Designing The Future KDDI

KDDI Cloud Inventory

マルウェアなどのPCに潜む怪しいソフトウェアを洗い出す

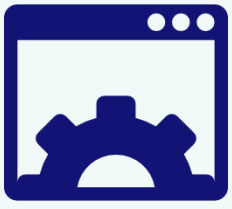
KCI Assessment Service

「攻撃者に利用されやすいソフトウェアが社内のPCに存在しないか？」
「過去にマルウェア感染した形跡のあるPCが存在しないか？」
このようなPC管理者の悩みをインストール不要の独自ツールを使って解決

1 問診票提出

PC台数やOS等の情報を記入・ご提出

2 ツール提供



問診票の内容に沿った実行ファイルを送付

3 ツール実行

調査対象端末でツールを実行

※データは自動で送信されます

4 分析

調査データを元にアナリストが分析

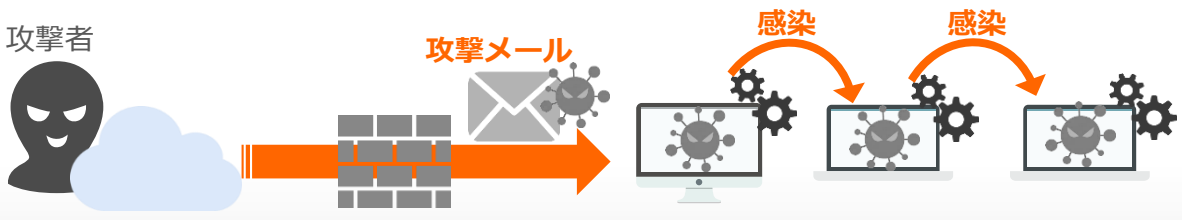
5 レポート提出 報告会実施

分析結果をレポートとして提供
報告会を実施

お客様の作業は“問診票の記入”と“ツールの実行”のみ

サービス提供イメージ

標的型攻撃は1台のマルウェア感染をきっかけに
社内で感染が拡大している可能性が



KCI Assessment Serviceで現状把握

調査対象PCに診断ツール配布

分析結果を報告会・レポートでご提供

アナリストによる結果分析

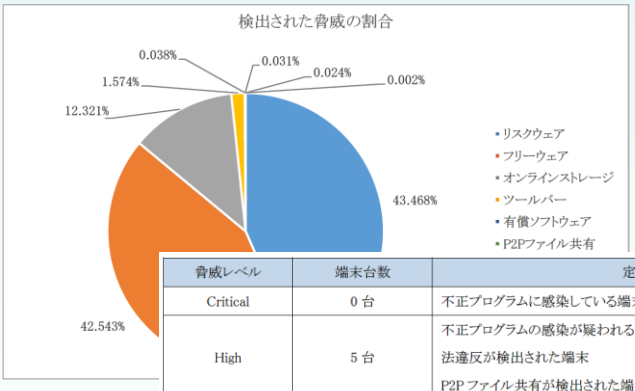
ツールを実行し対象端末の調査データ収集

経営課題とも言われるセキュリティ対策

グローバルセキュリティなら“ KDDI “

調査レポート イメージ

- **脅威レベル判定**
  - 不正プログラム感染
  - 不正通信
  - ポリシー違反
- **脆弱性情報**
  - 脆弱性のあるソフトウェア
  - MS社関連の脆弱性
- **リスクウェア情報**
  - 法令違反の可能性のあるソフト
  - P2P、遠隔操作、VPNソフト等
  - フリーウェア



脅威レベル	端末台数	定義
Critical	0 台	不正プログラムに感染している端末
High	5 台	不正プログラムの感染が疑われる端末 法違反が検出された端末 P2P ファイル共有が検出された端末
Middle	0 台	不正プログラムの可能性があるソフトウェアが検出された端末（不明な実行ファイルなど）
Low	234 台	セキュリティポリシー違反の可能性があるソフトウェアが検出された端末（アドウェアなど）
参考	0 台	ご確認いただきたいソフトウェアが検出された端末
脅威なし	0 台	脅威が検出されなかった端末

レポート項目	調査内容・結果事例	対策例
リスクウェア情報	マルウェアは発見されなかったがファイル共有ソフトや法違反の可能性のあるソフトなど、多数のリスクウェアを発見。	ポリシーの見直し、ソフトウェア起動制御等の対策が必要。
アドウェア情報	複数の端末からアドウェアを発見。広告配信ネットワークを経由し不正プログラムに感染する事例もあるため調査が必要。	操作ログによる原因の調査やWebレピュテーション等の対策が必要。
脆弱性情報（各種ソフトウェア）	Adobe製品、Java、QuickTime等、OS以外の脆弱性を狙われやすいソフトウェアの脆弱性を検出可能。	早急なパッチ適用および継続的なパッチ管理等の対策が必要。
脆弱性情報（Windows Update）	OSの脆弱性レポートではユーザーごとの最終アップデート日も確認可能。	早急なパッチ適用および継続的なパッチ管理等の対策が必要。
自動起動設定情報	組織内の標準ソフトではないVPNクライアントやアドウェアが自動起動に設定されていることが判明。	必要ないものは削除原因調査などが必要。
接続先情報	ソフトの内容だけでなく、接続先情報の把握が可能。	不正な通信を行うソフトがあった場合FWでのブロックやUTM導入等の対策が必要。

お問合せ

http://global.kddi.com/ja/