情報セキュリティ体制
(第 7.05 版)

株式会社　シャノン

株式会社シャノン

情報セキュリティ体制　（お客様公開資料）

SHANON
Marketing is Science

1　はじめに 3
1-1　情報セキュリティ基本方針 4
1-2　認証取得概要 4
2　情報セキュリティ体制 5
2-1　各種社内運用手順 5
2-1-1　サービスやインフラにおける各種作業に手順について 5
2-1-2　各種承認フローにおける承認権限者について 5
2-1-3　本番環境を変更する場合の事前検証について 5
2-1-4　運用変更の権限について 5
2-1-5　職務の分離について 5
2-1-6　OS やミドルウェアのバージョン変更について 5
2-2　個人情報の管理 6
2-2-1　個人情報の管理について 6
2-3　ウイルス対策 6
2-3-1　ウイルスの侵入および感染に対する体制について 6
2-3-2　ウイルス対策ソフトについて 6
2-3-3　ウイルス対策ソフトのパターンファイル 6
2-4　ネットワーク設定の管理 6
2-4-1　ネットワーク設定へのアクセスついて 6
2-4-2　ネットワーク設定情報の管理について 6
2-5　ファイアウォールの管理 7
2-5-1　不正アクセスの防止について 7
2-5-2　非武装セグメント(DMZ)構成について 7
2-5-3　セキュリティログの調査・分析について 7
2-6　管理用リモートログイン 7
2-6-1　リモートログインの制限について 7
2-6-2　リモートログインによる操作のログ取得 7
2-7　暗号鍵の管理 8
2-7-1　暗号鍵の運用について 8
2-7-2　暗号鍵の管理について 8
2-8　情報機器の管理 8
2-8-1　機器の持ち出しの管理について 8
2-8-2　機器のたな卸しについて 8
2-8-3　機器の保護、故障時の対応について 8
2-8-4　モバイル機器の取り扱いについて 8
2-8-5　情報機器の破棄について 8
2-9　障害対応の体制 9

2-9-1　リカバリー手順について……9
2-9-2　連絡体制について……9
2-9-3　緊急対応、復旧訓練について……9
2-9-4　再発防止策について……9
2-9-5　障害発生時の社内外への報告体制について……9
2-10　システム監視体制……10
2-10-1　システムエラー、サーバの監視について……10
2-10-2　照合チェック体制について……10
2-10-3　アクセス状況の管理について……10
2-11　アクセス管理……10
2-11-1　アクセス権限について……10
2-11-2　パスワードについて……10
2-11-3　物理的アクセスについて……10
2-11-4　データセンターについて……11
2-11-5　社内 LAN の接続ついて……11
2-11-6　重要なデータの通信について……11
2-12　監査体制……11
2-12-1　内部監査について……11
2-12-2　外部監査について……11
2-12-3　システム、機器の保守点検について……11
2-12-4　品質について……11
2-12-5　第三者組織によるセキュリティ監査……11
2-13　バックアップ……12
2-13-1　バックアップについて……12
2-13-2　保管について……12
2-14　アプリケーションの堅牢性……12
2-14-1　入力ミスについて……12
2-14-2　論理チェックについて……12
2-14-3　大量データ処理について……12
2-15　アプリケーションの修正……13
2-15-1　影響範囲の調査について……13
2-15-2　修正する際のテストについて……13
2-15-3　セキュリティの脆弱性対応について……13
3　お客様へのお願い……13
4　変更履歴……14

1　はじめに

株式会社シャノンでは、個人情報等の重要情報を取り扱う事業性から、アプリケーションの設計・開発・保守・運用において、各種セキュリティ対策を行うとともに、万全なセキュリティ体制をもってお客様にサービスを提供することを心がけております。

弊社は、2004 年 12 月 13 日に情報セキュリティマネジメントシステムの英国規格 BS7799、ならびに、日本における情報セキュリティの第三者認証制度である ISMS 適合性評価制度に基づく認証を同時取得し、以降更新審査においても高い評価を得ております。これにより、弊社の情報セキュリティマネジメントシステムが国際水準を満たすものであることが、第三者機関から認められております。

