



# 脆弱性診断って毎回やる意味あるの？

## 今年も脆弱性診断の時期がやってきた！

情報セキュリティ担当の若井くんは脆弱性診断サービスの選定を任され 出来杉先輩に相談することに...

出来杉先輩～  
脆弱性診断、今年もやらないとダメですか？



若井くん



出来杉先輩



去年診断してる  
みたいですし  
今年はやらなくて  
いいんじゃないですか？

そもそも脆弱性診断って毎年なんで受けるの？

他にもあるよ



脆弱性診断

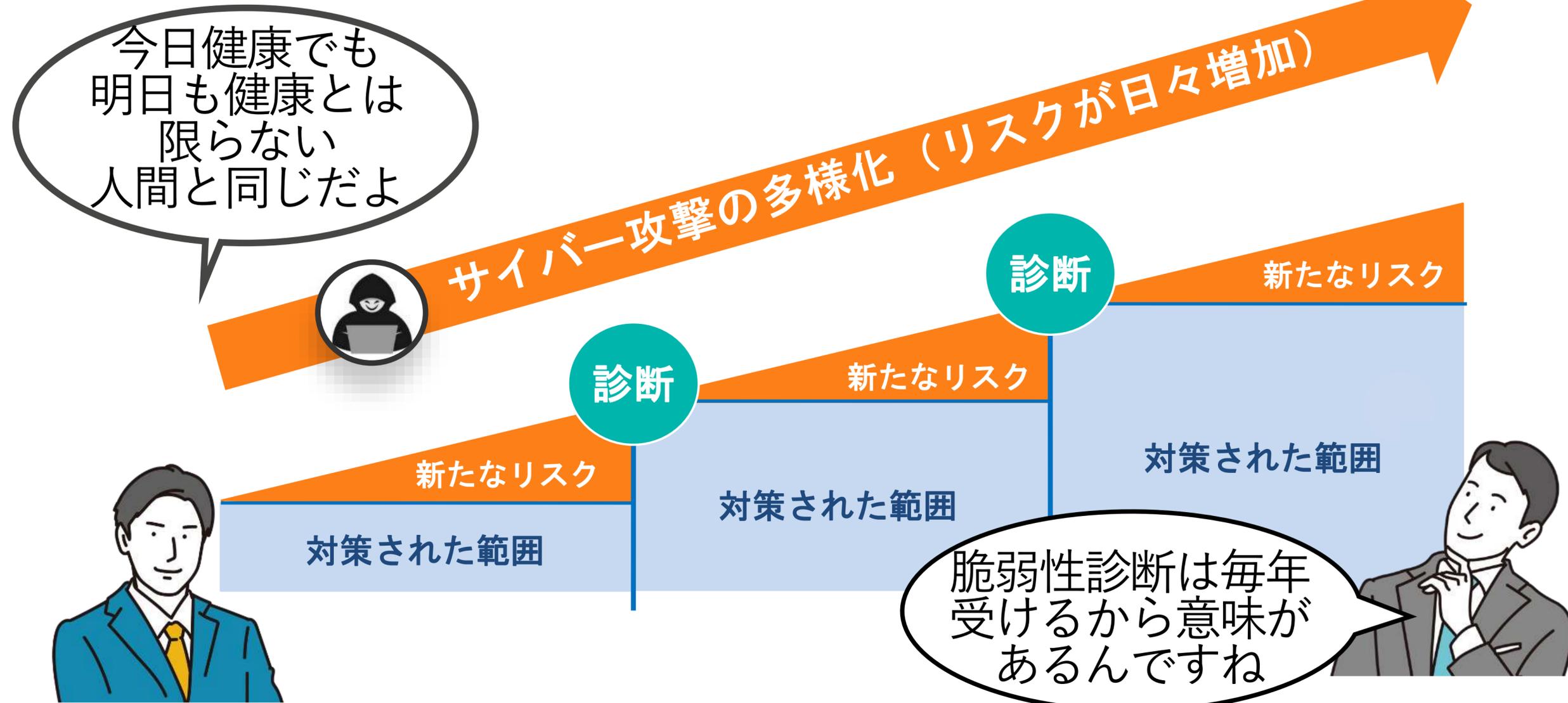
詳しくはコチラ



# 定期的に脆弱性診断を受けて対策しよう

一度受けたから一生安心とは限らない

脆弱性診断は 診断した時点での脆弱性を検出



その時点で対策しても、日々増加する新たなサイバー攻撃に対してはリスクが残る為、定期的に実施する必要がある

他にもあるよ



脆弱性診断

詳しくはコチラ



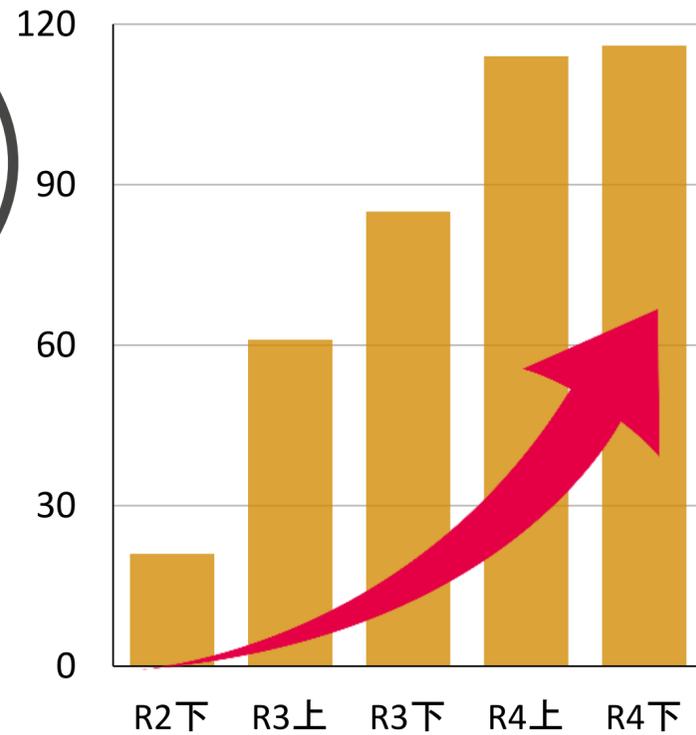
# サイバーセキュリティ対策が急務に

自社だけに留まらず国内外拠点や取引先まで被害が及ぶ場合も

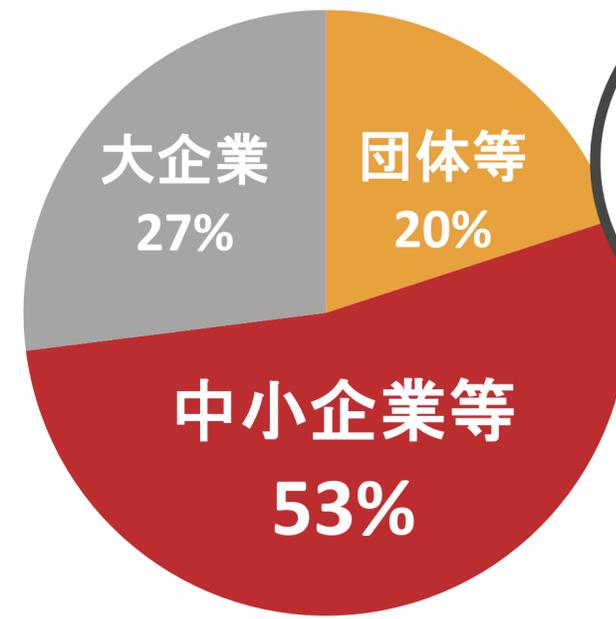
## 大企業から中小企業まで サプライチェーンの弱点を狙ったサイバー攻撃が顕在化・高度化している



企業・団体等におけるランサムウェア被害の報告件数



