Seculio セキュリティホワイトペーパー

2.17 版

LRM 株式会社

1　利用者との責任分界点

LRM の責任

LRM は、以下のセキュリティ対策を実施します。

- Seculio アプリケーションのセキュリティ対策
- Seculio アプリケーションに保管されたお客様データの保護
- Seculio アプリケーションの提供に利用するミドルウェア、OS、その他インフラのセキュリティ対策

お客様の責任

お客様は、以下のセキュリティ対策を実施する必要があります。

- 各利用者に付与されたパスワードの適切な管理
- Seculio アカウントの適切な管理（登録、削除、権限設定、組織管理者設定など）

2　データ保管場所

- お客様からお預かりしたデータは、AWS 東京リージョンに保管されます。

3　データの削除

- Seculio 利用に関する契約が終了した場合、契約終了から 90 日以内に、お客様からお預かりしたデータは完全に消去されます。ただし、サプライチェーンセキュリティ機能に基づいて、お客様が作成されたアンケートに関するデータは、質問データ及び回答データともに、匿名化した状態で保持します。メール送信記録をはじめとした通信記録や操作履歴などのログは適切なアクセス権のもとで保管されます。

4　ラベル付け機能

全般

- お客様は、ユーザーをお客様自ら追加したグループにグルーピングすることが可能です。

【操作手順書】

○　グループを新規作成する
(https://teachme.jp/3233/manuals/2488588)

○　複数のグループを一括で新規作成する
(https://teachme.jp/3233/manuals/3740828)

○　既存グループの変更(ユーザー追加・グループ名修正)をおこなう
(https://teachme.jp/3233/manuals/2489296)

○ 既存グループからユーザーを外す(減らす)
(https://teachme.jp/3233/manuals/2489005)

eラーニング機能

- お客様は、LRM から配信された、もしくはお客様自らが追加した教材の名称及びカテゴリを変更することが可能です。

【操作手順書】
○ 教材を Seculio へアップロード(登録)する
(https://teachme.jp/3233/manuals/2643044)
○ 教材を編集する
(https://teachme.jp/3233/manuals/3383682)

5 利用者登録および削除

- お客様は、契約の範囲内において、いつでも自由にユーザーの登録・削除を行うことが可能です。

【操作手順書】
○ Seculio に新規ユーザー(従業者)を登録する
(https://teachme.jp/3233/manuals/1890000)
○ メールアドレスを持っていない新規ユーザー(従業者)を Seculio に登録する
(https://teachme.jp/3233/manuals/1978983)
○ csv ファイルを使って Seculio に新規ユーザー(従業者)を一括登録する
(https://teachme.jp/3233/manuals/4316393)
○ ユーザーを削除する
(https://teachme.jp/3233/manuals/3383663)

6 アクセス権の管理

- お客様は、LRM から提供する権限を、ユーザーに対して自由に付与することが出来ます。

【操作手順書】
○ ユーザーの権限を変更する
(https://teachme.jp/3233/manuals/5323417)
○ ユーザー追加時にデフォルトで付与される権限を変更する
(https://teachme.jp/3233/manuals/5323390)
○ 各権限でどのような機能を利用できるのか確認する
(https://teachme.jp/3233/manuals/5323236)

- 組織管理者に設定することで、付与されている権限に関わらず、全機能を利用することが出来ます。

【操作手順書】
○ 組織管理者を追加する
(https://teachme.jp/3233/manuals/3142683)
○ 組織管理者を削減する
(https://teachme.jp/3233/manuals/3142683)

7 パスワードの配布方法

- 新規登録したユーザーに初期パスワードを配布する方法は 2 通りあります。お客様は、以下の 2 通りの方法から、好きな方法を選んで、ユーザーに初期パスワードを配布することが可能です。
  ① 新規ユーザーを追加したと同時に、新規ユーザーのメールアドレスに、初期パスワードを登録するための、一意の URL を含むメールが送信されます。
  新規ユーザーは、その URL にアクセスし、パスワードを入力・設定することで、サービスの利用を開始できます。
  ② 新規ユーザーを追加したと同時に、初期パスワードが生成され、ユーザー追加者に対して、新規ユーザーの初期パスワードが表示されます。
  ユーザー追加者は表示された初期パスワードを、メールや、紙媒体への記載など、組織の慣習に合わせた自由な方法で、新規ユーザーに配布することが可能です。

【操作手順書】
○ Seculio ユーザー登録手順
(https://teachme.jp/3233/manuals/1913715)

- ユーザーはパスワードを忘れた場合、自らパスワードの再設定を行うことが可能です。

【操作手順書】
○ パスワードを再設定する
(https://teachme.jp/3233/manuals/3239080)

8 暗号化の状況

全般

- データベースに保管される、お客様の各種情報（氏名、メールアドレス、各機能で利用するデータなど）は暗号化され、適切なアクセス権のもとで保管されます。また、パスワードは、不可逆暗号化(ハッシュ化)された状態で、データベースに保管されます。