また、ISMS 認証基準の国際規格化(ISO/IEC 27001:2013)及び JIS 化(JIS Q 27001：2014)に伴い、弊社の認証も 2015 年 1 月に ISO/JIS を取得いたしました。

1-1　情報セキュリティ基本方針

当社、株式会社シャノンは、クラウドサービス開発企業として、ただツールや技術だけを提供することにとどまらず、お客様が抱えている問題や、掲げている目的と目標を的確にとらえ、お客様とともに考え、解決する姿勢であり続けることを厳格な使命としています。その使命のもと、お客様の事業内容・組織内容設定手順など企業の極秘事項までも含み情報を収集・分析し知的情報を提供します。これらのサービスは、当社とお客様との信頼関係があってはじめて成り立つ事業です。

今後当社がお客様の信頼を保持し、さらなる事業努力により、より良いサービスを提供するためには、これらの情報を企業の最も重要な財産、いわゆる情報資産と位置づけ、適切な安全対策を実施し紛失・盗難・不正使用など様々な脅威から確実に保護しなければなりません。その為には物理的・環境的・技術的なセキュリティの具体的対策ともに 経営者・社員ともどもセキュリティに対して高い意識を持ち、セキュリティを尊重して行動を取ることが求められます。当社がこのような具体策と意識を持ち事業展開する姿勢が、お客様を最優先にとらえた顧客満足であり、事業継続性になります。

ここに「**情報セキュリティポリシー宣言書**」を定め、当社の定めた情報セキュリティ手順書の内容を熟知し遵守します。

1-2　認証取得概要

事業社名	株式会社シャノン
登録範囲	1. マーケティングクラウドサービスの企画・開発 2. マーケティングクラウドサービスの導入及び運用 3. マーケティングコンサルティング 4. デジタル化サービス 5. メタバースイベントサービスの企画・開発 6. メタバースイベントサービスの導入・運用
登録番号	IS 89514 / ISO 27001
認定機関	米国規格協会-米国品質協会による認定機関（ANAB） 一般財団法人日本情報経済社会推進協会(JIPDEC)
審査登録機関	BSI グループジャパン株式会社
登録日	2004 年 12 月 13 日

2　情報セキュリティ体制

弊社のアプリケーション開発・保守・運用体制、サービス提供体制において、重要である大別した項目を以下に列挙します。詳細な情報が必要な場合は、弊社営業担当にご連絡いただけますようお願いいたします。

2-1　各種社内運用手順

2-1-1　サービスやインフラにおける各種作業の手順について

インフラ、サービスの各種作業に対して操作手順書を設けており、その手順書に則った形で作業するという作業申請書を提出し、技術統括役員による承認の上、作業を行います。

2-1-2　各種承認フローにおける承認権限者について

各手順書の中で、その分野に精通している承認権限者を規定しています。

2-1-3　本番環境を変更する場合の事前検証について

本番環境を変更する場合は事前に申請を行い、品質管理者によるテストを実施し修正する開発プロセスが規定されています。このプロセスで承認された更新のみが本番環境へ適用されます。

2-1-4　運用変更の権限について

運用変更の影響範囲を調査し、問題やリスク分析は技術担当者が行い、技術統括役員が最終承認を行います。

2-1-5　職務の分離について

個人のミスおよび悪意を持った不正行為を排除するため、開発担当者、品質管理担当者、サービス運用担当者を分離しています。また、本番サービスにアクセスして作業を行う場合は、必ず許可権限をもった管理職の承認が必要となっており、作業できる担当者も限定されています。

2-1-6　OS やミドルウェアのバージョン変更について

バグフィクスやセキュリティ対応の観点から、重要度に応じて OS やミドルウェアへのバージョン変更作業を行います。更新を行う際は、本番環境とは切り離された社内環境で影響範囲の検証を行った上で、社内で規定された運用変更プロセスに従い技術統括役員の承認を行い、本番環境への適用を実施致します。

2-2　個人情報の管理

2-2-1　　個人情報の管理について

個人情報の取り扱いに関しましては、別途「シャノン個人情報保護体制」をご覧ください。

2-3　ウイルス対策

2-3-1　　ウイルスの侵入および感染に対する体制について

ウイルスの侵入および感染に対する防御策、検知方法、そして復旧の手順を規定しております。
また、随時新たな防御策等の導入を積極的に行っております。

2-3-2　　ウイルス対策ソフトについて

ウイルスの侵入および感染に備えて、ウイルスを検出し駆逐するための信頼度の高いウイルス対策ソフトを社内の全端末、サービスを提供しているアプリケーションサーバに導入しており、常に最新のウイルスに対応しております。

