（別紙1）

納品物件一覧

項番	納品物件名	納品数	納　入 形態	備考
1	設計書	2部（正、副）	電 子・ 紙	設計工程終了後
2	テスト計画書	2部（正、副）	電 子・ 紙	テスト工程開始前
3	テスト成績報告書	2部（正、副）	電 子・ 紙	テスト工程終了後
4	プログラム ソースコードを含む	1 式	電子	開発工程終了後 （修正した場合は再納品）
5	運用マニュアル	2部（正、副）	電 子・ 紙	集合教育実施前
6	プロジェクト管理資料 議事録など	2部（正、副）	電 子・ 紙	随時、本業務終了後

紙での提出は、バージョンアップ時等の差し替えが容易なようにバインダー方式とすること。

電子媒体での提出は、Microsoft Office 2016 で扱える形式にて、CD-R もしくは、DVD-R に格納すること。ただし、委託者担当者が別に定める形式による提出を求めた場合はこの限りでない。なお、事前にウイルスチェックを行い、チェックの際に用いたソフトウェア及び日時を記載したラベルを貼ること。

納入した成果物に修正等がある場合、紙については更新履歴と修正ページ、電子媒体につ

いては、修正後の全編を速やかに提出すること。

次期調達時において、第三者が当該成果物を閲覧し、内容を理解できるドキュメントを納入すること。

納入成果物の検査の結果、不適合の場合は適切な処置を行った上で再納入すること。

以上

個人情報及び機密情報に係る標準特記仕様書

受託者は、契約書及び仕様書等に定めのない事項について、この特記仕様書に定める事項に従って契約を履行しなければならない。

１　定義

本業務において、公益財団法人東京都中小企業振興公社（以下、公社という。）の保有する個人情報（以下、単に「個人情報」という。）とは、公社が貸与する原票、資料、貸与品等に記載された個人情報及びこれらの情報から受託者が作成した個人情報並びに受託者が公社に代わって行う本業務の過程で収集した個人情報のすべてをいい、受託者独自のものと明確に区分しなければならない。また、委託者が機密を要する旨を指定して提示した情報及び委託者からの貸与品等に含まれる情報は、全て委託者の機密情報である（以下「機密情報」という。）。ただし、委託者からの貸与品等に含まれる情報のうち、既に公知の情報、委託者から受託者に提示した後に受託者の責めによらないで公知となった情報、及び委託者と受託者による事前の合意がある情報は、機密情報に含まれないものとする。

２　受託者の責務

(1)　受託者は、この契約の履行に当たって、個人情報を取り扱う場合は、「東京都個人情報の保護に関する条例」（平成2年東京都条例第113号）を遵守して取り扱う責務を負い、以下の事項を遵守し、個人情報の漏えい、滅失、き損の防止その他個人情報保護に必要な措置を講じなければならない。

(2)　受託者は、東京都サイバーセキュリティ基本方針及び東京都サイバーセキュリティ対策基準の趣旨を踏まえ、以下の事項を遵守しなければならない。

３　業務の推進体制

(1)　受託者は、契約締結後直ちに委託業務を履行できる体制を整えるとともに、当該委託業務に関する責任者、作業体制、連絡体制及び作業場所について書面にし、委託者に提出すること。

(2)　(1)の事項に変更が生じた場合、受託者は速やかに変更内容を委託者に提出すること。

４　業務従事者への遵守事項の周知

(1)　受託者は、この契約の履行に関する遵守事項について、委託業務の従事者全員に対し十分に説明し周知徹底を図ること。

５　秘密の保持

受託者は、この契約の履行に関して知り得た秘密を漏らしてはならない。この契約終了後も同様とする。

６　目的外使用の禁止

受託者は、この契約の履行に必要な委託業務の内容を他の用途に使用してはならない。また、この契約の履行により知り得た内容を第三者に提供してはならない。

７　複写及び複製の禁止

受託者は、この契約に基づく業務を処理するため、委託者が貸与する原票、資料、その他貸与品等及びこれらに含まれる情報（以下「委託者からの貸与品等」という。）を、委託者の承諾なくして複写及び複製をしてはならない。

8　作業場所以外への持出禁止

受託者は、委託者が指示又は承認する場合を除き、委託者からの貸与品等（複写及び複製したものを含む。）について、３(1)における作業場所以外へ持ち出してはならない。

9　情報の保管及び管理

受託者は、委託業務に係る情報の保管及び管理に万全を期するため、委託業務の実施に当たって以下の事項を遵守しなければならない。

(1) 全般事項

ア　契約履行過程

(ｱ) 以下の事項について安全管理上必要な措置を講じること。

a　委託業務を処理する施設等の入退室管理

b　委託者からの貸与品等の使用及び保管管理

c　仕様書等で指定する物件（以下「契約目的物」という。）、契約目的物の仕掛品及び契約履行過程で発生した成果物（出力帳票及び電磁的記録物等）の作成、使用及び保管管理

d　その他、仕様書等で指定したもの

(ｲ) 委託者から(ｱ)の内容を確認するため、委託業務の安全管理体制に係る資料の提出を求められた場合は直ちに提出すること。

イ　契約履行完了時

(ｱ) 委託者からの貸与品等を、契約履行完了後速やかに委託者に返還すること。

(ｲ) 契約目的物の作成のために、委託業務に係る情報を記録した一切の媒体（紙及び電磁的記録媒体等一切の有形物）（以下「記録媒体」という。）については、契約履行完了後に記録媒体上に含まれる当該委託業務に係る情報を全て消去すること。

(ｳ) (ｲ)の消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日等を明示した書面で委託者に報告すること。

(ｴ) この特記仕様書の事項を遵守した旨を書面で報告すること。また、再委託を行った場合は再委託先における状況も同様に報告すること。

ウ　契約解除時

イの規定の「契約履行完了」を「契約解除」に読み替え、規定の全てに従うこと。

エ　事故発生時

契約目的物の納入前に契約目的物の仕掛品、契約履行過程で発生した成果物及び委託者からの貸与品等の紛失、滅失及び毀損等の事故が生じたときには、その事故の発生場所及び発生状況等を詳細に記載した書面をもって、遅滞なく委託者に報告し、委託者の指示に従うこと。

(2) アクセスを許可する情報に係る事項

受託者は、アクセスを許可する情報の種類と範囲、アクセス方法について、業務着手前に委託者から承認を得ること。

(3) 個人情報及び機密情報の取扱いに係る事項

個人情報及び機密情報の取扱いについて、受託者は、以下の事項を遵守しなければならない。

ア　個人情報及び機密情報に係る記録媒体を、施錠できる保管庫又は施錠及び入退室管理の可能な保管室に格納する等適正に管理すること。

イ　アの個人情報及び機密情報の管理に当たっては、管理責任者を定めるとともに、台帳等を設け個人情報及び機密情報の管理状況を記録すること。

ウ　委託者から要求があった場合又は契約履行完了時には、イの管理記録を委託者に提出し報告すること。

エ　個人情報及び機密情報の運搬には盗難、紛失、漏えい等の事故を防ぐ十分な対策を講じること。

オ　(1)エの事故が、個人情報及び機密情報の漏えい、滅失、毀損等に該当する場合は、漏えい、滅失、毀損した個人情報及び機密情報の項目、内容、数量、事故の発生場所及び発生状況等を詳細に記載した書面をもって、遅滞なく委託者に報告し、委託者の指示に従うこと。

また、受託者は二次被害の防止、類似事案の発生回避等の観点から、委託者に可能な限り情報を提供すること。

カ　(1)エの事故が発生した場合、委託者は必要に応じて受託者の名称を含む当該事故に係る必要な事項の公表を行うことができる。

キ　委託業務の従事者に対し、個人情報及び機密情報の取扱いについて必要な教育及び研修を実施すること。

ク　その他、東京都個人情報の保護に関する条例（平成2年東京都条例第113号）に従って、本委託業務に係る個人情報を適切に扱うこと。

10　委託者の施設内での作業

(1) 受託者は、委託業務の実施に当たり、委託者の施設内で作業を行う必要がある場合には、委託者に作業場所、什器、備品及び通信施設等の使用を要請することができる。

(2) 委託者は、(1)の要請に対して、使用条件を付した上で、無償により貸与又は提供することができる。

(3) 受託者は、委託者の施設内で作業を行う場合は、次の事項を遵守するものとする。

ア　就業規則は、受託者の定めるものを適用すること。

イ　受託者の発行する身分証明書を携帯し、委託者の指示があった場合はこれを提示すること。

ウ　受託者の社名入りネームプレートを着用すること。

エ　その他、(2)の使用に関し委託者が指示すること。

11　再委託の取扱い

(1) 受託者は、この契約の履行に当たり、再委託を行う場合には、あらかじめ再委託を行う旨を書面により委託者に申し出て、委託者の承諾を得なければならない。

(2) (1)の書面には、以下の事項を記載するものとする。

ア　再委託の理由

イ　再委託先の選定理由

ウ　再委託先に対する業務の管理方法

エ　再委託先の名称、代表者及び所在地

オ　再委託する業務の内容

カ　再委託する業務に含まれる情報の種類（個人情報及び機密情報については特に明記すること。）

キ　再委託先のセキュリティ管理体制（個人情報、機密情報、記録媒体の保管及び管理体制については特に明記すること。）

ク　再委託先がこの特記仕様書の１及び３から９までに定める事項を遵守する旨の誓約

ケ　その他、委託者が指定する事項

(3) この特記仕様書の１から10までに定める事項については、受託者と同様に、再委託先においても遵守するものとし、受託者は、再委託先がこれを遵守することに関して一切の責任を負う。

12　実地調査及び指示等

(1) 委託者は、必要があると認める場合には、受託者の作業場所の実地調査を含む受託者の作業状況の調査及び受託者に対する委託業務の実施に係る指示を行うことができる。

(2) 受託者は、(1)の規定に基づき、委託者から作業状況の調査の実施要求又は委託業務の実施に係る指示があった場合には、それらの要求又は指示に従わなければならない。

(3) 委託者は、(1)に定める事項を再委託先に対しても実施できるものとする。

13 情報の保管及び管理等に対する義務違反

(1) 受託者又は再委託先において、この特記仕様書の１から10までに定める情報の保管及び管理等に関する義務違反又は義務を怠った場合には、委託者は、この契約を解除することができる。

(2) (1)に規定する受託者又は再委託先の義務違反又は義務を怠ったことによって委託者が損害を被った場合には、委託者は受託者に損害賠償を請求することができる。委託者が請求する損害賠償額は、委託者が実際に被った損害額とする。

14 かし担保責任

(1) 契約目的物にかしがあるときは、委託者は、受託者に対して相当の期間を定めてそのかしの修補を請求し、又は修補に代えて、若しくは修補とともに損害の賠償を請求することができる。

(2) (1)の規定によるかしの修補又は損害賠償の請求は、契約履行完了後、契約目的物の引渡しを受けた日から１年以内に、これを行わなければならない。

15 著作権等の取扱い

この契約により作成される納入物の著作権等の取扱いは、以下に定めるところによる。

(1) 受託者は、納入物のうち本委託業務の実施に伴い新たに作成したものについて、著作権法（昭和45年法律第48号）第2章第3節第2款に規定する権利（以下「著作者人格権」という。）を有する場合においてもこれを行使しないものとする。ただし、あらかじめ委託者の承諾を得た場合はこの限りでない。

(2) (1)の規定は、受託者の従業員、この特記仕様書の10の規定により再委託された場合の再委託先又はそれらの従業員に著作者人格権が帰属する場合にも適用する。

(3) (1)及び(2)の規定については、委託者が必要と判断する限りにおいて、この契約終了後も継続する。

(4) 受託者は、納入物に係る著作権法第2章第3節第3款に規定する権利（以下「著作権」という。）を、委託者に無償で譲渡するものとする。ただし、納入物に使用又は包括されている著作物で受託者がこの契約締結以前から有していたか、又は受託者が本委託業務以外の目的で作成した汎用性のある著作物に関する著作権は、受託者に留保され、その使用権、改変権を委託者に許諾するものとし、委託者は、これを本委託業務の納入物の運用その他の利用のために必要な範囲で使用、改変できるものとする。また、納入物に使用又は包括されている著作物で第三者が著作権を有する著作物の著作権は、当該第三者に留保され、かかる著作物に使用許諾条件が定められている場合は、委託者はその条件の適用につき協議に応ずるものとする。

(5) (4)は、著作権法第27条及び第28条に規定する権利の譲渡も含む。

(6) 本委託業務の実施に伴い、特許権等の産業財産権を伴う発明等が行われた場合、取扱いは別途協議の上定める。

(7) 納入物に関し、第三者から著作権、特許権、その他知的財産権の侵害の申立てを受けた場合、委託者の帰責事由による場合を除き、受託者の責任と費用をもって処理するものとする。

16 運搬責任

この契約に係る委託者からの貸与品等及び契約目的物の運搬は、別に定めるものを除くほか受託者の責任で行うものとし、その経費は受託者の負担とする。

17 疑義についての協議

この特記仕様書の各項目若しくは仕様書で規定する個人情報の管理方法等について疑義等が生じたとき又はこの特記仕様書若しくは仕様書に定めのない事項については、両者協議の上定める。

別　紙

暴力団等排除に関する特約事項

（暴力団等排除に係る契約解除）

１　東京都契約関係暴力団等対策措置要綱（昭和６２年１月１４日付６１財経庶第９２２号。以下「要綱」という。）別表１号に該当する（共同企業体又は事業協同組合であるときは、その構成員のいずれかの者が該当する場合を含む。）として要綱に基づく排除措置を受けた場合は、催告なくこの契約を解除されても異議がないこと。また、この場合において、損害を生じても賠償の請求はできないこと。

２　１に定めるところによりこの契約を解除されたときは、契約保証金を納付している場合を除き、契約金額の100分の10に相当する違約金を支払うこと。

（再委託（下請負）禁止等）

３　要綱に基づく排除措置を受けた者又は東京都（以下「都」という。）の契約から排除するよう警視庁から要請があった者（以下「排除要請者」という。）に、再委託（下請負人には）できないこと。

４　排除措置を受けた者又は排除要請者のうち、要綱別表１号に該当する者を再委託（下請負人と）していた場合は、当該契約解除の求めに応じること。また、この場合において、契約の解除を求められたにもかかわらず、正当な理由がなくこれを拒否したと認められるときは、公社の契約から排除する措置を講じられても異議がないこと。

５　４に定めるところにより契約解除があった場合は、一切の責任を負うこと。

（不当介入に関する通報報告）

６　契約の履行に当たって、暴力団等から不当介入を受けた場合（再委託した者（下請負人）が暴力団等から不当介入を受けた場合を含む。以下同じ。）は、遅滞なく公社への報告及び警視庁管轄警察署（以下「管轄警察署」という。）への通報（以下「通報報告」という。）並びに捜査上必要な協力をすること。

７　６の場合において、通報報告に当たっては、別に定める「不当介入通報・報告書」を２通作成し、１通を公社に、もう１通を管轄警察署にそれぞれ提出すること。ただし、緊急を要し、書面による通報報告ができないときは、その理由を告げて口頭により通報報告を行い、後日、遅滞なく不当介入通報・報告書を公社及び管轄警察署に提出すること。

８　再委託した者（下請負人）が暴力団等から不当介入を受けた場合は、遅滞なく報告するよう当該再委託した者（下請負人）を指導すること。

９　不当介入を受けたにもかかわらず、正当な理由がなく公社への報告又は警視庁管轄警察署への通報を怠ったと認められるときは、公社の契約から排除する措置を講じられても異議がないこと。

東京都公式ホームページ作成に関する統一基準（改訂版）

平成 29 年 7 月

東京都公式ホームページ作成に関する統一基準

東京都公式ホームページ（以下「公式ホームページ」という。）は、都の施策などの都政情報の提供や都民との有力な情報共有手段として、重要なツールとなっている。今後更に、東京２０２０大会に向け、またそれ以降において、国内外に向けて東京の魅力を発信する媒体としても、公式ホームページの重要性はますます高まってくる。

これまで、総務局及び生活文化局において、公式ホームページのあり方等について検討を進め、平成 26 年４月、公式ホームページの作成に関し最低限遵守すべきルールとして「東京都公式ホームページ作成に関する統一基準」（以下「統一基準」という。）を策定した。統一基準は、高齢者や障害者を含めた誰もが必要な情報にアクセスできるウェブアクセシビリティの JIS 規格である JIS X 8341-3 に対応している。

このたび、JIS X 8341-3 が改訂されたこと、及び公的機関のウェブアクセシビリティ対応を支援するために総務省が「みんなの公共サイト運用ガイドライン」を策定したことを踏まえて、統一基準を改正する。

平成 28 年４月に「障害を理由とする差別の解消の推進に関する法律（障害者差別解消法)」が施行され、ウェブアクセシビリティについてもこれまで以上に一層の推進が求められている。これまでも統一基準準拠及びウェブアクセシビリティの向上に取り組んでいるところであるが、さらにウェブアクセシビリティの確保・維持・向上に努めて、誰もが必要な情報にアクセスでき、かつ誰もが使いやすい公式ホームページを目指していく。

第１　策定について

１　対象範囲

原則として、東京都が以下に示すウェブコンテンツで提供する情報及びサービスすべてとする。

⑴ 東京都公式ホームページ

⑵ 都民がブラウザを介して利用するもので、特定の用途向けに作成されたウェブアプリケーション及びウェブシステム

⑶ 東京都公式ホームページのスマートフォン向けサイト

⑷ 東京都公式ホームページのスマートフォンを除く携帯電話（フィーチャーフォン）向けサイト

⑸ 都民向けに KIOSK 端末等で提供されるウェブコンテンツ

⑹ 都民向けに CD・DVD 等の媒体に収録して配布するウェブコンテンツ

なお、⑷、⑸及び⑹については特性が異なるものもあるため、可能な限り対応することとする。

２　JIS 規格の適用

JIS X 8341-3:2016「高齢者・障害者等配慮設計指針－情報通信における機器，ソフトウェア及びサービス－第 3 部：ウェブコンテンツ」は、ホームページ作成に際して対応すべき項目を 61 項目に定め、これらの 61 項目は様々なユーザー層及び状況からくるニーズを満たすため、それぞれ「A」、「AA」、「AAA」と 3 段階の適合レベルに分類している。総務省が作成した「みんなの公共サイト運用ガイドライン（2016 年版）」では、公的機関に対し JIS X 8341-3:2016 における適合レベル AA に対応することが求められている。これを踏まえて、本統一基準では適合レベル AA に対応している。

また、アクセシビリティの確保に当たり、より詳細に規格の内容を検討する場合は、各自で JIS 規格、またはウェブアクセシビリティ基盤委員会が公開している解説書[1]と達成方法集[2]を参照すること。

