電子契約クラウドサービス

DocYou

セキュリティホワイトペーパー

日鉄日立システムソリューションズ株式会社

1. 目次

2. はじめに

DocYou は、複数企業にまたがる多様な取引書類を 1 つのプラットフォームで相互連携するクラウドサービスです。電子契約をはじめ、電子取引・書類配信・ドキュメント管理など、企業間取引のさまざまな書類業務をサポートします。各企業が保有する基幹システムと連携することで、部門レベルからエンタープライズレベルまで幅広い取引業務の DX を推進します。

本サービスを利用する際には、ご利用のお客様自身もクラウドサービスの特徴を踏まえたセキュリティ対策の実践が必要になります。「DocYou セキュリティホワイトペーパー」（以下「本ドキュメント」といいます）は、お客様がクラウドサービスを選定する際に有用な情報をご提供すると同時に、お客様が利用できるセキュリティ関連機能についても記載しています。DocYou を利用することで、安全な取引業務を行うことが可能となります。なお、個別の機能の仕様については DocYou の HP（https://docyou.nhs.co.jp/）をご参照ください。

1. 本ドキュメントは、日鉄日立システムソリューションズ株式会社（以下「当社」といいます）が情報提供のみを目的として作成したものです。

2. 本ドキュメントは、本ドキュメントを作成した時点における当社の見解を反映したものです。本ドキュメントの内容は事前の予告なく変更されることがあります。

3. 本ドキュメントのいかなる内容も、当社の保証、表明、義務、確約等を意味するものではなく、本ドキュメントの内容の正確性、特定の目的への適合性を含め、当社は、本ドキュメントに関するいかなる保証も行いません。また、当社は、本ドキュメントの利用により生じたいかなる状況についても、その理由の如何を問わず、一切の責任を負いません。

4. 当社と DocYou のお客様との間の契約条件は、「DocYou サービス利用規約」等に定めるとおりであり、本ドキュメントはその一部とはなりません。また、本ドキュメントによって当該契約条件が変更されることもありません。

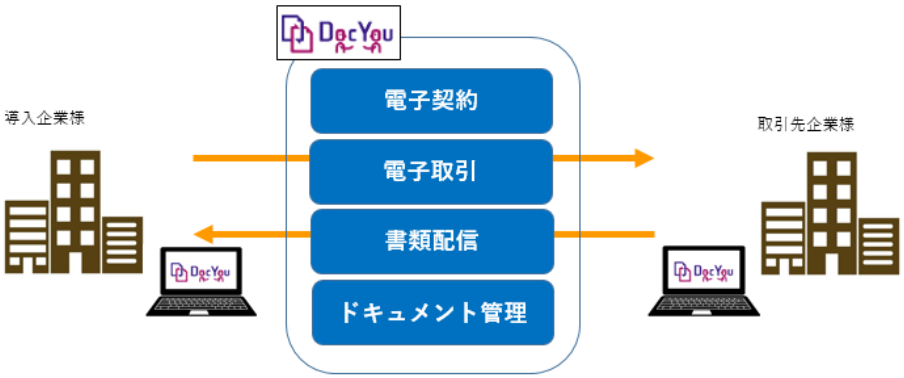
5. 本ドキュメントの内容の全部又は一部を無断転載することを禁じます。

6. 本ドキュメントに掲載されている会社名、製品名などは、それぞれ各社の商標、登録商標、製品名です。

3. DocYou とは

a. DocYou の仕組み

DocYou は、企業間取引で必要となる 4 つの機能（電子契約、電子取引、書類配信、ドキュメント管理）を 1 つでカバーしており、さまざまな契約書類を統合的に一元管理できるクラウドサービスです。



4. DocYou におけるセキュリティの考え方

a. クラウドセキュリティの基本的な考え方

クラウドセキュリティを考える際には、サービスの提供者がどのようなセキュリティ対策を実施しているかと、お客様がクラウドサービス上でどのようなセキュリティ対策を実施するかとの両方について考える必要があります。両者は相互に影響を与えています。

また、クラウドセキュリティを保つには技術的な対策によるものだけでなく、規約等による制限も含まれます。お客様はクラウドサービスの利用に際して、どのようなことができるのかを利用規約などから把握する必要があります。

