東北地域サイバーセキュリティセミナー

中小企業における
サイバーセキュリティ対策と導入事例

令和3年12月15日（水）

15:30～16:15

サイバーセキュリティ・ネットワークグループ

SOCチーム　清藤 雅高

［情報処理安全確保支援士 登録番号 018681］

株式会社 ハイテックシステム

本日の内容

【テーマ】中小企業におけるサイバーセキュリティ対策の推進

１．サイバーセキュリティのキーワード
２．セキュリティインシデントの事例
３．セキュリティ対策の現状
４．セキュリティ対策で何を重視すべきか
５．セキュリティ対策推進を阻む問題点
６．セキュリティ対策推進のポイント
７．セキュリティ対策の導入事例
８．まとめ

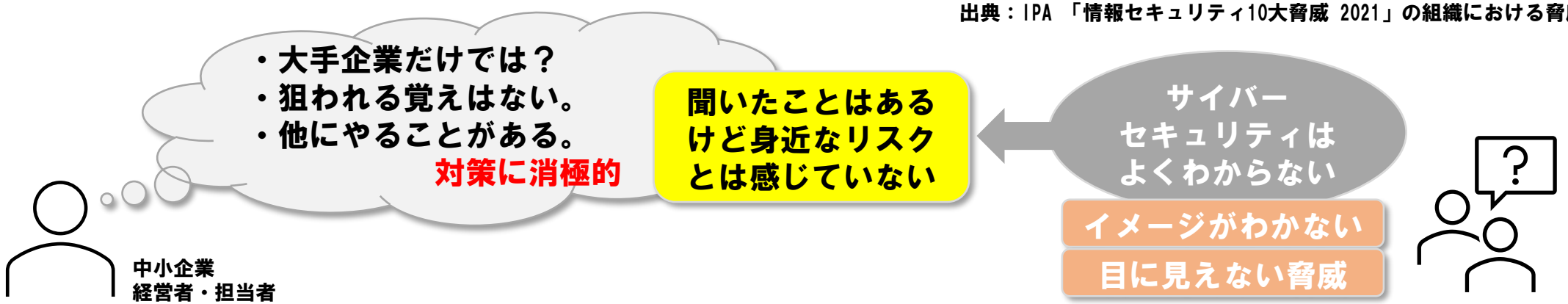
１．サイバーセキュリティのキーワード

1．サイバーセキュリティのキーワード

中小企業におけるサイバーセキュリティのキーワードとして…

順位	内容	順位	内容
1位	ランサムウェアによる被害	6位	内部不正による情報漏えい
2位	標的型攻撃による機密情報の窃取	7位	予期せぬIT基盤の障害に伴う業務停止
3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	8位	インターネット上のサービスへの不正ログイン
4位	サプライチェーンの弱点を悪用した攻撃	9位	不注意による情報漏えい等の被害
5位	ビジネスメール詐欺による金銭被害	10位	脆弱性対策情報の公開に伴う悪用増加

出典：IPA 「情報セキュリティ10大脅威 2021」の組織における脅威



1．サイバーセキュリティのキーワード

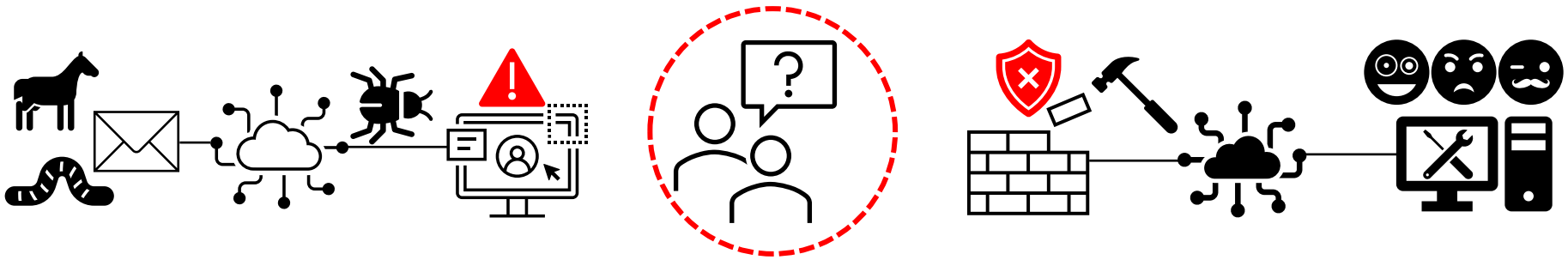
中小企業もキーワードにあるようなサイバー攻撃に遭うのか？

・**大手企業だけ**では？
・**狙われる覚えはない**。
・身近に**被害者がいない**。

中小企業
経営者・担当者

自社とは関係ない『稀なケース』と考える方が多い

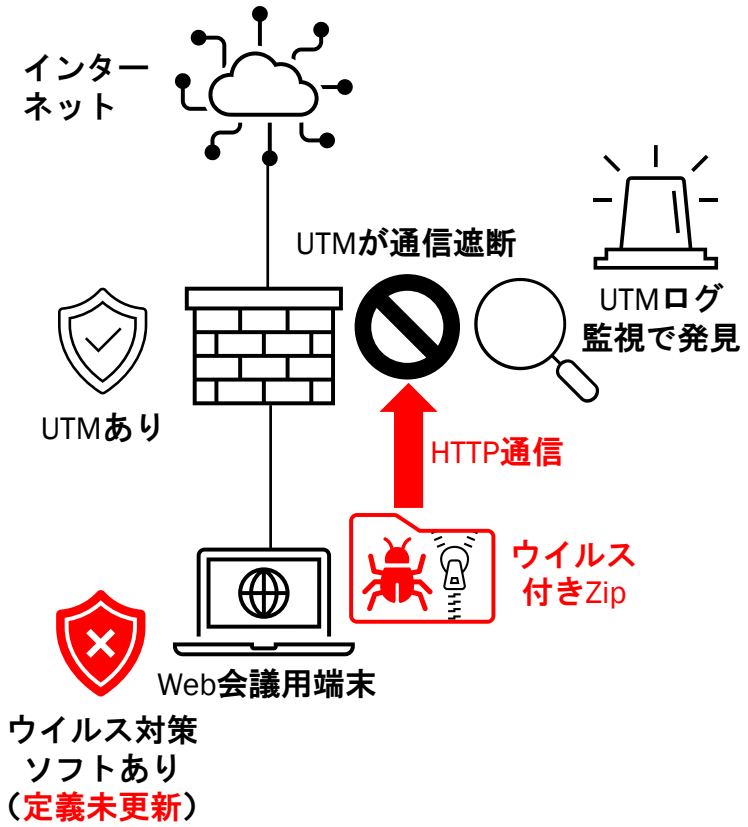
中小企業に対するサイバー攻撃は、稀なケースではありません。
身近に迫っている脅威に『気づいていない』、リスクが『見えていない』だけかもしれません。



