CLOUDSIGN

これからの100年、新しい契約のかたち。

セキュリティ ホワイトペーパー

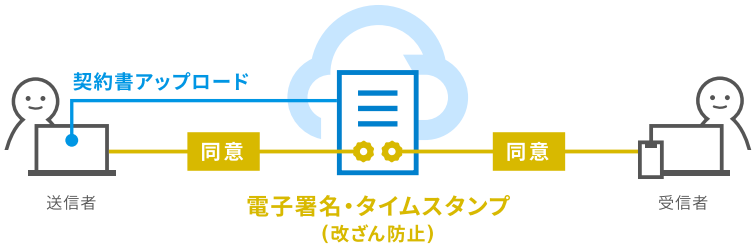
2021年7月16日版

CLOUDSIGN
WHITE PAPER

この文書について

この文書は、2021 年 7 月の時点におけるクラウドサインの情報セキュリティへの取り組みと、情報セキュリティの観点からお客さまにご注意いただきたい点について紹介するものです。

クラウドサインは、弁護士ドットコム株式会社（以下、「当社」といいます）が運営する、電子契約を実現するためのサービスです。
一方のお客さまが当サービス上に契約書等をアップロードし、もう一方のお客さまがこれに同意すると、当社による電子署名が施され、合意を締結した事実についての証跡を残すことができます。



クラウドサインでは、お客さまから預かる契約書等のデータを、重要な機密文書として扱います。お客さまの意思に反して第三者に読み取られたり、内容を改竄されることがないように、情報セキュリティに配慮した慎重な取り扱いを行います。

なお、この文書は「クラウドサイン」のサービス本体について記述したものです。他社サービスとの連携機能や一部のオプションサービスについては、この文書の記述が当てはまらない場合があります。詳細はご利用時にご確認ください。

目次

クラウドサインのセキュリティの取り組み

お客さまにご注意いただきたい点

［ 付録 ］

1

クラウドサインの
セキュリティの取り組み

クラウドサインのサービス側が実施している
セキュリティの取り組みについてご紹介します。

1-1. 所在地と法管轄

クラウドサインのサービスは、弁護士ドットコム株式会社が提供しています。当社は日本の法人であり、本店所在地は東京都です。クラウドサインのサービスの開発、運用は全て日本国内で行っています。

クラウドサインのシステムは、Amazon Web Services（AWS）を利用して構築しており、システムが保管するデータおよびそのバックアップデータは、いずれもAWS の管理するデータセンターに保管されています。

AWS はアメリカを本拠地とする企業ですが、日本国内にもデータセンターを所持しており、クラウドサインでは東京リージョン及び大阪リージョンにデータを保存しています。メール送信など一部の処理に海外のリージョンを利用することはありますが、データの保管にはすべて国内のリージョンを利用しており、海外のサーバーにお客さまのデータを保管することはありません。

また、AWS との契約においては準拠法を日本法とする契約を結んでいます。これにより、海外法の適用によるリスクを回避しています。

1-2. 暗号による保護

クラウドサインでは、通信内容や保存データ、パスワードを暗号技術によって保護しています。

暗号技術を採用する際には、CRYPTREC 電子政府推奨暗号リストを参照し、危殆化していない（暗号が古くなって破られるおそれのない）技術を採用すると同時に、暗号輸出入の規制に抵触することがないように配慮しています。

1-2-1. 通信の暗号化

クラウドサインでは、通信内容を暗号化することで、データの漏洩や改竄を防いでいます。暗号通信方式として TLS 1.2 を採用しており、CRYPTREC の「SSL/TLS 暗号設定ガイドライン」を参照しての「推奨セキュリティ型」の設定をすることとしています。

1-2-2. データの暗号化

クラウドサインでは、書類データをサーバーに保存する際にも暗号化を行い、これによってデータの漏洩や、内部不正による持ち出しを防いでいます。暗号アルゴリズムには AES-GCM を採用しており、秘密鍵は AWS Key Management Service（KMS）を利用して厳重に管理しています。

書類ファイル以外のお客さまが登録、入力されたデータは、データベースに保存しています。データベースについては透過的暗号化、フルディスク暗号化を実施しています。

1-2-3. パスワードのハッシュ化

クラウドサインの利用者のパスワードは平文では保存せず、ハッシュ化し、元の形に復元できないようにした上で保存しています。

1-3. データのバックアップと返却・削除

お客さまからお預かりした書類のデータは、クラウドサインのシステム上で保管されています。原則として保管期限の制限はなく、クラウドサインのサービスが続く限り、契約当事者が契約内容を確認できるようになっています。

