FJcloud-V IDS サービス

仕様書

第 1.4 版　2024 年 10 月 1 日

富士通株式会社

改訂履歴

版数	改訂日	改訂内容
1.0	2019 年 4 月 10 日	初版作成。
1.1	2020 年 6 月 15 日	5.1 利用料金の料金金額単位を修正
1.2	2020 年 9 月 23 日	お問い合わせ先を修正
1.3	2021 年 3 月 24 日	5.1 利用料金の料金金額を税込み価格に修正
1.4	2024 年 10 月 1 日	社名の変更 5.1 利用料金の料金金額を修正 5.2 利用料金の例の金額修正

１．サービス概要

IDS サービスでは、FJcloud-V 上のお客様のサーバーへの様々な不正アクセスや、サーバーに仕掛けられた悪意のあるプログラム（トロイの木馬、バックドア等）の発する情報を、24 時間 365 日昼夜を問わずネットワーク監視し、危険度の高いと思われる不正アクセスについては緊急報告書にて即座にお客様に報告をします。また、収集された不正アクセスの情報は、日次報告書や月次報告書でも定期的に報告をします。

監視業務の一部はセコムトラストシステムズ株式会社にて運営しています。

２．不正アクセスの検知について

2.1 ポリシーについて

不正アクセスの検知基準（ポリシー）は、デフォルトポリシーとカスタムポリシーから選択できます。なお、不正アクセスの手法は日々新しいものが発生しており、それに対応するためのポリシーのアップデートが適宜行われます。

■デフォルトポリシー
お客様のサーバー構成によらず富士通が設定した一律のポリシーを適用します。
Windows 用と Linux 用があります。

■カスタムポリシー（オプション）
お客様のサーバー構成に応じて最適なポリシーをチューニングして適用します。
カスタムポリシーのチューニングを行うために、監視対象サーバーの公開ポート番号やアプリケーションの情報（名称やバージョンなど）を富士通に連絡していただく必要があります。
チューニングしたポリシーの内容は、不正アクセスの重要度(※1)が「High」として報告されるものに限り、サービス開始時にお客様に通知いたします。

※1 不正アクセスの重要度につきましては「3.1 不正アクセスを検知した場合の対応」をご参照ください。

【注意】
サーバーを複数台作成していても、適用できるポリシーの数は 1ID につき 1 ポリシーのみとなります。

2.2 ポリシーの分類

■Windows 用ポリシー

（1）バックドア
各種ホストに対して行われるリモート制御を狙ったバックドアと想定される攻撃を検知します。

（2）BOT
ボットが行う通信（外部 IRC サーバへの接続等）を検出します。

（3）DoS/DDoS
ネットワーク内のホスト、または、通信相手のホストに DDoS 型攻撃ツールがインストールされ、DDoS 攻撃を実行している、または実行されている事を検知します。

