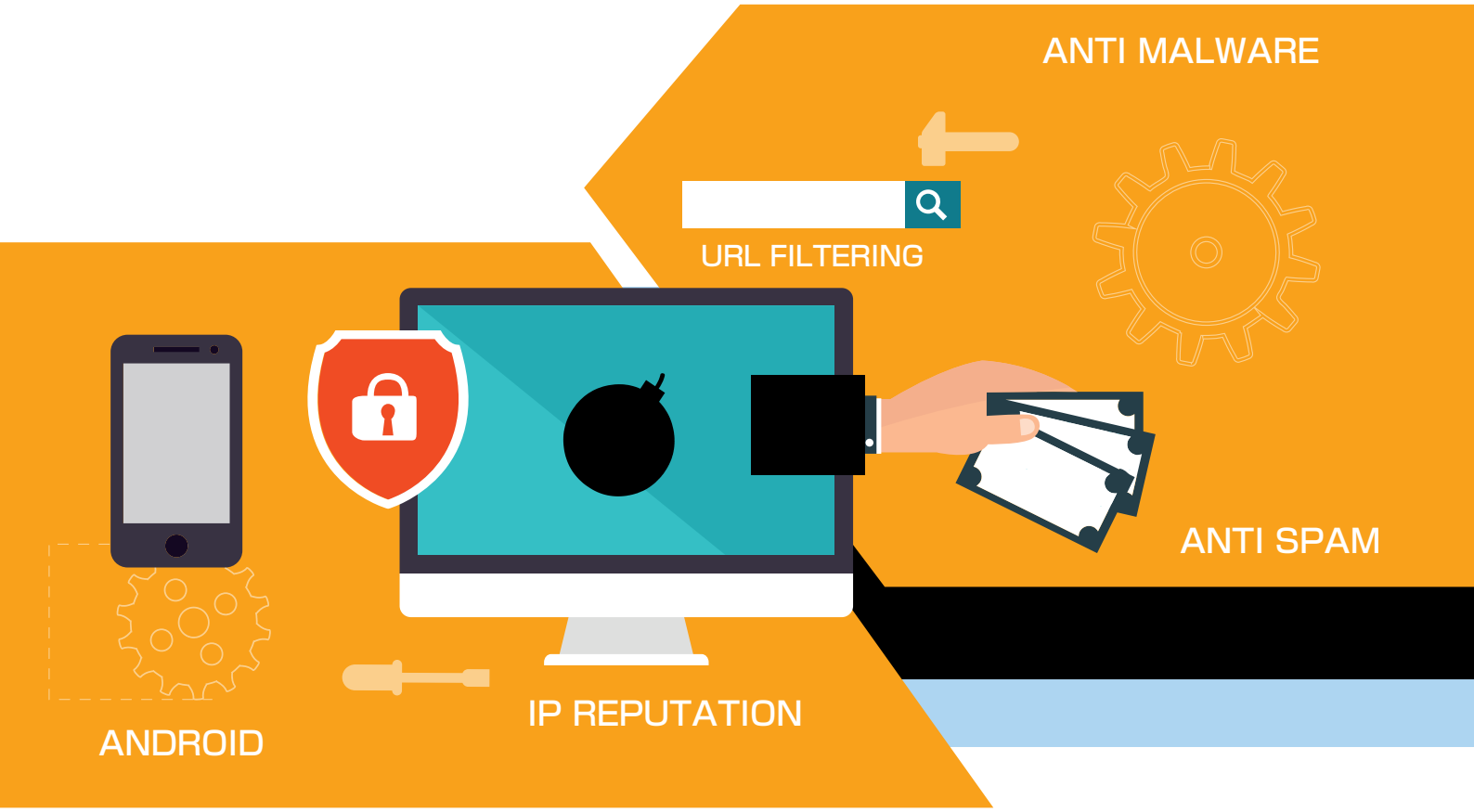
Security Intelligence Solution

脅威インテリジェンスサービス

CYREN

世界190か国、6億人以上のセキュリティを守る



JSECURITY

世界190か国、6億人以上のセキュリティを守る

CYREN SDK製品

CYREN社について

CYREN社は、Webセキュリティ、メールセキュリティ、アンチマルウェア製品などのインターネットセキュリティソリューションを提供するグローバルセキュリティ企業です。同社のセキュリティ製品は、世界190か国、6億人以上のユーザのトランザクションを日々進化する様々な脅威から守っています。CYREN社のアンチスパム、アンチウィルス、IPレピュテーション、URLフィルタリング、モバイルセキュリティなどの製品は、自社製品を設計する場合にも導入しやすく、容易に使えるように設計されています。

600M+	17B+	130M+
USERS PROTECTED	DAILY TRANSACTIONS	THREATS BLOCKED DAILY

The Most Security Data

CYRENは毎日、数千件の未知のIPアドレス、フィッシングサイト、疑わしいURLを検出しており、詳細な脅威情報を瞬時に提供することで、6億人以上をフィッシングサイトや有害なIPアドレスなどのWeb上の脅威から保護しています。

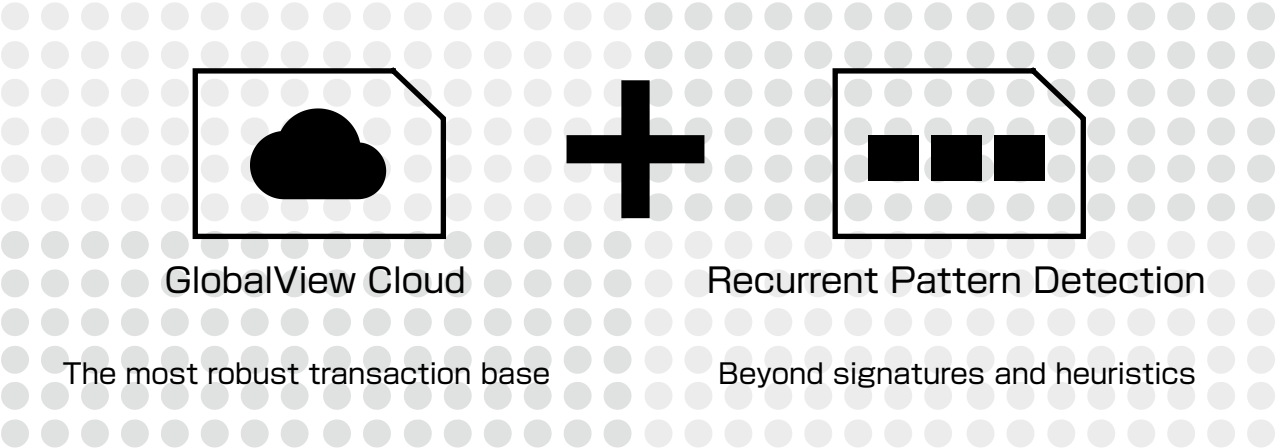
Big Data Analytics

CYRENのサイバーセキュリティプラットフォームでは、毎日170億件以上のトランザクションを分析して自動的にIPアドレス、ドメイン、ホスト、ファイルなどを調査し怪しい行動との関連付けを行いリスクスコアを構築しているため、瞬時に分類を行うことができます。

