第１回次世代型セキュリティアーキテクチャ検討会 議事概要

１．　**日時**：令和４年２月24日(木) 13:00～15:00

２．　**場所**：Web 会議による開催

３．　**出席者**：

（委員）

上原 哲太郎	立命館大学　情報理工学部　教授
河野 省二	日本マイクロソフト株式会社　技術統括室　チーフセキュリティオフィサー
木村 滋	シスコシステムズ合同会社　セキュリティ事業担当　エバンジェリスト/アーキテクト
後藤 厚宏	情報セキュリティ大学院大学　学長　※1
崎村 夏彦	OpenID Foundation　理事長
田原 祐介	株式会社ラック　インテグレーション推進事業部 インテグレーションサービス＆企画部　部長
楢原 盛史	タニウム合同会社　チーフ・IT・アーキテクト
名和 利男	株式会社サイバーディフェンス研究所　専務理事／上級分析官　※2
前田 典彦	株式会社ＦＦＲＩセキュリティ　社長室長
丸山 満彦	PwC コンサルティング合同会社　パートナー

（オブザーバー）

内閣サイバーセキュリティセンター（NISC）

高倉 弘喜　　国立情報学研究所

（デジタル庁（事務局））

戦略・組織グループ　セキュリティ危機管理チーム

（独立行政法人情報処理推進機構）

デジタルアーキテクチャ・デザインセンター

※1 令和４年３月２日(水)に個別ヒアリングを実施

※2 令和４年３月４日(金)に個別ヒアリングを実施

４．　　議事要旨：

・事務局より、資料１「サイバーセキュリティ戦略等」、資料２「ゼロトラストアーキテクチャ適用方針のガイドライン資料」、資料３「常時診断・対応型セキュリティアーキテクチャに関する技術レポート（仮称）について」について説明。

・「ゼロトラスト適用ガイドライン」に関する自由討議において、主に以下の発言。

・ゼロトラストにおいてはそのメリットとデメリットの両面が存在するため、並べて記載をする必要がある。各省庁にはインターネットにつながる前提ではなく、安定性が求められるようなシステムや境界型防御で成り立っているシステムもあり、スコープの明確化が必要。

・ゼロトラストはモニタリングを手厚く行うことになる。また運用を外注できないケースもあるため、運用負荷が上がる可能性があり、運用を視野に入れた原則の策定が必要。

・ゼロトラストは北極星であり、当面は Trusted 環境が残存する。特に金融機関などでは Trusted 環境についてはスコープ外とする意識が強いが、もし Trusted 環境を残すのであれば、リスクを洗い出し、トップマネジメントへの報告と承認が必要となる。

・Amazon、Microsoft、Google、Cisco などを中心に「OpenID Continuous Access Evaluation Profile 1.0」「OpenID Shared Signals and Events Framework Specification 1.0」等ゼロトラストに役立つ内容を推進しており、本取り組みの参考になると思う。

・ゼロトラストで情報の保護を行うことができるわけではなく、目的の明確化をした上で、対象範囲を明確にしていく必要がある。

・境界防御とゼロトラストを対立的に扱っているが、ゼロトラストアーキテクチャを用いた境界防御の考え方も出始めており、今後構図が変わってくる可能性があるため、ゼロトラストへの移行を強調しすぎる必要はない。

・ゼロトラストはキーワード先行となる場合があるが、実際は実装が非常に難しい。構築してからがゼロトラストの始まりであることを一つのポイントとして明記するのがよい。

・海外の民間企業の事例ではゼロトラスト構築後にアクセスした際、6 時間継続してアクセスしているとマルウェアに感染するといったケースがある。常時アセスメントが重要となる。

・現在は、ゼロトラストと境界防御の混在環境がスタンダードと言える。また、移行に関しても何かしらの示唆があるとユーザ目線のヒントとなる。

・ネットワークを利用したゼロトラスト、例えばマイクロセグメンテーションや SDN、IBN とい

ったネットワークを利用したコントロールについてもう少し触れてもらいたい。

・ユーザの利便性という観点でも負荷が上がる。ユーザの負荷を軽減するための取り組みなども触れるとよい。

・運用負荷が上がるため、言われてもできないという状況を作らないように注意しないといけない。

・アセットの 100%の管理は難しく、昨今ではクラウドの利活用などさらに困難さを増している。覚悟を持って実施していく必要がある。

・デジタルアイデンティティについてはジョブ型雇用形態となっていない日本では難しいと考えられる。また Security Clearance の対応もできた上での実現性という話になる。

・JNSA のアイデンティティを扱うワーキンググループが ID 管理等に詳しく、連携するのもよいと思う。

・ゼロトラストアーキテクチャを導入した組織の成功例などを元に議論を行う方が、理解しやすい。

・全体的にサイバーリスクを発見できる前提となっているが、潜在化したリスクを見つける点について触れるべきであり、しつこいくらいの権限確認、認証と認可をデバイスや認証に対して実施するなどの議論が必要。

・ゼロトラストの適用に伴い、既存の業務の変更が大きくなるため、体力また意識の変容が必要となる。読者側に覚悟が必要なため、その旨も明記する必要がある。

・アセットやネットワークアカウント、ワークフロー、データなどの守るべき対象は明確に定められているため、齟齬が無いように説明する必要があり。加えて、オペレーショナルフローのようなサービスも含める必要があり、入口出口だけではなく、一連の流れを監視する事が必要。

・アセットやリソースはサイバーセキュリティ戦略などの定義と整合性を取る必要がある

・ゼロトラストの概要の説明を丁寧にする必要がある。役割ベースから属性ベースにシフトする前に、何故シフトする必要があるのか、多要素認証等の追加認証が何故必要なのかなど。

・リスクベースという観点では脅威インテリジェンスは必要な観点であり、インテリジェンスのポリシーエンジンが重要となる。また民間の事例も合わせて紹介するのがよい。

・モニタリングは米国の eDiscovery に基づき、各アクティビティに対して時間軸での保存と迅速な閲覧が可能な事としている。

・成熟度が重要となる。SP800-171 や Risk Management Framework などをみても、成熟度は 6 割程度。ガイドラインは理想論であり、チャレンジングな内容となる。例えば API の暗号化など、証明書の管理等が発生する事を踏まえると困難である。相当な覚悟を持って取り組む必要がある。

・「常時診断・対応型セキュリティアーキテクチャに関する技術レポート（仮称）について」に関する自由討議において、主に以下の発言。

・理想的なコンフィグレーションマネジメントも視野に入れるとよい。また IT 資産の脆弱性に関しては人間のミスは関連しない。また構成管理は状態の管理となり、良し悪しの区別をつけるものではない。これらは学習の中で作っていくフィードバックループが理想的な形だと思われる。

・既に SIEM を導入している企業もあるため、他システムへのデータの提供について検討した方がいい。

・海外の AWARE のスコアリングは常時チェックかけており、スコアと ABAC を連携してゼロトラスト認証をかけるというのが最先端の取り組みとなっている。全体としては CRSA スコアと ABAC の連携を紐づけるといい。

・目指すべき像は静止点ではなくムービングターゲットであることを意識する必要がある。よって、うまく改善しながらスパイラルアップしていくことが重要。

・元々の SOC や NOC といった部分との役割分担について明確化していく必要がある。

・当初から有事の際の対応などを盛り込んだ議論を行う必要がある。

以上