同様に、「みんなの公共サイト運用ガイドライン（2016 年版）」では 1 年に 1 回、運用ガイドラインに基づいたウェブアクセシビリティ確保・維持・向上のための取組に

[1] http://waic.jp/docs/wcag2/understanding.html
[2] http://waic.jp/docs/wcag2/techs.html

ついて、取組内容を確認し、確認結果をホームページ等で公開することが勧奨されているため、JIS 規格の適用とあわせて取組内容確認及び確認結果公開の実施を推奨する。

３　優先度の設定

この統一基準の各項目には、JIS X 8341-3:2016 を参考に、次のとおり優先度を設定している。

［優先度 A］：ホームページの作成の際、必ず実施又は満たすべき項目
（優先度 A は JIS X 8341-3:2016 の適合レベル「A」及び「AA」を含む）
［優先度 B］：ホームページの作成の際、できる限り実施又は満たすべき項目

４　目標とする適合レベル

対象となるホームページは、優先度 A（JIS X8341-3:2016 の適合レベル「A」及び「AA」を含む）に準拠することを目標とする。

第２　ページデザイン

１　ユーザーの環境に左右されないデザイン

(1) ホームページでは、ユーザーエージェント（閲覧ソフト（以下「ブラウザ」という。）や支援技術など）がソースコードの構文を正確に解析できるように、仕様で認められている場合を除いて、HTML のソースコードが次の 4 点を満たすこと。

ア　開始タグ及び終了タグを仕様に準じて用いる。
イ　要素は仕様に準じて入れ子とする。
ウ　要素には重複した属性がないものとする。
エ　どの ID も一意的（ユニーク）であるものとする。

また、当該コントロールの識別名（ID など）、役割や状態（ステータス）などを、各種の支援技術プログラム（音声読み上げソフトなど）が解釈できるよう記述する。［優先度 A］[JIS 適合レベル A]

(2) コンテンツの情報と関係性を適切に記述（マークアップ）する。音声読み上げソフトなどのプログラムが解釈可能にすることができないコンテンツを提供する場合は、合わせてそれらの解釈をテキストで提供する。［優先度 A］[JIS 適合レベル A]

(3) ホームページの閲覧者（以下「ユーザー」という。）が使用している様々なサイズのディスプレイで問題なく表示できるようレイアウトする。［優先度 B］

(4) ユーザーが特定のアプリケーションを用意しないと見ることができない形式（Microsoft Word、Microsoft Excel など）のみにより、情報を提供することは行わない。［優先度 B］

(5) コンテンツの意味及び操作の順番と、音声読み上げソフトの読み上げの順番及びフォーカスの順番を一致させる。［優先度 A］[JIS 適合レベル A]

(6) ユーザーが使用する様々なデバイス（スマートフォンや携帯電話（フィーチャーフォン）など）におけるコンテンツの表示については、画面幅や解像度などを考慮し、最適化されたホームページを提供する。［優先度 A］

(7) Microsoft Word、Microsoft Excel の HTML 変換機能を利用したウェブページ作成は行わない。［優先度 B］

２　スタイルシート

(1) カスケーディング・スタイル・シート（CSS）を使用する場合は、別ファイルにリンクさせる形式を使う。［優先度 B］

(2) 使用しているウェブコンテンツ技術によって、意図している視覚的な表現が可能である場合は、次に掲げる場合を除き、画像化された文字ではなくテキストを用いて情報を伝える。［優先度 A］[JIS 適合レベル AA]

ア　カスタマイズ可能

画像化された文字がユーザーの要求に応じて視覚的にカスタマイズできる。

イ　必要不可欠

文字の特定の表現（ロゴなど）が、伝えようとする情報にとって必要不可欠である。

3　フレーム

(1) フレームは原則使わない。［優先度 A］

ただし、フレームを利用する必要がある場合には、以下（2）～（5）の項目に従うこと。

(2) フレーム内に表示される各ページには、音声読み上げソフトを利用しているユーザーが、その内容や役割が何であるのかを判断しやすいページタイトルを付ける。［優先度 A］

(3) フレームの境界線は「0」に指定し、ページ内に「戻る」ボタンの機能を付ける。［優先度 B］

(4) フレーム内に、外部のホームページを表示させない。［優先度 B］

(5) 外部サイトを埋め込むタイプのインラインフレーム（Twitter、Facebook、YouTube、Google マップなど）を使用する場合は、表示内容が、サイト運営者の完全な管理下に置けないときは、以下の項目を遵守すること。［優先度 A］

ア　インラインフレームで表示させる情報のうち広く周知が必要な情報については、公式ホームページ内に同様の内容を掲載する。

イ　フレーム内の表示内容が、公式ホームページ外へのリンクであり他の運営者の管理下にあることが分かるようにする。

第３　サイトデザイン

１　サイト構造

(1) 各ホームページの全体構成（以下「サイト構造」という。）は、ユーザーに分かりやすい形で情報を整理・分類化してデザインする。組織別の分類は、ユーザーにとって必ずしも分かりやすいものではないことに留意する。［優先度 B］

(2) サイト構造は、ユーザーが目的とする情報にたどり着きやすいよう、階層の幅を５～９、階層の深さを３～５以内に収めるよう工夫する。［優先度 B］

２　ナビゲーション機能

(1) すべてのページで、トップページ及び１つ上の階層や前ページに移動できるようにする。この場合、トップページへのリンクには、「ホームページ」ではなく「トップページ」の言葉を用いる。［優先度 B］

(2) ホームページの中にある複数のウェブページ上で繰り返されているナビゲーションのメカニズムは、繰り返されるたびに相対的に同じ順序で提供する。［優先度 A］[JIS 適合レベル AA]

(3) トップページには、ホームページ内のメニュー、コンテンツ一覧を分かりやすく表示する。例として、リピーターの多いホームページでは新着情報などのコンテンツ、ターゲットとするユーザーが明確な場合にはユーザー別のコンテンツ一覧を配置する。［優先度 B］

(4) ユーザーが東京都公式ホームページであると認識できるように、各ホームページは共通して次の内容を設定する。［優先度 A］

ア　ヘッダー部分に掲載する内容

(ｱ) 「東京都シンボルマーク」「所管局などのロゴタイプ」をページの左上に掲載し、所管局などのトップページへのリンクを設ける。

なお、本項目においては都立学校や警察、消防の章など、都の内部組織の章として広く認知されているマークについても、「東京都シンボルマーク」同等として扱うことができるものとする。

(ｲ) 「多言語へのリンク」「サイト内検索機能又はサイトマップ」「都庁総合トップページへのリンク」をページの右上に掲載する。ただし、スマートフォン向けコンテンツにおける配置についてはこの限りではない。

また、「多言語へのリンク」「サイト内検索機能又はサイトマップ」については、可能な限り対応するものとする。

イ　フッター部分に掲載する内容

「サイトポリシーへのリンク」「問合せ先」「著作権表記」のページの下部中央に掲載する。

(5) 入力フォームでは、トップページと前のページに戻るためのリンクを提供する。［優先度 B］

(6) 階層構造をもつホームページの場合には、パンくず式ナビゲーションを提供する。［優先度 B］

(7) ホームページの中から各ページに到達することのできる手段は、複数提供する。ただし、そのページが、検索結果ページや、フォーム入力後の確認ページなどプロセスの結果又はプロセスの中の一つのステップである場合はこの限りではない。［優先度 A］[JIS 適合レベル AA]

(8) コンポーネント（リンクやフォーム・コントロールなど）にフォーカスしただけでコンテキストの変化を引き起こしてはならない。

また、フォームのコントロールなどを選択しただけでコンテキストの変化を引き起こしてはならない。事前に何が起こるのかを説明しておくか、実行ボタンを提供し、ボタンが押下されるまでは変化が起こらないようにする。［優先度 A］[JIS 適合レベル A]

3　検索

(1) サイト内検索機能又はサイトマップはすべてのページからアクセスできるようにする。［優先度 A］

(2) 検索範囲が指定できる場合、はっきりと明示する。［優先度 B］

(3) 検索結果の精度を高めるため、メタデータ（HTML の<meta>タグ）で当該ページ又はホームページ全体に関する情報を提供する。メタデータには、当該ページ又はホームページ全体についての説明文、キーワードなどを記述する。［優先度 B］

(4) 検索結果は最も確率の高いページから順に表示する。［優先度 B］

(5) 検索結果ページには、検索キーワードを目立つように表示する。［優先度 B］

(6) 検索結果の数は必ず表示する。［優先度 B］

(7) ユーザーが、検索結果全体のどの部分を参照しているのかを表示する。［優先度 B］

４　問い合わせ先

フッターには、ホームページ全体または当該ページの掲載内容に関する問い合わせ先の組織名、所在地、電話、メールアドレスを掲載又は掲載ページへリンクする。［優先度 A］

５　サイトポリシーの掲載と運用

(1) ホームページ管理者はサイト運営に当たってユーザーに明示すべきサイトポリシーを作成し、公開する。作成に当たって準拠すべき法規制などがある場合には、これに従う。作成したサイトポリシーはユーザーがいつでも確認できるようフッターにそれらのページへのテキストリンクを設定する。該当する場合には、サイトポリシーに次のものを含める。［優先度 A］

ア　アクセシビリティ方針

対象範囲、目標を達成する期限、目標とする適合レベル、例外事項、目標とした適合レベル以上に追加した達成基準を記載し、サイトポリシー上に公開する。公開した達成期限までに、ウェブアクセシビリティ基盤委員会が定める「JIS X 8341-3:2016 試験実施ガイドライン」に基づく試験を実施し、達成基準をすべて満たし、試験結果を公開すること。すべてを満たせなかった場合にはその理由と準拠に向けたスケジュールを追記する。

なお、JIS X 8341-3：2010 への対応を実施し試験結果を公開している場合は、当分の間、本項目を充足しているものとみなす。

イ　多言語対応方針

専用ページを設置して多言語対応している場合には、目的、対応言語、対象ページを明記する。

多言語対応がプログラムを利用した翻訳の場合には、機械的に行われるため内容が 100%正確であるとは限らないことを明記する。

ウ　個人情報保護方針

行政機関の保有する個人情報の保護に関する法律に則り、個人情報保護方針をホームページに掲載する。また、施策に対する意見募集を行う場合など、入力フォームを使用して個人情報を収集（個人に関する情報の入力が任意である場合を含む。）する際には、第三者による不正アクセスから個人情報を保護するため、SSL 又はこれに準じる方法を使用し、安全性の確保に努める。

エ　著作権、リンク

著作権として、（ｃ）、公開年、著作権者名、クリエイティブ・コモンズ・ライセンスをフッターに掲載するなど、ホームページ上の文書や画像等の各ファイル、

及びその内容に関する諸権利の帰属、無断使用・転載、二次利用について、掲載資料の使用に際して発生する損害等についての責任を明記する。

オ　技術について

推奨ブラウザ、プラグイン、JavaScript、CSS、RSS、PDF などに関する、入手方法、インストール方法、利用方法、取り扱い上の注意及び情報システムのセキュリティなどを明記する。

カ　法的事項

遵守すべき法的事項として、免責事項、禁止事項、法的義務、管轄裁判所などについて明記する。

(2) ホームページ管理者は運営するサイトが上記サイトポリシーに掲載された内容や、達成基準を満たしていることを定期的に確認し、必要な場合には見直しを行う。確認に当たって準拠すべき法規制などがある場合には、これに従う。［優先度 A］

第４　コンテンツデザイン

１　記述

(1) コンテンツには、主題又は目的を説明する見出し及びラベルを必ず付ける。［優先度 A］[JIS 適合レベル AA]

(2) コンテンツは見出し、段落、リストなどの要素を用いて文書の構造を規定する。［優先度 A］[JIS 適合レベル A]

(3) ホームページの文章は、その内容に合わせた最も明瞭で簡潔なものにする。［優先度 B］

(4) 箇条書きは積極的に使い、本文から上下に１行程度の余白をとって配置する。［優先度 B］

(5) 重要な情報はページ上部に配置する。［優先度 B］

(6) 報告書など長い文章については、ユーザーが印刷して読めるよう、別途、印刷用のページや PDF 形式のファイルを用意する。［優先度 B］

(7) 各ページには、更新日や情報の公開日を記載するようにする。［優先度 B］

(8) ホームページ内でフォーカスを受け取ることのできるコンポーネントは、ユーザーがキーボード操作でフォーカスを移動させている際には、コンテンツの意味や操作性に沿った順序でキーボードフォーカスを移動させる。［優先度 A］[JIS 適合レベル A]

(9) ホームページの中で同じ機能性をもつコンポーネントは、同ホームページ内で一貫して識別できるような表現にする。［優先度 A］[JIS 適合レベル AA]

(10) 日本語のページでは、ユーザーにとって理解しにくいと考えられる外国語は、多用しない。使用するときは、最初に用いるときに解説する。［優先度 B］

(11) 省略語、専門用語、流行語、俗語などのユーザーにとって理解しにくいと考えられる用語は、多用しない。使用するときは、最初に用いるときに定義する。［優先度 B］

(12) ユーザーにとって、読みの難しい言葉（固有名詞など）は、多用しない。使用するときは、最初に用いるときに読み（ふりがな）を明示する。［優先度 B］

(13) コンテンツを理解し操作するための説明として、形、大きさ、視覚的な位置、方向や音を用いる際には、形や大きさ、音を知覚できない、あるいは空間的な位置や方向に関する情報を利用できないユーザーにも理解できるようにテキストで説明を提供する。［優先度 A］[JIS 適合レベル A]

２　ページタイトルとファイル名

(1)　ページタイトル（例：HTML の場合、<title>の内容）は、ブラウザの左最上部や検索結果などに表示される重要な部分であるため、すべてのページに付ける。［優先度 A］[JIS 適合レベル A]

(2)　ホームページには、その各ページのコンテンツの内容が分かるように、主題又は目的を説明したページタイトルを付ける。［優先度 A］[JIS 適合レベル A]

(3)　ファイルの名前は、半角英数文字（英文字については小文字のみとする。）でページ内容を的確に表す名前を付ける。［優先度 B］

(4)　ファイル名にはスペースを使わない。［優先度 A］

３　使用する言語の指定

(1)　ファイルの文字コードは Shift_JIS 又は、UTF-8 とし、UTF-8 を使用しない場合は、文字化けに留意して文字コードを設定する。［優先度 A］

(2)　html 要素の lang 属性に、ホームページの主たる自然言語として日本語（ja）を指定する。開発言語が XHTML の場合は、xml:lang 属性についても指定を行う。また、更新時に表示言語を変更した場合は、変更した言語を指定する。［優先度 A］[JIS 適合レベル A]

(3)　部分的にそのホームページにおける主たる自然言語 （ja）以外が用いられている場合、該当箇所の要素に lang 属性を用いてその自然言語がどの言語であるかを指定する。開発言語が XHTML の場合は、xml:lang 属性についても指定を行う。［優先度 A］[JIS 適合レベル AA]

４　フォントや文字の使い方

(1)　フォントの種類やサイズは、ブラウザの初期設定に従う。［優先度 B］

(2)　コンテンツ又は機能を損なうことなく、テキストを支援技術なしで 200%までサイズ変更できるようにする。ただし、写真や挿絵に添えた説明文及び画像化された文字は除く。［優先度 A］[JIS 適合レベル AA]

(3)　ユーザーが戸惑わないよう、下線や青と赤紫の色はリンク以外で使用しない。［優先度 B］

(4)　動きのある、点滅している、スクロールする、又は自動更新する画像、音声、フォント若しくは文字により情報を表示する場合は、ユーザーが「一時停止」、「停止」又は「非表示」にすることができるようにする。「自動更新」が開始される場

合には、ユーザーが「一時停止」、「停止」又は「非表示」を選択できるようにするか、あるいはユーザーが更新頻度を調整できるようにする。ただし、その動き、点滅又はスクロールが必要不可欠な動作の一部である場合を除く。［優先度 A］[JIS 適合レベル A]

(5)　レイアウト目的で一単語内にスペースや改行コードを挿入しない。［優先度 A］[JIS 適合レベル A]

(6)　単位や年月日などの情報は、文字で記述することとし、図形文字や記号を用いない。［優先度 B］

(7)　特定のシステム環境でのみ表示される機種依存文字は使用しない。［優先度 A］

5　色の使い方

(1)　テキスト及び画像化された文字の視覚的な表現は、少なくとも 4.5:1 のコントラスト比とする。大きな文字（太字でないテキストが少なくとも 18 ポイント（日本語は 22 ポイント）、太字のテキストが少なくとも 14 ポイント（日本語は 18 ポイント）の場合は、テキスト（及び画像化された文字）とその背景の間に、少なくとも 3:1 のコントラスト比を持たせる。ただし、次の場合は除く。［優先度 A］[JIS 適合レベル AA]

ア　テキスト及び画像化された文字が付随的で、装飾だけを目的にしている、誰も視覚的に確認できない、又は重要な他の視覚的なコンテンツを含む写真の一部分である。

イ　ロゴタイプ（ロゴ又はブランド名の一部である文字）である。

なお、画像化された文字について、編集可能な元データがない場合、著作権の関係で編集ができない場合など、達成が著しく困難な場合には可能な範囲での対応を実施する。

(2)　情報を伝える、何が起こるか若しくは何が起きたかを示す、ユーザーの反応を促す、又は視覚的な要素を区別するなど、視覚的な手段として色だけを使用しない。［優先度 A］[JIS 適合レベル A]

6　画像や動画、音声等非テキストコンテンツの取扱い

(1)　画像など非テキストコンテンツを使う場合は非テキストコンテンツの内容を表すなど同等の目的を果たす代替テキストなどを提供する。ただし、装飾目的や見た目の整形だけの場合や、ユーザーに提供されないもの、閲覧上無視できるものは対象外とする。［優先度 A］[JIS 適合レベル A]

(2)　高画質の画像や写真が必要な場合は、大きな画像へのリンクとしてサムネイル（サイズの小さい画像）を貼る。この場合、サムネイル画像の近くに、大きな画像のファイル容量とその画像の内容を的確に表現したテキストリンクを付ける。［優先度 A］

(3)　ファイルサイズの大きな画像に関しては、例えば画質を落とすなどの手法でサイズを小さくできるか検討する。［優先度 B］

(4)　音声のみで提供されているコンテンツは、その内容と同等のテキスト情報を同ページ内で提供する。ただし、その音声がテキストの代替メディアであって、代替メディアであることが明確にラベル付けされている場合は除く。［優先度 A］[JIS 適合レベル A]

