インシデント実対処から見える活きたログ

2015年11月19日

セコムトラストシステムズ株式会社
サイバーセキュリティ室
加治川 剛

自己紹介

- **氏名**
  加治川 剛（かじかわ ごう）
- **所属**
  セコムトラストシステムズ株式会社
  サイバーセキュリティ室
- **主な業務**
  ・サイバー攻撃の手口調査、解析、対策検討・評価
  ・サイバーセキュリティ事故の緊急対処（サイバー消防団）
  ・サイバー道場（社外IT担当者向け講習）の講師

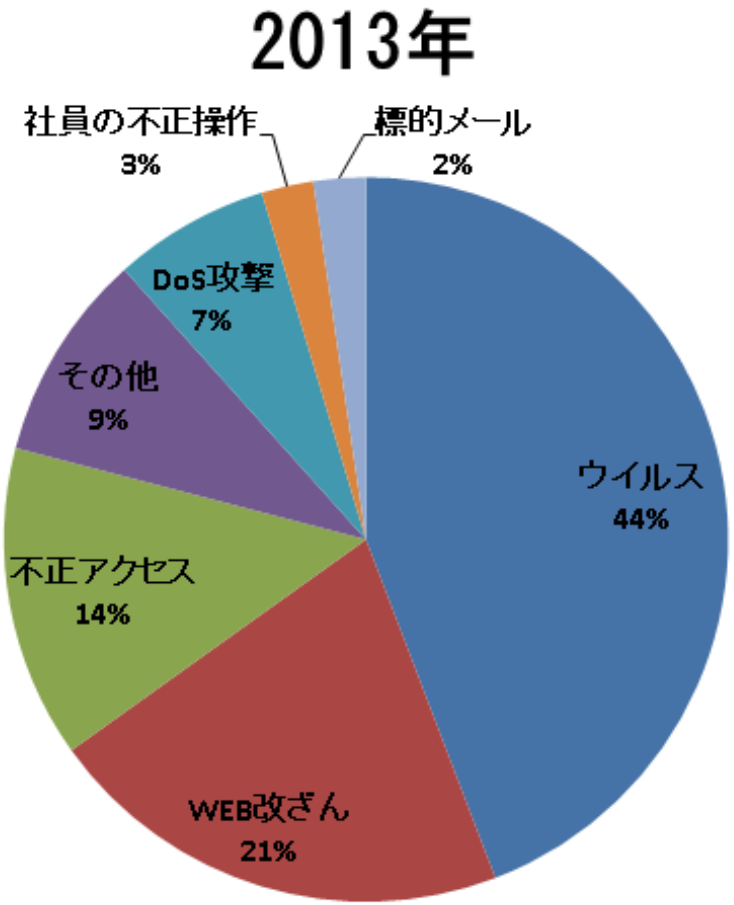
- **セコムトラストシステムズ株式会社**

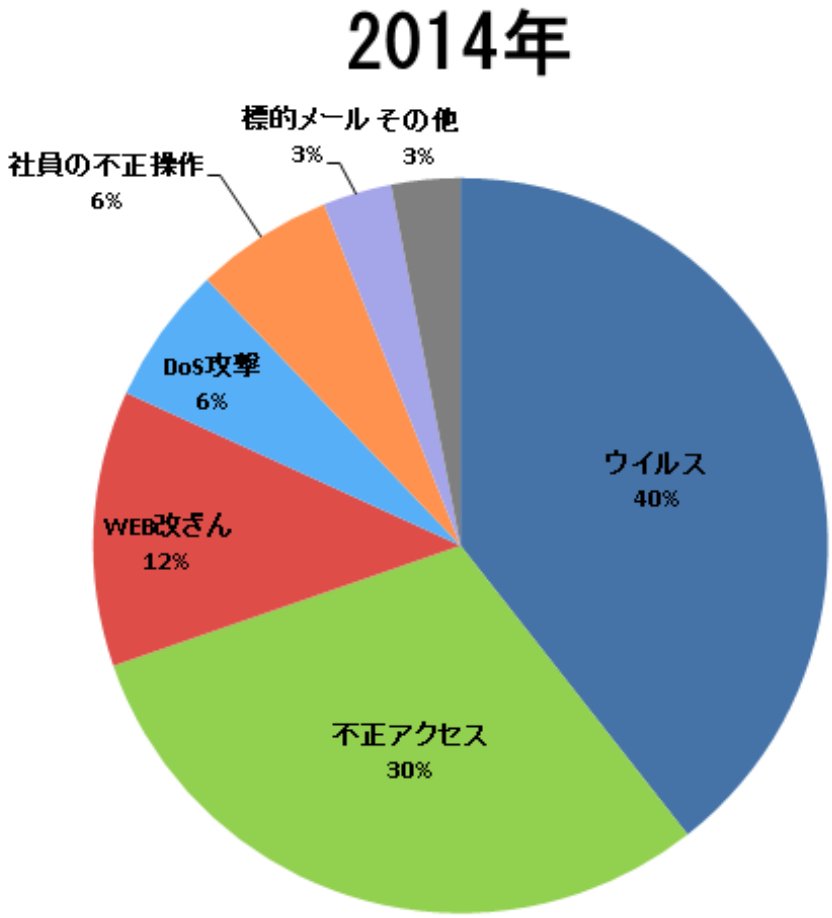
セコムトラストシステムズは、セコムグループの情報・ネットワークシステムの構築・運用を担うと共に、ここで培った技術力・運用力・ノウハウをベースとして、情報セキュリティ事業、データセンター事業を主力に、それぞれが緊密に連携し高品質なサービスを提供しています。

