D2-2 新技術に対応するセキュリティ運用とは ～変わりゆく技術の中でぼくらは～ 第1部

2019年11月27日

日本セキュリティオペレーション事業者協議会
新技術とオペレーションプロジェクト
セキュリティオペレーション連携WG(WG6)

司会進行

- 武井　滋紀　です。
- JNSAのISOG-Jの方から来ました
  - ISOG-J 副代表、セキュリティオペレーション連携WG(WG6)リーダー
- NTTテクノクロス株式会社
  - セキュアシステム事業部　第三ビジネスユニット　勤務
  - 2016年度までは社名が「NTTソフトウェア株式会社」でした
  - NTTグループ セキュリティプリンシパル
  - CISSP、情報処理安全確保支援士

講演者

- ももいやすなり
  株式会社インターネットイニシアティブ
  セキュリティ本部 セキュリティ情報統括室 リードエンジニア
  - サービス開発、システム開発、研究開発、ネタ披露、宴会調整
  - IIJ-SECT (CSIRT)、関連団体 (ISOG-J, ICT-ISAC, NCA など)、技術コミュニティ
  - 食べ物、ヘヴィメタル、ねこ



- SOC 見学やってます
- セキュリティ情報発信
  - wizSafe Security Signal
  - IIR, IIJ Security Diary, IIJ Engineers blog
    - IIR Vol.40 の記事を書きました

IIJ-SECT
IIJ Group Security Coordination Team
wizSafe
安全をあたりまえに

講演者

- **亀田　勇歩**

  SCSK株式会社　セキュリティアナリスト
  - Web/PF脆弱性診断
  - SOC監視業務
  - インシデントレスポンス

  ISOG-J / OWASP / 他
  - **ZAP**エヴァンジェリスト
  - **脆弱性診断士**の活動
  - 東京電機大学 国際化サイバーセキュリティ学特別コース(CySec) 外部講師

  趣味
  - 2019年のラスベガスで開催された**DEFCON OSINT CTF**で**5位**入賞してきました
  - 2019年の11/2に国内で4回目の**Open xINT CTF**を**開催**してきました

ISOG-J とは

- 日本セキュリティオペレーション事業者協議会
  - the Information Security Operation providers Group Japan
  - 2008年創立、2019年10月現在 51組織が加盟
  - プロのセキュリティオペレーター、事業者の集まり
  - 業界の発展のために課題を議論したり、互いに情報を出し合うことで外部へ成果を発表する団体です
  - 親団体は日本ネットワークセキュリティ協会(JNSA)
- http://isog-j.org/
  - Facebook ページ: /isogj
  - ISOG-J の読み方: いそぐじぇい

こんなドキュメントをリリースしています！

- セキュリティ対応組織(SOC,CSIRT)の教科書 v2.1
  - http://isog-j.org/output/2017/Textbook_soc-csirt_v2.html
  - ハンドブックや組織の成熟度を測るチェックリストも配布しています

- セキュリティ対応組織(SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」
  - http://isog-j.org/output/2017/5W1H-Cyber_Threat_Information_Sharing_v1.html

  ※英語版もあります！！
  Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT

- 是非ご活用ください！

参照されております！

- 経済産業省「サイバーフィジカルセキュリティ対策フレームワーク案」
  - 添付C 対策要件に応じたセキュリティ対策例
  - D.3 ISO/IEC 27001 の管理策群と「サイバー・フィジカル・セキュリティ対策フレームワーク」との対応表
- 経済産業省「サイバーセキュリティ経営ガイドライン Ver.2.0 実践のためのプラクティス集」
  - プラクティス 2-1 サイバーセキュリティリスクに対応するための、兼任のサイバーセキュリティ管理体制の構築
  - 付録 サイバーセキュリティリスクの管理体制構築(指示1,2,3)

ISOG-J ホームページ
https://isog-j.org
よりダウンロード可能

前回までのおさらい

（参考）2015年の10のコツ

1. 防御から対応までのすべてをSOCに統合せよ
2. 規模と透明性/俊敏性のバランスを取れ
3. SOCに適切な権限を与えよ
4. できる事をやろう
5. メンバーは量より質を重視せよ
6. 買った技術は最大限利用せよ
7. データを集めて整理せよ
8. SOCの任務遂行を保護する
9. 脅威情報の賢い消費者であり供給者であれ
10. 冷静に・計算高く、プロらしく対応せよ

