厚生科学研究費補助金(医療技術評価総合研究事業)分担 研究報告書

(3年継続の一年目)

「インターネットを活用した医療施設情報の提供と利用の促進及び安全な医療情報流通促進のための個人情報の取り扱いに関する調査研究」

・主任研究者　大櫛陽一　東海大学医学部

・分担課題 「インターネット利用におけるセキュリティの確保並びに個人情報の保護の在り方に関する調査研究」

・分担研究者

辰巳治之　札幌医科大学附属情報センター所長

・分担研究協力者

花井荘太郎　国立循環器病センター

大山博司　医療法人社団明人会田島病院

三谷博明　日本インターネット医療協議会

＜研究要旨＞

インターネットを利用して個人の医療情報を送受信する際には、扱われる情報が個人を特定できるものであることが多くなることから、プライバシー保護の観点から、情報の扱い方に留意しなければならない。今日、個人の医療情報が電子化して記録、保存される機会が増えてきているが、これらの情報が、ネットワークを介して広域的に容易に伝送されるようになってくると、個人にかかる重要な情報が不用意に漏洩したり、不正に利用されるリスクも高くなってくる。

とりわけ、インターネットにおいては、いわゆるパケット通信というかたちで、データが不特定経路を伝送されていくため、その途中において、第三者の盗聴行為により、不正に傍受されたり、改竄されたりする危険がある。また、医療機関内の情報システムが、インターネットに接続されている場合、外部から内部のシステムに侵入し、データを許可なく取得、改竄、消去されたり、保存されている個人情報が不正に利用される恐れがある。

ネットワーク環境におけるセキュリティの確保は、システムの安定運用だけでなく、内部に保存された個人情報等の機密情報を保護する上でも重要な課題である。

こうした状況を踏まえ、本分担研究では、実際のインターネット利用において、個人情報を送受信する際、情報暗号化やウェブサイトの認証機能を付与することにより、利用者の信頼度がどのように変化したかを調査するとともに、医療機関と患者・利用者の間 における暗号化メッセージの送受信システムの実用性を評価、また実際の医療機関のネットワークシステムにおけるセキュ

リティ強度を診断分析してみることにした。

＜研究目的＞

医療情報の安全な流通とその流通促進の為に、医療情報発信のサイト認証や医療相談における暗号化が利用者の意識にどのような影響を及ぼすかをアンケート調査し、セキュリティを上げたメッセージ交換システムの有用性、使用性を評価する。さらに、安全な情報提供のために、医療機関の情報提供システムを外部からセキュリティ診断する。

＜研究方法＞

1　医療機関のウェブサイト認証と医療相談における暗号化に対する利用者意識調査

東京都内にある本研究協力者の病院(田島病院)のウェブサイトにおいては、痛風に関する医療相談を実施している。利用者は、ウェブサイトの特定のページから、相談事項を自由に記入し、送信する仕組みになっているが、この時、病院のサーバーと利用者の端　末との間で、データを送受信する際、SSL による暗号化を行うことで、データの機密性を確保した。

また、ウェブサイトの真正性を保障するため、第三者機関による認証を取得し、ウェブサイト上からも確認できるようにした。その上で、ウェブサイトの利用者対象に、医療系ウェブサイトやメールによる医療相談への信頼感、セキュリティー、プライバシー保護対策への感想や他の医療系サイトでの同様の取り組みの必要性についてアンケート調査を行った。

参考ページ：http://www.tajima-hospital.or.jp/

2　医療機関と患者・利用者間でのセキュリティ度の高いメッセージ交換システムの評価

インターネット上で患者・利用者と医療機関が一般にメッセージをやりとりする際、情報やデータを暗号化し機密性を確保、セキュリティやプライバシーを保護するメッセージングシステムを試作運用し、分担研究協力者にその有用性、使用性を評価してもらった。

具体的には、メッセージの送受信に際し、一般の電子メールソフトを使用せず、いわゆるウェブメールの形態で、ウェブサイト上でメッセージを作成、送信する仕組みを採用した。

