

## 【別紙2】

# 電子書籍サービスシステム導入業務 非機能要件書

令和7年7月  
山形市立図書館

## 目次

1	取り扱う情報.....	1
2	目的外利用の禁止.....	1
3	SLA(サービスレベル) .....	2
4	具体的対策 .....	4

電子書籍サービス(以下「本外部サービス」という。)の提供においては、別紙1で規定した機能要件の他、以下に規定する非機能要件を満たすこと。

## 1 取り扱う情報

- (1) 本外部サービスで取扱う情報の種類(以下「山形市管理情報」という。)とその重要性は以下の通りである。情報資産の分類に応じ、取扱制限、運搬、送信及び消去等の情報の取扱いについて、受注者は、山形市の情報セキュリティポリシーに定める内容と同等の取扱いを可能とすること。

No	データ名称	データの概要	重要性
1	コンテンツ情報	使用可能なコンテンツのリスト	重要性Ⅳ
2	所蔵情報	所蔵状態等	重要性Ⅳ
3	利用者情報	ID・パスワード等	重要性Ⅳ
4	利用情報	貸出・予約状況等	重要性Ⅳ
5	各種設定情報		重要性Ⅳ
6	その他データ	統計情報等	重要性Ⅳ

※重要性の分類

重要性	内容
重要性Ⅰ	情報の漏えい等が、住民の生命、財産、プライバシー等へ重大な影響を及ぼす情報
重要性Ⅱ	情報の漏えい等が、行政事務の執行等に重大な影響を及ぼす情報
重要性Ⅲ	情報の誤りやサービス停止等が行政事務の執行及び住民の権利・利益等に重大な影響を及ぼす情報
重要性Ⅳ	上記以外の情報

- (2) 受注者は、情報の取扱状況を適宜把握できること。
- (3) 本サービスを提供するにあたり、受注者が業務委託や他の外部サービスを用いる場合、受注者以外の者と受注者の間において、山形市の情報セキュリティポリシーを遵守するよう合意すること。

## 2 目的外利用の禁止

受注者は、山形市管理情報、本外部サービスの提供に必要な範囲以外の目的で利用しないこと。

### 3 SLA(サービスレベル)

受注者は、以下に示すサービスレベル品質保証(稼働率、目標復旧時間、バックアップの保管方法など)を満たすこと。若しくは、受注者が示すサービスレベルが、山形市が示す事項を満たしていること。

No	分類	サービスレベル項目	条件
1	可用性	サービス時間	サービス提供時間は原則24時間365日とする ただし、メンテナンス、保守、その他緊急対応等のやむを得ない場合は、事前に山形市に連絡を行うこと
		計画停止予定通知	停止日14日前まで連絡すること
		サービス稼働率	99.5%以上
2	障害対応	障害通知プロセス	障害発生時に山形市に電話または電子メールにて通知すること
		障害通知時間	1時間以内目標
		障害監視間隔	1分/回以上
		ディザスタリカバリ	災害発生時のシステム復旧・サポート体制を有すること。併せて、デスクアレイなどの外部記憶装置を物理的に複数台用意するなど、冗長性が確保された同一の構成で情報システムを再構築すること。
		業務停止時の RPO (目標復旧地点)	平常時、業務停止を伴う障害が発生した際には、1 営業日前の時点(日次バックアップからの復旧)までのデータ復旧を目標とすること。
		業務停止時の RTO (目標復旧時間)	平常時、業務停止を伴う障害が発生した際には、1 営業日以内でのシステム復旧を目標とすること。
		業務停止時の RLO (目標復旧レベル)	平常時、業務停止を伴う障害が発生した際には、一部システム機能の復旧を実施すること。
		重大障害時の代替手段	1ヶ月以内に再開することを目指すこと。不可能な場合、同等機能の提供をすること。
3	性能	オンライン応答時間	平均5秒以内 (ただし、学校においてクラス全員が一斉に閲覧開始するなど、集中時は除く)

