資料１

自治体意見照会等の結果と
今年度のガイドライン改定案について

総 務 省

令和８年 ３月16日

自治行政局住民制度課

サイバーセキュリティ対策室

自治体意見照会等の実施概要・結果

前回の検討会で示した「地方公共団体における情報セキュリティポリシーに関するガイドライン」改定案を全国の自治体へ提示し、意見照会を行った。「機器の廃棄・データ消去」については、専門的な観点による確認が必要なことから事業者に対しても意見照会を行った。

１．自治体意見照会

（１）実施概要

項目	内容
期間	令和８年２月２日～令和８年２月26日
対象	全都道府県及び全市区町村
提示資料	地方公共団体における情報セキュリティポリシーに関するガイドライン改定案及び機器廃棄・データ消去に関する補足資料

（２）意見照会の実施結果（提出状況）

	提出団体数	意見数	質問数	その他※
都道府県	８団体	３４件	６件	３件
市区町村	２０団体	２３件	２０件	２件
計	**２８団体**	**５７件**	**２６件**	**５件**

※本照会以外に関する意見・質問（実施手順等の雛形の提示の検討や表現等の修正に関する意見や質問）

２．事業者意見照会

「データ適正消去実行証明協議会（Association of Data Erase Certification：ADEC）※」に対して、「機器の廃棄・データ消去」に関するガイドライン改定案及び補足資料に関する意見照会を行ったところ、表現等に関する内容について意見を頂いた。

※データの適正な消去のあり方を調査・研究し、その技術的な基準を策定するとともに、これに基づいてデータの適正消去が実行されたことを証明するための第三者的な証明制度の普及・啓発を図り、もって我が国における健全で安心安全な循環型IT社会の実現に寄与することを目的として設立された協議会（ADEC Webサイトより引用）

主な自治体の意見（１）

「機器の廃棄・データ消去」に関する意見（表現等に関する意見）が多かった。意見の一部については、ガイドライン及び参考資料として提示予定の「補足資料」に反映を行う。

項目（カテゴリ）	件数	主な意見の例	対応
機器の廃棄・データ消去①	1	補足資料「現行のガイドラインと改定案の比較（機器の廃棄）」の箇所：「マイナンバー利用事務系の領域において住民情報を保存する記録媒体」の箇所に示された（除去を行う際の）専用コマンドと「自治体機密性１に該当する情報を保存する記録媒体」の箇所に示された（消去を行う際の）**専用コマンドの違いが不明確**であり作業に混乱を招くのではないか。	**補足資料修正** 以下に修正する ・除去専用コマンド ・消去専用コマンド →補足資料5P
機器の廃棄・データ消去②	7	補足資料「その他（暗号化消去について）」の鍵を確実に消去する手順に関する記載の箇所：**鍵のバックアップが多岐にわたる場所に保存されている可能性がある**ため、すべて破棄するための手順とするべき。また、**BitLockerは暗号鍵ではなく回復キーという表現が一般的**なため誤解を招かない表記とすべき。	**補足資料修正** 消去手順を追記 回復キー、ロック解除キーに関する説明を追記 →補足資料28P～30P
機器の廃棄・データ消去③	1	補足資料「現行のガイドラインと改定案の比較（職員の作業立ち合い）」の箇所：**「データ消去作業」と「データ消去」**と表現されているが、誤解が生じないよう表現を変更した方が良いのではないか。	**補足資料修正** データ抹消作業に修正 →補足資料14P
機器の廃棄・データ消去④	2	補足資料「記録媒体の廃棄方法」の箇所：ハードディスクの消磁によりサーボトラック（データの読み書きに必要な位置決め情報）が損傷し、デバイスそのものが動作不能となる可能性があるため、**リユース不可の場合がある旨を記載**すべきではないか。	**補足資料修正** 消磁はリユース不可の可能性があることを追記 →補足資料7P,8P,11P
機器の廃棄・データ消去⑤	2	「図表43確実な履行を担保する方法」の箇所：「作業を委託する場合 」の庁舎内で除去作業時の職員の立ち会いで「データが復元できないことを目視で確認する」と表現されているが、復元の確認は困難なため、「**指定した方法で実施したことを目視で確認**」とするのはどうか。	**ガイドライン修正**

