資料1-1

「情報セキュリティポリシーガイドライン」の主要論点の改定案

2014年12月16日

総務省
MIC Ministry of Internal Affairs and Communications

議論テーマと内容要約

論点	議論テーマ	論点内容要約	論点整理票の項番※
①	外部委託（クラウドサービス等）	クラウドサービスを利用する場合の、サービス提供事業者の選定に係る要件について	26、40、63
②	外部委託（サプライチェーン・リスク）	ICTサービスを提供する委託先事業者のサプライチェーンに対するセキュリティ要件の整理と合意、調達品の保証について	61、62
③	外部委託（委託先管理）	再委託先を含めた委託先全体のセキュリティ管理について	65
④	ネットワークの利用（公衆通信網の利用）	無線LANによる庁外からのアクセス時のセキュリティ担保について（テレワーク含む）	18、21、25
⑤	支給以外のスマートデバイス等の業務利用	私物の端末を業務利用する場合の、利用条件の明確化	14
⑥	SMSの業務利用	SMSを業務で利用し、情報発信を行う場合のリスクとセキュリティ対策について	15
⑦	情報セキュリティインシデント対策体制の強化	情報セキュリティに関する統一的な窓口機能（CSIRT）の設置と地方公共団体での役割について	8、10、22、42、49、58

※凡例：赤数字＝管理強化、青数字＝明確化

議論テーマについてのご意見

論点	論点テーマ	ご意見
①	外部委託（クラウドサービス等）	・住民情報等の基幹系のデータがプライベートクラウド、それ以外のデータについてはパブリッククラウドというイメージであれば、両者を分けて考えた方がよい。 ・クラウドの利用においては、第三者による外部監査を受けている、など何らかの監査を実施していれば利用してもよい、とすることが必要ではないか。 ・クラウドはコントロールできないことを明記し、クラウドサービスを利用する場合のファシリティ面や運用面での選定要件(SLA)を書くべき。J-LISの非機能要求グレードを引用するとよい。 ・非機能要求グレードの引用は、「3.6.3. システム開発、導入、保守等」と「3.8.1. 外部委託」の両方に記載すべき。
②	外部委託（サプライチェーン・リスク）	・ここでの論点はICT製品に他の供給者から購入した好ましくない機能を内在した構成部品が含まれるリスクであり、開発や運用における再委託のセキュリティ体制確保とは分けて整理する必要がある。 ・開発や運用（クラウドサービスの提供含む）における再委託は、現状の改定案の通り、府省庁ガイドラインやクラウドサービス提供におけるガイドラインに基づいた再委託先の情報セキュリティの確保になると思うが、ICT製品のサプライチェーンリスクは「ISO27001：2013　A15.1.3 ICTサプライチェーン」の記載内容を元に自治体向けに書き直すのがよいと思われる。 ・本論点は抜けの無いよう記述すべきだが、実際の運用でできることには配慮する必要がある。供給者に厳しい要求をした結果、コストに跳ね返ってくることが考えられる。現実的に自治体が対応できる事は、調達仕様書にて供給者側に保証させる事等になると思われるが、国の調達基準等を参考にガイドラインに例示できるようにすると良い。

議論テーマについてのご意見

論点	論点テーマ	ご意見
②	外部委託（サプライチェーン・リスク）	・調達を要求する範囲を決めたり、調達仕様書に盛り込むべき委託先への要求事項を提案してはどうか。 ・改訂案の記載内容では自治体職員がサプライチェーンリスクを理解できない恐れがある。オープンソース等、事業者の部品導入時点で組み込まれたものまで、自治体職員がコントロールすることは困難なため、事業者から調達時点でチェックリストを用い確認することが現実的と思われる。J－LISの非機能要求グレード（地方公共団体版）活用シートが使えるのではないか。 ・「3.8.1. 外部委託」の（解説）（2）契約項目の説明の後の「・」による箇条書き、「〇番号」による箇条書き部分がつながって記載されており分かりにくい。
③	外部委託（委託先管理）	・外部委託する際には、個人情報保護に関わる条例も適用されることを特記事項に記載するべきである。
④	ネットワークの利用（公衆通信網の利用）	・状況に応じた条件が明記できるとよいのではないか。 （どのレベルであれば専用回線でなくても良いのか等） ・庁内ネットワークの無線LANと公衆無線LANを分けて記載すべき。なお、本ガイドラインは、自治体職員や職員が利用する情報システムが対象であり、住民サービス向上目的の公衆無線LANは対象外ではないか。 ・ここの論点は外部からのアクセスであり、無線LANにのみ言及するのではなく、公衆通信網として扱うべき。ただし、外部からのアクセスを許可する場合でも、基幹系システムへのアクセスは不可とすべき。

議論テーマについてのご意見

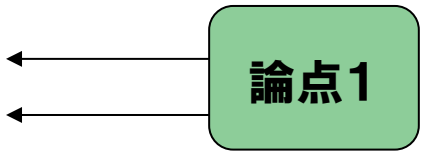
論点	論点テーマ	ご意見
⑤	支給以外のスマートデバイス等の業務利用	・私物でのアクセスを認めるのであれば利用を認める条件を提示し、条件を満たせば使えるようにするのが良いのでは。 ・職員なら誰でも利用できるのは問題と考える。リテラシーのある人のみ使えるなどの制限が必要ではないか。 ・事務フロアは私物の持ち込OKだが、マシン室には持ち込めない、撮影もできないというような範囲制限をかけたルール作りが必要。 ・基幹業務の仕方、情報の流し方等含めて検討する必要あり。 ・支給品以外は管理ができないため原則禁止とすべき。 ・学校の先生は自宅での作業を認めざるを得ない場合があり、適切な対策を実施した外部アクセスを認める配慮が必要。 ・支給品以外の端末の利用を許可する判断基準も解説に必用。 ・モバイル端末という表現は通信機能を持つイメージがあり、言葉の整理が必要。
⑥	SMSの業務利用	・SMS利用時は、ルールを定め、職員の啓発を行うことが必要。 ・解説の修正案に「以下の対策が考えられる」等の記載を追記した方が分かりやすい。

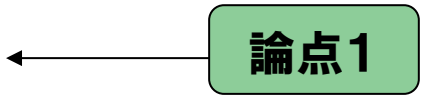
議論テーマについてのご意見

論点	論点テーマ	ご意見
⑦	情報セキュリティインシデント対策体制の強化	・CSIRTの定義をしっかりする必要がある −有事の際の窓口 −対処の指示を出す −CISOに報告する　など ・以下のような役割が考えられる −CIO：総務 −CISO：号令したり、謝罪したりする人 −CSIRT：何かあったら調査してCISOに報告する ・CSIRTの在り方は組織によってまちまちなところがある。自治体向けには国に合わせて、主に窓口業務を行う旨（コミュニケーションの核となる最低限の機能）を記載し、将来的には分析業務も含めることが望ましいという程度の記載が良いのではないか。 ・CSIRTという表現は今回のガイドラインの改訂には明記すべきであり、明記することにより、自治体でも考える機会になり、要員の育成等、対応が広がっていく事を期待したい。 ・インシデントが起きた場合の各部署への速やかな対応と再発防止がポイントで、組織として存在しなくとも機能があることが大切。 ・改定案の「統一的な窓口機能」であれば小規模団体でも実現可能と思われるが、それ以上の機能となると小規模団体では形骸化する恐れがある。県レベルでの指導、補助等が必要と思われる。

① 外部委託（クラウドサービス等）

※論点整理表：
項番26、40、63





※凡例：赤数字＝管理強化、青数字＝明確化

① 外部委託（クラウドサービス等）

論点整理表：
項番26、40、63

現状ガイドライン

- 外部委託の考え方は、人や物や作業のアウトソーシングが中心であり、クラウドサービスのような外部サービス利用の概念が弱かった

ガイドライン改定観点

- 情報システムやサービスの可用性が確保されていることを確認したうえで導入することを追記。

①（項番26）

（3.6.1 コンピュータ及びネットワークの管理）

NISC等の考え方	【クラウドサービスの提供における情報セキュリティ対策ガイドライン:13.1.4 仮想ネットワークにおいて重視すべき脆弱性】 【利用者接点とサプライチェーンにおける実務のポイント】 ● 仮想ネットワークを構築してクラウドサービスを提供する場合には、仮想ネットワークの管理ミスを防止し、オンプレミスから移行するクラウド利用者に対する移行中の悪意の攻撃にも留意するため、実務上以下を実施する必要がある。 (a) クラウドサービスの提供に当たり、仮想ネットワークを新たに構築する場合は、物理ネットワーク構成との対応関係が明確になるように仮想ネットワークを構成すること。 (b) 仮想ネットワークの運用設定方針と設定承認方針を、物理ネットワークの運用経験とノウハウに基づいて実施しやすい形で定義し、文書化すること (c) PaaS/IaaSを提供している場合は、クラウド利用者の構内設備をクラウドサービスに移行させる際に、仮想/物理ネットワークの再構成、移行、試験運用のプロセスで悪意の攻撃を受けないように、クラウド利用者にセキュリティ管理の徹底を助言すること

①（項番26）（資料1-3：P65）

改定案（3.6.1 コンピュータ及びネットワークの管理）（解説）

＜修正前＞

（解説）

（1） 文書サーバの設定等

文書サーバは、複数の課室等で共用している場合が多いため、職員等が利用可能な容量を取り決める必要がある。また複数の課室等で利用している場合には、アクセス制御を行う必要がある。

（中略）

（7） 障害記録

システム障害への対応を決める際、過去に起きた類似障害が参考になるので、障害記録を適切に保存しておく必要がある。

（注５）障害記録のデータベース化を図るなど、障害対応を決める場合に活用できるように保管しておくことが重要である。

（8） ネットワークの接続制御、経路制御等

ネットワーク上では、フィルタリング、ルーティング、侵入検知システム等が機能しているが、これらの機能を十分活用するため、ハードウェア及びソフトウェアの設定を適切に行うよう注意する必要がある。また、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

（9） 外部の者が利用できるシステムの分離等

電子申請受付システム、庁舎を訪問した住民等に対する庁舎案内システムなど、外部の人々が利用できるシステムは、不正アクセス等を防御するため、必要に応じ、他のシステムのネットワークと切り離すなどの措置が必要である。

