# サイバーセキュリティお助け隊 in 東北の活動から見えてきたこと

2021年1月29日

株式会社デジタルハーツ

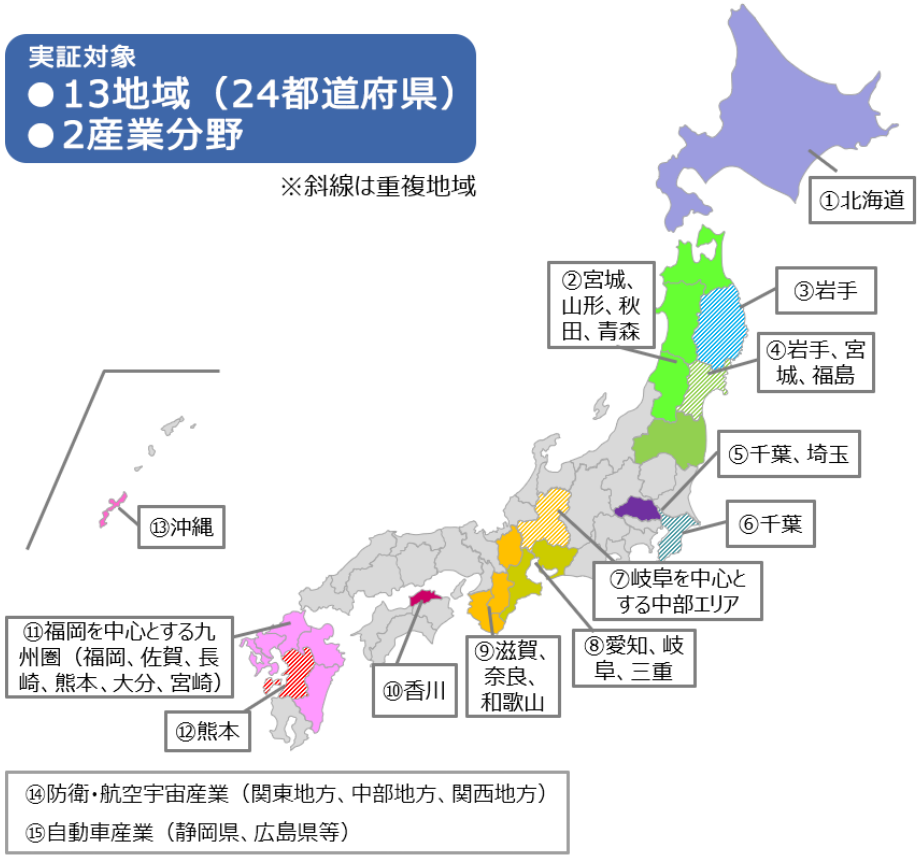
※株式会社デジタルハーツは、独立行政法人情報処理推進機構（IPA）の「中小企業向けサイバーセキュリティ事後対応支援実証事業」における請負事業者（宮城県・岩手県・福島県）です。
協力会社：東日本電信電話㈱宮城事業部、損害保険ジャパン㈱　等

