資料27－3

IoT端末等を踏み台にしたサイバー攻撃への対策強化の必要性

2020年12月3日

一般社団法人ICT-ISAC SC運営委員長
NTTコミュニケーションズ情報セキュリティ部長

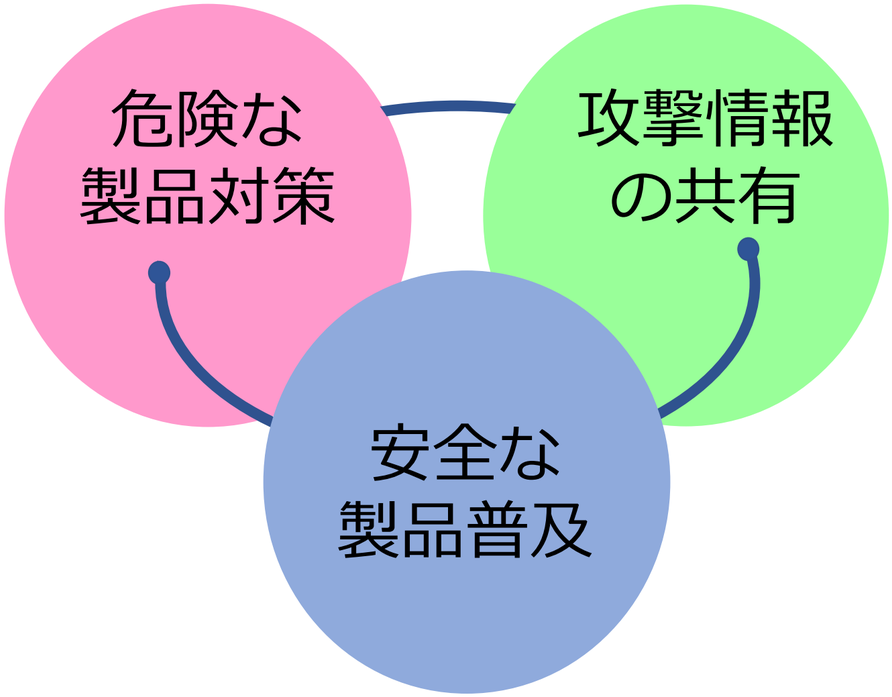
小山 覚

1. IoT端末等を踏み台にしたサイバー攻撃への対策強化の必要性
2. NOTICEにおける注意喚起の効果や課題・改善点
3. セキュリティに関してISPが抱えている課題

IoT端末等を踏み台にしたサイバー攻撃への対策の強化必要性

- ✓ IoT：インターネットに接続される端末数が増加中
- ✓ ５G：４Gと比較して、端末数→30倍・回線帯域→10倍・超低遅延→10倍
- ✓ IPv6：NOTICEで実施中のリモートからのスキャンが困難に

NICTがIoT機器を調査し、ISPを通じて利用者への注意喚起を行うプロジェクト「NOTICE」を実施中



DDoS攻撃への共同対処を行う第三者機関を総務大臣が認定する制度を創設

① 攻撃の送信元情報の共有*
② C&Cサーバの調査研究

※海外の端末を踏み台にしたDDoS攻撃への対策も課題

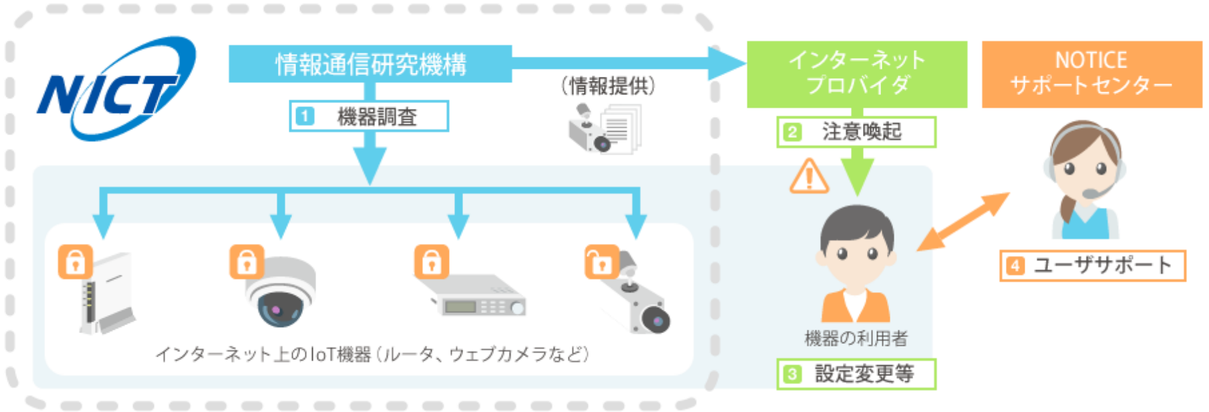
電気通信事業法の端末設備等規則を改正
技術基準(最低限のセキュリティ対策)を策定

