別表 ［ＦＥＮＩＣＳビジネスマルチレイヤーコネクト（タイプＫＯ） サイトセキュリティ］

１．ネットワークサービスの提供
当社（以下「乙」という）は、ネットワークサービスの利用者（以下「甲」という）に対し、第４項記載のネットワークサービス（以下「本ネットワークサービス」という）を提供します。

２．ネットワークサービスの概要
本ネットワークサービスは、ファイアーウォール装置をＦＥＮＩＣＳネットワーク用電気通信回線に接続し、甲専用の閉域ネットワーク（以下「コアネットワーク」という）からインターネットへ接続するにあたり各種セキュリティ機能を利用できるようにするネットワークサービスです。

ＦＥＮＩＣＳビジネスマルチレイヤーコネクト（タイプＫＯ） サイトセキュリティ
└基本サービス
｜　└初期サービス
｜　└利用サービス
｜　└セッション追加サービス
└オプションサービス
｜　└グローバルＩＰ追加サービス
｜　└アナライズオプションサービス
｜　└脅威レポートサービス
｜　└脅威ログオプションサービス
｜　└設定変更サービス
｜　└ユーザカスタマイズオプションサービス
｜　└振る舞い検知オプション
｜　└クラウドメールセキュリティ
└ドメインサービス
｜　└ドメイン取得代行サービス
｜　└ドメイン登録サービス
｜　└ドメイン管理サービス
｜　└ドメイン設定内容変更サービス
└ＤＮＳサービス
　└プライマリＤＮＳ＆セカンダリＤＮＳサービス
　└セカンダリＤＮＳサービス

３．ネットワークサービス提供の前提条件
本ネットワークサービスの提供にあたり、別途甲と乙の間において「ＦＥＮＩＣＳビジネスマルチレイヤーコネクト（タイプＫＯ） 基本サービス」のネットワークサービスの提供に関する契約がなされているものとします。また、あわせて、「ＦＥＮＩＣＳビジネスマルチレイヤーコネクト（タイプＫＯ） 基本サービス」にてＬ２ネットワークの提供に関する契約がなされている場合は「ＩＰ接続ＧＷ３」の契約が別途必要となります。

４．ネットワークサービスの内容
（１）基本サービス
ａ．初期サービス
乙は、甲が本ネットワークサービスを利用できるよう、ＦＥＮＩＣＳネットワークサービス用電気通信回線、ＦＥＮＩＣＳネットワークサービス用電気通信設備およびファイアーウォール装置に対して所定の準備作業を実施します。
ｂ．利用サービス
乙は甲に対し、コアネットワークからインターネットに接続するにあたり、以下の機能を継続して提供します。なお、以下の機能を提供するＦＥＮＩＣＳネットワークサービス用電気通信設備に対してコアネットワークから同時に接続できる数（以下「セッション数」という）は、２５０００とします。
ア．ファイアーウォール機能
通信先のＩＰアドレスやポート番号で通信制御を行う機能。なお、ファイアーウォールによる制限の対象となる通信は、甲が設定するものとします。
イ．アプリケーション制御
ＦＥＮＩＣＳネットワークサービス用電気通信設備を通過する通信を分析することにより当該通信を発生させたアプリケーション(ただし乙所定のアプリケーション検出データベースに登録されているアプリケーションに限る)を検出して通信制御を行う機能。なお、アプリケーション制御による制限の対象となる通信は、甲が設定するものとします。
ウ．アンチウイルス
インターネット接続において、乙のウイルス検出データベースに基づき、ウイルスの侵入を予防する機能。ただし、当該機能は、甲が設定し、有効にした場合のみ機能提供されるものとします。また、甲はウイルス検出データベースが随時乙の判断により追加・削除されることがあることを了承するものとします。
エ．アンチスパイウェア
インターネット接続において、乙のスパイウェア検出データベースに基づき、スパイウェアの侵入を予防する機能。ただし、当該機能は、甲が設定し、有効にした場合のみ機能提供されるものとします。また、甲はスパイウェア検出データベースが随時乙の判断により追加・削除されることがあることを了承するものとします。
オ．脆弱性防御
インターネット接続において、乙の脆弱性検出データベースに基づき、脆弱性攻撃を予防する機能。ただし、当該機能は、甲が設定し、有効にした場合のみ機能提供されるものとします。また、甲は脆弱性検出データベースが随時乙の判断により追加・削除されることがあることを了承するものとします。
カ．ＵＲＬフィルタリング
インターネット上のＷｅｂページ（乙が把握しているものに限る）のうち、甲が指定したカテゴリおよびＷｅｂページの閲覧を制限する事ができる機能。甲は、本機能で提供されるカテゴリ（乙が所定のカテゴリに属すると判断するインターネット上のＷｅｂページの一覧から構成される）が随時乙の判断により追加・削除されることがあることを了承するものとします。なお、制限となるカテゴリおよびＷｅｂページは、甲が設定するものとします。
キ．ファイルブロッキング
乙のファイル種別検出データベースに基づき、ＦＥＮＩＣＳネットワークサービス用電気通信設備を通過するファイルのアップロードやダウンロード通信の通信制御を行う機能。また、甲はファイル種別検出データベースが随時乙の判断により追加・削除されることがあることを了承するものとします。なお、制限の対象となるファイルは、甲が設定するものとします。
ク．脅威アラート通報
ＦＥＮＩＣＳネットワークサービス用電気通信設備を２４時間３６５日監視し、検出したセキュリティインシデントを乙が定めた条件に従い、甲へ電子メールで通報する機能。なお当該機能の利用については、甲が設定するものとします。

