# JSOC マネージド・セキュリティ・サービス（MSS）

2016年1月

株式会社ラック


# JSOC (Japan Security Operation Center)

# JSOC Japan Security Operation Center

- ☑24時間365日のリアルタイムセキュリティ監視
- ☑12年以上のセキュリティ監視サービスの継続実績
- ☑契約顧客は約600社以上 （センサー数1200台以上）
- ☑セキュリティ監視機器にマルチ対応
- ☑事件・事故を救急対応した結果のフィードバック
- ☑イードアワードで監視運用部門で第一位
- ☑監視サービスメニュー
  - ☑JSOC マネージド・セキュリティ・サービス（MSS）
  - ☑JSOC 24+ （FW・IPS・UTM・WAF・NGFW）

# JSOC マネージド・セキュリティ・サービス（MSS）

## ファイアウォール監視サービス

Firewallのアクセスログをリアルタイムに分析し、ネットワークの境界で、ワーム、ボットなどの脅威を見つける、
24時間365日リアルタイム セキュリティ監視サービス

| | |
|---|---|
| cisco | ASA5500-Xシリーズ |
| JUNIPER NETWORKS | SSGシリーズ<br>SRXシリーズ |
| Check Point | VPN-1/Firewall-1<br>UTM-1シリーズ |
| paloalto NETWORKS | PAシリーズ |

## IDS監視・運用サービス

IDSの不正アクセス検知機能を利用し、ネットワーク内部で発生するあらゆる脅威を見つけ出す、
24時間365日リアルタイムのセキュリティ監視サービス

## IPS監視・運用サービス

IPSの不正アクセス検知機能と、通信遮断機能を利用して、ネットワーク内部で発生するあらゆる脅威を見つけ、危険性が高い通信を遮断する、
24時間365日リアルタイムのセキュリティ監視サービス

| | |
|---|---|
| IBM | Security Network IPS GXシリーズ |
| McAfee | Network Security Platform<br>Virtual Network Security Platform |
| cisco | ASA5500-Xシリーズ<br>IPS 4200/4300/4500 シリーズ<br>ASA with Fire POWER |
| securesoft | SniperIPS |

LAC

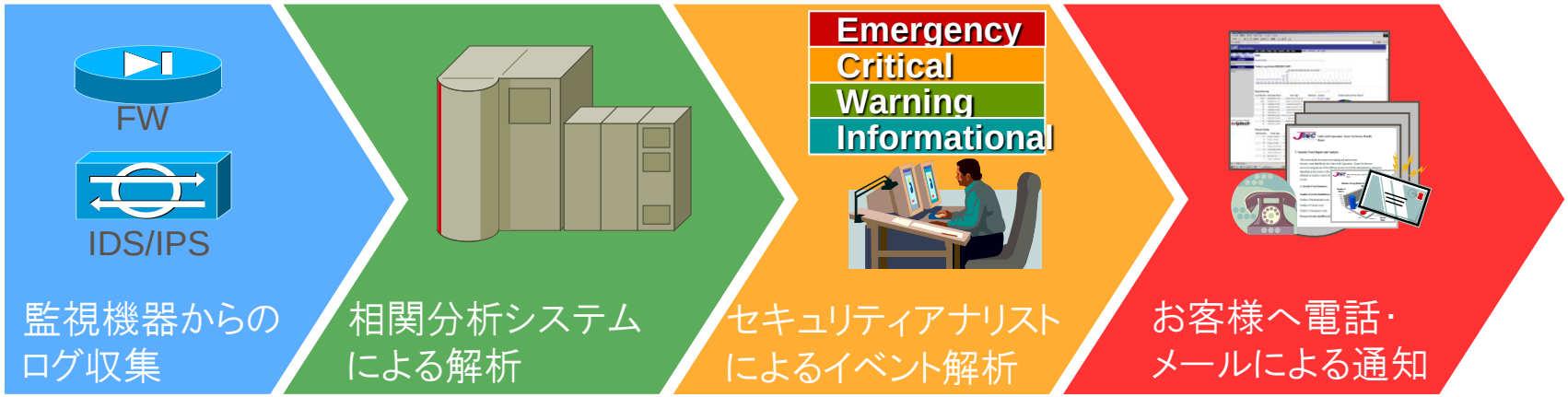
# 特長１　大量のログ対応の負荷を軽減

ログの分析結果から、高度な分析スキルを備えた**セキュリティアナリストがリアルタイムに攻撃の影響度を4段階に判定**し、本当に問題があるイベントのみをお客様へ**15分以内**でご連絡します。これにより、誤検知を含む大量のログからお客様自身が分析・判定する必要はありません。



