ＮＭＷシステムの安全性強化と
その広域ネットワークサービスへの応用

小野木 渡
91-0908-1
指導教官 木村 泉 教授

平成７年２月６日

目 次

図の一覧

第 1 章

はじめに

コンピュータネットワーク上に存在するサービスを利用する場合、現状では次のような問題がある。

- RTT(Round Trip Time)[1]が大きい場合に、対話的な作業が困難になる。
- 作業中にネットワークが切断されると作業を継続できない。
- 複数のホストからサービスを受けたい場合には、そのサービスをホストごとに複数回利用しなければならない。

そこで、エージェント[2]の考え方を利用して、上記の問題を解決することを考えた。エージェントの考え方を用いたシステムとして、ＮＭＷシステム（Network Management Worm System）[3] が存在するので、それを利用した。

しかし、現在のＮＭＷシステムではセキュリティの面が不十分である。実際ＮＭＷシステムでは、ネットワーク管理用の暗号化方法は提案されている [4] ものの、暗号化するための鍵の配送方法が考えられていない。そこで、一般ユーザが利用すること、および広域ネットワークにおけるサービスに応用することを前提とした暗号化方法および鍵の配送方法を提案する。これを前提として広域ネットワークにおける新サービスへの応用を考える。

---

[1] ネットワーク通信において、１つのパケットが始点から終点へ行き、終点で処理をした後、再び始点へ戻ってくるまでの合計時間のこと。

[2] ユーザから指令された仕事をユーザにかわって行なうプログラム。代理人。

第 2 章

ＮＭＷシステム

この章では、コンピュータネットワークの管理システムとして、木村・大野研究室修士２年の清水により開発されたＮＭＷシステムの概要について説明する [7]。

2.1 ネットワーク管理とＮＭＷシステム

従来のコンピュータネットワーク管理手法としては、実際に管理対象機器にリモートログインして対話形式で操作する方法、SNMP[1] による管理情報の取得、設定、操作を行なう方法などがある。これらの方法では、ネットワーク管理モデル [2] で説明されているように、コンピュータネットワークの管理を、それ自身を介して行なっているため、ネットワークに障害が起きた場合、障害が起きたこと自体はわかるが、その時点におけるネットワーク全体の状況を取得したり、ネットワークを制御したりすることが出来なくなるからである。さらに、この程のネットワーク管理方法ではネットワークの規模が大きく複雑になるにつれて、管理者への負担の増加が問題になってくる。

そこで、ネットワークワーム（以下ワームと略記する）を用いることにより、ネットワーク障害に強いネットワーク管理システムとしてＮＭＷシステム（Network Management Worm System）が、提案・開発された [3]。ＮＭＷシステムはネットワーク上を移動しながらの調査、分析、制御をする能力を持ち、さらに作業中にネットワークに障害が起きた場合にも復旧するまで待機していたり、なんらかの方法で管理者に障害が起こったことを報告したりする機能も持っている。

2.2 ＮＭＷシステムの仕組み

ＮＭＷシステムは、ワームとワーム支援系とから構成される。ワームとはプログラムの一種である。ＮＭＷシステムにおいては、ワームはワーム支援系によりホスト間を移動し、作業を行なうのである。ワーム支援系は以下の３つからなる。

- wsd:ワーム支援デーモン。ワーム、制御メッセージの配送などホスト間の通信を行い、owl を制御する。
- owl:ワーム実行インタプリタ。ワームを解釈、実行するインタプリタ。
- wormc:ワーム制御インタフェース。ワームを制御するためのユーザインタフェース。

