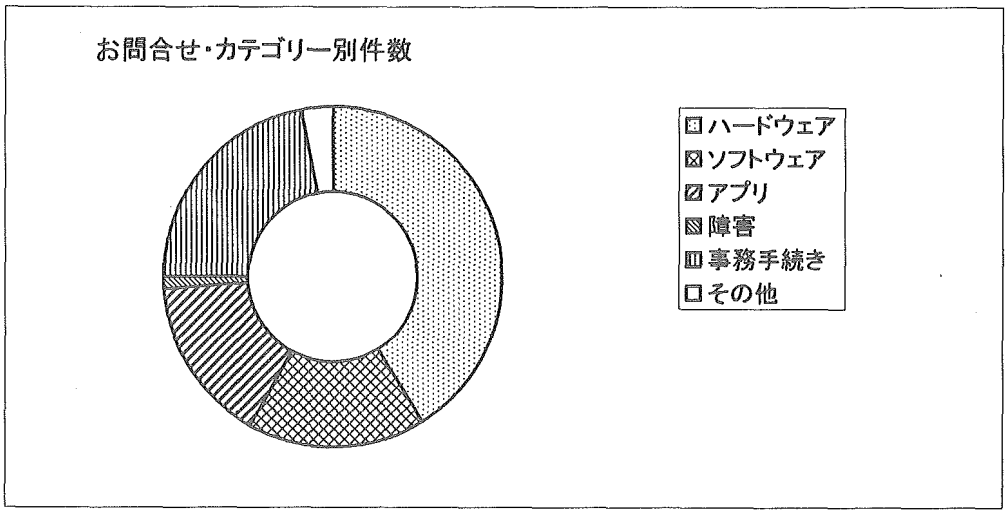
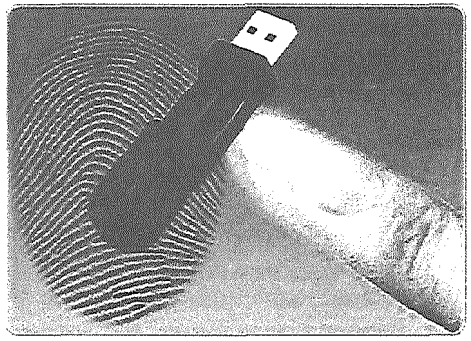
問合わせカテゴリ



Focus Systems
Bring Computer Solutions into Focus

C4Fingered

C4-Fingered

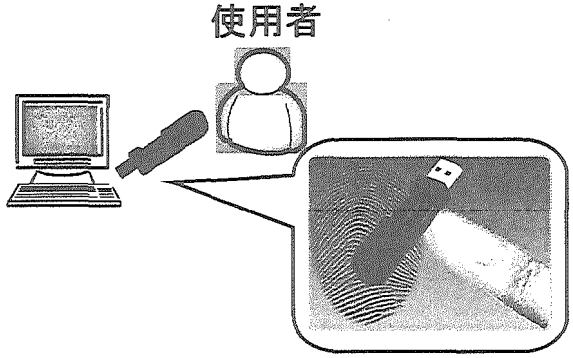


株式会社フォーカスシステムズ
新規事業推進室

C4-Fingeredとは?

A-net 接続用のコンピュータ利用者を限定し、よりセキュリティを高めるためには、
ログインの際に生体(指紋)認証を用いることが有用です。

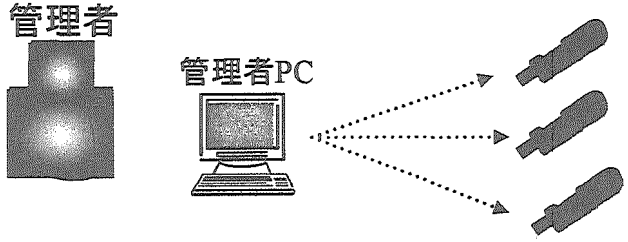
(1) C4-Fingered は、専用の指紋認証USBデバイスを用いてコンピュータへのログインを可能とする製品です。



