令和 2 年度 卒業論文概要			
所　　属	機械情報工学科	指導教員	光來 健一
学生番号	17237061	学生氏名	堀尾 周平
論文題目	複数ホストにまたがる仮想マシンの選択的なメモリ暗号化		

1　はじめに

近年，大容量メモリを持つ仮想マシン（VM）が利用されるようになってきている．VM はマイグレーションと呼ばれる技術によりホストのメンテナンス時などに別のホストに移動させることができるが，大容量メモリを持つ VM の場合は十分なメモリを持つ移送先ホストを常に確保できるとは限らない．そこで，VM のメモリを分割して複数の小さなホストに転送する分割マイグレーション [1] が提案されている．分割マイグレーション後には必要とされたメモリデータをホスト間で交換するリモートページングを行いながら VM が動作する．しかし，実行環境によっては分割マイグレーションやリモートページングの際にメモリデータを盗聴される危険性がある．メモリデータは暗号化することによって保護することができるが，暗号化のオーバヘッドにより性能が大幅に低下する．先行研究 [2] では暗号化・復号化を最適化することにより性能を改善しているが，限定的かつ不完全な実装にとどまっていた．

本研究では，分割マイグレーションとリモートページングにおいて，VM 内の様々な情報を用いた選択的なメモリ暗号化を行う SEmigrate を提案する．

2　複数ホストにまたがる VM のメモリ

分割マイグレーション [1] は図 1 のように VM のメモリを分割して複数のホストへの転送を行う．アクセスされそうなメモリのデータと仮想 CPU などの状態はメインホストへ転送され，それ以外のメモリのデータはサブホストへ転送される．マイグレーション後はメインホスト上で VM 本体が動作し，サブホストはその VM にメモリを提供する．VM はサブホスト上のメモリにはリモートページングを行ってネットワーク経由でアクセスする．VM がサブホストに存在するメモリデータを必要とした際には，そのデータをメインホストへ転送（ページイン）する．代わりに，不要なメモリデータをサブホストへ転送（ページアウト）する．

しかし，実行環境によっては分割マイグレーションやリモートページングの際にメモリデータを盗聴される危険性がある．

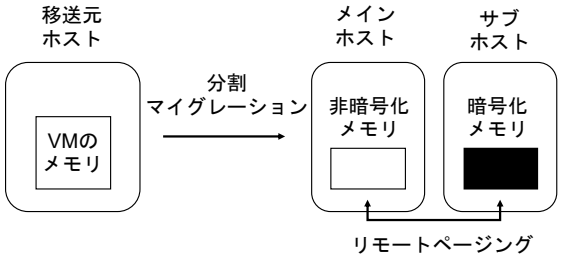

図 1　分割マイグレーション

例えば，メモリデータがデータセンタ間やクラウド間などで転送される場合には盗聴されやすくなる．また，メインホストと管理者が異なるサブホストを利用する場合にも盗聴されるリスクが高まる．情報漏洩を防ぐためにはメモリデータを保護する必要があるが，暗号通信を用いるとメモリデータを転送するたびに暗号化・復号化が行われるためオーバヘッドが大きくなる．また，暗号化が必要な機密情報かどうかは考慮されず，すべてのメモリデータが一律に暗号化される．

そこで，先行研究 [2] では図 1 のようにサブホストにおいてメモリデータを復号しないようにすることでオーバヘッドを削減し，サブホストにおける情報漏洩も防げるようにしている．分割マイグレーション時には，移送元ホストで暗号化したメモリデータを移送先メインホストでのみ復号する．リモートページング時にはメインホストでのみ暗号化・復号化を行う．また，メモリ属性に応じてメモリデータの一部を暗号化しないようにする最適化も行っている．しかし，この最適化は未使用メモリ領域とプログラム領域に限定されている上，これらの領域を正確に特定できていなかった．

3　SEmigrate

本研究では先行研究を拡張して，分割マイグレーションとリモートページングにおいて VM 内の様々な情報を用いた選択的なメモリ暗号化を行う SEmigrate を提案する．SEmigrate は機密情報が含まれないと判断できるメモリ領域は暗号化せずに転送することで，暗号化・復号化のオーバヘッドを削減する．そのために，SEmigrate は VM 内の OS データを解析して，メモリ属性やアプリケーションに関する情報を利用する．さらに，VM 内のアプリケーションのデータも解析して，アプリケーション固有の情報も利用する．

SEmigrate は VM 内で動作する OS として Linux に対応している．Linux ではメモリはページと呼ばれる 4KB の領域に分割して管理されており，SEmigrate もページ単位でメモリデータの転送を行う．

3.1　メモリ属性に基づく選択的暗号化

SEmigrate は VM 内の OS が使用していないメモ SEmigrate は VM 内の OS が使用していないメモ リ領域には機密情報は格納されていないと判断し，暗号化を行わない．先行研

