

ICS 35.030

CCS L 80



中華人民共和國標準規格

gb/t xxxxx-xxxx

データセキュリティ技術

政府業務におけるデータ処理のセキュリティ要件

データセキュリティ技術-政府データ処理のセキュリティ要件

(国際標準との整合性の度合いを示すマーカを追加するには、ここをクリックする)。

(公開草案)

(この草案の完成：2024年4月8日)

フィードバックを提出する際には、あなたが知っている関連特許があれば、裏付け資料とともに添付してほしい。

XXXX - XX - XX リリース

XXXX - XX - XX インプリメンテーション

国家市場監督管理总局
国家标准化管理委员会 发布

目次

前書き	2
1. 適用範囲	3
2. 参考文献	3
3. 用語と定義.....	3
4. 略語	4
5. 政府データ処理におけるセキュリティ要件の枠組み.....	4
6. 政府のデータ処理セキュリティ管理要件	5
6.1 政府のデータ処理におけるセキュリティの組織的要件.....	5
6.2 管理データの処理に関するセキュリティ体制の要件	6
6.3 管理データ処理のための第三者サービスに対するセキュリティ要件	7
7. 政府データ処理セキュリティの技術要件	8
7.1 データ収集	8
7.2 データ保管	8
7.3 データの使用と処理.....	9
7.4 データ送信	10
7.5 データの可用性	10
7.6 データ開示	11
7.7 データ破棄	12
8. 政府データにおける個人情報の取り扱いに関する保護要件	12
8.1 行政データにおける個人情報主体の権利保護	12
8.2 行政情報処理施設における個人情報のセキュリティ保護	12
9. 政府データ処理のセキュリティ運用要件	13
10. 政府のデータ処理セキュリティ監督要件	13
附属書 A (参考) 政府データ処理のセキュリティ評価方法と評価指標.....	15
A.1 行政データ処理のセキュリティ評価方法.....	15
A.2 政府業務におけるデータ処理のセキュリティ性を評価するための指標	16
参考文献	25

前書き

この文書は、GB/T 1.1-2020 Guidelines for Standardisation Work Part 1: Structure and Drafting Rules for Standardisation Documents の規定に基づいて作成されている。

本文書の他の要素が特許でカバーされている可能性があり、本文書の発行組織はそのような特許を特定する責任を負わないことに留意されたい。

本文書は、ネットワークセキュリティ標準化国内技術委員会（SAC/TC 260）により提案され、その支援を受けている。

本書の起草単位：国家情報センター、中国電子技術標準化研究院、貴州省情報センター、北京市ビッグデータセンター、中国科学院情報工学研究所、江西省情報センター、安徽省情報センター、広東省政府サービスデータ管理局、浙江省ビッグデータ発展管理局、無錫市ビッグデータ管理局、浙江省、浙江省発展測定有限公司 Ltd.

この文書の主な起草者：徐春雪、任飛、羅海寧、焦迪、宋博涛、余静、羅華陽、趙英、王軍、程魯耀、朱旬、程紫東、田子潘、王鵬彪、徐玉嘉。

データセキュリティ技術 政府業務におけるデータ処理のセキュリティ要件

1. 適用範囲

本書は、政府データ処理に対するセキュリティ要求事項を規定し、政府データ処理のセキュリティ管理に対する要求事項、政府データ処理のセキュリティ技術に対する要求事項、政府データ処理における個人情報保護に対する要求事項、政府データ処理のセキュリティ運用に対する要求事項、政府データ処理のセキュリティ監督に対する要求事項を規定している。

本書は、政府部門およびその技術支援部門が政府のデータ処理活動を規制する際の手引きとなるほか、監督当局および第三者機関が監督・管理・アセスメントを実施する際の参考資料となる。

2. 参考文献

以下の文書の内容は、本文中の規範的参照を通じて、本文書の必須規定を構成する。日付のある参考文献の場合、その日付に対応するバージョンのみがこの文書に適用される。日付のない参考文献の場合、最新バージョン（すべての変更指示を含む）がこの文書に適用される。

GB/T 22239-2019 情報セキュリティ技術 ネットワークセキュリティ等級保護の基本要素事項

GB/T 25069-2022 情報セキュリティ技術用語集

GB/T 35273-2020 情報セキュリティ技術 個人情報セキュリティ仕様

GB/T 37964-2019 個人情報の非識別化に関する情報セキュリティ技術ガイドライン

GB/T 38664.1-2020 情報技術ビッグデータ管理データの開発と共有 第1部：一般規定

GB/T 39477-2020 政府情報共有のための情報セキュリティ技術データセキュリティ技術要件

GB/T 39786-2021 情報セキュリティ技術 情報システム用暗号アプリケーションの基本要件

3. 用語と定義

GB/T 25069-2022、GB/T 38664.1-2020、および以下の用語と定義が本書に適用される。

3.1

政府データ

あらゆるレベルの政府部門およびその技術支援部門が、法律に従って職務を遂行する過程で収集、生成、保管、管理する各種データ資源。

[出典：GB/T 38664.1-2020、定義 3.1、修正]。

3.2

政府データ処理

政府データの収集、保管、使用、処理、送信、提供、開示、破棄。

3.3

政府データ処理業者

政府データの収集、保存、使用、処理、送信、提供、開示、破棄などの活動を行う個人または組織。

4. 略語

本書では以下の略語を使用する。

SFTP : Secured File Transfer Protocol (SFTP)。

5. 政府データ処理におけるセキュリティ要件の枠組み

政府データ処理セキュリティ要求事項の枠組みは、図 1 に示すように、政府データ処理セキュリティ管理要求事項、政府データ処理セキュリティ技術要求事項、政府データ処理における個人情報保護要求事項、政府データ処理セキュリティ運用要求事項、政府データ処理セキュリティ監督要求事項の 5 つの部分から構成されている。



図 1 行政データ処理に関するセキュリティ要件の枠組み

政府データ処理のセキュリティ管理に関しては、組織、システム、第三者サービスの 3 つの側面からセキュリティ管理要件が提示されている。政務データ処理のセキュリティ技術の分野では、データの収集、保存、使用、処理、送信、提供、開示、破棄などの政務データ処理活動に対するセキュリティ技術要件が提示されている。政務データにおける個人情報の保護に関しては、個人情報主体の権利保護と個人情報セキュ

リティ保護の観点から、対応するセキュリティ要求事項が提示されている。政務データ処理のセキュリティな運用に関しては、データセキュリティ遵守評価と監視、政務データ処理のセキュリティ評価、早期警告通知、緊急対応、トレーサビリティ分析、監査管理などのセキュリティ要求事項が提示されている。政務データ処理セキュリティ監督分野では、コンプライアンス検査、インシデント報告、苦情報告などのセキュリティ要求事項が規定されている。

