資料２

# 「地方公共団体における情報セキュリティポリシーに関するガイドライン」改定案（資料１関係部分抜粋）

総務省

2021年10月22日

地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会

# 改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（１/１１）

＜現行：対策基準（趣旨）＞

（新設）

4.2. 外部サービスの利用 ※参考として政府統一基準群抜粋を記載

4.2.1 要機密情報を取り扱う場合【目的・趣旨】

政府機関において今後クラウドサービスなどの外部サービスの利用の拡大が見込まれているところ、外部サービスの利用に当たっては、外部サービス基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を設計（構成）した上で、セキュリティを確保する必要がある。

機関等が外部サービス提供者に取扱いを委ねる情報は、当該提供者によって適正に取り扱われなければならないが、外部サービスの利用においては、適正な取扱いが行われていることを直接確認することが一般に容易ではない。また、外部サービスでは、複数利用者が共通の外部サービス基盤を利用する可能性があり、自身を含む他の利用者にも関係する情報の開示を受けることが困難になる場合もある。機関等が外部サービスを利用して要機密情報を取り扱う場合は、外部サービス提供者を適正に選択するために、このような外部サービスの特性を理解し、機関等による外部サービス提供者へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項を十分に考慮し、機関等と外部サービス提供者の役割や責任分担を明確にした上で、外部サービスが選定基準及びセキュリティ要件を満たすことを確実にすることが求められる。

さらに、外部サービスを利用する際のセキュリティ対策は、選定や契約時における対策だけでなく、契約後の情報システムの導入・構築、その後の運用・保守、更には契約終了時に至るまで情報システムのライフサイクル全般において行う必要がある。特に外部サービスのサービス内容は非常に早いサイクルで変化しており、利用開始時に行ったセキュリティ対策が途中で無効になることも考えられるため、運用・保守のフェーズにおける対策は定期的に漏れなく実施することが求められる。（続く）

＜改定案：対策基準(趣旨)＞

8.2. 外部サービスの利用(機密性２以上の情報を取り扱う場合)

【趣旨】

今後クラウドサービスなどの外部サービスの利用の拡大が見込まれているところ、外部サービスの利用に当たっては、外部サービス基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を設計した上で、セキュリティを確保する必要がある。

外部サービス提供者に取扱いを委ねる情報は、当該提供者によって適正に取り扱われなければならないが、外部サービスの利用においては、適正な取扱いが行われていることを直接確認することが一般に容易ではない。また、外部サービスでは、複数利用者が共通の外部サービス基盤を利用する可能性があり、自身を含む他の利用者にも関係する情報の開示を受けることが困難になる場合もある。外部サービスを利用して機密性２以上の情報を取り扱う場合は、外部サービス提供者を適正に選択するために、このような外部サービスの特性を理解し、本市による外部サービス提供者へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項を十分に考慮し、本市と外部サービス提供者の役割や責任分担を明確にした上で、外部サービスが選定基準及びセキュリティ要件を満たすことを確実にすることが求められる。

さらに、外部サービスを利用する際のセキュリティ対策は、選定や契約時における対策だけでなく、契約後の情報システムの導入・構築、その後の運用・保守、更には契約終了時に至るまで情報システムのライフサイクル全般において行う必要がある。特に外部サービスのサービス内容は非常に早いサイクルで変化しており、利用開始時に行ったセキュリティ対策が途中で無効になることも考えられるため、運用・保守のフェーズにおける対策は定期的に漏れなく実施することが求められる。（続く）

選定・契約・導入・構築・運用・保守・更改・廃棄までの
一連のサイクルにおけるマネジメントの重要性について記載

# 改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（２/１１）

＜現行：対策基準（趣旨）＞

（新設）

4.2. 外部サービスの利用 ※参考として政府統一基準群抜粋を記載

4.2.1 要機密情報を取り扱う場合【目的・趣旨】

（続き）

＜外部サービスの例＞

・クラウドサービス
・Ｗｅｂ会議サービス
・ＳＮＳ（ソーシャルネットワーキングサービス）
・検索サービス、翻訳サービス、地図サービス
・ホスティングサービス
・インターネット回線接続サービス

なお、民間事業者等が不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービスでは、セキュリティ対策やデータの取扱いなどについて機関等への特別な扱いを求めることができない場合が多く、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として要機密情報を取り扱うことはできない。

