MCRコンソーシアム参加団体向け

My City Report for citizens

情報セキュリティ対策

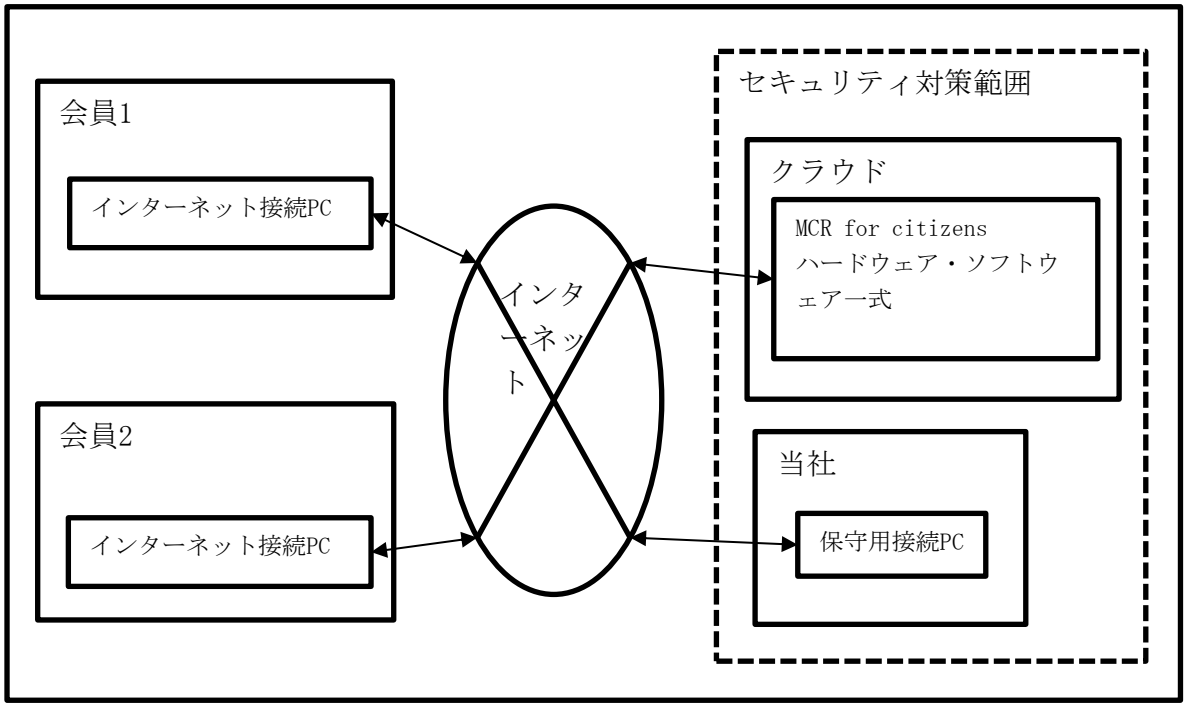
2020/4/1 初版

合同会社Georepublic Japan

ー目次ー

1 本書の適用範囲

本書の情報セキュリティ対策は下図の破線部分に適用するものです。会員とはコンソーシアム会員を指します。



MCR for citizensシステムはクラウド上に構築され、複数のお客様（自治体・団体）に共同でご利用いただく形式です。そのハードウェア及びソフトウェアに対しては当社が一元的にセキュリティ対策の立案と実施を行います。なお、サーバーはAWSの東京リージョンのサーバー（ISO/IEC27001及びISO/IEC27017認証を取得済み（https://aws.amazon.com/jp/compliance/iso-27001-faqs/））を使用しており、そちらのセキュリティ対策も併せて実施されます。

2 My City Report for citizens の情報セキュリティ方針

My City Report for citizensで提供されるサービスは、お客様に安心して快適にご利用頂けるよう以下の情報セキュリティ対策を定め、運用しています。

