情報系におけるサイバーセキュリティ

要　旨

インターネットの普及やネットワークの高度化に伴う情報システムの機能の増加・高度化に伴い、それらに対するセキュリティリスクが顕在化し、対策が進められている。また、スマートフォン、クラウド等の新しい情報通信技術の普及においても、それらに対するセキュリティリスクが存在し、対策の検討や普及啓発が進められている。

I　情報通信技術の発展とセキュリティ課題の顕在化

情報通信技術やその関連技術、関連する製品・サービスは、情報系と制御系に大きく分類することができる。ここでは、情報システムやネットワーク、クラウドといった技術及び製品・サービスを情報系と定義し、制御システムや組込みシステムといった技術及び製品・サービスを制御系と定義する。本論ではこのうち情報系における技術の発展とセキュリティ課題について論じる。制御系については次の概論「制御系におけるサイバーセキュリティ」で述べる。

1　情報通信技術の発展

情報システムやネットワークを始めとする情報通信技術は、1990年代からのおよそ20年間で格段に発展し、利便性が向上するとともに様々なサービスが登場してきた。しかしながら、利用者層の拡大や利用シーンの多様化に伴い、セキュリティ課題も顕在化し、それらに関連した多くのセキュリティインシデントが発生し、多くの対策が行われてきた。

近年では、スマートフォンの普及、クラウドの利用拡大、ビッグデータ分析の登場、モノがネットワークにつながりクラウド上でデータが処理されるIoT/M2M関連サービスの拡大など、新たな情報通信技術を活用した製品・サービスが普及し、それらに対しても特有のセキュリティ課題が顕在化しつつある。表1に主な情報通信分野の製品・サービスと関連する情報通信技術の発展を示す。以下では、情報システムやスマートフォンなど、主な情報通信分野の製品・サービスのセキュリティ課題について国内の状況を中心に取り上げる。

＊本稿におけるインターネット情報の最終アクセス日は、原則として、2015年1月13日である。

表1　主な製品・サービスと関連する情報通信技術

主な情報通信分野の製品・サービス	関連する情報通信技術の発展
情報システム	計算処理の高速化・リアルタイム化 情報システムの大規模化・複雑化 情報システムのネットワーク化 企業情報システムへの社内ネットワーク（LAN）、無線LAN、リモートアクセス等の整備
通信インフラ・ネットワーク（有線）	ネットワークのデジタル化 光ファイバー、ADSL等による高速化
通信インフラ・ネットワーク（無線）	無線LANの普及 高速な無線LAN規格の登場・普及
Web・インターネット	インターネットの普及 電子商取引の普及 ソーシャルメディアの拡大
携帯電話・スマートフォン	携帯通信の高速化 携帯端末の高機能化（処理の高速化、GPS、ICカードチップ搭載等）
クラウド	ネットワークの高速化や新たな仮想化技術の登場に伴うクラウドコンピューティングの普及拡大
IoT/M2M	センサの小型化・低消費電力化等に伴うIoT/M2Mの普及

（出典）各種資料を基に三菱総合研究所作成。

2　情報システム・ネットワークの発展とセキュリティ課題の顕在化

(1)　情報システム・ネットワークの発展

情報システムは、利用者の観点から、社会情報システムと企業情報システムに分類することができる。社会情報システムは社会の利用に供されている情報システムであり、企業情報システムは企業の内部で利用される情報システムである。(1)

