現場対応から見えたWEB改ざん事案

セコムトラストシステムズ株式会社
2013年8月22日

アジェンダ

- はじめに
- WEB改ざん対応事例の紹介
- 現場対応から見える問題
- 対策の注意点

会社紹介

Total Information Service

セコムトラストシステムズ株式会社

Secom Trust Systems Co.,Ltd.（略称:STS）

■設立:1985年(昭和60年)8月
■代表者:代表取締役社長　伊藤　博
■年間売上高:262億円(2011年3月期)
■社員数:837名(2011年3月31日現在)
■資本金:14億6,880万円
■URL:http://www.secom-sts.co.jp/

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ㈱

- 情報セキュリティと大規模災害対策をコアとしたトータル情報サービス会社
- ITをうまく活用して便利・快適・効率化を進めるとともに、あらゆる「不安」の無い社会実現を目指します

セコムプロフェッショナルサポート

Total Information Service

お客様の緊急事態にセキュリティのプロとして駆けつけ、事業継続、事業復旧を強力にサポートします。

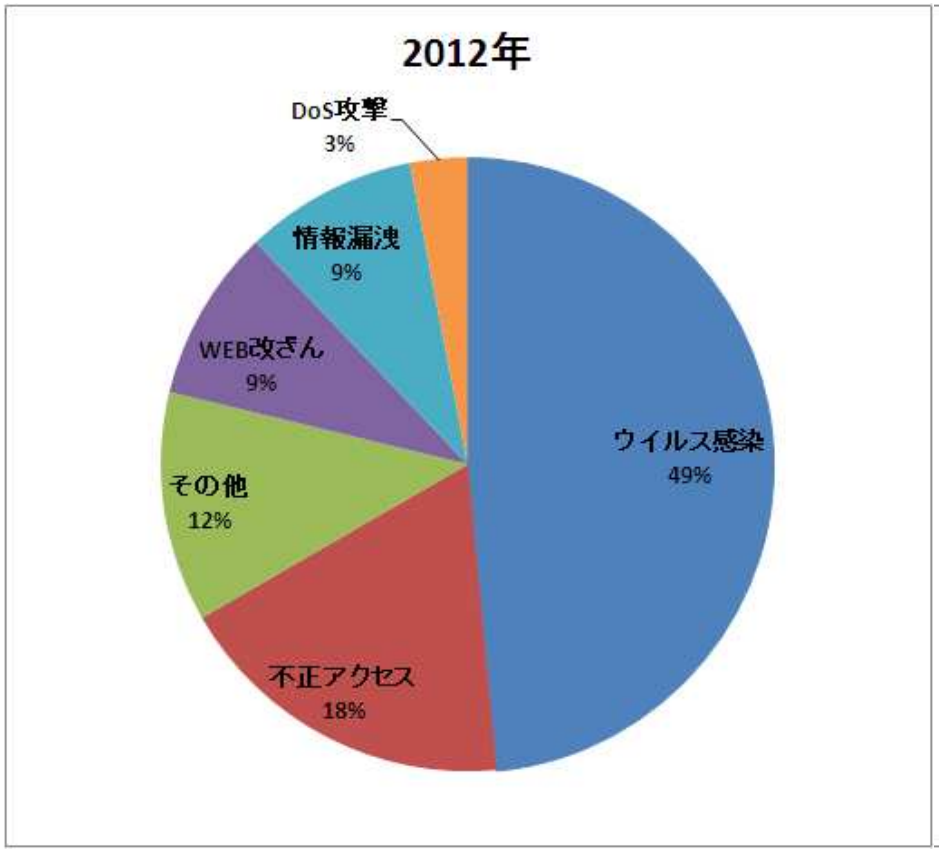
対象インシデント	・ウイルス感染 ・不正アクセス ・WEB改ざん
作業例	・ウイルス駆除、調査 ・不正アクセス調査 ・情報漏洩調査 ・WEB改ざんインシデント支援
特徴	お客様に生じた業務の混乱や停止からの早期復旧に向け、お客様先に駆けつけることを重視しています。