2-3-3　　ウイルス対策ソフトのパターンファイル

ウイルス対策ソフトは、パターンファイルの更新を１日１回以上おこなっています。

2-4　ネットワーク設定の管理

2-4-1　　ネットワーク設定へのアクセスついて

ネットワーク機器の設定情報が不正に変更されないように、特権権限者を設け、アクセス制限を行っております。

2-4-2　　ネットワーク設定情報の管理について

ネットワーク機器の設定情報の不正な変更、障害時に早急に対応するためにバックアップを取得し、バックアップの保管・管理方法を明確に規定しております。

2-5　ファイアウォールの管理

2-5-1　　不正アクセスの防止について

インターネットから不正アクセスを防止するため、外部と接続する部分にファイアウォールを設置しております。

2-5-2　　非武装セグメント(DMZ)構成について

外部からの不正なアクセスを排除し、かつ同時に内部ネットワークを守るため、DMZ 構成を採用しております。

2-5-3　　セキュリティログの調査・分析について

疑わしいアクセスの試行に関するログの調査・分析を定期的に行っております。

2-6　管理用リモートログイン

2-6-1　　リモートログインの制限について

本番環境のネットワークへリモートログインする場合は、特定の管理用サーバを経由するよう経路を限定しております。また、管理用サーバへログインできるネットワークアドレスも限定しており、弊社オフィスからのアクセスのみ許可しております。ユーザ認証方法は公開鍵方式を採用しており、ブルートフォース攻撃のリスクに対応しています。リモートログインできる社員は技術担当者の中でも一部に限定し、権限変更には情報セキュリティ推進責任者の承認が必要としています。

2-6-2　　リモートログインによる操作のログ取得

運用保守のため本番環境にリモートログインする際も、管理用サーバで全ての操作を録画監視しております。取得した録画ログは、管理者でも一部の者しかアクセス権限を有していない高セキュリティサーバにて保管し有事の際の監査対象として保存しております。

2-7　暗号鍵の管理

2-7-1　　暗号鍵の運用について

不正行為を防止するため、暗号鍵の生成、保管等に関わる手続きを規定しております。

2-7-2　　暗号鍵の管理について

暗号鍵の管理書類等は責任者が厳重に管理を行っております。

2-8　情報機器の管理

2-8-1　　機器の持ち出しの管理について

原則として、社外に機器を持ち出すことを禁止し、必要な場合は情報セキュリティ委員会の承認を必要としております。

2-8-2　　機器のたな卸しについて

社内における全ての情報機器のたな卸しを定期的に行っております。

2-8-3　　機器の保護、故障時の対応について

不正使用、破壊、盗難等を防止するため、重要なデータを扱うシステムを構成する機器は堅牢製の高い場所に保管し、厳重なルールに基づいて保護されております。

故障時等の緊急対応を迅速に行うため、重要な機器に対して代替機を用意しております。

2-8-4　　モバイル機器の取り扱いについて

使用している携帯電話・ノートPCは、認証機能や暗号化を使用することにより紛失や盗難時のデータ漏洩が発生しないようにしております。

2-8-5　　情報機器の破棄について

データを物理消去し、情報機器は廃棄業者に廃棄依頼を行います。委託する破棄業者は、事前に個人情報委託が可能か運用体制の監査を行い破棄証明書の発行が可能な破棄業者を利用することとしています。

2-9　障害対応の体制

2-9-1　　リカバリー手順について

復旧手順書を設けており、社内・社外の状況の変化によってリスクが変化する場合にその都度変更の必要性の有無を検証しております。変更を行う際は、変更の手順に則って変更を行います。

