外部サービスの利用等に関する基準

最終改正　令和７年７月４日

目次

1. 外部サービスの定義

本利用判断基準における用語の定義は、東京都サイバーセキュリティ基本方針に準じる。

> **東京都サイバーセキュリティ基本方針（抜粋）**
>
> **２　定義**
>
> （18）外部サービス
>
> 自組織以外の者が一般向けに情報システムの一部又は全部の機能を提供するクラウドサービス、Ｗｅｂ会議サービス、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等をいう。

2. 外部サービスの利用等に関する基本的な考え方

外部サービスは外部の企業により運営されることから、外部サービス上で都が保有する情報資産を取り扱う場合、そのセキュリティ対策も当該サービスに依存することとなる。このため、外部サービスの利用等に当たっては、当該サービスの約款や契約、その他のサービス提供条件、情報資産の管理、情報システムの業務継続性等を考慮し、当該サービスを利用することによって生じるリスクを可能な限り軽減し、受容できることを確認した上で、利用の可否や条件を判断する必要がある。

3. 外部サービスの利用が可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準

3.1 機密性Ａ又はＢの情報を取り扱う場合（対策基準 9.2（1））

3.1.1 利用可能な業務の範囲

職員等は東京都サイバーセキュリティ対策基準（以下「対策基準」という。）9.2(4)に基づく利用申請を行い、サイバーセキュリティ局統括責任者の許可を得た場合、外部サービスにて機密性Ａ又はＢの情報を取り扱うことができる。

マイナンバー利用事務系においては、原則外部サービスの利用を禁止する。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、ＬＧＷＡＮを経由して、マイナンバー利用事務系との双方向通信によるデータの移送を可能とする。

3.1.2 情報システムの範囲

「1.外部サービスの定義」に記載するサービスを主な範囲とする。

情報資産を所管する者は、当該情報システムにおける機密性の高い情報（例えば都民の個人情報や契約の予定価格情報等）の取り扱いは真に必要な場合に限定すること。

また、情報資産を所管する者は、利用するサービスは業務上必要なサービスのみに限定し、それ以外のサービスは利用させないこと。業務上不要な機能は使用できないように制限等を行うこと。

3.1.3 情報の取扱いを許可する場所を判断する基準

情報資産を所管する者は、外部サービスの利用に当たって、取り扱う情報資産の保存する場所

が適切であるか、対策基準 9.2(2)を参考に、後述する選定基準も踏まえて判断すること。

3.1.4 外部サービス提供者の選定基準

情報資産を所管する者が、外部サービス提供者を選定する際は、必要に応じてコンサルティング会社による支援や調査結果等を活用し、選定対象の外部サービス提供者におけるセキュリティ対策等を確認すること。

具体的な確認観点としては、以下の事項等が挙げられる。

■ 共存・共栄できる事業者

クラウドサービスを提供する事業者として適切な管理体制があるのか、関連する認証を取得しているのか、利用実績数や事例、品質に対する考え方など、クラウド事業者そのものの信頼性を確認する。具体的には、有事の際のインシデント対応において共に連携できること、利用者がクラウドを活用して提供するサービスの重要度に応じてクラウド事業者側のログデータ(ログの種類、保存期間など)等のインシデント対応に必要な情報を即座に提供できること、その情報の入手フローの確認を含め、想定外のインシデントでも問題解決のための提案ができること等、クラウド事業者のサポート方針やサポートレベルを見極める必要がある。

■ クラウドサービスの信頼性

サービスの稼働率やこれまでの障害の発生状況、クラウドサービスのセキュリティ対策、データの保管やバックアップの体制等のサービスそのものの信頼性を確認する。

■ 情報開示方針

情報開示の明瞭性を確認する。規約や約款などの契約面における適切な記載、サービス自体やそのサポート内容の公開方法や公開項目、障害発生時の情報開示の方法や体制など、目に見える形でクラウド事業者が情報公開に努めている様子があるか等を確認する。

