政府情報システムにおける
ゼロトラスト適用に向けた考え方

2020 年 6 月

西村 毅[1]、満塩 尚史[1]、細川 努[1]、楠 正憲[1]、田丸 健三郎[1]、梅谷 晃宏[1]

要旨

パブリック・クラウドの利用、働き方改革、API による官民連携等が政策上の大きなテーマとなっているが、これらを推進するには、これまでの境界型セキュリティの考え方だけでは、その実現が困難である。

本文書では、境界型セキュリティの限界を示し、ゼロトラストと呼ばれるこれからのセキュリティの考え方を紹介し、政府情報システムにおけるゼロトラストの適用の取り組みを 1)パブリック・クラウド利用可能システムと利用不可システムの分離、2)システムのクラウド化徹底とネットワークセキュリティ依存の最小化、3)エンドポイント・セキュリティの強化、4)セキュリティ対策のクラウド化、5)認証、及び認可の動的管理の一元化、として記述している。

[1] 政府 CIO 補佐官

目次

1　はじめに

1.1　背景と目的

政府情報システムにおけるパブリック・クラウドの利用、府省 LAN の外部での活動がキーとなる働き方改革、デジタル・ガバメントにおける API による官民連携等が政策上の大きな実現目標となっていますが、これらを推進するには、これまでのセキュリティの考え方だけでは、その実現が困難であり、十分なセキュリティレベルを確保できない場合もあります。

ゼロトラストとは利便性を保ちながら、クラウド活用や働き方の多様化に対応するため、ネットワーク接続を前提に利用者やデバイスを正確に特定、常に監視・確認する次世代のネットワークセキュリティの考え方です。セキュリティ対策は単に技術やソリューションが進化するだけではなく、その考え方も技術の進化に適応させていく必要があります。

本文書は、境界型セキュリティと呼ばれる従来の考え方の限界を示した上でゼロトラストと呼ばれるこれからのセキュリティの考え方を紹介し、政府情報システムにおけるゼロトラストの適用の考え方をディスカッションペーパーとして取りまとめたものです。

1.2　用語

本文書において使用する用語は、表 1-1 及び本文書に別段の定めがある場合を除くほか、標準ガイドライン群用語集の例によります。その他専門的な用語については、民間の用語定義を参照してください。

表　1-1　用語の定義

用語	意味
境界型セキュリティ	境界線（ペリメータ）で内側と外側を遮断して、外部からの攻撃や内部からの情報流出を防止しようとする考え方。境界型セキュリティでは、「信頼できないもの」が内部に入り込まない、また内部には「信頼できるもの」のみが存在することが前提となる。防御対象の中心はネットワーク。
ゼロトラスト	「内部であっても信頼しない、外部も内部も区別なく疑ってかかる」という「性悪説」に基づいた考え方。利用者を疑い、デバイス（機器）を疑い、許されたアクセス権でも、なりすまし等の可能性が高い場合は動的にアクセス権を停止する。防御対象の中心はデータ、デバイス等のリソース。

２　境界型セキュリティとゼロトラスト

２．１　境界型セキュリティとは

これまでのセキュリティの考え方において基本となっていた境界型セキュリティとは、境界（ペリメータ）で内側と外側を遮断して外部からの攻撃や内部からの情報流出を防止しようとする考え方です。境界型セキュリティは「信頼できないもの」が内部に入り込まない、また内部には「信頼できるもの」のみが存在することが前提となります。

具体的には強固な壁をつくり安全な内側と危険な外側を分離します。

城の防御にも似た考え方であり、組織や利用者グループで安全な内側の世界を構築し、外部との接続を可能な限り制限することが基本となります。

境界型セキュリティはネットワークでのセキュリティ実装が基本であり、〇〇ネットワークといったセキュアなネットワークの構築が中心となります。

２．２　境界型セキュリティにおける防御の限界

城の防御が崩されるのは、外部からの攻撃が防御よりも強力な場合と、何らかの理由で内部に攻撃者が存在する場合です。

境界型セキュリティでは、全体をもれなく壁で覆うことを前提に、「壁を強固にすること」、「内部に攻撃者を侵入させないこと」を重視します。

しかしながら、「壁を強固にすること」には限界があり、進化を続ける技術の世界では、無敵の壁は存在しません。セキュリティベンダーの主張も、一定の侵入を前提としつつ、情報流出の防止や損傷の最少化に変化しています。特に通信の暗号化が普及することで、侵入するマルウェアの検出や流出する情報の検出も困難になってきています。