＜改定案：対策基準(趣旨)＞

8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）

【趣旨】

（続き）

＜外部サービスの例＞

・クラウドサービス
・Ｗｅｂ会議サービス
・ＳＮＳ（ソーシャルネットワーキングサービス）
・検索サービス、翻訳サービス、地図サービス
・ホスティングサービス

なお、民間事業者等が不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービスでは、セキュリティ対策やデータの取扱いなどについて本市への特別な扱いを求めることができない場合が多く、機密性２以上の情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として機密性２以上の情報を取り扱うことはできない。

約款による外部サービスでは、機密性の高い情報を扱わないことは現行から変更なし

# 改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（３/11）

## ＜現行：対策基準（例文）＞

（新設）

4.2. 外部サービスの利用　※参考として政府統一基準群抜粋を記載

4.2.1 要機密情報を取り扱う場合【遵守事項】

(3)外部サービスの選定（クラウドサービス以外の場合）

(a)　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。

(b)　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

(ア) 外部サービスの利用を通じて機関等が取り扱う情報の外部サービス提供者における目的外利用の禁止

(イ) 外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

(ウ) 外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、機関等の意図せざる変更が加えられないための管理体制

(エ) 外部サービス提供者の資本関係・役員等の情報、外部サービスの提供が行われる施設等の場所、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

(オ) 情報セキュリティインシデントへの対処方法

(カ) 情報セキュリティ対策その他の契約の履行状況の確認方法

(キ) 情報セキュリティ対策の履行が不十分な場合の対処方法

(c)　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めること。

（続く）

## ＜改定案：対策基準(例文)＞

8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）

【例文】

（２）外部サービスの選定

①　情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。

②　情報セキュリティ責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

(ア)外部サービスの利用を通じて本市が取り扱う情報の外部サービス提供者における目的外利用の禁止

(イ)外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

(ウ)外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制

(エ)外部サービス提供者の資本関係・役員等の情報、外部サービスの提供が行われる施設等の場所、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

(オ)情報セキュリティインシデントへの対処方法

(カ)情報セキュリティ対策その他の契約の履行状況の確認方法

(キ)情報セキュリティ対策の履行が不十分な場合の対処方法

③　情報セキュリティ責任者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めること。（続く）

# 改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（４/１１）

＜現行：対策基準（例文）＞

（新設）

4.2. 外部サービスの利用 ※参考として政府統一基準群抜粋を記載

4.2.1 要機密情報を取り扱う場合【遵守事項】

（続き）

(d)　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスの利用を通じて機関等が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。

(ア) 情報セキュリティ監査の受入れ

(イ) サービスレベルの保証

(e)　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスの利用を通じて機関等が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて機関等の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。

(f)　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を機関等に提供し、機関等の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。

(g)　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定すること。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。（続く）

＜改定案：対策基準(例文)＞

8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）

【例文】

（続き）

④　情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。

（ア）情報セキュリティ監査の受入れ

（イ）サービスレベルの保証

⑤　情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。

⑥　情報セキュリティ責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。

⑦　情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定すること。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。【推奨事項】

（続く）

# 改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（５/１１）

＜現行：対策基準（例文）＞

（新設）

4.2. 外部サービスの利用 ※参考として政府統一基準群抜粋を記載

4.2.1 要機密情報を取り扱う場合【遵守事項】

（続き）

(h)　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めること。

(i)　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断すること。

＜改定案：対策基準(例文)＞

8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）

【例文】

（続き）

⑧　情報セキュリティ責任者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めること。

⑨　統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断すること。

# 改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（６/１１）

## ＜現行：対策基準（解説）＞

（新設）※章立ての変更

8.4. クラウドサービスの利用

【解説】

①　クラウドサービスの利用に当たっては、情報の管理や処理をクラウドサービス事業者に委ねるため、その情報の適正な取扱いの確認が容易ではなくなることを踏まえ、適切なクラウドサービス事業者を選定することによりリスクを低減することが考えられる。

（注１）クラウドサービスの利用に当たっては、「地方公共団体におけるASP・SaaS導入活用ガイドライン」（平成22年4月　総務省）を参照されたい。

②　インターネットを介してサービスを提供するクラウドサービスの利用に当たっては、クラウドサービス事業者の事業所の場所に関わらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、クラウドサービス事業者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、データセンターの設置されている国の法令により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、住民情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で運用できるデータセンターを選択する必要がある。

