FUJITSU Hybrid IT Service FJcloud-O IaaS

IPCOM VE2m 移行ガイド

Version 1.0

FUJITSU LIMITED

まえがき

本書の目的

本書は、FUJITSU Hybrid IT Service FJcloud-O IaaS(以下、IaaS)で利用されている IPCOM VA2 から、後継製品である IPCOM VE2m に移行するために必要な手順について記載します。

本書は、東日本第 1/第 2,西日本第 1/第 2 リージョンを対象としています。

本書の対象読者

本書は、IaaS 上で IPCOM VA2 をご利用されている方を対象としています。また、本書のご利用にあたり、基本的な IaaS の操作方法、ネットワークの知識、IPCOM VA2 の構築手順を有していることを前提としております。あらかじめご了承ください。

本書における語句の定義

本書で使用される語句の定義を下表に示します。

語句	定義の説明
IPCOM VE2m (一部の表内では VE2m と表記)	FUJITSU Hybrid IT Service FJcloud-O IaaS – IPCOM VE2m の略称です。IPCOM VE2 の FUJITSU Hybrid IT Service FJcloud-O IaaS 版派生製品であるため、IPCOM VE2 のドキュメントを参照可能です。なお、IPCOM VE2m と IPCOM VE2 は製品番号上、異なる製品になります。
IPCOM VA2 (一部の表内では VA2 と表記)	FUJITSU Hybrid IT Service FJcloud-O IaaS – IPCOM VA2 の略称です。
IaaS	FUJITSU Hybrid IT Service FJcloud-O IaaS の略称です。
Primary	IPCOM VE2m の装置二重化機能を有効にした場合の現用装置(プライマリ)です。
Secondary	IPCOM VE2m の装置二重化機能を有効にした場合の待機装置(セカンダリ)です。
仮想 IP アドレス	負荷分散対象のサーバ群を束ねる終端のアドレスとして IPCOM VE2m に定義する IP アドレスです。
代表 IP アドレス	2 台の IPCOM VE2m で共有するため、割り当てる IP アドレスです。冗長切り替え後に片方の IPCOM VE2m に引き継がれます。
ダミーポート	仮想 IP アドレス、代表 IP アドレスに対応する IaaS 上のポートです。IPCOM VE2m へのアタッチは不要です。
LB	ロードバランサー(Load Balancer)の略称です。
FW	ファイアーウォール(FireWall)の略称です。
LAN	IPCOM VE2m のネットワークインターフェースの名称です。
物理インターフェース	本書では、IaaS のポートに紐づく IPCOM VE2m のインターフェースを示します。

マニュアル体系

本書は IPCOM VE2m の設定に関する初期段階の説明を記載しております。 IPCOM VE2m の機能詳細は、本書と同 Web ページに掲載の製品マニュアルをご覧ください。下表に製品マニュアルの種類と目的・用途を示します。

マニュアル名称	目的・用途
IPCOM VE2m スタートガイド	IaaS 上で IPCOM VE2m を使用する際に必要な情報および構築例を記載しています。 はじめに必ずお読みください。
IPCOM VE2 ソフトウェアシリーズ マニュアル体系と読み方	マニュアルの構成と読み方、対象読者と前提知識、マニュアルで使用する名称や略称、マークの説明、コピーライトおよび商標などについて説明しています。 はじめに必ずお読みください。
IPCOM VE2 ソフトウェアシリーズ VE2 ユーザーズガイド	IPCOM VE2 が提供する機能、IPCOM EX2 シリーズとの機能差分などについて説明しています。IPCOM VE2 を操作する前にこのマニュアルをよく読み、書かれている留意点や注意事項を十分に理解してください。
IPCOM EX2 ソフトウェアシリーズ IPCOM EX2 保守ガイド	IPCOM EX2 ソフトウェアシリーズのメンテナンス方法やトラブル発生時の対処方法について説明しています。 また、プラットフォームが異なる IPCOM 間の環境定義情報・ファイルの移行について説明しています。

輸出管理規制

本書を輸出または第三者へ提供する場合は、お客様が居住する国および米国輸出管理関連法規等の規制をご確認のうえ、 必要な手続きをおとりください。

IPCOM VE2m の使用条件について

IPCOM VE2m をご使用いただくにあたり、ライセンス条項に同意いただく必要がございます。IPCOM VE2m をご使用の前に、以下の Web ページに掲載のライセンス条項をお読みいただき、同意のうえ IPCOM VE2m をご使用ください。

IPCOM VE2m の使用に関するライセンス条項
http://jp.fujitsu.com/solutions/cloud/k5/document/pdf/ipcom-covenant.pdf

お願い

- 本資料の無断複製、転載を禁じます。
- 本資料は仕様変更等により予告なく内容を変更する場合がございます。あらかじめご注意願います。
- 本書に記載されたデータの使用に起因する第三者の特許権およびその他の権利の侵害については、当社はその責を負いません。

変更履歴

版数	更新日	変更箇所	概要
1.0	2020 年 6 月 15 日	初版作成	

目次

第 1 章　本資料で提供する内容と構成

IaaS の IPCOM VA2 から IPCOM VE2m へのアップデート手順を記載します。

1.1 移行作業の流れ

(1) アップデート時の留意事項の確認

IaaS の IPCOM VA2 と IPCOM VE2m の差異に関する留意事項を確認して、必要に応じて留意事項に記載されている対処を行う準備を行います。詳細は以下をご確認ください。

- 第 2 章 IPCOM VE2m へのアップデート時の留意事項

(2) 環境定義情報の移出

現在利用中の IPCOM VA2 から config や証明書等の環境定義情報を取得します。詳細は以下をご確認ください。

- 第 3 章 環境の移行

(3) IPCOM VE2m の構築

IPCOM VE2m の仮想サーバを構築します。詳細は以下をご確認ください。

- IPCOM VE2m スタートガイド

利用中の IPCOM VA2 を考慮した IPCOM VE2m の構築手順例については、以下をご確認ください。

- 第 4 章 冗長化構成の移行手順例
- 第 5 章 シングル構成の移行手順例

(4) 環境定義情報の移入

「(2) 環境定義情報の移出」で取得した環境定義情報を IPCOM VE2m の仮想サーバに移入します。詳細は以下をご確認ください。

- 第 3 章 環境の移行

また、必要に応じて「(1) アップデート時の留意事項の確認」で確認した留意事項に対する対処を行ってください。

(5) IPCOM VE2m での運用開始

IPCOM VE2m を使用した検証を行い、IPCOM VA2 から IPCOM VE2m での運用に切り替えます。

運用中の IPCOM VA2 を考慮した IPCOM VE2m への運用切り替え手順例については、以下をご確認ください。

- 第 4 章 冗長化構成の移行手順例
- 第 5 章 シングル構成の移行手順例

第 2 章 IPCOM VE2m へのアップデート時の留意事項

本章では、IaaS の IPCOM VA2 から IPCOM VE2m へのアップデート時の留意事項について説明します。

2.1 IPCOM VE2m で未サポートとなった機能

IaaS の IPCOM VA2 から IPCOM VE2m で未サポートになった機能を以下に記載します。

(1) 基本コマンド

secure tcp-seq コマンド

(2) サーバ負荷分散機能

VMware View 負荷分散機能

(3) サーバ連携機能すべての機能

(4) 運用管理／保守機能

・Syslog サーバ(受信)

・ローリングアップグレード

2.2 構成定義編集に関わる留意事項

構成定義編集時に留意していただく事項を記します。

2.2.1 サーバ負荷分散機能の構成定義編集に関わる留意事項

2-2-1-1) slb http-keep-alive delayed-ack-timeout コマンド

デフォルト値を変更しています。

【IPCOM VA2】

コマンドを省略した場合、ACK 応答の最大遅延時間は、500 ミリ秒が設定されたものと見なされます。

【IPCOM VE2m】

コマンドを省略した場合、ACK 応答の最大遅延時間は、200 ミリ秒が設定されたものと見なされます。

【影 響】一般的に遅延 ACK は 200 ミリ秒で行うことが多く、対向ノードによってはパケットロストと見なされて、SLB が ACK 応答する前に再送されてしまう場合があることへの対応であり、影響はありません。

