標準様式第３号（第12条関係）

要求水準等説明書

令和８年５月18日

千代田区教育委員会事務局 指導課

目次

1　業務概要

(1) 業務名

ちよだリテラシー検定システム・教材コンテンツ開発業務

(2) 業務目的

SNS や生成 AI などの普及により、情報発信・取得が容易になった現代においては、自分の考えをもち、情報を正しく判断する力が重要である。

区では、区内の児童・生徒の「批判的に読み解く力」や「確かな情報を見極める力」等、メディアリテラシーを中心に育成するため、「ちよだリテラシー教育」を推進し、各学校において様々な取り組みを実施してきた（別紙１，２参照）。

今後、こうした取り組みをさらに加速させ、より効果的な指導につなげていくためには、児童・生徒がどの程度のリテラシーを有しているのかを把握するとともに、育成していくべきポイントを客観的データに基づき判断していく必要がある。

そこで、「ちよだリテラシー教育」が掲げる「７つの育成する力」を測定する検定システムと、それぞれの力を伸ばすための教材コンテンツを開発する。

検定によって判明した強みと弱みを踏まえた、効果的な教材・指導により、児童・生徒を「情報を読み解き自己の信念に従って行動ができる人」へと成長させることを目指す。

(3) 業務内容

２　システム要件を満たす「ちよだリテラシー検定システム・教材コンテンツ」の構築及びクラウドサービスの提供

(4) 契約期間及び履行期限

契約締結日の翌日から令和９年３月 31 日まで。

ただし、構築は令和９年１月から２月末までに履行を完了することとし、構築完了後速やかに利用者への公開を行い、サービスの提供を行うこととする。

※サービスの提供については、実施状況を毎年度区が評価し、最長で令和 14 年３月 31 日まで継続して契約を締結することがある。

(5) 支払方法

構築にかかる経費は一括払いとし、サービスの利用にかかる経費は毎月又は四半期払いとする。いずれも履行検査合格後、適正な請求書を受領した日から 30 日以内に支払う。サービスの利用にかかる経費は運用保守の経費を含んだ形で請求すること。

(6) 経費概算（上限額）

《令和８年度》　　6,044,000 円（税込）

《令和９～13 年度計》　8,404,000 円（税込）

※なお、見積書には令和 9 年度から令和 13 年度までの各年度の費用も記載すること。
※上限額を超えた提案があった場合は失格とする。

2　システム要件

(1) システム構成図

別紙３のとおり

(2) 共通要件

- クラウド型のサービスであること。
- 最新のブラウザ（Edge、Google Chrome、Safari、Firefox など）で利用できること。

(3) 利用者（予定）

- 区立小学校５～６年生（約 1,170 名）
- 区立中学校１～３年生（約 1,130 名）
- 小中学校教職員
- 教育委員会事務局職員

(4) 利用イメージ

- 別紙４のとおり

(5) アカウント管理機能要件

- 区内小学校の５～６年生及び区内中学校１～３年生の約 2300 名を目安に、リテラシー検定機能、教材コンテンツ利用機能、履歴確認等の権限を持つアカウントを発行可能であること。
- 管理者権限を持った教育委員会用アカウントを 1 つ、各生徒の情報を確認できる小中学校教職員用アカウントを学校別に 1 つ以上発行可能であること。
- 児童・生徒用アカウントについては、本区の学校教育システムにおける児童・生徒用アカウントからシングルサインオン（SAML 認証）できるように設定すること。設定に当たっては、学校教育システムの保守事業者と連携すること。

  ただし、本 SSO 連携における受託者の作業範囲は、「連携に必要な設定情報（メタデータ等）の提供」及び「本システム側での受入設定」までとする。統合 ID 管理側への組み込み設定及び両システム間の疎通テストの主導・進行管理については、保守事業者の責任範囲とする。

(6) 検定システム要件

- 別紙１，２において、区のこれまでの取組や実態調査の結果を示している。これらを踏

まえ、ちよだリテラシー教育が掲げる「７つの育成する力」を測定する検定システムを構築すること。
特に、別紙１で「今後重点的に育成が必要な内容」として挙げている「信頼性の高い情報の見極め」、「事実と意見の区別」、「情報を批判的に読み解く力」については、より確実に検定できるよう構築すること。

- 検定方法は多肢選択式問題等によることとし、受検者の回答結果を集計し、測定項目毎に数値化できるようにすること。
- 検定内容は、受託者の提案をベースに区と協議の上決定することとし、社会情勢の変化等を踏まえて随時追加、修正できるようにすること。
  なお、単に知識を問う設問だけでなく、図やイラストを交えながら、実際に起こりうるシチュエーションに対してどのように対応すべきかを判断させるような設問等、「７つの育成する力」を効果的に測定できる設問を提案すること。
- 検定受験後、個人、クラス及び学校毎にレポートを出力できるようにすること。
- 各レポートは、測定項目毎の数値を表やグラフで分かりやすく示すとともに、強みや弱み、改善方法等についても提案できるようにすること。また、過去の受検分と結果を比較し、成長度合いを確認できるようにすること。
- 検定結果を踏まえ、弱みとなる項目を伸ばすための最適な教材コンテンツに誘導する仕組みを設けること。

(7) 教材コンテンツ要件

- 別紙１，２を踏まえ、ちよだリテラシー教育が掲げる「７つの育成する力」を伸ばすための教材コンテンツを開発すること。
  検定システムと同様に、別紙１で「今後重点的に育成が必要な内容」として挙げている「信頼性の高い情報の見極め」、「事実と意見の区別」、「情報を批判的に読み解く力」については、より効果的に育成できるよう開発すること。
- 教材コンテンツは、クイズ形式やゲーム形式、動画形式のものなど、児童・生徒が興味関心を持って継続的に取り組めるものを提案すること。
- 各コンテンツの内容は、受託者の提案をベースに区と協議の上決定することとし、社会情勢の変化等を踏まえて随時追加、修正できるようにすること。
  なお、令和８年度は、「７つの育成する力」のうち、区が指定する項目に対応するコンテンツを計４本以上開発すること。
- 各コンテンツの受講状況・履歴を確認できるようにすること。

(8) セキュリティ要件

- 別紙５「Web サイト構築 【対策基準】 対策基準チェックシート (2) 重要度低」に該当する場合の対策一覧を全て満たすこと。
- 脆弱性への対応を迅速に行うことができるよう、サーバで使用している OS やソフトウェアの情報を管理すること。使用している OS やソフトウェアのサポート期限を把握し、サ

ポートが終了する前にアップデートできるよう計画をたてること。

- 使用している OS やソフトウェアの開発元等から提供される脆弱性情報や、JPCERT/CC や IPA 等から提供される注意喚起情報を継続的に入手し、ソフトウェアの更新や問題の回避を検討すること。
- サーバ・ネットワーク監視及びセキュリティの確保に必要なログを収集し、確認が行えるように 2 年以上保存すること。（クラウドサービスの保存期間を超えるログデータは、手動にてエクスポートし外部記録媒体等に保存する方法でも可能とする。）

(9) 運用保守要件

- 障害発生時の連絡体制や対応フロー等をあらかじめ区に提示すること。
- 故障や障害が発生した場合は速やかに区に報告し復旧を図ること。
- 管理するデータが消失しないようバックアップデータを定期的に取得し、バックアップデータから復旧作業を実施できること。
- 操作方法が記載してあるマニュアルを作成し、提供すること。
- 土日祝日年末年始を除く平日 9：00 から 17：00 まで、教育委員会事務局及び各学校からのシステムの操作方法等の問い合わせ対応を行うこと。

3　個人情報保護

個人情報の取扱いについては、個人情報保護法及び関連法令を遵守すること。

4　選定スケジュール概要

日付	事項	詳細
令和８年５月18日（月）から 令和８年５月29日（金）まで	公募公表、要求水準等説明書公開期間	５(1)
令和８年５月21日（木）まで	要求水準等説明書に関する質問受付期限	５(2)
令和８年５月29日（金）まで	参加申込書提出期限	５(3)
令和８年６月５日（金）	提案者選定結果通知	５(4)
令和８年６月17日（水）まで	提案書作成に関する質問受付期限	５(5)
令和８年６月30日（火）まで	提案書提出締め切り	５(6)
令和８年７月上～中旬	プレゼンテーション（ヒアリング）	５(7)
令和８年７月中～下旬	採用、不採用の通知	５(8)

5　選定スケジュール詳細

(1) 公募公表、要求水準説明書公開期間

ア　公開期間：令和８年５月 18 日（月）から令和８年５月 29 日（金）まで

イ　公開場所：千代田区ホームページ「プロポーザル情報」のページ
https://www.city.chiyoda.lg.jp/koho/kuse/nyusatsu/proposal/index.html

(2) 要求水準等説明書に関する質問

ア　受付期限：令和８年５月 21 日（木）まで

イ　受付方法：「質問書」の様式により、**６　担当課**へ電子メールで提出すること（電話による質問は受付不可）。件名は「ちよだリテラシー検定システム・教材コンテンツ開発業務事業者選定に係る質問」とし、要求水準等説明書等の資料のページ番号、質問対象の項目・引用文等を用いて、質問内容を具体的に記載すること。

ウ　回答方法：質問に対する回答は、電子メールにて当該質問者に対して令和８年５月 28 日（木）に回答するとともにホームページで公表する。

(3) 参加申込書の提出

ア　提出物　：①　参加申込書（様式第４号、様式４－２～８）

②　契約書の写し等、類似実績業務内容（様式４－４）を証明できるもの

③　その他

申込日現在、東京電子自治体共同運営電子調達サービスにおいて、区の競争入札参加資格を有しないものは、参加申込書の提出にあたり次に掲げる書類を併せて提出すること。

(ｱ) 身分（身元）証明書及び後見登記等ファイルに成年被後見人、被保佐人又は被補助人とする記録がないことの証明書（被補助人にあっては後見登記等ファイルに記録されている事項の証明書）（発行後３か月以内のもの。個人に限る。）

