厚生労働科学研究費補助金

エイズ対策研究事業

HIV診療支援ネットワークを活用した診療連携に関する研究

平成15年度総括研究報告書

主任研究者　秋山昌範

平成１６年３月

目　次

Ⅰ．総　括　研　究　報　告　書

平成15年度厚生労働科学研究費補助金（エイズ対策研究事業）
総括研究報告書

HIV診療支援ネットワークを活用した診療連携に関する研究

主任研究者　秋山 昌範　国立国際医療センター情報システム部長

研究要旨　本研究はＨＩＶ診療支援ネットワーク(A-nat)における有効活用のための検討を行った。診療情報の共有化を図るには、それを遂行するインフラや運用指針が必要である。患者データを共有するためには、高度のセキュリティレベルが要求される。今後の有効活用を図るためには、各施設内の診療システムとの有機的な連携を図る必要があり、その際にセキュリティを維持する方法は確立していない。そこで、構内LANにおけるセキュリティ上の問題点の調査検討するための方法論を検討した。今年度は汎用医療VPNを構築するための要件について、検討を行った。また、セキュリティ向上のため、LAN内での端末認証や端末制御技術及び指紋認証の有効性の検証を行った。

また、二次利用における患者のプライバシー保護とは、二次利用する際に、個人が特定できないことを意味する。そこで、どの様にすれば、患者のデータと患者個人が連結できない状態である無名性を確保できるかの検討を行った。その他、利用者や患者、国民の意識調査を行う必要性が判明し、各施設利用者への意識調査のためのアンケート表作成を行った。

一方で、PR(Public Relations)と呼ばれる啓発手法の調査研究を行った。また、各施設利用者への意識調査のためのアンケート表作成と啓発を目的としたビデオ制作を行った。その結果、利用者や患者、国民の意識調査を行う必要性が判明した。またアンケートは意識データの収集のみならず、啓発活動としても有用であることが分かり、同時にビデオ上映や配布による啓発が有効であることも示唆された。また、ソシュールの記号論を検討し、アプローチ手法の検証を行った。そこで、目標を「A-net の周知」から、「A-net『技術情報』の周知」と限定させ、その上で各ステークホルダー（利害関係者）の認知度や好感度等を調査する必要があると考えられた。

分担研究者
木内 貴弘
東京大学医学部附属病院中央医療情報部助教授
山本 隆一
大阪医科大学医学部病院医療情報部助教授
高橋 紘士
立教大学コミュニティ福祉学部教授

A. 研究目的

研究は、我が国で初めて導入された診療情報共有システムであるHIV診療支援ネットワークシステム(A-net)の導入により、エイズ拠点病院に指定されている全国の病院においてHIV診療の標準化を行うことを最終目標に、HIV診療情報の共有化や研究を行えるような方法論確立を目指すものである。A-net以外に大規模臨床データが蓄積されていないのが現状である。それには、いくつかの問題点があると予想されるが、大きく分けて、技術的側面と患者の心理的側面に分けられると考えられる。アンケート調査等を行い、それから得られる結果と併せて、患者が不安材料として抱える因子を抽出し、不安化要素の集計から、不安度により研究計画を3段階に分類し、「匿名性の確保の程度 VS 不安度」のマトリックス構造で、研究の安全性の指標化を図ることができると予測される。実際にその定量化にあたっては症例数を増やした検討や患者から見た場合の「ITというなじみのない技術を使うことによる躊躇」を克服するための方策も必要であり、集団心理面からの検討も行う。本研究により、集積されたデータについて、プライバシーを保護しながら解析研究するための方法（無名性の確保）を検討する。ネットワーク化した患者データベースはいわゆる電子カルテのようなものである。医療情報学の分野において、医療情報ネットワークや電子カルテ等の研究が行われているが、すべて実験段階であり、実際に運用している例は稀である。本研究において、無名性を確保するための指針を定めることができれば、他の臨床研究への応用や新技術であるデータマイニングへの利用が可能になると思われる。その結果、今後のエイズ対策に必要な臨床疫学研究を可能にする疾病データベースの構築が可能になると期待される。

B. 研究方法

研究は、１）情報技術を中心に検討、２）デー

タの二次利用におけるセキュリティ：無名性確保のための方法と運用ガイドラインの検討、3）プライバシー保護に関する社会学的、心理学的要因の検討に分担される。

1）情報技術を中心に検討　医療の情報化へのグランドデザインが出され、平成 18 年度までに60%以上の臨床研究指定病院や地域医療支援病院に電子カルテが導入されることになった。さらに、文部科学省の学術情報ネットワーク（SINET）や一般のインターネットにおいて、安全に個人情報が扱えるように、セキュリティのある情報基盤を整備する必要がある。そこで、A-net が各病院内における電子カルテ端末で利用できることが望ましい。しかし、現状では各病院内における端末のセキュリティレベルは低く、A-net の運用規定のレベルに達していない。本研究の初年度は、まず Virtual Private Network （ＶＰＮ：仮想専用線網）の技術を用いて、インターネットを介した安全な情報基盤の技術を確立し、大学病院内の情報システムを含めたブロック拠点病院や主要な拠点病院間での単一のネットワーク接続機種間での運用を目指す。さらに、次年度には、IPv6 などの普遍的な技術を導入し、異機種間の運用実験に必要な要件検討を行う。また、現在、コンピュータウィルスの侵入や情報漏洩など、内部の人間が関わるトラブルが深刻になると予想されている。A-net においても「端末の完全制御」について技術検討が必要である。また、個人認証技術の発達により、指紋等の生体認証を導入することで、利便性とセキュリティの両立を図ることが可能である。来るべきユビキタス時代を念頭に、医療の情報化に普遍的に寄与できるインターネット上でセキュリティを保持した情報基盤技術を確立し、各病院内における電子カルテ端末における A-net の相互利用を目指すものとする。

