# 地方独立行政法人東京都立産業技術研究センター
# 情報セキュリティ対策基準

地方独立行政法人東京都立産業技術研究センター
理事長　　奥村 次徳

目次

## １．目的

- 本基準は、地方独立行政法人東京都立産業技術研究センター（以下「都産技研」という。）における情報セキュリティ基本方針に基づき、より具体的な対策基準を定めるものである。

- 都産技研は、中小企業への技術支援を担うことにより、直接的な顧客である中小企業のみならず、都民及び社会経済に必要不可欠なサービスを提供している。ゆえに、これらを支える情報資産を様々な脅威から守ることは、都産技研に課せられた責務である。

- 雇用関係の有無を問わず、都産技研を構成する全ての者は、本基準に従って、情報セキュリティ対策を実施する。

## ２．本基準の位置付け

本基準の位置付けを図１に示す。

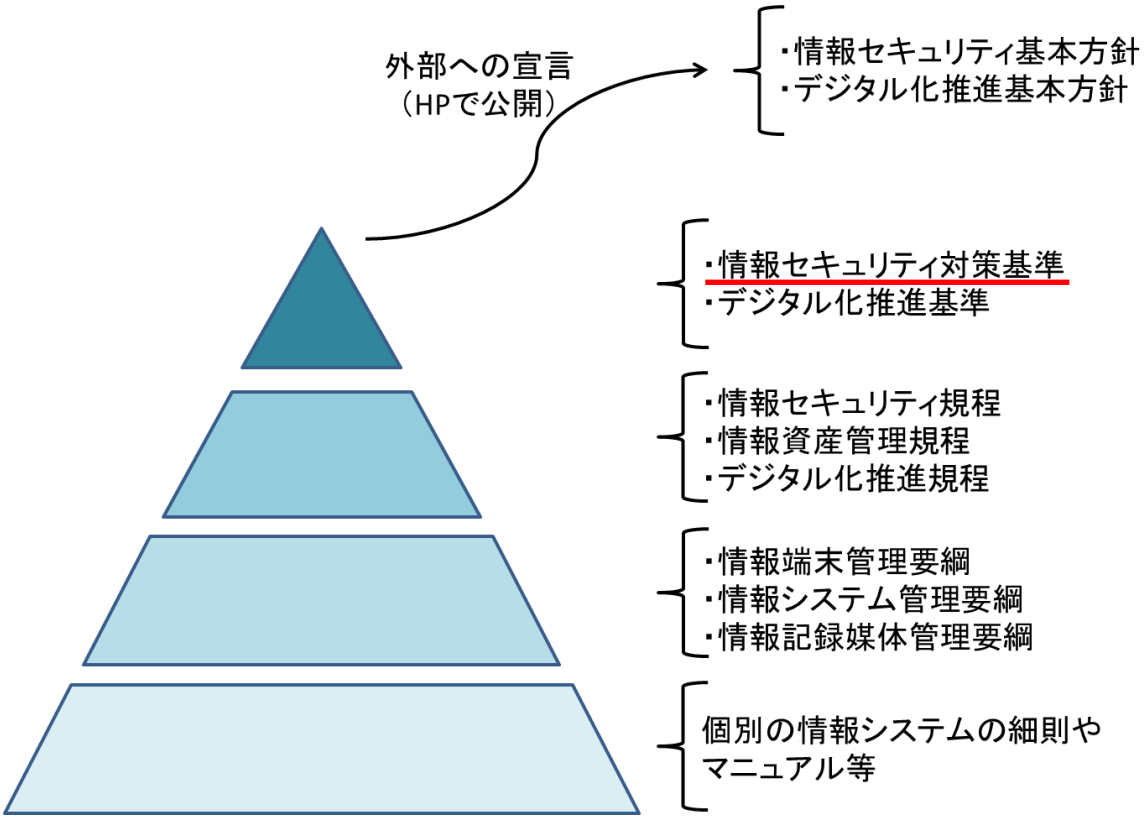


図１．本基準の位置付け

## ３．用語

（１） 情報セキュリティポリシー

情報セキュリティ基本方針及び本基準を合わせたものをいう。

（２） 職員等

雇用関係の有無を問わず、都産技研を構成する全ての者をいう。

（３） 情報資産

職員等が業務上作成、収集、又は取得した情報であって、書類に記録されたもの及び電子的な記憶媒体に保存されているもの

（４） 機密性

ある情報資産を取り扱うことを認められた者だけが、その情報資産を取り扱うことができる状態をいう。

（５） 完全性

情報資産が破壊、改ざん又は消去されていない状態をいう。

（６） 可用性

ある情報資産を取り扱うことを認められた者が、必要なときに中断されることなく、その情報資産を取り扱うことができる状態をいう。

（７） 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（８） 侵害

情報資産の機密性、完全性及び可用性のうち、いずれか一つ以上が維持できなくなることをいう。

（９） 脅威

侵害の要因もしくは現象をいう。

（１０） 端末

職員等に対し、業務上利用することが許可されたパソコン、モバイル端末等をいう。

（１１） 外部記録媒体

職員等に対し、業務上利用することが許可されたＵＳＢメモリや光ディスク等の外部記録媒体をいう。

（１２） 情報システム

都産技研の運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。

（１３） ネットワーク

端末や、情報システム等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

## ４．適用範囲及び遵守義務

- 本基準は、職員等に適用される。

- 職員等は、都産技研が保有する情報資産に対する脅威への対応の重要性について、常に共通の認識を持たなければならない。

- 職員等は、業務の遂行に当たって、本基準及び関連規程等を遵守する義務を負う。