資料URL（約100ページ、4.74MB）
https://www.nic.ad.jp/ja/materials/iw/2015/proceedings/s13/

(参考) 2016年の「失敗から学ぶ」から

- セキュリティの対応組織の構築時、運用時、インシデントレスポンス時に分けて、ありがちな「失敗あるある」を定義。

- 「失敗あるある」に陥らないために「セキュリティ対応組織の教科書 v1.0」をリリース。

資料URL（58ページ、5.1MB）

https://www.nic.ad.jp/ja/materials/iw/2016/proceedings/d1/d1-3-hayakawa.pdf

(参考) 2016年のセキュリティ対応組織の教科書から

- 組織全体を俯瞰すべく、**9つの機能と54の役割**で定義
- 54の役割を**4つの領域**に分類
- 4つの領域について、自組織で実施すべきもの（インソース）と専門組織へ依頼するもの（アウトソース）のパターンを**4つのパターン**で定義

(参考) 2017年の「今求められるSOC,CSIRTの姿とは」から

- 教科書を元にしたインシデント時の実際のフロー、何もない平時に何をすべきか。そこから成熟度モデルの紹介へ。

- 現在の情報共有のニーズと、一方現場で起きている課題の整理。

資料URL（2つ、5.24MB+3.78MB）

https://www.nic.ad.jp/ja/materials/iw/2017/proceedings/d1/

(参考) 2018年の「もう一人で困らない！セキュリティ対応のアウトソース」から

- 2009年公開のマネージドセキュリティサービス選定ガイドから、今のアウトソースの考え方に整理。

- 担当が一人で困るシーンが増えているなかで、組織の業務や網羅性、どの部分をどう考えてアウトソースするか。

資料URL（2つ、3.8MB+2.32MB）

https://www.nic.ad.jp/ja/materials/iw/2018/proceedings/d2/

今年は？

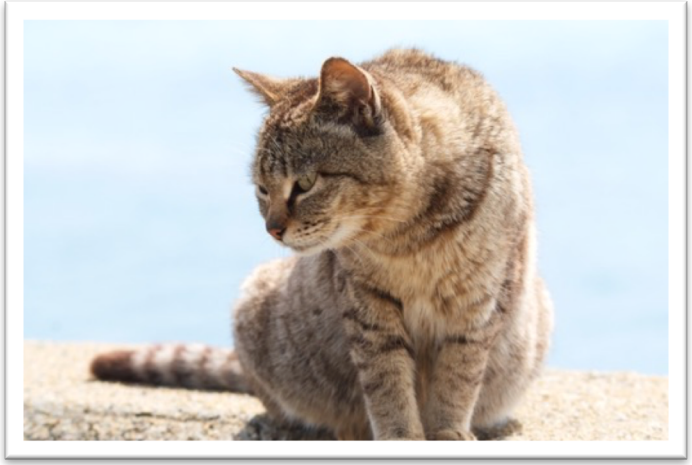
セキュリティは「新陳代謝」の速度が早い

10年前とは形も範囲もかなり変わってきた

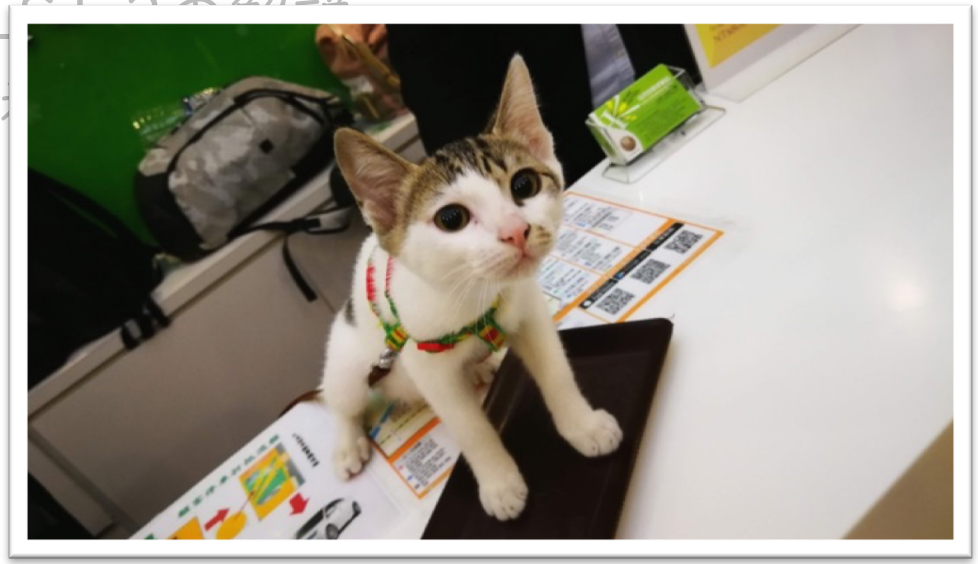
新たな技術とどう向きあうべきか考えます

前半の目次

- 新技術とオペレーションプロジェクト
- TLS1.3をとりあげた理由
- TLS1.3の解説
- 監視運用で困りそうなポイントQ&A



- 新技術とオペレーションプロジェクト
- TLS1.3をとりあげた理由
- TLS1.3の解説
- 監



新技術がセキュリティオペレーションに及ぼす影響を考える

- 新技術や環境の変化でセキュリティオペレーションも変化
  - FW, IDS/IPS, WAF, Application GW, ...
  - クラウドサービス, スマホ/タブレット, BYOD, ...
  - SOC/CSIRT, 法制度, 業界標準, ...