6. 政府のデータ処理セキュリティ管理要件

6.1 政府のデータ処理におけるセキュリティの組織的要件

6.1.1 全般

政府データ処理活動の組織には、意思決定レベル、管理レベル、執行レベルおよび監督レベルを含めるべきである。意思決定レベルの主な責任は、政府データ処理のセキュリティに関するガイドラインと政策を策定し、セキュリティ資源を提供することであり、管理レベルの主な責任は、意思決定レベルが策定した関連政策を実施し、政府データ処理に関する管理規範と制度を策定し、データセキュリティの管理を組織し推進することであり、執行レベルの主な責任は、意思決定レベルと管理レベルが策定した政策、規範、制度を実施し、政府データ処理のセキュリティを確保することである；監督層の主な責任は、意思決定層および管理層が策定した関連政策、規範および制度に従って、行政層が政府データ処理に関する政策、規範および制度を実施することを監督し、関連制度および規範を実施しない政府データ処理業者に対してセキュリティ管理措置を講じることである。

6.1.2 意思決定レベル

意思決定レベルは、政府データ処理者の組織のデータセキュリティリーダーシップチームのメンバーで構成され、具体的な責任は以下の通りである：

- a) 政府のデータ処理に関する全体的なセキュリティ目標とセキュリティ開発計画を策定する；
- b) 政府のデータ処理に関するセキュリティ管理システムと規範を公表する；
- c) 政府データ処理のセキュリティ計画、設計、構築、実施、運用の全プロセスにリソースを提供する；
- d) 政府のデータ処理で発生した重大なデータセキュリティ・インシデントに対する調整と意思決定を実施する；
- e) 国または地域のデータセキュリティ関連の監督・管理当局と連絡・調整する。

6.1.3 マネジメント

管理者は、政府データ処理者の事業部門の管理者及びデータセキュリティ管理部門の専任スタッフで構成され、具体的な責務は以下の通りである：

- a) 業務部門のデータセキュリティ管理体制と仕様を策定し、政府のデータ処理に関する権利と責任を明確にする。

- b) 事業部門のデータセキュリティ・プログラムを策定し、その実施を組織する；
- c) 政府のデータセキュリティの意思決定レベルでの決定を調整し、実施する；
- d) 事業部門を対象に、政府のデータセキュリティに関するビジネス・訓練や技術訓練を実施する；
- e) ネットワーク・セキュリティ・等級保護と情報システム・パスワード・アプリケーション・セキュリティの開発を主導する。

6.1.4 エグゼクティブ層

エグゼクティブ・レベルは政府のデータ処理担当者で構成され、具体的な責任は以下の通りである：

- a) 政府データセキュリティ・プログラムの実施；
- b) 政府のデータセキュリティ・システムと規範を導入する；
- c) 政府データセキュリティの運用と保守・運用；
- d) 政府のデータ資源を管理する；
- e) 政府のデータセキュリティ・リスクを監視する；
- f) 政府のデータセキュリティ・リスクアセスメント；
- g) 政府のデータセキュリティの脆弱性を監視し、修復する；
- h) 政府のデータセキュリティ・インシデントの処理とトレーサビリティ分析。

6.1.5 監督層

監督層は、政府データ処理者部門のセキュリティ監督者と監査員で構成され、具体的な責任には以下が含まれる：

- a) 政府のデータ処理に関するデータセキュリティ・システムおよび規範の実施を監督する；
- b) 政府データ処理中のセキュリティ・インシデントの処理プロセスおよび結果を監督する；
- c) 政府データの処理におけるセキュリティ・リスク管理措置の監視および監査；
- d) 政府のデータ処理におけるセキュリティ監視の結果を、意思決定者にタイムリーに報告する；
- e) ネットワーク・セキュリティ・等級保護と情報システム・パスワード・アプリケーション・セキュリティの実施を監督する。

6.2 管理データの処理に関するセキュリティ体制の要件

この要件には以下が含まれる：

- a) 政府のデータ処理に関する組織的保証メカニズムを確立すべきである；
- b) 政府のデータ処理に関するセキュリティ管理システムを開発すべきである；

- c) 政府機関のデータ処理に関するデータセキュリティの責任者を明確に定め、国のインターネット情報部門が指定した量までの個人情報を取り扱う個人情報保護の責任者を指定し、責任者の氏名と連絡先を関係主管機関に報告する；
- d) 政府データの区分とレベルを明確にし、個人情報と重要データを識別するために、政府データの区分と等級に関する仕様を策定すべきである；
- e) 政府のデータ処理に関するデータセキュリティ管理仕様を策定し、データの分類と等級付けに基づくセキュリティ管理措置、データ・アクセスの権限付与と承認の仕組みを規定すべきである；
- f) 政府データ処理における個人情報のセキュリティ管理に関する規定を策定し、個人情報および機微（センシティブ）個人情報のセキュリティ管理措置を明確化する；
- g) 政府データ処理に関するセキュリティ運用・保守仕様を策定し、データセキュリティリスク監視、データセキュリティ緊急対応、データセキュリティ・リスク評価、データセキュリティ監査、データバックアップ・復旧など、対応措置の要件を規定する；
- h) 関連する政府データセキュリティ管理規範は、政府データ分類規範、政府データ処理における個人情報セキュリティ管理規範、政府データ処理におけるセキュリティ運用・維持規範など、定期的に見直し、更新されなければならない；
- i) 政府のデータ処理のセキュリティに関する教育・訓練を組織し、全職員を対象にデータセキュリティに関する教育・訓練を毎年実施すべきである。また、教育・訓練計画は、訓練のフィードバック効果に基づいて定期的に見直し、更新すべきである；
- j) データセキュリティ・インシデント報告やデータセキュリティ・リスク評価報告などのシステム要件を明記した、政府データ処理に関するセキュリティ報告システムを策定すべきである；
- k) 政務データを扱う情報システムについては、ネットワークセキュリティ等級保護に関する基本要件に従い、GB/T に従って保護を実施する必要がある。
22239-2019 レベル要件に対応する；
- l) 政府データを扱う情報システムについては、パスワード適用に関するセキュリティ管理システムを策定し、GB/T 39786-2021 の対応するレベルの要求に従うべきである。

6.3 管理データ処理のための第三者サービスに対するセキュリティ要件

この要件には以下が含まれる：

- a) 政府データ処理施設の建設・維持および政府データ処理を他人に委任する場合、委任当事者は厳格な承認プロセスを経て委任者を選定し、委任者が政府データ処理に関するセキュリティ要件を履行するよう監督するものとする；
- b) 委託を受けた当事者は、法令および契約合意の規定に従い、政府データを保持、使用または他者に提供しなければならない、政府データ資源に許可なくアクセス、修正、開示、利用、移転または破棄してはならない；

