ISSN 1883-9045

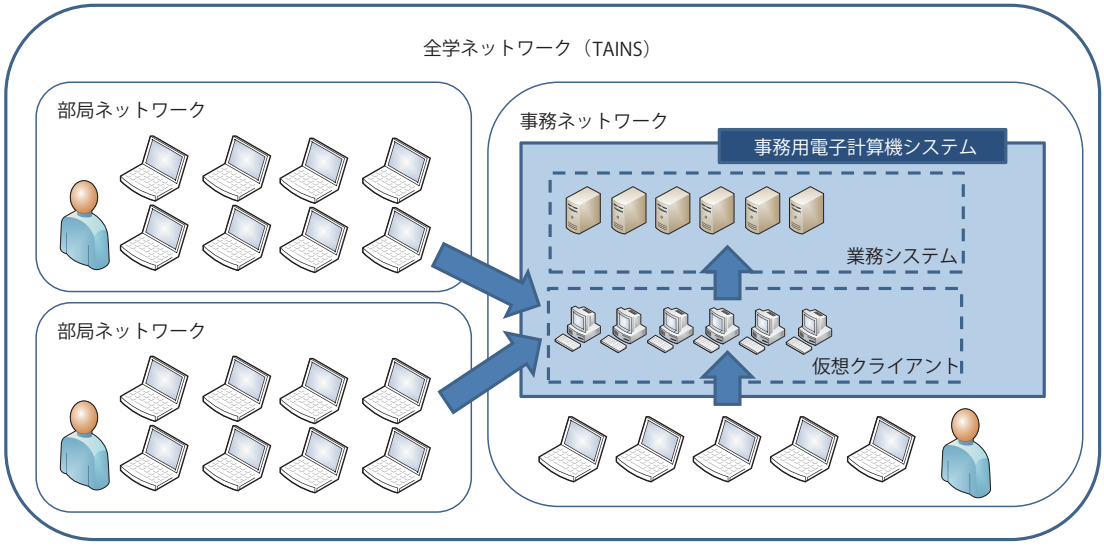
サイバーサイエンスセンター
情報部情報基盤課

東北大学情報シナジー機構

TAINSニュース

東北大学情報シナジー機構 情報シナジー広報室 TAINS ニュース編集グループ

2017.3.31 No.45



新しい事務用電子計算機システムの全体概要図

目 次

※ TAINS ニュースは，全教員および各研究室と事務等の各室に 1 部ずつ配布しています。職員・学生の皆さんにもご回覧ください。また，ウェブで見る場合は http://www.tains.tohoku.ac.jp/news/ をご指定ください。

全学ファイアウォールの申請メニューの強化について

情報部情報基盤課ネットワーク係　野田大輔
情報部情報基盤課ネットワーク係　森倫子
サイバーサイエンスセンター　水木敬明

1　はじめに

2014 年 7 月から運用開始した全学ファイアウォール [1, 2] は，学内に存在するサーバ等が意図せず学外へ公開されることを防止し，さらに 2015 年 6 月からは一部の P2P アプリケーションの通信を遮断するなど，TAINS のセキュリティ向上に貢献してきました。この度さらなるセキュリティの向上を目指し，全学ファイアウォールの許可ポート設定のメニューを拡充しました。本稿ではこの全学ファイアウォールの申請メニューの強化について記載します。

2　通信許可ポートの拡充について

これまで全学ファイアウォールの許可ポート設定は,「全許可」,「全不許可」，そしてウェブサーバ向けの「ウェブサーバのみ許可」の 3 種類でした。許可ポート設定を 3 種類とした理由は，導入初期に予想される多数の申請対応にあたる人的リソースを考慮してのものです。しかしながら実際にはウェブサーバ以外の用途のサーバも数多く存在するため，より適切なアクセス制御の実現を目指し全学ファイアウォールの許可ポート設定を拡充することとしました。

具体的には，これまで「ウェブサーバのみ許可」としていた設定を「サーバ機能」に変更し，その中でウェブサーバ以外のサーバ向けの許可ポート設定も選択できるようにしました。選択できるサーバ機能は「ウェブ」,「メール」,「DNS」,「リモートアクセス」,「サーバ管理」,「遠隔会議システム」の 6 種類です。それぞれの設定の許可ポートは学内向け TAINS ウェブページ [3] をご参照ください。

「サーバ機能」では複数のサーバ機能を組み合わせることができます。例えば当該サーバがウェブサーバとメールサーバを兼ねている場合，サーバ機能のうち「ウェブ」と「メール」を選択することで,「ウェブ」と「メール」のポートを全て許可することできます。これにより学外へ公開するサーバに合わせたより適切なアクセス制御を実施することができます。申請方法の詳細については学内向け TAINS ウェブページ [3] をご覧ください。

