危機管理マニュアル（情報漏洩に関する対応マニュアル）

第１　対応の原則

①　発見・報告（別紙１参照）

・情報漏えいに関する兆候や具体的な事実を確認した場合は、事務局総務部に報告し速やかに情報漏えい対応のための体制をとる。

・不正アクセスや不正プログラムなど情報システムからの情報漏えいの可能性がある場合は、不用意な操作をせず、システム上に残された証拠が消えないようにする。

・外部から通報があった場合は、相手の氏名・連絡先等を必ず控えるようにする。

②　初動対応

・総務部は当面の対応方針を決定し、情報漏えいによる被害の拡大、二次被害の防止のために必要な応急処置を行う。

・情報が外部からアクセスできる状態にあったり、被害が広がる可能性がある場合には、情報の隔離、ネットワークの遮断、サービスの停止などの外部からのアクセスを遮断する措置をとる。

③　調査（別紙２参照）

・適切な対応についての判断を行うために５Ｗ１Ｈ（いつ、どこで、誰が、 何を、なぜ、どうしたのか）の観点で 調査し情報を整理する。また、事実関係を裏付ける情報や証拠を確保する。

④　通知・報告・公表等

・総務部は、漏洩した個人情報の本人、取引先 などへの通知、スポーツ庁、警察、 IPA などへの届出、ホームページ、 マスコミ等による公表を検討する。

・漏洩した個人情報の本人については特別な理由がない限り通知を行う。

・紛失・盗難のほか不正アクセス、内部犯行、脅迫等不正な金銭の要求など犯罪性がある場合は警察へ届出る。

・すべての関係者への個別通知が困難な場合や、 広く一般に漏えい情報による影響が及ぶと考えられる場合などは、ホームページでの情報公開や記者発表による公表を行う。ただし、 情報の公表が被害の拡大を招く恐れがある時は、公表の時期、対象などを考慮する。

⑤　抑制措置と復旧

・総務部は、情報漏洩によって発生した被害の拡大の防止と復旧のための措置を行う。

・被害の規模が大きい場合には、専用の相談窓口を設置し、被害が発生した場合にはその動向を素早く察知し対応するようにする。また、再発防止に向けた具体的な取り組みを行い、停止したサービス、アカウント等を復旧する。

⑥　事後対応

・総務部は、抜本的な再発防止策を検討し実施する。

・総務部は、調査報告書を理事及び監事に提示した上で事件の概要及び再発防止策等について報告を行う。

・理事及び監事は、被害者に対する損害の補償等について検討し、必要な措置を行う。また、内部職員の責任を追及する必要がある場合には、必要な処分手続きを行う。

第２　紛失・盗難

１　事故事例

・パソコンやＵＳＢメモリ等を電車や飲食店等に置き忘れた。
・パソコンやＵＳＢメモリ等が入ったカバンを盗まれた。
・置き引きや車上荒らしや事務所荒らしに遭い、パソコンやＵＳＢメモリ等を盗まれた。

２　①発見及び報告

・情報を紛失し又は盗難された者並びに情報の紛失・盗難を発見した者は、直ちに事務局総務部に報告を行い、別紙１の「情報漏洩報告シート」に当該紛失・盗難の内容を記入する。

３　②初動対応

・総務部は、情報漏洩報告シートの内容等を基に、紛失し又は盗難にあった（以下「紛失等」という。）情報の種類・内容、情報が記録された媒体を特定する。
・電車内や飲食店等に情報が記録された媒体を置き忘れた場合や当該媒体を紛失等した場合、総務部は、直ちに警察や鉄道会社等に当該媒体を紛失したことを届け出、紛失物の捜索・回収を依頼する。
・紛失等した媒体内に、特定の web ページや秘密情報等にログインするためのＩＤやパスワード等の情報が含まれている場合、総務部は、直ちに当該ＩＤやパスワードを変更するなど、被害の拡大を防止する。

４　③調査

・総務部は、情報漏洩報告シートその他の情報・記録から、紛失等した情報を可能な限り正確に把握し、予想される二次被害を防止する。
・総務部は、調査によって得られた情報を精査し、紛失等した情報の重要性及び被害の程度等を判定する。

５　④通知・報告・公表等

・紛失等した情報に第三者の個人情報が含まれる場合、総務部は、直ちに当該第三者に対して個人情報を紛失等した旨を通知し、謝罪を行う。また、当該第三者が二次的な被害に遭った場合には報告を求める。なお、総務部は、当該謝罪等を、情報を紛失等した本人に行わせることができるものとする。
・紛失等した第三者の個人情報が多数含まれる場合には、総務部は、ホームページ上にて個人情報を紛失等した旨を掲載する。

