「政府機関の情報セキュリティ対策のための統一基準群」の現状及び見直しについて

景　山　忠　史

Current Status and Review of “Common Standards for Information Security Measures for Government Agencies and Related Agencies”

Tadashi KAGEYAMA

Abstract

The Common Standards Group(FY 2018),the collective term of “Common Standards for Information Security Measures for Government Agencies and Related Agencies” and Common Model, Guidance, and the Guidelines for establishing Standards, is regularly reviewed in response to changes in the security environment.

The review currently under consideration is uses of cloud services, and responding to the expansion of telework.

Expanding use of cloud services is progressing by “Cloud-by default principle”. Even on a small government agencies（including related agencies）uses Cloud information systems while ensuring security.

In a telework environment, it is necessary to ensure the security of the terminal equipment and network lines used because the information system is accessed from the outside such as at home.

In this paper, we analyzes these points and, although not included in the review items, advertising display on government agencies website.

Displaying advertisements on government agencies website, especially in programmatic advertisements, is not only the content of the displayed advertisements, but also the information of the accessing user is transmitted to the advertisement operator in terms of security.

Key Words

Cloud service, telework, programmatic advertisements

目　　次

はじめに

本稿では，政府機関における情報システム等に関するセキュリティ対策の一般的な基準である

「政府機関の情報セキュリティ対策のための統一基準群」（以下「統一基準群」という.）について，現在進められている見直し動向と，それ以外に見直しが期待される事項について論じる.

1　政府機関の情報セキュリティ対策のための統一基準群について

まず，統一基準群は，以下の複数の文書群の総称であり，すべての政府機関等において共通的に必要とされる情報セキュリティ対策であり，各機関の情報セキュリティ水準の斉一的な引き上げを図るために策定されている．いずれも，内閣サイバーセキュリティセンターのWebサイトにおいて全文が公開されている[1)].

政府機関「等」とは，国の行政機関のほかに，独立行政法人や，特にサイバーセキュリティ戦略本部が指定する法人（指定法人，日本年金機構や国家公務員共済組合連合会などが指定されている.）をも対象とする趣旨である．その意味で，中央省庁だけでなく，小規模な独立行政法人まで含む多様な主体に適用されるものとなっている.

この統一基準群は，定期的に見直しを行うこととされており，これまで概ね2年から3年程度を目安に改定が行われている.

サイバーセキュリティを巡る環境は日々更新されていくものではあるが，この統一基準群も参照しながら各政府機関等のセキュリティポリシーの見直しや情報システムの調達・更新等が行われることも勘案すると，頻繁に変更されていては各政府機関等での対応スケジュールが組みにくかったり，調達等に係る手続の過程における手戻りなどが発生する可能性もあるため，一定の期間ごとにまとめて改定が行われてきている.

もちろん，統一基準群は各政府機関・各情報システム共通の基準であることもあり，個々の政府機関等・個々の情報システムにおいてこれに特段の定めのない要素を盛り込むことも当然可能であり，その意味では統一基準群の改定がなされていないからという理由で，あるセキュリティ要素が盛り込めないといったことは生じない整理となっている（上述の統一基準群の位置づけの「すべての政府機関等において共通的に必要とされる」が，いわば最低限の基準であることを示している.）.

2　統一基準群の見直しの方向性について

この統一基準群の現行版は，2018年に改定された「平成30年度版」であるが，現在見直し作業がNISCにおいて行われており，2020年7月21日に開催されたサイバーセキュリティ戦略本部においてその見直し骨子が公表されている.

当該会議は，持ち回り開催であるとされており，議事録等は公表されていないが，特段の意見等はなかったものと考えられる.

この骨子の概要は以下のとおりである.（図①）

2.1　クラウドサービスに関する見直しについて

上述の見直しの方向性では，まず，「クラウドサービスの利用拡大を見据えた記載の充実」が掲げられている．政府機関等の情報システムにおいてもクラウドサービスの利用が進んできているが，従来のオンプレミス（個別の動作環境を準備して自らコントロールするもの）の情報システムとクラウドで構築・運用されるシステムでは，責任範囲が異なることが特徴として掲げられる.

