中央大学通信教育部学生会横浜支部

情報セキュリティ対策基準

（目的）

第１条　この基準は、中央大学通信教育部学生会横浜支部（以下、「当支部」とします。）における情報セキュリティ基本方針に基づき、人的、技術的、物理的な情報セキュリティ対策方式を定めると共に、個別の情報セキュリティ対策実施手順における標準を定めることを目的とします。

（適用範囲）

第２条　この基準は、当支部の活動を通じて収集する情報全般（個人情報を含みます。）及び当該情報が流通する情報システム（以下、「情報資産」とします。）並びにその運用に従事する者（以下、「運用担当者」とします。）に対し、当支部の統制が及ぶ限りにおいて、適用するものとします。

（改定）

第３条　この基準は、施行の状況及び当支部内外の環境の変化について検討を加え、その結果に基づき適切な見直しを行い、計画、実施、評価及び是正のマネジメントサイクルを確実に運用し、以て実効性を高めることを目的として、毎年度１回以上の改定を行うものとします。

（運用担当者）

第４条　運用担当者は、理事又は参事であって、当支部の活動を通じて収集する情報を用いて中央大学通信教育部学生会横浜支部規約（以下、「当支部の規約」とします。）に違反する行為をしない者であることを理事及び情報企画担当役員が全員一致により認める者でなければなりません。

２　運用担当者は、情報セキュリティ基本方針、及びこの基準の内容を正しく把握し、個別の情報セキュリティ対策実施手順を確実に遵守するため、教育又は訓練を定期的に受けるものとします。

３　運用担当者は、当支部の活動を通じて収集される情報を、正当な理由なく、第三者が存在する空間において公言し、又は第三者が参照できる状態としてはなりません。

４　運用担当者は、他の運用担当者との間で当支部の活動を通じて収集される情報を受け渡しするときは、これまでに実績のあるメールアドレス又は電話番号宛に行わなければなりません。

５　情報企画担当役員及び事務局長は、運用担当者が退任するとき、又はその他特に必要と認めたときは、当該運用担当者に対し、一定の作為又は不作為を求めることができるものとします。

６　情報企画担当役員及び事務局長は、事故及びインシデントへの対処、又は予防のために必要な範囲内において、運用担当者に対し、調査を行い、事情の説明を求めることができるものとします。

（パーソナルコンピュータ）

第５条　運用担当者は、自らが使用するパーソナルコンピュータ（以下、「PC」とします）を当支部の活動の用に供するときは、次の各号に掲げる基準を遵守しなければなりません。

(1).　法令上及びライセンス契約上、完全に使用を許諾されたソフトウェアのみを使用すること。

(2).　パーソナルファイアウォールの機能を導入し、原則として常時有効化すること。

(3).　アンチウィルスソフトウェアを導入し、原則として常時有効化すること。

(4). アンチスパイウェアを導入し、原則として常時有効化すること。
(5). 前各号のソフトウェアには、定義ファイルを含む更新プログラムを適時に適用すること。
(6). 運用担当者の不在時には、施錠により保護される安全な場所に設置するよう努めること。
(7). オペレーティングシステムへのログオン等は、適切な認証を経る方式とすること。
(8). ハードディスクドライブは、暗号化又は起動パスワードにより保護するよう努めること。
(9). 適切なアクセス制御を行い、利用状況が監査証跡により把握できるよう努めること。
(10). P2P ファイル共有ソフトウェアは、理由の如何に関わらず使用しないこと。
(11). 当支部の活動を通じて得た情報は、適時にバックアップを取得し、適切に管理すること。
(12). 当支部の活動を通じて得た情報は、退任時又は PC の処分時には、完全に消去すること。
(13). 当支部の活動上の機密情報を含む PC の運搬時は、酒類を摂取しないよう努めること。
(14). 当支部の活動上の機密情報を含む PC の消失時は、直ちに理事会へ報告すること。

2 運用担当者は、前項各号に掲げる基準を満たさない PC であっても、情報企画担当役員の承認を得た上で、自らの責任において、当支部の活動の用に供することができるものとします。

