

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

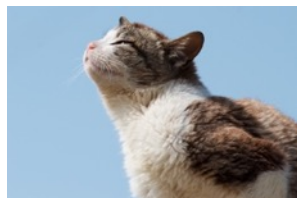
株式会社インターネットイニシアティブ

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



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: いそぐじえい

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「5WIH」
 - http://isog-j.org/output/2017/5WIH-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



The screenshot shows the ISOG-J website with a navigation menu and a main content area. The navigation menu includes: ISOG-Jについて (about us), 参加・関連団体 (members), 活動紹介 (activities), イベント (event information), and お問い合わせ (contact). The main content area features a header with the ISOG-J logo and name, followed by a paragraph in Japanese describing the organization's mission. Below this is a section titled '活動紹介' (Activities) with a sub-section '活動成果' (Activity Results). The '活動成果' section contains a link to 'セキュリティ対応組織の教科書 v2.1 (2018年9月)' and a detailed text block explaining the update of the textbook. At the bottom of the page, there is a '関連リンク' (Related Links) section with logos for JNSA, JPCERT/CC, IPA, IA Japan, and WASForum.jp.

ISOG-Jについて
about us

参加・関連団体
members

活動紹介
activities

イベント
event information

お問い合わせ
contact

HOME > 活動紹介 > 活動成果

活動紹介

WGの活動内容
活動成果

関連リンク
links

JNSA
JPCERT/CC®
IPA
IA japan
WASForum.jp
Web Application Security Forum

セキュリティ対応組織の教科書 v2.1 (2018年9月)

2018年9月に、「セキュリティ対応組織の教科書」の概要版となる「ハンドブック v1.0版」と54の役割を一覧できる別紙を追加しております。
2018年3月に、「セキュリティ対応組織成熟度セルフチェックシート」のアウトソースに関する基準を見直したv2.1版に更新しております。
【WG6】セキュリティオペレーション連携WGにおいて、「セキュリティ対応組織の教科書 v1.0」の改版に向けて議論を続けてきました。その中でセキュリティ対応組織に求められる9の機能と、54の役割を、実際のインシデント発生時や平時におけるフローとしてまとめました。また「セキュリティ対応組織成熟度セルフチェックシート」として組織の成熟度をポイント化するツールと合わせて「セキュリティ対応組織の教科書 v2.0」を公開しました(2017年10月 v2.0)。

- 「セキュリティ対応組織の教科書 ハンドブック v1.0」(PDF形式)
- 「セキュリティ対応組織の教科書 ハンドブック 別紙 v1.0」(PDF形式)
- 「セキュリティ対応組織成熟度セルフチェックシート」(Excel形式)
- 「セキュリティ対応組織の教科書 v2.1」(PDF形式)
- 「セキュリティ対応組織の教科書 別表 v2.0」(PDF形式)
- フィードバックはこちら(Surveymonkey)

