資料３－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
第1部 情報セキュリティ基本方針	第1部 情報セキュリティ基本方針
今日、県民生活の場に情報通信技術が急速に普及し、電子メールのやり取りや、ホームページの閲覧、電子商取引などが広く行われるようになり、経済面や生活面において様々な変化が起きています。	今日、県民生活の場に情報通信技術が急速に普及し、電子メールのやり取りや、ホームページの閲覧、電子商取引などが広く行われるようになり、経済面や生活面において様々な変化が起きています。
一方で、情報通信技術の利用に係る事故や犯罪、操作ミス、さらには、自然災害による情報システムの障害が発生すれば県民生活に多大な影響を与えます。	一方で、情報通信技術の利用に係る事故や犯罪、操作ミス、さらには、自然災害による情報システムの障害が発生すれば県民生活に多大な影響を与えます。
本県でも、行政サービスを提供するため、多くの業務において情報通信技術を活用しており、個人情報や行政運営上重要な情報などの多数の情報資産を保有しています。	本県でも、行政サービスを提供するため、多くの業務において情報通信技術を活用しており、個人情報や行政運営上重要な情報などの多数の情報資産を保有しています。
これらの情報資産を様々な脅威から防ぐことは、県民の権利及び利益を守り、行政サービスを継続して提供するために必要不可欠です。	これらの情報資産を様々な脅威から防ぐことは、県民の権利及び利益を守り、行政サービスを継続して提供するために必要不可欠です。
そこで、本県は、情報セキュリティ対策に以下のとおり取り組むことを宣言します。	そこで、本県は、情報セキュリティ対策に以下のとおり取り組むことを宣言します。
１～７　（略）	１～７　（略）
８　公社等外郭団体においては、本対策基準等を参考に、各団体において情報セキュリティ対策に係る基本方針を策定するなど、必要な情報セキュリティ対策を実施するよう、所管部局は適正に助言等を行うこととする。	
９　職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行において、情報セキュリティの関係法令並びに情報セキュリティ基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順を遵守	８　職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行において、情報セキュリティの関係法令並びに情報セキュリティ基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順を遵守

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
します。	します。

資料３－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
第2部 情報セキュリティ対策基準	第2部 情報セキュリティ対策基準
目次　（略）	目次　（略）
本対策基準は、情報セキュリティ基本方針を実行に移すための、本県における情報資産に関する情報セキュリティ対策の基準を定めたものである。	本対策基準は、情報セキュリティ基本方針を実行に移すための、本県における情報資産に関する情報セキュリティ対策の基準を定めたものである。
第１　（略）	第１　（略）
第２　組織及び体制 県の情報セキュリティ管理については、以下の組織体制とする。（別紙１参照） １～８　（略） ９　情報セキュリティ監査統括責任者 (1)　（略） (2) 情報セキュリティ監査統括責任者は、福島県情報セキュリティ監査実施要綱を定め、監査実施計画を立案し、定期的に又は必要に応じて監査を実施する。 (3)　（略） 10～11　（略）	第２　組織及び体制 県の情報セキュリティ管理については、以下の組織体制とする。（別紙１参照） １～８　（略） ９　情報セキュリティ監査統括責任者 (1)　（略） (2) 情報セキュリティ監査統括責任者は、福島県情報セキュリティ監査実施要領を定め、監査実施計画を立案し、定期的に又は必要に応じて監査を実施する。 (3)　（略） 10～11　（略）
第３　情報資産の分類及び管理	第３　情報資産の分類及び管理

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
１～８　（略）	１～８　（略）
９　情報の送信及び情報資産の運搬	９　情報の送信及び情報資産の運搬
(1)　（略）	(1)　（略）
(2) インターネット等安全ではないネットワークを用いて機密性２以上の情報を送信する者は、パスワード等による暗号化等により、第三者に入手されても解読できないような安全措置を講じた上で送信しなければならない。	(2) インターネット等安全ではないネットワークを用いて機密性２以上の情報を送信する者は、暗号化又はパスワード設定等により、第三者に入手されても解読できないような安全措置を講じた上で送信しなければならない。
(3) 車両等により機密性２以上の情報資産を運搬する場合は、鍵付きのケース等への格納又はパスワード等による暗号化等により、情報資産の不正利用を防止するための措置を講じなければならない。	(3) 車両等により機密性２以上の情報資産を運搬する場合は、鍵付きのケース等への格納又は暗号化若しくはパスワードの設定等により、情報資産の不正利用を防止するための措置を講じなければならない。
(4)　（略）	(4)　（略）
10　情報資産の提供及び公表	10　情報資産の提供及び公表
(1)　（略）	(1)　（略）
(2) 機密性２以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化等を行わなければならない。	(2) 機密性２以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定等を行わなければならない。
(3)～(4)　（略）	(3)～(4)　（略）
11　（略）	11　（略）
第４　ネットワークの強靭性の向上	第４　ネットワークの強靭性の向上
１　ネットワークの分離	１　ネットワークの分離
県の基幹ネットワークである福島県情報通信ネットワークシステムについて、所管する情報システム管理者は、次の三つのネットワークに分離した	県の基幹ネットワークである福島県情報通信ネットワークシステムについて、所管する情報システム管理者は、次の三つのネットワークに分離した