(5)　動画（映像と音声を含むもの）で提供されているコンテンツは、動画内に音声解説（副音声などの音声による補足）をつけ、その内容と同等のテキスト情報を同ページ内で提供する。ただし、その映像又は音声がテキストの代替メディアであって、代替メディアであることが明確にラベル付けされている場合は除く。［優先度 A］[JIS 適合レベル A/AA]

なお、編集可能な元データがない場合や、著作権の関係で編集ができない場合、動画がライブであり技術的に対応が難しい場合など、達成が著しく困難な場合には可能な範囲での対応を実施する。

(6)　アニメーション GIF は、ユーザーがホームページの文章を読む際に集中力の妨げとなるため、原則使用しない。［優先度 B］

(7)　音は自動再生させず、ユーザーの要求に応じてのみ再生する。また、その音声を一時停止又は停止することができるようにする。［優先度 A］[JIS 適合レベル A]

(8)　閃光するコンテンツは原則使用しない。使用する場合は、次のいずれかの基準を満たすこと。［優先度 A］[JIS 適合レベル A]

ア　どの 1 秒間においても閃光が 3 回以下である。

イ　一般せん（閃）光いき（閾）値及び赤色せん（閃）光いき（閾）値を下回っている。

7　表やフォーム

(1)　表、フォームは見た目の位置や視覚的な装飾だけではなく、適切な要素や属性を用いて記述（マークアップ）することにより、意図した「構造」や論理的な「関

係性」について音声読み上げソフトなどが理解できるようにする。[優先度 A][JIS 適合レベル A]

(2) ユーザーの入力を要求する場合（入力フォームなど）は、何を入力すればよいか、またエラーがあった際のエラー内容や修正方法などユーザーにわかりやすい説明を提供する。[優先度 A][JIS 適合レベル A/AA]

(3) フォームの情報にはフォーム要素を用いる。[優先度 A][JIS 適合レベル A]

(4) 次に挙げる操作を行う場合は、内容の取り消し、確認及び修正のうち、少なくとも一つができるようにする。[優先度 A][JIS 適合レベル AA]

ア 契約などの法的義務の発生を伴う操作
イ 金銭取引
ウ ユーザーがオーナーである情報についての操作
エ ユーザーからの情報送信

8 リンク設定

(1) リンクの目的は、リンクのテキスト、又はリンクのテキストとプログラムで解釈可能なリンクの文脈とを合わせることにより、解釈できるようにする。ただし、文脈や文全体の内容を確認することによってそのリンク先が明確になる場合は除く。[優先度 A][JIS 適合レベル A]

(2) リンク色はブラウザの初期設定（下線と青色や赤紫色）を使用し、リンク部分の位置を本文から離して表示する。[優先度 B]

(3) 各コンテンツページにおける 1 ページあたりのリンク数は、当該ページの内容に関連した情報に絞り込むなどにより、多くなりすぎないようにする。[優先度 B]

(4) ユーザーが誤って別のリンク先をクリックしてしまうことのないように、リンクとリンクの間は近づきすぎないよう配慮する。[優先度 B]

(5) リンクテキストやリンク画像は、ユーザーがクリックしやすいよう、文字や画像の大きさに配慮する。[優先度 B]

(6) 各ページのメインコンテンツ部分の前に、「複数のページ上で繰り返されているコンテンツのブロック」(ヘッダーやサイドメニューなど)がある場合には、各ページの先頭からメインコンテンツの開始位置まで「スキップできるメカニズム」を提供する。この際、このメカニズムはキーボードでも利用できるように提供する。[優先度 A][JIS 適合レベル A]

(7)　外部リンクを設定する場合は、注釈を設けるなどにより、ユーザーに外部リンクであることが分かるようにする。［優先度 B］

(8)　イメージマップ（一つの画像に複数のリンクを設定する方法）は、クライアントサイドを使用し、リンク先の内容が分かる適切な代替テキストを必ず付ける。［優先度 A］

９　関連技術の使用

(1)　PDF 形式で情報を提供する場合にも、本統一基準のうち、「JIS 適合レベル」と記載のある内容を遵守する。ただし、編集できる元データがない場合など、すべての対応が著しく困難な場合は可能な範囲での対応を実施する。［優先度 A］

(2)　PDF 形式で情報を提供する場合、Adobe Reader などの一般に入手可能な閲覧ソフトで正しく表示されることを確認する。［優先度 A］

(3)　内容が膨大であるなど、ページ内にすべて記述することが困難で、より詳細な内容を提供することを目的として PDF 形式で提供する場合、原則画像化されたファイルを使用せず、文字情報の入った状態で提供し、PDF ファイルに含まれる情報の概要をページの本文中で提供する。［優先度 B］

(4)　Flash の使用は、最小限に抑える。［優先度 B］

(5)　Flash や JavaScript の動作によって提供される情報がある場合は、等価な情報をテキストで提供する。［優先度 A］[JIS 適合レベル A]

(6)　RSS（Rich Site Summary）配信をする場合は、「どのコンテンツが RSS に対応しているか」「RSS の登録方法について」などの利用に当たっての前提条件、注意点を記載する。［優先度 B］

(7)　データなどを提供する場合、RDF（Resource Description Framework）形式を活用する。［優先度 B］

(8)　ダウンロードファイルについては、ファイルの形式名及び容量を表示する。［優先度 B］

(9)　申請書様式は PDF 形式による提供を基本とする。PDF 以外の形式（Microsoft Word、Microsoft Excel、一太郎など、ユーザーにおいて有償のアプリケーションを用意しないと利用できないもの）のみによる提供は行わない。［優先度 B］

１０　操作環境

(1)　すべての機能をキーボードから利用できるようにする。

プラグインやアプリケーション及びダイアログボックスは、それらをページに埋め込んだ場合、その部分にキーボードフォーカスが閉じ込められてしまう危険性があるため、原則埋め込まない。埋め込む場合は、キーボードフォーカスが閉じ込められないようにする。また、キー操作以外の方法で抜け出すことが可能であれば、その操作方法を分かりやすく明記する。ダイアログボックスは、［OK］ボタンや［キャンセル］ボタンなどを提供し、フォーカスが元の位置に戻るようにする。［優先度 A］[JIS 適合レベル A]

(2) キーボード操作が可能なユーザインタフェースには、キーボードフォーカスの状態が視覚的に認識できる操作モードを提供する。［優先度 A］[JIS 適合レベル AA]

(3) 入力フォームなどでは、入力に時間制限を設けない。

制限時間があるときは、ユーザーによって事前に時間制限を解除、調整又は延長できるようにする。ただし、制限時間が必須の要素で、その制限時間に代わる手段が存在しない場合で、制限時間を延長することがコンテンツの動作を無効にすることになる場合、又は、制限時間が 20 時間よりも長い場合は例外とする。［優先度 A］[JIS 適合レベル A]

東京都サイバーセキュリティ基本方針

改正　平成31年1月22日　30総情企第1688号
改正　平成31年1月22日　30共管会第501号
改正　平成31年1月22日　30交総第1211号
改正　平成31年1月22日　30水総企第464号
改正　平成31年1月22日　30下総総第771号
改正　平成31年1月22日　30教総情第432号
改正　平成31年1月22日　30選総第901号
改正　平成31年1月22日　30人委総第961号
改正　平成31年1月22日　30監総第830号
改正　平成31年1月22日　30議調第186号

目次

1　目的

東京都は、行政運営上、個人情報などの重要な情報を多数取り扱っているだけでなく、交通、水道、下水道等の公共インフラ事業を担うことにより、都民生活及び社会経済活動に必要不可欠なサービスを提供している。よって、これらを支える情報システムや制御システム（以下「情報システム等」という。）に加え、これらで取り扱う重要な情報などの情報資産を様々な脅威から守り、安全性を確保することは、行政及び公共インフラ事業の安定的・継続的な運営を実現するために、東京都に課せられた責務である。

そのため、東京都が実施するサイバーセキュリティ対策に関する基本的な事項を定め、サイバー攻撃等の様々な脅威から、東京都が保有する情報資産の機密性、完全性及び可用性を維持することを本基本方針の目的とする。

また、全ての職員等は、東京都が保有する情報資産に対する脅威への対応が重大かつ喫緊の課題であることをあらためて認識し、東京都におけるサイバーセキュリティ対策の推進に積極的に取り組むこととする。

2　定義

(1)　ネットワーク

コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウエア及びソフトウエア）をいう。

(2)　情報システム

東京都の運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。

(3)　制御システム

東京都の公共インフラ事業のうち、交通、水道、下水道、公共施設等の管理を行ううえで重要な制御機器類のハードウェア､ファームウェア(組込み機器に搭載されるソフトウェアをいう。)、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。

(4)　サイバーセキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(5)　サイバーセキュリティポリシー

本基本方針及びサイバーセキュリティ対策基準をいう。

(6)　職員等

常勤職員、非常勤職員及び臨時職員並びに派遣職員をいう。

(7)　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(8)　完全性

情報が破壊、改ざん又は消去がされていない状態を確保することをいう。

(9) 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(10) マイナンバー利用事務（個人番号利用事務）系の情報システム

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（平成 25 年法律第 27 号。以下「マイナンバー法」という。）に定められている個人番号利用事務（社会保障、地方税又は防災に関する特定の事務）又は戸籍事務等に関わる情報システムをいう。

(11) 内部事務（ＬGWAN接続）系の情報システム

人事及び給与に関する事務、財務及び会計に関する事務、文書の作成及び管理に関する事務等の内部事務を取り扱う情報システムをいう。

(12) インターネット接続系の情報システム等

内部事務（ＬGWAN接続）系の情報システムで使用する電子メール以外の電子メールやＷｅｂサイト管理システム等に関わるインターネットに接続された情報システムをいう。

(13) 業務用端末

職員等に対し、業務上利用することが許可されたパソコン、モバイル端末等をいう。

(14) 業務用外部記録媒体

職員等に対し、業務上利用することが許可されたＵＳＢメモリや光ディスク等の外部記録媒体をいう。

(15) 管理区域

情報システム室（ネットワークの基幹機器及び重要な情報システム等に係る機器等を設置し、専ら当該機器等の管理及び運用を行うための部屋）及び業務用外部記録媒体の保管に使用する保管庫を設置している区域をいう。

(16) 準管理区域

庁舎内執務室用フロア内に設定され、情報システムの機器類の設置、管理運用、保管等を行う専用の区域をいう。

(17) ＳＭＳ（ソーシャルメディアサービス）

インターネット上で展開される情報メディアであって、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアである、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サービスをいう。

(18) クラウドサービス

従来は手元のコンピュータに導入して利用していたソフトウェアやデータ、それらを提供するための技術基盤等を、インターネットなどのネットワークを通じて、利用できるサービスをいう。

3　対象とする脅威

情報資産に対する脅威として、以下のものを想定し、サイバーセキュリティ対策を実施するほか、新たな脅威の発生に備え、最新の脅威動向を確認するなど、適切に対応する。

(1)　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃及び部外者の侵入等の意図的な要因による、東京都が保有する情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取のほか、内部管理の欠陥など職員等による不正行為等

(2)　東京都が保有する情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンスの不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

(3)　地震、落雷、火災等の災害によるサービス及び業務の停止等

(4)　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

(5)　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4　適用範囲

(1)　行政機関の適用範囲

本基本方針が適用される範囲は、東京都組織規程（昭和２７年東京都規則第１６４号）第８条第１項に規定する本庁の局、青少年・治安対策本部、病院経営本部、中央卸売市場、収用委員会事務局及び労働委員会事務局（以下「知事部局等」という。）並びに東京都公営企業組織条例(昭和２７年東京都条例第８１号)第１条に定める局、教育庁、選挙管理委員会事務局、監査事務局、人事委員会事務局、議会局及び東京都職員共済組合事務局（以下「公営企業局等」という。）とする。

(2)　情報資産の適用範囲

本基本方針が対象とする情報資産は、次のとおりとする。

ア　情報システム等

イ　個人情報のほか、情報システム等で取り扱うデータ

ウ　情報システム等に関するシステム設計書、ネットワーク図等のシステム関連文書

5　地方独立行政法人等への指導

東京都が設立した地方独立行政法人及び東京都の監理団体においては、本基本方針等を参考に、各団体等においてサイバーセキュリティ対策に係る基本方針等を策定するなど、必要なサイバーセキュリティ対策を実施するよう、所管局は適正に指導を行うこととする。

6　職員等の遵守義務

職員等は、東京都が保有する情報資産に対する脅威への対応の重要性について共通の認識を持ち、業務の遂行に当たって、サイバーセキュリティポリシー及びサイバーセキュリティ実施手順等を遵守しなければならない。

7　サイバーセキュリティ対策

３の脅威から情報資産を保護するために、以下のサイバーセキュリティ対策を講じる。

(1)　組織体制の確立

東京都の情報資産についてサイバーセキュリティ対策を推進する全庁的な組織体制を確立する。

(2)　情報資産の分類と管理

東京都の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき、サイバーセキュリティ対策を講じる。

(3)　情報システム全体の強じん性の向上

情報システム全体に対し、マイナンバー利用事務（個人番号利用事務）系の情報システム、内部事務（ＬGWAN接続）系の情報システム及びインターネット接続系の情報システムという三層の情報システムからなる強じん性向上対策を講じる。

(4)　物理的セキュリティ対策

サーバ、管理区域、準管理区域、通信回線等及び業務用端末等の管理について、物理的な対策を講じる。

(5)　人的セキュリティ対策

サイバーセキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(6)　技術的セキュリティ対策

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(7)　運用面での対策

情報システムの監視及びサイバーセキュリティポリシー等の遵守状況の確認のほか、(8)の外部サービスを利用する際のセキュリティ確保等、サイバーセキュリティポリシーの運用面での対策を講じるものとする。

また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応体制を整備する。

(8)　外部サービスの利用に係る対策

東京都の業務を受託する事業者（当該事業者から派遣されている者を含む。）及び公的施設の管理を行う指定管理者等（以下併せて「外部委託事業者等」という。）に当該業務を行わせる場合には、東京都が定めるサイバーセキュリティ要件等、セキュリティ対策上、遵守させるべき事項を、外部委託事業者等の選定要件として提示する。

さらに、契約、協定等（以下「契約等」という。）の締結時等に、外部委託事業者等においても東京都が定めるセキュリティポリシーと同等のセキュリティ対策が確保されていることを、契約等事項に明記し、又は、別途、書面による提出を求める等の措置を講じる。

なお、約款による外部サービスを利用する場合には、当該利用に係る規定等を整備し、対策を講じる。

また、ＳＭＳを利用する場合には、ＳＭＳに関する運用手順を定めるとともに、ＳＭＳで発信できる情報を規定し、利用するＳＭＳごとの責任者を定める。

クラウドサービスの利用に当たっても、クラウドサービスの利用に関する手順等を定めるとともに、必要に応じて、当該利用の対象とする情報について定める等、規定を整備すること。

８　リスク評価の実施及び年度計画の策定

サイバーセキュリティに係る内部環境及び外部環境の変化を踏まえ、東京都が保有する情報資産のサイバーセキュリティ上のリスクを評価し、リスク対応方針を策定する。

また、策定したリスク対応方針に基づき、リスク対応計画を毎年度策定する。

９　自己点検及びサイバーセキュリティに関する監査の実施

サイバーセキュリティポリシーの遵守状況を検証するため、定期的に実施の可否を判断し、必要に応じて、自己点検及びサイバーセキュリティに関する監査を実施する。

10　サイバーセキュリティポリシーの見直し

自己点検及びサイバーセキュリティに関する監査の結果、サイバーセキュリティポリシーの見直しが必要となった場合、又は、サイバーセキュリティに関する状況の変化に対応するため、新たに対策が必要となった場合には、サイバーセキュリティポリシーを見直す。

11　サイバーセキュリティ対策基準の策定

７から 10 までに示す対策等を実施するため、具体的な遵守事項及び判断基準等を定めるサイバーセキュリティ対策基準を策定する。

なお、当該対策基準は、東京都におけるサイバーセキュリティ対策の基準を定めるものであり、公にすることにより、東京都行政の運営に重大な支障を及ぼすおそれがあることから、当該対策基準については、４(1)に定める行政機関の適用範囲以外に対しては非公開とする。

12　サイバーセキュリティ実施手順の策定

11に定めるサイバーセキュリティ対策基準を踏まえ、サイバーセキュリティ対策を実施するための具体的な手順を定めたサイバーセキュリティ実施手順を策定するものとする。

なお、当該実施手順は、関連する情報システム等のサイバーセキュリティ対策を具体的かつ詳細に定めるものであり、公にすることにより、関連する業務の運営に重大な支障を及ぼすおそれがあることから、４(1)に定める行政機関の適用範囲以外に対しては非公開とする。

附　則

本基本方針は、平成 31 年 4 月 1 日から施行する。ただし、７(3)、(4)及び(6)の規定については、2021（平成 33）年 3 月 31 日まで適用しないことができる。

東京都サイバーセキュリティ対策基準

平成 31 年 1 月 22 日
平成 30 年度第 2 回東京都サイバーセキュリティ委員会決定

目次

1　総則

1.1　目的

東京都サイバーセキュリティ基本方針（以下「基本方針」という。）に基づき、サイバーセキュリティ対策を実施するうえで、東京都における体制、知事部局等及び公営企業局等（以下「各局等」という。）における体制及び各情報システム等において、共通で実施すべき対策等の基準を示したものである。

1.2　用語の定義

基本方針２による。

2　組織体制

2.1　サイバーセキュリティに関する統括体制

2.1.1　東京都における統括体制

⑴　最高情報セキュリティ責任者（Ｃｈｉｅｆ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｓｅｃｕｒｉｔｙ　Ｏｆｆｉｃｅｒ。以下「ＣＩＳＯ」という。）

副知事をＣＩＳＯとし、次の事項を所掌するものとする。

①　知事部局等における、全ての情報資産の管理及びサイバーセキュリティに関する最終決定権限及び責任を有する。また、公営企業局等におけるサイバーセキュリティに関する事項について決定する際には、公営企業局等からの協議を受ける。

②　東京都におけるサイバーセキュリティ全般を統括する組織として、東京都Ｃｏｍｐｕｔｅｒ　Ｓｅｃｕｒｉｔｙ　Ｉｎｃｉｄｅｎｔ　Ｒｅｓｐｏｎｓｅ　Ｔｅａｍ（以下「東京都ＣＳＩＲＴ」という。）を設置し、各役割を明確化する。また、各局等内におけるサイバーセキュリティ全般を統括する組織として、局Ｃｏｍｐｕｔｅｒ　Ｓｅｃｕｒｉｔｙ　Ｉｎｃｉｄｅｎｔ　Ｒｅｓｐｏｎｓｅ　Ｔｅａｍ（以下「局ＣＳＩＲＴ」という。）を各局等内に設置するよう、各局等の長に要請する。