オンプレミスのシステムでは，ネットワーク，サーバ等の機器，OSやミドルウェアを含むソフ

1)・政府機関等の情報セキュリティ対策のための統一規範
https://www.nisc.go.jp/active/general/pdf/kihan30.pdf
・政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）
https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf
・政府機関等の対策基準策定のためのガイドライン（平成30年度版）
https://www.nisc.go.jp/active/general/pdf/guide30.pdf
・政府機関等の情報セキュリティ対策の運用等に関する指針
https://www.nisc.go.jp/active/general/pdf/shishin30.pdf

サイバーセキュリティ戦略本部第25回会合（持ち回り開催） 2020年7月21日　資料3－1抜粋

政府機関等の情報セキュリティ対策のための統一基準群の見直しについて（骨子）

1．クラウドサービスの利用拡大を見据えた記載の充実

●政府情報システムのためのセキュリティ評価制度（ISMAP）の管理基準も踏まえ、クラウドサービス利用者側として実施すべき対策や考え方に係る記載を追加。
⇒外部サービスを安全に利用するために、業務内容や取り扱う情報の格付や取扱制限に応じた情報セキュリティ対策を自ら講じられることが重要。

2．情報セキュリティ対策の動向を踏まえた記載の充実

●政府機関等を標的とした主要なサイバー攻撃や近年の情報セキュリティインシデント事例、最新のセキュリティ対策などを踏まえた記載、また今後取り組むべき情報セキュリティ対策の将来像について記載。
⇒従来からの境界型防御を補完するものとして「常時アクセス判断・許可アーキテクチャ」にも目を向ける。また、情報システムの「常時システム診断・対処」を引き続き推進するなど、情報セキュリティ対策基盤を着実に進化させることが重要。

3．多様な働き方を前提とした情報セキュリティ対策の整理

●新型コロナウイルス感染症対策として政府機関等においても急速に広まったテレワークや遠隔会議の経験も踏まえ、係る多様な働き方を前提とする場合に必要な情報セキュリティ対策について、参照すべき統一基準上の規定や解説を整理することで、政府機関等が実施すべき対策の水準を明確にする。
⇒危機管理や働き方改革への対応として、通常とは異なる環境下においても必要な情報セキュリティ水準を確保した上で業務の円滑な継続を図ることが重要。

図①　サイバーセキュリティ戦略本部第 25 回会合（持ち回り開催）2020 年 7 月 21 日
https：//www.nisc.go.jp/conference/cs/dai25/pdf/25shiryou03.pdf

トウェアのすべてが政府機関等の管理下にあり，その意味でこれらすべての範囲の情報を政府機関等が有していることを前提に，当該政府機関等が責任をもってセキュリティ対策を講じることが可能であるが，クラウドサービスにおいては，特にパブリック・クラウドにおいて顕著であるが，政府機関等以外の者も含む複数利用者が共通してクラウド基盤を利用するため，他の利用者にも関係する情報については情報開示を受けることができないのが通常である．

そのため，統一基準群においても，「4.1.4　クラウドサービスの利用」において．

・国内法以外の法令が適用されるリスクを評価して判断すること
・クラウドサービスの中断や終了時に円滑に業務を以降するための対策を検討すること
・クラウドサービス部分を含む全体でセキュリティ要件を定めること
・クラウドサービスに対する各種認定・認証制度の適用状況などから信頼性を総合的・客観的に評価し判断すること