（２）セッション追加サービス
乙は、基本サービスにおけるセッション数を、以下のとおり追加するものとします。
ａ．セッション追加　利用料　２５０００
セッション数を２５０００追加するものとします。
ｂ．セッション追加　利用料　５００００
セッション数を５００００追加するものとします。
ｃ．セッション追加　利用料　７５０００
セッション数を７５０００追加するものとします。

（３）グローバルＩＰ追加サービス
ａ．初期サービス
乙は、甲が本ネットワークサービスを利用できるよう、ＦＥＮＩＣＳネットワークサービス用電気通信回線、ＦＥＮＩＣＳネットワークサービス用電気通信設備およびファイアーウォール装置に対して所定の準備作業を実施します。
ｂ．利用サービス
乙は甲に対し、インターネットから、コアネットワーク内の特定のコンピュータへ接続するために必要となるグローバルＩＰアドレスを提供します。

（４）アナライズオプションサービス
ａ．初期サービス
乙は、甲が本ネットワークサービスを利用できるよう、ＦＥＮＩＣＳネットワークサービス用電気通信回線、ＦＥＮＩＣＳネットワークサービス用電気通信設備およびファイアーウォール装置に対して所定の準備作業を実施します。
ｂ．利用サービス
乙は甲に対し、ＦＥＮＩＣＳネットワークサービス用電気通信設備を通過するファイルを乙所定のファイルのうち、乙所定の条件に合致するものを分析し、当該ファイルがファイル分析装置によってマルウェア（不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称）であると乙所定の基準にて判定された場合は、Ｅ－ｍａｉｌにて甲へ通報します。また、乙は、当該ファイルを分析する時、日本国内および米国の乙所定のデータセンターに設置したファイル分析装置へファイルを転送します。転送されたファイルは、データを匿名化した上で、分析／統計の目的のため使用する、または、サードパーティのセキュリティ関連の研究者、ベンダーや顧客とサンプルデータとして共有する場合があります。本オプションサービスを有効にした時点で、甲はファイル分析装置への当該ファイルの転送を承諾し、転送されたファイルについては一切の権利を行使しないものとします。

（５）脅威レポートサービス
ａ．初期サービス
乙は、本ネットワークサービスを提供するにあたり、所定の準備作業を実施します。
ｂ．利用サービス
乙は甲に対し、毎週１回、ＦＥＮＩＣＳネットワークサービス用電気通信設備で検出したセキュリティインシデントに関するレポートを作成し、乙のＷｅｂサイトに掲載します。

