令和８年６月30日
第10回デジタル学習基盤特別委員会
参考資料2

一部加工済

事　務　連　絡
令和８年６月26日

各都道府県教育委員会担当課
各指定都市教育委員会担当課　御中

文部科学省初等中等教育局
参事官（デジタル学習基盤担当）付

総務省における「地方自治法施行規則の一部を改正する省令の公布等について（通知）」について

今般、地方自治法施行規則の一部を改正する省令（令和８年総務省令第８０号。以下「改正規則」という。）が公布されたことを踏まえ、総務省において、別紙１のとおり「地方自治法施行規則の一部を改正する省令の公布等について（通知）」が発出されました。

地方自治法の一部を改正する法律（令和６年法律第６５号。以下「改正法」という。）は、令和６年６月２６日に公布され、教育委員会を含めた普通地方公共団体は、情報システムの適正な利用を図るために必要な措置を講じなければならないものとされましたが（地方自治法（昭和２２年法律第６７号）第２４４条の５第２項、地方独立行政法人法（平成１５年法律第１１８号）第２４条の２において準用する場合を含む。）、改正規則は、改正法により改正された地方自治法を実施するため、サイバーセキュリティの確保等の情報システムの適正な利用を図るために必要な措置について、規定を整備するものです。

改正規則は、令和９年７月１日に施行されるため、別紙１をご確認の上、施行日までに必要な準備を行うようお願いします。

また、教育情報セキュリティポリシーを策定している自治体は、令和７年度時点で約 50%に留まっています。文部科学省では、改正規則を踏まえ令和８年度末までに改訂する「教育情報セキュリティポリシーに関するガイドライン」（以下「ガイドライン」という。）に加え、教育現場における情報セキュリティの基本的な考え方及びガイドラインの基本的な考え方とポイントを解説した「教育情報セキュリティポリシーハンドブック」（以下「ハンドブック」という。）も公開しています。現在、教育情報セキュリティポリシ

ーを策定していない各教育委員会におかれては、ガイドラインやハンドブックの内容も踏まえながら、早急に教育情報セキュリティポリシー策定又はそれに向けた準備を実施いただきますようお願いします。

なお、学校等教育現場において発生したインシデントについては、各都道府県情報セキュリティ担当課及び各市区町村情報セキュリティ担当課と連携の上、別紙２「年末年始期間等におけるインシデント報告等について」事務連絡）も参照の上、以下宛先までご連絡ください。

【加工】

（文部科学省初等中等教育局参事官（デジタル学習基盤担当）付）

各都道府県教育委員会担当課におかれては、本事務連絡の内容を御了知いただくとともに、域内の市区町村教育委員会（指定都市教育委員会を除き、学校組合等を含む。）に対して、本事務連絡の内容を周知いただきますようお願いします。

〈添付資料〉

別紙１：地方自治法施行規則の一部を改正する省令の公布等について（通知）

別紙２：年末年始期間等におけるインシデント報告等について（事務連絡）

【本件担当】
初等中等教育局参事官（デジタル学習基盤担当）付
教育DX室 校務データ連携企画係
喜屋武、伊藤、葉狩、杉本
電話　03-6734-3263
E-mail　kyoikudx@mext.go.jp

総行サ第４２号
令和８年６月２６日

各都道府県知事
各都道府県議会議長
各指定都市市長
各指定都市市議会議長
殿

総務省自治行政局長
（公印省略）

地方自治法施行規則の一部を改正する省令の公布等について（通知）

地方自治法施行規則の一部を改正する省令（令和８年総務省令第８０号。以下「改正規則」という。）が本日公布されました。

地方自治法の一部を改正する法律（令和６年法律第６５号。以下「改正法」という。）は、令和６年６月２６日に公布され、普通地方公共団体は、情報システムの適正な利用を図るために必要な措置を講じなければならないものとされましたが（地方自治法（昭和２２年法律第６７号）第２４４条の５第２項、地方独立行政法人法（平成１５年法律第１１８号）第２４条の２において準用する場合を含む。）、改正規則は、改正法により改正された地方自治法を実施するため、サイバーセキュリティの確保等の情報システムの適正な利用を図るために必要な措置について、規定を整備するものです。