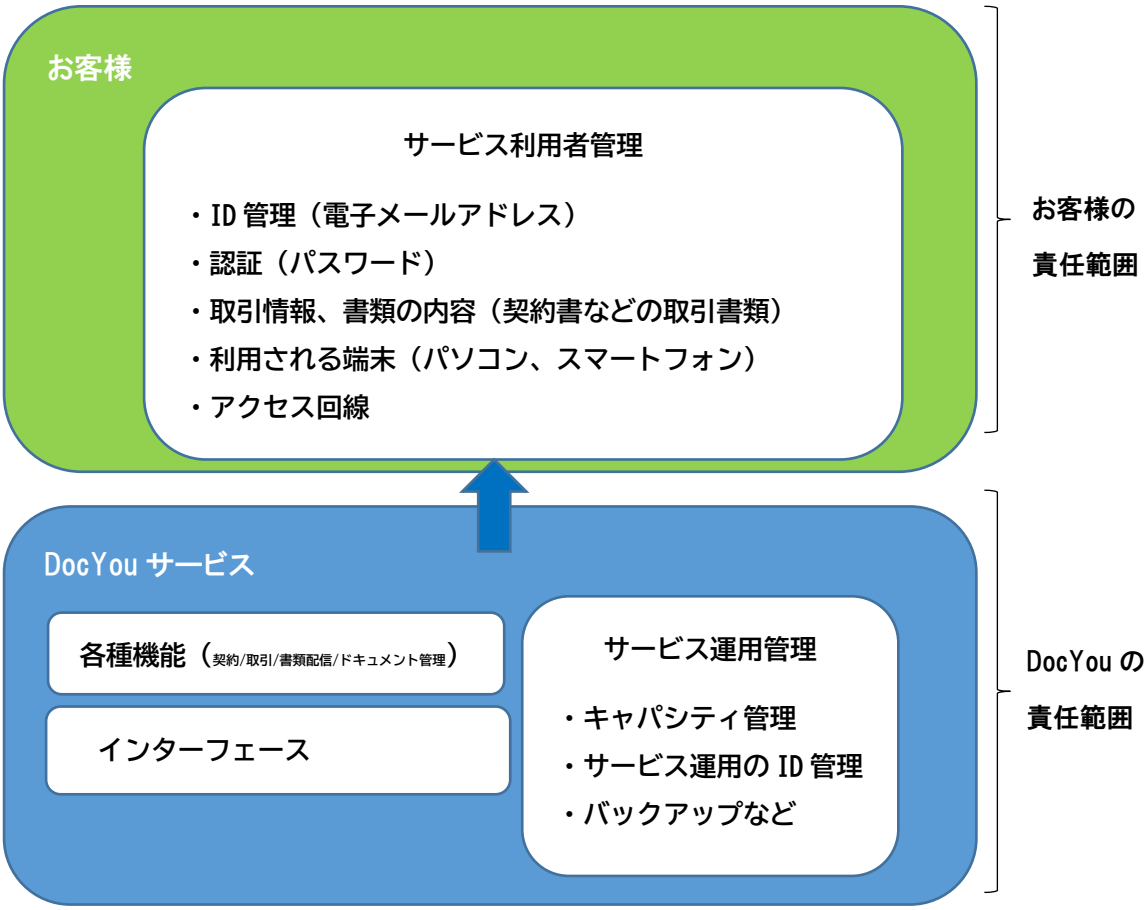
このような互いのセキュリティ対策の適切な実施のために、相互で役割と責任の理解の上、セキュリティ対策の実践が必要であるという考え方は「共同責任モデル（Shared Responsible

Model）」と呼ばれており、経済産業省の「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」及び「クラウドセキュリティガイドライン活用ガイドブック」にて解説されています。

本章では、共同責任モデルに基づいた DocYou での当社とお客様の役割と責任について解説し、DocYou におけるセキュリティ対策の概要を紹介します。

b. DocYou におけるセキュリティの基本的な考え方

DocYou は、以下の通り各種機能をサービスとして提供、責任を有しています。



お客様が DouYou のサービスを利用して登録したデータは、お客様が任意に変更・削除できます。DocYou の利用についてはお客様の責任となります。当社は、登録されたデータを、その内容については関知しない情報として扱います。DocYou の利用にあたっては、お客様によるリスクアセスメントを踏まえ、本ドキュメントを参考に必要な対策を検討し、実施してください。

5. DocYou におけるセキュリティ対策

a. 概要

本項では、当社が DocYou の継続的なサービス提供にあたり、実施しているセキュリティに関する情報を述べています。当社は、マルウェア感染からサイバー攻撃まで様々な脅威を考慮してサービス提供環境を構築し、継続的な見直しを行っております。

