

課題161 ドライブ・バイ・ダウンロード攻撃対策フレームワークの研究開発

安心・安全なネットワーク社会の実現に資するため、Webからの強制的なダウンロードを悪用した攻撃手法であるドライブ・バイ・ダウンロード(以下、DBD)攻撃について、その脅威の全容を解明し、DBD攻撃対策フレームワークの確立を目指す。

(1) DBD攻撃大規模観測網構築技術：

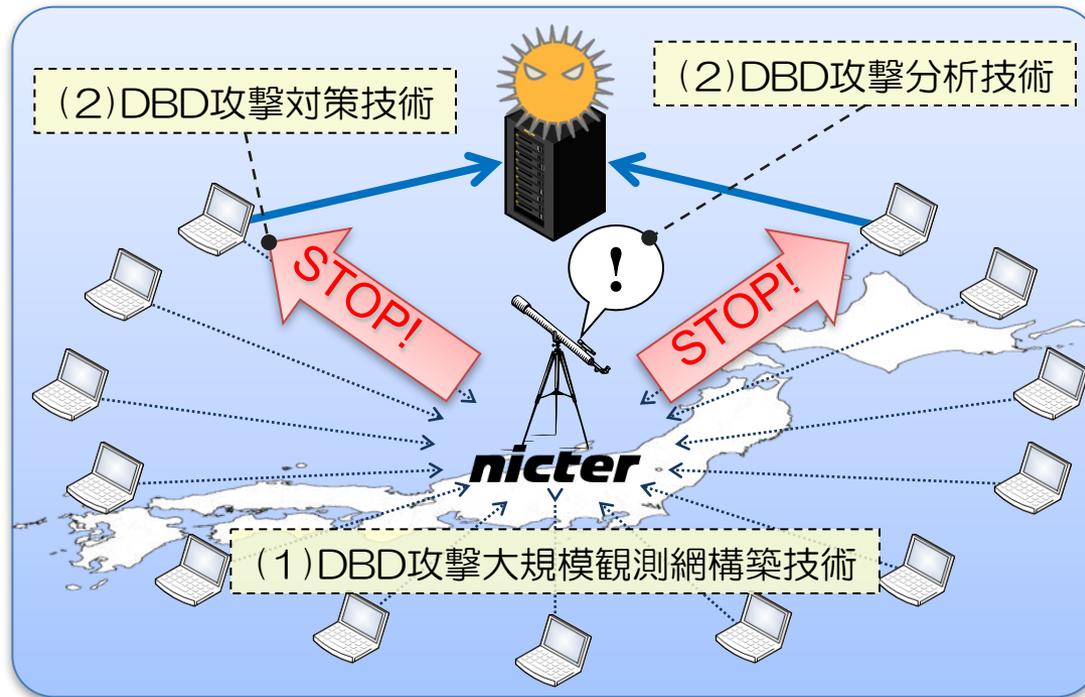
ユーザのWebブラウザ上の挙動を準リアルタイムに観測可能とする大規模（100万センサ以上を収容）観測網構築技術を確立する。

(2) DBD攻撃分析・対策技術：

上記の観測網から得られた情報をリアルタイムに自動分析し、DBD攻撃の発生やマルウェア配布サイト等を検出する技術を確立する。また、分析結果から有効な対策を導出し、ユーザのWebブラウザに自動展開する技術を確立する。

(3) DBD攻撃対策フレームワーク実証実験：

1000センサ程度のユーザ参加型実証実験を実施し、上記(1)～(2)の技術の有効性検証を行う。



研究期間: 契約締結日から平成27年度末まで(4年間)

予算: 平成24年度 総額130百万円(上限)

採択件数: 1件