① アクセス制御機能
② ID/パスワードの適切設定
③ ファームウェアの更新機能

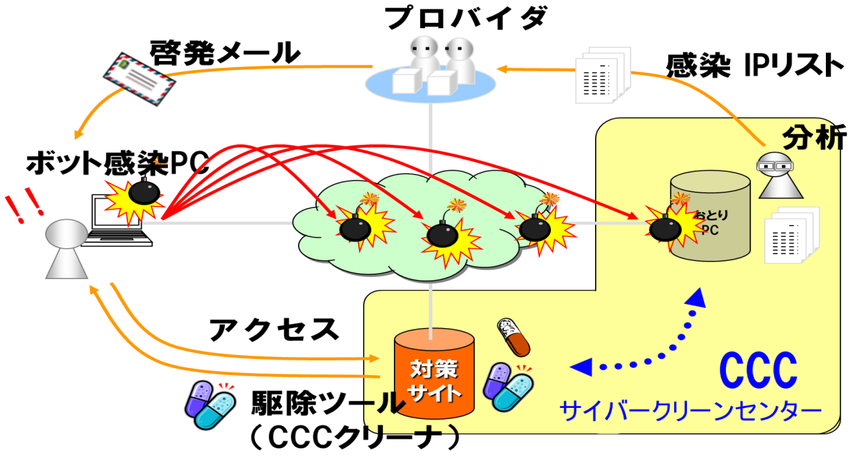
1. IoT端末等を踏み台にしたサイバー攻撃への対策強化の必要性
2. **NOTICEにおける注意喚起の効果や課題・改善点**
3. セキュリティに関してISPが抱えている課題

注意喚起施策の比較 NOTICE vs CCC（Cyber Clean Center）1/2

●NICTが調査した「脆弱なIoT機器」の回線契約者にISPから注意喚起を行う

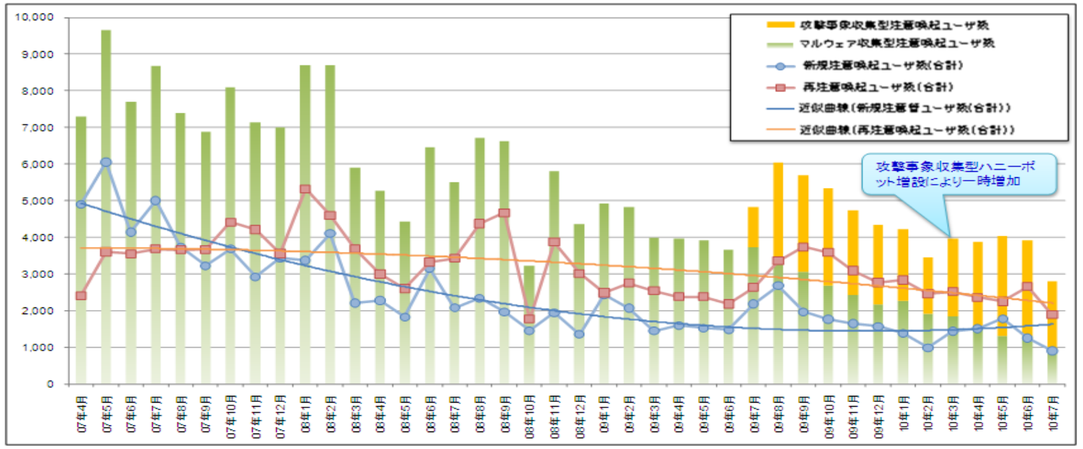


●CCCのハニーポットに攻撃した「マルウェア感染PC」の回線契約者にISPから注意喚起を行う



●注意喚起対象数が減らない

●注意喚起対象数が大きく減少した



注意喚起施策の比較 NOTICE vs CCC（Cyber Clean Center）2/2

●NOTICEの取り組みはCCCの当時と比較して、ISPを経由したユーザリーチが難しくなっている。さらに回線契約者とIoT機器管理者（保守者）が異なる場合もあり、回線契約者本人の被害がないことも多く、注意喚起による効果が期待できない状況になっているのではないか？

		NOTICE（2018～）	CCC（2006～）
注意喚起方法	電子メール	✓	✓
	郵送	–	✓
利用者による対策の難易度		×：難易度高い	○：難易度低い
注意喚起効果測定		△：IPアドレス数の推移で把握	○：ユーザを特定し把握
対策未実施ユーザへの個別対応		–	メール文面変更、封書や速達で 訴求度合いを向上
注意喚起の 到達性	読むか	×：あまり読まない	△：読ませる工夫をした
	動くか	×：自分には影響がない	○：自分の問題と理解
日本国内の網羅性		△：低い	○：高い