また、情報セキュリティマネジメントシステム（ISMS）の規格である、「JIS Q 27001:2023（ISO/IEC27001:2022）」や「JIS Q 27017:2016（ISO/IEC 27017:2016）」の第三者評価認証制度によるクラウドサービス提供の認証の取得等、信頼できる第三者による審査を積極的に活用しています。

DocYou では DocYou サービス及び、書類データやお客様の登録データの保護を行っています。本ドキュメントで述べている内容は、DocYou で実施しているセキュリティ対策の一部を記載しています。”附属 A：ISO/IEC 27001 Annex A との関連について”においては、ISMS における箇条に対する本ドキュメントの対応内容を示しています。

より詳細な情報をご希望の場合には DocYou の導入相談窓口へお問い合わせください。ただし、お問い合わせの内容によっては、開示をお断りする場合もありますので、あらかじめご了承ください。

ご相談窓口 https://docyou.nhs.co.jp/inquiry

b. 所在地と法管轄

DocYou は、日鉄日立システムソリューションズ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。当サービスの開発、運用は全て日本国内で行っています。

本システムは、Microsoft 社が提供する Azure 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 Azure の管理するデータセンターに保管されています。Microsoft 社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、DocYou では東日本リージョンにて稼働・データ管理をしています。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、書類データの管理はすべて国内のリージ

ョンを利用しており、データのアクセスについては東日本又は西日本リージョンが利用されます。日本マイクロソフト社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。一方、DocYou の操作に関するお問い合わせなどのサポート対応情報（お客様の連絡内容・対応履歴等）については、当社が利用するクラウドサービスの仕様により米国拠点に保存される場合があります。

c. サービス構成

i. 概要

DocYou は書類データやお客様の登録データの機密性、完全性、可用性を意識した設計及び、サービス提供を行っています。また、登録されるデータは、複数のお客様の情報が分類されるデータベース設計となっています。

ii. 機密性

サービス利用中の書類データやお客様の登録データの削除、もしくはサービス利用解除の際には、DocYou サービス及び、それを構成する機器および利用クラウドサービス等からデータの漏洩が生じないような防止策を導入しています。サービスインターフェースに対しては不正アクセス等の対策を実施しています。

iii. 完全性

DocYou は、保存した取引書類に対して、データを保護し、厳重管理しています。DocYou は、マルウェア等の不正プログラムによる被害を防ぐため、開発及び、運用で使用する機器およびクラウドサービスについて、ウイルスチェック・脆弱性チェックなどのセキュリティ対策を実施しています。インシデントが発生した場合は、定められた手順に従って報告、調査、駆除を行い、再発を防止します。

iv. 可用性

DocYou では書類データやお客様の登録データを Microsoft 社によりレプリケーションされており、アプリケーションも含め、いずれも Azure の東日本リージョンにて管理されています。DocYou は、障害が発生した場合に、Azure の西日本リージョンに切り替えることで DocYou サ

ービスを復旧する手順を定めています。このように DocYou は、Microsoft 社の多重化構造により可用性を担保しています。

また、その他障害発生時の回復についても手順を定めています。DocYou では事故・災害時に備えて責任者や役割、対応手順等をまとめたマニュアル類を策定しています。また、大規模な事故・災害を想定した訓練も実施しています。

d. サービス管理

i. サービスの運用体制

DocYou では、サービス提供に携わる要員を適切に育成しています。その中には、順守すべきセキュリティルールや最新のセキュリティ動向／対策等を反映した教育等も含まれます。

また、DocYou サービス本体を始めとした関連情報システムを利用する従業者を限定した上で、権限を設定しています。アカウント管理（発行、削除、棚卸し等）、パスワード管理及び、これに関連するルールを策定しています。

さらに、情報システムにアクセスした各種ログを一定期間保存することで、不正防止やインシデント発生を防止しています。社内ルールに基づいた情報システムの操作や運用管理等をまとめた文書類を策定、保管、見直しています。また、マニュアル類についてはバックアップを行っています。

当社では、ファイルのコピーや盗難等を防ぐために、保存先のアクセス制限やパスワードによる認証を行っています。認可されていないデータのコピーや盗難等を防ぐために、情報資産を重要度に応じて分類し、ストレージや通信の暗号化を行う等により、適切に管理しています。