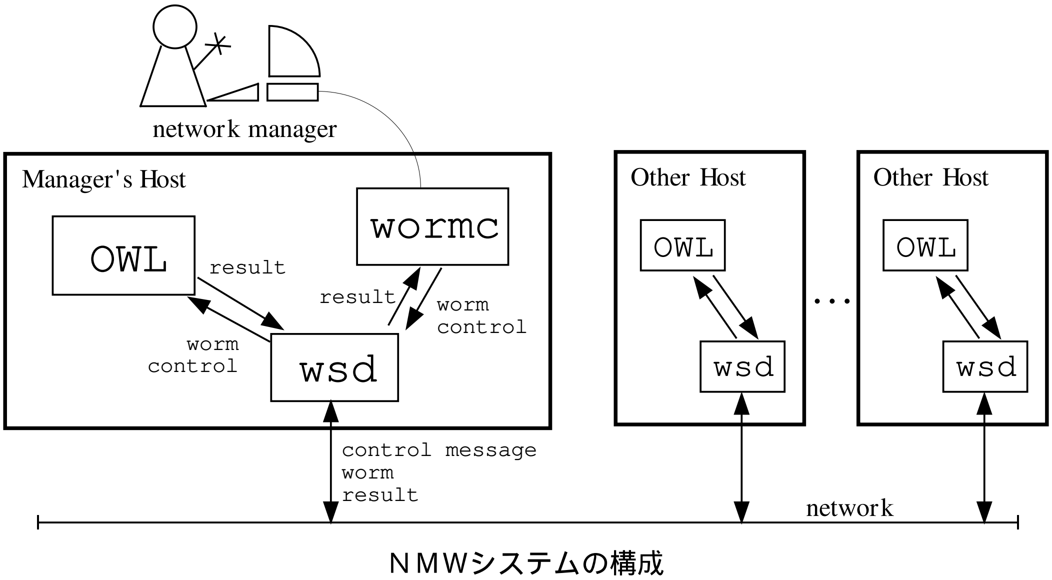


図 2.1 ＮＭＷシステムの仕組み（清水亮博氏の許可により掲載）

2.3 WIDE/PhoneShell との協調

ネットワーク管理システムにおいて、ネットワーク障害が起きた際にそのことを管理者に報告する機能は重要である。しかし、ネットワークを通じて報告するのでは、その通信路に障害が起きた場合に報告が困難となる。ＮＭＷシステムでは WIDE/PhoneShell[2] と協調することによりその問題を解決した。

WIDE/PhoneShell は、ネットワークに直接アクセスできない環境にいる管理者が、公衆電話網における資源、例えば電話回線、FAX、ページャ等を利用することにより、ネットワーク管理を実施するための手法、およびそれを実現するための機構である。

ＮＭＷシステムは、障害が起きたことを報告する際コンピュータネットワークが利用できない場合には、FAX やページャ等を利用して管理者に報告する。

2.4 ＮＭＷシステムの特徴

ＮＭＷシステムの特徴として以下の事柄を挙げることが出来る。

- ネットワークに事故が起きた場合に強い。
- セキュリティが確保されている。
- RTT(Round Trip Time) を気にせずに作業ができる。
- 利用者を端末の前に拘束する時間が少ない。

これらの特徴を利用することによりネットワーク管理において管理者の負担を軽減することが可能である。このような特徴を利用することはネットワーク管理だけでなく、ネットワークの利用全般においても有効であると考えられる。そこで、ＮＭＷシステムをネットワーク管理以外の広域ネットワークにおけるサービスに応用することを考える。

第 3 章

ＮＭＷシステムの安全性強化

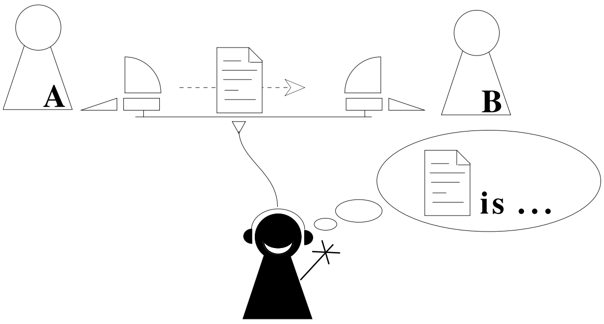
この章では、ネットワーク通信におけるセキュリティおよび暗号化方式について述べた上で、ＮＭＷシステムの安全性強化方法について論じる。

3.1 ネットワーク通信におけるセキュリティ

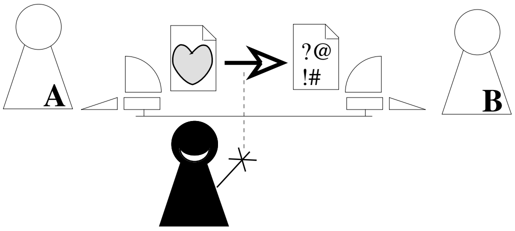
広域ネットワークにおける通信では、通信路の途中において通信の盗聴やパケットの改竄等を行なうことが決して不可能ではない。また、通信路および通信路上のホストは、必ずしも安全で信頼できるものであるとは言えない。したがって、ネットワークを介して通信を行なうアプリケーションではセキュリティが問題である。一般にネットワークを介した通信におけるセキュリティへの脅威としては以下の 3 つがある（図 3.1）。

- 盗聴 :ネットワークに流れているパケットの中身を覗き通信の内容を盗み見ること。
- 改竄 :通信を行なっているネットワークの途中で通信の内容を書き換えること。
- なりすまし :他人になりすまして通信を行なうこと。

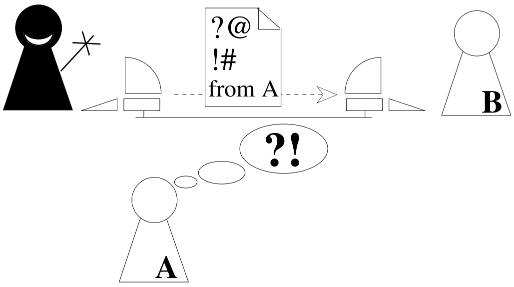
ネットワーク通信をともなうアプリケーションの中には、このような不正行為への対策をほどこしたものがいくつかある。例えばネットワークを利用したアプリケーションとして広く使われている電子メールにも、安全性を考慮した PEM （Privacy Enhanced Mail）[RFC1421,1422,1423,1424] が提案され、現在いくつかの実装が公開されている。PEM では盗聴、改竄、なりすましを防止するために公開鍵暗号方式による暗号化、電子署名を用いている。また、Internet Protocol(IP) のパケットのボディー部を暗号化することにより拡張した IP/Secure[5] などもある。