　管轄裁判所に関しては、国外の裁判所で裁判を行うこととならないよう、契約において日本国内の裁判所（必要に応じて地方公共団体の所在地を管轄する裁判所）を合意管轄裁判所として規定する必要がある。また、外国に本社を置く企業が提供するサービスを地方公共団体が利用する場合の紛争を当該企業の本社の所在地を管轄する裁判所が管轄することも考えられる一方、その場合は日本の国内法と同等の個人情報の保護などが確立されないおそれがあることについては利用者である地方公共団体において契約締結の際に十分な留意が必要となる。

## ＜改定案：対策基準(解説)＞

8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）

【解説】

（２）外部サービスの選定

①　外部サービスの利用に当たっては、情報の管理や処理を外部サービス提供者に委ねるため、その情報の適正な取扱いの確認が容易ではなくなることを踏まえ、適切な外部サービス提供者を選定することによりリスクを低減することが考えられる。

（注１）外部サービスの利用に当たっては、「地方公共団体におけるASP・SaaS導入活用ガイドライン」（平成22年4月　総務省）を参照されたい。

②　インターネットを介して提供される外部サービスの利用に当たっては、外部サービス提供者の事業所の場所に関わらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、外部サービス提供者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、データセンターの設置されている国の法令により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、日本の法令の範囲内で運用できるデータセンターを選択する必要がある。

　管轄裁判所に関しては、国外の裁判所で裁判を行うこととならないよう、契約において日本国内の裁判所（必要に応じて地方公共団体の所在地を管轄する裁判所）を合意管轄裁判所として規定する必要がある。また、外国に本社を置く企業が提供するサービスを地方公共団体が利用する場合の紛争を当該企業の本社の所在地を管轄する裁判所が管轄することも考えられる一方、その場合は日本の国内法と同等の個人情報の保護などが確立されないおそれがあることについては利用者である地方公共団体において契約締結の際に十分な留意が必要となる。

裁判管轄、準拠法に関する記載は、現行ガイドラインから変更なし

# 改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（７/１１）

＜現行：対策基準（解説）＞

（新設）※章立ての変更

8.4. クラウドサービスの利用

【解説】

③　クラウドサービスを利用するに当たり、サービスの中断や終了時に際し、円滑に業務を移行するための対策として、以下を例とするセキュリティ対策を実施することをクラウドサービスの選定条件とし、仕様内容にも含める必要がある。

・取り扱う情報の可用性区分の格付に応じた、サービス中断時の復旧要件

・取り扱う情報の可用性区分の格付に応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

④　情報セキュリティ管理者は、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティ対策を実施する必要がある。システムの重要度に応じて求められる可用性のレベル等（稼働率、目標復旧時間、バックアップの保管方法など）を十分に検討し、調達の際に、検討した結果を調達仕様書に具体的に盛り込まなければならない。また、必要となる条項（インシデントの報告義務、損害賠償等）を盛り込んだ契約及びサービスレベルを保証させるためのSLAを締結する必要がある。特に、バックアップについては、契約において、各業務システムの重要度を勘案した適切なバックアップレベルを設定し、別途のバックアップの取得など、レベルに応じた適切な対策を実施することが重要である。

＜改定案：対策基準(解説)＞

8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）

【解説】

（２）外部サービスの選定

③　外部サービスを利用するに当たり、サービスの中断や終了時に際し、円滑に業務を移行するための対策として、以下を例とするセキュリティ対策を実施することを外部サービスの選定条件とし、仕様内容にも含める必要がある。

・取り扱う情報の可用性区分の格付に応じた、サービス中断時の復旧要件

・取り扱う情報の可用性区分の格付に応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

④　情報セキュリティ管理者は、外部サービス部分を含む情報の流通経路全般にわたるセキュリティ対策を実施する必要がある。システムの重要度に応じて求められる可用性のレベル等（稼働率、目標復旧時間、バックアップの保管方法など）を十分に検討し、調達の際に、検討した結果を調達仕様書に具体的に盛り込まなければならない。また、必要となる条項（インシデントの報告義務、損害賠償等）を盛り込んだ契約及びサービスレベルを保証させるためのSLAを締結する必要がある。特に、バックアップについては、契約において、各業務システムの重要度を勘案した適切なバックアップレベルを設定し、別途のバックアップの取得など、レベルに応じた適切な対策を実施することが重要である。

