宮崎大学情報基盤センター年報
2016

宮崎大学
情報基盤センター

目次

1　平成 28 年度活動報告

1.1　会議・定例会等

【情報化推進会議】

○第１回（平成 28 年 7 月 28 日）

議題：１．平成 27 年度決算について
　　２．平成 28 年度事業計画について
　　３．平成 28 年度予算について

報告：１．平成 27 年度学部・研究科等の自己点検報告書について
　　２．平成 28 年度情報セキュリティ監査について
　　３．平成 28 年度情報セキュリティ講習について

○第 2 回（平成 28 年 10 月 24 日～27 日：メール会議）

議題：１．平成２８年度計画 統括体制 実施状況等（中間報告）（案）について

○第 3 回（平成 28 年 12 月 1 日～5 日：メール会議）

議題：１．第 3 期中期計画の検証及び平成 29 年度計画等の作成について

○第 4 回（平成 29 年 2 月 10 日～14 日：メール会議）

議題：１．第 3 期中期計画の検証及び平成 29 年度計画等の検証結果について

○第 5 回（平成 29 年 3 月 15 日）

議題：１．情報セキュリティ対策基本計画について
　　２．中期目標・中期計画に係る平成２８年度計画の実施状況等（最終報告）について

報告：１．平成２８年度情報セキュリティ監査中間報告について
　　２．平成２８年度情報セキュリティ対策講習の実施状況について
　　３．平成２９年度情報セキュリティ対策講習について
　　４．Web サーバ管理者・コンテンツ管理者向け講習会について
　　５．「eduroam」「FreeSpot」サービスの提供について

【情報基盤センター運営委員会】

○第１回（平成 28 年 4 月 25 日～27 日：メール会議）

議題：１．平成２８年度の実施事項の作成について
　　２．平成２７年度情報基盤センター自己評価報告書について

○第 2 回（平成 28 年 6 月 6 日）

議題：１．平成２７年度決算報告について
　　２．平成２８年度事業計画（案）について
　　３．情報基盤センターハウジング機器の電気代徴収について
　　４．平成２８年度予算案について

報告：１．平成２７年度事業報告について
　　２．情報セキュリティインシデントについて

○第 3 回（平成 28 年 9 月 21 日～27 日：メール会議）

議題：１．中期目標・中期計画に係る平成２８年度計画の実施状況等（中間報告）の

調査について
２．平成２７年度情報基盤センター自己評価報告書の点検結果について
○第４回（平成 28 年 12 月 20 日）
議題：１．宮崎大学 FreeSpot 利用規約について
報告：１．情報システムに関するアンケートの実施について
○第５回（平成 29 年２月 23 日～28 日：メール会議）
議題：１．中期目標・中期計画に係る平成２８年度計画の実施状況等（最終報告）について
○第６回（平成 28 年 12 月 20 日）
議題：１．宮崎大学 FreeSpot 利用規約について
報告：１．情報システムに関するアンケートの実施について

【情報セキュリティ委員会】
○第１回（平成 28 年４月 28 日～５月 10 日：メール会議）
議題：１．情報セキュリティ対策の運用管理部局に関する申合せの一部改正（案）について
○第２回（平成 28 年７月 28 日）
議題：１．情報セキュリティインシデントの再発防止策について
２．「情報セキュリティ対策基本計画」の策定について
３．情報セキュリティ講習受講義務化における年度途中赴任者・入学者への対応について
報告：１．平成 28 年度情報セキュリティ監査について
２．平成 25～27 年度情報セキュリティ対策講習会未受講者について
３．平成 28 年度情報セキュリティ対策講習会（対面・集合）について
○第３回（平成 28 年９月 23 日）
議題：１．宮崎大学情報セキュリティインシデント対応チーム要項の一部改正等について
報告：１．情報基盤センターの業務フローの見直しについて
２．平成 28 年度情報セキュリティ対策講習会について
３．eーラーニングによる情報セキュリティ対策講習について
○第４回（平成 28 年 10 月 17 日～20 日：メール会議）
議題：１．国立大学法人宮崎大学保有個人情報管理規程の一部改正について
○第５回（平成 28 年 10 月 24 日～27 日：メール会議）
議題：１．「大学間連携に基づく情報セキュリティ体制の基盤構築」の試行運用への協力の可否について
○第６回（平成 28 年 12 月 19 日）
協議題：１．宮崎大学における情報セキュリティ対策基本計画について
報告：１．部局運用 WEB サイトのファイル調査結果について
その他：１．教員が個人情報を保存して使用する USB メモリ等の管理について

２．平成２８年度情報セキュリティ対策講習の受講状況について

○第 7 回（平成 29 年 3 月 13 日）

議題：１．情報セキュリティ対策基本計画について
２．情報の格付けについて
３．平成２９年度情報セキュリティ対策講習について

報告：１．平成２８年度情報セキュリティ監査中間報告について
２．平成２８年度情報セキュリティ対策講習の実施状況について
３．Web サーバ管理者・コンテンツ管理者向け講習会について
４．大学間連携に基づく情報セキュリティ体制の基盤構築試行運用の開始について

【情報セキュリティ担当者連絡会】

○第 1 回（平成 28 年 4 月 20 日～22 日：メール会議）

議題：１．情報セキュリティ対策の運用管理部局に関する申合せの一部改正（案）について

○第 2 回（平成 28 年 7 月 1 日）

議題：１．平成２８年度情報セキュリティ監査（案）について
報告：１．部局情報技術責任者及び部局情報技術責任補助者について
２．情報セキュリティインシデントについて
３．部局運用 WEB サイトのファイル調査について
４．平成 28 年度国立大学法人等最高情報セキュリティ責任者会議について

○第 3 回（平成 28 年 10 月 26 日）

議題：１．教員が個人情報を保存して使用する USB メモリの管理について
報告：１．宮崎大学情報セキュリティインシデント対応チーム要項の一部改正等について
２．平成２８年度情報セキュリティ監査（中間報告）について
３．平成２８年度情報セキュリティ対策講習の開始について

○第 4 回（平成 29 年 3 月 9 日）

議題：１．情報の格付けについて
２．平成２９年度情報セキュリティ対策講習について
報告：１．情報セキュリティ対策基本計画について
２．平成２８年度情報セキュリティ監査中間報告について
３．平成２８年度情報セキュリティ対策講習の実施状況について
４．Web サーバ管理者・コンテンツ管理者向け講習会について

【情報セキュリティ対策基本計画策定 WG】

○第 1 回（平成 28 年 8 月 31 日）

報告：１．情報セキュリティ委員会からの報告について
２．情報セキュリティ対策基本計画の策定について
協議題：１．WG のスケジュールについて

○第 2 回（平成 28 年 10 月 24 日）
議題：１．情報セキュリティ対策基本計画の策定について
その他：１．次回 WG の開催について
○第 3 回（平成 28 年 11 月 17 日）
議題：１．情報セキュリティ対策基本計画の策定について
２．次回 WG の開催について
○第 4 回（平成 28 年 12 月 1 日）
議題：１．情報セキュリティ対策基本計画の策定について
○第 5 回（平成 28 年 12 月 7 日）
議題：１．情報セキュリティ対策基本計画の策定について
○第 6 回（平成 28 年 12 月 15 日～16 日：メール会議）
議題：１．情報セキュリティ対策基本計画の策定について
○第 7 回（平成 29 年 2 月 24 日）
議題：１．情報セキュリティ対策基本計画の策定について

【センター部局情報技術責任補助者会議】
○第 1 回（平成 28 年 11 月 21 日）
議題：１．センター教員が個人情報を保存して使用する USB メモリ等の管理についての申合せについて
○第 2 回（平成 28 年 12 月 16 日～19 日：メール会議）
議題：１．センター教員が個人情報を保存して使用する USB メモリ等の管理についての申合せについて

1.2　研究会・研修会等への参加状況

(1) NetApp Cloud Champions、デモンストレーション及びハンズオントレーニング、デモンストレーション及び検証（平成 28 年 4 月 20～22 日、東京）
(2) 情報セキュリティ EXPO、宮崎大学統一認証システム改修打合せ（平成 28 年 5 月 12～13 日、リードエグジビションジャパン株式会社主催、東京）
(3) 教育 IT ソリューション EXPO（平成 28 年 5 月 18～20 日、リードエグジビションジャパン株式会社主催、東京）
(4) 大学 ICT 推進協議会総会（平成 28 年 5 月 19 日、大学 ICT 推進協議会主催、東京）
(5) 第 9 回 ISMS 研修会（平成 28 年 5 月 26～27 日、山口大学主催、山口）
(6) Interop Tokyo2016（平成 28 年 6 月 8～10 日、Interop Tokyo 実行委員会主催、東京）
(7) シスコ アカデミックフォーラム 2016、セキュリティソリューション技術商会（平成 28 年 6 月 14～16 日、シスコシステムズ主催、東京）
(8) 第 13 回国立大学法人情報系センター協議会総会（平成 28 年 6 月 24～25 日、国立大学法人情報系センター協議会主催、京都）
(9) 国立大学法人等最高情報セキュリティ責任者会議（平成 28 年 6 月 29 日、文部科学省主催、東京）
(10) SINET 接続の打合せ、NetBoot,Zstrage 検証（平成 28 年 7 月 7～8 日、東京）
(11) 第 41 回九州大学情報基盤研究開発センター会議（平成 28 年 7 月 29 日、九州大学主催、福岡）
(12) 国立大学法人情報系センター研究集会、学術情報処理研究集会（平成 28 年 9 月 26～27 日、国立大学法人情報系センター協議会主催、滋賀）
(13) 平成 28 年度情報セキュリティ技術向上研修（平成 28 年 10 月 5～8 日、福岡）
(14) 情報セキュリティ EXPO（平成 28 年 10 月 26～28 日、リードエグジビションジャパン株式会社主催、千葉）
(15) 文部科学省関係機関 CISO 会議（平成 28 年 11 月 18 日、文部科学省主催、東京）
(16) SINET・学術情報基盤サービス説明会（平成 28 年 12 月 5～6 日、国立情報学研究所主催、福岡）
(17) 大学 ICT 推進協議会 2016 年次大会（平成 28 年 12 月 14～16 日、大学 ICT 推進協議会主催、京都）
(18) Security Days 福岡 2017（平成 29 年 1 月 30～31 日、株式会社ナノオプト・メディア主催、福岡）
(19) 2016 年度 IS 研九州ブロック研究会（平成 29 年 2 月 17～18 日、富士通株式会社主催、熊本）
(20) IS 研総会（平成 29 年 2 月 21～22 日、富士通株式会社主催、大阪）
(21) 文部科学省情報セキュリティセミナー（平成 29 年 2 月 27 日、文部科学省主催、

東京）

(22) 第 10 回統合認証シンポジウム（平成 29 年 2 月 28 日、佐賀大学主催、佐賀）

(23) SINET 接続打ち合せ、NII-SOC 研修、NIPC 事務局打ち合せ（平成 29 年 3 月 14 ～16 日、東京）

1.3　情報セキュリティ監査報告

平成 29 年 6 月 30 日

平成 28 年度 情報セキュリティ監査　報告書

1. 目的

宮崎大学情報セキュリティ基本規程第 9 条に基づき、本学の情報システムのセキュリティ対策が情報セキュリティポリシー及び関連規程に基づき実施されているかを点検するために、平成 24 年度から情報セキュリティ監査を行っている。平成 25 年には、平成 28 年度までの 4 年間で全ての研究室・部門の監査を行うことを決定し、年一回の監査を計画的に行ってきた。本年度はその最終年度に当たる。

２．監査手順

以下の手順により監査を実施した。

(1) 監査対象研究室の選定

部局情報技術責任者は、これまで監査が未実施の研究室を対象に監査計画を立案し、当該年度の監査対象研究室を情報基盤センターに報告する。

(2) 事前調査表による書面監査

監査対象研究室の責任者は、宮崎大学情報セキュリティ実施要項に定める情報セキュリティ対策の遵守状況を事前調査票（Excel）に記入し、情報基盤センターは事前調査票をもとに書面監査を行う。

(3) 実地監査

情報基盤センターの教員 1 名が監査人となり実地監査を行う。監査人は、監査対象研究室の責任者及び部局情報技術責任者又は部局情報技術責任補助者の立会いのもと研究室を巡視し、事前調査票の記載事項に間違いがないかを数台の情報機器を抽出して点検する。セキュリティ対策に問題がある場合は、監査対象研究室の責任者に改善の助言を行い、可能であれば改善をその場で実施する。

(4) 監査結果の報告

情報基盤センターは、監査結果のまとめを部局情報セキュリティ責任者に報告する。また、実地監査で問題が解決されなかった場合には、当該研究室の責任者に改善点を示した改善勧告書を送付する。

(5) 改善報告書の提出

改善勧告を受けた責任者は、指示されたセキュリティ対策を実施し、改善報告書を情報基盤センターに提出する。

３．監査項目

宮崎大学情報セキュリティ実施要項は、情報機器をクライアント機器、サーバ機器、ネットワーク機器の 3 種類に分類し、それぞれに対して実施すべき最低限のセキュリティ対策を定めている。実施要項に従い表１の監査項目を設定した。

表１　監査項目一覧

情報機器	監査項目	関連規定
クライアント機器	セキュリティアップデート	実施要項第 4 条 5 項(1)
	不正プログラム対策	実施要項第 4 条 5 項(2)
サーバ機器	セキュリティアップデート	実施要項第 4 条 4 項(1)
	ログ取得、時刻同期	実施要項第 4 条 4 項(2)
	アクセス制限	実施要項第 4 条 4 項(3)
	利用者制限	実施要項第 4 条 4 項(4)
	入退出管理	実施要項第 4 条 4 項(5)
	不正プログラム対策	実施要項第 4 条 4 項(6)
ネットワーク機器	セキュリティアップデート	実施要項第 4 条 3 項(1)
	ログ取得、時刻同期	実施要項第 4 条 3 項(2)
	アクセス制限	実施要項第 4 条 3 項(3)
	利用者制限	実施要項第 4 条 3 項(4)

４．監査の実施

平成 27 年度までに監査を実施していない全ての研究室等を監査対象とした。これまでに全部門の監査を終えた部局（センター、事務局）を除いた、教育学部、工学教育研究部、医学部、農学部、地域資源創成学部で監査を実施した。

監査人は情報基盤センターの松澤助教が務め、書面監査は、平成 28 年 6 月 16 日～平成 28 年 7 月 31 日に、実地監査は、平成 28 年 8 月 18 日～平成 28 年 10 月 13 日、平成 29 年 2 月 27 日～平成 29 年 4 月 12 日に行った。監査対象研究室は、教育学部 38 研究室、医学部 14 分野・課、工学教育研究部 28 研究室、農学部 16 研究室、地域資源創成学部 24 研究室である。実地監査の実施日と監査対象研究室を表２に示す。

当初、9 月までに監査を終える予定であったが、学部行事等で日程の調整がつかず、地域創成学部の 2 研究室及び教育学部の 6 研究室の監査は 10 月 13 日までかかった。また、教育学部の 10 研究室については、部局情報技術責任者から監査対象研究室の責任者への連絡がつかず、10 月 13 日までに監査を実施することができなかった。また、監査人と部局情報技術責任者の間で未監査の研究室についての情報共有がされていなかったため対応が遅れ、年度末に監査を実施した。

監査対象機器は、クライアント機器 726 台、サーバ機器 16 台、ネットワーク機器 123 台

である。クライアント機器の OS の内訳は、Windows 597 台、Mac 87 台、Linux 37 台、モバイル OS 5 台である。サーバ機器の OS の内訳は、Windows 1 台、Linux 15 台である。ネットワーク機器の内訳は、ネットワークプリンタ（複合機を含む）89 台、無線 LAN アクセスポイント 20 台、ネットワーク接続ストレージ（NAS）11 台、その他 3 台である。監査対象機器の部局別台数と種別台数を表３、表４に示す。

表３　監査対象機器の台数（部局別）

情報機器	教育学部	医学部	農学部	工学教育研究部	地域資源創成学部	計
クライアント機器	115	178	57	333	43	726
サーバ機器	1	1	1	13	0	16
ネットワーク機器	15	47	11	45	5	123

表４　監査対象機器の台数（種別）

情報機器	種別	台数
クライアント機器	Windows	597
	Mac	87
	Linux	37
	モバイル OS	5
サーバ機器	Windows	1
	Linux	15
ネットワーク機器	プリンタ・複合機	89
	無線 LAN アクセスポイント	20
	ネットワーク接続ストレージ	11
	その他	3

５．監査結果

実地監査では、事前調査票の記載事項に間違いがないかを数台の情報機器を抽出して点検を行った。実地監査を行った情報機器の学部別台数を表５に示す。監査対象台数に対するサンプル調査実施台数の割合は、クライアント機器が約 30%、サーバ機器とネットワーク機器が、それぞれ約 90%であった。サンプル調査とはいえ、サーバ機器とネットワーク機器については、監査対象機器の大半に対して実地監査を行っている。

実地監査でセキュリティ対策上の問題が見つかった際には、監査対象研究室の責任者に改善の助言を行い、可能であれば改善をその場で実施するが、その場で改善できない場合には情報基盤センターが当該機器を管理する研究室等の責任者に改善勧告を行う。実地監査時の改善件数を表５に示す。

今回の改善勧告は工学教育研究部のサーバ機器に対する１件であった。当該サーバは、工学部の学生・大学院生に対するｅラーニングシステムのサーバで、ｅラーニングソフトウェアのセキュリティアップデートが行われていなかった。ｅラーニングソフトウェアの保守契約を結んでいなかったため、すぐにアップデートすることができず、改善勧告となった。工学部教務委員会で対応が検討され、ｅラーニングサービスの提供を終了し、当該サーバを停止した旨の改善報告書が提出された。

クライアント機器については、定期的なセキュリティアップデートの未実施が実地監査台数の約 25%に見られ、教育学部と工学教育研究部で特に不備が多かった。教育学部では実習室 PC にまとまって不備が見つかり、工学教育研究部では Linux をインストールした PC に不備が多かった。また、不正プログラム対策の不備も実地監査台数の約 30%に見られた。不正プログラム対策は、ウイルス対策ソフトをインストールし、ウイルス定義ファイルの更新、定期的なシステムスキャンを行うことが必要だが、システムスキャンのスケジュール設定を行っていなかったり(Mac)、コンピュータが動作していない時間帯にスケジュールを設定したり(Windows)して、定期的なシステムスキャンが行われていない例が多かった。前年度の監査でも不正プログラム対策の不備は同程度（約 30%）であり、改善が進んでいないことがわかる。

サーバ機器については、必要最低限のセキュリティ対策はおおむね取られており、不備は４件であった。

ネットワーク機器については、ネットワークプリンタや無線アクセスポイントの利用者制限の不備が監査台数の約 40%に見られた。利用者制限の不備とは、機器の管理者のパスワードが設定されていないか、購入時の初期パスワードを変更しないで運用していることである。これらの機器は設定を Web で行っており、ネットワークを介して誰でも機器の設定変更や内部に蓄えられた情報の閲覧が可能になっていた。現在、学外から学内へのネットワークアクセスは許可制となっており学外からアクセスされることはないが、同一セグメント内または学内からはアクセスが可能となっており、危険な状態になっていた。前年度の監査でも約 30%の機器に利用者制限の不備があり、この点も改善が進んでいない。

表５　実地監査台数と実地監査時の改善件数

情報機器	監査項目	教	医	農	工	地	計
クライアント機器	セキュリティアップデート	34	3	0	17	0	54
	不正プログラム対策	13	11	7	24	5	60
	実地監査台数	79	38	21	54	26	218
サーバ機器	セキュリティアップデート	1	0	0	0	0	1
	ログ取得、時刻同期	0	0	0	0	0	0
	アクセス制限	0	0	1	1	0	2
	利用者制限	0	0	0	0	0	0

	入退出管理	1	0	0	0	0	1
	不正プログラム対策	0	0	0	0	0	0
	実地監査台数	1	0	1	13	0	15
ネットワーク機器	セキュリティアップデート	0	0	0	7	0	7
	ログ取得、時刻同期	0	0	0	0	0	0
	アクセス制限	0	0	0	0	0	0
	利用者制限	3	18	5	14	4	44
	実地監査台数	15	33	11	38	5	102

教：教育学部　医：医学部　農：農学部　工：工学部　地：地域資源創成学部

６．まとめ

平成 24 年度から本年度まで年１回の情報セキュリティ監査を行い、全学の監査を終えた。本年度はサーバのセキュリティアップデートについて１件の改善勧告があったが、直ぐに対策が取られており、本学のセキュリティ対策の実施状況は概ね良好である。しかし、実地監査時にセキュリティ対策の不備が指摘され、その場で改善された機器の台数は少なくない。クライアント機器では不正プログラム対策の不備が多く、ウイルス対策ソフトはインストールされているが、設定の不備で定期的なシステムスキャンが行われていない機器が多数あった。また、ネットワーク機器では管理者パスワードの未設定が多かった。この傾向と不備のあった機器の割合は昨年度とほぼ同じであり、注意すべき点が他の教職員に伝わっていっていないことを伺わせる。セキュリティ対策についての広報活動をこれまで以上に行い、周知を図っていく必要がある。

今回の監査では、監査責任者、監査人、部局情報技術責任者、監査対象研究室の責任者の連絡体制に問題があり、一部の研究室の監査実施が大幅に遅れてしまった。今後、監査の円滑な実施のために、監査の手順や連絡体制を明確にし、規程化していくことが望まれる。また、監査に係る負担を軽減するために、受審者向けのマニュアルの整備も必要である。

2　統計情報

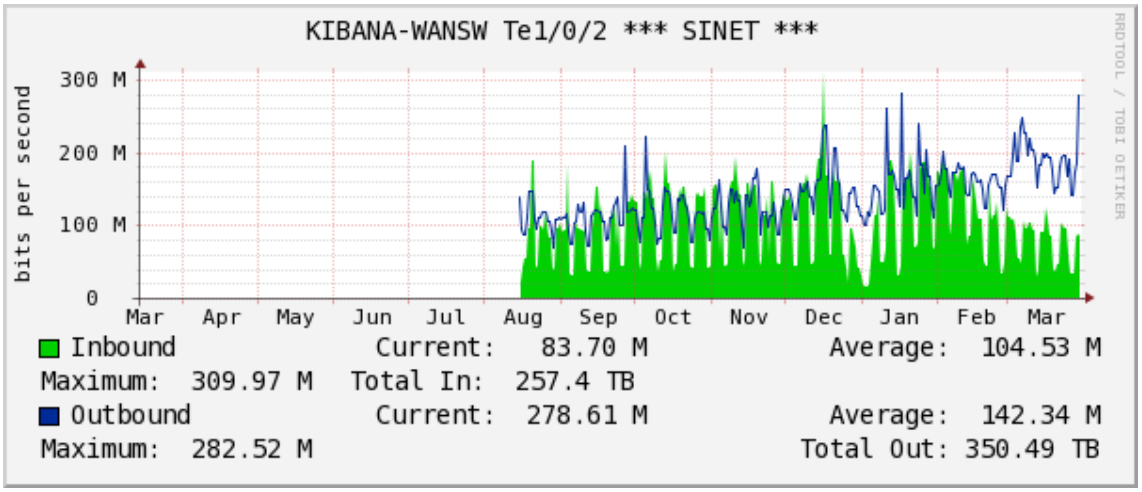
2016 年 4 月から 2017 年 3 月までの、ネットワーク、メール、仮想サーバ、パソコン実習室、宮大どこプリ、マイクロソフト包括ソフトウェア、大判プリンタ、オンラインストレージについて利用量を集計した。

2.1　ネットワーク

ネットワークトラフィック量の変化を以下の図に示す。ネットワーク統計は、1 日のトラフィック量を平均したものである。学内から学外へのトラフィック量が平均 142Mbps 程度、学外から学内へのトラフィック量が 105Mbps 程度であり、昨年度と比較すると学内、学外共にトラフィック量が増えており、年々増える傾向にある。今後もトラフィックは増えていくものと予想される。

また、各部局のトラフィック量は、事務局・図書館、教育文化学部、農学部、工学部、情報基盤センターの順に多くなっている。この傾向は毎年度変化がない。情報基盤センターのトラフィックが 100Mbps 程度で一番多く、次いで工学部、その他の部局は大きな差は見られなかった。さらに、平成 28 年度の途中より、ネットワーク構成が変更され、清武キャンパスからも学外ネットワークへ直接接続する構成となり、これまで木花キャンパスを経由して学外と通信していたものが、直接清武キャンパスから出入りすることとなった。これにより、木花-清武間の通信は学内通信のみとなり、キャンパス間のトラフィックは減少したものと考えられ、その通信量は数 Mbps 程度であった。