等の定めを置いている．

クラウドサービスの利用については，政府情報システムにおけるクラウドサービスの利用に係る基本方針（2018 年 6 月 7 日各府省情報化統括責任者（CIO）連絡会議決定）やデジタル・ガバメント実行計画（2019 年 12 月 20 日改訂（閣議決定））等において，クラウドサービス利用を徹底する方針，クラウド・バイ・デフォルトの原則（クラウドサービスの利用を第一候補として，政府情報システムの検討を行うこと）が定められ，新たに構築・更改する情報システムはまずクラウドサービスでの構築等が可能かどうかを検討し，著しく利用が困難であったり経費面の優位性も認められなかったりする場合にのみオンプレミスでの構築等を行うこととしている．

この方針のもとでは，小規模な政府機関等も含め，特に機密性の高い情報を扱うような例外的な場合を除いては，コストメリットの観点からもクラウドサービスの利用が増加していくことが見込

まれるが，上述の責任範囲の観点から，特にパブリック・クラウド（任意の組織で利用可能なクラウドサービスであり，リソースをクラウドサービス提供者が制御するもの）では具体的な情報セキュリティの確保のための措置を専らクラウドサービス提供者が実施することとなるため，統一基準群で求められるもの（又はそれ以外に当該システムに必要なセキュリティ対策として個々の政府機関等が要求するもの）を確保できるか否かは，クラウドサービス提供者が用意するセキュリティ水準に依存することになる．

そのため，当該クラウドサービス提供者が十分な情報セキュリティ対策を用意できる（契約書上で義務を課すというだけでなく，実際に確保できる体制があるかどうか）ということを確認する必要があるが，オンプレミスの場合と異なり，実際にハードウェアの設置状況を確認したりすることができないため，一定以上のセキュリティ水準にあるという信頼性について，何らかの方法で評価する必要がある．

ただし，このクラウドサービスの信頼性の評価というのは，各政府機関等が個々に行うのは困難であることもあり，統一的なセキュリティ要求基準が求められ，2020 年 1 月 30 日に「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」がサイバーセキュリティ戦略本部において決定され，「政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program：ISMAP（イスマップ））」が運用開始されている[2)]．（図②）

この ISMAP では，クラウドサービスに係る情報セキュリティ監査を行うことが認められる監査機関が公表されている，2020 年 8 月 20 日現在で，EY 新日本有限責任監査法人，有限責任監査法人トーマツ，有限責任あずさ監査法人，PwC あらた有限責任監査法人の 4 機関が指定されている．

現時点では，これら監査機関によって評価されたクラウドサービスリストは未だ公表されていないようであり，できるだけ早期の公表が望まれる．

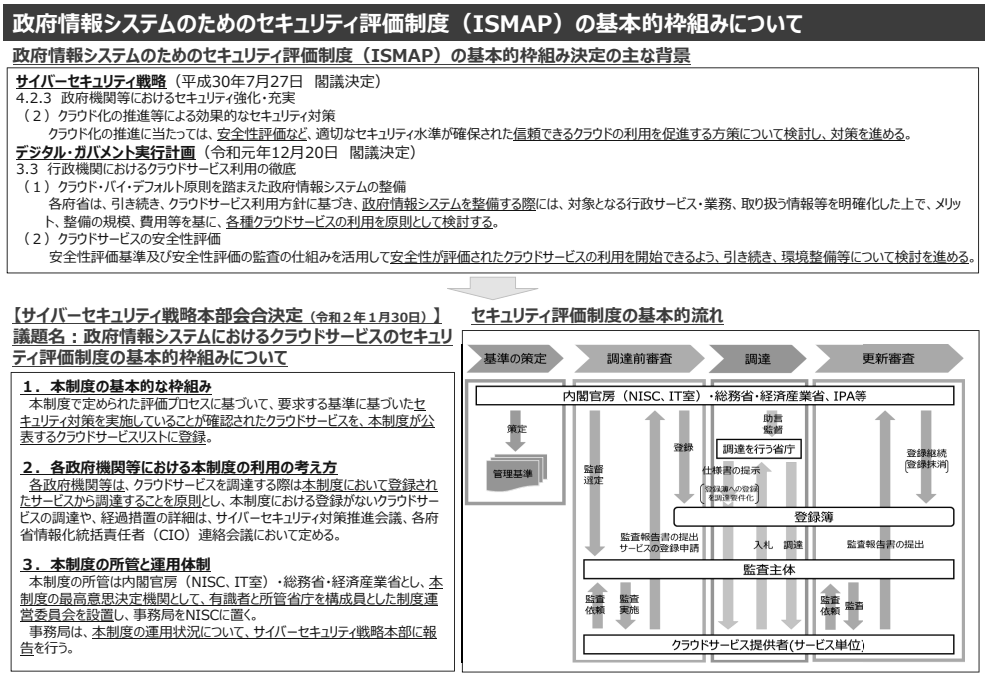
統一基準群の改定に際しては，これら ISMAP の取り組みを反映させ，実際に活用するための手引きとなる解説を追加することももちろんであるが，統一基準群の中で関連する部分である「4.1.2 約款による外部サービスの利用」の整理も望まれる．

