

1. ネットワークの安定提供に向けた課題

- ・ ネット家電や監視カメラなどの「IoT機器」は、「ボットネット」などDDoS攻撃等の基盤として悪用され、ネットワーク安定運用の脅威となっている。
- ・ しかし、IoT機器側でのマルウェア対策は、パソコンやスマホと比較しても難しく、問題の長期間化と大規模化の懸念がある。セキュリティ対策の責任とコストの分担について議論が必要である。

2. ボットネット対策「C&Cサーバの通信遮断」について

参考資料-2

- ・ 「ボットネット」に組み込まれた「IoT機器」等は、「C&Cサーバ」から命令を受け攻撃を行っている。
- ・ この通信を遮断することで、攻撃や犯罪を抑止し、通信サービスの安定提供と同時に、利用者のセキュリティも確保できる可能性が高い。
- ・ 海外では実績のある対策であり、国内で行う際の課題と対策について検討いただきたい。

3. C&Cサーバ調査と「通信の秘密」の関係

参考資料-3

- ・ C&CサーバのIPアドレス等を調査して「ブラックリスト」を作成する方法として、マルウェア感染機器が共通してアクセスする通信先を特定し、C&Cサーバをあぶり出す方法がある。
- ・ 「通信の秘密」に配慮した調査方法についてご議論をいただき、対策技術の研究開発と実装に役立てていきたい。

