サイバーセキュリティセミナー’23 in 東北

TSOC
TOTAL SECURITY OPERATION CENTER

実例からわかる

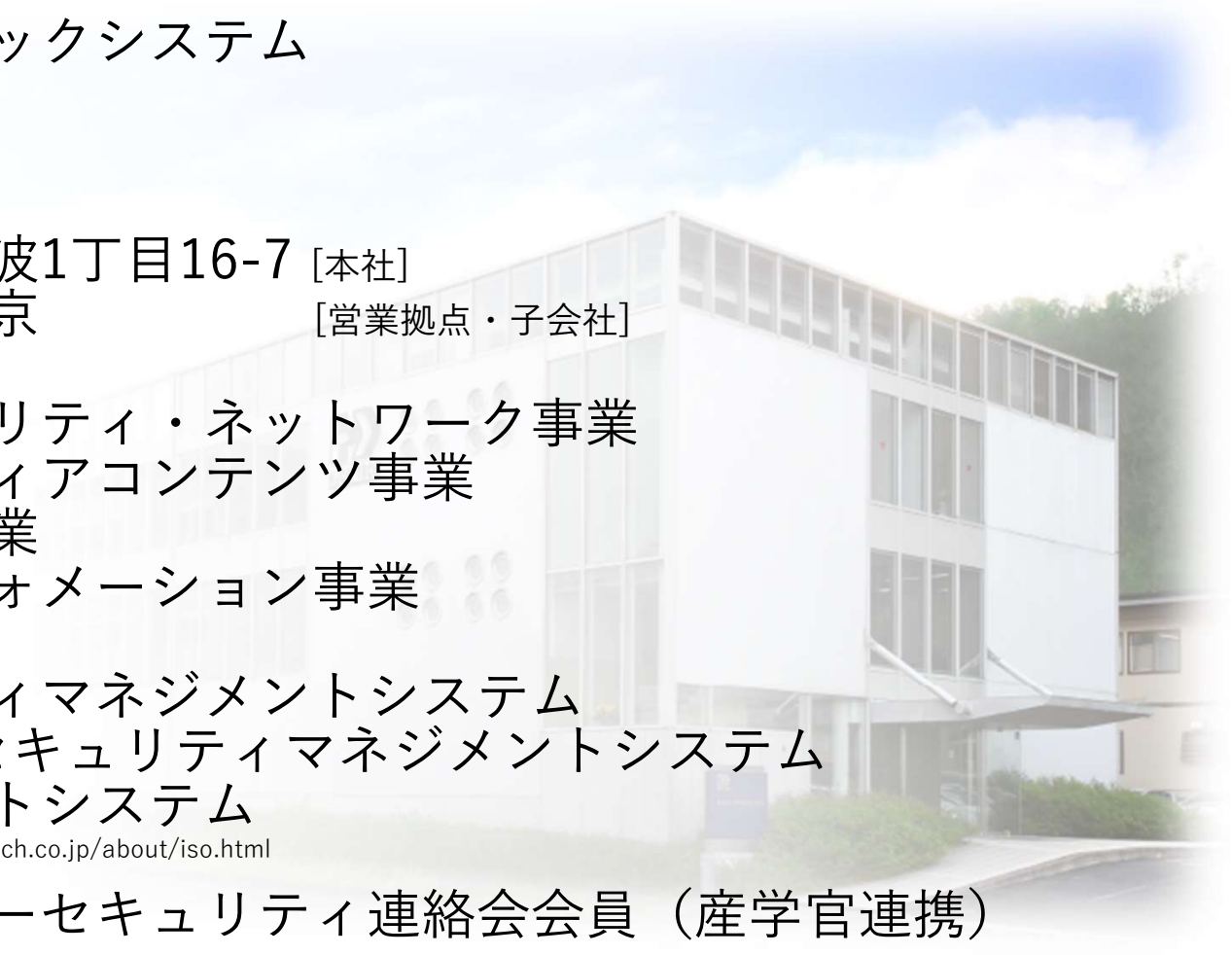
中小企業のサイバーセキュリティ強化策

2023/12/19（火）
オンライン開催

株式会社ハイテックシステム
HiGH TECH

はじめに

会社名	株式会社ハイテックシステム
設　立	1991年10月1日
所在地	山形県山形市松波1丁目16-7 [本社] 仙台・札幌・東京 [営業拠点・子会社]
事業内容	サイバーセキュリティ・ネットワーク事業 クラウド・メディアコンテンツ事業 保守サポート事業 デジタルインフォメーション事業
認証取得	情報セキュリティマネジメントシステム ISMSクラウドセキュリティマネジメントシステム 品質マネジメントシステム ISO情報URL：https://www.hightech.co.jp/about/iso.html
その他	東北地域サイバーセキュリティ連絡会会員（産学官連携）



はじめに

本日は、弊社TSOC（Total Security Operation Center）において、弊社の中小企業顧客で実際に起こったセキュリティインシデント事例を取り上げつつ、中小企業のサイバーセキュリティ強化策について考えて参りたいと思います。

