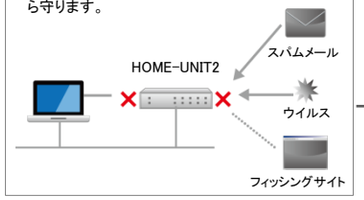
Canon Marketing Japan Solutions

御社のセキュリティ課題に応じ、最適なソリューションをご提案。

数々の企業で実績のある製品・システムとこれまで長く培ってきた経験、ノウハウにより、
個々のお客様の課題にフィットする包括的なセキュリティソリューションをご提案します。
どんなことでも、お気軽にご相談ください。

HOME UNIT2

ファイアウォール機能をベースに、アンチウイルス、アンチスパム、Webフィルターリングなど、さまざまなセキュリティー機能でオフィスを脅威から守ります。



HOME-BOX² Cloud Advanced Box

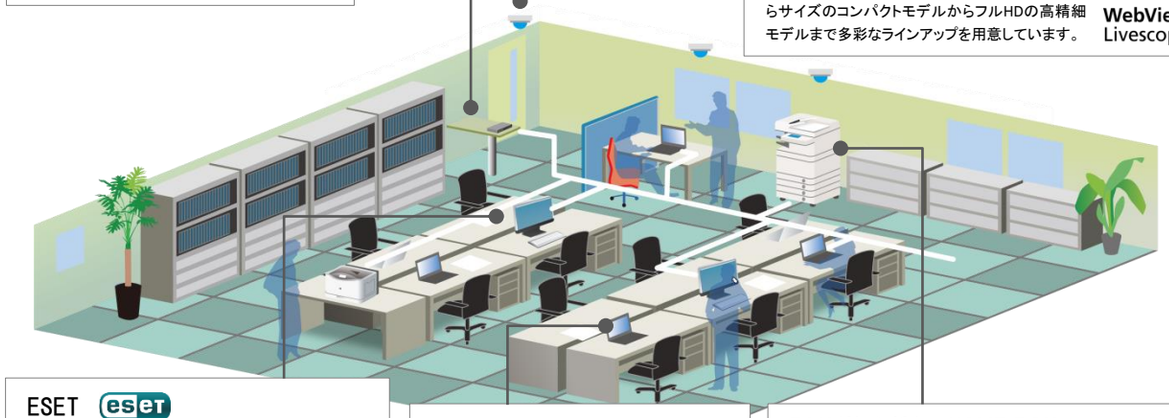
HOME BOX²

クラウドストレージである「HOME-BOX²」。HOME-BOX²との通信はすべてhttpsによる暗号化通信をおこなっていますのでデータをクラウド上に簡単・安全に格納できます。

ネットワークカメラ

店舗や工場からオフィスまで、さまざまなロケーションで高度なモニタリングを実現します。手のひらサイズのコンパクトモデルからフルHDの高精細モデルまで多彩なラインアップを用意しています。

WebView Livescope



ESET

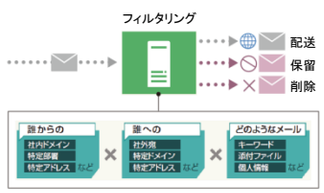
ESET（イーセット）セキュリティ ソフトウェア シリーズは、「高いウイルス検出率」と「軽快な動作」を両立。マルチデバイスに対応し、高度化・悪質化するマルウェアの脅威からあなたのインターネット生活を守ります。

ESET DESlock

フルディスク暗号化で内蔵のHDDやSSD全体を暗号化、さらにはOS起動時に利用するシステムドライブを暗号化することができます。万が一、PCやリムーバブルメディアを紛失したり、盗まれた場合でも、第三者への情報流出を防ぐことができます。

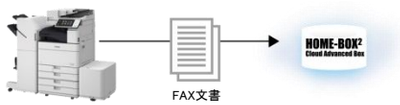
GUARDIANWALL Mailファミリー

3つのモデル体系から必要なモデル（機能）を自由に選択・組み合わせて利用いただける、メールに関する総合情報漏えい対策ソリューションで、相次ぐ情報漏えい事件や、標的型攻撃の増加など、情報漏えい対策が可能です。



