厚生労働科学研究費補助金
地域医療基盤開発推進研究事業

病院情報システム端末からの安全なインターネット直接接続に関する研究

平成２２年度　総括・分担研究報告書

主任研究者　山本　隆一

平成２３（２０１１年）年５月

目　　次

Ⅰ．総括研究報告

病院情報システム端末からの安全なインターネット直接接続に関する研究 ---------- 1

山本　隆一、中島直樹、田中勝弥、矢野一博

（資料１）インターネット上のセキュリティ脅威に関する調査 ----- 7

（資料２）Japan-Germany e-Health Symposium プログラム ----- 26

（資料３）e-Health in Japan 発表資料 ---------- 28

（資料４）Secure networks for internal and external information Exchange in hospital 発表資料 ---------- 37

II. 研究成果の刊行に関する一覧表 ---------- 47

III. 刊行物の別刷 ---------- 48

厚生労働科学研究費補助金　地域医療基盤開発推進研究事業
総括研究報告書

病院情報システム端末からの安全なインターネット直接接続に関する研究

主任研究者　山本　隆一　東京大学大学院情報学環・准教授
分担研究者　中島直樹　九州大学医学部付属病院医療情報部・准教授
分担研究者　田中勝弥　東京大学付属病院企画情報運営部・助教
分担研究者　矢野一博　日本医師会総合政策研究所・主任研究員

研究要旨

医療機関の大部分は何らかの情報システムを導入し、レセプトオンライン、緊急安全性情報へのアクセス、診療ガイドラインへのアクセスなど外部ネットワークへのアクセスへの医療機関側からの要求は増大している。またブロードバンド等の普及により、市民のネットワークリテラシは確実に向上しており、患者が自らの診療情報へのインターネットを介したアクセスを希望する場合も今後増加するであろう。しかし、たとえレセコンであってもプライバシーに機微な電子化情報を大量に保有しており、安全管理には万全を期すことが求められている。厚生労働省は「医療情報システムの安全管理に関するガイドライン」公表し、版を重ね適切な安全管理指針を示している。このガイドラインではインターネットへの接続を禁止はしていないが、かなり厳重な対策を求めており、一般の医療機関が安易に接続できる状況ではない。本研究の目的はこのような事情に対し、特別な専門知識を持たない医療機関が、自らの情報資産の安全を確保した上で安全にインターネットと通信できる状態にすることで、そのための要件を詳細に定義し、接続の程度に応じた現実的に可能な方法を示すとともに、さらに共通に利用可能なゲートウエイセンターを設置する場合のゲートウエイセンターの要件を明らかにする。さらに最近本格的な研究が開始されている新世代ネットワーク（NWGN）における自立的Overlay Network技術など、先端技術をサーベイし、今後の施策に視する提言も行う。

最初に本年度は研究初年度であり、主任研究者、分担研究者が意見交換を行いながら一体として研究を進めたために、総括研究報告書にまとめて記載をする。

A．研究目的

医療機関の大部分は何らかの情報システムを導入し、レセプトオンライン、緊急安全性情報へのアクセス、診療ガイドラインへのアクセスなど外部ネットワークへのアクセスへの医療機関側からの要求は増大している。またブロードバンド等の普及により、市民のネットワークリテラシは確実に向上しており、患者が自らの診療情報へのインターネットを介したアクセスを希望する場合も今後増加するであろう。しかし、たとえレセコンであってもプライバシーに機微な電子化情報を大量に保有しており、安全管理には万全を期すことが求められている。厚生労働省は「医療情報システムの安全管理に関するガイドライン」公表し、版を重

ね適切な安全管理指針を示している。このガイドラインではインターネットへの接続を禁止はしていないが、かなり厳重な対策を求めており、一般の医療機関が安易に接続できる状況ではない。本研究の目的はこのような事情に対し、特別な専門知識を持たない医療機関が、自らの情報資産の安全を確保した上で安全にインターネットと通信できる状態にすることで、そのための要件を詳細に定義し、接続の程度に応じた現実的に可能な方法を示すとともに、さらに共通に利用可能なゲートウエイセンターを設置する場合のゲートウエイセンターの要件を明らかにする。さらに最近本格的な研究が開始されている新世代ネットワーク（NWGN）における自立的Overlay Network技術など、先端技術をサーベイし、今後の施策に視する提言も行う。

B．研究方法

本研究は以下の５つのプロセスからなる。

１．現状の状況調査

ア）我が国の医療機関向けネットワークセキュリティに関する規制および各種指針の精査で、それぞれ特徴のある大学病院を３病院、訪問ならびにインタビュー調査を行った。

イ）諸外国における医療機関向けネットワークセキュリティに関する規制および各種指針の精査で、本年度はドイツでシンポジウムを開催し、意見交換するとともに一名の研究者と個別にインタビューを行った。

