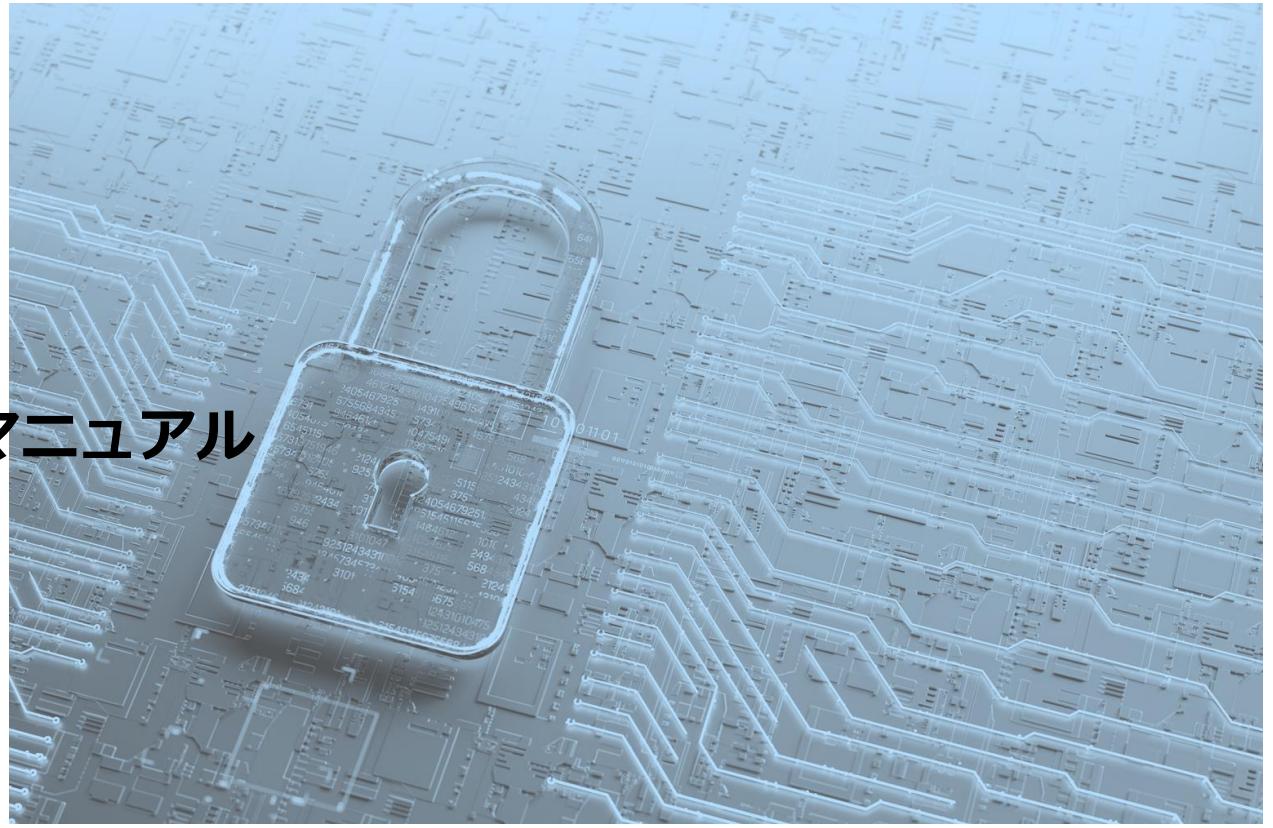
サイバーセキュリティ対策
インシデント(※)チェックリストマニュアル

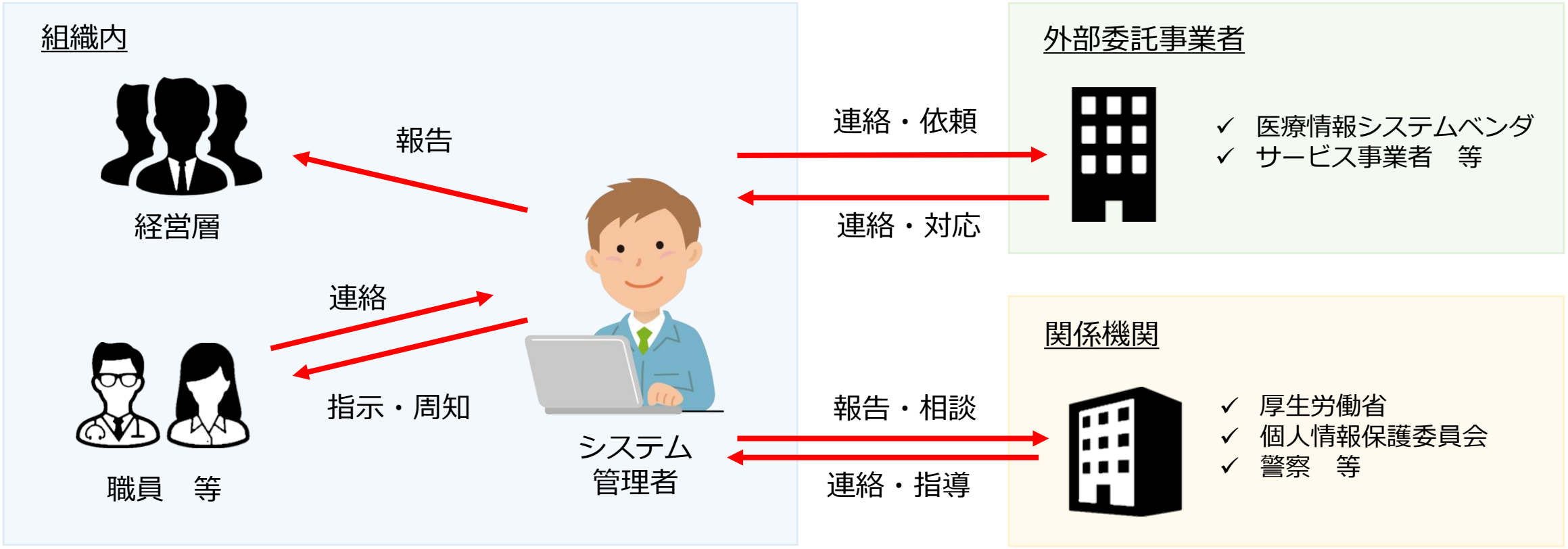


（※）インシデント：セキュリティインシデントのこと。望まない又は予期しない、単独又は一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。

徳島県　保健福祉部　医療政策課

インシデント発生時のシステム管理者の役割

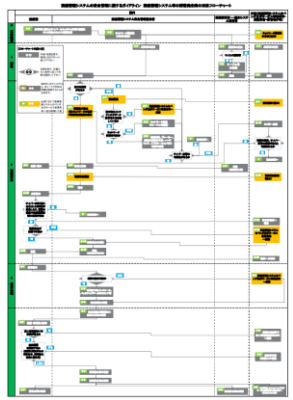
インシデント発生時は、影響や被害を最小限に抑えるために、より迅速な対応が求められます。そのため、システム管理者だけではなく、経営者や職員、必要に応じて、外部委託事業者等との連携が必要です。



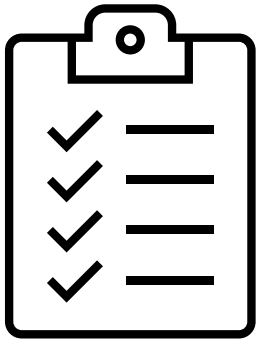
インシデント対応

　インシデント発生時に、漏れなく必要な対応がとれていることを確認できるよう、**インシデントチェックリスト**を活用しましょう。また、インシデントチェックリストは、医療情報システム等の障害発生時の対応フローチャート（※）の流れに対応して作成しています。合わせて確認しましょう。

