資料４－２

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 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。 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。 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。 １～９　（略）	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。 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。 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。 １～９　（略）

資料４－２

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	目次
第１～７（略）	第１～７（略）
第８　運用におけるセキュリティ対策	第８　運用におけるセキュリティ対策
１　情報システムの運用・保守時の対策	
２　情報システムの監視機能	
３　情報システムの監視	１　情報システムの監視
４　情報セキュリティポリシーの遵守状況の確認	２　情報セキュリティポリシーの遵守状況の確認
第９　（略）	第９　（略）
第10　業務委託とクラウド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	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　（略）	１　（略）
２　情報システムに関する業務委託	
３　クラウドサービスの利用（自治体機密性２以上の情報を取り扱う場合）	２　外部サービスの利用（自治体機密性２以上の情報を取り扱う場合）
４　クラウドサービスの利用（自治体機密性２以上の情報を取り扱わない場合）	３　外部サービスの利用（自治体機密性２以上の情報を取り扱わない場合）
５　職員等以外による情報システムの利用	４　職員等以外による情報システムの利用

資料４－２

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11～15　（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。 第１　（略） 第２　組織及び体制 １～６　（略） ７　情報システム管理者 (1)　（略） (2) 情報システム管理者は、所管する情報システムの情報セキュリティ＿＿に係る権限及び責任を有する 第３　情報資産の分類及び管理 １　（略） ２　情報資産の管理責任 (1)　（略） (2) 情報システム管理者は、所管する情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。	第11～15　（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。 第１　（略） 第２　組織及び体制 １～６　（略） ７　情報システム管理者 (1)　（略） (2) 情報システム管理者は、所管する情報システムの情報セキュリティ対策に係る権限及び責任を有する 第３　情報資産の分類及び管理 １　（略） ２　情報資産の管理責任 (1)　（略） (2) 情報システム管理者は、所掌する情報システムを管理する責任を有する。

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
(3)情報セキュリティ管理者は、情報資産が複製又は伝送された場合には、複製等された情報資産も別紙２の分類に基づき管理しなければならない。	(3)
3　　(略)	3　　(略)
4　情報システムで取り扱う情報資産の範囲	4　情報システムで取り扱う情報資産の範囲
(1)　　(略)	(1)　　(略)
(2)　取り扱う情報資産の範囲の確認 職員等は、情報システムに自治体機密性２以上、自治体完全性２又は自治体可用性２以上の情報資産を登録する場合は、(1)の情報システムで取り扱う情報資産の範囲を確認しなければならない。	(2)　取り扱う情報資産の範囲の確認 職員等は、情報システムに　機密性２以上、　完全性２又は　可用性２以上の情報資産を登録する場合は、(1)の情報システムで取り扱う情報資産の範囲を確認しなければならない。
5　情報資産の作成、編集	5　情報資産の作成、編集
(1)　　(略)	(1)　　(略)
(2)　情報システム管理者　は、その作成時に別紙２の基準に従い当該情報資産の分類を定めなければならない。	(2)　情報資産を作成する者は、その作成時に別紙２の基準に従い当該情報資産の分類を定めなければならない。
(3)　　(略)	(3)　　(略)
6　情報資産の入手、複写	6　情報資産の入手、複写
(1)情報システム管理者は、情報資産の　入手後又は複写後の情報資産の機密性については入手元又は複写元の情報資産の機密性の分類に従い、完全性と可用性については新たに情報資産の分類を定めなければならない。	(1)　情報資産　を入手し、又は複写する者は、入手後又は複写後の情報資産の機密性については入手元又は複写元の情報資産の機密性の分類に従い、完全性と可用性については新たに情報資産の分類を定めなければならない。
(2)情報システム管理者は、情報資産の分類の表示がない情報資産を入手し、又は複写した場合は、別紙２の基準に従い当該情報資産の分類を定めなければならない。	(2)　情報資産の分類の表示がない情報資産を入手し、又は複写した場合は、別紙２の基準に従い当該情報資産の分類を定めなければならない。

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
	(3) 入手し、又は複写した情報資産の分類が不明な場合は、情報セキュリティ管理者又は情報システム管理者に判断を仰がなければならない。
7　情報資産の利用	7　情報資産の利用
(1)～(2) (略)	(1)～(2) (略)
(3) 記録媒体を扱う者は、当該記録媒体に保管されている情報資産のうち、自治体機密性、自治体完全性、自治体可用性の最も高い分類に従い記録媒体を扱わなければならない。	(3) 記録媒体を扱う者は、当該記録媒体に保管されている情報資産のうち、＿＿機密性、＿＿＿完全性、＿＿＿可用性の最も高い分類に従い記録媒体を扱わなければならない。
8　情報資産の保管	8　情報資産の保管
(1)　(略)	(1)　(略)
(2) 自治体機密性２以上、自治体完全性２又は自治体可用性２以上の情報資産を記録した外部記録媒体を保管する場合は、施錠するなどの安全対策を講じた場所に保管しなければならない。	(2) ＿＿＿機密性２以上、＿＿＿完全性２又は＿＿＿可用性２以上の情報資産を記録した外部記録媒体を保管する場合は、施錠するなどの安全対策を講じた場所に保管しなければならない。
(3) 自治体完全性２又は自治体可用性２以上の情報資産を記録した外部記録媒体を保管する場合は、火災、異常発熱、漏水、結露及び静電気の安全対策を講じた場所に保管しなければならない。	(3) ＿＿＿完全性２又は＿＿＿可用性２以上の情報資産を記録した外部記録媒体を保管する場合は、火災、異常発熱、漏水、結露及び静電気の安全対策を講じた場所に保管しなければならない。
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自治体機密性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、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。
(3) 車両等により自治体機密性２以上の情報資産を運搬する場合は、鍵付きの	(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