ウ）我が国の医療機関におけるインターネット接続の実態および懸念事項に関する調査で、本年度は医療分野に限らず広く文献的に調査を行った。

２．上記アに加えてインターネットに部分的にでも接続している２大学病院で継続的にパケットモニタを実施し、実際の外部のネットワーク上のリソースの利用状況を測定した。ただし、これは継続的に計測中であり、今年度は結果を得るに至っていない。

３．複数の医療機関が共同利用可能なゲートウエイセンターと仮想医療機関を実験的に構築し、センターと医療機関間の接続および医療機関内のネットワーク構成に関するモデルを構築し、運用シミュレーションを行い、運用要件を明確にする。本年度はファイアウォール機器の一部について評価を行った。

C．研究結果

１．大学病院における実態調査

３つの大学病院で医療情報システム管理者を中心にインタビュー調査をおこなった。インタビュー項目は以下の３点を中心に、実際の対策を聞き取った。

Ｑ１．診療端末とメール、Webなど閲覧するインターネット端末が別ということで、安心だと思われる点（セキュリティ面）などありましたらお聞かせください。また、診療端末がインターネットに接続していなために不便な点などあればお聞かせください。

Ｑ２．診療の際にインターネットによる情報の閲覧、参照が必要と思われますか？

また、もし必要な場合どのような情報が必要もしくは便利だと思われますか。（例、医薬品の副作用情報、EBMなど）

Ｑ３．もし病院内の診療端末を直接インターネットに接続することになった場合、不安な点がありましたらお聞かせください。

結果はそれぞれ特色があるので個別述べたい。

T大学病院：

すでに診療端末はほぼ完全にインターネットに接続されている。したがってQ1に対しては前提が異なっており、回答はなかった。Q2においては例示した医薬品の副作用やEBMは重要性が低かったが、むしろ、初診患者の職業に関する検索など、患者の社会的背景の把握が重要という指摘があった。また診療業務外の利用（研究や教育など）も必要な時にすぐに出来る点は評価が高かった。Q3についてはこの病院はウイルス侵入などの事案があったものの、実際にはUSBメモリを介した感染であり、インターネット接続によるアクシデント・インシデントはこれまでになく、現状の対策（ファイアウォール、ウィルススクリーニング等）で特に不安は感じていないとのことであった。

A大学病院:

現状、診療端末はまったくインターネットに接続されていないが、Windows Serverのターミナルサービスを用いて、DMZにあるInternet接続Windows Serverを介して、診療情報端末上の仮想ターミナルでインターネットアクセスを許可する機構を完成させサービスイン直前であった。ターミナルサービスを拡張し、医局のPCやサーバとの情報転送などもサポートし、ユーザの要求にスペック上はほぼ完全に対応できるとのことであった。

Q1に関しては診療情報システム管理部門としては特に不安は感じていないが、これまで厳重に制限していた経緯から、それなりの説得あるセキュリティ対策が必要という認識であった。Q2についてはT大学病院と同様。Q3についてはサービスイン直前である仕組みは診療情報システムへの影響はなく、運用上の不安（不正サイトへのアクセスなど）以外は特に感じていないとのことであった。

K大学病院:

現状はもっとも複雑で、診療部署には２種類の端末がある。一つは完全に診療情報システムと隔離されたインターネット接続端末で、もう一つは診療情報システムの専用端末である。さらにこの診療情報システム専用端末には２種類あり、ひとつは外部インターネット接続がまったく不可能な端末であるが、もう一つは非常に限定されたWEBアクセスが許可された端末である。アクセスできるサイトは申請を行い許可されなければならない。Q1についてはA大学病院と同様で、特に不安は感じていないが、これまでの経緯で院内的には相当な説明責任を果たさなければ接続できない状況とのことである。Q2に関してはT大学病院と同様。Q3に関しては情報システム管理者としては特段の不安はないが、ユーザは運用上の不安を覚えているとのことであった。

２．海外調査

本年度はかねてから主任研究者がe-Healthに関して共同で研究を進めているドイツで調査を行った。オスナブルック大学とe-Healthならびにネットワークセキュリティに関するシンポジウムを開催し、意見交換をおこなった。ドイツでは診療情報システムのほぼすべては外部ネットワークと接続されてなく、現状では我が国のオンラインによるレセプト請求のようなネットワークアプリケーションも存在しない。しかし、2010年度に行ったアンケート調査があり（未発表のため、資料としては掲載できなかった）、そこでは地域基幹病院の多くは、近隣医療機関とオンライン共同診療を求めており、今後急速に要求が高まることが予想されている。ただ現状では国あるいは州レベルでのガイドライン等は存在していない。E-Healthプロジェクトは国として

