情報セキュリティポリシー
に関する説明会

令和５年6月

説明会の内容

１．守るべき情報とは

２．情報セキュリティポリシーとは

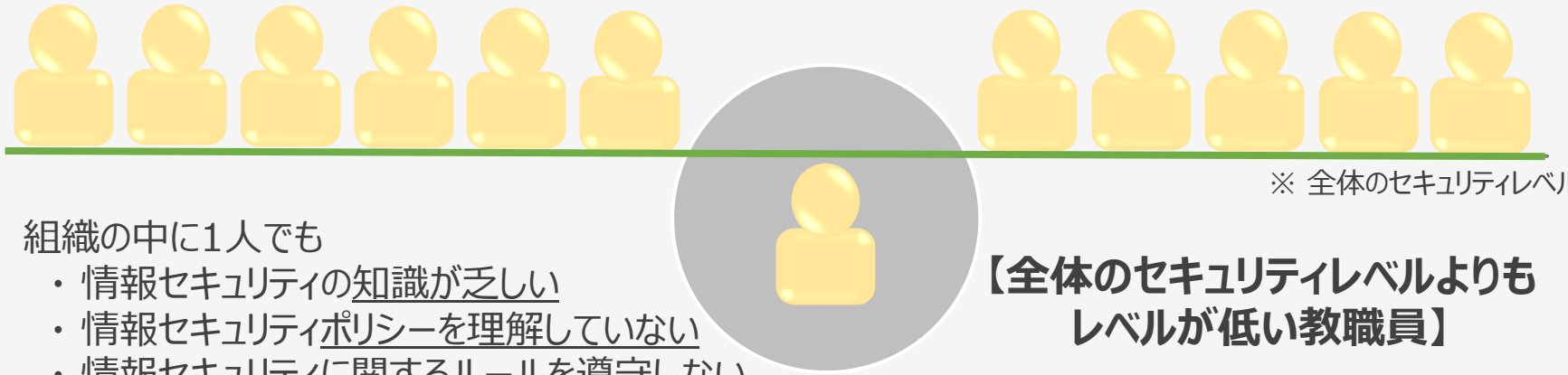
３．情報セキュリティポリシーの遵守事項

４．情報セキュリティの対策

説明会の目的

情報セキュリティ対策は、**全員で取り組なければ期待する効果が得られません。**

【全教職員】



※ 全体のセキュリティレベル

組織の中に1人でも
- 情報セキュリティの知識が乏しい
- 情報セキュリティポリシーを理解していない
- 情報セキュリティに関するルールを遵守しない

といった人物が存在すると**セキュリティインシデント（事件・事故）の発生可能性が高まります。**

**【全体のセキュリティレベルよりも
レベルが低い教職員】**

私一人くらい…という考えは捨て、全教職員に対策を徹底させることが重要です。
そのためにも、**全教職員を対象とした定期的な教育・研修が必要となります。**

１．守るべき情報とは
情報セキュリティとは

情報セキュリティとは

情報の **機密性**、**完全性**、**可用性** を維持すること。

機密性	完全性	可用性
Confidentiality 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。	**I**ntegrity 情報が破壊、改ざん又は消去されていない状態を確保することをいう。	**A**vailability 情報にアクセスする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、情報にアクセスできる状態を確保することをいう。

情報セキュリティの３要素は各英単語の頭文字をとり「CIA」とも呼ばれます

情報セキュリティ管理運用の取扱い（ 付録１　用語の定義 ）

1．守るべき情報とは
情報・情報資産とは

情報とは

- 職務上使用することを目的として本学が調達し、又は開発した情報処理若しくは通信の用に供する情報システム又は外部電磁的記録媒体に記録された情報
- 情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報

情報セキュリティ管理基本方針（ 第2条 2 ）

情報資産とは

- 情報及び情報システム、情報を格納・保存している外部記録媒体・機器・装置等をいう

具体的には

- 紙等の有体物に可視的に記録されたもの（文書、メモ、写真等）
- 外部記録媒体に記録されたデータ（音声・映像を含む）

  →CD、DVD、BD、USBメモリ、MO、SDカード、DAT、LTO、外付HDD　等
- サーバ、パソコン、タブレット、スマートフォン・携帯電話、デジタルカメラ、ICレコーダー等の機器に記録されたデータ（音声、画像、動画を含む）
- 会話の内容

