情報セキュリティ対策ソリューションのご紹介

特定非営利活動法人

長野県ITコーディネータ協議会

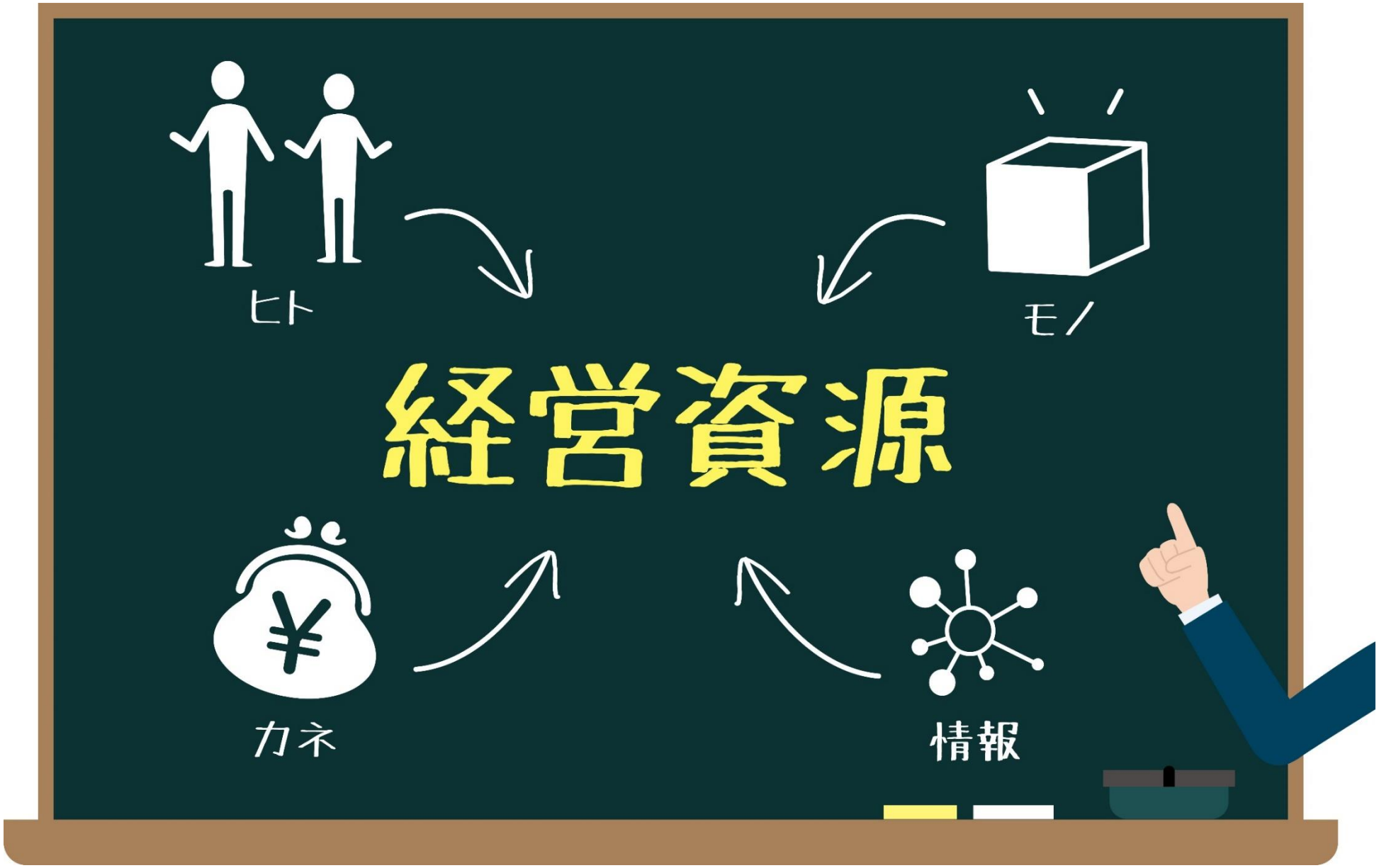
■最新の情報セキュリティリスク（抜粋）

■対策へ向けた簡単チェックポイント

■長野県ITコーディネータ協議会のご支援内容

様々な脅威から大切な情報資産を守る準備は整っていますか？

情報は重要な経営資源



情報セキュリティ10大脅威　2022

順位	組織における脅威	昨年順位
１位	ランサムウェアによる被害	１位
２位	標的型攻撃による機密情報の搾取	２位
３位	サプライチェーンの弱点を悪用した攻撃	４位
４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	３位
５位	内部不正による情報漏えい	６位
６位	脆弱性対策情報の公開に伴う悪用増加	１０位
７位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	ＮＥＷ
８位	ビジネスメール詐欺による金銭被害	５位
９位	予期せぬＩＴ基盤の障害に伴う業務停止	７位
１０位	不注意による情報漏えい等の被害	９位

