別紙

重要インフラ等で利用されるIoT機器の調査

＜実施内容＞

○ サイバー攻撃観測網やネットワークスキャンを活用して、重要インフラ等で利用される脆弱な重要IoT機器※を調査。

○ Webインタフェースに記載されている情報等から当該機器の所有者等を特定し、所有者等に当該機器の設置状況、システム構成等をヒアリングした上で、想定されるリスク、対策の必要性の説明などの注意喚起を実施。

○ また、必要に応じて製造事業者等に対しリスクに関する技術的な情報提供を実施。

※ 重要インフラ等で利用される機器は、国民生活等に直接影響を及ぼす可能性があることを踏まえ、脆弱な重要IoT機器とは、パスワード設定が適切になされていないものに加え、パスワード設定はなされているが、認証画面がインターネット上で公開されているものも含むこととした。

調査・注意喚起の流れ

①重要IoT機器の探索

日本国内のグローバルIPアドレス（IPv4）について、主に80/tcpに対してアクティブスキャン等を行い脆弱な状態にある機器を検出。

②利用事業者などの特定、コンタクト

Webインタフェースに記載されている情報等から、所有者・運用者・利用者等の特定を試みる。

③設置環境や設定状況等を現地でヒアリング（実地調査）、電話や電子メールで調査（類似事例調査）

所有者等にコンタクトをとり、必要な者から同意を得た上で、当該機器の設置環境、設定状況、システム構成等を現地調査
※ 類似案件については、電話又は電子メールでヒアリング

④脆弱性解消のための注意喚起、対策例の提示

所有者等に想定されるリスクを伝え、対策の必要性を説明。
（対策例：推測されにくいパスワードの設定、アクセス制御の実施、VPNの導入）

⑤対策状況の確認

調査結果（概要）

【調査結果概況】

- 本件調査により検出した脆弱な重要IoT機器は150件、そのうちWebインタフェースに記載されている情報から利用者等に関する情報が得られたものが77件、そのうち実際に利用者等にコンタクトが取れて、注意喚起等を行ったものが36件であった。
- 検出した重要IoT機器（工場、工事現場等）は、消費電力監視装置、水位監視装置、防災設備制御装置、ガス観測警報通知装置等であった。
- 36件の内訳は、パスワード設定が適切になされていないものが27件、パスワード設定はなされているが認証画面がインターネット上で公開されていたものが9件であった。

【ヒアリング調査等の結果（ポイント）】

- 関係者（所有者、利用者、運用者、導入者、製造者）の脅威に対する認識が十分でない、または、認識の共有が十分にできていない。
- 多様な関係者間の責任の所在が明確になっていない。

家庭用ルータ、防犯カメラ等の一般利用者向けIoT機器の調査①

＜実施内容＞

○ 日本国内のグローバルIPアドレス（IPv4）で接続されたIoT機器に広くネットワークスキャンを行うためのシステムを構築

○ 上記システムを用いてネットワークスキャンを行い、開放ポート（稼働しているサービス）の調査等を実施。

○ ネットワークスキャンによって得られるバナー情報等をもとにした機種特定について検証を実施。

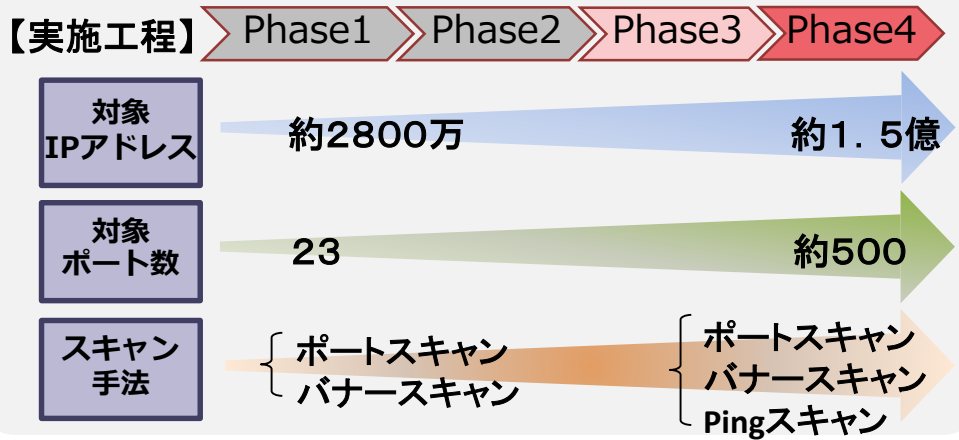
※ ネットワークスキャンで発見した脆弱な機器の所有者等への注意喚起にあたっては、IoT機器の機種を特定できれば、それぞれの製品毎の設定変更やファームウェアの適用、サポート等を行うことが可能となる。

