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

**FOR UMIDDELBAR UTGIVELSE** **nr. 3106**

*Denne teksten er en oversettelse av den offisielle engelske versjonen av pressemeldingen, og den er kun ment som et praktisk referanseverktøy. Du finner detaljene og spesifikasjonene i den originale engelske versjonen. Dersom tekstene ikke stemmer overens, er det den originale engelske versjonen som gjelder.*

*Kundeforespørsler*

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

*Medieforespørsler*

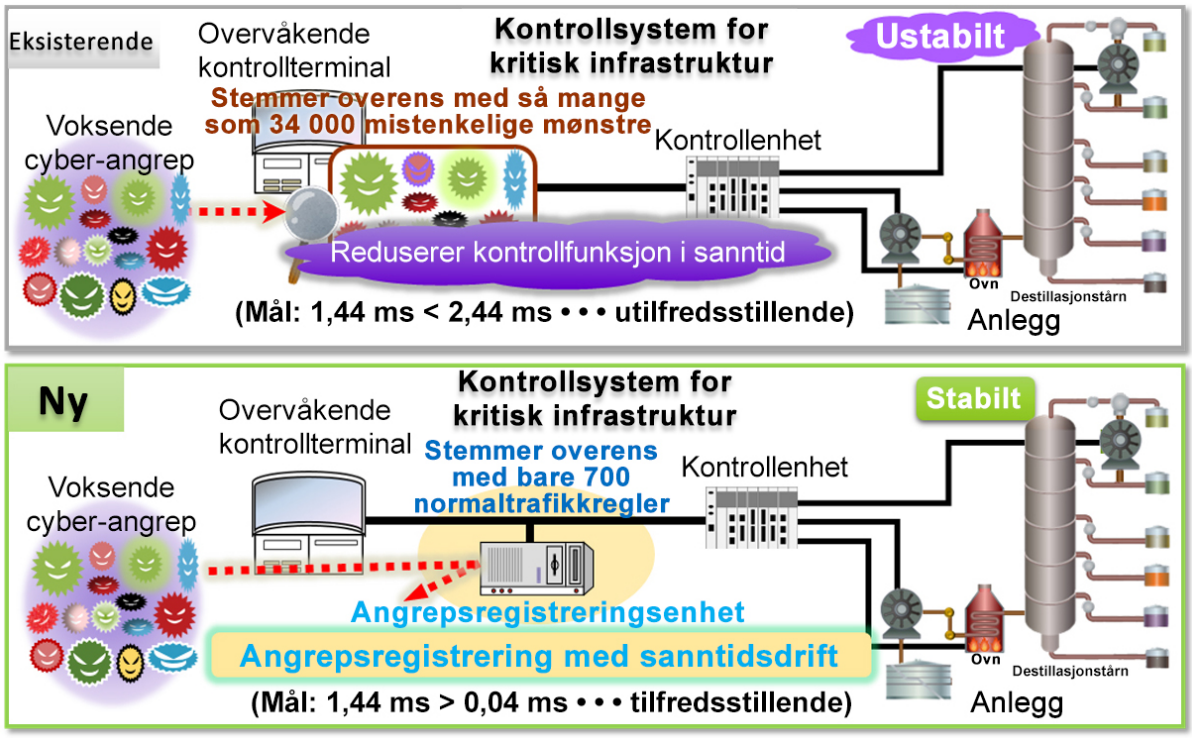
Public Relations Division
Mitsubishi Electric Corporation
prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

# Mitsubishi Electric utvikler teknologi for registrering av cyber-angrep for kritiske infrastruktursystemer

*Registrering av cyber-angrep på kontrollsystemer i sanntid bidrar til stabil infrastruktur*

**TOKYO, 17. mai 2017** – Mitsubishi Electric Corporation (TOKYO: 6503) kunngjorde i dag at de har utviklet en teknologi for registrering av cyber-angrep som raskt identifiserer nettverkstrafikk som avviker fra forhåndsdefinerte normale kommandoer i kontrollsystemene for kritisk infrastruktur. Teknologien oppdager geniale cyber-angrep forkledd som normale kommandoer, som er rettet mot kritisk infrastruktur for elektrisk strøm, naturgass, vann, kjemikalier og olje uten reduksjon av sanntidskontrollfunksjonen, som forventes å bidra til å sikre infrastrukturstabilitet.

Kommersialisering for infrastruktur for elektrisk strøm er planlagt fra rundt regnskapsåret 2018. Andre bruksområder vil bli utviklet i samarbeid med utfordringen fra Strategic Innovation Promotion Program (SIP – den japanske statens program for å fremme strategisk innovasjon) angående cyber-sikkerhet for kritisk infrastruktur.




Realiseringen av den nye teknologien ble delvis støttet av resultatene fra «Cyber-Security for Critical Infrastructure» (Cyber-sikkerhet for kritisk infrastruktur) gjennomført av Control System Security Center (CSSC). «Cyber-Security for Critical Infrastructure» er en del av det tverrministerielle Strategic Innovation Promotion Program (SIP) (program for å fremme strategisk innovasjon) promotert av Rådet for vitenskap, teknologi og innovasjon og er bestilt av New Energy and Industrial Technology Development Organization (NEDO).

