ネットワークセキュリティ標準化動向

門林雄基
奈良先端科学技術大学院大学 情報科学研究科

平成 28 年 11 月 4 日

1　はじめに

ネットワーク上に存在するさまざまな脅威に対して効率的に対処するために、数多くのセキュリティ標準が策定されている。これらのセキュリティ標準の多くは、正しく適用すれば、さまざまな脅威に対して効果を発揮する。しかし良質な標準は、モジュール性や汎用性、他の標準との役割分担を明確に意識してして作られているため、その活用方法や脅威との対応関係が明確でないことも多い。ここでは特定の標準化団体や標準ファミリにとらわれずに、セキュリティ向上に資する代表的な標準を紹介し、近年の脅威との関係にも触れることでセキュア調達[1][1] や研究開発の一助となることを目指す。

2　インフラ層のセキュリティ標準

本節ではインフラストラクチャ層におけるセキュリティ標準、具体的には経路制御、ドメイン名、電子メールおよびウェブのセキュリティ標準化動向について述べる。インフラ層では IP アドレス、ドメイン名、電子メールアドレスやユーザ ID など、サービスや端末、個人を識別する情報を取り扱っており、これらの真正性を損なう攻撃が今日大きな問題となっている。インフラ層におけるセキュリティ標準化ではこれらの脅威を予見し、積極的な研究開発と標準化が進められてきた。以下ではそれぞれについて述べる。

2.1　経路制御のセキュリティ

近年、インターネットにおいて経路ハイジャックが現実的な脅威となり、大きな問題となっている。これは経路制御プロトコル BGP[2] における、経路の公告情報をそのまま信用する、という性善説にもとづく仕様がもはや時代にそぐわなくなったことを示している。この問題に対処するため、RPKI (Resource Public Key Infrastructure, RFC[3] 6480) が標準化された。RPKI を用いると、ネットワークサービス事業者に付与された AS 番号と、AS に割り当てられた IP アドレスブロックを電子証明書によって認証することができる。これは IP アドレスと AS 番号の管理主体が認証局となって運用する公開鍵認証基盤を標準化し実現したものである。IP アドレスと AS 番号の割り当てに際し管理主体が電子証明書を発行し、それを用いて経路の公告情報が正当であることを証明する ROA (Route Origin Authorization) に署名を行う。これにより経路ハイジャックをある程度、防ぐことができる。

経路ハイジャックへの抜本的な解決策として、現在 BGPsec の標準化が IETF[4] SIDR 作業部会で進められている。これは BGP プロトコルへの拡張であり、ルータのソフトウェア改修が必要となる。

このほか、送信元 IP アドレスの詐称も、他のプロトコル脆弱性との組み合わせによっては大きな問題となる。このため IETF において送信元 IP アドレスを他組織や他国になりすますことを抑止する標準 BCP[5] 38, BCP 84 が策定され、米国のインターネット観測組織 CAIDA において Spoofer Project として、インターネット全体にわたる対策進捗の継続的測定が行われている [2]。

[1] セキュリティを考慮した調達

[2] Border Gateway Protocol
[3] Request for Comments
[4] Internet Engineering Task Force
[5] Best Current Practice

2.2 ドメイン名のセキュリティ

ドメイン名システムで用いられる DNS[6]も性善説に基づくプロトコルであり、個々の問い合わせに付与される問い合わせ番号が推測可能であるため、特定のドメインの問い合わせに対して応答を偽造することで不正な IP アドレスに誘導するといった攻撃が問題となっている。このような DNS 応答の信頼性に関する問題を解決するため、DNSSEC (DNS Security Extensions, RFC 4033) が標準として策定されている。DNSSEC は名前と IP アドレスの対応関係などを記したレコードに対し秘密鍵を用いて署名を行うもので、公開鍵を用いて誰もがその正当性を検証することができる。秘密鍵は当該ドメインの管理者しか知り得ないため、従来の DNS において問題となっていた応答偽造を抑止することができる。

DNSSEC 標準は各国のトップレベルドメイン (.jp など) での採用が数年前から進んでおり、ドメイン名登録を取り扱う事業者や、ドメイン名を有する各組織での対応が待たれる状況である。

