COMPANY Core
セキュリティスタンダード（公開版）

公益財団法人 金融情報システムセンター
「金融機関等コンピュータシステムの安全対策基準・解説書（第10版）」対応

Version 2.00

2023/07/27

株式会社Works Human Intelligence

目次

1. 改訂履歴

Version	改版内容	更新日
1.00	新規作成	2020/08/31
1.01	「2.5 補足事項」の修正	2021/02/03
1.10	第9版令和2年3月版対応	2021/03/12
1.20	第9版令和3年12月版対応	2022/06/10
2.00	第10版	2023/07/27

2. COMPANY Coreセキュリティスタンダード概要

ここではCOMPANY Coreセキュリティスタンダードの目的、対象とする範囲、策定手順を解説します。

○2.1. 目的

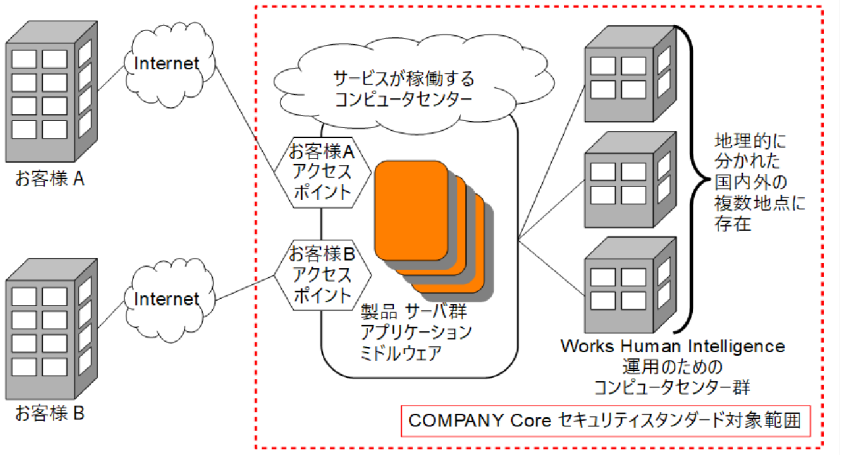
- お客様に製品の安全性について確認して頂くための情報を提供します
- COMPANY Coreクラウドサービスにおける安全対策の骨子を定めます

○2.2. 対象範囲

以下をCOMPANY Coreセキュリティスタンダードの対象範囲とします

- COMPANY Coreクラウドサービス
  アプリケーションのバージョンアップや PTF の適用を行う他、サービスが動作するサーバおよびサービスの提供に必要なミドルウェアの運用を行うサービスです

○2.3. 対象範囲イメージ



対象範囲イメージ

サービスはクラウド事業者が提供するコンピュータセンター (以下、サービスが稼働するコンピュータセンター) に構築されます。お客様はサービスを利用するために、インターネット経由でお客様用のアクセスポイントに接続します。

COMPANY Core クラウドサービスはWorks Human Intelligence及び業務の委託先の持つ運用のためのコンピュータセンター等から、リモート操作によって実施されます。運用のためのコンピュータセンターは地理的に分かれた複数地点に存在しています。

COMPANY Coreセキュリティスタンダードは COMPANY Coreクラウドサービスを対象とするため、サービスが稼働するコンピュータセンターおよび運用のためのコンピュータセンターが対象範囲となります。

○2.4. 策定方針

- 「金融機関等コンピュータシステムの安全対策基準」の考え方に基づきます
- Works Human Intelligenceのセキュリティポリシーに則ります
- ISO27001に基づいた情報セキュリティ管理を活用し、改善を図ります
- 弊社が必要と定めた社会的要求およびお客様の要望を必要に応じ
  COMPANY Core セキュリティスタンダードに反映します