1-3-1. サービス側でのバックアップ

クラウドサインのサービス側では、大切な契約書の内容が失われることがないよう、データのバックアップを行っています。バックアップは遠隔地に保存しており、サービスに障害が発生した場合でも、バックアップから復旧できるように備えています。

書類ファイルと、お客さまが入力されたデータについて、それぞれ以下のようにバックアップをとっています。

- **書類ファイルのバックアップ**

  書類ファイルがアップロードされた時点で遠隔地へのファイルのレプリケーション（複製）を行い、随時バックアップを取得しています。 バックアップの保存期間はなく、明示的な削除依頼がない限り永久に保存します。

- **入力データのバックアップ**

  データはデータベースに保存しており、自動バックアップで 10 分前のスナップショットを保持しているほか、日次でバックアップデータの取得も行っています。日次取得したデータは 7 日間保存しています。

バックアップデータは AWS 大阪リージョンに保存しており、東京で大規模な障害が起きても復旧できるよう備えています。

データの暗号化については「1-2-2. データの暗号化」に記載していますが、バックアップデータもそれぞれ同様に暗号化されています。

1-3-2. お客さま側でのバックアップ

書類の送信者、受信者、承認者として指定されている方は、必要に応じて書類ファイルをダウンロードすることができます。これを利用して、お客さまの側で書類のバックアップを保存することも可能です。

また、一括ダウンロードのサービスも提供しておりますので、大量のデータをバックアップしたい場合にはご相談ください（一括ダウンロードは有償となりますのでご了承ください）。

1-3-3. 解約時のデータの扱い

お客さまがクラウドサインのサービスを解約された場合、解約後は書類データをダウンロードできなくなります。必要に応じて、解約前にダウンロードを行ってください。

書類を送信したお客さまがクラウドサインのサービスを解約された場合も、書類データはサービス上に残ります。これは、クラウドサインが契約内容の証拠を残すことを目的としたサービスであるためです。契約当事者（書類の送信者、受信者、承認者となっている方）は、クラウドサインのサービスを解約しない限り、引き続き書類を閲覧し、ダウンロードすることができます。

ただし例外的に、契約当事者となる方全員（承認者や受信者が複数いる場合は、その全員）のデータ削除要望が揃った場合、ご依頼をいただくことで、クラウドサインの運営側で契約書データを物理削除する処理を行うことがあります。詳しくはお問い合わせください。

なお、削除の対象となるのは書類ファイルです。お客さまのアカウントデータ（登録されたメールアドレスやお名前など）は解約後も残り、契約相手の方の画面では引き続き表示されますので、ご了承ください。

1-4. タイムスタンプと時刻の同期

クラウドサインのサービスでは、締結された契約書にタイムスタンプを付与します。これにより、タイムスタンプの確定時刻に電子データが存在したこと（存在証明）、タイムスタンプの確定時刻以降に電子データが改ざんされていないこと(非改ざん証明)を証明する仕組みとなっています。

タイムスタンプの付与には、セイコータイムスタンプサービスを利用しています。セイコータイムスタンプは、日本データ通信協会が認定した時刻認証業務認定事業者（TSA, time stamping authority）です。

クラウドサインが認定タイムスタンプを利用していることは、日本データ通信協会のサイトでもご確認いただけます（登録番号 U00018-001）。

U00018-001	弁護士ドットコム株式会社 代表取締役　内田 陽介	クラウドサイン	電子契約関連 電子帳簿保存法関連	東京都港区六本木4-1-4黒崎ビル6階	2018年9月4日

認定タイムスタンプを利用しているサービス又は業務（日本データ通信協会）
https://www.dekyo.or.jp/touroku/contents/repository/index.html

このタイムスタンプの時刻は、きわめて正確に UTC（Coordinated Universal Time, 協定世界時）に同期されています。

お客さまが利用されている端末の設定時刻が正確でない場合、タイムスタンプとのずれが生じて見えることがあります。端末の設定時刻を UTC と同期されることをおすすめいたします（設定方法は OS によって異なります。お客さまの責任にて実施をお願いいたします）。