出典：独立行政法人情報処理推進機構（IPA）

■ ランサムウェア

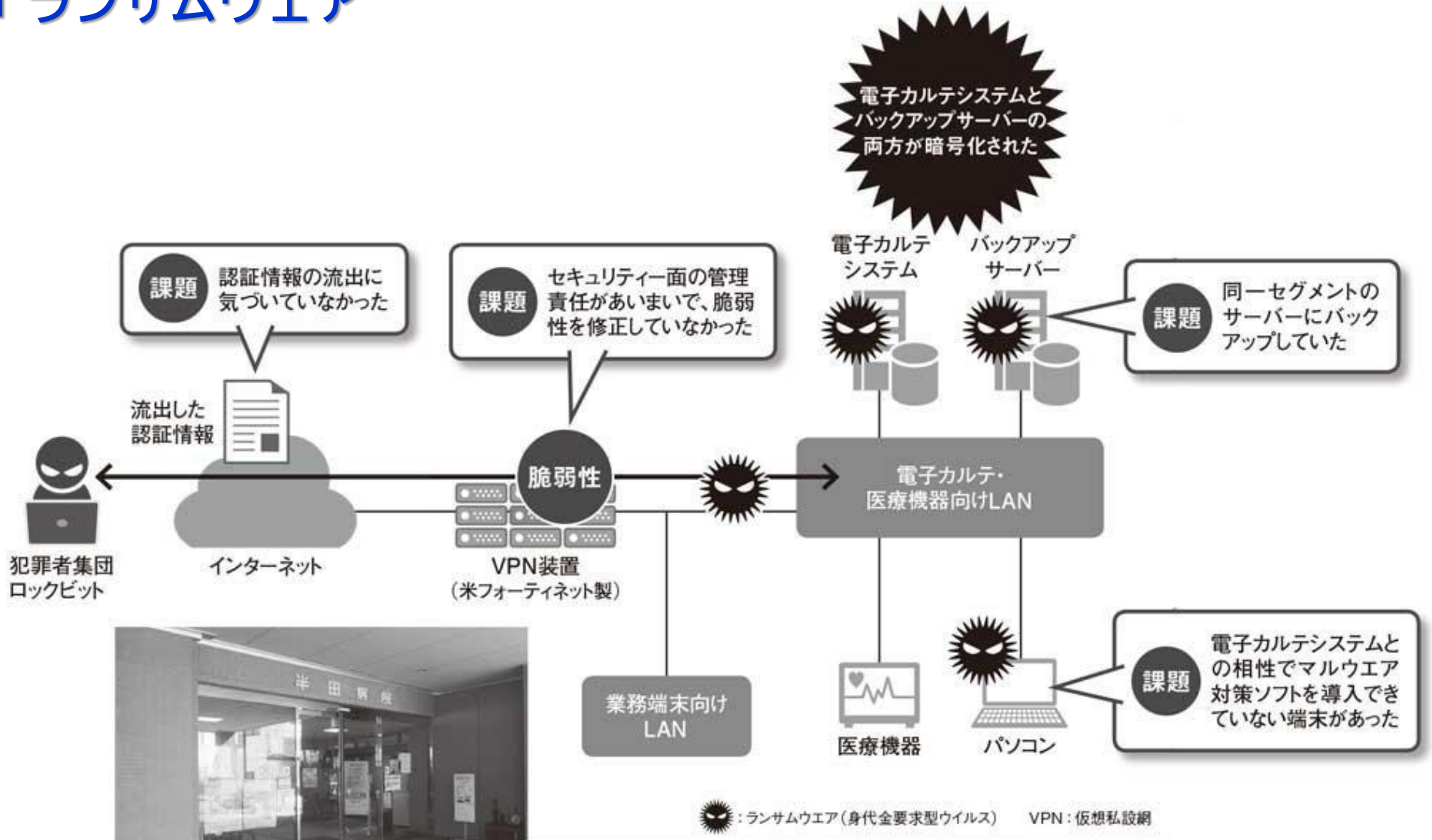
被害事例①　2021年10月

・徳島県つるぎ町立半田病院がサイバー攻撃を受け、
電子カルテをはじめとする院内システムがランサムウェアに感染し、
カルテなどが閲覧できない事案が発生

・ベンダがネットワークの保守のためにリモート接続していたVPN装置の
脆弱性が２年以上にわたって放置されていて、標的となった

・通常診療の再開まで約２カ月、約２億円の費用を要した

