岐阜県

情報セキュリティ事故対応マニュアル

Ver. 1.5

岐阜県情報セキュリティ委員会
（事務局：総務部情報企画課）

目　次

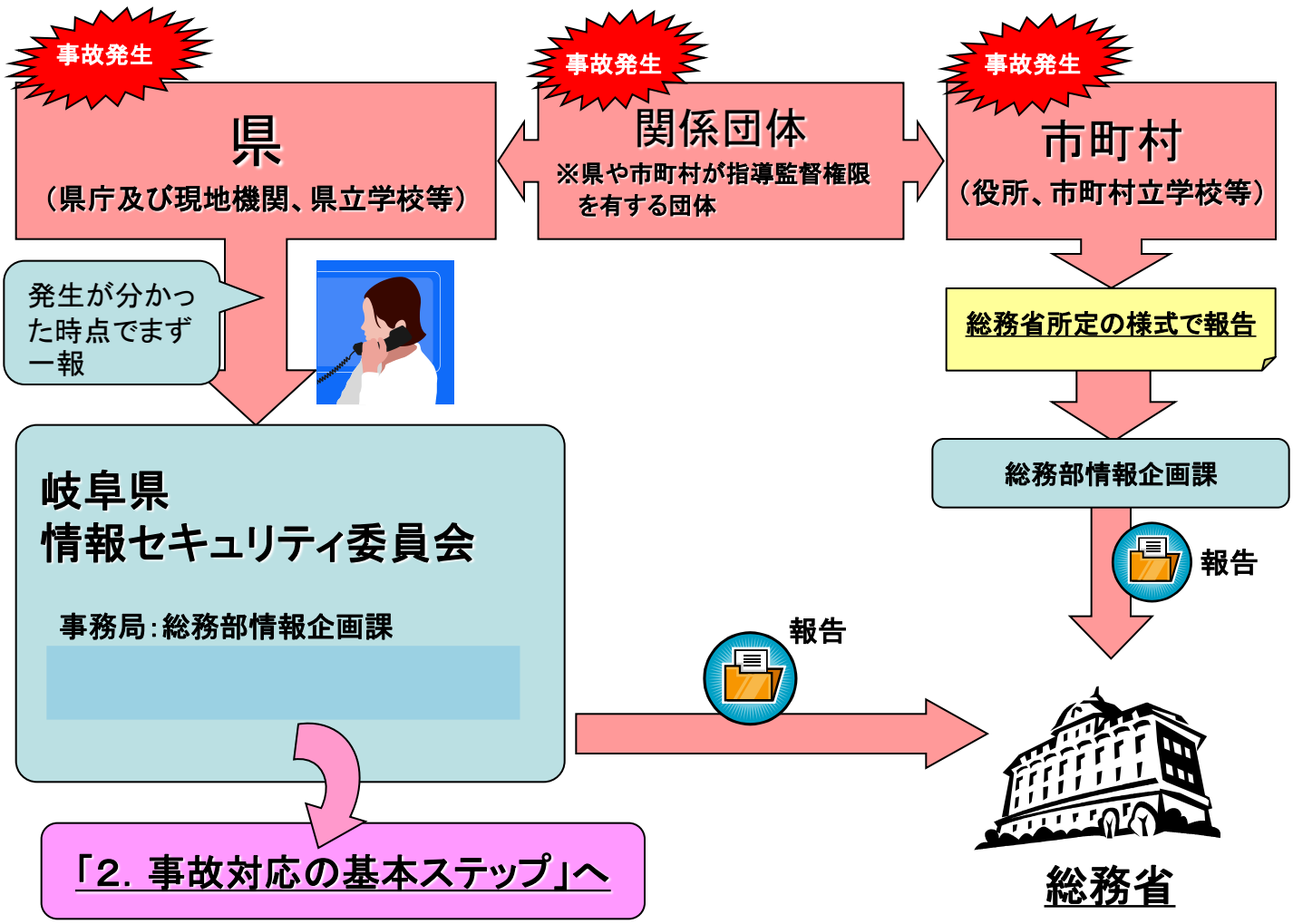
1．基本的な考え方

◆情報セキュリティ事故対応の目的

　情報セキュリティ事故後に対応を行う最大の目的は「情報セキュリティ事故による直接的・間接的被害を最小限に抑える」ことにあります。

　自分の所属（組織）だけでなく、情報セキュリティ事故の最終的な被害者、県民、業者、職員など情報漏えいによって被害を受ける様々な関係者の被害を最小限に抑える必要があります。

