公開版

学校法人東京電機大学

サイバー攻撃等による被害に備えたBCP
（Business Continuity Plan：事業継続計画）

令和6年（2024年）度版

目次

第１章 総則 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1

1.1 策定目的 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
1.2 基本方針 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
1.3 対象範囲 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
1.4 インシデント発生時優先業務 ・・・・・・・・・・・・・・・・・・・・・・ 2
1.5 文書の管理および周知 ・・・・・・・・・・・・・・・・・・・・・・・・・ 2
1.6 事業継続マネジメント（BCM） ・・・・・・・・・・・・・・・・・・・・・ 2

第２章 体制整備 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 4

2.1 情報機器等の把握と適切な管理 ・・・・・・・・・・・・・・・・・・・・・ 4
2.2 非常時に備えたサイバーセキュリティ体制 ・・・・・・・・・・・・・・・・ 6

第３章 サイバーインシデント発生時の対応 ・・・・・・・・・・・・・・・・・ 9

3.1 異常発見時の連絡先 ・・・・・・・・・・・・・・・・・・・・・・・・・・ 9
3.2 システム異常の検知と CISO への情報伝達 ・・・・・・・・・・・・・・・ １０
3.3 初動対応 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ １０
3.4 業務継続 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ １１
3.5 復旧処理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ １１

第４章 事後対応 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ １２

4.1 報告 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ １２
4.2 再発防止 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ １２
4.3 情報公開 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ １２

別紙１ 総合メディアセンターのインシデント発生時優先業務一覧表 ・・・・・ １３
別紙２ インシデント対応フロー ・・・・・・・・・・・・・・・・・・・・・・ 非公開

第 1 章 総則

1.1 策定目的

サイバー攻撃等による被害に備えた事業継続計画（以下、本 BCP という）は、学校法人東京電機大学（以下、本法人という）において、サイバーインシデント発生時に本法人への被害を最小限に食い止めることおよび中核事業（教育・研究・学園業務）を継続させることを目的とし、いち早く事業全体を復旧させるためのさまざまな対策・方法をまとめた計画である。

1.2 基本方針

本法人は、情報システムの継続性を確保するために、以下の方針に基づき、サイバーセキュリティ対策の水準を高めていく。主として総合メディアセンターと TDU-CSIRT が連携して対応する。

- 安全かつ持続的な IT サービス提供を実現する
- サイバーセキュリティに対する脅威からの被害から事業を保護する
- リスクマネジメントの対象としてサイバーセキュリティを確保する
- 平時、非常時を通じて事業継続に関する説明責任を果たす
- 被害後、安全を担保しつつ、迅速かつ合理的な業務復旧を行う

1.3 対象範囲

1.3.1 対象とする情報システム

対象とする情報システムは以下のとおりとする。

- 基幹ネットワークシステム
- 事務 PC システム
- 教学基幹システム
- ポータルシステム
- LMS システム
- 法人基幹システム
- 施設予約・出席管理システム
- 視聴覚システム
- メールシステム（教職員、学生）
- 統合 ID 管理システム
- 図書館業務システム　他

1.3.2 想定する事象

本 BCP で想定される事象において、中核業務に影響するものを以下に挙げる。なお、自然災害、大規模停電等による電源喪失などの計画は別に定めるものとする。

・ネットワークの接続不能
・各種システムの使用不能
・情報機器の操作不能・誤動作
・教職員および学生間の連絡不能
・その他

また、これらの被害を引き起こすサイバー攻撃の例として以下が挙げられる。

・不正アクセス等
・標的型メール攻撃
・マルウェア感染（ランサムウェアを含む）
・分散型サービス妨害（DDoS 攻撃）
・上記の予兆と思われる現象　他

1.4　インシデント発生時優先業務

総合メディアセンターの業務について、中核事業への影響度を評価し、インシデント発生時に優先すべき業務を別紙 1 のとおり定める。

1.5　文書の管理および周知

本 BCP は、原本および関連資料の整備ならびに管理を行い、情報戦略会議および情報セキュリティ戦略会議での審議を経た上で、本法人の全教職員に開示周知する。

1.6　事業継続マネジメント（BCM）

本 BCP は、「サイバーインシデント発生時に重要な事業を中断させない、又は中断しても可能な限り短い期間で復旧させるための方針、体制、手順等を示した計画」であり、事業継続マネジメント（BCM）（Business Continuity Management）は、「BCP 策定や維持・更新、事業継続を実現するための予算・資源の確保、対策の実施、取組を浸透させるための教育・訓練の実施、点検、継続的な改善などを行う平常時からのマネジメント活動」で、経営レベルの戦略的活動として位置付けられる。次の図に示すとおり、BCP は BCM の中に包含される関係になる。