C4-Fingered 専用の指紋認証USBデバイスは、小型で軽量ですので、ドアの鍵のようにユーザごとに所持して使用することができます。

(2) 指紋認証USBデバイスには、使用者の指紋データやユーザ情報を登録します。

(3) ユーザおよび指紋認証USBデバイスの管理は、管理者が専用の管理アプリケーションにて行います。

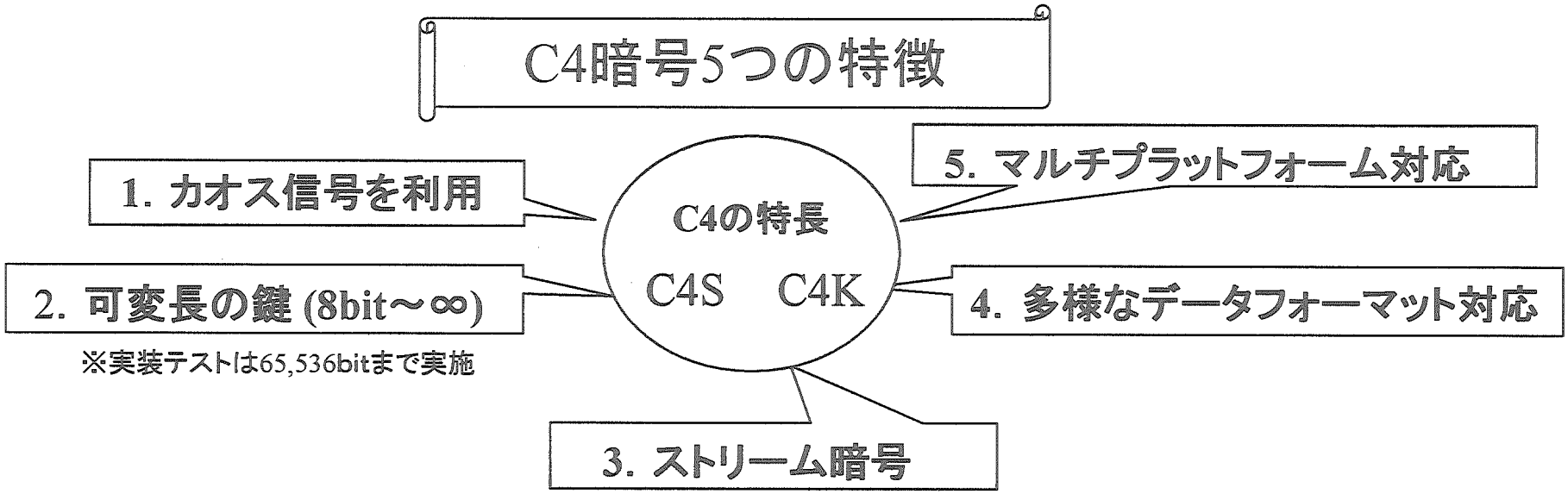


C4-Fingeredの安全性

C4-Fingered専用の指紋認証USBデバイス内に格納されるデータ(指紋データ、ユーザ情報、デバイス情報など)は、C4暗号にて暗号化された状態で保存されているので、万が一デバイスの紛失・盗難が発生した場合にも指紋データやユーザ情報は漏洩する心配はありません。

【C4暗号とは】

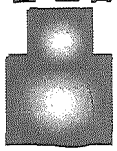
暗号化技術に求めれる要件とされていた「高速性」・「安全性」・「あらゆる機器への実装」をすべて満たす暗号化技術として開発されました。



C4-Fingered の概要

【使用するアプリケーション】

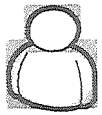
管理者



➧C4-Fingered 管理アプリケーション

(1) C4-Fingered の使用者情報および指紋認証USBデバイスを管理します。
(2) 使用者からの指紋認証USBデバイスの使用許可申請ファイルを確認します。
(3) 使用を許可する場合には、認証ファイルを作成します。

使用者



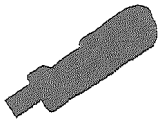
➧C4-Fingered 登録アプリケーション

(1) 指紋認証USBデバイス内に指紋データ等を入力します。
(2) 指紋認証USBデバイス使用申請ファイルを作成します。
(3) 管理者からの認証ファイルを確認し、指紋認証USBデバイスを使用可能とします。

➧C4-Fingered クライアントアプリケーション

指紋認証USBデバイスを用いてコンピュータへのログインを行います。

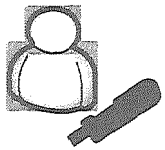
➧C4-Fingered 専用　指紋認証USBデバイス（＝C4-Fingeredデバイス）

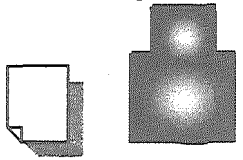


C4-Fingered の初期設定フロー

使用者

管理者



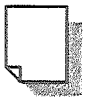


①登録に必要な暗号鍵ファイルを生成

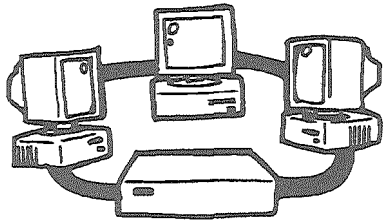
②暗号鍵ファイルを管理者へ送付

③暗号鍵ファイルを設定し、
指紋データ等をC4-Fingered
デバイスに入力

④申請ファイルを出力



⑤申請ファイルを管理者へ送付



⑥受信した申請ファイルを確認

⑦使用を許可する場合には
承認ファイルを出力

⑨受信した承認ファイルを
C4-Fingeredデバイスへ転送

⑧承認ファイルを使用者へ送付

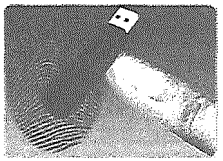
管理者は、ネットワークを利用することにより、遠隔地の使用者の
C4-Fingered デバイスも管理することができます。