ランサムウェア被害企業等の規模別件数



出典：警察庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について（令和5年3月16日）」

### 一度の被害でも想定以上の損失に繋がるおそれがある

他にもあるよ



脆弱性診断

詳しくはコチラ



# システムの健康診断「脆弱性診断」

## 脆弱性診断は何を基準に選ぶ？



ツール診断だけでなく複数人によるクロスチェックをしてくれる丁寧な脆弱性診断サービスが望ましい

結果だけでなく  
対策も教えてくれる  
から助かるね



詳しくない僕にも  
分かりやすいです



2. 検出脆弱性詳細

2.1. 危険度 Highレベルの脆弱性

WID001

クロスサイトスクリプティングの脆弱性

【補足】

① その結果、表示された画面内にパラメータが出力されます。この時、パラメータにスクレイプされずに出力されます。そのため、以下のようにiframeタグとして実行されて

【補足】

① パリテーションチェックを実施  
クライアントが送信したパラメータの値をプログラム側にて厳密にチェックし、文字種等は適切にエラー処理を行ってください。(例: 電話番号欄の場合は、半角数字11桁)

また、以下の例のように、パラメータ名を空にして、値のみを追加したパターンでも診断されます。(例: http://xxxxxxxxxxxxx/value1&value2?<script>...)