１．守るべき情報とは
情報セキュリティに関する脅威の動向

情報資産を取り巻く脅威は、多様化・高度化しており、多面的かつ強固な対策が求められます。

これらの脅威から情報資産を守るための対策が必要です。

外部からの攻撃

・不正アクセス（侵入）
・Webサイト改ざん
・DoS，DDoS攻撃
・ランサムウェア
・標的型攻撃　等

自然災害

・地震、風水害、落雷　等

システム障害

・システム停止
・データ消失　等

内部不正
（職員等・委託業者）

・不正利用、不正持出　等

人的過誤・失敗

・オペレーションミス
（誤送付・誤送信等）
（情報の滅失・毀損）
・紛失
・SNSの不適切な利用　等

1．守るべき情報とは
情報セキュリティに関する脅威の動向

■ 情報セキュリティ 10 大脅威 2023（組織編）

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	標的型攻撃による機密情報の窃取
4	内部不正による情報漏えい
5	テレワーク等のニューノーマルな働き方を狙った攻撃
6	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7	ビジネスメール詐欺による金銭被害
8	脆弱性対策情報の公開に伴う悪用増加
9	不注意による情報漏えい等の被害
10	犯罪のビジネス化（アンダーグラウンドサービス）

上位3件はすべて「外部からの攻撃」によるものです

外部からの攻撃による脅威が社会的影響の大きいものとして位置づけられています！

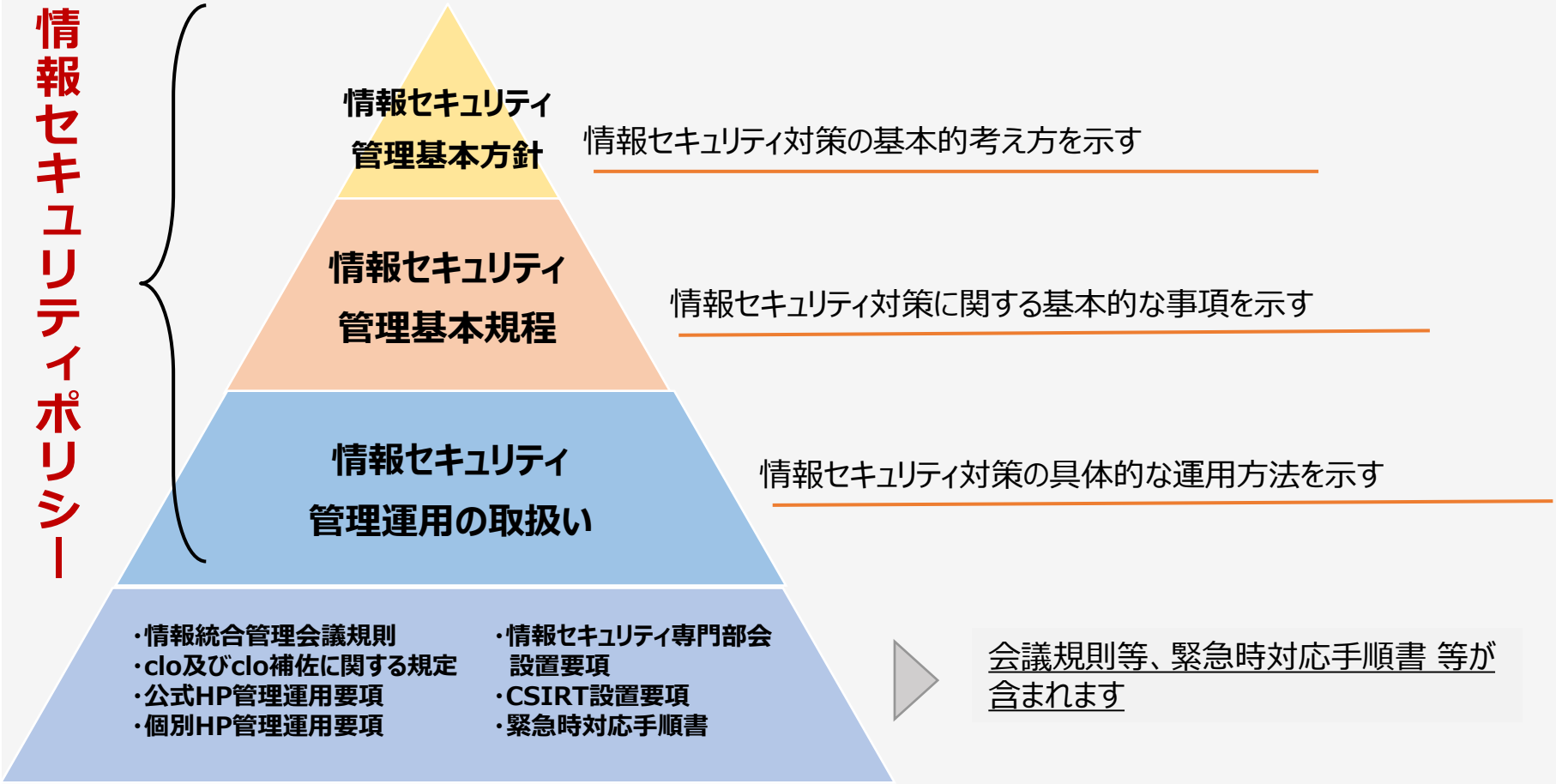
資料： 独立行政法人情報処理推進機構 セキュリティセンター 「情報セキュリティ10大脅威 2023」（ https://www.ipa.go.jp/security/vuln/10threats2023.html）

