テレワークアセスメント結果

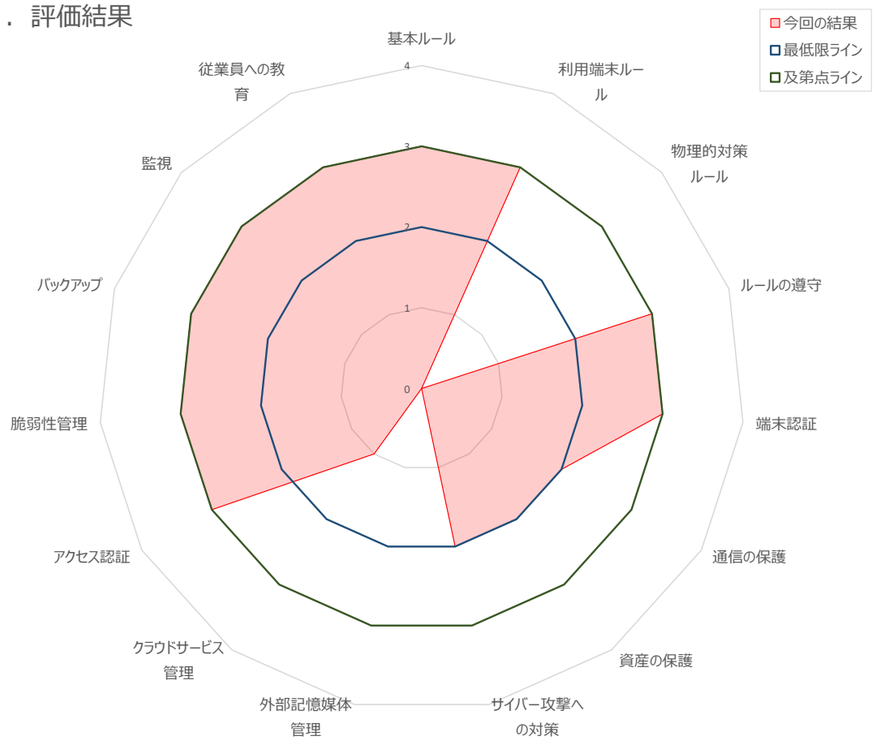
1．総評

評価結果の平均値	2.27
及第点ライン以上の項目	9
最低限ラインを満たす項目	3

評価コメント

評価結果の平均値は2.27点でした。
及第点ライン以上の項目が9項目、
最低限ラインを満たす項目が3項目あります。
及第点ライン以上の項目は「基本ルール」「利用端末ルール」「ルールの遵守」「端末認証」「アクセス認証」「脆弱性管理」「バックアップ」「監視」「従業員への教育」です。
最低限ラインを満たす項目は「通信の保護」「資産の保護」「サイバー攻撃への対策」です。
最低限ラインに満たない項目は、「物理的対策ルール」「外部記憶媒体管理」「クラウドサービス管理」です。
「３．項目別評価」の内容に従い、最低限ラインに満たない項目に優先して追加対策を実施することを推奨します。

