

セキュリティをテーマにした特集を2本同時に実施予定

ピックアップテーマ

- ・「有事の事業継続性を確保するサイバー攻撃からの回復戦略」
- ・「迫りくるサイバー攻撃！製造業が今すぐ取り組むべきOTセキュリティ対策」

■特集期間：2025年11月以降随時～2026年2月頃までの実施を予定

■お申込み締切：2025年12月26日（金）

セキュリティをテーマにした特集企画を緊急リリース

セキュリティリスクと事業継続の脆弱性が露呈した今だからこそ——
危機感が高まっている企業の経営層／情報システム部門／をターゲットにした特集企画を実施します

製造は一部再開

アサヒグループホールディングスへのサイバー攻撃 製造業が学ぶべき教訓とは

アサヒグループホールディングスのシステム障害に対して、ランサムウェア集団「Qilin」が犯行声明を出した。セキュリティの専門家は、製造業特有のITインフラの特徴と課題を指摘する。

2025年10月10日 09時00分 公開 [Alex Scroton, TechTarget]

印刷／PDF メール通知

関連キーワード
セキュリティ 災害対策 基幹システム 運用管理

2025年9月29日（日本時間）に発生した大手酒造会社アサヒグループホールディングス（以下、アサヒGHD）のシステム障害について、同年10月7日、ランサムウェア（身代金要求型マルウェア）攻撃集団「Qilin」が犯行声明を発表した。

アサヒGHDの事例から製造業が学ぶべき教訓は？

併せて読みたい関連記事

システム障害に備える

- ・ 給水システムの停止にどう対応する？ 災害に備える「復旧チェックリスト」
- ・ 事業損失や信頼ダウンに直結 システムを停止させる「4大原因」とは？

Qilinは、約9000件のファイル、合計27GBのデータを盗んだと主張しており、その中には財務書類、予算、契約書、計画および開発の予測、従業員情報が含まれているとしている。

アサヒGHDは2025年9月29日、システム障害に関する進捗（しんちよく）などをまとめた第1報を公開。復旧に向けた調査および対応を進めていることを報告した。同年10月3日に公開した第2報では、顧客や取引先の個人情報を含む重要データの保護を最優先にすると共に、被害を最小限にとどめるために障害の発生したシステムの遮断措置を講じたことを明らかにした。

アスクル、ランサム被害で注文キャンセル開始 「復旧に向け全社を挙げ対応中」

2025年10月21日 15時15分 公開

[ITmedia]



なぜ、いまエンジニアがコンサルへ？ 急成長企業が明かすその理由

なぜCopilot+ PCに“あの感震”が？ ACアダプタ不要で動くSnapdragonの威力

ランサム被害により受注と出荷を停止しているアスクル（東京都江東区）は、10月21日時点でユーザーの元に届いていない注文およびアスクルから発送する商品がキャンセルの対象になると発表した。メーカーからの直送品については出荷可否を確認中で、キャンセルとなる場合は別途案内するとしている。

ASKUL オフィス用品のアスクル(法人向け)

2025年10月21日

アスクル株式会社

【重要】ご注文キャンセルの対応とお詫び

平素よりアスクルをご利用いただき誠にありがとうございます。

現在、アスクルWebサイトにてランサムウェア感染によるシステム障害が発生しており、受注、出荷業務を停止しております。復旧にむかっています。

以下お客様に当てはまるご注文につきまして、誠に申し訳ございませんが、順次キャンセルさせていただきます。お客様には多大なるご迷惑、ご不便をおかけし、誠に申し訳ございません。

■キャンセルの対象となるご注文
・2025年10月21日現在で未出荷でございましてご注文
・アスクルから発送される商品
※商品によっては納期が延長される場合がございます。キャンセルの場合は別途ご連絡申し上げます。

■ご注文キャンセルの進捗について
10月21日より順次キャンセルを実施し、その後、ご案内メールを配信させていただきます。
※ご注文キャンセルのご案内メールはaskul@askul.co.jpからお送りいたします。
Webサイトでのご注文については、ご注文履歴の「ご注文履歴」画面（注文履歴）にてキャンセルをご確認いただけます。
※Webサイトの反映にお時間をいただく場合がございます。

