サイエンティフィック・システム研究会
ICTフォーラム2021
学術機関 x オンライン x セキュリティ x コンプライアンス
～ オンラインの課題と明日 ～

TDU 東京電機大学

CIA＋HSEからみたオンライン利用の再考

学術機関でのオンライン活用における
セキュリティ、コンプライアンスの観点から

2021年9月13日

寺田真敏

はじめに

- 世の中には「オンライン」がおおよそ浸透し、様々な場面で利活用されるようになってきた、というのは、本当なのだろうか？
- まだまだ、使いこなせていない、振り回されている状態なのではないか？
- 「オンライン」の使いこなしに向け、2020年、2021年を振り返りながら再考したい。

2020年の振り返り (2020年4月27日作成資料から)

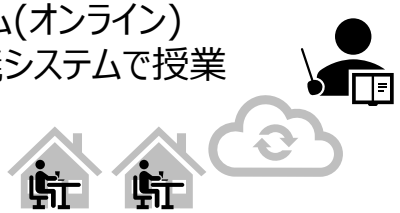
オンライン授業開始

- 学術系(大学)は、オンライン授業前提に動き始めている。
  - 次世代にとって、オンライン会合は当たり前の時代へ
  - リアルタイム(オンライン)型が主流
  - オンデマンド型は今のところリアルタイム(オンライン)のバックアップ
- 社会人のみなさんは、あっという間に、オールドタイプ

<u>オフライン</u>
リアルタイム(対面)
従来の授業

<u>ハイブリッド</u>
リアルタイム(対面＋オンライン)
教室＋Web会議システムで授業

<u>オンライン</u>
リアルタイム(オンライン)
Web会議システムで授業



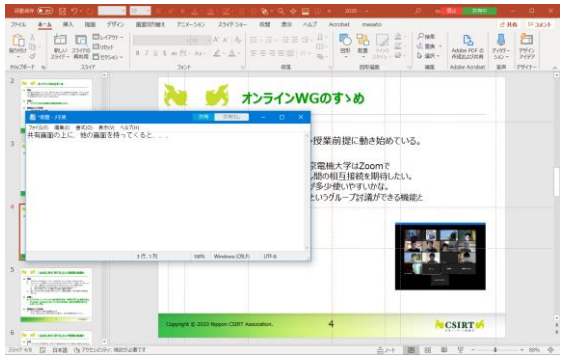
オンデマンド(オンライン)
学習システムで学生が各自学習

2020年の振り返り (2020年4月27日作成資料から)

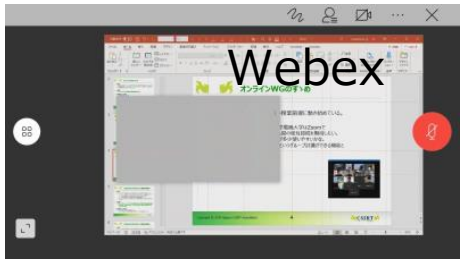
オンライン授業で使ったツール

- 中央大学はWebex、東京電機大学はZoom
- 画面共有の機能は、 Webexの方が多少使いやすい。
- 画面のオーバーラップ処理は、Zoomの方がオンライン会合にマッチしている。
- Zoomの魅力は、ブレイクアウトルームというグループ討議ができる機能と参加者の画面が一覧できるところ。
  注：2021年9月時点で機能の差はほとんどない。

発信者



受信者



Zoom

2020年の振り返り (2020年4月27日作成資料から)

Zoom問題：「やめる」から「育てる」という発想の転換へ

- 新型コロナウイルスの流行は、オフライン会合からオンライン会合への変化点となる。
- サプライチェーンも視野に入れなければならない状況下において、普及しているオンラインツールを、「使わない/やめる(自分だけを守る)」アプローチでは限界がある。
  - 2020年4月時点で、Zoomは2億ユーザ、Skypeは4000万ユーザ
  - 自社では禁止していても、顧客からの要望だと使わざる得ない。
- 使うことが当たり前/不可避な世代に向けて、問題を整理し、利用環境の改善を進めるべき。