復旧手順書は、障害の状況にあった対応をするため、縮退運用の方法や通常と異なる手順も規定しております。

2-9-2　　連絡体制について

障害時の緊急連絡体制を設け、指揮系統も明確にしております。

2-9-3　　緊急対応、復旧訓練について

定期的に内部 LAN、機器のネットワーク障害、サーバの H/W 障害によるサービス停止への対応等を想定した復旧訓練を行っております。

2-9-4　　再発防止策について

アプリケーションの障害が発生した場合は、品質管理担当者で再発防止策を決定し、対策が効果的であるかどうかも検証しております。

2-9-5　　障害発生時の社内外への報告体制について

障害時の初動ルール、顧客連絡ルールを情報セキュリティ委員会で制定しております。

2-10 システム監視体制

2-10-1 システムエラー、サーバの監視について

監視可能な全サーバ・ネットワークデバイスを対象に、24 時間監視ツールによる稼動監視とリソース使用状況の閾値監視を数分間隔で行っております。機器の停止や閾値を超過した場合は、運用管理者の携帯電話に通知されます。

2-10-2 照合チェック体制について

システムが正常に稼動していることを確認するために、HTTP、HTTPS、PING、SMTP、ディスク容量を監視しております。

2-10-3 アクセス状況の管理について

システムやデータへのアクセス記録としてログを取得し、定期的なログチェックを行い保管しております。また、統計情報として解析しインフラの増強計画に利用しております。

2-11 アクセス管理

2-11-1 アクセス権限について

社員の各情報に対するアクセス権限を設定しています。特に本番環境へのアクセス権限は、社員の中でも運用管理者のみが保持しておりアクセス権限の付与・削除は技術担当役員の承認を必要とします。

2-11-2 パスワードについて

パスワードに関する管理規定を設けております。パスワードは英数字を混ぜた 8 文字以上としています。(本番環境のサーバに関しては英数記号が含まれた 16 文字以上。また、一定期間で必ず変更するルールとなっております)。顧客に対しても利用規約等で漏洩防止の注意喚起をしております。

2-11-3 物理的アクセスについて

社内を低セキュリティエリアと高セキュリティエリアに明確に分離し電子錠による入退出管理を行っています。第三者が高セキュリティエリアに入る場合は入退室の記録を残しております。また、機密情報の媒体は施錠管理をした専用の保管場所で管理し、データに関しては専用ファイルサーバにて管理しています。ネットワーク経由の不正侵入に関しては、本番環境と同様の不正侵入対策を行っています。

2-11-4　サーバの設置場所について

サービスを提供しているサーバは、クラウドサービスの国内リージョンにて運用しています。

2-11-5　社内 LAN の接続ついて

第三者の社内 LAN への接続は原則禁止しており、機器のメンテナンス等で必要な場合のみ社員の監視の下で行っております。

2-11-6　重要なデータの通信について

データ送信時の漏洩を防止するため、重要なデータを取り扱うものは必ず SSL 通信の暗号化を用いており、サーバへのログインも厳重に制限しております。

2-12 監査体制

2-12-1　内部監査について

情報セキュリティ委員会内の内部監査委員会が、規程に基づき内部監査を行い、その結果をフィードバックし、セキュリティ体制のさらなる強化を行います。

2-12-2　第三者機関による審査について

年に一度、外部の認証機関に ISO27001 の審査をうけております。認証登録証をお客様に開示することが可能です。

2-12-3　システム、機器の保守点検について

サービスを円滑に運用するため、保守点検を定期的に実施し、点検内容および結果を情報セキュリティ委員会でフィードバックし、改善に努めております。

2-12-4　品質について

サービスの信頼性、安全性、効率性を確認するため、運用、開発、変更等に対して専任の品質管理担当者による監査体制を整備しております。

2-12-5　第三者組織による脆弱性診断

毎日深夜にネットワーク・サーバ・デバイス・アプリケーションを対象に脆弱性診断を受けています。

また、年に一度第三者組織によるペネトレーションテストを実施しています。

2-13 バックアップ

2-13-1 バックアップについて

データベースは、１日１回バックアップを取得しています。サーバの設定やソースコードは、１日１回バックアップを取得し、またバージョン管理システムにより世代管理を行っています。

2-13-2 保管について

データベースのバックアップは 30 日間分保管しています。サーバの設定やソースコードは、1 日 1 回専用バックアップサーバに保存されます。バックアップは障害時の復旧用のため１世代分しか保管しませんが、バージョン管理システムにより世代管理しています。