また、選定条件に以下に例示する認証等の取得等を付すことを推奨する。

・ISO/IEC 27017 ISMS クラウドセキュリティ認証
・政府情報システムのためのセキュリティ評価制度（ＩＳＭＡＰ）管理基準
・政府情報システムのためのセキュリティ評価制度（ISMAP）に基づいて安全性の評価を受けたクラウドサービスリスト
・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制度
・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（ＳＯＣ報告書）

3.1.5 外部サービスの利用申請の許可権限者と利用手続

情報資産を所管する者は、職員等が外部サービスにて機密性Ａ又はＢの情報を取り扱う場合は、サイバーセキュリティ局統括責任者の許可を得ること。なお、利用申請を行う者が利用申請の許可権限者を兼務することは職務の分離の観点から禁止とする。

情報資産を所管する者は、対策基準 6.1 及び 6.2 等を参考に、取り扱う情報の機密性に応じてサービス利用にかかる規定を整備すること。

また、職員等は、許可を受け利用する場合は、あらかじめユーザ登録等を行ったうえで、当該アカウントの認証・認可を受けて利用すること。

3.1.6　外部サービスの利用状況の管理

サイバーセキュリティ局管理者は、申請及び許可された日時、申請した外部サービスや部署等

を記録し、管理すること。

3.1.7 外部サービスの選定（対策基準 9.2（2））

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。

（注２）サイバーセキュリティ対策その他の契約の履行状況の具体的な確認方法に関しては、「政府機関等の対策基準策定のためのガイドライン」（令和３年７月７日内閣官房内閣サイバーセキュリティセンター）を参照されたい。

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 情報資産を所管する者は、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。

（注３）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４）契約に必要となる条項については「9.1. 業務委託（2）委託時の契約又は協定項目」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　情報資産を所管する者は、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。

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等については、東京都サイバーセキュリティ対策基準関連規程類「外部サービスの利用等に関する基準」3.1.4 を参照すること。

⑥　目的外利用の禁止

自組織が取り扱う情報は、外部サービス提供者において外部サービスの提供に必要な範囲で利用を認めるものであって、それ以外の目的で利用をさせてはならない。

目的外利用に当たる場合としては、例えば、外部サービス提供者が自組織の利用する外部サービスの契約情報等を保有し、今後の営業活動で利用するなどが考えられる。

⑦　各局等の意図しない変更が加えられないための管理体制

外部サービス提供者が行う外部サービスの開発及び運用において、「各局等の意図しない変更が加えられないための管理体制」が確保されることを求めている。具体的に外部サービス提供者の選定条件に含める内容としては、例えば以下が考えられる。

- 外部サービスの開発及び運用において、自組織の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。
- 外部サービスに自組織の意図しない変更が行われるなどの不正が見付かったときに、追跡調査や立入検査等、自組織と外部サービス提供者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

⑧　サイバーセキュリティインシデントへの対処方法

外部サービス提供者において発生したサイバーセキュリティインシデントによる被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について、外部サービス提供者の選定条件に含めておくとよい。対処方法についての合意がないと、インシデ

ントが発生しているにもかかわらず外部サービス提供者と連絡がつかない、営業時間外の対応を断られるなどのトラブルになるおそれがあるため、可能な範囲で事前に具体化することが重要である。対処方法には、例えば、復旧を優先する場合は外部サービスの利用を一時的に停止するための手順を規定し、業務継続を優先する場合は、外部サービスの利用を継続した上でサイバーセキュリティインシデントに対処する手順について、対処の主体とともに規定することが考えられる。また、サイバーセキュリティインシデントに係る外部サービス提供者と自組織間の情報エスカレーション方法やそのタイミングについて規定することも考えられる。