◆情報セキュリティ事故対応の主な流れ



2. 事故対応の基本ステップ

情報セキュリティ事故発生

発見・通報

◎情報セキュリティ事故に関する兆候や具体的な事実を確認した場合
◎不正アクセスや不正プログラム（ウイルスを含む）など情報システムからの情報漏えいやシステムが破壊される可能性がある場合
※不用意な操作をせず、システム上に残された証拠を消してしまわないようにする
◎外部から通報があった場合　**※相手の連絡先等を必ず控える**

同時に

初動対応

◎被害が広がる可能性がある場合や、情報が外部からアクセスできる状態にある場合、まずは、これらを遮断する措置をとる。（ネットワークの遮断、サービスの停止、情報の隔離など）
◎速やかに情報セキュリティ委員会（事務局：情報企画課IT最適化係）へ報告し、対応を協議する。
情報企画課IT最適化係

◆協議内容：ポリシー違反の有無、被害の収拾、個人情報漏洩への対応　等

◎情報セキュリティ責任者（所属長）のもと、速やかに事故対応のための体制をとり対応を行う。

報告協議

◎知事・副知事への報告・協議
◎関係課（広報課、県警、危機管理政策課）との協力

通知公表報告等

◎漏洩した個人情報の本人への謝罪と通知
◎不正アクセス、脅迫などがある場合は警察への届出
◎記者発表（公表が必要と判断された場合）
◎総務省報告書作成 → 情報企画課から総務省へ提出

措置復旧

情報漏洩による被害の拡大防止と復旧のための措置を行う。
◎専用の相談窓口の設置
◎停止したシステム等の復旧を行う

再発防止計画

抜本的な再発防止策を検討し実施する。
◎最終的な事故報告書の提出
◎再発防止計画の策定と実施
◎被害者への補償、職員の責任（処分）
→ 情報セキュリティ対策管理部会と協議

3. 事故のタイプ別対応のポイント
3-1 紛失・盗難の場合の対応

（1）発見および報告

◆紛失・盗難が間違いないか、もう一度確認

◆紛失場所の管理者（鉄道会社担当窓口、店舗窓口など）に連絡

	事故事例	発覚のきっかけ
1	パソコンやUSB メモリなどを電車の中、飲食店などに置き忘れた。	・自己申告 ・警察からの連絡 ・取得者からの連絡
2	パソコンやUSB メモリなどが入った鞄をひったくりに遭い盗まれた。	
3	置き引きや車上荒らしに遭い、パソコンやUSBメモリなどを盗まれた。	
4	事務所荒らしに遭い、事務所のパソコンが盗まれた。	
5	請負業者に送ったMO、CDなどが、輸送中に紛失した。	

（2）初動対応

◆何の情報がどの程度含まれていたのか、暗号化やアクセス制限の有無を確認

事実関係を整理する	
(1) 紛失、盗難の当事者は誰か？ (2) 何(物)が紛失、盗難したのか？ (3) 紛失、盗難の対象物に格納されていた情報は何か？ (4) いつ紛失、盗難が発生したのか？ (5) どこで紛失、盗難が発生したのか？ (6) なぜ紛失、盗難が発生したのか？ (7) 紛失、盗難が発覚した理由は何なのか？	a) 誰の情報か？ b) 何の情報か？ c) いつ頃の情報か？ d) 情報の量（件数）はどのくらいか？ e) どのような形で保存されていたか？ （暗号化or平文、HDD 保護、認証パスワード保護など）

◆警察に届出る （製造番号や製品固有の特徴情報があると発見しやすくなります）

◆アカウント情報が含まれる場合はパスワードの変更やアカウントの停止を行う

	応急処置例	留意点
1	紛失物の捜索・回収	・鞄の形状、大きさ、色などの特徴 ・パソコンの機種、製造番号など
2	警察への届出	
3	流失したアカウントの停止、パスワードの変更	

