「broad talk」におけるFISC安全対策基準（第9版改訂）への対応状況について

ブロードマインド株式会社　2020年10月1日

注意: 本文書は情報提供のみを目的としています。本文書は、発行時点における broad talk と対応を説明するものであり、予告なく変更される場合があります。お客様は、本文書の情報およびbroad talkの利用について、ご自身の評価に基づき判断する

『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』の改訂版（第9版改訂）へのbroadtalkにおける対応状況は、以下の通りです。

FISC安全対策基準（第9版改訂）の項目					FISC安全対策基準（第9版改訂）へのbroadtalkの対策実施状況
基準番号	基準大項目	中項目	小項目	基準分類	
統1	1 内部の統制	(1) 方針・計画	システムの安全対策に係る重要事項を定めた規程を整備すること	基礎	システムおよびサービスを安全に稼働させるために、運用ポリシーを設けております。
統2			中長期的視点に立ったシステムの企画・開発・運用に関する計画を策定すること	基礎	中長期的視点に立ったシステムの企画・開発・運用計画を策定しております。
統3			システム開発計画は中長期システム計画との整合性を確認するとともに、承認を得ること	基礎	システムの新規開発は常に既存システムとの整合性を確認し、責任者が確認し承認を行っています。
統4		(2) 組織体制	セキュリティ管理体制を整備すること	基礎	システムのセキュリティに関する情報を社内で共有しております。
統5			サイバー攻撃対応態勢を整備すること	基礎	インシデント発生時には問題の報告、改善するフローを設けております。
統6			システム管理体制を整備すること	基礎	システム、データ及びネットワークの運用管理に必要な手順や体制等を定めています。
統7			データ管理体制を整備すること	基礎	社内の管理体制や責任分担を明確化したうえで、管理手順の整備を行い、サービ
統8			ネットワーク管理体制を整備すること	基礎	スの安全性の向上を図っています。
統9			業務組織を整備すること	基礎	業務運営の組織体制を整備するとともに、役割分担、規則及び手順等を明確化することにより、サービス運営の安全を確保しています。
統10			防災組織を整備すること	基礎	ブロードトークを設置しているデータセンターでは情報セキュリティフレームワークと、COBITフレームワークに基
統11			防犯組織を整備すること	基礎	づいたポリシーを確立しています。
統12			各種業務の規則を整備すること	基礎	サービスに必要な業務に関する手順や体制等を定めています。
統13		(3) 管理状況の評価セ	セキュリティ遵守状況を確認すること	基礎	サービスには定期的にツールを用いてセキュリティチェックを行っております。
統14		(4) 人材（要員・教育）	セキュリティ教育を行うこと	基礎	サービス提供に携わる従業員に対して、スキルの把握を実施し、能力と責任に応じた教育と育成を実施しています。
統15			要員に対するスキルアップ教育を行うこと	基礎	
統16			障害時・災害時に備えた教育・訓練を行うこと	基礎	ブロードトークを設置しているデータセンターでは、情報セキュリティフレームワークと、COBITフレームワークに基づいたポリシーを確立しています。
統17			防災・防犯訓練を行うこと	基礎	
統18			要員の人事管理を行うこと	基礎	情報システムの運用管理に必要な要員については、全社計画や事業計画等を考慮し、適切に管理しています。
統19			要員の健康管理を行うこと	基礎	定期的な健康診断、感染症対策による在宅勤務の推奨などを行っております。
統20	2 外部の統制	(1) 外部委託管理	外部委託を行う場合は、事前に目的、範囲等を明確にするとともに、外部委託先選定の手続きを明確にすること	基礎	サービスに関する業務の外部委託は、行っておりません。
統21			外部委託先と安全対策に関する項目を盛り込んだ契約を締結すること	基礎	
統22			外部委託先の要員にルールを遵守させ、その遵守状況を確認すること	基礎	
統23			外部委託先における管理体制を整備し、委託業務の遂行状況を確認すること	基礎	
統24		(2) クラウドサービスの利用	クラウドサービスを利用する場合は、クラウドサービス固有のリスクを考慮した安全対策を講ずること	基礎	利用しているクラウドサービスは情報セキュリティフレームワークと、COBITフレームワークに基づいたポリシーを確立しています。
統25		(3) 共同センター	共同センターにおける緊急事態の発生に備えて安全対策を講ずること	基礎	対象外