主な自治体の意見（２）

項目（カテゴリ）	件数	主な意見の例	対応
機器の廃棄・データ消去⑥	2	「図表43確実な履行を担保する方法」の破壊、除去における「作業を委託する場合」の箇所：「委託事業者先で破壊作業を行う場合は、職員は、庁舎内において（３）に記載する方法によりデータ抹消を実施したことを目視で確認し」との記載があるが、（３）の抹消方法である**「消去」と記載**した方がよりわかりやすいのではないか。	**ガイドライン修正**
機器の廃棄・データ消去⑦	1	データを抹消する際は、データが格納される「フラッシュメモリチップ」や「NANDフラッシュチップ」を細断する必要があるため、図表41の「フラッシュメモリデバイス」という表現を「**フラッシュメモリチップ**」と表記とすべきではないか。	**ガイドライン修正**
		図表41、42、43で「ハードディスク」、「HDD」の表記が混在しているので**表現を統一**した方が良いのではないか。	**ガイドライン修正**
その他	1	対策基準「7.5. 法令遵守」の関係法令一覧の箇所において、自治法改正に伴い方針を定める公表する義務が生じているため、**地方自治法**を加えてもいいのではないか。	**ガイドライン修正**

令和８年３月のガイドライン改定（予定）のポイントについて

1.地方自治法改正に伴う対応

■ 令和６年の地方自治法の改正に伴い、大臣指針案が令和７年４月１日付で発出されており、ガイドライン第1編総則において記載内容が重複する箇所等について削除等を実施。

2. 機器の廃棄･データ消去について

■ 「政府機関等の対策基準策定のためのガイドライン」を参考にマイナンバー利用事務系の領域において住民情報を保存する記録媒体における機器の物理的破壊について、機器のリユース（再利用）が困難になることやコスト等の課題があることから、物理破壊以外の方法を追加。また、データ消去作業の職員の立ち合いを行う範囲を明確化。

3. USBメモリ等の利用におけるリスクへの対処

■ 「政府機関等の対策基準策定のためのガイドライン」と総務省のガイドラインを整合した上で不足している対策について追記。

４.その他

■ 「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）」を踏まえ、DNS設定情報を悪用する攻撃等について追記。

※ 上記2･3については第3編 対策基準（解説）を改定。
※ 地方公共団体における情報セキュリティ監査に関するガイドラインについては時点更新と形式修正のみ。

「機器の廃棄・データ消去」のガイドラインの改定案の修正（１）

図表42 情報の機密性に応じた機器の廃棄等の方法

分類	抹消方法	機器の廃棄等の方法	
（２）自治体機密性２以上に該当する情報を保存する記録媒体 （上記（１）に該当するものを除く。）	破壊	ハードディスク	当該媒体を細断するなどして情報を記録している内部の円盤を物理的に破壊する必要がある。ハードディスクの場合、筐体に対して不適当なサイズの円盤を組み込んでいるものが存在しており、穿孔する際は、円盤を確実に損傷するため多点方式で最下層の円盤まで損傷を与えることができる専用破壊装置を利用する必要がある。
		SSD	当該媒体を切断するなどして情報を記録している内部のメモリチップを破壊する方法が例として挙げられる。ハードディスク向けの一般的な物理的破壊方法では、裁断の細かさ等の点からフラッシュメモリ媒体を完全には破壊できないため、専用の破壊装置を使用し、メモリチップを破壊する必要がある。
		USBメモリ	
		光学媒体	• メディアシュレッダーやメディアクラッシャー等の専用の機器にて記録層を破壊
	除去	ハードディスク	• 暗号化消去 • ATA コマンドの~~「Enhanced SECURITY ERASE UNIT」~~「SECURITY ERASE UNIT」コマンドを「Enhanced Erase mode」で使用 • SCSIコマンドの「SCSI SANITIZE」コマンドや「SCSI Format」コマンドを使用 • 消磁
		SSD	• 暗号化消去 • ATA コマンドの「BLOCK ERASE」コマンドを使用 • SCSIコマンドの「SCSI SANITIZE」コマンドや「SCSI Format」コマンドを使用 • NVMe（PCIe）コマンドの「NVM Express Format」コマンドや「NVM Express SANITIZE」コマンドを使用
（３）自治体機密性１に該当する情報を保存する記録媒体 （ハードディスク、USBメモリ、SSDにおいては、上記（２）の抹消方法の除去選択も可）	破壊	光学媒体	• メディアシュレッダーやメディアクラッシャー等の専用の機器にて記録層を破壊
	消去	ハードディスク	• データ抹消ソフトウェア（もとのデータに異なるランダムなデータを1回以上、上書きすることでデータを消去するソフトウェア）によりファイルを抹消する方法
		USBメモリ	• データ抹消ソフトウェア（もとのデータに異なるランダムなデータを２回以上、上書きすることでデータを消去するソフトウェア）によりファイルを抹消する
		SSD	• データ抹消ソフトウェア（もとのデータに異なるランダムなデータを２回以上、上書きすることでデータを消去するソフトウェア）によりファイルを抹消する • ATAコマンドの「SECURITY ERASE UNIT」コマンドを「Normal Erase mode」で使用する方法