※ 独立行政法人情報処理推進機構（IPA）では、情報セキュリティ対策の普及を目的として2006年から、前年に発生した情報セキュリティ事故や攻撃の状況等から脅威を選出し、上位10位を公表している。
上記の「情報セキュリティ10大脅威2023」は、IPAが選出した脅威候補を元に、情報セキュリティ分野の研究者、企業の実務担当者など約150名のメンバーで構成する「10大脅威選考会」の投票を経て決定した。

2．情報セキュリティポリシーとは
情報セキュリティポリシーの定義

■ 情報セキュリティポリシーの定義

情報セキュリティ関係規定体系は図の通りとなります。



2．情報セキュリティポリシーとは
情報セキュリティポリシーの適応範囲

■ 情報セキュリティポリシーの適用対象

管理・運用の業務に携わる者
(情報の管理者)

本学の情報資産を利用する者
(情報の利用者)

情報セキュリティ管理運用の取扱い（ 第1章 総則 ）

２．情報セキュリティポリシーとは
情報セキュリティポリシーの適応範囲

情報の管理者及び利用者は次に掲げる事項が禁止されます。

（１）情報資産の目的外利用

（２）守秘義務に違反する情報の開示

（３）組織責任者の許可なく通信回線上を送受信される通信内容を監視し、
又は通信回線装置及びサーバ装置の利用記録を採取する行為

（４）組織責任者の要請に基づかずにセキュリティ上の脆弱性を検知する行為

（５）法令又は学内規則に違反する情報の発信

（６）管理者権限を濫用する行為

（７）上記の行為を助長する行為

情報セキュリティ管理運用の取扱い（ 第5章 5-3 ）

3．情報セキュリティポリシーの遵守事項
情報セキュリティにおける格付けの定義

■機密性についての格付けの定義

格付けの区分	区分の基準	具体例
機密性3情報	本学で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成23 年４月１日内閣総理大臣決定）に定める秘密文書に相当する機密性を要する情報を含む情報	（・全学的に影響のある情報） ・学生の成績 ・学位記 ・役職員及び学生の個人番号及び特定個人情報 ・学生の健康情報（ドック、健康診断の結果等） 等
機密性2B情報	本学で取り扱う機密性３以外の情報のうち、独立行政法人の保有する情報の公開に関する法律（平成13 年12 月５日法律第140 号。以下、「独立行政法人等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、その漏えいにより本学の情報資産を利用する者のうち、学内外を含む多数の者の権利が侵害され、又は本学の活動の遂行に支障を及ぼすおそれがある情報	・学生及び教職員名簿 ・非公開の研究情報 ・営業秘密やそれに係る技術情報 ・人事、給与、共済組合関係記録情報 ・本学のネットワーク、情報システムの構成等に関する情報 等
機密性2A情報	本学で取り扱う機密性３以外の情報のうち、独立行政法人等情報公開法第５条各号における不開示情報に該当すると判断される蓋然性が高い情報を含む情報であって、その漏えいにより本学の情報資産を利用する者のうち、特に学内の役職員等や学生の権利が侵害され、又は役職員等の活動の遂行に支障を及ぼすおそれがある情報	・非公開の会議において知り得た情報 ・勉強会、研修会資料 ・財務会計システムにおいて発行可能な伝票等 ・公開前会議資料 等
機密性1情報	機密性３情報、機密性２B 情報又は機密性２A 情報以外の情報	・大学戦略課、総務課、入試課等から発表される報道機関向け情報 ・研究室等から一般に告知される情報 ・公式ホームページ掲載資料（機密性２A情報を除く） ・学生・保護者向け情報 等

3．情報セキュリティポリシーの遵守事項
情報セキュリティにおける格付けの定義

■完全性についての格付けの定義

格付けの区分	区分の基準	具体例
完全性2情報	本学で取扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、利用者の権利が侵害され又は本学活動の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報	・学生の成績 ・実施前の入学試験問題 ・人事・給与・共済組合関係記録情報
完全性1情報	完全性２情報以外の情報（書面を除く。）	・公式ホームページ掲載資料（入学試験情報等）

