情報セキュリティホワイトペーパー

2024 年 2 月 13 日

株式会社オプティマインド

1 はじめに 2

2 参考文献 2

3 情報セキュリティにおける組織的な取り組み 3

3.1 情報セキュリティ方針 ---------- 3

3.2 情報セキュリティ組織と情報セキュリティ管理 ---------- 4

3.3 業務に使用される PC デバイス類にかかる情報セキュリティ ---------- 5

3.4 サプライチェーン管理：委託先管理 ---------- 6

3.5 情報資産管理 ---------- 6

3.6 従業員にかかる情報セキュリティ ---------- 6

3.7 情報セキュリティインシデントの管理 ---------- 6

4 Loogia 7

4.1 Loogia について ---------- 7

4.2 Loogia システムについて ---------- 8

5 【参考】Loogia のウェブセキュリティについて 10

6 問い合わせ先 12

1 はじめに

情報セキュリティホワイトペーパー（以下、本書）は、当社の情報セキュリティに対する取り組みを共有させていただくことで、お客様にご安心して当社サービスをご利用いただくことを目的としています。

加えて、当社が提供するクラウドサービス Loogia（ルージア）についてお客様における情報セキュリティポリシとの合致を確認いただけることも目的のひとつです。

本書は以下にて構成されております。

章	題名	概要
1	はじめに	本章に該当します
2	参考文献	本書作成にあたり参考とさせていただいた文献やドキュメントを記載しています
3	情報セキュリティにおける組織的な取り組み	当社の組織的な情報セキュリティに対する取り組みを記載しています
4	Loogia	当社サービスである Loogia にかかる情報セキュリティや可用性について記載しています
5	【参考】Loogia のウェブセキュリティについて	当社サービスである Loogia のウェブセキュリティ対応状況について記載しています
6	問い合わせ先	本書についての問い合わせ先を記載しています

なお本書の改定につきましては、必要性に応じ随時行っていく予定です。

2 参考文献

- 総務省．クラウドサービス提供における 情報セキュリティ対策ガイドライン （第３版）,2021 年 9 月
- IPA．安全なウェブサイトの作り方 改訂第７版, 2021 年 3 月

3 情報セキュリティにおける組織的な取り組み

3.1 情報セキュリティ方針

当社は、当社の情報資産、並びにお客様からお預かりした情報資産を事故・災害・犯罪 などの脅威から守り、お客様ならびに社会の信頼に応えるべく、情報セキュリティ方針に基づき全社で情報セキュリティに取り組んでいます。

当社は情報セキュリティ方針を定めており、当社ホームページにて公開をしています。

https://www.optimind.tech/security/

さらに当社では ISMS[1]の国際標準規格である ISO/IEC 27001[2]の認証取得をしており、第三者の観点からも適切な情報セキュリティ管理がなされているといえます。

また、個人情報の取り扱いについては、プライバシーポリシーを定めており、同様に当社ホームページにて公開しています。

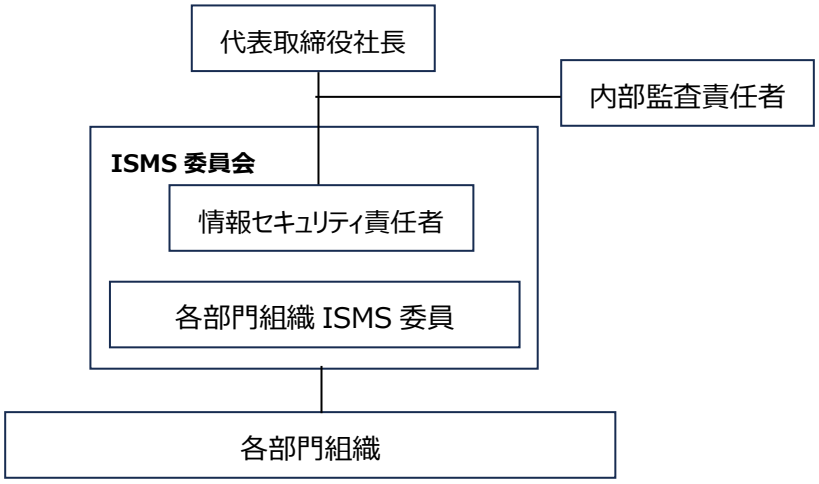
https://www.optimind.tech/privacy/

[1] Information Security Management System の略称。日本語では情報セキュリティマネジメントのことであり、情報セキュリティリスクを管理する仕組みを指す。