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/sl3/>

(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？

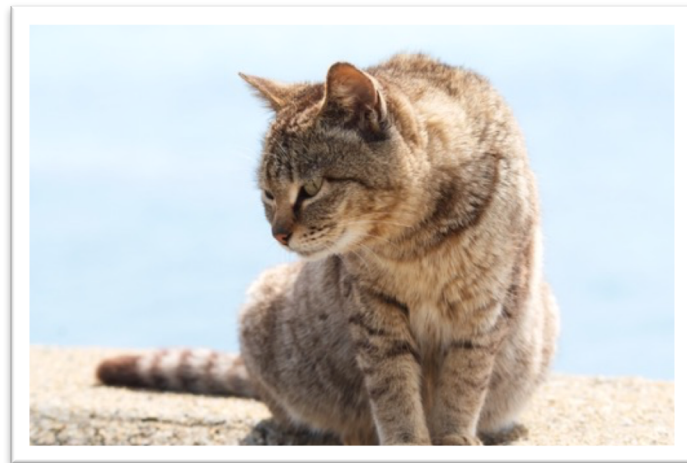
セキュリティは「新陳代謝」の速度が早い

10年前とは形も範囲もかなり変わってきた

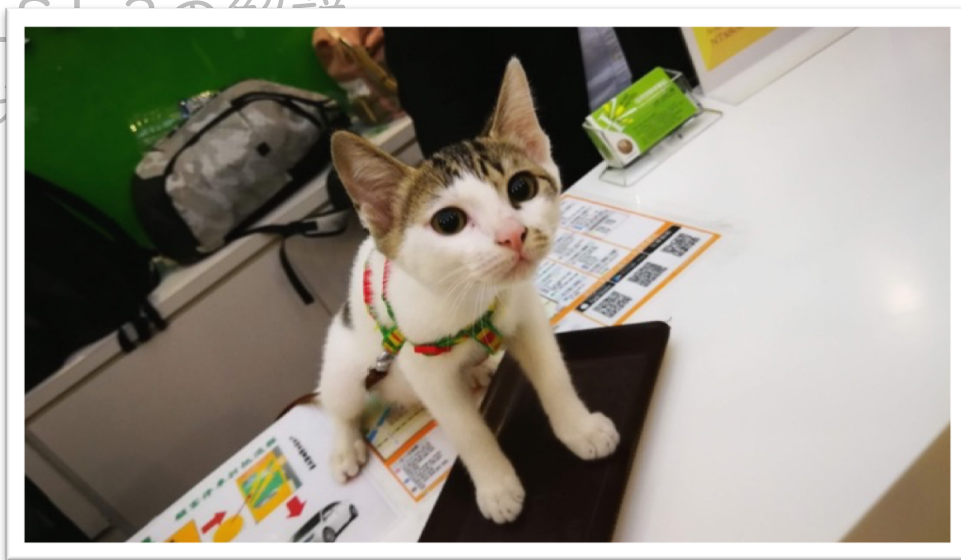
新たな技術とどう向きあうべきか考えます

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

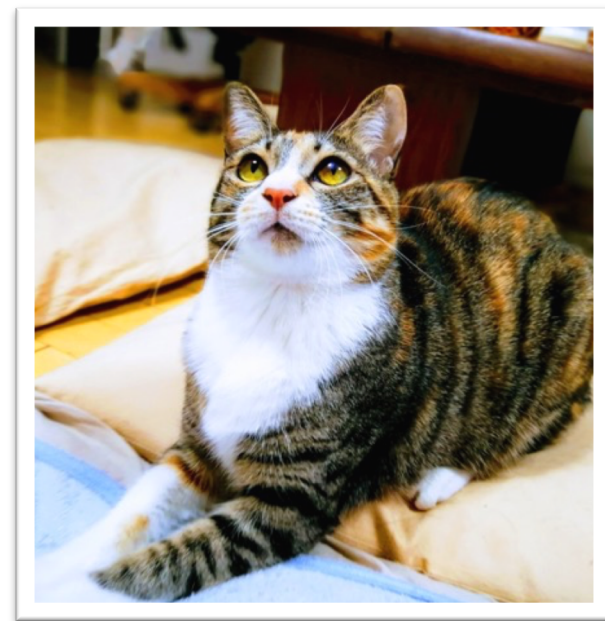
- 新技術とオペレーションプロジェクト
- TLS1.3をとりあげた理由
- TLS1.3の解説
- 監視運用で困りそうなポイント



TLS 1.3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

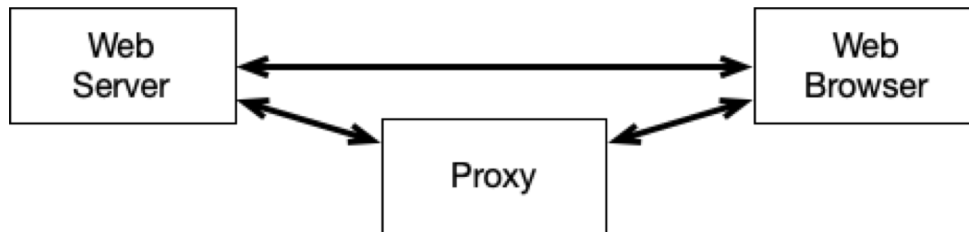
試してみようTLS1.3

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??

Congratulations!
 You should test y
<https://www.ssllc>

Configuration

Protocols

- TLS 1.3
- TLS 1.2**
- TLS 1.1
- TLS 1.0
- SSL 3
- SSL 2
- For TLS 1.3 test

Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0a8)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (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 x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits FS WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS WEAK	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits FS WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256

No
 Yes
 Yes
 Yes
 No
 No

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

TLS 1.2

TLS 1.1

TLS 1.0

SSL 3

SSL 2

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

Yes

Yes

No

No

No

No

動作確認(2)

A test page for Internet Week TLS1.3 session

official ISOG-J web page is [here](#).