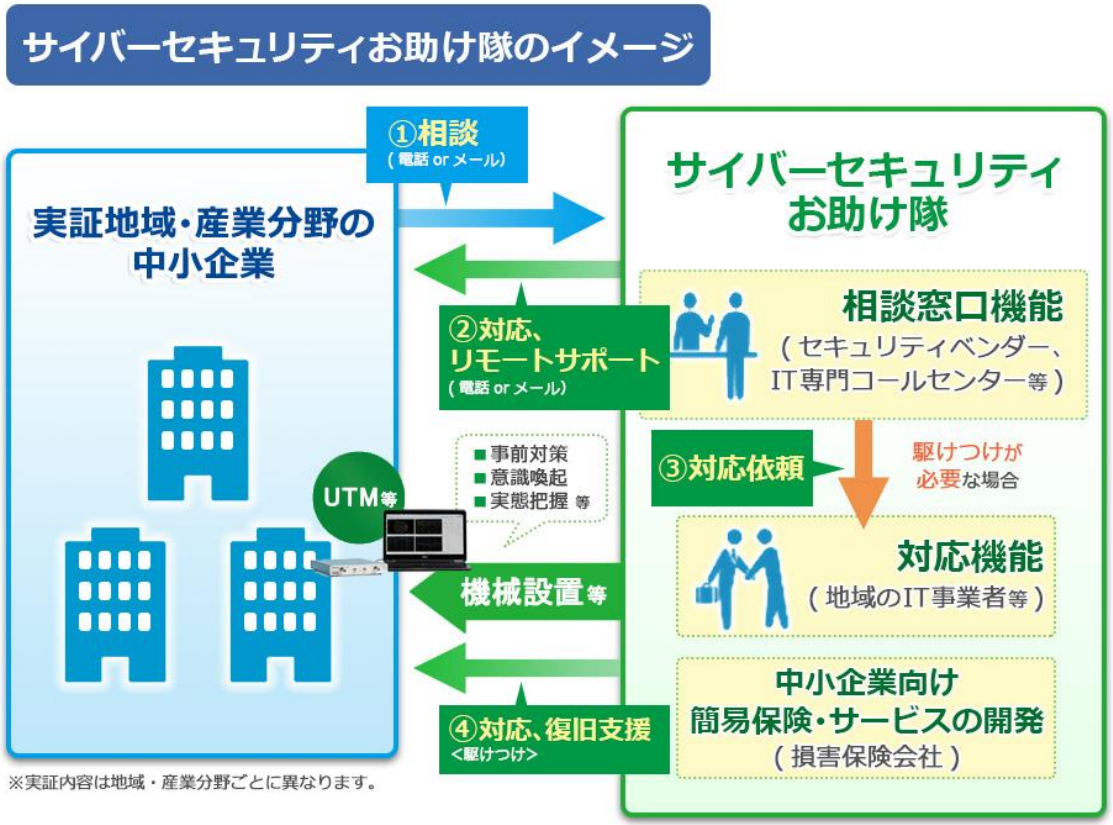
# 目次

# サイバーセキュリティお助け隊（令和２年度）

DIGITAL HEARTS

- 今年度は24道府県13地域と2産業分野の中小企業を対象として、中小企業サイバーセキュリティ対策支援体制の構築に向けた実証事業を実施。



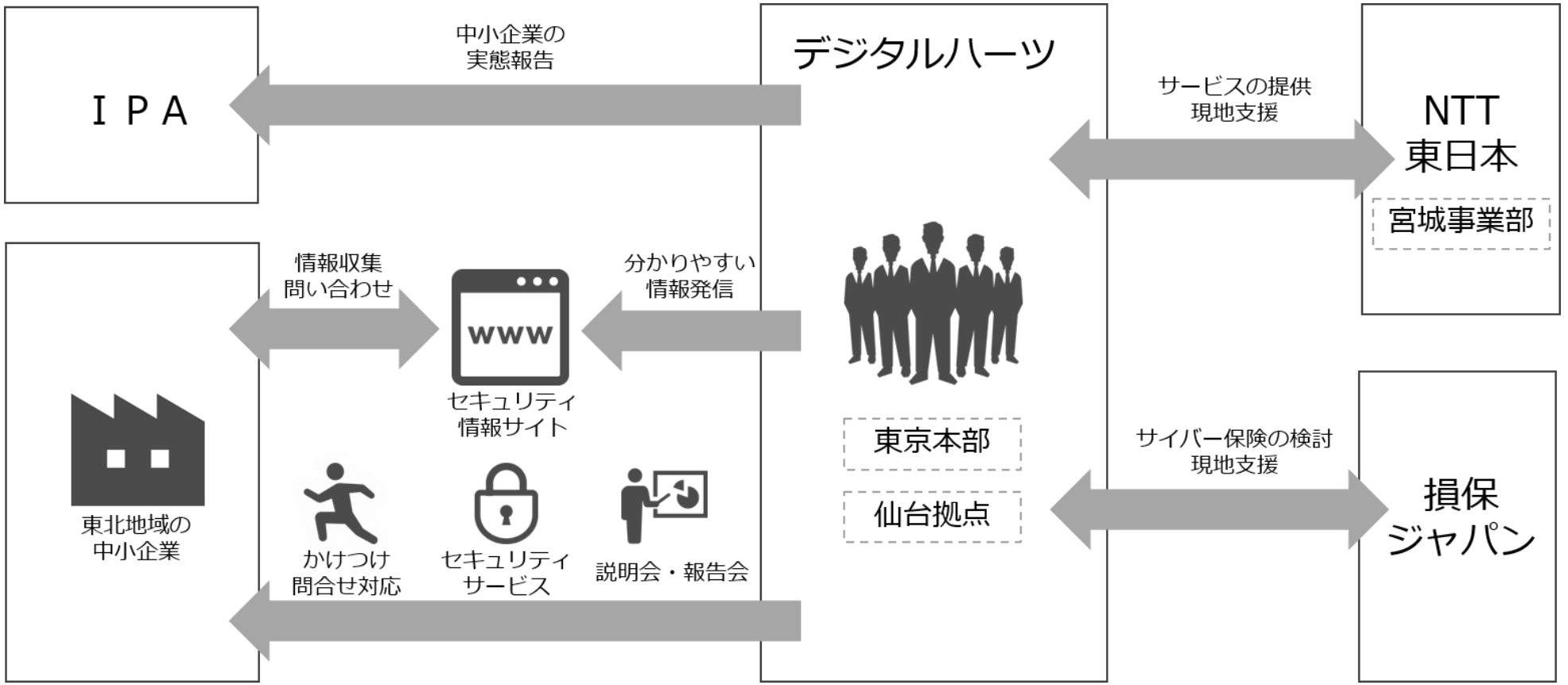

| ④岩手、宮城、福島 | 株式会社デジタルハーツ |
|---|---|

（IPAウェブサイト）

# 令和２年度　サイバーセキュリティお助け隊 in 東北の概要

DIGITAL HEARTS

- 昨年度に引き続き、宮城県、岩手県、福島県の中小企業を対象に実施。
- 対象地域内の中小企業５０社以上を対象に、サイバーセキュリティ対策を実施し、結果を政府（IPA）に報告。