3　おわりに

本稿では 2017 年 3 月に実施した全学ファイアウォールの許可ポート設定の拡充について述べました。メールサーバや DNS サーバ向けの許可ポート設定が追加され，より適切なアクセス制御を行うことが可能となりました。部局の管理者の皆様は，セキュリティ対策のさらなる強化のために全学ファイアウォールの設定を今一度ご確認いただき，必要に応じて申請をお願いいたします。

参考文献

[1] 野田大輔, 森倫子, 水木敬明, “全学ファイアウォールについて,” TAINS ニュース, No.43, pp.2–3, 2014. (http://www.tains.tohoku.ac.jp/news/news-43/0203.html)

[2] 野田大輔, 森倫子, 水木敬明, 曽根秀昭, “東北大学全学ファイアウォールの運用に関する報告,” SENAC, Vol.49, No.1, pp.37–39, 2016.

[3] 学内向け TAINS ウェブページ, https://www2.tains.tohoku.ac.jp/

基幹ルーティングによる部局ネットワークの収容について

情報部情報基盤課ネットワーク係　七尾晶士
サイバーサイエンスセンター　水木敬明

1　はじめに

StarTAINS では，部局ネットワークを収容する形態として，基幹ルーティング接続と呼ばれる方式を提供しています [1]。この接続では，部局側のネットワークにてルーティングをする必要がなく，高価な L3 スイッチやルータの導入を不要とすることが可能です。過去にもこの基幹ルーティングに関する TAINS ニュースの記事 [1, 2] がありましたが，本稿では改めて基幹ルーティング接続とその利用状況について簡単に説明します。

2　基幹ルーティング接続とは

StarTAINS 以前の TAINS では，幹線と部局のネットワークを接続する際に，L3 スイッチやルータを用いて接続していました。比較的規模の大きな部局のネットワークでは，大抵サブネットが複数構築されるのでサブネット間のルーティングのため L3 スイッチは自然と必要となり，導入の敷居は高いものではありませんでした。しかし，規模の小さな部局では，サブネットが一つしかないのに比較的高価な L3 スイッチを導入することは費用的に敷居が高いものでした。また，L3 スイッチの設定にはスイッチにログインしてテキストベース[1]で設定するなど，専門的な知識も必要となっていました。

2009 年運用開始の StarTAINS から提供を始めた基幹ルーティング接続を利用しますと，図 1 のように部局側で L3 スイッチを用意する必要がありません。そのため，比較的安価な L2 スイッチのみでネットワークを構築することが可能となり，ネットワークの導入や維持費用を低く抑えることができます。また設定についても複雑な L3 の設定をする必要が無いので，比較的簡単にネットワークを構築することが可能です。

3　セキュアプライベートネットワークとは

本学は 2014 年に全学ファイアウォールを導入しましたが [3]，近年グローバルアドレスを狙った攻撃はますます増えつつあります。StarTAINS ではセキュアプライベートネットワークを提供しています。

セキュアプライベートネットワークでは，クライアントに割り当てる IP アドレスをグローバルアドレスではなく，プライベートアドレスを割り当て，図 2 で示すように幹線側にて用意したファイアウォール (FW) を経由してアクセスするようになってます。費用的にあるいは維持管理に手間がかかるなどの理由で FW の導入が困難である場合は，こちらのサービスを利用することにより手軽にセキュアなネットワークを導入することが可能です。

