大分類No.	大分類	中分類No.	中分類	要求事項No.	★3	★4	要求事項名	要求事項	★3/★4	評価基準No.	評価基準	NIST CSFにおける機能	PassLogic対応
1	ガバナンスの整備	1-1	組織の状況	2001-1-1		○	社内ルール	セキュリティに関する法令等に規定された事項を考慮し、社内ルールを策定及び周知すること。	★4	1-1-1-1	・セキュリティに関連する以下の事項を把握した上で、社内ルールを定めること。 - 自社に関連する法令(事業法、個人情報保護法等) - 所管省庁及び関係団体における基準 - 取引先が提示する制限事項及び要求事項	統治(GV)	
										1-1-1-2	・No.1-1-1-1で定める事項の改定及び変更の状況について、年１回以上の頻度で確認を行い、社内ルールの内容を点検すること。		
										1-1-1-3	・策定・見直した社内ルールを役員、従業員、派遣社員及び受入出向者へと周知すること。		
		1-2	役割、責任、権限	2001-2-1	○	○	セキュリティ推進活動部門	セキュリティ推進活動を担当する部署、役員及び従業員を決定し、責任及び権限を割り当てること。	★3	1-2-1-1	・セキュリティを統括する役員(例えば、CISOを設置する会社の場合は、当該CISO)及びセキュリティ担当部署の役割・責任を定めること。		
										1-2-1-2	・平時のセキュリティ推進活動に必要な役員(例えば、CISOを設置する会社の場合は、当該CISO)及びセキュリティ担当部署の連絡先リストを定めること。		
										1-2-1-3	・年1回以上の頻度でNo.1-2-1-1及びNo.1-2-1-2にて定めた平時の体制について点検すること。		
									★4	1-2-1-4	・セキュリティリスクは、経営に重大な影響を及ぼすことを前提として、その対応について、経営層が参加する情報セキュリティ委員会等の経営判断ができる体制を設置すること。		
				2001-2-2		○	サイバー攻撃の監視・分析体制	サイバー攻撃及び予兆を監視・分析をする体制を整備すること。	★4	1-2-2-1	・サイバー攻撃及び脆弱性に関する公開情報又は非公開情報を活用する体制を整備すること。		
										1-2-2-2	・入手した情報又はログの相関分析等により、サイバー攻撃の予兆及びインシデントの発生の検知を可能とし、インシデントの防止及びインシデントが発生した場合の対応が導き出せる体制を整備すること。		
				2001-2-3	○	○	守秘義務のルール	守秘義務のルールを策定し、遵守させること。	★3	1-2-3-1	・役員、従業員、派遣社員及び受入出向者を対象に、自社の守秘義務のルールを定めること。		
										1-2-3-2	・入社時又は社外要員の受入れ時に守秘義務のルールを説明すること。		
									★4	1-2-3-3	・自社の機密情報を取り扱う役員及び従業員に、守秘義務の誓約書を提出させること。(社外要員を除く。)		
										1-2-3-4	・派遣社員及び受入出向者について、派遣元及び出向元の会社と業務開始前に守秘義務を締結すること。		
		1-3	ポリシー	2001-3-1	○	○	セキュリティ対応方針の策定	自社のセキュリティ対応方針を策定し、周知すること。	★3	1-3-1-1	・自社のセキュリティ対応方針を定めること。		
										1-3-1-2	・定常的に役員、従業員、派遣社員及び受入出向者が最新のセキュリティ対応方針を参照できるようにすること。		
										1-3-1-3	・セキュリティ対応方針の改正時に、当該改正内容を役員、従業員、派遣社員及び受入出向者に周知すること。		
									★4	1-3-1-4	・年１回以上の頻度でセキュリティ対応方針の内容を点検すること。		
		1-4	監督	2001-4-1		○	セキュリティ対策推進計画	セキュリティ対策推進計画を策定し、定期的に経営層へ対策実施状況に関する報告を行うとともに、報告結果を対策の推進に反映すること。	★4	1-4-1-1	・セキュリティ担当部署は、年１回以上、セキュリティを統括する役員(例えば、CISOを設置する会社の場合は、当該CISO)に対して、以下にて求める対策の点検の結果を踏まえたセキュリティ対策の実態及び当該実態を踏まえて策定した今後の対策推進計画を報告し承認を得た上で、当該報告結果を社内部署と共有すること。 [点検を求める対策(評価基準)] No.1-1-1-2、1-2-1-3、1-3-1-4、2-1-1-2、3-1-1-4、3-1-1-7、3-1-2-4、3-1-4-2、3-1-4-4、3-1-4-6、3-1-5-3、3-2-1-5、4-1-7-2、4-1-9-3、4-2-1-5、4-2-2-3、5-1-2-2、6-1-1-4		
										1-4-1-2	・No.1-4-1-1における対策推進計画の報告に際し、役員からの改善に向けた指示があった場合、セキュリティ担当部署は、当該指示内容の記録、計画への反映及び不備の是正を実施すること。		
2	取引先管理	2-1	サイバーセキュリティサプライチェーンリスクマネジメント	2002-1-1	○	○	取引先とのビジネス又はシステム上の関係	取引先と自社とのビジネス又はシステム上の関係を把握すること。	★3	2-1-1-1	・自社以外の組織(顧客・子会社・関係会社・クラウドサービス提供者を含む取引先)が管理・提供し、自社の資産が接続しているシステムを把握するための仕組みを整備すること。		
