D3101 例外措置手順書

国立情報学研究所 学術研究プラットフォーム運営・連携本部  
高等教育機関における情報セキュリティポリシー推進委員会

**改定履歴**

|  |  |  |
| --- | --- | --- |
| 日付・文書番号 | 改定内容 | 担当 |
| 2007年10月31日  A3102 | 新規作成 | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2015年10月9日  C3102 | 文書番号の変更のみ | － |
| 2021年3月25日  D3101 | 記述の追加（来訪者への無線LAN環境の提供の扱い） | 高等教育機関における情報セキュリティポリシー推進部会事務局 |
| 2024年5月8日  D3101 | 誤記修正 | 高等教育機関における情報セキュリティポリシー推進部会事務局 |

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。

sp-comment[at]nii.ac.jp　（[at]を＠に置き換えてください）

担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

**1. 目的**

本学における大学業務を遂行するに当たって、ポリシー・実施規程・手順の適用が大学業務の適正な遂行を著しく妨げる等の理由により、ポリシー・実施規程・手順とは異なる代替の方法を採用すること又は規定を実施しないことを認めざるを得ない場合がある。

こうした場合においても、あらかじめ定められた例外措置のための手続により、情報セキュリティを維持しつつ柔軟に対応できなければ、ポリシー・実施規程・手順の実効性を確保することは困難となる。

本書は、教職員等が例外措置の適用を希望する場合の手続を定め、もって例外措置において必要な情報セキュリティ水準を確保することを目的とする。

**2. 本手順書の対象者**

本書は、すべての教職員等を対象としている。

**3. 定義**

本書における用語の定義は次のとおりである。

(1) 「例外措置」とは、教職員等がその実施に責任を持つポリシー・実施規程・手順を遵守することが困難な状況で、大学業務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。

(2) 「申請者」とは、例外措置の適用を申請する者をいう。

(3) 「許可権限者」とは、例外措置の適用を審査する者をいう。

(4) 「代替措置」とは、例外措置の適用に伴い発生するリスクを低減するためにポリシー・実施規程・手順が定める内容とは異なる代替のセキュリティ対策をいう。

**4. 例外措置の許可権限**

4.1 許可権限者

(1) ポリシー・実施規程・手順の遵守事項に対する例外措置の許可権限者を下記に定める。

|  |  |  |  |
| --- | --- | --- | --- |
| 申請者  （遵守義務を負うもの） | | 許可権限者 | |
| 通常の場合 | その他 |
| 全学総括責任者 | | 全学情報セキュリティ委員会 | ポリシー・実施規程・手順の遵守事項に被報告者、被届出者、被返還者、被許可者、承認者、判断者がある場合は当該者 |
| 全学情報セキュリティ委員会 | | 全学総括責任者 |
| 全学実施責任者 | | 全学総括責任者 |
| 情報セキュリティ監査責任者 | | 全学総括責任者 |
| 情報セキュリティ監査を実施する者 | | 情報セキュリティ監査責任者 |
| 部局総括責任者 | | 全学実施責任者 |
| 部局技術責任者 | | 部局総括責任者 |
| 部局技術担当者 | | 部局技術責任者 |
| 職場情報セキュリティ責任者(上司) | | 部局総括責任者 |
| 教職員等 | [情報セキュリティ要件の明確化に基づく対策と情報システムの構成要素についての対策]に係る事項 | 部局技術責任者 |
| 上記以外の事項 | 職場情報セキュリティ責任者(上司) |