1-5. セキュリティを向上するオプション機能

クラウドサインでは、情報セキュリティを向上させるためのオプション機能をご用意しています。

1-5-1. プランを問わずにご利用いただける機能

プランを問わずに利用できるセキュリティ機能は以下の通りです。

- 2 要素認証

2 要素認証の詳細について、ヘルプページでご案内しています。
以下をご覧ください。

2 要素認証の利用を開始する
https://help.cloudsign.jp/ja/articles/3279982

1-5-2. ビジネスプランでご利用いただける機能

ビジネスプランをご契約いただくと、さらに以下のセキュリティ機能をご利用いただくことができます。

- アカウント登録制限機能
- 承認機能
- アクセス制限機能（IPアドレス制限機能）
- 高度な管理機能
- SSO（シングルサインオン）機能
- 親展機能
- 監査ログ機能

ビジネスプランでご利用いただける上記の機能について、ヘルプページでご案内しています。以下をご覧ください。

ビジネスプラン

https://help.cloudsign.jp/ja/articles/2833670

1-6. 開発体制

クラウドサインのシステム開発は、当社の社内で行っています。

※一部、業務委託の方に開発に参加していただいている部分があります。一部のオプションサービスについては他社にて開発をしている場合があります。他社サービスとの連携機能については、連携先の各社にて開発・運用が行われている場合があります。詳しくはお問い合わせください。

クラウドサインでは、開発時のガイドラインを設けており、セキュリティ上の注意点を含めています。さらに、開発時にはコードレビューを実施し、レビューを経なければ本番反映できない仕組みとすることで、実際のコードがガイドラインに従っていることを確認しています。

また、公開前にユニットテスト（プログラム部品単位での自動化テスト）と E2E テスト（End to End テスト、ブラウザ自動操作による結合テストおよび表示検証）

を実施して、コードの品質を担保しています。

さらに、第三者によるウェブアプリケーション脆弱性診断、プラットフォーム診断を半年に１回の頻度で実施しており、重ねて安全性を確認しています。

1-7. 情報セキュリティインシデントの取り扱いと通知

クラウドサインにおいて、情報セキュリティインシデント（情報漏洩など、情報セキュリティに関連した事故、事象。以下「インシデント」といいます）が起きた場合、以下のように対処を行います。

1-7-1. 報告するインシデントの範囲

インシデントのうち、利用者に明確な被害が及ぶか、もしくは、クラウドサインのサービスの継続に影響を及ぼすと判断したものを「重大インシデント」と定義します。重大インシデントの例には以下のようなものがあります。

- クラウドサインのサービスへの不正アクセスにより、情報流出が起きた
- 社内システムのウイルス感染により、情報流出や業務停止が起きた
- なりすましサイトにより、クラウドサインの利用者が実際に被害を受けた
- 外部からの攻撃により、クラウドサインのサービスが利用不可能になり、その状態が一定時間以上継続した

1-7-2. インシデントの通知手順

重大インシデントが発生した場合には、以下の手段で通知いたします。

- インシデントが多数のお客様に影響する場合は、サービスサイト上にて告知いたします。
- サービスの停止を伴う場合には、ステータスページ（https://status.cloudsign.jp/）でも告知いたします。
- インシデントにより特定のお客様に影響が出たと判断した場合、個別に電子メール等にてご連絡いたします。

インシデントが継続的に発生している場合や、調査報告に時間を要する場合、サービスサイト上で続報を提供いたします。

1-7-3. インシデント通知までの目標時間

クラウドサインでは、重大インシデントを認知した場合、可及的すみやかにお客さまに通知いたします。影響を受けたお客さまに対し、遅くとも、インシデントの認知から 24 時間以内に何らかの通知を行うことを目標としています。

1-8. BCP（事業継続計画）におけるクラウドサインの位置付け

1-8-1. クラウドサインの障害対応・復旧計画

何らかの理由でクラウドサインのサービスが停止した場合、クラウドサインの側では復旧計画に沿ってサービスの復旧を試みます。

クラウドサインは複数のデータセンター（アベイラビリティゾーン）を利用した冗長化を実施しています。障害により単一のデータセンターが停止しても、基本的にはサービスの継続的な提供が可能です（切替影響による遅延等は考えられます）。

また、契約書ファイルとデータベースのバックアップを実施しています。大規模災害等により複数のデータセンターがすべて停止した場合には、遠隔地にシステムを再構築することによりサービスを再開する計画となっています。

1-8-2. バックアップからの復旧と目標時間

データが破壊された場合にはバックアップからの復旧を行います。バックアップ復旧時の目標復旧時間（RTO）は 6 時間、目標復旧地点（RPO）は 10 分としています。