  - ブロッキング, DNS over HTTPS, Encrypted SNI, ...
- TLS1.3もそのひとつ
  - インターネットを安全にするため
  - セキュリティオペレーションの現場では？
- 新技術をセキュリティオペレーションの視点から分析する

- 新技術とオペレーションプロジェクト
- TLS1.3をとりあげた理由
- TLS1.3の解説
- 監視運用で困りそうなポイント

TLS1.3を調査した理由

- RFC8664としてリリース(2018/08)
  - 4年、draft 28

- 暗号系の話は難しい
  - ちゃんと調べて理解する必要がある
- 中間者攻撃ができなくなった？
  - つまり、通信路での通信記録ができなくなった？
  - セキュリティのため通信記録をとっているオペレーションに影響する
- みんなでちゃんと勉強して、理解して、議論しよう

- 新技術とオペレーションプロジェクト
- TLS1.3をとりあげた理由
- TLS1.3の解説
- 監視運用で困りそうなポイントQ&A

須賀さんにバトンタッチ

- 新技術とオペレーションプロジェクト
- TLS1.3をとりあげた理由
- TLS1.3の解説
- 監視運用で困りそうなポイントQ&A

困りそうなポイントQ&A

- 素朴な疑問、ちまたでよく見かける疑問
- 会場で専門家とオペレーターが直接ディスカッションします

いままでのようにはいかなくなる？ (1)

- これまでと同じようにプロキシログを監視する場合、通信先のURLしか見えなくなる？
- パケットを収集する機器での解析ができなくなる？
- 今でもhttpsの通信が大半だけど、TLS1.3でますます見えない部分が増えていく？

いままでのようにはいかなくなる？ (2)

- プロキシ製品を導入する時、今までとの違いはある？
- 拠点間やデータセンター間などの通信もTLS1.3化する必要がある？
- PCI DSSは現在TLS1.2推奨。1.3が推奨になったらどうするの？

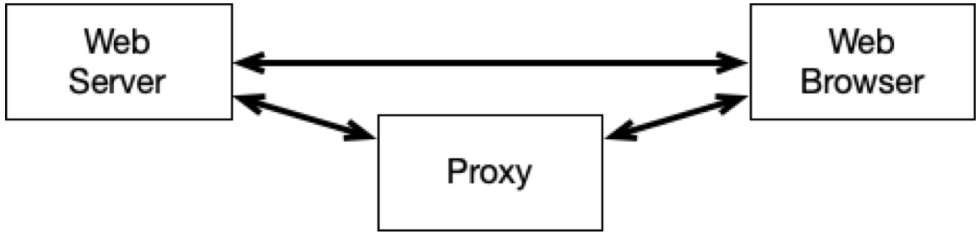
質疑

試してみようTLS1.3

TLS1.3を試してみたい人向けコーナー

- 実際に環境を作ってみよう
  - 手順と内容をご紹介します
- 環境の作り方 (あなたも試せます)
- サーバ、クライアントの動作確認
- 通信を記録してみる
- プロキシログを見る
- クライアントで通信内容を確認する

環境の作り方



- 必要なもの
  - サーバ (VPSなど)
  - FQDN
  - Web ブラウザ
- サーバ: OpenSSL 1.1.1 (最新は1.1.1d) を用意
  - Ubuntu 18.04.3 LTS ←今回はこちらで
  - CentOS 8
- openssl version で確認

```
ubuntu:~$ openssl version
OpenSSL 1.1.1  11 Sep 2018
```

```
centos8:~$ openssl version
OpenSSL 1.1.1 FIPS  11 Sep 2018
```