The Best Cyber Intelligence

CYRENのクラウドベースのエンタープライズWebとメールセキュリティサービスは200社以上のセキュリティベンダーで使われており、毎日1億3千万件の脅威をブロックしています。

CYRENのコア技術



より早くかつ正確に リアルタイム検知

CYREN GlobalView Cloud

インターネット上のデータを分類するためにデータを収集し分析しています。

収集

- 一日170億件のトランザクション
- 世界190か国以上の国から6億人以上のユーザクエリ
- 200社以上のグローバルパートナーからのデータは国や地域を限定せず、真のグローバルビューデータを提供
- 幅広い範囲のデータポイント IP, DNS, HTTP, SMTP, …

検査

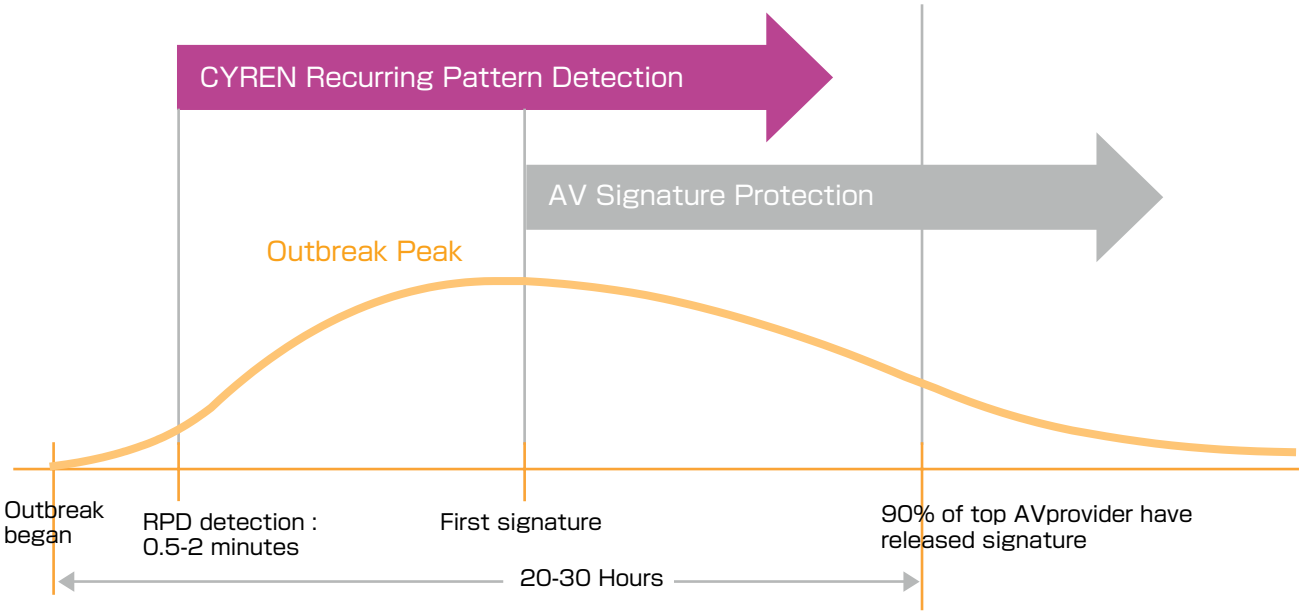
- ボットネットやURL、IPアドレス、スパイウェア、スクリプトなどのリアルタイム分類
- ZERO HOURマルウェアの高い検出率
- 低い誤検知率
- 世界19拠点のデータセンター
  CYRENは、国やお客様の地域の要件に対処するためにEMEA、アジア太平洋、米国内においてデータセンターを運営しています。

検知

- リアルタイムフィンガープリント
- インバウンドとアウトバウンドトラフィック
- Recurring pattern detection(RPD)技術※
- IPv6トラフィック対応

※反復的なパターンと大量流布されているスパムメールを検出する技術

CYRENの脅威検知



CYRENのRPD技術は、世界最大規模の検知インフラにより、
他社と比較して脅威検知速度が非常に速い

顧客とパートナー

多数のグローバル企業が自社のインフラと顧客を保護するためにCYRENの技術を使っています。

CYREN SDK 製品 ラインナップ

ANTISPAM

世界中で使用されその性能が証明されたCYREN組み込みアンチスパムエンジンは、Recurrent Pattern Detection(RPD)技術により、言語やフォーマットを問わず、低い誤検知率と確実なリアルタイムブロック機能で業界トップレベルの性能を提供します。

AntiMalware

AntiMalwareは、世界190か国60万個のデータ収集センサと、6億人以上のユーザ、170億件/日のリアルタイムトランザクションの自動分析により、脅威データを瞬時に把握できるGlobal View Cloudと連携して素早く正確にマルウェアを検出します。

IP REPUTATION

IP REPUTATIONは、毎日170億件のリアルタイムトランザクションを自動分析するGlobal View Cloudと連携してトラフィックを継続的に追跡することで、安全なIPアドレスと有害なIPアドレスをリアルタイムに正確に分類します。

URL FILTERING

URL FILTERINGは、Global View Cloudと連携してトラフィックを継続的に追跡することで安全なURLと有害なURLをリアルタイムに正確に分類します。例えば、ローカルストレージを持たないような小さな機器でも実装できるよう設計されています。

ANDROID MOBILE SECURITY

ANDROID MOBILE SECURITYはアンドロイド向けのセキュリティSDKです。未知のマルウェア検出やURLフィルタリング機能により、WEB上の脅威から機器を守ります。高速スキャン、低リソース使用率、低消費電力で、容易に実装できるように設計されています。

PHISHING URL FEED

Phising URL　FEEDは、CYRENセキュリティアライアンスとの連携とGlobalView Cloudで収集および分類したPhising URLを毎日CYREN クラウドデータベースに追加します。この脅威データは世界最高水準のグローバルセキュリティベンダとサービスプロバイダがユーザを守るために使っています。

SANDBOX ARRAY

進化し続けるAPT攻撃と悪性コードおよびランサムウェアなどは既存ウィルス対策とSandboxを迂回して攻撃します。CYREN Sandbox arrayのグローバルデータ収集と検知および分析技術は、未知のAPT攻撃と悪性コードに最も早く効果的に対応できます。

ANTISPAM

世界の主要なセキュリティベンダーとクラウドサービス事業者から認められたCYRENのアンチスパムエンジンは、言語や形式を問わず、リアルタイムにスパムメールをブロックする業界最高の検知率を誇っています。