さらに、送信されるパラメータを削除した場合(=パラメータを送信しない場合)や、存在すると、PHPの実行時エラーが発生します。必ず、「パラメータ名」と「パラメータ値」の両方が送信された場合は、即エラー処理してください。

以上の点から、「送信されたパラメータ名が、存在する正規のものであるかチェック対象のフォーマットであるかチェックすること」、「パラメータを画面内に出力する場合は」

1. 診断結果概要

総合評価

本Webアプリケーションの評価は下記の通りとなります。  
以下の通り脆弱性が検出されました。

Web アプリに関する脆弱性

詳細参照	危険度	脆弱性名称
WID001	High	クロスサイトスクリプティングの脆弱性
WID112	Medium	非公開ファイルの露呈
WID202	Low	ディレクトリリスティングが可能
WID203	Low	システム情報・テストページが露呈
WID208	Low	システム・アプリケーションエラーが表示
WID221	Low	URL インジェクションが可能
WID324	Info	HTML ソース内のコメント文について

【補足】

- 評価、危険度の基準については、巻末の**評価基準**を参照してください。

診断対象

サイト名	URL	診断日程	診断対象リソース数
PC 向け	-	xxxx/xx/xx~xxxx/xx/xx	-
SP 向け	http://xxxxxxxxxxxx.com/	-	xx
FP 向け	-	-	-

