脅威脆弱性リスト　　電子

承認
2014/10/1

想定脅威			想定脆弱性				
内容			NO	内容	A2005	A2013	
人的脅威外部（非許可者）	事務所	許可無くエリアに入ってきてしまう	1	・物理的なセキュリティ境界を明確にできていない。（受付、表示、扉、など）	911	1111	
			2	・物理的な入退室管理ができていない。（アクセス制御、外来者台帳、など）	912	1112	
			3	・部外者であることが名札などで識別できていない。（ので、統制できない）	912	1112	
			4	・外来者の受付手順がない。外来者の入室記録がとられていない。	912	1112	
			5	・受け渡しエリアなど、許可しているエリアがない。	916	1116	
			6	・打合せ場所、等がセキュリティ境界の内側にあり、入れざるを得ない。	913	1113	
			7	・許可された場所まで導くパーティションの区切りや立ち会う等のルールがない。	915	1115	
	PC 記憶媒体（保存）	許可無く情報にアクセスされてしまう。 他人になりすまされて情報にアクセスされてしまう。	8	・クリアスクリーンができていない。（スクリーンセイバーパスワード）	1133	1129	
			9	・無人状態にある装置の保護ができていない。（ｽｸﾘｰﾝｾｲﾊﾞﾊﾟｽﾜｰﾄﾞ）	1132	1128	
			10	・パスワードが設定されていない。または、推測できるパスワードとなっている。	1131	931	
			11	・必要のないアクセス権が設定されている。（アクセス制御ができていない）	1124	925	
			12	・不必要なビルトインアカウント(guest、等）やテストアカウントが有効になっている。	1121	921	
			13	・パスワードが、デフォルト値のまま有効になっている。	1123	924	
			14	・ユーザ認証（例えばID,パスワード等）がされていない。	1152	921	
			15	・ログオンの失敗回数を制限していない。	1151	942	
			16	・メンテナンスポートなど正規以外のアクセス経路がある。	1144		
			17	・システム的な脆弱性を防御できていない。（適切なパッチが当っていない）	1254		
			18	・やめた人などの古いIDが有効になっている。（定期的なアクセス権の見直しがNG)	833	926	
			19	・アクセスログ、履歴がとられていない。	10101	1241	
			20	・ログを保護していない。	10103	1242	
			21	・時刻が合っていない。（ログの時刻を合わせる必要がある）	10106	1244	
			22	・共有IDを使用している。	1121	921	
			23	・パスワードが定期的に変更されていない。	1131	931	
			24	・セキュリティの外側にアクセス制御されていないLANケーブルがあった。	1141	912	
			25	・（脆弱性がわかる）システム文書（社内ネットワーク図等）が適切に保管されていな	1074		
			26	・社外HPが適切に運用管理されていない。	1093		
			27	・社外からのリモートアクセスにおいて適切なユーザ認証がされていない。	1142		
		許可無く情報をこわされてしまう	28	・メディアが適切に保管されていない。	1071	831	
			29	・バックアップがとられていない。	1051	1231	
			30	・ウィルスワクチンソフトが導入されていない。	1041	1221	
			31	・システム的な脆弱性を防御できていない。（適切なパッチが当っていない）	1254		
			32	・許可されていないスパイウェアが起動させられてしまう。	1041	1221	
			33	・壊されたこと、無くなったことがわからない。	711	811	
			34	・情報資産のオーナが明確になっていない。	712	812	
			35	・装置が適切に保護されていない。（PCが通路側に立てて置いてあった、等）	921	1121	
			36	・ケーブルに足をひっかけて、装置が落下してしまいそうである。	923	1123	
		許可無く情報を持ち出されてしまう	28	・メディアが適切に保管されていない。	1071	831	
			32	・許可されていないスパイウェアが起動させられてしまう。	1041	1221	
			30	・ウィルスワクチンソフトが導入されていない。	1041	1221	
			31	・システム的な脆弱性を防御できていない。（適切なパッチが当っていない）	1254		
			34	・情報資産のオーナが明確になっていない。	712	812	
			37	・捨てたはずの情報を持ちだされてしまう。（廃棄がキチンとできていなかった）	1072	832	
			38	・機器の盗難防止がされていない。	921	1121	
			39	・渡して良い情報と渡していけない情報が区別できていない。	722	822	
			40	・重要度の分類の指針がない。	721	821	
			41	・持ち出されたことがわからない。	711	811	
	通信	通信データを盗聴されてしまう	42	・ルータやハブの空きポートからデータをのぞき見されてしまう。（ポートの保護）	923	1123	
			43	・無線LANに対するアクセス制御ができていない。	1061	1311	
			44	・重要な情報をやりとりするときに、暗号化やパスワードによる保護がされていない。	1084	1323	
			45	・電子メール、電子データの取扱いに対するルールが不十分である。	1084	1323	
	PC 記憶媒体（搬送・輸送）	輸送中に情報を紛失してしまう	46	・輸送物の重要度に応じた輸送業者を適切に選定していない。選定ルールがない。	1083	833	
			47	・媒体・情報の輸送時の取扱いに関するルールがない。	722	822	
			48	・輸送物の重要度に応じた保護策がとられていない。	1083	833	
	PC 記憶媒体	修理ミスが発生してしまう	49	・修理内容に応じた業者を適切に選定していない。選定ルールがない。	924	1124	
			50	・外部の人の作業の立会い、監視がおこなわれていない。	915	1115	
	PC 記憶媒体	画面や印刷物をのぞき見されてしまう。	8	・クリアスクリーンができていない。（スクリーンセイバパスワード）	1133	1129	
			9	・無人状態にある装置の保護ができていない。（ｽｸﾘｰﾝｾｲﾊﾞﾊﾟｽﾜｰﾄﾞ）	1132	1128	
			51	・外部の人の作業の監視が行なわれていない。	915	1115	
			52	・外部の人が通る通路、動線に対して目隠しなどの配慮がされていない。	1133	1129	
			53	・外部の人に許可している作業領域がない。不十分である。	916	1116	
			134	・プリンタに出力したものがおきっぱなしである。	1133	1129	

想定脅威			想定脆弱性				
内容			NO	内容	関連管理策		
人的脅威外部委託(許可者)	事務所	許可無くエリアに入ってきてしまう。	1	・物理的なセキュリティ境界を明確にできていない。(受付、表示、扉、など)	911	1111	
			2	・物理的な入退室管理ができていない。(アクセス制御、外来者台帳、など)	912	1112	
			3	・外部委託者であることが名札などで識別できていない。(ので、統制できない)	912	1112	
			54	・外部委託者の入室記録の記録がとられていない。(後からわかる仕組みがない)	912	1112	
			55	・非許可者の一時許可、の受付ルールがない。	912	1112	
			5	・受け渡しエリアなど、許可しているエリアがない。	916	1116	
			6	・打合せ場所、等がセキュリティ境界の内側にあり、入れざるを得ない。	913	1113	
			7	・許可された場所まで導くパーティションの区切りや立ち会う等のルールがない。	915	1115	
			56	・夜間、休日の入室ルールがない。	912	1112	
			57	・セキュリティに関するルールの説明ができていない。	822	722	
	PC 記憶媒体(保存)	許可されていない情報にアクセスされてしまう。 他人になりすまされて許可されてない情報にアクセスされてしまう。	58	・アクセス制御ポリシー(考え方や定義)がない。文書化されていない。	1111	911	
			8	・クリアスクリーンができていない。(スクリーンセイバーパスワード)	1133	1129	
			9	・無人状態にある装置の保護ができていない。(ｽｸﾘｰﾝｾｲﾊﾞｰﾊﾟｽﾜｰﾄﾞ)	1132	1128	
			10	・パスワードが設定されていない。または、推測できるパスワードとなっている。	1131	931	
			11	・必要のないアクセス権が設定されている。(アクセス制御ができていない)	1124	925	
			12	・不必要なビルトインアカウント(guest、等)やテストアカウントが有効になっている。	1121	921	
			13	・パスワードが、デフォルト値のまま有効になっている。	1123	924	
			14	・ユーザ認証(例えばID,パスワード等)がされていない。	1152	921	
			15	・ログオンの失敗回数を制限していない。	1151	942	
			16	・メンテナンスポートなど正規以外のアクセス経路がある。	1144		
			17	・システム的な脆弱性を防御できていない。(適切なパッチが当っていない)	1254		
			18	・やめた人などの古いIDが有効になっている。(定期的なアクセス権の見直しがNG)	833	926	
			19	・アクセスログ、履歴がとられていない。	10101	1241	
			20	・ログを保護していない。	10103	1242	
			21	・時刻が合っていない。(ログの時刻を合わせる必要がある)	10106	1244	
			22	・共有IDを使用している。	1121	921	
			23	・パスワードが定期的に変更されていない。	1131	931	
			24	・セキュリティの外側にアクセス制御されていないLANケーブルがあった。	1141	912	
			25	・(脆弱性がわかる)システム文書(社内ネットワーク図等)が適切に保管されていな	1074		
			27	・社外からのリモートアクセスにおいて適切なユーザ認証がされていない。	1142		
			59	・委託完了時のルールがない。	623	1512	
			60	・外部委託したソフトウェア開発を監督、監視ができていない。	1255	1427	
		許可なく情報を紛失してしまう	28	・メディアが適切に保管されていない。	1071	831	
			29	・バックアップがとられていない。	1051	1231	
			30	・ウィルスワクチンソフトが導入されていない。	1041	1221	
			31	・システム的な脆弱性を防御できていない。(適切なパッチが当っていない)	1254		
			32	・許可されていないスパイウェアが起動させられてしまう。	1041	1221	
			33	・壊されたこと、無くなったことがわからない。	711	811	
			34	・情報資産のオーナが明確になっていない。	712	812	
			35	・装置が適切に保護されていない。(PCが通路側に立てて置いてあった、等)	921	1121	
			36	・ケーブルに足をひっかけて、装置が落下してしまいそうである。	923	1123	
		許可無く情報を持ち出されてしまう。	37	・捨てたはずの情報を持ちだされてしまう。(廃棄がキチンとできていなかった)	1072	832	
			38	・機器の盗難防止がされていない。	921	1121	
			28	・メディアが適切に保管されていない。	1071	831	
			32	・許可されていないスパイウェアが起動させられてしまう。	1041	1221	
			30	・ウィルスワクチンソフトが導入されていない。	1041	1221	
			31	・システム的な脆弱性を防御できていない。(適切なパッチが当っていない)	1254		
			40	・重要度の分類の指針がない。	721	821	
			41	・持ち出されたことがわからない。	711	811	
			34	・情報資産のオーナが明確になっていない。	712	812	
			61	・持出して良い情報とよくない情報が区別できていない。	722	822	
			62	・持出し管理ルール／承認ルールが不十分。説明されていない。	927	1125	813
			63	・メディア(CD-R/DVD-R,等)に焼かれて持出されてしまう。	1071	831	
			64	・機密保持契約の締結がなされていない。	623	1512	
			65	・委託完了後のルールの説明がなされていない。	822	722	
			66	・委託完了後に情報・資産の返却ができていない。	832	814	
			67	・委託完了後のID、アクセス権等の無効処理ができていない。	833	926	
		操作を間違ってしまう。 オペミスしてしまう。	68	・操作手順書がない。	1011	1211	
			69	・特権管理がされていない。	1122	923	
			70	・管理者の作業記録が取られていないのでどこまでやったかわからない	10104	1243	
			71	・管理者権限のIDと一般権限のIDは分割できていない。	1013	612	
	通信	通信データを盗聴されてしまう	42	・ルータやハブの空きポートからデータをのぞき見されてしまう。(ポートの保護)	923	1123	
			43	・無線LANに対するアクセス制御ができていない。	1061	1311	
			44	・重要な情報をやりとりするときに、暗号化やパスワードによる保護がされていない。	1084	1323	
			45	・電子メール、電子データの取扱いに対するルールが不十分である。	1084	1323	
	メール	送信ミスしてしまう	72	・重要な情報を誤って異なる送信先へ送信してしまう。	1084	1323	
			73	・許可されてていない情報を送ってしまう。	722	822	
	PC 記憶媒体(搬送・輸送)	輸送中に情報を紛失してしまう	46	・輸送物の重要度に応じた輸送業者を適切に選定していない。選定ルールがない。	1083	833	