セキュアデータセンター（SDC）

緊急対処時の要望

緊急対処問合せの統計





- 2014年になりランサムウェアに関する問合せを受けるようになった
- 2013年に問合せの多かったWEB改ざんに関する問合せが減少

サイバー攻撃兆候の検出例

・攻撃による影響の確認
　⇒ランサムウェアによるファイルの暗号化・破壊
　⇒スパム送付により、自社IPアドレスがブラックリストへ登録される

・外部機関からの連絡
　⇒警察、JPCERT、IPAなどの組織より、ウイルス感染の連絡を受ける

・ウイルス対策ソフトによるウイルス検出
　⇒ネットワーク上のウイルス対策製品による検出
　⇒ホスト上のウイルス対策製品による検出

・NWログの監視による検出
　⇒FWログ
　⇒プロキシログ
　⇒IDS/IPS等のシグネチャによる検出

緊急対処時の要望

具体的要望

- マルウェア感染端末の特定
- マルウェア感染有無の確認
- マルウェア感染原因の特定
- サイバー攻撃による影響の特定

アドバイス・その他

- 対応の方向性が合っているか
- 対応に抜けが無いか
- どうしていいか分からない

実対処事例（ランサムウェア）

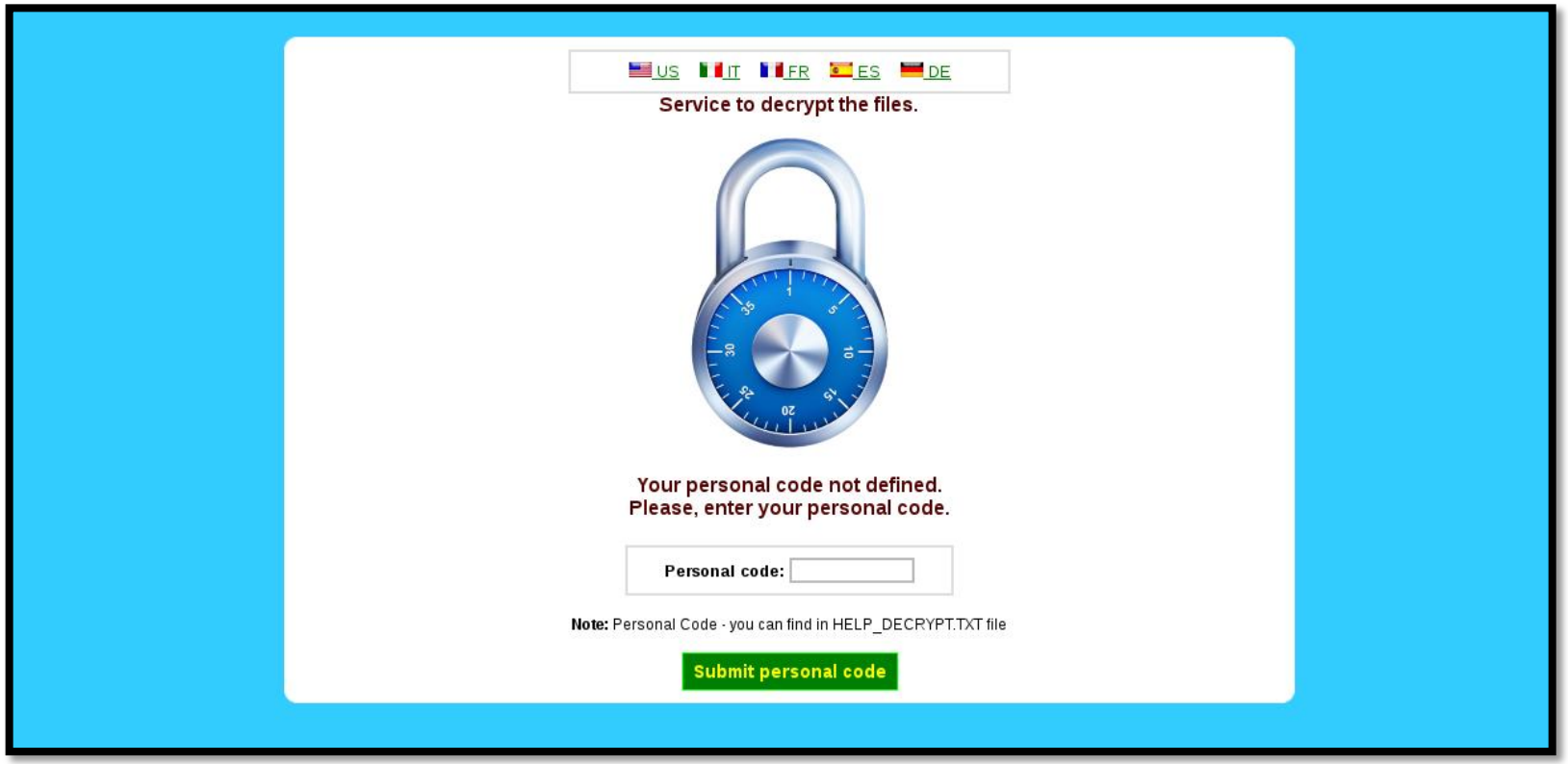
ランサムウェアとは（概要）

・感染によりPCやデータを利用できない状態に変更する
不正プログラムで、攻撃者はPCやデータを人質に見立て、
元に戻すために金銭を要求する。

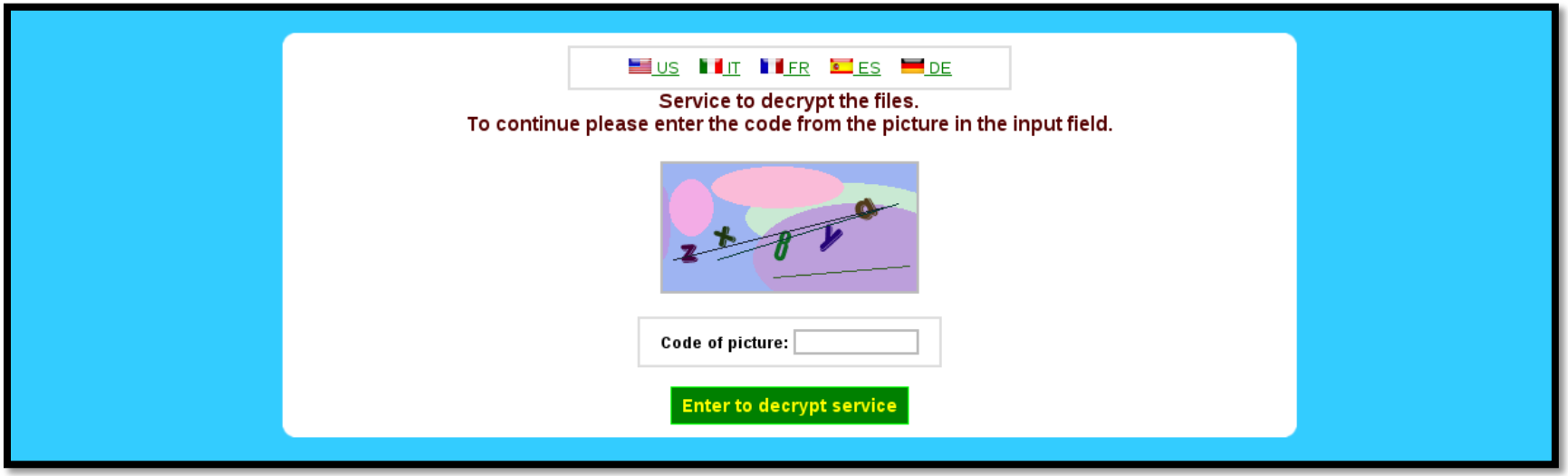
・cryptwallと呼ばれるランサムウェアが日本で流行しており、
多くの問合せを受けている。