※これらは社内目標値であり、お客さまに SLA として提供しているものではありませんのでご了承ください。

1-8-3. お客さまによる代替措置（縮退運用）

お客さまが BCP（事業継続計画）を立案する際、クラウドサインのサービス停止

が長期にわたり、復旧の見込みがないケースの検討が必要になる場合があります。その場合にお客さま側でとることができる代替措置（縮退運用）として、以下の選択肢が考えられます。

- **契約書の閲覧、契約内容の確認**

  契約に使用した書類は電子メールに添付されて送信先に届くため、当サービスが終了しても利用者の手元に残ります。クラウドサインで扱う書類ファイルはPDF 形式、電子署名は PAdES 仕様に準拠したものとなっていますので、一般的な PDF リーダーで閲覧することができ、署名の検証も可能です。

- **契約書の送付**

  上記の通り、書類ファイルは一般的な形式のものですので、一般的なファイル共有の方法で相手方に共有することができます。電子メールに添付して送信・転送する、クラウドストレージに保存してデータを共有するといったことが可能です。

- **紙での契約締結**

  電子契約を諦め、紙での契約締結を行う選択肢も想定できます。

2

お客さまに
ご注意いただきたい点

クラウドサインのサービスを安全に利用するために、
お客さまにご注意いただきたい点がいくつかあります。

2-1. サービスの利用に必要な環境とソフトウェア

クラウドサインは、SaaS（Software as a Service）型のクラウドサービスです。

サービスを利用するためには、インターネットに接続できる環境とパソコンが必要になります（書類の受信と同意についてはスマートフォンで利用することも可能です）。また、インターネット経由で電子メールを受信できる必要がありますので、電子メールを受け取る環境と電子メールアドレスが必要になります。

サービスを利用する際に、専用のソフトウェアをインストールする必要はなく、Web ブラウザのみでご利用いただけます。ただし、特定の機能を利用する際には、追加のソフトウェアが必要になる場合があります。

- 書類の電子署名を検証する際には、Adobe 社の Adobe Reader など PDF の署名を検証するソフトウェアが必要です。
- 2 要素認証の機能を利用する際には、ソフトウェアトークンが必要です。TOTP（time-based One-time Password Algorithm, RFC6238）に対応したアプリケーションがご利用いただけます。

以下のページに推奨環境を記載していますので、参考にしてください。

クラウドサインの推奨環境

https://help.cloudsign.jp/ja/articles/2570393

なお、サービスの利用にはインターネット接続が必要となります。2021 年 3 月現在、クラウドサインのサービスは IPv4 接続のみを提供しています。IPv6 では直接接続できませんのでご注意ください。また、専用線や VPN による接続はご利用いただくことができません。お客さまの社内データセンターにクラウドサインのサービスを構築することもできませんので、ご了承ください。

2-2. お客さまの環境におけるセキュリティ上の注意点

クラウドサインのシステムを構成するシステムについては、当社の責任において管理と運用を行っています。クラウドサービス側のアプリケーション、ミドルウェア、サーバー、ネットワーク機器については、クラウドサインが責任を持って管理いたします。お客さまにてソフトウェアのアップデートを行う必要もありません。

一方で、お客さまがインターネットに接続する環境、利用される端末（パソコンもしくはスマートフォン）、Web ブラウザ、電子メールアドレス等については、お客さま側でご用意いただく必要があります。これらの情報セキュリティについては、お客さまにて管理いただく必要があります。

お客さま側の環境について、特に以下の点についてご配慮ください。

- ネットワーク環境の安全性
- 端末の盗難防止策
- 端末 OS のセキュリティアップデート
- Web ブラウザのセキュリティアップデート
- その他のソフトウェアのセキュリティアップデート
- 電子メールの盗聴・傍受への対策
- 電子メールへのウィルス対策

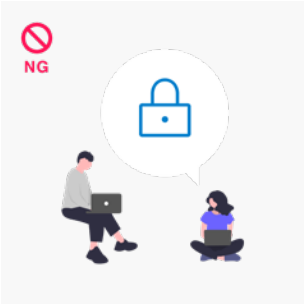
サービス上で扱うデータの内容につきましては、お客さまの責任となります。契約書の内容に不備がないか、法的な問題がないかといった点を十分にご検討の上、ご利用ください。

また、サービスの性質上、クラウドサインのシステム側では、書類の内容に対する改変・削除等を行いません。送信者が送信した PDF ファイルは、原則としてそのままの形で受信者に届きます。書類の内容については十分に注意してご確認いただき、必要に応じて送信者にお問い合わせください。

