一般社団法人オープン CAE 学会

情報セキュリティガイドライン

目　次

（Ver.1.0）

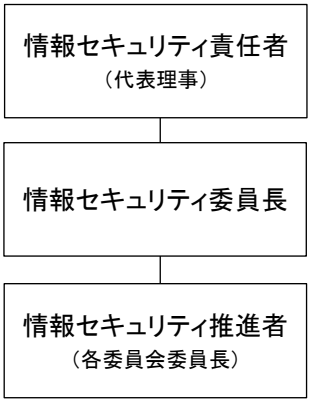
1	組織的対策	改訂日	2022/12/10
適用範囲	理事、事務局		

1.情報セキュリティのための組織

情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の委員構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

情報セキュリティ委員　役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報セキュリティ委員長	情報セキュリティ対策のための管理を行う。 情報セキュリティ対策を推進するために理事、委員会委員および事務局への教育を企画・実施する。 事故の影響を判断し、対応案を立案し、情報セキュリティ責任者に提案する。 情報セキュリティ対策が適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し、助言を行う。
情報セキュリティ推進者 （各委員会委員長）	各委員会における情報セキュリティの運用管理責任者。各委員会における情報セキュリティ対策を実施する。

＜情報セキュリティ委員会体制図＞



2.情報セキュリティ取組みの監査・点検/点検

情報セキュリティ委員長は、情報セキュリティ関連規程の実施状況について、6 月に点検を行い、監査・点検/点検結果を情報セキュリティ委員会に報告する。情報セキュリティ委員会は、報告に基づき、以下の点を考慮し、必要に応じて改善計画を立案する。

- 情報セキュリティ関連規程が有効に実施されていない場合は、その原因の特定と改善を実施する。
- 情報セキュリティ関連規程に定められたルールが、新たな脅威に対する対策として有効でない場合は、情報セキュリティ関連規程の改訂を実施する。
- 情報セキュリティ関連規程に定められたルールが、関連法令の情報セキュリティに対する要求を満たしていない場合は、情報セキュリティ関連規程の改訂を実施する。

3.情報セキュリティに関する情報共有

情報セキュリティ責任者および委員は、新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関する情報を専門機関等から適時に入手し、委員会で共有する。

＜専門機関＞

➢独立行政法人情報処理推進機構（略称：IPA）

[情報セキュリティ]

https://www.ipa.go.jp/security/

[ここからセキュリティ]

https://www.ipa.go.jp/security/kokokara/

➢JVN（Japan Vulnerability Notes）

https://jvn.jp/index.html

➢一般社団法人 JPCERT コーディネーションセンター（略称：JPCERT/CC）

https://www.jpcert.or.jp/

➢個人情報保護委員会

http://www.ppc.go.jp/

2	人的対策	改訂日	―
適用範囲	全関係者（理事、委員会委員および事務局）		

1. 理事、委員会委員および事務局の責務

理事、委員会委員および事務局は、以下を順守する。

- 理事、委員会委員および事務局は、本学会が情報資産として管理する情報及びその複製物の一切を、許可されていない組織ならびに人に提供してはならない。
- 理事、委員会委員および事務局は、本学会の情報セキュリティ方針及び関連規程を遵守する。違反時の懲戒については、定款に準じる。

2.情報セキュリティ教育

情報セキュリティ委員会は、以下の点を考慮し、情報セキュリティに関する教育計画を年度単位で立案する。

- 対象者：理事、委員会委員および事務局
- テーマは以下とする。
  - 情報セキュリティ関連規程の説明（就任時）
  - 最新の脅威に対する注意喚起（随時）
  - 関連法令の理解（関連法令の施行時）
  - 個人情報の取り扱いに関する留意事項