[1] ウェブブラウザ上の GUI で設定可能な機種もあります。

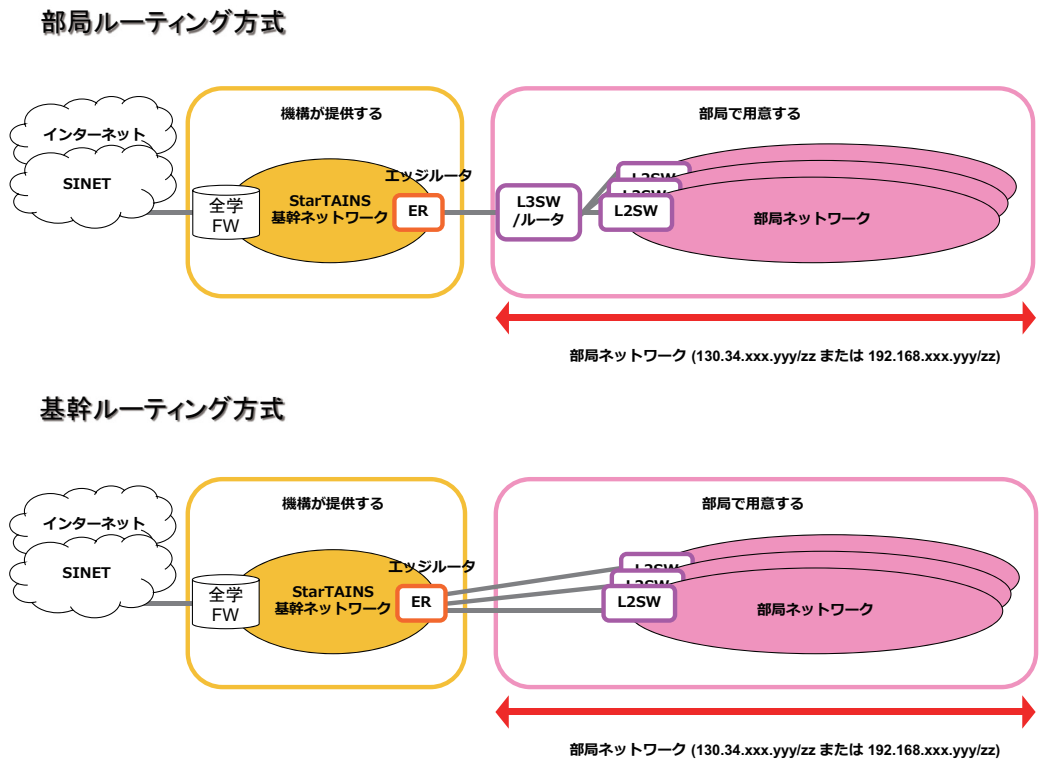


図 1: 部局ルーティング接続と基幹ルーティング接続

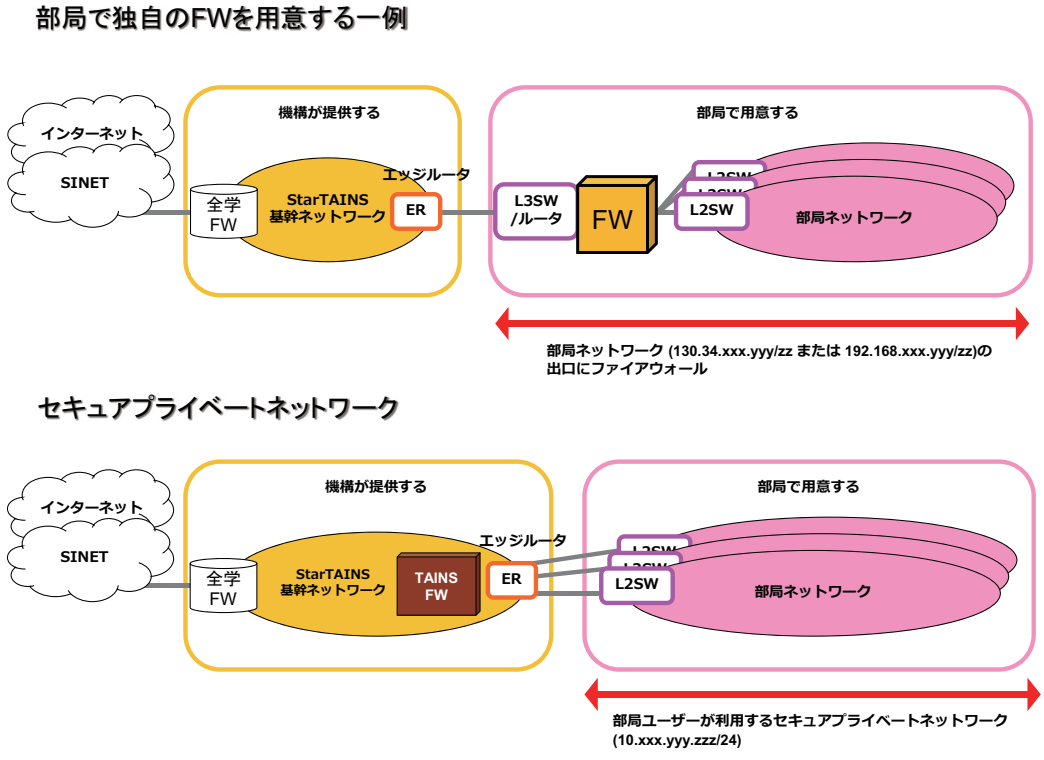


図 2: 部局で独自の FW を用意する一例とセキュアプライベートネットワーク

4 現在の利用状況

スモールスタートで運用を開始し，一部の部局から少しずつ利用が進んできた当基幹ルーティング接続も，現在では 18 部局に対してグローバルのサブネットが 185 個，学内流通プライベートのサブネットが 27 個，セキュアプライベートのサブネットが 459 個の提供を行うまでになりました[2]。サービス開始当初の事例として，工学研究科機械・知能系の StarTAINS への移行の記事 [2] があります，また最近では，理学研究科の一部の建物や，多元物質科学研究所の全ての建物で基幹ルーティング接続とセキュアプライベートネットワークが導入されています。導入にご尽力いただいた部局技術担当者の方々からコメントをいただきましたので掲載します。

部局技術担当者の声

全学で様々なサービスの提供が始まったおかげで，それぞれのケースに合ったネットワークを選択できるようになりました。例えば，新しくできた組織にネットワークを提供する事は，今までかなり苦労してきましたが，セキュアプライベートネットワークサービスを利用するとスイッチングハブを準備するだけで簡単にネットワークを導入できる場合が増えてきました。

このようなサービスを利用させて頂くことで今まで数十万円もするネットワーク機器が必要だったところが安価にすませられるようになったことは大変嬉(うれ)しく感じます。

理学研究科 部局技術担当者 千葉淳 様

エッジルータを用いた複数研究棟間通信について

部局でルータを用意する必要が無くなり，拡張性に優れたエッジルータを利用できることは非常に助かります。反面，障害発生時に部局サイドでエッジルータから情報を得られないため，少々トレースが面倒になるなどを感じました。

セキュアなプライベートネットワークを利用して

Type-A を使用していますが，プロキシを設定し忘れることがある以外は利用者側に大きな混乱もなく使用できています。通信速度も確保できているとのことです。

多元物質科学研究所 部局技術担当者 千葉裕輝 様

今後も基幹ルーティングの利用の拡大を進めたいと考えていますので，本記事を参考にして部局内でご検討いただけると幸いです。導入にあたってのご質問などは，お気兼ねなく情報部情報基盤課ネットワーク係へお問い合わせいただければと思います。

参考文献

