〇参考資料

【CSV の各フィールドについて（具体的な意味)】

・INDICATOR_VALUE：兆候を示す具体的な情報
・TYPE：情報の種別（ドメイン、E メール関連、IP アドレス、URL 等）
・COMMENT：コメント
・ROLE：用途（ドメイン監視、IP アドレス監視、メッセージ ID 監視、メール件名監視、URL 監視）
・ATTACK_PHASE：攻撃の段階
・OBSERVED_DATE：これらを利用した攻撃の観測時期
・HANDLING：情報の公開・共有範囲
・DESCRIPTION：詳細説明

【活用方法（例)】

・TYPE が FQDN、IP、URL の INDICATOR_VALUE を Proxy の接続拒否リストに設定して、不審サイトへのアクセスをブロックする
・TYPE が FQDN、IP、URL の INDICATOR_VALUE を Proxy ログ上で検索して、過去にアクセスした職員がいるか調査する
・TYPE が EMAIL の INDICATOR_VALUE をメールセキュリティ装置の隔離リストに設定して、自動隔離する
・TYPE が EMAIL の INDICATOR_VALUE を内部メールサーバログ上で検索して、過去に職員が受信し開封したメールを調査する

【活用形態】

・何らかのセキュリティ装置やネットワーク機器に上記情報を投入して活用する形態となります。