										2-1-1-2	・年1回以上の頻度でNo.2-1-1-1において把握した情報の内容を点検すること。		
									★4	2-1-1-3	・自社の機密情報を共有している子会社又は取引先について、以下の事項を把握するための仕組みを整備すること。 - 会社ごとに取り交わす手段(受発注の手段、情報のやり取り等) - 取引に伴い授受・使用される情報資産及びその取扱い		
				2002-1-2	○	○	機密情報の取扱い	自社の機密情報の取扱い方法を、共有先との間で明確にすること。	★3	2-1-2-1	・自社の機密情報を共有する子会社又は取引先との間で、業務開始前に機密情報の取扱いについて、以下の事項を取り決めること。 - 機密情報の定義 - 機密情報の利用制限、保管方法、複製可否及び第三者への提供可否 - 機密情報の返還又は廃棄		

				2002-1-3		○	取引先のセキュリティ対策状況	事業継続リスク及び情報管理リスクの観点から自社に影響を及ぼす可能性のある取引先のセキュリティ対策状況を把握すること。	★4	2-1-3-1	・以下に示す条件のいずれか若しくは複数に該当する子会社又は取引先を対象に、年1回以上の頻度で、以下の例を参考にセキュリティ対策状況を把握すること。 [対策状況把握の対象とする子会社又は取引先の条件] - 自社の重要な機密情報を提供・共有する - 自社の事業継続にとって重要な位置づけを持つ - 当該取引先の環境から発注者の内部システムへのアクセスが可能 [対策状況の把握方法(例)] - 本制度が定める★の取得状況について取引先から回答を受領する、又は本制度の運用主体が管理するWebサイト等で確認する - 取引先に訪問し点検を実施する - セキュリティ対策チェックシートを作成して回答を受領する		
				2002-1-4	○	○	セキュリティインシデント発生時の役割・責任	セキュリティインシデント発生時の他社との役割及び責任を明確にすること。	★3	2-1-4-1	・自社の機密情報を共有する子会社又は取引先との間で、セキュリティインシデント発生時の自社と子会社又は取引先の役割及び責任を定めること。		
				2002-1-5		○	機密情報の回収・破棄	取引先との契約終了時に自社の機密情報及び当該機密情報へのアクセス権を回収する又は破棄させること。	★4	2-1-5-1	・自社の機密情報を共有する子会社又は取引先から、契約終了時に機密情報及びアクセス権が回収又は破棄されていることについて確認する手順(例：回収物一覧のチェックシートの作成)を整備すること。		
3	リスクの特定	3-1	資産管理	2003-1-1	○	○	情報機器、OS及びソフトウェアに関する情報の把握	情報機器、OS及びソフトウェアに関する情報を把握すること。	★3	3-1-1-1	・パソコン及びシンクライアントの製造元、OS及び台数を把握するための仕組みを整備すること。	識別(ID)	
										3-1-1-2	・サーバ、仮想サーバ及びハイパーバイザの製造元、OS及び台数を把握するための仕組みを整備すること。		
										3-1-1-3	・情報機器、OS及びソフトウェアについて、導入、設置、ネットワーク接続及びセキュリティパッチ適用のルールを含む管理ルールを定めること。		
										3-1-1-4	・年1回以上の頻度でNo.3-1-1-3で定めた管理ルールの遵守状況について点検すること。		
									★4	3-1-1-5	・スマートデバイスの製造元、OS及び台数を把握するための仕組みを整備すること。		
										3-1-1-6	・重要なシステムを構成する情報機器について、設定情報を把握するための仕組みを整備すること。		
										3-1-1-7	・年1回以上の頻度でNo.3-1-1-1、No.3-1-1-2、No.3-1-1-5及びNo.3-1-1-6で把握した情報の内容について、点検すること。		
				2003-1-2	○	○	ネットワークに関する情報の把握	ネットワークに関する情報を把握するための仕組みを整備すること。	★3	3-1-2-1	・ネットワークを把握するための仕組みを整備すること。その際、把握すべき情報の中に各ネットワークの所在地及び用途に関する情報を含めること。		
										3-1-2-2	・ネットワーク機器を把握するための仕組みを整備すること。その際、把握すべき情報の中に各機器の製造元、モデル及び保守事業者に関する情報を含めること。		
									★4	3-1-2-3	・ネットワークを対象として、ネットワーク図を作成すること。		
										3-1-2-4	・年1回以上の頻度でNo.3-1-2-3で作成したネットワーク図の記載内容について点検すること。		
				2003-1-3	○	○	外部情報サービスの管理	自社の機密情報を扱う外部情報サービスを管理すること。	★3	3-1-3-1	外部情報サービスを利用する際のセキュリティ要件を定めたうえで、外部情報サービスの利用時に当該要件を満たしているかサービス内容を確認すること。		
										3-1-3-2	・外部情報サービスの提供事業者と機密情報の取扱いについて合意を取り交わすこと。		
