# Xen 上のドメイン間における covert timing channel の評価

岡 村 圭 祐† 大 山 恵 弘†

## 1. はじめに

悪意をもったプロセスにより、本来通信路として意図されていない媒体を用いて通信を行われる、covert channel 通信問題が古くから指摘されている 1)。この通信を行われると、正規の通信路のみ監視を行っていても情報の漏出を完全に防ぐことができなくなる。

計算機内のすべての共有資源は、covert channel として悪用される危険性がある。その代表的な共有資源として、CPU が挙げられる。特にシングルプロセッサの場合、計算機内のすべてのプロセスが共有することになるだろう。このとき、CPU による計算時間の長短を有意味な情報と解釈することで、管理者や監視プログラムなどに気付かれずにプロセス間通信が行われてしまうことになる。また、このようなイベントのタイミングを用いた covert channel のことを、特に covert timing channel と呼ぶ。

Xen 仮想マシンモニタ上にある各ドメインも、実 CPU を共有している状態にある。そこで本研究では、Xen 上のドメイン間において covert timing channel 通信を行うシステムを構築し、その通信の評価を行うことで、ドメイン間にまたがる covert channel がどの程度深刻な脅威となりうるのか指摘する。

## 2. 作成する covert timing chanel の概要

1 ビットの送信方法について以下に述べる。まず、receiver となるドメインは、sender となるドメインが CPU に負荷をかけるような処理を何も実行していないときに計算プログラムの計算時間を計っておき、これを基準時間として記憶しておく。続いて、sender と receiver 間においてあらかじめ示し合わされた通信開始時刻となったら、receiver は基準時間を測定したプログラムと同じプログラムの計算を開始する。同時に、sender はビット 1 を送信したい場合は CPU 負荷がかかるような処理をしばらく行う。ビット 0 を送信したい場合は引き続き CPU に負荷をかけない。最後に

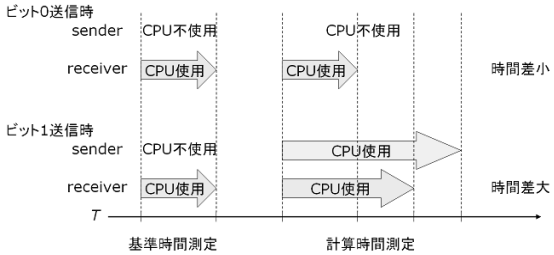


**図 1** covert timing channel の手法

receiver は、通信時のプログラムの計算時間と基準時間の比較をする (図 1)。これら 2 つの時間差が小さいとき、通信時に sender は CPU 負荷をかけていなかった、と考えられる。そこで、時間差が小さいときにはビット 0 を受信したとみなす。反対に、時間差が大きかったとき、通信時に sender は CPU 負荷をかけていたと考えられるので、ビット 1 を受信したとみなすことができる。

同様に、通信開始時刻を細かく区切り逐次的に何度も行うことで、2 ビット以上の情報も送信できると考えられる。

## 3. 現状と今後

現在、通信の主体となるドメインのみが存在する環境内において、CPU 負荷の有無を判定しビット情報として解釈するシステムを作成した。このシステムはドメイン U のユーザ空間上で動作するものであり、Xen やドメインのカーネルソースを変更する必要はない。

今後は、一般的な環境、例えば他のドメインやプロセスが稼動しているような環境で、どの程度の通信速度ならば通信の精度を損なわないか調査していく。また、現在のあらかじめ時刻を定めておく方法以外の通信開始手法を検討し、通信を手軽に行えるようにしたいと考えている。

## 参 考 文 献

1) B. Lampson: A Note on the Confinement Problem. *Communication of the ACM*, 16(10):613-615, October 1973.

† 電気通信大学 電気通信学部 情報工学科