改正規則は、令和９年７月１日に施行することとしていますので、施行日までに必要な準備を行うようお願いします。

特に、改正規則による改正後の地方自治法施行規則（昭和２２年内務省令第２９号。以下「新規則」という。別紙１及び別紙２において同じ。）における「情報システム等の開発、導入及び保守の適切な実施」（新規則第１６条の３第１項第５号）並びに「適切な業務委託（情報システム等に関するものを含む。）の実施」及び「インターネットその他の高度情報通信ネットワークを通じて電子計算機を他人の情報処理の用に供する役務の適切な利用」（新規則第１６条の３第１項第７号）については、別紙１「情報システム等のサプライチェーン・リスク対策について」を参照の上、適切に御対応ください。

また、新規則における「サイバーセキュリティに関する情報の収集」（新規則第１６条の３第１項第５号）については、別紙２「情報システム等の脆弱性診断について」を参照の上、適切に御対応ください。

貴職におかれては、下記事項に御留意の上、その円滑な施行に向け、格別の配慮をされるとともに、各都道府県知事におかれては、貴都道府県内の指定都市を除く市区町村長及び市区町村議会議長に対し、この旨周知願います。また、その際には、一部事務組合、広域連合及び地方独立行政法人にも、対応に遺漏なきよう併せて周知願います。

なお、地域の元気創造プラットフォームにおける調査・照会システムを通じて、各市区町村に対して本通知についての情報提供を行っていること、及び本通知は地方自治法第２４５条の４第１項に基づく技術的な助言であることを申し添えます。

記

第１　サイバーセキュリティに係る必要な措置に関する事項

地方自治法第２４４条の５第２項の規定による必要な措置は、次のとおりとされたこと。ただし、国又は他の地方公共団体の重要な情報又は重要な情報システムに影響を及ぼす可能性があるネットワークに電気通信回線で直接又は間接に接続されていない地方公共団体であって、かつ、個人情報を多量に保有していない団体及び公安委員会についてはこの限りではないこととされたこと。

①　組織体制の整備（新規則第１６条の３第１項第１号関係）
②　適切な情報資産の分類及び管理の実施（新規則第１６条の３第１項第２号関係）
③　物理的なサイバーセキュリティに関する対策の適切な実施（新規則第１６条の３第１項第３号関係）
④　人的なサイバーセキュリティに関する対策の適切な実施（新規則第１６条の３第１項第４号関係）
⑤　技術的なサイバーセキュリティに関する対策の適切な実施（新規則第１６条の３第１項第５号関係）
⑥　サイバーセキュリティに関する対策の適切な運用の実施（新規則第１６条の３第１項第６号関係）
⑦　適切な業務委託の実施及び外部サービス（クラウドサービス）の適切な利用（新規則第１６条の３第１項第７号）
⑧　サイバーセキュリティに関する対策の適切な評価及び見直しの実施（新規則第１６条の３第１項第８号）

第２　施行期日

改正規則の施行期日は、令和９年７月１日とされたこと。

第３　経過措置

改正規則の施行の際現に存する情報システム等及び現に実施されている業務委託については、新規則第１６条の３第１項第５号（技術的なサイバーセキュリティに関す

る対策）及び第７号（業務委託及び外部サービス（クラウドサービス）の利用）の規定にかかわらず、なお従前の例によることとされたこと。

第４　留意事項

第１に掲げた必要な措置の具体的な内容に関しては、「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」（以下「ガイドライン」という。）を参照すること。

また、本通知及び別紙１を参照の上、改正規則施行後に導入される情報システム等及び開始される業務委託については、サプライチェーン・リスク対策を含めたサイバーセキュリティに関する対策が適切になされるよう、準備すること。

なお、改正規則施行前に導入される情報システム等及び開始される業務委託についても、本通知及び別紙１の趣旨を踏まえ、可能な限り適切なサプライチェーン・リスク対策を講じること。