また、「内部に攻撃者を侵入させない」ためには外部と内部を遮断する必要がありますが、情報の厳密な遮断は利便性の観点から難しく、本来業務の生産性低下と運用負荷の増大を招き、逆にシャドーIT と呼ばれる抜け穴の拡大につながる可能性を否定できません。

仮にネットワーク上で内部と外部を 100%遮断できたとしても、USB メモリー等の媒体経由でのマルウェア感染、標的型攻撃による詐欺的な手法、内部犯行のリスク等も存在します。そして、これらの脅威は外部からの攻撃よりも深刻な場合があります。

外部（インターネット）と遮断されたネットワークでは、最も重要なセキュリティ対策である OS 等のアップデート、セキュリティパッチ適用の自動化が困難なため、運用負荷からこれらの適用が遅滞し、脆弱性が放置されてしまうと

いう状況を招く恐れがあります。

２．３　境界型セキュリティにおける環境変化への対応の限界

システム利用が組織内に閉じていた時代には境界型セキュリティは有効でしたが、外部との連携やパブリック・クラウドの利用が増大すると、その限界が顕在となってきました。

パブリック・クラウドの利用、働き方改革、デジタル・ガバメントによる官民連携が実現されると、今まで壁の内側で守られてきた「ユーザー」「データ」「デバイス」、あるいは「サーバ」などが、壁の外側で活用される局面が増大します。

これらは境界型セキュリティの前提と相容れないため、境界型セキュリティにのみセキュリティ対策を依存していると、これらの諸施策がセキュリティのために遅滞してしまいます。

従来の境界線セキュリティは、「縛る、制限する」セキュリティであり、壁を越えて企業や国民と連携しなければならない職員の足枷になるだけでなく、「すべてのデバイスがつながる」ことが前提の 5G、IoT、マルチデバイス環境において期待される職員の生産性向上の機会を大きく損ないます。

結果、組織や社会の DX（デジタルトランスフォーメーション）が立ち遅れ、国際競争力にも影響を与えることとなります。

２．４　ゼロトラストとは

ゼロトラストとは利便性を保ちながら、クラウド活用や働き方の多様化に対応するため、ネットワーク接続を前提に利用者やデバイスを正確に特定、常に監視・確認する次世代のネットワークセキュリティ環境です。また、「内部であっても信頼しない、外部も内部も区別なく疑ってかかる」という「性悪説」に基づいた考え方から、利用者を疑い、デバイス（機器）を疑い、データを疑い、アプリケーションを疑います。許可されていたアクセス権でも、なりすまし等の可能性が高い場合には、動的にアクセス権を制限する運用を行います。

アクセス権は、必要最小限を前提に、真に必要な利用者や機器等のみに限定して設定され、「デバイスがすでにマルウェアに感染している可能性がある」「利用者が不自然な利用をしている」「セキュアでない環境からアクセスしている」等、リスクを常に動的に評価し、高リスクな場合にはアクセスが制限されます。