送信者は、ID とパスワードによって指定のホームページにアクセスし、専用のウェブ画面上で（一般のメール操作画面と同様なもの）セキュアメール・モードを指定し、特定の相手宛にメッセージ本文や添付ファイル指定して送信する。この際、ログイン用のパスワードとは別に、暗号用鍵を生成する為に任意のパスワードを入力しセンターサーバー上に共通鍵を生成し、メール本文或いは添

付ファイルを暗号化する。ブラウザを使うクライアントとウェブサーバー間はSSL暗号化でデータが伝送され、ウェブサーバーからさらにデータを格納するリレーショナル・データーベース(RDB)サーバー間はトリプルDESにて暗号化を行う。本システムの特長は、データの通信路のみを暗号化で保護するだけでなく、センター DB で保管する情報も暗号化で保護している点にあり、システム管理者であっても情報を参照できない点にある。これによって、送信者・受信者双方の安心感を確保することができる。

センター DB に受信者宛のメールが到着したことを、受信者には一般のメーラーを通じて配信到着の通知を行い、受信者は、指定されたアドレスのページにアクセスし、予め告知されたパスワードを使って、暗号化されたデータを復号化した。

参考ページ：https://enaa.securesites.com/IMECOS/imecos.html

3 医療機関のネットワークシステムに対する外部からのセキュリティ診断

医療機関のインターネットに接続したネットワークシステムを、比較的大きな規模から、小さなシステムまでモデル選定して、ISS 社のインターネットスキャナーを使い、ネットワークが潜在的に有している脆弱点（セキュリティホール）の有無に関する診断を行った。ネットワークパターンは図 1 にあるように A、B、C、D の 4 つのパターンがあり、それぞれどれに該当するか回答してもらった。

なお、今回はネットワークの外部からのリモート診断につき、外から見えるサービスのみを対象とし、サーバーへのバッファオーバーフロー攻撃等の、いわゆるサービス不能(Dos)攻撃テストの類いは含まれていなかった。

主な診断項目は次のとおりである。

・ ポートスキャンによる公開されているサービスの検出
・ バックドア（トロイの木馬）の検出
・ インターネットサービス（SMTP,HTTP,FTP 等）における弱点の検出
・ Unix サービス/ Windows 共有における弱点の検出

＜研究結果＞

1 医療機関のウェブサイト認証と医療相談における暗号化対策に対する利用者意識調査

田島病院のウェブサイト利用者より、2 月 1 日より 2 月 28 日までに 40 件の回答を得た。結果は以下の通りであった。

1．今までに医療系（病院、診療所、病気、健康など）のホームページをご覧になったことがありますか？

はい	いいえ
40	0

2．1ではいと回答された方へ
そのホームページの信頼性に不安を感じたことがありますか？

はい	いいえ	わからない
17	15	8

3．今までにインターネット上で医療相談をしたことがありますか？

はい	いいえ
25	15

4．3ではいと回答された方へ
その医療相談でセキュリティーや個人情報の保護に不安を感じたことがありますか？

はい	いいえ	わからない
19	5	1

5．痛風医療相談は、SSL による暗号化によってセキュリティーを高めていますが、 これについて安心や信頼を感じますか？

感じる	感じない	わからない
30	2	8

6．田島病院のホームページにおけるプライバシーポリシー（個人情報保護規定）をご覧になって安心や信頼を感じましたか？

感じる	感じない	わからない
32	0	8

7．認証や医療相談の暗号化、プライバシーポリシーなどで、田島病院のホームページに信頼感が増しましたか？

増した	変わらない	低下した
40	0	0

8．他の医療機関のホームページや医療相談にもセキュリティー対策や個人情報の保護が必要だと思いますか？

必要だ	必要ない	わからない
39	0	0

その他の意見、感想で以下のような回答があった。(回答文のまま記載)

