



サイバーセキュリティ対策講演

ネット犯罪・情報漏えいの実態と対策方法について

株式会社高山

デジタル支援グループ

盛 柁貴



サイバーセキュリティチーム
リーダー

盛 柁貴

2014年入社

出身:富谷市

経歴:泉松陵高等学校
東北学院大学 工学部卒業

資格

国家試験(経済産業大臣認定)
情報セキュリティマネジメント取得
個人情報保護士
宮城県警委託講師
IPAセキュリティプレSENター制度登録



私たちが目指すビジョン

東北に
サイバーセキュリティのバリアを張る。

サイバー攻撃の被害数は 増加傾向に



トヨタ きょう国内全工場停止 取引先へのサイバー攻撃の可能性

2022年3月1日 11時29分

トヨタ自動車は、主要な取引先の部品メーカーでシステム障害があったため、1日、国内のすべての工場の稼働を停止します。
会社では、サイバー攻撃を受けた可能性があるとして原因を調査するとともに、早期の稼働再開を目指してシステムの復旧を急ぐことにしています。

トヨタ自動車



東映アニメーション 不正アクセスでアニメ4作品の放送に影響

2022年3月11日 17時01分 IT・ネット

数多くのテレビアニメなどを手がけている「東映アニメーション」は、社内ネットワークに不正アクセスを受けて制作システムの一部を停止したため、現在放送している「ONE PIECE」などのテレビアニメ4作品の放送スケジュールに、遅れなどの影響が出ると発表しました。

東映アニメーションによりますと、今月6日に社内ネットワークへの不正アクセスが確認され、現在作品の制作などに関わるシステムの一部を停止しているということです。

東映アニメーション



デンソーに身代金要求型のサイバー攻撃が犯罪グループが声明

2022年3月13日 20時46分 サイバー攻撃

身代金要求型のコンピューターウイルスによるサイバー攻撃を行う犯罪グループが、トヨタグループの大手自動車部品メーカー「デンソー」の機密情報を盗み、公開すると、ネット上のウェブサイトで声明を出したことがわかりました。
デンソーは「ドイツにある拠点でネットワークへの不正アクセスを確認し、調査している」としています。

デンソー



セキュリティ対策はサイバー攻撃が来る前提で
経営者自らが率先して取り組むべき課題と
なってきています！

情報漏えい

どんなに対策をしても
感染リスクは残る

情報資産を守るために

インターネットを通じた 被害事例

▶ サプライチェーン攻撃



遠隔操作
情報搾取
本人になりすます

サイバーセキュリティは
「自社だけ」の問題ではない

知らぬ間に自由に遠隔操作されていることもあります。
感染後、「被害者」になるだけでなく、
遠隔で操作され「加害者」になりえます。

遠隔操作ウィルス・PC乗っ取り

■自分のメールアドレスを使用され、ウィルス付のメールを勝手に送信！

■被害企業

幼稚園

■事例概要

・幼稚園の園長先生にある日役所から電話が来ました
「**そちらからウィルス付のメールが大量に送られて来ているんだがどうゆうことだ！**」

確認してみると身に覚えのないメールを大量に送っていたのです。弊社の方でPCを調べたところ、ウィルスに感染していて**乗っ取られていた**のが分かったのです。

遠隔操作のウィルスは、パソコンに侵入しパソコン所有者が気付かないところで、**情報を盗んだり、不正な命令をしたりといった悪事を働くことが可能**となります。いわゆる、乗っ取られた状態となるのです。

■被害状況

- ・外部に対しての攻撃に利用され、被害者だけでなく加害者になってしまった。
- ・信用を大きく傷つけてしまった。
- ・パソコン内の情報が外部に漏えいしていた可能性有