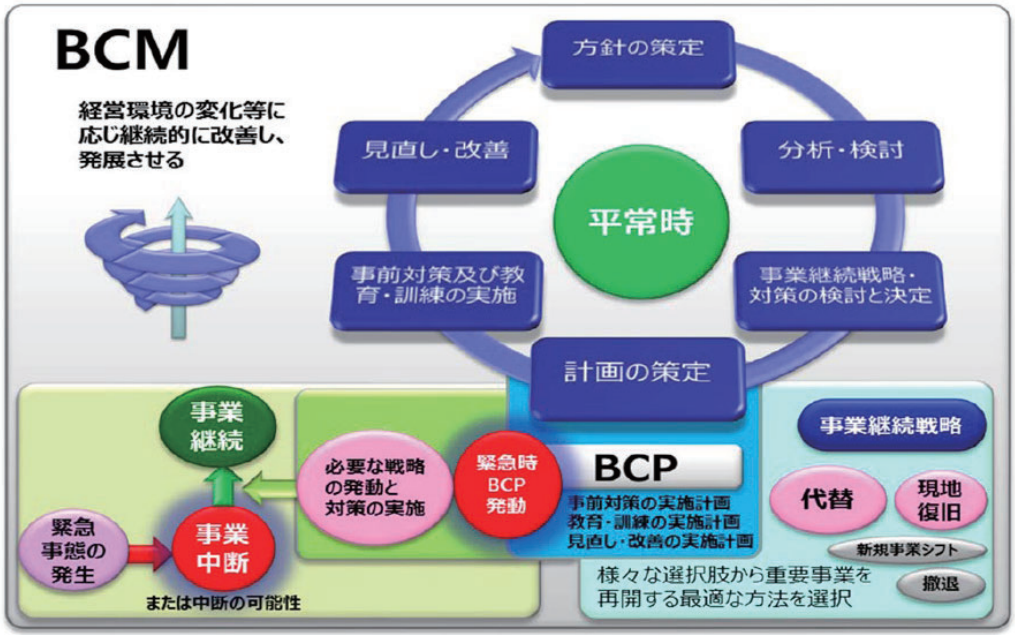

図１：BCP と BCM の関係

出典：内閣府「事業継続ガイドライン第三版」
http://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline03_ex.pdf