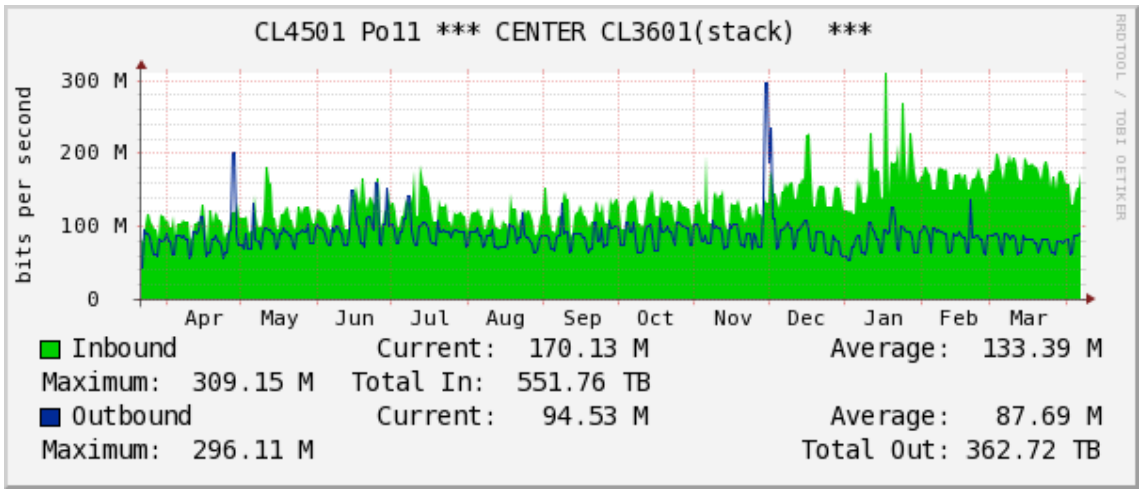
2.1.1 宮崎大学外部接続トラフィック



注1）　Inbound：学外から学内への通信

注2）　Outbound：学内から学外への通信

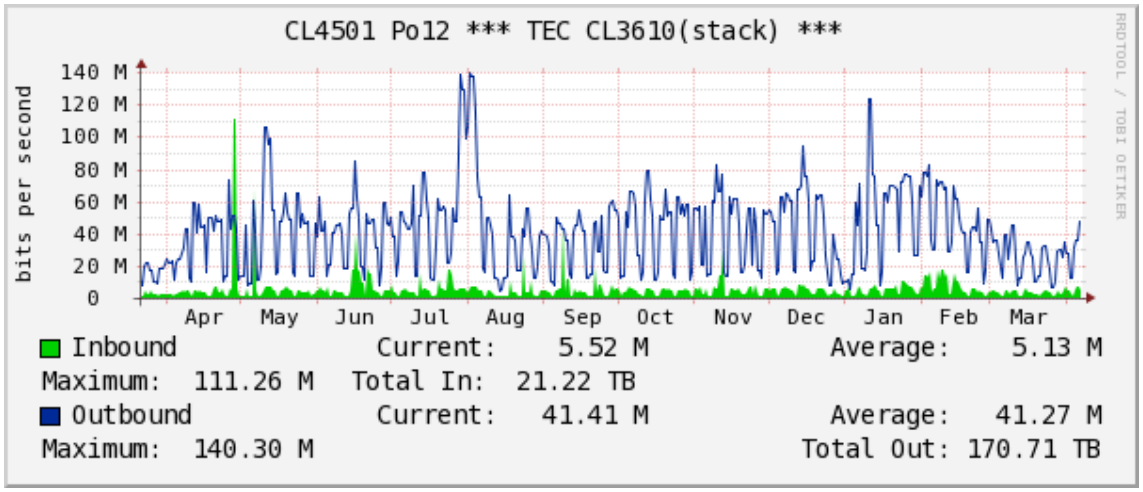
2.1.2 情報基盤センター外部接続トラフィック



注3)　Inbound：情報基盤センター内から情報基盤センター外への通信

注4)　Outbound：情報基盤センター外から情報基盤センター内への通信

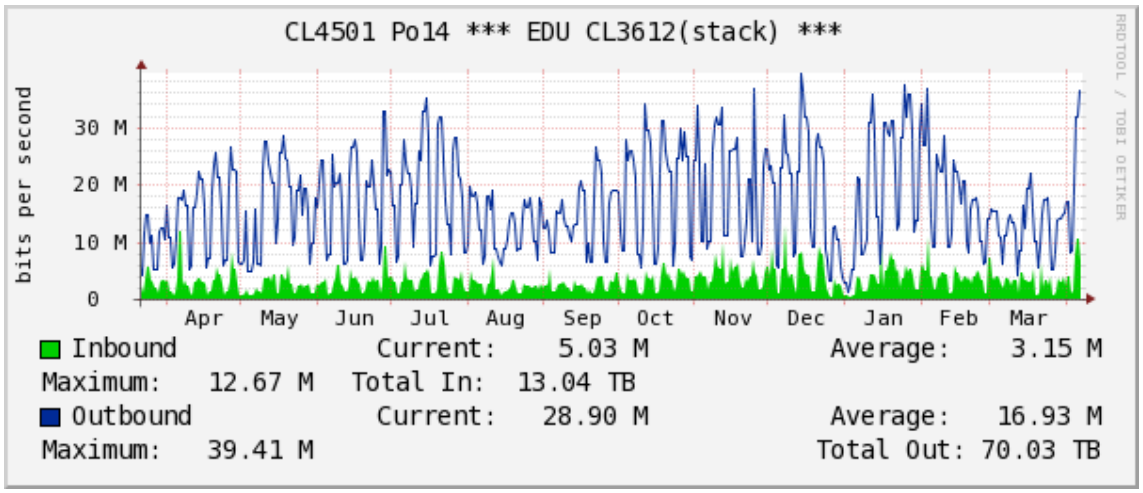
2.1.3 工学部外部接続トラフィック



注5)　Inbound：工学部内から工学部外への通信

注6)　Outbound：工学部外から工学部内への通信

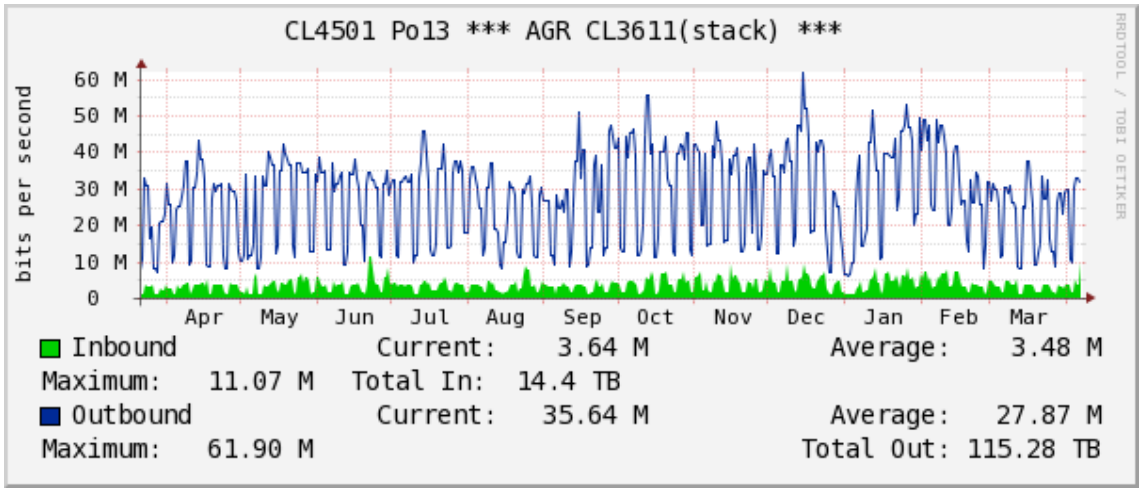
2.1.4 教育文化学部外部接続トラフィック



注7）　Inbound：教育文化学部内から教育文化学部外への通信

注8）　Outbound：教育文化学部外から教育文化学部内への通信

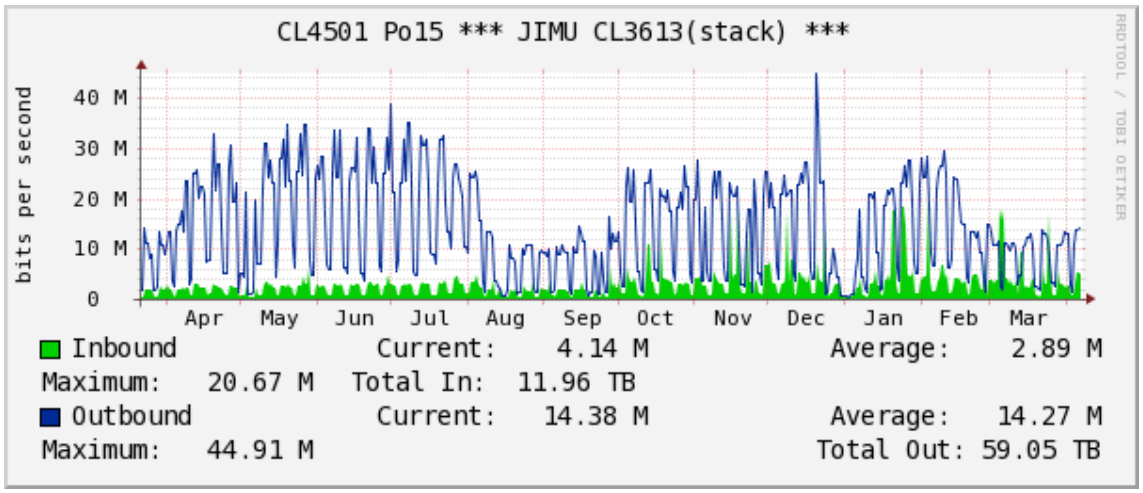
2.1.5 農学部外部接続トラフィック



注9）　Inbound：農学部内から農学部外への通信

注10）　Outbound：農学部外から農学部内への通信

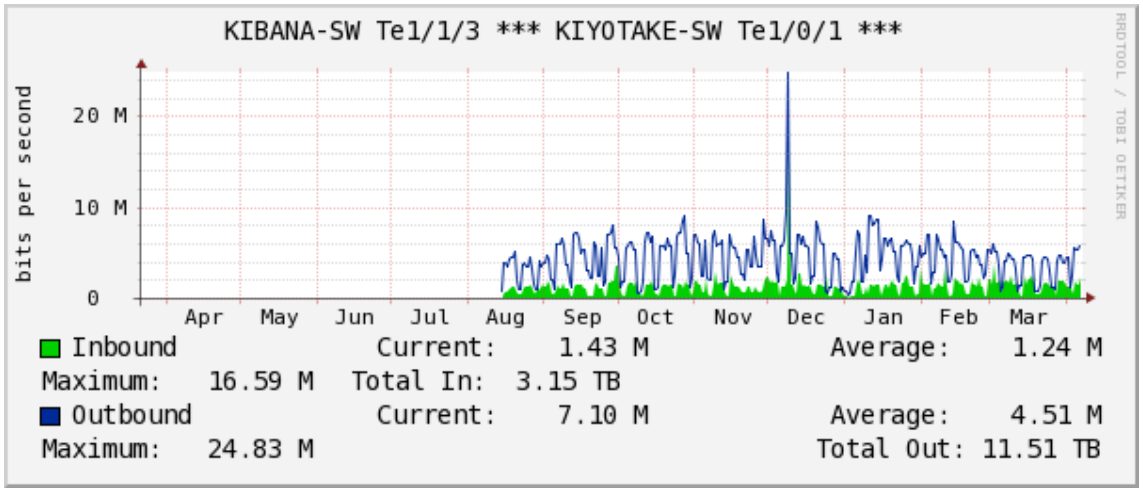
2.1.6 事務局・図書館外部接続トラフィック



注11）　Inbound：事務局・図書館内から事務局・図書館外への通信

注12）　Outbound：事務局・図書館外から事務局・図書館内への通信

2.1.7 木花キャンパス－清武キャンパス間トラフィック



注13）　Inbound：木花キャンパスから清武キャンパスへの通信

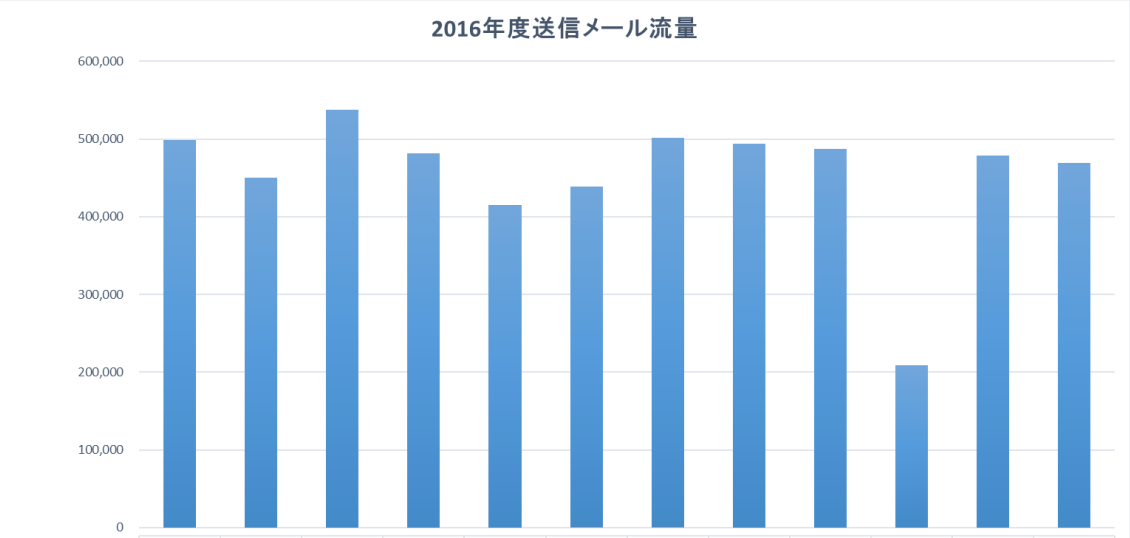
注14）　Outbound：清武キャンパスから木花キャンパスへの通信

2.2　メール

メールの送信量については、毎月 200,000～550,000 通程度で、昨年度と比べると同程度となっている。送信されたメールのほとんどが正常メールであり、コンテンツフィルタにブロックされた物やスパムとして検出されたものはなかった。しかし、ウィルスとして検出されたものがほぼ毎月一定程度確認されている。特に、9 月に多く検出されている。これらのウィルスメールは送信メール全体に対し極めて少なく、かつフィルタによって正常にブロックされていることから、外部に対して被害を与えていないものと考えられる。

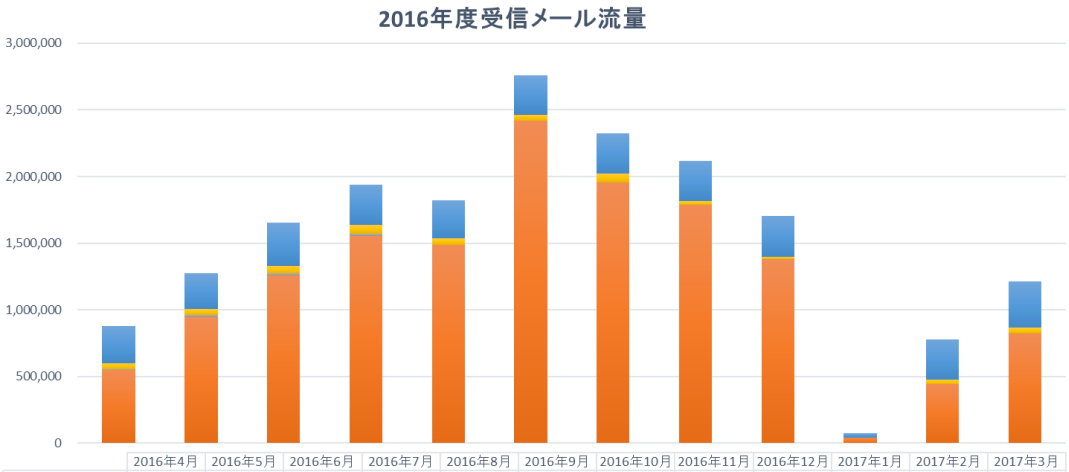
メールの受信量については、受信メールのうち、正常メールは 20%程度で毎月おおよそ一定であるが、多くを占める不正なメールは月毎に変動し、特に 9 月が多くなっている。昨年度と比較すると、正常メールの数に大きな変化は見られないものの、ブロックされる不正メールの量が増えている。

2.2.1 メール送信数



	2016年4月	2016年5月	2016年6月	2016年7月	2016年8月	2016年9月	2016年10月	2016年11月	2016年12月	2017年1月	2017年2月	2017年3月
正常メール	498,528	450,312	537,214	481,289	414,519	438,667	501,288	493,828	487,450	208,582	478,744	469,083
コンテンツフィルタによってブロック	0	0	0	0	0	0	0	0	0	0	0	0
ウイルス検出	26	136	201	121	156	403	293	53	41	0	23	7
スパム検出	0	0	0	0	0	0	0	0	0	0	0	0

2.2.2 メール受信数



	2016年4月	2016年5月	2016年6月	2016年7月	2016年8月	2016年9月	2016年10月	2016年11月	2016年12月	2017年1月	2017年2月	2017年3月
正常メール	284,189	267,516	317,594	301,946	286,070	292,119	302,475	300,209	301,683	32,051	301,459	344,929
コンテンツフィルタによってブロック	14	15	31	10	19	9	17	7	11	1	7	6
ウイルス検出	61	1,255	5,529	1,361	827	485	1,721	288	207	8	877	254
スパム検出	44,324	45,583	55,676	64,153	46,986	49,599	67,159	24,928	17,587	2,788	34,504	45,852
無効な受信者としてブロック	1,820	17,890	17,335	18,112	91	134	224	168	173	15	164	148
レピュテーションによるブロック	550,234	944,526	1,259,476	1,553,845	1,487,641	2,416,282	1,954,410	1,790,405	1,382,026	38,955	443,106	823,014

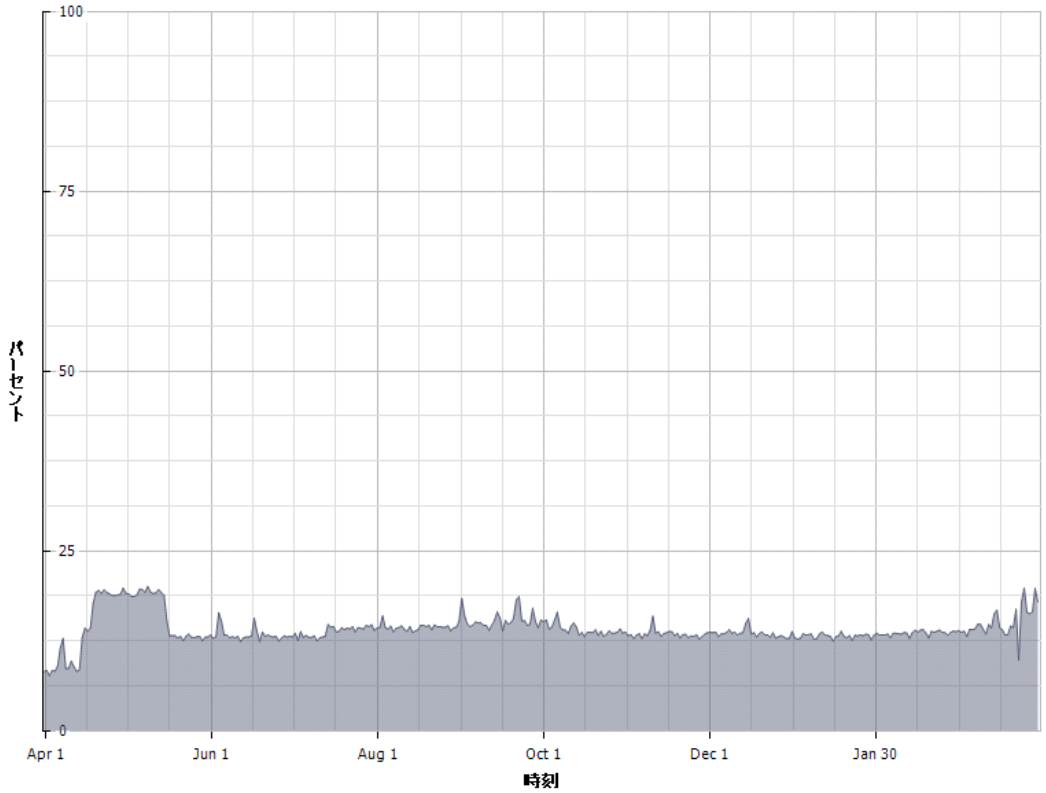
2.3　仮想サーバ

16 枚のブレードサーバで仮想サーバサービスを提供しており、ブレードサーバそれぞれについて CPU 使用率、メモリ使用率、ネットワーク I/O 量についてまとめた。

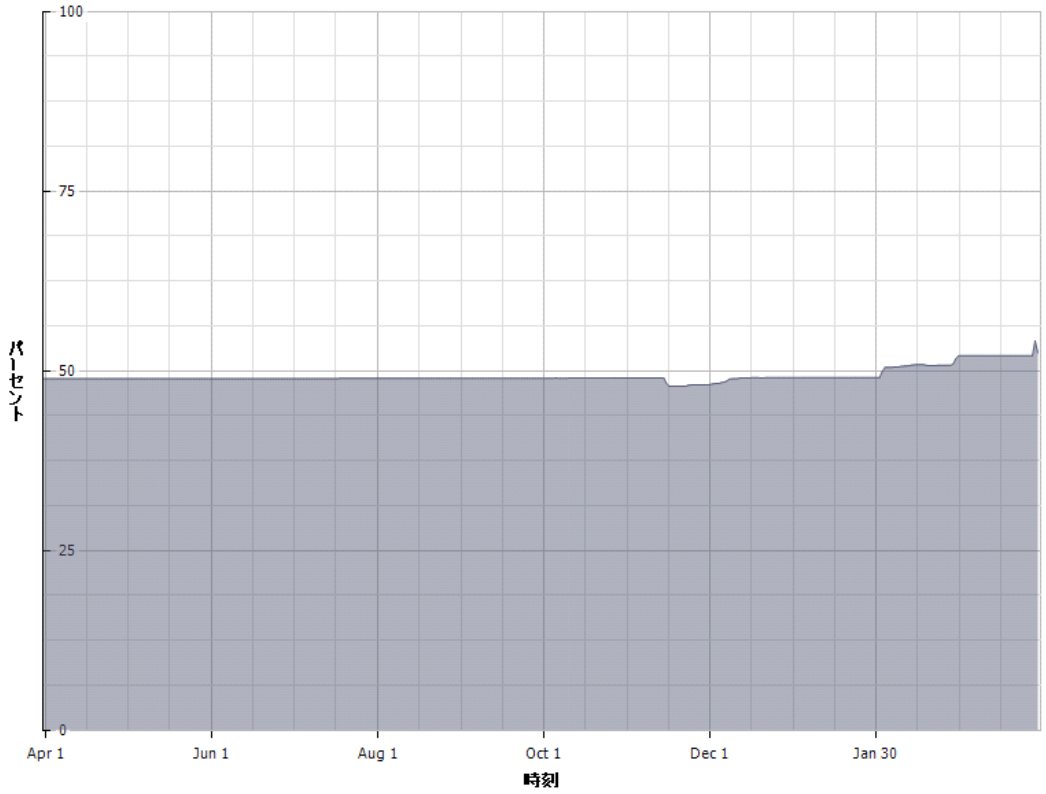
全般的に CPU 使用率、ネットワーク I/O 量については、短期的に上昇することがあるものの、定常的にはそれほど高くない状態で稼働しており、かなり余裕があるものと考えられる。メモリの使用率については、概ね 50%程度で稼働しているものがほとんどであるが、中には 90%を超えているものもあり、年々増加する仮想サーバの台数に対応するため、配置のバランスを考える必要がある。まだ物理資源には余裕が見られることから、更に新たな仮想サーバを設置する余裕があるものと考えられる。