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
上でネットワークごとの対策を講じる。	上でネットワークごとの対策を講じる。
(1) マイナンバー利用事務系（個人番号利用事務系）	(1) マイナンバー利用事務系（個人番号利用事務系）
ア～イ　（略）	ア～イ　（略）
ウ　やむを得ず、マイナンバー利用事務系と LGWAN 接続系との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、 その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。	ウ　やむを得ず、マイナンバー利用事務系と LGWAN 接続系との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。
エ～オ　（略）	エ～オ　（略）
(2)～(3)　（略）	(2)～(3)　（略）
第５　（略）	第５　（略）
第６　人的セキュリティ対策	第６　人的セキュリティ対策
１　職員等の遵守事項	１　職員等の遵守事項
(1)～(7)　（略）	(1)～(7)　（略）
(8) 異なるネットワークへの接続 職員等は、県が管理している情報機器及び記録媒体を、有線・無線を問わず、当該情報機器及び記録媒体を接続して利用するよう情報システム管理者	

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
によって定められたネットワークと異なるネットワークに接続してはならない。	
(9) 持ち出し及び持ち込みの記録 情報セキュリティ管理者及び情報システム管理者は、業務上必要な場合において、端末や記録媒体等の持ち出し及び持ち込みを許可する場合について、記録を作成し、保管しなければならない。	(8) 持ち出し及び持ち込みの記録 情報セキュリティ管理者及び情報システム管理者は、業務上必要な場合において、端末や記録媒体等の持ち出し及び持ち込みを許可する場合について、記録を作成し、保管しなければならない。
(10) 端末におけるセキュリティ設定変更の禁止 職員等は、端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。	(9) 端末におけるセキュリティ設定変更の禁止 職員等は、端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。
(11) 机上の端末等の管理 職員等は、席を離れるときは、端末をロックし、及びディスプレイを消去し、並びに記録媒体、文書等を容易に閲覧されない場所へ保管するなどの適正な措置を講じなければならない。	(10) 机上の端末等の管理 職員等は、席を離れるときは、端末をロックし、及びディスプレーを消去し、並びに記録媒体、文書等を容易に閲覧されない場所へ保管するなどの適正な措置を講じなければならない。
(12) 退職時等の遵守事項 職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を外部へ漏らしてはならない。	(11) 退職時等の遵守事項 職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を外部へ漏らしてはならない。
２～３　（略）	２～３　（略）
４　委託事業者に対する説明 情報システム管理者又は情報セキュリティ管理者は、ネットワーク及び情報システムの開発、保守等を事業者に委託する場合は、委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち	４　外部委託事業者に対する説明 情報システム管理者又は情報セキュリティ管理者は、ネットワーク及び情報システムの開発、保守等を外部事業者に委託する場合は、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
委託事業者が遵守しなければならない事項を説明しなければならない。	部委託事業者が遵守しなければならない事項を説明しなければならない。
５　（略）	５～６　（略）
６　情報セキュリティに関する事案の報告	６　情報セキュリティに関する事案の報告
(1) 庁内からの情報セキュリティに関する事案の報告	(1) 庁内からの情報セキュリティに関する事案の報告
ア～キ　（略）	ア～キ　（略）
ク　事案のうち重大なものは「第９　緊急時におけるセキュリティ対策」により対処する。	ク　事案のうち重大なものは「第８　緊急時におけるセキュリティ対策」により対処する。
(2) 県民等外部からの事案の報告	(2) 県民等外部からの事案の報告
ア～オ　（略）	ア～オ　（略）
カ　事案のうち重大なものは「第９　緊急時におけるセキュリティ対策」により対処する。	カ　事案のうち重大なものは「第８　緊急時におけるセキュリティ対策」により対処する。
(3)　（略）	(3)　（略）
第７　技術的セキュリティ対策	第７　技術的セキュリティ対策
１　（略）	１　（略）
２　情報システムの仕様書、作業記録等の管理	２　情報システムの仕様書、作業記録等の管理
(1)～(2)　（略）	(1)～(2)　（略）
(3) システム管理記録及び作業の確認	(3) システム管理記録及び作業の確認
ア～イ　（略）	ア～イ　（略）
ウ　情報システム担当者又は契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、２名以上で作業を行わなければならない。ただし、１名で作業する場合において、作業直後に他の担当者が確認で	ウ　情報システム担当者又は契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、２名以上で作業を行わなければならない。ただし、１名で作業する場合において、作業直後に他の担当者が確認で

