仕様書

１　件名

お客さま向けアンケートの作成・発送・回収・データ入力及び賞品発送等業務の委託

２　委託概要

株式会社ゆうちょ銀行（以下、「当行」という。）にて実施するお客さま応対に関するお客さま向けアンケート（以下、「アンケート」という。）について、当該アンケートの作成・発送、返送物（電磁的方法による回答結果を含む）、還付物に係る事務処理等を委託する。

３　委託期間等

契約締結日から2025年3月31日（月）まで

期間満了の3か月前までに株式会社ゆうちょ銀行お客さまサービス統括部（以下「主管担当」という。）又は受託者から解除の通知を行わないときは、期間満了の翌日から起算して1年間効力を有する。以後においても、2028年3月31日を限度としてまた同様とする。

なお、本件サービス提供開始日（予定）は、2024年8月とする。

４　委託内容

委託内容は次のとおり。

受託後速やかに、業務概要、体制図、業務フロー、スケジュール等を作成すること。

なお、詳細については、事前に主管担当の確認を受け確定させること。

おって、(5)、(6)、(10)の業務については、再委託禁止とし、同施設内で作業を完了させること。

(1) アンケートの作成・発送（店舗あて）

ア　店舗でお客さまに配布するアンケートはがき（料金受取人払）を作成し、1 店舗当たり 400 枚（200 枚×2 セット）を店舗あて発送すること。発送時期は主管担当の指示を受けること。

イ　用紙の規格は上質紙（ＮＩＰ対応用紙　メートル坪量１４３±３g/㎡相当）で両面とする。

ウ　アンケートはがきのレイアウト及び印字文言等については、主管部の指示を受けること。なお、文言の書体については、「みんなの文字」を使用すること。それ以外の書体を使用する場合は、事前に主管部の承認を得ること。

エ　用紙には、あらかじめ別途主管部が指示する文言、ロゴマーク、地紋、社印等の印刷加工を行うこと。この場合、刷色は表裏で8色以内とする。

オ　WebサイトのURLを格納したQRコード（リンク先へ遷移可能なもの）の印刷加工を行うこと。

(2) アンケートの作成・発送（顧客向け）

ア　半期に一度、当行から送付先のデータを媒体にて受領し、速やかに当該データの内容に基づき、圧着はがきを使用してアンケート発送状を作成し、圧着加工を施した上、普通郵便により顧客あて発送を行うこと。

イ　アンケート発送状等の作成にあたっては、以下の点に留意すること。

(ｱ) 1 年以内にアンケート発送状等を発送した顧客は除外すること。

(ｲ) Web サイトの URL を格納した QR コード（リンク先へ遷移可能なもの）の印刷加工を行うこと。

なお、URL は、アンケート発送状等の固有番号等を付与した可変のものとする。

ウ　アンケート発送状等の作成及び発送に当たっては、以下の検査を行うこと。

(ｱ) 印刷処理が正常に行われ、かつ、汚染及びき損のないこと。

(ｲ) 圧着処理が正常に行われていること。（圧着漏れ又は不良圧着がないこと）

(ｳ) アンケート発送状等の個々の生産履歴を追跡できるようにし、主管部の指示がある場合は全通数の作成漏れがないことを証明する資料を提出すること。

(ｴ)　アンケート発送状等の作成漏れ及び発送漏れがないこと。

エ　アンケート発送状等のレイアウト及び印字文言等については、主管部の指示を受けること。

なお、文言の書体については、「みんなの文字」を使用すること。それ以外の書体を使用する場合は、事前に主管部の承認を得ること。

オ　圧着はがき用紙は受託者において以下の要件を満たす用紙を準備すること。この場合、当該用紙の購入及び印刷加工等準備に要する一切の費用は受託者が負担すること。

(ｱ)　用紙の規格は感圧接着用紙（再剥離可能な特殊感圧接着剤を表裏全体に塗布した用紙）とし、原紙は上質紙（ＮＩＰ対応用紙）メートル坪量１４３±３g/㎡相当）で片面開封とする。

(ｲ)　圧着はがき内面に印字された内容が外側から容易に判読できないよう適切な措置を講じたものであること。なお、当該措置のために印刷する地紋等については、主管部の指示を受けること。

(ｳ)　用紙には、あらかじめ別途主管部が指示する文言、ロゴマーク、地紋、社印等の印刷加工を行うこと。この場合、刷色は表裏で8色以内とする。

カ　前記アにおける普通郵便物は、料金後納郵便（受託者において郵便料金を負担しない郵便物）として差出を行うことから、主管部が指示する手続に従って差出を行うこと。

キ　発送前の帳票について、局出し日の前日までに主管部より引き抜き指示があった場合、可能な限り対応すること。

ク　送付先のデータを格納した媒体の授受においては、セキュリティ便、もしくはそれに類するセキュリティを確保した便で行うこと。

(3) 返送アンケートの回収等

店舗で配付した(1)で作成した葉書と(2)で作成しお客さまに送付したアンケートを受け取るため、私書箱（当行から50km以内に設置すること。下記(11)エのとおり）を準備し、返送されたアンケートはがき(差出枚数の30%～50%程度を想定(1年間換算で55,920～93,200通））の回収を、セキュリティ対策を講じた方法にて行うこと。

また、アンケートはがきは料金受取人払いとし、料金受取人払いの費用は主管担当の負担として実績払いとすること。差出有効期間については主管担当から別途指示する。料金受取人払いに必要な手続きは受託者が行うこと。

なお、私書箱の設置及び料金受取人払いの手続きは、アンケートはがきの版内容確定に間に合うよう、主管担当と相談の上、速やかに行うこと。

(4) アンケート回答用 WEB サイトの作成

アンケート回答用 WEB サイトを作成すること。WEB サイトのアンケート内容は、4(2)で指示するレイアウト及び印字文言等と連動し、同一の項目の回答が得られるように作成すること。文言・レイアウトについては、予め主管部の承認を得ること。

なお、WEB サイトのブラウザ要件は以下を満たすこと。

【ブラウザ要件】

2024 年 4 月時点において以下ブラウザにて閲覧可能であることが検証されていること。

[PC]Windows: Microsoft Edge／Firefox／Google Chrome／Safari の各最新版

[SP（スマートフォンページ）] iPhone iOS17 Safari／Android 12×Chrome／Android 13×Chrome

また、WEB サイトのアンケートページは、4（2）で発送するはがきから回答する顧客については、どの顧客からの回答かが分かるように、URL を顧客ごとにユニークに設定すること。

4（1）で作成したはがきで回答する顧客については、景品を送付するための住所・氏名を記載する欄を設けること。

(5) アンケート回答用WEBサイトによる回答データの取得等

アンケート回答用WEBサイトから、アンケート回答データ（４(2)で返送されたアンケートの5%～30%程度（見込））を主管担当と協議して定めたスケジュールでダウンロードすること。

(6) アンケート回答に係るデータ入力等

４(3)で返送されたアンケート結果（選択方式とフリーワード形式の2種類）をデータ入力するとともに、アンケートはがきの発送時の情報を入力したデータ（以下、「発送マスタ」という）と、入力データとを紐付けること（発送マスタと、入力データとを紐づけしたデータを「納

品データ」という）。納品データの正当性は必ず２名以上でベリファイ作業を行うことにより担保すること。

WEB 回答データの取扱いを行う作業施設内は、入退室を IC カード、生体認証等で行い、セキュリティを確保すること。作業エリア毎に入退者のログを管理し、個人情報流出等のトラブルが発生した場合は、速やかに主管担当宛に連絡し、記録を提出すること。

データ入力結果（納品データ）については、主管担当あて納品すること。納品にあたってはセキュリティ対策を講じた方法で、５に定める期限で納品すること。アンケート回答用WEBサイトの回答データは、当該クラウドサービス上に1ヶ月間保管すること。

(7) データの分類等

４(6)で入力されたフリーワードのデータを、大項目(4～5項目程度)と小項目(20項目程度)等で分類すること。

(8) 納品データ作成等

アンケートデータの納品にあたっては、紙のアンケート入力データ、WEBアンケート回答データ及び発送データを突合させた上でアンケート返送者情報を特定し、納品データに含めること。

なお、紙とWEBの回答者の重複チェックを行う。納品データの項目及び数の詳細に関しては、主管担当と協議の上決定するものとする。

納品データは、下記アからオを納品すること。

ア. 発送マスター一覧に対し期限内の紙及びWEB回答者のデーター一覧
イ. 発送マスター一覧に対し期限外の紙及びWEB回答者のデーター一覧
ウ. 抽選対象者一覧
エ. 発送マスタと紙及びWEBの回答者とのアンマッチ用データー一覧
オ. 発送マスター一覧を問わず、一定期限の間に受け付けた紙及びWeb回答者のデーター一覧

(9) 還付対応

当行から発送するアンケートはがきに関し、還付された郵便物は、印字されたQRコードを読取り、４(4)にて連携する発送データと紐付けた上で、住所、氏名について還付一覧表を作成し、４(8)の納品データとともに主管担当あて納品すること。納品にあたってはセキュリティ対策を講じた方法とすること。

(10) 抽選業務

返送されたアンケートはがきを対象に厳正な抽選作業を行うこと。

抽選対象者は、4(8)においてアンケートはがきの回答入力データ、WEBアンケート回答データを突合して抽出し、抽選作業を実施すること。抽選作業実施後、当選順位に並びかえた顧客一覧データを作成し、主管担当に納品すること。当選順位は全件に付与すること。

抽選の具体的な方法等については、主管担当と事前に調整し、抽選フロー等に係る計画書等を主管担当に提出し承認を得ること。

(11) 賞品発送に係るあいさつ状等の制作及び発送等

次のとおり、宛名台紙、あいさつ状及び洋封筒のデザイン制作、印刷を行うこと。デザインについては、主管担当と協議のうえ決定すること。なお、ロゴマーク等を表示する場合には、必要な素材を主管担当から提供する。宛名台紙、あいさつ状および洋封筒の仕様等は以下のとおり。