4. セキュリティ情報の共有について

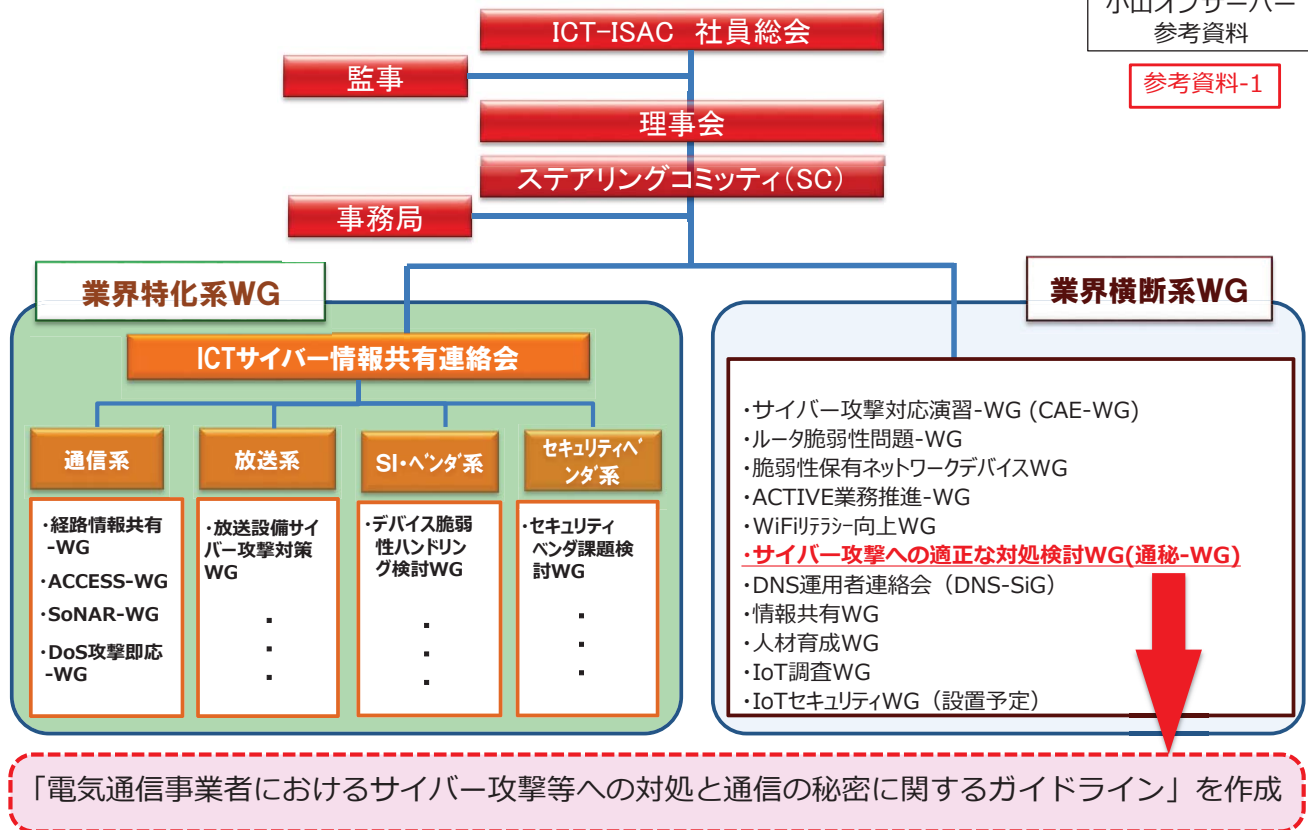
参考資料-4

- ・ 同時多発的に発生するサイバー攻撃に対応するためには、自社ネットワークで確認した攻撃情報を他事業者と共有するなど、通信事業者間での情報共有が有効である。
- ・ 例えば「ICT-ISAC」が情報共有のコアとなり、情報の分析・検証と結果の共有を行う場合の、「通信の秘密」に配慮した情報共有のあり方について、さらに通信事業者以外と「ブラックリスト」を共有可能な条件等について議論いただきたい。

5. IoT機器のセキュリティ対策基準の必要性

- ・ 大規模なDDoS攻撃の回避または、被害から早期に回復するためには、攻撃の踏み台となった脆弱なIoT機器のセキュリティ対策が急務である。
- ・ しかし現状では、端末設備のセキュリティに関する対策基準が整理されておらず、危険な機器であっても、注意喚起やネットワークへの接続を制限できないため、今後の検討課題にしていきたい。

