通信インフラの
サイバーセキュリティ対策

東京都市大学　林 正博

目次

サイバー攻撃の現状

NECによる分析

https://jpn.nec.com/techrep/journal/g17/n02/170204.html

重要インフラへの攻撃件数

2010年にイランにあるウラン濃縮工場の遠心分離器を破壊したマルウェアStuxnetの登場以降，海外ではエネルギー分野や重要機器製造分野，通信分野などへのサイバー攻撃が増加しています．そのなかで，ウクライナでは電力システムを狙ったサイバー攻撃によって大規模停電が2015年と2016年に連続して発生している．このことから，電力など特に経済への影響が大きいエネルギー分野では、高度なサイバー攻撃を受ける恐れがあると考えられる．

攻撃件数は年々増大！

重要インフラへの攻撃事例の一部

発生国	公表時期	事例内容	原因
米国	2001	SCADAシステム改修のため２週間停止	契約ベンダー向けVPN接続システムのアクセス保護の不備
米国	2003	デービス・ベッセ原子力発電所のSCADAシステムが約5時間、プロセスコンピュータが約6時間停止	Slammerが契約ベンダーが使用するVPN接続を介して侵入・感染
EU	2003	多数の配電変電所の管理機能が３日間喪失	分散SCADAシステムへのマルウェア感染
日本	2005	原子力発電所の機密情報がファイル共有ソフト経由で流出	従業員が機密情報を格納していた自宅PCにマルウェアが感染
日本	2006	火力発電所の機密情報がファイル共有ソフト経由で流出	従業員が機密情報を格納していた自宅PCにマルウェアが感染
米国	2006	ブラウンズ・フェリー発電所の再循環水ポンプの制御喪失	発電所統合ICSネットワーク上の過度のトラフィックによるSiemens Perfect Harmony VFDコントローラーの誤動作
米国	2010	コンピュータの誤作動により、ガスパイプラインからガスが漏えい	コンピュータの誤作動（誤作動の原因は不明）
イラン	2010	マルウェアStuxnetにより、ナタンズ燃料濃縮工場で遠心分離器が破壊	マルウェア感染
米国	2012	2つの発電所で制御システム環境内のコンピュータへマルウェアが感染し、片方は再稼働が3週間遅延、もう片方は運用制限が発生	作業用USBドライブへのマルウェア感染
米国	2014	米国とカナダの防衛航空会社や航空会社、EUを含めたエネルギー企業を標的とした攻撃による情報漏えい	Dragonflyハッカーグループによる攻撃によってSCADAシステムにマルウェア（Havex）が感染
米国	2015	FirstEnergy社に対する大規模DoS攻撃（被害なし）	不明
ウクライナ	2015	ウクライナ西部（イヴァーノ＝フランキーウシク州）で数時間停電が発生	マルウェアBlack Energy 3を用いたサイバー攻撃
イスラエル	2016	コンピュータシステムの一部がサイバー攻撃対応のため、2日間停止	フィッシング攻撃によるマルウェア感染
ドイツ	2016	2013年または2014年頃にサイバー攻撃によって混乱が発生した事実の公表	不明
ウクライナ	2016	キエフ市内の電力供給先の５分の１が約１時間停電	マルウェアIndustroyer/Crash Overrideを用いたサイバー攻撃
ウクライナ	2017	チェルノブイリ原子力発電所の放射線モニタリングシステムへのマルウェアNotPetyaの感染によって手動制御を余儀なくされる	マルウェア感染（ランサムウェア）

- 以前は情報漏洩や過負荷による異常動作などの被害が多かったが，最近では物理的被害（停電など）が多い．
- 通信（あるいは電力）インフラは，単一障害に対する耐性は保持しているが，多重障害には強くないことで被害発生．

政府の対応

読売新聞　8月３日の記事

　政府が、サイバー攻撃などによる「大規模インフラ障害」に関する対応方針を初めて取りまとめたことがわかった。電力や水道の障害が長期化するような事例を自然災害と同様に法律上の「災害」と位置づけることが柱で、迅速に行政支援を行う狙いがある。

首相官邸

　対応方針は、関係省庁による連絡会議で６月末にまとめた。サイバー攻撃が巧妙化する中、甚大な社会的影響に的確に対処するためのもので、大規模インフラ障害として、人為的ミスを含むシステム障害で引き起こされた大規模停電、通信障害などを想定している。

サイバー攻撃は「災害」！

本発表のスコープ

最近では，物理的な攻撃(ウィルスを仕込んだUSBを物理的にパソコンに差し込むなど）も大きな問題であるが，本発表では，ソフト的な攻撃に話を絞る.

