IIJ C-SOCサービス

セキュリティインシデント対応を ワンストップでサポート

セキュリティログの分析を行い、インシデント発見から対策提案、IIJ運用機器の設定変更等までを実施。
お客様のセキュリティ対策を強力に支援します。
分析レベルは維持しつつ対応時間を限定した、低コストな「IIJ C-SOCサービス ベーシック」もご用意。

IIJ C-SOCサービスの特長

特長1 セキュリティインテリジェンスで脅威を可視化

セキュリティ機器のログやアラートに加え、バックボーントラフィックやDNSクエリ、外部情報なども含めた分析を実施。それらをセキュリティインテリジェンスとして蓄積し、事前防御としての活用、脅威の早期発見、セキュリティ対策の提案などを行います。

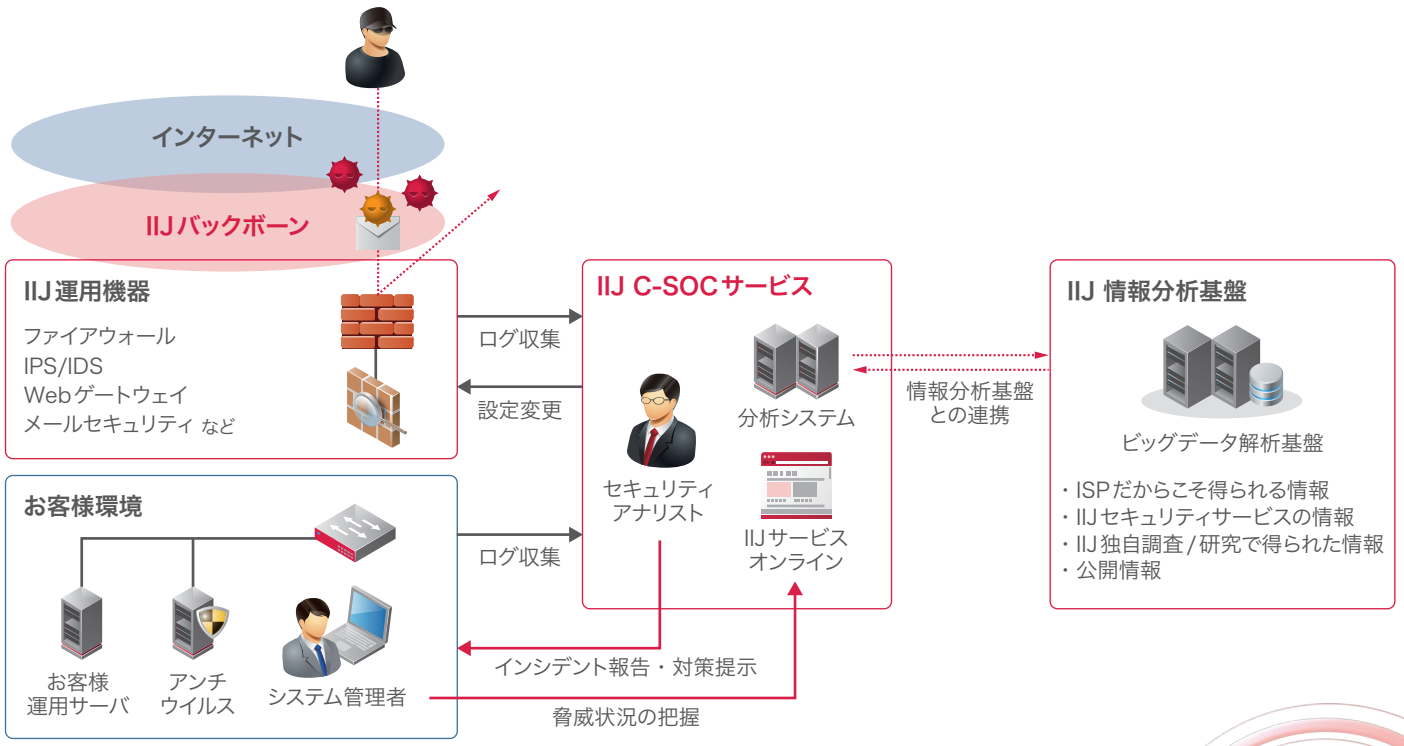
特長2 機器の運用からインシデント対応までワンストップで提供

セキュリティ機器の設置から運用、ログの収集、解析までをワンストップで提供。インシデント発生時には、必要に応じてIIJ運用機器の設定をIIJが変更することで、緊急度の高い攻撃に対しても迅速な対処が可能です。

