

セキュリティ 概要書

CONTRACT **CROSS**
企業をつなぐ電子取引プラットフォーム。

日鉄ソリューションズ株式会社

2025 年 10 月 1 日

目 次

1. はじめに.....	2
2. 組織及び人的セキュリティ	2
3. データに対するセキュリティ	3
4. サービスの開発・運用に関するセキュリティ	4
5. インシデントに対する対応	5
6. コンプライアンス	5
7. 取得している認証制度	6

1. はじめに

日鉄ソリューションズ株式会社（以下、当社）は、クラウドサービスの提供及び利用における情報セキュリティ水準を維持向上させるため、さまざまな取り組みを行っております。

当セキュリティ概要書では、当社が提供する CONTRACT CROSS のサービスに対するセキュリティ施策について説明いたします。本サービスは電子取引・電子契約サービスプラットフォームです。さまざまな形式の電子取引・電子契約に対応しており、契約書や請求書など関連する書類のやりとりをデジタル化することが可能です。

2. 組織及び人的セキュリティ

- 本サービスでは、情報セキュリティ方針及びクラウドサービス情報セキュリティ基本方針を定め、方針に従いサービスを提供しております。
- 本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ございます。具体的な内容については利用規約をご参照ください。お客様の責任範囲が記載されております。
- 当社の所在地は東京都です。本サービスが取り扱うデータは全て国内に保存されております。
- 当社ではセキュリティ教育及び訓練を定期的を実施し、セキュリティ意識の向上に努めております。

3. データに対するセキュリティ

- 利用者が本サービスの利用を終了した場合のデータ削除については利用規約に基づき処理いたします。内容をご参照ください。
- グループ管理機能では、ユーザーの追加・管理者権限・ロールの設定が可能です。詳細については、サービスマニュアルをご参照ください。
- お客様のアカウント管理者について、ログイン ID、パスワード認証によるセキュリティ対策を提供しております。アカウント管理者は他のユーザーにはない特権を有しておりますので、お客様の責任で適切に管理をお願いいたします。
- お客様のアカウント管理者はユーザーのアクセス権限をロール割り当てなどにより管理することが可能です。サービスマニュアルをご確認のうえ、適切に設定をお願いいたします。
- 利用者に対し、セキュリティ手順を回避し各種サービス機能の利用を可能とするユーティリティプログラムの提供は行っておりません。
- 通信データや保存データは暗号化により保護されております。暗号鍵は本サービスにおいて適切に管理いたします。
- 記憶媒体を内蔵したサーバー等の装置を処分する場合は、情報を完全に消去し、復元不可能な状態で処分いたします。
- 地震・台風などの自然災害に対応するため、本サービスに使用する機器は必要な対策が講じられたデータセンターに設置しております。

4. サービスの開発・運用に関するセキュリティ

- 提供するサービスの変更やお客様に大きな影響が生じる作業の場合、利用規約に基づき、メール又はお客様への直接連絡、HP 若しくは本サービスログイン後のお知らせのいずれかの方法で事前に通知いたします。ただし、利用規約に定める提供対象時間外の場合を除きます。
- 安定的なサービス提供を行うため、各サーバーのリソースを監視し、必要に応じてキャパシティの増強を行っております。
- 管理者向け機能の操作方法は、サービスマニュアルをご参照ください。
- 本サービスでは、バックアップデータを東日本の複数データセンターへ保管しております。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おります。
- 本サービスでは、操作ログの出力機能を提供しており、文書の各種操作情報を出力し確認することが可能です。詳細はサービスマニュアルをご参照ください。
- 本サービスでは各サーバーおよび各アプリケーションにおいて時刻を日本標準時間に同期しております。
- 本サービスでは基盤システムが取得しているログを定期的に確認し、アクセス侵害が発生していないことを確認しております。また、WAF やログのパターンマッチによる自動監視を行っております。
- 本サービスでは継続的に脆弱性情報の収集を実施いたします。弊社とお客様で共有すべき技術的脆弱性情報については、適宜お客様へもご提供いたします。
- 本サービスが提供するクラウドサービスは、アプリケーションによる制御にてデータを分離・保護する形態で情報セキュリティの確保を行っております。また、お客様のご要望により環境を論理的に隔離する形態でのサービス提供が可能です。
- 本サービスでは、セキュリティに配慮した開発手順を定め、定期的に内部・外部による脆弱性診断やネットワーク診断を行っております。
- 本サービスでは、本サービスが利用するクラウドサービスプロバイダの情報セキュリティ水準を把握し、本サービスの情報セキュリティ水準を満たしていることを確認しております。

5. インシデントに対する対応

- お客様に影響を与えるセキュリティインシデント（データの消失・漏洩、システム停止等）が発生した場合は、利用規約に基づき速やかに通知を行います。
- セキュリティインシデントやセキュリティに関する問合せは、サポートデスクにて受け付けております。
- 本サービス関係組織では、サービス事業継続計画（BCP）を策定し、定期的に事業継続訓練を実施しております。大規模災害が発生した場合、サービスの目標復旧時間（RTO）は2週間以内、目標復旧時点（RPO）は1日前としております。

6. コンプライアンス

- 本サービスのクラウドサービスにおける準拠法は日本法となっております。関連法令を特定し、定期的に見直しを実施しております。
- 知的財産権に対する苦情、ご相談等については、サポートデスクで受け付けております。
- 本サービスでは、裁判所からの開示請求など、法律に基づいた正当な開示請求が行われた場合、お客様の同意なく、データを開示することがあります。詳細は、利用規約をご参照ください。お客様のサービスご利用に関して蓄積された記録に対しては、不正アクセス・改ざんなどを防ぐためアクセス制限を実施しております。また、利用規約に基づき蓄積された記録をサービス提供用途以外で利用しておりません。
- 本サービスではお預かりしたデータを法規制に合致する形で暗号化し、保管しております。

7. 取得している認証制度

- ISMS (ISO/IEC 27001:2022・JIS Q 27001:2023)
- ITSMS (ISO/IEC 20000-1:2018・JIS Q 20000-1:2020)
- プライバシーマーク (JIS Q 15001)
- JIIMA 認証
 - 電子取引ソフト法的要件認証制度
 - 電帳法スキャナ保存ソフト法的要件認証制度

改訂履歴

版	改訂日	改訂内容
1.0	2025/10/01	初版作成

NS (ロゴ)、NS Solutions、CONTRACT CROSS、CONTRACT CROSS (ロゴ) は、日鉄ソリューションズ株式会社の登録商標です。

本文記載の会社名及び製品名は、それぞれ各社の商標又は登録商標です。