通信の内容が盗聴されている。



通信の内容が改竄されている。



他人になりすまされている。

図 3.1 ネットワーク通信における脅威 (清水亮博氏の許可により掲載)

3.2 暗号化方式

暗号化の手法を、秘密鍵暗号方式と公開鍵暗号方式の 2 つに分類することができる [6]。ここでは、この 2 つを説明し、公開鍵暗号方式による電子署名についても説明する。

3.2.1 秘密鍵暗号方式

秘密鍵暗号方式は暗号化、復号化に同じ鍵を用いる方式で、送信者と受信者とが同じ鍵を秘密に共有し通信を行なう。この方法では、鍵を第三者に盗まれると、その第三者は通信の内容を解読することが可能となる。そのため、鍵を共有するための鍵の配送を安全に行わなければならないが、その方法が難しく、多くの場合問題となる。また、複数の人とそれぞれ秘密に通信を行いたい場合には、異なる鍵をそれぞれの通信相手と共有する必要

がある（図 3.2）。そのため、人数が多くなると秘密に保持する鍵の数が大きくなる。

秘密鍵暗号方式の代表例としては、データ暗号化規格（Data Encrypion Standard, 略称 DES）がある。DES は、米国商務省標準局が行なったコンピュータデータの暗号化方式の公募に対して、IBM 社が提案し 1977 年に公布された方式である。

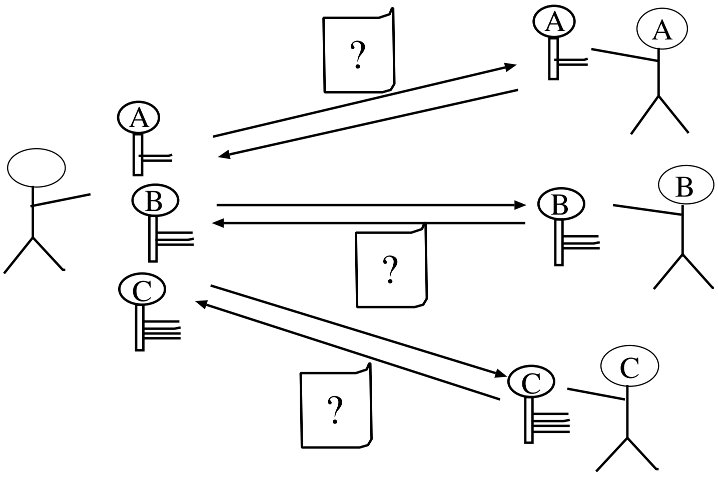


図 3.2 秘密鍵暗号方式

3.2.2 公開鍵暗号方式

公開鍵暗号方式は暗号化と復号化に異なる鍵を用いる方法で、暗号化の鍵を公開（この鍵を公開鍵と呼ぶ）し、復号化の鍵は受信者が秘密に持つ（この鍵を秘密鍵と呼ぶ）ことにより秘密通信を行う。このとき、公開鍵から秘密鍵を推定することが困難であるようにする。そのため、公開鍵を第三者が手に入れたとしても、通信の内容を解読することは出来ない。また、複数の人と秘密に通信を行なう場合には、それぞれの相手に同じ公開鍵を渡せば良い。

公開鍵暗号方式を具体的なアルゴリズムにしたもののうち、現在もっとも有力であると言われているものが、RSA 公開鍵暗号である（RSA は、発明した Rivest、Shamir、Adleman の 3 人の名前からついている）。RSA 公開鍵暗号の基本原理は非常に大きな（100 桁以上）異なる 2 つの素数の積を計算するのは容易であるが、その積を素因数分解し、元の素数を求めるのは計算量的に難しいというものである。

3.2.3 電子署名

手紙を書くとき、クレジットカードで買い物をするときなどには、自分の名前を書きその筆跡により本人であることを確かめる。それと同じように通信文の送信者が正しいかどうかを検査する認証と呼ばれる機能がある。認証は、送信者が通信文に署名をし、受信者

がその署名を検査して通信文が確かに送信者からのものかどうかを確認することで行なわれる。特に、電子通信において行われる署名は電子署名と呼ばれている。

公開鍵暗号における電子署名は、送信者が自分のみが知っている秘密鍵で署名（暗号化）する。そのため秘密鍵を知らない他の誰も同じ署名を作ることが出来ないので偽造することは不可能であり、送信者の公開鍵を知っている受信者はその署名（暗号化された文）を復号化することによって通信文が送信者からのものであることを確認できる。