# 改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（８/11）

＜現行：対策基準（解説）＞

（新設）※章立ての変更

8.4. クラウドサービスの利用

【解説】

（外部委託事業者の選定基準）

（注２）クラウドサービスの大規模障害により、自治体の業務に長時間支障が発生した事案を踏まえたセキュリティ対策については、「「Jip-Base」事案を踏まえたクラウドサービスの利用に係る注意喚起」（令和2年5月22日　総行情第76号　総務省自治行政局地域情報政策室長通知）を参照されたい。

（注３）契約に必要となる条項については「8.1.外部委託（３）契約項目」及び「地方公共団体におけるASP・SaaS導入活用ガイドライン」（平成22年4月　総務省）を参照されたい。また、セキュリティ要件の検討を行う際は、「非機能要求グレード（地方公共団体版）利用ガイド」（平成26年3月　地方自治情報センター）も併せて参照されたい。

⑤　情報セキュリティ管理者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

　クラウドサービス事業者及び当該サービスの信頼性が十分であることを総合的に判断するためには、クラウドサービスで取り扱う情報の機密性・完全性・可用性が確保されるように、クラウドサービス事業者のセキュリティ対策を含めた経営が安定していること、クラウドやアプリケーションに係るセキュリティ対策が適切に整備され、運用されていること等を評価する必要がある。

＜改定案：対策基準(解説)＞

8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）

【解説】

（２）外部サービスの選定

（注２）外部サービスの大規模障害により、自治体の業務に長時間支障が発生した事案を踏まえたセキュリティ対策については、「「Jip-Base」事案を踏まえたクラウドサービスの利用に係る注意喚起」（令和2年5月22日　総行情第76号　総務省自治行政局地域情報政策室長通知）を参照されたい。

（注３）契約に必要となる条項については「8.1.業務委託（３）契約項目」及び「地方公共団体におけるASP・SaaS導入活用ガイドライン」（平成22年4月　総務省）を参照されたい。また、セキュリティ要件の検討を行う際は、「非機能要求グレード（地方公共団体版）利用ガイド」（平成26年3月　地方自治情報センター）も併せて参照されたい。

⑤　情報セキュリティ管理者は、外部サービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

　外部サービス提供者及び当該サービスの信頼性が十分であることを総合的に判断するためには、外部サービスで取り扱う情報の機密性・完全性・可用性が確保されるように、外部サービス提供者のセキュリティ対策を含めた経営が安定していること、サービスを提供する基盤環境やアプリケーションに係るセキュリティ対策が適切に整備され、運用されていること等を評価する必要がある。

# 改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（９/１１）

＜現行：対策基準（解説）＞

（新設）※章立ての変更

8.4. クラウドサービスの利用

【解説】

（外部委託事業者の選定基準）

　このような評価に当たって、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用することが考えられる。

　なお、参考となる認証には、ISO/IEC 27017 によるクラウドサービス分野におけるISMS 認証の国際規格がある。また、日本セキュリティ監査協会のクラウド情報セキュリティ監査やクラウドサービス事業者等のセキュリティに係る内部統制の保証報告書であるSOC報告書（Service Organization Control Report）を活用することも考えられる。クラウドサービス利用時のセキュリティ対策や内部統制に関する報告書等については、以下を参照されたい。

参考：国際規格

「ISO/IEC 27017（安全なクラウドサービス利用のための分野別ISMS 規格）」

参考：日本セキュリティ監査協会

「クラウド情報セキュリティ管理基準」

「クラウド情報セキュリティ監査制度規程」

ISMAPを参考とすべき第三者認証の一つとして追加し、監査報告書や認証を積極的に利用するように記載を見直し

＜改定案：対策基準(解説)＞

8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）

【解説】

（２）外部サービスの選定

　このような評価に当たって、外部サービス提供者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用する必要がある。

　なお、選定条件となる認証にはISO/IEC 27017 によるクラウドサービス分野におけるISMS 認証の国際規格がある。また、ISMAPの管理基準を満たすことの確認やISMAPクラウドサービスリスト等のほか、日本セキュリティ監査協会のクラウド情報セキュリティ監査や外部サービス提供者等のセキュリティに係る内部統制の保証報告書であるSOC報告書（Service Organization Control Report）を活用することを推奨する。外部サービス利用時のセキュリティ対策や内部統制に関する報告書等については、以下を参照されたい。

