”気づき”を提供する　マルウェア・センサー

VISUACT-V

アズビル セキュリティフライデー株式会社

※この資料中では、直感的にご理解をいただくために、あえて「マルウェア」ではなく「ウィルス」という用語を使って説明している部分がございます。

azbil

制御システムのセキュリティ対策に困っていませんか？

セキュリティ対策を施したくても施せない
- 独自にセキュリティ対策を施すと制御ベンダーから保証が受けられなくなる／対策を禁止されている
- 制御システムにセキュリティを加えると運転に悪影響が無いか心配だ

→ 制御システムに悪影響を与えないセキュリティ・ソリューションを探している

セキュリティ調査を専門家に依頼したいが、制御システムに手を加えられては困る
- セキュリティ専門家は制御システムの運用の実態を理解していない
- 稼働中の制御システムに調査作業が行われると、運転に悪影響がないか心配だ

→ 制御システムを直接操作すること無く調査を行うことは出来ないか？

トラブルシュートが描けない
- ウィルスやセキュリティ問題が発生したとき、どんな現象が起きるのか分からない／知らない
- 経験がないのでトラブルシュートが描けていない

→ トラブルの原因がセキュリティ問題かもしれないと疑う「気づき」が欲しい

万が一侵入されてしまっても被害は最小限に抑えたい

→ ウィルスの侵入やセキュリティ問題を出来るだけ早期に検知したい

制御システム　セキュリティ対策の課題

azbilの目指すソリューション

VISUACT-Vは

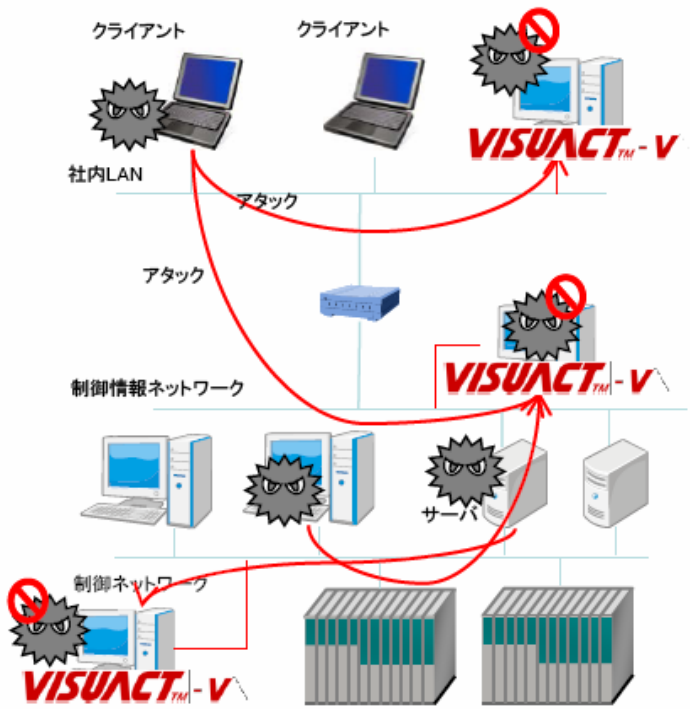
制御ネットワークにおいて
ウィルスの活動を検知する「マルウェアセンサー」