3.3　ＮＭＷシステムに対する脅威

ＮＭＷシステムはネットワーク通信をともなうシステムであるので、前節にあるようにセキュリティを考える必要がある。前節にあるようにセキュリティとしては盗聴、改竄、なりすましの３つに対する対策が必要であるが、ＮＭＷシステムにおけるセキュリティとしては、改竄・なりすまし対策の２つが特に重要である。その理由としては以下の事柄が挙げられる。

- ワーム本体や、実行結果の報告等を改竄されると、誤った情報を得ることになる。さらに、管理者がその情報を信じてしまうと正しい（管理等の）作業を行うことが不可能になる。
- ワームの発信者になりすまされると、不正ユーザにＮＭＷシステムの実行権限を与えてしまうことになる。

主なネットワークセキュリティにはもう一つ、盗聴対策がある。ＮＭＷシステムの本来の目的であるネットワーク管理に限ってみた場合には、管理対象のネットワークは限られており、その管理作業を盗み見て得られる情報の大部分がそのネットワークにアカウントを持つユーザならいつでも知ることの出来るものであると考えられるので、管理域内での盗聴はそれほど問題ではないとすることも出来る。しかし、ＮＭＷシステムの利用方針によっては一般ユーザに公開していない情報（例えば/etc/master.passwd 等）を扱う事も考えられるので、場合によっては盗聴対策も必要となる。管理域外で盗聴されるのは重大な問題となるが、管理用ワームは管理域外に出ていかない（管理域外に出て管理作業を行なうことはない）ので、管理域外で盗聴されることはない。

ＮＭＷシステムを広域ネットワークサービスに応用することを考えた場合には、盗聴対策は重要になる。この場合、通信の内容（ワームの中身）は利用者のプライバシーとなるので、通信内容の秘密を保証する必要がある。

3.4　ＮＭＷシステムのセキュリティ対策方法

盗聴、改竄、なりすまし対策、つまりＮＭＷシステムのセキュリティ強化として、ＮＭＷシステムの暗号化を清水氏が提案している [4]。

現在ＮＭＷシステムで提案されているものは、公開鍵暗号方式を用いてワームの暗号化および認証を行なう方法である。公開鍵暗号方式をもちいた暗号化方法のなかでも、その方法を具体的なアルゴリズムにしたRSA公開鍵暗号を用いることが提案されている。

3.5　ＮＭＷシステムの暗号化

3.5.1　記号の定義

最初にこの節で用いる記号を定義する。

W	ワーム本体
a	ユーザＡの識別子（証明書）
K_a^s	ユーザＡの秘密鍵
K_a^p	ユーザＡの公開鍵
K_i^s	ホストiにおけるwsdの秘密鍵
K_i^p	ホストiにおける公開鍵
K_W	ワームが運ぶ情報を暗号化するための秘密鍵方式による鍵(DES鍵)
R_i	ホストiで得られた実行結果
I_i	ホストiにある情報（資源、公開鍵等。場合によってはR_iも含む）
$\xrightarrow{K_W}$	鍵（K_W）で暗号化する
$[I_1]K_W$	鍵（K_W）で暗号化されたI_1
$\xrightarrow{+a}$	ワームにaを追加する
$\{...\}$	１匹のワーム

3.5.2　ＮＭＷシステムの暗号化方法

通常の公開鍵暗号方式による秘密通信では、通信相手の公開鍵で暗号化して送るので、複数のホストを回って作業を行うＮＭＷシステムにそのまま用いることが出来ない。そこでＮＭＷシステムでは、送信者の秘密鍵でワームを暗号化したものを送るという方法を考える。この方法では、各ホストが送信者の公開鍵を知っていればワームを復号化することができ、暗号化されているワームをそのまま次のホストに送ることにより複数のホストを回ることが可能になる。

この方法によれば、送信者の秘密鍵により暗号化が行なわれるため、ワームの改竄や送信者になりすましてワームを送り実行することへの防止ができる。

ここでは、ワームの発信者Ａがホスト１・ホスト２で作業するワーム(W)を実行する場合を例にして、ＮＭＷシステムにおける暗号化方法を３通り説明する。

方法１

1. 発信者ＡはK_Wを作成し、ワーム(W), Ａの識別子(a)と共にＡの秘密鍵K_a^sで暗号化し、平文のaを付けてホスト１へ送る。

$$a, W, K_W \xrightarrow{K_a^s} [a, W, K_W]K_a^s \xrightarrow{+a} \{a, [a, W, K_W]K_a^s\}$$

2. ホスト１のwsdは、平文aをみて公開鍵K_a^pを選びワームを復号化する。平文のaと中身のaとが一致する場合にWを実行する。実行して得た結果(R_1)をＡの公開鍵で暗号化してＡに送る。

$$\{a, [a, W, K_W]K_a^s\} \xrightarrow{K_a^p} a, a, W, K_W$$
$$R_1 \xrightarrow{K_a^p} \{[R_1]K_a^p\}$$

