リスクアセスメント手法

改訂：2011 /1 /12

1. リスクアセスメント手法の基本的要求要件

リスクアセスメント手法は「ISMS 基本方針」に従ったものでなくてはならない。また，学術研究における大学内外での幅広い通信形態の要求観点から,可用性を強く制限するものであってはならない。同時に，「山口大学諸規則」，「日本国憲法」，「刑法」，「個人情報保護法」，「不正アクセス禁止法」，「不当競争防止法」，「著作権法」の遵守に対して特に注意を払うものでなければならない。

2. 受容リスク基準

2.1 受容リスク基準の定義

リスクは受容リスク基準 1，2 に基づいてセキュリティ計画による対応の必要性を評価する。

a)受容リスク基準 1（リスク値に基づく基準）

受容リスク基準 1 では **3.2～3.5** に述べる資産価値，脅威レベル値，脆弱レベル値，リスク値の算定式に基づく総合判断を行うものであり，リスク値を受容リスク基準値と比較することでセキュリティ計画の必要性の有無を決定する。受容リスク基準値は次のように定義する：

> 資産価値が 4 レベルの資産が，脅威レベルと脆弱レベルの積が 8 以下のリスク値に晒される場合，即ち**受容リスク基準値を 32** とする。

これに基づき，機密性，完全性，可用性の受容リスク基準値をそれぞれ次のように決定する:

> 機密性（C）の受容リスク基準値：32（32 以下を受容）
> 完全性（I）の受容リスク基準値：32（32 以下を受容）
> 可用性（A）の受容リスク基準値：24（24 以下を受容）

なお，『ISMS 基本方針』が機密性と可用性を重視し，更に可用性に特別に配慮することを謳っていることに鑑み，可用性については機密性，完全性の受容リスク基準値よりも約 30%増の基準を設定した。受容リスク基準値を超えるリスクについてはセキュリティ計画を実施しなくてはならない。

b)受容リスク基準 2（資産価値，脆弱レベルに基づく基準）

受容リスク基準 2 は脆弱性のあるリスクへの計画的な対応を確実にするためのものであり,次のように定義する:

> 資産価値のレベルが 2 以上で，かつ脆弱レベル 3 を持つリスクについては，セキュリティ計画を実施しなくてはならない。

2.2 セキュリティ計画

セキュリティ計画はリスク対応計画，事業継続計画，是正措置計画，予防措置計画の組み合わせによって構成される。ISMS 構築フェーズにおけるリスクアセスメントでは，リスク対応計画の立案を基本とするが，受容リスク基準 2 に基づいて対応が必要となったリスクについては，2.1 2)に述べた通り，適宜事業継続計画の立案，あるいは監視の仕組みの導入を構築フェーズにおいて検討する。また，運用フェーズでは，リスク値の変化に注意を払い，必要に応じて是正計画，予防計画によって適切なリスク対応を行う。リスク対応を行う際には、本学が契約している国立大学法人総合損害保険を考慮

する。

セキュリティ計画はCIOによる承認を得なくてはならない。また，セキュリティ計画を実施しない場合は，その理由を明確にしてCIOに報告し，受容の許可を得なければならない。

リスク対応計画は本文書の別紙にある様式に準じた形式で作成を行う。なお，計画の予算規模が小さく，かつ対応期間が短い場合には別途リスク対応計画を作成せず，「リスク対応一覧」に書き込む方法を採用しても良い。

2.3　リスク値テーブル

受容リスク基準値１、基準２に基づく非受容基準値の範囲は,機密性，完全性，可用性のそれぞれに対して次表のように色分けされる。ここで，桃色：基準１及び基準２，橙色：基準１のみ，及び黄色：基準２のみのリスク値である。

機密性（C）に関する受容リスク値：32以下

脅威		1				2				3				4			
脆弱性		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
資産価値	1	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
	2	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
	3	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
	4	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

完全性（I）に関するリスク受容リスク値：32以下

脅威		1				2				3				4			
脆弱性		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
資産価値	1	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
	2	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
	3	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
	4	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

可用性（A）に関するリスク受容リスク値：24以下

脅威		1				2				3				4			
脆弱性		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
資産価値	1	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
	2	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
	3	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
	4	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

3.　リスクアセスメント

3.1　資産の識別

ISMS適用範囲内の全ての情報資産の一覧を作成する。各資産又は資産グループ(次節3.2参照）は次の全ての情報が容易に識別可能な状態で記述されていること。

a)　資産（グループ）名

b)　管理者（その資産を実際に操作し，取り扱っている真の管理者）

c) 情報資産の形態
d) 保管形態・場所
e) 保管期限
f) 廃棄方法
g) 用途
h) 利用者の範囲
i) この資産に依存しているサービス
j) 実装済み適用管理策（機密性，完全性，可用性に係わる脅威別に記載されていること）
k) 個人情報の有無