（10） 外部ネットワークとの接続制限等

＜修正後＞

（7） 障害記録

システム障害への対応を決める際、過去に起きた類似障害が参考になるので、障害記録を適切に保存しておく必要がある。

（注５）障害記録のデータベース化を図るなど、障害対応を決める場合に活用できるように保管しておくことが重要である。

（8） ネットワークの接続制御、経路制御等

ネットワーク上では、フィルタリング、ルーティング、侵入検知システム等が機能しているが、これらの機能を十分活用するため、ハードウェア及びソフトウェアの設定を適切に行うよう注意する必要がある。また、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

なお、クラウドサービスを利用し、住民情報等の重要な情報を外部のデータセンターとやり取りする場合は、高度なセキュリティ対策を行う必要がある。さらに仮想ネットワークを構築する場合には、仮想ネットワークと物理ネットワークとの対応関係、仮想ネットワークの運用設定方針と設定承認方針及び庁内設備をクラウドサービスに移行する場合の注意事項等について確認し、適切な対策を実施する必要がある。

①（項番40）

（ 3.6.3 システム開発、導入、保守）

NISC等の考え方	【クラウドサービス提供における情報セキュリティ対策ガイドライン: 17.1.2 情報処理施設の可用性】 情報処理施設の可用性を保証するためには、情報処理施設の十分な冗長性を確保した上で、障害時には運用系から冗長系への切替を確実に行うことが求められる。運用系から冗長系への切替を確実にするためには、切替が意図通りに動作することを定期的に確認することが望ましい。 さらに、クラウドサービスの提供にあたっては、実務上以下を実施することが望ましい。 (c)情報処理施設やネットワークにおいて、単一障害点となっている設備を特定し、十分な冗長性と障害時の円滑な切替を確保すること。 (f)広域災害の発生に際しては、クラウドサービスの継続を優先するか、情報セキュリティ対策の確保を優先するかについての方針を定め、クラウド利用者の同意を得ること。

①（項番40）（資料1-3：P75）

改定案（3.6.3 システム開発、導入、保守）【例文】

＜修正前＞

（３） 情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

3.6.3. システム開発、導入、保守等

（ア） 情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。【推奨事項】

（イ） 情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

（ウ） 情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

②テスト

（ア） 情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

（イ） 情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

＜修正後＞

3.6.3. システム開発、導入、保守等

（ア） 情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。【推奨事項】

（イ） 情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

（ウ） 情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

(エ) 情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

①（項番40）（資料1-3：P77）

改定案（3.6.3 システム開発、導入、保守）【解説】

＜修正前＞

（解説）

（１） 情報システムの調達

情報システムを調達する場合は、当該情報システムで取り扱う情報の重要性に応じて、システム運用及び利用面で必要となるセキュリティ機能を洗い出し、調達要件に含める必要がある。例えば、アクセス制御の機能、パスワード設定機能、ログ取得機能、データの暗号化等である。

（注１）情報機器及びソフトウェア等の情報セキュリティ機能の評価に当たっては、第三者機関による客観的な評価である、ISO/IEC15408に基づくITセキュリティ評価及び認証制度による認証の取得の有無を評価項目として活用すること、又は構築する情報システムに重要な情報セキュリティ要件があると認められた場合には、第三者機関による当該情報システムのセキュリティ設計仕様書（ST: Security Target）のST評価・ST確認を活用することも考えられる。「ITセキュリティ評価及び認証制度（JISEC）」については、独立行政法人情報処理推進機構のサイトを参照のこと。

（注２）システム調達、開発、導入を行うに当たっては、最高情報統括責任者の許可を得て実施することが望ましい。

（注３）情報システムの利用を満足できるものにするためには、情報システムが当該利用に足りる十分な処理能力と記憶容量を持つことが必要である。また、処理能力と記憶容量の使用状況を監視し、将来的に必要とされる能力・容量を予測して、ハードディスクの増強等適切な措置をとることが望まれる。

＜修正後＞

（注４）情報システムは可用性の観点から、冗長性を組み入れることを考慮することが望ましい。ただし、冗長性を組み入れることにより、情報システムの完全性、機密性に対するリスクが生じる可能性があるため、この点についても考慮すること。

・機密性を高める対策例
　サーバを．．．
・完全性を高める対策例
　二重化した．．．
（他論点：項番39対応）

（注５）ICT製品の調達において、その製品に他の供給者から供給される構成部品やソフトウェアが含まれる場合には、そのサプライチェーン全体に適切なセキュリティ慣行を伝達するよう、直接の供給者に要求することが必要である。また、提供されたICT製品が機能要件として取り決められたとおりに機能すること、構成部品やソフトウェアについてはその供給元が追跡可能であることを保証させることが望ましい。
（他論点：項番61、62対応）

（注６）導入する情報システムに応じた要件の詳細については、「非機能要求グレード（地方公共団体版）利用ガイド」（平成26年3月　地方自治情報センター）を参照されたい。

①（項番63）

（ 3.8.1 外部委託）

NISC等の考え方	【府省庁対策基準策定のためのガイドライン:4.1.1 外部委託（２）外部委託に係る契約】 ● 遵守事項4.1.1(1)(a)(ア)「委託先によるアクセスを認める情報及び情報システムの範囲」について 委託先や第三者による許可されていない情報及び情報システムへのアクセス等が行われないように、委託先におけるそれらの取扱いに関する府省庁の基準を規定することを求めている。 特に、委託業務において使用される情報システムが海外のデータセンターに設置されている場合等においては、保存している情報に対して現地の法令等が適用されるため、国内であれば不適切と判断されるアクセスをされる可能性があることに注意が必要である。「行政機関の保有する個人情報の保護に関する法律」（平成15年法律第58号）で定義する個人情報については、国内法が適用される場所に制限する必要があると考えるため、個人情報を取り扱う委託業務においては、保存された情報等において国内法令が適用されること等を外部委託の際の判断条件としておくべきである。

①（項番63）（資料1-3：P105）

改定案（3.8.1 外部委託）【解説】

＜修正前＞

3.8.1. 外部委託

者に通知しておく必要がある。連絡網には、職員の個人情報が記載される場合もあるため、取扱いに注意する。

⑪市による監査、検査

外部委託事業者が実施する情報システムの運用、保守、サービス提供等の状況を確認するため、当該委託事業者に監査、検査を行うことを明確に規定しておくことが必要である。

なお、地方公共団体において、当該委託事業者に監査、検査を行うことが困難な場合は、地方公共団体による監査、検査に代えて、第三者や第三者監査に類似する客観性が認められる外部委託事業者の内部監査部門による監査、検査又は国際的なセキュリティの第三者認証の取得等によって確認する。

⑫市による事故時等の公表

委託業務に関し、情報セキュリティに関する事件・事故等が発生した場合、住民に対し適切な説明責任を果たすため、当該事故等の公表を必要に応じ行うことについて、外部委託事業者と確認しておく。

⑬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)

外部委託事業者においての情報セキュリティポリシーが遵守されなかったため、被害を受けた場合には、当該委託事業者が損害賠償を行うことを契約上明記しておく。

（注４）これらの契約項目については、「地方公共団体における業務の外部委託事業者に対する個人情報の管理に関する検討」報告書（平成 21年 3月 総務省）を参照し、「個人情報の取扱いに関する特記仕様書（雛型）」を活用されたい。

（注５）外部委託事業者に対して、情報セキュリティポリシーの該当部分について、十分に説明しておくことが必要である。

（注６）指定管理者制度に関する考慮事項

指定管理者制度においては、条例により、地方公共団体と指定管理者との間で協定を締結することになるが、その協定において、委託内容に応じた情報セキュリティ対策が確保されるよう必要な事項を定める必要がある。

＜修正後＞

（注７）クラウドサービスの利用に関する考慮事項

インターネットを介してサービスを提供するクラウドサービスの利用に当たっては、クラウドサービス事業者の事業所の場所にかかわらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、クラウドサービス事業者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、データセンターの設置されている国の法令により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、住民情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で運用できるデータセンターを選択する必要がある。

なお、クラウドサービスの利用に当たっては、契約の形態が従前の委託や請負と異なることが想定されることから、「地方公共団体におけるASP・SaaS導入活用ガイドライン」（平成22年4月　総務省）を参照されたい。

② 外部委託（サプライチェーン・リスク）

※論点整理表：
項番61、62

論点2

※凡例：赤数字＝管理強化、青数字＝明確化

② 外部委託（サプライチェーン・リスク）

論点整理表：
項番61、62

現状ガイドライン

- 自治体側でセキュリティ要件を考慮し、委託先を選定していた。また、監査についても必要に応じて実施するという考え方であった。
- 委託先による不正行為のリスクについての検討が弱かった。（調達の際に、知らないうちに不要なソフトウェアが導入される等）
- 再委託に関する考慮が弱かった。（原則禁止）

ガイドライン改定観点

- 組織へICTサービスを提供する供給者のサプライチェーンに対するセキュリティについて、供給者との合意を行う事項を追記。
- クラウドサービスを利用する場合の、ICTサプライチェーンにおけるセキュリティ対策の確認と選択について追記。
- 調達仕様書への要求事項例を【例文】に記載し、自治体において調達仕様を作成できるような記述に修正。

（参考：府省庁対策基準策定のためのガイドライン 4.1.1、ISO/IEC27001:2013 A15.1.3）

②（項番61、62）

（3.8.1 外部委託）

NISC等の考え方	【府省庁対策基準策定のためのガイドライン:4.1.1 外部委託（2）外部委託に係る契約】 ● （a）情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。 （ウ） 委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制 （を仕様内容に含めること） 【政府機関の情報セキュリティ対策のための統一基準 4.1.1 外部委託】 ● (2) 外部委託に係る契約 (a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。 (ア) 委託先に提供する情報の委託先における目的外利用の禁止 (イ) 委託先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) 委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制 (エ) 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・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 (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 【ISO/IEC27001:2013 A.15.1.3 ICTサプライチェーン】 ● 供給者との合意には、情報通信技術（ICT）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めなければならない。 【 ISO/IEC27002:2013 15.1.3 ICTサプライチェーン】 ● サプライチェーンのセキュリティについては、供給者との合意に次の事項を含めることを考慮することが望ましい。 c) ICT製品に関して、その製品に他の供給者から購入した構成部品が含まれる場合には、そのサプライチェーン全体に適切なセキュリティ慣行を伝達するよう供給者に要求する。 f) 重要な構成要素及びその供給元が、サプライチェーン全体を通じて追跡可能であるという保証を得る。 g) 提供されるICT製品が期待どおりに機能し、予期しない又は好ましくない特性をもたないという保証を得る。