2.1 用語の定義

機密性・完全性・可用性については、下記の通り定義します。

・機密性：認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性

・完全性：資産の正確さ及び完全さを保護する特性

・可用性：認可されたエンティティが要求したときに、アクセス及び使用が可能である特性

2.2 本サービスで取り扱う情報資産

自治体住民の下記情報を取り扱います。

・氏名

・電話番号

・メールアドレス

・住所（任意）

・誕生年（任意）

・性別（任意）

・職業（任意）

2.3 機密性の保持

（1） ファイアウォールを設置してインターネットからの直接アクセスをできないようにし、不正アクセスを防ぎます。アクセスする際は、下記（2）に記述の通りVPN経由でSSHで暗号化された経路のみが利用可能で、それ以外は遮断します。この経路でサーバーOSにログイン後に初めてデータベースにアクセス可能となりま

す。データベースについてはローカルセグメントに設置します。ログについてはALB（ファイアウォール、ルーター機能を兼ねるロードバランサ）で５分に一回取得し、内容は週次で確認します。ファイアウォールの脆弱性情報は日次でAWSのセキュリティ情報掲示板（https://aws.amazon.com/jp/security/security-bulletins/）を確認し、何らかの対応が必要な内容があれば対応します。

（２）　データベースにアクセスするポートはインターネットに向けては閉じられています。当社システム運営担当者がメンテナンスなどでサーバーOSにアクセスする場合には、踏み台サーバを介してVPN経由でのみアクセスできるように経路を制限し、SSHで暗号化された経路を使用してアクセスします。また、データベース接続のためのユーザーID、パスワードはシステム管理者が専用のものを発行します。その際、パスワードについては自動生成された10桁以上の強固なものを使用します。

（３）　ユーザー登録情報のうち、パスワードについてはハッシュ化して復号化を不可能にします。パスワード以外のユーザー登録情報については暗号化します。

（４）　開発に際してはセキュリティに十分配慮してSQLインジェクション等による不正アクセスを予防するとともに、メジャーリリース時には脆弱性検査（詳細は後述）を実施し、検査結果に対して適切な対処を行います。

（５）　システムの操作に関わるログを取得し、最低１年間は保管することで操作を追跡可能とします。異常操作ログを日次で監視し、必要に応じて手動でアカウントロックなどの対策を実施します

（６）　自治体・団体ユーザーはPCのブラウザからIDとパスワードにより認証を行います。パスワードについてはシステム管理者が自動生成された10桁以上の強固なものを初期設定し、自治体・団体ユーザーの初回ログイン時に、改めて任意のパスワードに変更してもらいます。パスワードを忘れた際には自治体・団体ユーザーユーザー自身の操作によりメールでリセット用のURLを入手してリセットすることができます。ログイン後、一定期間（期間を設定可能）操作をしない場合は、自動的にログアウトします。ログインに失敗した場合にはIDとパスワードのどちらが誤っているかが分からないエラーメッセージを表示します。認証された自治体・団体ユーザーは、予め取り決められた権限設定により、必要なレポートとユーザー情報にアクセスすることができます。その際、操作ログを取得し処理内容を追跡可能とします。

市民ユーザーはモバイル端末を用いてIDとパスワードにより、認証を行います。パスワードについては8桁以上の強固なものを使用します。IDと同じパスワードは設定しないようにユーザー登録画面で案内します。パスワードを忘れた際には市民ユーザー自身の操作によりメールでリセット用のURLを入手してリセットすることができます。ログインに失敗した場合にはIDとパスワードのどちらが誤っているかが分からないエラーメッセージを表示します。認証された市民ユーザーは、モバイル端末を用いて自身が投稿したレポート及び公開設定されたレポート、そして自身のユーザー情報だけにアクセスを限定されます。

MCRシステムへのアクセス権限は、ロール（部門管理者、市民など）と権限（参照のみ可、更新可など）の組み合わせで当社のシステム管理者が一元的に管理します。通常は初期設定後、変更することはありません。

サーバーOSへのアクセスについては上記（２）の通り当社のシステム管理者だけが踏み台サーバを介してVPNを経由する経路のみでログインします。

（７）　ネットワークセグメントは他社と分離されています。

（８）　データベースにアクセスするためのポートを閉じ、インターネット側からのアクセスを遮断します。ネットワークセグメントをWEB/APサーバ配置のDMZとデータベースサーバ配置のローカルセグメントは分離されています。

2.4 完全性の保持

OSについてはセキュリティ自動アップデート機能により、脆弱性のあるアプリケーション・ライブラリのアップデートを自動的に実施します。その他関連するライブラリなどで深刻な脆弱性が報告された場合にはアップデートを実施します。