特許技術: RPD

- RPD:メールタイトル、本文の特定な文字、URL、送信者IP、添付ファイルのハッシュ値などを統合分析して反復的なパターンと大量流布されているスパムメールを検出する技術
- マルチパターン分析：送信者IP、メール構造、添付ファイルなど様々な情報から分析。
- マルチ検出経路：送信者、スパムの活動期間、送信元IP、URLなどにより場所や形式を問わずスパムメールを検出。

高い検出率

- 高い顧客満足度：コンテンツや言語に関係なく検出可能な検出技術により高度な迷惑メールもブロック。
- 優れた検出率と低メンテナンスコスト：新しいタイプのスパム攻撃の検出と容易に利用可能なエンジン。
- リアルタイムモニタリング：1日に10億件以上のメールをリアルタイム分析しフィッシング対策に反映。

"当社のメールサービスである「Trust Layer」の顧客に99%以上のスパム検出率を保証する必要がありました。CYRENのAnti-Spam SDKはこの要件をクリアする性能を持っていたので、私たちは、CYREN ANTISPAMを選択しました。"

Jose Antonio Lopez, Corporate Solutions Director, Panda Security

"CYRENの高いスパム検出率のおかげで、顧客は完全にスパムメールから解放され大変満足しています。"

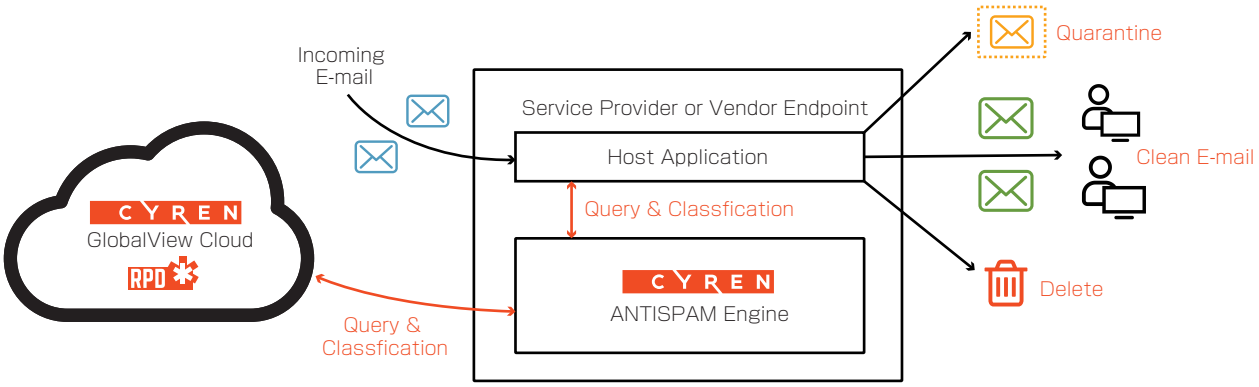
Eric Aarrestad VP, Marketing WatchGuard

ANTISPAMを利用するメリット

- 費用の削減：開発者が進化するスパムパターンと攻撃戦略について新たに対応する必要はありません。CYERNが変わりに対応します。
- TCO削減：高い性能と低いサポート費用、現在のプラットフォームに簡単に連携できますのでコスト削減と適切なタイミングで対応できます。
- 低いリソース：少ないリソース、最小限の帯域幅とCPUで使用できますので既存ハードウェアとソフトウェアの性能に影響が殆どありません。

スパムメールの検出アーキテクチャ

CYRENのGlobalView Cloudは、グローバル拠点に配置されたデータセンターと複数のトラフィック収集ノードにより、毎日10億件以上のインターネットメールを収集します。RPD技術は、このように収集されたメールトラフィックを自動的に分析して、全世界に流布されているスパムメールを検出しています。



スパムシグネチャは、ローカルキャッシュを利用して、すぐにアプリケーションに判定結果を提供し、ローカルキャッシュで判定できない場合はGlobal View Cloudの非常に高速なクエリを利用して解決します。シグネチャの更新はリアルタイムに提供されるのですぐに適用が可能です。長い間、顧客やパートナーとの親密な協力の結果、CYREN Anti-Spam SDKは、現存する最も柔軟性の高いアンチスパムエンジンとなっており、インフラストラクチャの設計、セキュリティソフトウェアの開発、ネットワークセキュリティ製品の開発に不可欠なSDKとして認められています。CYREN Anti-Spam SDKは様々なハードウェア、ソフトウェアで使用できるように柔軟に設計されているため現在幅広く活用されており、以下のような製品に使用して製品の価値を高めることができます。

- アンチスパムシステム
- MTA エンジン/グループウェア/ウェブメール/クラウドサービス
- UTM /Firewall
- アンチウィルスソフトウェア

ANTISPAMの特徴

- リアルタイムシグネチャの更新
- 99% 以上の検出率
- 低いCPUおよびメモリ使用率
- 簡単かつ迅速に適用/様々なプラットフォームのサポート
- シングルプロセスで毎秒数百件の処理
- 言語/地域を問わない検出能力

AntiMalware

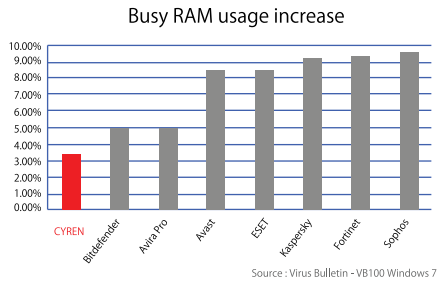
CYREN Anti-Malwareエンジンは、様々な機器やソフトウェアに搭載するために最適化されたAnti-Malware SDKエンジンです。CYRENは優れたマルウェア検出能力を様々なハードウェアおよびソフトウェアに効率的に搭載できるAnti-Malware SDKエンジンを提供しています。

日々進化するマルウェアに積極的に対応するために、Cyren AntiMalwareは優れた検知能力を提供します。

世界的なアンチウィルス専門比較テスト機関のAV-Test(www.av-test.org)は、アンチウィルスベンダー別のマルウェア検知時刻のレポートを毎日発表しており、ほとんどのケースでCYRENによる検知が一番早いことを確認できます。
http://www.cyren.com/security-center/malware-outbreak-detection