また電子証明書を発行する認証局への不正アクセスなどを背景として、不正な認証局が任意のドメイン名に対して虚偽の証明書を発行できる点が問題視されており、当該ドメインの管理組織が正当な電子証明書に裏書きする目的で DNSSEC を活用することが積極的に検討されている。DANE (DNS-Based Authentication of Named Entities, RFC 6698) はこのための標準で、TLSA レコードに当該ドメインが用いる電子証明書の情報を記載することができる。

2.3 電子メールのセキュリティ

電子メールによるなりすまし攻撃が今日も大きな問題となっている。これは幾つかの問題に分解して考えることができる。まずは、他の組織が送信ドメインを詐称してメールを送れてしまう、という問題である。この問題に対しては SPF (Sender Policy Framework, RFC 7208) 標準が策定されている。電子商取引サイトや政府機関などで SPF を採用することにより、攻撃者による送信ドメインのなりすましを抑止することができる。

[6]Domain Name System

なお SPF を採用していても、ネットワーク構成次第ではあるが、メールサーバを迂回してメールを送れてしまう、という問題がある。この場合、内部犯が他の利用者になりすまして任意のアドレスを騙る可能性もある。この問題に対し、DKIM (DomainKeys Identified Mail, RFC 6376) 標準が策定されている。メールサーバにおいて秘密鍵を用いて送信メールに署名を付加することで、メールの受信者側で、そのメールが確かに送信者から、そして送信ドメインから送られたことを検証することができる。

DMARC (Domain-based Message Authentication, Reporting, and Conformance, RFC 7489) は電子メールによるなりすまし攻撃に悩まされる大手事業者によって策定された標準で、DKIM, SPF を前提とし、これらの送信ドメイン認証標準において認証エラーとなった場合のレポーティングなどについて定めている。

世界的には、大手メール事業者を中心として DKIM, SPF, DMARC の採用が急激に進展しており、これらの設定を怠ったり誤った場合、メールが届かなくなるのが一般的である。迷惑メール対策、なりすましメール対策の一環として、メールサーバを有する各組織での対応が待たれる状況である [3]。

なお DKIM, SPF ともに DNS をメール送受信者間の情報交換に用いているため、これらの標準の活用にあたっては DNS におけるセキュリティ対策が前提となる。

2.4 ウェブ・セキュリティ

ウェブサイトにおける情報漏洩は継続的な脅威である。これには様々な原因があるが、サーバ側で最新の標準を活用して対策を施すことにより、ある種の脅威を抑止することができる。ここではスクリプト提供元の抑制、暗号通信の強制、クッキーの保護に役立つ標準を紹介する。

Web ブラウザは Web ページの表示と並行して、様々なサイトから提供されたスクリプトを実行することが出来るが、悪意あるサイトからスクリプトを読み込んでしまった場合、情報漏洩につながる可能性がある。このようなリスクを減らすため、CSP (Content Security Policy, W3C CSP 1.0) が標準化された。CSP ヘッダをサーバ側で設定することで、利用者のブラウザが読み込むスクリプト等の提供元を制限することができる。

このほか、HSTS ヘッダ (HTP Strict Transport Security, RFC 6797) を指定することで、サーバ側で HTTPS 通信が必須であることをクライアントに対して明示することができる。また HttpOnly ヘッダ (RFC 6265) を指定することで、スクリプトからクッキーを読み取ることを禁止することができる。

このほか、マッシュアップに用いられるサイト埋め込みの技術を濫用したセキュリティ問題を解決するため、X-Frame-Options ヘッダ (RFC 7034) が標準化されている。これらの標準をうまく活用することで、今やチューリング完全となった Web ブラウザにおいて、電子商取引サイトとユーザ生成型コンテンツサイトなど、信頼性の異なるサイト間の望まない相互作用を排除していくことが重要である。

なお、これら成立した標準に加えて現在、IETF httpbis ワーキンググループと W3C において注目すべき標準化が推し進められている。

2.5 インフラ層の課題

インフラ層では以上で述べてきたように、近年、事業者および利用者のセキュリティ向上に資する重要な標準が数多く策定されているが、大きな問題がある。それは各事業者における標準の採用が遅れていることである。Lars Eggert 氏が各国における普及率を測定し公開しているが[7]、それによれば本稿執筆時点における DKIM の普及率は日本で 24%（米国では 50%）、DNSSEC は日本で 1.4%（米国では 2.6%）という状況である。DKIM の標準策定は 2007 年、DNSSEC の標準策定は 2008 年にほぼ終わっており、そろそろ 10 年が経とうとしているにもかかわらず、普及しているとは言い難い状況である。送信元 IP アドレスの詐称対策は最も進んでおり、インターネットに公告されている IP アドレスの 8 割が対策済みであるが、15% は依然として詐称可能である。