（注）上記にかかわらず、必要がある場合は、当該許可権限者の上位を許可権限者とする。

**5. 例外措置の申請**

5.1 前提条件

(1) 申請者は、以下の場合に、例外措置の申請を行わなければならない。

・部局固有の手順を作成するに当たって、ポリシー及び実施規程の遵守事項への準拠性を満足できない場合

・情報、情報システムを取扱う業務を遂行するに当たって、ポリシー・実施規程・手順の遵守事項への準拠性を満足できない場合

(2) 申請者は、例外措置を申請する理由と例外措置の実施により想定される被害の大きさと影響を検討・分析した上で、例外措置の申請を行わなければならない。

5.2 事前申請の原則

例外措置の申請は、原則として事前に行わなければならない。

5.3 事前協議の原則

他の組織と関連のある事項は、事前に協議し、調整を行った上で例外措置の申請を行わなければならない。

5.4 例外措置の申請

申請者は、付録に示す例外措置申請書に以下の事項を記入し押印した上、許可権限者に提出する。

(1) 申請日

(2) 申請者の氏名、所属、連絡先

(3) 例外措置の適用を申請するポリシー・実施規程・手順の適用箇所（規程名と条項等）

(4) 例外措置の適用を申請する期間

(5) 例外措置の適用を申請する措置内容（講ずる代替手段等）

(6) 例外措置の適用を終了したときの報告方法

(7) 例外措置の適用を申請する理由

5.5 関係書類の添付

申請者は、申請内容を明確化するために参考資料が必要となる場合、これを添付する。またやむを得ない事情で、事後申請となった場合は、経緯書を添付する。

**6. 例外措置の審査**

6.1 例外措置の申請の受理

(1) 例外措置の申請を受理した許可権限者は、リスクを分析し、それに対する意見を記述する。

(2) 許可権限者は、必要がある場合は、例外措置申請書を上位の許可権限者に回付する。

6.2 審査の手続

(1) 当該例外措置申請に対する許可権限者は、速やかに審査手続を実施し、例外措置申請書に以下の事項を記載する。

• 申請を審査した者の情報（氏名、役割名、所属、連絡先）

• 審査決定日

• 審査結果の内容

○ 許可又は不許可の別（許可の場合、許可番号）

○ 許可又は不許可の理由

○ 例外措置の適用を許可したポリシー・実施規程・手順の適用箇所（規程名と条項等）

○ 例外措置の適用を許可した期間

○ 許可した措置内容（講ずるべき代替手段等）

○ 終了報告の方法

(2) 許可権限者は、例外措置申請書に対して疑義又は意見のある際は、その旨の意見書を添付する。

6.3 審査基準

許可権限者は、以下の条件をいずれも満たした場合に限り、例外措置の適用を許可すること。

(1) ポリシー・実施規程・手順の遵守事項を実施しないことについて、合理的理由があると認められるとき。

(2) ポリシー・実施規程・手順の遵守事項とは異なる代替の方法を採用する場合に、当該方法を採用した場合に想定される被害の大きさ・影響と採用しなかった場合の大学業務遂行への影響を比較、検討、分析した上で、その内容及び期間につき合理的理由があると認められるとき。

6.4 審査結果の通知

許可権限者は、例外措置申請書の副本を作成し、申請者に副本を返却して、審査結果を通知する。

6.5 例外措置の効力

例外措置は、例外措置の適用許可期間の開始日より効力を生ずる。ただし、承認された事項が次の各号のいずれかに該当した場合はその効力を失う。

(1) 適用を許可された期間を終了した場合

(2) 許可後、半年以内に実施できない場合

(3) 実施後、一時中断して、その中断期間が半年以上に及ぶ場合

**7. 例外措置の適用**

7.1 例外措置の関係者への周知

(1) 許可権限者は、適用した例外措置を、教職員等が参照可能な状態としておく。

7.2 例外措置の適用期間中のリスク管理

(1) 申請者は、例外措置によって行われる代替措置が暫定的な措置であることを認識し、その適用期間中におけるリスク管理に留意する。

**8. 例外措置の修正**

8.1 例外措置の修正

(1) 申請者は、許可された例外措置が以下に該当する場合は、速やかに許可権限者に例外措置申請書の修正申請を提出して承認を得る。

・許可された措置内容に大きな変更を加える場合

・例外措置の適用期間を延長する場合

(2) 申請者は、想定される被害の大きさと影響に変更がある場合は、必要に応じて別途の代替措置を適用し、速やかに許可権限者に例外措置申請書の修正申請を提出して承認を得る。

**9. 例外措置の終了**

9.1 終了の報告

申請者は、例外措置の適用終了時、速やかに許可権限者に付録に示す例外措置終了報告書を提出して確認を得る。ただし、許可権限者が報告を要しないとした場合は、この限りではない。