③　東京都におけるサイバーセキュリティに関する重要な事項を審議・決定する組織として、「東京都サイバーセキュリティ委員会」を設置し、主宰し、統括する。

④　サイバーセキュリティを取り巻く状況の変化及び組織体制の変動等に応じ、サイバーセキュリティインシデント対応体制を見直す。

⑤　知事部局等のサイバーセキュリティ局統括責任者より、8.3⑴に基づく申請があった場合は、当該申請内容を検討し、例外措置として許可すること。

⑵　サイバーセキュリティ統括責任者（以下「ＣＩＳＯ補佐官」という。）

総務局情報政策担当部長をＣＩＳＯ補佐官とし、次の事項を所掌するものとする。

①　ＣＩＳＯの命を受け、包括的にＣＩＳＯの所掌事務を補佐する。

②　知事部局等におけるサイバーセキュリティに関する統括的な権限及び責任を有する。

③　東京都におけるサイバーセキュリティに係る事項の企画・立案をするとともに、各種方針案を策定する。

④　外部のサイバーセキュリティの専門家による支援を受けることができるよう、当該専門家による支援体制を整備する。

⑤　全ての職員等を対象としたサイバーセキュリティに関する研修及びサイバーセキュリティインシデント対応訓練（以下「サイバーセキュリティ研修等」という。）について、年度計画を策定し、実施する。

⑥　各局等におけるサイバーセキュリティ対策、サイバーセキュリティリスク評価、サイバーセキュリティインシデント対応等に関する助言、指導、評価、調査・報告依頼等を行う。

⑦　(1)⑤に基づく知事部局等からの例外申請に関する資料等を保管する。

(3)　サイバーセキュリティ統括管理者

総務局情報通信企画部サイバーセキュリティ担当課長をサイバーセキュリティ統括管理者とし、次の事項を所掌するものとする。

①　ＣＩＳＯ補佐官を補佐する。

②　(4)に定める東京都ＣＳＩＲＴに関する年間活動計画を策定し、2.1.2(4)に定める局ＣＳＩＲＴに対する支援時の対応も含め、東京都ＣＳＩＲＴの活動について管理・監督する。

③　各局等及び各区市町村におけるサイバーセキュリティインシデント時において、緊急対応が必要な場合に備え、連絡体制を整備し、管理する。

(4)　東京都ＣＳＩＲＴ

総務局情報通信企画部企画課セキュリティ担当により、東京都ＣＳＩＲＴを構成し、次の事項を所掌するものとする。

①　各局等と適宜連携して、サイバーセキュリティインシデントによる影響を最小限とするよう努めなければならない。

②　局ＣＳＩＲＴより支援の要請を受けた場合は、その求めに応じて、その活動を支援しなければならない。

③　②での支援時を含め、サイバーセキュリティインシデントに関する活動の際は、当該サイバーセキュリティインシデントの原因について分析し、記録し、及び保管しなければならい。

④　その他、東京都ＣＳＩＲＴに関する事務は、別途定めるところによる。

(5)　東京都サイバーセキュリティ委員会

東京都サイバーセキュリティ委員会は、ＣＩＳＯの主宰により、次の事項を所掌する。

①　東京都におけるサイバーセキュリティに関する重要な事項（サイバーセキュリティポリシー等）を審議し、決定する。

②　(2)③に基づき策定された各種方針案について審議し、承認した上、必要に応じて、その実施

状況等を確認する。

③　その他、東京都サイバーセキュリティ委員会に関する構成及び事務については、別途定めるところによる。

2.1.2　各局等における統括体制

(1)　サイバーセキュリティ局統括責任者

各局等の長をサイバーセキュリティ局統括責任者とし、次の事項を所掌するものとする。

①　各局等におけるサイバーセキュリティに関する統括的な権限及び責任を有する。

②　2.1.1(1)②に基づき、各局等において、局ＣＳＩＲＴを設置し、その体制を整備し、維持する。

③　各局等におけるサイバーセキュリティに関する重要な事項を審議・決定する組織として、(5)に定める局サイバーセキュリティ委員会を設置し、主宰し、統括する。

④　各局等におけるサイバーセキュリティに関する監査の実施要綱を定めるとともに、当該監査の責任者として、2.2(5)に定めるサイバーセキュリティ局監査責任者を任命する。

⑤　各局等におけるサイバーセキュリティ対策に関する事項について、必要に応じて、ＣＩＳＯに対し、協議する。

(2)　サイバーセキュリティ局責任者

(4)に定める局ＣＳＩＲＴが所属する部又は部に相当する所の長を、サイバーセキュリティ局責任者とし、次の事項を所掌するものとする。

①　各局等におけるサイバーセキュリティ局統括責任者を補佐する。

②　各局等におけるサイバーセキュリティ対策の推進に関する権限及び責任を有する。

③　各局等におけるサイバーセキュリティ対策の年度計画を定め、これを推進する。

④　各局等内のサイバーセキュリティに関係する全ての職員等を対象としたサイバーセキュリティ研修等について、年度計画を作成し、実施する。

⑤　各局等内における情報資産の持ち出し等に関する安全管理措置等を策定し、管理するとともに、職員等に周知し、遵守させなければならない。

(3)　サイバーセキュリティ局管理者

(4)に定める局ＣＳＩＲＴが所属する課の長を、サイバーセキュリティ局管理者とし、次の事務を所掌するものとする。

①　各局等におけるサイバーセキュリティ局責任者を補佐する。

②　(4)に定める局ＣＳＩＲＴに関する年間活動計画を作成し、その活動を指揮し、管理・監督する。

③　(2)③で定められた年度計画に基づき、各局等内におけるサイバーセキュリティ対策を実施するよう、各課のサイバーセキュリティ管理者及び情報システム管理者（以下「情報資産を所管

する者」という。）に対し、指示する。

④　各課で所管する情報システムに関する実施手順、運用手順、10.1①に定めるリスク評価の実施結果を基に、10.1②に基づき定めるサイバーセキュリティリスク対応方針案等の策定状況のほか、リスク評価及び監査等の実施状況等について、必要に応じて、確認する。

⑤　各局等における全ての職員等に対し、(2)④において作成された年度計画に基づき実施するサイバーセキュリティ研修等に参加するよう、周知する。

⑥　各局等におけるサイバーセキュリティインシデント時において、緊急対応が必要な場合に備え、各局等において所管する監理団体も含めた連絡体制を整備し、管理する。

(4)　局ＣＳＩＲＴ

局ＣＳＩＲＴは、各局等のサイバーセキュリティ局統括責任者において設置され、次の事項を所掌する。

①　2.1.1(4)に定める東京都ＣＳＩＲＴと適宜連携して、当該各局等内でのサイバーセキュリティインシデントによる影響を、最小限とするよう努めなければならない。

なお、当該活動時においては、必要に応じて、東京都ＣＳＩＲＴに支援を要請することができる。

②　各局等におけるサイバーセキュリティインシデントに関する活動の際は、当該サイバーセキュリティインシデントの原因について分析し、記録し、及び保管しなければならない。

③　その他、局ＣＳＩＲＴに関する事務は、別途定めるところによる。

(5)　局サイバーセキュリティ委員会

局サイバーセキュリティ委員会は、サイバーセキュリティ局統括責任者の主宰により、次の事項を所掌する。

①　各局等におけるサイバーセキュリティに関する重要な事項を審議し、決定する。

②　2.2(1)②に基づき策定された各種方針案等について承認し、その実施状況等を確認した結果について、必要に応じて、東京都サイバーセキュリティ委員会に報告する。

③　その他、委員会に関する構成及び事務については、別途定めるところによる。

2.2　サイバーセキュリティ実施体制

(1)　サイバーセキュリティ部責任者

各部等におけるサイバーセキュリティ対策の適正な管理を行うため、各部等の長をサイバーセキュリティ部責任者とし、次の事項を所掌するものとする。

①　各部等におけるサイバーセキュリティ対策に関する権限及び責任を有する。

②　各部等で所管する情報システムについて、10.1①に定めるサイバーセキュリティに係るリスク評価を実施し、その実施結果を基に、10.1②に基づき定めるサイバーセキュリティリスク対応方針案を策定する。

③　2.1.2(2)③で作成された年度計画に基づき、各部等におけるサイバーセキュリティ対策に係る年度計画を作成し、それに基づく対策を管理し、監督する。

(2)　サイバーセキュリティ管理者

各課におけるサイバーセキュリティ対策を確実に実施するため、各課の長をサイバーセキュリティ管理者とし、次の事項を所掌するものとする。

①　各課及び各管理区域等におけるサイバーセキュリティ対策を実施する責任を有する。

なお、実施に際しては、各課における情報処理指導主任（以下「ＩＣＴリーダー」という。）を補助者とし、作業を行わせることができる。

②　(1)③で作成された年度計画に基づき、各課におけるサイバーセキュリティ対策を遂行する。

(3)　情報システム管理者

各局等における各情報システムの運用を担当する課の長等を情報システム管理者とし、所管する情報システムにおいて、次の事項を所掌するものとする。

①　サイバーセキュリティポリシー等に基づき、所管する情報システムに必要なサイバーセキュリティ対策を実施する責任を有するものとし、適正な対策を実施する。

②　所管する情報システムの運用及び利用に関するサイバーセキュリティ対策事項を定めた実施手順のほか、運用手順等を策定し、当該情報システムの維持及び管理をする。

③　②で策定した各種手順等について、当該情報システムの運用等を担当する情報システム担当者、利用する職員等のほか、当該情報システムに係る外部委託事業者等、関係者への周知を徹底する。

(4)　情報システム担当者

情報システムを所管する課において、当該情報システムの開発、設定の変更、運用、更新等を担当する職員等を情報システム担当者とし、情報システム管理者の指示に従い、情報システムに関する各種手順等に沿って、担当する情報システムについて必要な作業を行うものとする。

(5)　サイバーセキュリティ局監査責任者

当該各局等におけるサイバーセキュリティ対策の実効性を検証し、是正改善措置を促す者として、2.1.2(1)に定めるサイバーセキュリティ局統括責任者により任命されたサイバーセキュリティ局監査責任者は、当該局等において、次の事項を所掌するものとする。

①　各局等におけるサイバーセキュリティに係る監査方針及び監査計画のほか、監査手順等を策定する。

②　各局等におけるサイバーセキュリティに関する監査を実施する。また、その結果、実施しているサイバーセキュリティ対策について是正が必要と判断した場合は、必要に応じて、是正改善措置を勧告する。

なお、勧告した場合は、勧告内容に対する是正改善の措置が適正であるかのフォローアップ

監査を実施する。

③　②の各実施結果等について、サイバーセキュリティ局統括責任者及び局サイバーセキュリティ委員会に報告する。

2.3　兼務の禁止

①　サイバー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、承認申請を行う者とその承認者は、同じ者が兼務してはならない。また、同様に、許可申請を行う者とその許可者についても、同じ者が兼務してはならない。

②　サイバーセキュリティに関する監査を行う際は、やむを得ない場合を除き、当該監査を受ける者と当該監査を実施する者とはそれぞれ同一の者が兼務してはならない。

3　情報資産の分類と管理

(1)　情報資産の分類

情報資産は、機密性、完全性及び可用性の視点から、情報資産を所管する者が次のとおり分類し、これに応じた管理基準、取扱いの条件及び制限等を設定し、必要な環境を整備し、運用するなど、適切にサイバーセキュリティ対策を実施しなければならない。

なお、分類については、所管する情報システムにおいて総合的に判断し、重要度（総合重要度）を設定しなければならない。

①　機密性による情報資産の分類

分類	分類基準	必要な対策、取扱条件等
機密性A	行政事務及び公共インフラ事業で取り扱う情報資産のうち、秘密文書に相当する、高い機密性を要する情報資産	情報資産について、権限を有しない者の利用、接触等が絶対にないよう、特段の取扱い制限を行う。
機密性B	行政事務及び公共インフラ事業で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	情報資産について、東京都の職員等又は東京都の業務に関連する者以外の利用、接触等がないよう、取扱い制限を行う。
機密性C	機密性A又は機密性B以外の情報資産	

※　「別表 1-1」に例示する。

② 完全性による情報資産の分類

分類	分類基準	必要な対策、取扱条件等
完全性A	行政事務及び公共インフラ事業で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、都民等の権利が侵害される、又は行政事務及び公共インフラ事業の的確な遂行に重大な支障を及ぼすおそれがある情報資産	情報資産への不正なアクセスの遮断、誤操作、機器障害等からの情報資産破損の防御など情報システムの制御、監視等を特に厳重に行う。
完全性B	行政事務及び公共インフラ事業で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、行政事務及び公共インフラ事業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情報資産	情報資産への不正なアクセスの遮断、誤操作、機器障害等からの情報資産破損の防御など情報システムの制御、監視等を行う。
完全性C	完全性A又は完全性B以外の情報資産	

※ 「別表 1-2」に例示する。

③ 可用性による情報資産の分類

分類	分類基準	必要な対策、取扱条件等
可用性A	行政事務及び公共インフラ事業で取り扱う情報資産のうち、滅失、紛失又は利用不能により、都民等の権利が侵害される、又は行政事務及び公共インフラ事業の安定的な遂行に重大な支障を及ぼすおそれがある情報資産	自然災害、停電又はサービス不能攻撃等に際し、情報システムの停止を最小限とし、ほぼ連続的な稼動を保証させること。また情報資産が消失することのないよう、特段の措置を講じること。
可用性B	行政事務及び公共インフラ事業で取り扱う情報資産のうち、滅失、紛失又は利用不能により、行政事務及び公共インフラ事業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情報資産	自然災害、停電又はサービス不能攻撃等に際し、情報システムが停止しても、一定時間内に再稼動させること。
可用性C	可用性A又は可用性B以外の情報資産	

※ 「別表 1-3」に例示する。

④ 情報システムの総合重要度による情報資産の分類

情報資産を所管する者は、①から③までを踏まえ、所管する情報システムにおいて総合的に

判断し、情報資産について次のように総合重要度を設定しなければならない。

ア　機密性・完全性・可用性の分類のうち、１以上の分類で階級がＡである場合、情報システムの総合重要度をＡとする。

イ　機密性・完全性・可用性の分類のうち、２以上の分類で階級がＣで、かつ、いずれの分類にもＡを含まない場合、情報システムの総合重要度をＣとする。

ウ　これら以外の場合、情報システムの総合重要度をＢとする。なお、全ての分類で階級がＢであり、特に業務遂行における情報システムの重要度が高い場合、情報システムの総合重要度をＡとすることができる。

(2)　情報資産の管理

①　情報資産に係る管理責任

情報資産を所管する者は、情報資産の管理に当たり、次の措置を講じなければならない。

ア　所管する情報資産について管理責任を有する。

イ　情報資産が複製又は伝送された場合には、複製先又は伝送先においても、(1)の分類に基づき、当該情報資産についても管理させること。

ウ　職員等が情報資産を、都庁本庁舎（第一本庁舎及び第二本庁舎並びに議会棟等）並びに各局等に付随する出張所及び出先事務所等以外の施設等（以下「庁舎外」という。）へ移動又は持ち出しをしようとする場合は、定められた安全管理措置に基づき実施するよう、職員等に周知し、遵守させること。

②　情報資産の分類の表示

情報資産を所管する者は、情報資産の分類に当たり、次の措置を講じなければならない。

ア　基本方針４(2)に定めるもののうち、機密性Ａの情報資産を含むファイル等については、一目で「機密性Ａのもの」であることが認識できるよう、ファイルにあってはその名称や格納先の記録媒体の外側に、関連文書にあってはその隅等に表示したうえ、必要に応じて、取扱い制限についても明示する等、適切な管理を行うこと。

イ　情報システムに記録される情報等、直ちに情報資産の分類に関する表示が困難な場合は、情報資産の分類を規程等により明記し、当該情報システムを利用する全ての職員等のほか、必要に応じて、関係者に周知すること。

③　情報の作成

情報資産を所管する者は、情報の作成に当たり、次の措置を講じなければならない。

ア　職員等に、業務上必要のない情報を作成させないこと。

イ　職員等に情報を作成させる場合には、(1)の分類に基づき、当該情報の分類と取扱いの条件、制限等を定めること。

ウ　職員等に情報を作成させる場合には、作成途上の情報においても、紛失、流出等を防止させること。また、作成途上で当該情報が不要になった場合は消去するよう周知すること。

④　情報資産の入手

情報資産を所管する者は、情報資産の入手に当たり、次の措置を講じなければならない。

ア　自らが所属する組織以外の組織が所管する情報資産を入手した場合は、入手元の情報資産の分類に基づいた取扱いをすること。

イ　職員等以外の者が作成した情報資産を職員等が入手した場合は、(1)の分類に基づき、当該情報資産の分類と取扱いの条件、制限等を定めること。

ウ　職員等が機密性の高い情報資産を入手しようとする場合は、入手元に対して情報資産の暗号化又はパスワード設定の措置を講じてもらうことを要請するよう、周知すること。

⑤　情報資産の利用

情報資産を所管する者は、情報資産の利用に当たり、次の措置を講じなければならない。

ア　職員等が情報資産を利用する場合は、業務以外の目的に情報資産を利用させないこと。

イ　職員等が情報資産を利用する場合は、情報資産の分類に応じ、適切な取扱いをするよう周知すること。

ウ　職員等が、情報資産の分類が異なる情報が複数記録されている電磁的記録媒体を利用する場合、その中での最高度の分類に従って、当該電磁的記録媒体を取り扱うよう周知すること。

エ　職員等が、マスターデータから複写して情報資産を利用しようとする場合、複写の権限を有する者又は当該情報資産を所管する者の許可を得るよう、職員等に周知すること。

なお、その際の複写範囲は必要最低限となるよう注意させること。

オ　情報資産を利用した者がマスターデータへの書き戻しをする場合に備え、書き戻しの手続等を定めること。

⑥　情報資産の保管

情報資産を所管する者は、情報資産の保管に当たり、次の措置を講じなければならない。

ア　情報資産は、情報資産の分類に従って、適正に保存し、保管すること。

イ　機密性Ａ又は機密性Ｂの情報が保管されている情報資産については、盗難及び情報漏えいの防止のため、適切な物理的構造等となっている施錠できる保管庫等に保管し、その保管庫等の鍵の管理について万全を期するとともに、保管状況等を定期的に点検すること。

ウ　総合重要度Ａの情報システムの情報を保管する場合、原則、耐火、耐熱、耐水及び耐湿を講じた施錠可能な安全な場所に保管すること。

エ　都民等、外部に公開する情報資産を保管する場合は、当該情報資産について、完全性を確保すること。ただし、完全性を保障しないことが免責事項として定められている場合は、この限りではない。

