Vol.2018-IOT-40 No.11
2018/3/5

粗い分割のキャンパスネットワークにおける IP アドレス棚卸作業

鈴木聡[†1]　村上直[†1]　湯浅富久子[†1]　金子敏明[†1]
馬場亮一[†1]　中村貞次[†1]　橋本清治[†1]　西口三夫[†1]

概要： 教育研究ネットワークに対するサイバー攻撃が激化していることからキャンパスネットワークでの IP アドレス利用状況を従来にも増して正確に把握することが求められている．
当機構では比較的サブネットの分割単位が粗く人事上の区分との関係が弱い．キャンパスネットワークの利用には申請と承認が必要であるが，申請者は転出している可能性がある．また共同利用者も多数利用しているため，業務指揮系統を通じた利用状況の点検だけでは回答の回収が不十分になることが予想された．
そこで 2016 年~2017 年にかけて （1）Web アプリケーションを通じて管理者本人もしくはサブネット管理者が代理で機器毎に利用状況を回答，（2）無回答機器についてサブネット管理者もしくは上位職から確認，（3）さらに無回答の機器について認証を一時無効化し問題と感じた利用者からの通報による対処，の 3 段階で管理者情報の更新と不要機器の強制廃止を行った．この更新作業の概要と結果を報告する．

キーワード：キャンパスネットワーク，IP アドレス管理

Survey procedure of IP address usage in roughly divided campus network

SOH Y. SUZUKI[†1]　TADASHI MURAKAMI[†1]　FUKUKO YUASA[†1]
TOSHIAKI KANEKO[†1]　RYOICHI BABA[†1]　TEIJI NAKAMURA[†1]
KIYOHARU HASHIMOTO[†1]　MITSUO NISHIGUCHI[†1]

1. はじめに

研究活動の自主性を尊重してきた研究教育ネットワークにも近年はサイバー攻撃が及んでいる．従来は組織の保有する IP アドレスの管理はサブネット単位に移譲されている形態が一般的であった．小規模なサブネットであればよいが，最終的な分割単位が粗いとサブネット管理者から実際の利用者まで目が届きにくい．

高エネルギー加速器研究機構（以下，KEK）は大学共同利用機関であり，職員数の 10 倍程度の共同利用者が研究活動を行っている．キャンパスネットワークの IP アドレスは概ねプロジェクト単位に分割されているが，プロジェクトの参加人数が数十人から数百人と大きいためサブネットの大きさが/22~/21 程度である．この規模になるとサブネット管理者は全ての機器の状況を完全に把握することは難しい．サブネット管理者任せにすることなく，直接各機器の管理者との連絡が取れることは重要である．

管理者情報の内容を更新する為，KEK で 2016~2017 年にかけて行った棚卸作業を報告する．

2. キャンパスネットワークと IP アドレス管理

KEK ではキャンパスネットワークの利用に当たっては MAC アドレスを明記した申請が必須である．申請 1 件毎に 2 段階の承認を得る必要があり（図 1），認証システムは台帳の MAC アドレス等を参照しているので台帳登録が完了して初めて利用可能になる．キャンパスネットワークでは認証スイッチは Apresia シリーズを，認証サーバは FreeRADIUS を，FreeRADIUS が参照するデータは PostgreSQL に独自のスキーマを使用して格納している．インシデントや何らかの問題が疑われた場合，この台帳上の管理者に連絡を取る．台帳は認証システムを運用している計算科学センターが管理している．MX レコードや TTL 等の個別対処を求められることがある為，DNS や DHCP は別途手作業で登録が行われる．

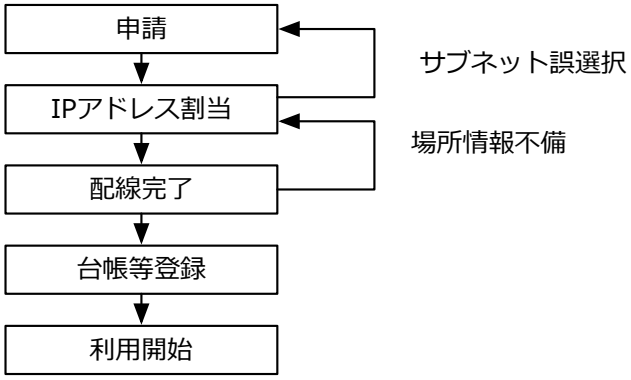

図 1　KEK におけるネットワーク申請の流れ．

†1 高エネルギー加速器研究機構
High Energy Accelerator Research Organization.