2．評価結果



3．項目別評価

対策分類	対策項目	質問内容	質問の意図	回答	最低限ライン	及第点ライン	今後実施すべき対応
ルール整備	基本ルール	テレワークについて全社的な規程、ルールがありますか。	自社の業務状況に応じた、テレワークの規程、ルールを策定しましょう	3	2	3	テレワークに関する全般的な規程のみでなく、より具体的なセキュリティに関するルール整備により、レベル向上が可能です。
	利用端末ルール	テレワークが可能な端末のルールを定めていますか。	会社支給でない私物のPCやスマホの無断業務利用は、リスクが高くなります	3	2	3	必要な対策が取られています。取り組みの継続により、サイバー攻撃への対応力が維持・向上されます。
	物理的対策ルール	テレワークが可能な場所のルールを定めていますか。	カフェや公共の場での端末利用は、覗き見や不正操作、盗難、紛失のリスクが高いです	0	2	3	社外での端末利用状況について、まず把握しましょう。
	ルールの遵守	テレワーク対象の従業員より規程、ルールを遵守する誓約書を取得していますか。	策定した規程、ルールの確実な遵守には、誓約書の取得が効果的です	3	2	3	必要な対策が取られています。全従業員への誓約書取得により、ルールの周知がされています。
端末環境の技術対策	端末認証	端末ログインにどのような認証を導入していますか。	テレワークは利用する場所により部外者が不正操作するリスクが高いため、強固なログイン認証が望ましいです	3	2	3	多要素による認証を行うことで、パスワードの漏洩を原因とする不正アクセスを、更に高いレベルで防止できます。
	通信の保護	テレワーク端末の通信をどのように保護していますか。	自宅等あまり安全でないネットワークの業務利用を前提とすると、暗号通信が不可欠です	2	2	3	テレワーク端末をサイバー攻撃から保護するために、インターネット通信を保護する仕組みの導入・選定が必要です。
	資産の保護	テレワーク端末内部の記憶媒体について、どのようなデータ保護対策を実施していますか。	テレワークは物理的な紛失・盗難リスクが高いため、端末内部の記憶媒体暗号化等、対策が不可欠です	2	2	3	端末紛失・盗難の際の情報漏洩を防止するため、データの自動暗号化、無意味化といった記憶媒体にデータが平文のまま残らない仕組みを導入することが必要です。
	サイバー攻撃への対策	テレワーク端末にどのようなマルウェア対策を実施していますか。	端末へのアンチウイルスソフトの導入や、アラートの監視による即時の対応が重要です	2	2	3	アンチウイルスソフトでは検知できないサイバー攻撃への対応力向上のためには、EDRを導入することが必要です。
	外部記憶媒体管理	SDカード、USBメモリなどの外部記憶媒体などの利用を制限していますか。	テレワークは利用状況が見えないため、媒体利用はなるべく監視・制限すべきです	0	2	3	外部記憶媒体の利用制限状況について、まず把握しましょう。
システム環境の技術対策	クラウドサービス管理	テレワークで利用するクラウドサービス等外部サービスにどのような認証を導入していますか。	クラウドサービスは世界中どこからでもアクセスできるため、利用者を識別するための強固な認証（多要素認証、デバイス認証等）によるアクセス制御が不可欠です	1	2	3	不正アクセスを防止するために、制御の適用を原則とするルールを策定し、導入することが必要です。
	アクセス認証	社内ネットワークへの接続（VPN、リモートデスクトップ、VDI等）にどのような認証を導入していますか。	社内ネットワークへの侵入を防止するために、強固な認証（多要素認証、デバイス認証等）が不可欠です	3	2	3	多要素による認証は機器盗難時にも不正アクセスが防止されるため、更に高いレベルの対策効果が期待できます。
	脆弱性管理	テレワークで利用するシステム（業務システムのOS・アプリケーション、通信機器、端末）の脆弱性を管理していますか。	脆弱性管理による継続的なパッチ適用等運用が、サイバー攻撃対策として不可欠です	3	2	3	管理・運用の対象を業務システムに広げられるのであれば、サイバー攻撃への更なる対応力向上が期待できます。
	バックアップ	テレワークでアクセス可能な重要データは定期的にバックアップしていますか。	テレワークアクセスはリスクが高くなるため、攻撃に備えたバックアップが重要です	3	2	3	取得したバックアップが確実に復元できるようにテストを行うことで、万一のデータ消失や改ざんにおける迅速な復旧が期待できます。
インシデント対応	監視	端末の操作状況を監視し、通知する仕組みを運用していますか。	テレワークは利用状況が見えないため、端末操作状況のリアルタイム監視が望ましいです	3	2	3	ログ分析により、不正につながる操作を検出することで、内部不正の未然防止・検知のレベル向上が期待できます。
	従業員への教育	テレワークを悪用した標的型メール攻撃等への対策教育・訓練を実施していますか。	テレワークを悪用した標的型メール攻撃が増加しているため、教育・訓練は重要です	3	2	3	テレワークについて教育・訓練を定期的に行うことで、更なる従業員のセキュリティ意識の定着が期待できます。