⑨　情報の取扱手順

格付及び取扱制限の明示等、運搬又は送信、消去等の情報の取扱いに関して、外部サービス提供者においても自組織の対策基準に定める内容と同等の取扱いが行われるよう、あらかじめ外部サービス提供者と合意しておくことが重要である。また、外部サービス提供者に提供する情報は必要最小限にとどめる必要があるが、情報システムの利用等において目的外の不必要なアクセスが行われる可能性も考慮し、外部サービス提供者における情報の取扱状況を適宜把握することも重要である。

なお、外部サービス提供者において、業務委託、他の外部サービス等を用いて外部サービスを提供することが考えられる場合は、「9.1 業務委託」、「9.2 外部サービスの利用（機密性Ａ又はＢの情報を取り扱う場合)」の規定を外部サービス提供者においても遵守させるよう仕様書等に規定し、外部サービス提供者とあらかじめ合意しておくことが望ましい。

（注５）外部サービスには様々なサービスがあり、利用においては以下のような点に留意する必要がある。

- ＳＮＳサービスの利用においては、公式アカウントを利用した相談業務等を行う際に、ＳＮＳサービス提供事業者とは別の委託先に適切にセキュリティが確保されたシステムを構築させ、相談内容や住民の個人情報がＳＮＳサービス提供事業者側に残らず、委託先等のデータベース等に直接格納・保管されるシステム構成とする必要がある。ただし、機密性Ａ又はＢの情報を取り扱わない場合は、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の利用が許容される。
- オンライン申請サービスの利用においては、住民側のスマートフォンアプリ上のＱＲコードを後日窓口でかざし申請手続を行うようなサービスの場合、住民等の個人情報が外部サービス提供事業者側に残らないシステム構成とする必要がある。
- 検索サービス、翻訳サービス及び地図サービスの利用においては、検索の文言、写真、動画、翻訳の内容及び履歴などがマーケティングや情報収集のために蓄積される場合がある。
- 各局等が直接契約する収納代行業者がＳＮＳサービスを介してキャッシュレスサービスを利用する場合は、各局等が保有する住民等の個人情報をキャッシュレスサービス事業者に提供する仕組みとならない構成とする必要がある。

⑩　外部サービスに係るアクセスログ等の証跡の保存

外部サービス上におけるアクセスログ等の証跡に係る保存期間については、情報システム又は当該システムに保存される情報の特性に基づき、設定される。ただし、標的型攻撃に関

し、攻撃の初期段階から経緯を確認する観点からは、過去の事例を踏まえ、ログは１年間以上保存することが望ましい。

なお、記憶媒体に保存する期間については、過去に遡って調査する期間や頻度、どの程度のコストをログの保存にかけられるかを考慮して決定する（「7.1 コンピュータ及びネットワークの管理(6)ログの取得等」を参照のこと。）。

⑪　外部サービス提供者による情報の管理・保管

情報管理上の問題として、仮に情報が外部サービス上にあったとしても、当該情報の責任は利用者である情報オーナーが負うことになるため、利用者は外部サービス提供者による情報の管理・保管方法について事前に把握する必要がある。

また、外部サービス提供者が情報の管理・保管を他の事業者へ委託する場合、当該情報が外部サービス利用者の意図しない場面で二次利用されることも懸念されるため、当該事業者におけるサイバーセキュリティ水準や情報の取扱方法に関して外部サービス提供者に確認の上、合意しておく必要がある。

⑫　情報開示請求に対する開示項目や範囲

外部サービスに関し、外部サービス提供者が一般に公開している内容以上の情報提供について、サイバーセキュリティ対策や監査の観点から、事前に自組織と外部サービス提供者が協議の上、外部サービス提供者が提供する内容の項目や範囲を契約において明記することが必要である。また、対象情報の機密性が高い場合、両者間で秘密保持契約（ＮＤＡ：Ｎｏｎ－Ｄｉｓｃｌｏｓｕｒｅ Ａｇｒｅｅｍｅｎｔ）を締結するなど必要な措置を講じた上で取得することが求められる。