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
きるような作業詳細を記録し、複数人でその作業結果を確認するときはこの限りでない。	きるような作業詳細を記録し、複数人でその作業結果を確認するときはこの限りでない。
(4)～(5)　（略）	(4)～(5)　（略）
３　（略）	３　（略）
４　電子メール、クラウドサービス等の管理	４　電子メール、クラウドサービス等の管理
(1) 電子メールシステムのセキュリティ管理	(1) 電子メールシステムのセキュリティ管理
ア～イ　（略）	ア～イ　（略）
ウ　電子メールシステムを運用する情報システム管理者と各情報システム管理者は、システム開発や運用、保守等のため庁舎内に常駐している委託事業者の作業員が電子メールアドレスの利用を行う場合、委託事業者を含めた三者で利用方法を取り決めなければならない。	ウ　電子メールシステムを運用する情報システム管理者と各情報システム管理者は、システム開発や運用、保守等のため庁舎内に常駐している外部委託事業者の作業員が電子メールアドレスの利用を行う場合、外部委託事業者を含めた三者で利用方法を取り決めなければならない。
エ　（略）	エ　（略）
オ　電子メールシステムを運用する情報システム管理者は、迷惑メール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。	オ　電子メールシステムを運用する情報システム管理者は、大量の迷惑メール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。
(2) 電子メール、クラウドサービスの利用制限	(2) 電子メール、クラウドサービスの利用制限
ア～キ　（略）	ア～キ　（略）
ク　職員等は、機密性２以上又は完全性２の電子データを外部へ送信する場合は、パスワード等による暗号化等を行わなければならない。	ク　職員等は、機密性２以上又は完全性２の電子データを外部へ送信する場合は、CISO 補佐が別に定める電子署名、暗号化又はパスワード設定の方法を使用して、送信しなければならない。
ケ　（略）	ケ　（略）
５　ソーシャルメディアサービスの利用	

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
(1) 情報セキュリティ管理者は、県が管理するアカウントでブログ、ソーシャルネットワーキングサービス、動画共有サイト等のソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。 ア　ソーシャルメディアサービスで発信できる情報を規定する。 イ　庁内で管理しているウェブサイト内において、利用するソーシャルメディアサービスのサービス名と当該アカウントページへのハイパーリンクを明記するページを設ける。 ウ　運用しているソーシャルメディアサービスの自由記述欄において、庁内ウェブサイト上のページの URL を記載する。 エ　ソーシャルメディアサービスの提供事業者が、「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合は、これを利用する。 オ　パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適正に管理するなどの方法で、不正アクセス対策を講じること。 (2) 機密性２以上の情報はソーシャルメディアサービスで発信してはならない。 (3) 利用するソーシャルメディアサービスごとの責任者を定めなければならない。 (4) アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。	

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
(5) 可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、本県の自己管理 Web サイトに当該情報を掲載して参照可能としなければならない。	
6　ユーザ ID の管理	5　ユーザ ID の管理
(1)　(略)	(1)　(略)
(2) 情報システム管理者による特権を付与されたユーザ ID の管理等	(2) 情報システム管理者による特権を付与されたユーザ ID の管理等
ア～ウ　(略)	ア～ウ　(略)
エ　情報システム管理者は、特権を付与された ID 及びパスワードの変更について、委託事業者に行わせてはならない。	エ　情報システム管理者は、特権を付与された ID 及びパスワードの変更について、委託事業者に行わせてはならない。
オ　(略)	オ　(略)
(3)　(略)	(3)　(略)
(4) 職員等のパスワードの取扱い	(4) 職員等のパスワードの取扱い
ア～キ　(略)	ア～キ　(略)
ク　職員等間でパスワードを共有しないこと（ただし、共用 ID に対するパスワードは除く。）。	ク　職員等間でパスワードを共有しないこと（ただし、共有 ID に対するパスワードは除く。）。
(5)～(6)　(略)	(5)～(6)　(略)
7　情報システムの調達及び保守等	6　情報システムの調達及び保守等
(1)～(8)　(略)	(1)～(8)　(略)
8　不正プログラム対策	7　不正プログラム対策
(1) CISO 補佐の措置事項	(1) CISO 補佐の措置事項
コンピュータウイルス等の不正プログラム対策として、次の事項の措置を講じなければならない。	コンピュータウイルス等の不正プログラム対策として、次の事項の措置を講じなければならない。