9.2 終了報告の確認

許可権限者は、例外措置の適用期間が終了した月の月末に例外措置終了報告書の提出の有無を確認する。ただし、報告を要しないとした場合は、この限りではない。

**10. 例外措置の管理**

10.1 例外措置の適用審査記録の管理

審査された例外措置申請書の正本は許可権限者が管理し、申請者に返却された副本は申請者が管理する。

10.2 例外措置の適用審査記録の提出

許可権限者は、毎月１回例外措置申請書の副本をもう一部作成し、全学総括責任者に提出する。

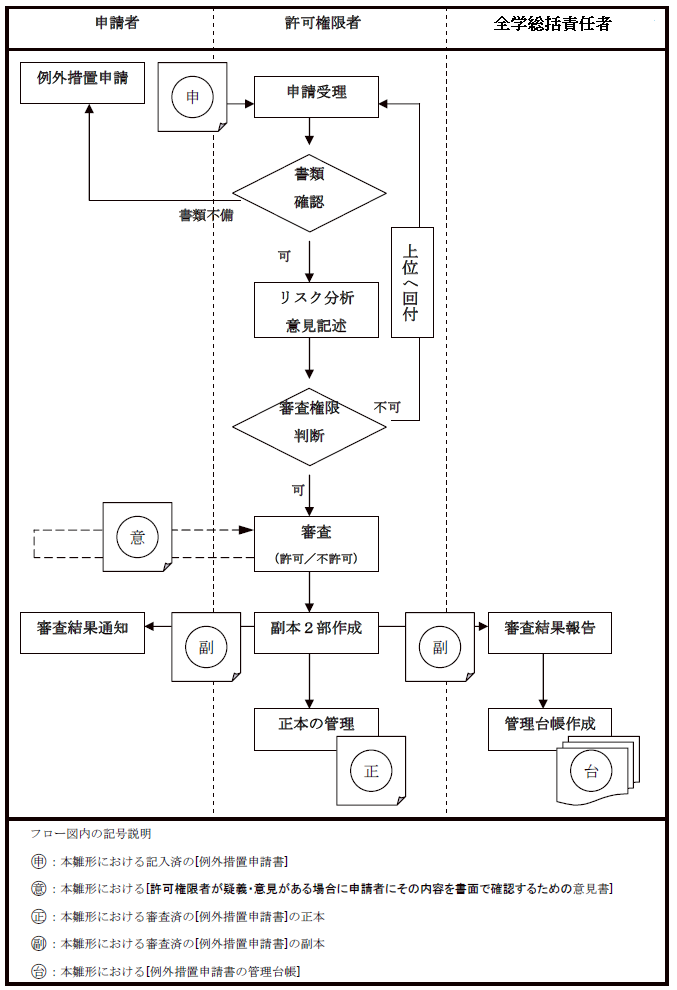
10.3 全学総括責任者による例外措置の適用審査記録の保管

全学総括責任者は、許可権限者から提出された例外措置申請書の副本を例外措置申請書の管理台帳として保管し、情報セキュリティ監査を実施する者からの申請に応じて閲覧を許可する。

**11. 事務手続の代行**

(1) 許可権限者は、書類の受付、書類の形式要件確認、書類の回付及び管理に関わる事務手続を、あらかじめ指定した総務担当者に行わせることができる。

付図 例外措置業務フロー



参考　例外措置の申請事例　＜来訪者への無線LAN環境の提供の扱い＞

解説：赤字部分は各大学の規程に合わせて修正が必要な箇所である。

　大学において，研究会合等へ学外から参加する訪問者に対して無線LAN環境によるネットワークアクセスを提供することがある。無線LAN環境の構築について，このサンプル規程集の体系では，D2101 情報セキュリティ対策基準第百七十九条で検討すべき措置の事項を，D2201 情報サービス利用規程第三条で利用者の範囲を定めているので，訪問者が許可を受けて所定の措置がなされた無線LAN環境を利用することは可能である。また，十分に管理された会議室のケースや，訪問者も個人認証により特定できるケースでは，訪問者ごとの許可を不要とする例外措置が考えられる。

（１）臨時の申請を代行するケース

　実際の運用において，短時間の研究会合などでは訪問者が申請して許可を受ける手続きは現実的ではないので，あらかじめ主催者が来訪者に代わって許可と臨時の全学アカウント（またはそれに準じるアカウント）を得る手続きを済ませておくなどする措置が考えられる。この場合に，弾力的運用とみなして例外措置として扱わないことも考えられる。

