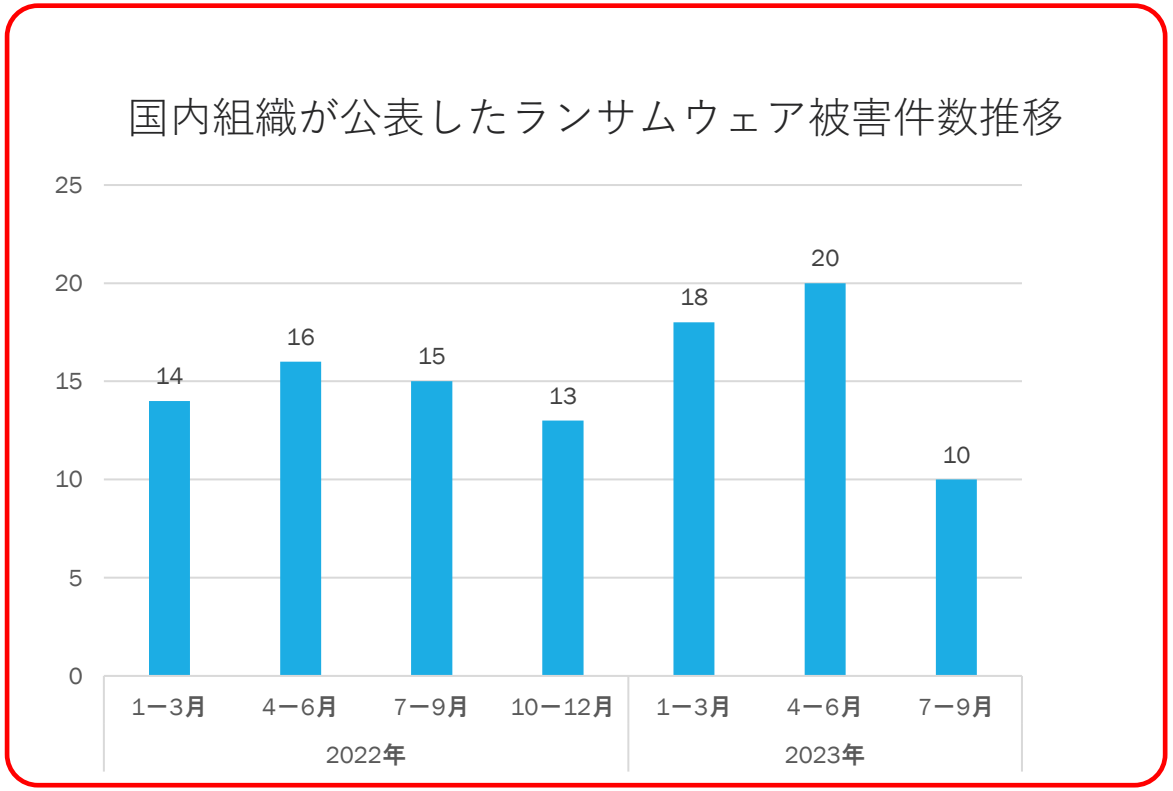
セキュリティのトランスフォーメーション

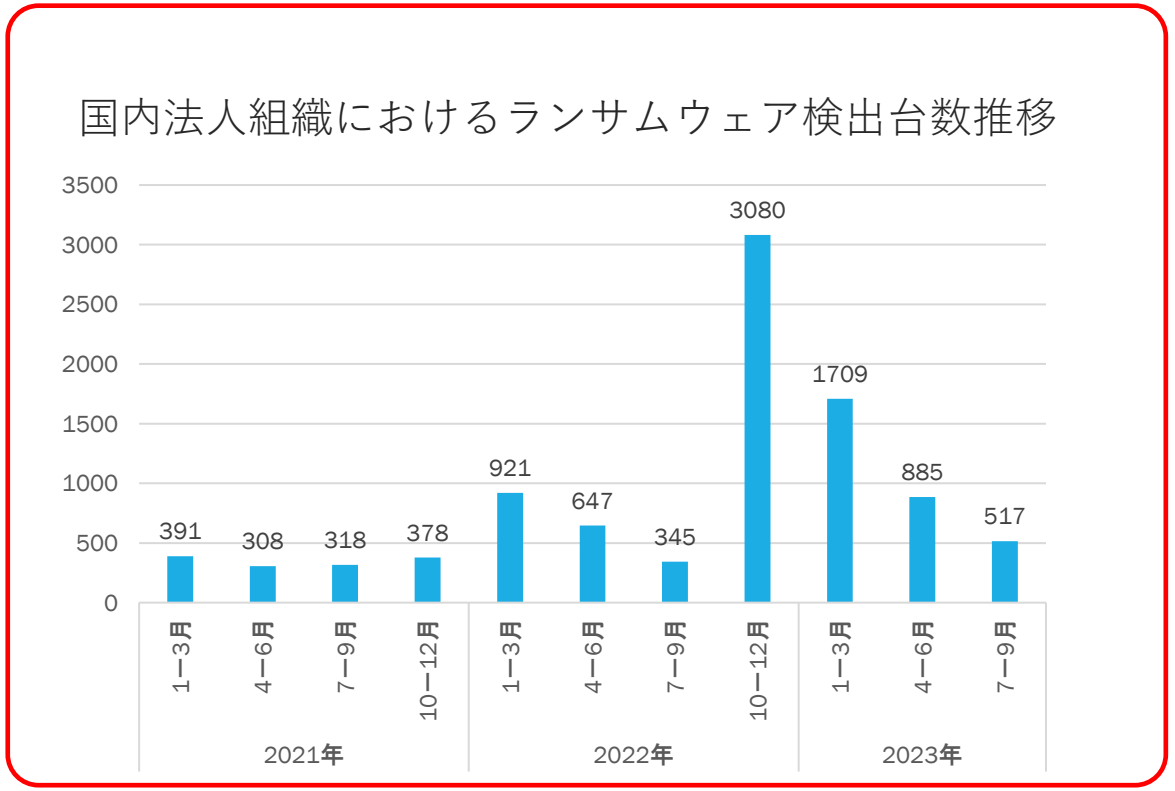
株式会社クロスポイントソリューション

マネージドセキュリティサービス事業部　斎数真人

セキュリティの脅威について

- トレンドマイクロ社の調査データによると**ランサムウェアの被害については減少傾向**にあるとされています。ただ、ランサムウェアの**検出台数は2021年に比べ高い水準**となっており、予断を許しません。