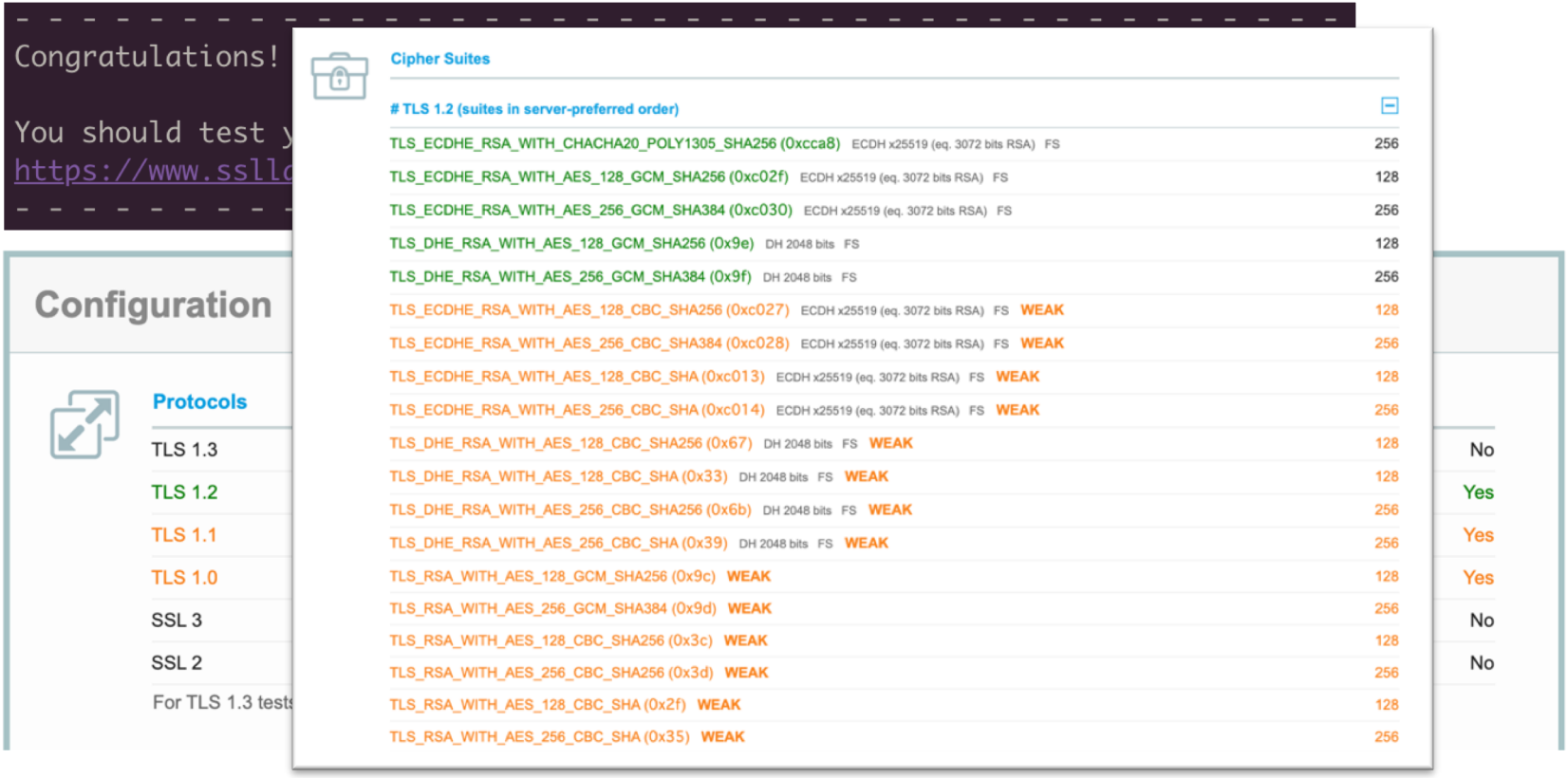
Web サーバ周りをインストール & 設定

- nginx, Apache などお好みのものを
  - それに対応した certbot をあわせて…
- 設定
  - ひな形は /etc/nginx/sites-available/default
- ufw 設定
- certbot を実行する
  - nginx と FQDN を指定
  - 質問に答える
    - HTTP -> HTTPS にリダイレクト
  - 設定を確認…

```
sudo ufw status
sudo ufw allow from any to any port http
sudo ufw allow from any to any port https
```

```
sudo certbot --nginx -d tls2.isog-j.org
```

動作確認??