2011年　ラック調べ

# ログ収集からお客様へ通知まで




High

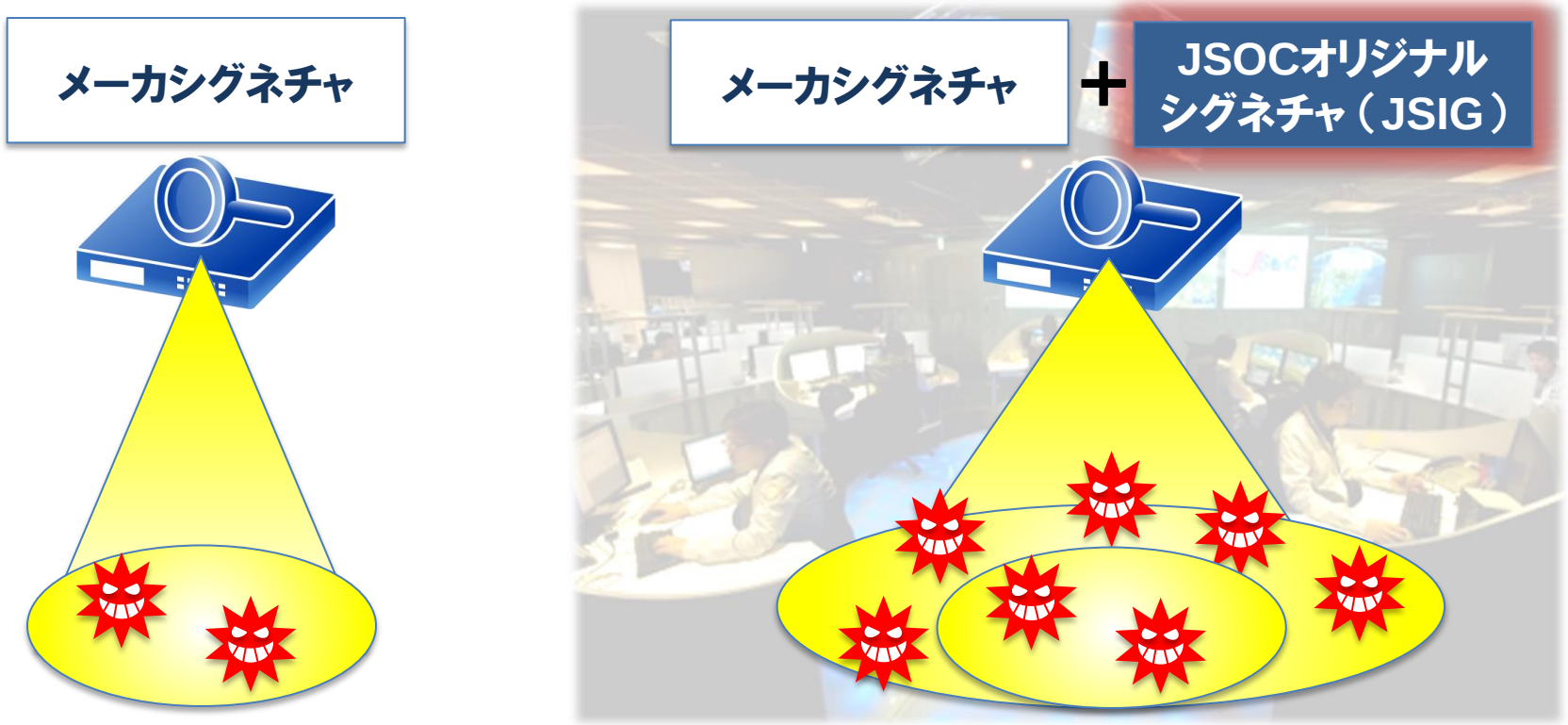
Severity

Low

| | | | |
|---|---|---|---|
| Emergency | 攻撃が成功したと判断された場合 | 即時連絡 | 15分以内、電話・メール |
| Critical | 攻撃の失敗を確認できない場合。または成功している可能性が高いと判断された場合 | | |
| Warning | 実害を狙った攻撃だが、失敗を確認している場合 | 安全宣言 | 専用WEBポータル |
| Informational | 偵察活動のような、実害のない攻撃活動を検出した場合 | | |
| 誤検知 | 通常通信もしくは誤検知と判断された場合。殆どが該当。 | | |

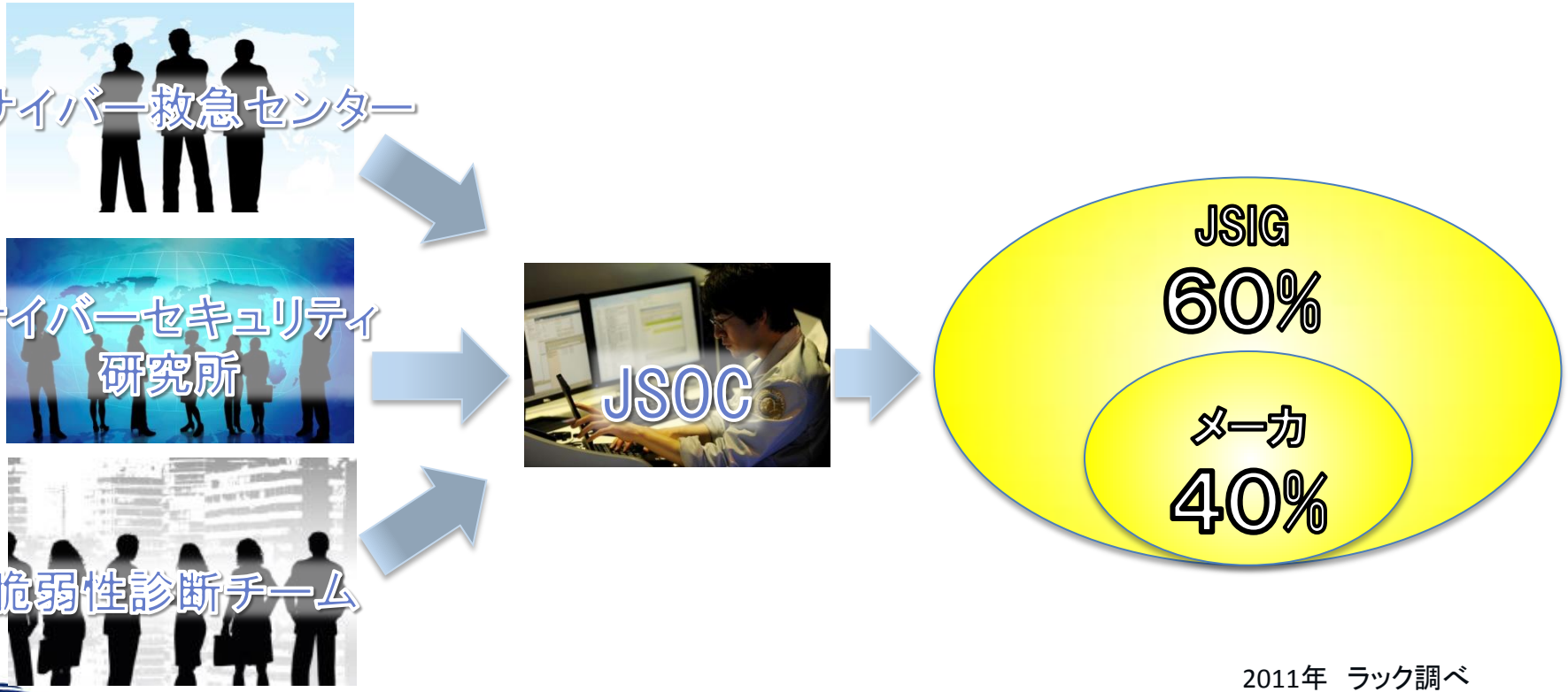
# 特長２　メーカ標準シグネチャをJSIGで補完

メーカ標準のシグネチャでは検知できない新たな脅威には、**JSOCが独自に開発したJSOCオリジナルシグネチャ（JSIG）で対応し、従来見えなかったインシデントを早期発見**、早期対応することを可能にします。



# JSIGの有効性

多数の情報セキュリティ事件・事故に対応する“サイバー救急センター”、
マルウェアやサイバー戦に熟知した“サイバーセキュリティ研究所”、
圧倒的な実績を誇る“脆弱性診断チーム”と“JSOC”は連携して、**日本固有の環境や新たな脅威が発生した際にも、迅速かつ確実にJSIGを開発しセキュリティ機器に反映**することで広範囲な検知を可能とします。