- c) 受託当事者は、データ処理のセキュリティを保護するためにデータ処理組織を設立し、受託当事者は組織的保護監督層に関する責任を引き受けるものとする；
- d) 受託当事者は、要員セキュリティ管理システムを確立し、募集、採用、訓練、評価、選抜、入社、異動、退社における要員セキュリティ管理の運用手順を規定し、必要な身元調査を実施し、政府データの処理に関与する要員の秘密保持契約を締結するものとし、受託当事者は、受託当事者の要員のセキュリティレビューを定期的実施するものとする；
- e) 受託者は、データセキュリティ評価報告書及びレビュー報告書について、校長に定期的にフィードバックを行い、校長のコメントに基づいて最適化及び改善を行う。

7. 政府データ処理セキュリティの技術要件

7.1 データ収集

この要件には以下が含まれる：

- a) データ収集施設は、データ分類・等級付け機能を有し、政府データ分類・等級付け仕様に 従って、収集した政府データのデータ分類・等級付けを行うべきである；
- b) データ収集施設は、データを暗号化して保存し、収集されキャッシュされたデータを暗号化して保存し、キャッシュされたデータをパーズできる能力を持つべきである；
- c) 収集されたデータが他の業務システムに送信される場合、データ収集のコンプライアンス要件と送信のセキュリティ要件を満たすために、認証されなければならない；
- d) データ収集施設は、収集データのデータソースを特定し、データソースの真正性要件を満たすべきである；
- e) データ収集施設は、収集されたデータの完全性要件を満たすために、データ検証機能を持つべきである；
- f) データ収集施設は、データ収集プロセスの監査可能性および追跡可能性を満たすために、データ収集プロセスを記録する能力を有するべきである；
- g) データ収集施設は、過剰なスケールや過剰なスコープのデータ収集行動を警告し、必要最小限のデータ収集という原則を満たす機能を持つべきである；
- h) データ収集の範囲、プロセス、頻度、チャネル、モードは、データ収集業務のコンプライアンス、正当性、一貫性の要件を満たすために、定期的なアセスメントされるべきである；
- i) データを収集する前に、政府データ処理者はネットワークサービスのパフォーマンスをアセスメントし、ネットワークサービスへの影響が最も少ない許容可能な方法を選択すべきである。

7.2 データ保管

この要件には以下が含まれる：

- a) データ保管施設（データベース、クラウドストレージシステム、ビッグデータプラットフォームなどを含む）は、バックアップ機構を備え、バックアップデータなどの完全性と可用性を定期的に検証し、データ保管の適時性要件を満たすために、業務データ、バックアップデータ、ログデータなど、さまざまな種類のデータの保管期限を確認する必要がある；
- b) データ保管施設は、異なるプロセス/ツール/アプリケーションが法的に許可されたデータのみにアクセスできるという要件を満たすために、セキュリティ分離と権限管理手段を備えるべきである；
- c) データ保管施設は、本人確認、権限管理、ログ監査、データ暗号化などの手段を備えるべきである；
- d) 例えば、機微な個人情報や重要なデータは暗号化して保管する；
- e) 統一認証、アカウント権限の最小構成、データの非感覚化、操作ログの記録と監査など、データ保管施設の操作に関するセキュリティ管理メカニズムを確立すべきである；
- f) 重要データの機密保護は、暗号技術に基づいて提供されるべきである；
- g) 政府データの完全性保護は、暗号技術に基づいて提供されるべきである；
- h) 政府データの保管施設は、公共情報ネットワークから隔離されたセキュリティな場所に配置されるべきである；
- i) 政府業務データ保管施設のセキュリティ保管保護対策、データ保管媒体のセキュリティ管理戦略、管理規定など、政府業務データ保管のセキュリティ戦略と運用手順を明確に定めるべきである；
- j) 政府データは中華人民共和国内で保管されるべきであり、国外に出る必要がある場合は、国内法、行政法規および関連規定の要件を満たす必要がある。

7.3 データの使用と処理

7.3.1 システム・セキュリティ

この要件には以下が含まれる：

- a) データセキュリティ保護対策は、処理されるデータの種類と等級に応じて実施されなければならない；
- b) データ処理プロセスは、監査可能かつ追跡可能であることを保証するために記録されなければならない；
- c) データ利用・処理のプロセスは、処理の目的、処理方法、適用場面などを含めて明確化されるべきであり、データ利用・処理のプロセスは、データ処理の全プロセスの監査を実現するように文書化されるべきである。

7.3.2 データ・インターフェースのセキュリティ

この要件には以下が含まれる：

- a) データ・インターフェースによって送信されるデータのセキュリティ性を確保するために、暗号技術を使用すべきである；
- b) データ署名や多要素などの技術を使用して、きめ細かな認証とアクセス制御を行う；
- c) データ・インターフェースのセキュリティ管理は、データ・アプリケーション当事者の一意的な識別に基づくアプリケーション識別、状態検証、権限管理に基づいて実施されるべきである；
- d) データインターフェースのセキュリティ管理戦略は、識別、認可ポリシー、アクセス制御、デジタル署名、タイムスタンプ、セキュリティプロトコル、ホワイトリスティングシステムなど、データインターフェースの使用に関するセキュリティ制約とセキュリティ管理手段を規定するために確立されるべきである；
- e) 特殊なインターフェース・パラメーターの注入を防ぐために、データ・インターフェース・パラメーターのフィルタリングや制限などの対策を講じる必要がある；
- f) データインターフェースのコールログを分析し、アクセスユーザー、アクセス頻度、アクセス時間、アクセスデータ量などの次元からデータインターフェースのコール動作を分析し、アラートとブロックのメカニズムを通じて異常なイベントのリアルタイム通知とブロックを実行する；
- g) データインターフェースの資産管理、監視・監査メカニズムを確立し、データインターフェースを資産化し、データインターフェースを通じて交換されるデータのセキュリティ監視・監査を実施すべきである。

7.4 データ送信

この要件には以下が含まれる：

- a) データ送信プロセスの機密性要件を満たすために、セキュア・チャネル、データ暗号化、その他の手段を導入すべきである；
- b) データ送信タスクの信頼性を保証するために、ブレイクポイントで送信を継続し、タイムアウト後に再接続する機能を持つべきである；
- c) データ送信施設は、政府のデータ分類および等級別セキュリティ戦略に従い、機微な個人情報や重要データの暗号化送信など、適切なデータセキュリティ保護措置を実施すべきである；
- d) データ送信プロセスの監査可能かつ追跡可能な要件を満たすために、データ送信プロセスはログに記録されるべきである。

7.5 データの可用性

7.5.1 基本的なセキュリティ

この要件には以下が含まれる：

- a) データを提供する両当事者の身元が正当であることを保証するために、データ提供前に両当事者の身元を確認すべきである；
- b) データ提供施設は、提供されるデータの種類と等級に応じて、データ暗号化、データ非感覚化、電子透かしなど、適切なデータセキュリティ保護措置を実施すべきである；
- c) データ提供施設は、ID 識別、権限管理、ログ監査、データ暗号化、パッチアップグレードなどのセキュリティ保護機能を備えていなければならない；
- d) データ提供施設は、データ提供プロセスの監査可能かつ追跡可能な要件を満たすために、データ提供プロセスを記録すべきである。

