マルチメディア通信と分散処理　111－7
コンピュータセキュリティ　20－7
（2003．2．27）

ハイブリッドチャネルによるセキュア通信方式

大杉俊典* 西垣正勝* 曽我正和† 中村逸一‡

あらまし:

通信路の安全性を高めるために，通信チャネルの多重化による「ハイブリットチャネル」を用いた通信方式を提案する．本稿では特に，携帯電話と有線のインターネットによる通信路の2重化に焦点を当て，「セキュアだが狭帯域な通信路」と「アンセキュアだが広帯域な通信路」の2本の通信路によるハイブリットチャネル通信に対する考察を行う．本方式により実現されるセキュア通信方式，セキュア通信システムを説明し，通信チャネルを多重化することが，盗聴などの攻撃に対する耐性を向上させるだけでなく，秘密データの効率的・機能的な伝送に対しても効果的であることを示す．

キーワード：セキュア通信，通信路の多重化，暗号化通信，ワンタイムパスワード，携帯電話

Secure data communication over hybrid channels

Toshinori Ohsugi*, Masakatsu Nishigaki*, Masakazu Soga†, Itsukazu Nakamura‡

Abstract:

This paper proposes to use multiple data communication channels for secure data communication. Especially, we here focus on a portable phone and the Internet, that is, the hybrid channel by means of "a secure and narrow channel" and "an unsecure and wide channel". By explaining some secure communication schemes and secure communication systems achieved with the hybrid channel communication, it is shown that data communication over hybrid channels is efficient for a secure/effective/functional data transmission.

Keywords: secure data communication, hybrid channels, cipher communication, one-time password, Portable phone

1. はじめに

近年のインターネットの爆発的な普及によって，あらゆる場所で様々なデータ通信を行う機会が増えている．それと同時に悪意を持ったユーザによってネットワークを盗聴され，データが漏洩，あるいは改竄，削除されてしまうという被害が起きている．

特にインターネットは，不正者の介在を考慮する必要のない土壌で開発が進められた歴史を持つ上に，その仕様がオープンになっているため，悪意を持ったユーザによる通信の盗聴は根本的には可能であると言える．また，従来，一般ユーザの使用する端末のコンピュータにおいては，通信を行うコンピュータ間には1

* 静岡大学情報学部情報科学科　Faculty of Information, Shizuoka University
† 岩手県立大学ソフトウェア情報学部　Faculty of Software and Information, Iwate Prefectural University
‡ (株)NTT データ　セキュリティ事業部　NTT Data Corp., Security Business Division
E-mail: nisigaki@cs.inf.shizuoka.ac.jp

つの通信路しか用意されていないことが一般的であった．このため，秘密データを送信するために，暗号通信に関する各種技術・研究が盛んに行われ，実装されるに至っている．

しかし，最近は携帯電話が広く普及し，一般ユーザが備える通信路は単一ではなくなった．すなわち，DSL回線により自宅のデスクトップ PC をインターネットに接続しているユーザや会社の PC を社内 LAN に接続しているユーザが，携帯電話を使って自分の PC にもう一つの通信路を付加することが可能になった．携帯電話は会話というプライバシーが強く求められるデータの送信を担うため，その通信路においてはセキュリティが十分に考慮されている．実際には，i)独自のプロトコルやエンコード方式を採用し，これらの仕様は開示しない☆，ii)基地局の管理を徹底し，また，バックボーンの専用線通信路を地中深く埋めるなどにより物理的な盗聴を困難にしている，iii)基地局から携帯端末間の無線通信に関しては十分な強度のスクランブルを施している，などの方法により安全性が保たれており[2][3]，暗号通信を行わずとも秘密データを送信可能である．

このような現状を踏まえ，複数の通信路を利用した際の通信の安全性を議論することは有意義であると考える．そこで本稿では，多重化された通信路を用いることにより，通信路のセキュリティを高める方式を検討する．特に「セキュアだが狭帯域な通信路」と「アンセキュアだが広帯域な通信路」による通信路の 2 重化に対する考察を行い，ハイブリットチャネルによる通信が盗聴などの脅威を激減させるだけでなく，秘密データの効率的・機能的な伝送に対しても効果的な方式であることを示す．