2011年　ラック調べ

# 特長3　他サービスと連携を行い安心・安全をご提供

## Critical以上のインシデントの対応事例

**セキュリティ監視サービス**

・危険度レベル
・IPアドレス
・分析結果
・対応策
・参考情報など

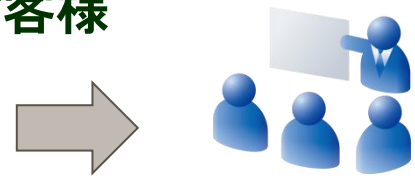
**応急対応サービス**

**救急対応サービス**


**1**　電話連絡

お客様

管理者様



社内対応チーム

**2**　リモート対応

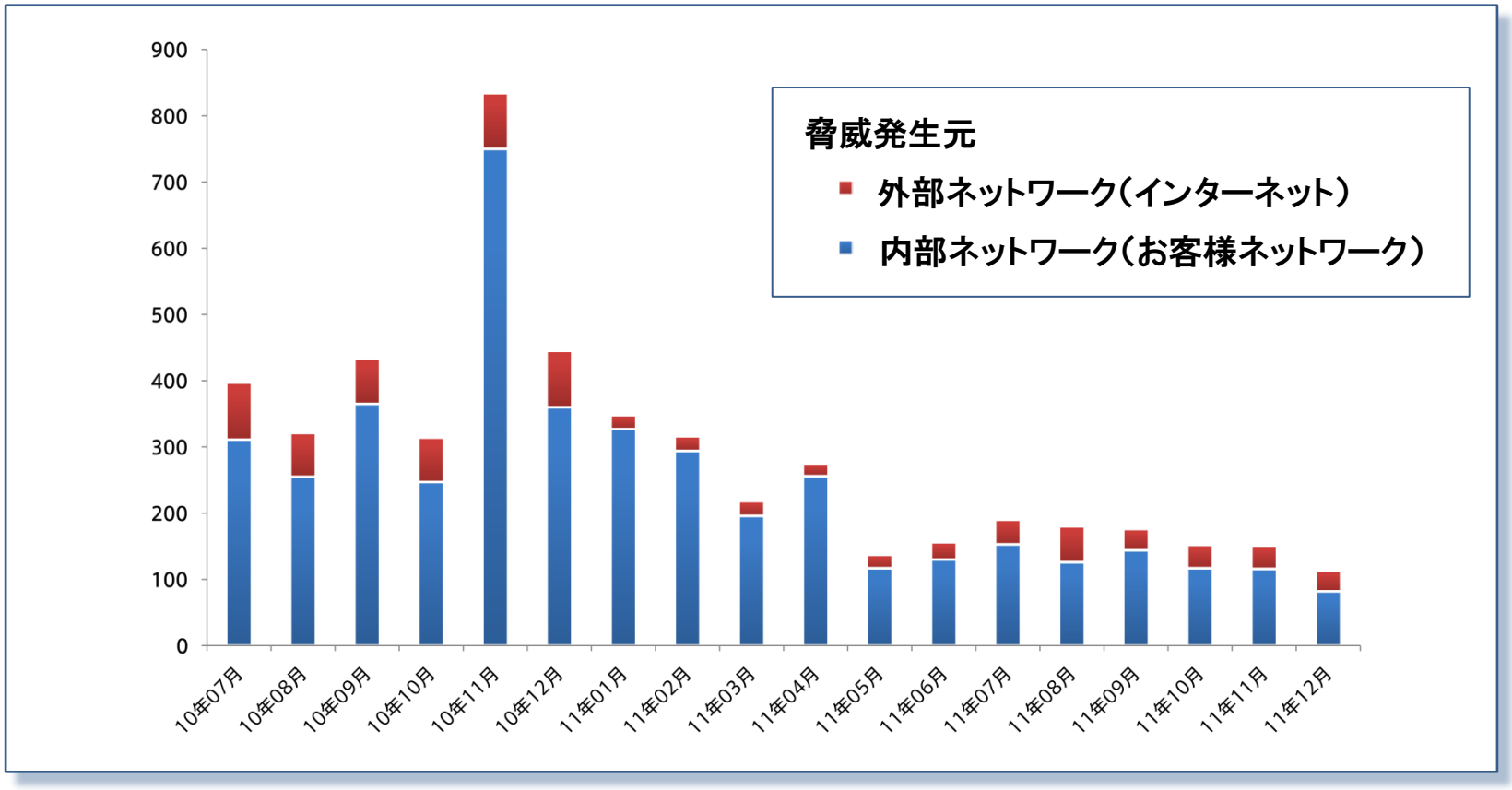
攻撃者からの通信を遮断することで、2次被害を最小限に抑えます

**3**　現地対応

初期対応、事後対策などあらゆる面で、お客様をサポートします

# JSOC侵入傾向分析レポート

下記のグラフは、JSOCが監視しているファイアウォール、IDS/IPS　1100台の分析結果、高危険度（Critical/Emergency）と判断した脅威がどこから発生したかの割合です。
以下の様に外部ネットワーク（外→内 通信）と比べ内部ネットワーク（内→外 通信）で発生する脅威が占める割合が非常に多い結果となっています。