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
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。	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。
(4) 自治体機密性２以上の情報資産を運搬する場合は、所管する情報セキュリティ管理者又は情報システム管理者の許可を得なければならない。	(4) ＿＿機密性２以上の情報資産を運搬する場合は、所管する情報セキュリティ管理者又は情報システム管理者の許可を得なければならない。
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) 自治体機密性２以上の情報資産を外部に提供する者は、提供する相手方のシステムの運用方針及びセキュリティ対策が当該情報資産の自治体機密性と合致していることを確認の上、提供しなければならない。	(1) ＿＿機密性２以上の情報資産を外部に提供する者は、提供する相手方のシステムの運用方針及びセキュリティ対策が当該情報資産の＿＿機密性と合致していることを確認の上、提供しなければならない。
(2) 自治体機密性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、必要に応じパスワード等による暗号化等を行わなければならない。
(3) 自治体機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理者又は情報システム管理者の許可を得なければならない。	(3) ＿＿機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理者又は情報システム管理者の許可を得なければならない。
(4)　（略）	(4)　（略）
11　情報資産の廃棄等	11　情報資産の廃棄等
(1)～(2)（略）	(1)～(2)（略）
(3) 自治体機密性３Ａ～Ｃの情報資産を扱ったことがある記録媒体が不要になった場合は、その記録を保持しているディスクそのもの又は記憶素子を物理的に破壊し、又は記録媒体完全消去用のソフトウェア等で、データの復活が不可能になるよう処理した上で廃棄等を行わなければならない。	(3) ＿＿機密性３＿＿の情報資産を扱ったことがある記録媒体が不要になった場合は、その記録を保持しているディスクそのもの又は記憶素子を物理的に破壊し、又は記録媒体完全消去用のソフトウェア等で、データの復活が不可能になるよう処理した上で廃棄等を行わなければならない。
(4)　（略）	(4)　（略）
第４　（略）	第４　（略）

資料４－２

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５　物理的セキュリティ対策 １　サーバ等の設置条件 (1)　　（略） (2) 情報システム管理者は、自治体可用性２以上の情報を格納するサーバ、セキュリティサーバ、住民サービスに関するサーバ等重要なサーバ等を多重化し、同一データを複数保持しなければならない。 (3) 情報システム管理者は、自治体可用性３の情報を格納しているサーバ等については、必要に応じ、移設できるように設置するものとする。 ２　電源 (1) 自治体可用性２以上のサーバ等の機器については、電源の停止時に自動的にサーバ等を停止する機能を備えた予備電源を設置することとし、予備電源の容量は、当該機器を安全に停止するまでの間、十分に電力を供給することができるものとする。 (2)　　（略） ３　　（略） ４　機器の定期保守及び修理 (1) 情報システム管理者は、自治体可用性２以上のサーバ等の機器について、重要性に応じ定期保守を実施しなければならない。 (2)　　（略） ５　　（略） ６　情報システム室	第５　物理的セキュリティ対策 １　サーバ等の設置条件 (1)　　（略） (2) 情報システム管理者は、＿＿＿可用性２以上の情報を格納するサーバ、セキュリティサーバ、住民サービスに関するサーバ等重要なサーバ等を多重化し、同一データを複数保持しなければならない。 (3) 情報システム管理者は、＿＿＿可用性３の情報を格納しているサーバ等については、必要に応じ、移設できるように設置するものとする。 ２　電源 (1) ＿＿＿可用性２以上のサーバ等の機器については、電源の停止時に自動的にサーバ等を停止する機能を備えた予備電源を設置することとし、予備電源の容量は、当該機器を安全に停止するまでの間、十分に電力を供給することができるものとする。 (2)　　（略） ３　　（略） ４　機器の定期保守及び修理 (1) 情報システム管理者は、＿＿＿可用性２以上のサーバ等の機器について、重要性に応じ定期保守を実施しなければならない。 (2)　　（略） ５　　（略） ６　情報システム室

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
(1)～(8)（略）	(1)～(8)（略）
(9) 情報システム管理者は、自治体可用性３の情報資産に係るサーバ等については、耐震対策が講じられた建物に設置すること。	(9) 情報システム管理者は、自治体可用性３の情報資産に係るサーバ等については、耐震対策が講じられた建物に設置すること。
(10)　（略）	(10)　（略）
７　ネットワーク	７　ネットワーク
(1)　（略）	(1)　（略）
(2) 情報システム管理者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。	
(3) 情報システム管理者は、外部の場所とのネットワーク接続は必要最小限に限定し、かつ、できる限り接続ポイントを減らさなければならない。また、外部の場所とのネットワーク接続について CISO 補佐へ報告しなければならない。	(2) 情報システム管理者は、外部の場所とのネットワーク接続は必要最小限に限定し、かつ、できる限り接続ポイントを減らさなければならない。また、外部の場所とのネットワーク接続について CISO 補佐へ報告しなければならない。
(4) 情報システム管理者は、自治体機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。	(3) 情報システム管理者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。
(5) 情報システム管理者は、ネットワークに使用する回線について、伝送途中に情報の破壊、盗聴、改ざん、消去等が生じないよう、不正な通信の有無を監視する等の十分なセキュリティ対策を講じなければならない。	(4) 情報システム管理者は、ネットワークに使用する回線について、伝送途中に情報の破壊、盗聴、改ざん、消去等が生じないよう、十分なセキュリティ対策を講じなければならない。
(6) 情報システム管理者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めなければならない。また、必要なソフ	