※インターネットを利用する場合出来るだけ個人情報(氏名、住所、電話番号)などを記入しないように心がけています。
※インターネットやメールを利用している以上セキュリティーの不安がいつもあります。
※ベリサインのことなどはよくわかりませんが、安心して情報などをかける点は良いと思います。
※ハッカーやメールでのなりすましなどは、今後も予想されます。
※今まで医療機関だ、と言うだけで無条件に安心しきっていた感がありました。でも医療機関のホームページの方からこういった問題に積極的に取り組んでいただけたと言う 点で自分の認識の甘さを改めて自覚することが出来ました。
※ホームページは、その病院の診療内容や専門がわかり病院を選ぶときの非常に有効な判断材料になります。
※痛風などもそうですが、重い病気の場合医療相談は特に個人情報の保護が必要です。
※医療機関を WEB でつなぎ、個人の病歴(カルテ)などを一括管理しようという記事を新聞で読みましたが、WEB に対してそこまでの信頼感を持っている方は少ないのではないかと思います。

2 医療機関と患者・利用者間でのセキュリティ度の高いメッセージ交換システムの評価

医療機関と患者・利用者の間におけるメッセージのやりとりを通常の電子メールによらずウェブサイト上で送受信し、サーバーの外に出さないシステムは、PGP などの送受信の相手とも鍵の発行を要する PKI(公開鍵認証基盤)を使った暗号化メールに比べると、使いやすさの点で有利であった。また、メールソフトや端末の設定に依存しないので、ブラウザさえあれば、どこからでも利用できる簡便性があった。

ただ、ウェブ上で相手がメールを解読するこのシステムは、共通鍵方式で相手にパスワードを送る必要があるため、何らかの方法でこのパスワードを送らなければならない面倒さはあった。パスワードを知らない相手に自動でこのパスワードを生成、メールで送る方法は、多少、セキュリティー面での難があるが、初めての相手に秘匿性の高いメールを送るには便利であった。

3 医療機関のネットワークシステムに対する外部からのセキュリティ診断

ネットワークのセキュリティ診断は、個別のネットワークシステムのセキュリティーホールの有無を指摘するものであり、診断結果はデリケートな情報を含んでいるため、医療機関名を特定しない

方法で、分析する必要があった。また、システム構成が個別に異なるため、均一な質問の設定、またその集計ができなかった。

そこで、個別に問題が指摘された点を提示できる部分について聞き取り可能なところからのみ回答をもらった。診断を実施した場所は、全部で 6 施設 7 カ所であったが、そのうち、実際に回答を得たのが 5 施設であった。

その要点を以下に記す。

1）A 医療機関における診断結果

図 1 のネットワークパターン[A]を構成するウェブサーバーに対して診断を行った。 問題点として、ウェブサーバーがプロキシサーバーとしても機能していて、さらにプロキシペネトレーション(プロキシ透過)を許可していることが指摘された。 まず、1 番目にプロキシサーバーのプロキシサービスは、ほとんど制限なしにプロキシペネトレーションを許可していた。プロキシペネトレーションを許可すると、当該サーバーを経由して、他のウェブサイトへの自由なアクセスが可能となり、悪意あ
る第三者によって、当該サーバーが踏み台にされる恐れがあった。

2 番目に、使用されているウェブサーバーシステムには、http サービスをプロキシサーバーとして作動できる機能があり、当該ウェブサーバーがプロキシサーバーとしても動作していることが判明した。プロキシサーバーはファイアウォールとしての機能を有することもあり、このようなかたちでサーバーが構築されると、万一、ウェブサーバーが攻撃され侵入されると、プロキシ(ファイアウォール)サーバーも攻撃され、ひいてはネットワーク全体が無防備となってしまう恐れも否定できないものであった。

以上の診断結果から、当該医療機関のシステムにおいて、1 番目の問題点に対しては、踏み台にされないようなアクセス制限を行い、2 番目の問題点に対しては、ウェブサーバーとプロキシサーバーの同居をやめる設定変更を行い、セキュリティ対策の向上をはかることが勧告された。