２．セキュリティインシデントの事例

２．セキュリティインシデントの事例

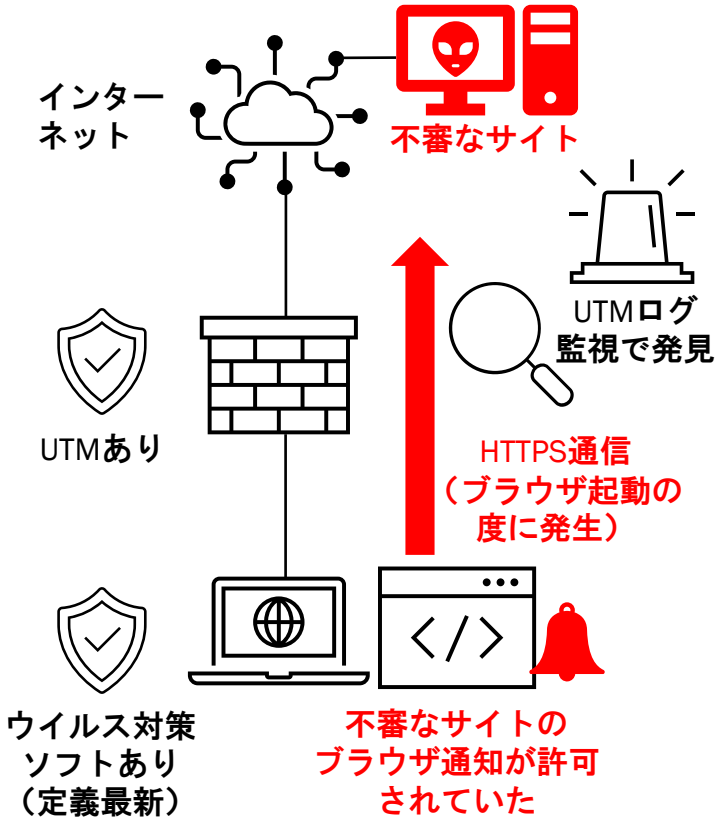
■事例１　社内から社外への圧縮ファイル（ウイルス付き）送信



- Web会議で使用していた端末にて、ウイルス対策ソフトはインストールされていたが、定義ファイルは未更新のまま放置されていた。
- 社内から社外へのHTTP通信がUTMで複数回遮断されている記録を、UTMログ監視で発見。
- 通信元の端末で改めてウイルススキャンを実施した結果、ウイルス検出が複数あり駆除。駆除後はウイルス付き圧縮ファイルの送信が止まった。

２．セキュリティインシデントの事例

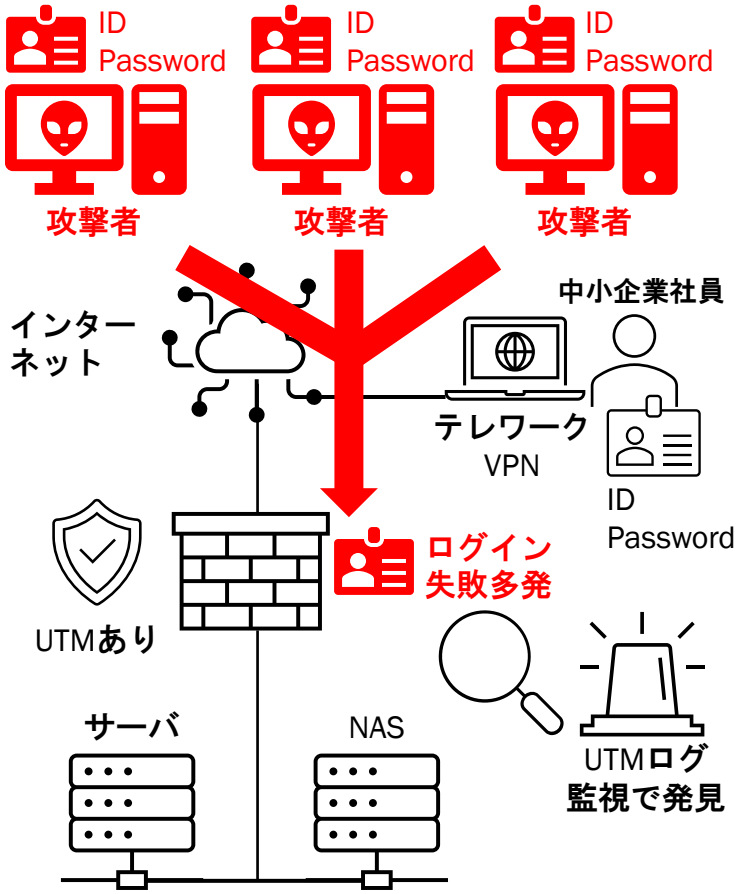
■事例２　ブラウザ通知許可による不審なサイトへの通信発生



- エンドポイントのウイルス対策は実施、定義ファイルも最新化されていた。
- 業務時間内に限り、ウイルス感染の可能性がある不審なサイトを宛先として通信が発生している記録を、UTMログ監視で発見。
- ウイルススキャンでは何も検出されず、ブラウザ設定から不審なサイトの通知許可を削除した結果、発生しなくなった。
- 偽装メッセージの表示や、ブラウザ利用中の不審なサイトへの誘導等はなかった。