セキュリティを取り巻く技術的インパクトについて述べ，その後、私の考える対策を述べる.

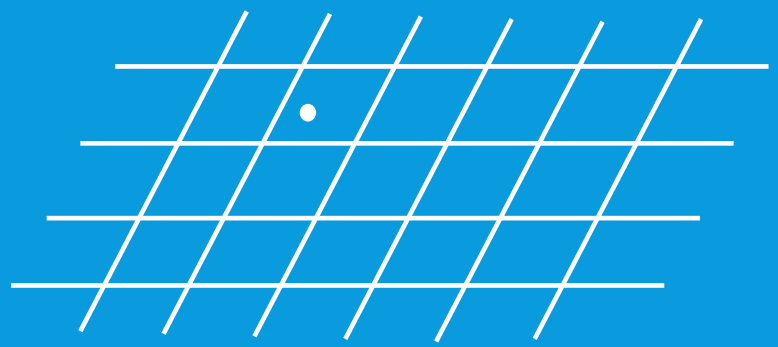
最後に，小さな故障（サイバー攻撃による障害を含む）が別業種のネットワークに波及し，大規模災害に近い状況を引き起こす現象についての研究について述べる.

カスケード故障

テクノロジーからのインパクト

量子コンピュータからのインパクト

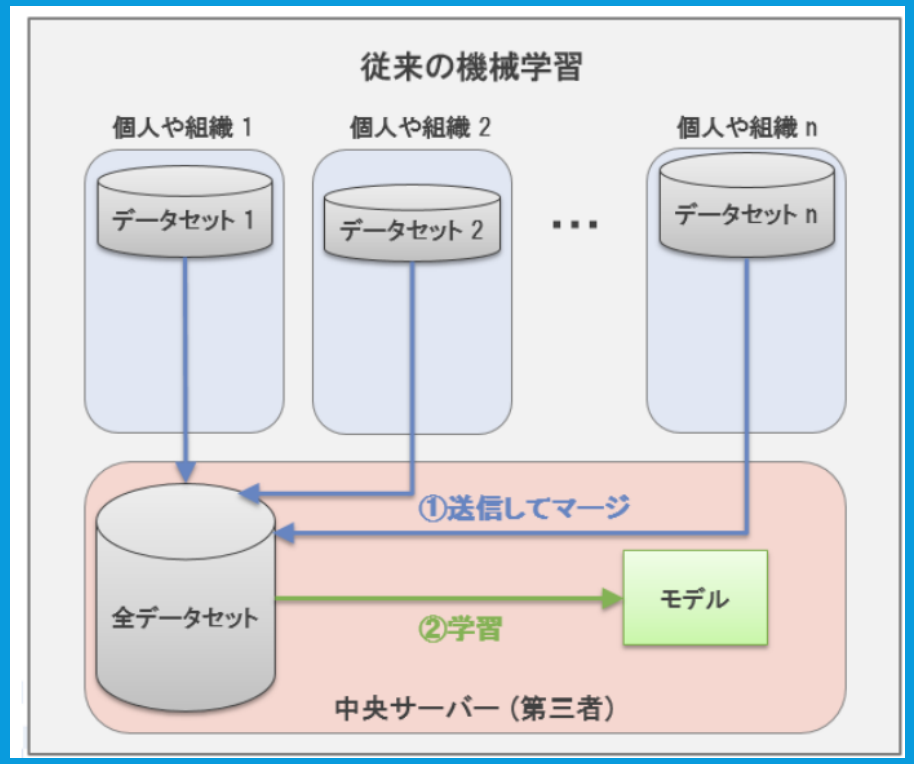
- 現代の暗号システムは，素因数分解が高速に実行できると破られてしまう.
- 量子コンピュータが実現されれば、素因数分解は高速に実行可能(ショアのアルゴリズム, 1994)
- 格子暗号への転換！