なお、下記の数量とは別に 10 部を主管担当に提出すること。

また、賞品は 500 円分の QUO カードとし、本契約に含めるものとする。QUO カードの選定については主管担当と協議の上決定すること。枚数は 1 回あたり 20 枚、全 40 枚（予定）とする。

印刷物	サイズ	材質等	印刷	数量（予定）※1
宛名台紙兼あいさつ状	展開サイズ：A4 仕上りサイズ： 210 ㎜×100 ㎜程度	上質紙 (81.4g/m^2)	片面 4 色 (CMYK)	各 40 枚

商品発送用 封筒	230㎜×120㎜＋35㎜程度 （横×縦＋ベロ） 窓1箇所あり ※2	上質紙 （127.9g/㎡）	表4 （CMYK） 裏1色(地紋)	各50枚 （予備込）
QUOカード封入用小封筒	95㎜×65㎜×30㎜程度 （横×縦＋ベロ）	上質紙 （127.9ｇ/㎡）	片面4色	各50枚 （予備込）

※1　数量の増減幅については、増は30%、減は20%を限度とする。
※2　透かし窓　ポリスチレンフィルム　厚さ0.03㎜　グラシン紙（メートル坪量３５g/㎡）

ア　発送先の印字作業

４（10）で抽選した当選者の氏名・郵便番号・住所等の必要情報（以下、「宛先情報データ」という。）を宛名台紙に印字すること。印字には「みんなの文字」を使用することとし、宛先情報データは外部メール受信可能な端末、インターネットに接続可能なシステム、クラウドサービス等で取り扱わないこと。

交付する宛先情報データの住所・氏名に外字フォントが含まれている場合は、当行の外字フォントを電子記録媒体（CD-R（予定））にて交付するので、外字フォントを登録すること。外字フォントについても「みんなの文字」を使用することとし、文字コードとの対応は対応表に基づき実施すること。登録外外字が含まれている場合は、別途主管担当と協議の上、対応方法を決定すること。

また、宛先情報データの印字前に主管担当あてテスト印字結果を提出し、その承認を受けること。

イ　賞品の封入・封緘

次の内容を1セットとして、洋封筒（項番4（11）で制作したもの）に封入・封緘し、1回あたり20セット、合計40セット（予定）の発送物を用意すること。

封入作業を行う場合は金券を取り扱う為、特別室を設け、作業者の出入りを制限し、個人の特定が可能な入退室記録を残すこと（手書き禁止）。トラブルが発生した場合は、主管担当の指示に応じて記録を提出する事。

封入作業状況については映像で記録し、トラブルが発生した場合等、工場へ主管担当が往訪した際、映像記録の確認を可能とすること。また、封入物の入り数の機械的保証（記録）を行うこと（手書き禁止）。トラブルが発生した場合は、主管担当の指示に応じて記録を提出すること。

セット内容は以下のとおり。

品名	数量	セット(予定)
宛名台紙兼あいさつ状	1枚	40セット
QUOカード（小封筒入り）	1枚	

※ 数量の増減幅については、増は30%、減は20%を限度とする。

ウ　賞品の発送

前項イにて封入・封緘した発送物を、任意の郵便局に普通郵便を利用して差出を行うこと。発送費は全て委託費に含めるものとする。

エ　私書箱の設置および回収

東京都内1か所（当行から50km以内）に本賞品発送用の私書箱を設置すること。設置にあたりかかる費用は受託者負担とする。

私書箱に還付された発送物の回収を、セキュリティ対策を講じた方法にて行うこと。毎日（土・日・祝日以外）回収を行い、還付枚数について回収日毎に件数を記録することとし、回収記録について一覧にした表を主管担当あて月1回報告すること。なお、回収は委託期間の最終日まで行うこと。また、各月ごとに還付された賞品の管理番号等を一覧にした還付状況一覧表を作成し、翌月主管担当あて提出すること。なお、還付状況一覧表の様

式については、事前に主管担当の了解を得ること。

５　納入成果物、納入期限（履行期限）等

	提出物	形式	数量	提出期限
1	事務局運営マニュアル	紙（様式適宜）	1部	2024年7月19日（金）
2	版下データ （はがき、当せん者向けあいさつ状、および洋封筒）	CD-R （ｲﾗｽﾄﾚｰﾀ、PDF）	1式	2024年7月19日（金）
3	アンケートはがき	紙	4（1）のとおり	2024年7月31日（水）
3	アンケート結果(直営店別) アンケート結果(顧客別) 還付状況一覧 抽選結果	データ ※データ形式等については、主管担当の了承を得ること。	各1部	年に2回とする。 具体的な期限は主管担当の指示による
4	廃棄証明書 データ廃棄証明書	様式適宜	各1部	廃棄証明書は年2回 2025年3月31日（月） ※自動更新した場合は、自動更新期間の最終日とする。
5	事務局運営報告書	様式適宜	1部	2025年3月31日（月） ※自動更新した場合は、自動更新期間の最終日とする。

６　データ等の廃棄

返送物、還付物は１か月間保管し、保管終了後、「焼却」、「溶解」等により、復元不可能な状態としたうえで廃棄すること。廃棄の都度、廃棄証明書を提出すること。

また、委託期間終了後、本件業務において使用した全ての保有データ（バックアップ等を含む。）を消去及びドキュメントの廃棄を実施し、データ廃棄証明書を提出すること。

７　作業上の注意事項

(1) 作業上のスケジュール等は、主管担当と緊密に連絡を取りながら設定すること。

(2) 作業の進捗状況等については、作業の責任者が常に把握し、作業遅延が発生した際は、速やかに発生状況・原因・処理状況等を主管担当に報告すること。

(3) インターネットに接続するシステムを使用する場合、次に掲げる事項が整備等されていること。

① 通信を監視し、不審な通信を検知・遮断する機器等が整備されていること

② セキュリティ診断を実施していること（※１）

③ 不正アクセス等による被害発生時の対処フローが整備されていること

④ クラウドサービス等他社とリソースを共有する場合、他社システムへのサイバー攻撃が当該システムに与えるリスクを認識していること（※２）

※１　受託者において新たなシステムを構築する場合は、新たなシステムによるサービス開始前にセキュリティ診断を実施することとし、診断項目についてあらかじめ主管担当の確認を受けるとともに、診断結果を主管担当に提出し承認を受けること。

※２　受託者において新たなシステムを構築する場合で、クラウドサービス等他社とリソースを共有する場合、他社システムへのサイバー攻撃が当該システムに与えるリス

クを明確化すること。

８　著作権の帰属等

⑴　受託者は、本契約の履行過程で生じた成果物に対し、著作権法第27条及び第28条に定める権利を含むすべての著作権を当行に譲渡し、当行が独占的に使用する。

なお、受託者は当行に対し、一切の著作者人格権を行使しないこととし、また、第三者をして行使させないものとする。

おって、受託者が、本契約の成果物に係る著作権を自ら行使しまたは第三者をして使用させる場合は、当行と別途協議するものとする。

⑵　成果物に、第三者が権利を有する著作権が含まれる場合は、当行が特に使用を指示した場合を除き、受託者が当該著作権の目的たる著作物の使用に必要な費用の負担および使用許諾契約の締結その他の第三者による使用許諾に係る一切の手続を行うこと。

なお、この場合、受託者は当該使用許諾の内容について事前に書面にて提出し、主管担当の承認を得ることとし、当行は当該著作物について当該使用許諾の範囲内で使用するものとする。

⑶　本仕様書に基づく作業に関し、第三者との間に著作権に係る権利侵害の紛争等が生じた場合は、当該紛争等の原因が専ら当行の責めに帰す場合を除き、受託者の責任、負担において一切を処理すること。

なお、この場合、当行はかかる紛争等の事実を知ったときは、受託者に通知し、必要な範囲で訴訟上の防衛を受託者に委ねる等の協力措置を講じるものとする。

９　その他

⑴ 交付した資料等は、作業を終了した後速やかに主管担当へ返却すること。また、製造過程で発生した予備等の成果物については、速やかに断裁処理等を施し再利用できないことを確認の上、適正に廃棄すること。なお、加工等の工程を第三者に再委託する場合も同様に処理すること。

⑵ 個人情報の取扱いを再委託する場合（再委託以降、全てを含む。）には、主管担当に事前報告すること。

⑶ 本契約の内容および解釈等について疑義が生じた場合は主管担当（TEL：03-3477-1659）あてに連絡すること。

⑷ 本契約の履行に従事する貴社労働者に対する作業指示、労務管理、安全衛生管理等に関する指揮命令は、すべて受託者の責任においておこなうこと。また本契約の履行に従事する貴社労働者に対する作業指示は、作業責任者を配置し、作業責任者を通じて行うこと。

⑸ 緊急時において本契約を履行するためのコンティンジェンシープランを策定すること。

⑹ 契約変更が必要と認められる事情が発生した場合は、受託者に契約変更の申し入れすることができること、それを受けて受託者は誠実に対応すること。

⑺ 委託情報の安全管理のため、従業者に対する必要かつ適切な監督を行うこと。

⑻ 本仕様書における疑義については、主管担当の指示及び解釈によること。

⑼ 受託者は、履行終了後速やかに完了届・報告書・納品書等（様式適宜）を主管担当に提出し、請求書発行依頼が到着後、請求書を主管担当に提出すること。

⑽ 本契約の履行に従事する受託者の労働者に対し、公益通報者保護法に係る当行の通報窓口について当行指定の周知文を受領したことを確認の上、当該周知文を用いて周知に努めること。