また、当社運用・開発環境とサービス実行環境との通信を暗号化することで盗聴による漏洩防止策を行っています。情報または情報通信の保護に暗号化を用いる場合は、CRYPTREC 暗号リストに準じた強度の暗号技術を用いています。DocYou の運用管理時には、緊急対応で社外・在宅で対応を行う場合も含め暗号化通信による機密性を保持した通信を行っています。

DocYou は、お客様が個別にクラウド上に保存している情報資産の分類、ラベル付け等の管理機能は提供していません。お客様は、自身の責任で情報資産を分類、ラベル付け等の管理策及び、

後述の「6. DocYou ユーザーのためのセキュリティ関連機能」を活用して適切な情報管理・漏洩対策を実施してください。

ii. サービスの継続的な開発及び提供

DocYou は、中長期のロードマップに基づいてシステムを開発しています。立案した開発計画は、責任者によって確認と承認がなされています。

DocYou では、本番システムのセキュリティを維持するため、複数の環境を保有しています。セキュリティ管理の方針、及び、実装や運用で考慮すべき要件を定めて、設計段階から品質を確保するためのプロセスを実施しています。システム開発に際しては、標準化や自動化に取り組みつつ、仕様書に基づいた開発とテストを行っています。テスト工程では検証環境と稼働環境との整合性を確認しています。また、ウイルスチェック、脆弱性チェックなどを実施しています。

DocYou サービス本体などの情報システムの変更に際しては、変更管理を行っています。また、定型的変更作業については、作業手順書に従って実施しています。変更機能に加えて既存機能のテストを実施し、影響度の検証、障害の有無を検証することで、機能変更時の品質を確保しています。

定常運用におけるオペレーションや監視、チェック機能については、必ず複数名が多面的にチェックを行います。また、プログラムによる自動化等により品質を確保しています。

なお、サービスのリリース及び、エンハンスに関する情報は、事前に関連部門と共有した上で適切に実施しています。

iii. システムライフサイクル

DocYou ではシステム構成サービスの変更に際して、機能もしくは性能に関して評価をした上で実施しています。また、サポート契約、ベンダーとのリレーションシップ、バージョン管理を含むシステムの運用管理を実施しています。

システム実行環境・リソースの廃棄の際には、不正防止、機密保護対策を含めた計画、手順を策定しています。

iv. ネットワーク管理

DocYou ではネットワークセキュリティ方針に従い Azure 内にネットワークを構築しています。DocYou のサービス管理機能については必要な通信のみを許可し、ウイルス対策ソフトや不正アクセス検知装置、迷惑メールフィルタ等の技術的な対策を Azure のマネージドサービスを利用することで実現しています。

DocYou はインターネット上に公開されています。利用についての通信は適切に暗号化されますが、アクセスする端末のセキュリティについてはお客様にて適切に保護を実施してください。

v. 暗号化

1） 暗号による保護

DocYou では通信及び保存データを暗号化技術によって保護しています。暗号化技術については CRYPTREC 暗号リスト（電子政府推奨暗号リスト）を参照し、適切な暗号化技術でシステムを構成しています。また、暗号に関する輸出入規制に抵触することが無いよう配慮しています。

2） 通信の暗号化

DocYou では、CRYPTREC の「TLS 暗号設定ガイドライン」の推奨セキュリティ型の要求設定を参照して、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。また、サーバー証明書についてもパブリック認証局から安全性の高いものを入手し、利用しています。

3） 保存データの暗号化

DocYou では書類データ及びお客様の登録データを Azure 内のストレージサービスに保管することで、透過的に暗号化を行い、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。また秘密鍵・アクセスキー等の情報は Azure Key Vault を利用して厳重に管理しています。

vi. 認証情報の管理

DocYou の認証情報は Azure Active Directory B2C（Azure AD B2C）を利用し、厳重に管理しております。また、個別のご契約により SSO（シングルサインオン）機能を利用いただく事も可能です。

vii. バックアップ

DocYou では書類データ、お客様の登録データを Azure 内のストレージサービスに保管し、7日間のバックアップと、地理冗長オプションによる継続的な遠隔地へのレプリケーションを行っております。サービスに障害が発生した場合でも、レプリケーションよりサービスの復旧を行う事ができるよう備えています。

viii.監視の実施

DocYou は、DocYou サービス利用における各クラウドリソース（仮想マシン、ストレージ、仮想ネットワーク）、システムの性能・API などサービス全体に対する監視を実施しています。DocYou は、異常を迅速に検知・通知する監視機能を実装しています。