■可用性についての格付けの定義

格付けの区分	区分の基準	具体例
可用性2情報	本学で取扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、利用者の権利が侵害され又は本学活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。	・学生の成績 ・実施前の入学試験問題 ・人事・給与・共済組合関係記録情報
可用性1情報	可用性２情報以外の情報（書面を除く。）	・電子メール、グループウェア等の情報システム及び当該システムで取扱う情報

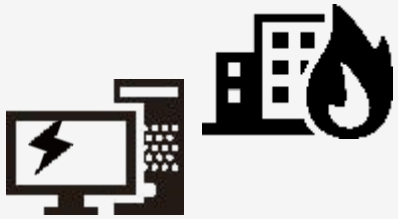
3．情報セキュリティポリシーの遵守事項
情報セキュリティインシデント（事件・事故）の定義

■ 情報セキュリティインシデント（事件・事故）の定義

ネットワーク系インシデント
（事件・事故）

- 大量のスパムメールの送信
- 不正プログラム等のマルウェアの蔓延や意図的な配布
- アクセス権限設定の不備等の管理上の過失による秘密情報(個人情報を含む)の漏えい
- データの消失又は改ざん

物理的インシデント
（事件・事故）



- 落雷を原因とする停電による通信回線の障害に伴う全学的な学内LAN・情報システムの停止
- 情報システムを構成する一部の通信回線装置の盗難を原因とする通信回線の滅失に伴う情報システムの機能不全

3．情報セキュリティポリシーの遵守事項
情報セキュリティインシデント（事件・事故）の定義

■ 情報セキュリティインシデント（事件・事故）の定義

盗難・紛失インシデント
（事件・事故）

- 学内LAN への侵入を許すようなアカウントを格納した端末の盗難・紛失
- 学生の要配慮情報等が記載された書類の紛失
- 未公表の研究情報の盗難
- 悪意のある内部者による窃盗

外部（クラウド）サービス
インシデント（事件・事故）

- アカウントハイジャック
- データ喪失・悪用・乱用
- 不正使用
- アクセス管理不備
- データの改ざん
- 情報漏えい
- データ滅失

情報セキュリティインシデントの定義について「運用管理の取扱い 第6章 第4節」に記載されておりますのでご確認ください。

3．情報セキュリティポリシーの遵守事項
情報セキュリティインシデント（事件・事故）の事例

■ 教育機関における情報セキュリティインシデント（事件・事故）の事例

メール誤送信

【放送大学】 令和５年4月
熊本学習センターにおいて、「入学生募集のご案内」メールについて、資料請求を行った218名の方に「Bcc」ではなく「To」（送信先メールアドレスが表示）で送信してしまう誤送信事例が発生。

外部記録媒体の紛失

【新潟大学】 令和5年3月
所属する教員が、同大学生や事業に関与した人物ら合計1,178名の個人情報を記録したUSBメモリを紛失。同大は令和4年4月20日に報告を受けていましたが公表していませんでした。

マルウェア感染

【埼玉大学】 令和４年6月
学務部で手元作業用のデータを保存するために使用していたNAS内の一部データがランサムウェア「Phobos」により暗号化された。また、ファイルを復号化するにはBitcoinを支払うように脅迫文が残っていた。

不正アクセス

【明治大学】 令和5年2月
運用・管理する教育研究システムが第三者による不正アクセスを受け、サーバーに保管されていたメールアドレス合計3万6,692件が外部に流出した可能性があると判明。