【対 処】

不要です。

2-2-1-2) slb web-accelerate delayed-ack-timeout コマンド

デフォルト値を変更しています。

【IPCOM VA2】

コマンドを省略した場合、ACK 応答の最大遅延時間は、500 ミリ秒が設定されたものと見なされます。

【IPCOM VE2m】

コマンドを省略した場合、ACK 応答の最大遅延時間は、200 ミリ秒が設定されたものと見なされます。

【影 響】

一般的に遅延 ACK は 200 ミリ秒で行うことが多く、対向ノードによってはパケットロストと見なされて、

SLB が ACK 応答する前に再送されてしまう場合があることへの対応であり、影響はありません。

【対 処】

不要です。

2-2-1-3) slb-rule / distribution-rule / error-action tcp reassign コマンド

高負荷状態または故障中と判断したときに、新たに確立要求を行う分散対象サーバの台数の設定範囲を変更しています。

【IPCOM VA2】

確立要求を行う分散対象サーバの台数の最大数は以下のとおりです。

・IPCOM VA2 1300 LB(EX) ：最大 255 個まで

・IPCOM VA2 2500 LB(SSL) ：最大 1023 個まで

【IPCOM VE2m】

確立要求を行う分散対象サーバの台数の最大数は 10 個までです。

【影 響】

11 個以上設定すると、整合性検査時(validate コマンド/commit コマンド実行)にエラーになります。

【対 処】

確立要求を行う分散対象サーバの台数は、10 個以内で設定してください。

2-2-1-4) slb-rule / distribution-rule / error-action tcp reassign コマンド

slb-rule / distribution-rule / error-action tcp reassign コマンドで、高負荷状態または故障中の判断基準となる TCP コネクションの確立要求の再送回数の設定範囲を変更しています。

【IPCOM VA2】

TCP コネクションの確立要求の再送回数は、1 ～ 99 回の範囲で設定します。

【IPCOM VE2m】

TCP コネクションの確立要求の再送回数は、1 ～ 12 回の範囲で設定します。

【影 響】

13 回以上設定すると、エラーになります。

【対 処】

TCP コネクションの確立要求の再送回数は、1 ～ 12 回の範囲で設定してください。

2.2.2 QoS 制御機能の構成定義編集に関わる留意事項

2-2-2-1) interface / qos-flow / packet-base-size コマンド

interface / qos-flow / packet-base-size コマンドのデフォルト値を変更しています。

【IPCOM VA2】

コマンドを省略した場合、帯域幅の算出に使用するパケットのベースサイズは default（MAC ヘッダー ＋ データ部までの長さ（GAP、Preamble、padding 及び FCS は含まない））が設定されたものと見なされます。

【IPCOM VE2m】

コマンドを省略した場合、帯域幅の算出に使用するパケットのベースサイズは ieee802.3（GAP+Preamble+MAC ヘッダー+データ部+padding+FCS までの長さ）が設定されたものと見なされます。

【影 響】

パケットのベースサイズを default でネットワークを設計していて、コマンドを省略している場合に影響があります。

【対 処】

packet-base-size コマンドの見直しが必要です。

2-2-2-2) interface / qos-flow / packet-base-size コマンド

interface / qos-flow / packet-base-size コマンドのパラメーター「default」を「mac-frame-without-fcs」に変更しています。なお、「mac-frame-without-fcs」を設定した場合のパケットサイズの基準値は、「default」と同一で、MAC ヘッダー + データ部までの長さです。

【IPCOM VA2】

packet-base-size { default | mac-frame | ieee802.3 | atm-aal5 }

packet-base-size <-14-1600> no packet-base-size

【IPCOM VE2m】

packet-base-size { mac-frame-without-fcs | mac-frame | ieee802.3 | atm-aal5 }

packet-base-size <-14-1600> no packet-base-size

【影 響】

packet-base-size に default が指定されている場合、config が更新できません。

【対 処】

startup-config と running-config の packet-base-size に「default」が設定されている場合、「mac-frame-without-fcs」に書き換えてください。

2.2.3 アノマリ型 IPS 機能の構成定義編集に関わる留意事項

2-2-3-1) Very Small IP Fragment 攻撃の検査機能を装置全体の一括設定

Very Small IP Fragment 攻撃の検査機能を装置全体（装置の全インターフェース）で一括して、「有効」/「検出だけ」/「無効」に設定する機能を提供します。

【IPCOM VA2】

Very Small IP Fragment 攻撃の検査機能を装置全体（装置の全インターフェース）で一括して、「有効」/「検出だけ」/「無効」に設定する機能はサポートしていません。

【IPCOM VE2m】

Very Small IP Fragment 攻撃の検査機能を装置全体（装置の全インターフェース）で一括して、「有効」/「検出だけ」/「無効」に設定する機能（"protect small-ip-frg" コマンドで設定）をサポートします。

構成定義ファイルを新規に作成した場合、

"protect small-ip-frg detect-only audit-normal min-size 400"の定義が設定され、Very Small IP Fragment 攻撃の検出だけが行われます。400 バイト未満のフラグメントサイズを持つパケットは廃棄されずに、一定時間に連続した監査結果を 1 項目としてまとめてメッセージログに記録されます。

IPCOM VA2 で作成した構成定義ファイルを使用している場合、"protect small-ip-frg" コマンドは設定されず、装置全体の Very Small IP Fragment 攻撃の検査は行われません。

また、"no protect small-ip-frg"を設定し、"protect small-ip-frg" コマンド の設定を削除した場合も、Very Small IP Fragment 攻撃の検査は行われません。

【影 響】

IPCOM VA2 の構成定義ファイルを使用している場合は、影響はありません。

【対 処】

作成した構成定義ファイルで、装置全体の Very Small IP Fragment 攻撃の検査機能を使用したい場合は、"protect small-ip-frg" コマンドを設定してください。

2.2.4 Web アプリケーション・ファイアーウォール機能の構成定義編集に関わる留意事項

2-2-4-1) Web アプリケーション・ファイアーウォール機能のデフォルト値・省略値の変更

ポリシー(ページ単位)設定のデフォルト値や、ポリシー(ページ単位)設定の cookie 設定で値を指定しなかった場合の省略値を、サイトポリシー設定のデフォルト値と同一に変更しています。

【影 響】

ポリシー(ページ単位)設定のデフォルト値の変更によって、従来、ポリシーに違反し防御されていた通信が、通過する可能性があります。

【対 処】

従来と同様の検査を行いたい場合は、ポリシー(ページ設定)の設定を行ってください。

設定項目	サイトポリシー設定のデフォルト値	ポリシー(ページ単位)設定のデフォルト値 IPCOM VA2	ポリシー(ページ単位)設定のデフォルト値 IPCOM VE2m
非標準%uXXYY エンコード文字検証	検査を行いません	検査します	検査を行いません
リクエストラインの長さ制限	最大長は 8190 バイト	最大長は 2180 バイト	最大長は 8190 バイト
リクエスト URI の長さ制限	最大長は 8177 バイト	長さを制限しません	最大長は 8177 バイト
クエリー文字列の長さ制限	最大長は 8176 バイト	最大長は 2048 バイト	最大長は 8176 バイト
HTTP メソッド制限	「GET」、「POST」、「HEAD」、「PUT」、「DELETE」、「TRACE」、「CONNECT」、「OPTIONS」、「WebDAV」が使用可能	「GET」、「POST」、「HEAD」が使用可能	「GET」、「POST」、「HEAD」、「PUT」、「DELETE」、「TRACE」、「CONNECT」、「OPTIONS」、「WebDAV」が使用可能
HTTP ヘッダー数の制限	検査を行いません	最大数は 80 個	検査を行いません
HTTP ヘッダー名の長さ制限	検査を行いません	最大長は 128 バイト	検査を行いません
HTTP ヘッダー値の長さ制限	検査を行いません	最大長は 2048 バイト	検査を行いません
PUT ファイルアップロードの制限	検査を行いません	検査します	検査を行いません