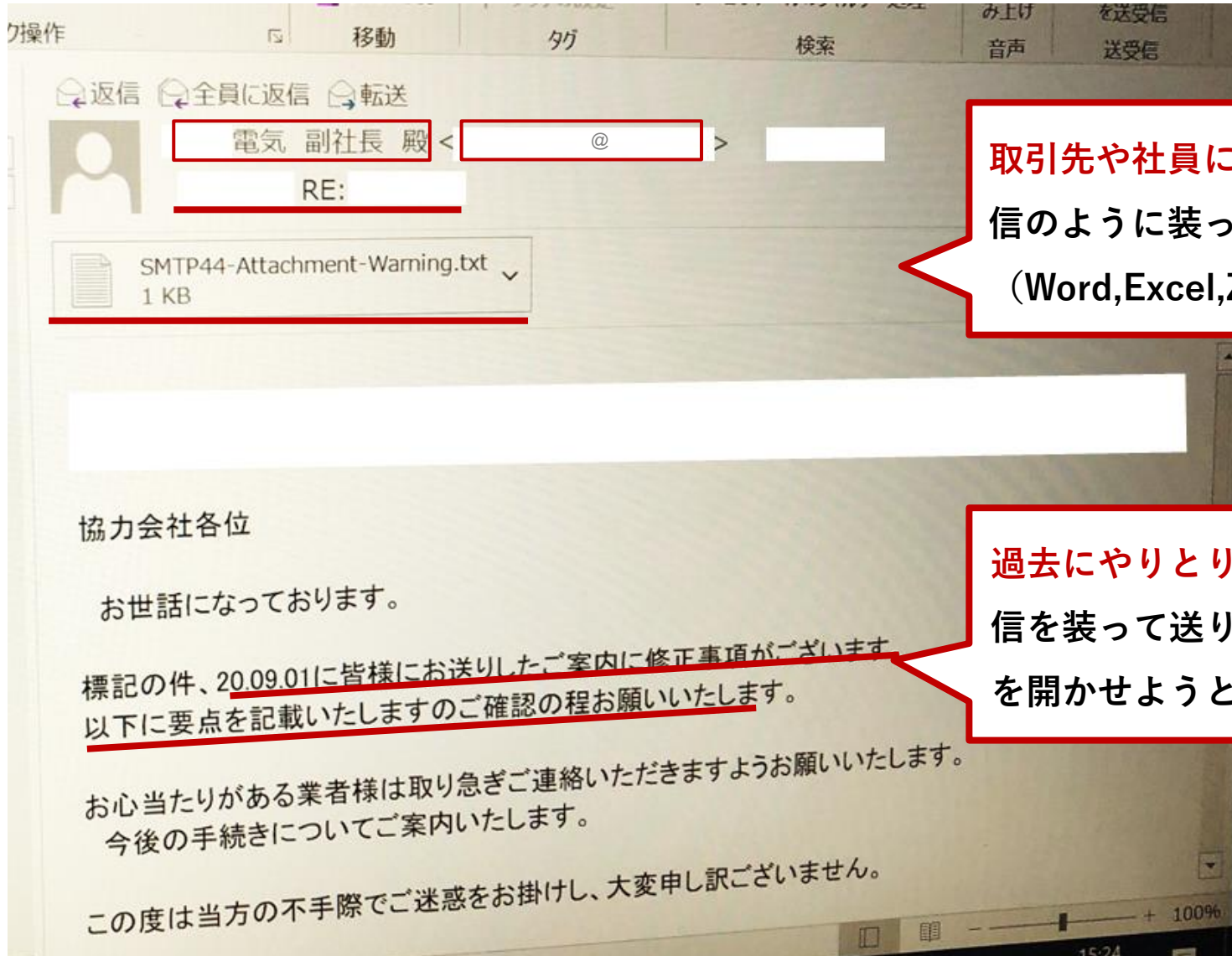


▲個人情報簡単に盗まれてしまう



**自分が知らない間に外部への攻撃に利用されることも…
最悪の場合、取引停止や訴訟問題にもなりえます。**

▶ なりすましメール（Emotetウイルス）

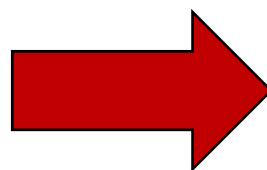
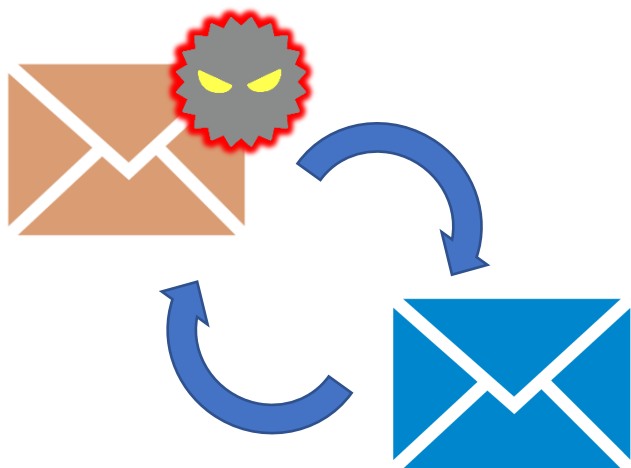


取引先や社員になりすまし、返信のように装っている
(Word, Excel, Zipファイル)

過去にやりとりしたメールの返信を装って送り、添付ファイルを開かせようとする

感染しないための工夫を進めていこう！

脱メール



LINE WORKS

Chatwork

Microsoft Teams

コミュニケーションをチャットツールで行う

ランサムウェアの脅威増加

▼社内のデータが暗号化

企業経営に関することなら、どんな事業でもお気軽にご相談ください。

☎022-222-1310

受付
8:30



サイト内検索

ホーム

支援メニュー

機構案内

アクセス

不正アクセス被害について

宮城県産業復興相談センター、宮城県中小企業活性化協議会及び宮城県事業承継・引継ぎ支援センター並びに機構復旧いたしました。

なお、メールの送受信は一部のパソコンに限られるためご不便をおかけいたしますが引き続きよろしくお願いたします。

11月22日（火）9:00から下記メールアドレスが復旧いたしました。

- 総務企画課
 - soumu@joho-miyagi.or.jp
 - digital@joho-miyagi.or.jp
- 事業支援課
 - soudan@joho-miyagi.or.jp