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
トウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。	
(7) 情報システム管理者は、自治体可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。	(5) 情報システム管理者は、＿＿可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。
７～10　（略）	７～10　（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)～(3)（略）	(1)～(3)（略）
(4) 自治体可用性２以上である情報の処理を行う職員等は、ネットワークが長期に停止した場合を想定し、手作業での処理方法を参照できるよう準備しなければならない。	(4) ＿＿可用性２以上である情報の処理を行う職員等は、ネットワークが長期に停止した場合を想定し、手作業での処理方法を参照できるよう準備しなければならない。
(5)　（略）	(5)　（略）
(6)　端末の持ち出し及び外部における情報処理作業の制限	(6)　端末の持ち出し及び外部における情報処理作業の制限
ア　情報システム管理者は、所管の情報システムで使用する自治体機密性２以上、自治体可用性２以上又は自治体完全性２の情報資産を外部で使用又は処理する場合における安全管理措置を定めなければならない。	ア　情報システム管理者は、所管の情報システムで使用する＿＿機密性２以上、＿＿可用性２以上又は＿＿完全性２の情報資産を外部で使用又は処理する場合における安全管理措置を定めなければならない。
イ　CISO 補佐は、特定の情報システム以外で使用する自治体機密性２以上、自治体可用性２以上又は自治体完全性２の情報資産を外部で使用する場合における、安全管理措置を定めなければならない。	イ　CISO 補佐は、特定の情報システム以外で使用する＿＿機密性２以上、＿＿可用性２以上又は＿＿完全性２の情報資産を外部で使用する場合における、安全管理措置を定めなければならない。

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
ウ　（略） エ　職員等は、外部で情報処理作業を行う際、県が管理していない情報機器を用いる場合には、事前に情報セキュリティ管理者又は情報システム管理者の許可を得、かつ、該当する安全管理措置に関する規定を遵守しなければならない。また、自治体機密性３の情報資産については、秘密保守契約を結んだ業者によるもの以外、県が管理していない情報機器による情報処理を行ってはならない。 (7)～(12)（略） ２～４　（略） ５　教育及び訓練 (1)～(3)（略） (4) 情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し、統括情報セキュリティ責任者及び情報セキュリティ責任者に対して、報告しなければならない。 (5) CISO 補佐は、緊急時におけるセキュリティ対策について、すべての職員等及び関係者に周知しなければならない。また、必要に応じて、緊急時対応を想定した訓練を実施することとする。 (6) CISO 補佐は、新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。 (7) 情報セキュリティ管理者は、新規採用の職員等を対象に、業務上必要となる情報資産の取り扱いに関し、情報セキュリティ対策について事前に研修を実施しなければならない。	ウ　（略） エ　職員等は、外部で情報処理作業を行う際、県が管理していない情報機器を用いる場合には、事前に情報セキュリティ管理者又は情報システム管理者の許可を得、かつ、該当する安全管理措置に関する規定を遵守しなければならない。また、機密性３の情報資産については、秘密保守契約を結んだ業者によるもの以外、県が管理していない情報機器による情報処理を行ってはならない。 (7)～(12)（略） ２～４　（略） ５　教育及び訓練 (1)～(3)（略） (4) CISO 補佐は、緊急時におけるセキュリティ対策について、すべての職員等及び関係者に周知しなければならない。また、必要に応じて、緊急時対応を想定した訓練を実施することとする。 (5) CISO 補佐は、新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。 (6) 情報セキュリティ管理者は、新規採用の職員等を対象に、業務上必要となる情報資産の取り扱いに関し、情報セキュリティ対策について事前に研修を実施しなければならない。

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
(8) 研修は、各職員等それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。	(7) 研修は、各職員等それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。
(9) 幹部を含めたすべての職員等は、定められた研修及び訓練に参加しなければならない。	(8) 幹部を含めたすべての職員等は、定められた研修及び訓練に参加しなければならない。
(10) 情報システム管理者は、所管の情報システムが長期にわたり停止することを念頭に置き、手作業での処理方法を明示しておかなければならない。	(9) 情報システム管理者は、所管の情報システムが長期にわたり停止することを念頭に置き、手作業での処理方法を明示しておかなければならない。
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～ク　（略）	ア～ク　（略）
ケ　事案により、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告しなければならない。	
(2)～(3) （略）	(2)～(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) バックアップの実施	(2) バックアップの実施
ア　情報セキュリティ管理者又は情報システム管理者は、サーバ及び端末に記録された情報について、情報システムの多重化措置にかかわらず、その重要性に応じ、期間を設定し、定期的にバックアップを行うこととする。	情報セキュリティ管理者又は情報システム管理者は、サーバ及び端末に記録された情報について、情報システムの多重化措置にかかわらず、その重要性に応じ、期間を設定し、定期的にバックアップを行うこととする。
イ　情報システム管理者は、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。	

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
ウ　情報システム管理者は、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。	
(3)～(5)（略）	(3)～(5)（略）
(6) 持ち出した端末の取扱い	(6) 持ち出した端末の取扱い
情報セキュリティ管理者又は情報システム管理者は、執務室外に持ち出すことを前提に導入した端末については、盗難等の際に第三者により情報が窃取されることを防止するための端末のデータの暗号化、著しい回数認証に失敗した場合のデータの自動消去、自治体機密性２以上の情報は端末ではなくサーバ等に保存するなどの対策を講じなければならない。	情報セキュリティ管理者又は情報システム管理者は、執務室外に持ち出すことを前提に導入した端末については、盗難等の際に第三者により情報が窃取されることを防止するための端末のデータの暗号化、著しい回数認証に失敗した場合のデータの自動消去、機密性２以上の情報は端末ではなくサーバ等に保存するなどの対策を講じなければならない。
(7)～(8)（略）	(7)～(8)（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) 情報システム仕様書等の管理	(1) 情報システム仕様書等の管理
情報システム管理者は、ネットワーク構成図、情報システム仕様書、操作マニュアル等について、記録媒体にかかわらず、権限のない者が閲覧又は紛失することがないよう、適正に管理しなければならない。	情報システム管理者は、ネットワーク構成図、情報システム仕様書、操作マニュアル等について、記録媒体に関かかわらず、権限のない者が閲覧したり、紛失することがないよう、適正に管理しなければならない。
(2)　　（略）	(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　情報システム管理者は、所管する情報システムの設定又は構成の変更を行った場合は、その記録を残し、詐取、改ざん等をされないように適正に管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければな	ア　情報システム管理者は、所管する情報システムの設定又は構成の変更を行った場合は、その記録を残し、詐取、改ざん等をされないように適正に管理しなければな