お客様にはご迷惑をおかけしておりますことを重ねてお詫び申し上げます。
ただし、復旧に向けて全社を挙げて対応中であり、何卒ご理解を賜いますようお願い申し上げます。

以上

アスクルの発表より

同日からキャンセル処理を順次始め、処理が完了した注文から順次メールで通知する。案内メールは「info@askul.co.jp」のアドレスから送信する。

ピックアップテーマの特徴

編集部で注目するテーマや最新のトピックにフォーカスし、編集記事やコンテンツを集約したミドルページを開設します。ピックアップテーマとしてメディアで盛りあがりを作り、関心を持った読者からリード獲得します



特集ページを開設

編集部による解説や、関連する編集記事を掲載したミドルページをオープンします。貴社コンテンツも掲載されるので、特集に連動したリード獲得が可能です。



認知向上も実現

TechTargetジャパンやホワイトペーパーダウンロードセンターのバナー広告枠を利用し、本特集ページへ誘導をかけます。通常のリード獲得案件よりメディアでの認知向上も実現できます。



本プランならではの おすすめプラン

本特集ならではの効果的なプランで、テーマに関心を持つ読者のリードをご提供します。



有事の事業継続性を確保する サイバー攻撃からの回復戦略

■特集期間

2025年11月（お申込みいただき次第随時開始）～

■お申込締切：2025年12月26日（金）

特集テーマ

有事の事業継続性を確保する サイバー攻撃からの回復戦略

「いつ遭遇してもおかしくない現実」だったサイバー攻撃は、2025年10月のアスクルやアサヒグループホールディングスへのランサムウェア攻撃により、事業の即時停止という危機として顕在化した。ランサムウェアによりシステム停止、データ喪失といった危機に陥った後、どう事業を継続・復旧させるか——その体制を整備することは喫緊の経営課題だ。

この切迫したタイミングだからこそ、攻撃を前提とした「回復戦略（リカバリー戦略）」を自社できちんと構築できているのか、改めて見直したい。本特集では、サイバー攻撃に直面した際の事業継続性を確保する回復戦略の構築を検討中の担当者に役立つ情報を提供する。

■ 特集期間：

2025年11月以降随時～2026年2月頃までの実施を予定

■ お申込み締切：

2025年12月26日（金）

■ 実施スケジュール等：

- ・ 本企画はお申込みいただいた後、随時、リード獲得の開始と特集ミドルページへの掲載を行います
- ・ お申込み後、最短約4営業日～9営業日でリード獲得とミドルページへの掲載が可能です
- ・ ミドルページの掲載順はお申込みいただいた順となります
- ・ ミドルページないには、1社様あたりコンテンツ最大3本まで掲載可能です

※2025年12月27日～2026年1月4日は休業期間となります

ミドルページ（イメージ）

ビジネスの効率化と競争力強化を実現
クラウド ERP

クラウド環境で提供される統合的な経営システムである「クラウドERP」。グローバルなビジネス環境の変化やリモートワークのよう迅速にワークスタイルに対応し、スタートアップや中小企業にリアルタイムのデータにアクセスし、迅速な意思決定を可能にする。クラウドERPは、従来のERPシステムよりも柔軟性が高く、導入コストも低く、拡張性も高い。また、クラウドERPは、最新のセキュリティ対策を備えているため、データの漏洩や不正アクセスのリスクを大幅に低減できる。また、クラウドERPは、最新のセキュリティ対策を備えているため、データの漏洩や不正アクセスのリスクを大幅に低減できる。

おすすめホワイトペーパー・Webキャスト

日本オウカム株式会社
時代遅れのレガシーERPが企業にもたらす「8つの弊害」とは？
企業経営に不可欠なツールとして多くの企業が活用するERPだが、アップグレードせずに「バージョンロック」されたERPが、ビジネスを阻害しているケースは少なくない。そこで、レガシーERPがもたらす8つの弊害と、解決策を解説する。

日本オウカム株式会社
今、企業が「クラウド財務会計」へ移行している理由
ビジネスの継続的な成長には欠かせなくクラウドERPへの移行が加速しているが、導入効果を実感するには、そのERPが「真のクラウドERP」であるかを判断する必要がある。クラウドERPの真偽を判断するポイントとは何だろうか。