・端末内のドキュメントが暗号化されると、同フォルダ内に
HELP_DECRYPTというファイルが「txt」「png」「html」の3つの
拡張子にて作成される

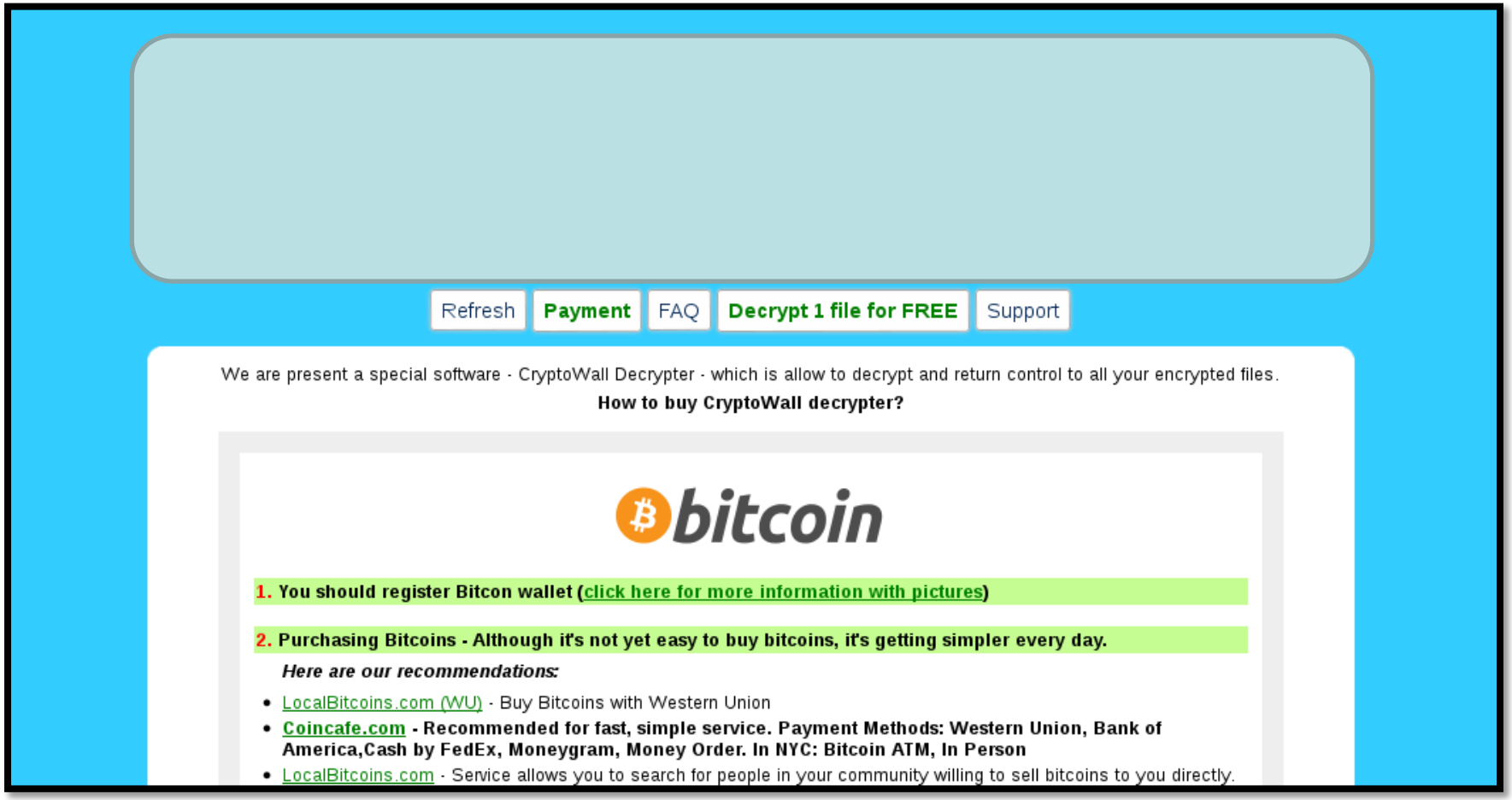
ランサムウェアとは（支払）



ランサムウェアとは（支払）



ランサムウェアとは（支払）



インシデント事例パターン①

■事象

・社内ファイルサーバ上のファイルが壊れて見られない
状況であり、社内から多数の問合せを受けている。
・help_dycryptのファイルが見つかり、調べた結果
ランサムウェアによる被害であることを認識している。

■備考

・ファイルサーバはWindowsサーバOS
・本社は東京、支社は全国に点在しており、該当の
ファイルサーバは全国から利用するもの

■要望

・ランサムウェア感染端末を特定したい

インシデント事例パターン①

ランサムウェア感染端末の特定に活きた情報

①NW上の通信ログ

対象ログ：FW、ルーター、ファイルサーバーなど

ログ閲覧切口：通信量、通信時刻(ファイル更新時刻と照合）

②社員や現場担当者へのヒアリング

ファイルの暗号化(破壊)はランサムウェア感染端末自体でも発生している想定

③暗号化(破壊)されたファイルに注目

ファイルサーバ上の暗号化されたファイルのアクセス権に注目する。

インシデント事例パターン②