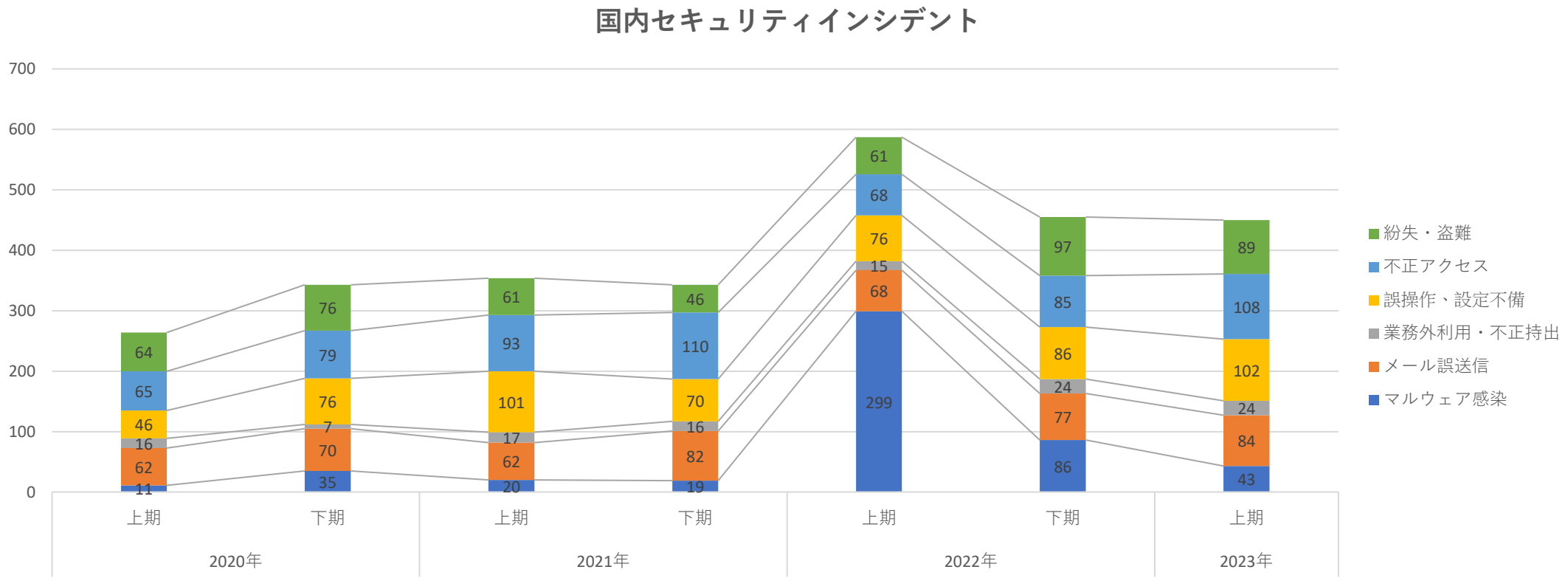




出展：トレンドマイクロ　Security GO　https://www.trendmicro.com/ja_jp/jp-security.html

セキュリティの脅威について

- 2023年も様々な業種・業界でセキュリティ事故が発生してしまいました。
  2023年はEmotetの活動が下火になり、ランサムウェアの感染は減少傾向にあります。
  しかし、それ以外の事故については高止まりの状況が続いています。