2.3.1 ESX1

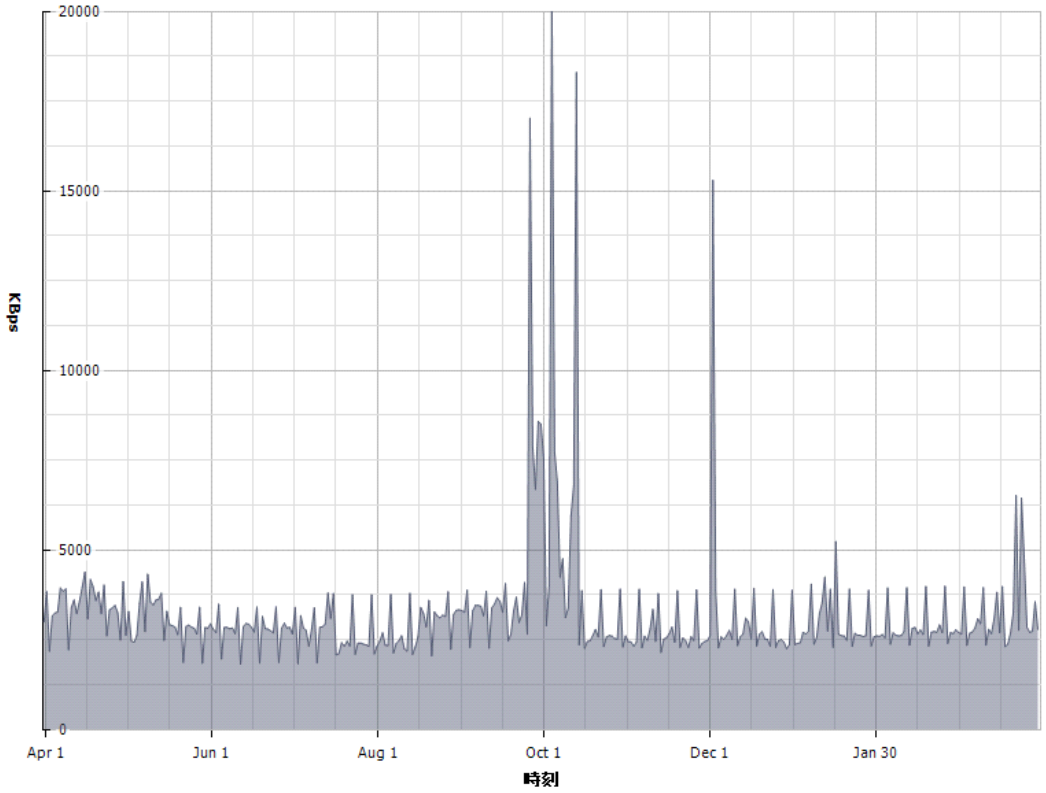
CPU 使用率



メモリ使用率

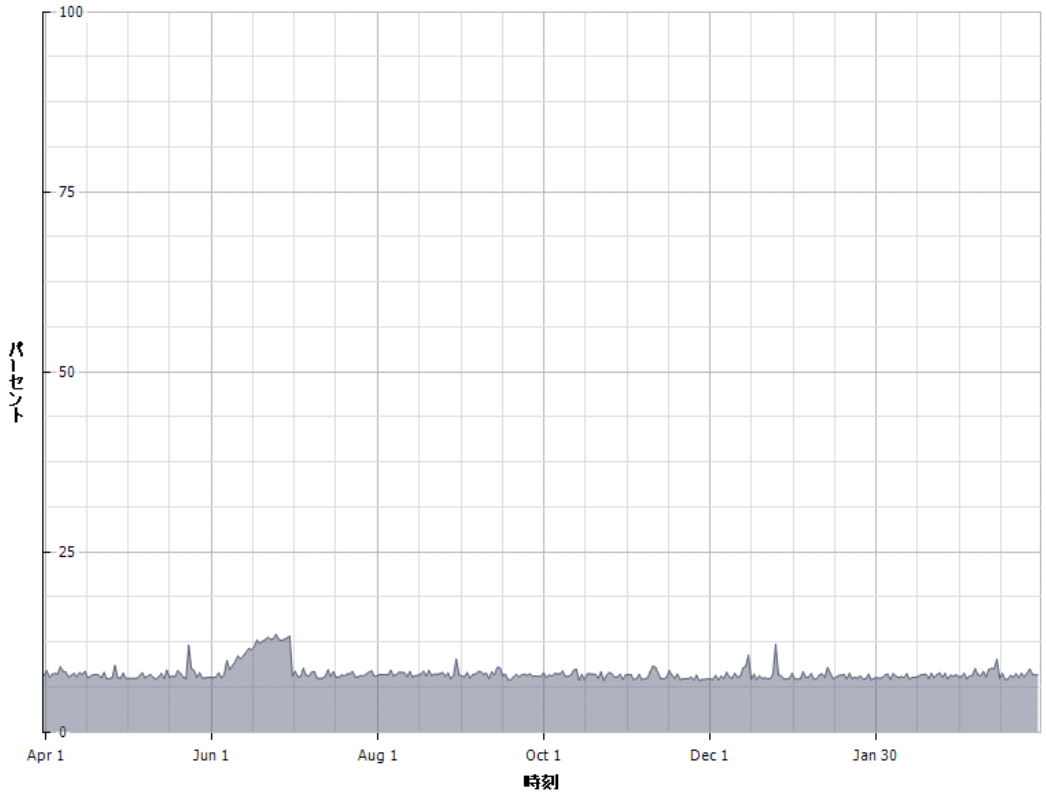


ネットワーク I/O 量

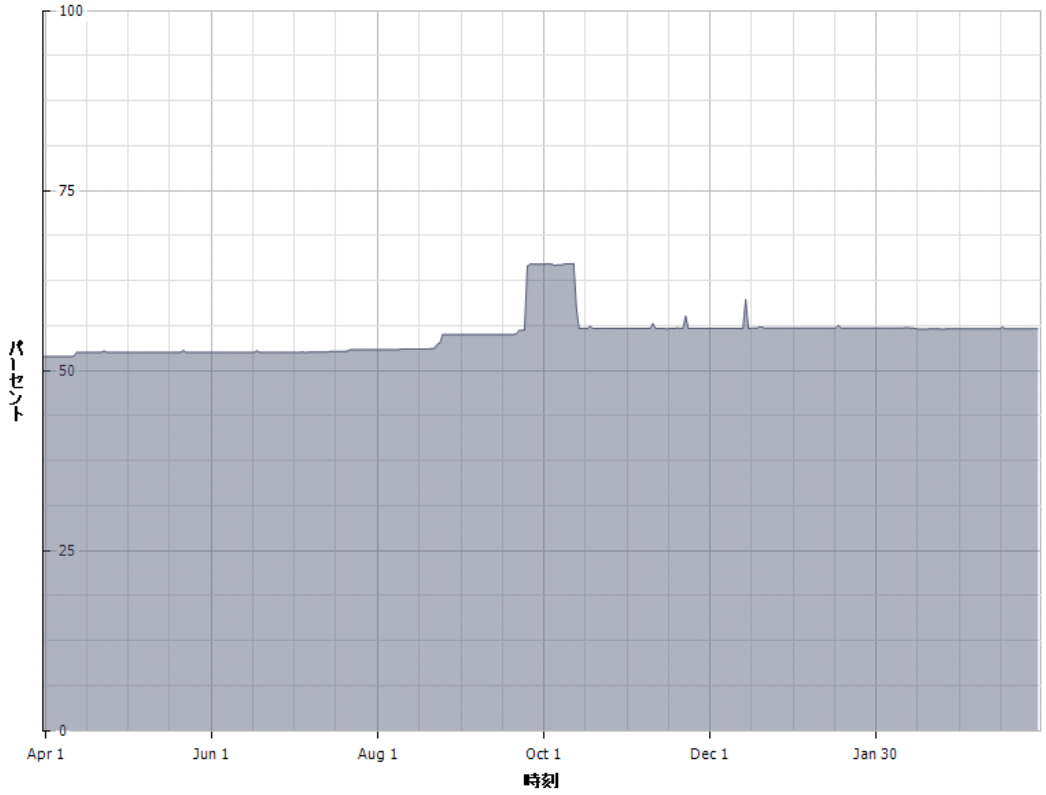


2.3.2 ESX2

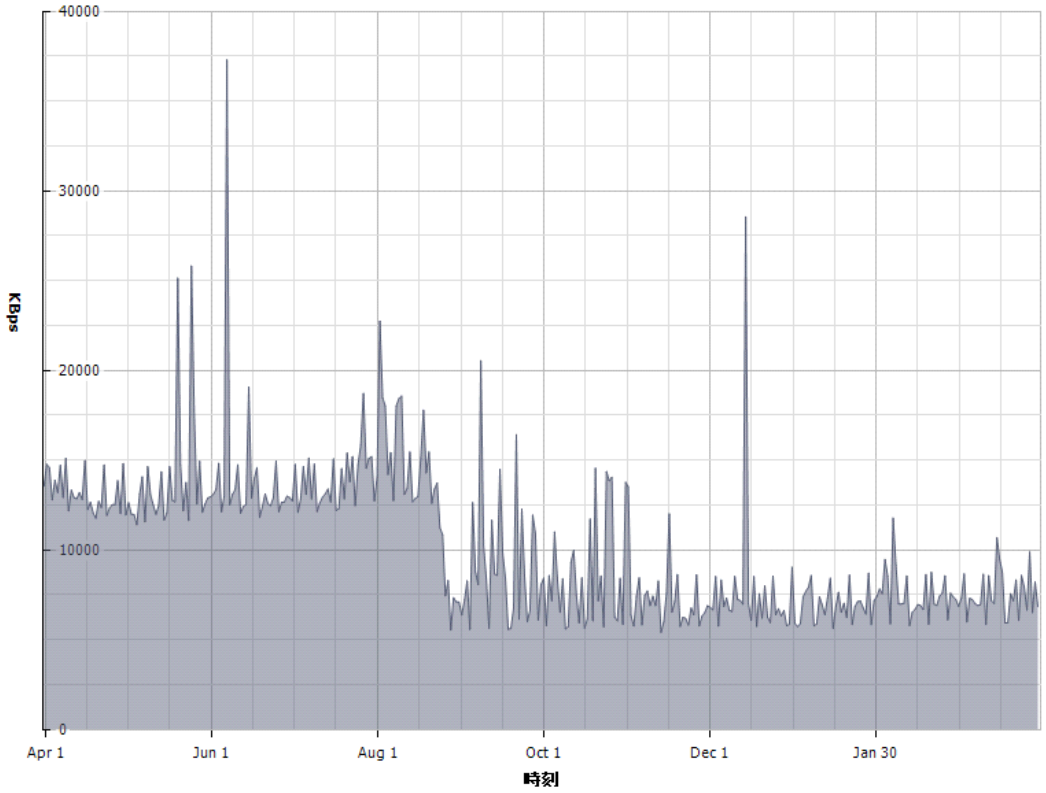
CPU 使用率



メモリ使用率

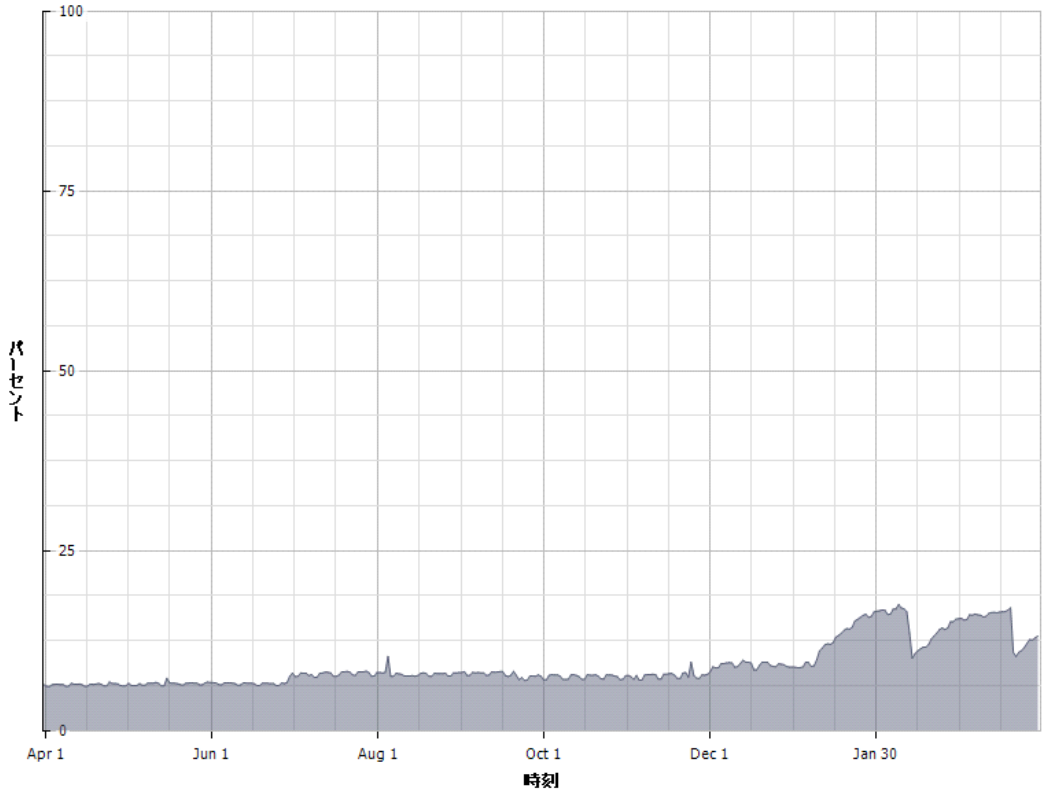


ネットワーク I/O 量

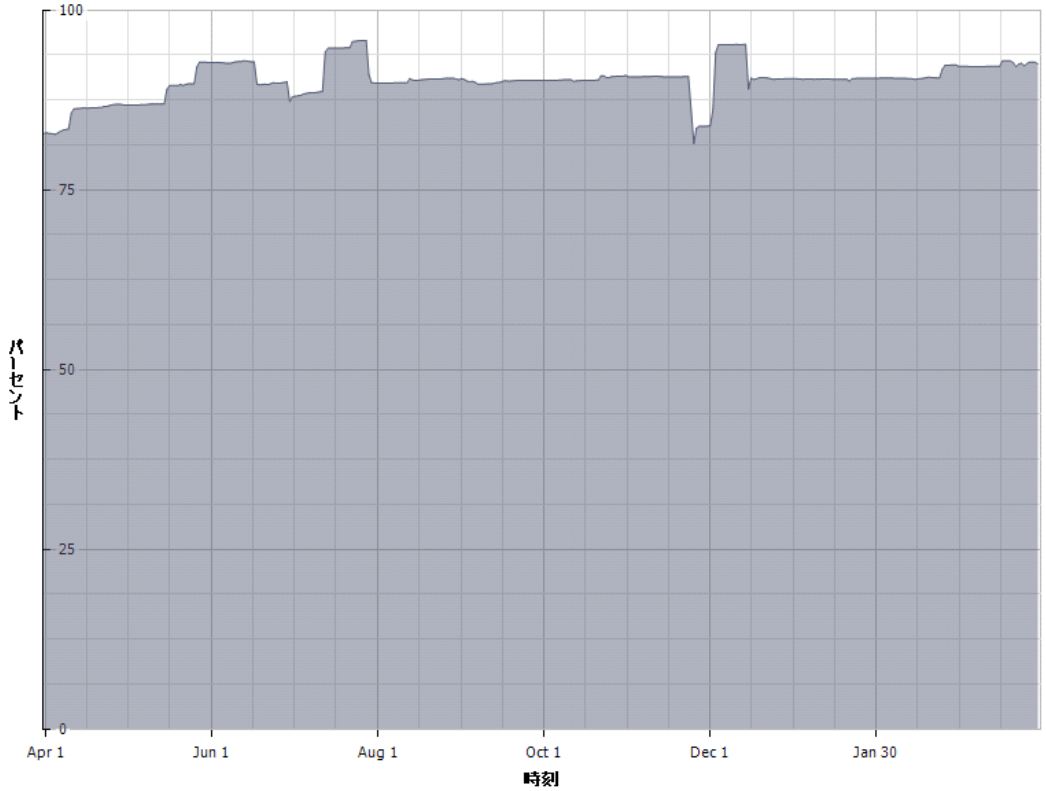


2.3.3 ESX3

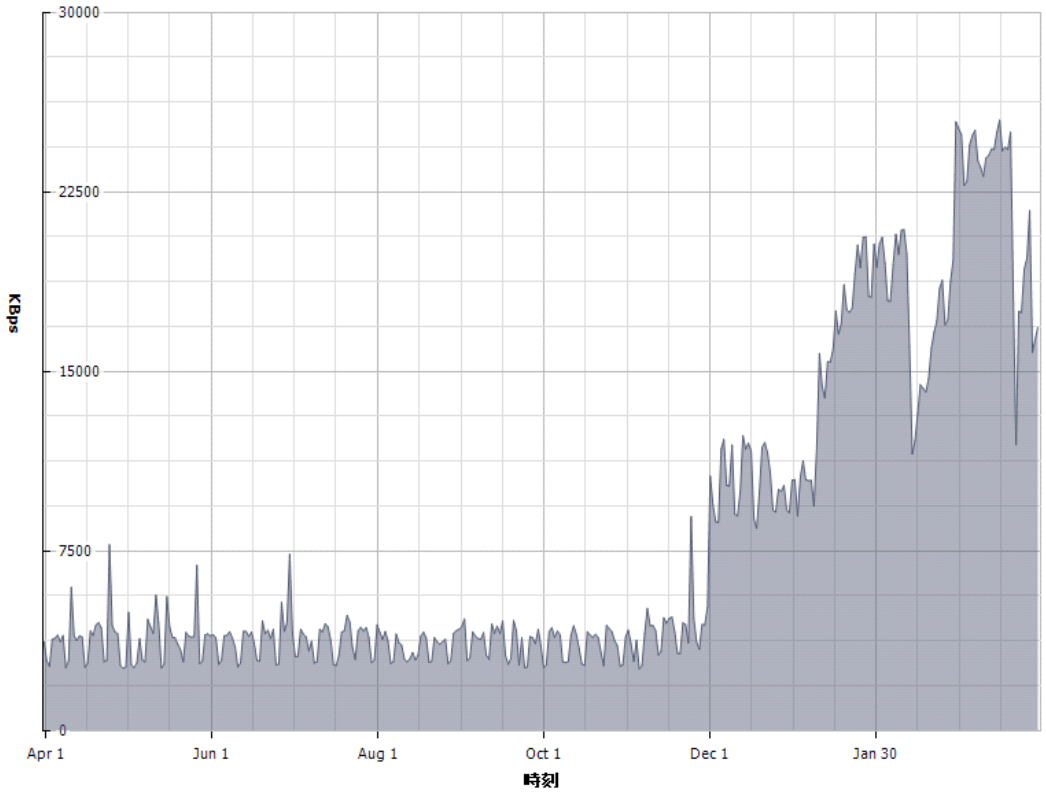
CPU 使用率



メモリ使用率

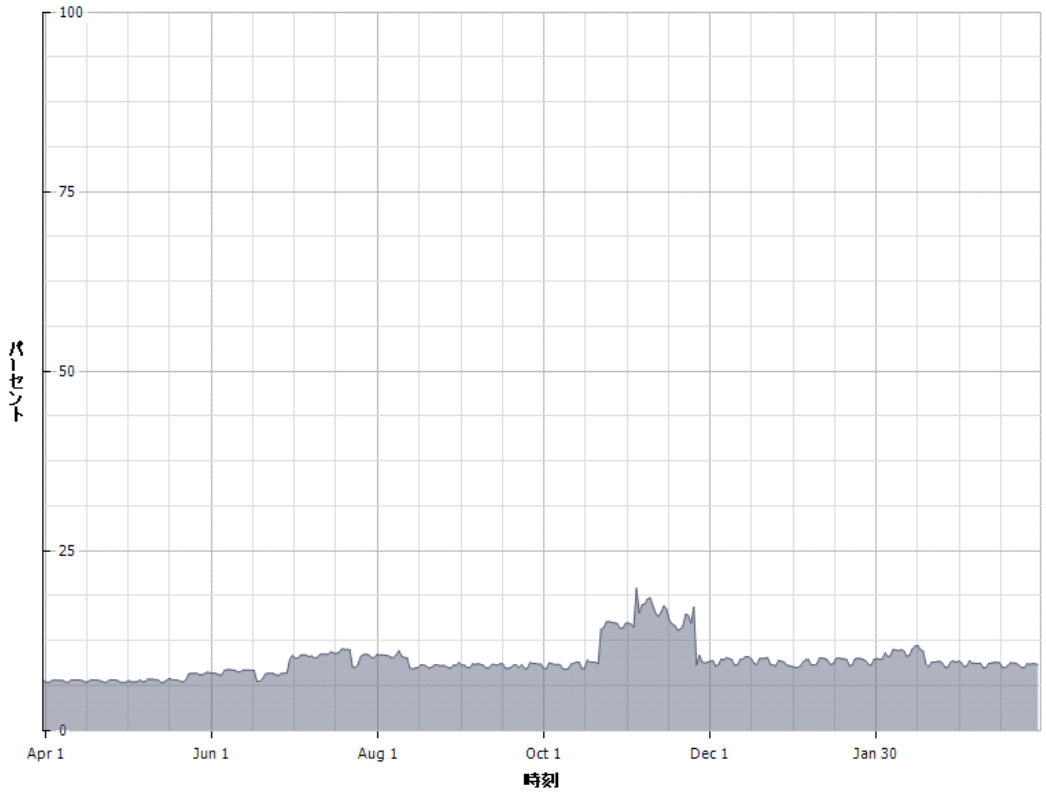


ネットワーク I/O 量

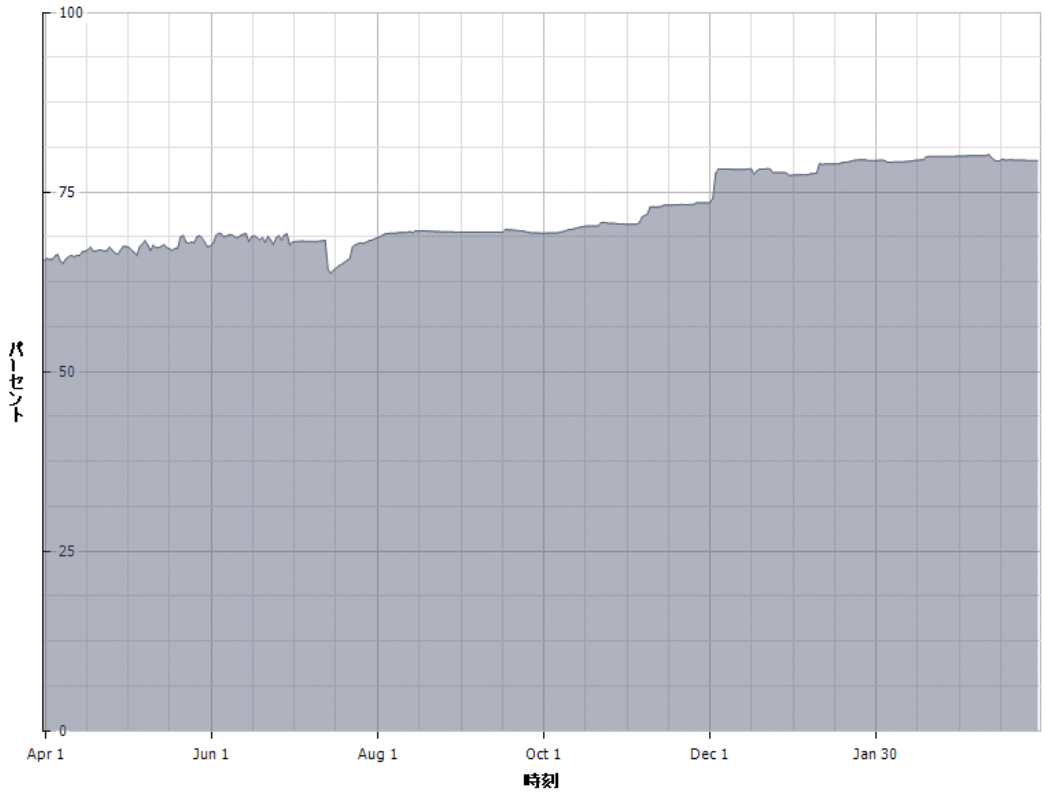


2.3.4 ESX4

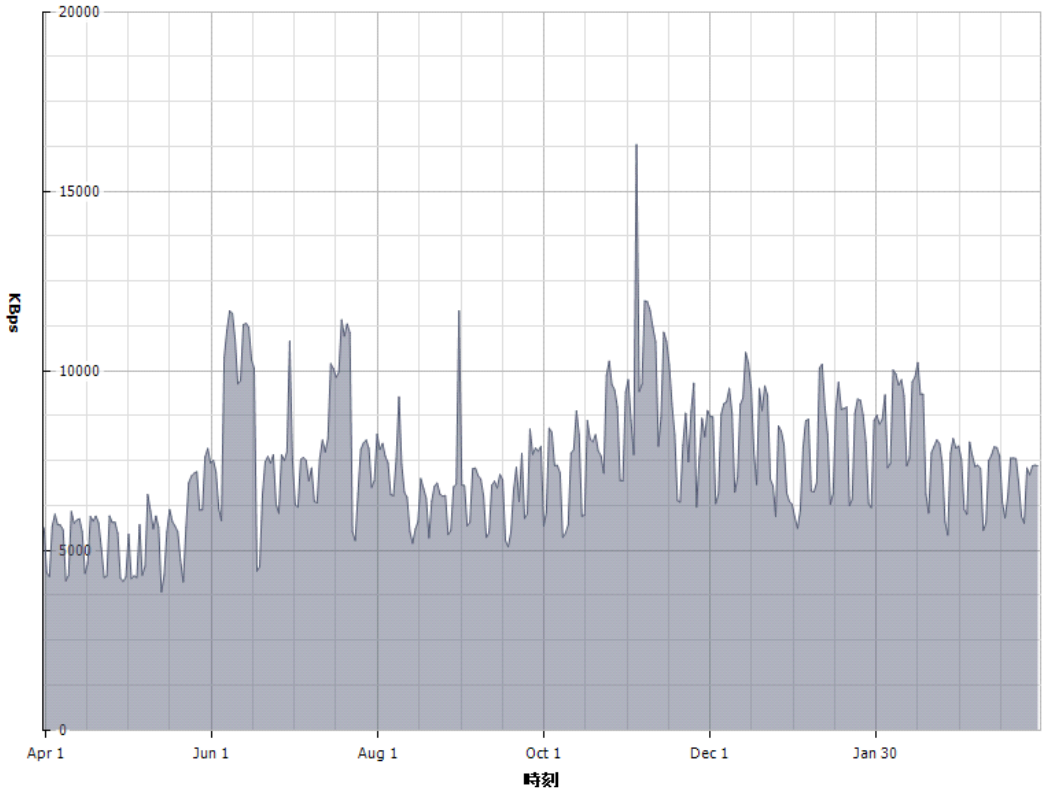
CPU 使用率



メモリ使用率

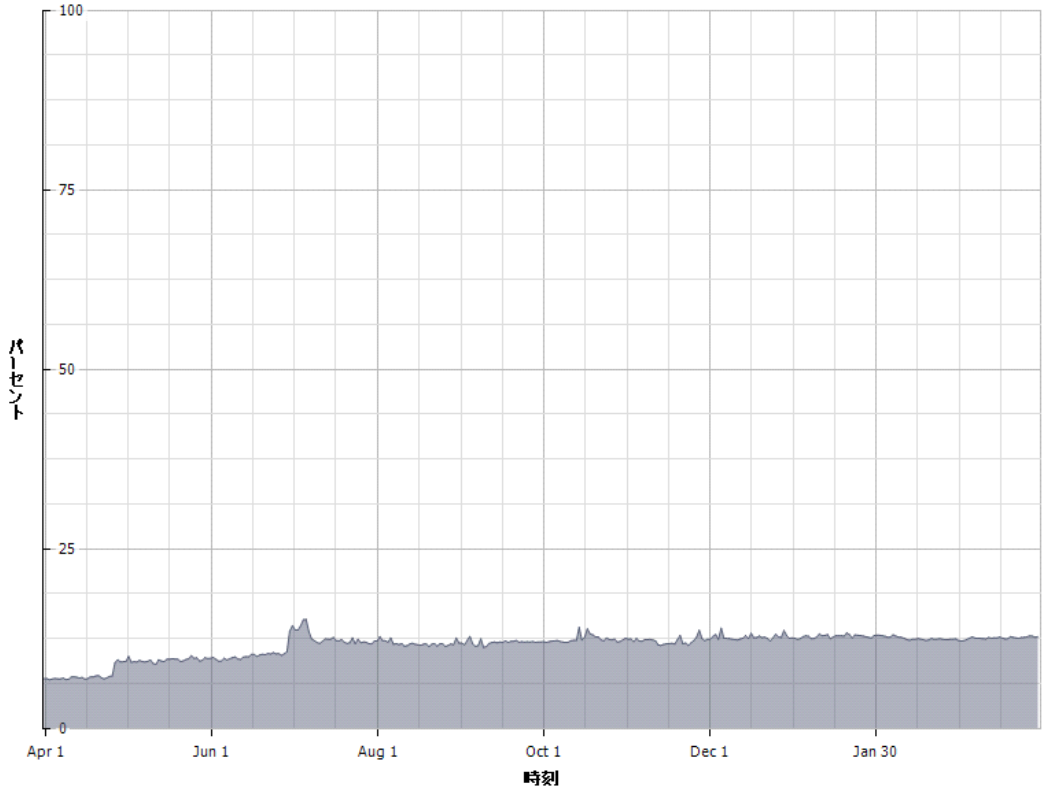


ネットワーク I/O 量

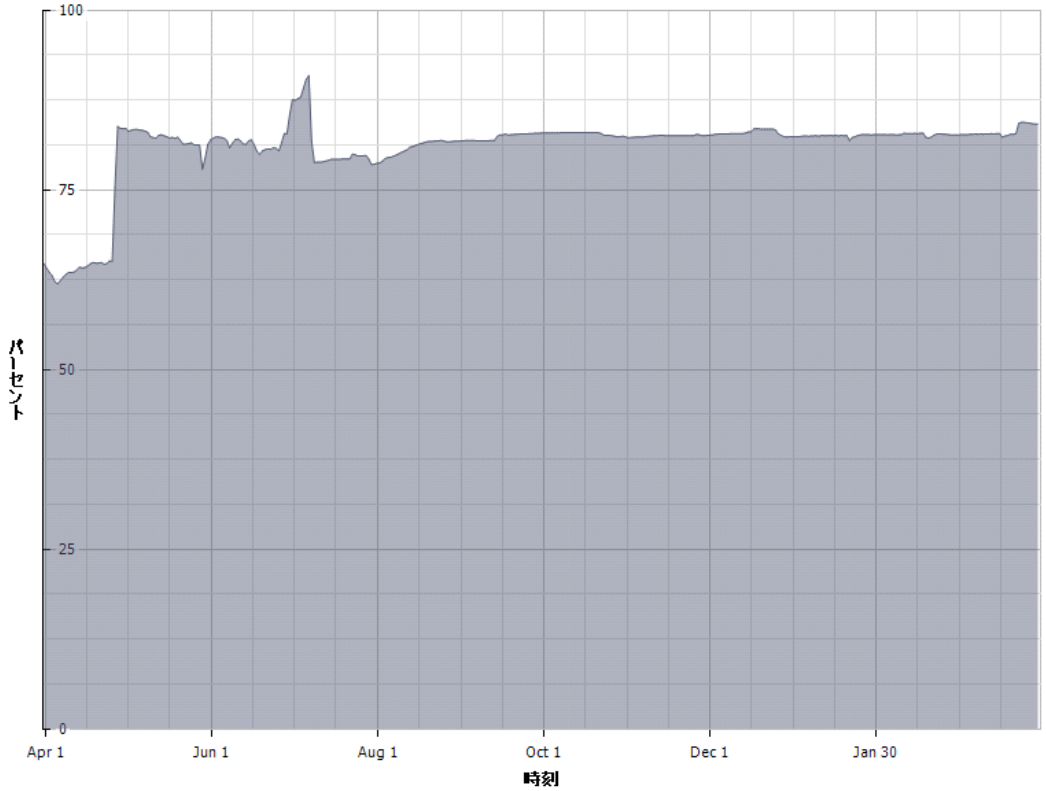


2.3.5 ESX5

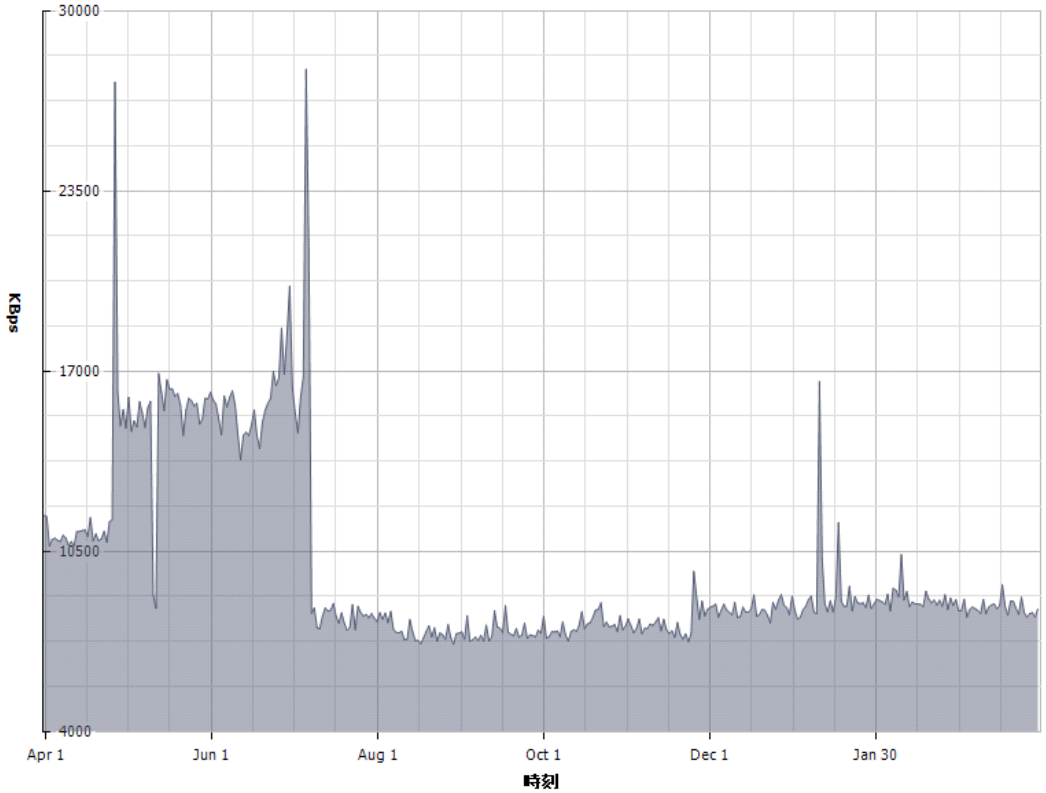
CPU 使用率



メモリ使用率

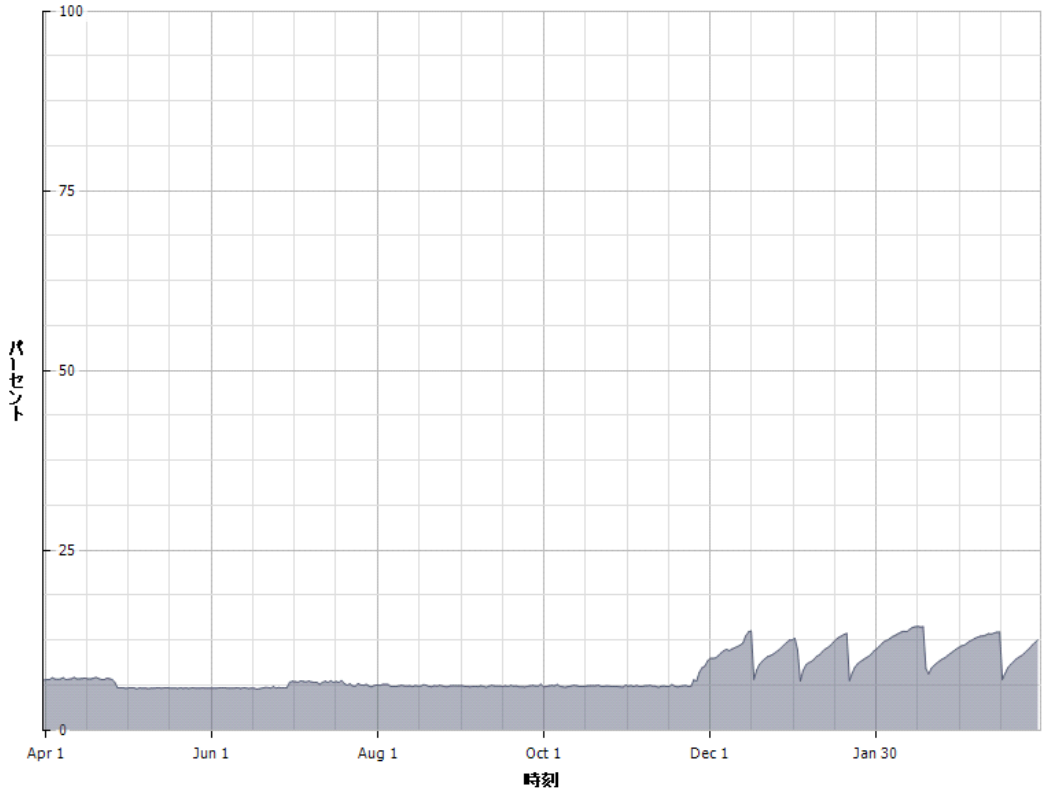


ネットワーク I/O 量

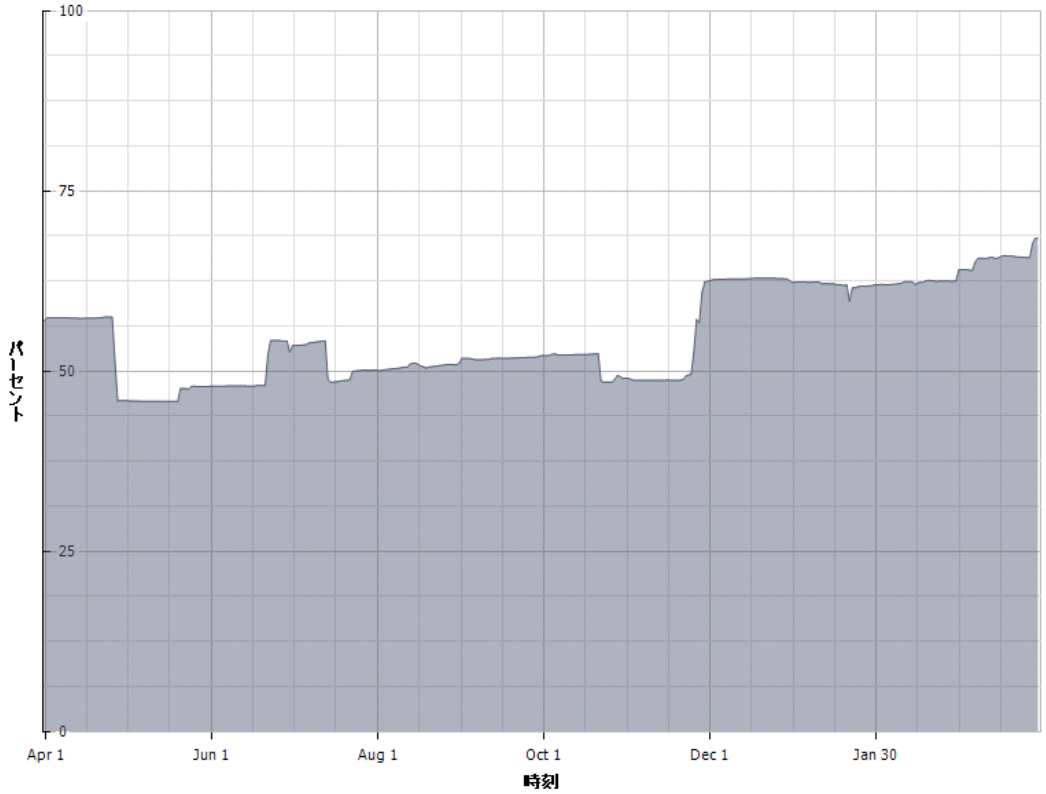


2.3.6 ESX6

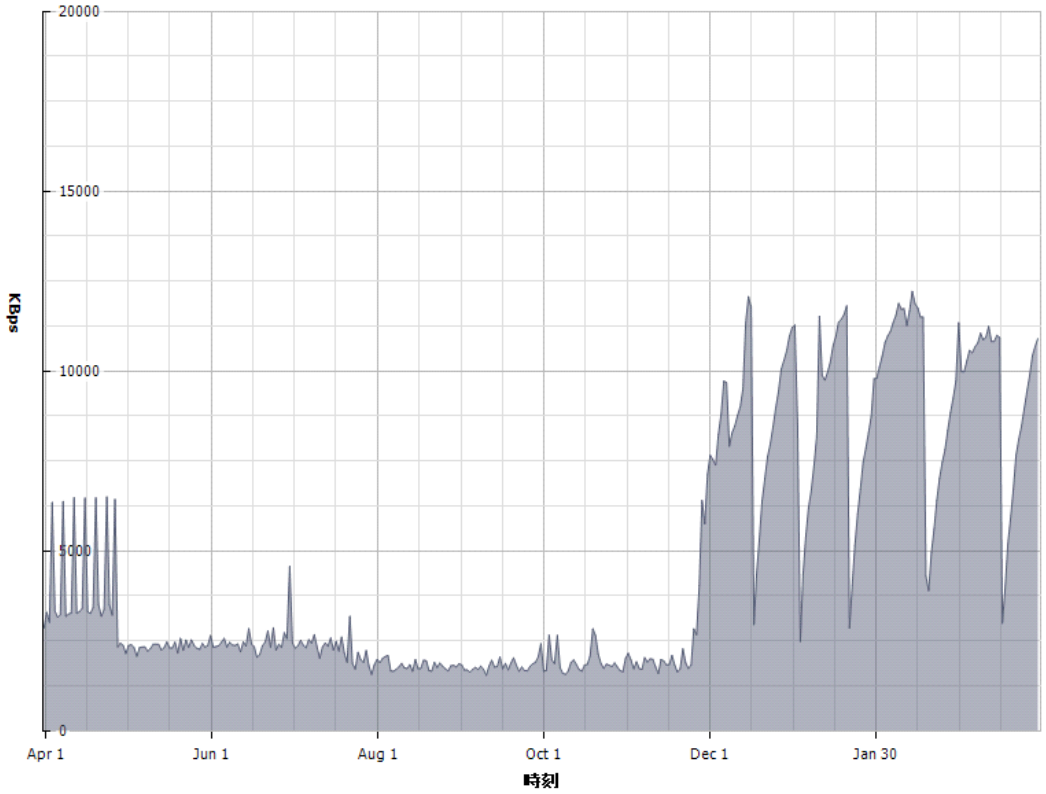
CPU 使用率



メモリ使用率

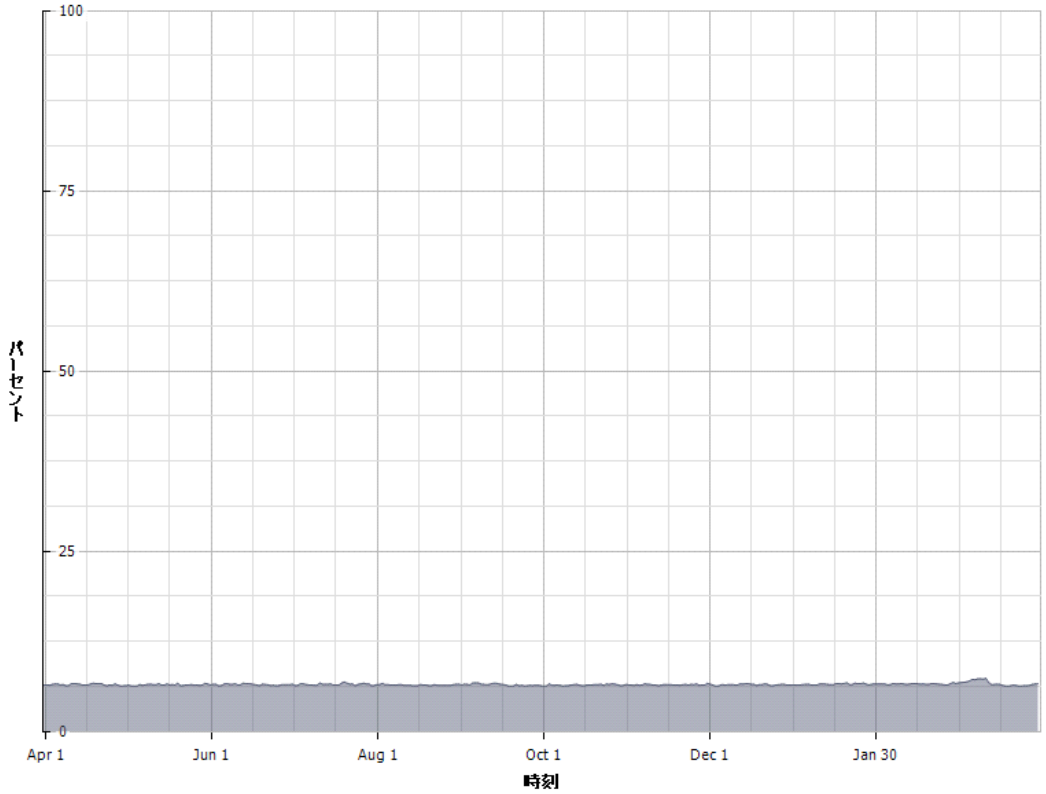


ネットワーク I/O 量

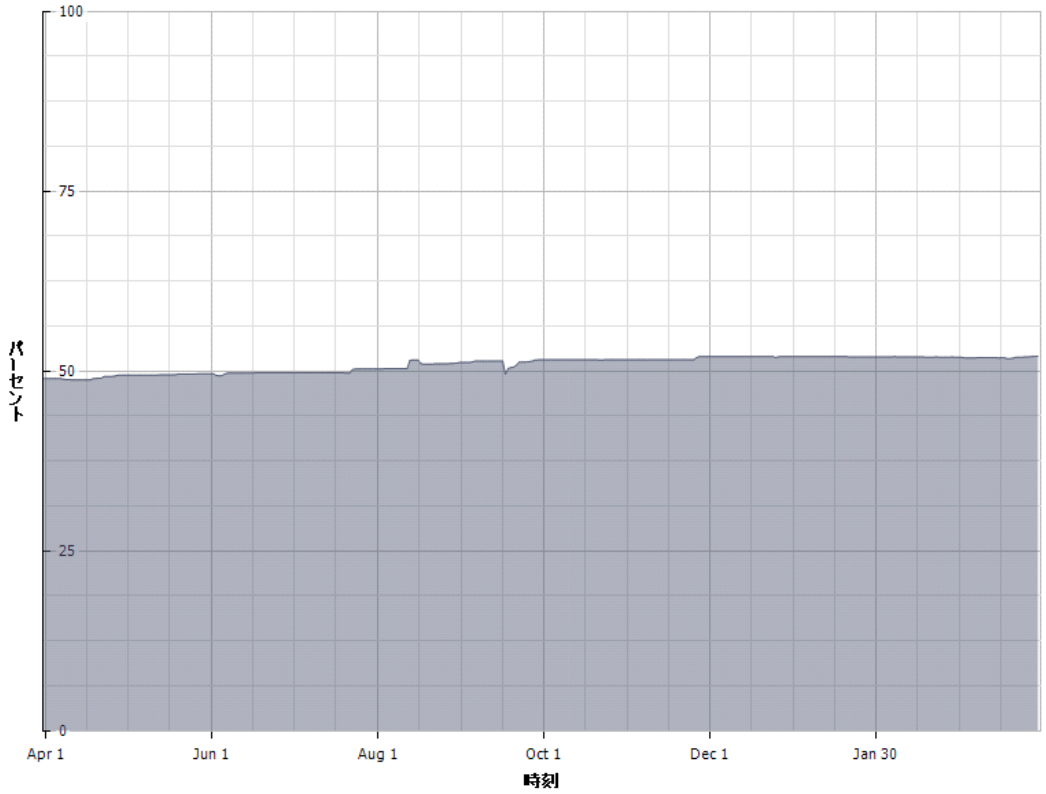


2.3.7 ESX7

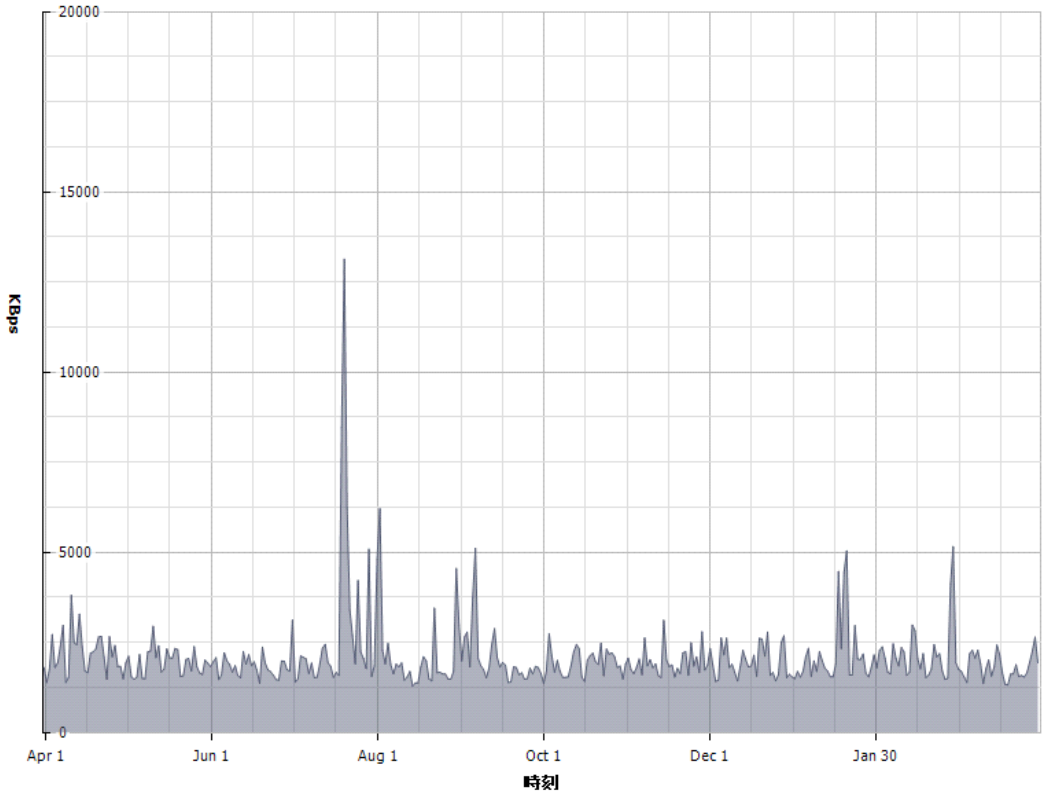
CPU 使用率



メモリ使用率

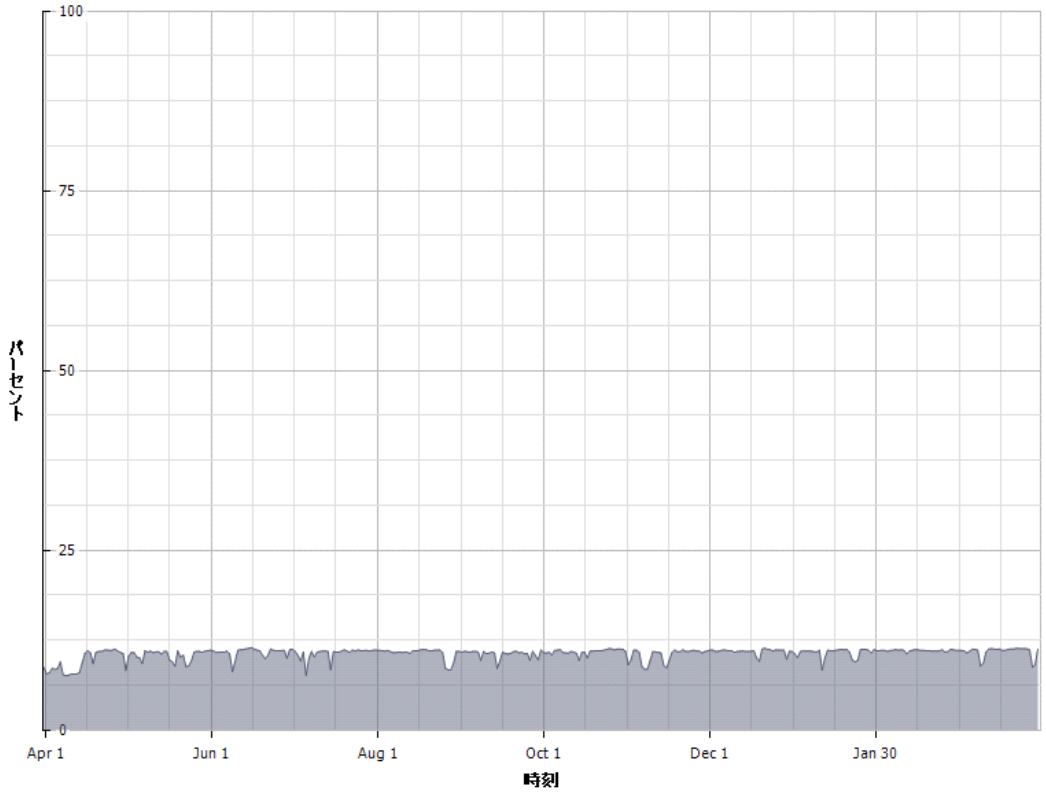


ネットワーク I/O 量

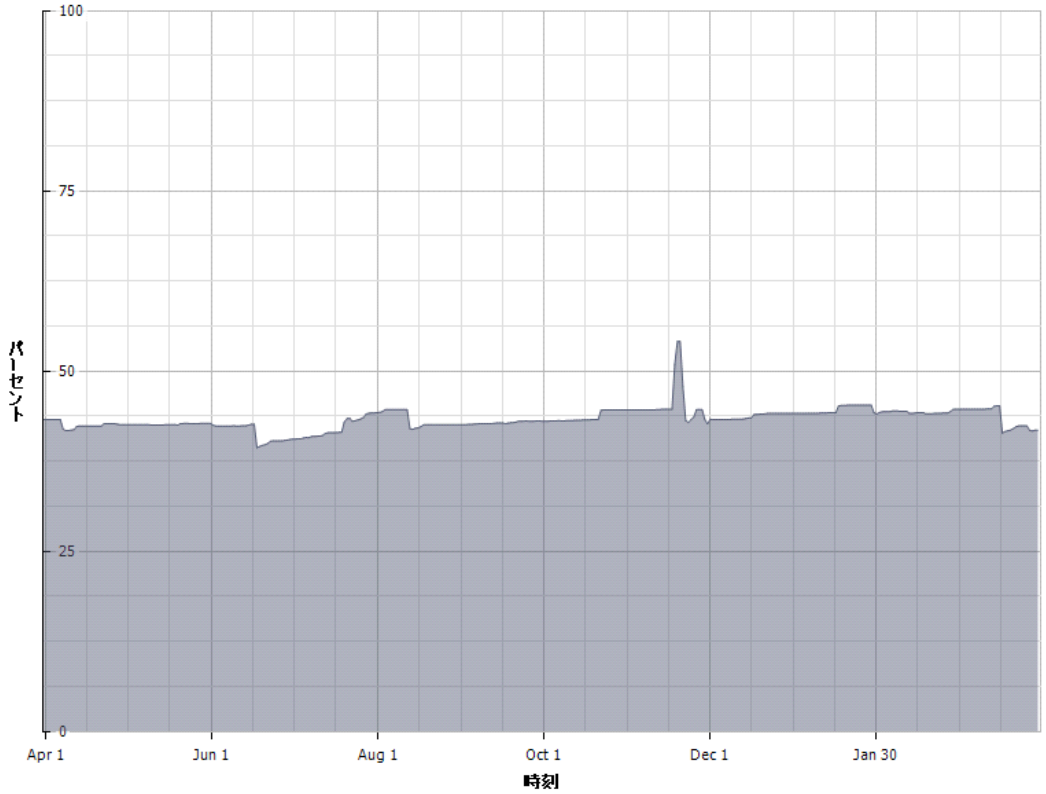


2.3.8 ESX8

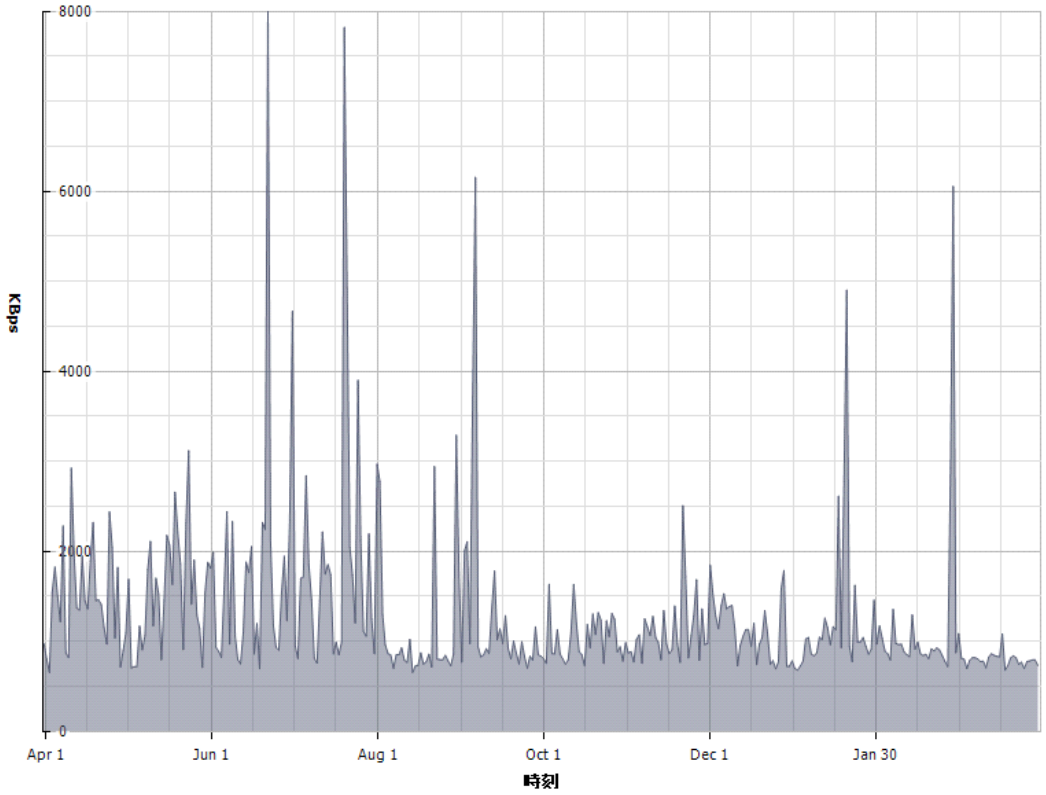
CPU 使用率



メモリ使用率

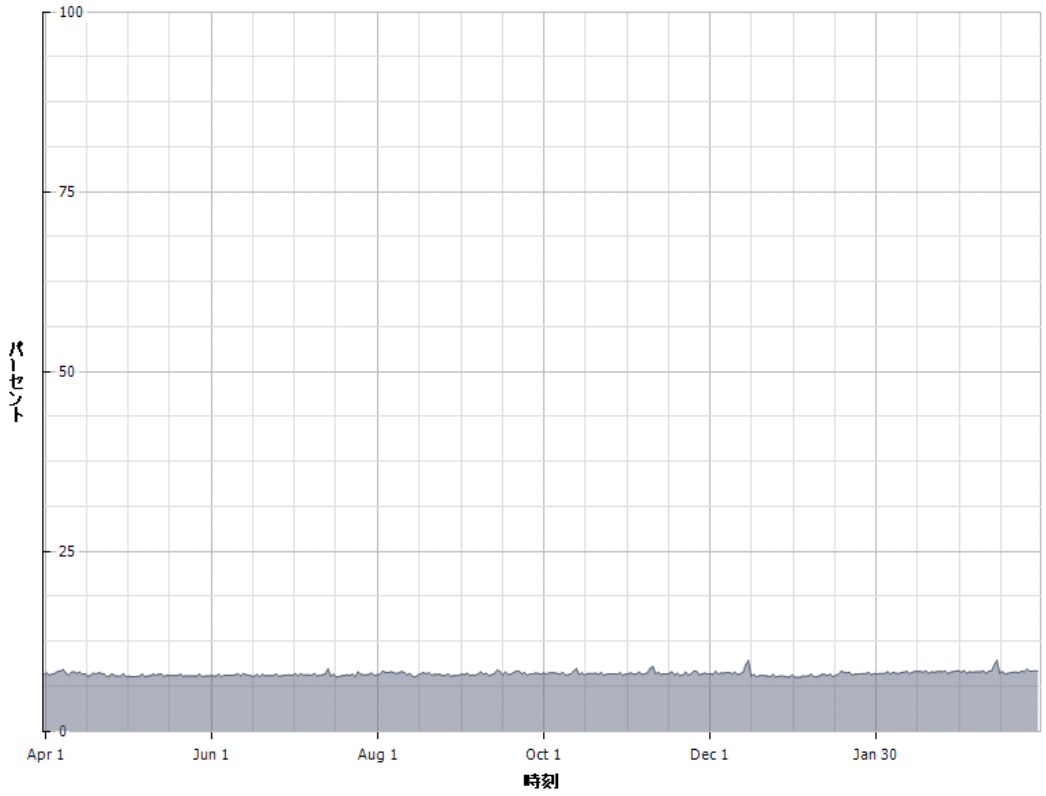


ネットワーク I/O 量

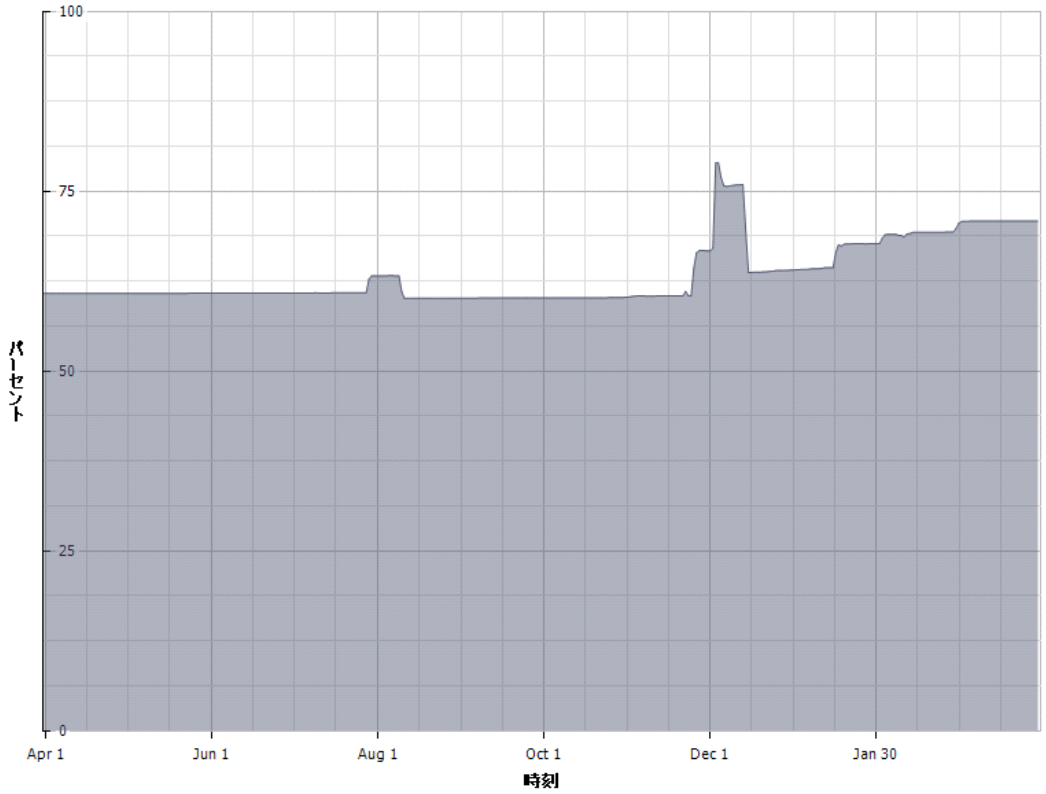


2.3.9 ESX9

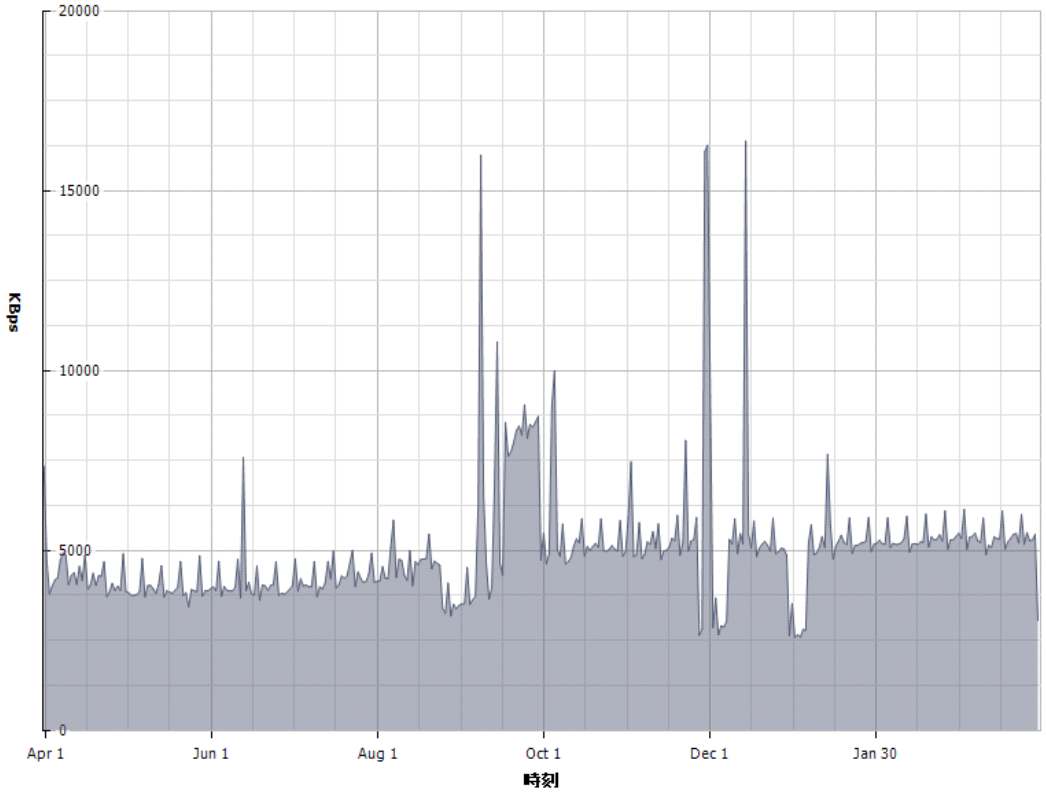
CPU 使用率



メモリ使用率

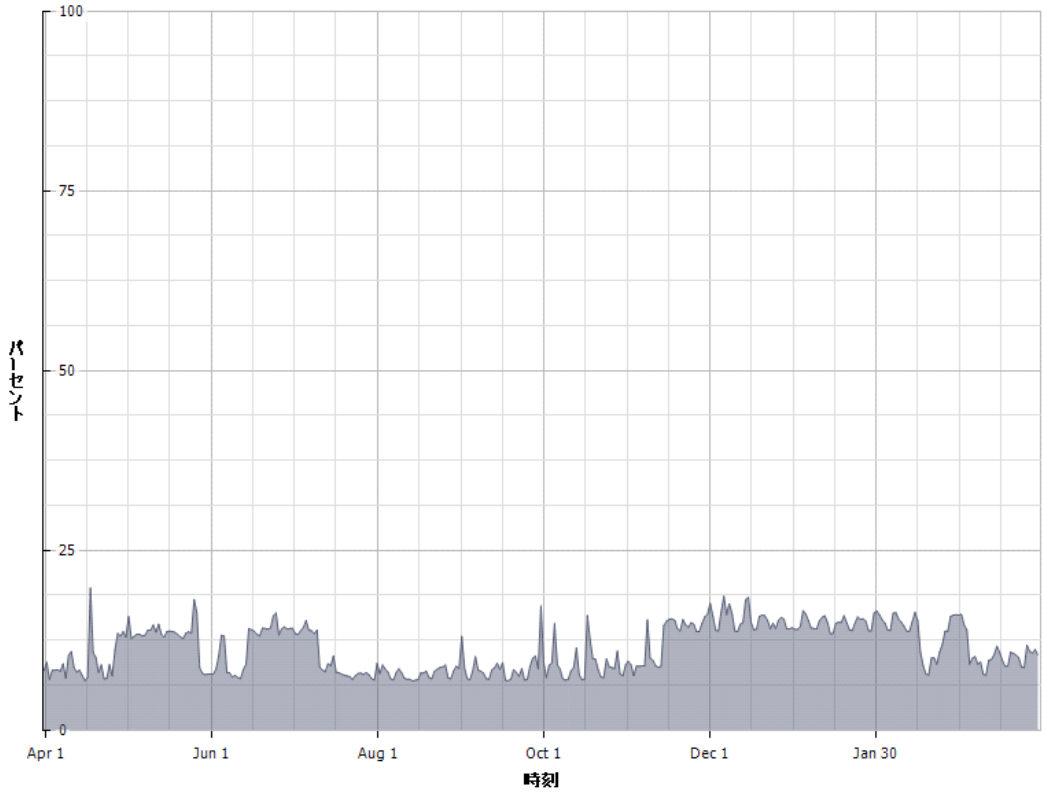


ネットワーク I/O 量

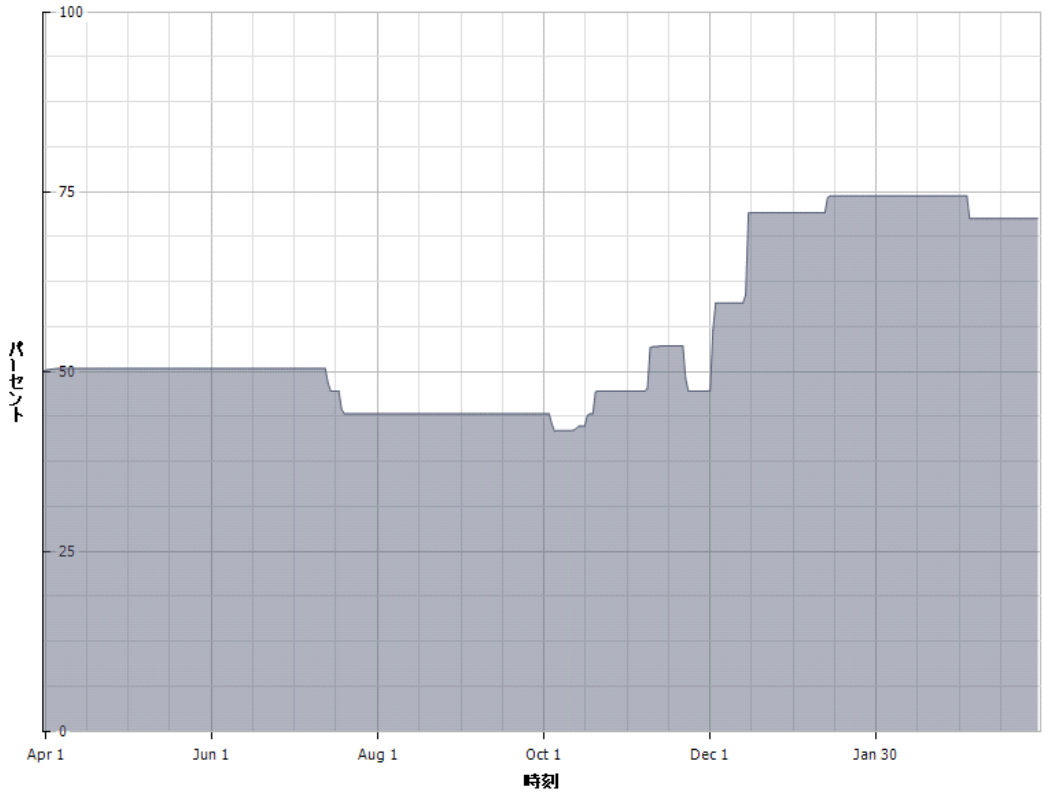


2.3.10　ESX10

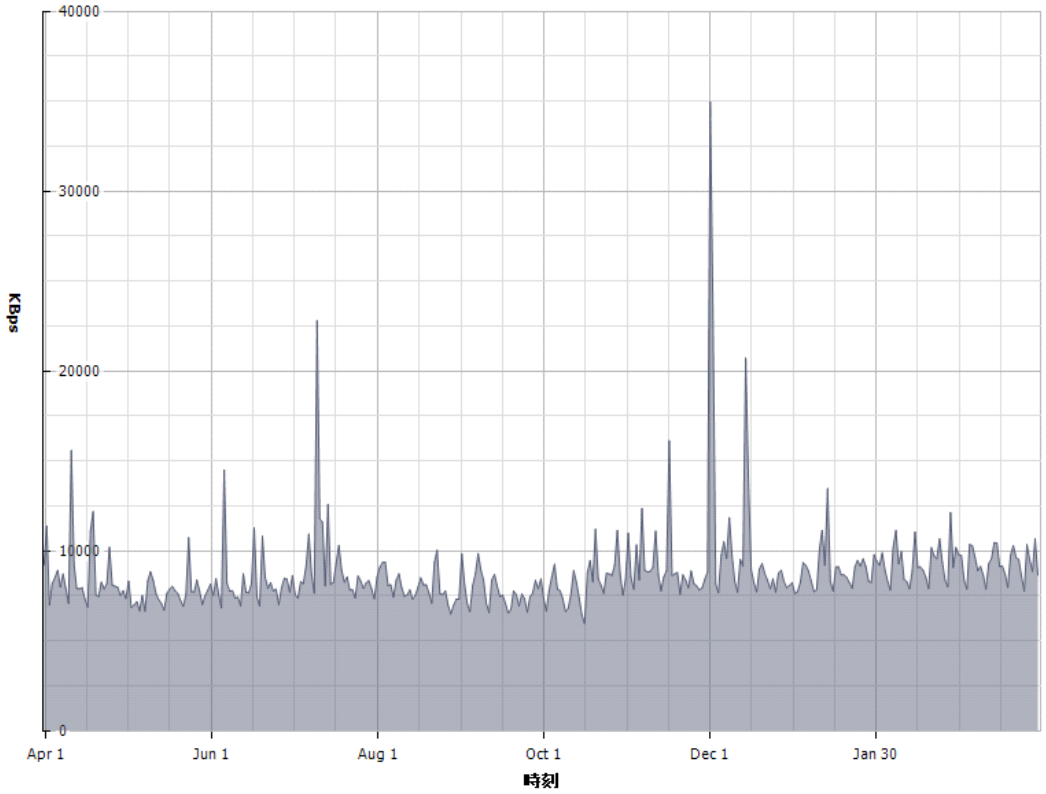
CPU 使用率



メモリ使用率

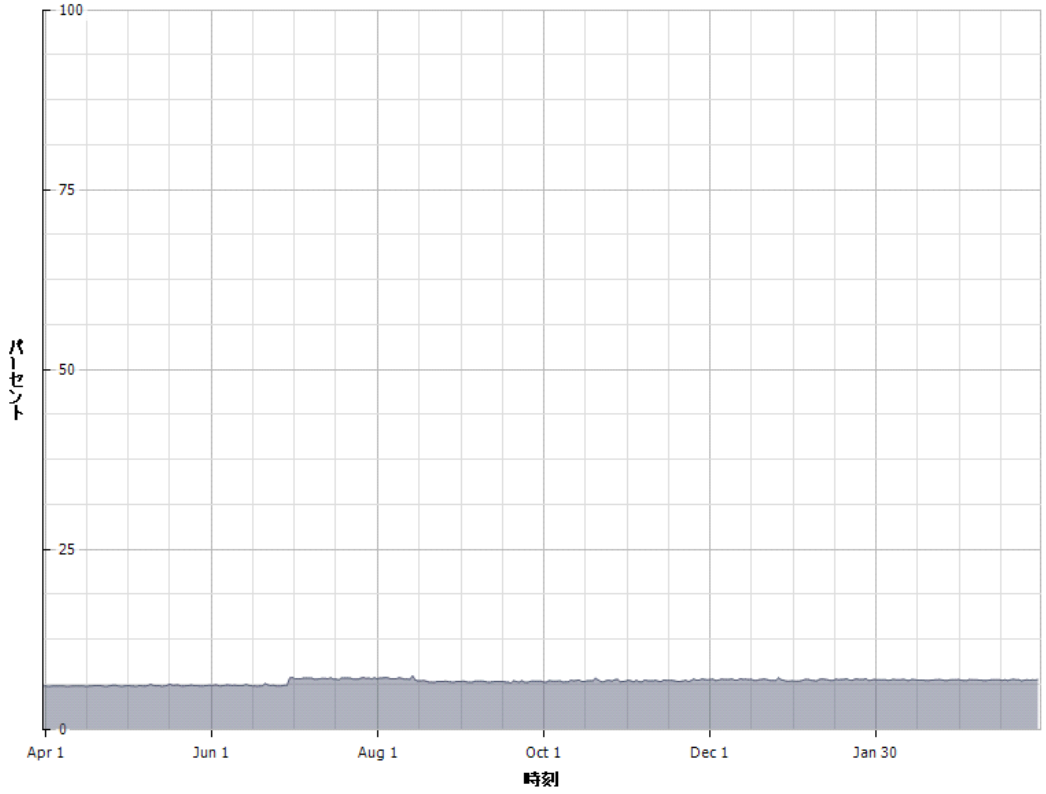


ネットワーク I/O 量

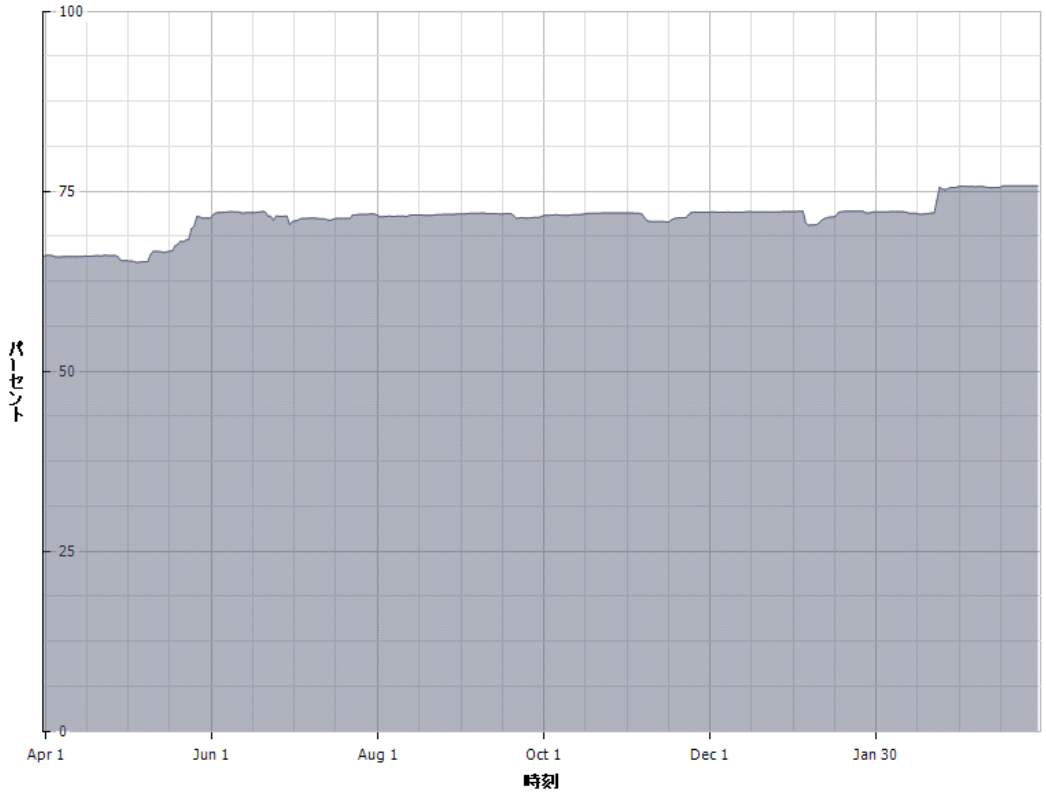


2.3.11　ESX11

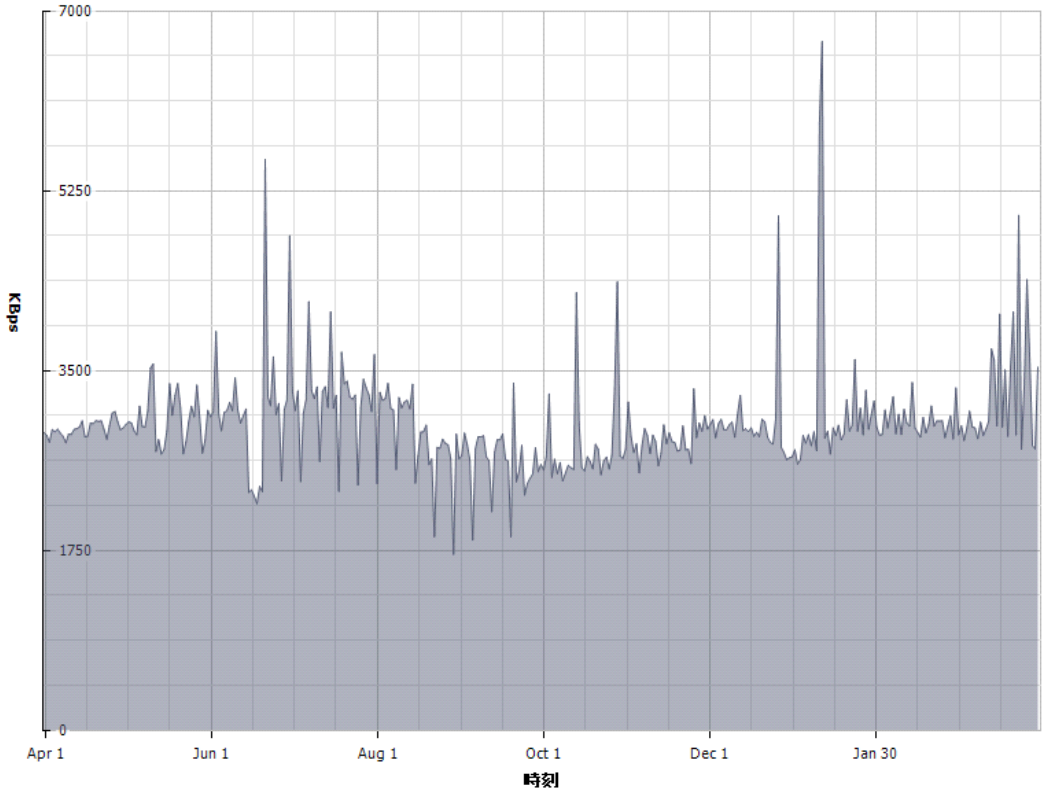
CPU 使用率



メモリ使用率

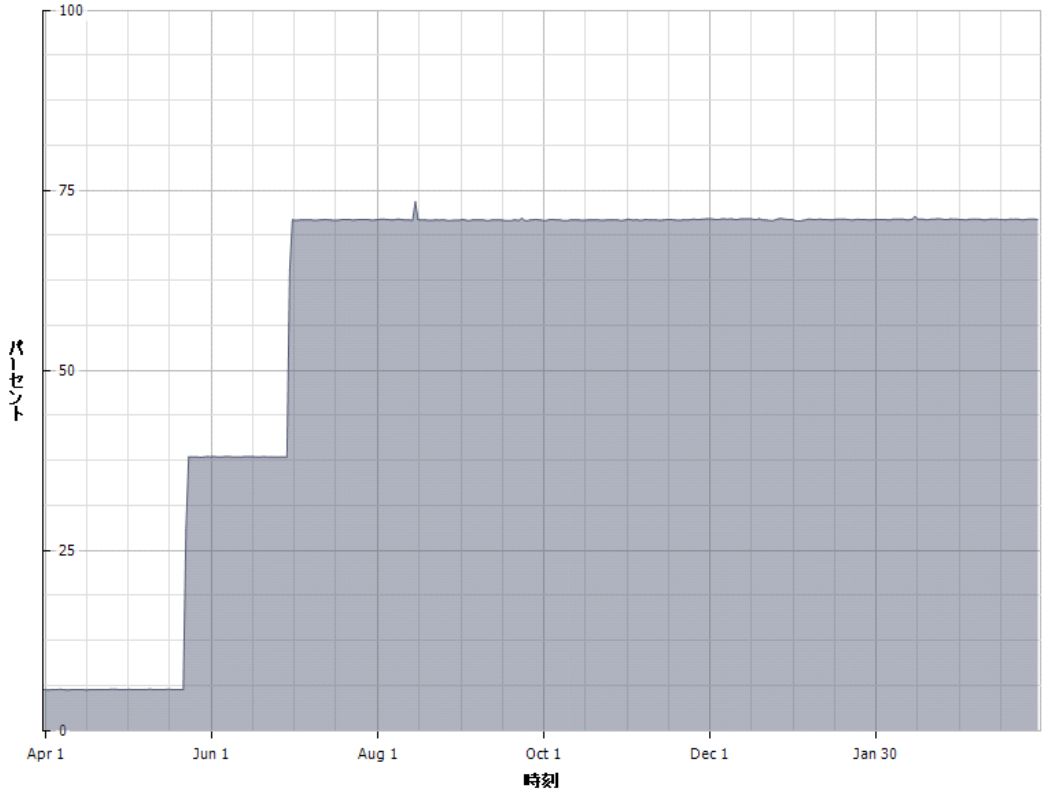


ネットワーク I/O 量

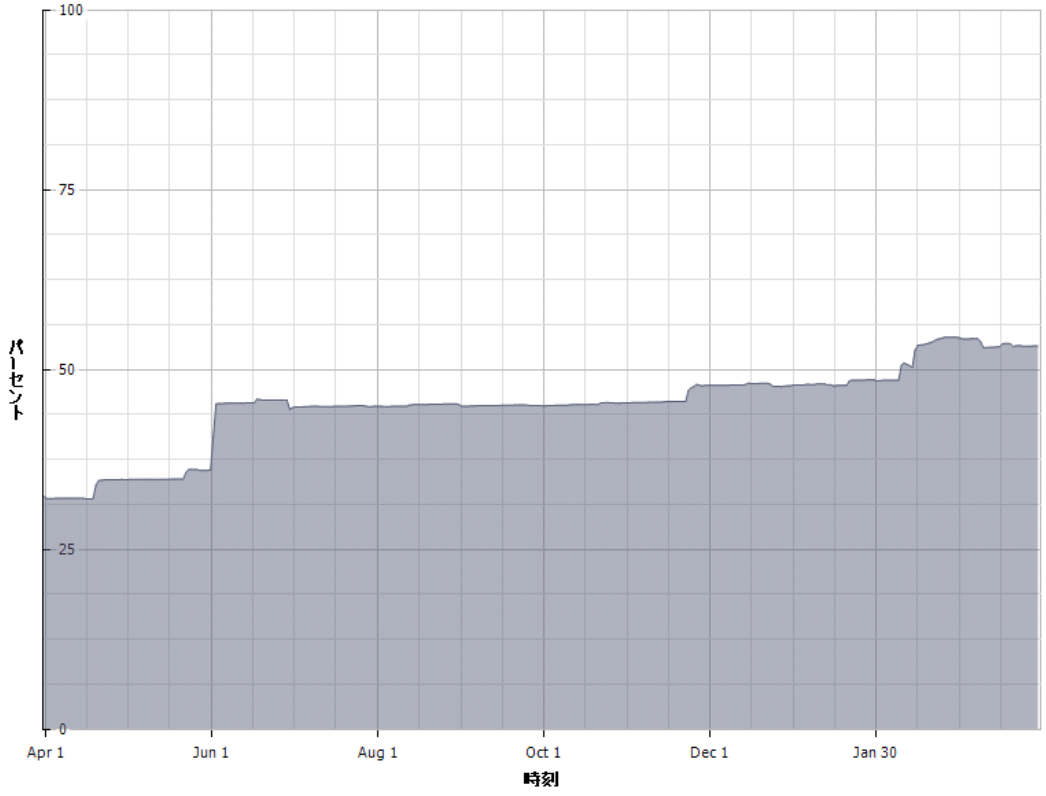


2.3.12　ESX12

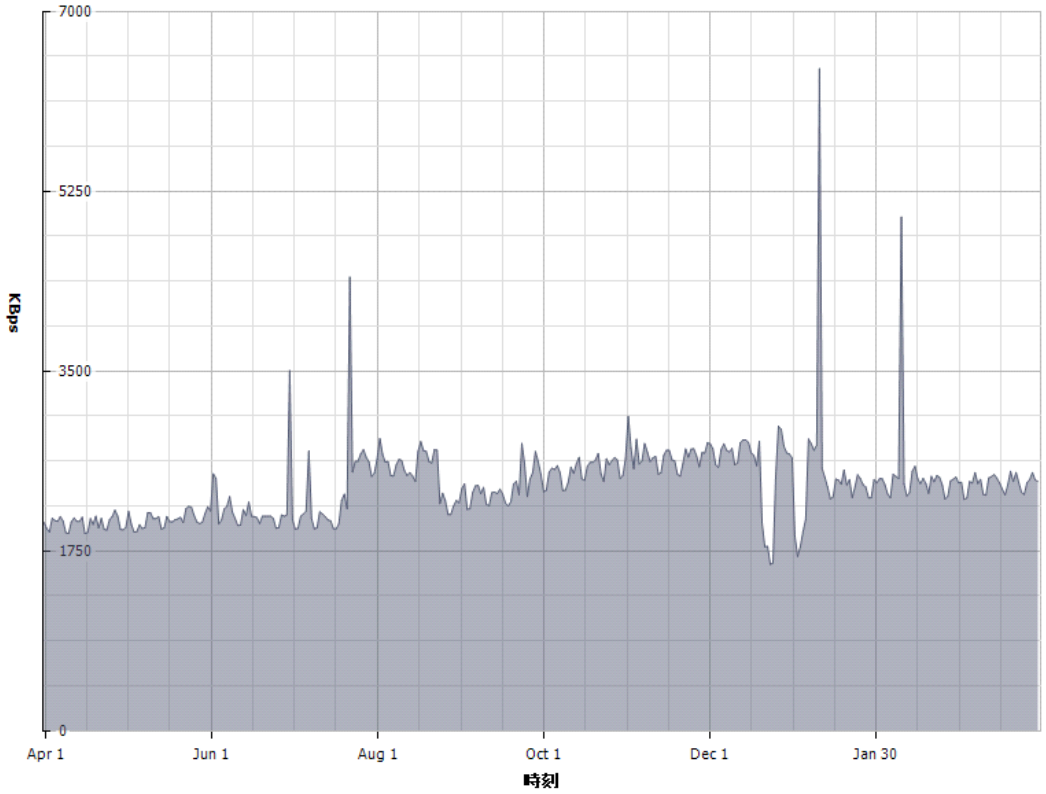
CPU 使用率



