CYBER SECURITY TREND IN 2018 FROM LAS VEGAS

仙台CTF推進プロジェクト
運営委員　戸羽秀人
（東北インフォメーション・システムズ株式会社）

1. Black Hat USA 2018

■過去最大の参加者。攻撃者視点のセキュリティ技術への関心は世界的に高まっている。
■安全計装、サイレン等様々な機器への攻撃手法がBriefing（講演）で公開された。
■日本を含め多くの攻撃者視点のセキュリティツールがArsenal（技術展示）で公開された。

Black Hat USA 2018 概要

- 8/4～9の5日間、米国ネバダ州ラスベガスのホテルで開催。21回目。
- 世界112カ国から過去最大の1万7000人が参加（2017年は1万5000人）。Briefing（講演）、Arsenal（技術展示）、Business Hall（製品展示）、Training（教育）等で構成される。

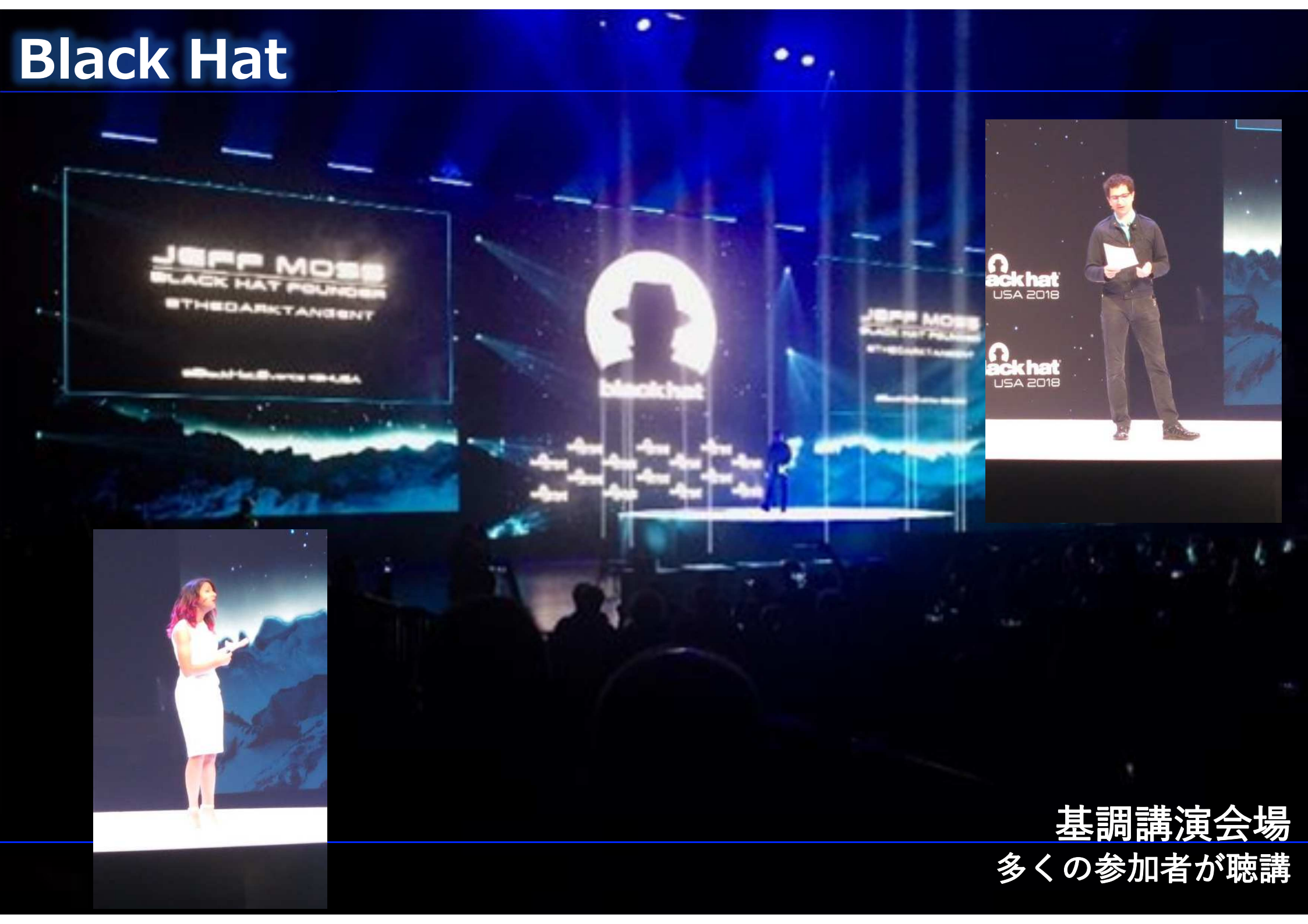
Briefing(講演) トピックス

- 基調講演：Jeff Moss氏、Google社Parisa Tabriz氏両名は、「攻撃者優位の現状」であることを指摘した上で、「攻撃者の後手に回らない」ことが重要と述べた。
- 2017年に引き続き、次に示すような様々な機器への攻撃手法が公開。
  - 安全計装システム（制御システムの異常発生時に安全な状態に移行させるシステム）
  - サイレン（警報発令システム。無線で命令・情報を送信している。）

Arsenal(技術展示) トピックス

- 2017年に引き続き、多くの攻撃者視点のセキュリティツール（疑似攻撃ツール）が公開。その多くが無償利用可能。例えば、機械学習、IPv6、制御システムをテーマとしたツールがあった。
- 国内勢の活躍。
  - 三井物産ｾｷｭｱﾃﾞｨﾚｸｼｮﾝ高江氏：Metasploitと機械学習を連携させたﾃｽﾄﾂｰﾙ「Deep Exploit」
  - ｱｸﾃｨﾌﾞﾃﾞｨﾌｪﾝｽ研究所 小池氏他：ｳｨﾙｽをﾀﾞｳﾝﾛｰﾄﾞする通信を自動的に分析するﾂｰﾙ「EKTotal」

