Vol.2013-CSEC-61 No.27
Vol.2013-IOT-21 No.27
2013/5/10

岡山大学における大規模認証ネットワークの運用と課題 (2)*1

山井 成良[1,a)]　岡山 聖彦[1]　大隅 淑弘[1]　藤原 崇起[1]　河野 圭太[1]　稗田 隆[1]

概要：
岡山大学では，2009 年度に旧キャンパス情報ネットワークを更新し，2010 年 6 月から新ネットワーク (ODnet2010) の運用を開始した．ODnet2010 では，ネットワークの高速化・高信頼化に加え，新機能としてフロアスイッチにおけるネットワーク認証とロケーションフリー (認証 VLAN) 機能を導入している．本稿では，「生活系ネットワーク」と称する認証・ロケーションフリーネットワークにおいて，特に様々な資源の不足により生じた課題について報告する．

キーワード：
キャンパスネットワーク，認証ネットワーク，動的 VLAN

Operation Issues of Large Scale Authentication Network in Okayama University (2)

Nariyoshi Yamai[1,a)]　Kiyohiko Okayama[1]　Yoshihiro Ohsumi[1]　Takaoki Fujiwara[1]
Keita Kawano[1]　Takashi Hieda[1]

Abstract:
We replaced Okayama University Campus Information Network in 2009 fiscal year, and have operated the new network called ODnet2010 since June 2010. ODnet2010 not only improves its bandwidth and reliability, but also provides some new functions such as user authentication by floor switches, location-free function for VLANs. In this paper, we explain the operation of authenticated location-free VLANs called "Living Networks", and discuss some issues mainly caused by lack of resources.

Keywords: campus network, authentication network, Dynamic VLAN

1. はじめに

岡山大学（以下，本学）は学生数約 14,000 人，教職員数約 2,600 人，11 学部を擁する，地方大学としては比較的大規模の総合大学である．主要なキャンパスとしては岡山市内の津島キャンパス（医療系を除く学部，情報統括センター，事務局など），鹿田キャンパス（医療系学部，岡山大学病院など），東山キャンパス（教育学部附属学校園），倉敷市の倉敷キャンパス（資源植物科学研究所など），鳥取県三朝町の三朝キャンパス（地球物質科学研究センター，岡山大学病院三朝医療センター）がある．

本学では，2009 年度に旧キャンパス情報ネットワークを更新し，2010 年 6 月から新ネットワーク ODnet2010 の運用を開始した．ODnet2010 では旧ネットワークで問題となっていた (1) ネットワークの高速化，(2) 信頼性の向上，(3) セキュリティの強化，(4) 利便性の向上の 4 項目を目標に掲げて設計を行った．特に (3)，(4) については Web 認証に基づいてアクセス制御機能を行い，また認証されたユーザの属性に応じて接続先 VLAN を動的に決定するよ

[1] 岡山大学情報統括センター
Center for Information Technology and Management, Okayama University
3-1-1, Tsushima-naka, Kita, Okayama 700–8530, Japan
[a)] yamai@okayama-u.ac.jp

うなネットワーク（生活系ネットワーク）を導入し，ロケーションフリー，すなわちキャンパス内ではユーザの場所に依存しないで同一の条件で利用できるアクセス環境の提供を目指した [2].

現在，ODnet2010 では従来の認証を要しないネットワークから新しいネットワークへの移行を進めている最中である．しかし移行過程において，スケーラビリティを十分に考慮して設計していなかった，機器や端末の動作を十分に理解していなかった，あるいは機器や端末の持つ脆弱性が顕在化したなどの理由により，導入当初には想定していなかった様々なトラブルが露見するようになった．これらのトラブルには設計や運用の見直しにより対処できたものもあれば，未だに原因が不明であるものや，原因は判明しているものの対処方法が不明であるものが多数存在する．

本稿では ODnet2010 の運用において発生した様々なトラブルのうち，特にネットワーク機器のリソース不足が原因と思われるものについて紹介する．なお，主要なトラブルのうち本稿で述べられていないものについては [1] を参照されたい．

