北海道大学における情報セキュリティ対策基本計画

平成 31 年 4 月 1 日

全体方針

（1）情報セキュリティ対策基本計画の策定

本学では，国立大学法人の責務を果たすため，情報セキュリティの確保に関する次に掲げる施策を実施する。

・インシデントの発生を前提とした情報セキュリティ管理体制の整備及び強化
・情報資産の保護
・情報システムのセキュリティの維持及び向上
・情報セキュリティに関する教育・訓練及び啓発活動等
・情報セキュリティの監査，点検及び関連規程等の更新等

個別取り組み

（2）情報セキュリティインシデント対応体制及び手順書等の整備

①情報セキュリティインシデントが発生した場合のインシデント対応体制を，最新のセキュリティ脅威や脆弱性を意識して随時見直しを行う。
②インシデントが発生した場合に備えて，学内情報機器の把握および，情報機器の停止，ネットワークの遮断等の手順書を整備し，関係者間で共有するとともに，随時見直しを行う。
③インシデントが発生した場合に，インシデント対応体制に則って迅速かつ的確に対応するために，インシデント対応を行う職員を対象とした教育訓練を定期的（少なくとも年１回以上）に実施する。

（3）情報セキュリティポリシーや関連規程の組織への浸透

①構成員に対して「情報セキュリティポリシー」や「関連規程等」を，ホームページに掲載する等いつでも入手可能な状態にするとともに，説明会等の機会を利用し，周知徹底を図り，その内容については必要に応じ見直しを行う。
②「情報資産格付けや取扱区分」を浸透させるために，格付けや取扱区分を構成員が理解しやすい運用方法を策定し，説明会や情報セキュリティ関連のセミナー等で周知を図り，学内への浸透を図る。

また，運用方法等については，実情に即して見直しを行う。

（４）情報セキュリティ教育・訓練及び啓発活動の実施

①情報セキュリティ教育・訓練や啓発活動を定期的に実施し，役員やその責任に応じ情報セキュリティ対策の理解を深める。
②インシデント発生時における迅速・的確な対応が実施できるよう実践的なインシデント対応模擬訓練を実施し，インシデントへの対応力を高める。
③情報セキュリティ対策に係る「対策ガイドライン（マニュアル）(外国語版を含む)」,「リーフレット」等を作成し，教職員，学生，留学生に対し周知徹底を図る。
④本学における情報セキュリティ対策，最新のサイバーセキュリティ動向等の情報を，ホームページを利用して周知を図る。
⑤訓練やセミナーの参加状況を把握し，未受講者に受講を促す。

（５）情報セキュリティ対策に係る自己点検・監査の実施

①「情報セキュリティ対策基本計画」の進捗状況を把握するため，自己点検及び監査を定期的又は必要に応じ実施する。
②情報セキュリティ監査責任者が実施する監査結果に基づき,「情報セキュリティ対策基本計画」の取り組み事項を必要に応じて見直す。
③リスクアセスメントを行い，本学の情報資産に内在するリスクを検証し，情報セキュリティ対策に反映する。

（６）情報機器の管理状況の把握及び必要な措置の実施

①グローバル IP アドレスを付与する全ての情報機器の管理状況や通信要件を把握し，適切なアクセス制御を実施する。
②グローバル IP アドレス管理台帳を作成し，プライベート IP アドレスの移行準備を行うと共に，これらについて定期的に棚卸し等を実施する。
③適切なソフトウェアバージョン管理の周知徹底を行うと共に，ソフトウェアの脆弱性情報について，随時情報提供を行う。
④自己点検及び監査等に基づく，効果的な機器導入の検討を行う。
⑤学内に設置している監視カメラ等の IoT 機器の設置状況を把握し，適切なアクセス制御を行う。
⑥パスワードの適切な管理について，他との使いまわしをさせない等，第三者による不正利用を防止するために，啓発活動を継続して実施する。

⑦ペネトレーションテスト等の実施により，本学に設置されている機器のセキュリティ状況の把握と，対策を実施及び指導をする。
⑧情報基盤システムやネットワーク構成等に際し，上記の項目を適切に反映させる。

（7）情報セキュリティ人材の育成と外部連携

①文部科学省や民間企業等が実施している情報セキュリティ関連の研修に参加し，本学情報セキュリティ担当者のスキル向上を図る。
②JPCERT コーディネーションセンター，日本シーサート協議会，民間の業者等の外部機関と連携を図り，最新のサイバー攻撃の情報収集・対策等を行う。