（3）調査

◆組織内に残された記録から紛失・盗難にあった情報をなるべく正確に把握する。

◆予想される二次被害を確認

被害の重要度を判定する
(1) 漏えいした情報区分は？　個人情報（分類Ⅰ）／行政情報（分類ⅡⅢ）／一般情報（分類Ⅳ） (2) 漏えいした情報の保護策は、何を実施していたか？ (3) 影響はどこにあるか？（県民／行政／企業） (4) 管理上の問題点は？

◆機器・媒体がオークションや中古市場に出回っていないか確認する。

（4）通知・報告・公表等

◆個人情報が含まれる場合で漏えいの恐れがある場合は、本人への通知と謝罪を行う。

◆総務省へ報告義務がある。（所定の様式）

◆規模や影響範囲が大きい場合は経緯を公表する。

3. 事故のタイプ別対応のポイント
3-2 誤送信・Webでの誤公開

（1）発見および報告

◆ミスをした本人、もしくはそれを発見した第三者からの指摘により発見される。

◆外部からの指摘を受けた場合は連絡先を確認。

	事故事例	発覚のきっかけ
1	相手のメールアドレスを打ち間違え、他人に誤送信した	・自己申告(内部発見) ・受信者からの指摘(風評を含む) ・Web閲覧者からの通報
2	同報メールの宛先をBCC:に書くべきところ、CC:にして送信した	
3	情報公開システムで個人情報を記載したまま公開してしまった	
4	Web関係のぜい弱性により、非公開情報が参照できていた	
5	Webアプリケーションのミスで、他人の個人情報を表示した	
6	Webで誤って非公開情報を公開情報としていた （サーバ移行時の非公開情報削除もれ、IDパスワードで保護さ.れるべき情報がサーバの設定ミスで公開エリアに保管した、公開サーバへ誤って非公開情報を転送したなど）	

（2）初動対応

◆何の情報がどの程度含まれていたのか、暗号化やアクセス制限の有無を確認。

事実関係を整理する	
(1) 誤送信・Web誤公開の当事者は誰か？ (2) 何を誤送信・Web誤公開したのか？ (3) 誤送信・Web誤公開の対象物に格納されていた情報は何か？ (4) いつ誤送信・Web誤公開が発生したのか？ (5) どこで誤送信・Web誤公開が発生したのか？ (6) なぜ誤送信・Web誤公開が発生したのか？ (7) 誤送信・Web誤公開が発覚した理由は何なのか？	a) 誰の情報か？ b) 何の情報か？ c) いつ頃の情報か？ d) 情報の量（件数）はどのくらいか？ e) どのような形で保存されていたか？ （暗号化／平文、パスワード保護など）

◆誤送信で送信先が明らかな場合は受信者に対しミスについて謝罪し、受信した情報について削除を依頼。

◆誤公開の場合は直ちに当該情報を削除するか、アクセス制限措置を施し外部から参照できないようにする。

	応急処置例	留意点
1	【メールの誤送信】 受信者への連絡と情報の廃棄	・受信者に連絡が取れない場合の対応 ・該当Web 情報を保持または掲載している第三者が情報削除に応じない場合の対応
2	誤ってWeb に公開した情報の削除	

（3）調査

◆漏えいした情報の範囲、原因、被害の状況等について調査。

◆誤公開の場合は、どういった範囲で何人が参照したかアクセスログを使って調査。

◆予想される二次被害を確認。

被害の重要度を判定する
(1) 漏えいした情報区分は？　個人情報（分類Ⅰ）／行政情報（分類ⅡⅢ）／一般情報（分類Ⅳ） (2) 漏えいした情報の保護策は、何を実施していたか？ (3) 影響はどこにあるか？（県民／行政／企業） (4) 管理上の問題点は？