メモリ使用率

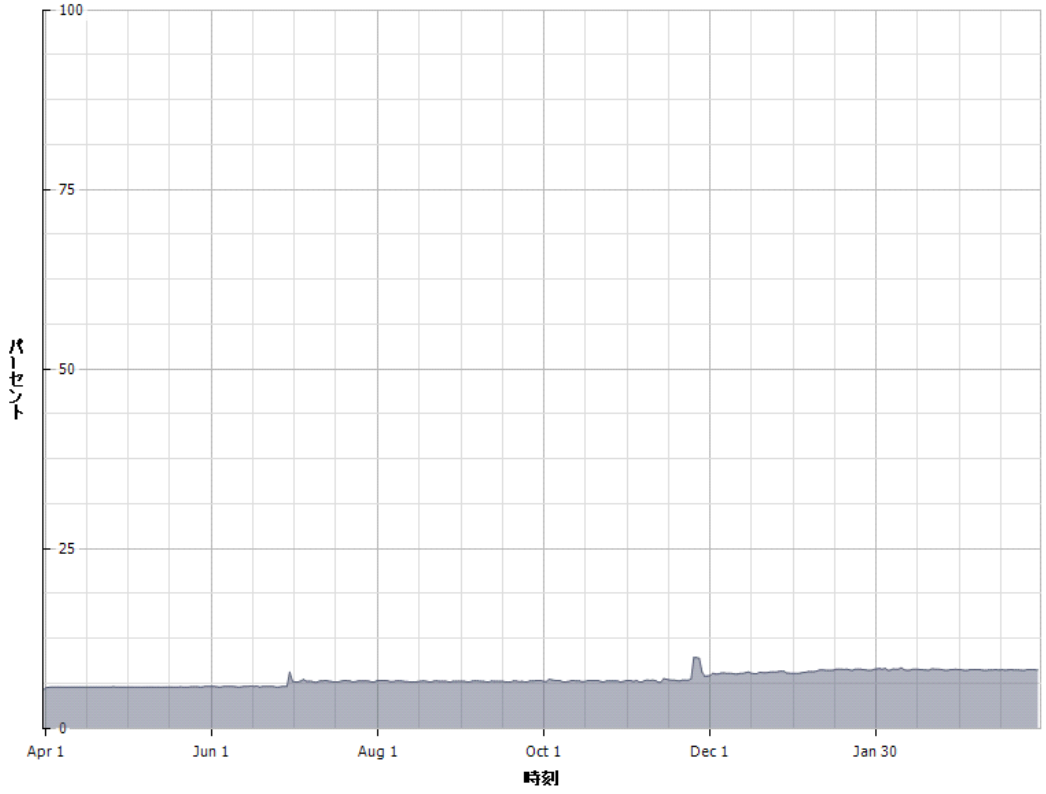


ネットワーク I/O 量

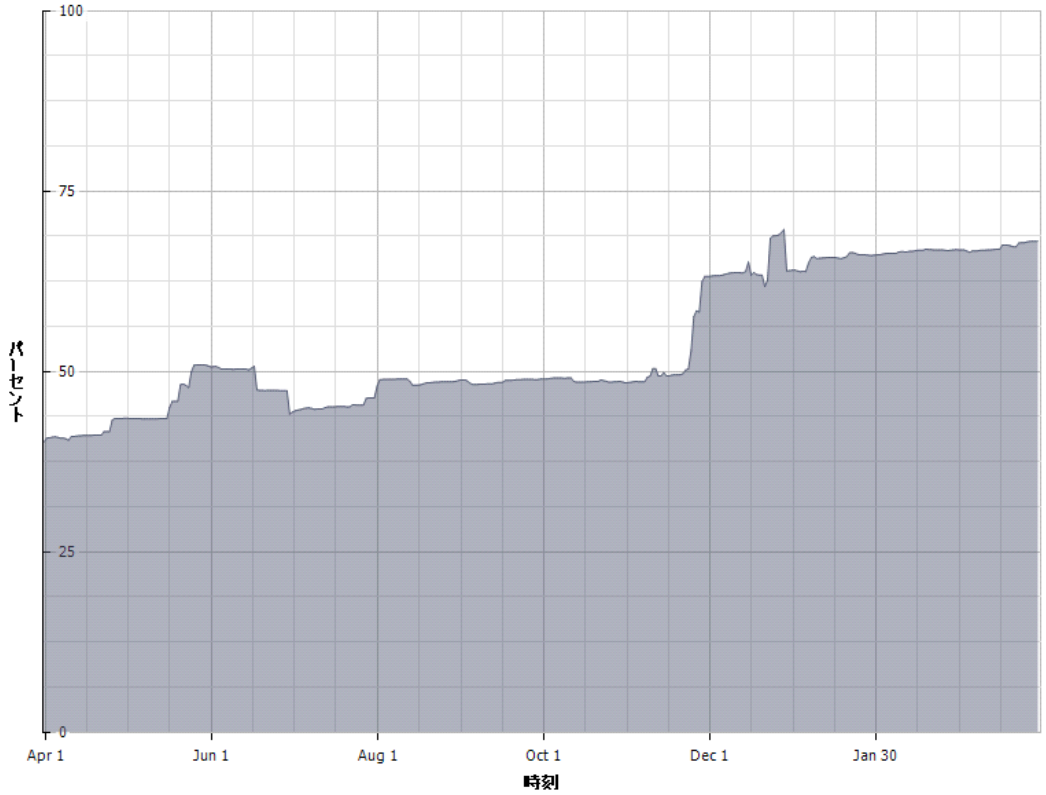


2.3.13　ESX13

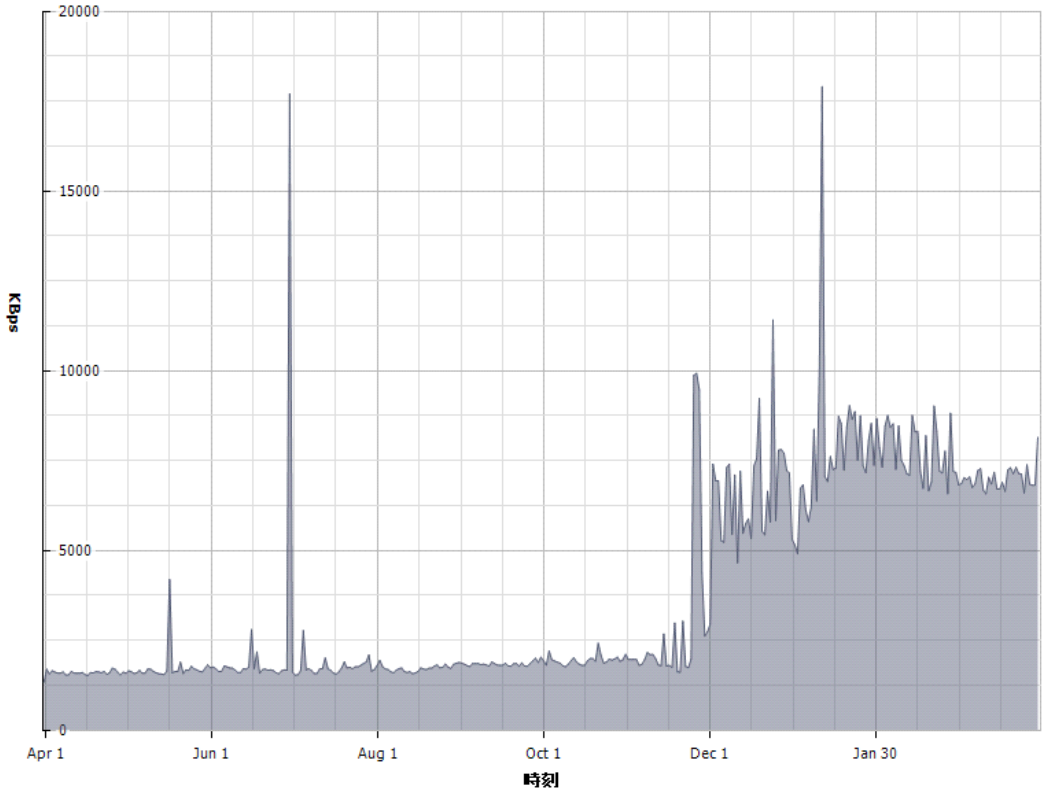
CPU 使用率



メモリ使用率

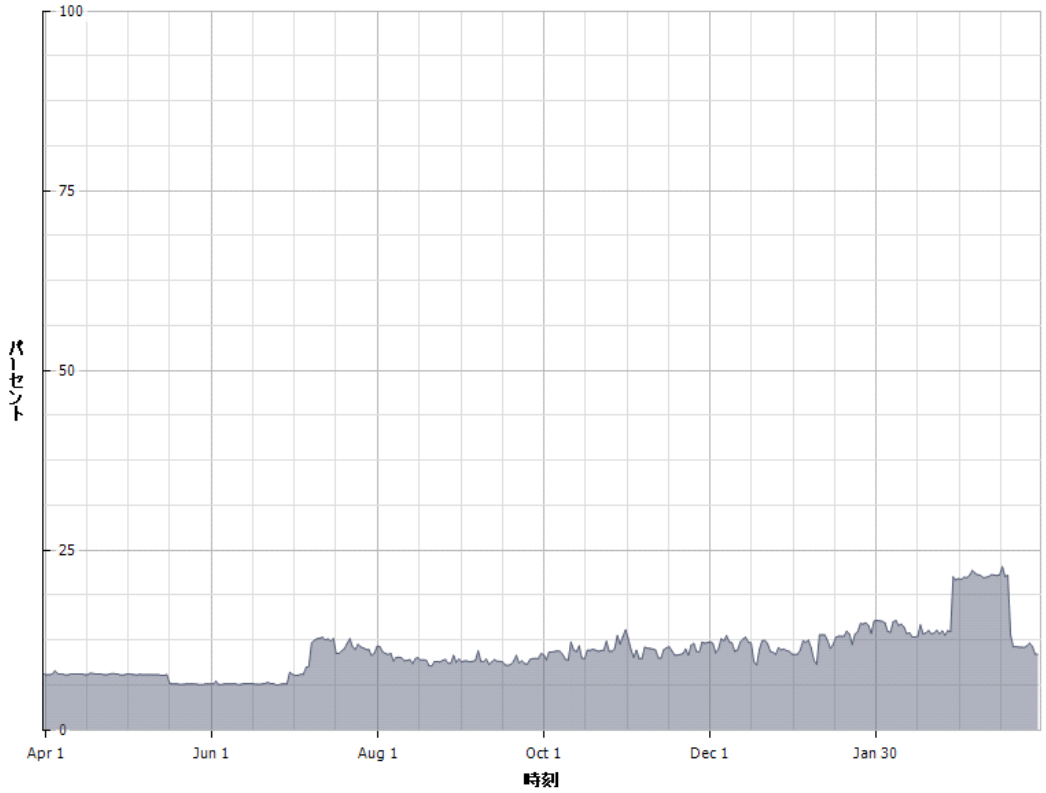


ネットワーク I/O 量

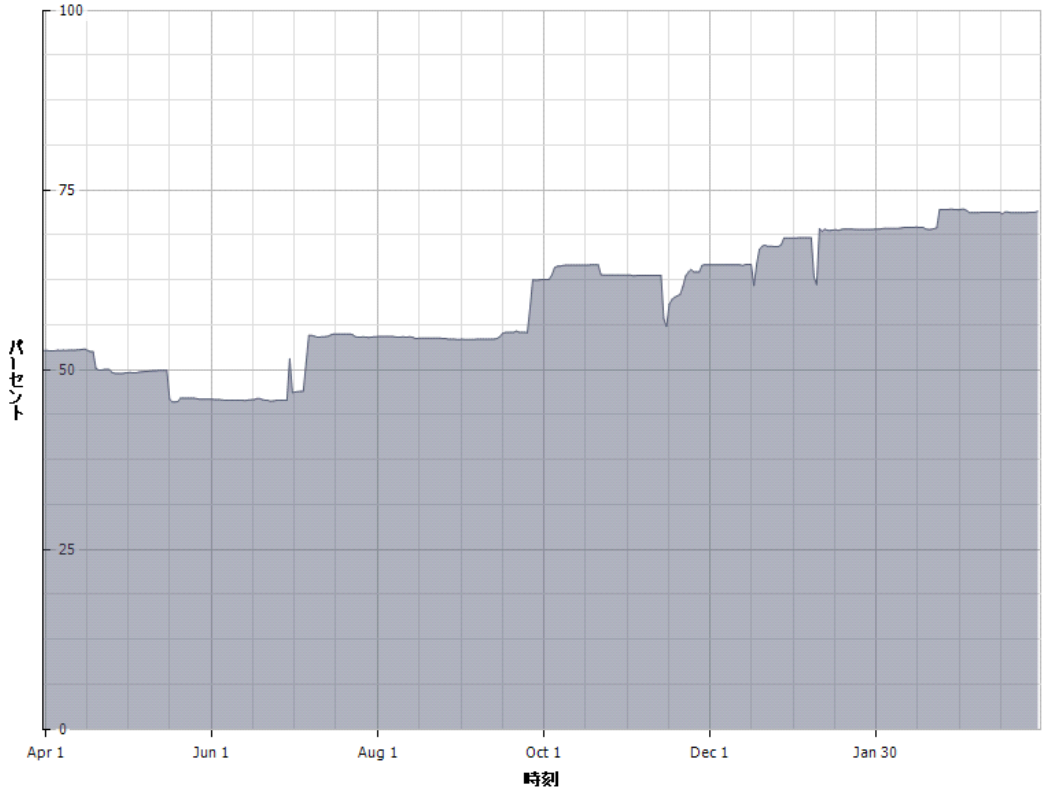


2.3.14　ESX14

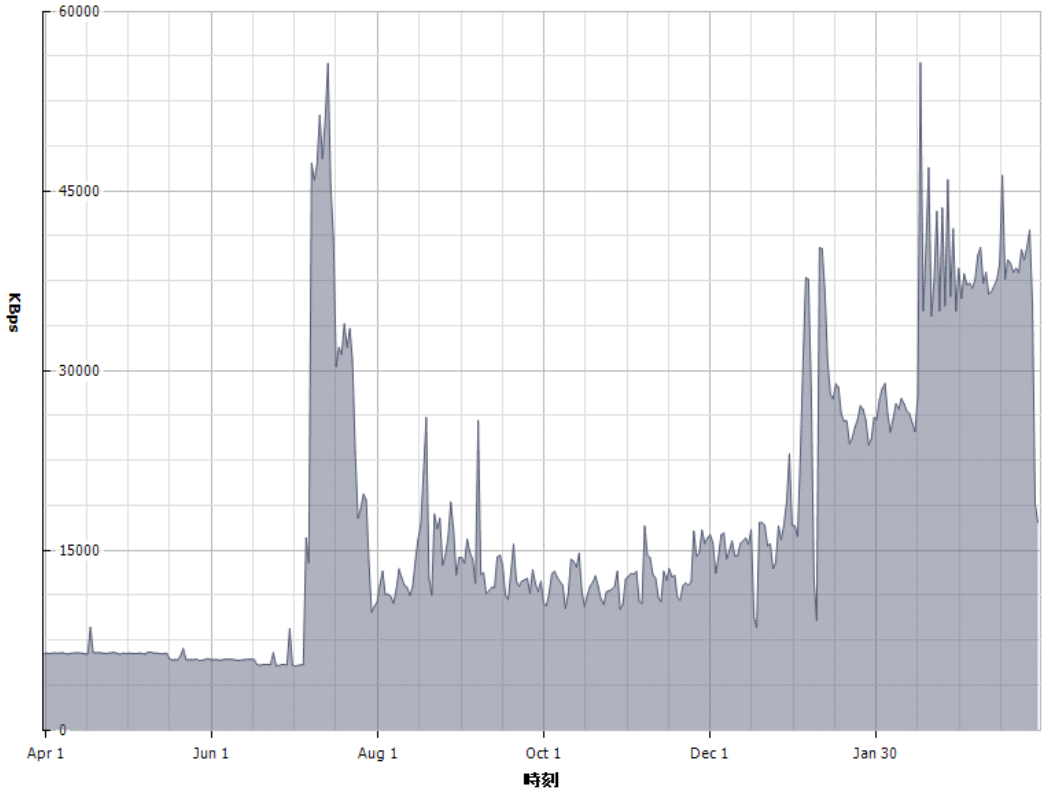
CPU 使用率



メモリ使用率

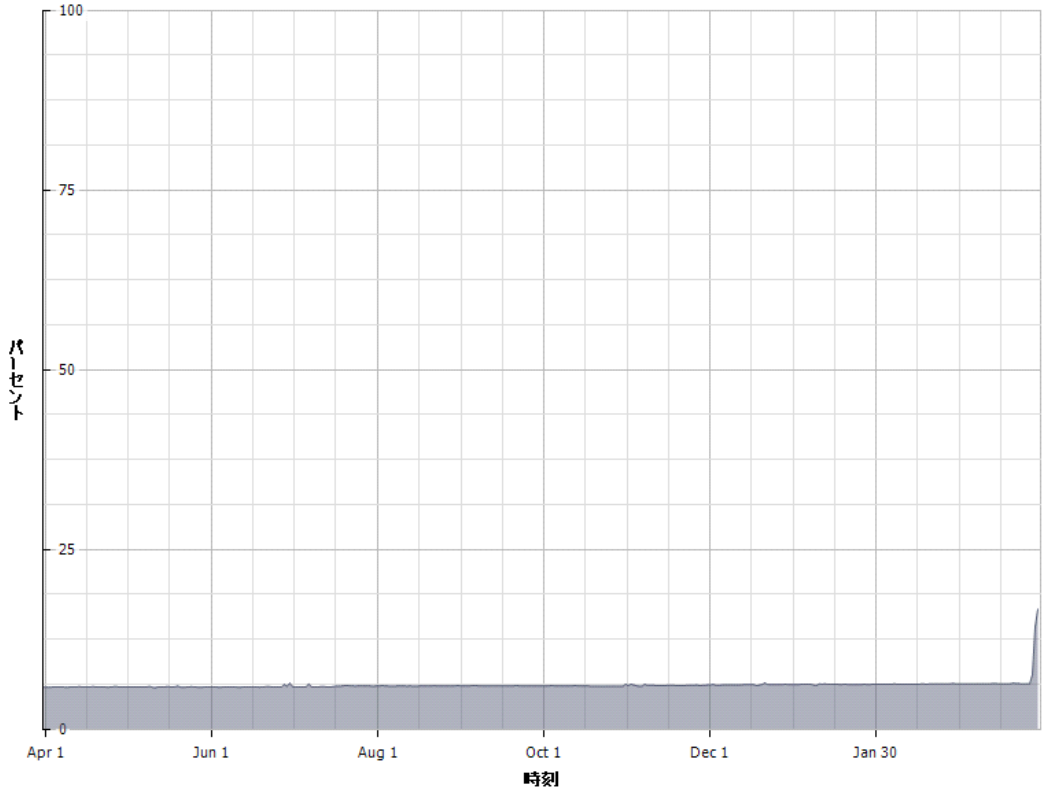


ネットワーク I/O 量

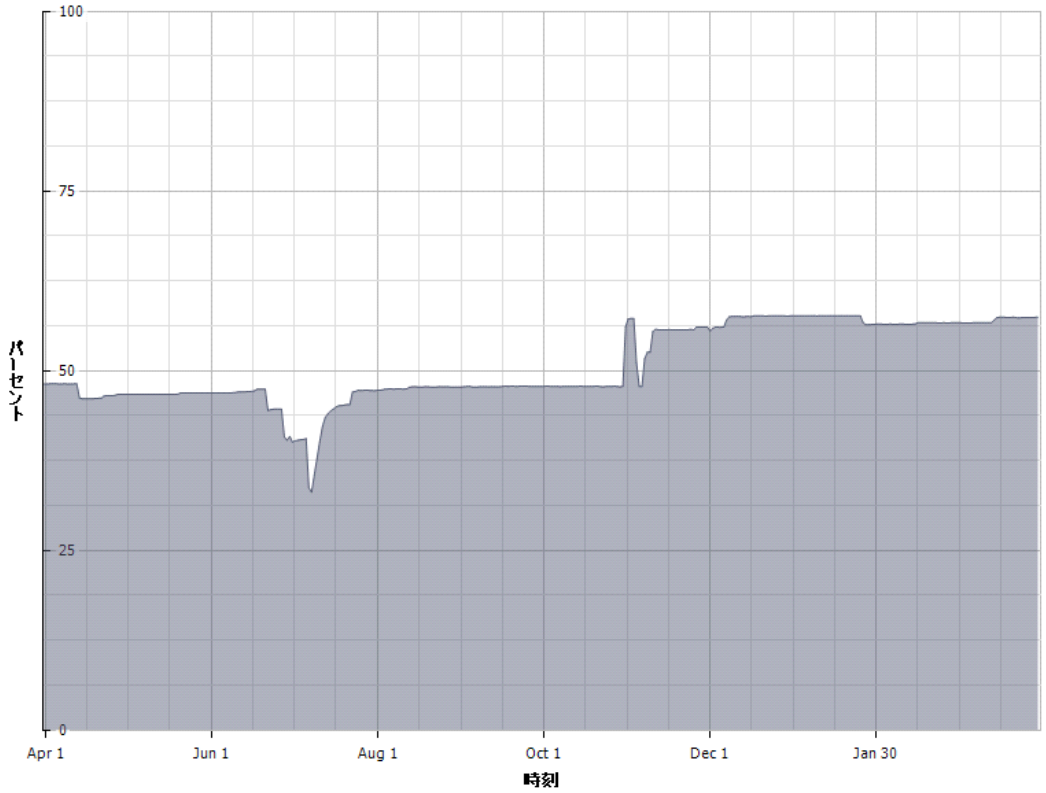


2.3.15　ESX15

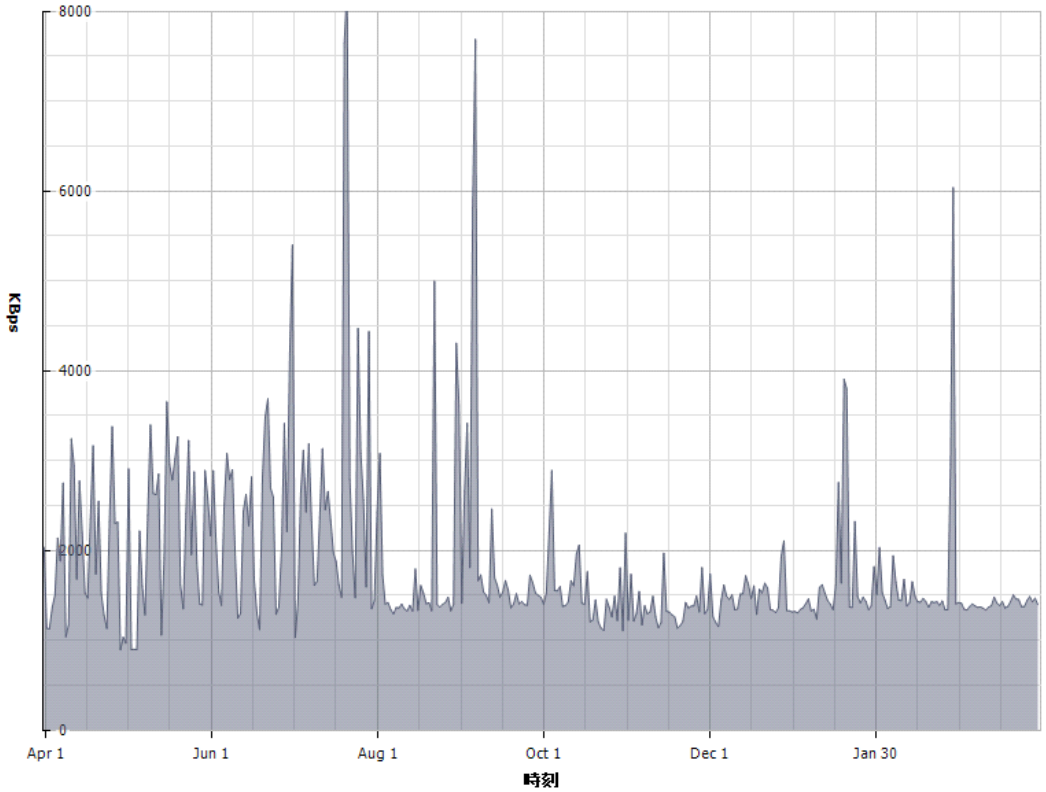
CPU 使用率



メモリ使用率

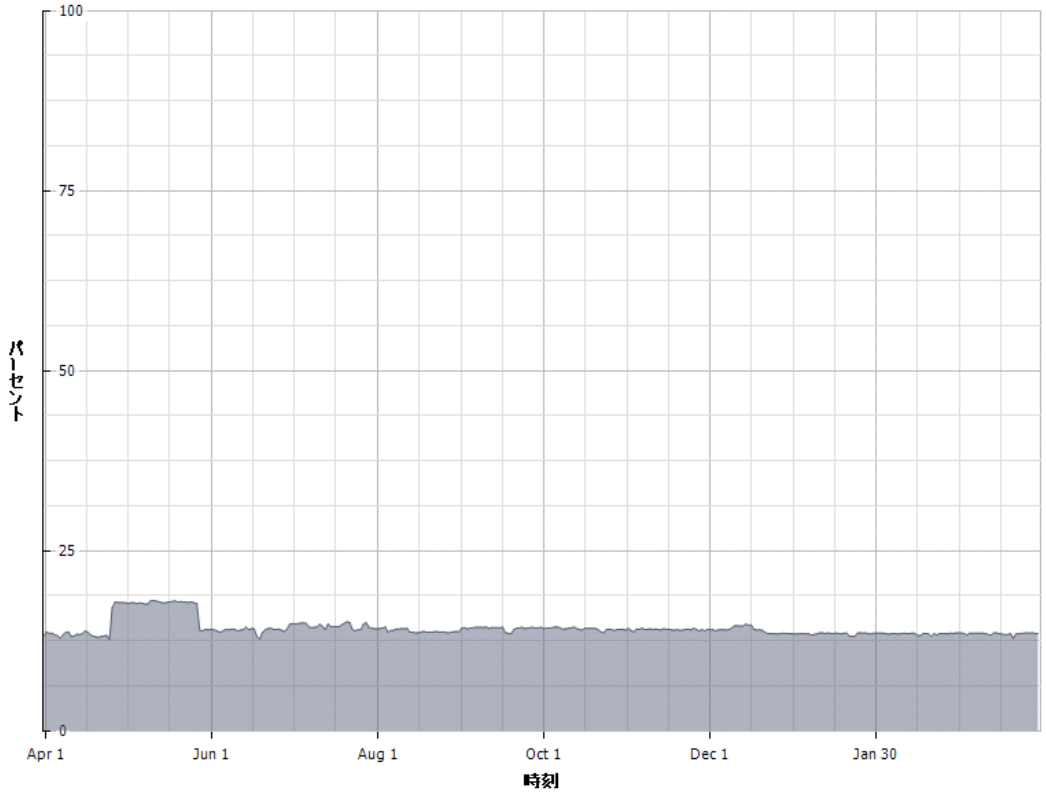


ネットワーク I/O 量

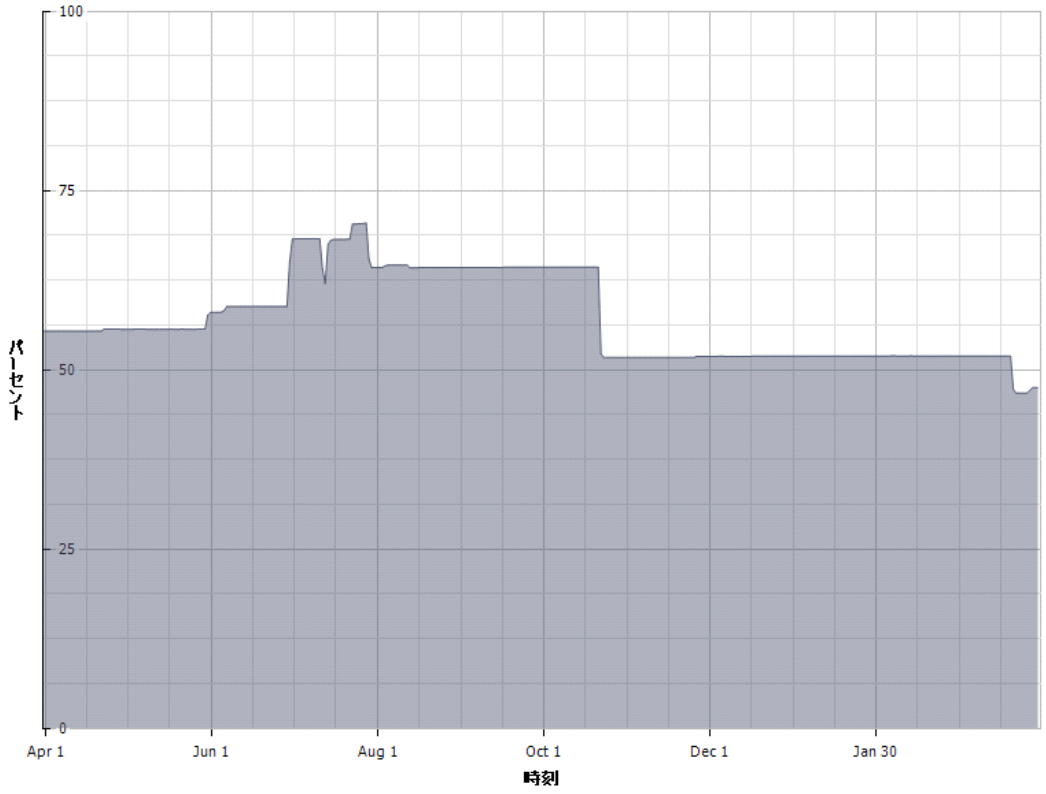


2.3.16　ESX16

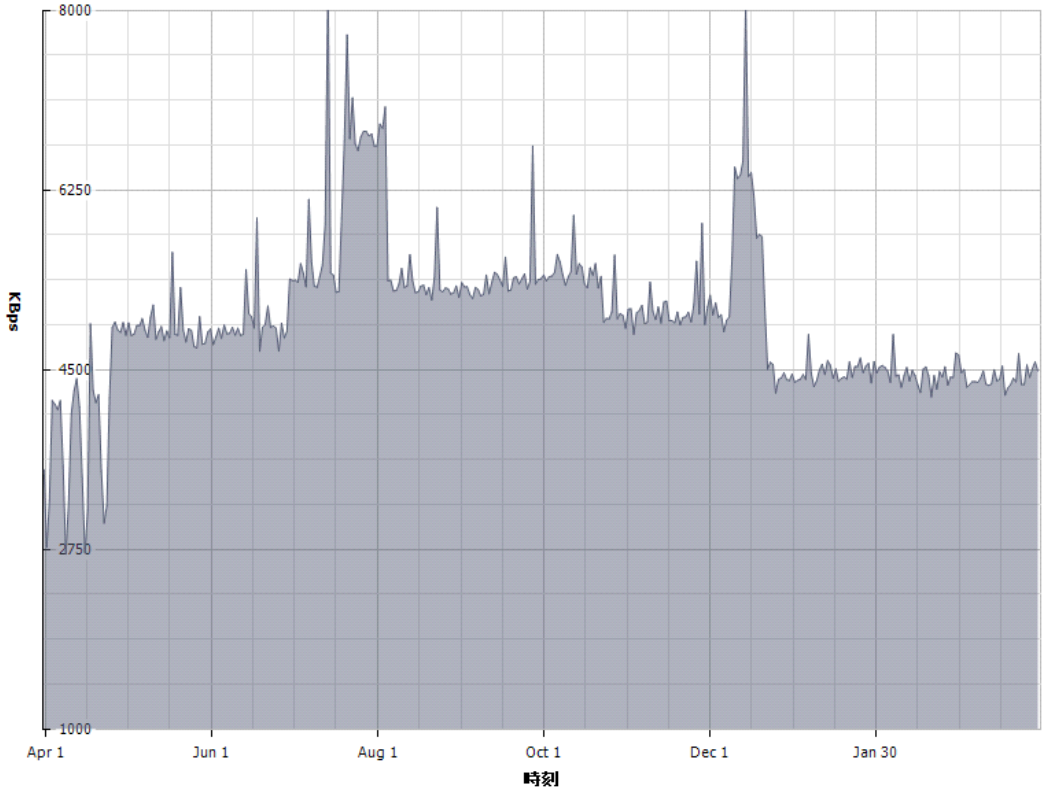
CPU 使用率



メモリ使用率



ネットワーク I/O 量


8000
6250
4500
2750
1000
kBps
Apr 1
Jun 1
Aug 1
Oct 1
Dec 1
Jan 30
時刻

2.4　実習室

実習室の利用状況については、平成 22 年度からパソコン必携化に伴い、平成 26 年度より B2 室のパソコンを図書館に移設し、自習利用しやすい環境を整備し、B1 室についても平成 27 年度よりパソコンの設置を廃止した。したがって、B1 及び B2 室にはパソコンが備えられていない。定常的な利用は、前期については 8 授業、後期については 7 授業であった。昨年度に比べ、3 授業増加している。パソコンの設置が A 室のみとなったため、授業での利用が減っているが、CAD 等の専門的なソフトウェアが必要な授業やスポット的にパソコンを使用する授業、研修などでよく使われている。

2.4.1 平成 28 年度前期

<table>
<tr><th>曜日</th><th>室</th><th>1〜2</th><th>3〜4</th><th>5〜6</th><th>7〜8</th><th>9〜10</th></tr>
<tr><td rowspan="3">月</td><td>A</td><td rowspan="3" colspan="2">保守</td><td colspan="2">工・機械設計システム工学科
機械要素設計製図及び CAD 実習(大西)</td><td></td></tr>
<tr><td>B1</td><td>工・電子物理工学科
工学英語 I(大崎,荒井)</td><td></td><td></td></tr>
<tr><td>B2</td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">火</td><td>A</td><td colspan="2">(9/6,9/13)1-9 時限
情報リテラシー研修</td><td>工・情報システム工学科
データベース(青木)</td><td colspan="2">(9/6,9/13)
情報リテラシー研修</td></tr>
<tr><td>B1</td><td></td><td></td><td></td><td>(9/6)学生支援部
全国一斉 WEB 模擬テスト(中原)</td><td></td></tr>
<tr><td>B2</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">水</td><td>A</td><td>教・学校教育デザイン I
(大泉)</td><td>(9/14)1-9 時限
情報リテラシー研修</td><td colspan="2">工・環境ロボティクス学科
プログラミング演習 II(横道)</td><td>(9/14)1-9 時限
情報リテラシー研修</td></tr>