例外措置申請の記入例：

申請者：　研究会合等の主催者である教職員

適用開始日・終了日：　研究会合等の開催期間

申請対象規程：　D2201 情報サービス利用規程　第三条

申請対象システム名：　会議室無線LAN環境

申請理由：　研究会合の参加者が会議室無線LAN環境を利用することについて、訪問者が個別に許可を受けると著しく非効率なので、主催者があらかじめ人数分の臨時アカウントを申請して、会場において訪問者へ割り当てる。

代替措置の内容：　訪問者の身元を確認して臨時アカウントを割り当てて、その割当の対応を記録する。

（２）十分に管理された会議室で共用させるケース

　少人数の会議室で鍵の貸し出しと施錠及び入室が十分に管理されているケースなどでは，無線LANの接続鍵を会議室内に掲出するなどしてネットワークアクセスを提供する運用について，十分にセキュリティ維持できるよう措置したうえで，訪問者ごとの許可と利用者認証を行わない例外措置があり得る。この場合にも，会議室の無線LAN環境を設置・運用する者が訪問者が接続鍵を共用することについて年度ごとに例外措置を申請するべきである。セキュリティを維持できる代替措置として，接続鍵を定期的（1か月～1年ごと，あるいは会議室の利用ごと）に変更することや，会議室外からの接続を防ぐ対策の採用などがあり得る。

例外措置申請の記入例：

申請者：　会議室の管理者である教職員

適用開始日・終了日：　年度ごと

申請対象規程：　D2201 情報サービス利用規程　第三条

申請対象システム名：　会議室無線LAN環境

申請理由：　会議室で開催する研究会合の参加者が会議室無線LAN環境を利用することについて、訪問者が個別に許可を受けると著しく非効率なので、会議室の無線LAN環境のアクセスポイントに個人認証を要しない接続鍵を設定して、その接続鍵を会議室内に掲出して会議室利用者へ伝える。

代替措置の内容：　会議室に不審者が入室して接続鍵を知ることが無いよう、利用時以外に施錠することとして、鍵の貸し出し状況を記録する。接続鍵は1か月（～1年）ごとに変更する。会議室の無線LAN環境は室外から接続しにくいよう電波強度を調整する。

（３）大学間無線アクセスローミングシステムを用いるケース

　所属大学から発行されたアカウントを用いて，大学間認証連携によって来訪者を個人認証して無線LAN環境を来訪者へ提供する大学間無線アクセスローミングシステムがあり，国際的な運用としてeduroamがある。このケースでは，大学から個別に許可しなくても個人認証によって十分にセキュリティ維持できることを加入時及び年度ごとに運用規約などにより確認して，例外措置を申請するべきである。

　なお，eduroamについては，運用体制として2010年にGlobal eduroam Governance Committee (GeGC)が組織され，ここでCompliance Statementが作成され，参加機関はこれに記された技術要件に従うことが求められる。また，日本国内のeduroam JPでもCompliance Statementの内容に合わせて、 正式な実施要領・運用基準を定めていくことになる。

例外措置申請の記入例：

申請者：　全学実施責任者（になるのか？）

適用開始日・終了日：　年度ごと

申請対象規程：　D2201 情報サービス利用規程　第三条

申請対象システム名：　eduroam無線LAN環境

申請理由：　学内において学外からの来訪者が無線LAN環境を利用することについて、訪問者が個別に許可を受ける代わりに、訪問者の所属機関における個人認証に基づく国際大学間無線LANローミングeduroamの方式で利用を可能とする。

代替措置の内容：　eduroam方式により訪問者の所属機関の個人認証に基づいて利用させる。無線LAN環境（アクセスポイント）のログにより、利用した日時等とともに訪問者の所属機関を記録して、調査が必要になった場合に所属機関へ調査依頼できるようにする。

（４）無線LAN環境を商用サービスに兼用させるケース

　大学が構築した無線LAN環境を商用無線アクセスサービスと兼用させるケースでは，その商用サービスの加入者である来訪者が大学に対する許可申請をすることなく，来訪者へ利用を提供することができる。ただし，商用サービスとの兼用をすることについて，施設の提供だけとみなして情報システムの例外措置とみなさない考えがあり得る。または、商用サービスの部分も本学情報システムの一部とみなす場合には、全学実施責任者がアクセス制限の分離や運用管理の分界点などを定めた契約を交わして例外措置の申請をする考えがありうる。