The screenshot shows the Chrome DevTools Security panel. The left sidebar has 'Overview' selected, and the main panel displays the 'Origin' and 'Connection' sections. The 'Origin' section shows a redacted URL and a button to 'View requests in Network Panel'. The 'Connection' section shows the following details:

Protocol	TLS 1.3
Key exchange group	P-256
Cipher	AES_256_GCM

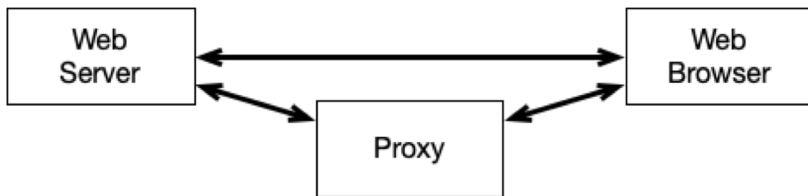
The 'Certificate' section shows the following details:

Subject	[Redacted]
SAN	[Redacted]
Valid from	Mon, 25 Nov 2019 06:07:39 GMT
Valid until	Sun, 23 Feb 2020 06:07:39 GMT
Issuer	Let's Encrypt Authority X3

There is a button 'Open full certificate details' at the bottom of the certificate section.

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](#).

The screenshot shows the Chrome Developer Tools Network tab. The 'Network' tab is selected, and a request for 'favicon.ico' is highlighted. The 'Response' tab is open, showing the HTML content of the response. The response is a test page for Internet Week TLS1.3 session.

Name	Headers	Preview	Response	Timing
favicon.ico			<pre>1 <!DOCTYPE html> 2 <html> 3 <head> 4 <title>A test page for Internet Week TLS1.3 session</title> 5 <style> 6 body { 7 width: 35em; 8 margin: 0 auto; 9 font-family: Tahoma, Verdana, Arial, sans-serif;</pre>	

通信を記録してみる(1)

- みんな大好き Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000			TCP	98	60155 → 80 [SYN, ECN, CWR] Seq=0 Win=65535
2	0.020330			TCP	94	80 → 60155 [SYN, ACK, ECN] Seq=0 Ack=1
3	0.020413			TCP	86	60155 → 80 [ACK] Seq=1 Ack=1 Win=131328
4	0.020586			HTTP	530	GET / HTTP/1.1
5	0.040154			TCP	86	80 → 60155 [ACK] Seq=1 Ack=445 Win=1536
6	0.052004			TCP	1514	80 → 60155 [ACK] Seq=1 Ack=445 Win=1536
7	0.052007			HTTP	1037	HTTP/1.1 200 OK (text/html)
8	0.052093			TCP	86	60155 → 80 [ACK] Seq=445 Ack=2380 Win=65535
9	0.595377			HTTP	499	GET /css/A.pure-min.css+bug.css,Mcc.FB:...
10	0.596524			TCP	98	60163 → 80 [SYN, ECN, CWR] Seq=0 Win=65535
11	0.610059			TCP	1514	80 → 60155 [ACK] Seq=2380 Ack=858 Win=65535
12	0.611382			TCP	1514	80 → 60155 [ACK] Seq=3808 Ack=858 Win=65535
13	0.611385			TCP	1514	80 → 60155 [ACK] Seq=5236 Ack=858 Win=65535
14	0.611432			TCP	86	60155 → 80 [ACK] Seq=858 Ack=5236 Win=65535

```

▶ Frame 4: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface 0
▶ Ethernet II, Src: Apple_94:e1:79 (dc:a9:04:94:e1:79), Dst: Buffalo_43:b8:de (34:3d:c4:43:b8:de)
▶ Internet Protocol Version 6, Src: 2409:10:a1e0:900:e12c:a429:2530:b8bd, Dst: 2403:3a00:202:1203:219:94:255:203
▶ Transmission Control Protocol, Src Port: 60155, Dst Port: 80, Seq: 1, Ack: 1, Len: 444
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1
    Connection: keep-alive\r\n
    DNT: 1\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3902.96 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ja-JP,j;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
0000 34 3d c4 43 b8 de dc a9 04 94 e1 79 86 dd 60 2a 4=C...y...*
0010 0c 51 01 dc 06 40 24 09 00 10 a1 e0 09 00 e1 2c Q...$...
0020 a4 29 25 30 b8 bd 24 03 3a 00 02 02 12 03 02 19 )%...$...
0030 00 94 02 55 02 03 ea fb 00 50 a0 3d 21 ef 2a b7 ..U...P=!*
0040 ca 5a 80 18 08 04 45 bd 00 00 01 01 08 0a 1b 8f ..Z...E...
0050 9e d4 18 2b b8 9a 47 45 54 20 2f 20 48 54 50 ...GE T / HTTP
0060 2f 31 2e 31 0d 0a 48 6f 7f 31 2e 31 0d 0a 48 6f 7f
0070 6f 72 67 0d 0a 43 6f 6e 6f 72 67 0d 0a 43 6f 6e 6f
0080 20 6b 65 65 70 2d 61 6c 6e 20 6b 65 65 70 2d 61 6c 6e
0090 3a 20 31 0d 0a 55 70 67 7f 3a 20 31 0d 0a 55 70 67 7f