⑬　外部サービスの各種リスクへの受容又は低減策の検討

外部サービス選定時には、下記のリスク等を受容又は低減することが可能か検討した上で選定する必要がある。

- 外部サービス提供者は、保存された情報を自由に利用することが可能である。また、約款、利用規約等でその旨を条件として明示していない場合がある。加えて、外部サービス提供者は、利用者から収集した種々の情報を分析し、利用者の関心事項を把握し得る立場にある。
- 情報が改ざんされた場合でも、利用形態によっては外部サービス提供者が一切の責任を負わない場合がある。
- 外部サービス提供者が海外のデータセンター等にサーバ装置を設置してサービスを提供している場合は、当該サーバ装置に保存されている情報に対し、現地の法令等が適用され、現地の政府等による検閲や接収を受ける可能性がある。
- 突然サービス停止に陥ることがある。また、その際に預けた情報の取扱いは保証されず、損害賠償も行われない場合がある。約款の条項は一般的にサービス提供者に不利益が生じないようになっており、このような利用条件に合意せざるを得ない。また、サービスの復旧についても保証されない場合が多い。
- 保存された情報が誤って消去又は破壊されてしまった場合に、サービス提供者が情報の復元に応じない可能性がある。また、復元に応じる場合でも復旧に時間がかかることがある。

・約款及び利用規約の内容が、外部サービス提供者側の都合で利用開始後事前通知等無しで一方的に変更されることがある。
・情報の取扱いが保証されず、一旦記録された情報の確実な消去は困難である。
・利用上の不都合、不利益等が発生しても、サービス提供者が個別の対応には応じない場合が多く、万が一対応を承諾された場合でも、その対応には時間を要することが多い。

3.1.8 外部サービスの利用に係る調達・契約（対策基準 9.2（3））

① 調達仕様の内容を契約に含める際、外部サービス提供者とのサイバーセキュリティに関する役割及び責任の範囲が明確になっていることを確認すること。

3.1.9 外部サービスの利用承認（対策基準 9.2（4））

① サイバーセキュリティインシデント発生時の連絡体制図には、休日・夜間の連絡先や委託事業者がいる場合は委託事業者の連絡先も含めて記載すること。

3.2 機密性Ｃの情報を取り扱う場合（対策基準 9.3（1））

3.2.1 利用可能な業務の範囲

情報資産を所管する者は、対策基準 9.3(2)に基づく利用申請を行いサイバーセキュリティ局責任者の許可を得た場合、外部サービスにて機密性Ｃの情報を取り扱うことができる。

3.2.2 外部サービスの利用申請の許可権限者と利用手続

情報資産を所管する者は、利用するサービスの約款や契約、運営状況、その他の提供条件等から、利用に伴うリスクが許容できることを確認した上で、サイバーセキュリティ局責任者に対し機密性Ｃのみの情報を取り扱う場合の外部サービスの利用を申請し、許可を得ること。

情報資産を所管する者は、職員等が利用するサービスは業務上必要なサービスのみに限定し、それ以外のサービスを使用させないこと。また、業務に不要な機能は使用できないように制限等を行うこと。

3.2.3 外部サービスの利用状況の管理

サイバーセキュリティ局責任者は、申請及び許可された日時、申請した外部サービスや部署等を記録し、管理すること。

4. 外部サービスを利用する際の運用手順

外部サービス管理者は、外部サービスを経由した不正プログラム等の侵入や不正な情報の持ち出し等の防止、人為的ミスによるインシデントの防止等を考慮し、外部サービスの利用に係る運用手順を定め、定期的に手順に沿った運用が行われているかを確認すること。

5. 利用申請を不要とする外部サービス

これまでに、外部サービス提供部署による包括的な利用申請が承認済み又は通知等で個別の利用申請が不要な外部サービスは、別紙「外部サービス・機密性別利用許可申請の要否一覧」に記載のとおりである。利用に当たっての注意事項は、個別の通知等を参考にすること。