サイバーセキュリティのキーワード

サイバーセキュリティのキーワード

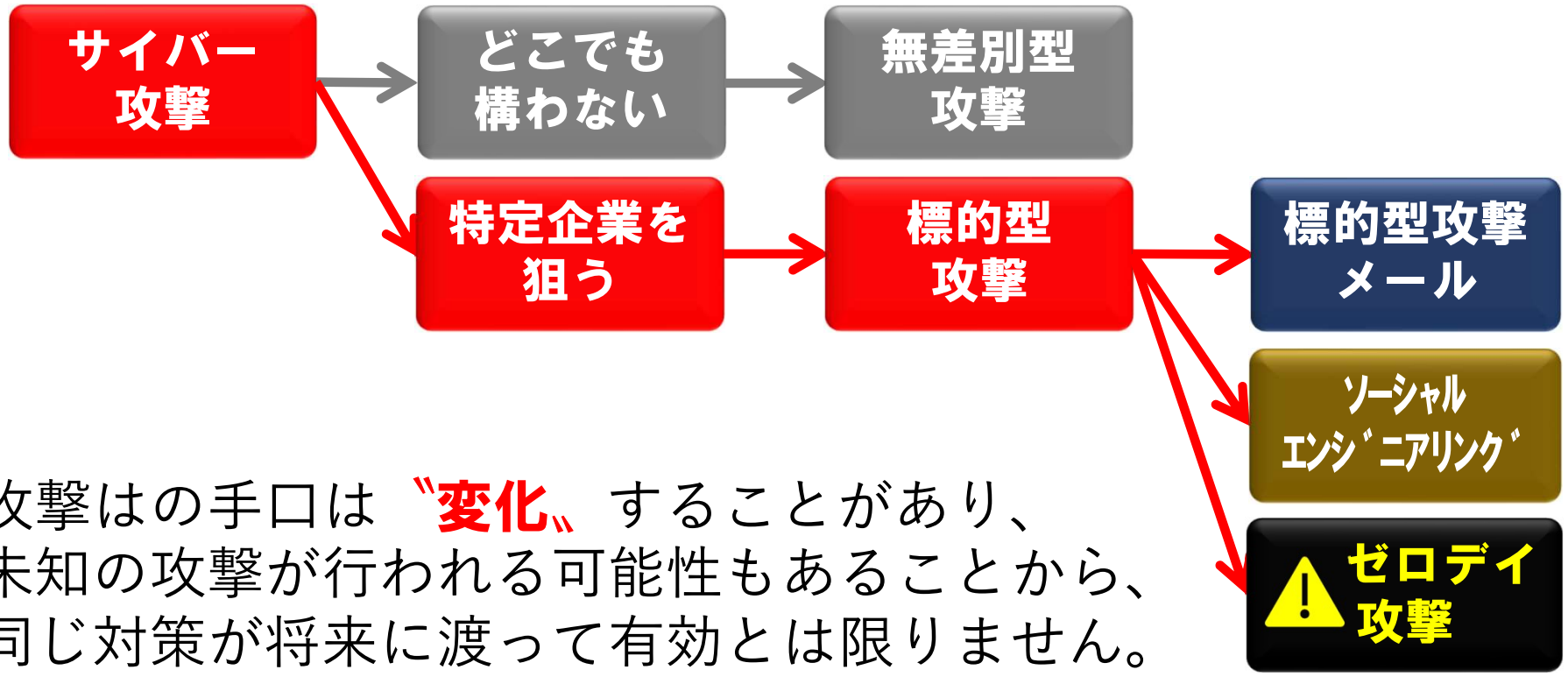
2021年「東北地域サイバーセキュリティセミナー」の時と比較

順位	2021年	2022年	2023年
1	ランサムウェアによる被害	ランサムウェアによる被害	ランサムウェアによる被害 連続1位
2	標的型攻撃による機密情報の窃取	標的型攻撃による機密情報の窃取	サプライチェーンの弱点を悪用した攻撃 ランクIN
3	テレワーク等のニューノーマルな働き方を狙った攻撃	サプライチェーンの弱点を悪用した攻撃	標的型攻撃による機密情報の窃取 上位維持
4	サプライチェーンの弱点を悪用した攻撃	テレワーク等のニューノーマルな働き方を狙った攻撃	内部不正による情報漏えい
5	ビジネスメール詐欺による金銭被害	内部不正による情報漏えい	テレワーク等のニューノーマルな働き方を狙った攻撃

出典：IPA 「情報セキュリティ10大脅威 2021・2022・2023」の組織における脅威（5位以内のみ）
https://www.ipa.go.jp/security/10threats/index.html