サブネット管理者は第 1 段階の承認として IP アドレスを割り当てる．情報コンセントのパッチ配線管理者が第 2 段階を承認するならば配線を行う．この 2 つの承認を通過したのち台帳に登録される．

しかし配線に必要な建物名・部屋名・情報コンセント名に関して申請に誤りがあると承認フローに差し戻しが発生し，申請から利用可能になるまで数営業日が経過することもある．

不要な機器は廃止を申請するよう促しているが，研究者は様々な業務に忙殺されていると火急の必要性がない廃止申請は後回しになりやすい．一旦廃止された機器であってもその後新規に申請することは禁止されていないが，新規申請から利用可能になるまで数営業日かかることが珍しくない為，本当に不要になるまで廃止しないという側面もある．

しかし不要機器が廃止されないと情報コンセントの配線が無用に肥大し，配線管理者の負担が増大する．また大規模なセキュリティインシデントを警戒し，全台調査を行わなくてはいけない場合，不要な機器は対象の台数に増やすことになり，百害あって一利なしと言える．

このような不要機器の廃止を促し，台帳の整理を行うべく棚卸作業を計画した．

3. 棚卸作業の目標と手順

棚卸作業の目標は以下の 2 つである．

- 必要でない機器は廃止する
- 必要な機器は管理者の登録を正しくする

前者にあたるのは退職者や転出者が不要機器を廃止する申請を行わなかったものを台帳から削除することを狙いとした．後者にあたるのは管理者の交代を補足することが狙いである．KEK では退職・転出しても共同研究者として KEK のプロジェクトに参加し続けることが非常に多い．退職者の機器を一律強制的に廃止することは進行中のプロジェクトに与える影響が懸念される為，現実的でない．従って，個々の機器毎に状況確認が必要であり，以下の 3 段階で棚卸確認を行うこととした．

1. 台帳上の管理者本人が自分の機器の必要性を回答する．不明という回答も可とする．
2. 回答がなかった機器に関して，サブネット管理者もしくは上長が必要性を回答する．不明という回答も可とする．必要な機器については正しい管理者を明らかにする．締め切り後に不明・無回答であった機器については認証を無効化する．
3. 無効化されている機器について，利用できないことが問題だと感じた者が連絡する．管理者が判明した場合は復活を申請する．締め切り後に不明・無回答であった機器は台帳から削除される．

いずれの段階にも締め切りを設ける代わり，不明という回答を許した．また，以下に該当する機器も対象外とした．

- 棚卸アナウンス後に申請された機器
- 機構外からアクセス可能な機器

棚卸アナウンス開始後に申請されている機器については使用中であることは自明であり，機構外からアクセス可能な機器は年度毎の DMZ 機器セキュリティ自己点検で管理者本人が詳しい管理状況を報告している[1]からである．おおまかな日程を図 2 に示す．

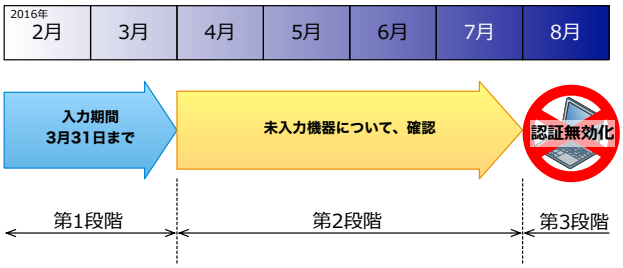

図 2　棚卸作業のスケジュール概要

機構の統括情報セキュリティ責任者及び情報セキュリティ担当理事に棚卸手順及びスケジュールについて判断を仰ぎ，管理者が回答しない場合は機構全体の判断として機器を台帳から削除することとした．

第 1 段階で回答率が悪い場合は第 2 段階でサブネット管理者の作業量が増えることが予見される．サブネット管理者向けの説明会を複数回行い，最も広いサブネットを含め一部のサブネットは事前にサブネット管理者が先回りして回答を入力できるようにし，約 370 台が処理された．

