福県医発第 １４４ 号（地）

平成１７年４月１５日

各 医 師 会 長 殿

福 岡 県 医 師 会
会長 竹 嶋 康 弘

ＯＲＣＡプロジェクト　セキュリティポリシーについて

標記の件につきまして、日本医師会総合政策研究機構所長より別添のとおり通知がありましたのでお知らせいたします。

本件は、本年４月１日より施行されました個人情報保護法に伴い、ＯＲＣＡプロジェクトにおいての安全管理方針が定められた旨の通知であります。

なお、本件につきましては、日医標準レセプトソフト利用医療機関へは、日本医師会総合政策研究機構より直接通知されております。

小郡三井医師会より　　**担当理事　友清　明**

写

(総研-5)
2005年 4月7日

都道府県医師会長　殿

日本医師会総合政策研究機構
所長　櫻井 秀也

ORCAプロジェクト　セキュリティポリシーについて

拝啓　時下益々のご清祥のこととお喜び申し上げます。

日頃より、当会が進めているORCAプロジェクトへのご理解、ご協力を賜り厚く御礼申し上げます。

さて、2005年4月1日から、個人情報保護法が全面施行されるにあたり、ORCAプロジェクトにおいての安全管理方針を定めました。

内容として、コンピュータを利用する際の安全管理や、日医標準レセプトご利用の医療機関と、認定サポート事業所の間に結ぶ、守秘義務に関する条項等を述べております。これらの内容を両者に遵守していただくことにより、安心してご利用できる環境を整えるためのものであります。

これに伴い、日医標準レセプトソフトご利用医療機関、並びに、日医認定サポート事業所に対して、別紙のとおり文書をお送りしましたので、ご参考までに、ご案内申し上げます。

敬具

別紙
・日医標準レセプトソフトご利用医療機関　宛
　ORCAプロジェクト　セキュリティポリシーについて
・認定サポート事業所　宛
　ORCAプロジェクト　セキュリティポリシーについて

以上

ORCA プロジェクト

医療機関向け　セキュリティポリシーについて

2005 年 3 月 30 日

1．「個人情報の保護に関する法律[1]（略称：個人情報保護法）」、「不正アクセス行為の禁止等に関する法律[2]（略称：不正アクセス禁止法）」ならびに「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律[3]（略称：プロバイダ責任法）」等について、理解を深め、情報システムを利用する医療機関に求められる対策をたて、組織的かつ定期的に遵法状況の確認を行ってください。

2．もし上記３法に抵触する等、個人の情報の漏洩や漏洩の危険性が高いと判断される状態があれば、速やかに防止・改善に努めるとともに、速やかに保守契約を行っている認定サポート事業所への報告を行い、再発防止の対策を講じてください。

3．日医標準レセプトソフトを含むシステムの設定や保守管理を契約している認定サポート事業所との間で、個人情報保護のための守秘義務と罰則規定等を含めた契約を締結してください。契約の雛形は、例として、添付してある「守秘義務に関する業務委託契約の条項」にありますので参考にしてください。

4．日医標準レセプトソフトのホームページに掲示された「エンドユーザー向けセキュリティの設定[4]」や各所から出ている安全管理指針[5]を充分に理解し、従業員への教育・啓発に努め、セキュリティポリシーを遵守してください。職員共通のアカウントやパスワードなどは決して使用しないでください。

5．日医標準レセプトソフトを含むシステムにおいて使用している OS やアプリケーションのセキュリティアップデートに関しては、認定サポート事業所と連携して常に最新のものを入れ、安全を計ってください。

1　内閣府　個人情報の保護に関する法律
http://www5.cao.go.jp/seikatsu/kojin/

2　総務省　不正アクセス行為の禁止等に関する法律
http://www.soumu.go.jp/joho_tsusin/security/kiso/k05_09.htm

3　総務省　プロバイダ責任の概要
http://www.soumu.go.jp/joho_tsusin/top/denki_h.html

4　ORCAプロジェクトホームページ　「ネットワークとセキュリティの設定」
http://www.orca.med.or.jp/orca/tec/network_cecurity/security.rhtml#01_00

5　厚生労働省　「医療情報システムの安全管理に関するガイドライン」
http://www.mhlw.go.jp/shingi/2005/03/s0331-8.html

６．診療業務の途中でも、日医標準レセプトソフトの端末の設置されている席を外すときには必ず、ログアウトして、引き続き他の人に利用されないように注意してください。

７．日医標準レセプトソフトを搭載しているサーバーや端末には、その他のアプリケーションをなるべくインストールしないでください。やむをえず、インストールが必要なアプリケーションについては、認定サポート事業所等と相談して自己責任において当該新規アプリケーションの利用を決定してください。

８．日医標準レセプトソフトの接続されている LAN 内には、診療にかかわらない機器を接続しないよう注意してください。

９．従業者（派遣を含む）に対して、個人情報保護法等に関する教育ならびに指導監督を定期的に行ってください。

１０．日医標準レセプトソフトの端末にアクセスできる職員は必要最小限に留めておき、利用の日誌を記録してください。

１１．個人情報保護のためには、インターネットに接続していなくても日常運用は可能ですので、単体での利用を認定サポート事業所と相談して行ってください。ただし業務メニュー画面のニュースやお知らせは見えなくなりますので、ホームページやメーリングリストによって最新情報を取得してください。

１２．日医標準レセプトソフトの動作や表示に関して異常や不安を感じたときには速やかに契約している認定サポート事業者に連絡をして、対策を立ててください。

以上

守秘義務に関する業務委託契約の条項

以下では、甲を医療機関、乙を事業者としています。

第〇条（再委託）

乙は、本件業務の一部又は全部を第三者へ再委託してはならない。ただし、甲が他の事業者（乙と同程度又はそれ以上の水準でセキュリティ対策及び個人情報保護対策を講じている事業者であって、乙がそのことを保証する場合に限る）に再委託することを事前に承諾した場合は、この限りではない。

第〇条（秘密保持）

1　秘密情報とは、契約の有効期間中に本件業務に関連して、乙が甲から開示を受ける業務管理等（技術上のものも含む）に関する有形無形の情報（本件業務に関連して、甲から直接的または間接的に乙に開示されるすべての情報を含む）であり、次の各号のいずれかに該当するものをいう。

（１）患者情報等個人のプライバシーに関する情報

（２）秘密である旨告知されたうえで開示された業務管理情報、技術資料、図面及びその他の関係書類並びに電子媒体を含む有体物により開示された情報

（３）本件業務に関して作成された議事録

（４）本件業務に関する、ＦＡＸ・電子メール・郵便等による通信内容

（５）本件業務に関し口頭で伝えられた情報で、事前又は事後に、甲が秘密であることを通知した情報

2　前項の規定にかかわらず、次の各号の一つに該当する情報については、秘密情報として取り扱わないものとする。

（１）開示時に既に公知であった情報、又は既に乙が保有していた情報

（２）開示後、乙の責によらず公知となった情報

（３）乙が正当な権限を有する第三者から適法に入手した情報

（４）乙が独自に開発・知得した情報

（５）法令に基づき政府機関や裁判所に開示する必要のある情報

3　本件業務に基づき甲が乙に開示する秘密情報について、乙は、次の各号の義務を負う。

（1）乙は、善良な管理者の注意義務をもって秘密情報を管理すること

（2）甲の承認なく秘密情報を複写、又は、第三者に提供若しくは貸与しないこと

（3）本件業務の目的以外に秘密情報を使用しないこと

（4）本件業務が終了した場合又は甲が要請した場合、当該秘密情報に関する一切資料及び媒体を遅滞なく返却または破棄すること

第〇条（個人情報の保護）

1　本契約における「個人情報」とは、個人に関する情報であって、当該情報に含まれる氏名､生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む｡）をいう。