3	情報資産管理	改訂日	2022/12/10
適用範囲	理事、委員会委員および事務局		

1.情報資産の管理

1.1 情報資産の特定と機密性の評価

本学会事業に必要で価値がある情報及び個人情報（以下「情報資産」という）を特定し、機密性は、以下の基準に従って評価する。

機密性 2：極秘	●法律で安全管理が義務付けられている ●守秘義務の対象として指定されている ●限定提供データ（一定の条件を満たす特定の外部者に提供することを目的とする情報）として指定されている ●漏えいすると取引先や顧客に大きな影響がある 例：学会員の個人情報、外注先発注内容など
機密性 1：対外秘	漏えいすると事業に大きな影響がある情報 例：学会外部に未公開の情報など
機密性 0：公開	漏えいしても事業に影響はない 例：学会ホームページ、ニュースレターなどで学会外部に公開する情報など

1.2 情報資産の管理責任者

情報資産の取り扱い関する情報セキュリティの運用管理責任者は、情報セキュリティ責任者とする。

ただし、委員会にて契約したサービス等については、当該情報資産を利用する委員会委員長とする。

1.3 情報資産の利用者

極秘、対外秘の情報資産の利用者の範囲は、理事、委員会委員および事務局とする。

2.情報資産の対外持ち出し

情報資産を対外に持ち出す場合には、以下を実施する。

- 対外秘の場合は情報セキュリティ委員会の許可を得る。
- 極秘の場合は代表理事の許可を得る。

3. 外国にある第三者への個人データの提供

外国にある第三者への個人データの提供時に、提供先の第三者における個人情報の取扱いについて本人への情報提供を実施することとする。

4. 違法な行為を営むことが疑われる事業者について

違法な行為を営むことが疑われる事業者について、違法又は不当な行為を助長するおそれが想定される場合は、個人情報を提供すること等、不適正な方法により個人情報を利用することを禁じる。

5. 個人関連情報の第三者提供の制限

個人関連情報の第三者提供の制限として、本学会では個人データに該当しないものの、提供先において個人データとなることが想定される情報の第三者提供について、本人同意を得ることとする。

個人関連情報には、端末識別子を通じて収集されたサイト閲覧履歴や、商品購買履歴、位置情報等が該当する。特定の個人を識別できる個人情報は、個人関連情報には当たらないものとする。

4	アクセス制御及び認証	改訂日	2022/12/10
適用範囲	情報資産の利用者及び情報処理施設		

1.アクセス制御方針

対外秘又は極秘の情報資産を扱う情報システム又はサービスに対するアクセス制御は以下の方針に基づいて運用する。

- 利用者の業務・職務に応じた必要最低限のアクセス権を付与する。
- 利用終了が終了した場合は速やかにアクセス権限を削除する。

2.利用者の認証

対外秘又は極秘の情報資産を扱う情報システムは以下の方針に基づいて利用者の認証を行う。

- 利用者の認証に用いるアカウントは、利用者 1 名につき 1 つを発行する。
- 複数の利用者が共有するアカウントの発行を禁止する。
- 例外的に一つのアカウントを複数の利用者で利用する必要がある場合は、情報セキュリティ委員会に報告する。

3.利用者アカウントの登録

利用者の認証に用いるアカウントは、代表理事又は情報セキュリティ責任者の承認に基づき登録する。

4.利用者アカウントの管理

利用者の認証に用いるアカウントが不要になった場合、情報セキュリティ委員は、当該アカウントの削除又は無効化を、当該アカウントが不要になる日の翌日までに実施する。

5.パスワードの設定

利用者の認証に用いるパスワードは、以下に注意して設定する。

- 十分な強度のあるパスワードを用いる。
- 他者に知られないようにする。

6.理事、委員会委員および事務局以外の者に対する利用者アカウントの発行

本学会の理事、委員会委員および事務局以外の者にアカウントを発行する場合は、代表理事又は情報セキュリティ責任者の承認を得る。

5	Ｉ Ｔ機器利用	改訂日	2022/12/10
適用範囲	業務で利用する情報機器		

1.ソフトウェアの利用

1.1 ウイルス対策ソフトウェアの利用

1.1.1 ウイルス検知

理事、委員会委員および事務局は、以下の方法でウイルス検知を行う。

- ネットワーク経由で入手するファイルは、自動検知機能を有効にしてウイルス検知を実施する。
- 電子媒体を用いてファイルの受け渡しを行う場合は、媒体内のファイルにウイルス検知を実施する。

