茨城大学情報セキュリティポリシーガイド

情報戦略機構
2023 年 3 月

茨城大学情報セキュリティポリシー（iISP）とは？

本学が研究・教育機関として運営していくには、情報資産の活用が不可欠です。茨城大学情報セキュリティポリシー（iISP）は、本学の情報資産を安全かつ効果的に活用するために、本学の全教職員・学生が守るべき約束事です。iISP では、「どのような情報資産を、どのような脅威から、どのように守るのか」といった基本的な考え方や方針、情報セキュリティを確保するための方針・体制・運用規定・対策基準などが網羅されています。

茨城大学情報セキュリティポリシーは、以下の URL に掲載されています（学外からは一部のみ閲覧可）
https://www.ibaraki.ac.jp/isp/

iISP の適用範囲　～何を守るのか、誰が守らなければならないのか～

【何を】**本学が掌握するすべての情報資産**が対象です。

情報資産とは、情報そのものばかりでなく、情報を管理する仕組みやそれらに関する情報も含まれています。具体的には、学内ネットワーク環境（有線 LAN・無線 LAN）、メール環境、PC、ソフトウェア、各種サーバ、各種業務データ（印刷物含む）など、有形の情報機器から無形の情報やソフトウェアまで、すべて情報資産になります。

【誰が】**本学の情報資産を利用する すべての人**が対象です。

本学の役員、教職員、学生（外国人留学生、科目等履修生、特別聴講学生、委託生、研究生その他これに準じる非正規生を含む。）だけでなく、派遣労働者や本学の業務を受託した業者、ID の臨時利用者など、情報資産を利用するすべての人が iISP の遵守を求められます。

iISP の構成

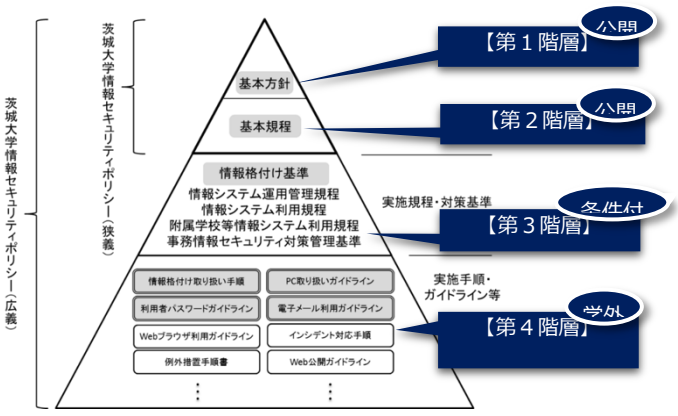
iISP は４つの階層からなります。

第１階層：【基本方針】
iISP の目的、考え方等の宣言です。

第２階層：【基本規定】
iISP を実施するための体制や役割などを定めています。

第３階層：【実施規定・対策基準】
「何を実施しなければならないのか」を定めています。

第４階層：【実施手順・ガイドライン】
第３階層で定めた事項を実際にどのように行うのかといったマニュアルやガイドラインを定めています。



iISP のうち一般の利用者向けの内容

1. **自分の ID やパスワードを適切に管理すること**
   - 自分自身が利用する PC やスマホなどには必ずパスワードをかける。
   - パスワードは他人に絶対に教えない。パスワードを他人に見える場所に貼り付けておくのもダメ。
   - 自分のアカウントを他人に使わせない。
2. **PC のセキュリティ対策を行う**
   - Windows, macOS, Linux などの OS を最新にする。
   - ウィルス対策ソフトを使用時にはウィルス定義ファイルが最新に保つ。
3. **情報漏洩しないように注意する**
   - USB メモリや PC の紛失・盗難に注意する。学外秘情報を格納するときには暗号化を。
   - SNS、個人ブログ、Twitter などで学内限定情報を発信しない。
4. **ソフトウェアの不正利用をしない**
   - 正当なライセンスのないソフトウェアやコンテンツの所有や利用をしない。
   - メーカーのサポートが終了したソフトウェアを利用し続けない。
   - 離職や卒業などによりライセンスが無効になったソフトウェアは速やかにアンインストールする。
5. **大学所有の PC では適切なソフトウェア管理を**
   - 教職員は大学所有の PC 等におけるソフトウェア管理に責任を持つこと。
   - 学生は大学所有の PC 等に指導教員の許可無くソフトウェアをインストールしないこと。
6. **情報発信者としてのリテラシーを身に付ける**
   - Twitter, Facebook, Instagram などで情報発信するときには情報の内容に責任をもつこと。
   - 不特定多数に閲覧されても恥ずかしくないか。特にリツイートは誤った情報の拡散になっていないか。
   - 自身の個人情報の取り扱いには注意する。攻撃に悪用される危険性を念頭におくこと。

iISP 違反が確認された場合

悪質な iISP 違反が確認された場合には懲戒処分などが課されたり茨大 ID の利用が制限されたりする場合があります。

以上