☆ ただし，各電話会社は既存電話網への投資を原則的に停止し，IP 電話網の構築、拡大に投資を集中させると発表[1]しており，今後は電話網とインターネット網の統合も進むものと推測される．

2. ハイブリッドチャネル

2.1. 通信路の多重化

通信路を多重化し，複数の異なる通信路により構成される通信路をハイブリッドチャネルと定義する．ARPANET が非常時に備えて複数の通信路を用意した（実際にデータが送られるのはその内の一つの通信路のみ）のに対し，複数の通信路を同時に使用して一つのデータが送られることに注意されたい．

通信路をハイブリッドチャネルにし，一つのデータを複数の通信路によって送信することにより，物理的な盗聴をより困難にすることが可能である．通信路の 2 重化を例に採り，これを説明する．

図 1 にデータ D を 1 本の通信路 C で送信するモデルを示す．クラッカーにより通信路 C が盗聴される危険性を「盗聴成功率 P」で表すとする．一方，図 2 はデータ D を 2 つのデータ片 D1 と D2 に分割し，D1 を通信路 C1 により，D2 を通信路 C2 により送信するハイブリットチャネル送信のモデルである．通信路 C1，C2 の盗聴成功率をそれぞれ P1，P2 とする．図 2 においては，クラッカーは 2 つの通信路 C1 と C2 の両方の盗聴に成功しないとデータ D を読み取れないので，ハイブリットチャネル全体の盗聴成功率は $P1 \times P2$ となる．例えば，$P=P1=P2=0.05$ を仮定した場合，$P1 \times P2=0.0025$ である．具体的には，クラッカーにとって，両通信路（例えば，ケーブルの信号と無線の電波）を同時に盗聴しなければならない，両方の通信路の通信方式を知らなければならない，などの負荷が発生し，盗聴が難しくなる．

2.2. 携帯電話とインターネットによるハイブリッドチャネル

特に本稿では，携帯電話と有線のインターネットによるハイブリットチャネルに焦点を当てる．携帯電話はクローズな通信路で安全性は高いが，無線のため通信帯域は狭く，言わば「セキュアだが狭帯域な通信路」である．インターネットは基本的にはオープンな通信路であり，盗聴などは容易いが，光ファイバーや DSL

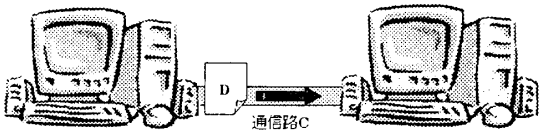

図1：データを1本の通信路で送信するモデル

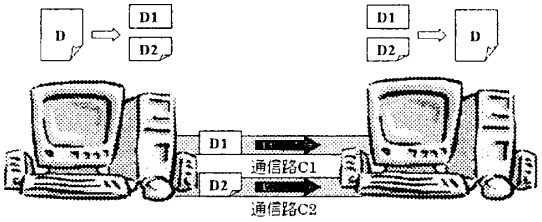

図2: データを2本の通信路で送信するモデル

による高速広帯域の通信が可能である．暗号化通信を行うことにより通信の安全性をも兼ね備えることが可能であるが，本稿ではこれを考慮から外し，インターネットを「アンセキュアだが広帯域な通信路」と考えることにする．

以降，「セキュアだが狭帯域な通信路」と「アンセキュアだが広帯域な通信路」の2本の通信路によるハイブリットチャネルの有用性を検討する．なお本稿では，セキュアだが狭帯域な通信路を SN チャネル（Secure and Narrow Channel），アンセキュアだが広帯域な通信路をUWチャネル（Unsecure and Wide Channel）と呼ぶことにする．

2.3. 関連研究

文献[4]では，2つの通信路を使用したワンタイムパスワード方式，電子決済方式が示されている．また，文献[5][6]では，インターネットと携帯電話を併用した電子決済方式が提案されている．

本稿はインターネットと携帯電話の2回線によるハイブリットチャネルに焦点を当ててはいるが，ハイブリットチャネルの本質は通信路のn重化を対象にするものであり，文献[4][5][6]を包含する上位概念を示すものだと言えよう．

また，文献[4][5][6]の目的がセキュアな第2通信路（携帯電話）を付加することにより電子商取引の安全性を高めることにあるのに対し，本稿は性質が全く異なる2つの通信路（SNチャネルとUWチャネル）を巧みに利用することにより実現され得る様々な効果を考察することを目的としている．