○2.5. 補足事項

本COMPANY Coreセキュリティスタンダードはお客様に広く公開するために作成された公開版となります。正式な最新版の提供は以下が条件となります。

・弊社と秘密保持契約を結んだお客様。

・金融情報システムセンター「金融機関等コンピュータシステムの安全対策基準・解説書」を購入頂いているお客様。

詳細は弊社ウェブサイト記載のお問い合わせ先よりお問い合わせください。

3. 安全対策の概要

ここではサービスの安全対策の概要を解説します。

○3.1. 設備について

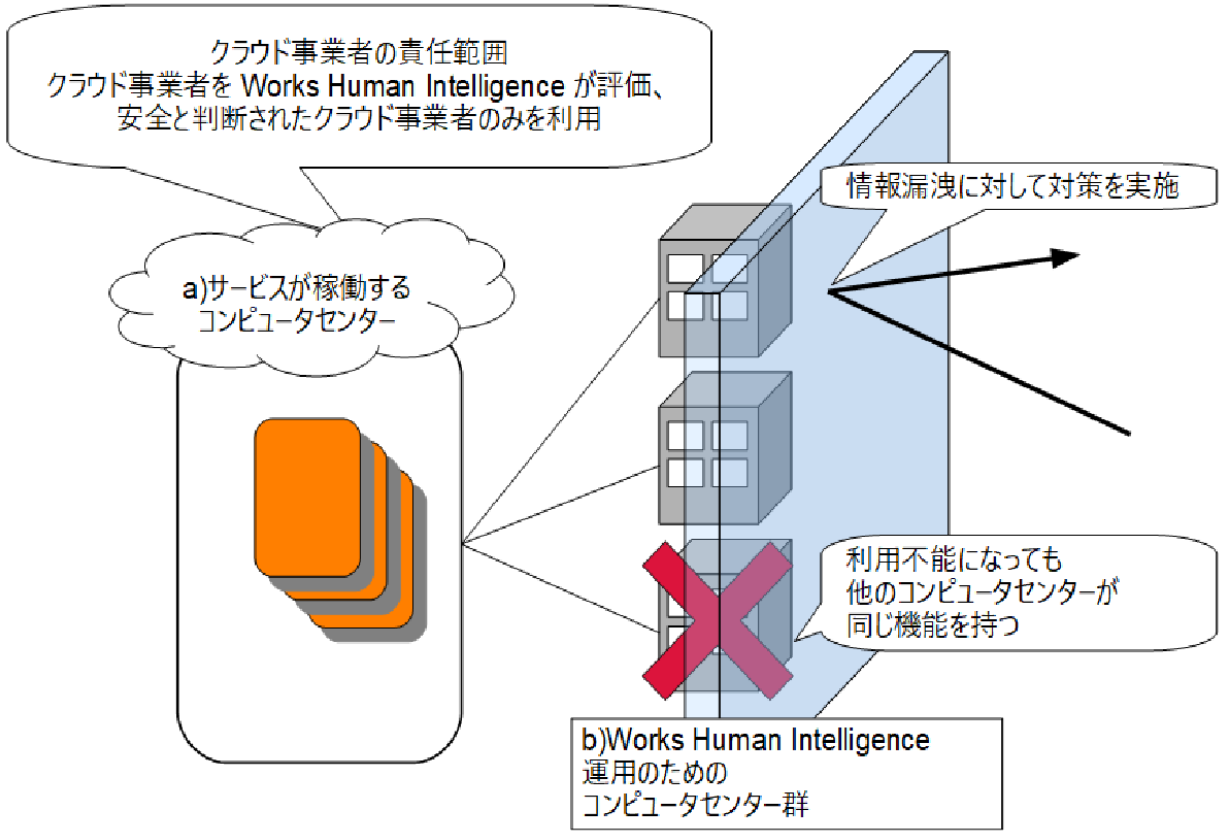
COMPANY Coreクラウドサービスに関係するコンピュータセンターは以下の2つです。

a) サービスが稼働するコンピュータセンター

このコンピュータセンターはクラウド事業者に安全対策の責任があります。Works Human Intelligenceはクラウド事業者が行う安全対策を確認し、安全であると判断されたクラウド事業者[1]を利用します。

b) 運用のためのコンピュータセンター

このコンピュータセンターはWorks Human Intelligence に安全対策の責任があります。コンピュータセンターは許可のない者は侵入できないようにし、情報の漏洩を防いでいます。さらに、コンピュータセンターが利用不能になった場合に備え、このコンピュータセンターは地理的に分離した複数拠点に同じ機能を持ったものを配置しています。これにより、コンピュータセンターは情報漏洩防止および事業継続性の両面から安全性を確保しています。



設備面の安全対策イメージ

[1] 判断方法については本書掲載の安全対策対応表で解説しています

○3.2. 運用について

COMPANY Coreクラウドサービスはそれぞれお客様が利用する環境とお客様の情報をWorks Human Intelligenceのオペレーターが操作するサービスです。この際に不正な操作が発生し、お客様の情報を破壊したり、漏洩してしまうことを防がなければなりません。

COMPANY Coreクラウドサービスのオペレーションは責任者から承認を受けた者のみが実施する権限が付与されるように制御されています。また、実施後は権限が剥奪されます。[2]

[2] 弊社が必要と判断した場合には 遠隔作業を行う場合がありますが、上記の承認手順は変わらず実施いたします
遠隔作業時も、WHI社内ネットワーク経由にてアクセスを行います
作業場所からの通信経路は暗号化されています。その他、詳細については安全対策対応表にてご確認ください

4. 金融機関等コンピュータシステムの安全対策基準・解説書への弊社およびクラウド事業者の対応

ここでは金融機関等コンピュータシステムの安全対策基準・解説書に対してCOMPANY Coreクラウドサービスを提供する弊社および、サービスが稼働するコンピュータセンターを管理するクラウド事業者がどのように対応するのかを解説します。

○4.1. なぜクラウド事業者の対応状況も確認するのか

COMPANY Coreセキュリティスタンダード概要の対象範囲で解説いたしました通り、サービスはクラウド事業者が管理するコンピュータセンター上で稼働しています。そのコンピュータセンターに対してWorks Human Intelligenceが持つ運用のためのコンピュータセンターからアクセスして管理・保守・運用を行います。

そのため、本セキュリティスタンダードのみではなく、クラウド事業者の対応状況も併せて参照する必要があります。各クラウド事業者の対応状況は各クラウド事業者が公表している資料をご参照ください。