統26	1 情報セキュリティ	(4) 金融機関相互のシステム・ネットワークのサービス	金融機関相互のシステム・ネットワークのサービス利用にあたっては、適切なリスク管理を行うこと	基礎	対象外
実1		(1) データ保護	他人に暗証番号・パスワード等を知られないための対策を講ずること	付加	パスワードは暗号化されております。
実2			相手端末確認機能を設けること	付加	対象外
実3			蓄積データの漏洩防止策を講ずること	付加	データベースは外部からアクセス不可能なサーバーに蓄積されています。
実4			伝送データの漏洩防止策を講ずること	付加	伝送データは全てSSLで暗号化されています。
実5			ファイルに対するアクセス制御機能を設けること	基礎	ファイルアクセスはユーザー認証を必要としています。
実6			不良データ検出機能を充実すること	基礎	ファイルの取り扱いにはウィルス対策ソフトを用いて対応しております。
実7			伝送データの改ざん検知策を講ずること	付加	伝送データは暗号化されているため、改ざんはできません。
実8		(2) 不正使用防止	本人確認機能を設けること	基礎	システムはパスワード認証を行い、サーバーは鍵認証を行っております。
実9			IDの不正使用防止機能を設けること	基礎	ログを監視を行い、不正なアクセスを試みた形跡が発生した場合には担当者に報告します。
実10			アクセス履歴を管理すること	基礎	利用者の会議システム利用状況履歴を保管しています。閲覧も可能になっています。
実11			取引制限機能を設けること	基礎	対象外
実12			事故等の取引禁止機能を設けること	付加	対象外
実13			電子化された暗号鍵を蓄積する機器、媒体、またはそこに含まれるソフトウェアには、暗号鍵の保護機能を設けること	基礎	データ保存を利用しているクラウドサービスは情報セキュリティフレームワークと、COBITフレームワークに基づいたポリシーを確立しています。
実14		(3) 外部ネットワークからの不正アクセス防止	外部ネットワークからの不正侵入防止策を講ずること	基礎	ファイヤウォールを設置して適切に対応しております。
実15			外部ネットワークからアクセス可能な接続機器は必要最小限にすること	基礎	
実16		(4) 不正検知策	不正アクセスの監視機能を設けること	基礎	常時アクセスログを監視して、不正なアクセスを試みた形跡が発生した場合には、担当者にアラートメールを送信しています。
実17			異常な取引状況を把握するための機能を設けること	付加	対象外
実18			異例取引の監視機能を設けること	付加	対象外
実19		(5) 不正発生時の対応策	不正アクセスの発生に備えて対応策、復旧策を講じておくこ	基礎	アクセスログを取得して、不正アクセスが疑われる場合の対応策及び復旧策を整備しています。
実20		(6) 不正プログラム対策	コンピュータウイルス等の不正プログラムへの防御対策を講ずること	基礎	ウイルス対策ソフトを導入するとともに、復旧手段を整備しています。
実21			コンピュータウイルス等の不正プログラムの検知対策を講ずること	基礎	
実22			コンピュータウイルス等の不正プログラムによる被害時対策を講ずること	基礎	
実23	2 システム運用共通	(1) マニュアルの整備	通常時マニュアルを整備すること	基礎	文書・マニュアル等は全て管理し保存しています。
実24			障害時・災害時マニュアルを整備すること	基礎	障害発生時の対応は全て記録しています。それに基づいたマニュアルも作成しています。
実25		(2) アクセス権限の管理	各種資源、システムへのアクセス権限を明確にすること	基礎	各種資源、システムへのアクセス権限は明確にされています。
実26			パスワードが他人に知られないための措置を講じておくこと	基礎	パスワードは暗号化されています。
実27			各種資源、システムへのアクセス権限の付与、見直し手続きを明確にすること	基礎	システムへのアクセス権限などの見直しは定期的におこなっています。
実28		(3) データ管理	データファイルの授受・管理方法を明確にすること	基礎	データ保存を利用しているクラウドサービスは情報セキュリティフレームワークと、COBITフレームワークに基づいたポリシーを確立しています。
実29			データファイルの修正管理方法を明確にすること	基礎	
実30			暗号鍵の利用において運用管理方法を明確にすること	基礎	
実31		(4) オペレーション習熟	オペレーション習熟のための教育及び訓練を行うこと	基礎	定期的にオペレーション習熟のための教育及び訓練を行っています。
実32		(5) コンピュータウイルス対策	コンピュータウイルス対策を講ずること	基礎	サーバーおよびクライアントPCにウィルス対策をしております。
実33		(6) 外部接続管理	接続契約内容を明確にすること	基礎	外部との接続の安全管理のため、ファイアウォールを設置しています。