 - navi@joho-miyagi.or.jp



サイバー攻撃で診療行えず、手術も停止 大阪急性期・総合医療センター

2022/10/31 23:23

社会 | 事件・疑惑 ライフ | からだ 地方 | 近畿 大阪 | 産経WEST | できごと



記者会見する大阪急性期・総合医療センターの嶋津岳士総長（左）ら＝31日、大阪市住吉区

大阪急性期・総合医療センター（大阪市住吉区）は31日、電子カルテのシステム障害が発生し、診療を停止したと発表した。サイバー攻撃が原因とみられる。紙のカルテで入院患者に対応しているが、過去の記録がないため緊急時を除き手術も停止した。患者約600～千人に影響があったとみられ、復旧の見通しは立っていない。

同センターは昭和30年に府立病院として開設。病床数は865床で、救命救急のほか、がんや腎移植など高度専門医療も行う。災害時に24時間対応する基幹災害医療センターにも指定されている。

同センターによると、31日午前6時40分ごろ、職員がシステムの異常に気付いた。連絡を受けたシステムの管理会社が午前8時半ごろに確認したところ、サーバー上に英語

<https://www.sankei.com/article/20221031-NXP5LNNWSNP2RG5HCAO6LZP7KA/>

ランサムウェア 通称:身代金ウィルス

■ファイルを暗号化され、パソコンのデータが使えなくなった

- 被害企業
 - 設備業
 - 建設業
 - 介護福祉業
- 事例概要

ある日突然データが「このファイルは開けません」と表示され、データが全て閲覧不能になってしまった。

バックアップを取っていたデータも暗号化されてしまい、最終的に身代金を要求された。現場は大パニックで弊社が駆け付けたがもう感染が進行してしまい、手が出せない状態だった。