2　乙は、本件業務に関して、本人の同意なく、当該個人情報を収集したときの目的の範囲（甲から明示された場合はその範囲、それ以外の場合は社会通念上合理的と考えられる範囲）を超えて、個人情報を使用してはならない。

3　乙はいかなる場合であっても甲から提供された個人情報を第三者提供してはならない。

4　乙は、個人情報の漏えい、滅失及び毀損防止その他の個人情報の適正な管理のために必要な措置を講じなくてはならない。

5　その他個人情報の取り扱いについて、乙は甲から指示を受けて適切に対処するものとする。

第〇条（損害賠償）

乙が、前３条に違反して甲又は第三者に損害を生じせしめた場合、その損害（当該紛争に係る一切の費用であって、賠償金、訴訟費用及び弁護士費用を含むがこれに限定されない）を賠償する責を負う。乙の従業員又は乙の再委託先（甲の事前の了解があったか否かは問わない）による行為を原因とする場合も乙はその責を負うものとする。

以上

ORCA プロジェクト

サポート事業所向け　セキュリティポリシー

2005 年 3 月 30 日

1．「個人情報の保護に関する法律[1]（略称：個人情報保護法）」の趣旨を十分理解するとともに「不正アクセス行為の禁止等に関する法律[2]（略称：不正アクセス禁止法）」ならびに「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律[3]（略称：プロバイダ責任法）」等を厳格に遵守し、日医標準レセプトソフトの認定サポート事業所に求められる対策を立て、組織的かつ定期的に遵法状況の確認を行うこと（医療機関の実データに当該機関からの許可なくアクセスすることは不正アクセス行為であることを改めて認識されたい）。

2．関連法令に違反する行為又は関連法令の趣旨に反する行為により個人の情報の漏洩や漏洩の危険性が高いと判断される状態があれば、速やかに防止・改善に努めるとともに、当該危険状態を発見した日を含め、３営業日以内に日医総研への報告を行うこと。当該危険状態を看過したり、発見したにもかかわらず放置することや、報告の著しい遅延などを認めた際には、認定サポート事業所の認定を取り消すことがある。

3．日医標準レセプトソフトを含むシステムの設定や保守管理を受託している医療機関との間には、必ず個人情報保護のための守秘義務と罰則規定等を含めた契約を締結すること。契約の雛形は、添付してある「守秘義務に関する業務委託契約の条項」を参考にされたい。

4．日医標準レセプトソフトのホームページに掲示された「ネットワークとセキュリティの設定[4]」を遵守すると共に各所から出ている安全管理指針[5]を熟知し、医療機関のエンドユーザーへの教育・啓発に努めること。

1　内閣府　個人情報の保護に関する法律
http://www5.cao.go.jp/seikatsu/kojin/

2　総務省　不正アクセス行為の禁止等に関する法律
http://www.soumu.go.jp/joho_tsusin/security/kiso/k05_09.htm

3　総務省　プロバイダ責任の概要
http://www.soumu.go.jp/joho_tsusin/top/denki_h.html

4　ORCAプロジェクトホームページ　「ネットワークとセキュリティの設定」
http://www.orca.med.or.jp/orca/tec/network_cecurity/security.rhtml

5　厚生労働省　「医療情報システムの安全管理に関するガイドライン」
http://www.mhlw.go.jp/shingi/2005/03/s0331-8.html

５．日医標準レセプトソフトを含むシステムにおいて使用している OS やアプリケーションのセキュリティアップデートに関しては常に最新のものを入れ、安全を計ること。

６．ベンダーから日医標準レセプトソフトを含むシステムの設置された医療機関へのネットワーク接続は、日医標準レセプトソフトの維持・保守にかかわるものに限り、必要最小限にすること。

７．ベンダーから医療機関へのネットワーク接続を行う者の権限をベンダーの機関内ルールなどにより明確にし、どの従業員が何時どこに接続し、何を行ったかなどのログを記録しておくこと。VPN 等で医療機関に接続する場合も同様とする。

８．医療機関の日医標準レセプトソフトを含むシステムへのアクセス権限のある担当者が権限変更・転勤・配置転換・退職などにより変更された場合、すみやかにそのアカウントやパスワードを削除・変更し、権限を失った者がネットワークやシステムにアクセスできないような措置をとること。

９．日医標準レセプトソフトを含むシステムの検証等に患者データが必要な場合は、ダミーのテストデータを用いること。患者の実データは必要最小限の時にかぎって、取り扱うものとし、実データを用いる場合は、書面により医療機関の承諾を得ること。また、実データ使用後には削除・返却等の責任を持って行い、医療機関側に報告をしておくこと。

１０．患者の実データは原則として当該医療機関のシステムからいかなる方法でも移動させないこと。最も個人情報漏洩の事故の多いノートパソコンや USB メモリなど移動可能な媒体に格納しないこと。やむを得ず格納して移動する場合には暗号化をしておくなど対策を立てておくこと。

１１．患者の実データを公開されたネットワーク領域に置かないこと。無線 LAN も公開されたネットワークであると考えること。

以上

守秘義務に関する業務委託契約の条項

以下では、甲を医療機関、乙を事業者としています。

第〇条（再委託）

乙は、本件業務の一部又は全部を第三者へ再委託してはならない。ただし、甲が他の事業者（乙と同程度又はそれ以上の水準でセキュリティ対策及び個人情報保護対策を講じている事業者であって、乙がそのことを保証する場合に限る）に再委託することを事前に承諾した場合は、この限りではない。

第〇条（秘密保持）

1　秘密情報とは、契約の有効期間中に本件業務に関連して、乙が甲から開示を受ける業務管理等（技術上のものも含む）に関する有形無形の情報（本件業務に関連して、甲から直接的または間接的に乙に開示されるすべての情報を含む）であり、次の各号のいずれかに該当するものをいう。

（１）患者情報等個人のプライバシーに関する情報

（２）秘密である旨告知されたうえで開示された業務管理情報、技術資料、図面及びその他の関係書類並びに電子媒体を含む有体物により開示された情報

（３）本件業務に関して作成された議事録

（４）本件業務に関する、ＦＡＸ・電子メール・郵便等による通信内容

（５）本件業務に関し口頭で伝えられた情報で、事前又は事後に、甲が秘密であることを通知した情報

2　前項の規定にかかわらず、次の各号の一つに該当する情報については、秘密情報として取り扱わないものとする。

（１）開示時に既に公知であった情報、又は既に乙が保有していた情報

（２）開示後、乙の責によらず公知となった情報

（３）乙が正当な権限を有する第三者から適法に入手した情報

（４）乙が独自に開発・知得した情報

（５）法令に基づき政府機関や裁判所に開示する必要のある情報

3　本件業務に基づき甲が乙に開示する秘密情報について、乙は、次の各号の義務を負う。

（1）乙は、善良な管理者の注意義務をもって秘密情報を管理すること

（2）甲の承認なく秘密情報を複写、又は、第三者に提供若しくは貸与しないこと

（3）本件業務の目的以外に秘密情報を使用しないこと

（4）本件業務が終了した場合又は甲が要請した場合、当該秘密情報に関する一切資料及び媒体を遅滞なく返却または破棄すること

第〇条（個人情報の保護）

1　本契約における「個人情報」とは、個人に関する情報であって、当該情報に含まれる氏名､生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む｡）をいう。

