説明資料３

企画課	カジノ管理委員会におけるサイバーセキュリティ対策に関する訓令の一部改正（案）について	令和７年５月３０日

１．趣旨

カジノ管理委員会においては、サイバーセキュリティに関する対策の基本方針として「カジノ管理委員会におけるサイバーセキュリティ対策に関する訓令」を制定し、当該訓令に基づき、最高情報セキュリティ責任者の統括の下、「カジノ管理委員会サイバーセキュリティ対策基準」（以下「対策基準」という。）及び対策基準に基づく実施手順を定め、情報セキュリティ対策の強化・充実を図っているところ。

今般、「政府機関等のサイバーセキュリティ対策のための統一基準群（令和５年７月７日サイバーセキュリティ本部決定）」等を踏まえ、当委員会の訓令について別添のとおり所要の改正を行い、引き続き情報セキュリティ対策の強化・充実に取り組むものである。

２．主な改正内容

・クラウドサービス利用の対応に係る規定の明確化（新規追加）
・情報セキュリティ対策の見直しに係る規定の明確化（条項の再整理）

等

３．今後のスケジュール

・改正訓令の施行（令和７年７月１日）
※　上記施行と合わせ、当該訓令に基づく対策基準等の改正等を予定

別　添

カジノ管理委員会におけるサイバーセキュリティ対策に関する訓令
（令和３年 11 月 18 日カジノ管理委員会訓令第 37 号）

※本件改正は、記載順の変更等をしているため、改正前の訓令に係る条項の記載順は一致していない。一部条項については、改正後との比較で、改正前の欄において便宜上異なる章に記載しており、括弧書き・斜体でその旨付記している。

改　正　後	改　正　前
カジノ管理委員会におけるサイバー セキュリティ対策に関する訓令 令 和 ３ 年 11 月 18 日 カジノ管理委員会訓令第 37 号 最終改正令和７年５月 30 日	カジノ管理委員会におけるサイバー セキュリティ対策に関する訓令 令 和 ３ 年 11 月 18 日 カジノ管理委員会訓令第 37 号
目次 第１章　目的及び適用対象（第１条－第２条） 第２章　情報セキュリティ対策のための基本方針（第３条－第 13 条） 第３章　情報セキュリティ対策のための基本対策（第 14 条－第 22 条）	目次 第１章　総則（第１条－第２条） 第２章　情報セキュリティ対策のための基本方針（第３条－第４条） 第３章　情報セキュリティ対策のための基本対策（第５条－第 23 条）
第１章　目的及び適用対象 （目的） 第１条　本訓令は、カジノ管理委員会（以下「委員会」という。）におけるサイバーセキュリティに関する対策の基本方針として、委員会がとるべき対策の枠組みを定め、委員会が自らの責任において対策を図り、委員会	第１章　総則 （目的） 第１条　この訓令は、カジノ管理委員会（以下「委員会」という。）におけるサイバーセキュリティに関する対策の基本方針として、委員会がとるべき対策の枠組みを定め、委員会が自らの責任において対策を図り、委員会全