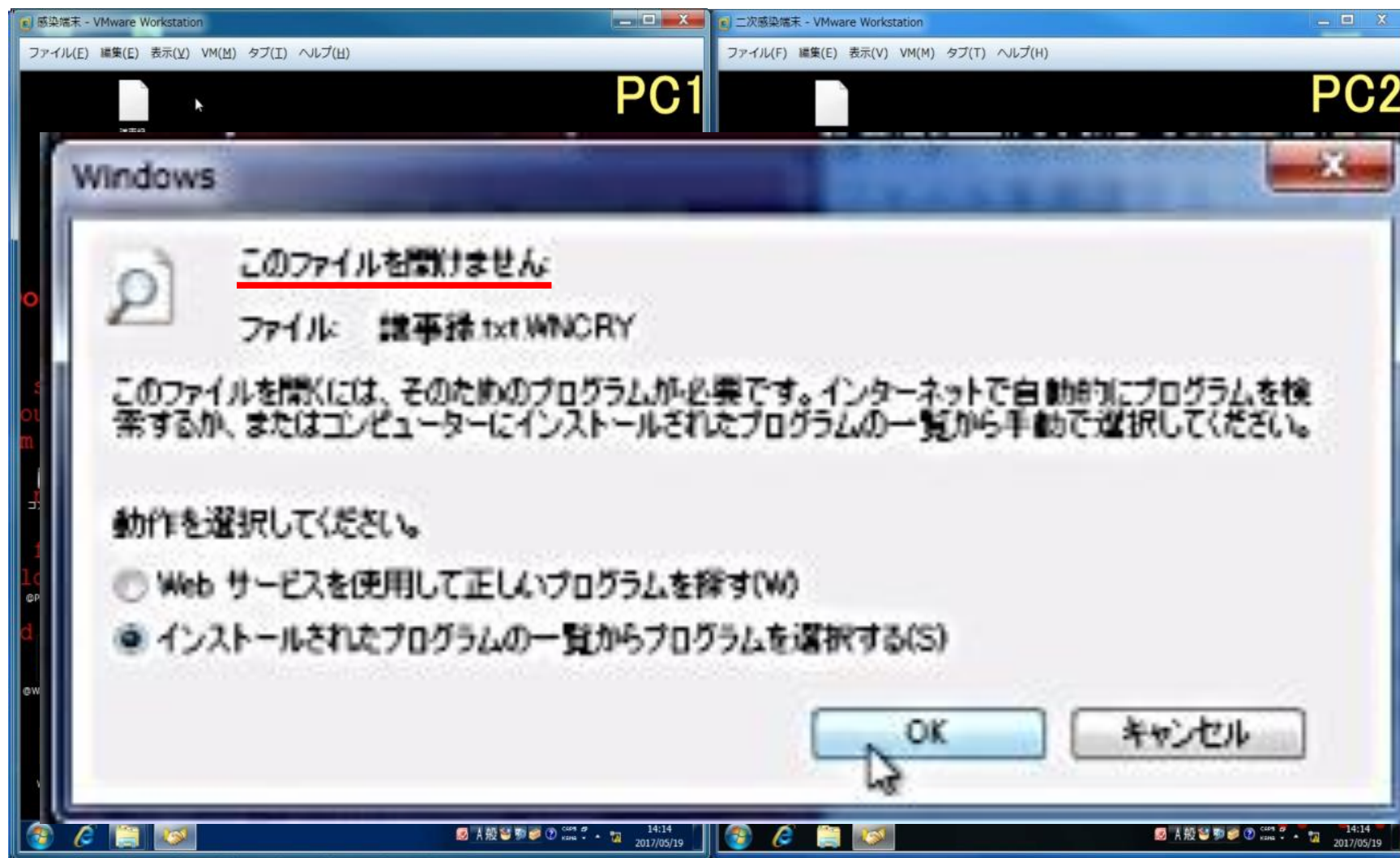
復元を業者に頼むとPC1台50万～80万、そして復旧まで1～2か月を要します。中には深刻で復旧できないPCも存在します。