2-14 アプリケーションの堅牢性

2-14-1 入力ミスについて

入力ミス、入力漏れを防止するための施策として、各種登録項目において入力必須設定やエラー設定しており、ユーザ側でも確認画面等で入力情報の再確認ができるようにしております。また、入力データの修正、削除、キャンセル機能を設けております。

2-14-2 論理チェックについて

ユーザ側、管理者側の両方において仕様書および設計書の作成を行い、それに基づいたテストを十分に行っております。

2-14-3 大量データ処理について

大量データに対する検索処理を行う際は、一覧の表示件数の制限等をかけております。また大量の一斉メール配信時もサーバ側に時間差で処理する制限をかけております。

2-15 アプリケーションの修正

2-15-1 影響範囲の調査について

既存アプリケーションの機能追加やバグフィックス等を行う際に、どの部分にどのような影響があるかの調査は技術統括役員に承認を得てからプロダクト担当チームが調査分析するプロセスとなっております。

2-15-2 修正する際のテストについて

本番に修正を反映させる前に、プロダクト担当のテストチームがテストケースを作成し、デモシステム上でテストケースに基づいて入念にテスト作業を行っております。品質管理担当者が確認のうえ、本番にリリースされます。

2-15-3 セキュリティの脆弱性対応について

利用中の情報システムの技術的脆弱性を管理するために、情報セキュリティ管理者が信頼できる団体等から常時最新情報を取得しています。セキュリティの脆弱性が発見された場合は、緊急度によって 3 段階で判断し、レベル高の場合は 5 営業日以内、レベル中の場合は 1 ヶ月以内、レベル低の場合は 3 ヶ月以内に対応致します。規程期間内に完了できない規模の大きな修正に関しましては、弊社セキュリティ委員会の管理の下、最優先で修正作業を実施致します。

3 お客様へのお願い

弊社では、WEB アプリケーション設計・開発・運用において、情報セキュリティ保護を目的として、お客様に対しても以下のような対応をお願いしております。

・弊社との間で重要な情報を含むデータをお客様とやりとりする必要性が発生した際には、SSL 通信対応済のファイル共有システムにより行っています(※)。

※特に、個人情報等の重要な情報はメールで送受信しないようにお願いしております。

4　変更履歴

項番	版	改定年月日	改定理由	改定内容	改定ページ	作成	審査	承認
1	第 1 版	2009 年 4 月 1 日	新規作成	新規作成	全項目	柳澤	永島	中村
2	第 2 版	2009 年 8 月 1 日	規程変更に伴う改訂	ウイルス対策の内容を変更	7	柳澤	永島	中村
3	第 3 版	2009 年 12 月 1 日	規程変更に伴う改訂	バックアップの内容を変更	13	柳澤	永島	中村
4	第 4 版	2010 年 6 月 1 日	規程変更に伴う改訂	脆弱性対応の内容を変更	14	柳澤	永島	中村
5	第 5 版	2011 年 7 月 27 日	規程変更に伴う改訂	規程内容を変更	7,8,12,13,14	柳澤	永島	中村
6	第6版	2014 年 3 月 27 日	規程変更に伴う改訂	登録範囲、認定機関名、審査登録機関名、ロゴの変更	6	柳澤	永島	中村
7	第7版	2015 年 3 月 20 日	規程変更に伴う改訂	全面改訂	全項目	桑江	永島	中村
8	第 7.1 版	2018 年 10 月 23 日	バックアップ手段変更に伴う改定	バックアップの内容を一部修正	12	石井	堀	永島
9	第 7.2 版	2018 年 11 月 1 日	運用変更に伴う改定	復旧手順、ログ種類数の変更など	1,11,12,13,14	石井	堀	永島
10	第 7.3 版	2019 年 5 月 31 日	運用変更に伴う改訂	アクセス権限についてなど	2-11	堀	堀	永島
11	第 7.4 版	2022 年 12 月 23 日	本番サーバの運用ルール変更に伴う改訂	本番サーバのパスワード設定とバックアップ方法について	2-11	石井	堀	永島
12	第 7.5 版	2023 年 8 月 21 日	ISMS 認証登録範囲の変更	認証登録範囲の変更	1-2	石井	堀	永島