閉域通信におけるセキュリティ機能の検討

3N－8

力石　徹也　Thomas Hardjono　荒木　禎史　太田　理

（株）ＡＴＲ通信システム研究所

１．はじめに

CCITTでは通信範囲を登録されたグループ内に限定する閉域通信サービス（Closed User Group：CUG）に関する勧告を行なっている。CUGは閉域内では相互に通信できるが外部との通信は禁止するサービスで、これを別の観点から見ると情報セキュリティを考慮したサービスであると考えられる。しかしCUGにはそれ自身が持つ機能により思いもよらない相手や不適切な相手との間に通信経路が存在するという“隠れパス”の問題がある。

本論文ではCUGに隠れパスが存在することを明らかにし、到達可能性解析を用いた解析法を示す。さらにその解析法を用いた対策案を示す。

２．Closed User Group

CUGは通信の範囲を同一のグループに属する端末（ユーザと呼ぶ）に限定し、グループ内でのユーザ間相互の通信は可能であるが、それ以外の端末との通信を基本的に禁止するサービスである。(1)

しかしユーザは複数のCUGに所属すること（複数所属と呼ぶ）が可能である。またグループ外との通信が必要な場合を考慮して、特定のユーザに対してCUGのグループに属さない端末（外部ユーザと呼ぶ）との間に次の機能を認めている。

①外部ユーザへアクセスできる。（CUG Outgoing Access：CUGOA）

②外部ユーザからのアクセスを受けられる。（CUG Incoming Access：CUGIA）

ただしユーザはどちらか一つの機能しか実行することができない。

CUGでのユーザ間のアクセスは次のようにして実行される。複数のユーザが集まってCUGのグループを構成した場合、Administrationと呼ばれる管理者からグループ毎にInterlock Codeという所属グループIDが割り当てられる。交換機はユーザ毎にこのInterlock Codeとユーザの資格を記録する。ユーザからCUGでのアクセス要求があった場合、要求したユーザ側の交換機および要求されたユーザ側の交換機は、Interlock Codeとユーザの資格にもとづき双方のユーザが正当なCUGのユーザであるかを確認する。その結果問題がなければ接続する。

３．CUGの持つ問題点

CUGはこのような閉域通信を目的としているが、複数所属およびCUGOA，CUGIAという機能によって、他グループに所属するユーザ（他グループユーザと呼ぶ）や外部ユーザとの間に通信経路（パスと呼ぶ）が形成される。

このパスが連鎖状に接続された場合、思いもよらない相手や不適切な相手との間の通信経路である隠れパスがネットワークに形成され、これにより情報が漏洩する可能性がある。次に隠れパスの例を示す。

［例１］隠れパスの例

図１のように、複数所属およびCUGOAとCUGIAによって各グループが連鎖状に接続された場合を考える。通常グループ１（Ｇ１と表す）のユーザは隠れパスの存在を知らない。しかしＧ１とグループ２（Ｇ２と表す）に所属するユーザ（共通ユーザと呼ぶ）が存在し、Ｇ２にCUGOAを行なえるユーザ（CUGOAユーザと呼ぶ），グループ３（Ｇ３と表す）にCUGIAを受けられるユーザ（CUGIAユーザと呼ぶ）が存在した場合、Ｇ１のユーザ→共通ユーザ→Ｇ２のユーザ→CUGOAユーザ→外部ユーザ（Ｏと表す）→CUGIAユーザ→Ｇ３のユーザという隠れパスが形成され、結果的にＧ１のユーザの情報がＧ３のユーザに漏洩する可能性がある。