②（項番61、62）（資料1-3：P77）

改定案（3.6.3 システム開発、導入、保守）【解説】

＜修正前＞

（解説）

（１） 情報システムの調達

情報システムを調達する場合は、当該情報システムで取り扱う情報の重要性に応じて、システム運用及び利用面で必要となるセキュリティ機能を洗い出し、調達要件に含める必要がある。例えば、アクセス制御の機能、パスワード設定機能、ログ取得機能、データの暗号化等である。

（注１）情報機器及びソフトウェア等の情報セキュリティ機能の評価に当たっては、第三者機関による客観的な評価である、ISO/IEC15408に基づくITセキュリティ評価及び認証制度による認証の取得の有無を評価項目として活用すること、又は構築する情報システムに重要な情報セキュリティ要件があると認められた場合には、第三者機関による当該情報システムのセキュリティ設計仕様書（ST: Security Target）のST評価・ST確認を活用することも考えられる。「ITセキュリティ評価及び認証制度（JISEC）」については、独立行政法人情報処理推進機構のサイトを参照のこと。

（注２）システム調達、開発、導入を行うに当たっては、最高情報統括責任者の許可を得て実施することが望ましい。

（注３）情報システムの利用を満足できるものにするためには、情報システムが当該利用に足りる十分な処理能力と記憶容量を持つことが必要である。また、処理能力と記憶容量の使用状況を監視し、将来的に必要とされる能力・容量を予測して、ハードディスクの増強等適切な措置をとることが望まれる。

＜修正後＞

（注４）情報システムは可用性の観点から、冗長性を組み入れることを考慮することが望ましい。ただし、冗長性を組み入れることにより、情報システムの完全性、機密性に対するリスクが生じる可能性があるため、この点についても考慮すること。

・機密性を高める対策例
　サーバを．．．
・完全性を高める対策例
　二重化した．．．
（他論点：項番39対応）

（注５）ICT製品の調達において、その製品に他の供給者から供給される構成部品やソフトウェアが含まれる場合には、そのサプライチェーン全体に適切なセキュリティ慣行を伝達するよう、直接の供給者に要求することが必要である。また、提供されたICT製品が機能要件として取り決められたとおりに機能すること、構成部品やソフトウェアについてはその供給元が追跡可能であることを保証させることが望ましい。

（注６）導入する情報システムに応じた要件の詳細については、「非機能要求グレード（地方公共団体版）利用ガイド」（平成26年3月　地方自治情報センター）を参照されたい。

②（項番61、62）（資料1-3：P102）

改定案（3.8.1 外部委託）（解説）

＜修正前＞

（解説）

（１） 外部委託事業者の選定基準

外部委託事業者を選定するに当たっては、情報セキュリティ上、重要な情報資産を取り扱う可能性があることから、技術的能力、信頼性等について考慮して、情報セキュリティ対策が確保されることを確認する必要がある。

また、外部委託事業者の選定に当たり、事業者の情報セキュリティ水準を評価する際には、国際規格の認証取得状況等を参考にして決定することが望ましい。

（注１）これらの選定方法については、「公共 IT におけるアウトソーシングに関するガイドライン」（平成 15 年 3 月 総務省）を参照されたい。

（注２）現在の最新の規格である ISO/IEC27001 については、一般財団法人日本情報経済社会推進協会のホームページ（ISMS 適合性評価制度）、又は一般財団法人日本規格協会のホームページを参照されたい。

（注３）ホスティングサービスの利用等においては、サービス提供者側のミスや機器の故障などの不測の事態によりデータの消失などの事態が発生する恐れがあるため、情報システムや取り扱う情報の重要度に応じたバックアップなどの必要な対策を講じておく必要がある。なお、ホスティング時のデータ消失に関する対策については、「ホスティングサービス等利用時におけるデータ消失事象への対策実施及び契約内容の再確認等について（注意喚起）」（平成 24 年 7 月 総務省 事務連絡）を参照されたい。

＜修正後＞

（解説）

（１） 外部委託事業者の選定基準

外部委託事業者を選定するに当たっては、情報セキュリティ上、重要な情報資産を取り扱う可能性があることから、技術的能力、信頼性等について考慮して、情報セキュリティ対策が確保されることを確認する必要がある。

また、外部委託事業者の選定に当たり、事業者の情報セキュリティ水準を評価する際には、国際規格の認証取得状況等を参考にして決定することが望ましい。

なお、外部委託事業者の選定条件として仕様等に盛り込む内容としては、例えば次のものがある。

- **外部委託事業者に提供する情報の委託事業者における目的外使用の禁止**
- **外部委託事業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**
- **外部委託事業の実施に当たり、外部委託事業者の組織又はその従業員、再委託事業者、若しくはその他の者による意図せざる変更が加えられないための管理体制**
- **外部委託事業者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・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**
- **情報セキュリティ事故への対処方法**
- **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**
- **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**

②（項番61、62）（資料1-3：P105）

改定案（3.8.1 外部委託）（解説）

＜修正前＞

（２） 契約項目

（中略）

⑱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)

外部委託事業者においての情報セキュリティポリシーが遵守されなかったため、被害を受けた場合には、当該委託事業者が損害賠償を行うことを契約上明記しておく。

（注４）これらの契約項目については、「地方公共団体における業務の外部委託事業者に対する個人情報の管理に関する検討」報告書（平成 21年 3月 総務省）を参照し、「個人情報の取扱いに関する特記仕様書（雛型）」を活用されたい。

（注５）外部委託事業者に対して、情報セキュリティポリシーの該当部分について、十分に説明しておくことが必要である。

（注６）指定管理者制度に関する考慮事項

指定管理者制度においては、条例により、地方公共団体と指定管理者との間で協定を締結することになるが、その協定において、委託内容に応じた情報セキュリティ対策が確保されるよう必要な事項を定める必要がある。

（注７）クラウドサービスの利用に関する考慮事項

インターネットを介してサービスを提供するクラウドサービスの利用に当たっては、クラウドサービス事業者の事業所の場所にかかわらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、クラウドサービス事業者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、データセンターの設置されている国の法令により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、住民情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で運用できるデータセンターを選択する必要がある。

なお、クラウドサービスの利用に当たっては、契約の形態が従前の委託や請負と異なることが想定されることから、「地方公共団体における ASP・SaaS導入活用ガイドライン」（平成 22年 4月　総務省）を参照されたい。

＜修正後＞

可能性があるため、住民情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で運用できるデータセンターを選択する必要がある。

なお、クラウドサービスの利用に当たっては、契約の形態が従前の委託や請負と異なることが想定されることから、「地方公共団体における ASP・SaaS導入活用ガイドライン」（平成 22年 4月　総務省）を参照されたい。

（注８）ICTサプライチェーンを構成して提供されるサービスを利用する場合は、外部委託事業者との関係におけるリスク（サービスの供給の停止、故意又は過失による不正アクセス、外部委託事業者のセキュリティ管理レベルの低下など）を考慮しそのリスクを防止するための事項について外部委託事業者と合意し、その内容を文書化しておくことが望ましい。

（注９）外部委託事業者に適用される法令としては、法律のほか、各地方公共団体の制定する個人情報保護条例も適用されることを明記しておく必要がある。（他論点：③対応）

（注１０）業務の内容に応じて規定する要件の詳細については、「非機能要求グレード（地方公共団体版）利用ガイド」（平成26年3月　地方自治情報センター）を参照されたい。

③ 外部委託（委託先管理）

※論点整理表：
項番65

論点3

※凡例：赤数字＝管理強化、青数字＝明確化

③ 外部委託（委託先管理）

論点整理表：
項番65

現状ガイドライン

- 自治体側でセキュリティ要件を考慮し、委託先を選定していた。また、監査についても必要に応じて実施するという考え方であった。
- 委託先による不正行為のリスクについての検討が弱かった。（作業場所への私物スマートデバイス等の持込み、定期的なログの確認等）
- 再委託に関する考慮が弱かった。（原則禁止）

ガイドライン改定観点

- 外部委託の際、委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先において自治体の要件に適合した情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とすることが必要である。
- 改訂観点は、以下となる。
  - ・地方公共団体は委託先の選定条件を定義すること（【解説】に例を記載）
  - ・地方公共団体は委託先の情報セキュリティ対策の履行状況を確認すること
  - ・地方公共団体は委託先がその業務の一部を再委託する場合は、再委託先でも情報セキュリティが確保されるよう委託先に担保させること

③（項番65）

（3.8.1 外部委託）

NISC等の考え方	【府省庁対策基準策定のためのガイドライン:4.1.1 外部委託（2）外部委託に係る契約】 ● (2) 外部委託に係る契約 (a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。 (ア) 委託先に提供する情報の委託先における目的外利用の禁止 (イ) 委託先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) 委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制 (エ) 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・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 (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 ● (3) 外部委託における対策の実施 (a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認すること。 (b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託した業務において、情報セキュリティインシデント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行政事務従事者より受けた場合は、当該サービスの利用を中止するなど、必要な措置を講じ、委託先に契約に基づく必要な措置を講じさせること。 (c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認すること。

③（項番65）（資料1-3：P103～104）

改定案（3.8.1 外部委託）（解説）

＜修正前＞

（２） 契約項目

（中略）

外部委託事業者に提供した情報について、不正な利用を防止させるために、業務以外での利用を禁止する。

⑥業務上知り得た情報の守秘義務

業務中及び業務を終了した後も、情報の漏えいを防止するために、業務上知り得た秘密を漏らしてはならない旨を規定する。

⑦再委託に関する制限事項の遵守

一般的に、再委託した場合、再委託先のセキュリティレベルは下がることが懸念されるために、再委託は原則禁止する。例外的に再委託を認める場合には、再委託先の業者における情報セキュリティ対策が十分取られており、外部委託事業者と同等の水準であることを確認した上で許可しなければならない。