（事業者意見）
一般的な表現に変更した方が良いのではないか

（事業者意見）
一般的な表現に変更した方が良いのではないか

「機器の廃棄・データ消去」のガイドラインの改定案の修正（２）

図表43 確実な履行を担保する方法

分類	抹消方法	確実な履行を担保する方法	
（１） マイナンバー利用事務系の領域において住民情報を保存する記録媒体 ※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ	破壊	各抹消方法における履行の担保	細断、切断等による抹消 • 細断、切断等の手法により、データを格納した記録媒体を完全に破壊する。 • 細断による破壊はデータの取得ができない大きさまでデバイスを破壊する。 • HDDを穿孔する場合は、専用の破壊装置を利用する。 • SSDやUSBメモリを破壊する場合は、専用の破壊装置やシュレッダーを利用する。 • 光学媒体の場合は、光学媒体の記録層を破壊可能なメディアシュレッダーやメディアクラッシャー等を利用する。
		作業手続きにおける履行の担保	作業場所等 • 庁舎内又は委託事業者先において破壊作業を実施する。 • 多数の破壊対象の端末を庁舎内の一室に一時保管する必要がある場合は、保管端末の一覧を作成するとともに、保管場所を施錠するなど、端末の紛失防止対策を講じること。 • 特定個人情報等が記録された電子媒体を管理区域又は取扱区域から外へ移動させる場合には、「特定個人情報に関する安全管理措置（行政機関等編）」を遵守する。 作業を委託する場合 • 庁舎内で破壊作業を行う場合は、職員は、当該作業に立ち会うなどして、~~**データが復元できないことを指定した方法で破壊したことを**~~目視で確認するとともに、作業記録を作成する。 • 委託事業者先で破壊作業を行う場合は、職員は、庁舎内において~~**（３）に記載する方法によりデータ抹消**~~**（３）に記載する「消去」によりデータ抹消**を実施したことを目視で確認し記録を作成した上で、委託事業者に引き渡す。破壊作業完了後、職員は、委託事業者が提出する完了証明書により作業内容を確認する。 • 当該完了証明書については、あらかじめ契約により、破壊処理の前後が確認できる証拠写真及び記録媒体のシリアルナンバーの添付並びに提出期限を定めておくこと。

