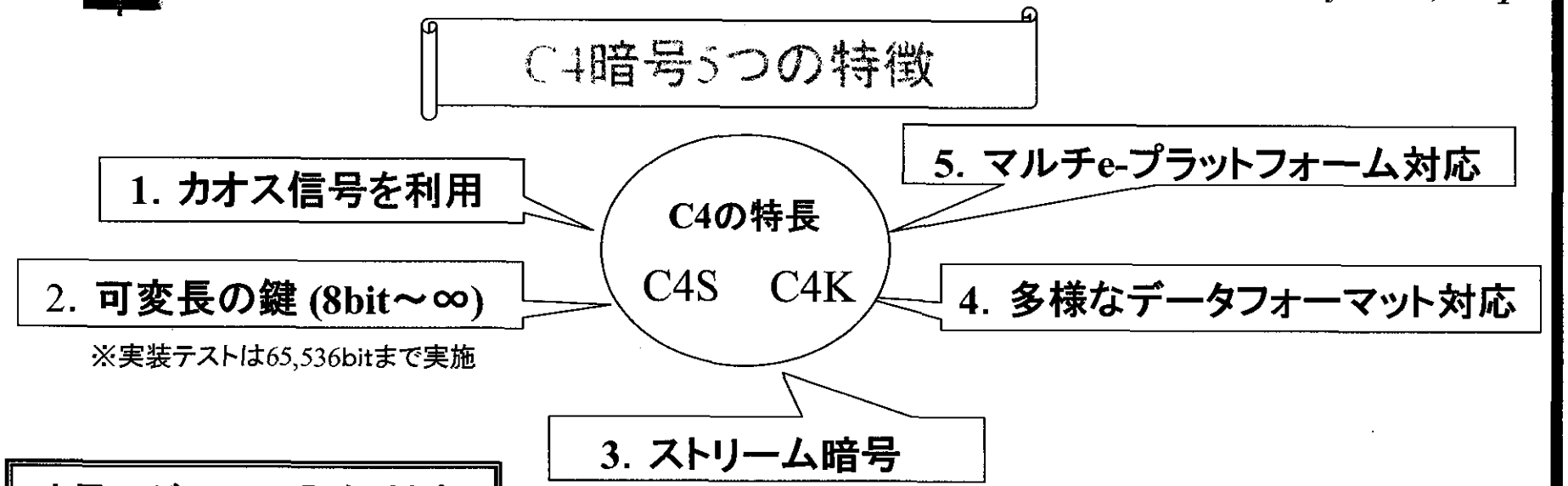
C4シリーズ

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

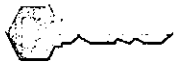
発生した複雑な振る舞いの例

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

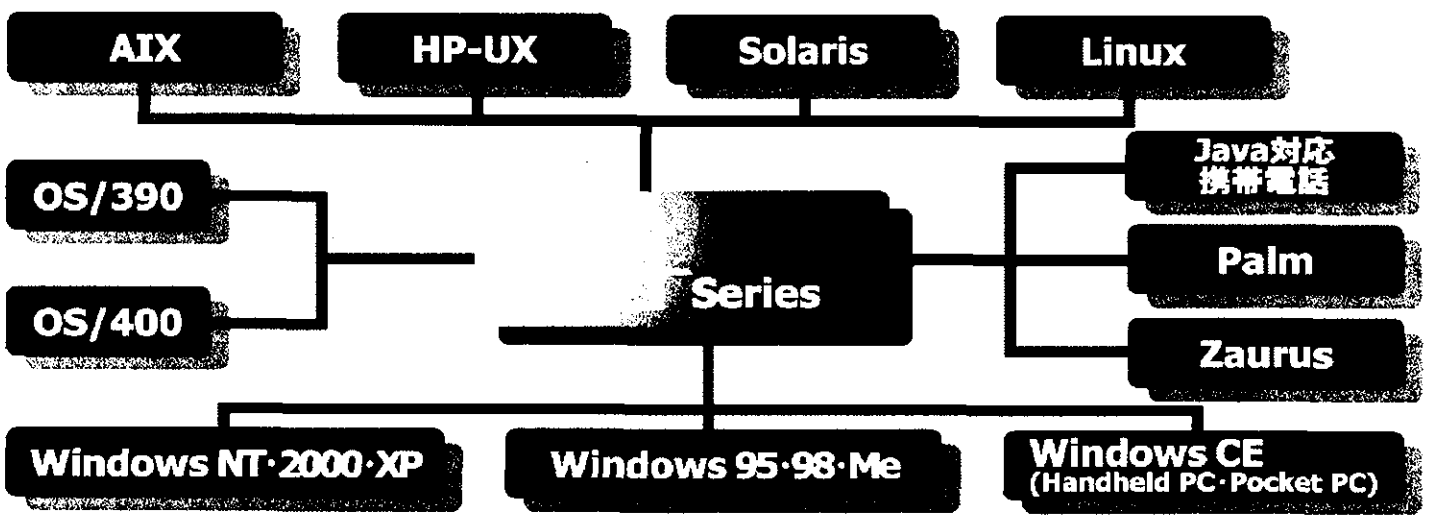
1. マルチメディアデータ対応