■ ランサムウェア



出所　日経コンピュータ

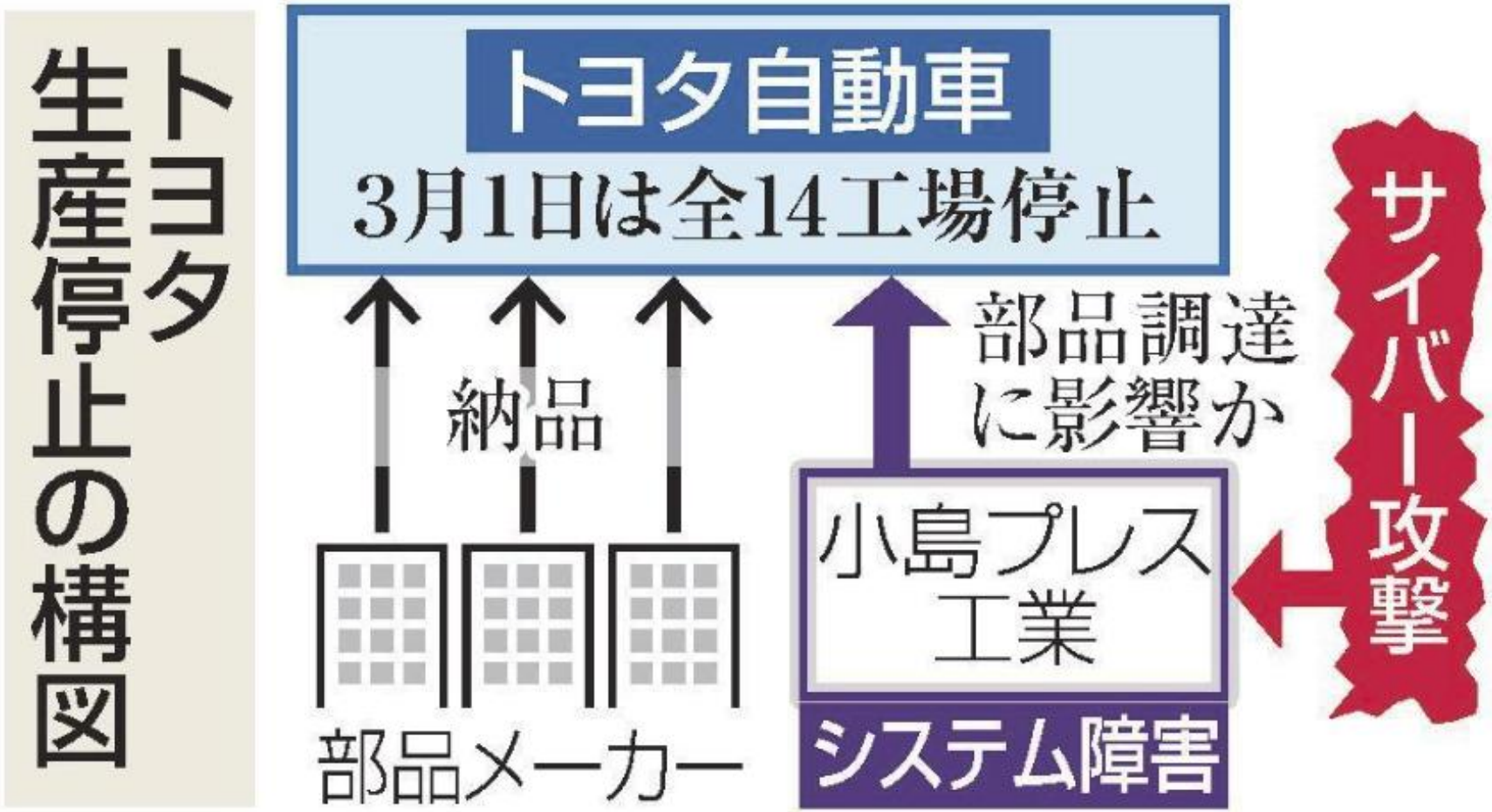
■ サプライチェーンの弱点

被害事例②　2022年2月

・トヨタ自動車のサプライチェーン（供給網）に連なる小島プレス工業がマルウエア被害を受けた。これがきっかけでトヨタの14工場の28ラインが止まった

・同社子会社で、外部事業者との通信にリモート接続機器（VPN装置）を使用しているが、今回の攻撃では同機器に存在した脆弱性が標的となった

■ サプライチェーンの弱点