				2003-1-4	○	○	機密区分に応じた情報の管理	機密区分に応じた情報の管理ルールを定め、それに基づく管理を行うこと。	★3	3-1-4-1	・自社の保有する情報を対象に、以下の内容を含む管理ルールを定めること。 - 機密の特定 - 機密区分のレベル判定及び表示 - 区分に応じた取扱方法 - 取扱エリアの区分及び制限		
										3-1-4-2	・年1回以上の頻度でNo.3-1-4-1で定めた管理ルールの内容について点検すること。		
										3-1-4-3	・重要な機密情報並びに当該情報ごとの管理者名、部署名、保管場所、保管期限、開示先及び管理者の連絡先を把握するための仕組みを整備すること。		
									★4	3-1-4-4	・年1回以上の頻度でNo.3-1-4-3で把握した項目の内容について点検すること。		
										3-1-4-5	・退職時及び任期満了時には機密情報及び情報機器を回収すること。 - 回収物には、情報(印刷物及び記憶媒体)、パソコン、スマートデバイス及びアクセス権(ID及び鍵)を含めること。 - 回収漏れが起こらない手順(例：回収物一覧のチェックシートの作成)を整備すること。		
										3-1-4-6	・年1回以上の頻度でNo.3-1-4-5で求める機密情報及び情報機器の回収の状況について点検すること。		

									3-1-4-7	・サーバ、会社支給のパソコン、スマートデバイス及び外部記憶媒体の廃棄時(リース終了時を含む。)はデータを復元できないよう抹消処理を行うこと。 ※ディスクのフォーマットは、データを復旧される可能性があるため不十分		
									3-1-4-8	・サーバ、会社支給のパソコン、スマートデバイス及び外部記憶媒体の記憶領域を抹消処理した記録を保管すること。		
				2003-1-5		○	リモートワークにおけるルール	リモートワークで使用する情報機器及び機密情報の条件についてのルールを定めること。	★4	3-1-5-1	・リモートワークを実施する場合は、リモートワークで使用する情報機器及び機密情報の条件について、以下の事項に関するルールを定めること。 - リモートワークで使用許可する情報機器及び当該許可の申請・承認の方法 - 個人所有機器にダウンロード可能なファイルの機密区分及び種類		
										3-1-5-2	・No.3-1-5-1で定めたルールをリモートワークを行う全ての役員、従業員、派遣社員及び受入出向者に対して周知すること。		
										3-1-5-3	・年1回以上の頻度でNo.3-1-5-1で定めたルールの内容及び遵守状況について点検すること。		
		3-2	リスクアセスメント	2003-2-1		○	脆弱性の管理体制	脆弱性の管理体制、管理プロセスを定め、それに基づく管理を行うこと。	★4	3-2-1-1	・脆弱性情報/脅威情報の収集から対応まで担当部署の役割・責任を定めること。		
										3-2-1-2	・脆弱性情報/脅威情報を収集する情報源、ツール及び頻度を定めること。		
										3-2-1-3	・収集した脆弱性情報/脅威情報の対応要否判断基準・対応手順を定めること。		
										3-2-1-4	・管理対象の情報機器における脆弱性の残存状況を把握するための仕組みを整備すること。		
										3-2-1-5	・収集した脆弱性情報/脅威情報に対する対応履歴を記録し、対応漏れがないかどうかについて月次で点検すること。		
4	攻撃等の防御	4-1	アイデンティティ管理、認証、アクセス制御	2004-1-1	○	○	ユーザIDの管理手続	ユーザIDの発行・変更・削除の手続を定めること。	★3	4-1-1-1	・自社の役員、従業員、派遣社員及び受入出向者に対するユーザIDの付与・変更・削除は申請・承認制にすること。	防御(PR)	PassLogic対応
										4-1-1-2	・ユーザIDの共有について、以下のいずれかを適用すること。 - ユーザIDを共有しない。 - やむを得ず共有IDが必要な場合(例えば、システムの仕様により、使用人数分のユーザIDを発行することができない場合)は、共有IDを利用したユーザを特定できるようにする。		PassLogic対応
										4-1-1-3	・ユーザIDが不要になった場合(例えば、ユーザが組織を退職した場合又はユーザIDが一定期間使用されなかった場合)、速やかにユーザIDを削除又は無効化すること。		PassLogic対応
										4-1-1-4	ユーザIDに付与したアクセス権が不要になった場合(例えば、ユーザの業務上の役割が変わった場合)は、当該権限を速やかに削除又は無効化すること。		PassLogic対応
				2004-1-2	○	○	管理者IDの管理手続	管理者IDの発行・変更・削除の手続を定めること。	★3	4-1-2-1	・すべてのサーバ及びネットワーク機器について、システム管理者及び責任者を定めること。		
										4-1-2-2	・管理者権限を付与する役員、従業員、派遣社員及び受入出向者を限定したうえで、管理者IDについて以下のいずれかを適用すること。 - 管理者IDを共有しない。 - やむを得ず管理者IDの共有が必要な場合(例えば、システムの仕様により、使用人数分のIDを発行することができない場合)は、共有の管理者IDを利用したユーザを特定できるようにすること。		PassLogic対応