- お客様の端末と、システムとの間のインターネット通信は、SSL/TLS 通信によって暗号化されます。なお、対応している SSL/TLS は、TLSv1.2 以降(SHA256 以上)となります。

eラーニング機能

- 教材の一部としてアップロードされた PDF ファイルは、暗号化(AES256)され、適切なアクセス権のもとで保管されます。

9　変更管理

- サービスのバージョンアップ情報を始めとした、各種の変更に関する情報は、下記のリンク先 Web ページより閲覧することが可能です。
  - ○　リリースノート　https://support.lrm.jp/hc/ja/sections/360011627331
- サービスのバージョンアップが実施された場合、メール通知を受け取れるようご設定いただけます。

【操作手順書】
○　Seculio に関するお知らせ、リリース情報をメールで受信する方法
(https://teachme.jp/3233/manuals/10823445/)

10 手順書の提供

- お客様が利用できる手順書は、下記リンク先より閲覧することが可能です。
  - ○　マニュアル　https://teachme.jp/r/seculio

11 バックアップの状況

全般

- データベースに保管される、お客様の各種情報（氏名、メールアドレス、各機能で利用するデータなど）は、日次でバックアップを取得しています。バックアップは、7 世代分保管されます。
- 但し、お客様によるバックアップデータの復元等に関する要望は、承っておりません。

eラーニング機能

- 教材の一部としてアップロードされた PDF ファイルは、AWS 東京リージョン内の複数のデバイスで、冗長的に格納されます。ある箇所でデータが破損しても、冗長データより自動で修復されます。

12 ログのクロックに関する情報

- Seculio サービス内で提供されるログは、タイムゾーン JST(UTC+9)で提供されます。

- ログの時間は、AWS が提供する NTP サービスと同期しています。

13 脆弱性管理に関する情報

- Seculio 開発チームは、システムで利用している OS、ミドルウェア等に関する脆弱性情報を、定期的に収集しています。
- システムで利用しているコンポーネントに対する脆弱性パッチが公開された場合は、テスト環境での検証を経た後、速やかに適用されます。

14 開発におけるセキュリティ情報

- Seculio システムの開発には、主に Ruby On Rails が用いられています。開発は Rails セキュリティガイド[1]および、社内で定められたコーディング規約に従って実施されます。
- 標的型攻撃メール訓練機能の開発には、node.js を利用しています。
- 安否確認機能およびセキュリティアウェアネス機能の開発には、Go を利用しています。

15 インシデント発生時の対応

- 情報セキュリティインシデントに関する問合せは、本セキュリティホワイトペーパー末尾の「Seculio サポート担当」窓口より受け付けています。
- お客様に大きな影響を与えるセキュリティインシデント(データの消失、長時間のシステム停止等) が発生した場合は、インシデント発生から 72 時間以内を目標に、下記のリンク先 Web ページに情報を掲載します。
  - ○ お知らせページ https://support.lrm.jp/hc/ja/sections/360011627911
- お知らせページには、インシデント情報、契約情報やアップデート情報といった重要な情報が多数掲載されますので、更新時にメール通知を受け取れるようご設定をお願いいたします。

【操作手順書】
○ Seculio に関するお知らせ、リリース情報をメールで受信する方法
(https://teachme.jp/3233/manuals/10823445/)

16 お客様データの保護及び第三者提供について

- お客様から預かったデータを適切に保護することは、LRM の責任です。ログデータを含むお客様デー

[1] https://railsguides.jp/security.html

タは、不正なアクセスや改ざんを防ぐため、Seculio 開発チームの一部の人間しかアクセスできない、限られたアクセス権のもとで保管されます。

- 但し、裁判所からの証拠提出命令など、法的に認められた形でお客様のデータの提供を要請された場合、LRM は、お客様の許可なく、必要最小限の範囲で、お客様情報を外部に提供する可能性があります。

17 適用法令

- お客様と LRM との間の契約は、日本法に基づいて解釈されるものとします。

18 認証

- LRM は、情報マネジメントシステム認定センター(ISMS-AC)が運営する、ISMS 適合性評価制度における、ISMS 認証[2]を取得しています。
- LRM は、情報マネジメントシステム認定センター(ISMS-AC)が運営する、ISMS 適合性評価制度における、ISMS クラウドセキュリティ認証[3]を取得しています。
- LRM は、情報マネジメントシステム認定センター(ISMS-AC)が運営する、ISMS 適合性評価制度における、ISMS-PIMS 認証[4]を取得しています。
- LRM は、BSI グループジャパン株式会社が実施する、ISO/IEC 27018 の審査を受審し、ISO/IEC 27018 の導入ガイダンスを考慮した ISMS を実施していることを認証されています。

【ISMS クラウドセキュリティ認証登録範囲】 Seculio の提供に係るクラウドサービスプロバイダとしてのシステム開発・運用・保守、及びアマゾンウェブサービスのクラウドサービスカスタマとしての利用に係る ISMS クラウドセキュリティマネジメントシステム
【ISMS-PIMS 認証登録範囲】 PII 管理者および PII 処理者としてのセキュリティ支援サービス
【ISO/IEC 27018 認証登録範囲】 SaaS 型情報セキュリティマネジメントシステム運用支援システムの開発、運用、カスタマーサポート