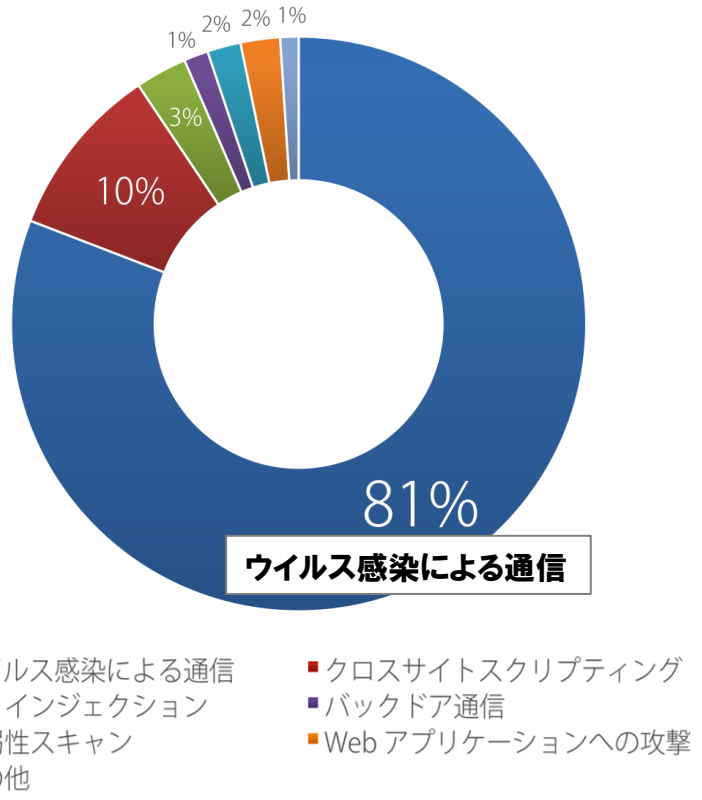



2011年　JSOC侵入傾向分析レポート
http://www.lac.co.jp/security/column/jsoc/

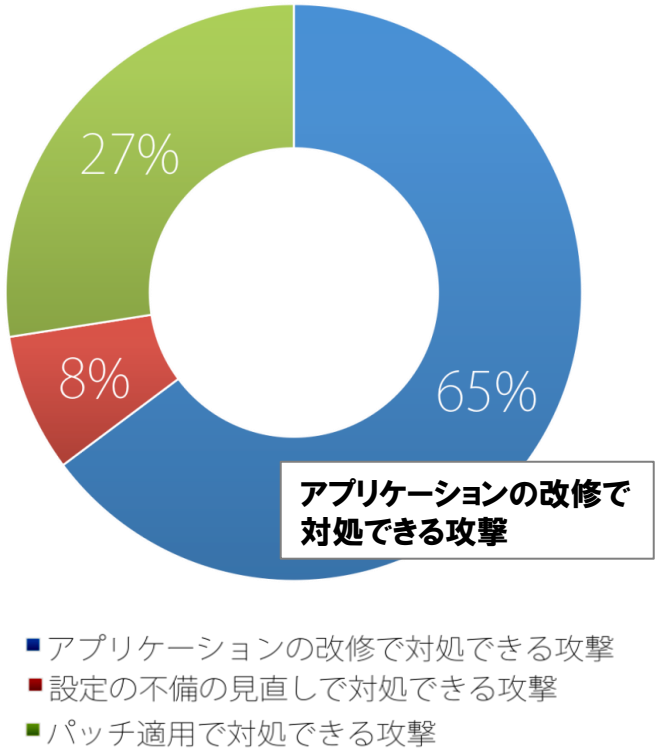
# JSOC侵入傾向分析レポート

**下記のグラフは、内部・外部ネットワークで発生する脅威の内訳です。**
**内部ネットワークで発生する脅威は、「ウイルス感染」が大半です。**

## 内部ネットワーク（お客様ネットワーク）

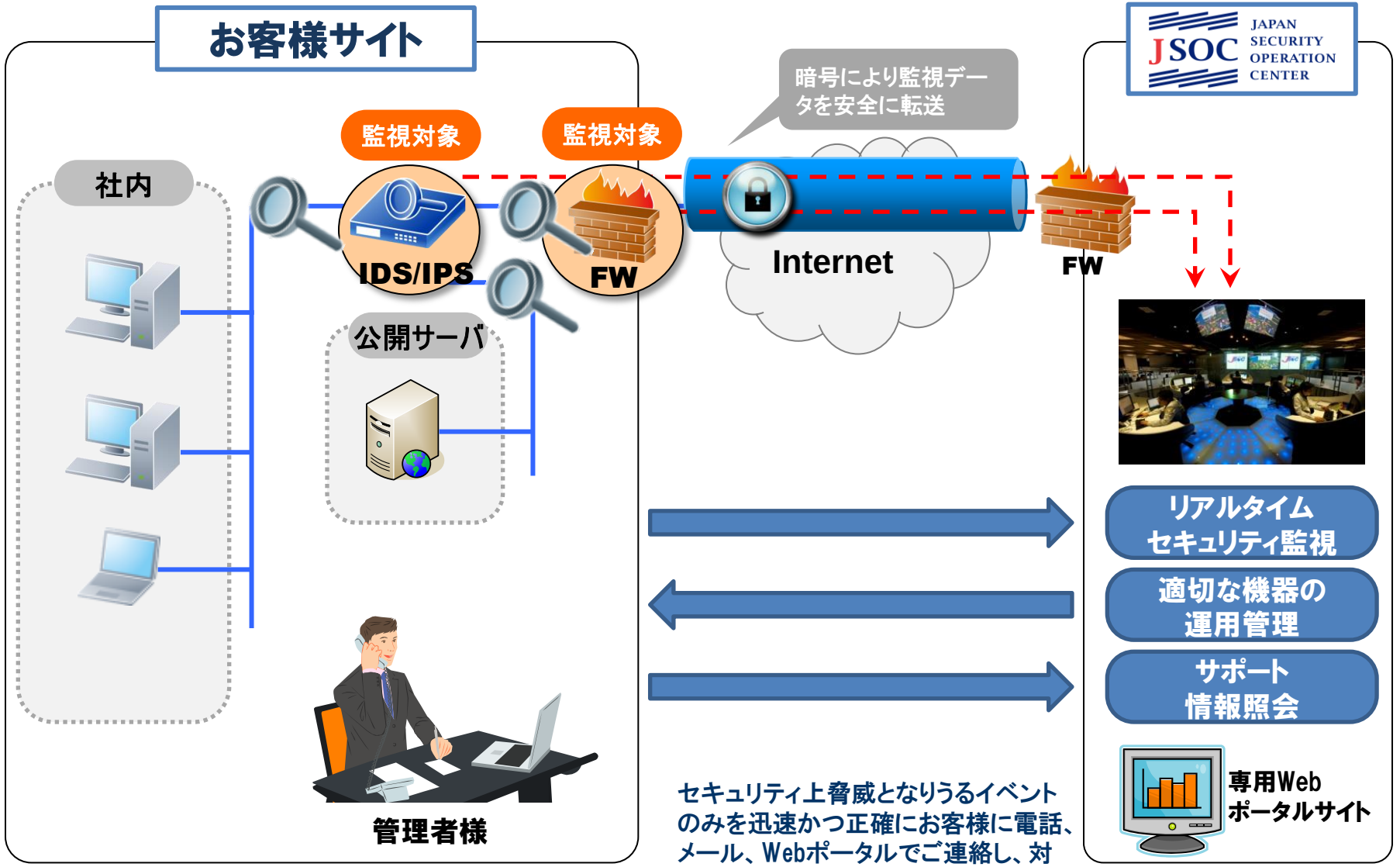



## 外部ネットワーク（インターネット）




2011年　JSOC侵入傾向分析レポート
http://www.lac.co.jp/security/column/jsoc/

# サービス構成イメージ



# JSOC監視サービス概要

| | | | ファイアウォール監視サービス | IDS 監視・運用サービス | IPS 監視・運用サービス |
|---|---|---|---|---|---|
| ① | 24時間365日 リアルタイム セキュリティ監視 | セキュリティ・インシデント監視 | ○ | ○ | ○ |
| | | ログのセキュリティ分析 | ○ | ○ | ○ |
| | | リアルタイム対策とアドバイス | ○ | ○ | ○ |
| ② | 適切な機器の 運用管理 | システムの稼働監視 | ○ | ○ | ○ |
| | | 障害対応１次切り分け | ○ | ○＊1 | ○＊1 |
| | | ポリシー変更 | — | ○ | ○ |
| | | シグネチャ更新 | — | ○ | ○ |
| | | 独自開発シグネチャ適用（JSIG） | — | ○＊2 | ○＊2 |
| | | 機器のバージョンアップ | — | ○＊3 | ○＊3 |
| ③ | サポート 情報の照会 | 緊急時の連絡と対策支援 | ○ | ○ | ○ |
| | | 問い合わせ対応 | ○ | ○ | ○ |
| | | Ｗｅｂポータルサイト | ○ | ○ | ○ |
| | | 月次レポート | ○ | ○ | ○ |
| | | セキュリティ情報の提供 | ○ | ○ | ○ |
| オプション （応急対応サービス） | | 応急対応（ＡＣＬ変更 など） | — | ○ | ○ |

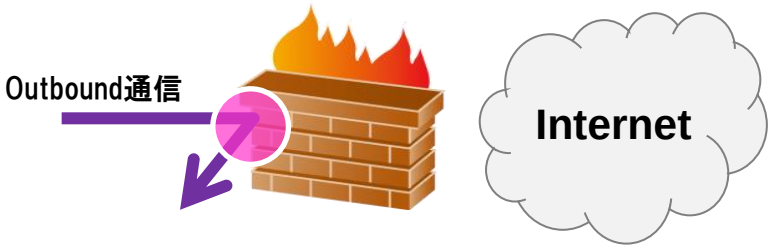
＊1 ラックからIDS/IPSをご購入いただいた場合、障害調査から復旧までをお客様に代わってJSOCが対応します。
＊2 製品の仕様上の制限により、独自開発シグネチャーJSIGが搭載できない機器があります。