Black Hat



基調講演会場

多くの参加者が聴講

Black Hat

Briefing 会場

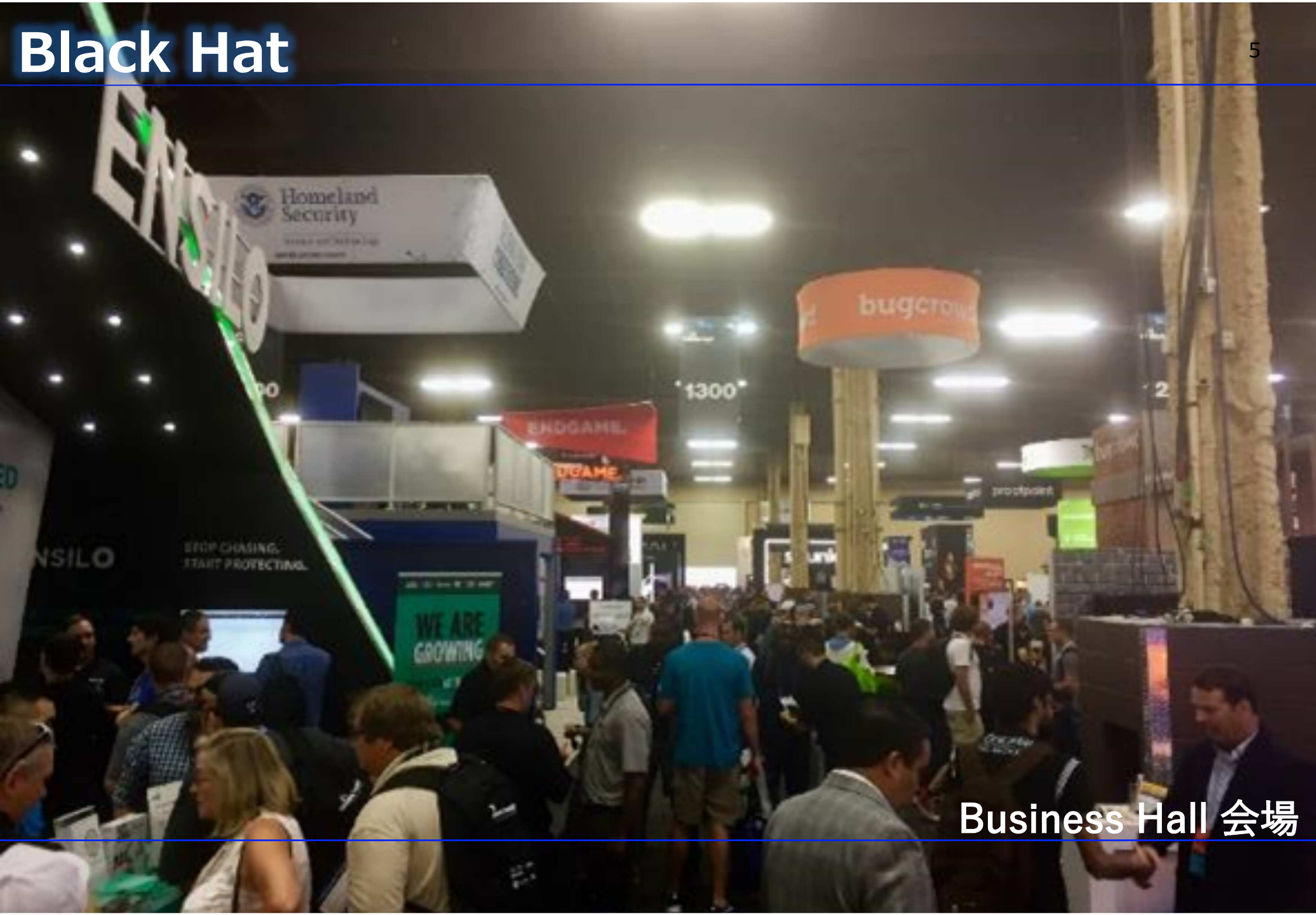
9つのセッションが同時に進行

Black Hat

Arsenal 会場

1セッション90分で聴講者に対して説明

Black Hat



Business Hall 会場

2. DEF CON 26

■Black Hat USA と同様に過去最大の参加者数。
■Village（テーマ型技術展示）は、2017年11種類と比較して28種類と大幅に増加。
■ソーシャルエンジニアリング攻撃手口を目の前で体験。

DEF CON 26 概要

- 8/10～12の3日間、米国ネバダ州ラスベガスの2つのホテルで開催(昨年はひとつのホテル)。26回目。
  世界各国から過去最大約2万7000人が参加（2017年は約2万4000人）。
- Presentation（講演）、Village（テーマ型技術展示）、CTF（旗取りゲーム）、Vender（ハッキングツールやマニュアルの展示即売会）等で構成。Black Hat USA より技術的。