⑾ 履行終了後も委託情報は他に漏らさないこと。

⑿ クラウド利用に当たっては、以下の内容を遵守し、主管担当の承認を得ること。

① データの入力・保管・処理・バックアップ・出力について、取扱者を限定すること。権限のない者が情報を閲覧等できないこと。

② クラウド提供事業者がデータにアクセスできないこと。またそれをサービス約款・契約書などで確認できること。

③ クラウド環境の暗号化の強度を十分に行い、暗号化漏れがないこと。

④ 情報漏えい等の不正行為が発生し得る操作については、ログが取得されること。不正行

為が発覚した場合等は、速やかに主管担当まで連絡し、ログを開示すること。なお、ログについては保存期間が十分であること。

⑤　バックアップを含むデータコピーの取得内容・保管場所・保管期間について、取扱者を限定していること。権限のない者が情報を閲覧等できないこと。保存期間が十分であること。

⑥　アクセス権限設定の仕様変更をする場合や、金融機関等による設定の変更時には、事前に主管担当まで連絡し合意を取ること。

(13) 社外からのメールが受信できる端末を使用する場合は、以下の内容を遵守すること。

①　通信を監視し、不審なメール等を検知・遮断する機能を整備すること。なお、当該内容については、当行（主管担当）の承認を得ること

②　侵入されることを前提とした被害発生時の対処フローを整備し、当行（主管担当）の承認を得ること

③　電子メールの運用にあたっては、信頼性、安全性を確保するため、その運用方針を明確にすること

④　業務目的以外の電子メールの送受信、ホームページの閲覧等に対処するため、不正使用防止対策が講じられていること

(14) インターネットに接続するシステムを使用する場合は、以下の内容を遵守すること。

① 通信を監視し、不審な通信を検知・遮断する機器等を整備すること。
なお、当該内容については、当行（主管担当）の承認を得ること

② 不正アクセス等を検知、監視する体制及び被害発生時の対処フローを整備し、当行（主管担当）の承認を得ること

③ クラウドサービス契約のように他社とリソースを共有する場合、他社のシステムへのサイバー攻撃が、当該システムに与えるリスクを明確にし、当行（主管担当）の承認を得ること

④ 不正アクセスによるコンピュータシステムへの侵入を防ぐため、外部からアクセス可能な通信経路、通信関連機器等は最小限とし、ネットワーク構成情報を適切に管理しているか。また、外部ネットワークからアクセス可能な機器へのセキュリティパッチの適用やファイアウォールにおける不要なポートの閉塞等の対応を実施し、感染を防止すること。

(15) データセンターはFISC安全対策基準に準拠していること。また、契約後に準拠状況を確認できること。

(16) 本件業務における利用データ・システムサーバの所在地、および作業者・アクセス者（クラウドサービスの提供・保守業者を含む）の所在地については、日本国内に限る。

１０　サイバーセキュリティ対策等

受託者は、本件業務を履行するためにシステムを利用する場合は、以下の事項について了知・厳守すること。

(1) クラウドサービスのアクセス権限設定に関する仕様変更や変更時には、当行所管部あて事前に通知すること。

(2) クラウドサービスのアクセス権限設定の仕様変更や変更時には、設定内容の妥当性を確認すること。

(3) 端末機における漏洩防止策として、暗証番号・パスワード等は、他人に知られないように、非表示、非印字、記号などへの置換え、覗き見防止等の対策を講ずること。
また、媒体上に暗証番号・パスワード等をそのまま記憶させない等の対策を講ずること。

(4) 機密・厳秘情報をシステム内（端末やバックアップ等も含む）に蓄積する際には、ファイルの不正コピーや盗難の際にもデータの内容がわからないようにするため、CRYPTRECに準拠した暗号アルゴリズムを用いて暗号化すること。

(5) システム管理端末について、電子記録媒体差込口の制御（システムによる規制、デバイス制御ソフトの導入、差込口の施錠管理）を行うこと。

(6) システム処理中に重要なデータを含む一時データファイルが生成される場合、重要なデータの漏洩を防止するため、利用状況に応じ不要となった時点で消去する機能を設けること。

(7) メール送付を含む機密・厳秘情報を伝送する場合には、CRYPTRECに準拠した暗号アルゴリズ

ムを用いて暗号化（TLS1.2以上）すること。
(8) 故意または過失によるファイルの破損、または不正アクセスからデータを保護するため、重要なファイルについては、ソフトウェアによるアクセス制御機能を設けること。
(9) ファイルに対するアクセス制御のため、ファイアウォール・統合脅威管理等でネットワークによるアクセス制御を行うこと。
(10) コンピュータシステムの不正使用及びネットワーク拡大による種々の端末を使用した不特定多数の者からの不正アクセスを防止するため、正当な権限を保有した本人であるか、もしくは正しい端末に接続されているかなど、接続相手先の正当性を確認すること。
(11) システム、データへのアクセス権を不正使用される危険性を考慮し、IDや暗証番号等の不正使用を防止するため、システムにログオンしたまま一定時間操作が行われない場合のセッションタイムアウト機能もしくは端末のスクリーンロック機能を有すること。
(12) アクセス履歴を取得し監査証跡として1年間保管すること。
正当なアクセス権を有する者の顧客情報の不正持ち出しを発見できるようにするため、顧客情報を閲覧した履歴（ＩＤ、日時、操作内容、件数等）を記録すること。
(13) ①以下の種類のログを取得すること。
・ログインとログオフ状況(指示端末、時刻、ID、回線種別、使用したシステムもしくはデータ、行った処理)
・不正なアクセス要求(指示端末、時刻、ID)
・システムによって失効とされたID
・システムにログインしたまま一定時間操作が行われないために、強制的にログオフされたID
・特権IDの利用履歴（成功時及び失敗時）
・印刷ログ
・厳秘、機密情報の取得（DL含む）および持出した記録
②アクセス記録を定期的にチェックしてサービス利用者が正当なアクセスなのかどうかを調査すること。
(14) 監査証跡に基づいて、許可されていないアクセスの分析、報告を可能とすること。
(15) 監査証跡、オペレーション記録、運転記録等は、改ざん及び不正アクセスを防ぐために、正当なアクセス権限者以外のものから以下のいずれかの方法により適切に保護すること。
・暗号化して保管する。
・ 書換え不能メディアに記録し、保護された場所に保管する。
・ネットワーク経由の不正アクセスや改ざんを防止するために、オフライン媒体に記録する。
(16) ①電子化された共通鍵、秘密鍵を蓄積するICカード等の機器、媒体あるいはそれに含まれるソフトウェアには、共通鍵、秘密鍵を保護する機能を具備すること。
②パソコン等を利用する場合においては、共通鍵、秘密鍵は別の機器及び媒体に確保し、必要時にその機器、媒体を接続して使用すること。
(17) 共通鍵、秘密鍵をパソコン等の端末機器側に蓄積する場合は、他人に解読されないような措置を講ずること。
(18) 外部ネットワークと接続する場合は、接続部分の不正侵入防止のため、入口対策を講ずること。
(19) 侵入したウイルスの検知、バックドアの構築防止、機密情報の流出防止等を目的とした出口対策(通信ログ、イベントログ等の分析による、不適切な通信の検知・遮断、DLP (Data Loss Prevention) 等)を講ずること。
(20) 外部ネットワークからの不正侵入の防止と早期発見のため、内部ネットワークへのアクセスを監視し、アクセス履歴のチェックを行うこと。
(21) 外部ネットワークからのアクセス経路は、不正アクセスを防止するため、ファイアウォール等で不要なポートを閉塞する等必要最小限にするとともに、ネットワーク構成情報を適切に管理すること。
(22) 基本ソフトウェアの脆弱性を最小限にするため、使用しない機能は停止、あるいは使用を制限すること。また、使用予定のないソフトウェアは搭載しないこと。
(23) アクセスの失敗及び不正アクセスを監視する機能を設けること。アクセスの失敗を記録す

る機能を設け、また、連続した何回かのアクセスの失敗に対しては、強制終了・取引禁止等を行う機能を設けること。

(24) 不正アクセスの拡大防止のための対応策、復旧策を明確にすること。

(25) パスワード等については、以下の通り推測されにくいものを設定するようシステム的に制御すること。

ア　英大文字／英小文字／数字／記号のうち最低3つを組み合わせること

イ　8桁以上とすること

(26) 初期設定されるパスワード等については、システム的に初回ログイン時のパスワード変更を強制すること。

(27) データファイルのバックアップを取得し、その保管管理方法を明確にすること。

(28) 業務継続上重要なデータについては、定期的なバックアップを実施し、本番環境から切り離した環境に保管する等ランサムウェア感染を考慮したバックアップを実施すること。

(29) 端末へのアプリケーションのインストール制限を行うツール等を活用し、端末への未許可のアプリケーションのインストールを制限すること。

(30) システム管理端末について、業務目的以外の電子メールの送受信、ホームページの閲覧等に対処するため、当該機能をシステム的に利用不可とする、またはホワイトリストで制限する等の不正使用防止対策を講ずること。

(31) メールサーバまたはメール送信機能を新たに構築（利用）する場合、送信のみで受信は不可とすること。

(32) ア　受託者は、本調達で構築するシステムがセキュリティ要件を満たしている事について、原則、別紙1に記載する要件を満たす第三者によるセキュリティ診断（WEBアプリケーション診断、ネットワーク診断等）を実施し、実施結果（修正対処後の再診断含む）をサービス開始前までに主管担当に報告し、承認を得ること。

イ　セキュリティ診断の実施にあたっては、システムの仕様に応じ必要な診断項目や検証パターン数、実施方法等が異なるため、リクエスト数やデータフロー等の仕様が確定した後、診断の項目及び実施方法について主管担当に説明し、承認を得ること。診断の項目については別紙2を満たすこと。