なお、ISMS 適応範囲内の全ての情報資産の管理責任者は CIO 補佐であることから、情報資産一覧に管理責任者を記載しなくてもよい。

次の条件を満たす場合，資産のグルーピングを行ない，その資産グループに対して効率よく適切なリスクアセスメントを適用してよい。

a) 同じ運用目的の資産
b) 同じ管理策の適用が可能である資産
c) 機密性，完全性，可用性の価値が同じ資産
d) 脅威が同じ資産

リスクアセスメントの実施において,これらの条件を満足しないグリーピング資産が発見された場合，速やかに対象の資産のみを分離できる仕組みが備わっていること。
なお,メディア基盤センターがサービスを提供する上で一体として運用される資産について集約して一つの資産として扱ってもよい。
その場合は，資産の内訳を明らかにした上で，リスクアセスメント内容が一部にしか関係しない場合はそれを明記すること。

3.2 資産価値の評価

各資産の機密性，完全性，可用性のそれぞれに，喪失が業務やサービスに与える影響を，次の評価尺度に基づき資産価値１～４を評価する。

資産価値 機密性 C	１：機密性が損なわれても業務やサービスへの影響が小(例: 学内限定開示文書の学外秘情報の漏洩)
	２：機密性が損なわれると業務やサービスにかなり影響(例: サーバ配置図等の部局等限定開示文書の漏洩)
	３:機密性が損なわれるとメディア基盤センターに甚大な被害(例: 管理者パスワード等の秘密・極秘情報の漏洩)
	４：機密性が損なわれるとユーザや大学へ甚大な被害(例: 秘密・極秘情報の中でも，個人情報のような特に厳密な保護が要求される情報の漏洩)

資産価値 完全性	１：完全性が損なわれても業務やサービスへの影響が小(例: 特定センター内業務で利用される情報であって，不整合があっても担当者の判断で修正可能なもの)

I	２：完全性が損なわれると業務やサービスにかなり影響(例: センター内業務の一部で利用される情報の不整合)
	３：完全性が損なわれるとメディア基盤センターに甚大な被害(例: センター内業務で広範に利用する情報の不整合)
	４：完全性が損なわれるとユーザや大学へ甚大な被害(例: ユーザが参照する情報の不整合)

資産価値 可用性 A	１：可用性が損なわれても代替手段により業務やサービスは遂行可能で影響軽微
	２:可用性が損なわれると一部の業務やサービスが停止し一部のユーザに被害(例　:特定クラスの学生の履修へに影響，特定学部や特定部の職員の業務に影響)
	３：可用性が損なわれると広範な業務停止となり多くのユーザに被害(例: 複数クラスの学生の履修に影響，複数学部や複数部にまたがる職員の業務に影響)
	４:可用性が損なわれると業務やサービスが大規模に停止。ユーザへの被害甚大(例　:半数を超える学生の履修に影響，全学的な職員の業務に影響)

3.3　脅威レベルの評価

各資産に対する脅威を機密性，完全性，可用性のそれぞれに対して，次の評価尺度に基づき脅威レベル１～４を評価する。ここで，脅威レベルはその発生頻度の程度に基づく識別を行なう。

レベル	脅威の発生頻度の程度
1	数年に１回程度しか発生しない。
2	年に１回程度発生する。
3	年に数回程度発生する。
4	月に１回程度発生する。

なお，メディア基盤センターが担う業務とサービス及びその役割の観点から，次の大項目で脅威が識別されていること，及びこれらの関連性が容易に識別できること。

a)　領域環境
b)　悪意攻撃
c)　管理運用
d)　故障障害
e)　法不適合

3.4　脆弱性レベルの評価

各資産が有する機密性，完全性，可用性のそれぞれの脅威への脆弱性を，次の評価尺度に基づき脆弱性レベル１～４を評価する。ここで，脆弱性レベルは脅威に利用できる可能性のあるシステム上の欠陥や仕様上の問題点のレベルに基づき行なわれる。

レベル	脆弱性の程度
1	脅威が発生してもほぼ完全に防御できる。(適切な管理策が講じられていて、きわめて安全である。)
2	脅威が発生してもほとんど防御できる。(適切な管理策が講じられていて安全であるが、改善の余地も考慮する)
3	脅威が発生してもある程度防御できる。(何らかの管理策はあるが、改善の余地がある。)
4	脅威が発生するとほとんど防御できない。(想定される脅威に対して、管理策が講じられていない。)

なお，識別される脆弱性の項目は，全て**3.3 脅威レベルの評価**で識別された各脅威項目との関連性が容易に識別可能な状態で記述されていなければならない。

3.5　リスク値の算定

各資産が有する機密性，完全性，可用性のそれぞれの脅威について，次式により全てのリスク値を算定する:

（リスク値）＝（資産価値）×（脅威レベル）×（脆弱性レベル）

算定したリスク値を**2.受容リスク基準値**に照らし合わせて，受容又はリスク対応が必要であるかを判断する。受容不要な場合は，**3.6 リスク対応計画**を行う。

3.6　リスク対応計画

受容基準値を超える全てのリスクに対しての対応を，低減，受容，回避，移転の中から選択し，リスク対応のための管理目的及び管理策を選択する。選択した管理策を実装し，管理運用するために「リスク対応一覧」を作成し，また，特に詳細な計画が必要とされるリスクについては，「リスク対応計画」を作成する。「リスク対応計画」の書式は添付の通りである。(ただし必要項目が網羅されていれば詳細の書式は適宜担当者が変更を行っても良い。)これらのリスク対応が適切に実施されるよう，本リスク対応の PDCA サイクルを確実に運用する。

4.　リスクアセスメント手法の実装

本リスクアセスメントは，リスクアセスメント表(図)を作成して行う。

5.　脅威・脆弱性の例

典型的な脅威や脆弱性については，別途マインドマップにてサンプルを提示する。

⇒ 脅威と脆弱性のサンプルを記載したマインドマップ

別紙

リスク対応計画書(承認日:　　，承認者:　　)

名　称	D		優先度：
立案者		立案日	
資産番号		対策目的	
資産名		導入コスト	円
管理者		維持コスト	0 円
脅　威			
脆弱性			

リスク	資産価値	脅威	脆弱性	リスク値	残留予定リスク
現在値					
目標値					

現状の問題点		
具体的対策		
管理策		有効性の測定(%)
管理策有効性測定方法		開始前：　0
		目標値：　100
		達成率：
備　考		

実施予定スケジュール	担当者	実施予定期間 4 月～3 月	完了日
立案・計画 調達・構築 動作確認・是正処置の完了確認			

大学情報機構メディア基盤センター】

セキュリティ事象・弱点報告書

No.	日時	所属・氏名・連絡先	内容・対応等
	／　　： 窓口・電話・メール	学生・教員・職員・その他 （　　　　　　）	内容 事象発生日時　2010年4月20日(月)　xxxx の Bot感染が報告された
	種別	対応者	対応策（結果）
	問合・○障害・連絡 事象・弱点	○○	TSC，CCC でクリーニングをしたが特には報告がされなかったが，netstat によると Microsoft-ds:syn による学外への通信行為が見られた事と，再起動時に update service が停止させられていることからレジストリ書き換えを含むウィルス感染が認められると判断し，OS の再インストール，サービスパックの適用，およびセキュリティパッチの適用を行っ
	／　　： 窓口・電話・メール	学生・教員・職員・その他 （　　　　　　）	内容 事象発生日時　　／　　：　　場所（　　　　　　）
	種別	対応者	対応策（結果）
	問合・障害・連絡 事象・弱点		
	／　　： 窓口・電話・メール	学生・教員・職員・その他 （　　　　　　）	内容 事象発生日時　　／　　：　　場所（　　　　　　）
	種別	対応者	対応策（結果）
	問合・障害・連絡 事象・弱点		
	／　　： 窓口・電話・メール	学生・教員・職員・その他 （　　　　　　）	内容 事象発生日時　　／　　：　　場所（　　　　　　）
	種別	対応者	対応策（結果）
	問合・障害・連絡 事象・弱点		

是正・予防措置細則

改訂：2011/ 1/12

1. 目的

大学情報機構メディア基盤センター(以下「センター」という。)の業務の範囲で発生する様々な事故,事件などの不適合及び不適合となる可能性のある状態を適切に取り扱うため,この細則を定める。

2. 是正措置と予防措置

2.1 是正措置

是正措置は，次の場合に実施するものとする。

a) 事故，事件が発生し，センター及び山口大学の一部又は全体に対して，重要な情報資産の改竄，消失又は流出，又はサービス停止に至るような重大な事故，事件が生じたとき。
b) 法律，学内規則及びセンター内の細則，内規，要項，手順書に規定した要求事項を満たしていない要素を発見したとき。
c) 法律，学内規則などが変更され，センター内の細則，内規，要項，手順書がそれに合致しなくなったとき。
d) 内部監査又は第三者の審査により，不適合又は要是正と指摘を受けたとき。
e) メディア基盤センター専門委員会をはじめとする学内委員会にて，センターに関わる是正措置の決議がなされたとき。
f) マネジメントレビューにより是正措置が指示されたとき。