実34			外部接続における運用管理方法を明確にすること	基礎	
実35	3 運行管理	(1) オペレーション管理	オペレータの資格確認を行うこと	基礎	オペレーションの実施体制、手順、ルールを明確化することにより、安全な運用を確保しています。
実36			オペレーションの依頼・承認手続きを明確にすること	基礎	
実37			オペレーション実行体制を明確にすること	基礎	
実38			オペレーションの記録、確認を行うこと	基礎	
実39		(2) データファイル管理	データファイルのバックアップを確保すること	基礎	データは定期的にバックアップを行っています。
実40		(3) プログラムファイル管理	プログラムファイルの管理方法を明確にすること	基礎	プログラムはgitを利用して管理しております。
実41			プログラムファイルのバックアップを確保すること	基礎	プログラムは定期的にバックアップを行っております。
実42		(4) ネットワーク設定情報管理	ネットワークの設定情報の管理を行うこと	基礎	ネットワークの設定情報はを管理しております。また構成図を作成しております。
実43			ネットワークの設定情報のバックアップを確保すること	基礎	
実44			運用時のドキュメントの保管管理方法を明確にすること	基礎	ドキュメント保存を利用しているクラウドサービスは情報セキュリティフレームワークと、COBITフレームワークに

実45		(5) 運用時ドキュメント管理	災害時の復旧対応に必要なドキュメントのバックアップを確保すること	基礎	ドキュメント保存を利用しているクラウドサービスは情報セキュリティレベル、COBITレベル等に基づいたポリシーを確立しています。
実46		(6) 運行監視	システムの運行状況の監視体制を整備すること	基礎	死活監視を実施しており、障害発生時に対応できる体制を整えています。
実47	4 各種設備管理	(1) 資源管理	各種資源の能力及び使用状況の確認を行うこと	基礎	負荷監視を実施しており、障害発生時に対応できる体制を整えています。
実48		(2) 機器の管理	ハードウェア及びソフトウェアの管理を行うこと	基礎	利用しているサーバーはISO27001規格に準じ、ハードウェア資産は独自の在庫管理ツールを使用して担当者によって管理、監視されています。
実49			機器の管理方法を明確にすること	基礎	
実50			ネットワーク関連機器の保護措置を講ずること	付加	
実51			機器の保守方法を明確にすること	基礎	
実52			機器の予防保守を実施すること	付加	
実53		(3) コンピュータ関連設備の保守管理	コンピュータ関連設備の管理方法を明確にすること	基礎	利用しているサーバーは物理的なセキュリティ対策としては、フェンス、壁、セキュリティスタッフ、監視カメラ、侵入検知システムやその他エレクトロニクスを含む手段を用いて厳重な管理を行っています。これには、ネットワークケーブルの適切な保護も含まれています。
実54			コンピュータ関連設備の保守方法を明確にすること	基礎	
実55			コンピュータ関連設備の能力及び使用状況の確認を行うこと	基礎	
実56		(4) 入退館（室）管理	入館（室）の資格付与及び鍵の管理を行うこと	基礎	利用しているサーバーは、入退室や各境界で厳密に管理されています。アクセスを許可された従業員は、データセンターに入るために2要素認証を最低2回パスする必要があります。すべての従業員は企業理念に沿った行動と倫理を行なうよう、定期的な情報セキュリティの訓練を行ない、それの完了の承認を得る必要があります。定期的に行なわれるコンプライアンスの監査は、これらを従業員が理解し、確立されたポリシーに従っていることを検証するために実行されます。
実57			入退館管理を行うこと	基礎	
実58			入退室管理を行うこと	基礎	
実59			入室後の作業を管理すること	基礎	
実60		(5) 監視	各種設備の監視体制を整備すること	基礎	
実61	5 システムの利用	(1) 取引の管理	各取引の操作権限を明確にすること	基礎	対象外
実62			オペレータカードの管理を行うこと	付加	対象外
実63			取引の端末機操作の内容を記録・検証すること	基礎	対象外
実64			顧客からの届出の受付体制を整備し、事故口座の管理を行うこと	付加	対象外
実65		(2) 入出力管理	データの入力管理を行うこと	基礎	入力時にバリデーションチェックを行っています。
実66			出力情報の作成、取扱いについて、不正防止及び機密保護対策を講ずること	基礎	出力情報は、都度記録される仕組みとなっています。
実67		(3) 帳票管理	未使用重要帳票の管理方法を明確にすること	付加	対象外
実68			重要な印字済帳票の取扱方法を明確にすること	基礎	対象外
