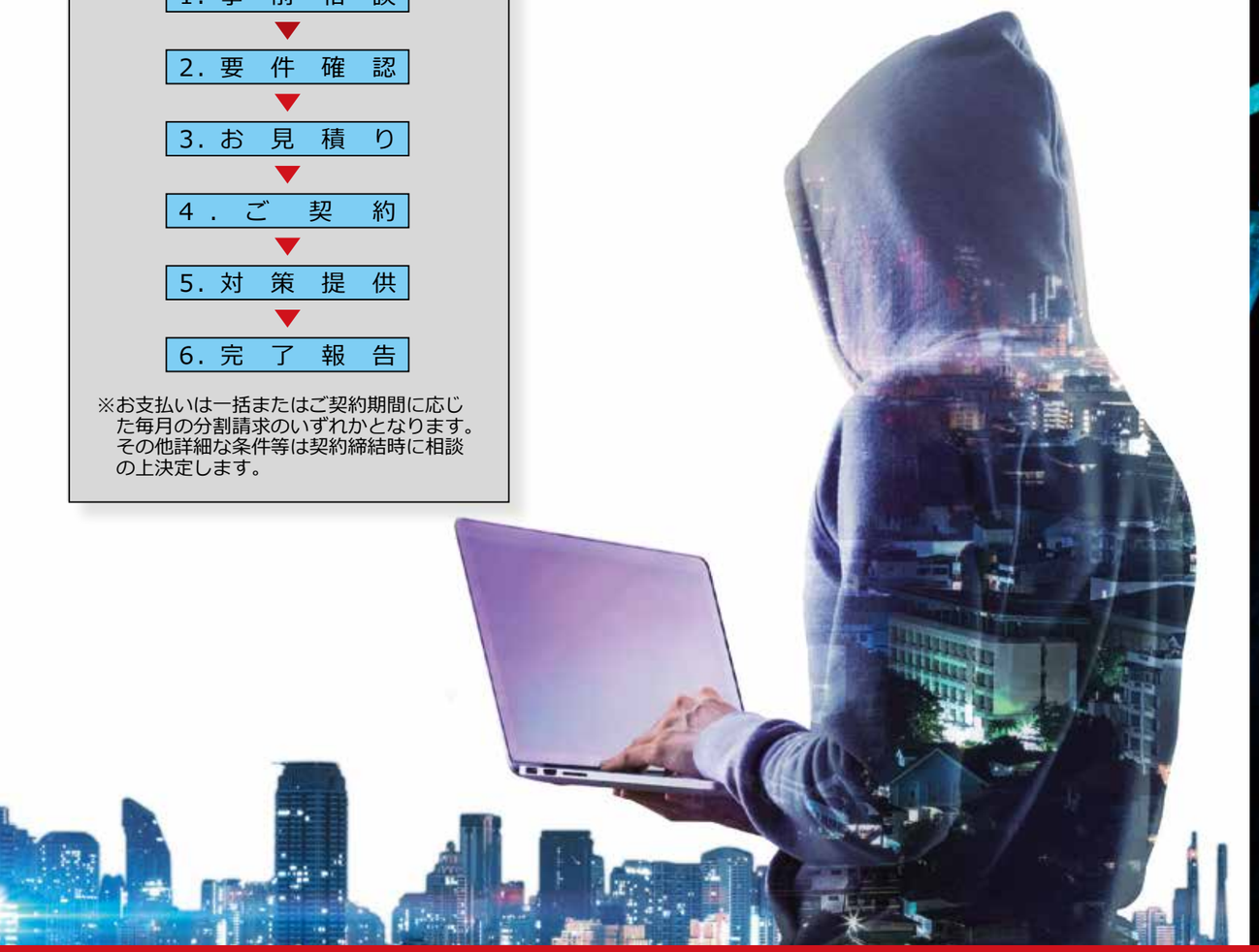
対策の進め方

1. 事　前　相　談
▼
2. 要　件　確　認
▼
3. お　見　積　り
▼
4. ご　　契　　約
▼
5. 対　策　提　供
▼
6. 完　了　報　告

※お支払いは一括またはご契約期間に応じた毎月の分割請求のいずれかとなります。その他詳細な条件等は契約締結時に相談の上決定します。



ホワイトハッカー監修

情報セキュリティ対策パッケージ

従業員のマイナンバーや
取引先の情報

これら

漏れてはいけない情報を守る
最低限の対策

デジタルの恩恵をすべてのひとに。

DIGITAL

ＩＴコンサルティング＆人材教育

デジタルデマンド株式会社

ＩＴコンサルティング＆人材教育

デジタルデマンド株式会社

法人番号：4-1000-0103-1113

〒380-0945 長野県長野市安茂里杏花台 590-13

電話：050-3204-4647
FAX：050-3488-4760
info@digitaldemand.jp
www.digitaldemand.jp

情報セキュリティ対策パッケージ

情報セキュリティ対策パッケージは、あなたの組織に必要な

「最低限の情報セキュリティ対策」

をホワイトハッカーが現地調査の上で策定し、

「ワンストップで提供」

するデジタルデマンドの IT コンサルティングパッケージです。

ホワイトハッカーとは

ハッカーとは一般的に、悪意を持ってＩＴシステムを攻撃し情報の盗取や破壊を行う存在です。これに対してホワイトハッカーは倫理観が１８０度異なり、悪意ある存在から情報資産を守る正義の存在です。

当社のホワイトハッカーは、試験で測れる範囲では国内最難関であるスキルレベル４の高度情報技術者「情報処理安全確保支援士」として、あなたの組織に最適な情報セキュリティ対策を立案し、提供します。

情報処理安全確保支援士

当社の立案する対策