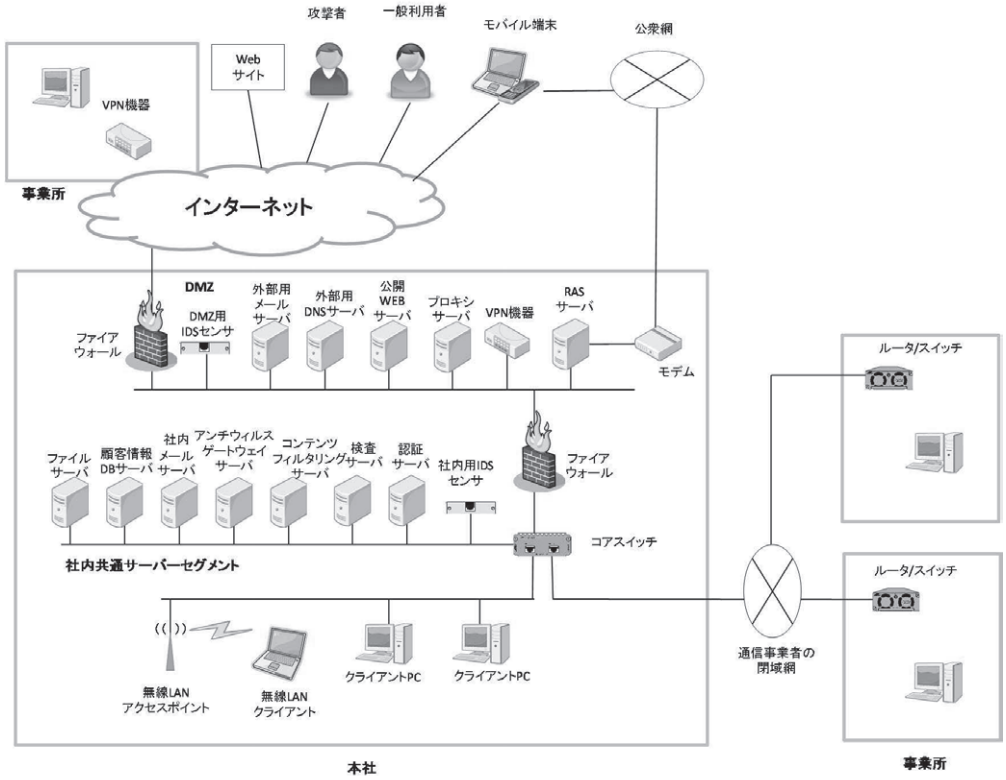
社会情報システムは、情報通信、金融、航空、鉄道等、多くの重要インフラで社会を支える基盤となっている。これらの情報システムは、技術の進歩に伴い、高速な処理が可能になるとともに、大規模化・複雑化しており、現在は多くのシステムがインターネットなどの外部ネットワークに接続している。

また、現在ではほとんどの企業が情報システムの構築を実施しており、企業情報システムは企業活動の要となっている。企業情報システムについても、社内ネットワーク（LAN）の整備、無線LANやリモートアクセスの採用、ネットワークの高速化などにより、ここ20年間で利便性が格段に向上してきた。

ここでは情報システムの例として、企業で構築される一般的な企業情報システムの構成例を図1に示す。情報システムは本社や事業所間を結ぶ企業内通信網やインターネットなどのネットワークと、本社・事業所等に設置されるファイアウォール、各種サーバ及びクライアントPC等から構成される。

(1)　佐藤敬「情報システムの分類」情報システム学会ウェブサイト <http://www.issj.net/is/02/index6.html>

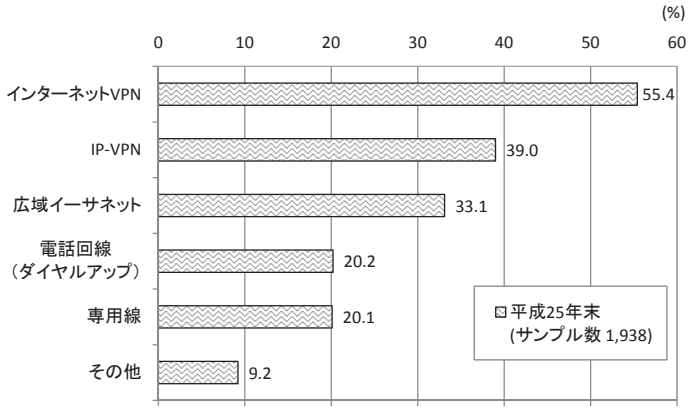
図1　一般的な企業情報システムの構成



（出典）情報処理推進機構「大企業・中堅企業の情報システムのセキュリティ対策―脅威と対策―」2007.4, p.5. <https://www.ipa.go.jp/security/fy18/reports/contents/enterprise/0.pdf>を基に三菱総合研究所作成。

我が国においては、企業内通信網とも呼ばれる社内ネットワーク（LAN）は2013年末時点では88.6%の企業が構築しており、多くの企業が社内業務の利便性と効率を高めるためにLAN上に構築したイントラネットを活用している。企業内通信網に企業間通信網も加えた企業通信網としては90.6%の企業が構築しており、図2に示すとおり、インターネットや通信事業者の保有する広域IP通信網が現在では主に使われている。(2)

図2　企業通信網で主に使われている通信サービス（複数回答）



（出典）総務省「平成25年通信利用動向調査の結果（概要）」2014.6.27, p.15. <http://www.soumu.go.jp/johotsusintokei/statistics/data/140627_1.pdf>を基に三菱総合研究所作成。