推進しており、GematikとよばれるICカード基盤の導入を直前に控えており、その意味でもネットワークセキュリティの整備が望まれるとのことであった。

３．我が国のネットワークセキュリティに関する懸念事項ならびに対応規制の調査

３－１インターネットの情報セキュリティに関わる事故およびインシデント

以下の事例を挙げることができた。

1. 2008年12月：早大Winny感染でセクハラ相談リスト流出
2. 2008年4月：サウンドハウスクレジットカード番号流出（SQLインジェクションによる）
3. 2007年6月：警視庁Winny感染で捜査情報流出（男性巡査長の私物パソコンから，少年事件や口座情報を含む捜査資料[文書類，画像など]がインターネット上に流出）
4. 2006年1月：防衛庁／自衛隊Winny感染で「秘」扱い情報流出
5. 2005年8月：三菱重工関連 Winny感染で原発機密情報流出
6. 2005年6月：三菱電機グループWinny感染で原発機密情報流出
7. 2005年5月：価格コム　メールアドレス流出（SQLインジェクション攻撃を受けウェブサイトを改変され，別サイトに誘導，ウイルス感染，さらにメールアドレスが流出）
8. 2005年3月：UFJ銀行のウェブサイトを偽装したフィシング詐欺
9. 2004年3月：ジャパネットたかた顧客情報流出（システム担当者とその上司が顧客情報を光磁気ディスクにコピー，名簿業者に売り渡す）
10. 2004年2月：ヤフーBB 450万人顧客情報流出（管理者IDを利用しサーバに接続して個人情報を取得，脅迫事件に発展）
11. 2002年5月：TBCエステ情報流出（WEBサーバの設定ミス）
12. 1999年5月：宇治市個人情報流出（システム開発時，データを持ち帰って作業，MOコピー，名簿業者に売り渡す）

この後Sony株式会社の子会社による１億件以上の個人情報の流出事故が起こったが、まだ全容が明らかになっていないために今年度の結果には含めていない。

12件の内、5件がファイル交換ソフトであるWinnyに関連するもので、2件がSQLインジェクションによるもの、1件がWEBサーバの設定ミス、１件がフィッシング詐欺で、他の案件は内部犯行による犯罪であった。

なお、この調査の詳細は資料１として後掲する。

４．ゲートウエイセンターに必要なファイアウォール機器の評価

今年度はファイアウォールならびにVPNアプライアンスとしてCISCO社のASX5500、SPAM対策アプライアンスとしてのBarracuda 400を評価した。いずれも評価の途中であり、詳細な結果は次年度に行うが、電子メールをアプリケーションとして用いる限りはSPAM対策は必須であり、SPAM Assassin等のソリューションに比べてBarracudaは明確なSPAMに対してはユーザが意識することなく、消し去ることが可能で、有用性が高いことが明らかになっている。

D．考察

本年度は主に研究のスコープを明確にするための調査を行ったが、比較的ＩＴリテラシが高く、人員にもゆとりがある大学病院での調査でも診療情報システムから必要な外部ネットワーク上のリソー

スに自由にアクセスできる環境は１病院でのみ実現されており、他は限定的であった。もっとも現在構築中の１病院はOpt in方式ではあるが、将来はかなり自由にアクセスできる環境になることが期待された。その一方で、現状行われている方法が必要十分な解であることは、いずれの病院のネットワーク管理者も確信を持ち得ていない状況といえる。本研究で示す現実的解によって、少なくとも一定規模以上の病院など、専属ではないにせよ、医療情報技師など一定の専門知識を持つ管理要員の配置が可能な医療機関では安全にインターネット上の資源にアクセス可能となるような、指針の必要性が明確になったと言える。ただ大部分の小規模医療機関はITリテラシーの点からも人員の点からも実際には利用不可能であり、管理要員が配置できなくても、安全な接続を可能とするためには管理を一括して行うゲートウエイセンターが有効な解決方法となりうる。本年度はゲートウエイセンターの構成要素である、ファイアウォールとSPAMフィルタの評価を行い一定の成果はあるものの、引き続き検討が必要であることがわかった。またインターネットのセキュリティ上の脅威の調査では、これまでの我が国での事例の内、４割は内部の従業者による犯罪であり、４割はファイル交換ソフトの誤用あるいはファイル交換ソフトへのウイルス感染によるもの、のこりは少数であるが、SQLインジェクションと、WEBサーバの設定ミスであった。従業者による犯罪は技術的に防止することは難しいが、その他はいずれも技術的に、あるいは技術的対策と運用規則で対応可能であり、本研究でさらに対策を具体的にする必要が明確になった。

