資料３

今年度のセキュリティポリシーガイドラインの改定内容について

総 務 省

令和８年 １月14日

総務省自治行政局住民制度課

サイバーセキュリティ対策室

令和７年度の改定内容について

■ 令和７年度のガイドラインの改定内容は、以下のとおり。
■ 地方自治法の改正に伴う対応として第１編の修正と対策基準の解説の内容について改定を予定。

検討テーマ

1. **電磁的記録媒体を使用しないデータ連携について**
   a. USBメモリ等を使用しないデータ連携
   b. USBメモリ等のリスクへの対処
2. **機器の廃棄･データ消去について**
3. **地方自治法改正に伴う対応**
4. **政府機関等の対策基準策定のためのガイドライン（令和７年度版）**
   令和７年９月５日 一部改定

→ 令和８年度の検討会において継続検討
→ **令和７年度改定（対策基準解説）**
→ **令和７年度改定（対策基準解説）**
→ **令和７年度改定（第１編総則）**
→ **令和７年度改定（対策基準解説）**

地方自治法改正に伴う大臣指針案とガイドライン（第１編総則）の構成比較

大臣指針案	新ガイドライン案（第1編総則）	現行ガイドライン（第1編総則）
第1　本指針の位置付け	第1章　本ガイドラインの目的等	第1章　本ガイドラインの目的等
新　本指針の位置づけ	ガイドラインの目的、経緯	ガイドラインの目的、経緯
第2　地方公共団体における情報セキュリティとその対策	第2章　地方公共団体における情報セキュリティとその対策	第2章　地方公共団体における情報セキュリティとその対策
地方公共団体における情報セキュリティの考え方		地方公共団体における情報セキュリティの考え方
情報セキュリティポリシーの必要性と構成	情報セキュリティポリシーの必要性と構成	情報セキュリティポリシーの必要性と構成
新 ・策定を要する方針及び方針の公表 ・方針を策定する必要がある主体		
情報セキュリティ対策の実施サイクル	情報セキュリティ対策の実施サイクル	情報セキュリティ対策の実施サイクル
第3　情報セキュリティの管理プロセス	第3章 情報セキュリティの管理プロセス	第3章　情報セキュリティの管理プロセス
自治法上の方針の策定及び導入	情報セキュリティポリシーの策定及び導入	策定及び導入
自治法上の方針の運用	情報セキュリティポリシーの運用	運用
自治法上の方針の評価・見直し	情報セキュリティポリシーの評価・見直し	評価・見直し
※改正法施行日（R8.4.1）までは、正式な「大臣指針」ではなく、地方公共団体の事務の便宜のために「大臣指針（案）」を発出済み	第4章以下　（略）	第4章以下　（略）

「政府機関等の対策基準策定のためのガイドライン」の一部改定（令和７年９月）

- 政府機関等のサイバーセキュリティ対策のための統一基準群（政府統一基準群）の構成要素である「政府機関等の対策基準策定のためのガイドライン」（以下「政府機関等策定ガイドライン」という。）の改定内容を一部ガイドラインに反映する。
- 「政府機関等策定ガイドライン」においては、大きな改定はされていないが、最近の脅威等を踏まえ、現行の総務省ガイドラインに記載がなく自治体のセキュリティ対策に有用な内容について追加する。

DNS設定情報を悪用する攻撃への対応

DNSに対する脅威や攻撃に関する記述と対策の追記

サービス不能攻撃に対する対策の追加

DNS設定情報を悪用する攻撃への対応

■ 「政府機関等策定ガイドライン」を参考にDNS設定情報を悪用する攻撃と対策について追記する。

現行：対策基準（解説）

6.5. 不正アクセス対策

（注１２）
庁外の者が地方公共団体の名前をタイトルに掲げるなどし、地方公共団体のウェブサイトと誤解されかねないウェブサイトを構築することがあり、これを完全に防ぐことは困難である。このため、以下を例とする対策を実施する必要がある。
（略）
・以前利用していたドメイン（旧ドメイン）を運用停止する場合は、第三者に再取得され元のウェブサイトへのアクセスを利用し、詐欺サイト等へ誘導されることのないようドメインを一定期間保持する。また、旧ドメインへのアクセスがあった際に後継となるサイト（後継サイトがない場合は終了を告知したページや団体トップページ等）へHTTP 応答コード301 を用いた転送を行うことで、旧ドメインが検索サイトの上位に表示される機会をできるだけなくすことが望ましい。