## ５．対象とする脅威

情報資産に対する脅威として、以下のものを想定し、情報セキュリティ対策を実施するほか、新たな脅威の発生に備え、最新の脅威動向を確認するなど、適切に対応する。

（１） 不正アクセス、マルウェア、サービス不能攻撃等のサイバー攻撃及び部外者の侵入等の意図的な要因による、都産技研が保有する情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取のほか、内部管理の欠陥など職員等による不正行為等

（２） 都産技研が保有する情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンスの不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３） 地震、落雷、火災等の災害によるサービス及び業務の停止等

（４） 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

（５） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

## ６．脅威への対策

脅威から情報資産を保護するために、以下の対策を講じる。

（１） 組織体制の確立
都産技研の情報資産について、情報資産の管理及び情報セキュリティ対策を実施する全所的な組織体制を確立する。

（２） 情報資産の分類と管理
保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき、情報セキュリティ対策を講じる。

（3） 物理的セキュリティ対策

サーバ、管理区域、準管理区域、通信回線等及び業務用端末等の管理について、物理的な対策を講じる。

（4） 人的セキュリティ対策

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（5） 技術的セキュリティ対策

端末や情報システム等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（6） 運用面での対策

端末や情報システムの監視、並びに本基準や関連規程等の遵守状況を定期的に確認するための対策を講じる。また、情報資産に対する侵害が生じた場合等に迅速かつ適正に対応するための対策を講じる。

（7） 外部サービスの利用及び業務委託に係る対策

都産技研の業務を受託する事業者に当該業務を行わせる場合には、本基準や関連規程等、遵守させるべき事項を、外部委託事業者等の選定要件として提示する。また、約款による外部サービスを利用する場合には、当該利用に係る規程等を整備し、対策を講じる。

## ７．自己点検及び監査

情報セキュリティ対策を自律的に見直す仕組みを構築し、実行する。

- 情報セキュリティに係る内部環境及び外部環境の変化を踏まえ、情報セキュリティの対策状況を自己点検し、必要に応じて改善策を講じる。

- 本基準及び関連規程等の遵守状況を検証するため、監査を実施する。

**附則**

本基準は、2021 年 6 月 1 日から施行する。