出展：デジタルアーツセキュリティレポート　https://www.daj.jp/security_reports/32/

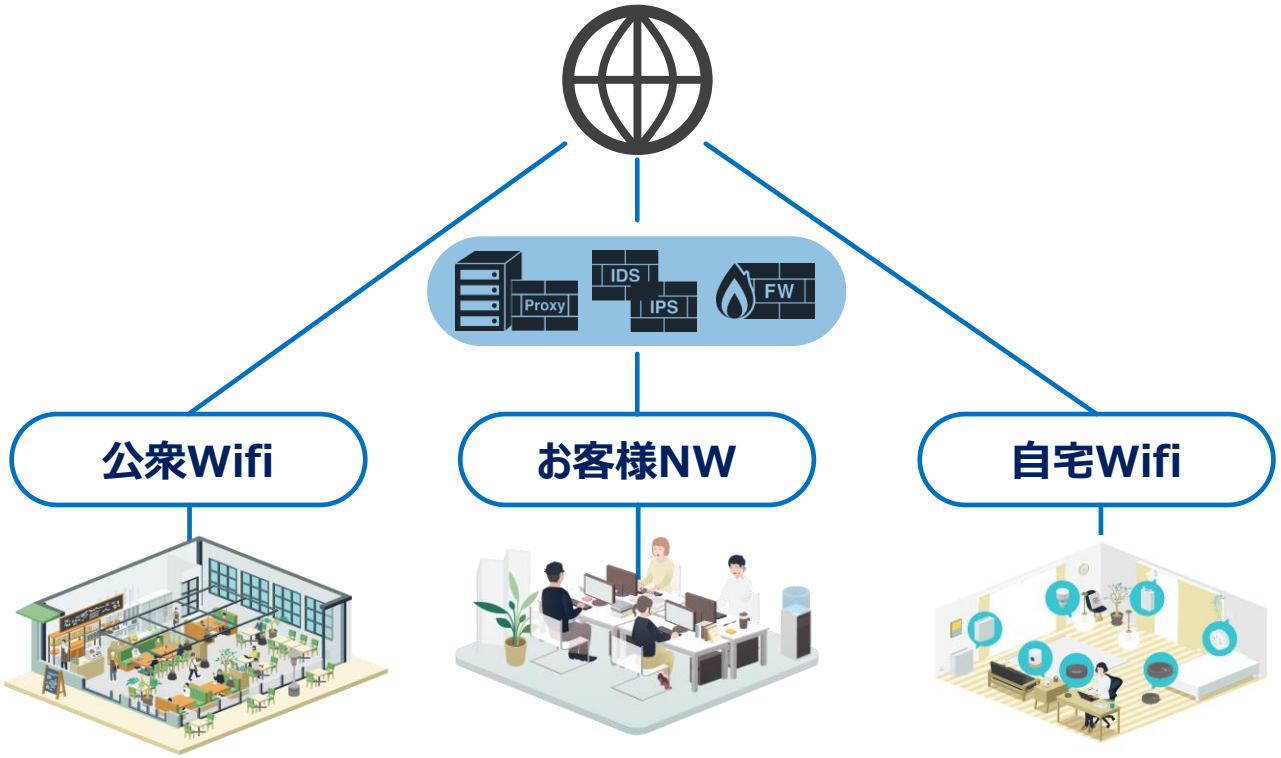
インシデントの事例について

- セキュリティインシデントの事例を見てみましょう。DXが推進されデータ化が進む中、セキュリティ事故は重大な事故に直結してしまいます。
- 本日はこうしたセキュリティ脅威への対応についてご紹介したいと思います。

業種	概要	被害
製造業	車載情報サービスの利用者情報が漏洩	215万人分の情報漏洩
ECサイト	ECサイトが不正アクセスの被害に遭いに個人情報が漏洩	275万件の個人情報漏洩
医療	委託先の企業を経由し病院システムに侵入、電子カルテデータが暗合化され利用不能になった	長期間の業務停止
公立高校	自宅で使っていた私用パソコンが遠隔操作され、保存した生徒の個人情報が流出	学生の個人情報23件が流出
地方自治体	USBメモリーを持ち出したまま泥酔し、かばんごと紛失	46万人の個人情報紛失
医療	フィッシングにより個人で利用していたクラウドサービスのID情報を流出。クラウド上には業務情報が保存されていた。	ログイン情報、業務データの流出

テレワーク環境における更なる課題について

- テレワークの導入により、従業員が様々な場所で働くことになると、ITサポートやインシデント対応が困難になる課題があります。
- 今は、何かあればシステム担当者が駆けつけてくれますが、テレワークになるとそうは行きません。さらに働き方が柔軟になり労働時間までバラバラになるとさらに対応は困難になります。



クラウド・バイ・デフォルト

IaaS　SaaS　PaaS

データセンター

Proxy　IDS　IPS　FW

脆弱な公衆無線LANを利用した盗聴

Wi-Fi6による高セキュリティ無線LANの導入

不正ログインによる情報漏洩リスク

多要素認証による認証強化

発進番号を活用した多要素認証（HY技研）

在宅時のセキュリティトラブル対応

セキュリティコラボレーションプログラム（クロスポイントソリューション）

データの不正持出しなど内部不正への対策

資産管理ツールによるPCの操作制御（クロスポイントソリューション）

公衆Wifi

お客様NW

自宅Wifi

PC持ち出しによる紛失･盗難リスク

- シンクライアントによる持出対策 → 3つの環境を活用した高セキュアシンクラ（アクロネット）
- 持出専用PCによる情報漏洩対策 → 端末の自動初期化によるキッティング簡素化（アルファシステムズ）