■事象

・社内1台の端末にて、ランサムウェアによる被害を検出。
・ランサムウェア被害に合わせ、ネットワークログから
該当IPにマッチしたアラートを検出している。

■備考

・該当端末を使用していたユーザに対する業務上の措置は
完了しており、該当端末を調査してもらいたい

■目的

・ランサムウェア感染の原因を知りたい

インシデント事例パターン②

ランサムウェア感染原因の追跡に活きた情報

①メール添付の実行による感染

- 不正なメール添付の実行履歴を検出
- ゼロデイウイルスの検出

②WEB閲覧によるウイルス感染

- IPSログ：クライアント上ソフトウェアの脆弱性を狙ったログを検出
- WEBアクセスログ：該当時間に海外へ誘導されている
- プログラム実行履歴：WEBキャッシュ上のtmpを実行
- ゼロデイウイルスの検出

まとめ

・ログが取得されていることは調査の大前提。

・ログに残された情報だけでなく、設定や状況、ヒアリング
などの情報も、場合によっては重要な情報になる。

・ログを見る場合には、脅威と結び付けて考える必要がある。
⇒攻撃者目線で考えることが重要

・攻撃者は痕跡を削除する、ということを前提に考え、
ログ情報は同種のログであっても複数取得していることが
望ましい。

ご清聴ありがとうございました。

信頼される安心を、社会へ。

SECOM

セコムトラストシステムズ株式会社