＊3 バージョンアップは原則として、JSOCからリモートで作業できる場合に実施します。

# ① 24時間365日リアルタイムセキュリティ監視

FW IDS/IPS

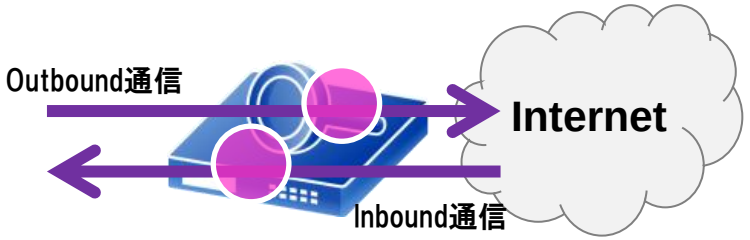
24時間365日、ファイアウォール、IDS/IPSのログをセキュリティアナリストによるリアルタイムの監視・分析を行い、お客様にとって問題があるイベントのみをお客様へご連絡します。

## ファイウォール監視




アクセス制御によるドロップログから不正プログラム感染後の外部接続などを検知

## IDS/IPS監視




＜メーカシグネチャ＞
OS、ミドルウェアの脆弱性をついた攻撃を検知/防御

＜JSOCオリジナルシグネチャ＞
不正プログラム感染後の外部接続、SQLインジェクション攻撃のWebアプリケーションレイヤの攻撃など

# ① リアルタイム対策とアドバイス

FW IDS/IPS

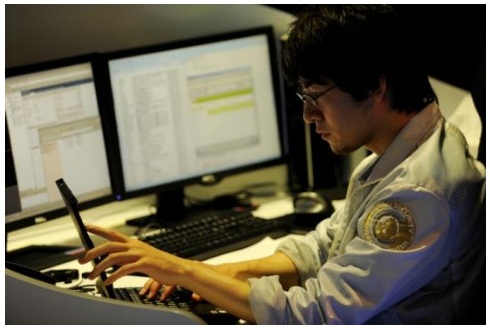
危険度の高いイベント(Critical,Emergency)は、セキュリティアナリストから指定されたお客様へ電話にて速やかにご連絡いたします。
単なる攻撃情報だけではなく、攻撃による影響範囲や必要な対応策など、具体的な内容などをお伝えいたします。緊急時には電話を通じて、お客様と一緒に全力で対策にあたります。
またご不明な点等に対するお問い合わせ対応も24時間365日でおこないます。

お客様

**通知連絡(24時間365日)**
- 危険度レベル
- IPアドレス
- 分析結果
- 推奨する対処方法、今後の対策
- 参考情報(URLなど)

**問い合わせ(24時間365日)**
- 対処方法について
- 確認方法について

など



JSOCセキュリティアナリスト

# ② 機器の稼働監視と障害対応

FW IDS/IPS

定期的に稼働監視を行っており、万が一障害が検出された場合は、速やかにご連絡と早期復旧に向けご支援いたします。

① 監視対象機器に対し、約3分おきにping送信、およびサービスポートへのアクセスによる稼動監視
② 応答がない場合、約1分間隔で2回リトライ確認
③ 2回目のリトライ失敗後、エンジニアによる手動での確認、およびログの到達状況の確認
④ 監視対象機器までの経路上のネットワーク機器に対してアクセス確認
⑤ 15分間継続的に監視対象機器からの応答がない場合、障害と判断して、お客様へ障害通知を実施
⑥ 障害対応開始

# ② シグネチャ更新とポリシーチューニング実施

IDS/IPS

日々、発見される最新の攻撃手法に対するシグネチャの更新や監視対象ネットワークの状態を考慮したポリシーチューニングにより、IDS/IPSのセキュリティ機能を最大限に引き出します。