第 2 章 体制整備

2.1 情報機器等の把握と適切な管理

平時において、非常時に備えたサイバーセキュリティの体制整備を以下のとおり行う。

2.1.1 組織体制図

学園業務継続および情報システムの復旧を目的とした非常時のサイバーセキュリティの組織体制を以下のとおり定める。担当部署、担当者、役割についても示す。

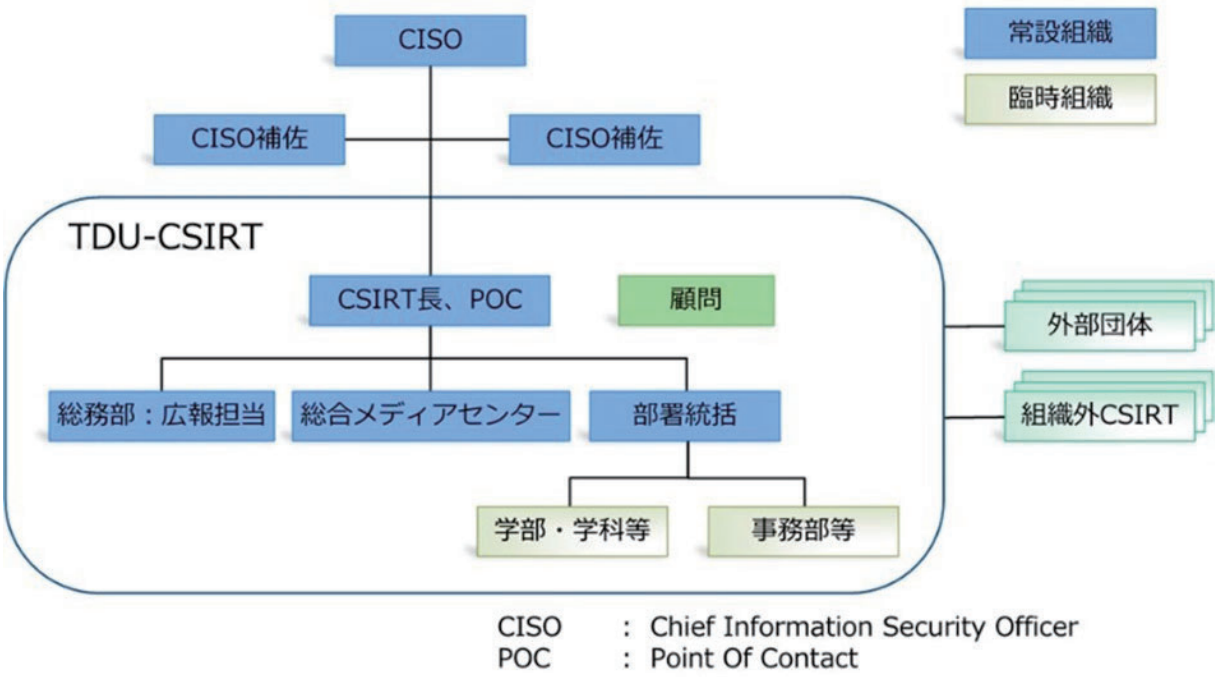

図 2 ：非常時の組織体制図

表 1 ：担当者の役割

役割	担当部署・担当者	役割の概要
情報セキュリティ最高責任者（CISO）	理事	本法人における情報セキュリティを統括し、本法人の教育研究および管理運営における情報セキュリティを重要な経営課題とし、その解決を図る。
CISO 補佐	-	CISO を補佐する。
東京電機大学シーサート（TDU-CSIRT）	総合メディアセンター、総務部	インシデント対応および発生の予防を行う。また、ネットワークやシステムへのサイバー攻撃や脅威の検知・分析を行う。

2.1.2 情報システム一覧

総合メディアセンターは、情報システムの現況を反映した管理台帳を整備する。管理台帳には以下の項目を記載する。併せて、定期的に棚卸しを行い、利用状況の確認を行う。

・システム名
・システム概要
・サービス運用担当者
・システム管理担当者
・導入時の情報
・主な製品名、メーカー
・利用状況
・扱う情報の概要
・個人情報の有無
・契約保守の有無
・更新予定時期
・備考　他

2.1.3 ネットワーク・システム構成図

総合メディアセンターは、本法人で導入している情報システムの全体構成図（ネットワーク図、システム構成図等）を整備する。併せて、構成、接続等に変更が生じた場合には構成図の更新を行い、常に最新の状態を保つ。

2.1.4 リスク評価

総合メディアセンターは、情報システム一覧に対しリスク評価を実施する。各システムに対し、リスクレベルを 3 段階で評価したうえで、どのようなリスクが存在しているか整理する。情報システム一覧の棚卸に併せて、リスク評価も再実施する。

2.1.5 脆弱性に関する対策

総合メディアセンターは、契約等で定められた責任分界をもとにサーバ、端末 PC、ネットワーク機器について脆弱性情報の収集を行う。脆弱性が発見された機器について、脆弱性対応プログラムの適応を行う。万が一、適応できない場合の代替手段（隔離運用、隔壁の追加、監視の強化、機器入れ替え等）について取り決め、実施する。

2.2　非常時に備えたサイバーセキュリティ体制

2.2.1 インシデント対応フロー

事業継続および情報システムの復旧に資するアクションを迅速に行う目的で、インシデント対応フローを別紙２のとおり定める（非公開）。また、インシデント発生時の外部関係機関の連絡先を以下のとおり定める。

表２：外部関係機関の連絡先一覧

外部関係機関	連絡先
非公開	

2.2.2 復旧対応体制

各システムについて、インシデント発生時に連絡する事業者を以下のとおり定める。

表３：システム・サービス事業者一覧

システム	事業者
基幹ネットワークシステム	非公開
事務 PC システム	
教学基幹システム	
ポータルシステム	
LMS システム	
法人基幹システム	
施設予約・出席管理システム	
視聴覚システム	
メールシステム（教職員、学生）	
統合 ID 管理システム	
図書館業務システム	

2.2.3 教育体制

本 BCP が迅速かつ適切に利用できるよう、TDU-CSIRT は年１回以上のトレーニング・研修に参加する。トレーニング・研修により、事前対策やサイバーインシデント発生時の対応計画等に解決すべき課題が判明した場合、課題の解決もしくは改善に向けた計画の立案をする。