3．情報セキュリティポリシーの遵守事項
情報の格付け区分

■情報の格付け区分

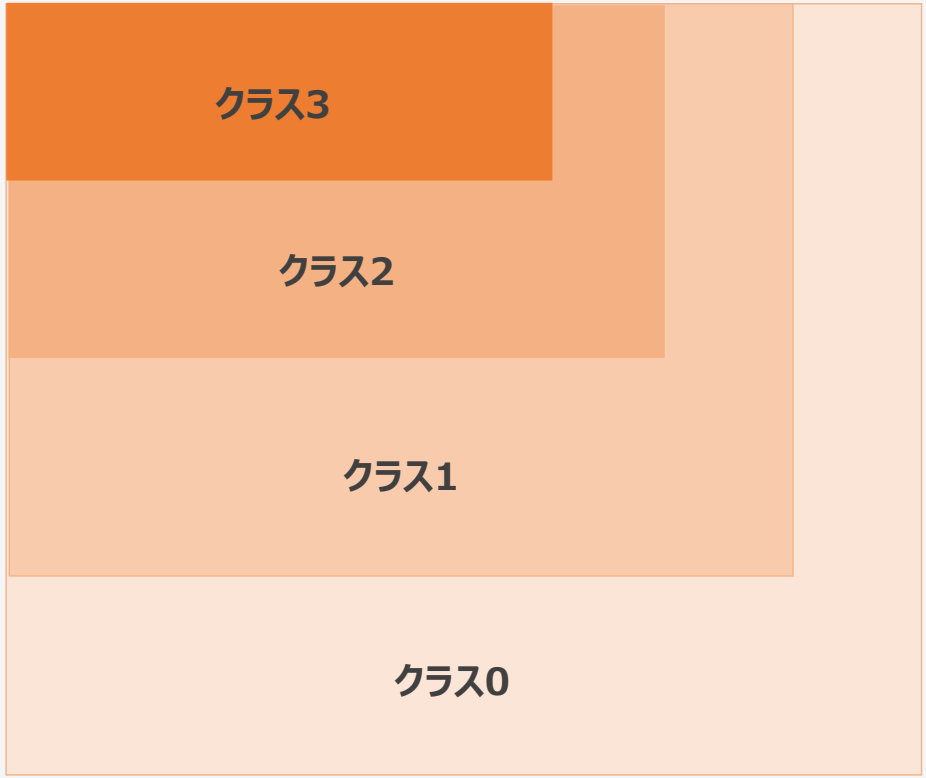
要保護情報

要機密情報	要保全情報	要安定情報
機密性３情報	完全性2情報	可用性2情報
機密性２B 情報		
機密性２A 情報		

3．情報セキュリティポリシーの遵守事項
情報を取扱う区域

■情報を取扱う区域

取扱う情報によってクラスが決められており、クラス3～1の区域を**要管理対策区域**と呼びます。
要管理対策区域では、物理的な対策と入退管理対策を実施する必要があります。



クラス3
- サーバ室
- 日常的に機密性が高い情報を取扱う研究室
- 事務室

クラス2
- 一般的な研究室
- 事務室や会議室

クラス1
- 教室、図書館

クラス0
- 受付、駐車場

3．情報セキュリティポリシーの遵守事項
情報を取扱う区域

■ 要管理対策区域における対策

物理的な対策

⇒許可されていない者が容易に立ち入ることができないようにするための対策
例．施錠可能な扉、間仕切り等の施設の整備、設備の設置等

入退管理対策

⇒許可されていない者の立入りを制限するため及び立入りを許可された者による
立入り時の不正な行為を防止するための対策
例．入室時における身分証明書等の提示、区域に立ちいるものの身元、訪問目的等の確認

3．情報セキュリティポリシーの遵守事項
情報の取扱制限

■情報の取扱制限

情報の取扱いに関する制限であって、複製禁止、持出禁止、配布禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを役職員等に確実に行わせるための手段をいう。

例．情報を保存・保管する場合

取扱方法	機密性3	機密性2B	機密性2A	機密性1	完全性2	完全性1	可用性2	可用性1
保存・保管期間の設定	○	○	△		○		○	
保存・保管場所の設定	○	○	△	△	○			
保存・保管場所の施錠	○	○	△		○			
電子ファイルの暗号化による保存・保管	○	△	△		○			

凡例　○:必ず行う　△:必要に応じて行う　空欄:行う必要はなし

３．情報セキュリティポリシーの遵守事項
情報の取扱い

情報は「格付け区分」及び「取扱い制限」に応じて取扱う必要があります。

（１）要保護情報を放置しない

（２）要機密情報を必要以上に複製しない

（３）電磁的記録媒体に要機密情報を保存する場合には、主体認証情報を用いて保護するか
又は情報を暗号化したり、施錠のできる書庫・保管庫に媒体を保存したりするなどの措置を講ずる

（４）電磁的記録媒体に要保全情報を保存する場合には、電子署名の付与を行うなど、
改ざん防止のための措置を講ずる

（５）情報の保存方法を変更する場合には、格付け、取扱制限及び記録媒体の特性に応じて
必要な措置を講ずる

３．情報セキュリティポリシーの遵守事項
情報の取扱い

■ 情報の取扱いにおける注意事項

（１）電磁的記録媒体に保存された情報が職務上不要となった場合は、
速やかに情報を消去すること。

（２）電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、
すべての情報を復元できないように抹消すること。