設定項目	サイトポリシー設定のデフォルト値	ポリシー(ページ単位)設定のデフォルト値 IPCOM VA2	ポリシー(ページ単位)設定のデフォルト値 IPCOM VE2m
アップロードファイル名の長さ制限	検査を行いません	最大長は 255 バイト	検査を行いません
cookie 定義数の制限	最大数は 40 個	最大数は 20 個	最大数は 40 個
cookie 名の長さ制限	最大長は 4096 バイト	最大長は 128 バイト	最大長は 4096 バイト
パラメーター名の長さ制限	検査を行いません	最大長は 128 バイト	検査を行いません
cookie の値の長さ制限	最大長は 4096 バイト	最大長は 2048 バイト	最大長は 4096 バイト

2.2.5 SSL アクセラレーター 機能の構成定義編集に関わる留意事項

2-2-5-1) rule ssl-accel server / protocol コマンド

設定できるプロトコルとデフォルト値を変更しています。

【IPCOM VA2】

i) 設定可能なプロトコル

tls1.2、tls1.1、tls1.0、ssl3.0、ssl2.0 の中から設定することができます

ii) デフォルト値

コマンドを省略した場合、「tls1.2、tls1.0、ssl3.0」が設定されたものと見なされます。

【IPCOM VE2m】

i） 設定可能なプロトコル

tls1.2、tls1.1、tls1.0、ssl3.0 の中から設定することができます

ii） デフォルト値

コマンドを省略した場合、「tls1.2、tls1.0」が設定されたものと見なされます。

【影 響】

i） 設定可能なプロトコル

protocol コマンドに ssl2.0 が設定されている構成定義ファイルを使用する場合、構成定義ファイルの読み込み時(load コマンド実行時)にエラーとなります。

ii） デフォルト値

ssl3.0 のプロトコルしかサポートしない SSL クライアントからの接続ができなくなります。

【対 処】

i） 設定可能なプロトコル

protocol コマンドで、ssl2.0 を設定している場合は、削除してください。

ii） デフォルト値

ssl3.0 を使用する場合は、protocol コマンドで ssl3.0 を設定してください。

2-2-5-2) rule ssl-accel server / cipher-suites コマンド

セキュリティ強度の低い暗号スイートや暗号スイートグループを削除し、新しい暗号スイートを追加しています。また、暗号スイートグループに含まれる暗号スイートも変更しています。

IPCOM VA2	IPCOM VE2m
«暗号スイート» TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_DES_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC4_40_MD5 TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA TLS_RSA_EXPORT1024_WITH_RC4_56_MD5 TLS_RSA_EXPORT1024_WITH_RC4_56_SHA TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5 SSL_DES_192_EDE3_CBC_WITH_MD5 SSL_RC4_128_WITH_MD5 SSL_RC2_CBC_128_CBC_WITH_MD5 SSL_DES_64_CBC_WITH_MD5 SSL_RC4_64_WITH_MD5 SSL_RC4_128_EXPORT40_WITH_MD5 SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5	«暗号スイート» TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5
«暗号スイートグループ» TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 SSL_DES_192_EDE3_CBC_WITH_MD5 SSL_RC4_128_WITH_MD5	«暗号スイートグループ» LS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
HIGH TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 SSL_DES_192_EDE3_CBC_WITH_MD5	HIGH TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA
MEDIUM TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA SSL_RC4_128_WITH_MD5	MEDIUM TLS_RSA_WITH_3DES_EDE_CBC_SHA
LOW TLS_RSA_WITH_DES_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	LOW TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5

	TLS_RSA_EXPORT_WITH_RC4_40_MD5 TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA TLS_RSA_EXPORT1024_WITH_RC4_56_MD5 TLS_RSA_EXPORT1024_WITH_RC4_56_SHA TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5 SSL_RC2_CBC_128_CBC_WITH_MD5 SSL_DES_64_CBC_WITH_MD5 SSL_RC4_64_WITH_MD5 SSL_RC4_128_EXPORT40_WITH_MD5 SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5		
	EXPORT TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC4_40_MD5 TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA TLS_RSA_EXPORT1024_WITH_RC4_56_MD5 TLS_RSA_EXPORT1024_WITH_RC4_56_SHA TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5 SSL_RC4_128_EXPORT40_WITH_MD5 SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5		未サポート
	EXPORT40 TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC4_40_MD5 TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 SSL_RC4_128_EXPORT40_WITH_MD5 SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5		未サポート
	EXPORT56 TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA TLS_RSA_EXPORT1024_WITH_RC4_56_MD5 TLS_RSA_EXPORT1024_WITH_RC4_56_SHA TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5		未サポート
	RSA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_DES_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC4_40_MD5 TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA TLS_RSA_EXPORT1024_WITH_RC4_56_MD5 TLS_RSA_EXPORT1024_WITH_RC4_56_SHA TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5 SSL_DES_192_EDE3_CBC_WITH_MD5 SSL_RC4_128_WITH_MD5 SSL_RC2_CBC_128_CBC_WITH_MD5 SSL_DES_64_CBC_WITH_MD5 SSL_RC4_64_WITH_MD5 SSL_RC4_128_EXPORT40_WITH_MD5 SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5		RSA TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5
	AES		AES

	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256		TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA
	未サポート		AES_GCM TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_GCM_SHA256
	SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA TLS_RSA_EXPORT1024_WITH_RC4_56_SHA		SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256		SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256
	未サポート		SHA384 TLS_RSA_WITH_AES_256_GCM_SHA384
	MD5 TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5 TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT1024_WITH_RC4_56_MD5 TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5 SSL_DES_192_EDE3_CBC_WITH_MD5 SSL_RC4_128_WITH_MD5 SSL_RC2_CBC_128_CBC_WITH_MD5 SSL_DES_64_CBC_WITH_MD5 SSL_RC4_64_WITH_MD5 SSL_RC4_128_EXPORT40_WITH_MD5 SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5		MD5 TLS_RSA_WITH_RC4_128_MD5
	SSL2.0(SSL2) SSL_DES_192_EDE3_CBC_WITH_MD5 SSL_RC4_128_WITH_MD5 SSL_RC2_CBC_128_CBC_WITH_MD5 SSL_DES_64_CBC_WITH_MD5 SSL_RC4_64_WITH_MD5 SSL_RC4_128_EXPORT40_WITH_MD5 SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5		未サポート
	SSL3.0(SSL3) または TLS1.0(TLS1) TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC4_40_MD5 TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA TLS_RSA_EXPORT1024_WITH_RC4_56_MD5 TLS_RSA_EXPORT1024_WITH_RC4_56_SHA		SSL3.0(SSL3) または TLS1.0(TLS1) TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5

	TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5		
	TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA		TLS1.1 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5
	TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256		TLS1.2 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5

【影 響】

cipher-suites コマンドに削除された暗号スイートや暗号スイートグループが設定されている構成定義ファイルを使用する場合、構成定義ファイルの読み込み時(load コマンド実行時)にエラーとなります。また、暗号スイートグループから削除された暗号スイートしかサポートしない SSL クライアントとの接続ができなくなります。

【対 処】

cipher-suites コマンドに削除された暗号スイートや暗号スイートグループが設定されている場合は、見直しが必要です。

2-2-5-3) TLS1.2 を使用して暗号通信を行う場合に、「MD5」ハッシュを利用した SSL 通信ができなくなる

TLS1.2 を使用して暗号通信を行う場合に、「MD5」ハッシュを利用した SSL 通信ができなくなります。

【IPCOM VA2】

1) ServerKeyExchange の署名に使用するハッシュについて

DH 系の暗号スイート(ECDHE)でネゴシエーションを行う際、クライアントが利用可能なハッシュアルゴリズムとして「MD5」を高優先度で通知してきた場合、クライアントに通知する ServerKeyExchange の署名に「MD5」を使用します。

2) クライアント証明書の提出要求(Certificate Request)について

クライアント証明書の提出を要求する際(client-authentication で require、opt-validate、または optional を指定)、SSL アクセラレーターからクライアントへ要求する「証明書提出要求(Certificate Request)」に含まれる「ハッシュアルゴリズム(supported_signature_algorithms)」に、「MD5 を含めて」クライアントに通知します。