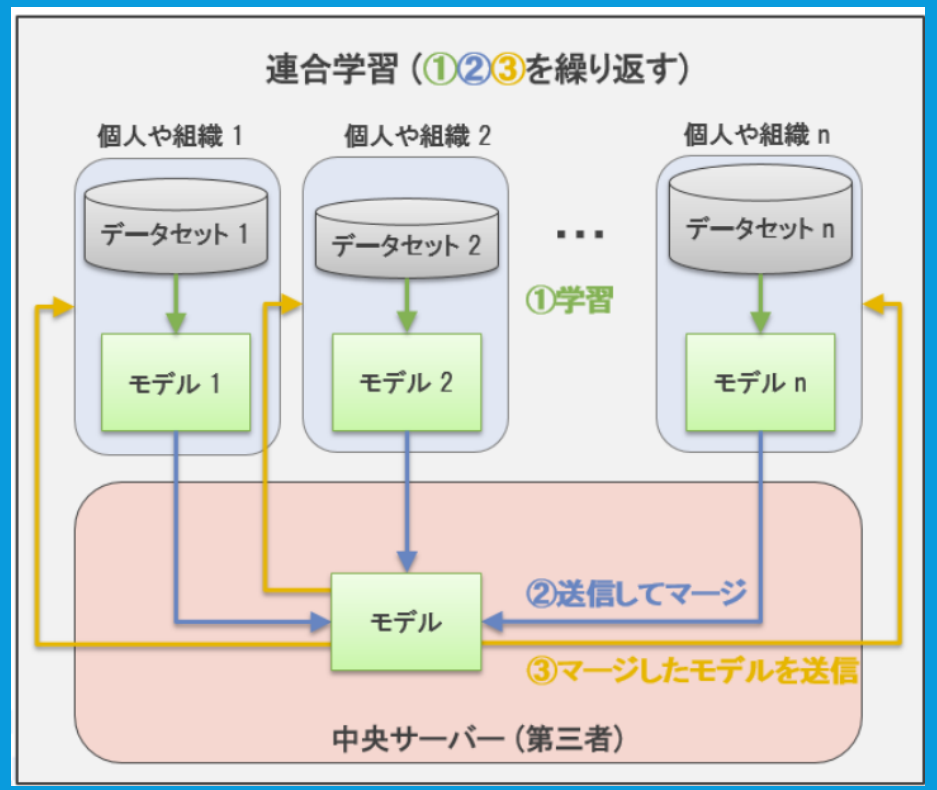


- 格子と点が与えられたとき，一番近い格子点(線が交わった点)からのずれのを計算することが極めて困難であることを利用

人工知能について

単一のコンピュータによる機械学習から複数コンピュータの連携による機械学習へ！　⇒　集中型→分散型　⇒　連合学習





https://www.msiism.jp/article/federated-learning.html

連合学習の問題点

複数のコンピュータが連携して計算を行うので，データ漏洩を防ぐために，計算そのものを秘密に行う必要がある.

秘密計算

秘密分散計算

計算すべきデータ(シークレット)を複数に分離し(シェアと呼ぶ),
シェアを一定数集めなければシークレットは復元できない.

⇒　秘密分散

シェアを用いて計算し，得られた結果を再び集め，計算結果を復元

⇒　秘密分散計算

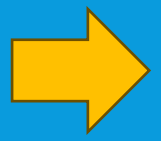
秘密分散計算のイメージ

3 + 2×5の計算

3を二つの別のデータに分離　⇒　** と##

2を二つの別のデータに分離　⇒　@&と＄％

5を二つの別のデータに分離　⇒　<>と”(



別々の計算機で「** + @& × <>」と「## + $% × ”(」を計算.

それぞれの計算結果を合わせて13を得る

二つの計算機同士間でデータのやり取りがなければ，計算内容は誰にも分らない！

いわゆる「鍵」を用いない点が特徴！

完全準同型暗号

以下の性質を満足する関数φを用意する.

$\varphi(x+y)=\varphi(x)+\varphi(y)$, $\varphi(x\times y)=\varphi(x)\times\varphi(y)$,
鍵を知るものみが$\varphi(\ )$の逆写像$\varphi(\ )^{-1}$を作成できる.

$3+2\times5$の計算をしたい場合，$3, 2, 5$をそれぞれφを使って暗号化し，$3+2\times5$の代わりに$\varphi(3)+\varphi(2)\times\varphi(5)$を計算する.