ix. キャパシティ管理

DocYou は、システムの性能及び、キャパシティ管理のプロセスを定めております。その中には監視対象、監視内容、監視方法が含まれ、管理表等のドキュメントを策定し、運用しています。また、監視から得られた情報や過去の動向などを基にして、コンピューティング資源の増強のためのプロセスを定め、監視により得られた情報などを基に随時増強を実施することで、書類データやお客様の登録データのためのコンピューティング資源の枯渇を未然に防ぎ、お客様がオンデマンドでデータの登録や管理をできるようにしています。

x. インシデント管理

DocYou では、DocYou サービスに対する監視や、JPCERT 等の外部機関からの情報提供に基づき、インシデント管理を行っています。インシデントの発生時には、手順に基づき関係者への情報伝達を行い、対処にあたっています。また、書類データやお客様の登録データに影響がある可能性があるインシデント、あるいはデータ侵害の可能性のあるインシデントの発生時には、

DocYou のログイン画面に通知を行っています。通知は DocYou サービスにおけるサービス障害のほか、お客様が禁止事項に抵触した際の、DocYou 側での対応結果も含まれます。

お客様がご利用中の DocYou サービスにおいて SLA 判定基準に該当する障害発生を当社が確認してから 30 分以内の通知を目標とします。

障害の告知方法は、6.ⅲ「障害・お知らせ通知」にてお知らせしています。

また、DocYou では過去の障害情報を蓄積、分析することにより、障害の再発防止に継続的に努めています。

xi. 端末管理

DocYou は、マルウェア等の不正プログラムによる被害を防ぐため、開発／運用で使用する機器について、マルウェア対策、脆弱性チェックを含んだセキュリティ対策を実施しています。特に、悪意のあるコードを検知した場合の対応手順は明確化及び、ルール化しているため、これに従って報告、調査、駆除、再発防止を実施しています。さらに、開発・運用 PC（社外持ち出し PC を含む）はハードディスクを暗号化しています。

xii. 供給者関係

システムの開発や運用等で外部委託を行う場合は、事前に目的や範囲等を明確にしています。また、外部委託先の選定に際しては手続きを明確にし、委託業者を客観的に評価しています。委託業者の決定にあたっては、機密保護、安全運行等に関する項目を盛り込んだ委託契約を締結しています。

xiii.顧客データの取扱記録の保管

DocYou は処理者として管理者または処理者に代わり行った顧客データの取扱い記録を保管しますが、GDPR への対応は想定していません。

xiv. タイムスタンプと時刻の同期

DocYou のサービスでは、Azure の NTP により時刻同期がなされています。また、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、セイコーソリューションズ株式会社が提供する長期署名クラウドサービスを利用しています。長期署名（PAdES）により、電子データの改ざんを防止しています。

e. その他

i. 規約

DocYou を利用するためには、DocYou サービス利用規約への同意が必要となります。

サービス利用規約ダウンロード　https://docyou.nhs.co.jp/download/kiyaku

ii. コンプライアンス

当社は日鉄ソリューションズ株式会社のグループ会社として、社員一人一人の行動規範として定められた「グローバル・ビジネス・コンダクト」に沿ってコンプライアンス遵守の取り組みを継続して推進しています。

https://www.nssol.nipponsteel.com/corporate/conduct.html

また、内部監査を実施するためのルールを策定しており、年に 1 回、DocYou を含めた情報システムを対象に、内部監査を実施して予防・是正に取り組んでいます。

DocYou では、お客様による直接の監査要求は受け入れていません。インシデント発生時には内部監査を実施し、その結果を開示できるようにしています。お客様が監査を受ける際に、DocYou からの情報提供が必要な場合は、あらかじめ個別にご相談ください。

その他、DocYou では、グレーゾーン解消制度（※）の照会を行い、デジタル庁・総務省・法務省・財務省から得た回答により、記名押印に代わる有効な電子署名として適法性を有することを確認いたしました。これにより、官公庁および地方公共団体との契約等においても DocYou を安心してご利用いただけます。

・20220314_policies_digitalsign_grayzone1_responses_02.pdf (cio.go.jp)