他にもあるよ



脆弱性の詳細をわかりやすく解説した報告書があると  
今後の対策にも役立つ

脆弱性診断

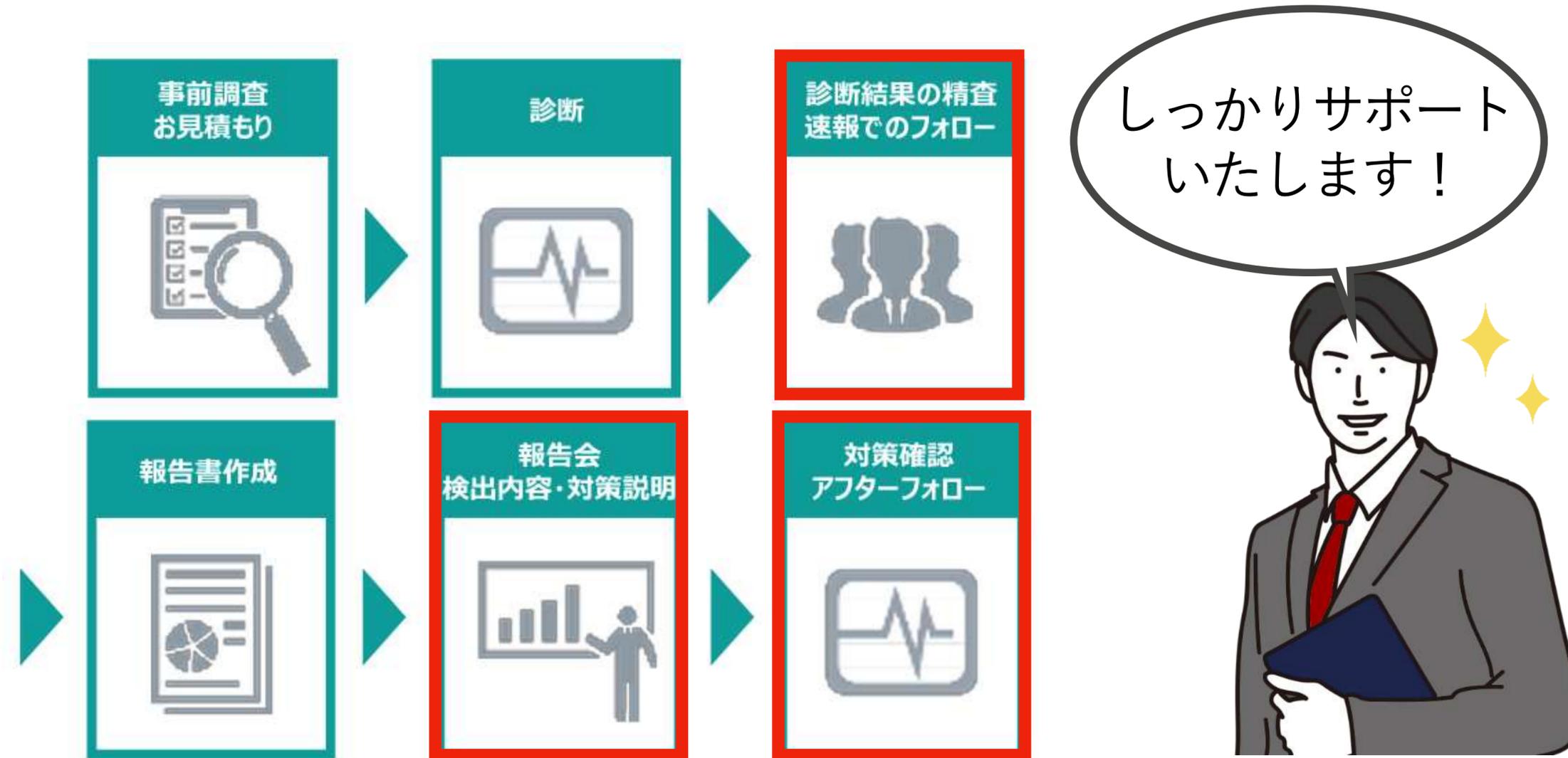
詳しくはコチラ



# システムの健康診断「脆弱性診断」

## 脆弱性診断は何を基準に選ぶ？

### アフターフォローの手厚さも重要な選択基準



日々高度化する脅威に対しての要改善箇所のアドバイス  
や改善後の再診断があるかどうかも大切なポイント

他にもあるよ



脆弱性診断

詳しくはコチラ



# 「サイバー保険付き脆弱性診断」で安心を買おう

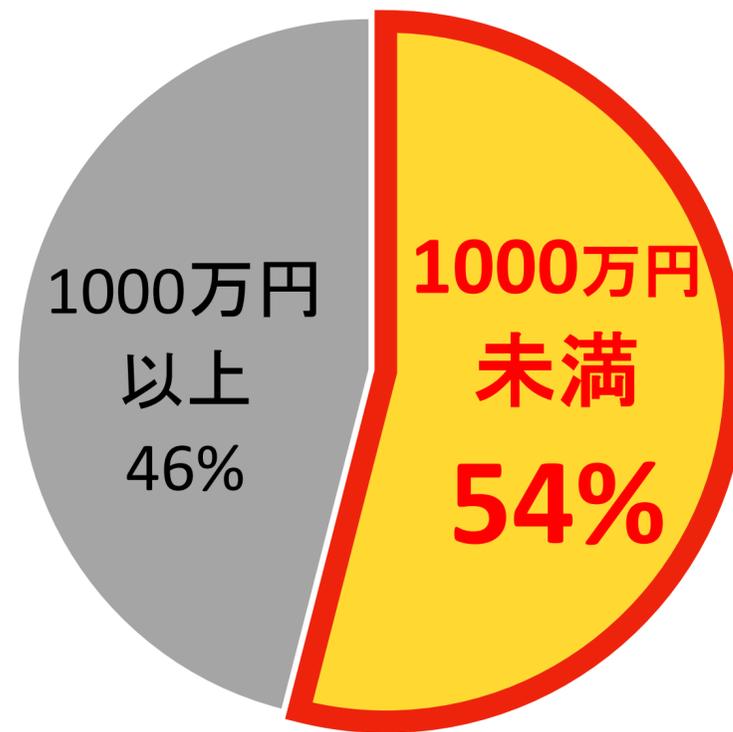
1,000万円まで補償可能なサイバー保険で迫り来る脅威に備える



## ランサムウェア被害に遭った約半分以上の企業が 調査・復旧に1,000万円ほどの費用を要している

調査・復旧費用の総額

脆弱性診断契約日から  
1年間補償が無料で  
自動付帯されるんだ※



医療保険付きの  
健康診断ってこと  
ですね！



出典：警察庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について（令和5年3月16日）」

脆弱性診断

詳しくはコチラ

## 診断だけでなく万が一の時の補償もまとめて備えられる

※サイバー保険は全てのメニューを対象に、ご契約頂いた総額が80万円以上（税抜）の場合に無償で自動的に付帯されます。7

他にもあるよ





# 脆弱性診断 ス



750

システムの  
検査実績\*

# いまこの瞬間に最適なアドバイスを 定期的なチェックで継続的なセキュリティ対策が大切

今回はNTTコムウェアのサイバー保険付き脆弱性診断を  
選択した若井くん



継続して診断を受けて常に対策することが  
企業と全てのステークホルダーを守ることに繋がる

他にもあるよ



脆弱性診断

詳しくはコチラ