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
ア～カ　（略）	ア～カ　（略）
キ　業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用していないことを確認すること。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認すること。	キ　業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用していないことを確認すること。
(2)　（略）	(2)　（略）
(3) 職員等の遵守事項	(3) 職員等の遵守事項
ア～オ　（略）	ア～オ　（略）
カ　コンピュータウイルス等の不正プログラムに感染した場合は、速やかに情報セキュリティ管理者及び CISO 補佐に報告すること。	カ　コンピュータウイルス等の不正プログラムに感染した場合は、LAN ケーブルを即時取り外し、手動で全ファイル及び全ディスク領域に対してウィルスチェックを行い、情報セキュリティ管理者及び CISO 補佐に報告すること。
(4)　（略）	(4)　（略）
9　不正アクセス対策	8　不正アクセス対策
(1)～(6)　（略）	(1)～(6)　（略）
(7) CISO 補佐又は情報システム管理者は、職員等又は委託事業者が使用している端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。	(7) CISO 補佐又は情報システム管理者は、職員等又は外部委託事業者が使用している端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。
(8)～(9)　（略）	(8)～(9)　（略）
(10) CISO 補佐又は情報システム管理者は、	(10) CISO 補佐又は情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、必要な人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するため

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。	に、アクセス記録等を点検するなどの内部対策を講じなければならない。
10　セキュリティ情報の収集	9　セキュリティ情報の収集
(1)～(2)　（略）	(1)～(2)　（略）
第８　（略）	第８　（略）
第９　緊急時におけるセキュリティ対策	第９　緊急時におけるセキュリティ対策
１　体制の整備	１　体制の整備
(1)　（略）	(1)　（略）
(2) 緊急時対応計画には、以下の内容を定めなければならない。	(2) 緊急時対応計画には、以下の内容を定めなければならない。
ア～ウ　（略）	ア～ウ　（略）
	エ　再発防止措置の策定
エ　大規模障害時等において優先的に復旧させる必要がある業務とその対応方法	オ　大規模障害時等において優先的に復旧させる必要がある業務とその対応方法
オ　大規模障害時等において可用性の確保のために緩和する必要がある制限とその対応方法	カ　大規模障害時等において可用性の確保のために緩和する必要がある制限とその対応方法
(3)～(4)　（略）	(3)～(4)　（略）

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
２～６　（略） 第 10　業務委託と外部サービスの利用及び職員等以外による情報システムの利用 １　業務委託 (1)　委託先の選定基準 情報システム管理者又は情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考に情報セキュリティが確保されることを確認の上、情報システムに係る委託先の事業者を選定しなければならない。 (2)　委託における契約項目 情報システムの運用、保守等を事業者に委託する場合は、必要に応じ、次の情報セキュリティ要件を明記した上で、事業者と契約を締結しなければならない。 ア～ス　（略） セ　委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法 ソ　サービス拠点及びサービス拠点で使用する外部回線に係る災害時及び原子力発電所事故時のサービスレベル タ　クラウドサービス基盤提供業者等の第三者が提供するサービス	２～６　（略） 第 10　外部委託及び職員等以外による情報システムの利用 １　外部委託先の選定基準 情報システム管理者又は情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考に情報セキュリティが確保されることを確認の上、情報システムに係る外部委託先の事業者を選定しなければならない。 ２　外部委託における契約項目 (1) 情報システムの運用、保守等を外部の事業者に委託する場合は、必要に応じ、次の情報セキュリティ要件を明記した上で、事業者と契約を締結しなければならない。 ア～ス　（略） セ　外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法 (2)　クラウドサービスを利用する場合は、上記(1)に加え、以下の点を確認の上、必要な情報セキュリティ要件を満たすことを明記した契約を締結しなければならない。 ア　サービス拠点及びサービス拠点で使用する外部回線に係る災害時及び原子力発電所事故時のサービスレベル イ　クラウドサービス基盤提供業者等の第三者が提供するサービスについて