3. 事故のタイプ別対応のポイント
3-2　誤送信・Webでの誤公開

（4）通知・報告・公表等
- ◆個人情報が含まれる場合で漏えいの恐れがある場合は、本人への通知と謝罪を行う。
- ◆規模や影響範囲が大きい場合は経緯を公表する。

（5）抑制措置と復旧
- ◆情報システムの不具合が原因の場合は、システムを修正するか使用を制限する。
- ◆人的な作業ミスの場合は、ミスを見逃さないよう作業手順にチェックの仕組みを追加。
- ◆職員の教育・啓蒙を行う。
- ◆すべてのWeb ページの設定を再確認。

3. 事故のタイプ別対応のポイント
3-3 内部犯行（委託業者含む）

（1）発見および報告

◆ダイレクトメールや架空請求、振り込め詐欺など県民から自分の情報が不正に利用されているようだとの問い合わせを受け発覚するケースが多い。

◆マスコミ等から情報が漏えいしているようだとの問い合わせを受け発覚することもある。

◆相手の連絡先を確認し、どういった情報を持っているのか提示してもらい漏えいの事実を確認する。

	事故事例	発覚のきっかけ
1	庁内のデータベース等から県民の情報を不正に持ち出した	・外部からの指摘（風評を含む）
2	過去に業務で使用していたID を利用してアクセスし、不正にデータを持ち出した	

（2）初動対応

◆何の情報がどの程度含まれていたのか、暗号化やアクセス制限の有無を確認する。

事実関係を整理する	
(1) 内部犯行の当事者は誰か？ (2) 何を持ち出したのか？ (3) 内部犯行の対象物に格納されていた情報は何か？ (4) いつ内部犯行が行われたのか？ (5) どこで内部犯行が行われたのか？ (6) なぜ内部犯行が発生したのか？ (7) 内部犯行が発覚した理由は何なのか？	a) 誰の情報か？ b) 何の情報か？ c) いつ頃の情報か？ d) 情報の量（件数）はどのくらいか？ e) どのような形で保存されていたか？ （暗号化／平文、HDD 保護、パスワード保護など）

◆内部犯行の場合は漏えいの規模や範囲が大きくなる傾向があり、慎重な対応が必要。

◆庁内（委託業者）に情報を持ち出した犯人がいると思われる場合は、重要な情報を証拠隠滅されないよう注意する。

	応急処置例	留意点
1	データベースサーバ、共用ファイルサーバ、イントラネットサーバのID の停止やアクセス制限の実施	・証跡保存を実施する際には、コンピュータフォレンジックを考慮した確保が必要なため、慎重に対応すること。（専門家への依頼など）
2	内部犯行当事者の使用した関連装置の確保(証跡保存)	

※「コンピュータ・フォレンジック」とは、システムがクラックされた後で実施される調査を意味する。
狭い意味で使われることがあって、その場合は法廷に提出する証拠を発見するための調査を意味する。

（3）調査

◆漏えいした情報の範囲、原因、被害の状況等を明らかにする。

◆漏えい情報の範囲から、持ち出された時期や当該情報にアクセスできた人物などを絞り込む。

◆予想される二次被害を確認する。

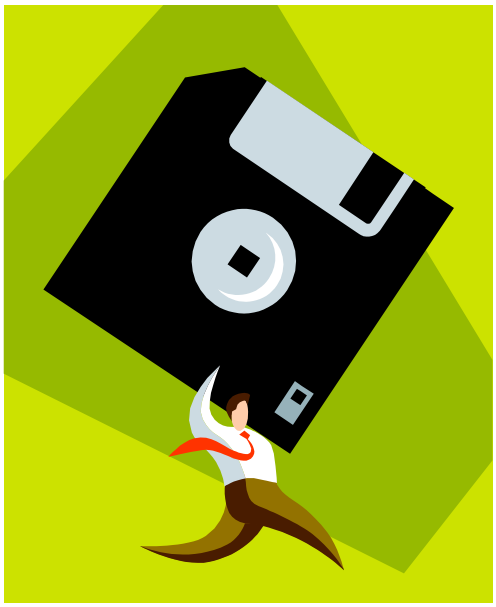
被害の重要度を判定する
(1) 漏えいした情報区分は？　個人情報（分類Ⅰ）／行政情報（分類ⅡⅢ）／一般情報（分類Ⅳ） (2) 漏えいした情報の保護策は、何を実施していたか？ (3) 影響はどこにあるか？（県民／行政／企業） (4) 管理上の問題点は？

