付録C インシデント発生時に組織内で整理しておくべき事項

インシデント発生時、原因調査等を行う際に組織内で整理しておくべき事項を示す。
本資料の内容を参考に原因調査等を行い、必要な事項については適宜経営者や関係者に報告を行うことが望ましい。

本付録では、以下の5つの表を提供する。インシデントの状況に応じて該当する表を利用すること（案件により複数の表を利用することもある。例えば、不正アクセスにより情報漏えいが発生した場合は表1、表2、表4を利用する）

表1	基本項目	全てのインシデントで共通して調査すべき項目
表2	情報漏えいに係る項目	情報漏えいが発生した際に調査すべき項目
表3	ウイルス感染に係る項目	ウイルス感染が発生した際に調査すべき項目
表4	不正アクセスに係る項目	不正アクセスを受けた際に調査すべき項目
表5	（D）DoSに係る項目	（D）DoS攻撃を受けた際に調査すべき項目

初動対応

- 被害範囲の確認
- サービス停止有無の判断
- 顧客・取引先対応
- 外部専門企業等への調査依頼

第一報

※表1の項番1-11を記載
インシデントが発生したことを速やかに周知。必要に応じてサービス停止や二次被害防止のための注意喚起を行う目的で報告

原因調査

- 侵害原因調査
- システムの脆弱性等の確認
- 被害の詳細確認

第二報以降

※インシデントの分類に応じた表を選択
調査の結果、判明した内容を記載
インシデントによる被害範囲がおおよそ確定し、原因が判明した後に、被害を受けた人に対する周知と他組織が同様の攻撃による被害を受けないための情報共有を行う目的で報告

事後対策

- 再発防止策の検討・実施

最終報

※再発防止策を含む全てを記載
被害に対する対応と、その後の再発防止策を含めた事後対策の実施等について、周知を行うことで関係者の安心と、他組織が参考とする目的で報告

表-1　基本項目の説明

フェーズ	項番	名称		説明
初動対応/第一報	1	インシデントの分類		ウイルス感染、不正アクセス、（D）DoS攻撃のいずれかを記載。
	2	事業分類		日本標準産業分類の中分類を記載。 複数の分類にまたがる場合は、最も売上げが高い業種で分類。 http://www.soumu.go.jp/toukei_toukatsu/index/seido/sangyo/02toukatsu01_03000044.html
	3	事業者名（会社名）		事業者名を記入。委託先の場合、委託元を含む関係事業者名も記載。 発生した時点と現時点での事業者の名称が異なる場合には現時点での名称も併記。
	4	責任者（担当者）		本件に関する責任者および担当者の所属部署、氏名を記載。
	5	連絡先		項番4の責任者および担当者に連絡が可能な電話番号を記載。　また、連絡が可能な曜日および時間帯も併記すること。
	6	発生日		調査により判明した本件の発生日時を記載。
	7	発覚日		本件を認知した日時を記載。
	8	事案の公表		事案の公表についての実施状況を記載。 ※検討中であれば検討中であることを記載。
	9	事案の概要		原因を含めて、事案の概要を可能な限り詳細に記載。
	10	経過（時系列）		発生から報告時点までの経過について、時系列で概要を記載。
	11	被害を受けたシステムの概要		被害を受けたシステムについての用途などを含めた概要を可能な限り詳細に記載。
原因調査/第二報以降	12	システムの運用状況		システムの稼動年月日、内製か外製か、運用の状態やセキュリティサービスの利用状況など侵害されたシステムに関するについての調査状況などを記載。
	13	システム構成		システムの物理的所在地や、OS、アプリケーションとそのバージョン構成などを可能な限り詳細に記載。 ※簡単な構成図なども可能であれば併記すること。
	14	備考		

