Orchestrating a brighter world NEC

WebSAM Network Flow Analyzer 3.1
WebSAM NetvisorPro V 9.4
強化内容のご紹介

2022年10月

日本電気株式会社

強化内容

- 情報セキュリティポリシーの監査ログ保持のガイドラインに対応
  - 全Syslogを取得して内外の不正アクセスの証跡を保全
  - 全フローデータを保持して内外の不正アクセスの証跡を保全

情報セキュリティポリシーのログ保持のガイドライン

地方公共案件などの情報セキュリティポリシーに関するガイドラインでは各種ログの一定期間の保持が求められています。

- 各種ログを取得したものを一定期間保持しておき、定期的に不正侵入、不正操作の有無についての点検、分析が求められています。
  - 総務省｜地方行政のデジタル化｜地方公共団体における情報セキュリティポリシーに関するガイドライン（soumu.go.jp）

（6） ログの取得等

①統括情報セキュリティ責任者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

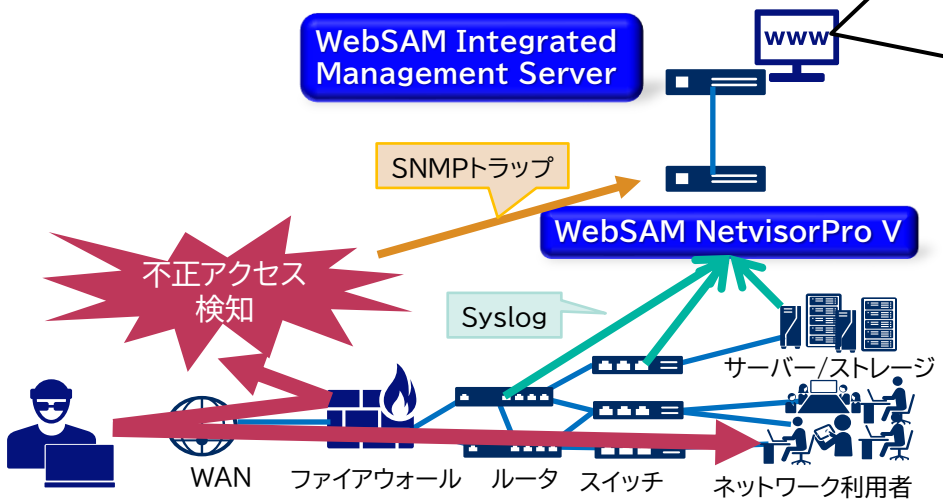
②統括情報セキュリティ責任者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

全Syslogを取得して内外の不正アクセスの証跡を保全

不正アクセス検知のSNMPトラップを受信した際に合わせてSyslogを一斉点検して調査することも可能

- SyslogDiagnosis機能のライセンスを割り当てている機器については全レベルのSyslogを保持し、検索可能
- WebSAM NetvisorPro VならWindows、Linux環境どちらでも構築可能



Syslogからアクセスログを検索してログイン失敗など不正アクセスの兆候が無いかを調査

全フローデータを保持して内外の不正アクセスの証跡を保全

受信した全フローのRawデータを保持することで簡易的なネットワークフォレンジック(※)として活用可能

- 受信した全フローのRawデータをCSVで保持可能
- 通信量の少ないフローのデータを残すことができ、ポートスキャンのように細かいフローが大量に発生するような攻撃も分析可能。
- WebSAM NetvisorPro Vと連携して不正アクセス検知のトラップ受信時に通信内容を確認し、想定外の通信が発生していないかなど影響を調査することも可能

recv_time	rc_address	dst_address	nexthop	input	output	packets	octets	first	last	src_port	dst_port	tcp_flags	protocol
2022/9/14 19:02	0.6.100.100	10.6.200.101		99		1	44	70702413	70702413	52915	5950	SYN (0x02)	TCP
2022/9/14 19:02	0.6.100.100	10.6.200.101		99		1	44	70702413	70702413	52915	2717	SYN (0x02)	TCP
2022/9/14 19:02	0.6.100.100	10.6.200.101		99		1	44	70702413	70702413	52915	8600	SYN (0x02)	TCP
2022/9/14 19:02	0.6.100.100	10.6.200.101		99		1	44	70702413	70702413	52915	1199	SYN (0x02)	TCP
2022/9/14 19:02	0.6.100.100	10.6.200.101		99		1	44	70702413	70702413	52915	1035	SYN (0x02)	TCP
2022/9/14 19:02	0.6.100.100	10.6.200.101		99		1	44	70702413	70702413	52915	52673	SYN (0x02)	TCP
2022/9/14 19:02	0.6.100.100	10.6.200.101		99		1	44	70702413	70702413	52915	1038	SYN (0x02)	TCP
2022/9/14 19:02	0.6.100.100	10.6.200.101		99		1	44	70702413	70702413	52915	9207	SYN (0x02)	TCP
2022/9/14 19:02	0.6.100.100	10.6.200.101		99		1	44	70702413	70702413	52915	48080	SYN (0x02)	TCP
2022/9/14 19:02	0.6.100.100	10.6.200.101		99		1	44	70702413	70702413	52915	5988	SYN (0x02)	TCP

短時間にランダムなTCPポートに対して大量のSYNパケットが観測されており、SYNスキャンによる攻撃を受けていることが分析可能

※ネットワークフォレンジックとは
セキュリティインシデント発生時に分析ができるように、いつどのような通信が流れていたのかを記録、分析、保持しておく対策

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。


Orchestrating a brighter world
NEC