FAX（複合機）→HOME-BOX

複合機に送られたFAX文書をクラウド上に簡単・安全に格納できます。HOME-BOX²との通信はすべてhttpsによる暗号化通信なので安全に格納できます。



imageWARE Desktop

異なるアプリケーションでつくられた複数のデータを、簡単に1つのPDFデータに。機密性の高い文書はパスワードを設定でき、メール添付用に圧縮することもできます。

●Canon、Canonロゴはキヤノン株式会社の登録商標です。●本紙に記載されている会社名、商品名は、一般に各社の登録商標または商標です。●記載の内容は2017年7月現在のものです。●弊社の都合により予告なく変更させていただく場合がありますのでご了承ください。

●お求めは信用のある当社で

2017年7月現在

Canon キヤノンマーケティングジャパン株式会社
〒108-8011 東京都港区港南2-16-6 CANON S TOWER

BUSINESS TREND NEWS

セキュリティ対策編

キヤノンマーケティングジャパンがお役に立てること

中小企業でもサイバー攻撃による被害が急増！

致命的な打撃を受ける前に 今すぐ有効な対策を！

- 甚大な被害を生む 国家レベルのサイバー攻撃が続発
- 取引先の大手企業への攻撃の踏み台として 中小企業が巧妙な サイバー攻撃の標的となる時代に
- 容易に作成、利用できる ランサムウェアにより 金銭被害や操業停止に 追い込まれる場合も
- ビジネスでの被害を 未然に防ぐために 対策のポイントを押さえましょう！

インターネットなしではビジネスが成り立たない今
中小企業もサイバー攻撃への対策を急ぎましょう。

2016年に発生した情報セキュリティにおける事案の中から、IPA（情報処理推進機構）が候補を選出し、有識者からなる「10大脅威選考会」が審議・投票で決定したランキングです。

1位：標的型攻撃による情報流出

2位：ランサムウェアによる被害

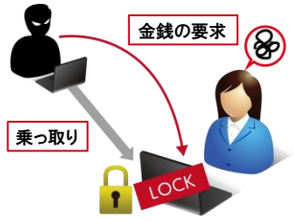
3位：ウェブサービスからの個人情報の窃取
4位：サービス妨害攻撃によるサービスの停止
5位：内部不正による情報漏えいとそれに伴う業務停止
6位：ウェブサイトの改ざん
7位：ウェブサービスへの不正ログイン
8位：IoT機器の脆弱性の顕在化
9位：攻撃のビジネス化（アンダーグラウンドサービス）
10位：インターネットバンキングやクレジットカード情報の不正利用

標的型攻撃とは

標的型攻撃は、情報や金銭を不正取得することなどを目的に、特定の組織・個人を狙って行われるサイバー攻撃です。その手口は年々ますます高度化しており、IPAのランキングでは前年に引き続いての1位となっています。

ランサムウェアとは

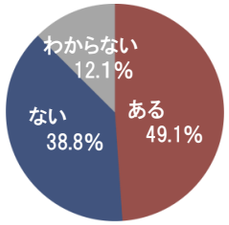
PC、スマートフォンにあるデータを勝手に暗号化したり、画面ロックし、その解除と引き換えに金銭を要求してくるというコンピュータウィルスです。主な感染経路としてはスパムメールが多く、IPAのランキングでも前年の7位から急上昇しています。



約半数がECサイトへのサイバー攻撃を受けた経験「あり」

サイバー攻撃が深刻化の一途をたどっています。中でも昨今、特に急増しているのが、中小企業の被害。個人レベルも含め、10万を超えるECサイトがあると言われる中、セキュリティの脆弱なサイトは格好の標的であり、また中小企業を経由し取引先の大企業の機密情報を入手しようとしたケースも報告されています。業務でのインターネット利用が当たり前となった今、「うちの会社は大丈夫」という意識は捨て、忍び寄るサイバー攻撃の脅威に備えて、日々対策を実施していくことが大切です。