- **自治体セキュリティクラウドにおいては、CDNが必須機能要件であり、利用が浸透している**
- **設定情報が残ったままの場合、悪用されるリスクがある**

改定案：対策基準（解説）

6.5. 不正アクセス対策

（注１２）
庁外の者が地方公共団体の名前をタイトルに掲げるなどし、地方公共団体のウェブサイトと誤解されかねないウェブサイトを構築することがあり、これを完全に防ぐことは困難である。このため、以下を例とする対策を実施する必要がある。
（略）
・以前利用していたドメイン（旧ドメイン）を運用停止する場合は、第三者に再取得され元のウェブサイトへのアクセスを利用し、詐欺サイト等へ誘導されることのないようドメインを一定期間保持する。また、旧ドメインへのアクセスがあった際に後継となるサイト（後継サイトがない場合は終了を告知したページや団体トップページ等）へHTTP 応答コード301 を用いた転送を行うことで、旧ドメインが検索サイトの上位に表示される機会をできるだけなくすことが望ましい。
なお、ホスティングサービスやCDN（content delivery network）等を用いてウェブサイトを公開した場合、公開時に設定した当該ドメイン名に関するDNS設定を、終了時に速やかに削除する必要があることに注意が必要である。DNS設定が残ったままになっている場合、その設定を第三者に利用され、使用を終了したドメイン名を使って意図しないウェブサイト等を公開されてしまうサブドメインテイクオーバー・NSテイクオーバーと呼ばれる攻撃を受ける可能性がある。

DNSに対する攻撃への対応

■ 「政府機関等策定ガイドライン」を参考にDNSに対する攻撃と対策について追記する。

現行：対策基準（解説）

6.5. 不正アクセス対策

（１） 統括情報セキュリティ責任者の措置事項
使用されていないTCP/UDPポートや不要なサービスは、不正アクセスによる侵入や悪用に利用される可能性が高いため、ポート閉鎖やサービス停止処理を行う。
（注１）重要なファイルの改ざんについては、改ざん検知ソフトウェアの利用によって、不正アクセス、不正プログラムの侵入を検知することが可能である。
（注２）DNS の導入時には以下の対策を講じなければならない。
・庁外からの名前解決の要求に応じる必要性があるかについて検討し、必要性がないと判断される場合は庁内からの名前解決の要求のみに応答をするよう措置を講じる。
・DNS キャッシュポイズニング攻撃から保護するための措置を講じる。
・キャッシュサーバにおいて、ルートヒントファイル（DNS ルートサーバの情報が登録されたファイル）の更新の有無を定期的（３か月に一度程度）に確認し、最新のDNS ルートサーバの情報を維持する。

- **オープンリゾルバに関する記述の追加**
- **DNSを悪用されるサービス不能攻撃（DNS水責め攻撃・DNSリフレクター攻撃）を追記**

- **DNSキャッシュポイズニング攻撃に対する対策を追記**

改定案：対策基準（解説）

6.5. 不正アクセス対策

（１） 統括情報セキュリティ責任者の措置事項
使用されていないTCP/UDPポートや不要なサービスは、不正アクセスによる侵入や悪用に利用される可能性が高いため、ポート閉鎖やサービス停止処理を行う。
（注１）重要なファイルの改ざんについては、改ざん検知ソフトウェアの利用によって、不正アクセス、不正プログラムの侵入を検知することが可能である。
（注２）DNS の導入時には以下の対策を講じなければならない。
・庁外からの名前解決の要求に応じる必要性があるかについて検討し、必要性がないと判断される場合は庁内からの名前解決の要求のみに応答をするよう措置を講じる。**庁外からの不特定多数に名前解決の要求応じるキャッシュサーバは、オープンリゾルバと呼ばれる。オープンリゾルバに対し存在しないホスト名の名前解決の問合せを大量に送信することで当該ホスト名の名前解決に関係するDNSサーバの過負荷を狙うランダムサブドメイン攻撃（DNS水責め攻撃）や、送信元IPアドレスを偽った問合せを大量に送信することで応答を攻撃対象に送り付け、サービス不能の状態にすることを狙うDNSリフレクター攻撃といったサービス不能攻撃等の踏み台として悪用される危険性がある。そのため、オープンリゾルバの制限やDNSの監視等が重要となる。**
・ DNSのキャッシュサーバに偽の応答をキャッシュさせることで、利用者のアクセスを攻撃者が用意したサイト等に誘導するDNS キャッシュポイズニング攻撃から保護するための措置を講じる。**DNSキャッシュポイズニング攻撃対策として、名前解決におけるIPフラグメンテーションの発生を回避するため、コンテンツサーバ及びキャッシュサーバのUDPメッセージサイズの上限を1,232バイトに設定することが望ましい。**
（続く）