		バ ッ チ 処 理 時 間	即時処理でない場合、日時・月次・年次とも利用者に影響を及ぼさない時間で処理されること(当初処理等を除く)
		サービス提供状況報告	年1回以上 レポートによる提供
4	拡 張 性	カ ス タ マ イ ズ 性	カスタマイズ可能な場合はその条件を提示すること
		外 部 接 続 性	外部接続用APIを有する場合は公開(提供)すること
		ユ ー ザ ー 数	利用者登録されたユーザーが閲覧・貸出が可能なこと。
		接 続 ユ ー ザ ー 数	同時接続 10,000 ユーザー/分に対応可能であること
		アップグレード方針	バージョンアップは必要に応じて随時実施し、バージョンアップ1カ月前まで概要資料を提供すること セキュリティパッチ適用は3ヶ月に1回以上とし、適用しない場合理由等を提供すること ただし、緊急性の高いパッチは即時に適用すること
5	サポ-ト	サービス提供時間帯 ( 障 害 対 応 )	受付時間 平日9時～17時 (年末年始除く)
		サービス提供時間帯 ( 一 般 問 合 せ )	受付時間 平日9時～17時 (年末年始除く)
		ヘルプデスク	受付時間 平日9時～17時 (年末年始除く)
6	運用管理	システム監視基準	死活監視 10分間隔 サーバ電源監視、サーバOS応答監視 サービス死活監視 10分間隔 Webサービス監視 OS閾値監視 システムログ監視 アプリケーションログ監視 等
7	データ管理	デ ー タ 保 証 要 件	日次バックアップ データベース、設定ファイル等 バックアップ場所 データセンター内

		バックアップデータ保 存 期 間	日次 3 世代(過去 3 日間分)以上
		デ ー タ 消 去 要 件	山形市管理情報については、サービス解 約後 1 カ月以内に別記仕様にに基づき消 去すること。
8	セキュリティ	公 的 認 証 取 得 要 件	情報セキュリティに関する公的認証等を 取得していること。若しくは、取得と同等 の信頼性を有することを客観的な事実等 により説明できること。
		情 報 取 扱 者 の 制 限	山形市管理情報には権限を有する者以 外がアクセスできないこと。
		情 報 取 扱 い 環 境	山形市管理情報にアクセスする場合は、 管理権限を有する者以外が物理的に閲 覧できない環境で行うこと。
		ロ グ の 取 得	アクセス及び管理者権限を有する ID に よる操作についてログを取得すること。
		セキュリティパッチ対応	OS・ミドルウェア等のセキュリティパッチ は速やかに適用すること。
		ウイルスチェック対応	保護ツール等によりリアルタイムで実施 すること。 ウイルス定義ファイルに更新があった場 合は、リリース後に速やかに適用するこ と。
		W e b 対 策	セキュアコーディング、Web サーバの設 定等、対策の強化を図ること。
		通信の暗号化レベル	TLS1.2 以上

#### 4 具体的対策

本サービス使用にあたってセキュリティ及び運用期間中の安定した稼働等を確保す  
るため、導入・構築時、運用・保守時、利用終了時の各段階に応じて次に示す具体的な  
対策をとること。

##### (1) 導入・構築時

1 不正なアクセスを防止するためのアクセス制御対策の実施	
(1)	外部サービスを利用するために付与されるID、パスワードの付与基準、許可基 準、更新基準、廃棄・削除基準等を明確化し、当該基準に沿った運用ができるよう 構築すること。