7.5.2 データ共有

この要件には以下が含まれる：

- a) データ共有のセキュリティ技術対策は GB/T 39477-2020 の規定に従うべきである；
- b) ファイル共有プロトコルによるデータ共有では、SFTP などのセキュリティブロトコルを採用し、共有データの暗号化、共有前の双方の本人確認、共有プロセスのロギングなどのセキュリティ対策を講じる必要がある；
- c) データ共有施設等を通じてデータを共有する場合、データ共有施設は、管理者の権限管理、共有施設内のキャッシュデータのセキュリティ管理、共有施設内のログの監査、共有施設内のデータセキュリティのリスク管理など、合理的なセキュリティ対策を提供すべきである；
- d) リムーバブル・ハードディスクなどのオフライン・コピー・メディアによるデータ共有については、データ保存メディアのセキュリティ管理策の策定、共有データの暗号化、共有完了後の保存メディア内のデータ破棄、共有プロセスのログ記録などのセキュリティ対策を講じる必要がある；
- e) 第三者との個人契約またはカスタム開発ドッキングによるデータ共有の場合、共有データの暗号化、共有前の両当事者の識別、共有プロセスのロギングを含むセキュリティ対策を講じるべきである；
- f) 共有データの内容識別とセキュリティ管理は、データ分類・等級仕様とデータ分類・等級セキュリティポリシーに基づくべきである。

7.6 データ開示

この要件には以下が含まれる：

- a) データ開示のカatalogを制定し、データ開示の受け手を明確に特定すべきである；
- b) 重要なデータや機微な個人情報を特定し、適時に開示を回避するために、開示前に開示対象データの内容チェックを実施すべきである；
- c) データのトレーサビリティを確立するために技術的手段を用いるべきであり、トレーサビリティのあるデータの完全性を保護するためにチェックサムまたは暗号技術を用いるべきである；

- d) 政府データの開示を監督するメカニズムを確立し、開示されたデータの品質やセキュリティ管理業務などを監督すべきである。

7.7 データ破棄

この要件には以下が含まれる：

- a) 不可逆的なデータ削除メカニズムを確立し、必要なデータ削除ツールを設定し、ビジネスシナリオのニーズに応じて、関連データと、そこから派生したさまざまなデータのコピーを不可逆的な方法で削除できるようにすべきである；
- b) 物理的および論理的なデータ消去の方法と技術を確立し、カテゴリやレベルごとのデータ消去方法とセキュリティ要件を明確にすべきである；
- c) データ削除のセキュリティ運用規範を法律や規制の要求事項に従って確立し、重要データや個人情報の多段階カスケード削除運用モードを確立し、セキュリティなデータ削除の運用手順を明確にすべきである；
- d) メディアへのアクセス、使用、破棄のプロセスは記録・監査されるべきであり、破棄記録とメディア破棄の有効性は定期的にチェックされるべきである。

8. 政府データにおける個人情報の取り扱いに関する保護要件

8.1 行政データにおける個人情報主体の権利保護

この要件には以下が含まれる：

- a) 政府データの個人情報が第三者（企業や機関など）から収集される場合、第三者は個人情報主体の権利保護を実施しなければならない、政府データを処理する設備は、第三者の個人情報とのリアルタイム同期を確保しなければならない；
- b) 個人情報主体から収集された政府データにおける個人情報は、個人情報主体に対し、データ収集の目的、方法および範囲、個人情報処理者の名称、連絡先、個人情報の保持期間、個人が法的権利を行使するための方法および手続きについて、明確かつ理解しやすい言語で、合理的な経路を通じて通知し、個人情報主体の正式な同意を得なければならない；
- c) 政府情報処理施設は、個人情報を撤回するための仕組みを提供しなければならない、個人情報の主体が撤回に同意した場合、個人情報の処理行為を直ちに停止し、撤回を要求された個人情報を消去しなければならない。

8.2 行政情報処理施設における個人情報のセキュリティ保護

この要件には以下が含まれる：

- a) 個人情報および機微（センシティブ）個人情報を自動的に識別・保護し、関連措置を講じる。

gb/t 35273-2020；

- b) 収集される個人情報、政府データ処理施設に対応する政府業務に必要なものに限られ、政府業務に関与しない個人情報は収集されない；
- c) 個人情報の処理を伴う政府データの処理を他の部門に委託する場合は、委託する部門との間で、委託の目的、期間、処理方法、個人情報の種類、保護措置、委託者双方の権利義務を取り決め、委託者の個人情報処理活動を監督する。

9. 政府データ処理のセキュリティ運用要件

この要件には以下が含まれる：

- a) 政府データ処理者の法令遵守要件は、組織、人員、システムおよび技術に関してアセスメントされるべきであり、政府データ処理プロセスの継続的なコンプライアンスをチェックすべきである；
- b) 政府データ処理セキュリティ評価は、政府データ処理に関わる政府データ及び主要なデータ処理施設（例えば、データベースやビッグデータプラットフォームなどのデータ保管担体、データ業務アプリケーション、データ分析ツールなど）について定期的実施する必要があり、その評価方法及び評価指標は附属書 A を参照することができる；
- c) 政府データ処理に関連するデータセキュリティイベントやリスク情報は、データ異常やデータアクセス異常行動などの分析・監視に重点を置いて監視されるべきである。発見されたあらゆる種類のデータセキュリティイベントやリスクに対して早期警告通知を行い、インスタントメッセージや電子メールを通じて関係責任者に通知し、検証・処理を行うべきである；
- d) 発見されたあらゆるタイプのデータセキュリティ・インシデントに対して、攻撃の影響の分析、攻撃をブロックするためのセキュリティ・ポリシーの設定、攻撃によって悪用されたセキュリティ・ホールの修復などの緊急対応策を講じる；
- e) 発生したあらゆる種類のデータセキュリティ・インシデントについて、技術的なツールを用いてデータセキュリティのトレーサビリティ分析を行うべきである。トレーサビリティの目的には、最初の攻撃源の発見、政府データ処理施設への攻撃の完全な経路、トレーサビリティ分析およびその他の廃棄措置で発見されたセキュリティ・ホールや隠れた危険を適時に修復することなどが含まれるべきである；
- f) リスクが特定されたデータセキュリティログは、さらに分析・検証を行い、隠れたデータセキュリティ・リスクを特定し、適切な廃棄措置を講じる。

10. 政府のデータ処理セキュリティ監督要件

この要件には以下が含まれる：

- a) 政府データ処理者のデータ収集、保存、使用処理、送信、提供、共有、開示、破棄およびその他の政府データ処理活動を監督し、政府データ処理のセキュリティ性とコンプライアンスを保証するため、政府データのセキュリティ性とコンプライアンスについて定期的な検査を実施する；