サイバーセキュリティのキーワード

『情報セキュリティ10大脅威』を見ると、直近3年間における上位の顔ぶれは似ています。ただし、**標的型攻撃** 1つをとっても…

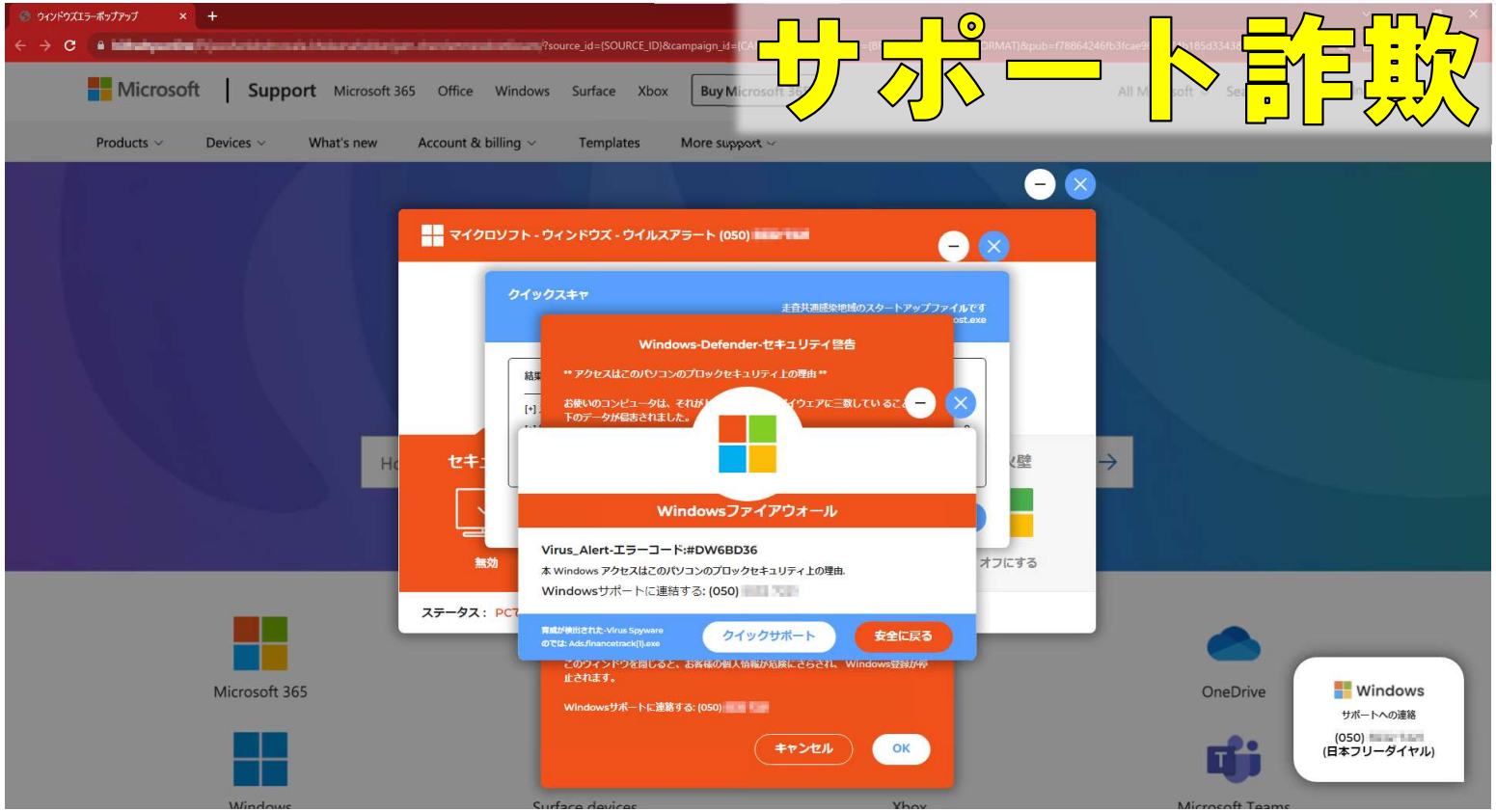


攻撃はの手口は〝**変化**〟することがあり、
未知の攻撃が行われる可能性もあることから、
同じ対策が将来に渡って有効とは限りません。

いま、起きていること
～セキュリティインシデント事例～

いま、起きていること

弊社セキュリティログ監視サービスにて、お客様の社内から不審な通信先IPアドレスへの通信を検知。お客様へご連絡をすると…



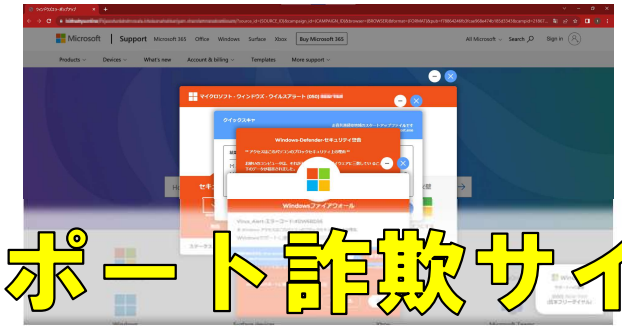
いま、起きていること

サポート詐欺のサイトは…

検索サイト

ブラウザ通知
許可要求サイト

ウイルス感染
偽メッセージ

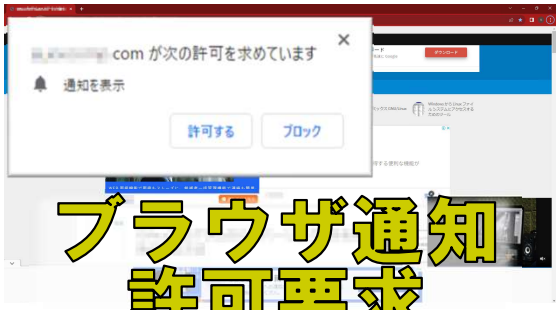


サポート詐欺サイト

- サポート詐欺サイトを開かせるために、複数の手口が存在。
- 中でも、**ウイルス感染の偽メッセージ**を出す手口が悪質。
- サポート詐欺サイトに表示された連絡先へ**電話したことにより、遠隔操作、情報窃取、ウイルス感染等の被害が発生**したというニュースも。

いま、起きていること