[1] 水木敬明, 曽根秀昭, “エッジルータにおける接続サービスの見通し,” TAINS ニュース, No.37, pp.9-10, 2009.
(http://www.tains.tohoku.ac.jp/news/news-37/0910.html)

[2] 2017 年 3 月時点の数値です。

[2] 鏡慎吾, 岩崎智彦, 大橋俊朗, 桑野博喜, 後藤英昭, 小林広明, 近野敦, 丹下和也, 永井大樹, 平田泰久, 琵琶哲志, “機械・知能系ネットワークの StarTAINS への移行,” **TAINS** ニュース, No.40, pp.3-7, 2012.
(http://www.tains.tohoku.ac.jp/news/news-40/0307.html)

[3] 野田大輔, 森倫子, 水木敬明, “全学ファイアウォールについて,” **TAINS** ニュース, No.43, pp.2-3, 2015.
(http://www.tains.tohoku.ac.jp/news/news-43/0203.html)

事務用電子計算機システムの更新について

情報部情報推進課事務情報係　藤本一之

1　はじめに

本稿では，2016 年 8 月に本稼働した事務用電子計算機システム（以下「本システム」という。）について記載します。本システムは，1,600 台の仮想クライアントと，6 つの業務システム（人事給与統合システム・財務会計システム・予算照会システム・学納金管理システム・授業料免除システム・勤務時間管理システム）が稼働し，事務系職員の日々の業務を支えています。

2　導入の目的

本学においてこれまで構築・稼働していた業務システムは，クライアント／サーバー方式，サーバーベースコンピューティング方式，Web 方式と多岐にわたり，それぞれのシステムが独立したサーバーで稼働していました。

本システムでは，これらの業務システムを，サーバー仮想化の技術を用いて統合・集約し，プライベート・クラウドを構築することにより，限られたサーバリソースを動的に割り当てることや，各業務システムがそれぞれ調達している機器のうち，共有可能な機器は共有し，同種の機器を複数調達することなく，中長期的な投資効果を高めることを目的としました。

また，事務系職員が利用する端末については，これまではすべて各学部の資産として管理されており，機種も仕様もばらばらで，問題発生時の対処が非常に困難でした。さらに，職員の異動時は継続して使うことができないため，USB メモリなどを使ってメールやドキュメントなどのデータを異動先の端末に移していました。これらの運用方法は，職員の作業負荷が増えるだけでなく，セキュリティの観点からも懸念事項でした。