なお、今後利用申請を不要とする外部サービスが追加となった場合には、別途周知する。

6. 外部サービスを利用する際の申請先

申請先		
機密性A	機密性B	機密性C
サイバーセキュリティ局統括責任者		サイバーセキュリティ局責任者（局CSIRTが所属する部又は部に相当する所の長）

7. 外部サービスを利用した情報システムの導入・構築時の対策（対策基準 9.2（5））

情報資産を所管する者は、外部サービスを利用して情報システムを構築する際に、以下のセキュリティ対策の実施及び実施状況を「外部サービス利用申請書」や「デジタルサービス開発プロセスにおけるセキュリティガイドライン」等を活用し、確認・記録すること。

ア　不正なアクセスを防止するためのアクセス制御

（ア）外部サービスを利用する際に外部サービス提供者が付与又は外部サービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管理

（イ）外部サービスを利用する際に使用するネットワークに対するサービスごとのアクセス制御

（ウ）外部サービスを利用する情報システムの管理者特権を保有する外部サービス利用者に対する強固な認証技術の利用

（エ）外部サービス提供者が提供する主体認証情報の管理機能が要求事項を満たすことの確認

（オ）外部サービス上に保存する情報や外部サービスの機能に対してアクセス制御できることの確認

（カ）外部サービス利用者による外部サービスに多大な影響を与える操作の特定と誤操作の抑制

（キ）外部サービス上で構成される仮想マシンに対する適切なセキュリティ対策の実施

（ク）インターネット等の外部の通信回線から庁内通信回線を経由せずに外部サービス上に構築した情報システムにログインすることの要否の判断と認める場合の適切なセキュリティ対策の実施

イ　取り扱う情報の機密性保護のための暗号化

（ア）外部サービス内及び通信経路全般における暗号化の確認

（イ）利用する情報システムに係る法令や規則に対する暗号化方式の遵守度合い

ウ　開発時におけるセキュリティ対策

（ア）情報システムの構築において外部サービスを利用する場合の外部サービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用

（イ）情報システムの構築において、外部サービス上に他ベンダが提供するソフトウェア等を導入する場合のそのソフトウェアの外部サービス上におけるライセンス規定

エ　設計・設定時の誤りの防止

（ア）外部サービス上に情報システムを構築する際の外部サービス提供者への設計、構築における知見等の情報の要求とその活用

（イ）外部サービス上に情報システムを構築する際の設定の誤りを見いだすための対策

（ウ）外部サービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件

の異なるネットワーク間の通信の監視

（エ）利用する外部サービス上の情報システムが利用するデータ容量や稼働性能についての監視と将来の予測

（オ）利用する外部サービス上で可用性 B の情報を取り扱う場合の可用性を考慮した設計

（カ）外部サービス内における時刻同期の方法の確認

8. 外部サービスを利用した情報システムの運用・保守時の対策（対策基準 9.2（6））

情報資産を所管する者は、外部サービスを利用して情報システムを運用する際に、以下のセキュリティ対策の実施及び実施状況を「外部サービス利用申請書」や「デジタルサービス開発プロセスにおけるセキュリティガイドライン」等を活用し、確認・記録すること。