			47	・媒体・情報の輸送時の取扱いに関するルールがない。	722	822	
			48	・輸送物の重要度に応じた保護策がとられていない。	1083	833	
			74	・モバイルPCに関する管理策がとられていない。	1171	621	
			75	・外部記憶媒体に関する管理策がとられていない。	1071	831	
			76	・携帯電話に関する管理策がとられていない（パスワード、ストラップ、等）	1073	833	
	PC 記憶媒体	修理ミスが発生してしまう	49	・修理内容に応じた業者を適切に選定していない。選定ルールがない。	924	1124	
			50	・外部の人の作業の立会い、監視がおこなわれていない。	915	1115	
	廃棄	廃棄したものから情報が漏れる	77	・重要度に応じた装置の廃棄ルールがない。わからない。	926	1127	
			78	・重要度に応じた媒体の廃棄ルールがない。わからない。	1072	832	
			79	・廃棄業者に対して、セキュリティ要求事項を明確にしていない。	1082	1322	
			80	・廃棄業者に対して、機密保持契約がなされていない。	623	1512	
	PC 記憶媒体	画面や印刷物をのぞき見されてしまう	8	・クリアスクリーンができていない。（スクリーンセイバパスワード）	1133	1129	
			9	・無人状態にある装置の保護ができていない。（ｽｸﾘｰﾝｾｲﾊﾞﾊﾟｽﾜｰﾄﾞ）	1132	1128	
			52	・外部の人が通る通路、動線に対して目隠しなどの配慮がされていない。	1133	1129	
			134	・プリンタに出力したものがおきっぱなしである。	1133	1129	
	引越し 移動	引越し時にものが無くなる	81	・引越し業者を適切に選定できていない。	1082	1322	
			82	・機密保持契約が取り交わされていない。	623	1512	
			83	・搬出数と搬入数の荷物チェックを行なっていない。	1083	833	
	顧客支給品	顧客の要求どおりに取扱いができない	84	・借用時に使用条件、管理ルールが明確になっていない。	1081	1321	
			85	・授受記録がない。	1082	1322	
			86	・使用期限満了時に速やかに返却、廃棄、消去ができていない。	832	814	
			87	・借用期間中の厳正な保管管理ができていない。1073	722	822	823
想定脅威			想定脆弱性				
内容			NO	内容	関連管理策		
人的脅威内部 （許可者）	マシン室 （セキュリティエリア）	許可されていないエリアに入ってきてしまう。	88	・物理的なセキュリティ境界を明確にできていない。（受付、表示、扉、など）	911	1111	
			89	・物理的な入退室管理ができていない。（アクセス制御、外来者台帳、など）	912	1112	
			90	・一時許可者であることが名札などで識別できていない。（ので、統制できない）	912	1112	
			91	・入室記録、外来者の記録がとられていない。（後からわかる仕組みがない）	912	1112	
			92	・非許可者の一時許可、の受付ルールがない。	912	1112	
			93	・受け渡しエリアなど、許可しているエリアがない。	916	1116	
			94	・打合せ場所、等がセキュリティ境界の内側にあり、入れざるを得ない。	913	1113	
			95	・許可された場所まで導くパーティションの区切りや立ち会う等のルールがない。	915	1115	
			96	・夜間、休日の入室ルールがない。	912	1112	
			97	・セキュリティに関するルールの説明ができていない。	822	722	
			98	・マシン室にはマシン室と表示しない、ができていない。	913	1113	
	PC 記憶媒体 （保存）	許可されていない情報にアクセスされてしまう。 他人になりすまされて許可されてない情報にアクセスされてしまう。	58	・アクセス制御ポリシー（考え方や定義）がない。文書化されていない。	1111	911	
			8	・クリアスクリーンができていない。（スクリーンセイバーパスワード）	1133	1129	
			9	・無人状態にある装置の保護ができていない。（ｽｸﾘｰﾝｾｲﾊﾞﾊﾟｽﾜｰﾄﾞ）	1132	1128	
			10	・パスワードが設定されていない。または、推測できるパスワードとなっている。	1131	931	
			11	・必要のないアクセス権が設定されている。（アクセス制御ができていない）	1124	925	
			12	・不必要なビルトインアカウント(guest、等）やテストアカウントが有効になっている。	1121	921	
			13	・パスワードが、デフォルト値のまま有効になっている。	1123	924	
			14	・ユーザ認証（例えばID,パスワード等）がされていない。	1152	921	
			15	・ログオンの失敗回数を制限していない。	1151	942	
			16	・メンテナンスポートなど正規以外のアクセス経路がある。	1144		
			17	・システム的な脆弱性を防御できていない。（適切なパッチが当っていない）	1254		
			18	・やめた人などの古いIDが有効になっている。（定期的なアクセス権の見直しがNG）	833	926	
			19	・アクセスログ、履歴がとられていない。	10101	1241	
			20	・ログを保護していない。	10103	1242	
			21	・時刻が合っていない。（ログの時刻を合わせる必要がある）	10106	1244	
			22	・共有IDを使用している。	1121	921	
			23	・パスワードが定期的に変更されていない。	1131	931	
			24	・セキュリティの外側にアクセス制御されていないLANケーブルがあった。	1141	912	
			25	・（脆弱性がわかる）システム文書（社内ネットワーク図等）が適切に保管されていな	1074		
			27	・社外からのリモートアクセスにおいて適切なユーザ認証がされていない。	1142		
		許可されていない情報にアクセスされてしまう。	28	・メディアが適切に保管されていない。	1071	831	
			29	・バックアップがとられていない。	1051	1231	
			30	・ウィルスワクチンソフトが導入されていない。	1041	1221	
			31	・システム的な脆弱性を防御できていない。（適切なパッチが当っていない）	1254		
			32	・許可されていないスパイウェアが起動させられてしまう。	1041	1221	
			33	・壊されたこと、無くなったことがわからない。	711	811	
			34	・情報資産のオーナが明確になっていない。	712	812	
			35	・装置が適切に保護されていない。（PCが通路側に立てて置いてあった、等）	921	1121	
			36	・ケーブルに足をひっかけて、装置が落下してしまいそうである。	923	1123	
		許可無く情報を持ち出されてしまう。	38	・機器の盗難防止がされていない。	921	1121	
			28	・メディアが適切に保管されていない。	1071	831	
			32	・許可されていないスパイウェアが起動させられてしまう。	1041	1221	
			30	・ウィルスワクチンソフトが導入されていない。	1041	1221	
			31	・システム的な脆弱性を防御できていない。（適切なパッチが当っていない）	1254		

