

総行サ第 83 号
令和 8 年 9 月 18 日

各都道府県知事
各都道府県議会議員
各市区町村長
各市区町村議会議員

殿

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長

ネットワークカメラにおけるサプライチェーン・リスク対策を含めた
サイバーセキュリティ対策の実施について（通知）

平素より、地方公共団体におけるサイバーセキュリティ対策の実効性の確保について、御理解と御協力を賜り、厚く御礼申し上げます。

近年、ネットワークカメラ（インターネットや庁内ネットワーク（LAN）等への接続機能を有するカメラをいう。以下同じ。）への不正アクセスやマルウェア感染に関する事案が相次いで発生しています。ネットワークカメラへの不正アクセスやマルウェア感染が発生した場合、映像の漏えいによるプライバシー侵害や機密情報の流出等の直接的な被害が生じるだけでなく、当該カメラが攻撃者の支配下に置かれ、マルウェアの拡散に利用されたり、サイバー攻撃の踏み台として悪用されたりするなど、第三者に対する二次被害が生じるおそれがあります。

不正アクセスやマルウェア感染が生じる要因として、推測されやすいパスワードの設定やファームウェアのアップデート未実施のほか、製造過程において悪意のある機能や不正な変更が機器等に組み込まれていることなどが挙げられ、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対策が喫緊の課題となっています。

地方公共団体におけるサプライチェーン・リスク対策の必要性等については、「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）において示したところですが、昨今の情勢を踏まえ、各地方公共団体におかれましては、下記のとおりネットワークカメラの使用におけるサプライチェーン・リスク対策を含めたサイバーセキュリティ対策を直ちに実施いただきますようお願いいたします。

各都道府県知事及び市区町村長におかれましては、一部事務組合、広域連合及び地方独立行政法人に対し、この旨周知願います。

なお、一斉通知・調査システムを通じて各都道府県及び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（昭和 22 年法

律第 67 号)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

1 ネットワークカメラの点検の実施

保有するネットワークカメラについて、次の(1)～(4)に掲げるとおりセキュリティ対策の実施状況を確認すること。

- (1) パスワード認証を設定しているか、パスワード認証を設定している場合は十分に長いパスワードとしているか。
- (2) ネットワークカメラのファームウェアのバージョンが最新であるか、機器の製品サポートは継続しているか。
- (3) 使用しない機能や設定が有効になっていないか。
- (4) サプライチェーン・リスク（※）に対する適切な対策が講じられているか。

（※）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をいう。

2 サイバーセキュリティ対策の確実な実施

1 の点検の結果、適切なサプライチェーン・リスク対策を含むサイバーセキュリティ対策が講じられていないと認められるネットワークカメラについては、次のとおり対策を実施すること。

(1)関連

パスワード認証を設定するとともに、パスワードを初期設定から変更した上で、適切に管理すること。また、パスワードは十分な長さとし、文字列は想像しにくいもの（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）を設定すること。

(2)関連

ファームウェアのバージョンを最新化するとともに、機器の製品サポートが終了し、適切なサポートを受けられない場合は、機器の交換を行うこと。

(3)関連

使用しない機能や設定については、無効化すること。

(4)関連

適切なサプライチェーン・リスク対策が講じられていないネットワークカメラについては、次のとおり対応すること。

・インターネットに接続されているネットワークカメラについては、直ちにイン

ターネットから切断すること。

- ・自治体情報セキュリティクラウド等のログを確認し、不審な宛先に対する通信が大量に発生しているなど不正な事象がないか確認すること。
- ・耐用年数にかかわらず、順次必要に応じてサプライチェーン・リスク対策を含むサイバーセキュリティ対策が適切に講じられた製品への交換を行うこと。

なお、ネットワークカメラの入れ替え・調達に当たっては、「セキュリティ要件適合評価及びラベリング制度（J C - S T A R）」の適合ラベルの取得を参照することとし、取得していない製品については、適切なサプライチェーン・リスク対策が講じられていることを確認すること。

3 その他

サプライチェーン・リスク対策が適切に講じられているかの確認に当たっては、「地方公共団体の機器等の調達におけるサプライチェーン・リスク対策のための選定基準及び仕様書策定手引書」について（通知）（令和8年7月31日付け総行サ第54号、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長通知）も併せて参照すること。

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

T E L：03-5253-5333（直通）

E-mail：lg-security@soumu.go.jp