(ｲ) 住民票の写し（発行後３か月以内のもの。個人に限る。）

(ｳ) 登記簿謄本（発行後３か月以内のもの。法人に限る。）

(ｴ) 別添「営業所表」（標準様式第５号）

(ｵ) 別添「委任状」（標準様式第６号。対象業務において代理人を置く場合に限る。）

(ｶ) 財務諸表（直前決算のもの。法人については貸借対照表及び損益計算書並びに剰余金処分計算書、個人については貸借対照表及び損益計算書）

イ　提出期限：令和８年５月 29 日（金）午後５時

ウ　提出場所：**６　担当課**のとおり

エ　提出方法：事前連絡の上、提出場所へ持参すること

オ　資格要件

・地方自治法施行令（昭和 22 年政令第 16 号）第 167 条の４第１項（同令第 167 条の 11 第１項において準用する場合も含む。）の規定に該当する者でないこと。

・千代田区競争入札参加有資格者指名停止措置要領（平成７年９月１日７千総経発第 92 号）による指名停止を受けていないこと。

・千代田区契約関係暴力団等排除要綱（平成 23 年８月 26 日 23 千政契担発第 71 号）に基づく入札参加除外を受けていないこと。

・経営不振の状態でないこと。

※契約締結までの間に参加資格を有しなくなった場合は、その時点で失格とする。

(4) 提案者の選定

ア　通知方法

参加申込事業者に対し、令和８年６月５日（金）に、書面により選定結果を通知する。提案者として選定されない旨の通知を受けた者は、通知のあった日の翌日から起算して７日以内に、書面により、区長に対して選定されなかった理由について説明を求めることができる。

当該書面は、**６　担当課**へ提出期限日までに郵送すること（必着）。この要望に対し、区は、説明を求めることができる最終日の翌日から起算して 10 日以内に書面により回答する。

イ　提案者を選定する概数　３者程度

ウ　選定基準

	評価項目	評価の視点	指標	配点
1	経営状況	安定して業務を遂行できる経営状況にあるか	資本金 自己資本比率　等	1
2	業務遂行力	当該業務を遂行するために必要な知識・経験を有するか	同種・類似業務の実績　等	3
3	実施体制	業務を遂行するための体制は妥当か	保有する技術者の数 本業務へ配置される従業員の数　等	3
4	情報管理力	個人情報の管理能力の有無	ISMS 認証（ISO/IEC 27001）及びプライバシーマーク認証の取得状況	2
5	社会・地域貢献	社会的貢献度の有無等	分野ごとの社会・地域貢献活動の内容等	1

(5) 提案書作成に関する区への質問

ア　受付期限：令和８年６月 17 日（水）まで

イ　受付方法：「質問書」の様式により、**６　担当課**へ電子メールで提出すること（電話による質問は受付不可）。件名は「ちよだリテラシー検定システム・教材コンテンツ開発業務事業者選定に係る質問」とし、要求水準等説明書等の資料のページ番号、質問対象の項目・引用文等を用いて、質問内容を具体的に記載すること。

ウ　回答方法：質問に対する回答は、電子メールにて全提案者に対して令和８年６月 24 日（水）に回答する。

(6) 提案書の提出

ア　提出物

提案書（任意様式）正本１部、副本９部

- 提案書の作成様式

提案書はＡ４判左綴じで作成することとし、文字サイズ 11 ポイント以上、表紙・目次を含めて３０ページ以内とすること（Ａ３版のページはＡ４版２ページとカウントし、Ａ４版に折り込むこと）。その他の様式は問わないが、次の「提案書に記載する内容」を具体的かつ明瞭に記載すること。

提出書類１セットごとにフラットファイル（Ａ４縦）１冊に綴り、正本の表紙のみに法人名等を記入すること。

審査は事業者名を伏せて行うため、副本９部のフラットファイルの表紙には法人名を記入せず、提案書内に会社名やロゴ等を使用しないこと。

- 提案書に記載する内容

(ｱ) 当該システムが**２　システム要件**を満たすことの説明

(ｲ) 検定システム及び教材コンテンツの構成、検定内容等に関する提案

(ｳ) 構築スケジュール及び見積額（令和８年度、令和９～13 年度の各年度毎）

(ｴ) その他、以下「(7)　プレゼンテーションヒアリング　エ　選定基準　提案内容評価」の各項目を評価するための説明

イ　提出期限：令和８年６月 30 日（火）午後５時

ウ　提出場所：**６　担当課**のとおり

エ　提出方法：事前連絡の上、提出場所へ持参すること

オ　その他　：・提案書の作成及び提出に係る費用は提出者の負担とする。

・提出された提案書は返却しない。

・提出された提案書は、提出者に無断で提案の採否決定以外の目的には使用しない。

・提出期限後における提案書の差し替え及び再提出は認めない。

・提案書に虚偽の記載をした場合は、提案書を無効とするとともに、虚偽の

記載をした者に対して区の競争入札参加資格上の指名停止を行うことがある。

(7)プレゼンテーションヒアリング

令和８年７月上～中旬にプレゼンテーションによる審査を実施し、提出書類及びヒアリング内容から総合的に評価する。詳細は提案者に選定された事業者に対し別途通知する。

ア　開催場所：千代田区役所会議室（予定）

イ　開催日時：令和８年７月上～中旬

ウ　持ち時間：各社プレゼンテーション時間 20 分程度、質疑応答時間 10 分程度

エ　選定基準

	評価項目	評価の視点・判断基準	配点
組織評価			
1	提案者の選定基準と同じ５項目	同上	10
提案内容評価（システム）			
2	取組方針	本区が推進する「ちよだリテラシー教育」のこれまでの取組や課題意識を理解した上で取組方針が示されているか	10
3	検定システム	検定内容や検定方法、検定後のレポートや教材コンテンツとの連動等について、具体的かつ効果的な内容が提案されているか。	15
4	教材コンテンツ	コンテンツの内容や検定結果との連動等について、具体的かつ効果的な内容が示されているか。	15
5	ユーザーインターフェース	操作に不慣れな者でも直感的に操作できるようなユーザビリティに優れたＵＩが提案されているか。	10
6	セキュリティ・運用保守	不正アクセスや情報漏えいへの対策が十分に取られているか。システム等を安定的に運用し、障害発生時も速やかに復旧できる体制が取られているか。	10
7	発展性・拡張性	検定内容や教材等、コンテンツの追加・変更が容易にできるように構成されているか。将来的な機能追加等が提案されているか。	10
提案内容評価（説明内容）			
8	取り組み姿勢	課題・目的等の理解度が高く、積極的に取組む意欲が感じられるか。	10
9	理解しやすさ	平易な表現により理解しやすく、説明内容が提案書の内容をよく補完しており、数値や図表等を用いた客観的な評価が可能な説明となっているか。	10

※選定経過の透明性確保のため必要な限度で参加者ごとの評価結果を事後に公表する。

(8) 提案採用者の選定

ア　選定方法

プレゼンテーションヒアリングの審査後、組織評価の得点に提案内容評価の得点（評価項目毎に、各審査員の平均点を算出し合計する。）を加え、合計得点が最も高い者を提案採用者に選定する。ただし、合計得点が 60 点を下回る場合は採用しない。

また、採用者が「**５　選定スケジュール詳細**（３）オ 資格要件」を喪失した場合、業務の仕様書等について区との合意が得られない場合、採用者が辞退した場合は次点を採用者とする。

ア　通知方法

各提案者に対し、令和８年７月中～下旬を目途に、書面により採用又は不採用の結果を通知する。不採用の通知を受けた者は、通知のあった日の翌日から起算して７日以内に、書面により、区長に対して不採用の理由について説明を求めることができる。説明請求は郵送でのみの受付とし、送付先は担当課宛とすること。この要望に対し、区は、説明を求めることができる最終日の翌日から起算して１０日以内に書面により回答する。

６　担当課

千代田区教育委員会　子ども部　指導課　茂木
〒102-8688 東京都千代田区九段南一丁目２番１号　千代田区役所４階
電話：03-5211-4283（直通）
Ｅ-mail：shidou@city.chiyoda.lg.jp

「ちよだリテラシー教育」の取組状況について

別紙１

１　背景

SNS などの普及により情報発信・取得が容易になった現代では、自分の考えをもち、情報を正しく判断する力が重要である。こうした力を育むために「ちよだリテラシー教育」を推進し、特にメディアリテラシーの育成に力を入れていく。

２　目指すべき子どもたちの姿

「情報を読み解き自己の信念に従って行動ができる人」（千代田区子育て・教育ビジョンより）

３　育成する力

（１）善悪を判断して行動する力
（２）類似情報を比較する力
（３）事実と意見を区別する力
（４）批判的に読み解く力
（５）発信者の意図を考える力
（６）確かな情報を見極める力
（７）自分の考えを形成する力

４　学校での取組

（１）国語科を中心とした言語能力を育む指導の充実
（２）読書活動の充実
（３）資料やデータの見方・活用における指導の充実
（４）情報モラル教育の充実
（５）AI など新たな技術の体験・活用

５　教育委員会及び学校のこれまでの取組

（１） 目指す姿、育成する力、学校での取組を可視化（各学校は教育課程に記載）
（２） メディアリテラシーに関する資料を整理・作成
（３） 管理職向け研修
（４） 児童・生徒向け実態調査
（５） 各学校の「ちよだスマートスクールの」での授業公開、講演会等
（６） 各学校独自の取組（外部団体を活用したセーフティ教室、ビブリオバトル等）

６　児童・生徒向け実態調査について（質問項目は裏面参照）

実施時期：令和７年５月８日（木）から令和７年５月 30 日（金）まで
対　　象：小学校５～６年生及び中学校・中等教育学校前期課程の児童・生徒
結　　果：〇高い達成度が示された内容
　　インターネット上での配慮や自分の行動の影響
　●今後重点的に育成が必要な内容
　　信頼性の高い情報の見極め、事実と意見の区別、情報を批判的に読み解く力