（4）DNS
DNS サーバーに対して行われる不正アクセスを検出します。

（5）FTP
FTP サービスに対して行われる不正アクセスを検出します。

（6）HTTP
WEB サーバアプリケーションに対して行われる不正アクセスを検出します。

（7）SMTP・POP3
ご利用中の SMTP・POP3 サーバーに対して行われる不正アクセスを検出します。

（8）TELNET・SSH
TELNET・SSH に関連した攻撃を検知いたします。

（9）Adobe 製品
Adobe 製品の脆弱性を悪用する攻撃を検知します。

（10）Java
Oracle Java の脆弱性を悪用する攻撃を検知します。

（11）データベース
データベースとして利用されるアプリケーションに対する攻撃を検知します。

（12）Microsoft 製品

Microsoft 製品に対する攻撃を検知します。

（13）その他

上記以外の不正アクセスを検知します。

■Linux 用ポリシー

（1）バックドア

各種ホストに対して行われるリモート制御を狙ったバックドアと想定される攻撃を検知します。

（2）BOT

ボットが行う通信（外部 IRC サーバへの接続等）を検出します。

（3）DoS/DDoS

ネットワーク内のホスト、または、通信相手のホストに DDoS 型攻撃ツールがインストールされ、DDoS 攻撃を実行している、または実行されている事を検知します。

（4）DNS

DNS サーバーに対して行われる不正アクセスを検出します。

（5）FTP

FTP サービスに対して行われる不正アクセスを検出します。

（6）HTTP

WEB サーバアプリケーションに対して行われる不正アクセスを検出します。

（7）SMTP・POP3

ご利用中の SMTP・POP3 サーバーに対して行われる不正アクセスを検出します。

（8）TELNET・SSH

TELNET・SSH に関連した攻撃を検知いたします。

（9）Adobe 製品

Adobe 製品の脆弱性を悪用する攻撃を検知します。

（10）Java

Oracle Java の脆弱性を悪用する攻撃を検知します。

（11）データベース

データベースとして利用されるアプリケーションに対する攻撃を検知します。

（12）その他

上記以外の不正アクセスを検知します。

３．検知時の対応

IDS サービスでは、ネットワーク上を流れるパケットを常時監視し、不正アクセスを検知した際は、リアルタイムに富士通のサービスセンターへ自動通報を行います。
サービスセンターへ自動通報されてきた不正アクセスの情報は、セキュリティ専門の技術者が解析を行い、不正アクセスの重要度により４段階のレベル分けを行った後、そのレベルに応じた手段でお客様の担当者へ通報を行います。
なお、センサーが収集した不正アクセスの情報は、定期的に集計・加工を実施した後、
お客様へ報告書として提出いたします。

3.1 不正アクセスを検知した場合の対応

不正アクセスを検知した場合、不正アクセスの重要度を４段階にレベル分けを行い、そのレベル毎に、定める時間内にお客様へ通報いたします。

重要度の分類	内容	報告書（連絡手段）
High （即時連絡）	・権限の取得を目的とした不正アクセス（管理者権限の取得、ファイルの書込み権限の取得等） ・サービス停止攻撃（対策が不可能なもの） ・システムの脆弱性の調査を目的とした不正アクセス	・緊急報告書（Mail、電話） ・日次／月次報告書（Web レポート）
Medium （24 時間以内に連絡）	・ネットワークの調査を目的とした不正アクセス（対策が不可能なもの） ・サービス停止攻撃（対策が可能なもの）	・日次／月次報告書（Web レポート）
Low （１ヶ月以内に連絡）	・ネットワークの調査を目的とした不正アクセス（対策が可能なもの）	・月次報告書（Web レポート）
Ignore （連絡は実施しない）	・クライアントのみ影響がある不正アクセス ・デコード系・CGI 系の不正アクセス	―

お客様へ緊急連絡を行う場合の連絡先につきましては、サービス開始時にお客様に担当者を 3 名まで選任して頂き、選任して頂いた担当者様に対して緊急通報を実施いたします。

3.2 緊急通報

侵入検知センサーが、重要度「High」の不正アクセスを検知した場合、お客様の担当者に対して緊急通報を実施します。

緊急通報は、下記の通り行います。

■電子メールによる通知　（必ず実施いたします。）
お客様の担当者様全員に対して、緊急報告書を送信いたします。

■担当者への電話による通知（お客様のご要望に応じて実施いたします。）
お客様より、下記 2 通りの時間帯毎に、各担当者に対して電話連絡を行う、行わないといった指定を事前に行って頂き、その指定に基づいて、電話での連絡を実施いたします。
①平日（月～金曜日）０９：００～１８：００
②平日（月～金曜日）１８：００～０９：００
　休日（土日祝祭日）終日

3.3 緊急報告書

IDS サービスでは、侵入検知センサーで重要度「High」の不正アクセスを検知した場合、お客様に対して緊急通報を実施しておりますが、その際、どういった不正アクセスを検知したのかをご報告する為、「緊急報告書」を提出しております。