別　添

カジノ管理委員会におけるサイバーセキュリティ対策に関する訓令
（令和３年 11 月 18 日カジノ管理委員会訓令第 37 号）

改　正　後	改　正　前
全体のサイバーセキュリティ対策を含む情報セキュリティ対策の強化・拡充を図ることを目的とする。	体のサイバーセキュリティ対策を含む情報セキュリティ対策の強化・拡充を図ることを目的とする。
（適用対象） 第２条　本訓令の適用対象とする者は、次項に規定する情報を取り扱う委員長、委員及び事務局の職員（以下「職員」という。）とする。 ２　本訓令の適用対象とする情報は、職員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情報システムに入力された書面に記載された情報を含む。）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。	（適用対象） 第２条　この訓令の適用対象とする者は、次項に規定する情報を取り扱う委員長、委員及び事務局の職員（以下単に「職員」という。）とする。 ２　この訓令の適用対象とする情報は、職員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２章　情報セキュリティ対策のための基本方針	第２章　情報セキュリティ対策のための基本方針 *（下記第５条及び第１７条は第３章から移動）*
（管理体制） 第３条　委員会に、最高情報セキュリティ責任者１人を置き、事務局次長をもって充てる。 ２　最高情報セキュリティ責任者は、第６条第１項に定める情報セキュリティポリシーの審議を行う機能を持つ組織として情報セキュリティ委員会を設置するものとする。 ３　最高情報セキュリティ責任者は、別に定めるカジノ管理委員会サイバ	（管理体制） 第５条　委員会に、最高情報セキュリティ責任者１人を置き、事務局次長をもって充てる。 ２　最高情報セキュリティ責任者は、ポリシーの審議を行う機能を持つ組織として情報セキュリティ委員会を設置する。

別　添

カジノ管理委員会におけるサイバーセキュリティ対策に関する訓令
（令和３年 11 月 18 日カジノ管理委員会訓令第 37 号）

改　正　後	改　正　前
ーセキュリティ対策基準（以下「対策基準」という。）において、情報セキュリティ委員会の構成員を定めるものとする。	
４　最高情報セキュリティ責任者は、本訓令に定める委員会における情報セキュリティ対策に関する事務を統括するとともに、その責任を負う。	３　最高情報セキュリティ責任者は、この訓令にて規定した委員会における情報セキュリティ対策に関する事務を統括するとともに、その責任を負う。
５　最高情報セキュリティ責任者は、本訓令に定められた自らの担務を、対策基準に定める責任者に担わせることができる。	４　最高情報セキュリティ責任者は、この訓令に定められた自らの担務を、対策基準に定める責任者に担わせることができる。
（資産管理） 第４条　最高情報セキュリティ責任者は、委員会の資産の状況を把握するため、委員会が所管する情報システムに係る文書及び台帳を整備するものとする。	（情報システムに係る文書及び台帳整備） 第１７条　最高情報セキュリティ責任者は、所管する情報システムに係る文書及び台帳を整備しなければならない。
（リスク評価と対策） 第５条　最高情報セキュリティ責任者は、第１１条に定める自己点検の結果、第１２条に定める情報セキュリティ監査の結果、サイバーセキュリティ基本法（平成２６年法律第１０４号。以下「法」という。）に基づきサイバーセキュリティ戦略本部が実施する監査の結果等を勘案した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、必要となる情報セキュリティ対策を講じるものとする。	（リスク評価と対策） 第３条　委員会は、第１０条に定める自己点検の結果、第１１条に定める監査の結果、サイバーセキュリティ基本法（平成２６年法律第１０４号。以下「法」という。）に基づきサイバーセキュリティ戦略本部が実施する監査の結果等を勘案した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、リスクを評価し、必要となる情報セキュリティ対策を講じるものとする。 ２　前項の評価に変化が生じた場合には、情報セキュリティ対策を見直すものとする。