2　乙は、本件業務に関して、本人の同意なく、当該個人情報を収集したときの目的の範囲（甲から明示された場合はその範囲、それ以外の場合は社会通念上合理的と考えられる範囲）を超えて、個人情報を使用してはならない。

3　乙はいかなる場合であっても甲から提供された個人情報を第三者提供してはならない。

4　乙は、個人情報の漏えい、滅失及び毀損防止その他の個人情報の適正な管理のために必要な措置を講じなくてはならない。

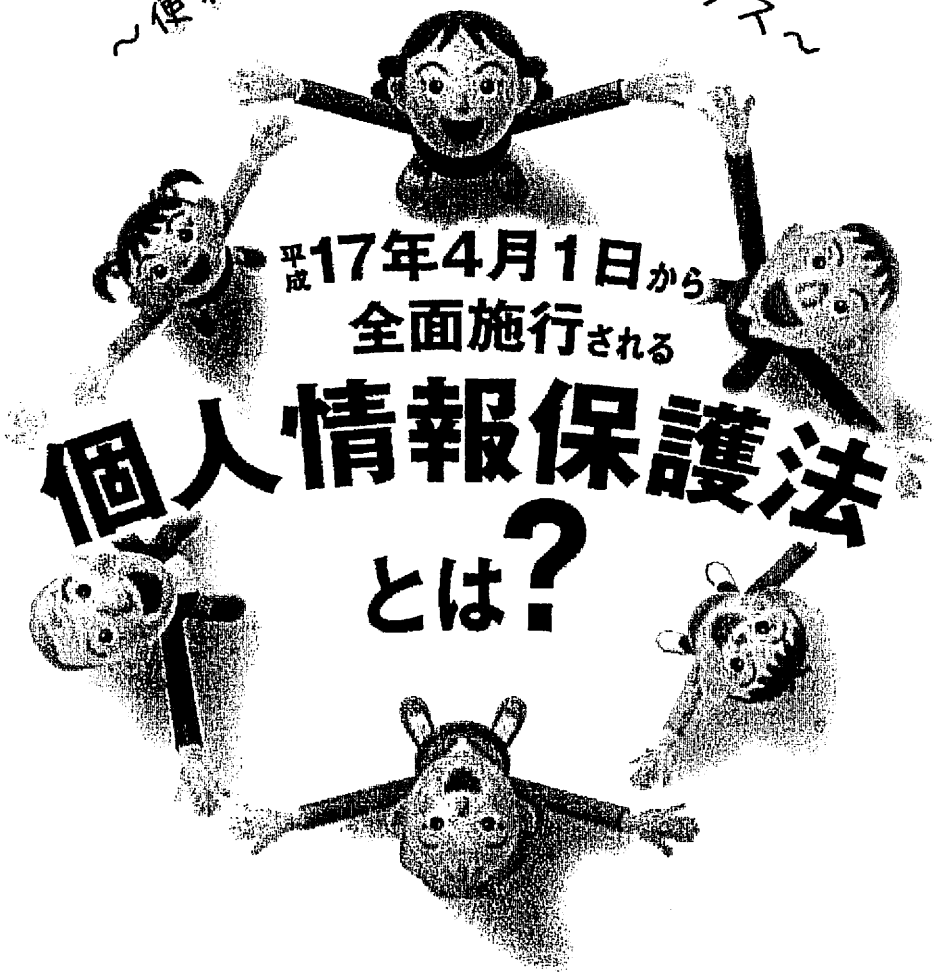
5　その他個人情報の取り扱いについて、乙は甲から指示を受けて適切に対処するものとする。

第〇条（損害賠償）

乙が、前３条に違反して甲又は第三者に損害を生じせしめた場合、その損害（当該紛争に係る一切の費用であって、賠償金、訴訟費用及び弁護士費用を含むがこれに限定されない）を賠償する責を負う。乙の従業員又は乙の再委託先（甲の事前の了解があったか否かは問わない）による行為を原因とする場合も乙はその責を負うものとする。

以上

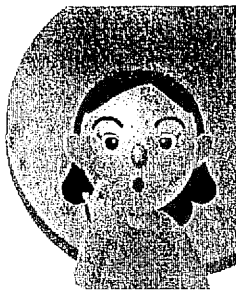
～便利なIT社会に安心をプラス～



平成17年4月1日から全面施行される 個人情報保護法とは？

家族構成　氏名　住所　年齢　学歴　職業　性別　メールアドレス

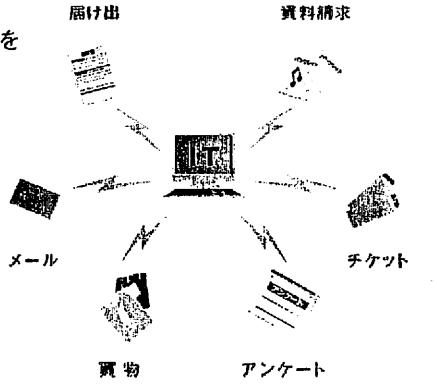
内閣府国民生活局



個人情報を保護する法律の必要性

経済・社会の情報化の進展を背景に

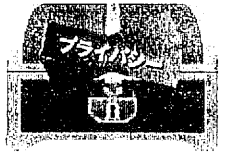
今日、「個人情報」を利用したさまざまなサービスが提供され、
私たちの生活は大変便利なものになっています。
その反面、「個人情報」が
誤った取扱いをされた場合、
個人に取り返しのつかない被害を
及ぼすおそれがあり、
国民のプライバシーに関する
不安も高まっています。



「個人情報」とは
個人に関する情報で、これに含まれる氏名、生年月日その他の記述等により、特定の個人を識別することができるものをいいます。

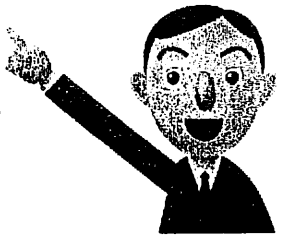
高度情報通信社会のメリットを安心して受けるために

このような状況を踏まえ、
「個人情報の保護に関する法律」が
平成15年5月に成立し、公布されました。
この法律では、国民が安心して
高度情報通信社会のメリットを享受できるよう、
個人情報の適正な取扱いを求めています。