２．セキュリティインシデントの事例

■事例３　SSL-VPN認証への総当たり攻撃

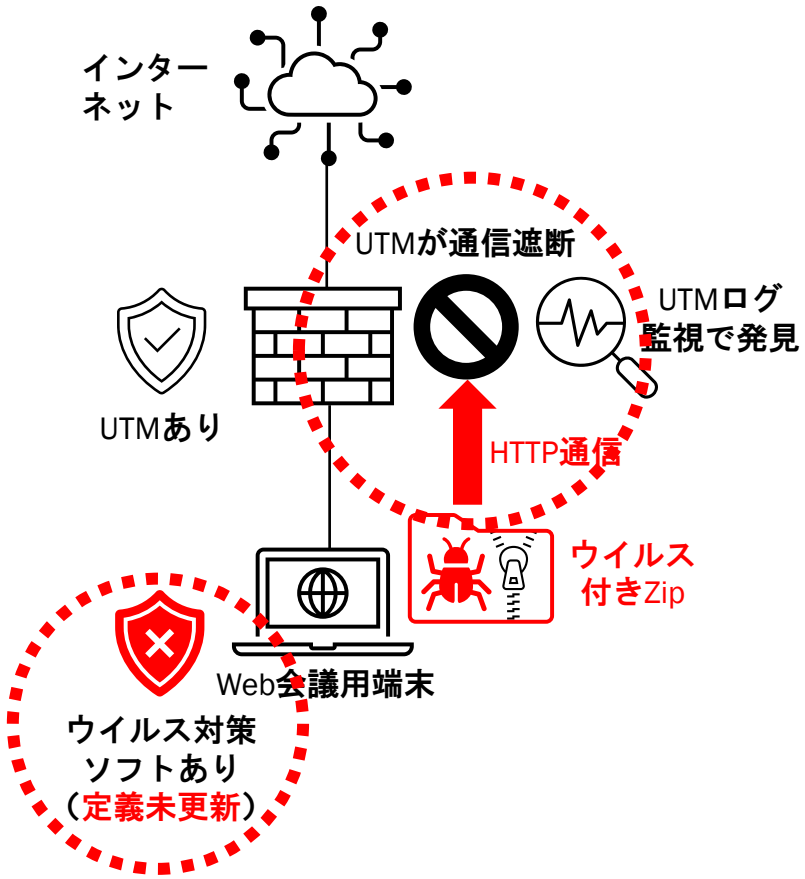


- テレワークのため、社外から社内へのリモートアクセスをUTMの認証機能で許可していた。
- UTMの認証機能でログイン失敗が多発している記録を、UTMログ監視で発見。
- 不特定多数の国内・海外の通信元から、IDとPasswordの組み合わせを変えた不正ログイン試行が数日間続いた。
- 推測可能なIDやPassword、簡易的なPassword設定は速やかに変更して頂くよう案内、不正ログイン被害等の報告はなかった。

３．セキュリティ対策の現状

3．セキュリティ対策の現状

■事例１の問題や課題として何があるでしょうか？



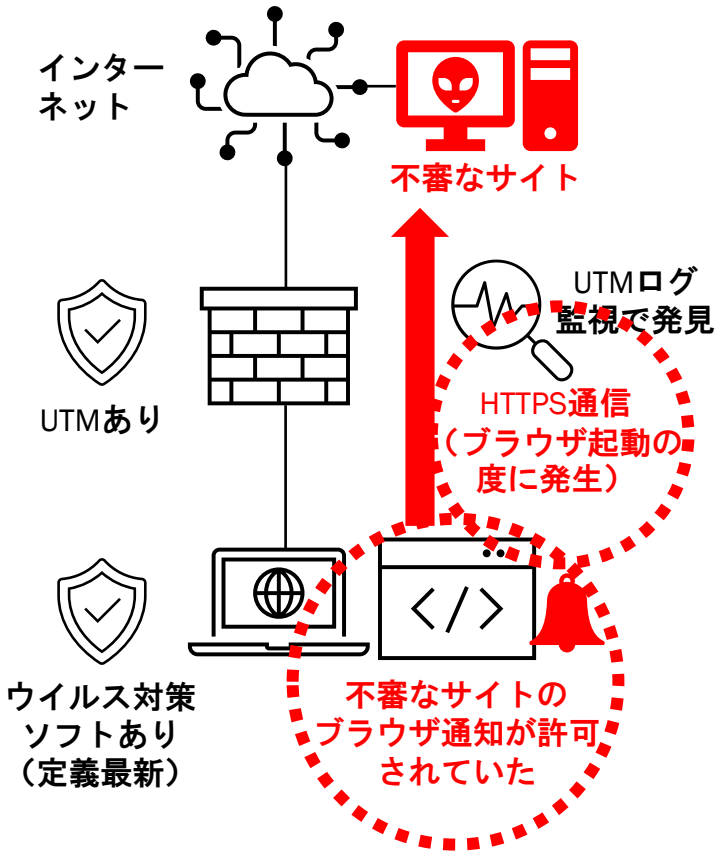
- ウイルス対策ソフトをインストールしていても、適切な管理がされていない『**放置**』状態では対策の有効性が低下。
- 通信がブロックされていて、実害がなかったとしても、決して『**安全ではない**』。

