東北地区の大学・高専等のウェブサーバにおけるサーバ証明書の利用状況

水木 敬明, 森 倫子, 曽根 秀昭

東北大学 サイバーサイエンスセンター
東北大学 情報部情報基盤課
tm-paper+axies@g-mail.tohoku-university.jp

概要：東北大学サイバーサイエンスセンターに事務局が置かれている東北学術研究インターネットコミュニティ（TOPIC）には，東北地区の大学・高専・学術研究機関が参加している。本発表では，各 TOPIC 参加組織が運用するウェブサーバに関して，サーバ証明書の利用状況を考察する。具体的には，証明書の発行者，署名アルゴリズム，公開鍵，及び Record Protocol で利用される暗号化アルゴリズムについて調査及び考察する。

1 はじめに

東北地区には，学術研究・教育活動を支援するコンピュータネットワーク環境の発展に貢献することを目的とした「東北学術研究インターネットコミュニティ（TOPIC)」があり，東北地区の大学・高専・学術研究機関が参加することによりコミュニティを形成している。2013 年 11 月現在の会員機関数は 57 であり，TOPIC の事務局は東北大学サイバーサイエンスセンターに置かれている。

本稿は，各 TOPIC 参加機関が運用するウェブサーバに関して，サーバ証明書や SSL/TLS 技術の利用状況について調査し，その結果をとりまとめたものである。より具体的には，各 HTTPS（HTTP over SSL/TLS）サーバに対して，サーバ証明書の発行者，署名アルゴリズム，公開鍵，及び Record Protocol で利用される暗号化アルゴリズムについて調査及び考察する。

ハッシュ関数なども含めた暗号化アルゴリズムや SSL/TLS 技術の概要については，文献[1]がわかり易く，2008 年当時における政府公共系・金融系の HTTPS サーバの状況も報告されている。 本稿の報告は，同様な調査を現在の東北地区の大学・高専等のサーバに対して試みるものである。

2 調査対象 HTTPS サーバの列挙

本節では，調査対象とする HTTPS サーバをどのように選定したかについて説明する。

2.1 Google 検索による発見

TOPIC 参加機関が運用する HTTPS サーバを見付けるにあたっては，Google 検索を利用した。すなわち，「allinurl:https://*tohoku.ac.jp/」等を検索文字列として入力し，得られる検索結果から各 FQDN に対して代表的な URL を保存し，HTTPS サーバの 1 つとして記録した。

TOPIC のウェブページの「参加組織一覧」においてリンクされている各機関のドメインに基づいて上述の検索を実施した。実施時期は 2013 年 9 月である（東北大学のドメインのみ 6 月に実施した)。

以上の要領で作成してあった HTTPS サーバのリストに基づき，再度 2013 年 11 月にリスト中のすべての URL に対してウェブブラウザで接続を試み，HTTPS として接続可能なもののみを抽出して，最終的な調査対象 HTTPS サーバとした。

2.2 調査対象サーバの概況

前述の方法で調査対象となった HTTPS サーバを有する TOPIC 参加機関は 38 機関であり，サーバの合計数は 171 であった。その内訳として，3 台以上のサーバを持つ機関を表に記す。

TOPIC 参加機関	台数
東北大学（tohoku.ac.jp）	64
秋田大学（akita-u.ac.jp）	10

北里大学（kitasato-u.ac.jp）	8
弘前大学（hirosaki-u.ac.jp）	7
東北学院大学（tohoku-gakuin.ac.jp）	7
会津大学（u-aizu.ac.jp）	5
岩手県立大学（iwate-pu.ac.jp）	5
山形大学（yamagata-u.ac.jp）	5
福島大学（fukushima-u.ac.jp）	5
仙台高等専門学校（sendai-nct.ac.jp）	4
岩手医科大学（iwate-med.ac.jp）	4
岩手大学（iwate-u.ac.jp）	4
石巻専修大学（isenshu-u.ac.jp）	4
八戸工業大学（hi-tech.ac.jp）	4
東北福祉大学（tfu.ac.jp）	3
福島県立医科大学（fmu.ac.jp）	3

