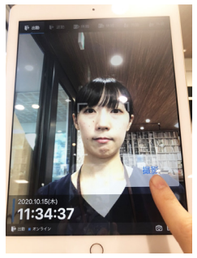
Imadokiアイテム　顔認証でスマートに出退勤！ 顔認証 AI エンジン「NeoFace」

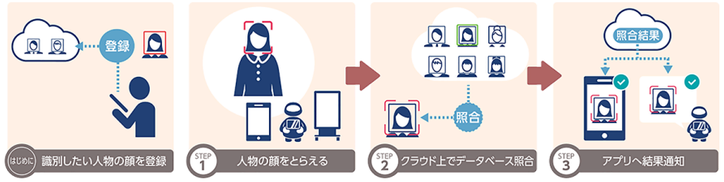
コムデックでも多くのお客様に導入させていただいているクラウド型勤怠管理システム「KING OF TIME」。
ID+パスワードを入力しての PC 打刻や、各自のスマホでの打刻、指紋・静脈を使った生体認証、IC カードを利用した打刻等、多彩な打刻方法を選ぶことができる KING OF TIME ですが、この度コムデックでは「顔認証」を導入致しました！



こちらの顔認証システム、なんと iPad があれば導入することができますので、省スペースかつネット回線を引いていない場所、例えば飲食店や小売店等の設置スペースが限られる場合でもすぐに使い始めることが可能です。打刻方法も、ログイン ID やパスワードは必要なく、「撮影」ボタンを押すだけなのでとっても簡単。登録も顔を映して写真を撮るだけで完了しますので、人の出入りが激しい会社様にもうれしいシステムとなっております。

KING OF TIME

管理者から見える画面



残念ながら体温を測る機能はついておりませんが、このコロナ禍において「なるべく触れずに」「素早く」、かつお手軽に導入できる顔認証システム。
御社の勤怠管理の見直しと共に、一度検討されてはいかがでしょうか？

今月の COMDEC LAB コムデックラボ PICK UP ピックアップ

事例１　クレーンメンテ広島様の事例

お客様からサインが必要な書類、たくさんありますよね？
「こちらにサインをお願いします！」とお客様にお願いし、サインをいただく。
そのあとに「すみません、こちらにもサインを･･･」と複数枚に渡りサインをいただかなくてはならないことはありませんか？
”めんどくさいけどこれ以外に方法がないから仕方ない･･･” と諦めているそこの企業様！
IT の力を使えば” めんどくさい” からも脱却でき、お客様からのイメージも大幅アップします！

記事全文はこちら

事例２　カワチョー様の事例

皆さん、スケジュール管理はどうしていますか？
Excel で作成した紙に手書き･･･ホワイトボードに手書き･･･。
「急な依頼が入ったので、以降の予定も変わります！」
せっかく手書きしたスケジュールを書き直して、現場の人たちに連絡･･･。
情報の更新と共有にどうしても時間と手間がかかってしまいますよね。
クラウドサービス” kintone" を使えば、そんな双方の課題が解決されるだけじゃなく、蓄積されたデータを基に、車両や従業員の稼働率がわかるようになるんです！

記事全文はこちら

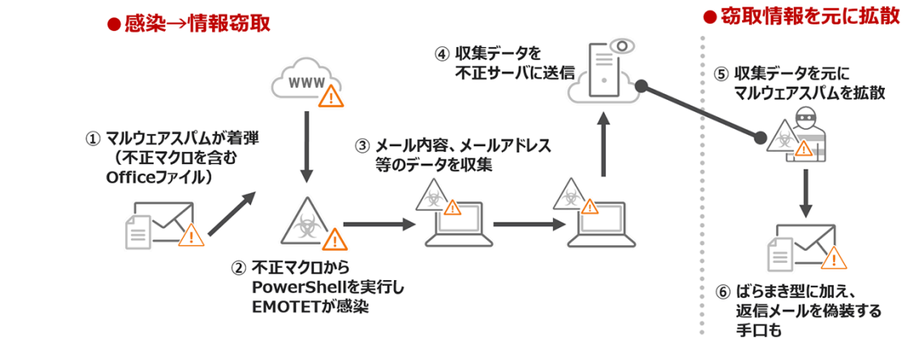
COMDEC
株式会社コムデック
〒516-0007　三重県伊勢市小木町 484-1
TEL 0596-31-1100　HP www.comdec.jp