外出先でのセキュリティレベル低下

- 端末の常時監視によるセキュリティの管理・可視化 → 端末の管理による外部デバイスの利用制限、操作の可視化による不正対策
- Cloudサーバを活用した常時情報収取・分析 → CloudProxyによるインターネットコンテンツ利用状況監視

CP-SOLセキュリティ コラボレーションプログラム のご紹介

CP-SOLセキュリティコラボレーションプログラムのご紹介

お客様にちょうどいいセキュリティ対策をご提供します

基本サービス　セキュリティサポートデスク

■ サービス概要

セキュリティに関することであれば、何でも、何度でもお気軽にご相談下さい。 専門のスタッフが分かりやすく解決のお手伝いをします。
基本サービスに含まれている「セキュリティ診断」の結果に関するお問合せもセキュリティサービスデスクがお答えします。

■ サービスイメージ

コンピュータウィルスに感染？

見たことのないセキュリティのエラーが！

セキュリティ診断の結果が良く分からない

退職した従業員が機密情報を持ち出したかも？

パソコンの動作が急に遅くなった・・・

社員が業務中に仕事に関係ないサイトを閲覧しているようだ

広告が大量に表示されて消えない

セキュリティに関する「困った」、「不安」、「知りたい」があったときは、お気軽に電話・メールでご相談ください。

セキュリティサービスデスク

専用フリーダイヤル、
専用メールアドレス

基本サービス　セキュリティ診断（PC）

■ サービス概要

基本サービスに同梱されたClient (5端末分同梱しています) をインストールいただくと、Clientが端末の操作ログやOS/ソフトウェアの情報を収集します。 収集した情報をセキュリティの専門家が分析・診断し、セキュリティ診断(PC)レポートを毎月お送りします。セキュリティ診断(PC)レポートの内容でご質問やご不明の点があれば、セキュリティサービスデスクにお問合せください。

■ サービスイメージ

※ 本ClientはWindows PCのみ対応しております。

基本サービスに同梱したClientをインストール

Clientが分析に必要な情報を収集

セキュリティの専門家が収集した情報を分析し、診断レポートを作成

フィッシングサイトなどの危険なサイトにアクセスしたのか？ということも分かります

セキュリティ健康診断票 【セキュリティ診断(PC)レポート】

診断項目	結果	所見
【情報漏えいにつながる可能性】 外部記憶媒体 (USBメモリ、スマートフォンなど) の接続	A	管理対象端末「15」台の内、USBメモリ等の「リムーバルディスク(記憶媒体)」の接続、iPhone・iPad等の「ポータブルデバイス(記憶媒体)」の接続はありませんでした。
【Webを媒介したセキュリティ事故につながる可能性】 不法・詐欺サイト、業務外サイトなどの閲覧	C	管理対象端末「15」台の内、ウィルス感染のリスクを伴う悪意のあるWebサイトへの接続、または業務上関係ないと思われるWebサイトへの接続が、以下の通り検知されました。 セキュリティ：「23」件、不法：「19」件、アダルト・フェティズム：「36」件、過剰な表現(暴力組織・カルトなど)：「8」件 悪意のあるWebサイトへの接続を介したウィルスへの感染リスクや、業務上関係がないと思われるWebサイトへの接続には注意が必要です。Webアクセス制御(フィルタリング)の導入や、企業内での利用規定などのルール導入を推奨します。
【セキュリティホールを狙ったセキュリティ事故につながる可能性】 Windows OSアップデートの未適用	D	管理対象端末「15」台の内、Windowsの緊急パッチ「Critical」が適用されていない端末が「8」台あります。 また、Windowsの重要パッチ「Important」が適用されていない端末が「12」台あります。 該当端末に対してサイバー攻撃が行われた場合、該当端末を踏み台に、企業全体・関連取引先に対するリスクが波及する可能性が高くなるため、早急にパッチ適用されることを推奨します。
【セキュリティホールを狙ったセキュリティ事故につながる可能性】 ソフトウェアアップデート未適用	C	管理対象端末「15」台の内、重要性の高いバージョンアップ「High」が適用されていない端末が「7」台あります。 緊急性が高いバージョンアップ「Critical」はありませんでしたが、脆弱性レベルの推移(更に新しいバージョンアップ情報)には注視が必要です。該当端末に対して、可能な範囲でバージョンアップを適用されることを推奨します。
【不正アクセスの可能性、許可のない時間外労働の可能性】 業務時間外(土日祝・深夜帯)でのPC利用	B	管理対象端末「15」台の内、平日深夜帯(22:00～5:00)にログインした端末が「7」台あります。 また、土日祝日にログインした端末が「4」台あります。 業務時間外での端末利用や自宅に端末を持ち帰ってのリモート利用は、セキュリティ上のリスクを伴うため、端末やネットワークに関するセキュリティ対策とともに、働き方改革や労基上の観点からも管理されることを推奨します。

