マルチメディア通信と分散処理　54－9
（１９９２．３．５）

分散形ソフトウェア開発環境のセキュリティ方式

浅見秀雄，宮脇正守，田中 清，福山峻一
ＮＴＴソフトウェア研究所

コンピュータネットワークを使った分散形ソフトウェア開発環境では、セキュリティが重要な問題である。特に、発注元企業と外注先企業とが協同でソフトウェア開発を行うとき、両者の情報セキュリティが問題となる。企業間の情報交換と企業の情報セキュリティは両立しなければならない。

本稿では、この両立のために環境を３つのセグメント（発注元の環境、発注元と外注先との協同作業のための環境、および外注先の環境）に分け、それらのセグメントの間での情報配送を制御するセキュリティ制御コンセプトを提案する。

本コンセプトは、ＴＣＰ／ＩＰプロトコルを用いた全国規模の社内用分散形ソフトウェア開発環境に適用され、その有効性が確認されている。

A Security System for Distributed Software Environment

Hideo ASAMI, Masashi MIYAWAKI, Kiyoshi TANAKA and Shun'ichi FUKUYAMA

NTT Software Laboratories

Nippon Telegraph and Telephone Corporation
1-9-1 Konan, Minato-ku, Tokyo, 108 Japan

In a distributed software development environment using a computer network, secureity is a critical issue. Especially, when an customer and subcontractor corporations unite for cooperative software development, a problem is the information security of both parties. Information interchange between corporations, and information security of corporations should be consistent with each other.

Such consistency is realized by partitioning the environment into three segments; an customer's environment, an environment for cooperative projects between customer and subcontractors, and a subcontractor's environment, and by controlling information delivery between these segments.

In this paper a security control concept for cooperative projects is proposed.

Nippon Telegraph and Telephone corporation (NTT) has applied this security control concept to its nationwide distributed software development environment with TCP/IP protocol for its internal use, and has confirmed its effectiveness.

1．はじめに

ソフトウェアの生産性の向上のための基盤の一つは、分散形ソフトウェア開発環境である。

これは、ＵＮＩＸワークステーションやターゲットマシンなどの装置を接続するローカルエリアネットワーク（ＬＡＮ）環境と、それらのすべての環境をワイドエリアネットワーク（ＷＡＮ）で相互接続したものからなるシステムである。

これにより、操作の容易なＵＮＩＸワークステーションによる効率的なソフトウェア開発、およびネットワークによる容易な情報配送、遠隔の資源の効果的な利用が可能となる。

ところで、大規模なソフトウェアを開発する企業では、外注を使うことが一般的である。発注元企業と外注先企業とがソフトウェア開発で協同作業をするとき、情報セキュリティが分散形ソフトウェア開発環境の実用性のキーポイントとなる。

開発環境を複数の企業で共用すると、ネットワーク上での情報配送の容易さゆえに、セキュリティの脅威が増大する。すなわち、分散形ソフトウェア開発環境での協同のソフトウェア開発には、次のような一見相反する条件が要求される。

- *発注元と外注先とで必要な情報をやりとりできること*
- *それぞれの企業の情報セキュリティが守られること*

研究分野での従来のコンピュータネットワークは、ふつう、厳重なセキュリティ制御メカニズムを必要としていなかった。これは、ネットワークを異なる組織で共用せず、他ネットワークとの接続点でのみ情報セキュリティを守ればよいケースが多かったからである。

本稿では、次の観点から、情報セキュリティ問題の解を提案する。

(a) 容易な情報セキュリティ制御のためのネットワーク構成

(b) ゲートウェイを用いた、情報種別ごとの情報配送制御方式

2．分散形ソフトウェア開発環境のネットワーク構成

2．1　ネットワークの階層構成

分散形ソフトウェア開発環境は、各開発サイトにあるＬＡＮ環境と、それらのすべての環境をＷＡＮで相互接続したものから構成されるシステムである。

このようなネットワークでは、セキュリティを確保するためのネットワーク管理が容易であることが要求される。この要求条件を満たすには、ネットワーク構成を階層化し、階層的なネットワーク管理体制に基づいて管理を分担する必要がある。