また、その他、ftp サービスが匿名のログオンを許可する設定になっていることが指摘されたが、ファイルへのアクセスには制限があり、アクセスできたディレクトリにもファイルは実在せず、アカウントなども取得できなかったので、この点においては問題はなかった。

2）B 医療機関における診断結果

図 1 のネットワークパターン[A]を構成するウェブサーバー、ファイアウォールに対して診断を行った。

今回の診断では外部からの侵入に結びつく弱点は検出されなかった。サービスも必要なものしか公開されておらず、またそのサービスから直接侵入に結びつくセキュリティホールは見つからな

かった。仮にインターネットからの攻撃があるとするならば、ウェブや Telnet を通したファイアウォールへのログイン攻撃、または高度なソーシャルエンジニアリングを使用したものに限定されると予想された。

ただ、危険性をはらむ問題点が 2 つほどあった。

ひとつは、ウェブサービスで、ディレクトリの一覧を許しているディレクトリがあって、今回の診断で有用な情報らしきものこそ確認できなかったが、管理者が何らかのファイルを置き忘れるなどして、侵入のために使用されるような情報を不用意に提供してしまう危険性を含んでいることが指摘された。

また、このウェブサイトでは、traceroute が制限されていなかった。traceroute はふたつのエンドポイント間でパケットが通過するルートを特定するユーティリティであるが、サイト内のパケットの経路情報を提供することで、ネットワークの構成が推測さる可能性もあり、セキュリティ上あまり推奨されるものではない。 traceroute はネットワーク障害時の保守に役立つメリットもあるが、今回はセキュリティを優先し、traceroute 使用を制限するほうが望ましいと勧告された。

3) C 医療機関における診断結果

図 1 のネットワークパターン[A]を構成するウェブサーバー、ファイアウォール、ルーターに対して診断を行った。

ウェブサーバーに関しては、2 台あるウェブサーバーに共通して FTP に関する弱点が検出された。それは、匿名 ftp でのログイン、さらには ftp ディレクトリーへの書き込みを許可していることであった。匿名 ftp の許可はそのサーバーの運用方針に関わることで、必ずしも弱点とは断定できない。ただ、この ftp で入ることのできるディレクトリーがさらに書き込みが許可されていた。匿名 ftp は、たとえば、対外的に公開している情報をダウンロードする場合に限り認めるといったような方針のもとに運用する場合は別として、特に今回のように一時的なファイルの保管場所のような形で、第三者の自由な書き込みを許しているような状態での運用はセキュリティ上好ましくないことが指摘された。悪意のある攻撃者がバックドアなどの攻撃用ツールを仕掛けてくる危険もある。

さらに、公開ウェブサーバーの 1 台から cgi-bin 関係の弱点が検出された。この弱点は cgi-bin ディレクトリーの下にリモートで実行可能なシェルインタープリターと推測できるファイルが発見されたというものであった。もし、実際にシェルインタープリターが存在している場合は、このページへのアクセスには認証を用いて制限を行うなどの対策をとるべきであろうと勧告された。

次に、ファイアウォールに関しては、ファイアウォールは本来、単独で稼働すべきホストであるにもかかわらず、今回比較的多くのサービスを行っていることが検出された。これは、ファイアウォールの役割を考えると問題であった。多くの攻撃は立ち上がっているサービスを通して行われ、サービスが多くあがっているということはそれだけ攻撃用のホールを用意しているということになる。ファイアウォールから多くのサービスがあがっていれば、いざという時にファイアウォールとしての役

目を果たせなくなる恐れがある。今回の診断では、ファイアウォールから telnet、ftp、smtp、pop3 といったサービスが検出された。これらのサービスは TCPwrapper 等でのアクセス制御を行っていたとしても、本来、ファイアウォールには不要なサービスであった。TCPwrapper にしても将来的にホールが見つからないという保証はない。

また、ファイアウォールの BIND のバージョンは特定できなかったが、BIND のバージョンが 8.2.2-P7 以前の場合は、すみやかなバージョンアップを行うことが推奨された。これは、2001 年の 1 月 29 日に報告された BIND のバッファオーバーフローの弱点であるが、これがファイアウォールに対して行われ、攻撃が成立するとファイアウォールが機能を停止し、ひいては内部のネットワークに大きい打撃を与える恐れがあることが指摘されている。