ただし、「client-authentication」コマンドで「submit-ca-list」パラメーターを設定し、「cert ca-group prohibit-hash」コマンドで「MD5」を禁止していた場合は、「MD5」を除外してクライアントに通知します。

【IPCOM VE2m】

1) ServerKeyExchange の署名に使用するハッシュについて

DH 系の暗号スイート(ECDHE 含む)でネゴシエーションを行う際、ServerkeyExchange の署名に使用するハッシュは「MD5 以外(SHA1、または SHA2)」となります。

2) クライアント証明書の提出要求(Certificate Request)について

クライアント証明書の提出を要求する際(client-authentication で require、opt-validate、または optional を指定)、SSL アクセラレーターからクライアントへ要求する「証明書提出要求(Certificate Request)」に含まれる「ハッシュア

ルゴリズム(supported_signature_algorithms)」に、「MD5」を除外してクライアントに通知します。

また、「client-authentication」コマンドで「submit-ca-list」パラメーターを設定し、「cert ca-group prohibit-hash」コマンドで「MD5」を有効としていた場合でも、「MD5」を除外してクライアントに通知します。

【影 響】

1)クライアントからの SSL 通信に対して以下の影響があります。

・クライアントが TLS1.2 のみ 許可している場合

クライアントが「MD5 のみ」を利用可能なハッシュアルゴリズムとしていた場合、SSL 通信が行えなくなります。

・ クライアントが TLS1.2 および TLS1.1 以下 も許可している場合クライアントが「MD5 のみ」を利用可能なハッシュアルゴリズムとしていた場合は、TLS1.1 以下のプロトコルへプロトコルバージョンを下げて通信を継続します。

【対 処】

1)接続できない場合は以下の対処を行ってください。

・ 本装置の SSL アクセラレーターの設定（「protocol」コマンド）およびクライアントの双方で、TLSv1.1 や TLSv1.0 を有効してください。

・TLS1.1，TLS1.0 を有効にできない場合は、「ssl-accel/unsafe-signature-hash」コマンドで MD5 の利用を有効にしてください。(非推奨)。

2.2.6 その他の構成定義編集に関わる留意事項

2-2-6-1) クラス識別子の構成定義編集に関わる留意事項

装置全体でマッチングルール数が、装置諸元値内かどうかの整合性検査(validate コマンド/commit コマンド実行)の対象に、サーバ負荷分散機能を追加します。

【IPCOM VA2】

装置全体のマッチングルール数の整合性検査対象となる機能は以下のとおりです。

・ファイアーウォール機能（アクセス制御ルール）

・アノマリ型 IPS 機能

・アドレス変換機能

・QoS 制御（帯域制御）機能

・リンク負荷分散機能

【IPCOM VE2m】

装置全体のマッチングルール数の整合性検査対象となる機能は以下のとおりです。

・ファイアーウォール機能（アクセス制御ルール）

・アノマリ型 IPS 機能

・アドレス変換機能

・QoS 制御（帯域制御）機能

・リンク負荷分散機能

・サーバ負荷分散機能

【影 響】

整合性検査の実行時に、サーバ負荷分散機能が使用するマッチングルール数を加えて算出された結果が装置全体で設定できるマッチングルール数を超えた場合に、WARNING メッセージを表示しますが、設定は可能で、継続して運用可能で

す。

【対 処】

no class-map コマンド、no time-period コマンド、または class-map 内で、no match コマンドにより何れかを削除するか、match コマンドの統廃合を行ってください。

2-2-6-2) secure tcp-minimum-send-mss コマンドの追加

TCP3 ウェイ・ハンドシェイク時に、リモートから通知された最大セグメントサイズ(MSS)が有効になる最小値を設定する機能を提供します。また、リモートから通知された MSS が有効になる最小値のデフォルトを変更しています。

【IPCOM VA2】

TCP3 ウェイ・ハンドシェイク時に、リモートから通知された MSS が有効になる最小値を設定する機能はサポートしていません。リモートから通知された MSS が有効になる最小値は、48 バイトです。

【IPCOM VE2m】

以下の機能を使用時、TCP3 ウェイ・ハンドシェイク時にリモートから通知された MSS が有効になる最小値を設定する機能（"secure tcp-minimum-send-mss" コマンドで設定）をサポートします。

・サーバ負荷分散機能
・Web アプリケーション・ファイアーウォール機能
・クラウドプロキシ機能
・SSL アクセラレーター機能
・SSL-VPN サービス機能
・HTTP コンテンツ圧縮機能
・FNA ルーティング機能
・運用管理/保守機能（運用管理装置と本装置を telnet/ssh/https(Web ブラウザ/ダウンロード版モニタ)で接続時）

"secure tcp-minimum-send-mss" コマンドを設定しない場合、リモートから通知された MSS が有効になる最小値は、216 バイトです。

【影 響】

リモートから通知された MSS が"secure tcp-minimum-send-mss" コマンドで設定された値（未設定の場合は 216 バイト）よりも小さい場合、通知された MSS 値は無視され、"secure tcp-minimum-send-mss" コマンドで設定された値（未設定の場合は 216 バイト）がリモートの MSS 値として動作します。このため、悪意の無い正常なリモート装置が本コマンドで設定された値より小さい MSS 値で通信しようとした場合に通信できない可能性があります。その場合は、"secure tcp-minimum-send-mss" コマンドの設定を見直してください。

【対 処】

ファームアップ後に通信ができなくなった場合は、"secure tcp-minimum-send-mss" コマンドで、システムで必要な最小 MSS 値を設定してください。

2.3 運用時の留意事項

構成定義編集時に留意していただく事項を記します。

2.3.1 サーバ負荷分散機能の運用時の留意事項

2-3-1-1) アクセス制限超過時に出力する mlog の出力レベルの変更 ※IPCOM VA2 1300 が対象

サーバ負荷分散ルール単位のアクセス制限設定時、アクセス制限超過時に出力する mlog [00805030]および[00805830]は、サーバ負荷分散ルールのログレベルが詳細レベル(audit-all)の場合のみ出力しましたが、サーバ負荷分散ルールのログレベルがすべてのレベル(audit-normal、audit-outline、audit-all) の場合に出力するように変更します。

【IPCOM VA2】

以下のサーバ負荷分散ルールへのアクセス数超過の mlog[00805030]および[00805830]はサーバ負荷分散ルールのログレベルが詳細レベル(audit-all)の場合に出力します。

《サーバ負荷分散ルールへのアクセス数超過》

NOTICE[00805030]【一般出力形式】

The number of access to a slb rule reached the maximum value.(SlbID=%1$u)

NOTICE[00805830]【ダイジェスト形式】

The number of access to a slb rule reached the maximum value. %2$S

【説明】サーバ負荷分散ルールへのアクセス数が、アクセス上限値に達しました。

・挿入文%1$u: サーバ負荷分散ルール ID

・挿入文%2$S:(N times / M sec) （M 秒間に N 回同じイベントが発生しました）

【IPCOM VE2m】

以下のサーバ負荷分散ルールへのアクセス数超過の mlog[00805030]および[00805830]はサーバ負荷分散ルールのログレベルが、すべてのレベル(audit-normal、audit-outline、audit-all)の場合に出力します。

《サーバ負荷分散ルールへのアクセス数超過》

NOTICE[00805030]【一般出力形式】

The number of access to a slb rule reached the maximum value.(SlbID=%1$u)

NOTICE[00805830]【ダイジェスト形式】

The number of access to a slb rule reached the maximum value. %2$S

【説明】サーバ負荷分散ルールへのアクセス数が、アクセス上限値に達しました。

・挿入文%1$u: サーバ負荷分散ルール ID

・挿入文%2$S:(N times / M sec) （M 秒間に N 回同じイベントが発生しました）

【影 響】ログレベルの設定によっては、従来よりもログ出力量が増える可能性があります。

【対 処】ありません。

2-3-1-2) established 状態のアクセスリミットを越える際の出力メッセージの変更 ※IPCOM VA2 1300 が対象

real-server 配下の access-limit mode connection established が定義されている場合、established 状態のアクセ