この「約款による外部サービスの利用」は，民間事業者等が約款に基づいて一律に利用ルールなどを定めてインターネット上で提供しているサービスで，サービス提供者の提供するサーバ上で情報の作成や保存等を行うものであるが，具体例としては電子メール，ファイルストレージ，グループウェア等としており，情報システム全体をクラウド上に構築する場合というよりは，単一の機能を利用するような形態，例えば Web メールやスケジュール共有ツールの利用といったもの（それらのうち，典型的には無料で利用できセキュアな環境の保証を特にうたっていないもの）を念頭に置いていたことがうかがえ，そのために，原則として「要機密情報を取り扱わないこと」を前提とした定めが置かれている．

クラウドサービスも，「約款に基づいて一律に利用ルールなどを定める」サービスに該当するほか，約款による外部サービスもセキュアな環境下で提供されるものも増えてくるものと考えられることから，要機密情報を取り扱うこともあるという前提で，それに必要なセキュリティ環境として何をどこまで要求するのかを明確にすることが望まれる．

もちろん，セキュリティ水準の低いサービス上で要機密情報を取り扱うことを容認することは適当でないので，実際に提供されているサービス実態に基づき，各政府機関等が具体的な利用シーンに応じて検討するための手引きとなる記述である

2)　政府情報システムのためのセキュリティ評価制度（ISMAP）について
https：//www.nisc.go.jp/active/general/ismap.html



図②　政府情報システムのためのセキュリティ評価制度（ISMAP）の基本的枠組みについて
https : //www.nisc.go.jp/active/general/pdf/wakugumi2020_gaiyou.pdf

ことが必要である．

2.2　テレワークの拡大等に関する見直しについて

このほか，「多様な働き方を前提とした情報セキュリティ対策の整理」が掲げられている．これまでも，政府機関等においてもテレワークの実施や，海外を含む出張先での情報システムの利用については考慮されていたが，新型コロナウイルス感染症対策のために一層のテレワークの実施や，各種会議のオンライン開催が大幅に増加している状況を踏まえて，統一基準群の規定や解説を整理することが掲げられている．

「政府機関等においても，時間や場所に柔軟性を持たせた働き方の拡大が見込まれるところ，自宅もしくは自宅以外のワーキングスペース等でテレワークを行う際の情報セキュリティ対策について，参照すべき統一基準上の規定や解説を整理する」とされているのみで，具体的な改定箇所は明示されていないが，例えば，「8.2　機関等支給以外の端末の利用」などが想定される．

この箇所で規定されているのはいわゆるBYOD, Bring Your Own Device，個人で保有する端末を業務に利用する場合である．

この部分では，そもそもの利用の可否の判断，利用する場合のルール整備などが掲げられている，業務の中にも取り扱う機密性の大小はさまざまあり，例えば最終的に公表するための資料（プレスリリース資料など）の作成業務などは，その中に特に秘密としなければならないような情報が含まれていることは少なく（もちろん，作成過程で公表することが不適当であると判断されて削除される情報もあるため，全くないとは言えない），機関等支給以外の端末の利用を容認しやすいものと考えられる．