インシデント発生



障害発生時の
対応フローチャート



インシデント
チェックリスト

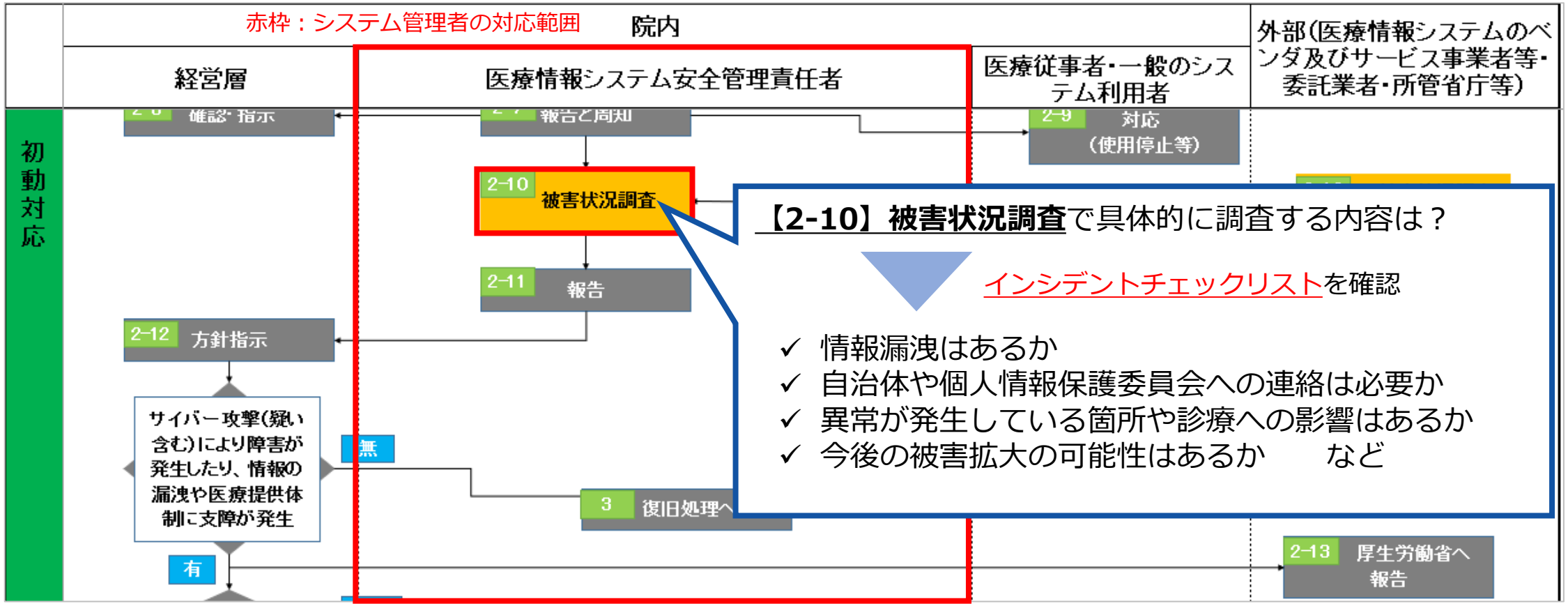
対応完了

（※）「医療情報システム等の障害発生時の対応フローチャート」（厚生労働省）
https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html

医療情報システム等の障害発生時の対応フローチャートとチェックリストの対応付け

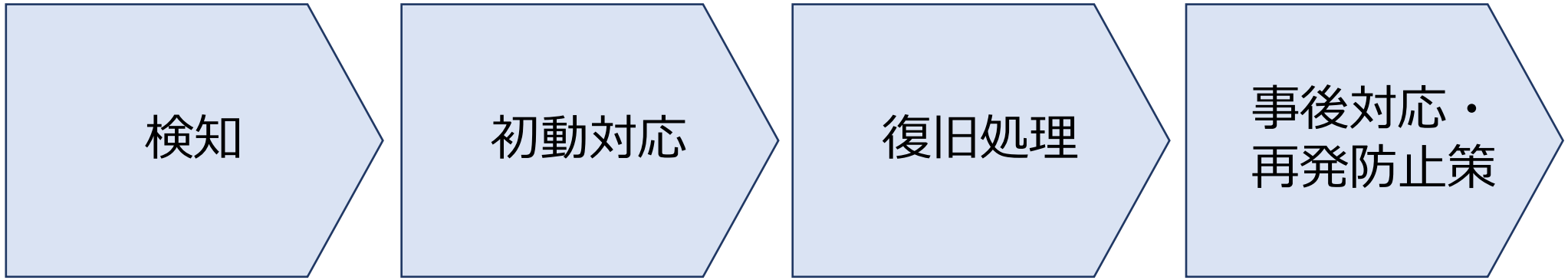
医療情報システム等の障害発生時の対応フローチャートは、緊急時に各役割が行うべき手順を可視化して整理しています。番号順に対応を進める際、具体的に行動する内容がインシデントチェックリストに記載してあります。