スリミットを越えるタイミングにより、 以下の 2 種類の mlog が出力される場合がありました。

・[00805031](ESTABLISHED 状態のコネクション数によるアクセス数超過)

・[00805013]または[00805014] (利用可能な転送先サーバなし)

access-limit mode connection established でのアクセスリミット使用時、アクセスリミット超過時は、[00805031](ESTABLISHED 状態のコネクション数によるアクセス数超過)を出力するように統一します。

【IPCOM VA2】

real-server 配下に access-limit mode connection established が定義されている場合、ESTABLISHED 状態のコネクション数によるアクセス数超過時に、以下の mlog NOTICE[00805013]または[00805014]のどちらか一つを出力します。

● NOTICE[00805013]

《仮想ポートに対する利用可能な転送先サーバなし》

【一般出力形式】

There is no service at the transfer destination that can be used as a virtual port.(SlbID=%1$u,DistID=%2$u)

【ダイジェスト出力形式】

There is no service at the transfer destination that can be used as a virtual port. %3$s

【説明】

仮想ポートに対する利用可能な転送先サービスがありません。

・挿入文%1$u: サーバ負荷分散ルール ID

・挿入文%2$u: 分散条件ルール ID

・挿入文%3$s:(N times / M sec) （M 秒間に N 回同じイベントが発生しました）

● NOTICE[00805014]

《利用可能な転送先サーバなし》

【一般出力形式】

There is no server at the transfer destination that can be used.(SlbID=%1$u,DistID=%2$u)

【ダイジェスト出力形式】

There is no server at the transfer destination that can be used. %3$s

【説明】

利用可能な転送先サーバがありません。

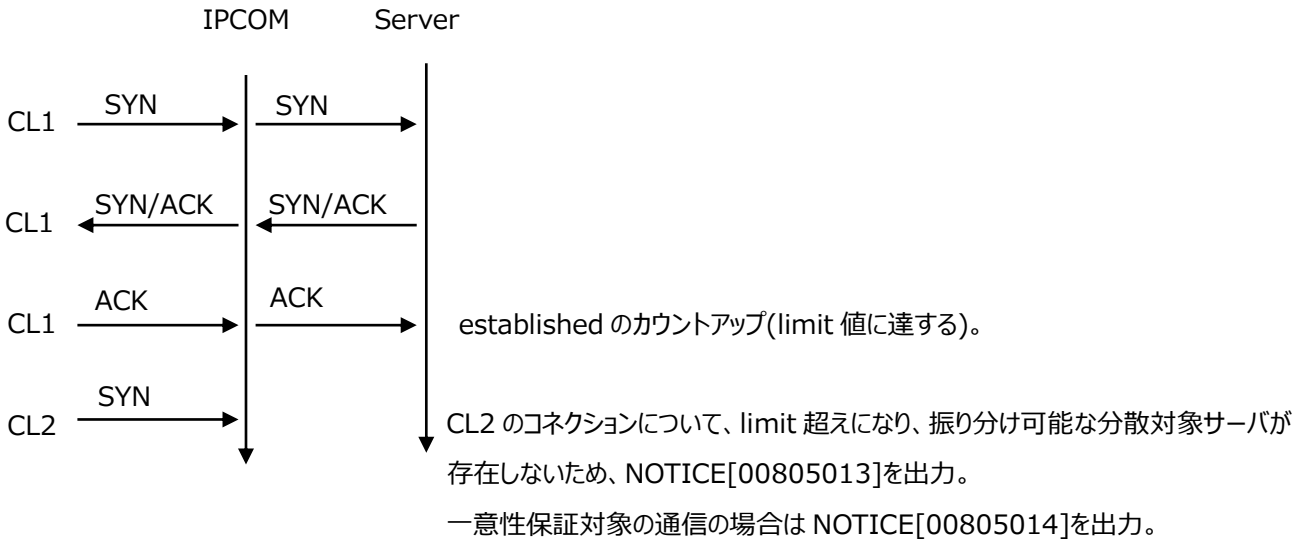
・挿入文%1$u: サーバ負荷分散ルール ID

・挿入文%2$u: 分散条件ルール ID

・挿入文%3$s:(N times / M sec) （M 秒間に N 回同じイベントが発生しました）

NOTICE[00805013]または[00805014]が出力されるシーケンスの例

（アクセス制限数が 1、分散対象サーバが 1 台として例示します。）



【IPCOM VE2m】

real-server 配下に access-limit mode connection established が定義されている場合に、ESTABLISHED 状態のコネクション数によるアクセス数超過時は以下の mlog を出力します。

● NOTICE[00805031]

《ESTABLISHED 状態のコネクション数によるアクセス数超過》

【一般出力形式】

The number of established connection reached the maximum value.(SlbID=%1$u, DistID=%2$u, Server=%3$s)

【ダイジェスト出力形式】

The number of established connection reached the maximum value. %4$S

【説明】

ESTABLISHED 状態のコネクション数が、上限値に達しました。

・挿入文%1$u: サーバ負荷分散ルール ID

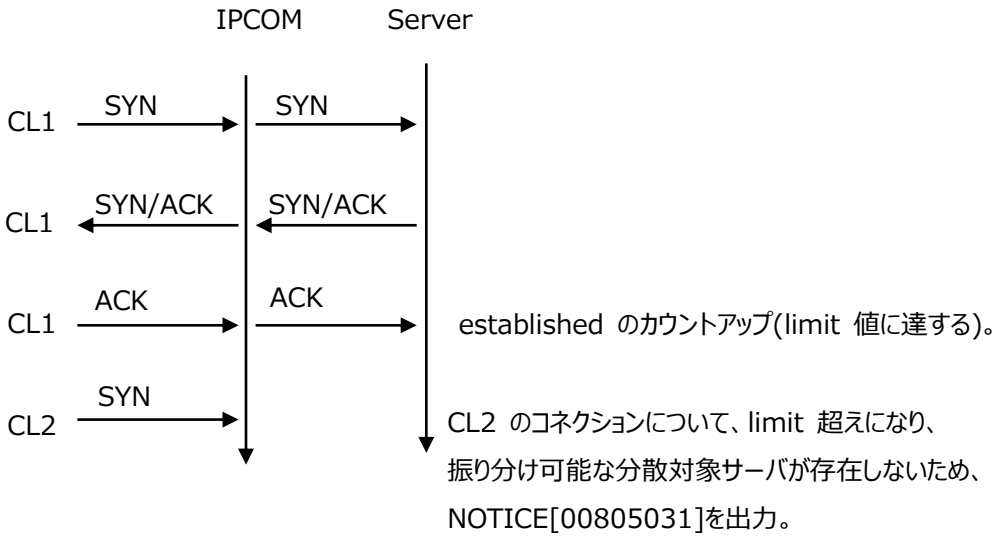
・挿入文%2$u: 分散条件ルール ID （サーバ単位のアクセス数超過の場合）

・挿入文%3$s: サーバの IPv4/IPv6 アドレス（サーバ単位のアクセス数超過の場合）

・挿入文%4$S:(N times / M sec) （M 秒間に N 回同じイベントが発生しました）

修正後のシーケンスの例

（アクセス制限数が 1、分散対象サーバが 1 台として例示します。）



【影 響】

real-server 配下に access-limit mode connection established が定義されている場合に、アクセス数超過発生時に[00805013]または[00805014]が出力されず、[0080531]が出力されるようになります。

【対 処】

real-server 配下に access-limit mode connection established が定義時、アクセス数超過をログによる監視を行っている場合は、[00805013]または[00805014]から、[0080531]に監視対象を変更してください。

2-3-1-3) サーバ負荷分散機能に関連するメッセージログの重大度とメッセージ ID の変更

メッセージログの重大度とメッセージ ID を変更しています。

【IPCOM VA2】

0083FF0A (8650506) INFO	《切り離し終了》 "clear maintenance slb" command succeeded.(slb-ext-monitor rule ID=%1$u command:%2$s)
0083FF10 (8650512) INFO	《拡張型故障監視（アプリケーション監視） で復旧検知》 Recovery of a monitor target was detected in Application(%1$s) monitor.(%2$s[%3$s] slb-ext-monitor ruleID=%4$u)