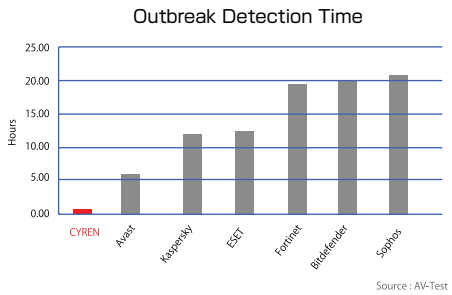
SDKに最適化されたエンジン

- 高速な正常ファイル判断：検査対象の大部分を占める正常ファイルを高速に処理できるように最適化。
- 低いリソース負荷：競合製品と比較して約半分のCPUとメモリ使用率を実現。
- コンパクトなエンジン：エンジンサイズは2MB以下。定義ファイルも35MB程度と非常にコンパクト。
- 低い帯域使用率：エンジンがコンパクトなため使用帯域が少なく、ネットワーク負荷が低い。



検証された優れた検出技術

- マルチレイヤ検出：ヒューリスティック、シグネチャ、エミュレーション検出による多層検出。
- モジュール型アーキテクチャ：新たな脅威への迅速な更新。
- 新しい検出技術：Global View技術を利用した新型脅威の迅速な検出。Virus Bulletin、West Coast Labs、ICSA Labs認証など、アンチウィルステストで常にTop 5の検出率。



Anti-Malwareは、様々な機器やソフトに広く使用可能な最も専門的なSDKエンジンです

ハードウェア、アプリケーション、ネットワークのセキュリティ

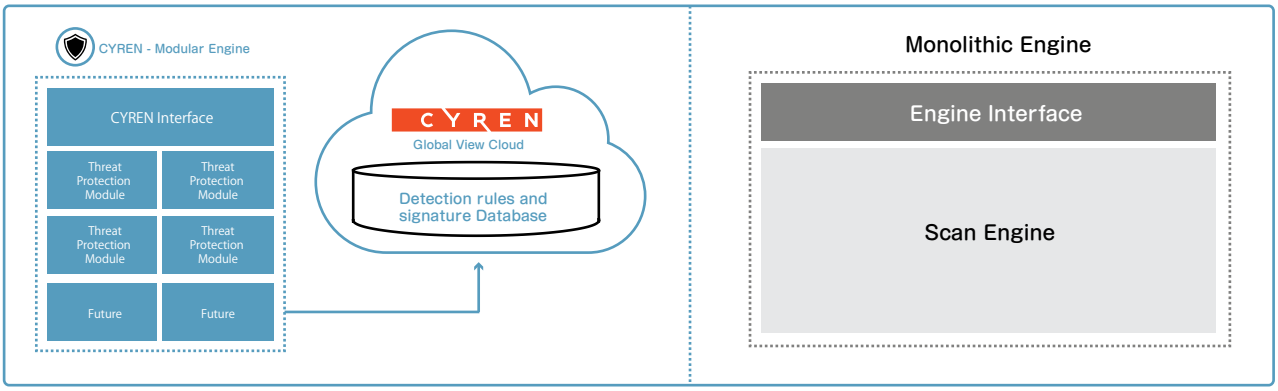
- メールサーバ、NAS、グループウェア
- アンチウィルス
- Web Gateway等のセキュリティ製品
- ネットワークセキュリティ製品(Firewall、UTM、IPSなど)
- デスクトッププログラム

インターネットサービス

- Software-as-a-Service (SaaS)
- Security-as-a-Service (SECaaS)
- Internet Service Providers (ISP)
- モバイルセキュリティ
- Webメール、オンラインストレージ

モジュール型アーキテクチャ - 柔軟でシンプルな実装方法

CYREN SDKエンジンは、モジュール化フレームワークに基づいており、Polymorphicウィルス検査モジュール、PDFファイルの検査モジュールなど、複数の精密な検査モジュールを提供しています。また、検査フレームワーク内でそれぞれの脅威防止モジュールは特定のオブジェクトの正確な検出ができるように設計されています。CYRENのモジュール型アーキテクチャ技術は、既存のモジュールを変更せずに新しいモジュールを迅速に追加して、新しい脅威に対して素早く対応することができます。そのためCYREN SDKエンジンを使用しているベンダーは新たな脅威に対して迅速に対処することができ、モノリシックエンジンを使用している他社製品に対して大きなアドバンテージを持つことができます。



CYRENエンジンのAPIは呼び出し処理が簡単で、プラットフォームが変わっても同じAPIを使用できますので、短期間に実装･変更することが可能です。新機能追加は既存環境を変更することなく新機能を追加できるため、手間をかけずに製品展開と管理が可能になります。

統合インターネットセキュリティ

- 統合インターネットセキュリティ：ウィルス、ワーム、トロイの木馬、スパイウェア、アドウェア、および潜在的な攻撃を検出。
- Global View Cloud分析：CYRENのGlobal View Cloudは毎日数十億件のフィッシング、スパムメール、Web攻撃などを分析しており、分析されたデータは、各ベンダーにリアルタイムに提供しています。

Anti-Malwareの特徴

- ウィルス、ワーム、トロイの木馬、スパイウェア、アドウェア、および、潜在的な攻撃を誘発するマルウェア検出
- zip, bzip2, 7-zip, RAR, CABなどの全ての圧縮ファイル検出
- 最適化された高い信頼性のi386, x86, x64と ARMエミュレータ
- 32-bit、64-bit対応、リトルエンディアン、ビッグエンディアン対応
- マルチプラットフォーム (Windows, Linux, UNIX, FreeBSDなど)
- シンプルなAPIを使用して検出結果をフィードバック
- .NET、スクリプトベースのインターフェースを容易に統合
- ネイティブ Windows COMインターフェース
- マルチコア、マルチスレッド対応の安定したライブラリ
- Sendmail/Postfixベースのメールサーバで使用可能なプラグイン
- 選択可能なさまざまな種類のシグネチャファイルを提供

IP REPUTATION

外部ネットワークからのトラフィックによる執拗な攻撃は決して終わりません。スパム送信者やハッカーは、セキュリティソリューションを突破するために常に変化しています。メッセージングセキュリティ企業は、ゾンビトラフィックが顧客の内部ネットワークに侵入する前に遮断するため、優れたパフォーマンスと検出レベルを経験するでしょう。
世界で最も広範なメールセキュリティネットワークであるCYREN Global View Cloudを利用して、リアルタイムに以下のような分析結果を得ることができます。

メールを分析する前に送信者のIPアドレスでリスクレベルを一次分類しますので、メール分析に必要なリソースを大幅に軽減するメリットがあります。現在、大手インターネットサービスプロバイダーのメールサービスに活用されています。

数十万の新しいゾンビPC（不正アカウントおよびホストコンピュータ）を毎日検出

数千万のIPアドレスからのトラフィックを継続的に追跡

数十億のメールメッセージをリアルタイムで正確に分析

GLOBAL VIEW REPUTATION

CYREN Global View Cloudは、各国のネットワークデバイスや、デスクトップソフトウェアなど、広範囲にわたり長期間蓄積した送信者の評価データと最新の評価データの両方のデータの統計情報を使用してリアルタイムに分析を行い、正当な送信者とスパム送信者、ゾンビ、不正プログラムを区別し情報を集約します。