- b) 重大な緊急保安事故が発生した場合、効果的な措置を講じて上級当局に報告し、保安事故の分析・判断と緊急対応を同時に実施する；
- c) 政府データセキュリティに関する苦情・報告ルート、受付・廃棄手続きを確立し、苦情・報告の方法に関する情報を公表し、政府データ処理に関するデータセキュリティおよび個人情報保護に関する苦情・報告を速やかに受け付ける。

附属書 A (参考) 政府データ処理のセキュリティ評価方法と評価指標

A.1 行政データ処理のセキュリティ評価方法

A.1.1 アセスメント目的の明確化

政府データ処理に関連する業務の発展およびデータセキュリティ関連法規の要求に従って、政府データ処理業務のセキュリティ保護の現状を整理し、政府データ処理業務の潜在的なデータセキュリティ・リスクを特定し、政府データ処理のセキュリティを向上させるための提案を行う。

A.1.2 アセスメント範囲の定義

政府データ処理のアセスメント目標に基づき、政府データ処理に関わるデータ・アプリケーション・プラットフォーム、データ管理プラットフォーム、その他の関連システム設備、および対応する内部・外部組織、試運転、運用、監督の責任者を特定する。

A.1.3 アセスメント手法の決定 アセスメント手法は、主に以下からなる：

- a) 担当者面談：関連する責任者、専門担当者、委託先などと面談を行い、システムや規則の実施状況、保護措置、セキュリティ責任などを把握する；
- b) 文書化検証：アセスメント実施者は、データセキュリティ関連の文書（データセキュリティポリシー、システム及び手順、訓練及び教育資料、並びに製品及び技術に関連する設計及び実施計画、構成記述、運用記録及びその他の裏付けとなる書式など）を提供し、アセスメントワーキンググループは、関連文書がデータライフサイクル全体のプロセス領域及び管理策をカバーしているかどうかを検証する；
- c) セキュリティ検証：アセスメントを受けた当事者から提供された技術資料に基づき、関連するシステム設備にログインし、そのセキュリティポリシー、設定および保護手段を検証する；
- d) 技術的テスト：テストツール、侵入テスト、その他の技術的手段を採用し、アセスメントシステムの権限管理ポリシー、脆弱性修復ポリシー、ID 認証管理ポリシー、権限付きアクセス制御ポリシー、その他の対策の完全性と有効性をテストする；
- e) サンプルングとテスト：アセスメント対象の一定割合をサンプルングしてアセスメントし、アセスメント結果に基づいてデータセキュリティ能力全体を判定する。この方法は、アセスメント対象物の数が膨大な場合に適用される。サンプルングは、サンプルング結果が代表的であることを保証するために、サンプルングの無作為性とサンプルング比率を考慮しなければならない。

A.1.4 アセスメントの実施

具体的な実施内容のアセスメントには、特に以下の項目が含まれる：

- a) 評価情報調査：評価作業部会は事前に政府データ処理評価調査を実施し、データ処理者の状況、データ資産の状況、データセキュリティ担当者の状況、データ委託の状況、データ利用システムの状況、データ処理活動の状況、セキュリティ保護措置の状況などを調査する；

- b) アセスメントの準備：アセスメント作業部会は、アセスメントの目的、アセスメントの範囲および調査に従って、アセスメントに必要な関連資料を準備する。この準備には、適用される基盤の選択、アセスメントの内容の決定、アセスメント計画の策定、アセスメントプログラムの作成、アセスメントを受ける当事者の承認および認可が含まれるが、これらに限定されない；
- c) アセスメント作業の実施：アセスメント作業部会は、被アセスメント当事者が承認したアセスメント計画に基づいてアセスメント作業を実施し、被アセスメント当事者の関連責任者、専任者、委託側の担当者を集めてアセスメントキックオフ会議を開催し、担当者面談、文書調査、セキュリティ検証などの方法を採用し、評価指標に基づいて、政府データおよび政府データ処理に関わる主要データ処理施設のセキュリティ・リスクを一つずつ検証し、セキュリティ検証を実施する。リスクを分析・評価し、得られた結果を正確に記録し、関連証拠を保存する；
- d) アセスメント報告書のアウトプット：アセスメント作業部会は、現地アセスメントで記録された結果及び関連証拠に基づき、政府データ処理に関するセキュリティ評価報告書を作成する。この報告書には、政府データ及び政府データ処理に関わる主要データ処理施設の現在のセキュリティ状況を反映する必要があり、既存のリスク問題に対応する改善勧告を提示する；
- e) アセスメント作業のまとめ：アセスメント作業部会は、被評価者の関係責任者、専門担当者、委託者の担当者を招集し、アセスメントのまとめ会議を開催する。この会議では、関係者の担当者が、アセスメントの結論が現状に沿っているか、アセスメントの結論が正確か、アセスメント報告書の記載内容に誤りがないかなどを共同で確認する。

A.2 政府業務におけるデータ処理のセキュリティ性を評価するための指標

政府データ処理セキュリティ評価指標は、セキュリティ管理要求事項、セキュリティ技術要求事項、個人情報保護要求事項、セキュリティ運用要求事項、セキュリティ監督要求事項の5つの部分からなる。

行政事務におけるデータ処理のセキュリティ評価の指標は、アセスメントの対象・範囲に応じ、該当する指標項目を選定し、該当しない指標項目については説明を行う。このうち、機微な個人情報及び重要なデータの処理活動に関する要件は、政務のデータ処理活動のハイリスク項目として設定されており、このような指標項目が不適合とアセスメントされた場合、政務のデータ処理のセキュリティ評価の結論は不合格に直結する。