別　添

カジノ管理委員会におけるサイバーセキュリティ対策に関する訓令
（令和３年 11 月 18 日カジノ管理委員会訓令第 37 号）

改　正　後	改　正　前
（情報セキュリティ文書） 第６条　最高情報セキュリティ責任者は、対策基準並びに対策基準に基づく実施手順及び運用規程を定めるものとする。本訓令、対策基準、実施手順及び運用規程を総称して情報セキュリティポリシー（以下「ポリシー」という。）という。 ２　対策基準は、「政府機関等のサイバーセキュリティ対策のための統一基準」（令和５年度版）（令和５年７月４日サイバーセキュリティ戦略本部決定。以下「統一基準」という。）に準拠し、統一基準と同等以上の情報セキュリティ対策が可能となるように定めるものとする。	（情報セキュリティ文書） 第４条　委員会は、対策基準（別に定める「カジノ管理委員会サイバーセキュリティ対策基準」をいう。以下同じ。）及び対策基準に基づく実施手順を定めるものとする。この訓令、対策基準及び実施手順を総称してサイバーセキュリティポリシー（以下「ポリシー」という。）という。 ２　対策基準は、政府機関等のサイバーセキュリティ対策のための統一基準（令和３年度版）（令和３年７月７日サイバーセキュリティ本部決定。以下「統一基準」という。）と同等以上の情報セキュリティ対策が可能となるように定めるものとする。 ３　前条第一項の評価の結果を踏まえ、ポリシーの評価及び見直しを行うものとする。
（対策推進計画） 第７条　最高情報セキュリティ責任者は、第５条の評価の結果を踏まえた情報セキュリティ対策を組織的・継続的に実施し、総合的に推進するための計画（以下「対策推進計画」という。）を定めるものとする。 ２　職員は、対策推進計画に基づき情報セキュリティ対策を実施しなければならない。	*（下記第６条から第 11 条までは第３章から移動）* （対策推進計画） 第６条　最高情報セキュリティ責任者は、第３条第１項の評価の結果を踏まえた情報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。）を定めなければならない。 ２　職員は、対策推進計画に基づき情報セキュリティ対策を実施しなければならない。 ３　最高情報セキュリティ責任者は、前項の実施状況を評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、対策推進計画の見直しを行わなければならない。

別　添

カジノ管理委員会におけるサイバーセキュリティ対策に関する訓令
（令和３年 11 月 18 日カジノ管理委員会訓令第 37 号）

改　正　後	改　正　前
（例外措置） 第８条　最高情報セキュリティ責任者は、ポリシーに定めた情報セキュリティ対策の実施に当たり、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ものとする。	（例外措置） 第７条　最高情報セキュリティ責任者は、ポリシーに定めた情報セキュリティ対策の実施に当たり、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なければならない。
（教育） 第９条　最高情報セキュリティ責任者は、職員が自覚をもってポリシーに定められた情報セキュリティ対策を実施するよう、情報セキュリティに関する教育を行うものとする。	（教育） 第８条　最高情報セキュリティ責任者は、職員が自覚をもってポリシーに定められた情報セキュリティ対策を実施するよう、情報セキュリティに関する教育を行わなければならない。
（情報セキュリティインシデントへの対応） 第１０条　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、実施するものとする。 ２　情報セキュリティインシデントの可能性を認知した者は、実施手順に定める報告窓口に報告しなければならない。 ３　対策基準に定める責任者は、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、必要な措置を講じなければならない。	（情報セキュリティインシデントへの対応） 第９条　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、必要な措置を講じなければならない。 ２　情報セキュリティインシデントの可能性を認知した者は、実施手順に定める報告窓口に報告しなければならない。 ３　対策基準に定める責任者は、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、必要な措置を講じなければならない。
（自己点検） 第１１条　最高情報セキュリティ責任者は、情報セキュリティ対策の自己点検を行うものとする。	（自己点検） 第１０条　最高情報セキュリティ責任者は、情報セキュリティ対策の自己点検を行わなければならない。

