2017年度 CYBEX Working Group 活動報告

宮本 大輔 (daisu-mi@is.naist.jp)　　門林 雄基 (youki-k@is.naist.jp)

2017年12月31日

目 次

1 CYBEX WG 2017年度の活動

近年，様々なサイバーセキュリティ技術が開発されており，その普及は急務である．これまでの CYBEX WG は，様々なサイバーセキュリティ技術の先端的研究成果や運用によって得られた知見について，国際標準化活動などの様々なチャネルを通じ，多くのステークホルダーに啓蒙することを目的とした活動に従事してきた．

今年度の主な活動内容は以下の通りである．

- サイバーセキュリティ情報交換に関する規制動向調査
- サイバーセキュリティ標準を学ぶための教材開発

2 サイバーセキュリティ情報交換に関する規制動向調査

サイバー犯罪に用いられる技術，それに対抗するサイバーセキュリティ技術は著しく進歩している．その一方で，サイバーセキュリティに関する運用では，組織の壁を越えた情報共有が求められる．この取り組みについて，欧州では NIS Directive によって，米国では CISA によって情報共有を推進している．この動向について調査を行った．

2.1 NIS Directive

NIS Directive（The Directive on security of network and information systems) は，欧州委員会が2016年7月に採択し，2016年8月に発効した指令である．EU の加盟国はこの指令をもとに国内法を改正することになるが，その期限は 2018 年 5 月である．ネットワークと情報システムのセキュリティの高度化を達成を目的とし，大きく 4 つの規約によって説明される．

- 加盟国の国家レベルにおけるサイバーセキュリティ機能の向上: 加盟国は戦略的目標や優先順位，ガバナンスの枠組みを含む NIS 戦略を採用する．また，NIS に対する備え，対応，回復の面からの対策をはかり，公的機関と民間を協力させる．また，セキュリティに関する国家レベルの管轄局をつくり，コンピュータセキュリティインシデント対応チーム（CSIRT）を指定する．
- 欧州域内での協調: 国家レベルの CSIRT 同士のネットワークの創出，これを用いた情報共有を行う．また，国家間でインシデント対応をするため

の協調作業の支援を行う．これらを通じ，NIS に関する協調作業グループを創出する．

- 基本サービス事業者 (OES) の義務: OES (Operators of Essential Service) は，電気，ガス，水道，交通，ヘルスケアなどの国民の生活にとって不可欠なサービス事業者を示す．各国はこの OES を識別し，リスクに応じた適切なセキュリティレベルを確保するための最小限のセキュリティ対策を行う．また，提供されるサービスを支える IT システムへのインシデントの影響を最小化するため，インシデントの通知が義務付けられる．また，担当当局には，OES のセキュリティ監査し，証拠を確認する能力があることが求められる．
- デジタルサービス事業者 (DSP) の義務: DSP (Digital Service Provider) も同様に，リスクに応じた技術的・組織的に最低限のセキュリティ対策をとるよう促される．また，インシデントの通知に関しても，フレームワーク指令 (2009/140/EC) の第 13 条 (a) により，IT システムに対するインシデントの悪影響を防ぎ，最小限にとどめるよう指示されている．

フレームワーク指令についての説明は，ENISA (European Network and Information Security Agency, 欧州情報セキュリティ庁）によるガイドライン [1] が詳しい．ENISA 及び欧州委員会への報告の必要があるインシデントは，以下の閾値で考えることができる．すなわち，

- 影響時間が 1 時間以上であり，影響をうけるユーザが 15%以上のとき
- 影響時間が 2 時間以上であり，影響をうけるユーザが 10%以上のとき
- 影響時間が 4 時間以上であり，影響をうけるユーザが 5%以上のとき
- 影響時間が 6 時間以上であり，影響をうけるユーザが 2%以上のとき
- 影響時間が 8 時間以上であり，影響をうけるユーザが 1%以上のとき

[1] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-on-incident-reporting-v-2-0

である．これらは OECD ガイドラインに由来している．

2.2 CISA

米国におけるサイバーセキュリティ情報共有法は CISA (Cybersecurity Information Sharing Act) である．サイバーセキュリティの脅威に関する情報の共有を強化し，米国のサイバーセキュリティを向上させるという目的の本法律は，2015 年サイバーセキュリティ法として発効された．

本法では，非連邦および連邦機関の間で法の下で共有することができるサイバー脅威情報の種類を指定する．また，情報および情報システムに対する脅威を記述または特定するためにそのような情報が必要とされる状況に限り，法律に基づく共有を限定する．これらはプライバシー保護にも対応したものである．NIS Directive が欧州と OES 及び DSP 間となっているのに対し，CISA では連邦政府と非政府機関（地方政府）と広くなっている一方で，第 106 条 (c)(1)(A)(B) にあるように情報を共有する義務，受け取った情報に基づいて行動する義務は負わない．