結果の見方
A：異常なし
B：経過観察
C：要精密検査
D：要治療

分析結果を「A:異常なし」、「B:経過観察」、「C:要精密検査」、「D:要治療」の四段階で評価

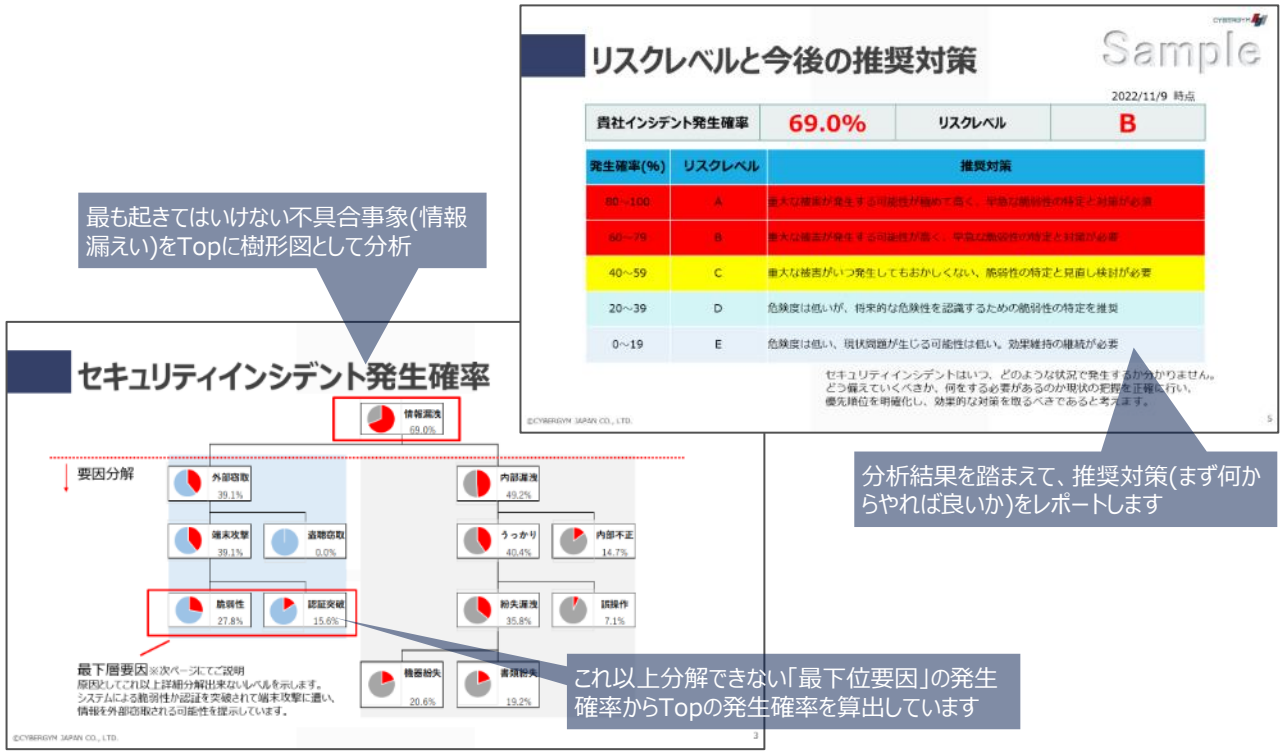
基本サービス　セキュリティ診断(企業)