			34	・情報資産のオーナが明確になっていない。	712	812	
			40	・重要度の分類の指針がない。	721	821	
			41	・持ち出されたことがわからない。	711	811	
			61	・持出して良い情報と持出していけない情報が区別できていない。	722	822	
			62	・持出し管理ルール／承認ルールが不十分。説明されていない。	927	1125	813
			63	・メディア（CD-R/DVD-R,等）に焼かれて持出されてしまう。	1071	831	
			99	・電子メールで関係がないところに送信してしまう。	1084	1323	
			100	・誓約書の提出がなされていない。	813	712	
			101	・ISMSルールの教育・説明がなされていない。	822	722	
			102	・退職時に情報・資産の返却ができていない。	832	814	
			103	・退職後のID、アクセス権等の無効処理ができていない。	833	926	
			104	・懲戒に関するルールがない。	823	723	
		操作を間違ってしまう オペミスしてしまう	68	・操作手順書がない。	1011	1211	
			69	・特権管理がされていない。	1122	923	
			70	・管理者の作業記録が取られていないのでどこまでやったかわからない	10104	1243	
			71	・管理者権限のIDと一般権限のIDは分割できていない。	1013	612	
	メール	情報を間違って送信してし まう	72	・重要な情報を誤って異なる送信先へ送信してしまう。	1084	1323	
			73	・許可されていない情報を送ってしまう。	722	822	
			105	・電子メールの同報リストをメンテナンスしていない。	1084	1323	
			106	・電子メールを使用する際のルールや手順を説明できていない。理解できていない。	822	722	
			107	・転送して良いのか、そうでないのか、区別できていない。	722	822	
	PC 記憶媒体 （搬送・輸送）	情報を誤って紛失してしまう	46	・輸送物の重要度に応じた輸送業者を適切に選定していない。選定ルールがない。	1083	833	
			47	・媒体・情報の輸送時の取扱いに関するルールがない。	722	822	
			48	・輸送物の重要度に応じた保護策がとられていない。	1083	833	
			74	・モバイルPCに関する管理策がとられていない。	1171	621	
			75	・外部記憶媒体に関する管理策がとられていない。	1071	831	
			76	・携帯電話に関する管理策がとられていない（パスワード、ストラップ、等）	1073	833	
	PC 記憶媒体	修理ミスが発生してしまう	49	・修理内容に応じた業者を適切に選定していない。選定ルールがない。	924	1124	
	廃棄	廃棄すべき情報から情報が漏れる	77	・重要度に応じた装置の廃棄ルールがない。わからない。	926	1127	
			78	・重要度に応じた媒体の廃棄ルールがない。わからない。	1072	832	
	PC 記憶媒体	画面や印刷物をのぞき見されてしまう	8	・クリアスクリーンができていない（スクリーンセイバパスワード）	1133	1129	
			9	・無人状態にある装置の保護ができていない。（ｽｸﾘｰﾝｾｲﾊﾞﾊﾟｽﾜｰﾄﾞ）	1132	1128	
			52	・外部の人が通る通路、動線に対して目隠しなどの配慮がされていない。	1133	1129	
			134	・プリンタに出力したものがおきっぱなしである。	1133	1129	
	引越し 移動	引越し時にものが無くなる	81	・引越し業者を適切に選定できていない。	1082	1322	
			82	・機密保持契約、誓約書等が取り交わされていない。	623	1512	
			83	・搬出数と搬入数の荷物チェックを行なっていない。	1083	833	
	顧客支給品	顧客の要求どおりに取扱いができない	84	・借用時に使用条件、管理ルールが明確になっていない。	1081	1321	
			85	・授受記録がない。	1082	1322	
			86	・使用期限満了時に速やかに返却、廃棄、消去ができていない。	832	814	
			87	・借用期間中の厳正な保管管理ができていない。	722	822	823
想定脅威			想定脆弱性				
内容			NO	内容	関連管理策		
システム	PC 記憶媒体	ハードウェアが故障してしまった。 動作が不安定となってしまった。	108	・供給者が推奨する間隔、仕様での保守が行なわれていない。	924	1124	
			109	・重要なサーバの物理的なセキュリティが確保できていない（マシン室、ラック、等）	921	1121	
			110	・通信ケーブルが整理整頓、保護されていない	923	1123	
			111	・敷地外に置かれている装置に何も保護が行われいていない	925	1126	
			112	・アウトソーシング先とのサービスに関する合意がとれていない。	1021	1521	
			113	・アウトソーシング先へのセキュリティ要求事項が明確に示せていない。	1021	1521	
			114	・空調、電源,等の環境を考慮できていない。	922	1122	
			115	・情報システムのリソースを定期的に確認していない	1031	1213	
			116	・システムの使用状況を監視できていない。	10102		
			117	・情報システム導入時、受入試験を行っていない	1032	1429	
			118	・障害時のログが取得できていない。	10105	1241	
			38	・機器の盗難防止策が無い	921	1121	
			68	・操作手順がない。	1011	1211	
			29	・バックアップがとられていない。	1051	1231	
		ソフトウェアに障害が起こってしまった。 動作が不安定となってしまった。	68	・操作手順が無い	1011	1211	
			30	・ウイルスワクチンソフトがインストールされていない	1041	1221	
			117	・情報システム導入時、受入試験を行っていない	1032	1429	
			31	・システム的な脆弱性を防御できていない。（適切なパッチが当っていない）	1254		
			118	・障害時のログが取得できていない。	10105	1241	

			119	・変更発生時の手順が無い	1012	1212	
			120	・最新のパターンファイルに更新されていない	1041	1221	
			121	・許可無くフリーウェアをインストールして使用している。	1254		1262
			122	・許可無くソフトウエアをインストールことができる（ライセンス管理ができていない）	1512	1812	
		ウィルス、スパイウェアに感染してしまった。	123	・事故発生時の報告手順が決まっていない	1311	1612	
			124	・事故発生後の是正処置が行われていない、監視できるしくみがない	1322	1616	
			125	・ヒヤリハットの報告手順がきまっていない	1312	1613	
			126	・脆弱性の管理体制がない。	1261	1261	
			127	・復旧対策、体制が確立されていない。	1321	1611	
			30	・ウイルスワクチンソフトがインストールされていない	1041	1221	
			121	・許可無くフリーウェアをインストールことができる	1512	1812	1262
			120	・最新のパターンファイルに更新されていない	1041	1221	
			31	・システム的な脆弱性を防御できていない。（適切なパッチが当っていない）	1254		
			118	・障害時のログが取得できていない。	10105	1241	
	通信	通信障害が起こってしまった	110	・通信ケーブルの整理整頓、保護がされていない	923	1123	
			114	・空調、電源,等の環境を考慮できていない。	922	1122	
			111	・敷地外に置かれている装置に何も保護が行われいていない	925	1126	
			68	・操作手順が無い	1011	1211	
			119	・変更発生時の手順が無い	1012	1212	
			113	・アウトソーシング先へのセキュリティ要求事項が明確に示せていない。	1121	921	
			117	・情報システム導入時、受入試験を行っていない	1032	1429	
			127	・復旧対策・体制が確立されていない	1321	1611	
	電源	停電してしまった。	128	・UPSが設置されていない。有効なバッテリが設置されていない。	922	1122	
			29	・バックアップができていない。	1051	1231	
			129	・復旧手順（操作手順）が定められていない。	1011	1211	
自然災害	記憶媒体（保存）	地震	130	・転倒防止策が無い	914	1114	
			29	・バックアップが取られていない	1051	1231	
			131	・災害が発生したときの復旧対策・体制が確立されていない	1411	1711	
		火災	132	・火災警報装置が設置されていない	914	1114	
			133	・消火設備が設置されていない	914	1114	
			29	・バックアップが取られていない	1051	1231	
			131	・災害が発生したときの復旧対策・体制が確立されていない	1411	1711	
		落雷	29	・バックアップが取られていない	1051	1231	
			131	・災害が発生したときの復旧対策・体制が確立されていない	1411	1711	