<tr><td>B1</td><td></td><td>工・電子物理工学科
工学英語 I(大崎,荒井)</td><td></td><td></td><td></td></tr>
</table>

	B2					
木	A	(9/15) 情報リテラシー研修		農・植物生産環境科学科 コンピュータ図学及び製図(日吉)		
	B1					
	B2					
金	A				教・人間社会課程 プレゼンテーション 論(塚本)	
	B1					
	B2					

2.4.2 平成 28 年度後期

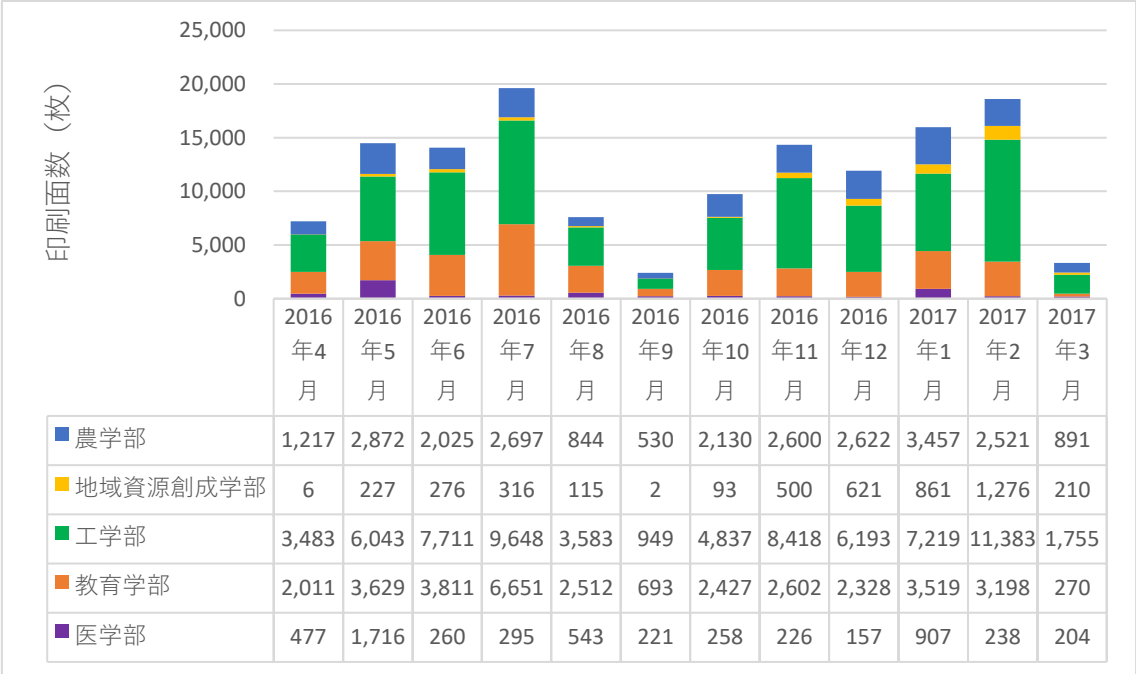
曜日	室	1～2	3～4	5～6	7～8	9～10
月	A	保守		工・機械システム工学科 プログラム言語及び演習(友松)		教・学校教育 デザイン II(大泉)
	B1			(2/27)農・獣医学科 獣医学共用試験【vetCBT】(保田)		
	B2			(2/27)農・獣医学科 獣医学共用試験【vetCBT】(保田)		
火	A	(3/21)1-10 限　農・獣医学科 獣医学共用試験【vetCBT】 追・再試験(保田)		(第 3 学期のみ)工・ 環境応用化学科 課題演習 I (廣瀬)	(2/7)学生支援部 全国一斉 WEB 模擬テスト	教・学校教育 デザイン III(樺島)
	B1	(3/21)農・獣医学科 獣医学共用試験【vetCBT】追・再試験(保田)				

	B2	(3/21)1-10 限 農・獣医学科 獣医学共用 試験 【vetCBT】追・ 再試験(保田)	工・大学院 (機械・情報系 コース) 生体情報工学 特論(青木)	(3/21)1-10 限　農・獣医学科 獣医学共用試験【vetCBT】追・再試験(保田)	
水	A	教・美術教育 デザイン I(大 泉)		(2/1)学生支援部 SPI 全国一斉 WEB 模擬テスト	
	B1			工・環境ロボティクス学科 プログラミング演習 I(高橋)	
	B2				
木	A	教・技術教育 情報処理学 (松澤)		(第 3 学期のみ)工・ 環境応用化学科 課題演習 I (廣瀬)	
	B1			(第 3 学期のみ)工・ 環境応用化学科 課題演習 I (廣瀬)	
	B2				
金	A			(1/20)農・獣医学科 【vetCBT】試験デモ(保田)	
	B1				
	B2				

2.5　宮大どこプリ（オンデマンドプリント）

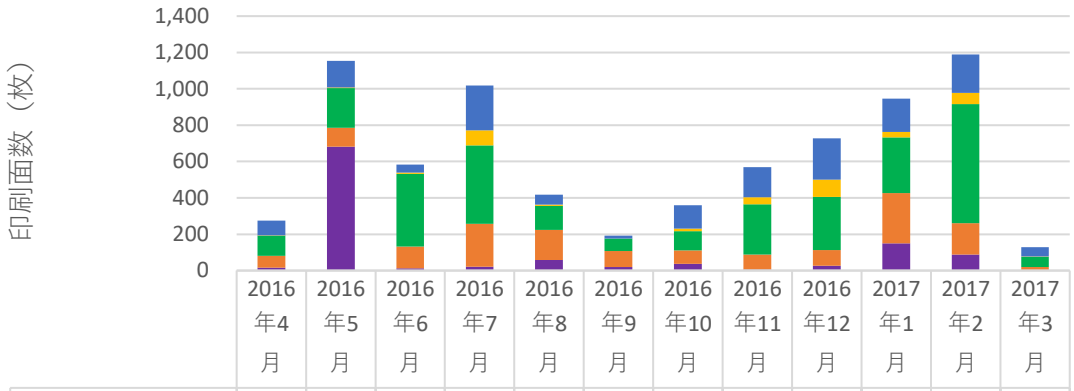
オンデマンドプリントサービスである「宮大どこプリ」は、利用の傾向は例年と変わらず 4 月から 7 月にかけて利用数が単調増加している。8 月および 9 月は夏休みのため利用があまりないが、9 月から 2 月にかけてまた利用数が増加している。7 月および 2 月の利用数が多くなっているが、この時期は学期末に当たるため、レポート等の提出のために印刷する機会が多くなっているものと思われる。平成 28 年度より、地域資源創成学部が新設されたが、全体としては、学部生、院生共に、昨年度ほとんど変わらない使用量であった。また、医学部生の利用が増えているのが特徴である。医学部のあるキャンパスにはプリンタを設置していないが、コンスタントに印刷があることから宮大どこプリの存在が認知されたのではないかと考えられる。

2.5.1 白黒印刷数（学部）



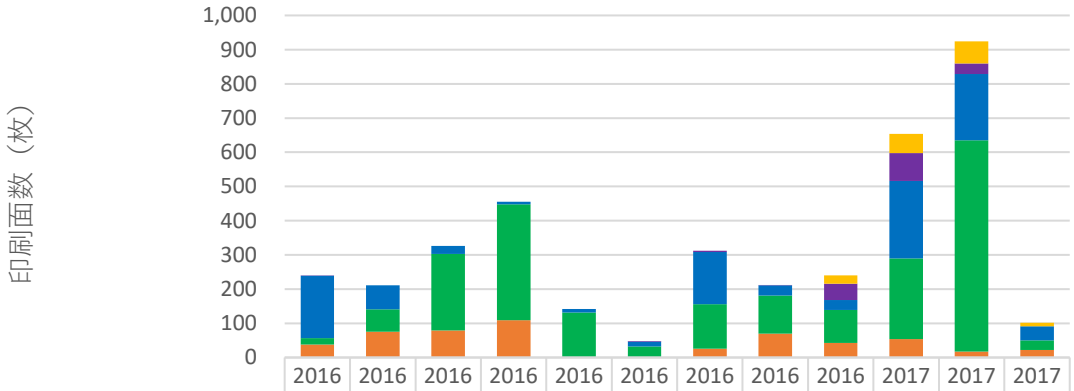
	2016年4月	2016年5月	2016年6月	2016年7月	2016年8月	2016年9月	2016年10月	2016年11月	2016年12月	2017年1月	2017年2月	2017年3月
農学部	1,217	2,872	2,025	2,697	844	530	2,130	2,600	2,622	3,457	2,521	891
地域資源創成学部	6	227	276	316	115	2	93	500	621	861	1,276	210
工学部	3,483	6,043	7,711	9,648	3,583	949	4,837	8,418	6,193	7,219	11,383	1,755
教育学部	2,011	3,629	3,811	6,651	2,512	693	2,427	2,602	2,328	3,519	3,198	270
医学部	477	1,716	260	295	543	221	258	226	157	907	238	204

2.5.2 カラー印刷数（学部）



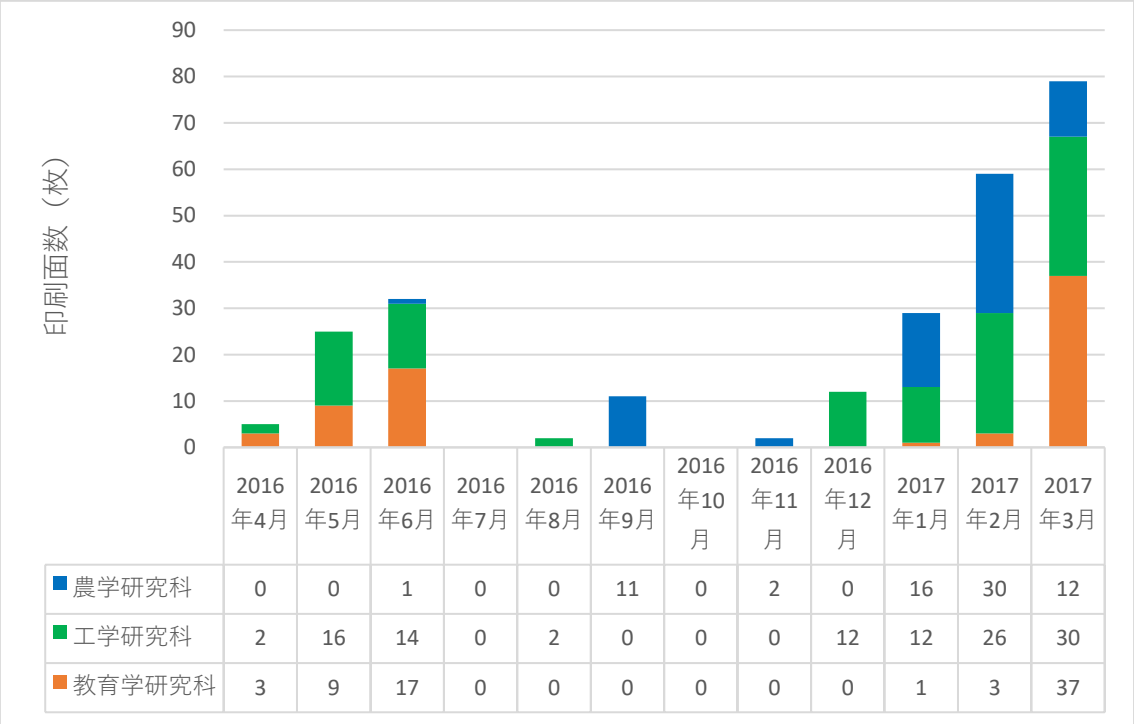
