山本レポート：システム安全性向上―世界の最前線（6）

セキュリティとシステム安全性

国立大学法人 名古屋大学
大学院 情報学研究科
教授　山本 修一郎
博士（工学）

今回は、2018 年 12 月 6 日午後に発生した通信システム障害事例に基づいて、セキュリティとシステム安全性の関係について考える。

通信システム障害事例

2018 年 12 月 6 日（木）午後 1 時 39 分頃から発生したソフトバンクの通信障害は午後 6 時 4 分に復旧した。この通信障害の影響回線数は過去最大の 3060 万件に達した。約 4 時間 25 分にわたって携帯通信ネットワークが利用できなくなったことから、テレビでも大騒ぎになった。携帯やスマホが使えないというので、初めて公衆電話を使うことになって戸惑う若い人たちの姿が放映される事態になった。公衆電話に行列ができるのは数十年ぶりのことだった。公衆電話があってよかった。

この大規模通信障害の発生原因の詳細はまだ不明だが、これまでの発表 [1,2] によると、エリクソン製交換機のソフトウェア証明書の日付が期限切れになったために、機器を認証できなくなったことで、正常な通信ができなくなったとのことだ。エリクソンは、次のように説明している [2]。

「コアネットワーク内の SGSN-MME（Serving GPRS Support Node - Mobility Management Entity）に生じた問題を特定しました。この問題は、本ノードおいて特定の二つのソフトウェアバージョンを利用している、複数の国におけるお客様のネットワーク障害を引き起こしました。」

「早期の段階での根本原因の解析結果では、今回影響を受けたソフトウェア証明書のバージョンの齟齬が示されています。完全かつ総合的な根本原因の解析は依然進行中となっており、現在は直近の問題解決に集中して対応しています。」

セキュリティ対策とシステム安全性

SGSN-MME のソフトウェア証明書が、MME が正しいことを保証するために用意されているのだと思われる。ということは、この証明書の真正性を確認しようとする通信相手側のコンポーネントがあって、そのコンポーネントが、証明書の有効期限が切れていたために MME が不正だと判断した結果、通信障害が発生したことになる。

交換機ノードの真正性を保証するためにソフトウェア証明書を登録しておくのは、セキュリティ対策としては常套手段である。ソフトウェア証明書に、有効期限をつけることも適切である。ソフトウェア証明書の有効期限が切れていないことを確認することも適切である。ところが、適切なはずの通信システムのセキュリティ対策で有効期限の更新が抜けているという欠陥があったことから、今回は大規模なシステム障害が発生した。セキュリティ対策をしていなかったのではなく、セキュリティ対策を実施していたにもかかわらず、そのセキュリティ対策の不備に起因する欠陥によって、システム全体の安全性に危機がもたらされることを今回の事例が示唆している。セキュリティ対策の十分性の確認と、不備があった場合のシステム安全性に対する影響波及効果の分析が求められている。

テストの十分性

エリクソン社の見解では、MME のソフトウェア障害ということになっている。ということは、MME のソフトウェアについてのテストが不十分だったのではないかという疑問が生まれる。ソフトウェア証明書の期限が切れること、切れた場合の対応などについてのテスト項目があったのか、あった場合、テストしたのかしなかったのかが問題になる。テスト項目として証明書の期限切れ対応があり、その妥当性をテストで確認したとすると、ソフトウェア障害を防げたはずである。したがって、MME のソフトウェアテストが不十

分だった可能性が高い。セキュリティ対策を実現するだけでなく、セキュリティ機能についての十分なテストが必要である。

証明書の有効期限の管理

ノードに付与されたソフトウェア証明書の有効期限をどこでどのように管理していたのか？ 自動的に更新するようになっていたのであれば、なぜ更新できなかったのか？ 更新契機はどのように定義されていたのか？ このように原因を追跡していくと、人的要素が浮かんでくるのではないか？ 自動更新する仕組みがあったにしても、それが適切に動作するような設定になっていなかったのではないか？

ソフトウェア証明書の発行や、期限の更新をどのような手順で実施していたのか？ また更新権限を持つ管理者はどこにいて、なぜ、更新しなかったのか？ 期限を自動的に更新するようになっていたのであれば、なぜ更新できなかったのか？

ソフトウェア証明書の期限が更新できなかった場合の影響範囲を特定していたのか？ 特定していた場合、なぜ通信システム障害になることを認識できなかったのか？

本当に、ソフトウェアだけの障害なのだろうか？ 今後の調査結果が待たれる。

システム運用

障害発生の検知からサービス復旧に向けた通信システムの運用活動は、どうなっていたのだろうか？ 次のような疑問がある。

今回の障害では、当初外部からのセキュリティ攻撃が疑われたようである。ソフトウェア障害がセキュリティ・コンポーネントで発生した場合、迅速なインシデント対応が重要になる。海外製品を使用している場合には、より的確な対応プロセスの構築が求められる。

また、ソフトウェア証明書の期限管理は通信システムの運用に関する情報である。システム運用情報の適切な管理プロセスの構築と、その監視が必要である。

分散システムの相互接続性

今回の通信システム障害では、無線通信が現代社会にとって欠かせない社会基盤になっていることを再認識することになった。たとえば、今後、自動運転が浸透していった場合、同様の通信システム障害が発生したら、大変な惨事を引き起こすところであった。無線通信システムと自動運転システムなどとのシステム連携が重要になる。自動運転システムでは地図情報を参照するために、通信システムとの相互接続が不可欠である。通信システムを使えなければ自動車が走行する場所についての正確な地図情報を獲得できなくなることから、安全な走行に支障をきたすことは間違いない。

したがって、通信システムの安全性を向上するとともに、連携システムとの相互運用性に対する安全性の保証が重要である。

網羅的な対策の必要性

あるテレビ番組でICT専門家だというコメンテータが、今回の通信システム障害の原因を「凡ミス」だと断定していた。このコメントを聞いていて、「果たして、そうなのか？」と疑問に思った。「凡ミス」などではなく、根が深い問題ではないのか？

上述したように、多くの「はずだ」が重なって、守るべき複数の基本動作が多重に抜けたことによって今回の支障が発生したのではないか？ そうだとすれば、これらのすべての「はずだ」について、「適切に実施されていることが、当たり前だから改めて確認するほどのことではない」と過信するのではなく、愚直に徹底して確認しなければ、このような障害を防ぐことはできないと思われる。

まとめ

上述したことをまとめると以下のとおりである。

- セキュリティ上の欠陥がシステム安全性に影響する
- セキュリティ対策の高信頼化を保証するためにテスト十分性を確認する必要がある
- セキュリティ・コンポーネントを保証する証明書の有効期限を管理する必要がある
- 分散システムの相互運用性を保証する仕組みを確立する必要がある

【参考】
[1] SoftBank、2018年12月6日「おうちのでんわ」、「SoftBank Air」がご利用できないまたはご利用しづらい状況について、https://www.softbank.jp/ybb/info/maintenance/
[2] エリクソン、ソフトバンクの障害情報に関するお知らせ、https://www.ericsson.com/jp/ja/press-releases/2/2018/12/1

<システム安全性のことなら下記へ>
yamamotosui@icts.nagoya-u.ac.jp