(2)　総務省「平成25年通信利用動向調査の結果（概要）」2014.6.27, p.15. <http://www.soumu.go.jp/johotsusintokei/statistics/data/140627_1.pdf>

遠隔地から公衆網を利用して社内ネットワークに接続するリモートアクセスについても過半数（2012年末で54.8%）の企業が構築しており、パソコンや電話・スマートフォン・携帯情報端末から社内システムにアクセスが可能となっている(3)。

ネットワークの面でも、有線、無線ともに高速化が進み、利用用途が拡大し、利便性も大きく向上してきた。有線は光ファイバー、ADSL（Asymmetric Digital Subscriber Line）等による高速化が進み、2002年時点では、自宅のパソコンからインターネットにアクセスする方法として71.8%が電話回線やISDN（Integrated Services Digital Network）回線などの低速なナローバンド（狭帯域）回線(4)を利用していたものの(5)、DSL（Digital Subscriber Line）、光ファイバーやケーブルインターネットなどのブロードバンド（広帯域）回線の利用は2003年末に47.8%、2004年末には62.0%と急増し(6)、現在では全体の97.4%を占める(7)。インターネット利用者数も2001年末の5593万人から2013年末には初めて利用者数が1億人を超えている(8)。無線に関しても、高速無線LAN規格や携帯電話の通信規格LTE（Long Term Evolution）等の登場により高速化・大容量化が進んでいる。

（2）　情報システム・ネットワークのセキュリティ課題及びその対策

前述した情報システム・ネットワークの発展に対して、高度化・巧妙化するサイバー攻撃による事故や人為的なミス等の非意図的要因によるIT障害、災害によるIT障害など、多くのセキュリティインシデントが発生してきた。特に近年顕在化している脅威としては、AnonymousやLulzSec等の国際的ハッカー集団によるサイバー攻撃や、2011年の衆議院・参議院のコンピュータへのマルウェア感染・情報漏えい等に代表される標的型攻撃などが挙げられる。

これらの状況に対し、それぞれの課題に対する多様なセキュリティ対策が推進されてきた。情報システムのセキュリティ対策として、古くは1995年の通商産業省（現：経済産業省）が情報システムの設置基準、技術基準及び運用基準を示した「情報システム安全対策基準」（平成7年通商産業省告示第518号）や、1996年の「コンピュータ不正アクセス対策基準」（平成8年通商産業省告示第362号）の策定から取組が進められてきている(9)。政府機関を対象とした「情報セキュリティポリシーに関するガイドライン」や「政府機関の情報セキュリティ対策のための統一基準（2005年12月版［全体版初版］）」の策定なども行われている(10)。また、標的型攻撃の増加に伴い、情報処理推進機構（IPA）による標的型攻撃メールの届出受付が2008年9月から開始され、「標的型サイバー攻撃 特別相談窓口」の設置による標的型攻撃メールの相談対応も2011年10月

(3)　総務省「平成24年通信利用動向調査（企業編）の概要」2014.1.24, p.12. <http://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR201200_002.pdf>
(4)　電話回線やISDN回線などの通信速度が遅い回線をナローバンド回線、ADSL、光ファイバーなどの通信速度が速い回線をブロードバンド回線という。
(5)　総務省「平成14年通信利用動向調査報告書（世帯編）」2003.3, p.41. <http://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR200200_001.pdf>
(6)　総務省「平成16年通信利用動向調査の結果―主な調査結果―」2005.5.10, p.3. <http://www.soumu.go.jp/johotsusintokei/statistics/data/050510_1.pdf>
(7)　総務省　前掲注(2), p.5.
(8)　同上, p.1.
(9)　「法律、ガイドライン等」『情報セキュリティ対策ポータル』経済産業省ウェブサイト <http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm>
(10)「「政府機関の情報セキュリティ対策のための統一基準に」ついて」内閣サイバーセキュリティセンターウェブサイト <http://www.nisc.go.jp/active/general/kijun01.html>

から実施されている(11)。

重要インフラを支える情報システムに対しては、2005年に情報セキュリティ政策会議において「重要インフラの情報セキュリティ対策に係る行動計画」が策定され、各分野の情報セキュリティ確保に係る安全基準の策定や情報共有の枠組みが定められている(12)。それ以降、重要インフラ各分野における情報共有・分析を行うセプター（CEPTOAR）及び分野を超えた情報共有のためのセプターカウンシル（用語集参照）の設置、重要インフラにおける分野横断的演習（CIIREX）の実施や第2次、第3次の行動計画の策定など、多くの取組が継続的に実施されている(13)。

