

インターネット環境があれば自席で受講できます

## 3月開催オンラインセミナーのご案内



### オフィス家具のオカムラ・オンラインセミナー オフィスの“使い方”から考える オフィスづくりのよくある失敗回避術

2026年

日時

3月18日(水) 15:00~15:50

“従業員のモチベーションアップ”“コミュニケーションの活性化”など、目的や改善点を定めてオフィスを変えてみても「期待通りの結果が出ない」「上手に活用されていない」といった失敗は少なくありません。この背景には、実際の「働くシーン」や日々の「使われ方」まで十分に考えられていない可能性があります。本セミナーでは、オフィスの「場と運用の連携」に着目し、課題の見極め方や軌道修正のステップなど、企業のありたい姿を実現するためのポイントが盛りだくさんです！ぜひ、ご参加ください。

#### 【こんな方におすすめ】

- ・今のオフィスに課題を感じている方
- ・これからオフィスや働き方の要件を決めていく方
- ・他社のよくある失敗事例を押さえておきたい方

#### 【お申込み方法】

右のQRコードからオカムラのセミナーサイトにアクセスしてお申し込みください



## 書類管理を、もっとスマートに。

“持ち運びやすさ”と“使いやすさ”を  
両立したキャリーボックス



### KOKUYO

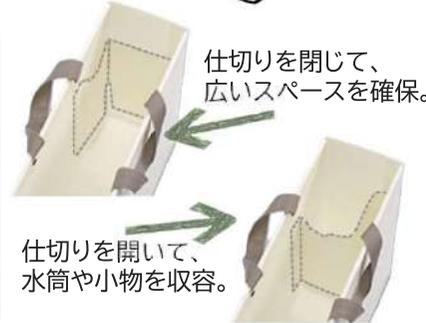
#### NEOSシリーズ

すっきり収納できるキャリーボックス

ワークツールをすっきりひとまとめ

- ◆A4サイズ
- ◆ノートパソコン(13.3インチPC対応)
- ◆他 A4 1/2サイズあり

内側に可動式L字仕切り付き  
収納スペースをあなたの好みで、  
確保できます！



仕切りを閉じて、  
広いスペースを確保。

仕切りを開いて、  
水筒や小物を収容。

スマートに運び、  
空間に溶け込む

- ◆サッと持ち運べる取っ手付き
- ◆オフィス空間に馴染む  
3色展開

社内での移動時にも、  
おすすめです！



★社屋建て替えのため、仮店舗にて営業しております★

【仮店舗】〒740-0018

岩国市麻里布町6丁目11番7号 ロイヤルメゾン1階

桧山事務器株式会社 TEL:0827-22-2255(代表)

【仮事務所】〒740-0017 山口県岩国市今津町1丁目7番16号

<https://hiyamajk.co.jp>



2026  
3

HIYAMA to~



「自分の会社は狙われないから大丈夫だろう」

その油断、ランサムウェア攻撃の対象です



ランサムウェアとは、不正にデータを暗号化して使用できなくし、復元と引き換えに身代金を要求するサイバー攻撃の一つです。昨年、大手企業が被害に遭い、我々の生活にも影響を及ぼしたことは、記憶に新しいのではないのでしょうか。ここでは、「ランサムウェア攻撃とは何か」「昨年の被害事例の一部紹介」「ランサムウェア攻撃の対策について」をご紹介します！

### ランサムウェア攻撃の流れ



データシステムの復旧と引き換えに身代金を要求  
+  
窃取したデータを公開しないことと引き換えに身代金を要求

身代金が払えない場合は、データの一部を公開し、日数の経過に伴い徐々に公開範囲を広げるなど、被害拡大へと繋がります。

独立行政法人情報処理推進機構【注意喚起】事業継続を脅かす新たなランサムウェア攻撃についてを基に作成  
<https://www.ipa.go.jp/archive/security/security-alert/2020/ransom.html>

### ▼情報セキュリティ10大脅威 2026【組織】

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い(2016年以降)
1	ランサム攻撃による被害	2016年	11年連続11回目
2	サプライチェーンや委託先を狙った攻撃	2019年	8年連続8回目
3	AIの利用をめぐるサイバーリスク	2026年	初選出
4	システムの脆弱性を悪用した攻撃	2016年	6年連続9回目
5	精密情報を狙った標的型攻撃	2016年	11年連続11回目
6	地政学的リスクに起因するサイバー攻撃(情報戦を含む)	2025年	2年連続2回目
7	内部不正による情報漏えい等	2016年	11年連続11回目
8	リモートワーク等の環境や仕組みを狙った攻撃	2021年	6年連続6回目
9	DDos攻撃(分散型サービス妨害攻撃)	2016年	2年連続7回目
10	ビジネスメール詐欺	2018年	9年連続9回目