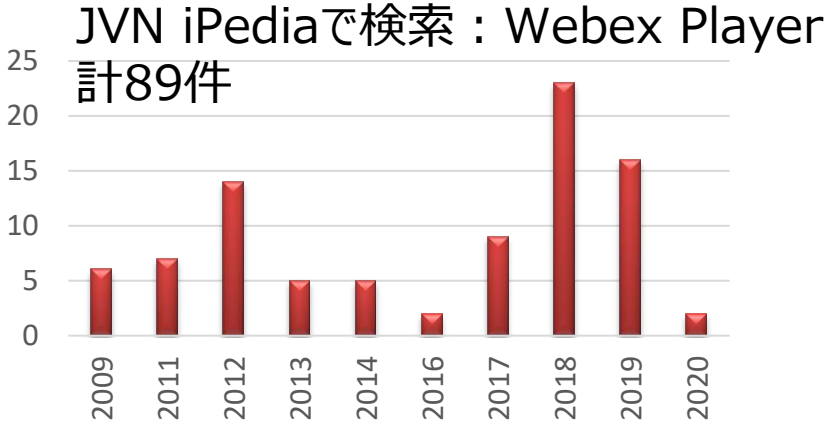
サプライチェーン＋オンライン会合世代に向け、分野を「育てる(全体の底上げ)」ために、「やめる」メッセージングだけではなく、新たな分野を「育てる」メッセージングを。

2020年の振り返り (2020年4月27日作成資料から)

Zoom問題：「やめる」から「育てる」という発想の転換へ

- NTIA(米国家電気通信情報管理庁)だって、Zoom使っているよ。
  カーネギーメロン大学だって、Zoom使っているよ。
  - 「使わない/やめる(自分だけを守る)」ということは、単に、ビジネス機会を失うことになるだけかもね(セキュリティ屋がビジネス機会を奪ってはいけない)。

  - 何のグラフか?



Skype、Webex使わない/やめる、基準は?

2020年の振り返り (2020年4月27日作成資料から)

Zoom問題：「やめる」から「育てる」という発想の転換へ

- 新型コロナウイルスの流行は、オフライン会合からオンライン会合への変化点となる。
  - オンライン会合は避けて通れない。

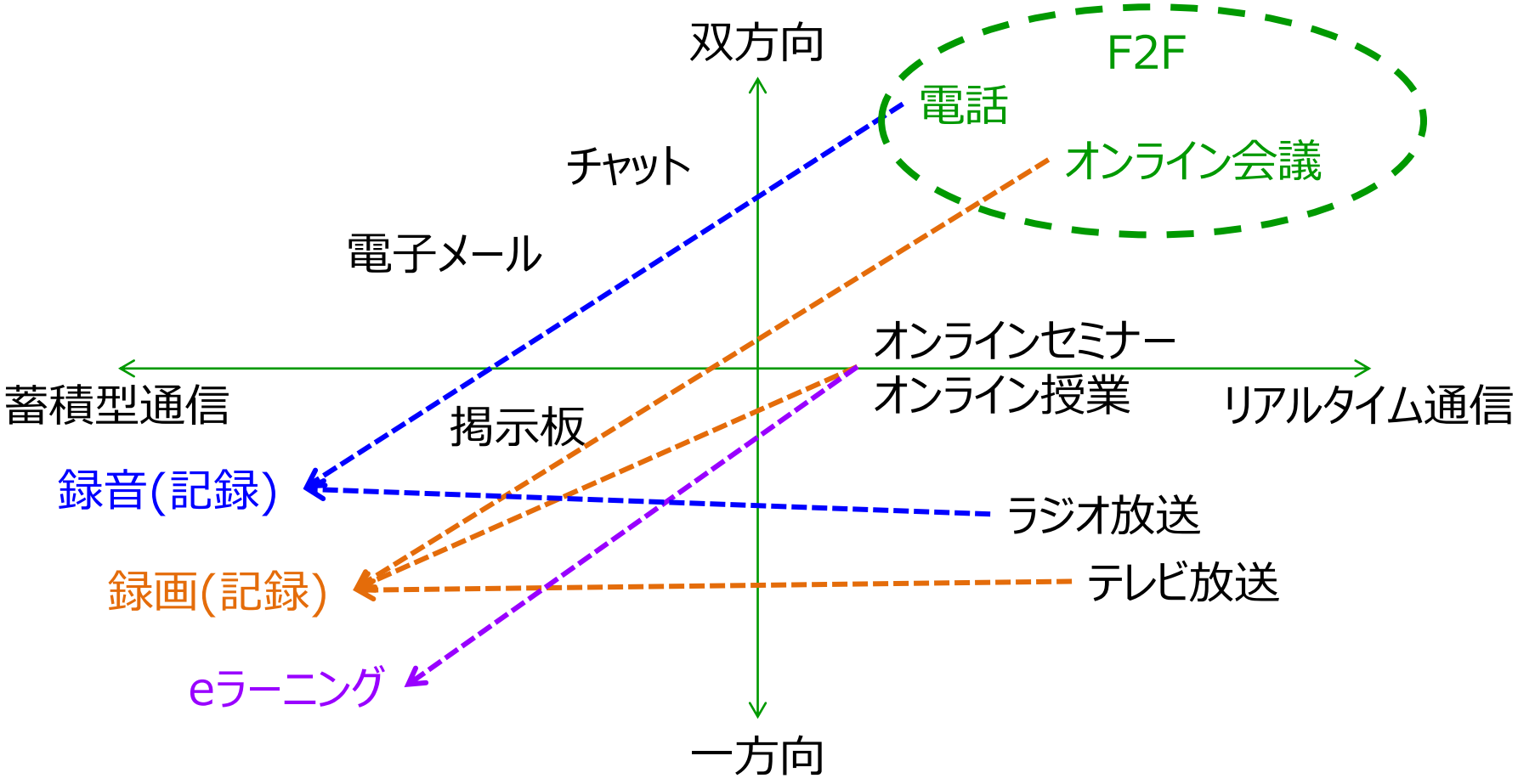
- セキュリティ業界、20年前から成長していない。もしかすると退化している。
  - 騒ぎに乗じて「使わない/やめる(自分だけを守る)」だけで、ソフトウェア等のセキュリティ上の問題と運用上の配慮で回避できる問題を整理せず。
  - 頑張っていたのは、東大の情報基盤センター(使わないといけない状況にある組織は違う)。