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

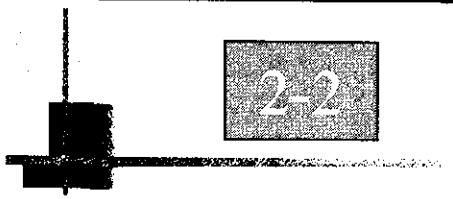
共通鍵暗号方式暗号エンジン

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

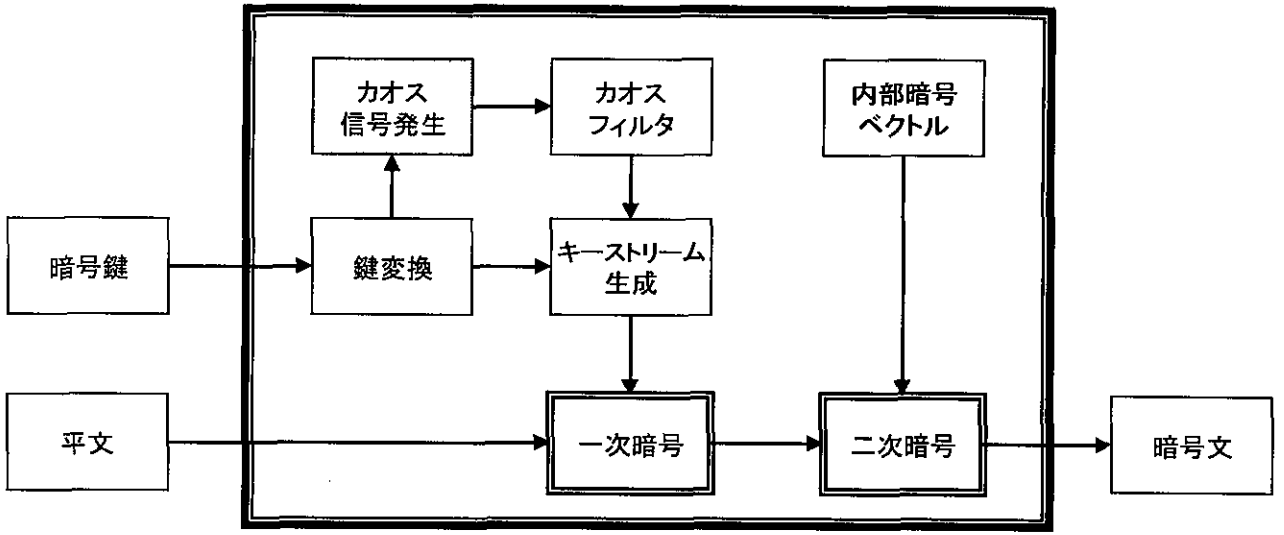
資料提供：JISA　1996年度情報通信委員会

＊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。