（３）要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。

（４）情報の格付けに応じて、適切な方法で情報のバックアップを実施すること。

（５）取得した情報のバックアップについて、格付け及び取扱制限に従って保存場所、
保存方法、保存期間等を定め、適切に管理すること。

3．情報セキュリティポリシーの遵守事項
端末の管理

■ 端末の管理

要保護情報を取扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策が必要です。

また、モバイル端末を除く端末について、**原則としてクラス2以上の要管理対策区域に設置する**必要があります。

端末の盗難及び不正な持ち出しを防止するための対策

⇒容易に切断できないセキュリティワイヤを用いて固定物又は搬出が困難な物体に固定する
利用者が施錠できる袖机やキャビネット等で保管する

第三者による不正操作及び表示用デバイスの盗み見を防止対策

⇒一定時間操作が無いと自動的にスクリーンロックするよう設定する
盗み見されるおそれがある場合にのぞき見防止フィルタを取り付ける

３．情報セキュリティポリシーの遵守事項
サーバ装置の管理

■ サーバ装置の管理

要保護情報を取扱うサーバ装置は**クラス2以上の要管理対策区域に設置する**必要があります。

また、要保護情報を取扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策が必要です。

無許可のアクセス等の不正な行為を監視するための対策を講じる必要があります。

（１）アクセスログ等を定期的に確認する

（２）IDS/IPS、WAF 等を設置する

（３）不正プログラム対策ソフトウェアを利用する

（４）ファイル完全性チェックツールを利用する

（５）CPU、メモリ、ディスクI/O 等のシステム状態を確認する

３．情報セキュリティポリシーの遵守事項
サーバ装置の管理

■ サーバ装置の管理

要安定情報を取扱うサーバ装置については、運用状態を復元するために対策を講じる必要があります。

（１）サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく

（２）定期的なバックアップを実施する

（３）サーバ装置を冗長構成にしている場合には、サービスを提供するサーバ装置を
代替サーバ装置に切り替える訓練を実施する

（４）バックアップとして取得した情報からサーバ装置の運用状態を復元するための訓練を実施する

3．情報セキュリティポリシーの遵守事項
情報セキュリティ体制

■ 情報セキュリティ体制

情報セキュリティインシデントに備えた体制の整備としてCSIRT（シーサート）※を整備することと定められています

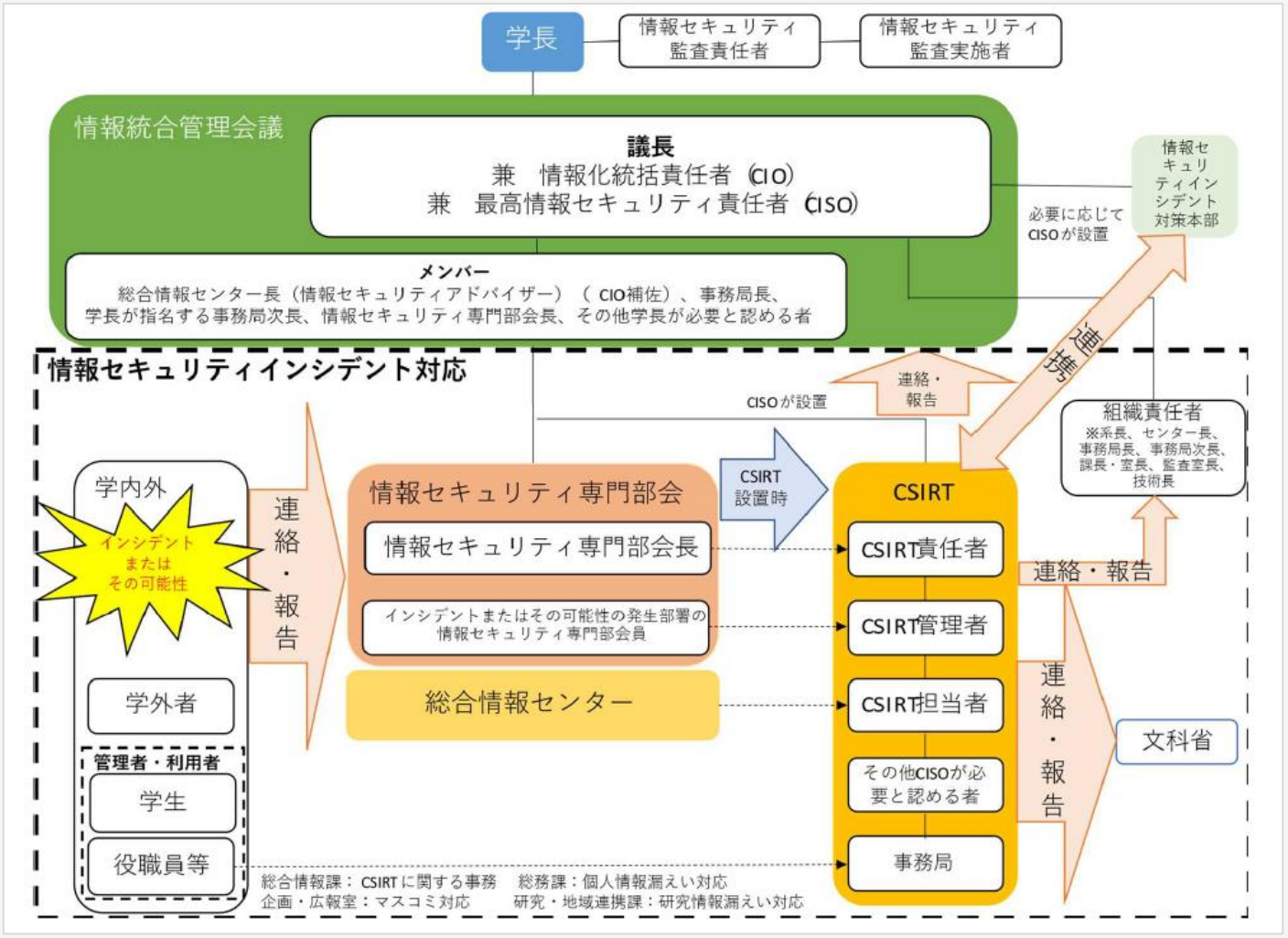
※CSIRTとは…セキュリティ上の問題としてインシデントが発生した際に対応するチーム、体制のこと