別　添

カジノ管理委員会におけるサイバーセキュリティ対策に関する訓令
（令和３年 11 月 18 日カジノ管理委員会訓令第 37 号）

改　正　後	改　正　前
（情報セキュリティ監査） 第１２条　最高情報セキュリティ責任者は、対策基準が統一基準に準拠し、かつ実際の運用が対策基準に従って行われていることを確認するため、情報セキュリティ監査を行うものとする。	（監査） 第１１条　最高情報セキュリティ責任者は、対策基準が統一規範及び統一基準に準拠し、かつ実際の運用が対策基準に従って行われていることを確認するため、情報セキュリティ監査を行わなければならない。
（対策の見直し） 第１３条　最高情報セキュリティ責任者は、第５条の評価に変化が生じた場合には、情報セキュリティ対策の見直しを行うものとする。 ２　最高情報セキュリティ責任者は、第５条の評価結果を踏まえ、ポリシーの評価及び見直しを行うものとする。 ３　最高情報セキュリティ責任者は、情報セキュリティ対策の運用及び自己点検・情報セキュリティ監査並びに法に基づきサイバーセキュリティ戦略本部が実施する監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、対策推進計画の見直しを行うものとする。	
第３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　最高情報セキュリティ責任者は、対策基準において情報の格付の区分を定めるものとする。 ２　職員は、取り扱う情報に、機密性、完全性及び可用性の観点に区別して、分類した格付を付さなければならない。	第３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１２条　職員は、取り扱う情報に、機密性、完全性及び可用性の観点に区別して、分類した格付を付さなければならない。

別　添

カジノ管理委員会におけるサイバーセキュリティ対策に関する訓令
（令和３年 11 月 18 日カジノ管理委員会訓令第 37 号）

改　正　後	改　正　前
３　職員は、法第２６条第１項第２号に定める国の行政機関、独立行政法人及び指定法人（以下「機関等」という。）への情報の提供、運搬及び送信に際しては、前項で定めた情報の格付のうち、いかなる区分に相当するかを明示等しなければならない。	２　職員は、他の機関等（法第２６条第１項第２号に定める国の行政機関、独立行政法人及び指定法人をいう。以下同じ。）への情報の提供、運搬及び送信に際しては、前項で定めた情報の格付のうち、いかなる区分に相当するかを明示等しなければならない。
（情報の取扱制限） 第１５条　最高情報セキュリティ責任者は、情報の格付に応じた取扱制限を定めるものとする。 ２　職員は、取り扱う情報に、前項で定めた取扱制限を付さなければならない。 ３　職員は、機関等間での情報の提供、運搬及び送信に際しては、情報の取扱制限を明示等しなければならない。	（情報の取扱制限） 第１３条　最高情報セキュリティ責任者は、情報の格付に応じた取扱制限を定めなければならない。 ２　職員は、取り扱う情報に、前項で定めた取扱制限を付さなければならない。 ３　職員は、機関等間での情報の提供、運搬及び送信に際しては、情報の取扱制限を明示等しなければならない。
（情報のライフサイクル管理） 第１６条　最高情報セキュリティ責任者は、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ものとする。 ２　職員は、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、必要な措置を実施しなければならない。	（情報のライフサイクル管理） 第１４条　最高情報セキュリティ責任者は、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、必要な措置を定めなければならない。 ２　職員は、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しなければならない。

別　添

カジノ管理委員会におけるサイバーセキュリティ対策に関する訓令
（令和３年 11 月 18 日カジノ管理委員会訓令第 37 号）

改　正　後	改　正　前
（情報を取り扱う区域） 第１７条　最高情報セキュリティ責任者は、委員会が管理する又は委員会以外の組織から借用している施設等、委員会の管理下にあり、施設及び環境に係る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決定し、実施するものとする。	（情報を取り扱う区域） 第１５条　最高情報セキュリティ責任者は、委員会が管理する又は委員会以外の組織から借用している施設等、委員会の管理下にあり、施設及び環境に係る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決定しなければならない。
（外部委託） 第１８条　最高情報セキュリティ責任者は、委員会の情報を取り扱わせる業務を委託する場合には、必要な措置を定めるものとする。 ２　職員は、業務委託を実施する際に要機密情報を取り扱わせる場合は、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情報セキュリティ対策が実施されることを選定条件とし、仕様内容にも含めなければならない。 ３　最高情報セキュリティ責任者は、委員会の情報を取り扱うクラウドサービスを利用する場合には、情報セキュリティを確保するための措置を定めるものとする。 ４　職員は、委員会の情報を取り扱うクラウドサービスを利用する場合には、情報セキュリティを確保するための措置を実施しなければならない。 ５　最高情報セキュリティ責任者は、機器等の調達に当たり、機器等の開発等で不正な変更が加えられない管理がなされている等のサプライチェーン・リスクへの適切な対処を含む選定基準を定めるものとする。	（外部委託） 第１６条　最高情報セキュリティ責任者は、情報処理に係る業務を外部委託する場合には、必要な措置を講じなければならない。 ２　職員は、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情報セキュリティ対策が実施されることを選定条件とし、仕様内容にも含めなければならない。 ３　最高情報セキュリティ責任者は、機器等の調達に当たり、既知の脆弱性に対応していないこと、危殆化した技術を利用していること、不正プログラムを埋め込まれること等のサプライチェーン・リスクへの適切な対処を含む選定基準を整備しなければならない。