C4-Fingeredの操作手順

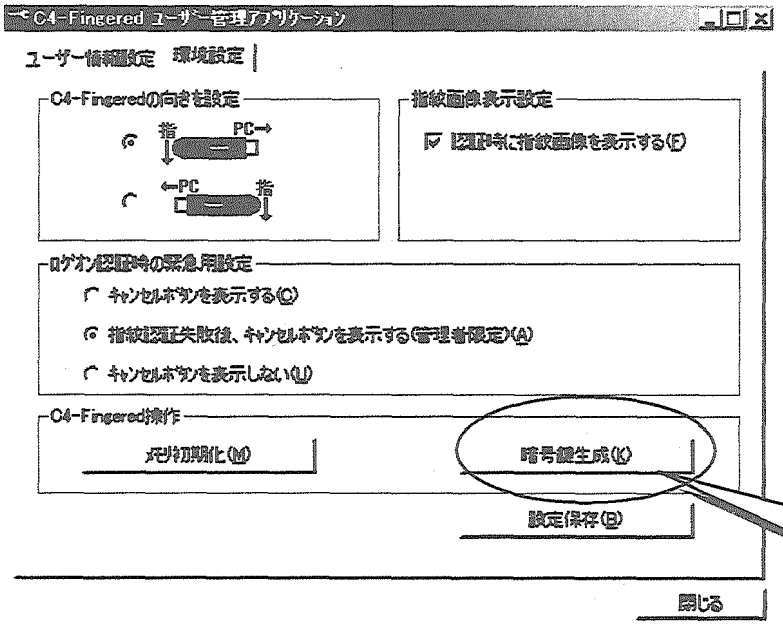
(1)管理者: 暗号鍵ファイルの生成

①指紋認証により、
管理アプリケーションを起動する

管理者



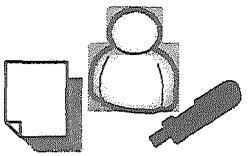
②登録に必要な暗号鍵ファイルを生成する



※C4-Figered管理アプリケーション「環境設定」画面

③暗号鍵ファイルを出力し、
使用者へ送付する

使用者

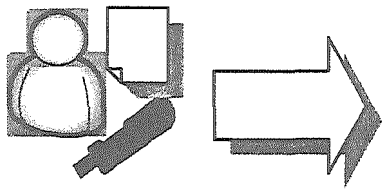


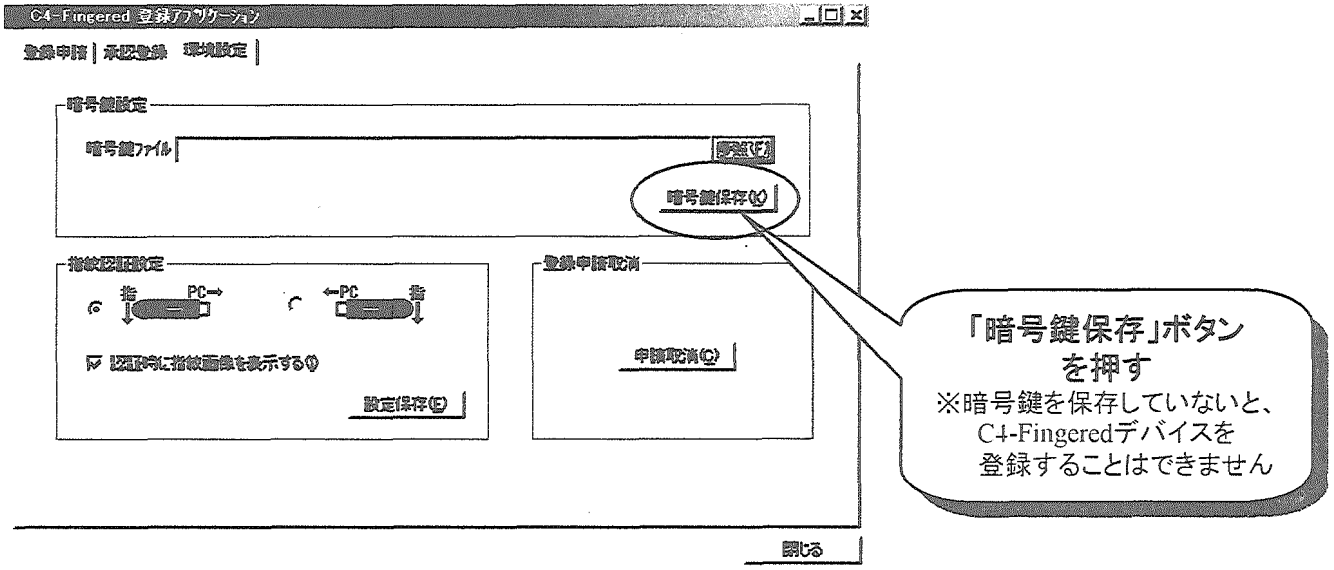
(2)使用者：暗号鍵ファイル保存

①新規発行するC4-Fingeredデバイス
を用意し登録アプリケーションを起動する

②管理者から受信した暗号鍵ファイルを保存する

使用者