1.1.2 ウイルス対策ソフト定義ファイルの更新

理事、委員会委員および事務局は、パソコン・スマートフォン・タブレットに導入したウイルス対策ソフトウェアの定義ファイルを随時更新する。

1.2 ウイルス対策の啓発

情報セキュリティ委員は、適宜ウイルスに関する情報を収集し、重大な被害を与えるウイルスに対しては、対応策及び対応に必要な修正プログラムを学会内に公開及び通知する。理事、委員会委員および事務局は、感染防止策が通知された場合は、速やかに実施完了すること。

2. Ｉ Ｔ機器の利用

理事、委員会委員および事務局は、業務に利用するパソコン・タブレット・スマートフォンには、ログインパスワードを設定する。利用するときには以下を実行する。

- ログインパスワードを他者の目に触れる所に書き記さない。
- 屋外で利用する場合は、他者が画面を盗み見可能な環境で利用しない。

3.インターネットの利用

理事、委員会委員および事務局は、インターネットを利用する際には以下を遵守する。

3.1 ウェブ閲覧

情報セキュリティ委員は、ウイルス等の悪意のあるソフトウェアに感染するおそれがあると認められる有害ウェブサイトは学会内周知/ウェブフィルタリングソフトを使用して、理事、委

員会委員および事務局の閲覧を制限する。理事、委員会委員および事務局は、業務でウェブ閲覧を行う場合は以下に注意する。

- 公序良俗に反するサイトへのアクセスを禁止する。
- 不審なサイトへのアクセス及び学会用メールアドレス登録を禁止する。
- 業務上、個人情報(メールアドレス、氏名、所属等)を入力する場合は、通信の暗号化、接続先の実在性等を十分に確認したうえで行う。
- 信頼できるサイトから署名付きのモバイルコードをダウンロードする場合を除き、モバイルコード(クライアントパソコン側で動作するプログラム)を実行しない。

3.2 オンラインサービス

理事、委員会委員および事務局は、インターネットで提供されているサービスを情報資産の運用を伴う業務で利用する場合は、情報セキュリティ委員長の許可を得る。利用する際には以下に注意する。

＜オンラインストレージ＞

- 対外秘又は極秘の情報資産を保存する場合は、情報セキュリティ委員長の許可を得る。
- メールアドレスの登録が必要な場合は学会用メールアドレスを登録する。
- セキュリティポリシーを公表していないサービスの利用は禁止する。
- 不審なベンダーが提供しているサービスの利用を禁止する。

3.3 SNS の個人利用

- 本学会の情報資産に関わる書き込みは行わない。ただし、機密性が公開レベルの情報で学会活動の PR に使う場合は除く。
- 本学会外の人と SNS 上で私的に交流する場合、双方の立場をわきまえ、社会人として良識の範囲で交流する。
- SNS 用のアプリケーションが提供するセキュリティ設定を行い、アカウントの乗っ取りやなりすましに注意する。
- 使用するパソコン、スマートフォン、タブレット上のデータ、写真、位置情報が、予期せず公開される可能性のあることに注意する。