3. ハイブリットチャネルによるセキュア通信方式

SNチャネルとUWチャネルの2つの通信路から成るハイブリットチャネルを考えた場合，以下のようなセキュア通信を実現することができる．

3.1. 共通鍵暗号化通信

共通鍵暗号による暗号化通信を行うに当たり，問題となるのが鍵の共有である．ハイブリットチャネルによる通信ならば，SN チャネルを使って鍵を安全に交換できる．鍵の共有が完了し次第，UW チャネルを使って暗号化コンテンツの送受信が可能となる．一般的に，鍵は「サイズは小さいが秘密に送信しないといけないデータ」であり，コンテンツは「サイズは大きいが（暗号化により守られているため）盗聴されてもよいデータ」であるため，SN チャネルと UW チャネルによるハイブリットチャネルを用いての通信に非常にマッチする．

なお，ハイブリットチャネルによる通信は SN チャネルとUWチャネルを同時に使用することを特徴としているため，以下に示すように共通鍵を動的に変更しながら暗号化通信を行うことが可能である．以下の例は，ハイブリットチャネルを通じサーバからクライアントにコンテンツが送られてくる際の，クライアント側の動作を記したものである．ここで，コンテンツはnブロックに分割されている．

フェーズ0.

SN チャネル：フェーズ 1 の暗号化通信にて使用する鍵K1を受信する．

フェーズ 1.

SN チャネル：フェーズ 2 の暗号化通信にて使用する鍵 K2 を受信する.

UW チャネル：K1 により暗号化されたコンテンツの第 1 ブロックを受信する.

フェーズ 2.

SN チャネル：フェーズ 3 の暗号化通信にて使用する鍵 K3 を受信する.

UW チャネル：K2 により暗号化されたコンテンツの第 2 ブロックを受信する.

以上をコンテンツの第 n ブロックを受信するまで繰り返す.

3.2. コンテンツの分離送信

図 3 は掛け算の九九の表であるが，これを「空白と改行の情報を除いたデータ（図 4）」と「2 桁おきに空白を入れ，20 桁おきに改行を入れるというインデント情報」に分離することができる．ここでは，図 4 の形式のデータをコンテンツの「ボディ」，インデント情報をコンテンツの「書式」と呼ぶことにする.

00	01 02 03 04 05 06 07 08 09
01	01 02 03 04 05 06 07 08 09
02	02 04 06 08 10 12 14 16 18
03	03 06 09 12 15 18 21 24 27
04	04 08 12 16 20 24 28 32 36
05	05 10 15 20 25 30 35 40 45
06	06 12 18 24 30 36 42 48 54
07	07 14 21 28 35 42 49 56 63
08	08 16 24 32 40 48 56 64 72
09	09 18 27 36 45 54 63 72 81

図 3: 掛け算の九九の表

000102030405060708090101020304050607080902020406
08101214161803030609121518212427040408121620242832360505101520253035404506061218243036424854070714212835424956630808162432404856647209091827364554637281

図 4: 図 3 から空白と改行の情報を除いたデータ

ボディのデータが膨大であり，書式のデータが少量であるコンテンツの場合，ボディを UW チャネルにより，書式を SN チャネルにより送受信するという「コンテンツの分離送信」は有効である.

特に，図 3，図 4 の例のようにボディだけを見てもその意味が判別できないようなコンテンツに対しては，分離送信の効果は大きい．すなわち，書式が SN チャネルで秘密に送信されることにより，不正者が UW チャネルを流れるボディのみを盗聴してもコンテンツを復元することが難しく，簡易的な暗号通信が達成されることになる．換言すれば，「サイズは小さいが秘密に送信しないといけないデータ」と「サイズは大きいが盗聴されてもよいデータ」に分離することができるコンテンツに対しては，SN チャネルと UW チャネルによるハイブリットチャネルを用いての分離通信は非常に効果的である.

4. ハイブリットチャネルによるセキュア通信システム

SN チャネルと UW チャネルの 2 つの通信路から成るハイブリットチャネルを利用することにより，以下のようなセキュア通信システムを構築することができる.