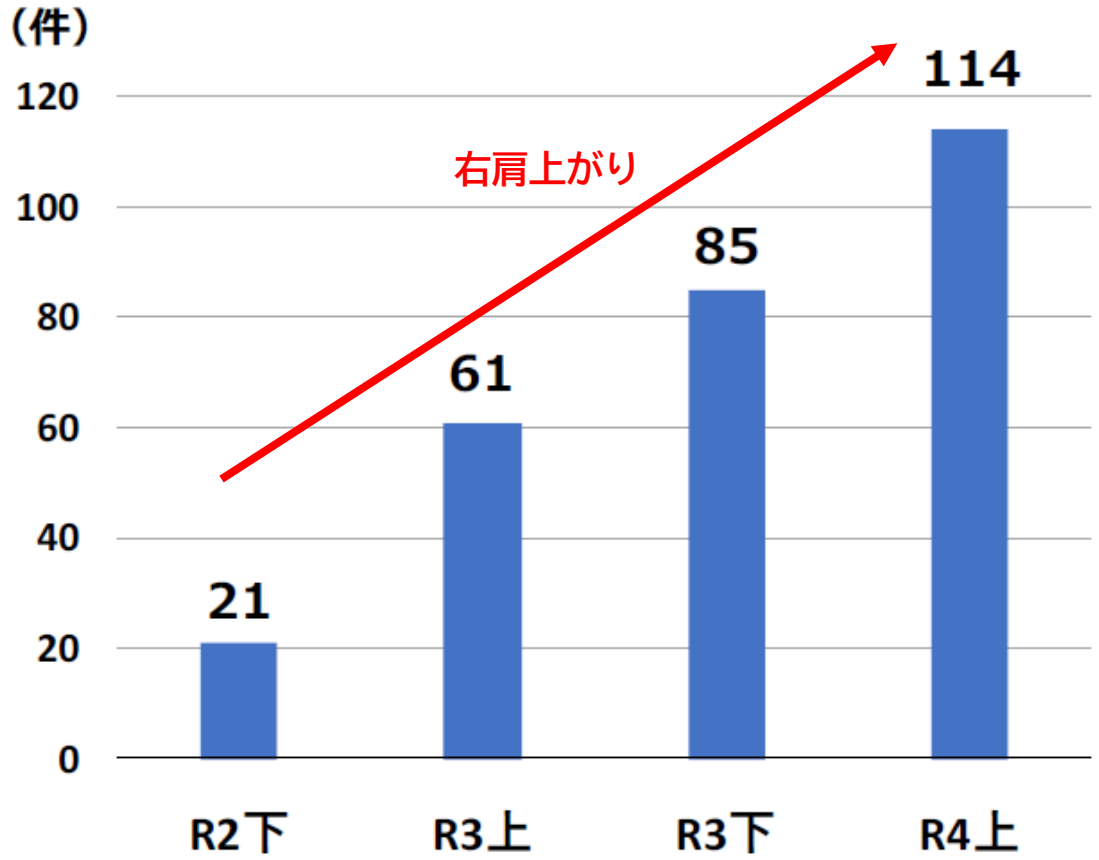


出所　山陰中央新報

■ ランサムウェア

ランサムウェア被害の報告件数

【図表１：企業・団体等におけるランサムウェア被害の報告件数の推移】

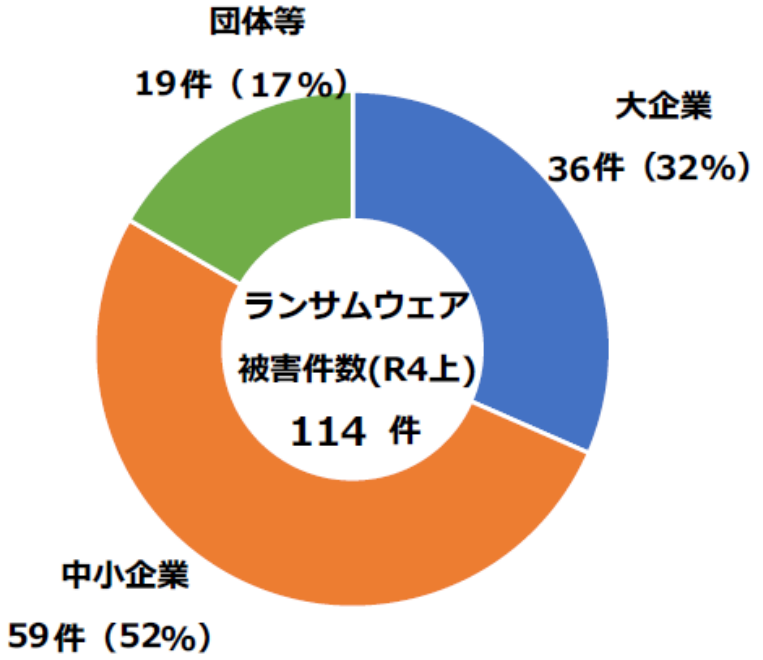


出典：令和4年9月15日警察庁広報資料

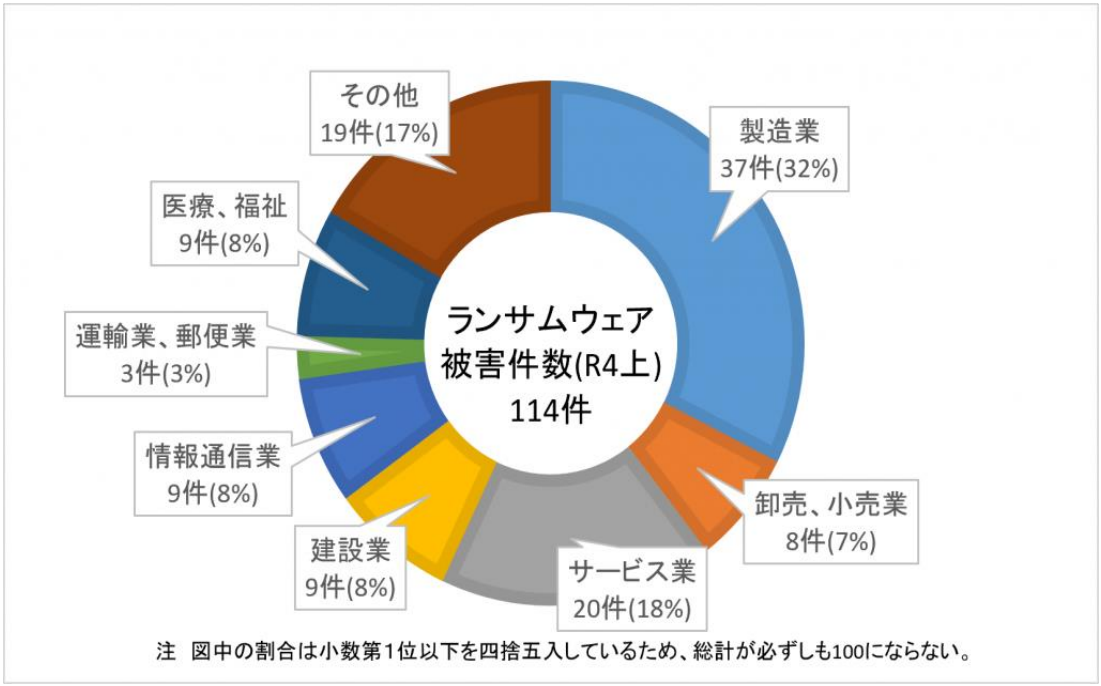
■ ターゲットの半数以上は中小企業

ランサムウェア被害企業統計