想定脅威			想定脆弱性				
内容			NO	内容	A2005	A2013	
人的脅威外部（非許可者）	事務所	許可無くエリアに入ってきてしまう。	1	・物理的なセキュリティ境界を明確にできていない。（受付、表示、扉、など）	911	1111	
			2	・物理的な入退室管理ができていない。（アクセス制御、外来者台帳、など）	912	1112	
			3	・部外者であることが名札などで識別できていない。（ので、統制できない）	912	1112	
			4	・外来者の受付手順がない。外来者の入室記録がとられていない。	912	1112	
			5	・受け渡しエリアなど、許可しているエリアがない。	916	1116	
			6	・打合せ場所、等がセキュリティ境界の内側にあり、入れざるを得ない。	913	1113	
			7	・許可された場所まで導くパーティションの区切りや立ち会う等のルールがない	915	1115	
	紙文書 キングファイル	許可無く情報にアクセスされてしまう。	8	・クリアデスクができていない。（重要な書類がおきっぱなし）	1133	1129	
			9	・クリアスクリーンができていない。（表向きに置きっぱなし、消し忘れ、等）	1133	1129	
			10	・重要な書類が鍵のかかったキャビネットに保管されていない。	722	822	
			11	・鍵が管理されていない。	722	822	
			12	・（脆弱性がわかる）システム文書（社内ネットワーク図等）が適切に保管され	1074		
		許可無く情報をこわされてしまう、持ち出されてしまう。	13	・書類、文書が適切に保管されていない。	722	822	
			14	・壊されたこと、無くなったことがわからない。	711	811	
			15	・捨てたはずの文書を持出された（キチンと破棄できなかった）	722	822	
			16	・渡して良い情報と渡していけない情報が区別できていない。	722	822	
			17	・重要度の分類の指針がない。	721	821	
			18	・持ち出されたことがわからない。	711	811	
			19	・情報資産のオーナが明確になっていない。	712	812	
	紙文書 （搬送・輸送）	輸送中に紛失してしまう。	20	・輸送物の重要度に応じた輸送業者を適切に選定していない。選定ルールが	1083	833	
			21	・文書の重要度に応じた保護策がとられていない。	722	822	
	広げたファイル、印刷	印刷物をのぞき見されてしまう。	8	・クリアデスクができていない。（重要な書類がおきっぱなし）	1133	1129	
			9	・クリアスクリーンができていない。（表向きに置きっぱなし、消し忘れ、等）	1133	1129	
			22	・外部の人の作業の監視が行なわれていない。	915	1115	
			23	・外部の人が通る通路、動線に対して目隠しなどの配慮がされていない。	1133	1129	
			24	・コピー・FAXにおきっぱなしである。	1133	1129	
想定脅威			想定脆弱性				
内容			NO	内容	関連管理策		
人的脅威外部委託（許可者）	事務所	許可無くエリアに入ってきてしまう。 許可されていないエリアに入ってきてしまう。	1	・物理的なセキュリティ境界を明確にできていない。（受付、表示、扉、など）	911	1111	
			2	・物理的な入退室管理ができていない。（アクセス制御、外来者台帳、など）	912	1112	
			3	・外部委託者であることが名札などで識別できていない。（ので、統制できない	912	1112	
			25	・入室記録、外来者の記録がとられていない。（後からわかる仕組みがない）	912	1112	
			26	・非許可者の一時許可、の受付ルールがない。	912	1112	
			5	・受け渡しエリアなど、許可しているエリアがない。	916	1116	
			6	・打合せ場所、等がセキュリティ境界の内側にあり、入れざるを得ない。	913	1113	
			7	・許可された場所まで導くパーティションの区切りや立ち会う等のルールがない	915	1115	
			27	・夜間、休日の入室ルールがない。	912	1112	
			28	・セキュリティに関するルールの説明ができていない。	822	722	
	紙文書 キングファイル	許可されていない情報にアクセスされてしまう。	8	・クリアデスクができていない。（重要な書類がおきっぱなし）	1133	1129	
			9	・クリアスクリーンができていない。（表向きに置きっぱなし、消し忘れ、等）	1133	1129	
			10	・重要な書類が鍵のかかったキャビネットに保管されていない。	722	822	
			11	・鍵が管理されていない。	722	822	
			12	・（脆弱性がわかる）システム文書（社内ネットワーク図等）が適切に保管され	1074		
		許可無く情報をこわされてしまう、持ち出されてしまう。	13	・書類、文書が適切に保管されていない。	722	822	
			14	・壊されたこと、無くなったことがわからない。	711	811	
			15	・捨てたはずの文書を持出された（キチンと破棄できなかった）	722	822	
			17	・重要度の分類の指針がない。	721	821	
			18	・持ち出されたことがわからない。	711	811	
			19	・情報資産のオーナが明確になっていない。	712	812	
			29	・持出し管理ルール／承認ルールが不十分。説明されていない。	713	813	
			30	・持ち出して良い情報と持ち出していけない情報が区別できていない。	722	822	
			31	・機密保持契約の締結がなされていない。	623	1512	
			32	・委託完了後のルールの説明がなされていない。	822	722	
			33	・委託完了後に情報・資産の返却ができていない。	832	814	
			34	・委託完了後のID、アクセス権等の無効処理ができていない。	833	926	
	紙文書（搬送・輸送）	輸送中に紛失してしまう	20	・輸送物の重要度に応じた輸送業者を適切に選定していない。選定ルールが	1083	833	
			21	・文書の輸送に関するルールがない。	722	822	

	廃棄	廃棄したものから情報が漏れる	35	・重要度に応じた廃棄ルールがない。わからない。	722	822	
			36	・廃棄業者に対して、セキュリティ要求事項を明確にしていない。	1082	1322	
			37	・廃棄業者に対して、機密保持契約がなされていない。	623	1512	
	広げたファイル、印刷	印刷物をのぞき見されてしまう	9	・クリアスクリーンができていない。（表向きに置きっぱなし、消し忘れ、等）	1133	1129	
			22	・外部の人の作業の監視が行なわれていない。	915	1115	
			23	・外部の人が通る通路、動線に対して目隠しなどの配慮がされていない。	1133	1129	
			24	・コピー・FAXにおきっぱなしである。	1133	1129	
			8	・クリアデスクができていない。（重要な書類がおきっぱなし）	1133	1129	
	引越し 移動	引越し時にものが無くなる	38	・引越し業者を適切に選定できていない。	1082	1322	
			39	・機密保持契約が取り交わされていない。	623	1512	
			40	・搬出数と搬入数の荷物チェックを行なっていない。	1083	833	
	顧客支給品	顧客の要求どおりに取扱いができない	41	・借用時に使用条件、管理ルールが明確になっていない。	1081	1321	
			42	・授受記録がない。	1082	1322	
			43	・使用期限満了時に速やかに返却、廃棄、消去ができていない。	832	814	
			44	・借用期間中の厳正な保管管理ができていない。	722	822	823
想定脅威			想定脆弱性				
内容			NO	内容	関連管理策		
人的脅威内部（許可者）	マシン室（セキュリティエリア）	許可されていないエリアに入ってきてしまう。	45	・物理的なセキュリティ境界を明確にできていない。（受付、表示、扉、など）	911	1111	
			46	・物理的な入退室管理ができていない。（アクセス制御、外来者台帳、など）	912	1112	
			47	・一時許可者であることが名札などで識別できていない。（ので、統制できない	912	1112	
			48	・入室記録、外来者の記録がとられていない。（後からわかる仕組みがない）	912	1112	
			49	・非許可者の一時許可、の受付ルールがない。	912	1112	
			50	・受け渡しエリアなど、許可しているエリアがない。	916	1116	
			51	・打合せ場所、等がセキュリティ境界の内側にあり、入れざるを得ない。	913	1113	
			52	・許可された場所まで導くパーティションの区切りや立ち会う等のルールがない	915	1115	
			53	・夜間、休日の入室ルールがない。	912	1112	
			54	・セキュリティに関するルールの説明ができていない。	822	722	
			55	・マシン室にはマシン室と表示しない、ができていない。	913	1113	
	紙文書 キングファイル	許可されていない情報にアクセスされてしまう。	8	・クリアデスクができていない。（重要な書類がおきっぱなし）	1133	1129	
			9	・クリアスクリーンができていない。（表向きに置きっぱなし、消し忘れ、等）	1133	1129	
			10	・重要な書類が鍵のかかったキャビネットに保管されていない。	722	822	
			11	・鍵が管理されていない。	722	822	
			12	・（脆弱性がわかる）システム文書（社内ネットワーク図等）が適切に保管され	1074		
		う、持ち出されてしまう。	13	・書類、文書が適切に保管されていない。	722	822	
			14	・壊されたこと、無くなったことがわからない。	711	811	
			15	・捨てたはずの文書を持出された（キチンと破棄できなかった）	722	822	
			29	・持ち出して良い情報と持ち出していけない情報が区別できていない。	722	822	
			17	・重要度の分類の指針がない。	721	821	
			18	・持ち出されたことがわからない。	711	811	
			19	・情報資産のオーナが明確になっていない。	712	812	
			29	・持出し管理ルール／承認ルールが不十分。説明されていない。	713	813	
			56	・誓約書の提出がなされていない。	813	712	
			57	・ISMSルールの教育・説明がなされていない。	822	722	
			58	・退職時に情報・資産の返却ができていない。	832	814	
			59	・退職後のID、アクセス権等の無効処理ができていない。	833	926	
			60	・懲戒に関するルールがない。	823	723	
	紙文書（搬送・輸送）	輸送中に紛失してしまう	20	・輸送物の重要度に応じた輸送業者を適切に選定していない。選定ルールが	1083	833	
			21	・文書の輸送に関するルールがない。	722	822	
	廃棄	廃棄したものから情報が漏れる	35	・重要度に応じた廃棄ルールがない。わからない。	722	822	
	広げたファイル、印刷	印刷物をのぞき見されてしまう	9	・クリアスクリーンができていない。（表向きに置きっぱなし、消し忘れ、等）	1133	1129	
			23	・外部の人が通る通路、動線に対して目隠しなどの配慮がされていない。	1133	1129	
			24	・コピー・FAXにおきっぱなしである。	1133	1129	
			8	・クリアデスクができていない。（重要な書類がおきっぱなし）	1133	1129	
	引越し 移動	引越し時にものが無くなる 情報が壊れる	38	・引越し業者を適切に選定できていない。	1082	1322	
			39	・機密保持契約が取り交わされていない。	623	1512	
			40	・搬出数と搬入数の荷物チェックを行なっていない。	1083	833	
	顧客支給品	顧客の要求どおりに取扱いができない	41	・借用時に使用条件、管理ルールが明確になっていない。	1081	1321	
			42	・授受記録がない。	1082	1322	
			43	・使用期限満了時に速やかに返却、廃棄、消去ができていない。	832	814	
			44	・借用期間中の厳正な保管管理ができていない。	722	822	823
想定脅威			想定脆弱性				
内容			NO	内容	関連管理策		
自然災害	紙文書	地震	61	・災害が発生したときの復旧対策・体制が確立されていない	1411	1711	
		火災	62	・火災警報装置が設置されていない	914	1114	
			63	・消火設備が設置されていない	914	1114	

			61	・災害が発生したときの復旧対策・体制が確立されていない	1411	1711	
		落雷	61	・災害が発生したときの復旧対策・体制が確立されていない	1411	1711	