【医療情報システム等の障害発生時の対応フローチャート】



インシデント対応の流れ

インシデント対応は、以下のような流れで進んでいきます。



✓異常等の検知
✓端末の隔離
✓連絡

✓被害範囲の確認
✓保守事業者等への
依頼
✓システムの調査
✓外部機関への報告

✓復旧指示
✓復旧対応
（※バックアップ
からの復元）

✓再発防止
✓外部への公表

検知（1/3）

フローチャート

【1-1】
異常等の検知

インシデントチェックリスト

―――発生事象ケース、発生事象――――――――――――――――――――――――――――――――

■ 異常等を認識した場合、または、職員等から連絡があった場合、どのような事象であるか確認してください。「発生事象ケース」の事象に当てはまる場合は、チェックをつけ、当てはまらない場合は、「発生事象」に事象を記載してください。

（例）

電子カルテシステムで患者情報を閲覧できなくなった！

・・・
☑ファイルが暗号化されて開けない。脅迫文が表示された。
　ランサムウェア攻撃と判断して下さい。
□アカウントがロックされてパソコンにログインできない。
・・・

―――発生ネットワーク――――――――――――――――――――――――――――――――

■ 異常等を認識した端末等は、どこのネットワークに属しているか確認し、チェックを付けてください。

（例）

電子カルテ端末の場合

☑診療系ネットワーク
・・・

診療系のネットワークでウイルスが拡散してしまう可能性あり

検知（2/3）

フローチャート

【1-1】
異常等の検知

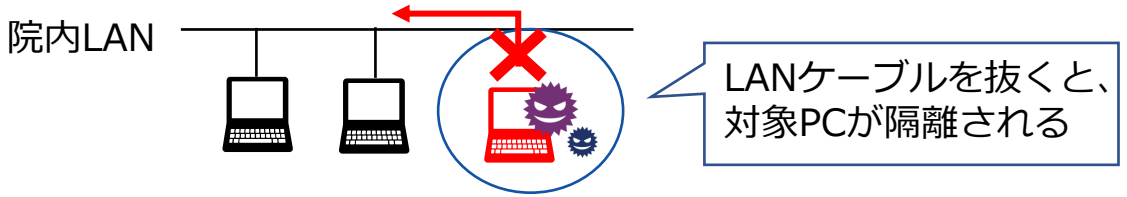
【1-4】
確認

インシデントチェックリスト

緊急措置

■ **<u>ウイルス感染（疑い含む）の場合</u>**は、対象パソコンのLANケーブルを抜き、ネットワークから切り離していることを確認してください。切り離していなければ、 LANケーブルを抜くことを指示してください。（無線LANの場合は、Wi-Fiをオフにする）

➢ **ウイルスの拡散**を防ぐことができます。



LANケーブル

緊急措置、発生状況

■ 証拠保全のため、対象PCや機器の**電源を停止しない**よう張り紙をしたり、発生事象の写真撮影等を行ってください。

➢ PCの電源を切ると、**調査に必要なログが消失する**場合があります。

■ 類似の事象が起こっていないか、**他の職員にも確認**してください。

➢ メールによる攻撃の場合は、他の職員にも届いている可能性があります。

検知（3/3）

フローチャート

【1-4】
確認

インシデントチェックリスト

―――発生状況――

■ 対象の職員へのヒアリング等により、以下のような事項を具体的に確認してください。

【不審メールによるウイルス感染が疑われる場合の記載例】

報告事項	ヒアリング内容	ポイント
いつ発生したか（日時）	2023年1月10日 14:00 NG例：１～２週間前	発生日時が具体的であれば期間が限定できるため、調査しやすくなる。
どこで発生したか	○○部の情報系端末（端末番号XXXX）	事故の発生した部署や該当機器等が具体的であれば、影響する範囲が特定しやすい。
どのような操作を行ったか	不審なメールの添付ファイルを開いて、マクロを有効化した（ウイルスは検知せず） NG例：不審なメールを開いた	「不審なメールを開いた」だけでは、適切な対応の判断ができないため、**どのような操作を行ったか詳細にヒアリング**する。

