

サイバー対策、五輪前に 重要インフラに指針 【イブニングスクープ】

2019/1/15 18:00 (2019/1/15 18:29更新) | 日本経済新聞 電子版

政府は今春にも、電力や水道といった重要インフラ14分野のサイバー防衛対策に関する安全基準の指針を改定する。当初は2020年の東京五輪・パラリンピック後に見直す予定だったが、巧妙化するサイバー攻撃や相次ぐシステム障害への危機感から前倒しする。重要インフラが攻撃を受ければ国民生活への影響は甚大だ。事業者は一層の対策強化が不可欠になる。

重要インフラは国民生活や経済活動の基盤となる社会資本を指す。近年は遠隔地からの監視や制御などIT（情報技術）化が進み、サイバー攻撃にさらされやすくなっている。攻撃によりシステムが止まれば電力や水道の供給が滞りかねない。航空機や鉄道の整備記録が流出したり、改ざんされたりしたら安全な運航や輸送に支障が出る。

イブニングスクープ

翌日の朝刊に掲載するホットな独自ニュースやコラムを平日の午後6時ごろに配信します。

20年の東京五輪には国内外から多くの観光客が首都圏に訪れ、交通機関や情報通信の利用者が膨らむ。19年も大阪での20カ国・地域（G20）首脳会議や横浜でのアフリカ開発会議（TICAD）といった外交日程があり、海外首脳がこぞって来日する。重要インフラの安全性向上は喫緊の課題になっている。

政府関係者によると、日本の重要インフラの機能がサイバー攻撃で停止したことはないが、事業者の事情による障害は起きている。たとえば18年12月に発生し、約3060万回線に影響した[ソフトバンク](#)の通信障害。原因はスウェーデン通信機器大手エリクソンの交換設備でソフトに異常が起きたためとされる。

政府はこうした事情を踏まえ、18年4月にまとめた重要インフラのサイバー対策に関する「安全基準等策定指針」を改定する。強制力はないが、事業者に求められる項目を整理したもので、取り組み状況を検証して公表する。事業者が指針に基づく対策を講じないままサイバー攻撃を受け、機能が停止した場合、厳しい行政処分を受けることもある。



重要インフラ14分野のサイバー対策に関する安全基準の指針を改定する

見直しの柱は官民の情報共有の強化だ。政府は今年4月、政府機関や重要インフラ事業者、大学などを集めて最新のサイバー攻撃の手口や防衛策を話し合う「サイバーセキュリティ

「協議会」を発足させる。この協議会を活用し、迅速な情報提供を呼びかける。

従来も内閣サイバーセキュリティセンター（NISC）などが個別に政府機関や企業の相談に応じていたが、官民が1カ所に集まり協議するのは初めて。メンバーに守秘義務を課し、情報流出のリスクが低い専用ネットワークでやりとりする。

事業者による情報通信機器の交換や、ソフトウェアの更新に伴うシステム障害への対策強化も盛り込む。外部からの攻撃だけでなく、ソフトバンクのような事業者の不備による機能停止を防ぐためだ。事前の点検を徹底するよう促し、危機を見越して手順や計画を詰めるよう求める。

重要インフラ14分野とサービス障害例

情報通信	通信、放送サービスの停止	¥
金融	預金払い戻しの遅延・停止	
航空	航空機の安全運航に支障	✈️
空港	空港警備態勢に支障	
鉄道	列車の安全輸送に支障	🚂
電力	電力供給の停止	
ガス	ガス供給の停止	🔥
行政	行政サービスに支障	
医療	医療機器の誤作動	🏥
水道	水の供給の停止	
物流	輸送の遅延・停止	🚚
化学	プラントの停止	
クレジット	カード情報の漏洩	💳
石油	石油供給の停止	

災害への備えも明記する。18年9月に北海道地震が発生し国内で初めて電力会社管内の大規模停電（ブラックアウト）が発生したことや、台風21号による高潮と高波で関西国際空港が機能停止に陥ったのを踏まえる。事業者のもつ電子データの海外流出を防ぐため、国内サーバーに保管することも求める。

政府はサイバーセキュリティ戦略本部の「重要インフラ専門調査会」を17日に開き、改定に向けた議論に取りかかる。政府が昨年12月にまとめた情報通信機器の調達に関する申し合わせも議論する。安全保障上のリスクのある機器は調達しない政府方針を説明し、事業者にも同様の対応を促す考えだ。

本サービスに関する知的財産権その他一切の権利は、日本経済新聞社またはその情報提供者に帰属します。また、本サービスに掲載の記事・写真等の無断複製・転載を禁じます。

Nikkei Inc. No reproduction without permission.