CCMS
セキュリティスタンダード

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12版）」対応

Version 4.00

2025/04/11

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 対応	2023/07/27
3.00	第11版 対応	2024/06/28
4.00	第12版 対応	2025/04/11

2. COMPANY on Cloud Managed Service （CCMS）セキュリティスタンダード概要

ここではCOMPANY on Cloud Managed Service （以下CCMS）セキュリティスタンダードの目的、対象範囲、策定方針を解説します。

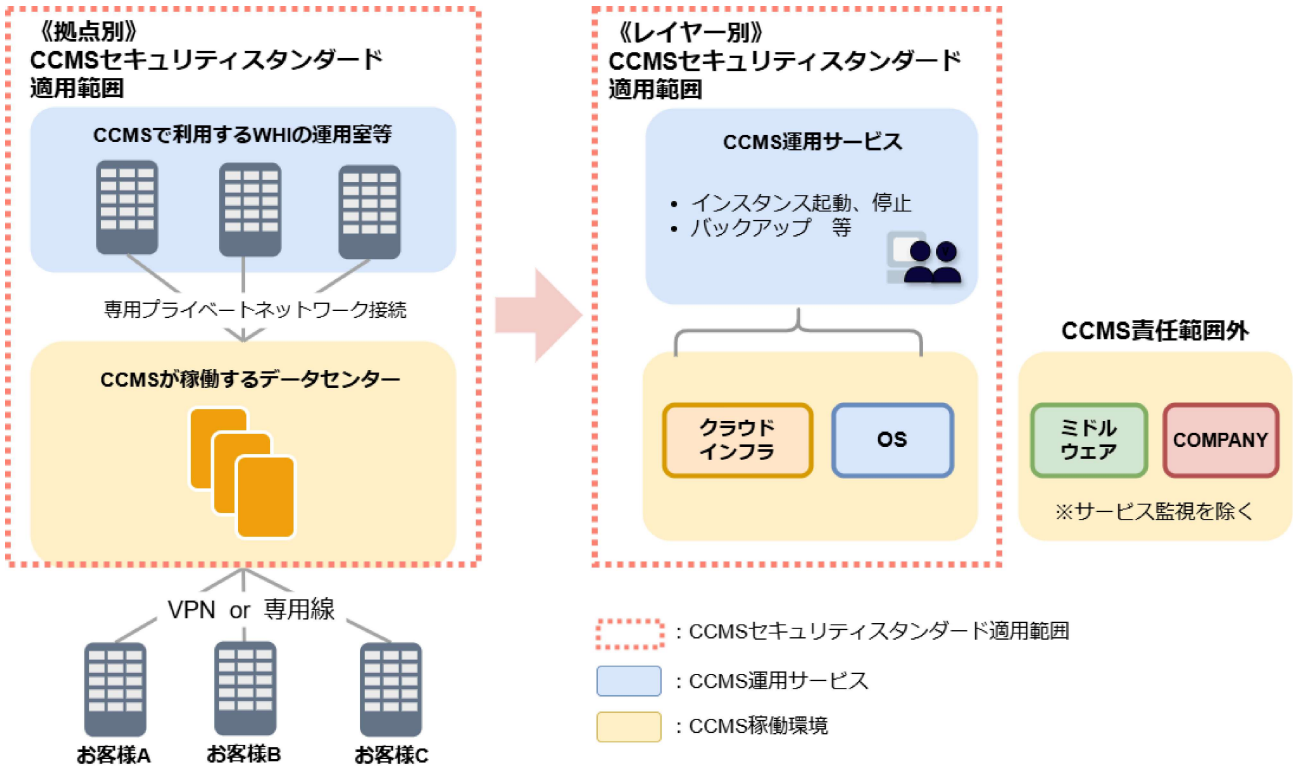
○2.1. 目的

- お客様がCCMSの安全性を確認するための情報を提供します。
- CCMSにおける安全対策の骨子を定めます。

○2.2. 対象範囲

- CCMSセキュリティスタンダードの対象範囲は、CCMSが提供する環境および運用保守サービスを対象とします 。
  ※COMPANYの保守サービス（GMS)は対象に含まれません。