2.2.4 バックアップ体制

サイバーインシデント発生時に備えた、各システムのバックアップの頻度、作成方法および復旧方法について以下のとおり定める。

表４：バックアップの作成と復旧方法

システム	頻度	作成方法	復旧方法
非公開			

第３章 サイバーインシデント発生時の対応

3.1 異常発見時の連絡先

異常発見時の連絡経路は別紙２インシデント対応フローに示すとおりとする。併せて、異常発見時の連絡先を以下のとおり示す。

表５：異常発見時の連絡先

担当	連絡先
東京電機大学シーサート （TDU-CSIRT）	tdu-csirt(at)csirt.dendai.ac.jp ※(at)は@に置き換え

表６：システム・サービス事業者一覧

システム	事業者
基幹ネットワークシステム	非公開
事務 PC システム	
教学基幹システム	
教学ポータルシステム	
LMS システム	
法人基幹システム	
施設予約・出席管理システム	
視聴覚システム	
メールシステム（教職員、学生）	
統合 ID 管理システム	
図書館業務システム	

3.2　システム異常の検知と CISO への情報伝達

学内関係者がシステム異常を検知した場合、あらかじめ定めた項目（発生場所、発生箇所、発生日時、連絡者、異常の内容・範囲）について TDU-CSIRT に報告できるように周知する。また、学内外から発出された異常において、TDU-CSIRT によりサイバー攻撃の可能性が思慮された場合、別紙２インシデント対応フローを基に、速やかに CISO ならびに関係各所・外部関係機関に共有され、意思決定できるように努める。なお、CISO は必要に応じて適宜、理事長・学長へ状況報告を行う。

3.3　初動対応

サイバーインシデント発生後は、以下のとおり対応する

3.3.1 原因調査

TDU-CSIRT は、学内での調査が可能か判断する。学内での調査が可能な場合、サイバーインシデントの原因や被害範囲の特定のために調査を実施する。必要に応じ、情報システム・サービス事業者へ以下の調査依頼を指示または実施する。

・ネットワーク機器やケーブル等の調査
・電源系統、ブレーカー、ハードウェア、ソフトウェア等の調査
・情報漏えいの有無に関する調査
・メンテナンスやデータ移行等の作業に関する調査
・その他、必要な調査等

3.3.2 被害拡大防止

TDU-CSIRT は、被害拡大防止のための対応を行う。まずは、外部との通信経路を遮断する。その上で、被害箇所から攻撃範囲および侵入経路の推定を行った上で、セグメンテーション境界において、通信を遮断して感染拡大防止を図る。

3.3.3 CISO への報告

TDU-CSIRT は、サイバーインシデントについて CISO に対して現在の被害状況を報告するとともにインシデント対応方法と情報保全を担保する運用方針案を提案する。この内容を踏まえて、CISO はシステム停止に伴う学園業務継続方針を検討し意思決定する。決定した内容は、速やかに別紙２インシデント対応フローで定める組織内ならびに外部関係機関へ周知を行う。なお、CISO は必要に応じて適宜、理事長・学長へ状況報告を行う。

3.4　業務継続

サイバーインシデント対応と業務継続について報告を受けた CISO は以下のとおり対応する。

3.4.1 情報システムの縮退運転判断

CISO は、TDU-CSIRT からの提案を受け、情報システム等の縮退運転または運転中止を判断する。また、インシデント対応中の業務継続においては、自然災害時を想定した事業継続計画に則り運用する。

3.4.2 被害状況等調査（フォレンジック調査＋証拠保全）

TDU-CSIRT は､証拠保全の作業と業務継続に関する作業を調整しながら両立させる。具体的には、アクセスログの分析や情報の改ざん、暗号化の有無等からサイバー攻撃の範囲、個人情報漏えいの有無等の調査を行う。必要に応じて情報システム・サービス事業者等へ協力依頼して調査を進める。なお、調査状況は随時 CISO に報告する。

3.4.3 組織対応方針の確認と外部関係機関への報告

被害状況および TDU-CSIRT の調査結果に基づき、CISO は復旧対応方針（復旧に向けた対応、広報への対応）を決定し、その対応を関係者に指示する。また、2.2.1 で定める外部関係機関へ報告を行う。外部関係機関へは被害拡大防止等の観点からできる限り早く連絡する。

3.5　復旧処理

復旧計画に基づいて、以下のとおり対応する。総合メディアセンターは情報システムの事業者およびサービス事業者等と協力して復旧を行う。

3.5.1 復旧指示と復旧作業

総合メディアセンターは、CISO からの復旧指示を起点とする復旧対応方針に基づき、システムの復旧作業(システムの再設定、再インストール、バックアップデータからの復元等)並びに検証作業を行う。必要に応じ情報システム・サービス事業者に対応を依頼する。