○4.2. 対応状況表の見方

金融機関等コンピュータシステムの安全対策基準・解説書第九版改定からの引用	対応状況
項番	
項目を一意に識別する識別記号	本項目に対してCOMPANY Coreクラウドサービスを行う弊社がどのような対応を行うか

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用 基準番号	対応状況
統1	ISO27001を基準としたセキュリティに関する責任の分担、ポリシーおよび手順が確立されています。 同基準は運用業務の実態に合っているか定期的に見直しがされています。
統2	全社的に中長期的視点に立った計画の策定を実施しています。
統3	提供サービスの開発計画は、中長期のシステム化計画と整合性が取れており、技術調査を実施して、開発責任者の承認を得て、計画を作成しています。
統4	ISO27001を基準とした Works Human Intelligence のセキュリティポリシーで情報セキュリティの確保を目的として「情報セキュリティ委員会」を設置すると共に、情報セキュリティの責任者として情報セキュリティ管理責任者を選任するように定めています。
統5	クラウド事業者が提供する機能およびセキュリティ情報を追跡し、見直しや訓練、対策を実施しています。
統6	ISO27001の取り組みの一環で、管理する情報資産を情報資産管理台帳に定め、その資産に対してリスクの評価と対応策の策定を行っています。また、システム管理は Operation Manual に従い、整備しています。また、権限は互いに牽制ができるように付与されています。
統7	Operation Manual で管理対象となるデータおよびその管理手順を定めて管理体制を整備しています。管理体制についてはISO27001 管理策に基づき確認、評価しています。また、権限は互いに牽制ができるように付与されています。
統8	ISO27001の取り組みの一環で、「情報システム管理規程」および管理体制を整備しています。また、権限は互いに牽制ができるように付与されています。
統9	事業や、職務別（営業・開発・運用・コンサルタント）に組織が整備されており、それに合致するように権限が付与されています。また、権限は互いに牽制ができるように付与されています。
統10	災害時に、「事業継続管理規程」に基づき、対策本部を立ち上げる体制が整備されています。
統11	弊社として防犯組織を明確に規定はしていませんが、各種防犯対策は実施しております。
統12	情報セキュリティの確保を目的に、情報セキュリティ委員会を設置しています。その委員会にて、各種規定を整備しています。
統13	情報セキュリティが遵守されていることを点検するために、定期的に内部監査を実施しています。この監査による改善に加え、情報システムの変更や新たな脅威などの環境変化に対応した見直しを行い、継続的な改善を実施しています。 また、全役職員(派遣社員を含む)のセキュリティレベルの向上を図るために、周知徹底し、情報セキュリティの維持に向けて必要な教育を継続的に実施しています。
統14	全役職員(派遣社員を含む)に対して、入社入場時に加え、定期的なセキュリティ教育を実施しています。業務内容により、追加の教育も実施しております。
統15	当社製品の開発、運用および利用に携わる要員(外部委託要員を含む)に対して、担当する業務内容等に応じた社内教育を実施しております。
統16	ISO27001に準拠し、障害時・災害時に備えた教育・訓練を実施しております。
統17	非常時に備えて防災訓練を実施しております。
統18	人員毎のスキル評価を実施し、要員の配置、交替、権限分離等の人事管理を適時行っております。
統19	社内規程に従い定期的な健康診断および産業医による面談等を実施しております。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用 基準番号	対応状況
統20	プライバシーマークおよびISO27001 の管理策に基づき外部委託先の選定手続きを明確にしています。 外部委託先はホワイトペーパーおよび第三者機関による認証・レポート、提供している機能などで状況を確認、評価しています。
統21	プライバシーマークおよびISO 27001の管理策に基づき契約を締結しています。
統22	外部委託先には弊社と同等の安全対策を行うことを要求した委託契約を結んでいます。その中には同等の教育および監査が含まれます。
統23	外部委託先に委託した業務については、弊社内で評価・検証を行っております。
統24	お客様は弊社の統制について SOC1 報告書や本セキュリティスタンダードによってご確認頂き、安全対策を講じることが可能です。 お客様と弊社間の責任分界点はCOMPANY Coreクラウドサービス説明書に明示されています。 弊社では、お客様からのご依頼に基づき、接続元の制限やネットワーク設定等を行っています。 依頼内容の妥当性については、お客様側でのご確認をお願いしています。
統25	緊急事態発生時に弊社が行う対応計画についてはCOMPANY Coreクラウドサービス説明書に定められています。お客様はこれをご確認頂き、安全対策を講じることが可能です。
統26	サービスの提供に際して金融機関相互ネットワークは使用しません。
統27	金融機関等の口座と連携した決済サービスは提供しておりません。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用 基準番号	対応状況
設1	運用室が存在する建物はいずれも火災リスクが低い場所に立地しております。 また、建物が浸水しやすい場所に立地している場合は防水板を設置し、浸水を防いでおります。 また、運用室は全て予備が用意されています。
設2	運用室が存在する建物はいずれも都市部に立地しているため津波、高潮、出水等に見舞われにくい環境にあります。電波障害・鉄道による振動障害に関しても過去に情報機器に対して悪影響を及ぼした事例はありません。 また、運用室は全て予備が用意されています。
設3	運用室が存在する建物は迅速に避難できるようレイアウトを組んでおります。
設4	運用室が存在する建物はいずれも周囲の建造物との間に十分な間隔が確保されております。
設5	運用室が存在する建物は敷地境界においては入退管理を行っていません。
設6	運用室は外部にその所在を示す表示板・看板を出してはいません。
設7	運用室が存在する建物は避雷設備が設置されています。
設8	運用室は運用室が存在する建物内に作られた独立区画内に存在します。
設9	運用室が存在する建物で用いられている通信回線や電力線はそれぞれ断線・延焼のための処置が行われております。
設10	運用室が存在する建物はその建物が存在する地域の耐火性に関する建築基準に従って建てられた建物内に存在します。
設11	運用室が存在する建物はそれぞれ存在する地域の構造に関する建築基準に従って建てられています。
設12	運用室が存在する建物はそれぞれ防水加工が施されております。