【IPCOM VE2m】

4083FF0A (8650506) WARNING	《切り離し終了》 "clear maintenance slb" command succeeded.(slb-ext-monitor rule ID=%1$u command:%2$s)
4083FF10 (8650512) WARNING	《拡張型故障監視（アプリケーション監視） で復旧検知》 Recovery of a monitor target was detected in Application(%1$s) monitor.(%2$s[%3$s] slb-ext-monitor ruleID=%4$u)

【影 響】

・監視プログラム等でログ ID をチェックしている場合は監視プログラム等の修正が必要です。

・logging collection level message を、warning に設定していた場合は、ログ出力に影響があります。なお、logging collection level message のデフォルト値は warning のため、初期状態の場合は影響があります。logging collection level message warning を設定していた場合 異常が発生した際、本ログは出力されません。

【対 処】

・監視プログラム等でログ ID をチェックしていなければ不要です。

・ログの必要性を踏まえ、必要に応じて logging collection level message の設定を見直してください。

3-3-1-4) ChallengeACK 対応

分散対象サーバ（あるいはクライアント）から送信される ChallengeACK に対して、本装置から RST 応答するように変更しています。

【IPCOM VA2】

以下の条件の場合、分散対象サーバ（あるいはクライアント）でコネクションが滞留します。

・L4 負荷分散以外の分散方式を使用している。

・パケットロスト等により、本装置が送信した RST が、受信側で期待しているシーケンス番号でない。

・受信側が RFC5961(ChallengeACK)に対応しており、上記 RST のシーケンス番号が、期待するものから Window サイズの範囲内である場合に、ChallengeACK を返送する。

【IPCOM VE2m】

以下の条件の場合、分散対象サーバ（あるいはクライアント）から送信される ChallengeACK に対して、本装置から RST 応答します。そのため、分散対象サーバ（あるいはクライアント）でコネクションは滞留しません。

・L4 負荷分散以外の分散方式を使用している。

・パケットロスト等により、本装置が送信した RST が、受信側で期待しているシーケンス番号でない。

・受信側が RFC5961(ChallengeACK)に対応しており、上記 RST のシーケンス番号が、期待するものから Window サイズの範囲内である場合に、ChallengeACK を返送する。

【影 響】

L4 負荷分散以外（HTTP Keep-Alive 負荷分散、IIOP 負荷分散でメソッド呼び出し単位の負荷分散、Web アクセラレーション機能、または以下のサーバ負荷分散のいずれかの機能）を使用したサーバ負荷分散ルールで、コネクション終了後、コネクション情報を解放するまでの時間、SYN 以外のパケットを受信した際に RST 応答を行います。(コネクション情報を解放するまでの時間については、後述します)

RFC5961 に対応しているクライアントまたは分散対象サーバから RST パケットの確認応答(Challenge ACK)を受信した場合でも、正しいシーケンス番号の RST の再送を行います。

・ コンテンツ単位の負荷分散

・ HTTP 情報による一意性保証 cookie

単位

cookie・URL リライト単位

HTTP ヘッダー情報単位 HTTP

認証ヘッダー単位

ASP.NET セッション ID 単位

・ HTTP レイヤーでのセッションリカバリー機能

・ 分散対象パケットの置換機能

・ HTTP ヘッダー挿入機能

・ エラーページ表示機能

コネクション情報を解放するまでの時間についてコネクション情報を解放するまでの時間は、コネクション終了後、以下のコマンドで指定された時間(秒)が満了するまでとなります。

－HTTP Keep-Alive 負荷分散を使用時 slb http-keep-alive tcp-advance コマンドを定義していない場合は
slb http-keep-alive tcp-disconnecting-timer コマンド（コマンド省略時：1 秒）
slb http-keep-alive tcp-advance コマンドを定義している場合は monitor tcp-disconnecting-timer コマンド（コマンド省略時：10 秒）

－IIOP 負荷分散でメソッド呼び出し単位の負荷分散を使用時
slb iiop tcp-advance コマンドを定義していない場合は slb iiop tcp-disconnecting-timer コマンド（コマンド省略時：1 秒）
slb iiop tcp-advance コマンドを定義している場合は monitor tcp-disconnecting-timer コマンド（コマンド省略時：10 秒）

－Web アクセラレーション機能を使用時
slb web-accelerate tcp-advance コマンドを定義していない場合は slb web-accelerate tcp-disconnecting-timer コマンド（コマンド省略時：1 秒）
slb web-accelerate tcp-advance コマンドを定義している場合は monitor tcp-disconnecting-timer コマンド（コマンド省略時：10 秒）

－HTTP Keep-Alive 負荷分散機能、IIOP 負荷分散でメソッド呼び出し単位の負荷分散、Web アクセラレーション機能を使用していない、かつ、上記のサーバ負荷分散のいずれかの機能を使用時 monitor tcp-disconnecting-timer コマンド（コマンド省略時：10 秒）

【対 処】

不要です。

3-3-1-5) 分散対象サーバの状態変化時刻の通知

分散対象サーバ本体や提供しているサービス毎に、状態が変化した時刻が出力されるようになります。また、モニタ表示やレポート出力で、「状態」の項目が、「動作状態」と「運用状態」に分かれます。

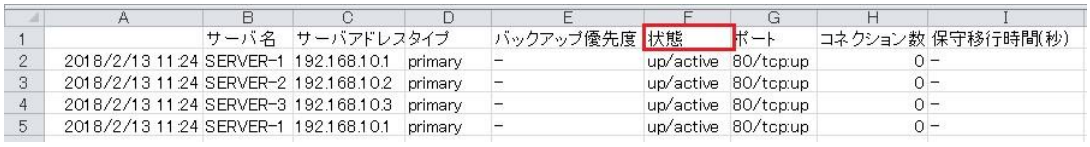
【IPCOM VA2】

・サーバ負荷分散モニタ

サーバ負荷分散モニタ

サーバ名	サーバアドレス	タイプ	バックアップ優先度	状態	ポート	コネクション数	保守移行時間(秒)
SERVER-1	192.168.10.1	primary	-	up/active	80/tcp:up	0	-
SERVER-2	192.168.10.2	primary	-	up/active	80/tcp:up	0	-
SERVER-3	192.168.10.3	primary	-	up/active	80/tcp:up	0	-

・条件負荷分散ルールのレポート出力



	A	B	C	D	E	F	G	H	I
1		サーバ名	サーバアドレス	タイプ	バックアップ優先度	状態	ポート	コネクション数	保守移行時間(秒)
2	2018/2/13 11:24	SERVER-1	192.168.10.1	primary	-	up/active	80/tcp:up	0	-
3	2018/2/13 11:24	SERVER-2	192.168.10.2	primary	-	up/active	80/tcp:up	0	-
4	2018/2/13 11:24	SERVER-3	192.168.10.3	primary	-	up/active	80/tcp:up	0	-
5	2018/2/13 11:24	SERVER-1	192.168.10.1	primary	-	up/active	80/tcp:up	0	-

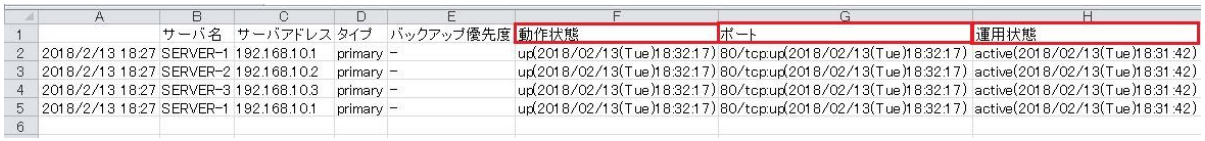
【IPCOM VE2m】

・サーバ負荷分散モニタ

サーバ負荷分散モニタ

サーバ名	サーバアドレス	タイプ	バックアップ優先度	動作状態	ポート	運用状態	コネクシ
SERVER-1	192.168.10.1	primary	-	up(2018/02/09(Fri)16:02:32)	80/tcp:up(2018/02/09(Fri)16:02:32)	active(2018/02/09(Fri)14:41:36)	
SERVER-2	192.168.10.2	primary	-	up(2018/02/09(Fri)16:02:32)	80/tcp:up(2018/02/09(Fri)16:02:32)	active(2018/02/09(Fri)14:41:36)	
SERVER-3	192.168.10.3	primary	-	up(2018/02/09(Fri)16:22:50)	80/tcp:up(2018/02/09(Fri)16:22:50)	active(2018/02/09(Fri)14:41:36)	