・220427_yoshiki1.pdf (meti.go.jp)

iii. 利用契約終了後の措置

解約その他の事由により利用契約が終了した後、DocYou は、サービス利用契約の終了日までにお客様の責任において登録済みのデータをダウンロードするもととし、サービス利用契約の終了日翌日以降 30 日（暦日）以内にお客様の登録データを削除します。サービス利用契約終了日の翌日以降において DocYou はお客様の登録データについて一切の責任を負わないものとします。

6. DocYou ユーザーの為のセキュリティ関連機能

本章では、お客様が DocYou を活用する際に役立つセキュリティ関連機能・サービスを紹介します。個々の機能・サービスの仕様については DocYou のホームページを参照してください。

機能紹介　https://docyou.nhs.co.jp/system

a. ログイン画面

DocYou のコントロールパネルへログインする際には、DocYou ID 及び、パスワードが必要です。DocYou ID 及び、パスワードはお客様自身で適切に管理してください。パスワードの変更はユーザーメニュー画面から行うことができます。パスワードの設定については DocYou で定められた複雑性の要件を満たす必要があります。なお、DocYou ID では、第三者による不正なログインを防ぐために、ID/パスワードの認証に加えて SMS によるワンタイム PW 認証を追加して多要素認証にすることが可能です。

b. ユーザー管理

DocYou ではユーザー管理画面よりお客様自身でアカウント内のユーザーについて追加・削除を行い適切に管理してください。新規ユーザーの追加及び削除は管理者権限のあるアカウント内のユーザーにて行う事が可能です。

c. 権限管理

DocYou ではアカウント内で管理者と一般ユーザーで権限を分けることできます。社外との契約・配信操作をできるユーザーを限定できます。また、普段は通知メールを受け取らない設定をしている一般ユーザーに対しても、特定の契約に対する送信依頼／承認依頼の通知メールを送ることができます。このように、お客様の業務に応じた柔軟な権限設定が可能です。

d. データへのアクセス権限

アカウント内のユーザーデータと書類データは、アカウントに紐づいたキー毎に、厳密にストレージに保管されています。管理者ユーザーはアカウント内のすべてのユーザーデータ・書類データにアクセスすることができます。一般ユーザーにつきましては、一部のユーザーデータへのアクセスが制限されます。すべての書類データについて閲覧ができますが、その操作は権限毎に制限されます。また、ご契約のプランによっては、アカウント内のユーザー毎の閲覧レベルと書類データの閲覧レベルを設定することで、ユーザー毎の書類アクセスを管理することができます。

電子契約・配信により取引先のアカウントに書類を送付した場合は、両アカウントのユーザーが書類にアクセス可能になります。各書類データへのアクセスは必ず当該書類を管理するアカウントへのログインが必要になります。通知メールに添付された URL や書類詳細画面に表示されるアクセス URL より書類データを閲覧するためには、かならず書類データが保管又は送付されたアカウントに対してのログインが必要となりますので、事前にユーザー追加を行っておく必要があります。

e. アクセスログ

ユーザーがアカウントにログインした情報はログイン履歴として記録され、8 年間保管されます。その他のアクセスログに関しましては、3 年間保管されますが、お客様に開示はいたしません。お客様のインシデントにより調査が必要な場合には DocYou のお問い合わせ窓口までご連絡ください。

f. お客様側でのバックアップ

書類の参照やアップロードの権限が付与されているお客様は、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ご利用ください。

g. メンテナンス及び各種通知

i. 通知について

DocYou では、お客様向けの情報として、メンテナンス・障害情報などのお知らせをトップ画面により通知しています。その他、新サービスの提供、仕様変更などについても、DocYou のトップ画面を通じて連絡しています。

ii. メンテナンスについて

メンテナンスの情報は、トップ画面に掲載します。掲載時期は、サービス停止日の5日（営業日）前までに、理由及び期間を表示します。但し、本サービスの運用上、緊急でやむを得ないときは、上記の限りではありません。

iii. 障害・お知らせ通知

障害・お知らせ通知は、DocYou で障害が発生した際、経過や復旧情報などを DocYou のログイン後のトップ画面にてご連絡するサービスとなります。また、メンテナンスなどのお知らせが発生した際も、同様にログイン後のトップ画面にてご連絡します。

h. 解約時のデータの扱い

お客様が DocYou のサービスを解約された場合、解約日まではお客様が入力したデータの参照や取引書類のダウンロードができます。必要に応じて、期間内にダウンロードを行ってください。DocYou は、解約日までにお客様の責任において登録済みのデータをダウンロードするもととし、解約から 30 日以内にお客様の登録データを削除します。これ以降において DocYou はお客様の登録データについて一切の責任を負わないものとします。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、書類データやお客様の登録データです。ただし、有効なお取引アカウントの書類データは解約後も残り、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。