設13	運用室が存在する建物はそれぞれ破壊行為などから防御可能な強度を持っています。
設14	運用室が存在する建物にある延焼の恐れのある窓には関係する法令に従って防火措置を施されております。
設15	運用室が存在する建物は侵入される恐れがある場合はそれぞれ常駐警備員の配置や防犯カメラによる監視などといった防犯措置が行われております。
設16	運用室が存在する建物において平時利用される出入り口は1つであり、電子錠が付けられております。電子錠は管理者が許可した者のみ開錠が可能です。また、各出入り口は防犯カメラが設置されており、入退室が撮影されております。
設17	運用室が存在する建物は適切な位置に非常口が設けられております。
設18	運用室が存在する建物の開口部には、防水処置が施されております。
設19	運用室が存在する建物はそれぞれ出入り口に電子錠が付いており、管理者によって許可された者にしか解錠ができません。ただし、防火措置や破壊行為への対策は取られておりません。
設20	運用室が存在する建物は内装壁に不燃材を用いています。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用 基準番号	対応状況
設21	運用室が存在する建物が地震リスクが高い地域にある場合、建物の天井・照明は全て吊り下げ金具とビス等で落下防止の固定によって地震による内装等の落下・損壊の防止措置を行っています。運用室が存在する建物が地震リスクが低い地域にある場合も、落下等が懸念される不安定構造物を設置しないことで地震による内装等の落下・損壊の防止措置を行っています。
設22	運用室は災害の際に大きな被害を受けやすい場所を避けて設置されております。
設23	運用室への入室には社内の部屋を通って入室する必要があり、出入口付近およびエレベータまたは階段で直接入れる位置を避けて実施しています
設24	運用室は部外者が確認可能な場所には室名などの表示はされていません。
設25	運用室は整理整頓や機器の積み上げ、通路への荷物の狭溢化がなされないよう社内で徹底することで必要空間を確保しています。
設26	運用室は独立した室となっております。
設27	運用室の出入り口は一か所のみです。前室はございません。
設28	運用室は出入り口に錠を設けた扉を設置していますが、扉は特定防火設備ではございません。
設29	運用室に配置された窓は防火・防水措置はとられておりません。2F以上にあるため、外部からの破損は防止されており、中を外部からのぞき込むことはできません。外ではなく執務室側に窓がある場合は執務室からは見えない角度で機器を配置しているため、中の機器を執務室から見ることはできません。
設30	運用室はいずれも災害時における避難経路が確保されております。
設31	運用室はそれぞれ独立した防火区画とはなっておりません。
設32	運用室には漏水防止対策が講じられています。
設33	運用室の床表面材料は静電気の発生や帯電などによる影響を防止する措置をとっていません。 ただし、運用室の筐体への直接変更を運用室内で行わないことで静電気や帯電による悪影響を避けています。
設34	運用室はそれぞれ内壁と天井および扉に不燃・防火材料を用いております。
設35	運用室が存在する建物が地震リスクが高い地域にある場合、建物の天井・照明は全て吊り下げ金具とビス等で落下防止の固定によって地震による内装等の落下・損壊の防止措置を行っています。運用室の存在する建物が地震リスクが低い地域にある場合も、落下等が懸念される不安定構造物を設置しないことで地震による内装等の落下・損壊の防止措置を行っています。
設36	運用室に配置されたフリーアクセス床そのものは耐震構造になっておりませんが、運用室が存在する建物が耐震構造となっております。
設37	運用室には自動火災報知設備が設置されております。
設38	運用室が存在している建物には非常時の為に非常用放送設備が配置されております。
設39	運用室が存在している建物には消火栓設備および消火器が設置されております。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用 基準番号	対応状況
設40	運用室で用いられているケーブルは絶縁措置や難燃化がされたものを用いております。また、運用室が存在する建物のケーブル貫通部は延焼防止措置が講ぜられています。
設41	運用室には排煙設備が設置されております。
設42	運用室が存在する建物は非常用照明装置が設置されておりますが、携帯用照明器具は設置されておりません。
設43	運用室には流し台、給湯室などの水を利用する設備はありません。
設44	運用室が存在する建物が地震リスクが高い地域にある場合、地震感知器が設置されており、地震時は地震放送が流れます。
設45	運用室の出入口の扉は管理者に許可された者のみ解錠が可能な仕組みになっています。また、防犯設備として出入り口の入退室を撮影する監視カメラを設置しています。
設46	運用室の温湿度は建物の集中管理室ないしは専用の監視設備によって監視・管理されております。
設47	運用室はそれぞれ衛生害獣防除や区画形成による侵入防止等といった手段によってネズミへの対策を行っております。
設48	運用室設置の什器には、一部木製の長机はございますが、基本不燃材ないしはスチール製の什器を設置しております。
設49	ビル衛生法管理法に準拠した湿度管理、加えて床置型加湿器等を設置し、静電気が生じない環境を構築しております。
設50	転倒リスクがある什器やコンピューター類は耐震措置が講じられております。
設51	運用室内に運搬車はありません。
設52	運用室が存在する建物の電源室および空調機械室は地震や浸水に強く、危険物貯蔵庫や火気使用設備と隣接しない場所に配置されているため災害を受ける危険性は少ないと判断しております。
設53	運用室が存在する建物の電源室および空調機械室はそれぞれ各地域の法規に従った空間が確保されております。
設54	運用室が存在する建物の電源室および空調機械室は独立した部屋となっております。事務室等他の用途として利用されることはなく、部外者の侵入も不可能となっております。
設55	運用室が存在する建物の電源室および空調機械室はいずれも施錠されており、管理者の許可を得た者だけが入室可能です。窓がある場合がありますが、小さな窓であり、この窓から侵入することはできません。
設56	運用室が存在する建物の電源室および空調機械室は耐火構造となっております。
設57	運用室が存在する建物の電源室および空調機械室には火災報知設備が設置されております。
設58	運用室が存在する建物の電源室および空調機械室の付近には消火器があり、万一火災が発生した際にはそれを用いて消化を行います。ただし、近隣に火気を使用する部屋がないので、火災のリスクは低いものとなっています。
設59	運用室が存在する建物の電源室および空調機械室には原則として漏水防止措置が取られております。 漏水防止措置がとられていない建物に位置する運用室が利用不能になった場合、その機能は他の運用室で代替されます。
設60	