・条件負荷分散ルールのレポート出力



	A	B	C	D	E	F	G	H
1		サーバ名	サーバアドレス	タイプ	バックアップ優先度	動作状態	ポート	運用状態
2	2018/2/13 18:27	SERVER-1	192.168.10.1	primary	-	up(2018/02/13(Tue)18:32:17)	80/tcp:up(2018/02/13(Tue)18:32:17)	active(2018/02/13(Tue)18:31:42)
3	2018/2/13 18:27	SERVER-2	192.168.10.2	primary	-	up(2018/02/13(Tue)18:32:17)	80/tcp:up(2018/02/13(Tue)18:32:17)	active(2018/02/13(Tue)18:31:42)
4	2018/2/13 18:27	SERVER-3	192.168.10.3	primary	-	up(2018/02/13(Tue)18:32:17)	80/tcp:up(2018/02/13(Tue)18:32:17)	active(2018/02/13(Tue)18:31:42)
5	2018/2/13 18:27	SERVER-1	192.168.10.1	primary	-	up(2018/02/13(Tue)18:32:17)	80/tcp:up(2018/02/13(Tue)18:32:17)	active(2018/02/13(Tue)18:31:42)
6								

【影 響】

「状態」の項目が、「動作状態」と「運用状態」の項目に分かれ、それぞれに状態が変化した時刻表示が追加されます。

また、モニタ表示、レポート出力ともに、「ポート」の項目にも時刻が表示されます。

【対 処】

レポート出力した CSV ファイルを加工して使用している場合、見直しが必要です。

2.3.2 QoS 機能の運用時の留意事項

2-3-2-1) QoS 拡張 MIB

QoS 拡張 MIB の取得値が仕様と異なっていたため、修正します。

【影 響】

QoS クラス(qos-class)を複数階層定義している場合、以下の MIB 取得値がファームアップの前後で変わることがありま

す。

1) isfexQosClsName

2) isfexQosClsDescr

3) isfexQosClsTable 配下のエントリー数(取得可能な qos-class の個数)

【対 処】

本装置(IPCOM)については対処不要です。

本装置(IPCOM)を監視している外部装置において、以下の対処が必要です。

1) ファームアップの前後で MIB 取得値が変更となっている場合、監視対象（QoS クラス(qos-class)）のリソース名を更新してください。

2) ファームアップの前後で MIB 取得値が変更となっている場合、監視対象（QoS クラス(qos-class)）のリソース名を更新してください。

エントリー数が増えていた場合、isfexQosClsName または isfexQosClsDescr により、監視要否を確認の上、監視が必要な場合は追加してください。

2.3.3 Web アプリケーション・ファイアーウォール機能の運用時の留意事項

2-3-3-1) メッセージログの重大度とメッセージ ID の変更

メッセージログの重大度とメッセージ ID を変更しています。

【IPCOM VA2】

40580002 (5767170) WARNING	《無通信監視タイムアウトによるコネクション切断》 【一般出力形式】 The connection has been disconnected because of the idle timeout. %1$s %2$s 【ダイジェスト出力形式】なし

【IPCOM VE2m】

00580002 (5767170) INFO	《無通信監視タイムアウトによるコネクション切断》 【一般出力形式】 The connection has been disconnected because of the idle timeout. %1$s %2$s 【ダイジェスト出力形式】なし

【影 響】

・監視プログラム等でログ ID をチェックしている場合は監視プログラム等の修正が必要です。

・logging collection level message を、warning に設定していた場合は、ログ出力に影響があります。なお、logging collection level message のデフォルト値は warning のため、初期状態の場合は影響があります。logging collection level message warning を設定していた場合、異常が発生した際、本ログは出力されます。

【対 処】

・監視プログラム等でログ ID をチェックしていなければ不要です。

・ログの必要性を踏まえ、必要に応じて logging collection level message の設定を見直してください。

2.3.4 SSL アクセラレーター 機能の運用時の留意事項

2-3-4-1) メッセージログの重大度とメッセージ ID の変更

メッセージログの重大度とメッセージ ID を変更しています。

【IPCOM VA2】

40520011 (5373969) WARNING	《無通信監視タイムアウトによるコネクション切断》 【一般出力形式】 The connection has been disconnected because of the idle timeout. %1$s%2$s 【ダイジェスト出力形式】なし
40520021 (5373985) WARNING	《アプリケーションレベルの無通信監視タイムアウトによるコネクション切断》 【一般出力形式】 The connection has been disconnected because of the application layer timeout. %1$s 【ダイジェスト出力形式】 The connection has been disconnected because of the application layer timeout. %1$s %2$s
40520121 (5374241) WARNING	

【IPCOM VE2m】

00520011 (5373969) INFO	《無通信監視タイムアウトによるコネクション切断》 【一般出力形式】 The connection has been disconnected because of the idle timeout. %1$s%2$s 【ダイジェスト出力形式】なし
00520021 (5373985) INFO	《アプリケーションレベルの無通信監視タイムアウトによるコネクション切断》 【一般出力形式】 The connection has been disconnected because of the application layer timeout. %1$s 【ダイジェスト出力形式】 The connection has been disconnected because of the application layer timeout. %1$s %2$s
00520121 (5374241) INFO	

【影 響】

・監視プログラム等でログ ID をチェックしている場合は監視プログラム等の修正が必要です。

・logging collection level message を、warning に設定していた場合は、ログ出力に影響があります。なお、logging collection level message のデフォルト値は warning のため、初期状態の場合は影響があります。logging collection level message warning を設定していた場合、異常が発生した際、本ログは出力されます。

【対 処】

・監視プログラム等でログ ID をチェックしていなければ不要です。

・ログの必要性を踏まえ、必要に応じて logging collection level message の設定を見直してください。

2-2-4-2) 一時鍵の生成

ECDHE_RSA 鍵交換の暗号スイートを利用する場合、SSL ネゴシネーションで利用する一時鍵を生成します。

この一時鍵の更新間隔を変更しています。

【IPCOM VA2】

一定期間ごとに一時鍵を生成します。

【IPCOM VE2m】

セッションごとに一時鍵を生成します。

【影 響】

楕円曲線暗号使用時、セキュリティ強度は向上しますが、トランザクション性能は低下します。

【対 処】

一定期間ごとに一時鍵を生成したい場合は、pfs-negotiation コマンドで、「term」を設定してください。

2.3.5 HTTP コンテンツ圧縮機能の運用時の留意事項

2-3-5-1) メッセージログの重大度とメッセージ ID の変更

メッセージログの重大度とメッセージ ID を変更しています。

【IPCOM VA2】

4061F004 (6418436) WARNING	《無通信監視タイムアウトによる HTTP 圧縮コネクション切断》 【一般出力形式】 The http-compress connection has been disconnected because of the idle timeout. %1$s %2$s 【ダイジェスト出力形式】なし

【IPCOM VE2m】

0061F004 (6418436) INFO	《無通信監視タイムアウトによる HTTP 圧縮コネクション切断》 【一般出力形式】 The http-compress connection has been disconnected because of the idle timeout. %1$s %2$s 【ダイジェスト出力形式】なし

【影 響】

・監視プログラム等でログ ID をチェックしている場合は監視プログラム等の修正が必要です。

・logging collection level message を、warning に設定していた場合は、ログ出力に影響があります。なお、logging collection level message のデフォルト値は warning のため、初期状態の場合は影響があります。logging collection level message warning を設定していた場合 異常が発生した際、本ログは出力されます。