# サイバーセキュリティ対策を、もう一歩踏み出す集団作り

- 事業者の実態に応じたサービスを選択提供することで、セキュリティレベルに底上げします。
- 中小企業にとって参加しやすいサービス提供に必要なデータを収集・分析します。
- 「お助け隊参加企業は、真剣に取り組んでいるので安心」というブランドを提供します。

## 想定ユーザー

必要なのは分かるけど、色々あって何をやればいいのか分からない…

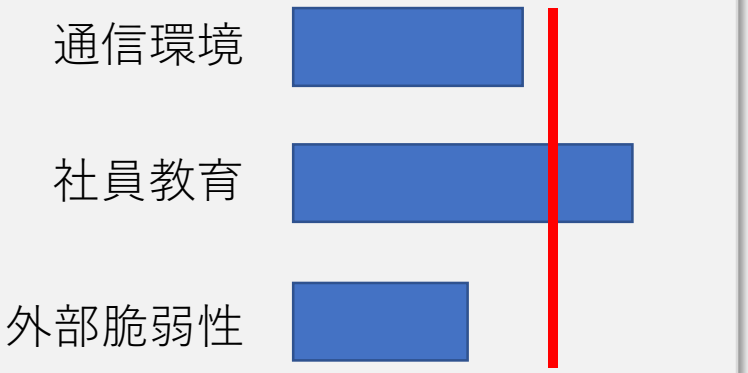
一応は対策をしているつもりなんだけど、漠然とした不安の日々…

**サイバーセキュリティお助け隊 in 東北**
現状把握をした上で、
さらに一歩を踏み出しましょう！

- まずは現状把握のための各種調査を実施。
- そのうえで、複数のサービスの中から適切な対策を実験的に導入。
- 併せて、IT・セキュリティに関する各種相談対応、インシデント発生時の対策支援なども提供。

## Ⅰ 現状把握

**まずは自社の置かれた現状を把握**




## Ⅱ 対策

- 出入口監視
- 端末監視
- 脆弱性診断

## Ⅲ サポートデスク

- 各種相談
- 被害発生時の対応

# 目次

# 実証参加申込企業の獲得結果

DIGITAL HEARTS

- 地場企業を通じた個別アプローチ等の勧誘活動により、効率よく参加企業を獲得することができた。
- サービス提供フローでの離脱が見られた。導入・運用の生産性向上が課題。

