NetStable ── ネットステイブル ──

ネットワーク無料診断サービス

インターネットからの攻撃に対応できていますか？

◉ 内部情報漏えいをブロック / 記録

◉ Web からの脅威をブロック / 記録

調査する脅威 ※弊社独自のIPSシグネチャ1,400種類以上使用

不正侵入防御装置「NetStable」をお客さまのネットワークに設置していただき、IDS (検知) ログを取得します。ログを基に弊社で**「NetStable ログ解析レポート」を無償で作成**します。

NetStable ログ解析レポートの内容例

通信名	940	防御タイプ	最終時間	送信元IP	受信先IP	通信数	UWTRV
BaiduIME Block 1	2100001	eg	2014/08/28 16:40	192.168.100.1	192.168.100.100	510	069
Foreign Country Access	3000066	検知	2014/08/28 17:51	192.168.100.35			
Fpcount access	1013	検知	2014/08/28 12:07	192.168.100.28			
Fpcount attempt	1012	検知	2014/08/28 12:07	192.168.100.28			
P2P BitTorrent traffic	1000026	eg	2014/08/28 15:40	192.168.100.56			
P2P Skype client login	1003163	検知	2014/08/28 12:34	192.168.100.28			
P2P Skype client login startup	1003164	検知	2014/08/28 12:32	192.168.100.28			
Worm VIRUS Sober.AA	1003027	eg	2014/08/28 23:31	192.168.100.56			

お客さまのネットワークで検知された通信ログを一覧でご確認いただけます。

□ P2P ソフトの使用

社会通念上、会社でのP2Pソフトの使用は控えられています。また、利用者が意識しないうちに情報を漏えいする危険性があります。

通信名	P2P BitTorrent traffic (1000026)
通信数	15,486
説明	P2Pソフト（ファイル共有ソフト）である、BitTorrentを使用してファイルダウンロードを行う場合に発生する通信です。 近年、P2Pソフトを使用しての個人情報漏洩が多発しており、気づかないうちにウイルスに感染してしまい、結果内部の情報漏えいにつながる危険性があるため使用には十分注意する必要があります。

送信元			受信先		
IP	国名	ネットワーク名、組織名	IP	国名	ネットワーク名、組織名
192.168.100.56	-	ローカルIPアドレス	67.215.246.204	アメリカ	Secured Private Network
192.168.100.56	-	ローカルIPアドレス	67.215.246.203	アメリカ	Secured Private Network
192.168.100.56	-	ローカルIPアドレス	94.100.28.59	オランダ	Swiftway Sp. z o.o.
192.168.100.56	-	ローカルIPアドレス	94.100.28.53	オランダ	Swiftway Sp. z o.o.
192.168.100.56	-	ローカルIPアドレス	94.100.28.51	オランダ	Swiftway Sp. z o.o.
192.168.100.56	-	ローカルIPアドレス	67.215.246.203	アメリカ	Secured Private Network
192.168.100.56	-	ローカルIPアドレス	67.215.246.204	アメリカ	Secured Private Network

【考察】

・警戒、監視が必要な通信が検出されました。

（LAN 側[ローカル側]から WAN 側[インターネット側]に対して）

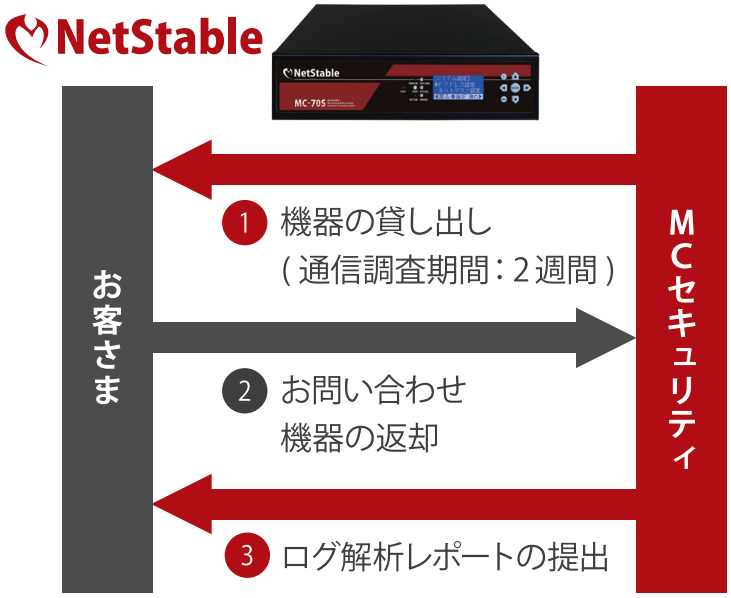
・P2P ソフトである、"Bittorrent"が社内から使用された形跡が確認されました。

