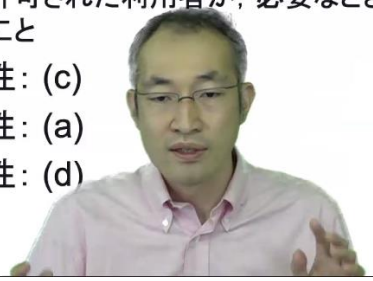
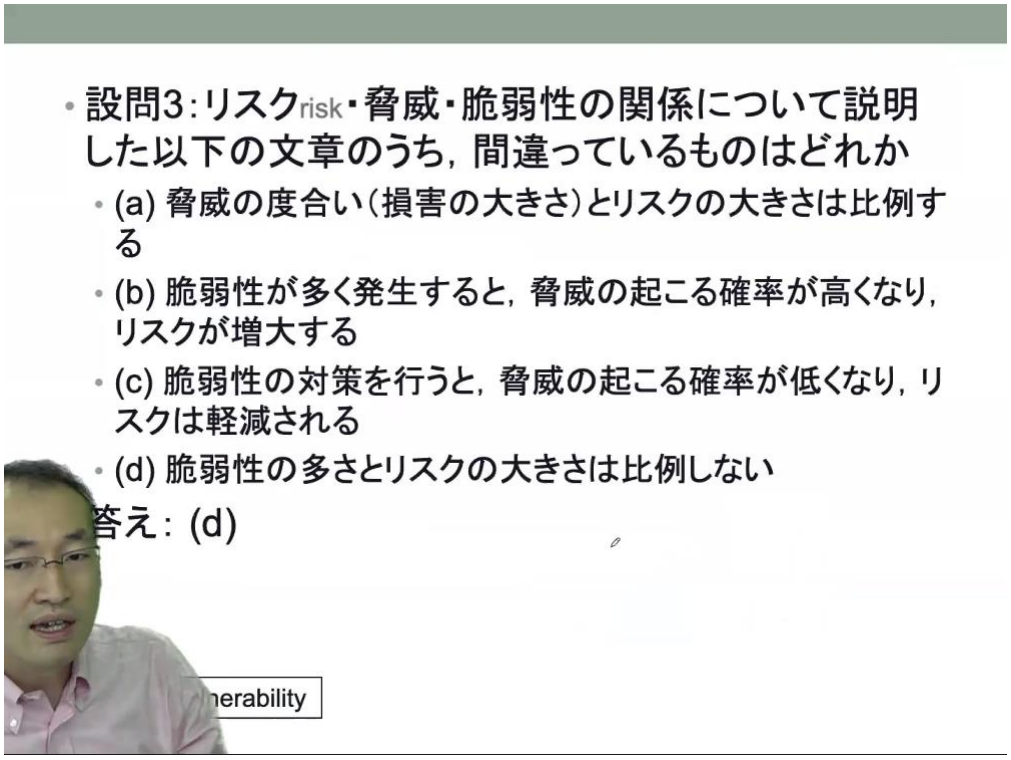
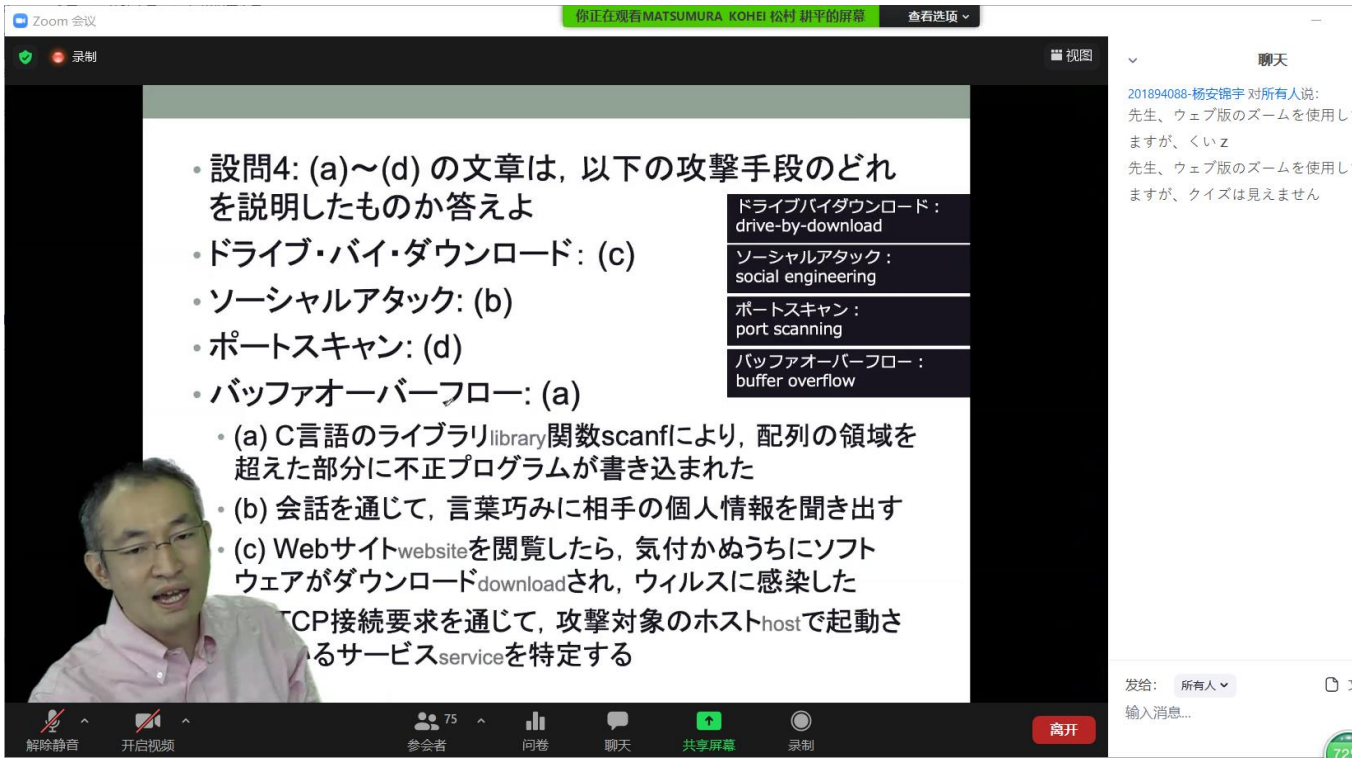
- 設問1：機密性，完全性，可用性について，それぞれ正しく説明している文章を以下から選べ
  - (a) 情報が改ざんされていないことを保証すること
  - (b) 情報にアクセスaccessするプログラムprogramにバグbugが無いことを保証すること
  - (c) アクセスを認可された者だけが情報にアクセスできることを確実にすること
  - (d) 許可された利用者が，必要なときに，情報にアクセスできること
- 機密性：(c)
- 完全性：(a)
- 可用性：(d)