（６）脅威ログオプションサービス
ａ．初期サービス
乙は、甲が本ネットワークサービスを利用できるよう、ＦＥＮＩＣＳネットワークサービス用電気通信回線およびＦＥＮＩＣＳネットワークサービス用電気通信設備に対して所定の準備作業を実施します。
ｂ．利用サービス
乙は甲に対し、ＦＥＮＩＣＳネットワークサービス用電気通信設備で検出したセキュリティインシデントに関するログをファイアーウォール装置から抽出、成型し、乙のＷｅｂサイトに掲載します。アプリケーション制御機能により生成された通信量のログを月に１回、アンチウイルス、アンチスパイウェア、脆弱性防御、ＵＲＬフィルタリング、およびアナライズオプションサービスにより生成されたログを毎週１回の頻度で乙のＷｅｂサイトに掲載します。
アナライズオプションサービスにより生成されたログの提供については、アナライズオプションサービスの契約を前提とします。
ただし、乙は脅威ログオプションサービスの内容及び実施結果について、その完全性、正確性、確実性又は有用性等につき、いかなる保証も行わないものとし、脅威ログオプションサービスの利用により生じた結果に対する損害賠償その他何らの責任も負いません。

（７）設定変更サービス
乙は、甲からの本ネットワークサービスに関する設定変更指示に従い、ファイアーウォール装置の設定変更を行います。

（８）ユーザカスタマイズオプションサービス
甲管理者は、乙が提供する管理者ＩＤおよびパスワードを利用し、インターネットブラウザ上の画面（以下「管理者向け画面」という）で４．（１）ｂ．ア～キに記載する機能の変更を実施することができます。ただし、ウ、エ、オ、キについては当該機能の有効・無効のみ変更できるものとします。

（９）振る舞い検知オプション
ａ．初期サービス
乙は、甲が本ネットワークサービスを利用できるよう、ＦＥＮＩＣＳネットワークサービス用電気通信回線およびＦＥＮＩＣＳネットワークサービス用電気通信設備に対して所定の準備作業を実施します。
ｂ．利用サービス
乙は、ＦＥＮＩＣＳネットワークサービス用電気通信設備を通過する甲が別途指定するＩＰアドレスの通信に、乙所定の条件に合致するものを分析し、当該通信が脅威解析センサによってボットネット（悪意ある攻撃者によりコンピューターウイルスの一種を送り込まれるネットワークの総称）について乙の基準にて判定された場合は、分析結果および簡易対処案について乙の監視センタより甲へ通報するものとします。
なお、本オプションはサイトセキュリティサービスを利用する甲の１０００端末を分析可能とし、別途契約により１０００端末単位で最大６０００端末まで分析が可能なものとします。
また、乙は、日本国内の乙所定のデータセンターに設置した脅威センサの分析結果を乙の監視センタへ転送します。本オプションサービスを有効にした時点で、甲は脅威センサからの分析結果の転送を承諾し、転送された結果については一切の権利を行使しないものとします。
ア．端末追加利用料　１０００
利用サービスに対して、解析可能となる端末数をさらに１０００追加するものとします。ただし、解析可能な端末は最大６０００端末までとします。
イ．端末追加利用料　３０００
利用サービスに対して、解析可能となる端末数をさらに３０００追加するものとします。ただし、解析可能な端末は最大６０００端末までとします。
ウ．端末追加利用料　５０００
利用サービスに対して、解析可能となる端末数をさらに５０００追加するものとします。ただし、解析可能な端末は最大６０００端末までとします。

（１０）クラウドメールセキュリティ
ａ．初期サービス
乙は甲に対し、初期サービスとして以下のサービスを提供します。
ア．サービス機能設定
乙は、甲が利用サービスを利用できるよう、乙のネットワークサービス用電気通信設備に乙所定の設定を行います。
イ．甲管理者ＩＤおよびパスワードの発行
乙は、甲において本ネットワークサービスの管理を行う者（以下「甲管理者」という）のＩＤ（以下「管理者ＩＤ」という）およびパスワードを甲に通知します。
ｂ．利用サービス
乙は甲に対し、甲が利用するメールシステムについて、社内外から送信されるメールについて、スパムメール（無差別かつ大量に一括して送信される迷惑メールの総称）およびセキュリティ脅威をブロックし、不慮による、または意図的なデータの漏えいを防止するために以下の機能を継続的に利用できる環境を提供します。
ア．管理者向け機能
甲管理者は、乙が提供する管理者ＩＤおよびパスワードを利用し、乙が動作環境として別途指定するインターネットブラウザソフトウェア上の画面（以下「管理者向け画面」という）で以下の機能を利用することができます。
・モニタリング機能
甲が利用するメールシステムの送受信メールの詳細、各機能の遮断情報を閲覧する機能。
・設定変更機能
甲管理者が各機能の設定変更を実施する機能。
イ．ＩＰレピュテーションフィルタ機能
乙のＩＰアドレス別スコア情報に基づき、スパムメールの侵入を予防する機能。なお、甲はＩＰアドレス別スコア情報が随時乙の判断により追加・削除されることがあることを了承するものとします。