○2.3. 対象範囲イメージ



《補足》

- CCMSが提供する環境（以下、サービス）はクラウド事業者が提供するデータセンター（以下、CCMSが稼働するデータセンター）に構築されます。
- お客様はそのサービスを利用するために、専用線 又は VPN にてお客様環境に接続します。
- CCMSが提供するサービスは Works Human Intelligence（以下、弊社）の運用室等から、リモート操作によって実施されます。

- CCMSで利用する運用室は地理的に分かれた国内の複数地点に存在し、接続が可能です。

- CCMSセキュリティスタンダードはCCMSが提供するサービスを対象としているため、以下が対象範囲となります。
  - **CCMSで利用する運用室**
    a）CCMS運用サービスを実施するための環境。本書では運用室を「 CCMSで利用する運用室」と定義し、運用保守作業を「 CCMS運用サービス」と定義します。

  - **CCMSが稼働するデータセンター**
    a）CCMS運用サービスを提供するために利用する環境。
    本書では「 CCMS管理環境」と定義します。
    b）CCMSが提供するお客様がCOMPANYを利用する環境。
    本書では「お客様環境」と定義します。

○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・解説書」の考え方に基づきます。
- 弊社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、CCMSセキュリティスタンダードに反映します。

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

CCMSに関係する設備は以下の 2 つです。

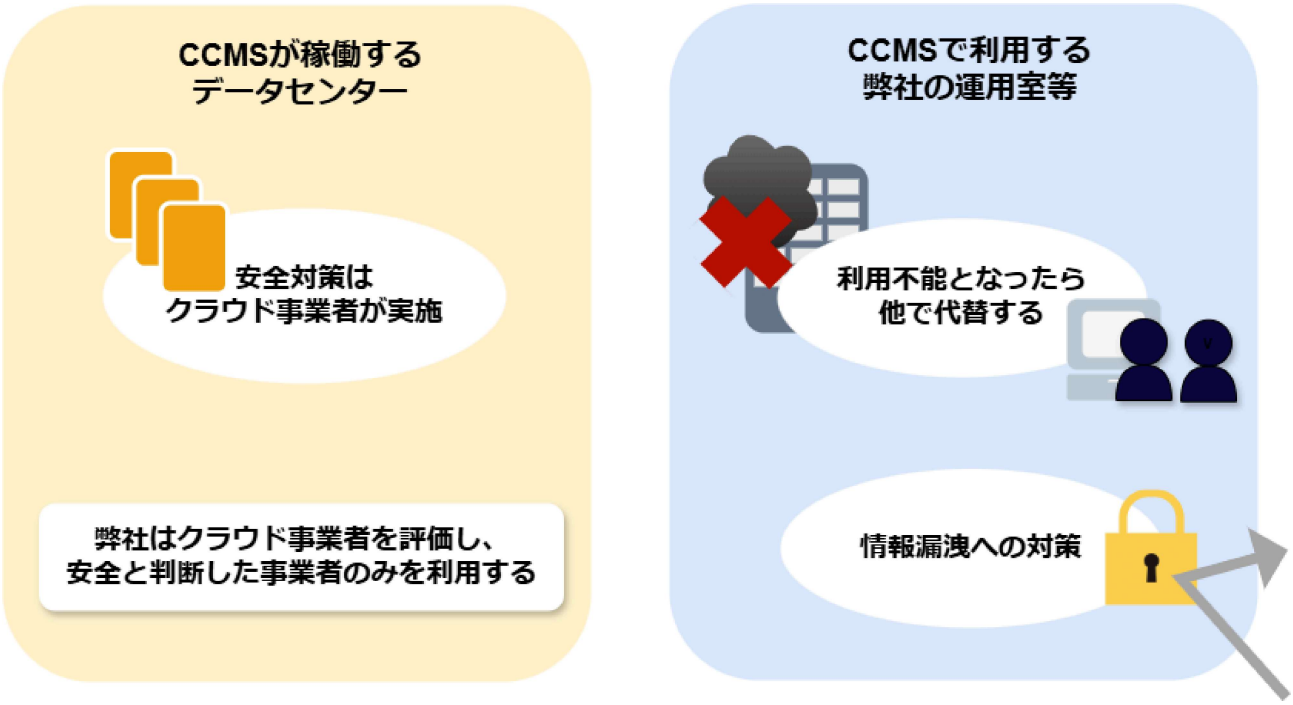
a)　CCMSが稼働するデータセンター

このデ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。
弊社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を利用します。

b)　CCMSで利用する運用室等

この運用室は、弊社に安全対策の責任があります。
運用室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、運用室が利用不能になった場合に備え、この運用室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、運用室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＞