3. 事故のタイプ別対応のポイント
3-3 内部犯行（委託業者含む）

（4）通知・報告・公表等
- ◆犯罪に発展する可能性がある場合は、早めに警察に相談する。
- ◆規模が大きい場合は、公表を検討する。
- ◆個人情報が含まれる場合は、対象が特定できた時点で、なるべく早く本人に通知できるようにする。

（5）抑制措置と復旧
- ◆犯人を特定した上で再発防止策を講じる。通常は認証やアクセス制御、ログの取得等社内の情報管理体制を強化する。
- ◆アカウントの再発行や登録情報の変更を行い通常の業務、サービスに復帰する。

	二次被害防止策例	留意点
1	警察への届出	・第三者からの情報回収該当情報を保持または掲載する第三者が情報回収に応じてくれない場合の対応
2	漏洩可能性のある情報の回収	
3	ID、パスワード、アクセス権限の見直し	
4	脆弱性の除去	



3. 事故のタイプ別対応のポイント
3-4 Winny/Share等への漏洩

（1）発見および報告

◆外部からの通報により発見することが多い。内閣官房情報セキュリティセンター（NISC）によるネット監視において流出が判明することも多い。

◆後々の調査のために通報者の連絡先を必ず確認しておく。またどのような情報が漏えいしているかについて詳しい情報を聞き、可能であれば取得した情報を提供してもらうようにする。

	事故事例	発覚のきっかけ
1	職員が重要情報や個人情報を自宅に持ち帰り(USB メモリでも持ち出しやメールを自宅メールに転送するなど)、個人パソコンに情報を保存しており、本人や家族がファイル交換ソフトを利用中に暴露ウイルスに感染し、ファイル交換ネットワークへ情報が漏えいした	・外部からの指摘（風評を含む）

（2）初動対応

◆漏えい情報の内容、範囲を確認する。

◆漏えい元を特定し、調査に対する本人の協力を得る。

事実関係を整理する	
(1) Winny/Share ネットに流出させた当事者は誰か？	a) 誰の情報か？
(2) Winny/Share ネットに流出した情報は何か？	b) 何の情報か？
(3) いつWinny/Share ネットへの流出が発生したのか？	c) いつ頃の情報か？
(4) どこでWinny/Share ネットへの流出が発生したのか？	d) 情報の量（件数）はどのくらいか？
(5) なぜWinny/Share ネットへの流出が発生したのか？	e) どのような形で保存されていたか？
(6) Winny/Share ネットへの流出が発覚した理由は何なのか？	（暗号化／平文、HDD 保護、パスワード保護など）

◆現在もWinny/Share を使用しているようであればただちに停止させる。

	応急処置例	**留意点**
1	インターネットからのパソコンの切り離し (Winny/Share の利用停止)	・パソコンは調査に必要なファイル等が削除されないように、極力使用時の状態に手を加えないままで提出させる
2	漏えいしたファイル(情報)の確保	

（3）調査

◆漏えい情報の内容、範囲、時期等について調査する。

◆本人がその情報を流出するに至った経緯についても調査する。

◆調査のためにWinny/Share 等を使用することは被害の拡大につながりかねませんので行なうべきではありません。

◆予想される二次被害を確認する。

被害の重要度を判定する
(1) 漏えいした情報区分は？　個人情報（分類Ⅰ）／行政情報（分類Ⅱ Ⅲ）／一般情報（分類Ⅳ）
(2) 漏えいした情報の保護策は、何を実施していたか？
(3) 影響はどこにあるか？（県民／行政／企業）
(4) 管理上の問題点は？

3. 事故のタイプ別対応のポイント
3-4 Winny/Share等への漏洩

（4）通知・報告・公表等

◆漏えい情報に個人情報が含まれる場合には本人に通知し謝罪する。

◆Winny/Share などは要求の多いファイルをネットワーク上の多くのコンピュータに拡散させる仕組みを持っているので、一旦人々の興味をそそり人気のあるファイルになってしまうと、ネットワーク上にファイルが拡散しいつまでも漏えいが続くことになる。事件の公表がWinny/Share のダウンロードを誘発する恐れがある場合は、しばらくの間公表を控えるという考え方もあり得る。被害防止の観点から最善と思われる措置をとる。