６　⑤抑制措置と復旧

・総務部は、調査によって得た情報や紛失等した情報の重要性及び被害の程度等に鑑み、必要な抑制措置を実施する。
・紛失等した情報にクレジットカード、銀行口座番号、ＩＤ、パスワード等が含まれていた場合、総務部は、当該情報が本協会の有する情報である場合には、直ちに当該パスワードを変更する等の措置をと

り、当該情報が第三者の有する情報である場合には、直ちに当該情報が紛失等したことを伝え、パスワードの変更等を促す。
・総務部は、紛失等した情報については、記録媒体やＷｅｂ上に残されたデータから、可能な限り復元する。

7　⑥事後対応
・総務部は、情報が紛失等した原因、情報の管理方法、アクセスの制限の有無等の事情を精査し、改善策を検討する。
・総務部は、検討した改善策を、理事及び幹事に対して報告する。

第３　誤送信・Ｗｅｂ等における誤公開

1　事故事例
・メールアドレスやＦＡＸ番号を誤って入力し、機密書類等を第三者に対して誤送信した。
・住所を誤って記載し、機密書類等を第三者に対して郵送した。
・Ｗｅｂ上に誤って機密情報等を掲載した。
・アクセス制限が課されているＷｅｂページのログインＩＤやパスワード等を、誤って第三者に送信した。

2　①発見及び報告
・情報を誤送信又は誤公開（以下「誤送信等」という。）した者又は情報が誤送信等されていることを発見した者は、直ちに事務局総務部に報告を行い、別紙１の「情報漏洩報告シート」に当該誤送信等の内容を記入する。

3　②初動対応
・総務部は、情報漏洩報告シートの内容等を基に、誤送信等した情報の種類・内容を特定する。
・誤送信を行った場合に、送信先が明らかである場合には、当該情報の受信者に対して誤って機密情報を送信したことを通知し、受信した情報の削除を求める。また機密情報を誤って郵送した場合、郵送した情報の内容の重要性が高い場合には、直接当該郵送物を回収するなどして、適切な対応をする。なお、総務部は、当該通知等を、誤送信を行った本人に対して行わせることができるものとする。
・誤公開を行った場合、総務部は、Ｗｅｂ上から直ちに当該情報を削除し、又は、当該情報に対してアクセス制限を設けるなど、被害が拡大しないように対応する。
・誤送信等した情報に、特定の web ページや秘密情報等にログインするためのＩＤやパスワード等の情報が含まれている場合、総務部は、直ちに当該ＩＤやパスワードを変更し、被害の拡大を防止する。

4　③調査
・総務部は、情報漏洩報告シートその他の情報・記録から、誤送信した情報を可能な限り正確に把握し、予想される二次被害を防止する。

・誤公開をした場合、総務部は、アクセスログ等を調査し、当該公開された情報にアクセスされた回数等を把握する。
・総務部は、調査によって得られた情報を精査し、誤送信等した情報の重要性及び被害の程度等を判定する。

5　④通知・報告・公表等

・第三者の情報を誤送信等した場合、総務部は、当該第三者に対して誤送信等をした事実を通知し、謝罪を行う。また、当該第三者が二次的被害に遭った場合には報告を求める。なお、総務部は、当該通知等を、誤送信を行った本人に対して行わせることができるものとする。
・総務部は、情報の重要性及び被害の程度等に鑑み、必要に応じてスポーツ庁に届け出る。また、必要に応じて誤送信等した事実及び経緯等をＷｅｂ等で公表する。

6　⑤抑制措置と復旧

・総務部は、調査によって得た情報や誤送信等した情報の重要性及び被害の程度等に鑑み、必要な抑制措置を実施する。
・誤送信等した情報にクレジットカード、銀行口座番号、ＩＤ、パスワード等が含まれていた場合、総務部は、当該情報が本協会の有する情報である場合には、直ちに当該パスワードを変更する等の措置をとり、当該情報が第三者の有する情報である場合には、直ちに当該情報を誤送信等したことを伝え、パスワードの変更等を促す。

7　⑥事後対応

・総務部は、情報が紛失等した原因、情報の管理方法、アクセスの制限の有無等の事情を精査し、改善策を検討する。
・総務部は、本協会が作成・使用しているＷｅｂページやシステムの安全性等を確認し、必要に応じてシステムの変更を行う。
・総務部は、検討した改善策を、理事及び幹事に対して報告する。