3. ホスト２へ送る情報がホスト１に存在する場合にはその情報(I_1)をワームの中に入っていた鍵(K_W)で暗号化し、Ａから来たワームに付加してホスト２へ送る。

$$I_1 \xrightarrow{K_W} [I_1]K_W$$
$$\{\{a, [a, W, K_W]K_a^s\}, \{[I_1]K_W\}\}$$

4. ホスト２のwsdもホスト１と同様にＡが送ったワームを復号化・実行・得た結果の報告を行う。

$$\{a, [a, W, K_W]K_a^s\} \xrightarrow{K_a^p} a, a, W, K_W$$
$$R_2 \xrightarrow{K_a^p} \{[R_2]K_a^p\}$$

5. ホスト１で付加された情報がある場合にはワームの中に入っていた鍵(K_W)で復号化し取り出す。さらに他のホストへ送る情報が存在する場合にはその情報(I_2)を再びK_Wで暗号化し送る。

$$[I_1]K_W \xrightarrow{K_W} I_1$$
$$I_1, I_2 \xrightarrow{K_W} [I_1, I_2]K_W$$

方法 2

1. 発信者 A はワーム （W）を作り自分の識別子 (a) と共に秘密鍵 (K_a^s) で暗号化し、平文の a を付けてホスト 1 へ送る。

$$a, W \xrightarrow{K_a^s} [a, W]K_a^s \xrightarrow{+a} \{a, [a, W]K_a^s\}$$

2. ホスト 1 の wsd は、平文 a をみて公開鍵 K_a^pを選びワームを復号化する。平文の a と中身の a とが一致する場合に W を実行する。実行して得た結果 (R_1) を A の公開鍵で暗号化して A に送る。

$$\{a, [a, W]K_a^s\} \xrightarrow{K_a^p} a, a, W$$
$$R_1 \xrightarrow{K_a^p} \{[R_1]K_a^p\}$$

3. ホスト 2 へ送る情報がホスト 1 に存在する場合にはその情報 (I_1) を自分の秘密鍵 (K_1^s) で暗号化し、ユーザ A から来たワームと一緒にホスト 2 へ送る。

$$I_1 \xrightarrow{K_1^s} [I_1]K_1^s$$
$$\{\{a, [a, W]K_a^s\}, \{[I_1]K_1^s\}\}$$

4. ホスト 2 の wsd もホスト 1 と同様にユーザ A の作ったワームを復号化し、実行し、得た結果を暗号化して報告を行う。

$$\{a, [a, W]K_a^s\} \xrightarrow{K_a^p} a, a, W$$
$$R_2 \xrightarrow{K_a^p} \{[R_2]K_a^p\}$$

5. ホスト 1 で付加された情報がある場合にはホスト 1 の公開鍵 (K_1^p) で復号化し取り出す。さらに他のホストへ送る情報 (I_2) が存在する場合にはそれをを自分の秘密鍵 (K_2^s) で暗号化し送る。

$$[I_1]K_1^s \xrightarrow{K_1^p} I_1$$
$$I_2 \xrightarrow{K_2^s} [I_2]K_2^s$$
$$\{\{a, [a, W]K_a^s\}, \{[I_1]K_1^s\}, \{[I_2]K_2^s\}\}$$

方法 3

1. 発信者 A はワーム (W) を作り自分の識別子 (a) と共に秘密鍵 (K_a^s) で暗号化し、平文の a を付けてホスト 1 へ送る。

$$a, W \xrightarrow{K_a^s} [a, W]K_a^s \xrightarrow{+a} \{a, [a, W]K_a^s\}$$

2. ホスト 1 の wsd は、平文 a をみて公開鍵 K_a^pを選びワームを復号化する。平文の a と中身の a とが一致する場合に W を実行する。実行して得た結果 (R_1) を A の公開鍵で暗号化して A に送る。

$$\{a, [a, W]K_a^s\} \xrightarrow{K_a^p} a, a, W$$
$$R_1 \xrightarrow{K_a^p} \{[R_1]K_a^p\}$$

3. ホスト 2 へ送る情報がホスト 1 に存在する場合にはその情報 (I_1) をホスト 2 の公開鍵 (K_2^p) で暗号化し、ユーザ A から来たワームと一緒にホスト 2 へ送る。

$$I_1 \xrightarrow{K_2^p} [I_1]K_2^p$$
$$\{\{a, [a, W]K_a^s\}, \{[I_1]K_2^p\}\}$$

4. ホスト 2 の wsd もホスト 1 と同様にユーザ A の作 ったワームを復号化し、実行し、得た結果を暗号化して報告を行う。

$$\{a, [a, W]K_a^s\} \xrightarrow{K_a^p} a, a, W$$
$$R_2 \xrightarrow{K_a^p} \{[R_2]K_a^p\}$$