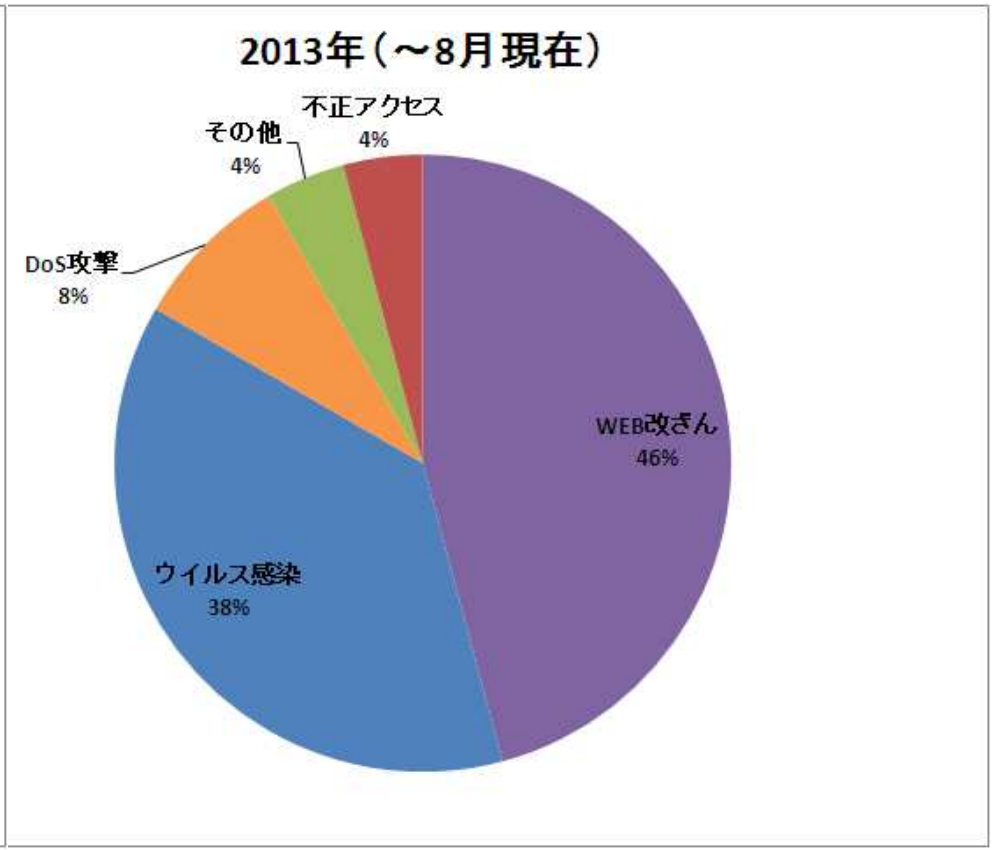
社内では…

サイバー消防団

WEB改ざんインシデントの増加

問合せインシデントの割合





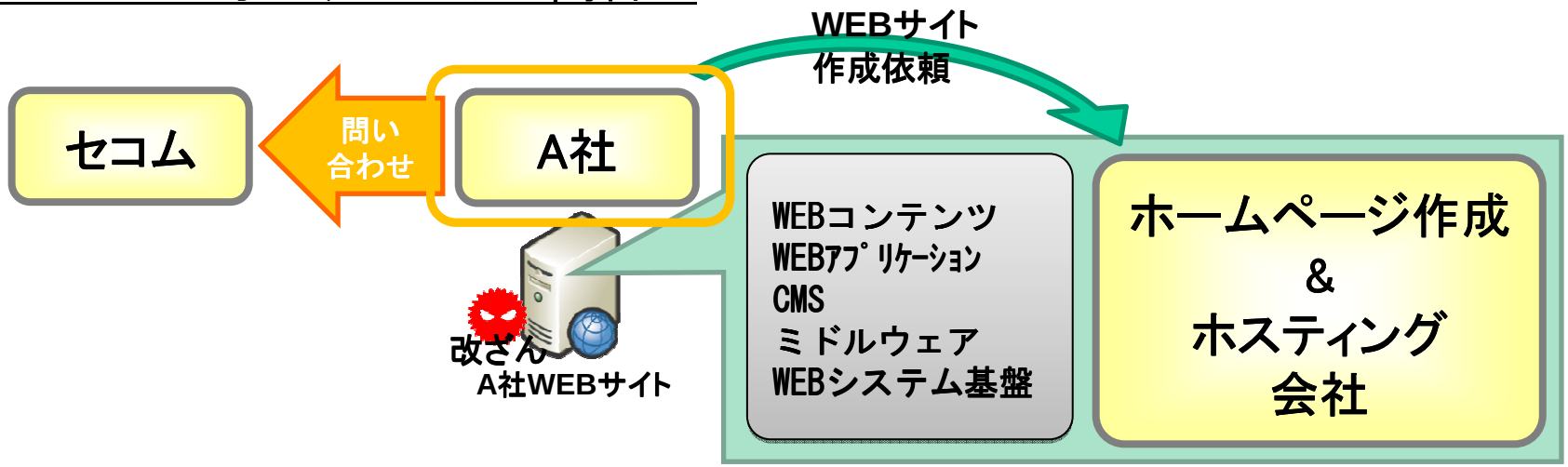
2013年はWEB改ざんインシデントが増加

WEB改ざん対応事例の紹介

WEB改ざんインシデント事例①

Total Information Service

ホームページオーナーからの問合せ



【背景】
再発防止に向けた原因の明確化

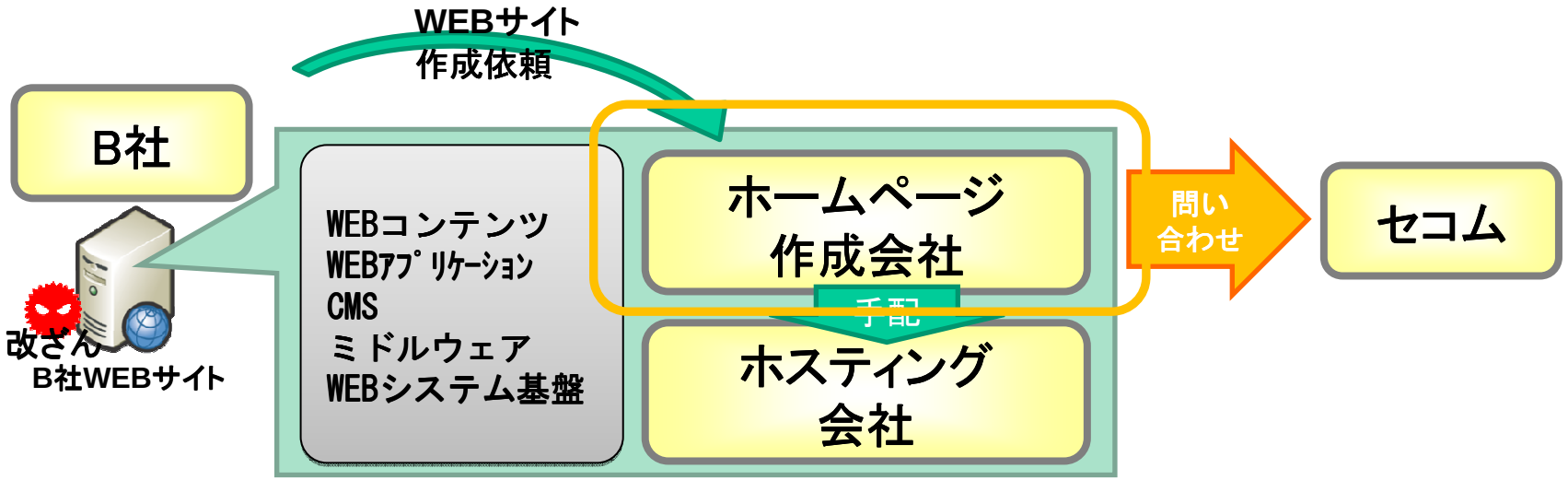
【要望】
改ざんされたWEBサーバの侵入経路、改ざん手法を知りたい

【結果】
・WEBサーバのFTPログを確認したところ、海外からのFTP接続が成功している事が判明
・FTPでの接続は1回で成功しており、アカウントハッキングや脆弱性攻撃の形跡見受けられない
・ほぼ全てのWEBコンテンツがFTPによりアップロードが行われていた(通常参照不可能なものも)
・アップロードされた全てのファイルに不正なJavaScriptが挿入されている事が判明
・WEBコンテンツ管理PCから、FTPアカウント情報やコンテンツが流出した可能性が高い

WEB改ざんインシデント事例②

Total Information Service

ホームページ作成会社からの問合せ



【背景】
　A社へのインシデント報告が必要

【要望】
　改ざんされたサイトに接続した際の影響を知りたい

【結果】
　・2種類の挿入スクリプトを検出
　　1種目:アメリカのドメインへ誘導するスクリプト(htmlファイルの末尾に挿入)
　　2種目:アクセス元情報を中国のドメインへ送信するスクリプト(index.phpに挿入)

現場対応から見える問題

現場対応から見える問題

① WEBシステム運用必要性の認識不足

② WEBメンテナンス用端末の未把握

③ 第三者からの通報によるWEB改ざんの認知

①:WEBシステム運用必要性の認識不足

◆WEB改ざんが行われたオーナーにおけるWEBシステム運用担当の認識

トップ

WEBコンテンツ管理 ⇒自社または外部業者
WEBシステム開発(アプリやサーバ等)⇒外部業者
WEBシステム運用　⇒不在(頭に無い)