最後にルーターに関しては、echo、chargen 二つのサービスが検出された。これらは、設定上の都合かも知れないが、必要に応じてサービス停止などの処置をとることが推奨された。

4) D 医療機関における診断結果

図 1 のネットワークパターン[C]を構成するウェブサーバー、メールサーバー、ルーターに対して診断を行った。

ウェブサーバーに関しては、使用している Bind のバージョンにおいて、バッファオーバーフローの弱点を有することが判明した。これは、放置しておくとリモートからルート権限を取得される恐れがあるというものだった。今回の診断では、サーバーを使用不能にする Dos 攻撃は行っていないので、実際に確認したわけではないが、他にも Bind に関しては、「xzfr」「sigdiv0」「srv」「infoleak」「tsig」と呼ばれる弱点が報告されている。特に、「tsig」は最近発見された非常にクリティカルなセキュリティホールで、攻撃者が類似の攻撃を仕掛けて来る可能性がないとはいえない。Bind については、これからもセキュリティホール情報を頻繁にチェックすることが勧告された。

次に、メールサーバーに関しては、今回の診断の範囲内では、セキュリティはかなり強固に構築されているとうかがえた。サービスが外部セグメントからは見えない構成になっていて、外部から内部への攻撃を成立させることは困難な状況であった。ただし、今回は、サービス不能攻撃等のシグニチャも含めたネットワーク内部からの診断を行ったものでないことから、内部セグメントで内部マシンに対する診断を行うことで、より高いセキュリティの確保が可能になることが推奨された。

なお、ルーターに関しては、今回の診断の範囲内においては弱点は検出されなかった。

5) E 医療機関における診断結果

図 1 のネットワークパターン[C]を構成するウェブサーバー、ファイアウォール、ルーターに対して診断を行った。

まず、1 番目にウェブサーバーの IIS4.0 に関係する弱点が三つ検出された。中でも、RDS(リモートデータサービス)に関する弱点は、攻撃者がアカウント、パスワード、テーブルに関する情報を持

っていることが前提となるが、特にパスワードが適切に設定されていない場合は、高いリスクを露呈してしまうことになり、早急な対策が勧告された。 IIS は、ごく最近においてもセキュリティホールが発見、報告され続けており、すでにくつかのホールに対してパッチ等で対策がとられている形跡もあったが、今後とも十分な注意が必要とされた。

2 番目に、当該サーバーがウェブサーバーとファイアウォールサーバーを兼ねていて、診断ログを解析した結果、CSM プロキシサーバーとウェブサーバーの共存が明らかになった。この状態では、万一、ウェブサーバーが攻撃され侵入されると、ファイアウォールサーバーも攻撃され、ひいてはネットワーク全体が無防備となってしまう恐れも否定できなかった。ウェブサーバーとファイアウォールサーバーは異なるマシンで構築することが勧告された。

3 番目に、当該サーバーはゾーン転送を許可していた。ゾーン転送の弱点は、DNS に登録されているホストの一覧を攻撃者に取得されてしまう、というものである。ゾーン転送は、一般的にセカンダリーネームサーバーに対してのみ許可しておけばいいとされている。セキュリティの観点からは、ゾーン転送は基本的に制限されるべきであると勧告された。

その他、BIND のバージョンが取得できたということがあった。これだけでは、即、危険があるとは言えないが、将来の更なる攻撃にこの情報が使用されることも否定できなかった。

ルーターの診断においては、重大な危機に結びつくようなセキュリティホールは発見できなかったが、致命的ではない弱点として、ネットマスク要求とタイムスタンプ要求のふたつが検出された。

