DM6-02-101

別紙２：雛形付録

外部委託における情報セキュリティ対策実施規程

雛形付録

（「約款による情報処理サービス」利用チェックリスト）

2011 年 4 月

内閣官房情報セキュリティセンター

改訂履歴

改訂日	改訂理由
2011/4/21	初版

目次

本雛形の利用方法

本雛形は、「約款による情報処理サービス」を利用するうえで注意すべき点について記述したものであり、別紙１：雛形から、「約款による情報処理サービス」の利用におけるサービス利用時の留意事項と「約款による情報処理サービス」の利用におけるサービス利用時のチェックリストに特化したものであるため、別紙１：雛形と併せて使用されたい。

雛形において想定する前提

本雛形は、以下のことを前提としている。

- 本雛形は、統括情報セキュリティ責任者が、府省庁の規定を整備するために利用することを想定している。
- サービスによっては無償で利用できるものもあり、その場合調達行為が無く、約款を承諾することで情報処理サービスを利用可能となる。そのような利用形態においても外部委託となることの認識が必要である。
- 本雛形記載の留意事項を把握しチェックリストに答えたうえで、情報処理サービスの約款を承諾するか判断いただきたい。
- 本チェックリストの項目は、約款による情報処理サービスを利用するにあたって一般的に想定されるリスクに基づいて作成されたものであり、各府省庁や利用するサービスの状況に合わせて、チェック項目を適宜修正・追加することが望ましい。

手直しポイント

「外部委託における情報セキュリティ対策実施規程」を策定するに当たり、以下の点を考慮して手直しをする必要がある。

- 本雛形は、統括情報セキュリティ責任者が、府省庁の規定を整備するために利用することを想定している。
- 府省庁での規定等に応じて、本雛形から該当する記事を選択し、不足する部分及び前提等が異なる部分は追加・修正をする。
- 雛形中に、*【チェックリスト作成者への補足説明】*という見出しの後に、斜体の文字書式で記載されている記述は、チェックリスト作成者への補足説明であり、作成後のチェックリストの一部にする記述ではない。

1　「約款による情報処理サービス」とは

約款が用意されており、情報セキュリティに関する事項について利用者による条件選択の余地が限られている情報処理サービス（以下、「約款による情報処理サービス」と言う。）を利用し、外部委託を行う場合である。（利用者に提供される機能など情報セキュリティ以外の契約内容については要求に基づいて用意される又は条件選択や修正ができるものであっても、情報セキュリティに関する事項に条件選択の制限があれば、「約款による情報処理サービス」に含む。）例えばクラウドサービス 等がこれに該当する。

なお、サービスの中には無償で利用できるものもあるが、無償で利用する場合でも外部委託に該当するとの認識が必要である。つまり、府省庁外の情報処理サービスを利用する場合には、それが有償で調達手続きを経る場合だけではなく、無償で利用を開始できる場合であっても、本規程を遵守することが求められる。無償で利用する例としては、無償で提供されているメールサービスの利用やアンケート記入及び集計に係るウェブサービスの利用等を挙げることができる。

こうした無償サービスの利用においては、その利用者が調達に従事する行政事務従事者に限られたものではないため、当該留意事項について本雛形付録に基づき、府省庁内に広く周知する必要がある。

2　「約款による情報処理サービス」の利用におけるサービス利用時の留意事項

「約款による情報処理サービス」利用時は、有償の場合には外部事業者が定めた規約等の約款に従うという附合契約が一般的であり、無償の場合には明示的な契約締結行為がなく利用申し込みの同意だけの場合もある。この場合、約款を修正する余地がなく、利用者ごとのサービス内容の変更要求は受け入れられず、約款に同意するかしないかの選択しかできないことが多い。この点を踏まえて、省庁対策基準及び規定と照らし合わせて、セキュリティレベルが確保されているかを確認のうえ、利用を検討することが求められる。約款でセキュリティレベルが明記されていない場合は、委託してはならない。

行政事務として「約款による情報処理サービス」を利用するにあたっては、課室情報セキュリティ責任者等のしかるべき者の承認を実施することが想定されているところ、実際の利用にあたっては、以下に示す脅威が考えられる。

表 1.「約款による情報処理サービス」の利用におけるサービス利用時の留意事項

	留意事項
1	サービスは約款の範囲でしか提供されない。
2	サービス時間とサポート時間が限られている場合がある。
3	サービスのセキュリティポリシーが開示されないことが多く、省庁対策基準及び規定を満たしているか判断が困難である。