										4-1-2-3	・各管理者IDに対して当該IDの用途に応じた必要最低限の権限のみを付与すること。		PassLogic対応
										4-1-2-4	・開発環境を利用する役員、従業員、派遣社員及び受入出向者が本番環境において、開発環境における管理者権限で操作できないようにすること。		
										4-1-2-5	・組織内でどの役員、従業員、派遣社員及び受入出向者が管理者IDを持っているかを把握するための仕組みを整備すること。		PassLogic対応
										4-1-2-6	・管理者IDが不要になった場合(例えば、管理者が組織を退職した場合及び管理者IDが一定期間使用されなかった場合)、速やかに管理者IDを削除又は無効化すること。		PassLogic対応
										4-1-2-7	・管理者IDの付与・変更・削除は申請・承認制にすること。		
										4-1-2-8	・管理者IDの付与・変更・削除並びにサーバ及びネットワーク機器の設定内容の変更を行う権限を業務上必要な役員、従業員、派遣社員及び受入出向者に限定すること。		
				2004-1-3	○	○	認証の強度・実装方法の決定	システム及び情報の重要度に応じて認証の強度及び実装方法を決定すること。	★3	4-1-3-1	・すべてのユーザID及び管理者IDについて、システム及び情報機器へのアクセスを許可する前に、ユーザIDごとに設定されている認証情報(パスワード等)でユーザを認証すること。		PassLogic対応
										4-1-3-2	・重要な機密情報を取り扱うクラウドサービスにおいて、ユーザ及び管理者がサービスにアクセスする場合は、常にNo.4-1-3-3で示す認証要素を利用した多要素認証を使用すること。		PassLogic対応

									4-1-3-3	・多要素認証の使用に当たっては、以下のいずれかの要素から2種類以上を選択し、利用すること。 - 知識情報(例：ID・パスワード) - 所有情報(例：ワンタイムパスワード※又は証明書) - 生体情報(例：指紋、顔、虹彩又は静脈) - その他の情報(例：IPアドレス) ※利用者のメールアドレス、電話番号等に対してワンタイムパスワードを送信して利用者に入力させる方法及びスマートフォンへの認証要求を利用した認証方式を含む。		PassLogic対応
									4-1-3-4	・多要素認証の知識情報として用いるパスワードは、8文字以上とすること。		PassLogic対応
								★4	4-1-3-5	・重要な機密情報を取り扱うシステムにおいて、No.4-1-3-2で対象としているクラウドサービスへのアクセスに加えて、以下に示す場合は、常にNo.4-1-3-3で示す認証要素を使用した多要素認証を使用すること。 - インターネットを経由して社内環境へ接続する場合 - 管理者がインターネット経由でシステムにアクセスする場合 - ユーザがインターネット経由で重要な機密情報を取り扱うシステムにアクセスする場合		PassLogic対応
				2004-1-4	○	○	アカウントロック制御	パソコン及びスマートデバイスにはロック制御を行うこと。	★3	4-1-4-1	・パソコンへのログオン及びスマートデバイスのロック解除にあたって、以下のいずれかを適用すること。 - 試行回数を調整し、試行が失敗するたびに試行間隔が長くなるようにする。 - 試行が少なくとも10回以上失敗すると端末をロックする。 - 上記で示す要件のいずれも設定することができない場合、No.4-1-5で求められるよりも強度の高いパスワードを用いる等の代替策を用いること。		PassLogic対応
									4-1-4-2	・パソコンへのログオン及びスマートデバイスのロック解除を行う場合、最低でも6文字以上のパスワード又はPINを利用すること。		PassLogic対応
				2004-1-5	○	○	パスワード設定ルール	パスワード設定に関するルールを定め、周知すること。	★3	4-1-5-1	・パソコン、サーバ、スマートデバイス及びクラウドサービスの利用者又は管理者は、それらにおけるデフォルトパスワードを変更するよう社内ルールを定めること。		
										4-1-5-2	・ユーザ認証にパスワードを利用する場合、推測されやすい単語の設定を禁止するよう社内ルールを定めること。		
										4-1-5-3	・ユーザ認証にパスワードを利用する場合、以下のいずれかの保護対策を講じるよう社内ルールを定めること。 - No.4-1-3-3で示す認証要素を利用した多要素認証を使用するか、又は試行が少なくとも10回失敗した場合にアカウントロックするように制限したうえで、パスワードの長さを8文字以上とする。 - 上記のとおり多要素認証又は試行回数の制限を実施できない場合、パスワードの長さは、英大文字小文字、数字を含めた10文字以上とする。		PassLogic対応
										4-1-5-4	・ユーザ認証にパスワードを利用する場合、情報機器及びサービス間でのパスワードを使い回さないよう社内ルールを定めること。		
										4-1-5-5	No.4-1-5-1からNo.4-1-5-4までで定めたパスワード設定に関するルールについて、役員、従業員、派遣社員及び受入出向者を対象に周知すること。		