また，機関等支給以外の端末の利用という場合にも，ハードウェアとしては個人所有の端末を利用するものの，USB ブート型のシンクライアントを用いることで，実質的に政府機関等が必要とする制御下において利用させることができる．

この場合，通常個人で使用しているディスク装置から起動するのではなく，USB ポートに装着した USB メモリにインストールされた OS を起動し，政府機関等の情報システムに VPN 接続してリモートデスクトップ環境で利用することになる．

この OS 環境では稼働させている端末にデータを保存することを禁止し，データの作成や更新，削除等の操作は政府機関等のシステム内で処理することとなる．

従来，テレワークを行う場合にはあらかじめ申請した上で出勤時にオフィスにおいて利用している端末を自宅に持ち帰り，自宅のネットワーク環境に接続して（ここで VPN 接続するのが通常と考えられる）利用しているケースが通常であると考えられるが，この場合，機関等支給端末を通勤経路で持ち運ぶ必要があるため，紛失や盗難のリスクが生じる．これまでにも，通勤電車内で業務で使用していたタブレット端末の入った鞄を盗難にあったケースがある[3)]．

なお，上記のディスク全体の暗号化については，「情報セキュリティインシデント事例を踏まえた記載の追加」において，「暗号化消去（ディスク全体を暗号化し，その復号のための鍵を廃棄することによる論理的削除方法）にかかる解説を追加」とされており，今般の改定における対応が予定されている．

もちろん，USB メモリそのものも紛失等する可能性はあるが，その場合でも，速やかにシステム管理者へ報告させることとし，当該 USB メモリで起動した OS からのアクセスを遮断するなどの措置を講じることで，被害を防止することができる．各政府機関等の運用ルールの中にこのような点を明記することが望ましい．

（現在の統一基準群 8.1.1 情報システムの利用においても，USB メモリの利用に関する記述はあるが，これは電磁的記録媒体としての USB メモリの取り扱いに関するものであり，主に外部機関とのデータの受け渡しにおける利用において，あらかじめ機関等支給の USB メモリを使用することや，外部提供のメモリを用いる際はデータの読み書きに際して安全確保措置を講じること（USB メモリの読み書きに特化した端末の利用など）などを定めているものである．

上記のほか，「情報セキュリティ対策にかかる最新の考え方等の反映」として，「電子ファイルの受け渡し方法について，暗号化したファイルを電子メールに添付する場合は，直後にパスワードを電子メールで送付するのではなく，あらかじめ送付先との間でパスワードを電子メールとは別の方法で伝達することについて，より明示的な記載とする．」と掲げている．

これは，いわゆる PPAP の回避である．PPAP とは，（一財）日本情報経済社会推進協会（JIPDEC）の大泰司章氏が命名したとされている[4)]が，

P assword つき zip 暗号化ファイルを送ります
P assword を送ります
A　ん号化
P rotocol

の意であるとしており，電子メールに添付ファイルとしてパスワードで暗号化した zip ファイルを添付して送信し，その直後に解凍のためのパスワードを記載した 2 通目のメールを送信するとい

3）国交省航空局長，電車内でカバン置き引き被害 飲酒で寝過ごし…職員連絡網など流出
https : //www.sankei.com/affairs/news/150614/afr1506140012-n1.html
（2020 年 10 月 9 日閲覧）
このケースでは，端末にパスワードロックがかかっていたこともあり，情報漏洩があったか否かは定かではないが，ディスク全体を暗号化していない PC などではディスク装置のみを取り外してデータを読み取ることができる可能性がある．

4）（一社）日本インターネットプロバイダー協会　第 52 回 ISP＆クラウド事業者の集い in 旭川（2019 年 9 月 12 日・13 日）
くたばれ PPAP！　～メールにファイルを添付する習慣を変えるところから始める働き方改革～
一般財団法人日本情報経済社会推進協会大泰司章氏
https : //www.jaipa.or.jp/event/isp_mtg/asahikawa_190912-13/190913-3.pdf

