CCS 2020 会議報告

CCS 2020 概要

CCS とは

The ACM Conference on Computer and Communications Security（CCS）は ACM が主催する情報セキュリティに関する国際会議である．IEEE Symposium on Security and Privacy（S&P），USENIX Security Symposium，The Network and Distributed System Security Symposium（NDSS）と今回紹介する（ACM-）CCS はセキュリティ 4 大国際会議と呼ばれ，サイバーセキュリティや暗号応用などに関するレベルの高い学術発表が多くなされる．その中でも CCS は例年最も規模が大きく，近年では毎年 100 件以上の発表が行われ，1,000 名を超える参加者が熱心に議論を重ねてきた．

CCS 2020 の全体概要

2020 年の CCS（CCS 2020）は 2020 年 11 月 9 日から 13 日の 5 日間（11/9 は Pre-Workshops，11/13 は Post-Workshops で，本会議は 11/10 ～ 11/12 日の 3 日間），アメリカのフロリダ州で開催される予定であったが，新型コロナウイルスの影響で他の多くの国際会議と同様にバーチャル開催となった．ここ数年は論文投稿件数が増えていることから，今年も分野ごとにチェアが選出され，論文投稿も 1 月および 5 月の 2 回受け付けられた．CCS に限った傾向ではなく他の 4 大会議も同様であるが，最終的に採録となる場合でも Minor/Major – Revision を経るケースがほとんどで，論文も 2 段組 12 ページが基準で短くはないなど，国際会議ではあるが論文誌に近い採択プロセスを採っている．採択率はほぼ例年通りの 17%（715 件投稿・121 件採録）であった．参加者数は明かされなかったが，オンライン開催となり参加費が安くなった（例年は 1,000USD 以上であるが今回は 35USD）こともあって，例年よりは増加したと思われる．参考までに，2020 年 5 月にバーチャル開催された S&P 2020 は参加者数が前年の 3 倍になっていた．

バーチャル会議の開催形態はさまざまで，本稿筆者もこれまでにオンライン開催された国内／国際会議にいくつか参加してきたが，CCS は**図 -1** に示す Gather Town（https://gather.town/）というオンライン交流ツールと Zoom を組み合わせた形で開催された．Gather Town に講演会場およびロビーが用意され，講演会場では特定の操作を行うと発表が行われている Zoom 会議が起動し，マイクの近くに行くと質問ができるようになっていた．ロビーにはスポンサーブース，コーヒースペース，ヘルプデスクなどが設置されており，アバターに近づくとその人との Zoom 会議が起動して交流できるようになっていた．本稿筆者も知り合いを見つけて多少話しかけてみたりはしたが，現地開催ほどの交流は生まれなかったというのが正直なところである．ただ，これは Gather Town の問題というよりはオンライン会議の限界のようにも思え，単に Zoom 等を利用して発表（場合によっては録画された動画）を視聴するという会議形態に比べれば今後の可能性を感じるスタイルではあった．ただし後述するように，参加者に慣れないツールの利用を強いて会議の価値を向上させることと，会議を安定的に運営することとのトレードオフは存在するように感じている．

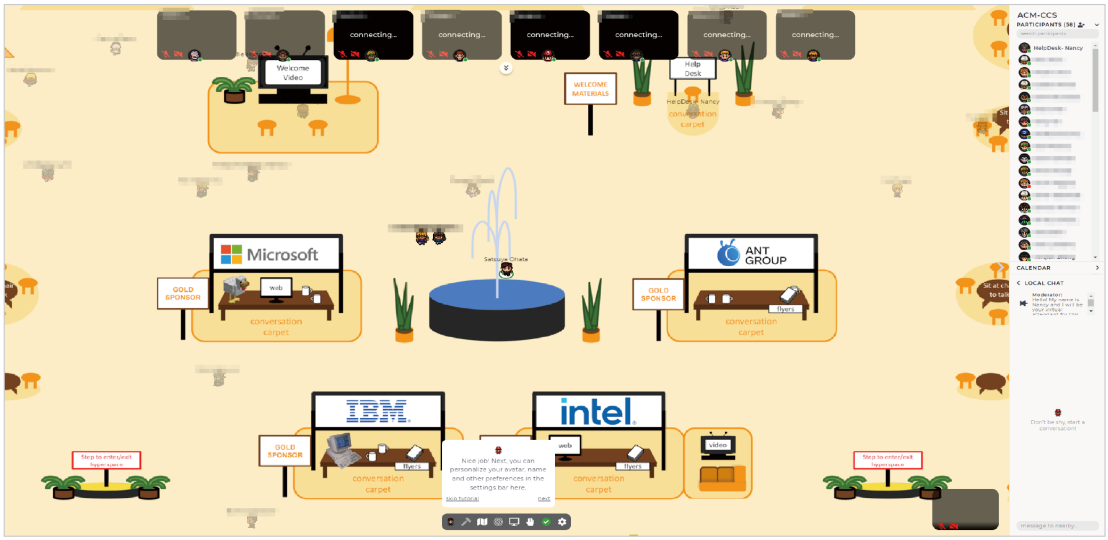

図 -1　Gather Town を利用して行われた CCS 2020 の休憩時間（ロビー）の様子

CCS 2020 研究発表概要

メイン会議

メイン会議では 121 件の論文発表のほか，2 件の招待講演が行われた．招待講演は Wenke Lee（Georgia Tech.）による「Machine Learning and Security : The Good, The Bad, and The Ugly」，および Alex Stamos（Stanford University）による「Realistic Threats and Realistic Users : Lessons from the Election」であり，オンライン講演であったが質疑も活発に行われた．