				2004-1-6	○	○	パスワード管理ルール	パスワードの管理に関するルールを定め、周知すること。	★3	4-1-6-1	・紙媒体への記載及び施錠保管、パスワード管理アプリの利用等により、パスワードを安全に保管するよう社内ルールを定めること。		
										4-1-6-2	・パスワードの漏洩が判明した場合、又はその疑いがある場合に速やかにパスワードを変更するための手順を定めること。		
										4-1-6-3	・No.4-1-6-1及びNo.4-1-6-2で定めたパスワードの管理に関するルールについて、役員、従業員、派遣社員及び受入出向者を対象に周知すること。		
				2004-1-7	○	○	アクセス権の管理ルール	アクセス権の管理ルールを定めること。	★3	4-1-7-1	・業務で利用するシステム及びパソコンへのログオン時のユーザのアクセス権並びに機密上の配慮が必要な場所及び部屋への入室について、以下の内容の管理ルールを定めること。 - アクセス権の発行・変更・削除は申請・承認制であること。 - 与える入室許可・アクセス権の範囲は必要な範囲に限定すること。 - 入室権限及びアクセス権の棚卸について定めていること。 - 与えた入室許可・アクセス権の申請書又は台帳を管理していること。		PassLogic対応
								★4	4-1-7-2	・年１回以上の頻度で役員、従業員、派遣社員及び受入出向者に付与したアクセス権の棚卸を実施すること。		PassLogic対応
									4-1-7-3	・重要な機密情報を扱うシステムは、アクセス権を付与するための条件を定めること。		
									4-1-7-4	・重要な機密情報を扱うシステムにおけるアクセス権の設定に当たっては、システム管理者の要件及び設定手順を定めること。		
									4-1-7-5	・重要な機密情報を扱うシステムは、ユーザ及び管理者ごとに必要最小限の権限を付与し、個人に権限が集中しない環境とすること。		PassLogic対応
									4-1-7-6	・重要な機密情報を扱うシステムは、付与したアクセス権の運用/利用状況を監視する仕組みを整備すること。		

				2004-1-8		○	サーバ設置エリアへの入退室管理	サーバの設置エリアへの入退室を管理し、記録すること。	★4	4-1-8-1	・サーバの設置エリアに入場可能な者を定めること。	
										4-1-8-2	・サーバの設置に当たって、以下のいずれかの安全確保策を適用すること。 - サーバの設置エリアを施錠すること。 - 施錠が出来ないエリアにサーバが設置されている場合、サーバを専用ラックに入れて施錠すること。	
										4-1-8-3	・No.4-1-8-2におけるサーバの設置エリア又は専用ラックの鍵等について、管理者を定めたうえで安全に管理すること。	
										4-1-8-4	・入退場日時及び入場者氏名を含めて、サーバの設置エリアの入退場記録を取得し、少なくとも6 ヶ月間保管すること。	
				2004-1-9		○	可搬媒体の制限	可搬媒体の持込み・持出しを制限すること。	★4	4-1-9-1	・パソコン、スマートデバイス、カメラ及び外部記憶媒体(個人所有機器の業務利用(BYOD)を含む。)を対象とした社内への持込みルールを定めること。	
										4-1-9-2	・パソコン、スマートデバイス、カメラ、外部記憶媒体(個人所有機器の業務利用(BYOD)を含む。)及び印刷物(図面等の機密書類)に関する社外への持出しルールを定めること。	
										4-1-9-3	・年1回以上の頻度でNo.4-1-9-1及びNo.4-1-9-2で定めたパソコン、スマートデバイス、カメラ及び外部記憶媒体(個人所有機器(BYOD)を含む。)における持込みルール及び持出しルールの内容及び遵守状況について点検すること。	
		4-2	意識向上とトレーニング	2004-2-1		○	セキュリティの意識向上のための教育・研修	経営層を含むすべての要員に対して、セキュリティの意識向上のための教育・研修を実施すること。	★4	4-2-1-1	・経営層が情報セキュリティに関する役割及び責任を理解するための機会を設けること。	
										4-2-1-2	・セキュリティに関する職場特有のリスクの理解及びルールの遵守が必要な場合、職場単位で重要なルール及びリスクについて、年１回以上の頻度で周知すること。	
										4-2-1-3	・以下のトピックについて、役員、従業員、派遣社員及び受入出向者を対象に、新規受入れ時、かつ、年１回以上、教育資料配布・掲示、e ラーニング、集合教育等による教育・研修を実施すること。 - 電子メールによるマルウェア感染の予防 - Web 閲覧によるマルウェア感染の予防 - 機密区分の定義と取扱い	
										4-2-1-4	・No.4-2-1-3で実施した教育・研修の実施状況を記録し、保管すること。	
										4-2-1-5	・年１回以上の頻度でセキュリティの意識向上のための教育・研修の実施内容について点検すること。	