⑧委託業務終了時の情報資産の返還、廃棄等

委託業務終了時に、不要になった情報資産を返還させるか廃棄させるか等その取扱いについて明確に規定する必要がある。委託終了後の取扱いを明確にすることにより、不要になった情報資産から情報が漏えいする可能性を下げる。

⑨委託業務の定期報告及び緊急時報告義務

定期報告及び緊急時報告の手順を定め、委託業務の状況を適切かつ速やかに確認できるようにすることが必要である。緊急時の職員への連絡先は、外部委託業者に通知しておく必要がある。連絡網には、職員の個人情報が記載される場合もあるため、取扱いに注意する。

⑩市による監査、検査

外部委託事業者が実施する情報システムの運用、保守等の状況を確認するため、当該委託事業者に監査、検査を行うことを明確に規定しておくことが必要である。

＜修正後＞

⑥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

外部委託事業者に提供した情報について、不正な利用を防止させるために、業務以外での利用を禁止する。

⑦業務上知り得た情報の守秘義務

業務中及び業務を終了した後も、情報の漏えいを防止するために、業務上知り得た秘密を漏らしてはならない旨を規定する。

⑧再委託に関する制限事項の遵守

一般的に、再委託した場合、再委託事業者のセキュリティレベルは下がることが懸念されるために、再委託は原則禁止する。例外的に再委託を認める場合には、再委託事業者における情報セキュリティ対策が十分取られており、外部委託事業者と同等の水準であることを確認し、外部委託事業者に担保させた上で許可しなければならない。

⑨委託業務終了時の情報資産の返還、廃棄等

委託業務終了時に、不要になった情報資産を返還させるか廃棄させるか等その取扱いについて明確に規定する必要がある。委託終了後の取扱いを明確にすることにより、不要になった情報資産から情報が漏えいする可能性を下げる。

⑩委託業務の定期報告及び緊急時報告義務

定期報告及び緊急時報告の手順を定め、委託業務の状況を適切かつ速やかに確認できるようにすることが必要である。緊急時の職員への連絡先は、外部委託業者に通知しておく必要がある。連絡網には、職員の個人情報が記載される場合もあるため、取扱いに注意する。

③（自治体様からのご意見）（資料1-3：P105）

改定案（3.8.1 外部委託）（解説）

＜修正前＞

（２） 契約項目

（中略）

⑱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)

外部委託事業者においての情報セキュリティポリシーが遵守されなかったため、被害を受けた場合には、当該委託事業者が損害賠償を行うことを契約上明記しておく。

（注４）これらの契約項目については、「地方公共団体における業務の外部委託事業者に対する個人情報の管理に関する検討」報告書（平成 21年 3月 総務省）を参照し、「個人情報の取扱いに関する特記仕様書（雛型）」を活用されたい。

（注５）外部委託事業者に対して、情報セキュリティポリシーの該当部分について、十分に説明しておくことが必要である。

（注６）指定管理者制度に関する考慮事項

指定管理者制度においては、条例により、地方公共団体と指定管理者との間で協定を締結することになるが、その協定において、委託内容に応じた情報セキュリティ対策が確保されるよう必要な事項を定める必要がある。

（注７）クラウドサービスの利用に関する考慮事項

インターネットを介してサービスを提供するクラウドサービスの利用に当たっては、クラウドサービス事業者の事業所の場所にかかわらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、クラウドサービス事業者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、データセンターの設置されている国の法令により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、住民情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で運用できるデータセンターを選択する必要がある。

なお、クラウドサービスの利用に当たっては、契約の形態が従前の委託や請負と異なることが想定されることから、「地方公共団体における ASP・SaaS導入活用ガイドライン」（平成 22年 4月　総務省）を参照されたい。

＜修正後＞

可能性があるため、住民情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で運用できるデータセンターを選択する必要がある。

なお、クラウドサービスの利用に当たっては、契約の形態が従前の委託や請負と異なることが想定されることから、「地方公共団体における ASP・SaaS導入活用ガイドライン」（平成 22年 4月　総務省）を参照されたい。

（注８）ICTサプライチェーンを構成して提供されるサービスを利用する場合は、外部委託事業者との関係におけるリスク（サービスの供給の停止、故意又は過失による不正アクセス、外部委託事業者のセキュリティ管理レベルの低下など）を考慮しそのリスクを防止するための事項について外部委託事業者と合意し、その内容を文書化しておくことが望ましい。（他論点：61、62対応）

（注９）外部委託事業者に適用される法令としては、法律のほか、各地方公共団体の制定する個人情報保護条例も適用されることを明記しておく必要がある。

（注10）業務の内容に応じて規定する要件の詳細については、「非機能要求グレード（地方公共団体版）利用ガイド」（平成26年3月　地方自治情報センター）を参照されたい。（他論点：61、62対応）

④　ネットワークの利用（公衆通信網の利用）

※論点整理表：
項番18、21、
25

論点4

論点4

※凡例：赤数字＝管理強化、青数字＝明確化

④　ネットワークの利用（公衆通信網の利用）

論点整理表：
項番18、21、25

現状ガイドライン

- 通信環境の変化により、無線LANや公衆通信網の普及が進み、庁舎外から業務を行うという観点での対策概念が弱かった。
- 庁内の端末からのアクセスが中心であり、ワークスタイルの変化やニーズに対する考慮が弱かった

ガイドライン改定観点

- 自治体庁舎外から庁内の情報システムにアクセスする環境を構築する場合、使用する通信回線は、安全な通信回線サービスを利用することが望ましいが、利用可能なサービスが限られている場合等、安全なサービスを利用できない場合を考慮する必要がある。
- 在宅勤務（テレワーク）等の業務も含め、リモートアクセスでの業務時におけるリスクを十分検討し、必要な対策を実施しておく必要がある。（状況に応じた条件の明記）

  ・原則、安全な通信回線サービスを利用すること
  ・リモートアクセス環境を構築する場合は、通信内容の暗号化等の対策を行うこと。
  ・自治体は、例外的に公衆通信網を利用する場合は、取り扱われる情報の制限等の精査を行うこと
  ・公衆通信網を利用する場合は、VPN接続、認証処理及び通信内容の暗号化等の対策を実施すること

④（項番18、25）

（3.6.2 アクセス制御）

NISC等の考え方	【政府機関の情報セキュリティ対策のための統一基準:7.3.1 通信回線】 ● 情報システムセキュリティ責任者は、府省庁内通信回線にインターネット回線、公衆通信回線等の府省庁外通信回線を接続する場合には、府省庁内通信回線及び当該府省庁内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずること ● 情報システムセキュリティ責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること

④（項番18、25）（資料1-3：P70）

改定案（3.6.2 アクセス制御）【例文】

＜修正前＞

（2） 職員等による外部からのアクセス等の制限

①職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

②統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③統括情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④統括情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

⑤統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するパソコン等の端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

⑥職員等は、持ち込んだ又は外部から持ち帰ったパソコン等の端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

（3） 自動識別の設定

統括情報セキュリティ責任者及び情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。【推奨事項】

＜修正後＞

⑤統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するパソコン等の端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

⑥職員等は、持ち込んだ又は外部から持ち帰ったパソコン等の端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

⑦統括情報セキュリティ責任者は、公衆通信回線（公衆無線LAN等）の庁外通信回線を庁内ネットワークに接続することは、原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のID及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ICカード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

（3） 自動識別の設定

統括情報セキュリティ責任者及び情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。【推奨事項】

④（項番18、25）（資料1-3：P72）

改定案（3.6.2 アクセス制御）（解説）

＜修正前＞

（2） 職員等による外部からのアクセス等の制限

外部から庁内ネットワークに接続を認める場合は、外部から攻撃を受けるリスクが高くなることから、本人確認手段の確保、通信途上の盗聴を防御するための暗号化等の必要な措置を取らなければならない。また、接続に当たっては許可制とし、許可は必要最小限の者に限定しなければならない。

（注３）持ち込んだ端末を確認するシステムとして、検疫システムがある。検疫システムとは、OS のパッチやコンピュータウイルス対策ソフトウェアのパターンファイルが最新でない、不正プログラムが侵入しているなど、十分なセキュリティ対策が取られていないモバイル用のパソコンを庁内ネットワークに接続させないシステムである。モバイル用のパソコンを庁舎内に持ち帰った場合等に、検疫システムによる確認を義務付けることにより、様々な脅威の発生を低減することができる。

（3） 自動識別の設定

ネットワークに不正な機器の接続を防止するために、MAC アドレス等の認証情報を利用し制限する必要がある。

＜修正後＞

（注３）持ち込んだ端末を確認するシステムとして、検疫システムがある。検疫システムとは、OS のパッチやコンピュータウイルス対策ソフトウェアのパターンファイルが最新でない、不正プログラムが侵入しているなど、十分なセキュリティ対策が取られていないモバイル用のパソコンを庁内ネットワークに接続させないシステムである。モバイル用のパソコンを庁舎内に持ち帰った場合等に、検疫システムによる確認を義務付けることにより、様々な脅威の発生を低減することができる。

（注４）庁外から庁内のネットワークにアクセスする際に公衆無線LAN等の庁外通信回線を利用することは原則禁止であるが、やむを得ず利用する場合は、統括情報セキュリティ責任者の許可を得たうえで、本人確認、VPN接続時の認証処理及び通信内容の暗号化等の対策を考慮しなければならない。