う手順（プロトコル）を指している．

これは現在でも政府機関等からの電子メールによるファイル送付で実際に行われている方法であり，その意図としては添付ファイルの内容が第三者に閲覧されることを防ぐ趣旨と考えられる．

これは，電子メールに限らず，外部に情報を送付する場合に機密性３情報（秘密文書に相当する機密性を要する情報）については暗号化措置を施すべきものとされていること（情報の運搬・送信参照）を受け，電子メールの添付ファイルについて zip ファイルで圧縮してパスワードを設定することが広く行われ，この手順を失念することを避けるために，システムで自動的に一定程度複雑なパスワードを設定するとともに当該パスワードを別メールで送信することとしているためである．（自動的にではなく，手動で送信している場合ももちろん存在する）

これは，当該添付ファイルのみが転々流通したような場合には一定の効果が期待できるかもしれないが，解凍後のファイルについてはその効果はない．特に，パスワードの送付を「直後に」「同じ宛先への電子メールで」行うため，添付ファイルを受信できる者は必然的に２通目のパスワードを受信していることになり，実質的には同じメール内でパスワードを記述しているのと変わらないことになる．

電子メールによる情報漏洩のメジャーな事例として「宛先入力ミスによる誤送信」が挙げられるが，自動的にパスワード通知メールを送信してしまっては誤送信先にパスワードも送信してしまうことになる．（手動で送信する場合には，二通目のメールを送信する際に気づくことがあればそこで送信を中止することがわずかながら期待できるかもしれない）この意味では，機密保持としての実質的な効果は期待できないと言ってよい．

さらに，以下のような（特に受信する側の）デメリットがある．

・別メールのパスワードを確認して入力する必要がある
・暗号化されたファイルであるため，メールのフィルタリング等で書庫内のファイルの危険性を検知することができない（特にこちらのデメリットは，受信側のセキュリティリスクが高まってしまうため，暗号化されたファイルを受け取らないようルール化する場合も想定される）

統一基準群ではこのいわゆる PPAP を記述しているわけではなく，もちろん推奨しているわけではないが，実際に広く活用されている実態に鑑み，情報の送信にあたって望ましい方法について具体的な記述を置き，少なくとも PPAP は行わないことと明記するものと考えられる．

その他の方法としては，電子メールでファイルを送信する場合にはパスワードを別の経路で送付すること，例えば対面で伝達することや，書留等の郵便による送付なども考えられる．また，電子メールであっても，経路を変える（ファイルの送信に先立ってあらかじめやりとりしておく）ことも，効果は限定的であるが一定程度は期待できる．

ただし，これらの方法は，送信側における問題点は相当程度改善できるが，受信側の問題点，特に「暗号化されたファイルの危険性検知ができない」点は改善されない．また，送信側のリスクとしても，誤送信があった場合，暗号化されていてもそのパスワード桁数が小さい場合，ローカル環境下での総当たり攻撃を受けるリスクがある．これは，電子メールに添付されてファイルそのものが届いてしまう以上，「本来の受け手ではないはずの者のもとにファイルが保存されている」状態にあるからである．

これらを防ぐためには，大容量ファイル送信システムやオンラインストレージといったファイル送信専用のサービスを構築又は利用することが考えられる，メリットとしては，

・電子メールでは添付ファイルを誤ると相手にそのまま届いてしまうが，ファイル送信システムでは相手がダウンロードするまでは停止や差し替えが可能
・ダウンロードのためにファイル送信システムにログインが必要なため，（ログイン試行回数の制限などの適切な処理が施されていれば）総当たり