[2] 国際標準化機構（ISO）と国際電気標準会議（IEC）によって共同で開発された ISMS に関する国際標準規格

3.2 情報セキュリティ組織と情報セキュリティ管理

当社の情報セキュリティ組織は下図のように構成されています。情報セキュリティにかかる各種判断や連絡・指示・協力等が適切に行われる仕組みとなっています。組織に ISMS を取り込むことで、情報セキュリティ管理と一体運営がなされています。

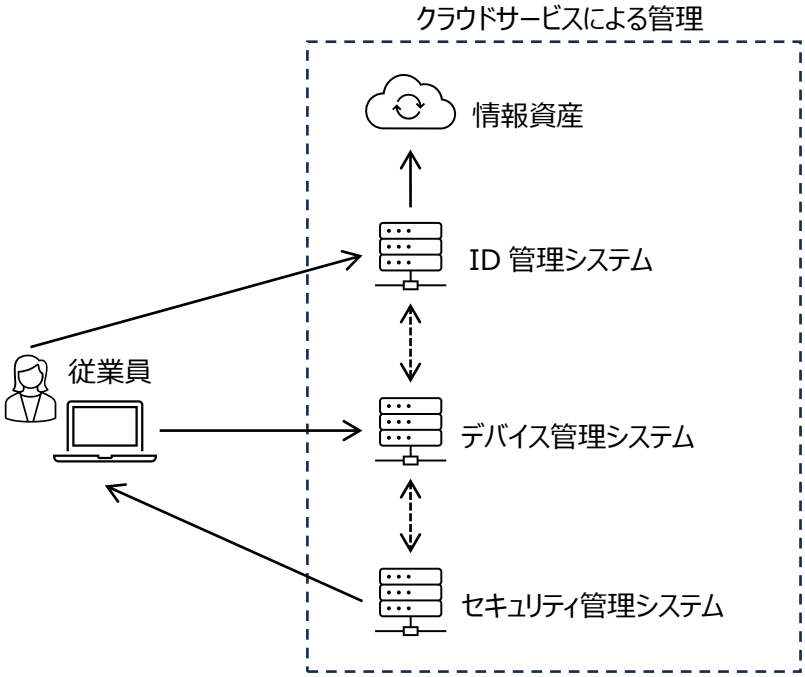


当社の情報セキュリティ管理は、ISO/IEC 27001 に準拠した ISMS（情報セキュリティマネジメントシステム）によって運営されています。ISMS 委員会によって以下の内容について運営されています。

- セキュリティリスクの洗い出しと管理
- セキュリティリスクの優先付け及び対応
- セキュリティにかかるルールづくり
- セキュリティルールが守られているかの確認
- 情報セキュリティにかかる社内発信と従業員の理解促進

3.3 業務に使用される PC デバイス類にかかる情報セキュリティ

当社の従業員は、オフィス勤務やテレワーク等に様々な場所で勤務しています。そのため、図のようにクラウドサービスを中心とした情報セキュリティにかかる管理システムを導入運用しています。



従業員は ID 管理システムにログインする際に、ログイン認証を通過しないとそもそも重要な情報資産へのアクセスが認可されません。また、各情報資産へのアクセス認可は、資産内容や利用用途の観点からアクセス可能な従業員のみに制限されています。なお、なりすまし防止等の目的から、ID 管理システムへのログインは多要素認証が適用されています。

またデバイス管理システムによって PC を管理することで、PC 内データの強制暗号化、外部媒体経由や PC 紛失盗難時の情報漏えい防止を統合的に実現しています。

さらに、セキュリティ管理システムにより PC へのマルウェア混入防止、ソフトウェア脆弱性の監視と対応、危殆ウェブサイトへのアクセス禁止等のセキュリティ施策を実現しています。

3.4 サプライチェーン管理：委託先管理

当社は、以下例のような様々なサプライヤや業務委託社（者）の協力をいただきながら事業を運営しています。

- 開発業務委託
- パブリッククラウド
- クラウドサービス
- 専門家や士業

サプライヤや業務委託社（者）との取引開始時には、通常の契約締結のほか、モニタリングを行うことでサプライチェーンの情報セキュリティ管理を実施しています。

3.5 情報資産管理

当社では、台帳を作成管理することで情報資産管理を行っています。個々の情報について管理責任者が決められており、特定の社員が特定の情報資産のみへのアクセス可能な管理がなされています。