・ファイル共有ソフトである Bittorrent の不正利用を監視する目的のシグネチャです。

・ダウンロードされたファイルには、ウイルスが潜んでいる場合が多くあるため、受信先 IP アドレスを持つパソコン

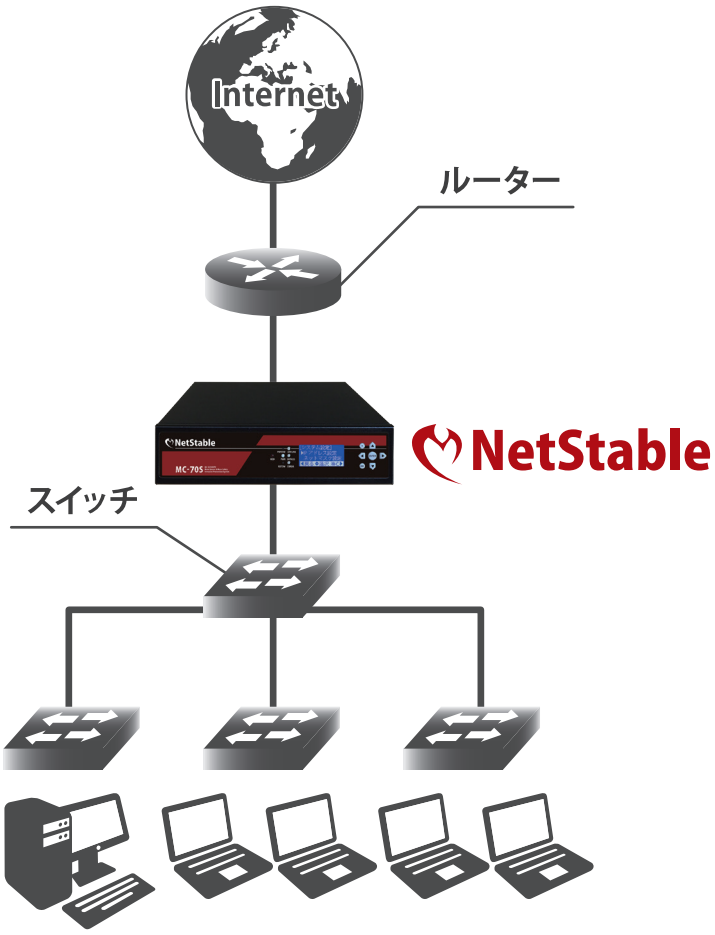
ログ解析レポートの詳細につきましては、サンプルレポートをご覧ください。
どのような内容で、どのようにお客さまの役に立つかを是非ご確認ください。

「NetStable ログ解析レポート」ご提供までの流れ



1. レポートを作成するために、お客さまのネットワークに **NetStable** を設置、ログデータを 2 週間、収集いたします。
2. お客さまには、**機器の返却** をお願いいたします。
3. 弊社へ機器到着後、1 週間程度で「ログ解析レポート」をご提出いたします。

NetStable 接続例



□接続位置について

インターネット用ルータの LAN 側 配下に、NetStableを設置してください。

※ スイッチにミラーポートを設定いただき、NetStableの WAN 側ポートに接続いただくことにより直接挟み込まずにログを収集することも可能です。

設定方法や接続場所につきまして、ご不明な点などございましたら、遠慮なくご相談ください。

《取得いただくログについて》

弊社は機器に取得されたログを、弊社内で本レポート作成の目的のみで使用します。また、レポート提出後に削除いたします。

お問い合わせ

株式会社 MCセキュリティ

〒690-0816　松江市北陵町51-2
TEL 0852-31-9001　FAX 0852-28-7240
http://www.mcsecurity.co.jp

株式会社MCセキュリティは、2006年9月28日 情報セキュリティマネジメントシステムの国際規格であるISO/IEC27001を、ソフトウェア開発、ネットワークセキュリティ機器の製造・販売及びサービスにおいて認証取得しました。