ウ　セキュリティ診断において重大な脆弱性が判明した場合、または、主管担当が問題と認識した場合は、原則サービス開始前に修正及び再診断を実施し、当該脆弱性が解消されたことを示す再診断結果等を主管担当に報告し、承認を得ること。

エ　セキュリティ診断は、サービス開始前に加え、最低１年に１回程度定期的に実施し、機能追加等の変更が行われた際にも当該機能のサービス開始前までに診断及び必要に応じた修正を実施すること。

オ　当行の責任範囲においては、上記のとおりセキュリティ診断を実施すること。

カ　クラウド（ASP）業者の責任範囲においては、当行のためにセキュリティ診断を実施できない場合、報告書等（別紙3）によりセキュリティ診断の実施を主管担当へ報告すること。報告書等の提出が難しい場合は、セキュリティ診断実施と同等のセキュリティを担保していることを証明する書類（SOC2レポート、PCIDSS準拠証明書等）を主管担当に提出することにより、代替を可とする。

(33)ア　当行の資産としてファイアウォール（同機能を持つ統合脅威管理等も含む）を設置した際は、実際のファイアウォールの設定値(コンフィギュレーションリスト・アクセスコントロールリスト等)が設計書(設定値を記載したドキュメント)どおりになっていることを定期的(四半期ごと)に検証し、前年度の結果を取りまとめて年に一度、4月末までに報告すること。また、当行用のファイアウォールの設定値もしくは設計書を修正した際は、その都度、当行に修正内容を報告すること。

イ　当行の資産でないファイアウォール（同機能を持つ統合脅威管理等も含む）を設置した際は、当行へのサービス提供にあたり、サービス利用時に経由する通信経路上にあるファイアウォールについて、受託者は設計書どおりに設定されていることを定期的(年1回以上)に確認し、証跡もしくは報告書等（別紙3）により確認結果を当行へ報告すること。報告書等の提出が難しい場合は、当行が求めるセキュリティ水準と同等のセキュリティを担保していることを証明する書類（SOC2レポート、PCIDSS準拠証明書等）を主管担当に提出

することにより、代替を可とする。

(34)ア　アカウントロック等を検知した場合、当該ログを取得し、１年間保管すること

イ　各サーバにおいて、特権ID（OS及びDBの管理者権限（root/admin等権限））の使用履歴（成功時及び失敗時）を取得し、１年間保管すること。

ウ　各サーバまたは認証ログを管理するサーバにおいて、アクセスログを取得し、１年間保管すること。

エ　特権IDを使用した日時について、リアルタイムまたは、日次～週次で不審な使用がないか作業記録等と突合して確認し、所管部署へ四半期に一度以上の頻度で報告すること。

オ　アカウントロック等のログについて、リアルタイムまたは、日次～週次で、大量の検知等、不審な点が無いかを確認し、所管部署へ四半期に一度以上の頻度で報告すること。

(35)　保守運用員、当行社員、顧客によるシステムへのアクセスにおいて、認証に一定回数失敗した場合のアカウントロック機能を実装すること。

(36) ア　ウイルス対策ソフトを導入すること。

イ　ウイルス対策ソフトのパターンファイルのリリース情報を定期的に収集し、更新すること。

ウ　ウイルス対策ソフト（本体およびパターンファイル）の適用状況を製品ホームページ等と比較し、最新化されている事を確認し、確認結果を台帳に記録すること。

エ　パターンファイルの更新頻度及び台帳更新頻度は、ウイルス対策ソフトの更新方法（自動／手動）によって、以下の①、②以上の頻度で対応すること。

①　自動の場合

【更新頻度】サーバ・端末：日次/随時

【台帳更新】サーバ・端末：月次

②　手動の場合

【更新頻度】サーバ・端末：月次

【台帳更新】サーバ・端末：更新の都度

オ　主管担当より上記の管理台帳について提出の依頼があった場合、受託者は速やかに管理台帳を提出、若しくは上記について適切に実施していることを示す証明書等の提出を行うこと。証明書等を提出する場合は、当行所定の様式に従うこと。

(37) ア　システムの構成要素（当行提供サービスに使用するOSやWEBアプリケーション等）の製品名、バージョン、サポート期限（EOL。製品提供元のサポート等提供期限）について、管理台帳を作成し、最新の状態となるようEOL情報の取得及び台帳の都度更新を行うとともに、最低年次で更新漏れがないこと、及び、原則としてEOL到来製品の使用がないことを確認すること（原則、契約期間中を通じて保守サービスの提供される製品を使用すること。ただし、やむを得ない事由により継続使用する場合は、継続使用によるリスクも考慮の上、受託者社内基準に従い継続して利用できることの判断が責任者によりされていること）。

イ　当行主管部より上記の管理台帳について提出の依頼があった場合、受託者は速やかに管理台帳を提出、若しくはEOL管理作業について適切に実施していることを示す証明書等の提出を行うこと。証明書等を提出する場合は、当行所定の様式に従うこと。

(38)　ア　資産管理及び脆弱性管理を行うために、システムの構成要素（当行提供サービスに使用するOSやWEBアプリケーション等）を網羅的に把握し、脆弱性情報の収集及びセキュリティパッチファイルの取得を継続的に行うこと。

イ　取得したセキュリティパッチファイル及びパッチ適用状況等を管理台帳等で管理し、定期的な更新（月次）を行い、主管部に報告を行うこと。

ウ　当行主管部より上記の管理台帳について提出の依頼があった場合、受託者は速やかに管理台帳を提出、若しくはセキュリティパッチ管理作業について適切に実施していることを示す証明書等の提出を行うこと。証明書等を提出する場合は、当行所定の様式に従うこと。

エ　当行からの脆弱性管理に関する問い合わせに応じること。

(39)　ア　受託者は、当行資産として導入する機器・ソフトウェアがある場合、主管担当より別途提示するフォーマットに従い、サービスインの3か月前を目途に、該当機器のIT資産情報を記入し、提出すること。具体的な提出時期は、主管担当の指示に従うこと。なお、

別途提示するフォーマットのイメージは別紙4のとおり。

イ　受託者は、上記で提出した資料について、主管担当からの指示に従い、適宜記載内容の修正を行うこと。また、サービスイン後に機器変更、若しくは使用するソフトウェアの変更等、IT資産情報に変更が生じる場合は、速やかに主管担当に報告するとともに、別途提示するフォーマットに記入し、提出すること。

(40) アンケート回答用WEBサイトのドメインは、主管担当が指定するものを使用すること。それが難しい場合は、以下の要件を満たすこと。

ア　ドメイン情報の設定変更に用いるアカウント（ＤＮＳサーバのアカウント）は、アカウントの不正利用によるデータ改ざん防止のため、厳格に管理・運用すること。

具体的な対策例は、以下のとおり。

・不正アクセス防止のため、ＤＮＳサーバへのログイン、もしくは設定変更を行う管理画面等へのログイン時に、ＩＤ･パスワード等による利用者認証を行うこと。

・パスワードは、推測されやすいパスワードを設定しないこと、パスワード等を他人に知られないようにすること、パスワード等を共用しないこと等の措置を講じること。

・パスワードの入力を一定回数失敗した場合は、当該ＩＤを一時的に使用不可とする機能を備えること。

イ　ＤＮＳ改ざん検知を行うこと。また、誤りを検知した場合は速やかに修正すること。

具体的な実施例は、以下のとおり。

・リソースレコードに誤りがないか、定期的にゾーンファイル内の設定を確認すること。

ウ　サービス利用終了の際には、主管部の指示に従い不要となったＤＮＳ設定を削除すること。また、主管部から確認依頼を受けた場合は、適切に削除した旨を、主管部宛てに報告すること。

エ　ＤＮＳサーバに対するサービス運用妨害攻撃（ＤｏＳ攻撃）係る対応を行うこと。

オ　ドメイン情報に係るデータ改ざん（ＤＮＳ改ざん）に係る対応を行うこと。

カ　レジストラ使用がある場合、悪意のある第三者による改ざんを防止するため、レジストラサービス利用時の認証に多要素認証を用いること、もしくは、悪意のある第三者がレジストラに対してドメイン登録情報の変更申請を行った際に、検知可能とする等の対策を講じること。

キ　ＣＤＮ（Ｃｏｎｔｅｎｔ　Ｄｅｌｉｖｅｒｙ　Ｎｅｔｗｏｒｋ）を使用する場合は、ドメインフロンティング対策を講じること。

	診断実施企業の条件
1	自社のセキュリティ診断サービスが、経済産業省が定める「情報セキュリティサービス基準」に適合するサービスとして、独立行政法人情報処理推進機構（IPA）の「情報セキュリティサービス基準適合サービスリスト」におけるサービス分野「脆弱性診断サービス」のリストに登録されていること。
2	過去３年間で当行以外の異なる３銀行に対し、仕様書記載のセキュリティ診断項目を含むセキュリティ診断の実績を有すること。
3	セキュリティ診断サービス提供年数を３年以上有すること。
4	セキュリティ診断作業実施者は脆弱性診断に関する業務経験を３年以上有すること。
5	セキュリティ診断作業実施者には以下の資格のいずれかもしくは、同等以上の知識・技術を保有している者が１名以上含まれること。 ・情報システムセキュリティプロフェッショナル認定資格（CISSP） ・情報処理安全確保支援士（登録セキスペ）
6	セキュリティ診断管理責任者は、プロジェクト管理経験を５年以上有すること。 （管理責任者の前職において経験がある場合は、それを含めた経験年数としてよい。）
7	セキュリティ診断員が１０名以上在籍していること。
8	情報保護資格（「プライバシーマーク」または「ISO27001」）を取得していること。
9	社内で情報（取引先情報を含む）管理に関するルールが定められ、社員に対する指導も十分に行われていること。

