BtoB プラットフォーム

セキュリティホワイトペーパー

株式会社インフォマート

目次

1　はじめに

本資料は、BtoB プラットフォームのご利用を検討されている企業様、または既にご利用いただいている企業様に向けて、BtoB プラットフォームのセキュリティ対策への取り組みについてご確認いただくとともに、BtoB プラットフォームをより安心・安全にご利用いただくための留意事項をご確認いただくことを目的としております。

2　セキュリティ対策

2-1　不正アクセス対策

2-1-1　ネットワーク

2-1-1-1　ファイアウォール

ファイアウォールはシステムを不正なアクセスから守るための装置です。
ファイアウォールにて必要最小限のポートのみを許可し、不正な探査やポートスキャンに対する対策を講じています。

2-1-1-2　IPS

IPS（Intrusion Prevention System）は、侵入防止システムと呼ばれ、システムへの不正な侵入を検知し、ブロックするシステムです。
シグネチャの更新は内容を確認し、週次で適用しています。また、緊急の場合は日次で適用しています。

2-1-1-3　WAF

WAF（Web Application Firewall）は、Web アプリケーションの脆弱性を悪用した攻撃から Web サイトを保護するセキュリティ対策です。
IPS と同様に、不正なアクセスを検知し、ブロックします。
シグネチャの更新は内容を確認し、週次で適用しています。また、緊急の場合は日次で適用しています。

2-1-1-4　DoS 攻撃対策

DoS 攻撃とは Denial of Service attack のことでサービス不能攻撃とも呼ばれています。サーバなどに負荷をかけてサービスを停止させる攻撃のことになります。
一定時間内に一定回数以上の同一 IP によるアクセスがあった場合にブロックし、アラートが送られる仕組みを構築しています。

2-1-2　サーバ

2-1-2-1　ウイルス対策

ウイルス対策ソフトを導入し、毎日最新のウイルス検出パターンファイルに更新することにより、ウイルス感染を未然に防止しています。
ウイルススキャンはリアルタイムスキャンおよび週次でのフルスキャンを行っています。

2-1-2-2 不要なサービスの停止

サーバの用途に応じて必要のないサービスを停止し、サーバの要塞化を図っています。

2-1-3 アプリケーション

2-1-3-1 セキュアコーディング

各種脆弱性に対応するため、入力値のサニタイジングやパラメータチェック、SQL 作成時のプレースホルダ利用などを開発規約として規定し、遵守しています。

2-1-4 脆弱性対策

2-1-4-1 パッチ適用

セキュリティパッチについて、サービスへの影響や緊急度を確認のうえ、原則月次にて適用を行います。
セキュリティパッチの適用状況については一覧表を作成し、適用記録を管理しています。
また、緊急の脆弱性が公表された場合のプロセスが明確化されており、影響や緊急度を確認し、速やかに対応を行います。

2-1-4-2 脆弱性診断

脆弱性検査については、第三者機関による脆弱性診断を行い、ネットワーク診断（ポートスキャンなどネットワーク層の診断）は日次で実施し、アプリケーション診断（XSS、SQL インジェクションなど）を週次で実施しています。
脆弱性診断の実施および情報の収集を行い、脆弱性が発見された場合には、サービスへの影響や緊急度から優先順位付けを行い、順次対応を行います。対応に伴い、お客様に影響のある変更を行う場合は、サイト内にて告知を行います。
また、お客様による脆弱性診断は禁止としています。

2-2 暗号化

2-2-1 CRYPTREC 暗号リスト

総務省及び経済産業省にて、電子政府で利用される暗号技術の評価を行っており、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」を策定しています。
暗号化を行う際は、このリストに基づいた暗号化方式によって暗号化を実施しています。

2-2-2 通信内容

2-2-2-1 EV-SSL 証明書を取得

EV-SSL 証明書とは、Web サイトの証明書として最も厳格な基準であり、運営元企業の法的、物理的な実在証明を必要とした証明書です。
全画面 HTTPS 化され、常時 SSL による暗号化通信を実施しています。