上記性質より,

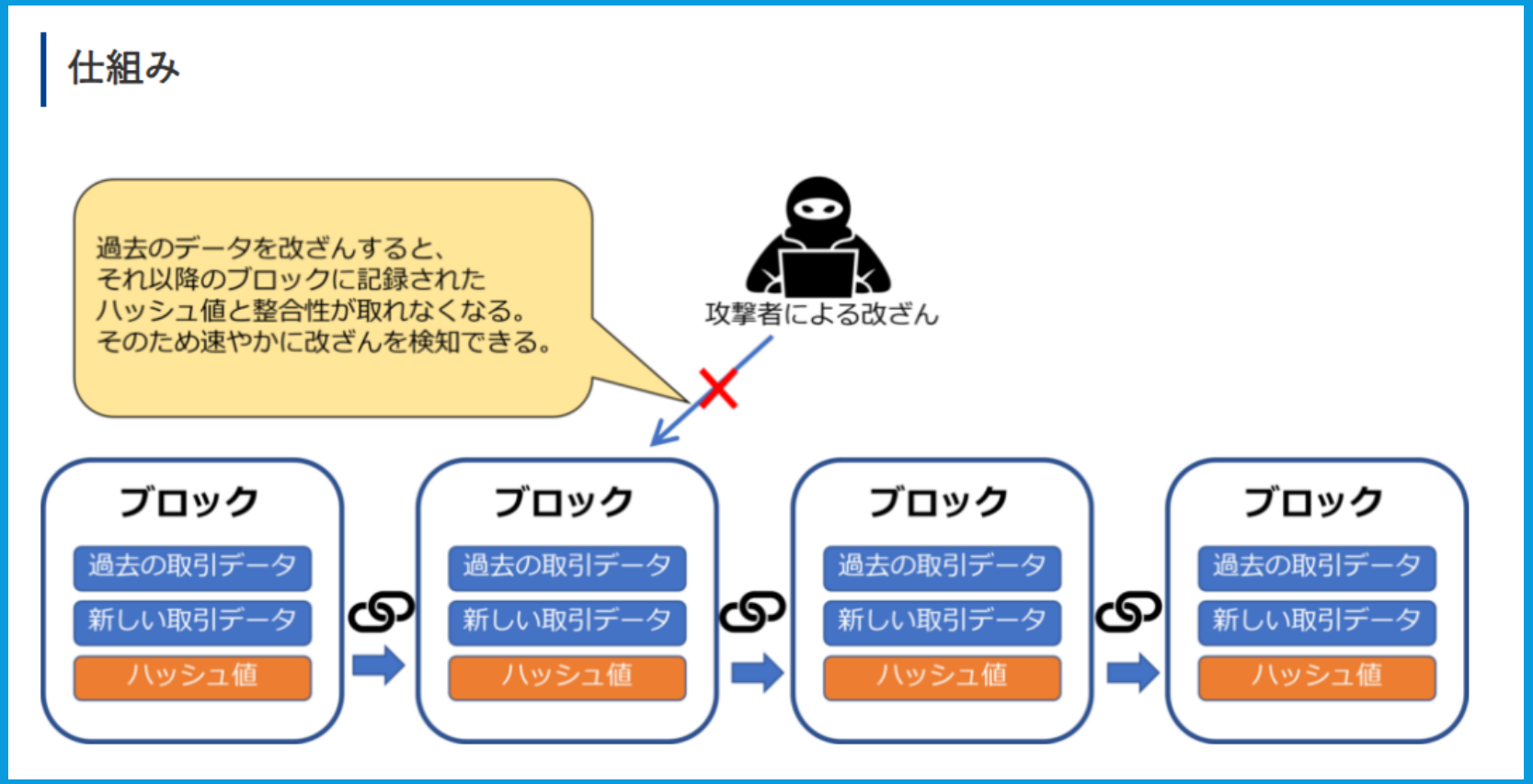
$$\varphi(3)+\varphi(2)\times\varphi(5)=\varphi(3+2\times5)=\varphi(13)$$

なので，鍵を知っていれば，$\varphi(\varphi(13))^{-1}=13$を得る.

完全準同型暗号は，長い間夢の技術であったが，2009年にジェントリが実用的な方法を提案した. ⇒ 格子暗号使用.

ブロックチェーン

取引データを「ブロック」という単位で記録し，それを「チェーン」として繋げて時系列に保存する.



https://www.kagoya.jp/howto/cloud/cloudtrend/blockchain/

鍵を使って秘密にするのではなく，逆に公開することによって，改ざんを防ぐ！

ビットコインなど，仮想通貨の実現に利用されている.

テクノロジーの側面からのまとめ

量子コンピュータ出現のインパクト！

⇒　これまで解けなかった暗号が解けてしまう.

⇒　格子暗号

秘密計算のインパクト！

鍵を用いた暗号から，そうではない秘密化技術の登場！

⇒　秘密分散，ブロックチェーン

秘密分散計算で，同じやり方を計算にまで利用せず，単にデータを秘密化するだけに用いるときは「秘密分散」と呼ぶ.