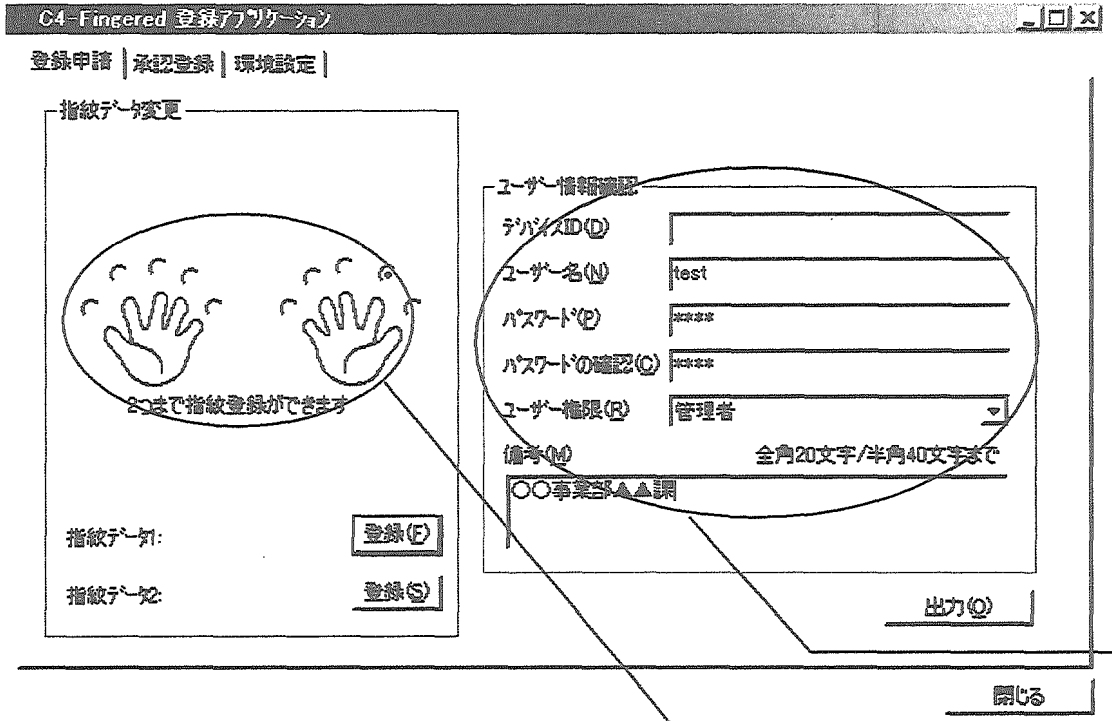




※C4-Figered登録アプリケーション「環境設定」画面

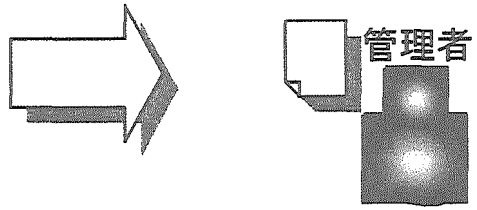
(3)使用者： ユーザ情報の登録と申請ファイルの作成

①指紋情報・ユーザ情報を入力し、申請ファイルを出力する



※C4-Figered登録アプリケーション「登録申請」画面

②出力した申請ファイルを
管理者へ送付する

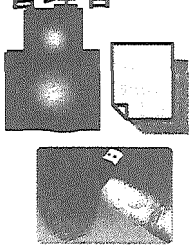


ユーザ情報:
Windowsログオンに必要なユーザ名と
パスワード、ユーザの権限(管理・一般)を
入力

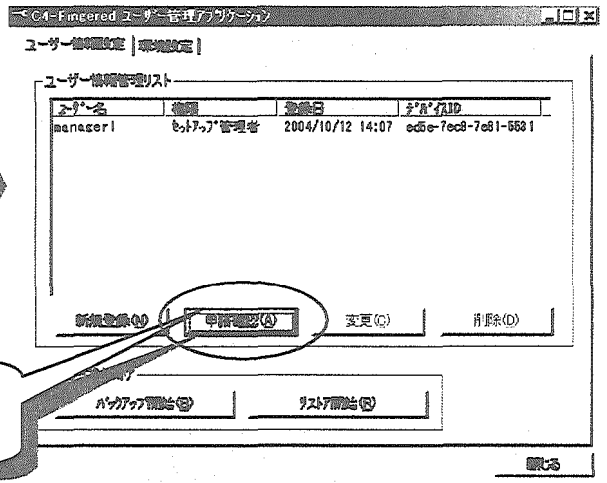
指紋情報:
どの指を登録するかを選択し、C4-Fingered
デバイス内に指紋データを保存