	(2)	付与したID、パスワードが不正に利用されないよう、また不正に利用された場合その状況を確認できるよう構築すること。
	(3)	外部サービスを利用するための管理者権限を有するIDについて、より強固な認証方式を採用するよう構築すること。
	(4)	パスワードは原則次のとおり設定できること。 ・長さ 6 文字以上の制限 ・英大文字、英小文字、記号及び数字を含む文字列が使用可能 →パスワードを暗号化した状態で保存
	(5)	外部サービスで提供される機能や外部サービス上に保存される情報に、アクセス権限のないものがアクセスできないよう制限すること。
	(6)	外部サービスに、データベースの中身を強制的に書き換えることができる機能や一時的にポートを開放する機能等の管理サービスが存在する場合、当該管理サービスで設定できる項目を最小限にすること。また管理サービスに接続できる場所を限定すること。またこれらの操作において、誤操作を防止できるよう、適切な示唆や確認メッセージが表示されるよう構築すること。
	(7)	外部サービス構築にあたり仮想マシン(ソフトウェアによって仮想的に再現された物理的なコンピュータと同等の機能を有するコンピュータ)を使用する場合は、不正プログラム対策(必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策、ログ取得等の実施)を確実に実施すること。また、適切なセキュリティ対策を実施した後、インターネット等外部ネットワークに接続する手順とすること。
<b>2 取り扱う情報の機密性保護のための暗号化</b>		
		外部サービスにおいて重要性Ⅰまたは重要性Ⅱの情報を取り扱うことを市が明示した場合、外部サービス内及び外部サービス利用者から外部サービスまでの通信経路全般において認証情報を暗号化すること。
	(1)	利用する暗号化方式は、「電子政府推奨暗号リスト」に記載された暗号化方式であるか、または記載された暗号化方式と同等以上の強度を持つ暗号化方式であること。
	(2)	当該外部サービスの暗号における一連の管理策が、関連する協定、法令及び規制を遵守していること。また、「電子政府推奨暗号リスト」に記載されていない暗号化方式を利用する場合、特に輸出規制に抵触していないこと。
<b>3 開発時におけるセキュリティ対策</b>		
	(1)	外部サービスによる情報システム構築時の仕様書やソースコード、設定情報、ネットワーク情報等の情報を漏えい等しないよう適切に管理すること。
	(2)	外部サービスによる情報システム構築時に使用する又は導入するソフトウェア等が当該ソフトウェアベンダーのライセンス規定に適合しているか確認すること。

	(3)	外部サービス構築時に利用するAPI等のサービス提供者以外のソース等を使用する際に、マルウェア等を混入させない等、情報セキュリティに配慮した開発の手順を確立するとともに、手順に基づき構築を行うこと。
<b>4 設計・設定の誤り</b>		
	(1)	外部サービスに係る設定が適切であるか、確認する方法を市と事前に協議すること。
	(2)	外部サービスに係る設定内容について、複数人で確認を行うこと。
	(3)	市が実施できる外部サービスに係る設定の範囲を極力最小化すること。また、その責任範囲を明確化すること。
	(4)	利用状況に応じて自動的にリソースの割り当てを変更する場合、リソース不足によるサービス停止とならないよう、適切に監視し、必要なリソースを確保できるよう構築すること。
	(5)	外部サービスにより提供するサービスが、定期保守等を除き停止させることが難しいものである場合、電源やネットワークの冗長化等、可用性を考慮した設計・設定となっているか確認すること。
	(6)	外部サービスで使用するシステムが、適切に時刻同期するよう設計・設定すること。

(2) 運用・保守時

<b>1 取り扱う情報資産の適切な管理の実施</b>		
	(1)	外部サービスで利用する情報システムに割り当てるCPU、メモリ等のリソースが適切であるか、適宜管理すること。
	(2)	外部サービスの脆弱性対策を実施すること。また、実施状況を報告すること。
<b>2 不正アクセスを防止するためのアクセス制御の実施</b>		
	(1)	外部サービス等の管理者権限を本市業務担当者及び当該外部サービス保守事業者以外の者に割り当てしないこと。
	(2)	管理者権限による操作について、全て記録・保存すること。
	(3)	当該外部サービスが不正利用されていないか監視すること。
<b>3 暗号化のための情報の適切な管理</b>		
	(1)	外部サービスを利用するための通信経路や外部サービスに保存するデータ等を暗号化する場合は、構築時の暗号化方式を採用しているか確認すること。
	(2)	構築時の暗号化方式の脆弱性の有無の確認や、脆弱性がある場合の対策を適宜実施すること。また、対策不可能な脆弱性が発見された場合は、安全性が確保された暗号化方式に変更すること。
	(3)	暗号化方式を変更する場合は、事前に市と協議すること。協議においては、変更後の暗号化方式がセキュリティ上適切であることを説明すること。