- サプライチェーンと言われている昨今、自分のところだけ守ってもダメなんでしょ。
  - メールやWebと異なり、オンライン会合の相互接続性は低い。
  - サプライチェーンを言われている今だからこそ、広く使われているものについては、禁止ではなく、より良くするために育てるという発想も必要である。
    公衆衛生って、「育てる」に近い発想があるような気がする。

2020年の振り返り (2020年4月27日作成資料から)

Zoom問題：「やめる」から「育てる」という発想の転換へ

- 双方向やリアルタイム通信の代替手段



2020年の振り返り (2020年5月16日作成資料から)

Zoom問題：「やめる」から「育てる」という発想の転換へ

組織間のセキュリティポリシー/ルールギャップとその折り合い

- [Q] オンライン会議ツールに関して、先方(顧客、取引先など)が利用したい/要望するツールが、自組織のセキュリティポリシー/ルールで許可されていない場合、どのような形で折り合いをつけているのか or つけるのか?

- [A] 本質的な問題は、先方(顧客、取引先など)とのセキュリティポリシー/ルールのギャップを、どのような形で折り合いをつけるのか?に帰着する。折り合いをつけられないということはビジネス機会を失う可能性がある。
  - ✓ 恒久的なルールの仕組みを持つ
  - ✓ 一時的な例外ルールを用意し対応する(先方にあわせる)
  - ✓ 一時的な例外ルールを用意し対応する(自組織にあわせてもらう)
  - ✓ 一時的な例外ルールを用意し対応する(自組織にあわせてもらうが、どうしてもダメな場合には、先方にあわせる)
  - ✓ 折り合いをつけない/つけられない

2020年の振り返り

Zoom プライベートチャットDDoS攻撃

- 授業で、とある簡単な演習課題を出したところ、大量のプライベートチャットが届く
- 約6分間に12名の学生(2名/分)から23メッセージ(4メッセージ/分)