日本オウカム株式会社
使ったが課題も多い、スプレッドシートから脱却する意義とその実現方法
スプレッドシートを使い続ける企業は少なくない。もちろん強い強みはあるものの、ビジネスがある一定の規模に達すると、データ量が膨れ上がり、1つのスプレッドシートに収めるユーザー数が増えたりして、効率的に運用できなくなってしまう。

日本オウカム株式会社
グローバル企業が抱える、コンプライアンスと内部統制の課題を解消する方法とは
海外に事業を展開していると、各国の税制や工場、子会社などの状況をきっちりと把握し、コンプライアンスとガバナンスの両面で不安が生じることも少なくない。不正を防止し、信頼を構築するにはどうすればよいのだろうか。

日本オウカム株式会社
CIOや情シスリーダーは必見。クラウドERPがもたらすメリットを享受するには
ERPの採用により業務効率やコスト、アクセス、事業継続性などでの効果が期待できる。とウレシイのはクラウドERPが注目されて取り、導入する企業も増えているが、そもそもクラウドという点に不安を感じるCIOや情シスリーダーも多いという。

日本オウカム株式会社
組織がビジネス成長を遂げるため、ポストモダンERPを導入すべき理由
クラウドベースで提供されるポストモダンERPの導入、あるいはアップグレードは組織が今後市場における競争力を確保し、ビジネス成長を遂げるための条件といえる。なぜなら適切な理由があるのが、さまざまな事例を交えながら解説する。

会員登録がまだの方はこちら
4000社以上のホワイトペーパーから、課題資料や導入事例など、17種類の課題解決に役立つ資料を簡単に入手できます。

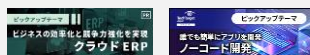
会員登録（無料）

編集コンテンツ

特集展開イメージ

ホワイトペーパー ダウンロードセンター特設枠

ホワイトペーパーダウンロードセンターに表示されるバナー広告で本特集を告知することで、ホワイトペーパーの閲覧を目的に訪れる読者を呼び込みます。



TechTargetジャパン サイト上での特集告知

TechTargetジャパン等に掲載されるバナー枠から、告知します。



ミドルページ (イメージ)



特集インデックスや活発に情報収集を行っている企業へのメールで貴社のホワイトペーパーに読者を誘導します。

※ミドルページPVの算出・レポートは行っておりません

パッケージプラン

パッケージプラン

		シルバープラン	ゴールドプラン
	ご提供価格 (Gross、税別)	1,000,000円	2,000,000円
含有率	50%以上の場合	60件	130件
	30～50%未満の場合	30件	65件
	10～30%未満の場合	25件	50件

本企画のポイント

本特集では、直近のセキュリティインシデントの影響で情報収集意欲が高まっている方のリード情報を迅速に獲得するため、【1カ月間】でのキャンペーン完了を目指します。

1. 最短納期保証

キャンペーン開始から最短1カ月間で保証件数の獲得を完了します

2. ターゲット属性保証

業種、職種、役職クラスなどの会員登録情報に基づきターゲットリードのみを件数保証します

3. 電話×メール両方を活用

コンテンツへの誘導には電話とメールを併用し、強力にキャンペーンを運用していきます

備考

- **コンテンツは2本以上ご用意ください。**1本しかご用意できない場合は、eBookやサーベイの併用をご相談させていただきます
- **掲載用タイトル／概要文の内容・変更は弊社にご一任いただきます**
- 貴社規定でテレマーケティングによる誘導が実施できない場合、本プランはご利用いただけません
- 誘導手法（メール、テレマーケティング）の内訳は弊社に一任いただきます。内訳のレポートもございませんのであらかじめご了承ください
- 含有率10%未満の条件のご実施をご希望の場合はご相談ください
- 1カ月で保証件数を獲得しきれなかった場合は下記対応をご相談させていただきます
 - 1カ月経過時点での獲得数での精算
 - 補填件数を上乗せした上で、獲得完了まで継続（補填件数は別途ご相談）