(4)管理者： 申請ファイルの承認

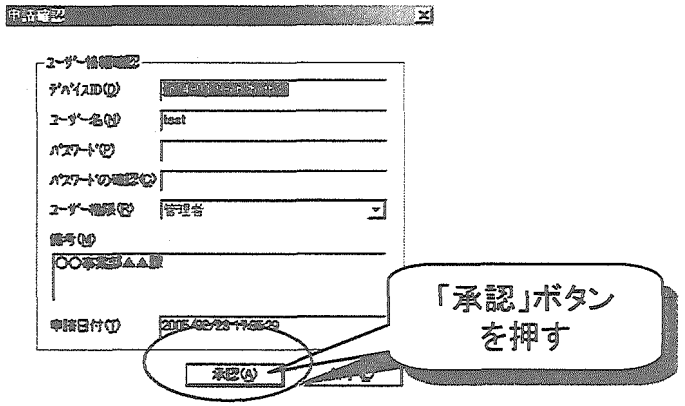
管理者



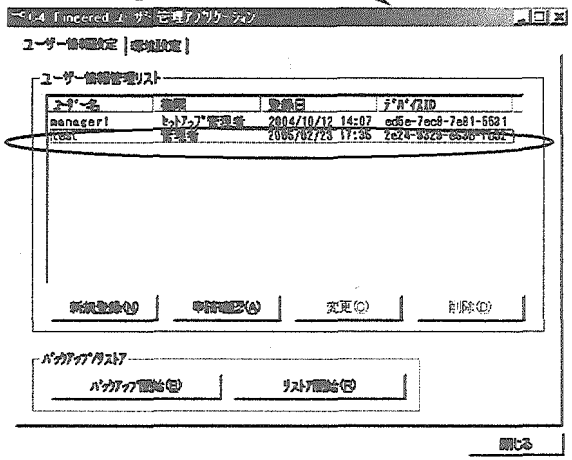
①使用者から送付された申請情報を確認する



②申請者の情報を確認し、OKであれば、
承認ファイルを作成する



※C4-Figered管理アプリケーション「ユーザー情報設定」画面



③承認ファイルを作成するとともに、
管理アプリケーションへユーザ情報が
追加される

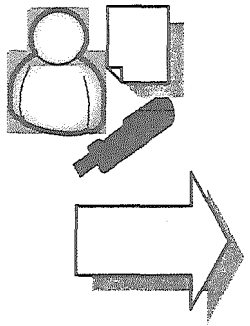
④承認ファイルを申請者へ送付する

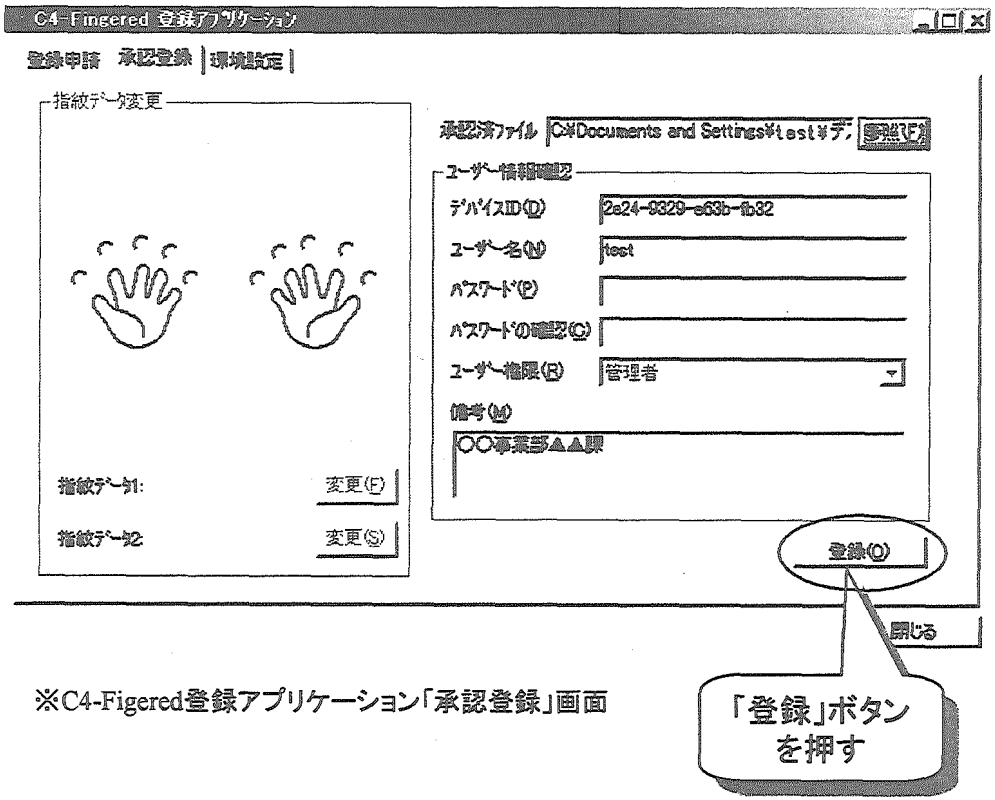
使用者

(5)使用者：承認ファイルの登録

①承認ファイルを選択し、「登録」ボタンを押す

使用者

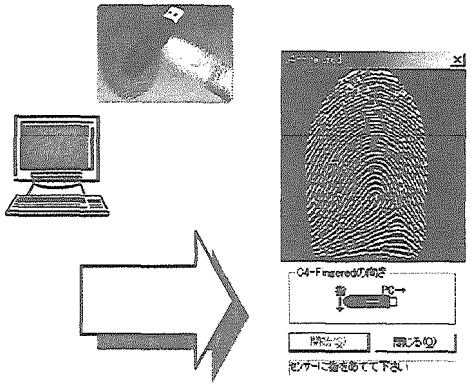




※C4-Figered登録アプリケーション「承認登録」画面

「登録」ボタンを押す

②指紋認証を行い、本人確認後、C4-Fingeredデバイスの登録が完了となる



③クライアントアプリケーションインストール後、C4-Fingeredが使用できる

Focus Systems
Bring Computer Solutions into Focus

デジタル・フォレンジック

株式会社フォーカスシステムズ
新規事業推進室

A-net とデジタル・フォレンジック

A-net において、コンピュータネットワークを通じて送受する情報は、要保護性が高く、第三者への情報の流出を防ぐためあらゆる対策が講じられております。一方でデジタルデータは、その特性から、複製や窃盗などの行為が比較的容易であり、さらにその行為が行われたことが判明しにくいという問題があります。従って、デジタルデータに対してどのような行為が行われたのかを明確にする手法も保持することが重要となってきます。