本システムでは，仮想クライアントを用い，統一された環境を一元的に管理することでセキュリティを高めること，また，各業務システムが OS やブラウザの種類に影響されずに使用できるようにすることで，本学既存の IT 資産を最大限活用するとともに，将来に渡り更新にかかるコストを削減することも目的に加えました。

3　導入効果

3.1　仮想クライアント

仮想クライアントを導入したことにより，以下のような効果を得ることができました。

1. 職員が利用する端末が仮想クライアント環境として統一され，セキュリティ対策ソフトの一元管理が可能になり，セキュリティの脅威が低減しました。
2. 人事異動時のデータ移行作業が不要になり，職員の負担が軽減されたとともに，USB メモリ等を使用する必要がなくなったことから，セキュリティリスクが低減しました。

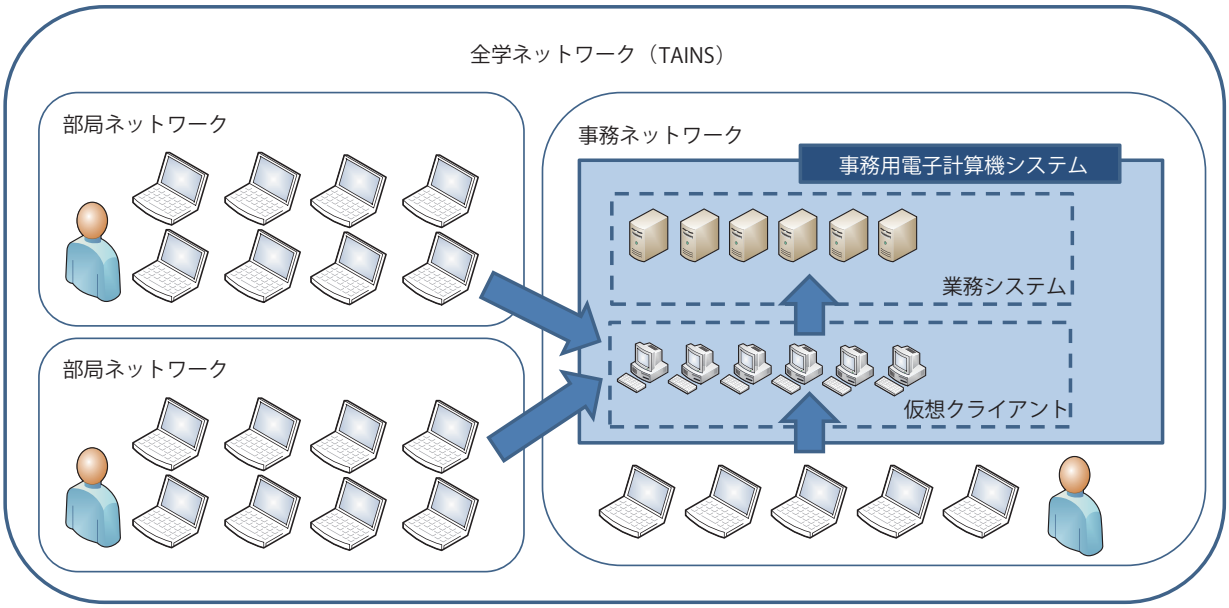


図 1: 本システムの全体概要図

3. 事務ネットワーク以外の全学ネットワーク (**TAINS**) 上のユーザーから要望があった場合に，新たに事務ネットワークを引く必要がなくなり，課題となっていたネットワークへの二重投資が不要になりました。

4. これまで使用していた机上の端末をそのまま利用し，仮想クライアントに接続することができるため，本システムの導入に伴い不必要な端末の買い替えを防ぐことができました。

3.2　業務システム

業務システムの仮想化統合を行ったことにより，以下のような効果を得ることができました。

1. これまでのように，各業務システムそれぞれでサーバーを準備する必要がなくなりました。

2. 各業務システムそれぞれでかかっていたサーバー保守費用が一元化されました。

3. 各業務システムの実際のリソース使用状況を確認し，それぞれの繁忙期・閑散期に応じて，リソースの割り当てを柔軟に変更することが可能となりました。

4　おわりに

本システムの導入により，事務系職員の業務を支える情報インフラ環境が整備されました。

仮想クライアントの導入により，一般的には相反することとされる【利便性】と【セキュリティ】の双方を両立することができたと考えます。また，増え続ける業務システムのリソースに対する投資の最適化，という効果を得ることができたと考えています。

