

# リスクグループ分析対策表

場所	1F-HD	情報資産分類	1F-IT-DT-HD	使用用途持出し	有り	発行主管	※※ ※※
保管形態	電子データ	情報資産価値	12	ネット接続	無し	管理責任者(保有者)	※※ ※※

情報資産の価値		リスクアセスメント											リスク対応計画				
		脅威		脆弱性			対策後(今回追加)										
		脅威	ポイント	考えられる脆弱性	現状の管理策	ポイント	リスク値	管理策	規程	項番	脆弱ポイント	管理策番号				リスク値	(対応) ・低減 ・受容 ・回避 ・移転
完全性 可用性	4	破壊	3	安全領域でのセキュリティ対策が不十分	重要な資産を許可されていないアクセス、損傷及び妨害から守る安全領域を定めていない。	3	36	重要な資産を許可されていないアクセス、損傷及び妨害から守る安全領域を定める。	物理的・環境的管理規程	2.1	1	A.9.1.1	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
完全性 可用性	4	破壊	3	安全領域でのセキュリティ対策が不十分	安全領域への入室許可するための手続きを定めていない。	3	36	安全領域への入室許可するための手続きを定める。	物理的・環境的管理規程	2.2	1	A.9.1.2	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
完全性 可用性	4	破壊	3	安全領域でのセキュリティ対策が不十分	安全領域でのセキュリティ対策の管理策を定めていない。	3	36	安全領域でのセキュリティ対策の管理策を定める。	物理的・環境的管理規程	2.3	1	A.9.1.3	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
完全性 可用性	4	破壊	3	安全領域でのセキュリティ対策が不十分	安全領域でのセキュリティ事項を定めていない。	3	36	安全領域での社員および第三者の作業における注意事項を定める。	物理的・環境的管理規程	2.5	1	A.9.1.5	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
完全性 可用性	4	破壊	3	安全領域でのセキュリティ対策が不十分	安全領域でのセキュリティレベルを保つため、宅配業者等の引き渡し場所と安全領域とを引き離すように定めている。	3	36	安全領域でのセキュリティレベルを保つため、宅配業者等の引き渡し場所と安全領域とを引き離すように定める。	物理的・環境的管理規程	2.6	1	A.9.1.6	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
完全性 可用性	4	破壊	3	システムの維持管理の手続きが不明確	障害が発生した場合、早期復旧のためバックアップを取得するように定めていない。	3	36	社内サーバ等についてバックアップを行い、媒体について定期的に検査するように定める。	通信・運用管理規程	6.1	1	A.10.5.1	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
機密性 可用性	4	盗難	3	安全領域でのセキュリティ対策が不十分	重要な資産を許可されていないアクセス、損傷及び妨害から守る安全領域を定めていない。	3	36	重要な資産を許可されていないアクセス、損傷及び妨害から守る安全領域を定める。	物理的・環境的管理規程	2.1	1	A.9.1.1	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
機密性 可用性	4	盗難	3	安全領域でのセキュリティ対策が不十分	安全領域への入室許可するための手続きを定めていない。	3	36	安全領域への入室許可するための手続きを定める。	物理的・環境的管理規程	2.2	1	A.9.1.2	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
機密性 可用性	4	盗難	3	安全領域でのセキュリティ対策が不十分	安全領域でのセキュリティ対策の管理策を定めていない。	3	36	安全領域でのセキュリティ対策の管理策を定める。	物理的・環境的管理規程	2.3	1	A.9.1.3	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
機密性 可用性	4	盗難	3	安全領域でのセキュリティ対策が不十分	安全領域でのセキュリティ事項を定めていない。	3	36	安全領域での社員および第三者の作業における注意事項を定める。	物理的・環境的管理規程	2.5	1	A.9.1.5	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
機密性 可用性	4	盗難	3	安全領域でのセキュリティ対策が不十分	安全領域でのセキュリティレベルを保つため、宅配業者等の引き渡し場所と安全領域とを引き離すように定めている。	3	36	安全領域でのセキュリティレベルを保つため、宅配業者等の引き渡し場所と安全領域とを引き離すように定める。	物理的・環境的管理規程	2.6	1	A.9.1.6	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
機密性 可用性	4	盗難	3	装置のセキュリティ対策が不十分	パソコン等の装置を外出する場合の取り扱いを定めていない。	3	36	社外へ持ち出す場合の手続きを定める。作業用パソコンの持ち出しルールを定める。	物理的・環境的管理規程	3.5	1	A.9.2.5	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
機密性 可用性	4	盗難	3	情報資産の持ち出し手続きが明確	管理責任者の許可なしに移動してはならないことを定めていない。	3	36	・情報資産は社外に持ち出さない。持ち出す場合は、許可を得るように定める。情報資産の持ち出しルールを定める。移動バックについては持ち出し許可をする。ただし、定期的な所在確認は行う。	物理的・環境的管理規程	3.7	1	A.9.2.7	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
機密性 可用性	4	盗難	3	情報の取扱い手続きが不明確	情報の取扱いについて定めていない。	3	36	情報の取扱いについて定める。	通信・運用管理規程	8.3	1	A.10.7.3	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
機密性 可用性	4	盗難	3	システムの維持管理の手続きが不明確	障害が発生した場合、早期復旧のためバックアップを取得するように定めていない。	3	36	社内サーバ等についてバックアップを行い、媒体について定期的に検査するように定める。	通信・運用管理規程	6.1	1	A.10.5.1	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ
機密性	4	不正アクセス	3	運用の手続きが不明確	サーバー等のバックアップや保守に関する操作手順書等を定めていない。	3	36	バックアップや設定変更(変更履歴を含む)の操作手順について定める。	通信・運用管理規程	2.1	1	A.10.1.1	12	低減	情報セキュリティ管理者	'06/10/10	人的工数のみ