ニューヨークだより番外編 2017 年 11 月

Healthcare Security Summit: New York City (2017/11/14-15)
(https://events.ismg.io/event/healthcare-security-summit-new-york-city/)

中沢　潔
JETRO / IPA New York

下記に概要等を記しますが、所感としては、(ヘルスケアに限らない内容が多かったことに加えて)
○あるスピーカーがサイバー被害への Response Plan を作成しているかと聴衆に聞いたところほとんど手が挙がらなかったのは意外でした。
○FBI 出身の弁護士、軍出身の CISO 等、人材の流動性を感じました。

(本イベントで語られていたことの中で印象に残ったこと)
○本イベントは 3 年前から開始。
○ヘルスケアにおけるサイバー被害は患者等のデータ漏洩(data breach)。
○ヘルスケア分野でサイバーセキュリティの優先度が上がらない理由
・安全性(Safety)と信頼性が優先される
・これまでサイバー攻撃自体で死亡事故が起きたことはない
・新しいチームが必要(コストが増える)　等
○何でも良いから情報共有組織に入って欲しい。色んな情報が得られて有益。(企業にとっては、被害発生が自動的に規制当局に共有されることには抵抗があることは理解。)
○パスワード認証は廃れており、今後は行動ベースの認証の普及がキーになる。FIDO　Alliance (First IDentity Online、ファイド、生体認証等、)や OASIS といった組織が重要になる。
○insider にも気をつけることが必要。内部活動では、IT sabotage(故意の損害)が最も多い。次に多いのが営業部分による情報窃盗(営業部門は新しい技術、製品情報に触れやすい)。派遣社員やボランティアも注意。対策として、社の信頼度の計測 (Measuring Trust)、適切な権限付与、行動モニタリングを行うことが重要である。
○リスクベースのセキュリティ対策が重要であり、CISO は CFO や PR 担当者

ともよくコミュニケーションして、各社の制約や対応方針を理解しながらセキュリティ対策を考えることが重要である。

○GDPR の影響は大きいと思う。

○情報管理手法としてブロックチェーンは素晴らしいが普及にはもう少し時間がかかるのではないか。

（興味深かった組織、企業）

○HiTrust Alliance (https://hitrustalliance.net/)

新たなサイバー攻撃になり得る構成要素（indicators）を事前に検知し、DHS、ヘルスケア関係企業等に共有する組織。WannaCry についても Windows の脆弱性公表後に WannaCry に含まれていた構成要素を検知して DHS に報告していた。

○Attivo Networks (https://attivonetworks.com/)

罠や仕掛けによりハッカーの攻撃情報を入手し対応策を講じる。

○Illumio (https://www.illumio.com/home)

重要なアプリケーションや規制に絞り、それらに関して顧客に問題が発生した際、数分で解決する。

○SecurityScorecard (https://securityscorecard.com/)

取引先も含めた企業のセキュリティリスクをレーティング。