事　務　連　絡
平成２５年５月１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）

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）

近年、インターネット上の様々なソーシャルメディアサービス（以下、「ソーシャルメディア」という。）の普及に伴い、政府機関においても、情報発信等を目的に、こうしたサービスの利用が増えています。一方で、先般、米国の通信社の公式ツイッターアカウントが乗っ取られ、虚偽の情報が発信される事案が発生するなど、ソーシャルメディアを狙った攻撃も顕在化しています。

万一、政府機関のソーシャルメディアのアカウントが攻撃者に乗っ取られ、虚偽の情報が発信された場合、国民生活等に大きな影響を及ぼすことが懸念されます。

こうした状況を踏まえ、内閣官房情報セキュリティセンターでは、ソーシャルメディア利用におけるなりすましやアカウント乗っ取りの防止等のために留意すべき事項を取りまとめましたので、各府省庁におかれては、これらの事項に十分留意し、ソーシャルメディアを利用するようお願いします。

なお、本事務連絡は、平成23年4月5日付け「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」（内閣官房情報セキュリティセンター、内閣官房情報通信技術（IT）担当室、総務省、経済産業省連名）をベースに、情報セキュリティの確保の観点から、新たに留意すべき事項を追加したものです。

記

（１）　ソーシャルメディアの特性を踏まえた利用

①　ソーシャルメディアを情報公開の主たる手段として利用しない

ソーシャルメディアは、以下のような特性があることから、原則として、国民に広く公開すべき情報の主たる公開手段としては利用せず、二次的・補助的な情報公開の手段として利用してください。

・　情報の閲覧がそのソーシャルディアの利用者に限られる場合があります。

・　ソーシャルメディアを提供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場合があります。

② 組織が管理するアカウントでの運用

ソーシャルメディアは、政府機関のような組織によるアカウントと、個人利用者のアカウントで同じ環境を利用することが多いため、情報発信が組織として行われていることを明確にする必要があります。また、後述する各種セキュリティ対策も、組織として対処する必要があります。このため、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でください。

③ 意図しないコミュニケーションが発生することを前提とした利用

ソーシャルメディアは、利用者間の相互コミュニケーションを促進するために、利用者の意見を表明しやすい環境となっています。このため、政府機関に対して、批判、苦情又は誹謗中傷が殺到してしまう、いわゆる「炎上」が発生したりする場合があります。

（２） なりすましの防止

① アカウントの運用組織の明示

政府機関からの情報発信であるかを明らかにするために、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、公的機関が運用していることを国民に明示することが必要です。

② 自己管理ウェブサイトとの相互リンク

政府機関からの情報発信であるかを明らかにするために、政府機関が自身で管理しているウェブサイト（.go.jpドメインが望ましい。以下、「自己管理ウェブサイト」という。）内において、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ページを設けるようにしてください。また、運用しているソーシャルメディアのアカウント設定の自由記述欄において、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自己管理ウェブサイト上のページのURLを記載してください。

③ 認証アカウント（公式アカウント）の利用

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、政府機関が利用するアカウントと、なりすまされたアカウントを区別する参考となるため、可能な限りこれを取得してください。

（３）アカウント乗っ取りの防止

第三者が何らかの方法で不正にログインを行い、偽の情報を発信する等の不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法については次のような適切な管理を行ってください。

① パスワードの適切な管理

以下に例示するような、パスワードの適切な管理を行ってください。

- ログインパスワードは十分な長さと複雑さを持たせる
- パスワードを知る担当者を限定する
- パスワードの使い回しはしない

② アカウント認証の強化策の利用

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、利用してください。

③ ログインに利用する端末の紛失・盗難の防止

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り盗難されたりした場合に、その端末を悪用されてアカウントを乗っ取られる可能性があるため、当該端末の管理は厳重に行ってください。

④ 使用する端末のセキュリティ確保

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ると、その端末が不正に遠隔操作されたり、端末に保存されたパスワードが窃取されたりする可能性があります。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アンチウイルス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してください。

（４）なりすましや不正アクセスを確認した場合の対処

① なりすましが発生していることを発見した場合

自己管理ウェブサイトに、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等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行ってください。

② アカウント乗っ取りを確認した場合

アカウント乗っ取りを確認した場合には、被害を最小限にするため、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し、自己管理ウェブサイト等で周知を行うとともに、自組織のCSIRTやNISCに報告するなど、適切な対処を行ってください。

（５） 発信又は公開する情報に関する留意事項

① 要機密情報の発信の禁止

要機密情報（機密性２以上に相当する情報）は発信しないでください。

② URL短縮サービスは使用しない

URL短縮サービスにより短縮したURLは、リンク先の本来のドメイン名が表示されず、利用者がドメイン名を判断材料にしてリンク先の安全性を確認することができなくなるため、URL短縮サービスは、原則使用しないでください。

③ リンク先の内容への留意

政府機関のアカウントにおいて、第三者アカウントの投稿の引用や、第三者が管理又は運用するページへのリンクを掲載することは、当該の投稿やページの内容を信頼性の

あるものとして認めていると受け取られることや、リンク掲載後に当該の投稿やページの内容が変更される可能性があることを考慮した上で、慎重に行うようにしてください。

④ 発信する情報の再確認

一旦発信した情報は、ソーシャルメディアを通じて瞬時に拡散してしまいますので、完全に削除することは不可能です。このため、当該情報が機密情報の漏えい等に繋がる可能性がないか等、情報発信する前にその影響を十分に再確認してください。

（６） 情報発信を円滑に行うための利用者への配慮

① アカウント運用ポリシーの策定と明示

- アカウント運用ポリシー(ソーシャルメディアポリシー)として策定してください。その際、以下の参考資料や他の公共機関・民間企業が公表しているものを参考にしてください。
- 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自己管理ウェブサイト上のページに、アカウント運用ポリシーを掲載してください。（自組織内にも周知しておくことが望ましい。）
- 特に、専ら情報発信用途に用いる場合には、その旨をアカウント運用ポリシーに明示してください。

(参考資料)

・法人における SNS 利用に伴うリスクと対策 (JPCERT コーディネーションセンター)
http://www.jpcert.or.jp/research/sns2012.html

・SNS の安全な歩き方 (日本ネットワークセキュリティ協会)
http://www.jnsa.org/result/2012/sns.html

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
横田、石原、古門
(03-3581-3959)