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
らない。 イ～ウ（略） (4)～(5)（略） ３　アクセス制御等 (1) アクセス制御 情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスできる者を定め、アクセスする権限のない職員等がアクセスしないように必要最小限の範囲で適切に設定する等、システム上制限しなければならない。 (2) 無線 LAN のセキュリティ対策及びネットワークの盗聴対策 ア～ウ（略） (3) 外部ネットワークとのネットワーク間接続制限等 ア～ウ（略） エ 情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、次のセキュリティ対策を実施しなければならない。 (ｱ) 庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。 (ｲ) 脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用しなければならない。 (ｳ) ウェブサーバからの不用意な情報漏えいを防止するための措置を講じなければならない。 (ｴ) 情報システム管理者は、ウェブコンテンツの編集作業を行う主体を限定	らない。 イ～ウ（略） (4)～(5)（略） ３　アクセス制御等 (1) アクセス制御 情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスできる者を定め、アクセスする権限のない職員等がアクセスしないように、システム上制限しなければならない。 (2) 無線 LAN 及びネットワークの盗聴対策 ア～ウ（略） (3) 外部ネットワークとのネットワーク間接続制限等 ア～ウ（略）

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
しなければならない。 オ　情報システム管理者は、外部の場所から県のネットワーク及び情報システムにアクセスする場合は、ファイアウォールなどの、アクセス制御可能な装置を介することとし、直接県のネットワークに接続できない措置を講じなければならない。 カ　情報システム管理者は、通信の手順や方式（プロトコル）は、業務上必要最小限のものに限定する。 キ　情報システム管理者は、利用者の真正性が確保できるよう、必要な措置を講じなければならない。 ク　情報システム管理者は、接続した相手先のセキュリティに問題が認められ、県の情報資産に脅威が生じることが想定される場合には、CISO 補佐の判断に従い、速やかに当該外部ネットワークとの接続を切断しなければならない。 (4)　　（略） (5) 情報システム間の接続制御及び経路制御並びに停止の連絡 ア～ウ（略） エ　情報システム管理者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保しなければならない。また、情報セキュリティ対策について、定期的な確認により見直さなければならない。 (6)～(7)（略） ４　電子メール、クラウドサービス等の管理	エ　情報システム管理者は、外部の場所から県のネットワーク及び情報システムにアクセスする場合は、ファイアウォールなどの、アクセス制御可能な装置を介することとし、直接県のネットワークに接続できない措置を講じなければならない。 オ　情報システム管理者は、通信の手順や方式（プロトコル）は、業務上必要最小限のものに限定する。 カ　情報システム管理者は、利用者の真正性が確保できるよう、必要な措置を講じなければならない。 キ　情報システム管理者は、接続した相手先のセキュリティに問題が認められ、県の情報資産に脅威が生じることが想定される場合には、CISO 補佐の判断に従い、速やかに当該外部ネットワークとの接続を切断しなければならない。 (4)　　（略） (5) 情報システム間の接続制御及び経路制御並びに停止の連絡 ア～ウ（略） (6)～(7)（略） ４　電子メール、クラウドサービス等の管理

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
(1)　　（略）	(1)　　（略）
(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、自治体機密性２以上又は自治体完全性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、パスワード等による暗号化等を行わなければならない。
ケ　職員等は、電子メール等で自治体可用性２以上の電子データを送信する場合は、送信先へ着信したことを確認しなければならない。	ケ　職員等は、電子メール等で＿＿＿可用性２以上の電子データを送信する場合は、送信先へ着信したことを確認しなければならない。
５　ソーシャルメディアサービスの利用	５　ソーシャルメディアサービスの利用
(1)　　（略）	(1)　　（略）
(2) 自治体機密性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。	(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)～(4)（略）	(3)～(4)（略）
(5) 自治体可用性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。	(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	６　ユーザ ID の管理
(1) 情報システム管理者によるユーザ ID の管理	(1) 情報システム管理者によるユーザ ID の管理
情報システム管理者は、ユーザ ID の管理に関し、以下の事項を遵守しなければならない。	情報システム管理者は、ユーザ ID の管理に関し、以下の事項を遵守しなければならない。
ア～オ（略）	ア～オ（略）
カ　利用者に不要なアクセス権限が付与されていないか定期的に確認すること。	＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
キ　上記に掲げるほか、利用者の登録、変更、抹消等の情報管理、職員等の異動、派遣、退職に伴うユーザ ID の取扱いの方法を定めること。	カ　上記に掲げるほか、利用者の登録、変更、抹消等の情報管理、職員等の異動、派遣、退職に伴うユーザ ID の取扱いの方法を定めること。
(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　（略）	ア　（略）
イ　情報システム管理者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じなければならない。	
ウ　情報システム管理者は、特権を付与された ID 及びパスワードについて、人事異動の際のパスワードの変更、入力回数制限等によりセキュリティ対策を強化しなければならない。	イ　情報システム管理者は、特権を付与された ID 及びパスワードについて、職員等の端末等のパスワードと比較して必要に応じて適宜変更するとともに、入力回数制限等によりセキュリティ対策を強化しなければならない。
エ　情報システム管理者は、特権を付与された ID による情報システムへの接続は、必要最小限の接続時間に制限しなければならない。	ウ　情報システム管理者は、特権を付与された ID による情報システムへの接続は、必要最小限の接続時間に制限しなければならない。
オ　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。
カ　情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。	オ　情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。
(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
職員等は、自己の保有するパスワードに関し、次の事項を遵守しなければならない。	職員等は、自己の保有するパスワードに関し、次の事項を遵守しなければならない。