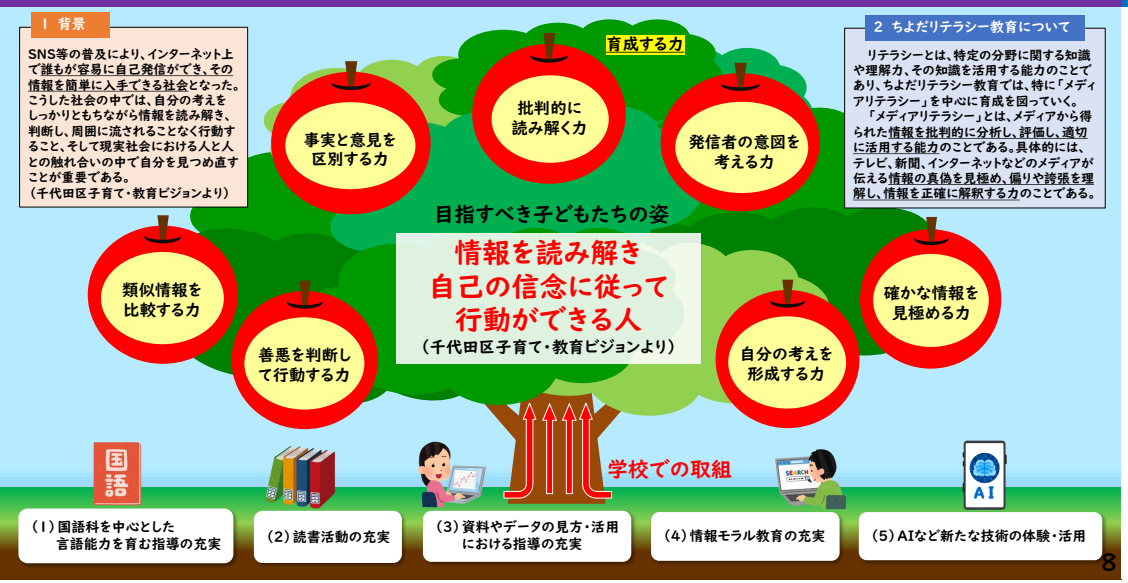
【質問項目】

小学校５～６年生	中学校/中等教育学校（前期課程）
善悪を判断して行動する力	
1.ネット上で発信するときに、相手を傷つけないための注意点を考えることができる。	1.オンラインでのコミュニケーションを図る際、適切な発信を心がけることができる。
2.自分の行動が周囲にどのような影響を与えるか考え、迷惑をかけないよう判断することができる。	2.自分の行動が社会にどのような影響を与えるかを深く考え、責任ある判断をすることができる。
類似情報を比較する力	
3.複数の方法を組み合わせて、どちらがより信頼できる情報かを考えることができる。	3.複数の情報源を比較し、それぞれの特徴や信頼性を分析することができる。
4.いくつかの意見を比べて、自分が賛成できるものを選ぶことができる。	4.異なる視点の意見を比較し、それらの背景や論拠を分析しながら、自分の立場を整理できる。
事実と意見を区別する力	
5.「事実」と「自分の考え」に分けて文章を書くことができる。	5.ニュースや記事を読んだとき、事実と意見を正しく分けながら、自分の考えを書くことができる。
6.ニュースや記事を読んで、どこまでが事実でどれが意見かを見つけることができる。	6.ニュースや記事の中で、客観的事実と解説・意見を区別することができる。
批判的に読み解く力	
7.ニュースや記事などの情報を簡単に信じず、疑いながら読むことができる。	7.映像作品や報道がどのようなメッセージを伝えているかを批判的に考察することができる。
8. 他者の主張や考えなどに触れたときに、矛盾点があれば指摘することができる。	8.本や記事の論点を整理し、問題点や矛盾点を指摘することができる。
発信者の意図を考える力	
9.作者や筆者、発表者の考えや意図を考えながら読んだり聞いたりすることができる。	9.本や映像作品など、作者の意図やねらいを考えながら読んだり視聴したりすることができる。
10.同じ出来事でも発信者の立場によって伝え方が違うことを考えることができる。	10.ニュースや記事、人の話は、発信者の立場によって伝え方が違うことを考えることができる。
確かな情報を見極める力	
11.インターネットの情報を正しいかどうか確認することができる。	11.インターネットから信頼できる情報を選ぶことができる。
12.調べた情報の出典を確認し、信頼性を考えることができる。	12.情報の発信元の違いを分析し、それぞれの信頼性について考えることができる。
自分の考えを形成する力	
13.自分の意見を他の人に説明するときに、そう考えた理由もしっかり伝えることができる。	13.自分の意見を論理的に整理し、他者に根拠を示しながら伝えることができる。
14.他の人の意見を聞いて、自分の考えに付け加えたり新しい考えをもったりすることができる。	14.意見をもった後も、新たな情報を踏まえて柔軟に考えを見直すことができる。

別紙２

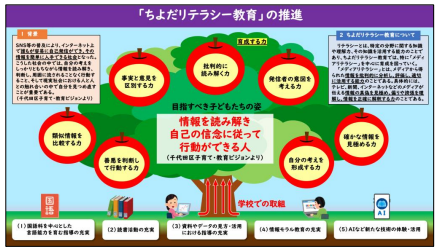
令和７年11月17日　第２回情報リテラシー意見交換会　参考資料２
（令和７年10月14日　文教福祉委員会　教育委員会資料　1-2）

「ちよだリテラシー教育」の推進



令和7年度「ちよだリテラシー教育」における教育委員会及び学校の取組

①目指す姿、育成する力、学校での取組を可視化



○教育課程届出説明会にて説明
○各学校が教育課程に記載
○校園長会、副園校長会、各種研修等で周知

②メディアリテラシーに関する資料を整理・作成

○国語科の年間指導計画　○事例で学ぶNetモラル
○企業等による出前授業　○NHK for School
○GIGAワークブックとうきょう　等を掲載

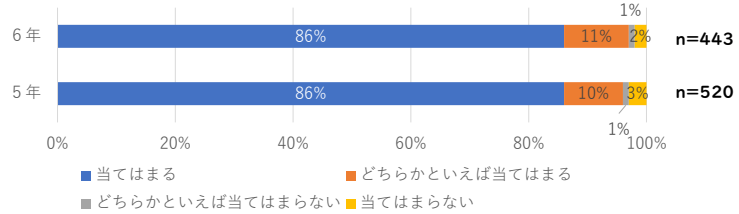
③管理職向け研修（5/7）
④児童・生徒向け実態調査（5月末）
⑤各学校の「ちよだスマートスクールの日」での授業公開、講演会等
⑥各学校独自の取組

学校での取組を支援

善悪を判断して行動する力

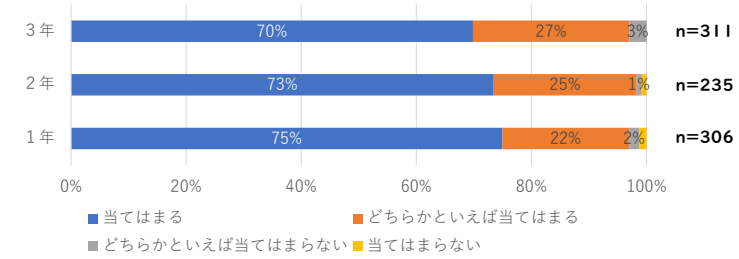
1.ネット上で発信するときに、相手を傷つけないための注意点を考えることができる。

小学校



1.オンラインでのコミュニケーションを図る際、適切な発信を心がけることができる。

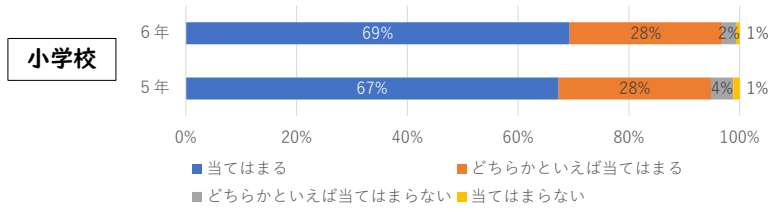
中・中等



善悪を判断して行動する力

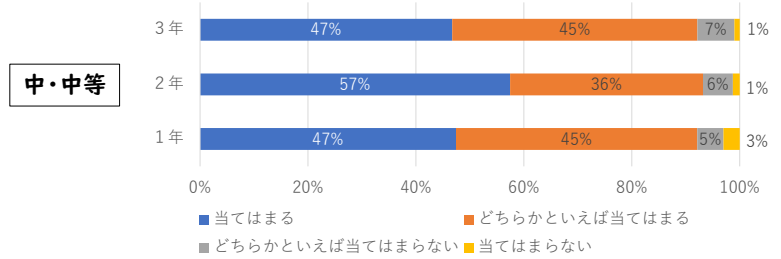
2.自分の行動が周囲にどのような影響を与えるか考え、迷惑をかけないよう判断することができる。

小学校



2.自分の行動が社会にどのような影響を与えるかを深く考え、責任ある判断をすることができる。

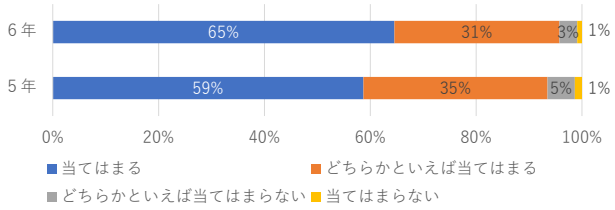
中・中等



類似情報を比較する力

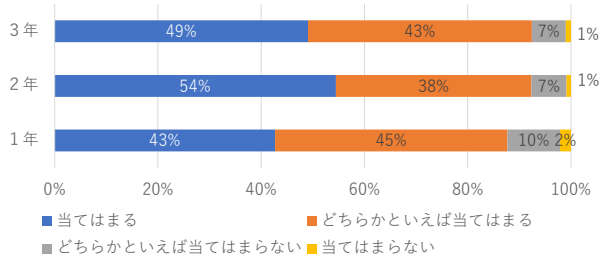
3.複数の方法を組み合わせて、どちらがより信頼できる情報かを考えることができる。