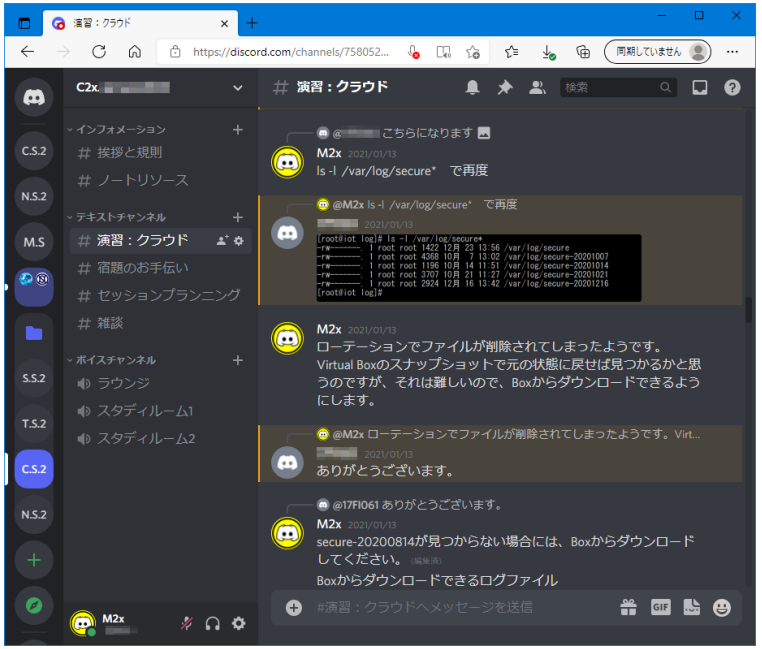
12:19:47 生徒A に 寺田(プライベート)：指定されたIPアドレスでnslookupを行うと見つけられませんとなってしまいます
12:20:08 寺田 に 生徒A(プライベート)：どの問題を解いていますか？
12:20:51 生徒B に 寺田(プライベート)：URLにアクセスできません。
12:21:21 生徒C に 寺田(プライベート)：エラーが出ます
12:21:24 生徒C に 寺田(プライベート)：Not Found The requested URL /netsec/test/tdub2-20200625cgi was not found on this server.
12:21:43 生徒A に 寺田(プライベート)：(1)(a1)でしたがもう一度試したらうまくいきました。何かミスしてたようです。すみません
12:21:50 寺田 に 生徒C(プライベート)：/netsec/test/tdub2-20200625(.)cgi
12:21:53 生徒D に 寺田(プライベート)：生徒Dです （1)でドメインが存在しないと言われました
12:22:11 寺田 に 生徒B(プライベート)：入力したURLを教えてください。
12:22:33 生徒E に 寺田(プライベート)：(1)で何度やっても下記のような表示になるのですが、これで転記してもいいのでしょうか？
12:22:34 生徒B に 寺田(プライベート)：http://jvnrss.ise.chuou.ac.jp/netsec/test/tdub2 20200625.cgi?
12:22:36 生徒E に 寺田(プライベート)：C:¥Users¥19fi081>nslookup 133.20.16.174 サーバー: UnKnown Address: 192.168.1.1 * UnKnown が 133.20.16.174 を見つけられません:
12:22:37 生徒F に 寺田(プライベート)：(1)「IPアドレスからホスト名を得る」の結果を報告しなさい。という問題において133.20.16.174 に対して nslookupを実行するとサーバーを見つけることができません
12:22:39 生徒B に 寺田(プライベート)：です
12:22:54 生徒G に 寺田(プライベート)：問題１でnslookup を実行すると見つけられませんと出てしまいます
12:22:59 生徒H に 寺田(プライベート)：課題(1)(a1)にてサーバー名がUnknownになってしまいました
12:23:07 生徒D に 寺田(プライベート)：数字が一つ足りないだけでした！解決しました！
12:23:14 生徒B に 寺田(プライベート)：http://jvnrss.ise.chuou.ac.jp/netsec/test/tdub2 20200625.cgi? 学籍番号
12:23:21 生徒I に 寺田(プライベート)：1.1で入力すると、「UnKnown が 93.184.216.34 を見つけられません」to
12:23:54 寺田 に 生徒B(プライベート)：学籍番号は、自分の学籍番号を入力
12:24:00 生徒I に 寺田(プライベート)：1.1で入力すると「UnKnown が 93.184.216.34 を見つけられません」と表示されました。
12:24:58 生徒J に 寺田(プライベート)：Mac を使っていてnslookup 133.20.16.174 のコマンドで調べたのですがホスト名が出てこないのですがどうすればいいですか。
12:25:07 生徒J に 寺田(プライベート)：Server
12:25:14 生徒B に 寺田(プライベート)：入力しても入れません
12:25:20 生徒J に 寺田(プライベート)：serverとadressはでます。
12:25:25 生徒K に 寺田(プライベート)：1番の結果が以下の様になりますが、合ってますか。nslookup 93.184.216.34 サーバー: UnKnown Address: 192.168.1.1 *** UnKnown が
12:25:42 生徒L に 寺田(プライベート)：コマンドプロンプトでnslookup 93.184.216.34を打ち込みましたが、「93.184.216.34 を見つけられません」と出たのですが何か操作方法を間違えたのでしょうか
12:25:56 寺田 に 生徒B(プライベート)：http://jvnrss.ise.chuou.ac.jp/netsec/test/tdub2 20200625.cgi? URLが間違っています。よく確認してください。