Presentation(講演) トピックス

- 2017年に引き続き様々な機器（水道スマートメーター、音声認証、FAX等）への攻撃手法が公開。

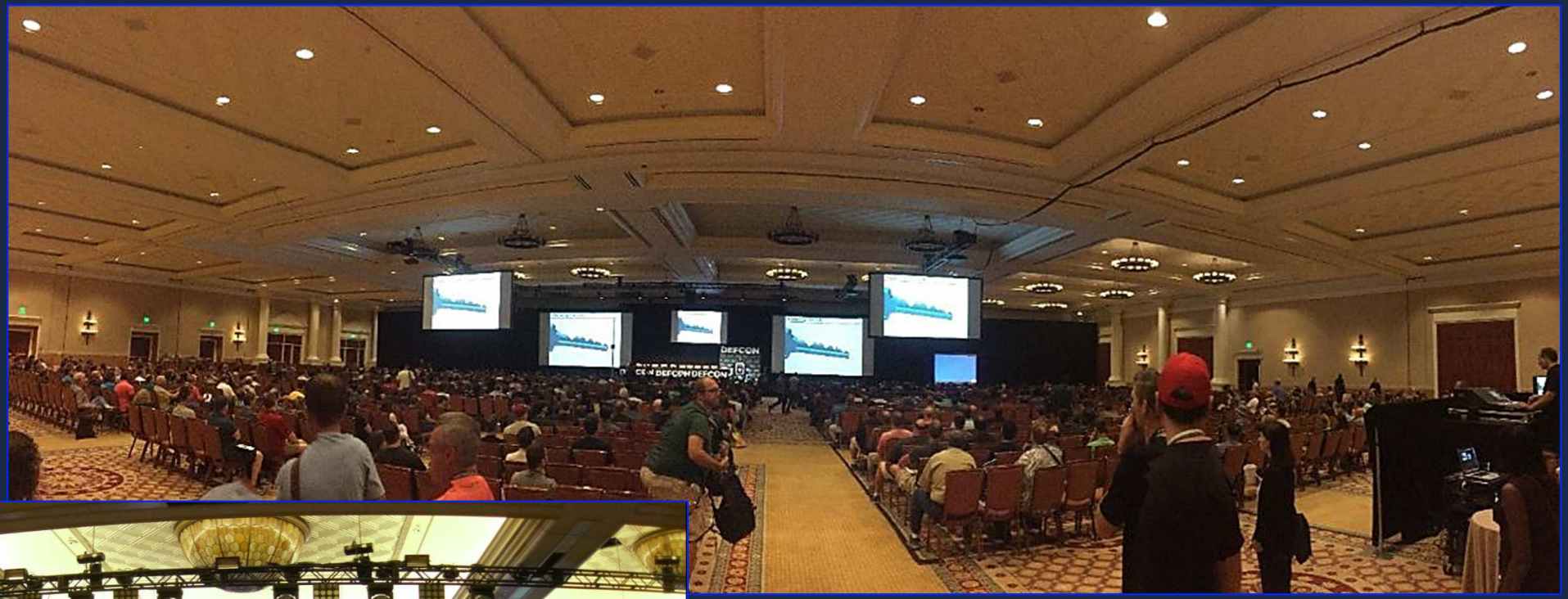
Village(テーマ型技術展示) トピックス