前述した通りであるが，CCS 2020 は査読において投稿論文を 9 つの分野に分け，各分野で選定が行われた．今回の分野分けは

- Applied Cryptography
- Blockchain and Distributed Systems
- Formal Methods and Programming-Language Security
- Hardware Security and Side Channels
- Machine Learning and Security
- Network Security
- Privacy and Censorship
- Software and Web Security
- Usability and Measurement

であった．この分類を見ても扱っているテーマの広範さが理解いただけるのではないだろうか．暗号応用やハードウェア，ネットワークといった伝統的なテーマもあれば，ブロックチェーン，機械学習，ユーザブルセキュリティなど比較的新しいテーマも一分野を確立している．また，近年では分野融合も目立つ．実際 CCS 2020 では，サイドチャネル攻撃（電力消費量などの物理量を用いて機密情報を盗む攻撃）を用いて DNS キャッシュポイゾニング攻撃の成功率を大幅に向上させるという，ハードウェアセキュリティとネットワークセキュリティにまたがるテーマを取り扱った結果が Distinguished Paper Award に選定されている．本レポート執筆者は暗号応用，特にマルチパーティ計算（あるいは秘密計算）と呼ばれる，複数のパーティが各々のデータを明かさずに何らかの処理を実行する技術を専門に研究開発を行っているが，ここにも分野融合の波が来ている．たとえば，CCS 2020 においては TensorFlow で書かれた機械学習を実行するコードを，最適化済みのマルチパーティ計算用のコードに自動変換するコンパイラの発表が Microsoft Research から行われた．これは暗号と機械学習の融合テーマであるが，このような 1 つの分野に閉じない研究成果が増加している．また，分野融合や論文誌と同等の採択プロセスになっていることとも関連するが，非常に高い完成度と重い実装エフォートを要求する傾向が強まっている．その結果，どちらかというと理論寄りの結果が多い暗号分野の国際会議（国際暗号学会 IACR が主催する CRYPTO 等）と比較すると，論文著者数の増加傾向が顕著であるように感じている．GAFA の研究グループのような大所帯であれば問題ないであろうが，筆者が所属しているような小規模な研究開発チームや，あるいは多くの日本の大学の研究室のような環境では，テーマによっては戦略なしで太刀打ちするのが徐々に難しくなってきているのかもしれない．

プレ・ポストワークショップ

CCS は例年，本会議の前後 1 日ずつに分野を絞ったワークショップを開催しており，他のセキュリティ 4 大国際会議と比較してこの数が多いという特徴がある．運営は各ワークショップが独立して行っており，プロシーディングスの有無や発表形態などは統一されていない．年によって開催数は異なるが，2020 年は Pre，Post ともにともに 6 つのワークショップが開催され，クラウドセキュリティ，IoT セキュリティ，AI セキュリティ，差分プライバシなどが取り上げられた．すべてを列挙するのは避けるが，興味のある読者は CCS 2020 の Web サイトを参照されたい．

まとめ・感想

情報セキュリティに関する国際会議 CCS 2020 の概要を紹介した．オンライン開催ではあったが成果のレベルは安定して非常に高く，参加を勧められる会議である．会議運営に関しては，Gather Town を採用していたのが非常に印象的である．本レポート執筆時点（2021 年 1 月）では他分野の会議でも採用実績があるようであるが，当時は非常に野心的な試みであったように思う．ただ，操作にはある程度の慣れが必要で，参加者間のインタラクションはともかく，プレゼンテーションに関しては非常にトラブルが多かったのも事実である．機材やシステムのトラブルで規定の時間に実施できなかったセッションに関しては，最終日の最終セッションにパラレル数を増やして実施するという措置が取られた．この点に関しては発表動画を事前提出し，それを視聴するスタイルを基本にするほうが安定性は高まりそうで，ライブ感との両立という意味では運営側にとって悩ましい問題である．また，日本からのアメリカ時間の会議に参加すると基本的には昼夜逆転生活になってしまう．今回の CCS は 5 日間連続で 23:00 〜翌 6:00 の参加となったため，事前の調整も含めて体力面が非常にシビアであった．オンラインではあるが会議が開催され，それに参加できるだけでも文句を言えない情勢ではあるが，可能な限り早く現地開催の会議に参加できる日々が戻ることを願うばかりである．

■大畑幸矢
（（株）デジタルガレージ DG Lab）