黒色：生徒から先生へ、灰色：先生から生徒へ

2020年の振り返り

Zoom プライベートチャットDDoS攻撃の対策

- 以降の対策
  - コミュニケーションツールDiscordの併用
    - 質問やトラブルについては
      Discordに投稿し、
      皆で問題解決する。



  - 質問方法に対する指示
    - Discordで質問する場合には、課題番号を指定して質問すること。
    - 単に「うまくいきません」という質問は受け付けない。 など

2021年の振り返り

オンライン | ハイブリッド | オフライン

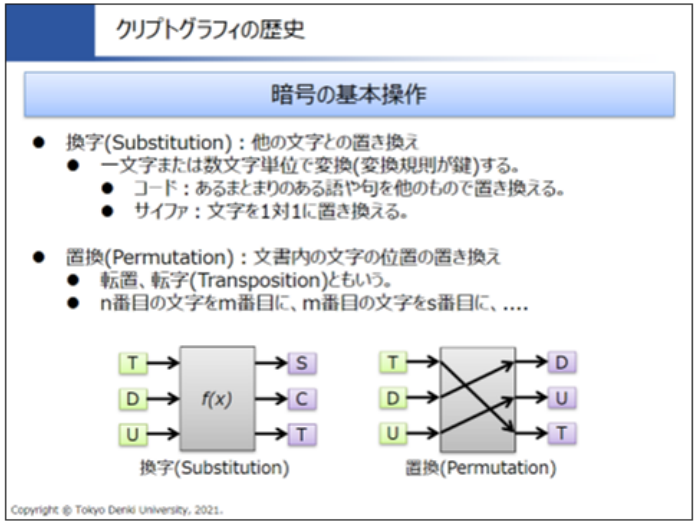
- 新型コロナウィルス感染症対策を通して、オンラインという強力なツールを得ることができた。経験したオンライン、ハイブリッド、オフラインの良い点、気を付けたい点を、今一度振り返ってみませんか?

	良い点	気を付けたい点
オンライン	● 物理的な場所に依存しない ● 個別対応に時間をかけられる ● 履修者を名前で指名しやすい	● 今まで以上に文字として伝えていく努力は必要(文章として伝えていくか or 映像として伝えていくか) ● 時間にルーズになりがち
ハイブリッド	● 良い点が見当たらない	● オンライン側とオフライン側とのコミュニケーション格差
オフライン	● 表情をみて対応できる ● 雰囲気という情報伝達が可能	● 授業終了時間を厳格に守らなければならない

2021年の振り返り

オンライン | ハイブリッド | オフライン

- 文章として伝えていくか or 映像として伝えていくか



暗号の歴史について眺めていくにあたり、暗号の基本操作について説明します。

換字(Substitution)：他の文字との置き換え
例えば、TをS、DをCに置き換える(-1文字分ずらした文字に置き換える)ことにより、
TDU⇒SCTとするというものです。

置換(Permutation)：文書内の文字の位置の置き換え。転置、転字(Transposition)と呼ぶこともあります。
例えば、Tを3番目に、Dを一番目に移動させる(-1文字分位置を移動させる)ことにより、
TDU⇒DUTとするというものです。