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
チ　入力又は保存された情報は、クラウドサービス基盤提供業者等の第三者によって、どのように利用されるか ツ　入力又は保存された情報は、削除することが可能か (3)　委託における確認、措置等 ① 情報システム管理者は、委託事業者が必要なセキュリティ対策を講じていることを定期的に確認し、必要に応じ、CISO 補佐に報告しなければならない。 ② 情報システム管理者は、クラウドサービスを利用する場合は、サービスの内容及び入力又は保存された情報に係るクラウドサービス基盤提供業者等による利用状況を定期的に確認し、サービスの利用を継続するかどうか判断しなければならない。 ２　外部サービスの利用（機密性２以上の情報を取り扱う場合） (1) 約款による外部サービスを利用し、機密性２以上の情報資産を扱ってはならない。 (2) 外部サービスの選定 ①　情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限を踏まえ、	(3) パブリッククラウドサービスを利用する場合は、上記(1)(2)に加えて、以下の点を確認の上、必要な情報セキュリティ要件を満たすことを明記した契約を締結しなければならない。 ア　入力又は保存された情報は、クラウドサービス基盤提供業者等の第三者によって、どのように利用されるか。 イ　入力又は保存された情報は、削除することが可能かどうか。 ３　外部委託における確認、措置等 (1) 情報システム管理者は、外部委託事業者が必要なセキュリティ対策を講じていることを定期的に確認し、必要に応じ、CISO 補佐に報告しなければならない。 (2) 情報システム管理者は、クラウドサービスを利用する場合は、サービスの内容及び入力又は保存された情報に係るクラウドサービス基盤提供業者等による利用状況を定期的に確認し、サービスの利用を継続するかどうか判断しなければならない。 ４　約款による外部サービスの利用 (1) 約款による外部サービスを利用し、機密性３の情報資産を扱ってはならない。 (2) 約款による外部サービスを利用する場合、CISO 補佐と協議し、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクを認識し、情報セキュリティ対策を適正に講じた上で利用しなければならない。

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
次の判断基準に従って、外部サービスの利用を検討しなければならない。	
ア　外部サービスを利用する目的の明確化	
イ　外部サービスを利用する業務範囲の明確化	
ウ　外部サービスを利用する際におけるリスク対策	
(ｱ)　外部サービス提供者の運用詳細等が公開されない場合に、利用者が情報セキュリティ対策を行うことが困難となるリスク	
(ｲ)　利用者が、利用する外部サービスを自組織のセキュリティポリシーに見合うサービスかどうか評価が適切に出来ない場合、セキュリティに対する影響が発生するリスク	
(ｳ)　外部サービス提供者が所有する資源の一部を利用者が共有し、その上に個々の利用者が管理する情報システムが構築されるなど、不特定多数の利用者の情報やプログラムを一つの外部サービス基盤で共用することにより、情報が漏えいするリスク	
(ｴ)　外部サービスで提供される情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることによるカントリーリスク	
(ｵ)　サーバ装置等機器の整備環境が外部サービス提供者の都合で急変する場合、サプライチェーン・リスクへの対策が容易に確認できないリスク	
エ　外部サービスで個人情報（特定個人情報を含む）を扱う場合は、個人情報保護法で定められた安全管理措置及び特定個人情報保護評価（PIA）の実施	
②　情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限を踏まえ、以下に示す事項について基本契約又はサービスレベル契約（SLA）で定める	

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
ことが出来る外部サービス提供者を選定しなければならない。	
ア　日本の裁判管轄、法令が適用される。海外への機密情報の流出リスクを考慮し、外部サービスを提供するリージョン（国・地域）を国内に指定する。国内の外部サービスにおいて、利用者のデータが、海外に保存されないこと。これらの事項を基本契約に定める	
イ　外部サービスの中断時の復旧要件について基本契約又はサービスレベル契約（SLA）に定める	
ウ　外部サービスの終了又は変更時における事前の通知等の取り決めや情報資産の移行方法について基本契約に定める	
エ　稼動率、目標復旧時間、目標復旧ポイント、バックアップの保管方法などの可用性に関する事項をサービスレベル契約（SLA）に定める	
オ　外部サービス提供者が、利用者の情報資産へ目的外のアクセスや利用を行わないように基本契約に定める	
カ　外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制について、公開資料や監査報告書（又は内部監査報告書・事業者の報告資料）の内容を確認する	
キ　外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、利用者の意図しない変更が加えられないための管理体制について、公開資料や監査報告書（又は内部監査報告書・事業者の報告資料）の内容を確認する	
ク　情報セキュリティインシデントへの対処方法について、外部サービス提供者との責任分担や連絡方法を取り決め、基本契約又はサービスレベル契約	

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
（SLA）に定める	
ケ　脅威に対する外部サービス提供者の情報セキュリティ対策（なりまし、情報漏えい、情報の改ざん、否認防止、権限昇格への対応、サービス拒否・停止等）の実施状況やその他契約の履行状況の確認方法を基本契約又はサービスレベル契約（SLA）に定める	
コ　情報セキュリティ対策の履行が不十分な場合の対処方法について、基本契約又はサービスレベル契約（SLA）に定める	
サ　外部サービス提供者により、利用規約、各種設定が変更される可能性があるため、変更内容の確認方法や連絡方法を基本契約又はサービスレベル契約（SLA）に定める	
③　情報セキュリティ管理者は、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めなければならない。	
ア　外部サービスの利用を通じて取り扱う情報の外部サービス提供者における目的外利用の禁止	
イ　外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制	
ウ　外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、意図しない変更が加えられないための管理体制	
エ　外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョ	

