．重要業務は紙運用の準備（記録・申し送り等）

③ 法人内 CSIRT（情報セキュリティ管理者）が指揮（５分）

【インシデント分類】（どれに近いか）

A：軽微（疑い）

・迷惑メール/広告表示/添付未開封　など

B：中度（感染・侵入の疑い）

・PC が異常に遅い/勝手に動く/不審送信の可能性　など

C：重大（ランサム・漏洩疑い）

・暗号化、身代金要求/共有フォルダが開かない/情報流出の可能性　など

④ 対応（分類別）

A：軽微（疑い）

・端末は隔離のまま

・委託先へ相談（点検、スキャン等）

・必要に応じてパスワード変更

・記録を残して経過観察

B：中度（感染、侵入疑い）

・影響範囲を確認（同一ネットワーク端末点検）

・共有フォルダ、メール等の確認

・委託先へ緊急連絡

・統括責任者へ第一報

C：重大（ランサム、漏洩疑い）

・ネットワーク全体の遮断を検討（拠点単位）

・介護ソフト/共有フォルダ停止→紙運用へ即切り替え

・委託先へ緊急連絡（復旧、調査）

・統括責任者へ即報告→対外報告判断へ

⑤ 統括責任者への第一報

・発生日時：

・発生拠点：

・端末/システム：

・現象（暗号化/不審送信等）：

・個人情報の関与：あり/なし/不明

・現在の対応（隔離・遮断・紙運用）：

・委託先連絡状況：済/未

⑥対外連絡のルール

外部連絡は原則、情報セキュリティ管理者（法人内 CSIRT）が実施。

※個人情報漏洩の疑いがある場合は「個人情報保護管理規定」に沿って対応する。