説明資料１

企画課	カジノ事業免許審査に向けたサイバーセキュリティ対策検討の進捗状況について	令和３年１１月１８日

１．背景

国内外において政府機関等に対するサイバー攻撃が続発している状況を踏まえ、今後カジノ事業の免許付与、事業者監督の段階に移行するにあたり、サイバー攻撃及び職員の故意・過失等による情報流出の対策を検討している。

２．セキュリティリスクのポイント

情報システムに対するサイバー攻撃は、クラウドサービスなどインターネット接続点からの攻撃や無線ＬＡＮへの不正接続が考えられるが、これら情報システムは、セキュリティ機能を最新の状態にすることでリスクを軽減している。

一方、人の介入によるリスクは、電子メールによる送信、USB メモリ等による情報及び書類の持ち出し、スマートフォン又はデジタルカメラによる画面、書類等の撮影など、多岐にわたりリスクが存在している。

３．免許審査等の業務において留意すべき点

カジノ事業免許審査等の業務を行う上で、カジノ事業関係者の個人情報、背面調査における質問票、機器の型式検定に係る資料等、機密性の高い情報を取り扱うため、情報管理のルールが必要であり、体制、教育、区域管理、監査等の情報管理に関するルールが必要となる。

４．セキュリティリスク軽減のための国際規格等

当委員会は国外の機密性の高い情報（個人情報含む）を取り扱うため、今後、統一基準群に加え、国際規格（ISO/IEC27001 等）、米国基準（NIST SP800-53 等）を満たす情報セキュリティ管理体制の構築が必要となる可能性がある。

５．カジノ管理委員会サイバーセキュリティポリシーの整備

日本政府の統一的な枠組みである統一基準群に準拠した情報セキュリティポリシーをカジノ管理委員会においても策定しているが、本年７月の統一基準群の改訂に合わせて見直しを行い、基本方針となる「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」を制定することとしたい。

６．今後のスケジュール

- 訓令の制定（本日）
- 対策基準及び実施手順の改訂（１月中旬）
- 施行（令和４年２月１日）

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●月●日
カジノ管理委員会訓令第●号

目次

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　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

（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。

（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。

第３章　情報セキュリティ対策のための基本対策

（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。

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。

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。

（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。

（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。

（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。

（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。

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。

（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。

（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。

（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。

（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

この訓令は、令和４年２月１日から施行する。