ではどうすればよいか！

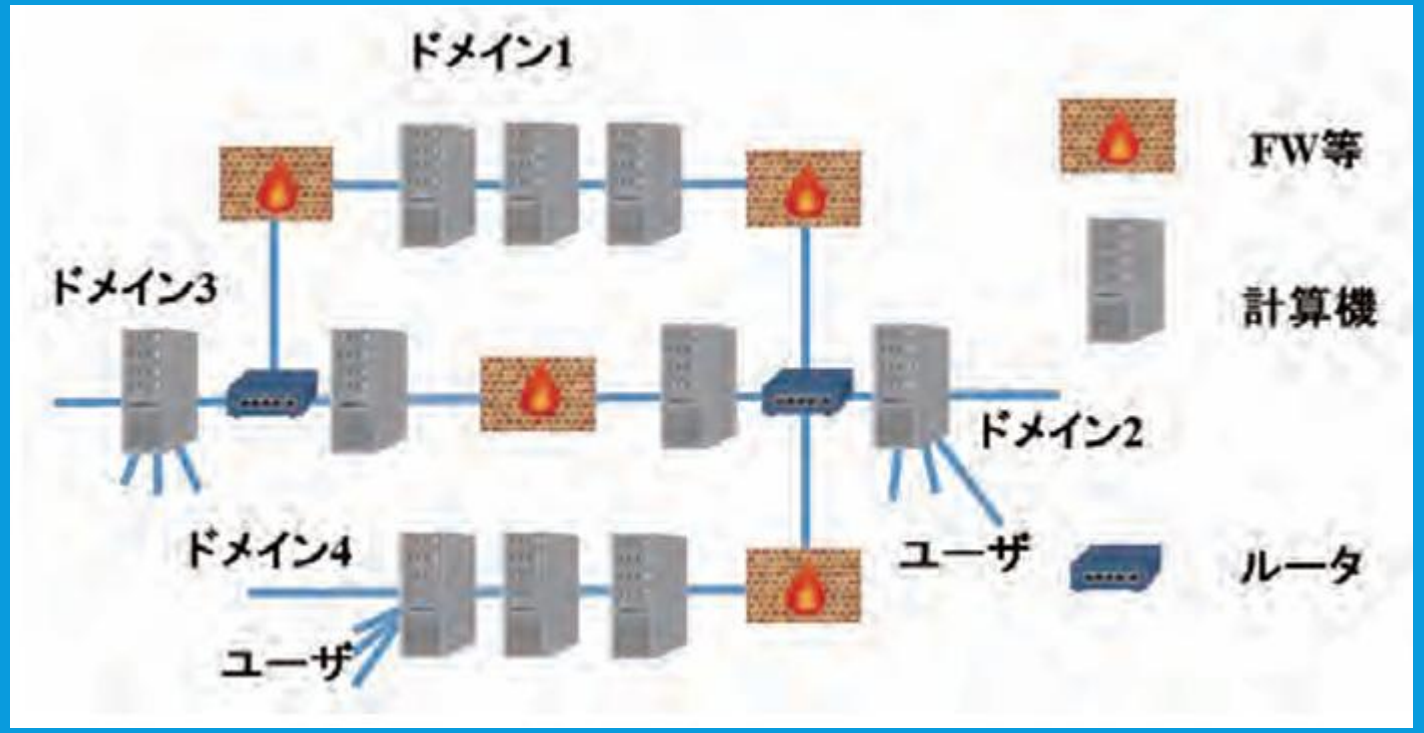
三つのレベルの対策がある.

- (1)個別技術レベルの対策 — 量子コンピュータに対して格子暗号を用意するなど
- (2)ネットワークレベルの対策 — ネットワーク内にはドメインと呼ばれる「同一ポリシーの下でセキュリティが管理されている単位」がある. ⇒　ドメインの在り方

林が最近考えていること⇒　(2)