2）データの二次利用におけるセキュリティ：無名性確保のための方法と運用ガイドラインの検討患者情報の収集や参照を行うためのネットワークとは別に、集積されたデータを臨床研究等に活用する際に、患者のプライバシー保護を行うためのセキュリティ要件を検討する。初年度は各種個人データの行政等における海外を含む事例やその利用形態について、調査研究を行う。次年度は初年度に行った調査の問題点の検討と運用面を検討し、HIV 診療における EBM 研究のための方法論を確立する。現在までに集積されたデータを解析して新規診断法や治療法の開発への応用が期待され、国際医療センターにおいて A-net のデータを用いた解析法の検討を行っている。さらに、A-net 構築にあたっては、原告団・弁護団と協議の上進めてきた経緯があるので、今後の診療体制のあり方やカルテ開示など、現在の診療体制の課題にも応用可能であると考えられており、A-net の管理体制・管理要綱・運用細則は、今後の診療支援システムの管理体制のモデルとなり、すでに肝ネットや腎ネットなど各政策医療ネットワークへの応用が始まっている。しかし、研究の利用者は A-net を利用する臨床医に限られており、研究データの有効活用という点で問題があった。すなわち、研究成果をあげるために、基礎医学者や生物統計学者への拡大が必要である。そこで、個人情報と診療情報を連結不可能な状態にするための情報学的検討と社会学的検討を行う。すなわち、連結不可能な状態である匿名性の定量化の検討を行う。最終年度では、集積されたデータを臨床研究等に活用する際の個人情報保護を踏まえた運用指針の作成を目指す。具体的には、個人情報保護のガイドラインを試作するために個人情報保護法案をポイント別に整理し、それに対応するプライバシー保護実施計画及び実施要件を定める。

3）プライバシー保護に関する社会学的、心理学的要因の検討 HIV 患者の身体障害者手帳利用の際の調査研究より、直接診療目的以外の利用におけるカミングアウトとそのコスト計量を社会学的・心理学的に行う必要があると考えられたが、研究利用ではさらに不安が強くなることが予想される。そこで、診療情報提供による結果としての「自分の病名を他者に知られる等のデメリットや不安感」と「治療の向上の利益をうけられる」というバランス意識を、社会制度や IT に対する理解などと関連づけて解析する研究を行う。具体的には、研究利用などにおいても治療技術の向上についての意識のありかたや自らの情報を提供することが仲間の治療の貢献できるのだという意識のありかた、自分の情報を提供しても医学の進歩貢献したという実感があるかないか等の調査研究のデザインを検討し、研究利用における社会学的問題点の検討を行う。以上のように、患者の個人情報を診療に使う場合と研究に使う場合では差があることが類推される。また、IT というなじみのない技術を使うことによる躊躇も見られる。

そこで、本研究ではマーケッティングの専門家に加わっていただき、新技術への適応に関し、集団心理面からの検討も行う。さらに、米国における個人情報法の指針である HIPPA を参考にしながら、我が国における個人情報保護を踏まえた上で、情報ネットワークシステムを利用した臨床研究における情報学的・社会学的指針を制定できると

考えられる。

（倫理面での配慮）

本研究は、A-net システム部会等を通じ、原告団や弁護団と情報交換を行いながら行う。また、インフォームドコンセントを取って行う予定であり、実験にあたり、個人が判別できるようなデータが一般の目に触れるようなことは原則としてない予定である。各施設内での倫理委員会においても、承認をいただくこととしている。

C. 研究結果

研究は、1）情報技術を中心に検討、2）データの二次利用におけるセキュリティ：無名性確保のための方法と運用ガイドラインの検討、3）プライバシー保護に関する社会学的、心理学的要因の検討に分担した。

1）情報技術を中心に検討

本研究の初年度は、まず Virtual Private Network （ＶＰＮ：仮想専用線網）の技術を用いて、インターネットを介した安全な情報基盤の技術を確立し、大学病院内の情報システムを含めたブロック拠点病院や主要な拠点病院間での単一のネットワーク接続機種間での運用を目指した。その結果、国立国際医療センターにおいて、院内の電子カルテシステム端末で A-net のアプリケーションを操作できる環境を提供できるようになった。従来は、診療時に A-net 端末と電子カルテ端末の２台を操作する必要があったが、同一端末で利用可能になったことより、利便性が向上した。さらに、今後、インターネットなどの普遍的な技術を導入し、異機種間の運用実験に必要な要件検討を行う。

今年度は、汎用医療 VPN を構築するための要件について、検討を行った。すなわち、現在は独自 VPN による A-net 運用となっているが、より効率的な運用のために汎用の医療 VPN ネットワークを活用し、これに A-net 独自のセキュリティ保護手段（128bitSSL）を併用する方法が有効である。そこで、汎用の医療 VPN ネットワーク亀板構築のための技術仕様と、これを活用して A-net を構築するための方法の検討を行った。最終的には、医療の情報化に普遍的に寄与できるインターネット上でセキュリティを保持した情報基盤技術を確立し、各病院内における電子カルテ端末における A-net の相互利用を目指すものである。

さらに、試作された指紋認証装置を評価し、臨床現場での利用について検討を行った。また、構内 LAN 上でセキュリティを確保する技術である 802.1x や、端末制御機能をもつ VPN ソフトウェアについて調査及び予備実験を行った。