COMDEC 公式アカウント

要回覧　確認印

COMDEC
Imadoki
2020 November 11
vol.67

Emotet 感染の流れ図



トレンドマイクロ様　https://www.trendmicro.com/ja_jp/business/campaigns/emotet.html　より

“Emotet（エモテット）”ウイルスメールによる感染拡大中！

「Emotet」（エモテット）と呼ばれるウイルスへの感染を狙う攻撃メールが、国内の組織へ広く着信しています。
特に、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攻撃メールに流用**され、「正規のメールへの返信を装う」内容となっている場合や、業務上開封してしまいそうな巧妙な文面となっている場合があり、注意が必要です。

請求書の件です。　ご入金額の通知・ご請求書発行のお願い　会議への招待　ドキュメント

といったタイトルでメールが届きますので、なかなか偽物と見破れず感染が広がるケースがありますので油断が出来ませんね。
また、上図のような流れで情報が盗まれるため、PC 端末と攻撃してくる端末が異なります。そのため、一度情報を盗まれると停止する手段がない点も特徴的です。

感染しないためには、該当のメールを開封しない事が一番いいのですが、私も Facebook メッセンジャーで届いた SPAM メールを開封してヒヤッとした経験があります。知り合いからの連絡には気が緩みますので、ただ注意をすれば済む話ではございません。
※Facebook には、ショートメッセージサービスを利用した二段階認証が設定済みでしたので被害はありませんでした。

コロナ禍により自宅や外部で業務を行うことが増えたため、会社のセキュリティ環境（UTM(統合脅威管理装置)）から離れる機会が増えました。それだけに人の誤謬をついてくるウイルスには、ウイルス対策は当たり前として、”Exchange Online”や "Gmail" によるメール対策など複合的な対策が必要となります。

いつ感染するかわからないのは、コロナウイルスと同じです。
最近はパスワード付き ZIP ファイルを使った攻撃まで出てきていますので、ますます対策が難しくなっている Emotet ウイルスには、十二分にご注意ください。

代表取締役社長　樋口 雅寿

COMDEC 公式アカウント

特集 MAXHUB

Imadoki8 月号でもご紹介した MAXHUB。
WEB 会議に必要なカメラ、マイク、スピーカーはもちろんのこと、Windows を搭載しているため Zoom は既にインストール済み。
届いて電源をつなげばすぐに WEB 会議ができる、そんなハード面・ソフト面両方でのオールインワンのミーティングボードとしてコムデックで絶賛活躍中の 65 インチモニターですが、使えば使うほど WEB 会議の強力な味方であることが分かってまいりました！
MAXHUB を導入することで、御社の WEB 会議の付加価値向上間違いなし！その魅力をお伝えいたします。

MAXHUB を使うことで WEB会議がこう変わる！

POINT.1 ワイヤレスドングル・専用アプリでシームレスに画面を共有

これまでの WEB 会議では、同じ会議に自分と同じ会場で参加している（同じモニターを見て会議をしている）人が画面共有をしたいと思ったときには、その人にも WEB 会議お URL やパスワードを共有して会議に入ってもらわなくてはならず、またその画面を全体で共有するためには各種配線を付け替える必要がありました。
それが、MAXHUB ではまず MAXHUB そのもので WEB 会議を開催し、そこに対して自分自身の画面を共有しに行きます。そのため、その場にいるすべての人がシームレスに画面共有を行うことができるのです。