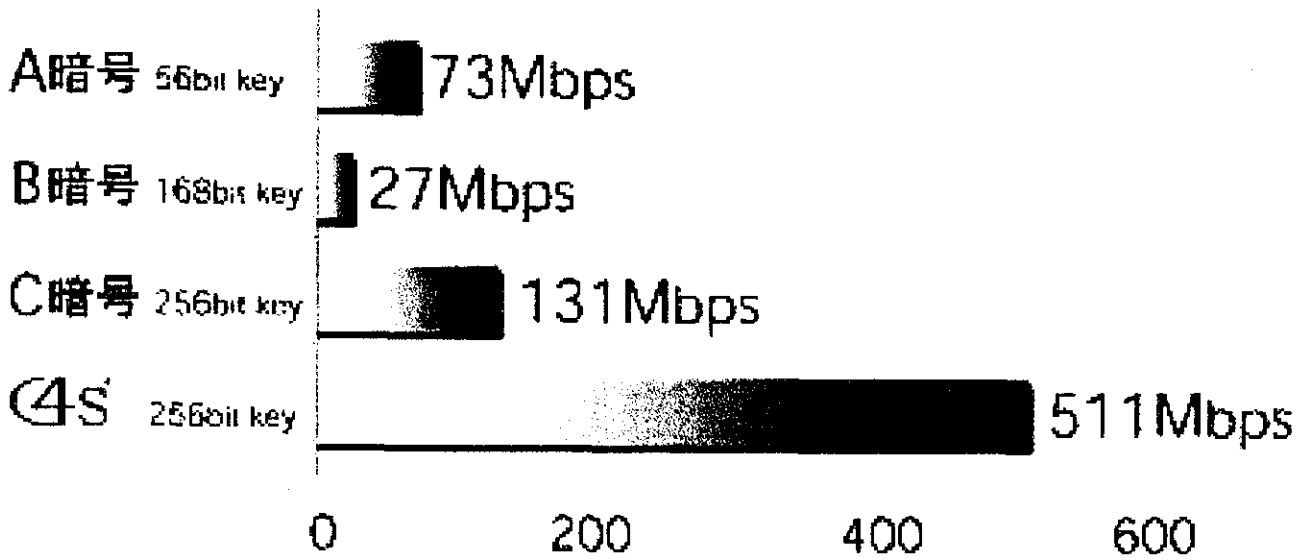
(5) 暗号ベクトルは、内部データを参照、合成することで、毎回新規に動的な変化(置換)を行っています。

✧ 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＞

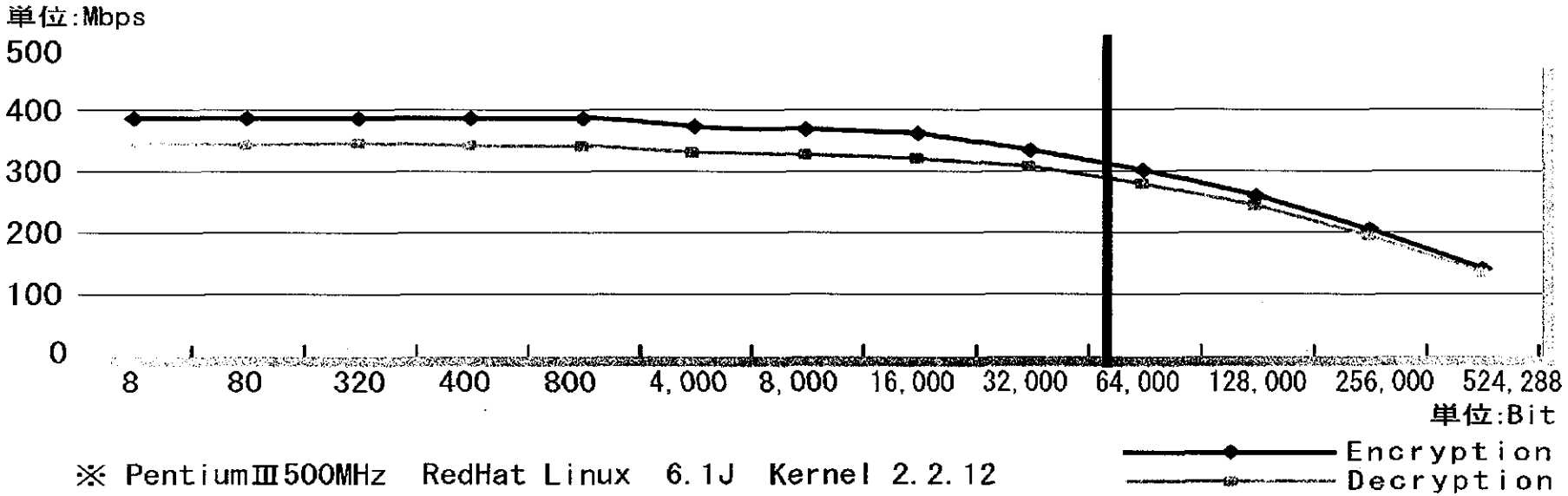
PentiumⅢ 733MHz Key 256bitの環境下で、511Mbpsの処理速度を実現。