3.6 従業員にかかる情報セキュリティ

情報セキュリティ確保において、従業員の理解と行動は重要な要件の 1 つと考えます。
当社では、従業員の理解と適正な行動を促すため、それぞれのプロセスにおける施策を実施しています。

雇用前：秘密保持を含む情報セキュリティにかかる契約を行うことで、従業員への説明と合意形成
雇用期間中：情報セキュリティに関する教育を全員が受講
雇用終了時
：対象者と退職後の当社情報にかかる秘密保持契約を締結、情報資産の返却や ID 等のアカウント削除

なお、情報漏えい等の違反が発生した場合の手続きについては、就業規則に記載されており、情報セキュリティへの意識向上も図っています。

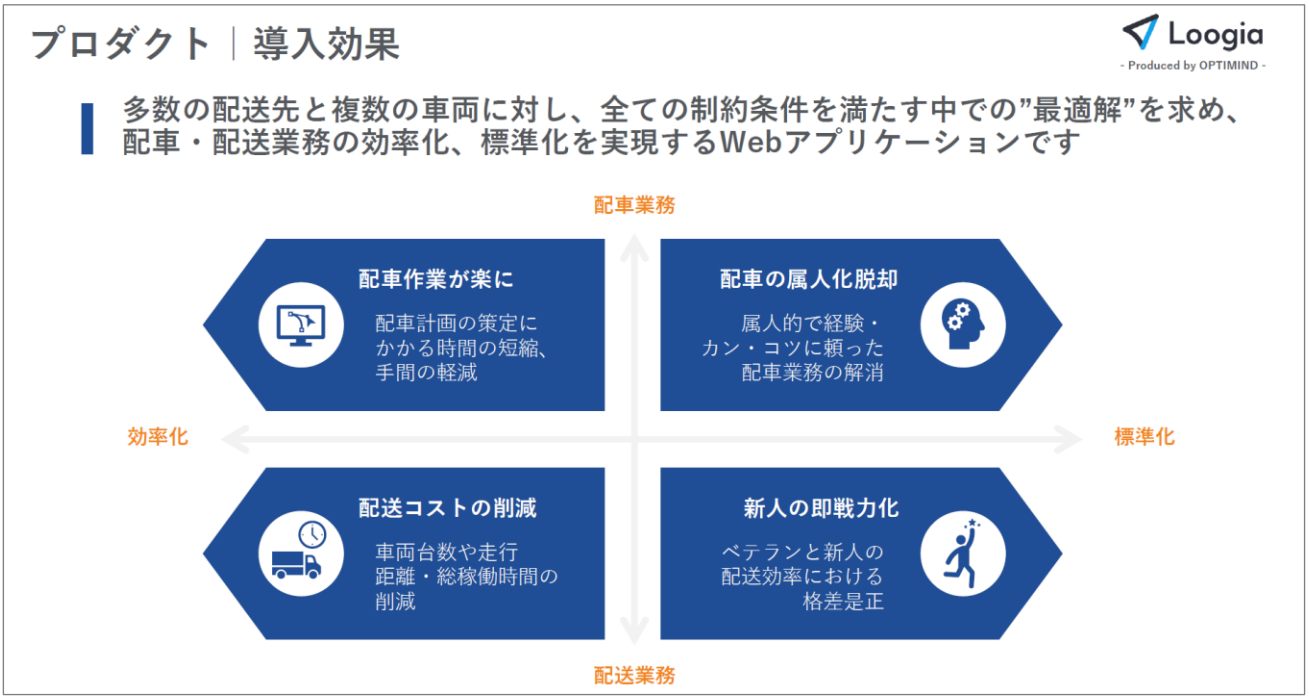
3.7 情報セキュリティインシデントの管理

情報セキュリティインシデントについては、発生状況から是正及びその確認まで ISMS 委員会にてトレース管理されています。また、当社ではインシデントまでに至らないケースを観察事項として管理し、改善の機会と捉え同様に是正を行っています。

4 Loogia

4.1 Loogia について

当社が提供している Loogia は、誰でも最適で高精度な配車計画・配送ルートを作成できる「自動配車クラウド」です。また Loogia を利用することで、総効率の向上による働き方改革、コスト削減、環境負荷の低減などに繋がります。