○3.2. 運用について

CCMSはお客様がご利用する環境をCCMS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。

CCMSのオペレーション作業では、責任者から承認を受けた者のみが作業権限を付与されるよう制御されており、作業実施後には権限が剥奪されます。

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、弊社および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

CCMSセキュリティスタンダード概要の対象範囲で解説した通り、サービスはクラウド事業者が管理するデータセンター上で稼働しています。そのデータセンターに対し、弊社が所有するCCMSで利用する運用室等からアクセスします。

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。
クラウド事業者の対応状況は、クラウド事業者の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CCMSを提供する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・解説書からの引用 基準番号	CCMSの対応状況
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「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、随時見直しを実施しています。 PSIRTの体制構築および運用も実施しており、セキュリティインシデントへの対策を整えています。 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、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 「運用手順書」に従い、整備しています。
統7	ISO27001の取り組みの一貫で、「運用管理手順書」にて管理対象となるデータと そのデータの管理手順を定め、管理体制を整備、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。 また、CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、各種災害、障害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
統11	防犯組織として明確に規定はしていませんが、各種防犯対策は実施しています。 また、CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、防犯対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
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（年1回以上）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います。
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います。
統16	ISO27001に準拠し、障害時・災害時に備えた教育・訓練を実施しています。 また、CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、各種災害、障害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
統17	非常時に備えて防災訓練を実施しています。 また、CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、防災・防犯対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
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います。
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・解説書からの引用 基準番号	CCMSの対応状況
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。 CCMS 拡張アクセス監査オプション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。
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。 また、CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、各種災害、障害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
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・検証を行っています。
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範囲は「CCMSサービス仕様書」に記載しています。 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。 ※SOC1報告書の提供には、CCMS 拡張アクセス監査オプションの利用が必須となります。
統25	緊急事態発生時に弊社が行う対応について「CCMSサービス仕様書」に定められ、お客様はこれをご確認できるようになっています。
統26	CCMSでは、金融サービスの提供は行っていません。 また、金融機関相互ネットワークへの接続もしていません。
統27	同上

○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・解説書からの引用 基準番号	CCMSの対応状況
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	CCMSには公衆通信網を通じて自動着信端末に出力する機能はありません。
実3	CCMS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CCMSは対象外です。ICカード、障害端末の利用はありません。
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。 暗号鍵は、クラウド事業者の提供する機能で管理しています。 また標準的な構成図については、CCMSサービス仕様書にてご確認が可能です。
実5	OSの備えるアクセス制限の方法を使用し、不正アクセス等のデータ保護を行っています。
実6	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が、CCMSではデータベースへのアクセスをしていません。
実7	外部との通信は HTTPS 通信を利用しています。
実8	CCMSでは、運用ツールの利用にあたり本人確認および接続元の確認を行っています。 またサービスが稼働するサーバへは、許可された接続元からの通信のみ許可するように設定しています。
実9	CCMS運用サービス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CCMSドキュメント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	CCMSではアクセス履歴として監査証跡を保管しており、お客様の要望に応じて提供が可能です。定期的なチェックについては、お客様側での対応となります。 詳細は、CCMSサービス仕様書にて記載しています。 サーバ内に保管されるログは、定期的なバックアップの設定が可能です。その他のログについては、冗長性を確保した状態で保管されています。 お客様がCOMPANY（もしくはその他のアプリケーション）を利用する際のログイン記録については、アプリケーション側の提供となります。
実11	CCMSでは、金融サービスの提供は行っていません。
実12	同上
実13	CCMSでは、セキュリティを確保したプロセスに沿って、暗号鍵の管理に必要な要件を文書化し、運用しています。暗号アルゴリズムや鍵の長さについては、CRYPTREC推奨の暗号リストに掲載されている設定値を使用しています。 弊社ではクラウド事業者の提供する機能を利用して、これらの暗号鍵を厳格に管理・統制しており、改変や紛失から保護しています。 なお、暗号鍵の所有権は弊社が保持しています。
実14	CCMSでは、クラウド事業者が提供する仮想プライベートネットワーク機能の利用およびアクセス可能な経路等をネットワークレベルで制限し、サーバー外部からの不正侵入を防止する策を講じています。 また情報セキュリティの遵守状況を確認するために定期的な内部監査を実施しており、監査結果に基づいた改善や情報システムの継続的な見直しも行っています。
実15	お客様が、クラウド事業者の管理インターフェースへアクセスすることは禁止しています。 また、クラウド事業者が提供する機能によって外部からアクセス可能な経路や機器はネットワークレベルで制限されています。