共用端末や利用頻度の低い端末の脆弱性を見落としていませんか？

外部からのサイバー攻撃ではなく、**内部から外部への不審な通信**を発見できますか？

３．セキュリティ対策の現状

■事例２の問題や課題として何があるでしょうか？



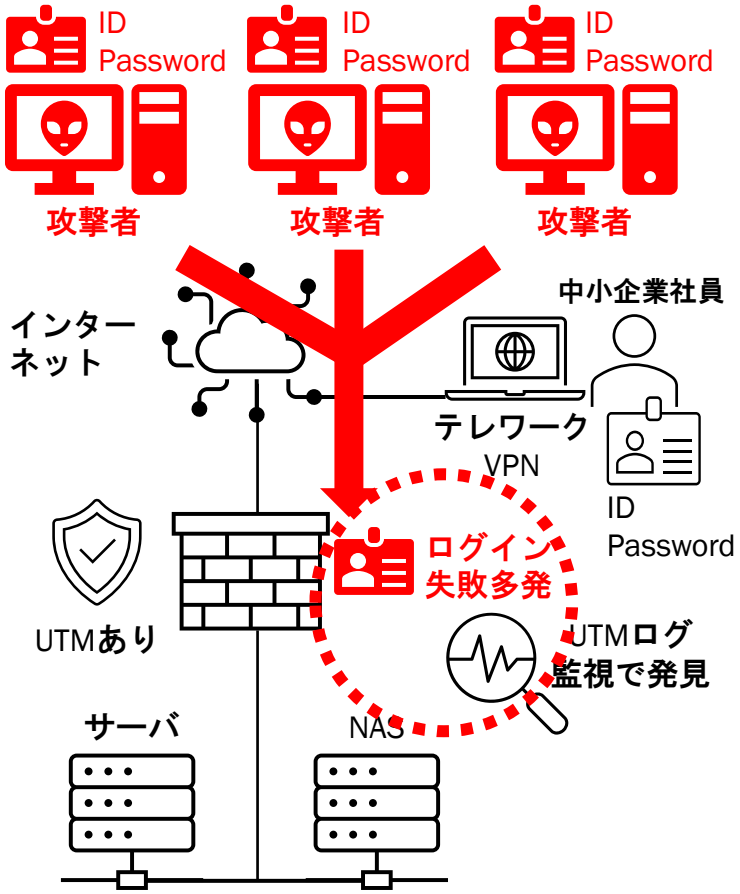
- ブラウザの『**設定**』に起因して発生しているため、ウイルス対策ソフトでは発見が難しい。
- 端末の画面に偽のメッセージが出たり、不審なサイトに誘導されたりといった、『**目に見える症状がない**』場合、脅威に気づけない。

ウイルス対策ソフトでは検出されない脅威への対応策はありますか？

目に見えない脅威をいち早く把握する手段はありますか？

３．セキュリティ対策の現状

■事例３の問題や課題として何があるでしょうか？



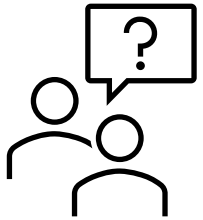
- 自社が攻撃の対象になっているかどうかは、『UTMログ』を見るなどしないとわからない。
- 不正ログインは成功しておらず、実害がなかったとしても、総当たり攻撃の場合は決して『安心できない』。