```

通信を記録してみる(2) TLS1.2

No.	Time	Source
1	0.000000	
2	0.004817	
3	0.004900	
4	0.005241	
5	0.010290	
6	0.011762	
7	0.013058	
8	0.013062	
9	0.013116	
10	0.013116	
11	0.066258	
12	0.066686	
13	0.072261	
14	0.072320	

- ▶ Frame 4: 583 bytes on wire (4664 bits), 58
- ▶ Ethernet II, Src: Apple_94:e1:79 (dc:a9:04
- ▶ Internet Protocol Version 4, Src: 192.168.
- ▶ Transmission Control Protocol, Src Port: 6
- ▼ Transport Layer Security

- ▼ TLSv1.2 Record Layer: Handshake Protocol

- Content Type: Handshake (22)

- Version: TLS 1.0 (0x0301)

- Length: 512

- ▼ Handshake Protocol: Client Hello

- Handshake Type: Client Hello (1)

- Length: 508

- Version: TLS 1.2 (0x0303)

- ▶ Random: 5606194140089d629ffdc4e29dcf8590a8dd5b634744394d...

- Session ID Length: 32

```

.....V..A@..b..... [cGD9M. [$..6.. ..`...0~c.....f..~.0.. [...W....".....+./.,.
0...../..5.
.....
.....
isog-j.org.....
..
**.....#.....h2.http/1.1.....
.....3.+.)**..... ;.....) -3.+a.....+.-.....$(-.....+..
**.....
.....
.....P..L..&...J.(.....Z.y...a.....vW... .x/./..$......#..... .http/1.1...
(..
$.
!...0...0..i..... L...M...^...-..0
.
*.H..
.....0J1.0..U...US1.0...U.
.
Let's Encrypt1#0!..U...Let's Encrypt Authority X30..
101120525207
.....1.....{v.N...
.....
V>~..0...U.#..
+.....0...#http://
isog-j.org

```


通信を記録してみる(3) TLS1.3

No.	Time	Source
4	11.837086	
5	11.862514	
6	11.862578	
7	11.866418	
8	11.891436	
9	11.892753	
10	11.892757	
11	11.892812	
12	11.893002	
13	11.893026	
14	11.894746	
15	11.898191	
16	11.899645	
17	11.923148	

- ▶ Frame 7: 583 bytes on wire (4664 bits)
- ▶ Ethernet II, Src: Apple_94:e1:79 (dc)
- ▶ Internet Protocol Version 4, Src: 192
- ▶ Transmission Control Protocol, Src Po
- ▼ Transport Layer Security
 - ▼ TLSv1.3 Record Layer: Handshake Pr
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 512
 - ▼ Handshake Protocol: Client Hello
 - Handshake Type: Client Hello
 - Length: 508
 - Version: TLS 1.2 (0x0303)

Wireshark - Follow TCP Stream (tcp.stream eq 1) - Wi-Fi: en0 (host tls2.isog-j.org)

.....A.^w.{"1...t}.4\GF0.....l. =.....Ar:....'...M...BS.zJ..D..\$......+./.....,0.

.....3.0/5

.....1.1.....3.k.i... 0!...Vc;E=n..0.D.-4..A..b.u..1..A....=R~.....