	2016年4月	2016年5月	2016年6月	2016年7月	2016年8月	2016年9月	2016年10月	2016年11月	2016年12月	2017年1月	2017年2月	2017年3月
農学部	81	145	44	246	55	17	129	166	226	183	211	51
地域資源創成学部	1	3	7	83	7	0	15	38	96	31	62	1
工学部	111	220	399	431	132	69	105	276	292	306	656	56
教育学部	66	104	120	237	166	87	74	83	87	276	171	16
医学部	16	681	13	21	58	20	37	6	26	150	89	4

2.5.3 白黒印刷数（大学院）



	2016年4月	2016年5月	2016年6月	2016年7月	2016年8月	2016年9月	2016年10月	2016年11月	2016年12月	2017年1月	2017年2月	2017年3月
農学工学総合研究科	0	0	0	0	0	0	0	0	24	56	64	11
医学獣医学総合研究科	1	0	0	0	0	2	4	1	48	82	31	0
農学研究科	182	70	23	7	10	14	152	30	29	226	194	41
工学研究科	19	66	224	339	132	32	130	111	96	236	618	28
教育学研究科	38	75	79	109	0	0	26	70	43	54	17	22

2.5.4 カラー印刷数（大学院）

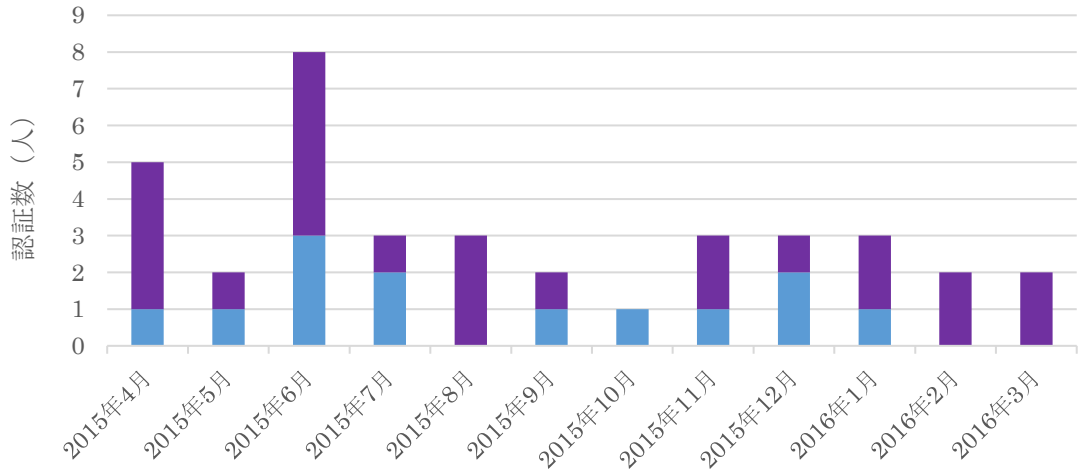


	2016年4月	2016年5月	2016年6月	2016年7月	2016年8月	2016年9月	2016年10月	2016年11月	2016年12月	2017年1月	2017年2月	2017年3月
農学研究科	0	0	1	0	0	11	0	2	0	16	30	12
工学研究科	2	16	14	0	2	0	0	0	12	12	26	30
教育学研究科	3	9	17	0	0	0	0	0	0	1	3	37

2.6　マイクロソフト包括ライセンスソフトウェア

マイクロソフト包括ライセンスにより利用できる Office 2010、Office 2013、Office 2016、Windows 7、Windows 8（Windows 8.1 を含む）及び Windows 10 について認証した人数をまとめた。昨年度までは、Office 2013 及び Windows 7 の使用が主流であったが、Office 2016 と Windows 10 の使用が主流となったことがとなったことがうかがえる。利用傾向としては、オフィスソフト、OS 共に年度初めの 4 月に集中しており、これは必携 PC へのインストールが大きく影響している。この傾向は毎年度変わらない傾向である。

2.6.1 Office 2010

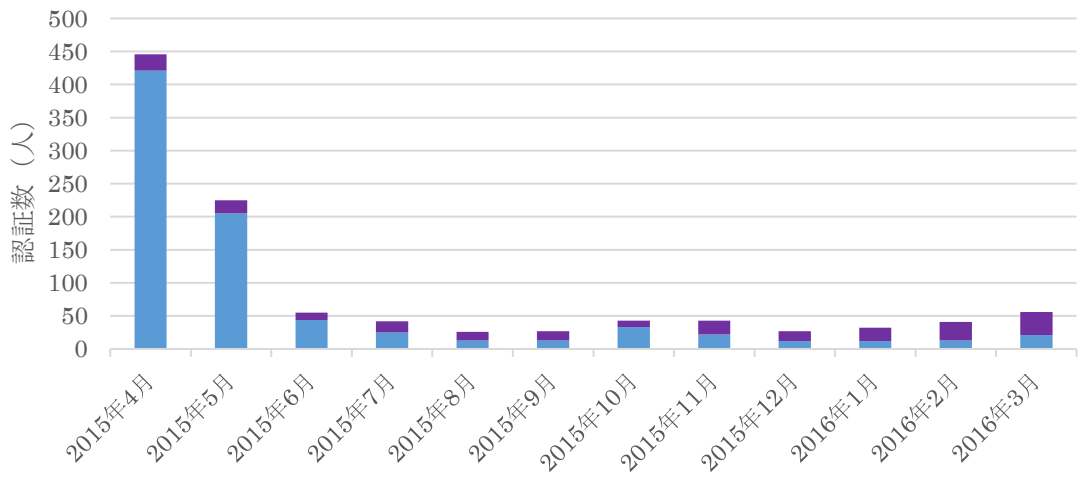


	2015年4月	2015年5月	2015年6月	2015年7月	2015年8月	2015年9月	2015年10月	2015年11月	2015年12月	2016年1月	2016年2月	2016年3月
■教職員	4	1	5	1	3	1	0	2	1	2	2	2
■学生	1	1	3	2	0	1	1	1	2	1	0	0

2.6.2 Office 2013

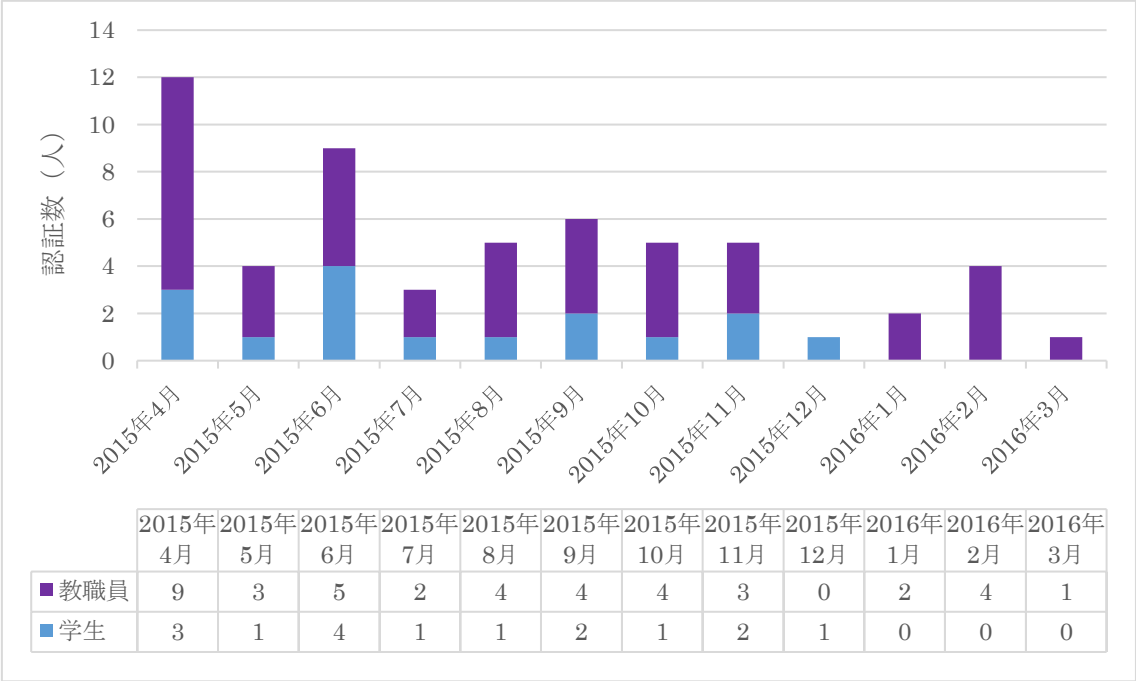
	2015年4月	2015年5月	2015年6月	2015年7月	2015年8月	2015年9月	2015年10月	2015年11月	2015年12月	2016年1月	2016年2月	2016年3月
■教職員	8	7	9	9	5	8	3	3	7	3	8	9
■学生	15	11	10	6	10	8	8	14	13	15	7	17

2.6.3 Office 2016



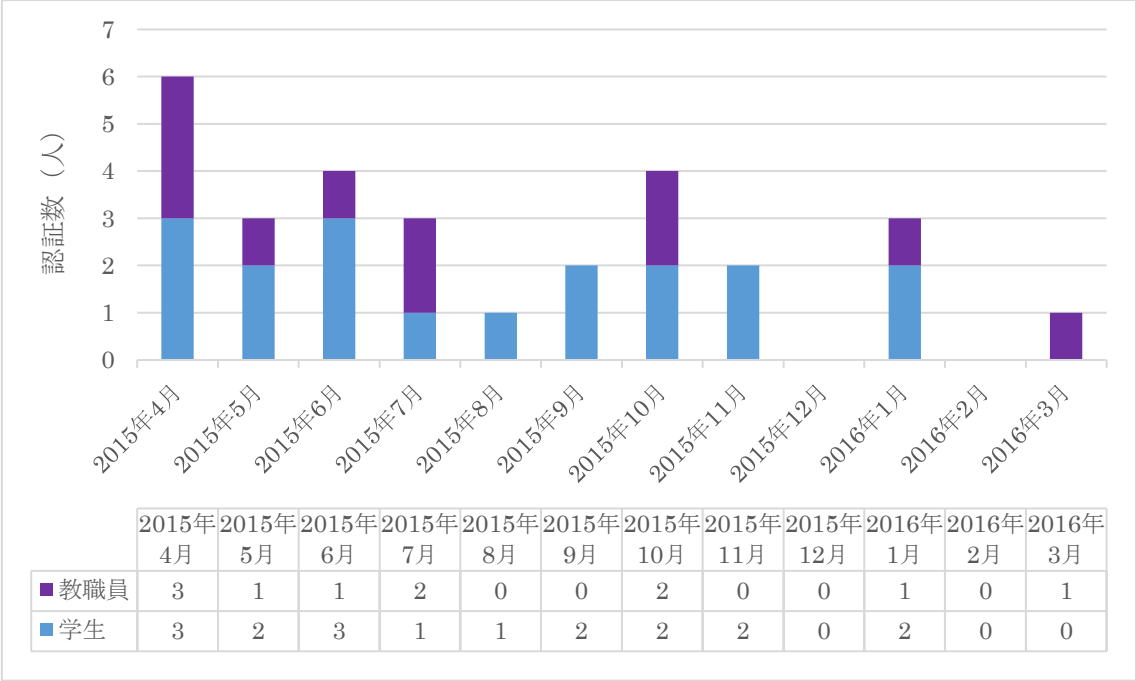
	2015年4月	2015年5月	2015年6月	2015年7月	2015年8月	2015年9月	2015年10月	2015年11月	2015年12月	2016年1月	2016年2月	2016年3月
■教職員	25	20	11	17	13	14	10	21	15	20	28	35
■学生	421	205	44	25	13	13	33	22	12	12	13	21