自社がサイバー攻撃の対象として狙われている状況に気づくことができますか？

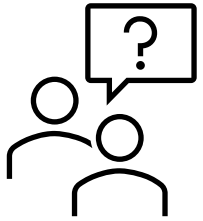
総当たり攻撃のように攻撃が続いている状況を把握できますか？

３．セキュリティ対策の現状

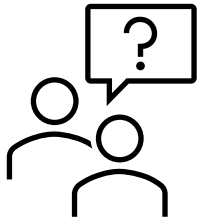
３つの事例から見えてくることは…



社内の脆弱性を『**見落としている**』ということはありませんか？

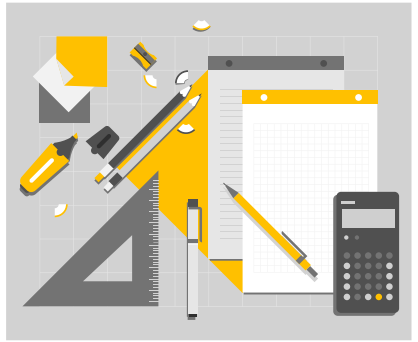


サイバー攻撃による脅威が『**見えていない**』ということはありませんか？



サイバー攻撃を受けていても『**気づいていない**』ということはありませんか？

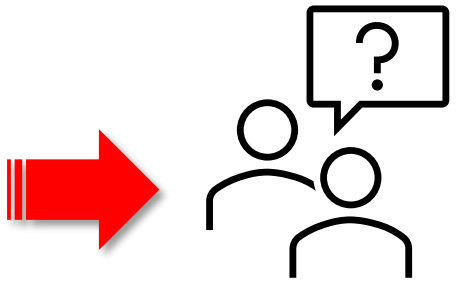
４．セキュリティ対策で何を重視すべきか



４．セキュリティ対策で何を重視すべきか

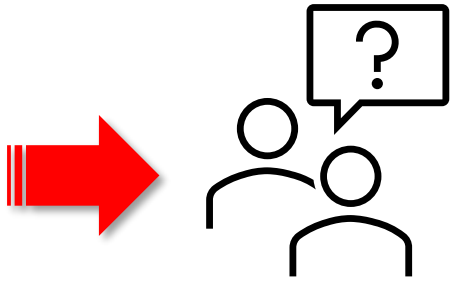
会社や自宅など建物の防犯を例に考えてみると…

施錠を忘れている



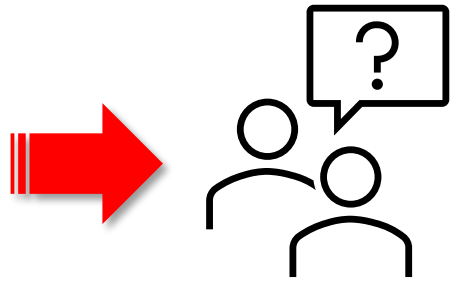
『見落としている』

空き巣に狙われている



『見えていない』

空き巣に入られかけた

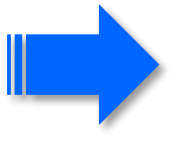


『気づいていない』

４．セキュリティ対策で何を重視すべきか

会社や自宅など建物の防犯を例に考えてみると…

施錠を忘れている

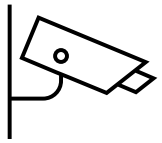


『チェックする』

空き巣に狙われている

『確認する』

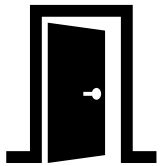
空き巣に入られかけた



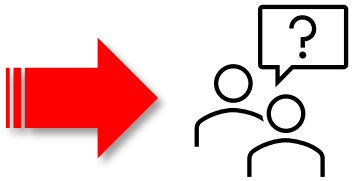
『監視する』

４．セキュリティ対策で何を重視すべきか

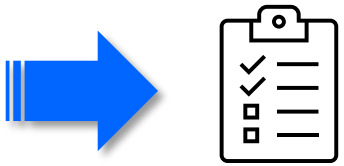
防犯の考え方をサイバーセキュリティ対策に当てはめてみると…



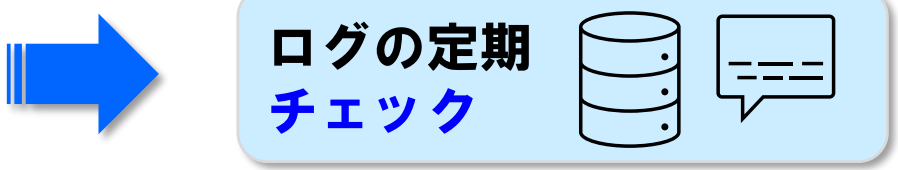
施錠を忘れている



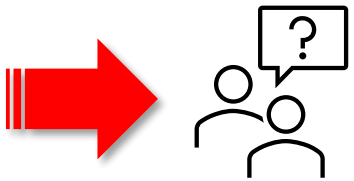
見落としている



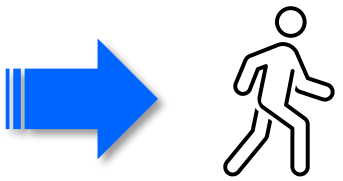
チェックする