連絡先：
自治行政局住民制度課サイバーセキュリティ対策室
桑折補佐、西本係長、松崎事務官
ＴＥＬ：03-5253-5333（直通）
E-mail：lg-security@soumu.go.jp

（別紙１）

# 情報システム等のサプライチェーン・リスク対策について

## １．地方公共団体の情報システム等のサプライチェーン・リスク対策の必要性等

近年、グローバルなサプライチェーン・リスクが深刻化する中、国家安全保障の観点からＩＴ製品等の信頼性を担保することへの重要性が高まっている。

国と地方公共団体の情報システムは、ネットワークを通じて相互接続しており、地方公共団体の情報システムのサプライチェーン上の脆弱性を突いたインシデントが発生した場合、その被害が政府機関へと波及する蓋然性は高い。

政府機関においては、「ＩＴ調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（平成３０年１２月１０日関係省庁申合せ）に基づき、実効性のあるサプライチェーン・リスク対策が講じられているが、地方公共団体においても、政府機関と歩調を合わせた対策を実施することが必要である。

そこで、新規則に規定するサプライチェーン・リスク対策の内容及び実施方法について、以下のとおり、詳細な事項を示す。

## ２．サプライチェーン・リスク対策を講じることが必要な情報資産の範囲

地方公共団体等（地方公共団体及び地方独立行政法人をいう。以下同じ。）の事務の処理に係る情報システムの適正な利用に関係する情報資産について、サプライチェーン・リスク対策を講じる必要があること。情報資産の種類ごとの主な例を次表で示すが、具体的に対象となる情報資産は主な例に限られない。

| 情報資産の種類 | 主な例 |
|---|---|
| ネットワーク | 通信回線、ルータ等の通信機器 等 |
| 情報システム | サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーティングシステム、ソフトウェア、ドローン、ネットワークカメラ、クラウドサービス 等 |
| ネットワーク又は情報システムに関する施設及び設備 | コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル 等 |
| 電磁的記録媒体 | サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体、ＵＳＢメモリ、外付けハードディスクドライブ、ＤＶＤ－Ｒ、磁気テープ等の外部電磁的記録媒体 等 |

| | |
|---|---|
| ネットワーク及び情報システムで取り扱う情報 | ネットワーク、情報システムで取り扱うデータ等 |
| 情報システム等に関連する文書 | システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図 等 |

## ３．新規則に規定するサプライチェーン・リスク対策

新規則第１６条の３第１項第５号に規定する「情報システム等の開発、導入及び保守の適切な実施」及び同条同項第７号に規定する「適切な業務委託（情報システム等に関するものを含む。）の実施」は、サプライチェーン・リスクに係る懸念が払拭できない機器等（ネットワーク、情報システム、ネットワーク又は情報システムに関する施設及び設備、電磁的記録媒体等の情報資産をいう。以下同じ。）を調達しない又は役務の提供を受けない、及びサプライチェーン・リスクに係る懸念が払拭できない企業から機器等を調達しない又は役務の提供を受けないようにするため、当該リスクを受容するか又は低減するための措置を講ずることが可能であるかを十分検討した上で、調達の可否を決定することを含む。

「サプライチェーン・リスク」の例としては、機器等を開発・供給する事業者及びそのサプライヤー・委託事業者（再委託事業者等を含む。以下同じ。）並びに当該機器等の設置、保守等の役務を提供する事業者及びその委託先事業者について、当該事業者等の本社等（当該事業者等の総株主等の議決権の過半数を直接又は間接に保有する者の本社等を含む。）の立地する場所の法的環境や外部主体の指示等により、当該機器等に係る開発・供給又は役務の提供等の適切性が影響を受け、これにより悪意ある機能や不正な変更が機器等に組み込まれる又は当該機器等が取り扱う情報が窃取・破壊される等のリスクがある。