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。

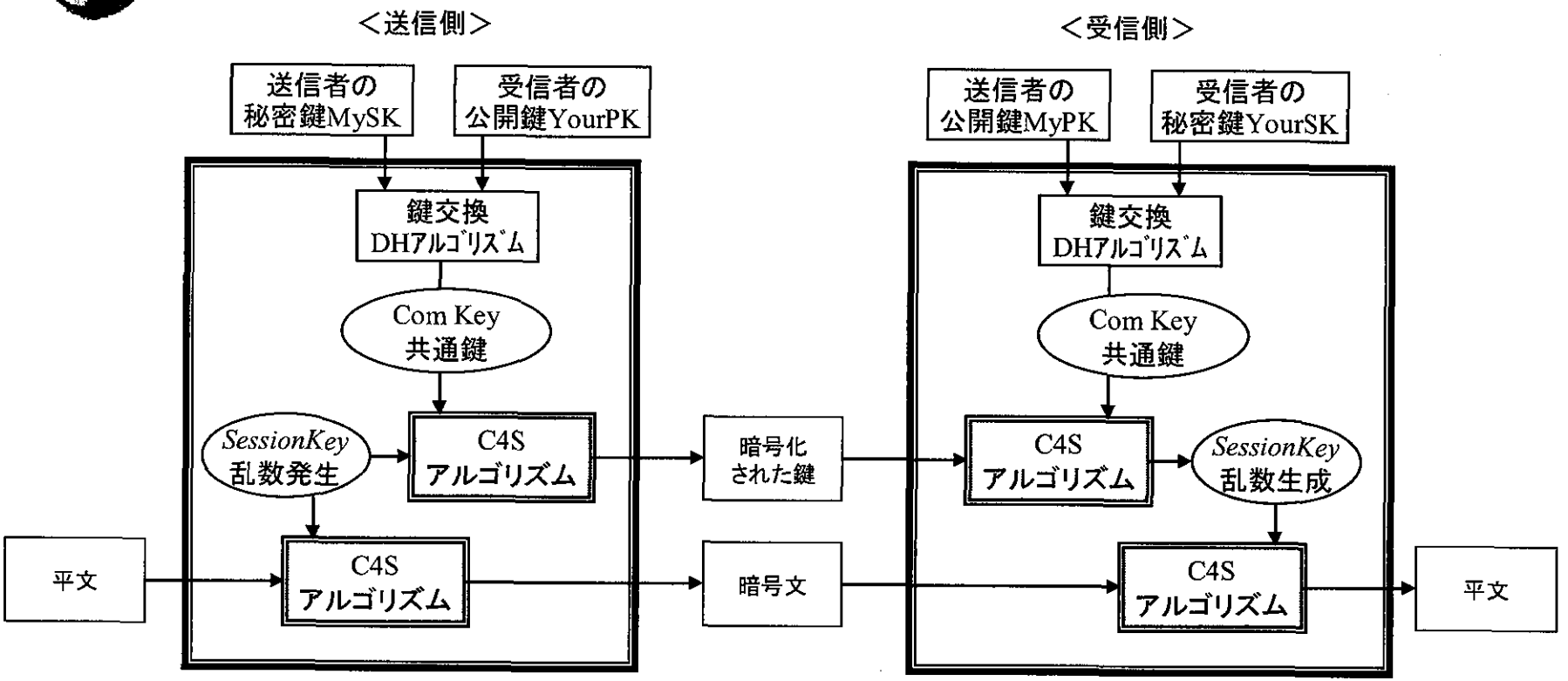
その両方を実現させ、強度・速度ともに優れたブロードバンド時代に

最適な暗号化を可能にしました。

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

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 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＞