アンチウィルスソフトのウィルスパターンファイルは月次で更新します。緊急時には月次以外にも別途対応します。

2.5 可用性の保持

AWSのCloudWatchサービス（参考：https://aws.amazon.com/jp/cloudwatch/）により、サーバ死活監視、リソース監視（ミドルウェア等の死活監視）、URL監視（ＷＥＢサイトへの接続可否）を行い、ダウン検知時、及びダウンからの復旧時にSlackで通知を受け、下記に定める障害時の対応手順に従い可及的且つ速やかに対応します。DBバックアップは深夜０時に行い、所定の手順でバックアップから復元できるよう対応しています。バックアップは、システム構成図の経路８に相当する「DBマスタ」からからのみアクセス可能なアベイラビリティーゾーン（https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/using-regions-availability-zones.html）に10世代保持しています。

バッチジョブは現在ありません。

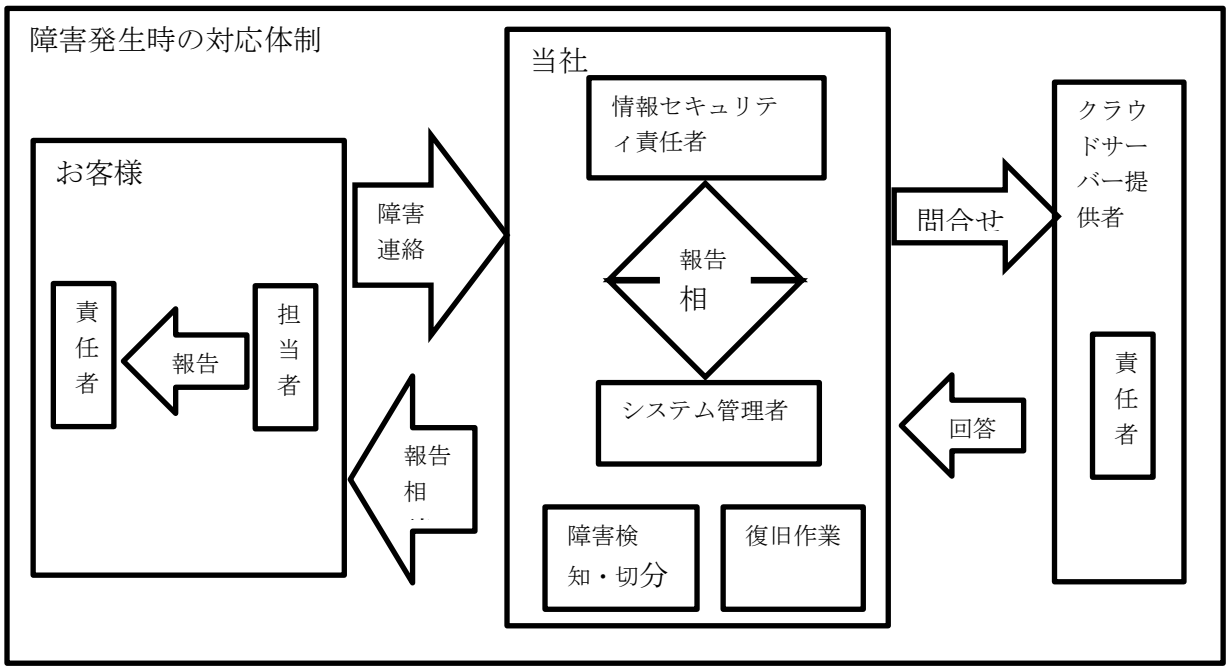
サーバーアクセスログ、アプリケーションアクセスログ、監視ログを取得して保管し、異常を検知した際などに追跡可能にします。保存期間は特に区切っていませんが、肥大化が見られる場合にはメディアにバックアップの上、古いものを削除します。

障害発生時は原則として以下の体制・手順で対応します。

障害が発生した際は、障害原因の一次切り分けを行い、クラウド提供者と連携し、解決作業を検討して適切な対応を行います。障害については、即日復旧を原則とします。ただし、当日中の復旧が不可能な障害であると判断される場合には、ただちに当該自治体・団体へ報告し、その指示に従って対応します。また、障害復旧後は、障害の内容及び対応結果について、随時当該自治体・団体にウェブサイト（自治体・団体管理者向け管理画面）上または書面により報告します。