小学校



3.複数の情報源を比較し、それぞれの特徴や信頼性を分析することができる。

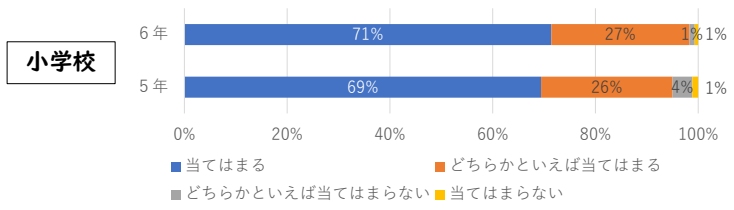
中・中等



類似情報を比較する力

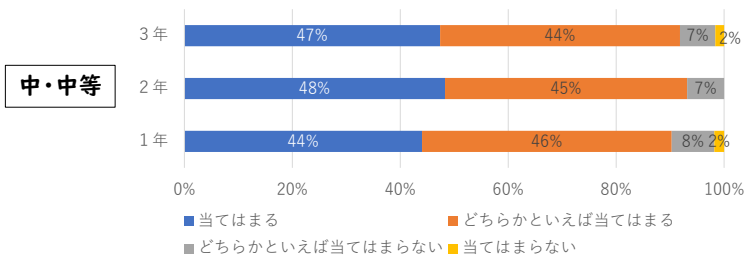
4.いくつかの意見を比べて、自分が賛成できるものを選ぶことができる。

小学校



4.異なる視点の意見を比較し、それらの背景や論拠を分析しながら、自分の立場を整理できる。

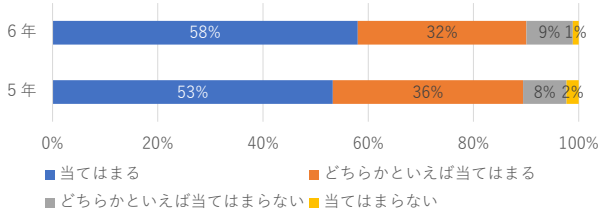
中・中等



事実と意見を区別する力

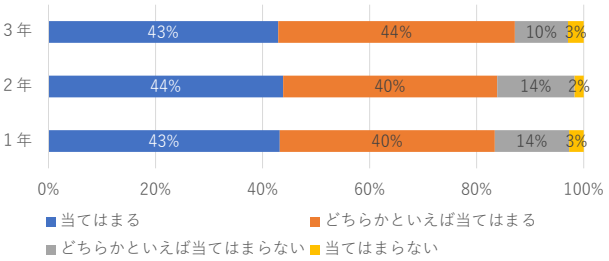
5.「事実」と「自分の考え」に分けて文章を書くことができる。

小学校



5.ニュースや記事を読んだとき、事実と意見を正しく分けながら、自分の考えを書くことができる。

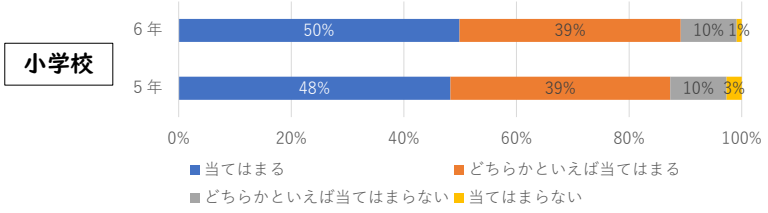
中・中等



事実と意見を区別する力

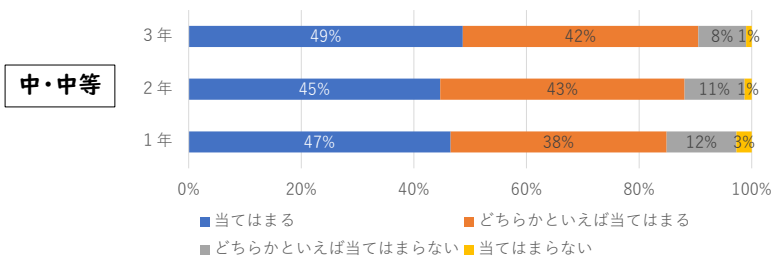
6.ニュースや記事を読んで、どこまでが事実でどれが意見かを見つけることができる。

小学校



6.ニュースや記事の中で、客観的事実と解説・意見を区別することができる。

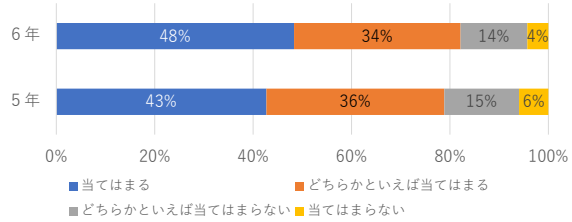
中・中等



批判的に読み解く力

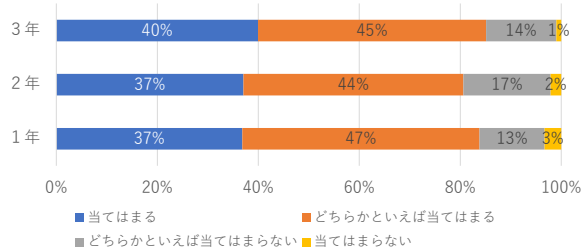
7.ニュースや記事などの情報を簡単に信じず、疑いながら読むことができる。

小学校



7.映像作品や報道がどのようなメッセージを伝えているかを批判的に考察することができる。

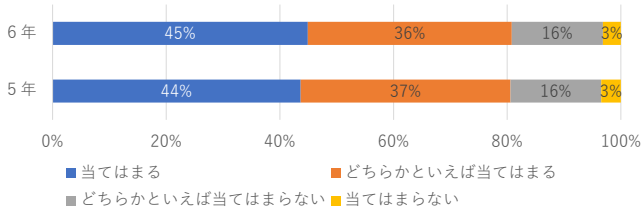
中・中等



批判的に読み解く力

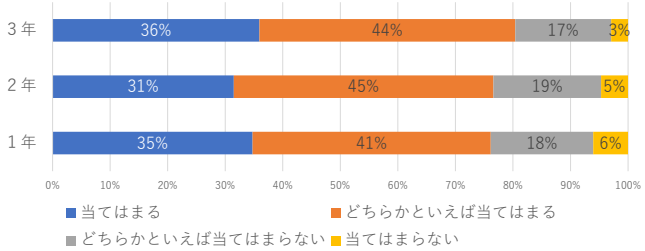
8. 他者の主張や考えなどに触れたときに、矛盾点があれば指摘することができる。

小学校



8.本や記事の論点を整理し、問題点や矛盾点を指摘することができる。

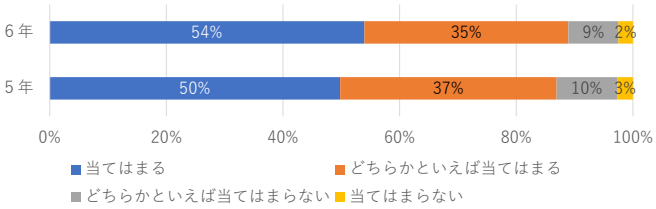
中・中等



発信者の意図を考える力

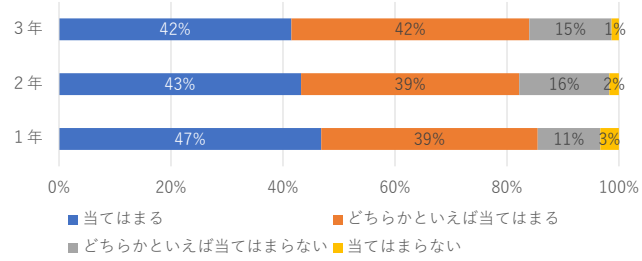
9.作者や筆者、発表者の考えや意図を考えながら読んだり聞いたりすることができる。