このような普及の遅れには様々な要因があろうが、インターネット技術がある時点でイントラネットとして企業ネットワークに転用され、企業ネットワーク関係者がインターネット運用技術への関心を失った結果、一部のネットワーク運用者を除いて、これらの技術革新への興味が薄れているのではないか。あるいは、ネットワーク技術を教える教育関係者が日本語の書籍のみに頼り、最新の技術動向を追いかけることをやめてしまっているのではないか。

普段、我々は目の前にあるパソコンやスマートフォンの安全性や、企業秘密や顧客情報の安全性には気を使うが、インターネットを用いて頻繁に情報をやりとりしている以上、エンドポイントだけを安全にすることは偽りのセキュリティを求めるようなものである。エンドポイントはインフラの安全性に大きく依存しており、経路ハイジャックや送信アドレスのなりすまし等がエンドポイントの安全性を根底から揺るがしていることを強く意識する必要がある。

エンドポイントとの対比で言えば、インフラ層におけるセキュリティ対策は分かりにくいためか、バグ報奨金プログラム (Bug bounty program) の対象となることも少ないように思われる。スマートフォンやパソコンのセキュリティは若者にとっても分かりやすいが、今後、目に見えない経路制御プロトコルや電子メールシステムのセキュリティへの興味を喚起するためにも、バグ報奨金プログラムあるいはそれに類する制度設計を工夫していく必要があろう。

3 エンドポイントのセキュリティ標準

本節ではエンドポイントにおけるセキュリティ標準について述べる。エンドポイントは利用されるソフトウェアも多様であり、利用者数や端末台数も多いため、効率的な管理が継続的な課題となっている。以下では、ネットワーク化された端末におけるソフトウェアのセキュリティ、利用者のセキュリティ、ハードウェアのセキュリティ向上に資する標準を紹介する。

3.1 脆弱性管理

エンドポイントではアクセス制御によって通信相手を限定することと並んで、脆弱性管理が重要となる。脆弱性は必ずしもネットワークと直接の関係のないものもあるが、ネットワーク経由で管理者権限を奪取されるものもある。これらの脆弱性に関する情報は様々なソフトウェアベンダから提供されるが、ソフトウェアベンダがつけた番号や脆弱性の発見者がつけた名前だけだと混乱をきたすため、共通脆弱性番号 CVE (Common

[7] https://eggert.org/meter/dkim

Vulnerability Enumeration, ITU-T[8] X.1520) が標準化された。

脆弱性データベースを CVE 番号やソフトウェア名で検索することで、市販または公開されているソフトウェアの既知の脆弱性を調べることができる。エンドポイントのセキュリティ管理にあたっては、利用するソフトウェアを網羅的に調べ、かつその脆弱性を網羅的にリストアップすることで脆弱性の検討に着手することができる。なお脆弱性対策の優先順位をつけるために CVSS (Common Vulnerability Scoring System, ITU-T X.1521) 標準を活用することで、ネットワーク経由で管理者権限を奪取されるような、深刻度の高い脆弱性から対策に着手することができる。

3.2 アイデンティティ管理

利用者へのなりすましを防ぐための古典的な手段といえばパスワードであったが、相次ぐパスワード漏洩やパスワードへの攻撃手法の進展に伴い、近年さまざまな認証技術が普及しつつあり、それらを組み合わせて認証の強度を上げることが求められている。言い換えれば、パスワード認証だけでは本人であると確信することは難しく、多要素認証によってはじめて高い確率で本人であると言える。このような本人確認レベル (Level of Assurance) を表 1 のように 4 段階に分類し、標準化がすでに行われている (Entity Authentication Assurance Framework, ITU-T X.1254)。これにより、利用者と相対する事業者がリスクの高い取引等にあたって高い本人確認レベルを求めることができる。

またパスワード以外の認証技術は従来メーカー独自であり、互換性のないものが多かったが、FIDO[9] UAF (Universal Authentication Framework) 標準により、各端末で利用可能な指紋、顔画像、音声など様々な認証技術をウェブサイトやクラウドの認証において活用することができる。これらの標準は大手ウェブサイトや主要なオペレーティングシステムにおいて採用が進んでいる。