初動対応（1/4）

フローチャート

【2-2】
医療情報システムのベンダ及びサービス事業者等へ確認

【2-1】
原因調査

【2-3】
ネットワーク機器やケーブル等の調査

【2-4】
電源系統、ブレーカー、ハードウェア等の調査

インシデントチェックリスト

原因調査依頼

■ 必要に応じて、ベンダやサービス事業者に原因調査の依頼を行ってください。
- ➢ インシデント発生時に、落ち着いて対応できるよう、**外部委託事業者の連絡先一覧等を作成**し、手元に準備しておくことが望ましいです。

対応状況/調査状況

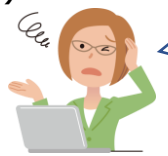
■ 以下のような事項を調査し、記載してください。

【調査内容】
- ✓ ネットワーク機器やケーブル等の問題かどうかの調査
- ✓ 電源やブレーカ等の電源系統の問題かどうかの調査
- ✓ 機器自体の故障、ハードウェア自体の故障の有無等の調査　　など

侵入経路確認

■ **サイバー攻撃（疑い含む）の場合**は、ネットワーク構成図等を使い、ウイルスがどこから侵入した可能性が高いか、確認してください。

（例）



急に電子カルテが閲覧できなくなったが心当たりはない。

・・・

☑その他
☑侵入経路不明

ネットワーク機器等が原因の可能性もある

初動対応（2/4）

フローチャート

【2-6】
被害拡大防止

【2-7】
報告と周知

インシデントチェックリスト

―――被害拡大防止――

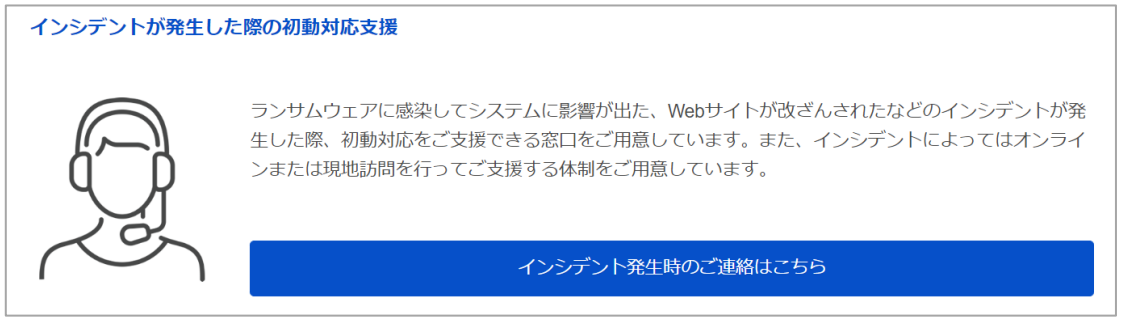
■ 被害拡大防止の対応を行ってください。

【ウイルス感染の場合の対応】

- ✓ バックアップデータを確認すること
- ✓ **バックアップデータをオフライン化**すること
- ✓ ネットワークの通信を遮断する
- ✓ ネットワーク停止や電子カルテシステム利用停止の判断を伝える　など