実69		(4) 顧客データ保護	顧客データの保護策を講ずること	基礎	対象外
実70	6 緊急時の対応	(1) 障害時・災害時対応策	障害時・災害時の関係者への連絡手順を明確にすること	基礎	障害発生時には担当者に自動的にメールが送信され、対応できる体制を整えており、担当を分離させて早期解決を図れるようにしています。
実71			障害時・災害時復旧手順を明確にすること	基礎	
実72			障害の原因を調査・分析すること	基礎	
実73		(2) コンティンジェンシープランの策定	コンティンジェンシープランを策定すること	基礎	
実74		(3) バックアップサイト	バックアップサイトを保有すること	付加	バックアップは常に保有しております。
実75	7 システム開発・変更	(1) システム開発・変更管理	システムの開発・変更手順を明確にすること	基礎	システムの開発・変更に関する管理手順を明確化しています。
実76			テスト環境を整備すること	基礎	本番環境とは別のテスト環境を用意して、事前に十分な検証を行った上で本番環境への移行を実施しています。
実77			本番への移行手順を明確にすること	基礎	
実78		(2) 開発・変更時ドキュメント管理	開発・変更時のドキュメントの作成手順を明確にすること	付加	開発に関するドキュメントを作成しております。
実79			開発・変更時のドキュメントの保管管理方法を明確にすること	基礎	ドキュメントは変更点があれば都度、加筆修正をしていｒます。
実80		(3) パッケージの導入	パッケージの評価体制を整備すること	付加	オープンソースソフトウェアを利用する場合には、レビューやリスク評価により安全性を確認しています。
実81			パッケージの運用・管理体制を明確にすること	付加	
実82		(4) システムの廃棄	システムの廃棄計画を策定するとともに、廃棄手順を明確にすること	基礎	リソース見通しに基づく廃棄計画を策定しています。
実83			システム廃棄時の情報漏洩防止対策を講ずること	基礎	
実84	8 システムの信頼性向上対策	(1) ハードウェアの予備	本体装置の予備を設けること	付加	クラウドサーバーを利用することでハードウェアの予備に関しての対応をしております。
実85			周辺装置の予備を設けること	付加	
実86			通信系装置の予備を設けること	付加	
実87			回線の予備を設けること	付加	
実88			端末系装置の予備を設けること	付加	
実89		(2) ソフトウェア等の品質向上対策	必要となるセキュリティ機能を取り組むこと	基礎	定期的なアップデートなどによって顧客に影響を与えるサービスの変更は、検証・試験・承認及び情報提供がなされるようになっています。
実90			設計段階におけるソフトウェアの品質を確保すること	基礎	
実91			プログラム作成段階における品質を確保すること	基礎	
実92			テスト段階におけるソフトウェアの品質を確保すること	基礎	
実93			プログラムの配布を考慮したソフトウェアの信頼性を確保すること	基礎	
実94			パッケージ導入にあたり、ソフトウェアの品質を確保すること	基礎	
実95			定型的な変更作業時の正確性を確保すること	基礎	
実96			機能の変更、追加作業時の品質を確保すること	基礎	
実97			ファイルに対する排他制御機能を設けること	付加	ファイルの取り扱いは、排他制御となっており、不整合が生じないようになっています。
実98			ファイル突合機能を設けること	付加	必要に応じて対応しております。
実99		(3) 運用時の信頼性向上対策	オペレーションの自動化、簡略化を図ること	付加	自動化できるモノに対しては自動化処理を行っております。
実100			オペレーションのチェック機能を充実すること	基礎	
実101			負荷状態の監視制御機能を充実すること	基礎	
実102		(4) 障害の早期発見・回復機能	システム運用状況の監視機能を設けること	基礎	システムへのアクセスや負荷は常に監視を続けております。
実103			障害の検出及び障害箇所の切り分け機能を設けること	付加	
実104			障害時の縮退・再構成機能を設けること	付加	障害時にサービスに影響を及ぼさないような対策を取っています。 また、復旧作業対策も実施しており、サービスを継続運用できる態勢を取っています。
実105			障害時の取引制限機能を設けること	付加	対象外
実106			障害時のリカバリ機能を設けること	基礎	障害時にサービスに影響を及ぼさないような対策を取っています。 また、復旧作業対策も実施しており、サービスを継続運用できる態勢を取っています。
実107	9 個別業務・サービス	(1) カード取引サービス	カードの管理方法を明確にすること	付加	対象外