オ　電磁的な情報の保管に当たっては、原則、業務用外部記録媒体に保管することを禁止し、セキュリティを確保したファイルサーバ又は情報システムのサーバに保管することとする。ただし、業務遂行上他の手段により難い場合で、情報資産を所管する者が許可を与えた場合は、以下の措置を講じた上で実施させること。

・　機密性Ａ又は機密性Ｂの電子的な情報を、業務用外部記録媒体に長期保管する場合は、書込禁止の措置を講じるとともに、当該業務用記録媒体の保管状況の確認及び点検を定期的に行うこと。

・　総合重要度Ａの情報システムに関する情報資産のうち、利用頻度が低いデータ又はバックアップで取得したデータについて長期保管する場合は、可能な限り、自然災害を被る可能性が低い遠隔地域などに保管すること。

・　機密性・完全性・可用性のいずれかで階級がＡの情報を記録した業務用外部記録媒体を保管する場合は、ウと同様、原則、耐火、耐熱、耐水及び耐湿を講じた施錠可能な安全な

場所に保管すること。

⑦　情報の送信

情報資産を所管する者は、機密性Ａの情報については、職員等による電子メール等を用いた情報の送信を禁止しなければならない。

ただし、業務遂行上、情報資産を所管する者が他の手段により難いと判断し、許可した場合は、この限りではない。なお、許可した場合は、職員等に対し、暗号化又はパスワード設定の措置を施した上で実施するよう求めなければならない。

なお、機密性Ｂの情報についても、必要に応じて、同様とする。

⑧　情報資産の運搬

情報資産を所管する者は、機密性Ａ及び機密性Ｂの電磁的な情報については、原則、職員等による業務用外部記録媒体での運搬を禁止しなければならない。ただし、業務遂行上他の手段により難いと情報資産を所管する者が判断し、許可を与えた場合は、以下の措置を講じた上で実施させなければならない。

ア　機密性Ａの情報資産について、車両等による運搬を許可した場合は、情報資産の不正利用を防止するための措置として、暗号化又はパスワード設定の措置を講じた上で、更に鍵付きのケース等に格納させること。また、必要に応じて、複数の職員等で対応するよう指示をすること。

イ　機密性Ｂの情報資産についても、必要に応じて、アと同様とする。

⑨　情報資産の提供・公表

情報資産を所管する者は、機密性Ａの情報資産について、職員等による外部への提供等を禁止しなければならない。ただし、法令等により提供が認められ、かつ情報資産を所管する者が判断し、許可を与えた場合は、以下の措置を講じた上で実施させなければならない。

ア　機密性Ａの情報資産について、外部の者への提供を許可した場合は、情報資産の不正利用を防止するための措置として、職員等に対し、暗号化又はパスワードの設定の措置を講じさせること。

イ　都民等、外部に公開する情報資産を所管する場合は、当該情報資産について、完全性を確保すること。ただし、完全性を保障しないことが免責事項として定められている場合は、この限りではない。なお、機密性Ｂの情報資産についても、必要に応じて、アと同様とする。

⑩　情報資産の廃棄

情報資産を所管する者は、情報資産の廃棄に当たり、次の措置を講じなければならない。

ア　職員等が情報資産を廃棄しようとする場合は、情報資産を所管する者の許可を得た上で廃棄するよう、職員等に周知すること。

イ　職員等が情報資産を廃棄する場合は、職員等に、廃棄の日時・担当者名・処理内容等を記録させること。

ウ　職員等が情報資産を保管している記録媒体を廃棄する場合は、電磁的記録媒体内の情報を復元できないように処置した上で廃棄させること。

エ　職員等が機密性Ａの紙媒体による情報資産を廃棄する場合は、溶解又は裁断により、紙媒体に記録された情報が復元できないように処置したうえで廃棄するよう、職員等に周知すること。なお、機密性Ｂの紙媒体による情報資産を廃棄する場合も、必要に応じて、同様とす

る。

オ　賃貸借契約の終了等に伴い、東京都が借り受けている端末、サーバ、その他電磁的記録媒体などの情報処理機器類を返却する際には、情報を復元できないよう消去した上で返却しなければならない。機器の撤去後にデータ消去を行う場合は、データ消去までの期間におけるサイバーセキュリティ対策を明確にすること。

カ　オの消去作業を事業者に委託する場合、あらかじめ、契約仕様書にその旨を明記するとともに、データ消去完了証明書を徴取すること。また、必要に応じて、消去作業に職員等を立ち合わせること。

キ　保守等委託先事業者が故障等による部品交換を行う際、当該部品に含まれる東京都に帰属する情報について復元不可能な形で消去する委託先事業者の義務を契約仕様書に明記すること。

4　情報システム全体の強じん性の向上

(1)　マイナンバー利用事務（個人番号利用事務）系の情報システム

情報資産を所管する者は、マイナンバー利用事務（個人番号利用事務）系の情報システムについて、次の措置を講じなければならない。

①　マイナンバー利用事務（個人番号利用事務）系の情報システムと他の領域との分離

マイナンバー利用事務（個人番号利用事務）系の情報システムと他の内部事務（ＬGWAN接続）系の情報システム及びインターネット接続系の情報システムとにおいて、通信できないようにすること。

②　情報システムへのアクセス制御及び持ち出しにおける対策

ア　情報システムへのアクセスにおける対策

情報システムに対するアクセスがアクセスを許可された利用者からのものかどうかを判断する認証方式として、「知識（パスワード等、利用者本人しか知りえない情報）」、「所持（利用者自身による物理的な所持を必要とする機器）」、「存在（指紋等、利用者個人を特定する情報）」を利用する認証手段のうち、原則、二つ以上を併用する認証（以下、「多要素認証」という。）を利用すること。

イ　情報の書き出し不可設定及び職員等による庁舎外への持ち出しにおける対策

原則として、職員等により、業務用端末から、業務用外部記録媒体への情報の書き出しができないよう設定し、また、外部へ持ち出さないよう職員等に対し、求めること。

(2)　内部事務（ＬGWAN接続）系の情報システム

情報資産を所管する者は、内部事務（ＬGWAN接続）系の情報システムとインターネット接続系の情報システムについて、両環境間の通信環境を分離した上で、必要な通信だけを許可できるよう、措置を講じなければならない。

なお、内部事務（ＬGWAN接続）系の情報システム以外からの電子メールやデータを内部事務（ＬGWAN接続）系の情報システムに取り込む場合は、原則、不正プログラムの可能性がある部分を取り除く等の措置を実施し、安全性の確保（以下「無害化」という。）を図らなければならない。

(3)　インターネット接続系の情報システム

情報資産を所管する者は、インターネット接続系の情報システムについて、次の措置を講じなければならない

①　通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、サイバーセキュリティインシデントの早期発見及び対処並びに内部事務（ＬGWAN接続）系の情報システムへの不適切なアクセス等の監視等のサイバーセキュリティ対策を講じること。

②　区市町村のインターネット接続口を集約する自治体情報セキュリティクラウドを運用し、管理するとともに、関係省庁や道府県等と連携しながら、サイバーセキュリティ対策を推進すること。

5　物理的セキュリティ

5.1　サーバ等の管理

(1)　機器の取付け

情報資産を所管する者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

(2)　サーバの冗長化

情報資産を所管する者は、情報システムの障害、誤動作、サービス不能攻撃等による運用停止時間を最小限とするよう、当該情報システムの可用性に応じて、サーバの冗長化対策等の措置を講じなければならない。

(3)　機器の電源

情報資産を所管する者は、機器の電源を管理するに当たり、情報システムの可用性に応じて、次の措置を講じなければならない。

①　サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備えること。

②　情報システムの可用性がＡの場合、情報システムの運用停止時間を極めて短時間とするよう、一定期間電力等を自給できる非常用電源を確保すること。

③　情報システムの可用性がＢの場合、当該機器が保持するデータ等を毀損しないよう、適切に停止するまでの間に十分な電力を供給する容量の予備電源を確保又は備え付けること。

④　情報システムの可用性にかかわらず、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じること。

(4)　通信ケーブル等の配線

情報資産を所管する者は、通信ケーブル等の配線に当たり、次の措置を講じなければならない。

① 通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用するなど必要な措置を講じること。

② 主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、施設管理部門と連携して対応すること。

③ ネットワーク接続（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理すること。

④ 自ら又は情報システム担当者及び契約により操作を認められた外部委託事業者等以外の者が配線を変更、追加できないように必要な措置を講じること。

(5) 機器の定期保守及び修理

情報資産を所管する者は、情報システムの安定稼働に必要な保守及び修理において、次の措置を講じなければならない。

① 可用性Ａ又は可用性Ｂのサーバ等の機器については、定期保守を実施すること。

② 記録媒体を内蔵する機器について、外部委託事業者等に点検・修理業務を委託する場合は、当該業務を受託する事業者との間で、次の事項を確認のうえ、実施させること。

ア ３(2)⑩キに定めるとおり、東京都に帰属する情報に関する消去方法等、受託する上での義務について、あらかじめ、契約仕様書に記載すること。

イ 守秘義務契約を締結するほか、秘密保持体制の確認などを実施すること。

(6) 庁舎外への機器の設置

サイバーセキュリティ局統括責任者は、庁舎外に総合重要度Ａの情報システムに係るサーバ等の機器を設置する場合、ＣＩＳＯの承認を得なければならない。

また、定期的に当該機器へのサイバーセキュリティ対策状況について確認しなければならない。

(7) 機器の廃棄等

情報資産を所管する者は、機器を廃棄、リース返却等をする場合は、３(2)⑩に基づき、機器内部の記録装置から、全ての情報を消去し、復元不可能な状態にする措置を講じた上で、適切に廃棄しなければならない。

5.2 管理区域及び準管理区域等の管理

(1) 総合重要度に応じた管理区域及び準管理区域等（以下「管理区域等」という。）の分類

情報資産を所管する者は、管理区域等の管理に当たり、次の措置を講じなければならない。

① 総合重要度Ａの情報システムに係る機器（管理区域外への持ち出しを許可された端末等を除く。）及び電磁的記録媒体は、管理区域に設置又は保管をすること。

② 総合重要度Ｂ又は総合重要度Ｃの情報システムに係る機器（管理区域等外への持ち出しを許可された端末等を除く。）及び電磁的記録媒体は、管理区域又は準管理区域に設置又は保管をすること。

(2)　管理区域等の構造等

情報資産を所管する者は、管理区域等の構造等について、次の対策を講じなければならない。

なお、準管理区域については、施錠管理が可能な部屋とし、原則、管理区域に準じた構造等とすること。

①　管理区域は、地階又は１階に設けてはならない。

②　外部からの識別・侵入が容易にできないようにすること。

③　管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって、許可されていない者の立入りを防止すること。

④　管理区域等内の機器等に、転倒及び落下防止等の耐震対策並びに防水等の措置等を講じること。

⑤　管理区域等に配置する消火薬剤及び消防用設備等が、機器等及び業務用外部記録媒体に影響を与えないようにすること。

(3)　管理区域等の入退室管理等

情報資産を所管する者は、管理区域等の入退室について、次の措置等を講じなければならない。

①　管理区域等への入退室は許可された者のみに制限する。また、管理区域については、指紋認証等の生体認証に係る情報等の認証情報を記録した媒体（以下「ＩＤカード等」という。）のほか、入退室管理簿の記載などにより入退室管理を行うこと。

②　外部からの訪問者が管理区域等に入室する場合は、外見上、職員等と区別できるようにした上で、必要に応じて、立ち入り区域を制限し、管理区域等への入退室を許可された職員等が付き添うこと。

③　管理区域等内に、許可なく当該情報システムに関連しないコンピュータ、通信回線装置、業務用外部記録媒体等を持ち込ませないようにすること。

④　管理区域等への入室許可、必要な物品の持込み又は物品の持ち出しの手続等、管理区域等の管理運営に関する規程等を整備すること。

⑤　職員等及び外部委託事業者等は、管理区域等に入室する場合、身分証明書等を携帯し、求めにより提示すること。

(4)　管理区域への機器等の搬入出

情報資産を所管する者は、管理区域へ機器等の搬入出において、当該機器等が、既存の情報システムに与える影響について、あらかじめ確認するとともに、搬入出時には、必ず、職員等が立ち会うなどの措置を講じなければならない。

5.3　通信回線及び通信回線装置の管理

情報資産を所管する者は、情報システムの機密性及び可用性に応じて、通信回線及び通信回線装置の管理に当たり、次の対策を講じなければならない。

① 都庁本庁舎（第一本庁舎及び第二本庁舎並びに議会棟等）並びに各局等に付随する出張所及び出先事務所等の施設内（以下「庁舎内」という。）における通信回線及び通信回線装置を、施設管理部門と連携し、適切に管理すること。また、通信回線及び通信回線装置に関連する文書を適切に保管すること。

② 外部ネットワークへの接続を必要最低限に限定し、可能な限り、接続ポイントを減らすこと。

③ 機密性Ａ又は機密性Ｂ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、適切な回線を選択すること。また、必要に応じて、送受信される情報の暗号化を行うこと。

④ ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なサイバーセキュリティ対策を実施すること。

⑤ 可用性Ａ又は可用性Ｂの情報資産を取り扱う情報システムに関す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すること。また、必要に応じて、回線を冗長構成にするなどの措置を講じること。

5.4 端末や業務用外部記録媒体等の管理

(1) 業務用端末等の管理

情報システム管理者は、職員等が使用する業務用端末について、盗難防止を目的とした物理的措置を、次のとおり講じなければならない。

① 業務用端末に関して、電源起動時のパスワード（ＢＩＯＳパスワード、ハードディスクパスワード等）の入力と、情報システムへのログイン時のパスワード入力を併用すること。

② マイナンバー利用事務（個人番号利用事務）系の情報システムで使用する端末では、多要素認証等を行うよう設定すること。

③ 業務用端末におけるデータの暗号化等の機能を有効に利用すること。なお、端末にセキュリティチップが搭載されている場合、その機能を有効に活用すること。

④ 職員等が、庁舎外での業務において、業務用端末を利用する際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じること。

(2) 業務用外部記録媒体の管理

情報資産を所管する者は、職員等に対し、やむを得ず、電磁的な情報を業務用外部記録媒体に保管する等の許可を与えた場合は、当該目的で使用する業務用外部記録媒体について、紛失及び盗難等防止を目的とした物理的措置を、次のとおり講じなければならない。

① 組織名等の視認しやすい表示を行うこと。

② 業務上、必要最小限の保有数とし、施錠できる保管庫等にて適切に管理・保管した上、当該管理・保管状況が確認できるよう、管理簿等を作成するなどし、定期的に紛失等がない旨を確認すること。

③ 管理・保管している業務用外部記録媒体が不要となった場合は、３(2)⑩に基づき、当該業務

用外部記録媒体内部の情報を復元できないように消去した上で廃棄させること。

④　業務用外部記録媒体を使用させる場合は、記録するデータについて、暗号化又はパスワード設定の措置を講じさせること。

6　人的セキュリティ

6.1　職員等の遵守事項

(1)　サイバーセキュリティポリシー等の遵守事項

全ての職員等は、サイバーセキュリティポリシー、実施手順、その他サイバーセキュリティの確保に必要な事項を遵守しなければならない。

また、サイバーセキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかにサイバーセキュリティ管理者に相談し、指示を仰ぐこと。

(2)　研修・訓練等への参加

全ての職員等は、定められたサイバーセキュリティ研修等に参加しなければならない。

(3)　職員等が利用するＩＤや付随するパスワード、各認証情報を記録した媒体等の取扱い

全ての職員等は、業務上での情報システム等の利用に当たって、個々の職員等を識別するために付与されたＩＤ（以下「利用者ＩＤ」という。）やそれに付随するパスワードのほか、ＩＤカード等について、次の事項を遵守しなければならない。

①　利用者ＩＤ及びＩＤカード等の取扱い

自己で管理する利用者ＩＤ及びＩＤカード等を、他人に貸与又は利用させないこと。

②　利用者ＩＤに付随するパスワードの取扱い

自己で管理する利用者ＩＤに付随するパスワードに関し、次の事項を遵守すること。

ア　他者からの照会等には一切応じないなど、第三者に知られないよう管理すること。

イ　他者から容易に推測されないように、十分な長さとし、推測が困難な文字列とすること。

ウ　仮のパスワードは、初回ログイン時に変更し、その後は、必要に応じて、定期的に変更すること。

エ　サーバ、ネットワーク機器及び業務用端末について、パスワード記憶機能を利用しないこと。

オ　複数の職員等間において共有しないこと。ただし、情報システム等で共有するＩＤに関するものは除くものとする。

カ　複数の情報システム等において、共有しないこと。

キ　自己のパスワードが流出したおそれがある場合は、情報資産を所管する者に速やかに報告し、指示に従うこと。

(4)　業務用端末における利用上の遵守事項

全ての職員等は、業務用端末の使用において、次の事項を遵守しなければならない。

①　業務以外の目的での使用の禁止

業務以外の目的で業務用端末を使用し、情報システム等へのアクセスのほか、電子メールアドレスの使用、Ｗｅｂサイトの閲覧等を行うためのインターネットへのアクセス等を行わないこと。

② 盗難防止の対策

盗難防止のため、庁舎内の自席において未使用時の場合は施錠可能な引き出し等に保管する等の対策を講じ、庁舎外などの自席以外にて使用する場合においても、自己の責任により手の届く範囲内で管理すること。

③ 庁舎外への業務用端末の持ち出し及び庁舎外での情報処理作業の制限

ア 職員等は、機密性A若しくは機密性B、完全性A若しくは完全性B又は可用性A若しくは可用性Bの情報資産を庁舎外に持ち出し、庁舎外において情報処理作業を行う場合は、本対策基準及び各局で定められた実施手順に基づき、実施すること。

イ 東京都が管理する業務用端末、業務用外部記録媒体、情報資産及びソフトウェアを庁舎外に持ち出す場合又は庁舎外で情報処理業務を行う場合には、あらかじめ、サイバーセキュリティ管理者又は当該情報処理機器類等を所管する情報システム管理者が指名する者の許可を得た上で実施すること。なお、庁舎外での情報処理作業の際、業務用端末の画面に表示される揮発性の情報等については、情報資産の持ち出しには該当しないものとする。

ウ 庁舎外での情報処理作業の際、画面に表示された情報を第三者により無断で閲覧されることがないように、周りに人が多い状況等で利用しないこと。

④ 機器構成の変更の制限

業務用端末について、無断で機器の改造及び増設・交換を行わないこと。ただし、業務遂行上、他の手段により難い場合で、かつ、情報資産を所管する者の許可を得た場合は、この限りではない。