参考：国際規格

「ISO/IEC 27017（安全なクラウドサービス利用のための分野別ISMS 規格）」

参考：日本セキュリティ監査協会

「クラウド情報セキュリティ管理基準」

（https://jcispa.jasa.jp/documents/）

「クラウド情報セキュリティ監査制度規程」

（https://jcispa.jasa.jp/cloud_security/jcispa_regulation/）

# 改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（10/11）

＜現行：対策基準（例文）＞

（新設）

＜改定案：対策基準(例文)＞

4.2. 外部サービスの利用 ※参考として政府統一基準群抜粋を記載
4.2.1 要機密情報を取り扱う場合【遵守事項】
（５）外部サービスの利用承認
(a)　情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。
(b)　利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。
(c)　利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。

8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）
【例文】
（４）外部サービスの利用承認
①　情報セキュリティ責任者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。
②　利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。
③　利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。

# 改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（11/11）

＜現行：対策基準（解説）＞

（新設）

4.2. 外部サービスの利用 ※参考として政府統一基準群抜粋を記載

4.2.1 要機密情報を取り扱う場合【基本対策事項】

4.2.1(8)-1 統括情報セキュリティ責任者は、更改・廃棄時における利用終了手順に係る規定を策定する場合、以下を含む内容を規定すること。

a) 外部サービスの利用を終了する場合の移行計画書若しくは終了計画書の作成

b) 移行計画書若しくは終了計画書の外部サービス利用者への事前通知

4.2.1(8)-2 統括情報セキュリティ責任者は、更改・廃棄時における情報の廃棄に係る規定を策定する場合、以下を含む内容を規定すること。

a) 情報の廃棄方法

b) 基盤となる物理機器の廃棄

4.2.1(8)-3 統括情報セキュリティ責任者は、更改・廃棄時におけるアカウントの廃棄に係る規定を策定する場合、以下を含む内容を規定すること。

a) 作成された外部サービス利用者アカウントの削除

b) 利用した外部サービス管理者アカウントの削除・返却と再利用の確認

c) 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の削除と関連情報の廃棄

＜改定案：対策基準(解説)＞

8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）

【解説】

（６）外部サービスを利用した情報システムの更改・廃棄時の対策

① 統括情報セキュリティ責任者は、更改・廃棄時における利用終了手順に係る規定を策定する場合、以下を含む内容を規定すること。

（ア）外部サービスの利用を終了する場合の移行計画書若しくは終了計画書の作成

（イ）移行計画書若しくは終了計画書の外部サービス利用者への事前通知

② 統括情報セキュリティ責任者は、更改・廃棄時における情報の廃棄に係る規定を策定する場合、以下を含む内容を規定すること。なお、情報資産の廃棄は「2. 情報資産の分類と管理（２）情報資産の管理 ⑩情報資産の廃棄」、「4.1. サーバ等の管理 （７）機器等の廃棄」を参照すること。

（ア）情報の廃棄方法

（イ）基盤となる物理機器の廃棄

③ 統括情報セキュリティ責任者は、更改・廃棄時におけるアカウントの廃棄に係る規定を策定する場合、以下を含む内容を規定すること。

（ア）作成された外部サービス利用者アカウントの削除

（イ）利用した外部サービス管理者アカウントの削除・返却と再利用の確認

（ウ）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の削除と関連情報の廃棄

# 改定のポイント２：情報セキュリティ対策の動向を踏まえた記載の充実（１/１）

＜現行：対策基準（解説）＞

３　情報システム全体の強靭性の向上
【解説】
（注１０）未知の不正プログラムへの対策（エンドポイント対策）
　未知の不正プログラム対策として、OSのプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、これを隔離する方式があり、不審な挙動を示す端末のホスト名やIPアドレスなどの情報をログとして取得し、管理者へ通知する必要がある

＜改定案：対策基準(解説)＞

３　情報システム全体の強靭性の向上
【解説】
（注１０）未知の不正プログラムへの対策（エンドポイント対策）
　未知の不正プログラム対策として、OSのプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、これを隔離する方式があり、不審な挙動を示す端末のホスト名やIPアドレスなどの情報をログとして取得し、管理者へ通知する必要がある。なお**製品の導入だけでは未知の不正プログラムの対策とはならない。監視体制やCSIRTとの連携等組織的な対策と合わせて検討が必要となることに留意する必要がある。**