平成17年4月1日から全面施行

個人情報保護法のポイント



ポイント1

個人情報の有用性に配慮しながら、
個人の権利や利益を保護することを目的としています。

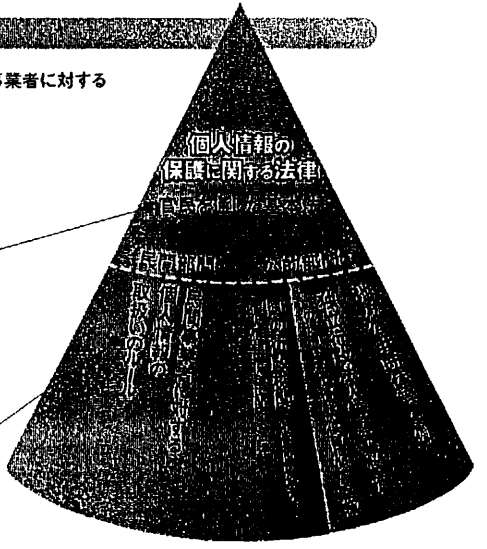
ポイント2

①この法律は、民間の事業者の個人情報の取扱いに関して
共通する必要最小限のルールを定めています。

②この法律の仕組みは、事業者が、事業等の分野の実情に応じ、
自律的に取り組むことを重視しています。

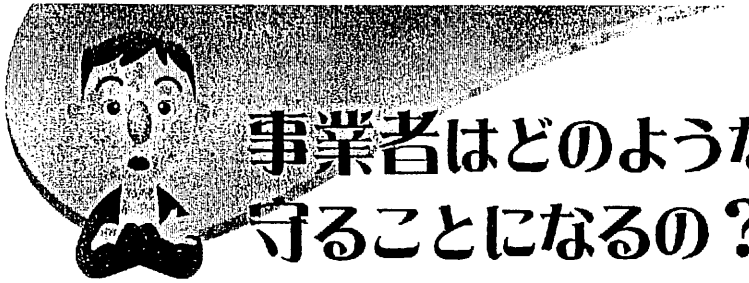
個人情報保護法制の体系イメージ

個人情報保護法は、官民を通じた基本法の部分と、民間の事業者に対する
個人情報の取扱いのルールの部分から構成されています。



- 基本理念
- 基本方針の策定
- 国の責務、施策
  - ●地方公共団体等への支援　●苦情処理のための措置等
- 地方公共団体の責務、施策
  - ●保有する個人情報の保護　●区域内の事業者等への支援
  - ●苦情の処理のあっせん等

- 個人情報取扱事業者の義務
  - ●利用目的による制限　●適正な取得　●安全管理措置
  - ●第三者提供の制限　●開示・訂正・利用停止　●その他
- 主務大臣（事業等所管官庁）による
  報告徴収、助言、勧告、命令



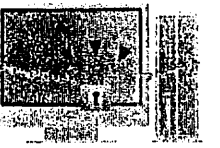
事業者はどのようなルールを守ることになるの？

個人情報取扱事業者※は次のようなルールを守らなければなりません。

利用・取得に関するルール

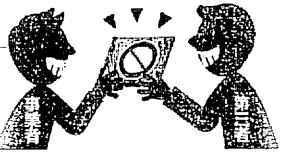
- 個人情報の利用目的をできる限り特定し、
  利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはなりません。
- 偽りその他不正な手段によって個人情報を取得することは禁止されます。
- 本人から直接書面で個人情報を取得する場合には、あらかじめ本人に利用目的を
  明示しなければなりません。間接的に取得した場合は、すみやかに
  利用目的を通知または公表する必要があります。

適正・安全な管理に関するルール



- 顧客情報の漏えいなどを防止するため、
  個人データ※を安全に管理し、従業者や委託先を監督しなければなりません。
- 利用目的の達成に必要な範囲で、
  個人データを正確かつ最新の内容に保つ必要があります。

第三者提供に関するルール

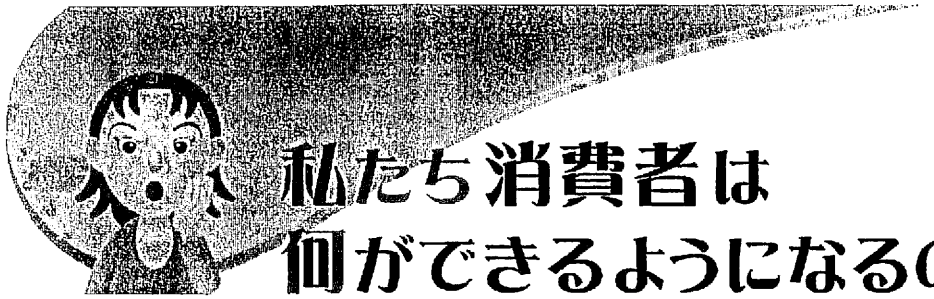


- 個人データをあらかじめ本人の同意を取らないで
  第三者に提供することは原則禁止されます。

開示等に応じるルール

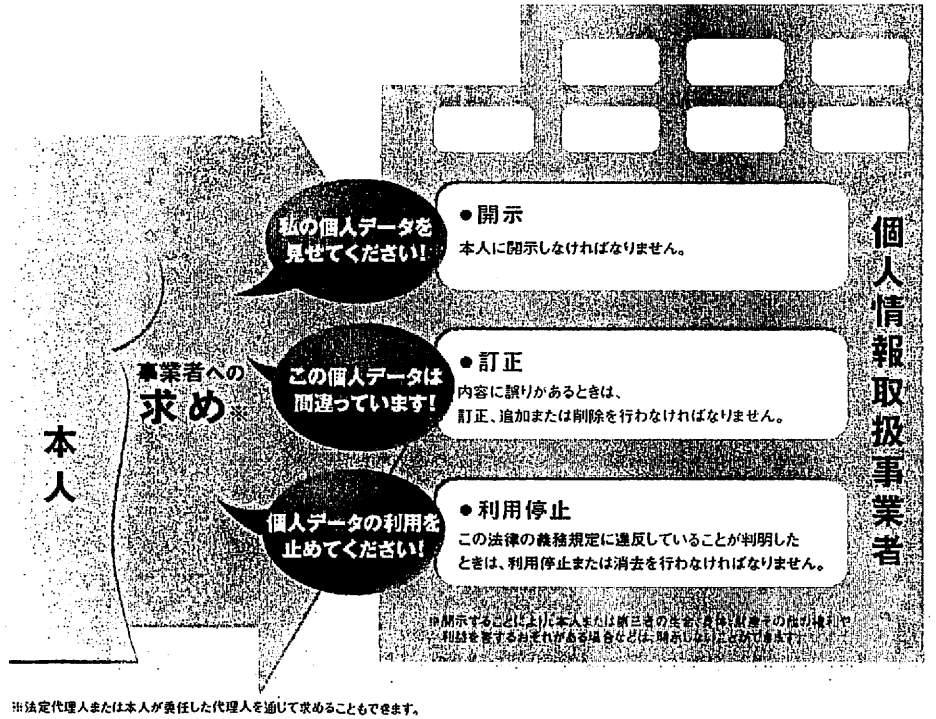
- 事業者が保有する個人データに関して、本人から求めがあった場合は、
  その開示、訂正、利用停止等を行わなければなりません。
- 個人情報の取扱いに関して苦情が寄せられたときは、
  適切かつ迅速に処理しなければなりません。

※「個人情報取扱事業者」とは、個人情報をコンピュータなどを用いて検索することができるよう体系的に構成した個人情報データベース等を事業活動に利用している事業者のことです。また、個人情報データベース等を構成する個人情報のことを「個人データ」といいます。

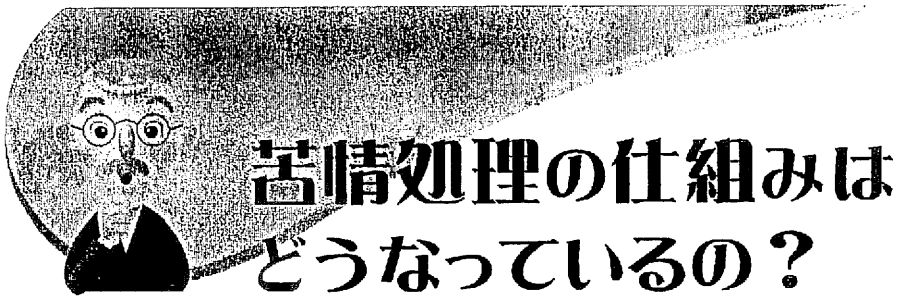


私たち消費者は何ができるようになるの？

個人情報保護法には、
事業者が保有する個人データに関して「本人が関与できる仕組み」が盛り込まれています。
この法律の全面施行（平成17年4月1日）により、
個人情報取扱事業者に対して、次の措置を求めることができます。