3.1 管理者本人による回答

第 1 段階用として専用の Web 回答システムを作成した．回答用 Web サーバは台帳データを格納している PostgreSQL サーバを参照する（図 3）．クローラは ARP テーブルおよびブリッジテーブルを毎時数回取得して PostgreSQL サーバに格納している．また，検索性能を上げるため IP アドレスを主キーとして MAC アドレス及び更新日付，MAC アドレスを主キーとして接続ポートと更新日付を上書き処理で更新するテーブルにも記録している．

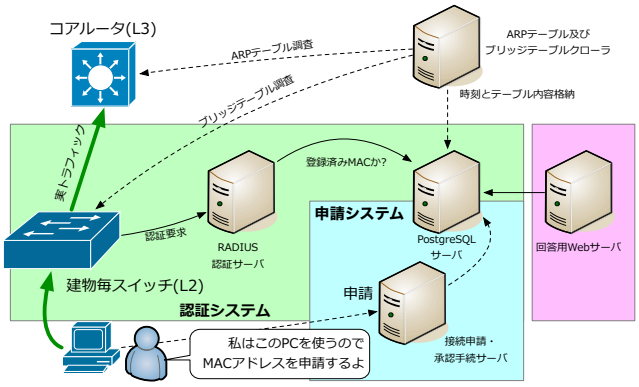

図 3　第 1 段階用 Web サーバの配置

プリンタなど，自らはネットワーク通信を行わない機器等があるため，ARP が観測されないこととネットワークから切り離されていることは完全に同一ではないが，少なくと

も観測日には接続されていたことは言える．
台帳上の管理者本人が回答するほか，サブネット管理者は自らの管理するサブネットについては回答状況を一覧することが出来る．

入力しようとする者は自分が管理者として登録されている機器を検索し，該当があれば対象者であるのでワンタイムパスワード取得操作を行う（図 4・図 5）．

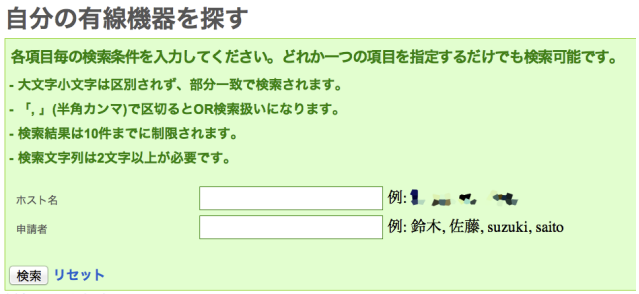

図 4 対象機器の中に自分のものがあるか検索する画面

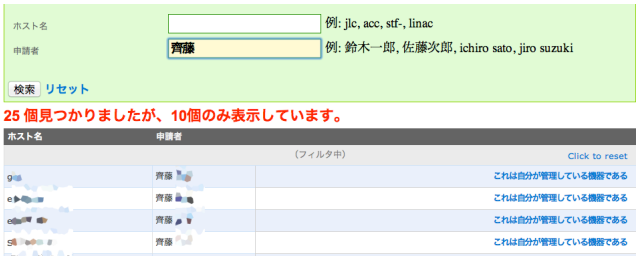

図 5 対象機器が見つかった場合

登録上の連絡先メールアドレスにワンタイムパスワードが送信されるので，それを用いてシステムにログインする．ログインすると同一の連絡先を持つ機器が一覧で表示される（図 6）．

図 6 ログインした者が管理する対象機器一覧画面

新規の接続申請の完了には数営業日かかることが珍しくない為，「ひょっとすると後日必要になるかも」と考えて廃止を見送っていた機器をこの機会に廃止してもらうべく，ARP テーブルと認証システムのログを参照して最終利用日を機器毎に表示した．各機器について使用中・不明・廃止をチェックする．1 ホストあたり 1 クリックでよい（図 7）．

図 7 回答ボタン

一度のログインで全てのホストについて回答する必要は無く，その時点で必要性の確定している機器のみ回答してよいとした．

不明という回答を許さず，救済措置を設けないとあらゆる機器を「使用中」と回答する方向に誘導することになる．「半年待ってみて必要なら直ちに有効化を申請できるので，必要性が不明な機器は様子を見る為とりあえず不明として回答してよい」とした．