2）データの二次利用におけるセキュリティ

無名性確保のための方法と運用ガイドラインの検討患者情報の収集や参照を行うためのネットワークとは別に、集積されたデータを臨床研究等に活用する際に、患者のプライバシー保護を行うためのセキュリティ要件を検討した。初年度は各種個人データの行政等における海外を含む事例やその利用形態について、調査研究を行った。具体的に第一点は、無名性の定義を定め、大学病院情報システムに蓄えられている診療情報項目を用い、無名性の定量化を試みた。第二点は、個人情報保護法案に基づいて、医療分野での個人情報保護ガイドラインを試作した。このような診療データの研究への二次利用に関する検討として、我が国では初めての研究であり、遺伝子情報データベースの研究応用などへの応用も期待される。ただし、患者のプライバシーの保護には十分配慮する必要がある。臨床利用でも研究等の二次利用でもプライバシー保護が重要な課題であるが、二次利用においては本質的にプライバシー情報を扱う必要さえない。そこで、二次利用における無名性確保の方法と有効性について検討を行ってきた。来年度は今年度に行った調査の問題点の検討と運用面を検討し、HIV 診療における EBM 研究のための方法論を確立する予定である。また、現在までに集積されたデータを解析して新規診断法や治療法の開発への応用が期待され、国際医療センターにおいて A-net のデータを用いた解析法の検討を行っている。さらに、A-net 構築にあたっては、原告団・弁護団と協議の上進めてきた経緯があるので、今後の診療体制のあり方やカルテ開示など、現在の診療体制の課題にも応用可能であると考えられており、A-net の管理体制・管理要綱・運用細則は、今後の診療支援システムの管理体制のモデルとなり、すでに肝ネットや腎ネットなど各政策医療ネットワークへの応用が始まっている。しかし、研究の利用者は A-net を利用する臨床医に限られており、研究データの有効活用という点で問題があった。すなわち、研究成果をあげるために、基礎医学者や生物統計学者への拡大が必要である。そこで、個人情報と診療情報を連結不可能な状態にするための情報学的検討と社会学的検討を行った。すなわち、連結不可能な状態である匿名性の定量化の検討を行った。今後、集積されたデータを臨床研究等に活用する際の個人情報保護を踏まえた運用指針の作成を目指す。具体的には、個人情報保護のガイドラインを試作するために個人情報保護法案をポイント別に整理し、それに対応するプライバシー保護実施計画及び実施要件を検討する予定である。

3）プライバシー保護に関する社会学的、心理学

的要因の検討

HIV 患者の身体障害者手帳利用の際の調査研究より、直接診療目的以外の利用におけるカミングアウトとそのコスト計量を社会学的・心理学的に行う必要があると考えられたが、研究利用ではさらに不安が強くなることが予想される。そこで、診療情報提供による結果としての「自分の病名を他者に知られる等のデメリットや不安感」と「治療の向上の利益をうけられる」というバランス意識を、社会制度や IT に対する理解などと関連づけて解析する研究を行う。具体的には、研究利用などにおいても治療技術の向上についての意識のありかたや自らの情報を提供することが仲間の治療の貢献できるのだという意識のありかた、自分の情報を提供しても医学の進歩貢献したという実感があるかないか等の調査研究のデザインを検討し、研究利用における社会学的問題点の検討を行う。以上のように、患者の個人情報を診療に使う場合と研究に使う場合では差があることが類推される。また、IT というなじみのない技術を使うことによる躊躇も見られる。そこで、本研究ではマーケッティングの専門家を加え、新技術への適応に関し、集団心理面からの検討も行う。さらに、米国における個人情報法の指針である HIPAA を参考にしながら、我が国における個人情報保護を踏まえた上で、情報ネットワークシステムを利用した臨床研究における情報学的・社会学的指針を制定できると考えられる。そのなかで、患者のプライバシーが保護されているという感情を前提として、臨床データを活用できる環境はどのような条件が必要かを患者がもつ自分はプライバシーが保護されつつ必要の受診をしているという意識がなりたつための条件を明らかにする必要がある。このような点をあきらするための研究デザインを検討することが本年度の課題であった。そのための手がかりの一つとして、免疫不全者を身体障害者法上の内部障害者として、福祉サービス給付の対象とされたことをふまえ、これらの事由の障害者が身体障害者手帳交付のなかでどのようなプライバシー意識を持っているかを調査したデータをてがかりに若干の検討を行う。本年度は研究デザインを策定し、最終年度は実際の調査研究を行った。

その結果、患者から見た医療機関への信頼性の定量的尺度が必要と考えられた。　一方で、本年度は、PR(Public Relations)と呼ばれる啓発手法の調査研究を行った。また、各施設利用者への意識調査のためのアンケート表作成と啓発を目的としたビデオ制作に着手した。その結果、利用者や患者、国民の意識調査を行う必要性が判明した。またアンケートは意識データの収集のみならず、啓発活動としても有用であることが分かり、同時にビデオ上映や配布による啓発が有効であることも示唆された。次年度以降は情報工学的な調査研究と社会学的な研究解析を平行して行い、啓発につなげる予定である。また、国民が求めるデータの二次利用におけるセキュリティ要件を明らかにしたい。

今年度は広報学的アプローチを用いソシュールの記号論を検討し、情報をデノテーション（内包的）、コノテーション（外延的）に分解してアプローチする手法の有効性を検討した。そこで、目標を「A-net の周知」から、「A-net『技術情報』の周知」と限定させ、その上で各ステークホルダー（利害関係者）の認知度や好感度等を調査する必要があると考えている。また記号論によると、「A-net」という名称も、わかりやすく親近感のあるものへ変更する必要性が示唆されている。

以上を踏まえ、最終年度はこれを実際に応用するプログラムを開発することで、A-net 利用者以外の研究利用という二次利用拡大を図りたい。

D．考察

1999 年度より国立ブロック拠点病院において A-net の稼動が始まり、その後全国の国立エイズ拠点病院にも利用が広がったことから、国立国際医療センターとブロック拠点病院間だけでは無く、国立ブロック拠点病院とエイズ拠点病院の連携強化の基盤が整った。医療情報学の分野において、我が国で初めて運用された広域ネットワーク版電子カルテシステムとして、技術的に高い評価を受けた。さらに、国際的にも HIV 感染症としては、すでに世界最大規模の臨床情報データベースであり、読売新聞、朝日新聞、東京新聞等にも大きく取り上げられ、HIV 感染症のみならず標準的な電子カルテの開発へと発展しつつある。さらに、診療データの研究への二次利用に関する検討では初めての研究であり、遺伝子情報データベースの研究応用などへの応用も期待される。平成 16 年 3 月末現在、全国 140 のエイズ拠点病院で 314 名の医療従事者登録を達成し、患者登録数も 498 例であったことより、A-net 導入後も緩やかながら常に右肩上がりで登録数が伸びている。また、無名性の検討や患者側の要因に関する検討の研究デザインが決められたので、今後はデザインに基づき以下に述べるように具体的な検討を行う予定である。