ア　外部サービス利用方針の規定

（ア）責任分界点を意識した外部サービスの利用

（イ）利用承認を受けていない外部サービスの利用禁止

（ウ）外部サービス提供者に対する定期的なサービスの提供状態の確認

（エ）利用する外部サービスに係るサイバーセキュリティインシデント発生時の連絡体制

イ　外部サービス利用に必要な教育

（ア）外部サービス利用のための規定及び手順について

（イ）外部サービス利用に係るサイバーセキュリティリスクとリスク対応について

（ウ）外部サービス利用に関する適用法令や関連する規制等について

ウ　取り扱う資産の管理

（ア）外部サービス上で利用する IT 資産の適切な管理

（イ）外部サービス上に保存する情報に対する適切な機密性の格付・取扱制限の明示

（ウ）外部サービスの機能に対する脆弱性対策について、外部サービス利用者の責任範囲の明確化と対策の実施

エ　不正アクセスを防止するためのアクセス制御

（ア）管理者権限を外部サービス利用者へ割り当てる場合のアクセス管理と操作の確実な記録

（イ）外部サービス利用者に割り当てたアクセス権限に対する定期的な見直し

（ウ）外部サービスのリソース設定を変更するユーティリティプログラムを使用する場合の機能の確認と利用者の制限

（エ）利用する外部サービスの不正利用の監視

オ　取り扱う情報の機密性保護のための暗号化

（ア）暗号化に用いる鍵の管理者と鍵の保管場所

（イ）鍵管理機能を外部サービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価

（ウ）鍵管理機能を外部サービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価

カ　外部サービス内の通信の制御

（ア）利用する外部サービスのネットワーク基盤が他のネットワークと分離されていることの確認

キ　設計・設定時の誤りの防止

（ア）外部サービスの設定を変更する場合の設定の誤りを防止するための対策

（イ）外部サービス利用者が行う可能性のある重要操作の手順書の作成と監督者の指導の下での実施

ク　外部サービスを利用した情報システムの事業継続

（ア）不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施（外部サービス提供者が提供する機能を利用する場合は、その実施の確認）

（イ）可用性Ｂの情報を外部サービスで取り扱う場合の十分な可用性の担保、復旧に係る手順の策定と定期的な訓練の実施

（ウ）外部サービス提供者からの変更通知の内容確認と復旧手順の確認

（エ）外部サービスで利用しているデータ容量、性能等の監視

ケ　外部サービスの利用のために作成するＩＤ及びアカウントの管理

（ア）必要最低限のＩＤ及びアカウント作成・発行

（イ）業務に不要な機能の使用制限

（ウ）利用者の登録状況の定期的な確認と継続的に管理できる体制の維持

（エ）システム利用において設定するパスワードの適正管理

（オ）正規の利用者かどうかを判断する認証方式のうち、二つ以上を併用する認証（多要素認証）等の利用検討

9. 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（対策基準 9.2（7））

情報資産を所管する者は、外部サービスの利用を終了する際に、以下のセキュリティ対策の実施及び実施状況を「外部サービス利用申請書」や「デジタルサービス開発プロセスにおけるセキュリティガイドライン」等を活用し、確認・記録すること。

ア　外部サービスの利用終了時における対策

（ア）外部サービスの利用を終了する場合の移行計画書又は終了計画書の作成

（イ）移行計画書又は終了計画書の外部サービス利用者への事前通知

イ　外部サービスで取り扱った情報の廃棄

（ア）情報の廃棄方法（対策基準 3(2)⑩）

（イ）基盤となる物理機器の廃棄（対策基準 5.1(7)）

ウ　外部サービスの利用のために作成したアカウントの廃棄

（ア）作成し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

10. ソーシャルメディアサービスの利用（対策基準 7.1(18)）

情報資産を所管する者は、ソーシャルメディアサービスの利用にあたり、外部サービスの利用に係る遵守事項に加え下記の事項を遵守すること。

ア　定義

X、Instagram、Facebook、YouTube、LINE など、インターネットを利用して利用者が情報を発

信又は相互に情報のやりとりを行うことができる情報伝達媒体をいう。

イ　アカウント運用ポリシーの策定

アカウント運用ポリシーを策定し、ソーシャルメディアのアカウント設定における自由記述欄又はソーシャルメディアアカウントの運用を行っている旨の表示をしている各課・学校等のＷｅｂサイトに掲載する。特に、専ら情報発信に用いる場合には、その旨をアカウント運用ポリシーに明示する。

ウ　取り扱う情報の範囲

（ア）機密性Ｂ以上の情報は、ソーシャルメディアサービスで発信してはならない。

（イ）可用性Ｂの情報の提供にソーシャルメディアサービスを用いる場合は、各課・学校等のＷｅｂサイトに当該情報を掲載して参照可能とすること。

エ　なりすまし対策

（ア） ソーシャルメディアの提供事業者がアカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得すること。