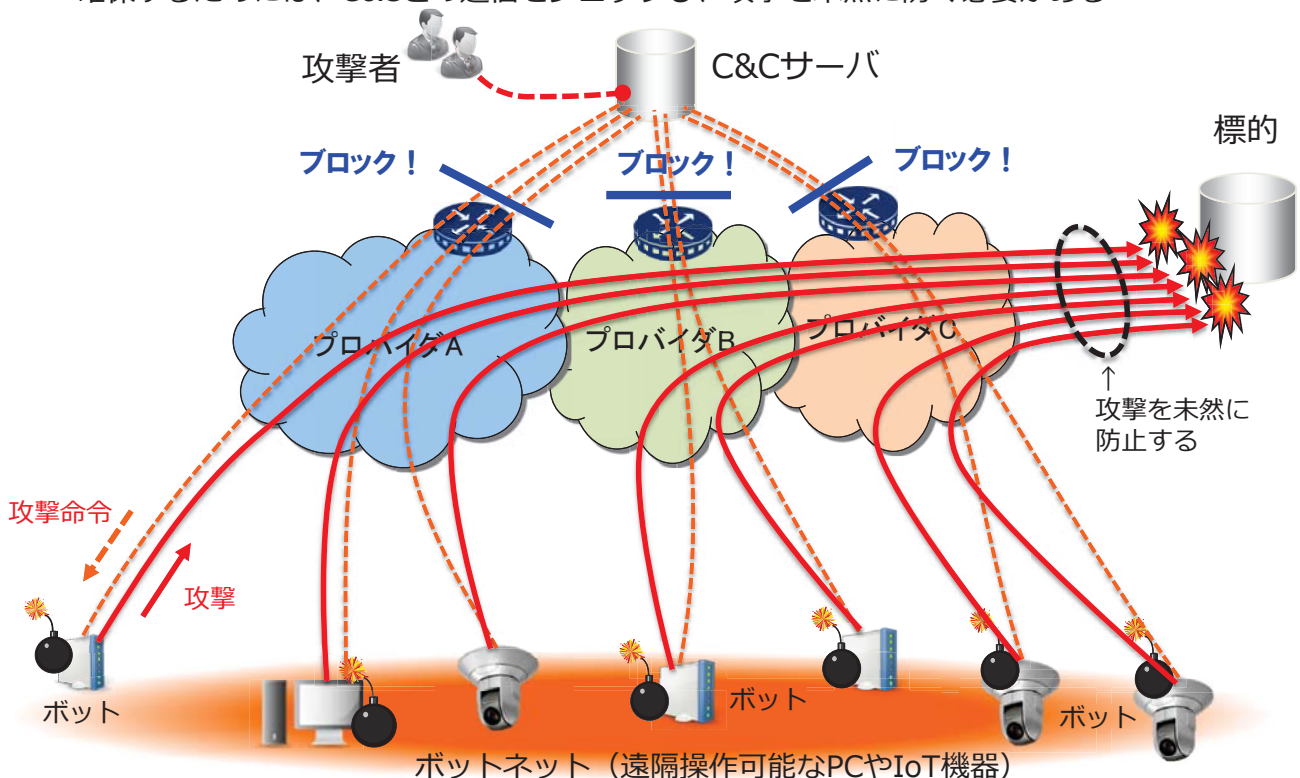
(一社) ICT-ISAC の体制と取り組み



Copyright©2017 ICT-ISAC Japan. All Rights Reserved

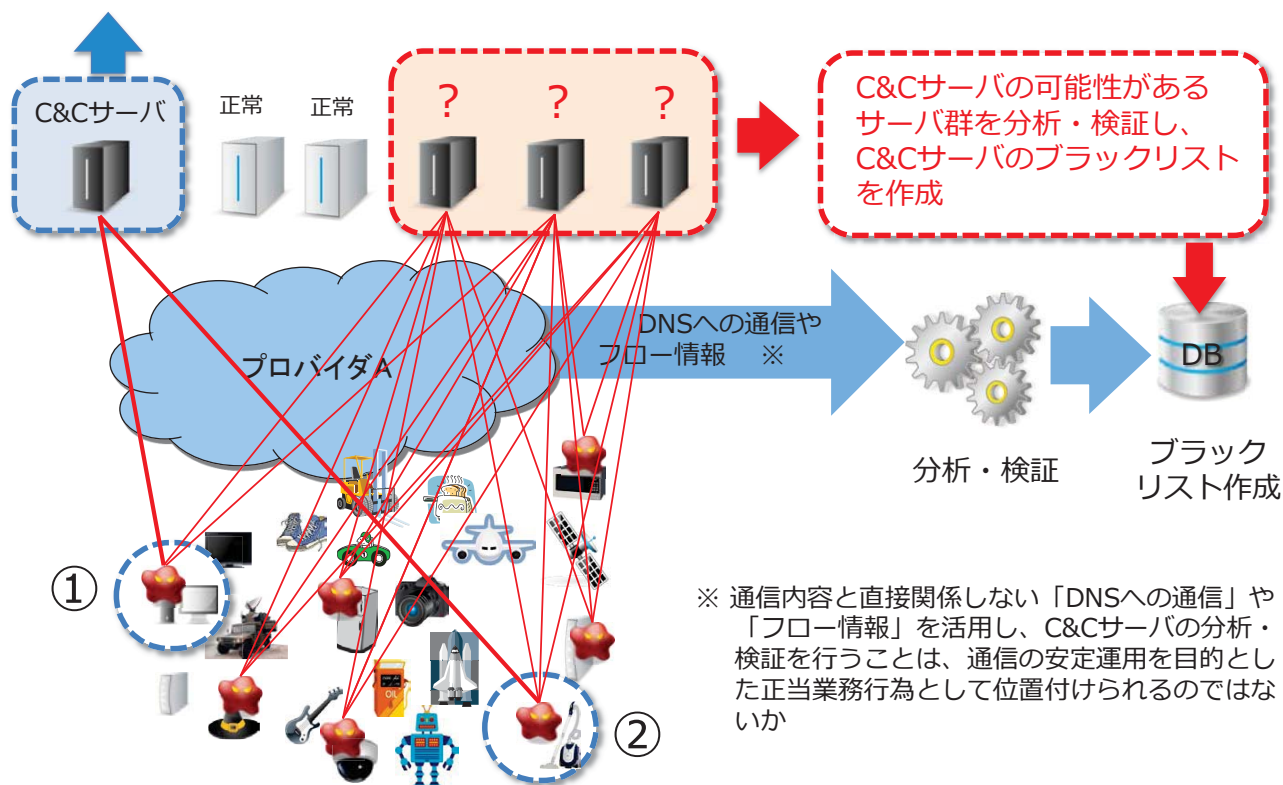
ボットネット対策「C&Cサーバの通信遮断」について

MIRAIボットネットのDDoS攻撃は1Tbpsに達した、通信サービスの安定運用を確保するためには、C&Cとの通信をブロックし、攻撃を未然に防ぐ必要がある



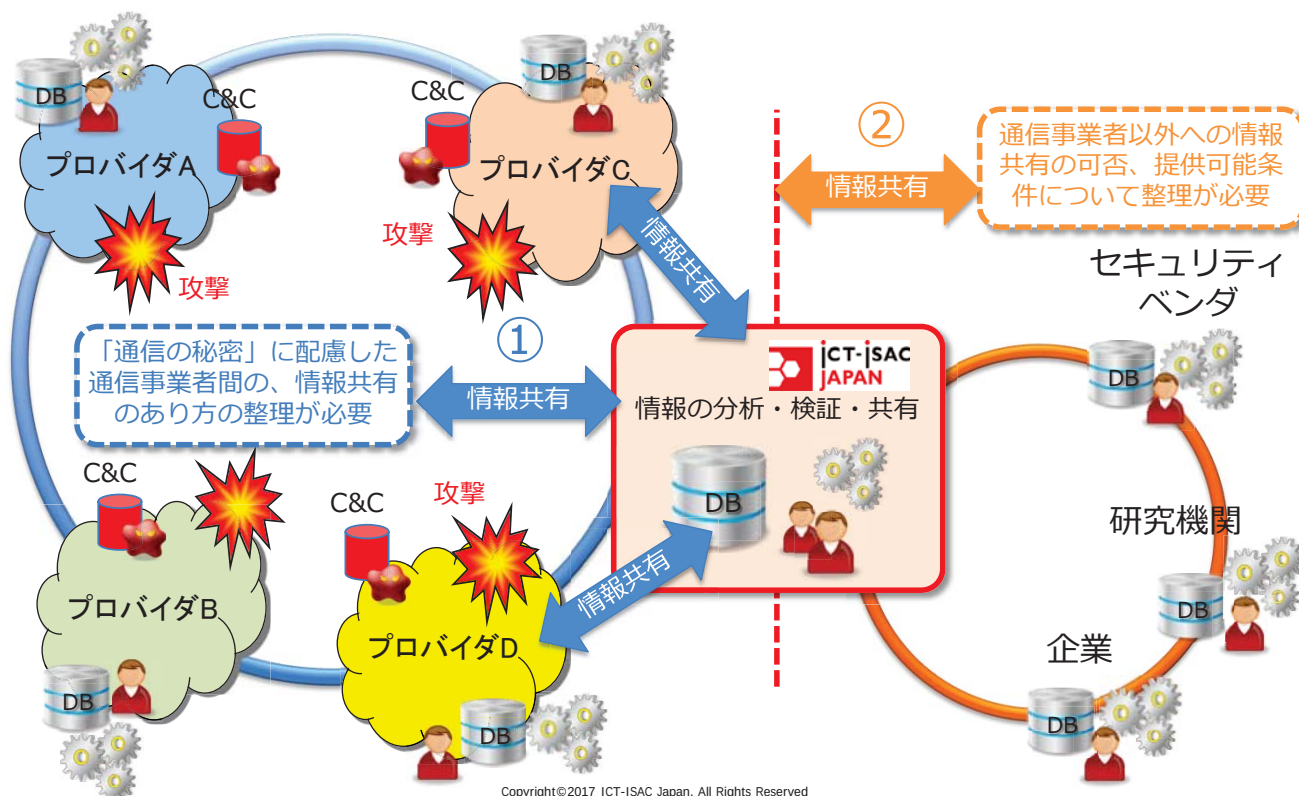
Copyright©2017 ICT-ISAC Japan. All Rights Reserved

C&Cサーバにアクセスしているマルウェア感染機器①と②が、共通してアクセスする通信先を特定し、分析・検証することで、C&Cサーバをあぶり出す



Copyright©2017 ICT-ISAC Japan. All Rights Reserved

大規模攻撃の蓋然性が高いC&Cとの通信情報（IPアドレスや時刻情報）や、各プロバイダが独自に作成したブラックリストを共有し、攻撃の検知や遮断に役立てたい



Copyright©2017 ICT-ISAC Japan. All Rights Reserved