

平成 25 年 7 月 30 日

各府省庁情報セキュリティ担当課室長 殿

内閣官房情報セキュリティセンター
内閣参事官（政府機関総合対策促進担当）

外部委託に係る情報セキュリティ対策等について（注意喚起）

先般、政府機関において民間企業が提供するグループメールサービスを業務利用した結果、必要な情報セキュリティが確保されなかった事案が発生しました。本事案は、統一管理基準で定める府省庁外情報システムの利用及び外部委託における重要な情報の取扱い並びに情報セキュリティ上必要な措置について十分理解されていないことが原因の一つと考えられますが、民間企業が提供する外部の情報処理サービスの利用に際して注意すべき事項を十分認識していないことも考えられます。

このような状況を踏まえ、下記のとおり民間企業による役務の提供を受ける場合の情報セキュリティ上の注意事項について改めて取りまとめましたので、適切な対応をとっていただくようお願いいたします。

記

（１）約款による情報処理サービスを業務で利用する際の注意事項

① 機密情報を扱う業務におけるグループメールサービス等の利用の禁止

平成25年7月11日開催の情報セキュリティ対策推進会議（CISO等連絡会議）における議長指示「民間企業の提供する約款によるグループメールサービスを、機密情報を扱う業務に利用することのないよう、各府省庁の情報セキュリティポリシーを職員に徹底すること。」のとおりですが、グループメールサービス以外についても、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」という。）では、情報セキュリティに関する特約を個別に締結できない等の問題があるため、機密性を要する情報を扱う業務での利用は原則認められませんので、各府省庁における情報セキュリティポリシーの徹底を図るようお願いいたします。なお、国民への情報提供等の目的で公開情報を扱う場合については、約款による情報処理サービスの利用を妨げるものではありません。

・再発防止策等の徹底について（平成25年7月11日情報セキュリティ対策推進会議）
<http://www.nisc.go.jp/conference/suishin/ciso/dai11/pdf/2.pdf>

② レンタルサーバ利用時のバックアップの実施

約款による情報処理サービスでは、一般的に、データのバックアップまでは保証されておらず、利用者側の責任となっている場合がありますので、約款の内容を踏まえた上で適切なバックアップの実施の必要性を検討する必要があります。

・レンタルサーバ業者におけるデータ消失事象について（注意喚起）（平成24年6月29日）
http://www.nisc.go.jp/active/general/pdf/rentalsv_kanki_120702.pdf

（2）ソーシャルメディアを利用する際の注意事項

政府機関においてソーシャルメディアを業務で利用する場合、ソーシャルメディアの特性を踏まえた利用が求められます。

ソーシャルメディアは拡散性が高いという特徴がある一方で、その過程で誤った情報が付加されたり、一部の情報のみが切り取られたりすることで、本来の意図とは異なる形で情報が伝搬する可能性があります。また、ソーシャルメディアを運営する民間事業者の都合でサービスが一時的に中断又は廃止されたり、扱っている情報の取扱い方法が変更されたりすることもあります。これらの理由から、重要な公開情報については、自己管理のウェブサイトの主たる情報として掲載した上でソーシャルメディアの投稿を活用する等の対応が必要です。

また、ソーシャルメディアの利用時は、組織が管理するアカウントで運用し、職員個人が私的に取得したアカウントは、組織としての情報発信には利用しないよう注意が必要です。さらに、なりすましやアカウント乗っ取りについても対策が必要です。

政府機関においてソーシャルメディアを業務で利用する場合について、平成25年5月1日に「政府機関におけるソーシャルメディアの利用に係る情報セキュリティ対策等について（注意喚起）」にて、情報セキュリティ対策等に関する注意事項を示していますので、再度徹底をお願いします。

・政府機関におけるソーシャルメディアの利用に係る情報セキュリティ対策等について（注意喚起）（平成25年5月1日）
http://www.nisc.go.jp/active/general/pdf/social_media_130501.pdf

（3）アプリケーション及びウェブコンテンツ等を作成する際の注意事項

政府機関がアプリケーションやウェブコンテンツ等を作成し国民に提供する際には、情報システムの情報セキュリティ対策措置及び機密情報の取扱い等について、安全性に注意した取扱い措置が求められます。

以下に、政府機関が提供するアプリケーションやウェブコンテンツ等（以下「政府機関提供コンテンツ」という。）の作成を外部に委託する際、近年の新しい情報通信技術の利用形態の発展を踏まえ、特に注意すべき事項について示します。

① 利用者個人の行動を追跡する機能の組込みに関する注意

民間企業が提供するアプリケーションやウェブコンテンツ等においては、広告を提供する等の目的で利用者個人の行動を追跡するトラッキングという手法がよく用いられています。トラッキングに際してはクッキーや端末識別番号、URL短縮サービス等が利用されますが、トラッキングは、行動履歴という利用者のプライバシーに係る情報（以下「利用者情報」という。）の第三者提供につながりますので、政府機関提供コンテンツにおいては、国民のプライバシーを不当に侵害することのないよう注意する必要があります。

政府機関提供コンテンツの作成を民間企業に業務委託する場合、委託先がこの点に留意せず不用意に利用者情報を収集又は第三者提供するトラッキング機能を組込んでしまう事態が想定されます。政府機関提供コンテンツとして不適切なサービスが国民に提供されてしまうことがないように、業務委託時の契約において、利用者個人の行動を追跡する機能を不用意に組込まないように、発注仕様を明確にする等の措置が必要です。

② 政府機関提供コンテンツへの広告表示に関する注意

民間企業が提供するアプリケーションやウェブコンテンツ等では一般的に広告を表示させることが多いため、政府機関提供コンテンツの作成を民間企業に業務委託した場合に、委託先が故意又は不用意に政府機関提供コンテンツ内に広告を表示させる機能を埋め込む可能性があります。政府機関提供コンテンツにおいて広告を表示させる場合には、「国のウェブサイトへのバナー広告掲載要領」（関係省庁申合せ 平成24年6月25日改定。以下「掲載要領」という。）の規定に従う必要がありますが、民間企業においては、掲載要領に適合しない広告を用いることもあることから、委託先が不用意に広告を表示させる機能を埋め込むと、掲載要領に違反するコンテンツが表示されたり、前記①のトラッキング手法が用いられたりするおそれがありますので、注意が必要です。

政府機関提供コンテンツの作成を民間企業に業務委託する場合、広告を表示させる機能の埋め込みを業務委託時の契約において禁止する、又は、掲載要領に適合する広告のみが表示されるよう、発注仕様を明確にする等の措置が必要です。

③ 委託先に係る詳細の確認に関する注意

外部にアプリケーション等の開発を委託するにあたり、委託先や再委託先が、悪意のある不正プログラムを含む不適切なプログラムを故意又は不用意に組込むリスクについて注意する必要があります。

こういった不適切なプログラムの組込みについては、委託先事業者の所在地や、委託先で設計・開発に係る者の所属、専門性（資格等）、実績及び国籍等を確認する等の対

応を行うことが重要です。また、委託先が再委託する場合においても、再委託先の会社名、代表者名、所在地、及び主な出資者等について確認することを推奨します。

以 上

本件問い合わせ先
内閣官房情報セキュリティセンター
政府機関総合対策促進担当
山下、石原
(03-3581-3959)