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
ア～カ（略）	ア～カ（略）
キ　サーバ、ネットワーク機器及び端末に、パスワードを記憶させないこと。パスワードを記憶させることで、パスワードの入力なしに認証を可能とする設定は行ってはならないこと。	キ　サーバ、ネットワーク機器及び端末に　パスワードを記憶させないこと。
ク　　（略）	ク　　（略）
(5)～(6)（略）	(5)～(6)（略）
７　情報システムの調達及び保守等	７　情報システムの調達及び保守等
(1) 機器等の調達に係る運用規程の整備	
ア　情報システム管理者は、機器等の選定基準を運用規程として整備しなければならない。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられないような対策を講じなければならない。	
イ　情報システム管理者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備しなければならない。	
(2) 機器等及び情報システムの調達	(1)　　情報システムの調達
ア　情報システム管理者は、情報システムの開発、導入、保守等に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。	ア　情報システム管理者は、情報システムの開発、導入、保守等に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。
イ～オ（略）	イ～オ（略）
(3) 情報システムの開発	(2) 情報システムの開発

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
ア～ウ（略）	ア～ウ（略）
エ　情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定し、それ以外のものを利用させてはならない。	エ　情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定し、それ以外のものを利用させてはなければならない。
オ　　（略）	オ　　（略）
カ　情報システム管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。	
(4) 情報システムの導入	(3) 情報システムの導入
ア～カ（略）	ア～カ（略）
キ　情報システム管理者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない。	
ク　情報システム管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。	
ケ　情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。	
(5) システム開発保守に関連する資料等の保管	(4) システム開発保守に関連する資料等の保管
ア　　（略）	ア　　（略）

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
イ　情報システム管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ責任者に報告しなければならない。 ウ　情報システム管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、次の全て含む実施手順を整備しなければならない。 (ｱ)情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順 (ｲ)情報セキュリティインシデントを認知した際の対処手順 (ｳ)情報システムが停止した際の復旧手順 エ　情報システム管理者は、テスト結果を一定期間保管しなければならない。 オ　情報システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。 (6) 情報システムにおける入出力データの正確性の確保 ア　　（略） イ　情報システム管理者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。 (ｱ)　利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直ししなければならない。 (ｲ)　運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。 (ｳ)　ウェブアプリケーションやウェブコンテンツにおいて、故意又は過失に	イ　情報システム管理者は、テスト結果を一定期間保管しなければならない。 ウ　情報システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。 (5) 情報システムにおける入出力データの正確性の確保 ア　　（略） イ　情報システム管理者は、 故意又は過失に

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
より情報が改ざんされ又は漏えいさせられるおそれがある場合、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。	より情報が改ざんされ又は漏えいさせられるおそれがある場合、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。
ウ　　（略）	ウ　　（略）
(7) 情報システムの変更管理 情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。	(6) 情報システムの変更管理 情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。
(8) ソフトウェアの更新等 情報システム管理者は、ソフトウェアの修正及び更新に際しては、不具合及び他のシステムとの不整合の有無を事前に確認しなければならない。	(7) ソフトウェアの更新等 情報システム管理者は、ソフトウェアの修正及び更新に際しては、不具合及び他のシステムとの不整合の有無を事前に確認しなければならない。
(9) システム更新又は統合時の検証等 情報システム管理者は、システムの更新又は統合に伴うリスク管理体制の構築、移行基準の明確化及び更新又は統合後の業務運営体制の検証を行わなければならない。	(8) システム更新又は統合時の検証等 情報システム管理者は、システムの更新又は統合に伴うリスク管理体制の構築、移行基準の明確化及び更新又は統合後の業務運営体制の検証を行わなければならない。
(10) 情報システムについての対策の見直し 情報システム管理者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。	
８～９　（略）	８～９（略）
10　セキュリティ情報の収集	10　セキュリティ情報の収集
(1) 情報システム管理者は、不正プログラム、サーバ装置、端末及び通信回線装置等におけるセキュリティホールに関する情報、ソフトウェアの更新等セキュリティに関する情報の収集に努め、所管する情報システムについて、緊	(1) 情報システム管理者は、不正プログラム、　　セキュリティホールに関する情報、ソフトウェアの更新等セキュリティに関する情報の収集に努め、所管する情報システムについて、緊

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
急度に応じて、セキュリティ対策計画を作成し、これに基づいてセキュリティ対策上適正な措置を講じなければならない。 (2)　　(略) 第８　運用におけるセキュリティ対策 １　情報システムの運用・保守時の対策 (1) 情報システム管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。 (2) 情報システム管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。 (3)情報システム管理者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。 ２　情報システムの監視機能 (1)情報システム管理者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。 (2)情報システム管理者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。 (3)情報システム管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。 (4)情報システム管理者は、サーバ装置上での情報セキュリティインシデント	急度に応じて、セキュリティ対策計画を作成し、これに基づいてセキュリティ対策上適正な措置を講じなければならない。 (2)　(略) 第８　運用におけるセキュリティ対策