**Viktige funksjoner**

- Teknologien er den første i verden, per 17. mai 2017, som definerer registreringsreglene på grunnlag av de normale kommandoene for hver driftstilstand for kontrollsystemet og som tolker avvik fra de normale kommandoene som angrep.
- Drift i sanntid av kontrollsystemet vi hadde til vurdering, er sikret når angrepsregistrering er i bruk fordi teknologien ikke innebærer en tidkrevende vurderingsprosess med tanke på mistenkelige mønstre.
- Teknologien bidrar til stabil infrastruktur ved å redusere registreringstiden og ved å sikre minimal innflytelse på kontrollsystemprosesser som må være ferdig innen en viss tid.

**Sammenligning med eksisterende teknologi**

| | Metode | Drift av systemer i sanntid | Gjennomførbarhet |
|---|---|---|---|
| Ny | Oppdager avvik fra normale kommandoregler fastsatt av driftsstatus | Lav innvirkning på grunn av konsise regler for normale kommandoer | Bevist effektivitet i anleggssystemsimuleringer |

| | | | |
|---|---|---|---|
| Eksi-sterende | Stemmer overens med mistenkelige mønstre med enorme sett med regler | Risiko for høy innvirkning på grunn av økende cyber-angrep | Brukes i dag i foretakssystemer |

Det har forekommet tilfeller hvor avanserte cyber-angrep har trengt inn i kontrollsystemer og utstedt kommandoer som later som om de er normale, og som er svært vanskelige å skille fra virkelige kommandoer. Det kan hende at eksisterende registreringsmetoder som sammenligner innkommende trafikk med kjente mistenkelige mønstre, ikke greier å oppdage slike angrep. Sammenligning med det enorme volumet av kjente mistenkelige mønstre kan ta tid og føre til at driften av kontrollsystemer svikter.

Mitsubishi Electric observerte at normal kontrollsystemtrafikk i kritisk infrastruktur er forskjellig hvis systemet er i drift, ikke i drift eller under vedlikehold, slik at den nye teknologien bruker forskjellige registreringsregler for hver driftstilstand. Ettersom cyber-angrep fortsetter å øke, tar det veldig lang tid å generere mistenkelige mønstre og søke etter overensstemmelser. Men normale kommandoer i kontrollsystemer er begrenset, slik at reglene kan begrenses, noe som gjør at Mitsubishi Electrics nye teknologi kan søke etter overensstemmelser raskt og oppdage angrep samtidig som den opprettholder drift i sanntid av kontrollsystemer. Selskapet evaluerte behandlingstiden for angrepsregistrering for kontrollsystemene vi hadde til vurdering. Evalueringen avdekket at den nye teknologien tar bare 0,04 ms, sammenlignet med 2,44 ms for en eksisterende teknologi, mens sanntidskravet er 1,44 ms.

**Bakgrunn**

Ettersom IoT gjennomsyrer infrastrukturfeltet, blir cyber-sikkerhet stadig viktigere for kritisk infrastruktur som underbygger samfunnet. Inntil nå har sikkerheten for infrastruktur for elektrisk strøm, naturgass, vann, kjemikalier og olje blitt ivaretatt gjennom fysisk avgrensning, brannmurer for trafikkontroll og streng driftsforvaltning. De senere årene har det imidlertid vært en økning, særlig i utlandet, i avanserte cyber-angrep som trenger inn i kontrollsystemer for infrastruktur og sender skadelige kommandoer forkledd som normale for å volde skade, som for eksempel strømbrudd og ødeleggelse av utstyr.

**Patenter**

Teknologien som er kunngjort i denne pressemeldingen, har sju patentanmeldelser i Japan og sju i utlandet.

###

**Om Mitsubishi Electric Corporation**

Med over 90 års erfaring med å levere pålitelige produkter av høy kvalitet er Mitsubishi Electric Corporation (TOKYO: 6503) en anerkjent verdensleder innen produksjon, markedsføring og salg av elektrisk og elektronisk utstyr som brukes innen informasjonsbehandling og kommunikasjon, romfart og satellittkommunikasjon, forbrukerelektronikk, industriteknologi, energi, transport og anleggsutstyr. Mitsubishi Electric følger konsernets slagord, Changes for the Better (Endringer til det bedre), og miljøslagordet, Eco Changes (Øko-endringer), og bestreber seg på å være et globalt, ledende grønt selskap som beriker samfunnet med teknologi. Selskapet registrerte en konsolidert konsernomsetning på 4 238,6 milliarder yen (37,8 milliarder amerikanske dollar*) i regnskapsåret som endte 31. mars 2017. Hvis du vil ha mer informasjon, kan du gå til:

www.MitsubishiElectric.com

*Ved en valutakurs på 112 yen per amerikanske dollar. Kursen er gitt av Tokyo Foreign Exchange Market 31. mars 2017