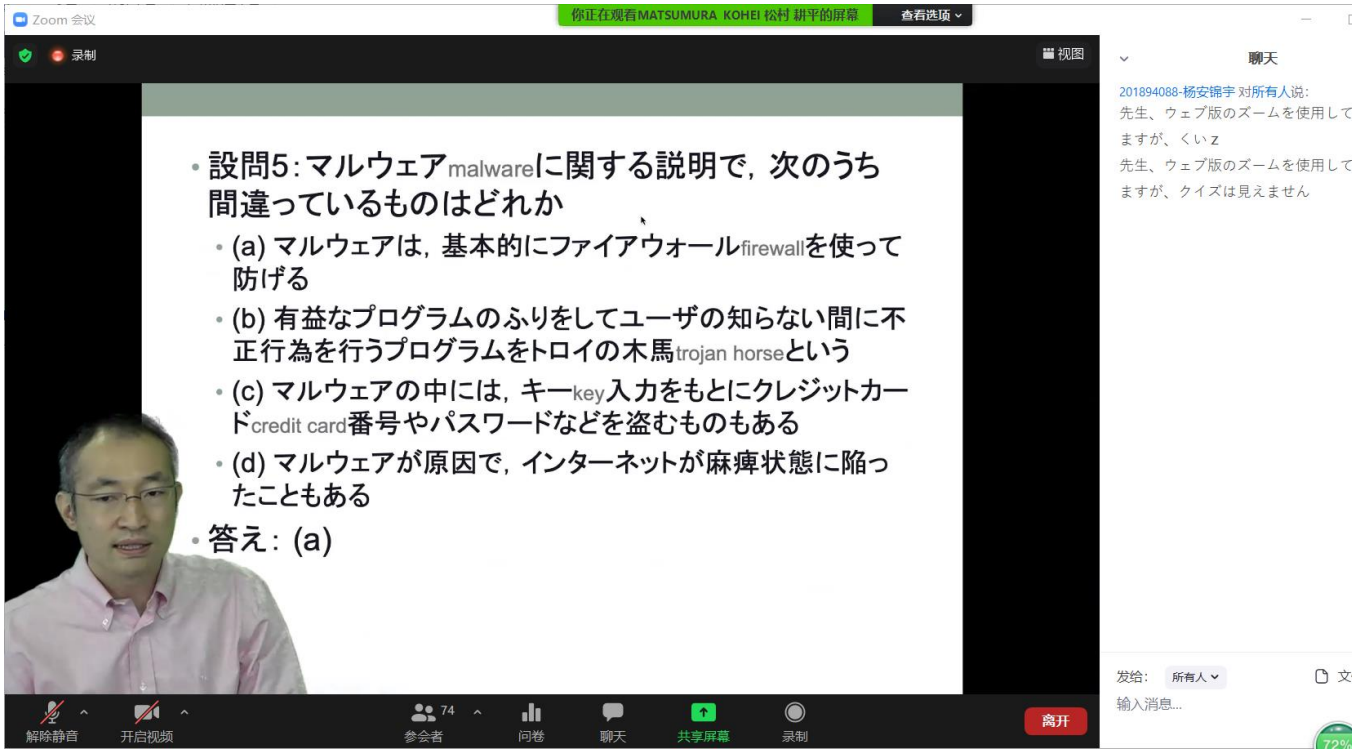


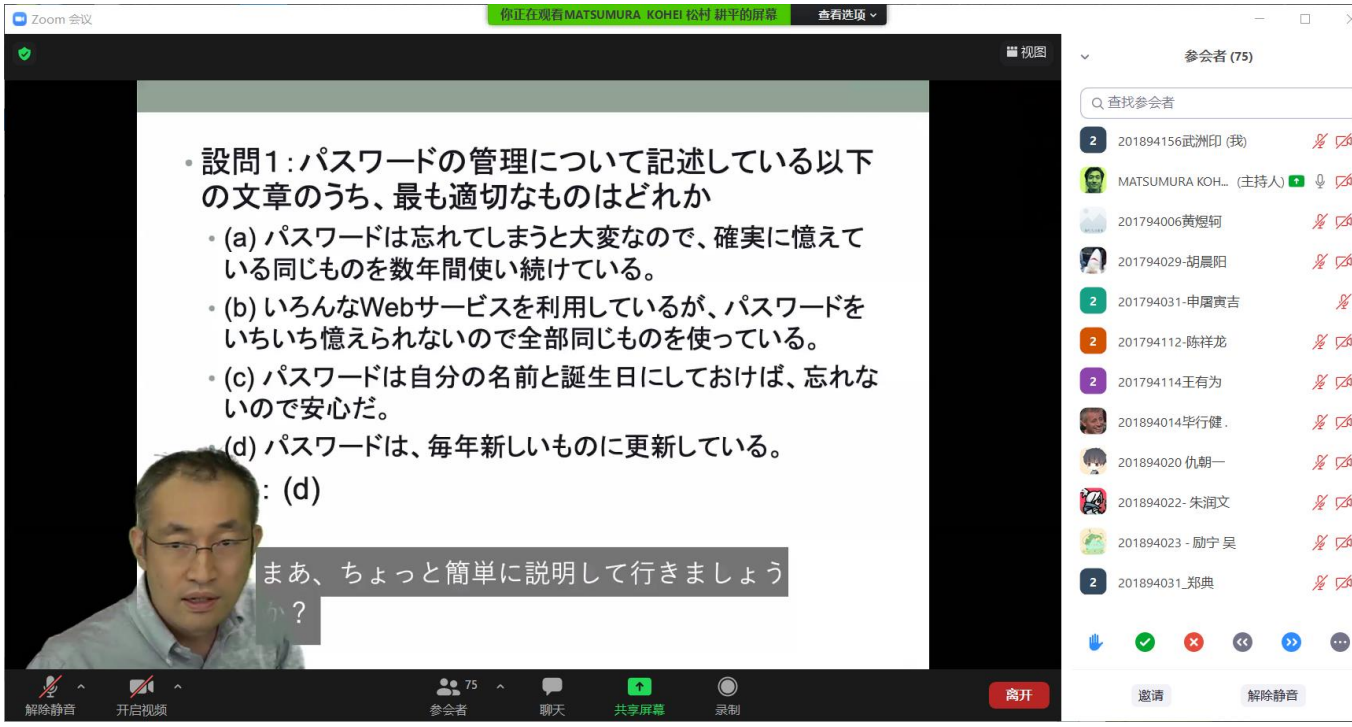
= “ ”

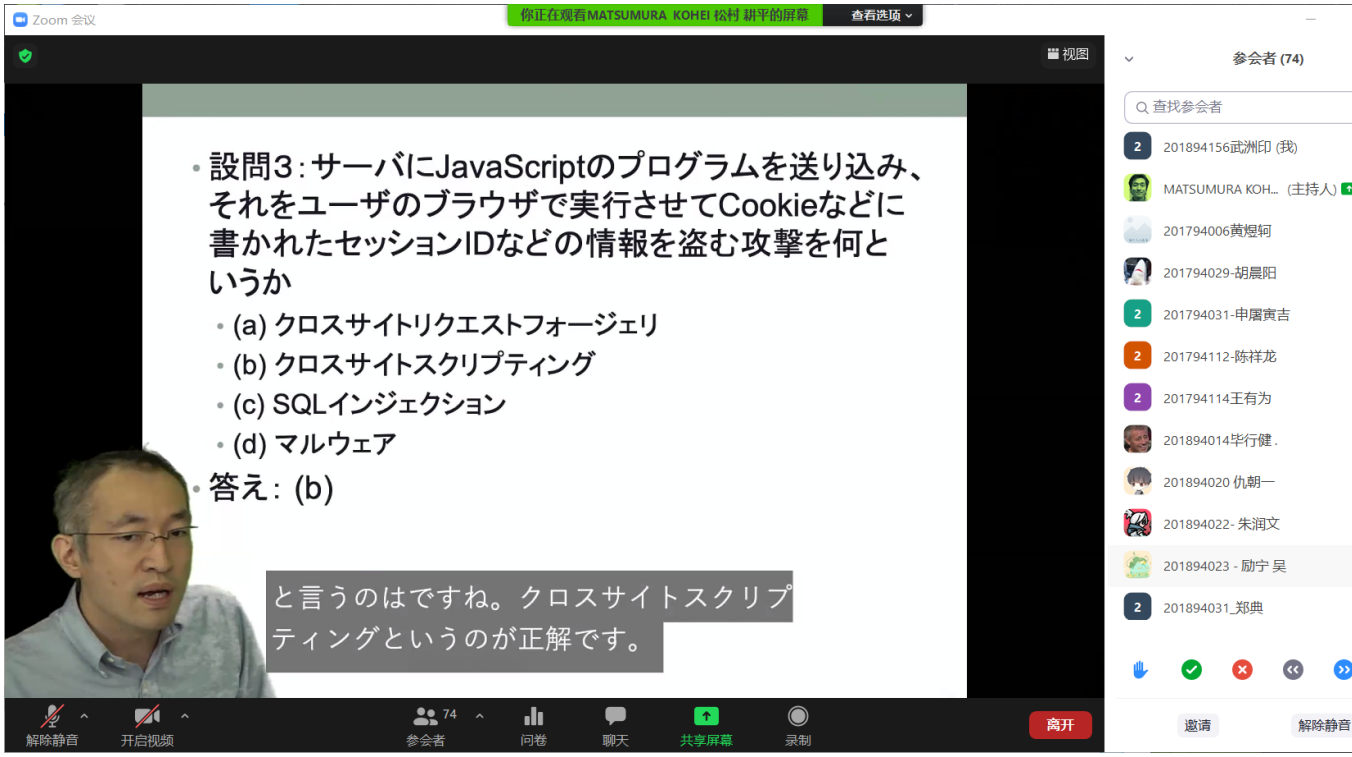
- 設問2：コンピュータcomputerに対する攻撃方法として，直接的攻撃に分類されないものは次のうちどれか
  - (a) 総当たり法でパスワードpasswordを解析し，他人になりすまして不正にログインloginした
  - (b) コンピュータウィルスcomputer virusをメールmailに添付して，不正な動作をするプログラムprogramを送りつけた
  - (c) 大量のパケットpacketを送りつけて，サービスserviceの正当な利用を妨害した
  - (d) セキュリティホールsecurity holeを利用して，遠隔地にあるコンピュータcomputerを不正に使用した
- え：(b)

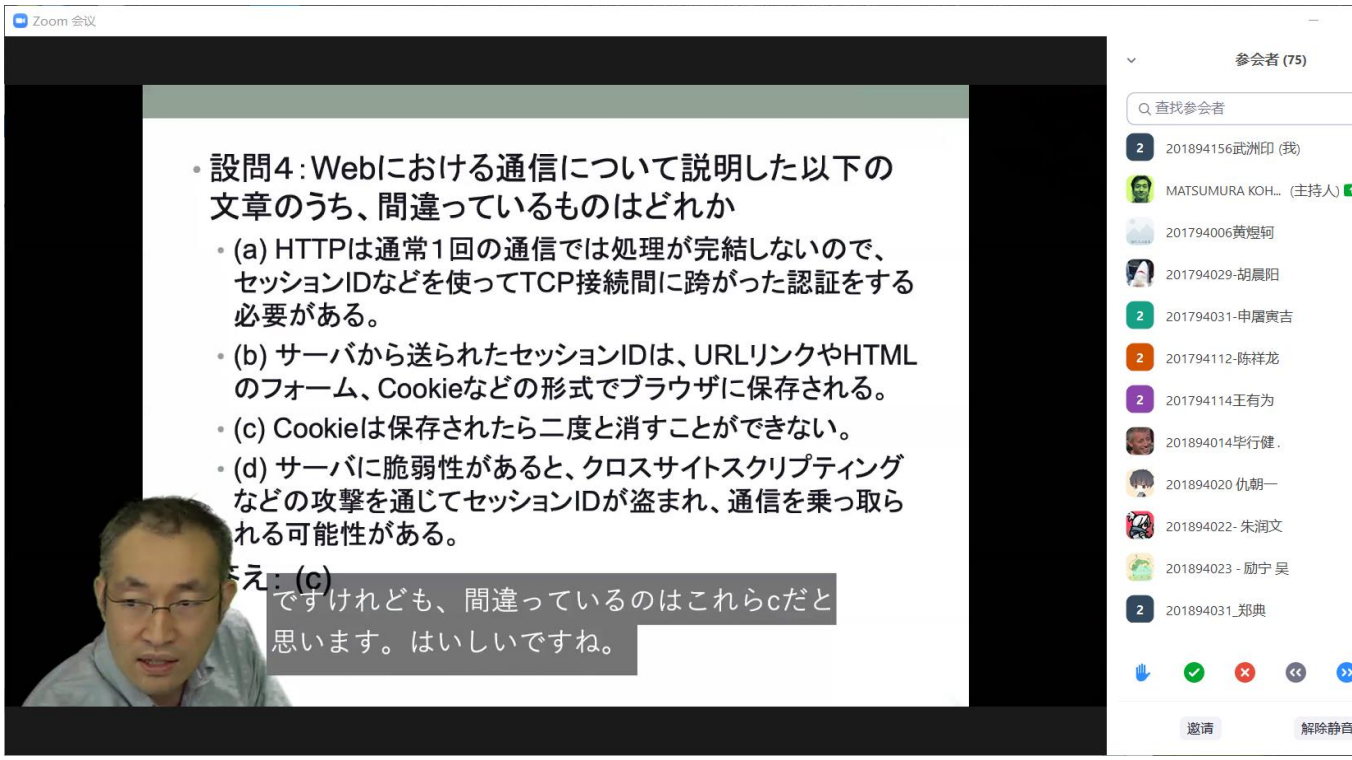

• 設問3：リスクrisk・脅威・脆弱性の関係について説明した以下の文章のうち，間違っているものはどれか
• (a) 脅威の度合い（損害の大きさ）とリスクの大きさは比例する
• (b) 脆弱性が多く発生すると，脅威の起こる確率が高くなり，リスクが増大する
• (c) 脆弱性の対策を行うと，脅威の起こる確率が低くなり，リスクは軽減される
• (d) 脆弱性の多さとリスクの大きさは比例しない
答え：(d)
nerability