そして、このような動的な権限管理の実現は人手では困難なため、運用の自動化が必要となります。

壁の内側も外側も同じように疑い、同じようにセキュリティ対策を施します

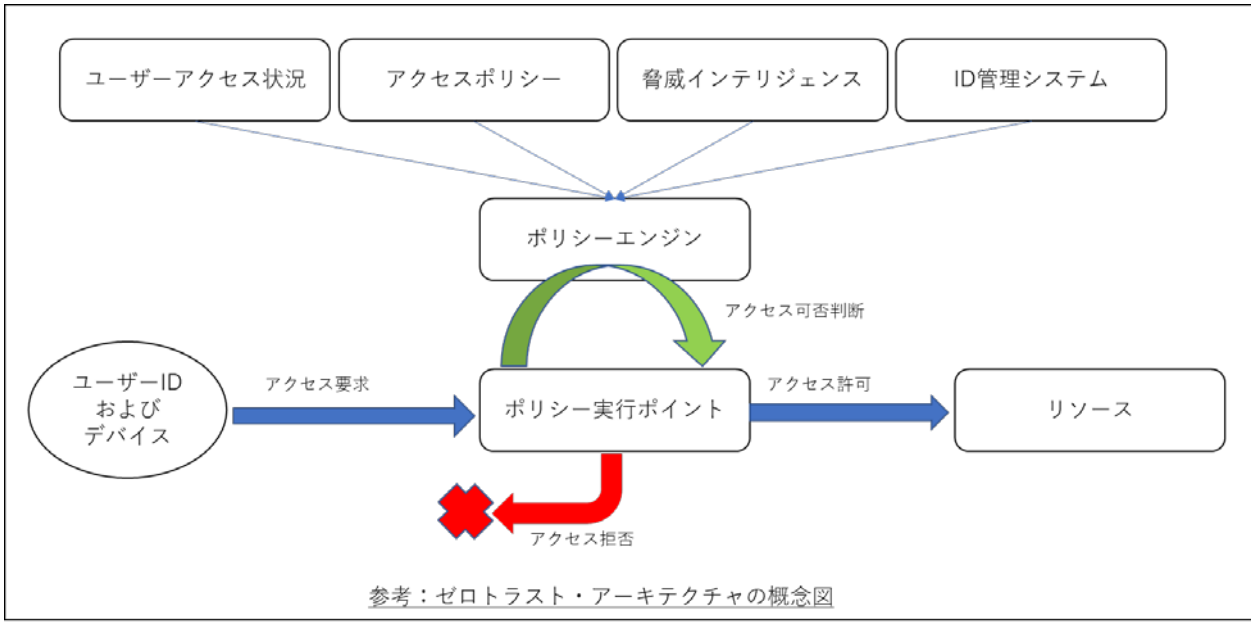
ので、最終的にはネットワークによる壁は意味がなくなります。

境界型が城のイメージだとすると、ゼロトラストは街のイメージです。壁はないものの、街の至る所で権限が確認され、その時点でアクセスを許可された人だけが、許可された範囲のことだけを実行できます。

また、このようなアクセス権の管理には、信頼性の高い認証が必須となるため、ゼロトラストでは認証を特に重視します。

以下にゼロトラスト・アーキテクチャの概念図と各要素の説明を示します。

図 3-1 ゼロトラスト・アーキテクチャの概念図



・ポリシーエンジン
静的に定義されたポリシーや、脅威インテリジェンスなどの動的な各種情報を解釈し、リソースに対する対象のクライアントのアクセス可否を決定。

・ポリシー実行ポイント
対象クライアントとリソースの間のコネクションを監視し、ポリシーエンジンの決定にしたがってコネクションの確立や切断を一元的に実行。

・アクセスポリシー
ポリシーエンジンに解釈されるユーザー属性情報、 OS やパッチバージョンなどのデバイス属性情報、それらを考慮してリソースに対するアクセス条件を定義した静的な情報。

・ID 管理システム
名前、email アドレス、証明書、所属組織、職種、アクセス権限と関連システム、等のユーザー属性情報を作成、保存、管理するシステム。

・ユーザーアクセス状況
該当組織に関連するユーザーのアクセス状況に関するログ、ネットワークトラフィック状況、リソースの状態監視情報などを含む動的な情報。
・脅威インテリジェンス情報
マルウェア情報、攻撃情報、脆弱性情報、IP アドレスや DNS のブラックリスト情報等、外部から得られる動的な情報。また、該当組織の SIEM 等による内部で得られる動的な情報。
・リソース
サーバ、クラウドサービス、API など該当組織が業務のために必要とする IT 関連リソース
・ユーザーID/デバイス
ID 管理システムに登録されたユーザーID を提示する仕組みと実装されたデバイスを含むエンドポイント

２.５　技術トレンドとしてのゼロトラスト

ゼロトラストの概念は 2010 年に Forrester Research の John Kindervag 氏によって提唱され、大手 IT 企業やセキュリティ企業が積極的に取り組んでいます。