3.3 接続端末の管理

ネットワーク接続端末の改ざんや、不正端末の正規端末へのなりすましは企業ネットワークにおいて大きな脅威である。この問題に対処するために TPM (Trusted Platform Module) 標準が用意されている。各端末に搭載された TPM チップには、端末の起動時に BIOS やオペレーティングシステムが改ざんされていないことを確認するためのレジスタがあり、これをネットワーク経由で確認することで改ざんやなりすましを検知することができる。TPM チップには電子証明書や秘密鍵を格納することもでき、ディスク暗号化などにも用いられている。TPM は米連邦政府が調達要件に挙げていることもあり、企業向け PC の 8 割以上に搭載されているが、端末数の大きな企業を除いては活用が進んでいないのが現状である。

3.4 エンドポイントの課題

ここまでの説明から、エンドポイントのセキュリティ向上のための標準化は相当程度進んでいると思われたかもしれない。しかしながらエンドポイントでは実のところ、最も基本的なところでネットワークセキュリティを確保できていない。

代表的な問題として ARP (Address Resolution Protocol) による中間者攻撃がある。ARP は IP アドレスと MAC アドレスの対応付けをおこなう、最も基本的なプロトコルであるが、性善説に基づいて設計されており、中間者攻撃により不正端末が正規端末になりすますことができてしまう。この問題に対し、IPv6 では SEND (Secure Neighbor Discovery, RFC 3971) が標準化されたが、セキュリティ機能のない NDP (Neighbor Discovery Protocol) の標準化が先行したため、普及していない。

この他にも、中間者攻撃、リプレイ攻撃、盗聴、セッション乗っ取り、サービス妨害攻撃の容易なプロトコルが数多く存在する。プロトコル脆弱性はソフトウェア脆弱性と異なり、脆弱性管理の対象となることは少ないが、制御システムなどのミッションクリティカル環境ではプロトコル脆弱性にも十分留意すべきである。

[8]International Telecommunication Union Telecommunication Standardization Sector
[9]Fast IDentity Online

表 1: ITU-T X.1254 における本人確認レベル

レベル	概要	例
LoA1 (Low)	本人であるという確証なし	使い捨てアカウント
LoA2 (Medium)	本人であるというある程度の確証あり	暗号通信による本人確認
LoA3 (High)	本人であるという確証あり	多要素認証と暗号通信による本人確認
LoA4 (Very high)	本人であるという確信あり	LoA3 に加え、対面での本人確認と TPM を利用

4 インシデント対応組織のためのセキュリティ標準

インシデント対応組織では早期警戒情報や脅威情報を効率的に交換することが重要である。これらの情報は受け手に関係があり、時宜を得たものであり、誤検知を含まず、自己完結しており、機械処理できることが望まれる [4]。

フィッシング対策やボット対策、迷惑メール対策では、それぞれに特化したブラックリスト等が維持管理されており、さまざまなツールからウェブや API, DNS 等を通じてアクセス可能である。ここでは特に、情報の構造が単純でないため標準化が進められているインディケータ情報とマルウェア情報について紹介する。

4.1 インディケータ情報

近年、アンチウイルスや侵入検知システム等による検知が困難な標的型攻撃が問題となっており、侵入の兆候 (IOC: Indicator of Compromise) をインディケータ情報として専門機関などから入手し、対策に役立てる動きが活発化している [5, 6]。ここで用いられる標準が STIX (Structured Threat Information eXpression) である。OASIS[10] CTI TC では STIX に加えて、STIX で記述したインディケータ情報を配送するプロトコル TAXII (Trusted Automated eXchange of Indicator Information), および STIX において用いるデータ型を定義する CybOX (Cyber Observable eXpression) の標準化を進めている。なおインディケータ情報としては、標準で定められた STIX 形式のほかに、オープンソース・コミュニティが活用する YARA などがある。

[10]Organization for the Advancement of Structured Information Standards

4.2 マルウェア情報

MAEC (Malware Attribute Enumeration and Characterization, ITU-T X.1546) はマルウェア解析結果を構造化し記述するための標準である。従来、マルウェアはアンチウイルス各社が付与した名称（検知名）により分類されてきたが、マルウェアの自動生成や多機能型マルウェアの登場などにより、名前での分類と特徴把握が難しくなっている。MAEC により、マルウェアのメカニズム、ふるまい、および個々の動作を構造化して記述することができるため、インディケータ情報として活用することや、トリアージや専門家によるマルウェア解析の結果を統合することが容易となる。

