北海道大学アカデミッククラウドのセキュリティ向上への取組み

金子 修己 [1)], 更科 高広 [1)], 吉川 浩 [1)], 林 卓也 [1)], 岩﨑 誠 [1)], 折野 神惠 [1)], 水戸 歩美 [1)]

1) 北海道大学 総務企画部情報企画課

kaneko@iic.hokudai.ac.jp

Approaches on security improvement of Academic Cloud Computer in Hokkaido University

Naoki Kaneko [1)], Takahiro Sarashina [1)], Hiroshi Yoshikawa [1)], Takuya Hayashi [1)], Makoto Iwasaki [1)], Kamie Orino [1)], Ayumi Mito [1)]

1) ICT Planning Division, General Affairs and Planning Department, Hokkaido Univ.

概要

北海道大学情報基盤センターで運用している主要サービスの１つに北大アカデミッククラウドがある。本稿では北大アカデミッククラウドにおけるセキュリティ向上への取組みについて述べる。

1 はじめに

現在の情報化社会においては、サイバー攻撃の急激な増加や個人情報などの情報漏えいが世間を騒がせることが少なくなく、セキュリティという言葉を耳にしない日は無いほどである。

北海道大学情報基盤センター（以下、「本センター」という）が現在運用している学際大規模計算機システムの主要サービスの一つに北大アカデミッククラウドがある。これは、IaaS 型のレンタルサーバ（以下、「サーバ」という）であり、利用者に管理者権限を与えることから、このサーバのセキュリティをいかに確保しながら運用するかが重要な課題となっている。本稿では、サーバのセキュリティ向上に向けて取組んできたこと、及び今後の課題について述べる。

2 北大アカデミッククラウドのサービス概要

本センターで提供しているサーバには、コア数やメモリ容量、耐障害性の違いによりパッケージ化された仮想サーバと、４０コア占有型の物理サーバが存在する。

仮想サーバには CentOS5(2016 年 12 月 1 日以降は CentOS7)のテンプレートが用意されており、オンラインによる利用申請を行うと自動で仮想サーバが提供される。サーバ利用時のインターフェースは TeraTerm などのターミナルソフトを利用したコンソールの他、ミドルウェアの利用によりサーバの起動や停止、ファイアウォールやポート転送などの設定が可能である。

これに対し物理サーバは、利用申請が承認されるとセンターの人員がサーバを構築し利用者へ提供する。OS については、特別な要望が無い限りは CentOS6 で構築し、利用の際はターミナルソフトで直接操作することになる。また、ネットワークの管理は OS の機能や学内ネットワーク機器での制御が必要となる。

以上のように仮想サーバと物理サーバには、提供に関する処理、方法が大きく異なっている。

表１．仮想サーバと物理サーバの比較表

項目	仮想サーバ	物理サーバ
起動方法	ミドルウェアを操作	サーバ本体を直接操作
リソース量の変更	可	不可
サーバ数	最大 2000 台(最小構成換算)	14 台
初期 OS 構築	自動	手動
標準利用 OS	CentOS7	CentOS6
利用形態	共用型	占有型
操作方法	ターミナルソフト、ミドルウェア	ターミナルソフト
ネットワーク制御	ミドルウェア、学内ネットワーク装置	学内ネットワーク装置

なお、サーバの利用に当たっては、以下の条件が利用者に課せられている。

・サーバ構築技術を有し、サーバの運用を適切に行う資質があること。
・OS のアップデートは適宜、適切に取り入れた運用を行うこと。
・アカウント及びパスワードは適切に管理すること。
・サーバが不正使用された場合、利用者の許可無く本センターがネットワークの切断を行えるものとする。
・セキュリティインシデントが発生した場合は、利用者がその責を追うものとする。
・利用者に十分な知識・技術が無い場合、その役割を担う代行者をおくことで上記項目を満たすこと。

3 セキュリティ向上への具体的取組み

3.1 サーバのテンプレート更新

Linux や Windows など多くの OS にはサポート期限が設けられており、主要 OS のサポート期限は表２のようになっている。[1][2]

表２．主な OS のサポート期限

OS 名称	サポート期限
RHEL6	2020/11/30
RHEL7	2024/6/30
CentOS5	2017/3/31
CentOS6	2020/11/30
CentOS7	2024/6/30
Windows7	2020/1/14