クラウドにおいても、AWS や Azure のセキュリティはゼロトラストの考え方をベースにしています。

また、グーグル社やマイクロソフトは自社ネットワークをゼロトラストに移行しています。

NIST（アメリカ国立標準技術研究所）では、2019 年 9 月にゼロトラストに関するアーキテクチャ（ドラフト）を公開しています。(https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft.pdf)

ゼロトラストは、主要 IT ベンダーや主要クラウドサービス提供者がコミットしていることから、不可逆的で強い技術トレンドになっています。

また、ゼロトラストの考え方に基づくソリューション・製品は、クラウド利用時に使用すること、ソリューション・製品自体がクラウド化されている場合が多く、ゼロトラストへの移行とクラウド利用の拡大は車輪の両輪として推進していく必要があります。

３　政府情報システムにおけるゼロトラストの適用

３.１　基本的な考え方

ゼロトラストの考え方を政府情報システムにおいて適用させるには、先ず、

境界型セキュリティに強く依存する現状の理解と、予算的な制約から段階的に複数年かけた移行計画が必須という前提への理解が必要となります。また、これまでの境界型セキュリティへの強い依存は、過度の多層防御によるネットワークセキュリティ対策の整合性の不備と高コスト化を招いているだけでなく、アプリケーションレベルでのセキュリティ対策の不十分さ、「外部と分離されていれば安心、分離されていなければ危険」といった感情面での強い依存も招いていることへも理解が必要です。

従って、フェイルセーフとしての境界型セキュリティを残しつつ、ゼロトラストを基本に境界型セキュリティも組み合わせた移行の検討が必要となります。

３．２　ゼロトラストを適用するための取り組み

政府情報システムにおいて、ゼロトラストを適用していくには、以下の取り組みが有効です。

1)パブリック・クラウド利用可能システムと利用不可システムの分離
2)システムのクラウド化徹底とネットワークセキュリティ依存の最小化
3)エンドポイント・セキュリティの強化
4)セキュリティ対策のクラウド化
5)認証と認可の動的管理の一元化

なお、2)～5)の取り組みは、予算やライフサイクルの制約がなければ、可能な限り同時に実施することが好ましい対策です。特に「システムのクラウド化徹底」、「エンドポイント・セキュリティの強化」、「セキュリティ対策のクラウド化」については、並行実施を原則に検討してください。

４　具体的な取り組み

４．１　パブリック・クラウド利用可能システムと利用不可システムの分離

ゼロトラストの適用は、パブリック・クラウドの利用が前提となります。「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2018 年 6 月決定）においては、特定秘密と極秘文書に該当する情報をパブリック・クラウド上で扱わないものとしており、これらを扱うシステムについては、パブリック・クラウドの利用可能なシステムとは分離して考える必要があります。

パブリック・クラウド利用不可システムにおけるゼロトラストの適用は、制度上の制限から現時点では困難です。

４．２　システムのクラウド化徹底とネットワークセキュリティ依存の最小化

業務システム（アプリケーション）を信頼できるクラウド（IaaS/PaaS/SaaS）に、メールやファイルサーバ等のコミュニケーション系システムをコミュニケーション系クラウドに移行させることが、最優先の取り組みとなります。現在、アプリケーションやデータを最も効果的に防御する仕組みは、常に進化し続けるクラウドによって提供されています。アプリケーションやデータを境界型セキュリティによるネットワークセキュリティに依存することなく、安全に保護するには、信頼できるクラウドへの移行が最も有効です。

システムのクラウド化を徹底することによって、全体的なセキュリティレベルを向上させつつ、併せてネットワークセキュリティ（境界型セキュリティ）で防御しなければいけない対象の最小化を図ります。

なお、信頼できるクラウドの詳細については、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2018 年 6 月決定）を参考にしてください。また、クラウド利用やクラウドへの移行についての考え方は、「パブリック・クラウドを利用した情報システムにおける計画・構築時の基本的な考え方」（ディスカッションペーパー、2019 年 4 月）、「情報システムのパブリック・クラウドへの移行方式について」（ディスカッションペーパー、2019 年 4 月）を参考にしてください。

４．３　エンドポイント・セキュリティの強化

併せて急がれるのが、端末等のエンドポイント・セキュリティの強化です。クラウドに移行できていないサーバが残る場合には、これらのサーバについても、セキュリティ強化の対象になります。