## シグネチャの更新

① メーカーが新規シグネチャをリリース

② JSOCの検証環境にて、新規シグネチャに対する安全性・信頼性について検証

③ 安全性・信頼性の確認後、サービス対象機器に適用

④ 常に最新のシグネチャを適用することによって、新しい攻撃に対する防御力が向上

## ポリシーチューニング

① お客様サイトの環境によって、大量のアラート発生を検知。

② セキュリティアナリストがアラートの内容を調査して、誤検知であるかを確認。

③ ポリシーチューニングを実施して誤検知を排除。

④ 適切な監視ポリシーで運用。

## JSIGの開発

① メーカーシグネチャでは対応できない未知の攻撃をJSOCで検知

② その攻撃に対するJSIGを緊急開発。

③ 有効性・安全性の確認後、サービス対象機器に適用。

④ メーカーが対応するまでJSIGで継続監視を実施。

# ② IDS/IPSのバージョンアップの実施

IDS/IPS

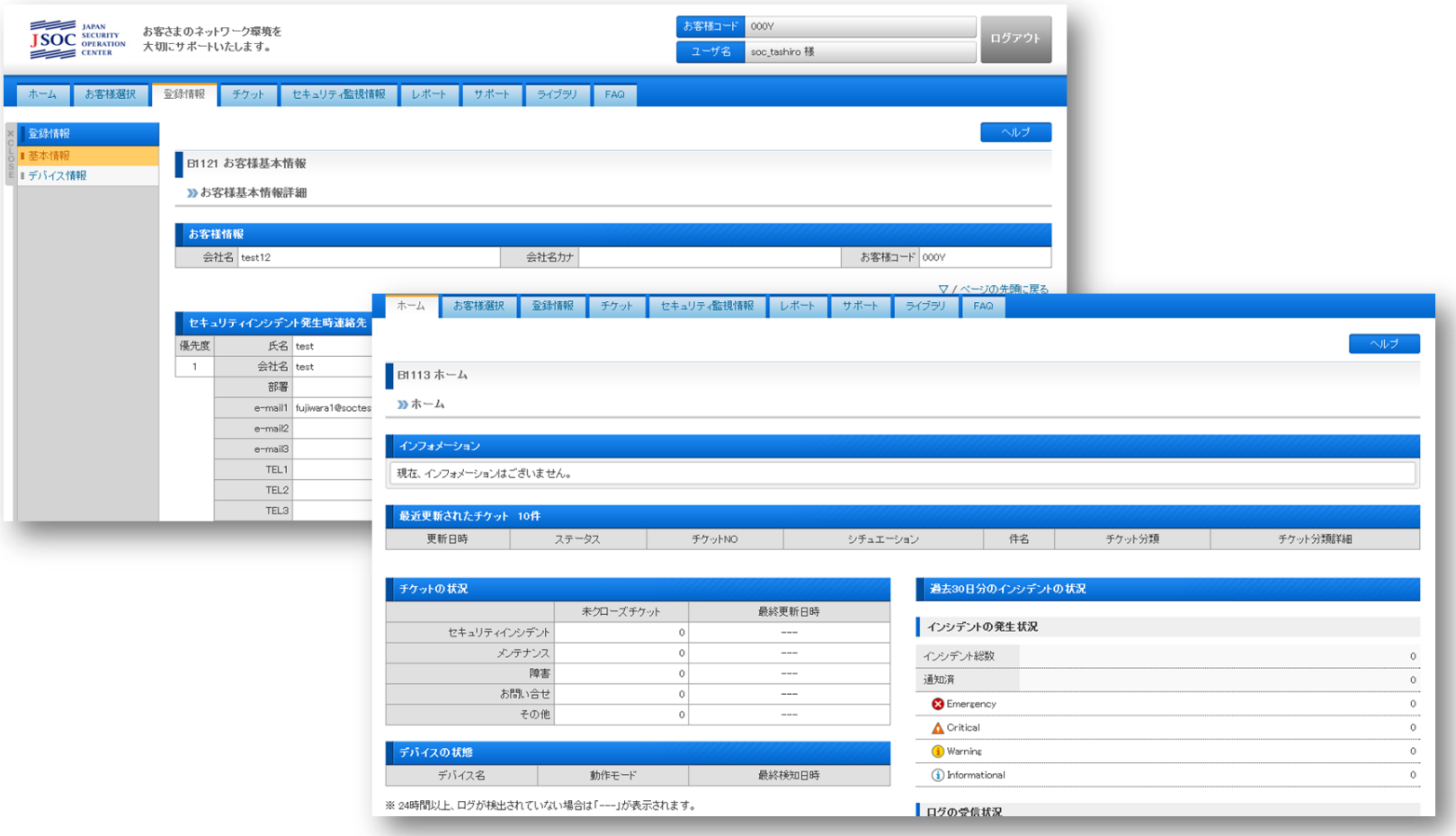
IDS/IPSメーカから新たにリリースされたファームウェアをJSOCにて事前検証を行い問題がないことを確認したうえで、リモートによるバージョンアップの作業を実施をおこない最適な状態にします。


※バージョンアップは原則として、JSOCからリモートで作業できる場合に実施いたします。

# ③ Webポータル(分析情報照会)の提供

FW IDS/IPS

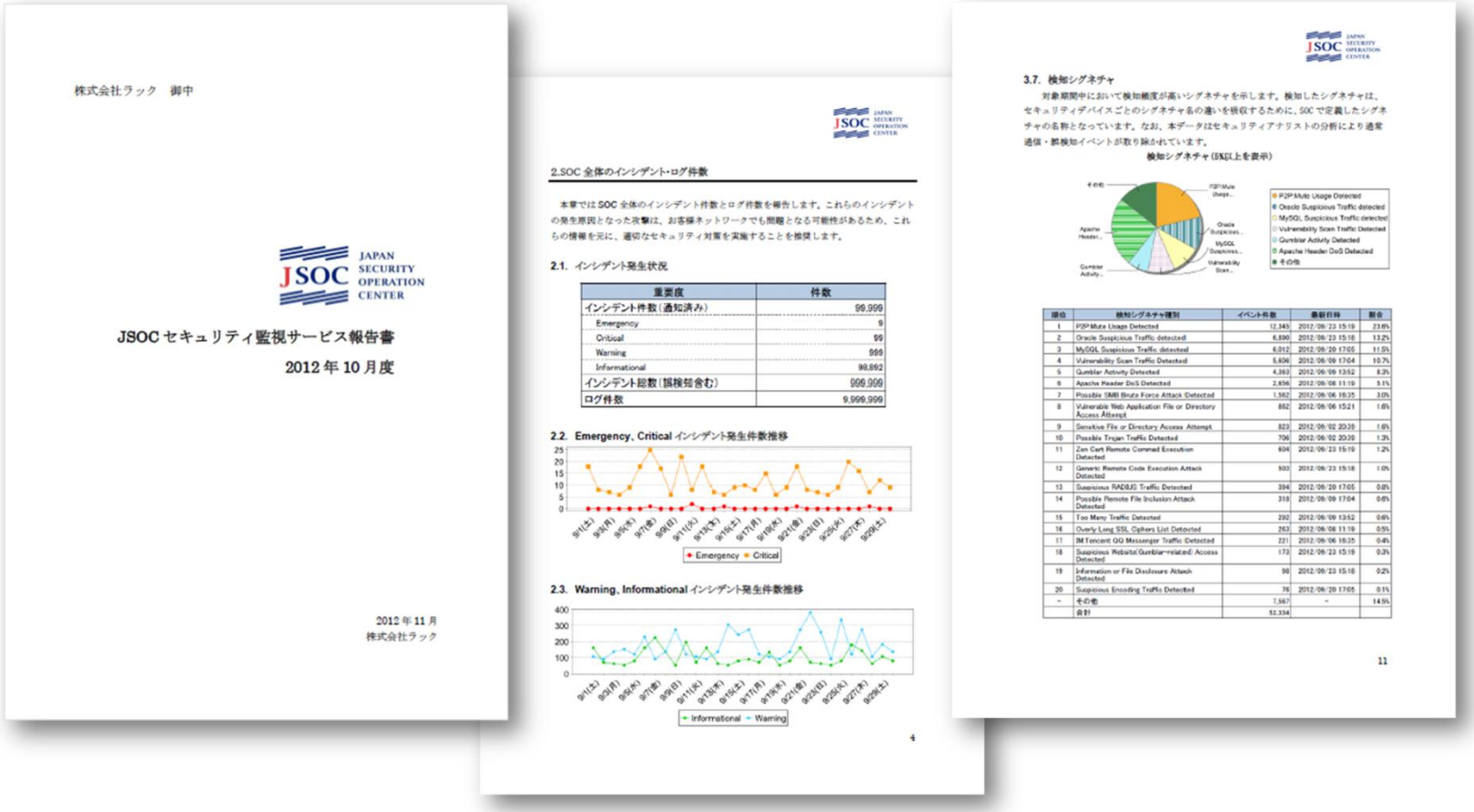
セキュリティ監視に関する情報は、お客様専用のWebポータルでリアルタイムに確認できます。
セキュリティ監視を通して、お客様のネットワーク環境がどのような脅威にさらされ、影響を受けたかなどが、分かりやすくまとめられています。