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
ンの指定	
オ　情報セキュリティインシデントへの対処方法	
カ　情報セキュリティ対策その他の契約の履行状況の確認方法	
キ　情報セキュリティ対策の履行が不十分な場合の対処方法	
④　情報セキュリティ管理者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めなければならない。	
⑤　情報セキュリティ管理者は、外部サービスの利用を通じて取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めなければならない。	
ア　情報セキュリティ監査の受入れ	
イ　サービスレベルの保証	
⑥　情報セキュリティ管理者は、外部サービスの利用を通じて取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。	
⑦　情報セキュリティ管理者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を提供し、県の承認を受けるよう、外部サービス提供者の選定条件に含めなければならない。	

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
⑧　情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定しなければならない。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めなければならない。（ISO/IEC 27017（クラウドサービスに関する情報セキュリティ管理策のガイドライン規格。「情報マネジメントシステム認証センター」が取得組織を公開）や、ISMAP（政府情報システムのためのセキュリティ評価制度。「サービスリスト」（事業者一覧）を公開）の基準等を満たしていること。）	
⑨　情報セキュリティ管理者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めなければならない。	
⑩　情報セキュリティ管理者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。	
(3) 外部サービスの利用に係る調達・契約	
①　情報セキュリティ管理者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。	
②　情報セキュリティ管理者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調	

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
達仕様の内容を契約に含めなければならない。	
(4) 外部サービスの利用承認	
①　情報セキュリティ管理者は、外部サービスを利用する場合には、情報セキュリティ管理者（総括担当）の許可を得なければならない。	
②　情報セキュリティ管理者（総括担当）は、外部サービスの利用を許可した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名しなければならない。	
(5) 外部サービスを利用した情報システムの導入・構築時の対策	
①　情報セキュリティ管理者又は情報システム管理者は、外部サービスを利用して情報システムを構築する際に以下のセキュリティ対策を実施しなければならない。	
ア　不正なアクセスを防止するためのアクセス制御	
イ　取り扱う情報の機密性保護のための暗号化	
ウ　開発時におけるセキュリティ対策	
エ　設計・設定時の誤りの防止	
②　外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録しなければならない。	
(6) 外部サービスを利用した情報システムの運用・保守時の対策	
①　情報セキュリティ管理者又は情報システム管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスを利用して情報システムを運用する際は以下のセキュリティ対策を実施しなければならない。	
ア　外部サービス利用に必要な教育	

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
イ　取り扱う資産の管理	
ウ　不正アクセスを防止するためのアクセス制御	
エ　取り扱う情報の機密性保護のための暗号化	
オ　外部サービス内の通信の制御	
カ　設計・設定時の誤りの防止	
キ　外部サービスを利用した情報システムの事業継続	
②　情報セキュリティ管理者又は情報システム管理者は、外部サービスで発生したインシデントを認知した際の対処手順を整備しなければならない。	
③　外部サービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録しなければならない。	
(7) 外部サービスを利用した情報システムの更改・廃棄時の対策	
①　情報セキュリティ管理者又は情報システム管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスの利用を終了する際に以下のセキュリティ対策を実施しなければならない。	
ア　外部サービスで取り扱った情報の廃棄	
イ　外部サービスの利用のために作成したアカウントの廃棄	
②　外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録しなければならない。	
３　外部サービスの利用（機密性２以上の情報を取り扱わない場合）	
(1) 外部サービスの利用における対策の実施	
①　職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で、情報セキュリティ管理者	

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
の許可を得なければならない。 ②　情報セキュリティ管理者は、外部サービスの利用を許可した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名しなければならない。 ③　承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講じなければならない。	5　ソーシャルメディアサービスの利用 (1) 情報セキュリティ管理者は、県が管理するアカウントでブログ、ソーシャルネットワーキングサービス、動画共有サイト等のソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。 ア　ソーシャルメディアサービスで発信できる情報を規定する。 イ　庁内で管理しているウェブサイト内において、利用するソーシャルメディアサービスのサービス名と当該アカウントページへのハイパーリンクを明記するページを設ける。 ウ　運用しているソーシャルメディアサービスの自由記述欄において、庁内ウェブサイト上のページの URL を記載する。 エ　ソーシャルメディアサービスの提供事業者が、「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合は、これを利用する。 オ　パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適正に管理するなどの方法で、不正アクセス対策を講