NOTICEのパワーアップ施策案

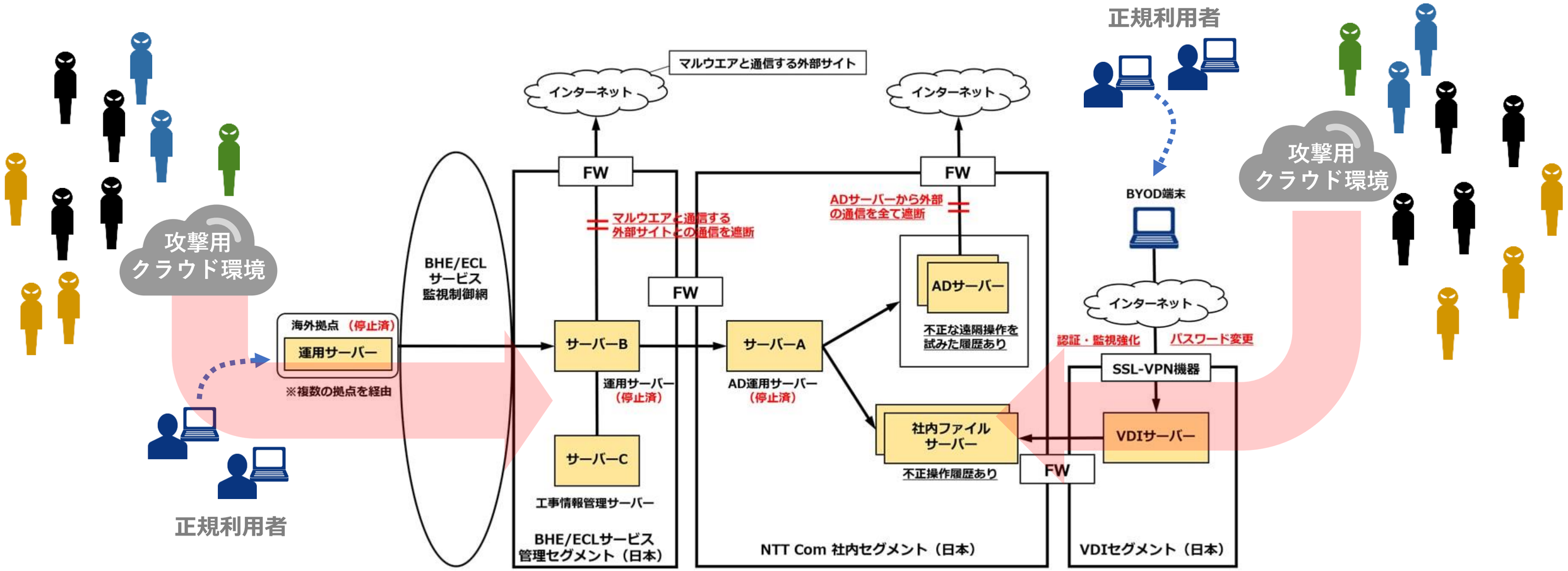
●NOTICEのポートスキャン対象の拡大を行い調査の網羅性を高め、対象者を把握し訴求力の高い方法で注意喚起を行うことで、脆弱なIoT機器の撲滅を図ってはどうか？（本格的な５GやIPv6の普及までに完了したい）

		NOTICE（～2020）	NOTICE（２021～）
注意喚起方法	電子メール	✓	継続
	郵送	–	総務省かNICT名で出す
利用者による対策の難易度		×：難易度高い	返信ハガキで調査
注意喚起効果測定		△：IPアドレス数の推移で把握	ユーザを特定しヒアリング
対策未実施ユーザへの個別対応		–	技適等の取り組み紹介し、 機器交換を促す
注意喚起の 到達性	読むか	×：あまり読まない	総務省封筒＋重要書類在中
	動くか	×：自分には影響がない	自分の問題と理解
日本国内の網羅性		△：低い	調査ポート・IP拡大

1. IoT端末等を踏み台にしたサイバー攻撃への対策強化の必要性
2. NOTICE・NICTER注意喚起の効果や課題・改善点
3. セキュリティに関してISPが抱えている課題

多数の攻撃元IPアドレスから執拗に攻撃された

商用クラウド等の正規IPアドレスから社員に成りすまして攻撃



☞ 攻撃専門集団の恐ろしさ、敵は本格的な体制で攻めてくる