Title	遮断制御機能を有するネットワーク環境
Sub Title	Network environment with remote shutdown functionality
Author	加藤, 朗(Kato, Akira)
Publisher	慶應義塾大学
Publication year	2024
Jtitle	学事振興資金研究成果実績報告書 (2023.)
JaLC DOI	
Abstract	現在、本研究科のコンピュータネットワークは、ルータのCAM容量の関係により、十分に細かいアクセス制御を実施できていなかった。そこで、アクセス制御の実装容量の大きなスイッチを導入し、スイッチはL2で動作させつつL4レベルのアクセス制御を実施するこで、上記の問題解決を図った。基本的なアクセス制御、たとえば、各subnetに割り当てられたIPアドレス(IPv4およびIPv6) 以外のIPアドレスから発信されたパケットを拒否するなどの機能はルータに残しつつ、各ホストに固有な制御はスイッチに移すことで、きめ細かい制御を実現している。 また、セキュリティインシデントの発見はCSIRTで運用している装置に依存している。これを改善することは容易ではないが、セキュリティ事案が疑われるホストが発見された場合、送受信をしているパケットを観測し、それを記録することは、10Gigabit Ethernetを使いつつある環境では必ずしも容易ではない。さらに、まだIPv6を活用したセキュリティ事案は少ないものの、IPv6では複数の、しかも時間に伴って変化するグローバルアドレスを使って通信することも多くなってきている。そのため、IPv4/IPv6両方を活用することで監視の目から逃れるような事案も、現在は幸いに発見されていないものの、IPv6の普及とともに除外することはできなくなっている。この場合、バックボーンでのL3での監視では十分ではない可能性がある。そのため、当該計算機のMACアドレスを指定して、収容しているサブネット上で監視することが必要である。ここでは当該計算機に対するパケットをスイッチによってし、それを観測・記録することによって、IPv4/IPv6両方を活用するセキュリティ事案に対応できる体制が整ってきている。 In the current computer network of the graduate school, fine-tuned access control is not possible due to the capacity of CAM in the router. In order to improve the situation, a layer-2 switch which large CAM capacity is introduced. It is possible to apply fine-tuned layer-4 access control list to be applicable to a subnet switched at layer-2. Common access control rules, such as ingress filtering to drop non-legitimate source IP (IPv4 or IPv6) address, sometimes referred to as uRPF, are remain in the router. Automatic discovery of security incidents is provided by university CSIRT with special appliance. When a host is considered to have a security incident, it is not very easy to observe and capture packets at 10Gigabit Ethernet. Furthermore, while the number of known cases is not large, security incidents which uses IPv6 may be expected. In IPv6, hosts may use randomized IPv6 addresses and usually the address is changed over time due to privacy enhancement. So it may possible to a security incident which fully use of both of IPv4 and IPv6 in order to avoid observation by security monitoring mechanism. This means observation at the contral backbone may offer limited functionality as addresses association may not be possible. In order to provide counter-solution to these kinds of incidents, it is required to provide packet observation based on the source MAC address. The introduced switch is capability to monitor packets related to a specified MAC address to observe such incidents.
Notes	
Genre	Research Paper
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=2023000013-20230007

2024年4月10日

2023年度　学事振興資金（共同研究）研究成果実績報告書

研究代表者	所属	大学院メディアデザイン研究科	職名	教授	補助額	1,900千円
	氏名	加藤 朗	氏名（英語）	Akira Kato		

研究課題（日本語）

遮断制御機能を有するネットワーク環境

研究課題（英訳）

Network Environment with Remote Shutdown functionality

研究組織

氏　　名 Name	所属・学科・職名 Affiliation, department, and position
加藤　朗 （Akira Kato）	メディアデザイン研究科
砂原　秀樹 （Hideki Sunahara）	メディアデザイン研究科

１．研究成果実績の概要

現在、本研究科のコンピュータネットワークは、ルータの CAM 容量の関係により、十分に細かいアクセス制御を実施できていなかった。そこで、アクセス制御の実装容量の大きなスイッチを導入し、スイッチは L2 で動作させつつ L4 レベルのアクセス制御を実施するこで、上記の問題解決を図った。基本的なアクセス制御、たとえば、各 subnet に割り当てられた IP アドレス (IPv4 および IPv6) 以外のIP アドレスから発信されたパケットを拒否するなどの機能はルータに残しつつ、各ホストに固有な制御はスイッチに移すことで、きめ細かい制御を実現している。

また、セキュリティインシデントの発見は CSIRT で運用している装置に依存している。これを改善することは容易ではないが、セキュリティ事案が疑われるホストが発見された場合、送受信をしているパケットを観測し、それを記録することは、10Gigabit Ethernet を使いつつある環境では必ずしも容易ではない。さらに、まだ IPv6 を活用したセキュリティ事案は少ないものの、IPv6 では複数の、しかも時間に伴って変化するグローバルアドレスを使って通信することも多くなってきている。そのため、IPv4/IPv6 両方を活用することで監視の目から逃れるような事案も、現在は幸いに発見されていないものの、IPv6 の普及とともに除外することはできなくなっている。この場合、バックボーンでの L3 での監視では十分ではない可能性がある。そのため、当該計算機の MAC アドレスを指定して、収容しているサブネット上で監視することが必要である。ここでは当該計算機に対するパケットをスイッチによってし、それを観測・記録することによって、IPv4/IPv6 両方を活用するセキュリティ事案に対応できる体制が整ってきている。

２．研究成果実績の概要（英訳）

In the current computer network of the graduate school, fine-tuned access control is not possible due to the capacity of CAM in the router. In order to improve the situation, a layer-2 switch which large CAM capacity is introduced. It is possible to apply fine-tuned layer-4 access control list to be applicable to a subnet switched at layer-2. Common access control rules, such as ingress filtering to drop non-legitimate source IP (IPv4 or IPv6) address, sometimes referred to as uRPF, are remain in the router.

Automatic discovery of security incidents is provided by university CSIRT with special appliance. When a host is considered to have a security incident, it is not very easy to observe and capture packets at 10Gigabit Ethernet. Furthermore, while the number of known cases is not large, security incidents which uses IPv6 may be expected. In IPv6, hosts may use randomized IPv6 addresses and usually the address is changed over time due to privacy enhancement. So it may possible to a security incident which fully use of both of IPv4 and IPv6 in order to avoid observation by security monitoring mechanism. This means observation at the contral backbone may offer limited functionality as addresses association may not be possible. In order to provide counter-solution to these kinds of incidents, it is required to provide packet observation based on the source MAC address. The introduced switch is capability to monitor packets related to a specified MAC address to observe such incidents.

３．本研究課題に関する発表

発表者氏名 （著者・講演者）	発表課題名 （著書名・演題）	発表学術誌名 （著書発行所・講演学会）	学術誌発行年月 （著書発行年月・講演年月）