E．結論

本年度は主に研究のスコープを明確にするための調査を行った。比較的ＩＴリテラシが高く、人員にもゆとりがある大学病院での調査でも診療情報システムから必要な外部ネットワーク上のリソースに自由にアクセスできる環境は１病院でのみ実現されており、他は限定的であった。その一方で、現状行われている方法が必要十分な解であることは、いずれの病院のネットワーク管理者も確信を持ち得ていない状況といえた。ゲートウエイセンターの構成要素である、ファイアウォールとSPAMフィルタの評価を行い一定の成果はあるものの、引き続き検討が必要であることがわかった。またインターネットのセキュリティ上の脅威の調査では、これまでの我が国での事例の内、４割は内部の従業者による犯罪であり、４割はファイル交換ソフトの誤用あるいはファイル交換ソフトへのウイルス感染によるもの、のこりは少数であるが、SQLインジェクションと、WEBサーバの設定ミスであった。従業者による犯罪は技術的に防止することは難しいが、その他はいずれも技術的に、あるいは技術的対策と運用規則で対応可能であり、本研究でさらに対策を具体的にする必要が明確になった。

F．研究発表

1.　論文発表

山本隆一，“保健医療分野での通信技術の課題”，電子情報通信学会誌，vol. 94，pp 380-384，2011

2.　学会発表

なし

G．知的財産権の出願・登録状況

（予定を含む。）

1. 特許取得

なし

2. 実用新案登録

なし

3. その他

なし

資料1

インターネットの情報セキュリティに係わる脅威の最新動向調査

目次

1．目的 2

2．調査項目 3

2-（1） インターネットの情報セキュリティに係わる脅威の最新動向調査 3

－ 調査結果 －

・インターネットの情報セキュリティに係わる脅威

・行政処分等

2-（2） 医療機関等の設置端末等からインターネットに接続する際の脅威への対策動向調査 10

－ 調査結果 －

・法制度に係わる事項

・技術的事項が記載されている対策文書

2-（3） 事例の調査 15

－ 調査対象 －

－ 調査期間 －

－ 調査事項 －

－ 調査結果 －

2-（4） 洗い出された課題，脅威への適切な対処の検討 18

－ 効率的かつ効果的な対処策 －

－ 別 紙 －

事例調査用紙Ａ　医療機関に設置されるインターネット接続端末の安全な利用に関する課題調査

事例調査用紙Ｂ　Ｈ２１年度厚労科研「病院情報システム端末からの安全なインターネット直接接続に関する研究」（研究代表者：東京大学大学院情報学環准教授／山本隆一）九大病院インタビュー調査

1．目的

医療機関等に設置される端末等からインターネットに接続し，情報収集，提供及び共有を行い，医療機関等におけるインターネット及び情報通信技術活用の活性化を促すことを見据え，現状の情報セキュリティ上の脅威，法制度上の課題，関連する対策について調査することを目的とする。

2. 調査項目

2-（1）インターネットの情報セキュリティに係わる脅威の最新動向調査

インターネットを活用するアプリケーション，デバイスは日々，増加の一途をたどっている。それに合わせて，犯罪者，不正行為者の手口も巧妙かつ複雑化している。このような最近のトレンドを調査する。

－ 調査結果 －

- **インターネットの情報セキュリティに係わる脅威**
- **行政処分等**

インターネットの情報セキュリティに係わる脅威

2008年12月　早大Winny感染でセクハラ相談リスト流出

2008年4月　サウンドハウスクレジットカード番号流出　⇒Xページ参照

2007年6月　警視庁Winny感染で捜査情報流出
⇒ 男性巡査長の私物パソコンから，少年事件や口座情報を含む捜査資料（文書類，画像など）がインターネット上に流出

2006年1月　防衛庁／自衛隊Winny感染で「秘」扱い情報流出

2005年8月　三菱重工関連Winny感染で原発機密情報流出

2005年6月　三菱電機グループWinny感染で原発機密情報流出

2005年5月　価格コム　メールアドレス流出
⇒ **SQLインジェクション攻撃**を受けウェブサイトを改変され，別サイトに誘導，ウイルス感染，さらにメールアドレスが流出