ゾンビ問題の深刻性

ゾンビPCは一日に約1200億個あまりのスパムの85%を送信している。

毎日、数十万個のゾンビが検出されている。

一般的なボットネットは数時間にわたって1億件のメッセージを送信する。

1つのボットネットあたり数万個から数十万個のゾンビPCがある。

IP REPUTATIONを利用するメリット

迅速かつ容易にメッセージングセキュリティソリューションの機能を拡張できる。

サービスレベルの改善と顧客満足度の向上。

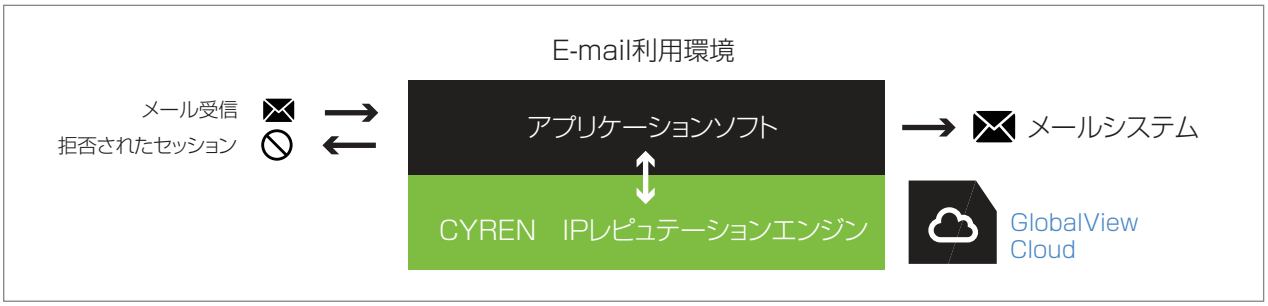
スループットの向上。

“すべての企業やサービスプロバイダは、スパム対策やウィルス対策で評判のサービスを導入することが不可欠だと考える。CYRENのグローバルモニタリングとリアルタイム分析は十分な競争力を提供する。”

Jose Antonio Lopez, Corporate Solutions Director, Panda Security

動作の仕組み

対象デバイスはSMTP接続要求を確認します。そして、送信IP アドレス情報を基にGlobal View Cloud に IP Reputationクエリを実行します。Global View Cloudからの結果によって、そのIP接続を受け入れるかどうか、一時的あるいは恒久的に遮断するかを決定します。



特徴

- リアルタイムでボットネットを検出
- CYRENのGlobal View Cloudに基づく正確な測定
  - ▶ 190か国、80以上のベンダー・ネットワークを活用
  - ▶ ソース：Firewall、メール機器、デスクトップソフトウェア、xSPs
- 属性収集：DNS情報、地域、動的IP、公開RBL
- Decision Managerがゾンビ防御件数を増加し、誤検知を低減
  - ▶ 一時遮断か接続かを瞬時に判断
  - ▶ 接続数制限
- IP別に提供される豊富なデータ
  - ▶ 推奨されるアクション：遮断、調整、許可
  - ▶ IP Class：アクション可能なクラスに詳細に分類
  - ▶ IPリスクレベル： 0-100まで詳細なレベル分類
  - ▶ 有効なバルクデータ分類 (例：ニュースレター)

IP REPUTATIONの特徴

- 標準のMail Transfer Agent(MTA)フラットフォーム対応
- 高い拡張性：毎秒4000件以上のメッセージに対応可能
- HTTP、UDP、RBL/RBL+ インタフェースが利用可能
- UDPを通じてクラウド接続：ソフトウェアインストール不要
- 様々な開発オプション：ビルトインキャシングのための、ローカルデーモンと
  フェイルオーバー (Linux, FreeBSD, Solaris and Windows)

URL FILTERING

CYREN Global Viewテクノロジーの URL FILTERINGは、前世代のURLフィルタリングソリューションの限界を飛び越え、リアルタイムの更新と信頼性の高い精度、セキュリティを容易に実現します。CYRENの独自技術であるGlobal Viewは、広範囲のカバレッジを実現するために世界中に配置されたデータセンターを活用しています。

グローバルURLデータベースに加えて、日本の優秀なパートナーとの連携により日本国内のURLもしっかりと対応します。

革新的なGLOBAL VIEW 検出技術

インターネットの膨大なURL情報に対して、伝統的なDBベースのURLフィルタリング製品では限界があります。URL FILTERINGは、これらの限界を飛び越え、顧客のニーズを満たすことができる情報を提供するために、クラウドベースのGlobalView技術を導入しました。

- グローバルURL情報/リアルタイム分析：毎日10億件以上のURL分析
- 限界がないクラウドデータベース：顧客が必要なすべてのURL分類および保存
- 低いリソース消費（CPU、メモリ、帯域幅）：多くのリソースが必要なシグネチャの更新をアンインストールして、必要な情報のみを使用できるように、ローカルキャッシュとリアルタイムの更新を同時使用
- セキュリティカテゴリを提供：マルウェア、フィッシングURLなどの詳細なセキュリティカテゴリ提供により顧客を保護

優れた精度と広い検査範囲

URL FILTERINGは各URLの情報を正確かつ迅速に提供します。

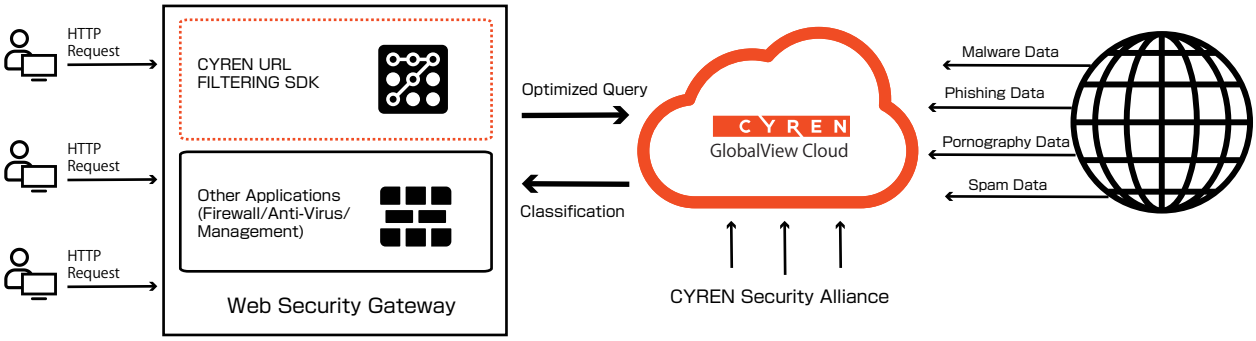
- 顧客が要求するカテゴリ分類は、迅速に検証して反映されます。
- URLの様々な分析とユーザ反応などを把握して分類レベルを判断します。
- 持続的な追跡が常にURLの正確な分類を可能にしています。