緊急報告書には以下の項目が記載されております。

（1）時刻
該当の不正アクセスを検知した時間を記載してあります。

（2）イベント名
検知した不正アクセスの名称を記載してあります。

（3）Source IP
該当の不正アクセスが、何処から仕掛けられてきたのかが記載してあります（※1）。

（4）Source Port
該当の不正アクセスが、どのサービスを使用して仕掛けられたのかが記載してあります。

（5）Destination IP
該当の不正アクセスが、どのサーバーに対して行われたのかが記載してあります。

（6）Destination Port
該当の不正アクセスが、どのサービスに対して行われたのかが記載してあります。

（7）発生回数
該当の不正アクセスが、一定時間に何回行われたのかが記載してあります。

（8）解説文
検知した不正アクセスがどのようなものなのか、また、どのように対応すればよいのかが記載してあります（※2）。

※1 不正アクセスの種類によっては、IP アドレスの偽造が可能なものがあります。その為、この Source IP が必ずしも不正アクセスを仕掛けてきた IP アドレスとは限りません。
※2 解説文に記載してある対応例は、あくまで参考です。
実際に対応を行われる場合は、お客様の責任で作業を行って下さい。

3.4 報告書サーバー

IDS サービスでは、ネットワーク上に設置したセンサーにて検知した日毎及び月毎の不正アクセスに関するイベント集計結果を日次報告書及び月次報告書として報告書サーバーにてご報告を行っております。

報告書サーバーの URL は報告書作成完了時に連絡先担当者様宛に電子メールにて送信させて頂いております。

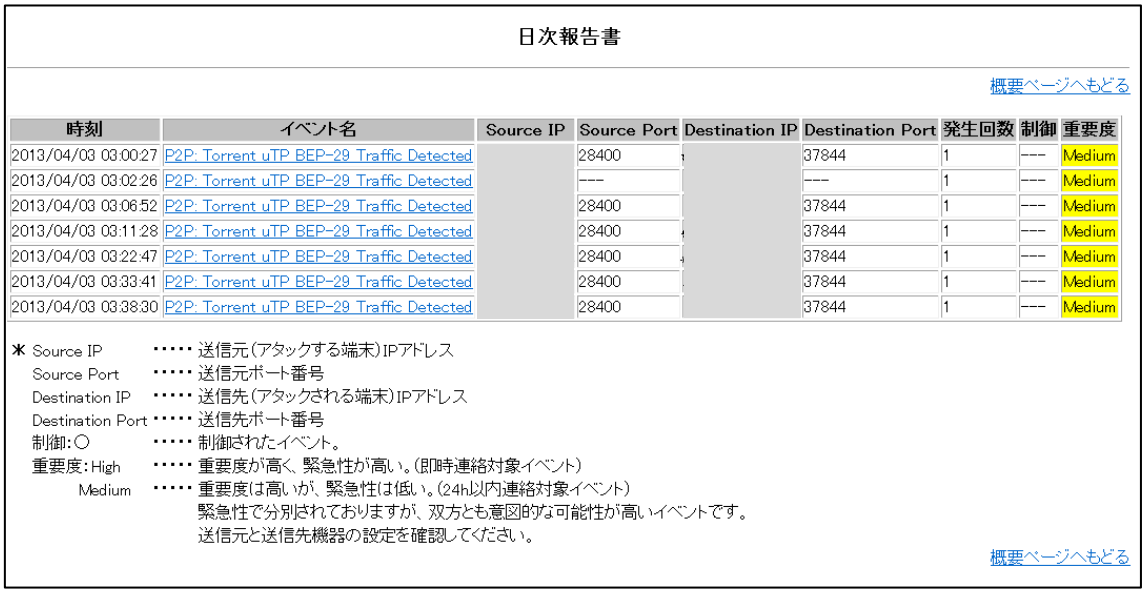
この報告書サーバーにはお客様専用の認証 ID（お客様 ID）及びパスワードを設定し、報告書の情報漏洩防止の措置を施しております。報告書の閲覧時（電子メールに記載した URL へのアクセス時）には認証 ID（お客様 ID）とパスワードを入力頂いております。