HIV 感染症に関して、約 500 例のデータを解析して、新規診断法や治療法の開発への応用が期待され、すでにデータマイニングの手法を用いた研

究応用を検討する。さらに、インフォームドコンセントのあり方や診療情報の研究利用のルールの確立なども応用可能であり、他分野への応用も視野に入れ、検討している。今後は、疾病ゲノムなどHIV感染症以外の他分野への応用が期待される。この研究の素地となる研究として、現在で検討中の個人情報保護法案に基づいて医療分野での個人情報保護ガイドラインを試作した。しかし、現場で実際に対応するためには医療機関の規模別や目的別のガイドラインが必要と考えられた。このような患者の個人情報をどこまで削除すれば個人を特定できないかの定量的検討は、我が国ではまだ十分行われていない。二次利用される診療データでプライバシーを保護するためには無名性を定量化することが重要である。本研究では無名性の指標として最小特定人数を用い、病院情報システムのデータベースで最小特定人数が利用可能なことを示した。本研究を行うことで、安全に二次利用できる方法を確立すれば研究利用者の拡大を図ることが可能になる。今後は、個人情報保護を踏まえた臨床研究における指針の分野別・具体的な検討を行うことで、EBM へとつなげていくことを可能としたい。

さらに、データマイニングの手法を用い、HIV診療におけるEBM研究のための方法論を確立する予定である。現在、国際医療センターにおいてA-net のデータを用いデータマイニングの手法による解析を行っている。なお、A-net 構築にあたっては、原告団・弁護団と協議の上進めてきた経緯があるので、今後の診療体制のあり方やカルテ開示など、現在の診療体制の課題にも応用可能であると考えられており、A-net の管理体制・管理要綱・運用細則は、今後の診療支援システムの管理体制のモデルとなり、すでに肝ネットや腎ネットなどの各政策医療ネットワークへの応用が始まった。一方で、今後の診療データベースの臨床疫学への応用のためには、患者側からの信頼を得ることも必須であり、本研究における無名性の科学的な検証や患者側の要因の検討により、個人情報保護法を見据えたプライバシー保護と公益性の高い臨床研究の両立が可能になると思われる。

F. 研究発表

1. 論文発表

1. 秋山昌範. 病院管理を行うための ERP (Enterprise Resource Planning) システム. 医療情報学 23,3-13.2003.
2. 秋山昌範, 斎藤澄. 遠隔病理診断におけるデジタルマイクロスコープの有用性. 遠隔医療研究会論文集 7,78-79.2003.
3. 秋山昌範. 電子タグのネットワーク利活用に関する検討. 医療情報学 23(Suppl.), 103-106.2003.
4. 秋山昌範. 薬事法改正に対応した医療材料・医薬品のトラッキング. 医療情報学 23(Suppl.),317-319,2003.

2. 学会発表

第23回 医療情報学連合大会
HOSPITALOG ASIA 2003. (Bangkok, Thailand)
Inaugural Symposium of the Seoul National University Bundang Hospital. (Seoul, Korea)
など、国際学会等2件、国内学会23件

G. 知的所有権の取得状況

1. 特許取得

特願 2003-118496 疾病予後モデルの作成方法、このモデルを用いた疾患予後予測方法、このモデルによる予後予測装置、ならびにプログラム、記憶媒体.

2. 実用新案登録

なし

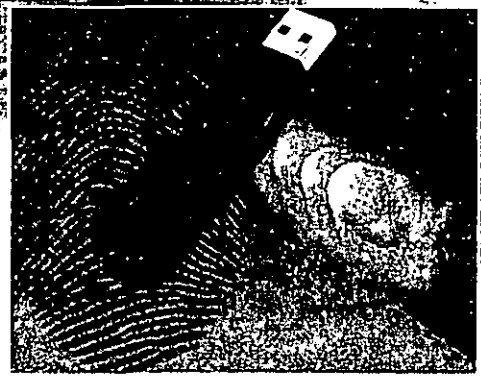
3. その他

なし

Confidence
Clever
Chaos
Crypto System

Focus Systems
Bring Computer Solutions Into Focus

C4 Fingered



C4 Fingeredは、指紋認証とC4暗号を組合わせたセキュリティツールです。
USB指紋認証製品で、持ち運びも簡単。PC利用者の本人認証およびデータの暗号化により、第三者によるPCの不正利用や盗難等による情報漏洩を防ぎ、大切な情報を守ります。

Concept

●指紋認証

パスワードやICカードによる認証は、忘却や盗難・紛失による第三者のPC不正利用の危険性があります。そこで、世界中でただ一人本人のみが持つ生体情報を利用した本人認証（バイオメトリクス認証）が重要とされてきており、中でも指紋認証は、低コストで比較的容易に導入・運用ができ、認証精度も向上していることから、最も広く普及している認証方法です。
パスワード入力等を意識することなく、自身の指を使い簡単かつ確実に本人認証を行うことができます。

●ファイル暗号化

指紋による本人認証に加え、PC内のデータを暗号化しておくことで、安全性をさらに高めることができます。USB暗号キー（デバイス内に格納してあるキー）を使用しての暗号化・復号化が可能ですので、暗号キーを覚える必要がなく、簡単な操作で処理が行えます。
また、データ削除の際に「シュレッダー削除」機能をお使いいただくことで、データを二度と復元できないように削除でき、PC廃棄後の情報漏洩対策としてもご利用いただけます。