＜考察＞

1 医療機関のウェブサイト認証と医療相談における暗号化に対する利用者意識調査

回答者全員が医療系のウェブサイトを閲覧した経験を持っていた。その半数以上の方が医療系サイトの信頼性に不安を感じていた。さらに、インターネット上で医療相談をしたことがある人のうち 76%が、セキュリティーや個人情報の保護に不安を感じていた。このことから、医療相談サイトなどを訪れても個人情報保護の不安から実際の相談を行っていないことも推察された。痛風医療相談の SSL 化とプライバシーポリシーの策定についてはわからないと答えたのが 20%だったが、残りの 80%が安心や信頼を感じるとの回答していた。

そして、回答者全員が、こうした取り組みで病院のウェブサイトへの信頼感が増し、他の医療系サイトでも同様の取り組みが必要であると考えていることがわかった。

ウェブサイトは誰でも開設できる反面、全くの第三者が名前を騙ることも容易である。このことは、医療機関にとっても重大な問題であるが、利用者にとってはより深刻で不安を感じているところである。現在、閲覧しているウェブサイトが本当に信頼できる医療機関のものなのか、またそこに送信した医療相談の個人情報が保護されているということを利用者に保証していく必要がある。第三者機関によるウェブサイトの認証を行い、それを告知するシステムが有効であることが確認できた。また、医療相談の送受信データの SSL 暗号化でセキュリティーに対する安心感を与えられる

ことがわかった。

2　医療機関と患者・利用者間でのセキュリティ度の高いメッセージ交換システムの評価

通常の電子メールでメッセージを送受信する際、いつどこで誰にデータを拾われているかわからない不安がある。個人の医療情報のような機密性の高い情報は、暗号化等で保護する必要があるが、お互いに認証 ID を持ちあったり、公開鍵を作成、公開するといった手間から普及が進んでいない。医療機関、医師どおしならまだしも、患者が独自に暗号化メールを使いこなすのは難しいものがある。こうした時に、秘匿性の高いメッセージの送受信が簡易に行えるウェブメール方式の利便性は高いものがあった。

テキスト文章だけでなく、ファイル等も暗号化して送受信できるので、電子データの伝送、保管に向いているといえる。暗号メッセージの解読には共通鍵を使用するため、パスワードを共有する必要とするが、このパスワードの伝達法には工夫の余地がある。

3　医療機関のネットワークシステムに対する外部からのセキュリティ診断

ネットワーク構築上のセキュリティ要件については、セキュリティについての考慮が、ネットワーク構築形態によって多種多様であり、個々の事例によって相当細かな点まで調査しないと安全度が評価できないという問題がある。

ネットワークにおけるセキュリティの保守は、技術的にも高度で専門的な知識が必要であり、日常のメンテナンスの程度も大きな要因になることから、誰もが安全にシステムの運用ができるわけではないことに注意を払わねばならない。医療機関において、「ウェブサイトを開設すること」と「安全に運用すること」の間には相当の技術的ギャップがあるということに留意する必要がある。

昨今のホームページ改ざん事件に見られるように、明らかに低い管理レベルのサーバーが外部から攻撃されたりする事例だけで、すべてのウェブサイトが危険だと見るのも早計ではあるが、管理が悪いサーバ、ネットワークがハッキングされ、その結果が外部から目に見える形で最初に現れるのがウェブサイトだと考えることもできる。

自院のネットワークシステムのセキュリティの確保で、技術的に不安がある場合は技術に通じた専任の担当者を配置するなり、外部の専門家のアドバイスを受けるなりして、必要なセキュリティ基準を確保することが重要である。また、そのような体制を組めない場合は、無理に自分でサーバやネットワークを管理せず、信頼できるプロバイダーなどの外部サービスを利用するのが賢明であると思われる。

＜結論＞

医療分野でのネットワーク利用において、完全にクラッカーなどの攻撃からシステムを守ること

は不可能に近いが、ある程度のセキュリティー対策を練ることにより、安全性は向上し、さらに利用者側に対する信頼感と安心感を与えることができる。このことからセキュリティ対策を練ることは、セキュリティ向上だけでなく、利用者側の安心感を高め、医療情報流通の促進が図れるものと考える。

