取引先各位

2026 年 11 月 1 日
株式会社 NSK

［D シリーズ製品］
ネットワークカメラ・録画装置のセキュリティに関するお知らせ

平素より弊社製品をご愛顧いただき、誠にありがとうございます。

昨今、ネットワークカメラや録画装置（NVR・DVR）などのネットワーク接続機器において、第三者による不正アクセスが疑われる事象が報告されています。弊社にも、一部のお客様から、身に覚えのないユーザーアカウントの追加や、カメラ名称・映像上の表示の変更などについてお問い合わせをいただいております。

これらの事象には、パスワードの管理状況、ネットワークの接続環境、機器のファームウェアなど複数の要因が関係する可能性があります。事象の発生だけで原因や影響範囲が確定するものではなく、すべての製品に同様の問題が存在することを示すものでもありません。

弊社製品を安全にご使用いただくため、以下の確認と対策をお願いいたします。

1. 確認されている主な事象

以下のような動作が見られた場合、不正アクセスや意図しない設定変更の可能性があります。

・登録した覚えのないユーザーアカウントが存在する。
・カメラ名称や映像上の文字表示が、意図せず変更されている。
・「YOUR DEVICE IS HACKED」など、設定した覚えのない文字列や外部サイトへの誘導表示がある。
・管理者アカウントの設定変更、ログイン不能、不審なアクセス履歴などが確認される。
※表示内容や機器の外観だけで、不正アクセスの原因や影響範囲を特定することはできません。

2. 日常的に実施いただきたい対策

（1）パスワードの管理

管理者を含む各アカウントに、推測されにくい固有のパスワードを設定してください。他の機器・サービスでの使い回しは避けてください。

（2）登録アカウントの確認

必要なユーザーだけが登録されているか確認してください。機器が対応している場合は、ONVIF ユーザーやアクセス権限も確認してください。

（3）適合ファームウェアへの更新

機器の型番・ハードウェア仕様・Build 情報に適合する、弊社案内のファームウェアをご使用ください。更新の可否や適用方法は製品ごとに異なります。

（4）外部アクセスの見直し

不要なポート開放を解除し、使用していない UPnP 機能や P2P 接続機能は無効にしてください。遠隔監視が必要な場合は、アクセス制限や VPN などの利用をご検討ください。

※ファームウェア更新やネットワーク設定変更は、事前に適合する手順と運用への影響を確認し、必要に応じてシステム管理者または施工業者へご相談ください。

3. 不審な動作が発生した場合

（1）事象を確認した場合は、画面の写真・スクリーンショット、発生日時、可能であれば機器のログを保存してください。表示された不審な URL や連絡先にはアクセスしないでください。初期化や不用意な設定変更により、調査に必要な情報が消失する場合があります。

（2）状況に応じて、インターネット側からのアクセスを一時的に制限してください。設定変更により遠隔監視が利用できなくなる場合があるため、システム管理者または施工業者と調整のうえ実施してください。

（3）製品型番、シリアル番号、ファームウェアのバージョン（Build 情報）、事象の内容・発生日時をご用意のうえ、ご購入先の販売店または弊社サポート窓口へご相談ください。復旧方法は確認した状況に応じてご案内いたします。

4. 旧型製品をご使用のお客様へ

長期間ご使用の製品では、セキュリティ対策を含むファームウェアの更新提供が終了している場合があります。適用可能な更新がない製品については、継続使用に伴うリスクを考慮し、後継製品への更新をご検討ください。

画面の色・外観や製造時期だけでは、脆弱性の有無は判断できません。対象の確認と適用可能なファームウェアのご案内は、製品型番や Build 情報等をもとに個別に行います。

5. お問い合わせ・今後の対応

弊社では引き続き、製品のセキュリティに関する情報の収集・確認と、必要な対策のご案内に努めてまいります。ご不明な点は、ご購入先の販売店または弊社サポート窓口へお問い合わせください。

今後とも弊社製品をご愛顧賜りますよう、よろしくお願い申し上げます。

以上