従来、端末等のセキュリティはネットワークセキュリティでの防御を前提に、マルウェア対策を中心としたセキュリティ対策が施されることが多く、その対策は部分的でした。ゼロトラストでは、ネットワークセキュリティでの防御を前提とせず、デバイス単体でのセキュリティ対策の自立が要求されます。

また、従来の行政端末は、庁舎内設置と府省ネットワークからの利用を前提とすることが一般的でしたが、今後はモバイル利用を前提とする必要があります。

具体的には、MDM（Mobile Device Management）、EDR(Endpoint Detection and Response)、SOC(Security Operation Center)による監視、SIG(Secure Internet Gateway)等による DNS やプロキシレベルのセキュリティ対策等の導入が推奨されます。

４．４　セキュリティ対策のクラウド化

前述の「エンドポイント・セキュリティの強化」で言及したセキュリティ対策を含め、セキュリティ対策のクラウド化を進めることも必要です。従来、ネットワークセキュリティでは、府省ネットワーク内に設置したサーバにインストールされたセキュリティソフトやアプライアンス機器がセキュリティ対策の中心でしたが、こういったセキュリティ製品自身の運用管理、タイムリーなアップデートは大きな運用負荷となっていました。

業務システムがクラウド化によって合理化、抜本的に刷新されつつあるのと同様に、セキュリティ製品においても、クラウド化による低コスト化、サービスの高度化が急速に進んでおり、むしろクラウドでないと最新のサービスが利用できない状況になりつつあります。特にセキュリティ対策は日進月歩の最たる世界のため、オンプレミスのセキュリティ製品を使い続けること自体がリスクとなりつつあります。

具体的には、前述の MDM 、EDR、SIG 等に加え、CASB(Cloud Access Security Broker)、SASE (Secure Access Service Edge)等が該当します。また、SOC 監視等の従来からマネージド・セキュリティ・サービスとして外部サービス化されていたものも、ここには含みます。

セキュリティ対策のクラウド化を行うことによって、全体的なセキュリティレベルを向上させつつ、府省ネットワーク内の機器を削減させることによって、ネットワークセキュリティで防御しなければいけない対象の最小化を図ります。

なお、信頼できるクラウドの詳細については、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2018 年 6 月決定）を参考にしてください。

４．５　認証、及び認可の動的管理の一元化

ゼロトラストでは、認証の強化と認可の動的管理が特に重要視される分野となっています。具体的には、前述の「ID 管理システム」を前提に「ポリシーエンジン」や「ポリシー実行ポイント」等を実装する部分です。しかしながら、政府情報システムでは、システムの縦割りが大きな弊害となっており、個別システムや個々の府省独自の取り組みでは、認証（ID 管理システム）の一元化が難しく、それを前提とする認可の動的管理（ポリシー実行ポイントの一元的な実装）も困難です。

よって、政府全体としての認証、及び認可の動的管理一元化については、予算一元化に向けた取組等をとりまとめている「グランドデザイン」における諸施策を具体化させることにより、一元的に体系化されたディレクトリを前提とする必要があります。

しかしながら、比較的、大規模で利用者が限定される独立性の高いシステムであれば、先行的な導入が可能です。

その場合は、利便性の高い多要素認証を前提に、クラウド化された認証、認可を動的に一元管理するシステムを検討してください。

５　参考情報へのリンク

本文書を作成するに当たり、以下の情報を参考にしています。

(1) Zero Trust Architecture (Draft NIST Special Publication 800-207)
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft.pdf
(2) The Road to Zero Trust (Security) (Kurt DelBene, Milo Medin, Richard Murray)
https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF
(3) What is Zero Trust? (Paloalto)
https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture
(4) Zero Trust Networks (Doug Barth, Evan Gilman)
https://www.oreilly.com/library/view/zero-trust-networks/9781491962183/ch01.html
(5) BeyondCorp (Google)
https://cloud.google.com/beyondcorp/
(6) Implementing a Zero Trust security model at Microsoft (Microsoft)
https://www.microsoft.com/en-us/itshowcase/implementing-a-zero-trust-security-model-at-microsoft
(7) Deciphering zero trust architecture (Wipro)
https://www.wipro.com/applications/deciphering-zero-trust-architecture/