想定脅威			想定脆弱性				
内容			NO	内容	A2005	A2013	
人的脅威外部（非許可者）	事務所	許可無くエリアに入ってきてしまう	1	・物理的なセキュリティ境界を明確にできていない。（受付、表示、扉、など）	911	1111	
			2	・物理的な入退室管理ができていない。（アクセス制御、外来者台帳、など）	912	1112	
			3	・部外者であることが名札などで識別できていない。（ので、統制できない）	912	1112	
			4	・外来者の受付手順がない。外来者の入室記録がとられていない。	912	1112	
			5	・受け渡しエリアなど、許可しているエリアがない。	916	1116	
			6	・打合せ場所、等がセキュリティ境界の内側にあり、入れざるを得ない。	913	1113	
			7	・許可された場所まで導くパーティションの区切りや立ち会う等のルールが	915	1115	
	装置	許可無く装置をこわされてしまう	8	・装置が適切に保護されていない。（PCが通路側に立てて置いてあった、等	921	1121	
			9	・壊されたこと、無くなったことがわからない。	711	811	
			10	・情報資産のオーナが明確になっていない。	712	812	
			11	・ケーブルに足をひっかけて、装置が落下してしまいそうである。	923	1123	
		許可無く装置を持ち出されてしまう	12	・捨てたはずの情報を持ちだされてしまう。（廃棄がキチンとできていなかっ	1072	832	
			13	・機器の盗難防止がされていない。	921	1121	
			14	・持ち出されたことがわからない。	711	811	
			15	・情報資産のオーナが明確になっていない。	712	812	
	装置（搬送・輸送）	輸送中に装置を紛失してしまう	16	・輸送物の重要度に応じた輸送業者を適切に選定していない。選定ルール	1083	833	
			17	・媒体・情報の輸送時の取扱いに関するルールがない。	722	822	
			18	・輸送物の重要度に応じた保護策がとられていない。	1083	833	
	装置	修理ミスが発生してしまう	19	・修理内容に応じた業者を適切に選定していない。選定ルールがない。	924	1124	
			20	・外部の人の作業の立会い、監視がおこなわれていない。	915	1115	
想定脅威			想定脆弱性				
内容			NO	内容	関連管理策		
人的脅威外部委託（許可者）	事務所	許可無くエリアに入ってきてしまう。 許可されていないエリアに入ってきてしまう。	1	・物理的なセキュリティ境界を明確にできていない。（受付、表示、扉、など）	911	1111	
			2	・物理的な入退室管理ができていない。（アクセス制御、外来者台帳、など）	912	1112	
			3	・外部委託者であることが名札などで識別できていない。（ので、統制できな	912	1112	
			21	・入室記録、外来者の記録がとられていない。（後からわかる仕組みがない	912	1112	
			22	・非許可者の一時許可、の受付ルールがない。	912	1112	
			5	・受け渡しエリアなど、許可しているエリアがない。	916	1116	
			6	・打合せ場所、等がセキュリティ境界の内側にあり、入れざるを得ない。	913	1113	
			7	・許可された場所まで導くパーティションの区切りや立ち会う等のルールが	915	1115	
			23	・夜間、休日の入室ルールがない。	912	1112	
			24	・セキュリティに関するルールの説明ができていない。	822	722	
	装置	許可なく装置をこわしてしまう。	8	・装置が適切に保護されていない。（PCが通路側に立てて置いてあった、等	921	1121	
			9	・壊されたこと、無くなったことがわからない。	711	811	
			10	・情報資産のオーナが明確になっていない。	712	812	
			11	・ケーブルに足をひっかけて、装置が落下してしまいそうである。	923	1123	
		許可無く装置を持ち出されてしまう。	12	・捨てたはずの情報を持ちだされてしまう。（廃棄がキチンとできていなかっ	1072	832	
			13	・機器の盗難防止がされていない。	921	1121	
			14	・持ち出されたことがわからない。	711	811	
			15	・情報資産のオーナが明確になっていない。	712	812	
			25	・持出し管理ルール／承認ルールが不十分。説明されていない。	927、713		
			26	・機密保持契約の締結がなされていない。	623	1512	
			27	・委託完了後のルールの説明がなされていない。	822	722	
			28	・委託完了後に情報・資産の返却ができていない。	832	814	
	装置（搬送・輸送）	輸送中に装置を紛失してしまう	16	・輸送物の重要度に応じた輸送業者を適切に選定していない。選定ルール	1083	833	
			17	・媒体・情報の輸送時の取扱いに関するルールがない。	722	822	
			18	・輸送物の重要度に応じた保護策がとられていない。	1083	833	
			29	・モバイルPCに関する管理策がとられていない。	1171	621	
			30	・携帯電話に関する管理策がとられていない（パスワード、ストラップ、等）	1073	833	
	装置	修理ミスが発生してしまう	19	・修理内容に応じた業者を適切に選定していない。選定ルールがない。	924	1124	
			20	・外部の人の作業の立会い、監視がおこなわれていない。	915	1115	
	廃棄	廃棄したものから情報が漏れる	31	・重要度に応じた装置の廃棄ルールがない。わからない。	926	1127	
			32	・廃棄業者に対して、セキュリティ要求事項を明確にしていない。	1082	1322	
			33	・廃棄業者に対して、機密保持契約がなされていない。	623	1512	

	引越し 移動	引越し時にものが無くなる	34	・引越し業者を適切に選定できていない。	1082	1322	
			35	・機密保持契約が取り交わされていない。	623	1512	
			36	・搬出数と搬入数の荷物チェックを行なっていない。	1083	833	
	顧客支給品	顧客の要求どおりに取扱いができない	37	・借用時に使用条件、管理ルールが明確になっていない。	1081	1321	
			38	・授受記録がない。	1082	1322	
			39	・使用期限満了時に速やかに返却、廃棄ができていない。	832	814	
			40	・借用期間中の厳正な保管管理ができていない。	722	822	823
想定脅威			想定脆弱性				
内容			NO	内容	関連管理策		
人的脅威内部（許可者）	マシン室（セキュリティエリア）	許可されていないエリアに入ってきてしまう	41	・物理的なセキュリティ境界を明確にできていない。（受付、表示、扉、など）	911	1111	
			42	・物理的な入退室管理ができていない。（アクセス制御、外来者台帳、など）	912	1112	
			43	・一時許可者であることが名札などで識別できていない。（ので、統制できな	912	1112	
			44	・入室記録、外来者の記録がとられていない。（後からわかる仕組みがない	912	1112	
			45	・非許可者の一時許可、の受付ルールがない。	912	1112	
			46	・受け渡しエリアなど、許可しているエリアがない。	916	1116	
			47	・打合せ場所、等がセキュリティ境界の内側にあり、入れざるを得ない。	913	1113	
			48	・許可された場所まで導くパーティションの区切りや立ち会う等のルールが	915	1115	
			49	・夜間、休日の入室ルールがない。	912	1112	
			50	・セキュリティに関するルールの説明ができていない。	822	722	
			51	・マシン室にはマシン室と表示しない、ができていない。	913	1113	
	装置	許可なく装置をこわしてしまう	8	・装置が適切に保護されていない。（PCが通路側に立てて置いてあった、等	921	1121	
			9	・壊されたこと、無くなったことがわからない。	711	811	
			10	・情報資産のオーナが明確になっていない。	712	812	
			11	・ケーブルに足をひっかけて、装置が落下してしまいそうである。	923	1123	
		許可無く装置を持ち出されてしまう	13	・機器の盗難防止がされていない。	921	1121	
			14	・持ち出されたことがわからない。	711	811	
			15	・情報資産のオーナが明確になっていない。	712	812	
			25	・持出し管理ルール／承認ルールが不十分。説明されていない。	927	1125	
			52	・誓約書の提出がなされていない。	813	712	
			53	・ISMSルールの教育・説明がなされていない。	822	722	
			54	・退職時に情報・資産の返却ができていない。	832	814	
			55	・懲戒に関するルールがない。	823	723	
	装置（搬送・輸送）	装置を誤って紛失してしまう	16	・輸送物の重要度に応じた輸送業者を適切に選定していない。選定ルール	1083	833	
			17	・媒体・情報の輸送時の取扱いに関するルールがない。	722	822	
			29	・モバイルPCに関する管理策がとられていない。	1171	621	
			30	・携帯電話に関する管理策がとられていない（パスワード、ストラップ、等）	1073	833	
			18	・輸送物の重要度に応じた保護策がとられていない。	1083	833	
	装置	修理ミスが発生してしまう	19	・修理内容に応じた業者を適切に選定していない。選定ルールがない。	924	1124	
	廃棄	廃棄すべき装置から情報が漏れる	31	・重要度に応じた装置の廃棄ルールがない。わからない。	926	1127	
	引越し 移動	引越し時にものが無くなる	34	・引越し業者を適切に選定できていない。	1082	1322	
			35	・機密保持契約、誓約書等が取り交わされていない。	623	1512	
			36	・搬出数と搬入数の荷物チェックを行なっていない。	1083	833	
	顧客支給品	顧客の要求どおりに取扱いができない	37	・借用時に使用条件、管理ルールが明確になっていない。	1081	1321	
			38	・授受記録がない。	1082	1322	
			39	・使用期限満了時に速やかに返却、廃棄、消去ができていない。	832	814	
			40	・借用期間中の厳正な保管管理ができていない。	722	822	823
想定脅威			想定脆弱性				
内容			NO	内容	関連管理策		
システム	装置	ハードウェアが故障してしまった。 動作が不安定となってしまった。	56	・供給者が推奨する間隔、仕様での保守が行なわれていない。	924	1124	
			57	・重要なサーバの物理的なセキュリティが確保できていない（マシン室、ラッ	921	1121	
			58	・通信ケーブルが整理整頓、保護されていない	923	1123	
			59	・敷地外に置かれている装置に何も保護が行われいていない	925	1126	
			60	・アウトソーシング先へのセキュリティ要求事項が明確に示せていない。	1021	1521	
			61	・空調、電源,等の環境を考慮できていない。	922	1122	
			62	・情報システム導入時、受入試験を行っていない	1032	1429	
			63	・障害時のログが取得できていない。	10105	1241	
			64	・復旧手順（操作手順）が定められていない。	1011	1211	
			13	・機器の盗難防止策が無い	921	1121	
自然災害	装置	地震	65	・転倒防止策が無い	914	1114	