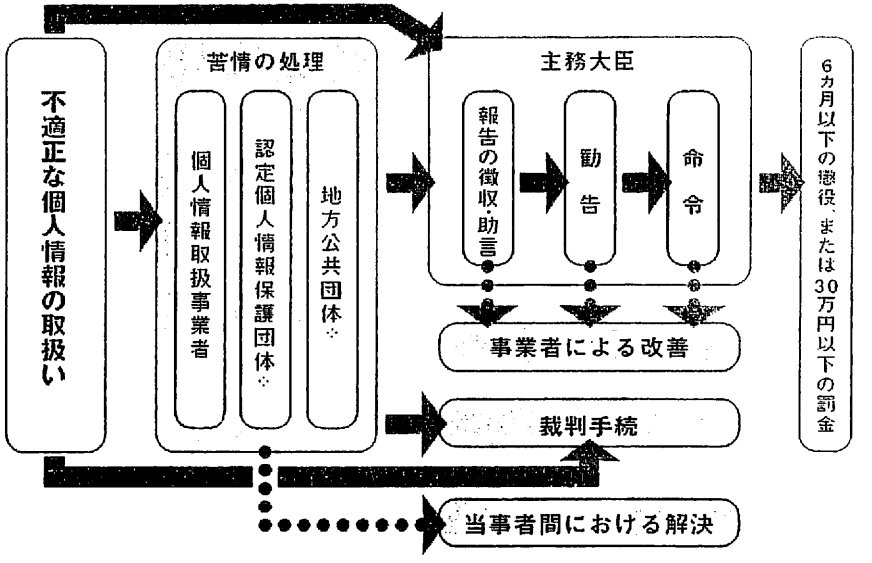
※法定代理人または本人が委任した代理人を通じて求めることもできます。



苦情処理の仕組みはどうなっているの？

個人情報に関する苦情については、
個人情報取扱事業者自身の取組みにより解決することを基本としながら
認定を受けた個人情報保護団体や地方公共団体によるあっせん等により
解決を図ることとしています。

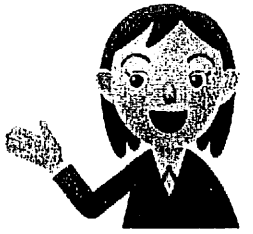
苦情処理の仕組み



※地方公共団体の窓口について
地方公共団体の個人情報に関する苦情相談窓口については、内閣府の「個人情報の保護」のホームページ（http://www5.cao.go.jp/seikatsu/kojin/index.html）に一覧が掲載されています。

※「認定個人情報保護団体」とは
個人情報の適正な取扱いの確保のため主務大臣が認定した、苦情の処理や対象事業者に対する情報の提供などを行う団体です。

ご質問にお答えします！



Q.1 この法律はいつから施行されますか？

A この法律のうち、基本理念や国の責務・施策等を規定する部分（第1章から第3章）は、公布の日（平成15年5月30日）から施行されていますが、個人情報をデータベース等の形で事業活動に用いる事業者の義務等を定める第4章以降は、平成17年4月1日から施行されます。

Q.2 個人情報保護とはどういうことですか。プライバシー保護とは違うのですか？

A 個人情報保護法は、個人情報取扱事業者が個人情報の適正な取扱いのルールを遵守することにより、プライバシーを含む個人の権利や利益の侵害を未然に防止することをねらいとしています。したがって、個人情報の取扱いとは関係のないプライバシーの問題などは、この法律の対象とはなりません。プライバシー侵害等が実際に発生した後の個人の権利や利益の救済については、従来どおり、民法上の不法行為や刑法上の名誉毀損罪等によって図られることになります。

Q.3 「個人情報データベース等」には、紙の情報（マニュアル情報）も含まれますか？

A この法律では、「個人情報データベース等」を事業活動に利用している事業者が個人情報取扱事業者として義務規定の対象となりますが、「個人情報データベース等」にはコンピュータ処理情報のほか、紙に書いてある情報であっても、個人情報を五十音順、生年月日順、勤務部署順など一定の方式によって整理し、目次・索引等をつけて容易に検索できる状態に置いてあるものも含まれます。

Q.4 この法律によって、消費者にはどのようなメリットがあるのですか？

A この法律によって、消費者は、事業者における個人情報の取扱いに不安を感じたような場合、自分に関する情報の開示や訂正、利用停止等を自ら求めることができるようになります。また、個人情報に関する苦情がある場合には、問題の事業者に直接申し出るだけでなく、認定個人情報保護団体や地方公共団体などにご相談できるようになります。

チェック！

あなたの大切な個人情報を守るために…

個人情報は思わぬところで悪用される可能性もあります。
“自分の情報は自分で守る”という意識も必要です。

- 個人情報は、気軽にアンケートへ回答することなどを通じて収集されることもあります。ご自分の個人情報をむやみに提供しないことも大切です。
- 悪質な事業者は、個人情報を架空請求等に悪用することもありますので、注意が必要です。
- 個人情報が思わぬ利用のされ方をして事業者とのトラブルの原因となることもあります。個人情報を提供するときは利用目的をしっかりと確認しておくことが大切です。

事業者が個人情報の適切な保護のための体制をしっかりと整備しているのかチェックしてみましょう。

- ☐ プライバシー・ポリシー（事業者の個人情報に関する考え方や方針）を公表しているなど、個人情報の保護に取り組む姿勢は示されているでしょうか。
- ☐ 個人情報の利用目的は、はっきり示されていますか。
- ☐ 利用目的に照らして、必要以上の個人情報を求められていませんか。
- ☐ 会社名や苦情受付窓口などの連絡先はきちんと示されていますか。

個人情報の取扱いに関するトラブルや疑問は？

個人情報に関する苦情は、その事業者に申し出るほかに、地方公共団体の苦情相談窓口などにご相談できるようになります。地方公共団体の窓口については、下記ホームページに一覧を掲載しています。

法律及び政令の条文等は内閣府国民生活局のホームページからご覧いただけます。

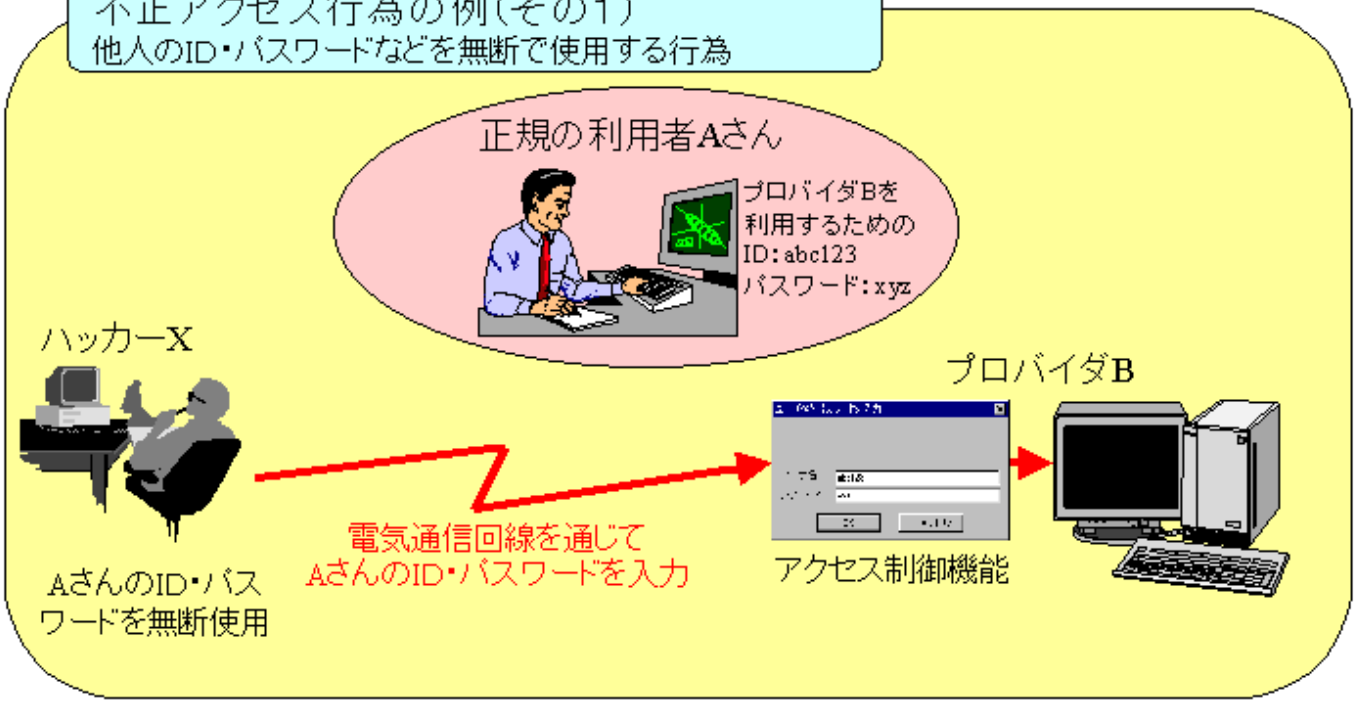
http://www5.cao.go.jp/seikatsu/kojin/index.html

