National center of Incident readiness and Strategy for Cybersecurity

政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月24日）のポイント

令和６年７月

内閣官房 内閣サイバーセキュリティセンター

制度・監督ユニット

ガイドライン（令和５年度版）一部改定の主なポイント

NISC

➢ 直近に発生した重大インシデントからの教訓・対策や最近の技術動向等を反映し、必要な改定を行うもの。

ポイント	内容
１．リスクの高い地域への出張時等におけるセキュリティ対策の強化	➢ リスクの高い地域に端末を携行する際には、第三者による物理的なアクセスのリスクへの対策を実施すること。例えば、USBポートをふさぐ等の対策を施した専用端末を常時携行することのほか、帰国後に端末を工場出荷時の状態に戻すことが望ましい。
２．サプライチェーン・リスク対策の強化	➢ 機器等やクラウドサービスの調達において、事業者等所在国の法的手続きのリスクに留意する等、サプライチェーン・リスク対策について、適切に対応すること。
３．情報セキュリティ早期警戒パートナーシップ	➢ 「情報セキュリティ早期警戒パートナーシップ※」の活動から通知された場合を含め、アプリケーション・コンテンツの脆弱性が発覚した場合には、速やかに必要な対応を行うこと。
４．SBOM（Software Bill of Materials: ソフトウェア部品表）	➢ サプライチェーン全体のソフトウェアに係るリスクに対して適切に対応するため、必要に応じて、SBOMの作成、提供等を調達先に求めること。
５．IoT製品に対するセキュリティ適合性評価制度	➢ IoT製品を調達する際には、「IoT製品に対するセキュリティ適合性評価制度」を活用して、選定・調達すること（IoT製品に対するセキュリティ適合性評価制度は2024年度中に開始予定の制度であるが、将来を見据えて先行的に記載）。

※平成29年経済産業省告示第十九号を踏まえた活動

https://www.nisc.go.jp/