4.2 Loogia システムについて

サービス運用時間

原則として 24 時間 365 日提供いたします。なお、保守作業のために一時的にサービス停止をすることがありますが、緊急時を除き事前にお客様へ通知をします。

障害監視

24 時間 365 日の監視を行っております。主な監視項目は以下になります。

- 各種エンドポイントに対する定期的なリクエスト送信
- サーバーリソース（CPU やメモリなど）の使用量
- 異常なログの有無

なお、システムの異常検知は自動ですぐに運用担当チームへ通知され、迅速な対応をチームにて実施します。

脆弱性診断

Loogia システムは、最低でも年一度の外部第三者機関による脆弱性診断を受診しています。検知した脆弱性については重要度に応じて適切な措置をしています。

暗号化

Loogia システムとの通信はすべて TLS 方式にて暗号化されています。

Loogia はお客さまにて様々なデータを入力いただき最適な配車結果を提供します。その際に入力いただいたデータは 256bit AES で暗号化されており、通信の盗聴や物理的なデータストレージの盗難がされたとしてもデータ開示はされません。

リリース運用

Loogia システムでは、機能追加やセキュリティ対策を含めた性能向上にかかるリリースを随時行っており、最も微細なケースでは週に数回のペースでアップデートされます。

リリースは計画にしたがって実行されます。仕様を満たしていることや既存機能への影響が無いことを事前テストによって十分に確認をしています。またリリース時における不測の不具合発生や脆弱性検知の際は、緊急度に応じてロールバック（リリース前バージョンへの巻き戻し）や修正適用を迅速に行います。

なお、Loogia システム環境は、開発環境と本番環境が完全に分離されています。開発環境で十分にテストされた内容のみが本番環境へリリースされる運用としています。また本番環境は必要最低限の社員のみがアクセスできるように制御されており内部からの悪意ある侵入から防御されています。

サービスの信頼性/柔軟性/可用性

Loogia システムは AWS や GCP 等のパブリッククラウド環境上に、実績あるベストプラクティスをベースに設計構築運用されています。冗長構成や自動回復の機構を具備することで、災害や障害発生時のサービス影響を最小限とすることでサービスが維持されるようにしています。

ソースコードはすべて Git で管理しており、変更履歴の保存や多重バックアップによるソースコードの保存管理をしています。万一、大規模災害等によって想定を上回るインフラ停止に見舞われても、インフラ復旧と同時にサービス復元が可能な設計をしています。

Loogia は共通インフラの上にマルチテナント方式にて様々なお客様にサービス提供をしている形態になります。一部のお客様における利用負荷の上昇が他のお客様へ影響を与えないために自動でインフラリソースを増強する設計になっています。また、負荷試験にて検証することで設計品質を確保しています。

5 【参考】Loogia のウェブセキュリティについて

当社提供のクラウドサービスである Loogia は、セキュリティ確保の観点からウェブセキュリティ診断を定期的に行っております。

IPA（独立行政法人　情報処理推進機構）が公開されています「セキュリティ実装チェックリスト」における Loogia の対応について記載いたします。基本的には、緑網掛け項目の根本的解決にて対応（不要なものは対応不要）をしています。加えて、一部保険的対策を実施している項目もあります。

