（地方公共団体情報システム機構 情報化支援戦略部（Security） → 地方公共団体）

情報提供 様式
（第1報）

各都道府県 情報セキュリティ対策担当者 殿
各市区町村 情報セキュリティ対策担当者 殿

識別番号	T387

連絡年月日	2017 年 12 月 19 日

連絡時刻	19:50

地方公共団体情報システム機構
情報化支援戦略部 担当：鈴木
Tel：03-5214-8040
e-mail：lasc_info@j-lis.asp.lgwan.jp

下記のとおり、内閣サイバーセキュリティセンターから情報提供がありましたので周知いたします。

記

緊急度*1				情報共有レベル*2
不明 高中低で表記	脅威の内容	概要	2017 年 11 月頃より、マルウェア Mirai の亜種による感染活動が国内において確認されておりますので、注意喚起いたします。 Mirai 及びその亜種は、ルータ製品の脆弱性を悪用して感染を広げることが確認されております。感染対象として確認されているルータ製品については、ベンダより修正済みのファームウェアが提供されております。影響を受けるルータ製品の機種及びバージョンをご確認いただき、ご利用中のルータ製品が該当する場合は、速やかに後述の対策を実施されるようお願いいたします。	W
		対象	重要インフラ事業者等 （該当するルータ製品を利用している事業者等）	W
	対処方針		影響を受けるルータ製品をご利用中の場合は、ベンダから提供されている修正版のファームウェアへのアップデートを適用願います。 また、Mirai 及びその亜種は、ファームウェアの脆弱性だけでなく、機器固有の ID やパスワードを悪用して感染を拡大することが知られています。前述の該当製品に加え、インターネットからアクセス可能な IoT 機器等について、以下の情報を参照し、適切な対策を実施されることを推奨いたします。	W
	その他		内閣サイバーセキュリティセンター（NISC）から情報の提供を受け、本情報提供を行っています。	W

*1 緊急度は以下により記載。
「高」: 72 時間以内に対応が必要となるもの。
「中」: 1 週間以内に対応が必要となるもの。
「低」: 「高」・「中」以外のもの。
緊急度が不明のものについては、「不明」と記載。

*2 付与する情報共有レベルにより、以下のとおり取り扱うこととする。
「A」: 本情報を共有可能な範囲を、地方公共団体内の関係する業務担当ラインの職員及び関係するシステムの保守業者等で、かつ業務の遂行にあたって、その情報を知る必要がある者のみに限定（それ以外の者には情報を提供することはできない）。
「G」: 自組織外を含む広い範囲への情報転送が可能。（ただし、Web サイトや公開のメーリングリストなどを使用して一般へ公開することは出来ない）
「W」: 公共向けの情報であり、ホームページ等での公表ができる。

（別紙）
2017 年 12 月 19 日

重要インフラ事業者等 御中

内閣サイバーセキュリティセンター
重要インフラグループ

Mirai亜種の感染活動に関する注意喚起

2017年11月頃より、マルウェアMirai の亜種による感染活動が国内において確認されておりますので、注意喚起いたします。
Mirai及びその亜種は、ルータ製品の脆弱性を悪用して感染を広げることが確認されております。感染対象として確認されているルータ製品については、ベンダより修正済みのファームウェアが提供されております。影響を受けるルータ製品の機種及びバージョンをご確認いただき、ご利用中のルータ製品が該当する場合は、速やかに後述の対策を実施されるようお願いいたします。

想定される脅威

Mirai及びその亜種に感染した機器は、ボットネットの一部となり、攻撃者により遠隔から命令を受けて、第三者への攻撃に悪用される可能性があります。

感染対象のルータ製品

本注意喚起の発出時点では、感染対象として以下のベンダのルータ製品が確認されております。影響を受けるバージョンについては、ベンダの公式ページをご参照ください。

・ロジテック株式会社
- ロジテック製 300Mbps 無線LANブロードバンドルータおよびセットモデル（全11モデル）に関する重要なお知らせとお願い
  http://www.logitec.co.jp/info/2017/1219.html

対策

影響を受けるルータ製品をご利用中の場合は、ベンダから提供されている修正版のファームウェアへのアップデートを適用願います。
また、Mirai及びその亜種は、ファームウェアの脆弱性だけでなく、機器固有のIDやパスワードを悪用して感染を拡大することが知られています。前述の該当製品に加え、インターネットからアクセス可能なIoT機器等について、以下の情報を参照し、適切な対策を実施されることを推奨いたします。

・JPCERT/CC
- Mirai亜種の感染活動に関する注意喚起
  https://www.jpcert.or.jp/at/2017/at170049.html
- インターネットに接続された機器の管理に関する注意喚起
  https://www.jpcert.or.jp/at/2016/at160050.html

以上