3.5.2 結果の確認

総合メディアセンターは、復旧作業により復旧したシステムが安全な状態で正常に稼働したことを確認する。正常に稼働することが確認できた時点で、CISO に報告する。CISO は業務状況を総合的に勘案し、緊急時運用から通常運用への復旧を宣言する。

第 4 章 事後対応

4.1 報告

復旧後、総合メディアセンターおよび TDU-CSIRT は、復旧結果と情報漏えい事実の有無等について CISO および組織内に報告する。不足していたと考えられる事前対策、連絡先ならびに連絡内容について振り返りを行う。

4.2 再発防止

4.2.1 再発防止策検討・策定

4.1 の後、総合メディアセンターおよび TDU-CSIRT は、サイバー攻撃により発生した被害を抑止する手段について検討を行い、実施可能な選択肢を整備し、CISO に提案する。CISO は長期的視点と事業継続性の両立について検討し、安全性を維持するため再発防止策の選択を決定する。CISO は決定した再発防止策について、連絡経路を用いて全職員に周知する。

4.2.2 事業者への指示

CISO によって決定された再発防止策は、総合メディアセンターにより、事業者が有するサービスや機器に対して対策を講じる必要があるかどうかを調査し、再発防止策の効果が出るよう対策実施を事業者へ打診する。事業者は、対策実施の時期や方法について、本法人と誠実に議論し、計画を立てて実施する。

4.3 情報公開

CISO は、類似のサイバー攻撃による被害拡大に対する警鐘を鳴らす目的、また本法人の関係者に注意を喚起する目的で、速やかに情報公開を行う。情報公開内容は、知覚日時、現象、被害範囲、想定される攻撃経路、1 次対応、復旧状況、事後対策などを含める。報告については、サイバー被害が発生した可能性が高い段階から迅速に行い、情報の更新を含めて複数回行う中で情報の確度を高めていく。

別紙１　総合メディアセンターのインシデント発生時優先業務一覧表

業務内容		目標復旧時間・期間							優先度
		１ｈ以内	３ｈ以内	24ｈ以内	72ｈ以内	１週間以内	２週間以内	１か月以内	
１．企画・開発に関する事項	（１）情報の収集、蓄積、サービス及び管理							⇒	
	（２）情報システム及び図書資料に関する各種調査及び調整							⇒	
	（３）情報システム及び図書資料に関する広報誌の編集及び発行							⇒	
	（４）情報システムに関する中・長期計画の企画、立案、調整並びに実施							⇒	
	（５）情報資源の導入（購入、レンタル及びリース）に関する事前調査							⇒	
	（６）学園のネットワーク及びキャンパス間ネットワークの運用			⇒	⇒	⇒	⇒	⇒	◎
	（７）システム運用に必要とされるプログラムの整備及び開発							⇒	
	（８）セキュリティの維持					⇒	⇒	⇒	○
	（９）図書資料に関する整備計画の立案と実施							⇒	
	（10）特別に組織されたプロジェクトの運営							⇒	
	（11）学外との情報交換及び協力							⇒	
	（12）運営委員会の運営							⇒	
	（13）総合メディアセンター全体の予算管理							⇒	
２．運用及び管理に関する事項	（１）教育、研究及び事務における情報処理の支援							⇒	
	（２）情報処理に係わる教育及び自主学習の支援							⇒	
	（３）情報システムの運用及び管理			⇒	⇒	⇒	⇒	⇒	◎
	（４）キャンパス内ネットワークの運用、保守管理			⇒	⇒	⇒	⇒	⇒	◎
	（５）図書資料の整備、収集、管理及び運用					⇒	⇒	⇒	○
	（６）視聴覚教材の整備、収集、管理及び運用					⇒	⇒	⇒	○
	（７）データベース等の情報の整備、管理及び運用					⇒	⇒	⇒	○
	（８）教育工学機器・設備の整備、管理及び運用			⇒	⇒	⇒	⇒	⇒	◎
	（９）利用者に対する広報及び利用の普及							⇒	
	（10）運営小委員会の運営							⇒	
３．その他の事項	（１）その他、企画・開発に関する事項							⇒	
	（２）その他、電算機処理・図書・メディア等に係わるサービスに関する事項							⇒	
	（３）入試センターからの委託業務							⇒	
	（４）ホームページ（所管するページ）の運営・管理					⇒	⇒	⇒	○
	（５）ホームページの技術支援に関する業務							⇒	
	（６）他部署からの委託業務							⇒	