2.6.4 Windows 7



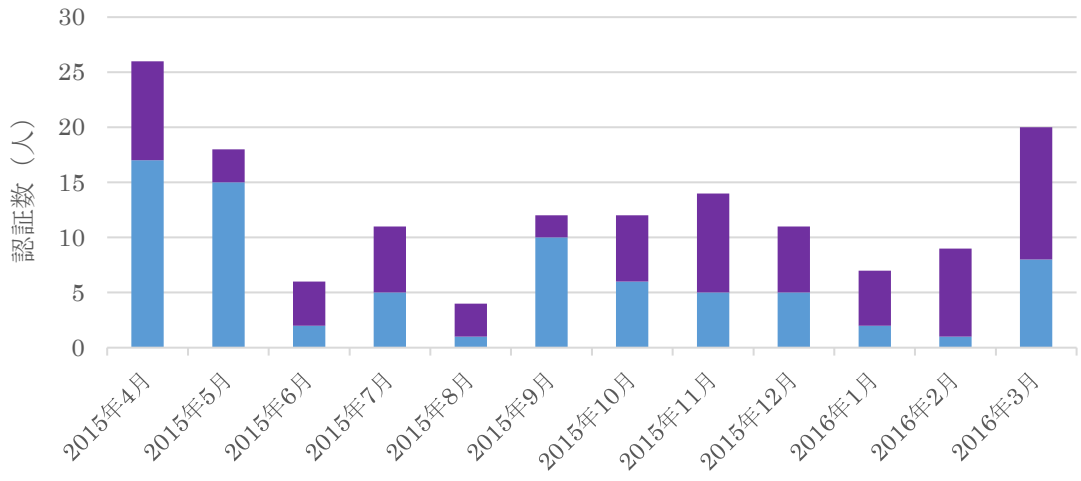
	2015年4月	2015年5月	2015年6月	2015年7月	2015年8月	2015年9月	2015年10月	2015年11月	2015年12月	2016年1月	2016年2月	2016年3月
■教職員	9	3	5	2	4	4	4	3	0	2	4	1
■学生	3	1	4	1	1	2	1	2	1	0	0	0

2.6.5 Windows 8（8.1 を含む）



	2015年4月	2015年5月	2015年6月	2015年7月	2015年8月	2015年9月	2015年10月	2015年11月	2015年12月	2016年1月	2016年2月	2016年3月
■教職員	3	1	1	2	0	0	2	0	0	1	0	1
■学生	3	2	3	1	1	2	2	2	0	2	0	0

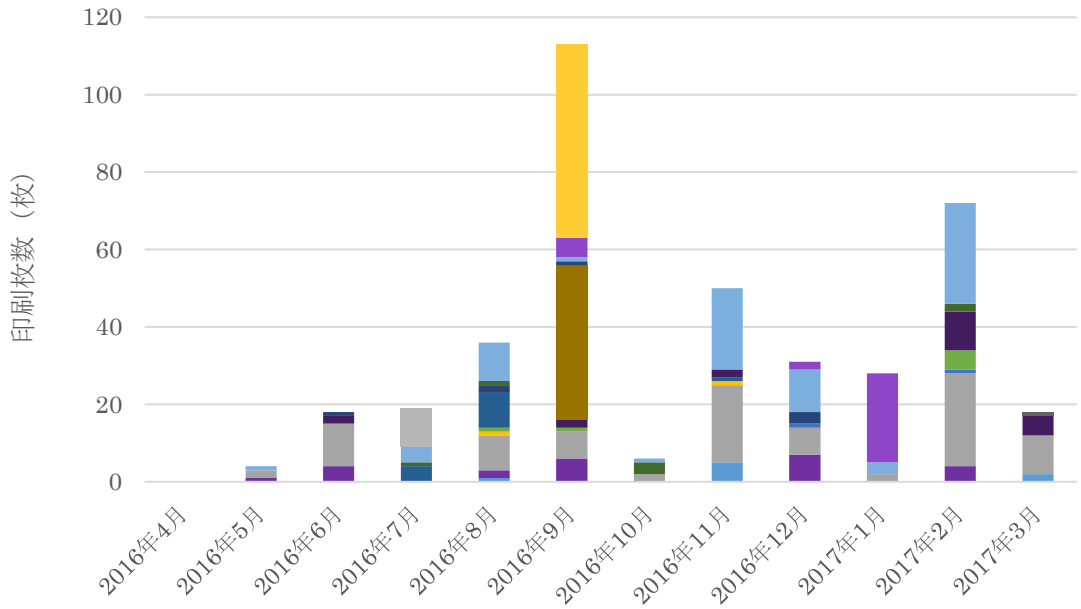
2.6.6 Windows 10



	2015年4月	2015年5月	2015年6月	2015年7月	2015年8月	2015年9月	2015年10月	2015年11月	2015年12月	2016年1月	2016年2月	2016年3月
■教職員	9	3	4	6	3	2	6	9	6	5	8	12
■学生	17	15	2	5	1	10	6	5	5	2	1	8

2.7　大判プリンタ

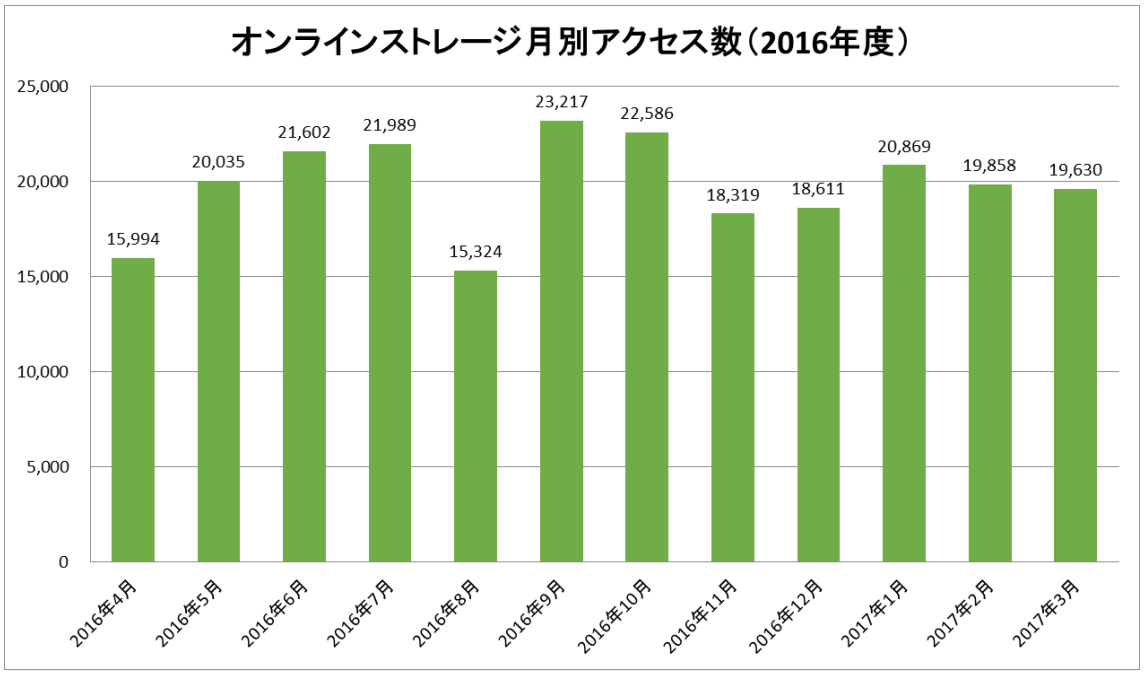
大判プリンタサービスは定常的に使用されないものの、11 月は学会シーズンで、2 月は卒論シーズンであるため利用が増えている。この傾向は昨年度と同様である。ただし、平成 28 年度は、9 月に特定の利用者によって大量に使用されたため、9 月の使用量が特出して増えている。また、用紙サイズとして A0 が最も多く使われており、用紙の種類として、光沢紙または普通紙が利用される頻度が高い。この傾向も昨年度と同様である。一部の利用者からは、布などを使いたいという要望も出ている。



	2016年4月	2016年5月	2016年6月	2016年7月	2016年8月	2016年9月	2016年10月	2016年11月	2016年12月	2017年1月	2017年2月	2017年3月
普通 B3						50						
普通 A2				10								
普通 A1						5			2	23		
普通 A0		1		4	10	1	1	21	11	3	26	
普通 B1				1	1		3				2	
普通 B0			1		2	1			3			
マット B3						40						
マット A1												1
マット A0			2			2		2			10	5
マット B1				4	9			1				
マット B0					1	1					5	
光沢 A2									1		1	
光沢 A1					1			1				
光沢 A0		2	11		9	7	2	20	7	2	24	10
光沢 B1		1	4		2	6			7		4	
光沢 B0					1			5				2

2.8　オンラインストレージ

平成 27 年度より、オンラインストレージサービスを開始した。全学生及び全教職員が使用することができ、ファイルの保存、共有、Web 公開の機能を持っている。8 月の夏期休暇時期にはアクセス数が減っているものの、毎月 20,000 回程度のコンスタントなアクセスがあった。平成 28 年度は、USB メモリの代替手段としてオンラインストレージの利用を推奨したことから、昨年度より利用が増えている。



3　関連規程等

○宮崎大学情報統括機構規則

平成 22 年 9 月 22 日
制定
改正平成 23 年 9 月 22 日
平成 27 年 10 月 1 日

（趣旨）
第 1 条　この規則は、国立大学法人宮崎大学基本規則第 16 条の 2 第 2 項の規定に基づき、宮崎大学（以下「本学」という。）における情報統括機構に関し、必要な事項を定めるものとする。
（情報統括機構）
第 2 条　情報統括機構に、情報化統括責任者（以下「CIO」という。）、情報化統括責任者補佐官（以下「CIO 補佐官」という。）、情報化推進会議及び情報基盤センターを置く。
（情報化統括責任者）
第 3 条　CIO は、本学の情報化推進及び情報運用実務の遂行等を統括し、また、本学の情報資産の適切かつ円滑な管理運用を統括する。
2　CIO は、研究・企画担当理事をもって充てる。
（情報化統括責任者補佐官）
第 4 条　CIO 補佐官は、戦略的・専門的知見をもって CIO に情報化推進に関する支援・助言を行う。
2　CIO 補佐官は、CIO が推薦し学長が任命する。
3　CIO 補佐官の任期は、2 年とする。ただし、CIO 補佐官の任期の末日は、CIO の任期の末日以前とする。
（情報化推進会議）
第 5 条　情報化推進会議は、本学の情報化推進業務の統括を行うとともに、本機構の自己点検・評価を行うものとする。
2　情報化推進会議の組織及び運営に関し必要な事項は、別に定める。
（情報基盤センター）
第 6 条　情報基盤センターは、本学における情報施策の立案・策定、点検・検証及び情報基盤、情報システム等の運用管理を行うとともに、情報利用者支援を行う。
2　情報基盤センターの組織及び運営に関し必要な事項は、別に定める。
（雑則）
第 7 条　この規則に定めるもののほか、情報統括機構に関し必要な事項は、別に定める。

附則
1　この規則は、平成 22 年 10 月 1 日から施行する。

２　宮崎大学情報化推進組織等に関する規程（平成 19 年 10 月 25 日制定）は、廃止する。

附則

この規則は、平成 23 年 10 月 1 日から施行する。

附則

この規則は、平成 27 年 10 月 1 日から施行する。

〇宮崎大学情報化推進会議規程

平成 19 年 10 月 25 日
制定
改正　平成 20 年 5 月 22 日
平成 22 年 9 月 22 日
平成 23 年 3 月 29 日
平成 28 年 3 月 25 日

（趣旨）

第１条　この規程は、宮崎大学情報統括機構規則（以下「規則」という。）第５条第２項の規定に基づき、宮崎大学情報化推進会議（以下「会議」という。）の組織及び運営に関し、必要な事項を定めるものとする。

（目的）

第２条　会議は、宮崎大学（以下「本学」という。）の情報化推進の統括を行うとともに、情報基盤センターの業務に対する自己点検・評価を行い、本学の情報化を適切かつ円滑に推進することを目的とする。

（任務）

第３条　会議は、次に掲げる事項を審議又は実施する。

(1) 本学の情報化推進における業務統括に関すること。
(2) 情報基盤センターの事業計画及び運営経費に関すること。
(3) 情報基盤センター専任教員の選考に関すること。
(4) 情報基盤センターの業務についての自己点検・評価に関すること。
(5) 本学の情報システム、情報ネットワーク等の計画・策定等に関すること。
(6) 情報セキュリティに関すること。
(7) 最適化計画及び各種ポリシーに関すること。
(8) 情報管理に関する将来構想に関すること。
(9) その他情報基盤センターの運営に関すること。

（委員）

第４条　会議は、次に掲げる委員をもって組織する。

(1) 情報化統括責任者（CIO）
(2) 副学長のうちから、CIO の推薦に基づき、学長が指名する者

(3) 総務担当理事
(4) 情報基盤センター長
(5) 情報化統括責任者補佐官（CIO 補佐官）
(6) 副情報基盤センター長
(7) 医学部附属病院医療情報部長
(8) 情報基盤センター事務長
(9) その他 CIO が必要と認める者
２ 前項の委員が事務職員の場合は、前条第３号に定める審議事項には加わらないものとする。
（委員長）
第５条　会議に委員長を置き、委員長は前条第１号の委員をもって充てる。
２ 委員長は会議を招集し、その議長となる。
（議事）
第６条　会議は、委員の３分の２以上の出席により成立する。
２ 議事は出席委員の過半数をもって決し、可否同数のときは議長の決するところによる。
（委員以外の出席）
第７条　会議が必要と認めたときは、委員以外の者を会議に出席させることができる。
（事務）
第８条　会議の事務は、情報図書部情報企画課において処理する。
（雑則）
第８条　この規程に定めるもののほか、会議の議事及び運営に関し必要な事項は、別に定める。

附則
この要項は、平成 19 年 11 月 1 日から施行する。
附則
この要項は、平成 20 年 5 月 22 日から施行する。
附則
この規程は、平成 22 年 10 月 1 日から施行する。
附則
この規程は、平成 23 年 3 月 29 日から施行する。
附則
この規程は、平成 28 年 4 月 1 日から施行する。

〇宮崎大学情報基盤センター規程

平成 22 年 9 月 22 日

制定
改正　平成 25 年 2 月 28 日
平成 28 年 3 月 25 日

（趣旨）
第１条　この規程は、宮崎大学情報統括機構規則第６条第２項の規定に基づき、宮崎大学情報基盤センター（以下「センター」という。）の組織及び運営に関し、必要な事項を定めるものとする。
（目的）
第２条　センターは、宮崎大学（以下「本学」という。）における情報施策の立案・策定、点検・検証及び情報基盤、情報システム等の運用管理を行うとともに、情報利用者支援を行うことを目的とする。
（清武分室）
第３条 前条の目的を達成するため、センターに清武分室（以下「分室」という。）を置く。
（部門及び業務）
第４条　第２条の目的を達成するため、センターに次の各号に掲げる部門を置き、当該各号に定める業務を行う。
(1) 情報基盤部門
ア　情報化推進の立案・策定・実施に関すること。
イ　事業計画の実施及び管理経費の執行に関すること。
ウ　学内情報基盤の整備、更新及び運用管理に関すること。
エ　学内情報ネットワーク及び情報システムの整備、更新及び運用管理に関すること。
オ　学外情報ネットワークとの連携、その利用及び支援に関すること。
カ　その他情報化支援に関すること。
(2) 利用者支援部門
ア　学内情報ネットワーク及び情報システム利用者の支援に関すること。
イ　情報教育の支援に関すること。
ウ　各種情報システムの支援に関すること。
エ　情報セキュリティに関すること。
オ　最適化計画及び各種ポリシーの策定・実施に関すること。
カ　その他利用者支援に関すること。
（職員）
第５条　センターに、次に掲げる職員を置く。
(1) センター長
(2) 副センター長
(3) 分室長
(4) 部門長
(5) 室員

⑹ 専任教員
⑺ 兼任教員
⑻ その他必要な職員
（センター長）
第６条　センター長は、センターの業務を統括する。
２ センター長は、本学専任の教授のうちから、宮崎大学センター管理運営委員会の議を経て学長が任命する。
３ センター長の任期は２年とし、再任を妨げない。ただし、欠員が生じた場合の後任者の任期は、前任者の残任期間とする。
（副センター長）
第７条　副センター長は、センター長の業務を補佐する。
２ 副センター長は、センター専任教員のうちからセンター長が指名する者をもって充てる。
３ 副センター長の任期は２年とし、再任を妨げない。ただし、欠員が生じた場合の後任者の任期は、前任者の残任期間とする。
（分室長）
第８条 分室長は、センター長の命を受け、分室の業務を掌理する。
２ 分室長は、医学部附属病院医療情報部長をもって充てる。
（部門長）
第９条　部門長は、当該部門の業務を掌理する。
２ 当該部門長は、センター専任教員のうちからセンター長が指名する者をもって充てる。
（室員）
第１０条 室員は、分室の業務を処理する。
２ 室員は、医学部附属病院医療情報部の専任教員をもって充てる。
（専任教員）
第１１条　専任教員は、当該部門の業務を処理する。
２ 専任教員の選考に係る事項については、別に定める。
（兼任教員）
第１２条　兼任教員は、当該部門の業務を処理する。
２ 兼任教員は、本学教員のうちからセンター長の推薦に基づき、学長が委嘱する。
３ 兼任教員の任期は２年とし、再任を妨げない。ただし、欠員が生じた場合の後任者の任期は、前任者の残任期間とする。
（運営委員会）
第１３条　センターの管理及び運営に関する重要事項を審議するため、宮崎大学情報基盤センター運営委員会（以下「運営委員会」という。）を置く。
２ 運営委員会の組織運営に関し必要な事項は、別に定める。
（部門会議）
第１４条　各部門の事業を円滑に推進するため、部門会議を置く。

２ 部門会議の組織運営に関し必要な事項は、別に定める。
（事務）
第１４条　センターの事務は、情報基盤センター事務部が行う。
（雑則）
第１５条　この規程に定めるもののほか、センターに関し必要な事項は、別に定める。

附則
１ この規程は、平成 22 年 10 月 1 日から施行する。
２ 宮崎大学情報戦略室要項（平成 19 年 7 月 19 日制定）及び宮崎大学情報支援センター要項（平成 19 年 10 月 25 日制定）は、廃止する。
附則
この規程は、平成 25 年 4 月 1 日から施行する。
附則
この規程は、平成 28 年 4 月 1 日から施行する。

〇宮崎大学情報基盤センター運営委員会規程

平成 22 年 9 月 22 日
制定
改定　平成 24 年 3 月 29 日
平成 25 年 2 月 28 日
平成 28 年 3 月 25 日

（趣旨）
第１条　この規程は、宮崎大学情報基盤センター規程第１３条第２項の規定に基づき、宮崎大学情報基盤センター運営委員会（以下「運営委員会」という。）の組織及び運営に関し、必要な事項を定めるものとする。
（審議事項）
第２条　運営委員会は、次に掲げる事項を審議する。
(1) 情報基盤センター（以下「センター」という。）の事業計画及び運営経費に関する事項
(2) センターの施設・設備の改善に関する事項
(3) 学内情報基盤の整備、更新に関する事項
(4) 情報セキュリティに関する事項
(5) 最適化計画及び各種ポリシーに関する事項
(6) 利用者支援に関する事項
(7) その他センターの運営に関する事項
（組織）
第３条　運営委員会は、次に掲げる委員をもって組織する。

(1) センター長
(2) 副センター長
(3) 分室長
(4) センター各部門の部門長
(5) 教育学部、医学部、農学部、地域資源創成学部及び工学教育研究部から選出された教授又は 准教授 各１人
(6) 情報基盤センター事務長
(7) その他運営委員会が必要と認める者

（任期）
第４条　前条第５号及び第７号の委員の任期は２年とし、再任を妨げない。ただし、委員に欠員が生じた場合の後任者の任期は、前任者の残任期間とする。

（委員長）
第５条　運営委員会に委員長を置き、第３条第１号の委員をもって充てる。
２ 委員長は、運営委員会を招集し、その議長となる。
３ 委員長に事故あるときは、第３条第２号の委員がその職務を代行する。

（議事）
第６条　運営委員会は、委員の半数以上の出席により成立する。
２ 議事は、出席委員の過半数をもって決し、可否同数のときは議長の決するところによる。

（委員以外の出席）
第７条　運営委員会が必要と認めたときは、委員以外の者を運営委員会に出席させることができる。

（専門委員会）
第８条　運営委員会は、必要に応じて専門委員会を置くことができる。
２ 専門委員会に関する必要な事項は、委員会が別に定める。

（事務）
第９条　運営委員会の事務は、情報基盤センター事務部において処理する。

（雑則）
第１０条　この規程に定めるもののほか、運営委員会の議事及び運営に関し必要な事項は、運営委員会が定める。

附則
この規程は、平成 22 年 10 月１日から施行する。
附則
この規程は、平成 24 年４月１日から施行する。
附則
この規程は、平成 25 年４月１日から施行する。
附則

１　この規程は、平成 28 年４月１日から施行する。
２　この規程の施行後、最初に選出される教育学部及び地域資源創成学部の委員、相談員又は兼任 教員（以下「委員等」という。）の任期の末日は、当該委員等の任期の規定にかかわらず他学部 選出の委員等の任期の末日と同じ日とする。

〇宮崎大学情報セキュリティ基本規程

平成 19 年 12 月 20 日
制定
改正　平成 22 年９月 22 日
平成 23 年３月 29 日
平成 26 年２月 27 日
平成 28 年３月 25 日

（趣旨）
第１条　この規程は、宮崎大学（以下「本学」という。）の「情報セキュリティ基本方針」に基づき、本学の情報資産、情報ネットワーク及び情報システムに関するセキュリティ対策に必要な措置についての基本事項を定めるものとする。
（適用範囲）
第２条　本規程は、本学における情報資産、情報ネットワーク及び情報システムを運用、管理、利用する全ての者に適用する。
（定義）
第３条　本規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。
(1) 情報資産記録の媒体を問わず、本学が所有又は管理する情報全般をいう。
(2) 情報ネットワーク本学により、所有又は管理されている全ての情報ネットワーク、本学との契約又は他の協定に従って提供される全ての情報ネットワークをいう。
(3) 情報システム情報処理及び情報ネットワークに係わる全てのシステムをいう。
(4) 情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報、情報システムに関係がある書面に記載された情報をいう。
(5) 教職員等 本学に勤務する常勤又は非常勤の役員・教職員（派遣職員を含む。）をいう。
(6) 学生等学生、研究生、研究員、研修員、研究者をいう。
(7) 利用者教職員等及び学生等で、本学の情報資産、情報ネットワーク又は情報システムを利用する者をいう。
(8) 情報セキュリティ情報資産の機密性、完全性及び可用性を維持することをいう。
(9) 電磁的記録電子的方式、磁気的方式などで作られる記録であって、コンピュータによる情報処理の用に供されるものをいう。
(10) インシデント情報セキュリティに関し、意図的又は偶発的に生じる、学内規則等又は法律に反する事故・事件をいう。

(11) 明示等情報を取り扱う全ての者が当該情報の格付けについて共通の認識となるように措置することをいう。

（最高情報セキュリティ責任者）

第４条　本学における情報セキュリティ対策の最高責任者として、最高情報セキュリティ責任者（Chief Information Security Officer；CISO、以下「CISO」という。）を置く。

２ CISO は、本学における情報セキュリティ対策に関する事項を統括するとともに、本学における情報セキュリティ対策の推進体制が十分機能するように管理する。

３ CISO は、本学の教職員等の中から、学長が任命する。

４ CISO に事故があるときは、CISO があらかじめ指名する者が、その職務を代行する。

５ CISO は、情報セキュリティに関する専門的な知識等の助言を受けるために情報セキュリティアドバイザーを置く。情報セキュリティアドバイザーには、CIO 補佐官をもって充てる。

（情報セキュリティ委員会）

第５条　本学の情報資産の円滑で適正な運用を実現するための方針及び情報セキュリティに関する事項を決定する機関として、宮崎大学情報セキュリティ委員会を置き、次に掲げる事項を審議する。

(1) 情報化推進会議及び情報基盤センターにおいて企画又は策定される情報セキュリティに関連する各種事案に関する事項

(2) 情報セキュリティ対策活動に係る実施計画及び実施結果に関する事項

(3) インシデントへの対応及び再発防止対策に関する事項

(4) 情報運用におけるリスク管理に関する事項

(5) その他情報セキュリティに関する事項

２ 情報セキュリティ委員会は、次に掲げる委員をもって組織する。

(1) CISO

(2) 情報化統括責任者（CIO）

(3) 情報基盤センター長

(4) 副情報基盤センター長

(5) 部局情報セキュリティ責任者

(6) その他 CISO が必要と認める者

３ 情報セキュリティ委員会に委員長を置き、委員長は前項第１号の委員をもって充てる。

４ 委員長は情報セキュリティ委員会を招集し、その議長となる。

（部局情報セキュリティ責任者）

第６条　CISO は、情報セキュリティ対策の運用に係る管理を行う単位としての部局を定め、部局における情報セキュリティ対策の責任者として部局情報セキュリティ責任者を置く。

２ 部局情報セキュリティ責任者は、当該部局における情報セキュリティ対策に関する事項を統括する。

３ 部局情報セキュリティ責任者は、部局の長又は部局情報運用を統括する者をもって充て

る。
４ 部局情報セキュリティ責任者は、当該部局の専任の教職員の中から部局情報技術責任者を任命し、部局の情報システムに対する情報セキュリティ対策の実施を委任する。
５ 部局情報セキュリティ責任者は、部局情報セキュリティ委員会を設置し、当該部局における情報セキュリティ対策を推進する。
（情報セキュリティ担当者連絡会）
第７条　本学の情報セキュリティ対策、インシデント対応及び再発防止策等の推進並びに各部局間の情報共有及び連絡・調整を行うため、宮崎大学情報セキュリティ担当者連絡会を置く。
２ 宮崎大学情報セキュリティ担当者連絡会の組織運営に関し必要な事項は、別に定める。
（情報セキュリティインシデント対応チーム）
第８条 本学において発生した情報セキュリティインシデントへの速やかな対応及び情報セキュリティインシデント発生の防止のために、宮崎大学情報セキュリティインシデント対応チームを置く。
２ 宮崎大学情報セキュリティインシデント対応チームの組織及び運営に関して必要な事項は、別に定める。
（情報セキュリティの監査・点検）
第９条　情報基盤センターは、情報セキュリティにおける調査及びセキュリティ監査・点検等に関する事項を実施する。
２ 情報基盤センターに情報セキュリティの監査・点検を行う責任者として、情報セキュリティ監査責任者を置き、部局情報セキュリティ責任者が所管する組織における情報セキュリティ監査・点検の実施を統括する。
３ 情報セキュリティ監査責任者は、情報システムのセキュリティ対策が本学の情報セキュリティポリシー及び関連規程に基づく手順等に従って実施されていることを監査する。
（情報セキュリティ対策の推進）
第１０条　情報基盤センターは、情報セキュリティ対策の具体的遂行や遂行の統括等を行う。
２ 情報基盤センターに情報セキュリティ対策の推進と実施を行う責任者として、情報セキュリティ対策実施責任者を置き、部局情報セキュリティ責任者が実施する対策事項を統括する。また、情報セキュリティ対策実施責任者は、情報セキュリティ関連規程中の対策項目の遵守を推進する。
（情報の格付け）
第１１条　情報の電磁的記録については機密性、完全性及び可用性の観点から、また、書面については機密性の観点から、当該情報の格付け及び取扱制限の指定並びに明示等を行わなければならない。
（利用者による情報セキュリティ維持）
第１２条　利用者は、本学の情報セキュリティポリシー及び関連規程を遵守し、本学及び本

学以外の情報セキュリティ水準の低下を招く行為を行ってはならない。
２ 利用者は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行う。
（外部委託管理）
第１３条　本学の情報又は情報システムの運用業務の全て又はその一部を第三者に委託する場合には、当該第三者による情報セキュリティの確保が徹底されるよう必要な措置を講じなければならない。
（違反及び例外措置）
第１３条　利用者は、情報セキュリティ関連規程への重大な違反（当該違反により本学の業務に重大な支障を来すもの又はその可能性のあるもの）を知った場合には、当該規程の実施に責任を持つ部局情報セキュリティ責任者にその旨を報告しなければならない。
２ 部局情報セキュリティ責任者は、前項に規定する報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じるとともに、CISO にその旨を報告しなければならない。
３ 情報セキュリティ関連規程の適用が職務の適正な遂行を著しく妨げる等の理由により、情報セキュリティ関連規程の規定とは異なる代替の方法を採用すること又は規定を実施しないことを認めざるを得ない場合については、情報基盤センターの審査承認によって例外措置を行うことができる。
４ 情報基盤センターは、前項に規定する例外措置を承認した場合、CISO にその旨を報告しなければならない。
（サイバー攻撃への対応）
第１５条　CISO は、被害を受けたサイバー攻撃に係る情報について、可能な限り速やかに文部科学省に連絡する。
（見直し）
第１６条　情報基盤センターは、情報セキュリティポリシー及び関連規程等について、適時見直しを行う。
（雑則）
第１７条　この規程に定めるもののほか、情報セキュリティ対策に必要な事項は、情報セキュリティに関する実施要項として別に定める。

附則
この規程は、平成 19 年 12 月 20 日から施行する。
附則
この規程は、平成 22 年 10 月 1 日から施行する。
附則
この規程は、平成 23 年 3 月 29 日から施行する。
附則

この規程は、平成 26 年 2 月 27 日から施行する。
附則
この規程は、平成 28 年 4 月 1 日から施行する。

〇宮崎大学情報セキュリティ実施要項

平成 23 年 3 月 29 日
制定
改訂　平成 26 年 2 月 27 日
平成 28 年 3 月 25 日

（趣旨）
第 1 条　この要項は、宮崎大学情報セキュリティポリシー基本方針（以下「ポリシー」という。）第 2 項及び宮崎大学情報セキュリティ基本規程第 14 条の規定に基づき、宮崎大学（以下「本学」という。）の保有する情報資産（データ類、情報システム及び情報ネットワーク）を安全、円滑、適正に管理・利用するために、ポリシー適用対象者が具体的に実施すべき項目に関し、必要な事項を定めるものとする。
（管理者）
第 2 条　情報資産の管理者は、次の者をいう。
(1) 情報機器の管理者情報機器を管理・運用している者(パソコンなどのクライアント機器においては利用者本人)
(2) データの管理者情報機器に利用者が入力したデータ等を管理・運用している者
(3) サービスの管理者ネットワークに接続している情報機器で提供しているサービスを管理・運用している者
(4) ネットワークの管理者ネットワークを管理・運用している者
（情報の管理）
第 3 条　本学における情報の分類は、次のとおりとする。
(1) 非公開情報　重要度が高く、かつ漏洩した場合著しく本学の信用や利益を損なう情報
(2) 限定公開情報　大学構成員等に限定された者のみに公開すべき情報
(3) 公開情報　不特定多数の者に公開してよい情報
2　前項に定める情報は、次のとおり取り扱うものとする。
(1) 非公開情報　職務上必要な者のみにアクセスを制限し、それ以外の者にアクセスさせてはならない。
(2) 限定公開情報　限定された者のみにアクセスを制限し、それ以外の者にアクセスさせてはならない。
(3) 公開情報　情報の改ざんや偽情報の流布に留意しなければならない。
3　情報機器又は携帯記憶媒体を廃棄する場合は、データを完全に読み取り不能な状態にして廃棄しなければならない。