個別の取組の実施時期（工程表）

・「北海道大学情報セキュリティ対策基本計画工程表（後期）」に基づき実施する。
・なお，2022 年度以降の工程表については，進捗状況等を踏まえ別途検討する。

北海道大学情報セキュリティ対策基本計画工程表【2019年度～2021年度】

年度		2019年度	2020年度	2021年度
個別方針	取組事項	工程		
（2）情報セキュリティインシデント対応体制及び手順書等の整備	インシデント対応体制を，最新のセキュリティ脅威や脆弱性に意識して随時見直す。	必要に応じた見直し		総括/見直し
	インシデント対応の手順書を整備し，関係者間で共有するとともに，随時見直す。	必要に応じた見直し		総括/見直し
	インシデント対応を行う職員を対象とした教育訓練を定期的（少なくとも年1回以上）に実施する。	随時実施	随時実施	随時実施 総括/見直し
（3）情報セキュリティポリシーや関連規程の組織への浸透	「情報セキュリティポリシー」や「関連規程等」を，大学構成員がいつでも入手可能な状態にする。	対策室ホームページの整備	ホームページの随時更新	総括/見直し
	「情報セキュリティポリシー」や「関連規程等」を説明会等の機会を利用し周知徹底を図り，その内容については必要に応じ見直す。	階層別研修・リーフレット等広報物等で周知 内容の随時見直し	階層別研修・リーフレット等広報物等で周知 内容の随時見直し	階層別研修・リーフレット等広報物等で周知 内容の随時見直し 総括/見直し
	「情報資産格付けや取扱区分」について構成員が理解しやすい運用方法を策定し説明会等で周知を図り，学内への浸透を図る。	運用方法検討・試行・周知	周知徹底	総括/見直し
（4）情報セキュリティ教育・訓練や啓発活動の実施	教育・訓練や啓発活動を定期的に実施する。	eラーニング研修等を実施	必要に応じて内容の見直し eラーニング研修等を実施	eラーニング研修等を実施 総括/見直し
	実践的なインシデント対応模擬訓練を実施する。	随時実施	随時実施	随時実施 総括/見直し
	「対策ガイドライン（マニュアル）（外国語版を含む）」，「リーフレット」等を作成し，教職員，学生，留学生に対し周知徹底を図る。	ガイドライン・リーフレット配布 前期総括リーフレット作成・配布	ガイドライン・リーフレット配布 教職員向けリーフレット作成・配布 学生(留学生)向けリーフレット作成・配布	ガイドライン・リーフレット配布 総括/見直し
	情報セキュリティ対策や最新のサイバーセキュリティ動向等の情報を，ホームページを利用して周知を図る。	対策室ホームページの整備	ホームページの随時更新	総括/見直し
	訓練やセミナーの参加状況を把握し，未受講者に受講を促す。	参加状況把握・受講促進	参加状況把握・受講促進	参加状況把握・受講促進 総括/見直し
（5）情報セキュリティ対策に係る自己点検・監査の実施	自己点検及び監査を定期的又は必要に応じて実施する。	自己点検実施 監査の実施	自己点検実施 監査の実施	自己点検実施 監査の実施 総括
	監査結果に基づき，「情報セキュリティ対策基本計画」の取組事項を必要に応じて見直す。	フォローアップ	フォローアップ	フォローアップ 見直し
	リスクアセスメントを行い，本学情報資産に内在するリスクを検証し，情報セキュリティ対策に反映する。	リスクの分析と対策の検討	リスクの分析と対策の検討	リスクの分析と対策の検討 基本計画の総括
（6）情報機器の管理状況の把握及び必要な措置の実施	グローバルIPアドレスを付与する全ての情報機器の管理状況等を把握する。	グローバルIPアドレスの把握		総括/見直し
	グローバルIPアドレス管理台帳を作成し，プライベートIPアドレスの移行準備を行うとともに，定期的に棚卸し等を実施する。	グローバルIPアドレス台帳の整備・棚卸の実施 一部部局での移行試行	対象部局を広げて試行実施	対象部局を広げて試行実施 総括/見直し
	ソフトウェアバージョン管理の周知徹底を行うとともに，ソフトウェアの脆弱性情報について随時情報提供を行う。	周知徹底と脆弱性情報の広報		総括/見直し
	自己点検及び監査等の結果に基づく，情報セキュリティ対策に効果的な機器導入の検討を行う。	自己点検及び監査等に基づく，効果的な機器の検討		総括/見直し
	IoT機器の設置状況を把握し，適切なアクセス制御を行う。	学内設置IoT機器の把握と，セキュリティ対策の指導		総括/見直し
	パスワードの適切な管理について，啓発活動を継続して実施する。	セミナー・研修・学内通知等で啓発を随時実施		総括/見直し
	ペネトレーションテスト等の実施により，本学に設置されている機器のセキュリティ状況を把握し，必要に応じて対策を講じる。	学内設置機器へのペネトレーションテストの実施 結果に基づく，対策方法の指導	学内設置機器へのペネトレーションテストの実施 結果に基づく，対策方法の指導	学内設置機器へのペネトレーションテストの実施 結果に基づく，対策方法の指導 総括/見直し
	情報基盤システムやネットワーク構成等に関し、各取組事項の結果を適切に反映させる。	情報収集等 調達及び更新	調達及び更新	総括/見直し
（7）情報セキュリティ人材の育成と外部連携	情報セキュリティ関連の研修に参加し，本学担当者のスキル向上を図る。	各種情報セキュリティ研修へ参加		総括/見直し
	外部機関等と連携を図り，最新のサイバー攻撃等の情報収集を行う。	外部機関との連携及び情報収集，ワーキンググループ等への参加による貢献		総括/見直し