			66	・災害が発生したときの復旧対策・体制が確立されていない	1411	1711	
		火災	67 68 66	・火災警報装置が設置されていない ・消火設備が設置されていない ・災害が発生したときの復旧対策・体制が確立されていない	914 914 1411	1114 1114 1711	
		落雷	66	・災害が発生したときの復旧対策・体制が確立されていない	1411	1711	

想定脅威			想定脆弱性				
内容			NO	内容	A2005	A2013	
人的脅威外部（非許可者）	事務所	許可無くエリアに入ってきてしまう	1	・物理的なセキュリティ境界を明確にできていない。（受付、表示、扉、など）	911	1111	
			2	・物理的な入退室管理ができていない。（アクセス制御、外来者台帳、など）	912	1112	
			3	・部外者であることが名札などで識別できていない。（ので、統制できない）	912	1112	
			4	・外来者の受付手順がない。外来者の入室記録がとられていない。	912	1112	
			5	・受け渡しエリアなど、許可しているエリアがない。	916	1116	
			6	・打合せ場所、等がセキュリティ境界の内側にあり、入れざるを得ない。	913	1113	
			7	・許可された場所まで導くパーティションの区切りや立ち会う等のルールが	915	1115	
	記憶媒体	許可無く情報を持ち出されてしまう	8	・捨てたはずの情報を持ちだされてしまう。（廃棄がキチンとできていなかっ	1072	832	
			9	・インストール媒体（メディア）が適切に保管されていない。	1071	831	
			10	・許可されていないスパイウェアが起動させられてしまう。	1041	1221	
			11	・ウィルスワクチンソフトが導入されていない。	1041	1221	
			12	・システム的な脆弱性を防御できていない。（適切なパッチが当っていない）	1254		
			13	・持ち出されたことがわからない。	711	811	
			14	・情報資産のオーナが明確になっていない。	712	812	
			15	・ライセンス管理ができていない。	1512	1812	
	記憶媒体（搬送・輸送）	輸送中に情報を紛失してしまう	16	・輸送物の重要度に応じた輸送業者を適切に選定していない。選定ルール	1083	833	
			17	・媒体・情報の輸送時の取扱いに関するルールがない。	722	822	
			18	・輸送物の重要度に応じた保護策がとられていない。	1083	833	

想定脅威			想定脆弱性				
内容			NO	内容	関連管理策		
人的脅威外部委託（許可者）	事務所	許可無くエリアに入ってきてしまう。 許可されていないエリアに入ってきてしまう	1	・物理的なセキュリティ境界を明確にできていない。（受付、表示、扉、など）	911	1111	
			2	・物理的な入退室管理ができていない。（アクセス制御、外来者台帳、など）	912	1112	
			3	・外部委託者であることが名札などで識別できていない。（ので、統制できな	912	1112	
			19	・入室記録、外来者の記録がとられていない。（後からわかる仕組みがない	912	1112	
			20	・非許可者の一時許可、の受付ルールがない。	912	1112	
			5	・受け渡しエリアなど、許可しているエリアがない。	916	1116	
			6	・打合せ場所、等がセキュリティ境界の内側にあり、入れざるを得ない。	913	1113	
			7	・許可された場所まで導くパーティションの区切りや立ち会う等のルールが	915	1115	
			21	・夜間、休日の入室ルールがない。	912	1112	
			22	・セキュリティに関するルールの説明ができていない。	822	722	
	記憶媒体	許可無く情報を持ち出されてしまう	8	・捨てたはずの情報を持ちだされてしまう。（廃棄がキチンとできていなかっ	1072	832	
			9	・インストール媒体（メディア）が適切に保管されていない。	1071	831	
			10	・許可されていないスパイウェアが起動させられてしまう。	1041	1221	
			11	・ウィルスワクチンソフトが導入されていない。	1041	1221	
			12	・システム的な脆弱性を防御できていない。（適切なパッチが当っていない）	1254		
			13	・持ち出されたことがわからない。	711	811	
			14	・情報資産のオーナが明確になっていない。	712	812	
			15	・ライセンス管理ができていない。	1512	1812	
			23	・持出し管理ルール／承認ルールが不十分。説明されていない。	927	1125	813
			24	・メディア（CD-R/DVD-R,等）に焼かれて持出されてしまう。	1071	831	
			25	・機密保持契約の締結がなされていない。	623	1512	
			26	・委託完了後のルールの説明がなされていない。	822	722	
			27	・委託完了後に情報・資産の返却ができていない。	832	814	
			28	・委託完了後のID、アクセス権等の無効処理ができていない。	833	926	
	記憶媒体（搬送・輸送）	輸送中に情報を紛失してしまう	16	・輸送物の重要度に応じた輸送業者を適切に選定していない。選定ルール	1083	833	
			17	・媒体・情報の輸送時の取扱いに関するルールがない。	722	822	
			18	・輸送物の重要度に応じた保護策がとられていない。	1083	833	
	廃棄	廃棄したものから情報が漏れる	29	・重要度に応じた媒体の廃棄ルールがない。わからない。	1072	832	
			30	・廃棄業者に対して、セキュリティ要求事項を明確にしていない。	1082	1322	
			31	・廃棄業者に対して、機密保持契約がなされていない。	623	1512	
	引越し移動	引越し時にものが無くなる	32	・引越し業者を適切に選定できていない。	1082	1322	
			33	・機密保持契約が取り交わされていない。	623	1512	
			34	・搬出数と搬入数の荷物チェックを行なっていない。	1083	833	
	顧客支給品	顧客の要求どおりに取扱いができない	35	・借用時に使用条件、管理ルールが明確になっていない。	1081	1321	
			36	・授受記録がない。	1082	1322	
			37	・使用期限満了時に速やかに返却、廃棄、消去ができていない。	832	814	

			38	・借用期間中の厳正な保管管理ができていない。	722	822	823
			39	・ライセンス管理ができていない。	1512	1812	
想定脅威			想定脆弱性				
内容			NO	内容	関連管理策		
人的脅威内部（許可者）	マシン室（セキュリティエリア）	許可されていないエリアに入ってきてしまう	40	・物理的なセキュリティ境界を明確にできていない。（受付、表示、扉、など）	911	1111	
			41	・物理的な入退室管理ができていない。（アクセス制御、外来者台帳、など）	912	1112	
			42	・一時許可者であることが名札などで識別できていない。（ので、統制できな	912	1112	
			43	・入室記録、外来者の記録がとられていない。（後からわかる仕組みがない	912	1112	
			44	・非許可者の一時許可、の受付ルールがない。	912	1112	
			45	・受け渡しエリアなど、許可しているエリアがない。	916	1116	
			46	・打合せ場所、等がセキュリティ境界の内側にあり、入れざるを得ない。	913	1113	
			47	・許可された場所まで導くパーティションの区切りや立ち会う等のルールが	915	1115	
			48	・夜間、休日の入室ルールがない。	912	1112	
			49	・セキュリティに関するルールの説明ができていない。	822	722	
			50	・マシン室にはマシン室と表示しない、ができていない。	913	1113	
	記憶媒体	許可無く情報を持ち出されてしまう	9	・インストール媒体（メディア）が適切に保管されていない。	1071	831	
			10	・許可されていないスパイウェアが起動させられてしまう。	1041	1221	
			11	・ウィルスワクチンソフトが導入されていない。	1041	1221	
			12	・システム的な脆弱性を防御できていない。（適切なパッチが当っていない）	1254		
			13	・持ち出されたことがわからない。	711	811	
			14	・情報資産のオーナが明確になっていない。	712	812	
			15	・ライセンス管理ができていない。	1512	1812	
			23	・持出し管理ルール／承認ルールが不十分。説明されていない。	927	1125	813
			24	・メディア（CD-R/DVD-R,等）に焼かれて持出されてしまう。	1071	831	
			51	・誓約書の提出がなされていない。	813	712	
			52	・ISMSルールの教育・説明がなされていない。	822	722	
			53	・退職時に情報・資産の返却ができていない。	832	814	
			54	・退職後のID、アクセス権等の無効処理ができていない。	833	926	
			55	・懲戒に関するルールがない。	823	723	
	記憶媒体（搬送・輸送）	情報を誤って紛失してしまう	16	・輸送物の重要度に応じた輸送業者を適切に選定していない。選定ルール	1083	833	
			17	・媒体・情報の輸送時の取扱いに関するルールがない。	722	822	
			18	・輸送物の重要度に応じた保護策がとられていない。	1083	833	
	廃棄	廃棄すべき情報から情報が漏れる	29	・重要度に応じた媒体の廃棄ルールがない。わからない。	1072	832	
	引越し移動	引越し時にものが無くなる	32	・引越し業者を適切に選定できていない。	1082	1322	
			33	・機密保持契約、誓約書等が取り交わされていない。	623	1512	
			34	・搬出数と搬入数の荷物チェックを行なっていない。	1083	833	
	顧客支給品	顧客の要求どおりに取扱いができない	35	・借用時に使用条件、管理ルールが明確になっていない。	1081	1321	
			36	・授受記録がない。	1082	1322	
			37	・使用期限満了時に速やかに返却、廃棄、消去ができていない。	832	814	
			38	・借用期間中の厳正な保管管理ができていない。	722	822	823
			39	・ライセンス管理ができていない。	1512	1812	
想定脅威			想定脆弱性				
内容			NO	内容	関連管理策		
システム	ソフトウェア	ソフトウェアに障害が起こってしまった。 動作が不安定となってしまった。	56	・操作手順が無い	1011	1211	
			57	・変更発生時の手順が無い	1012	1212	
			58	・最新のパターンファイルに更新されていない	1041	1221	
			11	・ウイルスワクチンソフトがインストールされていない	1041	1221	
			60	・情報システム導入時、受入試験を行っていない	1032	1429	
			61	・許可無くソフトウエアをインストールことができる（ライセンス管理ができて	1512	1812	
			12	・システム的な脆弱性を防御できていない。（適切なパッチが当っていない）	1254		
			63	・障害時のログが取得できていない。	10105	1241	
		ウィルス、スパイウェアに感染してしまった。	64	・事故発生時の報告手順が決まっていない	1311	1612	
			65	・事故発生後の是正処置が行われていない、監視できるしくみがない	1322	1616	
			66	・ヒヤリハットの報告手順がきまっていない	1312	1613	
			61	・許可無くフリーウェアをインストールことができる	1254		1262
			58	・最新のパターンファイルに更新されていない	1041	1221	
			69	・脆弱性の管理体制がない。	1261	1261	
			70	・復旧対策、体制が確立されていない。	1321	1611	
			11	・ウイルスワクチンソフトがインストールされていない	1041	1221	
			12	・システム的な脆弱性を防御できていない。（適切なパッチが当っていない）	1254		
			63	・障害時のログが取得できていない。	10105	1241	
自然災害	記憶媒体（保存）	地震	71	・災害が発生したときの復旧対策・体制が確立されていない	1411	1711	
		火災	72	・火災警報装置が設置されていない	914	1114	
			73	・消火設備が設置されていない	914	1114	