5. ホスト 1 で付加された情報がある場合には自分の秘密鍵 (K_2^s) で復号化し取り出す。さらに他のホスト 3 へ送る情報が存在する場合にはそれををホスト 3 の公開鍵 (K_3^p) で暗号化し送る。

$$[I_1]K_2^p \xrightarrow{K_2^s} I_1$$
$$I_1, I_2 \xrightarrow{K_3^p} [I_1, I_2]K_3^p$$
$$\{\{a, [a, W]K_a^s\}, \{[I_1, I_2]K_3^p\}\}$$

3.5.3 公開鍵の配送（取り寄せ）方法

ここでは、ワームを暗号化、復号化するために必要な公開鍵の配送方法についてネットワークサービス用とネットワーク管理用の２通りの場合に分けて述べる。

ネットワークサービス用ＮＭＷシステムの場合

- PEM(Privacy Enhanced Mail) で用いられている方法を利用する。つまり、ＮＭＷシステムを利用するユーザの公開鍵の登録、ユーザの証明書の発行、公開鍵の配布等を行う公証人ホストを用意する。ユーザは自分の秘密鍵・公開鍵の対を作成し、既に登録されているユーザ等に署名してもらうことにより公証人ホストに公開鍵を登録し、証明書を得ることが出来る。各 wsd(2.2 節) では、ユーザの秘密鍵で暗号化されたワームを復号化するためにユーザの公開鍵を公証人ホスト（配布局）から取り寄せる。そのユーザの公開鍵が公証人ホストに存在しない場合は、管理者とユーザにその旨を報告し、送られてきたワームを捨てる。公証人ホストと通信できない場合にはユーザにその旨を連絡し、通信できるまで待つか、送られてきたワームを捨てるかする。この方式は方法１～３の全てで有効である。
- 方法２、３の場合、各 wsd の公開鍵もインストールの際に管理者の署名で公証人ホストに登録しておくことにより、ユーザの公開鍵と同様に取り寄せることが可能になる。
- 上記のいずれの方法も鍵を新しく更新した場合には管理者もしくは wsd 自身が公証人ホストに届ればよい。

ネットワーク管理用ＮＭＷシステムの場合

管理用のワームに付加されている情報を暗号化・復号化するための公開鍵や管理者の公開鍵を必要なときに公証人ホストから取り寄せるという方法は、ＮＭＷシステムがネットワーク障害に強い管理システムとして考案された事を考えると、必ず公証人ホストと通信出来るという保証がない場合には用いることは出来ない。そのため別途方法を考える必要がある。

- 管理者の公開鍵

  管理者の人数は限られている。また管理者用の共通のアカウントを利用すれば鍵は１つで済む。つまり、管理者の鍵の数は少ないと考えられる。そのため、管理者の公開鍵を管理対象の全ホストがあらかじめ保持していることにしても問題はない。この場合は、wsd をインストールする時に管理者の公開鍵も一緒にインストールすれば良い。

- 各 wsd の公開鍵
  - 管理対象の全ホストの公開鍵を管理対象の wsd が常に持っている場合。

  - 管理対象の全ホストの公開鍵を持っていれば取り寄せる必要がなくなる。
  - 管理対象のホスト数が多くなると鍵の数も多くなってしまうので、規模の大きなネットワークを管理するには不適当である。
  - 鍵の更新時、wsd のインストール時に、全ての wsd に公開鍵を安全に配送しなければならない。管理者が全てのホストに手で (ディスク等で) 配って回るか、安全に鍵を配送できるシステムを作る必要がある。

- 各 wsd は隣接ホスト[1]の wsd の公開鍵を知っているものとする。その上で、ワームが自由に行き来することが可能な方法、または復号化・暗号化に必要な公開鍵を持っていない場合でも常に取り寄せることが可能な方法を考える。
  - ワームの移動を隣接ホストに限定すると、wsd は、隣接ホストの wsd の公開鍵を知っているので、取り寄せる必要が無くなる。また、wsd のインストール時、鍵の更新時は作成した公開鍵を同じサブネット内のホストに対して管理者が署名をして送れば良い。
  - ワームが到着出来たとすれば、出発したホストとの通信路が確保されていると考えられるので、その時点でのルーティングテーブルを参照して、隣接ホストグループに出発したホストの公開鍵を知らないか尋ね、知らない場合には、聞かれたホストが別の隣接ホストグループに所属している場合時には再びそちらの隣接ホストグループに尋ねる。隣接ホスト間の鍵の配送は、送り先の公開鍵で暗号化して送ることによって安全に渡すことが出来る。
  - 上記 2 つの方法でも、サブネット内のホスト数が大きくなると記憶しておく鍵の数が増えてしまうことがある。

---

[1] wsd が存在するホストで、そのホストに至るまでの経路上に別に wsd の存在するホストがないもの。例えば、同じサブネット上で wsd の存在するホスト同士は隣接ホストとなる。