◆機能

- 内部に侵入したウィルスの活動をいち早く検知します
- ウィルスの検体を安全に捕獲出来ます

◆特長

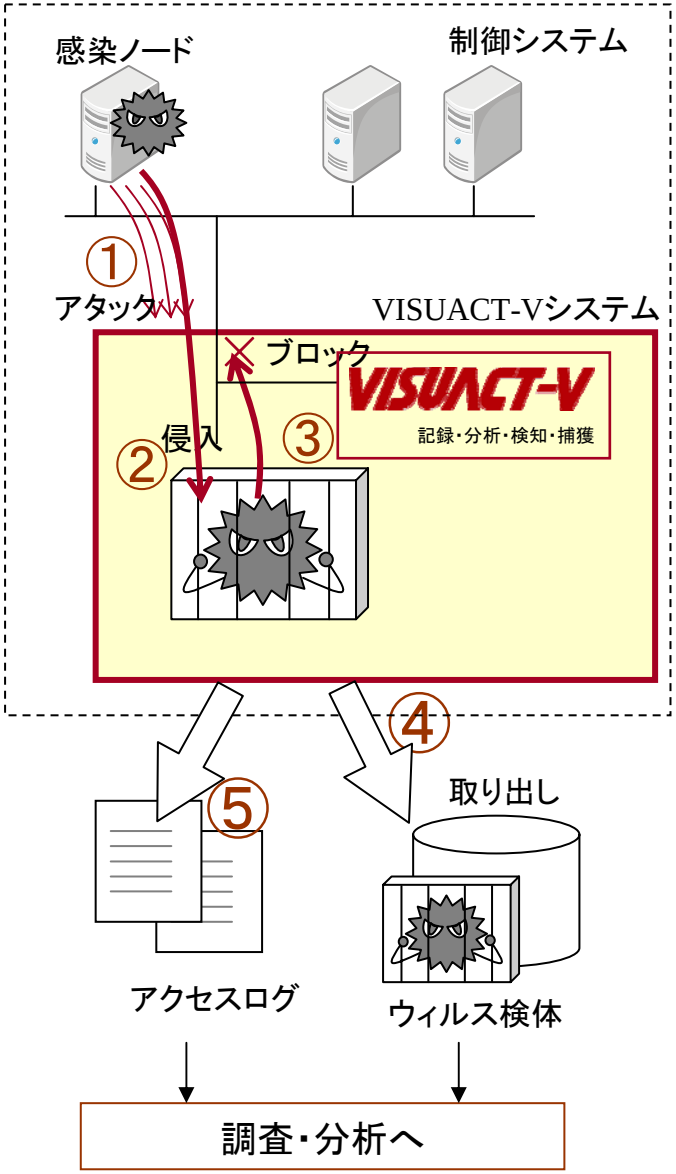
- VISUACTテクノロジーによりネットワークを監視／分析し、ウィルスの攻撃をいち早く検知し、通知します。
- 稼働中の制御システムでも安全に着脱できます。
  - ネットワークに接続するだけで使用出来ます
  - 制御ノードのへのソフトウェアのインストールが不要です。また、ネットワークへの通信負荷は一切ありません
- ファイヤーウォール機能により、捕獲したウィルスによる制御ネットワークへの攻撃を完全にブロックします。
- 捕獲したウィルスをPCイメージごと安全に取り出すことができます。



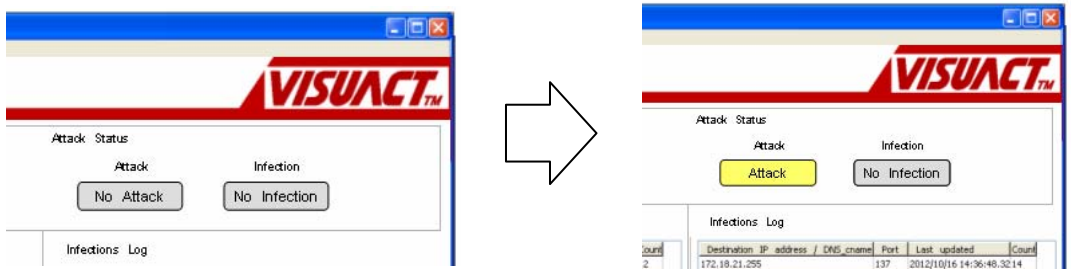
VISUACT-Vが提供する価値

- 気づき
  - 制御システムのトラブルシュートに、セキュリティ問題かもしれないという「気づきを提供」することで、セキュリティ問題に対応したトラブルシュートの構築が可能になります。
- セキュリティ調査の為の環境の提供
  - VISUACT-Vのデータを元に、セキュリティ専門家が、制御システムを直接操作すること無く、詳細調査を行うことが可能になります。
    - 未知のウィルスによる攻撃の場合でも、その検体を捕獲し、安全に取り出すことが可能です。
    - VISUACT技術により、攻撃（通信内容）の詳細ログを、制御システムの外部（VISUACT-V内）に記録します。
- 早期発見
  - ウィルスやハッカーによる活動や内部攻撃をいち早く発見します。