i. セキュリティを向上する機能

i. マルチアカウント機能

DocYou をご利用中のお客様が、操作範囲に制限を持たせたアカウントを作成できる機能です。複数部門で利用される際はアカウントを分けることで、各部門担当者が確認できる書類の範囲を制限することができます。不必要な情報を排除することで業務効率化でき、閲覧や承認してはいけない情報の漏えいを防ぐ情報統制としても有効です。管理者や監査者、兼務者の場合は、各部門アカウントを横断して書類を確認できるよう、アカウントの切り替えが可能となるユーザー設定が可能です。

ii. SSO（シングルサインオン）機能

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ます。その場合、DocYou 側でパスワードを管理いたしませんので、シングルサインオンのために必要なパスワードはお客様にて適切に保護していただくようお願いいたします。

j. BCP（事業継続計画）における DocYou の位置づけ

i. 障害対応復旧計画

何らかの理由で DocYou のサービスが停止した場合、DocYou の側では復旧計画に沿ってサービスの復旧を試みます。DocYou では障害により Azure の単一のリージョンが停止しても、サービスの継続が提供可能な別リージョンでの復旧について、マネージドサービスの再構成を手順化しております。また、書類データ、お客様の登録データを Azure 内のストレージサービスに保管し、地理冗長オプションによる継続的な遠隔地へのレプリケーションを行っております。サービスに障害が発生した場合でも、レプリケーションよりサービスの復旧を行う事ができるよう備えています。

ii. 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別リージョンからの復旧を行います。復旧時の目標復旧時間（RTO）は 6 時間としています。

※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。

iii. お客様による代替措置

お客さまが BCP（事業継続計画）を立案する際、DocYou 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一括ダウンロードが可能です。ダウンロードした書類は、当サービスが終了しても利用者の手元に残ります。DocYou 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。

7. お客様にご注意いただきたい点

a. サービスの利用に必要な環境とソフトウェア

DocYou 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、携帯電話が必要です。ＳＭＳに対応した携帯電話をご準備願います。

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。

DocYou よくあるご質問　https://docyou.nhs.co.jp/faq

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。2023 年 6 月現在、DocYou 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 DocYou 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。

b. お客様の環境におけるセキュリティ上の注意点

DocYou 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。DocYou 側のアプリケーションについては、DocYou 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
- 電子メールへのマルウェア対策

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、DocYou 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、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

c. お客様のパスワード管理

DocYou 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。

i. 安全なパスワードの設定

DocYou では、お客さまが自身でパスワードを設定します。自分や家族の名前、辞書に載っている単語、同じ文字の繰り返しや分かりやすい並びの文字列、短すぎる文字列を避けてください。パスワードの設定ルールにつきましては、DocYou に規定されていますので、マニュアルをご確認ください。

ii. パスワードの保管方法

パスワードは他人には教えず秘密にしてください。また、複数人で共有をしないでください。電子メールでのやりとりや、他人の目に触れるところへの記録をしないでください。パスワードを記録する場合は、パスワード管理ツール等を利用してください。万が一、パスワードが漏洩したときには、ただちに変更してください。

iii. パスワードを複数のサービスで使いまわさない

他のサービスから流出したパスワード情報により、DocYou に不正にログインされる可能性があります。

d. お客様によるインシデント報告とご連絡・ご依頼

お客さまが DocYou 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 DocYou のお問い合わせ窓口までご連絡ください。

i. 通常の連絡先

本サービスのサポートデスク（お問い合わせ窓口）は以下の通りです。

サポートデスクでは、操作、障害、情報セキュリティインシデント等問わず、トータルに受付を行います。

■お問い合わせ先　docyou-support@nhs.co.jp

ii. セキュリティに関する緊急連絡先

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。DocYou をご利用でない外部の方が DocYou 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。

■お問い合わせ先　docyou-support@nhs.co.jp

iii. ログ調査

お客さま側でのインシデント調査のために、DocYou のログの調査が必要になるケースが考えられます。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。

改定履歴

1.0　2023 年 6 月 1 日　初版

1.1　2023 年 7 月 1 日

1.2　2024 年 7 月２４日

1.3　2025 年 6 月２５日