- **サービス概要**

  一年に1回、企業の情報漏えいリスクを診断します。 数問のアンケートにお答えいただき、回答いただいた内容を集計・分析して、企業が情報漏えいを発生する可能性をパーセンテージで表し、「情報漏えい発生リスク」をA～Eの5段階で評価したセキュリティ診断(企業)レポートをお送りします。セキュリティ診断(企業)レポートの内容でご質問やご不明の点があれば、セキュリティサービスデスクにお問合せください。

- **サービスイメージ**

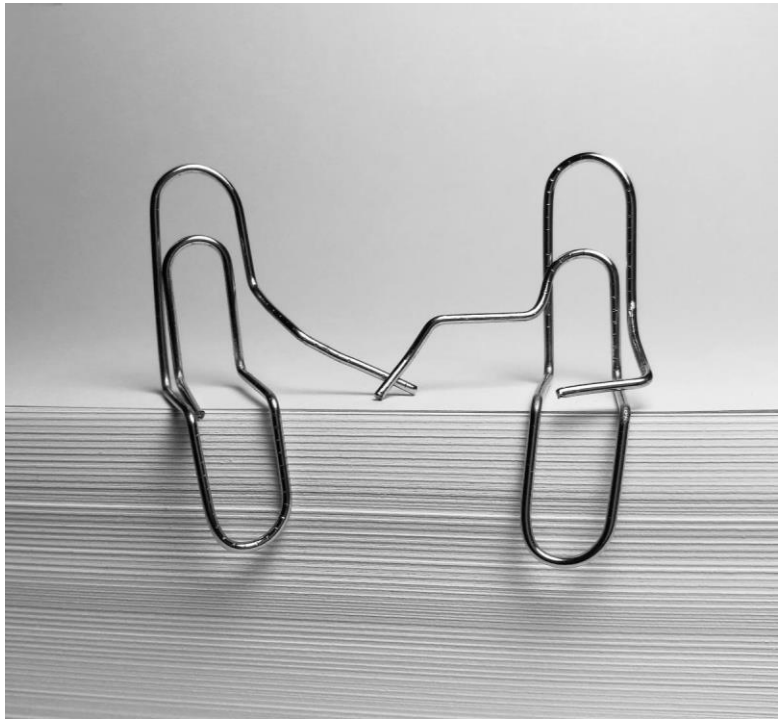
10問程度のアンケートにお答えいただきます



CP-SOLセキュリティコラボレーションプログラムのご紹介

お客様が必要な対策を選択して導入できます。

基本サービス	CP-SOLオプションサービス（内部不正対策）		TOPベンダオプションサービス（外部脅威対策）	
セキュリティサポートデスク	セキュリティ診断端末追加	不正Webサイトアクセス制御	マネージドEDR (Cybereason IR-Core)	Microsoft365全方位保護（WithSecure）
セキュリティ診断（PC）	OS、ソフトウェア脆弱性防御	PC操作ログ保管	マネージドEDR＋EPP (WithSecure)	メールセキュリティ (Vabe)
セキュリティ診断（企業）	データ持出し制御	標的型攻撃メール訓練＋E-Learning		



ご清聴ありがとうございました。

株式会社クロスポイントソリューション

(03) 6280-3163

mss.div@cp-sol.co.jp

https://cp-sol.co.jp/