次点

WEBコンテンツ管理 ⇒自社または外部業者
WEBシステム開発(アプリやサーバ等)⇒外部業者
WEBシステム運用　⇒外部業者がやっていると思っていた

WEBシステムは構築当時のまま

②：WEBメンテナンス用端末の未把握

◆WEBメンテナンス用端末の把握状況

・自分以外の担当者が使用するWEBメンテナンス用端末を把握していない

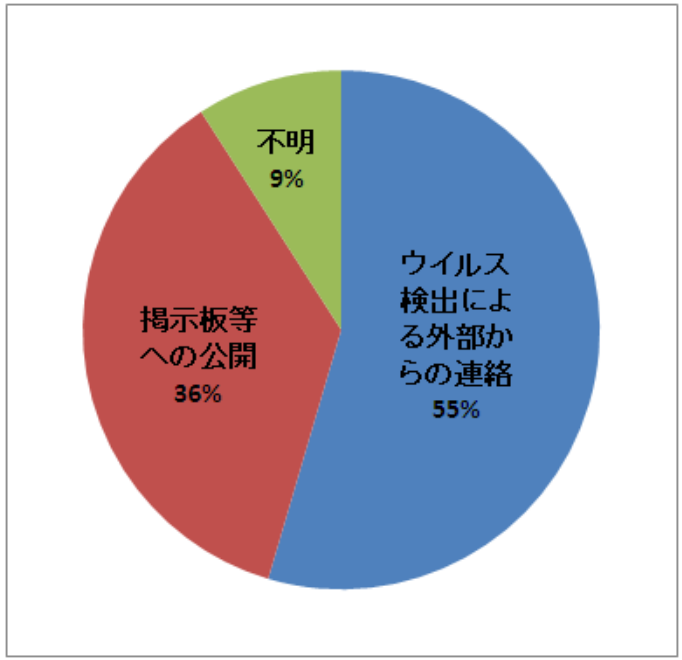
・自宅端末からの（直接的な）WEBメンテナンスが可能

組織としてWEBメンテナンス用端末を管理できていない

守るべき対象が不明確

③:第三者からの通報によるWEB改ざんの認知

◆WEB改ざん事象認知のきっかけ

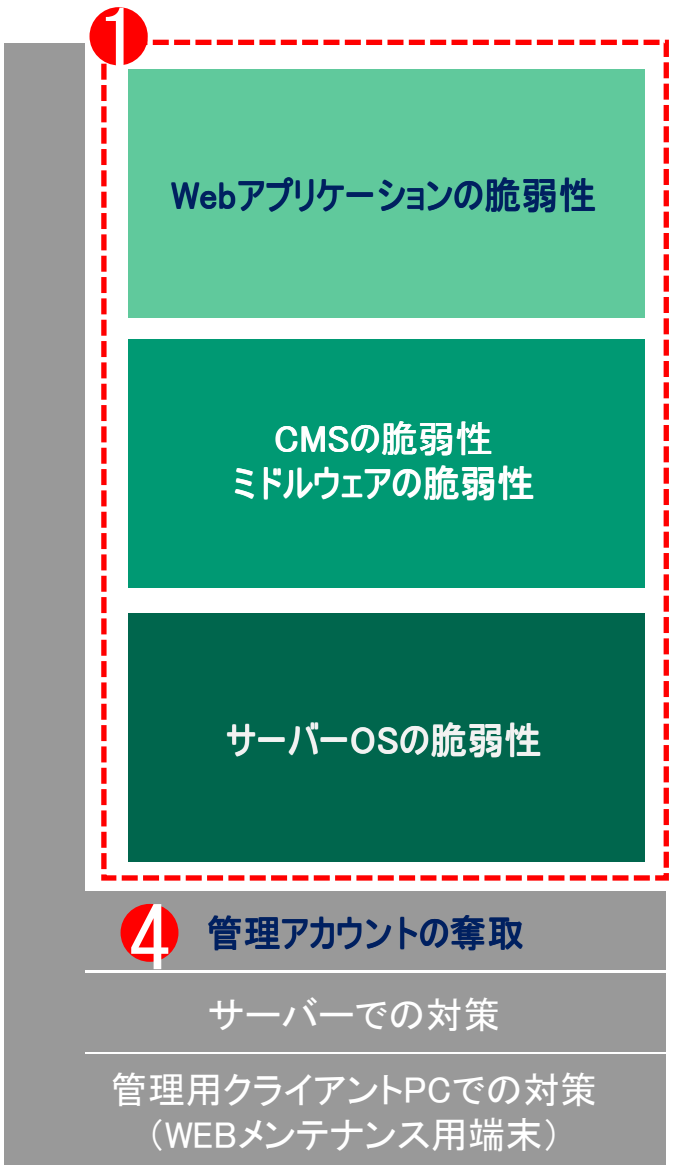


改ざん状態での公開が長くなり、風評被害につながる恐れ

WEB改ざん事象の被害拡大

対策の注意点

公開ウェブサイトのセキュリティー対策（基本方針）



1 ・脆弱性診断(インフラ & ウェブアプリ)
- −定期診断
- −新規および変更時診断

・セキュアプログラミング

2
・ウェブ・アプリケーションの改修
・ウェブ・アプリケーション・ファイアウォール（WAF)での防御

3
・パッチの適用
・侵入防御システム(IPS)での防御

4 <u>サーバーでの対策</u>
・強固な認証方法の使用
・管理アクセスの制限
・IPSやWAFによるブルートフォース・アタック等のアカウント奪取の試みの防御

<u>管理用クライアントPCでの対策</u>
・パッチ適用
・アンチウィルス
・PCの限定・固定

現場対応から見える対策の注意点

■WEBシステムの脆弱性解消

・脆弱性対応の必要性を認識する
・脆弱性対応を続ける担当を明確にし、恒常的に脆弱性対応を実施する。

■WEBメンテナンス用端末のセキュリティ対応

・WEBメンテナンス用端末を明確にする

■WEB改ざんを想定した準備

・WEB改ざんを検出する仕組みの検討
・WEB改ざんを検出した際の手順、フローの明確化

ご清聴ありがとうございました