医療系における高度情報化促進のためには、セキュリティ対策は必須のものと認識し、もっと当たり前のようにセキュリティ対策が練られるようにすべきであろう。そこで、ウェブサイトが正当なものであることの確認、利用者の確認、データ、メッセージの保護、それから秘密通信を行うための共通鍵方式のセッション鍵の交換、あるいは公開鍵方式の利用などが、容易にできるようになっていく必要があると考える。

その為にも今後 IPsec や QoS などが標準で考えられている IP v6 などの技術の発展が、医療系においては、より一層期待される。

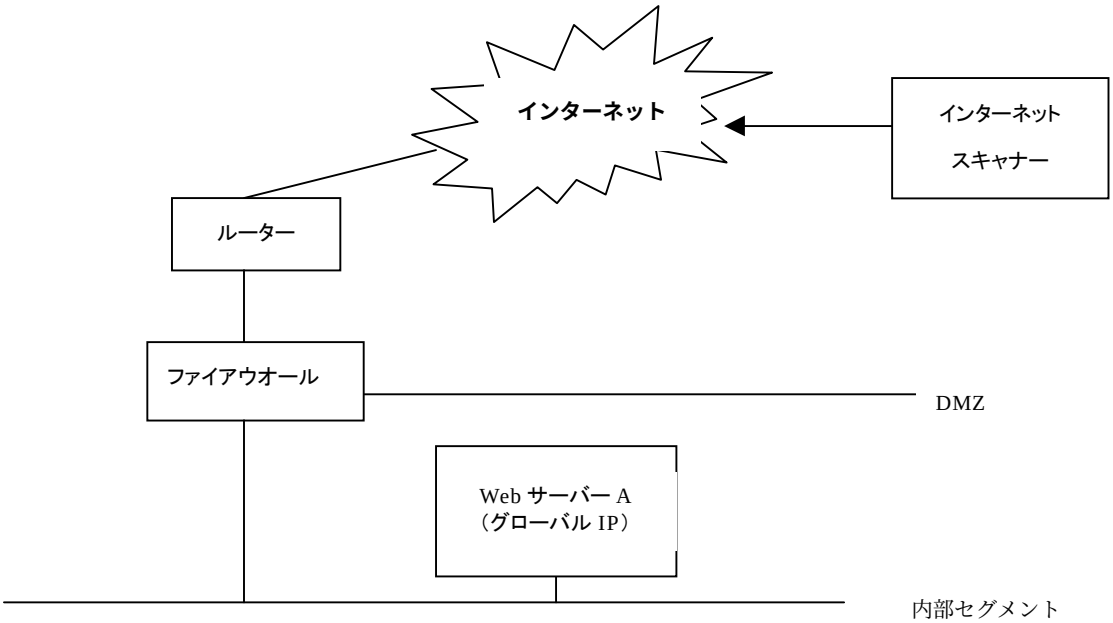
図 1 ネットワークのパターン: DMZ(DeMilitarized Zone:非武装地帯)

1) ネットワークパターン [A]

検査対象:・ルーター、ファイアウオール

・内部セグメントにある Web サーバー A1台(グローバル IP を持つもの)