政府のデータ処理セキュリティ評価指標と得点案を表1に示す：

表 A.1 政府事務におけるデータ処理のセキュリティ性を評価するための指標

第一指標	第二指標	第三指標	指標の説明	得点 提案	
セキュリティ管理 要求	セキュリティ組織要求	組織構造	政府のデータ処理に関する組織構造が明確化され、データセキュリティの全体的な計画と組織的調整に責任を負うデータセキュリティ主導グループが設置されているかどうか；	2	3
		職責	意思決定、管理、執行、監督の各レベルにおいて、責任者および専任スタッフがそれぞれ明確に特定され、それに対応する職務が策定されているかどうか；	1	
	セキュリティ制度要求	データセキュリティ管理システム	政府のデータ処理に関するデータセキュリティ管理システムが策定されているかどうか、またそれに対応する組織的な保護メカニズムが確立されているかどうか；	1	12
		データセキュリティ担当者	政府のデータ処理におけるデータセキュリティの責任者が任命されているかどうか、および責任者の氏名と連絡先が関係当局に報告されているかどうか； 個人情報の取り扱いが国家インターネット情報部門が定める量に達している場合、個人情報保護責任者が任命されているかどうか、および責任者の氏名と連絡先が関係機関に報告されているかどうか；	2	
		データ分類階層仕様	政府データの処理に関するデータ分類および等級規定が策定されており、政府データの分類およびレベルが規定され、個人情報、機微な個人情報、重要データが特定されているか；	1	
		データセキュリティ管理仕様	政府データ処理に関するデータセキュリティ管理仕様、データ分類・等級に基づく明確なセキュリティ管理措置、データ・アクセス権限付与・承認メカニズムを策定しているかどうか；	1	
		個人情報のセキュリティ管理に関する仕様	政府データ処理における個人情報のセキュリティ管理に関する規範を策定し、個人情報および機微（センシティブ）個人情報のセキュリティ管理措置を明確にしているかどうか；	1	
		データセキュリティ運用保守仕様	政府のデータ処理に関するセキュリティ運用・保守仕様が策定されているかどうか。データセキュリティ・リスクの監視、データセキュリティ緊急対応、データセキュリティ・リスク評価、データセキュリティ監査、データのバックアップとリカバリが規定されている；	1	
		機関規範の見直しと改訂	関連する政府のデータセキュリティ管理体制と規範が定期的に見直し・更新されているか、見直し・改訂・更新のための記録文書があるか；	1	
		データセキュリティ教育と訓練	政府データ処理のセキュリティに関する教育・訓練を定期的（毎年）に実施し、訓練の効果に基づき教育・訓練プログラムを定期的に見直し、更新するかどうか；	1	
政府データセキュリティ報告	データセキュリティインシデント報告やデータセキュリティ・リスク評価報告などのシステム要件を明記した、政府のデータ処理に関するセキュリティ報告システムが策定されているかどうか；	1			
等級保護セキュリティ管理	政務データを取り扱う情報システムは、ネットワークセキュリティ等級保護の基本要件に従って保護を実施し、GB/T 22239-2019 情報セキュリティ技術ネ	1			

第一指標	第二指標	第三指標	指標の説明	得点 提案	
			ネットワークセキュリティ等級保護の基本要件に対応するレベル要求に従っているかどうか；		
		パスワード・アプリケーションのセキュリティ管理	政府事務データを扱う情報システムがパスワードセキュリティ適用管理システムを構築し、GB/T 39786-2021 情報セキュリティ技術における情報システムのパスワード適用に関する基本要件に対応するレベルの要求事項に従っているかどうか；	1	
	サードパーティのセキュリティ要件	委託者による承認の監督	政府データ処理施設の建設や維持管理、政府データの処理を他人に委託するケースがあるかどうか； 存在する場合は、厳格な承認プロセスを通じて受託者が選定されているかどうか、また、政府データ処理に関するセキュリティ要件を受託者が満たしているかどうかを監視されているかどうか；	2	6
		受託者のコンプライアンス責任	委託先が政府機関のデータを保持、利用または他者に提供しているかどうか、提供している場合、委託先の業務が法令および契約合意の規定に準拠しているかどうか、委託先が適切な承認および同意を得ているかどうか；	1	
		受託者のセキュリティ責任	委託先が、委託業務に関わる重要なデータや個人情報の区分やセキュリティレベルを明確に認識し、重点的に保護しているか； 委託を受けた当事者が、データ処理のセキュリティ性を確保するための組織的保護メカニズムを確立しているかどうか、委託を受けた当事者が対応する組織的保護監督責任を確立しているかどうか；	1	
		受託者の責任	受託者が人事セキュリティマネジメントシステムを確立し、人事セキュリティマネジメントの各リンクの運用手順を明確にしているかどうか； 政府データの処理に携わる受託者の職員が、必要な身元調査を受け、守秘義務契約に署名しているかどうか； コミッショナーが、委託を受けた当事者の人事について定期的なレビューを行っているかどうか；	1	
		評議員アセスメント審査	受託者が、データセキュリティ評価およびレビュー報告書の状況について、校長に定期的にフィードバックしているかどうか； コミッショナーによる最適化・改善のためのコメント提供の有無；	1	
セキュリティ技術要求	データ収集	データ収集のコンプライアンス	収集されたデータが他の業務システムに送信される際に認証されるかどうか、データ収集がコンプライアンス要件および送信セキュリティ要件を満たしているかどうか；	1	9
		データ収集の信頼性	データ収集施設がデータ収集元のデータソースを特定し、データソースの真正性要件を満たしているかどうか；	1	
		データ収集の完全性	データ収集施設がデータ検証能力を持ち、収集データの完全性要件を満たしているかどうか；	1	
		データ収集のコンプライアンス要件	データ収集設備が、オーバーサイズやオーバースケールのデータ収集行動を警告する機能を備えているかどうか、必要最小限のデータ収集という原則を満たしているかどうか；	2	

第一指標	第二指標	第三指標	指標の説明	得点 提案	
			データ収集業務に関するコンプライアンス、正当性、一貫性の要件について、データ収集業務が定期的にあセスメントされているかどうか；		
		データ収集のパフォーマンスアセスメント	政府データ処理者がデータを収集する前にネットワークサービスのパフォーマンスがあセスメントされ、ネットワークサービスへの影響が最も少ない許容可能な方法が選択されるかどうか；	1	
		収集施設の分類	データの分類と等級付けが可能なデータ収集設備の有無； 収集された政府データのデータ分類および等級付けが、政府データ分類および等級付け仕様に 従って行われているかどうか；	1	
		収集施設での暗号化された保管	データ収集施設にデータ暗号化保存機能があるかどうか； 収集されたデータとキャッシュされたデータが暗号化されて保存されるかどうか、キャッシュされたデータがパーズされるかどうか；	1	
		収集施設のトレーサビリティの監査	データ収集施設にデータ収集プロセスを記録する能力があるかどうか、データ収集プロセスが監査可能で追跡可能であるかどうか；	1	
	データ送信	データ送信の機密性	セキュリティなチャンネルを導入するかどうか、データ暗号化を使用するかどうか、データ送信プロセスの機密性要件を満たすためにその他の措置を講じるかどうか；	2	7
		データ送信の完全性	セキュリティなチャンネルを導入するかどうか、データ暗号化を使用するかどうか、データ送信プロセスの完全性要件を満たすためのその他の手段を使用するかどうか；	2	
		データ送信の信頼性	データ送信タスクの信頼性を保証するために、ブレイクポイントで送信を継続したり、タイムアウト後に再接続したりする機能があるかどうかなどだ；	1	
		データ送信の監査証跡	データ送信プロセスが監査可能かつ追跡可能であるという要件を満たすために、データ送信プロセスが記録されているかどうか；	1	
		送信施設の分類	データ送信施設が、政府のデータ分類および等級別セキュリティ戦略に基づき、適切なデータセキュリティ保護措置を実施しているかどうか；	1	
	データ保管	保管施設の認可管理	データ保管施設が、異なるプロセス/ツール/アプリケーションが法的に許可されたデータのみアクセスできるという要件を満たすための、セキュリティ分離および権限管理手段を備えているかどうか； データ保管施設の運用に関するセキュリティ管理メカニズムが確立され、統一認証、アカウント権限の最小構成などに対応しているかどうか；	1	12
		保管施設のセキュリティな分離	政府データの保管施設が、公共情報ネットワークから隔離されたセキュリティな場所に配備されているかどうか；	1	
		保管施設の容量要件	データ保管施設が、ID 認証、権限管理、ログ監査、データ暗号化、パッチアップグレードなどの機能を備えているかどうか；	1	
		データ保管のバックアップ・メカニズム	データ保管施設がバックアップの仕組みを持ち、バックアップデータの完全性と可用性を定期的を検証しているかどうか；	2	