3.4 電子メールの利用

理事、委員会委員および事務局は、業務で電子メールを利用する際には以下を実施する。

＜誤送信防止＞

- 送信前にあて先を確認してから送付する。

＜メールアドレス漏えい防止＞

- 同報メール（外部の多数相手に同時に送信するとき）を送信する場合は、宛先（TO）に自分自身のアドレスを入力し、BCC で複数相手のアドレスを指定する。

＜傍受による漏えい防止＞

- 対外秘又は極秘の情報資産を送信する場合は、メール本文ではなく添付ファイルに記載し、ファイルを暗号化して送信する。

＜添付ファイル暗号化の方法＞

- パスワード保護の設定又はパスワード付きの ZIP ファイルにする。パスワードは先方と別の連絡方法で知らせるなど、パスワードが傍受されないよう配慮する。

＜禁止事項＞

- 業務に支障をきたすおそれがある使用。

3.5 ウイルス感染の防止

標的型攻撃メール等によるウイルス感染を防止するため、以下の内容に複数合致する場合は十分に注意し、添付ファイルを開く、又はリンクを参照するなどしない。受信した場合は、情報セキュリティ委員に報告し、情報セキュリティ委員は情報セキュリティ委員会に報告する。報告を受けた情報セキュリティ委員会は学会内に注意を促す。

6	ＩＴ基盤運用管理	改訂日	―
適用範囲	サーバー・ネットワーク及び周辺機器		

1.管理体制

情報セキュリティ委員は、ＩＴ基盤の運用に当たり情報セキュリティ対策を考慮し製品又はサービスを選択する。ＩＴ基盤の情報セキュリティ対策及び関連仕様は、情報セキュリティ責任者が承認する。IT 基盤は運用を担当する情報システム管理者を設置することができ、情報システム管理者は本ガイドラインに従って運用する。

2.ＩＴ基盤の情報セキュリティ対策

ＩＴ基盤の運用の際には以下の技術的情報セキュリティ対策を考慮すること。

2.1 サーバー機器の情報セキュリティ要件

ＩＴ基盤で利用するサーバー機器・サービスに求める情報セキュリティ要件は、情報セキュリティ委員が決定する。新規にサーバー機器・サービスを導入する場合は、情報セキュリティ要件を満たす製品を選択し、情報セキュリティ委員長の許可を得て導入する。

2.2 ネットワーク機器の情報セキュリティ要件

ＩＴ基盤で利用するネットワーク機器・サービスに求める情報セキュリティ要件は、情報セキュリティ委員が決定する。新規にネットワーク機器・サービスを導入する場合は、情報セキュリティ要件を満たす製品を選択し、情報セキュリティ委員長の許可を得て導入する。

3.ＩＴ基盤の運用

情報システム管理者は、ＩＴ基盤の運用を行う際には以下を実施すること。

- 情報システム管理者は、機器の管理画面にログインするためのパスワードは初期状態のまま使わず、推測不可能なパスワードを設定して運用する。
- 情報システム管理者は、通信ログについて以下の確認を定期的に行う。
  - 管理外のインターネット接続がないか
  - 許可なく接続された機器や無線 LAN 機器はないか
  - 不審な通信が行われていないか
- 遠隔診断ポートの利用は、保守サポートなど必要な場合のみに限定し、認証機能やコールバック機能等を備えるなど、適切なセキュリティ対策を施す。

4.クラウドサービスの導入

ＩＴ基盤の一部としてクラウドサービス等の外部サービスを導入する場合は、情報セキュリティ委員がサービスプロバイダの情報セキュリティ対策をあらかじめ評価したうえで選定する。新規クラウドサービス等の外部サービスを導入する場合は、情報セキュリティ委員長の許可を得て導入する。

5.脅威や攻撃に関する情報の収集

情報セキュリティ委員は、最新の脅威や攻撃に関する情報収集を行い、必要に応じて学会内で共有する。

6.ＩＴ基盤標準

6.1 クラウドサービス情報セキュリティ対策評価基準

- サービスプロバイダが公表する情報セキュリティ又は個人情報保護への取組方針が、処理しようとする情報資産の重要度に照らして適切であること。
- サービス仕様に含まれる情報セキュリティ対策が、処理しようとする情報資産の重要度に照らして適切であること。