			71	・災害が発生したときの復旧対策・体制が確立されていない	1411	1711	
		落雷	71	・災害が発生したときの復旧対策・体制が確立されていない	1411	1711	

想定脅威			想定脆弱性				
内容			NO	内容	A2005	A2013	
人的脅威外部委託(許可者)	サービス	サービスが停止してしまう。	1	・サービス業者を適切に選定していない。	623	1512	
			2	・アウトソーシング先とのサービスに関する合意がとれていない。	1021	1521	
			3	・アウトソーシング先へのセキュリティ要求事項が明確に示せていない。	1021	1521	
			4	・アウトソーシング先からサービスの報告を受けていない。	1022	1521	
			5	・アウトソーシング先のサービス提供の変更を管理できていない。	1023	1522	
			6	・情報資産のオーナが明確になっていない。	712	812	
			7	・機密保持契約の締結がなされていない。	623	1512	
			8	・委託完了後のルールの説明がなされていない。	822	722	
			9	・委託完了後に情報・資産の返却ができていない。	832	814	
			10	・事故発生時の報告を受ける手順が決まっていない	1022	1521	
自然災害	サービス	地震	1	・サービス業者を適切に選定していない。	623	1512	
			10	・アウトソーシング先へのセキュリティ要求事項が明確に示せていない。	1021	1521	
			11	・災害が発生したときの復旧対策・体制が確立されていない	1021	1521	
		火災	1	・サービス業者を適切に選定していない。	623	1512	
			3	・アウトソーシング先へのセキュリティ要求事項が明確に示せていない。	1021	1521	
			11	・災害が発生したときの復旧対策・体制が確立されていない	1021	1521	
		落雷	1	・サービス業者を適切に選定していない。	623	1512	
			3	・アウトソーシング先へのセキュリティ要求事項が明確に示せていない。	1021	1521	
			11	・災害が発生したときの復旧対策・体制が確立されていない	1021	1521	

項番	ISO/IEC 27001:2005	項番	ISO/IEC 27001:2013
5	5 セキュリティ基本方針		
51	5.1 情報セキュリティ基本方針	51	5.1 情報セキュリティのための経営陣の方向性
511	5.1.1 情報セキュリティ基本方針文書	511	5.1.1 情報セキュリティのための方針群
512	5.1.2 情報セキュリティ基本方針のレビュー	512	5.1.2 情報セキュリティのための方針群のレ
6	6 情報セキュリティのための組織		
61	6.1 内部組織		
611	6.1.1 情報セキュリティに対する経営陣の責任	721	7.2.1 経営陣の責任
612	6.1.2 情報セキュリティの調整		削除
613	6.1.3 情報セキュリティ責任の割当て	611	6.1.1 情報セキュリティの役割及び責任
614	6.1.4 情報処理設備の認可プロセス		削除
615	6.1.5 秘密保持契約	1324	13.2.4 秘密保持契約又は守秘義務契約
616	6.1.6 関係当局との連絡	613	6.1.3 関係当局との連絡
617	6.1.7 専門組織との連絡	614	6.1.4 専門組織との連絡
618	6.1.8 情報セキュリティの独立したレビュー	1821	18.2.1 情報セキュリティの独立したレビュー
62	6.2 外部組織		
621	6.2.1 外部組織に関係したリスクの識別		削除
622	6.2.2 顧客対応におけるセキュリティ		削除
623	6.2.3 第三者との契約におけるセキュリティ	1512	15.1.2 供給者との合意におけるセキュリティの取扱い
7	7 資産の管理		
71	7.1 資産に対する責任		
711	7.1.1 資産目録	811	8.1.1 資産目録
712	7.1.2 資産の管理責任者	812	8.1.2 資産の管理責任
713	7.1.3 資産利用の許容範囲	813	8.1.3 資産利用の許容範囲
72	7.2 情報の分類		
721	7.2.1 分類の指針	821	8.2.1 情報の分類
722	7.2.2 情報のラベル付け及び取扱い	822	8.2.2 情報のラベル付け 8.2.3 資産の取扱い
8	8 人的資源のセキュリティ		
81	8.1 雇用前		
811	8.1.1 役割及び責任	611	6.1.1 情報セキュリティの役割及び責任
812	8.1.2 選考	711	7.1.1 選考
813	8.1.3 雇用条件	712	7.1.2 雇用条件
82	8.2 雇用期間中		
821	8.2.1 経営陣の責任	721	7.2.1 経営陣の責任
822	8.2.2 情報セキュリティの意識向上、教育及び訓練	722	7.2.2 情報セキュリティの意識向上、教育及び訓練
823	8.2.3 懲戒手続	723	7.2.3 懲戒手続
83	8.3 雇用の終了又は変更		
831	8.3.1 雇用の終了又は変更に関する責任	731	7.3.1 雇用の終了又は変更に関する責任
832	8.3.2 資産の返却	814	8.1.4 資産の返却
833	8.3.3 アクセス権の削除	926	9.2.6 アクセス権の削除又は修正
9	9 物理的及び環境的セキュリティ		
91	9.1 セキュリティを保つべき領域		
911	9.1.1 物理的セキュリティ境界	1111	11.1.1 物理的セキュリティ境界
912	9.1.2 物理的入退管理策	1112	11.1.2 物理的入退管理策
913	9.1.3 オフィス、部屋及び施設のセキュリティ	1113	11.1.3 オフィス、部屋及び施設のセキュリティ
914	9.1.4 外部及び環境の脅威からの保護	1114	11.1.4 外部及び環境の脅威からの保護
915	9.1.5 セキュリティを保つべき領域での作業	1115	11.1.5 セキュリティを保つべき領域での作業
916	9.1.6 一般の人の立寄り場所及び受渡場所	1116	11.1.6 受渡場所
92	9.2 装置のセキュリティ		
921	9.2.1 装置の設置及び保護	1121	11.2.1 装置の設置及び保護
922	9.2.2 サポートユーティリティ	1122	11.2.2 サポートユーティリティ
923	9.2.3 ケーブル配線のセキュリティ	1123	11.2.3 ケーブル配線のセキュリティ
924	9.2.4 装置の保守	1124	11.2.4 装置の保守
925	9.2.5 構外にある装置のセキュリティ	1126	11.2.6 構外にある装置及び資産のセキュリティ
926	9.2.6 装置の安全な処分又は再利用	1127	11.2.7 装置のセキュリティを保った処分又は再利用