				2004-2-2	○	○	セキュリティインシデント発生時の教育・訓練	セキュリティインシデント発生時の対応に関する教育・訓練を行うこと。	★3	4-2-2-1	・役員、従業員、派遣社員及び受入出向者を対象に、新規受入れ時、かつ、年1回以上の頻度で、セキュリティインシデント発生時の対応について、教育資料の配布・掲示に加え、e ラーニング又は集合教育による教育・訓練を実施すること。	
										4-2-2-2	・No.4-2-2-1で実施した教育・訓練の実施内容、実施方法、実施時期及び受講状況を記録し、保管すること。	
										4-2-2-3	・年１回以上の頻度でセキュリティインシデント発生時の対応に関する教育・訓練の実施内容について点検すること。	
		4-3	データセキュリティ	2004-3-1		○	データの暗号化	情報機器及び情報システムの保管データを適切に暗号化するようルールを定め、周知すること。	★4	4-3-1-1	・社外に持ち出すパソコン及び記憶媒体の機密情報を暗号化するルールを定め、役員、従業員、派遣社員及び受入出向者を対象に周知すること。	
										4-3-1-2	・重要な機密情報を暗号化するルールを定め、役員、従業員、派遣社員及び受入出向者を対象に周知すること。	
				2004-3-2		○	データの保管ルール	データを適切な場所に保管するようルールを定め、周知すること。	★4	4-3-2-1	・マルウェアによる被害を受けた場合に業務に支障をきたすデータはパソコン以外の社内ネットワーク(クラウドサービスを含む。)上の相対的に安全な区域にあるサーバに保管するようルールを定め、役員、従業員、派遣社員及び受入出向者を対象に周知すること。	
				2004-3-3		○	取引先との情報共有ルール	取引先との情報共有及び情報送信に関するルールを定め、周知すること。	★4	4-3-3-1	・取引先との情報共有及び情報送信に関して、以下をルールとして定め、役員、従業員、派遣社員及び受入出向者へ周知すること。 -社外とファイル共有する場合は、信頼できる相手とのみ共有すること。 -社外へファイル転送をする場合は、送信履歴を残すこと。	
				2004-3-4	○	○	適切なバックアップ	適切なバックアップを行うこと。	★3	4-3-4-1	・取得対象、取得頻度及び保管期間を定めて自社で取り扱うデータのバックアップを取得すること。	
										4-3-4-2	・重要な機密情報については、No.4-3-4-1におけるバックアップに加えて、遠隔地バックアップを実施すること。	
										4-3-4-3	・バックアップ対象ごとにリストア手順書を整備すること。	
		4-4	プラットフォームセキュリティ	2004-4-1	○	○	情報機器、OS及びソフトウェアの安全な構成	情報機器、OS及びソフトウェアの安全な構成を確立し、維持すること。	★3	4-4-1-1	・パソコン、サーバ及びスマートデバイスで利用を許可していないソフトウェアをすべて削除若しくは無効化するか、又は利用を許可するソフトウェア以外を自由にインストールできないようにすること。	
										4-4-1-2	・外部記録媒体を使用する端末について自動実行(auto-run)又は自動再生(auto-play)を無効化すること。	
										4-4-1-3	・サーバ及びネットワーク機器の設定変更を申請・承認制にすること。	
									★4	4-4-1-4	・パソコン及びサーバ上で不要サービス及びプロトコルを無効化すること。	

									4-4-1-5	・パソコン及びサーバ上で使用されているデフォルトユーザ ID の利用を停止するか、又はログインに当たって多要素認証等の強固な認証を用いること。	PassLogic対応
									4-4-1-6	・利用するOS及びソフトウェアについて、標準構成・設定ルールを定めること。	
				2004-4-2		○	サポート期限の切れたOS及びソフトウェアへの対策	サポート期限の切れたOS及びソフトウェアの利用停止及び更改を実施すること。	★4	4-4-2-1	・利用するOS及びソフトウェアについて、以下のいずれかを適用すること。 - 全てのOS及びソフトウェアについてサポートのあるものを利用すること。 - やむを得ずサポート切れのOS及びソフトウェアを利用する場合(例えば、代替システムを調達する必要があり、直ちに更改できない場合)は、更改計画を策定した上で、更改するまでの間、No.4-4-4-2で求める脆弱性悪用のリスクを低減する対策を実施すること。	
				2004-4-3		○	ログの取得	システムに関するログを取得し、異常を検知するため、定期的にレビューを行うこと。	★4	4-4-3-1	・インシデント発生時に調査を円滑に行うために必要なログとして、以下を取得及び保管すること。(※) [取得するログ(保管期間)] -ファイアウォールのログ(6 カ月) ※取引先と接続する閉域網の入口に設置されるものも含む。 取得項目：日時、送信元 IP アドレス及び送信先 IP アドレス -プロキシサーバのログ(6 カ月) 取得項目：日時、リクエスト元 IP アドレス及びURL -認証サーバのログ(6 カ月) 取得項目：日時、接続元 IP アドレス、ユーザID及び成功/失敗 ※クラウドサービスの利用も対象に含む。 ※利用するクラウドサービス又はシステム構成の仕様上、上記の要件を満たせない場合は、インシデント発生時の調査ができるよう、他の機器又は機能を利用して上記の要件に相当するログを取得及び保管すること。	PassLogic対応