ウ．アンチスパム機能
　乙の脅威情報データベースに基づき、スパムメールの侵入を予防する機能。ただし、当該機能は甲が設定し、有効にした場合のみ機能提供されるものとします。なお、甲は脅威情報データベースが随時乙の判断により追加・削除されることがあることを了承するものとします。
エ．アンチウイルス機能
　乙のアンチウイルスエンジンに基づき、ウイルスを含むファイルの検査を行い、検知／遮断する機能。ただし、当該機能は甲が設定し、有効にした場合のみ機能提供されるものとします。なお、甲はアンチウイルスエンジンが随時乙の判断により追加・削除されることがあることを了承するものとします。
オ．アドバンスドマルウェアプロテクション機能
　以下の機能を提供します。ただし、当該機能は、甲が設定し、有効にした場合のみ機能適用されるものとします。
・ファイルレピュテーション機能
　乙のファイル格付け情報に基づき、メールに添付された悪意のあるファイルを排除する機能。なお、甲はファイル格付け情報が随時乙の判断により追加・削除されることがあることを了承するものとします。
・サンドボックス機能
　乙は甲に対し、ネットワークサービス用電気通信設備を通過する甲所定のファイルのうち、乙所定の条件に合致するものを分析し、当該ファイルがファイル分析装置によってマルウェアであると乙所定の基準にて判定された場合は、管理者画面にて甲へ通報します。また乙は、当該ファイルを分析する時、日本国内または海外の乙所定のデータセンターに設置したファイル分析装置へファイルを転送します。転送された当該ファイルは、データを匿名化した上で、分析／統計の目的のため使用する、または、サードパーティのセキュリティ関連の研究者、ベンダーおよび顧客のサンプルデータとして共有する場合があります。甲はファイル分析装置への当該ファイルの転送を承諾し、転送された当該ファイルについては一切の権利を行使しないものとします。
カ．コンテンツフィルタ機能
　メールの内容を監視し、甲が設定したポリシーに応じた処理を適用する機能。ただし、当該機能は、甲が設定し、有効にした場合のみ機能提供されるものとします。また、適用する処理内容は、甲が設定するものとします。
キ．アウトブレイクフィルタ機能
　メール添付ファイル内の新種マルウェアの拡散を防止し、また不正なＵＲＬへの安全なリンク接続を提供する機能。ただし、当該機能は、甲が設定し、有効にした場合のみ機能提供されるものとします。
ｃ．サービスの停止
　乙は、都合により（１０）に定める本クラウドメールセキュリティサービスの一部または全部を停止することがあり、甲はこれを了承するものとします。その場合、乙はその旨および停止日をすみやかに書面をもって甲に通知するものとします。
ｄ．利用ポリシー
　甲は、本クラウドメールセキュリティサービスを利用する際、他の条項に加え、最新のCisco Cloud Services Acceptable Use Policy(AUP)（https://www.cisco.com/c/en/us/about/legal/end-user-license-and-cloud-terms/cloud-services-acceptable-use-policy.html）を遵守するものとします。