4.1. ワンタイムパスワードシステム

ハイブリッドチャネルを利用し，以下のプロトコルにより，ワンタイムパスワードシステムを実現することができる．なお，システムの概観を図 5 に示す.

0. ユーザは，前もってユーザ ID と自分の携帯電話の番号をサーバに登録しておく.
1. ユーザは，UW チャネル（インターネット）によりサーバにアクセスし，ユーザ ID を入力して，ログイン要求をする.
2. サーバは，ワンタイムパスワードを生成し，SN チャネルにより（当該ユーザの携帯電話に電話をかけて）ワンタイムパスワードを送信する.
3. ユーザは，SN チャネルにより届けられたワンタ

イムパスワードを，UW チャネル（インターネット）によりサーバに送信する．

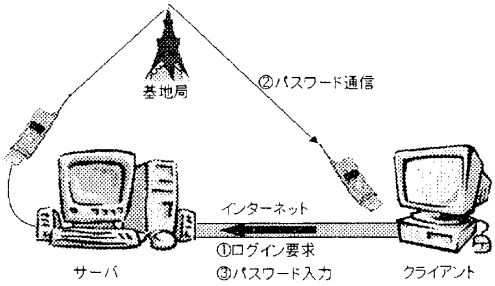

図 5: ワンタイムパスワードシステム

従来のワンタイムパスワードは，乱数同期式，カウンタ同期式，チャレンジ&レスポンス式に大別することができる．乱数同期式のワンタイムパスワードは，何らかの方法によりサーバとクライアント（ユーザ）間で乱数を同期させておき，クライアントが正しい乱数をサーバに呈示したときのみログインを許す方式[7]である．カウンタ同期式のワンタイムパスワードは S/KEY[8]が有名である．S/KEY では，まず，クライアント側で任意の初期値 V に対するハッシュ値 h(V)，h(h(V))，h(h(h(V)))，・・・を求め，これらを H_1，H_2，H_3，・・・とし，サーバに H_n のみを登録する．クライアントは 1 回目のログインの際にサーバに H_{n-1} を呈示し，サーバ側で $H(H_{n-1})=H_n$ が確認できたときのみログインを許可する．一方，チャレンジ&レスポンス式のワンタイムパスワードは，サーバとクライアントでレスポンス発生機構を共有しておき，サーバがその都度生成するチャレンジ値に対応するレスポンス値をクライアントが呈示できたときのみログインを許す方式である[9]．

結局，既存の方式でワンタイムパスワードシステムを実現する場合，乱数同期機構，初期値 V の記憶とハッシュ値計算機構，レスポンス値計算機構などの何らかのセキュアモジュールをクライアント側に実装しなければならない．これに対し，ハイブリットチャネルを利用したワンタイムパスワードシステムにおいては，サーバ側で生成されたワンタイムパスワードがその都度クライアントに通知されるだけであるため，クライアント側にはパスワード生成に関わるモジュールは何も存在しない．よって，不正者がクライアント側の PC や携帯電話をいくら解析してもパスワードに関する情報は一切漏れることがない．

また，本方式によるワンタイムパスワードシステムにおいては，不正者が正規ユーザに成りすましてサーバにログインを試みた場合も，サーバに登録されている正規ユーザの携帯電話にワンタイムパスワードが送信される．すなわち，正規ユーザは身に覚えのないワンタイムパスワードを受領することになり，不正アクセスに気付くことができる．

4.2. カスタマイズ配信システム

近年，ユーザのニーズや嗜好に応じてユーザごとにカスタマイズされた情報を配信するサービスが注目されている[10][11]．全てのユーザに同一の一般情報を配信するのと同時に，各々のユーザに各自の嗜好に合わせたオプショナル情報を伝えるようなカスタマイズ配信システムを考えた場合，広帯域な UW チャネルにより大量な一般情報を送信しつつ，狭帯域の SN チャネルを使って各ユーザにオプショナル情報を送れば，効率良く配信のパーソナライズ化を実現することができる．

ここで，オプショナル情報が各ユーザのニーズや嗜好を反映するものであると言うことは，逆に，オプショナル情報から当該ユーザのニーズおよび嗜好が推測され得ることを意味する．よって，オプショナル情報からユーザのプライバシーが漏れることを防止するために，オプショナル情報を安全な SN チャネルにより送信することは意義が大きい．