まずはインフラ面での最適化がなされたことから，今後は，各業務システム間のデータ連携を整備し，これまで手作業で行っていたような各業務システムを用いる担当者間での情報連携を，システム間のデータ連携として行うことにより，より業務を最適化できるだろう，と考えています。

情報「断・捨・離」のススメ

情報シナジー機構　折内新司

1　はじめに

近年，サイバー攻撃の手口はますます巧妙化しており，情報セキュリティに対する脅威も増大しています。

被害に遭わないように対策を取るのはもちろんですが，被害のリスク（損害を受ける可能性・影響度）を軽減する策を考えてみます。

2　現状の分析

2017 年 1 月末に，独立行政法人情報処理推進機構 (IPA) が「情報セキュリティ 10 大脅威 2017」を発表しました。これは，2016 年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から，約 100 名の選考メンバーによって,「個人」と「組織」という異なる視点で 10 大脅威を選出しているものです。

■「情報セキュリティ 10 大脅威 2017」　（IPA 情報セキュリティ 10 大脅威 2017 [1] より）

昨年順位	個人	順位	組織	昨年順位
1 位	インターネットバンキングやクレジットカード情報の不正利用	1 位	標的型攻撃による情報流出	1 位
2 位	ランサムウェアによる被害	2 位	ランサムウェアによる被害	7 位
3 位	スマートフォンやスマートフォンアプリを狙った攻撃	3 位	ウェブサービスからの個人情報の窃取	3 位
5 位	ウェブサービスへの不正ログイン	4 位	サービス妨害攻撃によるサービスの停止	4 位
4 位	ワンクリック請求などの不当請求	5 位	内部不正による情報漏えいとそれに伴う業務停止	2 位
7 位	ウェブサービスからの個人情報の窃取	6 位	ウェブサイトの改ざん	5 位
6 位	匿名によるネット上の誹謗（ひぼう）・中傷	7 位	ウェブサービスへの不正ログイン	9 位
8 位	情報モラル不足に伴う犯罪の低年齢化	8 位	IoT 機器の脆弱（ぜいじゃく）性の顕在化	ランク外
10 位	インターネット上のサービスを悪用した攻撃	9 位	攻撃の ビジネス化（アンダーグラウンドサービス）	ランク外
ランク外	IoT 機器の不適切管理	10 位	インターネットバンキングやクレジットカード情報の不正利用	8 位

これらの脅威に関しては，本学においても被害を受けるおそれがあり，日々の対策が欠かせない状況となっています。システムの脆弱（ぜいじゃく）性に対する修正ソフトの速やかな適用や，不適切なパスワードの運用を改めるこ

とは，被害を未然に防ぐためには非常に重要です。またコンピュータウィルスなどのマルウェアに感染をしない・ネットワークやシステムに侵入させないという「入口対策」と共に，情報を外に漏らさない「出口対策」も重要となります。TAINS でも，セキュリティ対策ソフトの配布や，全学ファイアウォールでの侵入防御，既知のマルウェア感染による通信先を遮断するなど，情報漏えいを防ぐための取り組みを順次行っています。

しかし，10 大脅威として 2016 年に続いて高い順位となっている標的型攻撃やランサムウェアによる被害，新たな脆弱(ぜいじゃく)性の露見によるゼロデイ攻撃など，マルウェアの感染や侵入を完全に防ぐのは難しくなっています。先日教職員を対象に行われた「標的型攻撃メール訓練」でも，何割かの方が訓練メールに添付された疑似ウィルスファイルを開いてしまいました。普段から注意はしていても，ちょっとした隙をつかれて感染被害に至ってしまう危険があることを示しています。これらのことからも，感染しないための対策と共に，万が一の感染の場合に被害を最小限にする対策も必要であることがわかります。

被害規模が拡大する要因のひとつとしては,「不要な情報を大量に保有していること」が挙げられます。不要な情報を大量に持ち続けることは，セキュリティ事故に対するリスクであると認識しなければなりません。

本部事務機構を対象に行ったリスクアセスメントでは，課のファイルサーバに数十万ファイルの業務データが保存されている事例がいくつかありました。また，保管期限が明確でないファイルや，無期限保存のファイルも数多く存在しています。ハードディスクの大容量化などで保存しておくことの障壁が小さくなり，とりあえず残しておくという場面が増えたことも一因と考えられます。

日々多くやり取りする電子メールに関しても，整理が追い付かずどんどん溜(た)まっていく傾向があります。Cc で受信したメールなどは自分が当事者ではない場面も多く，機密性の高い情報が紛れ込んでも管理が不十分になりがちです。パソコンに保存している大量の過去メールや添付ファイルは，マルウェア感染などが起こった場合に漏えいの大きなリスクとなります。