実108			カード取引等に関する犯罪について注意喚起を行うこと	付加	対象外
実109			CD・ATM等の機械式預貯金取引における正当な権限者の取引を確保すること	付加	対象外
実110			指定された口座のカード取引監視方法を明確にすること	付加	対象外
実111			カードの偽造防止対策のための技術的措置を講ずること	付加	対象外
実112		(2) インターネット・モバイルサービス	インターネット・モバイルサービスの不正利用を防止すること	付加	対象外
実113			インターネット・モバイルサービスの使用状況を利用者が確認できるようにすること	付加	対象外
実114			インターネット・モバイルサービスの安全対策に関する情報開示をすること	付加	対象外
実115			インターネット・モバイルサービスの顧客対応方法を明確にすること	付加	対象外
実116			インターネット・モバイルサービスの運用管理方法を明確にすること	付加	対象外
実117			インターネット・モバイルサービスにおいて口座開設等を行う場合は、本人確認を行うこと	付加	対象外
実118		(3) 渉外端末の管理	渉外端末の運用管理方法を明確にすること	付加	対象外
実119		(4) CD・ATM等及び無人店舗の管理	CD・ATM等及び無人店舗の運用管理方法を明確にし、かつ不正払戻防止の措置を講ずること	付加	対象外
実120			無人店舗の監視体制を明確にすること	付加	対象外
実121			無人店舗の防犯体制を明確にすること	付加	対象外
実122			無人店舗の障害時・災害時の対応方法を明確にすること	付加	対象外
実123			無人店舗の関係マニュアルの整備を行うこと	付加	対象外
実124			CD・ATM等の遠隔制御機能を設けること	付加	対象外
実125		(5) インストアブランチ	インストアブランチの出店先の選定基準を明確にすること	付加	対象外
実126		(6) コンビニATM	コンビニATMの出店先の選定基準を明確にすること	付加	対象外
実127			コンビニATMの現金装填等メンテナンス時の防犯対策を講ずること	付加	対象外
実128			コンビニATMの障害時・災害時対応手順を明確にすること	付加	対象外
実129			コンビニATMのネットワーク関連機器、伝送データの安全対策を講ずること	付加	対象外
実130			コンビニATMの所轄の警察及び警備会社等関係者との連絡体制を確立すること	付加	対象外

実131			コンビニATMの顧客に対して犯罪に関する注意喚起を行うこと	付加	対象外
実132		(7) デビッドカード・サービス	デビッドカード・サービスにおける安全対策を講ずること	付加	対象外
実133			デビッドカードの口座番号・暗証番号等の安全性を確保すること	付加	対象外
実134			デビッドカード利用時の顧客保護の措置を講ずること	付加	対象外
実135			デビッドカード利用上の留意事項を顧客に注意喚起すること	付加	対象外
実136		(8) 前払式支払手段	前払式支払手段における機器及び媒体の盗難、破損等に伴い、利用者が被る可能性がある損失及び責任を明示すること	付加	対象外
実137			前払式支払手段における電子的価値の保護機能、または不正検知の仕組みを設けること	付加	対象外
実138		(9) 電子メール・イントラネットの利用	電子メールの運用方針を明確にすること	付加	対象外
実139			電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること	付加	対象外
実140		(10) 生体認証	生体認証における生体認証情報の安全管理措置を講ずること	付加	対象外
実141			生体認証の特性を考慮し、必要な安全対策を講ずること	付加	対象外
実142		(11) QRコード決済	QRコード決済における安全対策を講ずること	付加	対象外
実143			QRコード決済利用時の顧客保護の措置を講ずること	付加	対象外
実144			QRコード決済利用時の留意事項を顧客に注意喚起すること	付加	対象外
設 1	1 コンピュータセンター	(1) 建物（環境）	各種災害、障害が発生しやすい地域を避けること	–	ブロードトークが稼働しているデータセンターは、革新的なデザインと工学的なアプローチを活用し、環境的なリスクに対して、物理的な保護を行なっています。
設 2		(2) 建物（周囲）	立地環境の変化に伴う災害及び障害の発生の可能性を調査し、防止対策を講ずること	–	ブロードトークが稼働しているデータセンターは、外部からはそれとはわからないようになっています。物理的なセキュリティ対策としては、フェンス、壁、セキュリティスタッフ、監視カメラ、侵入検知システムやその他エレクトロニクスを用いた厳重な管理を行っています。
設 3			敷地には通路を確保すること	–	