表-2　情報漏えいに係る項目

フェーズ	項番	名称		説明
原因調査/第二報以降	15	発覚の経緯		発覚の経緯について概要を記載。自社による検知か（対象のログやアラート）、第三者による通知か、などを記載。第三者である場合、セキュリティ監視などの業務委託先によるものか顧客によるものかも記載。
	16	原因及び経路		情報漏えいに至った原因を記載。 経路については外部ネットワーク経由による第三者によるものか、内部ネットワーク経由の内部犯行によるものかを記載。
	17	情報漏えいの有無		情報漏えいの有無と個人情報を含むか否かの記載。 ※調査中であればその旨を記載。 一部判明しているものがある場合は判明時点の日時を添えた上で記載。
	18	漏えいしたデータの項目及び件数		漏えいしたデータの内容について記載。 また、漏えい等の件数を記載。さらに、個人情報を含んでいた場合にはその件数について「顧客情報」「従業者情報」「その他の個人情報」の３つに分類してそれぞれ記載。上記に該当しないデータについても記載。 営業秘密が漏えいした場合は、その影響（事業へのインパクト等）についても記載。
	19	暗号化等の情報保護措置		漏えいした情報に関し、情報の暗号化などの情報保護のために予め講じられていた措置の有無について、「措置有」、「一部措置有」、「措置無」、「不明」にさらに分類し記載する。 ＊「一部措置有」とは、漏えいしたデータのうち、一部については暗号化や情報のマスキングなどの措置が行われていた場合を指す。
	20	漏えい元・漏えいした者		情報の漏えい元に関する情報、漏えいに関わった者（組織内部の者か否かについて）の情報、意図（過失によるものか、違反によるものか）について記載。調査中のため、不明の場合にはその旨も記載。
	21	情報所有者本人等への対応		情報所有者本人への連絡 有：情報所有者等本人および委託元すべてに通知し、連絡がついた場合。 無：情報所有者等本人および委託元すべてに連絡がついていない場合。 ＊謝罪の有無については、本項目では除外するものとする。 その他の対応 個人情報の漏えい等事案を受けて行った対応（予定を含む）について、それぞれ、「カード（銀行、クレジット等）の、差し替え」、「専用窓口の設置」、「商品券等の配布」、「詫び状の送付（郵送・メール・ＦＡＸ）」、「警察への届出（〇〇署）」などを記載。 いずれにも該当しないものがある場合は、その他として具体的に記載する。
	22	二次被害		情報漏えいによる二次被害の有無について記載。 有：本人に２次被害が発生している場合は、詳細な内容を記載する。本人から電話勧誘やダイレクトメールが増えた等の苦情があった場合も、本項目に記載する。 無：一切の２次被害が発生していない場合。現時点において確認できていない場合はその旨を記載。
原因調査/第二報以降 事後対策/最終報	23	事業者による対応（再発防止策を含む）		（注：単に「再発防止策の徹底等」の抽象的な記載に留まらず、当該再発防止策の具体的内容を記載すること。） 漏えいの事案を受けて、実施予定のものも含め、再発防止策について「組織的・人的安全管理措置」と「物理的・技術的安全管理措置」と区分して具体的な内容を記載する。 〔組織的・人的安全管理措置〕の例 安全管理責任者、個人情報保護委員会等の設置 個人情報保護に関する社内規定、プライバシーポリシー等の整備 全社員、派遣社員、業務委託先を対象とする個人情報保護教育の実施 定期的な内部監査・外部監査の実施 委託先管理の強化（委託先の選定基準・管理基準の作成、定期検査の実施） 〔物理的・技術的安全管理措置〕の例 外部とネットワーク接続している端末へのファイアウォールの構築 アクセス権限認証の強化（生体認証機能導入） 個人情報アクセス端末を対象に情報漏えい防止ソフトウェアを導入 データ保存の暗号化 個人データへのアクセス状況の監視