Technology

●ラインセンサー指紋認証

指紋の読み取りにラインセンサーを用いることで、デバイスの小型化（USBへの搭載）を実現しました。また、デバイス（C4-Fingered専用USBキー）内のユーザ情報や指紋情報は、C4S暗号で暗号化処理し、格納しています。
さらに、デバイス内には暗号化キーも格納されており、暗号キーの入力なしに暗号化・復号化処理を行うことができます。

●C4S搭載

指紋データおよびファイルの暗号化には、高速・安全を誇る純国産暗号化技術 "C4S" を採用しています。
C4Sは、マルチプラットフォームを基本とし、強固にデータを守りながらも、高速な処理でストレスなく暗号化処理を行います。

C4Fingered

C4-Fingeredの機能

■指紋認証によるログオン

本人のみが持つ指紋で認証を行い、PCへのログオンを行います。パスワードを忘れることや、ICカード等の紛失・盗難の心配をすることなく、確実な本人認証で高いセキュリティを確保します。

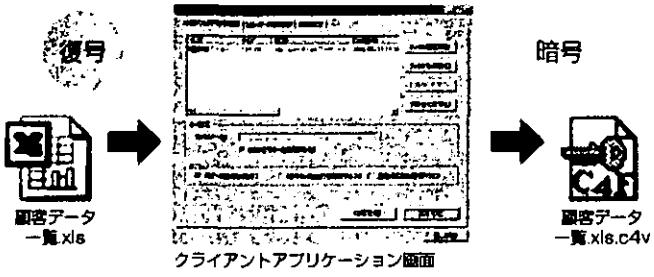
■指紋認証による スクリーンロック・スクリーンセーバーロック解除

スクリーンロックまたはスクリーンセーバーロック解除を指紋認証で行います。ちょっとした離席の際も、第三者によるPCの不正利用を防ぎます。

■ファイルプロテクト

フォルダやファイルの暗号化…簡単操作でデータを暗号化・復号化処理でき、重要な情報を守ります。

暗号書庫…データを圧縮して暗号化し、異なるドライブのフォルダやファイルも同一書庫へ格納し管理できます。

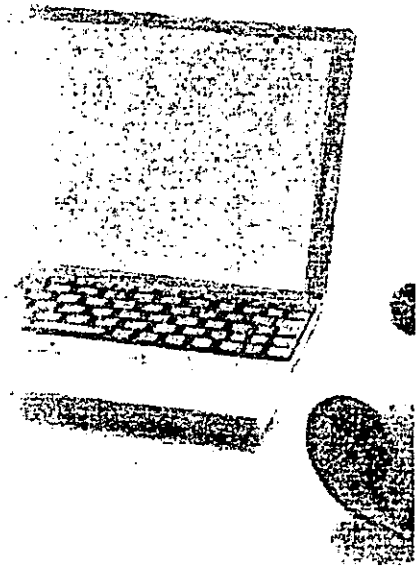


■シュレッダー削除

復元ソフトを使用しても、データを二度と復元することができないように削除します。

■指紋認証による 管理アプリケーション（C4-Fingered）の起動

C4-Fingeredの発行や設定変更を行う「管理アプリケーション」の起動には、管理者の指紋認証が必要となるため、管理者以外の人物にむやみに設定変更されることがなく、高いセキュリティレベルを維持できます。



対応OS	Microsoft® Windows® 2000 日本語版 Microsoft® Windows® XP 日本語版

標準価格（税別）

商品名	価格
C4-Fingered アプリケーション （管理アプリケーション、クライアントアプリケーション）	¥149,800
C4-Fingered 専用USBキー	オープン価格

※ストラップもあります。（オプション）

http://www.focus-s.com

販売元 Focus Systems
Bring Computer Solutions into Focus
株式会社フォーカスシステムズ
新規事業推進室
〒141-0022 東京都品川区東五反田1-23-1　フォーカス五反田第2ビル
TEL. 03-5420-3659　FAX. 03-5420-3634
E-mail prom@focus-s.com

※C4、C4Sは株式会社シーフォーテクノロジーの登録商標です。
C4-Fingeredプログラムの著作権はオープンテクノロジー株式会社が有します。

Confidence
Clever
Chaos
Crypto System

C4U Ver.2

わずらわしいID・パスワードの入力はもういらない
この1本でログオンから暗号まで!!

■こんな問題を解決します

- ●社内セキュリティ対策として何かはじめたい。
- ●難しい操作はできない。でもパソコンのデータは守りたい。
- ●Windowsのログオン、毎回毎回入力するのは面倒。
- ●外に持ち出すノートパソコン 、置忘れや盗難にあったら情報漏洩?
- ●経理情報、人事情報、査定報告に業務方針、会議等の離席時に
  見られてしまわないか。
- ●本社と支社の月次報告、添付ファイルが盗み見られることはないのか。
- ●ファイルサーバや共有パソコンの研究データや個人情報、
  人に見せるわけにはいかない。

C4Uとは・・・

こういう方のための簡単暗号ツールです!!

■簡単高度なセキュリティ

- ●初回暗号フォルダ設定後、ユーザの操作はC4Uキーの抜きさしのみです。
- ●暗号鍵の長さは自由に設定できます。(2048bitまで)
- ●専用USBキーにはアラジンジャパン社のeTokenを採用。
  コンパクトなボディに耐タンパ性を備えた制御チップを搭載、
  暗号キーを安全に格納するデバイスです。

■独自のC4Uキー再発行システム

- ●紛失等による再発行は、C4Uキーの発行時に設定した複数個のリカバリキーをそろえてはじめて可能となる新しいシステムを
  提供しています。

■最先端の暗号エンジン

C4Uの鍵となる暗号エンジンは最先端暗号化テクノロジー C4Sを採用しています。
C4Sは可変長鍵による強さ、機器に負荷をかけないスピードを持つ優れた純国産の暗号技術です。またそのエンジンの軽さのため汎用機から携帯電話まであらゆる場面に利用できるマルチプラットフォームを実現しました。
「誰でもできるファイルセキュリティ」をコンセプトに開発されたC4Uでは、この強力な暗号エンジンを簡単操作でご利用いただくことができます。