参加検討企業
102社

※セミナー等の不特定多数への集客よりも、地場企業等の協力を得て戸別勧誘を重視して実施

実証参加申込
59社

環境調査
59社

共通サービス
56社

メール訓練
56社

web診断
43社

※顧客都合によるキャンセル
3社（5%）

個別サービス
56社

UTM
22社

EDR
29社

脆弱性診断
5社

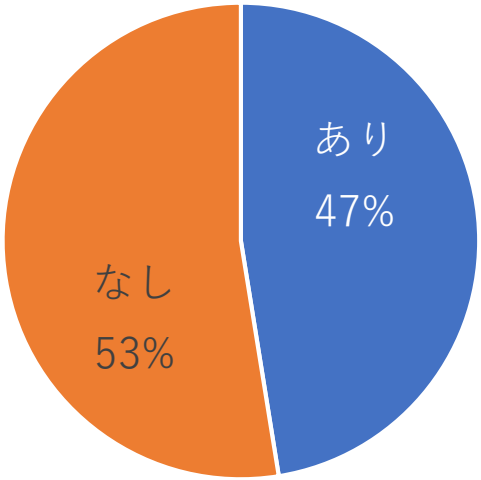
※このうち8社（14%）は導入時に問題が発生してサービス提供できず

# 申込企業の実態　1／3

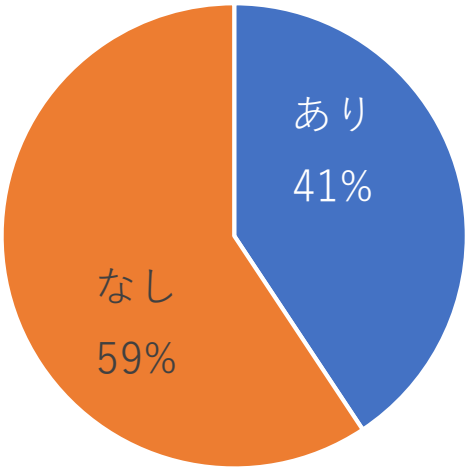
**IT資産に関する情報は半数以上は管理がなされていない状況。**

## IT資産管理に関する調査

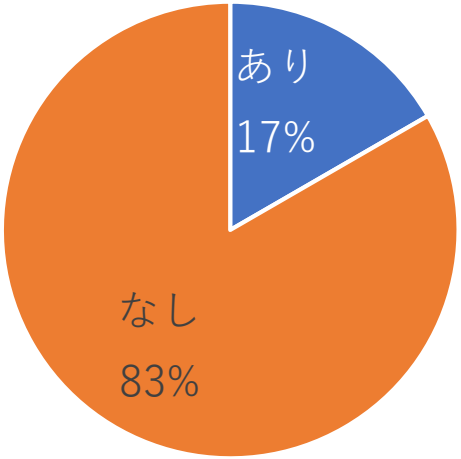
PC管理台帳
保有するPCのSW・HW情報、使用者等




ネットワーク構成図