設定を確認

- TLS1.3 を有効にする
  - 試しに TLS1.3 だけ有効にしてみた

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

```
ssl_protocols TLSv1.3;
```

動作確認???

Configuration

Protocols

TLS 1.3	Yes
TLS 1.2	No
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we only support RFC 8446.

Cipher Suites

 # TLS 1.3 (suites in server-preferred order)

TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS	128

Handshake Simulation

Android 8.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Chrome 69 / Win 7 R	Server sent fatal alert: protocol_version			
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Chrome 75 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Firefox 62 / Win 7 R	Server sent fatal alert: protocol_version			
Firefox 67 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.1.0k R	Server sent fatal alert: protocol_version			

設定を確認(2)

- CRYPTREC 設定ガイドを見る
  - TLSv1.2, TLSv1.3 を設定する (ガイドは TLSv1.2 のみ推奨)
  - DHE, ECDH, ECDHE 鍵パラメーターを設定する
    - certbot の設定で大丈夫そうでした
  - HSTS を設定する
    - リダイレクトは certbot が設定済み
  - OCSP stapling を有効化

動作確認(1)

Protoc

TLS 1.3 Yes
TLS 1.2 Yes
TLS 1.1 No
TLS 1.0 No
SSL 3 No
SSL 2 No
For TLS

Cipher Suites

 # TLS 1.3 (suites in server-preferred order)

TLS_AES_256_GCM_SHA384 (0x1302)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128

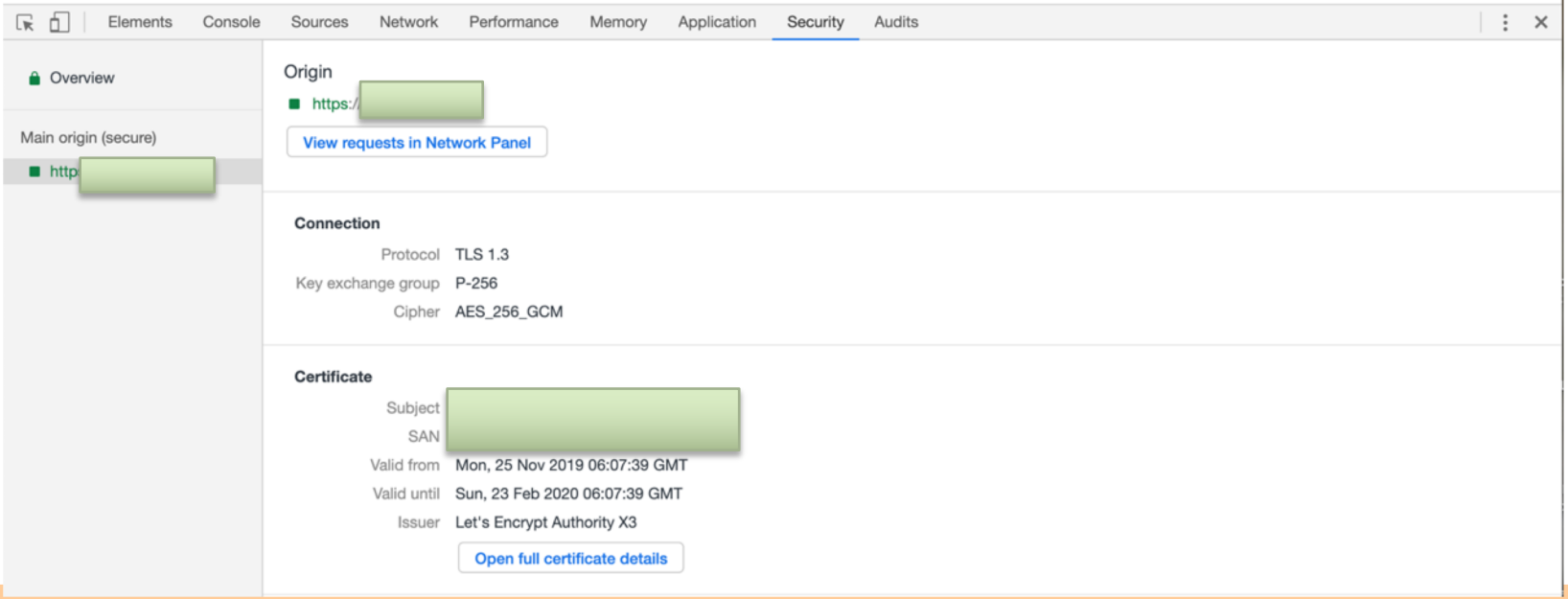
 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits FS **WEAK**	128