○ NICTERで観測したマルウェア感染機器に関する情報と連携した分析を実施。

※ ネットワークスキャンの結果から、マルウェア感染機器の特定、感染の可能性がある機器の事前把握などができれば、マルウェア対策に有益な情報となる。

＜ネットワークスキャン実施条件等＞

- 本調査で対象としたIPアドレスは、日本へ割り当てられているもののうち、海外で利用されている可能性があるものや到達性のないものなどを除外した約1．5億個。
- 調査対象ポートは、約500ポート（TCPポート）。
- 調査対象やネットワークへの影響を考慮し、またシステム稼動状態の確認を行いつつ調査規模を段階的に拡大。



調査結果（概要）

【ネットワークスキャンを行うシステムの構築】

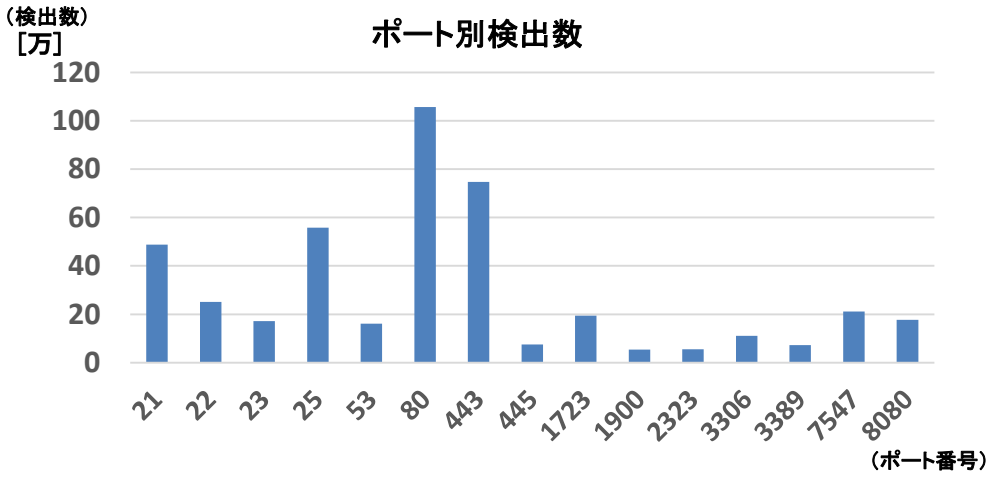
- オープンソースのツールをベースとして、設定、チューニング、機能追加し、独自のスキャンシステムを構築。
- 構築したスキャンシステムの機能については、「SHODAN」、「Censys」の情報と比較しても、遜色なく、十分な調査能力を有していることを確認。これにより、信憑性を確保した正確なスキャン結果の蓄積が可能となった。

家庭用ルータ、防犯カメラ等の一般利用者向けIoT機器の調査②

調査結果（概要）

【ネットワークスキャンに対する応答】

- 調査対象IPアドレスに対して、ネットワークスキャン（pingスキャン、ポートスキャン、バナースキャン）を行ったところ、その約6%で何らかの応答を確認。
- ポートスキャンの結果からは、ウェブサービス（TCP80, 443）、メールサービス（TCP25）、テルネットサービス（TCP23）、DNSサービス（TCP53）など多様なサービスの稼働を確認。



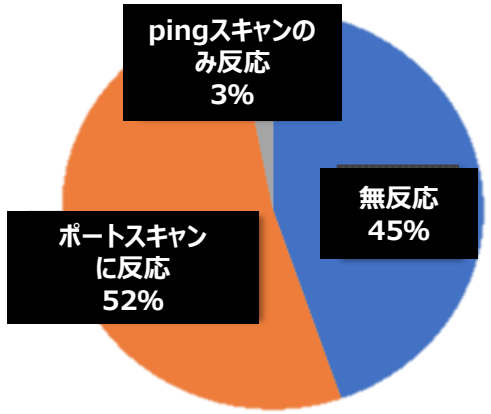
【バナー情報等をもとにした機種特定の実現性検証】

- バナー情報の分析等により、一部機種特定が可能であることを確認。また、機種は特定できない場合であっても、製造事業者名や機器類型（カメラ、ルータなど）などの機種特定につながる情報が多く得られることを確認。
- より精度を上げるために、別の手法との組み合わせを考慮するなど、分析手法の高度化が必要。

【NICTER観測データと連携した分析】

- 情報通信研究機構がNICTER※で捉えたマルウェア感染機器（TCP23又はTCP2323に対して感染拡大パケットを発信していた機器）に対してネットワークスキャンを実施。
- Mirai亜種が感染に用いたポート、Mirai亜種に対する脆弱性を持つ機器に固有のポート等から反応があった。全体の45%からは反応がなかった。

※ ダークネット（未使用IPアドレス）への通信をセンサーで観測し、サイバー攻撃の地理的情報や攻撃量、攻撃手法等を可視化するシステム



（想定される無反応の要因）
- マルウェア感染による要塞化。
- CGNAT等のサービス利用。
- 調査対象外のポートを経由して感染。
- ポートスキャンがブロックされるサービス利用。

- NICTER観測データと連携することで、マルウェア感染機器のより詳細な分析が可能となるなど、分析結果の正確性向上に寄与することを確認。
- 技術開発等も含めて、分析能力の向上を図ることが重要。