NW構成、IP等の情報




IT資産管理台帳
NW機器、サーバー、複合機等の情報

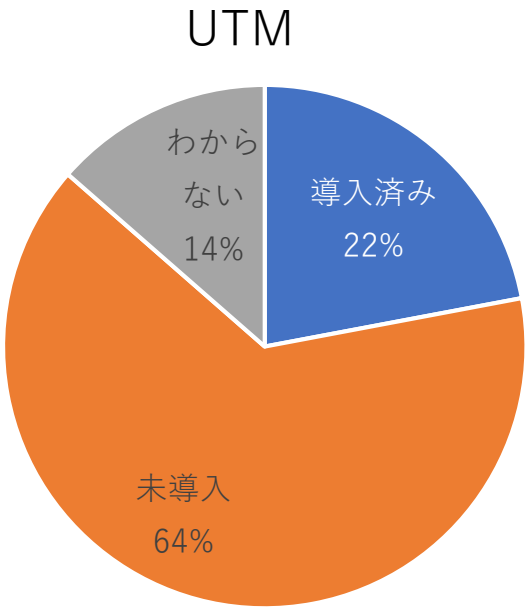


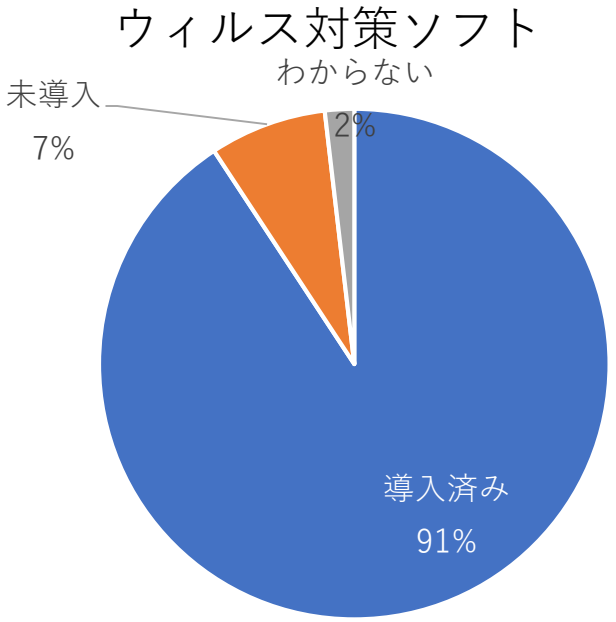

※n=59　実証参加申込企業

# 申込企業の実態　2／3

**UTMは約20%しか導入が進んでいない**
**ウィルス対策ソフトは90%以上が導入済み（EDRではなくアンチウィルス）**

## セキュリティ対策の導入状況の調査



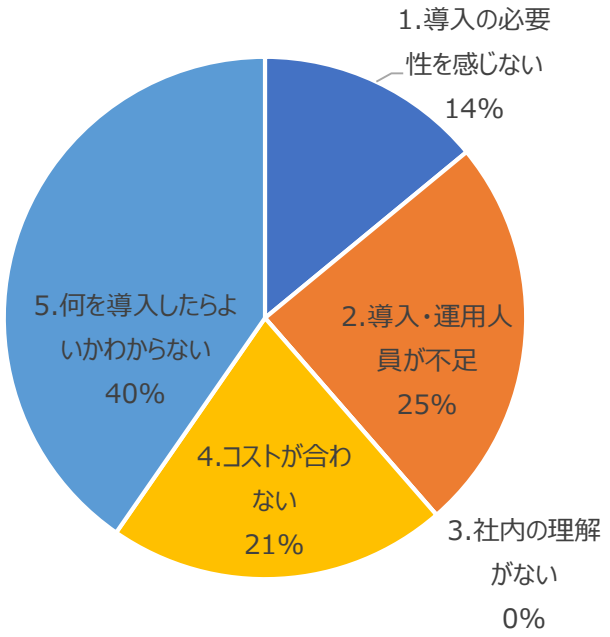

※n=59　実証参加申込企業

# 申込企業の実態　3／3

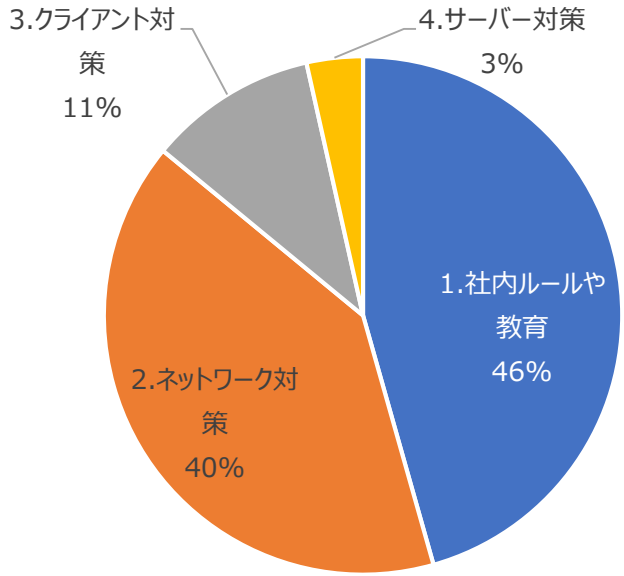
「何を導入すべきか？」が最も大きな課題となり、次いで人員面、コスト面となった。
強化点については対策以前に社内ルール・教育面が必要と考えている企業が多い