運用面に関する記載を追記

# 改定のポイント３：多様な働き方を前提とした情報セキュリティ対策（１/８）

＜現行：対策基準（解説）＞

（１） 職員等の遵守事項
【解説】
（略）
②支給以外のパソコンやモバイル端末等の業務利用
自宅や庁外等での情報処理作業においては支給された端末を使用することとし、支給以外の端末の使用は原則禁止とする。やむを得ず支給以外の端末を使用する場合は、以下のような対策を実施することが必要である。
・統括情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ管理者の許可を得る
（略）
・業務利用する必要がなくなった場合は、支給以外のパソコンやモバイル端末等から業務に関係する情報を削除する
さらに、支給以外の端末から庁内ネットワークに接続を行う可能性がある場合は、情報漏えいを防ぐため、以下のような対策を講じる必要がある。
・ファイル暗号化機能を持つアプリケーションでの接続のみを許可する

＜改定案：対策基準(解説)＞

（１） 職員等の遵守事項
【解説】
（略）
②支給以外のパソコンやモバイル端末等の業務利用
自宅や庁外等での情報処理作業においては支給された端末を使用することとし、支給以外の端末の使用は原則禁止とする。やむを得ず支給以外の端末を使用する場合は、以下のような対策を実施することが必要である。
・統括情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ管理者の許可を得る
（略）
・業務利用する必要がなくなった場合は、支給以外のパソコンやモバイル端末等から業務に関係する情報を削除する
（注５）
支給以外の端末の利用申請内容については、以下を含めること。
・申請者の氏名、所属、連絡先
・利用する端末の契約者の名義（スマートフォン等の通信事業者と契約を行う端末の場合）
・利用する端末の製造企業名、機種名、OSの種類及びバージョン
・利用目的、取り扱う情報の概要、機密性２以上の情報の利用の有無等
・主要な利用場所
・利用する主要な通信回線サービス
・利用する期間
さらに、支給以外の端末から庁内ネットワークに接続…

# 改定のポイント３：多様な働き方を前提とした情報セキュリティ対策（２/８）

＜現行：対策基準（解説）＞

5.1.職員等の遵守事項
(１)　職員等の遵守事項
【解説】
（略）
さらに、支給以外の端末から庁内ネットワークに接続を行う可能性がある場合は、情報漏えいを防ぐため、以下のような対策を講じる必要がある。
・シンクライアント環境やセキュアブラウザを使用する
・ファイル暗号化機能を持つアプリケーションでの接続のみを許可する
また、支給以外のパソコン、モバイル端末及び電磁的記録媒体を情報システム室に持ち込むことは禁止する。

＜改定案：対策基準(解説)＞

5.1.職員等の遵守事項
(１)　職員等の遵守事項
【解説】
（略）
さらに、支給以外の端末から庁内ネットワークに接続を行う可能性がある場合は、情報漏えいを防ぐため、以下のような利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を暗号化するための機能を設ける必要がある。
・シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。
・セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする。
・ファイル暗号化等のセキュリティ機能を持つアプリケーションを導入する。
・端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能を設ける。
・上記のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能を設ける。
・ハードディスク等の電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能を設ける。
　また、支給以外のパソコン、モバイル端末及び電磁的記録媒体を情報システム室に持ち込むことは禁止する。

# 改定のポイント３：多様な働き方を前提とした情報セキュリティ対策（３/８）

＜現行：対策基準（解説）＞

6.1. コンピュータ及びネットワークの管理
【解説】
（略）
(１９) 無許可でのネットワーク接続の禁止
セキュリティ上、ネットワークとの接続には適正な管理が必要であることから、無許可での接続を禁止する。あわせて、接続が許可されたものであることを確認するための措置を講じるとともに、許可手続を定める必要がある。（支給以外の端末を接続する場合も同様とする。）
（注１６）特に、庁内で無線LANを使用している場合に、職員等や外部委託事業者がパソコンやモバイル端末等を持込み、無許可でアクセスポイントへ接続する行為を禁止する必要がある。