体制	情報セキュリティポリシー上の役割名
CSIRT責任者	情報セキュリティ専門部会長
CSIRT管理者	（インシデント発生部署の）情報セキュリティ専門部会員
CSIRT担当者	総合情報センター及びCSIRT管理者が指名する者
その他CISOが必要と認める者	本学システムの開発・保守・運用委託先・データセンター・IPA、JPCERT/CC等、必要に応じて協力・情報提供を要請
事務局	総合情報課、大学戦略課企画・広報室、総務課、産学連携・研究推進課

3．情報セキュリティポリシーの遵守事項
情報セキュリティ体制

■ 情報セキュリティ体制

CSIRTの体制は図の通りとなります。



４．情報セキュリティの対策
インシデント（事件・事故）に対する準備・予防

■ インシデント（事件・事故）に対する準備・予防等

連絡網の整備	各部署では、インシデント発生時の速やかな連絡、情報交換を行うとともに、緊急時の初動体制を円滑に行うために、事前に緊急時連絡網を整備しておく。
前提となる規定の確認	情報セキュリティポリシー、手順等及び危機管理対応マニュアルを確認し、内容を把握しておく。
セキュリティ情報の収集	情報セキュリティインシデントにはあたらない「ヒヤリハット」に関しても情報収集する。
検査・分析に必要な情報の保全	インシデント発生時の迅速な検査・分析に不可欠な情報※について状態を確認する。 ※システム構成図、ネットワーク構成図、ログ 等の情報
訓練・演習	必要に応じインシデントの発生を想定した訓練・演習を定期的に実施する。

万が一の事態に備えて日ごろから情報収集・準備しておくことが大切です。

４．情報セキュリティの対策
インシデント（事件・事故）に対する準備・予防

【インシデント（事件・事故）の例】

PC画面

- ウイルス対策ソフトから、ウイルス等が検出・駆除・隔離された旨のメッセージが表示される
- インターネット環境の特定のURLへ誘導するような画面展開がみられる

電子メール

- 電子メールが利用できない、又は利用できても何らかの異常を示すメッセージが表示されている
- 不審なメールが再三送られている。（このようなメールは開けない、開けても添付ファイルの開封やクリック等を行わない）

システム操作・運用

- 情報システムにアクセスできない、動作が非常に遅い
- 情報システムのログが記録できない、ログのバックアップができない
- 端末が正常に作動しない、又は自らの操作通りに画面展開しない
- ネットワーク機器、監視装置、セキュリティ製品等からアラートが発せられた