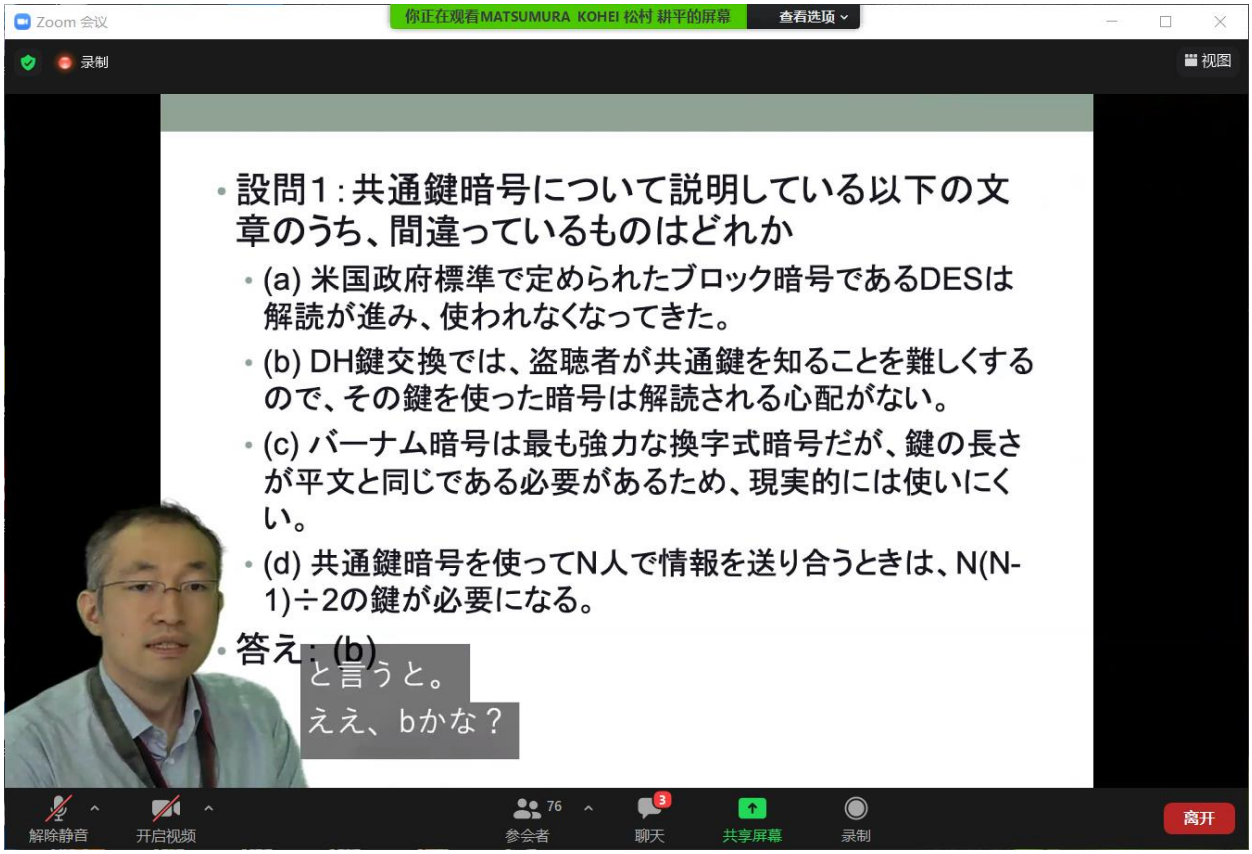

Zoom 会议
你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
• 設問4: (a)〜(d) の文章は，以下の攻撃手段のどれを説明したものか答えよ
• ドライブ・バイ・ダウンロード: (c)
• ソーシャルアタック: (b)
• ポートスキャン: (d)
• バッファオーバーフロー: (a)
• (a) C言語のライブラリlibrary関数scanfにより，配列の領域を超えた部分に不正プログラムが書き込まれた
• (b) 会話を通じて，言葉巧みに相手の個人情報を聞き出す
• (c) Webサイトwebsiteを閲覧したら，気付かぬうちにソフトウェアがダウンロードdownloadされ，ウィルスに感染した
CP接続要求を通じて，攻撃対象のホストhostで起動さるサービスserviceを特定する
ドライブバイダウンロード：drive-by-download
ソーシャルアタック：social engineering
ポートスキャン：port scanning
バッファオーバーフロー：buffer overflow
解除静音
开启视频
75
参会者
问卷
聊天
共享屏幕
录制
离开
聊天
201894088-杨安锦宇 对所有人说：
先生、ウェブ版のズームを使用しますが、くいｚ
先生、ウェブ版のズームを使用しますが、クイズは見えません
发给：
所有人
输入消息...

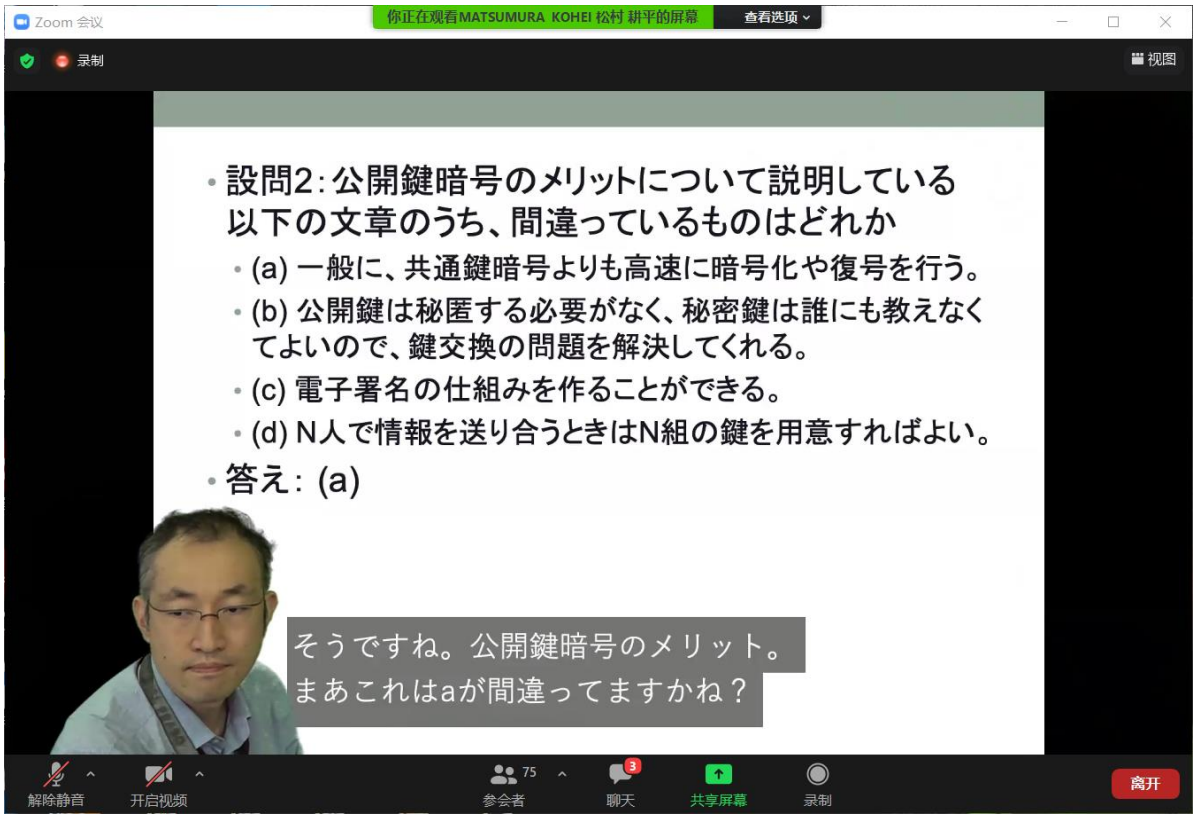

Zoom 会议
你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
聊天
201894088-杨安锦宇 对所有人说:
先生、ウェブ版のズームを使用してますが、くいz
先生、ウェブ版のズームを使用してますが、クイズは見えません
• 設問5：マルウェアmalwareに関する説明で，次のうち間違っているものはどれか
• (a) マルウェアは，基本的にファイアウォールfirewallを使って防げる
• (b) 有益なプログラムのふりをしてユーザの知らない間に不正行為を行うプログラムをトロイの木馬trojan horseという
• (c) マルウェアの中には，キーkey入力をもとにクレジットカードcredit card番号やパスワードなどを盗むものもある
• (d) マルウェアが原因で，インターネットが麻痺状態に陥ったこともある
• 答え：(a)
发给: 所有人
输入消息...
解除静音
开启视频
74
参会者
问卷
聊天
共享屏幕
录制
离开