別　添

カジノ管理委員会におけるサイバーセキュリティ対策に関する訓令
（令和３年 11 月 18 日カジノ管理委員会訓令第 37 号）

改　正　後	改　正　前
（情報システムのライフサイクル全般にわたる情報セキュリティの確保） 第１９条　最高情報セキュリティ責任者は、委員会が所管する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、情報セキュリティを確保するための措置を定めるものとする。 ２　職員は、委員会が所管する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、情報セキュリティを確保するための措置を実施しなければならない。	（情報システムのライフサイクル全般にわたる情報セキュリティの確保） 第１８条　最高情報セキュリティ責任者は、所管する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、情報セキュリティを確保するための措置を定めなければならない。 ２　職員は、所管する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、情報セキュリティを確保するための措置を実施しなければならない。
（情報システムの運用継続計画） 第２０条　最高情報セキュリティ責任者は、委員会が所管する情報システムに係る運用継続のための計画を整備する際には、業務継続計画、ポリシーとの整合性を確保し、整備及び運用するものとする。	（情報システムの運用継続計画） 第１９条　最高情報セキュリティ責任者は、所管する情報システムに係る運用継続のための計画（以下「情報システムの運用継続計画」という。）を整備する際には、非常時における情報セキュリティ対策についても、勘案しなければならない。 ２　最高情報セキュリティ責任者は、情報システムの運用継続計画の訓練等に当たっては、非常時における情報セキュリティに係る対策事項の運用が可能かどうか、確認しなければならない。
	（暗号・電子署名） 第２０条　最高情報セキュリティ責任者は、委員会における暗号及び電子署名の利用について、必要な措置を講じなければならない。

別　添

カジノ管理委員会におけるサイバーセキュリティ対策に関する訓令
（令和３年 11 月 18 日カジノ管理委員会訓令第 37 号）

改　正　後	改　正　前
	（インターネット等を用いた行政サービスの提供） 第２１条　最高情報セキュリティ責任者は、インターネット等を用いて行政サービスを提供する際には、利用者端末の情報セキュリティ水準の低下を招く行為を防止するために、必要な措置を講じなければならない。
（情報システムの利用） 第２１条　最高情報セキュリティ責任者は、職員の情報システムの利用に際して、情報セキュリティを確保するための必要な措置を定めるものとする。 ２　職員は、情報システムの利用に際して、情報セキュリティを確保するために必要な措置を実施しなければならない。	（情報システムの利用） 第２２条　最高情報セキュリティ責任者は、職員の情報システムの利用に際して、情報セキュリティを確保するために必要な措置を定めなければならない。 ２　職員は、情報システムの利用に際して、情報セキュリティを確保するために必要な措置を実施しなければならない。
（対策基準への委任） 第２２条　本訓令に定めるもののほか、本訓令の実施のため必要な要件は、最高情報セキュリティ責任者が対策基準で定めるものとする。	（対策基準への委任） 第２３条　この訓令に定めるもののほか、この訓令の実施のため必要な要件は、最高情報セキュリティ責任者が対策基準で定める。
附　則 本訓令は、令和７年７月１日から施行する。	附　則 この訓令は、令和４年２月１日から施行する。