設 4			隣接物との間隔を十分に取ること	–	
設 5			塀または柵及び侵入防止装置を設けること	–	
設 6			看板等を外部に出さないこと	–	
設 7			建物には避雷設備を設置すること	–	
設 8			建物はコンピュータシステム関連業務専用、または建物内においてコンピュータシステム関連業務専用の独立区画とすること	–	
設 9			敷地内の通信回線・電力線は、切断・延焼の防止措置を講ずること	–	
設 10		(3) 建物（構造）	耐火建築物であること	–	ブロードトークが稼働しているのデータセンターは環境的なリスクに対する物理的な保護を備えています。AWSの環境的なリスクに対する物理的な保護は、独立した監査人によって検証され、ISO27002のベストプラクティスに準拠することが承認されています。
設 11			構造の安全性を有すること	–	
設 12			外壁、屋根等は十分な防水性能を有すること	–	
設 13			外壁等に強度を持たせること	–	
設 14		(4) 建物（開口部）	窓には防火措置を講ずること	–	ブロードトークが稼働しているデータセンターは物理的なセキュリティ対策としては、フェンス、壁、セキュリティスタッフ、監視カメラ、侵入検知システムやその他エレクトロニクスを含む手段を用いて厳重な管理を行っています。
設 15			防犯措置を講ずること	–	
設 16			常時利用する出入口は1カ所とし、出入管理設備、防犯設備を設置すること	–	
設 17			非常口を設けること	–	
設 18			防水措置を講ずること	–	
設 19			出入口の扉は、十分な強度を持たせるとともに、錠を付けること	–	
設 20		(5) 建物（内装等）	不燃材料及び防炎性能を有するものを使用すること	–	ブロードトークが稼働しているデータセンターは環境的なリスクに対する物理的な保護を備えています。AWSの環境的なリスクに対する物理的な保護は、独立した監査人によって検証され、ISO27002のベス
設 21			地震による内装等の落下・損壊の防止措置を講ずること	–	
設 22		(6) コンピュータ室・データ保管室（位置）	災害を受けるおそれの少ない位置に設置すること	–	ブロードトークが稼働しているデータセンターは、外部からはそれとはわからないようになっています。物理的なセキュリティ対策としては、フェンス、壁、セキュリティスタッフ、監視カメラ、侵入検知システムやその他エレクトロニクスを用いた厳重な管理を行っています。
設 23			外部から容易に入れない位置に設置すること	–	
設 24			室名等の表示は付さないこと	–	
設 25			必要空間を確保すること	–	
設 26			専用の独立した室とすること	–	
設 27		(7) コンピュータ室・データ保管室（開口部）	常時利用する出入口は1カ所とし、前室を設けること	–	ブロードトークが稼働しているデータセンターは、外部からはそれとはわからないようになっています。物理的なセキュリティ対策としては、フェンス、壁、セキュリティスタッフ、監視カメラ、侵入検知システムやその他エレクトロニクスを用いた厳重な管理を行っています
設 28			出入口の扉は、十分な強度を持たせるとともに、錠を付けること	–	
設 29			窓に防火、防水、破損防止措置を講じ、外部から室内の機器等が見えない措置を講ずること	–	
設 30			非常口、避難器具、誘導灯等を設置すること	–	
設 31		(8) コンピュータ室・データ保管室（構造・内装等）	独立した防火区画とすること	–	ブロードトークが稼働しているデータセンターは環境的なリスクに対する物理的な保護を備えています。
設 32			漏水防止対策を講ずること	–	
設 33			静電気の防止措置を講ずること	–	
設 34			内装等には不燃材料及び防炎性能を有するものを使用すること	–	
設 35			地震による内装等の落下・損壊の防止措置を講ずること	–	
設 36			フリーアクセス床は地震時に損壊しない構造とすること	–	
設 37		(9) コンピュータ室・データ保管室（設備）	自動火災報知設備を設置すること	–	ブロードトークが稼働しているデータセンターは環境及びセキュリティに関するリスクに対する物理的な保護を備えています。これには、火気の検知と抑制、空気のコンディションを最適なレベルに調整する空調、物理的なセキュリティ制御などが含まれます。
設 38			非常時の連絡装置を設置すること	–	
設 39			消火設備を設置すること	–	
設 40			ケーブルの難燃化、延焼防止措置を講ずること	–	
設 41			排煙設備を設置すること	–	
設 42			非常用照明設備、携帯用照明器具を設置すること	–	
設 43			水使用設備を設置しないこと	–	
設 44			地震感知器を設置すること	–	