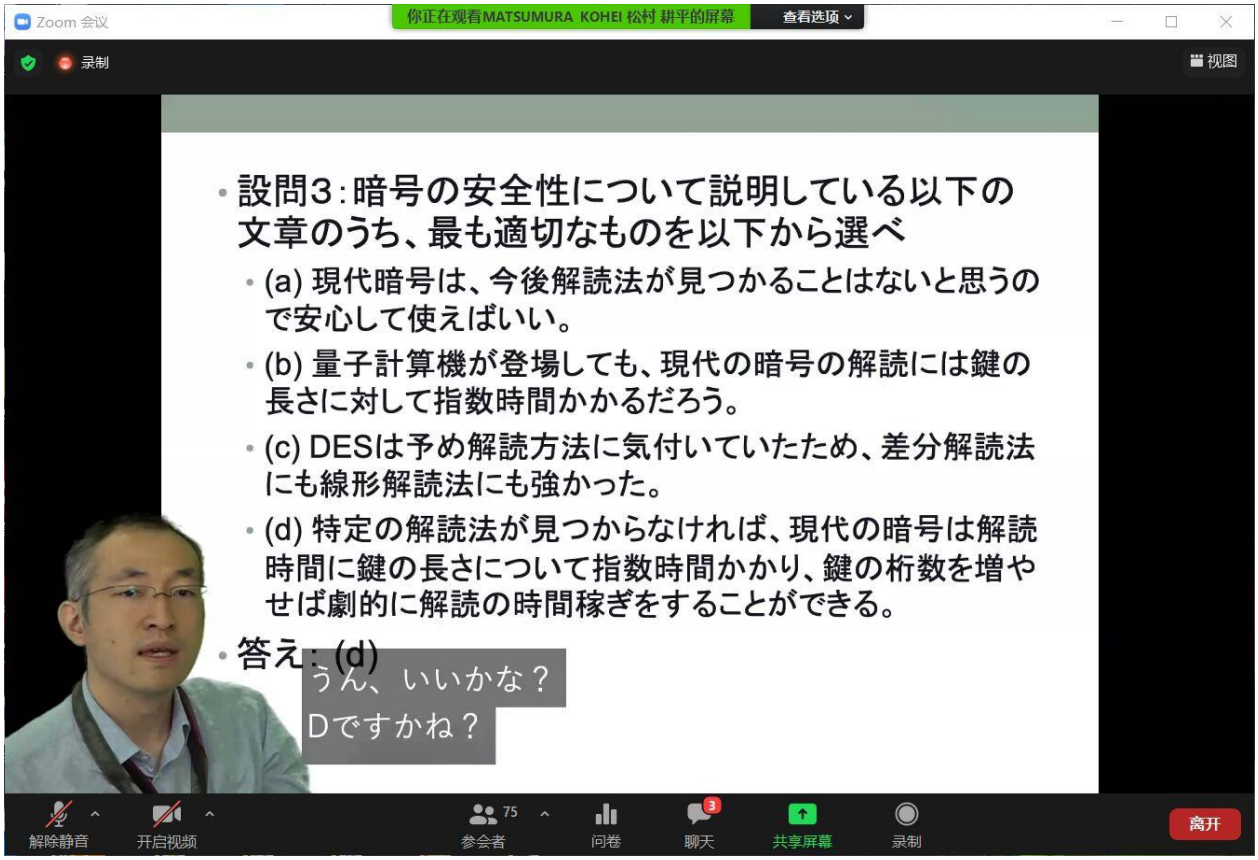

Zoom 会议
你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
视图
参会者 (75)
查找参会者
201894156武洲印 (我)
MATSUMURA KOH... (主持人)
201794006黄煜轲
201794029-胡晨阳
201794031-申屠寅吉
201794112-陈祥龙
201794114王有为
201894014毕行健.
201894020 仇朝一
201894022- 朱润文
201894023 - 励宁 吴
201894031_郑典
• 設問1：パスワードの管理について記述している以下の文章のうち、最も適切なものはどれか
• (a) パスワードは忘れてしまうと大変なので、確実に憶えている同じものを数年間使い続けている。
• (b) いろんなWebサービスを利用しているが、パスワードをいちいち憶えられないので全部同じものを使っている。
• (c) パスワードは自分の名前と誕生日にしておけば、忘れないので安心だ。
• (d) パスワードは、毎年新しいものに更新している。
: (d)
まあ、ちょっと簡単に説明して行きましょうか？
解除静音
开启视频
75
参会者
聊天
共享屏幕
录制
离开
邀请
解除静音

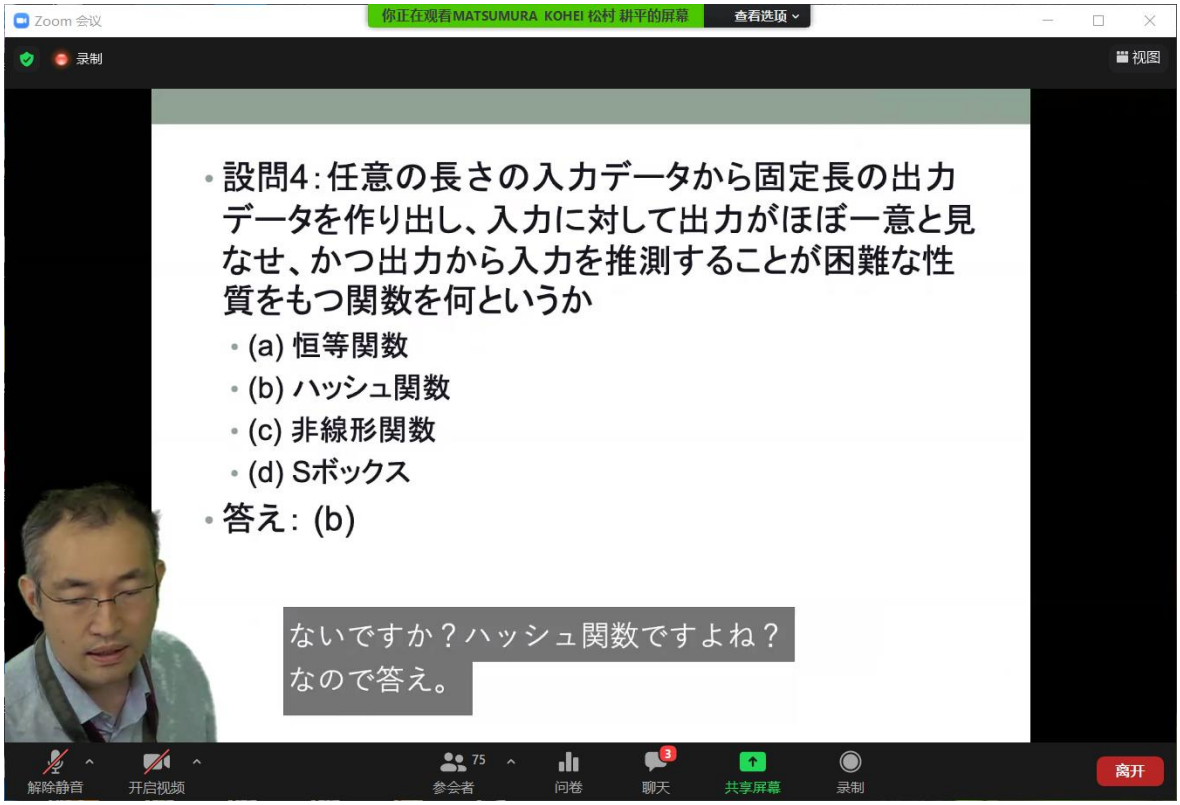

Zoom 会议
你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
视图
参会者 (74)
查找参会者
201894156武洲印 (我)
MATSUMURA KOH... (主持人)
201794006黄煜轲
201794029-胡晨阳
201794031-申屠寅吉
201794112-陈祥龙
201794114王有为
201894014毕行健.
201894020 仇朝一
201894022- 朱润文
201894023 - 励宁 吴
201894031_郑典
• 設問3：サーバにJavaScriptのプログラムを送り込み、それをユーザのブラウザで実行させてCookieなどに書かれたセッションIDなどの情報を盗む攻撃を何というか
• (a) クロスサイトリクエストフォージェリ
• (b) クロスサイトスクリプティング
• (c) SQLインジェクション
• (d) マルウェア
• 答え：(b)
と言うのはですね。クロスサイトスクリプティングというのが正解です。
解除静音
开启视频
74
参会者
问卷
聊天
共享屏幕
录制
离开
邀请
解除静音

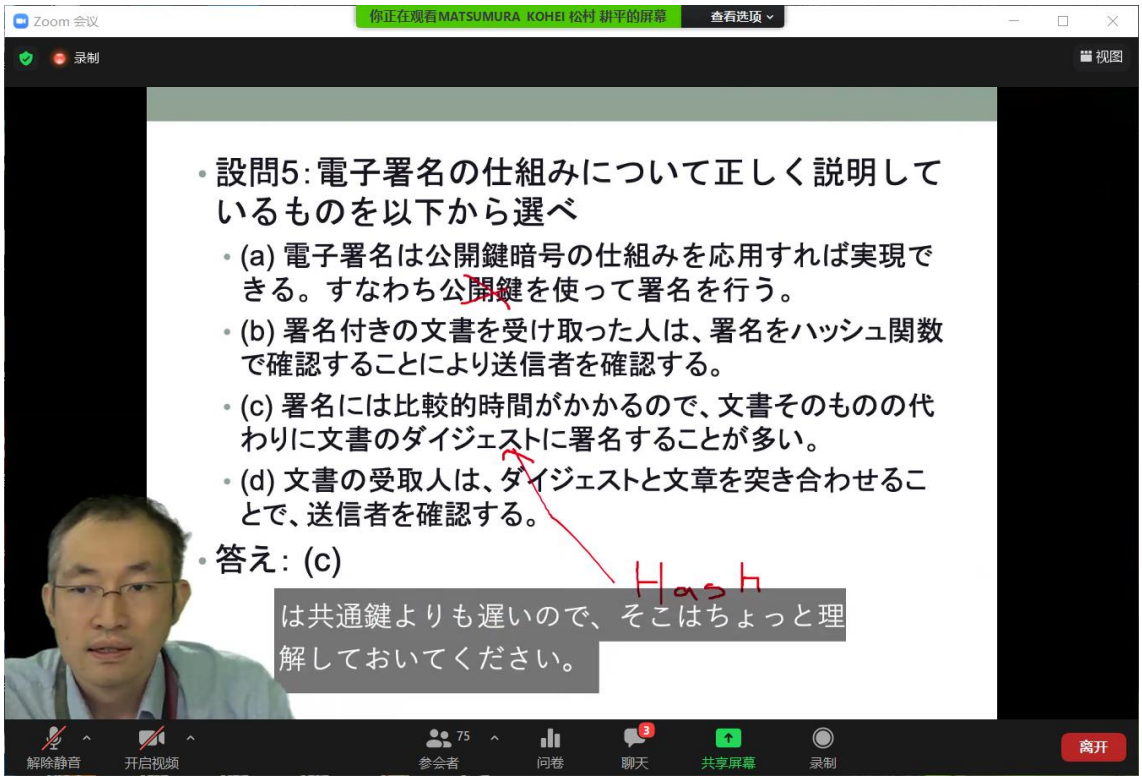

Zoom 会议
参会者 (75)
查找参会者
201894156武洲印 (我)
MATSUMURA KOH... (主持人)
201794006黄煜轲
201794029-胡晨阳
201794031-申屠寅吉
201794112-陈祥龙
201794114王有为
201894014毕行健.
201894020 仇朝一
201894022- 朱润文
201894023 - 励宁 吴
201894031_郑典
• 設問4：Webにおける通信について説明した以下の文章のうち、間違っているものはどれか
• (a) HTTPは通常1回の通信では処理が完結しないので、セッションIDなどを使ってTCP接続間に跨がった認証をする必要がある。
• (b) サーバから送られたセッションIDは、URLリンクやHTMLのフォーム、Cookieなどの形式でブラウザに保存される。
• (c) Cookieは保存されたら二度と消すことができない。
• (d) サーバに脆弱性があると、クロスサイトスクリプティングなどの攻撃を通じてセッションIDが盗まれ、通信を乗っ取られる可能性がある。
答え：(c)
ですけれども、間違っているのはこれらcだと思います。はいしいですね。
邀请
解除静音