2. ODnet2010 の構成と運用

2.1 ODnet2010 の概要

ODnet2010 の物理構成を**図 1** に示す．前節で述べた 4 つの目標を実現するため，ODnet2010 では以下のような構成を採用した．

まず，ネットワークの高速化を図るため，ODnet2010 では基幹ネットワークのうちコアスイッチと他の機器との間（コアスイッチ・建物集線スイッチ間，コアスイッチ・データセンタースイッチ間および津島・鹿田キャンパスコアスイッチ間）は 20Gbps（10Gbps × 2 回線），それ以外の建物集線スイッチ・フロアスイッチ間は 2Gbps（1Gbps × 2 回線）とし，従来の 1Gbps と比較するとそれぞれ 20 倍，2 倍の帯域を実現した．また，支線ネットワーク（フロアスイッチ以降）は 1Gbps の帯域を確保し，従来の 100Mbps の 10 倍の帯域を実現した．

次に，信頼性の向上を図るため，従来のキャンパスネットワークから構成を大幅に変更することになった．従来のキャンパスネットワークではクラスタと呼ばれるネットワークグループを設け，最も大規模な津島キャンパスでは各クラスタには L3 スイッチを 1 台設置して総合情報処理センター（現・情報統括センター，以下センター）に設置した L3 スイッチとの間でスター状に接続する構成を採用していた．ところが，この構成では単一障害点が多数存在し，特にセンターに設置されている L3 スイッチに障害が発生するとキャンパス全体に影響が及ぶ構成になっていた．そこで，ODnet2010 では L3 スイッチをキャンパス内で 1 台（コアスイッチ）に集約する代わりにコアスイッチの筐体内モジュールの二重化，建物集線スイッチの二重化，基幹ネットワークおよび建物内のフロア間での回線二重化を行い，主要箇所での単独故障に耐えうる構成になるように設計を行った．また，津島・鹿田キャンパス間の接続回線も二重化されているほか，図 1 には示されていないが，従来から津島・三朝キャンパス間接続や SINET との接続も二重化されている [3].

セキュリティの強化については，フロアスイッチに Web 認証，MAC アドレス認証などの認証機能を有する機器（認証スイッチ）を導入して，ネットワーク利用時に必ず端末認証を行わせるようにした．また，レイヤ 3 スイッチは津島，鹿田，倉敷，三朝，東山の各キャンパスに導入しているが，そのうち津島，鹿田キャンパスのコアスイッチには仮想網によるネットワークの分割機能（VRF: Virtual Routing and Forwarding）を有する機器を導入し，各サブネットの利用目的に応じて他のネットワークと分離できるようにしている．

一方，セキュリティの強化はユーザから見ると利便性の低下に繋がるため，本学で導入している統合認証基盤システムとの連携による認証 VLAN 機能や，SSL-VPN サーバの導入により，学内外を問わずロケーションに依存しないアクセス環境（ロケーションフリーネットワーク）の実現を目指した．また，ロケーションフリーネットワークのうち，主として講義室や会議室などの共用スペースや情報統括センター（以下，センター）が管理する全学無線 LAN など，構成員全員が利用する可能性があるサブネットや，特に文系学部のように専らユーザ端末を接続するためのサブネットについては，センターがユーザの属性（所属や身分）に応じたプライベートネットワークを「生活系ネットワーク」として提供し，ユーザ認証時のデフォルトネットワークとして利用できるようにしている．また，生活系ネットワーク以外のネットワーク（研究系ネットワーク）にも VLAN 番号を認証時に「user@VLAN-ID」の形式で指定することにより接続できるようにしている．

2.2 認証ネットワークの運用

前節で述べたように，ODnet2010 では生活系ネットワークと呼称する認証ネットワークを導入している．生活系ネットワークはプライベート IP アドレスで運用し，IP アドレスは DHCP で自動的に割り当てられる．生活系ネットワークでは 10.0.0.0/8 のプライベート IP アドレス空間を用い，次の 4 つのカテゴリーのネットワークを用いている．