第一指標	第二指標	第三指標	指標の説明	得点	提案
			データ保存の適時性要件を満たすために、あらゆる種類のデータの保存期限を定期的にチェックしているかどうか；		
		データ保管の分類階層	データ保管施設が、保管するデータの種類と等級に応じて、適切なデータセキュリティ保護措置を講じているかどうか；	1	
		重要なデータの機密性	重要なデータの機密性を保護するために、暗号技術に基づく機密保護手段が提供されているかどうか；	2	
		政府データの完全性	政府データの完全性を保護するために、暗号技術に基づく完全性保証手段が提供されているかどうか；	1	
		政府データセキュリティ戦略	政府データ保管施設のセキュリティ保管保護措置、データ保管媒体のセキュリティ管理戦略、管理規定など、政府データ保管セキュリティ戦略と運用手順が明確に定義されているかどうか；	1	
		政府のデータ保管場所	政府データが中華人民共和国に保存されているかどうか； (c) 本当に出国する必要がある場合、国内法、行政規則、関連規定の要件が満たされているかどうか；	2	
	データ使用加工	データ処理保護措置	処理されるデータの種類と等級に応じて、適切なデータセキュリティ保護対策が実施されているかどうか；	1	8
		データ処理の機密性	データを暗号化し、使用中および処理中のデータの機密性を保護するために暗号が使用されているかどうか；	1	
		データ処理の監査証跡	データの使用と処理のプロセスが明確に定義され、データ処理の全プロセスが監査可能かつ追跡可能であることを保証するために、データ処理プロセスが記録されているかどうか；	1	
		データ API モニタリング監査	API 資産管理と監視・監査メカニズムを確立するかどうか、API を通じて交換されるデータのセキュリティ監視と監査；	1	
		データ API 送信チャンネル	API データ送信路を保護するために暗号を使用するかどうか；	1	
		データ API 識別制御	データ署名や暗号化が、きめ細かな認証やアクセス制御を提供するために使用されるかどうか； データ API のセキュリティ管理を、アプリケーション識別、状態検証、許可制御のために、データアプリケーション当事者の一意の識別に基づいて行うかどうか；	1	
		データ API 制限ポリシー	データ API の使用に関するセキュリティ制約とセキュリティ管理策を明確に規定した、データ API セキュリティ管理戦略を確立するかどうか； データ API パラメーターのフィルタリング、制限、特殊なインターフェースパラメーターの注入を防ぐためのその他の手段を使用するかどうか；	1	
		データ API 分析ブロック	データ API のコールログが分析され、アラートとブロックのメカニズムを通じて、異常なイベントのリアルタイム通知とブロックが提供されるかどうか；	1	

第一指標	第二指標	第三指標	指標の説明	得点 提案	
	データ提供	データは識別を可能にする	データ供給者と需要者の身元が正当なものであることを保証するために、データが利用可能になる前にデータ供給者と需要者が特定されているかどうか；	1	8
		利用可能なデータの分類と階層	データ提供施設が、提供するデータの種類と等級に応じて、適切なデータセキュリティ保護措置を講じているかどうか；	1	
		施設のセキュリティ機能の提供	データ提供施設が、ID 識別、権限制御、ログ監査、データ暗号化、およびパッチアップグレードなどのセキュリティ保護機能を備えているかどうか；	1	
		施設監査証跡の提供	データ提供施設がデータ提供プロセスを記録し、データ処理プロセスが監査可能かつ追跡可能であるという要件を満たしているかどうか；	1	
		データ共有技術要件	データ共有のセキュリティ技術的措置が GB/T 39477-2020 情報セキュリティ技術管理情報共有データセキュリティ技術要求の規定に従っているかどうか； ファイル共有プロトコルによるデータ共有の場合、SFTP などのセキュリティブロトコルが使用されているかどうか、共有データの暗号化、共有前の両当事者の識別、共有プロセスのロギングなどのセキュリティ対策がとられているかどうか；	1	
		共用施設のセキュリティ対策	を通じたデータ共有について、合理的なセキュリティ対策を提供しているかどうかなどである； 第三者との個人契約やカスタム開発インターフェースなどによるデータ共有について、合理的なセキュリティ対策が講じられているかどうか；	1	
		データ共有の分類階層	共有データのコンテンツ識別とセキュリティ制御が、データ分類と階層仕様に基づいているかどうか；	1	
		オフラインでの共有セキュリティ対策	リムーバブルハードドライブなどのメディアのオフラインコピーによるデータ共有について、合理的なセキュリティ対策が講じられているかどうか；	1	
データ開示	データ開示	データ開示カタログ	データ開示のカタログが作成されているか、データ開示の対象者が特定されているか；	1	5
		データ開示の事前チェック	開示するデータの内容を事前に確認し、重要なデータや機微な個人情報を特定してデータ開示を停止しているか；	2	
		データ・トレーサビリティ	データのトレーサビリティを確立するために技術的手段を用いるかどうか、トレーサビリティ・データの完全性を保護するためにチェックサム技術や暗号技術を用いるかどうか；	1	
		データの公開モニタリング	政府データの開示を監督するメカニズムを確立し、開示されたデータの品質、セキュリティ・リスク、セキュリティ管理作業を監督するかどうか；	1	
データ破棄	不可逆的データ消去	不可逆的データ消去メカニズムが確立され、必要なデータ消去作業者が設定されているかどうか データは、ビジネスシナリオのニーズや、そこから派生したデータの様々なコピーに応じて、不可逆的な方法で削除することができる；	1	4	

