地元経営者のための『事業継続をサポートする』セミナーイベント

大多数の企業がウイルス攻撃をされている実態解明！セミナー!!

18社23名の方にご来場いただき盛況のセミナーを開催できました！

第1講座 最新セキュリティ事故事例

株式会社ビーエスサイトー
サイバーセキュリティチームリーダー
澤木　聡生

最新のセキュリティ事故事例やウイルス感染デモを通じて、サイバー攻撃がより身近で危険をはらんでいる事を認識頂けたと思います。
最近の攻撃手段として『メール経由での攻撃』が多く確認されております。身に覚えのないメールは開かず破棄して下さい。巧妙化する攻撃手段を**人が判断して対処するにも限界**があるため 、複数の対策 を講じる**「多層防御」**により自社の**情報資産を守る環境を構築**して下さい。
無料セキュリティ診断・各種ご相談を受け付けてますので ご一報ください！

ポイント!
①知る
②最新化
③多層防御

第2講座 BSSクラウドバックアップ

ゲスト講師　篠田 知範 氏

事業継続に必要なのはデータです！とデータバックアップの必要性について熱く説いて頂きました。自然災害・サイバー攻撃・盗難が起きても、確かなバックアップが出来ていれば万が一の事態が起きても事業の継続は可能です。
データを守る「3－2－1ルール」を行って頂ければ自社のデータが使えなくなる心配はなくなりますので以下におさらいをします。
「3」 3つ以上のデータを造る
「2」 2種類以上の記録メディアを使う
「1」 バックアップの1つは離れた場所に保管する。

ポイント！
クラウドバックアップは、
インターネット上の金庫に
預けるイメージなので
災害や盗難に強い

※お知らせ※
BSSの年末年始休暇は、2017/12/29（金）～2018/1/4（木）迄となっております。
プリンタ、コピー機のトナー等の御用命はお早めにお願いします。

BSS通信

～2017年12月号～

早いもので、今年も残すところあとわずかとなりました。一年間、BSS通信をご愛読頂きましてありがとうございました。
来年も、“お客様の頼れるパートナー”となるべく従業員一同、誠心誠意努力する所存でございます。
引き続き変わらぬご愛顧のほど、何卒よろしくお願い申し上げます。

【注意喚起】2015年以降のインテルCPUに遠隔攻撃を許す深刻な脆弱性が発覚！早急なファームウェア更新の呼びかけ

2015年以降に販売されたインテル製CPUが搭載するプロセス管理用ファームウェアに、深刻な脆弱性が発見されました。10点を最悪とする脆弱性評価(CVSS)による危険度は最大8.2点で、インテルは早急なファームウェアアップデートの適用を呼びかけています。

影響を受けるのは以下のCPU

- **第6～8世代(Skylake、Kaby Lake、Kaby Lake R)のCoreプロセッサー**
- **Atom C3000、Apllo Lale系Atom E3900シリーズ**
- **Apollo Lake系Pentium**
- **Celeron NおよびJシリーズ**
- **Xeon E3-1200 v5～v6シリーズ**
- **Xeon スケーラブル・プロセッサーシリーズ**
- **Xeon Wシリーズ**

CPUとは、コンピュータの頭脳的な部分で、ご利用中のパソコン全てに入っている部品のことです。

CPUの種類で処理速度が変わってきます。

最悪の場合は、攻撃者がユーザーとOSが検知できないままに任意のコードを読み込み実行させられたり、システムの特権情報にアクセスされてしまうこともあり得るとのこと。インテルはCPU判定ツールを提供し、使用中のPCやPCサーバーに影響があるかを確認可能としました。またインテルのサポートページからは、主要PCメーカーのサポートページへのリンクを紹介し、各メーカーからファームウェアを入手できるようにしています。

「インテル®マネジメント・エンジンの重要なファームウェア・アップデート」でダウンロードページを検索できます。

https://www.intel.co.jp/content/www/jp/ja/support/articles/000025619/software.html

お問い合わせ
株式会社ビー・エス・サイトー
TEL:018-865-7400
FAX:018-865-7401
担当：澤木

あくまでも対象は、2015年以降 に購入されたパソコンですのでご留意ください。