内閣府国民生活局企画課個人情報保護推進室　〒100-8914 東京都千代田区永田町1−6−1 TEL 03-3581-3712〜3713

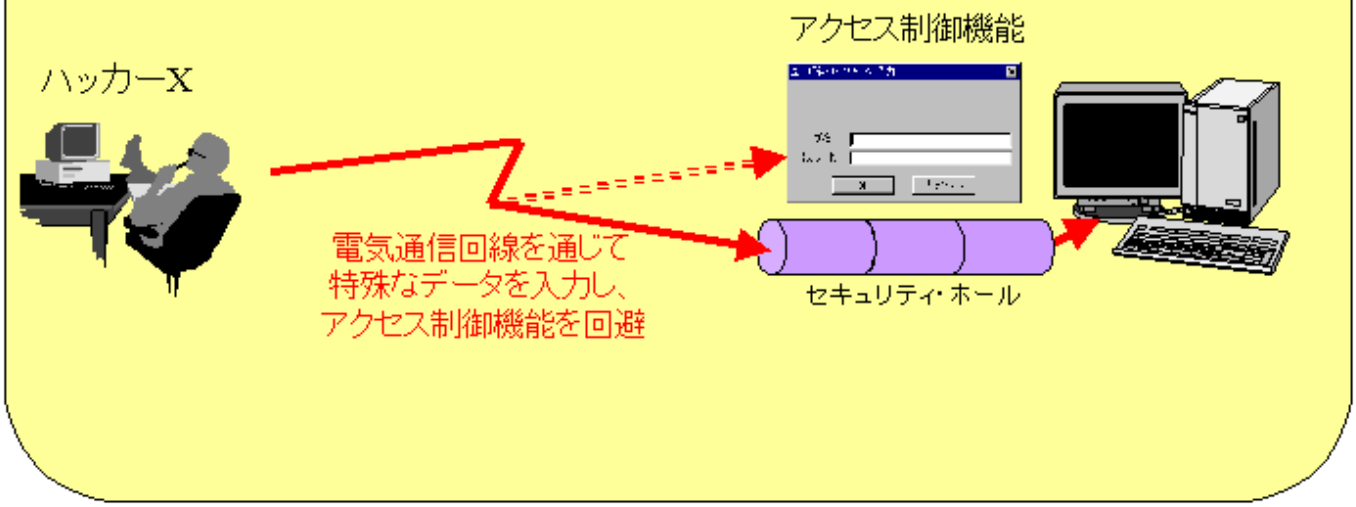
不正アクセス行為は処罰されます！

「不正アクセス行為の禁止等に関する法律」（不正アクセス禁止法）が平成12年2月13日から施行されます。以下の行為は「不正アクセス行為」や「不正アクセス行為を助長する行為」として禁止され、違反者は処罰されます。

不正アクセス行為の例（その1）
他人のID・パスワードなどを無断で使用する行為



不正アクセス行為の例（その2）
セキュリティ・ホールを攻撃してコンピュータに侵入する行為



- 不正アクセス行為とは、識別符号(※1)を入力することで利用(※2)できるようになっているコンピュータ(※3)にネットワークを通じて(※4)アクセスし、このような利用ができる状態にしてしまう行為(※5)です。コンピュータ以外の端末から行うもの(※6)も禁止・処罰されます。
- 他人の識別符号を無断で第三者に提供する行為は、不正アクセス行為を助長する行為として禁止・処罰されます。提供手段に限定はなく、オンラインで行っても、オフラインであっても禁止・処罰されます。提供行為によって金銭的な利益を得たかどうかは関係ありません。

※1 ID・パスワードのほか、指紋、虹彩、音声、署名などを用いるものも含まれます。
※2 ホームページの書き換え、インターネット・ショッピングの注文、データ閲覧、ファイル転送など利用内容に限定はありません。
※3 企業のものも個人のものも広く含まれます。
※4 インターネットなどのオープンネットワークのほか、企業内LANで外部と接続していないものなども含まれます。
※5 利用してしまう行為も含まれます。
※6 例えば、電話機から口座番号と暗証番号をプッシュボタンで入力する行為などです。

- 不正アクセス行為の禁止等に関する法律の条文
- 不正アクセス行為の禁止等に関する法律の概要

不正アクセス行為の禁止等に関する法律

（目的）

第一条　この法律は、不正アクセス行為を禁止するとともに、これについての罰則及びその再発防止のための都道府県公安委員会による援助措置等を定めることにより、電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与することを目的とする。

（不正アクセス行為の禁止）

第三条　何人も、不正アクセス行為をしてはならない。

2　前項に規定する不正アクセス行為とは、次の各号の一に該当する行為をいう。

一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）

二　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）

三　電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

（不正アクセス行為を助長する行為の禁止）

第四条　何人も、アクセス制御機能に係る他人の識別符号を、その識別符号がどの特定電子計算機の特定利用に係るものであるかを明らかにして、又はこれを知っている者の求めに応じて、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない。ただし、当該アクセス管理者がする場合又は当該アクセス管理者若しくは当該利用権者の承諾を得てする場合は、この限りでない。

（罰則）

第八条　次の各号の一に該当する者は、一年以下の懲役又は五十万円以下の罰金に処する。

一　第三条第一項の規定に違反した者

二　第六条第三項の規定に違反した者

第九条　第四条の規定に違反した者は、三十万円以下の罰金に処する。

参考 法律の全文

特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律の概要

趣　旨

特定電気通信による情報の流通によって権利の侵害があった場合について、特定電気通信役務提供者（プロバイダ、サーバの管理・運営者等。以下「プロバイダ等」という。）の損害賠償責任の制限及び発信者情報の開示を請求する権利につき定めるものとする。

内　容

(1)　プロバイダ等の損害賠償責任の制限

特定電気通信による情報の流通により他人の権利が侵害されたときに、関係するプロバイダ等が、これによって生じた損害について、賠償の責めに任じない場合の規定を設ける。

(2)　発信者情報の開示請求

特定電気通信による情報の流通により自己の権利を侵害されたとする者が、関係するプロバイダ等に対し、当該プロバイダ等が保有する発信者の情報の開示を請求できる規定を設ける。