2005年3月　UFJ銀行のウェブサイトを偽装したフィシング詐欺

2004年3月　ジャパネットたかた顧客情報流出
⇒ システム担当者とその上司が顧客情報を光磁気ディスクにコピー，名簿業者に売り渡す

2004年2月　ヤフーBB 450万人顧客情報流出
⇒ 管理者IDを利用しサーバに接続して個人情報を取得，脅迫事件に発展

2002年5月　TBCエステ情報流出　⇒Yページ参照

1999年5月　宇治市個人情報流出
⇒ システム開発時，データを持ち帰って作業，MOコピー，名簿業者に売り渡す

2008年4月 サウンドハウスクレジットカード番号漏洩流出

楽器や音響機器の通販サイトを運営するサウンドハウスの通販サイトがSQLインジェクションによる攻撃を受けクレジットカード情報を含むお客様情報の一部が流出，不正請求事件に発展

【攻撃内容と被害規模】 以下，サウンドハウス2008年4月7日より

1．**概要**

同社が運営するインターネットショッピングサイトにおいて，過去に購入されたお客様情報の一部が流出しているのではとのクレジットカード会社からの指摘を受け，セキュリティ対策を専門とする第三者機関に調査を依頼したところ，外部からの不正アクセスによりカード情報を含む個人情報が流出した可能性が高いとの報告がありました。流出の経路としましては，中国からのアクセスが確認されております。これに基づき，直ちに警察当局に被害届けを提出，経済産業省指定機関へ届出をすると共に，クレジットカード会社と連携を取りながら対策を講じております。

2．**流出した情報について**

2007年1月1日～2008年3月22日までに新規会員登録を行ったお客様のデータ，総数122,884件の内，最大97,500件まで下記のデータが流出した可能性があります(内カード情報保有データ27,743件)。・お名前 ・フリガナ ・性別 ・生年月日 ・ログイン用メールアドレス ・ログイン用パスワード **・クレジットカード情報（ご名義 / カード番号 /有効期限）**注：クレジットカードのパスワードにつきましては，弊社ではデータを保持していない為，流出の危険はありません。また，ご住所，お電話番号に関しては，調査の結果，流出の形跡はございませんでした。

3．**現在の対応状況**

セキュリティ対策を専門とする第三者機関からの提案に基づき，以下を実行しました。

① WEBシステム構成の再設計
② 侵入経路を遮断する不正侵入監視機器の設置
③ セキュリティ管理対策委員会を設置
④ 24時間体制の不正アクセス監視
⑤ ファイヤーウォールのアップグレード
⑥ 不正プログラムの除去
⑦ データベースからカード情報を削除

2002年5月 TBCエステ情報流出

2007年8月28日TBC（東京ビューティーセンター）情報漏洩事件について高裁判決

従来の個人情報漏洩事件と比較して，賠償認容額は相対的に高め

【事案の概要】

この事案は個人情報がインターネット上において第三者が閲覧できる状態になってしまい，実際に第三者がその情報にアクセスして個人情報が流出したというもの。被告が経営するエステティックサロンのTBCがインターネット上にWebサイトを開設し，そこでアンケート等を通じて原告らから提供された個人情報を保管管理していた。第三者が閲覧できる状態というのは，インターネット上の一般利用者が特定のURLを入力するだけで自由にアクセス，閲覧できる状態を指す。

原告14名はプライバシーを侵害されたとして，不法行為に基づき原告1人あたり慰謝料100万円および弁護士費用15万円の合計115万円，並びにこれに対する訴状送達の日から年5分の利息で計算した遅延損害金の支払いを求めていた。

東京地裁2007年2月8日判決は，原告14名のうち「情報保護のために安全対策を講じる法的義務を怠り，プライバシーを侵害した」として迷惑メールなどの2次被害を受けた13名に金3万5000円プラス遅延損害金，残り1名に2万2000円プラス遅延損害金の支払いを命じた。この地裁判決に対し，原告と被告の双方が控訴し，2007年8月28日の高裁判決となった。高裁判決では，損害賠償として認容された金額は地裁判決と同じになった。

【TBCエステ情報流出の概要】

2002年5月，エステティックサロンのTBCのサイトで約3万7000件の個人情報が誰にでも見られる状態で放置されていたことが判明。加えて放置された個人情報はP2P型のファイル交換ソフトを介してインターネット上に流出，全て削除することは事実上不可能になった。また，漏れた個人情報を元に迷惑メールなどの2次被害も発生している。

海外

2007年9月　韓国　SKテレコムの有無線ブログサービス「トシ（tossi）」個人情報流出事件

⇒ 2500人の個人情報が流出

SKテレコムは過失を認め，被害者に7万ウォン（約8930円）の商品券を支給。賠償総額は1億7500万ウォン（約2232万円）に及ぶ。

韓国では，2006年に韓国国民銀行が顧客の名前や住民番号，メールアドレスなどを流出した事件で，賠償額が1人当たり10万ウォン（約1万2750円）という判決が出ている。