URL FILTERINGを利用するメリット

- ウェブセキュリティ強化:
  マルウェアなどのウェブ攻撃からのリアルタイム保護
- 有害サイト遮断:
  アダルト、ギャンブルなどの有害サイトアクセスをブロック
- モバイルセキュリティ:
  モバイル端末からマルウェアダウンロードを防止
- 業務用以外のサイトをブロック:
  顧客ポリシーに合ったサイトを構成
- モニタリングシステム:ユーザのウェブサイト訪問履歴統計の作成
- Security-as-a-Service (SECaaS)

ZERO HOUR SECURITY

- 顧客が脅威にさらされる前に予測検出で有害サイトを判定
- ZERO HOUR SECURITY機能はGlobal Viewを介してすべてのCYREN製品に適用されます。
- 正確性向上のためにCYRENセキュリティアライアンスパートナーと連携して情報を蓄積しています。



利用イメージ

1. URL FILTERINGをWebセキュリティ製品、監視製品などにインストールします。
2. 次に一度httpリクエストを行った後、判断基準となるURL情報を受信します。
3. URLの安全性をチェックするために、既存のチェック情報はローカルキャッシュを優先的に確認し、最新の情報はGlobal Viewを利用して検査を行います。
4. 一般的に99%以上の検査は、ローカルキャッシュで判定されるので不必要なネットワーク帯域の使用を最小限に抑えます。
5. これを利用する製品はURL FILTERINGで受信したURL情報に応じて許可、ブロックを判断します。

URL FILTERINGの特徴

- 強化された8種類のセキュリティカテゴリ(全64カテゴリ)
- 言語、地域、コンテンツを問わず動作
- 低いリソース使用率で、毎秒50,000件以上のURL検査要求を処理
- 1億4千万件以上の最新URLを保有
- 自動的にローカルキャッシュを調整
- ローカルキャッシュの利用を選択可能

ANDROID MOBILE SECURITY

2012年CYRENの分析チームは、毎月6,000件以上の新種のマルウェアを発見し、現在もマルウェアは急激に増加しています。CYRENのANDROID MOBILE SECURITYは急増しているモバイルの脅威に対処するために、セキュリティ開発者およびモバイルサービス会社に他社と差別化した製品を提供しています。

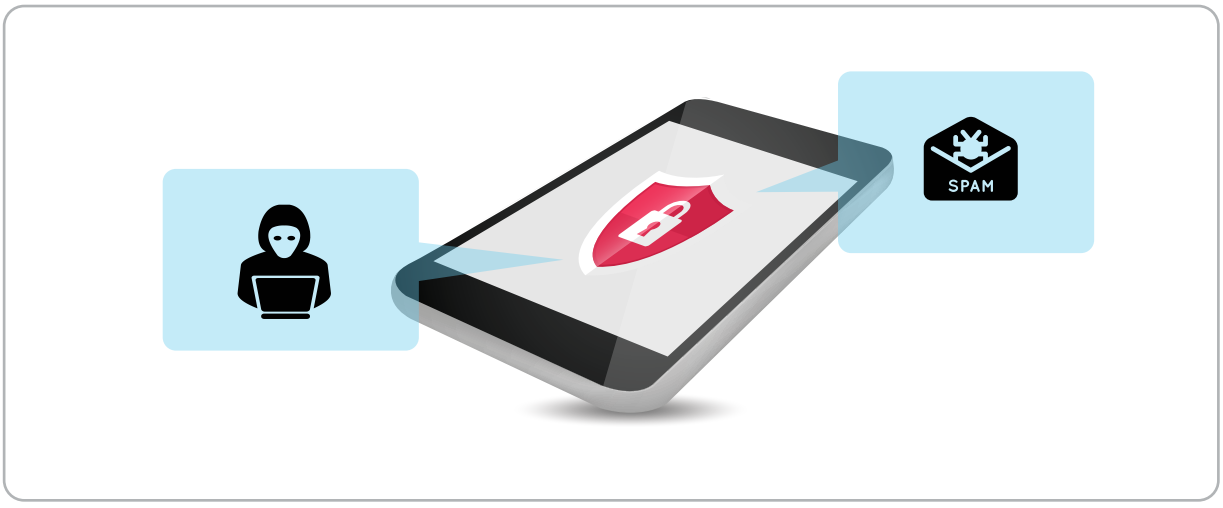
統合セキュリティ機能の提供

ANDROID MOBILE SECURITYはAndroidデバイス向けの統合セキュリティ機能を提供し、WEB上の脅威から機器を守ります。

- マルウェアの検出、不正なURLブロックと潜在的な攻撃の検出
- GlobalView Cloud分析：CYRENのGlobal View Cloudは、毎日数十億件のフィッシング、マルウェア、スパムメール、Web攻撃などを分析しており、分析されたデータは各ベンダーにリアルタイムに提供しています。

メリット

- 高性能検出エンジン：CYRENのGlobal View技術をベースにアンドロイドに最適化されたヒューリスティック、シグネチャ、クラウド検出エンジンを提供。
- 不正なURLをリアルタイムブロック：SDKに含まれているWebセキュリティ機能を利用して、リアルタイムに不正なURLをブロックします。
- 迅速かつ簡単な統合：応用製品に迅速かつ簡単に統合できるように設計されています。
- ユーザーの不便を最小限に抑える：低いリソース消費（メモリ、帯域幅、バッテリー）や、小さなシグネチャファイルによりユーザーの不便を最小化。
- 販売領域の拡張:企業のセキュリティコンプライアンスに適応した、有害サイト遮断アプリなどを開発できます。
- 差別化された製品の供給により各ベンダーの市場シェアの増加と売上高の成長を支援します。

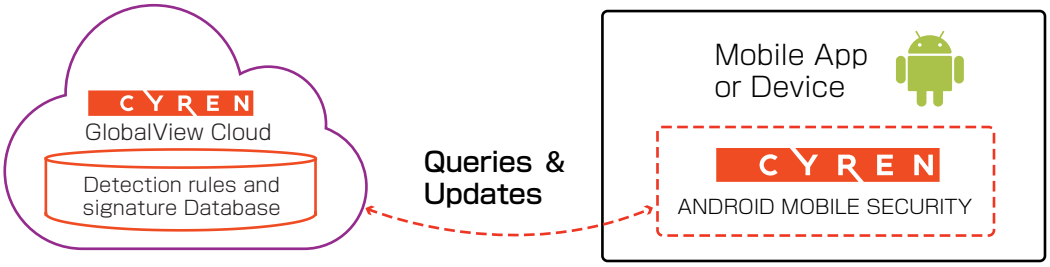


ANDROID MOBILE SECURITYの応用分野

- MDM / MAM
- 企業向けセキュリティアプリ
- モバイルアンチウィルス
- 有害遮断アプリ
- 金融アプリ
- Software-as-a-Service (SaaS)