前述の通り、クラウドシステム導入当初は CentOS5 のテンプレートでサーバを提供していた。しかし、CentOS5 は 2017 年 3 月 31 日にサポートが終了するため、2016 年の秋頃になると利用者からは CentOS7 へのバージョンアップについての問い合わせが相次ぐようになった。その時点ですぐにでも CentOS7 のテンプレートを公開できれば良かったのだが、環境構築に時間を要してしまい、2016 年 12 月 1 日に提供を開始した。なお、物理サーバについては CentOS7 がクラウドシステムのハードウェアに未対応のため、CentOS6 で提供を開始した。

CentOS7 テンプレート公開までの間は、新規サーバであっても利用者自身が OS を入替ることが余儀なくされた状況となったため、本センターとしては利用者の負担を少しでも軽減し確実に入替を行って頂けるよう、CentOS7 インストール用 ISO イメージのマウントを簡略化し、さらにインストールマニュアルを整備することで対応した。

3.2 利用者への周知

3.1 では、新規にサーバを利用開始する場合や、ある程度セキュリティに関心が有り自主的にサポート期限切れへの対応を行って頂く場合に効果が有る対応について述べてきた。しかし、問題となったのが CentOS5 での運用を行っており、サポート期限に関心が薄い利用者への対応であった。OS のバージョンアップを行うか、新たにサーバを借りるなど別のサーバを用意し、そこへ構築し直す作業を、年度末という忙しい時期に行う必要が有ったためである。

2016 年 9 月下旬から順次、メルマガ、広報誌、ホームページへの掲載によって利用者へ CentOS5 のサポート期限の終了が迫っていることを周知し始めた。しかし、メルマガは希望者のみに配信しており、広報誌やホームページは関心が無い人にとっては目に触れるものではなく、利用者全員に周知することの難しさを思い知らされた。最終的には、利用申請時に登録されたメールアドレスを利用し、利用者全員へ案内メールを送信して周知することとした。

3.3 サポートされた OS へのバージョンアップ

CentOS5 における OS のバージョンアップ作業とは、具体的にはいわゆるクリーンインストールである。しかし、CentOS4 から CentOS5 の場合や、Windows7 から Windows10 の場合は HDD の初期化を伴なわずにバージョンアップが可能であった。このため、CentOS5 では後継 OS へのバージョンアップが用意されていないことを理解してもらえないケースが目立った。後継 OS へのバージョンアップを行うには、まずデータを外部記憶装置などへ退避し、後継 OS をインストールした後、Web サーバなどのシステムを構築し直すという手順が必要となること、及びこれらの作業は本センターではなく全て利用者の作業であることを説明することとなった。

クラウドサービスの提供機関としては、サポートされた OS の利用のみを認めるといった方針に対し、一部の利用者からはさまざまな理由により継続利用を求める声が寄せられた。代表的な例を

以下に示す。

・特定アプリが CentOS5 でしか動作しない。
・クローズドネットワークで使用するのでサポート切れ OS でも問題ないはず。
・再構築する方法が判らない。
・サーバ構築が自分の仕事（研究）ではない。
・急に言われても、業者へ構築を依頼する予算が無い。
・当年度に使い始めたばかりのサーバである。

これらの要望に対しては、大学全体としての決定事項であることを丁寧に説明し、例外を認めずに納得して頂いた。なお、2017 年 4 月 1 日の時点で CentOS5 だったサーバについては強制的に停止し、利用者の操作による起動を抑止した上で利用者と連絡を取り、個別に対応を行った。

3.4 学外から学内への通信制限

本センターがクラウドサービスとして提供している全てのサーバは、初期値としてグローバル IP アドレスが付与される構成になっている。また、学内の業務用端末についてもグローバル IP アドレスを利用している端末が多数存在していながら、学外からの通信を制限していなかった。このような環境の中、本センターが提供しているサーバではないものの、学内のサーバにおいて不正アクセスと思われる情報セキュリティインシデントが発生した。