サポート詐欺を実例で取り上げた理由は…



ブラウザ通知
許可要求

ウイルス感染
偽メッセージ

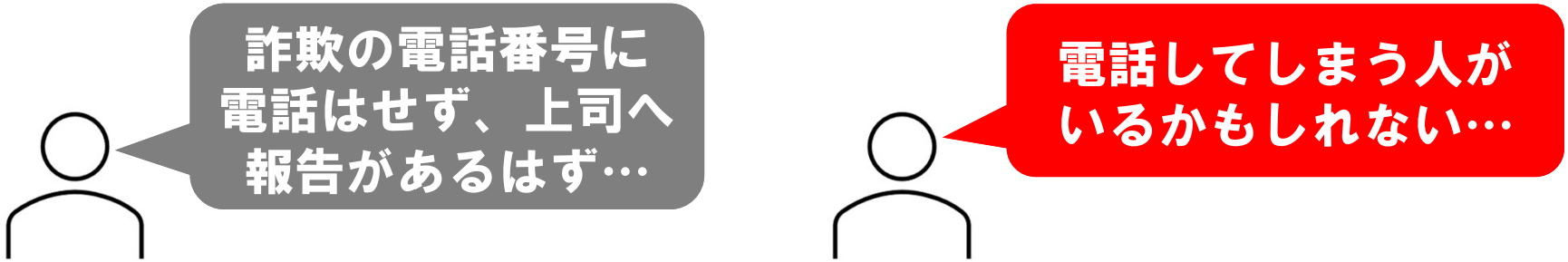
出典：IPA「ブラウザの通知機能から不審サイトに誘導する手口に注意」（公開日：2021年3月9日）
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210309.html

- **２年以上も前から**注意喚起されている手口。
- 偽メッセージの原因となるサイト自体は安全なサイトを装っており、URL**フィルタリングではブロックされない場合も**。

偽メッセージを通知するサイトにアクセスされてしまう事例が非常に多い

いま、起きていること

本日ご参加の皆様の企業内、組織内でサポート詐欺の画面を開いた方がいた場合、現状でどうなるか想定できますでしょうか。



例えば、次のような企業・組織で、**サポート詐欺（偽のウイルス感染メッセージ）**の画面を開いた方がいたらどうなるでしょうか。

- ウイルス対策は導入済みだが**管理機能がなく**、**ウイルス検出やスキャン実行の記録も残していない**ので、感染の有無を確認することが困難。
- 専任、兼任に関わらず、社内に**管理者となる社員がおらず**、サイバーセキュリティでトラブルがあった際の**相談先もわからない**。　　など