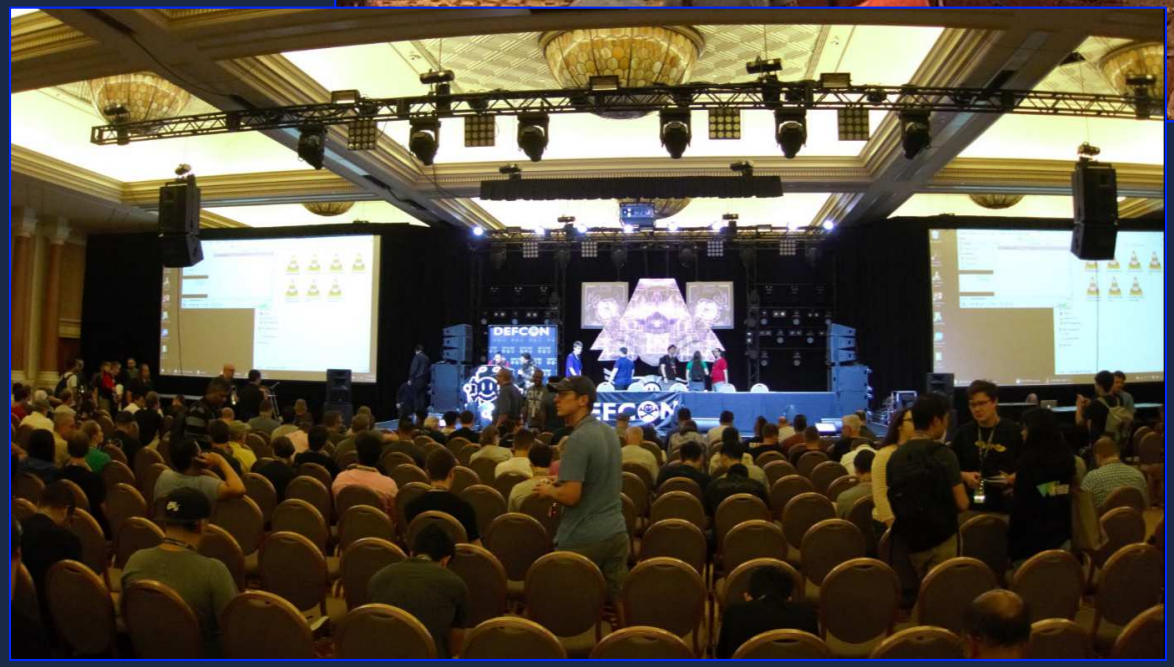
- 11→28種類へ増加（IoT、医療、AI、投票、ピッキング、防御チーム等）。細分化と新規テーマ。
- 2017年と比べ、多くのVillageでCTFが開催。