⑤ ソフトウェア等の更新

業務用端末に対するソフトウェア等の更新がなされる場合は、サイバーセキュリティ管理者、情報システム管理者又は局ＣＳＩＲＴ等の指示に従い、確実に実施すること。

⑥ 無許可のソフトウェア等の導入禁止

業務用端末に対し、ソフトウェアや定型的な事務作業等の自動化を目的として職員等自らが作成したマクロ等を無断で導入しないこと。ただし、あらかじめ、情報資産を所管する者により、導入予定の端末や関連する情報システムに対する影響がないこと、かつ、業務遂行上、必要であると判断され、当該情報資産を所管する者の許可を得た場合は、この限りではない。

なお、不正にコピーした又は出所の不明なソフトウェアは一切、使用してはならない。

⑦ 不正プログラム情報及びぜい弱性情報の確認

東京都ＣＳＩＲＴ、局ＣＳＩＲＴ又は情報システム管理者が提供する不正プログラム情報及びぜい弱性情報を、常に確認すること。

(5) 情報資産の盗用防止

全ての職員等は、情報処理作業を行うに当たって、次のとおり、対策を講じなければならない。

① 業務用端末の画面に表示された情報を、サイバーセキュリティ管理者の許可なく第三者に無断で使用されないよう、離席時には当該端末の画面ロックを実施すること。

② 機密性Ａ又は機密性Ｂの情報が保存された業務用外部記録媒体や当該情報が印刷された文書を使用して情報処理作業を行う場合は、サイバーセキュリティ管理者の許可なく、第三者に情報を閲覧されるなどの無断使用を避けるため、離席する際は、必要に応じて、当該情報資産を適切な場所へ保管するなどの措置を講じること。

(6) 業務以外の目的による情報資産の持ち出し等の禁止

全ての職員等は、業務以外の目的で情報資産を庁舎外へ持ち出してはならない。

(7) 電子メール等の利用

全ての職員等は、電子メール等の利用にあたって、次の事項を遵守しなければならない。

① 電子メール等の利用に当たって、適正な利用方法を理解した上で使用すること。

② 自動転送機能を用いて、電子メールを転送しないこと。

③ 業務上必要のない電子メールを送信しないこと。

④ 電子メールによる情報漏えいを防止するため、都民等外部の複数人に同時に電子メールを送信する場合、ＢＣＣ欄にメールアドレスを入力するなど、同時に送信する送信先アドレスが他者に知られないように設定すること。

⑤ 重要な電子メールを誤送信した場合、直ちにサイバーセキュリティ管理者に報告すること。

⑥ 内部事務（ＬＧＷＡＮ接続）系の情報システムで提供する電子メール以外の電子メールサービス等（約款で利用できるメールサービス等）を業務で使用しないこと。

⑦ 外部の者にファイルを添付した電子メールを送信する場合には、電子署名のほか、添付ファイルの暗号化又はパスワード設定などのセキュリティを考慮した措置を講じたうえで送信を実施すること。

なお、暗号化を行う場合は、定められた方法で行い、暗号のための鍵を適切に管理すること。

⑧ 外部の者からファイルが添付された電子メールを受信した場合には、必要に応じて、不正プログラム対策ソフトウェア等にてチェックした上で、添付ファイルを展開すること。

(8) 業務用端末以外のパソコン及びモバイル端末（以下「私物端末」という。）の業務における利用

全ての職員等は、原則、私物端末及び業務用外部記録媒体以外の外部記録媒体を業務で利用してはならない。ただし、私物端末については、業務遂行上、必要であると情報資産を所管する者が認めた場合は、この限りではない。

なお、私物端末を業務にて利用することを許可された場合は、情報漏えいや不正プログラムへの感染等のリスクに対し、次の措置を講じた上で利用しなければならない。

① 不正プログラム等で遠隔操作され、盗聴されないように不正プログラム対策等を行うこと。

② 当該私物端末を外部記録装置として利用しないこと。

③ 自己が管理する私物端末が発端となって、他の業務用端末が外部からの不正プログラムに感染しないように注意すること。

④ 内部ネットワークに接続しないこと。

(9)　各種報告義務

全ての職員等は、本対策基準に対する違反のほか、サイバーセキュリティインシデントについて、速やかに報告しなければならない。

①　本対策基準に対する重大な違反行為を発見した場合は、速やかに、情報資産を所管する者に報告すること。なお、当該違反行為が、サイバーセキュリティに重大な影響を及ぼす可能性があると、情報システム管理者において判断され、指示があった場合は、その指示に従うこと。

②　東京都が管理する情報資産について、サイバーセキュリティインシデントの発生又はそのおそれがある事象を認知した場合又は都民等外部から報告を受けた場合は、速やかにＩＣＴリーダー又は局ＣＳＩＲＴに報告すること。

また、自己が使用している業務用端末又は業務上での利用を許可された私物端末において、差出人不明のファイル又は不自然なファイルが添付された不審なメールを受信した場合や不正プログラムへの感染があった又は疑われる場合においても、直ちにネットワークから遮断した上で、同様に報告すること。

(10)　退職時等の対応

全ての職員等は、異動や退職等により業務を離れる場合には、速やかに、利用していた情報資産を返却するとともに、業務上知り得た情報を一切漏らしてはならない。

6.2　管理者の遵守事項

(1)　サイバーセキュリティポリシー等の掲示

サイバーセキュリティ管理者は､職員等が常にサイバーセキュリティポリシー及び実施手順等を閲覧できるように掲示しなければならない。

(2)　業務用端末の管理

①　業務用端末におけるセキュリティ設定変更の禁止

情報システム管理者は、職員等が業務用端末のソフトウェア（不正プログラム対策ソフトウェア等）に関するセキュリティ機能の設定を変更できないよう対策を講じなければならない。

②　不正プログラム対策

情報資産を所管する者は、外部からデータ又はソフトウェアを取り入れようとする場合は、必ず、不正プログラム対策ソフトウェアによるチェックを行うなど、無害化を図るよう周知しなければならない。

情報システム管理者は、業務用端末に対して、必要に応じて、不正プログラム対策ソフトウェアによる全領域のチェックを定期的に実施するよう周知しなければならない。

③　持ち出し及び持ち込みの記録

サイバーセキュリティ管理者は、業務用端末等の持ち出し及び持ち込みについて、必要に応じて確認できるよう、記録簿等を作成し、保管しなければならない。

(3)　職員等に関する利用者ＩＤ及びＩＤカード等に関する対策

情報システム管理者は、情報システムの不正利用を防止するため、職員等が情報システムを利用する際に使用する利用者ＩＤやＩＤカード等について、次の対策を講じなければならない

① 職員等に関する利用者ＩＤの登録、変更、抹消等の情報管理、職員等の異動、出向、退職に伴う利用者ＩＤの取扱い等の方法を定めること。

② 利用されていない利用者ＩＤが放置されないよう、人事管理部門と連携し、適宜、点検すること。

③ 複数の職員等に、一つの利用者ＩＤを共用させる場合は、その対象者を選定し、当該対象者である職員等以外が利用することがないよう、職員等に求めること。

④ 職員等より、ＩＤカード等の紛失等の報告があった場合は、速やかに、当該ＩＤカード等を使用してのアクセスを停止すること。

⑤ 職員等のＩＤカード等を切り替える場合は、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄すること。

⑥ ③に基づき、複数の職員等による共有を許可したＩＤカード等については、管理担当者を指名し、適切な管理を行わせること。

(4) 職員等が所持する私物端末の業務上での利用の制限

① サイバーセキュリティ管理者は、職員等が所持する私物端末を業務上で利用することを原則禁止しなければならない。ただし、サイバーセキュリティ管理者が、業務上での利用の必要性等を確認し、業務上での利用が妥当であると認めた場合は、この限りではない。私物端末の利用を認めた場合は、6.1(8)に定める事項を職員等に遵守させるほか、管理簿の作成等により、必要に応じて、当該私物端末の使用状況等を確認できるようにしておくこと。

② 情報システム管理者は、職員等が所持する私物端末を、所管する情報システムに接続することを原則禁止しなければならない。ただし、①に基づき、サイバーセキュリティ管理者から業務上での利用を認めた私物端末について連絡を受けた場合には、所管する情報システムへの接続に係る支障の有無を確認し、支障がないと判断した場合は、当該私物端末に対して、必要なセキュリティ対策を講じるよう求めた上で、当該私物端末から所管する情報システムへの接続を許可することができる。

(5) 非常勤職員及び臨時職員への対応

サイバーセキュリティ管理者は、職員等のうち、非常勤職員及び臨時職員に対しては、次の措置を講じなければならない

① サイバーセキュリティポリシー等の遵守

採用時に、サイバーセキュリティポリシー等において守るべき事項について周知・啓発をし、実施及び遵守させること。

なお、必要に応じて、サイバーセキュリティポリシー等を遵守する旨の同意書への署名を求めることができるものとする。

② インターネット接続及び電子メール使用等の制限

業務用端末を使用させる場合には、担当する作業等に必要な権限のみを付与するものとする。

(6) 外部委託事業者等に対する説明

情報資産を所管する者は、情報システムの開発・保守等を外部委託事業者等に発注する場合、当該外部委託事業者等から再委託を受ける事業者も含めて、サイバーセキュリティポリシー等のうち、外部委託事業者等が守るべき内容の遵守及びその機密事項を説明しなければならない。

6.3 サイバーセキュリティ研修等

(1) 年度計画の策定

ＣＩＳＯ補佐官は全ての職員等を対象とし、また、サイバーセキュリティ局責任者は当該局等内を対象として、当該局等内の全ての職員等が、年１回以上、サイバーセキュリティ研修等を受講できるよう、それらに関する年度計画を毎年度、策定しなければならない。

なお、研修に関しては、職員等に対して、それぞれの役割、サイバーセキュリティに関する理解度等に応じた内容となるように設定し、また、訓練においては、各情報システム等の規模等を考慮した上で範囲を定め、効果的に実施できるようにしなければならない。

(2) サイバーセキュリティに関する研修の実施

ＣＩＳＯ補佐官及びサイバーセキュリティ局責任者は、(1)で定めた年度計画に基づき、定期的に、サイバーセキュリティに関する研修を実施しなければならない。

(3) サイバーセキュリティインシデント対応訓練の実施

ＣＩＳＯ補佐官及びサイバーセキュリティ局責任者は、(1)で定めた年度計画に基づき、サイバーセキュリティインシデント対応を想定した訓練を、定期的に実施しなければならない。

(4) 職員等に対する研修及び訓練への参加の周知

サイバーセキュリティ局管理者は、サイバーセキュリティの実施に関わる全ての職員等に対し、定められた研修及び訓練に参加するよう周知しなければならない。

6.4 サイバーセキュリティインシデントの報告及び原因究明等の対応

(1) 局ＣＳＩＲＴの対応

① 局ＣＳＩＲＴは、各局等内の職員等から、サイバーセキュリティインシデントの報告を受けた場合には、報告されたセキュリティインシデントの可能性について、当該サイバーセキュリティインシデントが発生した部門の情報資産を所管する者と連携して状況を確認し、当該セキュリティインシデントに関する評価を行い、速やかにサイバーセキュリティ局管理者及び東京都ＣＳＩＲＴに報告しなければならない。

② 局ＣＳＩＲＴは、東京都ＣＳＩＲＴと連携し、当該サイバーセキュリティインシデントの原因を分析し、記録し、及び保管しなければならない。また、局ＣＳＩＲＴは、必要に応じて、

再発防止策を検討すること。

⑵　東京都ＣＳＩＲＴの対応

東京都ＣＳＩＲＴは、各局等内の局ＣＳＩＲＴから報告を受けた場合は、報告のあったサイバーセキュリティインシデントについて、速やかに、サイバーセキュリティ統括管理者に報告するとともに、当該局ＣＳＩＲＴからの依頼に応じて、当該局ＣＳＩＲＴを支援しなければならない。

また、局ＣＳＩＲＴを支援する場合も含め、サイバーセキュリティインシデントの原因を分析し、記録し、及び保管しなければならない。また、必要に応じて、再発防止策を検討すること。

⑶　サイバーセキュリティ統括管理者の対応

サイバーセキュリティ統括管理者は、東京都ＣＳＩＲＴから報告を受けた場合は、当該サイバーセキュリティインシデントについて、ＣＩＳＯ補佐官に報告するとともに、局ＣＳＩＲＴに対する支援内容も含め、東京都ＣＳＩＲＴの活動内容を管理し、監督しなければならない。

⑷　ＣＩＳＯ補佐官の対応

ＣＩＳＯ補佐官は、サイバーセキュリティ統括管理者から報告を受けた場合は、サイバーセキュリティインシデントのレベルに応じて、報告のあったサイバーセキュリティインシデントについて、ＣＩＳＯに報告しなければならない。

⑸　ＣＩＳＯの対応

ＣＩＳＯ補佐官から報告を受けたＣＩＳＯ は、その内容を確認し、ＣＩＳＯ補佐官及びサイバーセキュリティ局統括責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示をしなければならない。

また、必要に応じて、都民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

7　技術的セキュリティ

7.1　コンピュータ及びネットワークの管理

⑴　ファイルサーバの設定等

情報資産を所管する者は、職員等が利用可能なファイルサーバを設置する場合には、次の措置を講じなければならない。

①　ファイルサーバの容量を適切に設定すること。

②　ファイルサーバは適正なアクセス権限を設定すること。

⑵　バックアップの実施

情報資産を所管する者は、情報システム等やファイルサーバ等に記録された情報について、5.1⑵にかかわらず、総合重要度に応じて、定期的にバックアップを実施しなければならない。

⑶　他団体との情報システムに関する情報等の交換

情報システム管理者は、職員等が、外部の団体等との間で、情報システムに関する情報及びソフトウェアを交換しようとする場合は、あらかじめ、その取扱いに関する事項を定め、ＣＩＳＯの許可を得た上で、実施させなければならない。

(4)　システム管理記録及び作業の確認

情報システム管理者は、所管する情報システムに関する運用・管理について、次の対策を講じなければならない。

①　運用時の作業について、作業記録を作成すること。

②　機器、プログラム、設定等のシステム変更等を行った場合は、その内容について記録を作成し、詐取、改ざん等をされないように適切に管理すること。

③　情報システム管理者のほか、情報システム担当者及び契約により操作を認められた外部委託事業者等がシステム変更等を行う場合は、２名以上で作業し、互いにその作業を確認すること。

(5)　情報システムに関する設計図等の管理

情報システム管理者は、システム設計図、ネットワーク構成図、仕様書、ソースコード、テスト結果その他情報システムに関する一切の資料等について、業務上必要とする者以外の者による閲覧、紛失等がないよう、適切に管理しなければならない。

(6)　ログの取得等

情報システム管理者は、ログの取得等に際し、次の対策を講じなければならない。

①　各種ログ及びサイバーセキュリティの確保に必要な記録を取得し、一定の期間保存すること。

②　ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理すること。

③　取得したログを定期的に点検し、分析する機能を設け、必要に応じて、悪意ある第三者等による不正侵入、不正操作等の有無について点検又は分析を実施すること。

(7)　障害記録

情報システム管理者は、職員等からの情報システムに関する障害の報告のほか、システム等障害に対する処理結果又は問題等について、障害記録として記録し、適切に保存しなければならない。

また、ＣＩＳＯから説明等の求めがあった場合、これに応じなければならない。

(8)　ネットワークの接続制御、経路制御等

情報システム管理者は、ネットワークの接続について、次の対策を講じなければならない。

①　フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定すること。

②　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すこと。

③　6.2(4)②により、職員等が所持する私物端末について、内部ネットワークへの接続を許可し

た場合には、当該私物端末の全てにおいて、必要なセキュリティ対策を講じるよう職員等に求めること。

(9)　外部の者が利用できるサービスの分離等

情報システム管理者は、サービスの分離等について、次の対策を講じなければならない。

①　電子申請の汎用受付システム等、外部の者が利用できるサービスについて、必要に応じて、他のネットワーク及び情報システムと物理的に分離する等の措置を講じること。

②　外部の者が利用することを前提とした無線ＬＡＮを設置する場合には、次の対策を講じること。

ア　無線ＬＡＮ上を流れる情報の盗聴を防ぐため、解読が困難な暗号化技術を用いること。

イ　無線ＬＡＮアクセスポイントへの不正アクセスを防ぐため、強固な認証技術を用いること。

ウ　無線ＬＡＮの利用期間中においてアクセスログを取得・保存すること。

(10) 外部ネットワークとの接続制限等

情報システム管理者は、所管するネットワークについて、次の措置を講じなければならない。

①　外部ネットワークと接続しようとする場合には、ＣＩＳＯの許可を得ること。

②　接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、内部の全てのネットワーク及び情報システムの情報資産に影響が生じないことを確認すること。

③　接続した外部ネットワークの瑕疵（かし）により、データの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保すること。

④　Ｗｅｂサーバ等をインターネットに公開する場合、内部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すること。

⑤　接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、ＣＩＳＯ補佐官の判断に従い、速やかに当該外部ネットワークを物理的に遮断すること。

⑥　外部ネットワークとの接続に際しての仕様、制限条件、及び障害発生時の連絡体制等、必要な事項を当該外部ネットワーク管理者との間で定めておくこと。

⑦　⑥で定めた事項について、ＣＩＳＯ補佐官に報告すること。

(11) 複合機のセキュリティ管理

サイバーセキュリティ管理者は、複合機の使用に当たり、次の措置を講じなければならない。

①　複合機の機能及び設置環境並びに当該複合機が取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定すること。

②　複合機の機能について適切な設定を行うことにより、当該複合機に対するサイバーセキュリ

ティ対策を講じること。

③　複合機の撤去、保守作業における記録装置の交換、複合機の代替品の提供等において、当該複合機上の情報が漏えいしないよう、３(2)⑩に基づき、適切に対処すること。

(12) 特定用途機器のセキュリティ管理

情報システム管理者は、特定用途機器（テレビ会議システム、ＩＰ電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途に使用される情報システムであり、通信回線に接続し、又は電磁的記録媒体を内蔵している機器等）について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、必要に応じて、当該機器の特性に応じた措置を講じなければならない。

(13) 無線ＬＡＮのセキュリティ対策

ネットワークを所管する情報システム管理者は、職員等による無線ＬＡＮを利用した業務用端末での業務の実施に当たって、次の措置を講じなければならない。

①　職員等が無線ＬＡＮを利用して業務用端末を使用することを前提とし、情報の盗聴を防ぐため、解読が困難な暗号化技術を用いること。

②　無線ＬＡＮを設置（拡張等を含む。）する場合は、ＣＩＳＯ補佐官に報告するとともに、無線ＬＡＮアクセスポイントへの不正アクセスを防ぐため、強固な認証技術を用いること。