- 教員用ネットワーク
- 学生用ネットワーク
- ゲスト用ネットワーク
- 学内共通ネットワーク

これらのうち，教員用ネットワーク，学生用ネットワーク，およびゲスト用ネットワークでは Web 認証が必要で，

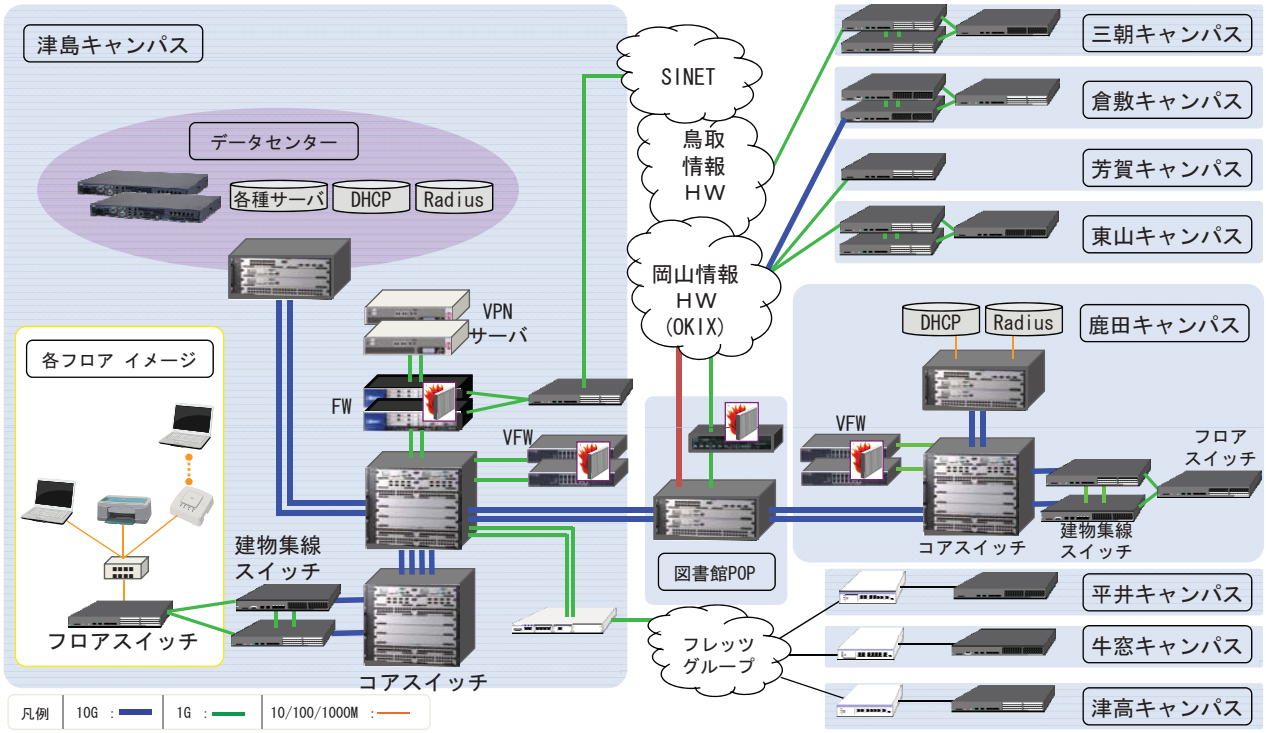

図 1 ODnet2010 の物理構成

アクセス可能範囲をキャンパスネットワーク管理者がカテゴリー単位で設定できるようになっている．また，これらのカテゴリーでは利用者の身分および所属により認証後に接続される VLAN が決定されるようになっている．したがって，IP アドレスを見ればサーバではクライアント PC 利用者の所属を判別でき，サーバ側で所属に応じた細かなアクセス制御を行うことができる．設定された VLAN は生活系ネットワークだけで 450 種類以上になる．さらに，電子ジャーナルなど場所に応じたサービスを提供するために，倉敷，三朝，東山キャンパスの生活系ネットワーク用 VLAN は VLAN-ID 変換を行ったうえで津島キャンパスのレイヤ 3 スイッチに収容されており [4]，研究系ネットワークを含めると各スイッチには仕様上利用可能な 4096 のうちの大半が設定されている．

生活系ネットワークや研究系ネットワークとは別に，各フロアスイッチには Web 認証を行うための特別の VLAN（認証前 VLAN）が必要である．この VLAN では DHCP により認証用の IP アドレスが一時的に提供される．端末が認証ネットワークを利用する場合の動作手順を以下に示す．