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用 基準番号	対応状況
設61	運用室が存在する建物の電源容量は余裕をもって確保されております。
設62	運用室は1回線受電となっております。停電によって運用室が利用不能になった場合、その機能は他の運用室で代替されます。
設63	運用室は通常の電源設備を利用しております。
設64	運用室が存在する建物には防災用の自家発電設備が設置されております。
設65	運用室は避雷設備が設置された建物内に存在します。
設66	運用室が存在する建物が地震リスクが高い地域にある場合、電源設備は耐震固定されています。
設67	運用室の分電盤は建物の受変電設備より専用線で接続しております。
設68	運用室の電源系統と建物の設備電源の電源系統は分けられています。
設69	運用室が存在する建物は原則として建物の電源設備にアースが設置されているため運用室内にはアースを設置しておりません。 建物にアースがない場合は運用室内に適切にアースを設置しております。
設70	運用室には過電流や漏電によって各機器に障害が及ぼされないようにするための措置がとられております。
設71	運用室が存在する建物には予備電源ないしは自家発電設備が存在します。
設72	運用室内で利用している空調設備は機器の発熱量に対して十分な空調機能を発揮することができる設備を要しています。
設73	運用室の空調設備は定期的にメンテナンスされております。
設74	運用室専用の空調設備はございません。
設75	運用室には空調設備の予備はございません。
設76	運用室が存在する建物にある空調設備に異常が生じた場合は、監視システムによって即座に故障が検知されます。
設77	運用室が存在する建物に空調室がある場合、許可を受けたものだけが入室できるように管理しております。
設78	運用室が存在する建物が地震リスクが高い地域にある場合、空調室は耐震施工を行っております。
設79	運用室が存在する建物は原則として空調設備のダクトには断熱材を、給気口には不燃材料を使用しております。 ただし、一部の建物の給気口は不燃材料を利用しておりません。
設80	運用室が存在する建物はそれぞれ集中管理室ないしは専用の監視設備によって設備障害を検知しております。
設81	運用室が存在している建物には中央管理室があります。この中央管理室で電源設備、空調設備、防災設備、防犯設備等の運営管理を円滑にし、かつ有効活用を図るため、これらの設備を集中管理しております。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用 基準番号	対応状況
設82	運用室が存在している建物にある回線関係の電気シャフトには鍵がかけられ、入退室管理がされています。
設83	運用室が存在している建物は通信回線の設備設置場所を示す表示をしておりません。
設83-1	運用室の位置している建物は弱電と強電がそれぞれ別シャフトとなっております。
設備基準84～137 は「本部・営業店等」「流通・小売店舗との提携チャネル」の基準であり、対象外	