7	情報セキュリティインシデント対応 ならびに事業継続管理	改訂日	―
適用範囲	情報資産及び保有する個人データに関わるインシデント		

1.対応体制

情報セキュリティインシデントが発生した場合には、以下の体制で対応する。

最高責任者	代表理事
対応責任者	情報セキュリティ委員長
一次対応者	発見者又は情報システム推進者

2.情報セキュリティインシデントの影響範囲と対応者

情報セキュリティインシデントが発生した場合、以下を参考に影響範囲を判断して対応する。

事故レベル	影響範囲	責任者
3	●会員、イベント・サービス利用書等に影響が及ぶとき ●個人情報が漏えいしたとき	代表理事
2	事業に影響が及ぶとき	対応責任者
1	理事、委員会委員および事務局の業務遂行に影響が及ぶとき	対応責任者
0	インシデントにまでは至らないが、将来においてインシデントが発生する可能性がある事象が発見されたとき	対応責任者

3.インシデントの連絡及び報告

レベル 1 以上のインシデントが発生した場合、責任者に速やかに報告し、指示を仰ぐ。

4.対応手順

インシデントを以下のとおりに区分し、それぞれの対応手順を示す。

区分	事件・事故の状況
漏えい・流出	対外秘又は極秘情報資産の盗難、流出、紛失
改ざん・消失・破壊 サービス停止	情報資産の意図しない改ざん、消失、破壊 情報資産が必要なときに利用できない
ウイルス感染	悪意のあるソフトウェアに感染

4.1 漏えい・流出発生時の対応

事故レベル	対応手順
3	①発見者は即座に対応責任者及び代表理事に報告する。 ②対応責任者は個人情報漏えいまたはその恐れがある場合には速報として本人および個人情報保護委員会に 3 日以内に報告を行う。 ③対応責任者は原因を特定するとともに、二次被害が想定される場合には防止策を実行する。 ④対応責任者は問い合わせ対応を準備する。 ⑤代表理事は学会内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。 ⑥対応責任者は個人情報漏えいまたはその恐れがある場合には確報を本人および個人情報保護委員会に 30 日以内に報告を行う。
2	①発見者は発見次第、情報セキュリティ委員に報告する。 ②情報セキュリティ委員は漏えい先を調査し、対応責任者に報告する。 ③情報セキュリティ委員は学会内関係者に周知する。
1	※情報漏えい・流出は全て事故レベル 2 以上

4.2 改ざん・消失・破壊・サービス停止発生時の対応

事故レベル	対応手順
3	①発見者は即座に対応責任者及び代表理事に報告する。 ②情報セキュリティ委員ならびに情報システム管理者は原因を特定し、応急処置を実行する。 ③対応責任者は学会内に周知する。 ④電子データの場合は情報セキュリティ委員ならびに情報システム管理者がバックアップによる復旧を実行する。 ⑤機器の場合は情報セキュリティ委員ならびに情報システム管理者が修理、復旧、交換等の手続きを行う。 ⑥書類･フィルム原本の場合は情報セキュリティ推進者が可能な範囲で修復する。 ⑦情報セキュリティ委員は原因対策を実施する。 代表理事は学会内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。
2	①発見者は発見次第、情報セキュリティ委員に報告する。 ②情報セキュリティ委員ならびに情報システム管理者は原因を特定し、応急処置を実行する。 ③対応責任者は学会内に周知するとともに情報システム管理者に連絡する。 ④電子データの場合は情報セキュリティ委員ならびに情報システム管理者がバックアップによる復旧を実行する。 ⑤機器の場合は情報セキュリティ委員ならびに情報システム管理者が修理、復旧、交換等の手続きを行う。 ⑥書類･フィルム原本の場合は情報セキュリティ推進者が可能な範囲で修復する。 ⑦情報セキュリティ委員は原因対策を実施する。
1	①発見者は発見次第､情報セキュリティ委員ならびに情報システム管