設 45			出入口には出入管理設備、防犯設備を設置すること	–	
設 46			温湿度自動記録装置または温湿度警報装置を設置すること	–	
設 47			ネズミの害を防止する措置を講ずること	–	
設 48		(10) コンピュータ室・データ保管室（コンピュータ機器、什器、備品）	什器・備品は不燃性とすること	–	ブロードトークが稼働しているデータセンターは地震を含む局所的な環境リスクに対する警報と物理的な保護を備えています。
設 49			静電気防止措置を講ずること	–	
設 50			耐震措置を講ずること	–	
設 51			運搬車等に固定装置を取り付けること	–	
設 52		(11) 電源室・空調機械室	災害を受けるおそれの少ない場所に設置すること	–	ブロードトークが稼働しているデータセンターは環境リスクに対する物理的な保護を備えています。これには、火気の検知と抑制、空気のコンディションを最適なレベルに調整する空調、完全に冗長化された電源システムなどが含まれます。物理的なセキュリティ対策としては、フェンス、壁、セキュリティスタッフ、監視カメラ、侵入検知システムやその他エレクトロニクスを使った手段を含む制限を行っています。
設 53			保守点検に必要な空間を確保すること	–	
設 54			専用の独立した室とすること	–	
設 55			無窓とし、錠を付けた扉を設置すること	–	
設 56			耐火構造とすること	–	
設 57			自動火災報知設備を設置すること	–	
設 58			ガス系消火設備を設置すること	–	
設 59			空調設備の漏水防止措置を講ずること	–	
設 60			ケーブル、ダクトからの延焼防止措置を講ずること	–	
設 61		(12) 電源設備	電源設備の容量には余裕を持たせること	–	ブロードトークが稼働しているデータセンターの電力システムは、完全に冗長性をもち、1日24時間・週7日、運用に影響を与えることなくメンテナンス可能な設計がなされています。施設内の重要かつ不可欠な箇所における電力障害に際しては、無停電電源装置（UPS）がバックアップ電力を供給します。データセンターは、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ます。
設 62			電源は複数回線で引き込むこと	–	
設 63			良質な電力を供給する設備を設置すること	–	
設 64			自家発電設備、蓄電池設備を設置すること	–	
設 65			電源設備には避雷設備を設置すること	–	
設 66			電源設備には耐震措置を講ずること	–	
設 67			分電盤からコンピュータ機器への電源の引込みは専用とすること	–	
設 68			負荷変動の激しい機器との共用を避けること	–	
設 69			コンピュータシステムのアースは適切に施工すること	–	
設 70			過電流、漏電により各機器に障害を及ぼさないよう措置を講ずること	–	
設 71			防災、防犯設備用の予備電源を設置すること	–	

設 72		(13) 空調設備	空調設備の能力には余裕を持たせること	–	ブロードトークが稼働しているデータセンターは環境的なリスクに対する物理的な保護を備えるよう開発されています。 サーバの過熱を予防し、サービスの中断の可能性を下げるためにサーバやその他のハードウェアを一定の温度に保つには、空調が必要です。データセンターは空気のコンディションを最適なレベルに保つよう、調整されています。作業員とシステムが、温度と湿度を適切なレベルになるよう監視及び制御を実施しています。
設 73			空調設備は安定的に空気調和できる措置を講ずること	–	
設 74			空調設備はコンピュータ室専用とすること	–	
設 75			空調設備の予備を設置すること	–	
設 76			空調設備には自動制御装置、異常警報装置を設置すること	–	
設 77			空調設備には侵入、破壊防止対策を講ずること	–	
設 78			空調設備には耐震措置を講ずること	–	
設 79			空調設備の断熱材料、給排気口は不燃材料とすること	–	
設 80		(14) 監視制御設備	監視制御設備を設置すること	–	ブロードトークが稼働しているデータセンターは電気的、機械的、物理的セキュリティ及び生存監視に関するシステムと設備を監視し、如何なる問題も速やかに特定されるようにしています。
設 81			中央管理室を設置すること	–	
設 82		(15) 回線関連設備	回線関連設備には錠をつけること	–	ブロードトークが稼働しているデータセンターは物理的なセキュリティ対策としては、フェンス、壁、セキュリティスタッフ、監視カメラ、侵入検知システムやその他エレクトロニクスを含む手段を用いて厳重な管理を行っています。これには、ネットワークケーブルの適切な保護も含まれています。
設 83			回線関連設備の設置場所の表示は付さないこと	–	