別紙２

セキュリティ診断実施内容

1　診断方法

(1) 委託事業者は診断等実施に際し、ツールによる自動的・画一的な診断に加え、作業実施者の手動による診断やペネトレーションテストなどを実施し、それぞれについて報告を行うこと。

(2) 委託事業者による診断は、項番 3 に示す診断項目を満たすこと。項番 3 を満たすことができない場合は、主管部と委託事業者間で相談すること。また、委託事業者は診断前にはシステムが提供する機能や目的等を主管部に確認し、以下のセキュリティ検証標準等も参考に、システムの特性に沿った診断を行うこと。

【参考】セキュリティ検証標準

① Web アプリケーション診断

OWASP アプリケーションセキュリティ検証標準（ASVS）

セキュリティ検証レベル	説明	例
ASVS レベル 1	全てのアプリケーションが満たすべきものです。	一般的なご案内のみ閲覧可能な web サイト
ASVS レベル 2	機微なデータを扱うアプリケーションが満たすべきものです。	個人情報が閲覧可能な web サイト
ASVS レベル 3	極めて重要なアプリケーションが満たすべきものです。高額取引を行うアプリケーション、機密性の高い医療データを持つアプリケーション、最高レベルの信頼性を必要とするアプリケーションのためのものです。	個人情報の閲覧に加え、資金移動や原簿の更新が可能な web サイト

② スマートフォンアプリケーション診断

OWASP モバイルアプリケーションセキュリティ検証標準(MASVS)

検証レベル	説明	例
MASVS-L1	一般的なセキュリティ要件であり、すべてのモバイルアプリに推奨されます。	一般的なご案内のみ閲覧可能なアプリ
MASVS-L2	機密性の高いデータを扱うモバイルアプリに適用します。	モバイルバンキングアプリ
MASVS-R（※）	追加の保護コントロールを対象としています。クライアント側の脅威を防止することが設計の目標である場合に適用できます。	オンラインゲームアプリ

※　アプリの特性により、MASVS-L1 や MASVS-L2 に追加（MASVS-L1+R、MASVS-L2+R）で求めるもの

(3) 委託事業者が診断にツールを使用する場合は、名称および使用目的を事前に開示すること。

(4) 原則、本番環境に対して診断を実施すること。ただし、システム停止等、サービスに影響がある場合などは、本番環境と同等の開発環境または災害対策環境で実施するため、診断環境については、主管部と委託事業者間で調整のうえ実施すること。

2　各種診断

(1) ネットワーク診断

ア　IP アドレスまたは FQDN 単位で診断を実施すること。詳細は主管部より提示する。

イ　ロードバランサの背後に同一構成のサーバが複数ある場合は、同一構成のサーバのうち 1IP、または VIP(Virtual IP)のみ診断を実施すること。

ウ　グローバル IP に対しては、インターネット（リモート）から診断を実施すること。

【参考】診断対象 IP アドレスの考え方

①　インターネット接続システム

インターネットから接続可能なグローバル IP アドレスに対して実施すること。

②　社内イントラネット接続システム

他システムとの境界から到達できる範囲の IP アドレス、または業務端末から到達できる範囲の IP アドレスに対して実施すること。詳細は、主管部と委託事業者間で相談の上決定すること。

(2) Web アプリケーション診断

ア　動的画面を診断対象とすること。詳細は主管部と委託事業者間で調整すること。

イ　WebAPI については、すべての機能を診断対象とすること。

【参考】動的画面、静的画面の考え方

①　利用者が入力した値(検索キーワードやアカウント情報等)に応じてその後の処理が変化するような画面を動的画面という。

②　利用者が入力した値に応じて内容やその後の処理が変化することがなくサーバに用意されたコンテンツをそのまま表示するような画面を静的画面という。

(3) スマートフォンアプリケーション診断

ア　Android や iOS 向けなど異なる OS でアプリケーションを提供する場合、いずれのアプリケーションでも診断を実施すること。

イ　主管部が提供した実行ファイル（apk,ipa など）に対し、動的診断を実施すること。

ウ　主管部は root 化/jailbreak 検知機能を無効化した実行ファイル（apk,ipa など）を提供すること。

(4) ペネトレーションテスト

ア　原則、グローバル IP アドレスを対象にインターネット（リモート）から診断を実施すること。

イ　事前に実施した脆弱性診断で発見された脆弱性または主管部から提示された脆弱性診断結果の脆弱性なども参考に、侵入の可能性と侵入された場合の影響に関するテストを実施すること。

ウ　大量ログイン試行（ブルートフォース攻撃、リバースブルートフォース攻撃、リスト型攻撃、パスワードスプレー攻撃）への耐性を確認すること。

エ　テスト実施中に、当初予定した IP アドレス以外への検証・診断が可能な際は、主管部と委託事業者間で調整のうえ、最大限診断を実施すること。

3　診断項目

(1) ネットワーク診断

項番		診断項目
ネットワーク調査		
	1	ポートスキャン（TCP 0-65535/UDP well-known port）
	2	不要と思われるサービスの稼動
各種サービスの脆弱性調査		
	3	稼動中のサービスからの情報取得（バナー情報取得等）
	4	OS やアプリケーションソフトウェアの既知の脆弱性
	5	脆弱なパスワード設定の存在
	6	各種サービス（FTP サービス、SSH サービス等）の既知の脆弱性
	7	サービス妨害の可能性
	8	SSL/TLS 暗号強度調査
DNS 調査		
	9	DNS ゾーン転送の可否
	10	DNS 再帰的問い合わせの可否
	11	DNS ダイナミックアップデートの可否
SMTP 等調査		
	12	メール不正中継の可否
	13	メールサーバによるユーザ情報漏洩問題
HTTP/HTTPS 調査		
	14	脆弱性の知られている CGI スクリプトの存在
	15	不適切な SSL 証明書の利用

(2) Web アプリケーション診断

項番		診断項目
Web サーバ		
	1	Web サーバ上のデフォルトコンテンツの存在
	2	ディレクトリ一覧、不要なファイルの存在
	3	バックアップファイルとデバッグオプション
	4	サーバなどの設定不備や既知の脆弱性
認証・認可		
	5	脆弱なパスワード設定の存在
	6	強制ブラウジング
	7	脆弱なパスワード
	8	認証・認可回避
	9	アカウントロックの設定

項番		診断項目
入力		
	10	OS コマンドインジェクション
	11	SQL インジェクション
	12	LDAP インジェクション
	13	XPath インジェクション
	14	バッファオーバーフロー
	15	HTTP レスポンス分割
	16	メタキャラクタインジェクション
	17	ディレクトリ・トラバーサル
セッション		
	18	Cookie の Secure 属性と HttpOnly 属性
	19	セッションハイジャック
	20	セッションリプレイ
	21	セッションフィクセーション
	22	セッション ID の推測
	23	セッション ID の HTTP/HTTPS の使い分け
	24	セッション ID の格納方法
	25	セッション ID の有効期限
	26	セッション ID の破棄方法
	27	クロスサイトリクエストフォージェリ
出力		
	28	クロスサイトスクリプティング
	29	エラーコード
	30	不要なコメント
通信		
	31	HTTPS の適用漏れ
サイトデザイン		
	32	エラーメッセージによる情報漏えい
	33	パラメータの操作（改ざん操作）
	34	Web 画面設計上の不備 （例） ・ログイン画面はあるがログアウト機能が無い。 ・ログイン画面にパスワード入力フォームが無い。 ・本来ブラウザのアドレスバー（URL）に非表示にすべき ID、パスワード等の重要情報が表示されている。
	35	サーバサイドリクエストフォージェリ
	36	Cookie、 WebStorage の不適切な利用

(3) スマートフォンアプリケーション診断（端末環境）

項番		診断項目
アプリケーション間連携		
	1	アクセス制限
	2	情報の送受信
通信		
	3	プロトコル
	4	暗号化の有無
	5	サーバ証明書検証
	6	通信内容
	7	プライバシーの保護
認証		
	8	認証機能
	9	連携機能
	10	ログアウト機能
端末内のデータの取扱		
	11	保存場所
	12	アクセス権限
	13	保存方法
	14	保存期間
アプリケーションファイル・ログ		
	15	不要な情報の有無
	16	不要な情報の出力有無
機能の利用		
	17	パーミッション設定

(4) ペネトレーションテスト

項番	診断項目
1	脆弱性の調査
2	設定不備等の調査
3	取得可能情報の調査
4	不正なログインの可否検証(※)
5	権限昇格の可否検証
6	データへのアクセスの可否検証（DB アクセスの実現、通信データの盗聴、データの改ざん）
7	データ持ち出しの可否検証（外部向け通信の実現、データ持ち出しの実現）
8	不正行為の可否検証（不正な取引の実行）

（※）項番 1～3 で得られた情報を利用するものおよび大量ログイン試行（ブルートフォース攻撃、リバースブルートフォース攻撃、リスト型攻撃、パスワードスプレー攻撃）への耐性検証

別紙３

サイバーセキュリティ対策実施報告書・証明書

▼ 提出対象にチェックを記載

	①	脆弱性診断実施報告書（ネットワーク診断）
	②	脆弱性診断実施報告書（Webアプリケーション診断）
	③	脆弱性診断実施報告書（スマートフォンアプリケーション診断）
	④	ペネトレーションテスト実施報告書
	⑤	ＦＷ設定検証実施報告書
	⑥	セキュリティパッチ管理作業実施報告書
	⑦	セキュリティパッチ管理作業実施証明書
	⑧	コンピュータウイルス対策ソフトの管理作業実施報告書
	⑨	コンピュータウイルス対策ソフトの管理作業実施証明書
	⑩	EOL管理作業実施報告書
	⑪	EOL管理作業実施証明書

