KeepEyeのご紹介

S&J株式会社

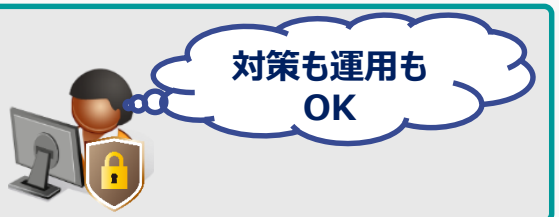
KeepEyeのサービスコンセプト

背景

- ✓ 高度化するサイバー攻撃を従来のFirewallやウイルス対策ソフトで防御することは困難になっています。
- ✓ 一方で、高度なサイバー攻撃を防御するセキュリティ専門家が運用する前提のツールが複数のベンダーから提供されるようになっていますが、各企業でそのツールを運用するセキュリティ専門家を雇用するのが難しく、実際運用ができずに、ツールを導入しただけになっていることがほとんどとなっております。

KeepEyeのサービスコンセプト

運用のほとんどをセキュリティ専門ベンダーのS&Jが行うことにより、「お客様にてセキュリティ専門家を雇用しないで最小限の運用」で、高度なサイバー攻撃への対策運用が実現できます。



KeepEyeの仕組み

- ✓ KeepEyeエージェントやS&J監視センターで、検出した脅威をリアルタイムで対処(プロセス停止やファイル群の隔離)を行い、ユーザや管理者に通知を行います。

- ✓ 脅威への対処が終わっているため、お客様は検出された脅威に対するログの分析や対処を行う必要はありません。また、脅威が誤検知だった場合のファイル復旧作業もS&Jに依頼するだけで済みます。
お客様にて運用していただきたい内容は、『KeepEye 簡易運用マニュアル』にてご案内いたします。

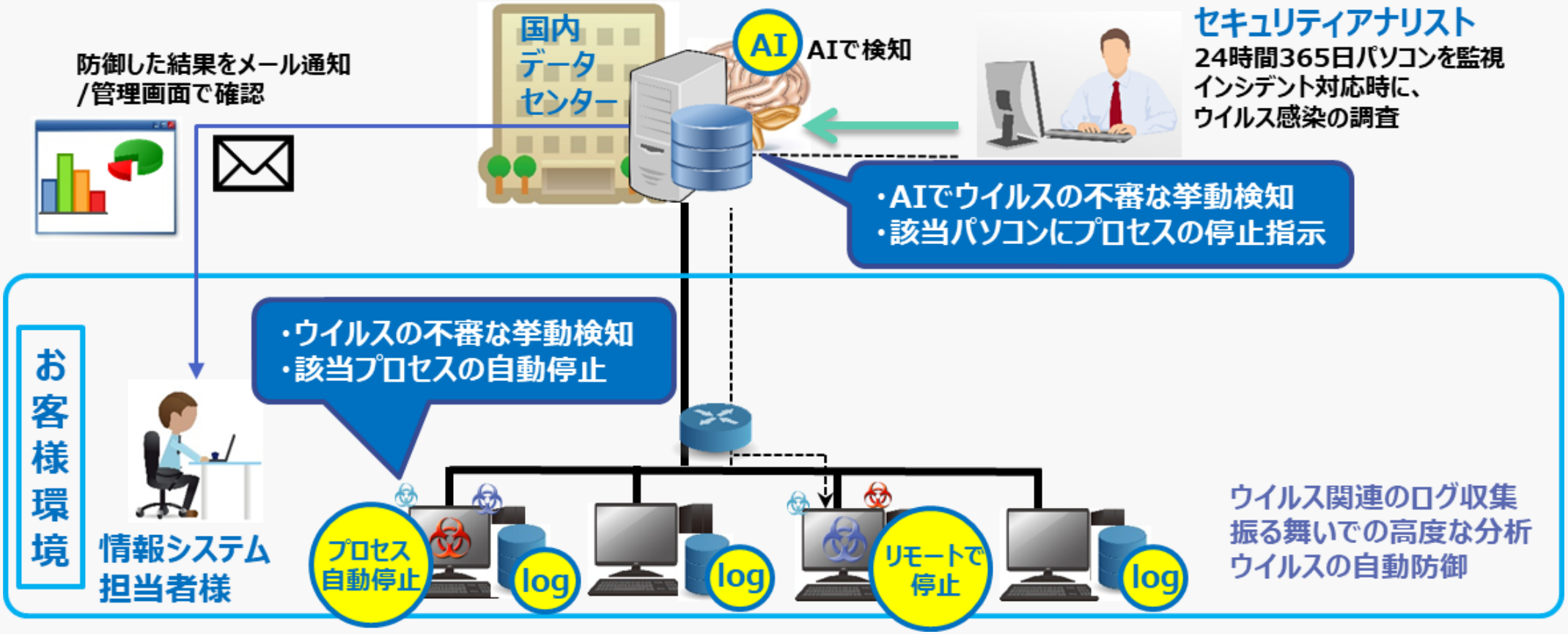
- ✓ KeepEyeはログの蓄積を行っておりいざという時に端末で何が起こっていたかのログや検体の分析をS&Jアナリストが行い、必要に応じて、リモートから対処（検体群隔離や端末隔離）まで行えます。