2003年7月　**W32.Blaster.Worm** 全世界に拡散

⇒ 感染すると，TCP135番ポートに対する短いパケットをネットワーク上に送信する

2002年2月　米国　コンピュータ緊急対応センター（CERT/CC）が**クロスサイト・スクリプティング**について勧告

2001年9月　**Nimda** 全世界に拡散

⇒ 感染すると，不正メールの大量発信とコンピュータ内のファイル改変により動作が不安定になり，かつ，ネットワーク通信量が急増する

2001年7月　**Code Red** 全世界に拡散

⇒ 感染すると，コンピュータ内のメモリに展開され，インターネット上の次の攻撃目標を探し回る

1992年3月　米国　世界中のコンピュータ関係者を震撼させた謎のウイルス

⇒ 3月6日の攻撃予告，ウイルス感染，オペレーティングシステム損傷

1989年12月　英国　「トロイの木馬」パニック

⇒ パリの大病院の医師宛に送られてきたWHOを騙ったエイズに関する情報の入ったFDを閲覧後，ウイルスに感染，オペレーティングシステム損傷

行政処分等

総務省　－　業務改善命令

2010年2月　電気通信事業紛争処理委員会からの答申を受け，**西日本電信電話株式会社**に対し，電気通信事業法（昭和59年法律第86号）に基づき，他の電気通信事業者等に関する情報の取扱いについて**業務の改善等を命じた。**

また，個人情報の保護に関する法律（平成15年法律第57号）及び電気通信事業における個人情報保護に関するガイドライン（平成16年総務省告示第695号）に違反する行為が行われたと認められることから，**同社**に対し文書による**厳重注意を行った。**
なお，**東日本電信電話株式会社**に対し，他の電気通信事業者等に関する情報の取扱いについて業務の運営の在り方の**改善を要請した。**

事案：西日本電信電話株式会社の従業員が他の電気通信事業者の電気通信設備との接続の業務に関して入手した電話番号移転に関する情報を西日本電信電話株式会社－兵庫の従業員に提供，次いで西日本電信電話株式会社－兵庫の従業員が販売代理店に提供

経済産業省　－　勧告

2007年3月　信用個人情報の取扱いで**ＵＦＪニコス株式会社**と**株式会社ソニーファイナンスインターナショナル**に個人情報保護法３４条に基づく**勧告を出した。**

事案：本人の同意を得ずに与信審査目的以外の目的で個人の信用情報を信用情報機関である株式会社シー・アイ・シー及び株式会社シーシービーに照会・取得し，第三者に提供

総務省　－　勧告

2007年3月　個人情報の漏洩で**ＫＤＤＩ株式会社**に個人情報保護法に基づく**勧告を出した。**
事案：　光磁気ディスク紛失・流出した疑い

金融庁　－　業務改善命令，勧告

2009年6月　個人情報の流出で**三菱ＵＦＪ証券株式会社**に「金融商品取引法」第51条に基づく**業務改善命令，**ならびに「個人情報保護法」第34条に基づく**勧告を出した。**

事案：顧客情報を持ち出し，名簿業者に販売

2006年4月　個人情報の流出で**株式会社みずほ銀行**に個人情報保護法に基づく**是正勧告を発動した。**

事案：顧客の個人情報などを第三者に漏出した業務上横領の疑い

総務省　－　厳重注意

2008年4月　「Yahoo!メール」のヘッダ情報が受信者以外に流出した問題で，同サービスを展開する**ヤフー株式会社**を文書により**指導した。**

2007年6月　西日本電信電話株式会社からグループ会社従業員の個人情報が流出した問題で，**西日本電信電話株式会社**を文書により**指導した。**

事案：NTT ラーニングシステムズにおいて，事務所移転の際，個人情報を記録したノートパソコンを紛失

2007 年４月　個人情報漏洩で，**日本郵政公社を厳重注意**とし，個人情報の適正な管理の徹底を文書により**指導した。**

事案：顧客情報が個人所有の記録媒体に保存・持ち出されて盗難に合い漏洩

2007 年３月　個人情報漏洩で，**ＮＴＴレゾナント（「ｇｏｏ」を運営）を厳重注意**とし,個人情報保護法及び電気通信事業における個人情報保護に関するガイドラインにおける安全管理措置に関する規定に違反したとして，文書により**指導した。**

事案：顧客情報をフラッシュメモリーに複写・持ち出し自宅の個人用パソコンに保存・盗難・漏洩

2007 年１月　個人情報漏洩で，**ＮＴＴドコモを厳重注意**とし,個人情報保護法及び電気通信事業における個人情報保護に関するガイドラインにおける安全管理措置に関する規定に違反したとして，文書により**指導した。**