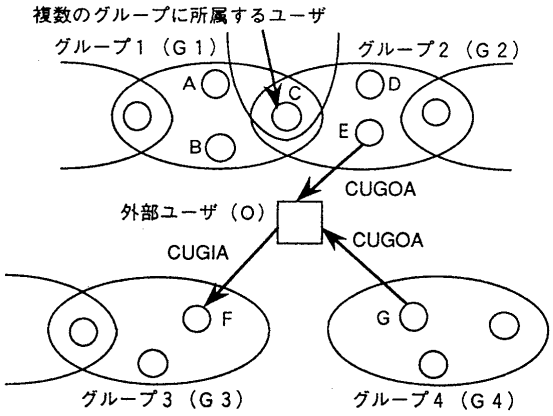

図１ CUGの隠れパスの例

この隠れパスは、２ユーザでグループを構成しその間に通信を限定したBilateral Closed User Group（BCUG）にも存在する。(2) (3) しかし例１に示したようにCUGの隠れパスは、グループに所属するユーザの数が多い，一ユーザが複数のグループに所属できる，CUGOAとCUGIAが行なえるという理由によりその形態が複雑になる。また図１の中の外部ユーザは実際には個々の外部ユーザの集合であり、個々の外部ユーザはネットワークの中に多数存在している。このためCUGの隠れパスの解析は難しくなる。

４．隠れパスの解析と対策

一般的にCUGの隠れパスは、ユーザ，外部ユーザを全て記述し、そのユーザ間での到達可能性解析(4)を行なうことにより解析できる。しかし現実的にはCUGの構成が複雑であるため解析の記述量や計算量が膨大になる。ここではこの問題を解決する方法を検討する。

4-1隠れパスの解析

（１）複数のグループに所属するユーザを介したパスの解析

図１に示すような複数のグループに所属するユーザを介したパスの存在は、到達可能性解析を行なうことにより解析できる。グループ内ではユーザは相互に通信できるためユーザ間のアクセス関係を表す行列の要素は全て１になる。これより図１のＧ１－Ｇ２間の到達可能性解析の結果を示す行列の要素も全て１となり、Ｇ１とＧ２の全ユーザ

A Study about Security Functions in Closed User Group Communication.

Tetsuya Chikaraishi , Thomas Hardjono , Tadashi Araki , Tadashi Ohta.

ATR Communication Systems Research Laboratories.

間にはパスが存在することを示している。（注：行列の要素が１であった場合、行から列に対してパスが存在し、０であった場合パスは存在しない）

この結果１ユーザが複数のグループに所属する場合、一般的にそのグループ間には必ずパスが存在する。

（２）CUGOA，CUGIAにより生じるパスの解析

図１に示すようなCUGOA，CUGIAによるパスの存在は到達可能性解析を行なうことにより解析できる。図１のCUGOAによるＧ２のユーザと外部ユーザのとの間のアクセス関係を示す行列は図２（ａ）になる。これより到達可能性解析の結果は図２（ｂ）になり、Ｇ２の全ユーザから外部ユーザへのパスの存在を示している。

同様にCUGIAによる外部ユーザとＧ３のユーザとの間のパスの存在も到達可能性解析により解析でき、外部ユーザからＧ３の全ユーザへのパスが存在する。

この結果グループにCUGOAまたはCUGIAを行なえるユーザが存在する場合、一般的にそのグループと外部ユーザ間には必ずパスが存在する。

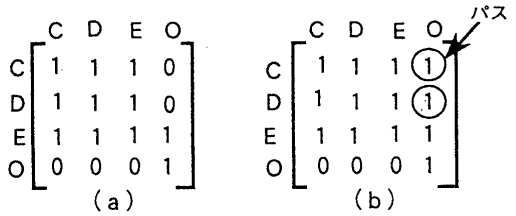

図２ CUGOAの到達可能性解析の例

（３）ユーザからグループへの縮退

以上の検討より次のことが明らかになる。

①（１）の他グループユーザ間のパスはグループ間のパスと等価である。

②（２）のユーザー外部ユーザ間のパスはグループ－外部ユーザ間のパスと等価である。

これより他グループユーザ間のアクセス関係を表す行列はグループ間のパスを表す行列に縮退でき、ユーザと外部ユーザとの間のアクセス関係を表す行列はグループと外部ユーザとの間のパスを表す行列に縮退できる。

（４）CUGの隠れパス解析

これらの縮退した行列を用いて到達可能性解析を行なうことによってCUGの隠れパスの解析が、縮退する前の記述形式による方法よりも少ない計算量で実現できる。次にCUGにおける隠れパス解析の例を示す。