フェーズ	項番	名称		説明
	24	報告先		既に報告を行っている場合には具体的な組織名を記載。法律に基づく場合にはその旨も記載。
	25	備考		

表-3　技術詳細（ウイルス感染）係る項目の説明

フェーズ	項番	名称	説明	説明
原因調査/第二報以降	26	発覚の経緯		発覚の経緯について概要を記載。自社による検知か（対象のログやアラート）、第三者による通知か、などを記載。第三者である場合、セキュリティ監視などの業務委託先によるものか顧客によるものかも記載。
	27	原因及び経路		ウイルス感染に至った原因及び経路を記載。 経路に関しては、メールによるものか、Webアクセス、もしくはUSBメモリなどの可搬媒体いずれによるものかを記載。現在調査中の場合にはその旨を記載。
	28	検出名およびアンチウイルスベンダ名		当該ウイルスがアンチウイルスソフトに検出された場合はその検出名およびアンチウイルスソフトの名称とパターンファイルのバージョンを記載。
	29	感染端末と影響の特定		ウイルスに感染した端末を特定し、当該端末から他の端末に感染が拡大していないかをPCの操作ログ等から確認し、記載。 また、ウイルスに感染した端末から外部に対してウイルスによる通信が発生していないかも記載。
	メール感染の場合			
	30	メールの送信日時		該当メールの送信された日時（メールから確認）を記載。
	31	送信元メールアドレス（名前、メールアドレス）		メールのFromに記載されているメールアドレスと名前を記載。
	32	送信先メールアドレス（名前、メールアドレス）		メールの送信先のメールアドレスと名前を記載。 そのアドレスが問い合わせ用などの公開アドレスか否かを併せて記載。 ※自分宛でなく、Bccによる配信の場合も可能な限り記載
	33	件名		メールの件名（Subject）を記載。
	34	本文		メールの本文を記載。
	35	添付ファイルの有無		添付ファイルの有無を記載。 有の場合には拡張子を含むファイル名も併せて記載。
	36	メール本文内のリンクの有無		メール本文内のリンクの有無を記載。 有の場合にはそのリンクのアドレスを記載。 HTMLメールの場合、メール内の文字列とリンク先が異なる場合があるため、異なる場合には記載と実際のリンク先を両方記載。
	37	MTA情報メールヘッダ		送信元サーバや経由サーバのアドレスなどを含むメールヘッダを記載。
	38	メールに関するその他事項		その他、特異点があれば記載。
	Web感染の場合			
	39	アクセス日時		感染のきっかけとなったWebサイトへアクセスした日時を記載。リダイレクト等で複数経由している場合にはわかる範囲で記載。 （プロキシログなどの証跡がある場合は
	40	アクセス先URL		感染の原因となったWebサイトのURLを記載。
	41	感染の原因となったURL		アクセス先URLから最終的に感染の原因となったサイトのURLを記載。
	42	攻撃手法		感染の原因となったWebサイトで行われた攻撃下記から選択し記載。 □ 脆弱性利用 □ ファイルのダウンロード 脆弱性利用の場合は、CVE番号などの利用された脆弱性の識別子を記載。
	ウイルス情報に関する共通事項			
	43	圧縮ファイル名		添付ファイルやダウンロードファイルが圧縮ファイルであった場合にそのファイル名を記載。感染のきっかけとなったファイル名を記載。ファイル名は拡張子までを記載。
	44	圧縮ファイルハッシュ値（上記が圧縮ファイルである場合のみ記載）		添付ファイルやダウンロードファイルが圧縮ファイルであった場合にそのファイルのハッシュ値を記載。感染のきっかけとなったファイルのハッシュ値を記載。ハッシュ値はMD5、SHA1、SHA256など可能な限り記載。
	45	スクリプトおよびマクロを含む文書ファイル名		添付ファイルやダウンロードファイル、または圧縮ファイル展開後のファイルがスクリプトファイル（.jsファイルや 場合にそのファイル名を記載。ファイル名は拡張子までを.wsfファイル、マクロを含む文書ファイルなど）であった記載。 添付ファイルやダウンロードファイルが圧縮ファイルであった場合、その展開後のファイル名を記載。

フェーズ	項番	名称	説明	説明
	46	スクリプトおよびマクロを含む文書ファイルハッシュ値		添付ファイルやダウンロードファイル、または圧縮ファイル展開後のファイルがスクリプトファイル（.jsファイルや.wsfファイル、マクロを含む文書ファイルなど）であった場合にそのファイルのハッシュ値を記載。ハッシュ値はMD5、SHA1、SHA256など可能な限り記載。
	47	スクリプトファイルおよびマクロを含む文書ファイル実行後のダウンロード先と日時(ドメイン/IPアドレス - IPアドレスは問い合わせ日時を記載)		添付ファイルやダウンロードファイル、または圧縮ファイル展開後のファイルがスクリプトファイル（.jsファイルや.wsfファイル、マクロを含む文書ファイルなど）であった場合にそのファイル実行後の接続先（ドメイン/IPアドレス、URL）とその確認日時を記載。この通信先がファイルをダウンロードするものであった場合のダウンロードされたファイルについては次項目以降にその情報を記載。 ドメイン： IPアドレス： IPアドレス問い合わせ日時：
	48	実行形式ファイル名		添付ファイルやダウンロードファイル、または圧縮ファイル展開後のファイルが実行形式であった場合にそのファイル名を記載。前項目のスクリプトファイルおよびマクロファイルが外部から実行形式ファイルをダウンロードするような振る舞いをするようなものであった場合はそのファイルの名前を記載。ファイル名は拡張子までを記載。
	49	実行形式ファイルハッシュ値		添付ファイルやダウンロードファイル、または圧縮ファイル展開後のファイルが実行形式であった場合にそのファイルのハッシュ値を記載。前項目のスクリプトファイルおよびマクロファイルが外部から実行形式ファイルをダウンロードするような振る舞いをするようなものであった場合はそのファイルのハッシュ値を記載。ハッシュ値はMD5、SHA1, SHA254など可能な限り記載。
	50	実行形式ファイル実行後の通信先と日時 ファイルの通信先(ドメイン/IPアドレス - IPアドレスは問い合わせ日時を記載)		添付ファイルやダウンロードファイル、または圧縮ファイル展開後のファイルが実行形式ファイルであった場合にそのファイル実行後の接続先（ドメイン/IPアドレス、URL）とその実行日時を記載。 ドメイン： IPアドレス： IPアドレス問い合わせ日時：
事後対策/最終報	51	事後対策内容		漏えいの事案をうけて、実施予定のものも含め、再発防止策について、具体的な内容を記載する。例えば、OS、アプリケーション、アンチウイルスソフト等の最新版や最新のパターンファイルへの更新。多層防御製品の導入。 ※情報漏えいの場合には、重複するため記載しなくてもよい。
	52	備考		