（１１）ドメイン取得代行サービス
　乙は、甲に代わって株式会社日本レジストリサービス（以下「ＪＰＲＳ」という）から属性型・地域型ドメイン、末尾が「．ｃｏｍ」、「．ｎｅｔ」、「．ｏｒｇ」、「．ｂｉｚ」、「．ｉｎｆｏ」、「．ｍｏｂｉ」、もしくは「．ａｓｉａ」のドメイン（以下「ｇＴＬＤドメイン」という）、末尾が「．ｃｃ」もしくは「．ｔｖ」のドメイン（以下「特定ｃｃＴＬＤドメイン」という）、または汎用ＪＰドメインを取得するための手続きを行います。なお、ドメイン取得代行サービスの利用にあたっては、ドメイン登録サービスおよびドメイン管理サービスの契約が別途必要となります。

（１２）ドメイン登録サービス
　乙は、ドメイン取得代行サービスにて甲のために取得した属性型・地域型ドメイン、ｇＴＬＤドメイン、特定ｃｃＴＬＤドメイン、もしくは汎用ＪＰドメイン、または甲が自己の責任と費用負担にて取得した属性型・地域型ドメイン、ｇＴＬＤドメイン、特定ｃｃＴＬＤドメイン、もしくは汎用ＪＰドメインをＪＰＲＳに登録します。なお、ドメイン登録サービスの利用にあたっては、ドメイン管理サービスの契約が別途必要となります。

（１３）ドメイン管理サービス
　乙は、ドメイン登録サービスにて甲のために登録したドメインを管理します。

（１４）ドメイン設定内容変更サービス
　乙は、ドメイン登録サービスにて甲のために登録したドメイン情報の設定変更を行います。

（１５）プライマリＤＮＳ＆セカンダリＤＮＳサービス
ａ．初期サービス
　乙は、プライマリＤＮＳ＆セカンダリＤＮＳ利用サービスを利用するために必要な所定の準備作業を実施します。
ｂ．利用サービス
　乙は、甲が甲のドメインを利用するためのプライマリＤＮＳおよびセカンダリＤＮＳを継続して提供するものとします。
ｃ．設定変更サービス
　乙は、甲が甲のドメインを利用するためのプライマリＤＮＳおよびセカンダリＤＮＳの設定変更を行います。

（１６）セカンダリＤＮＳサービス
ａ．初期サービス
　乙は、セカンダリＤＮＳ利用サービスを利用するために必要な所定の準備作業を実施します。
ｂ．利用サービス
　乙は、甲が甲のドメインを利用するためのセカンダリＤＮＳを継続して提供するものとします。
ｃ．設定変更サービス
　乙は、甲が甲のドメインを利用するためのセカンダリＤＮＳの設定変更を行います。

５．提供区域
　本ネットワークサービスの提供区域は、回線サービスの提供区域に準ずるものとします。

６．利用サービス提供時間帯
　本ネットワークサービスにおける利用サービスの提供時間帯は、２４時間３６５日とします。ただし、利用規約に基づき、乙は利用サービスの提供を中断することができるものとします。

７．利用サービス障害受付時間帯
　本ネットワークサービスにおける利用サービスの障害受付時間帯は、２４時間３６５日とします。ただし、アクセス回線の障害受付時間帯は、乙が当該ネットワークサービスの提供をうけている他の電気通信事業者、またはその他のアクセス回線提供者の障害受付時間帯に準ずるものとします。

８．利用サービス障害対応時間帯
　本ネットワークサービスにおける利用サービスの障害対応時間帯は、２４時間３６５日とします。ただし、アクセス回線の障害対応時間帯は、乙が当該ネットワークサービスの提供をうけている他の電気通信事業者、またはその他のアクセス回線提供者の障害対応時間帯に準ずるものとします。ただし、振る舞い検知オプションの障害対応時間帯は、月曜日から金曜日（祝日および乙の指定する休業日を除く）の９時から１７時とします。

９．従量月額払利用料金の算出
　本ネットワークサービスにおける従量月額払利用料金は、利用規約第８条第３項（２）の規定にかかわらず、サービス実施開始日およびサービス実施期間中における毎料金月の２１日に発生するものとします。

１０．留意事項

（１）甲は、本ネットワークサービスにおいて提供されるセキュリティ強化機能、防御機能および検知機能が、セキュリティリスクに繋がる全事象から完全に保護されるものでないことを了承するものとします。