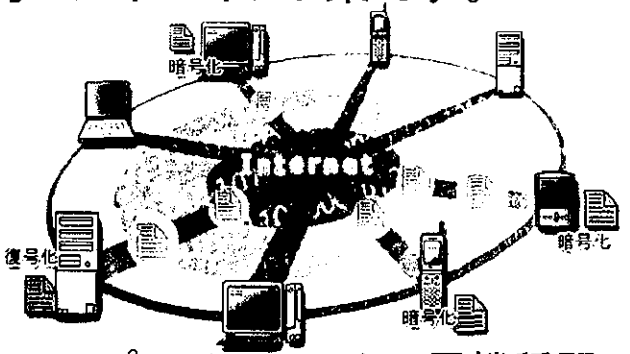
C4 i

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。

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。

Focus Systems, Corp

C4Custom

マルチプラットフォームをコンセプトに、安全性とスピードを高度に両立させたC4S暗号。そんなC4S暗号をベースにし、各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、より処理速度を上げることができました。

C4Customの優れた特徴

●共通鍵暗号モジュールの新シリーズ

C4Sをベースに、プログラムレベルの改良（CPU固有の命令セットの利用やメモリアクセスの最適化等）を行い、各プラットフォームごとに最適化しています。

●C4S比で2倍以上の暗号化速度を実現

C4Sの強みであった高速性な暗号処理を一層高め、Java環境においてはC4Sと比べ2倍強と、さらなる高速化を実現しました。

●C4Sの特徴を継承

C4Sと理論が同じであるため、共通鍵暗号方式、ストリーム暗号方式、暗号鍵が可変長等、C4Sの特徴を継承しています。※ただし、プログラムの大幅な変更により、C4Sとの互換性はありません。

3-4 C4VPN ～高速暗号通信ソリューション～ (1)