柔軟でシンプルな実装方法

ANDROID MOBILE SECURITYエンジンは、OEM製品のためのセキュリティ製品です。
CYRENは、各OEMメーカーがさまざまなビジネスモデルを用意し市場シェアと売上を増加するために、柔軟かつ迅速に自社製品にセキュリティ機能を実装できるように支援しています。OEM市場のために特別に設計されたANDROID MOBILE SECURITYは、強力なアンチウィルスおよびWebセキュリティ機能を、MDM / MAM、セキュリティアプリ、クラウドサービスアプリ、キャリアや端末メーカーに提供します。



CYRENエンジンは、高速検出機能と新しい脅威への対応機能を容易に強化･拡張できるようにモジュール化フレームワークに基づいて設計されています。これは、急増するモバイルマルウェアへの対応に特に有効です。フレームワーク内の各脅威防止モジュール(PDF検査モジュール、Polymorphicウィルス検査モジュールなど)は、様々な形態の脅威について迅速に検出することが可能です。ANDROID MOBILE SECURITYを使用することで悪質なコードの検出、不正なURLを検出することができ、CYREN独自のGlobal View Cloudの技術を利用してリアルタイム更新を行うことができます。

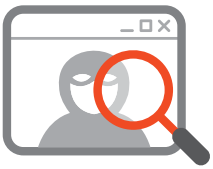
ANDROID MOBILE SECURITYの特徴

- マルウェアの検出
  Global View Cloudとローカルが連携しスキャン
- ルーティング検査
- 圧縮ファイル検査
- Webセキュリティ：不正なURLのチェックとURLカテゴリ分類
- エンジン、シグネチャの自動更新
- 少ないリソース消費(メモリ、帯域幅、バッテリー)
- シンプルなAPIを利用した詳細な検出結果のフィードバック
- File, Apps(apk), SMS/MMS, メールの添付ファイルのチェック
- Android専用のシグネチャファイル
- Android 2.2 以上全てのバージョンに対応

PHISHING URL FEED

CYREN セキュリティアライアンスとの連携とGlobalView Cloudで収集および分類したPhising URLを毎日CYREN クラウドデータベースに追加します。この脅威データは世界最高水準のグローバルセキュリティベンダとサービスプロバイダがユーザを守るために使っています。

特長



差別化された方式

- 多数のSub-domainを持っているサイトを探す。
- 知られているPhising Keywordを探す
- Fuzzy Logic検知アルゴリズムを適用
- 疑わしいPhising URLを確認して検知の正確性を高めるためにルールを詳細に調整可能

持続的かつ瞬時にPhisingから守る

- CYRENにより持続的かつ瞬時に提供される大量の正確なPhisingデータを使うことで他社と差別化されたサービスを提供可能
- 現在のアンチスパムもしくはURL Filteringのソリューションと簡単に連携できます。

増加するPhising攻撃から防御

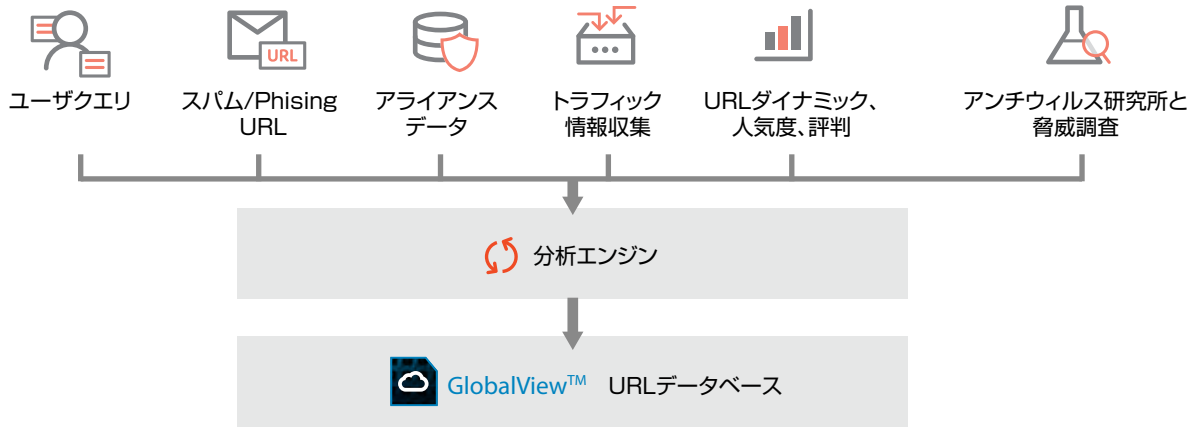
- CYREN　Phising URL Feedはスマートフォンとタブレットを含む全てのデバイスを新しい脅威から守ります。
- 新しいPhisingの脅威が発生した時には、CYRENの顧客にリアルタイムで情報を提供します。

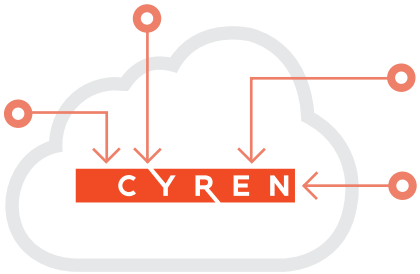
最高の情報提供

- CYRENのデータベースは、関連業界のデータベースの中で世界最大規模です。CYRENは毎日未知のPhisingの脅威にリアルタイムに正確な検知を実現する為に、200か国以上から230億件以上のインターネットトラフィックを分析します。