										4-4-3-2	・No.4-4-3-1で取得及び保管を求めるログを脅威から保護するため、ログを保存する媒体及びシステムにインターネット経由でアクセスする場合は、常にNo.4-1-3-3で示す要素を利用した多要素認証を使用すること。	PassLogic対応
										4-4-3-3	・No.4-4-3-1で取得及び保管を求めるログのうち、認証サーバのログについては、月1回以上の頻度でモニタリングを実施し、不審な認証試行を検知すること。	PassLogic対応
				2004-4-4	○	○	セキュリティパッチ・アップデートの手続	情報機器、OS及びソフトウェアへのセキュリティパッチ及びアップデートの適用に係る手続を定めること。	★3	4-4-4-1	・システム、情報機器及びソフトウェアは以下の状態とすること。 - ライセンスが付与され、サポートされている。 - サポートが終了した場合に削除されるか、又はインターネットとの全てのトラフィックを遮断することで適用範囲から削除される。 - 可能であれば、自動アップデートが有効化されている。	
										4-4-4-2	・利用している機能又は設定に関して、以下のいずれかに該当するアップデートプログラムがリリースされてから14日以内に、アップデートすること。 - 当該アップデートが、ベンダーにより「重大」(Critical)又は 「高リスク」(High Risk)と説明される脆弱性を修正するものである。 - 当該アップデートが、CVSSの基本値が7.0以上の脆弱性を修正するものである。 - 当該アップデートが修正する脆弱性のレベルの詳細がベンダーから提供されていない。 ・やむを得ず上記のとおりアップデートができない場合(例えば、動作検証に一定期間を要し、期限内にアップデートが完了しない場合)は、アップデート適用までの間、以下のいずれかにより脆弱性悪用のリスクを低減する対策を実施すること。 - 脆弱性悪用の対象となる機能を無効化すること。 - ベンダーが推奨する回避策を実施すること。 - 対象となる情報機器を適用範囲内のネットワークから分離すること。 - 対象となる情報機器と適用範囲内のネットワークとの通信を監視し、当該脆弱性を悪用する不正な通信を遮断する機器又はソフトウェアを導入すること。 [対象] -会社支給のパソコンの OS、ブラウザ及びOffice ソフト -サーバの OS及びミドルウェア -会社支給のスマートデバイスのOS及びアプリ -インターネットとの境界に設置されているネットワーク機器のOS及びファームウェア	
									★4	4-4-4-3	・インターネットとの境界に設置されているネットワーク機器のOS及びファームウェアについては、CVSS 基本値 7.0以上の脆弱性を有していないこと。	
				2004-4-5	○	○	マルウェア感染からの保護	システムをマルウェア感染から保護すること。	★3	4-4-5-1	・ネットワークに接続しているすべてのパソコン及びサーバに、マルウェア対策ソフトウェアを導入すること。	
										4-4-5-2	・パソコン及びサーバごとにマルウェア対策ソフトのスキャン範囲及び頻度を定め、スキャンを実行すること。	
										4-4-5-3	・マルウェア対策ソフトウェアのパターンファイルを、ベンダーの推奨に従ってアップデートすること。	

									★4	4-4-5-4	・パソコン/Web ゲートウェイを対象に、不正な Web サイトへのアクセスを制限すること。		
										4-4-5-5	・メールによるマルウェア感染を防止するため、メールゲートウェイ、メールサーバ等でマルウェアチェックを実施すること。		
		4-5	技術インフラのレジリエンス	2004-5-1	○	○	ネットワーク境界防護	ネットワークを適切に分離し、境界部分を防護すること。	★3	4-5-1-1	・全てのファイアウォール(又はファイアウォール機能を持つネットワーク機器)及びルータについて、デフォルトの管理パスワードを強固で一意のパスワードに変更する、又はリモートアクセスを完全に無効化すること。		
										4-5-1-2	・ファイアウォール(又はファイアウォール機能を持つネットワーク機器)及びルータのパスワードを変更する手順を定めること。		
										4-5-1-3	・ファイアウォール(又はファイアウォール機能を持つネットワーク機器)及びルータに係る認証は、No.4-1-5で定めるパスワード設定等に関する評価基準を満たすこと。		
										4-5-1-4	・全てのファイアウォール(又はファイアウォール機能を持つネットワーク機器)について、認証されていないインバウンド通信を遮断すること。		
										4-5-1-5	・全てのファイアウォール(又はファイアウォール機能を持つネットワーク機器)について、インバウンド通信に関するファイアウォール・ルールが定められていること。		
										4-5-1-6	・全てのファイアウォール(又はファイアウォール機能を持つネットワーク機器)について、不要になったファイアウォール・ルールを速やかに削除又は無効化すること。		
										4-5-1-7	・ファイアウォール・ルールの変更をインターネット経由で行う場合、No.4-1-3-3で示す認証要素を利用した多要素認証を適用するか、又は信頼できるIPアドレスにアクセスを制限すること。		