第 4 章

ＮＭＷシステムによる一般ユーザ向けサービス

この章では、暗号化によりセキュリティの強化されたＮＭＷシステムを広域ネットワークにおける一般ユーザ向けのサービスへ応用することについて述べる。

4.1 従来のネットワークサービス

従来からあるネットワークサービスの例としてファイル転送サービスおよび遠隔地ログインの2つを取り上げ、その特徴を述べる。

4.1.1 ファイル転送サービス

ファイル転送サービスに関係あるもとして、FTP、anonymous FTP、Archieを挙げることができる。

FTP(File Transfer Protocol)とは、ネットワーク上のホスト間でファイルの転送を行なうためのプロトコルのことである。そのプロトコルに従い実際にファイル転送を行なうのがftpというアプリケーションである。anonymous FTP（匿名FTP）は、anonymous、ftpの名前を用いることによって誰でもftpを実行できるようにしたサービスで、フリーウェアやドキュメントファイルの公開などに利用されている。anonymous FTP利用者は、FTPサーバに設定された制限の中で自由にファイルにアクセスができ、必要なファイルを取得することができる。Archieは、anonymous FTPサーバが所有するファイルの一覧表をキーワードで検索するシステムである。

これらはネットワーク上に公開されている資源の中から必要な情報を探し、取ってくるサービスである。自分の欲しい情報がネットワーク上のどこに存在するかわからない場合には、Archie等を用いて探すことになるが、必ずしもその情報が見つかるとは限らない。また、たとえ見つけることが出来たとしても、見つかるまでに長い時間がかかったり、見つけた場所がネットワーク的に非常に遠い所であったり、そこに至る経路中に非常に伝送

速度の遅い回線があったりすると、目的の情報を確実に得ることが難しくなってしまう。

4.1.2 遠隔地ログイン

遠隔地にあるホストにログインするには、主にTELNET、rloginの2つの方法がある。TELNETはInternetの標準的な端末エミュレーションプロトコルであり、TELNETプロトコルへのユーザインタフェースとしてtelnetがある。rloginは多くのUNIXシステムで提供されている端末エミュレーションプログラムである。

しかし、遠隔地にあるホストへログインする際には、トラストホストにログインする場合[1]を除いて、パスワードが必要となる。この際、パスワードは平文のままネットワークを流れてしまうため、通信路上で盗聴されると簡単にパスワードが盗まれることになってしまう。

また、ネットワークが混んでいる、回線の伝送速度が遅い、等の理由によりRTTが大きくなると作業が困難になってしまう。

4.2 ＮＭＷシステムのネットワークサービスへの応用

前節で述べたように従来のネットワークサービスにはいくつかの問題点がある。ＮＭＷシステムを利用することによりその問題点を解消したサービスや、ＮＭＷシステムの特徴を生かしたサービスを提供できる。

4.2.1 ＮＭＷシステムの利用

第2章で述べたＮＭＷシステムの持つ特徴は、以下のようにサービスに応用することができる。

- ネットワーク障害が起きた場合に強い。

  ＮＭＷシステムはネットワーク障害に強いネットワーク管理システムとして設計・開発された。そのためサービスの途中でネットワークに障害が起きた場合に、その場で待機し障害が回復してからサービスを続行したり、障害が起きたことを利用者に知らせるなど、状況に応じた処置を取ることができる。

- セキュリティが確保されている。

  暗号化によってセキュリティが強化されているため、ネットワークセキュリティの高いサービスを提供できる。また、ユーザ認証機能を生かしたサービスも提供できる。

- RTT(Round Trip Time)を気にせずに作業ができる。

---

[1] バークレーUNIXシステムにおいて、あるホストが別のホストをトラスト（信用）していれば、両ホストで同じユーザ名を持つユーザは、パスワード無しで互いにログインすることが出来る。

遠隔地にあるホストで作業する場合でも、ワームをローカルホストで作成することができるため、RTT を気にする必要がない。

- 利用者を拘束する時間が少ない。

  対話形式のサービスと違い、ワームを発信した後は別の作業をしたり、端末から離れたりすることができる。

4.2.2 ネットワークサービスを行うワーム

実際にどのようなサービスに応用できるかを述べる。

遠隔地ログインに代わるサービス

自分の所属するネットワークの外にあるホストからＮＭＷシステムを用いてワームに作業をさせる事を考える。ＮＭＷシステムの特徴により、ネットワーク通信におけるセキュリティへの脅威や、遅延時間にとらわれず作業できることになる。このサービスは、ＮＭＷシステムの運用方針によって、telnet するのと同じだけの作業をできるようにしたり、ある程度できることを制限したりすることができる。

ファイル転送を行なうサービス

ファイルの転送をワームを用いて行なう。例えば、回線の伝送速度が遅い、ネットワークが混んでいる等の理由で FTP が困難であるような FTP サイトからファイルを取ってきたい場合にワームを利用する。ＮＭＷシステムではネットワークの状態を調べながらワームを制御できるので、ワームの移動が困難なときには待機させるなどして、確実にファイルの転送を行なうことが出来る。