Zoom 会议
你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
設問1：共通鍵暗号について説明している以下の文章のうち、間違っているものはどれか
(a) 米国政府標準で定められたブロック暗号であるDESは解読が進み、使われなくなってきた。
(b) DH鍵交換では、盗聴者が共通鍵を知ることを難しくするので、その鍵を使った暗号は解読される心配がない。
(c) バーナム暗号は最も強力な換字式暗号だが、鍵の長さが平文と同じである必要があるため、現実的には使いにくい。
(d) 共通鍵暗号を使ってN人で情報を送り合うときは、N(N-1)÷2の鍵が必要になる。
答え：(b)
と言うと。
ええ、bかな？
解除静音
开启视频
76
参会者
聊天
共享屏幕
录制
离开

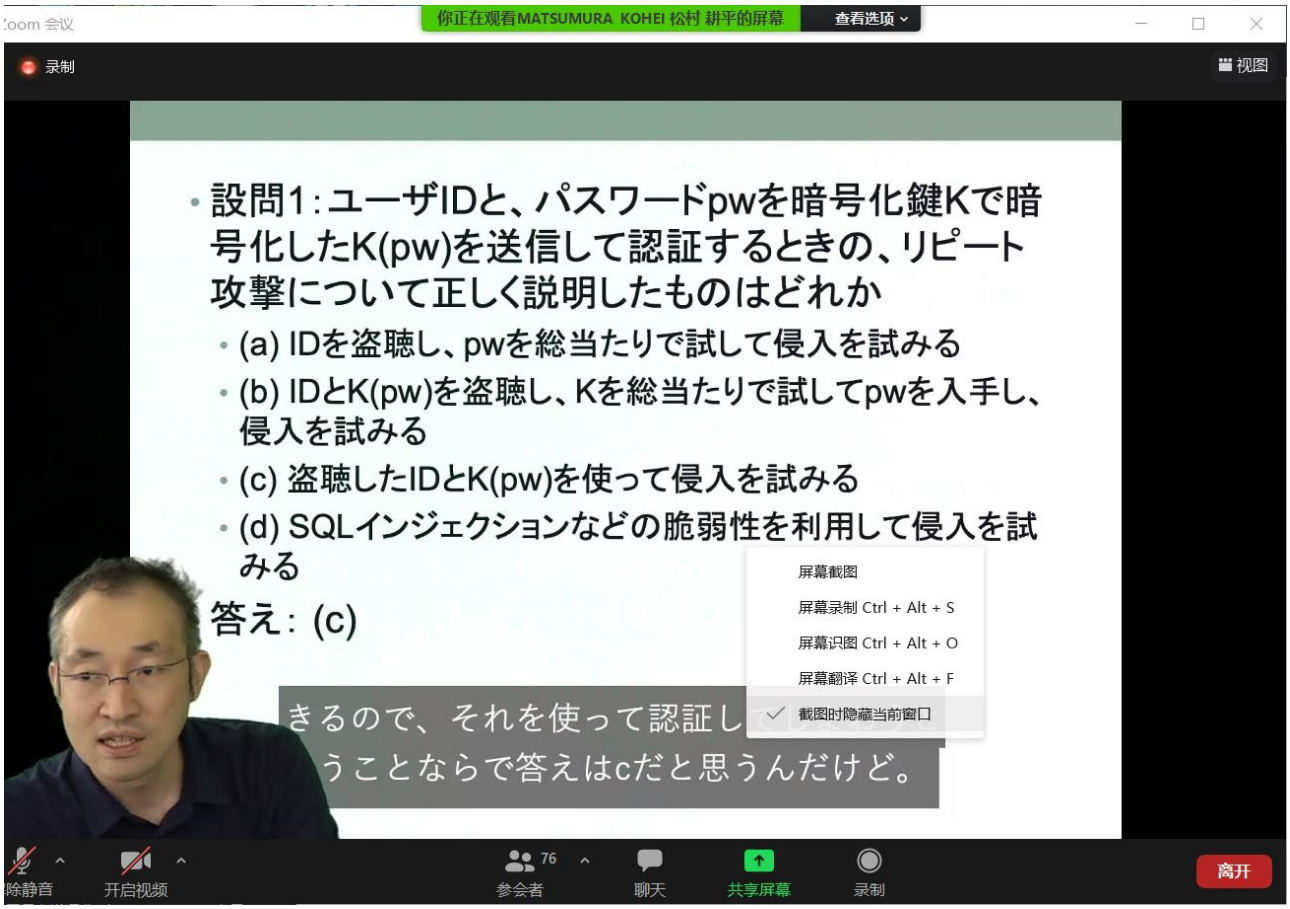

Zoom 会议
你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
設問2：公開鍵暗号のメリットについて説明している以下の文章のうち、間違っているものはどれか
(a) 一般に、共通鍵暗号よりも高速に暗号化や復号を行う。
(b) 公開鍵は秘匿する必要がなく、秘密鍵は誰にも教えなくてよいので、鍵交換の問題を解決してくれる。
(c) 電子署名の仕組みを作ることができる。
(d) N人で情報を送り合うときはN組の鍵を用意すればよい。
答え：(a)
そうですね。公開鍵暗号のメリット。
まあこれはaが間違ってますかね？
解除静音
开启视频
75
参会者
聊天
共享屏幕
录制
离开

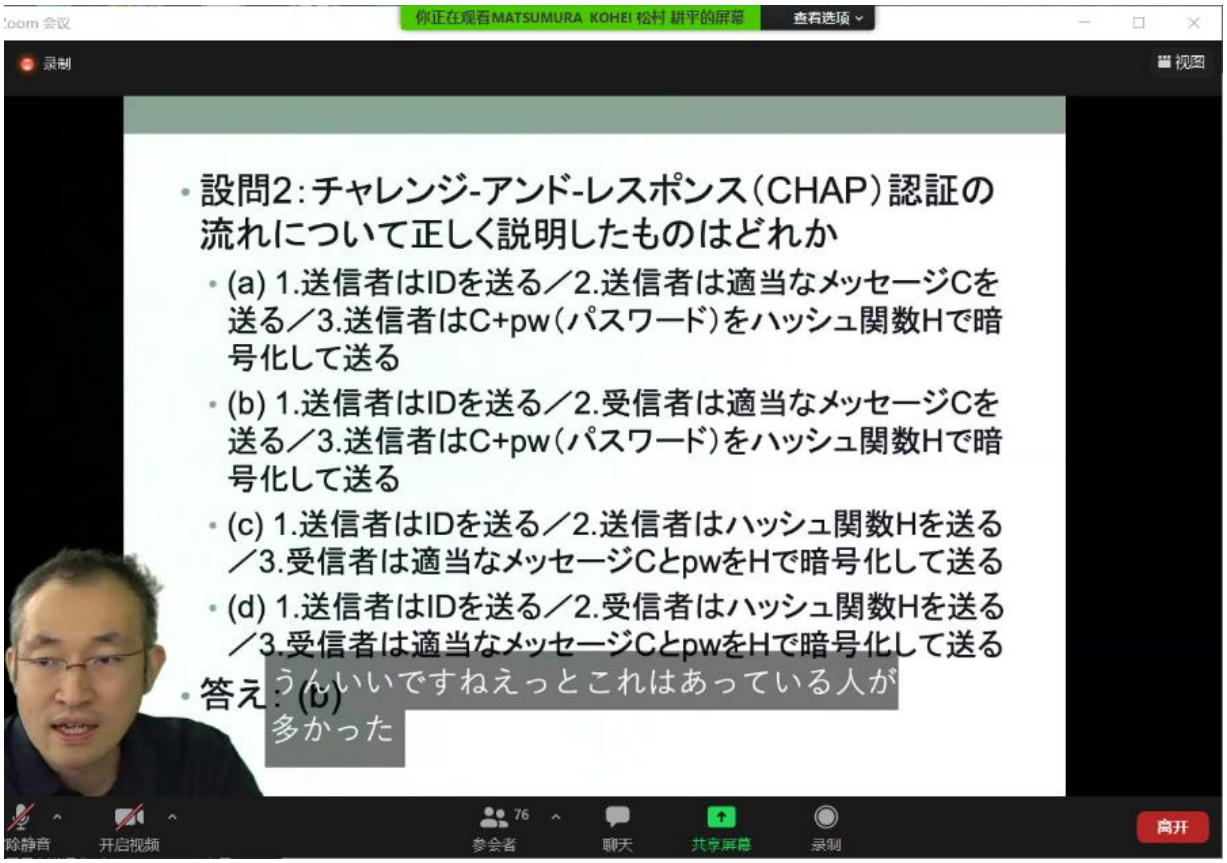

Zoom 会议
你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
• 設問3：暗号の安全性について説明している以下の文章のうち、最も適切なものを以下から選べ
• (a) 現代暗号は、今後解読法が見つかることはないと思うので安心して使えばいい。
• (b) 量子計算機が登場しても、現代の暗号の解読には鍵の長さに対して指数時間かかるだろう。
• (c) DESは予め解読方法に気付いていたため、差分解読法にも線形解読法にも強かった。
• (d) 特定の解読法が見つからなければ、現代の暗号は解読時間に鍵の長さについて指数時間かかり、鍵の桁数を増やせば劇的に解読の時間稼ぎをすることができる。
• 答え：(d)
うん、いいかな？
Dですかね？
解除静音
开启视频
75
参会者
问卷
聊天
3
共享屏幕
录制
离开