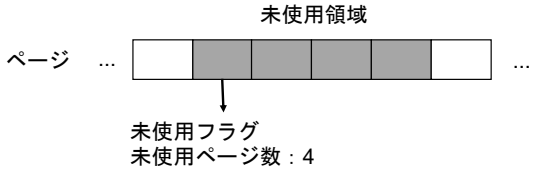

図 2　Linux における未使用メモリ領域の管理

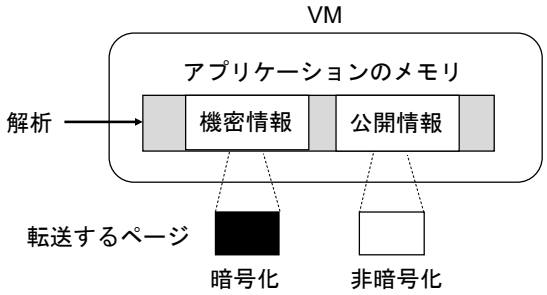

図 3　VM 内アプリケーションのメモリ解析

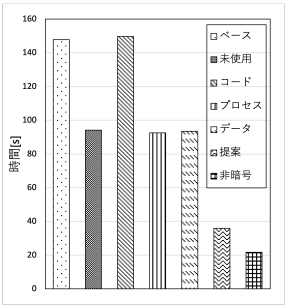

図 4　マイグレーション時間

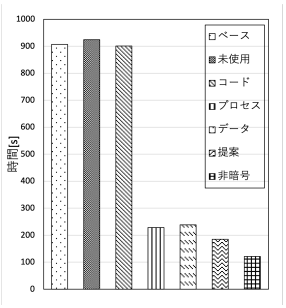

図 5　ベンチマーク実行時間

究では転送するページの管理情報を OS データから取得し，参照カウンタが 0 であれば未使用と判定していたが，これは一部のページについては正しくない．Linux では図 2 のように未使用領域の先頭ページにだけフラグを立てて，その未使用領域に含まれるページ数を保持させている．そのため，未使用領域の先頭ページ以外については未使用かどうかの判定を行うのが容易ではない．

そこで，SEmigrate では分割マイグレーションの際には基本的にページが順番に転送されることを利用して，効率よく未使用領域を判定する．未使用領域の先頭ページを転送した際にはそのページ情報を記録しておき，連続するページも即座に未使用と判定できるようにする．ページが順番に転送されない場合には，未使用領域のページ数が $2^n (n = 0, 1, \cdots, 10)$ であることを利用して，転送するページが含まれる可能性のある未使用領域の先頭ページの候補を調べることで判定を行う．

3.2　アプリケーション情報に基づく選択的暗号化

機密情報を扱わないアプリケーションを指定した場合，SEmigrate はそのアプリケーションを実行するプロセスのメモリを暗号化しない．例えば，暗号化された情報しか扱わないデータベースのメモリは暗号化する必要がない．SEmigrate は転送するページが含まれるメモリ領域を所有するプロセスを OS データの中から見つける．そして，そのプロセスの名前や ID が指定したものと一致すれば暗号化を除外するプロセスと判定する．

さらに，特定のアプリケーションの特定のメモリ領域を指定した場合，SEmigrate はそのメモリ領域を暗号化しない．例えば，暗号データと復号鍵をメモリ上に保持するデータベースの場合，暗号データについては転送時に暗号化する必要はない．SEmigrate は図 3 のようにプロセスのメモリを解析してアプリケーションのデータを取得し，暗号化を除外するメモリ領域の仮想アドレスを特定する．そして，転送するページに対応づけられた仮想アドレスを計算して，そのメモリ領域に含まれていれば暗号化を除外するページと判定する．

3.3　VM のメモリへのアクセス

SEmigrate はハードウェアによるメモリ再マップを考慮して VM の大容量メモリにアクセスする．VM 内では 3〜4GB の物理アドレスは PCI によって使用されるため，3GB を超えるメモリは 4GB 以降のアドレスに再マップされる．一方，VM の外から見ると VM のメモリは連続している．そのため，SEmigrate は 4GB より大きいアドレスを持つ VM 内のデータにアクセスする場合には，1GB を減じたアドレスを用いて VM のメモリにアクセスする．

4　実験

SEmigrate を用いて分割マイグレーションとリモートページングの性能向上を調べる実験を行った．比較として，サブホストで復号化を行わないようにしただけの場合（ベース），それぞれの選択的なメモリ暗号化も行う場合，暗号化を行わない場合 (非暗号) を用いた．選択的暗号化には，未使用領域の非暗号化（未使用），プログラム領域の非暗号化（コード），特定プロセスの非暗号化（プロセス），プロセスの特定領域の非暗号化（データ）を用いた．実験には，移送元ホストと移送先メインホストとして Intel Core i7-8700 の CPU，32GB のメモリを搭載したマシン，移送先サブホストとして Intel Xeon E3-1226 v3, 16GB のメモリを搭載したマシンを用い，10 ギガビットイーサネットで接続した．これらのマシンでは Linux 4.18.17 を 動作させ，仮想化ソフトウェアには QEMU-KVM 2.11.2 を用いた．この実験では 20GB のメモリを持つ VM を 2 台のホストに半分ずつに分割した．

分割マイグレーションにかかる時間を図 4 に示す．SEmigrate では選択的暗号化を行わない場合と比べて 111 秒短くなり，暗号化を行わない場合と比べると 14 秒長くなった．リモートページング性能を調べるために実行したベンチマークにかかった時間を図 5 に示す．SEmigrate は選択的暗号化を行わない場合と比べて 721 秒短くなり，暗号化を行わない場合と比べると 64 秒長くなった．

5　まとめ

本研究では，分割マイグレーションおよびリモートページングにおいて，VM 内の様々な情報を用いた選択的なメモリ暗号化を行う SEmigrate を提案した．SEmigrate では VM 内のメモリ属性やアプリケーション情報に基づいて機密情報の有無を判定し，機密情報が含まれない場合には転送するメモリデータの暗号化を行わない．この最適化により，VM のメモリを暗号化する際のマイグレーション性能とリモートページング性能を大幅に改善した．今後の課題は，実際に利用されているアプリケーションの情報を用いて選択的なメモリ暗号化が行えるかどうかを調べ，性能を測定することである．

参考文献

[1] M. Suetake et al. S-memV: Split Migration of Large-memory Virtual Machines in IaaS Clouds. *CLOUD 2018*.

[2] 高橋. 複数ホストにまたがる仮想マシンのデータ暗号化の最適化. 九州工業大学卒業論文, 2020.