○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・解説書からの引用 基準番号	CCMSの対応状況
実16	CCMS環境にはセキュリティソフトウェアおよびAWSのセキュリティサービスが導入されており、マルウェア対策、 侵入検知を行っています。 また、CCMS運用作業ではアクセス権限を制限し、ログイン失敗時の記録の取得を行っています。 なお、お客様によるアプリケーションのログイン記録は、アプリケーションの機能としての提供となります。
実17	CCMSでは、金融サービスの提供は行っていません。
実18	同上
実19	不正アクセスを検知した場合、インスタンスの停止、ネットワークの切り離し、アクセス可能な経路等をネットワークレベルで制限し、通信の制御等を行い対処します。
実20	CCMSでは、厳格なアクセス制御や通信の暗号化など不正侵入に対する重層的な防御策をとっています。もし不正プログラムの感染が検知された場合には、感染拡大を防ぐための対応措置を取ります。 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います。 なお、セキュリティ上の理由から操作手順の詳細については公開していません。
実21	同上
実22	同上
実23	弊社では、構築や運用などの各種手順に関するシステム運用マニュアルを整備しており、システムの変更が発生した場合など、必要に応じて手順を見直しています。 セキュリティ上の理由から、操作手順の詳細については公開していません。 また、アプリケーション操作に関するマニュアルは、弊社のサポートサイト上に公開しています。
実24	各種災害や大規模障害に対しては「事業継続管理規程」を制定しており、ISO27001の規定に基づいて、定期的に弊社の検証環境にて事業継続性の確認および手順の見直しを行っています。 また通常時障害対応についても、復旧作業の基本フローを確立しています。
実25	CCMSではアクセス管理のための台帳を作成し、アクセス可能な要員および職務に基づいたアクセス権のレベルを設定しており、定期的な見直しも行っています。 またサーバへのアクセス権は、作業ごとに作業報告書を提出し、責任者の承認を得た後に付与されるため、常にアクセス権限を持つオペレーターは存在しません。 なお、お客様による運用ツールや管理インターフェースへの操作は許可されていません。
実26	同上
実27	同上
実28	お客様のデータを取り扱う際には、個人情報保護に関する社内規程や手引書に基づき、適切な対策を行います。 ただし、CCMSではデータファイルの送受信は行っておらず、データファイルの修正や管理作業も行いません。 また、外部からアクセス可能な経路や機器については、クラウド事業者が提供する機能によってネットワークレベルで制限されています。
実29	同上
実30	CCMSでは、セキュリティを確保したプロセスに沿って、暗号鍵の管理に必要な要件を文書化し、運用しています。暗号アルゴリズムや鍵の長さについては、CRYPTREC推奨の暗号リストに掲載されている設定値を使用しています。 弊社ではクラウド事業者の提供する機能を利用して、これらの暗号鍵を厳格に管理・統制しており、改変や紛失から保護しています。 なおセキュリティ上の理由により、詳細はお客様へ公開していません。
実31	オペレーションの習熟のため、手順書の作成および担当業務に応じた教育を実施しています。 なお、お客様による運用ツールや管理インターフェースへの操作は許可されていません。