927	9.2.7 資産の移動	1125	11.2.5 資産の移動
10	10 通信及び運用管理		
101	10.1 運用の手順及び責任		
1011	10.1.1 操作手順書	1211	12.1.1 操作手順書
1012	10.1.2 変更管理	1212	12.1.2 変更管理
1013	10.1.3 職務の分割	612	6.1.2 職務の分離
1014	10.1.4 開発施設、試験施設及び運用施設の分	1214	12.1.4 開発環境、試験環境及び運用環境の分
102	10.2 第三者が提供するサービスの管理		
1021	10.2.1 第三者が提供するサービス	1521	15.2.1 供給者のサービス提供の監視及びレビュー
1022	10.2.2 第三者が提供するサービスの監視及びレビュー	1521	15.2.1 供給者のサービス提供の監視及びレビュー
1023	10.2.3 第三者が提供するサービスの変更に対する管理	1522	15.2.2 供給者のサービス提供の変更に対する管理
103	10.3 システムの計画作成及び受入れ		
1031	10.3.1 容量・能力の管理	1213	12.1.3 容量・能力の管理
1032	10.3.2 システムの受入れ	1429	14.2.9 システムの受入れ試験
104	10.4 悪意のあるコード及びモバイルコードからの保護		
1041	10.4.1 悪意のあるコードに対する管理策	1221	12.2.1 マルウェアに対する管理策
1042	10.4.2 モバイルコードに対する管理策		削除
105	10.5 バックアップ		
1051	10.5.1 情報のバックアップ	1231	12.3.1 情報のバックアップ
106	10.6 ネットワークセキュリティ管理		
1061	10.6.1 ネットワーク管理策	1311	13.1.1 ネットワーク管理策
1062	10.6.2 ネットワークサービスのセキュリティ	1312	13.1.2 ネットワークサービスのセキュリティ
107	10.7 媒体の取扱い		
1071	10.7.1 取外し可能な媒体の管理	831	8.3.1 取外し可能な媒体の管理
1072	10.7.2 媒体の処分	832	8.3.2 媒体の処分
1073	10.7.3 情報の取扱手順	833	8.2.3 資産の取扱い
1074	10.7.4 システム文書のセキュリティ		
108	10.8 情報の交換		
1081	10.8.1 情報交換の方針及び手順	1321	13.2.1 情報転送の方針及び手順
1082	10.8.2 情報交換に関する合意	1322	13.2.2 情報転送に関する合意
1083	10.8.3 配送中の物理的媒体	833	8.3.3 物理的媒体の輸送
1084	10.8.4 電子的メッセージ送信	1323	13.2.3 電子的メッセージ通信
1085	10.8.5 業務用情報システム		削除
109	10.9 電子商取引サービス		
1091	10.9.1 電子商取引	1412	14.1.2 公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮
1092	10.9.2 オンライン取引	1413	14.1.3 アプリケーションサービスのトランザクションの保護
1093	10.9.3 公開情報		削除
1010	10.10 監視		
1010	10.10.1 監視ログ取得	1241	12.4.1 イベントログ取得
1010	10.10.2 システムの使用状況の監視		削除
1010	10.10.3 ログ情報の保護	1242	12.4.2 ログ情報の保護
1010	10.10.4 実務管理者及び運用担当者の作業ロ	1243	12.4.3 実務管理者及び運用担当者の作業ログ
1010	10.10.5 障害のログ取得	1241	12.4.1 イベントログ取得
1010	10.10.6 クロックの同期	1244	12.4.4 クロックの同期
11	11 アクセス制御		
111	11.1 アクセス制御に対する業務上の要求事項		
1111	11.1.1 アクセス制御方針	911	9.1.1 アクセス制御方針
112	11.2 利用者アクセスの管理	9	
1121	11.2.1 利用者登録	921	9.2.1 利用者登録及び登録削除 9.2.2 利用者アクセスの提供(provisioning)
1122	11.2.2 特権管理	923	9.2.3 特権的アクセス権の管理
1123	11.2.3 利用者パスワードの管理	924	9.2.4 利用者の秘密認証情報の管理
1124	11.2.4 利用者アクセス権のレビュー	925	9.2.5 利用者アクセス権のレビュー

113	11.3 利用者の責任		
1131	11.3.1 パスワードの利用	931	9.3.1 秘密認証情報の利用
1132	11.3.2 無人状態にある利用者装置	1128	11.2.8 無人状態にある利用者装置
1133	11.3.3 クリアデスク・クリアスクリーン方針	1129	11.2.9 クリアデスク・クリアスクリーン方針
114	11.4 ネットワークのアクセス制御		
1141	11.4.1 ネットワークサービスの利用についての方針	912	9.1.2 ネットワーク及びネットワークサービスへのアクセス
1142	11.4.2 外部から接続する利用者の認証		削除
1143	11.4.3 ネットワークにおける装置の識別	1311	13.1.1 ネットワーク管理策
1144	11.4.4 遠隔診断用及び環境設定用ポートの保		削除
1145	11.4.5 ネットワークの領域分割	1313	13.1.3 ネットワークの分離
1146	11.4.6 ネットワークの接続制御		削除
1147	11.4.7 ネットワークルーティング制御		削除
115	11.5 オペレーティングシステムのアクセス制御		
1151	11.5.1 セキュリティに配慮したログオン手順	942	9.4.2 セキュリティに配慮したログオン手順
1152	11.5.2 利用者の識別及び認証	921	9.2.1 利用者登録及び登録削除 9.2.2 利用者アクセスの提供（provisioning）
1153	11.5.3 パスワード管理システム	943	9.4.3 パスワード管理システム
1154	11.5.4 システムユーティリティの利用	944	9.4.4 特権的なユーティリティプログラムの使用
1155	11.5.5 セッションのタイムアウト	942	9.4.2 セキュリティに配慮したログオン手順
1156	11.5.6 接続時間の制限	942	9.4.2 セキュリティに配慮したログオン手順
116	11.6 業務用ソフトウェア及び情報のアクセス制		
1161	11.6.1 情報へのアクセス制限	941	9.4.1 情報へのアクセス制限
1162	11.6.2 取扱いに慎重を要するシステムの隔離	941	9.4.1 情報へのアクセス制限
117	11.7 モバイルコンピューティング及びテレワーキング		
1171	11.7.1 モバイルのコンピューティング及び通信	621	6.2.1 モバイル機器の方針
1172	11.7.2 テレワーキング	622	6.2.2 テレワーキング
12	12 情報システムの取得、開発及び保守		
121	12.1 情報システムのセキュリティ要求事項		
1211	12.1.1 セキュリティの要求事項の分析及び仕様化	1411	14.1.1 情報セキュリティ要求事項の分析及び仕様化
122	12.2 業務用ソフトウェアでの正確な処理		
1221	12.2.1 入力データの妥当性確認		削除
1222	12.2.2 内部処理の管理		削除
1223	12.2.3 メッセージの完全性		削除
1224	12.2.4 出力データの妥当性確認		削除
123	12.3 暗号による管理策		
1231	12.3.1 暗号による管理策の利用方針	1011	10.1.1 暗号による管理策の利用方針
1232	12.3.2 かぎ（鍵）管理	1012	10.1.2 鍵管理
124	12.4 システムファイルのセキュリティ		
1241	12.4.1 運用ソフトウェアの管理	1251	12.5.1 運用システムに関わるソフトウェアの導入
1242	12.4.2 システム試験データの保護	1431	14.3.1 試験データの保護
1243	12.4.3 プログラムソースコードへのアクセス制	945	9.4.5 プログラムソースコードへのアクセス制御
125	12.5 開発及びサポートプロセスにおけるセキュリティ		
1251	12.5.1 変更管理手順	1422	14.2.2 システムの変更管理手順
1252	12.5.2 オペレーティングシステム変更後の業務用ソフトウェアの技術的レ ビュー	1423	14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的 レビュー
1253	12.5.3 パッケージソフトウェアの変更に対する	1424	14.2.4 パッケージソフトウェアの変更に対する
1254	12.5.4 情報の漏えい		削除
1255	12.5.5 外部委託によるソフトウェア開発	1427	14.2.7 外部委託による開発
126	12.6 技術的ぜい弱性管理		
1261	12.6.1 技術的ぜい弱性の管理	1261	12.6.1 技術的ぜい弱性の管理
13	13 情報セキュリティインシデントの管理		
131	13.1 情報セキュリティの事象及び弱点の報告		
1311	13.1.1 情報セキュリティ事象の報告	1612	16.1.2 情報セキュリティ事象の報告
1312	13.1.2 情報セキュリティ弱点の報告	1613	16.1.3 情報セキュリティ弱点の報告

132	13.2 情報セキュリティインシデントの管理及びその改善	16	
1321	13.2.1 責任及び手順	1611	16.1.1 責任及び手順
1322	13.2.2 情報セキュリティインシデントからの学	1616	16.1.6 情報セキュリティインシデントからの学
1323	13.2.3 証拠の収集	1617	16.1.7 証拠の収集
14	14 事業継続管理		
141	14.1 事業継続管理における情報セキュリティの側面		
1411	14.1.1 事業継続管理手続への情報セキュリティの組込み	1711	17.1.1 情報セキュリティ継続の計画 17.1.2 情報セキュリティ継続の実施
1412	14.1.2 事業継続及びリスクアセスメント	1711	17.1.1 情報セキュリティ継続の計画
1413	14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施	1711	17.1.1 情報セキュリティ継続の計画 17.1.2 情報セキュリティ継続の実施
1414	14.1.4 事業継続計画策定の枠組み		削除
1415	14.1.5 事業継続計画の試験、維持及び再評価	1713	17.1.3 情報セキュリティ継続の検証、レビュー及び評価
15	15 順守		
151	15.1 法的要求事項の順守		
1511	15.1.1 適用法令の識別	1811	18.1.1 適用法令及び契約上の要求事項の特
1512	15.1.2 知的財産権 (IPR)	1812	18.1.2 知的財産権
1513	15.1.3 組織の記録の保護	1813	18.1.3 記録の保護
1514	15.1.4 個人データ及び個人情報の保護	1814	18.1.4 プライバシー及び個人を特定できる情報(PII)の保護
1515	15.1.5 情報処理施設の不正使用防止		削除
1516	15.1.6 暗号化機能に対する規制	1815	18.1.5 暗号化機能に対する規制
152	15.2 セキュリティ方針及び標準の順守、並びに技術的順守		
1521	15.2.1 セキュリティ方針及び標準の順守	1822	18.2.2 情報セキュリティのための方針群及び標準の順守
1522	15.2.2 技術的順守の点検	1823	18.2.3 技術的順守のレビュー
153	15.3 情報システムの監査に対する考慮事項		
1531	15.3.1 情報システムの監査に対する管理策	1271	12.7.1 情報システムの監査に対する管理策
1532	15.3.2 情報システムの監査ツールの保護		削除