製造業の経営層・生産・工場部門モノづくりに関わる方
・情報システム職をターゲットにした特集

迫りくるサイバー攻撃！ 製造業が今すぐ取り組むべきOTセキュリティ対策

■特集期間

2025年11月（お申込みいただき次第随時開始）～

■お申込締切：2025年12月26日（金）

迫りくるサイバー攻撃！製造業が今すぐ取り組むべきOTセキュリティ対策

アサヒグループやアスクールへのランサムウェア攻撃でセキュリティリスクが顕在化している製造業へセキュリティ対策ツールを訴求する特集

製造現場ではスマートファクトリー化やDXに向けた取り組みが進む一方、工場内システムと外部ネットワークとのつながりが増えることで、サイバー攻撃のリスクが高まっています。その手口は年々高度かつ巧妙化しており、サイバー攻撃によって工場が停止したという事例も増加。製造現場におけるセキュリティ対策は急務となっています。こうした事態を受け、経済産業省では「工場システムにおけるサイバーフィジカルセキュリティ対策ガイドライン」を公開するなど、指針や法規制の整備が進められ、また海外でも法規制の厳格化が進み、現地企業と取引がある日本企業もセキュリティ対策の明示を求められる可能性があります。

キーワード

OTセキュリティ、産業用ファイアーウォール、産業用侵入制御システム、エンドポイント保護、セキュリティ検査ツール、ゼロトラスト、ネットワークセグメンテーション、IEC62443、NIST SP 800-171、経済産業省「工場セキュリティガイドライン」、半導体セキュリティ規格「SEMI E187」など

読者・会員 課題

人材不足、IT部門と生産部門の連携不足、ネットワークの混在や管理外端末の放置

想定リード属性

製造業の生産・工場部門モノづくりに関わる方、情報システム、経営企画職など

実施メディア

TechFactory/MONOist

実施期間

2025年11月以降随時～2026年2月頃までの実施を予定

申込締め切り

2025年12月26日（金）

スケジュール

お申込み後、最短約4営業日～9営業日でリード獲得・特集ページへの掲載が可能です
タイアップ記事制作は取材をしてから、約1カ月後のリード獲得・特集ページへの掲載となります

特集ページ イメージ

The image shows a digital magazine page titled 'Tech Factory'. The page layout includes a header with the magazine's name and navigation icons. The main content area is divided into several sections, each highlighted by a blue callout box with a white arrow pointing to it. The sections are: '特集テーマ' (Special Theme), 'タイアップ記事' (Tie-up Article), 'ご協賛社様 支給コンテンツ' (Sponsored Company Content), and 'テーマに関連する編集記事' (Edited articles related to the theme). To the right of the magazine page, there are three additional callout boxes: '貴社ロゴ掲載' (Your company logo is published), 'ご協賛社様コンテンツ掲載' (Sponsored company content is published), and '関連記事掲載' (Related articles are published). The 'ご協賛社様コンテンツ掲載' box contains text: '制作したタイアップ記事や貴社製品・ソリューションに関するホワイトペーパーやウェビナーを掲載' (We will publish white papers and webinars related to the tie-up articles you produced and your products/solutions). The '関連記事掲載' box contains text: 'テーマに関する最新事例などを紹介した編集記事を掲載' (We will publish edited articles introducing the latest cases related to the theme).

特集テーマ

タイアップ記事

ご協賛社様 支給コンテンツ

テーマに関連する編集記事

貴社ロゴ掲載

ご協賛社様コンテンツ掲載

制作したタイアップ記事や貴社製品・ソリューションに関するホワイトペーパーやウェビナーを掲載

関連記事掲載

テーマに関する最新事例などを紹介した編集記事を掲載

スポンサープラン

	ゴールドプラン ¥1,500,000 (40万円OFF)	シルバープラン ¥1,500,000 (40万円OFF)	ブロンズプラン ¥700,000 (20万円OFF)
ご提供リード数 ・セグメント条件の設定はありません	180件保証	110件保証	80件保証
コンテンツ数	2本	1本	2本
タイアップ記事制作		1本	
ホワイトペーパーご支給 ※お手持ちのコンテンツをご用意ください	2本		2本

- ※ 料金は税別、グロスです。
- ※ ホワイトペーパーをお持ちでない場合、別途費用が発生しますが制作プランがありますので、担当営業までご相談ください。
- ※ プランのカスタマイズも可能です。担当営業までご相談ください。
- ※ 特集ページの掲載順はお申込みいただいた順となります
- ※ 獲得期間は2カ月間を想定しています



アイティメディア株式会社 営業本部
<https://promotion.itmedia.co.jp/contact>

会員プロフィールや特集予定、お問い合わせはこちら
<https://promotion.itmedia.co.jp/>