「BCPortal ASP サービス」情報セキュリティ管理

BCPortal における情報セキュリティ及びクラウドサービスセキュリティへの取り組みついて、下記の通りご説明いたします。

記

(ア)　外部認証

第三者機関から以下の認証を取得しており、安全管理策を策定し、実施・維持・改善活動を行っております。

1. プライバシーマーク
   初回取得年月日：2001 年 8 月 14 日
   登録証番号：11820104(12)
   認証期限：2025 年 8 月 13 日
2. ISMS 認証
   初回取得年月日：2019 年 4 月 1 日
   登録証番号：IS 699260
   認証期限：2028 年 3 月 31 日
3. ISMS 認証（ISO/IEC 27017）
   初回取得年月日：2024 年 6 月 27 日
   登録証番号：CLOUD 805500
   認証期限：2028 年 3 月 31 日

(イ)　責任・役割

当社は、本サービスを提供するための設備（サーバ、OS、ミドルウェア、アプリケーション）に対し、情報セキュリティ対策の責任（マルウェア対策、システム復旧手段の確立）を負うものとします。ただし、契約者が使用する情報機器の情報セキュリティ対策については、契約者がその責任を負うものとします。

(ウ)　安全管理措置

具体的な取り組み内容の概要は以下のとおりです。

1. 組織的管理策
   A)　情報セキュリティのための方針群
   安全管理に係る基本方針および取扱規程を定めており、また ISMS においてはトップマネジメントによって承認された情報セキュリティ方針を定めています。
   B)　情報セキュリティの役割と責任
   管理規程に基づき管理責任者を設置し、従業者の役割・責任・権限を規定・ルール等で定めています。
   C)　職務の分離
   職務（開発と運用など）により担当領域を明確に分離して相互に干渉できないようにしてい

ます。また、管理者と担当者の役割を分離し相互に牽制する体制を構築しています。

D) 経営陣の責任
経営陣は情報セキュリティのための方針群を支持し、自らの情報セキュリティの責任を認識し、果たすために全従業員に要求しています。

E) 関係当局との連絡
重大インシデント発生時の報告手順を定め体制を構築し関係者に周知しています。

F) 脅威インテリジェンス
定期的に情報資産に対するリスクアセスメントを実施し、適切な低減措置を講じることができるようにしています。

G) 情報及びその他の関連資産の目録
自社の情報および関連資産を特定し、情報セキュリティの観点からその重要性を判断するため、適切な管理責任を割り当て定期的に目録のレビューをしています。

H) 資産の返却
契約終了時は提供したサービス環境を削除し預託されたデータの消去証明書を発行します。解約申込書に記載されたサービス終了日の翌営業日にサービス環境の削除作業を実施します。環境を削除するとバックアップデータ以外の全ての保管データが削除されます。環境削除から 30 日経過するとバックアップデータが削除されます。

I) アクセス制御とアクセス権
情報へのアクセスは職務に従事する担当者個別に識別子（ID）を提供し許可された端末および経路のみに限定しています。またアクセス権限は役割・責任に応じた設定を行い、付与しています。

2. 人的管理策

A) 雇用条件
従業者には、預託された個人データ、および業務上の機密情報の非開示誓約書の提出を義務づけています。

B) 教育と訓練
個人情報保護および情報セキュリティに関する教育（E-ラーニング）を定期的に受講しています。

C) 懲戒手続
要員および関係者が情報セキュリティ方針に違反した場合の正式な手続きを規定に定めています。

3. 物理的管理策

A) 物理的入退室
情報を管理する建屋（室）には、入退室管理システムで常時施錠され、監視カメラにて入退室および作業状況を監視しています。

B) オフィス、部屋及び施設のセキュリティ
予め許可された関係者のみが入室を許可され入退室管理システムによりログを取得しています。

C) セキュリティを保つべき領域での作業
システムへアクセスする環境は、特定の作業関係者のみアクセスできるよう制限し、全ての操作ログを取得、第三者による操作ログのモニタリングを実施しています。

D) クリアデスク・クリアスクリーン
執務室およびシステムへアクセスする作業エリアでは、机上またはスクリーン上に認可されていない情報を放置することを禁止し定期的な監査を行っています。

E) ストレージメディア
業務で使用するUSBやモバイル機器は、施錠付きロッカーまたはキャビネットに保管され、使用時には管理台帳に記録し入出庫管理をしています。また使用できる USB は予め登録された個体のみアクセスできるよう制限をしています。

F) クラウドサービスのストレージ
クラウドサービスで使用している HDD 等のストレージは、使用終了後にはクラウドサービス提供者の責任において、安全に廃棄されることを書面により確認しています。