以降同じ記載箇所について同様に修正

「機器の廃棄・データ消去」のガイドラインの改定案の修正（３）

ガイドライン改定案（新規図表41 データ抹消方法）

（事業者意見）具体的な大きさを示すことが難しいため削除した方が良いのではないか

抹消方法	説明	残存リスク等
破壊 **表現の修正**	• 細断、切断などの手法によりデータを格納した記録媒体を完全に破壊する。 ~~• HDD~~**ハードディスク(以下、「HDD」という。)**は、情報を記録している内部の円盤を物理的に破壊する必要がある • フラッシュメモリベースのストレージデバイス(以下、「SSD」という。)は、ハードディスク向けの粉砕シュレッダーでは、細断の細かさ等の点からフラッシュメモリ~~チップデバイス~~**チップデバイス**を完全には破壊できない。確実に内部の~~チップデバイス~~**チップデバイス**を破壊すること。	• 一般的な物理破壊装置では、~~細断の大きさにより~~**細断の大きさにより**破片から記録された情報を読み取ることでデータの復元の可能性がある。（専用の破壊装置やHDD/SSDシュレッダーを利用） • 穿孔する際は、専用の破壊装置を利用しないと、円盤に損傷を与えられないことや、最下層の円盤まで損傷を与えることができない点に注意が必要である。
除去	• 記録媒体専用のコマンドを使用して記録媒体の全エリアを抹消する。 • その他の抹消方法として、復号鍵の~~消去~~**消去抹消**（以下、「暗号化消去」という。）、消磁等の手法がある。 **（事業者意見）故障時は専用コマンドを利用できない可能性があることを追記するのはどうか**	• 記録媒体を機器から取り出し、直接記録媒体内の読み取りを行ったとしてもデータの復元は不可能。 • 記録媒体によっては、専用コマンドがサポートされていない場合がある。 • 専用コマンドが正常に動作し、除去が完了したか確認が必要。**故障時は専用コマンドを利用できない可能性があることに留意する。**
消去 **（事業者意見）ストレージの上書きは“その領域に新しい値を書き込む”動作であり、その値が 00 でも 01 でも FF でも、元のビットは上から完全に書き換えられるため01に限った記載を削除した方が良いのではないか**	• データ抹消ソフトウェア、記録媒体専用のコマンドを使用しOS 等からアクセス可能な領域を抹消する。 • 利用者がアクセス可能な全てのストレージ領域を非機密データ~~（01）~~で上書き~~（以下、上書き消去という）~~、対象のデータを非機密データにする。	• 一般的に入手可能な復元ツールの利用によるデータの復元は困難。 • OSから認識できない領域のデータは抹消されない。 • 記録媒体を機器から取り出し、直接記録媒体内を読み取りを行うことでOSから認識できない領域のデータの復元は可能。 • SSDの場合はOSからアクセスできない領域にデータが残るため、SSDからフラッシュメモリデバイスを取り出し直接、データを読み取ることで、元のデータを復元できる可能性がある。

「機器の廃棄・データ消去」のガイドラインの改定案の修正（４）

図表44　暗号化消去における留意事項

項目	留意事項
暗号化消去の前提条件	• 情報を記録媒体に格納する前に記録媒体の暗号化機能を有効にしておく。 • 記録媒体の暗号化機能が有効にされていない状態で情報を保存しない。
暗号の強度	• CRYPTREC暗号リスト（電子政府推奨暗号リスト）に記載されている強度の強い暗号アルゴリズムを使用する。
鍵の**削除消去**	• 鍵を確実に消去する。 • 鍵のバックアップがある場合は、バックアップも消去する。
暗号消去操作の記録	• 暗号化消去を実施したことを記録に残す。【記録の例】（実施日、記録媒体名、製造メーカー、シリアル番号、暗号方法（暗号化ソフト、バージョンなど）、実施者、確認者等）

（事業者意見）鍵の削除、消去と表記が複数あるので、統一した方が良いのではないか

「機器の廃棄・データ消去」のガイドラインの改定案の修正（５）

■ 情報システムの更新において移行元のデータを確実に抹消を行うことが重要である旨を「情報資産の廃棄」の解説に追加（赤字の箇所）。

現行：対策基準（解説）

2. 情報資産の分類と管理

（２）情報資産の管理
（前略）
③情報の作成～⑩情報資産の廃棄
（略）
（注９）情報の提供や公表に当たっては、情報漏えいを防ぐため、文書の作成者名、組織名その他の記録に使用できる「プロパティ」や、文書の作成履歴、PDFファイルの「しおり」等に残留した不要な情報を除去する必要がある。また、ソフトウェアを用いて文書の特定部分（提供・公表不可の情報が記載された部分）の情報を黒塗りして提供・公表する場合があるが、当該文書を入手した者が編集ソフト等を用いて黒塗り部分の情報の閲覧を試みる場合があるため、黒塗りされた部分の情報の削除や置換を行うなど、適切に措置する必要がある。

改定案：対策基準（解説）

2. 情報資産の分類と管理

（２）情報資産の管理
（前略）
③情報の作成～⑩情報資産の廃棄
（略）
（注９）情報の提供や公表に当たっては、情報漏えいを防ぐため、文書の作成者名、組織名その他の記録に使用できる「プロパティ」や、文書の作成履歴、PDFファイルの「しおり」等に残留した不要な情報を除去する必要がある。また、ソフトウェアを用いて文書の特定部分（提供・公表不可の情報が記載された部分）の情報を黒塗りして提供・公表する場合があるが、当該文書を入手した者が編集ソフト等を用いて黒塗り部分の情報の閲覧を試みる場合があるため、黒塗りされた部分の情報の削除や置換を行うなど、適切に措置する必要がある。
（注10）情報システムの更新等においてデータを移行する際は、移行完了後に移行元の機器やクラウドサービスにおけるデータを抹消する必要がある。データの抹消方法について本ガイドラインの第３編（第２章4.1. サーバ等の管理（７）機器の廃棄等）を参照されたい。

