第2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3月15日(火) 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　※1
後藤 厚宏	情報セキュリティ大学院大学　学長
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
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）

（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17日(木)にメールにてコメントを受領

４．　　議事要旨：

・事務局より、資料１「ゼロトラスト・アーキテクチャ適用方針について」、資料３「常時リスク診断・対処（CRSA）の導入に関する技術レポートについて」、資料５「CRSA の実装を見据えた今後の対応方針ついて」について説明。

・「ゼロトラスト・アーキテクチャ適用方針について」に関する自由討議において、主に以下の発言。

・ガイドラインの記載にはアクセスを受ける資産以外に、組織内のリソースにアクセスを求めるサブジェクトの評価も重要になるが、そのサブジェクトに関する記載がなかったため、設ける必要がある。

・「資産の把握」の「把握」という用語はガイドライン等の文書では利用しない。「識別」や「特定」といった次の作業プロセスにつながる用語に変更する方が適切と考える。

・言葉の定義が不明瞭な個所や、ゆらぎが見られる。例えば「きちんと」という言葉は定性的な表現となるため、ガイドライン上では利用を避けた方がよい。「リソース」という言葉が複数の意味で利用されている。言葉については見直す必要がある。また、「ジャーニー」という言葉への理解が得られない可能性がある。読み取り方が読者によって変わるため、利用を避けた方がよい。

・資産の管理と特定・識別・評価では地方の役所に見られるシャドーIT の問題につながる。そもそも地方の役所ではゼロトラスト・アーキテクチャ適用の前段で躓く状態だが、この施策によりシャドーIT の問題を浮かび上がらせることが可能となる。

・BYOD の記載が見られなかった。各省庁では公用のデバイスより BYOD の利用の方が多いというデータもあるため、含めることを検討する方がよい。

・ゼロトラスト・アーキテクチャに向かった結果どういう変化が起こるのかの記載があった方がよい。現在のシステムのイメージとゼロトラスト・アーキテクチャ適用後の世界をイメージしてもらう必要がある。

・「図１：ゼロトラストのコア論理コンポーネント」では厳密なゼロトラスト・アーキテクチャの世界を表現できていない。テレワークやリモートアクセスのみが対象というように誤解を与える可能性がある。また実際にはアクセス要求に対して様々なインタラクションがある。例えばリスクベース認証では追加の要素を確認するなど。そういったインタラクションが表現できていない。

・ゼロトラスト・アーキテクチャの世界を理解するには様々な用語の説明が必要となる。現状の用語は少なく、もっと拡充させる必要がある。

・サブジェクトとオブジェクトは時として変化する。この全体を元にリソースの整理が必要となる。

・「図１：ゼロトラストのコア論理コンポーネント」では ID 管理が直接 PEP に向かっているが、本来であれば、その前段にエンティティ認証が入る。認証された結果ポリシー実行ポイントで制御がかかる。こういった仕組みが表現できていない。

・ゼロトラスト・アーキテクチャを適用困難な従来システムの利用を継続しなければならない事情がある場合は、機能アップグレードするなどで、相互運用性を確保する努力を求めていることも必要と考える。

・適用(移行)プロセスにおいてはユーザーが困惑する可能性があるため、一時的に新旧システムを共存させるなどの移行期間などを設けるなど配慮も検討する必要がある。

・ゼロトラスト・アーキテクチャの周辺、例えば人事管理システムや ID 管理、資産管理、調達管理といった各システムとゼロトラスト・アーキテクチャとの関連が必要と思われる。

・ユーザーやアセットをゼロトラスト・アーキテクチャの原則に基づき管理することで、実際に管理している側の人々にも関係する内容として理解が得られる。

・用語含め、また全体を通して、言葉の使い方が粗く、見直しが必要である。書き手の中で定義を明確にして書き進めることを求める。

・ゼロトラストはコンセプトとアイディアのコレクションであり、サイバーセキュリティプランということもあり、システムデザインやアーキテクチャリファレンスではないが、設計者、導入検討者では常に実装方法を意識して考える。「Forrester's Zero Trust eXtended (ZTX)」のゼロトラスト適合技術エリア、1) Network security, 2) Data security, 3) Workload security, 4) People/workforce security, 5) Device security, 6) Visibility and analytics, 7) Automation and orchestration、は参考にできると思う。

・ゼロトラスト適用の事例を提示する。

・ゼロトラストに関連する民間企業で期待される DX 化の目的例は「システムのオープン化」「全体的なテレワーク適用」「Proxy のクラウド利用」「テレワーク端末のセキュリティ強化」「クラウド利用に適したネットワーク環境の変更」といったものが挙げられる。