4. 技術的管理策

A) 特権的アクセス権
許可された要員にのみ特権 ID は提供され、必要な作業時に許可された手順に従い使用される。

B) 情報へのアクセス制限
情報資産へのアクセスは、予め決められた利用者 ID で許可された端末および限定されたアクセス経路からのみ許可されます。また RDP サーバを介してのアクセスとなり利用者 ID と端末情報の多重認証を行っています。

C) マルウェアに対する保護
使用するすべての端末およびサーバにウィルス対策ソフトを導入し、ウィルス感染の予防・駆除を実施しています。またシステムへのソフトウェアの導入は変更管理に基づき実施されています。

D) 技術的脆弱性の管理
IPA などで公開される脆弱性情報をモニタリングし適宜リスクを評価しています。修正が必要な場合は、合理的な判断をして適切に対応しています。

E) 不正アクセスの防止
ネットワーク上に WAF を導入し、不正アクセスを監視・検知および防御しています。
検知結果は 24 時間 365 日検知できる体制を敷いています。

F) 情報のバックアップ
データの消失やシステムの復旧を可能にするため、バックアップ方針に基づき定期的にバックアップを取得し保全を図っています。
*顧客預託データ/操作ログ:30 世代（日）保持、毎日 0 時にローテートして古いものを削除
*アクセスログ　　：1 年保持、毎週 3 時にローテートして古いものを削除
*システムログ　　：1 か月保持、毎週 3 時にローテートして古いものを削除

G) 情報の保管
預託されたデータについては、日本国内のデータセンターにて保管しています。サービス環境の増強等を実施する場合も、日本国内のデータセンターを選択いたします。

H) 情報処理施設の冗長性
可用性の高いサービス提供を行うため、東日本および西日本のデータセンターにて冗長構成を構築しデータを保管しています。両データセンターは「データセンターファシリティスタンダード（日本データセンター協会）ティア３認定を受け、耐震性・継続性・セキュリティ等も基準を満足しています。

I) 監視活動
ネットワーク、システムおよびアプリケーションについて異常がないか監視し、適切に対処しています。

J) 脆弱性診断
外部の診断業者による定期的なアプリケーションおよびペネトレーションテストを実施し、指摘事項について必要なタイミングで対処しています。

K) 開発手順
適用している情報セキュリティ方針に配慮した開発手順での開発を実践しています。

L) 時刻情報の管理
NTP サーバとの同期については、1 分以内の間隔で NTP サーバへポーリングし、ずれがあった場合に正しい時刻に修正をします。同期をしている先は CentOS が提供する NTP サーバとなります。

M) ログの保全
アクセスログは 1 年間、システムログは 1 か月間保持し保全しています。ログへのアクセ

ス制御は「B)情報へのアクセス」と同様の管理策を実施しております。

N) 暗号の利用

通信の暗号化については TLS1.2 を利用しています。また、パスワードについてはハッシュ化して保存しています。

(エ) 契約者への通知/問い合わせ

1. 契約者への通知（セキュリティインシデント）

預託されたデータの漏洩や改ざんの疑いなど情報セキュリティに係るインシデント、ならびに、サービス利用に著しい影響がある障害発生を認知した場合には、速やかに契約者へ通知を行う体制を構築しております。

弊社がインシデントや障害を認知してから 72 時間以内を目標とし、契約者の運用担当者へ対してメール/電話/サポートサイトへの情報掲載などいずれかの通知手段を用いて通知を行います。また、情報セキュリティ事象の解決に時間を要する場合は、7 日間に 1 回以上を目安として途中経過についての通知を行います。

2. 契約者への通知（メンテナンス）

計画メンテナンスについて、作業時にサービス利用影響が発生する場合、もしくは、サービスの操作・機能に変更が生じる場合には、作業日の 1 か月前までを目途に、作業日時や変更内容の通知を行います。通知手段は契約者の運用担当者に対してメール/サポートサイトへの情報掲載などのいずれかの手段を用います。ただし、サービスの可用性と安全性確保のために弊社にて早急に実施すべき作業と判断した場合には、臨時メンテナンスとして作業日の直前の通知となること、または、事前の通知なく作業することがあります。

3. 契約者からの問い合わせ

契約者にて本サービスに係る情報セキュリティ事象が発生した場合、ならびに、障害発生が疑われる事象を検知した場合には、当社の下記問い合わせ先へ連絡・報告を行うことができます。

＜インフォコム株式会社　BCPortal サポートデスク＞

メール：bcportal-support@infocom.co.jp

電話：　0570-024-119

※情報セキュリティインシデント・障害連絡の受付：24 時間受付

2026 年 1 月 7 日更新

インフォコム株式会社
エンタープライズサービス事業本部
システムソリューション事業部門
デジタル・サステナビリティ事業部