DM2-05-063

別紙１：雛形

障害等対応手順書　雛形

2006 年 5 月

内閣官房情報セキュリティセンター

本書の位置付け

本書は、「障害等対処手順書」を策定する場合の雛形であり、「障害等対処手順書策定手引書」の２に示す実施手順に記載すべき事項を、同３に示す文書構成例の枠組みの中に記載したものである。

本書の利用方法

本書において想定する前提

雛形は、以下を前提として記述している。そのため、前提と異なる場合には、適宜、修正、追加又は削除する必要がある。

- 雛形は、統括情報セキュリティ責任者が府省庁の実施手順を整備するために利用することを想定している。
- 雛形を利用して整備した実施手順は、すべての行政事務従事者に適用されるものとなる。
- 統括情報セキュリティ責任者による障害等に備えた緊急連絡網が整備されており、当該連絡網において、障害等の対処を行う際に想定される関係者が網羅されていること。
- 府省庁において事業継続計画（BCP : Business Continuity Plan）がある場合には、本書を実施するにあたって必要となる具体的な対処手順（事案発生時の具体的な対処手順、あらかじめ定められていない対処方策を決定するにあたって必要となる調整先及びその権限者など）は、BCP 等と整合した内容として定められていること。

手直しポイント

政府機関統一基準に基づき策定された省庁基準に準拠した「障害等対処手順書」を策定する手順には、大別して、新規で策定するものと既存の文書を修正するものがあるが、そのどちらの場合でも以下の事項を踏まえて策定する必要がある。

(1) 役割分担については、組織によって様々であるため、各府省庁の実施手順では、自組織の構成や各担当者の責務を考慮した上で、追記又は変更を検討する。

(2) 雛形中に、*[・・・]* 形式で明記される部分（様式名、府省庁名、担当者等）については、各府省庁内の定めに合わせる。

(3) 既存の情報セキュリティ関係規程との整合性を考慮し、適切な分割、統合、相互参照を検討する。

改訂履歴

改訂日	改訂理由
2006/5/22	初版
2006/6/21	各府省庁からの意見に基づく修正
2006/11/22	各府省庁からの意見に基づく修正

目次

1　本書の目的

障害等（故障、インシデント等を含む。）が発生した場合、適切な対応により障害等の影響が拡大することを防ぐと共に復旧を図ることが必要である。このとき対応を誤ると無用な被害の拡大を招くことが懸念されるため、障害等の発見から対処にいたる手続きを定め、障害等に適切な対処を実施することが必要である。

本書では、障害等が発生した場合の手続き及び手続きに利用する様式を定め、もって*［○○省］*において必要とされる障害等への対処を適切に実施することを目的とする。

2　本書の対象者

本書は、すべての行政事務従事者を対象としている。

3　承認権限者

(1) 対処承認権限者（障害等に対する対処方針の適否を審査等する者）は、情報システムセキュリティ責任者又は課室情報セキュリティ責任者とする。ただし、障害等の内容に応じて必要がある場合は、その上位者を対処承認権限者とする。

(2) 再発防止策承認権限者（障害等の再発防止策の適否を審査等する者）は、情報セキュリティ責任者とする。

4　障害等発生時の対応

4.1　障害等発生時における全般的な注意事項

(1) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、緊急の対処が必要な障害等が発生した場合において、対処の遅延を防止し、これを円滑に実施するため、情報システム、組織等の状況を勘案し事前に詳細な手順を定め、これを関係者に周知すること。

(2) 行政事務従事者は、緊急の対処が必要な障害等が発生した場合において、報告、審査等の手続が遅延することにより、必要な対処の実施が遅れることのないようにすること。

(3) 緊急の対処が必要な場合は、報告書に代わって口頭での報告、審査等を先行することや、発見者に代わって報告受理者が報告書を記入し障害等の発見者から内容確認を得ること等により、遅滞なく障害等に対する対処を実施する。ただし、このような場合であっても、速やかに報告書を作成して記録を残すこと。

- 緊急の対処が必要な障害等の例
  - 不正プログラムに感染
  - 電子計算機への不正アクセスによるデータの改ざん
  - 安全区域への不正侵入等による電子計算機の不正利用
  - 可用性2情報を扱う情報システムの停止
  - 機密性3情報の漏えい

【事業継続計画（BCP：Business Continuity Plan）が策定されている場合】

(4) 行政事務従事者は、BCP と情報セキュリティ関係規程が定める要求事項において事前に想定されていない不整合が生じた場合、その旨を情報システムセキュリティ責任者又は課室情報セキュリティ責任者を通じて情報セキュリティ責任者に報告し、指示を得ること。