Social Engineering Village

- 制限時間20分以内に予めリストアップされた企業へチャレンジャーが電話をかけ、電話口で「OS」、「ブラウザ」、「ウイルス対策ソフト」の種別やバージョンを聞き出し、最終的にSE VillageのWebサイトにアクセスさせることで得点を得る。※企業には事前に通知なし。ただし、FBIには事前に連絡。
- チャレンジャーは、自らを「ITヘルプデスクのリサーチャー」と名乗り、上記の情報を聞き出した。

DEF CON





Presentation 会場

Black Hat USA Briefing 会場よりも大きい

CTF 会場

国内からは「binja」が参画

Vender 会場

ハッキングツールやマニュアルの展示即売

DEF CON Village

車載システムハッキング

国内参加者がCTF優勝

DEF CON
Village

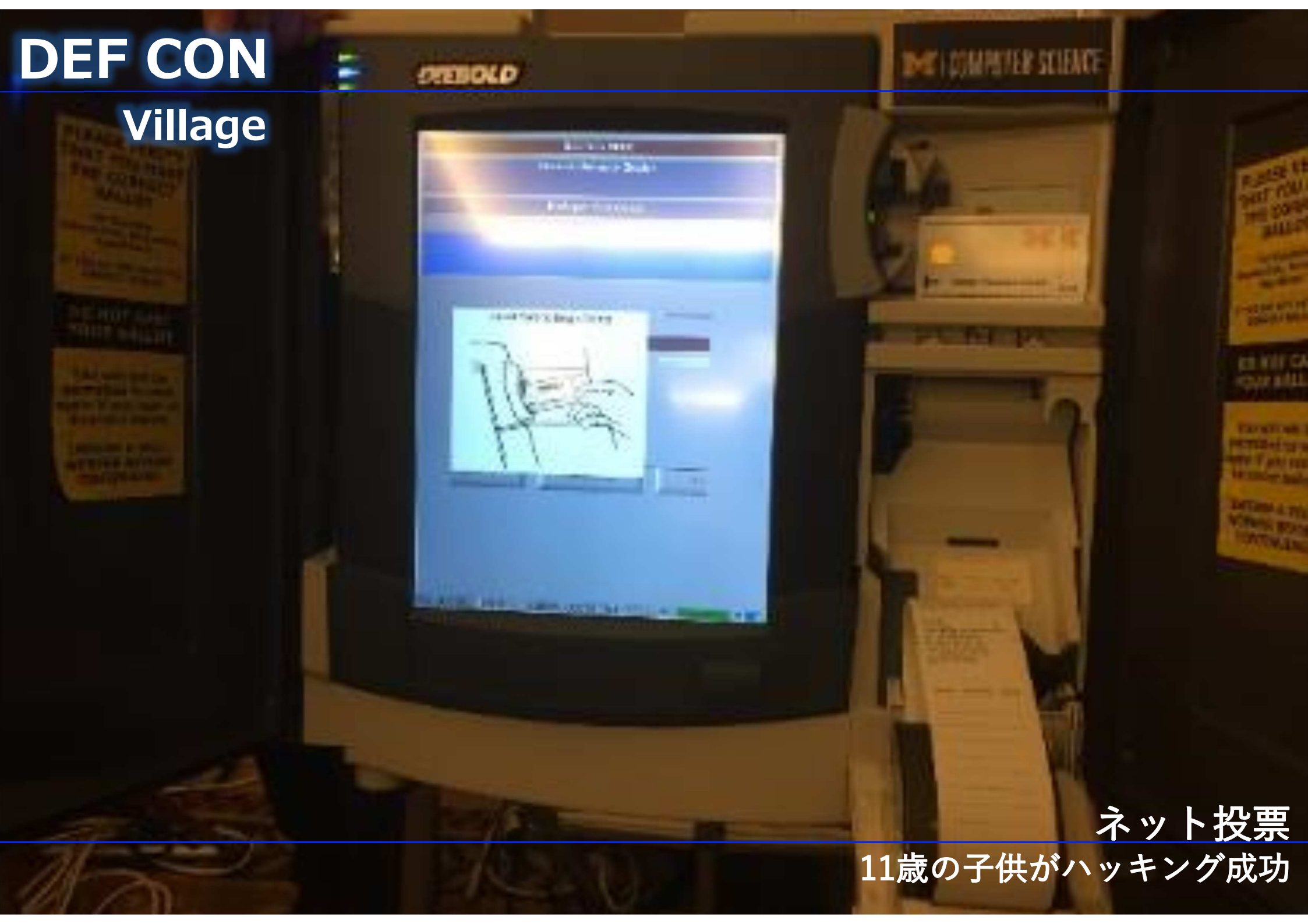
ソーシャルエンジニアリング
実企業に対する電話でのSE

DEF CON

Village

ロックピッキング

シリンダー錠のピッキング解説

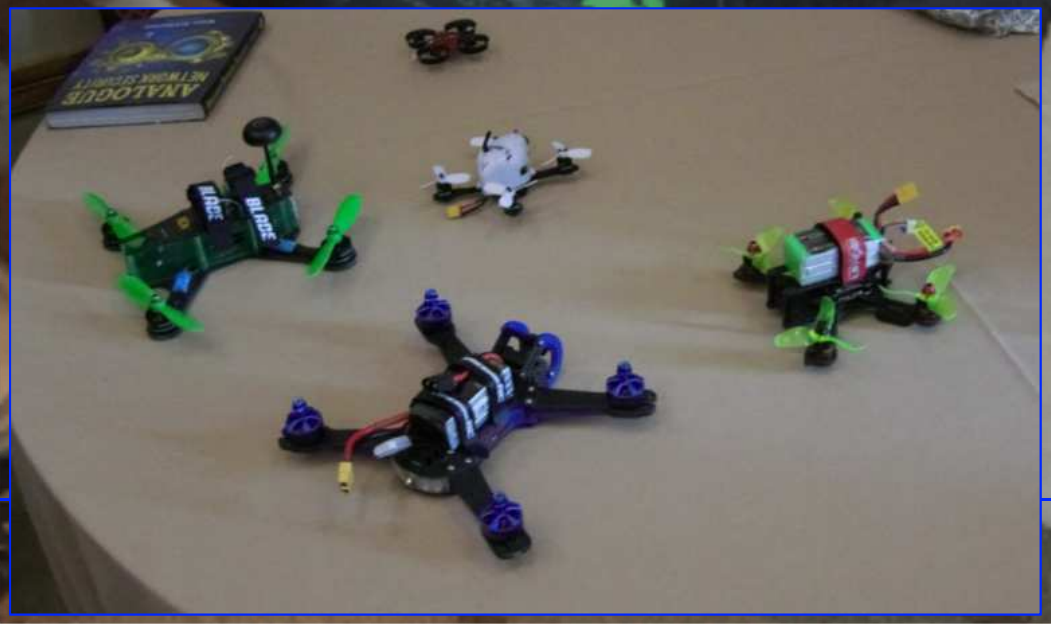

DEF CON
Village
ネット投票
11歳の子供がハッキング成功


DEF CON
Village
IoT
民製品の脆弱性発見

DEF CON
Village

制御システム
模擬プラントを使用したCTF

DEF CON