平常時においてインシデント（事件・事故）の予兆等の有無に注視し、検知、発見した場合は直ちに情報セキュリティ専門部会員に連絡すること

４．情報セキュリティの対策
機密性の高いファイルの取扱い

機密性が高い(機密性3、2B、2A)ファイルの取扱い対策

- パスワードを設定する（例．Word／Excelのパスワード機能を利用）
- パスワードを使い分ける
- 暗号化する
- 学外に持ち出さない

パスワードを設定する際は下記のことに注意してください。

パスワードは十分な長さと複雑さ（大文字･小文字･数字･記号を混合させる）を持たせ、パスワードの使い回しをしない･させない

管理するサーバやアカウントで使用するログインパスワードは、パスワードを知る担当者を限定する。特に管理者権限アカウントのパスワードは容易に推測できないものを設定しましょう！

４．情報セキュリティの対策
PCの取扱い／個々人の情報責任

PCの取扱い

- ログインパスワードを設定するとともに、部屋は施錠してから離れる
- 離席中に不正に操作されないように画面ロック設定を適用する
- ファイル交換ソフト※1は導入しない
- OSやプログラムは最新に保ち、不正プログラム対策のためにセキュリティソフトウェアを導入する

※1ファイル交換ソフトの例
Amoeba(アモエバ)、BitTorrent（ビットトレント）、Freenet（フリーネット）、Gnutella（グヌーテラ）、
Perfect Dark（パーフェクトダーク）、Share（シェア）、Winny（ウィニー）、WinMX（ウィンエムエックス） 等

離席時はPCやモバイル端末をロック。他人が操作できないようにしましょう！ ➡ クリアスクリーン

個々人の情報の管理責任

- 機密区分・有効期限の設定、適切なアクセス権限の設定並びに使用目的を明確にする
- 必要とする者にのみ当該情報へのアクセス権限を付与する
- 許可者のみ、正しい情報を、必要なときにいつまでも利用できるように維持管理する

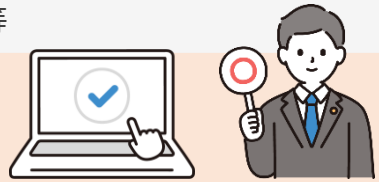
４．情報セキュリティの対策
不審なメールの取扱い

不審なメールの取扱い対策

- 添付ファイルを開く前、または実行する前に不審点を見つけること
- 送信者のメールアドレスが署名と異なっている
- 言い回しが不自然である
- 日本語では使用されない漢字（繁体字、簡体字）やカタカナが使用されている
- 正式名称を一部に含むような不審なURLまたはURIへのアクセスを指示するものである
- HTMLメールであり、表示と実際のURLまたはURIが異なるウェブリンクを使用している
- 署名の記載内容が不自然であり、存在しない部門の名称を使用している
- ショートカットファイル（.lnk、.pif、.url等）が添付されている
- 添付されたファイルが実行形式であるが、文書ファイルやフォルダのアイコンを使用している
- ファイル名が不審である
- 拡張子が二重に表示されている※2

※2ファイル拡張子の前に大量の空白文字が挿入されている
文字列が左右反転している
圧縮ファイルを実行せずにエクスプローラで表示すると、ファイル名が文字化けしている　等

添付ファイルを開く前に怪しい点がないか再確認しましょう！



４．情報セキュリティの対策
ソフトウェアの取扱い／コンピュータウイルス対策

端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定める、定期的に見直しを行う

- ソフトウェアベンダ等のサポート状況
- ソフトウェアと外部との通信の有無及び通信する場合はその通信内容
- インストール時に同時にインストールされる他のソフトウェア
- その他、ソフトウェアの利用に伴う情報セキュリティリスク

コンピュータウイルス対策

- ウイルス対策ソフトの設定を変更しない
- 外部から持ち込んだファイルは、必ずウイルス対策ソフトによる検査を実施する

外部から持ち込んだファイルを検査するだけでなく、

ウイルス対策ソフトによるパソコンの定期的なフルチェックを実施しましょう！

４．情報セキュリティの対策
コンピュータウイルス対策

コンピュータウイルス対策

対策をしていてもコンピュータウイルスに感染する可能性があります。
もしコンピュータウイルスに感染、又は感染の疑いがある場合は下記の対応を実施する。

- LANケーブルを抜き取り、ウイルスの蔓延を防止する
- 無線LANを利用している場合は、Wi-Fiを即時切断する
- 速やかに**情報セキュリティ専門部会**へ報告する
  （必ずパソコンの電源は落とさないこと！）

最後に

セキュリティインシデント（事件・事故）につながってしまった場合…

①業務の停止

②関係者への謝罪

③信用・信頼の失墜

④復旧にかかる膨大な費用

信頼を獲得するのには長い年月と努力を要しますが、**失うのは一瞬**です。

セキュリティ事故の防止に努めましょう。

ご清聴ありがとうございました