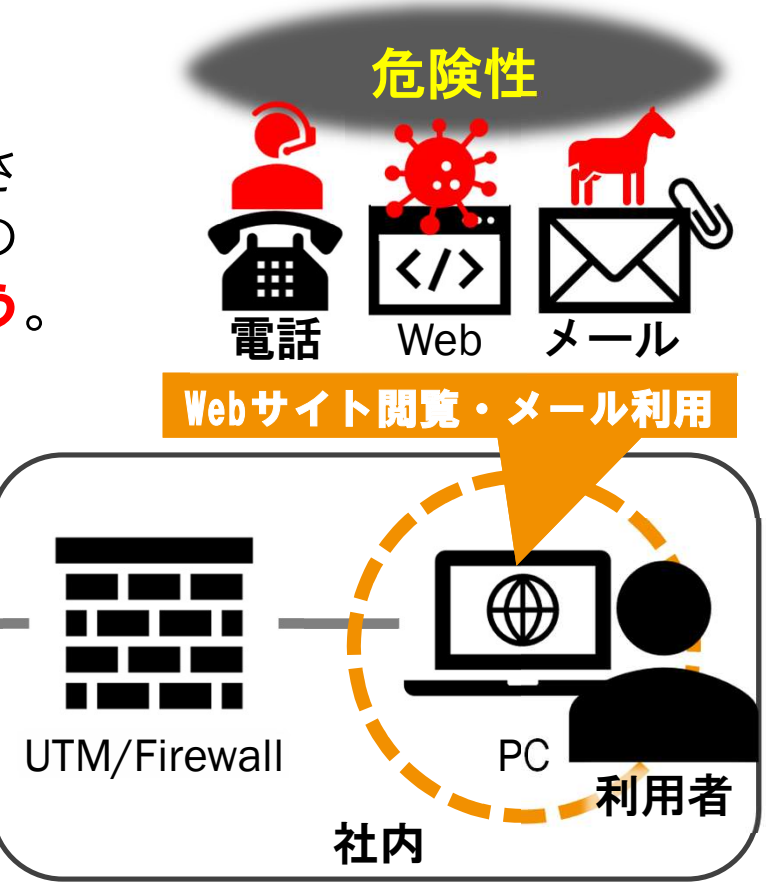
課題は何か

課題は何か

PC利用者がインシデントの引き金を引く可能性

- PC（エンドポイント）でのインシデント発生は、利用者の操作による所が大きい。
- ブロックされないWebアクセスや、駆除されない添付ファイル開封、サポート詐欺の電話等は、**利用者判断に委ねられてしまう**。
- 利用者の相談相手となる**管理者がいない中小企業ほどリスクが大きくなる**傾向も。

完全に防ぐことが難しいサイバー攻撃への対処をどうするか



課題は何か

完全に防ぐことが難しいサイバー攻撃（例）

サポート詐欺　ゼロデイ攻撃

- **サイバー攻撃の多様化・巧妙化**の影響は、中小企業にも及んでいます。
- サプライチェーン攻撃により、以前にも増して**中小企業が標的になりやすい**状況にあります。
- 残念ながら、「これさえあれば、どんな攻撃でも〝100%〟防げる」といった**完全なセキュリティ対策は、今の世の中には存在していません**。
- UTMやウイルス対策ソフトを導入して、後は「おまかせ」すればよい状況ではなく、企業や組織は刻々と**変化するサイバー攻撃の手口**にも対処していくことが求められています。