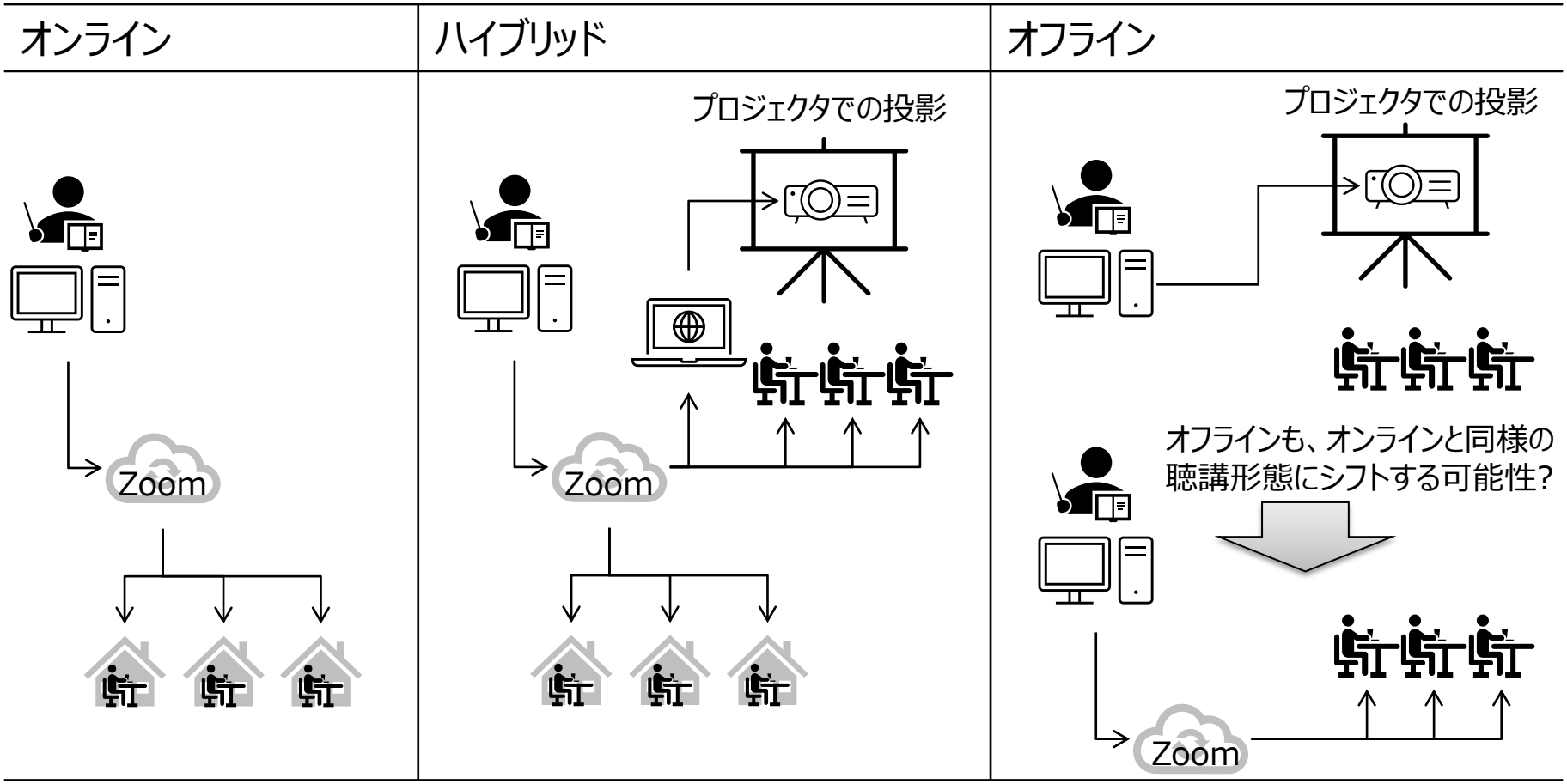
これら基本操作は、現代暗号においても、暗号を構成する基本要素となっています。

映像として残した場合、リアルタイムとオンデマンドとの違いは?
その他の課題は?

2021年の振り返り

オンライン | ハイブリッド | オフライン

- 聴講形態

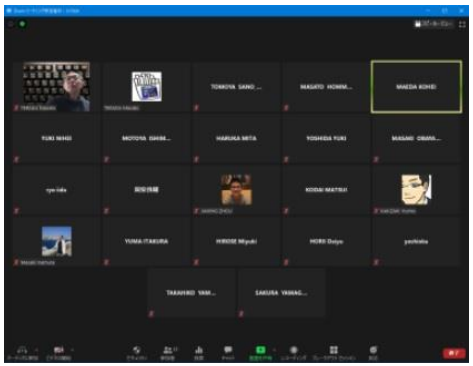


2021年の振り返り

オンライン | ハイブリッド | オフライン

- 聴講形態
  - 大学：ハイブリッドを推奨
  - 学生：ハイブリッドであっても、遠隔聴講を好む傾向が強い

形態	講師	履修者
オンライン	遠隔講義	遠隔聴講
ハイブリッド	遠隔講義	遠隔聴講 教室聴講
分散登校(半分は登校、半分はオンライン)	教室講義	
オフライン	教室講義	教室聴講