Village



ドローンウォーズ
ドローンを使用したCTF

DEF CON
Village

バイオハッキング
医療機器を使用したCTF


DEF CON
Village
ハードウェアハッキング
チップを半田ごてで外して解析

3．脅威動向

■ 攻撃対象と攻撃手法の多様化がセキュリティ技術者の興味関心を集めている。

これまで

情報システムの技術的脅威

が中心

- 対象：情報システム
- 手法：既存のIT系攻撃手法
- 経路：インターネット

脅威が増加

コンピュータリソースを有する全てのデバイスが攻撃対象

- 制御システム
- 車
- スマートシティー
- IoT機器
- 無線でアクセスできる機器
- 医療機器
- ドローン

脅威が増加

異なるレイヤ(技術・物理・人)の攻撃を組み合わせた複雑な攻撃手法

- 物理機器等からの情報取得
- ハードウェアのリバースエンジニアリング
- ソーシャルエンジニアリング

4．製品動向

- 昨年は「可視化」を目的とした製品が多かった。今年は「自動化」を目的とした製品が多い。

昨年

可視化

- ネットワーク上の不審通信
- クラウドサービスの利用
- ウィルスの動き

今年

自動化

- アラートと脅威情報の紐づけ
- アラートに基づくログ自動取得
- 脆弱性 自動診断

背景	セキュリティ技術者不足、人財の流出 →人に頼らない手段

5．IT動向（デジタルトランスフォーメーション）

- 世界が変わり始めている（もう変わっている）

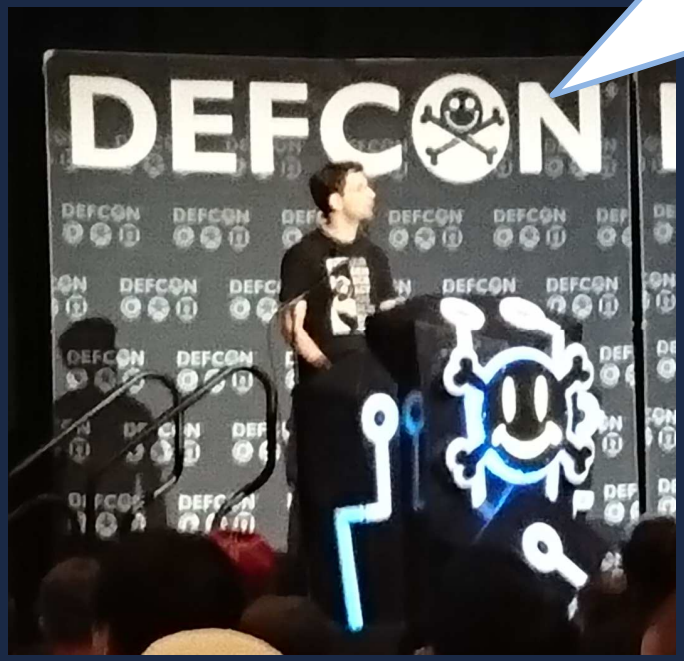
日本にいると気が付かない・・・

タクシー	▶	Uber
在宅時に配達	▶	冷蔵庫に配達 車のトランクに配達
現金・カード	▶	スマホのアプリで支払

共通点

ITを駆使することで、既成概念を破壊し、顧客の利益・利便性を最大化しようとしていること。
課題は多いが、デメリットよりメリットの総量が多い。

6．人脈形成の大切さ



これだけITが発達したのに
なぜこれほど人が集まるのか?
それは直接人と人が会うことでしか
共有できないものがあるからである。

Mr. Jeff Moss

DEF CON 25 presentation「Welcome to DEFCON25」より

表彰式後のティータイムにぜひご参加ください。

（参考）Reference

- Black Hat USA 2018
  Briefing プレゼン資料
  https://www.blackhat.com/us-18/briefings/schedule/index.html
  ・資料が公開されていないBriefingもある。
  ・講演では投影されていたスライドが削除されている部分がある。

- DEF CON 25
  presentation プレゼン資料
  https://media.defcon.org/DEF CON 26/DEF CON 26 presentations/
  ・一つ上の階層の「DEF CON 26」配下に、presentation以外の資料が多数ある。

※どちらも昨年度以前の資料も公開されている。