認証 ID（お客様 ID）とパスワードは、IDS サービスをお申し込み後にお客様に通知いたします。

報告書サーバー サンプル

3.5 日次報告書

日次報告書では、前日にどのような不正アクセスが、何時、何処から、何処に対して行われたのかが一目で分かるよう作成されています。
日次報告書の更新は毎日午前中に行っております。



日次報告書

概要ページへもどる

時刻	イベント名	Source IP	Source Port	Destination IP	Destination Port	発生回数	制御	重要度
2013/04/03 03:00:27	P2P: Torrent uTP BEP-29 Traffic Detected		28400		37844	1	---	Medium
2013/04/03 03:02:26	P2P: Torrent uTP BEP-29 Traffic Detected		---		---	1	---	Medium
2013/04/03 03:06:52	P2P: Torrent uTP BEP-29 Traffic Detected		28400		37844	1	---	Medium
2013/04/03 03:11:28	P2P: Torrent uTP BEP-29 Traffic Detected		28400		37844	1	---	Medium
2013/04/03 03:22:47	P2P: Torrent uTP BEP-29 Traffic Detected		28400		37844	1	---	Medium
2013/04/03 03:33:41	P2P: Torrent uTP BEP-29 Traffic Detected		28400		37844	1	---	Medium
2013/04/03 03:38:30	P2P: Torrent uTP BEP-29 Traffic Detected		28400		37844	1	---	Medium

＊ Source IP ・・・・・ 送信元(アタックする端末)IPアドレス
Source Port ・・・・・ 送信元ポート番号
Destination IP ・・・・・ 送信先(アタックされる端末)IPアドレス
Destination Port ・・・・・ 送信先ポート番号
制御:○ ・・・・・ 制御されたイベント。
重要度:High ・・・・・ 重要度が高く、緊急性が高い。(即時連絡対象イベント)
Medium ・・・・・ 重要度は高いが、緊急性は低い。(24h以内連絡対象イベント)
緊急性で分別されておりますが、双方とも意図的な可能性が高いイベントです。
送信元と送信先機器の設定を確認してください。