動作確認(2)

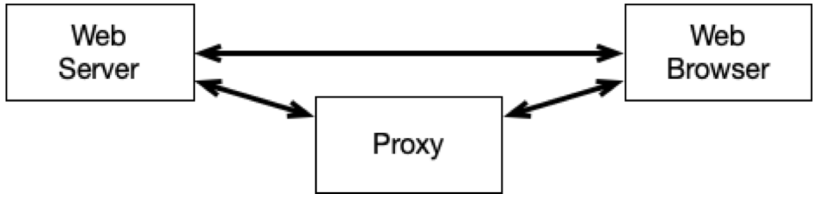
A test page for Internet Week
TLS1.3 session

official ISOG-J web page is here.



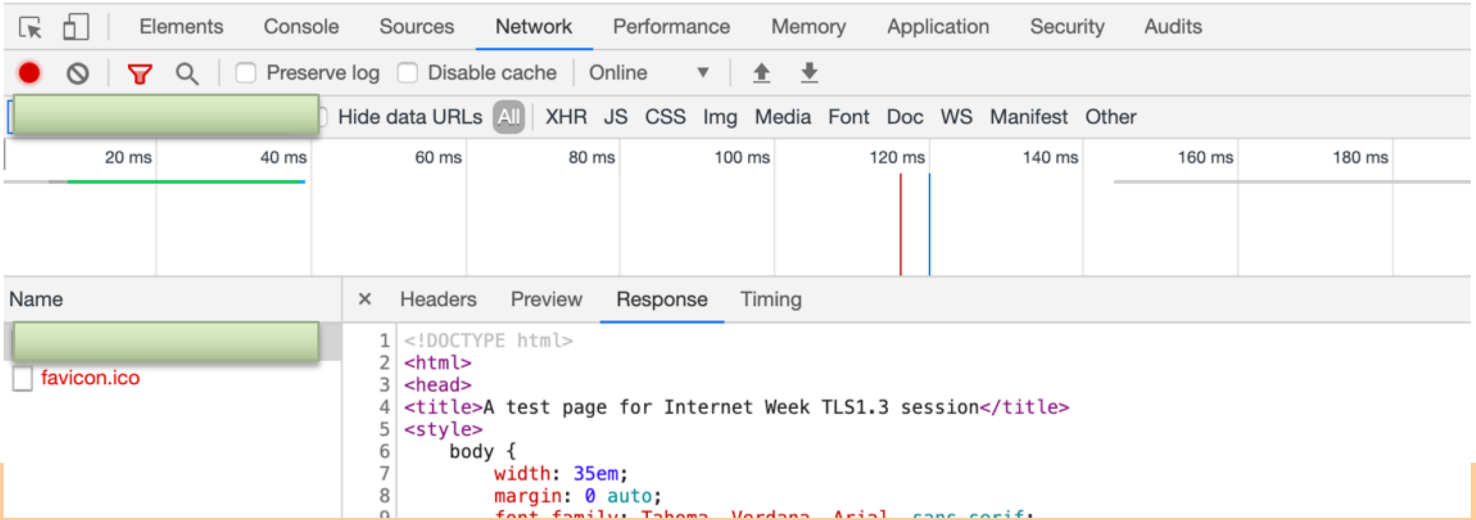
クライアント側で通信内容を確認する

- Chrome Developer Tools



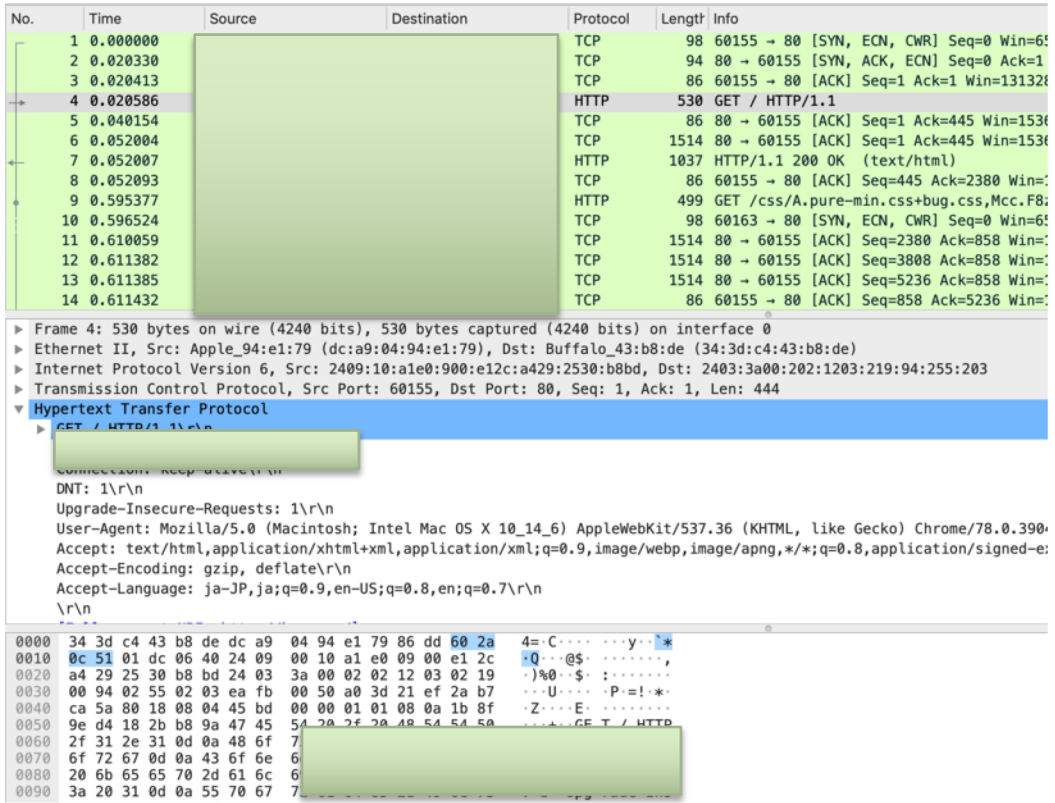
A test page for Internet Week TLS1.3 session

official ISOG-J web page is here.