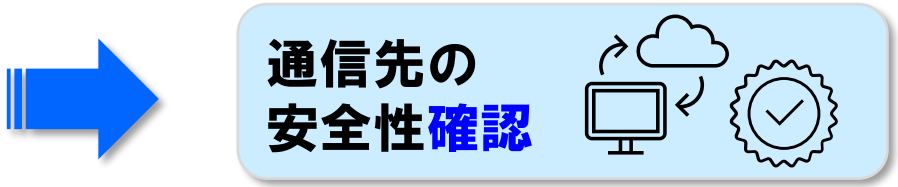
空き巣に狙われている



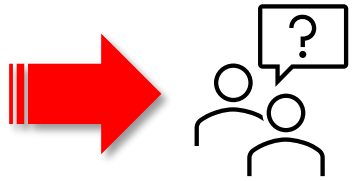
見えていない



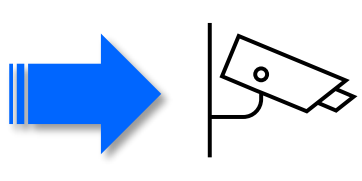
確認する



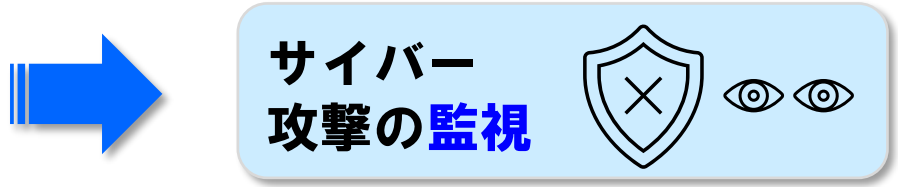
空き巣に入られかけた



気づいていない

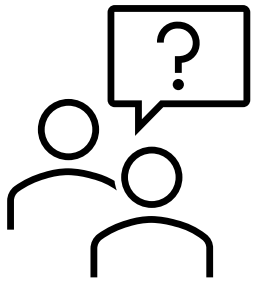


監視する

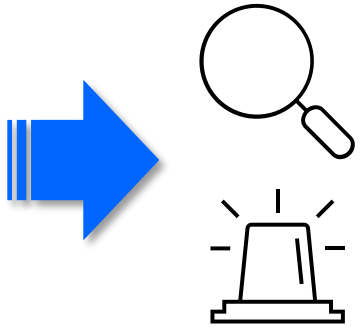


４．セキュリティ対策で何を重視すべきか

ご紹介した３つのセキュリティインシデント事例は…

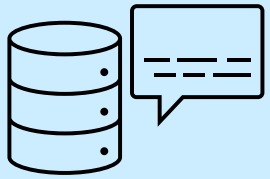


『見落としている』
『見えていない』
『気づいていない』

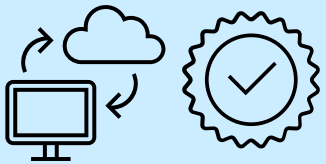


UTMの『ログ監視』でセキュリティインシデントが発見された。

ログの定期チェック

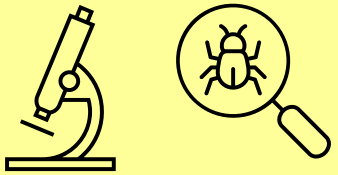


通信先の安全性確認



サイバー攻撃の監視

脅威をログ監視により『見える化』



５．セキュリティ対策推進を阻む問題点

５．セキュリティ対策推進を阻む問題点

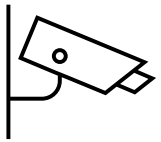
中小企業のセキュリティ対策がなかなか広まらない…

『チェックする』

- 施錠の記録を確認する
- 施錠箇所の現場を見る

『確認する』

- 不審者情報を確認する
- 防犯対策状況を確認する



『監視する』

- 映像を定期的に見る
- カメラが正常か点検する

５．セキュリティ対策推進を阻む問題点

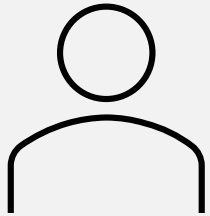
中小企業のセキュリティ対策推進を阻むものとは…

- 施錠の記録を確認する
- 施錠箇所の現場を見る

- 不審者情報を確認する
- 防犯対策状況を確認する

- 映像を定期的に見る
- カメラが正常か点検する

どれをやるにも
手間がかかる・知識がいる



・パソコン管理者
・情報システム担当

中小企業の
経営者が**兼務**
担当者が**ひとり**

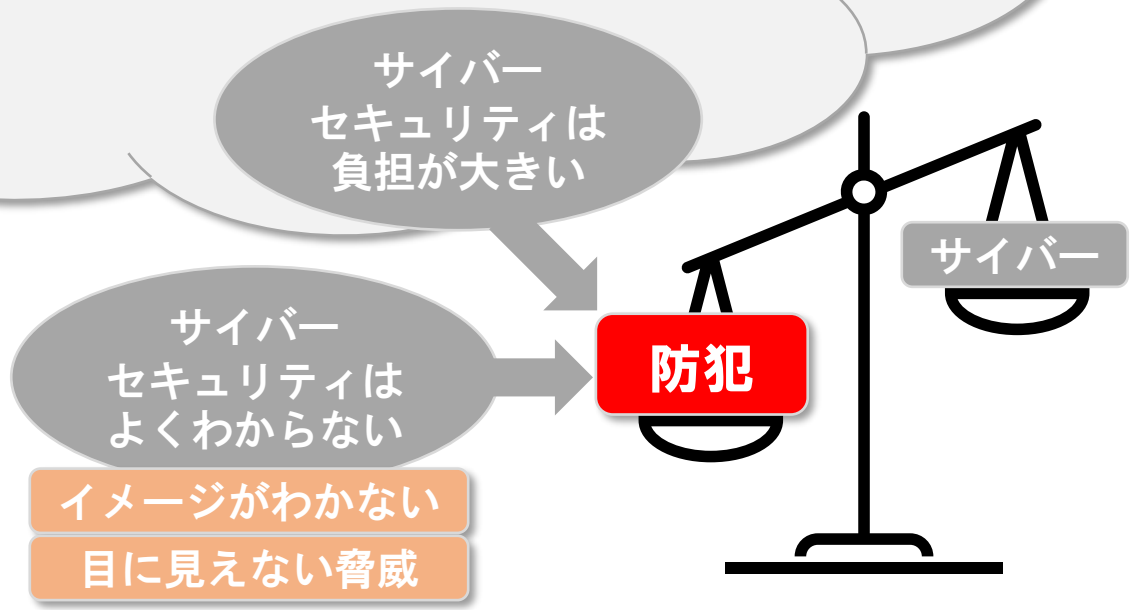
５．セキュリティ対策推進を阻む問題点

中小企業のセキュリティ対策推進を阻むものとは…