その他のサービス

- メールの読み書きを行なうワーム。

  旅行先や出張先からメールを読み書きしたいことがある。その際、その場に telnet 端末があるとは限らない。そこで、携帯端末を用いて公衆電話やホテルの電話等にモデムをつなげて電話回線を通してログインすることがある。その場合、ログインしたままの作業では、RTT が気になる、電話の前に拘束される、など不便な面ある。メールの読み書きをワームを利用して行なうと、それらの問題が解決できる。

第 5 章

評価と考察

5.1　ＮＭＷシステムの安全性強化

3.5 節で示したＮＭＷシステムの暗号化の評価として、通信路におけるセキュリティの脅威（盗聴、改竄、なりすまし）に対する有効性、ユーザの暗号化鍵が盗まれた場合、各ホストにおける wsd のセキュリティが破られた場合について述べる。

5.1.1　通信路上に脅威がある場合

ワーム本体の暗号化を発信者の秘密鍵で暗号化するため、ワーム本体の改竄と、他人になりすましてのＮＭＷシステムの使用は防ぐことが可能となった。また、秘密鍵で暗号化するため公開鍵を盗まれなければ盗聴も防ぐことが出来る。

実行結果、ワームが運ぶ情報については、送り先の公開鍵で暗号化する事が出来るため、盗聴、改竄を防ぐことができ、電子署名を施すことによりなりすましも防止できる。

5.1.2　ホストセキュリティが破られた場合

- ユーザの秘密鍵が盗まれた場合

  秘密鍵が盗まれた場合には、盗まれたユーザになりすますことが可能になってしまうので、そのユーザがＮＭＷシステムを用いて実行できる全ての機能を利用されてしまう。

- ホスト (wsd) の鍵が盗まれた場合。

  wsd の公開鍵、秘密鍵が盗まれた場合、そのホストに来たワームは盗聴されてしまうが、ワーム本体がユーザの秘密鍵で暗号化されているのでワームの改竄、各ユーザへのなりすましはできない。ただし、ワームの実行結果、他の wsd へ送る情報については改竄されてしまう。

5.1.3 ユーザの公開鍵が盗まれた場合

- 公開鍵が盗まれた場合

  公開鍵が盗まれた場合には、盗まれたユーザの発信したワームが盗聴されてしまうが、ワームの改竄やなりすましをされることはない。また、実行結果については公開鍵を盗まれても影響はない。

5.2 今後の展開

ＮＭＷシステムを一般ユーザへのサービスに応用するために、ＮＭＷシステムのセキュリティ強化、公開鍵の配送方法の確立が必要であった。そのための方法を本論文で述べたが、現在、まだその実装は終了していない。

今後はＮＭＷシステムのセキュリティ強化の実装を行ない、どの程度セキュリティが向上したのか、それが実行速度にどの程度影響するのか等の評価をしていく。また、清水氏の提案した現在の暗号化方法[4]では公開鍵が盗まれた場合に盗聴を許してしまうが、一般ユーザへのサービスへ応用する場合にそれで良いかどうかを検討していく必要がある。

また、その上で4.2節にあるようなサービスへ応用し、従来までのサービスと比較してその性能の評価を行なう。

第6章

謝辞

日頃からたいへん熱心に御指導をいただいた木村 泉教授、大野 浩之講師に深く感謝いたします。

色々な面でお世話になりました、木村研究室の先輩方、Titanet 運用センターの新美 誠さんに感謝いたします。

また、面倒を見て下さいましたＮＭＷシステムの開発者である清水 亮博先輩に感謝いたします。

参考文献

[1] Jeffrey D. Case, Mark S. Fedor, Martin L. Schoffstall, and James R. Davin. A Simple Network Management Protocol (SNMP). Request for Comments 1157, May 1990.

[2] Hiroyuki Ohno. Improved Network Management using WIDE/PhoneShell. In *Proceedings of INET '93*, 1993.

[3] 清水亮博. 寄生プログラム (ネットワークワーム) を用いたコンピュータネットワークの管理方式. 平成4年度卒業論文, 東京工業大学理学部情報科学科, February 1993.

[4] 清水亮博, 大野浩之. ネットワークワームを利用したネットワーク管理システムのためのセキュリティ向上手法. 第49回 (平成6年度後期) 全国大会 講演論文集 (1). 情報処理学会, September 1994.

[5] Y.Shinoda T.Tanida. IP/Secure: Providing Security on Datagram Delivery for Mobile Host Environment. In *Proceedings of INET'94*, 1994.

[6] 池野信一, 小山謙二. 現代暗号理論. 電子情報通信学会, 1986.

[7] 清水亮博. ワームによるコンピュータネットワーク管理システムの資源探索機構およびセキュリティ機構. 平成6年度修士論文, 東京工業大学大学院理工学研究科, 1995.