第４　内部犯行

1　事故事例

・協会内データベースから顧客情報を不正に持ち出し、転売した。
・協会内に保管していた機密書類等を不正に持ち出し、第三者に譲渡した。

2　①発見及び報告

・情報を不正に持ち出した者又は情報が不正に持ち出されたことを発見した者は、直ちに事務局総務部に報告を行い、別紙１の「情報漏洩報告シート」に当該誤送信等の内容を記入する。

3　②初動対応

・総務部は、情報漏洩報告シートの内容等を基に、誤送信等した情報の種類・内容を特定する。また、誰が情報を不正に持ち出したのかを特定する。
・情報を不正に持ち出した人物が協会内に存在する可能性がある場合、総務部は、当該情報にかかるアクセスや持ち出し等を可能な限り制限し、証拠の隠滅を防止する。
・情報を不正に持ち出した人物が特定できる場合、総務部は、当該人物の使用したパソコン等の機器を確保する。
・不正に持ち出された情報に、特定の web ページや秘密情報等にログインするためのＩＤやパスワード等の情報が含まれている場合、総務部は、直ちに当該ＩＤやパスワードを変更し、被害の拡大を防止する。
・情報を不正に持ち出された可能性がある場合、総務部は、直ちに警察や専門家に対して通報・相談し、二次被害を防ぐための専門的な助言を受ける。

4　③調査

・総務部は、情報漏洩報告シートその他の情報・記録から、不正に持ち出された情報を可能な限り正確に把握し、予想される二次被害を防止する。
・総務部は、調査によって得られた情報を精査し、不正に持ち出された情報の重要性及び被害の程度等を判定する。

5　④通知・報告・公表等

・総務部は、第三者の情報が不正に持ち出された場合、当該第三者に対して情報が不正に持ち出された事実を通知し、謝罪を行う。また、当該第三者が二次的被害に遭った場合には報告を求める。
・総務部は、情報の重要性及び被害の程度等に鑑み、警察に対して被害届を提出し、情報が不正に持ち出された事実を届け出る。
・総務部は、情報の重要性及び被害の程度等に鑑み、必要に応じてスポーツ庁に届け出る。また、必要に応じて情報が漏えいした事実及び経緯等をＷｅｂ等で公表する。

6　⑤抑制措置と復旧

・総務部は、調査によって得た情報や不正に持ち出された情報の重要性及び被害の程度等に鑑み、必要な抑制措置を実施する。
・不正に持ち出された情報にクレジットカード、銀行口座番号、ＩＤ、パスワード等が含まれていた場合、総務部は、当該情報が本協会の有する情報である場合には、直ちに当該パスワードを変更する等の措置をとり、当該情報が第三者の有する情報である場合には、直ちに当該情報を誤送信等したことを伝え、パスワードの変更等を促す。
・総務部は、不正に持ち出した人物に対して、何らかのアカウント、ログインＩＤ、パスワード等を提供・共有している場合には、当該アカウント等の利用を停止し又は登録情報の変更等を行い、更なる情報を持ち出されないよう対応する。

7　⑥事後対応

・総務部は、情報が不正に持ち出された原因、情報の管理方法、アクセスの制限の有無等の事情を精査し、改善策を検討する。
・総務部は、本協会が作成・使用しているＷｅｂページやシステムの安全性等を確認し、必要に応じてシステムの変更を行う。
・総務部は、情報の重要性及び被害の程度等に鑑み、情報を持ち出した者に対して課す処分の内容を検討する。
・総務部は、検討した改善策及び処分の内容を、理事及び幹事に対して報告する。
・理事及び幹事は、総務部の報告を受け、当該情報を持ち出した者に対する処分の有無及び内容を決定する。

第５　不正プログラム（ウイルス・スパイウェア等）・不正アクセス

1　事故事例

・協会が有するパソコン等の機器がウイルスに感染し、当該機器内に存在する機密情報を第三者に窃取された。
・協会が有するパソコン等の機器がウイルスに感染し、機密情報がＷｅｂサイト等に掲載され、不特定多数の人に閲覧可能な状態となった。
・協会の職員が有する個人のパソコン等の機器がウイルスに感染し、当該機器内に存在する機密情報を第三者に窃取された。