DNSに対する攻撃への対応

■ 「政府機関等策定ガイドライン」を参考にDNSに対する攻撃と対策について追記する。

現行：対策基準（解説）

6.5. 不正アクセス対策

- **DNSキャッシュポイズニング攻撃に対する対策を追記**

改定案：対策基準（解説）

6.5. 不正アクセス対策

（続き）

また、UDPポート番号をランダム化することにより、攻撃者がキャッシュポイズニング攻撃を行う際にUDPポート番号の推測を困難にすることができ、攻撃の成功確率を低下させることが可能となる。その場合、キャッシュサーバからコンテンツサーバへの問合せにおいて、通信経路上のファイアウォールにてネットワークアドレス変換（NAT）処理が行われる場合、UDPポート番号が推測可能な形に変換されてしまうことのないように留意が必要である。
さらにコンテンツサーバの応答に追加された電子署名をキャッシュサーバがその検証を行うDNSSECにより、応答が改ざん等されていないか確認することができる。DNSSECは、公開鍵暗号技術を用いるため、その導入には情報の提供側であるコンテンツサーバと情報の問合せ側であるキャッシュサーバの双方に対応が必要となる。

・キャッシュサーバにおいて、ルートヒントファイル（DNS ルートサーバの情報が登録されたファイル）の更新の有無を定期的（３か月に一度程度）に確認し、最新のDNS ルートサーバの情報を維持する。

（続く）

サービス不能攻撃に対する対策

■ 「政府機関等策定ガイドライン」を参考にサービス不能攻撃の対策について追記する。

現行：対策基準（解説）

6.5. 不正アクセス対策

（６） サービス不能攻撃
（略）
①情報システムを構成する機器の装備している機能による対策の実施
・サーバ装置、端末及び通信回線装置について、サービス不能攻撃に対抗するための機能が実装されている場合は、これらを有効にする。

- **サービス不能攻撃に対抗するための機能における具体的な機能について追記**

改定案：対策基準（解説）

6.5. 不正アクセス対策

（６） サービス不能攻撃
（略）
①情報システムを構成する機器の装備している機能による対策の実施
・サーバ装置、端末及び通信回線装置について、サービス不能攻撃に対抗するための機能が実装されている場合は、これらを有効にする。

パケットフィルタリング機能は、通信パケットのヘッダ部の情報（送信元および送信先のIPアドレス、ポート番号、通信プロトコル等）を条件として、パケットの許可/遮断を行う機能である。これにより、攻撃に利用されているIPアドレスが明らかになっている場合、攻撃を遮断することが可能である。

3-way handshake時のタイムアウトの短縮は、TCP通信時に用いられる3-way handshakeの一連の通信（通信の可否確認、通信の可否応答、通信セッションの確立）の上限時間を短縮することにより、DDoS攻撃によって大量の通信セッションが同時に確立されサーバ等のCPUやメモリ等のリソースがひっ迫することを防止する方法である。

各種Flood攻撃への防御は、3-way handshakeの仕組みを悪用したSYN FloodやACK Flood、DNS通信において問い合わせパケットに比べて応答パケットのサイズが大きくなることを悪用したDNS Flood等に対する防御である。具体的な方法として、帯域制限機能により特定のIPアドレスからの一定時間内の通信数の上限を設定したり、アラート機能によりサーバ等のCPUやメモリ等のリソースひっ迫を検知し攻撃を遮断し一時的にリソースを増強する機能等がある。

アプリケーションゲートウェイ機能は、パケットフィルタリング機能で用いるヘッダ部の情報のみならず、通信の本体部（ペイロード部）を条件として、パケットの許可/遮断を行う機能である。

今年度の改定までのスケジュール（大日程）

- 自治体への意見照会期間を**４週間**確保するものとする。
- 意見照会の結果を反映したガイドライン改定案を第21回検討会で提示する。

項目	令和7年度		
	1月	2月	3月
ガイドライン改定案の提示（一部）	第20回 検討会		
ガイドライン改定案の修正	→	→	
自治体意見照会		→	→
意見照会の反映			→
最終版のガイドライン改定案の提示			第21回 検討会
ガイドラインの改定（予定）			★