○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・解説書からの引用 基準番号	CCMSの対応状況
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います。
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います。
実34	相手先確認や接続条件(パスワード等)の登録・変更管理をISO27001に準じた社内規程で管理しています。 また、お客様からの依頼に基づきWindows Update を実施しています。 外部からアクセス可能な経路や機器については、クラウド事業者が提供する機能によってネットワークレベルで制限されています。 当社ではお客様からの要望に基づき、サーバーへの接続元やネットワーク設定などを制限する対策を行っています。
実35	正当な権限がなければCCMSで利用する運用室等のコンピュータシステムを利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	CCMS運用サービス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	定常的なオペレーションを実施するチームと障害対応などを実施するチームを分け、作業特性に沿ったチーム編成を行っています。
実38	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39	CCMSサービス仕様書によって、サービスのバックアップおよび、データ破損時のリカバリについて定義しています。 バックアップ取得時には、データファイルだけでなく、利用するクラウド環境の設定情報も取得しています。 ISO27001の規定に基づいて、定期的に弊社の検証環境にて事業継続性の確認および手順の見直しを行っています。
実40	CCMSのサービス提供にあたり、運用ツールを利用しています。 また開発物は定められた手順により管理されています。
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。
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	CCMSが稼働するコンピュータセンターの環境のうち、CCMS管理環境はCCMSドキュメントにより定義し、管理しています。 また、お客様環境はお客様と合意し、管理を行っています。
実44	CCMSの運用ドキュメントはバージョン管理システムで管理され、アカウントを付与されたものしか参照できないものになっています。 また、編集の際には更新履歴を残す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	CCMSで利用する運用室等にある各機器は保守点検が定期的に実施され、これにより機器の障害を防止しています。
実47	CCMSはクラウド上のリソースの監視を行い、リソースを調整しています。 また、お客様環境におけるリソースについては、リソース調整の提案を行っています。 監視サービスの詳細については、CCMSサービス仕様書にて記載しています。
実48	CCMSが稼働するコンピュータセンターのハードウェアはクラウド事業者が管理しています。 CCMS内で利用している各種ツールについてはバージョン管理を行い、その仕様等をインフラ仕様書で管理しており、周辺機器に関しても適切に管理を実施しています。 CCMSで利用するOSのバージョンアップについては、お客様からの依頼により実施します。

○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・解説書からの引用 基準番号	CCMSの対応状況
実49	CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、盗難や不正利用への対策が建物、敷地内にとられており、特にカスタマーデータを保持するエリアでは厳重な管理が実施されていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。 また、CCMSではアクセス管理のための台帳を作成し、サービスの資産にアクセスが可能な要員及びそれぞれの職務に基づいたアクセス権のレベルを設定しています。
実50	同上
実51	CCMSで利用するデータセンターの管理はクラウド事業者に依存しますが、専門知識を有する担当者によって定期的に予防保守が実施され、設備の安定運用に努めていることをクラウド事業者のFISC安全対策基準対応リファレンス等にて確認しています。 また、CCMS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52	同上
実53	同上
実54	同上
実55	同上
実56	CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、盗難や不正利用への対策が建物、敷地内にとられており、特にカスタマーデータを保持するエリアでは厳重な管理が実施されていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。 また、システムへのアクセス権限についても、作業ごとに申請を提出し責任者の承認を得た後にのみ付与される仕組みとなっており、適切に管理しています。作業後には権限が剥奪されるため、常時アクセス権限を取得する者はいません。
実57	同上
実58	同上
実59	同上
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	CCMSでは、金融サービスの提供は行っていません。
実62	同上
実63	同上
実64	同上
実65	定期運用作業は定常作業として手順化し実施しています。 ※CCMSではデータの入力業務は実施していないので、設定作業としての回答になります。
実66	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。 また、CCMSでは作業報告を提出し責任者の承認を得た後に作業担当者に権限が付与され、作業後には剥奪されます。
実67	CCMSの運用作業では、未使用重要帳票の利用や管理、帳票の出力は行いません。