3 携帯端末については、本条各項の規定を準用するものとします。

（パスワード）

第 6 条 運用担当者は、情報資産においてパスワードを設定するときは、次の各号に掲げる事項を遵守しなければなりません。

(1). 正当な理由なく他人（権限を有しない他の運用担当者を含みます。）と共有しないこと。
(2). 少なくとも英字及び数字を組み合わせた 6 文字以上のものとすること。
(3). 容易に推測されるものではないこと。
(4). 過去 2 年以内に使用した履歴を有するものではないこと。
(5). 外部に漏洩した疑いがあるときは、直ちに変更すること。
(6). 運用担当者の変更があったときは、速やかに変更すること。
(7). 運用担当者の変更がないときでも、少なくとも 180 日ごとに変更するよう努めること。
(8). 媒体の如何に関わらず、他人が直接的に認識できる態様で保持しないこと。

2 運用担当者は、情報資産におけるパスワードを連携するときは、当該情報資産又はその伝送の用に供したものとは異なる伝送手段を用いなければなりません。

（電子メール）

第 7 条 運用担当者は、自らの責任において、当支部の活動に係る一切の電子メールを送受信するものとします。当支部は、運用担当者が送受信した電子メールについて一切の責任を負いません。

2 運用担当者は、電子メールを送信するときは、相手先メールアドレスについて慎重に確認すると共に、To・Cc・Bcc の別及び不適切な文字が混入していないことを十分に確認するものとします。

3 運用担当者は、支部員、聴講生、学習会講師その他一切のステークホルダに対して、当支部の活動上知り得た情報を利用して、私的な電子メールを自ら送信してはなりません。

4 運用担当者は、当支部の活動上必要な電子メールを役員以外に送信するときは、同時に、Cc 又は Bcc により、理事会又は任意の他の役員へ写しを送信しなければなりません。但し、ハラスメントの相談及びメンタリングに係る電子メールを送信するときは、この限りではありません。

5 運用担当者は、電子メールアドレスにおいて、理事会における事前の承諾なく、当支部を代表

するかのような外観を作出してはなりません。

6　運用担当者は、当支部のドメイン名を含む電子メールアドレスを用いて、当支部の活動上必要でない電子メールを送信してはなりません。

（公式サイト）

第8条　情報企画担当役員は、運用責任者として運用担当者を監督すると共に、その協力の下、自らの責任において、当支部の活動に係る公式サイトの企画、構築、運用及び保守を行うものとします。

2　情報企画担当役員は、公式サイトの企画、構築、運用及び保守を行う上で、中央大学通信教育部所定のガイドライン等を遵守するほか、著作権、産業財産権その他の知的財産権、プライバシー権、肖像権、名誉権その他の人格権等を侵害しないようにしなければなりません。

3　情報企画担当役員は、公式サイトを開設するインターネットサーバにおいて、パスワードその他の情報セキュリティに係る設定値として、既定値を使用してはなりません。

4　情報企画担当役員は、公式サイトの情報を更新したときは、直ちに理事会へその旨を報告するものとします。但し、定常的に行われる情報の更新については、この限りではありません。

（機密情報の保護）

第9条　運用担当者は、当支部の活動を通じて収集される情報の内、有用性、秘密管理性及び非公知性を有するものは、すべて機密情報として保護しなければなりません。

2　個人情報は、公開を前提として収集されるもの及び事務局長又は情報企画担当役員が指定するものを除き、すべて機密情報と見做します。

3　機密情報は、Need to Know の原則に基づき、正当な理由に基づき当該機密情報を必要とする運用担当者のみが、必要最小限の範囲内においてのみ、アクセスすることができるものとします。