［例２］CUGにおける隠れパス解析の例

図１の隠れパスの解析を行なう。縮退したＧ１－Ｇ２，Ｇ２－Ｏ，Ｏ－Ｇ３間のパスを表す行列を図３（ａ）（ｂ）（ｃ）に示す。これらより図４（ａ）のような全体でのパスを示す行列を作成する。ここでは比較のためＧ４と外部ユーザとの間にCUGOAを設定した。この行列をブール代数演算で４乗して到達可能性解析を行なう。その結果は図４（ｂ）になり、Ｇ１→Ｇ２→Ｏ→Ｇ３，Ｇ４→Ｏ→Ｇ３という隠れパスは存在するが、Ｇ１，Ｇ２とＧ４との間には存在しないことがわかる。

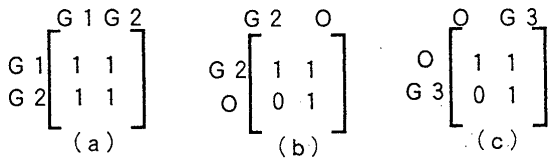

図３ 縮退した行列

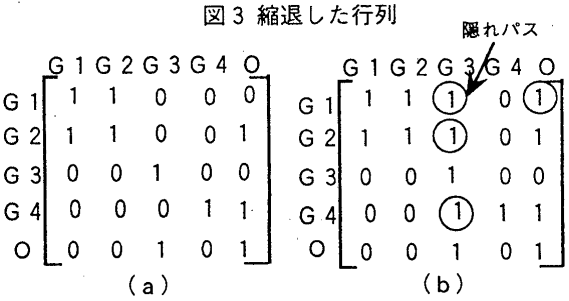

図４ 到達可能性解析の例

4-2 CUGでの隠れパス対策

CUGでの隠れパス対策案を次に示す。

①隠れパス解析はCUGの管理者であるAdministrationが行なう。

②Administrationは複数のグループに所属しているユーザ毎の所属グループのリストとCUGOA，CUGIAを行なうユーザのリストを作成しておく。

③ユーザは特定の相手との間の隠れパスの解析をAdministrationに対して依頼する。

④Administrationは縮退したグループ間またはグループ－外部ユーザ間のパスを示す行列を用いて到達可能性解析を行なう。

⑤特定の相手との間に隠れパスが存在した場合、Administrationは依頼したユーザに対して警告を発する。

この際Administrationが依頼したユーザに対して無制限に隠れパスが存在することを通知するのは、プライバシ上の問題があると思われ適切でない。またCUGの状態を知ることを目的として悪意を持ってこの解析を利用する可能性がある。このためこれらを防止する何等かの制限が必要であろう。

また到達可能性解析を行なった結果、大多数のユーザ間に隠れパスが存在する可能性がある。この原因はCUGでの複数所属とCIGIA，CUGOAの機能のためである。これよりCUGの隠れパス問題を解決するには、これらの機能を廃止するか、またはこの機能の実行を監視する必要がある。

５．まとめと今後の課題

CCITT勧告の閉域通信であるCUGに隠れパスが存在することを示した。その隠れパスを解析するには到達可能性解析が有効であるが、CUGの構成が複雑になるためそのままでは解析の記述量，計算量ともに増加する。そこでCUGのグループ間，グループ－外部ユーザ間のパスを示す縮退した行列を導入し、これにより少ない計算量で解析が実現できることを示した。さらに対策の例としてCUGでの隠れパスの通知法を示した。

今後はCUGなどのネットワークでの隠れパス対策について、プロトコルを含めより具体的な方法を検討する予定である。

［参考文献］

（１）CCITT , Recommendation X.301

（２）力石徹也，竹中豊文：“閉域通信におけるセキュリティ問題”，信学会1991春大，SB-6-1（1992年3月）

（３）力石徹也，荒木禎史，Thomas Hardjono，竹中豊文：“閉域通信におけるセキュリティ問題の解析”，1992年暗号と情報セキュリティシンポジウム，SCIS92-9C（1992年4月）

（４）Tetsuya Morizumi，Hiroshi Nagase，Toyofumi Takenaka，Koichi Yamashita：“An Evaluation of Security Requirements Based on the Capability Model”，IEICE TRANSACTIONS，VOL. E 74，NO. 8，AUGUST 1991