なお、その場合でも基幹系ネットワークへのアクセスは禁止とし、電子メールやグループウェア等へのアクセスに限定することが求められる。

（3） 自動識別の設定

ネットワークに不正な機器の接続を防止するために、MAC アドレス等の認証情報を利用し制限する必要がある。

④（項番21）

（3.5.1 職員等の遵守事項）

NISC等の考え方	【政府機関の情報セキュリティ対策のための統一基準:7.3.1 通信回線】 ● 情報システムセキュリティ責任者は、府省庁内通信回線にインターネット回線、公衆通信回線等の府省庁外通信回線を接続する場合には、府省庁内通信回線及び当該府省庁内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずること ● 情報システムセキュリティ責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること 【テレワークセキュリティガイドライン（第3版）】 ● システム管理者が実施すべき対策 　● 情報セキュリティ保全対策の大枠 　● 悪意のソフトウェアに対する対策 　● 端末の紛失・盗難に対する対策 　● 不正侵入・踏み台に対する対策 ● テレワーク勤務者が実施すべき対策 　● 情報セキュリティ保全対策の大枠 　● 悪意のソフトウェアに対する対策 　● 端末の紛失・盗難に対する対策 　● 重要情報の盗聴に対する対策 　● 不正侵入・踏み台に対する対策

④（項番21）（資料1-3：P50）

改定案（3.5.1 職員等の遵守事項）（解説）

＜修正前＞

（注１）モバイル端末の持ち出しを許可した場合にも、モバイル端末は常に携行することを職員等に周知する必要がある。特に交通機関（電車、バス、自家用車等）による移動時の携行に際しては、紛失、盗難等に留意する必要がある。
（注２）共用しているモバイル端末の持ち出しでは、管理者が不明確認になりやすく、その結果として所在不明になりやすいので特に注意する必要がある。
（注３）持ち出し専用パソコンによる情報の持ち出しにおいては、万一当該パソコンを紛失した場合に、記録されている情報を容易に特定するため、日

3.5.1. 職員等の遵守事項

常においては当該パソコンに情報を記録しないようにし、持ち出し時においては持ち出し情報が必要最小限であるかどうか確認を行った上で情報を記録し、返却時においては情報の完全削除をするといった運用を行う必要がある。

＜修正後＞

（注４）テレワークを導入する場合は、**本人確認手段の確保、通信途上の盗聴を防御するために、安全な通信回線サービスを利用しなければならない。その際、通信する情報の機密性に応じて、ファイル暗号化、通信経路の暗号化等の必要な措置を取ることが求められる。**なお、テレワークセキュリティ対策については、「テレワークセキュリティガイドライン（第3版）」（平成25年3月　総務省）を参照されたい。

⑤ 支給以外のスマートデバイス等の業務利用

※論点整理表：
項番14

論点14

※凡例：赤数字＝管理強化、青数字＝明確化

⑤ 支給以外のスマートデバイス等の業務利用

論点整理表：
項番14

現状ガイドライン

- 支給以外のパソコンについての考慮はされていたが、常に持ち歩き、インターネットに接続できるスマートデバイスについての概念が弱かった。
- デバイスはパソコンが中心であり、デバイスの進化によりスマートデバイスの機能が強化されることに関する考慮が弱かった。

ガイドライン改定観点

- 行政事務は、自治体から支給された端末を用いて行うべきだが、出張や外出等の際に自治体支給以外の端末の使用を検討する団体が今後出てくることも考えられる。その際は、行政事務を行う職員等が定められた手順及び安全管理措置の実施を順守するよう、責任者の厳格な管理が必要となる。

  ・自治体は、組織の実情を把握し、支給以外の端末の持ち込みによるリスクを認識する

  ・支給以外の端末の利用頻度が高ければ、自治体から端末を支給すること、又は、厳格な管理の下、安全に支給以外の端末を利用させることを考える。

  ・利用できる職員の制限をかける（教育等を受けたリテラシーのある人のみ使えるなど）

  ・事務フロアは私物の持ち込OKだが、マシン室には持ち込めない、撮影もできないというような範囲制限をかけたルール作り

⑤（項番１４）

（3.5.1 職員等の遵守事項）

NISC等の考え方	【政府機関の情報セキュリティ対策のための統一基準:8.2 府省庁支給以外の端末の利用】 ● (1) 府省庁支給以外の端末の利用規定の整備・管理 (a) 統括情報セキュリティ責任者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合の許可等の手続に関する手順を定めること。 (b) 統括情報セキュリティ責任者は、要機密情報について府省庁支給以外の端末により情報処理を行う場合の安全管理措置に関する規定を整備すること。 (c) 情報セキュリティ責任者は、府省庁支給以外の端末による行政事務に係る情報処理に関する安全管理措置の実施状況を管理する責任者を定めること。 (d) 前号で定める責任者は、要機密情報を取り扱う府省庁支給以外の端末について、端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための措置を講ずるとともに、行政事務従事者に適切に安全管理措置を講じさせること。 ● (2) 府省庁支給以外の端末の利用時の対策 (a) 行政事務従事者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合には、遵守事項8.2.1(1)(c)で定める責任者の許可を得ること。 (b) 行政事務従事者は、要機密情報を府省庁支給以外の端末で取り扱う場合は、課室情報セキュリティ責任者の許可を得ること。 (c) 行政事務従事者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合には、府省庁にて定められた手続及び安全管理措置に関する規定に従うこと。 (d) 行政事務従事者は、情報処理の目的を完了した場合は、要機密情報を府省庁支給以外の端末から消去すること。

⑤（項番１４）（資料1-3：P50）

改定案（3.5.1 職員等の遵守事項）（解説）

＜修正前＞

（解説）

（１） 職員等の遵守事項

情報セキュリティを確保するために、情報セキュリティポリシー及び実施手順に定められている事項等、すべての職員が遵守すべき事項について定めたものである。

情報セキュリティ管理者は、異動、退職等により業務を離れる場合、職員等が利用している情報資産を返却させる。また ID についても、速やかに利用停止等の措置を講じる必要がある。

①パソコン等の端末等の持ち出し

情報の漏えいは、不正なパソコンの持出しや移動中にパソコンが盗難に遭うなどしたことが原因で発生する場合が多い。重要な情報資産を使って外部で作業する場合には、庁舎内の安全対策に加え、安全管理に関して追加的な措置を定めた上で、パソコン等の持ち出しや外部での作業の実施については許可制とするのが適切である。

（注１）パソコン等の持ち出しを許可した場合にも、パソコン等は常に携行することを職員等に周知する必要がある。特に交通機関（電車、バス、自家用車等）による移動時の携行に際しては、紛失、盗難等に留意する必要がある。

また、自宅や庁外等の外部での情報処理作業において私物のパソコンを使うときには、特に情報漏えい等に留意する必要がある。したがって、私物パソコンの使用は許可制とし、機密性の高い情報資産については私物パソコンでの作業を禁止するのが適当である。

（注２）私物パソコンの使用を許可する場合にも、私物パソコンにコンピュータウイルスチェックやファイル共有ソフトウェアの導入がされていないか確認させるなどの対策を講じる必要がある。共用しているパソコン、記録媒体は管理がずさんになりやすい傾向があることから、特に注意する。

（注３）持ち出し専用パソコンによる情報の持ち出しにおいては、万一当該パソコンを紛失した場合に、記録されている情報を容易に特定するため、日常においては当該パソコンに情報を記録をしないようにし、持ち出し時においては持ち出し情報が必要最小限であるかどうか確認を行った上で情報を記録し、返却時においては情報の完全削除をするといった運用を行う必要がある。

（注４）テレワークを導入する場合は、更なるセキュリティポリシー遵守の徹

＜修正後＞

（注１）モバイル端末の持ち出しを許可した場合にも、モバイル端末は常に携行することを職員等に周知する必要がある。特に交通機関（電車、バス、自家用車等）による移動時の携行に際しては、紛失、盗難等に留意する必要がある。

（注２）共用しているモバイル端末の持ち出しでは、管理者が不明確になりやすく、その結果として所在不明になりやすいので特に注意する必要がある。

②支給以外のパソコンやモバイル端末等の業務利用

自宅や庁外等の外部での情報処理作業においては支給された端末を利用することとし、支給以外の端末の使用は原則禁止とする。

なお、やむを得ず支給以外の端末を使用する場合は許可制とし、機密性3の情報資産については支給以外の端末での作業を禁止するのが適当である。

また、支給以外の端末の使用を許可する場合には、地方公共団体側で端末の使用環境をコントロールすることが求められる。具体的には、支給以外の端末にコンピュータウイルスチェックが実施されていることやファイル共有ソフトウェアの導入がされていないことを情報セキュリティ管理者が職員等に確認させたり、パスワードによる端末ロック機能や遠隔消去機能などの要件を満たした支給以外の端末の場合のみ使用を許可するといった対策を講じる必要がある。さらに、支給以外の端末から庁内ネットワークに接続を行う可能性がある場合は、支給以外の端末からの情報漏えいを防ぐため、シンクライアント環境やセキュアブラウザの使用、ファイル暗号化機能を持つアプリケーションでの接続のみを許可するといった対策を講じる必要がある。

なお、支給以外の端末の使用に当たっては、支給以外の端末のセキュリティに関する教育を受けた者のみ使用を許可するなどの対策も有効である。

⑥ SMS(ソーシャルメディアサービス：SNS、ストリーミング等)の業務利用

※論点整理表：
項番15

論点6

※凡例：赤数字＝管理強化、青数字＝明確化

⑥ SMS(ソーシャルメディアサービス：SNS、ストリーミング等)の業務利用

論点整理表：
項番15

現状ガイドライン

- スマートデバイスやタブレット端末が普及しておらず、様々なモノがインターネットにつながっていたわけではなかったことから、SNSやストリーミング等、ソーシャルメディアサービスを利用した情報発信を行うという概念が弱かった。

ガイドライン改定観点

- 住民への情報提供など、ソーシャルメディアサービスを使う場合は約款による外部サービスを利用することが考えられる。当該サービスを利用した情報発信を行う場合は、なりすましの防止や可用性の確保等の対策が必要となる。

- 改訂観点としては、以下となる。
  - ・SMS利用時は、ルールを定め、職員の啓発を行うことが必要
  - ・自治体は発信する情報の内容の精査を行うこと（住民情報などの機密性の高い情報の発信の禁止）
  - ・自治体は、アカウントのなりすまし、乗っ取りによる虚偽情報の発信の防止対策を実施すること
  - ・自治体は、予告なしでのサービスの中断・停止対策を検討すること