設 83-1			回線は、専用の配線スペースに設けること	–	
設 84	2 本部・営業店等	(1) 建物（周囲）	敷地内の通信回線・電力線の切断・延焼の防止措置を講ずること	–	対象外
設 85		(2) 建物（構造）	耐火建築物であること	–	対象外
設 86			構造の安全性を有すること	–	対象外
設 87			外壁、屋根等は十分な防水性能を有すること	–	対象外
設 88			外壁等の強度を確保すること	–	対象外
設 89		(3) 建物（開口部）	窓には防火措置を講ずること	–	対象外
設 90			窓・扉には防犯措置を講ずること	–	対象外
設 91			出入口の扉は十分な強度を持たせるとともに、鍵を付けること	–	対象外
設 92			通用口には、入室者の識別設備を設置すること	–	対象外
設 93			出入口には防水措置を講ずること	–	対象外
設 94		(4) 建物（内装等）	天井及び壁は、遮熱、吸音機能を持たせること	–	対象外
設 95			地震による内容等の落下・損壊の防止措置を講ずること	–	対象外
設 96			床表面は、塵埃や静電気が発生しにくい材質のものとすること	–	対象外
設 97			端末機器への回線等は、切断のおそれのない措置を講ずること	–	対象外
設 98			端末機器に接続している回線、電源ケーブル等への漏水防止対策を講ずること	–	対象外
設 99		(5) 建物（設備）	自動火災報知設備及び消火器を設置すること	–	対象外
設 100			設備等の耐震措置を講ずること	–	対象外
設 101			耐火金庫を設置すること	–	対象外
設 102			避雷設備を設置すること	–	対象外
設 103			防犯措置を講ずること	–	対象外
設 104		(6) 建物（回線関連設備）	回線関連設備の設置場所の表示は付さないこと	–	対象外
設 105			回線関連設備には錠をつけること	–	対象外
設 106			回線関連設備から各端末機器までの配線を二重化すること	–	対象外
設 107		(7) 建物（電源設備）	電源ケーブルは、端末機器等に支障を来さないよう布設すること	–	対象外
設 108			防災、防犯設備用の予備電源を設置すること	–	対象外
設 109			自家発電設備等を設置すること	–	対象外
設 110		(8) 建物（空調設備）	空調設備を設置すること	–	対象外
設 111		(9) 建物（自動機器室）	通話装置を設置すること	–	対象外
設 112			非常通報装置を設置すること	–	対象外
設 113			防犯措置を講ずること	–	対象外
設 114			照明設備及び非常用照明設備を設置すること	–	対象外
設 115			扉は、一部を素通しにすること	–	対象外
設 116			自動機器の現金の装填と保守のための必要な空間を確保すること	–	対象外
設 117			自動運行設備を設置すること	–	対象外
設 118		(10) 建物（端末機器）	端末機器には耐震措置を講ずること	–	対象外
設 119			機器のアースを確実に取ること	–	対象外
設 120			漏水及び塵埃等に対する保護措置をとること	–	対象外
設 121		(11) サーバー設置場所（位置）	災害を受けるおそれの少ない位置とすること	–	対象外
設 122			外部から容易に入れない位置とすること	–	対象外
設 123			室名等の表示は付さないこと	–	対象外
設 124			専用の区画とすること	–	対象外
設 125		(12) サーバー設置場所（構造・内装等）	防火区画に設置すること	–	対象外
設 126			漏水防止対策を講ずること	–	対象外
設 127			フリーアクセス床は地震に備えて耐震措置を講ずること	–	対象外
設 128		(13) サーバー設置場所（設備）	消防設備を有すること	–	対象外
設 129			地震感知器を設置すること	–	対象外
設 130			サーバーを設置した室の出入口には出入管理設備、防犯設備を設置すること	–	対象外
設 131			温湿度自動記録装置または温湿度警報装置を設置すること	–	対象外
設 132			空調設備を設置すること	–	対象外
設 133			ネズミの害を防止する措置を講ずること	–	対象外
設 134			電源コンセントの抜け防止対策を講ずること	–	対象外
設 135		(14) インストアブランチ	他の区画からの侵入防止措置を講ずること	–	対象外
設 136			使用するストアの設備状況に応じて、適切な補強策を講ずること	–	対象外
設 137	3 流通・小売店舗との連携チャネル	(1) コンビニATM	防犯措置を講ずること	–	対象外
監1	1 システム監査	(1) システム監査	システム監査体制を整備すること	基礎	随時、システム監査体制の見直しを行っております。