[2] https://isms.jp/lst/ind/CR_IS_x0020_605509.html

[3] https://isms.jp/isms-cls/lst/ind/CR_CLOUD_x0020_682774.html

[4] https://isms.jp/isms-pims/lst/ind/CR_PM_x0020_740706.html

19 外部クラウドサービスの利用

- Seculio では、次に示す機能を運用するために、外部のクラウドサービスを利用しています。

クラウドサービス	機能	運営会社	情報
AWS	インフラ構築,運用	Amazon	個人名,メールアドレス,PDF ファイル 等
SendGrid[5]	メール送信	SendGrid	メールアドレス,メール内容,送信日時 等
Wrike[5]	お問い合わせ管理	Wrike	個人名,会社名,お問い合わせ内容 等
Zendesk[5]	お問い合わせ管理	Zendesk	メールアドレス,お問い合わせ内容 等
Zoho[5]	ご契約管理、メール送信	Zoho	個人名,会社名,ご契約内容 等

この資料に関するお問い合わせ

LRM 株式会社
Seculio(セキュリオ)サポート担当
050-1741-9630
seculio@lrm.jp

[5] 当セキュリティホワイトペーパーに記載されている内容は、クラウドサービスにおいて管理されている範囲には及ばず、また、その内容の遵守を保証するものではありません。

改訂履歴

版	改訂日	改訂内容
1.0	2017/03/01	初版発行
1.1	2017/06/20	「4. ラベル付け機能」E ラーニング機能 における、ラベル付けの新たな機能として、「テーマのカテゴリ」を追加。 新規ユーザー登録のサービス仕様変更に伴い、「7. パスワードの配布方法」の記載内容を刷新。
1.2	2017/07/07	「17. 認証」に記載されている内容を明確化。 「18. 免責」を追加。
2.0	2017/10/23	デザインを刷新。 資料名称を「Seculio セキュリティホワイトペーパー」に変更。
2.1	2017/12/27	「9. 変更管理」を追加。 「9. 変更管理」の追加に伴い、「10. 手順書の提供」以降の見出し番号を修正。 「18. 認証」に記載されている内容を変更。
2.2	2018/02/15	操作方法の記載から、該当操作手順書のリンクの記載に変更。 「18. 認証」の ISMS クラウドセキュリティ認証に注釈を追加。
2.3	2018/04/25	「19. 免責」の表記方法を変更し、「G Suite」を対象に追加。
2.4	2018/07/26	「4. ラベル付け機能」「5. 利用者登録および削除」にマニュアルを一部追加
2.5	2018/08/15	「8.暗号化の状況」に記載されている内容を変更。
2.6	2018/10/18	管理者を組織管理者に変更。 「15. インシデント発生時の対応」に報告までの目標時間を明記。 「19. 免責」を「19. 外部クラウドサービスの利用」とし、AWS を追加、また、一部の外部クラウドサービスがホワイトペーパーの範囲外であることを注釈として追加。
2.7	2018/11/19	「19. 外部クラウドサービスの利用」に「Zendesk」を追加。
2.8	2019/01/25	権限管理機能の提供に伴い、「1. 利用者との責任分界点」「6. アクセス権の管理」「7. パスワードの配布方法」に記載されている内容を変更。 操作手順書の URL を変更。 「E ラーニング」から「e ラーニング」に表記を変更。
2.9	2019/06/20	「18. 認証」に ISO/IEC27018 を追加。
2.10	2020/04/22	「19. 外部クラウドサービスの利用」の「G Suite」を「Wrike」に変更。
2.11	2020/05/01	問い合わせ先電話番号を変更。
2.12	2020/05/12	標的型攻撃メール訓練の提供に伴い、「2. データ保管場所」にシドニーリ

		ージョンを追加。新機能の提供に合わせ、サービス全体に関わるデータ削除のポリシーを変更。「9. 変更管理」についてバージョンアップの際の周知のポリシーを変更。「14. 開発におけるセキュリティ情報」に node.js の使用について追記。
2.13	2020/08/26	「テーマ」の表記を「教材」に統一
2.14	2020/09/03	標的型攻撃メール訓練機能のメール送信ログ保管場所がシドニーから東京に変更になったことに伴い、一部表記を削除。 問い合わせ先メールアドレスを変更。
2.15	2020/11/11	インシデント発生時の通知先の表記を変更。安否確認機能に関する記載を追加。
2.16	2021/6/7	暗号化の状況に関する記載を変更。教材ファイルの復元について、詳細を追加。外部クラウドサービスに「Zoho」を追加。お問い合わせ先を変更。ISMS-PIMS 認証に関する記載を追加。お知らせやリリース情報の通知方法を変更。
2.17	2021/7/2	「14. 開発におけるセキュリティ情報」にセキュリティアウェアネス機能に関する説明を追加。