4.2 障害等の発見

(1) 行政事務従事者は、障害等を発見した場合は、障害等の内容に応じて情報システムセキュリティ責任者又は課室情報セキュリティ責任者に、*「障害等の発生に関する報告・申請書（様式○○）」*により報告を行うこと。

- 情報システムセキュリティ責任者に報告する障害等の例
  - サービス不能攻撃（DoS攻撃）による情報システムの停止
  - サーバへの不正アクセスの痕跡の発見
  - 不正プログラム等の感染による情報流出
- 課室情報セキュリティ責任者に報告する障害等の例
  - 機密性2情報を保存した外部記録媒体の紛失・盗難
  - 不正プログラム等の感染による情報流出

(2) 行政事務従事者は、障害等を発見した場合であって、被害の拡大が懸念されるときは、速やかに応急措置を実施し被害拡大の防止に努めること。

- 応急措置の例
  - 不正プログラムへの感染のおそれがある端末をネットワークから切り離す（LANケーブルを端末から抜く）

(3) 障害等の報告を受けた情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、対処を実施する者を選び、対処の指示を与えること。なお、口頭により報告を受けた場合は、*「障害等の発生に関する報告・申請書（様式○○）」*の障害等の詳細についても記録すること。

(4) 障害等の報告を受けた情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、報告された内容を確認し、必要に応じて情報セキュリティ責任者及び関係部署等に通知すること。また、通知先を *「障害等の発生に関する報告・申請書（様式○○）」*に記録すること。

(5) *[障害等の報告を受けた情報システムセキュリティ責任者、課室情報セキュリティ責任者又は広報担当者]*は、危機管理、国民の意識向上に資するものについて、情報セキュリティ対策上支障のない範囲で広報に努めること。

4.3 障害等の対処

(1) 障害等の対処を実施する者は、対処方針を決定し *「障害等の発生に関する報告・申請書（様式○○）」*により対処承認権限者の承認を得ること。ただし、情報システムセキュリティ責任者又は課室情報セキュリティ責任者が定めた詳細な手順において、対処方針が規定されている場合には、承認を受けたものとみなす。なお、対処方針を決定する際には、必要に応じて通知先の関係部署と連携すること。

(2) 障害等の対処を実施する者は、障害等が発生する前の状態に復旧するだけでは障害等が再発するおそれがあると思料する場合には、*「障害等の再発防止策に関する報告・申請書（様式△△）」*も速やかに承認を受けること。

(3) 障害等の対処を実施する者は、承認を得た対処方針に従い障害等の対処を実施すること。なお、対処を実施する際には、必要に応じて通知先の関係部署と連携すること。

(4) 障害等の対処を実施する者は、対処の実施結果について*「障害等の発生に関する報告・申請書（様式○○）」*により対処承認権限者に報告し、確認を求めること。

(5) 障害等の対処を実施する者は、実施結果について確認を得た*「障害等の発生に関する報告・申請書（様式○○）*」の提出をもって、障害等の対処結果について障害等の発生を報告した情報システムセキュリティ責任者又は課室情報セキュリティ責任者に報告すること。

4.4 障害等の対処及び再発防止の承認

(1) 障害等の対処を実施する者から対処方針の承認を求められた対処承認権限者は、対処方針を審査し、適切な対処が実施されると思われる場合には承認を与え、その旨を*「障害等の発生に関する報告・申請書（様式○○）」*に記録すること。ただし、申請の内容に応じて必要がある場合は、上位の対処承認権限者に回付する。

(2) 障害等の対処結果について確認を求められた対処承認権限者は、障害等の対処結果について点検し、適切な対処が実施された結果と思われる場合には、確認した旨を*「障害等の発生に関する報告・申請書（様式○○）」*に記録すること。

(3) 障害等の対処結果について報告を受けた情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、*「障害等の発生に関する報告・申請書（様式○○）」*を保管すること。

(4) 再発防止策の申請を受けた対処承認権限者及び再発防止策承認権限者は、再発防止策を審査し、適切な再発防止が実施されると思われる場合には承認を与え、その旨を*「障害等の再発防止に関する報告・申請書（様式△△）」*に記録すること。ただし、申請の内容に応じて必要がある場合は、上位の対処承認権限者に回付する。

(5) 再発防止策について承認を与えた再発防止策承認権限者（情報セキュリティ責任者）は、*「障害等の再発防止策に関する報告・申請書（様式△△）」*の提出をもって、再発防止策について最高情報セキュリティ責任者に報告すること。

(6) 最高情報セキュリティ責任者は、再発防止策について、自らが実施する事項がある場合は、それを実施すること。

(7) 最高情報セキュリティ責任者は、報告を受けた*「障害等の再発防止策に関する報告・申請書（様式△△）」*を保管すること。

【参考】障害等対応の処理フロー