【対 処】

・監視プログラム等でログ ID をチェックしていなければ不要です。

・ログの必要性を踏まえ、必要に応じて logging collection level message の設定を見直してください。

2.3.6 その他の運用時の留意事項

2-3-6-1) Web コンソールの TLS1.1/1.2 の対応 ※IPCOM VA2 1300 が対象

TLS1.1/1.2 での Web コンソール接続に対応しました。

【IPCOM VA2】

TLS1.1/1.2 のプロトコルでは Web コンソール接続できません。

【IPCOM VE2m】

TLS1.1/1.2 のプロトコルで Web コンソール接続が可能です。

【影 響】

Web コンソールのサーバ証明書のハッシュアルゴリズムに MD5 を使用している場合は、TLS1.2 では Web コンソール接続できません。

【対 処】下記のいずれかの作業を実施してください。

・運用管理コマンドの web-console ssl-cert renew でハッシュアルゴリズムに md5 以外を指定して Web コンソール用証明書を更新する。

・ブラウザのインターネットオプション設定にて「TLS1.2 の使用」のチェックを外す。

・構成定義コマンドの web-console protocol で TLS1.2 を使用しないよう定義変更する。

2-3-6-2) Web コンソールの CVE-2016-2183 の対応

CVE-2016-2183 の対応として、Web コンソールの接続に TLS_RSA_WITH_3DES_EDE_CBC_SHA の暗号スイートがデフォルトでは使用できないように変更します。

【IPCOM VA2】

Web コンソールの接続に TLS_RSA_WITH_3DES_EDE_CBC_SHA の暗号スイートが使用できます。

【IPCOM VE2m】

Web コンソールの接続に TLS_RSA_WITH_3DES_EDE_CBC_SHA の暗号スイートがデフォルトでは使用できません。

【影 響】

特に影響はありません。

なお、過去にサポートしていましたが、現在は未サポートの以下の OS から Web コンソールへデフォルトでは接続ができなくなります。

・Windows XP

・Windows Server 2003

【対 処】

対処は不要です。

なお、web-console cipher-suites コマンドで以下のように定義することで IPCOM VA2 と同じ動作となります（1 行で記述します）。

TLS_RSA_WITH_3DES_EDE_CBC_SHA も使用できるようになります。

```
web-console cipher-suites +TLS_RSA_WITH_AES_128_GCM_SHA256
+TLS_RSA_WITH_AES_256_GCM_SHA384 +TLS_RSA_WITH_AES_128_CBC_SHA256
+TLS_RSA_WITH_AES_256_CBC_SHA256 +TLS_RSA_WITH_AES_128_CBC_SHA
+TLS_RSA_WITH_AES_256_CBC_SHA +TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

第 3 章 環境の移行

本章では、IPCOM VE2m 作成前に必要となる環境準備作業について説明します。

3.1 IPCOM VA2 から IPCOM VE2m への環境の移行

IPCOM VA2 と IPCOM VE2m は、ソフトウェアプラットフォームが異なるため、IPCOM VA2 の環境定義情報のバックアップデータ(backup environment)を IPCOM VE2m でレストア(restore environment)することができません。手動による環境の移出・移入を行う必要があります。

環境の移出・移入に関しては、以下の手順を参考に実施してください。

IPCOM EX2 ソフトウェアシリーズ 保守ガイド 1-7 環境を移出・移入する

第 4 章 冗長化構成の移行手順例

本章では、運用中の冗長化構成の IPCOM VA2 に対する IPCOM VE2m の構築手順例と運用切り替え手順例を記載します。IPCOM VA2 から IP アドレスの引き継ぎ有無で、構築手順や切り替え手順が異なります。

4-1 冗長化構成時の構築手順例・運用切り替え手順例

IP アドレス引継		構成手順例	運用切り替え手順例
物理	仮想 代表		
無	有	VA2 を停止せずに VE2m を構築する。 1. VA2 と異なる新規の IP 体系で VE2m を構築 2. テストを実施 ・新規の仮想/代表 IP アドレスによる疎通確認 ・冗長化切り替え	代表 IP アドレス、仮想 IP アドレスを変更して、VE2m に運用を切り替える。 1. VE2m の ACT の config を VA2 の仮想/代表 IP アドレスに変更。(commit しない) 2. VA2 を STANBY, ACT の順で停止 3. VE2m の ACT を commit。SBY に反映。 4. 新規に作成したダミーポートを削除 想定サービス中断時間： commit 反映：30 秒程度 バックアウト方法： 全 VE2m 停止後、VA2 を起動
無	無	同上	対向先サーバ、仮想ルータに対して、VE2m の IP アドレスに置き換えて切り替えます。 1. 対向サーバで VA2 へのルーティング設定がある場合、VE2m へのルーティングに変更 2. VA2 で FIP を使用している場合、関連付けを解除し、VE2m に関連付けする。 3. 仮想ルータに FW やルーティング設定がある場合、VE2m 用の IP 体系に変更 4. VA2 を STANBY, ACT の順で停止 ※VA2 を削除する際、VA2 のダミーポートを削除 想定サービス中断時間： その他の通信：1 つの対向サーバごとに 60 秒程度 FIP の通信：5 秒程度 バックアウト方法： 全 VE2m 停止後、VA2 を起動 上記の「1.」、「2.」、「3.」の変更を元に戻す。

有	有	VA2 を停止して VE2m を構築する。 1. VA2 を SBY, ACT の順で停止 2. VA2 の IaaS のポートを順にデタッチ 3. VA2 と同じ IP 体系で VE2m を構築 ※2.のポートを指定して、VE2m の仮想サーバを作成 4. テストを実施 ・仮想/代表 IP アドレスによる疎通確認 ・冗長化切り替え 5. VA2 の仮想サーバを削除	左記手順を実施する。 想定サービス中断時間： VE2m の構築：2 時間程度 バックアウト方法： できません。

第 5 章 シングル構成の移行手順例

本章では、シングル構成の IPCOM VA2 に対する IPCOM VE2m の構築手順例と運用切り替え手順例を記載します。IPCOM VA2 から IP アドレスの引き継ぎ有無で、構築手順や切り替え手順が異なります。

5-1 シングル構成の構築手順例・運用切り替え手順例

IP アドレス引継		構成手順例	運用切り替え方式例
物理	仮想		
無	有	VA2 を停止せずに VE2m を構築する。 1. VA2 と異なる新規の IP 体系で VE2m を構築 2. テストを実施 ・新規の仮想 IP/物理 IP アドレスによる疎通確認	VA2 の仮想 IP アドレスに変更して、VE2m に運用を切り替える。 1. VE2m の ACT の config を VA2 の仮想 IP アドレスに変更。(commit しない) 2 VA2 を停止 3. VE2m を commit。 想定サービス中断時間： commit 反映：30 秒程度 バックアウト方法： 全 VE2m 停止後、VA2 を起動
無	無	同上	対向先サーバ、仮想ルータに対して、VE2m の IP アドレスに置き換えて切り替える。 1. 対向サーバで VA2 へのルーティング設定がある場合、VE2m へのルーティングに変更 2. VA2 で FIP を使用している場合、関連付けを解除し、VE2m のダミーポートに関連付けする。 3. 仮想ルータに FW やルーティング設定がある場合、VE2m 用の IP 体系に変更 4. VA2 を停止 想定サービス中断時間： 対向サーバの設定：1 つの対向サーバごとに 30 秒程度 仮想ルータの更新：1 秒程度 FIP の通信　　：5 秒程度 バックアウト方法： 全 VE2m 停止後、VA2 を起動 上記の「1.」、「2.」、「3.」の変更を元に戻す。

有	有	VA2 を停止して VE2m を構築する。 1. VA2 を停止 2. VA2 の IaaS のポートを順にデタッチ 3. VA2 と同じ IP 体系で VE2m を構築 ※2.のポートを指定して、VE2m の仮想サーバを作成 4. テストを実施 ・仮想 IP アドレスによる疎通確認 5. VA2 の仮想サーバを削除	左記手順を実施する。 想定サービス中断時間： VE2m の構築： 1 時間程度 バックアウト方法： できません。

FUJITSU Hybrid IT Service FJcloud-O IaaS
IPCOM VE2m 移行ガイド 1.0 版

発行日 2020 年 6 月

●本書の内容は、改善のため事前連絡なしに変更することがあります。

●本書の無断複製・転載を禁じます。