＜改定案：対策基準(解説)＞

6.1. コンピュータ及びネットワークの管理
【解説】
（略）
(１９) 無許可でのネットワーク接続の禁止
セキュリティ上、ネットワークとの接続には適正な管理が必要であることから、無許可での接続を禁止する。あわせて、接続が許可されたものであることを確認するための措置を講じるとともに、許可手続を定める必要がある。（支給以外の端末を接続する場合も同様とする。）
（注１６）庁外の通信回線に接続した支給以外の端末を庁内の通信回線に接続することの許可手続として、以下を含む手続を規定し、職員等に遵守させること。
・利用時の許可申請手続
・手続内容（利用者、目的、利用する情報、端末等）
・利用期間満了時の手続
・庁内通信回線への接続時の手続（端末の事前検疫等）
・許可権限者（情報セキュリティ管理者）による手続内容の記録
（注１７）特に、庁内で無線LANを使用している場合に、職員等や外部委託事業者がパソコンやモバイル端末等を持込み、無許可でアクセスポイントへ接続する行為を禁止する必要がある。さらに、支給以外の端末から庁内ネットワークに接続を行う可能性がある場合は、情報漏えいを防ぐため、以下のような対策を講じる必要がある。

# 改定のポイント３：多様な働き方を前提とした情報セキュリティ対策（４/８）

＜現行：対策基準（解説）＞

6.2　アクセス制御
（２）職員等による外部からのアクセス等の制限
【解説】
（注４）テレワークのセキュリティ対策については、「テレワークセキュリティガイドライン（第4版）」（平成30年4月　総務省）を併せて参照されたい。
（注５）持ち込んだモバイル端末を確認するシステムとして、検疫システムがある。検疫システムとは、OSのパッチやコンピュータウイルス対策ソフトウェアのパターンファイルが最新でない、不正プログラムが侵入しているなど、十分なセキュリティ対策が実施されていないモバイル端末を庁内ネットワークに接続させないシステムである。モバイル端末を庁内に持ち帰った場合等に、検疫システムによる確認を義務付けることにより、様々な脅威の発生を防止する。
（注６）庁外から庁内のネットワークや情報システムにアクセスする際に公衆無線LAN等の庁外通信回線を利用することは原則禁止であるが、やむを得ず利用する場合は、統括情報セキュリティ責任者の許可を得た上で、必要最小限の範囲のみのアクセスとする。さらに、ログを取得し、不正なアクセスがないかを定期的に確認することが求められる。

＜改定案：対策基準(解説)＞

6.2　アクセス制御
（２）職員等による外部からのアクセス等の制限
【解説】
（注４）テレワークのセキュリティ対策については、「テレワークセキュリティガイドライン（第５版）」（令和３年５月　総務省）を併せて参照されたい。
（注５）持ち込んだモバイル端末を確認するシステムとして、検疫システムがある。検疫システムとは、OSのパッチやコンピュータウイルス対策ソフトウェアのパターンファイルが最新でない、不正プログラムが侵入しているなど、十分なセキュリティ対策が実施されていないモバイル端末を庁内ネットワークに接続させないシステムである。モバイル端末を庁内に持ち帰った場合等に、検疫システムによる確認を義務付けることにより、様々な脅威の発生を防止する。
（注６）庁外から庁内のネットワークや情報システムにアクセスする際に公衆無線LAN等の庁外通信回線を利用することは原則禁止であるが、やむを得ず利用する場合は、統括情報セキュリティ責任者の許可を得た上で、必要最小限の範囲のみのアクセスとする。さらに、ログを取得し、不正なアクセスがないかを定期的に確認することが求められる。
（注７）画面ののぞき見や盗聴を防止できるような環境を選定することで情報の漏えい対策につながる。また、テレワーク実施時の離席時の端末等の盗難に注意する。
（注８）統括情報セキュリティ責任者及び情報システム管理者は、テレワーク実施時の情報セキュリティ対策を確実に実施させるため、テレワーク実施前及び実施後に職員がチェックすべき項目を定め、職員等に当該チェックを実施させること。

# 改定のポイント３：多様な働き方を前提とした情報セキュリティ対策（５/８）

＜現行：対策基準（解説）＞

6.1.コンピュータ及びネットワークの管理
【例文】
（略）
（２０） 業務以外の目的でのウェブ閲覧の禁止
①職員等は、業務以外の目的でウェブを閲覧してはならない。
②統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