.....m.S[.....}..B.9..C[.%.+.....

.....@.....

.....+..Y...r..K.4?...

6M2.....*vb... =.....Ar:....'...M...BS.zJ..D.....0+.....3.E...A..?..M.K...K.S.h.{ Y|

[.*...).k..f.y.B...5.[wE...9.TO.F...H.....&0a`..&.k.(...;;.6,\$.V.g.;...\$6h.....*.....3.....)

T..Z..A..u.9.h.8.Rj.

Xb&.Q"C.&.p).T.L].E..(....N..8..W..V6.....EC...m.BHS.....4J..R%.)

.....b2...^..a...".J...!.L.2;.%.....-{HNw.#D+.-. {. =2.....AQ ..D...../..#.6..?.....W'W

9I.&...g...9.6....._.....u...T.....{...o.a...'.Es.u;a..}.L.l.]..d..._,!

1.....;oG.....]a.j...{.....\9...4V.R..U/.{.

v03.Nw.l.>P{..

.....;<.&8...6v6...0.0...Gf.a.ON...P.....d.w.Vf.....N^7b..1E.V..Z8LP.eS/.S...

7#"..c..h.Q.o.....".....v.....n CeS.....J.\$..H\$.<....._.....aEE...m.&.o.:+j.i5.x55W,..^o .Y7...

...:DC..D.LS

%..vn...@.{Wv.vT..[.k.../;.1.a.(.)6c.?~Bg.....D.<v...tp.p...7/nl.g.f.rph).-...|...>.. .d....5....\N<.

|Km.+1.|I.3Jb.....d...a.`.B.g.:.....6...M*..._i...q...M.>P.....z.v.i.....X.Q.....

.v.F...w^E

)....."U...V...f..Y.p...3..w..'T..

...#/.@.....{.w%.xe.....X.|l.,'.E..0..

0..a.....\..C/+..BQt\t..?.....e..dti...{%.T.xf...[u..

;d5.v.....&...#^[(.K.=. eRo..0..s...~j@q..U.+...~FE.....<...N,,,2.M.nh...i.{.dTR,...*%.vD.VB%.....

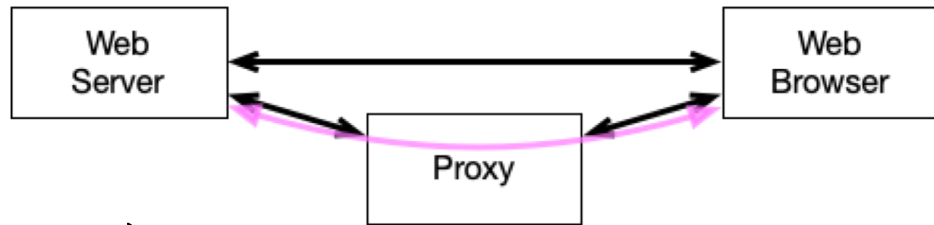
L..bn..G\$.oqv.<l.T0.\!T..".3:3.....fJ.g...w.....'t.5.....2..M.E.k)u..*i..0+e...4.....i.

{e.fQ...r).....f.5:P..k..u.....

...2.....yV:.....Y...\$h..D...t<Zw).J....?..*%...1.<.f..5hb.....!w..zjM...].0.ep2.S.v.t..Q|.

プロキシログをしてみる

- 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_DIRECT/[redacted].94 -
x.x.x.x TCP_TUNNEL/200 692 CONNECT [redacted]org:443 - HIER_DIRECT/[redacted].94 -
x.x.x.x TCP_TUNNEL/200 39 CONNECT [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)

たにいさん、ももい

- ・本資料の著作権は日本セキュリティオペレーション事業者協議会(以下、ISOG-J)に帰属します。
- ・引用については、著作権法で引用の目的上正当な範囲内で行われることを認めます。引用部分を明確にし、出典が明記されるなどです。
- ・なお、引用の範囲を超えられる場合もISOG-Jへご相談ください(info (at) isog-j.org まで)。
- ・本文書に登場する会社名、製品、サービス名は、一般に各社の登録商標または商標です。®やTM、©マークは明記しておりません。
- ・ISOG-Jならびに執筆関係者は、このガイド文書にいかなる責任を負うものではありません。全ては自己責任にてご活用ください。