# ③ 月次レポートの提供

FW IDS/IPS

1ヶ月間のセキュリティ監視の結果は、分かりやすくまとめた月次レポートをご提供します。
お客様専用のWebポータルからダウンロードすることが可能です。



# ③ セキュリティ情報提供

FW IDS/IPS

情報セキュリティに関してのさまざまな情報を、セキュリティレポートや、サービスを利用するお客様向けのメルマガなどを通してご提供します。

| | | |
|---|---|---|
| セキュリティ関連情報の提供 | セキュリティ情報のメールマガジン（定期：隔週） | JSOC監視ユーザのセキュリティインシデントのランキング、世間のセキュリティ的話題などを取り上げたコラムなどを発信するメールマガジンをご提供いたします。 |
| | JSOC緊急注意喚起情報（不定期） | JSOC独自の収集情報を中心に、セキュリティ上緊急対策が必要と判断したものについて、JSOCセキュリティアラート「注意喚起」情報としていち早く配信いたします。 |

【ご参考】
ラックのセキュリティ事業のベースとなる情報源は数多くございますが、特長的なのは「サイバーセキュリティ研究所」です。
幅広く情報を収集し、分析を行っています。その成果として、脆弱性の発見、報告やハニーポットに関するレポートなどがあり、さらに講演やセミナーという形で、お客様やパートナー様に還元することに主眼を置いています。

# オプション：緊急対応サービス

IDS/IPS

IDS/IPSのセキュリティ監視により危険な通信を検知した場合、JSOCのセキュリティアナリストが、お客様のFirewallに緊急でACLを追加して危険な通信を遮断、被害の拡大を防止するサービスです。
攻撃者によりお客様ネットワークへの侵入が成功した、またはその可能性が著しく高い事象を検知した場合、ワームなどのウイルス感染が確認された場合にサービスを発動します。

JSOC JAPAN SECURITY OPERATION CENTER

- 攻撃者の侵入を検知
- Emergency発生を確認
- 顧客に緊急連絡

JSOC JAPAN SECURITY OPERATION CENTER

- 応急対応を開始
- FirewallのACLを変更し、被害の拡大を防止

お客様側

応急対応で防いでいる間に、被害サーバの対処を実施

## ■セキュリティイベントの危険度が高い時に発動

| 危険度 | セキュリティイベント |
|---|---|
| Emergency | お客様のシステムに対する攻撃が成功していることが確認できる場合<br>・Webサイトが改ざんされている<br>・JSOCのセキュリティアナリストによる監視対象機器のログ分析により、不正にデータが取得されていることが判明した場合、不正侵入が成功した場合、あるいは不正侵入の成功の可能性が著しく高い場合 |
| Critical | お客様のシステムに対する攻撃の成否は確認できないが、攻撃された可能性が高いとJSOCのセキュリティアナリストが判断した場合<br>お客様のネットワークが、ワームやボットに感染した場合 |

## ■マルチベンダーのFirewall機器に対応

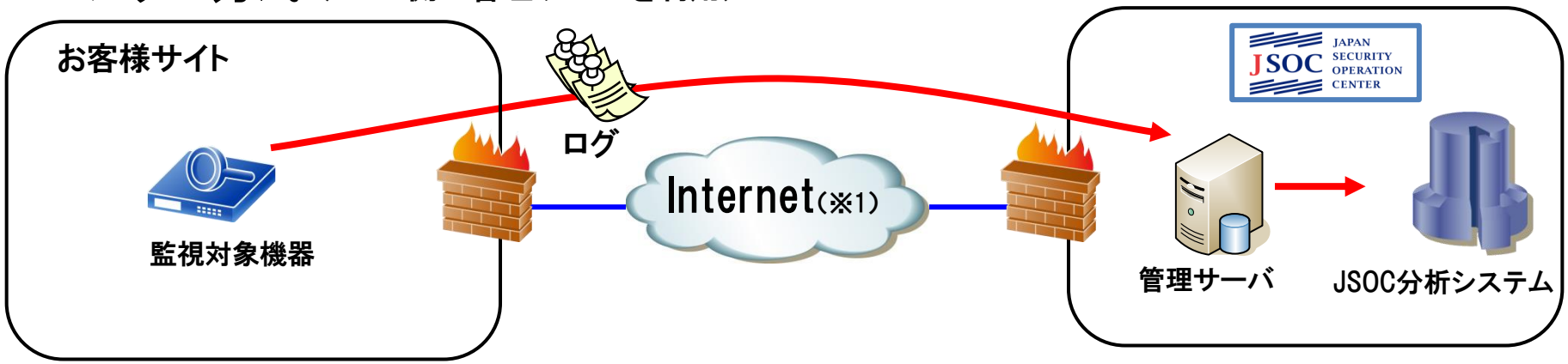
CISCO　JUNIPER NETWORKS　Check Point SOFTWARE TECHNOLOGIES LTD.　McAfee　その他