（イ） 各課・学校等のＷｅｂサイトに、利用するソーシャルメディアのサービス名とそのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記すること。

（ウ） アカウント名やアカウント設定の自由記述欄等を利用し、各課・学校等が運用していること及び当該アカウントの運用を行っている旨の表示をしている各課・学校等のＷｅｂサイトURL を利用者に明示すること。

オ　「アカウント乗っ取り」の防止

（ア） 教育庁サイバーセキュリティ安全管理措置に記載のパスワードポリシー（１２文字以上で、英字の大文字と小文字・数字・記号の中から少なくとも３種類を使うこと）を遵守し、パスワードを知る担当者を限定し、パスワードの使い回しをしないこと。

（イ） 二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。

（ウ） ソーシャルメディアへのログインに利用する端末を紛失した又は当該端末が盗難に遭った場合は、当該端末を悪用され、アカウント乗っ取りの可能性があるため、当該端末の管理を厳重に行うこと。

（エ） ソーシャルメディアへのログインに利用する端末が不正アクセスされた場合、当該端末が不正に遠隔操作される又は、当該端末に保存されたパスワードが窃取される可能性がある。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施すること。

カ　監視事務

情報資産を所管する者は、定期的に公式アカウントでの発信及び返信内容等をチェック（監視）すること。

キ　トラブルへの対応

トラブルが発生した場合は次のような対応をとること。

（ア）なりすまし、乗っ取り等の不正アクセス

・　各課・学校等のＷｅｂサイト内に、なりすましアカウントが存在することや当該ソーシャ

ルメディアを利用していないこと等の周知を行うとともに、信用できる機関やメディアを通じて注意喚起を行う。

・ ログインパスワードの変更やアカウントの停止を速やかに実施する。
・ サイバーセキュリティ管理者（課長又は校長）及び教育庁 CSIRT へ報告する。
・ なりすまし等により投稿された内容について、当該ソーシャルメディアの管理者に削除依頼を行う。

（イ）炎上

・ 反論や抗弁は控え、冷静に対応すること。
・ 問題になった部分を修正し、謝罪すること。
・ 対応に時間を要する場合はその旨を説明するなど、不要な誤解を招かないようにすること。

（ウ）事実と反するデマ的な内容が返信された場合

正しい情報を発信し、必要に応じてホームページへ誘導すること。

（エ）運用停止又は削除

アカウントの運用が困難と判断される場合は、教育庁 CSIRT へ一報するとともに、各課・学校　等のＷｅｂサイトに明記した上で速やかにソーシャルメディアを停止又は削除する。

ク　動画での情報発信

（ア）動画に対するコメントは書き込めないよう設定すること。
（イ）動画に対する評価ができないよう設定すること。
（ウ）上記ア・イまでが設定できない場合には、サイバーセキュリティ管理者（課長又は校長）の指示により適切に管理する。
（エ）生徒の作品等のアップロードを行う場合は当該生徒及び保護者から書面により承諾をもらい、校内で決裁を得た上で公開を行う。

ケ　その他注意事項

（ア）ＵＲＬ短縮サービスは、利用するソーシャルメディアサービスが自動的にＵＲＬを短縮する機能を持つ場合等、その使用が避けられない場合を除き、原則使用しないこと。
（イ）職員として自覚と責任を持った発言を行うこと。
（ウ）地方公務員法その他の関係法令並びに職員の服務及び情報の取扱いに関する規程を遵守すること。
（エ）基本的人権、肖像権、プライバシー権、著作権等に十分留意すること。
（オ）発信する情報は、正確に記述し、その内容について誤解を招かないよう留意すること。一度ネットワーク上に公開された情報は完全には削除できないことを理解しておくこと。
（カ）意図せず、自らが発信した情報により他者を傷つけたり、誤解を生じさせたりした場合は、誠実に対応するとともに正しく理解されるよう努めること。また、発信した情報に関し攻撃的な反応があった場合には、冷静に対応し、無用な議論は避けること。
（キ）職務上知り得た秘密や個人情報の取扱いに十分注意すること。
（ク）他の利用者の投稿を引用することや第三者が管理又は運用するページへのリンクの掲載は、当該投稿やページの内容を信頼性のあるものとして受け取られる可能性があることから、原則行わないこと。
（ケ）次に掲げる情報発信は、禁止する。