新規則第１６条の３第１項第７号に規定する「インターネットその他の高度情報通信ネットワークを通じて電子計算機を他人の情報処理の用に供する役務の適切な利用」は、データセンターの存在地の国の法律の適用を受け、適切なかつ透明性のある手続（令状主義、透明性の確保、不利益処分に関する手続等をいう。）に則らない形でクラウドサービス内の情報が外国の法執行機関の命令により強制的に開示されるといったリスクがあると判断される場合には、クラウドサービスの利用を行わないことを含む。

## ４．適切なサプライチェーン・リスク対策の実施方法

３．で示したサプライチェーン・リスク対策を含めたセキュリティ対策の実施方法については、次の事項を参照の上、適切に対応すること。

（１）適切な選定基準の整備等

サプライチェーン・リスク対策を含めたセキュリティ対策がなされた調達を行うため、各地方公共団体等において機器等の選定に関する基準（以下「選定基準」という。）を策定すること。

選定基準の中に基本的なセキュリティ対策及びサプライチェーン・リスク対策に関する事項を規定すること。

情報資産の分類に応じて、原則として、「セキュリティ要件適合評価及びラベリング制度（ＪＣ－ＳＴＡＲ）[1]」、「政府情報システムのためのセキュリティ評価制度（ＩＳＭＡＰ、ＩＳＭＡＰ－ＬＩＵ）[2]」又は「デジタルマーケットプレイス（ＤＭＰ）[3]」（以下「政府の評価・登録制度」という。）に登録等がなされている製品を調達することにより、サプライチェーン・リスク対策を含めたセキュリティ対策がなされた調達を行うものとする。ただし、政府の評価・登録制度に登録等がなされていない機器等（政府の評価・登録制度の対象とならない製品分野に属する機器等を含む。以下同じ。）に関しては、適切なサプライチェーン・リスク対策が講じられていると各地方公共団体において判断できるものを調達すること。

（２）契約方式

機器等の調達に当たっては、価格と価格以外の要素とを総合的に評価して、最も評価の高い者を落札者として決定する方法である総合評価一般競争入札（地方自治法施行令（昭和２２年政令第１６号）第１６７条の１０の２第１項及び第２項）を採用するなど、調達内容に応じて適切な契約方式を選定すること。

（３）仕様書・契約書等

選定基準に従って、仕様書及び契約書等を作成すること。

５．総務省において設置予定の総合相談窓口について

サプライチェーン・リスク対策を含めた地方公共団体からの相談を受け付ける総合窓口を総務省に設置する予定であり、詳細については今後通知すること。

---

[1] 2024 年 8 月に経済産業省が公表した「IoT 製品に対するセキュリティ適合性評価制度構築方針」に基づき構築された制度で、インターネットとの通信が行える幅広い IoT 製品を対象として、共通的な物差しで製品に具備されているセキュリティ機能を評価・可視化することを目的とする制度。
https://www.ipa.go.jp/security/jc-star/index.html

[2] 「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」（令和 2 年 1 月 30 日サイバーセキュリティ戦略本部決定）に基づき、国家サイバー統括室、デジタル庁、総務省、経済産業省が運営している、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度。
https://www.digital.go.jp/news/1b3ebb05-27bf-464a-8859-abcc771b8cc2

[3] 2024 年度に運用を開始した、デジタル庁と事前に基本契約を締結した事業者がソフトウェア・サービスの登録を行い、登録情報を集約したカタログサイトから各行政機関が最適なプランを選択し、個別契約を行う調達手法。
https://www.dmp-official.digital.go.jp/

## ６．その他

選定基準及び仕様書・契約書等に関しての詳細については、今後通知すること。

（別紙２）

# 情報システム等の脆弱性診断について

総務省では、地方公共団体が単独で脆弱性診断システムを導入する場合、脆弱性診断システムの導入・運用のコストが大きいこと等の課題があることから、全ての地方公共団体が利用可能な脆弱性診断システム（地方版アタックサーフェスマネジメント（ＡＳＭ）システム）を、令和８年度中に一括して構築し、その効果を実証した上で、本格運用を開始する予定である。