その他（自治法の改正）に関するガイドライン改定案の修正

現行：対策基準（解説）

7.5. 法令遵守

（略）
①地方公務員法(昭和25年法律第261号）
②著作権法（昭和45年法律第48号）
③不正アクセス行為の禁止等に関する法律（平成11年法律第128号）
④個人情報の保護に関する法律（平成15年法律第57号）
⑤行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）
⑥サイバーセキュリティ基本法（平成26年法律第104号）
⑦○○市個人情報保護法施行条例（令和○○年条例第○○号）

改定案：対策基準（例文）

7.5. 法令遵守

（略）
①地方自治法（昭和22年法律第67号）
~~①~~②地方公務員法(昭和25年法律第261号）
~~②~~③著作権法（昭和45年法律第48号）
~~③~~④不正アクセス行為の禁止等に関する法律（平成11年法律第128号）
~~④~~⑤個人情報の保護に関する法律（平成15年法律第57号）
~~⑤~~⑥行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）
~~⑥~~⑦サイバーセキュリティ基本法（平成26年法律第104号）
⑧重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第42号）[5]
~~⑧~~⑨○○市個人情報保護法施行条例（令和○○年条例第○○号）

脚注5 公布後１年６月以内施行

ドメイン（lg.jp）使用に関する契約における記載の追加

■ lg.jpドメインの使用を従来より促しているが、業務委託契約においては、除外されているケースがあることから、業務委託契約においてもlg.jpの利用を原則とする旨を記載（赤字の箇所）。

現行：対策基準（解説）

6.3. システム開発、導入、保守等

（８）情報システムにおける入出力データの正確性の確保
（注１１）ウェブアプリケーションの開発においては、セキュリティを考慮した実装を行わなければ脆弱性を作り込んでしまうおそれがある。（略）
また、対外的に公表するウェブサイトや情報システムを構築する場合は、その構築基盤がどこにあるかを問わず、「.lg.jp」で終わるドメイン名（以下「『lg.jp』ドメイン」という。）の使用を調達仕様書に含めることが必要である。

改定案：対策基準（解説）

6.3. システム開発、導入、保守等

（８）情報システムにおける入出力データの正確性の確保
（注１１）ウェブアプリケーションの開発においては、セキュリティを考慮した実装を行わなければ脆弱性を作り込んでしまうおそれがある。（略）
また、対外的に公表するウェブサイトや情報システムを構築する場合は、**当該ウェブサイト等の構築を直接委託する場合に限らず、事業運営等の業務委託の中でウェブサイト等が構築される場合も含め、**その構築基盤がどこにあるかを問わず、「.lg.jp」で終わるドメイン名（以下「『lg.jp』ドメイン」という。）**を** ~~の~~使用**することとし、その旨**を調達仕様書に含めることが必要である。
（注１２）
（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。

lg.jpドメインが利用できない場合は、一定期間ドメインを保持する旨は現行のガイドラインに記載済み

サブドメインテイクオーバーに関する記載の追加

■　DNS設定情報の削除に関して、自治体が行うのか、委託事業者が行うのか、役割を明確化する旨を記載（赤字の箇所）。

現行：対策基準（解説）

6.3.　システム開発、導入、保守等

（８）情報システムにおける入出力データの正確性の確保
（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。詳細は「Web サイト等の整備及び廃止に係るドメイン管理ガイドライン 」（平成30 年3 月30 日 各府省情報化統括責任者（CIO）連絡会議決定）を参照されたい。

改定案：対策基準（解説）

6.3.　システム開発、導入、保守等

（８）情報システムにおける入出力データの正確性の確保
（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。詳細は「Web サイト等の整備及び廃止に係るドメイン管理ガイドライン 」（2025（令和 7）年 5 月 27 日 デジタル社会推進会議幹事会決定~~平成30 年3 月30 日 各府省情報化統括責任者（CIO）連絡会議決定~~）を参照されたい。**また DNSからドメイン設定を確実に削除するため、削除を地方公共団体が行うのか当該ウェブサイトの委託事業者等が行うのかを契約等において明確にするとともに、ドメインの運用停止後、当該削除が実施されたことを地方公共団体が確認する必要がある。**

