ネット漏洩　知らぬ間に

内部文書や私生活・会議の映像…

内部文書や私生活の画像、会議などが他人の目にさらされている。各地の大学で今月、コピーやファクスなどの機能を持つ複合機の蓄積データがインターネット上で誰でも閲覧可能になっていた問題が発覚。検索サイトを使えば、ウェブカメラやテレビ会議システムなどにも比較的容易にたどり着けるという。知らぬ間に身近に迫っていた情報漏洩の危険。どうすれば防げるのか。

東京大は外部から閲覧できる複合機が他にないか調べている（15日、東京都文京区）

複合機・ウェブカメラに盲点
専門家「設定の変更を」

「このサイトを利用すれば、ネットに接続した機器が簡単に検索できます」。情報セキュリティーに詳しい会津大（福島県会津若松市）の山崎文明特任教授が、パソコンの画面上に特定の海外検索サイトを表示した。

検索欄にウェブカメラや複合機、テレビ会議システムの機種名などを英語入力すると、世界中で稼働中の機器が一覧表示される。国別や都市別で絞り込め、個別の機器にもアクセスが可能だ。

試しに「webcamera」と打ち込んだ途端、画面にウェブカメラのリンク先が並んだ。日本の大手携帯通信の子会社名を選んでクリックすると、映し出されたのは東京都内の同社販売店とみられる店内に設置された防犯カメラの静止画像。いすに座って本を読む男性に男児が甘えている。山崎特任教授は「動画やテレビ会議システムの映像もリアルタイムで見られる」と話す。

今月上旬、東京大医科学研究所など複数の大学で、複合機で読み取った書類が、検索サイトを使えば外部から閲覧できることが表面化。これらの複合機は初期設定が変更されていなかった。

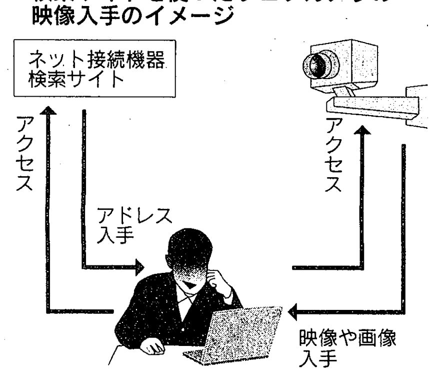
ネットと接続する機器の初期設定は、多くで利用者のIDとパスワードの設定がなかったり、その文字列が取扱説明書に明記されたりしている。IDなどはネット上にも流出しており、簡単に入手できるという。山崎特任教授によると、流出したIDなどを打ち込んで機器にアクセスした場合、不正アクセス禁止法に違反する恐れがある。

経済産業省所管の情報処理推進機構（東京・文京）の担当者は「ウェブカメラなどの大半はネットとの接続を前提にしている。情報流出のリスクは高まっており、パソコン同様の安全対策が必要だ」と強調する。

初期設定を変更しないずさんな情報管理は7月、グーグルの共用サービスを利用していた環境省など4省庁でも発覚。職員のメールが閲覧可能になっていたケースもあり、機密情報が漏洩する恐れもあった。

情報セキュリティー会社「NRIセキュアテクノロジーズ」（東京・港）の木内雄章セキュリティコンサルタントは「最低限の対応として初期設定を変更すべきだ。安全度を高めるため、不正侵入を防ぐファイアウオールも設定してほしい」と呼びかけている。

検索サイトを使ったウェブカメラの映像入手のイメージ



フォローアップ

対策強化すると利便性に影響
安全との両立難しく
メーカー、対応に追われる

ネットに接続する機器は、業者や利用者が保守点検、遠隔操作などに使う「ウェブサーバー」が組み込まれ、保存したデータや映像を管理している。顧客ニーズに対応するためのシステムだが一方で〝侵入〟の余地を与える穴となった形だ。

蓄積データが公開状態になっていた複合機を大学や企業に納入していたリコー。問題発覚後、顧客に連絡を取り、アクセス制限をかける設定変更を急いだ。対象の複合機は数十台あった。同社は「複合機は個人ではなく共用で使われることが多く、利用者ごとにIDやパスワードを設定すると使い勝手が悪くなる」（広報室）と説明。ウェブカメラメーカーの関係者も「安全対策を強化すればコストが高くなり、販売にも影響が出る」と漏らす。

メーカー側は機器の利便性と安全対策の両立に頭を痛めるが、会津大の山崎特任教授は「パスワードを機器1台ごとに変えるなど、利用者が初期設定を変更しなくても、侵入を防げる仕組みづくりをメーカー側も考える時期に来ている」と話す。