Focus Systems,Corp

C4VPN C4VPN

インターネットを介した企業間通信、企業内部の特定部署等との通信のセキュリティを実現します。

C4VPNの優れた特徴

●IP通信の業界標準セキュリティ規格の採用

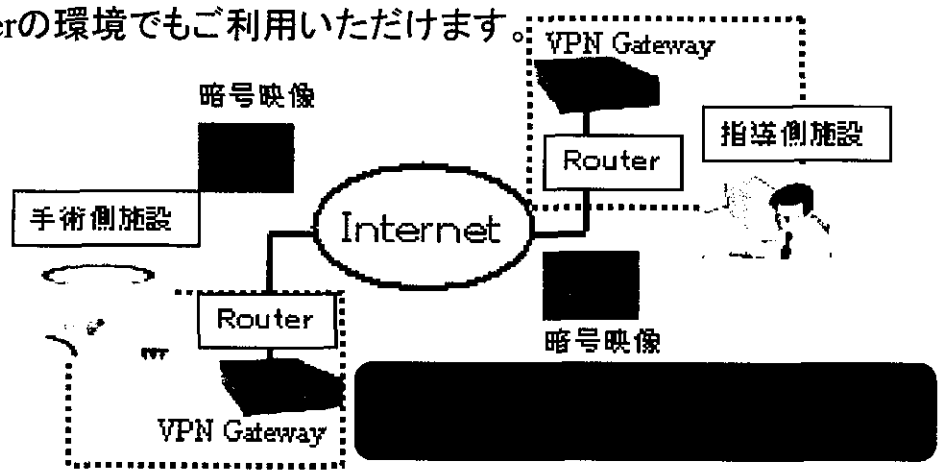
TCP/IP通信にセキュリティを実装するためのIPsec規格に準拠しています。

● ファイアウォール機能・・・パケットフィルタリング機能のファイアウォールを標準搭載。

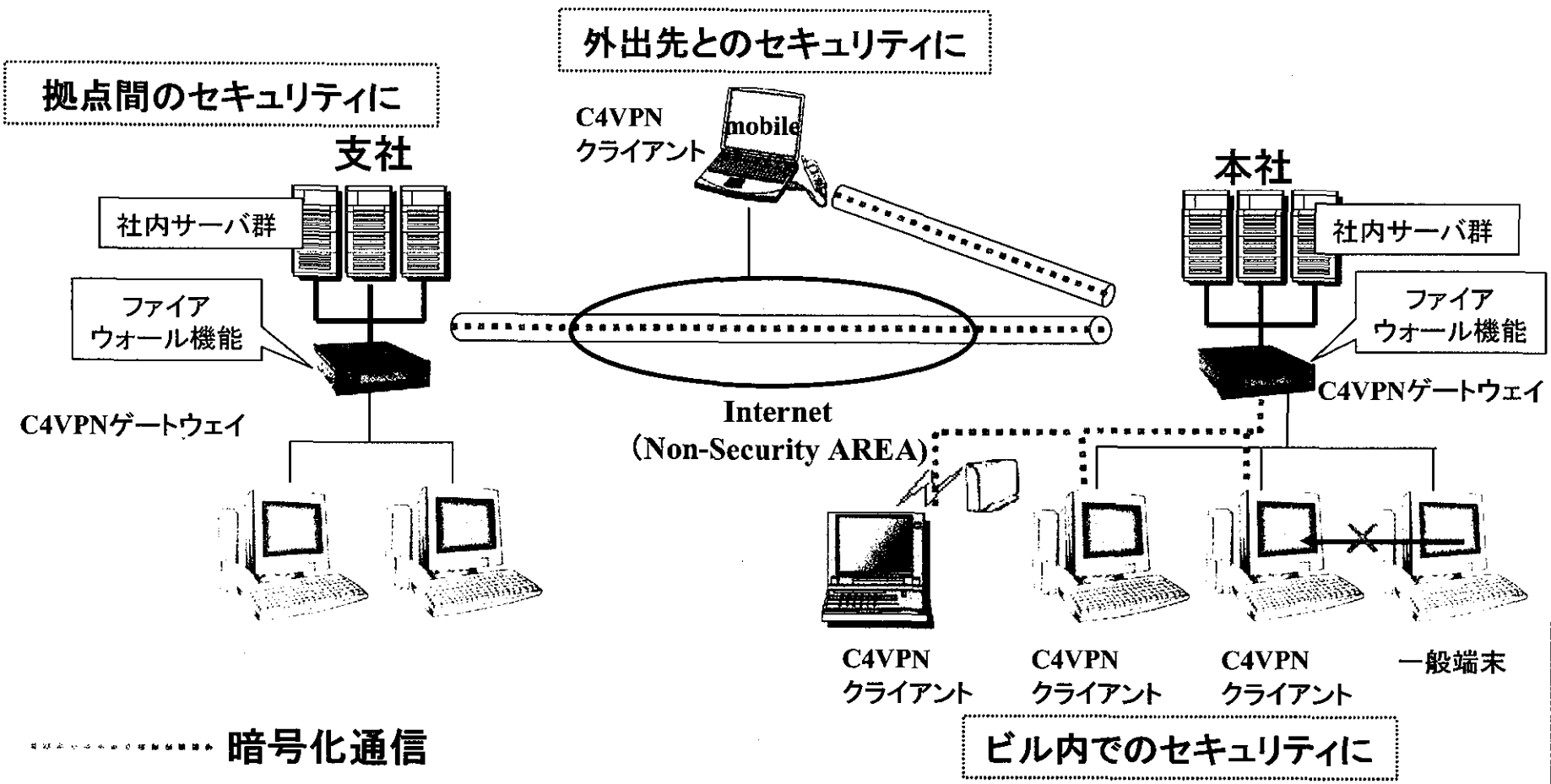
●無線・有線イーサネット対応・・・無線LAN(802.11a、11b、11g)や、FastEther/ギガビットEtherの環境でもご利用いただけます。

＜遠隔医療共同研究で採用＞

指導医側病院(慶應義塾大学病院)と手術側病院(東京医療センター)とをインターネット回線でつなぎデータをやり取りする遠隔医療研究において、セキュリティ確保の為にC4VPNを利用しています。



C4VPN C4VPNのセキュリティ構成図



3-5

C⁴ FILE PROTECTOR

～情報漏洩対策ソリューション～ (1)

Focus Systems, Corp

C⁴ FILE PROTECTOR

企業のPC内のデータは重要な情報であふれています。そんな大切な資産をぞんざいに扱っていませんか？予期せぬ紛失、盗難であなたの大切な情報が他者に漏洩することを防ぎます。

C⁴ FILE PROTECTORの優れた特徴

●簡単なファイル操作でも高いセキュリティ対策

エクスプローラから、クリックメニューから、ユーティリティからと、ユーザー操作の選択肢の豊富さや、シャットダウンの際に暗号化操作を忘れないための自動暗号化など、ユーザーフレンドリーな機能が満載です。