中小企業の
サイバーセキュリティ
強化策

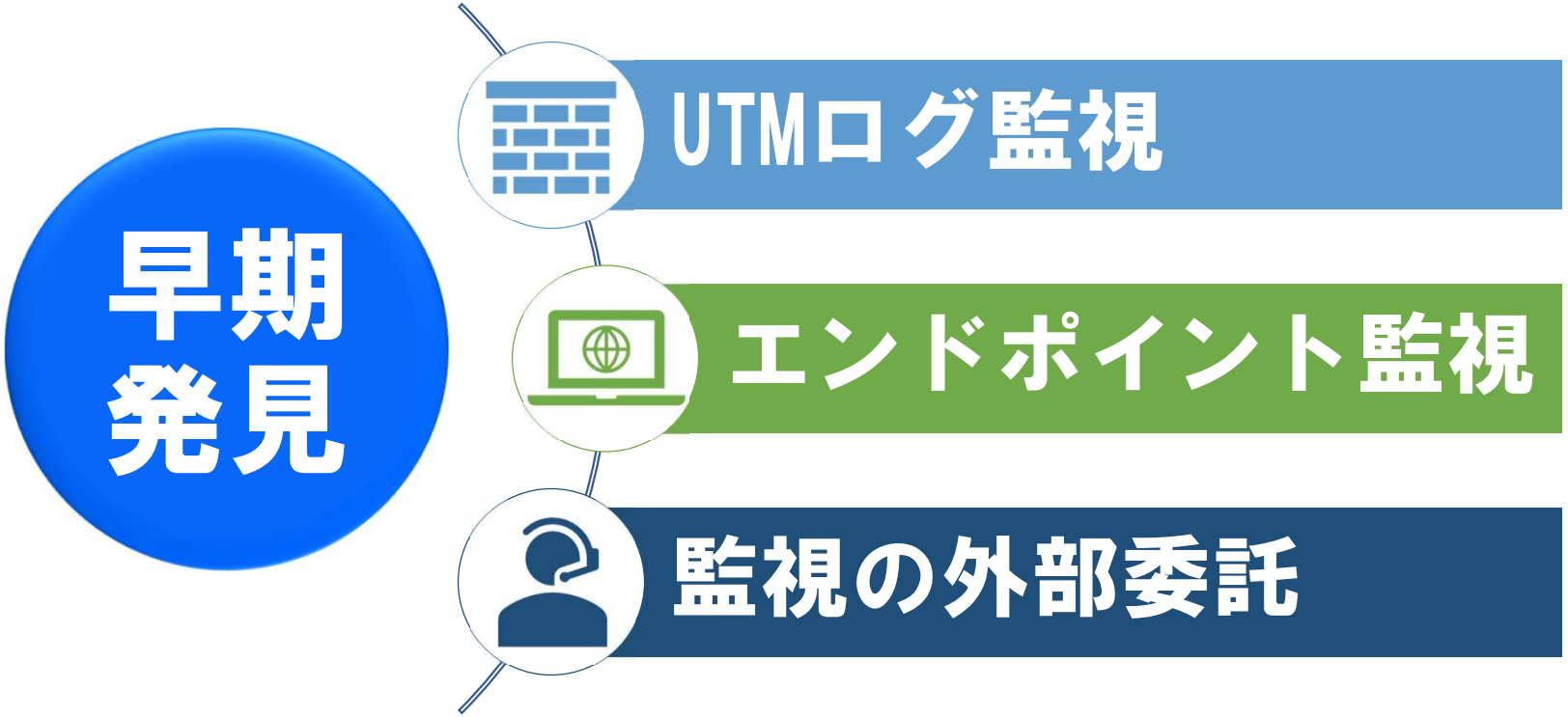
中小企業のサイバーセキュリティ強化策

結論、完全に防ぐことが難しいサイバー攻撃を念頭に置くと…

- 「攻撃をいかに防ぐか」ではなく「**攻撃が成功したらどうするか**」に軸足を移して対策を考える必要があります。
- 攻撃成功時の影響を最小限に留めるには、**早期発見が何よりも重要**です。

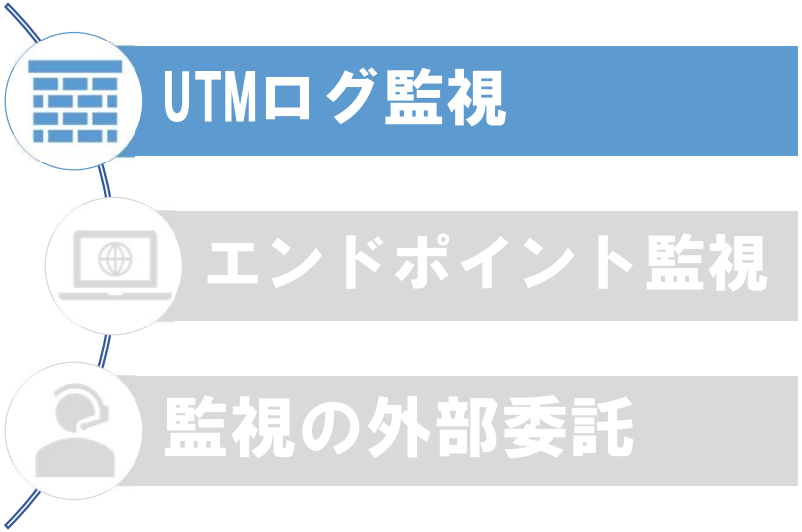
中小企業のサイバーセキュリティ強化策

中小企業が早期発見のために注力すべきと考えられるのは…



中小企業のサイバーセキュリティ強化策

インターネットの接続点となるUTMは監視が必須



- インターネット接続を伴うサイバー攻撃を、**実害が生じる前の予兆も含めて早期に発見**できる可能性あり。
- 弊社ログ監視サービス導入後、**導入前から発生していた可能性**がある、海外への不審な通信を検知し、お客様に連絡を行ったケースも。

目に見える実害がないだけで
既に問題が起きている可能性も

UTMログ監視で予兆も含めて発見

中小企業のサイバーセキュリティ強化策

利用者が操作するエンドポイントの管理・監視も必須

・ウイルスが駆除されていれば安心ということではなく、**駆除発生を把握できる仕組み**があるかどうかが重要。

・テレワーク含めて、PCがどこにあっても管理可能な**クラウド型の管理機能があるウイルス対策ソフトの導入**の必要性が中小企業においても高まっている。

利用者の操作や判断を完全にコントロールすることは不可能

エンドポイント監視でリスクを発見

中小企業のサイバーセキュリティ強化策

管理者の選任が難しい場合は、部分的にでも監視の外部委託を

- 早期発見には、各種監視が必要不可欠、誰かが**異常に気付ける仕組み**を。
- 限られた予算、人員で新しい対策を検討するより、**現行対策の利活用を優先**。
- SOCに業務委託することで、**セキュリティの相談窓口ができる**メリットも。

管理者不在により現行対策が活かし切れていない可能性も

監視の外部委託で早期発見を実現

中小企業のサイバーセキュリティ強化策

〝早期発見〟の重要性を示すものとして…

順位	2021年	2022年	2023年
1	ランサムウェアによる被害	ランサムウェアによる被害	ランサムウェアによる被害
2	標的型攻撃による機密情報の窃取	標的型攻撃による機密情報の窃取	サプライチェーンの弱点を悪用した攻撃
3	テレワーク等のニューノーマルな働き方を狙った攻撃	サプライチェーンの弱点を悪用した攻撃	標的型攻撃による機密情報の窃取
4	サプライチェーンの弱点を悪用した攻撃	テレワーク等のニューノーマルな働き方を狙った攻撃	内部不正による情報漏えい
5	ビジネスメール詐欺による金銭被害	内部不正による情報漏えい	テレワーク等のニューノーマルな働き方を狙った攻撃

