GMO グローバルサインのセキュリティ対策について

GlobalSign by GMO

GMO グローバルサイン（以下「弊社」）は、弊社サービスおよびお客様のデータの安全を最優先事項としています。本書をもって、弊社環境にて機密性、完全性、および可用性を確保するために実施されているセキュリティ対策の概要を説明します。

情報セキュリティに対するグローバルサインの取り組み

弊社は、最も歴史ある業界最大手として数えられるパブリック認証局（以下「パブリック CA」）であり、安全性の高い公開鍵暗号基盤（以下「PKI」）ソリューションを長年にわたり提供しています。情報セキュリティは取締役会における重要な議題であり、弊社サービスの機密性、完全性、および可用性を確保すべくセキュリティポリシーを策定・施行するにあたっては、経営陣が深く関与しています。

弊社においては、セキュリティおよびコンプライアンス専任チームが、グローバル体制にて情報セキュリティマネジメントシステムを運用しています。このシステムは ISO 27001 の規格および、パブリック CA 運用の国際的フレームワークである「WebTrust Principles and Criteria for Certification Authorities」に基づいています。弊社は管理体制の中に、以下をはじめとする情報セキュリティ対策の主要分野を全て組み込んでいます：

- 情報セキュリティのガバナンスおよび戦略
- 脅威に対する分析、リスク評価、およびリスク管理の継続
- 従業員の情報セキュリティ認識および信頼性
- 物理環境面のセキュリティ
- セキュリティの運用および監視
- アクセス管理
- システム開発および保守
- インシデント管理および情報漏洩時の対応
- 事業継続および災害復旧

弊社は事業に不可欠なセキュリティポリシーを定義し全社に浸透させるとともに、弊社の PKI サービスを保護すべく、以下をはじめとした手続的かつ技術的なセキュリティ管理を導入しています：

- 弊社の全アプリケーションおよびシステムにおける多要素認証
- 強固なフィルタリングを備えた多層ネットワーク
- 高度なマルウェア検知
- ルート CA 鍵等の重要な鍵データのエアギャップ
- 弊社データセンターにおける軍事用レベルの物理的アクセス制限
- 弊社オフィスおよびデータセンターの両ネットワークにおける侵入検知（IDS）および侵入防止システム（IPS）
- 弊社 IT 機器のフルディスク暗号化
- 定期的な脆弱性診断（四半期ごと）および侵入テスト（年次）の実施
- 重要なアプリケーションのソースコードへのレビュー
- 迅速なパッチ管理

弊社環境において最高のセキュリティ水準を追求すると同時に、弊社は長年にわたり、CA/B Forum や CASC（Certificate Authority Security Council ）、IIC（Industrial Internet Consortium ）といった、極めて重要な規格を主導する団体・組織の一員として役割を担っています。また、北米エネルギー規格委員会（NAESB）、アメリカ国立標準技術研究所（NIST）、および NCCoE に準拠しています。

従業員の情報セキュリティ認識および信頼性

急速に拡大する情報セキュリティの脅威に際し、弊社による従業員への情報共有、説明、訓練の拡充は必須です。データのプライバシーや情報セキュリティへの脅威に対し確固とした認識を持つには継続的な努力が必要ですが、弊社は従業員への専門的なトレーニングだけでなく、その他様々な全社向けの認識促進を行っています。例えば、警戒心の維持を目的とし、フィッシングのテストや、その他のソーシャルエンジニアリング攻撃のシミュレーションを、従業員を対象に定期的に行っています。

また、弊社は組織内にて重要な役割を果たしている従業員の信頼性を審査しています。この審査においては、（従業員が所属する地域にて法的に許可されている場合、）技能、学歴、前職、経歴推薦状、犯罪歴などを確認します。

事業継続および災害復旧

弊社環境は回復力を備えて設計されており、主要な災害や、組織的または計画的なサービス妨害、また設備やサービスの損失への耐性があります。弊社の事業継続マネジメントおよび災害復旧の方法論は ISO 22301 の規格に基づいており、以下を取り入れています：