KeepEyeのサービス全体イメージ

KeepEyeの検知機能として、端末内のプロセス等の振る舞いを独自の検知ロジックにより検知する機能と、組織全体の中で特異な動作をするPCを検知するためにSOC Engineクラウドに集約された各端末のプロセス起動情報を横断的にAIで分析した内容をアナリストが監視を行います。

脅威があると判断した検知事象は、自動で防御を行います。お客様は、管理画面で防御状況などを確認することができます。

さらに、KeepEyeがインストールされている端末では、プロセス等の動作をログとして保存しています。IR Advanced では、アナリストがプロセス等の動作のログを分析しマルウェアの生成履歴などを調査し、必要に応じて検体ファイルをアナリストが遠隔操作により抽出/分析をします。



KeepEyeの２つのサービス

サービス

KeepEyeは、**EDR** と オプションの**IR Advanced** の2種類のサービスがあります。

EDRサービスは、振る舞い防御のEDR機能やAIとアナリストによる監視、ローカルに各種ログを一定量（1GB）保存する機能等をご利用できるサービスを提供します。お客様が管理画面の検知状況を確認し、正規のプロセスが検知されていることが判明した場合は、S&Jが検知対象外リスト（ホワイトリスト）へ登録します。

IR Advancedサービスは、マルウェア感染の疑いがあった場合に、お客様から詳細の調査依頼に応じて弊社アナリストが端末上に保存しているログや検体の取り出しをリモートで実施して、調査分析を行うチケット制のサービスを提供します。

各機能/サービス	EDR	IR Advanced
端末上の振る舞いからマルウェアの検知・防御する機能	○	–
クラウド上のAIを用いてマルウェアの検知する機能	○	–
AIで検知した脅威を、24時間365日でアナリストが監視して防御するサービス	○	–
PCのログ（Webブラウザ以外で接続したドメイン等）を端末内に保存（1GB）する機能	○	–
防御結果のメール通知機能 / 管理画面機能	○	–
防御した内容が誤検知の可能性がある場合の問合せ対応やホワイトリストに登録するサービス	○	–
防御した脅威について、念のため影響がなかったかの検体やログの分析を依頼するオプションサービス	–	○

KeepEye　運用簡易マニュアル

KeepEyeが防御モードで運用が開始した後に、お客様にて対応頂きたいのは以下の2点となります。

1．　KeepEyeが誤検知した場合の対応

1．対応が求められるシチュエーション

①ユーザから利用したいソフトウェアを実行した際に、
KeepEyeが実行を停止したメッセージが
通知されて、使えなかったと連絡があった場合
※管理者にもメールで通知されます

②管理者宛にメールでKeepEyeが対処した通知された内容を確認したところ、プロセス停止/ファイル隔離されたファイルが自社の業務で利用するソフトウェアだった場合 等

