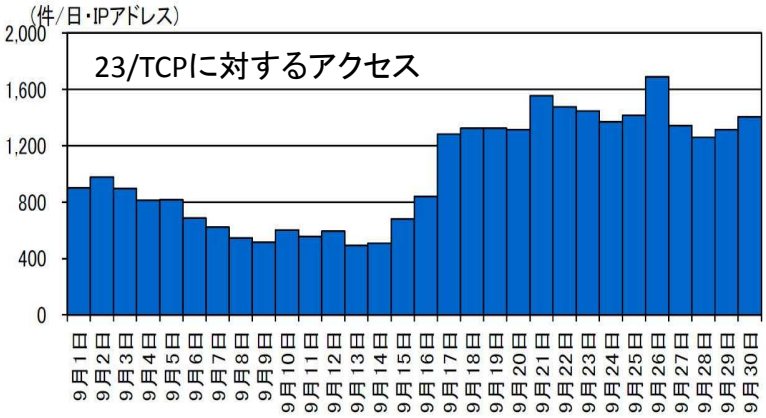
モノづくりプリザーブ
Preservation for Industries in kyoto
モノプリ・ニュース！ 第14号

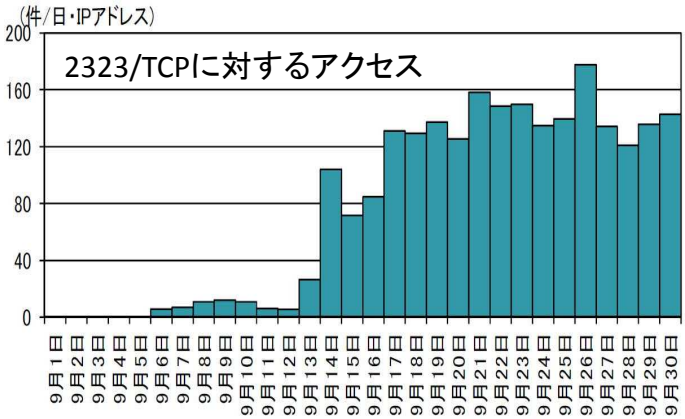
社内にネットに繋がった「モノ（物）」はありませんか？

「Mirai」感染機器からのアクセス増加中！

９月中旬以降、「Mirai」に感染したデジタルビデオレコーダー、ウェブカメラ等のIoT機器が発信元と考えられるアクセス（宛先ポート23/TCP及び2323/TCP）が増加（警察庁のインターネット観測結果による）

参照：警察庁@police 「インターネット観測結果等（平成28年９月期）」
https://www.npa.go.jp/cyberpolice/detect/pdf/20161020.pdf





不正プログラム「Mirai」とは

「Mirai」は、IoT機器をボット化（遠隔操作を可能に）する不正プログラムです。感染したIoT機器は他のIoT機器に感染を広げ、攻撃者からの指令を受けて、DoS攻撃等を行います。

本年10月、「Mirai」のソースコードがインターネット上で公開され、同月、米国で発生した大規模なDNSサーバへのDDoS攻撃でも「Mirai」に感染したIoT機器が使用されたといわれています。

対策

- ユーザ名とパスワードを推測されにくいものに変更する。
- ファイアーウォール等によって不必要な外部からのアクセスを遮断し、特定のIPアドレスからのみ、アクセスを許可する。
- 製造元のウェブサイト等でぜい弱性情報を確認し、ぜい弱性がある場合はアップデートを行う。

京都府警察本部モノづくりプリザーブ事務局　075-451-9111(内線 5821)