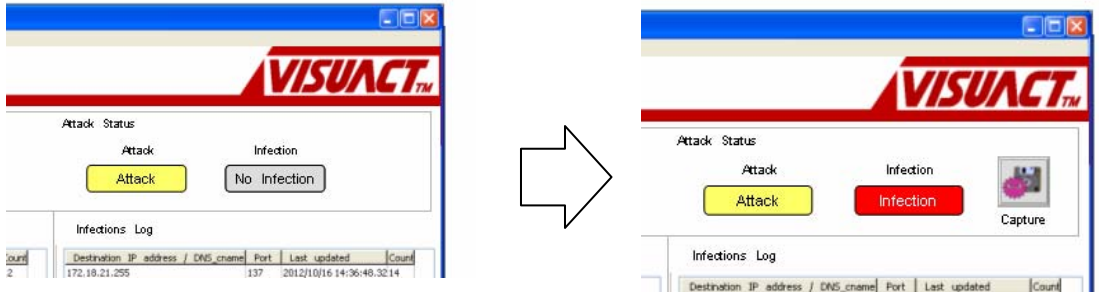
VISUACT-V機能イメージ



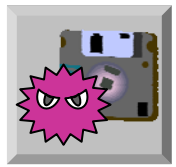
①攻撃→内部へのウィルスの侵入を検知



②侵入
③感染（拡散活動はブロック）

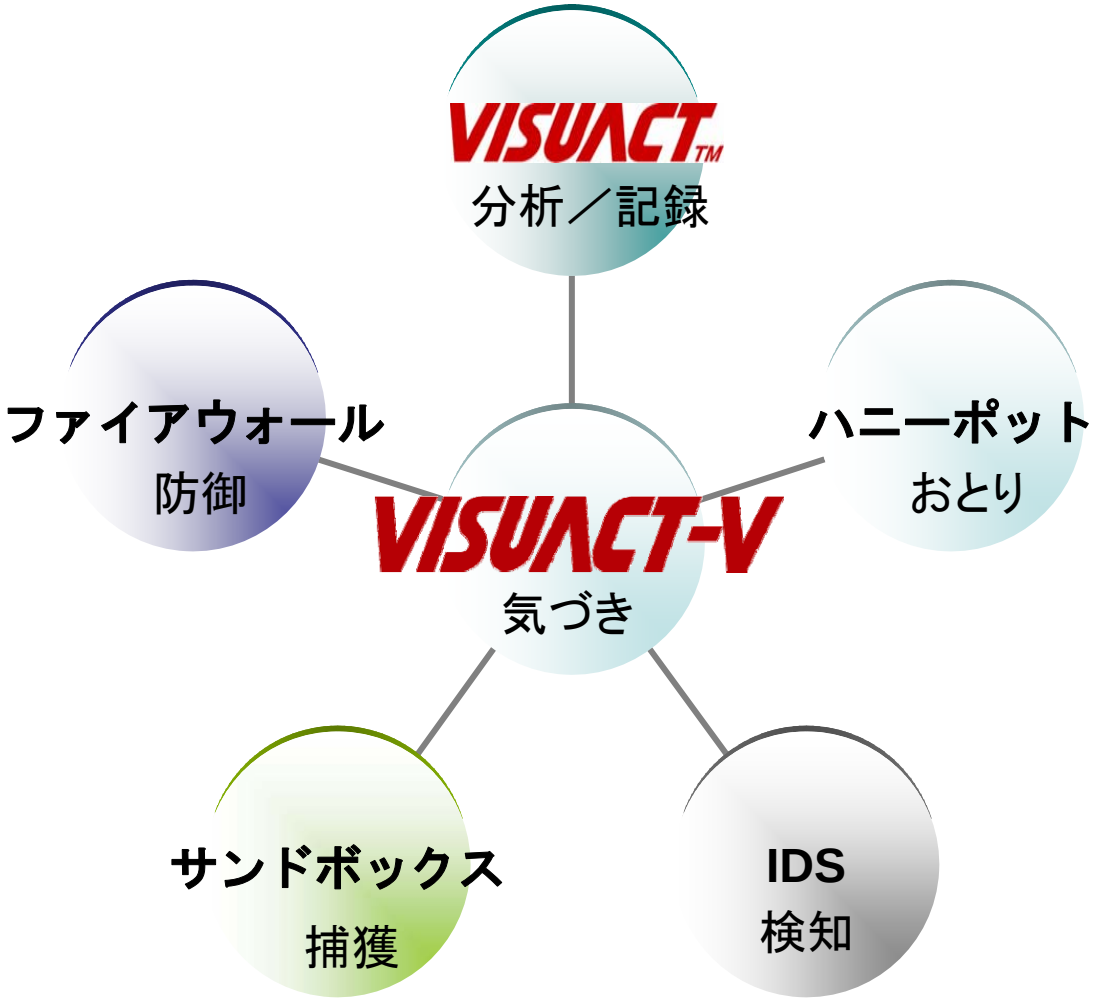


④ウィルスの検体を保存（捕獲）



⑤アクセスログを出力

VISUACTーV　テクノロジー



VISUACT-V　スクリーンショット