○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・解説書からの引用 基準番号	CCMSの対応状況
実68	同上
実69	CCMSでは、金融取引等において取得された金融機関等の顧客データを取り扱いません。 そのため顧客データの適正利用に関する管理も実施していません。
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。 障害発生時のサポート内容については、CCMSサービス仕様書に記載しています。
実71	CCMS障害については、弊社にて復旧作業を実施します。 多くの障害は自動復旧システムにより復旧されますが、復旧できない場合の対応手順も規定しています。 また、対応手順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72	検知した障害ごとに対応方法が確立されており、発生した障害の原因・対応方法を記録、管理しています。 また、お客様環境にて生じたインフラ起因の障害については、定期的にお送りするレポートにて報告しています。
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	CCMSで利用する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。 デ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、利用している拠点（アベイラビリティゾーン）が利用不能になった場合は別拠点（アベイラビリティゾーン）に環境を構築します。 なお、CCMSのRPO/RTOについては、CCMSサービス仕様書に記載しています。
実75	お客様環境へのCCMS運用作業は、作業手順を明確にしています。 またCCMSでは、本番環境とは論理的に分離されたテスト環境が構築されるため、お客様にてテスト環境で検証を行った後に、本番環境への適用を行うことが可能です。 詳細については、CCMSサービス仕様書をご確認ください。
実76	同上
実77	移行手順は明確化しています。 また、これらはテストを経て出荷され、その過程で整合性も確認されています。
実78	CCMSのドキュメントは、アカウント付与された者しか参照、編集できない様に管理しています。
実79	CCMSのドキュメントは、バージョン管理システムで管理され、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、編集の際には更新履歴が残るようになっています。
実80	定められた基準を合格したアプリケーションを提供しています。 アプリケーションとしての設定や運用方針はサービス利用者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	アプリケーション導入後の保守は別契約にて実施する体制を整えています。
実82	システムの廃棄については、CCMSサービス仕様書に記載しています。 また弊社での廃棄手順については、「運用手順書」にて規定しています。
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	CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、各種災害、障害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
実85	同上
実86	同上
実87	同上
実88	同上

○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・解説書からの引用 基準番号	CCMSの対応状況
実89	CCMS運用サービス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。 また内部統制にて開発者と評価者を別々に選任し、開発責任者の承認を得てリリースをしています。
実90	同上
実91	同上
実92	同上
実93	同上
実94	アプリケーション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	CCMS運用サービスの定型的作業はすべて作業手順に従い、評価されたツールによって実施しています。
実96	CCMS運用サービスのツール群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	CCMSでは、アプリケーションが管理するファイルへアクセスはしません。
実98	同上
実99	CCMSでは、監視やシステム起動などの一部の定型作業にオペレーションツールを導入し、システムの自動化・簡略化を図っています。 また、これらのツールは事前に設定値のチェックが行われ、運用試験に合格したもののみが採用されます。 データセンターのオペレーション等のセキュリティについては、クラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
実100	同上
実101	CCMSでは、クラウド上のリソースの監視を行い、リソースを調整しています。 また、 お客様環境におけるリソースについては、リソース調整の提案を行っています。
実102	CCMSでは、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	CCMSでは、障害を検知すると、障害箇所を切り分けて、障害箇所に応じて復旧するサービスを提供しています。 またお客様への情報提供等については、サポート用WEBサイトを利用しています。
実103-1	CCMSでは冗長構成・バックアップ構成は採用していませんが、クラウドサービスの特性を生かし、多くの障害は自動復旧システムにより復旧しています。 自動復旧ができなかった場合の復旧手順も定めています。 また、AMIイメージで環境バックアップを提供しており、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	CCMSの死活監視、ウイルス対策、バックアップなどのサービスは、それぞれのサーバを分散して配置しているため、各々のサーバ障害時に、全てのサービスが止まることがないようにシステムを構成しています。 なおCCMSでは、金融サービスの提供および金融機関のオンラインシステムへの接続は行っていません。
実105	CCMSでは、金融サービスの提供および周辺機器、店舗、キャッシュカード等の管理は行っていません。
実106	CCMSでは障害を検知すると、障害箇所を切り分けて、障害箇所に応じて復旧するサービスを提供しています。
実107	CCMSでは、金融サービスの提供および周辺機器、店舗、キャッシュカード等の管理は行っていません。

○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・解説書からの引用 基準番号	CCMSの対応状況
実108	同上
実109	同上
実110	同上
実111	同上
実112	同上
実113	同上
実114	同上
実115	同上
実116	同上
実117	同上
実118	同上
実119	同上
実120	同上
実121	同上
実122	同上
実123	同上
実124	同上
実125	同上
実126	同上
~~実127~~	（欠番）
~~実128~~	
~~実129~~	
~~実130~~	
~~実131~~	