2．お客様の管理者様の対応

上記１が発生した場合、管理者に届いたメールに対して以下の文言を記載して、返信してください。
「誤検知のため、確認して、ホワイトリストに登録してください」

3．S&Jからの対応結果の通知

ご依頼内容に対しての対応結果を、S&Jから返信します。
＜対応結果＞
次回以降検知しないようにホワイトリストに登録を行い、また検知した端末に対して隔離したファイルを元の場所に戻す対応を行った

2．KeepEyeが対処した重要端末の詳細分析依頼

1．対応が求められるシチュエーション

管理者宛にメールでKeepEyeが対処した通知された内容を確認したところ、対処された端末が自社の重要端末だった場合に事業継続上問題がなかったか、念のため確認したい場合
【重要端末例】
役員端末、経理端末、個人情報を大量に保有する端末、　研究開発部門端末　等

2．お客様の管理者様の対応

上記１が発生した場合、管理者に届いたメールに対して、以下の文言を記載して、返信してください。
「重要端末のため、IR Advancedのチケットを消費して、詳細分析をお願いします」

3．S&Jからの対応結果の通知

依頼を基にログの分析や検体の調査などの詳細分析を実施し、調査結果の報告書を、メールにて送付します。

KeepEye　導入ガイド

KeepEyeをご導入の際に、以下のご対応をお願い致します。詳細は、サービス仕様書をご確認ください。

1．　本番運用（防御モード）までの手続き

1．利用者申込書_問診票提出

利用者申込書_問診票をご記載頂き、提出をお願いします。

2．管理画面ログイン･パスワード変更

S&Jから提供された管理画面のアカウント情報で、管理画面にログインを行ってください。管理画面ログイン後に、管理画面のログインパスワードを任意のパスワードに変更してください。

3．検知モードでの動作テスト

KeepEyeインストール後に、動作不良などありましたら、製品サポートにご連絡ください。1か月間検知モードでS&Jが動作テストを行い、報告書を提供します。

4．ホワイトリスト案の確認

動作テスト終了後の報告書内に問題ないと考えられて監視対象外とするソフト一覧（ホワイトリスト）をご案内しますので、ご確認お願いします。

5．防御モードへの切り替え承認

報告書の内容が問題ないようでしたら、本番運用となる防御モードにS&J側で切り替えます。承認をお願いします。

2.お客様環境の対応

1．KeepEyeサーバへのアクセス確認

KeepEyeサーバへアクセス可能か確認をお願いします。アクセスできない場合は、設定変更をお願いします。

・管理画面を利用する端末のアクセス確認
管理画面を提供するkeepeye.jpドメインに対して宛先ポート番号5601を利用したSSL/TLS通信が可能か

・KeepEyeをインストールする端末のアクセス確認
サーバーに対して宛先ポート番号443を利用したSSL/TLS通信が可能か

2．PCのウイルス対策ソフトへのホワイトリストに登録

ウイルス対策ソフトがKeepEyeを誤検知してしまう可能性があるため、KeepEyeの動作を許可する設定をしてください。

3．PCにKeepEyeへのインストール作業

上記１と２の対応後に、KeepEyeのインストールを実施してください。

KeepEye　試用版の導入の流れ

試用版は、KeepEyeの導入をご検討されているお客様にお試し利用していただくためにご提供します。

なお、試用版のため、検知モードのみでのご提供となります。

試用版の利用申込書_問診票を弊社にご送付頂けましたら、その後の対応は弊社側にて進めさせて頂くことを想定しております。

試用期間（1か月）が終わってから10営業日目を目途に、S&Jから試用版の報告書を提出します。

＜管理画面でダウンロードできるもの＞

・管理画面利用マニュアル
・インストーラー
・インストールマニュアル
・サービス仕様書（最新版）

S&J

サイバーセキュリティのプロ集団として、
お客様のネットワークを守ります。

S & J 株式会社
〒105-0003
東京都港区西新橋1-18-17 明産西新橋ビル8階
TEL：03-6205-8500 FAX：03-6205-8510
sales@sandj.co.jp
www.sandj.co.jp