2-3. お客さまのパスワードの管理

クラウドサインのパスワードは、お客さま本人を認証するための大切なものです。

以下に注意して厳重に管理してください。



パスワードは秘密にし、誰にも知らせない

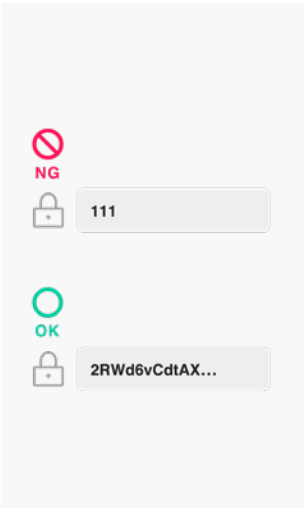
知人や関係当局の者に対しても知らせてはなりません。決して漏洩することがないように管理してください。

パスワードを他人に見られる可能性のあるところに記録したり、メモしたりすることは避ける

パスワードを記録する必要がある場合は、パスワード管理用の専用ソフトなど、安全性が確保された方法を利用してください。

パスワードが漏洩したら、ただちに変更する

クラウドサインでは、お客さまが自身でパスワードを変更することができます。パスワードが漏洩してしまったような場合には、ただちにパスワードを変更してください。

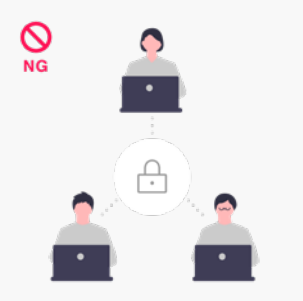


弱いパスワードや推測できるパスワードを避ける

クラウドサインでは、お客さまが自身でパスワードを設定します。

（システム側で初期パスワードを発行することはありません）

クラウドサインでは、短すぎるもの、辞書に載っている単語一語だけのもの、同一の文字を繰り返したものといった弱いパスワードは利用できないようになっています。お客さまの生年月日等のプロフィールを使うなど、推測されやすいパスワードにならないよう注意してください。

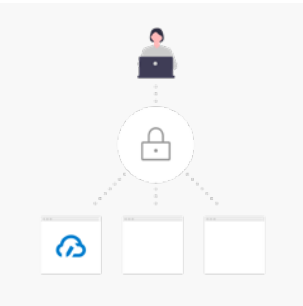


パスワードを共有しない

パスワードを共有して、ひとつのアカウントを複数人で共有することは避けてください。

他のサービスと同じパスワードを利用しない

他のサービスから漏洩したパスワードを利用する手法（リスト型攻撃）による不正アクセスが増えているため、必ず他のサービスと異なるパスワードを使用するようにしてください。



シングルサインオンのパスワードは適切に保護

ご契約プランによっては、シングルサインオンの機能をご利用いただける場合があります。
その場合、クラウドサインの側でパスワードを管理する必要はありませんが、シングルサインオンのために必要なパスワードは適切に保護していただくようお願いいたします。

2-4. お客さまによるインシデント報告とご連絡・ご依頼

お客さまがクラウドサインに関するインシデントを発見された場合、もしくは、インシデントに発展する可能性のある不審な事象を発見された場合には、速やかにクラウドサインのお問い合わせ窓口までご連絡ください。

2-4-1. 通常の連絡先

お客さまがクラウドサインをご利用中の場合、通常のお問い合わせと同様に、チャットサポートの窓口からご連絡いただくことができます。

チャットサポートがご利用いただけない場合や緊急性の高い場合には、下記の緊急連絡先のご利用もご検討ください。

2-4-2. セキュリティに関する緊急連絡先

なんらかの理由でチャットサポートがご利用いただけない場合や、緊急で連絡を取る必要がある場合、当社の情報セキュリティ窓口に電子メールでご連絡いただくことができます。

窓口のメールアドレスは、情報セキュリティポリシーの「情報セキュリティに関するお問い合わせ」の項目に記載しています。

クラウドサインをご利用でない外部の方がクラウドサインのインシデントを認知された場合も、下記の窓口からご連絡ください。

情報セキュリティポリシー

https://www.bengo4.com/corporate/privacy/it-security

2-4-3. ログ調査

お客さま側でのインシデント調査のために、クラウドサインのログの調査が必要になるケースが考えられます。ビジネスプランでは監査ログ機能を提供しており、必要に応じてお客様にてログの調査を行うことが可能です。詳細は以下をご覧ください。