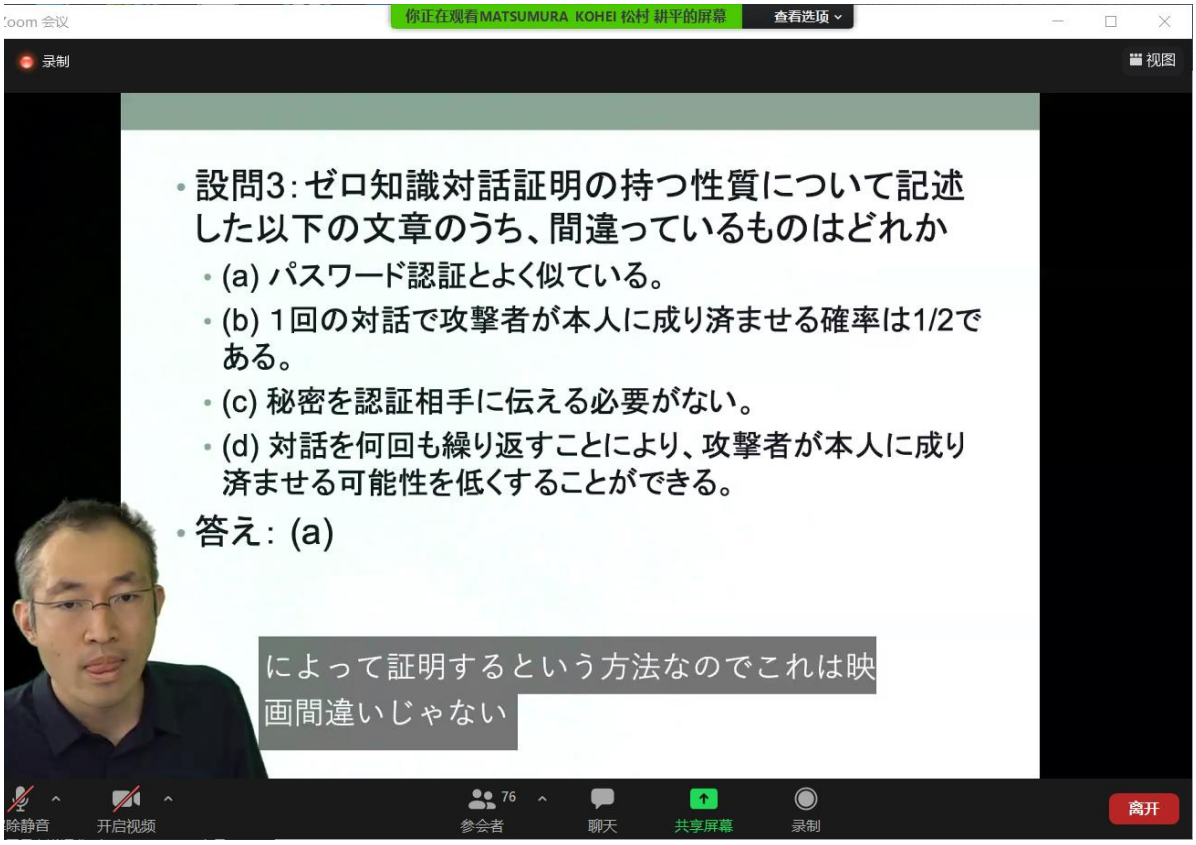

Zoom 会议
你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
• 設問4：任意の長さの入力データから固定長の出力データを作り出し、入力に対して出力がほぼ一意と見なせ、かつ出力から入力を推測することが困難な性質をもつ関数を何というか
• (a) 恒等関数
• (b) ハッシュ関数
• (c) 非線形関数
• (d) Sボックス
• 答え：(b)
ないですか？ハッシュ関数ですよね？
なので答え。
解除静音
开启视频
75
参会者
问卷
聊天
3
共享屏幕
录制
离开

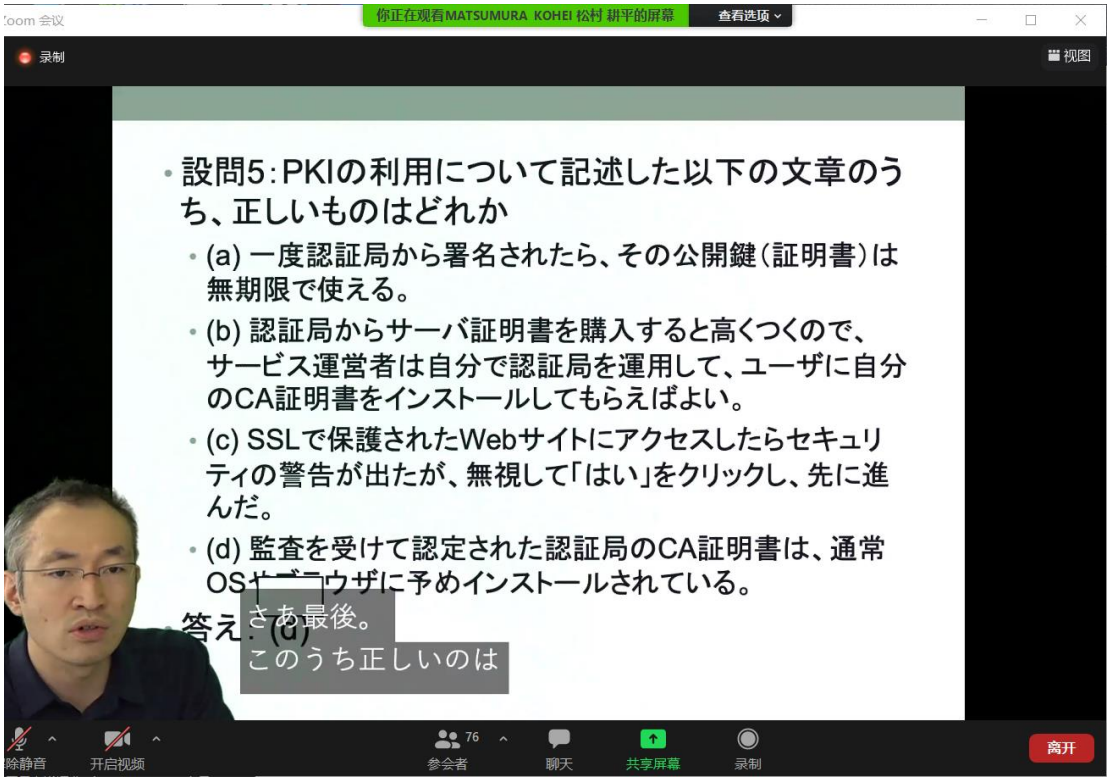

Zoom 会议
你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
• 設問5:電子署名の仕組みについて正しく説明しているものを以下から選べ
• (a) 電子署名は公開鍵暗号の仕組みを応用すれば実現できる。すなわち公開鍵を使って署名を行う。
• (b) 署名付きの文書を受け取った人は、署名をハッシュ関数で確認することにより送信者を確認する。
• (c) 署名には比較的時間がかかるので、文書そのものの代わりに文書のダイジェストに署名することが多い。
• (d) 文書の受取人は、ダイジェストと文章を突き合わせることで、送信者を確認する。
• 答え: (c)
Hash
は共通鍵よりも遅いので、そこはちょっと理解しておいてください。
解除静音
开启视频
参会者
75
问卷
聊天
3
共享屏幕
录制
离开

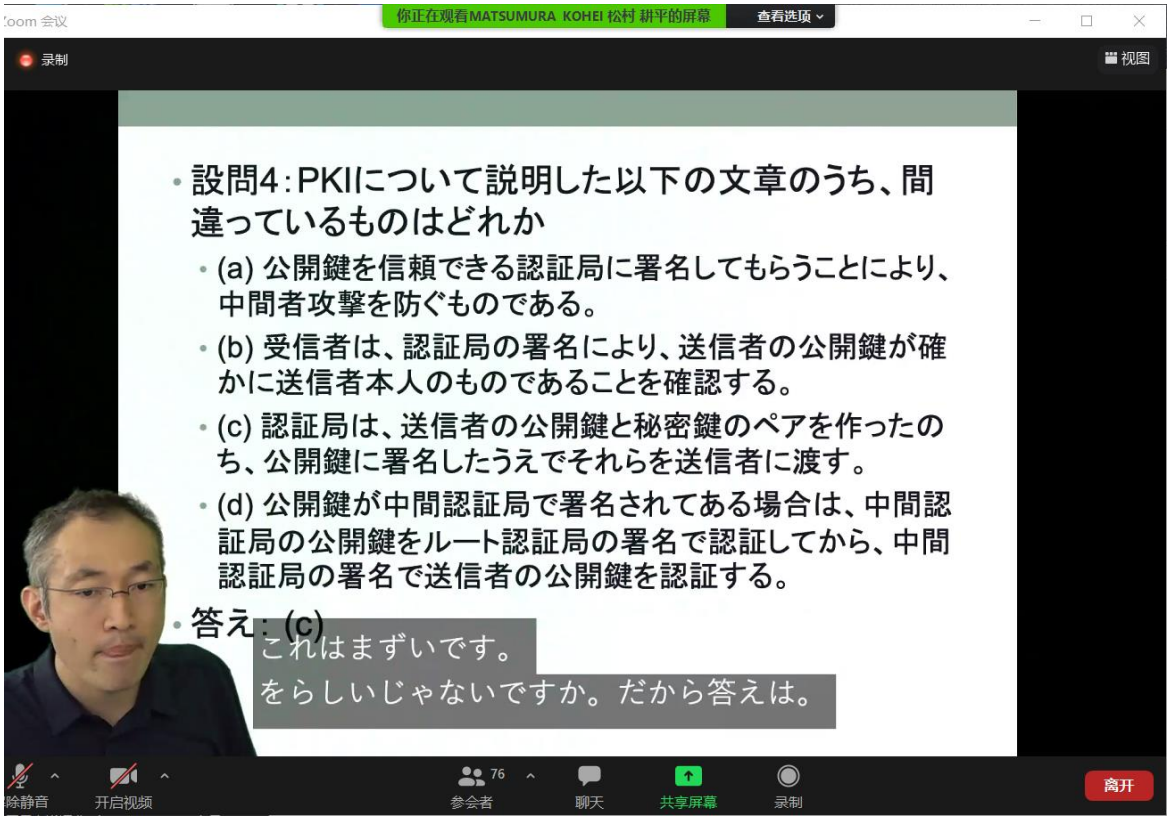
? ?