検査方法: インターネット越しのリモートスキャン

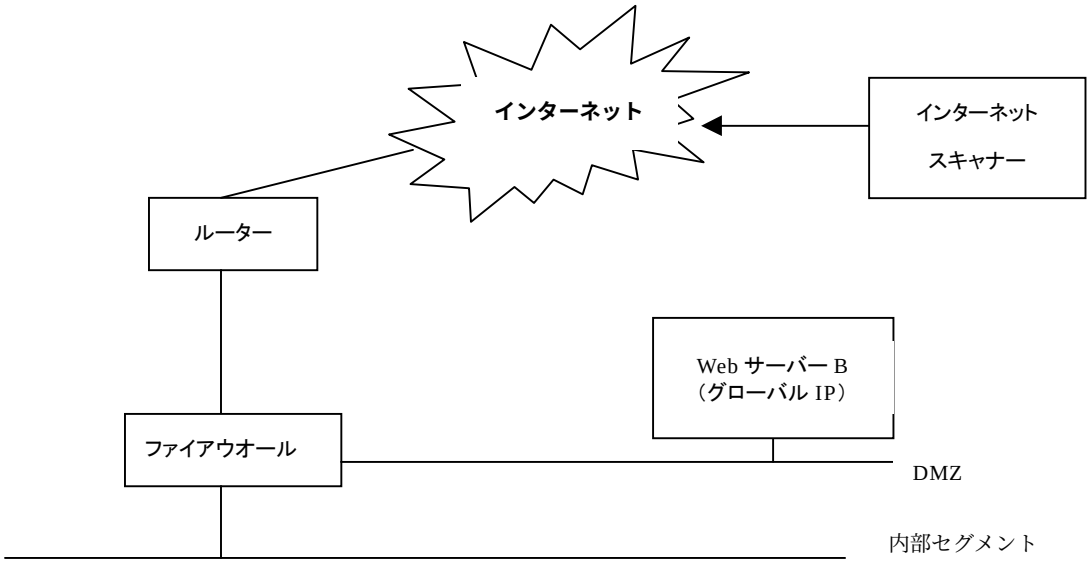


2) ネットワークパターン[B]

検査対象：・ルーター、ファイアウオール

・DMZ にある Web サーバー B1台（グローバル IP を持つもの）

検査方法： インターネット越しのリモートスキャン

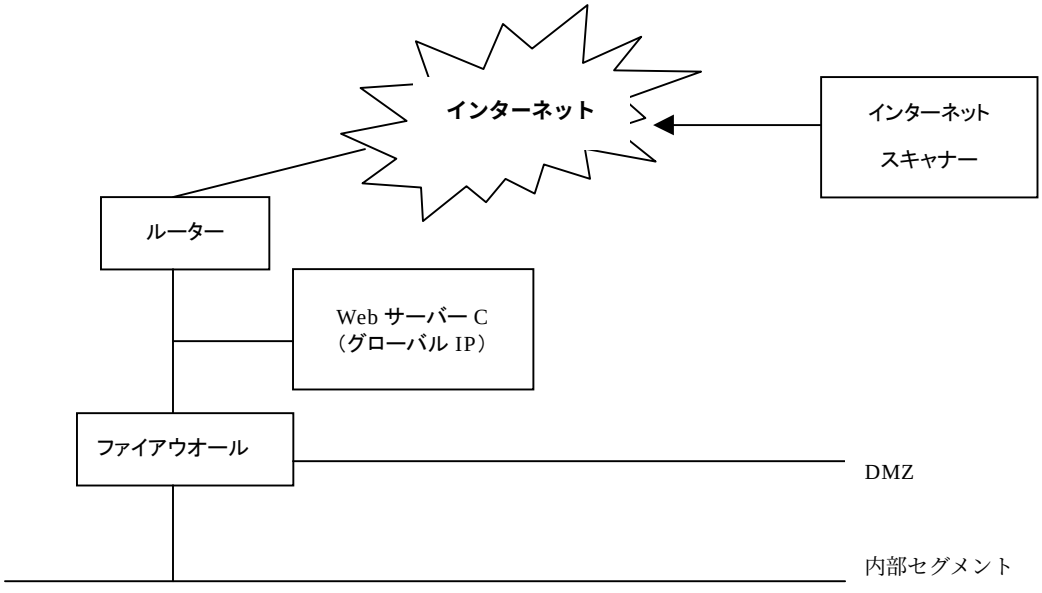


3) ネットワークパターン[C]

検査対象：・ルーター、ファイアウオール

・ルーター直下に有る Web サーバー C1台（グローバル IP を持つもの）

検査方法： インターネット越しのリモートスキャン



4） ネットワークパターン[D]（ファイアウオールが存在しない場合）

検査対象：・ルーター、

・ルーター直下に有る Web サーバー D1台（グローバル IP を持つもの）

検査方法： インターネット越しのリモートスキャン