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2026」を基に作成  
<https://www.ipa.go.jp/security/10threats/10threats2026.html>

### 2025年9月以降のランサムウェア攻撃被害事例

- 9月29日 某大手ビールメーカー  
サイバー攻撃によるシステム障害を公表。パスワード管理の脆弱性を突かれ、複数のサーバーに侵入されたとみられる。顧客や取引先に関する191万件を超える個人情報漏洩の可能性も。競合企業の生産活動にも影響を与えた事例の一つ。
- 10月17日 某旅客鉄道会社  
グループ会社(50社以上)に所属している従業員、退職者や派遣スタッフを含めた合計1万4,500人以上の個人情報が漏洩した可能性。
- 10月19日 某流通企業  
物流サービスの一部停止を公表。取引先の情報が一部漏洩していることが確認された。多方面で取引先に大きな影響を与え、本格的な事業活動復旧は2か月後となった。
- 11月7日 某ソフトウェア開発会社  
当初は情報漏洩の可能性は低いとされていたが、後に可能性は大きいと再度公表。
- 12月22日 某公立大学法人  
教育支援システムに障害発生。大学側は、外部への情報漏洩の可能性は完全には否定できないと説明している。

上記記事の事例は、サイバーセキュリティ.comの公開記事及び、日経メディカル(2026/02/13)、サイバーセキュリティラボ(2026/02/18)に基づき作成しています。

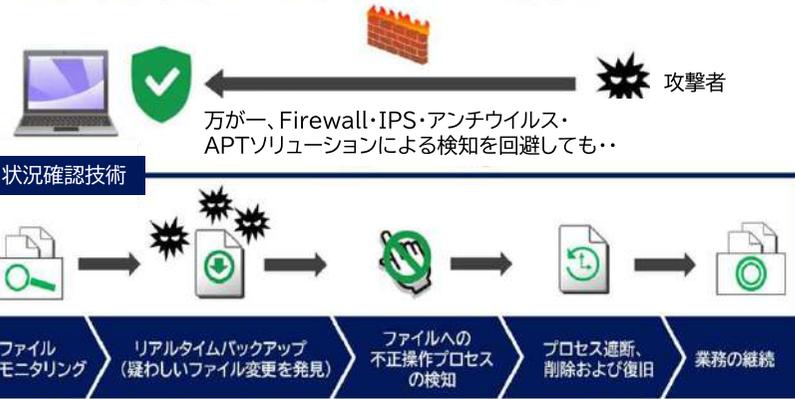
- 2026年1・2月 ランサムウェア攻撃被害事例
- 1月6日 某映像メディア支援企業  
認証サーバーへ攻撃を受け、一部サービスに障害発生。外部への情報漏洩は極めて低いと公表。
- 1月7日 某化学品専門商社  
受注や出荷に遅れが生じたが、外部への情報漏洩は確認されていない。
- 1月15日 某清涼飲料メーカー  
会計ソフトに登録されていた仕入先の銀行口座情報の漏洩を確認済み。調達や生産活動には影響は無いとしている。

- 1月18日 某産業廃棄物処理会社  
外部への情報漏洩の可能性有。一部業務に遅れなどの影響が発生。
- 2月5日 某レジャー施設運営会社  
発券システムで障害発生。最大1,518名の顧客情報が漏洩した可能性。
- 2月9日 神奈川県内の大規模大学付属病院  
ナースコールシステムサーバーで障害発生。約1万人の個人情報漏洩を確認済み。身代金として1億ドル(約150億円)を要求された。
- 2月13日 某大手ホテル運営会社  
業務データの不正アクセスにより、一部、クレジットカード端末が使用できない障害が発生。外部への情報漏洩は確認されていない。

### ランサムウェア攻撃対策に特化したソフト【AppCheck】をご紹介します！

#### AppCheckで解決！

AppCheckの状況確認技術により、未知のランサムウェアも検出・遮断し、復旧します



#### AppCheckの特徴

**状況確認技術を搭載**  
ファイル自体の変化を検出し、ランサムウェアによるファイル毀損をブロックします。

**リアルタイムバックアップ・復元**  
ファイルをリアルタイムでバックアップし、正常なファイルを保護します。万が一、ファイルが感染しても、元の状態へ復元可能です。

**軽快な動作**  
※シングネチャを使用しないため、軽快に動作します。そのため、既存のセキュリティ環境に追加してご利用可能です。

※シングネチャとは、既知のランサムウェアやウイルスの特徴を記録したパターンファイルのことです。

ご紹介している内容につきましては、ヒヤマの営業担当までお気軽にお問い合わせください。

楡山事務器株式会社 0827-22-2255(代表)



実際にAppCheckが検知・遮断・復旧を行う映像はこちら



キャンノンITソリューションズ AppCheckの詳細はこちら

