

事 務 連 絡
令和5年10月12日

各都道府県・市町村保育主管課
各都道府県・指定都市・中核市認定こども園主管課
各都道府県・指定都市・中核市・
児童相談所設置市認可外保育施設担当課（室）

御中

こども家庭庁成育局保育政策課
こども家庭庁成育局保育政策課認可外保育施設担当室

ネットワークカメラ等におけるセキュリティ対策のお願い（注意喚起）

標記については、総務省より、別添のとおり、防犯カメラ等における適切なセキュリティ対策について注意喚起がありました。

つきましては、貴管内の市区町村並びに各保育所、認定こども園、認可外保育施設等に対して、この内容について周知していただきますようお願いいたします。

総サ統第139号

令和5年10月2日

こども家庭庁成育局保育課長

こども家庭庁成育局保育政策課認可外保育施設担当室長

総務省サイバーセキュリティ統括官付

参事官（政策担当）

ネットワークカメラ等におけるセキュリティ対策のお願い（注意喚起）（依頼）

標記について、保育所等に設置されている一部の防犯カメラ等において十分なセキュリティ対策が行なわれていないことにより、マルウェア（悪性ソフトウェア、ウィルス等をいう。）に感染した事案が発見されている。ついては、類似事案の発生防止の観点から、防犯カメラ等における適切なセキュリティ対策について、別紙のとおり貴課所管施設への注意喚起を依頼する。

ネットワークカメラ等におけるセキュリティ対策のお願い（注意喚起）

標記について、一部の小学校及び保育所に設置されているネットワークカメラ等（レコーダー、センサー及び登下校の記録システム等を含む。）において十分なセキュリティ対策が行われていないことにより、マルウェア（悪性ソフトウェア、ウイルス等をいう。）に感染した事案が発見されました。類似事案の発生防止の観点から、ネットワークカメラ等における適切なセキュリティ対策について、全国の保育所、認定こども園、地域型保育事業、認可外保育施設（以下、「保育所等」という。）に対して下記のとおり注意喚起を行います。

記

1. 事案について

一部の小学校及び保育所に設置されているネットワークカメラ及び登下校の記録システムに脆弱性（プログラムの不具合や設計上のミス、設定等が原因となって発生した情報セキュリティ上の欠陥）があり、これを悪用しマルウェアに感染した事例を国立研究開発法人情報通信研究機構（NICT）が確認しました。（NICTが発見したネットワークカメラ等については、利用者、メーカー等に対処を求め対処が完了しています。）

2. 注意喚起の目的

保育所等においてネットワークカメラ等の設置が進められているところです。当該ネットワークカメラ等にも上記事案と同様な脆弱性が存在した場合、ネットワークカメラ等にマルウェアがインストールされること等により、個人情報等の流出の可能性、ネットワークカメラ等が使用できなくなる可能性、また、当該ネットワークカメラ等が他者を攻撃するサイバー攻撃のインフラとして悪用される可能性等が生じるため、それを軽減することを目的として注意喚起を行います。

3. 注意喚起の内容

1. 事案を踏まえ以下の項目について対処をお願いします。

- （ア） ネットワークカメラ等のインターネット接続の有無について確認をしてください。
- （イ） ネットワークカメラ等をインターネットに接続している場合、インターネットからのアクセスが想定されている範囲内に制限されているのかを確認してください。
- （ウ） 機器のファームウェア（ソフトウェア）はサポート期間内となっているか及び最新のものになっているか確認をしてください。

なお、詳細については次頁を参照してください。

4. その他

総務省、国立研究開発法人情報通信研究機構（NICT）及びインターネットプロバイダは連携し、IoT機器へのアクセスによるサイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行うNOTICEという取組を実施しておりますので、併せてご参照ください。

URL: <https://notice.go.jp/>

ネットワークカメラ等における設定確認のお願いについて

下記（ア）～（ウ）について、必要に応じ可能な範囲でネットワークカメラ等の開発メーカー、販売事業者、ネットワークカメラ等を設置した事業者等にご確認ください。

（ア） ネットワークカメラ等のインターネット接続の有無について確認をしてください。

- ・ネットワークカメラ等が、モバイル回線（携帯電話回線による接続）や光ファイバ等により、インターネットに接続されているかについて確認をしてください。なお、インターネットに防犯カメラの画像等を公開していない場合であっても、ネットワークカメラ等を設置した事業者がメンテナンス等のためインターネットに接続している場合があることに留意してください。

（イ） ネットワークカメラ等がインターネットに接続している場合、インターネットからのアクセスが想定されている範囲内に制限されているかを確認してください。

- ・ネットワークカメラ等をインターネットに接続して画像等を公開している場合、ネットワークカメラ等へアクセスするためのID・パスワードやアクセス元IPアドレスの制限等により、不要な範囲からアクセスを受けない設定にしているかを確認してください。（パスワード制限を行うことになっていたが、実機では設定されていなかった事例も存在します。）
- ・ID・パスワードが設定されている場合であっても、容易に推測される簡易なパスワードになっていないか、他のシステム等で同一のパスワードの使い回しをしていないか等について確認をしてください。
- ・インターネットからのアクセスを想定していないポート（サービス）がインターネットに公開されていないか確認をしてください。また可能であれば、ツール等を使用してポートスキャンを行ない、High Portを含め確認をお願い致します。（防犯カメラの仕様書にないポートにおいてサービスが動作していた事例も存在します。）

上記確認の結果、適切な設定がされていない場合には、機器設定、パスワードの再設定及びルータ等による通信遮断の実施をご検討ください。

（ウ） 機器のファームウェア（ソフトウェア）はサポート期間内となっているか及び最新のものになっているか確認をしてください。

- ・ネットワークカメラ等の開発メーカー、販売事業者、ネットワークカメラ等を設置した事業者等において、有効なサポートが受けられるか確認をしてください。販売から時間が経過したネットワークカメラ等については、サポート期間が終了し、脆弱性が発見された場合でも新しいファームウェアが提供されない可能性があります。
- ・ネットワークカメラ等で使用しているファームウェアについて、最新のものに更新がされているのかを確認してください。古いファームウェアについては、脆弱性が発見され、攻撃に悪用される可能性があります。

サポート期間が終了した機器を使い続けることは、脆弱性への対応がなされず攻撃を受け、機器自体が悪用されるだけでなく、他者に攻撃を行う踏み台になってしまう危険性が高まります。サポート期間が有効な機器への更新をご検討ください。