gBizConnect セキュリティ管理方針

1 基本原則

1.1 「政府機関等の情報セキュリティ対策のための統一基準(平成 30 年度版)」※1に基づき、政府機関等において求められる情報セキュリティ対策の基準に準拠すること

1.2 国際標準・国内規格の考え方も参考に、情報セキュリティ及びプライバシー保護対策を徹底すること（例：JISQ15001 個人情報保護マネジメントシステム（要求事項）、ISO/IEC29100（JIS X 9250）プライバシーフレームワーク）

2 遵守基準

2.1 サイバーセキュリティ戦略本部のとりまとめる「政府機関等の情報セキュリティ対策のための統一基準」に準拠すること、また、本統一基準が改正された場合は、改正後の規定等を準拠すること

2.2 クラウドサービスを利用する場合、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されているサービスを利用すること

2.3 情報処理推進機構の「TLS 暗号設定ガイドライン」※2に準拠すること

3 情報セキュリティマネジメントの確立

3.1 組織は情報セキュリティを確保、維持するために、「政府機関等の情報セキュリティ対策のための統一基準」に従い、導入・計画、運用、点検、見直しというサイクルを確立していること

4 情報資産の管理

4.1 情報を利用等する全ての者が情報の取扱いについて認識を合わせるため、「政府機関等の情報セキュリティ対策のための統一基準」に従い、情報の取扱いに係る規定を整備し、明示等していること

4.2 情報セキュリティを確保するため、「政府機関等の情報セキュリティ対策のための統一基準」に従い、情報の作成、入手、利用、保存、提供、運搬、送信、消去等、適切に情報を取り扱うこと

4.3 サーバ装置、端末等が、不特定多数の者により物理的に接触できる設置環境にある場合は、情報漏洩等の恐れがあることから、情報の安全を確保するため、「政府機関等の情報セキュリティ対策のための統一基準」に従い、情報を取り扱う区域を定め、区域ごとの対策の決定等、管理しておくこと

4.4 クラウドサービスで提供される情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることによるカントリーリスクが存在するため、クラウドサービスなど活用する場合や、委託を行う場合に相手方事業者との間で、裁判管轄と準拠法を合意しておくこと

4.5 秘密鍵、サーバ証明書、ルート証明書、設定ファイル等は、情報セキュリティを確保するための重要な情報資産であるため、安全管理を徹底すること

5 技術的情報セキュリティ

5.1 コンピューターウイルスや不正アクセス等から情報資産を保護するため、「政府機関等の情報セキュリティ対策のための統一基準」に従い、ファイアーウォールやセキュリティ対策ソフトを導入する等、技術的な情報セキュリティ対策を講じること

※1「政府機関等の情報セキュリティ対策のための統一基準(平成 30 年度版)」(https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf)

※2「TLS 暗号設定ガイドライン」(https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3001-3.0.1.pdf)

5.2　高い安全性を確保するため、「TLS 暗号設定ガイドライン」の「高セキュリティ型」の設定を行うこと
5.3　セキュアな通信でデータの連携を行うため、秘密鍵、サーバ証明書、ルート証明書、設定ファイル等について、適切に管理、設定を行うこと

6　物理的及び環境的情報セキュリティ

6.1　自然災害、悪意のある攻撃又は事故等、外部及び環境の脅威からの損傷を回避するため、物理的な保護を設計し、適用すること
6.2　物理的な不正アクセスによる妨害、損傷等の脅威を防止するため、情報及び情報処理施設への入退室管理、情報を扱う区域の管理、定期的な検査を行うこと
6.3　データセンターにおける災害対策や侵入対策等、情報セキュリティ対策がされているか確認すること
6.4　情報を取り扱う機器等のソフトウェア、ハードウェア等の最新情報を入手し適用判断を行って、対応すること。

7　運用の情報セキュリティ

7.1　情報処理設備の正確かつ情報セキュリティを保った運用を確実にするため、操作手順書・管理策の策定、実施すること
7.2　情報及び情報処理施設がマルウェア等から保護されることを確実にするため、マルウェア等からの保護のための検出、予防、回復の管理策の策定し、実施すること
7.3　技術的脆弱性の悪用を防止するため、利用中の情報システムの技術的脆弱性に関する情報は、時機を失せずに獲得し、また、そのような脆弱性に組織がさらされている状況を評価し、それらと関連するリスクに対処するための適切な手段を講じること
7.4　情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うため、必要なログを取得し、保持し、定期的に点検又は分析を実施すること
7.5　情報セキュリティインシデントに対する迅速、効果的な対応のため、責任体制の整備、対処手順の明確化を行うこと
7.6　情報セキュリティインシデント発生時は、被害の拡大を防ぐため、速やかに対応（復旧・改善）、再発防止策の検討及び gBizConnect 運営事務局へ報告を行うこと

8　委託先との関係

8.1　委託先との間で、委託する業務の範囲や委託先の責任範囲等を明確化し、関連する全ての情報セキュリティ要求事項を確立させ、情報セキュリティ対策の詳細について合意し、定期的に監視すること
8.2　クラウドサービスを利用する場合、適正な取扱いが行われていることを直接確認することが一般に容易ではない、また、自身を含む他の利用者にも関係する情報の開示を受けることが困難である等のクラウドサービスの特性を理解し、委託先へのガバナンスの有効性や利用の際の情報セキュリティ確保のために必要な事項を考慮し、サービスの利用における対策を講じること

9　事業継続マネジメント

9.1　組織の情報セキュリティ及び情報セキュリティマネジメントの継続のため、「政府機関等の情報セキュリティ対策のための統一基準」に従い、情報システムの運用継続計画の整備・整合的運用の確保を行うこと

以　上