2-2-2-2 TLS1.2 未満の通信無効化

SSL3.0、TLS1.0、TLS1.1 といった脆弱性が存在する古いプロトコルの使用を禁止するため、
TLS1.2 未満の通信はエラーとして処理しています。

2-2-3 データ

2-2-3-1 機密情報の暗号化

パスワード等の機密情報については、暗号化して保存しています。

2-2-4 ハードディスク

2-2-4-1 ストレージシステム

ストレージシステムによりハードディスク全体のデータを暗号化しています。

2-3 物理的セキュリティ

2-3-1 オフィス・執務室

業務を行うオフィスでは入室時に非接触 IC カードによる認証を行っています。
また、執務室とセキュリティエリアの区画は分離され、荷物の受渡等によりセキュリティエリアに立ち入ることができないよう管理しています。

2-3-2 データセンター

BtoB プラットフォームのサービスはデータセンター事業者のホスティングサービスを利用しており、サーバおよびネットワークの管理を委託しています。
委託先とは秘密保持契約および SLA を締結し、安全管理措置について月次報告会にて確認を行うなど、適切に管理しています。
サーバはデータセンター内の施錠ラックに設置され厳重に管理しています。

2-3-2-1 入退室管理

非接触 IC カードおよび生体認証にて入退室管理を実施し、記録は 3 年間保存しています。

2-3-2-2 監視カメラ

24 時間かつ全範囲を網羅する監視カメラを配置し、90 日間のデジタル録画を保存しています。

2-3-2-3 24 時間有人監視

24 時間 365 日の有人監視で不測の事態に備えています。

2-4 ユーザー側管理機能

2-4-1 権限設定

管理者権限を有するユーザーにて、利用者 ID（社員）の追加・削除や権限設定が可能です。
利用者毎に利用できる機能やアクセスできる画面を制限可能です。

2-4-2 シングルサインオン

SAML 認証や OpenIDConnect を使用したシングルサインオンに対応しています。

2-5　セキュリティ強化オプション

企業様のセキュリティポリシーに対応できるよう、セキュリティを強化するためのオプションをご用意しております。但し、これらの機能は、プラットフォーム ID をご利用の企業様に限ります。また、無料会員様においてはご利用いただけない機能がございます。

2-5-1　パスワード有効期限

任意の日数で、パスワードの有効期限を設定することが可能です。

2-5-2　セッションタイムアウト

セッションタイムアウト機能を備えており、ログイン後、一定時間操作が行われなかった場合に自動ログアウトします。

機能の ON/OFF、セッションタイムアウトまでの時間の設定が可能となっています。

2-5-3　アカウントロック

一定時間内に連続してパスワードを間違えた場合、一定時間アカウントをロックします。

ロック時間やロックまでの回数について変更が可能となっています。

2-5-4　IP アクセス制限

接続元グローバル IP アドレスによる接続制限が可能です。

2-6　パスワードポリシー

パスワードは 8 桁以上 15 桁以下かつ、英大文字、英小文字、数字、記号から 3 種類以上を設定することが必須となっています。

3　運用体制

3-1　監視

3-1-1　24 時間 365 日

システムを安定稼働させるため、24 時間 365 日の監視を行っています。

3-1-2　有人監視

有事の際に対応できるよう、有人監視を行っています。

3-1-3　監視内容（死活監視、リソース）、監視間隔

ハードウェア、ミドルウェア、アプリケーションなど、お客様のご利用に影響にあるものは全て監視対象としています。

また、各監視の間隔は以下の通りとなります。異常を検知した場合はアラート通知される仕組みを構築しています。
・機器死活監視：1 分
・サービス稼働監視：1 分
・システムリソース監視：1 秒

3-2　運用環境

3-2-1　閉域網

インターネットとは分離された専用の閉域網にてデータセンターと接続しています。
閉域網を使用し、システムの運用を行っています。

3-2-2　専用 PC

インターネットへアクセスすることができない専用 PC からのみデータセンターへアクセス可能となっています。
専用 PC はすべての操作ログを取得し作業内容を管理しています。