監査ログ機能

https://help.cloudsign.jp/ja/articles/5264188

また、当社の運用ルールと法令に従い、ログを監査法人や第三者機関へ開示することがございますので、ご了承ください。

［付録］

セキュリティ
チェックシート

「クラウドサービスレベルのチェックリスト」（経済産業省）に基づき、弁護士ドットコム株式会社の提供する CloudSign のセキュリティについてまとめたものです。

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
1	可用性	**サービス時間**	サービスを提供する時間帯（設備やネットワーク等の点検／保守のための計画停止時間の記述を含む）	時間帯	24 時間365日(計画停止／定期保守を除く）となります。
2		**計画停止予定通知**	定期的な保守停止に関する事前連絡確認（事前通知のタイミング／方法の記述を含む）	有無	有 1 週間前にステータスページ（https://status.cloudsign.jp/) にて通知します。
3		**サービス提供終了時の事前通知**	サービス提供を終了する場合の事前連絡確認（事前通知のタイミング／方法の記述を含む）	有無	無 現状定義しておりませんが判明次第サイト、ステータスページ上で通知します。
4		**突然のサービス提供停止に対する対処**	プログラムや、システム環境の各種設定データの預託等の措置の有無	有無	無 現状定義しておりません。
5		**サービス稼働率**	サービスを利用できる確率（(計画サービス時間ー停止時間）÷計画サービス時間）	稼働率（%）	SLO は公開しておりません。 参考値として、2020 年度の正常稼働率は 99.44% となっております（外部連携機能、ベータ版機能を除く）。
6		**ディザスタリカバリ**	災害発生時のシステム復旧／サポート体制	有無	有 国内遠隔地のデータセンターにデータをバックアップしております。 遠隔地に予備システムの構築はございません。
7		**重大障害時の代替手段**	早期復旧が不可能な場合の代替措置	有無	有 当サービスで扱う書類は標準的な PDF に電子署名を施した形式のものですので、他のサービスでもご利用いただけます。また、一般的な PDF リーダーで閲覧することができます。当サービスが停止した際も、契約に使用した書類を閲覧したり、一般的な電子メールで送信したりすることが可能です。 送信済みの書類については、PDF の署名の検証も可能です。ただし、新たに電子署名を付与することはできなくなり、当社が契約内容を証明する機能はご利用いただけなくなります。
8		**代替措置で提供するデータ形式**	代替措置で提供されるデータ形式の定義を記述	有無（ファイル形式）	有 PDF 形式
9		**アップグレード方針**	バージョンアップ／変更管理／パッチ管理の方針	有無	有 お客様に影響のある機能変更等を伴うアップデートは、サイト上およびステータスページで事前に告知しております。 サービスのソースコードレベルの変更管理は Git を利用して行なっています。 セキュリティパッチは、AWS Systems Manager Patch Manager により管理し、適用を半自動化しています。
10	信頼性	**平均復旧時間（MTTR）**	障害発生から修理完了までの平均時間（修理時間の和÷故障回数）	時間	2020 年下期の実績ベースで 196 分となります。
11		**目標復旧時間（RTO）**	障害発生後のサービス提供の再開に関して設定された目標時間	時間	6 時間を目標としております。
12		**障害発生件数**	1 年間に発生した障害件数／ 1 年間に発生した対応に長時間（1 日以上）要した障害件数	回	2020 年度のメインサービスに関する障害は 15 件です。 対応に 1 日以上要した障害はございません。
13		**システム監視基準**	システム監視基準（監視内容／監視・通知基準）の設定に基づく監視	有無	有 社内基準に則り監視を実施しております。
14		**障害通知プロセス**	障害発生時の連絡プロセス（通知先／方法／経路）	有無	有 サービス内、およびステータスページ（https://status.cloudsign.jp/）にて告知いたします。ステータスページにて Subscribe（購読）の手続きを行なっていただくと、障害発生時に通知メールを受け取ることもできます。