株式会社ゆうちょ銀行　御中

脆弱性診断実施報告書（ネットワーク診断）

弊社は、「***(※契約名、またはサービス名)***」を提供するにあたり、以下のとおり、ネットワーク診断を実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】
- 診断実施者　：***(診断事業者の会社名を記載)***
- 診断実施日　：***(ネットワーク診断の実施日をそれぞれ記載)***
- 診断実施環境　：***(本番／開発／ステージング／テスト用など、環境の種類を記載)***
- 診断範囲　：***(診断を実施したサーバ等を記載)***

【診断結果情報】

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	件	
	危険度：高	件	
	危険度：中	件	
	危険度：低	件	
危険度ごとの対応方針・対応予定時期等	危険度：緊急		
	危険度：高		
	危険度：中		
	危険度：低		

【診断実施内容】

確認項目	回答欄	備考
IPアドレス単位で診断を実施している。		
当該システムがインターネットに接続している場合、インターネットから接続可能なグローバルIPアドレスに対して、リモート（インターネット）から診断を実施している。		
他システムとの境界から到達できる範囲のIPアドレス又は、業務端末から到達できる範囲のIPアドレスに対して診断を実施している。		
ネットワーク診断で使用したツール等		

【取得している認証等】

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証		
その他（　　）		

〇〇〇〇年〇〇月〇〇日
会社名：***(委託事業者の会社名を記載)***
所在地：***(委託事業者の所在地を記載)***
氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

脆弱性診断実施報告書（ネットワーク診断）

弊社は、「***システム***」を提供するにあたり、以下のとおり、ネットワーク診断を実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】
- 診断実施者　　：***株式会社*****
- 診断実施日　　：***20**年**月**日、**日***
- 診断実施環境　：***本番環境***
- 診断範囲　　：***サーバ（1IP）、**サーバ（1IP）***

【診断結果情報】

検出件数を記載

危険度をCVSS値に依らず評価している場合に記入

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	*1件*	***【評価方法】 危険度は、以下の方法にて評価を実施。 ・～～～（評価方法を記載）***
	危険度：高	*0件*	
	危険度：中	*2件*	
	危険度：低	*0件*	
危険度ごとの対応方針・対応予定時期等 検出事項、対応方針の詳細を確認できる資料を添付（提示が可能な場合）	危険度：緊急	*20**年*月*日*	***緊急：ソフトウェアアップデートを実施 中①：ソフトウェアアップデートを実施 中②：機能の無効化を実施 検出事項の詳細は別添「****」を参照***
	危険度：高		
	危険度：中	*20**年*月*日*	
	危険度：低		

【診断実施内容】

実施している場合は"○"
未実施の場合は"×"を記載し、備考欄に理由を記載

確認項目	回答欄	備考
IPアドレス単位で診断を実施している。	○	
当該システムがインターネットに接続している場合、インターネットから接続可能なグローバルIPアドレスに対して、リモート（インターネット）から診断を実施している。	○	
他システムとの境界から到達できる範囲のIPアドレス又は、業務端末から到達できる範囲のIPアドレスに対して診断を実施している。	○	
ネットワーク診断で使用したツール等 ***Nessus *.*.*(plugin-set ***)*** ***Nmap *.**** ***手動診断***		

開示可能な範囲で記載
非開示の場合は、その理由を記載

【取得している認証等】

取得している認証等がある場合は"○"
ない場合は空欄

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証	○	
その他（　　）		

その他、ネットワーク診断の実施を証明する認証等があれば、具体的に記載

〇〇〇〇年〇〇月〇〇日
会社名：株式会社〇〇〇〇
所在地：東京都～
氏名：〇〇　〇〇

株式会社ゆうちょ銀行　御中

脆弱性診断実施報告書（Webアプリケーション診断）

弊社は、「***(※契約名、またはサービス名)***」を提供するにあたり、以下のとおり、Webアプリケーション診断を実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】

・診断実施者　　：***(診断事業者の会社名を記載)***
・診断実施日　　：***(Webアプリケーション診断の実施日をそれぞれ記載)***
・診断実施環境　：***(本番／開発／ステージング／テスト用など、環境の種類を記載)***
・診断範囲　　：***(お客さま用公開画面／システム管理用画面等の実施した範囲を記載)***

【診断結果情報】

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	件	
	危険度：高	件	
	危険度：中	件	
	危険度：低	件	
危険度ごとの対応方針・対応予定時期等	危険度：緊急		
	危険度：高		
	危険度：中		
	危険度：低		

【診断実施内容】

確認項目	回答欄	備考
貴行に提供するWebアプリケーションの動的画面は、すべて診断対象としている。		
貴行に提供するWebAPI機能は、すべて診断対象としている。		
Webアプリケーション診断で使用したツール等		

【取得している認証等】

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証		
その他（　　）		

〇〇〇〇年〇〇月〇〇日
会社名：***(委託事業者の会社名を記載)***
所在地：***(委託事業者の所在地を記載)***
氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

脆弱性診断実施報告書（Webアプリケーション診断）

弊社は、「***システム***」を提供するにあたり、以下のとおり、Webアプリケーション診断を実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】
- 診断実施者　　：***株式会社*****
- 診断実施日　　：***20**年**月**日、**日***
- 診断実施環境　：***本番環境***
- 診断範囲　　：***お客さま用公開画面、システム管理用画面***

【診断結果情報】

検出件数を記載

危険度をCVSS値に依らず評価している場合に記入

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	*1件*	***【評価方法】 危険度は、以下の方法にて評価を実施。 ・～～～（評価方法を記載）***
	危険度：高	*0件*	
	危険度：中	*2件*	
	危険度：低	*0件*	
危険度ごとの対応方針・対応予定時期等	危険度：緊急	*20**年*月*日*	***緊急：入力文字列のエスケープ処理を実装 中　：ソフトウェアアップデートを実施 検出事項の詳細は別添「****」を参照***
	危険度：高		
	危険度：中	*20**年*月*日*	
	危険度：低		

検出事項、対応方針の詳細を確認できる資料を添付（提示が可能な場合）

【診断実施内容】

実施している場合は"○"
未実施の場合は"×"を記載し、備考欄に理由を記載

確認項目	回答欄	備考
貴行に提供するWebアプリケーションの動的画面は、すべて診断対象としている。	○	
貴行に提供するWebAPI機能は、すべて診断対象としている。	○	
Webアプリケーション診断で使用したツール等		
Burp Suite*.*.* 手動診断		

開示可能な範囲で記載
非開示の場合は、その理由を記載

【取得している認証等】

取得している認証等がある場合は"○"
ない場合は空欄

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証	○	
その他（　　）		

その他、Webアプリケーション診断の実施を証明する認証等があれば、具体的に記載

〇〇〇〇年〇〇月〇〇日
会社名：株式会社〇〇〇〇
所在地：東京都～
氏名：〇〇　〇〇

株式会社ゆうちょ銀行　御中　　様式７

脆弱性診断実施報告書（スマートフォンアプリケーション診断）

弊社は、「(※契約名、またはサービス名)」を提供するにあたり、以下のとおり、スマートフォンアプリケーション診断を実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】
・診断実施者　　：***(診断事業者の会社名を記載)***
・診断実施日　　：***(スマートフォンアプリケーション診断の実施日をそれぞれ記載)***
・診断実施環境　：***(本番／開発／ステージング／テスト用など、環境の種類を記載)***
・診断範囲　　：***(診断を実施したアプリケーション等を記載)***

【診断結果情報】

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	件	
	危険度：高	件	
	危険度：中	件	
	危険度：低	件	
危険度ごとの対応方針・対応予定時期等	危険度：緊急		
	危険度：高		
	危険度：中		
	危険度：低		

【診断実施内容】

確認項目	回答欄	備考
Android やiOS 向けなど異なるOS でアプリケーションを提供する場合、すべてのアプリケーションに対して診断を実施している。		
貴行が提供した実行ファイル（apk,ipa など）に対し、動的診断を実施している。		
スマートフォンアプリケーション診断で使用したツール等		

【取得している認証等】

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証		
その他（　　）		

〇〇〇〇年〇〇月〇〇日
会社名：***(委託事業者の会社名を記載)***
所在地：***(委託事業者の所在地を記載)***
氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中　　様式７

脆弱性診断実施報告書（スマートフォンアプリケーション診断）

弊社は、「***システム***」を提供するにあたり、以下のとおり、スマートフォンアプリケーション診断を実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】
- 診断実施者　　：***株式会社****
- 診断実施日　　：*20**年**月**日、**日*
- 診断実施環境　：***本番環境***
- 診断範囲　　：***アプリ（Android,iOS)***

【診断結果情報】

検出件数を記載

危険度をCVSS値に依らず評価している場合に記入

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	*1件*	***【評価方法】 危険度は、以下の方法にて評価を実施。 ・～～～（評価方法を記載）***
	危険度：高	*0件*	
	危険度：中	*2件*	
	危険度：低	*0件*	
危険度ごとの対応方針・対応予定時期等	危険度：緊急	*20**年*月*日*	***緊急：ソフトウェアアップデートを実施 中　：ソフトウェアアップデートを実施 検出事項の詳細は別添「****」を参照***
	危険度：高		
	危険度：中	*20**年*月*日*	
	危険度：低		

検出事項、対応方針の詳細を確認できる資料を添付（提示が可能な場合）

【診断実施内容】

実施している場合は"○"
未実施の場合は"×"を記載し、備考欄に理由を記載

確認項目	回答欄	備考
Android やiOS 向けなど異なるOS でアプリケーションを提供する場合、すべてのアプリケーションに対して診断を実施している。	○	
貴行が提供した実行ファイル（apk,ipa など）に対し、動的診断を実施している。	○	
スマートフォンアプリケーション診断で使用したツール等		
Secure Coding Checker*.*.* 手動診断		