【図表４：ランサムウェア被害の企業・団体等の規模別報告件数】



注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

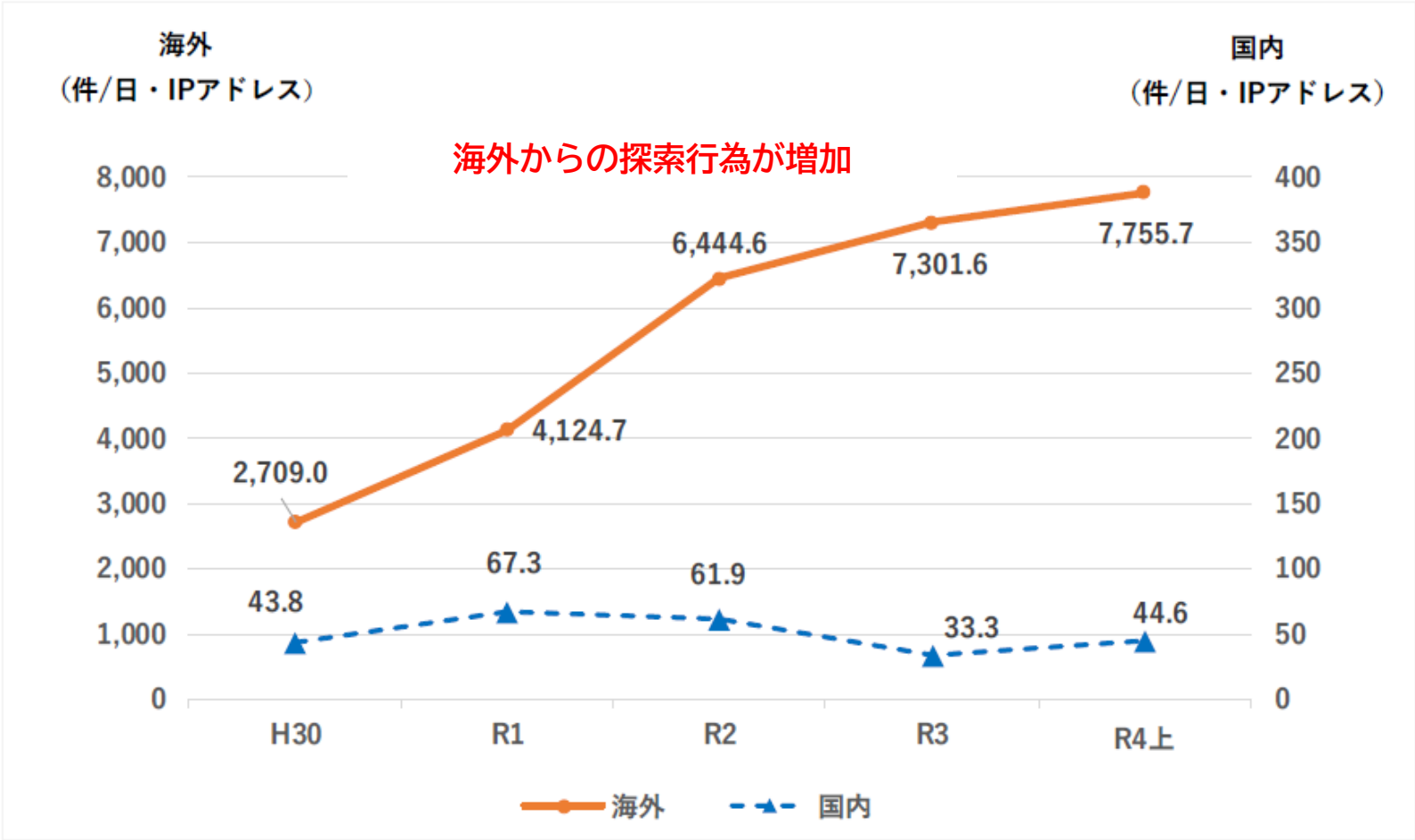


出典：令和4年9月15日警察庁広報資料

■ ランサムウェア

探索行為

【図表17：検知したアクセスの送信元で比較した１日・１ＩＰアドレス当たり件数の推移】

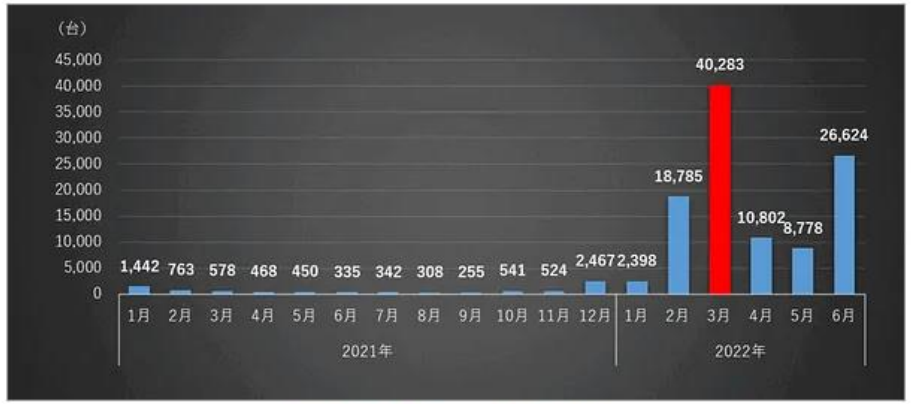