※ Firewall機器については、対応機種に制限はございません。どのFirewall機器をご利用でも対応できます。
※ McAfee社Network Security Platformを用いてIPS監視サービスを実施している場合、機器の通信監理機能を用いて本サービスの提供が可能です。

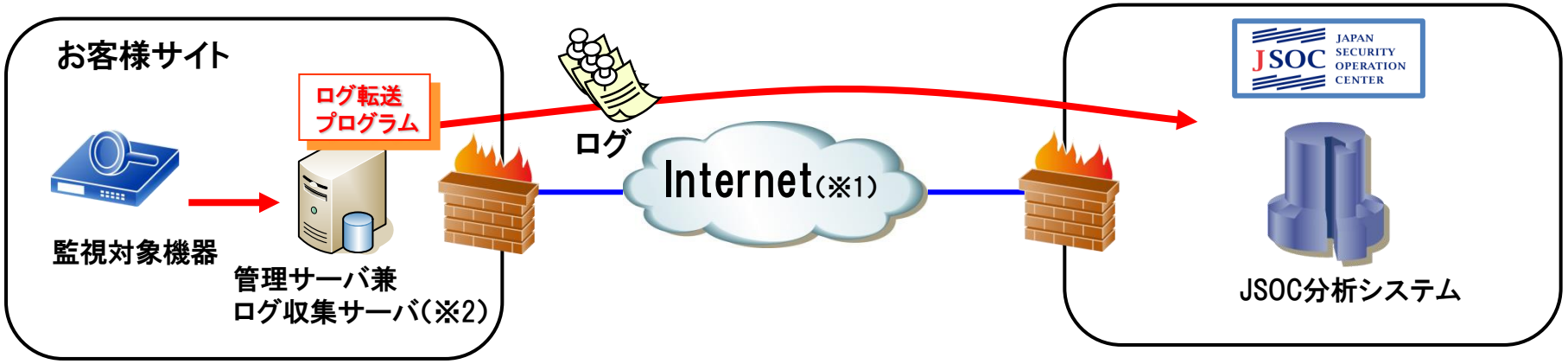
LAC

# サービス提供方式

## 1. センター方式（JSOC側の管理サーバを利用）



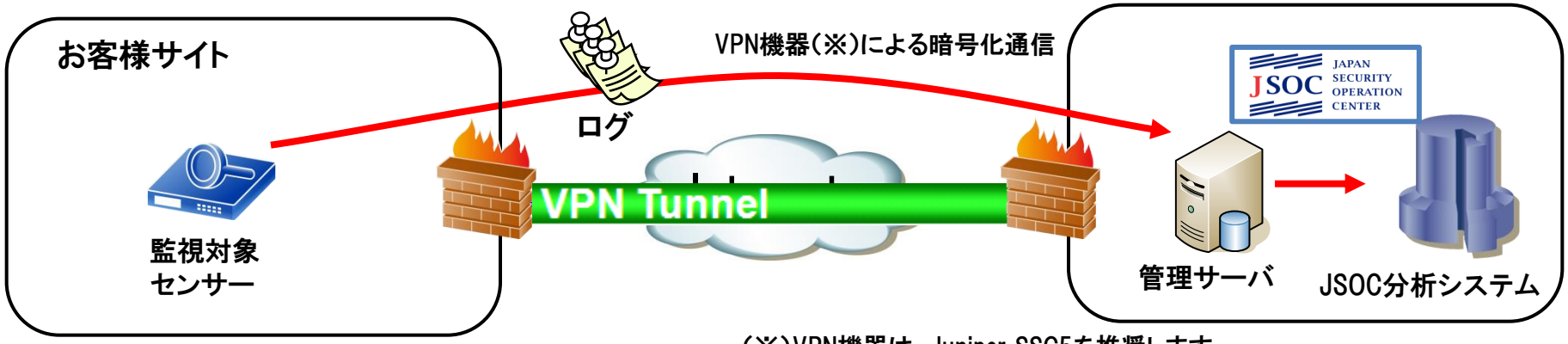

## 2. エージェント方式（お客様サイトに管理サーバ兼ログ収集サーバを設置）




（※1）サービス提供に必要な回線帯域は1.5Mbps以上を推奨します。サービス提供にあたっての通信要件は別途、ご提示いたします。
（※2）推奨スペックは別途、ご提示いたします。

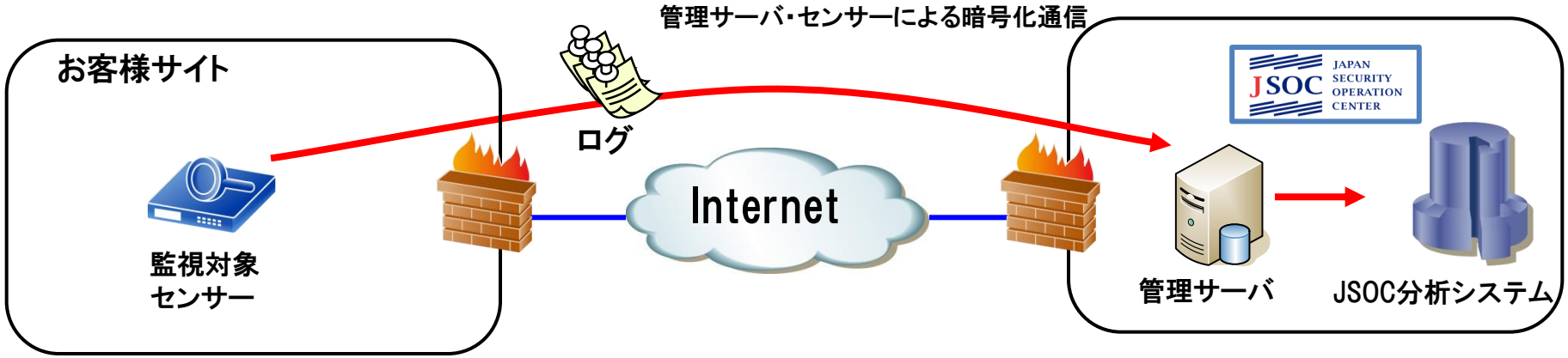
# JSOCとの接続形態

## 1. Internet VPN 接続（IPSec VPNによる暗号化通信）




（※）VPN機器は、Juniper SSG5を推奨します。

## 2. Internet 接続（管理サーバ・センサーによる暗号化通信）




本接続イメージはセンター方式です。エージェント方式でも同様の接続形態でJSOCと接続が可能です。

Thank you. Any Questions ?

**株式会社ラック**
**E-mail : sales@lac.co.jp**
**FAX : 03-6757-0193**

**〒102-0093**
**東京都千代田区平河町2-16-1 平河町森タワー**