3　スマートフォンの普及とセキュリティ課題の顕在化

スマートフォンやタブレット端末などの携帯端末（スマートデバイス）の利用が広まっている中、スマートデバイス向けのアプリケーション（以下「アプリ」という。）の中には利用者が想定していない動作をするものがあり、架空の利用料金の請求画面を繰り返し表示させる不正なアプリによる架空料金請求や、便利な機能を持つアプリを偽った不正なアプリによる個人情報の不正収集などの事例が発生している(14)。こういった不正なアプリは急増しており、GoogleのAndroidをOS（基本ソフト）として搭載しているスマートデバイス向けの不正アプリは、2014年3月には全世界で累積200万種を突破し、うち65万種が2014年1月から3月までの増加分となっている(15)。

これらの問題に対し、総務省では2011年から「スマートフォン・クラウドセキュリティ研究会」を開催し、その成果を2012年6月に「スマートフォンを安心して利用するために実施されるべき方策」として公開している(16)。また、IPAでは、スマートフォンのセキュリティに関して、随時、事故事例や脆弱性情報を始めとする注意喚起を行っているほか、「スマートフォンのセキュリティ＜危険回避＞対策のしおり」や漫画などを利用した「I♥スマホ生活」と題した啓発コンテンツなどを公開し、普及啓発を推進している(17)。

---

(11) 情報処理推進機構「IPA Technical Watch　標的型攻撃メールの傾向と事例分析＜2013年＞を公開」2014.1.30, pp.1-2. <https://www.ipa.go.jp/files/000036583.pdf>

(12) 情報セキュリティ政策会議「重要インフラの情報セキュリティ対策に係る行動計画」2005.12.13. <http://www.nisc.go.jp/active/infra/pdf/infra_rt.pdf>

(13)「重要インフラ防護に関する内閣官房のこれまでの取組」内閣サイバーセキュリティセンターウェブサイト <http://www.nisc.go.jp/active/infra/torikumi_past.html>

(14)「特徴やリスクって？」国民を守る情報セキュリティサイト <http://www.nisc.go.jp/security-site/smartphone/risk.html>

(15) トレンドマイクロ「TrendLabs2014年第1四半期セキュリティラウンドアップ　新たな獲物を見つけたサイバー犯罪者―狙われたPOSシステムと仮想通貨―」2014.5.20, pp.31-32. <http://www.trendmicro.co.jp/cloud-content/jp/pdfs/security-intelligence/threat-report/pdf-2014q1-20140520.pdf?cm_sp=Corp-_-sr-_-2014Q1>

(16) スマートフォン・クラウドセキュリティ研究会「スマートフォン・クラウドセキュリティ研究会 最終報告―スマートフォンを安心して利用するために実施されるべき方策―」2012.6.29. <http://www.soumu.go.jp/main_content/000166095.pdf>

(17) 情報処理推進機構「スマートフォンのセキュリティ＜危険回避＞対策のしおり―便利な道具 スマートフォン 安全・安心利用のためのセキュリティ対策で危険回避!! ―」2012.6.8. <http://www.ipa.go.jp/files/000011456.pdf>;「I♥スマホ生活」情報処理推進機構ウェブサイト <http://www.ipa.go.jp/security/keihatsu/love_smartphone_life/>

4　クラウドの普及とセキュリティ課題の顕在化

クラウドサービスの利用が大きく進展している。2013年末の我が国企業のクラウドサービスの利用率は33.1%と約3分の1の企業が利用しており、今後のさらなる普及も見込まれている(18)。そのような中で、クラウド特有のセキュリティ対策が求められている。クラウドは情報を外部に預ける形のビジネスモデルであるため、情報漏えいや情報消失などのリスクについて検討する必要があるとされている。ファーストサーバ株式会社が提供するクラウドサービスでは顧客の大量のデータ消失及び一部のデータの情報漏えいが発生するなど(19)、実際にクラウドサービスが関連する大きな事故も起きた。