2　①発見及び報告

・パソコン等の機器がウイルスに感染したことを発見した者は、直ちに事務局総務部に報告を行い、別紙１の「情報漏洩報告シート」にウイルス感染の内容等を記入する。

3　②初動対応

・総務部は、情報漏洩報告シートの内容等を基に、感染した機器、感染の経緯、程度を特定し、ウイルスに感染した範囲を把握する。また、当該ウイルスに感染したことにより窃取された情報を可能な限り特定する。
・ウイルスに感染したことが発覚した場合、総務部は、直ちに感染した機器の使用を停止し、当該機器をネットワークから切り離し又は切り離させる。また、総務部は、ネットワーク上のシステムがウイルスに感染した場合には、当該システムへのアクセスを行わないよう徹底し又はこれを徹底させる。
・不正に持ち出された情報に、特定の web ページや秘密情報等にログインするためのＩＤやパスワード等の情報が含まれている場合、総務部は、直ちに当該ＩＤやパスワードを変更し、被害の拡大を防止する。
・ウイルスに感染したことが発覚した場合、総務部は、直ちに警察や専門家に対して通報・相談し、二次被害を防ぐための専門的な助言を受ける。
・総務部は、重要なデータを外部メディアに移すなどし、バックアップを作成する。なお、当該バックア

ップには、不正プログラムが存在している可能性もあることから、必ず専門家の助言を受け、適切な方法・態様により対処する。

4　③調査

・総務部は、情報漏洩報告シートその他の情報・記録から、漏洩した情報を可能な限り正確に把握し、予想される二次被害を防止する。
・総務部は、調査によって得られた情報を精査し、漏洩した情報の重要性及び被害の程度等を判定する。

5　④通知・報告・公表等

・第三者の情報が漏洩した場合、総務部は、当該第三者に対してウイルス感染により情報が漏洩した事実を通知し、謝罪を行う。また、当該第三者が二次的被害に遭った場合には報告を求める。
・総務部は、情報の重要性及び被害の程度等に鑑み、警察に対して被害届を提出し、ウイルス感染により情報が漏洩した事実を届け出る。
・総務部は、情報の重要性及び被害の程度等に鑑み、必要に応じてスポーツ庁に届け出る。また、必要に応じて情報が漏えいした事実及び経緯等をＷｅｂ等で公表する。

6　⑤抑制措置と復旧

・総務部は、調査によって得た情報や漏洩した情報の重要性及び被害の程度等に鑑み、必要な抑制措置を実施する。
・総務部は、専門家の助言を受け又は専門家に委託する方法により、ウイルスや不正プログラムを除去する。
・漏洩した情報にクレジットカード、銀行口座番号、ＩＤ、パスワード等が含まれていた場合、総務部は、当該情報が本協会の有する情報である場合には、直ちに当該パスワードを変更する等の措置をとり、当該情報が第三者の有する情報である場合には、直ちに当該情報が漏洩したことを伝え、パスワードの変更等を促す。
・総務部は、ウイルスに感染した機器を、専門家の助言を受けたうえで初期化を行うなどし、当該機器が再び感染源とならないよう対処する。

7　⑥事後対応

・総務部は、機器やシステムがウイルスに感染した原因、情報の管理方法、アクセスの制限の有無等の事情を精査し、改善策を検討する。
・総務部は、本協会が作成・使用している機器やＷｅｂページ、システム等の安全性等を確認し、必要に応じてシステムやウイルス対策ソフトの変更を行う。
・総務部は、検討した改善策及び処分の内容を、理事及び幹事に対して報告する。

第６　風評被害・ＳＮＳへの掲載

１　事故事例

・機密情報が掲示板やＳＮＳに書き込まれ、不特定多数の第三者に公開されていた。

２　①発見及び報告

・機密情報を公開した者又は機密情報が公開されていることを発見した者は、直ちに事務局総務部に報告を行い、別紙１の「情報漏洩報告シート」に情報が公開された経緯や内容等を記入する。

３　②初動対応

・総務部は、情報漏洩報告シートの内容等を基に、公開した人物や公開された情報を特定する。
・協会内の人物が情報を公開していた場合、総務部は、直ちに当該人物に対して当該情報が掲載された記事、投稿等を削除させ、必要に応じてアカウントを停止・削除させるなどして、情報の拡散を防止する。
・第三者が情報を公開していた場合、総務部は、当該第三者に連絡をとり、機密情報を公開していること、直ちに当該情報が掲載された記事、投稿等を削除するよう依頼する。
・公開された情報に、特定の web ページや秘密情報等にログインするためのＩＤやパスワード等の情報が含まれている場合、総務部は、直ちに当該ＩＤやパスワードを変更し、被害の拡大を防止する。
・記事、投稿等の削除を依頼したにも関わらず、当該記事、投稿等が削除されない場合、総務部は、当該記事、投稿等がなされたデジタルプラットフォームにおける管理者等に対して、記事、投稿等の削除を依頼する。