なお，本法律は米国 DHS がガイドラインを提供しており，有名な STIX フォーマット及び TAXII プロトコルによって自動的な脅威インジケータの共有を促進することが明記されている．

3 サイバーセキュリティ標準を学ぶための教材開発

自システムへの脅威に対応するためにサイバーセキュリティの管理策をまとめた標準は複数存在する．The Critical Controls for Effective Cyber Defense (CSC) [2] は既知のサイバー攻撃から効果的に資産を防御するために，20 個の管理策に絞った内容になっている．管理策は最初に実施しなければならない管理策（CSC1〜5）とそれ以外（CSC6〜20）に分類され，管理策の優先順位がわかるようになっている．20 個の管理策はさらにサブ管理策に細分化されており，具体的な内容が記述されている．管理策の有用性は CIS コミュニティ

[2] https://www.cisecurity.org

脅威モデル [3]とセキュリティベンダーが公表する脅威レポートを活用し，確認している．CIS コミュニティ脅威モデルではサイバーキルチェーンの攻撃段階を横軸，NIST フレームワーク [4]の防御段階を縦軸にしたマトリックスを定義している．CSC の各管理策はマトリックスのいずれか 1 つ以上のセルに対応することができる．ベライゾン社 [5]及びシマンテック社 [6]等が公開している複数の脅威レポートから得られる最新の攻撃手法が CSC の管理策で適切に防御できるか分析している．分析により，有効性の確認及び管理策の改善を実施することで最新の脅威にも適切に対応できるように整備されている．

これらの標準はセキュリティにおいて重要な意思決定をする上で非常に役立てられ，海外のセキュリティ業界では業界標準として受け入れられている．一方で，我が国のセキュリティオペレータも同様に重要な概念であるため，これを学ぶ必要が認められる．そこで，被教育者の学習意欲を維持・向上させるため本ツールに以下のようにゲーミフィケーション・フレームワークを適用した．

- プレイヤーの分類: 本ツールはサイバー攻撃及び対策について専門的な用語等を使用するため，プレイヤーの他にゲームマスターを追加した．ゲームマスターはセキュリティ分野に知見を有する者が担当する．
- 目的・ゲームコンセプト: 様々なサイバー攻撃手法に有効な対策を理解する．
- 目標: 攻撃を防ぐための防御カード選択し，高ポイントを得る．
- 可視化・フィードバック: 攻撃・防御手法をカードにより可視化し，ポイント加減算により優劣を判定するためスコア表に得点を記録する．
- ソーシャルアクション: サイバー攻撃への対策の有効性を口頭で説明することで他プレイヤーに理解させる．
- プレイサイクルデザイン: 初級者でもわかりやすいルール設定にし，ターン毎に手持ちの防御カード枚数が増減する仕組みとする．
- 改善・運用: 攻撃カードセットを 2 種類用意し，プレイヤーの能力に応じた難易度の攻撃カードセットを使用する．

防御カードは CSC のサブ管理策の内容をカード内に収まるようにまとめ，記載した．CSC のサブ管理策は対策の難易度から標準的な対策と高度な対策の 2 つに分類される．高度な対策は組織内に高度な知見を有する人材が存在することを条件としていることから，標準的な対策のみをカード化した．図 1 に防御カードのイメージを示す．CSC の管理策は重要度に応じて最初に実施すべき管理策とそれ以外に分類される．最初に実施すべき管理策を出した場合はそれ以外の防御カードを出した場合よりも 2 倍の得点を獲得できることとした．優先度の識別のため，優先度の高いカードに識別子を付加した．カードには CSC のカテゴリとサブ管理策の記述を簡略した内容を記述した．プレイヤーはこれらの内容から攻撃カードへの対応の可否を判断できる．

攻撃カードは一般的な攻撃手法（Type A）及びサイバーキルチェーンに基づく手法（Type B）の 2 種類のカードセットにまとめた．一般的な攻撃手法の内容は CSC Appendix B の内容をカード内に収まるようにまとめた．CSC 開発時に管理策の脅威への網羅性は Type A の攻撃手法を用いた紐付けを実施することで確認されている．Type A のカードは抽象化された内容が記述されているため，対応可能な防御カードは多く存在する．プレイヤーは手持ちカードから適切な防御カードを選択し易く，ゲームの難易度は低く設定できる．