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
の発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。	
3　情報システムの監視	1　情報システムの監視
(1)～(3)　(略)	(1)～(3)　(略)
4　情報セキュリティポリシーの遵守状況の確認	2　情報セキュリティポリシーの遵守状況の確認
(1)～(5)　(略)	(1)～(5)　(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)～(3)　(略)	(1)～(3)　(略)
(4) 情報システム管理者は、自治体可用性３の情報システムにあっては、自然災害等により情報システム、電源及びネットワークが被災した場合並びに情報システム担当者及び委託事業者が被災して、活動できない場合に備えて、所管の情報システムに係る業務継続計画を定めなければならない。	(4) 情報システム管理者は、　可用性３の情報システムにあっては、自然災害等により情報システム、電源及びネットワークが被災した場合並びに情報システム担当者及び委託事業者が被災して、活動できない場合に備えて、所管の情報システムに係る業務継続計画を定めなければならない。
２～６　(略)	２～６　(略)
第10　業務委託とクラウド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	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　業務委託
(1) 委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）	
ア　情報システム管理者は、業務委託を許可（又は禁止）する業務の範囲（委	

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
託事業者に開示できない情報を取り扱う業務は業務委託不可等）を明確にしなければならない。 イ　情報システム管理者は、業務委託への提供を許可（又は禁止）する情報の範囲（委託業務に関係しない情報は提供不可等）を明確にしなければならない。 ウ　情報システム管理者は、情報資産の分類及び取扱制限その他提供する情報の特性に応じた、情報の取扱いを許可（又は禁止）する場所（自治体機密性３情報は要管理対策区域外での取扱いを禁止するなど）を明確にしなければならない。	
(2) 委託先の選定基準 情報システム管理者は、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。	(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。
(3) 業務委託実施前の対策 ア　情報システム管理者は、業務委託の実施までに、次の全て含む事項を実施しなければならない。 (ｱ)　委託する業務内容の特定 (ｲ)　委託事業者の選定条件を含む仕様の策定 (ｳ)　仕様に基づく委託事業者の選定 (ｴ)　情報セキュリティ要件を明記した契約の締結（委託における契約項目）	(2) 業務委託実施前の対策 委託における契約項目

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
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。	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。
a　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守	ア　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
b　個人情報漏えい防止のための技術的安全管理措置に関する取り決め	
c　委託先の責任者、委託内容、作業者の所属及び作業場所の特定	イ　委託先の責任者、委託内容、作業者の所属及び作業場所の特定
d　提供されるサービスレベルの保証	ウ　提供されるサービスレベルの保証
e　従業員に対する教育の実施	エ　従業員に対する教育の実施
f　提供された情報の目的外利用及び受託者以外の者への提供の禁止	オ　提供された情報の目的外利用及び受託者以外の者への提供の禁止
g　業務上知り得た情報の守秘義務	カ　業務上知り得た情報の守秘義務
h　再委託に関する制限事項の遵守	キ　再委託に関する制限事項の遵守
i　委託業務終了時の情報資産の返還、廃棄等	ク　委託業務終了時の情報資産の返還、廃棄等
j　委託業務の定期報告及び緊急時報告義務	ケ　委託業務の定期報告及び緊急時報告義務
k　県による監査又は検査	コ　県による監査又は検査
l　県による事案の公表	サ　県による事案の公表
m　情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)	シ　情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)
n　自治体可用性２以上のシステムに係る災害時及び原子力発電所事故時の対応	ス　＿＿＿可用性２以上のシステムに係る災害時及び原子力発電所事故時の対応
o　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	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
p　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	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
q　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	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

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
r　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	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
s　入力又は保存された情報は、削除することが可能か	ツ　入力又は保存された情報は、削除することが可能か
(ｵ)　委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）の締結 情報システム管理者は、業務委託の実施までに、委託の前提条件として、次の全て含む事項の実施を委託事業者に求めなければならない。	
a　仕様に準拠した提案	
b　契約の締結	
c　委託事業者において重要情報を取り扱う場合は、秘密保持契約（NDA）の締結	
(3) 業務委託実施期間中の対策	
ア　情報システム管理者は、業務委託の実施期間において、次の全て含む対策を実施しなければならない。	
(ｱ)　委託判断基準に従った重要情報の提供	
(ｲ)　契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施	
(ｳ)　統括情報セキュリティ責任者へ措置内容の報告(重要度に応じてCISO に報告)	
(ｴ)　委託した業務において、事案の発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求	
	(3)委託における確認、措置等

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
	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、クラウドサービスくを利用する場合は、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。
イ　情報システム管理者は、業務委託の実施期間において、次の全て含む対策の実施を委託事業者に求めなければならない。 (ｱ)　情報の適正な取扱いのための情報セキュリティ対策 (ｲ)　契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告 (ｳ)　委託した業務において、事案の発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処	
(4) 業務委託終了時の対策 ア　情報システム管理者は、業務委託の終了に際して、次の全て含む対策を実施しなければならない。 (ｱ)　業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収 (ｲ)　委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認	
イ　情報システム管理者は、業務委託の終了に際して、次の全て含む対策の実施を委託事業者に求めなければならない。	

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
(ｱ)　業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検	
(ｲ)　提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消	
2　情報システムに関する業務委託	
(1)　情報システムに関する業務委託における共通的対策	
情報システム管理者は、情報システムに関する業務委託の実施までに、情報システムに意図しない変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。	
(2)　情報システムの構築を業務委託する場合の対策	
情報システム管理者は、情報システムの構築を業務委託する場合は、契約に基づき、次の全て含む対策の実施を委託事業者に求めなければならない。	
ア　情報システムのセキュリティ要件の適切な実装	
イ　情報セキュリティの観点に基づく試験の実施	
ウ　情報システムの開発環境及び開発工程における情報セキュリティ対策	
(3)　情報システムの運用・保守を業務委託する場合の対策	
ア　情報システム管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。	
イ　情報システム管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に	