③　無線ＬＡＮアクセスポイントを設置する場合は、必要に応じて、電波の外部への漏えい及び干渉を防止すること。

④　無線ＬＡＮの利用期間中においてアクセスログの取得・保存をすること。

⑤　その他、機密性に応じた必要な対策を検討すること。

(14) 電子メールのセキュリティ対策

情報資産を所管する者は、職員等の電子メールの利用に当たって、次の措置を講じなければならない。

①　導入時の対策

ア　外部の利用権限のない利用者により、外部から外部への電子メール転送（電子メールの不正な中継処理）を行うことを不可能とするよう、電子メールサーバを設定すること。

イ　電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。

ウ　電子メールのなりすましの防止に努めること。

エ　インターネットを介して通信する電子メールの盗聴及び改ざんの防止に努めること。

オ　職員等に対し、遵守事項及び適正な利用方法を周知した上で利用させること。

②　運用時の対策

ア　大量のスパム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するなど、必要な措置を講じること。

イ　職員等が利用するメールの送受信容量の上限を設定し、上限を超える電子メールの送受信

を不可能にするとともに、メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知すること。

ウ　電子メールのなりすましの防止策を講じること。

エ　システム開発、運用等のため庁舎内に常駐している外部委託事業者等の作業員による電子メール利用について、当該外部委託事業者等との間で利用方法を取り決めること。

③　添付ファイルの無害化

職員等に、添付ファイルが付いた電子メールを送受信させる場合は、不正プログラム対策ソフトウェアによるチェックを行う等の無害化を図るよう周知すること。

(15) Ｗｅｂサイト構築に対するセキュリティ対策

情報システム管理者は、Ｗｅｂサイトの構築・運用にあたり、サイバーセキュリティ確保のため、次の措置を講じなければならない。

①　Ｗｅｂサーバの導入・運用時の対策

ア　Ｗｅｂサーバが備える機能のうち、不要な機能を停止し、制限すること。

イ　Ｗｅｂコンテンツの編集作業を担当する職員等又は当該業務を委託した外部委託事業者等を限定すること。

ウ　公開してはならない又はサービスの提供に必要のないＷｅｂコンテンツが公開されないように、Ｗｅｂサーバに保存する情報を管理すること。

エ　Ｗｅｂコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理すること。

オ　インターネットを介して転送される情報の盗聴及び改ざんの防止のため、Ｗｅｂサイト全てのページをＨＴＴＰＳ化するとともに、電子証明書による認証の措置を講じること。

②　Ｗｅｂアプリケーションの開発時・運用時の対策

情報システム管理者は、Ｗｅｂアプリケーションの開発において、既知の種類のＷｅｂアプリケーションのぜい弱性を排除するための措置を講じること。また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行うこと。

(16) 電子署名・暗号化

情報システム管理者は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

また、職員等が、総合重要度Ａの情報システムに係るデータを外部に送る場合には、定められた電子署名、暗号化又はパスワード設定などのセキュリティを考慮した措置を講じたうえで、送信するよう、職員等に周知しておかなければならない。

7.2　アクセス制御

(1)　アクセス制御等

情報システム管理者は、職員等による情報システムへのアクセスについて、アクセスする権限のない職員等がアクセスできないよう、所管する情報システムごとに、次の措置を講じなければ

ならない。

① 職員等に関する利用者ＩＤの管理

ア 6.2(3)①で定める利用者ＩＤの取扱方法等に基づき、職員等に関する利用者ＩＤを適切に管理すること。

イ 6.2(3)②にて点検した結果に基づき、利用されていない利用者ＩＤがあった場合は、当該利用者ＩＤに関する利用の権限を削除する等、適切に措置すること。

ウ 6.2(3)③に基づき、共用を許可した利用者ＩＤについて、利用者である職員等以外には利用させてはならない。また、定期的に、その利用状況等を確認すること。

② 管理者権限等の特権を付与されたＩＤ（以下「特権者ＩＤ」という。）の管理等

管理者権限等の特権の悪用を防ぐため、特権者ＩＤについては、①の措置に加えて、次の措置を講じなければならない。

ア 特権者ＩＤを利用する者を必要最小限にするとともに、当該ＩＤのパスワードの漏えい等を防ぐため、当該ＩＤ及びパスワードを厳重に管理すること。

イ サイバーセキュリティ局統括責任者及びサイバーセキュリティ局責任者の特権を代行する者は、サイバーセキュリティ局責任者が指名し、サイバーセキュリティ局統括責任者が認めた者でなければならない。

ウ サイバーセキュリティ局統括責任者は、代行者を認めた場合、速やかに情報資産を所管する者に通知しなければならない。

エ 特権者ＩＤに付与されたパスワードは、速やかに、初期設定以外のものに変更させること。

オ 特権者ＩＤ及び当該ＩＤに付与されたパスワードに対する、変更頻度、入力回数制限等のセキュリティ機能については、職員等の利用者ＩＤに対するセキュリティ機能よりも強化すること。

カ 特権者ＩＤ及び当該ＩＤに付与されたパスワードの変更を、外部委託事業者等に無断で行わせないこと。

(2) 職員等による外部ネットワークから内部ネットワークへのアクセスの制限

ネットワークを所管する情報システム管理者は、職員等による外部ネットワークから内部ネットワークへのアクセスについて、アクセス権限のない職員等がアクセスできないよう、次の措置を講じなければならない。

① 職員等に対し、あらかじめ、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るよう求めること。

② 職員等による外部ネットワークから内部ネットワークへのアクセスについて許可する場合は、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、アクセス権を設定すること。

なお、許可に当たっては、情報システムにおいて利用者の本人確認を行う機能を確保するとともに、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ること。

③ 外部ネットワークからのアクセスが可能な端末を職員等に配備する場合、セキュリティ確保のために必要な措置を講じること。

④ 職員等が、庁舎外から持ち帰った業務用端末又は業務上の利用を許可された私物端末を、内

部ネットワークに接続しようとする場合は、接続前に、最新のパターンファイルを用いた不正プログラム対策ソフトウェアによるスキャン等で不正プログラムに感染していないことを確認したうえで接続させること。

⑤　職員等に対し、公衆通信回線を内部ネットワークに接続することを禁止すること。ただし、ＶＰＮ等による通信のセキュリティを確保した上で接続する場合には、ネットワークを所管する情報システム管理者は、接続を許可することができる。

(3)　自動識別の設定

情報システム管理者は、内部ネットワークで使用される機器について、原則、機器固有情報によって当該機器と内部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情報システムについて設定しなければならない。

(4)　利用者ＩＤ及び特権者ＩＤに関するログイン設定等

情報システム管理者は、利用者ＩＤ及び特権者ＩＤに関するログイン時の管理について、次の措置を講じなければならない。

①　利用者ＩＤについては、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定、ログイン・ログアウト時刻を表示すること等により、正当なアクセス権を持つ職員等がログインしたことを職員等自身が確認できるよう情報システムを設定すること。

②　特権者ＩＤについても、①の設定と同様とする。ただし、接続時間については、業務上必要最小限に制限するよう設定すること。

(5)　認証情報の管理

情報システム管理者は、職員等に関する認証情報の管理において、次の措置を講じなければならない。

①　職員等の認証情報を厳重に管理すること。なお、認証情報ファイルを不正利用から保護するため、オペレーティングシステム等に認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用すること。

②　職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後、速やかに仮のパスワードから変更させること。

③　認証情報の不正利用を防止するための措置を講じること。

7.3　情報システムの開発、導入、保守等

(1)　情報システムの開発、導入、保守等に関する調達

情報システム管理者は、調達しようとする情報システム及びソフトウェアが本対策基準を満たすことを確実なものとするため、次の措置を講じなければならない。

①　情報システム及びソフトウェアの開発、導入、保守等の調達に当たっては、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すること。

② 機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、サイバーセキュリティ上、問題のないことを確認すること。

③ 機器及びソフトウェアの調達に当たっては、機器等におけるリース又は償却期間において、最新のセキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関するぜい弱性対策計画を策定するなど、サイバーセキュリティ対策の速やかな支援を得られるよう、契約書等に明記すること。

(2) 情報システムの開発時における管理

情報システム管理者は、開発しようとする情報システムが本対策基準を満たすことを確実なものとするため、次の措置を講じなければならない。

① システム開発における責任者及び作業者の特定

システム開発における責任の所在及び実施体制を把握するため、責任者及び作業者について、職員等又は外部委託事業者等の中から特定すること。

② システム開発における責任者用及び作業者用のＩＤの管理

システム開発で用いられる開発用ＩＤの不正利用等を防ぐため、次の措置を講じること。

ア システム開発の責任者及び作業者が使用する開発用ＩＤを管理し、開発完了後、当該開発用ＩＤを削除すること。

イ システム開発の責任者及び作業者のアクセス権限を設定すること。

③ システム開発に用いるハードウェア及びソフトウェアの管理

システム開発で用いられる開発用のハードウェア及びソフトウェアがもたらすサイバーセキュリティインシデントを防ぐため、次の措置を講じること。

ア 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すること。

イ アで特定したソフトウェア以外のソフトウェアがインストールされている場合は、速やかに、情報システムから削除させること。

(3) 情報システムの導入

情報システム管理者は、情報システムが本対策基準を満たすことを確実なものとするため、次の措置を講じなければならない

① 開発環境と運用環境の分離及び移行手順の明確化

情報システム管理者は、運用環境で使用しているプログラム及びファイルの誤消去、故意による改変等を防ぐため、次の措置を講じること。

ア 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すること。

イ 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すること。

ウ 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すること。

エ　(2)③アにおいて、特定したソフトウェアについて、導入後又は移行後のシステム運用においても必要であると認める場合を除き、情報システムから削除すること。

オ　エのソフトウェア以外に、新たに導入予定のソフトウェアがある場合には、移行前に、当該ソフトウェアに対するぜい弱性及び不正プログラム等の脅威がないことを確認すること。

カ　導入するサービス又は情報システムの可用性が確保されていることを負荷テスト等により確認した上で導入すること。

② テスト

情報システム管理者は、運用環境への移行テストがもたらしうるサイバーセキュリティインシデントを防止するため、次の措置を講じること。

ア　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うこと。

イ　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うこと。

ウ　個人情報及び機密性の高いデータを、テストデータに使用しないこと。

エ　開発したシステムについて受入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行うこと。

(4)　システム開発・保守に関連する資料等の整備・保管

情報システム管理者は、システム開発・保守に関連する資料等について、保守及び機器更新の際に必要となるだけでなく、外部に漏えいした場合は攻撃に利用されるおそれがあるため、次の措置を講じなければならない。

① システム開発・保守に関連する資料及び文書を適切な方法で保管すること。特に、ネットワーク構成図、情報処理システム仕様書について、機密性Aとし、業務上必要とする者以外の者による閲覧、紛失等がないよう、適切に管理すること。

② テスト結果を一定期間保管すること。

③ 情報システムに係るソースコードを適切な方法で保管すること。

(5)　情報システムにおける入出力データの正確性の確保

情報システム管理者は、情報システムによる処理の正確性を確保するとともに、不正な入力を受け付けることによる情報漏えい等を防ぐため、次の措置を講じなければならない。

① 情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むよう、設計すること。

② 故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むよう、設計すること。

③ 情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるよう、設計すること。

(6)　情報システムの変更管理

情報システム管理者は、情報システムの変更による障害等を防ぐため、次の措置を講じなけれ

ばならない。

① 情報システムを変更する場合は、その変更目的を明らかにし、変更によるセキュリティ上のリスクについて検証すること。

② プログラム仕様書等の変更履歴を作成すること。

(7) 開発・保守用のソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェア等の更新又は修正プログラムの適用をする場合は、ソフトウェアのバージョンの違いによる障害等を防ぐため、影響の有無を事前に確認しなければならない。

(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、システム更新・統合時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・統合後の業務運営体制の検証を行わなければならない。

7.4 ソフトウェアに関するぜい弱性対策

情報資産を所管する者は、次の事項を措置しなければならない。

① 情報システムの導入又は運用開始時に、当該情報システムで利用するソフトウェアに関連する公開されたぜい弱性についての対策を実施すること。

② 情報システムで利用するソフトウェアにおけるぜい弱性対策の状況を定期的に確認すること。

③ ぜい弱性対策の状況の定期的な確認により、ぜい弱性対策が講じられていない状態が確認された場合又は情報システムで利用するソフトウェアに関連するぜい弱性情報を入手した場合には、最新のセキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関するぜい弱性対策計画を策定し、措置を講じること。

7.5 不正プログラム対策

情報資産を所管する者は、サイバーセキュリティ確保のため、次の措置を講じなければならない。

① 外部ネットワークと送受信するファイルについて、ゲートウェイにおいて、不正プログラム対策ソフトウェアによるチェックを行う等の無害化を図り、内部の情報システムへの不正侵入又は外部への拡散を防止すること。

② 不正プログラムに関する情報を収集し、必要に応じて、職員等に対して注意喚起すること。

③ 所管するサーバ及び端末等に、不正プログラム対策ソフトウェア等を常駐させた上、当該不正プログラム対策ソフトウェア及びそのパターンファイルはついては、定期的に更新し、常に最新の状態に保つこと。

なお、インターネットに接続していないサーバ及び端末等についても、同様とする。

④ 情報システムで利用するソフトウェア（ＯＳを含む。）については、修正プログラムやバー

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はならない。

⑤　職員等に対し、情報システムにおいては、東京都が管理している業務用外部記録媒体のみを使用させること。

7.6　不正アクセス対策

(1)　事前対策

情報システム管理者は、不正アクセス対策として、あらかじめ、次の措置を講じなければならない。

①　使用されていないＴＣＰ／ＵＤＰポートを閉鎖すること。

②　不要なサービスについて、機能を削除又は停止すること。

③　重要な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すること。

④　不正アクセスによるＷｅｂサイトの改ざんを検知するために、データの書換えを検出する措置を講じること。

また、改ざんを検知した場合に速やかに情報資産を所管する者へ通知する体制を確立すること。

(2)　外部からの攻撃への備え

情報システム管理者は、サーバ等への攻撃を受けた場合、受けることが明確になった場合又は受ける可能性が高くなったと判断した場合は、情報システムの停止を含め、それぞれの攻撃に応じた措置を講じなければならない。

なお、攻撃を受けた場合は、当該攻撃が不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）違反等の犯罪の可能性があることを念頭に、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。

①　サービス不能攻撃

外部からアクセスできる情報システムについて、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、次の措置を講じること。

ア　情報システムの可用性がＡ又は可用性Ｂの場合、サービス不能攻撃を検知できるようにすること。

イ　情報システムの可用性がＡの場合、サービス不能攻撃を拒否又は無効化できるようにすること。

②　標的型攻撃

複数の攻撃段階を経て、攻撃者の目的が遂行されることを念頭に、外部ネットワークと接続している情報システムについて、次の措置を講じること。

また、外部ネットワークに接続していない情報システムについても、必要に応じて、同様とする。

ア　7.5 の対策を確実に実施し、既知の不正プログラムに感染することを未然に防ぐこと。

また、総合重要度がＡの情報システムにおいては、新たな不正プログラムの侵入を検出できるようにすること。

イ　業務用端末又はサーバ等が不正プログラム等に感染した場合を鑑み、業務用端末又はサーバ等が、攻撃者の用意したサーバと通信することを防ぐ又はその動きを検出できるようにすること。

ウ　業務用端末又はサーバ等が攻撃者により、リモートにて操作されうる状態となった、又はその可能性がある場合において、攻撃者により内部ネットワークの探査や情報収集等の行動を防ぐ又はその動きを検出できるようにすること。

エ　攻撃者により情報がネットワーク経由で外部に送信されることを防ぐ又は検出できるようにすること。

(3)　内部における不正行為等への対策

情報システム管理者は、職員等の内部における対策として、次の措置を講じなければならない。

①　所管する情報システム及び外部のＷｅｂサイト等に対する攻撃への対処

職員等及び外部委託事業者等が使用している端末等から所管する情報システムに対する攻撃及び外部のＷｅｂサイト等に対する攻撃を直ちに察知できるよう、監視すること。

②　職員等による不正アクセス時の対処

職員等による不正アクセス又はその痕跡を発見した場合には、当該職員等が所属する課のサイバーセキュリティ管理者に連絡し、適切な処置を求めること。

7.7　サイバーセキュリティに関する専門家による支援体制の整備

ＣＩＳＯ補佐官は、東京都において実施している不正プログラム対策や不正アクセス対策等では不十分な事態が発生した場合に備え、外部のサイバーセキュリティに関する専門家の支援を受けられるようにしておかなければならない。

7.8　セキュリティ情報の収集及び共有並びに情報システムへの反映

(1)　セキュリティ情報の収集・共有

サイバーセキュリティ統括管理者及びサイバーセキュリティ局管理者は、東京都が保持する情報資産を脅威等から保護するため、次の対策を講じなければならない。

①　セキュリティホールに関する情報を収集し、必要に応じて、職員等及び関係者間で共有すること。

②　不正プログラム等のセキュリティ情報を収集し、必要に応じて、対応方法も含めて、職員等及び関係者で共有すること。

③　サイバーセキュリティに関する情報を収集し、必要に応じて、職員等及び関係者間で共有すること。また、サイバーセキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じること。

(2)　情報システムへの共有情報の反映

情報資産を所管する者は、(1)で共有したセキュリティ情報について、情報システムの総合重要度に応じて、情報システムへ反映しなければならない。

8　運用

8.1　情報システムの監視

情報システム管理者は、情報システムへの攻撃・侵入、職員等の不正な利用、自らの情報システムが他の情報システムに対する攻撃に悪用されたこと等を検知するため、次の措置を講じなければならない。

① 情報システムについて、稼働時間における監視を実施すること。なお、総合重要度Ａ又は外部と接続している情報システムについては、常時監視すること。

② 不正アクセスの発生を事後的に検証できるよう、情報システムのアクセス記録について、次の措置を講じること。

ア　アクセス記録として取得する項目、保存期間、取扱方法及びアクセス記録が取得できなくなった場合の対処等について定めること。

イ　各種アクセス記録及びサイバーセキュリティの確保に必要な情報を取得し、一定の期間保存するなど適切にログを管理すること。

ウ　アクセス記録等が窃取、改ざん、誤消去等されないように必要な措置を講じること。

エ　総合重要度Ａの情報システムについて、情報システムから自動出力したアクセス記録等について、必要に応じて、業務用外部記録媒体にバックアップすること。

オ　サーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じること。

8.2　サイバーセキュリティポリシーの遵守状況の確認

(1)　遵守状況の確認及び対処

サイバーセキュリティ局管理者は、2.1.2(2)③で定められた年度計画に基づき、サイバーセキュリティ対策の実施を指示し、その進捗状況をモニタリングするなどの対策を講じること。