## サイバーセキュリティに関する意識調査

対策を進める上での障壁・課題




業務特性上、強化すべき点

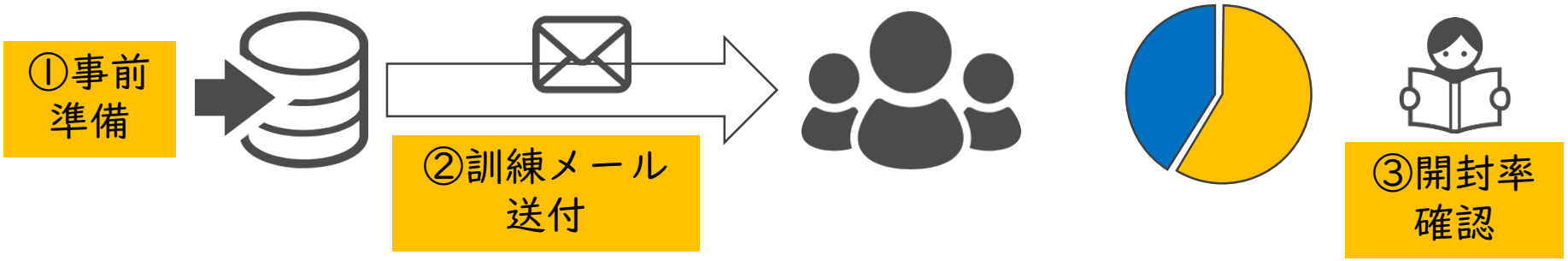



※n=59　実証参加申込企業

# 共通サービス　1　メール訓練

DIGITAL HEARTS

- 社員教育に関する調査（標的型攻撃メール訓練）



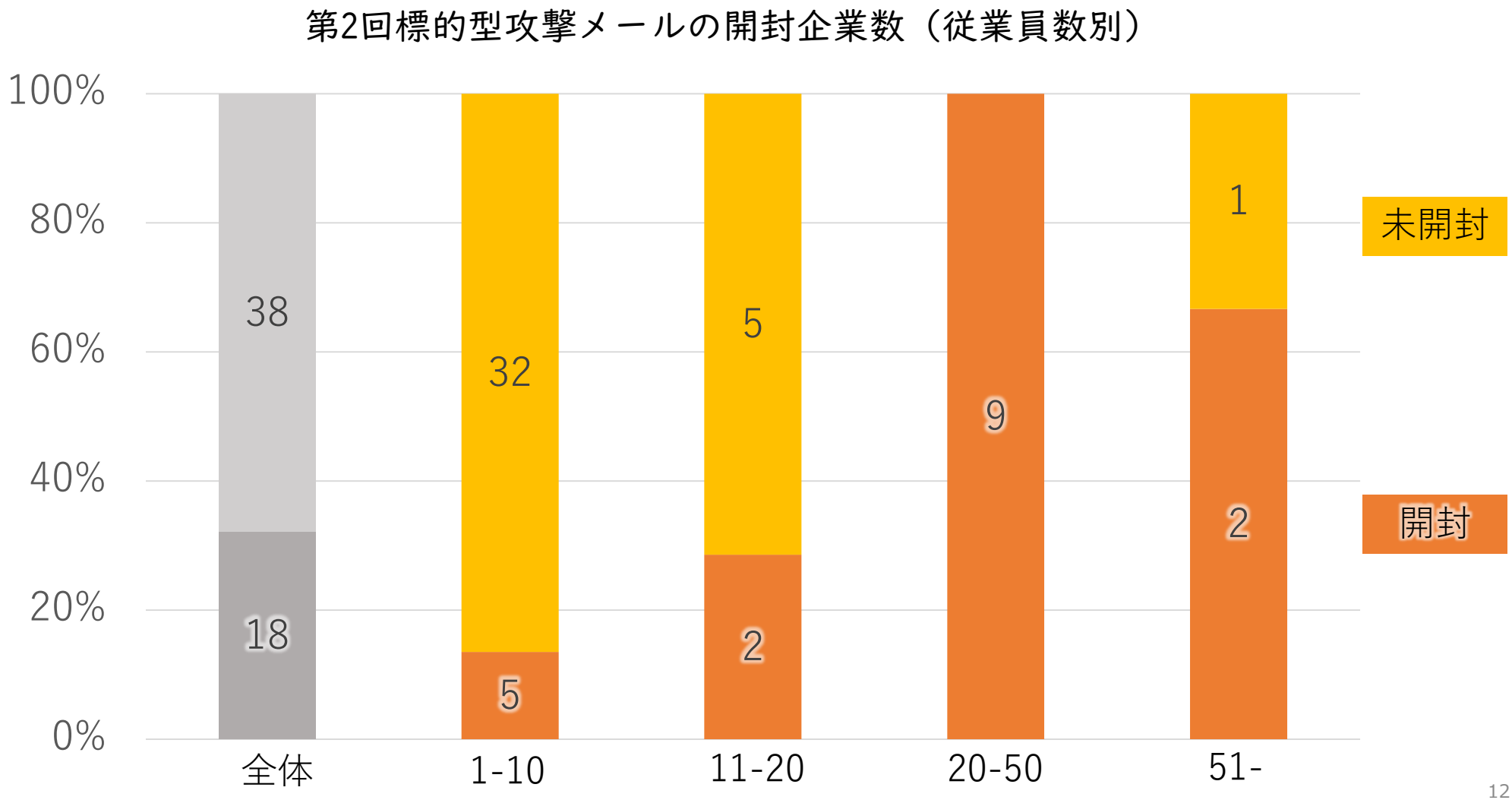

| 内容 | 実施企業数 | 送信数 | 開封検知数 | 検知率 |
|---|---|---|---|---|
| 第１回（10月） | 42 | 543 | 13 | 2.4% |
| 第２回（11月） | 56 | 886 | 77 | 10.0% |
| 第３回（12月） | 56 | 856 | 25 | 2.9% |
| 合計 | ー | 1429 | 90 | 6.3% |

【偽装メール内容】

- 第１回：取引先を名乗る企業よりセキュリティアップデートを促すURLリンクへ誘導するメール
- 第２回：健康管理センターを名乗る団体から新型コロナウィルス健康調査アンケートのURLへ誘導するメール
- 第３回：定期会議参加者を名乗る担当者より議事録送付としてPDF閲覧を誘導するメール

# 共通サービス　1　メール訓練（続き）

**第2回の訓練に参加した56社のうち、1件以上の開封検知があった企業は18社（32%）**
**特に従業員20名以上の企業で開封率が高くなる結果が得られた。**



# 共通サービス　2　ウェブ診断

DIGITAL HEARTS

- 外部脆弱性に関する調査（webセキュリティ診断）

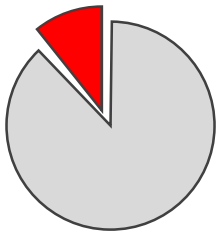

①脆弱性がないか調査

危険

No.1
SQLインジェクションの危険性を検出
https://www.example.com/.../.../

No.2 …

②調査結果を報告



100サイト中
Nか所に脆弱性

| 検知内容 | 検知数 | 危険性 |
|---|---|---|
| OSコマンドインジェクション | 1 | 悪意ある改ざん、情報漏洩 |
| クロスサイトスクリプティング | 2 | 悪意ある改ざん、情報漏洩 |
| ディレクトリインデックス | 3 | 情報漏洩 |
| 合計 | 6 | |