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
15	信頼性	**障害通知時間**	異常検出後に指定された連絡先に通知するまでの時間	時間	30 分以内を目安としております。
16		**障害監視間隔**	障害インシデントを収集／集計する時間間隔	時間（分）	1 分間隔で収集しております。
17		**サービス提供状況の報告方法／間隔**	サービス提供状況を報告する方法／時間間隔	時間	ステータスページ（https://status.cloudsign.jp）にてサービスの稼働状況を確認いただけます。サービスの停止時には自動的に状況が反映されます。その他の障害については 30 分程度を目安に反映しています。
18		**ログの取得**	利用者に提供可能なログの種類（アクセスログ、操作ログ、エラーログ等）	有無	ビジネスプランでは、クラウドサインのサービス上で監査ログを出力する機能をご用意しております。 取得可能なログ範囲や取得可能期間など詳しくはこちらをご覧ください。 https://help.cloudsign.jp/ja/articles/5264188
19	性能	**応答時間**	処理の応答時間	時間（秒）	ページやファイルサイズによって左右されますが、平均で 0.5 秒程度となります。書類の送信時には外部サービスによる電子署名が施されるため、署名サービスの負荷状況によっては遅延が生じることがございます。
20		**遅延**	処理の応答時間の遅延継続時間	時間（分）	処理が遅延した場合、60 秒でタイムアウトとなり切断されます。
21		**バッチ処理時間**	バッチ処理（一括処理）の応答時間	時間（分）	定期的なバッチ処理はございません。
22	拡張性	**カスタマイズ性**	カスタマイズ（変更）が可能な事項／範囲／仕様等の条件とカスタマイズに必要な情報	有無	無 サービス自体のカスタマイズには未対応となっております。
23		**外部接続性**	既存システムや他のクラウド・コンピューティング・サービス等の外部のシステムとの接続仕様（API、開発言語等）	有無	有 API を公開しております。
24		**同時接続利用者数**	オンラインの利用者が同時に接続してサービスを利用可能なユーザ数	有無 （制約条件）	無 接続上限に達した場合スケールアウトで対応を行うため基本的に制限はございません。
25		**提供リソースの上限**	ディスク容量の上限／ページビューの上限	処理能力	無 容量上限に達した場合スケールアウトで対応を行うため基本的に制限はございません。
26	サポート	**サービス提供時間帯（障害対応）**	障害対応時の問合せ受付業務を実施する時間帯	時間帯	基本的には一般問い合わせと変わらず平日 10:00-18:00（メール、チャット）を予定。 ステータスページで状況は随時更新予定
27		**サービス提供時間帯（一般問合せ）**	一般問合せ時の問合せ受付業務を実施する時間帯	時間帯	チャットで受け付けており、受付は 24 時間 365 日、対応は平日 10:00-18:00 となります。
28	データ管理	**バックアップの方法**	バックアップ内容（回数、復旧方法など）、データ保管場所／形式、利用者のデータへのアクセス権など、利用者に所有権のあるデータの取扱方法	有無／内容	有 • データベース：日次でフルバックアップ、IaaS 機能により差分バックアップを随時取得 • 書類ファイル：随時遠隔地にレプリケーション • ログ：随時レプリケーション アクセス権はデータベース、ログはインフラチームのみ、書類ファイルは基本的にインフラチームもアクセス権なし