無論,今回対象となったHTTPSサーバでTOPIC参加機関が運用するすべてのものを網羅しているわけでは決してなく，ここで見付からなかったサーバも潜在的に数多く存在することが予想される（例えば，もちろん各機関の内部ネットワーク等で利用されているサーバは見付からないし，Google 検索にクロールされていないサーバも漏れている)。

次に，171 個の各 FQDN から（冒頭の）ホスト名を取り出して数え上げ，2 個以上のものを並べると次の表のようになった。

ホスト名	個数
www	58
webmail	9
wm	4
portal	4
ia	3
www3	2
wmail	2
ssl	2
menkyo	2
mail	2
lms	2

必ずしもホスト名の文字列が SSL/TLS の上にのっているサービスを表すとは限らないが，おおよその傾向は見て取ることができる。文字列として最も数の多かった「www」は，その機関や機関内の部局等における情報を発信するウェブサイトであるケースが多い。また，例えば「webmail」,「wm」,「wmail」及び「mail」は，その名の通り，ウェブメールのサービスを提供するものばかりであった。その他，(ID/PW によるユーザのログインを必要とする）ポータルサービスや VPN サービス，教育コンテンツ系サービス等の提供において HTTPS サーバが活用されている様子がわかる。

3　サーバ証明書の発行者の調査

本節では，調査対象の HTTPS サーバが利用しているサーバ証明書の発行者の情報を調査する。具体的には，OpenSSL を用いて，次のコマンドにより得られる Issuer の情報を取得し，とりまとめる。これ以降に記載する調査はすべて 2013 年 11 月に行った。

```
% openssl s_client -connect www.tohoku.ac.jp:443
–showcerts < /dev/null
```

以下に，発行者となっている数が多かったものの上位 6 つを示す。

発行者	サーバ数
NII Open Domain CA - G2	69
VeriSign Class 3 Secure Server CA - G3	23
GlobalSign Domain Validation CA - G2	13
RapidSSL CA	9
Cybertrust Japan Public CA G2	7
AlphaSSL CA - G2	5

最も数の多い「NII Open Domain CA - G2」は，国立情報学研究所の「UPKI オープンドメイン証明書自動発行検証プロジェクト」[2]によるもので，このプロジェクトに参加する機関は費用の負担なくサーバ証明書を発行してもらえることもあり，TOPIC 参加機関も非常に大いに利用していることがわかる。すなわち，全体の 171 サーバ中，69 サーバが NII の証明書を利用しており，その率は約 4 割である。

なお，表には含まれない発行者によるサーバ証明書の中には，自己署名証明書（いわゆるオレオレ証明書）のものもいくつか散見された。

また，各サーバから送られてくる（上位のものも含めた）証明書の数をカウントすると，次のような結果となった。

送られてくる証明書数	サーバ数
1	27
2	105
3	32
4	7

送られてくる証明書が1つしかない27サーバのうち，自身の証明書が自己署名証明書ではなかったものは3つであった。

また，送られてくる証明書の数が 4 である 7 サーバについて調べてみると，そのうちの 2 つのサーバは，自身のサーバ証明書を 2 個（同じものを）送っていた。残りの 5 つのサーバは，自身の証明書，中間証明書，クロス証明書，及び（1024 ビットの）ルート証明書を送っていた（ベリサインのクロスルート方式による検証に対応しているものと考えられる)。

4　署名アルゴリズムの調査

本節では，サーバ証明書に付いてくる署名について，その生成アルゴリズムを調査する。得られた結果は次の通りである。

署名アルゴリズム	サーバ数
sha1WithRSAEncryption	166
md5WithRSAEncryption	4
sha256WithRSAEncryption	1

この表からわかる通り，ほとんどのサーバ証明書では， RSA とハッシュ関数 SHA-1 との組み合わせによる署名アルゴリズムが用いられていた。それ以外の組み合わせのものも含めて，RSA の実体としてはすべて RSASSA-PKCS1-v1_5 が使用されている。