**実施対象４3社**が指定した自社のWEBサイトをツールによる自動診断を行った。

そのうち３社において合計６件の脆弱性を発見。

# 個別サービス　1　UTM・EDRによるセキュリティ監視

DIGITAL HEARTS

- UTMやEDRにより不正なアクセスを検知・防御することができた。
- 期間中、個別支援が必要なサイバーセキュリティインシデントは発生せず。

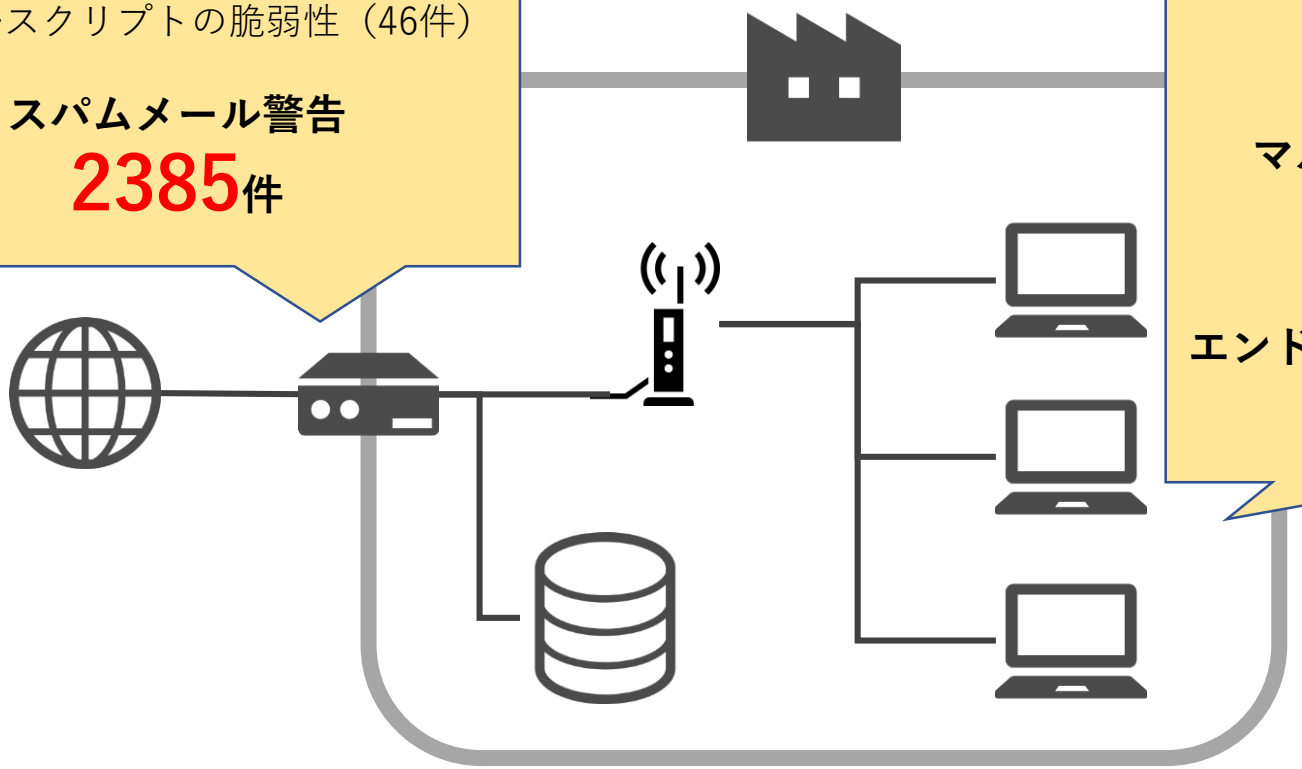
**外部からの不正アクセス検知**

**430件**

・UDPのLand攻撃(129件)
・OpenSSLの脆弱性(50件)
・シェルスクリプトの脆弱性（46件）
など

**スパムメール警告**

**2385件**



**内部不正プログラム検知**

**219件**

**不正サイトアクセスブロック**

**52件**

**マルウェア検知・無害化**

**7件**

**エンドポイントのアラート検知**

**392件**

※12月31日までの
アラート状況

# 個別サービス　1（続き）　セキュリティインシデントではないが・・・

12月の月次報告において、12社（EDR監視企業の50%）に対して以下の事項を指摘。

**●疑わしい挙動をするマルウェア（悪意のある動作をするソフトウェア）や業務上不要と考えられるアプリケーションの自動除去（６件）**

→従業員が業務PCでフリーゲーム等をダウンロードして利用している可能性

→業務上必要なソフトだとしても、システム管理者に申請してインストールする等の手続きが未整備で把握できていない

**●スパムURLやマルウェアのダウンロードに繋がるサイトへのアクセス自動ブロック（４件）**

→従業員が業務と関係のないウェブサイトにアクセスしている可能性

**●非推奨ブラウザ、バージョンの古いブラウザの使用（２件）**

→サポートを受けられないブラウザの継続使用はセキュリティ上のリスク

- EDR導入により、従業員の不適切なインターネット利用の実態を明らかにすることが出来た。これは将来的なサイバー攻撃の潜在的リスクとなり得るもの。
- フリーソフトの利用等に対するシステム管理者への申請手続きを整備するなど、従業員のIT利用の実態把握と適正管理に向けた継続的努力が必要。

# 個別サービス　2　脆弱性診断（手動）の結果

- **実施対象5社**のWEBサイトを当社エシカルハッカーにて手動診断（1社につき2日程度）。
- 5社すべてにおいて実害を受ける可能性がある脆弱性を発見。うち3社は緊急に対応が必要な状況であった。

| 危険度 | 内容 | 検知数 | A | B | C | D | E |
|---|---|---|---|---|---|---|---|
| 1.critical | xmlrpc.phpが有効となっている | 1 | 1 | | | | |
| 2.high | サポート切れソフトウェアの使用 | 1 | 1 | | | | |
| | メールヘッダインジェクション | 1 | | 1 | | | |
| | WordPressにおけるXML-RPCの悪用 | 1 | | | 1 | | |
| 3.mid | Cookieのセキュア属性不備 | 1 | | 1 | | | |
| | xmlrpc.phpが有効となっている | 1 | | | | 1 | |
| | クロスサイト・スクリプティング(蓄積型) | 1 | | 1 | | | |
| | 脆弱性のあるBootstrapの使用 | 1 | | 1 | | | |
| | 脆弱性のあるJQueryの使用 | 2 | | 1 | 1 | | |
| | 脆弱性のあるlazysizesの使用 | 1 | | 1 | | | |
| | 認証なしにアクセス可能な非公開情報 | 1 | | | 1 | | |
| | 脆弱性のあるソフトウェアの使用 | 1 | | | | | 1 |
| 4.low | クリックジャッキング　等 | 18 | 4 | 3 | 1 | 6 | 4 |
| 5.info | PHPのバージョン露出　等 | 12 | 3 | 3 | 2 | 3 | 1 |
| 総計 | | 43 | 9 | 12 | 6 | 10 | 6 |