この状況を踏まえ、経済産業省は「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」を、また総務省は「クラウドサービス提供における情報セキュリティ対策ガイドライン」を公表するなどの取組を行っている(20)。また、「JASA－クラウドセキュリティ推進協議会」（JCISPA）では、クラウド情報セキュリティ管理基準、クラウド情報セキュリティ監査技術ガイド等の策定を行っており、クラウド事業者向けの「クラウド情報セキュリティ監査制度」を2014年から開始している(21)。

クラウドに関しては、サーバ所在国のカントリーリスクも指摘されている。クラウドのサーバが海外に位置する場合、その国の法令によっては、当該国の政府に対して通信のデータ内容等の開示義務が課されることもある。そのため、データの機密性が保たれない場合が想定される。実際に、米国では愛国者法（USA PATRIOT ACT）(22)に基づき米国内に存在するデータに対して連邦捜査局（FBI）及び司法当局は調査権限を有しており、差押え・閲覧の対象となる可能性がある。

Ⅱ　情報セキュリティに関する国際標準・認証

情報セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計・実装されているかを第三者が標準に基づいて評価及び認証する仕組みが整備されている。これらの仕組みは、政府機関を含め調達者が適切な情報セキュリティ対策を確保することや、利用者自身のセキュリティ能力を高めることを目的としており、多くの枠組みが活用されてきた。

製品に関するものでは、セキュリティ評価基準の国際標準であるISO/IEC 15408に基づいて第三者が評価・認証する「ITセキュリティ評価及び認証制度（JISEC）」(23)や、暗号モジュー

(18)　総務省　前掲注(2), p.20.
(19)　ファーストサーバ株式会社第三者調査委員会「調査報告書（最終報告書）＜要約版＞」2012.7.31, p.3. <http://support.fsv.jp/urgent/pdf/fs-report.pdf>
(20)　経済産業省「企業のクラウドサービス利用に際しての最新事例に対応！「クラウドセキュリティガイドライン改訂版」と「活用ガイドブック」を作成しました」2014.3.14. <http://www.meti.go.jp/press/2013/03/20140314004/20140314004-1.pdf>; 総務省「クラウドサービス提供における情報セキュリティ対策ガイドラインの公表」2014.4.2. <http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000073.html>
(21)「クラウド情報セキュリティ監査制度」クラウドセキュリティ推進協議会ウェブサイト <http://jcispa.jasa.jp/cloud_security/>
(22)　Uniting and Strengthening America by Providing Appropriate Tools Required to Interrupt and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, (P.L. 107-56)
(23)「評価認証制度（JISEC）概要」情報処理推進機構ウェブサイト <https://www.ipa.go.jp/security/jisec/scheme/index.html>

ル[24]が、その内部に格納するセキュリティ機能並びに暗号鍵及びパスワード等の重要情報を適切に保護していることを、第三者が試験・認証する制度である「暗号モジュール試験及び認証制度（JCMVP）」[25]が代表的である。組織に関するものでは、企業や組織が情報セキュリティの確保・維持のために継続的に運用すべき枠組みを定めたISO/IEC 27001:2013に基づいて第三者が認定する制度「情報セキュリティマネジメントシステム（Information Security Management System: ISMS）適合性評価制度」が日本情報経済社会推進協会（JIPDEC）により運用されている[26]。

情報セキュリティに関する評価・認証制度は、上述のように多くの制度が整備されている。今後は、制度活用の促進のため、普及啓発と併せて、審査時間の短縮や審査費用の低減といった課題に取り組む必要がある。

執筆：株式会社三菱総合研究所　情報通信政策研究本部　研究員　松本（まつもと）　尭（たかし）
監修：独立行政法人情報通信研究機構
ネットワークセキュリティ研究所　主管研究員
KDDI株式会社　情報セキュリティフェロー　中尾（なかお）　康二（こうじ）

(24) 暗号モジュールとは、暗号化機能、ハッシュ機能、署名機能等のセキュリティ機能を実装したハードウェア、ソフトウェアのこと。後述する「暗号モジュール試験及び認証制度（JCMVP）」の対象は、電子政府推奨暗号リスト等に記載されている暗号化機能、ハッシュ機能、署名機能等の承認されたセキュリティ機能を実装したハードウェア、ソフトウェア。

(25)「暗号モジュール試験及び認証制度（JCMVP）」情報処理推進機構ウェブサイト <https://www.ipa.go.jp/security/jcmvp/index.html>

(26)「情報セキュリティマネジメントシステム（ISMS）適合性評価制度の概要」2014.4.14. 日本情報経済社会推進協会ウェブサイト <http://www.isms.jipdec.or.jp/about/>