01 MAXHUB で WEB 会議を開催

MAXHUB にインストールされている Zoom にログイン

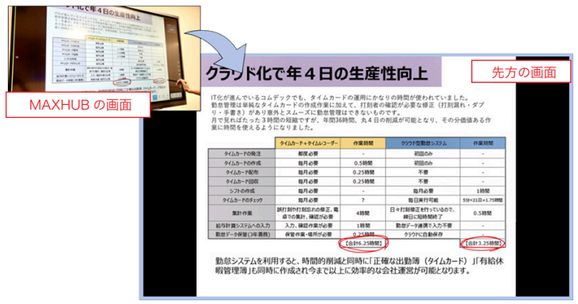
02 MAXHUB の画面を共有

MAXHUB の画面を相手に共有

03 ワイヤレスドングル or アプリで「MAXHUB」に自分の PC 画面を表示する

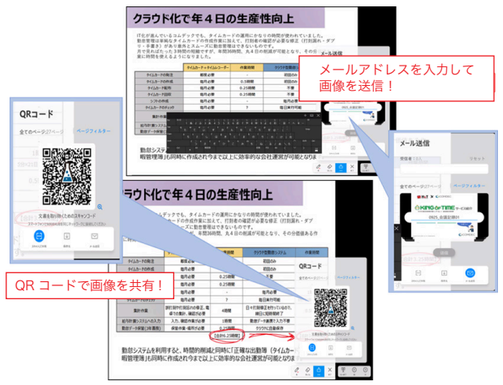
POINT.2 ホワイトボード・ペン機能で指示語が格段にわかりやすく

対面であれば「ここが」「これが」と画面に表示させた情報を指させば伝わりますが、身振り手振りが見えない WEB 会議ではそうはいきません。
MAXHUB では、そんなときでも「ペン機能」を使うことで相手に明確に意図を伝えることができます。



POINT.3 書き込み資料も即共有、便利な QR コード機能も

会議中に資料に書き込んだ情報や、ホワイトボードに書いていった情報、もちろん相手にも共有したいですよね。そんな時でも、MAXHUB では直接メールで書き込んだページのスクリーンショットを送ったり、QR コードで共有することが可能です。

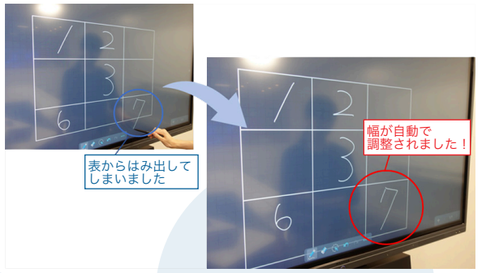


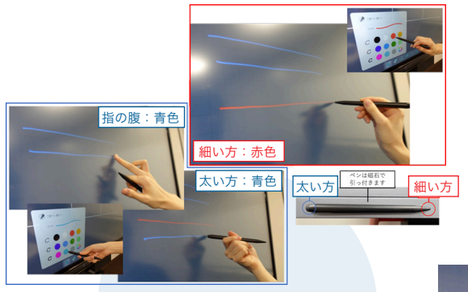
MAXHUB

まだまだ盛だくさん！

知って得する嬉しい機能

基本機能だけでも十分に利便性を感じていただけるのですが、
ちょっとした小技を知っているとより付加価値が向上します！





付属のタッチペンにはマジックペンのように「太い方」と「細い方」があります。
それぞれに色を設定し、無駄な動作なく色を切り替えることが可能です。

MAXHUB の認識は三段階
「太い方（指の腹もこちらになります）」と「細い方」に加えてもう一段階、「指の腹より大きい面積」では黒板消しの役割になります。広範囲を消せて便利！

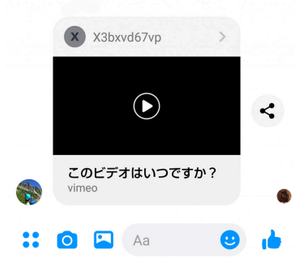
自動補正機能付きの表
ホワイトボードに表を挿入する機能があります。挿入した表の中に記入すると、記入した文字の大きさに合わせて表の幅を自動調整してくれます。

さらに詳しい機能解説はコムデックラボにも掲載しておりますので、是非ご覧下さい！
https://comdeclab.com/maxhub/

経営者様向け情報 IT 会社の社長が、Facebook の不正メッセージをクリックした話

どんなに気を付けていても、人間の隙をついてくるウイルス / スパムには勝てません。
私の場合、お恥ずかしながら女性からのメッセージには更に脇が甘くなりますので、引っ掛かってしまいました。

誤り①
母校である鳥羽商船の同窓会関係者からのメッセージであったことで油断しました。
同窓会で放映するビデオの話？と脳内で勝手に話を作ってクリックしました。



誤り②
次に Facebook の偽ログイン画面が出るのですが、迷わず ID、パスワードを打ち込みました。
当然これで ID/ パスワードを盗られたわけです。

その後 ...
直ぐに第三者がログインを試みる SMS の通知届きましたので、ID、パスワードが盗まれたのが確定しました ...
可能な限りのサービスで、二段階認証を設定する習慣に今回は救われましたが、簡単に騙された自分にショックです（涙）

皆様に言うのもナンですが、ご注意くださいませ。そして二段階認証は必ず設定しましょう！