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用 基準番号	対応状況
実1	暗証番号・パスワードは非表示・非印字としています。また、既に利用していない運用者からは権限を剥奪し、利用を停止した運用者からの漏洩に対策しています。
実2	サービスには公衆通信網を通じて自動着信端末に金融情報を出力する機能はありません。
実3	運用作業者には必要最低限のアクセス権限を付与しており、会社貸与PCにも本人確認機能等を設けています。 バックアップはクラウド事業者に適切に保管されており、アクセス制御も講じられています。 また、COMPANYへのログインユーザ・パスワード等 重要なデータは、ハッシュ化、暗号化等の対策をしています。 ※電子的取引についてはCOMPANYおよび本サービスは対象外です。ICカード、障害端末の利用はございません。
実4	サービスにおいては異なるネットワーク間の通信は、すべて適切な方式で暗号化されます。
実5	OSの備えるアクセス制限の方法を使用し、不正アクセス等からのデータ保護を行っています。
実6	サービスはアプリケーション、または、データベースの機能を用いて、不良データが入力されないようにしています。
実7	外部との通信は HTTPS 通信を利用しています。
実8	運用のためのツールは本人確認および接続元確認が行われ、適切なユーザ、適切な接続元からの利用でなければ利用することができません。サービスが稼働しているサーバへの通信は許可された接続元からの接続のみを許可するように設定されています。
実9	運用のためのツールのユーザは定期的に棚卸がされます。また、推測し難いようにパスワードのルールが Operation Manual に定められています。より漏洩による被害が大きいと考えられるツールは二段階認証等を用いて防御しています。 サービスが稼働しているサーバへの通信は許可された接続元からの接続のみを許可するように設定されています。
実10	運用のためのツールはシステムやデータへのアクセス履歴が取得・保管され、定期的にチェックが行われています。 サービスにはアクセス履歴の管理機能が用意されています。
実11 実12	サービスでは金融サービスは提供していません。
実13	クラウド事業者の提供する機能で暗号鍵を管理しています。
実14	クラウド事業者の提供する、仮想プライベートネットワーク機能、およびファイヤウォール機能を利用してサーバより外側で不正侵入防止策を講じております。
実15	クラウド事業者提供の機能によって外部からアクセス可能な経路・機器はネットワークレベルで制限されています。
実16	運用のためのツールはログインに失敗した場合にも記録がとられます。サービスが動作しているサーバは、エンドポイントセキュリティを導入・利用して不正アクセスを監視しています。 また、サービスへのログインについても記録がとられています。
実17 実18	サービスでは金融サービスは提供していません。
実19	不正アクセスを検知した場合に、サーバの停止、ネットワークの切り離し、ファイアウォール機能で通信を制御などを行って対処します。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用 基準番号	対応状況
実20	サービスが稼働しているサーバは、コンピュータウイルス等の不正プログラムに対する検知・防護策を講じています。 またバックアップについては、クラウド事業者により適切に保管されており、不正プログラムの発見時からシステム復旧までの対策も講じております。
実21	
実22	
実23	各種手順(構築・運用など)を定めた Operation Manual が整備されています。Operation Manual はシステム変更等が発生した場合には、見直されます。
実24	障害時・災害時共に「事業継続管理規程」がございます。災害発生時の場合、当該規程で規定されたWorks Human Intelligence 全社での対応を実施いたします。また、サービスでは、障害対応（インスタンスの障害など）の基本フローが確立されていて Operation Manual に記載されています。
実25	システムの運用上必要なデータは、特定のオペレーターしか使用できないように、アカウントの管理を行っています。 アクセス権限は作業毎に作業報告を提出し責任者の承認を得た後に付与されます。常時アクセス権限を保持するオペレーターはいません。
実26	アクセス権限を付与する手続きが定められています。また、アクセス権限は定期的に見直しがされています。
実27	
実28	お客様のデータを取り扱う場合、個人情報保護に関する社内規程、手引書等一覧に準じて実施いたします。 ただし、サービスではデータファイルの授受を行っていません。 データファイルに不整合が生じた場合のデータファイルの修正および管理作業も実施していません。
実29	
実30	暗号鍵を利用する作業は Operation Manual 内で運用管理方法を定めております。
実31	業務オペレーションへの習熟のため、手順書の作成および担当業務等に応じた教育を実施しております。
実32	サービスが稼働しているサーバは、コンピュータウイルス等の不正プログラムに対する検知・防護策を講じています。 またバックアップについては、クラウド事業者により適切に保管されており、不正プログラムの発見時からシステム復旧までの対策も講じております。
実33	お客様とクラウド事業者間の接続の設備および回線は、クラウド事業者から提供されるものを除き、お客様で調達、構築および維持する契約となっております。
実34	相手先確認や接続条件(パスワード等)の登録・変更管理方法が Operation Manual に定められています。
実35	正当な権限がなければコンピュータシステムを使用できないようにオペレータの資格確認が行われています。
実36	コンピュータシステムのオペレーション実施依頼・権限付与依頼・権限付与の手続きは明文化されています。
実37	オペレーション実行体制はオペレーションの実行前に定められ、記録されています。定められた体制に従い、オペレーションを所定のオペレータが記録し、作業承認者が確認します。
実38	
実39	「クラウドサービス説明書」によって、サービスのデータのバックアップ方法を定義しています。
実40	バージョン管理システムを用いてプログラムファイルが管理されています。
実41	プログラムのバックアップを確保しています。このバックアップについては管理方法が定められています。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用 基準番号	対応状況
実42	クラウド事業者提供のコンソールから関連設定を変更する際には、変更手続きを経た上で実施しています。ネットワーク設定変更は、権限を持つ担当者のみが実施しています。
実43	サービスを提供するネットワーク設定の為のスクリプトがサービスのプログラムの一部として出荷ファイルに含まれ管理されています。 この出荷ファイルはバックアップが確保・管理されています。
実44	Operation Manual はバージョン管理システムで管理されていて、アカウントを付与されたものしか参照、編集できないものになっています。また、編集の際にはログが残るようになっています。
実45	復旧に必要なドキュメントは世代管理とバックアップが行われています。
実46	運用室等にある各機器は保守点検が定期的に実施されており、これによって機器の障害を防止しています。
実47	サービスが稼働するサーバ上のリソースの監視、およびリソース調整をしています。 （お客様が外部連携のために使用するサーバ等については、クラウドサービスの責任範囲外となります。）
実48	サービスが用いるハードウェアはサービスが稼働するコンピュータセンターを提供するクラウド事業者が管理しています。 サービスのソフトウェアおよび、ソフトウェアの構成はバージョン管理システムで管理されており、周辺機器に関しても適切に管理を実施しております。
実49	運用室等にある各機器の管理は「情報システム管理規程」に則り、不正使用や破壊、盗難等を防止しております。
実50	運用室等にある各機器の管理は　ISO27001 に基づいてルールを定め、それに基づいて保護措置をとっております。