2.2 予防措置

予防措置は，次の場合に実施するものとする。

a) 2.1 是正措置で定める是正措置を必要とする状態になる可能性が高いとき。
b) 新しいセキュリティホールが発見され，それがセンターの持つ設備に影響を与えるとき。
c) 事故，事件の是正措置の後，再発防止策を必要とするとき。
d) メディア基盤センター専門委員会をはじめとする学内委員会にて，センターに関わる予防措置の決議がなされたとき。
e) マネジメントレビューにより予防措置が指示されたとき。

3. 事故，事件の通知義務

ISMS スタッフは，事故，事件を発見した場合，「国立大学法人山口大学情報セキュリティ緊急時対応基準」に従い，直ちに管理者（以下，プロジェクト制の場合，プロジェクトリーダのことを管理者という。必要に応じて，プロジェクトリーダの役割をプロジェクトメンバーに委譲できるものとする。）に報告しなければならない。管理者は，報告された事故,事件が誤報でないかどうかを確認し，事故，事件であるかどうかを判別することとする。事故，事件の発見は，次の通報・通知などによるものとする。

a) 学外の第三者からの通報
b) 学内者からの通報
c) ISMS スタッフによる具体的事実に基づく異常の発見
d) 不正アクセス検知システムから送られる自動通知
e) 利用率，ディスク容量，負荷などの各サーバ，ネットワーク装置からの自動通知
f) ログ調査による異常の発見

4. 重大な事故，事件の基準

事故，事件が重大であるかどうかの判別は，原則として，「国立大学法人山口大学情報セキュリティ緊急時対応基準」に従い，次の基準とする。

a) センター内で取り扱う法律によって定められた個人情報を含むファイルの流出，改竄，消失
b) 山口大学吉田キャンパス，常盤キャンパス，小串キャンパスのいずれかの全域において，業務時間内で 4 時間以上のネットワークサービス停止が見込まれるとき，又はそのような状態が発生したとき。
c) 業務時間内で 4 時間以上にわたる認証サービスの停止，業務時間内で 8 時間以上にわたるメールサービスの停止，24 時間以上にわたるファイルサービスの停止
d) 1 週間以上にわたる演習室利用サービスの停止が見込まれるとき，又はそのような状態が発生したとき。

5. 事故，事件の取扱手順

管理者は事件，事故について次の通り取扱うものとする。

a) 事故，事件を学内に通知する必要がある場合， Web ページなど的確な手段を用いて速やかに通知する。
b) 緊急を要する場合，状況がそれ以上悪化しないようにするための暫定措置を実施することができる。
c) 事件,事故が重大である場合,真の原因を特定しそれを取り除くため,ISMS 是正措置計画(ISMS 予防措置計画)を作成して，是正措置(予防措置)に努めるものとする。計画書は，任意形式又は是正措置計画書(様式 1)(予防措置計画書(様式 2))に従うこと。
d) 是正措置計画(予防措置計画)を CIO 補佐に報告する。
e) CIO 補佐から実施確認が得られれば，是正措置(予防措置)を実施することができる。
f) 是正措置方法(予防措置方法)を検討するため,臨時 ISMS スタッフ会議の開催を CIO 補佐に依頼することができる。
g) 是正措置(予防措置)に必要な手順をまとめ，ISMS スタッフに必要な措置を依頼することができる。
h) 是正措置(予防措置)は，メールなど的確な手段を利用して実施する。
i) 是正措置及び予防措置の経過を ISMS スタッフ会議で報告し，必要であれば計画を変更する。
j) 是正措置(予防措置)終了後，有効性の達成率など必要事項を記入の上，CIO 補佐に報告する。

大学情報機構メディア基盤センター

（様式１）

ISMS 是正措置計画書

名　称			優先度：
発見者		発見日	20　．　．
起票者		起票日	20　．　．
実施確認者		実施確認日	20　．　．
発見の方法			
発見者の連絡先			
不適合の状況 （リスクの識別（完全・機密・可用）を記入すること。）			
不適合に至る 真の原因			
暫定措置			

管理策		有効性の測定(%)
管理策 有効性 測定方法		開始前：
		目標値：
		達成率：
予算コスト		
残留リスク 備　考		

実施予定スケジュール	担当者	実施予定期間　　月～　月	完了日
			20　．　．　．

大学情報機構メディア基盤センター

（様式２）

ISMS 予防措置計画書

名　称			優先度：
発見者		発見日	20　．　．
起票者		起票日	20　．　．
実施確認者		実施確認日	20　．　．
発見の方法			
発見者の連絡先			
不適合となる可能性のある状況（リスクの識別（完全・機密・可用）を記入すること。）			
不適合に至る真の原因			
暫定措置			

管理策		有効性の測定(%)
管理策 有効性 測定方法		開始前：
		目標値：
		達成率：
予算コスト		
残留リスク 備　考		

実施予定スケジュール	担当者	実施予定期間　　月～　月	完了日
			200　．　．　．