① サイバーセキュリティポリシーを確実に運用していくため、情報システムの監視及びサイバーセキュリティポリシーの遵守状況の確認を実施し、情報資産に対するセキュリティ侵害及びサイバーセキュリティポリシー違反に対し、適正に対応すること。

② 各局にて策定したサイバーセキュリティ対策が年度計画に基づき確実に遂行されていることを確認するため、年度計画の進捗状況について、必要に応じて、モニタリングすること。

(2)　端末及び業務用外部記録媒体等の利用状況調査

ＣＩＳＯ補佐官及びサイバーセキュリティ統括管理者は、不正アクセス、不正プログラム等の調査が必要となる事案が発生した場合は、職員等が使用している業務用端末及び業務用外部記録媒体等の使用に関するログのほか、電子メールの送受信記録やＷｅｂサイトの閲覧履歴記録等を基に、利用状況について調査しなければならない。

(3)　サイバーセキュリティに対する違反時の対応

サイバーセキュリティに対する違反等に対し、速やかに、次の措置を講じなければならない。

① 情報資産を所管する者は、職員等によるサイバーセキュリティポリシーの遵守状況について問題が認められた場合は、発生した問題について、速やかに、サイバーセキュリティ統括管理

者又は当該職員等が所属する局等のサイバーセキュリティ局責任者に通知し、適切な措置を求めること。

② 情報システム管理者は、東京都が管理する情報処理機器類について、職員等による業務以外の目的での使用が明らかであると認める場合は、その程度及び状況に応じ、当該職員等が所属する局等のサイバーセキュリティ管理者に通知し、適切な対策を求めること。

③ 情報資産を所管する者は、違反行為が、直ちにサイバーセキュリティ上重大な影響を及ぼす可能性があると判断された場合は、局ＣＳＩＲＴの指示に従って、速やかに対処すること。

④ 情報資産を所管する者は、違反及び対応のうち重大な事案について、サイバーセキュリティ局責任者及びサイバーセキュリティ統括管理者に報告すること。

8.3 例外措置

(1) 例外措置の許可

情報資産を所管する者は、サイバーセキュリティ関係規定を遵守することが困難な状況であって、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には、期間を明示して、ＣＩＳＯの許可を得た上で、例外措置（遵守事項とは異なる方法を採用した措置をいう。以下同じ。）を実施することができる。

(2) 緊急時の例外措置

情報資産を所管する者は、行政事務及び公共インフラ事業の遂行に緊急を要する等の場合であって、例外措置を実施したときは、事後速やかにＣＩＳＯに報告しなければならない。

(3) 例外措置に関する申請書の管理及び確認

ＣＩＳＯ補佐官は、例外措置の申請書及び審査結果について、適切に保管した上、定期的に申請状況を確認しなければならない。

(4) 例外措置の状況確認に対する対応

サイバーセキュリティ局統括責任者は、ＣＩＳＯ補佐官より、ＣＩＳＯが許可した例外措置について報告を求められた場合は、その求めに応じなければならない。

なお、11 に基づき、サイバーセキュリティ局統括責任者が行った特例措置について、ＣＩＳＯ補佐官がサイバーセキュリティ局統括責任者に対して情報提供を求めた場合も同様とする。

8.4 法令遵守

職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令の遵守について、サイバーセキュリティ局統括責任者は、職員等に徹底しなければならない。また、職員等は、これらを遵守しなければならない。

① 地方公務員法（昭和 25 年法律第 261 号）

② 著作権法（昭和 45 年法律第 48 号）

③ 不正アクセス行為の禁止等に関する法律

④ 個人情報の保護に関する法律（平成 15 年法律第 57 号）

⑤ 東京都個人情報の保護に関する条例（平成 2 年東京都条例第 113 号）

⑥ 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(平成 25 年法律第 27 号)

⑦ 東京都特定個人情報の保護に関する条例（平成 27 年東京都条例第 141 号）

⑧ サイバーセキュリティ基本法（平成 26 年法律第 104 号）

8.5 違反時の処分等

サイバーセキュリティポリシーに違反し、重大なサイバーセキュリティインシデントを発生させた職員等及び重大なサイバーセキュリティインシデントを発生させかねない状況に至らしめた職員等並びにその管理監督者は、その重大性、発生した事案の状況等に応じて、地方公務員法による処分の対象となる。

9 外部サービスの利用

9.1 契約に基づき、外部サービスを利用する場合

(1) 外部委託事業者等の選定基準

情報資産を所管する者は、外部委託事業者等に業務を委託する場合には、次の措置を講じなければならない。

① 外部委託事業者等の選定に当たり、委託内容に応じたサイバーセキュリティ対策が確保されていることを確認すること。

② サイバー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、サイバーセキュリティ監査の実施状況等を参考にして、事業者を選定すること。

③ 外部委託事業者等及び外部委託事業者等から再委託を受けている事業者等に対して、サイバーセキュリティポリシーのうち、外部委託事業者等が遵守すべき事項について説明し、同意書等を求めること。

④ 外部委託事業者等に対し、サイバーセキュリティ実施体制及びサイバーセキュリティインシデント対応体制を整備・維持するよう指示すること。

(2) 外部委託時の契約又は協定項目

情報資産を所管する者は、(1)により、外部に業務を委託する場合には、当該外部委託事業者等との間で次のサイバーセキュリティに関する要件を明記した契約を締結しなければならない。

① サイバーセキュリティポリシー及び実施手順等の遵守

② 委託先の責任者、委託内容、作業者及び作業場所の特定

③ 提供されるサービスレベルの保証

④　外部委託事業者等にアクセスを許可する情報の種類と範囲、アクセス方法

⑤　従業員に対する教育の実施

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

⑦　業務上知り得た情報の守秘義務

⑧　再委託に関する制限事項の遵守

⑨　委託業務終了時の情報資産の返還、廃棄等

⑩　委託業務の定期報告及び緊急時報告義務

⑪　発注者又はサイバーセキュリティ局統括責任者による監査・点検・検査があり得ること及びその場合の協力義務

⑫　サイバーセキュリティインシデント発生時の報告及び対応の義務

⑬　遵守事項についての同意書等の提出

⑭　サイバーセキュリティに関する要件が遵守されず、サイバーセキュリティインシデントが発生した場合の規定（損害賠償等）

⑮　サイバーセキュリティインシデント発生時のインシデント内容、事業者名等の公表があり得ること。

(3)　確認・措置等

情報資産を所管する者は、(2)により、外部に業務を委託した場合には、外部委託事業者等において必要なサイバーセキュリティ対策が確保されていることを定期的に確認し、当該契約内容に基づく措置をしなければならない。

また、その重要度に応じて、ＣＩＳＯ及びＣＩＳＯ補佐官は、各局等に対し、各局等が実施した措置について報告を求めることがきる。

(4)　その他の契約における取扱い

情報システム管理者は、機器の賃借契約など、委託契約以外の契約について、サイバーセキュリティ確保の観点から必要と認める場合は、(1)から(3)までについて、必要に応じて、適用するものとする。

9.2　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の利用に係る規定の整備

情報資産を所管する者は、有料・無料にかかわらず、約款への同意又は簡易なアカウントとの登録等により利用することが可能となる外部サービス（以下「約款による外部サービス」という。）を職員等が利用しようとする場合は、機密性Ａ又は機密性Ｂの情報を取り扱わないよう徹底しなければならない。

ただし、業務遂行上他の手段によることができず、やむを得ず、利用を認める場合には、以下の事項を含む規程等をあらかじめ整備した上、職員等に周知しなければならない。

①　約款による外部サービスを利用してよい業務の範囲

② 利用許可の対象となる外部サービス名

③ 利用手続及び運用手順

(2) 約款による外部サービスの利用における対策の実施

情報資産を所管する者は、(1)において、約款による外部サービスの利用を認めた場合には、利用するサービスに関する約款、その他提供条件から、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、職員等に対し、当該外部サービスの利用について事前に申請するよう求め、適切な措置を講じた上で、利用させなければならない。

なお、業務上必要な情報収集の目的のために、インターネットのページの閲覧や検索等の外部サービスについては、申請を要しないものとする。

9.3 個別の外部サービスの利用

情報資産を所管する者は、以下の外部サービスを利用する場合には、必要な措置を講じなければならない。また、以下の外部サービス以外の外部サービスを利用する場合には、あらかじめ、ＣＩＳＯ補佐官に相談すること。

(1) ＳＭＳの利用

情報資産を所管する者は、東京都が管理するアカウントでＳＭＳを利用する場合、次の措置を講じなければならない。

① 利用するＳＭＳについて、サイバーセキュリティ対策に関する事項を含めた運用手順を策定し、利用するＳＭＳごとに責任者を定めること。

② 機密性Ａ又は機密性Ｂの情報はＳＭＳで発信しないこと。

(2) クラウドサービスの利用

情報資産を所管する者は、クラウドサービスを利用する場合、次の措置を講じなければならない。

① クラウドサービス上で取り扱われる情報に対して、国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて、委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定すること。

② 東京都又はクラウドサービス事業者の都合により、クラウドサービスの利用の中断又は終了等の措置を取らざるを得ない場合を想定し、他のクラウドサービスへの円滑な移行等の対策について、委託先を選定する際の受託者要件として明示すること。

③ バックアップ及び復元機能の有無、クラウドサービスを利用するネットワーク経路の暗号化等、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用すること。

④ クラウドサービスにて機密性Ａの情報を取り扱う場合は、ＣＩＳＯの許可を得ること。また、同様に機密性Ｂの情報を取り扱う場合は、あらかじめＣＩＳＯ補佐官に報告すること。

⑤ 契約期間満了後に全ての情報を復元が困難な状態にする旨を契約書に記載すること。

9.4　指定管理者への対応

公の施設の管理を指定管理者に委任する場合においては、所管する局等のサイバーセキュリティ局統括責任者は、管理業務においてサイバーセキュリティが確保されるよう、9.1(2)を参考として協定に必要事項を定めるなど、適切な対応をとらなければならない。

１０　評価・見直し

10.1　リスク評価の実施と年度計画の策定

サイバーセキュリティに係る内部及び外部環境の変化を踏まえ、サイバーセキュリティ上のリスクを評価し、リスク対応方針案を策定する。

また、リスク対応方針案に基づき、サイバーセキュリティ対策の年度計画を策定する。

① サイバーセキュリティ局統括責任者は、サイバーセキュリティ部責任者に対して、リスク評価の実施を指示する。

② 各部等におけるサイバーセキュリティ部責任者は、各部・所等において所管する情報システムについて、サイバーセキュリティに係るリスク評価を実施し、リスク対応方針案を策定する。

③ ＣＩＳＯ補佐官は、各局等において策定されたリスク対応方針案を取りまとめ、ＣＩＳＯに提出する。

④ ＣＩＳＯは各局等より提出されたリスク対応方針案の内容を検討し、リスク対応方針として承認する。

⑤ ＣＩＳＯにより承認されたリスク対応方針に基づき、各局にてサイバーセキュリティ対策の年度計画を策定する。

10.2　自己点検

(1)　実施方法

① サイバーセキュリティ部責任者は、所管する情報システムについて、定期的に、及び必要に応じて、自己点検を実施しなければならない。

② サイバーセキュリティ部責任者は、所管する組織における本対策基準に沿ったサイバーセキュリティ対策状況について、毎年度及び必要に応じて、自己点検を行わなければならない。

(2)　報告

サイバーセキュリティ局統括責任者は、自己点検結果及び自己点検結果に基づく改善策を取りまとめ、局サイバーセキュリティ委員会に報告しなければならない。

(3)　自己点検結果の活用

① サイバーセキュリティ部責任者は、自己点検の結果に基づき、改善を図らなければならない。

② サイバーセキュリティ局統括責任者は、自己点検結果を集約し、実施手順の見直し、その他サイバーセキュリティ対策の見直し等に活用しなければならない。

10.3 監査

(1) 実施方法

各局等におけるサイバーセキュリティ局統括責任者は、サイバーセキュリティ局監査責任者を指名し、当該局等における実施手順の遵守状況等について、定期的に、及び必要に応じて、監査を実施させなければならない。

なお、ＣＩＳＯは、必要に応じて、当該監査結果及び各局等におけるその後の対応について、説明を求めることができる。

(2) 監査を行う者の要件

① サイバーセキュリティ局監査責任者は、監査を実施する場合に、被監査部門から独立した者に指示をして、監査を実施しなければならない。

② 監査を行う者は、監査及びサイバーセキュリティに関する専門知識を有する者でなければならない。

(3) 監査実施計画の立案及び実施への協力

① サイバーセキュリティ局監査責任者は、監査等を行うに当たって、監査の実施計画を立案し、サイバーセキュリティ局統括責任者の承認を得なければならない。

② 被監査部門は、監査の実施に協力しなければならない。

(4) 外部委託事業者等に対する監査

サイバーセキュリティ局監査責任者は、各局等において業務の一部又は全部について外部委託事業者等に対して委託している情報システムについて、外部委託事業者等から再委託を受けている事業者も含め、外部委託事業者等側でのサイバーセキュリティポリシーの遵守状況に関する監査を、定期的に又は必要に応じて実施しなければならない。

(5) 監査結果の報告

サイバーセキュリティ局監査責任者は、監査の結果を取りまとめ、サイバーセキュリティ局統括責任者及び局サイバーセキュリティ委員会に報告するものとする。

(6) 保管

サイバーセキュリティ局監査責任者は、監査の実施を通して収集した監査の証拠、報告書の作成のための調書を、紛失・毀損等が発生しないように適切に保管しなければならない。

(7) 監査結果への対応

サイバーセキュリティ局統括責任者は、監査の結果を踏まえ、指摘事項について、当該指摘事項に該当する情報システムを所管するサイバーセキュリティ部管理者のほか、当該所管部署以外において、同種の課題及び問題点を持つ可能性がある情報システムを所管するサイバーセキュリティ部管理者に対しても、当該課題及び問題点について、必要に応じて、対処を指示しなければならない。

また、併せて、その指示内容を含め、ＣＩＳＯ補佐官にも報告しなければならない。

10.4　サイバーセキュリティポリシーの見直し

10.1から10.3までの実施結果に基づく対応又はサイバーセキュリティに関する状況の変化への対応が必要となった場合には、サイバーセキュリティポリシーを見直す。

１１　公営企業局等における特例措置

① 各公営企業局等における局長等は、サイバーセキュリティ対策について重要な事案を決定する場合は、必要に応じて、ＣＩＳＯに対して協議することとする。

② 2.1.1(2)⑥に規定する「助言、指導」を「助言」に読み替える。

③ 5.1(6)、7.1(3)(7)(10)①、8.3(1)(2)、9.3(2)④に規定する「ＣＩＳＯ」を「サイバーセキュリティ局統括責任者」と読み替える。

④ 7.1(10)⑤⑦、7.1(13)②、7.7、8.2(2)、8.3(3)、9.3、9.3(2)④及び12に規定する「ＣＩＳＯ補佐官」を「サイバーセキュリティ局責任者」と読み替える。

⑤ 前3項により読み替えた場合において、ＣＩＳＯは、サイバーセキュリティ局統括責任者に、ＣＩＳＯ補佐官は、サイバーセキュリティ局責任者に対して、情報提供を求めることができることとし、サイバーセキュリティ局統括責任者及びサイバーセキュリティ局責任者は、必要に応じて、情報提供を行うものとする。

１２　委任

本対策基準の運用に必要な事項は、ＣＩＳＯ補佐官が別に定める。

附　則

この基準は、平成31年4月1日から施行する。ただし、次の(1)及び(2)に掲げる規定については、当該(1)及び(2)に定める日までの間、適用しないことができる。

(1) 項番7.1(14)③及び項番7.7　　2020（平成32）年3月31日

(2) 項番4、項番5.4(1)、項番7.1(9)・(12)・(13)④・(15)①オ及び項番7.6(2)・(3)①　　2021（平成33）年3月31日

別表 1-1　機密性による情報資産の例示

分類	情報資産の例示
機密性A	・特定個人情報（マイナンバーを含む個人情報） ・個人情報※1（生活歴、心身の状況、所得、財産状況等の情報のほか、電話番号、メールアドレス、住所、氏名、生年月日又は性別といった基本情報を含む。） ・職員等に関する情報で、職員等の任用、退職、給与、分限、懲戒、健康管理等に関する情報 ・訴訟、審査請求等に関する情報 ・サイバーセキュリティ実施手順のファイル ・予算見積書及び関係ファイル ・積算基準、単価表、予定価格調書その他契約関係ファイル ・公的資格試験、採用・昇任選考の問題及び採点結果情報 ・プレス発表前その他公開前の行政情報 ・システム設計書、ネットワーク構成図、仕様書、ソースコード、テスト結果、情報システム等に関する資料
機密性B	・内部通達、通知、事務連絡等のファイル ・事案決定手続を経ていない企画・検討段階のファイル（資料文書） ・既存事業・経常的業務に関する事務手順、実績等情報 ・調査照会・回答文書に関するファイル ・公開前会議資料情報 ・その他一般公文書ファイル
機密性C	・プレス発表、ホームページ、東京都広報等で一般に公開済の情報 ・東京都の組織機構図・電話番号情報 ・条例、規則、規程及び訓令のファイル

※1　なお、個人情報を加工して特定の個人を識別することができないようにした情報及び当該個人情報を復元することができないようにした情報については、機密性Aとして扱う個人情報には含まない。

別表 1-2　完全性による情報資産の例示

分類	情報資産の例示
完全性A	・公的証明書を発行する情報システム ・行政処分など直接、住民の権利義務に影響を及ぼす業務に係る情報システム ・改ざん、誤びゅうがあった場合、修正回復が極めて困難な情報資産 ・上記情報システムで取り扱う電磁的記録
完全性B	・ホームページ等の情報システム ・内部事務処理等の一般業務に係る情報システム ・上記情報システムで取り扱う電磁的記録
完全性C	・情報資産の改ざん、誤びゅうがあっても、行政事務の遂行に軽微な支障が生じるにとどまる情報システム

別表 1-3　可用性による情報資産の例示

分類	情報資産の例示
可用性A	・公的証明書を発行する情報システム ・行政処分など直接、住民の権利義務に著しく影響を及ぼす業務に係る情報システム ・改ざん、誤びゅうがあった場合、修正回復が極めて困難な情報資産 ・上記情報システムで取り扱う電磁的記録
可用性B	・一般的な行政情報を提供する情報システム ・経常的な事務処理に関する業務に係る情報システム ・システム障害時、停止許容時間が 24 時間未満の情報システム ・システム停止により、行政事務遂行に支障が生じるが、経済的損失など後日回復可能な支障にとどまる情報システム ・上記情報システムで取り扱う電磁的記録
可用性C	・行政事務の遂行に影響があったとしても軽微な支障が生じるにとどまる情報システム