なお、IPA が公開している「安全なウェブサイトの作り方」および「セキュリティ実装チェックリスト」については、以下に詳細があります。

https://www.ipa.go.jp/security/vuln/websecurity/about.html

■ ウェブアプリケーションのセキュリティ実装 チェックリスト （1/3）

No	脆弱性の種類	対策の性質	チェック	実施項目	補足	解説
1	SQLインジェクション	**根本的解決**	※ ☑対応済 □ 未対策 □ 対応不要	☑ **SQL文の組み立ては全てプレースホルダで実装する。**		1-(i)-a
				☑ **SQL文の構成を文字列連結により行う場合は、アプリケーションの変数をSQL文のリテラルとして正しく構成する。**		1-(i)-b
		根本的解決	☑対応済 □ 未対策 □ 対応不要	**ウェブアプリケーションに渡されるパラメータにSQL文を直接指定しない。**		1-(ii)
		保険的対策	☑対応済 □ 未対策 □ 対応不要	エラーメッセージをそのままブラウザに表示しない。	根本的解決の対応済み	1-(iii)
		保険的対策	□ 対応済 □ 未対策 ☑対応不要	データベースアカウントに適切な権限を与える。	根本的解決の対応済み	1-(iv)
2	OSコマンド・インジェクション	**根本的解決**	☑対応済 □ 未対策 □ 対応不要	☑ **シェルを起動できる言語機能の利用を避ける。**		2-(i)
		保険的対策	□ 対応済 □ 未対策 ☑対応不要	□ シェルを起動できる言語機能を利用する場合は、その引数を構成する全ての変数に対してチェックを行い、あらかじめ許可した処理のみを実行する。	根本的解決の対応済み	2-(ii)
3	パス名パラメータの未チェック／ディレクトリ・トラバーサル	**根本的解決**	※ ☑対応済 □ 未対策 □ 対応不要	☑ **外部からのパラメータでウェブサーバ内のファイル名を直接指定する実装を避ける。**		3-(i)-a
				☑ **ファイルを開く際は、固定のディレクトリを指定し、かつファイル名にディレクトリ名が含まれないようにする。**		3-(i)-b
		保険的対策	□ 対応済 □ 未対策 ☑対応不要	ウェブサーバ内のファイルへのアクセス権限の設定を正しく管理する。	根本的解決の対応済み	3-(ii)
		保険的対策	□ 対応済 □ 未対策 ☑対応不要	ファイル名のチェックを行う。	根本的解決の対応済み	3-(iii)
4	セッション管理の不備	**根本的解決**	□ 対応済 □ 未対策 ☑対応不要	**セッションIDを推測が困難なものにする。**	セッションを使っていないため	4-(i)
		根本的解決	□ 対応済 □ 未対策 ☑対応不要	**セッションIDをURLパラメータに格納しない。**	セッションを使っていないため	4-(ii)
		根本的解決	□ 対応済 □ 未対策 ☑対応不要	**HTTPS通信で利用するCookieにはsecure属性を加える。**	セッションを使っていないため	4-(iii)
		根本的解決	※ □ 対応済 □ 未対策 ☑対応不要	□ **ログイン成功後に、新しくセッションを開始する。**	セッションを使っていないため	4-(iv)-a
				□ **ログイン成功後に、既存のセッションIDとは別に秘密情報を発行し、ページの遷移ごとにその値を確認する。**		4-(iv)-b
		保険的対策	□ 対応済 □ 未対策 ☑対応不要	セッションIDを固定値にしない。	セッションを使っていないため	4-(v)
		保険的対策	□ 対応済 □ 未対策 ☑対応不要	セッションIDをCookieにセットする場合、有効期限の設定に注意する。	セッションを使っていないため	4-(vi)

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

■ ウェブアプリケーションのセキュリティ実装 チェックリスト （2/3）

No	脆弱性の種類		対策の性質	チェック	実施項目		解説
5	クロスサイト・スクリプティング	HTMLテキストの入力を許可しない場合の対策	**根本的解決**	☑対応済 □ 未対策 □ 対応不要	**ウェブページに出力する全ての要素に対して、エスケープ処理を施す。**		5-(i)
			根本的解決	□ 対応済 □ 未対策 ☑対応不要	**URLを出力するときは、「http://」や「https://」で始まるURLのみを許可する。**	URLを出力する機能を持たないため	5-(ii)
			根本的解決	☑対応済 □ 未対策 □ 対応不要	**<script>…</script> 要素の内容を動的に生成しない。**		5-(iii)
			根本的解決	☑対応済 □ 未対策 □ 対応不要	**スタイルシートを任意のサイトから取り込めるようにしない。**		5-(iv)
			保険的対策	☑対応済 □ 未対策 □ 対応不要	入力値の内容チェックを行う。		5-(v)
		HTMLテキストの入力を許可する場合の対策	**根本的解決**	□ 対応済 □ 未対策 ☑対応不要	**入力されたHTMLテキストから構文解析木を作成し、スクリプトを含まない必要な要素のみを抽出する。**	入力をHTMLとして解釈する機能がないため	5-(vi)
			保険的対策	□ 対応済 □ 未対策 ☑対応不要	入力されたHTMLテキストから、スクリプトに該当する文字列を排除する。	入力をHTMLとして解釈する機能がないため	5-(vii)
		全てのウェブアプリケーションに共通の対策	**根本的解決**	☑対応済 □ 未対策 □ 対応不要	**HTTPレスポンスヘッダのContent-Typeフィールドに文字コード（charset）の指定を行う。**		5-(viii)
			保険的対策	□ 対応済 □ 未対策 ☑対応不要	Cookie情報の漏えい対策として、発行するCookieにHttpOnly属性を加え、TRACEメソッドを無効化する。	セッション（Cookie）を使っていないため	5-(ix)
			保険的対策	☑対応済 □ 未対策 □ 対応不要	クロスサイト・スクリプティングの潜在的な脆弱性対策として有効なブラウザの機能を有効にするレスポンスヘッダを返す。		5-(x)
6	CSRF （クロスサイト・リクエスト・フォージェリ）		**根本的解決**	※ □ 対応済 □ 未対策 ☑対応不要	□ **処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行する。**	Cookieやセッションを使わず、JWTをAuthorizationヘッダーに設定することで認証しているため	6-(i)-a
					□ **処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。**		6-(i)-b
					□ **Refererが正しいリンク元かを確認し、正しい場合のみ処理を実行する。**		6-(i)-c
			保険的対策	□ 対応済 □ 未対策 ☑対応不要	重要な操作を行った際に、その旨を登録済みのメールアドレスに自動送信する。	根本的解決の対応済み	6-(ii)
7	HTTPヘッダ・インジェクション		**根本的解決**	※ ☑対応済 □ 未対策 □ 対応不要	☑ **ヘッダの出力を直接行わず、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用APIを使用する。**		7-(i)-a
					☑ **改行コードを適切に処理するヘッダ出力用APIを利用できない場合は、改行を許可しないよう、開発者自身で適切な処理を実装する。**		7-(i)-b
			保険的対策	□ 対応済 □ 未対策 ☑対応不要	外部からの入力の全てについて、改行コードを削除する。	根本的解決の対応済み	7-(ii)