攻撃を防ぐことが可能
・ダウンロード時に受信側のシステムで危険性の検知が可能
といったものが挙げられる．

もちろん，メリットばかりではなく，ファイル送信システムを独自に構築する場合にはその構築や運用のコストが，外部のオンラインストレージサービスを利用する場合にはそのサービスそのものの信頼性の確認が，それぞれ必要になってくる（このオンラインストレージサービスは，通常「約款による外部サービス」にも該当する）．こういった点も踏まえて，政府機関等の実情に応じて適切な方法を選択できるようにするための考え方まで示した解説の充実が期待される．

3　見直し項目として掲げられていないが充実が求められる事項について

これまで掲げた改定項目には含まれていないが，より記載を充実すべき項目として，政府機関等のウェブサイトにおける広告表示に関する点が考えられる．

本件については，気象庁の気象情報を提供するウェブサイトにおいて広告表示を実施しようとしたが，直後に広告掲載基準に沿わない可能性がある広告が掲載されたとして一時停止することとなったという事案が発生している[5]．（広告掲載は2020年9月15日14時以降掲載としているが，翌日16日には停止しており，掲載された期間は1日に満たないと考えられる．9月30日現在でも掲載は再開されていない．）

本件は，直接的には気象庁の広告掲載基準への適合性の問題である（公的機関のウェブサイトに広告を掲載する際にどのような内容が許容されるのかはそれ自体検討が必要なテーマであるが，本稿では対象としない）が，今回気象庁が広告を掲載するに際して用いた「運用型広告」という手法については，それを実現する仕組みが情報セキュリティの観点からも問題になりうる．

運用型広告とは，一般的に，ウェブサイトの所有者が個別に広告主と契約するのではなく（例えば，公共機関の庁舎の掲示スペースにポスターを掲示するような場合，個別に承認を得た旨のシールや押印を付したりするが，それに近い仕組み），ウェブサイト所有者は広告の枠を一括して，広告運用受託事業者に委託し，気象庁が定める広告掲載基準[6]に合致するものを掲載するものと定めている．

この基準は，法令違反のおそれはもちろん，広く社会規範又は公序良俗に反するおそれのある内容を含むものを対象外とするとしており，相当程度厳しい基準となっていると考えられる．今回は，結果としてこの基準に抵触する広告が表示され，それを改善することが短期的には困難であったため，一律広告掲載を停止したものと想定される．

統一基準群では，ウェブサイトを含む「アプリケーション・コンテンツ」について，「6.3　アプリケーション・コンテンツの作成・提供」として，利用者の情報セキュリティ水準の低下を招くことを避けるために一定の対策を講じるべき旨を記述している．

その中で，「サービス利用に当たって必須ではない．サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないように開発すること」としており，具体的な解説として以下のように記述している．

5）気象庁ホームページへのウェブ広告掲載開始について（2020年9月11日）
http://www.jma.go.jp/jma/press/2009/11a/press_kokoku_20200911.html
（2020年10月9日閲覧）
気象庁ホームページへのウェブ広告掲載停止について（2020年9月16日）
http://www.jma.go.jp/jma/press/2009/16b/20200916_koukoku.html
（2020年10月9日閲覧）

6）気象庁HPの広告掲載基準
https://www.jma.go.jp/jma/kishou/info/besshi.pdf

（多少長いものの，該当項目全体を引用する．）

これに該当する典型的な例は，機関等のウェブサイトを構成する各 HTML ファイルの中に，機関等外のサイト（例として広告事業者の広告提供サーバ）のコンテンツを見えない形又は見える形で組み込むことで，機関等のウェブサイトの閲覧者のアクセス履歴を当該広告サーバへ自動的に送信する．いわゆる「トラッキング処理」を行う機能である．このとき，当該広告提供サーバが HTTP の cookie 機能を用いて閲覧する利用者に識別番号を付番している場合は，アクセス履歴等の，サービス利用に当たって必須ではない．サービス利用者その他の者に関する情報が，本人の意思に反して当該広告提供サーバを運営する第三者に提供されることになるので，本号はこのような機能がアプリケーション・コンテンツに組み込まれることがないようにすることを求めている．
また，トラッキング処理ではなくとも，例えば，利用者のキー入力の全てを当該利用者が意図しない形で送信するなどの機能も，「サービス利用に当たって必須ではない．サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能」に該当し得る．
なお，対象はウェブサイトの HTML ファイルに限られず，アプリケーションプログラムを提供する場合に，そのプログラムに含まれ得る機能についても同様である．
（統一基準群　遵守事項 6.3.1（2）（a）（カ）の解説より引用）