（5）抑制措置と復旧

◆Winny/Share の漏えい情報については、とにかく話題性を高めずネットワーク上のファイルが自然に消滅することを待つのが得策の場合もある。

◆多くの場合自宅において業務データを漏えいするケースが多いので、庁舎外へのデータ持ち出しの制限などを再徹底する。

◆職員に対してファイル交換ソフトの利用の危険性を周知する。

	二次被害防止策例	留意点
1	ウイルス駆除	・Winny/Share ネットワーク上の情報を完全削除することはほぼ不可能です
2	個人パソコンから、行政情報・個人情報の削除	
3	ID、パスワードが含まれる場合は、アクセス権限停止	

3. 事故のタイプ別対応のポイント
3-5 不正プログラム

※GAIBパソコンに及びRENTAIネットワーク上でウイルス等が発見された場合、まずはパソコン等をネットワークから切り離し、速やかに情報企画課IT最適化係に報告し、対応を協議すること！

（1）発見および報告

◆不正プログラムの存在は多くの場合、ウイルス対策ソフトやネットワークの監視、メール等を受信した外部からの通知により発覚する。

	事故事例	発覚のきっかけ
1	ウイルスに感染し、パソコンを不正操作され、パソコン内の重要情報が悪意のある第三者に搾取された	・自己申告／内部発見 ・外部からの指摘（風評を含む）
2	ウイルスに感染し、重要情報がWeb サイトに掲載され、不特定多数の人に閲覧可能な状態になった	

（2）初動対応

◆何の情報がどの程度含まれていたのか、暗号化やアクセス制限の有無を確認する。

事実関係を整理する	
(1) ウイルス感染した当事者は誰か？ (2) 何がウイルス感染したのか？ (3) ウイルス感染により漏えいした情報は何か？ (4) いつウイルス感染したのか？ (5) どこでウイルス感染したのか？ (6) なぜウイルス感染したのか？ (7) ウイルス感染が発覚した理由は何なのか？	a) 誰の情報か？ b) 何の情報か？ c) いつ頃の情報か？ d) 情報の量（件数）はどのくらいか？ e) どのような形で保存されていたか？ （暗号化／平文、HDD 保護、パスワード保護など）

◆不正プログラムの存在が確認された場合は、直ちにシステムの使用を停止し、システムから不正プログラムの除去などの対応を行う。

◆不正プログラムの種類が特定できる場合は、ウイルス対策ベンダなどの情報に基づき対処する。

	応急処置例	**留意点**
1	ウイルス感染したパソコンの特定	
2	ウイルス感染したパソコンのネットワークからの切り離し	

（3）調査

◆重要なデータをいったん外部メディアにバックアップする。バックアップには不正プログラムが混入している可能性も高いので取扱いに注意する。

◆パソコンに残されたデータやアクセスの履歴から漏えいした情報を特定する。

被害の重要度を判定する
(1) 漏えいした情報区分は？　個人情報（分類Ⅰ）／行政情報（分類Ⅱ Ⅲ）／一般情報（分類Ⅳ） (2) 漏えいした情報の保護策は、何を実施していたか？ (3) 影響はどこにあるか？（県民／行政／企業） (4) 管理上の問題点は？

3. 事故のタイプ別対応のポイント
3-5 不正プログラム

（4）通知・報告・公表等
◆漏えい情報に個人情報が含まれる場合には本人に通知し謝罪する。
◆規模や影響範囲が大きい場合は経緯を公表する。

（5）抑制措置と復旧
◆被害にあったパソコンは念のためOS からインストールしなおした方が良い。
◆プログラムもバックアップから戻さず、再インストールしなおした方が良い。
◆バックアップのデータについて、最新のウイルス定義ファイル等を使用して検査し復旧する。

