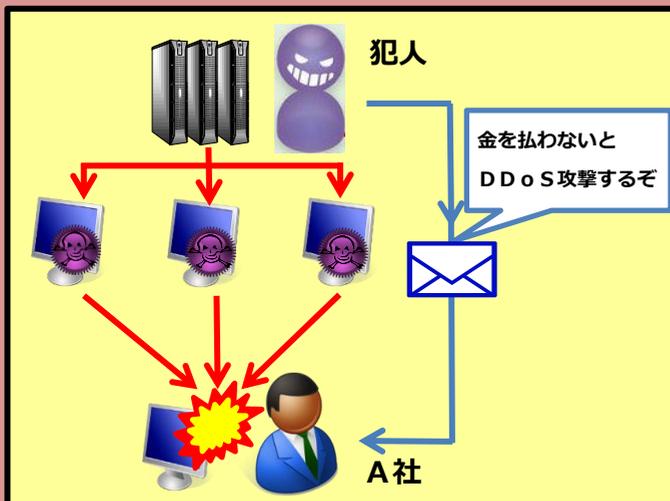


# CyberCrime Control Project

平成29年第3号

広島県警察本部  
サイバー犯罪対策課  
082-228-0110

## 企業を狙う「ランサムDDoS攻撃」とは!?



### 手口の概要

- ① 犯人は企業に対して、「金銭を支払わなければ、企業に対してDDoS攻撃を仕掛ける。」旨の脅迫メールを送信する。
- ② メールを受け取った企業が脅迫を無視すると、企業に対してDDoS攻撃を仕掛ける。
- ③ 攻撃を受けた企業は、サーバーがダウンし、WEBサービスが停止に追い込まれてしまう。



### DDoS攻撃とは

Distributec Denial of attack  
の略です。  
分散サービス拒否攻撃と訳します。

ウイルスに感染したパソコンに指令を出し、一斉にWEBサーバーに対して膨大なデータを送りつけます。攻撃を受けたWEBサーバーはデータを処理仕切れずダウンしてしまい、企業のWEBサービスが停止します。他人のパソコンを経由して攻撃することから、犯人の特定が困難です。

### 最近国内で発生した事例

本年9月19日頃から「Phantom Squad」を名乗る攻撃グループがDDoS攻撃の停止と引き替えに金銭を要求するメールを国内の複数の企業へ送信しました。また、本年9月14日頃から複数の企業に対してDDoS攻撃が仕掛けられています。メールの送信者と攻撃者の関連性は不明ですが、今後の発生に備えて平素からDDoS攻撃発生時の対策について検討することが必要です。

### 脅迫メールが届いたら

- ① 金銭を支払っても、攻撃を受けないという保証はありません。
- ② 一度支払ってしまうと、脅迫に屈する企業として認識され、何度も同じ被害に遭う可能性があります。



A社は脅せばお金を払うぞ、また、脅してやろう。

### 被害に遭わないために

- ① WEBサービスのセキュリティホール(脆弱性)を早期に発見し、改善する。
- ② 各企業内で被害時の体制・マニュアルを整備し被害に備える。
- ③ DDoS対策ソフトを導入する。
- ④ 同一IPからのアクセス回数を制限、アクセスの対象者が国内限定であれば、海外IPの遮断等を検討する。

\* IPのアクセスを制限することでサービスの利便性を損なう恐れがあります。各企業で慎重に検討して、ご判断ください。

平成28年~平成32年

「めざそう!  
安全・安心・日本一」  
ひろしまアクション・プラン

運動目標

県民だれもが穏やかに幸せな暮らしを実感できる  
日本一安全・安心な広島県の実現

重点項目

- 身近な犯罪被害の抑止
- 子供・女性・高齢者等の安全確保
- 新たな犯罪脅威への対応

なくそう特殊詐欺被害

アンダー

5 ↓  
作戦