- 事業への影響を定量化し、適切な事業継続戦略を決定するための事業影響度分析
- お客様が希望される重要業績評価指標（KPI）に沿った、サービスの目標復旧時間(以下「RTO」)および目標復旧時点(以下「RPO」)の設定
- お客様やその他依拠当事者への緊急連絡および通知手順
- 事業所内外における情報の継続的なバックアップ
- 事業継続戦略および事業継続計画に対する年次の再評価
- RTO および RPO の実現性を保証するための、事業継続計画および復旧手順の定期的な試験
- 鍵の危殆化などCA特有の災害に特化した復旧プロセス・計画

高可用性を確保するために、弊社は世界中にデータセンターを展開しています。仮にこのうちの一つに自然災害や人為的な事故が発生したとしても、規定の RTO および RPO の範囲内に、別所へ障害迂回がなされます。さらに、これらのデータセンターおよび電子証明書を発行する施設には、複数の検知システム、複数回線、そして 24 時間 365 日の監視といった、標準的な予防的防護措置が講じられています。つまり、こうした事態の発生時または発生前に、最適な対応を行えるよう、最も早期の段階に警告を受ける仕組が用意されています。

データプライバシー

弊社はお客様のプライバシー権を尊重しています。弊社はプライバシーポリシーを EU 一般データ保護規則（GDPR）に沿って策定し、弊社の全ネットワーク、ならびに弊社の全製品およびサービスの提供にあたり収集した全情報に対し適用しています：

- 弊社は適切な物理、技術および組織的なセキュリティ対策のもと、個人情報を保護しています。
- 弊社はお客様が個人情報を提供される前に必ず明確な同意を求めます。
- 弊社はお客様が提供されない限り個人情報を収集しません。

- 弊社はお客様が提供された情報を弊社プライバシーポリシーによって定義された目的でのみ使用します。
- 弊社は使用後の個人情報を安全に消去します。
- お客様は、弊社が所有する個人情報を確認し、その整合性を照合する権利を保有します。
- お客様は、弊社の記録に万が一誤りがあった場合、情報を修正する権利を保有します。

コンプライアンスおよび監査

弊社は外部要求への準拠を評価および立証するために、下記をはじめとした複数の内部・外部監査を実施しています：

- 以下に記載する CA 向けの業界最先端のフレームワークに照らした、独立した外部監査人による年次の ISAE3000 SOC3 Type II 監査において、2001 年より毎年認証されています。— この年数は業界内第二位を誇ります。：WebTrust for Certification Authorities, Extended Validation, SSL Baseline Requirements, Code Signing and EV Code Signing
- ヨーロッパの適格トラストサービスプロバイダ向けの eIDAS 規則および ETSI の規格に基づいた、隔年の eIDAS 準拠評価
- ネットワークのフィルタリング、構成管理、パッチ管理、アプリケーションのセキュリティ、およびインフラストラクチャのセキュリティに重点を置いた脆弱性スキャン
- コンプライアンスおよびセキュリティ管理が効果的にデザイン・実施されていることを保証するために行う、これらの有効性に対する継続的な監視
- 独立した外部監査人より、ISO 27001（情報セキュリティマネジメントシステム）および ISO 22301（事業継続マネジメントシステム）の監査を年次にて受けています。弊社はこれら両認証を取得した初の国際的 CA です。

これらの評価報告書は、下記リンクに公開されています：
https://jp.globalsign.com/repository/

グローバルサインについて

グローバルサインは、信頼のおけるアイデンティティとセキュリティソリューションを提供するリーディングカンパニーです。世界中のビジネス、大企業、クラウドサービスプロバイダ、IoT のイノベーターに対し、安全なオンラインコミュニケーション、数百万を超えるデジタルアイデンティティの検証管理、認証・暗号化の自動化を実現し貢献しています。こうした多岐にわたる公開鍵暗号基盤（PKI）とアイデンティティソリューションの展開により、幾多のサービス、デバイス、人、モノを支え、IoE（Internet of Everything）を促進していきます。

GMO グローバルサイン株式会社
〒150-0043 東京都渋谷区道玄坂 1-2-3　渋谷フクラス
TEL : 03-6370-6500　https://jp.globalsign.com