サイバーキルチェーンはサイバー攻撃の目的を達成するまでの段階を定義している．CSC の脅威モデルはサイバーキルチェーンを含むマトリックスを使用しているため，サイバーキルチェーンとの相性が良い．MITRE 社はサイバーキルチェーンの各段階における具体的な攻撃をまとめた攻撃ライブラリ（ATT&CK）[7]を公開している．攻撃カードの Type B に記載する攻撃手法を検討する際に活用することとした．

[3] https://www.cisecurity.org/white-papers/cis-community-attack-model

[4] https://www.ipa.go.jp/files/000038957.pdf

[5] http://www.verizonenterprise.com/DBIR

[6] https://www.symantec.com/ja/jp/security-center/threat-report

[7] https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats\%20with\%20att\%26ck-based-analytics.pdf

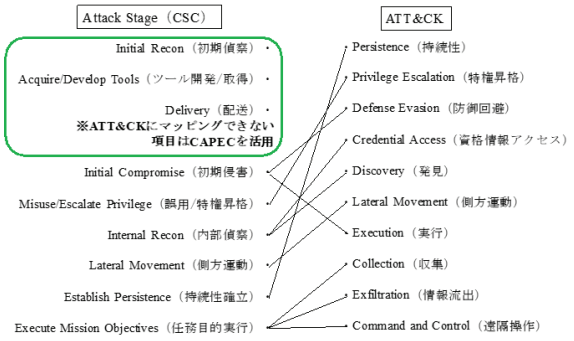

図 1: CSC Attack Stage と ATT&CK の関係

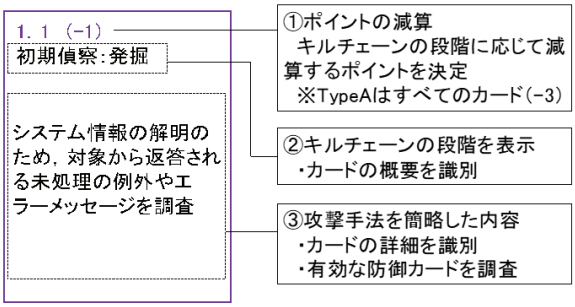

図 2: 攻撃カード Type B のイメージ

図 1 に CSC Attack Stage と ATT&CK の関係を示す．ATT & CK は攻撃を 10 個の段階に分類しているが CSC の脅威モデルで定義されている脆弱性調査に関連する内容は含まれていない．このため，同じく MITRE 社で公開している攻撃ライブラリである CAPEC [8] を活用し，ATT & CK では分類できない CSC のサイバーキルチェーンでの攻撃段階に該当する内容をカード化することとした．図 2 に攻撃カード Type B のイメージを示す．防御カードを提示できなかった場合の減算ポイントを明記している．減算ポイントはサイバーキルチェーンの段階により大きくなるように付加した．カードにはキルチェーンの段階及び攻撃内容を簡略化し，記載した．プレイヤーはこれらの内容から対応可能な防御カードを選択することができる．攻撃カードの内容は具体的であり，対応可能な防御カードが限定されるため，ゲームの難易度を高く設定することができる．

より詳細な内容については，文献 [1] を参照されたい．

[8] https://capec.mitre.org

4 国際標準化団体における CYBEX WG の活動

CYBEX WG に参加しているメンバーらは，サイバーセキュリティに関する国際標準に関する議論や，標準化提案，その支援を行ってきた．この結果，2017 年には IETF において 2 件の，ITU-T において 1 件の提案が結審した．それぞれの内容の詳細については，RFC 8134 [2]，RFC8274 [3], X.1212 [4] を参照されたい．

5 今後の予定

今年度は標準化活動を通じ，あるいは標準化された技術の新たな利用方法を考えることにより，幅広いステークホルダーにセキュリティに関する知識を啓蒙していく研究を行った．来年度も継続し，CYBEX WG のみならず他の WG，あるいは全世界で創出される素晴らしいセキュリティ技術を，より多くのステークホルダーに広めていく活動を継続していきたい．

参考文献

[1] 近江谷 旦, 宮本 大輔, 門林 雄基, “サイバー攻撃の脅威に対応する具体的な管理策を学ぶための教育ツールの検討,”, 信学技報, *vol. 117, no. 316, ICSS2017-40, pp. 11-16*, 2017 年 11 月.

[2] Christopher Inacio and Daisuke Miyamoto, *“Management Incident Lightweight Exchange (MILE) Implementation Report,”*, *IETF RFC8134*, March 2017.

[3] Panos Kampanakis and Mio Suzuki, *“Incident Object Description Exchange Format Usage Guidance,”*, *IETF RFC8274*, November 2017.

[4] X.1212, *“Design considerations for improved end-user perception of trustworthiness indicators,”*, *Question 4, Study Group 17, ITU-T*, March 2017.