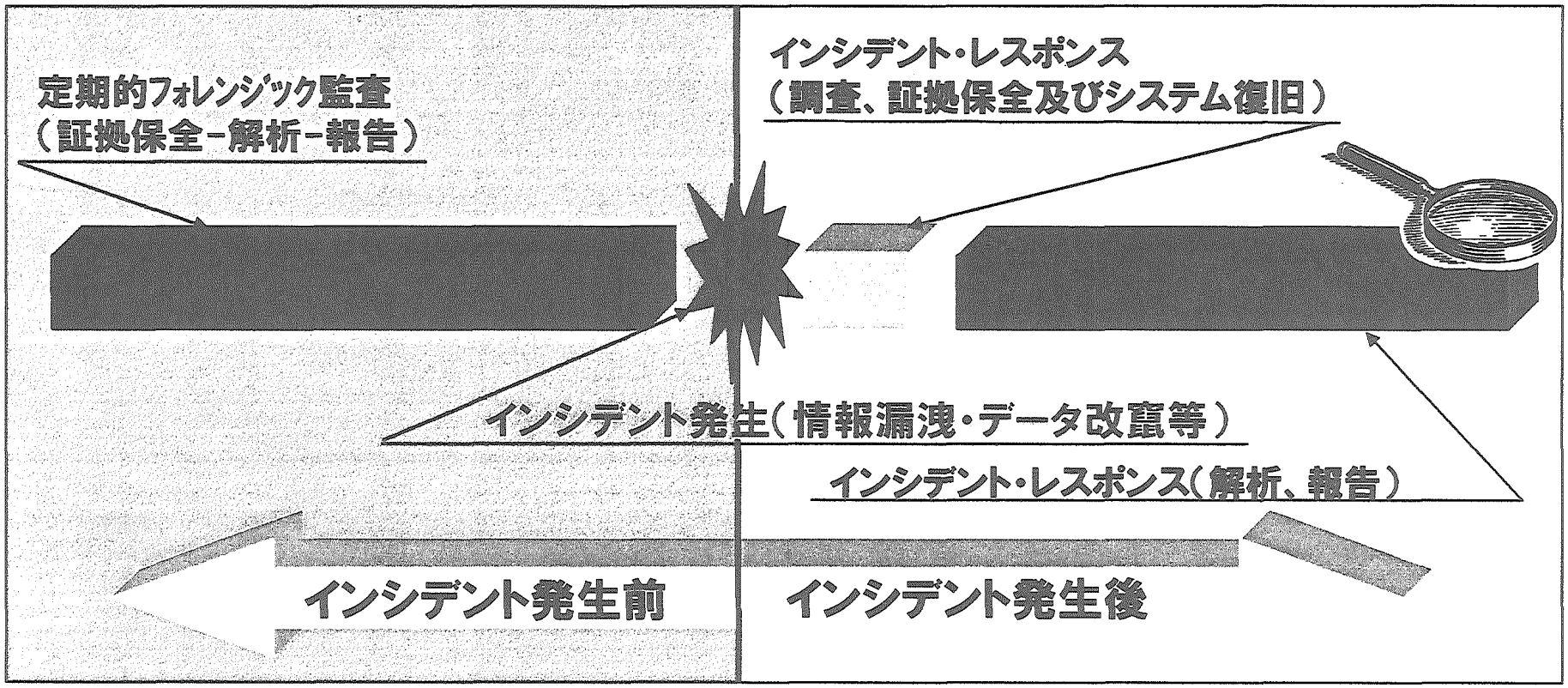
具体的には、例えば A-net 利用施設において情報漏洩の疑いが発生した場合、使用しているコンピュータなどを調査、分析して情報漏洩の発生源を明確にし、しかも、その事実について証拠性を確保しながら説明する必要が生じてきます。

こうした、デジタルデータに対して、証拠保全、改ざん・毀損等についての調査・分析、情報収集等を行う一連の科学的調査手法、即ち「デジタル・フォレンジック」は、A-net をはじめ医療機関においても考慮に入れるべき重要な手法・概念・技術であり、これにより患者の利益と医療機関業務の正当性または過誤の事実証明を実現することができます。

デジタル・フォレンジックとは?

「デジタル・フォレンジック」とは、インシデント・レスポンス(コンピューターやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらに至るための行為(事象)等への対応等をいう。)や法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術をいう。

(デジタル・フォレンジック研究会による定義)



デジタル・フォレンジックの種類

ネットワーク・フォレンジック

“ログ情報”（コンピュータへのログイン、アプリケーションの利用、インターネット／e-mailの利用履歴、サーバ／ファイルへのアクセス履歴など）を収集し一元管理するツール。ログ情報を管理することで、万一インシデントが発生した際の迅速な対応が可能となります。

コンピュータ・フォレンジック

コンピュータ内のデータを調査・解析し、そのコンピュータでいつ、誰が、何を行ったかなどを特定するためのツール。一連の作業で得られた結果は、デジタル的証拠性を完全に維持しているため、法廷闘争にも耐えることができます。

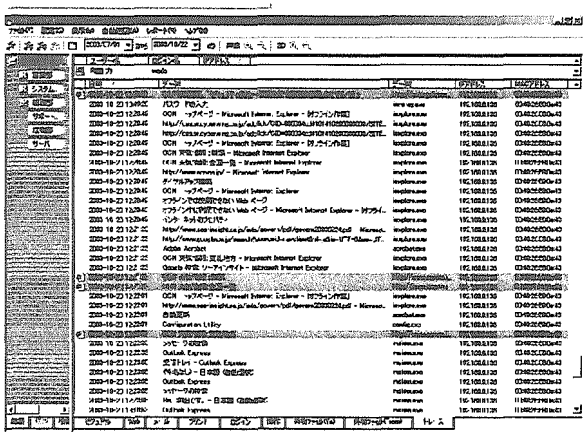
「ネットワーク・フォレンジック」で日々のログ情報などを収集・管理し、万が一インシデントが発生した場合に、「コンピュータ・フォレンジック」を用いて調査・解析を行うことで、インシデントの原因特定や正当性の証明など、迅速に対応することが可能となります。