⑥（項番１５）

（3.8.2 SMS（ソーシャルメディアサービス）の利用）

NISC等の考え方	【政府機関の情報セキュリティ対策のための統一基準:4.1.3 ソーシャルメディアサービスによる情報発信】 ● (1) ソーシャルメディアサービスによる情報発信時の対策 (a) 統括情報セキュリティ責任者は、府省庁が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する運用手順等を定めること。 (ア) 府省庁のアカウントによる情報発信が実際の府省庁のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。 (イ) パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。 (b) 情報セキュリティ責任者は、府省庁において情報発信のためにソーシャルメディアサービスを利用する場合は、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ること。 (c) 行政事務従事者は、要安定情報の国民への提供にソーシャルメディアサービスを用いる場合は、府省庁の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。(2) 府省庁支給以外の端末の利用時の対策 【府省庁対策基準策定のためのガイドライン:4.1.3 ソーシャルメディアサービスによる情報発信】 ● a) 府省庁からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、府省庁が運用していることを利用者に明示すること。 ● b) 府省庁からの情報発信であることを明らかにするために、府省庁が政府ドメイン名を用いて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のサービス名と、そのサービスにおけるアカウント名又は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こと。 ● c) 運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている府省庁ウェブサイト上のページのURLを記載すること。 ● d) ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「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には、可能な限りこれを取得すること。

⑥（項番15）（資料1-3：P107）

改定案（3.8.2 SMS（ソーシャルメディアサービス）の利用）【例文】（新規）

＜修正前＞

記載なし

＜修正後＞

3.8.2 SMS（ソーシャルメディアサービス）の利用

【趣旨】

住民への情報提供など、ソーシャルメディアサービスを利用する場合は、約款による外部サービスを利用することが多くなるが、なりすましやサービス停止のおそれがあるため、ソーシャルメディアサービスによる情報発信時の対策を講じる必要がある。

【例文】

SMS（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、本市が管理するアカウントでSMS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SMS運用手順を定めなければならない。

（ア）本市のアカウントによる発信が、実際の本市のものであることを明らかにするために、アカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

（イ）パスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ICカード等）を適切に管理するなどの方法で、不正アクセス対策を行うこと。

②機密性2以上の情報はSMSで発信してはならない。

③利用するSMSごとの責任者を定めなければならない。

⑥（項番１５）（資料1-3：P107～P108）

改定案（3.8.2 SMS（ソーシャルメディアサービス）の利用）（解説）（新規）

＜修正前＞

記載なし

＜修正後＞

（解説）

SMS（ソーシャルメディアサービス）の利用

インターネット上における、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SMSは、積極的な広報活動等に利用することができるが、外部サービスを利用せざるを得ず、第三者によるなりすましやアカウントの乗っ取り、予告なしでサービスが停止するといった事態が発生する可能性がある。そのため、利用にあたっては、SMSの運用ポリシーや運用手順を定め、ルールに沿った利用を行うことが求められる。具体的には次の事項が考えられる。

①なりすまし対策

・庁内で管理しているウェブサイト内において、利用するSMS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

・運用しているSMS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

・ソーシャルメディアの提供事業者が、「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。

②アカウント乗っ取り対策

・パスワードを適切に管理する

・二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用する

・SMSへのログインに利用する端末が不正アクセスや盗難されないよう、最新のセキュリティパッチや不正プログラム対策ソフトウェアの導入、端末管理等のセキュリティ対策を行う

③サービスが終了・停止した場合の対応

・あらかじめ発信した情報のバックアップを庁内に保管しておく等、スムーズに別のサービスへの移行が行えるよう適切な準備をしておく

⑦ 情報セキュリティインシデント対策体制の強化

※論点整理表：
項番8、10、22、
42、49、58

論点7

論点7

論点7

論点7

※凡例：赤数字＝管理強化、青数字＝明確化

⑦ 情報セキュリティインシデント対策体制の強化

論点整理表：
項番8、10、22、
42、49、58

現状ガイドライン

- 緊急時の報告ルートや責任者の存在、情報セキュリティ委員会でのセキュリティポリシーの策定等、それぞれの活動の必要性は説明しているが、情報セキュリティインシデントにおける情報収集、調査、対処、窓口機能等、包括的に対応する体制を整備するという概念が弱かった。

ガイドライン改定観点

- 自治体における、セキュリティ事件・事故への一元的な窓口組織の位置づけ、役割の検討(インシデント発生部署以外への情報提供、ベンダとの連絡調整、マスコミ対応等)を追記
- CISO機能の位置づけ、役割の検討、窓口組織との関係性を追記（CIOとCISOの兼務など、自治体規模に応じた体制作りも含む）
- 構成するメンバの役割、意識づけ、人材確保のための施策を追記
- 自治体CEPTOAR、J-LIS、NISC等との連携について追記

⑦（項番８）

（3.2 組織体制）

NISC等の考え方	【府省庁対策基準策定のためのガイドライン／政府機関のための情報セキュリティ対策のための統一基準】ともに、人材育成に関しての記述はなし。 ● 人材育成例として、アドバイザーやCISO補佐官の民間人活用、内部教育への活用などが考えられる

⑦（項番８）（資料1-3：P26～P27）

改定案（3.2 組織体制）（解説）

＜修正前＞

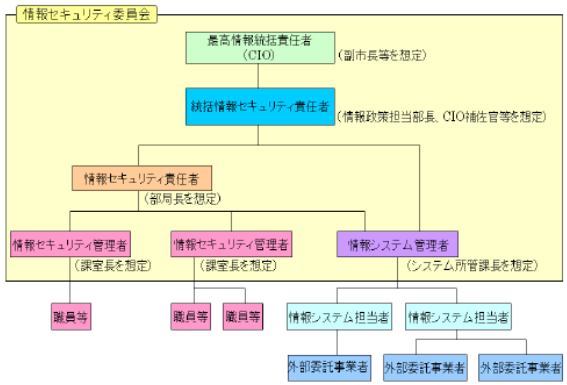
（1） 最高情報統括責任者

最高情報統括責任者は、地方公共団体におけるすべてのネットワーク、情報システム等の情報資産の管理や情報セキュリティに関する権限及び責任を有する。

（注３）最高情報統括責任者（CIO: Chief Information Officer）は、副知事、副市長等、庁内を全般的に把握でき、部局間の調整や取りまとめを行うことができる上位の役職者を充てることが望ましい。

（注４）例文では、最高情報統括責任者が情報セキュリティ対策に関する最終決定権限及び責任を有するとしているが、内部統制を徹底するという観点からは、情報セキュリティ対策が進んだ段階では、最高情報統括責任者とは別に最高情報セキュリティ責任者（CISO: Chief Information Security Officer）を置くことが望ましい。

また、適切に情報セキュリティ対策を講じていくには専門知識を必要とするため、情報セキュリティに関する専門家をアドバイザーとして設置することが推奨される。



図表 11 情報セキュリティ推進の組織体制例

＜修正後＞

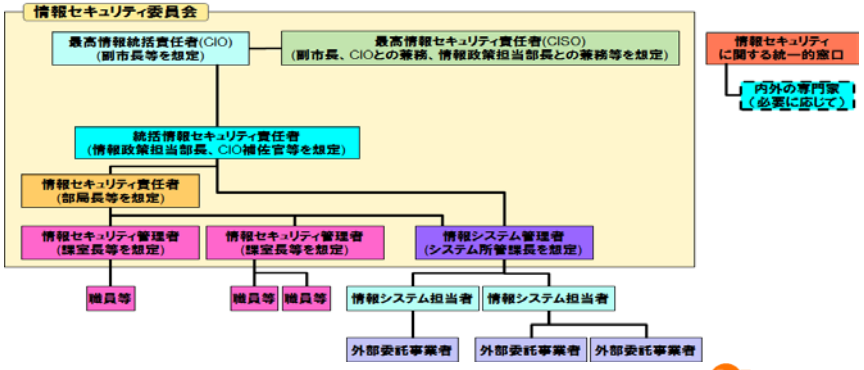
（1） 最高情報統括責任者（CIO: Chief Information Officer）

最高情報統括責任者は、地方公共団体におけるすべてのネットワーク、情報システム等の情報資産の管理や情報セキュリティに関する権限及び責任を有する。

例文では、最高情報統括責任者が情報資産の管理や情報セキュリティ対策に関する最終決定権限及び責任を有することとしているが、内部統制を徹底するという観点からは、情報セキュリティ対策が進んだ段階では、最高情報統括責任者とは別に最高情報セキュリティ責任者（CISO: Chief Information Security Officer）を置くことが望ましい。（ただし、小規模の地方公共団体では、CIOとの兼務や情報政策担当部長と兼務など、柔軟な対応が必要となる。）

また、適切に情報セキュリティ対策を講じていくには専門知識を必要とするため、情報セキュリティに関する外部の専門家のみならず、内部の職員をアドバイザーやCISO補佐官として置くことが望ましい。

（注３）最高情報統括責任者及び最高情報セキュリティ責任者は、副知事、副市長等、庁内を全般的に把握でき、部局間の調整や取りまとめを行うことができる上位の役職者を充てることが望ましい。



⑦（項番10）

（3.2 組織体制）

NISC等の考え方	【府省庁対策基準策定のためのガイドライン:2.1.1 組織・体制の整備 (6) 情報セキュリティインシデントに備えた体制の整備】 ● （6）-1 最高情報セキュリティ責任者は、以下を含むCSIRTの役割を規定すること。 a) 報告窓口からの情報セキュリティインシデントの報告の受付 b) 情報セキュリティインシデントの最高情報セキュリティ責任者等への報告 c) 内閣官房情報セキュリティセンターへの連絡 d) 被害の拡大防止を図るための応急措置の指示又は勧告 ● （6）-2 最高情報セキュリティ責任者は、CSIRTの代表者を置くこと。 【政府機関のための情報セキュリティ対策のための統一基準:2.1.1 組織・体制の整備 (6) 情報セキュリティインシデントに備えた体制の整備】 ● (a) 最高情報セキュリティ責任者は、CSIRTを整備し、その役割を明確化すること ● (b)最高情報セキュリティ責任者は、行政事務従事者のうちからCSIRTに属する職員として専門的な知識又は適性を有すると認められる者を選任すること。そのうち、府省庁における情報セキュリティインシデントに対処するための責任者としてCSIRT責任者を置くこと。 ● (c) 最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備すること。 ● (d)最高情報セキュリティ責任者は、CYMATに属する職員を指名すること。

