MITSUBISHI ELECTRIC CORPORATION
PUBLIC RELATIONS DIVISION
7-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo, 100-8310 Japon

POUR DIFFUSION IMMÉDIATE **N° 3106**

Ce texte est une traduction de la version anglaise officielle de ce communiqué de presse. Il est fourni à titre de référence et pour votre confort uniquement. Pour tout détail ou spécificité, veuillez vous reporter à la version anglaise d'origine. La version anglaise d'origine prime, en cas de divergence.

Demandes de renseignements des clients

Information Technology R&D Center
Mitsubishi Electric Corporation
www.MitsubishiElectric.com/ssl/contact/company/rd/form.html
www.MitsubishiElectric.com/company/rd/

Contacts presse

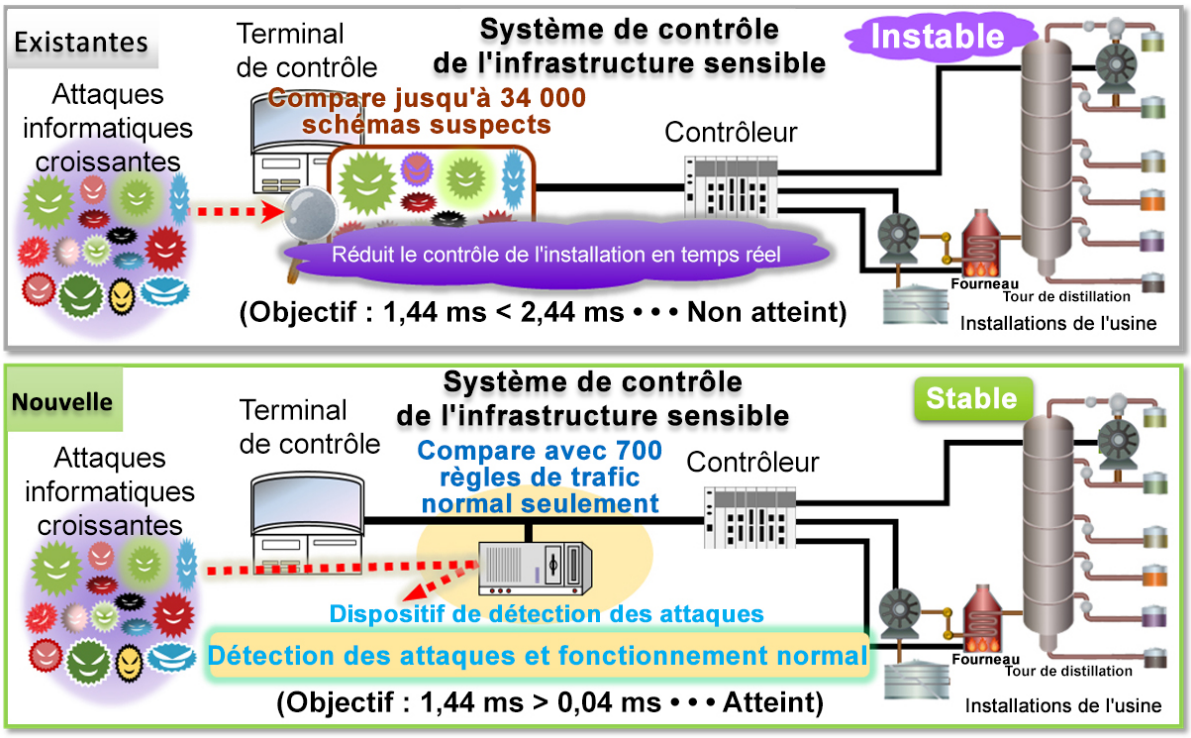
Public Relations Division
Mitsubishi Electric Corporation
prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

Mitsubishi Electric développe une technologie de détection des attaques informatiques destinées aux systèmes d'infrastructures sensibles

La détection en temps réel d'attaques informatiques visant les systèmes de contrôle contribuera à la stabilité des infrastructures

TOKYO, 17 mai 2017 – Mitsubishi Electric Corporation (TOKYO : 6503) a annoncé aujourd'hui le développement d'une technologie de détection des attaques informatiques capable d'identifier rapidement tout trafic inhabituel par rapport aux commandes normales au sein des systèmes de contrôle d'infrastructures sensibles. Cette technologie repère des attaques informatiques sophistiquées dissimulées sous forme de commandes usuelles qui visent des infrastructures sensibles de divers domaines : électricité, gaz naturel, eau, produits chimiques et pétrole. En outre, elle n'affecte pas le contrôle en temps réel exercé sur l'installation, aidant ainsi à garantir sa stabilité.

Cette technologie devrait être commercialisée à compter de l'exercice 2018 pour les infrastructures dédiées à l'électricité. D'autres applications seront développées dans le cadre de l'initiative Strategic Innovation Promotion Program (SIP, Programme de promotion de l'innovation stratégique) lancée par le gouvernement japonais pour soutenir la sécurité informatique des infrastructures sensibles.



Cette nouvelle technologie a pu être élaborée en partie grâce aux résultats obtenus au terme du projet « Cyber-Security for Critical Infrastructure » (« Sécurité informatique des infrastructures sensibles ») effectué par le Control System Security Center (CSSC, Centre de sécurité des systèmes de contrôle). Le projet « Cyber-Security for Critical Infrastructure » fait partie du « Cross-ministerial Strategic Innovation Promotion Program » (SIP, « Programme de promotion de l'innovation stratégique ») soutenu par le Council for Science, Technology and Innovation (Conseil des sciences, de la technologie et de l'innovation) et demandé par la New Energy and Industrial Technology Development Organization (NEDO, Organisation pour le développement des énergies nouvelles et des technologies industrielles).