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
基づき、委託事業者に速やかな報告を求めなければならない。	
(4)　情報システムの一部の機能を提供するサービスを利用する場合の対策	
ア　情報システム管理者は、外部の一般の者が重要情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。	
イ　情報システム管理者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。	
ウ　情報システム管理者は、委託事業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。	
エ　情報システム管理者は業務委託サービスを利用する場合には、統括情報セキュリティ責任者又は情報セキュリティ責任者へ当該サービスの利用申請を行わなければならない。	
オ　情報システム管理者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。	
カ　情報システム管理者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。	
３　　クラウドサービスの利用（自治体機密性２以上の情報を取り扱う場合）	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) 約款のみによる外部サービス（クラウドサービス、以下「クラウドサービ	(1) 約款　による外部サービス

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
ス」という。）を利用し　てはならない。	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) 自治体機密性３Ａに相当する情報（「政府機関等のサイバーセキュリティ対策のための統一基準」（令和５年度版）の機密性３情報に相当）については、クラウドサービスで取り扱ってはならない	
(3)　クラウドサービスの選定	(2) 外部サービス　の選定
ア　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、次の判断基準に従って、業務に係る影響度等を検討した上で　クラウドサービスの利用を検討しなければならない。	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、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)　クラウドサービスを利用する目的の明確化	ア　外部サービス　を利用する目的の明確化
(ｲ)　クラウドサービスを利用する業務範囲の明確化	イ　外部サービス　を利用する業務範囲の明確化
(ｳ)　クラウドサービスを利用する際におけるリスク対策	ウ　外部サービス　を利用する際におけるリスク対策
a　クラウド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	(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
b　利用者が、利用するクラウド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	(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
c　クラウド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	(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
d　クラウド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	(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

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
によるカントリーリスク	によるカントリーリスク
e　（略）	(オ)　（略）
(エ)　クラウド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	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
イ　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）で定めることが出来るクラウドサービス提供者を選定しなければならない。	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、クラウド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。国内のクラウドサービスにおいて、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	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)　クラウド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	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)　クラウド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	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自治体可用性に関する事項をサービスレベル契約（SLA）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)　クラウドサービス提供者が、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	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)　クラウドサービス提供者における情報セキュリティ対策の	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

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
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	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)　クラウド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	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、クラウド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（SLA）に定める	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（SLA）に定める
(ｹ)脅威に対するクラウドサービス提供者の情報セキュリティ対策（なりすまし、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	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（なりすまし、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	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)　クラウド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	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
ウ　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クラウドサービス提供者の選定条件に含めなければならない。	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)　クラウド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	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

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
(ｲ)　クラウド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	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)　クラウドサービスの提供に当たり、クラウド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	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)　クラウドサービス提供者の資本関係・役員等の情報、クラウド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ンの指定	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	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	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	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
エ　情報セキュリティ管理者は、クラウド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、クラウドサービス提供者の選定条件に含めなければならない。	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。
オ　情報セキュリティ管理者は、クラウド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クラウド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	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	イ　サービスレベルの保証
カ　情報セキュリティ管理者は、クラウド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	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

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
評価してクラウド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。	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。
キ　情報セキュリティ管理者は、クラウド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、クラウドサービス提供者の選定条件で求める内容をクラウド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、クラウドサービス提供者の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。
ク　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、クラウドサービスを選定しなければならない。また、クラウド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 又は ISMAP-LIU（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。）ただし ISMAP 又は ISMAP-LIU クラウドサービスリストのサービスであっても、そのサービスの「言明対象範囲」、「基本言明要件のうち実施している統制目標の管理策」で安全性を確認する必要がある。	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、外部サービス提供者を選定しなければならない。また、外部サービス提供者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。）
ケ　情報セキュリティ管理者は、クラウドサービスの特性を考慮	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

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
した上で、クラウド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。	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。
コ　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、クラウド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。	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。
(4)　クラウドサービスの利用に係る調達・契約	(3)　外部サービスの利用に係る調達・契約
ア　情報セキュリティ管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウド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。	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。
イ　情報セキュリティ管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約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、調達仕様の内容を契約に含めなければならない。
(5)　クラウドサービスの利用承認	(4)　外部サービスの利用承認
ア　情報セキュリティ管理者は、クラウド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。	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。
イ　情報セキュリティ管理者（総括担当）は、クラウドサービス	②　情報セキュリティ管理者（総括担当）は、外部サービス

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
の利用を許可した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名しなければならない。	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。
(6) クラウドサービスを利用した情報システムの導入・構築時の対策	(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
ア　情報セキュリティ管理者又は情報システム管理者は、クラウド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。	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	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	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	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	エ　設計・設定時の誤りの防止
イ　クラウドサービス管理者は、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。	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。
(7) クラウドサービスを利用した情報システムの運用・保守時の対策	(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
ア　情報セキュリティ管理者又は情報システム管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウド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。	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)　クラウドサービス利用に必要な教育	ア　外部サービス利用に必要な教育
(ｲ)　取り扱う資産の管理	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	ウ　不正アクセスを防止するためのアクセス制御