出典：令和4年9月15日警察庁広報資料

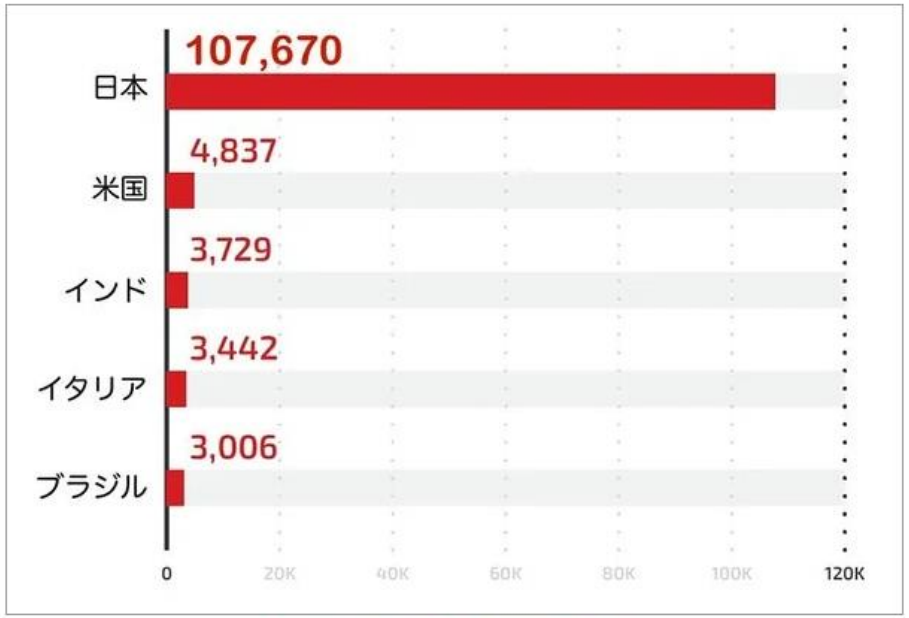
■ 危険なウィルスＥｍｏｔｅｔ

エモテット検出件数

・2022年3月に入り、2020年の感染ピーク時の約5倍以上に急増
（活動が沈静化したはずが、2021年以降に活動再開）



国内におけるEmotet検出台数推移



Emotet国別検出台数（2022年1～6月）

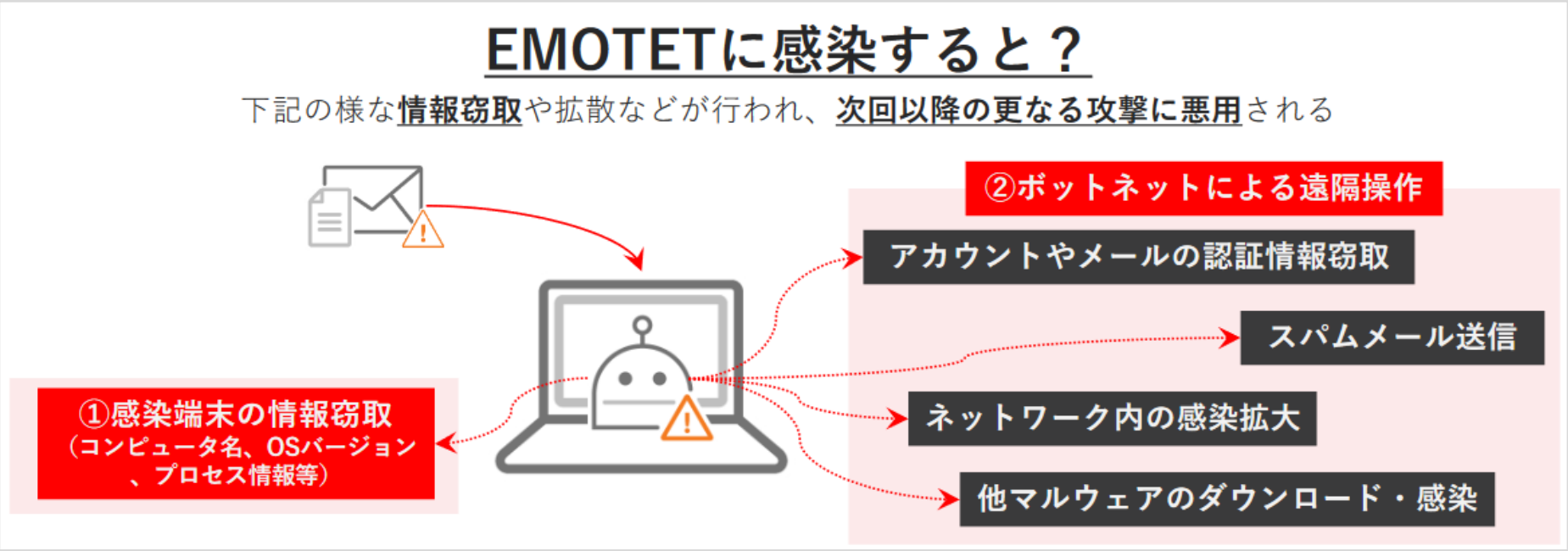
出典：トレンドマイクロ