ネットワークレベルでの対策

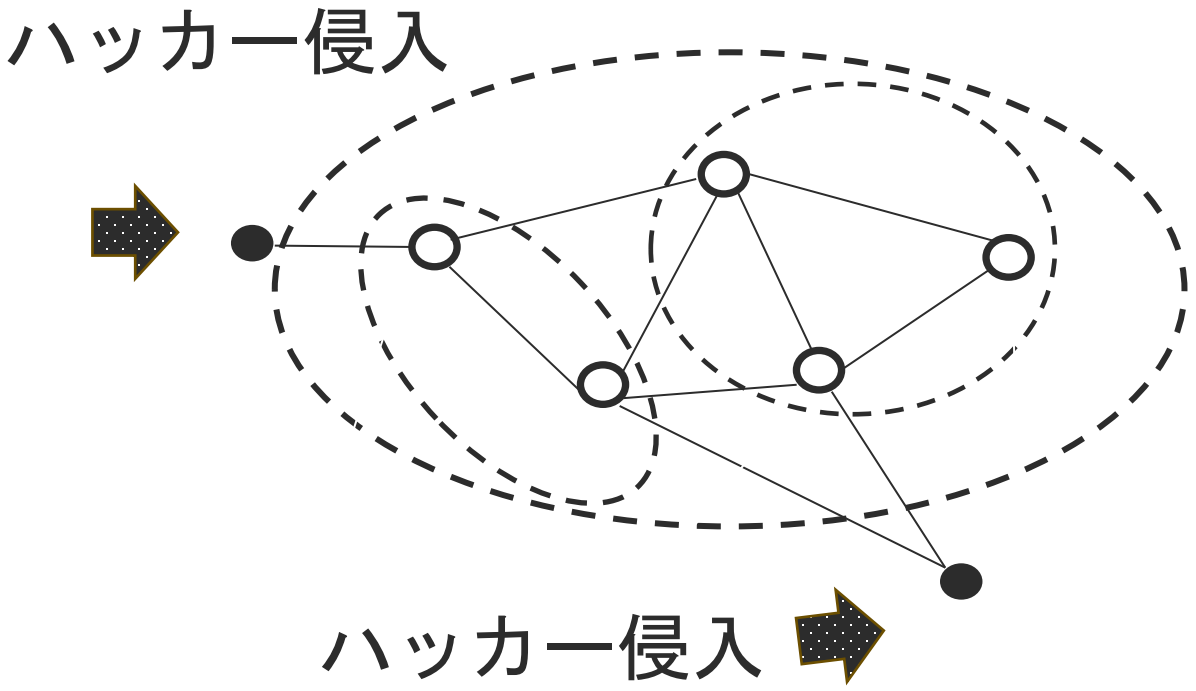
ドメイン：同一のポリシーの下でセキュリティ対策が施される単位
⇒　単一企業内ネットワークなど