入力内容は第 1 段階の締め切りまでは任意に訂正可能とした．ただし，廃止の取り消しは入力後一週間のみとした．これは以下のような理由からである．

廃止は台帳の変更が生じ，DNS および DHCP からの登録抹消作業も必要で，作業担当者の負荷を時間的に分散させる必要がある．廃止を選択した場合は第 1 段階の締め切りを待たず，確定した機器について順次廃止操作を行うこととした．もちろん，廃止されてしまった後でも当該機器を新規接続として申請することは可能である．

入力締め切り後に各サブネットの機器について回答状況をまとめ，各サブネット管理者にレポートを送付することとした．

Web アプリケーションは Ruby on Rails [2] と ActiveScaffold [3]で作成した．台帳本体のデータが格納されている PostgreSQL を参照するが，アプリケーションに対する入力は別途 SQLite3 で独立したファイルに格納する．画面遷移を極力減らすため，回答に使用するボタンは全て ActiveScaffold のアクションリンクで作成してある．

3.2 サブネット管理者もしくは上長による回答

第 2 段階は台帳上の管理者以外も必要性を判断する．第 1 段階締め切りまでに回答されなかった機器であってもプロジェクトにとって不可欠な機器については，サブネット管理者もしくはプロジェクトの上長が台帳上の回答しない管理者に代わって適切な管理者を指名し，使用中と回答するように求めた．第 1 段階と同様，締め切りを設ける代わり「不明」の回答も引き続き可とした．

第 2 段階終了時にも「不明」もしくは無回答であった機器は認証を無効化することとした．KEK では年に一度の全所計画停電があり，この期間はキャンパス内のネットワーク通信は不可能になる．進行中のプロジェクトであってもネットワーク通信がないことが確実な停電期間に認証データを一斉に無効化することとした．多くの実験装置は計画停電終了後に担当者の管理の下に手動で再立ち上げが行われる．停電前の停止作業よりも復電後の再立ち上げ作業の方が時間的に分散する傾向にあるため，対応作業が取りやすいと考えた．

3.3 不明機器の再有効化と廃止

第 3 段階は第 2 段階終了時に無効化された機器について必要性を確認する．
第 1 段階と同様に Web アプリケーションに対してログインし，自分が管理者である機器について再有効化を申請できるようにした（図 8）．

図 8　再有効化申請画面

4. 棚卸作業の実行

4.1 第 1 段階

2016 年 1 月 13 日に機構職員向けに電子メールで事前アナウンスを行い，2016 年 2 月 8 日～3 月 31 日を第 1 段階とした．アナウンス開始時点で対象機器は約 8800 台であった．入力数の分布を図 9 に示す．

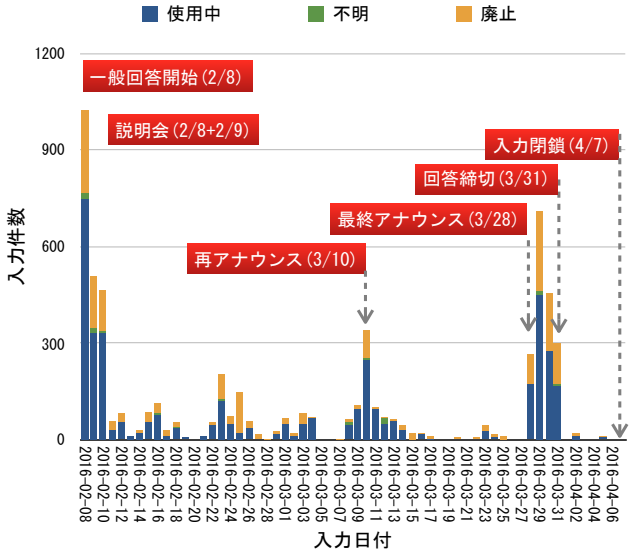

図 9　第 1 段階の回答進捗

入力開始直後に多くの入力があったが，三日程度で一服した．3 月 10 日に締め切りとその時点の回答率をアナウンスし，一時的に入力数が増えたがこれも一週間程度で終息している．3 月 28 日に締め切り直前のアナウンスを行ったところ，入力数は再び増え，締め切り期日後も入力が継続した．締め切りに間に合わない者が多数いることを想定していたが一週間以内に一日あたりの入力数が 0 になった．締め切り一週間後である 4 月 7 日に Web アプリケーションの入力のみ不能にした．その後，第 2 段階による連絡があるまでログイン試行履歴はなかった．第 1 段階の入力結果は以下であった．回答率は約 70%である．