ウィルス対策ソフトがあるにも関わらず、私たちは日々悪意あるメールやプログラム（マルウェア、ウィルス）やフィッシング詐欺、標的型サイバー攻撃による情報漏洩やランサムウェアによるデータ破壊など、あらゆる脅威にさらされています。

当社はこれらの様々な脅威に同時に対応するため、最低限の情報セキュリティ対策として、統合的な脅威対策（ＵＴＭ）を立案し、提供します。

ワンストップで提供

情報セキュリティ対策というと、難しいイメージをお持ちのことと思います。それゆえ普及の途上であり、あなたを含め多くの方がその恩恵を十分に受けているとは言えません。

当社は、専任のホワイトハッカーが必要な対策をワンストップで提供します。

※調査、立案、実施まですべて当社とのやりとりのみで完結することをワンストップと表記しています。

対　策　の　流　れ　※一例です。

1. 現地に通信検査機器を設置（悪影響はありません）
2. 半月～１ヶ月程度、実際の通信内容を検査
3. 検査結果に基づき、必要な対策を立案
4. 統合的な脅威対策（ＵＴＭ）機器をチューニングの上、導入
5. 経過観察し、結果を報告
6. 必要に応じて、従業員への情報セキュリティ研修

※集合研修となることがあります

補足事項：この商品はお客様の業務の成果や情報セキュリティ対策を保証するものではありません。商品のご利用にあたり、お客様と当社の間でコンサルティング業務委託（または委任）契約及び秘密保持契約を締結します。当社が提供したノウハウ（知見）は、秘密保持契約により第三者への提供等を制限することがあります。

期待される効果

ハッカー対ホワイトハッカーの暗闘は長年続いており、まさにイタチごっこの様相を呈しています。このため「絶対安全な対策」は存在しないものの、基本的には次のような効果があります。

悪意あるメールのブロック

標的型サイバー攻撃（あなたの組織を狙い撃ちにする巧妙に作り込まれた攻撃）の発端はメールであることが多く、悪意あるメールはＵＴＭ機器により受信者に到達しないようにします。