＜改定案：対策基準(解説)＞

6.1.コンピュータ及びネットワークの管理
【例文】
（略）
（２０） 業務以外の目的でのウェブ閲覧の禁止
①職員等は、業務以外の目的でウェブを閲覧してはならない。
②統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適正な措置を求めなければならない。
（２１） Web会議サービスの利用時の対策
①統括情報セキュリティ責任者は、Web会議を適切に利用するための利用手順を定めなければならない。
②職員等は、本市の定める利用手順に従い、Web会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。
③職員等は、Web会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。
④職員等は、外部からWeb会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い承認を得なければならない。

# 改定のポイント３：多様な働き方を前提とした情報セキュリティ対策（６/８）

＜現行：対策基準（解説）＞

6.1. コンピュータ及びネットワークの管理
【解説】
（略）
（２０） 業務以外の目的でのウェブ閲覧の禁止
（略）
統括情報セキュリティ責任者は、業務外での閲覧を発見した場合は、情報セキュリティ管理者に通知し、対応を求めなければならない。

＜改定案：対策基準(解説)＞

6.1. コンピュータ及びネットワークの管理
【解説】
（略）
（２０） 業務以外の目的でのウェブ閲覧の禁止
（略）
統括情報セキュリティ責任者は、業務外での閲覧を発見した場合は、情報セキュリティ管理者に通知し、対応を求めなければならない。
（２１） Web会議サービスの利用時の対策
職員等は、Web会議サービスの利用に当たり、以下の情報セキュリティ対策を実施する必要がある。
・支給する端末を利用すること。
・許可されたWeb会議サービスを利用すること。
・利用するWeb会議サービスのソフトウェアが、最新の状態であることを確認すること。
・機密性２以上の情報を取り扱う場合は、可能な限りエンドツーエンド（E2E）の暗号化を行うこと。
・機密性２以上の情報を取り扱う場合は、Web会議サービスの議事録作成機能、自動翻訳機能及び録画機能等、E2Eの暗号化を利用できなくなる機能を可能な限り使用しないこと。
・音声を扱う場合は、ヘッドホンを使用するなど、内容が周囲に漏れないよう注意すること。

# 改定のポイント３：多様な働き方を前提とした情報セキュリティ対策（７/８）

＜現行：対策基準（解説）＞

6.1. コンピュータ及びネットワークの管理
【解説】
（略）
（２０） 業務以外の目的でのウェブ閲覧の禁止
（略）
統括情報セキュリティ責任者は、業務外での閲覧を発見した場合は、情報セキュリティ管理者に通知し、対応を求めなければならない。

＜改定案：対策基準(解説)＞

6.1. コンピュータ及びネットワークの管理
【解説】
（略）
（２０） 業務以外の目的でのウェブ閲覧の禁止
（略）
統括情報セキュリティ責任者は、業務外での閲覧を発見した場合は、情報セキュリティ管理者に通知し、対応を求めなければならない。
（２１） Web会議サービスの利用時の対策
（略）
また、職員等は、Web会議を主催する場合、会議に無関係の者が参加できないよう以下の情報セキュリティ対策を講ずる必要がある。
・会議室にアクセスするためのパスワード等をかける。
・会議の参加者に会議室にアクセスするためのパスワード等を通知する際は、第三者に知られないよう安全な方法で通知する。
・待機室を設けて参加者と確認できた者だけを会議室に入室させる。
・なりすましたり入れ替わりが疑われるなどの不審な参加者を会議室から退室させる。

# 改定のポイント３：多様な働き方を前提とした情報セキュリティ対策（８/８）

＜現行：対策基準（解説）＞

6.1. コンピュータ及びネットワークの管理
【解説】
（略）
（２０） 業務以外の目的でのウェブ閲覧の禁止
（略）
統括情報セキュリティ責任者は、業務外での閲覧を発見した場合は、情報セキュリティ管理者に通知し、対応を求めなければならない。

＜改定案：対策基準(解説)＞

6.1. コンピュータ及びネットワークの管理
【解説】
（略）
（２０） 業務以外の目的でのウェブ閲覧の禁止
（略）
統括情報セキュリティ責任者は、業務外での閲覧を発見した場合は、情報セキュリティ管理者に通知し、対応を求めなければならない。
（２１） Web会議サービスの利用時の対策
（略）
（注１８）Web会議サービスを利用する場合、Web会議サービスのソフトウェアで録画等を防止する設定を行っていても、ビデオカメラで撮影されれば会議内容は保存されるため、会議内容は会議の参加者に保存されることを前提として、会議で取り扱う情報を確認する必要がある。