ランサムウェアの場合、
バックアップデータを暗号化される可能性がある

➢ 厚生労働省のホームページにはインシデント発生時に、初動対応を支援する窓口を設置しています。（※）



■ 発生した事象について、職員等に周知してください。

➢ **サイバー攻撃（疑い含む）の場合**は、**感染の疑いがある医療情報システムや機器等の使用の中止等を指示**してください。

（※）「インシデントが発生した際の初動対応支援」（厚生労働省）　https://mhlw-training.saj.or.jp/

初動対応（3/4）

フローチャート

【2-10】
被害状況調査

【2-14】
証拠保全の実施

インシデントチェックリスト

―――情報漏洩、被害状況等調査――――――――――――――――――――――――――――――――――――

■ 以下ような内容について確認し、**被害範囲を調査**してください。

【確認内容】
- ✓ 情報漏えいしている可能性はあるか
- ✓ 異常が発生している箇所はどこか
- ✓ 診療への影響はどのくらいあるか　など

■ **サイバー攻撃（疑い含む）の場合**、アクセスログの分析や情報の改ざん、暗号化の有無等から、情報漏えいの有無等を確認してください。

- ➢ **必要に応じて、ベンダやサービス事業者等へ協力依頼**をしましょう。

―――証拠保全――

■ **サイバー攻撃（疑い含む）の場合**は、以下のようなログが残っているか確認し保全してください。

- ➢ **必要に応じて、ベンダやサービス事業者等へ協力依頼**をしましょう。
- ➢ ログが残っていなかったり、サイバー攻撃を受けた時の状態が保たれていなければ、**原因の特定、被害範囲の特定が困難**になります。ログを取得して下さい。

【調査等を行う上で確認できることが望ましいもの】

- ✓ インターネットVPN機器のログ
- ✓ ファイアウォールのログ
- ✓ 対象パソコンのログ
- ✓ セキュリティソフトのログ　など

初動対応（4/4）

フローチャート

【2-13】
厚生労働省へ報告

【2-18】
警察への届け出

インシデントチェックリスト

―――関連機関連絡――

■ **<u>サイバー攻撃（疑い含む）場合</u>**は、厚生労働省等の**関係機関へ報告**を行ってください。

【報告先の例】

- ✓ 厚生労働省　医政局特定医薬品開発支援・医療情報担当参事官室
- ✓ 個人情報保護委員会
- ✓ 警察（徳島県警察等）
- ✓ 徳島県　保健福祉部　医療政策課　　など

➢ 厚生労働省のホームページには報告先が公開されています。（※）

医療機関等がサイバー攻撃を受けた際の厚生労働省連絡先

「医療情報システムの安全管理に関するガイドライン」では、医療機関等がサイバー攻撃を受けた（疑い含む）場合等の際には、厚生労働省等の所管省庁への連絡等、必要な対応を行うほか、そのための体制を整備する必要があることを示しています。

医療機関等がサイバー攻撃を受けた場合等の厚生労働省連絡先

医政局特定医薬品開発支援・医療情報担当参事官室
TEL:　03-6812-7837
MAIL:　igishitsu×mhlw.go.jp
※迷惑メール防止のため、メールアドレスの一部を変えています。
「×」を「@」に置き換えてください。

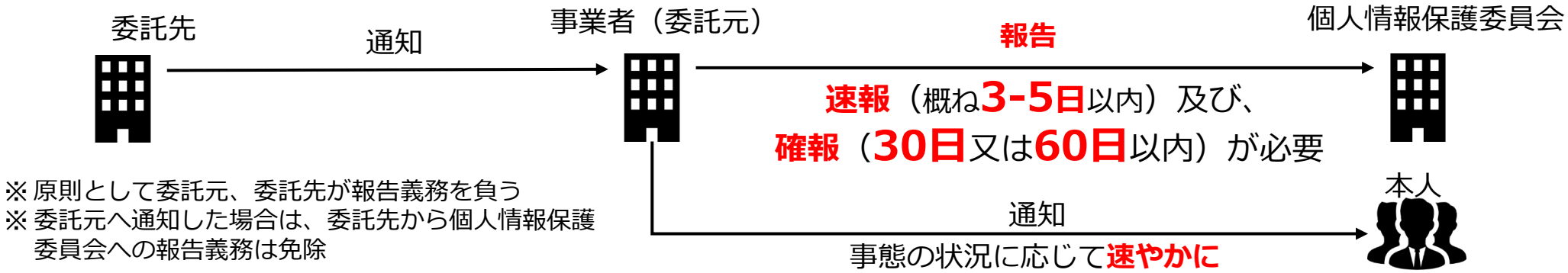
（※）「医療機関等がサイバー攻撃を受けた際の厚生労働省連絡先」（厚生労働省）
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

【参考】個人情報保護法における報告義務等

個人データの**漏えい、滅失、毀損その他個人データの安全の確保に係る事態**であって「**個人の権利利益を害するおそれが大きいもの**」として、次の事態が発生し、又は発生したおそれがある場合は、**個人情報保護委員会への報告及び本人への通知義務**（※）が発生します。