FW: ファイアウォール

ドメインのイメージ

ドメイン：同一のポリシーの下でセキュリティ対策が施される単位
⇒　単一企業内ネットワークなど

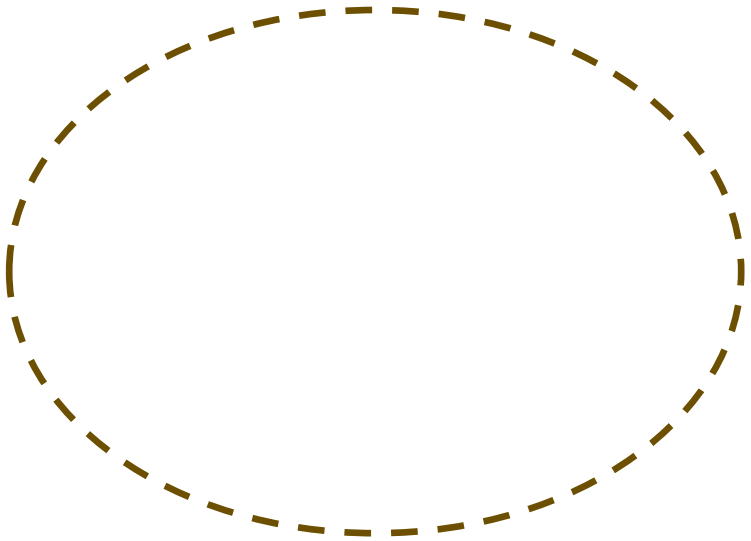


ドメイン

ハッカーはどこかのノードから侵入し，各ドメインを突破し，データを盗む，あるいは改ざんする．

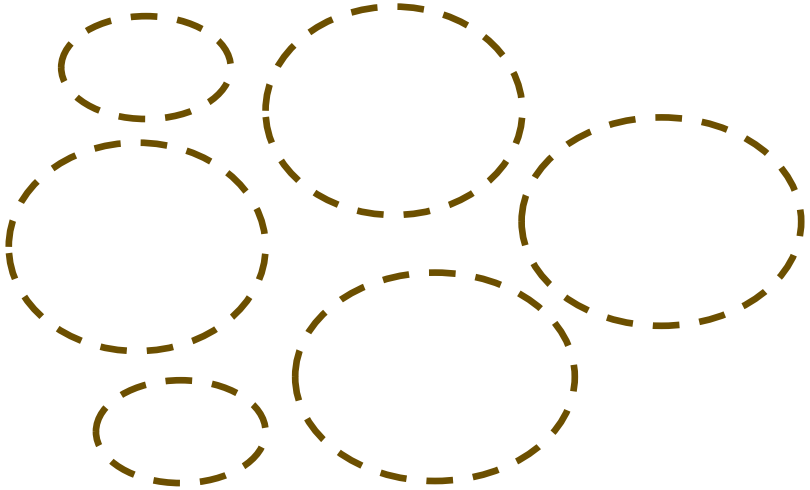
セキュリティ対策の観点からのドメインの在り方を検討すべき？

巨大で強力な一つのドメインを用意！



管理は楽になるが，万が一突破されると深刻な事態発生！

一つ一つのドメインの強度は弱いが，多数用意！



小さな被害がそこそこ発生！

中間に解あり？

前頁の考え方に基づいた，秘密分散の効果検証の研究を現在実行中！

谷瀬，他，“秘密分散化のシェア配置に関するセキュリティ強度の新評価法“，日本信頼性学会論文誌, vol. 46, no. 5 pp. 245-259, 2024.

カスケード故障について

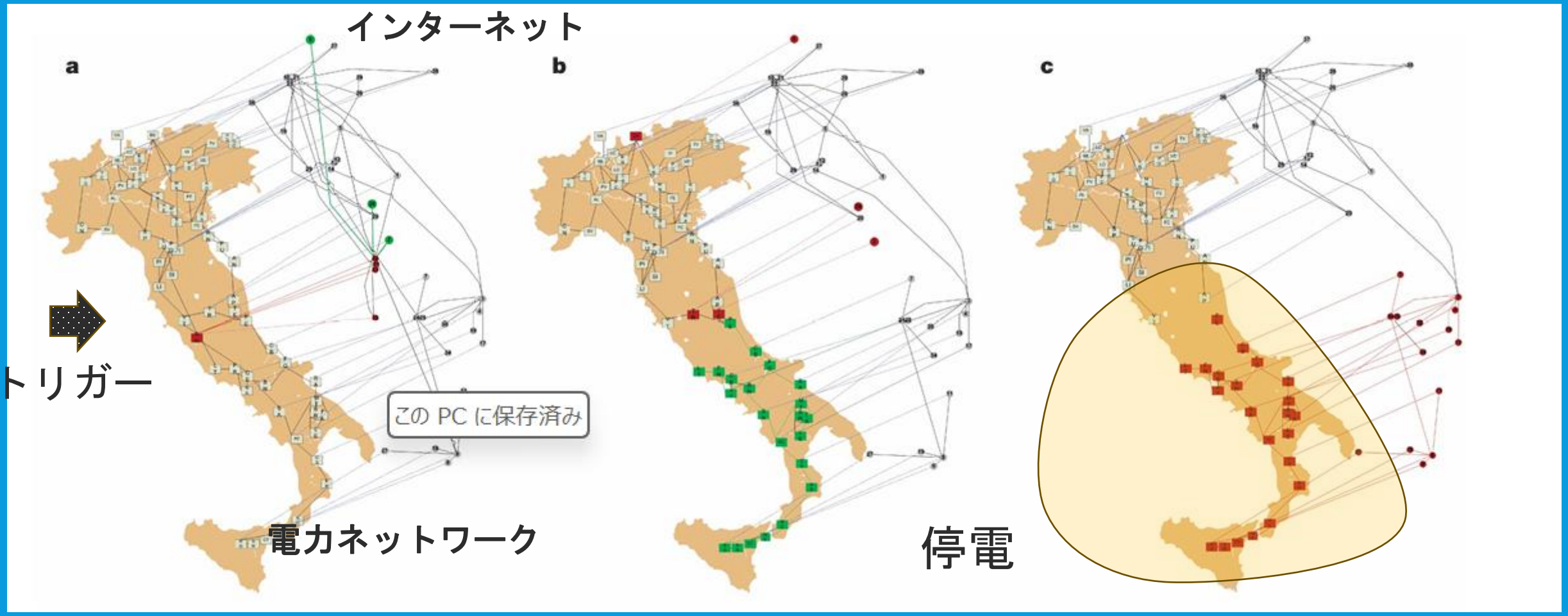
小さな障害(トリガー: セキュリティに限らない)が別のネットワーク障害を引き起こし，これが，元のネットワークの障害を引き起こし，…を繰り返すことで，大規模災害に匹敵する被害が発生する，

⇒ 現実に発生(イタリア，2003年9月)