（２）振る舞い検知プションにより乙より通報されるのは脅威への簡易対処案であり、脅威への対処は甲が自らの責任で実施するものとします。

（３）ネットワークサービス条項第７条第２項（６）として、次の内容を加えるものとします。
　乙がネットワークサービスの実施の過程で得た情報の集計および分析を行い、統計資料を作成し、ネットワークサービス、乙の環境ならびに乙の製品およびサービスの安全性向上等のために限定して利用および処理する場合

（４）ネットワークサービス条項第７条第２項（７）として、次の内容を加えるものとします。
　乙がネットワークサービスの実施の過程で分析した情報を、当該情報が甲の情報であることが識別できないように加工したうえで、情報セキュリティの研究、開発、改善、啓蒙またはその他の目的のために、利用および公表する場合

１１．品目一覧

本ネットワークサービスにおける品目は、以下の通りとします。

品名	型名	備考	支払種別	単位
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　基本サービス　初期費	ＮＳ２８４５０ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　基本サービス　利用料	ＮＳ２８４５０ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　グローバルＩＰ追加　初期費	ＮＳ２８４５１ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　グローバルＩＰ追加　利用料	ＮＳ２８４５１ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　アナライズオプション　初期費	ＮＳ２８４５２ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　アナライズオプション　利用料	ＮＳ２８４５２ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　脅威レポート　初期費	ＮＳ２８４５３ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　脅威レポート　利用料	ＮＳ２８４５３ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　脅威ログオプション　初期費	ＮＳ２８４６３ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　脅威ログオプション　利用料	ＮＳ２８４６３ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　設定変更費	ＮＳ２８４５４ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　ドメイン取得代行サービス　初期費	ＮＳ２８４５５ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　ドメイン登録サービス　初期費	ＮＳ２８４５６ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　ドメイン管理サービス　利用料	ＮＳ２８４５６ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　ドメイン管理サービス　設定変更費	ＮＳ２８４５７ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　プライマリＤＮＳ＆セカンダリＤＮＳサービス　初期費	ＮＳ２８４５８ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　プライマリＤＮＳ＆セカンダリＤＮＳサービス　利用料	ＮＳ２８４５８ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　プライマリＤＮＳ＆セカンダリＤＮＳ　設定変更費	ＮＳ２８４５９ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　セカンダリＤＮＳサービス　初期費	ＮＳ２８４６０ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　セカンダリＤＮＳサービス　利用料	ＮＳ２８４６０ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　セカンダリＤＮＳサービス　設定変更費	ＮＳ２８４６１ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫＯ）　サイトセキュリティ　ユーザカスタマイズオプション　利用料	ＮＳ２８４７４ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　振る舞い検知オプション　初期費	ＮＳ２８４６５ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　振る舞い検知オプション　利用料	ＮＳ２８４６５ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　振る舞い検知オプション　端末追加利用料　１０００	ＮＳ２８４６６ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　振る舞い検知オプション　端末追加利用料　３０００	ＮＳ２８４６７ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　振る舞い検知オプション　端末追加利用料　５０００	ＮＳ２８４６８ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　振る舞い検知オプション　月次レポート　利用料	ＮＳ２８４６９ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　セッション追加　利用料　２５０００	ＮＳ２８４７１ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　セッション追加　利用料　５００００	ＮＳ２８４７２ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　セッション追加　利用料　７５０００	ＮＳ２８４７３ＫＧ		従量料金制（月額払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　クラウドメールセキュリティ　初期費	ＮＳ２８４７０ＫＳ		従量料金制（一括払）	式
ＢＭＬＣ（タイプＫ）　サイトセキュリティ　クラウドメールセキュリティ　利用料	ＮＳ２８４７０ＫＧ		従量料金制（従量払）	ＩＤ

［変更内容］
（２０１５年３月３０日）本別表を適用します。
（２０１７年９月５日）セッション追加サービスおよび振る舞い検知オプションを追加しました。
（２０１７年９月２９日）クラウドメールセキュリティを追加しました。
（２０１８年１月３１日）脅威ログオプションサービスを追加しました。
（２０１８年３月１４日）ユーザカスタマイズオプションを追加しました。
（２０１９年１２月１７日）品名一覧の型名の誤記を修正しました。

［凡例］
本別表では、以下の略称を用いています。

略　称	名　称
ＩＰ	Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ
ＶＰＮ	Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ
ＵＲＬ	Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ

以　上