Confidence
Clever
Chaos
Crypto System

C4U Ver.2

いる人だけが使える。
いるだけで使える。

■操作はキーの抜きさしだけ

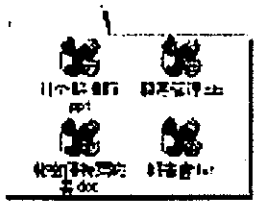
Ⅰ.ログオン・ログオフ機能

PC起動時にC4Uキーを
さすだけでログオンします。

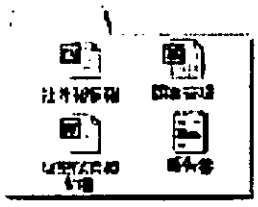
※機能Ⅰにおいて、Windows®98SE、Windows®MEは一部利用制限がございます。

C4Uキーを抜くだけで、
ログオフします。

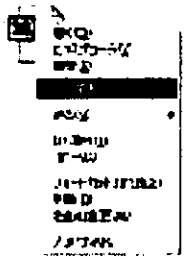
Ⅱ.自動暗号・復号機能



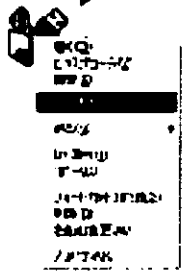
C4Uキーを抜きさしだけで指定されたフォルダ内のファイルが全て暗号・復号されます。



Ⅲ.手動暗号・復号機能



C4Uキーがさしてあれば右クリックで指定したファイルを自由に暗号・復号できます。



Ⅳ.改竄チェック機能

復号時には改竄されていないか確認します。
※暗号化されたファイルはC4Uキーがなければ開くことができません。

※これらの機能は組み合わせてお使いいただくことができます。
※1つのC4Uキーで複数のフォルダを指定することができます。
※1つのPCで複数のC4Uキーを使い分けることができます。

■Price

❶C4Uアプリケーションセット……¥149,800／1セット
（鍵管理1ライセンス、クライアントフリーライセンス）

❷C4U専用USBキー……¥88,600／1セット（10本）

❸旧VersionからVer.2へのUpdate（USBキー はそのままご利用いただけます）…¥25,000／1セット

〔対応OS〕 Windows®98SE / Windows® Me / Windows®2000 / Windows® XP/ Windows® Server 2003（32bit版のみ）

URL:http://www.focus-s.com

開発元

Focus Systems
株式会社 フォーカスシステムズ
〒141-0022 東京都品川区東五反田1-4-1 ハニー五反田第2ビル
TEL:03-5421-1071 FAX:03-5421-1019
E-mail: c4@focus-s.com

※掲載されている会社名、製品名は一般に各社の登録商標または商標です。
文中の内容は予告なく変更する場合がありますので、ご了承ください。

2004-01

目 次

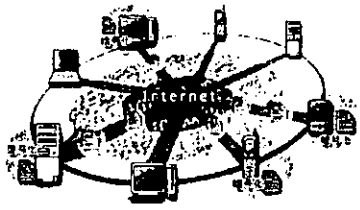
Focus Systems,Corp

1-1 C4シリーズ

Focus Systems,Corp

インターネット普及に伴い、常時接続によるサービスの多様化・利便性の向上が成されてきました。
しかし、非常に便利になった反面、常時外部からの侵入や情報漏洩、改竄等の様々な危険にも
さらされていると言うことができます。
目には見えません(実害が分かりにくい)が常に様々なスキャンやアタックなどが行われており、
それらの危険性から情報やデータを守るための有効且つ強力な対策として「暗号化」が挙げられます。

C4シリーズは、暗号化技術に求めれる要件とされていた
「高速性」・「安全性」・「あらゆる機器への実装」を
すべて満たす暗号化技術として開発されました。
高速性と安全性を兼ね備え、軽量なプログラムによって
情報家電やその他の情報端末にも搭載可能です。



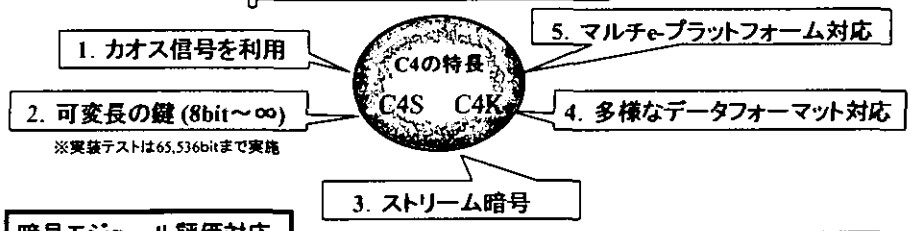
C4シリーズは、これからのIT社会におけるセキュリティ対策に対応した

高速 , 安全 , 軽量 な暗号化システムです。

C4シリーズ

Focus Systems,Corp

C4暗号5つの特徴



暗号モジュール評価対応

独立行政法人情報処理推進機構（IPA）では、国際標準化の流れを視野に入れて、国内における暗号モジュール評価制度の整備が進められています。
暗号アルゴリズムだけでなく、暗号技術の実装レベルでの安全性が問われ、暗号モジュール評価の必要性が高まってきています。

C4製品（C4CS※1）も、米国（NIST）とカナダ（CSE）が行う暗号モジュール評価プログラム（CMVP）において、評価テストを受けている段階にあり、**9月頃には認定される予定**となっております。

※1 C4CS ： C4Custom暗号エンジンに加え、NIST(*1)が規定したAESなど複数のアルゴリズムを含む製品で、様々なセキュリティニーズへの柔軟な対応が可能となります。

1-2 カオス信号を利用

Focus Systems,Corp

カオス信号を利用

カオス＝混沌（物事がはっきりとしない様子）。ギリシア神話のKhaosより。

((定義))

あるシステムにおいて、「ある時点での状態（初期値）が決まればその後の状態が原理的に全て決定される」という決定論的法則に従っているにもかかわらず、非常に複雑で不規則かつ不安定な振る舞いを示す事象。