開示可能な範囲で記載
非開示の場合は、その理由を記載

【取得している認証等】

取得している認証等がある場合は"○"
ない場合は空欄

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証	○	
その他（　　）		

その他、スマートフォンアプリケーション診断の実施を証明する認証等があれば、具体的に記載

○○○○年○○月○○日
会社名：株式会社○○○○
所在地：東京都～
氏名：○○　○○

株式会社ゆうちょ銀行　御中

ペネトレーションテスト実施報告書

弊社は、「(***※契約名、またはサービス名)***」を提供するにあたり、以下のとおり、ペネトレーションテストを実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】
- 診断実施者　　：***(ペネトレーションテスト事業者の会社名を記載)***
- 診断実施日　　：***(ペネトレーションテストの実施日をそれぞれ記載)***
- 診断実施環境　：***(本番／開発／ステージング／テスト用など、環境の種類を記載)***
- 診断範囲　　：***(お客さま用公開画面／システム管理用画面等の実施した範囲を記載)***

【診断結果情報】

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	件	
	危険度：高	件	
	危険度：中	件	
	危険度：低	件	
危険度ごとの対応方針・対応予定時期等	危険度：緊急		
	危険度：高		
	危険度：中		
	危険度：低		

【診断実施内容】

確認項目		回答欄	備考
以下の項目を含むペネトレーションテストを実施			
事前に実施した脆弱性診断結果を用いた攻撃の試行			
大量ログイン試行攻撃（※）による権限奪取不正取引の可否			
大量ログイン試行攻撃（※）を抑止する機能(アカウントロック等)の有無			
※大量ログイン試行攻撃には、以下の4種を含めること ・ブルートフォース攻撃 ・リバースブルートフォース攻撃 ・リスト型攻撃 ・パスワードスプレー攻撃			
攻撃準備活動として実施			
(脆弱性の調査) 攻撃に利用可能なソフトウェアの脆弱性の調査			
(設定不備等の調査) 攻撃可能にする設定上の不備の調査			
(取得可能情報の調査) システム上に残存する攻撃のヒントになる情報、他所で入手可能な攻撃に使える情報の調査収集			
侵害可能性の検証として実施			
不正なログインの可否			
権限昇格の可否			
データへのアクセスの可否	DBアクセスの実現		
	通信データの盗聴		
	データの改ざん		
データ持ち出しの可否	外部向け通信の実現		
	データ持ち出しの実現		
不正行為の可否	不正な取引の実行		
その他（　　）			

【取得している認証等】

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証		
その他（　　）		

〇〇〇〇年〇〇月〇〇日
会社名：***(委託事業者の会社名を記載)***
所在地：***(委託事業者の所在地を記載)***
氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

ペネトレーションテスト実施報告書

弊社は、「*******システム***」を提供するにあたり、以下のとおり、ペネトレーションテストを実施し、発見された脆弱性を修正する等適切に対応していることを報告いたします。

【診断実施情報】
- 診断実施者　　：***株式会社*******
- 診断実施日　　：***20**年**月**日、**日***
- 診断実施環境　：***本番環境***
- 診断範囲　　：*******（お客さま用公開画面）***

【診断結果情報】

検出件数を記載

危険度をCVSS値に依らず評価している場合に記入

確認項目		回答欄	備考
検出事項 【補足】 ・危険度の基準は、CVSS値換算で以下のとおり 緊急：9.0以上　高：7.0以上 中　：4.0以上　低：3.9以下 ・別の評価方法で評価している場合は、具体的な評価方法を備考欄に記載	危険度：緊急	*1件*	***【評価方法】 危険度は、以下の方法にて評価を実施。 ・～～～（評価方法を記載）***
	危険度：高	*0件*	
	危険度：中	*2件*	
	危険度：低	*0件*	
危険度ごとの対応方針・対応予定時期等 検出事項、対応方針の詳細を確認できる資料を添付（提示が可能な場合）	危険度：緊急	*20**年*月*日*	***緊急：ソフトウェアアップデートを実施 中①：ソフトウェアアップデートを実施 中②：機能の無効化を実施 検出事項の詳細は別添「****」を参照***
	危険度：高		
	危険度：中	*20**年*月*日*	
	危険度：低		

【診断実施内容】

実施している場合は"○"
未実施の場合は"×"を記載し、備考欄に理由を記載

確認項目		回答欄	備考
以下の項目を含むペネトレーションテストを実施			
事前に実施した脆弱性診断結果を用いた攻撃の試行		○	
大量ログイン試行攻撃（※）による権限奪取不正取引の可否		○	
大量ログイン試行攻撃（※）を抑止する機能(アカウントロック等)の有無		○	
※大量ログイン試行攻撃には、以下の4種を含めること ・ブルートフォース攻撃 ・リバースブルートフォース攻撃 ・リスト型攻撃 ・パスワードスプレー攻撃			
攻撃準備活動として実施			
（脆弱性の調査） 攻撃に利用可能なソフトウェアの脆弱性の調査		○	
（設定不備等の調査） 攻撃可能にする設定上の不備の調査		○	
（取得可能情報の調査） システム上に残存する攻撃のヒントになる情報、他所で入手可能な攻撃に使える情報の調査収集		○	
侵害可能性の検証として実施			
不正なログインの可否		○	
権限昇格の可否		○	
データへのアクセスの可否	DBアクセスの実現	○	
	通信データの盗聴	○	
	データの改ざん	○	
データ持ち出しの可否	外部向け通信の実現	○	
	データ持ち出しの実現	○	
不正行為の可否	不正な取引の実行	○	
その他（　　）			

その他、ペネトレーションテストとして実施している項目がある場合は"○"を記入し、「その他（）」の（）内に具体的に記載ない場合は空欄

【取得している認証等】

確認項目	回答欄	備考
PCI DSS 準拠証明書（AOC）		
SOC2/SOC3レポート		
ISMS/ISO27001/JIS Q27001認証	○	
その他（　　）		

取得している認証等がある場合は"○"
ない場合は空欄

ペネトレーションテストの実施を証明する認証等があれば、具体的に記載

○○○○年○○月○○日
会社名：株式会社○○○○
所在地：東京都～
氏名：○○　○○

株式会社ゆうちょ銀行　御中

ＦＷ設定検証実施報告書

弊社は、「(***※契約名、またはサービス名)***」を提供するにあたり、以下のとおり、サービス利用時に経由する通信経路上にあるＦＷについて設計書通りに設定されていることを確認し、発見された不備等を修正する等適切に対応していることを報告いたします。

【検証実施情報】

・検証実施者　　：***(検証実施事業者の会社名を記載)***

・対象期間　　：　　年度　□年次

□第一四半期　□第二四半期　□第三四半期　□第四四半期

□その他（　　）

・検証実施日　　：***(検証実施日を記載)***

【検証結果情報】

回答欄		備考
【結果】 不備無し・不備有り・非開示 【原因】 【対処状況】		

【取得している認証等】

回答欄		備考

〇〇〇〇年〇〇月〇〇日

会社名：***(委託事業者の会社名を記載)***

所在地：***(委託事業者の所在地を記載)***

氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

ＦＷ設定検

以下の検証頻度に応じて、チェックボックスに記入
・1回／四半期　：年度分、該当する四半期に✔
・1回／半期　：年度分、該当する期間に✔
→上半期の場合、第一四半期・第二四半期に✔
→下半期の場合、第三四半期・第四四半期に✔
・1回／年の場合　：年度分に✔
・上記以外　：その他に✔、チェックボックス右側（）内に具体的な対象期間を記載

弊社は、「***システム***」を提供するにあたり、以
ＦＷについて設計書通りに設定されていることを確認
とを報告いたします。

【検証実施情報】

・検証実施者　：***株式会社****

・対象期間　：　2022 年度　☑年次
☐第一四半期　☐第二四半期　☐第三四半期　☐第四四半期
☐その他（　　）

対象期間の年度を記載

・検証実施日　：***2022年12月1日***

【検証結果情報】

回答欄		備考
【結果】 不備無し・不備有り・非開示 【原因】 【対処状況】		

ＦＷ設定値の不備の有無を選択
非開示の場合は非開示を選択

不備有りの場合、原因を記載

不備有りの場合、対処状況を記載

【取得している認証等】

回答欄		備考

ＦＷ設定検証の実施を証明する認証等がある場合は具体的に記載、
ない場合は空欄

〇〇〇〇年〇〇月〇〇日
会社名：株式会社〇〇〇〇
所在地：東京都～
氏名：〇〇　〇〇

株式会社ゆうちょ銀行　御中

セキュリティパッチ管理作業実施報告書

弊社は、「***(※契約名、またはサービス名)***」を提供するにあたり、下記のとおりセキュリティパッチ管理作業を実施しましたので、実施結果を報告します。

【実施内容】

セキュリティパッチ管理について以下を確認。

①脆弱性情報、セキュリティパッチ情報に関して　　で収集していること。

②取得した情報については影響調査を実施し、対応が必要と判断したものについては漏れなく対応を実施していること。

【実施期間】

〇〇〇〇年〇〇月〇〇日　～　〇〇〇〇年〇〇月〇〇日

【実施結果】

上記①②について、問題ないことを確認。

〇〇〇〇年〇〇月〇〇日

会社名：***(委託事業者の会社名を記載)***

所在地：***(委託事業者の所在地を記載)***

氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

セキュリティパッチ管理作業実施報告書

弊社は、「*******システム***」を提供するにあたり、下記のとおりセキュリティパッチ管理作業を実施しましたので、実施結果を報告します。

契約名またはサービス・システム名をご記入ください。

情報の収集頻度をプルダウンからお選びください。
該当する選択肢がない場合は、実態をご記入ください。

【実施内容】

セキュリティパッチ管理について以下を確認。

①脆弱性情報、セキュリティパッチ情報に関して　　随時　　で収集していること。

②取得した情報については影響調査を実施し、対応が必要と判断したものについては漏れなく対応を実施していること。

【実施期間】

2022年　4月　1日　～　2023年　3月　31日

確認の実施期間をご記入ください。

【実施結果】

上記①②について、問題ないことを確認。

〇〇〇〇年〇〇月〇〇日

会社名：***（委託事業者の会社名を記載）***

所在地：***（委託事業者の所在地を記載）***

氏名：（***委託事業者の責任者の氏名を記載）***

株式会社ゆうちょ銀行　御中

セキュリティパッチ管理作業実施証明書

弊社は、「***(※契約名、またはサービス名)***」を提供するにあたり、下記のとおりセキュリティパッチ管理作業を実施し、セキュリティパッチ管理について適切に対応していることを証明いたします。