・経営や本業の傍らでサイバーセキュリティまでとても**手が回らない**。
・担当者が自分だけなので、セキュリティ対策で仕事の**負担が増える**。

・パソコン管理者
・情報システム担当

中小企業の経営者が兼務担当者がひとり

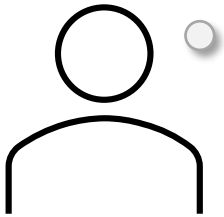


６．セキュリティ対策推進のポイント

６．セキュリティ対策推進のポイント

中小企業におけるセキュリティ対策推進のポイント

・経営や本業の傍らでサイバーセキュリティまで**手が回らない**。
・担当者が自分だけなので、セキュリティ対策で仕事の**負担が増える**。



・パソコン管理者
・情報システム担当

中小企業の経営者が兼務担当者がひとり

経営課題にする ステップ１

▼

優先順位をつける ステップ２

▼

外部委託も検討する ステップ３

６．セキュリティ対策推進のポイント

中小企業におけるセキュリティ対策推進のポイント

中小企業でもサイバー攻撃は身近な危険ということを社内で共有する（経営課題）

ステップ１

- ITは業務に無くてはならない存在
- セキュリティ事故は**信用失墜**に直結
- 信用失墜は**死活問題**になる恐れ

一度情報漏洩が起きた会社の信用は…

防犯対策と同じようにシンプルに考えて弱い所から対策をしていく（優先順位）

ステップ２

- いわゆる**防犯対策**をイメージ
- いま**一番不用心**なところはどこか
- 問題時に**業務影響**が大きいのは何か

ランサムウェアで電子カルテが…

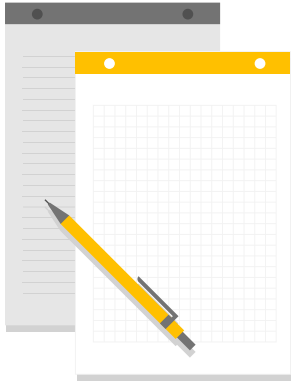
サイバーセキュリティ対策は導入後の業務負担軽減とセットで考える（外部委託）

ステップ３

- 担当者が**無理なく運用できる**対策か
- 対策導入後**放置**される恐れはないか
- **外部に頼む**方が良い部分はないか

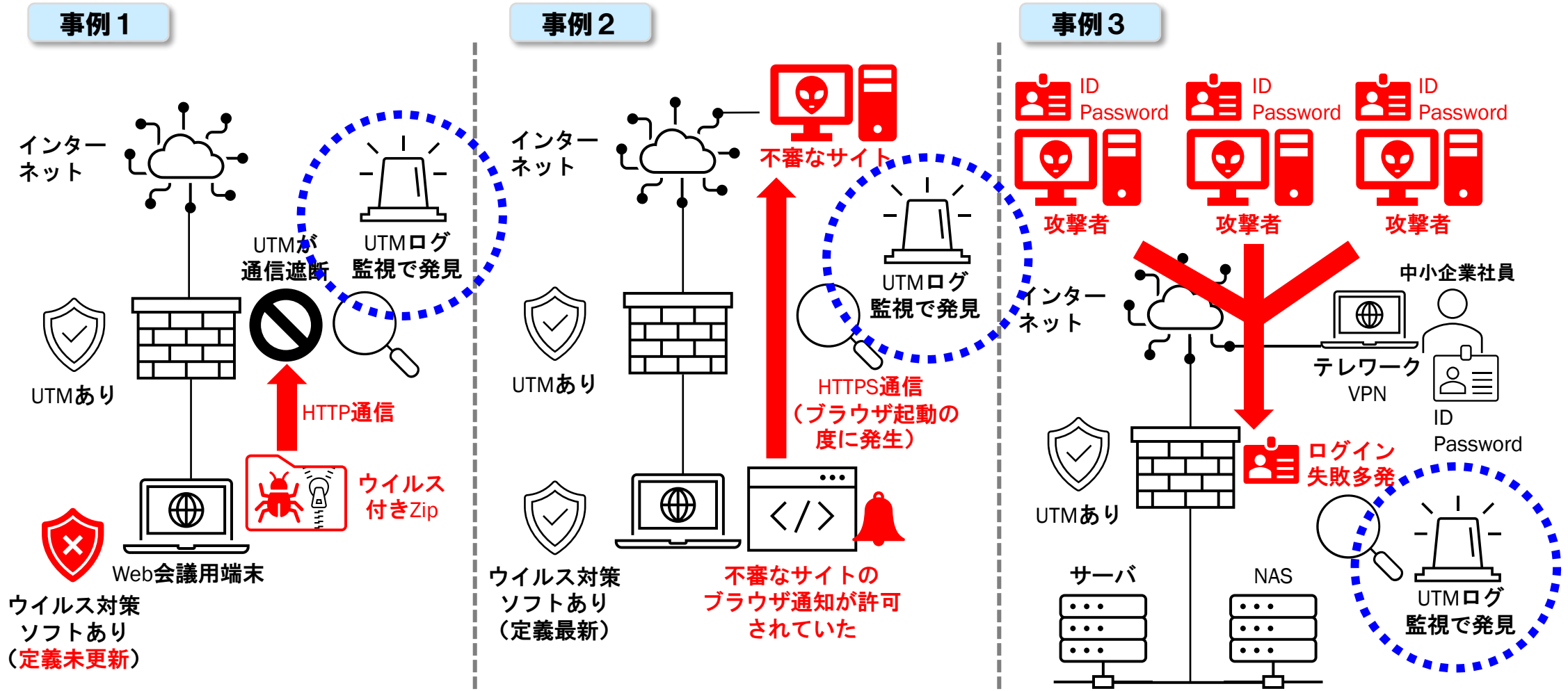
ログの監視を社内でやるには…

7．セキュリティ対策の導入事例



7．セキュリティ対策の導入事例

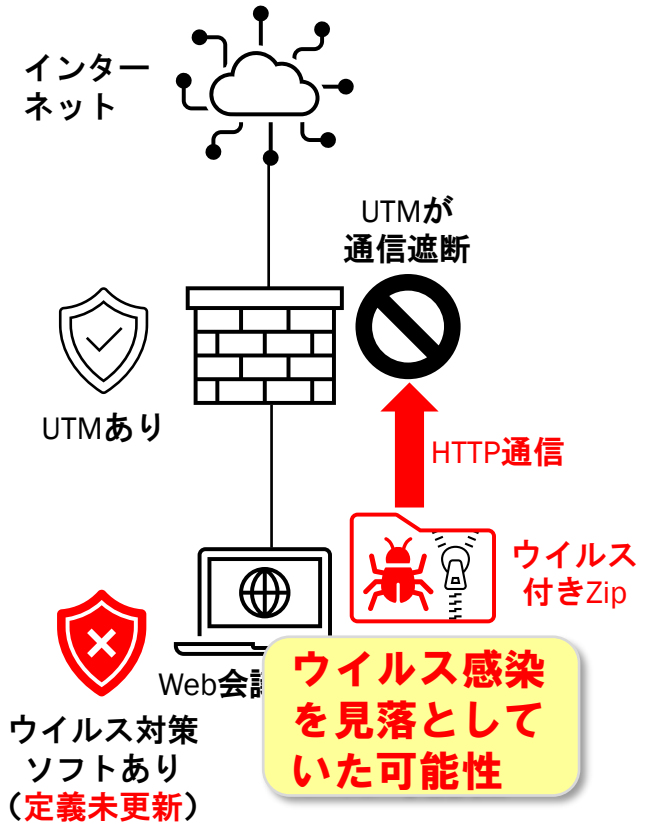
ご紹介した３つの事例は『ログ監視』サービスを導入済みだった



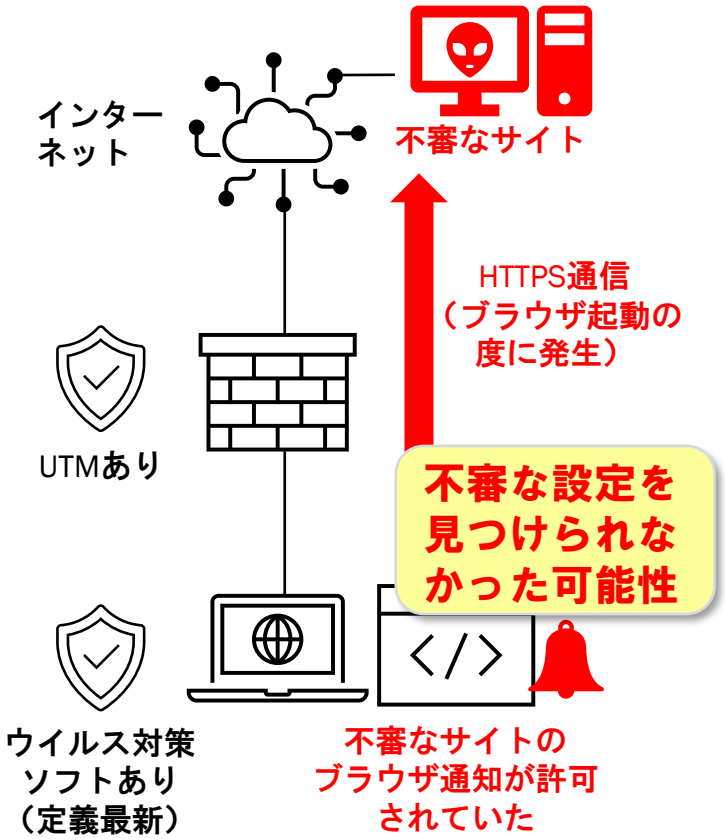
7．セキュリティ対策の導入事例

もし『ログ監視』サービスを導入していなかったら…

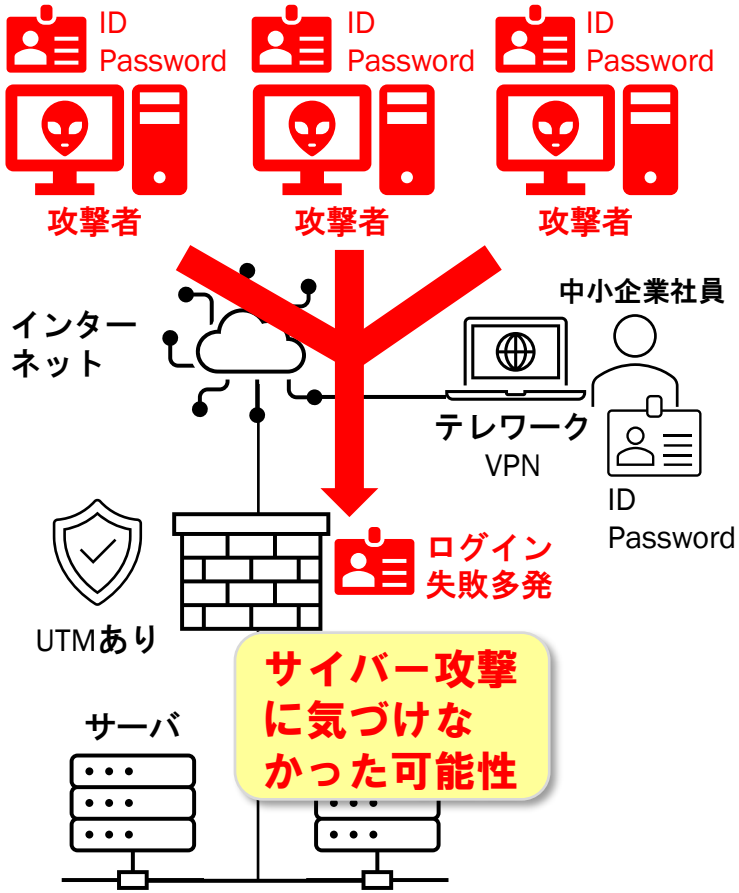