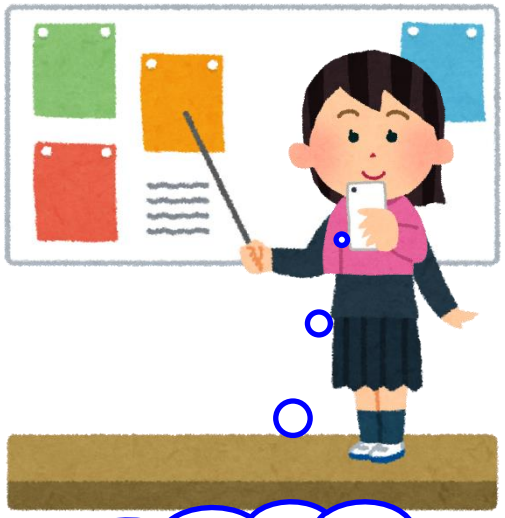
遠隔聴講

教室聴講

2021年の振り返り

オンライン | ハイブリッド | オフライン

- スマートフォンが究極の発表者支援ツールになる?

オンライン	ハイブリッド	オフライン
		

CIA

C：機密性　I：完全性　A：可用性

- 情報セキュリティの3大要素
  - Confidentiality：機密性
    認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性(機密情報が漏えいする可能性)
  - Integrity：完全性
    資産の正確さ及び完全さを保護する特性(情報が改ざんされる可能性)
  - Availability：可用性
    認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること(業務停止の可能性)
- 規格
  - ISO/IEC 27001:2013／Information technology — Security techniques — Information security management systems — Requirements
    さまざまな情報資産を守り有効に活用するためのマネジメントシステム規格

HSE

H：健康　S：安全　E：環境

- 環境及び労働安全衛生を一体としてマネジメントする3大要素
  - Health：健康(労働衛生)
  - Safety：安全
  - Environment：環境
- 規格
  - ISO 14001:2015／Environmental management systems — Requirements with guidance for use
    環境を保護し、環境パフォーマンスを向上させるマネジメントシステム規格
  - ISO 45001:2018／Occupational health and safety management systems — Requirements with guidance for use
    労働安全衛生におけるリスクを除去または最小化するマネジメントシステム規格

CIA＋HSEからみたオンライン利用の再考

CIA+HSE

区分	懸案事項
C：機密性	● 参加者がどこから参加しているのかわからない ● 参加者の隣で誰が聞いているのかもわからない
I：完全性	● 参加者がそこに居るのかわからない ● 相手を識別する能力の低下(対面で会っても分からない)
A：可用性	● 参加者がどの程度集中しているのかわからない ● オフラインを断る理由の妥当性を検証できない
H：健康	● 時間にルーズとなりがち ● 休み時間なく連続する打合せの嵐 ● 打合せのタブルブッキング
S：安全	● 参加者がどこから参加しているのかわからない ● ながら仕事による集中力低下(注意散漫) ● 容赦のない割り込みによる集中力低下(注意散漫)
E：環境	● 画面共有により共通認識が取れているという誤解 ● オンラインが安易な言い訳ツールとなってしまう可能性

CIA＋HSEからみたオンライン利用の再考

CIA+HSE

- 二値化への懸念
  - 会場を出たら、すべて忘れる、というアナログ発想が適用できなくなるため、すべてが二値化する。
  - 新たな懸念事項への対応要
    - 「否認防止(Non-repudiation)：ある活動又は事象が起きたことを、後になって否認されないように証明する能力」の悪用
    - 「やったという事実を説明はしやすいが、やっていないという事実を説明することが難しい」の悪用

まとめ

- 世の中には「オンライン」がおおよそ浸透し、様々な場面で利活用されるようになってきた、というのは、本当なのだろうか？

  利活用の幅は確実に広がっている。

- まだまだ、使いこなせていない、振り回されている状態なのではないか？

  とは言うものの、いろいろと考えていくことがありそう。

- 「オンライン」の使いこなしに向け、2020年、2021年を振り返りながら再考したい。

  いろいろと考えていくにあたり、そのヒントになれば幸いです。

Collaborate
together
to make our
Internet
secure.