▶ 単なるメールのフィルタリングではなく、悪意あるメールかどうか総合的に判断します。また、仮に受信者が悪意あるメールを開いて不正な通信が発生しても、このような通信を遮断するなど、多層的に防御することができます。

悪意あるプログラムのブロック

あなたや組織の一員が日常のインターネット利用で、悪意のあるプログラムを判別するのは容易ではありません（なぜなら、判別しにくいように作られているからです）。悪意あるプログラムも、ＵＴＭ機器によりダウンロードを防止します。

▶ 単なるウィルス検査ではないため、ウィルスではないが悪意のあるプログラム（広告表示、詐欺アプリ、意味のないソフトなど）が入り込まないように防御することができます。もちろん、ウィルスのダウンロードも防御します。

ランサムウェアのブロック

ランサムウェアはあなたの守るべきデータに勝手に鍵をかけて人質にとり、返してほしければ金を振り込むように要求します。ＵＴＭ機器はランサムウェアに関連する活動のブロックを試みます。

▶ ランサムウェアは巧妙に作り込まれている場合があり、ウィルス対策ソフトだけでは防御しきれない事例が後を絶ちません。このような場合にも効果が期待できます。

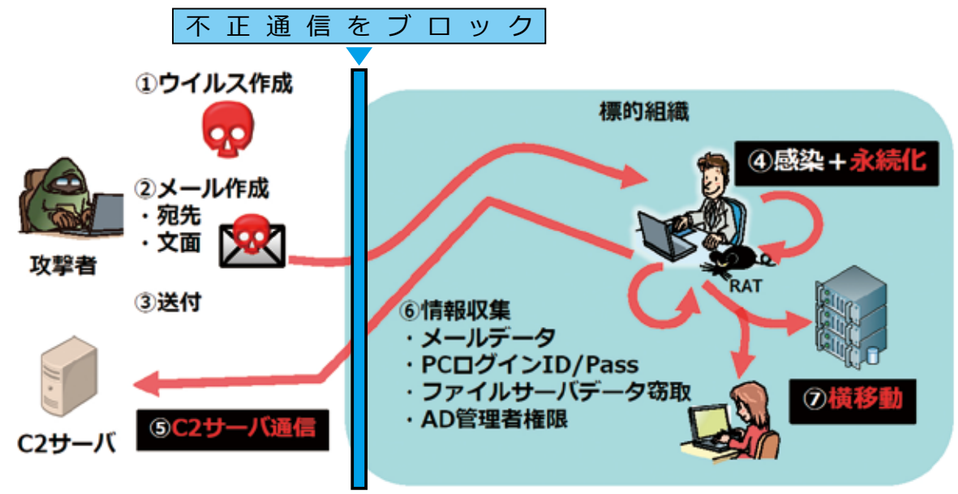
インターネット閲覧の制御

副次的な効果として、あなたが希望すれば、従業員のインターネット閲覧に制限をかけることもできます。例えば、業務中にギャンブルやアダルトコンテンツの閲覧ができないようにするなど、組織の生産性向上を図ることが可能です。

▶ 教育機関等で、子供たちに見せるにはまだ早いコンテンツ（暴力やＳＮＳ）の閲覧ができないようにするなどの使い道もあります。

参考：標的型攻撃の進行例

下図は標的型サイバー攻撃の進行例を表しています。ウィルス付きメールを開いたことが原因で組織内で悪意あるプログラムが潜み、攻撃者が任意のタイミングでＣ２サーバを通して組織の情報を抜き取れる状態ですが、当社の情報セキュリティ対策パッケージに含まれるＵＴＭ機器により、不正通信をブロックします。



※ＲＡＴとはリモートアクセスツールのことで、指令を送るＣ２サーバと通信し、⑥を行います。
※図は独立行政法人情報処理推進機構の作成した資料からの抜粋です。