個人の権利利益を害するおそれが大きいもの	個人データの件数
不正の目的をもって行われたおそれがある個人データ	**1人**以上
要配慮個人情報が含まれる個人データ	
不正に利用されることにより**財産的被害**が生じるおそれがある個人データ （例：クレジットカード番号やインターネットバンキングのＩＤ・パスワード等）	
個人データに係る本人の数が**1,000人を超える**	**1,000人**を超える

個人の権利利益を害するおそれが大きい漏えい等の事態が発生した場合の報告の流れ



※原則として委託元、委託先が報告義務を負う
※委託元へ通知した場合は、委託先から個人情報保護委員会への報告義務は免除

（※）個人情報保護員会への報告フォーム：https://www.ppc.go.jp/personalinfo/legal/leakAction/

【参考】個人情報保護法における報告義務等

漏えい、滅失、毀損とは、次のことを主に指します。

漏えい 機密性に相当	**個人データが外部に流出することをいう**。例えば・・・ • 個人データが記載された書類を第三者に**誤送付**した場合 • 個人データを含むメールを第三者に**誤送信**した場合 • インターネット上で個人データの**閲覧が可能な状態**となっていた場合（閲覧されていない場合を除く）
滅失 可用性に相当	**個人データの内容が失われることをいう**。例えば・・・ • 個人情報データベース等から出力された氏名等が記載された帳票等を**誤って廃棄**した場合（バックアップがある場合等は除く） • 個人データが記載又は記録された書類・媒体等を社内で**紛失**した場合
毀損 完全性に相当	**個人データの内容が意図しない形で変更されることや、内容を保ちつつも利用不能な状態となることをいう**。例えば・・・ • 個人データの内容が**改ざん**された場合 • ウイルス等により個人データが暗号化され、**復元できなくなった**場合 ※当該データと同じデータが他に保管されている場合は毀損に該当しません。

【参考】関連機関への報告

厚生労働省、個人情報保護委員会への報告の他、各種届出制度が定められています。

コンピュータ 不正アクセス届出制度	根拠	：コンピュータ不正アクセス対策基準 ※事後対応として、「不正アクセス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること」を規定
	届出先	：独立行政法人 情報処理推進機構
	参考URL	：https://www.ipa.go.jp/security/outline/todokede-j.html
コンピュータ ウイルス届出制度	根拠	：コンピュータウイルス対策基準 ※事後対応として、「ウイルス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること」を規定
	届出先	：独立行政法人 情報処理推進機構
	参考URL	：https://www.ipa.go.jp/security/outline/todokede-j.html
ソフトウェア等の 脆弱性関連情報に 関する 届出制度	根拠	：ソフトウエア製品等の脆弱性関連情報に関する取扱規程 ※「発見者は、受付機関に脆弱性関連情報を届け出る」を規定 ※「情報セキュリティ早期警戒パートナーシップガイドライン」も関連
	届出先	：独立行政法人 情報処理推進機構　（受付機関）
	参考URL	：https://www.ipa.go.jp/security/vuln/report/index.html

復旧処理/事後対応・再発防止策

フローチャート

【3-3】
再設定や再インストール、バックアップデータのリストア等

【3-4】
復旧結果の確認

【4-5】
再発防止策の検討

【4-6】
再発防止策の周知

インシデントチェックリスト

――――復旧処理――

■ **復旧処置**を記載してください。（ベンダが実施した処置でも可）

【記載内容の例】

- ✓ ソフトウェアに問題が発生していたため、設定変更を行い、再インストールを行った。
- ✓ 再インストール後に、ソフトウェアのアップデート、バックアップデータのリストアを実施した。

■ 復旧したシステムや機器が正常に動作することを確認した後、復旧処理の内容を経営者等に報告し、承認をもらってください。

――――事後対応・再発防止策――――――――――――――――――――――――――――――――――――――

■ **再発防止策**を検討し、記載してください。

【記載内容の例】

- ✓ ネットワーク機器の脆弱性が原因であったため、ネットワーク機器の脆弱性対応を保守契約内に含める。

■ 再発防止策に対して、経営者等からコメント、承認をもらい、再発防止策を実施してください。