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
(ｴ)　取り扱う情報の機密性保護のための暗号化	エ　取り扱う情報の機密性保護のための暗号化
(ｵ)　クラウドサービス内の通信の制御	オ　外部サービス内の通信の制御
(ｶ)　（略）	カ　（略）
(ｷ)　クラウドサービスを利用した情報システムの事業継続	キ　外部サービスを利用した情報システムの事業継続
イ　情報セキュリティ管理者又は情報システム管理者は、クラウド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。	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。
ウ　クラウドサービス管理者は、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。	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。
(8)　クラウドサービスを利用した情報システムの更改・廃棄時の対策	(8)　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
ア　情報セキュリティ管理者又は情報システム管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウド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。	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)　クラウドサービスで取り扱った情報の廃棄	ア　外部サービスで取り扱った情報の廃棄
(ｲ)　クラウドサービスの利用のために作成したアカウントの廃棄	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
イ　クラウドサービス管理者は、前項において定める規定に対し、クラウド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。	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。
4　クラウドサービスの利用（自治体機密性２以上の情報を取り	3　外部サービスの利用（機密性２以上の情報を取り

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
扱わない場合） (1)　クラウドサービスの利用における対策の実施 ア　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の許可を得なければならない。 イ　情報セキュリティ管理者は、クラウドサービスの利用を許可した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名しなければならない。 ウ　承認時に指名されたクラウドサービス管理者は、当該クラウド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　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　（略） 第 12　（略） 第 13　評価	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。 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） 第 11　（略） 第 12　（略） 第 13　評価

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
１　監査 (1) 情報セキュリティ監査統括責任者は、ネットワーク及び情報システムの情報資産における情報セキュリティ対策の実施状況について、毎年度及び必要に応じて、監査実施計画を立案し、監査を実施しなければならない。 (2)～(4)　　(略) (5) 情報セキュリティ監査統括責任者は、被監査部門が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)～(7)　　(略) (8) CISO は、監査の結果、指摘事項があった場合、CISO 補佐及び指摘事項を所管する情報セキュリティ管理者又は情報システム管理者に対し、当該事項への対処を指示しなければならない。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。 (9)　CISO は、所管外の情報セキュリティ管理者及び情報システム管理者に対しても、同種の課題及び問題点の有無を確認させなければならない。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。 (10) 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。 ２　　(略) 第 14　　(略)	１　監査 (1) 情報セキュリティ監査統括責任者は、ネットワーク及び情報システムの情報資産における情報セキュリティ対策の実施状況について、毎年度、監査実施計画を立案し、監査を実施しなければならない。 (2)～(4)　　(略) (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。 (6)～(7)　　(略) (8) CISO は、監査の結果、指摘事項があった場合、CISO 補佐及び指摘事項を所管する情報セキュリティ管理者又は情報システム管理者に対し、当該事項への対処を指示しなければならない。また、 所管外の情報セキュリティ管理者及び情報システム管理者に対しても、同種の課題及び問題点の有無を確認させなければならない。 (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。 ２　　(略) 第 14　　(略)

資料４－２

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 15　（略）	第 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、令和７年〇月〇日から施行する。	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。 附　則 この対策基準は、令和５年６月５日から施行する。

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
別紙１　　（略）	別紙１　　（略）

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新	旧
別紙２ 機密性による情報資産の分類	別紙２ 機密性による情報資産の分類

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新

分類	分類基準	情報資産＜例＞	取扱制限
自治体機密性３A	「行政文書の管理に関するガイドライン」（平成23年４月１日内閣総理大臣決定）に定める秘密文書に相当するもの	・極秘文書：秘密保全の必要が高く、その漏えいが国の安全、利益に損害を与えるおそれのある情報を含む行政文書 ・秘文書：極秘文書に次ぐ程度の秘密であって、関係者以外には知らせてはならない情報を含む極秘文書以外の行政文書	・県が管理する端末以外での作業の原則禁止 ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の記録媒体の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・記録媒体の施錠可能な場所への保管
自治体機密性３B	漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべきもの	・データベースや台帳形式になった住民情報を含む個人情報ファイル及びこれに準ずる情報	
自治体機密性３C	自治体機密性３B以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべきもの	・職員としての属性に基づく個人情報 ・オンライン申請の処理等により、システム処理上一時的にインターネット上に保管されるデータ ・文書管理システムの決裁文書として保存されている個人情報 ・施設設計情報や入札予定価格など非公開情報	
自治体機密性２	自治体機密性３A～C以外の情報資産のうち、直ちに一般に公表することを前提としていないもの	・政策検討に関する情報	
自治体機密性１	自治体機密性２又は自治体機密性３A～C以外のもの	・将来公表する予定の文書（白書の案等） ・公表された情報	

完全性による情報資産の分類

旧

分類	分類基準		取扱制限
機密性３	個人情報を含むもの又は秘密の取扱いを必要とするもの		・県が管理する端末以外での作業の原則禁止 ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の記録媒体の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・記録媒体の施錠可能な場所への保管
機密性２	機密性３以外の情報資産のうち、直ちに一般に公表することを前提としていないもの		
機密性１	機密性２又は機密性３以外のもの		

完全性による情報資産の分類

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新

分類	分類基準	取扱制限
自治体完全性２	改ざん、誤びゅう又は破損により、個人の権利が侵害され、又は行政事務の的確な遂行に支障（軽微なものを除く）を及ぼすおそれがあるもの	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・記録媒体の施錠可能な場所への保管
自治体完全性１	自治体完全性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）	

可用性による情報資産の分類

旧

分類	分類基準	取扱制限
完全性２	改ざん、誤びゅう又は破損により、個人の権利が侵害され、又は行政事務の的確な遂行に支障（軽微なものを除く）を及ぼすおそれがあるもの	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・記録媒体の施錠可能な場所への保管
完全性１	完全性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）	

可用性による情報資産の分類

資料４－２

福島県情報セキュリティポリシー改正　新旧対照表

新

分類	分類基準	取扱制限
自治体可用性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
自治体可用性２	自治体可用性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	
自治体可用性１	自治体可用性２又は自治体可用性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

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）	