○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・解説書からの引用 基準番号	CCMSの対応状況
実132	CCMSでは、金融サービスの提供および周辺機器、店舗、キャッシュカード等の管理は行っていません。
実133	同上
実134	同上
実135	同上
実136	同上
実137	同上
実138	同上
実139	CCMSでは、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	CCMSでは、生体認証の利用および管理は行っていません。
実141	同上
実142	CCMSでは、金融サービスの提供および周辺機器、店舗、キャッシュカード等の管理は行っていません。
実143	同上
実144	同上
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います。
実146	CCMS環境へのアクセス用アカウントには、多要素認証等の不正アクセス防止策を講じています。また、CCMS運用サービスでは、弊社の運用室内に設置された保守用端末からのみCCMS環境への接続を可能にしており、テレワークは実施していません。
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います。 また通信の暗号化を含めた対策も講じています。
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います。
実149	CCMSでは、金融サービスの提供および周辺機器、店舗、キャッシュカード等の管理は行っていません。

○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・解説書からの引用 基準番号	CCMSの対応状況
設1	CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、各種災害、障害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。 またデータセンタの場所は公表されておらず、外部からはそれとはわからないようになっています。
設2	同上
設3	同上
設4	同上
設5	同上
設6	同上
設7	同上
設8	同上
設9	同上
設10	同上
設11	同上
設12	同上
設13	同上
設14	同上
設15	同上
設16	同上
設17	同上
設18	同上
設19	同上
設20	同上
設21	同上
設22	同上
設23	同上
設24	同上
設25	同上
設26	同上
設27	CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、各種災害、障害に対する対策が建物、敷地内にとられており、特にカスタマーデータを保持するエリアでは厳重な管理が実施されていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
設28	同上
設29	同上
設30	同上

○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・解説書からの引用 基準番号	CCMSの対応状況
設31	CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、自動火災検知および消火装置や、漏水検知デバイス等、各種災害、障害に対する対策が建物内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
設32	同上
設33	同上
設34	同上
設35	同上
設36	同上
設37	同上
設38	同上
設39	同上
設40	同上
設41	同上
設42	同上
設43	同上
設44	同上
設45	同上
設46	同上
設47	同上
設48	CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、地震を含む各種災害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
設49	同上
設50	同上
設51	同上
設52	CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、自動火災検知および消火装置や、漏水検知デバイス等、各種災害、障害に対する対策が建物、敷地内にとられていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。 また、データセンターの場所は公表されておらず、外部からはそれとは分からないようになっています。
設53	同上
設54	同上
設55	同上
設56	同上
設57	同上
設58	同上
設59	同上

○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・解説書からの引用 基準番号	CCMSの対応状況
設60	
設61	CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、電源設備は冗長化されており、電力障害の際にもバックアップ電力を供給すること、データセンター一施設全体へのバックアップ電力を供給する発電機を備えていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
設62	同上
設63	同上
設64	同上
設65	同上
設66	同上
設67	同上
設68	同上
設69	同上
設70	同上
設71	同上
設72	CCMSで利用するデータセンターの管理はクラウド事業者に依存しますが、温度と湿度をモニタリングし制御することで、サーバの過熱を防止し、サービス停止を抑制することをクラウド事業者のFISC安全対策基準対応リファレンス等にて確認しています。
設73	同上
設74	同上
設75	同上
設76	同上
設77	同上
設78	同上
設79	同上
設80	CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、システムおよび設備の監視を行い、早急に対応する体制を整えていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。
設81	同上
設82	CCMSで利用するデータセンターのセキュリティはクラウド事業者に依存しますが、ネットワークケーブルの適切な保護が実施されていることをクラウド事業者が提供するFISC安全対策基準対応リファレンス等にて確認しています。 またデータセンターの場所は公表されておらず、外部からはそれとはわからないようになっています。
設83	同上
設83-1	同上
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・解説書からの引用 基準番号	CCMSの対応状況
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います。 CCMS 拡張アクセス監査オプション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。