これらの大量に蓄積された情報に対してセキュリティ事故が起きると，大規模な情報漏えいにつながるのはもちろんのこと，漏えいしたものの把握・影響範囲を特定することも非常に困難な作業となります。被害を最少に抑えると共に，被害範囲を明確にすることは事故処理の迅速化にも重要ですが，数十万ファイルの中身を把握することは大変難しい作業となります。

3 リスクを低減するために

前述のように，情報セキュリティ上のリスクとなる不要な情報は，できるだけ溜(た)め込まないように削減していくことが，被害を抑えることにつながります。

以下に対策の一例を記します。

- 法人文書に該当するものは,「国立大学法人東北大学法人文書管理規程」に準拠して保存・廃棄の管理を行う必要があります。ルールに従って，保存ないし廃棄の処置をしてください。
- ファイルを溜(た)め込んでしまってから整理をするのは大変で，なかなか実施できないものです。
  最終版が出来あがったところで作成途中の版やコピーした関連資料を捨てる，といったちょっとした習慣で，そもそも保存対象の情報量を増やさないことが重要です。
- 電子メールも，溜(た)め込まない工夫が必要です。Cc 受信や係メーリングリスト宛といった自分で保存する必要性の低いメールは，順次削除しましょう。メールの振り分け機能で分類し一ヶ月ごとに消す，といったシンプルな策が有効です。
  またメールを発信する場合も，不必要な Cc を増やさないことを意識しましょう。

- 学外へ持ち出すパソコンに保存するファイルは最小限にしましょう。特に学会などの海外渡航では紛失盗難のリスクが高く，強盗被害などは本人の注意だけでは避けられません。ハードディスク暗号化などの対策とともに，持ち出す情報を最小限にする対応も必要です。日常使用で大量にデータやメールの入ったノートパソコンをそのまま持ち出すのは極めて危険です。

- 収集・作成する情報の内容についても，不用意に機密性や重要度の高い情報を集めないようにする注意が必要です。例えばマスタファイルから抽出した一覧を作る場合でも，レコード中の不必要な項目は除外して最小限の項目とすることで，万が一の漏えい時の実害を抑えることが出来る場合もあります。必要でないメールアドレスや連絡先電話まで流用元ファイルからそのまま転記，としていないか，本当にその情報項目は必要か一考しましょう。

- 利用頻度が低いが消せないファイルに関しては，取り外し型の HDD や CD/DVD などのオフライン媒体に移動してしまうのもマルウェアによる漏えい防止策の一つです。これはランサムウェアによる暗号化被害の対策としても有効です。
  ただしこの場合は，媒体の紛失や誤廃棄が起こらないように管理を行う必要があり，台帳管理と施錠保管が望まれます。（バックアップ媒体が紛失すれば，漏えいと同様のセキュリティ事故となります）

- 研究室や学生サークルでも，個人情報を含んだ名簿などがあちこちに分散して残っていないでしょうか。歴代の記録は大切ですが，OB やすでに退会した人など構成員でなくなった人の個人情報を保有し続けることは望ましくありません。

- 自宅のパソコンに関しても，保存情報の確認をしましょう。情報統制が緩かった昔に持ち帰ったり転送していた情報が残っていて，攻撃の大規模化・巧妙化により何年も経過した今になって漏えいする，という例もあります。不必要な情報はきちんと削除しましょう。
  また，ランサムウェアは個人の被害も多く発生しています。家族の思い出の写真データが全て失われるといった被害に遭わないよう，事前のバックアップなどが望まれます。

- 容量の小さなハードディスクを「いつか使うかも」と保存していませんか。その中に情報は残っていませんか。機器の進化が早い昨今，実際に活用できる場面はほとんど無いと想像されます。反面，万が一情報機器を紛失すると，その中に漏えい被害を起こす情報が無かったことを証明するのは困難です。リスクとなりますので，きちんと破砕して廃棄しましょう。

これらは，情報資産をスリム化するために「断・捨・離」[1]すること，と言えるかもしれません。不要なものを取り込まない・溜めない「断」と，不要なものを捨てる「捨」で，保有する情報資産を削減することがリスク低減につながり，また本当に守るべきものを明確化することにつながります。「離」には「物への執着やこだわりから離れる」という意味があるそうです。「今までこうやって来たから」というこだわりを捨てて，業務のやり方（情報の集め方や保管ルール）の見直しを進めていくことと共通点があります。