新規則における「サイバーセキュリティに関する情報の収集」（新規則第１６条の３第１項第５号）の具体的な実施手法の一つとして、情報システム等の脆弱性を定期的に探索し、発見された脆弱性を踏まえて、リスクや影響が大きいものを中心に、適時適切な対応（情報システム等の改修やパッチ適用等）を実施する脆弱性診断システムを活用することが有効と考えられる。

地方版ＡＳＭシステムを利用することで、地方公共団体において低価格かつ低負担で脆弱性診断が可能となることから、地方公共団体におかれては、積極的に地方版ＡＳＭシステムの利用をご検討いただきたい。

事　務　連　絡
令和７年12月16日

各都道府県情報セキュリティ担当課
各市区町村情報セキュリティ担当課　御中

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
総務省自治行政局住民制度課デジタル基盤推進室

【重要】年末年始期間等におけるインシデント報告等について（事務連絡）

平素より、地方公共団体における情報セキュリティ対策の徹底について、御理解と御協力を賜り、厚く御礼申し上げます。
年末年始期間等におけるインシデント報告及び最近のインシデント事例を踏まえた注意喚起について、次のとおりお知らせしますので、対応に遺漏なきよう、よろしくお願いいたします。

１．令和７年４月７日付け総行サ第２号で通知しているとおり、各地方公共団体で覚知したインシデントについて報告をお願いしているところです。年末年始期間等においても、適切な報告を行うことができるよう、庁内における連絡体制の確保等、必要な事項の確認・準備をお願いいたします。

２．令和７年から令和８年にかけての年末年始期間等においては、非常に多くの団体において標準準拠システムへの移行作業が予定されており、通常のインシデントに加えて移行作業に伴うインシデントの発生も予測されることから、**令和７年12月20日（土）～令和８年２月１日（日）のインシデント報告については、標準準拠システムへの移行に関連すると考えられるインシデントの報告について通常の連絡先に加えて宛先の追加をお願いすることとしております**。つきましては、別添「令和７年から令和８年にかかる年末年始期間等における緊急時連絡方法・連絡先について」をご参照の上、適切な対応をお願いいたします。

３．最近、地方公共団体の業務委託先がランサムウェア攻撃を受けたことによって約1,000件の個人情報が漏洩した事案、業務委託先がwebページの設定ミスをしたことによって約6,000件の個人情報が漏洩した事案等、業務委託先起因による情報漏洩事案が相次いでいます。業務委託に際しての情報セキュリティ確保については、「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」において、情報セキュリティ要件を明記した契約の締結、業務委託実施期間中においても情報セキュリティ対策の履行状況を定

期的に確認すること等を規定しているところ、今一度対応を徹底するよう、お願いいたします。

また、職員によるメールの誤送信やUSB等の電磁的記録媒体の紛失等といった人為的なミスによる個人情報の漏えい事案も散見されますので、併せて、基本的な対策の徹底をお願いいたします。

なお、改めてインシデント報告の提出における注意事項等を記載した資料及び様式を送付しますので御確認のほどよろしくお願いします。

加えて、年末年始休暇期間中のGCASヘルプデスクの対応とガバメントクラウドへの円滑かつ安定な移行に係る留意事項については、デジタル庁の事務連絡（令和７年12月16日）をご参照ください。

＜送付資料＞

・ 令和７年から令和８年にかかる年末年始期間等における緊急時連絡方法・連絡先について
・【様式1】インシデント報告（IT障害）
・【様式1_別紙】分類表
・【様式2】インシデント報告（情報漏えい）

サイバーセキュリティ対策室
担　当：田中、三橋、河村、佐々木、藤見、宮薗、岩尾
電　話：03-5253-5333（直通）
メール：cyb-security@ml.soumu.go.jp
lg-security@soumu.go.jp

デジタル基盤推進室
担　当： 加藤、菊田、東島、山口、松尾、細川、三宅
電　話： 03-5253-5364（直通）
メール：digi-kiban@ml.soumu.go.jp
digital-kiban@soumu.go.jp