消 防 消 第 261 号
令和８年６月２６日

各都道府県消防防災主管部（局）長
東京消防庁・各指定都市消防長 } 殿

消防庁消防・救急課長
（ 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係る
消防防災分野における対応について（通知）

平素より、消防防災行政の推進につきまして、格別の御協力を賜り厚く御礼申し上げます。

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、別紙１のとおり本日公布されました。

また、これにあわせて、「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）」（令和８年６月２６日付け総行サ第４２号総務省自治行政局長通知。以下「自治行政局長通知」という。）が、別紙２のとおり発出されました。

改正規則は令和９年７月１日に施行することとされており、消防本部、地方公共団体の消防防災部局におかれては、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。）及び自治行政局長通知を参照の上、施行日までに必要な準備を行っていただくようお願いします。

特にドローンについては、従前より、「消防防災分野におけるドローンの活用について（通知）」（令和８年３月３１日付け消防消第１１０号消防庁消防・救急課長、消防災第４５号消防庁国民保護・防災部防災課長、消防地第３１６号消防庁国民保護・防災部地域防災室長通知。以下「３月３１日付け通知」という。）等により、その調達等に当たって、機微情報漏洩はもとより、操縦不能や乗っ取り等による業務への支障等が生じないよう適切に対応いただきたい旨を通知してきたところですが、新規則に基づきサプライチェーン・リスク対策を講じることが必要な情報資産にはドローンも含まれていることに御留意いただき、その調達等に当たっては、自治行政局長通知を参照の上、適切なサプライチェーン・リスク対策を講じていただくようお願いします。

なお、３月３１日付け通知も引き続き参照いただき、必要に応じて消防庁担当課へお問い合わせください。

各都道府県知事におかれては、貴都道府県内の市町村（消防の事務を処理する一部事務組合等を含む。）に対し、この旨周知いただくようお願いします。

なお、本通知は、消防組織法（昭和２２年法律第２２６号）第３７条の規定に基づく助言として発出するものであることを申し添えます。

消防庁　消防・救急課
担　当：岩熊補佐、熊事務官
ＴＥＬ：03-5253-7522（直通）
E-mail：shokuin@soumu.go.jp

別紙１

○総務省令第八十号

地方自治法（昭和二十二年法律第六十七号）を実施するため、地方自治法施行規則の一部を改正する省令を次のように定める。

令和八年六月二十六日

総務大臣　林　芳正

地方自治法施行規則の一部を改正する省令

地方自治法施行規則（昭和二十二年内務省令第二十九号）の一部を次のように改正する。

次の表により、改正後欄に掲げるその標記部分に二重傍線を付した規定（以下「対象規定」という。）は、これを加える。

改正後	改正前
第十六条の三　地方自治法第二百四十四条の五第二項の規定による必要な措置は、次に掲げるものとする。ただし、地方公共団体総合行政ネットワーク（全ての地方公共団体においてその使用する電子計算機を相互に電気通信回線で接続して情報の電磁的方式（電子的方式、磁気的方式その他人の知覚によつては認識することができない方式をいう。以下同じ。）による流通及び情報処理を行うための情報通信ネットワークをいう。）その他の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普通地方公共団体であつて、かつ、個人情報の保護に関する法律（平成十五年法律第五十七号）第二条第一項に規定する個人情報を多量に保有していないもの及び公安委員会については、この限りでない。 一　責任者の設置、各責任者への適切な責任の分担等の組織全体の体制の整備 二　保有する情報資産の適切な分類及び当該分類に基づく取扱方法の制限の実施、保有する情報資産の適切な管理その他の適切な情報資産の分類及び管理の実施 三　情報システム等の適切な管理、管理区域の適切な管理、電気通信回線（入出力装置を含む。）の適切な管理、職員の利用する通信端末機器及び電磁的記録媒体（電磁的方式で作られた記録に係る記録媒体をいう。以下同じ。）の適切な管理その他の物理的なサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。以下同じ。）に関する対策の適切な実施 四　職員の遵守事項の遵守等のための適切な措置の実施、研修及び訓練の実施、サイバーセキュリティに関するインシデントの報告、不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第二項に規定する識別符号の適切な管理その他の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 五　情報資産の適切な管理、不正アクセス行為の禁止等に関する法律第二条第三項に規定するアクセス制御機能の適切な整備、同法同条第四項に規定する不正アクセス行為を防止するための適切な対策の実施、刑法（明治四十年法律第四十五号）第百六十八条の二第一項各号に掲げる電磁的記録その他の記録を通じた電子計算機に対する不正な活動による被害の防止のための適切な対策の実施、情報システム等の開発、導入及び保守の適切な実施、サイバーセキュリティに関する情報の収集その他の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 六　情報システムに対する監視の適切な実施、サイバーセキュリティに関する方針等のサイバーセキュリティに関する規程の遵守状況の確認、情報資産に対するサイバーセキュリティに関するインシデントへの適切な対応その他の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 七　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	［新設］

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

八　監査及び自己点検の実施、サイバーセキュリティに関する方針等のサイバーセキュリティに関する規程の見直しその他の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

2　この条において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一　情報資産　情報通信ネットワーク、情報システム、情報通信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（この条において「情報システム等」という。）、情報通信ネットワーク及び情報システムによつて取り扱う情報並びに情報システム等の仕様書及び構成図その他の情報システム等に関連する文書（電磁的記録を含む。）をいう。

二　管理区域　情報通信ネットワークの基盤となる機器及び重要な情報システムを設置し、当該機器及び当該情報システムの管理及び運用の用に供するもの並びに電磁的記録媒体の保管の用に供するものをいう。

三　サイバーセキュリティに関するインシデント　意図しないサイバーセキュリティに関する方針等のサイバーセキュリティに関する規程の違反若しくはサイバーセキュリティに関する対策の管理の方法の不具合の可能性若しくはサイバーセキュリティに関係する可能性がある情報通信ネットワーク、情報システム若しくは役務の状態に関する事象（以下「サイバーセキュリティ事象」という。）又は予期せざるサイバーセキュリティ事象であつて、業務の実施に支障が生ずるおそれ及びサイバーセキュリティが害されるおそれがあるものをいう。

備考　表中の［　］の記載及び対象規定の二重傍線を付した標記部分を除く全体に付した傍線は注記である。

附　則

（施行期日）

1　この省令は、令和九年七月一日から施行する。

（経過措置）

2　この省令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、この省令による改正後の地方自治法施行規則第十六条の三第一項第五号及び第七号の規定にかかわらず、なお従前の例による。

別紙２

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。