SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

ゼロトラストを利用したIRMによる情報流出対策の考察
Information leakage prevention by IRM using Zero Trust

宇野 正人 * 角尾 幸保 *
UNO Masato TSUNOO Yukiyasu

キーワード ゼロトラスト, 動的ポリシー, IRM

あらまし

近年では，リモートオフィスやモバイル端末，クラウドサービスの利用など，多くの組織が，日常的にインターネットを利用している．ネットワークを介し組織の内外を容易にアクセスできる環境の変化は，業務の効率性や利便性を高めた一方で，組織内と組織外のネットワーク境界の定義を困難にし，組織の情報セキュリティのリスクを高めている．すなわち，利用者のアクセス場所やサービスの提供場所が不特定となり，攻撃者の介入を容易にし，防御体制の構築を困難にしている[1].

安全で信頼できる情報システムは，リソースへのアクセスを許可する仕組みを持つ必要がある．組織内のリソースを守るための考え方に境界型モデルがある．内部ネットワークと外部ネットワークを区分し，その区分境界をファイアウォールで防御するシステムは，境界型モデルに基づいている．境界型モデルでは，ファイアウォールのアクセスコントロールリストにより，パケットを中継又は遮断でき，また，防御すべき場所を境界に限定できることから，システム構成が簡潔で運用が容易になる．しかし，何らかの手法で攻撃者に境界を突破されれば，以降は内部ネットワークの横断移動や情報窃取を防ぐことが困難である．実際，新たなサイバー攻撃の手口による事象が多く発生しており，ランサムウェアに感染し身代金の支払いを強要されるだけでなく，データを暴露される例が存在する[2]．これらは，境界型モデルでは，不正アクセス行為による情報窃取及びデータ暴露に対して十分な効果を持たない可能性を示唆すると言える．このため，新たな防御技術の導入が必要と考えられる．

多くの現行システムが不正アクセス行為等の侵害を受ける状況の中で，ゼロトラストモデルが注目されている．ゼロトラストモデルとは，ネットワークが侵害されている場合であっても，リソースへのアクセスを判断する際の不確実性を最小化するために設計された概念とアイデアの集合体のことである[3]．リソースへのアクセスは，クライアントやリソースの状態，その他の環境属性を含めた動的ポリシーにより決定される[4]．また，情報窃取後のデータ暴露の対処には暗号が有効である． IRM(Information Rights Management)は，文書ファイルなどを暗号化し，閲覧や編集などを管理・制限したりする機能や専用のソフトウェアのことである．

本研究では，不正アクセス行為の情報窃取及びデータ暴露の防止をするために，ゼロトラストを利用したIRMモデルを提案する．提案するモデルでは，ゼロトラストの動的ポリシー決定に必要な情報収集と動的ポリシー適用に着目しており，IRMの暗号化機能により情報窃取後のデータ暴露の防止を可能としている．提案するモデルは，境界を突破した後でも認証や認可の仕組みが動作するため，境界型モデルより，脆弱性を利用した攻撃から組織や個人の情報漏えいを防止する能力が高いことが期待できる．

本研究では，提案モデルが動的ポリシーを効果的に機能させるために必要となる収集すべき情報を整理した．

参考文献

[1] Evan Gilman, Doug Barth 著,鈴木研吾訳,「ゼロトラストネットワーク」オライリー・ジャパン,2019
[2] 独立行政法人情報処理推進機構「情報セキュリティ白書 2021―進むデジタル，広がるリスク：守りの基本を見直そう―」,2021
[3] 独立行政法人情報処理推進機構「ゼロトラスト導入指南書―情報系・制御系システムへのゼロトラスト導入―」,2021
[4] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly 著,PwC コンサルティング合同会社訳,“ゼロトラスト・アーキテクチャ”, NIST Special Publication 800-207,2020

* 東京通信大学，東京都新宿区西新宿 1-7-3, Tokyo Online University, 1-7-3 NISHI-SHINJYUKU SHINJYUKU-KU TOKYO JAPAN,