Fonctions clés

- Au 17 mai 2017, cette technologie était la première à définir des règles de détection basées sur les commandes usuelles utilisées quel que soit l'état du système de contrôle et à interpréter les écarts par rapport à ces commandes comme des attaques.
- Les systèmes dotés de cette technologie continuent de fonctionner normalement lors de la détection d'attaques, car elle ne repose pas sur un processus chronophage de repérage de schémas suspects.
- Cette technologie contribue à la stabilité des infrastructures en réduisant la durée de détection des attaques et en garantissant un impact minimal sur les processus des systèmes de contrôle, qui doivent être exécutés dans des délais déterminés.

Comparaison avec les technologies existantes

	Méthode	Fonctionnement en temps réel des systèmes de contrôle	Utilisation
Nouvelle	Détecte les écarts par rapport aux règles de commande habituelles déterminées par l'état de fonctionnement	Impact limité grâce aux règles concises appliquées aux commandes habituelles	Efficacité prouvée lors de simulations au sein des systèmes d'installations
Existantes	Comparent les schémas suspects à un nombre élevé de règles	Risque d'impact sérieux en raison des attaques informatiques croissantes	Actuellement utilisées au sein des systèmes d'entreprises

Par le passé, des intrusions au sein de systèmes de contrôles ont été commises par le biais d'attaques informatiques complexes afin d'émettre des commandes a priori habituelles qui sont pratiquement impossibles à distinguer de commandes réelles. Les méthodes de détection existantes, qui comparent le trafic entrant à des schémas suspects connus, ne parviennent pas toujours à détecter de telles attaques. Cette comparaison peut prendre du temps en raison du nombre colossal de schémas et provoquer l'échec d'opérations relatives aux systèmes de contrôle.

Mitsubishi Electric a constaté que le trafic normal d'un système de contrôle des infrastructures sensibles change selon que le système est en fonctionnement, éteint ou fait l'objet d'opérations d'entretien. Par conséquent, la nouvelle technologie emploie différentes règles de détection pour chaque état. En raison de l'augmentation des attaques informatiques, l'élaboration de schémas suspects et la recherche de correspondances requièrent un temps considérable. Cependant, les commandes habituellement employées au sein des systèmes de contrôle sont limitées, par conséquent, les règles peuvent l'être aussi. La nouvelle technologie proposée par Mitsubishi Electric est ainsi en mesure de rechercher rapidement des correspondances et de repérer les attaques sans nuire au fonctionnement en temps réel des systèmes de contrôle. L'entreprise a évalué le délai de traitement de détection des attaques perpétrées contre les systèmes de contrôle dont elle est responsable. Il s'est avéré que la nouvelle technologie requiert 0,04 ms seulement pour opérer, contre 2,44 ms dans le cas des technologies existantes, alors que la durée nécessaire au contrôle en temps réel s'élève à 1,44 ms.

Contexte

À une époque où les infrastructures recourent de plus en plus fréquemment à l'Internet des objets (IoT), la sécurité informatique des installations sensibles constituant les piliers des entreprises devient un aspect crucial. Jusqu'à ce jour, la sécurité d'infrastructures sensibles dédiées à l'électricité, au gaz naturel, à l'eau,

aux produits chimiques ou encore au pétrole reposait sur l'isolation physique, des pare-feu de contrôle du trafic et une gestion stricte des opérations. Ces dernières années ont cependant été marquées par l'augmentation d'attaques informatiques élaborées, notamment à l'étranger. Ces attaques visent à s'introduire dans les systèmes de contrôle d'infrastructures afin d'émettre des commandes malveillantes sous forme d'instructions usuelles. Ces dernières provoquent des dégâts en causant par exemple des coupures de courant ou la destruction d'équipements.

Brevets

Sept dépôts de brevet au Japon et sept à l'étranger concernent la technologie présentée dans ce communiqué de presse.

###

À propos de Mitsubishi Electric Corporation

Forte de plus de 90 années d'expérience dans la création de produits fiables et de haute qualité, l'entreprise Mitsubishi Electric Corporation (TOKYO : 6503) est un leader mondial reconnu pour la fabrication, la mise sur le marché et la vente d'équipements électriques et électroniques utilisés dans les domaines du traitement de l'information et des communications, du développement spatial et des communications par satellite, des appareils électroniques grand public, de la technologie industrielle, de l'énergie, du transport et de l'équipement de construction. En se conformant à l'esprit de sa devise « Changes for the Better » et de son engagement environnemental « Eco Changes », Mitsubishi Electric s'efforce d'être une entreprise pionnière et propre en plaçant la technologie au service de la société. L'entreprise a enregistré un chiffre d'affaires consolidé du Groupe de 4 238,6 milliards de yens (37,8 milliards de dollars US*) au cours du dernier exercice qui a pris fin le vendredi 31 mars 2017. Pour plus d'informations, veuillez consulter :
www.MitsubishiElectric.com

*À un taux de change de 112 yens pour 1 dollar US, taux indiqué par le Tokyo Foreign Exchange Market le vendredi 31 mars 2017