●暗号化に加え、情報漏洩・保護対策機能の充実

ファイルの完全削除、ファイルのセキュリティバックアップなど、ユーティリティツールとしての高い情報メインテナンスを実現しています。

C4 FILE PROTECTOR

～情報漏洩対策ソリューション～(2)

Focus Systems, Corp

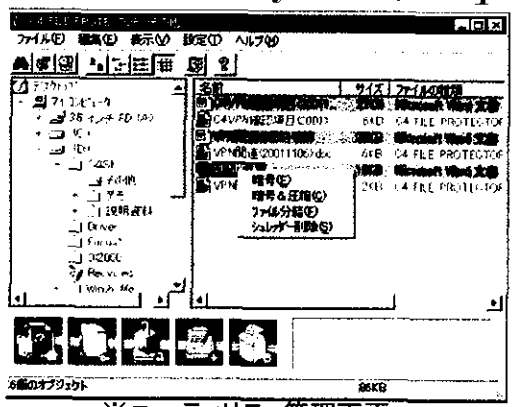
機能

■ ファイル暗号

簡易操作でPC内のファイルやフォルダを暗号化

★右クリックで暗号　→　ユーティリティ、エクスプローラ、デスクトップなどで、直接ファイルを右クリックしての簡単な 暗号、復号を実現します。

★直感的な操作イメージ　→　アイコンへのドラッグ &ドロップでも各種機能が実行されます。



※ユーティリティ管理画面

■ ファイル分割暗号

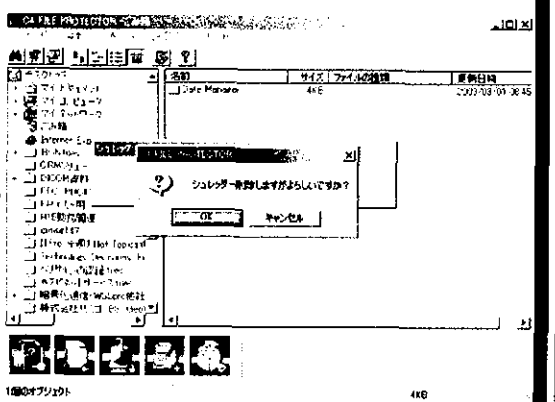
大きなファイルを一定の指定サイズまたはメディアの容量に合わせて分割暗号

■ 暗号圧縮

複数のファイルやフォルダをまとめて圧縮して暗号化し、同一暗号書庫に格納

■ シュレッダー削除

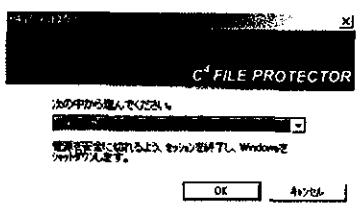
データを二度と復元できない形にして削除



※シュレッダー削除画面

■ セキュアシャットダウン

シャットダウンとともに設定ファイル・フォルダを自動暗号化処理



セキュアシャットダウン画面

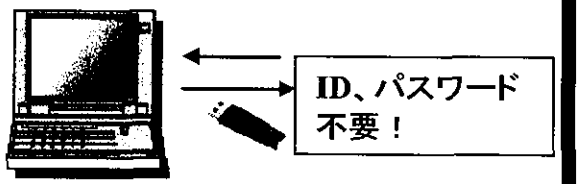
3-6 C4U ～ファイル暗号化アプリケーション～(1)

Focus Systems,Corp

C4U C4U

企業内PCの重要なデータを情報漏洩から守るため、暗号化処理はしたい。
しかし、「パソコン初心者で扱い方が分からない」、「IDやパスワードの入力を手間だと感じる」、または「忘れてしまう」、そういった方でも簡単な操作でファイル暗号化ができるファイル暗号化アプリケーションです。

C4Uの優れた特徴



●簡易操作

初回の暗号化フォルダ設定以後は、C4Uキー（USBキー）の抜き差しのみの操作です。

キーを抜いた状態が暗号化、キーの挿入で復号化と、わずらわしいIDやパスワードなどが不要です。

●耐タンパ性

C4Uキーは耐タンパ性を備えた制御チップを搭載しており、不正にキー情報を読み取ろうとすると、中の情報が壊れ、読み取れないようになっています。

また、キーの再発行には複数個のリカバリーキーを揃えてはじめて可能となる新しいシステムを搭載しています。