たとえば、数千のノードを含む大規模な企業ネットワークの場合には、以下のような３階層のモデル（図１）に基づいて構成するのがよい。

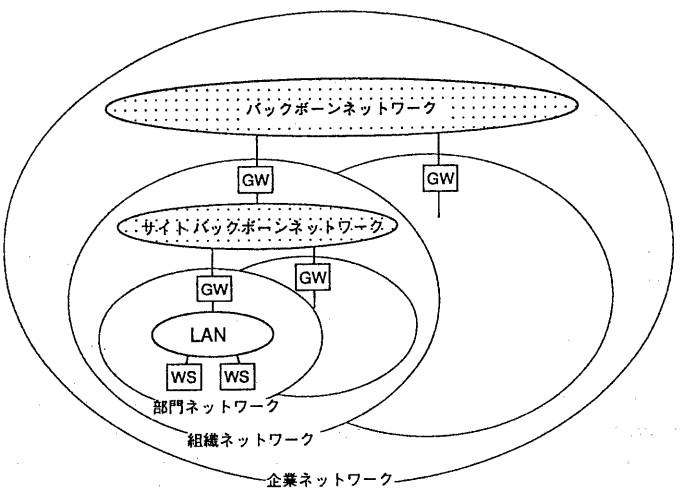

図１　ネットワークの階層構成

部門ネットワーク：部門単位でワークステーションやターゲットマシンを接続するＬＡＮからなるネットワーク

組織ネットワーク：組織単位で部門ネットワークを組織内のサイトバックボーンネットワークによって結合したネットワーク

企業ネットワーク：高速通信回線を使ったバックボーンネットワークによって組織ネットワークを相互接続した全社的ネットワーク

２．２　部門ネットワークの分割

部門ネットワーク内で行われるソフトウェア開発に外注が用いられるとき、次の３つの共同体が存在すると考えることができる。

(a) *発注元メンバだけからなる共同体*
(b) *発注元メンバと外注先メンバの双方からなる共同体*
(c) *外注先メンバだけからなる共同体*

これらの共同体に合わせて、部門ネットワークを次のように３つのセグメントに分割する（図２）。

(a) 発注元メンバだけからなる共同体のための発注元ネットワーク。発注元企業の機密情報はここに保持する。

(b) 発注元メンバと外注先メンバの双方からなる協同体のための協同ネットワーク。協同作業に必要なターゲットマシンなどの設備はここに置く。

(c) 外注先メンバだけから成る共同体のための外注先ネットワーク。外注先企業の機密情報はここに保持する。

これらのセグメント相互間でのセキュリティ制御を次章で述べる。

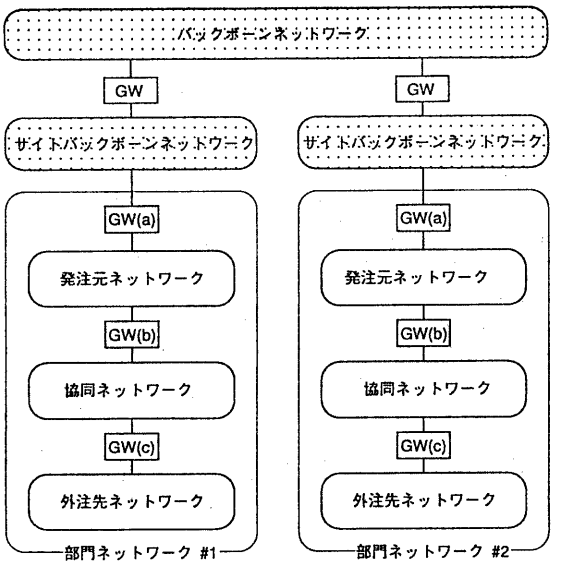

図2 部門ネットワークの分割

3．セキュリティ制御コンセプト

3．1　ネットワーク利用上の要求条件

分散形ソフトウェア開発環境の利用者がネットワークで行いたいこと、および利用上の禁止事項についての要求条件は次のとおりである。

[ネットワークで行いたいこと]

・発注元メンバと外注先メンバとが協同ネットワーク内で相互にコミュニケーションができる。

・三つのセグメントの間でのファイル転送ができる。

・協同ネットワーク内のターゲットマシンに、発注元ネットワークと外注先ネットワークの双方からアクセスできる。

[ネットワーク利用上の禁止事項]

・外注先メンバは、発注元企業が持つ公式ドメイン名による電子メールやニュース（電子掲示板）を利用しない。

・発注元メンバと外注先メンバは、互いの機密情報が保持されている環境にアクセスしない。

3．2　セキュリティ制御条件

3．1で論じた要求条件を満たすために、セキュリティ制御条件を決定する。それらの条件は、次のような3つのタイプの通信に分類される。

・トランスポートレイヤプロトコルでのコネクションによって二点間で情報伝送が行われる直接通信（リモートログイン、ファイル転送など）

・ワークステーションによって情報伝送の中継が行われうる間接通信（電子メール、ニュース）

（1）直接通信のためのセキュリティ制御条件

直接通信のためのセキュリティ制御条件は、図2のネットワークモデルに応じて、表1のように決定される。

表1　直接通信のためのセキュリティ制御条件

通信元＼通信先		部門ネットワーク #1			部門ネットワーク #2		
		発注元	協同	外注先	発注元	協同	外注先
部門ネットワーク #1	発注元	○	○ *1	× *5	○ *6	○ *7	× *10
	協同	× *2	○	○ *4	× *8	○ *9	× *10
	外注先	× *5	○ *3	○	× *10	× *10	× *10
部門ネットワーク #2	発注元	○ *6	○ *7	× *10	○	○ *1	× *5
	協同	× *8	○ *9	× *10	× *2	○	○ *4
	外注先	× *10	× *10	× *10	× *10	○ *3	○

凡例）　発注元：発注元ネットワーク
協同　：協同ネットワーク
外注先：外注先ネットワーク
○　：許可
×　：禁止
＊n　：本文で参照する条件の番号

（2）間接通信のためのセキュリティ制御条件

間接通信のためのセキュリティ制御条件は、表2のように決定される。この条件においては、同一部門ネットワーク内の通信か複数部門ネットワーク間の通信かの区別は無関係である。