事案：業務委託先の社員が事務所移転準備作業中に事務所備品購入のためショッピングセンターの駐車場に車を駐車，車から離れている間に車上あらしに遭い個人情報を記録したＵＳＢフラッシュメモリーの入ったバッグが盗難に遭い個人情報が漏洩

2006 年９月　個人情報漏洩で，**ＫＤＤＩ株式会社**を電気通信事業における個人情報保護に関するガイドラインにおける個人情報の適正管理に関する規定に違反したとして，文書により**指導した。**

事案：顧客情報管理システムの検証業務に携わっていた業務委託先社員が自宅で作業を行う目的で業務用パソコンを持ち帰り，個人所有のパソコンに当該データを保存，知人に提供したことにより発生。ＫＤＤＩのインターネット接続サービスである「ＤＩＯＮ」の顧客情報を提示し，金銭を要求したとして２名が恐喝未遂容疑で逮捕・起訴，その後，個人情報の流出に関わった２名が著作権法違反で書類送致された。

社団法人生命保険協会　－　勧告

2010 年３月　**アリコジャパン**に対して認定個人情報保護団体業務規程第６条第２項の規定に基づき，生保指針および生保安全管理実務指針に基づく，従業者・委託先の適切な監督等を通じ，個人情報の適正な取扱いの徹底を図るよう**勧告した。**

事案：ホストコンピュータに不正にアクセスし，顧客情報を社外に持ち出す

財団法人日本情報処理開発協会　－　プライバシーマーク付与認定の一時停止措置

2011 年２月　**千代田興産株式会社**に対して，財団法人日本情報処理開発協会の定めるプライバシーマーク制度設置及び運営要領第 21 条の２第１項に基づき，同社が納入，運営を行った図書館管理システムにおいて，図書館の利用者に係わる個人情報が漏洩した事故について，**プライバシーマーク付与認定の一時停止措置**を講ずることとした。

事案：図書館ホームページの更新作業対応時に，確認漏れにより，一時的にパス

ワード設定が外れ，外部からのアクセスが可能に

2011年1月　**三菱電機インフォメーションシステムズ株式会社**に対して，財団法人日本情報処理開発協会の定めるプライバシーマーク制度設置及び運営要領第21条の2第1項に基づき，同社が開発した図書館システムにおいて図書館利用者に係わる個人情報が漏洩した事故について，**プライバシーマーク付与認定の一時停止措置**を講ずることとした。

事案：個人情報が含まれていることを認識せず，パートナー会社へ図書館システムを販売し，かつ，パートナー会社がサーバを誰でもアクセスできる状態（アノニマス設定）に設定，第三者にプログラムおよびデータをダウンロードされ，そこに含まれていた個人情報が流出

財団法人日本情報処理開発協会　－　改善要請

2007年3月　**大日本印刷株式会社**に対して個人情報の取り扱いが適切であることを示す「プライバシーマーク」の認定を行なっている財団法人日本情報処理開発協会（JIPDEC）は約864万件の個人情報漏洩事故を起こした大日本印刷に対して**改善要請**の処分を**決定した。**

⇒カード情報を社外に持ち出し，ネット通販詐欺などに発展

2. 調査項目

2-（2）医療機関等の設置端末等からインターネットに接続する際の脅威への対策動向調査

医療機関等の設置端末からインターネットに接続する際に留意すべき法制度に係わる事項および技術的事項が記載されている対策文書を調査する。

－ 調査結果 －

- 法制度に係わる事項
- 技術的事項が記載されている対策文書

法制度に係わる事項

日本国憲法	第21条（集会・結社・表現の自由，通信の秘密）
高度情報通信ネットワーク社会形成基本法	第22条（高度情報通信ネットワークの安全性の確保等）
刑法	第134条（秘密漏示） 第157条1（虚偽申請による公文書の虚偽記録） 第158条1（偽造公文書の行使） 第161条2（電磁的記録不正作出及び供用） 第163条2（支払用カード電磁的記録不正作出等） 第163条3（不正電磁的記録カード所持） 第163条4（支払用カード電磁的記録不正作出準備） 第233条（信用毀損及び業務妨害） 第234条2（電子計算機損壊等業務妨害） 第246条2（電子計算機使用詐欺） 第258条（公文書電子データ損壊） 第259条（私用電子データ損壊）
民法	第96条（詐欺又は強迫）
著作権法	
特許法	
不正競争防止法	第21条（罰則） ・退職者による営業秘密の不正使用・開示に対する罰則 ・営業秘密を不正に取得して使用・開示した者が属する法人等に対する罰則
不正アクセス行為の禁止等に関する法律	
個人情報の保護に関する法律	
医療法および各種業法等	医療法　第八章　罰則　第七十二条 正当な理由がなくその秘密を漏らしたとき