カスタマイズ配信システムの一例として，ニュース配信システムを図 6 に示す．ヘッドラインニュースが一般情報としてインターネット経由で受信されているのに対し，ユーザが事前に登録しておいた自分の趣味に関係した「個人宛ニュース」が携帯電話を通じて送られてきている．また，図 7 はユビキタスなコンピュ

ータ環境を想定し，街頭のディスプレイを使って図 6 と同様のニュースを複数のユーザに一斉に配信するシステムを表した図である．街頭ディスプレイにインターネット経由で送信されたヘッドラインニュースが表示されると同時に，個人宛ニュースが携帯電話により各ユーザに個別に送られ，ユーザのヘッドマウントディスプレイに表示される．ユーザは街頭ディスプレイの表示とヘッドマウントディスプレイの表示を重ねて見ることにより，カスタマイズされたニュースを読むことができる．

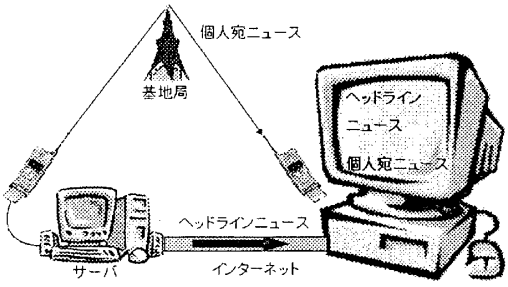

図 6: カスタマイズ配信システム

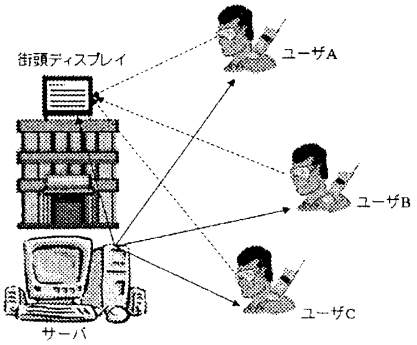

図 7: ユビキタス環境におけるカスタマイズ配信システム

5. まとめ

本稿では，データ通信の安全性を高めるために，通信路を多重化したハイブリットチャネルによる通信を提案し，特に「セキュアだが狭帯域な通信路」と「アンセキュアだが広帯域な通信路」による通信路の２重化について検討した．本方式を利用することにより実現されるセキュア通信方式，セキュア通信システムを説明し，ハイブリットチャネルによる通信が盗聴などの攻撃に対する耐性を向上させるだけでなく，秘密データの効率的・機能的な伝送に対しても効果的であることを示した．

6. 参考文献

[1] 「NTT 営業利益 1.7 倍に」，朝日新聞，2002 年 4 月 20 日，朝刊，11 面

[2] 高橋健太郎，「携帯電話のしくみを探る」，日経 NETWORK，No.19，pp59-75，2001.11

[3] 「とまどう通信業者」，日経産業新聞，1999 年 8 月 13 日，日刊，1 面

[4] 塩田岳彦，田中琢也，情報サービス提供方法，特許公報，特開 2002-32692

[5] 藤井治彦，塩野入理，携帯電話を用いた匿名購入システム，FIT2002，M-3，2002.9

[6] 藤井治彦，携帯電話を用いた認証方式，情報処理学会第 64 回全国大会，Vol3,pp429-430，2002.3

[7] セキュリティ研究会，「最新インターネットセキュリティがわかる」，技術評論社，ISBN4-7741-0945-2，2002.2

[8] 多治見寿和，「ワンタイムパスワード」，UNIX MAGAZINE，1 月号，pp59-67，1999. 1

[9] 山本和彦，「OTP(One-Time Password)」，UNIX MAGAZINE ，2 月号，pp68-77，1996.2

[10] 野々下裕子, ASCII24 ニュース, 2000 年 6 月 26 日，「米国ビジネススクールのエッセンスを―シリコンバレーの名物 IT コンサルタントが講演」，http://ascii24.com/news/i/topi/article/2000/06/26/609781-000.html

[11] 上野寿，「デジタルコミュニケーションの新たな地平」，JAGAT，http://www.jagat.or.jp/story_memo_view.asp?StoryID=2490