重要機能

幅広いカバレッジと精度の高さ





GlobalView クラウドデータベース

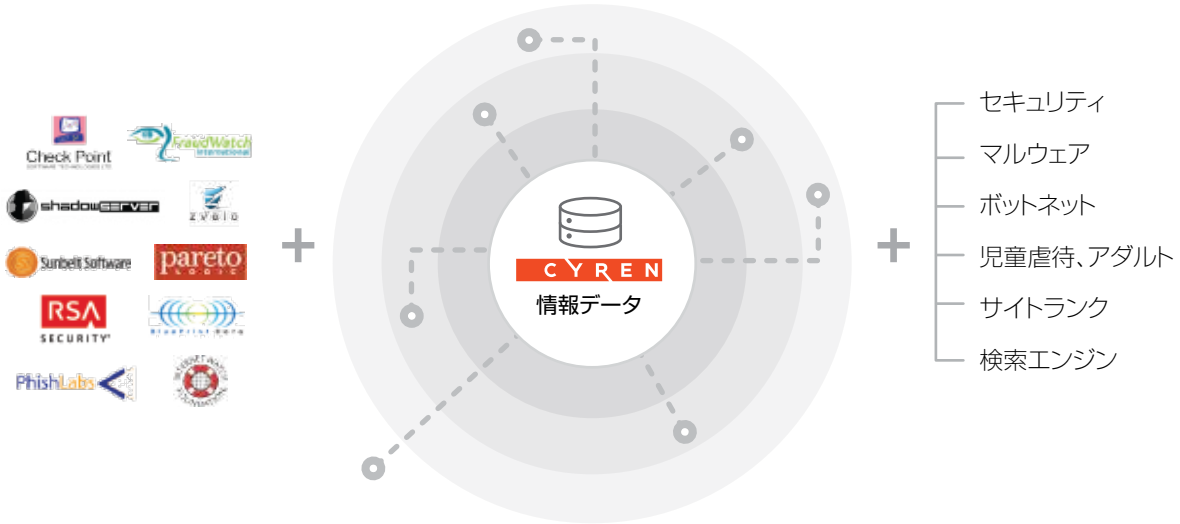
最も関連性があるウェブカバレッジ

確実な自動学習

全てのCYREN製品を通じて収集され共有される情報

セキュリティアライアンスで拡張されるCYRENデータ

200社以上のアライアンスのデータ + CYREN情報データ



SANDBOX ARRAY

進化し続けるAPT攻撃と悪性コードおよびランサムウェアなどは既存ウィルス対策とSandboxを迂回して攻撃します。
CYREN Sandbox arrayのグローバルデータ収集と検知および分析技術は、未知のAPT攻撃と悪性コードに最も早く効果的に対応できます。

特徴

検知性能

- 多様なOSで同時比較および分析
- 物理ハードウェア比較分析
- AI技術をベースとして自動化された分析
- マルチ分析により隙の無い検知力を提供

無限システム拡張およびクラウドサービス

- どんな場合でも止めない高可用性
- ピークタイムでも性能低下がない安定性
- 世界19箇所のデータセンター運営により、迅速で正確な分析
- 保守不要

迅速な分析スピード

- 多様なOS環境で同時に動的分析することで最も早い分析レポートを提供
- 全世界で最も多い分析データベースを保有

詳細なレポート

- 多様な環境で分析された結果を統合レポートで提供
- 脅威レベル、ファイル分析結果などを提供して統合脅威情報をレポート

適用分野

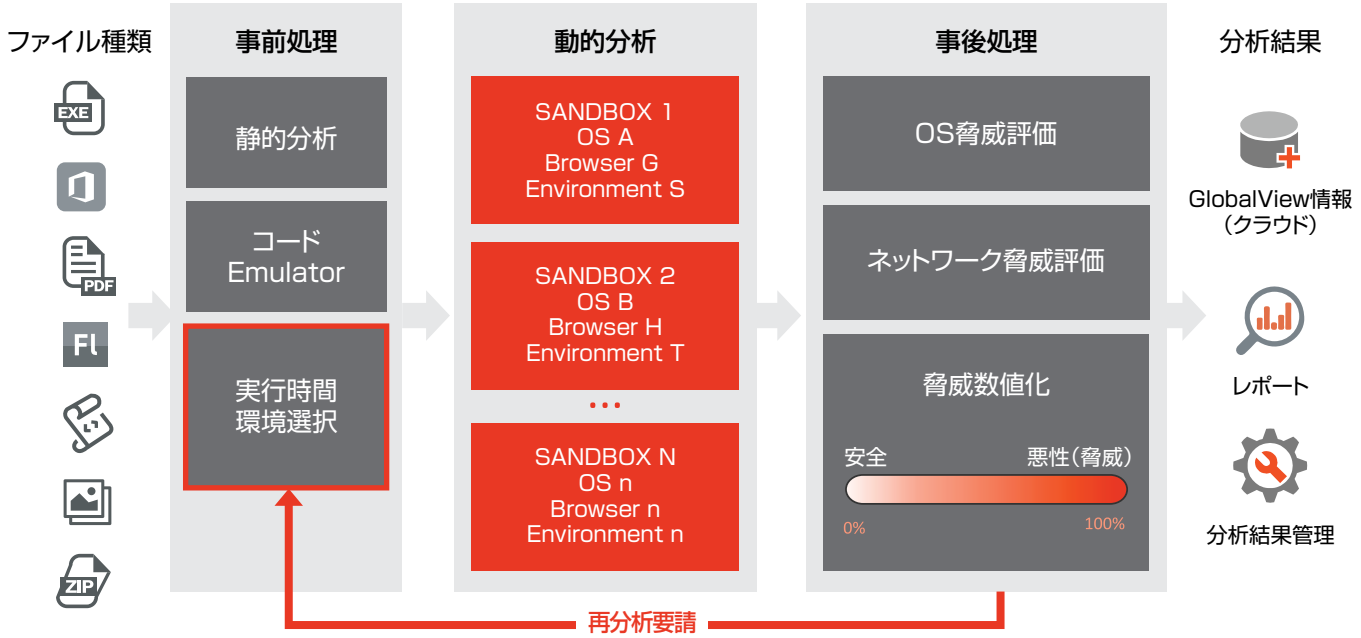
*脅威インテリジェンスサービス(クラウドOEM)

- Threat Lookup/Sandboxサービス
- インターネットセキュリティに連携(SWG/SEG/UTM), MSSPs, ISPs

*企業用Sandboxサービス

- SOC(Security Operation Centers)と連携
- 既存セキュリティサービスと連携

Sandbox array 動作方式



1 予測分析
予測/静的分析技術で
対象ファイルの予想行動を
予想して適合な
Sandbox arrayを選択

2 動的分析
選択された各Sandboxから
動的分析を実行して悪意的な
行動監視および全ての行為予測

3 総合分析
多様なOS、ブラウザ、仮想環境、
物理環境などで分析された異常
行為、行動分析結果を総合的な
脅威スコアとして判断

4 情報提供
分析された結果をベースに
レポートを作成して提供

Sandbox array サービスレベル

ハッシュ検査ベースの脅威検知

ヒューリスティックおよびシグネチャベースの精密脅威検知

Sandbox Arrayによるファイル精密分析

統合レポート、IOCなど提供

Sandbox　プレミアム
(全てのファイルをSandbox分析)

Sandbox array のメリット

- APT 攻撃に対する完璧なライフサイクルを提供
- 要求するセキュリティレベルによって段階別選択導入可能
- 最も効率的な費用構成で柔軟に提供可能

総代理店

JSECURITY

株式会社 JSecurity

東京都港区東新橋二丁目12番1号 PMO東新橋7階

TEL:03-6826-1915　FAX: 03-6826-1916

E-mail : sales@jsecurity.co.jp

URL : https://www.jsecurity.co.jp

お求めは信頼の