また，署名に使われた鍵の長さについて，送られてくる上位のサーバ証明書に基づいて（サーバから複数の証明書が送られてくるものを対象に機械的に）チェックしたところ，1 つを除きすべて 2048 ビットであった。その例外の 1 つは鍵長が 1024 ビットであったが，個別に調査したところ，送られてくる（有効期限切れの）中間証明書に含まれる鍵の長さが 1024 ビットというだけで，実際の署名は 2048 ビットのものでなされており，（ストアされているルート証明書と中間証明書により）ウェブブラウザでの接続には問題がなかった。

5　公開鍵の調査

本節では，各サーバの公開鍵の情報を調査する。その結果，すべてのサーバで rsaEncryption が用いられていることがわかり，鍵長も含めた内訳は次の通りである。

公開鍵	サーバ数
rsaEncryption (2048bit)	149
rsaEncryption (1024bit)	20
rsaEncryption (512bit)	2

近年指摘されているように，2048 ビット未満の RSA 鍵の利用は適切ではないと考えられる。

6　Record Protocol における暗号化通信

本節では，SSL/TLS の Record Protocol において，各サーバがどのような暗号化アルゴリズムを受け入れるかを調査する。具体的には，OpenSSL を用いて，次の 5 つの暗号スイートを対象にして実験を実施した。

(a) CAMELLIA256-SHA
(b) AES256-SHA
(c) AES128-SHA
(d) RC4-SHA
(e) RC4-MD5

実験の結果を次に示す。

(a)	(b)	(c)	(d)	(e)	サーバ数
	✔	✔	✔	✔	109

✔	✔	✔	✔	✔	39
			✔	✔	8
✔	✔	✔	✔		5
✔	✔	✔			4
	✔	✔	✔		3
		✔	✔	✔	2
	✔	✔			1

この表では，チェック（✔）の入っている暗号スイートに対応しているサーバの台数を記載している。この結果からは，利用可能な暗号スイートについて，チューニングを行っているサーバは少ないように見受けられる。

7 おわりに

本稿では，東北地区の大学・高専・学術研究機関が参加している TOPIC 参加組織を対象に，サーバ証明書の利用状況や HTTPS サーバの設定状況を調査した。

今回の調査はごく基本的なものであるが，おおよその動向の把握はできたと考える。よりセキュリティ脆弱性等に特化した項目も含め大規模な調査が文献[3]で報告されている。また，サーバの暗号設定の確認に適したツールも提案されている[4, 5]。鍵の作成時に共通の素数を使ってしまうことによる脆弱性の問題も昨年来，注目を集めている[6]。今後もよりきめ細かい調査を継続してゆきたい。なお，ウェブブラウザが利用可能な暗号スイートの確認には，「SSL Client Test」のサイト[7]が便利である。

謝辞

2.1 節で述べた 2013 年 6 月と 9 月の検索による HTTPS サーバのリスト化にあたっては，東北大学工学部曽根・水木研究室の 4 年生の皆さんにご尽力頂いた。

参考文献

[1] 神田雅透, 暗号アルゴリズムの安全性のお話, Internet Week 2008 プレゼンテーション, 2008. https://www.nic.ad.jp/ja/materials/iw/2008/proceedings/H10/IW2008-H10-01.pdf

[2] 国立情報学研究所, UPKI オープンドメイン証明書自動発行検証プロジェクト. https://upki-portal.nii.ac.jp/docs/odcert

[3] 須賀祐治, 地方自治体 Web サイトの SSL 設定状況に関する 2012 年度と 2013 年度の比較・考察（速報版）, コンピュータセキュリティシンポジウム 2013, pp.1002-1009, 2013.

[4] 佐藤亮太, 吉田勝彦, 知加良盛, 関良明, 神田雅透, SSL における暗号設定確認ツールの提案と評価, 情報科学技術フォーラム, FIT 2011, pp.119-126, 2011.

[5] Qualys SSL Labs, SSL Server Test. https://www.ssllabs.com/ssltest/index.html

[6] 黒川貴司, 野島良, 盛合志帆, "Mining Your Ps and Qs" のその後, コンピュータセキュリティシンポジウム 2013, pp.986-993, 2013.

[7] Qualys SSL Labs, SSL Client Test. https://www.ssllabs.com/ssltest/viewMyClient.html