この事態を本学としては重大なインシデントとして受け止め、2016 年 1 月から段階的に、2 月下旬には全学的にインバウンドの通信を制限することとなった。

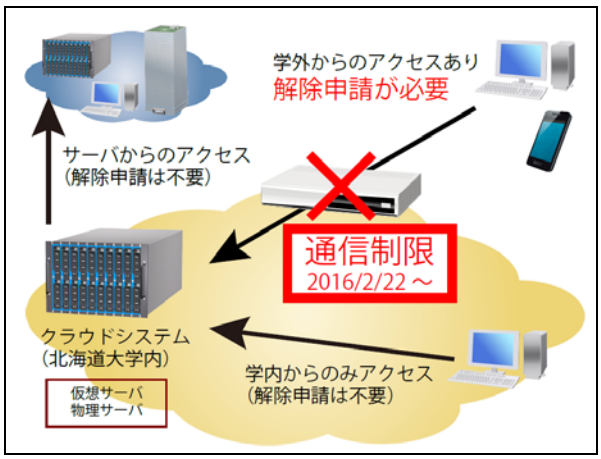

図 1　通信制限イメージ

Web サーバやメールサーバなど学外からの通信が必要な場合には、利用者がサーバへの接続元・接続先 IP アドレスやプロトコルなどの情報を添えて「通信制限解除申請」を行い、サイバーセキュリティセンターの承認を得た後、本センターのネットワーク担当によって学際大規模計算機システムの上位に位置するファイアウォールの設定が変更され、学外からの通信が可能となる制度とした。

3.5 情報セキュリティ関連規程の整備

以上のように技術的な対策を進める一方、従来から運用されて来た規程や組織の整備などの管理的対策も同時に進めた。

情報セキュリティに関連する規程として、施策についての基本理念を定めた「情報セキュリティ基本規程」が施行され、また組織及び体制を整備するとともに情報資産の円滑な運用及び保全を図ることを目的とする「情報セキュリティ対策規程」を施行した。

3.6 利用者向け手引き書の作成

さらに、各種規程は表現が抽象的であったり、大きな枠組みでの話であり、本センターが提供しているサービスに当てはめた場合、利用者によって解釈が異なる恐れがあった。このため、本センターの利用に特化して前述の利用者へ課せられた条件や各種規程の要点をまとめた冊子を作成することとなった。こうして「システム適正利用の手引き」を作成し、2017 年 8 月には既存の全利用者へメールで案内し、さらに新規利用者には利用承認に関する通知書を送付する際に手引き書への URL を案内する運用を開始した。

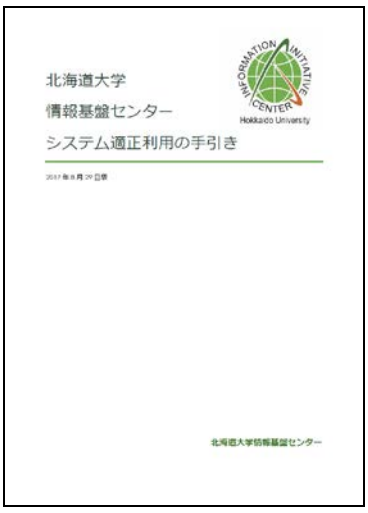

図 2　手引き書表紙

3.7 区分 CSIRT の設置

組織面の整備としては、本センターでサービスしているレンタルサーバを含めた大型計算機システムに係わるセキュリティ確保のための施策、及びインシデント発生などの有事の際の迅速な対応を図るため、区分 CSIRT（Computer Security Incident Response Team）を設置した。これにより、インシデントの発生、又はその疑いの通報があった場合の連絡体制や対策の決定権の所在が明確になり、迅速な初動が期待できる体制を整えた。

4 今後の課題

本学、及び本センターとして講じてきた取り組みは以上の通りである。これらの取り組みの中には、運用組織としての作業と、利用者の作業が存在していた。中でも、CentOS のバージョンに係わる作業については、利用者ごとにそれぞれ事情があり、全ての利用者に対策を施してもらうには非常に手間と時間を要する取り組みであった。

このことから、今回の経験として特に利用者の作業となる部分については、年単位での作業を想定し、周知時期、周知方法についての改善が必要であることが判った。ただ、それはあくまでも周知の話であって、本来は利用者自ら意識すべき部分である。その点では、利用者に適切な運用を行って頂けるよう、情報セキュリティへの意識・関心を向上させることが今後の課題である。

5 おわりに

現在は、次期大型計算機システムの入札に向け準備を進めているところであるが、クラウドシステムについては現在と同様に、利用者に root 権限を与える IaaS 型のレンタルサーバを提供し、全ての管理は利用者に任せる見込みである。

新たな脅威の出現は終わりがなく、セキュリティ対策もまた終わりが無いのが実情である。このような状況の中、セキュリティインシデントを予防するには、常に最新の動向を把握しつつ、必要に応じて対策を実施出来る体制を継続していくことが必要であり、利用者の協力が無ければ成り立つものではない。本センターのみならず、北海道大学全体のセキュリティ向上のため、利用者と共に安全なシステムを運用できるよう努めていきたい。

参考文献

[1] Red Hat Enterprise Linux のライフサイクル
https://access.redhat.com/ja/support/policy/updates/errata

[2] Microsoft at Life
https://www.microsoft.com/ja-jp/atlife/article/windows10-portal/eos.aspx