4　おわりに

ビッグデータ時代を迎えて，蓄積された大量の情報が新たな価値を生むという事例も増えています。しかし，情報セキュリティに関する領域では，情報の溜め込みはリスクを増大させる要因の一つです。
情報資産を「断・捨・離」して，スリム化によるリスク低減を進めましょう。

[1]「断捨離」は，やましたひでこ氏の登録商標です。(http://yamashitahideko.com/)

参考文献

[1] 独立行政法人情報処理推進機構 (IPA), 情報セキュリティ10 大脅威 2017,
http://www.ipa.go.jp/security/vuln/10threats2017.html

編集後記

■サイバーサイエンスセンターに 30 年以上も勤務し，定年を迎えることができました。これも多くの方々のご指導があってのことです（言うまでもなく）。ありがとうございました。振り返れば，**TAINS88**，**SuperTAINS**，**TAINS/G**，**StarTAINS** などに夢中で取り組み，気が付けば定年になってしまったというのが実感です。

TAINS を通して多くの方々に出会い，長い間良い関係で過ごすことができ，さらに様々な場面で助けていただいたことに感謝いたします。定年後の人生を良い思い出を抱きながら過ごしたいと考えています。長い間お世話になりました。

(ch)

■この度，長年 **TAINS** の運用にご尽力いただきました，情報基盤課千葉課長が退職されることとなりました。インターネットとは何なのか，という時代に始まり，長きに渡って東北大学の基幹ネットワーク **TAINS** を支えていただきました。

みなさんご存知の通り，ネットワーク，情報セキュリティの技術革新や情勢の変化は凄まじいものです。そんな中，常に最新の技術を取り入れ，一つとして前例のないような困難な状況の下，予算獲得から設計，構築，保守，運用まで，持ち前の高いコミュニケーションスキルを生かして学内外の多方面との連携・調整をしていただくなど，正に **TAINS** にとってなくてはならない存在でした。

また，情報基盤課の職員の育成にもご尽力いただきました。情熱と愛情を持って **TAINS** と職員を育てていただいたことはいつまでも忘れません。課長に教えていただいたたくさんのことを糧にこれからもネットワーク係一同 **TAINS** の運用に励んでいきたいと思います。

(nm)

TAINS ニュース投稿案内

TAINS ニュースでは皆さんから投稿していただいた原稿についても積極的に掲載していこうと考えております。下記の注意事項に沿って，どしどし原稿をお寄せください。

- 術語以外は常用漢字を用い，新かなづかいを用いて「ですます体」でお書きください。表外字についてはふりがなを振らせていただく場合があります。句読点は,「,」と「。」に統一させていただきます。
- 本文については原則として電子的に提出するものとします。tainsnews06［AT］tains.tohoku.ac.jp あてに電子メールで投稿してください。
- LaTeX 2_ε形式の原稿を歓迎します。クラスファイルとテンプレートは
  http://www.tains.tohoku.ac.jp/news/tainsnews.cls
  http://www.tains.tohoku.ac.jp/news/template.tex
  に置いてありますので，お手持ちのウェブブラウザにより取り出してください。
- 図は十分に精細で鮮明なものを提出してください。図についても PostScript 形式で電子的に投稿していただくことを歓迎します。
- 手書きで投稿したいなど，事前のご相談は，以下までお願いします。

〒 980-8578 仙台市青葉区荒巻字青葉 6–3
東北大学サイバーサイエンスセンター内
情報部情報基盤課ネットワーク係
email: tains［AT］tains.tohoku.ac.jp
TEL: 内線（青葉山）6253 / 022-795-6253
FAX: 内線（青葉山）6098 / 022-795-6098

投稿していただいた原稿は，情報シナジー機構情報シナジー広報室 **TAINS** ニュース編集グループで閲読のうえ採否を判断させていただきます。閲読の結果，編集グループが必要と認めた場合には，原稿の訂正や修正をお願いすることがあります。転載や図版の使用については，著作権者の承諾を得ておくようお願いします。また，**TAINS** ニュースが，東北大学のウェブサイトを通して電子的にも公開されることを，予めご了承ください。

TAINS ニュース 第 45 号
発行日　2017 年（平成 29 年）3 月 31 日
編　集　東北大学情報シナジー機構 情報シナジー広報室
TAINS ニュース編集グループ
曽根 秀昭，水木 敬明，後藤 英昭，阿部 亨，
森 倫子，七尾 晶士, 北澤 秀倫，野田 大輔
発　行　東北大学情報シナジー機構
〒 980-8578 仙台市青葉区荒巻字青葉 6–3
（東北大学サイバーサイエンスセンター内）