表-4　技術詳細（不正アクセス）係る項目の説明

フェーズ	項番	名称	説明	説明
原因調査/第二報以降	53	発覚の経緯		発覚の経緯について概要を記載。自社による検知か（対象のログやアラート）、第三者による通知か、などを記載。第三者である場合、セキュリティ監視などの業務委託先によるものか顧客によるものかも記載。
	54	原因および経路		原因及び経路について記載、利用された脆弱性が判明している場合には利用された脆弱性のCVE番号などの識別番号を記載。認証（Web,FTP,SSH等）による不正アクセスの場合にはそのサービス名を記載。また、奪取された権限も記載。
	55	当該原因が発生（残存）していた理由		本件の原因となった事象が発生（残存）していた理由。修正プログラムを適用できなかった理由や不正アクセスに利用されたアカウントが脆弱な状態であった理由を記載。
	56	攻撃元情報		不正アクセスに利用された攻撃元の情報（ドメイン/IPアドレスなど）を記載。 ドメイン： IPアドレス： IPアドレス問い合わせ日時：
	影響範囲			
	57	改ざん		改ざんを行われた場合に当てはまる改ざんの種別を以下から選択。 □ Webサイト改ざん □ ウイルス配布 □ ファイル設置 □ リダイレクトコード挿入 リダイレクト先URL: □ 追加ファイル設置 □ WebShell □ (D)DoSボット □ 上記以外のファイル □ DNS改ざん
	58	メール不正中継踏み台		メールの不正中継を行われた場合に送信されたメールの件数及び、送信されたメールの内容（件名、本文など）を記載。 送信数： 送信内容：
	59	情報漏えいの有無		□有 □無 ※有の場合には、情報漏えいの項目に記載のこと。
事後対策/最終報	60	事後対策内容		本件を受けて行った事後対策内容を記載。 IDS/IPS、WAF、改ざん検知などの監視の導入、セキュリティ診断の実施
	61	備考		

表-5　技術詳細（（D）DoS攻撃）係る項目の説明

フェーズ	項番	名称		説明
原因調査/第二報以降	62	発覚の経緯		発覚の経緯について概要を記載。自社による検知か（対象のログやアラート）、第三者による通知か、などを記載。第三者である場合、セキュリティ監視などの業務委託先によるものか顧客によるものかも記載。
	63	犯行声明の有無		（D）DoSの予告、または（D）DoSを行ったことを示す犯行声明の有無。 犯行声明の有無： 媒体（メール、SNS、テキスト共有サイトなど）：
	64	犯行声明内容		犯行声明の内容について記載。 インターネット上で閲覧可能であったものについてはそのURLなどの所在も併せて記載。
	65	攻撃手法		どのような攻撃手法であったかを記載。利用されたプロトコルなどログから判明する情報を可能な限り詳細に記載。
	66	日時		（D）DoSの開始日時、発覚日時、終了日時についてそれぞれ記載。
	67	攻撃概要		（D）攻撃の通信量やリクエスト数などを時系列で記載。プロトコル（DNS、HTTP、NTP）が複数ある場合はプロトコルごとに記載。必要に応じてグラフなども添付のこと。
	68	影響範囲		（D）DoSにより発生した影響範囲を記載。 システムの停止時間（（D）DoSの継続時間のみではなく自身でサービスを停止させていた時間を含む）や停止により発生した金銭的損失を記載。攻撃を受けた対象に複数のユーザ、Webサイトが存在する場合はその数も記載。
事後対策/最終報	69	事後対策内容		本件を受けて行った事後対策内容を記載。
	70	備考		