実51	運用室等にある各機器は保守点検が定期的に実施されており、これによって機器の障害を防止しています。
実52	運用室等に存在するハードウェアは重要度に応じて必要なものは保守点検を実施しております。
実53 実54	運用室内の設備の管理責任者、管理方法は「リモートセキュリティポリシー」および「職務分掌規程」・「施設管理規程」に定められており、管理責任者が保守点検を実施しております。
実55	運用室内の設備の管理責任者、管理方法は「リモートセキュリティポリシー」および「職務分掌規程」・「施設管理規程」に定められており、設備の容量及び性能、使用状況が確認されています。 また、サービスの物理リソースの管理はクラウド事業者に依存しています。詳しくはクラウド事業者が公開している対応状況をご覧ください。サービスが稼働している論理リソースはモニタリングされ、異常事態が発生した場合は関係者に告知されます。
実56 実57 実58	運用室の入退室権限は作業報告を提出し責任者の承認を得た後に付与され、作業後には剥奪されます。 運用室への入退室管理は、特定の部門を設け、資格付与等を行っています。
実59	運用室の入退室および利用権限は、作業報告を提出し責任者の承認を得た後に付与され、作業後には剥奪されます。 また、運用室内での作業時の不正を防止するために、行った作業は監視カメラなどの方法で記録されています。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用 基準番号	対応状況
実60	サービスの物理リソースの管理はクラウド事業者に依存しています。詳しくはクラウド事業者が公開している対応状況をご覧ください。 サービスが稼働している論理リソースはモニタリングされ、異常事態が発生した場合は関係者に告知されます。
実61	運用上、取引管理は実施しません。
実62	
実63	
実64	
実65	Operation Manual でデータの入力手順が定められています。
実66	作業担当者は、作業報告を提出し責任者の承認を得た後に権限を付与されます。また、作業後に権限は剥奪されます。 作業内容はあらかじめ定められたものである他、作業報告書として記録されます。 自動実行ツールで行う作業の際にも、実行スケジュールは責任者の承認がなければ設定されません。また、作業内容はあらかじめ定められたものである他、作業ログが出力されます。
実67	クラウドサービスで行われるオペレーションにおいては、帳票管理は実施しません。
実68	
実69	サービスでは顧客データへのアクセスを行っていません そのため顧客データの適正利用に関する管理は実施していません。
実70	障害時・災害時には、関係者へ連絡する方法が確立されています。
実71	多くの障害は自動復旧システムにより復旧しています。また、復旧できない場合の復旧手順も定めています。
実72	検知した障害ごとに対応方法が確立されています。 また、発生した障害の原因・対応方法を記録し、障害管理されています。
実73	サービスの BCP に従い、策定しています。この BCP は定期的にテストされており、合わせて方法が適切であるかの見直しがされています。
実74	運用室等は複数拠点にバックアップサイトが存在します。サービスが稼働するコンピュータセンターは複数の場所に拠点を持つクラウド事業者から提供されており、利用しているコンピュータセンターが利用不能になった場合は別のコンピュータセンターにサービスを復旧させます。
実75	各種手順を記載した Operation Manual を整備し、管理しています。
実76	サービスのテスト環境が用意されており、そこで検証を行った後に本番環境への適用を実施します。
実77	サービスには本番へ移行するためのスクリプトおよび手順書が含まれており、移行手順は明確になっています。また、これらはテストされた末に出荷され、その過程で整合性も確認されています。
実78	Operation Manual はドキュメントの範囲、体系、様式、記述方法が定められ明文化されています。
実79	Operation Manual はバージョン管理システムで管理しているため、改ざんはできません。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用 基準番号	対応状況
実80	お客様に向けて導入されるパッケージは社内で定められた基準に従い、評価部門によって評価されたのちに合格した物のみ出荷されます。アプリケーションの設定・運用方針はサービス利用者個々に設定変更が可能であり、有効性・信頼性・生産性に関する評価については、お客様にて行っていただく必要があります。
実81	サービスにおけるトラブル対応および機能拡張の流れは Operation Manual に定義されており、その通りに運用されています。
実82	システムの廃棄については COMPANY Coreクラウドサービス説明書に記載されている通りです。
実83	データの破棄はクラウド事業者に依存しています。詳しくはクラウド事業者が公開している対応状況をご覧ください。
実84 実85 実86 実87 実88	サービスが稼働するコンピュータセンターの信頼性向上対策は、クラウド業者に依存しています。 運用室等は全て予備が用意されています。
実89 実90	保守・運用・管理のためのツール群は全て評価を受け、必要な機能が取り込まれていることが確認されてから開発されています。サービスも同様に計画段階で評価を受け、機能が十分であることを確認したうえで開発が開始されます。
実91	保守・運用・管理のためのツール群及びアプリケーションは評価されたプログラム仕様書に基づいて開発されます。プログラム作成作業は標準化・自動化されており、これによって、ソフトウェアの品質は確保されます。
実92 実93	保守・運用・管理のためのツール群及びアプリケーションは定められたテストプロセスに従って評価されます。
実94	サービスの機能およびお客様の既存システムとの整合性の確認はお客様が行う必要があります。
実95	サービスの運用における定型的作業は全て Operation Manual に従い、評価されたツールによって行われます。
実96	保守・運用・管理のためのツール群及びアプリケーションは定められたテストプロセスに従って評価され、合格した物だけがお客様に提供されます。
実97 実98	サービスでは、製品側のファイルへはアクセスしておりません。
実99 実100	オペレーションの信頼性・効率性を上げるために、監視やシステムの起動などのオペレーションをツールで自動化を図っています。ツールは設定値のチェックが行われ、チェックに合格しなければツールを使うことができません。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用 基準番号	対応状況
実101	運用室は必要に応じて運用のための計算機を追加しています。サービスは計算機資源の状況を監視し、不足した場合に計算機資源を追加します。また、過剰な場合にはとりのぞきます。
実102	サービスの、障害の早期発見・回復のために、コンピュータシステムの運用状況(稼働状態、停止状態、エラー状態)を監視する機能を設けています。
実103	障害箇所に応じて復旧する機能を設けています。
実103-1	サービスを構成する重要なサーバは冗長化されており、障害により一部の処理が中断されてもシステム全体を停止することなく、運転が継続されます。 またISO27001の規定に則り、事業継続性の確認を弊社検証環境で実施しています。
実104	サービスを構成する重要なサーバは冗長化されており障害により一部の処理が中断されてもシステム全体を停止することなく、運転が継続されます。
実105	サービスでは取引を管理しません。
実106	障害箇所に応じて復旧する機能を設けています。
実107	サービスではカードは管理しません。
実108	
実109	サービスではCD/ATMは管理しません。
実110	サービスではカードは管理しません。
実111	サービスでは金融サービスは提供していません。
実112	
実113	
実114	
実115	
実116	
実117	サービスではインターネットバンキングのサービスは提供していません。
実118	サービスでは渉外端末は使用しません。
実119	サービスではCD/ATMは管理しません。
実120	
実121	
実122	
実123	
実124	

