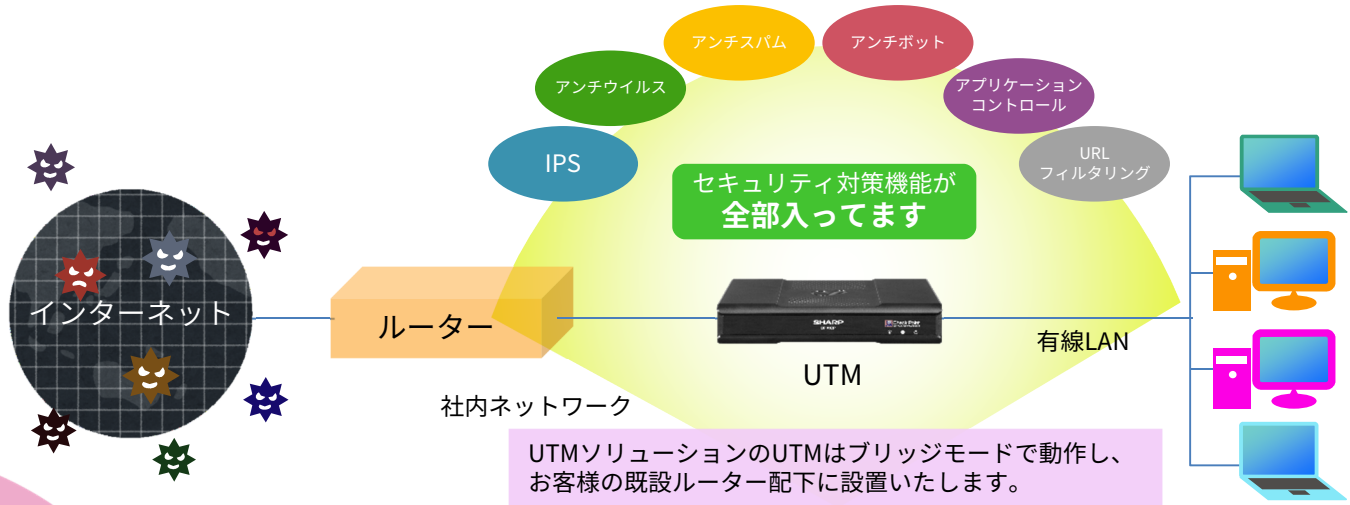
テレワーク拡大により増大する
ネットワーク脅威の対策に

SHARP　UTM　BP-X1CPシリーズ

チェック・ポイント・ソフトウェア・テクノロジーズ社製ベースエンジン採用

■UTM（統合脅威管理）セキュリティ■

異なるバラバラなセキュリティ対策機能を1つに統合し運用管理コストを削減。



UTM(統合脅威管理)ソリューション

ネットワークセキュリティ対策に求められるさまざまな機能を一体化
複数のセキュリティを統合的に管理しコスト削減と安心・安全を提供

ポイント1 外部からの脅威を防御

IPS

- 脅威の振る舞いとシグネチャに基づく、数千種類におよぶ外部からの攻撃に対する防御機能を提供します。

アンチウイルス

- 脅威情報配信サービス「ThreatCloud™」から配信されるリアルタイムのウイルス・シグネチャとアノーマリ・ベースの検出機能を使用して、マルウェアをゲートウェイで検出し遮断することで、ネットワークの手前でマルウェアを阻止し、パソコンへの影響を防ぐことができます。

アンチスパム

- 送信者のIPレピュテーションをチェックすることにより、スパムやマルウェアを接続レベルでブロックします。
- 画像を利用したスパムや各国語のスパムなど、最新のスパムをパターン・ベースで検出します。
- メッセージ本文と添付ファイルのスキャンなどにより、多様なウイルスおよびマルウェアをブロックします。

ポイント2 内部からのリスクを軽減

アンチボット

- ボットに感染したパソコンを検出し、ボットと指令（C&C）サーバと呼ばれる制御システム間の通信を遮断して、被害を予防できます。

ポイント3 ネットワークの利用を制限

URLフィルタリング

- URLのカテゴリ毎にWebアクセスの許可・禁止・制限の設定ができます。
- 特定のURLをホワイト・リストとブラック・リストに登録することでポリシーをきめ細かく調整ができます。

アプリケーションコントロール

- 8,600以上のWeb 2.0アプリケーションや約25万のウィジェット※1を識別し、その利用を禁止または制限するきめ細かいポリシーをユーザーやグループごとに容易に作成することが可能になります。

ポイント4 リアルタイムな防御情報を配信

ThreatCloud™

- 脅威情報配信サービス「ThreatCloud™」は、世界中にあるゲートウェイから収集した情報をもとに、ゲートウェイに対して防御情報をアップデートするクラウドサービスになります。

※1：各識別数は、2021年6月時点のCheck Point AppWiki（https://appwiki.checkpoint.com/appwikisdb/public.htm）に基づきます。