- 特定の個人や団体等を誹謗(ひぼう)中傷する内容
- 人種、思想、信条、職業等で差別、又は差別を助長する内容
- 違法行為、又は違法行為を助長する内容
- 職員の個人的見解や意見等
- 職務上知り得た秘密や個人情報
- 東京都及び第三者の権利を侵害する内容
- セキュリティを脅かすおそれのある内容
- 信ぴょう性・信頼性のない情報又は噂や風評等を助長させる内容
- 公序良俗に反する内容
- 施策の意思形成過程の未確定情報等（東京都が積極的に意見等を求める場合を除く。）
- 職員の身分以外の者に情報発信させること。
- その他、東京都教育委員会が不適切と判断するもの

11. 連絡用メール配信サービスの利用

情報資産を所管する者は、連絡用メール配信サービスの利用にあたり、外部サービスの利用に係る遵守事項に加え下記の事項を遵守すること。

ア　定義

利用者のメールアドレスをデータベース化し、インターネット環境があれば、どこからでもメール一斉配信が可能なサービスのこと。

利用者（児童・生徒及び保護者等）が予め各自でメールアドレス等を登録し、学校から配信されたメールを確認できる。

イ　運用方針の策定

連絡用メール配信サービス運用方針を策定し、必要に応じ利用者へ周知すること。

なお、別紙のとおり記載例を掲載する。

ウ　その他注意事項

（ア）利用に当たっては、希望者を対象とし、利用目的や利用方法等を明らかにした上で同意書等を徴取すること。利用を希望しない者に利用を強制しないこと。

（イ）利用を希望しない児童・生徒及び保護者等が不利益にならないよう代替手段を確保すること。

別紙

令和　年　月　日
（文書番号）号
東京都立●●学校長　●●　●●

都立●●学校
連絡用メール配信システム運用方針

1　利用目的
（1）地震等による災害時、天候による登下校時刻変更等を確実に連絡するため、一斉配信を行う。
（2）行事、部活動の日程変更などの連絡を利用対象者に配信する。

2　利用対象者
東京都立●●学校　生徒・保護者及び教職員
※ 利用を希望する生徒・保護者から利用についての同意をとる。

3　発信する機器
管理担当者 TAIMS 端末を基本とする。

4　サービスの提供事業者及びサービスの名称
株式会社●●　●●●●

5　サービスの提供事業者が定めた利用規約
別紙●●利用規約のとおり

6　利用料及び利用料の支出方法等
利用料単価●●●円※税別
生徒・保護者分は、私費（PTA）会計から支出する。
教職員分は、自律経営推進予算（役務費）から支出する。

7　トラブルが発生した場合の対応
伝達事項は、本システムに加え、本校のホームページにも記載する。電話回線が不通の場合等、本システムが有効に使用できない状況になった場合は、本校のホームページを閲覧するよう、保護者会や保護者宛通知を通じて周知する。

8　その他
（1）年度途中に転退学者が出た場合、年間契約のため利用料の返金は行わない。
（2）年度途中の転入者に対しては、料金の請求は行わない。
（3）年度途中に転退学者が出た場合、登録を削除する。
（4）年度途中、または在学中に登録先を変更する場合は、保護者が個別に変更する。
（5）東京都サイバーセキュリティポリシー等に則り、個人情報等機密性の高い情報は送信しない。
（6）緊急時・非常時のみの利用とし、教職員間の日常的な連絡には使用しない。