	二次被害防止策例	留意点
1	ウイルス名の特定と駆除	・第三者からの情報回収該当情報を保持または掲載する第三者が情報回収に応じてくれない場合の対応
2	脆弱性の除去	
3	漏洩した情報の回収	
4	ID、パスワードが含まれる場合は、アクセス権限停止	

3. 事故のタイプ別対応のポイント
3-6 不正アクセス

※不正アクセスの疑いがある場合、まずはサーバ等の機器をネットワークから切り離し、速やかに情報企画課IT最適化係に報告し、対応を協議すること！

（1）発見および報告

◆不正アクセスの多くは、インターネットに接続しているサーバに対して行われ、ログの確認やセキュリティ対策機器の警報によって発見されることが多い。

◆重要な情報が格納されているパソコンやサーバに対する不正アクセスが確認された場合は、情報漏えいの危険性があるので対策が必要。

◆不正アクセスが明らかな場合は警察に相談します。

	事故事例	発覚のきっかけ
1	Web でのID パスワードを不正利用され、情報を他のサイトに掲示された	・自己申告／内部発見 ・外部からの指摘（風評を含む）
2	Web でのぜい弱性を悪用し不正アクセスされ、非公開情報を搾取された	
3	Web アプリケーションのぜい弱性を悪用され、データベースサーバの非公開情報を搾取された	
4	Web アプリケーションのぜい弱性を悪用され、Web サーバにウイルスを埋め込まれた	

（2）初動対応

◆何の情報がどの程度含まれていたのか、暗号化やアクセス制限の有無を確認する。

事実関係を整理する	
(1) 不正アクセスした当事者は誰か？ (2) 何を不正アクセスされたのか？ (3) 不正アクセスされた情報は何か？ (4) いつ不正アクセスが行われたのか？ (5) どこで不正アクセスが行われたのか？ (6) なぜ不正アクセスが発生したのか？ (7) 不正アクセスが発覚した理由は何なのか？	a) 誰の情報か？ b) 何の情報か？ c) いつ頃の情報か？ d) 情報の量（件数）はどのくらいか？ e) どのような形で保存されていたか？ （暗号化／平文、HDD 保護、パスワード保護など）

◆不正アクセスによって個人情報や機密情報が漏えいする危険性が確認された場合は、直ちにネットワークから切り離してサービスを停止するなどの処置が必要となる。

◆アカウント情報などが漏えいした場合は、アカウント停止などの緊急処置を行う。

	応急処置例	**留意点**
1	不正アクセスを受けた機器(サイト)のネットワークからの切り離し	・不正アクセスされた原因、経路を特定せずに、代替サイトを立ち上げると、再び不正アクセスされる可能性が高い
2	不正アクセスを受けた機器（サイト）の停止	
3	代替サイトの立ち上げ	

3. 事故のタイプ別対応のポイント
3-6 不正アクセス

（3）調査

◆不正アクセスの場合、機器に残された記録は重要な証拠となるため、内容が変更されたり損なわれたりしないよう証拠保全の措置をとる。

◆どのようにして侵入が行われたのか、どういった情報にアクセスした形跡があるかなどについて調査する。

被害の重要度を判定する
(1) 漏えいした情報区分は？　個人情報（分類Ⅰ）／行政情報（分類ⅡⅢ）／一般情報（分類Ⅳ） (2) 漏えいした情報の保護策は、何を実施していたか？ (3) 影響はどこにあるか？（県民／行政／企業） (4) 管理上の問題点は？

（4）通知・報告・公表等

◆個人情報にアクセスされた可能性がある場合は、その範囲を特定し本人に通知し謝罪する。

◆規模が大きい場合は公表を検討する。

（5）抑制措置と復旧

◆侵入されたサーバ等の内容をバックアップし、再発防止措置を行った上でサービスを復旧する。

◆アカウント情報等が漏えいした場合には、アカウントの再発行やパスワードの変更等の措置を行う。

	二次被害防止策例	留意点
1	漏洩した情報の回収	・第三者からの情報回収該当情報を保持または掲載する第三者が情報回収に応じてくれない場合の対応
2	Webサーバ設定の見直し	
3	ID、パスワード、アクセス権の見直し	
4	サーバ、Webアプリケーションの脆弱性の除去