ゼロトラストセキュリティ対策の構築に係る調達仕様書

本仕様書は，常総市立小中学校ＩＣＴ環境更新事業におけるゼロトラストセキュリティ対策の構築（以下「本業務」という。）について，基本的な考えを示したものである。

したがって，本仕様書に明記していない事項でも，本業務の目的を達成するために，効果的な取り組みと認められるものは，上限額の範囲内で追加提案することも可能である。

１．本業務の概要について

（１）業務名

常総市立小中学校ＩＣＴ環境更新事業におけるゼロトラストセキュリティ対策の構築

（２）業務目的

校務支援システムのクラウド化を実施し，ロケーションフリーで校務系・学習系システムへ接続可能な環境を整備し，職員一人ひとりの事情に合わせた柔軟かつ安全な働き方を可能とするため，ゼロトラストの考え方に基づき，セキュリティ対策を講じる。

（３）業務概要

下記環境を構築するとともに，運用保守を実施すること。

①アクセスの真正性に関する要素技

・多要素認証環境の構築

・リスクベース認証の構築

・シングルサインオン環境の構築

②通信の安全性に関する要素技術

・通信経路の暗号化

・Ｗｅｂフィルタリング

③端末・サーバの安全性に関する要素技術

・アンチウイルス

・データ暗号化

・ＥＤＲ（Endpoint Detection and Response）

・ＩＤＳ/ＩＰＳ（Intrusion Detection System/Intrusion Prevention System）

・ＷＡＦ（Web Application Firewall Firewall）

図２　いわゆるゼロトラストセキュリティに関する要素技術

①アクセスの真正性に関する要素技術		
①-1	多要素認証	情報・データへのアクセスに対する認証に当たり、記憶（ID・PW等）、所持（端末の電子証明書、ICカード等）、生体（指紋、顔等）の３要素のうち、２つ以上の要素を求めることで、なりすましや不正アクセスを防止する技術
①-2	リスクベース認証	情報・データへのアクセスに対する認証に当たり、端末のIPアドレスや位置情報、使用されているWebブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める技術
①-3	シングルサインオン（SSO）	セキュリティが確保された複数のクラウドサービスを一回の認証でアクセス可能とすることで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術 ※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる
②通信の安全性に関する要素技術		
②-1	通信経路の暗号化	通信経路を暗号化することで、第三者により通信内容が盗み見られることを防止する技術
②-2	Webフィルタリング	マルウェアへの感染につながりうるセキュリティリスクの高いWebページへの接続を防止する技術 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある。ただし、同時に教育・学習目的外のコンテンツにはアクセスしない等の情報教育との併用が推奨される
③端末・サーバの安全性に関する要素技術		
③-1	モバイル端末管理（MDM） (Mobile Device Management)	端末等のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防止するとともに、紛失・盗難に遭った際は、データの遠隔消去等を行う技術
③-2	アンチウイルス	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術（ふるまい検知） ※OSとしてマルウェア感染リスクが低い仕組みとなっている製品もある
③-3	データ暗号化	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術
③-4	EDR (Endpoint Detection and Response)	パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術
③-5	IDS/IPS (Intrusion Detection System/Intrusion Prevention System)	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術
③-6	WAF (Web Application Firewall)	インターネットと繋がっているサーバ（Webサーバ）への外部からの攻撃を検知し、防御する機能。主に情報資産へのアクセスを取り扱うWebサーバとインターネットなど外部接続ネットワークとの中間に設置され、事前に定義した不正アクセスパターンとマッチングすることによりWebサーバへの不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする。

※これらは、「教育情報セキュリティポリシーに関するガイドライン」（令和4年3月改訂・文部科学省）において取り上げられているセキュリティ技術のうち、いわゆるゼロトラストセキュリティに関するもの中心に整理したものであり、今後の技術動向等により変化しうるものであることに留意。

（出典）https://www.mext.go.jp/content/20230308-mxt_jogai01-000027984_001.pdf
「GIGA スクール構想の下での校務 DX について　～教職員の働きやすさと教育活動の一層の高度化を目指して～」文部科学省　令和５年３月８日　GIGA スクール構想の下での校務の情報化の在り方に関する専門家会議

２．本事業の実施要件について

①機能要件

多要素認証	セキュリティレベルを向上させ，不正アクセスや情報漏洩のリスクを低減するため，端末ログオン時やシステムログイン時に顔認証等の生体認証を利用できる仕組みを導入すること。
リスクベース認証	ユーザーの行動や利用環境を分析し，不審なアクセスだと判断された場合にのみ追加の認証を求める仕組みを導入すること。
ＳＳＯ	一度のログイン認証で複数のアプリケーションやサービスへログインできる仕組みを導入すること。
通信経路の暗号化	機密性の高い情報資産を取り扱う情報システムに通信回線を接続する場合，必要なセキュリティ水準を検討の上，インターネットを通信経路とする回線の場合は通信の暗号化を行うこと。 出先にて利用する場合，認証による本人確認手段の確保と，通信する情報の機密性に応じて，データ暗号化，通信の暗号化等の必要な措置を取

	ること。
Web フィルタリング	インターネットへの接続に際しては，フィルタリングが可能なものを導入すること。また，Web フィルタリングに関しては，多様なカテゴリにより異なる制限が適応できるものを想定している。なお，校務系端末に導入すること。
ＭＤＭ	管理者が離れた場所からでも端末をロックする，あるいは必要に応じてデータの削除や端末の初期化を行うリモートワイプなどの仕組みを導入すること。
アンチウイルス／ＥＤＲ	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し，駆除する仕組みを導入すること。
データ暗号化	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し，アクセス権限が無い者の情報の閲覧・ 編集を制限する仕組みを導入すること。
ＩＤＳ／ＩＰＳ	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）又は遮断（IPS）する仕組みを導入すること。
ＷＡＦ	インターネットと繋がっているサーバ（Web サーバ）への外部からの攻撃を検知し，防御する機能。主に情報資産へのアクセスを 取り扱う Web サーバとインターネットなど外部接続ネットワークとの中間に設置され，事前に定義した不正アクセスパターンとマッチングすることにより Web サーバへの不正なアクセスを監視し，攻撃とみなしたアクセスをブロックする仕組みを導入すること。
ＳＯＣ	提案する学校ＩＣＴ環境において，ゼロトラストセキュリティに関する要素技術で示された対策だけでなく，復旧及び原因究明を迅速化する必要があると判断される場合は，監視対象について常時監視を行い，本調達で対象となる製品のメール，ネットワーク及びエンドポイントの全ての領域の相関分析が可能かつ対象製品から送信されたログ，データ，不審イベントを監視し脅威インテリジェンス，攻撃手法等と関連付けてインシデントと想定される事象の特定が可能な仕組みを導入すること。