■ 商品構成

構成	V80スタンダードモデル 5年/6年タイプ	V80ハイスピードモデル 5年/6年タイプ	V80WスタンダードWi-Fiモデル 5年/6年タイプ
UTM本体 UTM（統合脅威管理）BP-X1CPシリーズ			
導入時設置/設定サービス	○（導入時）		
ソフトウェアライセンス	5年/6年 ライセンス付属		
ヘルプデスク、UTM監視サービス、オンサイトハードウェア保守	5年/6年間		
簡易定期レポート（月1回メール配信）	5年/6年間		

Check Point SOFTWARE TECHNOLOGIES LTD

チェック・ポイント・ソフトウェア・テクノロジーズ社は、サイバーセキュリティ分野のリーディングカンパニーです。

米調査会社Gartner社の2020年度「Magic Quadrant for Network Firewalls」分野において、21年連続でリーダーに選出されています。

■ 商品価格

商品名	品番	価格
V80スタンダードモデル　5年タイプ	Y9CA35PV	オープン
V80スタンダードモデル　6年タイプ	Y9CA36PV	オープン
V80ハイスピードモデル　5年タイプ	Y9CA55PV	オープン
V80ハイスピードモデル　6年タイプ	Y9CA56PV	オープン
V80WスタンダードWi-Fiモデル　5年タイプ	Y9CA35PW	オープン
V80WスタンダードWi-Fi-モデル　6年タイプ	Y9CA36PW	オープン

シャープマーケティングジャパン株式会社
ビジネスソリューション社
〒261-8520 千葉市美浜区中瀬一丁目9番地の2
https://smj.jp.sharp/bs/

2021年7月 作成

Emotet(エモテット)への感染がまた急激に拡大しています。

Emotet(エモテット)に感染したかも？？

・取引先等から変なメールが送られてきた（との報告を受けた）
・メールの添付ファイルの「コンテンツの有効化」ボタンを押してしまった（との報告を受けた）
・コンテンツの有効化ボタンを押したが、その後何も表示されなかった（との報告を受けた）

こんな時！！

まずは感染有無のチェック！！
感染していた場合、感染を拡げないことが大切です！！

対策のポイントは次の６つ

①エモテット感染の有無をチェックする
②感染した端末のネットワークをインターネットから遮断する
③他のマルウェア感染の有無を調査する
④感染したアカウントのメールアドレスとパスワードを変更する
⑤感染した端末を初期化する
⑥感染拡大を防止する

対策の実行には下記のサイトが参考になります。

『警察庁HP　Emotet(エモテット)感染を疑ったら』
https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/emotet.html

①　EmoCheckを使用して感染の有無を確認する

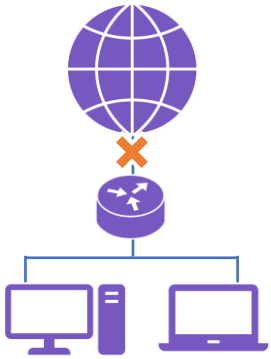
上記のサイトにEmoCheckの入手方法と実行手順が丁寧に掲載されております。

JPCERT/CCのマルウェアEmotetへの対応FAQ
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

② 感染した(または疑いのある)端末のネットワークを
インターネットから遮断する

②-1
有線LANの場合は、
LANケーブルを外す

無線LANの場合は
無線ネットワークを
切断する



②-2
感染端末が繋がって
いたネットワーク自体
もインターネットから
遮断しましょう

③ Emotet以外のマルウェアに
感染していないか調査する

EmoCheckでEmotetが検出
されなくても他のマルウェア
に感染していないかお使いの
ウイルス対策ソフトを最新の
状態にしてフルスキャンを
実行しましょう

④ 感染したアカウントのメールアドレス
とパスワードを変更する

Emotetはメール経由で外部に
感染を拡大します。感染疑いの
端末も含めて、感染の拡大を
防止し二次被害を防ぐ為に変更
しておきましょう

⑤ 感染した端末を初期化する

Emotetを含むマルウェアに
感染した端末は駆除出来たと
してもバックドアが残り再び
攻撃者の侵入を許す可能性が
あります。端末を初期化する
ことをお勧めします。

⑤ 感染拡大を防止する

もしEmotetに感染し、取引先
等へマルウェア感染メールを
発信してしまっている様な時は
出来るだけ早く被害状況を通知
し、自社名で出されたメールで
も注意を促すようにして、拡大
防止に努めましょう

EmoCheckを配布しているJPCERT/CC (ｼﾞｪｰﾋﾟｰｻｰﾄｺｰﾃﾞｨﾈｰｼｮﾝｾﾝﾀｰ)では
「マルウェアEmotetへの対応FAQ」を公開し、このサイトでEmotetの脅威や
先に説明したEmotet感染の確認方法と対策などについて動画で説明しています。
被害に合わない・感染を早期に確認する為の社員教育などにご活用頂けます。

日本中で感染が拡がる
マルウェアEmotet

https://youtu.be/wvu9sWiB2_U

Emotet感染の
確認方法と対策

https://youtu.be/nqxikr1x2ag