((特徴))

- 単純な関数形であるが、複雑な信号を発生
- 初期値に敏感に反応
- 一方向性を有する

発生した複雑な振る舞いの例

上記の特徴を活用し、高速で強固な暗号システムを実現しました。また、既存の暗号技術で利用されている理論とは異なるため、これまで確立されている暗号解読法では解読されにくいと言えます。

1-3 可変長の鍵

Focus Systems,Corp

可変長の鍵 (8bit～∞)

データを暗号化するときに使用する鍵は、可変長に対応しており、理論的には8bit～∞の使用が可能です。

実際には、65,536bitもの鍵の使用が実用に耐え得ると確認されています。この長さは、今後十数年内で解読されるだろうと言われている鍵長をはるかに上回っています。

なぜ鍵が長いと良いの？

鍵長が長いと、考えられる鍵の種類が多くなります（鍵の生成空間が広い）。そのため、実際にどの鍵を使用しているのか予測しにくいので、安全性が高くなると言えます。（鍵を総当りで探索することは、現実的ではなくなります）

1-4 ストリーム暗号

Focus Systems,Corp

ストリーム暗号

暗号には、ストリーム暗号とブロック暗号があります。

C4シリーズはストリーム暗号方式です。

ストリーム暗号

データを1ビットもしくは1文字単位で暗号化する方式。

C4シリーズ以外に「RC4」、「MULTI-S01」などがあります。

ブロック暗号

データをある一定の長さ（ブロック長）に分割し、そのブロック長ごとに暗号化する方式。

「DES」、「MISTY」、「Rijndael」などがあります。

なぜ、ストリーム暗号方式なの？

一般的に、処理が軽くなるので高速暗号化に適しているためです。

1-5 マルチに対応

Focus Systems,Corp

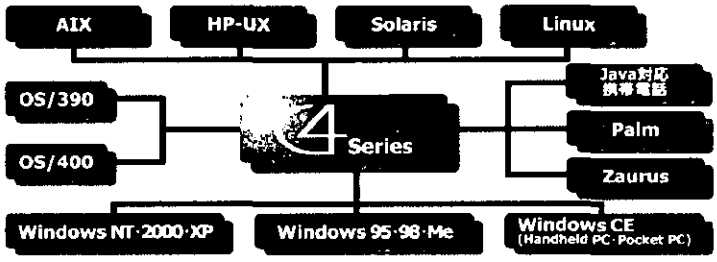
1. マルチメディアデータ対応

text、graphic はもちろん、sound 、video 、voice 、movie など、あらゆるデータに対応しています。

暗号化処理が高速なので、データ量が多くてもストレスがありません。

2. マルチe-プラットフォーム対応

メインフレームからワークステーション、PCはもちろん、携帯電話や携帯端末、情報家電にも搭載可能です。



2-1 C4シリーズの種類

Focus Systems,Corp

C4S

速度と強度を兼ね備えた、共通鍵暗号方式の暗号。大量のデータでも、高速に暗号化できます。

C4K

データの暗号化にはC4Sを用い、公開鍵の鍵交換方式には定評のあるDHを利用しています。

C4S 共通鍵暗号方式暗号エンジン
C4S (Confidence Clever Chaos Crypto System)

C4k 公開鍵暗号方式暗号エンジン
C4k (Confidence Clever Chaos Crypto key)

2-2 暗号化の方式

Focus Systems,Corp

共通鍵暗号方式と公開鍵暗号方式は、次のような違いがあります。

	共通鍵暗号方式	公開鍵暗号方式
鍵の関係	暗号鍵 ＝ 復号鍵	暗号鍵 ≠ 復号鍵
代表例	C4S DES IDEA FEAL MULTI MISTY	C4K RSA RABIN DSA ElGamal
鍵の受け渡し	考慮必要	考慮不要
処理速度	速い	遅い
認証	困難	容易
利用方法	比較的大きなデータ(通信文本体など)の暗号化	小さなデータ(共通鍵暗号方式で使用した鍵など)の暗号化

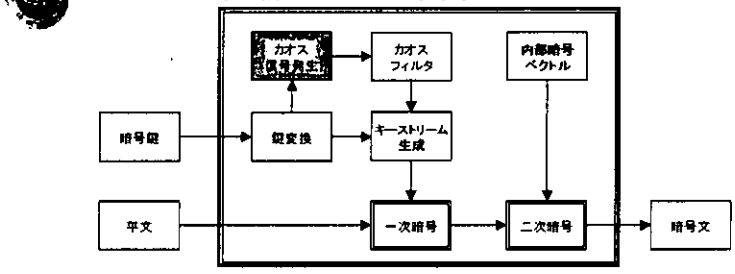
資料提供：JISA　1996年度情報通信委員会

＊この他に、共通鍵暗号と公開鍵暗号を用いてシステム化するハイブリット型も存在します

2-3 C4S

Focus Systems,Corp

C4Sは次のような構造になっています。



(1) 入力された鍵は2経路に分かれ処理されます。

(2) 入力された鍵を変換し、変換された鍵からカオス信号を発生させます。

(3) 変換された鍵とカオス信号を合成し、キーストリームセットを生成します。

(4) キーストリームセットと平文、暗号ベクトルを合成することで、暗号化処理を行います。

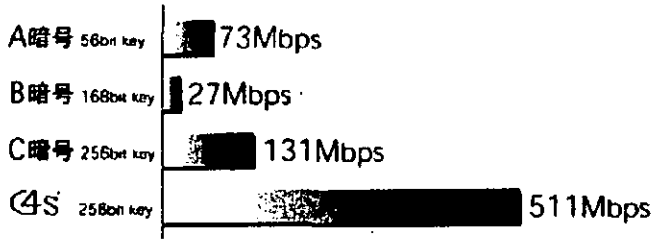
(5) 暗号ベクトルは、内部データを参照、合成することで、毎回新規に動的な変化(置換)を行っています。