	(4)	外部サービスを利用するための通信経路や外部サービスに保存するデータ等を暗号化する場合は、当該鍵の管理者を明確化すること。
	(5)	当該鍵の管理者が外部サービス提供者となる場合、次の事項について、サービス利用中定期的に確認すること。また、管理方法を変更する場合事前に市と協議すること。 <ul style="list-style-type: none"> <li>・ 鍵が搾取されていないこと、搾取されている恐れのないこと</li> <li>・ 鍵の管理方法が搾取される恐れがないこと</li> <li>・ 鍵の保管場所が国内サーバであること</li> <li>・ 鍵の管理方法が運用中に変更されていないこと</li> </ul>
	(6)	当該鍵の生成、更新、失効、廃棄方法について事前に確認するとともに、それぞれの行為を実施する際は、規定どおりに実施されたか確認すること。
<b>4 設計・設定時の誤りの防止対策の実施</b>		
	(1)	利用する外部サービスの設定を変更する必要がある場合は、事前に市と協議を行うこと。
	(2)	設定変更を行う場合は、当該変更箇所について、変更前、変更後の設定内容を記録日時とともに保存すること。
	(3)	利用者設定や通知等の運用に大きな影響を及ぼさない設定変更を市が行う場合の手順書を整備するとともに、整備した手順書に変更すべき点がないか、定期的に市と協議すること。
<b>5 外部サービスを利用した情報システムの事業継続の確保</b>		
	(1)	障害等の事態に対応できるよう、外部サービスで提供するシステムや設定情報を構築時や設定変更時等に必要なバックアップを取得すること。
	(2)	仕様書に規定した間隔でバックアップを取得すること。また、取得されているか定期的に確認すること。
	(3)	バックアップを用いてシステムを復旧させるための手順書を整備するとともに、訓練の実施などにより当該手順を実施できる体制を確保すること。
	(4)	外部サービスで利用しているデータ容量、性能等を監視し、未然に障害発生等を防止すること。

(3) 利用終了時

1 外部サービスで取り扱った情報等の廃棄	
(1)	<p>以下を例とする外部サービス利用時に取り扱ったすべての情報及び外部サービス利用するために必要となった設定情報等の情報を、復元できない方法により削除すること。</p> <ul style="list-style-type: none"> <li>・外部サービスに保存された情報</li> <li>・仮想リソース (仮想マシン、仮想ストレージ、仮想ネットワーク等)</li> <li>・ファイル (ストレージサービスに格納したファイル、各サービスのログ、開発関連ファイル、設定ファイル 等)</li> <li>・暗号化された情報の復号に用いる鍵</li> <li>・ドメイン情報</li> <li>・上記のバックアップデータ</li> </ul>
(2)	(1)で規定する情報が暗号化されている場合においても、同様に削除すること。
(3)	外部サービス利用時に取り扱った情報について、(1)、(2)に基づき情報を廃棄した旨の実施報告書を提出すること。
2 外部サービスで取り扱った機器廃棄時の情報廃棄	
(1)	外部サービス利用時に使用した基盤となる物理機器を、外部サービス利用終了とともに廃棄する場合は、当該機器に保存した情報を、研究所レベルでの攻撃から耐えられるレベルで削除すること。
(2)	外部サービス利用時に使用した基盤となる物理機器に保存した情報について、(1)に基づき廃棄した旨の実施報告書を提出すること。
3 外部サービス利用のための作成したアカウントの廃棄	
(1)	作成した外部サービス利用者アカウントを全て削除すること。または、市が削除できること。
(2)	利用した外部サービス管理者アカウントを削除すること。または、市が削除できること。
(3)	削除した管理者アカウントが再利用できないことを確認すること。
(4)	外部サービス利用者アカウント以外の特殊なアカウント(ミドルウェアアカウント等)を作成した場合、当該アカウントを確実に削除すること。または、市が削除できること。
(5)	外部サービス利用者アカウント以外の特殊なアカウントを使用して作成したデータについても、復元できない方法により削除すること。