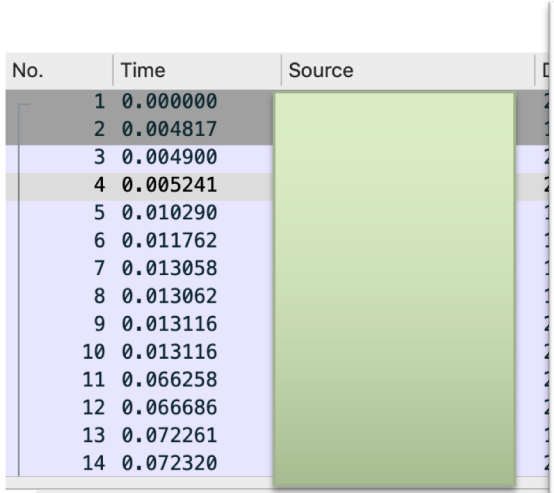


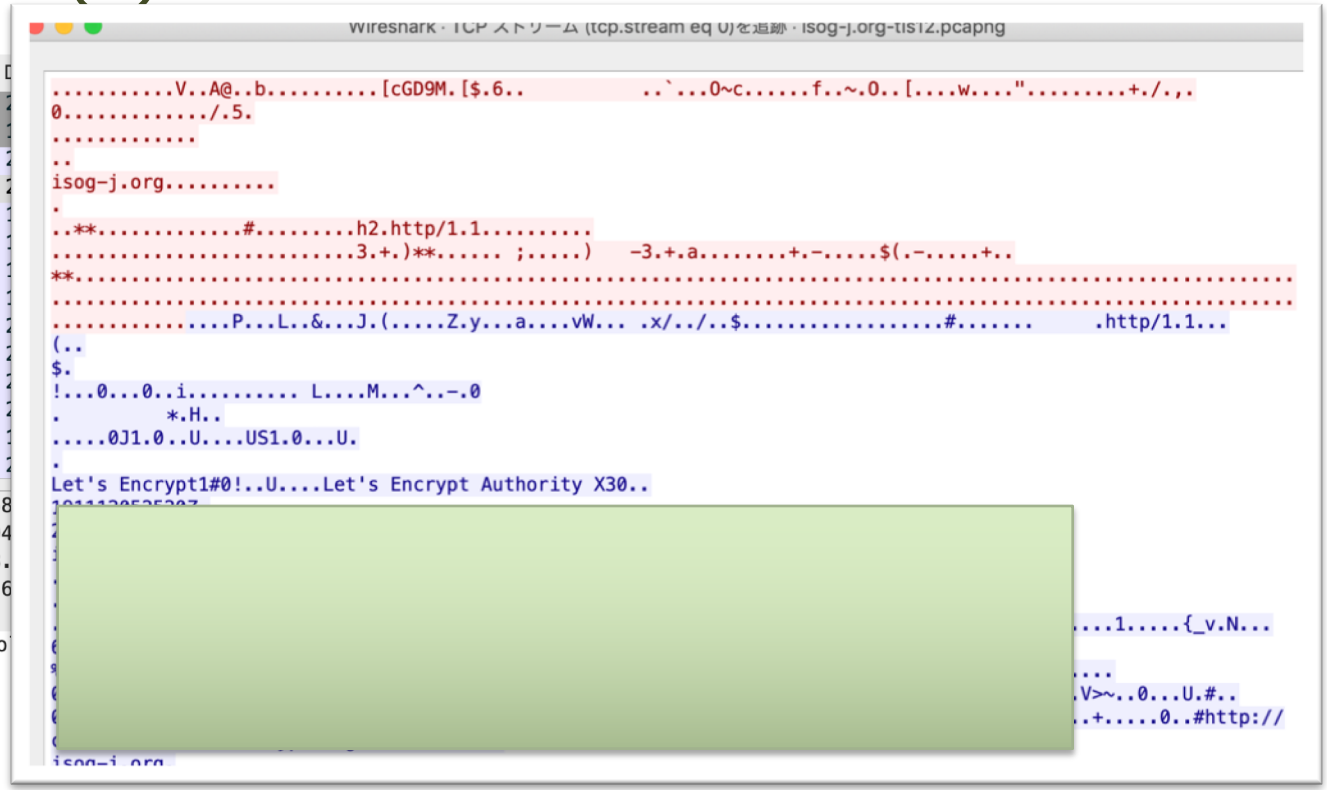
通信を記録してみる(1)

- みんな大好き Wireshark



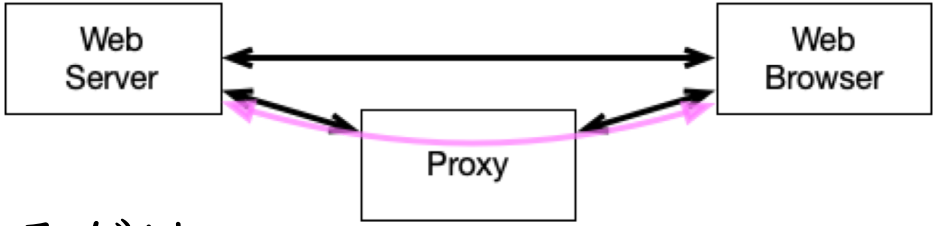
通信を記録してみる(2) TLS1.2





通信を記録してみる(3) TLS1.3

プロキシログを見てみる



- Squid cache を設定
- TLS は CONNECT で仲介するだけ
- SSL Bump
  - TLS ログ、透過プロキシなど
  - TLS1.3 未対応？

```
x.x.x.x TCP_MISS/200 3020 GET http://[redacted]~momo/ - HIER_DIRECT/[redacted] text/html
x.x.x.x TCP_MISS/200 2780 GET http://[redacted]image/apache_pb.gif - HIER_DIRECT/[redacted] image/gif
```

```
x.x.x.x TCP_TUNNEL/200 692 CONNECT [redacted]org:443 - HIER_DIREC[redacted].94 -
x.x.x.x TCP_TUNNEL/200 692 CONNECT [redacted]org:443 - HIER_DIREC[redacted].94 -
x.x.x.x TCP_TUNNEL/200 39 CONNECT ww[redacted]m:443 - HIER_DIRECT/[redacted]96 -
x.x.x.x TCP_TUNNEL/200 28306 CONNECT [redacted]:443 - HIER_DIRECT/2[redacted] -
x.x.x.x TCP_TUNNEL/200 805 CONNECT [redacted]43 - HIER_DIRECT/27.[redacted]
```

10分休憩

(参考：アイコン、漫画素材)
http://www.security-design.jp/
http:// www.chojugiga.com/
(写真素材) たにぃさん、ももい