■被害状況

- ・データの損失
- ・データが使用不能による業務停止
- ・復旧に高額な費用が掛かった

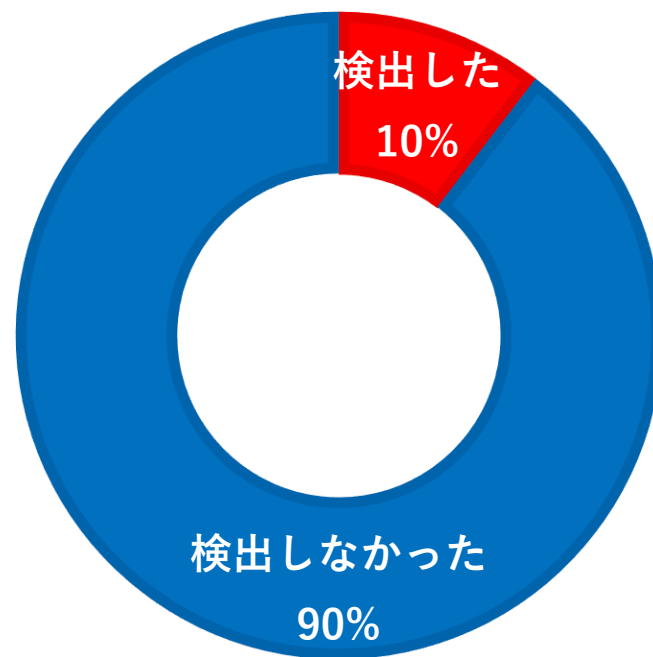
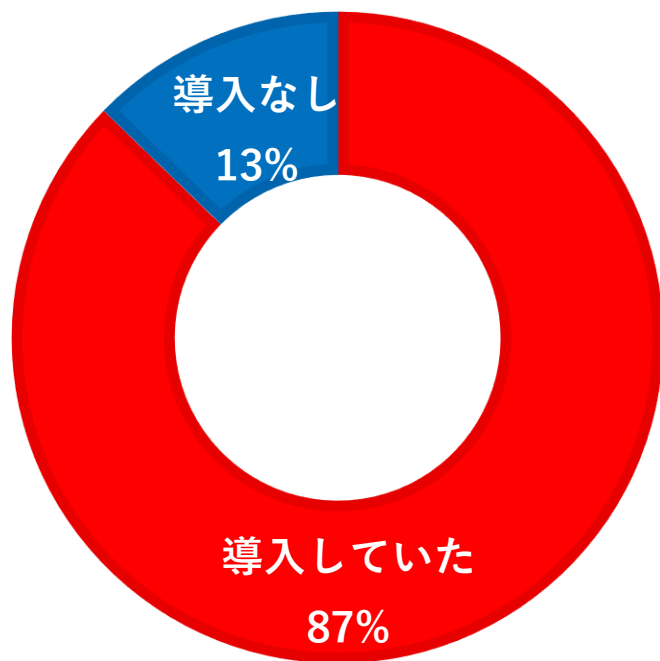