ネットワーク・フォレンジック

SEERINSIGHT

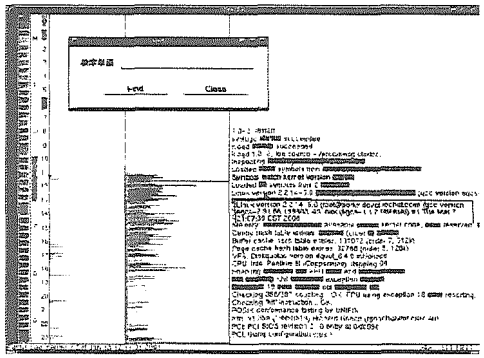
● ツール

SEER INNER ™



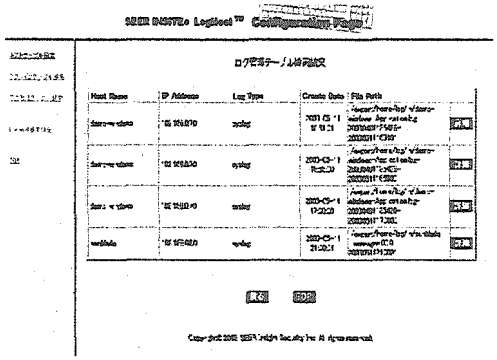
コンピュータの操作ログを“収集-異常検知-監査”するシステム

SEER Tracker ™



情報システムネットワークの多様なログ情報を解析する管理者用ツール

SEERINSITE Log Host ®



情報システムネットワークの“ログ情報”をセキュアに収集し一元管理“するソフトウェア

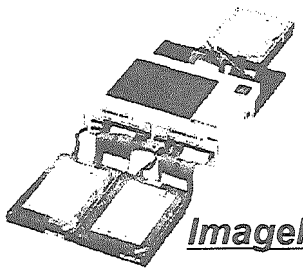
コンピュータ・フォレンジック

UBIC
Intelligence for security

● ツール

証拠保全(コピー)

証拠保全のため、対象のハードディスクをコピーして調査用のハードディスクを作成する



ImageMASSter Solo3

調査・解析

Forensic Toolkit®
Find Computer Evidence Quickly and Easily

調査・分析ツール

Password Recovery Toolkit™
Recover Passwords Quickly & Easily

パスワード解析

Find Registry Data Quickly & Easily

レジストリ保護領域の解析

● 調査サービス

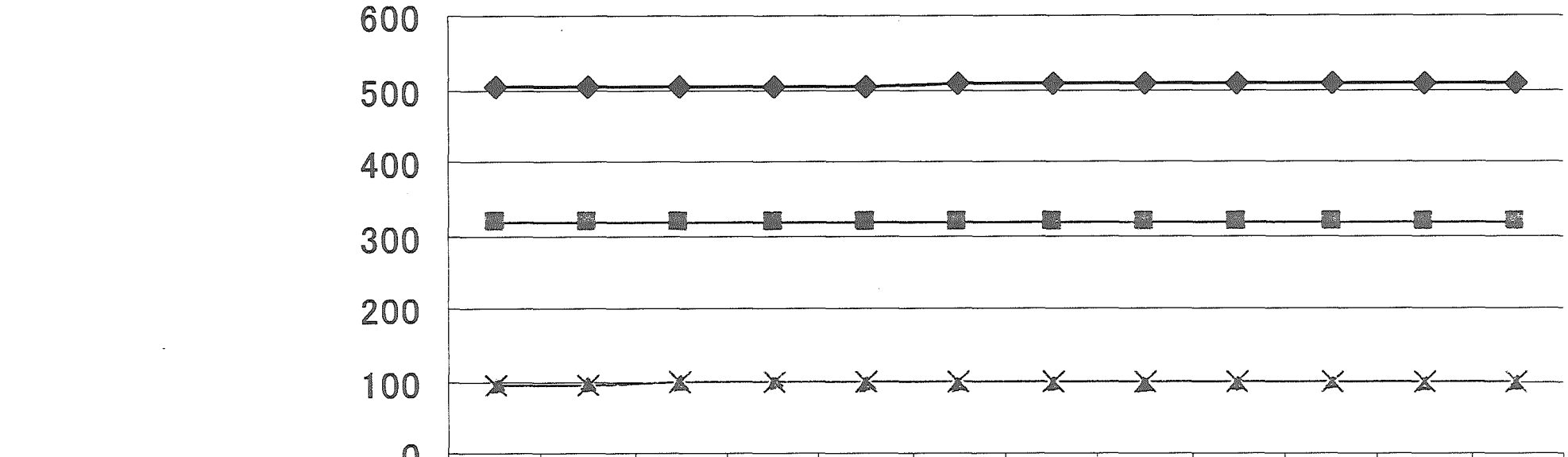
インシデント発生時、専門のフォレンジック調査士により、素早く、データの証拠保全、解析を行い、報告書を提出します。コンピュータ・フォレンジックツールを保有していなくても、万が一の場合に迅速に対応できます。