概要ページへもどる

日次報告書 サンプル

日次報告書には以下の項目が記載されております。

（1）時間
不正アクセスを検知した時間です。

（2）イベント名
検知した不正アクセスの名前です。各イベント名をクリックすると、該当の不正アクセスの説明が表示されます。

（3）Source IP
該当の不正アクセスが、何処から仕掛けられてきたのか記載してあります（※１）。

（4）Source Port
該当の不正アクセスが、どのサービスを使用して仕掛けられたのかが記載してあります。

（5）Destination IP
該当の不正アクセスが、どのサーバーに対して行われたのかが記載してあります。

（6）Destination Port
該当の不正アクセスが、どのサービスに対して行われたのかが記載してあります。

（7）発生回数
一定時間内に検出したイベント回数を記載しています。

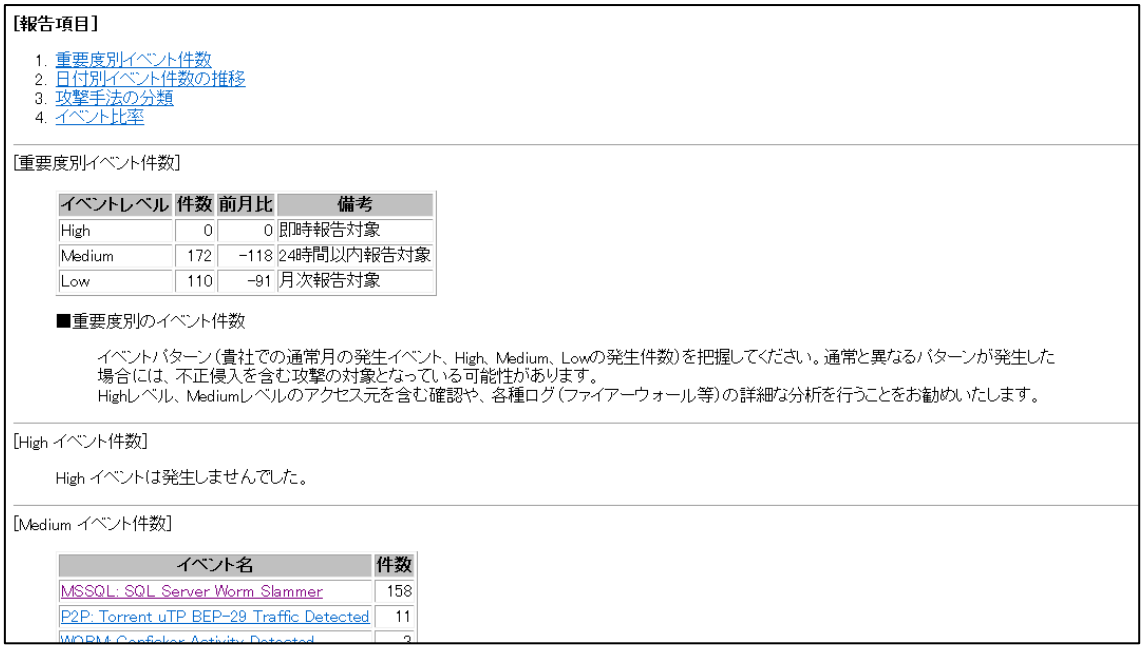
（8）制御
制御されたイベントには〇印を記載しています。

（9）重要度
イベントを重要度と緊急性の度合いにより“High”、“Medium”に分けて記載しています。

※1 不正アクセスの種類によっては、IP アドレスの偽造が可能なものがあります。その為、この Source IP が必ずしも不正アクセスを仕掛けてきた IP アドレスとは限りません。

3.6 月次報告書

月次報告書では、月間にセンサーが収集した不正アクセスの情報を集計して、表にしています。月間にどのような不正アクセスをどのくらい検出したのか、どのような不正アクセスを受けているのかが分かります。月次報告書の更新は毎月２営業日までに行っております。



[報告項目]

1. 重要度別イベント件数
2. 日付別イベント件数の推移
3. 攻撃手法の分類
4. イベント比率

[重要度別イベント件数]

イベントレベル	件数	前月比	備考
High	0	0	即時報告対象
Medium	172	-118	24時間以内報告対象
Low	110	-91	月次報告対象

■重要度別のイベント件数

イベントパターン（貴社での通常月の発生イベント、High、Medium、Lowの発生件数）を把握してください。通常と異なるパターンが発生した場合には、不正侵入を含む攻撃の対象となっている可能性があります。
Highレベル、Mediumレベルのアクセス元を含む確認や、各種ログ（ファイアーウォール等）の詳細な分析を行うことをお勧めいたします。

[High イベント件数]