資料３－２

福島県情報セキュリティポリシー改正　新旧対照表

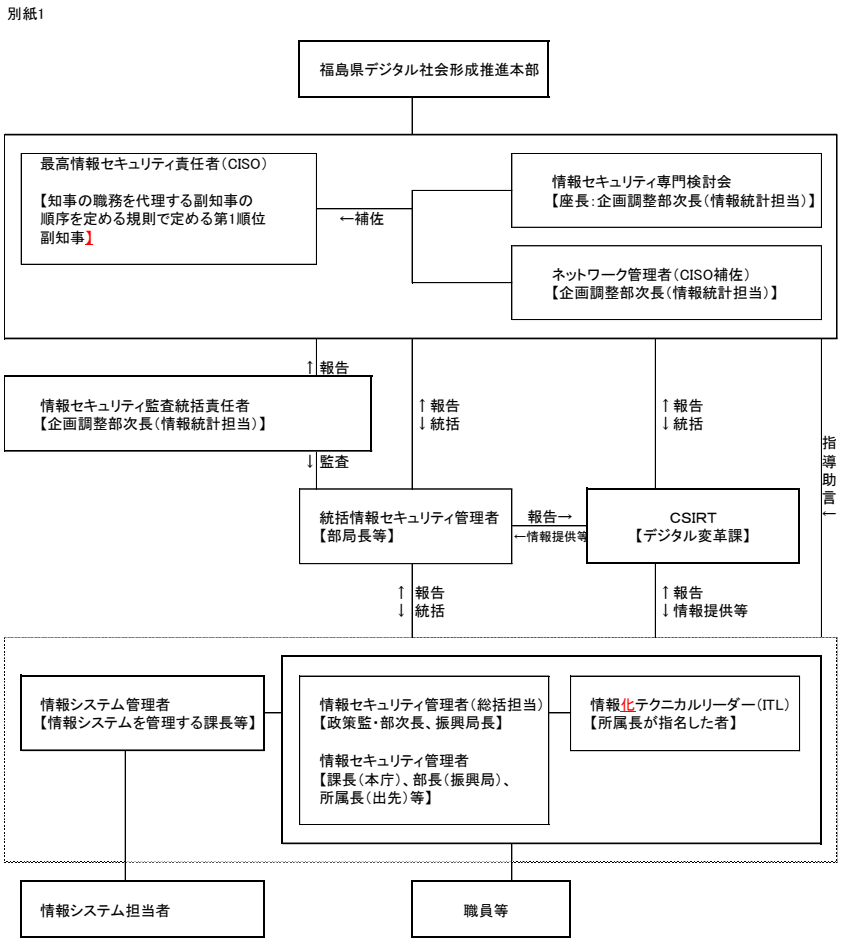
新	旧
	じること。 (2)　機密性２以上の情報はソーシャルメディアサービスで発信してはならない。 (3)　利用するソーシャルメディアサービスごとの責任者を定めなければならない。
4　職員等以外による情報システムの利用 情報システム管理者又は情報セキュリティ管理者は、次の要件をすべて満たす場合、事前に CISO 補佐の許可を得て職員等以外の者に情報システムを利用させることとする。 (1)～(2)　（略）	6　職員等以外による情報システムの利用 情報システム管理者又は情報セキュリティ管理者は、次の要件をすべて満たす場合、事前に CISO 補佐の許可を得て職員等以外の者に情報システムを利用させることとする。 (1)～(2)　（略）
第 11　例外措置 １～２　（略） ３　例外措置の記録 CISO 補佐は、例外措置を記録して適正に保管し、定期的に状況を確認しなければならない。	第 11　例外措置 １～２　（略） ３　例外措置の記録 CISO 補佐は、例外措置を記録し、これを保管しなければならない。
第 12　（略）	第 12　（略）
第 13　評価 1　監査 (1)～(4)　（略）	第 13　評価 1　監査 (1)～(4)　（略）