✧ 鍵要素、カオス信号、内部暗号ベクトルの有効的な合成により、より強固な仕組みとなっています。

2-4 C4Sの速度 - (1)

Focus Systems,Corp

暗号化処理スピードグラフ



Pentium'Ⅲ 733MHz Windows2000 Professional 当社調べ
(測定環境により、測定結果が異なる場合がございます)

＜快適さを誇るスピード＞

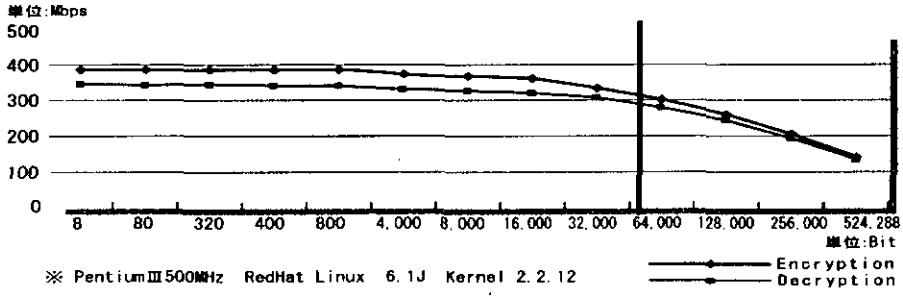
Pentium Ⅲ 733MHz Key 256bitの環境下で、511Mbpsの処理速度を実現。

次世代標準暗号として利用が広まっている「AES」の約4倍の処理スピードを誇ります。

C4Sの速度 - (2)

Focus Systems,Corp

■各鍵長における実処理速度



※ PentiumⅢ500MHz RedHat Linux 6.1J Kernel 2.2.12

＜セキュリティバランス＞

安全性を高める長い鍵、ストレスを感じることのない高速な処理。

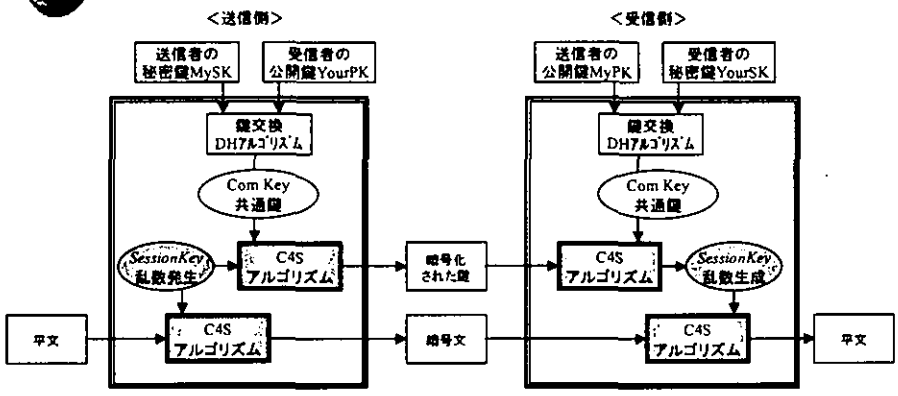
その両方を実現させ、強度・速度ともに優れたブロードバンド時代に

最適な暗号化を可能にしました。

2-5 C4K

Focus Systems,Corp

C4Kは次のような構造になっています。



- 平文と鍵の暗号化 ： C4S
- 共通鍵の交換 ： DH(Diffie-Hellman)

✧ 高速暗号のC4Sと鍵交換方式で定評のあるDHを組合わせた公開鍵暗号方式です。

3-1 C4S、C4Kを使用した製品群(1)

Focus Systems,Corp

＜暗号化エンジン＞

C4ライブラリ(C4S, C4K)

独自のアルゴリズム、設計方法で開発した暗号ライブラリ。

C4Custom C4Custom

C4Sをベースにし、プラットフォームに合わせてパフォーマンスを最適化した暗号ライブラリ。

＜暗号化通信には＞

C4VPN C4VPN

LAN、WAN及びインターネット網で、データの暗号化通信を行うためのソフトウェア。

C4S、C4Kを使用した製品群(2)

Focus Systems,Corp

＜PC内のファイルの暗号化には＞

C⁴ FILE PROTECTOR

PC内に保存してあるデータを本格的に暗号化保管する電子金庫のようなアプリケーション。

C4U

USBキーの抜き差しという簡易操作で、指定フォルダ内のファイルを暗号化するアプリケーション。

＜指紋認証によるログインとファイルの暗号化には＞

C4-Fingered

小型USBキーによる指紋認証でPCへ簡単ログオン。PC内のファイルやフォルダも暗号化できる、認証+暗号化のアプリケーション。

＜メールの暗号化には＞

C4i

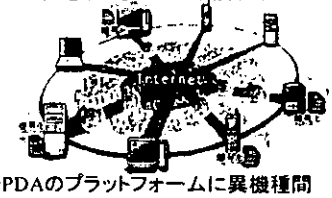
iアプリを使用した、携帯電話対応の暗号メールソリューション。

3-2 C4ライブラリ ～暗号化機能コンポーネント～

Focus Systems,Corp

C4ライブラリ(C4S,C4K)

暗号化は企業のあらゆる情報システムの中に不可欠になっています。C4ライブラリは、C言語やJava言語など、現在スタンダードな開発環境でのセキュリティ実装を容易にした、信頼性の高い暗号コンポーネント集です。



C4ライブラリの優れた特徴

●多様化したシステムプラットフォームへの対応

Windows系はもちろん、Unix系、オフコン系、更に携帯電話やPDAのプラットフォームに異機種間の暗号化／復号機能を提供し、今後多様化するシステムに安心して柔軟に対応することができます。

●高い安定性とパフォーマンス

ライブラリとして提供される本製品は、暗号演算の高速ルーチン化、軽量サイズ化などのチューニングを初め、何億回もの処理テストをクリアした非常に安定性の高いライブラリ 集です。