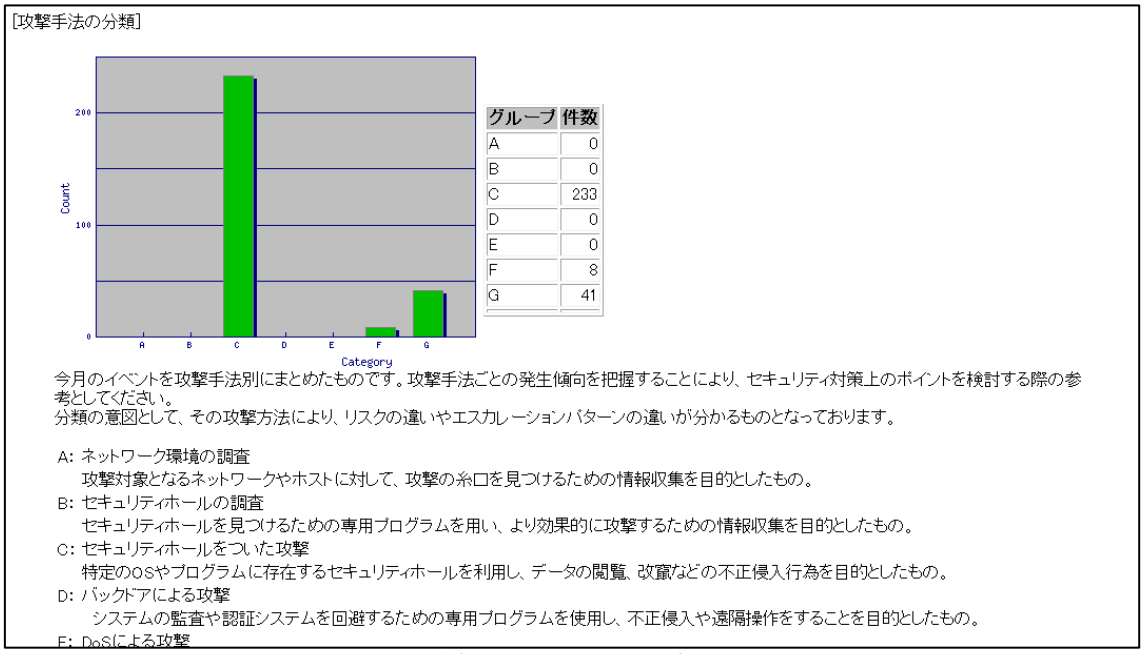
High イベントは発生しませんでした。

[Medium イベント件数]

イベント名	件数
MSSQL: SQL Server Worm Slammer	158
P2P: Torrent uTP BEP-29 Traffic Detected	11
WORM Conficker Activity Detected	3

月次報告書 サンプル

月次報告書では、１ヶ月間にセンサーが収集したイベントを攻撃手法別にまとめていますので、攻撃手法ごとの発生傾向を把握することができます。



[攻撃手法の分類]

グループ	件数
A	0
B	0
C	233
D	0
E	0
F	8
G	41

今月のイベントを攻撃手法別にまとめたものです。攻撃手法ごとの発生傾向を把握することにより、セキュリティ対策上のポイントを検討する際の参考としてください。
分類の意図として、その攻撃方法により、リスクの違いやエスカレーションパターンの違いが分かるものとなっております。

A: ネットワーク環境の調査
　攻撃対象となるネットワークやホストに対して、攻撃の糸口を見つけるための情報収集を目的としたもの。
B: セキュリティホールの調査
　セキュリティホールを見つけるための専用プログラムを用い、より効果的に攻撃するための情報収集を目的としたもの。
C: セキュリティホールをついた攻撃
　特定のOSやプログラムに存在するセキュリティホールを利用し、データの閲覧、改竄などの不正侵入行為を目的としたもの。
D: バックドアによる攻撃
　システムの監査や認証システムを回避するための専用プログラムを使用し、不正侵入や遠隔操作をすることを目的としたもの。
E: DoSによる攻撃

攻撃手法の分類 サンプル

攻撃手法毎に分類されたイベントグループに関する説明は下記の通りです。

A：ネットワーク環境の調査
攻撃対象となるネットワークやホストに対して、攻撃の糸口を見つけるための情報収集を目的としたもの。

B：セキュリティホールの調査
セキュリティホールを見つけるための専用プログラムを用い、より効果的に攻撃するための情報収集を目的としたもの。

C：セキュリティホールをついた攻撃
特定の OS やプログラムに存在するセキュリティホールを利用し、データの閲覧、改竄などの不正侵入行為を目的としたもの。

D：バックドアによる攻撃
システムの監査や認証システムを回避するための専用プログラムを私用し、不正侵入や遠隔操作をすることを目的としたもの。

E：DoS による攻撃
大量パケットの送信、または不正なパケットを送信することにより、サービスの停止を目的としたもの。

F：疑いのある動作
直接攻撃には結びつくのではないが、正常なネットワーク環境では通常発生せず、何らかの攻撃がされる可能性があるもの。

G：デコード
正常なネットワーク環境でも発生するが、何らかの攻撃や情報収集に利用可能なもの。

４．各種手続きについて

IDS サービスに関する各種手続きを行う場合は、所定の入力フォームをご利用ください。

■手続きの流れ
①入力フォームに必要事項を入力し、富士通に手続き内容を連絡。
②富士通にて内容を確認し、設定作業を実施。
③設定作業終了後、お客様に完了を連絡。

4.1 新規利用

IDS サービスのご利用を開始するには、監視対象となるサーバーの情報および不正アクセス検知の連絡先となる担当者の情報の登録が必要となります。所定の入力フォームから登録してください。登録された情報が反映されるまで 10 営業日程度かかります。