特長3 経験豊富なセキュリティアナリストによる運用

1994年、国内初のファイアウォールサービスを提供開始して以来、金融業や官公庁、大企業、ECサイトなど、セキュリティの第一線で高度な対応を行ってきたセキュリティアナリストが多数在籍。それらの実績で培われたノウハウで、日々高度化する脅威からお客様を守ります。

サービスイメージ

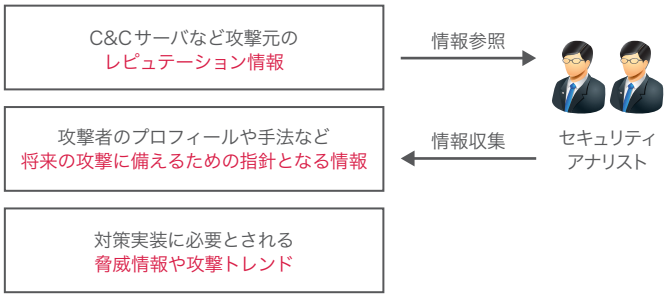


インシデントの発見から対策の提案、IIJ運用機器の設定変更などまでを行い、セキュリティ対策を支援

IIJ独自のセキュリティインテリジェンスの活用

情報分析基盤で収集した大量のログからIIJ独自のセキュリティインテリジェンスを生成し、インシデント対応に活用

インテリジェンスの例



提供機能

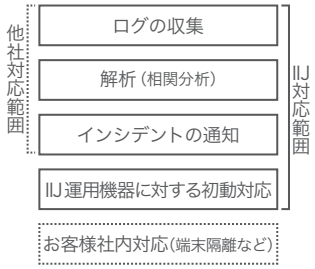
セキュリティログ分析	セキュリティログ及び、脅威情報データを分析することで、単体のセキュリティログでは、検知できないセキュリティインシデントを検出
セキュリティインシデント対応	IIJ運用機器に対しては、お客様運用管理担当者様から実施依頼もしくは、承認をいただいた上でIIJにて対策に必要な設定変更及び、調査を実施※1
セキュリティインシデント通知※2	セキュリティインシデントを検出した場合、セキュリティアナリストが確認を行い、重大度レベルの高いインシデントに関してお客様に通知
個別ログ収集機器の運用（お客様運用機器利用の場合）※3	お客様環境設置の接続用ルータからセキュリティログをログ収集基盤に集約し、個別ログ収集機器を介してSOCにセキュリティログを転送。お客様からSOCのネットワーク及び個別ログ収集機器の構築・運用・保守を提供
月次報告書	チケットの内容やセキュリティインシデントの発生状況やログ収集基盤の稼働情報などの統計情報を報告書にまとめ、PDF形式で提供
現地報告（オプション）※3	IIJのアナリストがお客様に訪問し、オンサイトで月次報告書の解説やセキュリティ対策のディスカッションを行う
ログ保管オプション	セキュリティ監視対象であるIIJサービス（IIJセキュアMXサービスを除く）及びお客様運用機器のログを、IIJセキュリティオペレーションセンターで一定期間保管。保管期間のお申し込みは、1年間から10年間までの1年単位
インシデント対応支援オプション	お客様のセキュリティインシデント対応における支援として、有事の際に電話やメールによるサポートや、現地に駆け付け被疑端末内のログ調査を行います
IIJサービスオンライン	インシデントの対応記録や、お問い合わせ、機器のメンテナンスなど、お客様とのやり取りをIIJサービスオンラインにチケットとして記録