4．セキュリティ制御の実現方法

4．1　ゲートウェイの設定によるセキュリティ制御

第3章で論じたセキュリティ制御条件を満たすために、次のように3つのプロトコルレイヤに応じた制御をゲートウェイに設定する。

（1）ネットワークレイヤ制御

図2におけるゲートウェイに、ネットワークレイヤ制御として、次のようにルーティング設定を行う。

・ゲートウェイGW（b）は、発注元ネットワークと協同ネットワークだけのためにパケットをルーティングする。

・ゲートウェイGW（c）は、協同ネットワークと外注先ネットワークだけのためにパケットをルーティングする。

これにより、表1における禁止条件＊5および＊10が満たされる。

（2）トランスポートレイヤ制御

図2におけるゲートウェイに、トランスポートレイヤ制御として、次のようにアクセス制限を設定する。

・ゲートウェイGW（b）は、許可条件＊1および禁止条件＊2のために一方向アクセスに限定する。

・ゲートウェイGW（c）は、許可条件＊3および＊4に基づくアクセスを許可する。

・ゲートウェイGW（a）は、許可条件＊6に基づくアクセスを許可する。

・ゲートウェイGW（b）およびGW（a）は、許可条件＊7および禁止条件＊8のために一方向アクセスに限定する。

・ゲートウェイGW（b）およびGW（a）は、許可条件＊9に基づくアクセスを許可する。

これらにより、表1の各条件が満たされる。

表2　間接通信のためのセキュリティ制御条件

通信元＼通信先	発注元	協同	外注先
発注元	○	× *12	× *12
協同	× *12	○ *11	○ *11
外注先	× *12	○ *11	○ *11

凡例）　発注元：発注元ネットワーク
協同　：協同ネットワーク
外注先：外注先ネットワーク
○　：許可
×　：禁止
＊n　：本文で参照する条件の番号

（3）アプリケーションレイヤ制御

図2におけるゲートウェイGW（b）は、表2における禁止条件＊１２を満たすために、電子メール・ニュース用のパケットを阻止する。

表2における許可条件＊１１に基づく電子メール・ニュース通信は、協同ネットワーク内のワークステーションによる中継で実現できる。

4．2　ルーティング設定の統一性の保証

ゲートウェイによるパケットルーティングの方式としては、ルーティング情報をゲートウェイに固定的に設定するスタティックルーティング方式と、ルーティング情報をゲートウェイが自律的に交換し合うダイナミックルーティング方式がある。

ルーティング設定を4．1（1）で述べたように限定するには、現状のゲートウェイ製品を利用する限りは、ダイナミックルーティング方式よりもスタティックルーティング方式の方が好都合である。しかし、スタティックルーティング方式では、人為的誤りによってゲートウェイ相互間にルーティング情報の矛盾が生じ、通信が不能になることがある。

この問題への対策として、我々はルーティング情報自動生成プログラムを開発した[1]。これは、各ゲートウェイのノードのＩＰアドレス情報からネットワークの全体形状を解析し、これに基づいて全ゲートウェイのルーティング情報を生成するものである。これにより、ルーティング設定の統一性を保証することができる。

4．3　セキュリティ管理作業の分担

大規模なソフトウェア開発環境では、階層的なネットワーク管理分担が必要である。すなわち、2．1で述べた階層的ネットワーク構成においては、次のようにネットワーク管理を分担する。

・**部門ネットワーク管理者**は、部門ネットワーク内のセキュリティを管理する。

・**組織ネットワーク管理者**は、部門ネットワークを統括して、組織ネットワーク内のセキュリティを管理する。

・**企業ネットワーク管理者**は、組織ネットワークを統括して、企業ネットワーク全体のセキュリティを管理する。

このような管理分担により、ネットワーク内のセキュリティ問題に対する迅速な処置が可能になる。

5．おわりに

本稿では、外注先と共用する分散形開発環境のためのネットワーク構成と情報配送制御方式を述べた。

本稿で述べたセキュリティ制御コンセプトは、現実に使えるプロトコルと装置を用いることを前提としたものである。

ＮＴＴでは、3,000ノードを超える全国規模の社内用分散形ソフトウェア開発環境[2]にこのコンセプトを適用し、その有効性を確認している。

今後、ネットワークの拡大、利用の活発化に伴って顕在化することが予想される問題に対処するために、次の項目の検討を進めていく考えである。

(a) 回線コストの低減のために低トラフィック回線に公衆回線（広帯域ＩＳＤＮなど）を導入した場合の、不特定の発呼者からの接続によるセキュリティ侵害の防御策

(b) 特定当事者間の通信の機密保護のための、暗号方式の導入

(c) コンピュータウィルスなどの、ソフトウェア流通を利用した意図的な侵害に対する防御策

[参考文献]

[1] 浅見、田中、福山「ルーティング情報の自動生成方式」電子情報通信学会１９９２年春季大会

[2] 福山、浅見、他「分散形ソフトウェア開発環境の構成方式」NTT R&D Vol.39, 1990