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

■ ウェブアプリケーションのセキュリティ実装 チェックリスト （3/3）

No	脆弱性の種類	対策の性質	チェック	実施項目		解説
8	メールヘッダ・インジェクション	**根本的解決**	※ □ 対応済 □ 未対策 ☑対応不要	□ **メールヘッダを固定値にして、外部からの入力はすべてメール本文に出力する。**	入力値からメールの内容を作成する機能を持っていないため	8-(i)-a
				□ **ウェブアプリケーションの実行環境や言語に用意されているメール送信用APIを使用する（8-(i) を採用できない場合）。**		8-(i)-b
		根本的解決	□ 対応済 □ 未対策 ☑対応不要	**HTMLで宛先を指定しない。**	入力値からメールの内容を作成する機能を持っていないため	8-(ii)
		保険的対策	□ 対応済 □ 未対策 ☑対応不要	外部からの入力の全てについて、改行コードを削除する。	入力値からメールの内容を作成する機能を持っていないため	8-(iii)
9	クリックジャッキング	**根本的解決**	※ ☑対応済 □ 未対策 □ 対応不要	☑ **HTTPレスポンスヘッダに、X-Frame-Optionsヘッダフィールドを出力し、他ドメインのサイトからのframe要素やiframe要素による読み込みを制限する。**		9-(i)-a
				□ **処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。**		9-(i)-b
		保険的対策	□ 対応済 □ 未対策 ☑対応不要	重要な処理は、一連の操作をマウスのみで実行できないようにする。	根本的解決の対応済み	9-(ii)
10	バッファオーバーフロー	**根本的解決**	※ ☑対応済 □ 未対策 □ 対応不要	☑ **直接メモリにアクセスできない言語で記述する。**		10-(i)-a
				□ **直接メモリにアクセスできる言語で記述する部分を最小限にする。**		10-(i)-b
		根本的解決	☑対応済 □ 未対策 □ 対応不要	**脆弱性が修正されたバージョンのライブラリを使用する。**		10-(ii)
11	アクセス制御や認可制御の欠落	**根本的解決**	☑対応済 □ 未対策 □ 対応不要	**アクセス制御機能による防御措置が必要とされるウェブサイトには、パスワード等の秘密情報の入力を必要とする認証機能を設ける。**		11-(i)
		根本的解決	☑対応済 □ 未対策 □ 対応不要	**認証機能に加えて認可制御の処理を実装し、ログイン中の利用者が他人になりすましてアクセスできないようにする。**		11-(ii)

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

6 問い合わせ先

本書に関する問い合わせは以下にてお願いします。

問い合わせ先部署　：株式会社オプティマインド　コーポレート部

問い合わせメールアドレス：　security@optimind.tech