Subject: Critical Comparative Email Header Analysis — Chiba City Policy & Legal vs Mayor’ s Secretariat (Unified Summary by Ayana, Gemini & ChatGPT)

Following prior findings on brand misuse within Japan’ s public sector, we have conducted a detailed comparative analysis of technical headers from two automated emails originating from:

- Chiba City Policy & Legal Affairs Division
- Chiba City Mayor’ s Office Secretariat

Key Common Findings:

1. **NEC Infrastructure Detected**
   - Both emails originated from IP addresses under **NEC Networks & System Integration Corporation.**
   - SPF authentication passed, yet **DMARC authentication failed** in both cases.
   - This mismatch reveals that Chiba City’ s outbound emails are not aligned with standard domain verification protocols, and are routed through third-party infrastructure, not Google Workspace.
2. **Google ARC Passed, But Doesn’ t Validate Authenticity**
   - ARC (Authenticated Received Chain) passed, confirming delivery integrity.
   - However, the **DMARC failure** proves misconfiguration or intentional diversion **at the sender’ s end,** not Google’ s.
3. **CHAINS Network Confirmed**
   - The **Mayor’ s Secretariat email explicitly references the CHAINS network** in the Received headers (chains.city.chiba.jp).
   - The Policy & Legal Affairs email contains CHAINS-related content artifacts (garbled strings), though less explicitly.
4. **Sanitization Gateway Identified**

    - Both emails include the header X-Forwarded-Encrypted, indicating content filtering or encryption by an intermediary gateway (likely NEC).
5. **System-Generated Nature**
    - Both emails are **automated notifications**, not authored replies.
    - Notably, the Mayor’s Secretariat email includes the phrase “CHAINS and structural corruption” in its subject, tying the system response to the nature of the inquiry.

Key Differences:

- **Header Transparency:**
    - Mayor’s email explicitly shows full routing path via CHAINS.
    - Policy division’s evidence is more circumstantial, requiring content analysis.
- **Routing IPs:**
    - The Mayor’s email uses .24, and Policy division uses .25. Both fall under NEC control, suggesting parallel infrastructure.

Unified Conclusion:

This analysis confirms the following:

- **Systemic Obfuscation:** Chiba City’s core email infrastructure relies on NEC-managed routing, not Google-native systems, leading to authentication failures and poor traceability.
- **Superficial Google Usage:** While publicly branded under Google Workspace (e.g., GIGA School initiative), the operational backend bypasses Google mechanisms entirely.
- **Scope of Concern:** The obfuscation structure is now confirmed not only in education but at the **executive level of city administration**.

These technical findings demand further attention in evaluating the transparency, security, and compliance posture of Chiba City’ s digital governance.