HIV診療支援ネットワークを活用した診療連携の利活用に関する研究

平成17年度　エイズ対策研究事業　研究

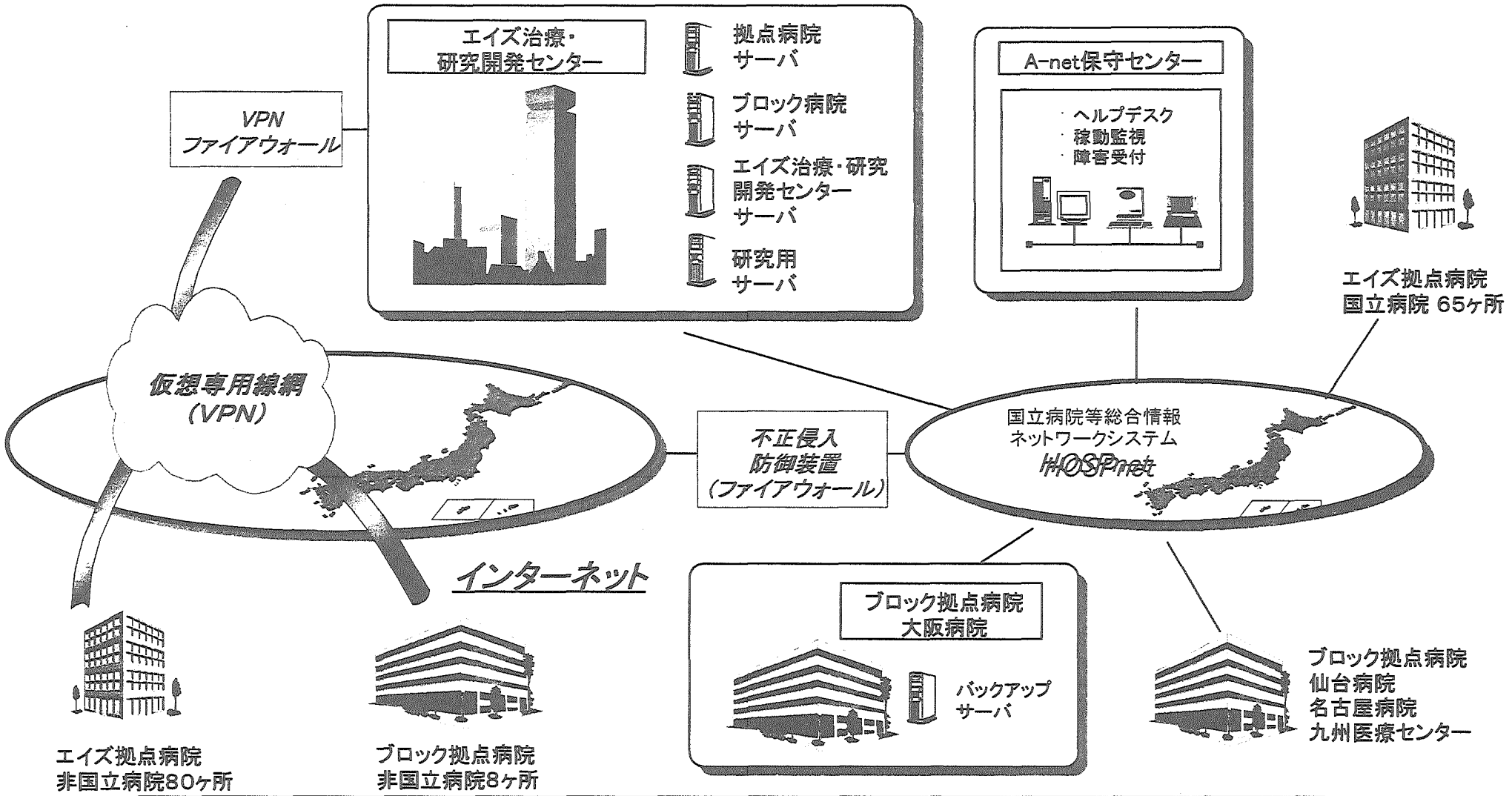
主任研究者:
秋山昌範(国立国際医療センター内科・医療情報システム開発研究部)
分担研究者:
山本隆一(東京大学情報学環)
高橋紘士(立教大学コミュニティ福祉学部)
横内清光(文教大学情報学部広報学科)
木内貴弘(東京大学医学部附属病院中央医療情報部)
研究協力者
菊池　嘉(国立国際医療センター/エイズ治療・研究開発センター)

患者登録数



	1	2	3	4	5	6	7	8	9	10	11	12
国立国際医療センター	314	314	314	314	314	315	315	315	315	315	316	316
ブロック拠点病院	92	92	93	93	93	93	93	93	93	93	93	93
全国拠点病院	95	95	96	96	97	97	97	97	97	98	98	98
合計	501	501	503	503	504	505	505	505	505	506	507	507

□HIV診療支援ネットワークシステム概要図（平成16年1月末現在）



概要説明

A－netは厚生労働省が運営管理し、HIV診療支援ネットワークシステム部会において患者さんの声を反映させてまいります。
A－netの通信環境は国立病院の場合、専用の国立病院等総合情報ネットワーク（HOSPnet）を利用します。
国立病院以外へ拡張する場合は専用の安全保護（セキュリティ）の仕組を前提として利用します。
A－netの診療データはエイズ治療・研究開発センター内に設置された3つのサーバに記録されます。
このデータは国立大阪病院に設置されたサーバにおいてバックアップされます。
A－netの運用を支援するためにA－netの運用センターが設置されます。