技術的事項が記載されている対策文書

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」

－　関連する要求事項　－

6.5 技術的安全対策

B. 考え方

技術的な対策のみで全ての脅威に対抗できる保証はなく，一般的には運用管理による対策との併用は必須である。

しかし，その有効範囲を認識し適切な適用を行えば，技術的な対策は強力な安全対策の手段となりうる。ここでは「6.2.3 リスク分析」で列挙した脅威に対抗するために利用できる技術的な対策として下記の項目について解説する。

(1) 利用者の認識及び認証

(2) 情報の区分管理とアクセス権限の管理

(3) アクセスの記録（アクセスログ）

(4) 不正ソフトウェア対策

(5) ネットワーク上からの不正アクセス

なお，情報及び情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については，別途，「6.9 情報及び情報機器の持ち出しについて」に記載しているので参照されたい。

以下，

(1) 利用者の認識及び認証

＜認証強度の考え方＞

＜IC カード等のセキュリティ・デバイスを配布する場合の留意点＞

＜バイオメトリクスを利用する場合の留意点＞

(2) 情報の区分管理とアクセス権限の管理

(3) アクセスの記録（アクセスログ）

(4) 不正ソフトウェア対策

(5) ネットワーク上からの不正アクセス

(6) その他

の順に考え方を記載

6.11 外部と個人情報を含む医療情報を交換する場合の安全管理

B. 考え方

ここでは，組織の外部と情報交換を行う場合に，個人情報保護及びネットワークのセキュリティに関して特に留意すべき項目について述べる。ここでは，双方向だけではなく，一方向の伝送も含む。外部と診療情報等を交換するケースとしては，地域医療連携で医療機関，薬局，検査会社等と相互に連携してネットワークで診療情報をやり取りする，診療報酬の請求のために審査支払機関等とネットワークで接続する，ASP・SaaS 型のサービスを利用する，医療機関等の従事者がノートパソコンの様なモバイル型の端末を用いて業務上の必要に応じて医療機関等の情報システムに接続する，患者等による外部からのアクセスを許可する，等が考えられ

る。

医療情報をネットワークを利用して外部と交換する場合，送信元から送信先に確実に情報を送り届ける必要があり，「送付すべき相手に」，「正しい内容を」，「内容を覗き見られない方法で」送付しなければならない。すなわち，送信元の送信機器から送信先の受信機器までの間の通信経路において上記内容を担保する必要があり，送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」及び「改ざん」，通信経路への「侵入」及び「妨害」等の脅威から守らなければならない。

ただし，本ガイドラインでは，これら全ての利用シーンを想定するのではなく，ネットワークを通じて医療情報を交換する際のネットワークの接続方式に関して幾つかのケースを想定して記述を行う。また，ネットワークが介在する際の情報交換における個人情報保護とネットワークセキュリティは考え方の視点が異なるため，それぞれの考え方について記述する。

なお，可搬媒体や紙媒体を用いて情報を搬送する場合は，付則１及び２を参照願いたい。

以下，

B-1. 医療機関等における留意事項

① 「盗聴」の危険性に対する対応

② 「改ざん」の危険性への対応

③ 「なりすまし」の危険性への対応

B-2. 選択すべきネットワークのセキュリティの考え方

Ⅰ．クローズドなネットワークで接続する場合

① 専用線で接続されている場合

② 公衆網で接続されている場合

③ 閉域 IP 通信網で接続されている場合

Ⅱ．オープンなネットワークで接続されている場合

Ⅲ．モバイル端末等を使って医療機関等の外部から接続する場合

1) 公衆網（電話網）を経由して直接ダイアルアップする場合

2) インターネットを経由して接続する場合

B-3. 従業者による外部からのアクセスに関する考え方

B-4. 患者等に診療情報等を提供する場合のネットワークに関する考え方

の順に考え方を記載

厚生労働省「医療情報システムを安全に管理するために」

厚生労働省「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」

－ 関連する要求事項 －

Ⅲ 4. (1) ⑦技術的安全管理措置より

・ 個人データの盗難・紛失等を防止するため，個人データを取り扱う情報システムについて以下のような技術的安全管理措置を行う。

－個人データに対するアクセス管理（ID やパスワード等による認証，各職員の業務内容に応じて業務上必要な範囲にのみアクセスできるようなシステム構成の採用等）

－個人データに対するアクセス記録の保存