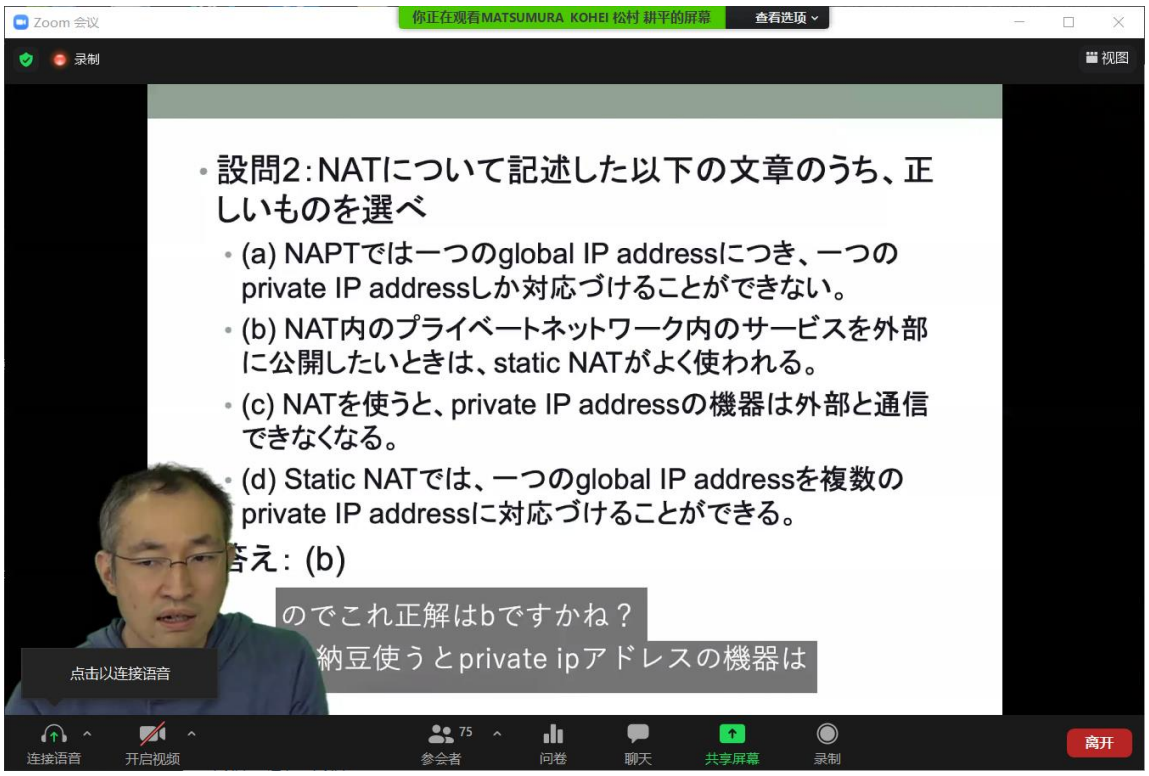

oom 会议
你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
• 設問1:ユーザIDと、パスワードpwを暗号化鍵Kで暗号化したK(pw)を送信して認証するときの、リピート攻撃について正しく説明したものはどれか
• (a) IDを盗聴し、pwを総当たりで試して侵入を試みる
• (b) IDとK(pw)を盗聴し、Kを総当たりで試してpwを入手し、侵入を試みる
• (c) 盗聴したIDとK(pw)を使って侵入を試みる
• (d) SQLインジェクションなどの脆弱性を利用して侵入を試みる
答え: (c)
きるので、それを使って認証し
うことならで答えはcだと思うんだけど。
屏幕截图
屏幕录制 Ctrl + Alt + S
屏幕识图 Ctrl + Alt + O
屏幕翻译 Ctrl + Alt + F
截图时隐藏当前窗口
除静音
开启视频
参会者
76
聊天
共享屏幕
录制
离开

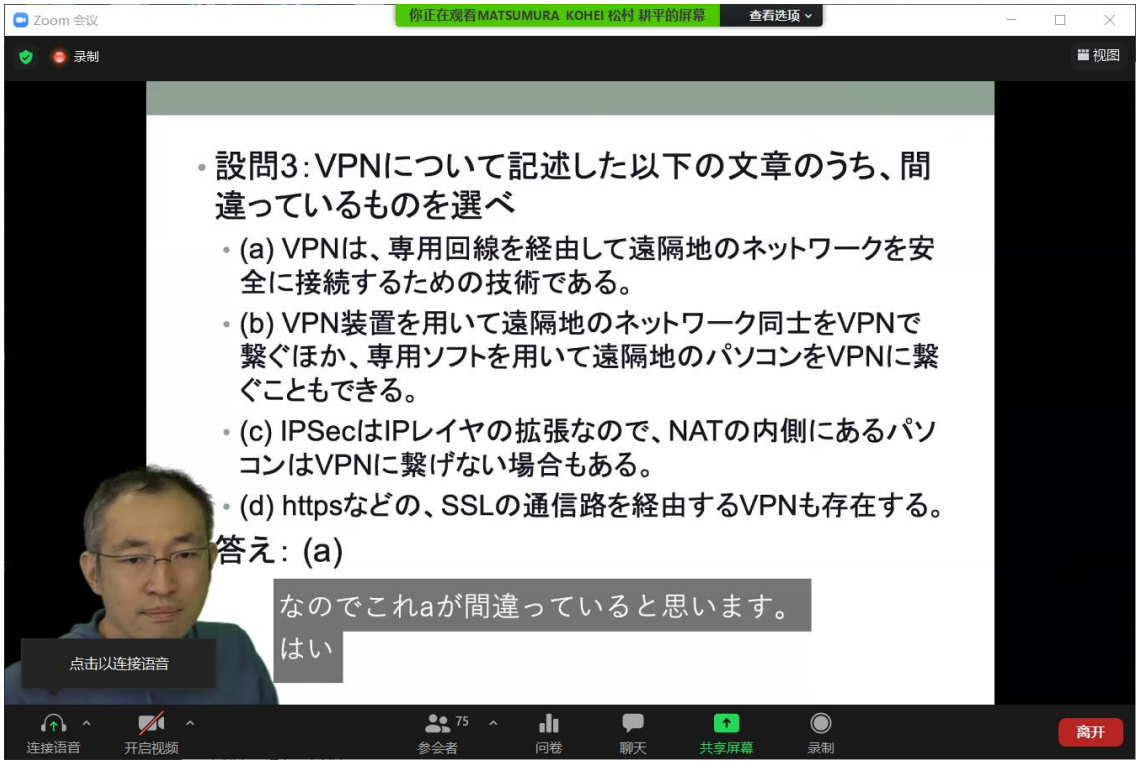

你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
• 設問2：チャレンジ-アンド-レスポンス（CHAP）認証の流れについて正しく説明したものはどれか
• (a) 1.送信者はIDを送る／2.送信者は適当なメッセージCを送る／3.送信者はC+pw（パスワード）をハッシュ関数Hで暗号化して送る
• (b) 1.送信者はIDを送る／2.受信者は適当なメッセージCを送る／3.送信者はC+pw（パスワード）をハッシュ関数Hで暗号化して送る
• (c) 1.送信者はIDを送る／2.送信者はハッシュ関数Hを送る／3.受信者は適当なメッセージCとpwをHで暗号化して送る
• (d) 1.送信者はIDを送る／2.受信者はハッシュ関数Hを送る／3.受信者は適当なメッセージCとpwをHで暗号化して送る
• 答え：(b)
うんいいですねえっとこれはあっている人が多かった
除静音
开启视频
76
参会者
聊天
共享屏幕
录制
离开

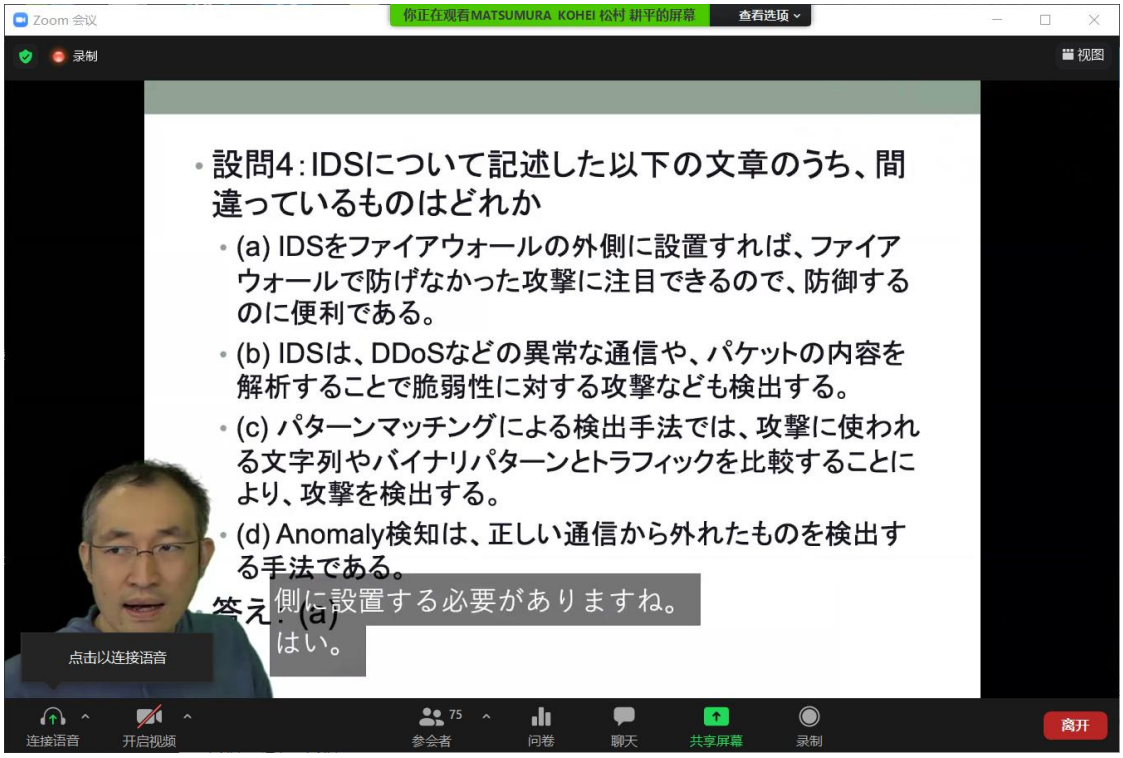

你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
• 設問3：ゼロ知識対話証明の持つ性質について記述した以下の文章のうち、間違っているものはどれか
• (a) パスワード認証とよく似ている。
• (b) 1回の対話で攻撃者が本人に成り済ませる確率は1/2である。
• (c) 秘密を認証相手に伝える必要がない。
• (d) 対話を何回も繰り返すことにより、攻撃者が本人に成り済ませる可能性を低くすることができる。
• 答え：(a)
によって証明するという方法なのでこれは映画間違いじゃない
除静音
开启视频
76
参会者
聊天
共享屏幕
录制
离开