小学校



9.本や映像作品など、作者の意図やねらいを考えながら読んだり視聴したりすることができる。

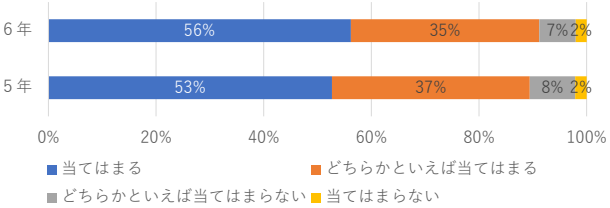
中・中等



発信者の意図を考える力

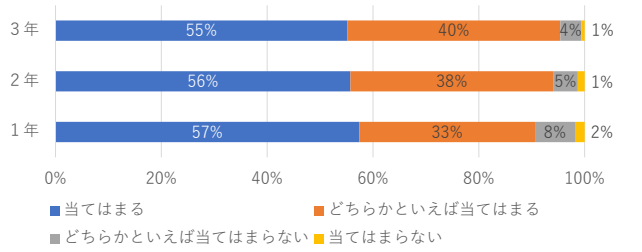
10.同じ出来事でも発信者の立場によって伝え方が違うことを考えることができる。

小学校



10.ニュースや記事、人の話は、発信者の立場によって伝え方が違うことを考えることができる。

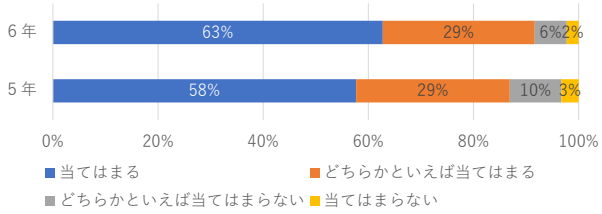
中・中等



確かな情報を見極める力

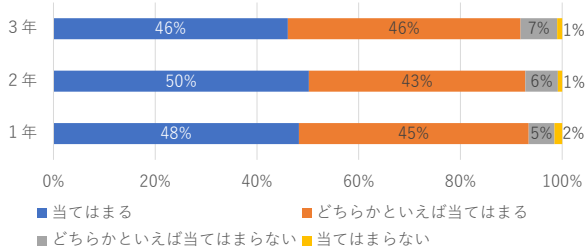
小学校

11.インターネットの情報を正しいかどうか確認することができる。



中・中等

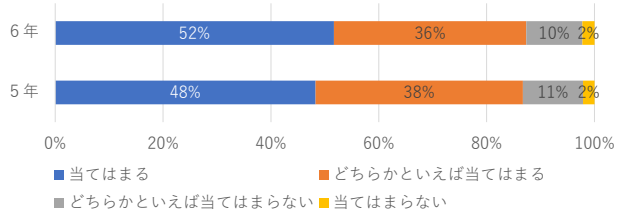
11.インターネットから信頼できる情報を選ぶことができる。



確かな情報を見極める力

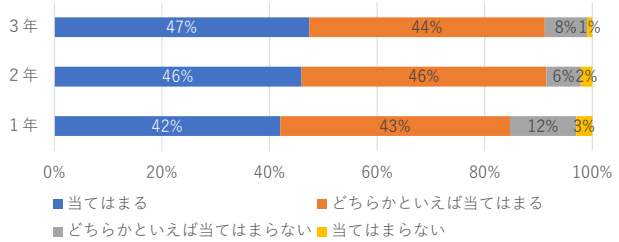
小学校

12.調べた情報の出典を確認し、信頼性を考えることができる。



中・中等

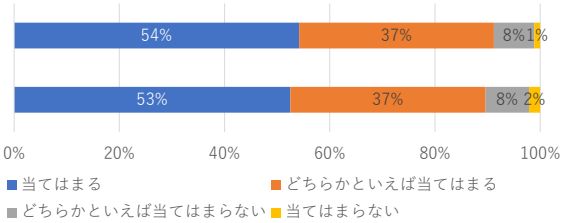
12.情報の発信元の違いを分析し、それぞれの信頼性について考えることができる。



自分の考えを形成する力

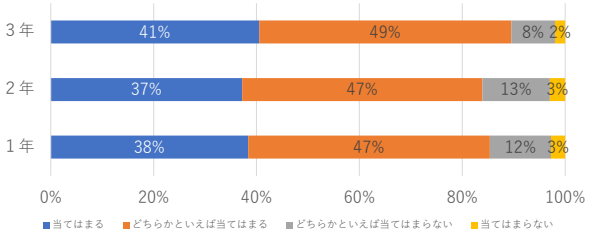
小学校

13.自分の意見を他の人に説明するときに、そう考えた理由もしっかり伝えることができる。



中・中等

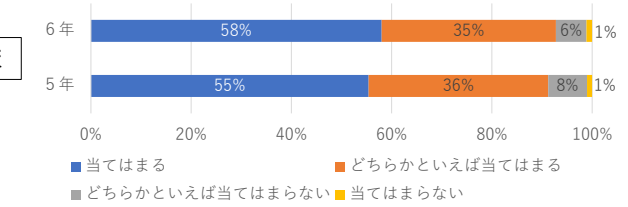
13.自分の意見を論理的に整理し、他者に根拠を示しながら伝えることができる。



自分の考えを形成する力

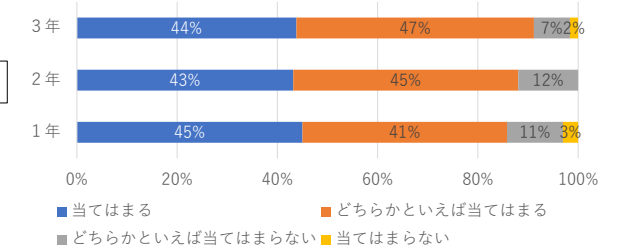
小学校

14.他の人の意見を聞いて、それをもとに新しい考えをもつことができる。

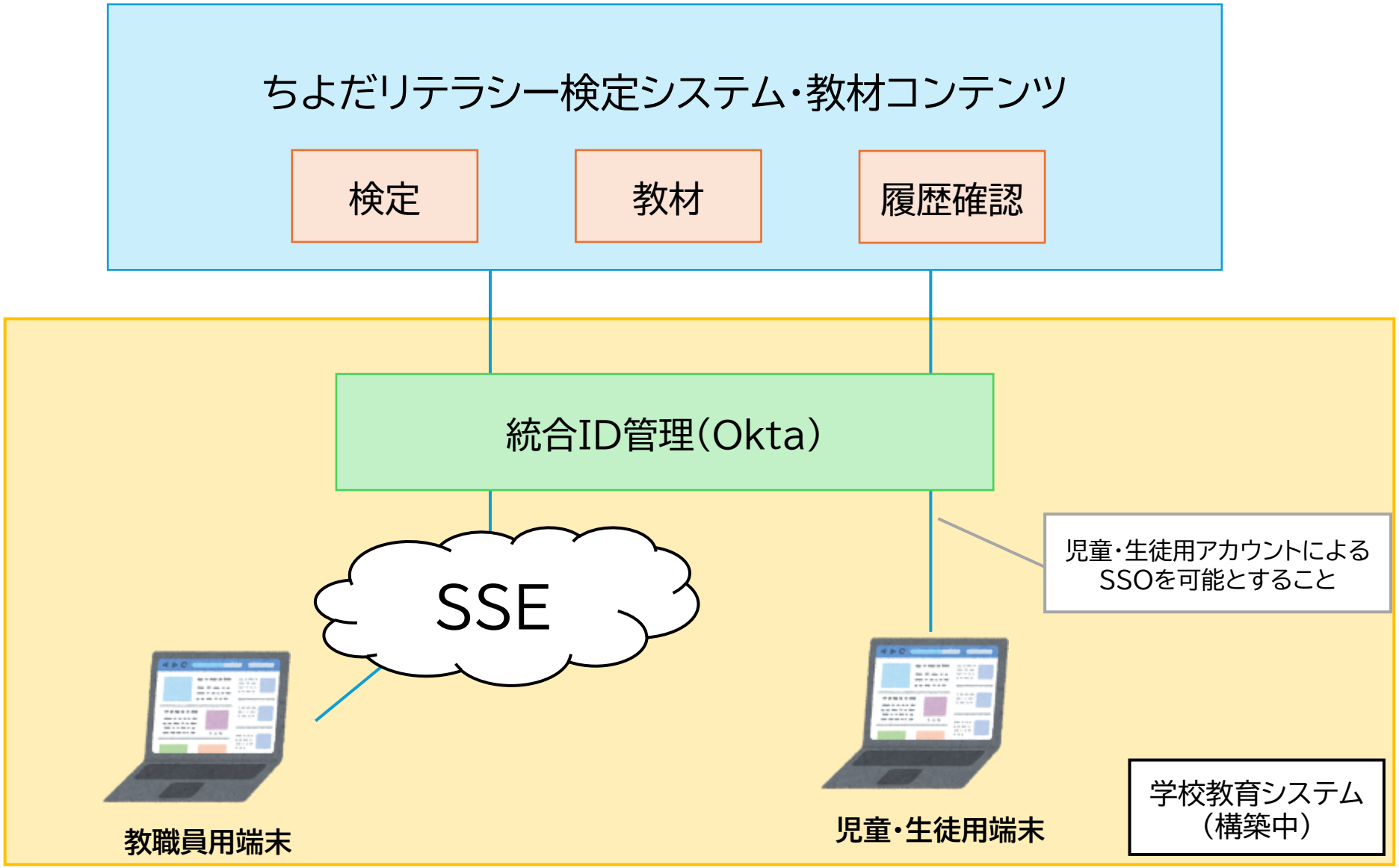


中・中等

14.意見をもった後も、新たな情報を踏まえて柔軟に考えを見直すことができる。



別紙3　システム構成図


ちよだリテラシー検定システム・教材コンテンツ
検定
教材
履歴確認
統合ID管理（Okta）
SSE
児童・生徒用アカウントによる
SSOを可能とすること
教職員用端末
児童・生徒用端末
学校教育システム
（構築中）

別紙４　利用イメージ

定期的に再検定を実施（検定内容、教材も必要に応じて更新）

児童・生徒

検定受験

教職員

現状の
強み・弱み
を把握

最適な教材
コンテンツ
を活用

指導方針に
反映

リテラシー
向上

効果的な
指導

Web サイト構築
【対策基準】

新版改定:令和 4 年 10 月 1 日

第 2.1 版

千代田区

＜改定履歴＞

	版　数	制定(改定)年月日	備考
1	1.1	平成 31 年 4 月 1 日	
2	2.0	令和元年 10 月 24 日	7.6. ドメインの管理の追加
3	2.1	令和 4 年 10 月 1 日	TLS バージョンの変更（TLS1.1 から 1.2 へ）
4			

※修正や改定における版数管理の条件を以下に定める。

＜版数管理条件＞

	条件	判断	版数
1	・文字等の修正、追記、削除等	修正	0.１版毎に増やす (例)第 1.1 版、第 1.2 版
2	・項目の追加、変更、削除、移動等 ・項番の変更が生じた時 ・大幅な基本方針、対策基準の変更	改定	1.0 版毎に増やす (例)第 2.0 版、第 3.0 版

※修正並びに改定の場合、版数履歴に必ずその旨記載する。

総　則

1. 総則

1.1. 目的

「千代田区 Web サイト構築対策基準」は、「千代田区情報セキュリティポリシー対策基準」に基づき、千代田区((以下、区とする。) の Web サイト構築及びそれに伴う職務において、情報セキュリティ対策を実現するために定めるものである。