⑦（項番10）（資料1-3：P26）

改定案（3.2 組織体制）【例文】

＜修正前＞

（7） 情報セキュリティ委員会
①本市の情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。
②情報セキュリティ委員会は、毎年度、本市における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。【推奨事項】

（8） 兼務の禁止
①情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。
②監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

（解説）
各地方公共団体においては、図表 11 のような組織体制を構築して、情報セキュリティ対策に取り組むことを想定している。

＜修正後＞

（8） 兼務の禁止
①情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。
②監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

（9） 情報セキュリティに関する統一的な窓口機能
①情報セキュリティに関する事故の統一的な窓口機能を有する組織を整備し、情報セキュリティに関する事故について部局より報告を受けた場合には、その状況を確認し、最高情報統括責任者に報告を行う。
②最高情報統括責任者による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局に提供する。
③情報セキュリティ事故を認知した場合には、その重要度や影響範囲等を勘案し、マスコミへの通知・公表対応を行わなければならない。
④情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口機能、外部の事業者等との情報共有を行う。

⑦（項番10）（資料1-3：P29）

改定案（3.2 組織体制）（解説）

＜修正前＞

（8） 兼務の禁止

情報セキュリティ対策に係る組織において、申請者と承認者が同一であることや監査人と被監査部門の者が同一である場合は、承認や監査の客観性が担保されない

ため、兼務の禁止を定める。

「やむを得ない場合」とは、例えば、統括情報セキュリティ責任者のみに認められた承認について、統括情報セキュリティ責任者が申請する場合や小規模団体で代替する者がいない場合などをいう。

＜修正後＞

ため、兼務の禁止を定める。

「やむを得ない場合」とは、例えば、統括情報セキュリティ責任者のみに認められた承認について、統括情報セキュリティ責任者が申請する場合や小規模団体で代替する者がいない場合などをいう。

（9） 情報セキュリティに関する統一的な窓口機能

情報システムに対するサイバー攻撃等の情報セキュリティ事故が発生した際に、情報セキュリティ事故のとりまとめ、CIO・CISOへの報告、マスコミ等への通知・公表、関係機関との情報共有など、情報セキュリティ事故に関するコミュニケーションの核となる体制を既存の枠組み等を活用するなどして構築する必要がある。

また、地方公共団体情報システム機構（自治体CEPTOAR）等の関係機関や他の地方公共団体の同様の窓口機能、外部の事業者等と連携して体制を強化することが求められる。

（注11）一般的に情報システムに対するサイバー攻撃等の情報セキュリティ事故が発生した際に、発生した事案を正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制はCSIRT（Computer Security Incident Response Team）と呼ばれている。

CSIRTの持つ機能や在り方は組織によって様々であるが、まずは、地方公共団体においては情報セキュリティに関する統一的な窓口機能の体制を整えることが必要である。

⑦（項番22）

（3.5.2 研修・訓練）

NISC等の考え方	【府省庁対策基準策定のためのガイドライン／政府機関のための情報セキュリティ対策のための統一基準】ともに、人材育成に関しての記述はなし。 ● 人材育成例として、アドバイザーやCISO補佐官の民間人活用、内部教育への活用などが考えられる

⑦（項番22）（資料1-3：P54）

改定案（3.5.2 研修・訓練）（解説）

＜修正前＞

3.5.2. 研修・訓練

【趣旨】

情報セキュリティを適切に確保するためには、情報セキュリティ対策の必要性と内容を幹部を含めすべての職員等が十分に理解していることが必要不可欠である。情報セキュリティに関する事故の多くが、職員等の規定違反に起因している。情報セキュリティの向上は、利便性の向上とは、必ずしも相容れない場合があり、職員等の意識として業務優先で情報セキュリティ対策の軽視につながることもある。また、情報セキュリティ

（中略）

（解説）

（1） 情報セキュリティに関する研修・訓練

情報セキュリティに関する研修・訓練を実施する責任は最高情報統括責任者にあり、かつ、研修・訓練は定期的に行わなければならない。

（2） 研修計画の立案及び実施

最高情報統括責任者は、幹部を含めたすべての職員等が、情報セキュリティの重要性を認識し、情報セキュリティポリシーを理解し、実践するために、研修及び訓練を定期的かつ計画的に実施する必要がある。

また、最高情報統括責任者は、研修計画を通じて将来の情報セキュリティを担う人材の育成や要員の管理を行うとともに、地方公共団体の長によるメールでの周知等、研修効果を向上させる施策を講じることが望ましい。

＜修正後＞

また、最高情報統括責任者は、研修計画を通じて将来の情報セキュリティを担う人材の育成や要員の管理を行うとともに、地方公共団体の長によるメールでの周知等、研修効果を向上させる施策を講じることが望ましい。

なお、外部の専門家や専門知識を持つ内部の職員をアドバイザーやCISO補佐官等として登用している場合は、それら専門家等を内部教育に有効活用することも考えられる。

⑦（項番42）

（3.6.5 不正アクセス対策）

NISC等の考え方	【府省庁対策基準策定のためのガイドライン:2.1.1 組織・体制の整備 (6) 情報セキュリティインシデントに備えた体制の整備】 ● （6）-1 最高情報セキュリティ責任者は、以下を含むCSIRTの役割を規定すること。 a) 報告窓口からの情報セキュリティインシデントの報告の受付 b) 情報セキュリティインシデントの最高情報セキュリティ責任者等への報告 c) 内閣官房情報セキュリティセンターへの連絡 d) 被害の拡大防止を図るための応急措置の指示又は勧告 ● （6）-2 最高情報セキュリティ責任者は、CSIRTの代表者を置くこと。 【政府機関のための情報セキュリティ対策のための統一基準:2.1.1 組織・体制の整備 (6) 情報セキュリティインシデントに備えた体制の整備】 ● (a) 最高情報セキュリティ責任者は、CSIRTを整備し、その役割を明確化すること ● (b)最高情報セキュリティ責任者は、行政事務従事者のうちからCSIRTに属する職員として専門的な知識又は適性を有すると認められる者を選任すること。そのうち、府省庁における情報セキュリティインシデントに対処するための責任者としてCSIRT責任者を置くこと。 ● (c) 最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備すること。 ● (d)最高情報セキュリティ責任者は、CYMATに属する職員を指名すること。

⑦（項番42）（資料1-3：P84）

改定案（3.6.5 不正アクセス対策）【例文】

＜修正前＞

3.6.5. 不正アクセス対策

【趣旨】

情報システムに不正アクセス対策が十分に行われていない場合は、システムへの攻撃、情報漏えい、損傷、改ざん等の被害を及ぼすおそれがある。このことから、不正アクセスの防止又は被害を最小限にするため、不正アクセス対策として取るべき措置、攻撃を受けた際の対処及び関係機関との連携等について規定する。

【例文】

（1） 統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

①使用されていないポートを閉鎖しなければならない。

②不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定しなければならない。

③重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。【推奨事項】

（2） 攻撃の予告

最高情報統括責任者及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

（3） 記録の保存

最高情報統括責任者及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

＜修正後＞

【例文】

（1） 統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

①使用されていないポートを閉鎖しなければならない。

②不要なサービスについて、機能を削除または停止しなければならない。

③不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定しなければならない。

④重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。【推奨事項】

⑤統括情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口機能と連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

（2） 攻撃の予告

最高情報統括責任者及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

⑦（項番49）

（3.6.5 不正アクセス対策）

NISC等の考え方	【府省庁対策基準策定のためのガイドライン:2.1.1 組織・体制の整備 (6) 情報セキュリティインシデントに備えた体制の整備】 ● （6）-1 最高情報セキュリティ責任者は、以下を含むCSIRTの役割を規定すること。 a) 報告窓口からの情報セキュリティインシデントの報告の受付 b) 情報セキュリティインシデントの最高情報セキュリティ責任者等への報告 c) 内閣官房情報セキュリティセンターへの連絡 d) 被害の拡大防止を図るための応急措置の指示又は勧告 ● （6）-2 最高情報セキュリティ責任者は、CSIRTの代表者を置くこと。 【政府機関のための情報セキュリティ対策のための統一基準:2.1.1 組織・体制の整備 (6) 情報セキュリティインシデントに備えた体制の整備】 ● (a) 最高情報セキュリティ責任者は、CSIRTを整備し、その役割を明確化すること ● (b)最高情報セキュリティ責任者は、行政事務従事者のうちからCSIRTに属する職員として専門的な知識又は適性を有すると認められる者を選任すること。そのうち、府省庁における情報セキュリティインシデントに対処するための責任者としてCSIRT責任者を置くこと。 ● (c) 最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備すること。 ● (d)最高情報セキュリティ責任者は、CYMATに属する職員を指名すること。

⑦（項番49）（資料1-3：P85）

改定案（3.6.5 不正アクセス対策）（解説）

＜修正前＞

（解説）

（1） 統括情報セキュリティ責任者の措置事項

使用されていない TCP/UDP ポートは、不正アクセスによる侵入が行われる可能性が高いために閉鎖する。

（注1）重要なファイルの改ざんについては、改ざん検知ソフトウェアの利用によって、不正アクセス、不正プログラムの侵入を検知することが可能である。

（2） 攻撃の予告

情報システムに対する攻撃予告があり、攻撃を受けることが確実な場合には、システム停止等の措置をとらなければならない。また、関係機関との連絡を密にし、情報収集に努めなければならない。

（注2）攻撃を受けた際の対応として、「緊急時対応計画」に基づき、ログの確保、被害を受けた場合の復旧手順の策定、庁内関係者の役割等を再確認しておく必要がある。

（3） 記録の保存

外部から不正アクセスを受けた場合に、その記録としてアクセスログ、対応した記録等を保存しておくことは、事実確認、原因追及及び対策検討のため、必要であり、記録の保存について定めておく必要がある。

（注3）不正アクセスについてログ解析を行う場合は、証拠保全用と解析用と分けて保管する必要がある。

（4） 内部からの攻撃

庁内ネットワークに接続したパソコン等の端末や不正プログラムに感染した庁内サーバを使って、庁内のサーバや外部のサーバ等に攻撃を仕掛けられる場合があり、これらを監視しなければならない。