你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
• 設問5：PKIの利用について記述した以下の文章のうち、正しいものはどれか
• (a) 一度認証局から署名されたら、その公開鍵（証明書）は無期限で使える。
• (b) 認証局からサーバ証明書を購入すると高くつくので、サービス運営者は自分で認証局を運用して、ユーザに自分のCA証明書をインストールしてもらえばよい。
• (c) SSLで保護されたWebサイトにアクセスしたらセキュリティの警告が出たが、無視して「はい」をクリックし、先に進んだ。
• (d) 監査を受けて認定された認証局のCA証明書は、通常OSやブラウザに予めインストールされている。
• 答え：(d)
さあ最後。
このうち正しいのは
76
除静音
开启视频
参会者
聊天
共享屏幕
录制
离开

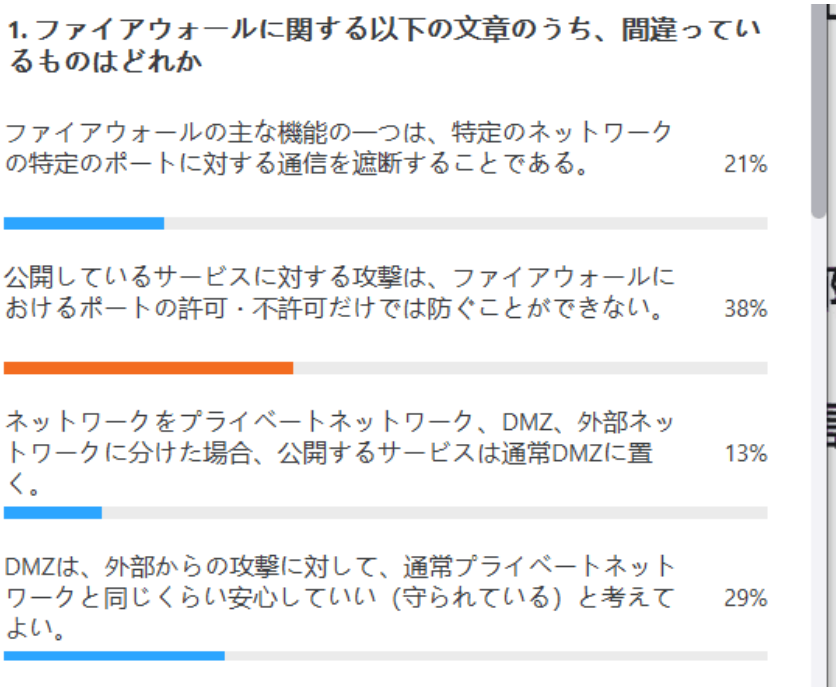

你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
• 設問4：PKIについて説明した以下の文章のうち、間違っているものはどれか
• (a) 公開鍵を信頼できる認証局に署名してもらうことにより、中間者攻撃を防ぐものである。
• (b) 受信者は、認証局の署名により、送信者の公開鍵が確かに送信者本人のものであることを確認する。
• (c) 認証局は、送信者の公開鍵と秘密鍵のペアを作ったのち、公開鍵に署名したうえでそれらを送信者に渡す。
• (d) 公開鍵が中間認証局で署名されてある場合は、中間認証局の公開鍵をルート認証局の署名で認証してから、中間認証局の署名で送信者の公開鍵を認証する。
• 答え：(c)
これはまずいです。
をらしいじゃないですか。だから答えは。
76
除静音
开启视频
参会者
聊天
共享屏幕
录制
离开

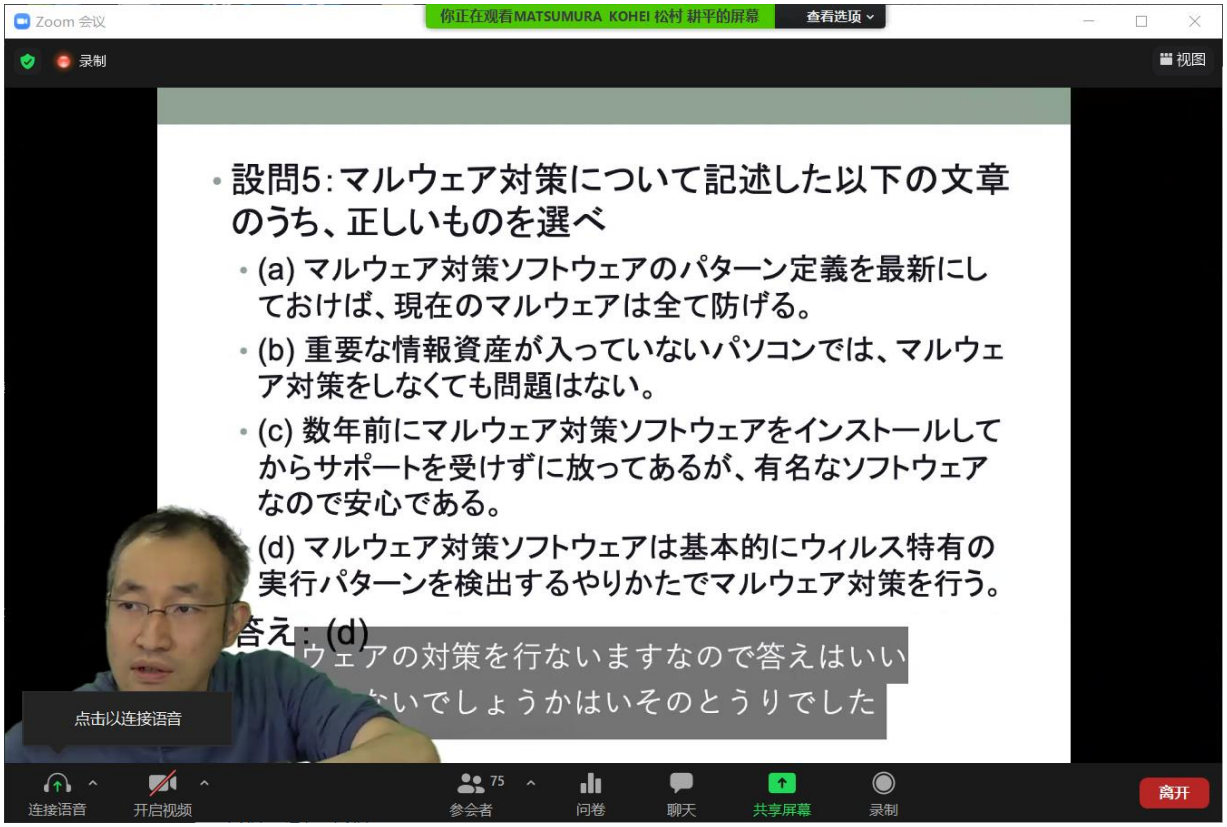

Zoom 会议
你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
• 設問2：NATについて記述した以下の文章のうち、正しいものを選べ
• (a) NAPTでは一つのglobal IP addressにつき、一つのprivate IP addressしか対応づけることができない。
• (b) NAT内のプライベートネットワーク内のサービスを外部に公開したいときは、static NATがよく使われる。
• (c) NATを使うと、private IP addressの機器は外部と通信できなくなる。
• (d) Static NATでは、一つのglobal IP addressを複数のprivate IP addressに対応づけることができる。
答え：(b)
のでこれ正解はbですかね？
納豆使うとprivate ipアドレスの機器は
点击以连接语音
连接语音
开启视频
75
参会者
问卷
聊天
共享屏幕
录制
离开


Zoom 会议
你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
• 設問3：VPNについて記述した以下の文章のうち、間違っているものを選べ
• (a) VPNは、専用回線を経由して遠隔地のネットワークを安全に接続するための技術である。
• (b) VPN装置を用いて遠隔地のネットワーク同士をVPNで繋ぐほか、専用ソフトを用いて遠隔地のパソコンをVPNに繋ぐこともできる。
• (c) IPSecはIPレイヤの拡張なので、NATの内側にあるパソコンはVPNに繋げない場合もある。
• (d) httpsなどの、SSLの通信路を経由するVPNも存在する。
答え：(a)
なのでこれaが間違っていると思います。
はい
点击以连接语音
连接语音
开启视频
75
参会者
问卷
聊天
共享屏幕
录制
离开


Zoom 会议
你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
• 設問4：IDSについて記述した以下の文章のうち、間違っているものはどれか
• (a) IDSをファイアウォールの外側に設置すれば、ファイアウォールで防げなかった攻撃に注目できるので、防御するのに便利である。
• (b) IDSは、DDoSなどの異常な通信や、パケットの内容を解析することで脆弱性に対する攻撃なども検出する。
• (c) パターンマッチングによる検出手法では、攻撃に使われる文字列やバイナリパターンとトラフィックを比較することにより、攻撃を検出する。
• (d) Anomaly検知は、正しい通信から外れたものを検出する手法である。
答え：(a)
側に設置する必要がありますね。
はい。
点击以连接语音
连接语音
开启视频
75
参会者
问卷
聊天
共享屏幕
录制
离开

D


1. ファイアウォールに関する以下の文章のうち、間違っているものはどれか
ファイアウォールの主な機能の一つは、特定のネットワークの特定のポートに対する通信を遮断することである。 21%
公開しているサービスに対する攻撃は、ファイアウォールにおけるポートの許可・不許可だけでは防ぐことができない。 38%
ネットワークをプライベートネットワーク、DMZ、外部ネットワークに分けた場合、公開するサービスは通常DMZに置く。 13%
DMZは、外部からの攻撃に対して、通常プライベートネットワークと同じくらい安心していい（守られている）と考えてよい。 29%


Zoom 会议
你正在观看MATSUMURA KOHEI 松村 耕平的屏幕
查看选项
录制
视图
• 設問5：マルウェア対策について記述した以下の文章のうち、正しいものを選べ
• (a) マルウェア対策ソフトウェアのパターン定義を最新にしておけば、現在のマルウェアは全て防げる。
• (b) 重要な情報資産が入っていないパソコンでは、マルウェア対策をしなくても問題はない。
• (c) 数年前にマルウェア対策ソフトウェアをインストールしてからサポートを受けずに放ってあるが、有名なソフトウェアなので安心である。
• (d) マルウェア対策ソフトウェアは基本的にウィルス特有の実行パターンを検出するやりかたでマルウェア対策を行う。
答え：(d)
ウェアの対策を行ないますなので答えはいい
ないでしょうかはいそのとうりでした
点击以连接语音
连接语音
开启视频
75
参会者
问卷
聊天
共享屏幕
录制
离开