	理者に報告する。 ②情報セキュリティ委員ならびに情報システム管理者は原因を特定し、応急処置を実行する。 ③電子データの場合は情報セキュリティ委員ならびに情報システム管理者がバックアップによる復旧もしくは再作成・入手を実行する。 ④機器の場合は情報セキュリティ委員ならびに情報システム管理者が修理、復旧、交換等の手続きを行う。 ⑤書類・フィルム等の原本の場合は情報セキュリティ推進者が可能な範囲で修復する ⑥情報セキュリティ委員は原因対策を実施する
0	発見者は発見次第、発生可能性のあるインシデントと想定される被害を情報セキュリティ委員に報告する。

4.3 ウイルス感染時の初期対応

理事、委員会委員および事務局は、業務に利用しているパソコン、サーバー又はスマートフォン、タブレット（以下「コンピュータ」といいます。）がウイルスに感染した場合には、以下を実行する。

①ネットワークからコンピュータを切断する。
②情報セキュリティ委員に連絡する。
③ウイルス対策ソフトの定義ファイルを最新版に更新する。
④ウイルス対策ソフトを実行しウイルス名を確認する。
⑤ウイルス対策ソフトで駆除可能な場合は駆除する。
⑥駆除後再度ウイルス対策ソフトでスキャンし、駆除を確認する。
⑦情報セキュリティ委員に報告する。

以下の場合など理事、委員会委員および事務局自身で対応できないと判断される場合は情報セキュリティ委員に問い合わせる。

- ●ウイルス対策ソフトで駆除できない。
- ●システムファイルが破壊・改ざんされている。
- ●ファイルが改ざん・暗号化・削除されている。

4.5 届出及び相談

情報セキュリティ委員は、インシデント対応後に以下の機関への届け出、報告又は相談を検討する。

＜届出・相談・報告先＞

【独立行政法人 情報処理推進機構セキュリティセンター(IPA/ISEC)】

- ウイルスの届出

https://www.ipa.go.jp/security/outline/todokede-j.html
TEL: 03-5978-7518
E-mail : virus@ipa.go.jp

- 不正アクセスに関する届出

E-mail : crack@ipa.go.jp
FAX : 03-5978-7518

- 情報セキュリティ安心相談窓口

https://www.ipa.go.jp/security/anshin/index.html
TEL:03-5978-7509
E-mail : anshin@ipa.go.jp

【個人情報保護委員会】

- 個人データの漏えい等の事案が発生した場合等の対応

①要配慮個人情報の漏えい等
②財産的被害の恐れがある漏えい等
③不正の目的による恐れがある漏えい等
④1000 件を超える漏えい等
※①～③については件数によらず報告義務がある。
漏えい等事案が発覚した場合は、速やかに下記 URL を参照して個人情報保護委員会等に対し、報告すること
https://www.ppc.go.jp/personalinfo/legal/leakAction/

4.6 個人情報の利用停止・消去の請求について

漏えい等事案が発生した際に本学会が保有する個人情報について本人から開示請求・ならびに利用停止、消去の請求があった場合は本人要求に従って対応する。

また、６か月以内に消去するデータについて、開示請求の対象となる。個人データを提供・受領した際の記録も開示請求の対象となる。

開示方法については、本人の指示に従う。

5.情報セキュリティインシデントによる事業中断と事業継続管理

代表理事は、情報セキュリティインシデントの影響により本学会事業が中断した場合に備え、以下を定める。

5.1 想定される情報セキュリティインシデント

以下のインシデントによる事業の中断を想定する。

- 情報セキュリティインシデント : 大型地震の発生に伴う設備の倒壊、回線の途絶、停電等によるシステム停止

- 想定理由 : 本学会の事業は、商品の販売から請求回収までの業務をシステムに依存しているため、停止した場合は事業の継続が困難になり多大な損失が発生

5.2 事業継続計画

対応責任者は、想定する情報セキュリティインシデントが発生し、事業が中断した際の復旧責任者の役割認識及び関係者連絡先について、有効に機能するか検証する。復旧責任者は、被害対象に応じて復旧から事業再開までの計画を立案する。