									★4	4-5-1-8	・利用中のOSが対応していない場合を除いて、すべてのパソコン及びサーバにおいて、ソフトウェアファイアウォールを有効化すること。		
										4-5-1-9	・社外公開サーバ及び重要な機密情報を扱うサーバについて、それぞれ専用のネットワークセグメントに設置し、セグメント内外のアクセスを必要最小限に限定すること。		
5	攻撃等の検知	5-1	継続的監視	2005-1-1	○	○	ネットワーク接続・データの監視	ネットワーク上の適切な場所でネットワーク接続及びデータ転送を監視すること。	★3	5-1-1-1	・社内外ネットワークの境界又は端末において、インターネットから社内への通信及び社内から不正なサーバへの通信の双方について、不正アクセスをリアルタイム検知・遮断する仕組みを導入すること。	検知(DE)	
										5-1-1-2	・ネットワーク機器のログ及びアラートを分析し、セキュリティ担当部署の担当者又は管理者により不審な事象が発見された場合に、それがセキュリティインシデントに該当するかが判断されること。		
										5-1-1-3	・No.5-1-1-1で設置したネットワーク機器又はサービスについて、以下の要件を満たす異常時に通知する仕組みを導入すること。 -アラートが速やかに発報されること。 -インシデントの速報レポートが作成され、通知されること。		
				2005-1-2		○	情報機器及びソフトウェアの挙動監視	情報機器及びソフトウェアの状態及び挙動を監視すること。	★4	5-1-2-1	・会社支給のパソコンを対象に、社内で利用を許可するソフトウェアの一覧を作成すること。		
										5-1-2-2	・年1回以上の頻度で会社支給のパソコンにおけるソフトウェアのインストール状況について点検すること。		
										5-1-2-3	・外部から受け取ったファイルについて安全性を確認するため、マルウェア対策ソフトのリアルタイムスキャンを実行する、又は仮想環境上で安全性を確認する仕組みを整備する。		
		5-2	有害事象の分析	2005-2-1		○	セキュリティインシデントのレベルごとの対象範囲	セキュリティインシデントのレベル及びレベルごとの対象範囲を明確にすること。	★4	5-2-1-1	・自社におけるセキュリティインシデントのレベル及びレベルごとの対象範囲を定め、役員、従業員、派遣社員及び受入出向者に周知すること。		
										5-2-1-2	・No.4-4-3-3において不審な認証試行を検知した場合又はNo.5-1-1-1で導入されるネットワーク機器若しくはサービスからのアラートを受け取った場合は、No.5-2-1-1で定めたレベル及び対象範囲に基づき、どのレベルのインシデントに該当するかを分析し、判断すること。		
6	インシデントへの対応	6-1	インシデント管理	2006-1-1	○	○	インシデント対応手順	セキュリティインシデントへの対応手順、対応体制等を定めること。	★3	6-1-1-1	・以下の手順を含んだセキュリティインシデントへの対応手順を定めること。 ①発見報告、 ②初動、③調査・対応、④復旧、⑤最終報告	対応(RS)	
										6-1-1-2	・セキュリティインシデント発生時における社内外組織(関係当局及び所管省庁を含む。)の連絡先及び報告・情報共有ルートを定めること。		
										6-1-1-3	・セキュリティインシデント発生時におけるセキュリティを統括する役員(例えば、CISOを設置する会社の場合は、当該CISO)及びセキュリティ担当部署の役割・責任を定めること。		
										6-1-1-4	・年1回以上の頻度でNo.6-1-1-2及びNo.6-1-1-3にて定めたセキュリティインシデント発生時の体制について点検すること。		
										6-1-1-5	・セキュリティインシデントの報告フォーマットを整備すること。		
										6-1-1-6	・年１回以上及び社内外で重大なセキュリティインシデントが発生した際に、インシデント事例及びその対応策を社内部署へ共有していること。		

7	インシデントからの復旧	7-1	インシデント復旧計画の実行	2007-1-1	○	○	事業継続要件に沿った復旧準備	事業上重要なシステムについて、事業継続の要件に沿う復旧に必要な準備を行うこと。	★3	7-1-1-1	・事業継続上重要なシステムについて、サイバー攻撃を念頭に、業務の目標復旧レベルを定めたうえで、当該レベルまで業務を回復するために必要な対策を、以下の例を参考として整備すること。 [復旧のための対策(例)] - システムによる業務継続(例:予備機、クラウド環境等により待機系を整備する。) - 人手による業務継続(例:電話、FAX等による連絡又は業務の実施に備え、影響のある取引先の連絡先及び複数の連絡手段を整備する。)	復旧(RC)	
									★4	7-1-1-2	・事業継続上重要なシステムについて、サイバー攻撃を念頭に、以下の対策を構じること。 - 目標復旧時点への復旧ができるようにNo.4-3-4-1及びNo.4-3-4-2で取得したバックアップを保管すること。 - No.4-3-4-3で定めたリストア手順書どおりに、かつ、目標復旧時間内でバックアップの復元ができることを確認すること。		