桧山事務器からのお知らせ

HIYAMAto~

ヒヤマと

キヤノンマーケティングジャパン株式会社
3月開催のオンラインセミナーのお知らせ

会場に出向くことなく自席のPCで情報収集が出来ます

採用ミスマッチのシンプルな解消の仕方
～他社にない、御社独自の魅力をつくる～

開催日：**2021年3月19日(金)** 14:00～15:00

登壇者：ヤマゼンコミュニケイションズ株式会社
常務取締役　山本 純子 氏

対　象：経営者・総務人事部門のお客様

参加費：無料

内　容：

「良い人を採用したいけれど、なかなか出会えない」「入社してもすぐに辞めてしまう」「辞めてしまった本当の理由がわからない」などなど、人材の採用や育成には常にこのような悩みがつきまとります。

新型コロナウイルスでますます難しくなる人材採用、人材育成の悩みをこの機会に解消して、**本質をとらえた新たな採用スタイル**にチャレンジしてみませんか。

本セミナーでは、講師の企業向け人材育成経験と大学での講師経験双方の実体験を基に、**企業のどこに課題があるのか？学生は何を求めているのか？** をシンプルに伝えていきながら、皆様の採用ミスマッチを解消するお力になりたいと考えております。

お申し込みURL　https://canon.jp/business/event
（申込締切日：3月16日（火）17:30まで）

※お取引いただいているお客様へのご招待制セミナーの為、
お申し込みには事前登録が必要です。
弊社コード『**G11191**』をご入力の上お申し込みください。

桧山事務器株式会社
〒740-0017
山口県岩国市今津町1丁目7番16号
TEL：0827－22－2255（代表）
https://hiyamajk.co.jp

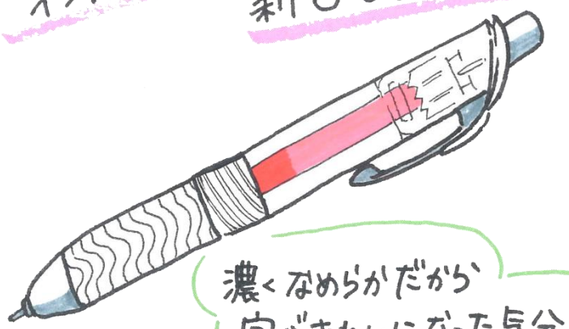
今月のイチオシ文具

スッと書けて
サッと乾く。

ゲルインキボールペン
ENERGEL
エナージェル

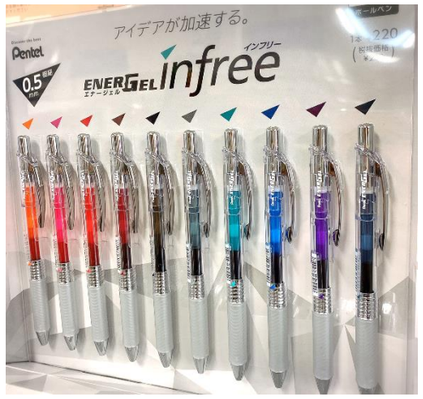
イラスト by 小坂

クリア軸
インフリーシリーズに
新色でました!!!



濃くなめらかだから
字がきれいになった気分♪

＼NEW／
バーガンディ
ラフグレー
レッド
ピンク
バイオレット



一般的なゲルボールペン
乾きが速い

エナージェル
乾きが速い

一般的な
油性ボールペン　　エナージェル
濃　濃

ぺんてる
エナージェルインフリー
定価￥200-
セヤマ税抜￥160-

ぜひ店頭でお試しください！

HIYAMA to~
2021
03

サイバー攻撃は絶え間なく続いています！
手口を知り、常に対策を行いましょう！

サイバー攻撃は日々、巧妙化・多様化しています。
その脅威は製造業に留まらず、法律事務所や建設業などにも広がっています。
今一度、サイバー攻撃への対策をヒヤマと一緒に見直してみませんか？

情報セキュリティ10大脅威 !! 2021

昨年の順位	個人	順位	組織	昨年の順位
1位	スマホ決済の不正利用	**1位**	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報の詐取	**2位**	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	**3位**	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**4位**	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	**5位**	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	**6位**	内部不正による情報漏洩	2位
10位	インターネット上のサービスからの個人情報の窃取	**7位**	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	**8位**	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	**9位**	不注意による情報漏洩等の被害	7位
8位	インターネット上のサービスへの不正ログイン	**10位**	脆弱性対策情報の公開に伴う悪用増加	14位

出典：独立行政法人情報処理推進機構「情報セキュリティ10大脅威2021」
https://www.ipa.go.jp/index.html

ランサムウェアってどんなもの？

ランサムウェアとは・・・
まずパソコンやサーバーのデータを暗号化して使用不可能にします。
次に暗号化したデータを復旧することを引き換えに身代金を要求する
メッセージを表示する、ウイルスの総称です。
最近では、窃取したデータを公開しないことと引き換えに、二重に身代金を
要求する脅迫被害も発生しています。

桧山事務器株式会社
Tel:0827-22-2255

御社のセキュリティに対する課題解決を
ヒヤマがお手伝いいたします！

巧妙な「なりすまし」にご注意ください！

山口県内の事業所宛てにも・・・
取引先企業を装った「なりすましメール」の受信が確認されています。

攻撃メールの中には、**正規のメールへの返信を装う手口**が使われている場合があります。
これは、攻撃対象者（攻撃メールの受信者）が過去にメールのやり取りをしたことのある、
実在の相手の氏名、メールアドレス、メールの内容等の一部が流用された、
あたかもその相手からの返信メールであるかのように見える攻撃メールです。

このメールには「Emotet」（エモテット）と呼ばれるウイルスへの感染を狙うファイルの添付
やURLが記載されています。業務上開封してしまいそうな巧妙な文面になっていることも
ありますので十分にご注意ください。

POINT

- OSやアプリケーション、セキュリティソフトを常に**最新の状態に**する
- 身に覚えのないメールの添付ファイルは開かない！メール本文中のURLリンクは**クリックしない！**
- 身に覚えのない警告ウインドウが表示されたら警告の意味が分からない場合**操作を中断！**
- 身に覚えのないメールや添付ファイルを開いてしまったらすぐにシステム管理部門等へ**連絡する！**
- 信頼できないメールに添付されたWord文書やExcelファイルを開いた時にマクロやセキュリティに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンは**クリックしない！**
- 自分が送ったメールへの返信に見えても不自然なメールの添付ファイルは**開かない！**

POINT

ウイルスはしっかり予防！きちんと対策！

侵入されないための対策

- **現状の識別** 現状のセキュリティ環境を把握することからスタート
- **攻撃の防御** 外部攻撃から守る！

重要!!
侵入されてしまった場合の対策

- **侵入の検知** 攻撃をいち早く検知！
- **感染の対応** スピーディーに対応し感染拡大を防ぐ！
- **正常に復旧** 適切な措置を検討・実施！感染前の状態に復旧