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用 基準番号	対応状況
実125	サービスではインストアブランチは管理しません。
実126	サービスではコンビニATMは管理しません。
実127	
実128	
実129	
実130	
実131	
実132	サービスではカードは管理しません。
実133	
実134	
実135	
実136	サービスでは取引管理は実施しません。
実137	サービスでは金融サービスは提供していません。
実138	サービスではお客様に対して取引通知や情報提供、問い合わせのために電子メールを利用することはありません。
実139	システム監視や定期的なセキュリティ教育の実施など、不正使用防止策を講じています。
実140	サービスでは生体認証は行っていません。
実141	
実142	サービスではQRコード決済は行っていません。
実143	
実144	
実145	テレワークで使用するハードウェア及びソフトウェアについては、管理方針を策定し、テレワーク勤務者に周知しております。
実146	情報システムにアクセスするためのアカウントには、多要素認証など不正なアクセスを防止するための対策を講じています。
実147	テレワークにおける情報漏洩を防止するため、重要なデータの管理方針を定めております。 また通信の暗号化を含めた対策も講じております。
実148	テレワークにおける物理的な手段による情報漏洩やWeb会議での情報漏洩を防止するため、全役職員(派遣社員を含む)への注意喚起および対策を実施しております。

○4.3. 安全対策対応表

金融機関等コンピュータシステムの安全対策基準・解説書 第10版改定からの引用	対応状況
基準番号	
監1	ISO27001、27017、27701およびJISQ15001に基づき、システム等の運用監査体制を整備しております。 サービスをご利用中のお客様は、SOC1報告書にて弊社の統制状況をご確認いただけます。