# 目次

# サービス化に向けた検討　個別ヒアリング等から得られた示唆

| 項目 | 要点 |
|---|---|
| 参加動機 | • 取引先からの要請（行政機関、電力系団体、自動車メーカー）<br>• サイバー犯罪被害に関する報道。<br>• セキュリティ専任ではない。何をすべきか、どこまで取り組むべきかが分からない。<br>• 従業員からの情報漏洩が怖い。コロナでリモート拡大。 |
| 導入の手間 | UTM：訪問設置の日程調整が困難。申込29社中5社（17%）は、訪問時に他社製品を確認したこと等を理由にキャンセル。（自社の現状が把握できていない）<br>EDR：インストーラを送付して作業を依頼するだけでは進まない。訪問して実施したケースも多数。申込25社中3社（12%）は、既存アンチウィルスソフトのパスワードが分からないからサービス終了後に元に戻せないことを懸念してキャンセル。 |
| 従業員教育 | • メール訓練は多くの顧客から好評。時事ネタ（コロナ関連メール）の開封率が高い。<br>• EDRが、業務PCでフリーソフト（ゲーム）のダウンロードを検知・自動削除した事例。 |
| 脆弱性 | • ウェブサイトが改ざん可能な状態で放置されている（特にWordpress関連）<br>• 手動で診断したすべての企業において修正すべき脆弱性を検出。<br>• IEの継続利用、古いバージョンのOSの利用なども見られた。 |
| 商用化に向けて | • 継続的な従業員教育に対する課題を感じている企業は多い。<br>• UTMやEDRのセキュリティレポートに関しては関心が低い（技術的で理解しづらい）<br>• 生産設備への投資は惜しまないが、セキュリティにお金をかけるのは… |

# サービス化に向けた検討　カスタマージャーニーマップで考える

| | 認知 | 情報収集 | 参加 | 継続 |
|---|---|---|---|---|
| 行動 | • 取引先からの要求<br>• 報道情報<br>• 身近な被害事例 | • ネット検索<br>• セミナー参加<br>• 仲間に聞いてみる | • 従業員教育<br>• ソフトウェア導入<br>• ハードウェア設置 | • サービス継続<br>• 追加対策<br>• 最新の情報収集 |
| 顧客心理 | • やる必要は感じつつあるが、専任じゃないし。 | • 何をやるべきか、どこまでやるべきか。 | • 導入が面倒。きっとこれで大丈夫なんだろう。 | • 余裕があればやるけど、他にもやるべきことが…。 |
| 課題 | 日本全体でPRを徹底的に行い「対策を講じているのが普通」という機運を醸成。 | 「まずはこれ」というサービスを認定して最初の一歩を踏み出させる。 | スムーズな導入に向けた手順。顧客に分かりやすく情報提供。可視化する仕組み。 | 「攻めのセキュリティ」投資が報われる仕組み作り。継続するインセンティブ。 |
| 対策 | PR活動 | 認定サービス紹介 | サービス提供 | サービス改善 |

サプライチェーン・サイバーセキュリティ・コンソーシアム

実態報告

お助け隊事業者

# サービス化に向けた検討　コンソーシアムと連携したビジネス化の必要性

**顧客獲得フェーズ**

**コンソーシアムへの期待**
- 取引先からの要求がより高まる発信（業界団体等の意識啓発）
- 類似の被害事例などの情報（お助け事業者間の連携）
- 最低限のサービスが導入される仕組み（認定制度）

**事業者が努力すべき事項**
- 優良なサービス設計・プロモーション（Web広告等）
- 営業代理店へのインセンティブ設計

**導入フェーズ**
- 申込から導入完了までのフローを出来る限り効率化
- 地場企業との連携により、きめ細かい伴走サポート

**運用フェーズ**
- 緊急時の駆けつけ支援、簡易サイバー保険
- サービスの継続的な改善、コンソへの実態の情報提供

**コンソーシアムへの期待**
- お助け隊企業から情報を吸い上げる仕組み（被害事例等）
- 参加企業が報われる仕組み（可視化、優良企業表彰制度など）

# サービス化に向けた検討　行動経済学で考える

## ◆セキュリティ領域に継続的に投資し続けてもらう仕組み

・保有効果：自分が選んだものには価値があると思う心理効果。

・コンプリート欲求：欠けている状態が可視化されると揃えたくなる心理効果。

・コンコルド効果：ある程度投資が積み重なると途中で辞めるのが惜しくなる心理効果。

## ◆セキュリティ投資を面的に拡大する仕組み

・ソーシャルネットワークインセンティブ

①「お助け隊参加企業リスト」をweb上に掲示して可視化。「あなたと同規模の企業がN社参加しています！」といった情報が表示される仕組み。「入っているのが当たり前」という空気を作る。（c.f. Security Actionの星取得）

②複数の参加企業でグループを作り、自社が頑張ると仲間にギフトポイントが付与される設計にする。（省エネやヘルスケア領域での実証例）

# サービス化に向けた検討　実証終了後の自主事業化構想

現状把握、セキュリティ力向上に向けた対応を伴走支援

デジタルハーツ
お助け隊

お助け隊
ダッシュボード
（開発中）

ここにログインすれば自社の状況がすぐに分かる

月額
課金

サービス利用企業

お助け隊認定サービス
（EDRタイプ）

月額2000円／PC以内の価格体系を検討

★EDRログ
UTMログ
メール訓練結果
脆弱性診断結果
Etc…

企業規模・実態に応じて必要項目を選択

インシデント対応
簡易サイバー保険

何かあったらすぐ相談できる

## サイバーセキュリティお助け隊

**WEB** ：www.cyber-otasuke.jp

**メール** ：otasuke_r2cs@digitalhearts.com

**電話** ：0570-098-098（ナビダイヤル）

**法 人 名** ： 株式会社デジタルハーツ

**所 在 地** ： 〒163-1441 東京都新宿区西新宿3-20-2 東京オペラシティ41F

DIGITAL HEARTS

*SAVE the DIGITAL WORLD*