出典：IPA 「情報セキュリティ10大脅威 2021・2022・2023」の組織における脅威（5位以内のみ）
https://www.ipa.go.jp/security/10threats/index.html

中小企業のサイバーセキュリティ強化策

内部不正も企業・組織にとって非常に大きな脅威

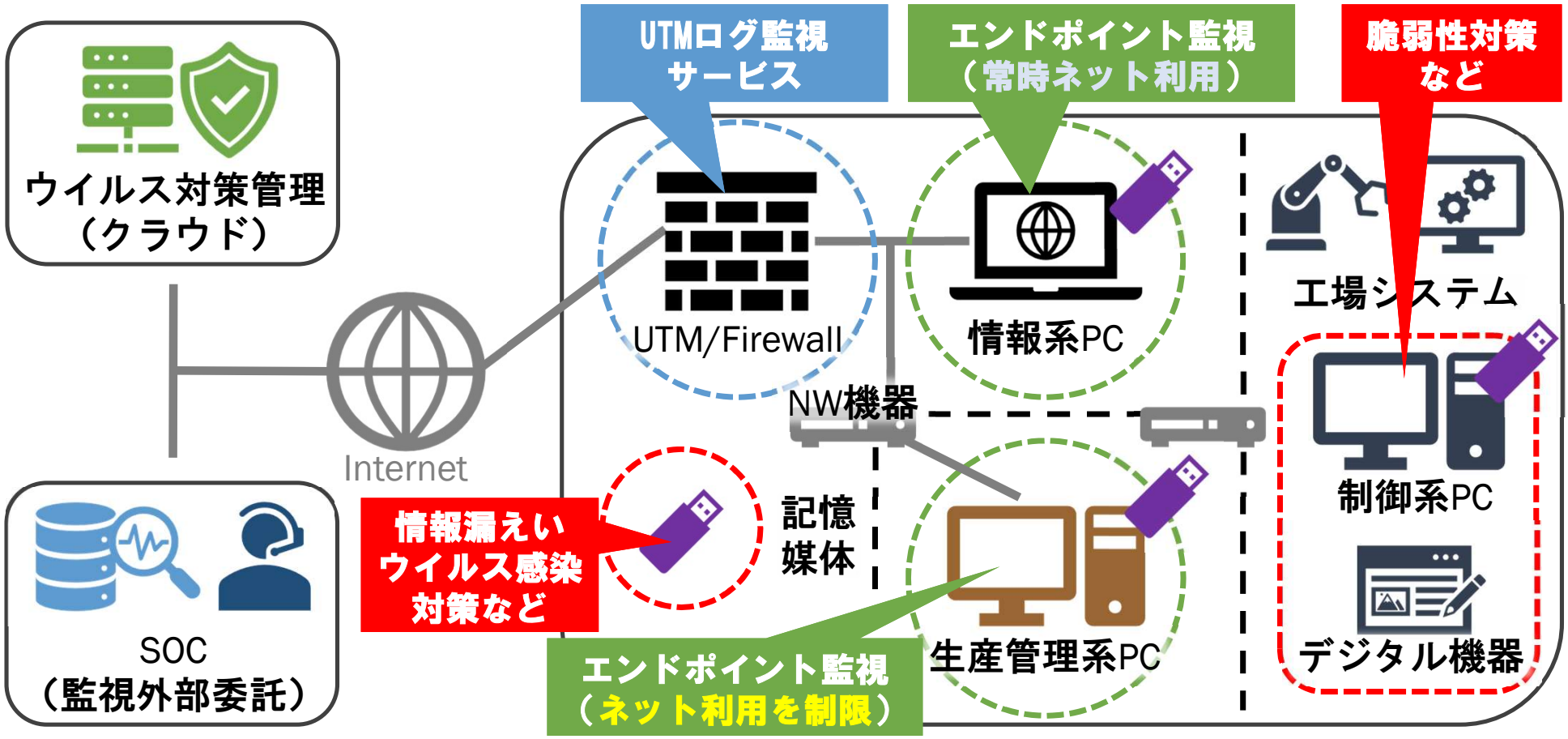
2023年10月　通信事業者（N社）の子会社において、元派遣社員が顧客情報900万件を不正に持ち出し、第三者に流出させていたとの報道

- 企業、組織は、外部からのサイバー攻撃だけでなく、**内部不正**にも目を光らせておく必要があります。
- 適切な権限管理や不正防止機能導入などの「事前策」も重要ですが、外部からのサイバー攻撃と同じく**「どんな不正でも〝100%〟防げる」という対策は存在しない**と考え、**不正された後で気付けるのかという視点で対策を考える**ことも重要と言えます。
- 不正も含めたインシデントが発生した際に、それを**早期発見できるようにすることの重要性**を示している直近の事例ではないでしょうか。