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
29	データ管理	**バックアップデータを取得するタイミング(RPO)**	バックアップデータをとり、データを保証する時点	時間	データベースは IaaS 機能により当日 10 分前まで保証 ファイル、ログは随時レプリケーションしているので直前まで保証
30		**バックアップデータの保存期間**	データをバックアップした媒体を保管する期限	時間	バックアップはクラウド上に保持しており、外部媒体へは保管しておりません。 保存期限は以下の通りです。 ・ データベース : 7 日間 ・ ログについて : 2 年間保管 サービスの性質上、書類ファイルについては無期限に保存いたしております。
31		**データ消去の要件**	サービス解約後の、データ消去の実施有無／タイミング、保管媒体の破棄の実施有無／タイミング、およびデータ移行など、利用者に所有権のあるデータの消去方法	有無	一部有 データベース、ログは保管期間経過後に削除 書類ファイルは契約書という性質上、削除なし
32		**バックアップ世代数**	保証する世代数	世代数	データベースは 8 世代 書類ファイル、ログは基本的に世代なし
33		**データ保護のための暗号化要件**	データを保護するにあたり、暗号化要件の有無	有無	有 書類ファイルは AES-GCM で暗号化して保存しております。
34		**マルチテナントストレージにおけるキー管理要件**	マルチテナントストレージのキー管理要件の有無、内容	有無／内容	無 ストレージの分離は行なっていません。 アプリケーション側でアクセス制御を行なっています。
35		**データ漏えい・破壊時の補償／保険**	データ漏えい・破壊時の補償／保険の有無	有無	有 利用規約に保証について記載がございます。
36		**解約時のデータポータビリティ**	解約時、元データが完全な形で迅速に返却される、もしくは責任を持ってデータを消去する体制を整えており、外部への漏えいの懸念のない状態が構築できていること	有無／内容	有 解約時には書類ファイルの一括ダウンロードが可能です。 サービスの性質上、書類ファイルの削除は行っておりません。契約締結相手からは引き続き閲覧可能です。
37		**預託データの整合性検証作業**	データの整合性を検証する手法が実装され、検証報告の確認作業が行われていること	有無	有 書類ファイルについては電子署名の付与により改ざんされていないことを担保しております。
38		**入力データ形式の制限機能**	入力データ形式の制限機能の有無	有無	有 アップロードされるファイルは適切な PDF 形式のデータである必要があります。
39		**データの外部保存方針**	データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する制約条件を把握しているか	把握状況	データは AWS の国内リージョンに保存しております。 AWS との契約においては準拠法を日本法に変更する契約を行なっています。
40	セキュリティ	**公的認証取得の要件**	JIPDEC や JQA 等で認定している情報処理管理に関する公的認証（ISMS、プライバシーマーク等）が取得されていること	有無	有 ISMS 認証を取得しております。 詳細は以下をご覧ください。 https://isms.jp/lst/ind/CR_JP16_x002F_080413.html
41		**アプリケーションに関する第三者評価**	不正な侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ていること	有無／実施状況	有 外部企業による脆弱性診断を半期に一度実施し、指摘事項について対応しております。
42		**情報取扱い環境**	提供者側でのデータ取扱環境が適切に確保されていること	有無	有 運用者は限定されております。
43		**通信の暗号化レベル**	システムとやりとりされる通信の暗号化強度	有無	有 ユーザーとサービス間の通信は TLS1.2 以上を利用しております。

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
44	セキュリティ	**会計監査報告書における情報セキュリティ関連事項の確認**	会計監査報告書における情報セキュリティ関連事項の監査時に、担当者へ以下の資料を提供する旨 「最新の SAS70Type2 監査報告書」 「最新の 18 号監査報告書」	有無	有 SOC2 Type1 に対応しております。 詳しくは以下をご覧ください。 https://www.bengo4.com/corporate/news/article/h_lxvax8oscz
45		**マルチテナント下でのセキュリティ対策**	異なる利用企業間の情報隔離、障害等の影響の局所化	有無	無 データベースやサーバーのテナントごとの分離は行っておりません。 アプリケーションレベルでアクセス制御を行っております。
46		**情報取扱者の制限**	利用者のデータにアクセスできる利用者が限定されていること 利用者組織にて規定しているアクセス制限と同様な制約が実現できていること	有無／設定状況	有 クラウドサインではチームの管理者権限の付与により限定しております。
47		**情報取扱者の行動把握**	情報取扱者が不審な行動をした際、検知できるか	有無／設定状況	有 管理者によるパスワード変更等の通知はございますが、書類のダウンロード等は通常機能であるため通知はございません。
48		**ネットワークのセキュリティ対策**	ファイアウォールでの侵入遮断、IDS での侵入検知などの対策を行っているか	有無／設定状況	有 FW でポートを制限、合わせて WAF を導入しております。
49		**セキュリティインシデント発生時のトレーサビリティ**	ID の付与単位、ID をログ検索に利用できるか、ログの保存期間は適切な期間が確保されており、利用者の必要に応じて、受容可能に期間内に提供されるか	設定状況	ID は個人に付与されており、ログ検索に利用可能です。 ログは 2 年間保存しております。 ログの提供について、ビジネスプランではクラウドサインのサービス上で監査ログを出力する機能をご用意しております。取得可能なログ範囲や取得可能期間など詳しくはこちらをご覧ください。 https://help.cloudsign.jp/ja/articles/5264188
50		**ウイルススキャン**	ウイルススキャンの頻度	頻度	以下のようになっております。 サーバ → ウイルス対策ソフト導入なし 運用者端末 → 随時スキャン
51		**二次記憶媒体の安全性対策**	バックアップメディア等では、常に暗号化した状態で保管していること、廃棄の際にはデータの完全な抹消を実施し、また検証していること、USB ポートを無効化しデータの吸い出しの制限等の対策を講じていること	有無	有 バックアップはクラウド上に保持しており、持ち出し可能な外部媒体への保管は行わないようにしております。