

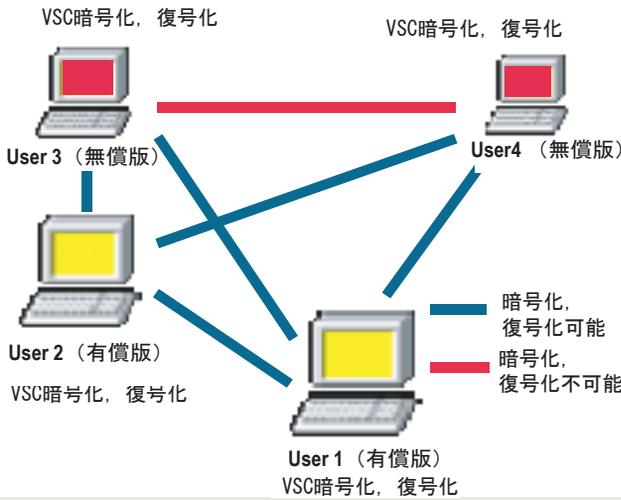
Protect your data

Get ready:

VSC Peer to Peer Version 1.01



ChaosWare Inc.
VSC P2P Version 1.01



株式会社カオスウェアは8月31日にピアツーピア型のセキュリティソフトウェア VSC-P2PVersion1.01 (有償版, 無償版) を出荷開始することになりました。機密性の高いデータを安全な暗号化通信 (ファイル送信) によりユーザーに届ける事が可能になりました。対応OS Windows 2000 及び Windows XPに対応しています。VSC Peer to Peer は機密性の高いファイル (動画ファイルやドキュメントファイル) を暗号化し相手と暗号化通信を行うことができるアプリケーションです。

株式会社カオスウェアは独立行政法人情報通信研究機構 (NICT) プレベンチャー制度及び科学技術振興機構 (JST) プレベンチャー制度により誕生したNICT発第1号のベンチャー企業です。

VSC-P2Pの暗号化通信

VSC-P2Pは機密性の高いファイルを暗号化通信を行い、セキュリティを高めます。この時、以下、三つのプロセスを行いユーザーの一方通信、双方通信、マルチキャスト通信を可能にします。



(1) 公開鍵及び秘密鍵の生成

公開鍵は他者 (B) に対して公開可能な鍵です。VSC-P2Pにて暗号化、復号化したい機密情報を相手に渡したい場合、この公開鍵をVSC-P2Pで作ります。この公開鍵を相手にメール等で送信します。また公開鍵を作った時、同時にできる自分用鍵を秘密鍵ともうします。

注意: 自分 (A)、他者 (B)、ここでは一方通信を例にいたします。

特徴

すぐれたセキュリティ機能

カオスウェア社が独自に開発した世界最速の秘密鍵暗号方式VSC (Vector Stream Cipher) と、公開鍵暗号方式RSAを用いた二重のセキュリティシステムで重要なデータを暗号化するため、極めて機密性の高いデータを保護するために安心して御利用いただけます。

軽量のプログラムと高速な暗号・復号化処理

カオスウェア社によるVSC暗号は極めて高速かつ効率のすぐれた暗号方式であるため、VSC-P2P実行プログラムはフロッピーディスク1枚に保存できるほどファイルサイズの軽量化が実現され、快適に動作させることができます。また、暗号化処理も高速に行えるので、非常にファイルサイズの大きいデータも簡単に暗号化することができます。

有償版および無償版の提供

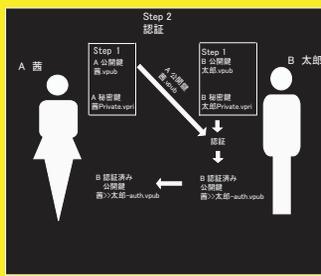
VSC-P2Pでは、有償版のほかに無償版を提供しています。VSC-P2Pの主な利用方法として、電子メールでデータを交換する際のセキュリティを保持するための暗号化・復号化に御利用していた際には、電子メールの送信者・受信者ともにVSC-P2Pをお持ちいただく必要があります。ただし、受信者は必ずしも有償版を御購入していただく必要がなく、弊社をはじめとしたダウンロードサイトより提供する無償版で復号化を行うことができます。そのため多くの方々と暗号化データの交換を可能にする一方、初期導入コストを低く抑えることができます。

広範な御利用方法の提案

- 以上の特徴から、本製品では次のようにさまざまな御利用方法が考えられます。
- (インターネット通信におけるセキュリティ保護の例)
 - 送信者が暗号化データを電子メールで交換し、公開鍵認証された受信者が復号化する。
 - ダウンロードサイトのデータを暗号化し、公開鍵認証されたユーザのみが取得データを復号化できる。
 - (コンピュータ共有環境におけるセキュリティ保護の例)
 - 御利用のコンピュータに存在するデータを、自分専用の鍵で暗号化して保存する
 - (場所を選ばない利便性の例)
 - VSC-P2Pプログラムと必要な鍵をフロッピーディスクやUSBメモリーに保存して携帯し、外出先で受け取った暗号化データをその場で復号化できる。

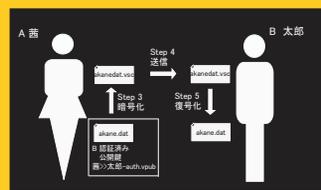
1対多の同時暗号化が可能

VSC-P2Pでは、1対1の相互認証に加え1対多の相互認証を可能にしています。すなわち、1人の送信者は、特定の1人または複数の受信者のみが復号化できるように指定して、データを暗号化できます。



(2) 公開鍵の認証

送った公開鍵を (他者B) の持っている秘密鍵を使って認証を行います。この認証が行われた鍵を認証済み公開鍵ともうします。この公開済み認証鍵を自分 (A) にメール等で送り返します



(3) 暗号化

自分 (A) におくられた公開済み認証鍵を使い、VSC-P2Pにより、ファイルを暗号化します。このファイルは認証を行ったユーザーのみが復号化 (解読) できます。この暗号化されたファイルを他者 (B) に送信いたします。

復号化

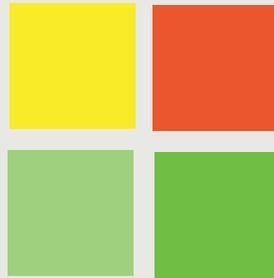
他者Bが受け取った暗号化ファイルをVSC-P2Pを使い復号化を行います。

有償版と無償版の違い		
暗号化	復号化	
有償版	有償版	可
有償版	無償版	可
無償版	有償版	可
無償版	無償版	不可

VSCとは?

VSC (Vector Stream Cipher) は、独立行政法人情報通信研究機構 (<http://www.nict.go.jp/>) とその他の共有する日本国特許第3030341号、特許第3455748号、及び米国特許第6,668,265号で保護されている独自暗号アルゴリズムのストリーム暗号です。

VSC Peer to Peer Version 1.01



ChaosWare Inc.

<開発元・販売元>

株式会社カオスウェア

〒184-8795

東京都小金井市貫井北町4-2-1 独立行政法人情報通信研究機構3号館

Tel : 042-359-6299 Fax : 042-359-6339

URL : <http://www.chaosware.com/> E-mail : p2p@chaosware.com

製品の詳細資料のご請求は、下記で承っております。お気軽にお問い合わせください。