ランサムウェア攻撃は今後益々増加する傾向にあります
1台感染すると、瞬時に他端末に被害拡散する恐れがあります・・・



ランサムウェアの脅威増加

- セキュリティソフトを導入していても検出ができない被害企業がほとんど
- これまでのウイルス対策ではランサムウェアを検出できない



警察庁『令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について』より

瞬時に同一NW端末に被害拡散の恐れ

感染した際にはパソコンを隔離

バックアップで復旧していく



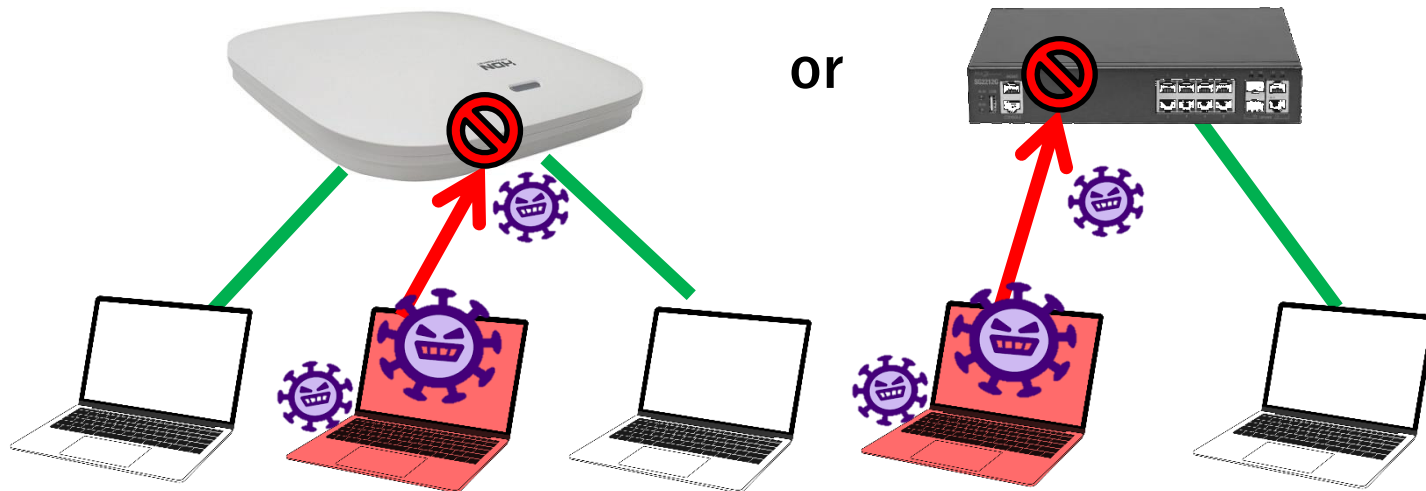
ウィルスの押さえ込み

▼セキュリティハブ・AP

ウィルスに感染しても社内拡散を防止し
企業内クラスターを防ぐ



被害を最小限に
抑えられえる



▶ クイズ

Aさんは、会社で新しく利用するクラウドサービスのアカウントを登録作業中です。IT部門からパスワードは各自設定し利用を開始するよう言われました。

次のうち一番解読されにくいパスワードはどれでしょうか？

A **493819485739205334**

B **TkymFCsAsgiG**

C **aR#23dcb**



ハッカーが2022年にパスワードを 総当たり攻撃して解読にかかる時間

文字数	数字のみ	小文字と数字	大文字と小文字	数字、大文字 小文字	数字、大文字 小文字、記号
4文字	瞬時	瞬時	瞬時	瞬時	瞬時
5文字	瞬時	瞬時	瞬時	瞬時	瞬時
6文字	瞬時	瞬時	瞬時	瞬時	瞬時
7文字	瞬時	瞬時	2秒	7秒	31秒
8文字	瞬時	瞬時	2分	7分	39分
9文字	瞬時	10秒	1時間	7時間	2日
10文字	瞬時	4分	3日	3週間	5ヶ月
11文字	瞬時	2時間	5ヶ月	3年	34年
12文字	2秒	2日	24年	200年	3000年
13文字	19秒	2ヶ月	1000年	12000年	202000年
14文字	3分	4年	64000年	750000年	1600万年

パスワードは極力使い回ししない
数字・英大小文字・記号11~14文字以上が理想
多要素認証を導入することも効果的です

今日からできる！

—— 具体的な対策 ——





サイバーセキュリティ経営ガイドライン
Ver 2.0

経済産業省
独立行政法人 情報処理推進機構

セキュリティ向上のための

5つの観点

特定

防御

検知

対応

復旧

セキュリティ向上のための

5つの観点

「100%守れる状態はない」

侵入してきても被害を最小限に抑える

通常業務に戻れる体制づくり

情報セキュリティのレベルアップ

「多層防御」

次世代ファイヤーウォール (UTM)

