

テレワーク環境セキュリティチェックリスト

自宅・外出先からの業務を安全に行うための16項目

情シス365 | <https://www.josis365.com>

1. 端末のセキュリティ

- 業務用PCにEDR / ウイルス対策ソフトが導入されている
- OSとアプリケーションのセキュリティアップデートが適用されている
- BitLocker (Windows) またはFileVault (Mac) でディスク暗号化が有効
- Intune等のMDMでデバイスが管理されている

2. 認証・アクセス制御

- Microsoft 365 / Google Workspaceに多要素認証 (MFA) が有効
- 条件付きアクセスポリシーで、社外アクセス時のセキュリティを強化している
- VPN経由でのアクセスが必要な場合、VPN接続が正しく設定されている
- 個人デバイス (BYOD) からのアクセスルールが明確に定められている

3. ネットワーク

- 自宅のWi-Fiルーターのファームウェアが最新版に更新されている
- 自宅のWi-FiがWPA3またはWPA2で暗号化されている (WEPは使用禁止)
- 公衆Wi-Fi (カフェ、ホテル等) での業務利用ルールが定められている

4. データ管理

- 業務データはクラウド (SharePoint / OneDrive) に保存し、ローカル保存を最小限にしている
- USBメモリ等の外部記録媒体への業務データコピーを制限している
- 画面共有時に機密情報が映り込まないように注意喚起している

5. 運用・教育

- テレワーク時のセキュリティルールが文書化され、社員に周知されている
- インシデント発生時 (PC紛失、不審メール等) の報告先と手順が明確

判定目安

14～16項目：十分な対策ができています。

10～13項目：基本はできていますが、未対応の項目を優先的に対策しましょう。

9項目以下：テレワーク環境のセキュリティリスクが高い状態です。早急にご相談ください。

テレワーク環境のセキュリティ対策は 情シス365 まで

<https://www.josis365.com> | 無料相談: <https://meetings-na2.hubspot.com/e-kameta>