例外措置に関する記載の追加

■　例外措置が定常化することでセキュリティリスクが生じる懸念があるため、ポリシーを見直す必要性を追加（赤字の箇所）。

現行：対策基準（解説）

7.4.　例外措置

例外措置は、情報セキュリティポリシーの適用を例外的に排除するものであることから、その承認は、ポリシーの適用が著しく行政事務の遂行を妨げる、緊急を要し通常の手続を取る時間的な猶予がない、技術的に困難であるなどの合理的な理由が必要である。なお、その場合でも、例外措置は単に適用を排除するだけでなく、リスクに応じて代替措置を定めること及び期限を設けて認めることが望ましい。
CISOは、例外措置についての手続を定め、明示することによって、ローカルルールの氾濫や、対策の未実施を防止することができる。
（注１）例外措置の内容から判断し、情報セキュリティポリシーの遵守自体に無理があると判断される場合には、当該ポリシーの見直しについて検討する必要がある。

改定案：対策基準（解説）

7.4.　例外措置

例外措置は、情報セキュリティポリシーの適用を例外的に排除するものであることから、その承認は、ポリシーの適用が著しく行政事務の遂行を妨げる、緊急を要し通常の手続を取る時間的な猶予がない、技術的に困難であるなどの合理的な理由が必要である。**また、例外措置を認める場合は、**単に適用を排除するだけでなく、リスクに応じ**た**代替措置を定**めるとともに、**期限を設けて認めること**~~が望ましい~~**。
CISOは、例外措置についての手続を定め、明示**したうえで承認する**ことによって、ローカルルールの氾濫や、対策の未実施を防止することができる。**また、定めた例外措置が運用上常態化していないか、確認する。例外措置が常態化していることを把握した場合には、リスク分析を行い、必要な運用方法を定めるとともに、情報セキュリティポリシーの見直しについて情報セキュリティ委員会に検討を指示する。**
（注１）例外措置の内容から判断し、情報セキュリティポリシーの遵守自体に無理があると判断される場合には、当該ポリシーの見直しについて検討する必要がある。

DMARC設定に関する記載の追加

■ DMARCにおける適切な設定内容について補足を追加（赤字の箇所）。

現行：対策基準（解説）

6.1.コンピュータ及びネットワークの管理

6.1.コンピュータ及びネットワークの管理
(14) 電子メールのセキュリティ管理
メールサーバに対するセキュリティ対策等、電子メールのセキュリティ管理について定める。外部からの電子メール受信及び外部への電子メール送信においてなりすましを防ぐため、メールサーバのセキュリティ対策として電子署名を用いたDKIM（DomainKeys Identified Mail）やSPF（Sender Policy Framework）等の対策を実施するとともに、DMARC（Domain-based Message Authentication, Reporting & Conformance）も実施しなければならない。

改定案：対策基準（解説）

6.1.コンピュータ及びネットワークの管理

6.1.コンピュータ及びネットワークの管理
(14) 電子メールのセキュリティ管理
メールサーバに対するセキュリティ対策等、電子メールのセキュリティ管理について定める。外部からの電子メール受信及び外部への電子メール送信においてなりすましを防ぐため、メールサーバのセキュリティ対策として電子署名を用いたDKIM（DomainKeys Identified Mail）やSPF（Sender Policy Framework）等の対策を実施するとともに、DMARC（Domain-based Message Authentication, Reporting & Conformance）も実施しなければならない。**DMARCを含む送信ドメイン認証の設定がされていないことで地方公共団体から発信する住民等向けのメールを受信するインターネットプロバイダにて迷惑メールと扱われないためにも重要な措置となる。なお、DMARCの設定を監視（none）にとどめている場合は、外部の受信者がなりすましメールによる被害を受けるリスクを十分に低減できないことから、DMARCレポートを確認しながら、隔離（quarantine）、さらに拒否（reject）の設定へと段階的に移行すること。**

【参考】DMARCパラメータの意味
■ 「p」は認証失敗したメールに対して受信側に実行し欲しい対応を定義する
- p=none
  「none」は未定義であり、メールの監視は行うが全てのメールを受信する
- p= quarantine
  DMARCが失敗した場合、スパムまたは隔離フォルダにメールを振り分ける
- p= reject
  DMARCが失敗した場合、メールの受信を拒否(削除)する