サイバーセキュリティ対策規程

（令和５年 10 月１日都市づくり公社規程第 122 号）

公益財団法人東京都都市づくり公社サイバーセキュリティ対策規程を次のように定める。
公益財団法人東京都都市づくり公社サイバーセキュリティ対策規程

第１章　目的及び適用対象

（目的）

第１条　本規程は、公益財団法人東京都都市づくり公社（以下「公社」という。）における各種システムやネットワーク等のハードウェア及びソフトウェア、電磁的情報及び記録媒体、これらに関する仕様等の文書（以下「情報資産」という。）について、サイバー攻撃をはじめとする様々な脅威に対応するためのサイバーセキュリティ対策や役職員の責務に関する基本的な方針を定め、公社事業の着実な推進に向けて情報資産の適切な運用及び管理を実現することを目的とする。

（適用対象）

第２条　本規程の適用対象とする者は、役職員その他公社の指揮命令に服している者であって、次項に規定する情報を取り扱う者（以下「職員等」という。）とする。

２　本規程の適用対象とする情報は、職員等が職務上取り扱う情報であって、情報処理若しくは通信の用に供するシステム（以下「情報システム」という。）又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）及び情報システムの設計又は運用管理に関する情報とする。

第二章　サイバーセキュリティ対策のための基本方針

（管理体制）

第３条　サイバーセキュリティ対策を推進するため、以下の体制を整備する。

(1)　最高情報セキュリティ責任者

最高情報セキュリティ責任者を置き、公社の情報資産の適切な運用や、必要な対策の策定及び実施に関するサイバーセキュリティ委員会等の報告や提案等について、経営的な知見や判断力によりサイバーセキュリティ対策を推進する。

(2)　サイバーセキュリティ委員会

サイバーセキュリティ対策の実施や状況把握を行い、必要に応じて対策の見直しや教育の実施、情報共有等を推進する。

また、以降の各条項で定める内容について実施者の明記が無い場合は原則とし

てサイバーセキュリティ委員会が実施または実施者を指定して必要な指示等を行う。

（資産管理）

第４条　情報システムに関する資産状況を把握するための台帳を整備し、資産管理を適切に行う。

なお、当該台帳については、公社のサイバーセキュリティ対策等に重大な支障を及ぼす可能性があることから、非公開とする。

（リスク評価と対策）

第５条　公社事業を推進する上で求められる要件やサイバーセキュリティに係る環境の変化を踏まえ、情報資産に係る脅威発生の可能性や顕在時の損失等を分析してリスクを評価し、必要なサイバーセキュリティ対策を講じる。

（サイバーセキュリティ文書）

第６条　前条に基づき策定するサイバーセキュリティ対策等の実施に必要な規則等を以下のとおり定める。

なお、当該規則等については、公社の事業運営やサイバーセキュリティ対策等に重大な支障を及ぼす可能性があることから、非公開とする。

(1)　サイバーセキュリティ対策に関する達

サイバーセキュリティ対策等を実施するため、具体的な遵守事項や判断基準等を定める。

(2)　関連する要綱または要領等

前号で定めた事項等の執行や運用等について、必要に応じて定める。

（対策推進計画）

第７条　サイバーセキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定める。

２　前項により定めた対策推進計画に基づき、適切にサイバーセキュリティ対策を実施する。

３　前項の実施状況や環境変化等を踏まえ、対策推進計画の見直しを行う。

（例外措置）

第８条　規則等の例外措置を適用するために必要な申請、審査、承認のための手順と担当者を定める。

（教育）
第９条　職員等が自覚をもって公社情報資産を適切に運用し、脅威への対策を実施するために必要なサイバーセキュリティに関する教育を行う。

（情報セキュリティインシデントへの対応）
第 10 条　サイバーセキュリティ対策の不具合又はこれを阻害する行為等（以下「情報セキュリティインシデント」という。）に対処するため、適正な体制を構築するとともに、必要な措置を定めて実施する。
２　職員等は、情報セキュリティインシデントの可能性を認知した場合は、速やかにサイバーセキュリティ対策委員会に報告しなければならない。
３　情報セキュリティインシデントに関して報告を受け又は認知したときは、必要な措置を講じる。

（自己点検）
第 11 条　定期的及び必要に応じて情報セキュリティ対策の自己点検を行う。

（監査）
第 12 条　本規程に基づき定められた規則等が本規程に準拠し、かつ実際の運用が本規程等に準拠していることを確認するため、情報セキュリティ監査を実施する。

（サイバーセキュリティ文書及び対策の見直し）
第 13 条　リスク評価、自己点検、監査の結果や、サイバーセキュリティに関する状況の変化等に対応するため、対策の見直しや新たな対策を講じる必要がある場合は、サイバーセキュリティ文書及び対策の見直し等を行う。

第三章　情報セキュリティ対策のための基本対策
（情報の格付）
第 14 条　取り扱う情報に、気密性、完全性及び可用性の観点に区別して、分類した格付を付すための方法及び範囲を定める。

（情報の取扱制限）
第 15 条　職員等は、情報の格付に応じて定められた取扱制限に従い、適切な措置を行う。

（情報のライフサイクル管理）
第 16 条　情報の作成、入手、利用、保存、提供、運搬、送信及び消去の各段階で、情報の格付及び取扱制限に従って必要とされる取扱いが損なわれることがないように、必要な

措置を定める。

（情報を取り扱う区域）

第17条　サイバーセキュリティ対策が必要な区域の範囲を定め、その特性に応じて対策を定める。

（外部委託）

第18条　職員等は、情報処理に係る業務を外部委託する場合には、必要な措置を定め、実施しなければならない。

２　外部委託を実施する際に要機密情報を取り扱う場合は、委託先において情報漏えい対策や、委託内容に意図しない変更が加えられない管理を行うこと等の必要なサイバーセキュリティ対策が実施されることを選定条件とし、仕様内容に含める。

３　機器等の調達に当たっては、既知の脆弱性への対策実施や、不正プログラムの埋め込みを防ぐ等の調達過程でのセキュリティリスクに対する適切な対処を含む選定基準を整備する。

（情報システムのライフサイクル全般にわたるサイバーセキュリティの確保）

第19条　情報システムの企画、調達・構築、運用・保守、更改・廃棄及び見直しの各段階において、サイバーセキュリティを確保するための措置を定める。

（情報システムの運用継続計画）

第20条　情報システムに係る運用継続のための計画（以下「情報システム運用継続計画」という。）を整備する際には、事業継続計画等と整合性を確保し、整備及び運用を行う。

（情報システムの利用）

第21条　職員等は、情報システムの利用に際して、サイバーセキュリティの重要性を認識し、本規程等を遵守してサイバーセキュリティを確保するために必要な措置を行わなければならない。

（サイバーセキュリティ対策に関する達への委任）

第22条　本規程に定めるもののほか、本規程の実施のため必要な要件は、サイバーセキュリティ対策に関する達で定める。

附則

この規程は、令和５年10月１日から施行する。