【実施内容】

セキュリティパッチ管理について以下を確認。

①脆弱性情報、セキュリティパッチ情報に関して　　で収集していること。

②取得した情報については影響調査を実施し、対応が必要と判断したものについては漏れなく対応を実施していること。

〇〇〇〇年〇〇月〇〇日

会社名：***(委託事業者の会社名を記載)***

所在地：***(委託事業者の所在地を記載)***

氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

セキュリティパッチ管理作業実施証明書

弊社は、「*******システム***」を提供するにあたり、下記のとおりセキュリティパッチ管理作業を実施し、セキュリティパッチ管理について適切に対応していることを証明いたします。

契約名またはサービス・システム名をご記入ください。

情報の収集頻度をプルダウンからお選びください。
該当する選択肢がない場合は、実態をご記入ください。

【実施内容】

セキュリティパッチ管理について以下を確認。

①脆弱性情報、セキュリティパッチ情報に関して　　随時　　で収集していること。

②取得した情報については影響調査を実施し、対応が必要と判断したものについては漏れなく対応を実施していること。

〇〇〇〇年〇〇月〇〇日

会社名：***（委託事業者の会社名を記載）***

所在地：***（委託事業者の所在地を記載）***

氏名：（***委託事業者の責任者の氏名を記載）***

株式会社ゆうちょ銀行　御中

コンピュータウイルス対策ソフトの管理作業実施報告書

弊社は、「***（※契約名、またはサービス名）***」を提供するにあたり、下記のとおりコンピュータウイルス対策ソフトの管理作業を実施しましたので、実施結果を報告します。

【実施内容】

コンピュータウイルス対策ソフトの管理について、以下の作業を実施。

①原則本サービスを構成するシステムに、コンピュータウイルス対策ソフトを導入する。

②***（※頻度を記入）***でパターンファイルのリリース情報を収集し、***（※自動／手動）***更新している。

③***（※頻度を記入）***でコンピュータウイルス対策ソフト（本体、及びパターンファイル）が更新されていることを確認し、確認結果を管理台帳に記録し、管理している。

【実施結果】

上記①②③について、問題ないことを確認。

〇〇〇〇年〇〇月〇〇日
会社名：***（委託事業者の会社名を記載）***
所在地：***（委託事業者の所在地を記載）***
氏名：（***委託事業者の責任者の氏名を記載）***

株式会社ゆうちょ銀行　御中

コンピュータウイルス対策ソフトの管理作業実施報告書

弊社は、「*******システム***」を提供するにあたり、下記のとおりコンピュータウイルス対策ソフトの管理作業を実施しましたので、実施結果を報告します。

契約名またはサービス・システム名をご記入ください。

週次、随時等の頻度をご記入ください。

【実施内容】

コンピュータウイルス対策ソフトの管理について、以下の作業を実施。

①原則本サービスを構成するシステムに、コンピュータウイルス対策ソフトを導入する。

②***随時***でパターンファイルのリリース情報を収集し、***自動***更新している。

自動または手動かをご記入ください。

③***随時***でコンピュータウイルス対策ソフト（本体、及びパターンファイル）が更新されていることを確認し、確認結果を管理台帳に記録し、管理している。

※③について、管理台帳による記録・管理に代わり、自動ツール等で更新状態を管理している場合は、実態にあわせて、適宜修正してください。
修正時には、管理台帳に代わり、コンピュータウイルス対策ソフト（本体、及びパターンファイル）の更新漏れを防止するための手段があることが分かるように記載をお願いします。
自動ツール等により更新漏れを防止している場合は、以下例のとおり記載。
《例1》日次でコンピュータウイルス対策ソフト（本体、及びパターンファイル）が更新されていることを自動ツールで確認し、管理している。
《例2》随時、コンピュータウイルス対策ソフト（本体、及びパターンファイル）が自動更新に失敗した場合に通知されるメールを確認し、更新漏れが発生しない管理をしている。

【実施結果】

上記①②③について、問題ないことを確認。

〇〇〇〇年〇〇月〇〇日
会社名：***（委託事業者の会社名を記載）***
所在地：***（委託事業者の所在地を記載）***
氏名：（***委託事業者の責任者の氏名を記載）***

株式会社ゆうちょ銀行　御中

コンピュータウイルス対策ソフトの管理作業実施証明書

弊社は、「***（※契約名、またはサービス名）***」を提供するにあたり、下記のとおりコンピュータウイルス対策ソフトの管理作業を実施し、適切に対応していることを証明いたします。

【実施内容】

コンピュータウイルス対策ソフトの管理について、以下の作業を実施。

①原則本サービスを構成するシステムに、コンピュータウイルス対策ソフトを導入する。

②***（※頻度を記入）***でパターンファイルのリリース情報を収集し、***（※自動／手動）***更新している。

③***（※頻度を記入）***でコンピュータウイルス対策ソフト（本体、及びパターンファイル）が更新されていることを確認し、確認結果を管理台帳に記録し、管理している。

〇〇〇〇年〇〇月〇〇日
会社名：***（委託事業者の会社名を記載）***
所在地：***（委託事業者の所在地を記載）***
氏名：（***委託事業者の責任者の氏名を記載）***

株式会社ゆうちょ銀行　御中

コンピュータウイルス対策ソフトの管理作業実施証明書

弊社は、「*******システム***」を提供するにあたり、下記のとおりコンピュータウイルス対策ソフトの管理作業を実施し、適切に対応していることを証明いたします。

契約名またはサービス・システム名をご記入ください。

【実施内容】

コンピュータウイルス対策ソフトの管理について、以下の作業を実施

①原則本サービスを構成するシステムに、コンピュータウイルス対策ソフトを導入する。

②***随時***でパターンファイルのリリース情報を収集し、***自動***更新している。

週次、随時等の頻度をご記入ください。

自動または手動かをご記入ください。

③***随時***でコンピュータウイルス対策ソフト（本体、及びパターンファイル）が更新されていることを確認し、確認結果を管理台帳に記録し、管理している。

※③について、管理台帳による記録・管理に代わり、自動ツール等で更新状態を管理している場合は、実態にあわせて、適宜修正してください。
修正時には、管理台帳に代わり、コンピュータウイルス対策ソフト（本体、及びパターンファイル）の更新漏れを防止するための手段があることが分かるように記載をお願いします。
自動ツール等により更新漏れを防止している場合は、以下例のとおり記載。
《例1》日次でコンピュータウイルス対策ソフト（本体、及びパターンファイル）が更新されていることを自動ツールで確認し、管理している。
《例2》随時、コンピュータウイルス対策ソフト（本体、及びパターンファイル）が自動更新に失敗した場合に通知されるメールを確認し、更新漏れが発生しない管理をしている。

〇〇〇〇年〇〇月〇〇日
会社名：***（委託事業者の会社名を記載）***
所在地：***（委託事業者の所在地を記載）***
氏名：（***委託事業者の責任者の氏名を記載）***

株式会社ゆうちょ銀行　御中

EOL管理作業実施報告書

弊社は、「***(※契約名、またはサービス名)***」を提供するにあたり、下記のとおりEOL管理作業を実施しましたので、実施結果を報告します。

【実施内容】

EOL管理台帳について以下を確認。

①システムを構成している製品が漏れなく記載されていること。

②収集した最新のEOL情報が反映されていること。

③EOL期限切れの製品がある場合、継続使用によるリスクも考慮のうえ、社内基準に従い継続して利用できることの判断が責任者によりされていること。

【実施結果】

上記①②③について、問題ないことを確認。

〇〇〇〇年〇〇月〇〇日
会社名：***(委託事業者の会社名を記載)***
所在地：***(委託事業者の所在地を記載)***
氏名：(***委託事業者の責任者の氏名を記載)***

株式会社ゆうちょ銀行　御中

EOL管理作業実施証明書

弊社は、「***(※契約名、またはサービス名)***」を提供するにあたり、下記のとおりEOL管理作業を実施し、EOL管理について適切に対応していることを証明いたします。

【実施内容】

EOL管理台帳について以下を確認。

①システムを構成している製品が漏れなく記載されていること。

②収集した最新のEOL情報が反映されていること。

③EOL期限切れの製品がある場合、継続使用によるリスクも考慮のうえ、社内基準に従い継続して利用できることの判断が責任者によりされていること。

〇〇〇〇年〇〇月〇〇日
会社名：***(委託事業者の会社名を記載)***
所在地：***(委託事業者の所在地を記載)***
氏名：(***委託事業者の責任者の氏名を記載)***

別紙4

入力項目												
システムID	システム名	所管担当	端末種別	機器名	HW製品名	アンチウイルス導入有無	EDR導入有無	インターネット接続有無	OS有無	サービス利用状況	ホスト名	基準日

入力項目		
システムID_システム名	機器名	OS・SW製品名