施行期日

公布の日（平成１３年１１月３０日公布）から６か月以内の政令で定める日から施行する。

（参　考）

(1) e-Japan重点計画（平成13年3月29日高度情報通信ネットワーク社会推進戦略本部決定）

4.電子商取引等の促進 (3) 具体的施策 2) 新たなルールの整備

イ） インターネットサービスプロバイダー等の責任ルール（総務省）

「インターネット上の情報流通に関して、ウェブページ等への情報掲載による他人の権利利益の侵害に、プロバイダー等が迅速かつ適切な対応が行えるよう責任を明確化する・・・ため、必要なルールの整備を行う。このため、「特定電気通信による情報の流通の適正化及び円滑化に関する法律案」（仮称）を2001年中に国会に提出する。

(2) 規制改革推進３か年計画（平成13年3月30日閣議決定）

II 1 (3) ウ 電子商取引ルールと新たな環境整備

（事項名） 14) インターネットサービスプロバイダー等の責任ルール（総務省）

（措置内容）インターネット上の情報流通に関して、ウェブページ等への情報掲載による他人の権利利益の侵害にプロバイダー等が迅速かつ適切な対応が行えるよう責任を明確化するため、必要なルールの整備を行う。

（実施予定時期）平成13年度　法案提出

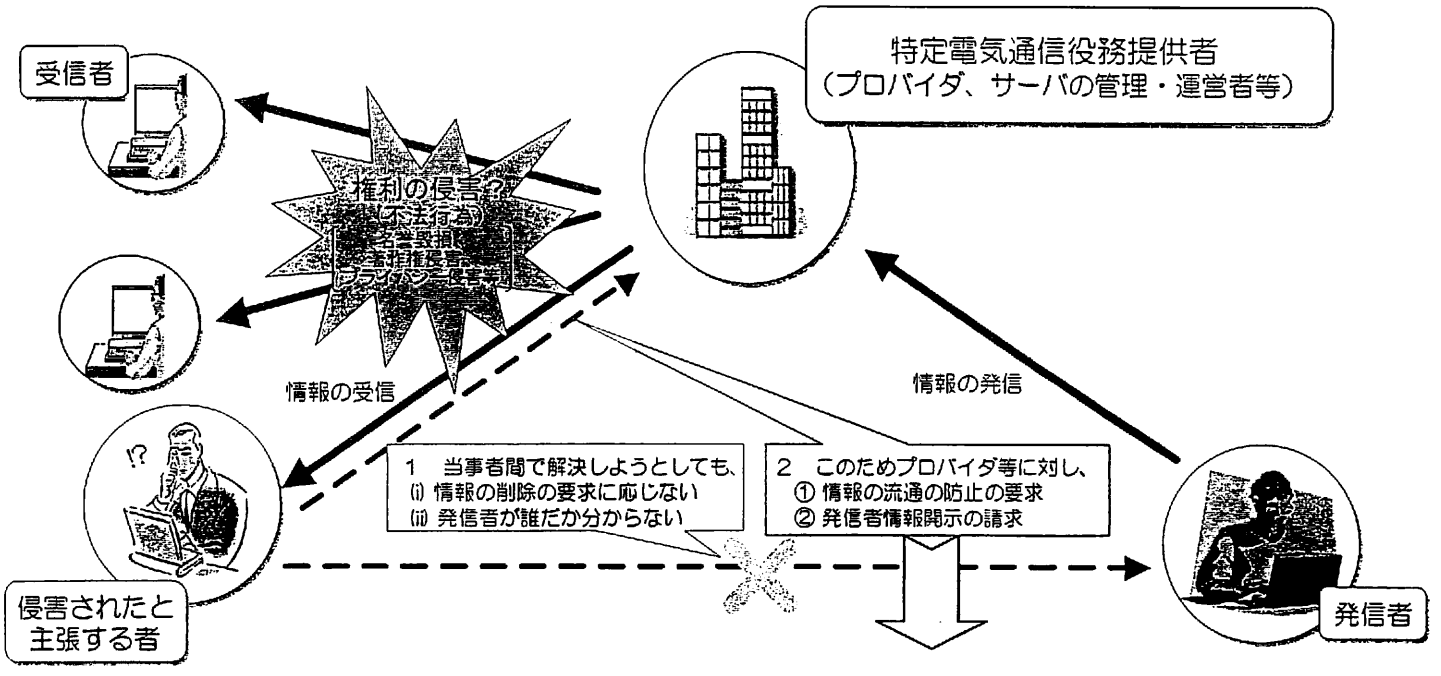
(3) 改革工程表（平成13年9月21日第20回経済財政諮問会議後公表）

１ 1) (2) ＩＴに関する規制改革の推進

○インターネットサービスプロバイダ等の責任ルールの整備のために、法案を提出する。

（次期臨時国会で措置）

プロバイダ等の自主的対応を促すための環境整備の必要性



(a)　情報の違法性の判断が困難等自主対応による措置の責任が不明確な場合がある

(b)　民事事件ではほとんど発信者情報の開示はされず、被害者救済が困難なことがある

⇨ プロバイダ等による自主的対応を促し、その実効性を高める環境整備の必要

プロバイダ等の責任の明確化の概要

被害者（侵害されたとする者）に対する責任

以下の①、②の場合でなければ、責任なし

① 他人の権利が侵害されていることを知っていたとき

② 違法情報の存在を知っており、他人の権利が侵害されていることを知ることができたと認めるに足りる相当の理由があるとき

プロバイダ等による対応

削除せず

削除

発信者に対する責任

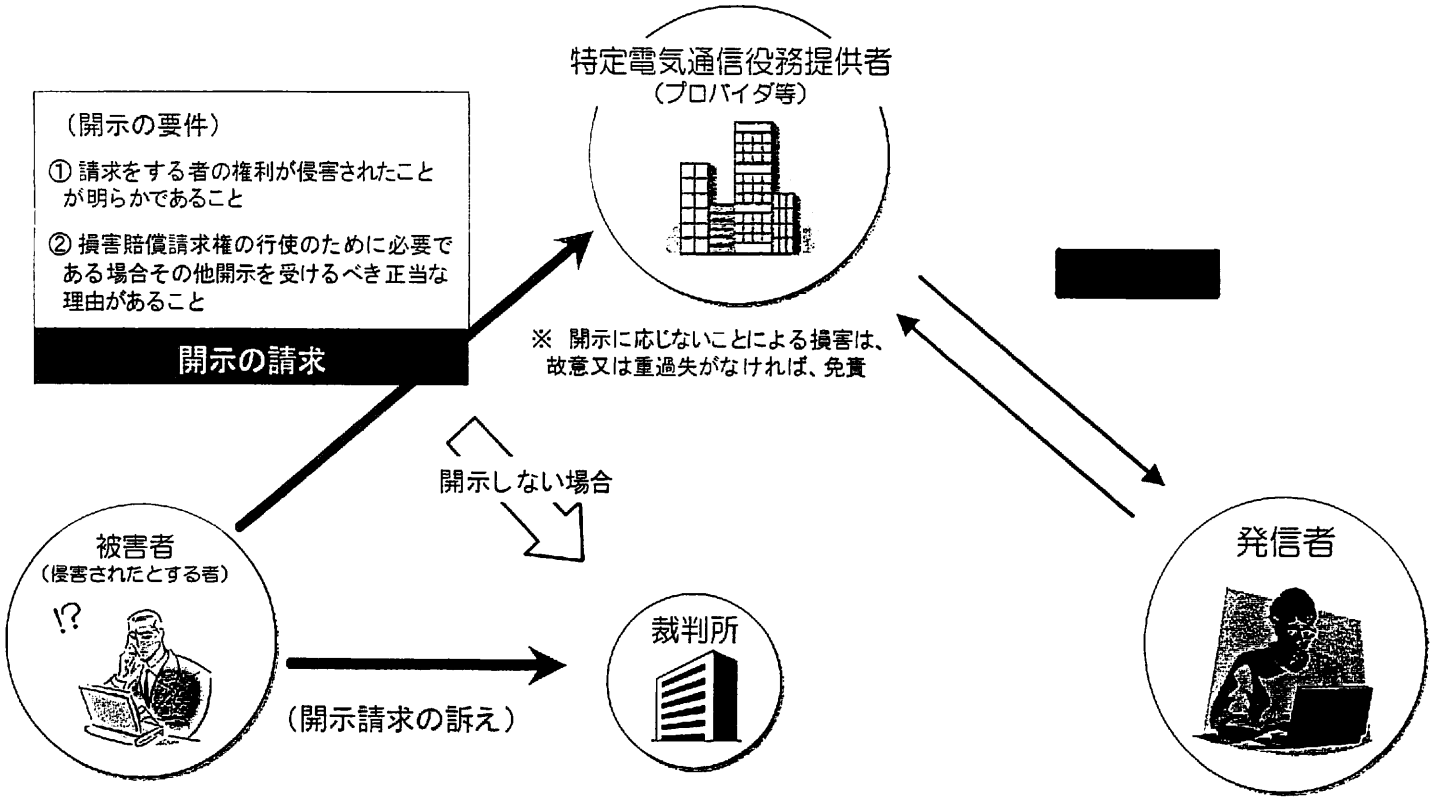
以下の①、②の場合は、いずれも責任なし

① 他人の権利が侵害されていると信じるに足りる相当の理由があったとき

② 権利を侵害されたとする者から違法情報の削除の申出があったことを発信者に連絡し、7日以内に反論がない場合

資料
- 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律のあらまし（PDF）
- 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律条文（PDF）
- 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律の図解（PDF）
- 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律の逐条解説（PDF）

発信者情報開示の概要


特定電気通信役務提供者
（プロバイダ等）
（開示の要件）
① 請求をする者の権利が侵害されたことが明らかであること
② 損害賠償請求権の行使のために必要である場合その他開示を受けるべき正当な理由があること
開示の請求
※ 開示に応じないことによる損害は、故意又は重過失がなければ、免責
開示しない場合
被害者
（侵害されたとする者）
!?
裁判所
（開示請求の訴え）
発信者

セキュリティ

INDEX

エンドユーザ向けセキュリティポリシー

パスワードについて

概要

パスワードは、コンピュータ上のユーザを証明するための方法として、安価に、そして広く使われている認証の手段です。
パスワードを設定することで、安易に関係者以外の人がアクセスすることを防ぐことができます。
しかし、パスワードの管理を怠りますと、関係者以外の人の侵入を受けることになり、個人情報の流出など、さまざまな被害を被る可能性があります。
そのため、パスワードの管理について、以下の点に気を付けなければなりません。

パスワードを他人に知られないようにする

パスワードが他人に知られた場合、そのパスワードは、セキュリティを確保するという使命を失うことになります。