４　③調査

・総務部は、情報漏洩報告シートその他の情報・記録から、公開された情報を正確に把握し、予想される二次被害を防止する。
・第三者が情報を公開していた場合、総務部は、当該第三者に対して事実関係を聴取し、当該情報を取得した経緯等を把握する。
・総務部は、調査によって得られた情報を精査し、公開された情報の重要性及び被害の程度等を判定する。

５　④通知・報告・公表等

・協会内の人物によって第三者の情報が公開された場合、総務部は、当該第三者に対して情報が公開された事実を通知し、謝罪を行う。また、当該第三者が二次的被害に遭った場合には報告を求める。なお、総務部は、当該通知や謝罪等を、情報を公開した本人に行わせることができる。
・総務部は、情報の重要性及び被害の程度等に鑑み、必要に応じてスポーツ庁に届け出る。また、必要に応じて情報が公開された事実及び経緯等をＷｅｂ等で公表する。

６　⑤抑制措置と復旧

・総務部は、調査によって得た情報や漏洩した情報の重要性及び被害の程度等に鑑み、必要な抑制措置を

実施する。

・記事、投稿等を行った人物が特定できない場合、総務部は、必要に応じて発信者情報の開示等を行うなど、法的手続を検討する。

・公開された情報にクレジットカード、銀行口座番号、ＩＤ、パスワード等が含まれていた場合、総務部は、当該情報が本協会の有する情報である場合には、直ちに当該パスワードを変更する等の措置をとり、当該情報が第三者の有する情報である場合には、直ちに当該情報が公開されたことを伝え、パスワードの変更等を促す。

7　⑥事後対応

・総務部は、情報が公開・拡散された経緯、情報の管理方法、アクセスの制限の有無等の事情を精査し、改善策を検討する。

・総務部は、検討した改善策及び処分の内容を、理事及び幹事に対して報告する。

以上

別紙 1

情報漏洩報告シート	
件名	
報告者氏名	
報告者電話番号	
報告者メールアドレス	
報告者所属	
【情報漏洩が判明した日時】	
【情報漏洩が発生した日時】	
【漏洩した情報の内容・件数】	
【情報漏洩が判明した経緯】	
【情報が漏洩した原因・経緯】	
【漏洩した情報にはパスワード等の保護がなされているか】	

別紙２【調査項目】

流出の確度、可能性	・断定できるのか、可能性にとどまるのか ・どの程度の可能性があるのか ・今後の調査で確度は高まるのか、変わらないのか ※本人への通知、ホームページへの公開等の有無及び内容の判断材料となる
流出した個人情報の項目	・銀行口座番号やクレジットカード番号など、不正使用されると経済的被害に直結するような情報が含まれているか ・病歴や犯罪歴など、公表により当然に精神的苦痛をもたらすセンシティブな情報が含まれているか ・資産状況や信用状態など、一般に人に知られたくない情報が含まれているか ・趣味嗜好や学業成績など、一般には入手し難い情報が含まれているか ・勤務先や役職などビジネス上の情報が含まれているか、又は、自宅や家族構成などプライベートに関する情報が含まれているか ・氏名、住所、電話番号など、開示される頻度が高い情報が含まれているか ※被害者の二次被害の危険性に影響する ※情報が流出する範囲・程度に影響する ※被害者に対する慰謝料額、損害賠償額に影響する
流出した件数、規模	・被害者の数は何人か ・件数を特定できるのか、できないのか ・流出した期間、流出の始期を特定できるのか、できないのか ※協会の損失や被害者に対する慰謝料額、損害賠償額に影響する
流出した範囲	・１か所にとどまっているか ・不特定多数の者に拡散されているか ※被害者の二次被害の危険性に影響する ※各被害者に対する慰謝料額、損害賠償額に影響する
流出した原因	・協会の落ち度によるものか ・委託先など他社・他協会の落ち度によるものか ・悪意者の介在によるものか ・単なる事務ミスによるものか ・制度的欠陥、恒常的欠陥によるものか ・犯罪被害によるものか ・原因を特定できるか、できないことに落ち度がないか ※会社の過失の有無・程度に影響する ※社会的非難の程度や改善策の有無内容に影響する
流出から察知までの期間	・協会はすぐに察知できたのか ・察知が遅れた場合何故察知が遅れたのか ・協会は事態を放置していたとは評価されないか ・協会は事態を隠蔽していたと評価されないか ※被害拡大に対する社会の落ち度に影響する ※社会的非難の程度に影響する
再発防止の可能性	・実効性のある再発防止策がとれるのか ・再発防止策はすぐにとれるのか、時間がかかるのか ・再発防止策がとれないのか、再発の可能性がのこるのか ※協会の損失の程度に影響する ※社会的非難の程度に影響する