4　運用担当者は、次の各号に掲げるときは、自らの責任において、情報企画担当役員が指定する方法により、情報を暗号化しなければなりません。

(1).　機密情報を電子メールで送信するとき。

(2).　機密情報を第5条第1項各号に掲げる基準を満たさない PC へ保存するとき。

(3).　機密情報を情報企画担当役員が指定していないインターネット上のサービスへ保存するとき。

(4).　機密情報を可搬性のある記録媒体へ保存するとき。

5　運用担当者は、暗号化された機密情報を当支部の活動の用に供する PC に保存したときは、自らの責任において、情報企画担当役員が指定する方法により、当該データを復号化するものとします。

6　運用担当者は、複数件（個人情報にあっては複数名分）の機密情報を物理的な媒体に格納して伝送するときは、当該媒体の特性に応じて厳重に梱包した上で、一般書留若しくは簡易書留の扱いとした郵便又はセキュリティサービスを適用した「ゆうパック」により送付しなければなりません。

7　運用担当者は、機密情報を印刷するときは、自らが所有権を有する印刷装置であって、第三者が技術的又は物理的な管理に関与していないものを利用しなければなりません。印刷した機密情報は、印刷装置から速やかに取り除き、自己の責任において適正に管理しなければなりません。

8　運用担当者は、機密情報をファクシミリにより伝送するときは、予め電話により相手先に伝送の内容及び枚数を通知した上で待機を要請し、自己のセンシティブな個人情報の伝送におけるのと同一の注意義務を以て送信し、事後に電話により相手先に伝送の完了の確認を行わなければなりません。

（個人情報の保護）

第 10 条 運用担当者は、当支部の活動を通じて個人情報を収集するときは、予め利用目的を特定し、被収集者にこれを通知し、その同意を得て、適正な手段により取得するものとします。

2　運用担当者は、被収集者の承諾を得ることなく、被収集者に通知した利用目的を逸脱若しくはその範囲を超えた個人情報の利用を行い、又は被収集者の個人情報を第三者に開示若しくは提供してはなりません。但し、当支部の規約に基づく場合、裁判官の発する令状に基づく場合、又は人の身体的な安全を確保するために必要であって緊急かつやむを得ない場合は、この限りではありません。

3　運用担当者は、利用目的の達成に必要な範囲内において個人情報を正確かつ最新の内容に保つと共に、個人情報の保存における安全管理のために必要かつ適切な措置を講じるものとします。

4　運用担当者は、原則として、センシティブな個人情報を保存してはなりません。

5　運用担当者は、被収集者から当該被収集者本人の個人情報の開示、訂正、削除及び利用停止に係る依頼又は苦情を受け付けたときは、学生証、運転免許証その他の本人確認書類、又は電磁的方法により本人確認を行った上で、本人に不利益を与えることのないよう措置を講じるものとします。

6　事務局長は、個人情報管理責任者として運用担当者を監督し、その範囲内において一定の作為又は不作為を求める指導、勧告、助言その他の措置を講じることができるものとします。

（情報の廃棄）

第 11 条 運用担当者は、当支部の活動を通じて収集した情報を廃棄するときは、物理的媒体においては裁断、溶解又は破砕の方法、その他の媒体においては情報企画担当役員が指定する方法により、確実に廃棄又は消去を行い、事後の復元が不可能となるようにしなければなりません。

（事故及びインシデントへの対処）

第 12 条 運用担当者は、情報セキュリティ事故が発生したとき、若しくは情報セキュリティ事故に至り得る事象（以下、「インシデント等」とします）が発生したとき、又はその可能性があるときは、自己の判断により対処を行わず、直ちに理事会へ報告しなければなりません。

2　理事会は、インシデント等が発生したとき、又はその可能性があるときは、情報企画担当役員を中心として、あらゆるステークホルダに対する当該インシデント等に起因する影響及び損害を最小限に抑え、当支部の継続性を確保することを目的として、適切な対処を直ちに行うものとします。

（罰則）

第 13 条 理事会は、この基準に違反した運用担当者に対し、当支部の規約又は別途規定する罰則基準に基づき、その議決により、厳正な処分を行うものとします。

【附則】

第 1 条　この基準は、改定の日から適用します。

平成 23 年 1 月 7 日　制定
平成 24 年 1 月 9 日　改定
平成 25 年 2 月 1 日　改定