この対策基準は、Web サイトを構築する際の基本となるものであり、情報資産の重要度に適合したセキュリティ機能の実現、Web サイト構築や運用におけるセキュリティ要件の作成を行う際の基準となるものである。

1.2. 対策基準見直しの実施サイクル

対策基準の陳腐化を防ぐため、最新技術の導入や現状の運用手順等を鑑み、定期的に見直しを行う。

Web サイト構築
対策基準

Web サイト構築対策基準

2. 対象とする Web サイト

本書では、インターネットからアクセス可能な Web サイトのうち、以下に該当する Web サイトを対象とする。

・千代田区が運営する Web サイト
・千代田区指定管理者が運営する Web サイト
・その他千代田区に関連する団体等が運営する Web サイト

新規に構築する Web サイト及びすでに運営している Web サイトについても本対策基準に従ったセキュリティ対策を実施することとする。

3. 情報資産の重要度の判定基準

情報セキュリティの三要素である機密性・完全性・可用性に基づき、その情報資産の重要度を判定する基準を示す。判定結果に基づいて、対策すべき基準を判断するものとする。

表 2-1　情報資産の重要度の判定基準

三要素	判定基準	重要度
機密性	情報漏洩により利用者や社会への影響が大きい可能性のある個人情報等を扱っているシステム	高
	情報漏洩により利用者や社会への影響が少ない一般的な公開情報のみを扱っているシステム	低
完全性	扱っている情報が改ざんされることにより、利用者や社会への影響が大きい可能性のあるシステム	高
	扱っている情報が改ざんされた場合でも、利用者や社会への影響が少ないシステム	低
可用性	システムが一時的にでも停止することにより、利用者や社会への影響が及ぶ可能性があるシステム	高
	システムが一日停止しても、利用者や社会に影響が及ぶ可能性が少ないシステム	低

4. 物理的セキュリティ

情報資産の重要度の判定結果に関わらず、「千代田区情報セキュリティポリシー対策基準 6.物理的セキュリティ」に準拠することとする。

5. 人的セキュリティ

「千代田区情報セキュリティポリシー対策基準　7.人的セキュリティ」に準拠することとする。なかでも構築した Web サイトにおける ID 及びパスワード等の管理について、外部委託事業者にも同様の管理を徹底させることとする。

6. 技術的セキュリティ

6.1. サーバ基本設定

Web サーバの基本的な事項について規定する。

(1) 不要なサービスの停止

Web サイトの運営に必要のないサービスは停止すること。

(2) 外部公開が不要なポートの遮断

外部に公開する必要のないポートは遮断すること。

(3) システム情報の非表示

サーバが外部に出力する情報に、利用している OS やミドルウェアのバージョン等、攻撃のヒントとなりうる情報が外部に出力されないように隠蔽すること。

(4) 公開不要なファイルの確認

① 公開を想定していないファイルを公開用のディレクトリに保管しないこと。

② ディレクトリ構造が画面表示されないようにすること。

(5) 管理用インタフェースの制限

運用保守のための管理用画面等のインタフェースは原則としてインターネットに公開しないこと。

やむを得ず公開する場合は、アクセス元 IP アドレスによるフィルタリング等のアクセス制限を行うこと。また、通信内容の暗号化を行うこと。

6.2. 認証

認証機能における対策事項を規定する。

(1) 認証の実施

特定のユーザのみに表示・実行を許可すべき画面や機能には、認証を必要とすること。

管理者用画面には認証を必要とすること。

(2) 不要アカウントの削除

運用開始前に、検証用アカウント等不要なアカウントを削除すること。

(3) パスワード規則

① パスワード文字列は少なくとも大小英字と数字の両方を含み、最低 8 文字以上であること。

② 画面にパスワード文字列を表示しないこと。

(4) 認証時におけるメッセージ

認証画面において、ユーザ ID とパスワードのどちらが間違っているか推測できるようなメッセージを表示しないこと。（例：「パスワードが間違っています」というメッセージにはせず、「ユーザ ID もしくはパスワードが違います」というようなメッセージにすること。）

また、ユーザ ID とパスワードの長さや文字種を推測できるようなメッセージを表示しないこと。

(5) パスワードの保存

パスワードをサーバ内で保管する際は、平文ではなくソルト付きハッシュ値の形で保管すること。

(6) アカウントロック

【機密性または完全性の重要度が「高」の場合】

認証時に無効なパスワードで一定回数（例：10 回）の試行があった場合、一定時間（例：30 分間）はアカウントがロックアウトされた状態にすること。

6.3. セッション管理

セッション管理機能における対策事項を規定する。

(1) セッション ID の生成

① 自前でセッション管理の仕組みを構築せずに、ミドルウェアやフレームワーク等が提供するセッション管理の仕組みを利用すること。

② セッション ID を推測が困難なものにすること。

(2) セッション ID の扱い

セッション ID を URL パラメータに格納せずに、Cookie に格納するか、POST メソッドの hidden パラメータに格納して受渡しをすること。

(3) Cookie の設定

HTTPS 通信で利用する Cookie には secure 属性を設定すること。

(4) CSRF（クロスサイト・リクエスト・フォージェリ）

登録・変更・削除等の処理が実行される箇所において、CSRF の脆弱性への対策を施すこと。

対策例）

・処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行する。

・処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。

・Referer が正しいリンク元かを確認し、正しい場合のみ処理を実行する。

(5) セッション ID の破棄

① 認証済みのセッションが一定時間（例：60 分）以上アイドル状態にあるときはセッションタイムアウトとし、サーバ側でセッションを破棄しログアウトすること。

② ログアウト機能を用意し、ログアウト実行時にはサーバ側でセッションを破棄すること。

6.4. セキュリティ実装

ウェブアプリケーションの開発においては、セキュリティを考慮した実装を行わなければ脆弱性を作り込んでしまうおそれがある。IPA が公開している「安全な Web サイトの作り方」に挙げられている対策を基本として、最低限以下の脆弱性について対策をすること。

(1) SQL インジェクション

SQL インジェクションの脆弱性への対策を施すこと。

【根本的解決】

① SQL 文の組み立ては全てのプレースホルダで実装する。

② SQL 文の構成を文字列連結により行う場合は、アプリケーションの変数を SQL 文のリテラルとして正しく構成する。

③ ウェブアプリケーションに渡されるパラメータに SQL 文を直接指定しない。

【保険的対策】

④ ミドルウェアやフレームワークが出力する SQL 文等を含むエラーメッセージをそのままブラウザに表示しないこと。

⑤ データベースアカウントに適切な権限を与える。

(2) OS コマンド・インジェクション

OS コマンド・インジェクションの脆弱性への対策を施すこと。

【根本的解決】

①シェルを起動できる言語機能の利用を避ける。

【保険的対策】

②シェルを起動できる言語機能を利用する場合は、その引数を構成する全ての変数に対してチェックを行い、あらかじめ許可した処理のみを実行する。

(3) パス名パラメータの未チェック/ディレクトリ・トラバーサル

ディレクトリ・トラバーサルの脆弱性への対策を施すこと。

【根本的解決】

① 原則として、外部からのパラメータにファイル名を直接指定しないようにし、ファイル名を指定する必要がある場合には想定外のファイル名であるかどうかのチェックを行うこと。

② ファイルを開く際は、固定のディレクトリを指定し、かつファイル名にディレクトリ名が含まれないようにする。

【保険的対応】

③ ウェブサーバ内のファイルへのアクセス制限の設定を正しく管理する。

④ ファイル名のチェックを行う

(4) クロスサイト・スクリプティング

クロスサイト・スクリプティングの脆弱性への対策を施すこと。

対策例）

・ウェブページに出力する全ての要素に対して、エスケープ処理を施す。

・URL を出力するときは、「http://」や「https://」で始まる URL のみを許可する。

・<script>…</script>要素の内容を動的に生成しない。

・スタイルシートを任意のサイトから取り込めるようにしない。

・入力された HTML テキストから構文解析木を作成し、スクリプトを含まない必要な要素のみを抽出する。

・HTTP レスポンスヘッダの Content-Type フィールドに文字モード（charset）を指定する。

(5) HTTP ヘッダ・インジェクション

HTTP ヘッダ・インジェクションの脆弱性への対策を施すこと。

対策例）

・ヘッダの出力を直接行わず、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用 API を使用する。

・改行コードを適切に処理するヘッダ出力用 API を利用できない場合は、改行を許可しないよう、開発者自身で適切な処理を実装する。

(6) メールヘッダ・インジェクション

メール送信処理が行われる箇所において、メールヘッダ・インジェクションの脆弱性への対策を施すこと。

対策例）

・メールヘッダを固定値にして、外部からの入力はすべてメール本文に出力する。

・メールヘッダを固定値にできない場合、ウェブアプリケーションの実行環境や言語に用意されているメール送信用 API を使用する。

・HTML で宛先を指定しない。

(7) クリックジャッキング

クリックジャッキングの脆弱性への対策として、HTTP レスポンスヘッダに X-Frame-Options ヘッダを出力すること。

(8) その他

① URL パラメータにユーザ ID やパスワード等の情報を格納しないこと。

② 入力値の文字種や文字列長の検証を行うこと。
③ ミドルウェアやフレームワークが出力する詳細なエラー内容をブラウザに表示しないこと。
④ 重要な処理（例：認証の失敗、アカウント情報の変更）が行われた際にログを記録すること。

6.5. 通信の暗号化

Web サーバとブラウザ（クライアント）との通信の暗号化について規定する。

(1) HTTPS の使用

Web サイトの全てのページにおいて、HTTPS を使用すること。

(2) SSL サーバ証明書

SSL サーバ証明書は Web サイトへのアクセス時に警告（発行者、発行先、有効期間等の不備によるもの）が出ないものを使用すること。

(3) SSL/TLS のバージョン

TLS1.2 以上を使用し、SSL2.0／3.0、TLS1.0、TLS1.1 を無効にすること。

6.6. その他

その他、Web サイトの情報セキュリティ対策に関わる事項を規定する。

(1) マルウェア対策

【機密性、完全性または可用性の重要度が「高」の場合】

外部からコマンド実行やファイル転送が可能なプロトコル（例：HTTP、HTTPS、FTP、SSH 等）を使用しているサーバについて、マルウェア対策ソフトを導入すること。