(1) ユーザ端末はフロアスイッチに接続されると DHCP サーバから認証用 IP アドレスを取得する．
(2) ユーザ端末は Web ブラウザで任意のページにアクセスを行う．フロアスイッチはこのアクセスを Web 認証サーバにリダイレクトする．Web 認証サーバは認証ページを Web ブラウザに表示し，ユーザ名とパスワードの入力を求める．
(3) ユーザはユーザ名とパスワードを入力する．必要であればユーザ名の一部として接続先 VLAN ID を指定する．Web 認証サーバはユーザ認証を行い，接続先 VLAN ID が指定されていた場合にはその VLAN へのアクセス権限も確認したうえで，フロアスイッチと協調して指定された VLAN に接続する．接続先 VLAN ID が明示されていない場合にはユーザ毎に割り当てられたデフォルト VLAN（多くの場合，ユーザの身分や所属に応じた生活系ネットワーク）に接続する．
(4) ユーザ端末は認証用 IP アドレスのリース切れにより IP アドレスの再取得を試みる．DHCP サーバは新たな VLAN 用の IP アドレスを割り当て，ユーザ端末はこれ以降自由にネットワークにアクセスできるようになる．
(5) ユーザ端末はネットワークから切断する際にログアウト処理を行う．ログアウト処理では端末の IP アドレスをもとに，レイヤ 3 スイッチの ARP テーブルを検索してクライアントの MAC アドレスを特定し，さらに認証ログをもとに端末が接続されているレイヤ 2 スイッチを特定したうえで，そのスイッチの認証情報を強制的に無効化する方法を用いている．

3. 大規模認証ネットワーク運用における課題

ODnet2010 の構築にあたり，特に生活系ネットワークが関連する課題がいくつか発生した．本節ではそのうちリソース不足が原因となったものを中心に述べる．

3.1 認証スイッチに起因する問題点と対策

前節で述べたように，ODnet2010 ではネットワーク接続時にユーザ認証を行い，その際に接続先 VLAN ID を指定することができる．もしユーザが他の VLAN に接続し直そうとした場合には一度ログアウトする必要がある．

当初の設計では，ログアウト処理はフロアスイッチ自身に行わせる予定であった．すなわち，フロアスイッチには Web 認証専用のアドレス（たとえば 10.10.10.10）にユーザ端末がアクセスするとログアウト画面を表示する機能を有するため，この機能を活用する予定であった．ところが，設計の途中の段階で，この機能を利用するためには各スイッチに SVI（Switch Virtual Interface）を設定し，ユーザ端末から直接スイッチにアクセスできるようにする必要があることが判明した．これはログアウトを行う必要がある各 VLAN において各フロアスイッチが 1 つの SVI を持つ必要があることを意味し，ODnet2010 の場合，フロアスイッチが約 400 台，VLAN が生活系ネットワークだけで約 450 本以上存在するため，1 つの VLAN につき SVI 用に 400 アドレス以上，1 台のフロアスイッチにつき 450 以上の SVI を設定する必要が生じる．多くの VLAN（特に既存の研究系ネットワーク）ではアドレス空間は/24 であるため，400 アドレスの設定は不可能であり，また 1 台のフロアスイッチで設定できる SVI の上限数は 100 であったことから，フロアスイッチ自身でのログアウト処理を断念し，前節で述べたように外部プログラムが端末の接続されているレイヤ 2 スイッチを特定したうえで，そのスイッチの認証情報を強制的に無効化する方法を採用している．

3.2 L3 スイッチのメモリ不足に起因する問題点と対策

ODnet2010 において，従来の旧研究系ネットワークを収容した時点では発生していなかったが，生活系ネットワークへの移行が進むにつれて L3 スイッチのメモリ不足 [*1] により顕在化した問題がいくつかある．本節ではこれらの問題とその対策について述べる．

3.2.1 メモリ不足の原因

旧研究系ネットワークでは，たとえば VLAN 内の IP アドレスを節約するため，外部からの攻撃を防止するため，あるいは機器や端末の設定を省力化するためなど様々な理由により，ユーザ側で家庭用ブロードバンドルータや無線ルータなどの機器（以下，総称して小型ルータ）を導入し，これらの機器の配下に多数のユーザ端末を接続する運用形態がしばしば見られた．このような形態ではユーザ端末には小型ルータからプライベート IP アドレスが割り当てられ，フロアスイッチからは小型ルータしか接続されていないように見えるため，見かけ上の接続台数は少なく，特に問題は発生しなかった．