サイバーセキュリティ強化策の例

サイバーセキュリティ強化策の例

ご紹介した強化策を製造業に当てはめてみると…



サイバーセキュリティ強化策の例

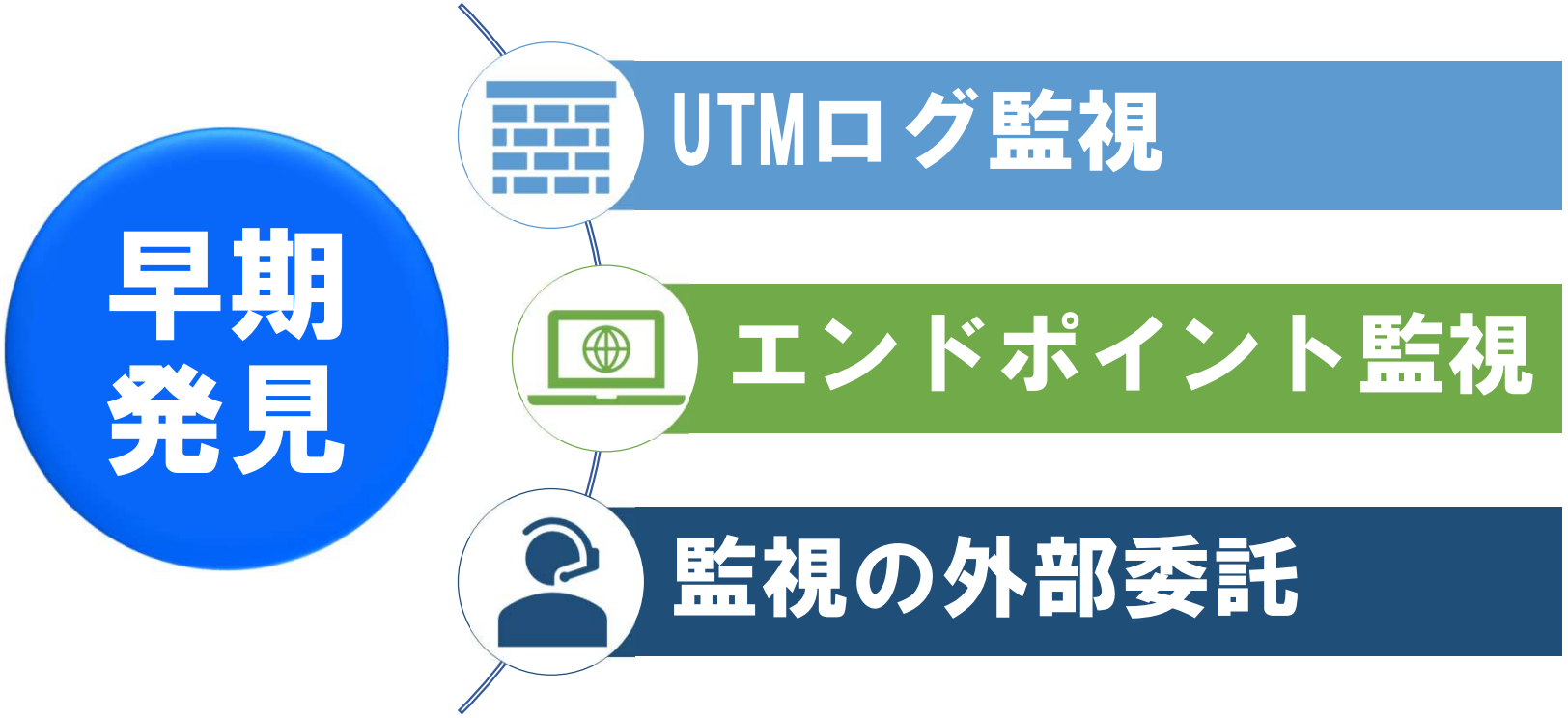
一般的なサイバーセキュリティ強化策（製造業の場合）

- **攻撃対象領域[アタックサーフェス]**になり得る部分を確認、インターネット接続やUSBメモリ等の記憶媒体を介して、外部ネットワークや外部端末と接点を持つ部分などに注意。 ➡ **攻撃侵入経路を明確に**
- 攻撃対象領域と接するPCやデジタル機器が攻撃を受けた場合、それぞれ何ができて、何ができなくなるかを確認。 ➡ **影響度と範囲を明確に**
- 攻撃者側は、より影響が大きくなる（被害が拡大しやすい）所を狙う可能性があるため、生産管理系や制御系のPCやデジタル機器が攻撃を受けた場合の対策や、早期発見の仕組み、影響を最小限に留める仕組みがあるかを確認。 ➡ **自社環境で必要とされる対策、優先すべき対策が何かを明確に**
- 工場含めて、社内の環境に変化（新しい端末の導入やシステムの入れ替え、バージョンアップなど）が生じた場合、上記の確認を改めて行う。 ➡ **PDCAでリスク低減を**

まとめ

まとめ

サイバー攻撃の発生にいち早く気付ける仕組みのご検討を



ハイテックシステム

【 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
TEL 080-4879-7319

【 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

2023年12月現在