Applying the state-of-the-art and learning in the real field have both been invaluable for practical cyber defense, but they still remain challenging. NTT R&D is developing LRR\(^*1\), a platform for accelerating the collaboration between R&D and operation. This demo showcases URL Inspector, a capability provided by LRR for detection and analysis of Website-based threats.

### Features
- Applies cutting-edge research results including proprietary honeypots, domain evaluation engine, machine learning analytics, and intelligence data accumulated over a long period --- (1 in the diagram)
- Flexibly and effectively combines multiple research results to implement capabilities accessible via API and GUI over the Internet. --- (2 in the diagram)
- Collects and learns real-field expertise such as security appliance logs and analysts’ operational know-how to continuously improve the system's accuracy and usability. --- (3 in the diagram)

### Application Scenarios
- Analyzing suspicious network logs for security monitoring activities with MSS\(^*2\) automatically by using a system or manually by an operator.
- Analyzing infected Web servers for incident response or forensics activities in CSIRTs\(^*3\).

* Beta trial with security operators at NTT Security is planned to start in April 2017 for feasibility evaluation.

---

\(^*1\) LRR(ler): Internal code name for this system. It is not an acronym.
\(^*2\) MSS(Managed Security Service): operates and monitors security appliances and their logs at client environment.
\(^*3\) CSIRT(Computer Security Incident Response Team): conducts investigations of causes or impacts of security incidents.