現在、複数の自動マルウェア解析システムにおいて MAEC 形式で解析結果を出力できるようになっており、今後インシデント対応組織において活用が期待される。

5 セキュリティ標準の方向性

ここまで、既存のセキュリティ標準を駆け足で紹介してきたが、今後セキュリティ標準への提案を検討される方のために、標準化の方向性について手短に述べておきたい。

特定の脅威に対応した標準を策定することは非効率的であり、２年から４年かけて標準を策定している間に脅威が変容してしまい役に立たなくなる場合もある。このため、そのような特定脅威にあわせた標準プロトコルを作るのではなく、できるだけ汎用プロトコ

ルと API, ツール等を用いて対策に役立てることが望ましい。

近年、北東アジアを中心として、標準化提案の件数が研究開発の達成度評価のものさしとして濫用されており、このため標準化団体においても重箱の隅をつつくような提案のダメージコントロールに追われている。標準化提案にあたっては、できれば本稿で言及した標準すべてを読破し、標準の相互依存関係や機能分担、モジュール性や汎用性、各標準化団体の役割分担などを考慮したうえで腰を据えて関わっていただければと思う。

6 その他のセキュリティ標準

最後に、本稿では取り扱わなかったその他のセキュリティ標準を挙げておく。TLS, IPsec のような暗号プロトコルや、そこで用いられるハッシュ関数や暗号アルゴリズムについても標準化が進展している [7]。また Kerberos, OAuth などのネットワーク型認証プロトコルについても対応する IETF の作業部会が存在する。

またセキュアコーディングはネットワーク上で協調動作するソフトウェアの安全性を高めるうえで重要である。CWE (Common Weakness Enumeration, ITU-T X.1524), CAPEC (Common Attack Pattern Enumeration and Classification, ITU-T X.1544) はセキュアコーディングのための脆弱性と脅威をそれぞれ分類し、共通番号と知識ベースを整備した標準である。

7 おわりに

今日、各種メディア報道やセキュリティ事業者のレポートなどにおいて高度なサイバー攻撃が注目を集めることが多いが、実際には多くの攻撃がインフラやエンドポイントにおける管理の不備や設備老朽化を何らかの形で活用しており、本稿で挙げた主要なセキュリティ標準を使っていれば防げたと思われるケースは多い。

ネットワークセキュリティ標準の多くはオプトインであり、採用しなくても通信できなくなるケースは稀であるため、認知度が低いものも多いが、意識して調べれば、インターネットビジネスを大規模に展開する大企業は積極的にこれらを活用していることがお分かりいただけるだろう。

公共空間であるインターネットの安全性を向上させ、その上で安心してビジネスや研究開発を行うためには、ネットに繋がる全てのステークホルダーが各自の役割を果たさねばならない。本稿で示したように、今日、先進的企業による主要なネットワークセキュリティ標準の導入が進んでおり、その他大勢の参加組織によるキャッチアップを待っている段階である。

本稿がネットワークセキュリティ標準の普及・浸透と、それによるセキュリティ向上の一助となれば幸いである。

参考文献

[1] ENISA: “Secure ICT Procurement in Electronic Communications”, Technical report, ENISA (2014).

[2] R. Beverly, R. Koga and kc claffy: “Initial Longitudinal Analysis of IP Source Spoofing Capability on the Internet”, ISOC Briefing Papers (2013).

[3] Z. Durumeric, D. Adrian, A. Mirian, J. Kasten, E. Bursztein, N. Lidzborski, K. Thomas, V. Eranti, M. Bailey and J. A. Halderman: “Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Email Delivery Security”, Proceedings of IMC (2015).

[4] CERT Polska: “Actionable Information for Security Incident Response”, Technical report, ENISA (2014).

[5] ENISA: “Detect, SHARE, Protect - Solutions for Improving Threat Data Exchange among CERTs”, Technical report, ENISA (2013).

[6] C. Johnson, L. Badger, D. Waltermire, J. Snyder and C. Skorupka: “Guide to Cyber Threat Information Sharing” (2016). NIST SP800-150 Second draft.

[7] ENISA: “Study on cryptographic protocols”, Technical report, ENISA (2014).