■ 危険なウィルスＥｍｏｔｅｔ

「EMOTET」とは？

・マクロ付きのWordやExcelファイルをメールに添付して、大量に送付する「ばらまき攻撃」を仕掛けてくる。エモテットのメールだと知らずにファイルを開くと感染し、メールアカウントやパスワード、アドレス帳等の情報が抜き取られる

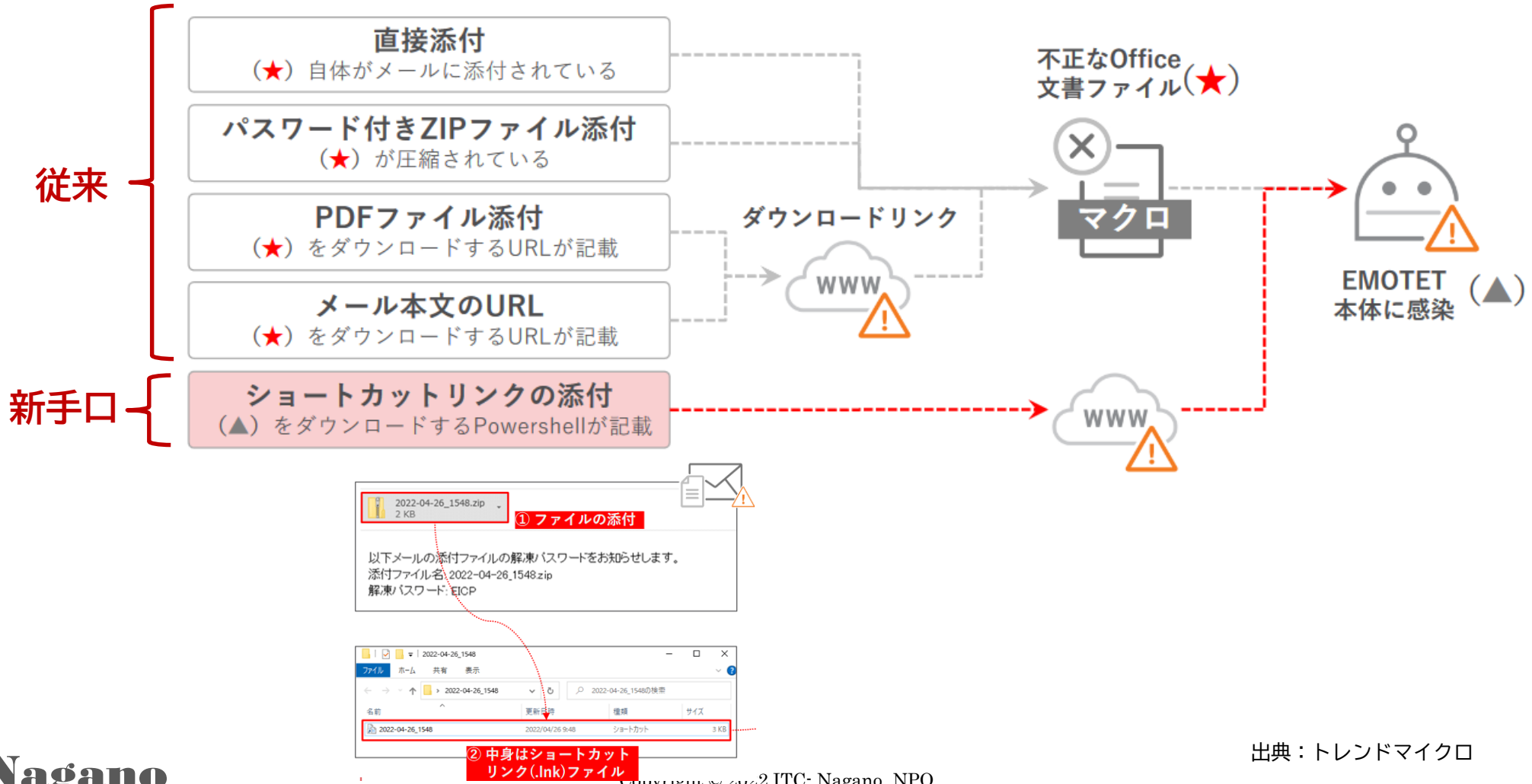
・普段やり取りする取引先や所属組織の別部門、同僚など、実在する名前やメールアドレス、メール内容を利用してメールを送信してくる



