サイバーセキュリティ

診断チェック表

第６回：具体的な構築・運用の実践

check 01	☐	エンドポイント機器でアクセス可能な情報を保護している。
check 02	☐	特権アクセスを最小化し、定期見直ししている。
check 03	☐	アクセス制御方針に基づき権限を設定している。
check 04	☐	ソースコード等のアクセス権を管理している。
check 05	☐	多要素認証などの安全な認証を運用している。
check 06	☐	容量・性能などの資源利用を監視し、調整している。
check 07	☐	マルウェア対策と利用者周知を実施している。
check 08	☐	脆弱性情報を収集し、評価・対処している。
check 09	☐	セキュア構成のベースラインを維持している。
check 10	☐	不要情報を削除している。
check 11	☐	データマスキングを方針・要求事項に従って適用している。
check 12	☐	データ漏えい防止対策を適用している。
check 13	☐	バックアップを取得し、定期的に検査している。
check 14	☐	可用性要件に応じて冗長化を構成している。
check 15	☐	ログを取得・保護し、分析している。
check 16	☐	監視を行い、異常時に対応している。
check 17	☐	システム時刻を基準時刻と同期している。
check 18	☐	特権ユーティリティの使用を制限し、厳しく管理している。
check 19	☐	本番環境へのソフト導入を手順化し管理している。
check 20	☐	ネットワークのセキュリティを管理・制御している。

令和７年度
中小企業サイバーセキュリティ支援事業 実践力強化プログラム
※当事業は東京都より委託を受け、株式会社 NTT ExC パートナー（エヌ・ティ・ティ エクシーパートナー）が運営しています。
事業の公式サイトはこちら
https://zissenkyouka.metro.tokyo.lg.jp/