ウイルスに感染した場合については、ただちに感染物をネットワークから切り離し、ウイルスの除去等を行います。なお、復旧後は、ウイルスの内容、感染経路及び対応結果について、随時当該自治体・団体へウェブサイト（自治体・団体管理者向け管理画面）上または書面により報告します。

＜障害時の対応手順＞



事象	内容	会員	当社
障害発生	・サーバダウン ・アプリケーション異常終了 ・ネットワーク障害など	操作中に発見	監視サービスからの通知で発見
障害発見 連絡 自動検知	・障害アラーム受信、システムメッセージの受信など ・サポート窓口への連絡 ・監視サービスからの通知	○ →	 ○ ○
一次切り分け	・障害発生箇所の特定。 ・ログ、コンソールによる確認		○
障害対応支援	・お客様への状況報告 ・障害発生箇所を関連する担当者と連携して対応の指示、依頼を行う	○	← ○
暫定復旧	・直接原因の排除（データのパッチ、整合性修復等） ・プログラム修正/テスト、動作確認 ・システムの再起動		○
二次切り分け	・障害を再現し原因を特定 ・詳細ログの解析		○
完全復旧	・データ/環境の臨時バックアップ実施 ・プログラム、モジュール等の入替 ・環境定義変更 ・データ/環境リストアの実施 ・動作確認		○

2.6 その他

2.6.1 サービスの設計及び実装

お客様からの情報セキュリティ要求事項及び本方針を適用し、サービスの設計及び実装を行います。

2.6.2 会員データへの当社従業員によるアクセス及び保護

当社は、サービスの運営に必要な技術的な問題の解決のために、会員のデータにアクセスすることがあります。

それ以外の目的では会員の事前の許可なくアクセス致しません。

2.6.3 会員への変更通知

サービスに関する仕様変更等については、MCRホームページへの掲載等を通じて情報提供いたします。

2.6.4 会員でのパスワード管理等について

会員でパスワードを管理する際には当社での対策以外に下記のような対策をされることを推奨します。（参考「総務省：パスワード設定と管理のあり方」https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01-2.html）

（1）安全なパスワードの設定

桁数を10桁以上にする、英字、英記号、数字などを組合わせる、自動生成するなどの対策により強固なパスワードを作成、設定する。

（2）パスワードの管理

パスワードをメールでやりとりしない、人目に触れる場所に貼ったりしない、メモする場合は施錠された場所に保管する、といった対策を行う。

（3）パスワード使い回しの回避

同じパスワードを別のシステムやサービスで使い回ししない、パスワードの先頭にシステムの識別子を付加する、といった対策をおこなう。

3 脆弱性対応方針

脆弱性検査ツール「OWASP ZAP」の最新リリースを用いて、メジャーバージョンアップのタイミングで検査を行い、脆弱性が発見された場合には深刻度に応じて必要な対策を行います。

以下に「OWASP ZAP」にて行う脆弱性診断の概略を示します。

分類	診断名
インジェクション	書式文字列エラー
	リモート OSコマンドインジェクション
	パラメータ改ざん
	バッファ オーバーフロー
	クロスサイト・スクリプティング(反射型)
	クロスサイト・スクリプティング(持続型) ー スパイダー
	クロスサイト・スクリプティング(持続型) ー Prime
	クロスサイト・スクリプティング(持続型)
	SQL インジェクション
	Server Side Include
	Server Side Code Injection
	CRLF インジェクション
サーバ・セキュリティ	パス トラバーサル
	リモート ファイル インクルージョン
一般	Script Active Scan Rules
	外部リダイレクト
情報収集	Source Code Disclosure - /WEB-INF folder
	ディレクトリ部ライジング

診断結果については下記方針で対応します。

・深刻度がHighのもの：可及的速やかに対応する。

・深刻度がMediumのもの：内容を調査し、重大性・緊急性を勘案して対応を決定する。

・深刻度のLowのもの：内容は確認するが、基本的に対応はしない。ただし簡易に対応できる場合は対応することがある。

以上