※1：アラートのレベルによって、必要な設定変更内容を提案します。IIJセキュアWebゲートウェイ連携モジュールのタイプF、FV、F/CE、FV/CE及びIIJセキュアMX連携モジュールを利用されている場合に、設定変更を代行します。
※2：メール、チケットのみで通知します。
※3：ベーシックでは提供していません。

運用からインシデント対応までワンストップで提供

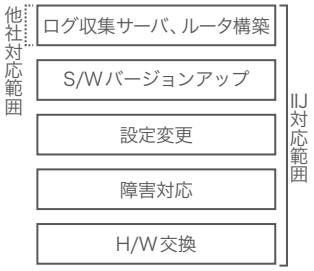
■インシデント発生時の対応

インシデント発生時、初動対応までを実施し、被害の拡大を食いとめます。



■ログ収集機器の構築・運用

ログ収集サーバ、ルータの運用を実施し、運用負荷を軽減します。

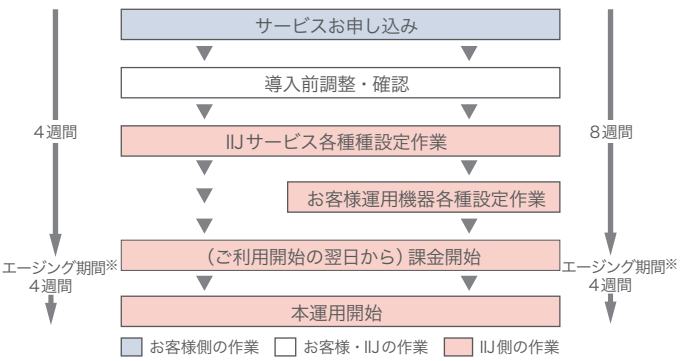


監視対象

IIJセキュアWebゲートウェイサービス	・タイプFV　・タイプF　・タイプV ・タイプFV/CE　・タイプF/CE　・タイプV/CE
IIJセキュアMXサービス	・基本機能 ・サンドボックスオプション
IIJマネージドIPS/IDSサービス	・McAfee社 Network Security Platform Mシリーズ
IIJマネージドファイアウォールサービス	・CheckPoint社 CPアプライアンス ・Fortinet社 FortiGateアプライアンスシリーズ ・Juniper Networks社 SRXシリーズ ・Palo Alto Networks社 PAシリーズ
IIJセキュアエンドポイントサービス	・アンチウイルス：Symantec ・アンチウイルス：Cylance ・IT資産管理
IIJマネージドWAFサービス	・タイプA
お客様ご利用機器個別ログ収集・個別ログ監視（オプション）	・アンチウイルスソフトウェア/マネージャ（McAfee社製品、Symantec社製品、Trend Micro社製品） ・認証サーバ（Microsoft社 Active Directory） ・サンドボックス（FireEye社 NXシリーズ）

※対応製品については都度更新されていますので詳細は別途お問い合わせください。
※ご利用料金に関しては別途お問い合わせください。
※IIJセキュアWebゲートウェイに対して本サービスを利用する場合は、IIJセキュアWebゲートウェイバイパスオプションが必須となります。
※IIJセキュアエンドポイントサービスのIT資産管理単独でのご利用では外部脅威の発見が難しいため、他の対象サービスとの組み合わせたご利用を推奨いたします。詳しくは、事前にご相談ください。
※IIJマネージドWAFサービスに対して本サービスをご利用の場合は、アドバンスドサポートのご契約が必要となります。

お申し込みからご利用開始まで



※エージング期間：セキュリティ分析開始後の分析精度向上のためのセキュリティインシデント検知状況の調査を行う期間です。
※インシデント対応支援オプションに関してはお申し込みからご利用開始まで4週間です。

Internet Initiative Japan

お問い合わせ（IIJインフォメーションセンター）
株式会社インターネットイニシアティブ
TEL：03-5205-4466（9:30～17:30 土・日・祝日除く）
E-Mail：info@iij.ad.jp
URL：www.iij.ad.jp

IIJ-CSOC005-0007