●監視対象情報

項目	記入例
OS（Windows/Linux）	Linux
IP アドレス ※ロードバランサーの IP アドレスも登録可能。	111.64.92.23
ホスト名	test1
公開ポート番号	80/tcp [HTTP]
アプリケーション情報（アプリケーション名やバージョンなど）	mysql-5.0.77-4

●担当者情報

項目	記入例
氏名	大森 太郎
会社名	富士通株式会社
部署名	営業部
連絡先メールアドレス	oomori@example.com
連絡先電話番号（昼）	03-1234-5678
連絡先電話番号（夜）	090-1234-5678

4.2 登録情報変更

登録情報に変更がある場合は、登録時と同様に所定の入力フォームからお申し込みください。変更された情報が反映されるまで 10 営業日程度かかります。

4.3 利用解除

IDS サービスのご利用を終了するには、解除希望月の登録が必要となります。所定の入力フォームから登録してください。登録後、終了処理が完了するまでに 10 営業日程度かかります。そのため、解除希望月末日の 10 営業日より前にご登録ください。

５．料金

5.1 利用料金

IDS サービスのご利用料金は下記の通りです。カスタムポリシーをご利用の場合は、オプション料金が追加されます。

●基本料金

サービス	金額(税込)
基本利用料金（1ID あたり）	214,500 円/ID/月
監視対象料金（1IP あたり）	21,450 円/IP/月

●オプション料金

サービス	金額(税込)
カスタムポリシー導入作業料金（作業 1 回あたり）	829,400 円/回
カスタムポリシー利用料金（1ID あたり）	107,250 円/ID/月

※ 開始処理完了を通知した日をサービス利用開始日とし、サービス利用開始日を含む月から利用料金が発生します。日割り計算はいたしません。

※ 終了処理完了を通知した日をサービス利用終了日とし、サービス利用終了日を含む月まで利用料金が発生します。日割り計算はいたしません。

5.2 利用料金の例

[料金例 1]　1ID／3IP／デフォルトポリシーの場合

	初月	2 ヶ月目以降
基本利用料金(税込)	214,500 円	214,500 円
監視対象料金(税込)	21,450 円 ×3	21,450 円 ×3
合計	278,850 円	278,850 円

[料金例 2]　1ID／3IP／カスタムポリシーの場合

	初月	2 ヶ月目以降
基本利用料金(税込)	214,500 円	214,500 円
監視対象料金(税込)	21,450 円 ×3	21,450 円 ×3
カスタムポリシー導入作業料金(税込)	829,400 円	－
カスタムポリシー利用料金(税込)	107,250 円	107,250 円
合計	1,215,500 円	386,100 円

６．お問い合わせ

（1）お問い合わせ先は以下の URL よりご確認ください。

https://pfs.nifcloud.com/inquiry/support.htm

（2）お問い合わせ時に必要な項目

・IPS 番号

・貴社名

なお、セキュリティの観点から、事前にご登録いただいた担当者様からのみお問い合わせを受付いたします。

７．注意事項

・IDS サービスに対応しているゾーンは、下記の通りです。

ゾーン	監視対象
east-11	○
east-12	○
east-13	○
east-14	○
その他のゾーン	×

・システムメンテナンスのためにサービスの提供を一時的に停止することがあります。
その場合はその理由および実施期間を、メールもしくはそれに類する方法にて、お客様に事前に通知します。

・ IDS サービスでは製品の特性上、DoS 攻撃のようなトラフィックの増大による攻撃を検知することはできません。

・ IDS サービスは、FJcloud-V 品質保証制度(SLA)利用規約に基づく保証の対象外です。