- 使用中: 4100 台
- 廃止:約 2000 台
- 不明:100 台
- 無回答: 約 2600 台

多数の機器について「不明」が選択され，廃止は少ないと想定していたが，不明よりは廃止がずっと多かった．第 1 段階で廃止と回答された機器の台帳処理が完了したのは 4 月 15 日である．

4.2 第 2 段階

4 月 14 日にサブネット管理者にエクセルシートで回答内容を送付し，6 月末日までに不明機器の中に必要な機器があるかの調査を依頼し，7 月 7 日に第 2 段階の結果として確定した．約 890 台について情報が更新された．この時点で廃止とされた機器については廃止作業を開始した．第 2 段階で廃止とされた機器の約 430 台の台帳処理が完了したのは 9 月 16 日である．

サブネット管理者では判断が付かない場合はプロジェクトの上長の判断も可としていたが，上長が新たな管理者を割り当てて使用中とした機器はなく，多数の機器が不明となった．また，サブネット管理者からの連絡を受けてから入力を開始するべく第 1 段階の Web アプリケーションの入力を開始しようとする者がいた．回答率の低いサブネットは以下の特徴があった．

- サブネット内に多数のグループがいる．
- グループは少人数である．
- 個人で使用する機器がほとんどである．
- 外来研究員が多く，かつ転入・転出など異動も多い．
- 長年勤めたサブネット管理者が代替わりし，利用者との面識がほとんどない．

引き続き必要性が不明であった機器については停電時の無効化対象機器として集計した．

計画停電の 2 週間前に認証システムの認証履歴と照合した結果，このうち約 220 台は 4 月 1 日以降の利用が観測された．これらの機器の台帳上の管理者 130 名に対し，回答がなければ認証が停電後無効化される旨の通知メールを 8 月 2 日に送信した．回答締め切りはその週末の 8 月 5 日と非常に短い期限で設定したが，90 名以上から回答があり約 150 台が無効化対象から外れた．最終的には約 1800 台が無効化された．

4.3 第 3 段階

想定通り復電後に「なぜか機器が使えなくなった．停電によるネットワーク障害ではないか」という相談が多数寄せられ，再有効化申請の手順を回答した．締め切りである年度末までに約 40 台の再有効化の申請があった．このほか，通常の手続きによる廃止がありさらに台数が減少した．

第 3 段階締め切り時である 2017 年 3 月 31 日に無効化されたまま残存している機器を強制廃止対象とした．

4.4 強制廃止作業

5 月 1 日時点で残存していた約 1600 台については管理者の同意がなくとも台帳から削除することとなった．

5 月 10 日に対象機器の台帳上の管理者に 5 月末日までに回答がなければ台帳から削除することを通知するメールを送信した．これに対し，5 名から 11 台について利用継続の回答があった．それら以外の機器について廃止を行い，全

ての台帳操作が終わったのは 2017 年 9 月 4 日である．

5. 結果と考察

5.1 目標の達成

対象機器約 8800 台中，無回答機器を含めて約 4100 台が台帳から削除された．棚卸期間中に管理者の割り当てができなかった機器は全て廃止された．管理者情報は全て更新され，当初の目標は達成した．

当初，広いサブネットであればあるほど回答率が低いと想定していたがサブネットの広さと回答率にはほとんど関係がなく，雑居度による差が顕著であった．この観点からは，サブネット分割の粗さはアドレスの広さではなく，構成グループの大きさとあっているかどうかが重要である．

5.2 認証履歴による最終使用日の提示

全ての段階において，機器の最終使用日が不正確ながらも表示されることに関しておおむね好評であった．最も重要なことは前回（1 年前）の計画停電から一度も利用されたことがないかどうかであった．また，無回答機器の無効化作業後には利用者の記憶違いによる問い合わせが見られたため，認証の試行・失敗の記録も保持しておくべきであった．