トレンドマイクロ社の実施したECサイトの実務担当者619名を対象とした調査によれば、全体の49.1%にあたる304名が、自社のECサイトに対してサイバー攻撃を「受けたことがある」と回答しています。



「企業におけるECサイトのセキュリティ実態調査2016」
（トレンドマイクロ調べ）

中小企業が受けたサイバー攻撃の実例

従業員10人以下でも、サイバー攻撃の標的に

A社では、自社が運営するECサイトへの不正アクセスで顧客情報が流出した可能性を公表

第三者からの不正アクセスで、管理者権限が奪われ・・・

B社では、カード決済代行会社からの連絡で、3,989件のクレジットカード情報の流出が発覚

突然、注文メールが大量に届いたことで被害が発覚

C社では、Amazonの出店アカウントへの不正アクセスにより、意図せず25,000アイテムが出品

連続した不正アクセスを確認し、サイバー攻撃と認識

D社では、ホームページへの連続した不正アクセスを確認、その後のログの調査で漏えいを確信

Webサイトの改ざんが発生し、サーバを緊急停止

E社では、会員管理画面への不正アクセスと個人情報領域での攻撃を確認し、サービスを全面停止

中小企業が今やらなければいけないこと

最近のサイバー攻撃は非常に巧妙化しています。システム環境の更新やセキュリティ対策ソフトの導入はもちろん、不審な送信元や本文に違和感が残るメールには最大限に注意を払うなど、入念な対策を進めましょう。

まずは 基本的な対策

OSやソフトウェアは常に最新の状態にしよう！

セキュリティ上の問題を放置せず、常に修正プログラムの適用や最新版の利用を心がけましょう。

ウィルス対策ソフトを導入しよう！

ウィルス対策ソフトを導入し、ウィルス定義ファイルが常に最新の状態になるようにしましょう。

パスワードを強化しよう！

「長く」「複雑に」「使いまわさない」ことに注意して、パスワードが推測・解析されるのを防ぎましょう。

共有設定を見直そう！

クラウドサービスや機器が必要な人にのみ共有されるように、もう一度設定をチェックしましょう。

脅威や攻撃の手口を知ろう！

取引先を偽ったメールや正規のウェブサイトに似せたサイトへのアクセスに気をつけましょう。

社員教育を徹底しましょう！

サイバー攻撃から企業を守るために、社員教育を徹底し、一人一人の意識を変革しましょう。

さらに 標的型攻撃、ランサムウェア対策

不審なメールの添付ファイルやリンクに注意

最近の不正メールは、受信者が疑いを抱かないようにさまざまな騙しのテクニックが施されています。添付ファイルや本文に記載されたサイトへのリンクをクリックする際には、細心の注意を払ってください。

重要なファイルは定期的にバックアップ

ランサムウェアは、感染した端末からアクセスできる共有サーバー内のファイルも暗号化してしまいます。定期的にファイルのバックアップを取得し、PCやサーバーから切り離して保管してください。

要求されても絶対に金銭は払わない

犯人の要求どおりに身代金を払ってもファイルが復元される保証はなく、お金を払う会社であることが認識されれば、次なる攻撃の標的にもなりかねないことから、金銭の支払いは推奨されていません。

キヤノンマーケティングジャパンの取り組み

キヤノンマーケティングジャパンでは、従業員一人ひとりのコンプライアンス意識向上および浸透を促進するとともに、ワークフローの至るところに漏えい対策のしくみを導入。特別意識しなくても、日頃の業務を通じて知らず知らずのうちに情報セキュリティ対策が徹底できています。

取り組み例
情報セキュリティ報告書2016
キヤノン情報セキュリティ　検索

もし被害にあってしまったら…

下記のリンク先は、ウィルスおよび不正アクセスに関するご相談窓口です。万が一被害にあった場合には、こちらへご相談ください。

■情報処理推進機構（IPA）情報セキュリティ安心相談窓口
https://www.ipa.go.jp/security/anshin/index.html