4	サービス提供事業者から提供されるサービスレベルは可用性のみであることが多い。
5	サービス提供事業者は利用者による監査を基本的に受け入れない。
6	バックアップ実施や障害発生時の復旧等の実施内容やタイミングといった、情報システムの運用に関しては約款に記載されていないことが多い。
7	バックアップするデータ形式が他の事業者のサービスに移行できない場合がある。
8	利用者側で情報のバックアップができない場合がある。
9	同一サーバ上で複数の業務（利用者）を実行しているケースがあり、その場合セキュリティ対策が十分に実行されていない業務の影響を受ける可能性がある。
10	同一サーバ上で複数の利用者が情報処理を実行しているため、別の利用者情報を盗み見し、別の利用者に成りすまして処理を行う可能性がある。
11	サーバ資源の利用者ごとの分割が不適切なことによる情報漏えいが発生する可能性がある。
12	情報の置き場所が特定の場所に固定されず、海外の法執行機関等による予期せぬアクセスが行われうることがある。
13	サービスを有期契約した場合、契約終了後の情報の取り扱い（確実な消去）が不明瞭な場合がある。
14	サービス提供事業者の経営が破たんしたり突然のサービス停止に陥った場合、預けた情報の行方は保証されず、損害賠償も支払われない場合がある。
15	サービス提供事業者の従業員が不正を行う可能性がある。
16	約款の内容はサービス提供者側の都合で利用開始後一方的に変更される可能性がある。
17	準拠法に外国法を指定される場合がある。
18	管轄裁判所に海外の裁判所を指定される場合がある。

3 「約款による情報処理サービス」の利用におけるサービス利用時のチェックリスト

2.「約款による情報処理サービス」の利用におけるサービス利用時の留意事項を踏まえてチェックリストを作成した。チェックリストに基づき省庁対策基準及び規定と照らし合わせて、セキュリティレベルが確保されているかを確認のうえ、契約を検討することが求められる。約款でセキュリティレベルが確認できない場合は、委託することを避けなければならない。

表 2 「約款による情報処理サービス」の利用におけるサービス利用時のチェックリスト

（下記チェックリスト中の「問題ありませんか？」の表記は**サービスを利用する上でリスクを許容できるものであるかという**意味を含むものであることに留意されたい。）

	チェック項目	チェック
可用性に関するチェック項目		
1	サービス時間について約款上の記載があり、その記載内容は利用上問題ありませんか？	□
2	サポート時間について約款上の記載があり、その記載内容は利用上問題ありませんか？	□
3	計画停止予定通知の有無について約款上の記載があり、その記載内容は利用上問題ありませんか？	□
4	サービス稼働率について約款上の記載があり、その記載内容は利用上問題ありませんか？	□
5	利用者側でデータバックアップできるかどうかについて約款上の記載があり、その記載内容は利用上問題ありませんか？	□
6	災害などによるシステム障害からの情報システム復旧の有無について約款上の記載があり、その記載内容は利用上問題ありませんか？	□
7	サービス提供事業者が経営破たんした場合、情報の行方が保証されない可能性があることは利用上問題ありませんか？	□
機密性および完全性に関するチェック項目		
8	同一サーバ上で複数の利用者が実行するサービスであることは利用上問題ありませんか？	□
9	セキュリティ意識の低い他の利用者の影響（成りすましでの情報の盗み見等）を受ける可能性があることは利用上問題ありませんか？	□
10	情報が海外で保管される場合には、万一、海外の法執行機関等による予期せぬアクセスが行われた際に問題ありませんか？	□
11	サービス終了後、情報がどのように消去されるかについて確認した結果は利用上問題ありませんか？	□
12	サービス提供事業者の従業員が不正を行う可能性があることは利用上問題ありませんか？	□

【チェックリスト作成者への補足説明】

上記チェックリストの項目は、約款による情報処理サービスを利用するにあたって一般的に想定されるリスクに基づいて作成されたものであり、各府省庁や利用するサービスの状況に合わせて、チェック項目を適宜修正・追加することが望ましい。この際の参考文献として、以下を参照することが望ましい。

・「SaaS 向け SLA ガイドライン」（平成 20 年 1 月　経済産業省）

・「ASP・SaaS における情報セキュリティ対策ガイドライン」（平成 20 年 1 月総務省）

・「クラウドサービスレベルのチェックリスト」（平成 22 年 8 月　経済産業省）など

また、運用における考え方の例としては、以下を参照することが望ましい。

・「国、地方公共団体等公共機関における民間ソーシャルメディアを活用した情報発信についての指針」（平成 23 年 4 月　内閣官房、総務省、経済産業省） など