ウェブサイトの HTML の記述の中に，広告事業者の広告提供サーバのコンテンツが組み込まれることで，アクセス履歴を外部サービスに送信することについて，閲覧者本人の意思に反して提供されることのないように求めている．

今回の気象庁ウェブサイトの場合は，あらかじめ広告表示をする旨を予告し（とはいえ，周知から掲載開始までの期間が十分確保されていたかについては疑問点なしとしない），その運用方針についても明確に定めた上で実施しているため，サイトの閲覧者は運用型広告が表示されることを認識しうること，希望すればサイト上で広告表示をオフに設定できること[7]など，一定の措置は講じられていたものの，他の政府機関等が同様の検討を行おうとした場合に同等以上の措置を講じたうえで実施できるかどうかについては不安もある．

情報セキュリティの観点からは，運用型広告が，その仕組み上，個別の利用者に最適（と判断する）広告を動的に表示させるため，一定のアクセス履歴情報を利用するため，実際に表示される広告の内容（広告主としての妥当性だけでなく，利用者の情報を提供する相手方としての妥当性）を確保するためには運用型広告であったとしても相当程度広告主を限定する必要がある[8]．（注）

特に，気象庁ウェブサイトのように多数の訪問者があり広告媒体としての価値の高いサイトでない場合，広告掲載しようとする場合にできるだけ広告媒体としての価値が生かせるように運用型広告を検討する場合も想定される（運用する組織も小規模であることが想定される）ことから，そのような場合に検討すべき項目についての解説を充実させることが望ましいのではないか．

おわりに

以上，いくつかの論点について統一基準群の改定の方向性について論じてきたが，統一基準群はガイドラインも含めると 300 ページ超にもなる大部のドキュメントとなっており，全体を通して内

7）この点について気象庁側としては問題はないが，広告運用受託事業者としては広告主を募集する場合の大きな制約となりうる，ただし，この点もあくまで広告運営としての是非の問題である．

8）気象庁では，運用型広告ではなくあらかじめ広告主を絞り込む方法で 10 月にも再開する方向で検討しているとの報道がなされている．
気象庁 HP 広告，10 月にも再開 「運用型」やめ広告主絞り込み検討（2020 年 9 月 27 日）
https : //www.sankei.com/affairs/news/200927/afr2009270010-n1.html
（2020 年 10 月 9 日閲覧）

容を把握するために相当程度の労力を要するものとなってしまっている.

統一基準群の，全政府機関等において共通的に必要とされる情報セキュリティ対策を定めるという性格上，改定ごとに内容が大きく変更されるものではないが，新たな事項の追加を繰り返すことでどうしてもつぎはぎで記述される部分も増えてくるため，最新のセキュリティ動向を反映した部分と，従前から引き続き記載されている基本的な部分の見分けも徐々につきにくくなっていくものと考えられる.

情報セキュリティの確保のために必要な事項は年々増加していくのでむやみに軽量化を図る必要はないが，今後は，さまざまな政府機関等においてその組織の実情に応じて必要な項目を必要な範囲で参照できるよう，「統一基準群の読み方ガイド」のようなガイダンス資料が必要となってくるのではないだろうか.

特に，各政府機関等のシステム担当者は組織全体の責任者から個別システムの責任者まで多岐にわたり，一定期間でどんどん入れ替わっていくため，その組織・システムにとってさしあたって必要な項目を一瞥できるようにしておくことはトータルでの情報セキュリティを確保する体制の構築・維持に大きく資するものになると考えられる.