3-2-3　権限管理

サーバ操作は、弊社情報セキュリティ管理責任者が承認した社員のみが可能であり、閉域網・専用 PC を利用したリモートアクセスにて行います。

3-3　ログの取得について

システムログや操作ログ、アクセスログなど各種ログを取得し、一定期間保存しています。

3-4　特権 ID について

データへのアクセスは弊社の情報セキュリティ管理責任者が承認した社員のみに権限を付与しております。

4　災害対策/障害対策

4-1　データセンター

利用しているデータセンターは、データセンターファシリティスタンダード Tier3 相当となっています。

4-1-1　UPS・発電機

受電構造の冗長化（スポットネットワーク方式）および、UPS、非常用発電機装置を配備しています。
UPS のバッテリー保持時間は 90 分、
非常用発電設備は常備燃料で 20 時間以上の電力供給可能であり、燃料補給を行うことにより継続して電源供給可能です。

4-1-2 空調設備

床置型空冷式 CRAC ユニット（N+2 冗長構成）を配備しています。

4-1-3 消火設備

防火対策としてガス消火設備（ハロン 1301 消火設備）、高温度検知装置、VESDA（早期高感度煙感知）を備えています。

4-1-4 地震対策

耐震構造（震度 7 クラス対応）、耐震架台にボルト固定したラックにサーバを固定設置しています。

4-1-5 水害対策

浸水予想 50cm 未満地域に位置し、さらに高層階への設置および屋上防水措置がとられています。

4-2 障害対策

4-2-1 冗長化

全てのネットワーク機器やサーバ、アプリケーション、回線は冗長構成で設計されているため、一部の障害が全体に影響しないような構成となっています。

4-2-2 リソース拡張

システムリソースの利用傾向を分析の上、適宜スケールアップやスケールアウトを行っています。

4-2-3 対応フローの整備

システム障害を想定した対応手順書や、対応フロー、体制、連絡網などを整備しており、定期的な訓練および見直しを行っております。

4-3 データバックアップ

4-3-1 取得種別

データベースやアプリケーションを含むシステム全体のバックアップを取得しています。

4-3-2 取得間隔

日次で差分バックアップを取得、月次にてフルバックアップを取得しています。

4-3-3 保持期間

バックアップの保持期間は 6 か月です。

4-3-4 遠隔地保存

取得したバックアップは国内遠隔地にて保管しており、正常にリストアできることを定期的に確認しています。遠隔地での保管についても、データセンターにて厳重に管理・保管しています。

5 コンプライアンス

5-1 認証

5-1-1 ISMS

ISMS（Information Security Management System）は情報セキュリティマネジメントシステムと呼ばれ、組織における情報資産のセキュリティを管理するための枠組みです。
ISMS の認証(ISO/IEC 27001:2013)を取得し、すべての従業員への教育・管理を徹底しています。規定した ISMS に則り、大規模障害時を想定した訓練を定期的に実施しております。

5-1-2 クラウドサービス認定

クラウドサービス認定は、一般社団法人クラウドサービス推進機構がクラウドを活用した IT 経営の促進を目指し、中小企業の経営者が安全にかつ安心して継続的に利用できるクラウドサービスであることを認定するプログラムです。BtoB プラットフォームはクラウドサービス認定を取得しています。

5-1-3 情報開示認定

情報開示認定制度は、クラウドサービス事業者が安全・信頼性に係る情報を適切に開示している事を第 3 者が認定し、同一フォーマットで公開することにより、クラウドサービス利用者のサービス比較、評価、選択を支援し安全性向上を目指す制度です。
BtoB プラットフォームは ASP・SaaS の安全・信頼性に係る情報開示認定を取得しています。
以下の URL より開示内容を確認することができます。
https://www.aspicjapan.org/nintei/files/1ec4daadda149c8a.pdf

5-2 準拠法

データセンターは国内に位置し、日本の法律に準拠します。

6　改訂履歴

版数	日付	改訂内容
初版	2020/9/24	初版発行
第 1.1 版	2020/11/11	書式および文章の重複箇所を修正