ウイルス対策ソフト

持出端末の防御

セキュリティハブ

ログ管理ソフト

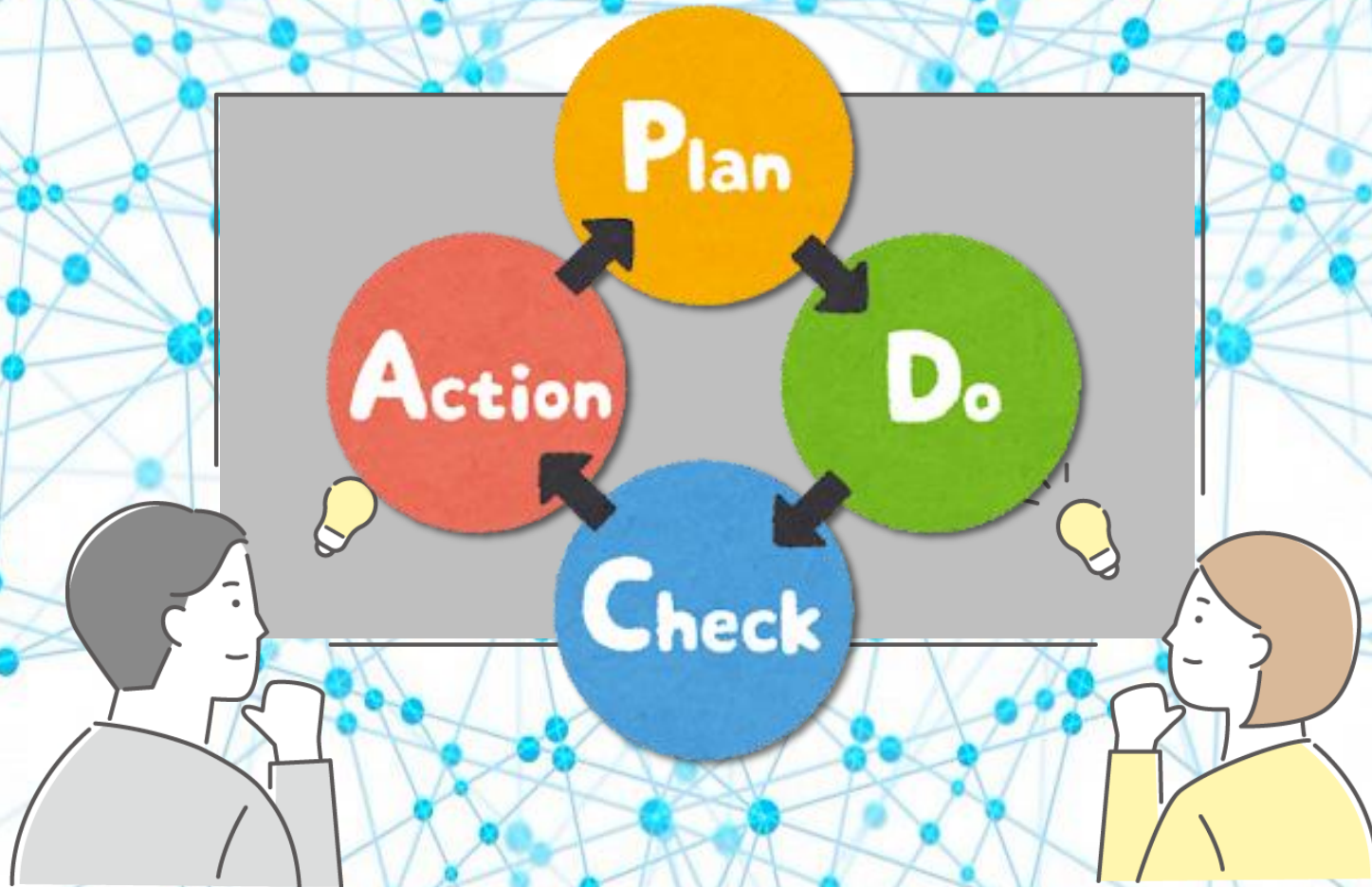
バックアップ




対策機器・ソフトウェア
+
ルール作り・社員教育

現状を
「知ること」
が大事です







自社に
サイバーセキュリティのバリアを張る。



▶セキュリティ無料相談&診断

自社のネットワーク環境を知れる、
サイバーセキュリティ特化型相談！



▶サイバーセキュリティ 講演・勉強会

宮城県警察本部委託事業「サイバーセキュリティ講演」をオンライン・リアルで開催！

