セキュリティ対策実施状況調査票

1　基本要件　（全てのシステムが対象）

No.	項目	対策状況	備考
1.1	管理画面等について、ファイアウォール等によりアクセス制限を実施しているか。		
1.2	（OS・ミドルウェア等の）セキュリティパッチを定期的に適用しているか。 ※SaaSなど、県の責任範囲では適用する必要がない場合は「不要」を選択し、具体的な説明を備考欄に記入		
1.3	（OS・ミドルウェア等の）緊急のセキュリティパッチは早急に適用しているか。 ※SaaSなど、県の責任範囲では適用する必要がない場合は「不要」を選択し、具体的な説明を備考欄に記入		
1.4	（すべてのサーバ及び専用端末に対し）ウイルス対策ソフトを導入し、定義ファイルを最新に保っているか。 ※SaaSなど、県の責任範囲では適用する必要がない場合は「不要」を選択し、具体的な説明を備考欄に記入 ※AWS等のクラウドサービスの場合、EC2等のインスタンスベースのサービスについては市販のウイルス対策ソフトの導入が必要です。Amazon GuardDuty、AWS Shield、AWS WAFなど、AWSのサービスのみではウイルス対策ソフトの代替としては認められません。		
1.5	（すべてのサーバ及び専用端末に対し）ウイルス対策ソフトによるチェックの頻度はいくらか。 ※SaaSなど、県の責任範囲では適用する必要がない場合は「不要」を選択し、具体的な説明を備考欄に記入		
1.6	バックアップを取得する頻度はいくらか。 ※SaaSなど、県の責任範囲では適用する必要がない場合は「不要」を選択し、具体的な説明を備考欄に記入		
1.7	アクセスログを保存する期間はいくらか。 ※SaaSなど、県の責任範囲では適用する必要がない場合は「不要」を選択し、具体的な説明を備考欄に記入		
1.8	緊急時の連絡体制表、対応フロー等を策定しているか。		

2　大規模系システム要件　（構築費が5,000万円以上のシステムが対象）

○ 対象　○ 対象外

No.	項目	対策状況	備考
2.1	停止すると県民に重大な影響が出るサーバについては冗長化しているか。		
2.2	物理的なセキュリティや、耐震設備・防火設備などを備えた堅牢なデータセンター等にサーバを設置しているか。		

3　外部公開系システム要件　（ウェブサイトなど外部公開しているシステムが対象）

○ 対象　○ 対象外

No.	項目	対策状況	備考
3.1	各種サイバー攻撃に対応した安全なプログラミングを実施しているか。		
3.2	ログインパスワードは何文字以上としているか。		
3.3	ログインパスワードに含む必要のある文字種は何種類か。 ※アルファベット大文字、アルファベット小文字、数字、記号をそれぞれ１つの文字種としてカウントすること ※システム上制御しているパスワードポリシーを回答すること。運用上制御しているポリシーがある場合は、その旨備考欄に記入すること。		
3.4	外部インターネットサーバに機密情報を保存しない構成としているか。 ※単一サーバ構成の場合、機密情報は適切に設定された外部公開しない領域に保存されているか		

4　外部公開系かつ機密系システム要件　（３に該当し、かつ、個人情報など外部に漏えいできない機密情報を取り扱うシステムが対象）

○ 対象　○ 対象外

No.	項目	対策状況	備考
4.1	機密情報を含む外部との通信は暗号化しているか。		
4.2	サーバ上および操作端末上の機密情報は暗号化して保存しているか。		

5　外部公開系かつ無停止系システム要件　（３に該当し、かつ、停止すると住民の権利の侵害や行政運営の支障につながるシステムが対象）

○ 対象　○ 対象外

No.	項目	対策状況	備考
5.1	稼働状況を常時監視しているか。		
5.2	サーバを冗長化しているか。		

6　個人情報保有系システム要件　（県民または職員の個人情報を取り扱うシステムが対象）

○ 対象　○ 対象外

No.	項目	対策状況	備考
6.1	システムの運用時・変更時に、作業内容や作業日時等が記載された作業報告を作成し、当該作業者以外の職員等が確認しているか。		
6.2	システム変更時、複数人で作業しているか（単独作業には事前承認、事後確認等の手続きを行っているか）。		
6.3	不要なアカウントや権限を削除しているか。		
6.4	個人情報を外部に持ち出す際は、使用する記憶媒体等について事前に許可を求めているか。		
6.5	システム管理者のアクセス履歴や操作履歴を定期的に当該職員以外の職員等が確認しているか。		
6.6	契約期間の満了や情報機器の処分のタイミングで、不要なデータを復元不可能な形で消去しているか。		

※１　本調査票におけるシステム管理者とは、職員・委託先事業者を問わず、システムの管理権限を持つものを指す