# NEWS RELEASE

2020 年 12 月 11 日
株式会社ブロードバンドセキュリティ

## 総合的ランサムウェア対策のご提供を開始

### ～事業継続を脅かすランサムウェアへの備えを～

株式会社ブロードバンドセキュリティ（本社：東京都新宿区、代表取締役 CEO：持塚 朗、以下 BBSec）は、独立行政法人情報処理推進機構によるランサムウェア注意喚起の再発出を受け、「今、そこにあるリスク」を明確にしてランサムウェア※攻撃への不安を軽減する総合的なサービスのご提供を開始いたしました。

**【サービス提供の背景】**
本年夏より Emotet の再流行が観測されています。それと同時にランサムウェアも再活発化しており、8 月には独立行政法人情報処理推進機構セキュリティセンターより「事業継続を脅かす新たなランサムウェア攻撃について」の注意喚起が公表され、11 月に再度発出されるなど、その状況は年末に差し掛かる現在でも変わりません。

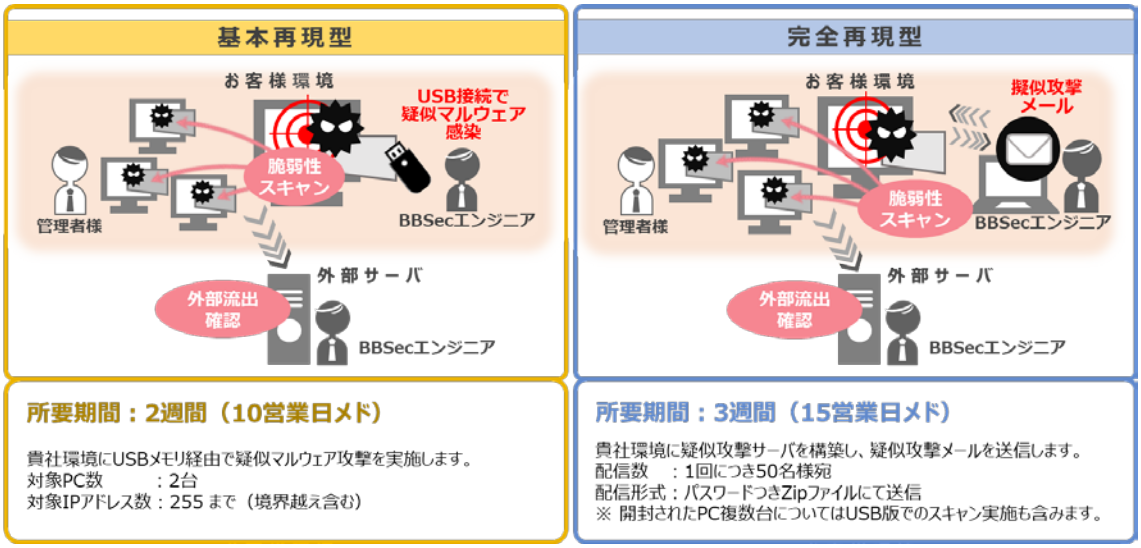
このような背景から、BBSec では疑似的に作成したマルウェアを用いて、実際に社内でランサムウェア感染した場合、どこまで感染が広がる可能性があるのかを可視化する「ランサムウェア感染リスク可視化サービス」を中心に、サブドメイン乗っ取り発生の有無を調査するサービス等を組み合わせ、総合的にランサムウェア対策の総点検をするサービスを開始いたしました。本サービスをご利用いただくことで、沈静化の兆しを見せないランサムウェア攻撃に対し、現状のリスク把握と対策の点検が可能になります。

※ランサムウェア： ランサムウェア（Ransomware）とはマルウェアの一種で、身代金（Ransam）とソフトウェア（Software）を組み合わせた名称です。その名のとおり、システム内のデータを勝手に暗号化し、システムの操作を不能にし、復号化するための身代金を要求するというものです。日本のあらゆる業種が規模の大小を問わず狙われていると言われています。

**【本サービスの特長】**
お客様の社内環境にある PC がランサムウェアに感染したと想定し、疑似マルウェアによる攻撃を実施します。
お客様のニーズに合わせ、特定の端末が感染したと想定する/感染している可能性を調査す

る「基本再現型」、より現実に近い形で攻撃をシミュレーションする「完全再現型」を選択いただくことが可能です。

疑似マルウェアにより取集した周辺情報に対して脆弱性スキャンを実施し、脆弱性および不要なポート/サービスを検出するとともに、データ外部流出の可能性について検証します。感染した PC より接続可能な他のクライアント PC およびサーバにどれほどランサムウェアの影響が及ぶか、実態に即した確認ができます。




**【提供金額】**

ご提供タイプは下記の２種類となります。

| タイプ | 価格(税別) | メニュー | 条件 |
|---|---|---|---|
| 基本再現型 | 350万円 | ランサムウェア感染リスク可視化サービス | USBメモリ経由で疑似マルウェア攻撃を実施<br>対象PC数　　：2台<br>対象IPアドレス数：255 まで（境界越え含む） |
| | | サブドメイン乗っ取り対策サービス | 10FQDN |
| | | ネットワークスキャンサービス | サブネットマスク：/25（128IP） |
| 完全再現型 | 500万円 | ランサムウェア感染リスク可視化サービス | 貴社環境に疑似攻撃サーバを構築して疑似攻撃メールを送信<br>配信数　：1回につき50名様宛<br>配信形式：パスワードつきZipファイル |
| | | サブドメイン乗っ取り対策サービス | 10FQDN |
| | | ネットワークスキャンサービス | サブネットマスク：/25（128IP） |

**本サービスの詳細はこちら**

https://www.bbsec.co.jp/campaign/202012_ransomware/

以上

**【本サービスに関するお問合せ】**
株式会社ブロードバンドセキュリティ　セキュリティサービス本部
TEL：03-5338-7417　E-mail：sales@bbsec.co.jp

**【本リリースに関するお問合せ】**
株式会社ブロードバンドセキュリティ
管理本部　経営企画部　コーポレートコミュニケーション課
TEL：03-5338-7430　E-mail：press@bbsec.co.jp