[*1] 正確には IPv4 ユニキャストリソース（最大 65,536 エントリ）の不足．

ところが，認証ネットワークへの移行に伴い，このような形態では個々の端末のユーザが把握できなくなる点が問題となった．そこで，旧研究系ネットワークを認証ネットワークに移行する際にこれらの小型ルータをブリッジモードになるように設定変更を依頼した．これにより，配下の端末を個別に認証できるようになったが，これに伴いレイヤ 3 スイッチではそれまで小型ルータの配下に隠蔽されていた端末の MAC アドレスが ARP テーブルに格納されることになった．認証ネットワークへの移行が進むにつれ，レイヤ 3 スイッチの ARP テーブルに登録される MAC アドレスが増加し，最終的にオーバフローが発生して一部の端末で通信が行えない状態が発生するようになった．

上記のようにメモリ不足の直接的な原因は小型ルータのブリッジモードでの運用であるが，他にも間接的な原因が考えられる．まず，最近ではスマートフォンやタブレット PC が急速に普及しているが，これらは無線 LAN へのアクセス機能を有しているため端末台数が以前と比べて増加している点が挙げられる．また，従来のネットワークと比較するとレイヤ 3 スイッチが集約化されたため，全ての端末の MAC アドレスが唯一のレイヤ 3 スイッチに登録されることになるという，構造上の問題も挙げられる．

3.2.2 メモリ不足への対策

この問題が顕在化した時点では既に生活系ネットワークへの移行がかなり進んでいた状態であったため，ネットワークの構成を大幅に変更することは事実上不可能であった．そこで，登録される MAC アドレスの削減を図るとともに，他の方法で使用しているメモリ量を削減することになった．調査の結果，経路情報がかなり多くのメモリ量を使用していることが判明したため，その削減を図ることにした．具体的には (1)ARP キャッシュテーブルの有効期限の調整，(2)VRF の削減，(3) 経路情報の集約化の 2 点を実施した．以下では，それぞれについて詳細を述べる．

(1) ARP キャッシュテーブルのエージング時間の調整

ARP キャッシュテーブルのエージング時間は標準では 14400 秒（4 時間）であり，レイヤ 2 スイッチの MAC アドレステーブル（300 秒）と比較しても相当長く設定されている．このため，現在接続されていない端末についても ARP キャッシュテーブルに MAC アドレスが残されたままになり，メモリ使用量を押し上げる結果になっていた．特に，認証前ネットワークについては一時的にしか使用しないにも関わらず MAC アドレスが無駄に ARP キャッシュテーブルに残された状態になっていた．そこで，この値を認証前ネットワークでは 300 秒に設定することにより，ARP キャッシュテーブルのエントリ数を約 1500 減らすことができた．これ以外のネットワークについては現時点では設定変更していないが，今後実施する予定である．

(2) VRF の削減

ODnet2010 ではレイヤ 3 スイッチを集約した代わりに

レイヤ 3 スイッチ内に多くの VRF を設け，VRF 間の通信を制限することによりセキュリティを強化している．ところが，経路制御情報は各 VRF で独立して管理されるため，VRF 数に比例した数の経路情報が L3 スイッチ内で管理されることになり，メモリ消費量が増加する．そこで，似たようなポリシを持つ VRF を統合し，ポリシの違いは ACL（Access Control List）で記述することにより VRF を削減した．

(3) 経路情報の集約化

ODnet2010 では旧研究系ネットワーク，新研究系ネットワークに加え，生活系ネットワークや認証前ネットワークなど，多数のネットワークが追加されている．追加したネットワークの多くはプライベートアドレスで運用されているが，その経路情報は主として/24 単位で扱われ，同じような経路情報が個別に多数存在する状況になっていた．そこで，これらの経路情報を集約することにより，メモリ使用量を津島キャンパスで約 4000 エントリ分，鹿田キャンパスで約 6500 エントリ分削減することができた．

3.3 L3 スイッチの CPU リソース不足に起因する問題点と対策

2010 年 6 月まで稼働していた旧キャンパス情報ネットワークでは，セキュリティインシデント発生の際のトレーサビリティを高めるため，各クラスタのレイヤ 3 スイッチに定期的に SNMP により ARP キャッシュテーブルの内容を問い合わせ，記録するようにしていた．ODnet2010 においても旧キャンパス情報ネットワークの目的を引き継ぎ，同様の処理を行っていた．