5.3 入力受付期間

第 1 段階の入力頻度を見ると，期間をあまり長くとっても回答率は上がらない. 無効化後に「入力期間が短すぎる」といった苦情が多数発生することを警戒していたが，苦情は入力期間の短さではなく締め切りがあることそのものに対する苦情であった．しかし単なる再アナウンス後よりも締切直前の入力の方がずっと多かったので，締切の設定は不可欠と考えられる．

5.4 連絡方法

機構職員全体へのアナウンス，サブネット管理者からの連絡，機器の管理者への個人宛連絡を行った．非常勤や兼務が多い近年では，職員全体へのアナウンスだけでは当事者意識の喚起が不十分と考えられる．サブネット管理者からの連絡は全体アナウンスに比較すれば回答率はよいが，サブネット管理者の負担が増える．第 1 段階終了の時点で回答率 100%のサブネットもあれば, 40%台のサブネットもあったことから，先に全体アナウンスを行った方が全体の労力は低く抑えられる．

第 2・3 段階終了時に計算科学センターから管理者個人宛連絡メールを多数送信したが，回答率は使用中機器の無効化警告以外は極めて低かった．個人宛の連絡は管理者が切迫感を受けてからの回答であったためか，自由形式の文章による返信が多く，対応労力が大きい．返信内容に使用中の機器が明示されていないなどの理由で返信に対してさらに問い合わせを送ると回答が途絶える割合が高かった．

5.5 Web からの回答入力

第 2 段階は管理者本人以外が入力する前提であったため，期間中は Web からの回答はできないようにしていた．回答率の低いサブネットは，サブネット管理者は全く集計を行わず，アナウンスを転送するだけだった例もある．第 2 段階期間中はサブネット毎に Web からの回答入力可否を切り替えられるようにするべきであった．

5.6 Web アプリケーションの設計

当初，Web アプリケーションはネットワーク接続の申請システムの認証情報を使用することを想定していた．しかし締切直前になってから亡失パスワードのリセット依頼が大量に発生することを警戒し，ワンタイムパスワードを前提とするアプリケーションに変更した．この方法は意外と好評だったようで，他の入力システムでも亡失を心配する必要がないワンタイム型にならないかという要望を受けることがある．多くのユーザーがパスワードの到着を待つことができず，1 回の操作につきワンタイムパスワードを 2 回以上発行していた．本システムではワンタイムパスワードそれぞれに有効期限が設置されており，2 つめを発行しても 1 つめは無効化されないようにした．

台帳本体のデータのスキーマは元々別アプリケーション用に設計されているため，Ruby on Rails の規約に従っておらず，大半のテーブルの主キーが複合キーになっている．複合キーのテーブルについて ActiveScaffold でページ処理を行うと CASE 文 SQL 文が肥大しやすい. さらに元データの複合キーに文字列が含まれていたため，クエリ文字列長の制限に達しやすい．結果として 1 ページ当たりの表示レコード数が大きくできず，一覧性が悪かった．

またアプリケーションが参照するデータが PostgreSQL と SQLite3 の 2 つに分散したことによって回答数が増えるに従い無回答機器のサブネット単位の集計に必要な時間が延び，これも一覧性の悪さに繋がった．

この 2 つの問題は棚卸用アプリケーションのデータは PostgreSQL の別データベースに格納し，Foreign Data Wrapper [4]と Materialized View を用いて Ruby on Rails の規約に沿った形式に整形することで改善できる見込みである．

6. まとめ

本報告では IP アドレス管理台帳から不要機器の廃止と管理者情報を更新するため，手順と使用した Web アプリケーションについて概説した．棚卸作業を機構全体として行ったことは初めてであるが，回答の傾向を見ると定期的な実施が必要と考えられる．Web アプリケーションの改善を含め，次回の棚卸の効率化を目指す．

参考文献

[1] 村上直,湯浅富久子,金子敏明. “DMZ ネットワークのサーバ管理者自身による脆弱性診断”, IOTS2016, pp. 41-48. （2016）
[2] http://rubyonrails.org/
[3] https://github.com/activescaffold/active_scaffold/
[4] https://wiki.postgresql.org/wiki/Foreign_data_wrappers/