・「境界型セキュリティ」「ゼロトラスト・アーキテクチャ（以降、ZTA)」の用語が定義されているが、ここは参照文献の定義を参照するべきと考える。

・記載のソリューションについては NIST SP800-207 では「インテリジェントスイッチ」「ルータ」「Firewall」「特殊用途のゲートウェイ」「ソフトウェアエージェント」「エンドポイント Firewall」「SDP」「低レイヤーのネットワークスタック」「SDN」IBN」というに合わせた記載の検討を求める。

・「常時リスク診断・対処（CRSA）の導入に関する技術レポートについて」に関する自由討議において、主に以下の発言。

・通常状態をベンチマークとして作り続け、アラートを上げる、その保存先が ASO であり、モデリングを ASO で回していく。また ASO レポジトリとダッシュボードのそれぞれの観点等を要約部分に記載した方が良いと感じた。

・米国 CDM にて定義のないネットワークセキュリティの範疇が現在定義されていない。ここについて検討が必要。

・スレットインテリジェンス等実際に起きている事象自体の深堀についても今後検討していく必要がある。

・海外の取り組みでは、CVSS では判別つかなかった場合に、「システムコンプライアンス(公開されている CIS ベンチマークの活用等)」、「特権 I D(最少特権モデルのモニタリング等)、パスワード(プレーンテキストによる保存等)」、「契約切れの証明書(証明書の失効ステータス等)」、「セキュアでない TLS や SSL(TLS1.3 以外や SSL3.0 以外)」という 5 つのトータルスコアで管理を行おうとしている。

・資料 3 については GSOC、政府情報システム管理データベース(ODB)など既存のシステムとの位置づけを整理する項目を追加すべきと考える。

・「2.1. 常時リスク診断・対処（CRSA）の位置づけ」について、現在の書き方だと CRSA は、ゼロトラスト・アーキテクチャを実現するための 1 要素としてだけとらえられてしまうため、前段に CRSA 自体の仕組みの説明が必要と考える。

・「(3) ネットワークで何が起こっているのか？ どのようなシステム間のトラフィックパターンやメッセージが発生しているのかを把握する」は意図が伝わりづらいため、記載を改める必要がある。

・「2.1. 常時リスク診断・対処(CRSA)の位置づけ」について「ゼロトラスト・アーキテクチャを構成している論理コンポーネント間の関係を示した概念図があるが、そもそもはゼロトラストが CDM を参照しうるという程度の関係であり、ゼロトラストに利用されるべく CDM が規定される、あるいは CDM の存在意義がゼロトラストに依拠している、といったものではないと考える。

・「図 2-2 ゼロトラスト・アーキテクチャの展開サイクル」は、ゼロトラストの実現方法なのでここでは不適切。第 2 回検討資料の「DADC における次世代型セキュリティアーキテクチャの検討について」の P10「常時診断を実現する日本 ToBe モデル概要」の図をなどに差し替えるのはどうか。

・「常時リスク診断・対処（CRSA）は、資産管理ツールなどを活用して資産の把握を推進することを目的としている。（2.4. ゼロトラスト・アーキテクチャの適用方針との関係（1）資産の把握について）」だと、CRSA の目的が資産管理だけのように見えため、「常時リスク診断・対処（CRSA）は、資産管理ツールなどを活用し、資産を把握して、3.2.1 に記載された（1）-（4）を実現することを目的としている」という記載に変えるのはどうか。

・「(2) 資産の状態確認 について」について、現在の記載では、CRSA として実現すべきことが伝わりづらい。属性ベースの認証・認可はゼロトラストで実現することで、CRSA としては、属性情報をゼロトラストに提供するという位置づけになると考えるため、そのことが伝わるように修正してはどうか。

・「3.1. アーキテクチャ全体」について、CDM の「Tools and Sensors」にあたる、ダッシュボードに取り込まれる一次情報（IT 資産情報、認証ログ、ネットワークログ、アラート情報、データ監査ログ、クラウド情報）がどこにあたるのかが明確でない。政府内の参照データベースシステム」単体、もしくは「政府内の参照データベースシステム」「政府外の参照データベースシステム」「府省庁の政府情報システム」がそれにあたるのであれば、それとわかるように明確に記述、表現するべきと考える。

・「3.2 ガバナンスレイヤー」について、ガバナンスレイヤーの記載についてはおおむね問題ないと考える。「3.2.2 対象領域（1）端末とサーバ装置等の管理」について、今後、監視対象を通信回線装置、その他機器（複合機や IoT 機器等)、クラウドに拡張することが必要であるため、そのことを明記すべきと考える。

・資産管理の把握の点について、脆弱性管理を追加し、機能要件だけでなく、実運用を見据え、運用が破綻しない運用要件の言及のご検討をお願いする。

・資産管理＋脆弱性管理が必要と判断される場合、米国の CISA の潮流なども鑑みて、「サイバー・ハイジーン」というキーワードを改めてご検討頂きたい。

以上