＜修正後＞

（解説）

（１）統括情報セキュリティ責任者の措置事項

使用されていないTCP/UDPポートや、不要なサービスは、不正アクセスによる侵入や悪用に利用される可能性が高いため、ポート閉鎖やサービス停止処理を行う。

（注１）重要なファイルの改ざんについては、改ざん検知ソフトウェアの利用によって、不正アクセス、不正プログラムの侵入を検知することが可能である。

（注２）情報セキュリティに関する統一的な窓口機能を活用してCISOへの報告、各部部局への指示、ベンダとの情報共有、及びマスコミへの通知・公表などの対応を行うとともに、地方公共団体情報システム機構（自治体CEPTOAR）等の関係機関や他の地方公共団の情報セキュリティに関する統一的な窓口機能と連携して情報共有を行うことが望ましい。

（2） 攻撃の予告

情報システムに対する攻撃予告があり、攻撃を受けることが確実な場合には、システム停止等の措置をとらなければならない。また、関係機関との連絡を密にし、情報収集に努めなければならない。

（注2）攻撃を受けた際の対応として、「緊急時対応計画」に基づき、ログの確保、被害を受けた場合の復旧手順の策定、庁内関係者の役割等を再確認しておく必要がある。

⑦（項番58）

（3.7.3 侵害時の対応）

NISC等の考え方	【政府機関の情報セキュリティ対策のための統一基準:2.2.4 情報セキュリティインシデントへの対処】 (2) 情報セキュリティインシデントの認知時における報告・対処 (b) CSIRT責任者は、情報セキュリティインシデントを認知した場合にはその状況を確認し、情報セキュリティインシデントについて最高情報セキュリティ責任者に速やかに報告すること。 (c) CSIRTは、認知した情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び情報セキュリティインシデントからの復旧に係る指示又は勧告を行うこと。 (d) 情報システムセキュリティ責任者は、所管する情報システムについて情報セキュリティインシデントを認知した場合には、府省庁で定められた対処手順又はCSIRTの指示若しくは勧告に従って、適切に対処すること。 (f) CSIRTは、府省庁の情報システムについて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、内閣官房情報セキュリティセンターに連絡すること。また、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行うこと。さらに、国民の生活、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのある大規模サイバー攻撃事態等においては、「大規模サイバー攻撃等への初動対処について（平成22年3月19日内閣危機管理監決裁）」に基づく報告も行うこと。 (g) CSIRTは、情報セキュリティインシデントに関して、府省庁を含む関係機関と情報共有を行うこと。 (h) CSIRTは、CYMATの支援を受ける場合には、支援を受けるに当たって必要な情報提供を行うこと。 (3) 情報セキュリティインシデントの原因調査・再発防止 (a) 情報セキュリティ責任者は、CSIRTの指示を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として最高情報セキュリティ責任者に報告すること。

⑦（項番58）（資料1-3：P94）

改定案（3.7.3 侵害時の対応）（解説）

＜修正前＞

3.7.3. 侵害時の対応

【趣旨】

（中略）

（解説）

（1） 緊急時対応計画の策定

情報セキュリティが侵害された場合又は侵害されるおそれがある場合等における具体的な措置について、緊急時対応計画として定める。

緊急時対応計画には、情報資産への侵害が発生した場合等における連絡、証拠保全、被害拡大の防止、復旧等の迅速かつ円滑な実施と、再発防止策の措置を講じるために必要な事項を定める必要がある。

また、自らが所有する情報資産における被害拡大防止のほか、外部への被害拡大のおそれがある場合には、その防止に努めることを定める必要がある。情報が漏えいすることなどにより被害を受けるおそれのある関係者に対し早急に連絡することが重要である。

当該事案が不正アクセス禁止法違反等の犯罪の可能性がある場合には、警察・関係機関と緊密な連携に努めることも重要である。

（注1）緊急時対応計画を策定する場合は、他の危機管理に関する規程等と整合性を確保し策定する必要がある。また、他の危機管理に関する規程の改定と情報セキュリティポリシーの見直しの時期が異なることにより一時的に不整合が生じないよう、配慮する必要がある。

2） 緊急時対応計画に盛り込むべき内容

緊急時対応計画に定める事項としては、例えば次のものがある。

①関係者の連絡先

- 地方公共団体の長
- 最高情報統括責任者
- 統括情報セキュリティ責任者
- 情報システム管理者
- ネットワーク及び情報システムに係る外部委託事業者
- 広報担当課
- 都道府県の関係部局
- 警察
- 関係機関
- 被害を受けるおそれのある個人及び法人

＜修正後＞

が重要である。

当該事案が不正アクセス禁止法違反等の犯罪の可能性がある場合には、警察・関係機関と緊密な連携に努めることも重要である。

（注1）緊急時対応計画を策定する場合は、他の危機管理に関する規程等と整合性を確保し策定する必要がある。また、他の危機管理に関する規程の改定と情報セキュリティポリシーの見直しの時期が異なることにより一時的に不整合が生じないよう、配慮する必要がある。

（注2）情報セキュリティに関する統一的な窓口機能が担う役割についても緊急時対応計画を策定する場合に考慮することが望ましい。

2） 緊急時対応計画に盛り込むべき内容

緊急時対応計画に定める事項としては、例えば次のものがある。

①関係者の連絡先

- 地方公共団体の長
- 最高情報統括責任者
- 統括情報セキュリティ責任者
- 情報システム管理者
- **情報セキュリティに関する統一的な窓口**
- ネットワーク及び情報システムに係る外部委託事業者
- 広報担当課
- 都道府県の関係部局

⑦（項番58）（資料1-3：P95）

改定案（3.7.3 侵害時の対応）（解説）

＜修正前＞

②発生した事案に係る報告すべき事項

セキュリティに関する事案を発見した者は、次の項目について速やかに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。

・事案の状況
・事案が発生した原因として、想定される行為
・確認した被害・影響範囲（事案の種類、損害規模、復旧に要する額等）
・記録

また、統括情報セキュリティ責任者は、事案の詳細な調査を行うとともに、最高情報統括責任者及び情報セキュリティ委員会へ報告しなければならない。

（注２）統括情報セキュリティ責任者が事案の詳細な調査を行うに当たっては、必要に応じて外部専門家のアドバイスを受ける、JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター）等に相談する等、事実確認を見誤らないように努める必要がある。

③発生した事案への対応措置

（ア） 統括情報セキュリティ責任者は、次の事案が発生した場合、定められた連絡先へ連絡しなければならない。

・サイバーテロその他の市民に重大な被害が生じるおそれのあるとき

＜修正後＞

（注３）統括情報セキュリティ責任者が事案の詳細な調査を行うに当たっては、必要に応じて外部専門家のアドバイスを受ける、JPCERT/CC（一般社団法人JPCERT コーディネーションセンター）、及び地方公共団体情報システム機構（自治体CEPTOAR）等の関係機関に相談する等、事実確認を見誤らないように努める必要がある。
（他論点：項番59対応）

（注４）情報セキュリティに関する統一的な窓口機能に報告を集約し、窓口経由で外部への問合せや相談を行うことが考えられる。

（注５）情報共有や相談については、「地方公共団体における情報セキュリティ対策及び政府の一層の充実・強化について（依頼）」（平成23年10月　総務省）の通知文を参照されたい。
（他論点：項番59対応）

参考（資料1-3：P3～4）

最新法令を考慮した経緯の修正

＜修正前＞

また、平成21年2月3日、政府の情報セキュリティ政策会議は、「第1次情報セキュリティ基本計画」に基づく各種の取組み進展や社会環境の変化などを踏まえ、引き続き我が国全体として情報セキュリティ問題への取組みを力強く推進するために、平成21年度以降を念頭に置いた「第2次情報セキュリティ基本計画」を決定し、この中で、地方公共団体に関して、小規模な地方公共団体も含め、全ての地方公共団体において、望ましい情報セキュリティ対策が実施されることを目指し、対策の促進を行うこととされた。

さらに、平成22年5月11日、政府の情報セキュリティ政策会議は、「第2次情報セキュリティ基本計画」に基づく官民の各主体による取組を継続しつつ、新たな環境変化に対応した政府の取組を進めるために、「第2次情報セキュリティ基本計画」を含有する、「国民を守る情報セキュリティ戦略」を決定し、平成32年までに、インターネットや情報システム等の情報通信技術を利用者が活用するに当たっての脆弱性を克服し、全ての国民が情報通信技術を安心して利用できる環境（高品質、高信頼性、安全・安心を兼ね備えた環境）を整備し、世界最先端の「情報セキュリティ先進国」を実現することを目標としている。

なお、重要インフラ指針については、平成18年2月2日に政府の情報セキュリティ政策会議によって決定以降、平成19年6月14日及び平成22年5月11日に改定され、平成22年7月30日には「対策編」が策定されている。

総務省では、これらの新たな対策技術の動向、政府の情報セキュリティ政策の改定等を踏まえ、横断的に俯瞰して必要度が高い項目や先進的な取組みを参考とすることにより、地方公共団体の情報セキュリティ水準の向上及び情報セキュリティ対策の浸透を推進するため、今般、ガイドラインを改定したものである。

＜修正後＞

その他、地方公共団体に関連する法令として、平成25年5月24日に成立し、平成25年5月31日に公布された社会保障・税の分野における給付と負担の公平化や各種行政事務の効率化のための「行政手続における特定の個人を識別するための番号の利用等に関する法律」や平成26年11月6日に成立し、平成26年11月12日に公布された国家の安全保障にかかわるサイバー攻撃への対応に国が責任を持ち、サイバーセキュリティに関する施策を総合的かつ効果的に推進することを目的とした「サイバーセキュリティ基本法」がある。

総務省では、これらの新たな対策技術の動向、政府の情報セキュリティ政策の改定及び新たに成立した法令等を踏まえ、横断的に俯瞰して必要度が高い項目や先進的な取組みを参考とすることにより、地方公共団体の情報セキュリティ水準の向上及び情報セキュリティ対策の浸透を推進するため、今般、ガイドラインを改定したものである。