カスケード故障！

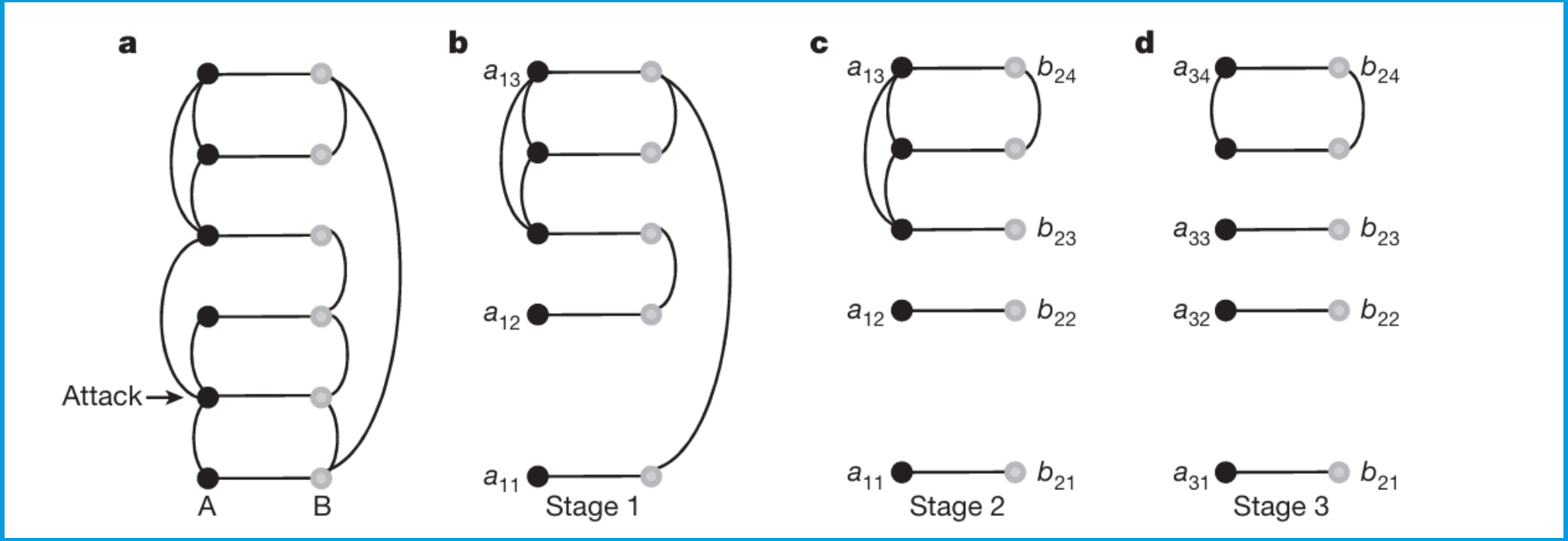
電力ネットワーク断　→　インターネット断　→　電力ネットワーク断　→　…

a ➡ b ➡ c



S. V. Buldyrev, et al., “Catastrophic cascade of failures in interdependent networks”, Nature, vol. 464, no. 15 pp. 1025-1028, 2010.

前頁の原理　a ➡ b ➡ c ➡ d



●と●が繋がらないとと，それらに対応する○と○も繋がらなくなる．⇒　繰り返し

2018年の北海道胆振地方東部地震による北海道大停電も，恐らくカスケード故障の1つ！

M. Hayashi, “A new study on cascading failures in power networks “, ICETC, D4-2. 2020.

カスケード故障はこれからも実際に発生すると考えられる.

一応，林の研究によれば，冗長構成(予備の経路など）を事前に確保すれば，カスケード故障の発生の程度は引き下げられる.

しかし，複数のネットワークの相互作用を考慮に入れると，ネットワーク中のどの部分を冗長化すれば効率的かはなかなか分からない.

既存の信頼性工学などを用いて，適切な冗長構成は明らかにできるであろうが，解析が対象が大規模すぎて，解析が容易ではない.

計算機の発達で高速計算ができるようになれば，
解析の見込みができる可能性がある.

まとめと今後

サーバー攻撃攻撃は深刻化している　⇒　実態紹介

セキュリティの関連する技術革新も進んでいる.

⇒　量子コンピュータ，秘密計算，ブロックチェーン

対策には二つのレベルがある.

⇒　(1)個別技術レベル　⇒　(2)ネットワークレベル

(2) に着目！

⇒ ドメインの在り方を考える！

カスケード故障の研究動向の一部を紹介.

今後，ドメインの在り方と，カスケード故障分析を軸とした検討を行う.