パスワードが他人に知られる機会は、以下のようなことが考えられます。

- パスワードを書いた紙を、人に見られた
- パスワードを書いた紙を、シュレッダにかけずに捨てた
- パスワードを記述したデータをコンピュータのディスク上に保管した
- パスワードの入力をしているところを盗み見された
- パスワードを声に出していたのを人に聞かれた

他にもありますが、多くの場合は上記のような場合に、パスワードの流出があると考えられます。
また、管理者と名前を偽り、調査という名目でパスワードをメールや電話で聞き出す手口があります。
不審に思った場合には、即答をしないで、かならず管理者に確認をとってください。

パスワードを紙に書いた場合

できる限り、パスワードは頭の中に記憶して、人に知られないようにしてください。
記憶できない場合は、紙に書いてもかまいませんが、その管理はしっかり行ってください。
その際に気を付けることとして、以下のことに注意する必要があります。

- パスワードを書いた紙を見られないようにする
- パスワードを書いた紙の廃棄には、シュレッダを使って、判読不能にする
- パスワードの保管場所に気を付ける

上の2点は「パスワードを他人に知られないようにする」と同じ内容になっています。
パスワードは、その保管に際し、なるべく他人の目に触れることが無い場所へ保管する必要があります。

(たとえば、金庫など鍵のかかる場所)

他人に予測されにくいパスワードにする

パスワードは、他人から勝手に侵入されないために、推理されにくくする必要があります。
以下のようなパスワードは、推理されやすいので、さけてください。

- 辞書に載っているような単語
- キーボード配列や番号順などの単純なパターン
- 関係者や有名な人
- ユーザーIDなどの名前
- 誕生日や住所
- 電話番号などの個人情報を使った名前
- 4文字や6文字などの短いパスワード
- ローマ字のパスワード
- 単語を少しいじっただけのパスワード

上記の点に気を付けて、パスワードを決めてください。
特に、ユーザーIDとパスワードが同じというのは、パスワードが無いのに等しいので、必ず避けてください。

その他の対策

上記以外にも、パスワードに関して、以下の点に気を付ける必要があります。

- パスワードを定期的に変更すること
- パスワードが漏れた可能性がある場合(あるいはあった場合)、速やかにパスワードを変更すること

ネットワークについて

概要

ネットワークでやりとりを行う際、診療所単位のネットワークは、外部のネットワークとの不要なやりとりをできるだけ遮断する必要があります。
それによって、外部からの不正アクセスを減らし、グローバルなインターネットなどからの侵入を防ぐことができます。
そのため、ネットワークについて、以下の点に気を付けなければなりません。

- 日医標準レセプトサーバを接続しているLANとグローバルネットワークの間は、必ずルータ(あるいはプロキシサーバ)を設置すること
- 日医標準レセプトソフトサーバを運用するLANと院外のネットワークを接続するルータにはIPフィルタリングを設定すること(特に、glserverとglclientをつなぐ8000番ポートは遮断しなければならない)
- 遠隔地からのリモートログインを原則禁止とする(リモートでのメンテナンスを除く)
- コンピュータの構成を把握すること(接続しているコンピュータに名前を書いたシールを貼り付けるなど)

コンピュータの利用について

概要

ネットワーク経由の不正侵入は防ぐことができても、物理的にコンピュータにふれることで、個人情報を持ち出すことは可能です。
そのため、コンピュータの利用について、以下の点に気を付けなければなりません。

- 関係者以外のLAN内での日医標準レセプトソフトサーバの利用を禁止する
- ログインした状態で、長時間席から離れないこと(離れることがある場合、たとえば、スクリーンセーバーが起動するようにし、スクリーンセーバーの設定である「パスワードを要求する」の設定を有効にして、離れた隙の不正侵入を防ぐこと)
- 管理者以外が重要なユーザで操作することを禁止する
- 不要なアプリケーションのインストールをしてはならない(ポートが開く可能性がある)
- 許可なくフロッピー・CD−ROM・MOなどの記録媒体を使用しない
- 設定ファイルを書き換えてはならない

なお、日医標準レセプトソフトサーバ(DebianLinuxプラットホーム)以外については、ここには記載しません。

▲ページトップへ