

✿ 個人情報が流出した際、確認すべきポイントについて ✿

連日の報道にもありますが、企業への不正アクセスや個人情報が漏えいする被害が急増しています。個人情報が流出すると、なりすましや不正送金、詐欺等の二次被害につながる恐れがあります。自分の個人情報漏えいが判明した際に確認すべきポイントをご紹介します。

【何が漏れたか確認】

漏えい元の事業者からの通知内容を確認し、再発防止策や問合せ窓口を確認する。

【パスワードの変更】

パスワードや暗証番号を直ちに変更する。

同じパスワードを使い回している他のサービスも含め、すぐに別の強力なパスワードへ変更する。

【利用停止の依頼】

クレジットカードや銀行口座の番号が含まれていた場合は、カード会社や銀行へ連絡して利用停止や再発行の依頼をする。

【アクセス履歴・明細の確認】

アカウントのログイン履歴や、クレジットカード・銀行の利用明細に身に覚えのない不審な動きがないか確認する。

【不審な連絡への警戒】

漏えいした情報を元にしたりすまし電話やフィッシング詐欺メールが増えるため、安易に個人情報を伝えない。

URLは正規サイトからアクセスし、メール内リンクは極力開かない様にする。

✿ 美味しいお店の紹介 ✿



ご紹介するのは、以前から気になっていた高松市茜町の「洋食 Grazie (グランチエ)」。

ランチで伺いました。

わたしは「讃岐夢豚のポークジンジャー Aセット(ライス・みそ汁)」、友人は「讃岐夢豚のポークカツレツ Aセット(ライス・スープ)」を頼みました。

なんといっても盛り付けが繊細でとても美しい。キャベツの千切りは極細ふわふわ、きゅうりは飾り切りされていて、店主の丁寧さが伝わります。そして豚肉が肉厚なのに驚くほど柔らかくて感動。ジンジャーソースたっぷりで豚肉の旨みもしっかり感じられます。ジンジャーとブタミンパワーで元気をチャージ。お腹いっぱい大満足!(^^)!他のお客さんが頼んでたオムライスも美味しそうだったな！

お店には赤玉ワインのボトルがたくさん並べられていたから、友人が頼んだポークカツレツのソースにも使われてるのかな～

見た目の美しさと美味しさの両方を楽しめる素敵なランチをいただいて、ちょっと贅沢な気分になりました！帰りに飴ちゃんいただきましたよ～ 🍭

駐車場はお店の前に2・3台ほど。人気店なので予約がおすすめです。



讃岐夢豚のポークジンジャー



讃岐夢豚のポークカツレツ



赤松事務機株式会社
代表取締役 片松 保佳

『社長のつぶやき VOL.107』



10月になりました。朝晩はひんやりしてきましたが日中はまだ半袖でもいけるのでは？という日々が続いています。道を歩いていると金木犀の香りがふんわり漂ってきて秋を感じさせてくれますが、日中の気温のせいで何だかスパッと秋だなと感じられない10月です。9月のシルバーウィークに続き今月も3連休がありました。今月の連休はスカッと秋晴れで行楽日和でしたね。お出かけされた方も多いのではないのでしょうか？日中の気温は高めとはいえ、ボーッとしているとすぐに冬の足音が聞こえてきて素晴らしい気候の秋を取り逃がしてしまいそうです。「食欲の秋」「スポーツの秋」など様々な「秋」がありますが皆様はどのような秋をお過ごしでしょうか？

表面冒頭にサイバーセキュリティに関する記載がありました。最近は毎日のように（ではなく本当に毎日）各種メディアで大手企業やデータ管理会社のインシデントが報道されています。が、報道されているのは本当にごくごく一部分です。実際は数えきれないほどのインシデントが日々起こっています。先日もデンマークで「デンマーク版マイナンバー約880万人分の個人情報に不正アクセスがあった」という報道がありました。情報漏えいが明るみになる（情報漏えいが確認できる）ということはそれなりの対策をしているから判明するのです。中小企業は大手企業に比べてセキュリティ対策にける人も予算も圧倒的に少ないのが現状です。「すでにやられているのに分からない（やられていることを認識できていない）」そんなケースが圧倒的に多いのではないかと推測できます。世界中に存在する攻撃者は攻撃を試みる際に企業名・企業規模などで判断しません。「どこが侵入しやすいか（どこに塞がれていない脆弱性があるか）」で攻撃の判断をします。そして侵入が成功した後に企業規模や業種などを見て脅迫内容を決めます。また、ここ最近はAIが凄いいスピードで進化しているためにAIを使って脆弱性があるかどうか調査します。例えばAIを使って攻撃先を調査して脆弱性が残されたままである入口を探す作業がマンパワーのみである場合と比べて数百分の一の時間と工数でできるようになります。だからサイバー攻撃はより増えていく、そんな構図になっています。それでは私たちはどのように脅威に対応していけばいいのでしょうか？少しの予算でもできる対策はあります。また、お金をかけなくてもできる対策も多くあります。①VPN機器・ルーター・無線アクセスポイントなどの通信機器の最新ファームウェアへのアップデート ②①の機器類やクラウド・WEBサイトなどにアクセスする際のパスワードをできれば12桁以上で類推されにくいものとし、2段階認証などを必須とする ③WindowsUpdateの確実な実施 ④メール・SNS・ショートメッセージなどからのリンクをクリックする場合には十二分に注意する、もしくは送信者が信頼できることを確認するなどを日々行っていれば被害に遭うリスクはかなり下がります。是非、できることから確認して実施していきましょう。もし、「どんな対策をしていいかわからない」など不明な点がございましたら弊社までお問い合わせ下さい。

来月は11月です。もう年末が近くなっていますね。それだけでなんだか心がざわつくのは私だけではないはず（だと思います）です。そんな心持ちになった際には楽しいこと（楽しくなること）を考えてざわつきをトキめきに変えたいですね(^^)

IT用語

■ 不正アクセス ■

「不正アクセス」とは、本来はアクセス権限を持たない者が、サーバや情報システムの内部へ侵入する行為です。その結果、サーバや情報システムが停止したり、重要情報が漏えいするなど、企業や組織の業務やブランド・イメージなどに大きな影響を及ぼします。

顧客情報などが漏えいすると、その企業や組織の信用が大きく傷つけられてしまうのは言うまでもないことですが、過去には損害賠償にまで発展した事例もあります。このように、不正アクセスは甚大な被害をもたらしかねません。

インターネットは世界中とつながっているため、不正アクセスは世界中のどこからでも行われる可能性があります。

出典：総務省ウェブサイト https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/risk/07/

弊社では、情報セキュリティ対策商品、UTM(統合脅威管理)等の取扱いをしております！
HPでも紹介しておりますのでぜひご覧頂ければと思います!!!
対策は早目にしましょう！

ホームページはこちら ▶▶



<https://akamatsu-jim.co.jp/>

情報セキュリティ
経営リスク対策に

詳細はこちら >

次世代型ミーティングボード
MAXHUB

詳細はこちら >