導入後は、定期的（例：1 日 1 回）にマルウェア定義ファイルを更新すること。

(2) 不正アクセス検知・防御

【機密性、完全性または可用性の重要度が「高」の場合】

サーバへの不正アクセスを検知するため、IPS/IDS を導入すること。導入後は、攻撃パターン情報（シグネチャ）を適宜更新（フォールスポジティブが発生した際のシグネチャの見直し、最新のシグネチャの適用等）すること。

(3) WAF

【機密性、完全性または可用性の重要度が「高」の場合】

重大な脆弱性への暫定対処を可能とするために、WAF を導入すること。

(4) 重要情報の暗号化

【機密性の重要度が「高」の場合】

重要な情報（個人情報等）をサーバ等に保存する場合には、情報の重要度に応じて暗号化を実施すること。

7. 運用

7.1. 構成管理

Web サイトの構成に関わるセキュリティ対策について規定する。

(1) 使用している OS、ソフトウェアの管理

脆弱性への対応を迅速に行うことができるよう、サーバで使用している OS やソフトウェアの情報を管理すること。使用している OS やソフトウェアのサポート期限を把握し、サポートが終了する前にアップデートできるよう計画をたてること。

(2) 脆弱性情報の取得

使用している OS やソフトウェアの開発元等から提供される脆弱性情報や、JPCERT/CC や IPA 等から提供される注意喚起情報を継続的に入手し、ソフトウェアの更新や問題の回避を検討すること。

7.2. 管理用アカウントの管理

Web サイトの管理用アカウントに関わるセキュリティ対策について規定する。

(1) アカウント共用の禁止

管理者用アカウントは複数人で共有せずに、個人毎に割り当てること。なお、やむを得ず複数人で共用する場合には、当該アカウントを使用した者が特定できるように運用すること（例：対象サーバにアクセスするための端末のアカウントを個人毎に割り当てる等）。

(2) 不要アカウントの定期的な確認

管理者アカウントのうち、不要となったアカウントは速やかに削除又は無効化

すること。また、定期的に不要となったアカウントがないか確認すること。

(3) パスワードの管理

6.2.認証（3）パスワード規則を踏襲すること。やむを得ず複数人でアカウントを共有している場合には、管理者の変更等が発生したタイミングでパスワードの変更を実施すること。

7.3. ログの監視

ログの監視によるセキュリティ対策について規定する。

(1) 取得すべきログの明確化と収集

サーバの監視に必要なログを目的に応じて明確化し、対象のログを収集すること。

(2) 認証ログの確認

認証がある Web サイトについて、パスワードリスト攻撃等を検知するため、認証ログ(認証エラー発生件数の急激な増加､特定 IP アドレスからの大量アクセス等)を定期的に確認すること。監視システムのアラームによる確認でも可とする。

7.4. データのバックアップ

Web サイトに求められる可用性や完全性の基準に応じて、バックアップ対象のデータ及びバックアップ方法を定めること。

7.5. 対策状況の報告

セキュリティ対策の状況について、以下のタイミングにて区へ報告すること。

(1) 新規構築時

・本稼動前に実施した脆弱性診断の結果および対策結果

(2) 運用時

以下の事項について最低年 1 回、及び区からの求めがあった場合に報告すること。

・使用している OS、ソフトウェアの一覧およびバージョン（最新バージョンでない場合には、その旨および最新バージョンを使用していない理由を報告すること。）

・管理用アカウントについて、7.2 の事項を確認した結果
・監視しているログの確認結果
・個別に脆弱性診断を実施した場合には、その診断結果および対策結果

7.6. ドメインの管理

Web サイト構築のために使用するドメインの取り扱いについて以下の通り行うこと。

(1) ドメインの取得
・ドメインを取得する場合は、そのドメインの管理方法を明確にすること。

(2) ドメイン変更の必要性の検討
・ドメインの変更については、利用を停止するドメインが悪用される危険性が高いことから、必要性について慎重に検討を行うこと。（ドメイン変更の必要がない場合、変更を行わないこと。）

(3) ドメインの利用停止、変更について
・一度作成した Web サイトのドメインについては、極力変更しないこと。
・万が一、Web サイトのドメインの変更や利用停止を行う場合、使用しなくなるドメインについては、二次利用もしくは不正に取得される恐れがあるため、契約を続けて保管すること。
・ドメインの利用停止を行う場合は、ドメインを利用停止する旨を関連する案内ページを用いて案内を行うこと。※1
・ドメインの変更を行う場合は、新ドメインへのサービス移行を行った上で、新ドメインの案内ページの表示を行うこと。※1
また、旧ドメイン運用停止後一定期間は、検索エンジン、お気に入り等から旧ドメインへのアクセスを考慮して対策を講じること。

※1. 提示内容例
・現行ドメインの運用停止期間
・現行ドメインの運用停止後は当該ドメインからの情報提供は行わない
・運用停止するドメインで提供している情報の新ドメインでの掲示先
・運用停止するドメインをなりすまし防止の為一定期間所有を行う旨の記載

8. 外部サービスの利用

Web サイト構築のために外部のクラウドサービス等を利用する場合に確認すべき内容を規定する。

(1) 選定基準

① 事業者の信頼性

サービスを提供する事業者は信頼できる事業者であること。

・日本国内の事業者によるサービスであること。
・日本の法律が適用できること。
・個人情報の取扱いに関する規定があること。
・守秘義務に関する規定があること。
・情報セキュリティに関する基本方針・規定等が整備されていること。
・事業継続に関する基本方針・規定等が整備されていること。

② サービスの信頼性

サービスの稼働率などのサービスレベルが示されていること。

・サービスの稼働率の目標値が規定されていること。
・プライバシーマーク（JIS Q 15001）等、ISMS（JIS Q 27001 等）の認証を取得していること。
・サービスが停止しない仕組み（冗長化、負荷分散等）を設けていること。
・SLA が契約書に添付されていること。
・日本国内にデータセンターがあること。

③ セキュリティ対策

サービスにおけるセキュリティ対策が具体的に公開されていること。

・死活監視を実施していること。
・マルウェア対策を実施していること。
・セキュリティパッチ管理が一定の間隔で実施されること。
・データの暗号化措置への対応があること。
・ファイアウォール等の不正アクセスを防止する措置があること。
・不正なサーバ侵入に対する検知等の仕組みがあること。
・ネットワークの暗号化措置への対応があること。

④ 管理者用インタフェースのセキュリティ対策

管理者用インタフェースに対する認証やアクセス制限が適切にされていること。

・IP アドレスによるアクセス制限、ワンタイムパスワード等

⑤ 基盤環境のセキュリティ対策

サービス側に基盤環境の管理責任がある場合に、必要なポート、サービスのみを有効とする等の対応が可能であること。また、使用している OS、ミドルウェアの設定変更やバージョンアップが可能であること。

⑥ サポート

サービスの利用や設定等について問い合わせを受け付ける窓口が用意されていること。

(2) 選定結果の確認

(1)選定基準の①から⑥について確認した結果に基づき、区に確認を求めること。

9. 評価

9.1. 脆弱性診断

Web サイトの新規構築時には、本稼動前に脆弱性診断を実施し、その結果に基づいて対策を実施すること。

また、Web サイトのリニューアルの際には、変更のあった箇所についてセキュリティ対策が十分に実施されているか確認を行うこと。

10. 対策基準チェックシート

技術的セキュリティ、運用、外部サービスの利用、評価における対策基準を以下の表に一覧でまとめる。

(1) 重要度高に該当する場合

機密性、完全性、可用性のいずれかが重要度高に該当する場合に必要となる対策を一覧で示す。

○：要実施

分類	要件	機密性	完全性	可用性
サーバ基本設	不要なサービスの停止	○	○	○

分類	要件	機密性	完全性	可用性
定	外部公開が不要なポートの遮断	○	○	○
	システム情報の非表示	○	○	○
	公開不要なファイルの確認	○	○	○
	管理用インタフェースの制限	○	○	○
認証	認証の実施	○	○	○
	不要アカウントの削除	○	○	○
	パスワード規則	○	○	○
	認証時におけるメッセージ	○	○	○
	パスワードの保存	○	○	○
	アカウントロック	○	○	-
セッション管理	セッション ID の生成	○	○	○
	セッション ID の扱い	○	○	○
	Cookie の設定	○	○	○
	CSRF	○	○	○
	セッション ID の破棄	○	○	○
セキュリティ実装	SQL インジェクション	○	○	○
	OS コマンド・インジェクション	○	○	○
	パス名パラメータの未チェック	○	○	○
	クロスサイト・スクリプティング	○	○	○
	HTTP ヘッダ・インジェクション	○	○	○
	メールヘッダ・インジェクション	○	○	○
	クリックジャッキング	○	○	○
	その他	○	○	○
通信の暗号化	HTTPS の使用	○	○	○
	SSL サーバ証明書	○	○	○
	SSL/TLS のバージョン	○	○	○
その他	マルウェア対策	○	○	○
	不正アクセス検知・防御	○	○	○
	WAF	○	○	○
	重要情報の暗号化	○	-	-
構成管理	使用している OS、ソフトウェアの管理	○	○	○
	脆弱性情報の取得	○	○	○
管理用アカウントの管理	アカウント共用の禁止	○	○	○
	不要アカウントの定期的な確認	○	○	○