福島県情報セキュリティポリシー改正　新旧対照表

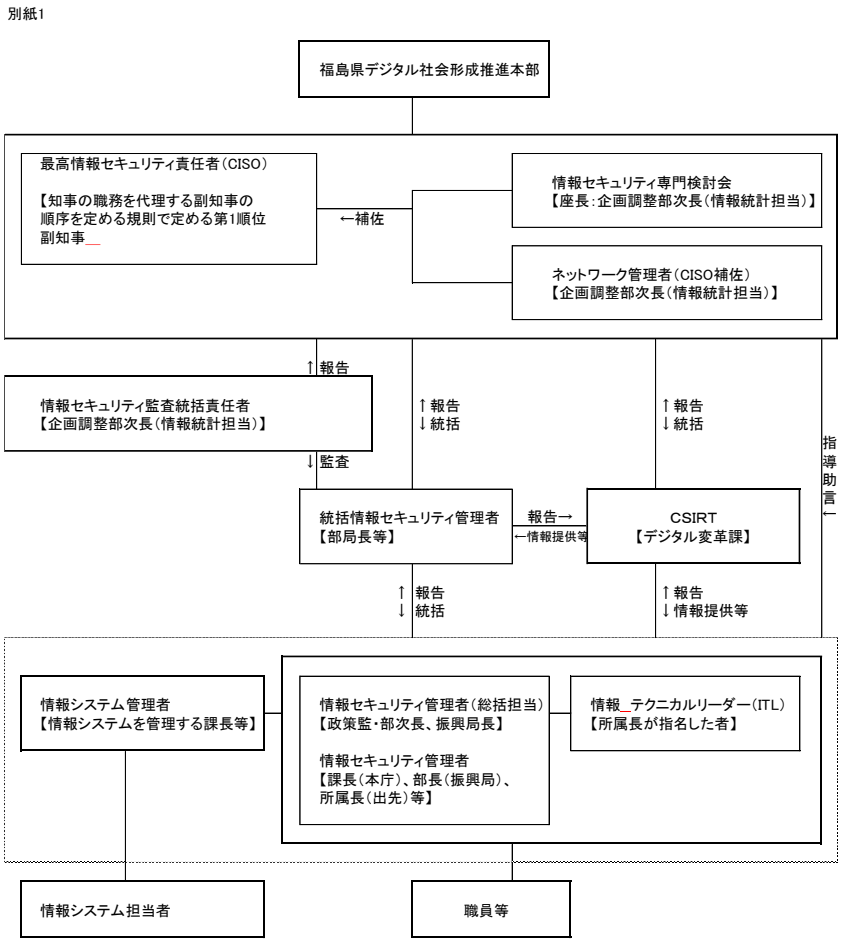
新	旧
(5)　情報セキュリティ監査統括責任者は、　事業者に業務委託している場合、再委託事業者も含めて、情報セキュリティポリシーの遵守に係る監査を実施しなければならない。	(5)　情報セキュリティ監査統括責任者は、外部事業者に業務委託している場合、再委託事業者も含めて、情報セキュリティポリシーの遵守に係る監査を実施しなければならない。
(6)～(8)　（略）	(6)～(8)　（略）
(9)　CISO は、監査結果を情報セキュリティポリシー及びその他の情報セキュリティ対策の見直しに活用しなければならない。	(9)最高情報セキュリティ責任者は、監査結果を情報セキュリティポリシー及びその他の情報セキュリティ対策の見直しに活用しなければならない。
２　（略）	２　（略）
第 14～15　（略）	第 14～15　（略）
附　則 この対策基準は、平成２５年１月１日から施行する。 附　則 この対策基準は、平成２６年４月２１日から施行する。 附　則 この対策基準は、平成２８年４月２５日から施行する。 附　則 この対策基準は、令和元年７月１１日から施行する。 附　則 この対策基準は、令和３年４月１日から施行する。 附　則 この対策基準は、令和５年６月５日から施行する。	附　則 この対策基準は、平成２５年１月１日から施行する。 附　則 この対策基準は、平成２６年４月２１日から施行する。 附　則 この対策基準は、平成２８年４月２５日から施行する。 附　則 この対策基準は、令和元年７月１１日から施行する。 附　則 この対策基準は、令和３年４月１日から施行する。

福島県情報セキュリティポリシー改正　新旧対照表

新



旧



福島県情報セキュリティポリシー改正　新旧対照表

新

別紙２

機密性による情報資産の分類　（略）

完全性による情報資産の分類　（略）

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性３	利用不能になった場合、県の経済に大きな損失を与え、又は行政事務全体に影響を与えるもの	・バックアップ、指定する時間以内の復旧 ・記録媒体の施錠可能な場所への保管
可用性２	可用性３以外の情報資産のうち、滅失、紛失又は利用不能により、個人の権利が侵害され、又は行政事務の安定的な遂行に支障（軽微なものを除く）を及ぼすおそれがあるもの	
可用性１	可用性２又は可用性３以外のもの（複写であることが明らかな文書を含めてもよい）	

旧

別紙２

機密性による情報資産の分類　（略）

完全性による情報資産の分類　（略）

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性３	利用不能になった場合、県の経済に大きな損失を与え、又は行政事務全体に影響を与えるもの	・バックアップ、指定する時間以内の復旧 ・記録媒体の施錠可能な場所への保管
可用性２	可用性３以外の情報資産のうち、滅失、紛失又は利用不能により、個人の権利が侵害され、又は行政事務の安定的な遂行に支障（軽微なものを除く）を及ぼすおそれがあるもの	
可用性１	可用性３又は可用性２以外のもの（複写であることが明らかな文書を含めてもよい）	