第一指標	第二指標	第三指標	指標の説明	得点 提案	
		データ消去技術	物理的および論理的なデータ削除の方法と技術を確立するかどうか、カテゴリーとレベルごとにデータ削除の方法とセキュリティ要件を明確にするかどうか；	1	
		データ削除の仕様	法令に基づくデータ削除のセキュリティ運用規範を定め、重要データや個人情報のマルチカスケード削除の運用形態を定め、セキュリティなデータ削除の運用手順を明確にするかどうか；	1	
		データ削除の監査監督	メディアへのアクセス、使用、破棄のプロセスが記録され、監査され、破棄記録とメディア破棄の有効性が定期的にチェックされているかどうか；	1	
個人情報 の保護要 求	個人情報主 体の権利保 護	第三者施設収集	政府データ中の個人情報が第三者施設から収集されたかどうか； 第三者施設からの収集の場合、当該第三者施設が個人情報主体の権利保護を実施しているかどうか； 政府データを処理する施設が、第三者施設の個人情報とリアルタイムで同期しているかどうか；	1	4
		個人情報主体の 権利	政府データにおける個人情報が、個人情報の主体から収集されたものかどうか； 個人情報の主体から個人情報を収集する場合、個人情報の主体が、データ収集の目的、方法および範囲、個人情報の処理者の名前および連絡先、個人情報の保持期間、個人の法的権利の行使について、明確かつ理解しやすい言葉で、合理的なルートを通じて知らされているかどうか。 当社は、当社の方法および手続き等に従い、個人情報の主体から権限を与えられた同意を得るものとする； GB/T 35273-2020 情報セキュリティ技術個人情報セキュリティ仕様」に基づき、個人情報主体の権利の履行を保証するかどうか； 死亡した個人情報主体の権利の履行を保護するための措置が講じられているかどうか；	2	
		個人情報の撤回 メカニズム	政府データ処理施設が、個人情報を撤回するための仕組みを提供しているかどうか； 撤回に同意した個人情報主体の個人情報の処理行為を直ちに停止し、撤回を要求された個人情報を消去できるかどうか；	1	
	個人情報処 理施設にお ける個人情 報のセキュ リティ保護	個人情報の分類 と保護	政府のデータ処理施設が、個人情報および機微な個人情報を自動的に識別する能力を有するかどうか； 関連措置が GB/T 35273-2020 個人情報セキュリティ情報セキュリティ技術仕様の関連要求事項に従っているかどうか； GB/T 41817-2022 情報セキュリティ技術個人情報セキュリティ工程ガイドライン」に基づき、個人情報の処理を伴うネットワーク製品・サービス（情報システムを含む）の同時企画・同時構築を行うかどうか；	1	
		個人情報の収集 に必要な場合	政府データ処理施設が収集した個人情報が、対応する政府の業務に必要な場合かどうか；	2	

第一指標	第二指標	第三指標	指標の説明	得点 提案	
		預託された個人情報 情報の監督	組織が、個人情報の処理を伴う政府機関のデータ処理を、他の部門に委託しているかどうか； また、委託先が存在する場合は、委託先との間で、個人情報の利用目的、期間、処理方法、種類、保護措置、双方の権利義務について合意しているか、委託先の個人情報処理活動を監督しているか；	1	
セキュリ ティ運用 要求	セキュリテ ィコンプラ イアンスア セスメント	セキュリティ・ コンプライア ンス評価	政府データ処理者の法令遵守要件が定期的（毎年）にアセスメントされ、その 評価報告書が3年以上保管されるかどうか； 政府データの処理について、継続的なコンプライアンスチェックが行われている かどうか；	1	13
	セキュリテ ィ・リスク アセスメン ト	セキュリティ・ リスク評価	政府データ処理に関わる政府データおよび主要データ処理施設について、政府 データ処理のセキュリティ評価が定期的（年次）に実施されているかどうか、 また評価報告書を3年以上保管できるかどうか； 政府データおよび政府データ処理に関わる重要なデータ処理施設について、継 続的なセキュリティチェックが行われているかどうか；	2	
	セキュリテ ィ・リスク コントロー ル	モニタリング・ ポイント	政府のデータ処理に関連するデータセキュリティ・イベントやリスク情報を監 視し、さまざまな種類の異常行動を監視・分析するかどうか；	1	
		通知し、処分す る	特定されたさまざまな種類のデータセキュリティ・インシデントやリスクにつ いて、早期に警告通知を行い、インスタント・メッセージを通じて関係責任者 に通知し、確認と処分を行うかどうか；	1	
	セキュリテ ィ・インシ デントへの 対応 レスポンス シブ	廃棄対策	データセキュリティ・インシデントが発生したかどうか、データセキュリティ ・インシデントに緊急対応する能力があるかどうか；	1	
		避難訓練	データセキュリティインシデントに対する緊急訓練が定期的（年1回）に実施 されているかどうか；	2	
	セキュリテ ィトレサ ビリティ分 析済み	トレサビリテ ィ分析	発生したさまざまなデータセキュリティインシデントのデータセキュリティト レサビリティ分析を実施し、攻撃の最初の発生源と、政府データ処理プラッ トフォームへの攻撃の完全な経路を発見できるようにするために、技術的ツ ールを使用しているかどうか；	1	
		修復と廃棄	トレサビリティ分析が可能かどうかは、セキュリティの脆弱性や隠れた危険 を発見した場合、適時に修復やその他の措置を講じる必要がある；	1	
	セキュリテ ィログ 監査	ログ監査	政府のデータ処理に関連するすべてのデータセキュリティログが、定期的に、 またはイベントトリガーなどに基づいて監査されているかどうか；	2	
		分析して処分す る	データセキュリティ・リスクを分析・検証し、リスクが特定されたデータセキ ュリティ・ログに対して適切な措置を講じるかどうか；	1	
セーフテ ィ・モニ タリング	コンプラ イアンスの監 督プローブ	コンプライア ンス検査の監督	政府データ処理者が、プロセスの様々な時点で政府データ処理活動を監督され ているかどうか；	1	5

第一指標	第二指標	第三指標	指標の説明	得点 提案
要求			政府のデータセキュリティ・コンプライアンスチェックが定期的に行われているかどうか；	
	主なセキュリティ・インシデント緊急事態に対応する	重大なセキュリティ・インシデントへの緊急対応	重大な緊急セキュリティ・インシデントを処理し報告するための効果的なメカニズムを確立するかどうか、重大な緊急セキュリティ・インシデントに対する調査、判断、緊急対応の実施を同期させる能力を持つかどうか；	2
	苦情報告体制	苦情報告	政府データセキュリティに関する苦情・報告ルート、受入・廃棄プロトコルを確立し、苦情・報告方法に関する情報を公表しているかどうか；	1
		受取処理	政府のデータ処理に関連するデータセキュリティや個人情報保護に関する苦情や報告を迅速に受け付ける能力を有しているかどうか。	1

参考文献

- [1] 中華人民共和国全国人民代表大会常務委員会.中華人民共和国サイバーセキュリティ法.2016年11月7日.
 - [2] 中華人民共和国全国人民代表大会常務委員会.中華人民共和国暗号法.2019.10.26 .
 - [3] 中華人民共和国全国人民代表大会常務委員会.データセキュリティに関する中華人民共和国法律.2021年6月10日.
 - [4] 中華人民共和国全国人民代表大会常務委員会.中華人民共和国個人情報保護法 2021年8月20日だ。
 - [5] 中華人民共和国国務院.2021年7月30日、重要情報インフラのセキュリティ保護に関する規則が公布された。
-