分類	要件	機密性	完全性	可用性
	パスワードの管理	○	○	○
ログの監視	取得すべきログの明確化と収集	○	○	○
	認証ログの確認	○	○	○
-	データのバックアップ	○	○	○
-	対策状況の報告	○	○	○
外部サービスの利用	事業者の信頼性	○	○	○
	サービスの信頼性	○	○	○
	セキュリティ対策	○	○	○
	管理用インタフェースのセキュリティ対策	○	○	○
	基盤環境のセキュリティ対策	○	○	○
	サポート	○	○	○
評価	脆弱性診断	○	○	○

(2) 重要度低に該当する場合

機密性、完全性、可用性のいずれも重要度が低に該当する場合に必要となる対策を一覧で示す。

○：要実施

分類	要件	重要度低
サーバ基本設定	不要なサービスの停止	○
	外部公開が不要なポートの遮断	○
	システム情報の非表示	○
	公開不要なファイルの確認	○
	管理用インタフェースの制限	○
認証	認証の実施	○
	不要アカウントの削除	○
	パスワード規則	○
	認証時におけるメッセージ	○
	パスワードの保存	○
	アカウントロック	-
セッション管理	セッション ID の生成	○
	セッション ID の扱い	○
	Cookie の設定	○
	CSRF	○

分類	要件	重要度低
	セッション ID の破棄	○
セキュリティ実装	SQL インジェクション	○
	OS コマンド・インジェクション	○
	パス名パラメータの未チェック	○
	クロスサイト・スクリプティング	○
	HTTP ヘッダ・インジェクション	○
	メールヘッダ・インジェクション	○
	クリックジャッキング	○
	その他	○
通信の暗号化	HTTPS の使用	○
	SSL サーバ証明書	○
	SSL/TLS のバージョン	○
その他	マルウェア対策	-
	不正アクセス検知・防御	-
	WAF	-
	重要情報の暗号化	-
構成管理	使用している OS、ソフトウェアの管理	○
	脆弱性情報の取得	○
管理用アカウントの管理	アカウント共用の禁止	○
	不要アカウントの定期的な確認	○
	パスワードの管理	○
ログの監視	取得すべきログの明確化と収集	○
	認証ログの確認	○
-	データのバックアップ	○
-	対策状況の報告	○
外部サービスの利用	事業者の信頼性	○
	サービスの信頼性	○
	セキュリティ対策	○
	管理用インタフェースのセキュリティ対策	○
	基盤環境のセキュリティ対策	○
	サポート	○
評価	脆弱性診断	○

11. 用語の定義

本対策基準の用語の定義は次に定めるところによる。

【か】

●「機密性」

アクセスを認可された者だけが、情報にアクセスできることを確実にすること。

●「完全性」

情報および処理方法が正確であること及び完全であることを保護すること。

●「可用性」

認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

●「クロスサイト・スクリプティング」

Web アプリケーションの中には、検索キーワードの表示画面や個人情報登録時の確認画面、掲示板、Web のログ統計画面など、利用者からの入力内容や HTTP ヘッダの情報を処理し、Web ページとして出力するものがある。ここで、Web ページへの出力処理に問題がある場合、その Web ページスクリプト等を埋め込まれてしまう。この問題を「クロスサイト・スクリプティング攻撃」と呼ぶ。

●「クリックジャッキング」

Web サイトの中には、ログイン機能を設け、ログインしている利用者のみが使用可能な機能を提供しているものがある。該当する機能がマウス操作のみで使用可能な場合、細工された外部サイトを閲覧し操作することにより、利用者が誤操作し、意図しない機能を実行させられてしまう可能性がある。このような問題を悪用した攻撃を「クリックジャッキング攻撃」と呼ぶ。

【さ】

●「ソルト」

パスワードを暗号化する際に付与されるデータのこと。

●「セッション管理」

一般的な Web ブラウジングでは特に問題にはならないが、電子商取引サイトのように Web サーバにユーザがログインしてからログアウトするまで、ログイン情報を保持したままページを移管するには、このままでは問題がある。そこで、クライアントとサーバ間でその情報

を保持し、アクセス制御を一つの集合体として管理する仕組みが必要となる。この仕組みをセッション管理と呼ぶ。

●「セッション ID」
Web アプリケーションなどで、アクセス中のユーザの識別や行動の捕捉（セッション管理）のために付与される固有の識別情報。ユーザがアクセスしたりログインした際に発行され、一定時間アクセスが無かったりログアウトすると破棄される。

●「冗長化」
耐障害性を高めるためにネットワークを含むシステム全体を二重化して予備システムを準備すること。

●「死活監視」
コンピュータやシステムが動作しているかどうか外部から継続的に調べること。

【た】
●「ディレクトリ・トラバーサル」
Web アプリケーションの中には、外部からのパラメータに Web サーバ内のファイル名を直接指定しているものがある。このような Web アプリケーションでは、ファイル名指定の実装に問題がある場合、攻撃者に任意のファイルを指定され、Web アプリケーションが意図しない処理を行ってしまう可能性がある。このような問題を悪用した攻撃を「ディレクトリ・トラバーサル攻撃」と呼ぶ。

【は】
●「ハッシュ値」
「0」と「1」からなるデータを一定の法則で同じ長さに短縮した数値のこと。MD5 や SHA-1 などのハッシュ関数を使ってハッシュ値を求める。

●「フォールスポジティブ」
検出すべきイベントは検出するものの、余計なイベントまで検出してしまう誤診のこと。

●「パスワードリスト攻撃」
攻撃者が何らかの方法で事前に入手した ID とパスワードのリストを使用し、自動的に入力するプログラムなどを用いて、ログイン機能を持つインターネットサービスにログインを試みる攻撃手法のこと。

●「負荷分散」
同種の複数の機器やシステムの間で、負荷がなるべく均等になるように処理を分散して割り当てること。

【ま】
●「メールヘッダ・インジェクション」
Web アプリケーションの中には、利用者が入力した商品申し込みやアンケート等の内容を、特定のメールアドレスに送信する機能を持つものがある。一般に、このメールアドレスは固定で、Web アプリケーションの管理者以外の人は変更できないが、実装によっては、外部の利用者がこのメールアドレスを自由に指定できてしまう場合がある。このような問題を引き起こす脆弱性を「メールヘッダ・インジェクション」と呼ぶ。

●「マルウェア」
ボット、トロイの木馬、ワームなどの不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称である。

【わ】
●「ワンタイムパスワード」
本人認証手続きを行うごとに異なるパスワードを使い、二度と同じものを使わない方式。パスワードを生成するトークンやソフトウェアモジュールを使う。

【C】
●「Cookie」
HTTP プロトコルの通信において、Web サーバが Web クライアントに預けておくと、Web クライアントから Web サーバへ自動取得される小さなデータ。Cookie は、1 つの「名前=値」の対、およびいくつかの属性からなる。

●「CSRF（クロスサイト・リクエスト・フォージェリ）」
Web サイトにおいてログイン機能を設けているものがある。ここで、ログインした利用者からのリクエストについて、その利用者が意図したリクエストであるかどうかを識別する仕組みを持たない Web サイトは、外部サイトを経由した悪意のあるリクエストを受け入れてしまう場合がある。このような Web サイトにログインした利用者は、悪意のある人が用意した罠により、利用者が予期しない処理を実行されてしまう可能性がある。このような問題を悪用した攻撃を「CSRF 攻撃」と呼ぶ。

【H】

●「hidden パラメータ」
画面には表示されず、複数の Web ページ間でデータの受渡しを行う際に利用される HTML フォーム項目のこと。

●「HTTP ヘッダ・インジェクション」
Web アプリケーションの中には、リクエストに対して出力する HTTP のレスポンスヘッダのフィールド値を、外部から渡されるパラメータの値等を利用して動的に生成するものがある。このような Web アプリケーションで、HTTP レスポンスヘッダの出力処理に問題がある場合、攻撃者は、レスポンス内容に任意のヘッダフィールドを追加したり、任意のボディを作成したり、複数のレスポンスを作り出すような攻撃を仕掛ける場合がある。このような問題を悪用した攻撃を「HTTP ヘッダ・インジェクション攻撃」と呼ぶ。

【I】
●「IDS/IPS」
IDS はファイアウォールで防ぐことのできない不正プログラムの侵入や行為を発見する仕組みである。IPS は、管理者に検知内容を通知するのではなく、直ちにそのアクセスを禁止する。

【O】
●「OS コマンド・インジェクション」
Web アプリケーションによっては、外部からの攻撃により、Web サーバの OS コマンドを不正に実行されてしまう問題を持つものがある。このような問題を悪用した攻撃手法を、「OS コマンド・インジェクション攻撃」と呼ぶ。

【S】
●「SQL インジェクション」
データベースと連携した WEB アプリケーションの多くは、利用者からの入力情報を基に SQL 文を組み立てる。ここで、SQL 文の組み立て方法に問題がある場合、攻撃によってデータベースの不正利用を招く可能性がある。このような問題を悪用した攻撃を、「SQL インジェクション攻撃」と呼ぶ。

●「SSL サーバ証明書」
SSL 暗号通信時に利用する証明書である。電子証明書のひとつでサーバに対する印鑑証明書のような役割がある。

●「SSL/TLS」

セッション層に位置するセキュアプロトコルで、通信の暗号化、データ完全性の確保、サーバ（場合によりクライアント）の認証を行うことができる。区では TLS1.2 以上を推奨している。

●「SLA」

Service Level Agreement の略で、「サービス品質保証」の意味。サービスを提供する事業者が契約者に対し、サービスを保証する契約のこと。一般的な内容として、サービス内容と範囲、品質水準の明確化と、守られなかった場合のルールなどが含まれる。「サービスレベルアグリーメント」や「サービスレベル合意書」とも呼ばれる。

【W】

●「WAF」

Web アプリケーションの脆弱性を悪用した攻撃などから Web アプリケーションを保護するソフトウェア、またはハードウェアのこと。WAF は脆弱性を修正するといった Web アプリケーションの実装面での根本的な対策ではなく、攻撃による影響を低減する対策である。

以上