出典：トレンドマイクロ

■ 危険なウィルスＥｍｏｔｅｔ

EMOTETの拡散手法



出典：トレンドマイクロ

■ 危険なウィルスＥｍｏｔｅｔ

Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて

最終更新日：2022年11月4日
独立行政法人情報処理推進機構
セキュリティセンター

（2019年12月2日）
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。今後も同様の手口による攻撃メールが出回り続ける可能性があるため、事例と手口を解説するとともに、対策や関連情報を紹介します。

（2022年11月4日）
2022年7月13日頃より、Emotetの攻撃メールの配信が観測されない状態が続いていましたが、2022年11月2日から再開されたことを観測しました。攻撃の手口はこれまでと大きくは変わっていませんが、攻撃メールに添付されたExcelファイル内に書かれている偽の指示が、特定のフォルダにExcelファイルをコピーして開かせるように促す内容に変化しています。
詳しくは「Excelファイル内に書かれている偽の指示の変更について」をご参照ください。

危険なマルウェア　国際合同調査のニュース

17

■ 対策に向けた簡単チェックポイント

以下、一つでもできていない事があれば要注意、被害にあう確率が高くなります。

- 全社員が最新の攻撃手口を知っている。
- 自社が保有する情報資産が、どこに、どのような形で存在するか把握している。
- 自社の情報セキュリティ対策ルールを作成して全社員に周知し、遵守してる。
- 情報セキュリティ対策推進責任者／担当者を設定している。（兼務でOK)
- サーバー、パソコンのソフトウエアを常に最新にしている。
- ウィルス対策ソフト／パターンの最新化を行っている。
- パスワード設定における会社のルールがあり、全社員が遵守している。
- 会社のネットワーク、サーバーの構築を外部業者にお任せしていて、
  自社ではでどうなっているか把握できていない
- 情報セキュリティ対策ルールどおり運用できていることを定期的に点検している。
- セキュリティ事故が起きた時の対応方法の取り決めがある。

■ 長野県ITコーディネータ協議会のご支援メニュー

各社の実態に合わせた伴走支援を実施しています。

簡易診断	自社のセキュリティ対策レベル（概要）を把握し 弱点が理解できます。	初回無料
情報セキュリティ 教育	最新の手口と注意ポイントを専門家より解説を行う講習会を 実施します。	5万円 /回
情報資産 リスク分析	自社が保有している情報資産の棚卸とリスク値を分析し、 守るべき情報資産の状況と対策方針が明確となります。	個別見積
情報セキュリティ ポリシーの策定	自社に合った情報セキュリティポリシーの整備が行えます。 （情報資産リスク分析を行っていることが前提です）	個別見積
情報セキュリティ 内部監査員育成	社内でPDCAを回し改善を行うために内部監査員の育成を 行います。	個別見積

上記以外のご相談も受け付けております。

ITC-Nagano

お気軽にお問合せしてください

TEL：050-3488-2160

メール：info@itc-nagano.jp

特定非営利活動法人長野県ITコーディネータ協議会