（情報機器の管理）
第４条　この要項においては、対象となる設備機器を次のように分類する。
(1) ネットワーク機器　ネットワークを維持管理するために必要な機器をいう。
　(例)ルータ、スイッチ、無線 LAN アクセスポイント及びファイアウォール等
(2) サーバ機器　ネットワーク機器以外で、多数の利用者にサービスを提供している機器をいう。
(例)Web サーバ及びデータベースサーバ等
(3) クライアント機器　ネットワーク機器、サーバ機器以外の情報機器をいう。
　(例)パーソナルコンピュータ(パソコン、PC)、プリンタ及び計測設備機器等
２ ネットワークへの接続は、最新のセキュリティアップデートがなされた機器のみ接続できるものとする。ただし、セキュリティアップデートを適用すると適正にサービスを提供できない場合は、日付、当該セキュリティアップデート名及び理由を記録し、管理者の責任で運用すること。セキュリティアップデートがされていない、又はセキュリティアップデートがメーカーから提供されていない機器はネットワークに接続しない状態(スタンドアロン)では利用できるものとする。
３ ネットワーク機器の管理事項は、次のとおりとする。
(1) セキュリティアップデートを行わなければならない。ただし、セキュリティアップデートを適用すると適正にサービスを提供できない場合は、日付、当該セキュリティアップデート名及び理由を記録し、管理者の責任で運用すること。
(2) ログの取得が可能な機器ならば、ログの取得と監視を行わなければならない。また、正確なログを取得するために、常に適切に時刻を設定しなければならない。
(3) アクセス制限が可能な機器は、アクセス制限を行わなければならない。基本的に全てのアクセス及びサービスの利用を禁止し、必要最低限のアクセス及びサービスのみ利用を許可することが望ましい。
(4) 利用者制限が可能な機器ならば、ID 等を用いた利用者の制限を行わなければならない。
４ サーバ機器の管理事項は、次のとおりとする。
(1) セキュリティアップデートを行わなければならない。ただし、セキュリティアップデートを適用すると適正にサービスを提供できない場合は、日付、当該セキュリティアップデート名及び理由を記録し、管理者の責任で運用すること。
(2) ログの取得と監視を行わなければならない。また、正確なログを取得するために、常に適切に時刻を設定しなければならない。
(3) アクセス制限を行わなければならない。基本的に全てのアクセス及びサービスの利用を禁止し、必要最低限のアクセス及びサービスのみ利用を許可することが望ましい。
(4) ID 等を用いた利用者の制限を行わなければならない。
(5) 鍵などで入室者を制限できる場所に設置しなければならない。
(6) 不正プログラム(ウィルス等)への対策を行わなければならない。
(7) 電源を供給する際は、電圧の変動や突発的な停電、過電流に対応する装置を経由するこ

とが望ましい。
５ クライアント機器の管理事項は、次のとおりとする。
(1) セキュリティアップデートを行わなければならない。ただし、セキュリティアップデートを適用すると適正にクライアント機器を運用できない場合は、日付、当該セキュリティアップデート名及び理由を記録し、管理者の責任で運用することが望ましい。
(2) 不正プログラム(ウィルス等)への対策を行わなければならない。
(3) アクセス制限を行うことが望ましい。基本的に全てのアクセス及びサービスの利用を禁止し、必要最低限のアクセス及びサービスのみ利用を許可することが望ましい。
(4) ID 等を用いた利用者制限を行うことが望ましい。
（ネットワークの管理）
第５条　ネットワークの管理者は、接続する情報機器の IP アドレス、ドメインネーム(DN)及び管理者等の情報を適正に管理し、ネットワークを安全かつ円滑に運営するために、トラフィックなどの情報を収集しなければならない。
（インシデント対応）
第６条　インシデントが発生した場合、インシデントの発見者は、可能な限り情報機器からネットワークへの物理的接続を切らなければならない。
２ インシデントの発見者は、宮崎大学情報セキュリティインシデント対応チーム（以下「CSIRT」という。）に直ちにインシデント発生を知らせなければならない。
３ 前項でインシデントの報告を受けた CSIRT は、直ちに対応を行わなければならない。
（インシデント発生者への対応）
第７条 インシデントが利用者によって故意に起こされた場合、部局情報技術責任者及び情報基盤センターは、部局情報セキュリティ責任者に対してその旨を通報し、当該利用者（以下 「発生者」という。）への指導を要請する。
２ 発生者が、部局情報セキュリティ責任者の指導によってもインシデントの解消又は解決を行わない場合は、情報基盤センターは、発生者に事前通告した上で、発生者のネットワーク接続に必要な全ての ID 及び発生者の利用している PC のネットワークへの接続を停止し、所属する部局の部局情報セキュリティ責任者及び CISO に連絡する。
３ 学内情報ネットワークの利用を停止された者への指導がなされ、所属する部局の部局情報セキュリティ責任者から CISO への当該者の学内情報ネットワークの利用再開の申出により、CISO が認めた場合において、情報基盤センターは学内情報ネットワークの利用を再開する。
（指針の遵守）
第７条　情報資産の管理者及び利用者は、別に定める次の指針を遵守しなければならない。
(1) 宮崎大学情報資産管理者ガイドライン
(2) 宮崎大学情報資産の利用心得

附則

この要項は、平成 23 年 3 月 29 日から施行する。
附則
この要項は、平成 26 年 2 月 27 日から施行する。
附則
この要項は、平成 28 年 4 月 1 日から施行する。

〇宮崎大学情報資産管理者ガイドライン

平成 23 年 3 月 29 日
情報基盤センター運営委員会決定

このガイドラインは、宮崎大学情報セキュリティ実施要項第 7 条に基づき、宮崎大学（以下「本学」という。）が保有する情報資産（データ類、情報システム、情報ネットワーク）の安全、円滑、適正な管理・利用を図り、管理者の心得や行動の指針とするために定めるものとする。本学において、情報資産を管理する者は、このガイドラインを遵守しなければならない。

１．管理者

⑴情報機器の管理者
情報機器を管理・運用している者(パソコンなどのクライアント機器では利用者本人)

⑵データの管理者
情報機器に利用者が入力したデータ等を管理・運用している者

⑶サービスの管理者
ネットワークに接続している情報機器で提供しているサービスを管理・運用している者

⑷ネットワークの管理者
ネットワークを管理・運用している者

２．情報資産管理者の心得

⑴ 情報資産の「管理」とは、単に機器等の保守管理のみを指すのではなく、アクセス等の活動や情報交換行為に対する適正な管理運用を図ることである。特に、留意すべき管理の原則は、出来る限り利用者の利便性を損なうことなく、適切かつ適正であるよう管理することである。

⑵ 管理者が実際に管理できない情報資産を運用することは好ましくない。万一、業者等に管理を委託せざるを得ない場合には、具体的な管理内容の契約や秘密保持が保証されるような手段を講じる必要がある。いずれにせよ最終的な管理責任は管理者にある。

３．　情報の管理

３．１　情報の分類

⑴ 非公開情報　重要度が高く、かつ漏洩した場合著しく本学の信用や利益を損なう情報

⑵ 限定公開情報　大学構成員等に限定された者のみに公開すべき情報

(3) 公開情報 不特定多数の者に公開してよい情報

３．２ 情報の取り扱い

(1) 非公開情報 職務上必要な者のみにアクセスを制限し、それ以外の者にアクセスさせてはならない。

(2) 限定公開情報 限定された者のみにアクセスを制限し、それ以外の者にアクセスさせてはならない。

(3) 公開情報 情報の改ざんや偽情報の流布に留意しなければならない。

４． セキュリティの確保

４．１ 記憶媒体の廃棄

情報機器又は携帯記憶媒体を廃棄する場合、データを完全に読み取り不能な状態にして廃棄しなければならない。

４．２ ネットワークへの接続

ネットワークには、最新のセキュリティアップデートがなされた機器のみ接続できるものとする。ただし、セキュリティアップデートを適用すると適正にサービスを提供できない場合は、日付、当該セキュリティアップデート名と理由を記録し、管理者の責任で運用すること。セキュリティアップデートがされていない、或いはセキュリティアップデートがメーカーから提供されていない機器はネットワークに接続しない状態(スタンドアロン)では利用できるものとする。

４．３ パスワードの管理

(1) 管理者パスワードは厳重に管理し、他人に発覚しないようにする。

(2) 利用者に対して定期的なパスワードの変更を推奨する。また、容易に発覚するような不適当なパスワードを使用しないように指導する。

(3) 利用者が ID やパスワード等を忘れた場合、電話等で容易に通知や再発行せず、利用者本人であることをしっかりと確認した上で対応する。第三者が利用者になりすまして、ID やパスワードを不正に取得できないよう対処する。

４．４ セキュリティホールになる可能性の排除

(1) 不必要なサービスを停止したり、不必要なポートを閉じる。

(2) 利用者に情報資産を不正に利用しないよう指導する。

(3) 利用者に不用意なプログラムの利用を避けるように指導する。

４．５ セキュリティ情報の収集

管理者向けに配信されている情報を積極的に参照し、セキュリティホールに関する情報を常時、取得・収集して、必要な対応を行う。

５． 情報機器毎のセキュリティの確保

５．１ 情報機器の分類

(1)ネットワーク機器 ネットワークを維持管理するために必要な機器

ルータ、スイッチ、無線 LAN アクセスポイント、ファイアウォール等

(2)サーバ機器 ネットワーク機器以外で、多数の利用者にサービスを提供している機器

Web サーバ、データベースサーバ等
(3)クライアント機器 ネットワーク機器、サーバ機器以外の情報機器
パーソナルコンピュータ(パソコン、PC)、プリンタ、計測設備機器等
５．２ ネットワーク機器
(1)セキュリティアップデートを行わなければならない。ただし、セキュリティアップデートを適用すると適正にサービスを提供できない場合は、日付、当該セキュリティアップデート名と理由を記録し、管理者の責任で運用すること。
(2)ログの取得が可能な機器ならば、提供するサービスに応じて、必要で適切な量のログを収集・保存し、日常的にログを監視することで、セキュリティホール等から侵入する不正な利用者を排除しなければならない。また、正確なログを取得するために、常に適切に時刻を設定しなければならない。
(3)アクセス制限が可能な機器は、アクセス制限を行わなければならない。基本的に全てのアクセス、サービスの利用を禁止し、必要最低限のアクセスとサービスのみ利用を許可することが望ましい。
(4)利用者制限が可能な機器ならば、ID 等を用いた利用者の制限を行わなければならない。
５．３ サーバ機器
(1)セキュリティアップデートを行わなければならない。ただし、セキュリティアップデートを適用すると適正にサービスを提供できない場合は、日付、当該セキュリティアップデート名と理由を記録し、管理者の責任で運用すること。
(2)提供するサービスに応じて、必要で適切な量のログを収集・保存し、日常的にログを監視することで、セキュリティホール等から侵入する不正な利用者を排除しなければならない。syslog、messages、maillog、authlog などの確認を行う。また、正確なログを取得するために、常に適切に時刻を設定しなければならない。
(3)アクセス制限を行わなければならない。基本的に全てのアクセス、サービスの利用を禁止し、必要最低限のアクセスとサービスのみ利用を許可することが望ましい。
(4)ID 等を用いた利用者の制限を行わなければならない。
(5)鍵などで入室者を制限できる場所に設置しなければならない。
(6)不正プログラム(ウィルス等)への対策を行わなければならない。
(7)電源を供給する際は、電圧の変動や突発的な停電、過電流に対応する装置を経由することが望ましい。
５．４ クライアント機器
(1)セキュリティアップデートを行わなければならない。ただし、セキュリティアップデートを適用すると適正にクライアント機器を運用できない場合は、日付、当該セキュリティアップデート名と理由を記録し、管理者の責任で運用することが望ましい。
(2)不正プログラム(ウィルス等)への対策を行わなければならない。
(3)アクセス制限を行うことが望ましい。基本的に全てのアクセス、サービスの利用を禁止し、必要最低限のアクセスとサービスのみ利用を許可することが望ましい。

(4)ID 等を用いた利用者制限を行うことが望ましい。

６．　ネットワークの管理

ネットワークの管理者は、接続する情報機器の IP アドレス、ドメインネーム(DN)や管理者などの情報を適正に管理し、ネットワークを安全、円滑に運営するために、トラフィックなどの情報を収集しなければならない。

７．情報資産の目的外使用の禁止

(1) 本学の情報資産は公的なものであり、教育・研究・業務の目的でのみ利用できる。

(2) 個人情報を扱う場合、事前の利用目的を超えて収集・利用してはならない。

８．権利侵害への対処

(1) ホームページ等に他者のロゴ、マーク、画像など著作権等を侵害する物を掲載しない。また許可無く個人情報を掲載したり、他人を誹謗・中傷するような情報を掲載しない。

(2) 利用者に対して権利の侵害が起こらないように指導する。

(3) 著作権等を侵害したり、許可無く個人情報が掲載される、誹謗中傷を受けるなど個人の権利が侵害されている事案が発生した場合、セキュリティ事故として、部局技術責任者及び情報基盤センターに速やかに届けでる。

９．秘密の厳守

管理者は、管理業務上知り得た情報などの扱いについて、以下の事項に留意する。

(1) 管理上知り得た情報は、情報の関係者からの許諾を得た場合、或いは必要止むを得ない理由がある場合を除いて、情報を第三者に漏らしてはならない。

(2) システムに保存されている情報は、必要止むを得ない理由がある場合を除いて、所有する利用者の許可なく見てはならない。

(3) 特定の利用者の許諾を得た場合、或いは必要やむを得ない理由がある場合を除いて、特定の利用者の利用状況を調べる行為を行ってはならない。

１０．セキュリティ事故での対応

不正な侵入が行われた場合、或いは情報漏えい等が行われた場合には、速やかに次の対処を行わなければならない。

(1) 情報機器からネットワークへの物理的接続を切る。

(2) 部局情報技術責任者および情報基盤センターに連絡する。

(3) サービスの運用を停止し、セキュリティホールを調査する。また、ログ等を解析し、不正侵入の方法など調査する。その結果、OS やアプリケーションのバージョンアップ、patch を当てる、不要なサービスの停止及びパスワードの変更など必要な措置を講ずる。

(4) 必要な措置を講じた後、セキュリティが確保されたことを検証し、その後にネットワークに接続する。

附則

このガイドラインは、平成２３年４月１日から実施する。

○宮崎大学情報資産の利用心得

平成 23 年 3 月 29 日
情報基盤センター運営委員会決定

この利用心得は、宮崎大学情報セキュリティ実施要項第 7 条に基づき、宮崎大学（以下「本学」という。)の情報資産(データ類、情報システム、情報ネットワーク)の安全、円滑、適正な利用を図り利用者の保護のために定めるものとする。
本学において、情報資産を利用する者は、この利用心得を遵守しなければならない。
1. 情報資産の利用にあたって避けるべき行為
1.1 犯罪行為、または民事訴訟の対象となる行為
1.1.1 不正アクセスなどの行為
(1) 他人のユーザー名(ID)やパスワードなどを無断で使用する。
(2) 他人のユーザー名(ID)やパスワードなどを無断で第三者に教える。
(3) 利用許諾の無い情報資産を不正に利用する。
(4) 情報資産を不正に破壊する。
1.1.2 基本的人権の侵害となる行為
(1) 人種、性別、思想信条などに基づく差別的な内容を公開する。
(2) 他人を誹謗中傷する内容を公開する。
(3) プライバシーを侵害する。
1.1.3 著作権などの権利の侵害となる行為
(1) 図書や雑誌、ホームページ等に掲載されている文書、写真、図、音楽、動画などの著作物を権利者に無断で転載・改変する。
(2) 許諾された権利を超えて、ソフトウェアをコピー・利用・改変する。
(3) ファイル交換（共有）ソフトウェアなどを利用して、権利者の許可なく音楽や動画などのファイルの入手や配信を行う。
1.1.4 その他の行為
(1) 猥褻(わいせつ)とみなされるものを公開する。
1.2 公序良俗に反する行為
(1) 事実と異なる情報やデマを公開する。
(2) 匿名、または他人の名前をかたって、情報を発信する。
(3) 大量のメールを無差別に発信する。
(4) 他人のファイルやディレクトリ(フォルダー)を当人に無断で見る。
(5) 大きなサイズのファイルをメールに添付し送信する。
1.3 大学における教育・研究・業務目的に反する行為
(1) 情報資産を営利目的など教育・研究・業務の目的以外に利用する。
(2) 猥褻情報や反社会的情報に関わるサーバ等へのリンクを張る。
1.4 情報資産の管理運用への妨害

(1) 情報資産の管理者・運用者の指示に従わない。
(2) 不必要で大量のメールやファイルをサーバに残す。
(3) 管理者に無断でソフトウェアをインストールする。
(4) 他人とユーザー名(ID)やパスワードの貸し借りを行う。
(5) 自分のユーザー名(ID)やパスワードを不適切に管理し、他人に利用される。
1.5 他の利用者に対する配慮に欠ける行為
(1) 実習室で複数のパソコンを一人で占有したり、ゲーム等に興じる。
(2) 教育研究に不必要な大きなサイズのファイルなどをダウンロードするなど、ネットワークに連続的に不必要な負荷をかける。
2. トラブルを回避し、自分自身を守るための心得
2.1 パスワードの管理を適正に行う。
(1) パスワードはできる限り暗記し、容易に他人の目に触れるようなところに保存または書き置きしない。
(2) パスワードは自分の電話番号や誕生日など、容易に第三者に推測されやすい文字列の使用は避ける。
(3) 長期間同じパスワードを使い続けることは避ける。
2.2 個人情報を保護する。
(1) 個人情報をホームページ等に掲載する場合は、必ず本人に公開の許諾を得る。
(2) 許諾を得た個人情報を公開する場合でも、それらの情報が悪用される場合もあるので、内容について十分に配慮する。
(3) 個人情報の流出を避けるため、セキュリティのアップデート、ウイルス対策やスパイウェア対策を十分に行う。
(4) ファイル交換（共有）ソフトウェアを利用すると、意図せず個人情報の流出、及び著作権等の侵害を起こすことがあるので、ファイル交換（共有）ソフトウェアをインストールしない。
2.3 電子メールの利用にあたって留意すべきこと。
(1) 電子メールは、情報ネットワークを利用した「手紙」であると認識する。
(2) 言葉足らずの説明や独りよがりの内容は、受け取った相手を困惑させたり、誤解を招く恐れがあるので、送信する前に、内容を読み直す。
(3) 電子メールはメール・アドレスのみで配信されるため、相手のメール・アドレスを十分に確認し、間違った相手にメールを送らないようにする。
(4) 電子メール・アドレスは悪用される場合があるので、不用意に他人に教えない。また、他人の電子メール・アドレスについても第三者に不用意に伝えない。
(5) 知らない他人からの電子メールには不用意に返事をしない。
2.4 ホームページを利用するに当たって留意すべきこと。
(1) 公開の許諾があったとしても、不用意に個人情報を公開しない。
(2) 不正な料金の請求は無視する。

附則
この利用心得は、平成２３年４月１日から実施する。

○宮崎大学における電子情報の取扱いに関するガイドライン

平成 26 年 3 月 7 日
情報基盤センター運営委員会決定

1　目的

本ガイドラインは、宮崎大学（以下「本学」という。）の構成員が、電子情報（以下「情報」という。）を取り扱う場合において、セキュリティへの対応等情報を適切に管理するための最低限遵守すべき事項を定めるものとする。

2　遵守事項

2.1　一般的な事項

(1) 情報の管理者と情報を保存する機器の管理者を定めること。情報（ファイル）を所有した時点で情報の管理者となることに留意すること。
(2) 情報の管理者は、情報を非公開情報、限定公開情報、公開情報に分類し、非公開情報及び限定公開情報はアクセスできる者及び機器を定めること。
(3) 必要のない情報まで公開しないように情報の利用について十分な分析を行い、公開する情報とアクセスの範囲を定めること。
(4) 非公開情報及び限定公開情報の複製、配布は必要最小限の範囲に限定すること。
(5) 機器の管理者は、許可された者・機器以外が情報にアクセスできないように、ファイルのアクセス権等を設定すること。また、重要情報は暗号化すること。
(6) 限定公開情報及び非公開情報を保存する機器は可能な限り少数に限定し、厳重にセキュリティ管理を行うこと。
(7) 情報を保存した記憶媒体は、データを完全に読み取り不可能な状態にして破棄すること。
(8) 外部に流出した情報の取消しはできないことを十分認識し、取り扱う情報の取捨選択及び利用は慎重に行うこと。
(9) 個人情報については、本学の「個人情報保護規則」及び「保有個人情報管理規程」に従って慎重に扱うこと。些細な情報であっても組み合わせることで個人が特定されプライバシーが侵害される恐れがあるので公開する情報の内容に注意すること。
(10) 情報を公開する場合は、誤記載がないように十分に注意し、情報の信頼性を担保するための手段を講じること。

2.2　携帯可能な機器で情報を取り扱う場合の事項

「携帯可能な機器」とは、USB メモリー、ノートパソコン、タブレット、スマートフォン、携帯電話等の情報を記録し持ち歩くことのできる機器をいう。これらの機器で情報を取扱う場合の事項は以下のとおりとする。

(1) 学外に持ち出す機器を限定し、機器の持ち出し管理を行うこと。
(2) 不用意に情報を学外に持ち出さないように、機器には原則として限定公開情報及び非公開情報を保存しないこと。
(3) 業務上の必要性から止むを得ず機器に情報を保存して学外に持ち出す場合は、情報を暗号化するなどの処置を講ずること。
(4) 必要がなくなった情報は速やかに機器から消去すること。

2.3　インターネット上のサービスで情報を取り扱う場合の事項

「インターネット上のサービス」とは、本学と契約関係にない学外の事業者が管理運営するメールやオンラインストレージ、動画配信、ソーシャルメディアなどをいう。これらのサービスで情報を取扱う場合の事項は以下のとおりとする。

(1) インターネット上のサービスを利用して情報を取り扱う場合は、情報の「学外への持ち出し」となることに留意すること。
(2) 法律及び利用するサービスの規約等を遵守し、本学の構成員としての自覚を持ち責任ある利用を行うこと。
(3) 業務に利用する場合及び業務以外に利用する場合それぞれ別アカウントを利用し、情報管理を分離すること。
(4) サービスの設定によっては不用意に情報を公開してしまう場合もあるので、利用する前に十分試験を行ってから利用すること。
(5) サービスによっては、日本国の法律に従わない場合があり、どのように情報が保護されるのか明確でない場合もあるため、重要な情報を扱う場合は利用しないこと。
(6) 利用するサービスの提供側による情報の二次利用についての有無を規約等で確認し、問題がないか確認すること。
(7) インターネット上のサービスの利用及びこのサービスで情報を利用することについて、関係組織（部局等）や構成員に十分な説明を行い、同意と承認を得ること。
(8) サービスの利用を停止する場合は、停止操作とアカウントの廃止を行うこと。可能であれば情報の削除操作又は削除依頼を行うこと。

○情報基盤センター情報システムの運用継続計画

平成 26 年 3 月 28 日
情報基盤センター運営委員会決定

1　目的

本計画は、情報基盤センターが運用管理する情報システムについて災害や事故等の非常

時における継続運用に関する計画と対策を定めたものである。

２　情報システムの分類

情報基盤センターは、通常様々な情報システムにより、多くの情報機能を提供しているが、非常時において情報の収集・共有・伝達する機能は、災害対応の初動段階で最も必要な機能であり、この機能が停止することは災害対応業務そのものにも深刻な影響が生じる。このため、情報の収集・共有・伝達機能の確保を最優先事項とし、この機能を提供する情報システムを A ランクとする。また、災害発生による混乱のため大学機能が通常通りでない状態にある時、必ずしも運用を継続する必要のない情報システムを B ランクとする。この基準に従い、情報基盤センターが運用管理する情報システムを分類すると下表のようなランク分けとなる。

（情報システムのランク）

情報システム	ランク
ドメインネームシステム（DNS）	A
Web システム（大学ホームページ）	
Web システム（教職員、学生用）	B
メールシステム	
ホスティングシステム	
学内貸出用仮想基盤システム	
認証基盤システム	
ネットワーク認証システム	
ログ管理システム	
ネットワークモニタシステム	
実習室システム	
大学情報データベースシステム	
e ラーニングプラットフォームシステム	

３　情報システムへの想定被害

大規模災害が発生した際に、上記の情報システムの運用に直接的または間接的に支障を及ぼす被害について、被害要素とこれに起因する被害事象を下表のとおり想定する。

（想定する被害事象）

被害要素	被害事象
(3-1) 商用電力停止	機器および空調設備の停止
(3-2) 外部接続ネットワーク光回線停止	学外との通信の停止
(3-3) キャンパス間ネットワーク光回線停止	キャンパス間の通信の停止
(3-4) キャンパス内ネットワーク光回線停止	学内建物間の通信の停止
(3-5) 搭載ラックの転倒やラックからの脱落	機器の停止
(3-6) 建物の倒壊	機器の停止

4　被害事象への対策

災害の発生により上述した被害事象が起こった場合、これを補うための対策として以下が考えられる。

(4-1)　商用電力停止

商用電力が停止した場合、自動で切り替えが行われ、停電発生から 72 時間の電力供給が可能である自家発電機を設置し運用する。また、切り替え中も機器に電力を供給できるように大型 UPS を設置する。

(4-2)　外部接続ネットワーク光回線停止

外部接続回線を木花キャンパスと清武キャンパスのぞれぞれで保有し、外部接続回線を冗長化することにより一方の回線が停止した場合においても継続して学外との通信ができるようにする。また、冗長化した回線の経路は外部接続ポイントまで重複しない構成とし、両方の回線が同時に切断される可能性を極力低くする。

さらに、光回線が全停止した場合においても、最低限のインターネット利用を確保できるように、衛星を使ったインターネット接続回線を整備し、情報基盤センターと医療情報部、宮崎大学の災害対策本部が設置される事務局 4 階会議室で利用できるようにする。

(4-3)　キャンパス間ネットワーク光回線停止

木花キャンパスと清武キャンパスを接続するキャンパス間ネットワーク光ケーブルは複数回線により冗長化する。しかし、回線の配線経路が同一であるため冗長回線のすべてが断線した場合に備え、キャンパス間無線ネットワークを整備し、別経路での接続を担保する。

(4-4)　キャンパス内ネットワーク光回線停止

情報基盤センターを起点とし各部局棟へ敷設する光回線を複数回線により冗長構成とする。また、主要な部局棟の配線経路を地下ピット内への敷設とすることにより、断線の可能性を低くする。

(4-5)　搭載ラックの転倒やラックからの脱落

機器を搭載するラックに耐震架台を設置してラックを固定することにより、地震な

どの揺れによってラックが転倒しないようにする。また、ラックに搭載された機器の脱落を防ぐため、サーバレールの固定やロック式全面扉付のラックを導入する。

(4-6)　建物の倒壊

機器を設置している情報基盤センターの建物が倒壊した場合は機器の損壊も免れないため、情報基盤センター設備より堅牢であり、地理的に離れた宮崎地域外のデータセンター等の施設に機器を分散配置する。

５　運用継続のための対策計画

第 2 項の各ランクに対して、第 4 項の対策をそれぞれ行うことにより、災害時における情報システムのランクに従った継続運用を行う。

B ランクの情報システムについては、上記(4-1)～(4-5)の対策を実施し、小規模な災害が発生した場合も停止しないようできる限り運用を続ける。ただし、これらの対策を行っていたにも関わらず、運用を継続できないような災害状況においては、ランク B のシステムが停止することはやむを得ないものとし、大学機能が通常状態に復帰した後に、復旧、運用再開を行うものとする。

A ランクの情報システムについては、B ランクの情報システムと同様に上記(4-1)～(4-5)の対策を施して小規模な災害では停止しないようにする。さらに、大規模災害が発生し(4-1)～(4-5)の対策が有効に機能しない場合や建物が倒壊した場合においても、情報システムの機能を停止しないために上記(4-6)の対策を実施する。

○教員における個人情報ファイルの取り扱い方針

平成 27 年 8 月 11 日

最高情報セキュリティ責任者（CISO）決定

【基本的セキュリティ対策】

個人情報に限らず、情報ファイルを取り扱うパソコンでは、以下の基本的なセキュリティ対策を行うこと。

1. 本学が無償提供しているウィルス対策ソフト（ESET）を必ずインストールし、毎日のウィルス定義ファイルの更新及び定刻のスキャンを行うこと。
2. OS 及び各ソフトウェアのセキュリティアップデートを定期的に行うこと。
3. ログインパスワードを設定し、席を離れる際にはロックすること。
4. パソコンやファイル等に設定するパスワード（以下「PW」という。）は、8 桁以上の数字、記号、英大文字小文字を必ず含んだものとすること。PW の使いまわしはやめること。PW を書いたメモをパソコン画面や机等に貼っておかないこと。
5. 標的型攻撃メールと疑われるメールの添付ファイルや、メールに記載された URL を開かないこと。標的型攻撃メールか正規のメールか判断が難しい場合は、差出人に電話などで確認をとること。なお、@マーク以下が、フリーメールのアドレス（例@gmail.com、

@yahoo.co.jp、@hotmail.com 等）であれば、標的型攻撃メールである可能性が高い。

【個人情報ファイルの取り扱い】

個人情報ファイルを取り扱うパソコンは、上記【基本的セキュリティ対策】を行ったパソコンであること。

１．個人情報ファイルの保存

・個人情報ファイルには、このファイルを使った作業が終了した時点で PW をかけること。

・個人情報ファイルは管理用のフォルダ内にまとめて保存し、管理用フォルダには PW をかけること。

・可能であれば、一つ一つの個人情報ファイルに PW をかけることが望ましい。

（注：PW のかかったフォルダにドラッグ&ドロップによりファイルを保存しても、このファイルには PW がかからないので注意すること）

・業務上不要になった時点で個人情報ファイルを消去すること。

■ファイル及びフォルダへ PW をかける方法は下記の URL からマニュアルを参照

http://www.cc.miyazaki-u.ac.jp/internal/newsystem/H27/windows_compress.pdf

http://www.cc.miyazaki-u.ac.jp/internal/newsystem/H27/osx_compress.pdf

２．個人情報ファイルの持ち出し禁止

・個人情報ファイルは原則学外に持ち出さないこと。特に重要な個人情報ファイルは、研究室からも持ち出さないこと。

・ファイルを保存した記録媒体（HDD、USB メモリ、SD カード等）の学外への持ち出し、学外のオンラインストレージ（例 Dropbox、OneDrive、Google ドライブ 等）への保存、メール添付での学外送信は全てファイルの学外持ち出しとなる。

・どうしても持ち出さなければならない場合は、学部長等の上司に許可を得た上で、そのファイル及びフォルダには PW を設定すること。持ち出す場合は、暗号化機能付き外部記録媒体の使用を推奨する。

３．個人情報ファイルの共有・配布

・個人情報ファイルの共有・配布は業務の遂行に不可欠な場合に限り行い、共有・配布の範囲を最小限にすること。共有・配布するファイル及びフォルダには PW を設定すること。

・個人情報ファイルの共有・配布には、情報基盤センターが提供する学内のオンラインストレージの利用を推奨する。

・個人情報ファイルの配布には、オンラインストレージの「Web　公開」の機能を使用する。

・個人情報ファイルの共有には、オンラインストレージの「共有フォルダ」の機能を使用する。特定のグループで共有する場合は、情報基盤センターが発行する組織用アカウントを使

用して共有を行う。
（※ 組織用アカウントは、学部、学科、講座、部、課、係、附属施設（部門毎も可）、委員会（全学、学部、学科）に対して発行することができる。）

■組織用アカウントの申請は下記のオンライン申請の「情報基盤センター利用申請」から行い、利用区分は「組織」を選択する。

http://himuka.cc.miyazaki-u.ac.jp/E-application/login.php

■オンラインストレージの利用方法は下記の URL からマニュアルを参照

http://www.cc.miyazaki-u.ac.jp/internal/newsystem/H27/onlinestrage_web.pdf
http://www.cc.miyazaki-u.ac.jp/internal/newsystem/H27/onlinestrage_share.pdf

・個人情報ファイルは、原則メール添付では送らないこと。どうしても送らなければならない場合は、ファイルに PW をかけた上、添付で送った後、別メールあるいは電話で PW のみを伝えること。

【記録媒体の廃棄】
・個人情報ファイルを保存したことのあるパソコン及び記録媒体を廃棄するときは、物理的に破壊する等の完全に読み取りが不可能になる処理を施して廃棄すること。

【紙媒体の個人情報の取り扱い】
・紙媒体の個人情報（教授会資料中の学生関連名簿、入試判定資料、就職関連資料等）は、研究室外及び会議室外へ持ち出さないこと。それらの資料については事務的に回収し、シュレッダーにかけて廃棄すること。研究室等でそれらの資料を発見した場合、自主的にシュレッダーにかけること。
・安易に紙媒体の個人情報をスキャンして電子データにしないこと。

【個人情報ファイルとは】
・「個人情報ファイル」とは、個人に関する情報（氏名、生年月日、その他特定の個人を識別できるもの）が記録されている電子ファイルのことを言う。
・「重要な個人情報ファイル」とは、氏名または学籍番号に加え、成績、電話番号、住所等が記録された個人情報ファイルのことを言う。

宮崎大学情報基盤センター年報　2016

平成 29 年 7 月発行

編集／発行　宮崎大学情報基盤センター

〒889-2192　宮崎市学園木花台西 1 丁目 1 番地

0985（58）2867

http://www.cc.miyazaki-u.ac.jp