事例１



事例２



事例３



7．セキュリティ対策の導入事例

『ログ監視』サービスとは？

MSS（Managed Security Service）と呼ばれたりする、お客様のセキュリティシステムの運用管理や監視などを請け負うサービス。

ログの定期チェック

通信先の安全性確認

サイバー攻撃の監視

脅威をログ監視により『見える化』

外部に委託

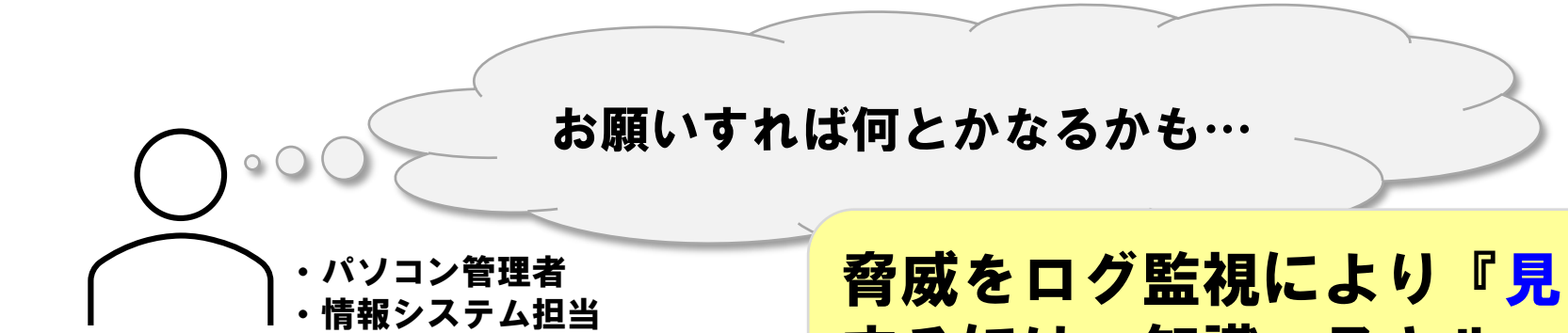
SOC（Security Operation Center）

7．セキュリティ対策の導入事例

『ログ監視』における外部委託のメリットは？

- 中小企業の経営者や担当者の**業務負担軽減**
- ログ監視に必要となる**知識やスキルの習得が不要**
- ログ分析に必要となる**システムの調達が不要**
- 通報サービスでインシデント発生を**いち早く知ることが可能**

など



脅威をログ監視により『**見える化**』するには、知識・スキル・システムなど必要になるものが多くある

８．まとめ

８．まとめ

- **中小企業へのサイバー攻撃は稀なケースではありません。**
  見えていない、気づいていないだけということはありませんか？

- **サイバーセキュリティ対策は企業の経営課題です。**
  インシデント発生は信用失墜、中小企業は死活問題になる恐れも。

- **サイバーセキュリティ対策の優先順位を考えましょう。**
  シンプルに考え、一番不用心なところ業務影響が大きいところから対策を。

- **サイバーセキュリティ対策導入後のことも考えましょう。**
  放置や極端な業務負担増にならないかを見極め、必要に応じて外部委託の検討を。

ご清聴ありがとうございました。

株式会社ハイテックシステム

https://www.hightech.co.jp/

【 本　社 】〒990-0023　山形県山形市松波1-16-7
TEL 023-628-9455 / FAX 023-628-9456

【札幌営業所】〒060-0063　北海道札幌市中央区南3条西8丁目2-1 SAKURA-S3
TEL 011-522-6308 / FAX 011-596-9271

【仙台オフィス】〒980-0803　宮城県仙台市青葉区国分町1丁目4-9　enspace

【 東京窓口 】子会社：株式会社デジタルファクトリー
〒100-0005　東京都千代田区丸の内2-2-1 岸本ビルヂング6階
TEL 050-5491-6960 / FAX 050-3488-9562

2021年11月現在