ところが，この処理がレイヤ 3 スイッチの CPU リソースを消費し，CPU 使用率がほぼ 100%になる状態が定期的に発生するようになった．このため，レイヤ 3 スイッチの死活監視，3.1 節で述べたログアウト処理の他，ARP 処理や DHCP リレー処理など CPU リソースを使用する他の処理に影響を及ぼすようになった．そこで，SNMP による ARP キャッシュテーブルの問合せを中止し，その代わりに DHCP サーバや RADIUS サーバのログを用いるようにした．

3.4 その他の問題点

前稿 [1] や本稿でこれまでに述べた問題以外にも，まだ多数の問題が発生している．以下では，そのうちのいくつかを紹介する．

- プリンタに対して端末から SNMP で定期的に状態を問い合わせている状況において，端末からの SNMP request パケットが TTL を 2 つずつ減らしながら全ネットワークにフラッディングされる現象が発生している．原因は現在調査中であるが，ネットワークに接続されている小型ルータの中に宛先 MAC アドレスを無視してパケットを受け取り，中継するものが存在すると推測している．
- ODnet2010 では DHCP サーバや RADIUS サーバなどから大量のログが出力される．これを syslog サーバで記録する際，信頼性を高めるために TCP でログを送信するように設定すると，syslog サーバが単一障害点になり得る．すなわち，syslog サーバに対してログの送信ができなくなったとき，送信側ではある程度はログ情報をバッファに収容できるが，このバッファが満杯になるとログ情報の書込み中にブロックされ，動作を停止する．
- 一度認証に成功した端末をしばらく放置した後に再度利用する際，再認証が必要になる状況が発生した．利用者からの要望により，認証状態のエージング時間（正確には polling interval）を延長したが，それでも再認証が必要な状況が生じている．
- 逆に，一部では接続を解除したにも関わらず，認証状態のエージング時間を過ぎても認証状態が維持される現象も発生した．原因はある小型ルータをブリッジモードで使用した場合に小型ルータ自身が学習した MAC アドレスを逆流させているためと推測している．

4. まとめ

本稿では岡山大学における新キャンパス情報ネットワーク ODnet2010 について，特に認証ネットワークの設計と運用を紹介した．ODnet2010 では特にレイヤ 3 スイッチを集約したためにリソース不足が発生し，これに起因する様々なトラブルが発生した．大規模なネットワークの設計・運用では，調達の段階では気付かず設計段階で初めて判明したり，設計や試験運用の段階では気付かず本格的な運用を行って初めて露見したりする問題が少なからず存在する．大規模ネットワークの更新時にはカタログやマニュアルなどでは明記されていない，あるいは気付きにくい制限値についても注意を払う必要がある．

現在，ODnet2010 は旧研究系ネットワークから生活系ネットワークへの移行を継続して実行しているが，今後も様々なトラブルを経験するであろうと予想している．このようなトラブルについては，機会があれば報告したい．

本稿が他組織におけるネットワークの設計・運用の一助になれば幸いである．

参考文献

[1] 山井成良，岡山聖彦，大隅淑弘，藤原崇起，河野圭太，稗田隆: “岡山大学における大規模認証ネットワークの運用と課題”，情報処理学会インターネットと運用技術研究会研究報告，Vol.2013-IOT-20，No.10，平成 25 年 3 月．
[2] 岡山聖彦，山井成良，大隅淑弘，河野圭太，藤原崇起，稗田隆: “岡山大学における認証・ロケーションフリーネットワークの構築”，学術情報処理研究，No.15，pp.161–165，

平成 23 年 9 月.
[3] 山井成良, 岡山聖彦, 金勇, 河野圭太, 大隅淑弘：“岡山大学における地域 IX と SINET を利用したネットワーク冗長化”, 情報処理学会インターネットと運用技術研究会研究報告, 2009-IOT-004-20, pp.113–118, 平成 21 年 3 月.
[4] 大隅淑弘, 岡山聖彦, 山井成良, 藤原崇起, 稗田 隆: “電子ジャーナルの地理的なサイトライセンス契約条件に適応するロケーションフリーネットワークシステム”, 情報処理学会インターネットと運用技術研究会インターネットと運用技術シンポジウム 2011 論文集, pp.51–58, 平成 23 年 12 月.